Entwicklerhandbuch

AWS Config

Copyright © 2025 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

AWS Config: Entwicklerhandbuch

Copyright © 2025 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Die Handelsmarken und Handelsaufmachung von Amazon dürfen nicht in einer Weise in Verbindung mit nicht von Amazon stammenden Produkten oder Services verwendet werden, durch die Kunden irregeführt werden könnten oder Amazon in schlechtem Licht dargestellt oder diskreditiert werden könnte. Alle anderen Handelsmarken, die nicht Eigentum von Amazon sind, gehören den jeweiligen Besitzern, die möglicherweise zu Amazon gehören oder nicht, mit Amazon verbunden sind oder von Amazon gesponsert werden.

Table of Contents

Was ist AWS Config? ... 1
Überlegungen ... 1
Verwendungsmöglichkeiten AWS Config ... 1
Verwaltung von Ressourcen ... 2
Überprüfung und Compliance ... 2
Verwalten von Konfigurationsänderungen und Beheben von Problemen, die dabei auftreten können ... 2
Sicherheitsanalyse ... 2
Partnerlösungen ... 3
Features ... 3
Wie AWS Config funktioniert ... 4
Entdeckung von Ressourcen ... 5
Nachverfolgung von Ressourcen ... 6
Lieferung von Konfigurationselementen ... 6
Steuern Sie den Zugriff auf AWS Config ... 10
Terminologie und Konzepte ... 10
AWS Config Schnittstellen ... 11
Ressourcenmanagement ... 12
Configuration Recorder ... 13
Übermittlungskanal ... 6
AWS Config Regeln ... 15
Konformitätspakete ... 19
Aggregatoren ... 20
AWS Serviceintegrationen ... 21
AWS Organizations ... 21
AWS Control Tower ... 21
AWS CloudTrail ... 22
AWS Security Hub ... 22
AWS Trusted Advisor ... 22
AWS Audit Manager ... 23
AWS Systems Manager ... 23
AWS Firewall Manager ... 24
EC2 Dedizierte Amazon-Hosts ... 24
Application Load Balancer ... 25

AWS CodeBuild ... 25
AWS X-Ray ... 25
AWS Service Management Connector ... 25
Amazon API Gateway ... 26
Unterstützung von Regionen ... 26
Überlegungen ... 26
Liste der unterstützten Regionen ... 27
Service Limits ... 31
Zusätzliche Informationen ... 34
AWS Software-Entwicklungskits für AWS Config ... 35
Erste Schritte ... 37
Melde dich an für AWS ... 37
Melde dich an für ein AWS-Konto ... 37
Erstellen eines Benutzers mit Administratorzugriff ... 38
Möglichkeiten zum Einstieg mit AWS Config ... 39
Einrichten von (Konsole) ... 39
Einrichtung ... 39
Einrichtung mit einem Klick ... 40
Manuelle Einrichtung ... 44
Einrichtung (AWS CLI) ... 51
Einrichtung ... 52
Voraussetzungen ... 52
Beginnend AWS Config ... 118
Überprüfen der Einrichtung ... 122
Arbeitet mit AWS SDKs ... 124
Configuration Recorder ... 126
Überlegungen zum vom Kunden verwalteten Konfigurationsrekorder ... 127
Überlegungen zu serviceverknüpften Konfigurationsrekordern ... 128
Unterstützte Services ... 129
Drifterkennung für den Konfigurationsrekorder ... 129
Starten des vom Kunden verwalteten Konfigurationsrekorders ... 130
Den vom Kunden verwalteten Konfigurationsrekorder beenden ... 130
Änderung der Aufzeichnungsfrequenz für den vom Kunden verwalteten Konfigurationsrekorder ... 131
Umbenennen des vom Kunden verwalteten Konfigurationsrekorders ... 134
Ihre Konfigurationsrekorder anzeigen ... 135

Löschen Ihrer Konfigurationsrekorder ... 137
Übermittlungskanal ... 138
Überlegungen ... 138
Terminologie ... 139
Komponenten eines Konfigurationselements ... 140
Den Lieferkanal anzeigen ... 143
Aktualisieren des Übermittlungskanals ... 144
Umbenennen des Übermittlungskanals ... 148
Bereitstellung von Konfigurations-Snapshots ... 149
Bereitstellung von Konfigurations-Snapshots ... 150
Überprüfen des Übermittlungsstatus ... 150
Konfigurations-Snapshots anzeigen ... 151
Konfigurations-Snapshots anzeigen ... 151
Beispiel für einen Konfigurations-Snapshot ... 152
Beispielbenachrichtigungen ... 157
Beispiel für Benachrichtigungen bei Änderung eines Konfigurationselements ... 158
Beispiel einer Benachrichtigung über den Konfigurationsverlauf ... 174
Beispiel einer Benachrichtigung über den Beginn der Lieferung eines Konfigurations-Snapshot ... 175
Beispiel einer Benachrichtigung über die Lieferung eines Konfigurations-Snapshots ... 175
Beispiel einer Benachrichtigung über eine Compliance-Änderung ... 176
Beispiel einer Benachrichtigung über den Beginn der Bewertung von Regeln ... 180
Beispiel einer Benachrichtigung über die Änderung eines übergroßen Konfigurationselements ... 181
Beispiel einer Benachrichtigung über eine fehlgeschlagene Sendung ... 184
AWS Config Armaturenbrett ... 186
Compliance und Ressourcenbestand ... 186
AWS Config Nutzungs- und Erfolgsmetriken ... 188
Ressourcenmanagement ... 192
Unterstützte Ressourcentypen ... 193
Amazon AppStream ... 194
Amazon AppFlow ... 195
... 195
Amazon API Gateway ... 195
Amazon Athena ... 196
Amazon Bedrock ... 197

Amazon CloudFront 197
Amazon CloudWatch 198
Amazon CodeGuru 198
Amazon Cognito 199
Amazon Connect 200
Amazon Detective 201
Amazon-DynamoDB 201
Amazon EC2 201
Amazon ECR 210
Amazon ECS 211
Amazon EFS 212
Amazon EKS 212
Amazon EMR 213
Amazon EventBridge 213
Amazon Forecast 214
Amazon Fraud Detector 214
Amazon GuardDuty 215
Amazon Inspector 216
Amazon IVS 216
Amazon Keyspaces 217
OpenSearch Amazon-Dienst 217
Amazon Personalize 218
Amazon Pinpoint 219
Amazon QLDB 220
Amazon Kendra 220
Amazon Kinesis 220
Amazon Lex 221
Amazon Lightsail 221
Amazon Lookout für Metrics 222
Amazon Lookout für Vision 222
Amazon Macie 223
Amazon Managed Grafana 223
Amazon Managed Service für Prometheus 223
Amazon MemoryDB 223
Amazon MQ 224
Amazon MSK 224

Amazon QuickSight 225
Amazon Redshift 225
Amazon RDS 227
Amazon Route 53 228
Amazon SageMaker KI 230
Amazon SES 231
Amazon SNS 232
Amazon SQS 232
Amazon S3 232
Amazon WorkSpaces 234
AWS Amplify 235
AWS AppConfig 235
AWS App Runner 236
AWS App Mesh 237
AWS AppSync 238
AWS Audit Manager 238
AWS Auto Scaling 238
AWS Backup 239
AWS Batch 240
AWS Budgets 241
AWS Certificate Manager 241
AWS CloudFormation 241
AWS CloudTrail 242
AWS Cloud9 242
AWS Cloud Map 243
AWS CodeArtifact 243
AWS CodeBuild 244
AWS CodeDeploy 244
AWS CodePipeline 245
AWS Config 245
AWS DMS 246
AWS DataSync 247
AWS Device Farm 248
AWS Elastic Beanstalk 249
AWS FIS 250
AWS Global Accelerator 250

AWS Glue ... 251
AWS Ground Station ... 251
AWS HealthLake ... 252
AWS ICH BIN ... 252
AWS IoT ... 253
AWS KMS ... 257
AWS Lambda ... 257
AWS Mainframe Modernization ... 258
AWS Network Firewall ... 258
AWS Network Manager ... 259
AWS Panorama ... 260
AWS Private CA ... 261
AWS Resilience Hub ... 261
AWS Ressourcen Explorer ... 262
AWS RoboMaker ... 262
AWS Signer ... 263
AWS Secrets Manager ... 263
AWS Security Hub ... 263
AWS Service Catalog ... 263
AWS Shield ... 264
AWS Step Functions ... 265
AWS Systems Manager ... 265
AWS Transfer Family ... 266
AWS WAF ... 266
AWS X-Ray ... 268
Elastic Load Balancing ... 269
MediaConnect ... 270
MediaPackage ... 270
MediaTailor ... 271
Ressourcenabdeckung nach regionaler Verfügbarkeit ... 271
Nord- und Südamerika ... 271
Europa ... 313
Asien-Pazifik ... 348
China ... 394
Afrika und Naher Osten ... 413
GovCloud ... 440

AWS Ressourcen aufzeichnen ... 463
Überlegungen ... 464
Regionale und globale Ressourcen ... 465
AWS Config Regeln und globale Ressourcentypen ... 469
Aufnahmefrequenz ... 470
Nicht aufgezeichnete Ressourcen ... 471
Ressourcen aufzeichnen (Konsole) ... 472
Ressourcen aufzeichnen (AWS CLI) ... 476
Ressourcen ausschließen ... 484
Die Aufnahme wird beendet ... 485
Aufzeichnen von Ressourcen von Drittanbietern (AWS CLI) ... 485
Ressourcen hinzufügen ... 486
Konfigurationselemente aufzeichnen ... 490
Konfigurationselemente lesen ... 490
Löschen von Ressourcen ... 492
Aufzeichnen von Softwarekonfigurationen ... 492
Voraussetzungen ... 492
Softwarekonfigurationen aufzeichnen ... 493
Ressourcen nachschlagen ... 495
Ressourcen anzeigen ... 497
Anzeigen der Compliance (Konsole) ... 497
Konformität anzeigen (AWS SDKs) ... 498
Anzeigen des Compliance-Verlaufs ... 504
Konformitätsverlauf anzeigen (Konsole) ... 505
Konformitätsverlauf anzeigen (AWS CLI) ... 505
Für Ressourcen und Regeln ... 511
Abfragen des Compliance-Verlaufs ... 513
Markieren Ihrer Ressourcen ... 514
Einschränkungen beim Markieren ... 514
Verwaltung von Tags mit AWS Config API-Aktionen ... 515
AWS Config ... 516
Überlegungen ... 516
Unterstützung von Regionen ... 519
Komponenten einer Regel ... 527
So funktionieren AWS Config Regeln ... 528
Auslösertypen ... 529

Evaluierungsmodi ... 530
Regel-Metadaten ... 531
Verwaltete Regeln ... 533
Liste der verwalteten -Regeln ... 534
Liste der verwalteten Regeln nach Auswertungsmodus ... 1019
Liste der verwalteten Regeln nach Auslösertyp ... 1042
Liste der verwalteten Regeln nach Regionen und Verfügbarkeit ... 1064
Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen ... 1618
Benutzerdefinierte Regeln ... 1620
Benutzerdefinierte Richtlinienregeln ... 1620
Benutzerdefinierte Lambda-Regeln ... 1620
Formatunterschiede für benutzerdefinierte Regeln AWS Config ... 1621
Erstellen von benutzerdefinierten Richtlinienregeln ... 1621
Erstellen von benutzerdefinierten Lambda-Regeln ... 1628
Gelöschte Ressourcen für benutzerdefinierte Lambda-Regeln verwalten ... 1651
Serviceverknüpfte Rollen ... 1653
Organisatorische Regeln ... 1654
Überlegungen ... 1654
Bereitstellung ... 1656
Unterstützung von Regionen ... 1656
Regeln hinzufügen ... 1660
Verwenden der Konsole ... 1660
Mit dem AWS SDKs ... 1664
Regeln aktualisieren ... 1667
Verwenden der Konsole ... 1668
Mit dem AWS SDKs ... 1668
Regeln löschen ... 1672
Überlegungen ... 1672
Verwenden der Konsole ... 1673
Mit dem AWS SDKs ... 1674
Regeln anzeigen ... 1676
Verwenden der Konsole ... 1676
Mit dem AWS SDKs ... 1677
Proaktive Bewertung aktivieren ... 1686
Verwenden der Konsole ... 1687
Verwenden des AWS SDKs ... 1690

Bewertungen an Security Hub senden ... 1694
Senden von Regelauswertungen an Security Hub ... 1694
Auswerten von Ressourcen mit -Regeln ... 1694
Löschen von Auswertungsergebnissen ... 1699
Fehlerbehebung ... 1700
Konformitätspakete ... 1703
Dashboard für Konformitätspakete ... 1704
Navigieren auf der zentralen Seite für Konformitätspakete ... 1704
Voraussetzungen ... 1705
Schritt 1: Starten Sie AWS Config die Aufnahme ... 1705
Schritt 2: Zusätzliche Voraussetzungen je nach Conformance Pack-Typ ... 1705
Unterstützung von Regionen ... 1711
Prozessprüfungen ... 1718
Beispielvorlage ... 1719
Prozessprüfungen erstellen ... 1720
Der Konformitätsstatus wird geändert ... 1720
Ansehen und Bearbeiten ... 1722
Beispielvorlagen für Konformitätspakete ... 1722
AWS Control Tower Detective Guardrails Konformitätspaket ... 1727
Bewährte Methoden für den Betrieb von ABS CCIG 2.0 Material Workloads ... 1727
Bewährte Methoden für den Betrieb von ABS CCIG 2.0 Standard Workloads ... 2001
Bewährte Methoden für die Implementierung von ACSC Essential 8 ... 2199
Bewährte Methoden für die Implementierung von ACSC ISM ... 2229
Bewährte Methoden für die Ausführung von KI und ML ... 2388
Bewährte Methoden für die Implementierung von Amazon API Gateway ... 2388
Bewährte Betriebspraktiken für Amazon CloudWatch ... 2388
Bewährte Methoden für die Ausführung von Amazon DynamoDB ... 2388
Bewährte Methoden für die Ausführung von Amazon S3 ... 2388
Bewährte Methoden für die Implementierung von APRA CPG 234 ... 2389
Bewährte Methoden für die Ausführung des Asset-Managements ... 2660
Bewährte Methoden für die Ausführung von AWS Backup ... 2661
Operative Best Practices für AWS Identitäts- und Zugriffsmanagement ... 2661
Operative Best Practices für die AWS Zuverlässigkeit eines gut konzipierten Frameworks 2661
Bewährte betriebliche Verfahren für die AWS Sicherheitssäule eines Well-Architected Frameworks ... 2759
Bewährte Methoden für die Ausführung von BCP und DR ... 2966

Bewährte Betriebspraktiken für BNM T RMi 2967
Bewährte Methoden für das Canadian Centre for Cyber Security (CCCS)-Medium-Cloud-Kontrollprofil 3326
Best Practices für den Betrieb von CIS AWS Foundations Benchmark v1.4 Level 1 5110
Best Practices für den Betrieb von CIS AWS Foundations Benchmark v1.4 Level 2 5154
Bewährte Betriebspraktiken für kritische Sicherheitskontrollen der GUS v8 IG1 5215
Bewährte Betriebspraktiken für kritische Sicherheitskontrollen der GUS v8 IG2 5331
Bewährte Betriebspraktiken für kritische Sicherheitskontrollen der GUS v8 IG3 5537
Bewährte Methoden für die Ausführung von CIS Top 20 5760
Bewährte Methoden für die Ausführung von CISA Cyber Essentials 5854
Bewährte Methoden für die Ausführung von Criminal Justice Information Services (CJIS) 6103
Bewährte Methoden für die Ausführung von CMMC 2.0 Level 1 6257
Bewährte Methoden für die Ausführung von CMMC 2.0 Level 2 6400
Bewährte Methoden für die Ausführung von Datenverarbeitungsservices 6891
Bewährte Methoden für die Erreichung von Ausfallsicherheit 6891
Bewährte Methoden für die Ausführung von Datenbankservices 6891
Bewährte Methoden für die Ausführung von Data Lakes und Analyseservices 6891
Bewährte Methoden für die Ausführung von DevOps 6892
Bewährte Methoden für die Ausführung von EC2 6892
Bewährte Methoden für die Verwendung von Verschlüsselung und Schlüsselverwaltung ... 6892
Leitfaden für bewährte Betriebspraktiken für die ENISA-Cybersicherheit für SMEs 6893
Bewährte Methoden für die Implementierung des Esquema Nacional de Seguridad (ENS) Low 7123
Bewährte Methoden für die Implementierung des Esquema Nacional de Seguridad (ENS) Medium 7253
Bewährte Methoden für die Implementierung des Esquema Nacional de Seguridad (ENS) High 7401
Betriebliche bewährte Methoden für FDA Titel 21 CFR Teil 11 7563
Bewährte Methoden zur Implementierung von FedRAMP(Low) 8038
Bewährte Methoden für die Ausführung von FedRAMP(Moderate) 8357
Bewährte Betriebspraktiken für FedRAMP (High Part 1) 9015
Bewährte Betriebspraktiken für FedRAMP (High Part 2) 9720
Betriebliche bewährte Methoden für FFIEC 9873
Bewährte Methoden für die Implementierung des deutschen Kriterienkatalogs C5 (Cloud Computing Compliance Criteria Catalogue) 10142
Bewährte Methoden für die Implementierung des Gramm Leach Bliley Act (GLBA) 10245

Bewährte Methoden für die Implementierung Anhang 11 zum EG-Leitfaden der Guten Herstellungspraxis 10307
Betriebliche bewährte Methoden für die HIPAA-Sicherheit 10492
Bewährte Methoden für die Ausführung von IRS 1075 11064
Bewährte Methoden zur Ausführung von K-ISMS 11314
Bewährte Methoden für die Ausführung von Load Balancing 11417
Betriebliche bewährte Methoden für die Protokollierung 11417
Bewährte Methoden für die Ausführung von Management- und Governance-Services 11417
Bewährte Methoden für die Verwendung der MAS Notice 655 11417
Bewährte Methoden für die Ausführung von MAS TRMG 11467
Bewährte Methoden für die Überwachung 11744
Bewährte Methoden für die Implementierung von NBC TRMG 11744
Bewährte Methoden für die Ausführung von NERC CIP BCSI 12337
Bewährte Methoden für die Ausführung von NCSC-Cloud-Sicherheitsprinzipien 12410
Bewährte Methoden für die Implementierung des Cyber Assessment Framework des NCSC 12542
Bewährte Methoden für die Ausführung von Services für Netzwerke und zur Bereitstellung von Inhalten 12763
Bewährte Methoden für die Implementierung von NIST 800-53 Rev. 4 12763
Bewährte Methoden für die Ausführung von NIST 800-53 Rev. 5 13157
Bewährte Methoden für die Ausführung von NIST 800 171 13953
Bewährte Methoden für die Ausführung von NIST 800 172 14363
Bewährte Methoden für die Ausführung von NIST 800 181 14449
Bewährte Methoden für die Ausführung von NIST 1800 25 15064
Bewährte Methoden für die Ausführung von NIST CSF 15271
Bewährte Betriebspraktiken für NIST Privacy Framework v1.0 15710
Bewährte Methoden für die Ausführung von NYDFS 23 16009
Bewährte Betriebspraktiken für NZISM 3.8 16252
Bewährte Methoden für die Ausführung von PCI DSS 3.2.1 16428
Operative Best Practices für PCI DSS 4.0 (ohne globale Ressourcentypen) 16811
Operative Best Practices für PCI DSS 4.0 (einschließlich globaler Ressourcentypen) 17194
Bewährte Methoden für die Ausführung von öffentlich zugänglichen Ressourcen 17661
Operative Best Practices für das RBI Cyber Security Framework für UCBs 17661
Bewährte Methoden für die Ausführung von RBI MD-ITF 17720
Bewährte Methoden für Sicherheits-, Identitäts- und Compliance-Services 17901
Bewährte Methoden für die Ausführung von Serverless 17901

Bewährte Methoden für die Ausführung von Speicherservices 17901
Bewährte Methoden für die Ausführung von SWIFT-CSP 17902
Bewährte Methoden für die Sicherheit in Amazon Elastic Container Service (Amazon ECS) 17945
Bewährte Methoden für die Sicherheit in Amazon Elastic File System (Amazon EFS) 17945
Bewährte Methoden für die Sicherheit in Amazon Elastic Kubernetes Service (Amazon EKS) 17945
Bewährte Sicherheitsmethoden für Amazon CloudFront 17946
Bewährte Sicherheitsmethoden für Amazon OpenSearch Service 17946
Bewährte Methoden für die Sicherheit in Amazon Redshift 17946
Bewährte Methoden für die Sicherheit in Amazon Relational Database Service (Amazon RDS) 17946
Bewährte Sicherheitsmethoden für AWS Auto Scaling 17947
Bewährte Sicherheitsmethoden für AWS CloudTrail 17947
Bewährte Sicherheitsmethoden für AWS CodeBuild 17947
Bewährte Methoden für die Sicherheit in Amazon ECR 17948
Bewährte Sicherheitsmethoden für AWS Lambda 17948
Bewährte Sicherheitsmethoden für AWS Network Firewall 17948
Bewährte Sicherheitsmethoden für Amazon SageMaker AI 17948
Bewährte Sicherheitsmethoden für AWS Secrets Manager 17949
Bewährte Sicherheitsmethoden für AWS WAF 17949
Beispielvorlagen mit Korrekturmaßnahmen 17949
Benutzerdefinierte Vorlagen erstellen 17950
Terminologie 17950
Anpassen der Vorlage 17950
Bereitstellung von Conformance Packs 17955
Conformance Packs bearbeiten 17958
Löschen von Conformance Packs 17960
Überlegungen 17960
Um ein Conformance Pack zu löschen 17961
Conformance Packs anzeigen 17962
Anzeigen des Compliance-Verlaufs 17965
Anzeigen der Compliance-Zeitleiste 17966
Abfragen des Compliance-Verlaufs 17966
Verwalten von Konformitätspaketen für Organisationen 17968
Überlegungen 17968

Bereitstellung ... 17970
Unterstützung von Regionen ... 17970
Fehlerbehebung ... 17974
Status „Fehlgeschlagen“ für ein Conformance Pack ... 17975
Hängende Regeln in einem Konformitätspaket ... 17976
Abhilfe ... 17978
Unterstützung von Regionen ... 17978
Manuelle Problembehebung einrichten ... 17982
Automatische Problembehebung einrichten ... 17984
Löschen von Behebungsmaßnahmen ... 17986
Aggregatoren ... 17988
Anwendungsfälle ... 17988
Terminologie ... 17989
Unterstützung von Regionen ... 17989
Aggregator-Dashboard ... 17994
Verwenden des Aggregator-Dashboards ... 17994
Compliance-Dashboard ... 17997
Inventory-Dashboard ... 18000
Aggregatoren erstellen ... 18002
Registrierung eines delegierten Administrators ... 18008
Aggregatoren bearbeiten ... 18010
Aggregatoren löschen ... 18012
Autorisieren von Aggregator-Konten ... 18012
Überlegungen ... 18013
Autorisierung wird hinzugefügt ... 18013
Autorisierungen löschen ... 18015
Überlegungen ... 18015
Autorisierung wird gelöscht ... 18016
Aggregatoren anzeigen ... 18016
Fehlerbehebung ... 18018
Erweiterte Abfragen ... 18020
Features ... 18021
Abfragekomponenten ... 18021
Syntax ... 18021
Parameter ... 18022
Beispiele ... 18022

Abfrage-Editor (Konsole) ... 18023
Überlegungen ... 18023
Verwenden Sie eine AWS Beispielabfrage ... 18024
Erstellen einer benutzerdefinierten Abfrage ... 18024
Abfrage-Editor (AWS CLI) ... 18025
Überlegungen ... 18025
Abfragen von Konfigurationsdaten für Ressourcen ... 18026
Speichern einer Abfrage ... 18028
Anzeigen aller gespeicherten Abfragen ... 18028
Abrufen von Details zu einer gespeicherten Abfrage ... 18029
Löschen einer gespeicherten Abfrage ... 18030
Prozessor für Abfragen in natürlicher Sprache ... 18030
Überlegungen ... 18030
Abfragen mithilfe des Abfrageprozessors für natürliche Sprache ... 18024
Beispielaufforderungen ... 18032
Feedback geben ... 18035
Unterstützung von Regionen ... 18036
Beispiele für Abfragen ... 18036
Beispiel für Beziehungsabfragen ... 18042
Einschränkungen ... 18044
CIDR-Bereich notation/IP ... 18046
Mehrere Eigenschaften innerhalb eines Arrays ... 18047
Unterstützung von Regionen ... 18048
Löschen von -Daten ... 18053
Festlegen des Aufbewahrungszeitraums für Daten (Konsole) ... 18055
Sicherheit ... 18057
Datenschutz ... 18058
Verschlüsseln von Daten während der Übertragung. ... 18059
Verschlüsseln von Daten während der Übertragung. ... 18059
Identitäts- und Zugriffsverwaltung ... 18059
Zielgruppe ... 18060
Authentifizierung mit Identitäten ... 18060
Verwalten des Zugriffs mit Richtlinien ... 18064
Wie AWS Config funktioniert mit IAM ... 18067
Beispiele für identitätsbasierte Richtlinien ... 18075
AWS verwaltete Richtlinien ... 18094

Berechtigungen für die IAM-Rolle ... 18260
Aktualisieren der IAM-Rolle ... 18264
Berechtigungen für den Amazon S3 S3-Bucket ... 18266
Berechtigungen für den KMS-Schlüssel ... 18271
Berechtigungen für das Amazon-SNS-Thema ... 18274
Fehlerbehebung ... 18277
Verwenden von serviceverknüpften Rollen ... 18279
Vorfallreaktion ... 18282
Compliance-Validierung ... 18282
Ausfallsicherheit ... 18284
Sicherheit der Infrastruktur ... 18284
Konfigurations- und Schwachstellenanalyse ... 18285
Serviceübergreifende Confused-Deputy-Prävention ... 18285
Bewährte Methoden ... 18286
Protokollieren und Überwachen ... 18287
Protokollierung ... 18287
AWS Config Informationen in CloudTrail ... 18287
Grundlegendes zu AWS Config Protokolldateieinträgen ... 18289
Beispiele für Protokolldateien ... 18289
Überwachen ... 18297
Verwenden von Amazon SQS ... 18297
Amazon verwenden EventBridge ... 18300
Amazon VPC-Endpunkte ... 18307
Erstellen eines VPC-Endpunktes ... 18307
FAQs ... 18308
Meine letzten Konfigurationsänderungen können nicht angezeigt werden ... 18308
Kann ich damit rechnen, dass ich meine Konfigurationsänderungen sofort sehe? ... 18308
Indirekte Beziehungen in AWS Config ... 18308
Was ist eine Ressourcenbeziehung? ... 18308
Was ist eine direkte und eine indirekte Beziehung in Bezug auf eine Ressource? ... 18309
Welche indirekten Beziehungen werden AWS Config unterstützt? ... 18310
In welchen Szenarien werden indirekte Beziehungen verwendet? ... 18311
Wie werden die Konfigurationselemente aufgrund der direkten und indirekten Beziehung erstellt? ... 18313
Welche Konfigurationselemente werden aufgrund indirekter Beziehungen generiert? ... 18313
Wie deaktiviere ich die indirekte Beziehung? ... 18315

Wie rufe ich Konfigurationsdaten ab, die sich auf indirekte Beziehungen beziehen? 18316
Codebeispiele 18317
Grundlagen 18318
Aktionen 18318
Dokumentverlauf 18349
Frühere Aktualisierungen 18500
..... 18575

Was ist AWS Config?

AWS Config bietet einen detaillierten Überblick über die Konfiguration der AWS Ressourcen in Ihrem AWS Konto. Dazu gehört auch, wie die Ressourcen jeweils zueinander in Beziehung stehen und wie sie in der Vergangenheit konfiguriert wurden, damit Sie sehen können, wie sich die Konfigurationen und Beziehungen im Laufe der Zeit verändern.

Eine AWS Ressource ist eine Entität, mit der Sie arbeiten können AWS, z. B. eine Amazon Elastic Compute Cloud (EC2) -Instance, ein Amazon Elastic Block Store (EBS) -Volume, eine Sicherheitsgruppe oder eine Amazon Virtual Private Cloud (VPC). Eine vollständige Liste der AWS Ressourcen, die von unterstützt werden AWS Config, finden Sie unter. Unterstützte Ressourcentypen für AWS Config

Überlegungen

- AWS-Konto: Sie benötigen eine aktive AWS-Konto. Weitere Informationen finden Sie unter Registrierung für AWS.
- Amazon S3 S3-Bucket: Sie benötigen einen S3-Bucket, um Daten für Ihre Konfigurations-Snapshots und den Verlauf zu empfangen. Weitere Informationen finden Sie unter Berechtigungen für den Amazon-S3-Bucket.
- Amazon SNS-Thema: Sie benötigen ein Amazon SNS, um Benachrichtigungen zu erhalten, wenn es Änderungen an Ihren Konfigurations-Snapshots und Ihrem Verlauf gibt. Weitere Informationen finden Sie unter Berechtigungen für das Amazon SNS SNS-Thema.
- IAM-Rolle: Sie benötigen eine IAM-Rolle, die über die erforderlichen Zugriffsberechtigungen verfügt. AWS Config Weitere Informationen finden Sie unter Berechtigungen für die IAM-Rolle.
- Ressourcentypen: Sie können entscheiden, welche Ressourcentypen Sie aufzeichnen AWS Config möchten. Weitere Informationen finden Sie unter AWS Ressourcen aufzeichnen.

Verwendungsmöglichkeiten AWS Config

Wenn Sie Ihre Anwendungen darauf ausführen AWS, verwenden Sie in der Regel AWS Ressourcen, die Sie gemeinsam erstellen und verwalten müssen. Mit der steigenden Nachfrage nach Ihrer Anwendung wächst auch Ihr Bedarf, den Überblick über Ihre AWS Ressourcen zu behalten. AWS Config wurde entwickelt, um Ihnen bei der Verwaltung Ihrer Anwendungsressourcen in den folgenden Szenarien zu helfen:

Verwaltung von Ressourcen

Um die Konfigurationen der Ressourcen besser zu kontrollieren und Fehlkonfigurationen zu erkennen, benötigen Sie detaillierte Erkenntnisse darüber, welche Ressourcen vorhanden sind und wie diese Ressourcen zu jeder Zeit konfiguriert sind. Sie können es verwenden, AWS Config um Sie zu benachrichtigen, wenn Ressourcen erstellt, geändert oder gelöscht werden, ohne dass Sie diese Änderungen überwachen müssen, indem Sie die Aufrufe der einzelnen Ressourcen abfragen.

Sie können AWS Config Regeln verwenden, um die Konfigurationseinstellungen Ihrer AWS Ressourcen auszuwerten. Wenn AWS Config festgestellt wird, dass eine Ressource gegen die Bedingungen in einer Ihrer Regeln verstößt, wird die AWS Config Ressource als nicht konform gekennzeichnet und eine Benachrichtigung gesendet. AWS Config bewertet Ihre Ressourcen kontinuierlich, wenn sie erstellt, geändert oder gelöscht werden.

Überprüfung und Compliance

Möglicherweise arbeiten Sie mit Daten, die häufigen Überprüfungen unterliegen, um die Compliance mit internen Richtlinien und bewährten Methoden sicherzustellen. Um die Compliance nachzuweisen, benötigen Sie Zugriff auf historische Konfigurationen Ihrer Ressourcen. Diese Informationen werden bereitgestellt von AWS Config.

Verwalten von Konfigurationsänderungen und Beheben von Problemen, die dabei auftreten können

Wenn Sie mehrere AWS Ressourcen verwenden, die voneinander abhängen, kann eine Änderung der Konfiguration einer Ressource unbeabsichtigte Auswirkungen auf verwandte Ressourcen haben. Mit können Sie überprüfen AWS Config, wie die Ressource, die Sie ändern möchten, mit anderen Ressourcen zusammenhängt, und die Auswirkungen Ihrer Änderung abschätzen.

Sie können auch die von AWS Config bereitgestellten historischen Konfigurationen der Ressourcen nutzen, um Probleme zu beheben und auf die letzte als funktionierend bekannte Konfiguration einer Problemressource zuzugreifen.

Sicherheitsanalyse

Um potenzielle Sicherheitslücken zu analysieren, benötigen Sie detaillierte historische Informationen über Ihre AWS Ressourcenkonfigurationen, z. B. die AWS Identity and Access Management (IAM-) Berechtigungen, die Ihren Benutzern gewährt wurden, oder die EC2 Amazon-Sicherheitsgruppenregeln, die den Zugriff auf Ihre Ressourcen kontrollieren.

Sie können AWS Config damit jederzeit die IAM-Richtlinie einsehen, die einem Benutzer, einer Gruppe oder einer Rolle zugewiesen wurde, während der Aufzeichnung durchgeführt AWS Config wurde. Anhand dieser Informationen können Sie die Berechtigungen bestimmen, über die ein Benutzer zu einer bestimmten Zeit verfügt hat. Sie können beispielsweise ermitteln, ob der Benutzer `John Doe` am 1. Januar 2015 berechtigt war, Amazon-VPC-Einstellungen zu ändern.

Sie können AWS Config damit auch die Konfiguration Ihrer EC2 Sicherheitsgruppen anzeigen, einschließlich der Portregeln, die zu einem bestimmten Zeitpunkt geöffnet waren. Mit diesen Informationen können Sie bestimmen, ob eine Sicherheitsgruppe den eingehenden TCP-Datenverkehr für einen bestimmten Port blockiert hat.

Partnerlösungen

AWS arbeitet mit externen Spezialisten für Protokollierung und Analyse zusammen, um Lösungen bereitzustellen, die AWS Config Ergebnisse verwenden. Weitere Informationen finden Sie auf der AWS Config Detailseite unter AWS Config.

Features

Bei der Einrichtung AWS Config können Sie wie folgt vorgehen:

Ressourcenmanagement

- Geben Sie die Ressourcentypen an, die Sie aufzeichnen AWS Config möchten.

- Richten Sie einen Amazon-S3-Bucket für den Empfang eines Konfigurations-Snapshots (auf Anfrage) und eines Konfigurationsverlaufs ein.
- Richten Sie ein Amazon-SNS-Thema ein, um Benachrichtigungen für den Konfigurations-Stream zu senden.
- Gewähren Sie ihm AWS Config die Berechtigungen, die für den Zugriff auf den Amazon S3 S3-Bucket und das Amazon SNS SNS-Thema erforderlich sind.

  Weitere Informationen finden Sie unter AWS Ressourcenkonfigurationen und Verlauf anzeigen und AWS Ressourcenkonfigurationen und Verlauf verwalten.

Regeln und Conformance Packs

- Geben Sie die Regeln an, anhand derer Sie AWS Config die Konformitätsinformationen für die aufgezeichneten Ressourcentypen auswerten möchten.
- Verwenden Sie Konformitätspakete oder eine Sammlung von Regeln, die als eine Einheit in Ihrem AWS-Konto System bereitgestellt und überwacht werden können.

  Weitere Informationen finden Sie unter Evaluierung von Ressourcen mit AWS Config Regeln und Konformitätspaketen.

Problembehebung

- Korrigieren Sie Ressourcen, die nicht den Vorschriften entsprechen und von bewertet wurden. AWS-Config-Regeln

  Weitere Informationen finden Sie unter Problembehebung.

Aggregatoren

- Verwenden Sie einen Aggregator, um einen zentralen Überblick über Ihren Ressourcenbestand und die Compliance zu erhalten. Ein Aggregator sammelt AWS Config Konfigurations- und Compliance-Daten aus mehreren AWS-Konten AWS Regionen in einem einzigen Konto und einer Region.

  Weitere Informationen finden Sie unter Datenaggregation für mehrere Konten und Regionen.

Erweiterte Abfragen

- Verwenden Sie eine der Beispielabfragen oder schreiben Sie Ihre eigene Abfrage, indem Sie auf das Konfigurationsschema der AWS Ressource verweisen.

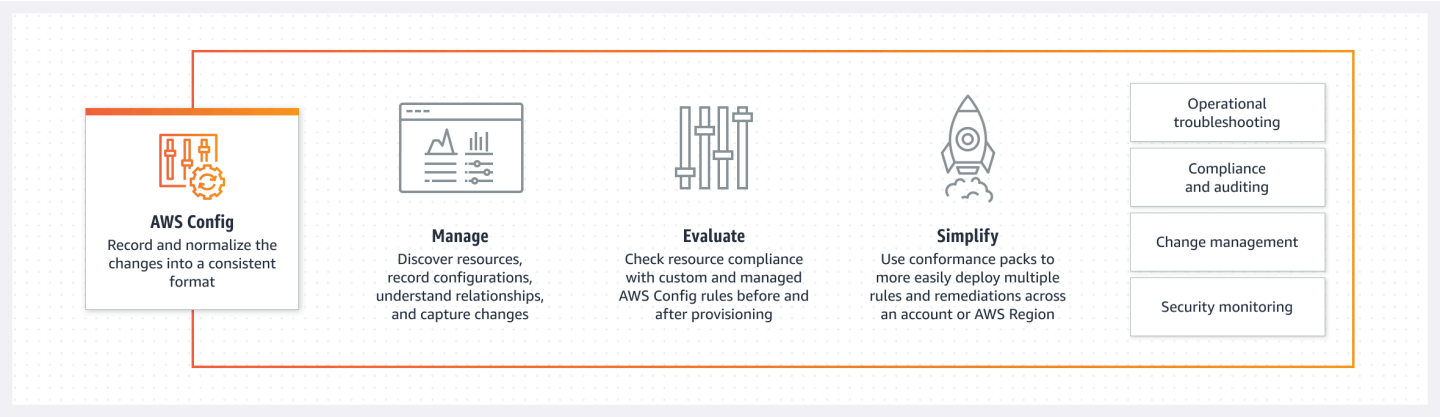
  Weitere Informationen finden Sie unter Abfragen des aktuellen Konfigurationsstatus von AWS Ressourcen.

Wie AWS Config funktioniert

AWS Config bietet eine detaillierte Ansicht der Konfiguration der AWS Ressourcen in Ihrem AWS Konto. Dazu gehört auch, wie die Ressourcen jeweils zueinander in Beziehung stehen und wie sie

in der Vergangenheit konfiguriert wurden, damit Sie sehen können, wie sich die Konfigurationen und Beziehungen im Laufe der Zeit verändern.

Eine AWS Ressource ist eine Entität, mit der Sie arbeiten können AWS, z. B. eine Amazon Elastic Compute Cloud (EC2) -Instance, ein Amazon Elastic Block Store (EBS) -Volume, eine Sicherheitsgruppe oder eine Amazon Virtual Private Cloud (VPC). Eine vollständige Liste der von unterstützten AWS Ressourcen finden Sie unter AWS Config. Unterstützte Ressourcentypen für AWS Config



Entdeckung von Ressourcen

Wenn Sie die Option aktivieren AWS Config, werden zunächst die unterstützten AWS Ressourcen erkannt, die in Ihrem Konto vorhanden sind, und für jede Ressource wird ein Konfigurationselement generiert.

AWS Config generiert außerdem Konfigurationselemente, wenn sich die Konfiguration einer Ressource ändert, und verwaltet historische Aufzeichnungen der Konfigurationselemente Ihrer Ressourcen ab dem Zeitpunkt, an dem Sie den Konfigurationsrekorder starten. AWS Config Erstellt standardmäßig Konfigurationselemente für jede unterstützte Ressource in der Region. Wenn Sie nicht Konfigurationselemente für alle unterstützten Ressourcen erstellen möchten AWS Config , können Sie die Ressourcentypen angeben, die nachverfolgt werden sollen.

Bevor Sie einen Ressourcentyp für AWS Config die Nachverfolgung angeben, überprüfen Sie die Ressourcenabdeckung nach regionaler Verfügbarkeit, um festzustellen, ob der Ressourcentyp in der AWS Region unterstützt wird, in der Sie die Einrichtung vornehmen AWS Config. Wenn ein Ressourcentyp AWS Config in mindestens einer Region unterstützt wird, können Sie die Aufzeichnung dieses Ressourcentyps in allen Regionen aktivieren, die von unterstützt werden AWS Config, auch wenn der angegebene Ressourcentyp in der AWS Region, in der Sie einrichten, nicht unterstützt wird AWS Config.

Nachverfolgung von Ressourcen

AWS Config verfolgt alle Änderungen an Ihren Ressourcen, indem es den Describe- oder den List-API-Aufruf für jede Ressource in Ihrem Konto aufruft. Der Service verwendet dieselben API-Aufrufe zur Erfassung von Konfigurationsdetails für alle zugehörigen Ressourcen.

Wenn Sie beispielsweise eine Ausgangsregel aus einer VPC-Sicherheitsgruppe entfernen, wird ein AWS Config Describe-API-Aufruf für die Sicherheitsgruppe aufgerufen. AWS Config ruft dann einen Describe-API-Aufruf für alle Instances auf, die der Sicherheitsgruppe zugeordnet sind. Die aktualisierten Konfigurationen der Sicherheitsgruppe (Ressource) und der einzelnen Instances (den zugehörigen Ressourcen) werden als Konfigurationselemente aufgezeichnet und in einem Konfigurations-Stream an einen Amazon Simple Storage Service (Amazon S3)-Bucket übermittelt.

AWS Config verfolgt auch die Konfigurationsänderungen, die nicht von der API initiiert wurden. AWS Config untersucht die Ressourcenkonfigurationen regelmäßig und generiert Konfigurationselemente für die Konfigurationen, die sich geändert haben.

Wenn Sie AWS Config Regeln verwenden, werden Ihre AWS Ressourcenkonfigurationen AWS Config kontinuierlich auf die gewünschten Einstellungen überprüft. Je nach Regel AWS Config werden Ihre Ressourcen entweder als Reaktion auf Konfigurationsänderungen oder in regelmäßigen Abständen bewertet. Jede Regel ist mit einer AWS Lambda -Funktion verknüpft, die eine für die Regel logische Auswertung enthält. Bei der AWS Config Auswertung Ihrer Ressourcen wird die Funktion der Regel aufgerufen. AWS Lambda Die Funktion gibt den Status der ausgewerteten Compliance-Ressourcen zurück. Wenn eine Ressource gegen die Bedingungen einer Regel verstößt, werden die Ressource und AWS Config die Regel als nicht konform gekennzeichnet. Wenn sich der Compliance-Status einer Ressource ändert, AWS Config sendet eine Benachrichtigung an Ihr Amazon SNS SNS-Thema.

Lieferung von Konfigurationselementen

AWS Config kann Konfigurationselemente über einen der folgenden Kanäle bereitstellen:

Amazon S3 Bucket

AWS Config verfolgt Änderungen an der Konfiguration Ihrer AWS Ressourcen und sendet regelmäßig aktualisierte Konfigurationsdetails an einen von Ihnen angegebenen Amazon S3 S3-Bucket. Für jeden AWS Config aufgenommenen Ressourcentyp wird alle sechs Stunden eine Konfigurationsverlaufsdatei gesendet. Jede Konfigurationsverlaufsdatei enthält Informationen zu den Ressourcen, die in diesem Zeitraum von sechs Stunden geändert wurden. Jede Datei enthält

Ressourcen eines Typs, z. B. EC2 Amazon-Instances oder Amazon EBS-Volumes. Wenn keine Konfigurationsänderungen vorgenommen werden, sendet AWS Config keine Datei.

AWS Config sendet einen Konfigurations-Snapshot an Ihren Amazon S3 S3-Bucket, wenn Sie den deliver-config-snapshotBefehl mit der AWS CLI oder wenn Sie die DeliverConfigSnapshotAktion mit der AWS Config API verwenden. Ein Konfigurations-Snapshot enthält Konfigurationsdetails für alle Ressourcen, die AWS Config in Ihrem gespeichert sind AWS-Konto. Die Konfigurationsverlaufsdatei und der Konfigurations-Snapshot liegen im JSON-Format vor.

> **Note**
>
> AWS Config übermittelt nur die Konfigurationsverlaufsdateien und Konfigurations-Snapshots an den angegebenen S3-Bucket. Die Lebenszyklusrichtlinien für Objekte im S3-Bucket werden AWS Config nicht geändert. Mithilfe von Richtlinien für den Lebenszyklus können Sie angeben, ob Sie Objekte löschen oder in Amazon S3 Glacier archivieren möchten. Weitere Informationen finden Sie im Abschnitt zum Verwalten der Lebenszykluskonfiguration im Benutzerhandbuch für Amazon Simple Storage Service. Informationen finden Sie außerdem im Blogbeitrag Archiving Amazon S3 Data to Amazon Glacier.

Amazon SNS-Thema

Ein Amazon Simple Notification Service (Amazon SNS)-Thema ist ein Kommunikationskanal, den Amazon SNS für die Übermittlung von Nachrichten (oder Benachrichtigungen) an abonnierende Endpunkte verwendet, z. B. eine E-Mail-Adresse oder Clients. Andere Arten von Amazon-SNS-Benachrichtigungen sind Push-Benachrichtigungen an Apps auf Mobiltelefonen, SMS-Benachrichtigungen an SMS-fähige Mobiltelefone und Smartphones sowie HTTP-POST-Anforderungen. Um die besten Ergebnisse zu erzielen, verwenden Sie Amazon SQS als Endpunkt Ihrer Benachrichtigungen für das SNS-Thema und verarbeiten Sie anschließend programmgesteuert die Informationen in der Benachrichtigung.

AWS Config verwendet das von Ihnen angegebene Amazon SNS SNS-Thema, um Ihnen Benachrichtigungen zu senden. Der Typ der Benachrichtigung, die Sie erhalten, wird durch den Wert des `messageType`-Schlüssels im Nachrichtentext wie im folgenden Beispiel angegeben:

```
"messageType": "ConfigurationHistoryDeliveryCompleted"
```

Bei den Benachrichtigungen kann es sich um einen der folgenden Nachrichtentypen handeln.

Art der Nachricht	Beschreibung
ComplianceChangeNotification	Der Konformitätstyp einer Ressource, die AWS Config bewertet, hat sich geändert. Der Konformitätstyp gibt an, ob die Ressource einer bestimmten AWS Config Regel entsprich t, und wird durch den `ComplianceType` Schlüssel in der Nachricht dargestellt. Die Nachricht enthält `newEvaluationResult` - und `oldEvaluationResult` -Objekte für den Vergleich.
ConfigRulesEvaluationStarted	AWS Config hat begonnen, Ihre Regel anhand der angegebenen Ressourcen auszuwerten.
ConfigurationSnapshotDeliveryStarted	AWS Config hat begonnen, den Konfigura tions-Snapshot an Ihren Amazon S3 S3-Bucket zu senden. Der Name des Amazon-S3 -Buckets wird für den `s3Bucket`-Schlüssel in der Nachricht bereitgestellt.
ConfigurationSnapshotDeliveryCompleted	AWS Config hat den Konfigurations-Snapshot erfolgreich an Ihren Amazon S3 S3-Bucket gesendet.
ConfigurationSnapshotDeliveryFailed	AWS Config konnte den Konfigurations-Sna pshot nicht an Ihren Amazon S3 S3-Bucket senden.
ConfigurationHistoryDeliveryCompleted	AWS Config hat den Konfigurationsverlauf erfolgreich an Ihren Amazon S3 S3-Bucket gesendet.
ConfigurationItemChangeNotification	Eine Ressource wurde erstellt, gelöscht oder in Bezug auf die Konfiguration geändert. Diese Nachricht enthält die Details des Konfigura tionselements, das für diese Änderung AWS Config erstellt wurde, sowie die Art der

Art der Nachricht	Beschreibung
	Änderung. Diese Benachrichtigungen werden wenige Minuten nach einer Änderung übermitte lt und werden im Allgemeinen als Konfigura tions-Stream bezeichnet.
OversizedConfigurationItemChangeNotification	Dieser Nachrichtentyp wird übermittelt, wenn die Änderungsbenachrichtigung für ein Konfigurationselement die von Amazon SNS maximal erlaubte Größe überschre itet. Die Nachricht enthält eine Zusammenf assung des Konfigurationselements. Mit Ausnahme von SMS-Nachrichten können Amazon-SNS-Nachrichten bis zu 256 KB an Textdaten enthalten, darunter XML, JSON und unformatierten Text. Sie können die vollständ ige Benachrichtigung an dem angegebenen Amazon-S3-Bucket-Speicherort anzeigen.
OversizedConfigurationItemChangeDeli veryFailed	AWS Config konnte die Benachrichtigung über die Änderung des übergroßen Konfigura tionselements nicht an Ihren Amazon S3 S3-Bucket senden.

Beispielbenachrichtigungen finden Sie unter Benachrichtigungen, die AWS Config an ein Amazon SNS SNS-Thema gesendet werden. Weitere Informationen zu Amazon SNS finden Sie im Amazon-Simple-Notification-Service-Entwicklerhandbuch.

> **Note**
>
> Warum kann ich meine letzten Konfigurationsänderungen nicht sehen?
> AWS Config zeichnet in der Regel Konfigurationsänderungen an Ihren Ressourcen auf, unmittelbar nachdem eine Änderung erkannt wurde, oder in der von Ihnen angegebenen Häufigkeit. Dies erfolgt jedoch nach bestem Wissen und kann manchmal länger dauern. Wenn die Probleme nach einiger Zeit weiterhin bestehen, wenden Sie sich an uns Supportund geben Sie Ihre von Amazon unterstützten AWS Config Messwerte an.

CloudWatch Informationen zu diesen Kennzahlen finden Sie unter AWS Config Nutzungs- und Erfolgsmetriken.

Steuern Sie den Zugriff auf AWS Config

AWS Identity and Access Management ist ein Webservice, der es Kunden von Amazon Web Services (AWS) ermöglicht, Benutzer und Benutzerberechtigungen zu verwalten.

Um Zugriff zu gewähren, fügen Sie Ihren Benutzern, Gruppen oder Rollen Berechtigungen hinzu:

- Benutzer und Gruppen in AWS IAM Identity Center:

  Erstellen Sie einen Berechtigungssatz. Befolgen Sie die Anweisungen unter Erstellen eines Berechtigungssatzes im AWS IAM Identity Center -Benutzerhandbuch.
- Benutzer, die in IAM über einen Identitätsanbieter verwaltet werden:

  Erstellen Sie eine Rolle für den Identitätsverbund. Befolgen Sie die Anleitung unter Eine Rolle für einen externen Identitätsanbieter (Verbund) erstellen im IAM-Benutzerhandbuch.
- IAM-Benutzer:
  - Erstellen Sie eine Rolle, die Ihr Benutzer annehmen kann. Befolgen Sie die Anleitung unter Eine Rolle für einen IAM-Benutzer erstellen im IAM-Benutzerhandbuch.
  - (Nicht empfohlen) Weisen Sie einem Benutzer eine Richtlinie direkt zu oder fügen Sie einen Benutzer zu einer Benutzergruppe hinzu. Befolgen Sie die Anweisungen unter Hinzufügen von Berechtigungen zu einem Benutzer (Konsole) im IAM-Benutzerhandbuch.

AWS Config Terminologie und Konzepte

Um Ihnen das Verständnis zu erleichtern AWS Config, werden in diesem Thema einige der wichtigsten Konzepte erläutert.

Inhalt

- AWS Config Schnittstellen
  - AWS Config Konsole
  - AWS Config CLI
  - AWS Config APIs

- AWS Config SDKs
- Ressourcenmanagement
  - AWS Ressourcen
  - Ressourcenbeziehung
- Configuration Recorder
- Übermittlungskanal
  - Konfigurationselemente
  - Konfigurationsverlauf
  - Konfigurations-Snapshot
  - Konfigurations-Stream
- AWS Config Regeln
  - Ergebnisse der Bewertung
  - Regeltypen
  - Auslösertypen
  - Auswertungsmodi
- Konformitätspakete
- Datenaggregation für mehrere Konten und Regionen
  - Quellkonto
  - Quellregion
  - Aggregator
  - Mit einem Dienst verbundener Aggregator
  - Aggregatorkonto
  - Autorisierung

AWS Config Schnittstellen

AWS Config Konsole

Sie können den Dienst über die AWS Config Konsole verwalten. Weitere Informationen zu dem finden AWS Management Console Sie unter AWS Management Console.

AWS Config CLI

Das AWS Command Line Interface ist ein einheitliches Tool, mit dem Sie über die AWS Config Befehlszeile interagieren können. Weitere Informationen finden Sie im AWS Command Line Interface -Benutzerhandbuch. Eine vollständige Liste der AWS Config CLI-Befehle finden Sie unter Verfügbare Befehle.

AWS Config APIs

Neben der Konsole und der CLI können Sie auch AWS Config direkt die AWS Config RESTful APIs zur Programmierung verwenden. Weitere Informationen finden Sie in der AWS Config -API-Referenz.

AWS Config SDKs

Als Alternative zur Verwendung der AWS Config API können Sie eine der verwenden AWS SDKs. Jedes SDK enthält Bibliotheken und Beispiel-Code für verschiedene Programmiersprachen und Plattformen. SDKs Sie bieten eine bequeme Möglichkeit, programmatischen Zugriff auf zu AWS Config erstellen. Sie können das beispielsweise verwenden, um Anfragen kryptografisch SDKs zu signieren, Fehler zu verwalten und Anfragen automatisch zu wiederholen. Weitere Informationen finden Sie unter Tools für Amazon Web Services.

Ressourcenmanagement

Wenn Sie die grundlegenden Komponenten von verstehen, können AWS Config Sie den Ressourcenbestand und die Änderungen nachverfolgen und die Konfigurationen Ihrer Ressourcen bewerten. AWS

AWS Ressourcen

AWS Ressourcen sind Entitäten, die Sie mit den AWS Management Console Tools AWS Command Line Interface (CLI) AWS SDKs, oder AWS Partnern erstellen und verwalten. Zu den AWS Ressourcen gehören beispielsweise EC2 Amazon-Instances, Sicherheitsgruppen VPCs, Amazon und Amazon Elastic Block Store. AWS Config bezieht sich auf jede Ressource unter Verwendung ihrer eindeutigen Kennung, z. B. der Ressourcen-ID oder eines Amazon-Ressourcennamens (ARN). Eine Liste der AWS Config unterstützten Ressourcentypen finden Sie unterUnterstützte Ressourcentypen für AWS Config.

Ressourcenbeziehung

AWS Config erkennt AWS Ressourcen in Ihrem Konto und erstellt dann eine Übersicht der Beziehungen zwischen AWS Ressourcen. Eine Beziehung kann beispielsweise ein Amazon EBS-Volume beinhalten, das an eine EC2 Amazon-Instance `vol-123ab45d` angehängt ist`i-a1b2c3d4`, die einer Sicherheitsgruppe `sg-ef678hk` zugeordnet ist.

Weitere Informationen finden Sie unter Unterstützte Ressourcentypen für AWS Config.

Configuration Recorder

Der Konfigurationsrekorder speichert die Konfigurationsänderungen an den Ressourcentypen im Gültigkeitsbereich als Konfigurationselemente. Weitere Informationen finden Sie unter Arbeiten mit dem Konfigurationsrekorder.

Es gibt zwei Arten von Konfigurationsrekordern.

Typ	Beschreibung
Vom Kunden verwalteter Konfigurationsrekorder	Ein von Ihnen verwalteter Konfigurationsrekorder. Die im Geltungsbereich enthaltenen Ressourcentypen werden von Ihnen festgelegt. Standardmäßig zeichnet ein vom Kunden verwalteter Konfigurationsrekorder alle unterstützten Ressourcen in dem Bereich auf, in AWS-Region dem er ausgeführt AWS Config wird.
Mit dem Dienst verbundener Konfigurationsrekorder	Ein Konfigurationsrekorder, der mit einem bestimmten AWS-Service verknüpft ist. Die im Gültigkeitsbereich angegebenen Ressourcentypen werden vom verknüpften Dienst festgelegt.

Übermittlungskanal

Da AWS Config kontinuierlich die Änderungen an Ihren AWS Ressourcen aufgezeichnet werden, werden Benachrichtigungen und aktualisierte Konfigurationsstatus über den Bereitstellungskanal

gesendet. Sie können den Lieferkanal verwalten, um zu kontrollieren, wohin Konfigurationsupdates AWS Config gesendet werden.

Konfigurationselemente

Ein Konfigurationselement stellt eine point-in-time Ansicht der verschiedenen Attribute einer unterstützten AWS Ressource dar, die in Ihrem Konto vorhanden ist. Zu den Komponenten eines Konfigurationselements gehören Metadaten, Attribute, Beziehungen, die aktuelle Konfiguration und verwandte Ereignisse. AWS Config erstellt ein Konfigurationselement, wenn es eine Änderung an einem Ressourcentyp erkennt, den es aufzeichnet. Wenn beispielsweise Amazon S3 S3-Buckets aufgezeichnet werden, AWS Config wird jedes Mal, wenn ein Bucket AWS Config erstellt, aktualisiert oder gelöscht wird, ein Konfigurationselement erstellt. Sie können auch auswählen AWS Config , ob ein Konfigurationselement mit der von Ihnen festgelegten Aufzeichnungsfrequenz erstellt werden soll.

Weitere Informationen finden Sie unter Components of a Configuration Item Aufzeichnungsfrequenz.

Konfigurationsverlauf

Ein Konfigurationsverlauf ist die Sammlung der Konfigurationselemente für eine bestimmte Ressource über einen beliebigen Zeitraum. Ein Konfigurationsverlauf kann Ihnen bei der Beantwortung von Fragen helfen: z. B. wann die Ressource erstmalig erstellt wurde, wie die Ressource im letzten Monat konfiguriert wurde und welche Konfigurationsänderungen gestern um 9.00 Uhr eingeführt wurden. Der Konfigurationsverlauf steht Ihnen in verschiedenen Formaten zur Verfügung. AWS Config liefert automatisch eine Konfigurationsverlaufsdatei für jeden Ressourcentyp, der in einem von Ihnen angegebenen Amazon S3 S3-Bucket aufgezeichnet wird. Sie können eine bestimmte Ressource in der AWS Config Konsole auswählen und mithilfe der Zeitleiste zu allen vorherigen Konfigurationselementen für diese Ressource navigieren. Zusätzlich können Sie über die API auf historische Konfigurationselemente für eine Ressource zugreifen.

Weitere Informationen finden Sie unter Konformitätsverlauf anzeigen und Kompatibilitätsverlauf abfragen.

Konfigurations-Snapshot

Ein Konfigurations-Snapshot ist eine Sammlung der Konfigurationselemente der unterstützten Ressourcen in Ihrem Konto. Dieser Konfigurations-Snapshot liefert ein vollständiges Bild der derzeit aufgezeichneten Ressourcen und deren Konfigurationen. Die Konfigurations-Snapshot ist ein nützliches Tool für die Validierung Ihrer Konfiguration. Sie können beispielsweise den Konfigurations-Snapshot regelmäßig auf falsch konfigurierte Ressourcen oder solche, die potentiell nicht vorhanden

sein sollten, hin prüfen. Der Konfigurations-Snapshot ist in mehreren Formaten verfügbar. Der Konfigurations-Snapshot kann an einen von Ihnen angegebenen Amazon Simple Storage Service (Amazon S3)-Bucket übermittelt werden. Darüber hinaus können Sie in der AWS Config Konsole einen Zeitpunkt auswählen und mithilfe der Beziehungen zwischen den Ressourcen durch den Snapshot der Konfigurationselemente navigieren.

Weitere Informationen finden Sie unter Bereitstellen von Konfigurations-Snapshots, Anzeigen von Konfigurations-Snapshots und Beispiel für einen Konfigurations-Snapshot.

Konfigurations-Stream

Ein Konfigurationsstream ist eine automatisch aktualisierte Liste aller Konfigurationselemente für die Ressourcen, AWS Config die aufgezeichnet werden. Bei jeder Erstellung, Änderung oder Löschung einer Ressource wird von AWS Config ein neues Konfigurationselement erstellt und dem Konfigurations-Stream hinzugefügt. Der Konfigurationsstream verwendet ein Amazon Simple Notification Service (Amazon SNS)-Thema Ihrer Wahl. Der Konfigurationsstream ist hilfreich, um Konfigurationsänderungen sofort zu beobachten, sodass Sie potenzielle Probleme erkennen können, Benachrichtigungen zu generieren, wenn bestimmte Ressourcen geändert werden, oder externe Systeme zu aktualisieren, die die Konfiguration Ihrer AWS Ressourcen widerspiegeln müssen.

AWS Config Regeln

Eine AWS Config Regel ist eine Konformitätsprüfung, mit der Sie Ihre idealen Konfigurationseinstellungen für bestimmte AWS Ressourcen verwalten können. AWS Config bewertet, ob Ihre Ressourcenkonfigurationen den relevanten Regeln entsprechen, und zeigt die Konformitätsergebnisse an.

Ergebnisse der Bewertung

Es gibt vier mögliche Bewertungsergebnisse für eine AWS Config Regel.

Ergebnis der Bewertung	Beschreibung
`COMPLIANT`	Die Regel erfüllt die Bedingungen der Konformitätsprüfung.
`NON_COMPLIANT`	Die Regel erfüllt die Bedingungen der Konformitätsprüfung nicht.

Ergebnis der Bewertung	Beschreibung
`ERROR`	Einer der erforderlichen/optionalen Parameter ist ungültig, hat nicht den richtigen Typ oder ist falsch formatiert.
`NOT_APPLICABLE`	Wird verwendet, um Ressourcen herauszuf iltern, auf die die Logik der Regel nicht angewendet werden kann. Die alb-desync-mode-checkRegel überprüft beispielsweise nur Application Load Balancer und ignoriert Network Load Balancers und Gateway Load Balancers.

Regeltypen

Es gibt zwei Arten von Regeln. Weitere Informationen zur Struktur von Regeldefinitionen und Regelmetadaten finden Sie unter Komponenten einer AWS Config Regel.

Typ	Beschreibung	Weitere Informationen
Verwaltete Regeln	Vordefinierte, anpassbare Regeln, erstellt von AWS Config.	Eine Liste der verwalteten Regeln finden Sie unter Liste der AWS Config verwalteten Regeln.
Benutzerdefinierte Regeln	Regeln, die Sie von Grund auf neu erstellen. Es gibt zwei Möglichkeiten, AWS Config benutzerdefinierte Regeln zu erstellen: Lambda-Funktionen (AWS Lambda Developer Guide) und Guard (Guard GitHub Repository)	Weitere Informationen finden Sie unter AWS Config Benutzerdefinierte Richtlinienregeln erstellen und AWS Config Benutzerdefinierte Lambda-Regeln erstellen.

Auslösertypen

Nachdem Sie Ihrem Konto eine Regel hinzugefügt haben, werden Ihre Ressourcen mit den Bedingungen der Regel AWS Config verglichen. Nach dieser ersten Evaluierung werden die Evaluierungen jedes Mal, wenn eine ausgelöst wird, AWS Config fortgesetzt. Die Evaluierungsauslöser sind als Teil der Regel definiert und können die folgenden Typen beinhalten.

Typ des Auslösers	Beschreibung
Konfigurationsänderungen	AWS Config führt Evaluierungen für die Regel durch, wenn es eine Ressource gibt, die dem Geltungsbereich der Regel entspricht, und wenn sich die Konfiguration der Ressource ändert. Die Evaluierung wird ausgeführt, nachdem eine Benachrichtigung über eine Änderung des Konfigurationselements AWS Config gesendet wurde. Sie können auswählen, welche Ressource n die Auswertung auslösen, indem Sie den Umfang der Regel definieren. Im Umfang kann Folgendes enthalten sein: • Mindestens ein Ressourcentyp • Eine Kombination aus einem Ressourcentyp und einer Ressourcen-ID • Eine Kombination aus einem Tag-Schlüssel und einem Wert • Wann alle aufgezeichneten Ressourcen erstellt, aktualisiert oder gelöscht wurden AWS Config führt die Evaluierung aus, wenn eine Änderung an einer Ressource erkannt wird, die dem Geltungsbereich der Regel entspricht. Sie können den Umfang verwenden

Typ des Auslösers	Beschreibung
	, um zu definieren, welche Ressourcen Auswertungen auslösen.
Regelmäßig	AWS Config führt Evaluierungen für die Regel in einer von Ihnen festgelegten Häufigkeit durch, z. B. alle 24 Stunden.
Hybrid	Einige Regeln werden sowohl durch Konfigurationsänderungen als auch nach einem Zeitplan ausgelöst. Bei diesen Regeln werden Ihre Ressourcen AWS Config ausgewertet, wenn eine Konfigurationsänderung erkannt wird, und auch in der von Ihnen angegebenen Häufigkeit.

Auswertungsmodi

Es gibt zwei Bewertungsmodi für AWS Config Regeln.

Bewertungsmodus	Beschreibung
Proaktiv	Verwenden Sie die proaktive Auswertung, um Ressourcen vor der Bereitstellung auszuwerten. Auf diese Weise können Sie auswerten, ob ein Satz von Ressourceneigenschaften, wenn er zur Definition einer AWS Ressource verwendet würde, angesichts der proaktiven Regeln, die Sie in Ihrem Konto in Ihrer Region haben, als KONFORM oder NICHT KONFORM gelten würde. Weitere Informationen finden Sie unter Auswertungsmodi. Eine Liste der verwalteten Regeln, die eine proaktive Bewertung unterstützen, finden Sie unter Liste der AWS Config verwalteten Regeln nach Testmodus.

Bewertungsmodus	Beschreibung
Detektivisch	Mit der detektivischen Auswertung können Sie Ressourcen auswerten, die bereits bereitgestellt wurden. Auf diese Weise lassen sich die Konfigurationseinstellungen Ihrer vorhandenen Ressourcen auswerten.

> **Note**
>
> Durch proaktive Regeln werden keine Ressourcen korrigiert, die als NON_COMPLIANT gekennzeichnet sind, und sie verhindern auch nicht, dass diese bereitgestellt werden.

Konformitätspakete

Ein Konformitätspaket ist eine Sammlung von AWS Config Regeln und Korrekturmaßnahmen, die einfach als einzelne Einheit in einem Konto und einer Region oder unternehmensweit in einem Unternehmen eingesetzt werden können. AWS Organizations

Conformance Packs werden erstellt, indem eine YAML-Vorlage erstellt wird, die die Liste der von AWS Config verwalteten oder benutzerdefinierten Regeln und Korrekturmaßnahmen enthält. Sie können die Vorlage mithilfe der AWS Config -Konsole oder der AWS CLI bereitstellen.

Verwenden Sie eine der Mustervorlagen für Conformance Packs, um schnell loszulegen und Ihre AWS Umgebung zu evaluieren. Sie können auch eine YAML-Datei für ein Conformance Pack von Grund auf neu erstellen. Weitere Informationen finden Sie unter Custom Conformance Pack. Ein benutzerdefiniertes Conformance Pack ist eine einzigartige Sammlung von AWS Config Regeln und Behebungsmaßnahmen, die Sie gemeinsam in einem Konto und einer AWS Region oder unternehmensweit einsetzen können. AWS Organizations

Prozessprüfungen sind eine Art von AWS Config Regel, mit der Sie Ihre externen und internen Aufgaben, die im Rahmen der Konformitätspakete überprüft werden müssen, nachverfolgen können. Diese Prüfungen können einem vorhandenen Conformance Pack oder einem neuen Conformance Pack hinzugefügt werden. Sie können die gesamte Einhaltung der Vorschriften, einschließlich AWS Config der Dauer und manueller Prüfungen, an einem einzigen Ort nachverfolgen.

Datenaggregation für mehrere Konten und Regionen

Durch die Datenaggregation mehrerer Konten und mehrerer Regionen AWS Config können Sie AWS Config Konfigurations- und Compliance-Daten aus mehreren Konten und Regionen in einem einzigen Konto zusammenfassen. Die Datenaggregation mit mehreren Konten und mehreren Regionen ist für zentrale IT-Administratoren nützlich, um die Einhaltung der Vorschriften für mehrere Benutzer im Unternehmen zu überwachen. AWS-Konten Durch die Verwendung von Aggregatoren fallen keine zusätzlichen Kosten an.

Quellkonto

Ein Quellkonto ist das Konto, AWS-Konto von dem aus Sie AWS Config Ressourcenkonfigurations- und Compliance-Daten aggregieren möchten. Ein Quellkonto kann ein einzelnes Konto oder eine Organisation in AWS Organizations sein. Sie können Quellkonten einzeln bereitstellen oder sie über abrufen AWS Organizations.

Quellregion

Eine Quellregion ist die AWS Region, aus der Sie AWS Config Konfigurations- und Compliance-Daten aggregieren möchten.

Aggregator

Ein Aggregator sammelt AWS Config Konfigurations- und Compliance-Daten aus mehreren Quellkonten und Regionen. Erstellen Sie einen Aggregator in der Region, in der Sie die aggregierten AWS Config Konfigurations- und Compliance-Daten sehen möchten.

> **Note**
>
> Aggregatoren bieten eine schreibgeschützte Ansicht der Quellkonten und Regionen, zu deren Anzeige der Aggregator berechtigt ist, indem sie Daten aus den Quellkonten in das Aggregatorkonto replizieren. Aggregatoren bieten keinen mutierenden Zugriff auf ein Quellkonto oder eine Quellregion. Dies bedeutet beispielsweise, dass Sie Regeln nicht über einen Aggregator bereitstellen oder Snapshot-Dateien nicht über einen Aggregator an ein Quellkonto oder eine Quellregion übertragen können.

Mit einem Dienst verbundener Aggregator

Ein dienstgebundener Aggregator ist mit einem bestimmten verknüpft. AWS-Service Die im Geltungsbereich enthaltenen Konfigurations- und Compliance-Daten werden vom verknüpften Dienst festgelegt.

Aggregatorkonto

Ein Aggregatorkonto ist das Konto, in dem Sie einen Aggregator erstellen.

Autorisierung

Als Inhaber eines Quellkontos bezieht sich die Autorisierung auf die Berechtigungen, die Sie einem Aggregatorkonto und einer Region zur Erfassung Ihrer AWS Config Konfigurations- und Compliance-Daten gewähren. Die Autorisierung ist nicht erforderlich, wenn Sie Quellkonten aggregieren, die Teil von AWS Organizations sind.

AWS Serviceintegrationen mit AWS Config

AWS Config unterstützt Integrationen mit mehreren anderen AWS Diensten. Diese Liste erhebt keinen Anspruch auf Vollständigkeit.

AWS Organizations

Sie können AWS Organizations damit die Konten definieren, die für die Datenaggregationsfunktion für AWS Config mehrere Konten und Regionen verwendet werden sollen. AWS Organizations ist ein Kontoverwaltungsservice, mit dem Sie mehrere Konten zu einer Organisation AWS-Konten zusammenfassen können, die Sie erstellen und zentral verwalten. Durch die Angabe Ihrer AWS Organizations Daten können Sie den Compliance-Status in Ihrer gesamten Organisation überwachen. Weitere Informationen AWS Config und AWS Organizations im AWS Organizations Benutzerhandbuch.

AWS Control Tower

AWS Control Tower AWS Config aktiviert für alle registrierten Konten, sodass es die Einhaltung der Vorschriften durch detektive Kontrollen überwachen, Ressourcenänderungen aufzeichnen und Ressourcenänderungsprotokolle an das Protokollarchivkonto senden kann. Weitere Informationen finden Sie im AWS Control Tower Benutzerhandbuch unter Überwachen von AWS Config Ressourcenänderungen mit.

AWS CloudTrail

AWS Config integriert sich in AWS CloudTrail , um Konfigurationsänderungen mit bestimmten Ereignissen in Ihrem Konto zu korrelieren. Sie können die CloudTrail Protokolle verwenden, um die Details des Ereignisses abzurufen, das die Änderung ausgelöst hat, einschließlich der Person, die Anfrage gestellt hat, zu welchem Zeitpunkt und von welcher IP-Adresse. Sie können von der CloudTrail Konsole aus zur AWS Config Timeline navigieren, um sich die Konfigurationsänderungen im Zusammenhang mit Ihren AWS API-Aktivitäten anzusehen.

Weitere Informationen finden Sie unter Protokollieren von AWS Config API-Aufrufen mit AWS CloudTrail im AWS Config Entwicklerhandbuch und Erstellen eines Ereignisdatenspeichers für AWS Config Konfigurationselemente mit der Konsole im AWS CloudTrail Benutzerhandbuch.

AWS Security Hub

AWS Security Hub zentralisiert Sicherheitsüberprüfungen anderer AWS Dienste, einschließlich Regeln. AWS Config Security Hub aktiviert und kontrolliert AWS Config Regeln, um zu überprüfen, ob Ihre Ressourcenkonfigurationen den Best Practices entsprechen. AWS Config Aktivieren Sie diese Option für alle Konten in allen Regionen, in denen Security Hub Sicherheitsüberprüfungen für die Ressourcen Ihrer Umgebung durchführen soll. Weitere Informationen finden Sie im AWS Security Hub Benutzerhandbuch unter AWS Dienste, die Ergebnisse an Security Hub senden.

> **Einige Regeln im Zusammenhang mit Security Hub sind periodisch und hängen nicht von Konfigurationselementen ab**
>
> Einige Regeln im Zusammenhang mit Security Hub gelten in regelmäßigen Abständen. Diese Regel kann ausgeführt werden, ohne dass der Konfigurationsrekorder aktiviert ist, und sie hängen nicht von Konfigurationselementen (CI) ab.
> Das bedeutet, dass auf der Regelseite kein CI oder keine unterstützte Ressource aufgeführt ist. Wenn Sie die Ressourcen-ID auswählen, wird der folgende Fehler angezeigt:The `provided resource ID and resource type cannot be found`. Dieses Verhalten wird erwartet.

AWS Trusted Advisor

AWS Config verwaltete Regeln ermöglichen eine Reihe von Trusted Advisor Prüfungen in allen Kategorien. Wenn Sie bestimmte verwaltete Regeln aktivieren, werden die entsprechenden Trusted

Advisor Prüfungen automatisch aktiviert. Informationen darüber, welche Trusted Advisor Prüfungen auf bestimmten AWS Config verwalteten Regeln basieren, finden AWS Trusted Advisor Sie in der Prüfreferenz im AWS -Support Benutzerhandbuch.

Die AWS Config Powered Checks stehen Kunden mit AWS Business Support-, AWS Enterprise On-Ramp - und AWS Enterprise Support-Plänen zur Verfügung. Wenn Sie einen dieser AWS Support-Pläne aktivieren AWS Config und über einen verfügen, werden Ihnen automatisch Empfehlungen angezeigt, die auf den entsprechenden bereitgestellten AWS Config verwalteten Regeln basieren.

> **Aktualisierungsanforderungen sind nicht zulässig und Ressourcen können nicht ausgeschlossen werden**
>
> Die Ergebnisse dieser Prüfungen werden auf der Grundlage von durch Änderungen ausgelösten Aktualisierungen der verwalteten Regeln automatisch aktualisiert. AWS Config Aktualisierungsanfragen sind nicht zulässig. Derzeit können Sie keine Ressourcen von dieser Prüfung ausschließen.

Weitere Informationen finden Sie AWS Config im Benutzerhandbuch unter View Trusted Advisor checks powered by.AWS -Support

AWS Audit Manager

Sie können Audit Manager verwenden, um AWS Config Bewertungen als Nachweis für Audits zu erfassen. Wenn Sie ein benutzerdefiniertes Steuerelement erstellen oder bearbeiten, können Sie eine oder mehrere AWS Config Regeln als Datenquellenzuordnung für die Erfassung von Nachweisen angeben. AWS Config führt Konformitätsprüfungen auf der Grundlage dieser Regeln durch, und Audit Manager meldet die Ergebnisse als Nachweis der Konformitätsprüfung. Weitere Informationen finden Sie AWS Audit Manager im AWS Audit Manager Benutzerhandbuch unter Unterstützte AWS Config Regeln von.

AWS Systems Manager

AWS Config lässt sich in Systems Manager integrieren, um Konfigurationsänderungen an der Software auf Ihren EC2 Amazon-Instances und -Servern in Ihrer lokalen Umgebung aufzuzeichnen. Mit dieser Integration erhalten Sie Einblick in Betriebssystemkonfigurationen (OS), Updates auf Systemebene, installierte Anwendungen, Netzwerkkonfigurationen und mehr. AWS Config bietet außerdem einen Verlauf der Konfigurationsänderungen auf Betriebssystem- und Systemebene sowie die für EC2 Amazon-Instances aufgezeichneten Änderungen der Infrastrukturkonfiguration. Sie

können von der Systems Manager Manager-Konsole aus zur AWS Config Timeline navigieren, um sich die Konfigurationsänderungen Ihrer verwalteten EC2 Amazon-Instances anzusehen. Sie können AWS Config damit den Systems Manager Manager-Inventarverlauf anzeigen und Änderungen für all Ihre verwalteten Instanzen nachverfolgen.

Weitere Informationen finden Sie im AWS Systems Manager Benutzerhandbuch unter Integration mit AWS Diensten | Verwaltung und Steuerung, AWS Config Konfigurationsrekorder und Bereitstellung von AWS Config Konformitätspaketen.

AWS Firewall Manager

Um den Firewall Manager verwenden zu können, müssen Sie AWS Config ihn für jedes Ihrer AWS Organizations Mitgliedskonten aktivieren. Wenn neue Anwendungen erstellt werden, ist Firewall Manager der einzige Dienst, der Firewallregeln und Sicherheitsrichtlinien erstellt und diese konsistent durchsetzt. Weitere Informationen finden Sie unter Enable AWS Config im AWS WAF, AWS Firewall Manager, und AWS Shield Advanced Developer Guide.

> **Note**
>
> Firewall Manager ist auf kontinuierliche Aufzeichnungen angewiesen, um Ihre Ressourcen zu überwachen. Wenn Sie den Firewall Manager verwenden, wird empfohlen, die Aufzeichnungsfrequenz auf „Kontinuierlich“ einzustellen. Weitere Informationen zur kontinuierlichen Aufzeichnung und zur täglichen Aufzeichnung finden Sie unter Aufzeichnungsfrequenz.

EC2 Dedizierte Amazon-Hosts

AWS Config lässt sich in Amazon EC2 Dedicated Hosts integrieren, um die Einhaltung der Lizenzbestimmungen zu überprüfen. AWS Config zeichnet auf, wann Instances auf einem Dedicated Host gestartet, gestoppt oder heruntergefahren werden, und verknüpft diese Informationen mit Informationen auf Host- und Instance-Ebene, die für die Softwarelizenzierung relevant sind, wie Host-ID, Amazon Machine Image (AMI) IDs, Anzahl der Sockets und physische Kerne. Dies hilft Ihnen bei der Verwendung AWS Config als Datenquelle für Ihre Lizenzberichte. Sie können von der Amazon EC2 Dedicated Hosts-Konsole aus zur AWS Config Timeline navigieren, um die Konfigurationsänderungen Ihrer Amazon EC2 Dedicated Hosts einzusehen.

Weitere Informationen finden Sie unter Konfigurationsänderungen verfolgen im Amazon Elastic Compute Cloud-Benutzerhandbuch für Linux-Instances oder unter Verfolgen von

Konfigurationsänderungen im Amazon Elastic Compute Cloud-Benutzerhandbuch für Windows-Instances.

Application Load Balancer

AWS Config integriert sich in den Elastic Load Balancing (ELB) -Service, um Konfigurationsänderungen an Application Load Balancers aufzuzeichnen. AWS Config umfasst auch Beziehungen zu zugehörigen EC2 Amazon-Sicherheitsgruppen und Subnetzen. VPCs Sie können diese Informationen für Sicherheitsanalysen und zur Fehlerbehebung verwenden. Sie können beispielsweise jederzeit überprüfen, welche Sicherheitsgruppen Ihrem Application Load Balancer zugeordnet sind. Sie können von der ELB-Konsole aus zur AWS Config Timeline navigieren, um sich die Konfigurationsänderungen Ihrer Application Load Balancer anzusehen.

AWS CodeBuild

AWS Config bietet eine Bestandsaufnahme Ihrer AWS Ressourcen und einen Verlauf der Konfigurationsänderungen an diesen Ressourcen. AWS Config unterstützt AWS CodeBuild; als AWS Ressource, was bedeutet, dass der Dienst Ihre CodeBuild Projekte verfolgen kann. Weitere Informationen finden Sie im AWS CodeBuild Benutzerhandbuch unter Verwendung AWS Config mit CodeBuild Beispiel.

AWS X-Ray

AWS X-Ray integriert sich in AWS Config , um Konfigurationsänderungen aufzuzeichnen, die an Ihren X-Ray-Verschlüsselungsressourcen vorgenommen wurden. Sie können AWS Config damit Ressourcen für die X-Ray-Verschlüsselung inventarisieren, den X-Ray-Konfigurationsverlauf überprüfen und Benachrichtigungen auf Grundlage von Ressourcenänderungen versenden. Weitere Informationen finden Sie unter Verfolgen von Konfigurationsänderungen der X-Ray-Verschlüsselung mit AWS Config im AWS X-Ray Entwicklerhandbuch.

AWS Service Management Connector

Das AWS Service Management Connector for ServiceNow kann AWS Config Daten aus mehreren Konten und Regionen mithilfe eines Aggregators synchronisieren. Weitere Informationen finden Sie unter Integrieren AWS Config ServiceNow im AWS Service Management Connector Administratorhandbuch.

Amazon API Gateway

Sie können AWS Config damit Konfigurationsänderungen an Ihren API-Gateway-API-Ressourcen aufzeichnen und Benachrichtigungen auf der Grundlage von Ressourcenänderungen senden. Die Pflege eines Konfigurations-Änderungsverlaufs für API Gateway-Ressourcen ist nützlich bei Fehlerbehebung im Betrieb sowie Anwendungsfällen wie Audit und Compliance. Weitere Informationen finden Sie unter Monitoring API Gateway API-Konfiguration mit AWS Config im API Gateway Developer Guide.

Regionalunterstützung für AWS Config

Überlegungen

Einige Funktionen von AWS Config werden nur in einer Teilmenge der AWS Regionen unterstützt, in denen sie AWS Config unterstützt werden.

Ressourcenmanagement

- Eine Liste der AWS Ressourcentypen, die in welchen Regionen unterstützt werden, finden Sie unter Ressourcenabdeckung nach Verfügbarkeit in Regionen.

AWS Config Regeln

- Eine Liste der AWS Config Regeln, die in welchen Regionen unterstützt werden, finden Sie unter Liste der AWS Config verwalteten Regeln nach Verfügbarkeit in Regionen.
- Eine Liste der Regionen, die die organisatorische Implementierung von AWS Config Regeln Support, finden Sie unter Organisationsregeln | Regionalunterstützung.

Konformitätspakete

- Eine Liste der Regionen, die Konformitätspakete und die organisatorische Bereitstellung von Konformitätspaketen unterstützen, finden Sie unter Konformitätspakete | Unterstützte Regionen.

Behebung

- Eine Liste der Regionen, die Behebungsmaßnahmen für AWS Config Regeln Support, finden Sie unter Abhilfemaßnahmen | Regionalunterstützung.

Aggregatoren

- Eine Liste der Regionen, die Aggregatoren unterstützen, finden Sie unter Aggregatoren | Unterstützte Regionen.

Erweiterte Abfragen

- Eine Liste der Regionen, die erweiterte Abfragen unterstützen, finden Sie unter Erweiterte Abfragen | Unterstützte Regionen.
- Eine Liste der Regionen, die den Abfrageprozessor für natürliche Sprache für erweiterte Abfragen Support, finden Sie unter Abfrageprozessor für natürliche Sprache für erweiterte Abfragen | Regionsunterstützung.

Liste der unterstützten Regionen

In der folgenden Tabelle sind die AWS Regionen aufgeführt, in denen Sie die Option aktivieren können AWS Config.

Name der Region	Region	Endpunkt	Protocol (Protokoll)
USA Ost (Ohio)	us-east-2	config.us-east-2.amazonaws.com	HTTPS
		config-fips.us-east-2.amazonaws.com	HTTPS
USA Ost (Nord-Virginia)	us-east-1	config.us-east-1.amazonaws.com	HTTPS
		config-fips.us-east-1.amazonaws.com	HTTPS
USA West (Nordkalifornien)	us-west-1	config.us-west-1.amazonaws.com	HTTPS
		config-fips.us-west-1.amazonaws.com	HTTPS

Name der Region	Region	Endpunkt	Protocol (Protokoll)
USA West (Oregon)	us-west-2	config.us-west-2.amazonaws.com config-fips.us-west-2.amazonaws.com	HTTPS HTTPS
Afrika (Kapstadt)	af-south-1	config.af-south-1.amazonaws.com	HTTPS
Asien-Pazifik (Hongkong)	ap-east-1	config.ap-east-1.amazonaws.com	HTTPS
Asien-Pazifik (Hyderabad)	ap-south-2	config.ap-south-2.amazonaws.com	HTTPS
Asien-Pazifik (Jakarta)	ap-southeast-3	config.ap-southeast-3.amazonaws.com	HTTPS
Asien-Pazifik (Malaysia)	ap-southeast-5	config.ap-southeast-5.amazonaws.com	HTTPS
Asien-Pazifik (Melbourne)	ap-southeast-4	config.ap-southeast-4.amazonaws.com	HTTPS

Name der Region	Region	Endpunkt	Protocol (Protokoll)
Asien-Pazifik (Mumbai)	ap-south-1	config.ap-south-1.amazonaws.com	HTTPS
Asien-Pazifik (Osaka)	ap-northeast-3	config.ap-northeast-3.amazonaws.com	HTTPS
Asien-Pazifik (Seoul)	ap-northeast-2	config.ap-northeast-2.amazonaws.com	HTTPS
Asien-Pazifik (Singapur)	ap-southeast-1	config.ap-southeast-1.amazonaws.com	HTTPS
Asien-Pazifik (Sydney)	ap-southeast-2	config.ap-southeast-2.amazonaws.com	HTTPS
Asien-Pazifik (Taipeh)	ap-east-2	config.ap-east-2.amazonaws.com	HTTPS
Asien-Pazifik (Thailand)	ap-southeast-7	config.ap-southeast-7.amazonaws.com	HTTPS
Asien-Pazifik (Tokio)	ap-northeast-1	config.ap-northeast-1.amazonaws.com	HTTPS

Name der Region	Region	Endpunkt	Protocol (Protokoll)
Kanada (Zentral)	ca-central-1	config.ca-central-1.amazonaws.com	HTTPS
Kanada West (Calgary)	ca-west-1	config.ca-west-1.amazonaws.com	HTTPS
Europa (Frankfurt)	eu-central-1	config.eu-central-1.amazonaws.com	HTTPS
Europa (Irland)	eu-west-1	config.eu-west-1.amazonaws.com	HTTPS
Europa (London)	eu-west-2	config.eu-west-2.amazonaws.com	HTTPS
Europa (Mailand)	eu-south-1	config.eu-south-1.amazonaws.com	HTTPS
Europa (Paris)	eu-west-3	config.eu-west-3.amazonaws.com	HTTPS
Europa (Spanien)	eu-south-2	config.eu-south-2.amazonaws.com	HTTPS
Europa (Stockholm)	eu-north-1	config.eu-north-1.amazonaws.com	HTTPS
Europa (Zürich)	eu-central-2	config.eu-central-2.amazonaws.com	HTTPS
Israel (Tel Aviv)	il-central-1	config.il-central-1.amazonaws.com	HTTPS

Name der Region	Region	Endpunkt	Protocol (Protokoll)
Mexiko (Zentral)	mx-central-1	config.mx-central-1.amazonaws.com	HTTPS
Naher Osten (Bahrain)	me-south-1	config.me-south-1.amazonaws.com	HTTPS
Naher Osten (VAE)	me-central-1	config.me-central-1.amazonaws.com	HTTPS
Südamerika (São Paulo)	sa-east-1	config.sa-east-1.amazonaws.com	HTTPS
AWS GovCloud (US-Ost)	us-gov-east-1	config.us-gov-east-1.amazonaws.com	HTTPS
AWS GovCloud (US-West)	us-gov-west-1	config.us-gov-west-1.amazonaws.com	HTTPS

Servicebeschränkungen für AWS Config

In der folgenden Tabelle werden die darin enthaltenen Grenzwerte beschrieben AWS Config. Sofern nicht anders angegeben, können die Kontingente auf Anfrage erhöht werden. Sie können eine Kontingenterhöhung beantragen.

Informationen zu anderen Beschränkungen finden Sie AWS unter AWS Service Limits.

Ressourcen-Tags

Beschreibung	Grenzwert	Kann erhöht werden
Maximale Anzahl von Tags pro Ressource	50	Nein

AWS Config Regeln

Beschreibung	Grenzwert	Kann erhöht werden
Maximale Anzahl von AWS Config Regeln pro Region pro Konto	1000	Nein

Conformance Packs für Einzelkonten

Beschreibung	Grenzwert	Kann erhöht werden
Maximale Anzahl an Conformance Packs pro Konto	50	Nein
Maximale Anzahl von AWS Config Regeln pro Conformance Pack	130	Nein

> **Note**
>
> AWS Config Regeln in Konformitätspaketen zählen zum Limit für die maximale Anzahl von AWS Config Regeln pro Region pro Konto.

Conformance Packs für Organisationen

Beschreibung	Grenzwert	Kann erhöht werden
Maximale Anzahl an Conformance Packs pro Organisation	50	Nein
Maximale Anzahl von AWS Config Regeln pro Unternehmens-Konformitätspaket	130	Nein

> **Note**
>
> Die Bereitstellung auf Organisationsebene zählt zum Limit für Kinderkonten. AWS Config Regeln in Conformance Packs zählen zum Limit für die maximale Anzahl von AWS Config Regeln pro Region und Konto.

Aggregatoren

Beschreibung	Grenzwert	Kann erhöht werden
Maximale Anzahl der Konfigurations-Aggregatoren	50	Ja
Maximale Anzahl von Konten in einem Aggregator	10000	Nein
Maximale Anzahl der pro Woche hinzugefügten oder gelöschten Konten für alle Aggregatoren	1000	Ja

> **Note**
>
> Aggregatoren auf Organisationsebene und Aggregatoren für einzelne Konten werden beide in das Limit für die maximale Anzahl von Konfigurationsaggregatoren einbezogen.

Erweiterte Abfragen

Beschreibung	Grenzwert	Kann erhöht werden
Maximale Anzahl von gespeicherten Abfragen in einem einzelnen Konto und einer Region	300	Ja

Zusätzliche Informationen und verwandte Ressourcen für AWS Config

Die folgenden verwandten Ressourcen bieten Ihnen nützliche Informationen für die Arbeit mit diesem Service.

- AWS Config— Die primäre Webseite für Informationen über AWS Config.
- AWS Config – Preise
- Häufig gestellte technische Fragen zu https://aws.amazon.com/config/faq/
- AWS Config Rule Development Kit (RDK) — Ein Open-Source-Tool, mit dem Sie Regeln einrichten AWS Config, verfassen und anschließend mit einer Vielzahl von AWS Ressourcentypen testen können.
- Partner — Links zu Partnerprodukten, die vollständig integriert sind und Ihnen helfen, AWS Config die Daten aus Ihrem Konfigurations-Stream, Ihren Konfigurations-Snapshots oder Ihrem Konfigurationsverlauf zu visualisieren, zu überwachen und zu verwalten.
- Kurse und Workshops — Links zu rollen- und Spezialkursen sowie zu Übungen zum Selbststudium, mit denen Sie Ihre AWS Fähigkeiten verbessern und praktische Erfahrungen sammeln können.

- AWS Developer Center — Erkunden Sie Tutorials, laden Sie Tools herunter und erfahren Sie mehr über Veranstaltungen für Entwickler. AWS
- AWS Entwicklertools — Links zu Entwicklertools SDKs, IDE-Toolkits und Befehlszeilentools für die Entwicklung und Verwaltung von AWS Anwendungen.
- Ressourcencenter für die ersten Schritte — Erfahren Sie AWS-Konto, wie Sie Ihre erste Anwendung einrichten, der AWS Community beitreten und sie starten.
- Praktische Tutorials — Folgen Sie den step-by-step Tutorials, um Ihre erste Anwendung zu starten. AWS
- AWS Whitepapers — Links zu einer umfassenden Liste von technischen AWS Whitepapers zu Themen wie Architektur, Sicherheit und Wirtschaft, die von Solutions Architects oder anderen technischen Experten verfasst wurden. AWS
- AWS -Support Center — Die zentrale Anlaufstelle für die Erstellung und Verwaltung Ihrer Fälle. AWS -Support Enthält auch Links zu anderen hilfreichen Ressourcen wie Foren, technischen FAQs Informationen, Servicestatus und AWS Trusted Advisor.
- Support— Die wichtigste Webseite mit Informationen über Support einen Support-Kanal mit schnellen Reaktionszeiten one-on-one, der Sie bei der Entwicklung und Ausführung von Anwendungen in der Cloud unterstützt.
- Kontakt – Zentraler Kontaktpunkt für Fragen zu AWS -Abrechnung, Konten, Ereignissen Missbrauch und anderen Problemen.
- AWS Nutzungsbedingungen der Website — Detaillierte Informationen zu unseren Urheberrechten und Marken, zu Ihrem Konto, Ihrer Lizenz und Ihrem Zugriff auf die Website sowie zu anderen Themen.

AWS Software-Entwicklungskits für AWS Config

Ein AWS Software Development Kit (SDK) erleichtert die Erstellung von Anwendungen, die auf kostengünstige, skalierbare und zuverlässige AWS Infrastrukturdienste zugreifen. Mit einem einzigen herunterladbaren Paket AWS SDKs, das die Bibliothek, Codebeispiele und Referenzdokumentation enthält, können Sie innerhalb von Minuten loslegen. In der folgenden Tabelle sind die verfügbaren Bibliotheken SDKs und Bibliotheken von Drittanbietern aufgeführt, mit denen Sie AWS Config programmgesteuert zugreifen können.

Zugriffstyp	Beschreibung
AWS SDKs	AWS stellt Folgendes bereit: SDKs

Zugriffstyp	Beschreibung
	• AWS SDK for C++ C++-Dokumentation • AWS Mobile SDK for iOS Dokumentation • AWS SDK for Go – Dokumentation • AWS SDK für Java Dokumentation • AWS SDK für JavaScript Dokumentation • AWS SDK für .NET Dokumentation • AWS SDK für PHP Dokumentation • AWS SDK for Python (Boto) Dokumentation • AWS SDK für Ruby Dokumentation
Bibliotheken von Drittanbietern	Entwickler in der AWS Entwickler-Community stellen auch ihre eigenen Bibliotheken zur Verfügung, die Sie in den folgenden AWS Developer Centern finden: • AWS Java Developer Center • AWS JavaScript-Entwicklerzentrum • AWS PHP-Entwicklungszentrum • AWS Python-Entwicklerzentrum • AWS Ruby Developer Center • AWS Windows- und .NET Developer Center

Erste Schritte mit AWS Config

AWS Config bietet einen detaillierten Überblick über die Konfiguration der AWS Ressourcen in Ihrem AWS-Konto. Mit AWS Config können Sie Änderungen an Konfigurationen und Beziehungen zwischen AWS Ressourcen überprüfen, den Verlauf der Ressourcenkonfiguration untersuchen und Regeln verwenden, um die Einhaltung der Vorschriften zu ermitteln. Weitere Informationen finden Sie unter Was ist AWS Config? und wie AWS Config funktioniert.

Melde dich an für AWS

Themen

- Melde dich an für ein AWS-Konto
- Erstellen eines Benutzers mit Administratorzugriff

Melde dich an für ein AWS-Konto

Wenn Sie noch keine haben AWS-Konto, führen Sie die folgenden Schritte aus, um eine zu erstellen.

Um sich für eine anzumelden AWS-Konto

1. Öffnen Sie https://portal.aws.amazon.com/billing/die Anmeldung.
2. Folgen Sie den Online-Anweisungen.

   Ein Teil des Anmeldevorgangs umfasst den Empfang eines Telefonanrufs oder einer Textnachricht und die Eingabe eines Bestätigungscodes auf der Telefontastatur.

   Wenn Sie sich für eine anmelden AWS-Konto, wird eine Root-Benutzer des AWS-Kontoserstellt. Der Root-Benutzer hat Zugriff auf alle AWS-Services und Ressourcen des Kontos. Als bewährte Sicherheitsmethode weisen Sie einem Administratorbenutzer Administratorzugriff zu und verwenden Sie nur den Root-Benutzer, um Aufgaben auszuführen, die Root-Benutzerzugriff erfordern.

AWS sendet Ihnen nach Abschluss des Anmeldevorgangs eine Bestätigungs-E-Mail. Du kannst jederzeit deine aktuellen Kontoaktivitäten einsehen und dein Konto verwalten, indem du zu https://aws.amazon.com/gehst und Mein Konto auswählst.

Erstellen eines Benutzers mit Administratorzugriff

Nachdem Sie sich für einen angemeldet haben AWS-Konto, sichern Sie Ihren Root-Benutzer des AWS-Kontos AWS IAM Identity Center, aktivieren und erstellen Sie einen Administratorbenutzer, sodass Sie den Root-Benutzer nicht für alltägliche Aufgaben verwenden.

Sichern Sie Ihre Root-Benutzer des AWS-Kontos

1. Melden Sie sich AWS Management Consoleals Kontoinhaber an, indem Sie Root-Benutzer auswählen und Ihre AWS-Konto E-Mail-Adresse eingeben. Geben Sie auf der nächsten Seite Ihr Passwort ein.

   Hilfe bei der Anmeldung mit dem Root-Benutzer finden Sie unter Anmelden als Root-Benutzer im AWS-Anmeldung Benutzerhandbuch zu.
2. Aktivieren Sie die Multi-Faktor-Authentifizierung (MFA) für den Root-Benutzer.

   Anweisungen finden Sie unter Aktivieren eines virtuellen MFA-Geräts für Ihren AWS-Konto Root-Benutzer (Konsole) im IAM-Benutzerhandbuch.

Erstellen eines Benutzers mit Administratorzugriff

1. Aktivieren Sie das IAM Identity Center.

   Anweisungen finden Sie unter Aktivieren AWS IAM Identity Center im AWS IAM Identity Center Benutzerhandbuch.
2. Gewähren Sie einem Administratorbenutzer im IAM Identity Center Benutzerzugriff.

   Ein Tutorial zur Verwendung von IAM-Identity-Center-Verzeichnis als Identitätsquelle finden Sie IAM-Identity-Center-Verzeichnis im Benutzerhandbuch unter Benutzerzugriff mit der Standardeinstellung konfigurieren.AWS IAM Identity Center

Anmelden als Administratorbenutzer

- Um sich mit Ihrem IAM-Identity-Center-Benutzer anzumelden, verwenden Sie die Anmelde-URL, die an Ihre E-Mail-Adresse gesendet wurde, als Sie den IAM-Identity-Center-Benutzer erstellt haben.

  Hilfe bei der Anmeldung mit einem IAM Identity Center-Benutzer finden Sie im AWS-Anmeldung Benutzerhandbuch unter Anmeldung beim AWS Access-Portal.

Weiteren Benutzern Zugriff zuweisen

1. Erstellen Sie im IAM-Identity-Center einen Berechtigungssatz, der den bewährten Vorgehensweisen für die Anwendung von geringsten Berechtigungen folgt.

   Anweisungen hierzu finden Sie unter Berechtigungssatz erstellen im AWS IAM Identity Center Benutzerhandbuch.

2. Weisen Sie Benutzer einer Gruppe zu und weisen Sie der Gruppe dann Single Sign-On-Zugriff zu.

   Eine genaue Anleitung finden Sie unter Gruppen hinzufügen im AWS IAM Identity Center Benutzerhandbuch.

Möglichkeiten zum Einstieg mit AWS Config

Nachdem Sie sich für eine angemeldet haben AWS-Konto, können Sie AWS Config mit dem AWS Management Console, AWS CLI oder dem beginnen AWS SDKs.

- Einrichtung AWS Config mit der Konsole
- Einrichtung AWS Config mit dem AWS CLI
- Verwenden des AWS Config Dienstes mit dem AWS SDK

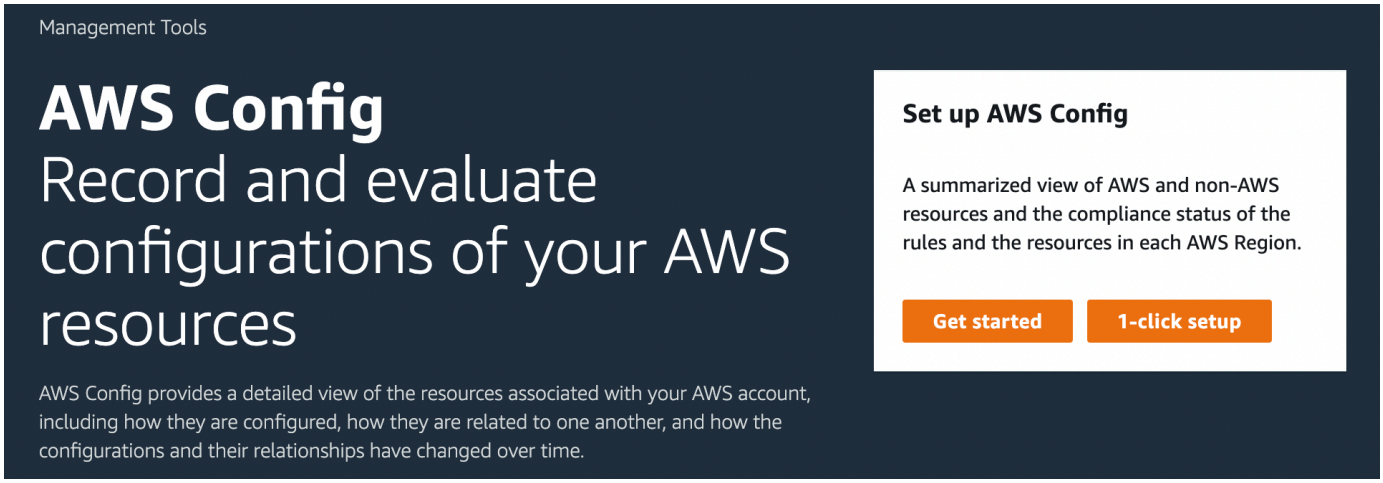
Einrichtung AWS Config mit der Konsole

Das AWS Management Console bietet einen schnellen und optimierten AWS Config Einrichtungsprozess.

Einrichtung

Zur Einrichtung AWS Config mit der Konsole

1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die AWS Config Konsole zu https://console.aws.amazon.com/config/Hause.
2. Wenn Sie die Konsole zum ersten Mal öffnen oder wenn Sie die AWS Config Konsole AWS Config in einer neuen Region einrichten, sieht die AWS Config Konsolenseite wie folgt aus:



3. Wählen Sie das 1-Klick-Setup aus, um es auf AWS der AWS Config Grundlage von Best Practices zu starten. Sie können auch Erste Schritte wählen, um einen detaillierteren Einrichtungsprozess durchzuführen.

Themen

- 1-Klick-Setup für AWS Config
- Manuelle Einrichtung für AWS Config

1-Klick-Setup für AWS Config

AWS Config Die Einrichtung mit einem Klick vereinfacht den Einstieg für AWS Config Konsolenkunden, indem die Anzahl der manuellen Auswahlen reduziert wird. Informationen zu allen manuellen Auswahlen des Einrichtungsvorgangs finden Sie unter Manuelle Einrichtung.

Zur Einrichtung AWS Config mit der Konsole mit 1-Klick-Setup

1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die AWS Config Konsole zu https://console.aws.amazon.com/config/Hause.
2. Wählen Sie Einrichten mit einem Klick aus.

Die Einrichtungsseite umfasst drei Schritte, aber durch den Workflow zum Einrichten mit einem Klick werden Sie automatisch zu Schritt 3 (Überprüfung) weitergeleitet. Im Folgenden finden Sie eine Aufgliederung dieses Verfahrens.

- Einstellungen: Wählen Sie aus, wie die AWS Config Konsole Ressourcen und Rollen aufzeichnet, und wählen Sie aus, wohin der Konfigurationsverlauf und die Konfigurations-Snapshot-Dateien gesendet werden sollen.
- Regeln: Für AWS-Regionen diese AWS Config Support-Regeln steht Ihnen dieser Schritt zur Verfügung, um erste verwaltete Regeln zu konfigurieren, die Sie Ihrem Konto hinzufügen können. Nach der Einrichtung AWS Config werden Ihre AWS Ressourcen anhand der von Ihnen ausgewählten Regeln bewertet. Zusätzliche Regeln können erstellt und bestehende Regeln nach der Einrichtung in Ihrem Konto aktualisiert werden.
- Überprüfung: Um Ihre Einrichtungsdetails zu überprüfen.

Schritt 1: Einstellungen

Strategie für die Aufzeichnung

Die Option zum Aufzeichnen aller Ressourcentypen mit anpassbaren Überschreibungen ist für Sie ausgewählt. AWS Config zeichnet alle aktuellen und future unterstützten Ressourcentypen in dieser Region auf. Weitere Informationen finden Sie unter Unterstützte Ressourcentypen.

- Standardeinstellungen

  Die Standardaufzeichnungsfrequenz ist für Sie auf Kontinuierlich eingestellt. Das bedeutet, dass Konfigurationsänderungen bei jeder Änderung kontinuierlich AWS Config aufgezeichnet werden.

  AWS Config unterstützt auch die Option, die Aufnahmefrequenz auf Täglich einzustellen. Wenn Sie nach der Einrichtung diese Option wählen, erhalten Sie ein Konfigurationselement (CI), das den aktuellen Status Ihrer Ressourcen in den letzten 24 Stunden repräsentiert, nur dann, wenn es sich von dem zuvor aufgezeichneten CI unterscheidet. Weitere Informationen finden Sie unter Aufzeichnungsfrequenz.

  > **Note**
  >
  > AWS Firewall Manager hängt von der kontinuierlichen Aufzeichnung ab, um Ihre Ressourcen zu überwachen. Wenn Sie den Firewall Manager verwenden, wird empfohlen, die Aufzeichnungsfrequenz auf „Kontinuierlich“ einzustellen.

- Einstellungen überschreiben – optional

Sie können nach der Einrichtung optional die Aufzeichnungsfrequenz für bestimmte Ressourcentypen außer Kraft setzen oder bestimmte Ressourcentypen von der Aufzeichnung ausschließen. Um die Standardeinstellungen zu überschreiben, wählen Sie im linken Navigationsbereich der AWS Config Konsole Einstellungen und dann Bearbeiten aus.

Überlegungen beim Aufzeichnen von Ressourcen

Hohe Anzahl von AWS Config Bewertungen

Möglicherweise stellen Sie während Ihres ersten Monats, in dem Sie mit AWS Config aufgezeichnet haben, eine erhöhte Aktivität in Ihrem Konto im Vergleich zu den Folgemonaten fest. AWS Config Führt während des ersten Bootstrapping-Vorgangs Evaluierungen aller Ressourcen in Ihrem Konto durch, die Sie für AWS Config die Aufzeichnung ausgewählt haben.

Wenn Sie flüchtige Workloads ausführen, sehen Sie möglicherweise eine erhöhte Aktivität durch AWS Config , da Konfigurationsänderungen im Zusammenhang mit dem Erstellen und Löschen dieser temporären Ressourcen aufgezeichnet werden. Eine flüchtige Workload ist eine vorübergehende Nutzung von Computing-Ressourcen, die bei Bedarf geladen und ausgeführt werden. Beispiele hierfür sind Amazon Elastic Compute Cloud (Amazon EC2) Spot-Instances, Amazon EMR-Jobs und AWS Auto Scaling. Wenn Sie die erhöhte Aktivität durch die Ausführung kurzlebiger Workloads vermeiden möchten, können Sie den Konfigurationsrekorder so einrichten, dass diese Ressourcentypen von der Aufzeichnung ausgeschlossen werden, oder Sie können diese Arten von Workloads in einem separaten Konto ausführen, das AWS Config ausgeschaltet ist, um eine erhöhte Konfigurationsaufzeichnung und Regelauswertung zu vermeiden.

Globale Ressourcentypen | Die globalen Aurora-Cluster sind zunächst in der Aufzeichnung enthalten

Der `AWS::RDS::GlobalCluster` Ressourcentyp wird in allen unterstützten AWS Config Regionen aufgezeichnet, in denen der Konfigurationsrekorder aktiviert ist.

Wenn Sie `AWS::RDS::GlobalCluster` nicht in allen aktivierten Regionen aufzeichnen möchten, können Sie diesen Ressourcentyp nach der Einrichtung von der Aufzeichnung ausschließen. Wählen Sie in der linken Navigationsleiste Einstellungen und dann Grundlegend. Wechseln Sie von Bearbeiten zu Einstellungen überschreiben im Abschnitt Aufzeichnungsverfahren, wählen Sie `AWS::RDS::GlobalCluster` und dann „Von Aufzeichnung ausschließen“.

Globale Ressourcentypen | IAM-Ressourcentypen sind zunächst von der Aufzeichnung ausgeschlossen

„Alle global aufgezeichneten IAM-Ressourcentypen“ sind zunächst von der Aufzeichnung ausgeschlossen, um Ihnen zu helfen, die Kosten zu senken. Dieses Paket umfasst IAM-Benutzer, -Gruppen, -Rollen und vom Kunden verwaltete Richtlinien. Wählen Sie Entfernen, um die Überschreibung zu entfernen und diese Ressourcen in Ihre Aufzeichnung aufzunehmen.

Darüber hinaus können die globalen IAM-Ressourcentypen (`AWS::IAM::User`, `AWS::IAM::Group`, `AWS::IAM::Role` und `AWS::IAM::Policy`) nicht in Regionen erfasst werden, die AWS Config nach Februar 2022 unterstützt. Eine Liste dieser Regionen finden Sie unter AWS Aufzeichnungsressourcen | Globale Ressourcen.

Datenverwaltung

In diesem Abschnitt wird für Sie die Standarddauer für die Aufbewahrung von AWS Config Daten für 7 Jahre (2557 Tage) ausgewählt.

Die Option „Eine bestehende AWS Config serviceverknüpfte Rolle verwenden“ wird für Sie ausgewählt und auf die AWS Config Rolle festgelegt. Dienstbezogene Rollen sind durch alle Berechtigungen vordefiniert AWS Config und enthalten alle Berechtigungen, die der Dienst benötigt, um andere AWS Dienste aufzurufen.

Bereitstellungsmethode

In diesem Abschnitt ist die Option Bucket aus Ihrem Konto auswählen bereits für Sie ausgewählt. Bei dieser Auswahl wird standardmäßig der Bucket in Ihrem Konto verwendet, der im Format `config-bucket-`*`accountid`* benannt ist. Beispiel, `config-bucket-012345678901`. Wenn Sie keinen Bucket in diesem Format erstellt haben, wird einer für Sie erstellt. Informationen zum Erstellen eines Buckets finden Sie unter Erstellen eines Buckets im Benutzerhandbuch für Amazon Simple Storage Service.

Weitere Informationen über S3-Buckets finden Sie unter Bucket-Übersicht im Benutzerhandbuch für Amazon Simple Storage Service.

Schritt 2: Regeln

Unter AWS -verwaltete Regeln werden in diesem Schritt keine Regeln für Sie ausgewählt. Stattdessen werden Sie aufgefordert, Regeln zu erstellen und zu aktualisieren, nachdem Sie die Einrichtung Ihres Kontos abgeschlossen haben.

Schritt 3: Prüfen

Überprüfe deine AWS Config Einrichtungsdetails. Sie können die Änderungen für jeden Abschnitt auch zu einem späteren Zeitpunkt noch bearbeiten. Wählen Sie Bestätigen, um die Einrichtung abzuschließen AWS Config.

Manuelle Einrichtung für AWS Config

Mit dem Workflow Erste Schritte können Sie alle manuellen Auswahlen des Einrichtungsvorgangs durchführen, um mit der AWS Config Konsole zu beginnen. Einen vereinfachten Vorgang für die ersten Schritte finden Sie unter Einrichtung mit einem Klick.

So richten Sie die Einrichtung AWS Config über die Konsole mithilfe von Get Started ein

1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die AWS Config Konsole zu https://console.aws.amazon.com/config/Hause.
2. Wählen Sie Erste Schritte.

Die Einrichtungsseite umfasst drei Schritte. Im Folgenden finden Sie eine Aufgliederung dieses Verfahrens, nachdem Sie Erste Schritte ausgewählt haben.

- Einstellungen: Wählen Sie aus, wie die AWS Config Konsole Ressourcen und Rollen aufzeichnet, und wählen Sie aus, wohin der Konfigurationsverlauf und die Konfigurations-Snapshot-Dateien gesendet werden sollen.
- Regeln: Für AWS-Regionen diese AWS Config Support-Regeln steht Ihnen dieser Schritt zur Verfügung, um erste verwaltete Regeln zu konfigurieren, die Sie Ihrem Konto hinzufügen können. Nach der Einrichtung AWS Config werden Ihre AWS Ressourcen anhand der von Ihnen ausgewählten Regeln bewertet. Zusätzliche Regeln können erstellt und bestehende Regeln nach der Einrichtung in Ihrem Konto aktualisiert werden.
- Überprüfung: Um Ihre Einrichtungsdetails zu überprüfen.

Schritt 1: Einstellungen

Strategie für die Aufzeichnung

Wählen Sie im Abschnitt Aufzeichnungsverfahren eine Aufzeichnungsstrategie aus. Sie können die AWS Ressourcen angeben, die Sie aufzeichnen AWS Config möchten.

All resource types with customizable overrides

AWS Config So eingerichtet, dass Konfigurationsänderungen für alle aktuellen und future unterstützten Ressourcentypen in dieser Region aufgezeichnet werden. Sie können die Aufzeichnungsfrequenz für bestimmte Ressourcentypen außer Kraft setzen oder bestimmte Ressourcentypen von der Aufzeichnung ausschließen. Weitere Informationen finden Sie unter Unterstützte Ressourcentypen.

- Standardeinstellungen

  Konfigurieren Sie die Standardaufzeichnungsfrequenz für alle derzeit und zukünftig unterstützten Ressourcentypen. Weitere Informationen finden Sie unter Aufzeichnungsfrequenz.

  - Kontinuierliche Aufzeichnung — AWS Config zeichnet Konfigurationsänderungen kontinuierlich auf, wenn eine Änderung eintritt.
  - Tägliche Aufzeichnung – Sie erhalten ein Konfigurationselement (CI), das den aktuellen Status Ihrer Ressourcen in den letzten 24 Stunden nur dann darstellt, wenn es sich von dem zuvor aufgezeichneten CI unterscheidet.

  > **Note**
  >
  > AWS Firewall Manager hängt von der kontinuierlichen Aufzeichnung ab, um Ihre Ressourcen zu überwachen. Wenn Sie den Firewall Manager verwenden, wird empfohlen, die Aufzeichnungsfrequenz auf „Kontinuierlich“ einzustellen.

- Überschreibungseinstellungen

  Setzen Sie die Aufzeichnungsfrequenz für bestimmte Ressourcentypen außer Kraft oder schließen Sie bestimmte Ressourcentypen von der Aufzeichnung aus. Wenn Sie die Aufzeichnungsfrequenz für einen Ressourcentyp ändern, bleiben die bereits aufgezeichneten Konfigurationselemente unverändert.

Specific resource types

Legen AWS Config Sie fest, dass Konfigurationsänderungen nur für die von Ihnen angegebenen Ressourcentypen aufgezeichnet werden.

- Bestimmte Ressourcentypen

Wählen Sie einen Ressourcentyp und dessen Aufzeichnungsfrequenz aus. Weitere Informationen finden Sie unter Aufzeichnungsfrequenz.

- Kontinuierliche Aufzeichnung — AWS Config zeichnet Konfigurationsänderungen kontinuierlich auf, wenn eine Änderung eintritt.
- Tägliche Aufzeichnung – Sie erhalten ein Konfigurationselement (CI), das den aktuellen Status Ihrer Ressourcen in den letzten 24 Stunden nur dann darstellt, wenn es sich von dem zuvor aufgezeichneten CI unterscheidet.

> **Note**
>
> AWS Firewall Manager hängt von der kontinuierlichen Aufzeichnung ab, um Ihre Ressourcen zu überwachen. Wenn Sie den Firewall Manager verwenden, wird empfohlen, die Aufzeichnungsfrequenz auf „Kontinuierlich“ einzustellen.

Wenn Sie die Aufzeichnungsfrequenz für einen Ressourcentyp ändern, bleiben die bereits aufgezeichneten Konfigurationselemente unverändert.

Überlegungen beim Aufzeichnen von Ressourcen

Hohe Anzahl von AWS Config Bewertungen

Möglicherweise stellen Sie während Ihres ersten Monats, in dem Sie mit AWS Config aufgezeichnet haben, eine erhöhte Aktivität in Ihrem Konto im Vergleich zu den Folgemonaten fest. AWS Config Führt während des ersten Bootstrapping-Vorgangs Evaluierungen aller Ressourcen in Ihrem Konto durch, die Sie für AWS Config die Aufzeichnung ausgewählt haben.

Wenn Sie flüchtige Workloads ausführen, sehen Sie möglicherweise eine erhöhte Aktivität durch AWS Config , da Konfigurationsänderungen im Zusammenhang mit dem Erstellen und Löschen dieser temporären Ressourcen aufgezeichnet werden. Eine flüchtige Workload ist eine vorübergehende Nutzung von Computing-Ressourcen, die bei Bedarf geladen und ausgeführt werden. Beispiele hierfür sind Amazon Elastic Compute Cloud (Amazon EC2) Spot-Instances, Amazon EMR-Jobs und AWS Auto Scaling. Wenn Sie die erhöhte Aktivität durch die Ausführung kurzlebiger Workloads vermeiden möchten, können Sie den Konfigurationsrekorder so einrichten, dass diese Ressourcentypen von der Aufzeichnung ausgeschlossen werden, oder Sie können diese Arten von Workloads in einem separaten Konto ausführen, das AWS Config ausgeschaltet ist, um eine erhöhte Konfigurationsaufzeichnung und Regelauswertung zu vermeiden.

Considerations: All resource types with customizable overrides

Global aufgezeichnete Ressourcentypen | Die globalen Aurora-Cluster sind zunächst in der Aufzeichnung enthalten

Der `AWS::RDS::GlobalCluster` Ressourcentyp wird in allen unterstützten AWS Config Regionen aufgezeichnet, in denen der Konfigurationsrekorder aktiviert ist.

Wenn Sie `AWS::RDS::GlobalCluster` nicht in allen aktivierten Regionen aufzeichnen möchten, wählen Sie „AWS RDS GlobalCluster“ und dann die Option „Von der Aufzeichnung ausschließen“.

Globale Ressourcentypen | IAM-Ressourcentypen sind zunächst von der Aufzeichnung ausgeschlossen

Die globalen IAM-Ressourcentypen sind zunächst von der Aufzeichnung ausgeschlossen, um Ihnen zu helfen, die Kosten zu senken. Dieses Paket umfasst IAM-Benutzer, -Gruppen, -Rollen und vom Kunden verwaltete Richtlinien. Wählen Sie Entfernen, um die Überschreibung zu entfernen und diese Ressourcen in Ihre Aufzeichnung aufzunehmen.

Darüber hinaus können die globalen IAM-Ressourcentypen (`AWS::IAM::User`, `AWS::IAM::Group``AWS::IAM::Role`, und`AWS::IAM::Policy`) nicht in Regionen aufgezeichnet werden, die AWS Config nach Februar 2022 unterstützt werden. Eine Liste dieser Regionen finden Sie unter AWS Aufzeichnungsressourcen | Globale Ressourcen.

Beschränkungen

Sie können bis zu 100 Frequenzüberschreibungen und 600 Ausschlussüberschreibungen hinzufügen.

Die tägliche Aufzeichnung kann für die folgenden Ressourcentypen nicht angegeben werden:

- `AWS::Config::ResourceCompliance`
- `AWS::Config::ConformancePackCompliance`
- `AWS::Config::ConfigurationRecorder`

Considerations: Specific resource types

Verfügbarkeit in Regionen

Bevor Sie einen Ressourcentyp für AWS Config die Nachverfolgung angeben, überprüfen Sie, ob der Ressourcentyp in der AWS Region, in der Sie ihn eingerichtet haben, unterstützt wird AWS Config. Wenn ein Ressourcentyp AWS Config in mindestens einer Region unterstützt wird, können Sie die Aufzeichnung dieses Ressourcentyps in allen Regionen aktivieren, die von unterstützt werden AWS Config, auch wenn der angegebene Ressourcentyp in der AWS Region, in der Sie ihn eingerichtet haben, nicht unterstützt wird AWS Config.

Beschränkungen

Keine Beschränkungen, wenn alle Ressourcentypen dieselbe Frequenz haben. Sie können bis zu 100 Ressourcentypen mit täglicher Aufzeichnungsfrequenz hinzufügen, wenn mindestens ein Ressourcentyp auf „Kontinuierlich“ gesetzt ist.

Die tägliche Frequenz wird für die folgenden Ressourcentypen nicht unterstützt:

- `AWS::Config::ResourceCompliance`
- `AWS::Config::ConformancePackCompliance`
- `AWS::Config::ConfigurationRecorder`

Datenverwaltung

- Wählen Sie unter Datenaufbewahrungszeitraum entweder den Standardaufbewahrungszeitraum für die Aufbewahrung von AWS Config Daten für 7 Jahre (2557) oder legen Sie einen benutzerdefinierten Aufbewahrungszeitraum für Elemente fest, die von aufgezeichnet wurden. AWS Config

  AWS Config ermöglicht es Ihnen, Ihre Daten zu löschen, indem Sie eine Aufbewahrungsfrist für Ihre Daten angeben. `ConfigurationItems` Wenn Sie einen Aufbewahrungszeitraum angeben, bewahrt AWS Config Ihre `ConfigurationItems` im angegebenen Zeitraum auf. Sie können einen Zeitraum zwischen mindestens 30 Tagen und maximal 7 Jahren (2557 Tage) wählen. AWS Config löscht Daten, die älter sind als die angegebene Aufbewahrungsfrist.
- Wählen Sie unter IAM-Rolle für AWS Config entweder eine bestehende AWS Config serviceverknüpfte Rolle oder eine IAM-Rolle aus Ihrem Konto aus.
  - Mit Diensten verknüpfte Rollen sind durch alle Berechtigungen vordefiniert AWS Config und enthalten alle Berechtigungen, die der Dienst zum Aufrufen anderer Dienste benötigt. AWS

> **Note**
>
> Empfehlung: Verwenden Sie die mit dem Dienst verknüpfte Rolle
> Es wird empfohlen, die dienstverknüpfte Rolle zu verwenden. Eine dienstverknüpfte Rolle fügt alle erforderlichen Berechtigungen hinzu, damit sie wie erwartet ausgeführt werden AWS Config kann.

- Andernfalls wählen Sie eine IAM-Rolle aus einer Ihrer bereits vorhandenen Rollen und Berechtigungsrichtlinien aus.

> **Note**
>
> Richtlinien und Compliance-Ergebnisse
> IAM-Richtlinien und andere Richtlinien, die in verwaltet werden, AWS Organizations können sich darauf auswirken, ob Sie AWS Config berechtigt sind, Konfigurationsänderungen für Ihre Ressourcen aufzuzeichnen. Darüber hinaus bewerten Regeln direkt die Konfiguration einer Ressource, und Regeln berücksichtigen diese Richtlinien bei der Durchführung von Evaluierungen nicht. Stellen Sie sicher, dass die geltenden Richtlinien mit der Art und Weise übereinstimmen, wie Sie sie verwenden möchten AWS Config.
> Behalten Sie bei der Wiederverwendung einer IAM-Rolle die Mindestberechtigungen bei
> Wenn Sie einen AWS Dienst verwenden, der beispielsweise AWS Security Hub oder verwendet AWS Config AWS Control Tower, und bereits eine IAM-Rolle erstellt wurde, stellen Sie sicher, dass die IAM-Rolle, die Sie bei der Einrichtung verwenden, dieselben Mindestberechtigungen wie die bereits vorhandene IAM-Rolle AWS Config beibehält. Sie müssen dies tun, um sicherzustellen, dass der andere AWS Dienst weiterhin wie erwartet ausgeführt wird.
> Wenn er beispielsweise AWS Control Tower über eine IAM-Rolle verfügt, die das Lesen von S3-Objekten ermöglicht AWS Config , stellen Sie sicher, dass der IAM-Rolle, die Sie bei der Einrichtung verwenden, dieselben Berechtigungen gewährt werden. AWS Config Andernfalls kann es zu Störungen der Funktionsweise von AWS Control Tower kommen.

Bereitstellungsmethode

- Wählen Sie als Bereitstellungsmethode den S3-Bucket aus, an den AWS Config Konfigurationsverlaufs- und Konfigurations-Snapshot-Dateien sendet:

- Bucket erstellen – Geben Sie im Feld für den Namen des S3-Buckets einen entsprechenden Namen ein.

  Der von Ihnen eingegebene Bucket-Name muss unter allen in Amazon S3 vorhandenen Bucket-Namen eindeutig sein. Eine Möglichkeit, Eindeutigkeit sicherzustellen, besteht darin, ein Präfix einzufügen, z. B. den Namen Ihres Unternehmens. Sie können den Bucket-Namen nicht ändern, nachdem er erstellt wurde. Weitere Informationen finden Sie unter Bucket-Einschränkungen und -Limits im Benutzerhandbuch zu Amazon Simple Storage Service.
- Bucket aus Ihrem Konto auswählen – Wählen Sie unter Namen des S3-Buckets Ihren bevorzugten Bucket aus.
- Bucket aus einem anderen Konto auswählen – Geben Sie unter Namen des S3-Buckets den Bucket-Namen ein.

  > **Note**
  >
  > Bucket-Berechtigungen
  > Wenn Sie einen Bucket aus einem anderen Konto auswählen, muss dieser Bucket über Richtlinien verfügen, die Zugriffsberechtigungen für gewähren AWS Config. Weitere Informationen finden Sie unter Berechtigungen für den Amazon S3 S3-Bucket für den AWS Config Lieferkanal.

- Wählen Sie für Amazon SNS SNS-Thema die Option Konfigurationsänderungen und Benachrichtigungen zu einem Amazon SNS SNS-Thema streamen, um Benachrichtigungen wie die Lieferung des Konfigurationsverlaufs, die Bereitstellung von Konfigurations-Snapshots und die Einhaltung von Vorschriften zu AWS Config senden.
- Wenn Sie sich für den AWS Config Stream zu einem Amazon SNS SNS-Thema entschieden haben, wählen Sie das Zielthema aus:
  - Thema erstellen – Geben Sie unter Themenname einen Namen für Ihr SNS-Thema ein.
  - Thema aus Ihrem Konto auswählen – Wählen Sie unter Themenname Ihr bevorzugtes Thema aus.
  - Thema aus einem anderen Konto auswählen – Geben Sie unter Thema-ARN den Amazon-Ressourcennamen des Themas ein. Wenn Sie ein Thema aus einem anderen Konto auswählen, muss das Thema über Richtlinien verfügen, die Zugriffsberechtigungen für gewähren AWS Config. Weitere Informationen finden Sie unter Berechtigungen für das Amazon-SNS-Thema.

> **Note**
>
> Region für das Amazon SNS SNS-Thema
> Das Amazon SNS SNS-Thema muss in derselben Region existieren wie die Region, in der Sie es eingerichtet AWS Config haben.

Schritt 2: Regeln

Wenn Sie AWS Config in einer Region einrichten, die Regeln unterstützt, wählen Sie Weiter.

Schritt 3: Prüfen

Überprüfen Sie Ihre AWS Config Einrichtungsdetails. Sie können die Änderungen für jeden Abschnitt auch zu einem späteren Zeitpunkt noch bearbeiten. Wählen Sie Bestätigen, um die Einrichtung abzuschließen AWS Config.

Weitere Informationen

Informationen zum Nachschlagen der vorhandenen Ressourcen in Ihrem Konto und zum Verständnis der Konfigurationen Ihrer Ressourcen finden Sie unter Ressourcen suchen, Compliance-Informationen anzeigen und Konformitätsverlauf anzeigen.

Sie können Amazon Simple Queue Service auch verwenden, um AWS Ressourcen programmgesteuert zu überwachen. Weitere Informationen finden Sie unter Überwachen von AWS Ressourcenänderungen mit Amazon SQS.

Einrichtung AWS Config mit dem AWS CLI

Das AWS CLI ist ein einheitliches Tool zur Verwaltung Ihrer AWS Dienste. Mit nur einem Tool zum Herunterladen und Konfigurieren können Sie mehrere AWS Dienste von der Befehlszeile aus steuern und mithilfe von Skripten automatisieren. Weitere Informationen zu den Tools AWS CLI und Anweisungen zur Installation der AWS CLI Tools finden Sie im Folgenden im AWS Command Line Interface Benutzerhandbuch.

- AWS Command Line Interface Benutzerhandbuch
- Einrichtung der AWS Command Line Interface

Geben Sie bei Bedarf ein, `aws configure` um das so zu konfigurieren AWS CLI , dass es eine AWS Region verwendet, in der sie verfügbar AWS Config ist.

Einrichtung

Informationen zur Einrichtung AWS Config mit dem finden Sie in den folgenden Themen AWS CLI.

Themen

- Voraussetzungen für die Einrichtung AWS Config mit dem AWS CLI
- Beginnend AWS Config mit einem vom Kunden verwalteten Konfigurationsrekorder unter Verwendung des AWS CLI
- Überprüfen, ob AWS Config dies erfolgreich gestartet wurde mit dem AWS CLI

Voraussetzungen für die Einrichtung AWS Config mit dem AWS CLI

Vor der AWS CLI Einrichtung AWS von müssen Sie einen Amazon S3-Bucket, ein Amazon SNS SNS-Thema und eine IAM-Rolle mit angehängten Richtlinien als Voraussetzungen erstellen. Anschließend können Sie den AWS CLI Bucket, das Thema und die Rolle für angeben. AWS Config Gehen Sie wie folgt vor, um Ihre Voraussetzungen für AWS Config einzurichten.

Themen

- Schritt 1: Einen Amazon S3 S3-Bucket erstellen
- Schritt 2: Erstellen eines Amazon SNS SNS-Themas
- Schritt 3: Eine IAM-Rolle erstellen

Schritt 1: Einen Amazon S3 S3-Bucket erstellen

Wenn Sie in Ihrem Konto bereits über einen Amazon-S3-Bucket verfügen und diesen verwenden möchten, überspringen Sie diesen Schritt und gehen zu Schritt 2: Erstellen eines Amazon SNS SNS-Themas über.

Verwenden der S3-Konsole

So erstellen Sie einen Bucket

1. Öffnen Sie die Amazon S3 S3-Konsole unter https://console.aws.amazon.com/s3/.
2. Wählen Sie Create Bucket (Bucket erstellen) aus.

3. Geben Sie unter Bucket name (Bucket-Name) einen DNS-kompatiblen Namen für Ihren Bucket ein.

   Der Bucket-Name muss ...:

   - überall in Amazon S3 eindeutig sein.
   - zwischen 3 und 63 Zeichen lang sein,
   - Enthält keine Großbuchstaben.
   - mit einem Kleinbuchstaben oder einer Zahl beginnen.

   Der Name eines einmal erstellten Buckets kann nicht nachträglich geändert werden. Stellen Sie sicher, dass der von Ihnen gewählte Bucket-Name unter allen in Amazon S3 vorhandenen Bucket-Namen eindeutig ist. Weitere Informationen zu Namensregeln und -konventionen für Buckets finden Sie unter Beschränkungen und Einschränkungen von Buckets im Benutzerhandbuch für Amazon Simple Storage Service.

   > **Important**
   >
   > Vermeiden Sie es, vertrauliche Informationen in den Bucket-Namen aufzunehmen. Der Bucket-Name ist in dem Punkt sichtbar URLs , auf den die Objekte im Bucket verweisen.

4. Wählen Sie unter Region die AWS Region aus, in der sich der Bucket befinden soll.

   Wählen Sie eine Region in der Nähe aus, um Latenz und Kosten auf einem Minimum zu halten und behördliche Vorschriften zu erfüllen. In einer Region gespeicherte Objekte verbleiben so lange in der Region, bis sie explizit in eine andere Region verschoben werden. Eine Liste der Amazon S3 AWS S3-Regionen finden Sie unter AWS Service-Endpunkte in der Allgemeine Amazon Web Services-Referenz.

5. Wählen Sie unter Bucket settings for Block Public Access (Bucket-Einstellungen für den öffentlichen Zugriff) die Einstellungen für den öffentlichen Zugriff aus, die Sie auf den Bucket anwenden möchten.

   Es wird empfohlen, alle Einstellungen aktiviert zu belassen, es sei denn, Sie wissen, dass Sie eine oder mehrere dieser Einstellungen für Ihren Anwendungsfall deaktivieren müssen, z. B. um eine öffentliche Website zu hosten. Einstellungen für den öffentlichen Zugriff, die Sie für den Bucket aktivieren, werden auch für alle Zugriffspunkte aktiviert, die Sie für den Bucket erstellen.

Weitere Informationen zum Blockieren des öffentlichen Zugriffs finden Sie unter Verwenden von Amazon S3 Block Public Access im Amazon Simple Storage Service-Benutzerhandbuch.

6. (Optional) Wenn Sie die S3-Objektsperre aktivieren möchten:

   a. Wählen Sie Fortschrittliche Einstellungen aus und lesen Sie die anschließend angezeigte Meldung.

   > **Important**
   >
   > Sie können die S3-Objektsperre für einen Bucket nur aktivieren, wenn Sie ihn erstellen. Wenn Sie die Objektsperre für den Bucket aktivieren, können Sie es später nicht mehr deaktivieren. Durch Aktivieren der Objektsperre wird auch die Versionssteuerung für den Bucket aktiviert. Nachdem Sie die Objektsperre für den Bucket aktiviert haben, müssen Sie die Objektsperreneinstellungen konfigurieren, bevor Objekte im Bucket geschützt werden. Weitere Informationen zum Konfigurieren des Schutzes für Objekte finden Sie unter Konfigurieren der S3 Object Lock mit der Amazon-S3-Konsole.

   b. Wenn Sie die Objektsperre aktivieren möchten, geben Sie in das Textfeld enable (Aktivieren) ein und wählen Sie Confirm (Bestätigen) aus.

   Weitere Informationen zur S3-Objektsperrenfunktion finden Sie unter Sperren von Objekten mit der Amazon S3-Objektsperre im Amazon Simple Storage Service-Benutzerhandbuch.

7. Wählen Sie Create Bucket (Bucket erstellen) aus.

Mit dem AWS SDKs

Wenn Sie den verwenden, AWS SDKs um einen Bucket zu erstellen, müssen Sie einen Client erstellen und dann den Client verwenden, um eine Anfrage zum Erstellen eines Buckets zu senden. Als bewährte Methode sollten Sie Ihren Client und Ihren Bucket in derselben AWS-Region erstellen. Wenn Sie beim Erstellen eines Clients oder Buckets keine Region angeben, verwendet Amazon S3 die Standardregion USA Ost (Nord-Virginia).

Um einen Client für den Zugriff auf einen Dual-Stack-Endpunkt zu erstellen, müssen Sie einen AWS-Region angeben. Weitere Informationen finden Sie unter Dual-Stack-Endpunkte von Amazon S3. Eine Liste der verfügbaren AWS-Regionen Regionen und Endpunkte finden Sie unter Regionen und Endpunkte in der. Allgemeine AWS-Referenz

Wenn Sie einen Client erstellen, wird die Region dem regionsspezifischen Endpunkt zugeordnet. Der Client verwendet diesen Endpunkt für die Kommunikation mit Amazon S3: `s3.<region>.amazonaws.com`. Wenn Ihre Region nach dem 20. März 2019 gestartet wurde, müssen sich Ihr Client und Ihr Bucket in derselben Region befinden. Sie können jedoch einen Client in der Region USA Ost (Nord-Virginia) verwenden, um einen Bucket in einer beliebigen Region zu erstellen, die vor dem 20. März 2019 gestartet wurde. Weitere Informationen finden Sie unter Legacy-Endpunkte.

Diese AWS SDK-Codebeispiele erfüllen die folgenden Aufgaben:

- Erstellen Sie einen Client, indem Sie explizit eine AWS-Region angeben – Im Beispiel verwendet der Client den Endpunkt `s3.us-west-2.amazonaws.com`, um mit Amazon S3 zu kommunizieren. Sie können eine beliebige AWS-Region angeben. Eine Liste von AWS-Regionen finden Sie unter Regionen und Endpunkte in der AWS allgemeinen Referenz.
- Senden einer Bucket-Erstellungs-Anfrage durch Angabe eines Bucket-Namens – Der Client sendet eine Anfrage an Amazon S3, um den Bucket in der Region zu erstellen, in der Sie einen Client erstellt haben.
- Abrufen von Informationen zum Standort des Buckets – Amazon S3 speichert Informationen zum Standort des Buckets in der Subressource location (Standort), die dem Bucket zugeordnet ist.

Die folgenden Code-Beispiele zeigen, wie `CreateBucket` verwendet wird.

.NET

SDK für .NET

> **Note**
>
> Es gibt noch mehr dazu. GitHub Hier finden Sie das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel- einrichten und ausführen.

```
/// <summary>
/// Shows how to create a new Amazon S3 bucket.
/// </summary>
/// <param name="client">An initialized Amazon S3 client object.</param>
/// <param name="bucketName">The name of the bucket to create.</param>
```

```
        /// <returns>A boolean value representing the success or failure of
        /// the bucket creation process.</returns>
        public static async Task<bool> CreateBucketAsync(IAmazonS3 client, string
bucketName)
        {
            try
            {
                var request = new PutBucketRequest
                {
                    BucketName = bucketName,
                    UseClientRegion = true,
                };

                var response = await client.PutBucketAsync(request);
                return response.HttpStatusCode == System.Net.HttpStatusCode.OK;
            }
            catch (AmazonS3Exception ex)
            {
                Console.WriteLine($"Error creating bucket: '{ex.Message}'");
                return false;
            }
        }
```

Erstellen Sie einen Bucket mit aktivierter Objektsperre.

```
    /// <summary>
    /// Create a new Amazon S3 bucket with object lock actions.
    /// </summary>
    /// <param name="bucketName">The name of the bucket to create.</param>
    /// <param name="enableObjectLock">True to enable object lock on the
bucket.</param>
    /// <returns>True if successful.</returns>
    public async Task<bool> CreateBucketWithObjectLock(string bucketName, bool
enableObjectLock)
    {
        Console.WriteLine($"\tCreating bucket {bucketName} with object lock
{enableObjectLock}.");
        try
        {
            var request = new PutBucketRequest
            {
```

```
                BucketName = bucketName,
                UseClientRegion = true,
                ObjectLockEnabledForBucket = enableObjectLock,
            };

            var response = await _amazonS3.PutBucketAsync(request);

            return response.HttpStatusCode == System.Net.HttpStatusCode.OK;
        }
        catch (AmazonS3Exception ex)
        {
            Console.WriteLine($"Error creating bucket: '{ex.Message}'");
            return false;
        }
    }
```

- Einzelheiten zur API finden Sie CreateBucketin der AWS SDK für .NET API-Referenz.

Bash

AWS CLI mit Bash-Skript

> **Note**
>
> Es gibt noch mehr dazu. GitHub Hier finden Sie das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel- einrichten und ausführen.

```
###############################################################################
# function iecho
#
# This function enables the script to display the specified text only if
# the global variable $VERBOSE is set to true.
###############################################################################
function iecho() {
  if [[ $VERBOSE == true ]]; then
    echo "$@"
  fi
}

###############################################################################
```

```
# function errecho
#
# This function outputs everything sent to it to STDERR (standard error output).
###############################################################################
function errecho() {
  printf "%s\n" "$*" 1>&2
}

###############################################################################
# function create-bucket
#
# This function creates the specified bucket in the specified AWS Region, unless
# it already exists.
#
# Parameters:
#       -b bucket_name  -- The name of the bucket to create.
#       -r region_code  -- The code for an AWS Region in which to
#                          create the bucket.
#
# Returns:
#       The URL of the bucket that was created.
#     And:
#       0 - If successful.
#       1 - If it fails.
###############################################################################
function create_bucket() {
  local bucket_name region_code response
  local option OPTARG # Required to use getopts command in a function.

  # bashsupport disable=BP5008
  function usage() {
    echo "function create_bucket"
    echo "Creates an Amazon S3 bucket. You must supply a bucket name:"
    echo "  -b bucket_name    The name of the bucket. It must be globally
 unique."
    echo "  [-r region_code]    The code for an AWS Region in which the bucket is
 created."
    echo ""
  }

  # Retrieve the calling parameters.
  while getopts "b:r:h" option; do
    case "${option}" in
      b) bucket_name="${OPTARG}" ;;
```

```
      r) region_code="${OPTARG}" ;;
      h)
        usage
        return 0
        ;;
      \?)
        echo "Invalid parameter"
        usage
        return 1
        ;;
    esac
  done

  if [[ -z "$bucket_name" ]]; then
    errecho "ERROR: You must provide a bucket name with the -b parameter."
    usage
    return 1
  fi

  local bucket_config_arg
  # A location constraint for "us-east-1" returns an error.
  if [[ -n "$region_code" ]] && [[ "$region_code" != "us-east-1" ]]; then
    bucket_config_arg="--create-bucket-configuration LocationConstraint=
$region_code"
  fi

  iecho "Parameters:\n"
  iecho "    Bucket name:   $bucket_name"
  iecho "    Region code:   $region_code"
  iecho ""

  # If the bucket already exists, we don't want to try to create it.
  if (bucket_exists "$bucket_name"); then
    errecho "ERROR: A bucket with that name already exists. Try again."
    return 1
  fi

  # shellcheck disable=SC2086
  response=$(aws s3api create-bucket \
    --bucket "$bucket_name" \
    $bucket_config_arg)

  # shellcheck disable=SC2181
  if [[ ${?} -ne 0 ]]; then
```

```
    errecho "ERROR: AWS reports create-bucket operation failed.\n$response"
    return 1
  fi
}
```

- Einzelheiten zur API finden Sie CreateBucketin der AWS CLI Befehlsreferenz.

C++

SDK für C++

> **Note**
>
> Es gibt noch mehr dazu GitHub. Hier finden Sie das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel- einrichten und ausführen.

```
bool AwsDoc::S3::createBucket(const Aws::String &bucketName,
                              const Aws::S3::S3ClientConfiguration &clientConfig)
 {
    Aws::S3::S3Client client(clientConfig);
    Aws::S3::Model::CreateBucketRequest request;
    request.SetBucket(bucketName);

    if (clientConfig.region != "us-east-1") {
        Aws::S3::Model::CreateBucketConfiguration createBucketConfig;
        createBucketConfig.SetLocationConstraint(

 Aws::S3::Model::BucketLocationConstraintMapper::GetBucketLocationConstraintForName(
                        clientConfig.region));
        request.SetCreateBucketConfiguration(createBucketConfig);
    }

    Aws::S3::Model::CreateBucketOutcome outcome = client.CreateBucket(request);
    if (!outcome.IsSuccess()) {
        auto err = outcome.GetError();
        std::cerr << "Error: createBucket: " <<
                  err.GetExceptionName() << ": " << err.GetMessage() <<
 std::endl;
    } else {
        std::cout << "Created bucket " << bucketName <<
```

```
                    " in the specified AWS Region." << std::endl;
    }

    return outcome.IsSuccess();
}
```

- Einzelheiten zur API finden Sie CreateBucketin der AWS SDK für C++ API-Referenz.

CLI

AWS CLI

Beispiel 1: Um einen Bucket zu erstellen

Im folgenden `create-bucket` Beispiel wird ein Bucket mit dem Namen erstelltamzn-s3-demo-bucket:

```
aws s3api create-bucket \
    --bucket amzn-s3-demo-bucket \
    --region us-east-1
```

Ausgabe:

```
{
    "Location": "/amzn-s3-demo-bucket"
}
```

Weitere Informationen finden Sie unter Erstellen eines Buckets im Amazon S3 S3-Benutzerhandbuch.

Beispiel 2: Um einen Bucket zu erstellen, bei dem der Besitzer erzwungen wird

Im folgenden `create-bucket` Beispiel wird ein Bucket mit dem Namen erstellt, der `amzn-s3-demo-bucket` die Einstellung Bucket Owner erforced für S3 Object Ownership verwendet.

```
aws s3api create-bucket \
    --bucket amzn-s3-demo-bucket \
    --region us-east-1 \
    --object-ownership BucketOwnerEnforced
```

Ausgabe:

```
{
    "Location": "/amzn-s3-demo-bucket"
}
```

Weitere Informationen finden Sie unter Kontrolle des Besitzes von Objekten und Deaktivierung ACLs im Amazon S3 S3-Benutzerhandbuch.

Beispiel 3: Um einen Bucket außerhalb der Region ``us-east-1`` zu erstellen

Im folgenden `create-bucket` Beispiel wird ein Bucket mit dem Namen der Region erstellt. `amzn-s3-demo-bucket` `eu-west-1` Für Regionen außerhalb von `us-east-1` müssen die entsprechenden `LocationConstraint` Felder angegeben werden, um den Bucket in der gewünschten Region zu erstellen.

```
aws s3api create-bucket \
    --bucket amzn-s3-demo-bucket \
    --region eu-west-1 \
    --create-bucket-configuration LocationConstraint=eu-west-1
```

Ausgabe:

```
{
    "Location": "http://amzn-s3-demo-bucket.s3.amazonaws.com/"
}
```

Weitere Informationen finden Sie unter Erstellen eines Buckets im Amazon S3 S3-Benutzerhandbuch.

- Einzelheiten zur API finden Sie CreateBucketunter AWS CLI Befehlsreferenz.

Go

SDK für Go V2

> **Note**
>
> Es gibt noch mehr dazu GitHub. Hier finden Sie das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel- einrichten und ausführen.

Erstellen Sie einen Bucket mit Standardkonfiguration.

```
import (
 "bytes"
 "context"
 "errors"
 "fmt"
 "io"
 "log"
 "os"
 "time"

 "github.com/aws/aws-sdk-go-v2/aws"
 "github.com/aws/aws-sdk-go-v2/feature/s3/manager"
 "github.com/aws/aws-sdk-go-v2/service/s3"
 "github.com/aws/aws-sdk-go-v2/service/s3/types"
 "github.com/aws/smithy-go"
)

// BucketBasics encapsulates the Amazon Simple Storage Service (Amazon S3)
 actions
// used in the examples.
// It contains S3Client, an Amazon S3 service client that is used to perform
 bucket
// and object actions.
type BucketBasics struct {
 S3Client *s3.Client
}



// CreateBucket creates a bucket with the specified name in the specified Region.
func (basics BucketBasics) CreateBucket(ctx context.Context, name string, region
 string) error {
 _, err := basics.S3Client.CreateBucket(ctx, &s3.CreateBucketInput{
  Bucket: aws.String(name),
  CreateBucketConfiguration: &types.CreateBucketConfiguration{
   LocationConstraint: types.BucketLocationConstraint(region),
  },
 })
 if err != nil {
  var owned *types.BucketAlreadyOwnedByYou
  var exists *types.BucketAlreadyExists
```

```
  if errors.As(err, &owned) {
   log.Printf("You already own bucket %s.\n", name)
   err = owned
  } else if errors.As(err, &exists) {
   log.Printf("Bucket %s already exists.\n", name)
   err = exists
  }
 } else {
  err = s3.NewBucketExistsWaiter(basics.S3Client).Wait(
   ctx, &s3.HeadBucketInput{Bucket: aws.String(name)}, time.Minute)
  if err != nil {
   log.Printf("Failed attempt to wait for bucket %s to exist.\n", name)
  }
 }
 return err
}
```

Erstellen Sie einen Bucket mit Objektsperre und warten Sie, bis er existiert.

```
import (
 "bytes"
 "context"
 "errors"
 "fmt"
 "log"
 "time"

 "github.com/aws/aws-sdk-go-v2/aws"
 "github.com/aws/aws-sdk-go-v2/feature/s3/manager"
 "github.com/aws/aws-sdk-go-v2/service/s3"
 "github.com/aws/aws-sdk-go-v2/service/s3/types"
 "github.com/aws/smithy-go"
)

// S3Actions wraps S3 service actions.
type S3Actions struct {
 S3Client  *s3.Client
 S3Manager *manager.Uploader
}
```

```
// CreateBucketWithLock creates a new S3 bucket with optional object locking
 enabled
// and waits for the bucket to exist before returning.
func (actor S3Actions) CreateBucketWithLock(ctx context.Context, bucket string,
 region string, enableObjectLock bool) (string, error) {
 input := &s3.CreateBucketInput{
  Bucket: aws.String(bucket),
  CreateBucketConfiguration: &types.CreateBucketConfiguration{
   LocationConstraint: types.BucketLocationConstraint(region),
  },
 }

 if enableObjectLock {
  input.ObjectLockEnabledForBucket = aws.Bool(true)
 }

 _, err := actor.S3Client.CreateBucket(ctx, input)
 if err != nil {
  var owned *types.BucketAlreadyOwnedByYou
  var exists *types.BucketAlreadyExists
  if errors.As(err, &owned) {
   log.Printf("You already own bucket %s.\n", bucket)
   err = owned
  } else if errors.As(err, &exists) {
   log.Printf("Bucket %s already exists.\n", bucket)
   err = exists
  }
 } else {
  err = s3.NewBucketExistsWaiter(actor.S3Client).Wait(
   ctx, &s3.HeadBucketInput{Bucket: aws.String(bucket)}, time.Minute)
  if err != nil {
   log.Printf("Failed attempt to wait for bucket %s to exist.\n", bucket)
  }
 }

 return bucket, err
}
```

- Einzelheiten zur API finden Sie CreateBucketin der AWS SDK für Go API-Referenz.

Java

SDK für Java 2.x

> **Note**
>
> Es gibt noch mehr dazu GitHub. Hier finden Sie das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel- einrichten und ausführen.

Erstellen Sie einen Bucket.

```
   /**
    * Creates an S3 bucket asynchronously.
    *
    * @param bucketName the name of the S3 bucket to create
    * @return a {@link CompletableFuture} that completes when the bucket is
created and ready
    * @throws RuntimeException if there is a failure while creating the bucket
    */
   public CompletableFuture<Void> createBucketAsync(String bucketName) {
       CreateBucketRequest bucketRequest = CreateBucketRequest.builder()
           .bucket(bucketName)
           .build();

       CompletableFuture<CreateBucketResponse> response =
getAsyncClient().createBucket(bucketRequest);
       return response.thenCompose(resp -> {
           S3AsyncWaiter s3Waiter = getAsyncClient().waiter();
           HeadBucketRequest bucketRequestWait = HeadBucketRequest.builder()
               .bucket(bucketName)
               .build();

           CompletableFuture<WaiterResponse<HeadBucketResponse>>
waiterResponseFuture =
               s3Waiter.waitUntilBucketExists(bucketRequestWait);
           return waiterResponseFuture.thenAccept(waiterResponse -> {
               waiterResponse.matched().response().ifPresent(headBucketResponse
-> {
                   logger.info(bucketName + " is ready");
               });
           });
```

```
        }).whenComplete((resp, ex) -> {
            if (ex != null) {
                throw new RuntimeException("Failed to create bucket", ex);
            }
        });
    }
```

Erstellen Sie einen Bucket mit aktivierter Objektsperre.

```
    // Create a new Amazon S3 bucket with object lock options.
    public void createBucketWithLockOptions(boolean enableObjectLock, String
bucketName) {
        S3Waiter s3Waiter = getClient().waiter();
        CreateBucketRequest bucketRequest = CreateBucketRequest.builder()
            .bucket(bucketName)
            .objectLockEnabledForBucket(enableObjectLock)
            .build();

        getClient().createBucket(bucketRequest);
        HeadBucketRequest bucketRequestWait = HeadBucketRequest.builder()
            .bucket(bucketName)
            .build();

        // Wait until the bucket is created and print out the response.
        s3Waiter.waitUntilBucketExists(bucketRequestWait);
        System.out.println(bucketName + " is ready");
    }
```

- Einzelheiten zur API finden Sie CreateBucketin der AWS SDK for Java 2.x API-Referenz.

JavaScript

SDK für JavaScript (v3)

> **Note**
>
> Es gibt noch mehr dazu GitHub. Hier finden Sie das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel- einrichten und ausführen.

Erstellen Sie den Bucket.

```
import {
  BucketAlreadyExists,
  BucketAlreadyOwnedByYou,
  CreateBucketCommand,
  S3Client,
  waitUntilBucketExists,
} from "@aws-sdk/client-s3";

/**
 * Create an Amazon S3 bucket.
 * @param {{ bucketName: string }} config
 */
export const main = async ({ bucketName }) => {
  const client = new S3Client({});

  try {
    const { Location } = await client.send(
      new CreateBucketCommand({
        // The name of the bucket. Bucket names are unique and have several other
 constraints.
        // See https://docs.aws.amazon.com/AmazonS3/latest/userguide/
bucketnamingrules.html
        Bucket: bucketName,
      }),
    );
    await waitUntilBucketExists({ client }, { Bucket: bucketName });
    console.log(`Bucket created with location ${Location}`);
  } catch (caught) {
    if (caught instanceof BucketAlreadyExists) {
      console.error(
        `The bucket "${bucketName}" already exists in another AWS account. Bucket
 names must be globally unique.`,
      );
    }
    // WARNING: If you try to create a bucket in the North Virginia region,
    // and you already own a bucket in that region with the same name, this
    // error will not be thrown. Instead, the call will return successfully
    // and the ACL on that bucket will be reset.
    else if (caught instanceof BucketAlreadyOwnedByYou) {
      console.error(
        `The bucket "${bucketName}" already exists in this AWS account.`,
      );
```

```
    } else {
      throw caught;
    }
  }
};
```

- Weitere Informationen finden Sie im AWS SDK für JavaScript -Entwicklerhandbuch.
- Einzelheiten zur API finden Sie CreateBucketin der AWS SDK für JavaScript API-Referenz.

Kotlin

SDK für Kotlin

> **Note**
>
> Es gibt noch mehr dazu GitHub. Hier finden Sie das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel- einrichten und ausführen.

```
suspend fun createNewBucket(bucketName: String) {
    val request =
        CreateBucketRequest {
            bucket = bucketName
        }

    S3Client { region = "us-east-1" }.use { s3 ->
        s3.createBucket(request)
        println("$bucketName is ready")
    }
}
```

- API-Details finden Sie CreateBucketin der API-Referenz zum AWS SDK für Kotlin.

PHP

SDK für PHP

> **Note**
>
> Es gibt noch mehr dazu. GitHub Hier finden Sie das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel- einrichten und ausführen.

Erstellen Sie einen Bucket.

```
        $s3client = new Aws\S3\S3Client(['region' => 'us-west-2']);

        try {
            $this->s3client->createBucket([
                'Bucket' => $this->bucketName,
                'CreateBucketConfiguration' => ['LocationConstraint' => $region],
            ]);
            echo "Created bucket named: $this->bucketName \n";
        } catch (Exception $exception) {
            echo "Failed to create bucket $this->bucketName with error: " .
$exception->getMessage();
            exit("Please fix error with bucket creation before continuing.");
        }
```

- Einzelheiten zur API finden Sie CreateBucketin der AWS SDK für PHP API-Referenz.

Python

SDK für Python (Boto3)

> **Note**
>
> Es gibt noch mehr dazu GitHub. Hier finden Sie das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel- einrichten und ausführen.

Erstellen Sie einen Bucket mit Standardeinstellungen.

```
class BucketWrapper:
    """Encapsulates S3 bucket actions."""

    def __init__(self, bucket):
        """
        :param bucket: A Boto3 Bucket resource. This is a high-level resource in
 Boto3
                       that wraps bucket actions in a class-like structure.
        """
        self.bucket = bucket
        self.name = bucket.name


    def create(self, region_override=None):
        """
        Create an Amazon S3 bucket in the default Region for the account or in
 the
        specified Region.

        :param region_override: The Region in which to create the bucket. If this
 is
                                not specified, the Region configured in your
 shared
                                credentials is used.
        """
        if region_override is not None:
            region = region_override
        else:
            region = self.bucket.meta.client.meta.region_name
        try:
            self.bucket.create(CreateBucketConfiguration={"LocationConstraint":
 region})

            self.bucket.wait_until_exists()
            logger.info("Created bucket '%s' in region=%s", self.bucket.name,
 region)
        except ClientError as error:
            logger.exception(
                "Couldn't create bucket named '%s' in region=%s.",
                self.bucket.name,
                region,
            )
            raise error
```

Erstellen Sie einen versionierten Bucket mit einer Lebenszyklus-Konfiguration.

```
def create_versioned_bucket(bucket_name, prefix):
    """
    Creates an Amazon S3 bucket, enables it for versioning, and configures a
 lifecycle
    that expires noncurrent object versions after 7 days.

    Adding a lifecycle configuration to a versioned bucket is a best practice.
    It helps prevent objects in the bucket from accumulating a large number of
    noncurrent versions, which can slow down request performance.

    Usage is shown in the usage_demo_single_object function at the end of this
 module.

    :param bucket_name: The name of the bucket to create.
    :param prefix: Identifies which objects are automatically expired under the
                   configured lifecycle rules.
    :return: The newly created bucket.
    """
    try:
        bucket = s3.create_bucket(
            Bucket=bucket_name,
            CreateBucketConfiguration={
                "LocationConstraint": s3.meta.client.meta.region_name
            },
        )
        logger.info("Created bucket %s.", bucket.name)
    except ClientError as error:
        if error.response["Error"]["Code"] == "BucketAlreadyOwnedByYou":
            logger.warning("Bucket %s already exists! Using it.", bucket_name)
            bucket = s3.Bucket(bucket_name)
        else:
            logger.exception("Couldn't create bucket %s.", bucket_name)
            raise

    try:
        bucket.Versioning().enable()
        logger.info("Enabled versioning on bucket %s.", bucket.name)
    except ClientError:
```

```
        logger.exception("Couldn't enable versioning on bucket %s.", bucket.name)
        raise

    try:
        expiration = 7
        bucket.LifecycleConfiguration().put(
            LifecycleConfiguration={
                "Rules": [
                    {
                        "Status": "Enabled",
                        "Prefix": prefix,
                        "NoncurrentVersionExpiration": {"NoncurrentDays":
expiration},
                    }
                ]
            }
        )
        logger.info(
            "Configured lifecycle to expire noncurrent versions after %s days "
            "on bucket %s.",
            expiration,
            bucket.name,
        )
    except ClientError as error:
        logger.warning(
            "Couldn't configure lifecycle on bucket %s because %s. "
            "Continuing anyway.",
            bucket.name,
            error,
        )

    return bucket
```

- Einzelheiten zur API finden Sie CreateBucketin AWS SDK for Python (Boto3) API Reference.

Ruby

SDK für Ruby

> **Note**
>
> Es gibt noch mehr dazu. GitHub Hier finden Sie das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel- einrichten und ausführen.

```
require 'aws-sdk-s3'

# Wraps Amazon S3 bucket actions.
class BucketCreateWrapper
  attr_reader :bucket

  # @param bucket [Aws::S3::Bucket] An Amazon S3 bucket initialized with a name.
 This is a client-side object until
  #                                 create is called.
  def initialize(bucket)
    @bucket = bucket
  end

  # Creates an Amazon S3 bucket in the specified AWS Region.
  #
  # @param region [String] The Region where the bucket is created.
  # @return [Boolean] True when the bucket is created; otherwise, false.
  def create?(region)
    @bucket.create(create_bucket_configuration: { location_constraint: region })
    true
  rescue Aws::Errors::ServiceError => e
    puts "Couldn't create bucket. Here's why: #{e.message}"
    false
  end

  # Gets the Region where the bucket is located.
  #
  # @return [String] The location of the bucket.
  def location
    if @bucket.nil?
      'None. You must create a bucket before you can get its location!'
    else
```

```
      @bucket.client.get_bucket_location(bucket:
 @bucket.name).location_constraint
    end
  rescue Aws::Errors::ServiceError => e
    "Couldn't get the location of #{@bucket.name}. Here's why: #{e.message}"
  end
end

# Example usage:
def run_demo
  region = "us-west-2"
  wrapper = BucketCreateWrapper.new(Aws::S3::Bucket.new("amzn-s3-demo-bucket-
#{Random.uuid}"))
  return unless wrapper.create?(region)

  puts "Created bucket #{wrapper.bucket.name}."
  puts "Your bucket's region is: #{wrapper.location}"
end

run_demo if $PROGRAM_NAME == __FILE__
```

- Einzelheiten zur API finden Sie CreateBucketin der AWS SDK für Ruby API-Referenz.

Rust

SDK für Rust

> **Note**
>
> Es gibt noch mehr dazu GitHub. Hier finden Sie das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel- einrichten und ausführen.

```
pub async fn create_bucket(
    client: &aws_sdk_s3::Client,
    bucket_name: &str,
    region: &aws_config::Region,
) -> Result<Option<aws_sdk_s3::operation::create_bucket::CreateBucketOutput>,
 S3ExampleError> {
    let constraint =
 aws_sdk_s3::types::BucketLocationConstraint::from(region.to_string().as_str());
```

```
    let cfg = aws_sdk_s3::types::CreateBucketConfiguration::builder()
        .location_constraint(constraint)
        .build();
    let create = client
        .create_bucket()
        .create_bucket_configuration(cfg)
        .bucket(bucket_name)
        .send()
        .await;

    // BucketAlreadyExists and BucketAlreadyOwnedByYou are not problems for this
 task.
    create.map(Some).or_else(|err| {
        if err
            .as_service_error()
            .map(|se| se.is_bucket_already_exists() ||
 se.is_bucket_already_owned_by_you())
            == Some(true)
        {
            Ok(None)
        } else {
            Err(S3ExampleError::from(err))
        }
    })
}
```

- Einzelheiten zur API finden Sie CreateBucketin der API-Referenz zum AWS SDK für Rust.

SAP ABAP

SDK für SAP ABAP

> **Note**
>
> Es gibt noch mehr dazu GitHub. Hier finden Sie das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel- einrichten und ausführen.

```
    TRY.
        " determine our region from our session
```

```
        DATA(lv_region) = CONV /aws1/s3_bucketlocationcnstrnt( lo_session-
>get_region( ) ).
        DATA lo_constraint TYPE REF TO /aws1/cl_s3_createbucketconf.
        " When in the us-east-1 region, you must not specify a constraint
        " In all other regions, specify the region as the constraint
        IF lv_region = 'us-east-1'.
          CLEAR lo_constraint.
        ELSE.
          lo_constraint = NEW /aws1/cl_s3_createbucketconf( lv_region ).
        ENDIF.

        lo_s3->createbucket(
            iv_bucket = iv_bucket_name
            io_createbucketconfiguration  = lo_constraint ).
        MESSAGE 'S3 bucket created.' TYPE 'I'.
      CATCH /aws1/cx_s3_bucketalrdyexists.
        MESSAGE 'Bucket name already exists.' TYPE 'E'.
      CATCH /aws1/cx_s3_bktalrdyownedbyyou.
        MESSAGE 'Bucket already exists and is owned by you.' TYPE 'E'.
    ENDTRY.
```

- Einzelheiten zur API finden Sie CreateBucketin der API-Referenz zum AWS SDK für SAP ABAP.

Swift

SDK für Swift

> **Note**
>
> Es gibt noch mehr dazu. GitHub Hier finden Sie das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel- einrichten und ausführen.

```
import AWSS3

    public func createBucket(name: String) async throws {
        var input = CreateBucketInput(
            bucket: name
        )
```

```
        // For regions other than "us-east-1", you must set the
 locationConstraint in the createBucketConfiguration.
        // For more information, see LocationConstraint in the S3 API guide.
        // https://docs.aws.amazon.com/AmazonS3/latest/API/
API_CreateBucket.html#API_CreateBucket_RequestBody
        if let region = configuration.region {
            if region != "us-east-1" {
                input.createBucketConfiguration =
 S3ClientTypes.CreateBucketConfiguration(locationConstraint:
 S3ClientTypes.BucketLocationConstraint(rawValue: region))
            }
        }

        do {
            _ = try await client.createBucket(input: input)
        }
        catch let error as BucketAlreadyOwnedByYou {
            print("The bucket '\(name)' already exists and is owned by you. You
 may wish to ignore this exception.")
            throw error
        }
        catch {
            print("ERROR: ", dump(error, name: "Creating a bucket"))
            throw error
        }
    }
```

- Einzelheiten zur API finden Sie CreateBucketin der API-Referenz zum AWS SDK für Swift.

> **Note**
>
> Sie können auch den Amazon-S3-Bucket eines anderen Kontos verwenden. Allerdings müssen Sie ggf. eine Richtlinie für den Bucket erstellen, die AWS Config Zugriffsberechtigungen erteilt. Weitere Informationen zum Erteilen von Berechtigungen für einen Amazon-S3-Bucket finden Sie unter Berechtigungen für den Amazon S3 S3-Bucket für den AWS Config Lieferkanal. Rufen Sie anschließend Schritt 2: Erstellen eines Amazon SNS SNS-Themas auf.

Schritt 2: Erstellen eines Amazon SNS SNS-Themas

Wenn Sie in Ihrem Konto bereits über ein Amazon-SNS-Thema verfügen und dieses verwenden möchten, überspringen Sie diesen Schritt und machen Sie bei Schritt 3: Eine IAM-Rolle erstellen weiter.

Verwenden der SNS-Konsole

Erstellen eines Amazon SNS-Themas

1. Öffnen Sie die Amazon SNS SNS-Konsole unter https://console.aws.amazon.com/sns/v3/home.
2. Führen Sie eine der folgenden Aktionen aus:
   - Wenn noch nie zuvor Themen unter Ihrem AWS-Konto Konto erstellt wurden, lesen Sie die Beschreibung von Amazon SNS auf der Startseite.
   - Wenn AWS-Konto zuvor Themen unter Ihrem Konto erstellt wurden, wählen Sie im Navigationsbereich die Option Themen aus.
3. Klicken Sie auf der Seite Themen auf Create New Topic.
4. Führen Sie auf der Seite Create subscription (Abonnement erstellen) im Abschnitt Details die folgenden Schritte aus:
   a. FürTypWählen Sie einen Thementyp aus (Standard-oderFIFO).
   b. Geben Sie den Namen des neuen Themas ein. Für eineFIFO-ThemaFügen SieFIFOam Ende des Namens hinzu.
   c. (Optional) Geben Sie einen Display name (Anzeigenamen) für Ihr Thema ein.
   d. (Optional) Für ein FIFO-Thema können SieDeduplizierung für inhaltsbasierte Nachrichten, um die Standardnachrichtendeduplizierung zu aktivieren. Weitere Informationen finden Sie unter Nachrichtendeduplizierung für FIFO-Themen.
5. (Optional) Erweitern Sie den Abschnitt Encryption (Verschlüsselung) und gehen Sie wie folgt vor. Weitere Informationen finden Sie unter Verschlüsselung im Ruhezustand.
   a. Wählen Sie Enable encryption (Verschlüsselung aktivieren) aus.
   b. Geben Sie den Kundenmasterschlüssel (CMK) an. Weitere Informationen finden Sie unter Schlüsselbegriffe.

Für jeden CMK-Typ werden Description (Beschreibung), Account (Konto) und CMK ARN (CMK-ARN) angezeigt.

> **Important**
>
> Wenn Sie nicht der Besitzer des CMK sind oder wenn Sie sich mit einem Konto anmelden, das über keine `kms:ListAliases` und `kms:DescribeKey`-Berechtigungen verfügt, können Sie auf der Amazon SNS-Konsole keine Informationen über den CMK aufrufen.
> Bitten Sie den Inhaber des CMK, Ihnen diese Berechtigungen zu erteilen. Beispiele und weitere Informationen zu AWS KMS -Berechtigungen finden Sie unter API-Berechtigungen: Referenztabelle für Aktionen und Ressourcen im AWS Key Management Service Benutzerhandbuch.

- Das AWS verwaltete CMK für Amazon SNS (Standard) alias/aws/sns ist standardmäßig ausgewählt.

  > **Note**
  >
  > Beachten Sie Folgendes:
  >
  > - Wenn Sie das erste Mal verwenden AWS Management Console , um das AWS verwaltete CMK für Amazon SNS für ein Thema anzugeben, AWS KMS wird das AWS verwaltete CMK für Amazon SNS erstellt.
  > - Alternativ können Sie, wenn Sie die `Publish` Aktion zum ersten Mal für ein Thema verwenden, bei dem SSE aktiviert ist, das AWS verwaltete CMK für Amazon SNS AWS KMS erstellt.

- Um ein benutzerdefiniertes CMK aus Ihrem zu verwenden AWS-Konto, wählen Sie das Feld Customer Master Key (CMK) und wählen Sie dann das benutzerdefinierte CMK aus der Liste aus.

  > **Note**
  >
  > Anweisungen zur Erstellung benutzerdefinierter CMKs Schlüssel finden Sie unter Creating Keys im Developer Guide AWS Key Management Service

- Um einen benutzerdefinierten CMK-ARN von Ihrem AWS-Konto oder einem anderen AWS Konto zu verwenden, geben Sie ihn in das Feld Customer Master Key (CMK) ein.

6. (Optional) Standardmäßig kann nur der Eigentümer des Themas das Thema abonnieren oder Veröffentlichungen dazu vornehmen. Um zusätzliche Zugriffsberechtigungen zu konfigurieren, erweitern Sie den Abschnitt Access policy (Zugriffsrichtlinie). Weitere Informationen finden Sie unter Identity and Access Management in Amazon SNS und Beispiele für die Zugriffskontrolle in Amazon SNS.

> **Note**
>
> Wenn Sie ein Thema mit der Konsole erstellen, verwendet die Standardrichtlinie den Bedingungsschlüssel `aws:SourceOwner`. Dieser Schlüssel ist ähnlich wie `aws:SourceAccount`.

7. (Optional) Um zu konfigurieren, wie Amazon SNS fehlgeschlagene Nachrichtenzustellversuche wiederholt, erweitern Sie den Abschnitt Delivery retry policy (HTTP/S) (Richtlinie für die Zustellungswiederholung (HTTP/S)). Weitere Informationen finden Sie unter Wiederholungsversuche bei der Nachrichtenzustellung Amazon SNS.
8. (Optional) Um zu konfigurieren, wie Amazon SNS die Zustellung von Nachrichten protokolliert CloudWatch, erweitern Sie den Abschnitt Protokollierung des Lieferstatus. Weitere Informationen finden Sie unter Amazon-SNS-Nachrichtenzustellungsstatus.
9. (Optional) Wenn Sie Metadaten-Tags zum Thema hinzufügen, erweitern Sie den Tag-Abschnitt, geben Sie einen Schlüssel und einen Wert ein (optional), und wählen Sie Tag hinzufügen aus. Weitere Informationen finden Sie unter Markierung von Amazon-SNS-Themen.
10. Wählen Sie Thema erstellen aus.

    Das Thema wird erstellt und die ***MyTopic***Seite wird angezeigt.

    Das ThemaName,ARN, (optional)Anzeigename, undEigentümer des ThemasS AWS -Konto-ID werden auf derDetailsSeite angezeigt.
11. Kopieren Sie das Thema ARN in die Zwischenablage, zum Beispiel:

```
arn:aws:sns:us-east-2:123456789012:MyTopic
```

So hinterlegen Sie eine E-Mail-Adresse für das abonnierte Amazon-SNS-Thema

1. Öffnen Sie die Amazon SNS SNS-Konsole unter https://console.aws.amazon.com/sns/v3/home.
2. Wählen Sie im linken Navigationsbereich Subscriptions (Abonnements).
3. Wählen Sie auf der Seite Subscriptions (Abonnements) die Option Create subscription (Abonnement erstellen)aus.
4. Führen Sie auf der Seite Create subscription (Abonnement erstellen) im Abschnitt Details die folgenden Schritte aus:

   a. Wählen Sie für Topic ARN den Amazon Resource Name (ARN) eines Themas.

   b. Für Protocol wählen Sie einen Endpunkttypen. Folgende Endpunkttypen stehen zur Verfügung:

      - HTTP/HTTPS
      - E-Mail/E-Mail-JSON
      - Amazon Data Firehose
      - Amazon SQS

      > **Note**
      > Um ein SNS FIFO-Thema zu abonnieren, wählen Sie diese Option.

      - AWS Lambda
      - Plattformanwendungs-Endpunkt
      - SMS

   c. Für Endpoint, geben Sie den Endpunktwert ein, wie z. B. eine E-Mail-Adresse oder die ARN einer Amazon-SQS-Warteschlange.

   d. Nur Firehose-Endpunkte: Geben Sie für den ARN der Abonnementrolle den ARN der IAM-Rolle an, die Sie für das Schreiben in Firehose-Lieferdatenströme erstellt haben. Weitere Informationen finden Sie unter Voraussetzungen für das Abonnieren von Firehose-Lieferstreams für Amazon SNS SNS-Themen.

   e. (Optional) Für Firehose, Amazon SQS und HTTP/S Endpoints können Sie auch die Zustellung von Rohnachrichten aktivieren. Weitere Informationen finden Sie unter Übermittlung unformatierter Nachrichten Amazon SNS.

f. (Optional) Um eine Filterrichtlinie zu konfigurieren, erweitern Sie den Abschnitt Abonnement-Filterrichtlinie. Weitere Informationen finden Sie unter Filterrichtlinien für Amazon-SNS-Abonnements.

g. (Optional) Um eine Warteschlange für unzustellbare Nachrichten für das Abonnement zu konfigurieren, erweitern Sie den Abschnitt Redrive-Richtlinie (Warteschlange für unzustellbare Nachrichten). Weitere Informationen finden Sie unter Amazon SNS SNS-Warteschlangen für unzustellbare Briefe (). DLQs

h. Wählen Sie Create subscription (Abonnement erstellen) aus.

   Die Konsole erstellt das Abonnement und öffnet die Seite Details des Abonnements.

Mit dem AWS SDKs

Um ein AWS SDK verwenden zu können, müssen Sie es mit Ihren Anmeldeinformationen konfigurieren. Weitere Informationen finden Sie unter Die Dateien für die gemeinsame Konfiguration und die Anmeldeinformationen im AWS SDKs Referenzhandbuch zu Tools.

Die folgenden Code-Beispiele zeigen, wie `CreateTopic` verwendet wird.

.NET

SDK für .NET

> **Note**
>
> Weitere Informationen finden Sie unter GitHub. Hier finden Sie das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel- einrichten und ausführen.

Erstellen Sie ein Thema mit einem bestimmten Namen.

```
using System;
using System.Threading.Tasks;
using Amazon.SimpleNotificationService;
using Amazon.SimpleNotificationService.Model;

/// <summary>
/// This example shows how to use Amazon Simple Notification Service
/// (Amazon SNS) to add a new Amazon SNS topic.
/// </summary>
```

```
    public class CreateSNSTopic
    {
        public static async Task Main()
        {
            string topicName = "ExampleSNSTopic";

            IAmazonSimpleNotificationService client = new
 AmazonSimpleNotificationServiceClient();

            var topicArn = await CreateSNSTopicAsync(client, topicName);
            Console.WriteLine($"New topic ARN: {topicArn}");
        }

        /// <summary>
        /// Creates a new SNS topic using the supplied topic name.
        /// </summary>
        /// <param name="client">The initialized SNS client object used to
        /// create the new topic.</param>
        /// <param name="topicName">A string representing the topic name.</param>
        /// <returns>The Amazon Resource Name (ARN) of the created topic.</
returns>
        public static async Task<string>
 CreateSNSTopicAsync(IAmazonSimpleNotificationService client, string topicName)
        {
            var request = new CreateTopicRequest
            {
                Name = topicName,
            };

            var response = await client.CreateTopicAsync(request);

            return response.TopicArn;
        }
    }
```

Erstellen Sie ein neues Thema mit einem Namen und spezifischen FIFO- und Deduplizierungsattributen.

```
    /// <summary>
    /// Create a new topic with a name and specific FIFO and de-duplication
 attributes.
```

```
    /// </summary>
    /// <param name="topicName">The name for the topic.</param>
    /// <param name="useFifoTopic">True to use a FIFO topic.</param>
    /// <param name="useContentBasedDeduplication">True to use content-based de-
duplication.</param>
    /// <returns>The ARN of the new topic.</returns>
    public async Task<string> CreateTopicWithName(string topicName, bool
 useFifoTopic, bool useContentBasedDeduplication)
    {
        var createTopicRequest = new CreateTopicRequest()
        {
            Name = topicName,
        };

        if (useFifoTopic)
        {
            // Update the name if it is not correct for a FIFO topic.
            if (!topicName.EndsWith(".fifo"))
            {
                createTopicRequest.Name = topicName + ".fifo";
            }

            // Add the attributes from the method parameters.
            createTopicRequest.Attributes = new Dictionary<string, string>
            {
                { "FifoTopic", "true" }
            };
            if (useContentBasedDeduplication)
            {
                createTopicRequest.Attributes.Add("ContentBasedDeduplication",
 "true");
            }
        }

        var createResponse = await
 _amazonSNSClient.CreateTopicAsync(createTopicRequest);
        return createResponse.TopicArn;
    }
```

- Einzelheiten zur API finden Sie CreateTopicin der AWS SDK für .NET API-Referenz.

C++

SDK für C++

> **Note**
>
> Es gibt noch mehr dazu GitHub. Hier finden Sie das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel- einrichten und ausführen.

```
//! Create an Amazon Simple Notification Service (Amazon SNS) topic.
/*!
  \param topicName: An Amazon SNS topic name.
  \param topicARNResult: String to return the Amazon Resource Name (ARN) for the
 topic.
  \param clientConfiguration: AWS client configuration.
  \return bool: Function succeeded.
 */
bool AwsDoc::SNS::createTopic(const Aws::String &topicName,
                              Aws::String &topicARNResult,
                              const Aws::Client::ClientConfiguration
 &clientConfiguration) {
    Aws::SNS::SNSClient snsClient(clientConfiguration);

    Aws::SNS::Model::CreateTopicRequest request;
    request.SetName(topicName);

    const Aws::SNS::Model::CreateTopicOutcome outcome =
 snsClient.CreateTopic(request);

    if (outcome.IsSuccess()) {
        topicARNResult = outcome.GetResult().GetTopicArn();
        std::cout << "Successfully created an Amazon SNS topic " << topicName
                  << " with topic ARN '" << topicARNResult
                  << "'." << std::endl;

    }
    else {
        std::cerr << "Error creating topic " << topicName << ":" <<
                  outcome.GetError().GetMessage() << std::endl;
        topicARNResult.clear();
    }
```

```
    return outcome.IsSuccess();
}
```

- Einzelheiten zur API finden Sie CreateTopicin der AWS SDK für C++ API-Referenz.

CLI

AWS CLI

So erstellen Sie ein SNS-Thema

Das folgende `create-topic`-Beispiel erstellt ein SNS-Thema namens `my-topic`.

```
aws sns create-topic \
    --name my-topic
```

Ausgabe:

```
{
    "ResponseMetadata": {
        "RequestId": "1469e8d7-1642-564e-b85d-a19b4b341f83"
    },
    "TopicArn": "arn:aws:sns:us-west-2:123456789012:my-topic"
}
```

Weitere Informationen finden Sie unter Verwenden der AWS Befehlszeilenschnittstelle mit Amazon SQS und Amazon SNS im Benutzerhandbuch für die AWS Befehlszeilenschnittstelle.

- Einzelheiten zur API finden Sie unter CreateTopic AWS CLIBefehlsreferenz.

Go

SDK für Go V2

> **Note**
>
> Es gibt noch mehr dazu GitHub. Hier finden Sie das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel- einrichten und ausführen.

```
import (
 "context"
 "encoding/json"
 "log"

 "github.com/aws/aws-sdk-go-v2/aws"
 "github.com/aws/aws-sdk-go-v2/service/sns"
 "github.com/aws/aws-sdk-go-v2/service/sns/types"
)

// SnsActions encapsulates the Amazon Simple Notification Service (Amazon SNS)
 actions
// used in the examples.
type SnsActions struct {
 SnsClient *sns.Client
}



// CreateTopic creates an Amazon SNS topic with the specified name. You can
 optionally
// specify that the topic is created as a FIFO topic and whether it uses content-
based
// deduplication instead of ID-based deduplication.
func (actor SnsActions) CreateTopic(ctx context.Context, topicName string,
 isFifoTopic bool, contentBasedDeduplication bool) (string, error) {
 var topicArn string
 topicAttributes := map[string]string{}
 if isFifoTopic {
  topicAttributes["FifoTopic"] = "true"
 }
 if contentBasedDeduplication {
  topicAttributes["ContentBasedDeduplication"] = "true"
 }
 topic, err := actor.SnsClient.CreateTopic(ctx, &sns.CreateTopicInput{
  Name:       aws.String(topicName),
  Attributes: topicAttributes,
 })
 if err != nil {
  log.Printf("Couldn't create topic %v. Here's why: %v\n", topicName, err)
 } else {
  topicArn = *topic.TopicArn
```

```
 }

 return topicArn, err
}
```

- Einzelheiten zur API finden Sie CreateTopicin der AWS SDK für Go API-Referenz.

Java

SDK für Java 2.x

> **Note**
>
> Es gibt noch mehr dazu GitHub. Hier finden Sie das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel- einrichten und ausführen.

```
import software.amazon.awssdk.regions.Region;
import software.amazon.awssdk.services.sns.SnsClient;
import software.amazon.awssdk.services.sns.model.CreateTopicRequest;
import software.amazon.awssdk.services.sns.model.CreateTopicResponse;
import software.amazon.awssdk.services.sns.model.SnsException;

/**
 * Before running this Java V2 code example, set up your development
 * environment, including your credentials.
 *
 * For more information, see the following documentation topic:
 *
 * https://docs.aws.amazon.com/sdk-for-java/latest/developer-guide/get-
started.html
 */
public class CreateTopic {
    public static void main(String[] args) {
        final String usage = """

                Usage:    <topicName>

                Where:
```

```
                    topicName - The name of the topic to create (for example,
 mytopic).

                """;

        if (args.length != 1) {
            System.out.println(usage);
            System.exit(1);
        }

        String topicName = args[0];
        System.out.println("Creating a topic with name: " + topicName);
        SnsClient snsClient = SnsClient.builder()
                .region(Region.US_EAST_1)
                .build();

        String arnVal = createSNSTopic(snsClient, topicName);
        System.out.println("The topic ARN is" + arnVal);
        snsClient.close();
    }

    public static String createSNSTopic(SnsClient snsClient, String topicName) {
        CreateTopicResponse result;
        try {
            CreateTopicRequest request = CreateTopicRequest.builder()
                    .name(topicName)
                    .build();

            result = snsClient.createTopic(request);
            return result.topicArn();

        } catch (SnsException e) {
            System.err.println(e.awsErrorDetails().errorMessage());
            System.exit(1);
        }
        return "";
    }
}
```

- Einzelheiten zur API finden Sie CreateTopicin der AWS SDK for Java 2.x API-Referenz.

JavaScript

SDK für JavaScript (v3)

> **Note**
>
> Es gibt noch mehr dazu GitHub. Hier finden Sie das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel- einrichten und ausführen.

Erstellen Sie den Client in einem separaten Modul und exportieren Sie ihn.

```
import { SNSClient } from "@aws-sdk/client-sns";

// The AWS Region can be provided here using the `region` property. If you leave
 it blank
// the SDK will default to the region set in your AWS config.
export const snsClient = new SNSClient({});
```

Importieren Sie das SDK- und Client-Module und rufen Sie die API auf.

```
import { CreateTopicCommand } from "@aws-sdk/client-sns";
import { snsClient } from "../libs/snsClient.js";

/**
 * @param {string} topicName - The name of the topic to create.
 */
export const createTopic = async (topicName = "TOPIC_NAME") => {
  const response = await snsClient.send(
    new CreateTopicCommand({ Name: topicName }),
  );
  console.log(response);
  // {
  //   '$metadata': {
  //     httpStatusCode: 200,
  //     requestId: '087b8ad2-4593-50c4-a496-d7e90b82cf3e',
  //     extendedRequestId: undefined,
  //     cfId: undefined,
  //     attempts: 1,
  //     totalRetryDelay: 0
  //   },
```

```
  //   TopicArn: 'arn:aws:sns:us-east-1:xxxxxxxxxxxx:TOPIC_NAME'
  // }
  return response;
};
```

- Weitere Informationen finden Sie im AWS SDK für JavaScript -Entwicklerhandbuch.
- Einzelheiten zur API finden Sie CreateTopicin der AWS SDK für JavaScript API-Referenz.

Kotlin

SDK für Kotlin

> **Note**
>
> Es gibt noch mehr dazu GitHub. Hier finden Sie das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel- einrichten und ausführen.

```
suspend fun createSNSTopic(topicName: String): String {
    val request =
        CreateTopicRequest {
            name = topicName
        }

    SnsClient { region = "us-east-1" }.use { snsClient ->
        val result = snsClient.createTopic(request)
        return result.topicArn.toString()
    }
}
```

- API-Details finden Sie CreateTopicin der API-Referenz zum AWS SDK für Kotlin.

PHP

SDK für PHP

> **Note**
>
> Es gibt noch mehr dazu. GitHub Hier finden Sie das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel- einrichten und ausführen.

```
require 'vendor/autoload.php';

use Aws\Exception\AwsException;
use Aws\Sns\SnsClient;


/**
 * Create a Simple Notification Service topics in your AWS account at the
 requested region.
 *
 * This code expects that you have AWS credentials set up per:
 * https://docs.aws.amazon.com/sdk-for-php/v3/developer-guide/
guide_credentials.html
 */

$SnSclient = new SnsClient([
    'profile' => 'default',
    'region' => 'us-east-1',
    'version' => '2010-03-31'
]);

$topicname = 'myTopic';

try {
    $result = $SnSclient->createTopic([
        'Name' => $topicname,
    ]);
    var_dump($result);
} catch (AwsException $e) {
    // output error message if fails
    error_log($e->getMessage());
}
```

- Weitere Informationen finden Sie im AWS SDK für PHP -Entwicklerhandbuch.
- Einzelheiten zur API finden Sie CreateTopicin der AWS SDK für PHP API-Referenz.

Python

SDK für Python (Boto3)

> **Note**
>
> Es gibt noch mehr dazu GitHub. Hier finden Sie das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel- einrichten und ausführen.

```
class SnsWrapper:
    """Encapsulates Amazon SNS topic and subscription functions."""

    def __init__(self, sns_resource):
        """
        :param sns_resource: A Boto3 Amazon SNS resource.
        """
        self.sns_resource = sns_resource


    def create_topic(self, name):
        """
        Creates a notification topic.

        :param name: The name of the topic to create.
        :return: The newly created topic.
        """
        try:
            topic = self.sns_resource.create_topic(Name=name)
            logger.info("Created topic %s with ARN %s.", name, topic.arn)
        except ClientError:
            logger.exception("Couldn't create topic %s.", name)
            raise
        else:
            return topic
```

- Einzelheiten zur API finden Sie CreateTopicin AWS SDK for Python (Boto3) API Reference.

Ruby

SDK für Ruby

> **Note**
>
> Es gibt noch mehr dazu. GitHub Hier finden Sie das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel- einrichten und ausführen.

```
# This class demonstrates how to create an Amazon Simple Notification Service
 (SNS) topic.
class SNSTopicCreator
  # Initializes an SNS client.
  #
  # Utilizes the default AWS configuration for region and credentials.
  def initialize
    @sns_client = Aws::SNS::Client.new
  end

  # Attempts to create an SNS topic with the specified name.
  #
  # @param topic_name [String] The name of the SNS topic to create.
  # @return [Boolean] true if the topic was successfully created, false
 otherwise.
  def create_topic(topic_name)
    @sns_client.create_topic(name: topic_name)
    puts "The topic '#{topic_name}' was successfully created."
    true
  rescue Aws::SNS::Errors::ServiceError => e
    # Handles SNS service errors gracefully.
    puts "Error while creating the topic named '#{topic_name}': #{e.message}"
    false
  end
end

# Example usage:
```

```
if $PROGRAM_NAME == __FILE__
  topic_name = 'YourTopicName' # Replace with your topic name
  sns_topic_creator = SNSTopicCreator.new

  puts "Creating the topic '#{topic_name}'..."
  unless sns_topic_creator.create_topic(topic_name)
    puts 'The topic was not created. Stopping program.'
    exit 1
  end
end
```

- Weitere Informationen finden Sie im AWS SDK für Ruby -Entwicklerhandbuch.
- Einzelheiten zur API finden Sie CreateTopicin der AWS SDK für Ruby API-Referenz.

Rust

SDK für Rust

> **Note**
>
> Es gibt noch mehr dazu GitHub. Hier finden Sie das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel- einrichten und ausführen.

```
async fn make_topic(client: &Client, topic_name: &str) -> Result<(), Error> {
    let resp = client.create_topic().name(topic_name).send().await?;

    println!(
        "Created topic with ARN: {}",
        resp.topic_arn().unwrap_or_default()
    );

    Ok(())
}
```

- Einzelheiten zur API finden Sie CreateTopicin der API-Referenz zum AWS SDK für Rust.

SAP ABAP

SDK für SAP ABAP

> **Note**
>
> Es gibt noch mehr dazu GitHub. Hier finden Sie das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel- einrichten und ausführen.

```
   TRY.
       oo_result = lo_sns->createtopic( iv_name = iv_topic_name ). " oo_result
is returned for testing purposes. "
       MESSAGE 'SNS topic created' TYPE 'I'.
     CATCH /aws1/cx_snstopiclimitexcdex.
       MESSAGE 'Unable to create more topics. You have reached the maximum
number of topics allowed.' TYPE 'E'.
   ENDTRY.
```

- Einzelheiten zur API finden Sie CreateTopicin der API-Referenz zum AWS SDK für SAP ABAP.

Swift

SDK für Swift

> **Note**
>
> Es gibt noch mehr dazu. GitHub Hier finden Sie das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel- einrichten und ausführen.

```
import AWSSNS

        let config = try await SNSClient.SNSClientConfiguration(region: region)
        let snsClient = SNSClient(config: config)

        let output = try await snsClient.createTopic(
            input: CreateTopicInput(name: name)
```

```
        )

        guard let arn = output.topicArn else {
            print("No topic ARN returned by Amazon SNS.")
            return
        }
```

- Einzelheiten zur API finden Sie CreateTopicin der API-Referenz zum AWS SDK für Swift.

> **Note**
>
> Sie können auch ein Amazon-SNS-Thema in einem anderen Konto verwenden, allerdings müssen Sie dann ggf. eine Richtlinie für Themen erstellen, die Zugriffsberechtigungen für AWS Config gewährt. Weitere Informationen zum Erteilen von Berechtigungen für ein Amazon-SNS-Thema finden Sie unter Berechtigungen für das Amazon-SNS-Thema. Rufen Sie anschließend Schritt 3: Eine IAM-Rolle erstellen auf.

Schritt 3: Eine IAM-Rolle erstellen

> **Important**
>
> (Empfohlen) Verwenden Sie die AWS Config serviceverknüpfte Rolle
> Es wird empfohlen, die AWS Config dienstverknüpfte Rolle zu verwenden:. `AWSServiceRoleForConfig` Dienstbezogene Rollen sind vordefiniert und enthalten alle Berechtigungen, die zum Aufrufen anderer Rollen AWS Config erforderlich sind. AWS-Services Die AWS Config dienstverknüpfte Rolle ist für dienstverknüpfte Konfigurationsrekorder erforderlich.
> Weitere Informationen finden Sie unter Verwenden von Service-verknüpften Rollen für AWS Config.

Verwenden der IAM-Konsole

Sie können die IAM-Konsole verwenden, um eine IAM-Rolle zu erstellen, die AWS Config Berechtigungen für den Zugriff auf Ihren Amazon S3-Bucket, für den Zugriff auf Ihr Amazon SNS SNS-Thema und für das Abrufen von Konfigurationsdetails für unterstützte Ressourcen gewährt.

AWS Wenn Sie eine IAM-Rolle über die Konsole erstellen, fügt AWS Config automatisch die benötigten Berechtigungen an die Rolle an.

> **Note**
>
> Wenn Sie einen AWS Dienst verwendet haben, der verwendet AWS Config (z. B. AWS Security Hub oder AWS Control Tower) und bereits eine AWS Config Rolle erstellt wurde, sollten Sie sicherstellen, dass die IAM-Rolle, die Sie bei der Einrichtung verwenden, dieselben Mindestberechtigungen wie die bereits erstellte AWS Config Rolle AWS Config beibehält, damit der andere AWS Dienst weiterhin wie erwartet ausgeführt werden kann. Wenn AWS Control Tower beispielsweise über eine IAM-Rolle verfügt, die das Lesen von Amazon S3 S3-Objekten ermöglicht AWS Config , sollten Sie sicherstellen, dass innerhalb der IAM-Rolle, die Sie bei der Einrichtung verwenden, dieselben Berechtigungen gewährt werden. AWS Config Andernfalls kann es den Betrieb des AWS Control Tower beeinträchtigen.
> Weitere Informationen zu IAM-Rollen für finden Sie AWS Config unter AWS Identity and Access Management.

Um eine Rolle für einen Dienst zu erstellen AWS

1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die IAM-Konsole unter https://console.aws.amazon.com/iam/.
2. Klicken Sie im Navigationsbereich der IAM-Konsole auf Rollen, und wählen Sie dann Rolle erstellen.
3. Wählen Sie für Select trusted entity (Vertrauenswürdige Entität auswählen) die Option AWS - Dienst.
4. Wählen Sie den gewünschten Anwendungsfall für AWS Config: Config — Customizable, Config — Organizations, Config oder Config — Conformance Packs. Wählen Sie anschließend Weiter.
5. Überprüfen Sie auf der Seite Name, prüfen und erstellen die Details zu Ihrer Rolle und wählen Sie Rolle erstellen aus.

Verwenden des AWS SDKs

Um ein AWS SDK verwenden zu können, müssen Sie es mit Ihren Anmeldeinformationen konfigurieren. Weitere Informationen finden Sie unter Die Dateien für die gemeinsame Konfiguration und die Anmeldeinformationen im AWS SDKs Referenzhandbuch zu Tools.

Die folgenden Code-Beispiele zeigen, wie `CreateRole` verwendet wird.

.NET

SDK für .NET

> **Note**
>
> Weitere Informationen finden Sie unter GitHub. Hier finden Sie das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel- einrichten und ausführen.

```
    /// <summary>
    /// Create a new IAM role.
    /// </summary>
    /// <param name="roleName">The name of the IAM role.</param>
    /// <param name="rolePolicyDocument">The name of the IAM policy document
    /// for the new role.</param>
    /// <returns>The Amazon Resource Name (ARN) of the role.</returns>
    public async Task<string> CreateRoleAsync(string roleName, string
rolePolicyDocument)
    {
        var request = new CreateRoleRequest
        {
            RoleName = roleName,
            AssumeRolePolicyDocument = rolePolicyDocument,
        };

        var response = await _IAMService.CreateRoleAsync(request);
        return response.Role.Arn;
    }
```

- Einzelheiten zur API finden Sie CreateRolein der AWS SDK für .NET API-Referenz.

Bash

AWS CLI mit Bash-Skript

> **Note**
>
> Es gibt noch mehr dazu. GitHub Hier finden Sie das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel- einrichten und ausführen.

```
###############################################################################
# function errecho
#
# This function outputs everything sent to it to STDERR (standard error output).
###############################################################################
function errecho() {
  printf "%s\n" "$*" 1>&2
}

###############################################################################
# function iam_create_role
#
# This function creates an IAM role.
#
# Parameters:
#       -n role_name -- The name of the IAM role.
#       -p policy_json -- The assume role policy document.
#
# Returns:
#       The ARN of the role.
#     And:
#       0 - If successful.
#       1 - If it fails.
###############################################################################
function iam_create_role() {
  local role_name policy_document response
  local option OPTARG # Required to use getopts command in a function.

  # bashsupport disable=BP5008
  function usage() {
    echo "function iam_create_user_access_key"
    echo "Creates an AWS Identity and Access Management (IAM) role."
```

```
  echo "  -n role_name   The name of the IAM role."
  echo "  -p policy_json -- The assume role policy document."
  echo ""
}

# Retrieve the calling parameters.
while getopts "n:p:h" option; do
  case "${option}" in
    n) role_name="${OPTARG}" ;;
    p) policy_document="${OPTARG}" ;;
    h)
      usage
      return 0
      ;;
    \?)
      echo "Invalid parameter"
      usage
      return 1
      ;;
  esac
done
export OPTIND=1

if [[ -z "$role_name" ]]; then
  errecho "ERROR: You must provide a role name with the -n parameter."
  usage
  return 1
fi

if [[ -z "$policy_document" ]]; then
  errecho "ERROR: You must provide a policy document with the -p parameter."
  usage
  return 1
fi

response=$(aws iam create-role \
  --role-name "$role_name" \
  --assume-role-policy-document "$policy_document" \
  --output text \
  --query Role.Arn)

local error_code=${?}

if [[ $error_code -ne 0 ]]; then
```

```
    aws_cli_error_log $error_code
    errecho "ERROR: AWS reports create-role operation failed.\n$response"
    return 1
  fi

  echo "$response"

  return 0
}
```

- Einzelheiten zur API finden Sie CreateRolein der AWS CLI Befehlsreferenz.

C++

SDK für C++

> **Note**
>
> Es gibt noch mehr dazu GitHub. Hier finden Sie das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel- einrichten und ausführen.

```
bool AwsDoc::IAM::createIamRole(
        const Aws::String &roleName,
        const Aws::String &policy,
        const Aws::Client::ClientConfiguration &clientConfig) {
    Aws::IAM::IAMClient client(clientConfig);
    Aws::IAM::Model::CreateRoleRequest request;

    request.SetRoleName(roleName);
    request.SetAssumeRolePolicyDocument(policy);

    Aws::IAM::Model::CreateRoleOutcome outcome = client.CreateRole(request);
    if (!outcome.IsSuccess()) {
        std::cerr << "Error creating role. " <<
                  outcome.GetError().GetMessage() << std::endl;
    }
    else {
        const Aws::IAM::Model::Role iamRole = outcome.GetResult().GetRole();
        std::cout << "Created role " << iamRole.GetRoleName() << "\n";
        std::cout << "ID: " << iamRole.GetRoleId() << "\n";
```

```
        std::cout << "ARN: " << iamRole.GetArn() << std::endl;
    }

    return outcome.IsSuccess();
}
```

- Einzelheiten zur API finden Sie CreateRolein der AWS SDK für C++ API-Referenz.

CLI

AWS CLI

Beispiel 1: So erstellen Sie eine IAM-Rolle

Mit dem folgenden `create-role`-Befehl wird eine Rolle mit dem Namen `Test-Role` erstellt und ihr eine Vertrauensrichtlinie angefügt.

```
aws iam create-role \
    --role-name Test-Role \
    --assume-role-policy-document file://Test-Role-Trust-Policy.json
```

Ausgabe:

```
{
    "Role": {
        "AssumeRolePolicyDocument": "<URL-encoded-JSON>",
        "RoleId": "AKIAIOSFODNN7EXAMPLE",
        "CreateDate": "2013-06-07T20:43:32.821Z",
        "RoleName": "Test-Role",
        "Path": "/",
        "Arn": "arn:aws:iam::123456789012:role/Test-Role"
    }
}
```

Die Vertrauensrichtlinie ist als JSON-Dokument in der Datei Test-Role-Trust-Policy.json definiert. (Der Dateiname und die Erweiterung sind nicht von Bedeutung.) Die Vertrauensrichtlinie muss einen Prinzipal angeben.

Verwenden Sie den `put-role-policy`-Befehl, um die Berechtigungsrichtlinie der Rolle anzufügen.

Weitere Informationen finden Sie unter Erstellen von IAM-Rollen im AWS -IAM-Benutzerhandbuch.

Beispiel 2: So erstellen Sie eine IAM-Rolle mit angegebener maximaler Sitzungsdauer

Mit dem folgenden `create-role`-Befehl wird eine Rolle mit dem Namen `Test-Role` erstellt und eine maximale Sitzungsdauer von 7 200 Sekunden (2 Stunden) festgelegt.

```
aws iam create-role \
    --role-name Test-Role \
    --assume-role-policy-document file://Test-Role-Trust-Policy.json \
    --max-session-duration 7200
```

Ausgabe:

```
{
    "Role": {
        "Path": "/",
        "RoleName": "Test-Role",
        "RoleId": "AKIAIOSFODNN7EXAMPLE",
        "Arn": "arn:aws:iam::12345678012:role/Test-Role",
        "CreateDate": "2023-05-24T23:50:25+00:00",
        "AssumeRolePolicyDocument": {
            "Version": "2012-10-17",
            "Statement": [
                {
                    "Sid": "Statement1",
                    "Effect": "Allow",
                    "Principal": {
                        "AWS": "arn:aws:iam::12345678012:root"
                    },
                    "Action": "sts:AssumeRole"
                }
            ]
        }
    }
}
```

Weitere Informationen finden Sie im AWS IAM-Benutzerhandbuch unter Ändern der maximalen Sitzungsdauer (AWS API) einer Rolle.

Beispiel 3: So erstellen Sie eine IAM-Rolle mit Tags

Mit dem folgenden Befehl wird eine IAM-Rolle `Test-Role` mit Tags erstellt. In diesem Beispiel wird das `--tags`-Parameter-Flag mit den folgenden JSON-formatierten Tags verwendet: `'{"Key": "Department", "Value": "Accounting"}' '{"Key": "Location", "Value": "Seattle"}'`. Alternativ kann das `--tags`-Flag mit Tags im Kurzformat `'Key=Department,Value=Accounting Key=Location,Value=Seattle'` verwendet werden.

```
aws iam create-role \
    --role-name Test-Role \
    --assume-role-policy-document file://Test-Role-Trust-Policy.json \
    --tags '{"Key": "Department", "Value": "Accounting"}' '{"Key": "Location",
 "Value": "Seattle"}'
```

Ausgabe:

```
{
    "Role": {
        "Path": "/",
        "RoleName": "Test-Role",
        "RoleId": "AKIAIOSFODNN7EXAMPLE",
        "Arn": "arn:aws:iam::123456789012:role/Test-Role",
        "CreateDate": "2023-05-25T23:29:41+00:00",
        "AssumeRolePolicyDocument": {
            "Version": "2012-10-17",
            "Statement": [
                {
                    "Sid": "Statement1",
                    "Effect": "Allow",
                    "Principal": {
                        "AWS": "arn:aws:iam::123456789012:root"
                    },
                    "Action": "sts:AssumeRole"
                }
            ]
        },
        "Tags": [
            {
                "Key": "Department",
                "Value": "Accounting"
            },
            {
                "Key": "Location",
```

```
                "Value": "Seattle"
            }
        ]
    }
}
```

Weitere Informationen finden Sie unter Taggen von IAM-Rollen im AWS -IAM-Benutzerhandbuch.

- Einzelheiten zur API finden Sie unter CreateRole AWS CLIBefehlsreferenz.

Go

SDK für Go V2

> **Note**
>
> Es gibt noch mehr dazu GitHub. Hier finden Sie das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel- einrichten und ausführen.

```
import (
 "context"
 "encoding/json"
 "log"

 "github.com/aws/aws-sdk-go-v2/aws"
 "github.com/aws/aws-sdk-go-v2/service/iam"
 "github.com/aws/aws-sdk-go-v2/service/iam/types"
)

// RoleWrapper encapsulates AWS Identity and Access Management (IAM) role actions
// used in the examples.
// It contains an IAM service client that is used to perform role actions.
type RoleWrapper struct {
 IamClient *iam.Client
}
```

```
// CreateRole creates a role that trusts a specified user. The trusted user can
 assume
// the role to acquire its permissions.
// PolicyDocument shows how to work with a policy document as a data structure
 and
// serialize it to JSON by using Go's JSON marshaler.
func (wrapper RoleWrapper) CreateRole(ctx context.Context, roleName string,
 trustedUserArn string) (*types.Role, error) {
 var role *types.Role
 trustPolicy := PolicyDocument{
  Version: "2012-10-17",
  Statement: []PolicyStatement{{
   Effect:    "Allow",
   Principal: map[string]string{"AWS": trustedUserArn},
   Action:    []string{"sts:AssumeRole"},
  }},
 }
 policyBytes, err := json.Marshal(trustPolicy)
 if err != nil {
  log.Printf("Couldn't create trust policy for %v. Here's why: %v\n",
 trustedUserArn, err)
  return nil, err
 }
 result, err := wrapper.IamClient.CreateRole(ctx, &iam.CreateRoleInput{
  AssumeRolePolicyDocument: aws.String(string(policyBytes)),
  RoleName:                 aws.String(roleName),
 })
 if err != nil {
  log.Printf("Couldn't create role %v. Here's why: %v\n", roleName, err)
 } else {
  role = result.Role
 }
 return role, err
}
```

- Einzelheiten zur API finden Sie CreateRolein der AWS SDK für Go API-Referenz.

Java

SDK für Java 2.x

> **Note**
>
> Es gibt noch mehr dazu GitHub. Hier finden Sie das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel- einrichten und ausführen.

```
import org.json.simple.JSONObject;
import org.json.simple.parser.JSONParser;
import software.amazon.awssdk.services.iam.model.CreateRoleRequest;
import software.amazon.awssdk.services.iam.model.CreateRoleResponse;
import software.amazon.awssdk.services.iam.model.IamException;
import software.amazon.awssdk.regions.Region;
import software.amazon.awssdk.services.iam.IamClient;
import java.io.FileReader;

/*
*   This example requires a trust policy document. For more information, see:
*   https://aws.amazon.com/blogs/security/how-to-use-trust-policies-with-iam-
roles/
*
*
*  In addition, set up your development environment, including your credentials.
*
*  For information, see this documentation topic:
*
*  https://docs.aws.amazon.com/sdk-for-java/latest/developer-guide/get-
started.html
 */

public class CreateRole {
    public static void main(String[] args) throws Exception {
        final String usage = """
                Usage:
                    <rolename> <fileLocation>\s

                Where:
                    rolename - The name of the role to create.\s
```

```
                    fileLocation - The location of the JSON document that
represents the trust policy.\s
                """;

        if (args.length != 2) {
            System.out.println(usage);
            System.exit(1);
        }

        String rolename = args[0];
        String fileLocation = args[1];
        Region region = Region.AWS_GLOBAL;
        IamClient iam = IamClient.builder()
                .region(region)
                .build();

        String result = createIAMRole(iam, rolename, fileLocation);
        System.out.println("Successfully created user: " + result);
        iam.close();
    }

    public static String createIAMRole(IamClient iam, String rolename, String
fileLocation) throws Exception {
        try {
            JSONObject jsonObject = (JSONObject)
readJsonSimpleDemo(fileLocation);
            CreateRoleRequest request = CreateRoleRequest.builder()
                    .roleName(rolename)
                    .assumeRolePolicyDocument(jsonObject.toJSONString())
                    .description("Created using the AWS SDK for Java")
                    .build();

            CreateRoleResponse response = iam.createRole(request);
            System.out.println("The ARN of the role is " +
response.role().arn());

        } catch (IamException e) {
            System.err.println(e.awsErrorDetails().errorMessage());
            System.exit(1);
        }
        return "";
    }

    public static Object readJsonSimpleDemo(String filename) throws Exception {
```

```
        FileReader reader = new FileReader(filename);
        JSONParser jsonParser = new JSONParser();
        return jsonParser.parse(reader);
    }
}
```

- Einzelheiten zur API finden Sie CreateRolein der AWS SDK for Java 2.x API-Referenz.

JavaScript

SDK für JavaScript (v3)

> **Note**
>
> Es gibt noch mehr dazu GitHub. Hier finden Sie das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel- einrichten und ausführen.

Erstellen Sie die -Rolle.

```
import { CreateRoleCommand, IAMClient } from "@aws-sdk/client-iam";

const client = new IAMClient({});

/**
 *
 * @param {string} roleName
 */
export const createRole = (roleName) => {
  const command = new CreateRoleCommand({
    AssumeRolePolicyDocument: JSON.stringify({
      Version: "2012-10-17",
      Statement: [
        {
          Effect: "Allow",
          Principal: {
            Service: "lambda.amazonaws.com",
          },
          Action: "sts:AssumeRole",
        },
      ],
```

```
    }),
    RoleName: roleName,
  });

  return client.send(command);
};
```

- Einzelheiten zur API finden Sie CreateRolein der AWS SDK für JavaScript API-Referenz.

PHP

SDK für PHP

> **Note**
>
> Es gibt noch mehr dazu GitHub. Hier finden Sie das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel- einrichten und ausführen.

```
$uuid = uniqid();
$service = new IAMService();

$assumeRolePolicyDocument = "{
                \"Version\": \"2012-10-17\",
                \"Statement\": [{
                    \"Effect\": \"Allow\",
                    \"Principal\": {\"AWS\": \"{$user['Arn']}\"},
                    \"Action\": \"sts:AssumeRole\"
                }]
            }";
$assumeRoleRole = $service->createRole("iam_demo_role_$uuid",
 $assumeRolePolicyDocument);
echo "Created role: {$assumeRoleRole['RoleName']}\n";

    /**
     * @param string $roleName
     * @param string $rolePolicyDocument
     * @return array
     * @throws AwsException
     */
    public function createRole(string $roleName, string $rolePolicyDocument)
```

```
    {
        $result = $this->customWaiter(function () use ($roleName,
 $rolePolicyDocument) {
            return $this->iamClient->createRole([
                'AssumeRolePolicyDocument' => $rolePolicyDocument,
                'RoleName' => $roleName,
            ]);
        });
        return $result['Role'];
    }
```

- Einzelheiten zur API finden Sie CreateRolein der AWS SDK für PHP API-Referenz.

PowerShell

Tools für PowerShell V4

Beispiel 1: In diesem Beispiel wird eine neue Rolle mit dem Namen **`MyNewRole`** erstellt und die in der Datei **`NewRoleTrustPolicy.json`** gefundene Richtlinie daran angefügt. Beachten Sie, dass Sie den **`-Raw`**-Switch-Parameter verwenden müssen, um die JSON-Richtliniendatei erfolgreich zu verarbeiten. Das in der Ausgabe angezeigte Richtliniendokument ist URL-codiert. Die Dekodierung erfolgt in diesem Beispiel mit der **`UrlDecode`** .NET-Methode.

```
$results = New-IAMRole -AssumeRolePolicyDocument (Get-Content -raw
 NewRoleTrustPolicy.json) -RoleName MyNewRole
$results
```

Ausgabe:

```
Arn                      : arn:aws:iam::123456789012:role/MyNewRole
AssumeRolePolicyDocument : %7B%0D%0A%20%20%22Version%22%3A%20%222012-10-17%22%2C
%0D%0A%20%20%22Statement%22
                           %3A%20%5B%0D%0A%20%20%20%20%7B%0D%0A
%20%20%20%20%20%20%22Sid%22%3A%20%22%22%2C
                           %0D%0A%20%20%20%20%20%20%22Effect%22%3A%20%22Allow
%22%2C%0D%0A%20%20%20%20%20%20
                           %22Principal%22%3A%20%7B%0D%0A
%20%20%20%20%20%20%20%20%22AWS%22%3A%20%22arn%3Aaws
                           %3Aiam%3A%3A123456789012%3ADavid%22%0D%0A
%20%20%20%20%20%20%7D%2C%0D%0A%20%20%20
```

```
                              %20%20%20%22Action%22%3A%20%22sts%3AAssumeRole%22%0D
%0A%20%20%20%20%7D%0D%0A%20
                              %20%5D%0D%0A%7D
CreateDate                  : 4/15/2015 11:04:23 AM
Path                        : /
RoleId                      : V5PAJI2KPN4EAEXAMPLE1
RoleName                    : MyNewRole

[System.Reflection.Assembly]::LoadWithPartialName("System.Web.HttpUtility")
[System.Web.HttpUtility]::UrlDecode($results.AssumeRolePolicyDocument)
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "",
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::123456789012:David"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

- Einzelheiten zur API finden Sie unter CreateRole AWS -Tools für PowerShellCmdlet-Referenz (V4).

Python

SDK für Python (Boto3)

> **Note**
>
> Es gibt noch mehr dazu. GitHub Hier finden Sie das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel- einrichten und ausführen.

```
def create_role(role_name, allowed_services):
    """
    Creates a role that lets a list of specified services assume the role.
```

```
    :param role_name: The name of the role.
    :param allowed_services: The services that can assume the role.
    :return: The newly created role.
    """
    trust_policy = {
        "Version": "2012-10-17",
        "Statement": [
            {
                "Effect": "Allow",
                "Principal": {"Service": service},
                "Action": "sts:AssumeRole",
            }
            for service in allowed_services
        ],
    }

    try:
        role = iam.create_role(
            RoleName=role_name, AssumeRolePolicyDocument=json.dumps(trust_policy)
        )
        logger.info("Created role %s.", role.name)
    except ClientError:
        logger.exception("Couldn't create role %s.", role_name)
        raise
    else:
        return role
```

- Einzelheiten zur API finden Sie CreateRolein AWS SDK for Python (Boto3) API Reference.

Ruby

SDK für Ruby

> **Note**
>
> Es gibt noch mehr dazu. GitHub Hier finden Sie das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel- einrichten und ausführen.

```
 # Creates a role and attaches policies to it.
 #
 # @param role_name [String] The name of the role.
 # @param assume_role_policy_document [Hash] The trust relationship policy
document.
 # @param policy_arns [Array<String>] The ARNs of the policies to attach.
 # @return [String, nil] The ARN of the new role if successful, or nil if an
error occurred.
 def create_role(role_name, assume_role_policy_document, policy_arns)
   response = @iam_client.create_role(
     role_name: role_name,
     assume_role_policy_document: assume_role_policy_document.to_json
   )
   role_arn = response.role.arn

   policy_arns.each do |policy_arn|
     @iam_client.attach_role_policy(
       role_name: role_name,
       policy_arn: policy_arn
     )
   end

   role_arn
 rescue Aws::IAM::Errors::ServiceError => e
   @logger.error("Error creating role: #{e.message}")
   nil
 end
```

- Einzelheiten zur API finden Sie CreateRolein der AWS SDK für Ruby API-Referenz.

Rust

SDK für Rust

> **Note**
>
> Es gibt noch mehr dazu GitHub. Hier finden Sie das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel- einrichten und ausführen.

```
pub async fn create_role(
    client: &iamClient,
    role_name: &str,
    role_policy_document: &str,
) -> Result<Role, iamError> {
    let response: CreateRoleOutput = loop {
        if let Ok(response) = client
            .create_role()
            .role_name(role_name)
            .assume_role_policy_document(role_policy_document)
            .send()
            .await
        {
            break response;
        }
    };

    Ok(response.role.unwrap())
}
```

- Einzelheiten zur API finden Sie CreateRolein der API-Referenz zum AWS SDK für Rust.

Swift

SDK für Swift

> **Note**
>
> Es gibt noch mehr dazu GitHub. Hier finden Sie das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel- einrichten und ausführen.

```
import AWSIAM
import AWSS3


    public func createRole(name: String, policyDocument: String) async throws ->
 String {
        let input = CreateRoleInput(
            assumeRolePolicyDocument: policyDocument,
```

```
            roleName: name
        )
        do {
            let output = try await client.createRole(input: input)
            guard let role = output.role else {
                throw ServiceHandlerError.noSuchRole
            }
            guard let id = role.roleId else {
                throw ServiceHandlerError.noSuchRole
            }
            return id
        } catch {
            print("ERROR: createRole:", dump(error))
            throw error
        }
    }
```

- Einzelheiten zur API finden Sie CreateRolein der API-Referenz zum AWS SDK für Swift.

Beginnend AWS Config mit einem vom Kunden verwalteten Konfigurationsrekorder unter Verwendung des AWS CLI

Sie können damit beginnen, einen AWS Config vom Kunden verwalteten Konfigurationsrekorder zu erstellen. Verwenden Sie die folgenden Befehle AWS CLI, um einen vom Kunden verwalteten Konfigurationsrekorder mit dem zu erstellen: `put-configuration-recorder`put-delivery-channel, und `start-configuration-recorder`.

- Der `put-configuration-recorder` Befehl erstellt einen vom Kunden verwalteten Konfigurationsrekorder.
- Der `put-delivery-channel` Befehl erstellt einen Bereitstellungskanal, über den AWS Config Konfigurationsinformationen an einen S3-Bucket und ein SNS-Thema gesendet werden.
- Das `start-configuration-recorder` startet den vom Kunden verwalteten Konfigurationsrekorder. Der vom Kunden verwaltete Konfigurationsrekorder beginnt mit der Aufzeichnung von Konfigurationsänderungen für die von Ihnen angegebenen Ressourcentypen.

Themen

- Überlegungen

- Schritt 1: Führen Sie den put-configuration-recorder
- Schritt 2: Führen Sie den put-delivery-channel Befehl aus
- Schritt 3: Führen Sie den start-configuration-recorder Befehl aus

Überlegungen

S3-Bucket, SNS-Thema und IAM-Rolle sind erforderlich

Um einen vom Kunden verwalteten Konfigurationsrekorder zu erstellen, müssen Sie einen S3-Bucket, ein SNS-Thema und eine IAM-Rolle mit angehängten Richtlinien als Voraussetzungen erstellen. Informationen zur Einrichtung Ihrer Voraussetzungen für finden Sie AWS Config unter Voraussetzungen.

Ein vom Kunden verwalteter Konfigurationsrekorder pro Konto und Region

Sie können jeweils AWS-Konto nur einen vom Kunden verwalteten Konfigurationsrekorder verwenden AWS-Region.

Ein Lieferkanal pro Konto und Region

Sie können für jede Region jeweils AWS-Konto nur eine Lieferkanalregion angeben AWS-Region.

Richtlinien und Ergebnisse zur Einhaltung von Vorschriften

IAM-Richtlinien und andere Richtlinien, die in verwaltet werden, AWS Organizations können sich darauf auswirken, ob Sie AWS Config berechtigt sind, Konfigurationsänderungen für Ihre Ressourcen aufzuzeichnen. Darüber hinaus bewerten Regeln direkt die Konfiguration einer Ressource, und Regeln berücksichtigen diese Richtlinien bei der Durchführung von Evaluierungen nicht. Stellen Sie sicher, dass die geltenden Richtlinien mit der Art und Weise übereinstimmen, wie Sie sie verwenden möchten AWS Config.

Schritt 1: Führen Sie den put-configuration-recorder

Verwenden Sie den `put-configuration-recorder`Befehl, um einen vom Kunden verwalteten Konfigurationsrekorder zu erstellen:

Dieser Befehl verwendet die `---recording-group` Felder `--configuration-recorder` und.

```
$ aws configservice put-configuration-recorder \
--configuration-recorder file://configurationRecorder.json \
--recording-group file://recordingGroup.json
```

Das **`configuration-recorder`** Feld

Die `configurationRecorder.json` Datei spezifiziert `name` und `roleArn` auch die Standardaufzeichnungsfrequenz für den Konfigurationsrekorder (`recordingMode`). Sie können dieses Feld auch verwenden, um die Aufzeichnungsfrequenz für bestimmte Ressourcentypen zu überschreiben.

```
{
  "name": "default",
  "roleARN": "arn:aws:iam::123456789012:role/config-role",
  "recordingMode": {
    "recordingFrequency": CONTINUOUS or DAILY,
    "recordingModeOverrides": [
        {
            "description": "Description you provide for the override",
            "recordingFrequency": CONTINUOUS or DAILY,
            "resourceTypes": [ Comma-separated list of resource types to include in the
 override ]
        }
    ]
  }
}
```

Das **`recording-group`** Feld

Die `recordingGroup.json` Datei gibt an, welche Ressourcentypen aufgezeichnet werden.

```
{
    "allSupported": boolean,
    "exclusionByResourceTypes": {
        "resourceTypes": [ Comma-separated list of resource types to exclude ]
    },
    "includeGlobalResourceTypes": boolean,
    "recordingStrategy": {
        "useOnly": "Recording strategy for the configuration recorder"
    },
    "resourceTypes": [ Comma-separated list of resource types to include]
}
```

Weitere Informationen zu diesen Feldern finden Sie `put-configuration-recorder`in der AWS CLI Befehlsreferenz.

Schritt 2: Führen Sie den put-delivery-channel Befehl aus

Verwenden Sie den `put-delivery-channel`Befehl, um einen Lieferkanal zu erstellen:

Dieser Befehl verwendet das `--delivery-channel` Feld.

```
$ aws configservice put-delivery-channel --delivery-channel file://deliveryChannel.json
```

Das **`delivery-channel`** Feld

Die `deliveryChannel.json` Datei spezifiziert Folgendes:

- Die `name` für den Lieferkanal.
- Das `s3BucketName` Where AWS Config sendet Konfigurationsschnappschüsse.
- Der `snsTopicARN` Ort, an den Benachrichtigungen AWS Config gesendet werden
- Damit wird festgelegt`configSnapshotDeliveryProperties`, wie oft AWS Config Konfigurations-Snapshots geliefert werden und wie oft Evaluierungen für periodische Regeln aufgerufen werden.

```
{
    "name": "default",
    "s3BucketName": "config-bucket-123456789012",
    "snsTopicARN": "arn:aws:sns:us-east-1:123456789012:config-topic",
    "configSnapshotDeliveryProperties": {
        "deliveryFrequency": "Twelve_Hours"
    }
}
```

Weitere Informationen zu diesen Feldern finden Sie `put-delivery-channel`in der AWS CLI Befehlsreferenz.

Schritt 3: Führen Sie den start-configuration-recorder Befehl aus

Verwenden Sie den `start-configuration-recorder`Befehl, um zu starten AWS Config:

```
$ aws configservice start-configuration-recorder --configuration-recorder-
name configRecorderName
```

Weitere Informationen zu diesen Feldern finden Sie `start-configuration-recorder`in der AWS CLI Befehlsreferenz.

Überprüfen, ob AWS Config dies erfolgreich gestartet wurde mit dem AWS CLI

Nachdem Sie gestartet haben AWS Config, können Sie mithilfe von AWS CLI Befehlen überprüfen, ob der AWS Config läuft und ob ein Konfigurationsrekorder und ein Lieferkanal erstellt wurden. AWS Config Sie können auch bestätigen, AWS Config dass mit der Aufzeichnung und Übermittlung von Konfigurationen an den Bereitstellungskanal begonnen wurde.

Themen

- Schritt 1: Überprüfen Sie, ob ein Lieferkanal erstellt wurde
- Schritt 2: Überprüfen Sie, ob ein Konfigurationsrekorder erstellt wurde
- Schritt 3: Überprüfen Sie, ob die AWS Config Aufnahme gestartet wurde

Schritt 1: Überprüfen Sie, ob ein Lieferkanal erstellt wurde

Verwenden Sie den Befehl `describe-delivery-channels`, um zu überprüfen, ob Ihr Amazon-S3-Bucket und Amazon-SNS-Thema konfiguriert sind.

Sie können das `--delivery-channel-names` Feld verwenden, um eine Liste von Lieferkanälen anzugeben. Wenn kein Lieferkanal angegeben ist, gibt dieser Befehl die Details aller mit dem Konto verknüpften Lieferkanäle zurück.

```
$ aws configservice describe-delivery-channels
{
    "DeliveryChannels": [
        {
            "snsTopicARN": "arn:aws:sns:us-west-2:0123456789012:my-config-topic",
            "name": "my-delivery-channel",
            "s3BucketName": "my-config-bucket"
        }
    ]
}
```

Schritt 2: Überprüfen Sie, ob ein Konfigurationsrekorder erstellt wurde

Verwenden Sie den `describe-configuration-recorders`Befehl, um zu überprüfen, ob ein Konfigurationsrekorder erstellt wurde.

Sie können die `configuration-recorder-names` Felder `arn` und verwenden, um eine Liste von Konfigurationsrekordern anzugeben. Wenn kein Konfigurationsrekorder angegeben ist, gibt dieser Befehl die Details aller Konfigurationsrekorder zurück, die dem Konto zugeordnet sind.

```
$ aws configservice describe-configuration-recorders
{
    "ConfigurationRecorders": [
        {
            "roleARN": "arn:aws:iam::012345678912:role/myConfigRole",
            "name": "default"
        }
    ]
}
```

Schritt 3: Überprüfen Sie, ob die AWS Config Aufnahme gestartet wurde

Verwenden Sie den `describe-configuration-recorder-status`Befehl, um zu überprüfen, ob der Konfigurationsrekorder die Ressourcentypen im Gültigkeitsbereich erfolgreich aufzeichnet.

Sie können die `configuration-recorder-names` Felder `arn` und verwenden, um eine Liste von Konfigurationsrekordern anzugeben. Wenn kein Konfigurationsrekorder angegeben ist, gibt dieser Befehl die Details aller Konfigurationsrekorder zurück, die dem Konto zugeordnet sind.

```
$ aws configservice describe-configuration-recorder-status
{
    "ConfigurationRecordersStatus": [
        {
            "name": "default",
            "lastStatus": "SUCCESS",
            "lastStopTime": 1414511624.914,
            "lastStartTime": 1414708460.276,
            "recording": true,
            "lastStatusChangeTime": 1414816537.148,
            "lastErrorMessage": "NA",
            "lastErrorCode": "400"
        }
```

```
    ]
}
```

Der `true` Wert in dem `recording` Feld bestätigt, dass der Konfigurationsrekorder mit der Aufzeichnung von Konfigurationen begonnen hat. AWS Config zeichnet die Zeit in UTC auf. Die Ausgabe wird als Unix-Zeitstempel angezeigt.

Verwendung AWS Config mit einem AWS SDK

AWS Software Development Kits (SDKs) sind für viele gängige Programmiersprachen verfügbar. Jedes SDK bietet eine API, Codebeispiele und Dokumentation, die es Entwicklern erleichtern, Anwendungen in ihrer bevorzugten Sprache zu erstellen.

SDK-Dokumentation	Codebeispiele
AWS SDK für C++	AWS SDK für C++ Codebeispiele
AWS CLI	AWS CLI Code-Beispiele
AWS SDK für Go	AWS SDK für Go Code-Beispiele
AWS SDK für Java	AWS SDK für Java Code-Beispiele
AWS SDK für JavaScript	AWS SDK für JavaScript Code-Beispiele
AWS SDK für Kotlin	AWS SDK für Kotlin Code-Beispiele
AWS SDK für .NET	AWS SDK für .NET Code-Beispiele
AWS SDK für PHP	AWS SDK für PHP Code-Beispiele
AWS -Tools für PowerShell	Tools für PowerShell Codebeispiele
AWS SDK für Python (Boto3)	AWS SDK für Python (Boto3) Code-Beispiele
AWS SDK für Ruby	AWS SDK für Ruby Code-Beispiele
AWS SDK for Rust	AWS SDK for Rust Code-Beispiele
AWS SDK für SAP ABAP	AWS SDK für SAP ABAP Code-Beispiele

SDK-Dokumentation	Codebeispiele
AWS SDK for Swift	AWS SDK for Swift Code-Beispiele

Beispiel für die Verfügbarkeit

Sie können nicht finden, was Sie brauchen? Fordern Sie ein Codebeispiel an, indem Sie unten den Link Provide feedback (Feedback geben) auswählen.

Arbeiten mit dem Konfigurationsrekorder

Der Konfigurationsrekorder speichert die Konfigurationsänderungen an den Ressourcentypen im Gültigkeitsbereich als Konfigurationselemente (CIs).

Es gibt zwei Arten von Konfigurationsrekordern.

Typ	Beschreibung
Vom Kunden verwalteter Konfigurationsrekorder	Ein von Ihnen verwalteter Konfigurationsrekorder. Die im Geltungsbereich enthaltenen Ressourcentypen werden von Ihnen festgelegt. Standardmäßig zeichnet ein vom Kunden verwalteter Konfigurationsrekorder alle unterstützten Ressourcen in dem Bereich auf, in AWS-Region dem er ausgeführt AWS Config wird.
Mit dem Dienst verbundener Konfigurationsrekorder	Ein Konfigurationsrekorder, der mit einem bestimmten AWS-Service verknüpft ist. Die im Gültigkeitsbereich angegebenen Ressourcentypen werden vom verknüpften Dienst festgelegt.

Themen

- Überlegungen zum vom Kunden verwalteten Konfigurationsrekorder
- Überlegungen zu serviceverknüpften Konfigurationsrekordern
- Drifterkennung für den Konfigurationsrekorder
- Starten des vom Kunden verwalteten Konfigurationsrekorders
- Den vom Kunden verwalteten Konfigurationsrekorder beenden
- Änderung der Aufzeichnungsfrequenz für den vom Kunden verwalteten Konfigurationsrekorder
- Umbenennen des vom Kunden verwalteten Konfigurationsrekorders
- Ihre Konfigurationsrekorder anzeigen
- Löschen Ihrer Konfigurationsrekorder

Überlegungen zum vom Kunden verwalteten Konfigurationsrekorder

Ein vom Kunden verwalteter Konfigurationsrekorder pro Konto und Region

Sie können jeweils AWS-Konto nur einen vom Kunden verwalteten Konfigurationsrekorder verwenden AWS-Region.

Standardmäßig werden alle unterstützten Ressourcentypen aufgezeichnet, mit Ausnahme der globalen IAM-Ressourcentypen

Standardmäßig zeichnet ein vom Kunden verwalteter Konfigurationsrekorder alle unterstützten Ressourcentypen auf, mit Ausnahme der folgenden globalen IAM-Ressourcentypen:`AWS::IAM::Group`,, und `AWS::IAM::User` Sie können angeben `AWS::IAM::Policy``AWS::IAM::Role`, welche Ressourcentypen Sie in die Aufzeichnung einbeziehen oder von der Aufzeichnung ausschließen möchten.

Weitere Informationen finden Sie unter AWS Ressourcen aufzeichnen mit AWS Config.

Für die Nutzung des vom Kunden verwalteten Konfigurationsrekorders werden Ihnen Gebühren für die Nutzung des Dienstes berechnet

Ihnen werden Gebühren für die Nutzung des Dienstes berechnet, wenn Sie mit der Aufzeichnung von Konfigurationen mit dem vom Kunden verwalteten Konfigurationsrekorder AWS Config beginnen.

Preisinformationen finden Sie unter AWS Config – Preise.

Wird verwendet AWS Systems Manager , um einen vom Kunden verwalteten Konfigurationsrekorder in einem Unternehmen zu erstellen

Sie können AWS Systems Manager Quick Setup verwenden, um einen vom Kunden verwalteten Konfigurationsrekorder für mehrere Organisationseinheiten (OUs) zu erstellen und dabei AWS bewährte Methoden zu AWS-Regionen verwenden.

Weitere Informationen finden Sie unter Erstellen eines AWS Config Konfigurationsrekorders mithilfe von Quick Setup im Systems Manager Manager-Benutzerhandbuch.

> **Important**
>
> Richtlinien und Konformitätsergebnisse

IAM-Richtlinien und andere Richtlinien, die in verwaltet werden, AWS Organizations können sich darauf auswirken, ob Sie AWS Config berechtigt sind, Konfigurationsänderungen für Ihre Ressourcen aufzuzeichnen. Darüber hinaus bewerten Regeln direkt die Konfiguration einer Ressource, und Regeln berücksichtigen diese Richtlinien bei der Durchführung von Evaluierungen nicht. Stellen Sie sicher, dass die geltenden Richtlinien mit der Art und Weise übereinstimmen, wie Sie sie verwenden möchten AWS Config.

Veraltete Evaluierungsergebnisse für gelöschte Ressourcen können bestehen bleiben, wenn der Konfigurationsrekorder ausgeschaltet ist

Wenn der vom Kunden verwaltete Konfigurationsrekorder ausgeschaltet ist, ist AWS Config Config nicht in der Lage, Änderungen an der Konfiguration der von Ihnen angegebenen Ressourcen nachzuverfolgen, einschließlich deren Löschungen. Das bedeutet, dass Sie möglicherweise veraltete Evaluierungsergebnisse für Ressourcen erhalten, die gelöscht werden, wenn der vom Kunden verwaltete Konfigurationsrekorder ausgeschaltet ist, da Löschereignisse AWS Config nicht erfasst werden können, wenn die Aufzeichnung nicht aktiviert ist.

Überlegungen zu serviceverknüpften Konfigurationsrekordern

Die AWS Config serviceverknüpfte Rolle muss verwendet werden

Die AWS Config dienstverknüpfte Rolle ist für dienstverknüpfte Konfigurationsrekorder erforderlich.

Weitere Informationen finden Sie unter Verwenden von Service-verknüpften Rollen für AWS Config.

Mit Diensten verknüpfte Konfigurationsrekorder zeichnen immer auf

Sie können die Aufzeichnung für serviceverknüpfte Konfigurationsrekorder nicht beenden oder starten. Um die Aufzeichnung zu beenden, müssen Sie den mit dem Dienst verknüpften Konfigurationsrekorder löschen.

Weitere Informationen finden Sie unter Löschen des Konfigurationsrekorders.

Der Umfang der Aufzeichnung bestimmt, ob Sie Konfigurationselemente erhalten

Der Umfang der Aufzeichnung wird von dem Dienst festgelegt, der mit dem Konfigurationsrekorder verknüpft ist, und bestimmt, ob Sie Konfigurationselemente (CIs) im Bereitstellungskanal erhalten. Wenn der Umfang der Aufzeichnung intern ist, erhalten Sie keine Daten CIs im Bereitstellungskanal.

Der Umfang der Aufzeichnung bestimmt, ob Ihnen eine Servicegebühr berechnet wird

Der Umfang der Aufzeichnung wird von dem Dienst festgelegt, der mit dem Konfigurationsrekorder verknüpft ist, und bestimmt, ob die im Umfang enthaltenen Konfigurationselemente (CIs) kostenlos aufgezeichnet werden (INTERN) oder ob er sich auf die Kosten Ihrer Rechnung auswirkt (KOSTENPFLICHTIG).

Unterstützte Services

Mit Diensten verknüpfte Konfigurationsrekorder werden für die folgenden Dienste unterstützt:

AWS Service nicht zulässig	Principal des Dienstes	Vorteile der Verwendung mit AWS Config	Weitere Informationen
Amazon CloudWatch	`observability admin.amazonaws.com`	Sie können Amazon CloudWatch Observability Admin verwenden, um den Status der Telemetriekonfiguration CloudWatch für Ihre AWS Organisation oder Ihr Konto zu ermitteln und zu verstehen.	Weitere Informationen finden Sie unter Prüfen von CloudWatch Telemetriekonfigurationen im CloudWatch Benutzerhandbuch.

Drifterkennung für den Konfigurationsrekorder

Der Ressourcentyp `AWS::Config::ConfigurationRecorder` ist ein Konfigurationselement (Configuration Item, CI) für den Konfigurations-Recorder, das alle Änderungen am Status des Konfigurations-Recorders verfolgt. Sie können mit diesem CI überprüfen, ob sich der Status des Konfigurations-Recorders von seinem vorherigen Status unterscheidet. Dies wird auch als Abweichung bezeichnet.

Dieses CI verfolgt beispielsweise, ob Aktualisierungen von Ressourcentypen vorliegen, deren Nachverfolgung Sie in AWS Config aktiviert haben, ob Sie den Konfigurations-Recorder beendet

oder gestartet haben oder ob Sie den Konfigurations-Recorder gelöscht oder deinstalliert haben. Ein abweichender Konfigurations-Recorder weist darauf hin, dass Änderungen an den beabsichtigten Ressourcentypen nicht genau erkannt werden. Wenn Ihr Konfigurations-Recorder abweicht, kann dies zu falsch negativen oder falsch positiven Compliance-Ergebnissen führen.

Der `AWS::Config::ConfigurationRecorder` Ressourcentyp ist ein Systemressourcentyp von, AWS Config und die Aufzeichnung dieses Ressourcentyps ist standardmäßig in allen unterstützten Regionen aktiviert. Für die Aufzeichnung des Ressourcentyps `AWS::Config::ConfigurationRecorder` fallen keine zusätzlichen Kosten an.

Starten des vom Kunden verwalteten Konfigurationsrekorders

Sie können die AWS Config Konsole verwenden oder den vom Kunden verwalteten Konfigurationsrekorder AWS CLI starten.

To start the customer managed configuration recorder (Console)

1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die AWS Config Konsole zu https://console.aws.amazon.com/config/Hause.
2. Wählen Sie im Navigationsbereich Settings (Einstellungen) aus.
3. Wählen Sie auf der Registerkarte Vom Kunden verwalteter Rekorder die Option Aufnahme starten aus. Wenn Sie dazu aufgefordert werden, wählen Sie Bestätigen.

To start the customer managed configuration recorder (CLI)

Verwenden Sie den -Befehl:`start-configuration-recorder`

```
$ aws configservice start-configuration-recorder --configuration-recorder-
name configRecorderName
```

Den vom Kunden verwalteten Konfigurationsrekorder beenden

> **Note**
>
> Mit Diensten verknüpfte Konfigurationsrekorder zeichnen immer auf
> Sie können einen serviceverknüpften Konfigurationsrekorder nicht beenden, da dienstgebundene Konfigurationsaufzeichner immer aufzeichnen. Um die Aufzeichnung zu

beenden, müssen Sie den mit dem Dienst verknüpften Konfigurationsrekorder löschen. Weitere Informationen finden Sie unter Löschen des Konfigurationsrekorders.

Sie können die AWS Config Konsole verwenden oder den vom Kunden verwalteten Konfigurationsrekorder AWS CLI beenden.

To stop the customer managed configuration recorder (Console)

1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die AWS Config Konsole zu https://console.aws.amazon.com/config/Hause.
2. Wählen Sie im Navigationsbereich Settings (Einstellungen) aus.
3. Wählen Sie auf der Registerkarte Vom Kunden verwalteter Rekorder die Option Aufzeichnung beenden aus. Wenn Sie dazu aufgefordert werden, wählen Sie Bestätigen.

To stop the customer managed configuration recorder (CLI)

Verwenden Sie den -Befehl:`stop-configuration-recorder`

```
$ aws configservice stop-configuration-recorder --configuration-recorder-
name configRecorderName
```

Änderung der Aufzeichnungsfrequenz für den vom Kunden verwalteten Konfigurationsrekorder

AWS Config unterstützt kontinuierliche Aufnahme und tägliche Aufnahme:

- Durch die kontinuierliche Aufzeichnung können Sie Konfigurationsänderungen kontinuierlich aufzeichnen, wenn eine Änderung auftritt.
- Durch die tägliche Aufzeichnung können Sie nur dann ein Konfigurationselement (CI) erhalten, das den neuesten Status Ihrer Ressourcen in den letzten 24 Stunden darstellt, wenn es sich von dem zuvor aufgezeichneten CI unterscheidet. Weitere Informationen finden Sie unter Aufzeichnungsfrequenz.

Sie können die AWS Config Konsole verwenden oder die Aufnahmefrequenz AWS CLI ändern.

To change the recording frequency for the customer managed configuration recorder (Console)

1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die AWS Config Konsole zu https://console.aws.amazon.com/config/Hause.
2. Wählen Sie im Navigationsbereich Settings (Einstellungen) aus.
3. Wählen Sie auf der Registerkarte Vom Kunden verwalteter Rekorder die Option Aufnahme starten aus.
4. Wählen Sie unter Aufzeichnungsmethode verwalteter Rekorder die Option Alle Ressourcentypen mit anpassbaren Überschreibungen aus.
5. Wählen Sie für die Standardeinstellungen eine Aufzeichnungsfrequenz aus.
6. Wählen Sie Speichern.

To change the recording frequency (CLI)

Verwenden Sie den `put-configuration-recorder`-Befehl, um die Aufzeichnungsfrequenz für den Konfigurations-Recorder zu ändern:

```
$ aws configservice put-configuration-recorder \
--configuration-recorder file://configurationRecorder.json
```

Die `configurationRecorder.json` Datei spezifiziert `name` und `roleArn` auch die Standardaufzeichnungsfrequenz für den Konfigurationsrekorder (`recordingMode`). Sie können dieses Feld auch verwenden, um die Aufzeichnungsfrequenz für bestimmte Ressourcentypen zu überschreiben.

```
{
  "name": "default",
  "roleARN": "arn:aws:iam::123456789012:role/config-role",
  "recordingMode": {
    "recordingFrequency": CONTINUOUS or DAILY,
    "recordingModeOverrides": [
        {
            "description": "Description you provide for the override",
            "recordingFrequency": CONTINUOUS or DAILY,
            "resourceTypes": [ Comma-separated list of resource types to include in
 the override ]
        }
    ]
```

```
  }
}
```

put-configuration-recorder verwendet die folgenden Felder für den `--configuration-recorder`-Parameter:

- `name`— Der Name des Konfigurationsrekorders. AWS Config weist bei der Erstellung des Konfigurationsrekorders automatisch den Namen „Standard“ zu.
- `roleARN`— Amazon-Ressourcenname (ARN) der IAM-Rolle, die vom Konfigurationsrekorder angenommen AWS Config und von diesem verwendet wird.
- `recordingMode`— Gibt die Standardaufzeichnungsfrequenz an, mit AWS Config der Konfigurationsänderungen aufgezeichnet werden. AWS Config unterstützt kontinuierliche Aufnahme und tägliche Aufnahme. Mit der kontinuierlichen Aufzeichnung können Sie Konfigurationsänderungen kontinuierlich aufzeichnen, wenn eine Änderung auftritt. Mit der täglichen Aufzeichnung können Sie nur dann ein Konfigurationselement (CI) erhalten, das den neuesten Status Ihrer Ressourcen in den letzten 24 Stunden darstellt, wenn es sich von dem zuvor aufgezeichneten CI unterscheidet.
  - `recordingFrequency`— Die Standard-Aufnahmefrequenz, die zum Aufzeichnen von Konfigurationsänderungen AWS Config verwendet wird.

    > **Note**
    >
    > AWS Firewall Manager hängt von der kontinuierlichen Aufzeichnung ab, um Ihre Ressourcen zu überwachen. Wenn Sie den Firewall Manager verwenden, wird empfohlen, die Aufzeichnungsfrequenz auf „Kontinuierlich“ einzustellen.

  - `recordingModeOverrides` – In diesem Feld können Sie Ihre Überschreibungen für den Aufzeichnungsmodus angeben. Dies ist ein Array aus `recordingModeOverride`-Objekten. Jedes `recordingModeOverride`-Objekt im `recordingModeOverrides`-Array besteht aus drei Feldern:
    - `description` – Eine Beschreibung, die Sie für die Überschreibung angeben.
    - `recordingFrequency` – Die Aufzeichnungsfrequenz, die auf alle in der Überschreibung angegebenen Ressourcentypen angewendet wird.
    - `resourceTypes`— Eine durch Kommas getrennte Liste, die angibt, welche Ressourcentypen in der AWS Config Überschreibung enthalten sind.

> **Note**
>
> Erforderliche und optionale Felder
>
> Das `recordingMode`-Feld für `put-configuration-recorder` ist optional. Standardmäßig ist die Aufzeichnungsfrequenz für den Konfigurations-Recorder auf „Kontinuierliche Aufzeichnung“ eingestellt.

> **Note**
>
> Beschränkungen
>
> Die tägliche Aufzeichnung wird für die folgenden Ressourcentypen nicht unterstützt:
>
> - `AWS::Config::ResourceCompliance`
> - `AWS::Config::ConformancePackCompliance`
> - `AWS::Config::ConfigurationRecorder`
>
> Für die Aufzeichnungsstrategie Aufzeichnen aller derzeit und zukünftig unterstützten Ressourcentypen (`ALL_SUPPORTED_RESOURCE_TYPES`) werden diese Ressourcentypen auf „Kontinuierliche Aufzeichnung“ gesetzt.

Umbenennen des vom Kunden verwalteten Konfigurationsrekorders

Sie müssen den verwenden AWS CLI , um den vom Kunden verwalteten Konfigurationsrekorder umzubenennen. Um den Namen des vom Kunden verwalteten Konfigurationsrekorders zu ändern, müssen Sie ihn löschen und einen neuen Konfigurationsrekorder mit dem angegebenen Namen erstellen.

Umbenennen des vom Kunden verwalteten Konfigurationsrekorders mithilfe des AWS CLI

1. Verwenden Sie den `describe-configuration-recorders`Befehl, um den Namen Ihres aktuellen vom Kunden verwalteten Konfigurationsrekorders nachzuschlagen:

```
$ aws configservice describe-configuration-recorders
{
```

```
    "ConfigurationRecorders": [
        {
            "roleARN": "arn:aws:iam::012345678912:role/myConfigRole",
            "name": "default"
        }
    ]
}
```

2. Verwenden Sie den `delete-configuration-recorder`Befehl, um Ihren vom Kunden verwalteten Recorder für die aktuelle Konfiguration zu löschen:

```
$ aws configservice delete-configuration-recorder --configuration-recorder-
name default
```

3. Verwenden Sie den `put-configuration-recorder`Befehl, um einen vom Kunden verwalteten Konfigurationsrekorder mit dem neuen Namen zu erstellen:

```
$ aws configservice put-configuration-recorder --configuration-recorder
 name=configRecorderName,roleARN=arn:aws:iam::012345678912:role/myConfigRole
```

4. Verwenden Sie den Befehl „`start-configuration-recorder`“, um die Aufzeichnung fortzusetzen:

```
$ aws configservice start-configuration-recorder --configuration-recorder-
name configRecorderName
```

Ihre Konfigurationsrekorder anzeigen

Sie können die AWS Config Konsole verwenden oder die Details zu Ihren Konfigurationsrekordern AWS CLI anzeigen.

To view your configuration recorders (Console)

1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die AWS Config Konsole zu https://console.aws.amazon.com/config/Hause.
2. Wählen Sie im Navigationsbereich Settings (Einstellungen) aus.
3. Für den vom Kunden verwalteten Konfigurationsrekorder können Sie die Details auf der Registerkarte Kundenverwalteter Rekorder einsehen.

4. Wählen Sie für serviceverknüpfte Konfigurationsrekorder auf der Registerkarte Serviceverknüpfte Konfigurationsrekorder einen serviceverknüpften Konfigurationsrekorder aus und klicken Sie dann auf Anzeigen.

To view your configuration recorders (CLI)

Verwenden Sie den `describe-configuration-recorders`Befehl, um Details zu Ihren Konfigurationsrekordern anzuzeigen:

```
$ aws configservice describe-configuration-recorders
{
    "ConfigurationRecorders": [
        {
            "roleARN": "arn:aws:iam::012345678912:role/myConfigRole",
            "name": "default"
        }
    ]
}
```

Verwenden Sie den `describe-configuration-recorder-status`Befehl, um den aktuellen Status Ihrer Konfigurationsrekorder anzuzeigen:

```
$ aws configservice describe-configuration-recorder-status
{
    "ConfigurationRecordersStatus": [
        {
            "name": "default",
            "lastStatus": "SUCCESS",
            "lastStopTime": 1414511624.914,
            "lastStartTime": 1414708460.276,
            "recording": true,
            "lastStatusChangeTime": 1414816537.148,
            "lastErrorMessage": "NA",
            "lastErrorCode": "400"
        }
    ]
}
```

Für diese beiden Befehle können Sie die `configuration-recorder-names` Felder `arn` und verwenden, um eine Liste von Konfigurationsrekordern anzugeben. Bei serviceverknüpften

Konfigurationsrekordern können Sie das `service-principal` Feld verwenden, um einen Konfigurationsrekorder anzugeben.

Wenn kein Konfigurationsrekorder angegeben ist, gibt dieser Befehl die Details aller Konfigurationsrekorder zurück, die dem Konto zugeordnet sind.

Löschen Ihrer Konfigurationsrekorder

Sie müssen den verwenden AWS CLI , um den vom Kunden verwalteten Konfigurationsrekorder zu löschen. Sie können die AWS Config Konsole oder den verwenden AWS CLI , um einen mit einem Dienst verknüpften Konfigurationsrekorder zu löschen.

To delete the customer managed configuration recorder (CLI)

Verwenden Sie den -Befehl:`delete-configuration-recorder`

```
$ aws configservice delete-configuration-recorder --configuration-recorder-
name default
```

To delete a service-linked configuration recorder (Console)

1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die AWS Config Konsole zu https://console.aws.amazon.com/config/Hause.
2. Wählen Sie im Navigationsbereich Settings (Einstellungen) aus.
3. Wählen Sie auf der Registerkarte Serviceverknüpfte Rekorder auf der Registerkarte Serviceverknüpfte Rekorder eine serviceverknüpfte Konfiguration aus, und klicken Sie dann auf Löschen. Wählen Sie bei Aufforderung Löschen.

To delete a service-linked configuration recorder (CLI)

Verwenden Sie den -Befehl:`delete-service-linked-configuration-recorder`

Dieser Befehl verwendet das Feld. `--service-principal`

```
$ aws configservice delete-service-linked-configuration-recorder --service-principal
 "The service principal of the AWS-Service for the service-linked configuration
 recorder that you want to delete"
```

Mit dem Delivery Channel arbeiten

Da AWS Config kontinuierlich die Änderungen an Ihren AWS Ressourcen aufgezeichnet werden, werden Benachrichtigungen und aktualisierte Konfigurationsstatus über den Bereitstellungskanal gesendet. Sie können den Bereitstellungskanal verwalten, um zu kontrollieren, wohin Konfigurationsupdates AWS Config gesendet werden.

Themen

- Überlegungen
- Terminologie
- Komponenten eines Konfigurationselements
- Den Lieferkanal anzeigen
- Aktualisieren des Übermittlungskanals
- Umbenennen des Übermittlungskanals
- Bereitstellung von Konfigurations-Snapshots an einen Amazon S3 S3-Bucket
- Überprüfen des Übermittlungsstatus
- Konfigurations-Snapshots im Amazon S3 S3-Bucket anzeigen
- Beispiel für einen Konfigurations-Snapshot von AWS Config
- Benachrichtigungen, die AWS Config an ein Amazon SNS SNS-Thema gesendet werden

Überlegungen

Ein Lieferkanal pro Region und Konto

Sie können nur einen Lieferkanal pro AWS Region und Region pro Region haben AWS-Konto, und der Lieferkanal muss verwendet AWS Config werden.

Benachrichtigungen über übergroße Konfigurationselemente enthalten eine kurze Zusammenfassung

Wenn eine Konfigurationsänderung für eine Ressource AWS Config erkannt wird und die Benachrichtigung die von Amazon SNS zulässige maximale Größe überschreitet, enthält die Benachrichtigung eine kurze Zusammenfassung des Konfigurationselements. Sie können sich die vollständige Benachrichtigung an dem im Feld `s3BucketLocation` angegebenen Amazon S3-Bucket-Speicherort ansehen. Weitere Informationen finden Sie im Beispiel einer Benachrichtigung über die Änderung eines übergroßen Konfigurationselements.

AWS Config unterstützt die AWS KMS Verschlüsselung für Amazon S3 S3-Buckets, die von verwendet werden AWS Config

Sie können einen AWS Key Management Service (AWS KMS) -Schlüssel oder Alias Amazon Resource Name (ARN) angeben, um die an Ihren Amazon Simple Storage Service (Amazon S3) -Bucket übermittelten Daten zu verschlüsseln. Überträgt standardmäßig den AWS Config Konfigurationsverlauf und Snapshot-Dateien an Ihren Amazon S3 S3-Bucket und verschlüsselt die ruhenden Daten mit der serverseitigen S3 AES-256-Verschlüsselung, SSE-S3. Wenn Sie jedoch Ihren KMS-Schlüssel oder Alias-ARN angeben AWS Config , wird dieser KMS-Schlüssel anstelle der AES-256-Verschlüsselung AWS Config verwendet.

AWS Config unterstützt nicht den Lieferkanal zu einem Amazon S3 S3-Bucket, bei dem die Objektsperre aktiviert ist und die Standardspeicherung aktiviert ist. Weitere Informationen finden Sie unter Funktionsweise von S3-Objektsperre.

Terminologie

Ein Konfigurationselement stellt eine point-in-time Ansicht der verschiedenen Attribute einer unterstützten AWS Ressource dar, die in Ihrem Konto vorhanden ist. Zu den Komponenten eines Konfigurationselements gehören Metadaten, Attribute, Beziehungen, die aktuelle Konfiguration und verwandte Ereignisse. AWS Config erstellt ein Konfigurationselement, wenn es eine Änderung an einem Ressourcentyp erkennt, den es aufzeichnet. Wenn beispielsweise Amazon S3 S3-Buckets aufgezeichnet werden, AWS Config wird jedes Mal, wenn ein Bucket AWS Config erstellt, aktualisiert oder gelöscht wird, ein Konfigurationselement erstellt. Sie können auch auswählen AWS Config , ob ein Konfigurationselement mit der von Ihnen festgelegten Aufzeichnungsfrequenz erstellt werden soll.

Ein Konfigurationsverlauf ist die Sammlung der Konfigurationselemente für eine bestimmte Ressource über einen beliebigen Zeitraum. Ein Konfigurationsverlauf kann Ihnen bei der Beantwortung von Fragen helfen: z. B. wann die Ressource erstmalig erstellt wurde, wie die Ressource im letzten Monat konfiguriert wurde und welche Konfigurationsänderungen gestern um 9.00 Uhr eingeführt wurden. Der Konfigurationsverlauf steht Ihnen in verschiedenen Formaten zur Verfügung. AWS Config liefert automatisch eine Konfigurationsverlaufsdatei für jeden Ressourcentyp, der in einem von Ihnen angegebenen Amazon S3 S3-Bucket aufgezeichnet wird. Sie können eine bestimmte Ressource in der AWS Config Konsole auswählen und mithilfe der Zeitleiste zu allen vorherigen Konfigurationselementen für diese Ressource navigieren. Zusätzlich können Sie über die API auf historische Konfigurationselemente für eine Ressource zugreifen.

Ein Konfigurations-Snapshot ist eine Sammlung der Konfigurationselemente der unterstützten Ressourcen in Ihrem Konto. Dieser Konfigurations-Snapshot liefert ein vollständiges Bild der derzeit

aufgezeichneten Ressourcen und deren Konfigurationen. Die Konfigurations-Snapshot ist ein nützliches Tool für die Validierung Ihrer Konfiguration. Sie können beispielsweise den Konfigurations-Snapshot regelmäßig auf falsch konfigurierte Ressourcen oder solche, die potentiell nicht vorhanden sein sollten, hin prüfen. Der Konfigurations-Snapshot ist in mehreren Formaten verfügbar. Der Konfigurations-Snapshot kann an einen von Ihnen angegebenen Amazon Simple Storage Service (Amazon S3)-Bucket übermittelt werden. Darüber hinaus können Sie in der AWS Config Konsole einen Zeitpunkt auswählen und mithilfe der Beziehungen zwischen den Ressourcen durch den Snapshot der Konfigurationselemente navigieren.

Ein Konfigurationsstream ist eine automatisch aktualisierte Liste aller Konfigurationselemente für die Ressourcen, AWS Config die aufgezeichnet werden. Bei jeder Erstellung, Änderung oder Löschung einer Ressource wird von AWS Config ein neues Konfigurationselement erstellt und dem Konfigurations-Stream hinzugefügt. Der Konfigurationsstream verwendet ein Amazon Simple Notification Service (Amazon SNS)-Thema Ihrer Wahl. Der Konfigurationsstream ist hilfreich, um Konfigurationsänderungen sofort zu beobachten, sodass Sie potenzielle Probleme erkennen können, Benachrichtigungen zu generieren, wenn bestimmte Ressourcen geändert werden, oder externe Systeme zu aktualisieren, die die Konfiguration Ihrer AWS Ressourcen widerspiegeln müssen.

Komponenten eines Konfigurationselements

Ein Konfigurationselement stellt eine point-in-time Ansicht der verschiedenen Attribute einer unterstützten AWS Ressource dar, die in Ihrem Konto vorhanden ist. Zu den Komponenten eines Konfigurationselements gehören Metadaten, Attribute, Beziehungen, die aktuelle Konfiguration und verwandte Ereignisse. AWS Config erstellt ein Konfigurationselement, wenn es eine Änderung an einem Ressourcentyp erkennt, den es aufzeichnet. Wenn beispielsweise Amazon S3 S3-Buckets aufgezeichnet werden, AWS Config wird jedes Mal, wenn ein Bucket AWS Config erstellt, aktualisiert oder gelöscht wird, ein Konfigurationselement erstellt. Sie können auch auswählen AWS Config , ob ein Konfigurationselement mit der von Ihnen festgelegten Aufzeichnungsfrequenz erstellt werden soll.

Ein Konfigurationselement besteht aus den folgenden Komponenten.

Komponente	Beschreibung	Enthält
Metadaten	Informationen zu diesem Konfigurationselement	• Versions-ID • Erfassungszeitpunkt der Konfigura tionselemente

Komponente	Beschreibung	Enthält
		• Status des Konfigurationselements, der angibt, ob das Element erfolgreich erfasst wurde • Status-ID, die die Reihenfolge der Konfigurationselemente einer Ressource angibt
Attribute	Ressourcenattribute	• Ressourcen-ID • Liste der key-value-Tags für diese Ressource • Ressourcentyp (siehe Unterstützte Ressourcentypen für AWS Config) • Amazon-Ressourcenname (ARN) • Availability Zone mit dieser Ressource, sofern zutreffend • Uhrzeit der Ressourcenerstellung
Beziehungen	Der Zusammenhang der Ressource mit anderen dem Konto zugewiesenen Ressourcen	Beschreibung der Beziehung, z. B. das Amazon EBS-Volume `vol-1234567` ist an eine EC2 Amazon-Instance angehängt `i-a1b2c3d4`

Komponente	Beschreibung	Enthält
Aktuelle Konfiguration	Die über einen Aufruf des "Describe"- oder "List"-API der Ressource zurückgegebenen Informationen	Beispielsweise gibt die `DescribeVolumes` -API die folgenden Informationen über das Volume zurück: • Availability Zone, in der sich das Volume befindet • Zeitpunkt, zu dem das Volume angefügt wurde • ID der EC2 Instance, an die es angehängt ist • Aktueller Status des Volumes • Staat der DeleteOnTermination Flagge • Gerät, dem das Volume angefügt ist • Volume-Typ, z. B. `gp2`, `io1`, oder `standard`

Hinweise

1. Die Beziehung eines Konfigurationselements schließt keine Netzwerkfluss- oder Datenflussabhängigkeiten ein. Konfigurationselemente können nicht zur Darstellung Ihrer Anwendungsarchitektur angepasst werden.
2. Ab Version 1.3 ist das Feld "relatedEvents" leer. Sie können in der LookupEvents API-Referenz auf die AWS CloudTrail API zugreifen, um die Ereignisse für die Ressource abzurufen.
3. Ab Version 1.3 ist das Feld ConfigurationItem MD5 Hash leer. Sie können das configurationStateId Feld verwenden, um sicherzustellen, dass Sie über das neueste Konfigurationselement verfügen.
4. Wenn ein Ressourcentyp kein Tagging unterstützt oder keine Tag-Informationen in seiner Describe-API-Antwort enthält, AWS Config werden keine Tag-Daten in den Konfigurationselementen (CIs) für diesen Ressourcentyp erfasst. AWS Config zeichnet diese Ressourcen trotzdem auf. Funktionen, die auf Tag-Daten basieren, funktionieren jedoch nicht. Dies wirkt sich auf Tag-basierte Filterung, Gruppierung oder Konformitätsbewertung aus, die auf Tag-Daten basiert.

Den Lieferkanal anzeigen

Sie müssen den verwenden AWS CLI , um Details zum Bereitstellungskanal anzuzeigen.

Die folgenden Code-Beispiele zeigen, wie `DescribeDeliveryChannels` verwendet wird.

CLI

AWS CLI

Um Details zum Lieferkanal zu erhalten

Der folgende Befehl gibt Details zum Lieferkanal zurück:

```
aws configservice describe-delivery-channels
```

Ausgabe:

```
{
    "DeliveryChannels": [
        {
            "snsTopicARN": "arn:aws:sns:us-east-1:123456789012:config-topic",
            "name": "default",
            "s3BucketName": "config-bucket-123456789012"
        }
    ]
}
```

- Einzelheiten zur API finden Sie DescribeDeliveryChannelsin der AWS CLI Befehlsreferenz.

PowerShell

Tools für PowerShell V4

Beispiel 1: In diesem Beispiel wird der Lieferkanal für die Region abgerufen und Details angezeigt.

```
Get-CFGDeliveryChannel -Region eu-west-1 | Select-Object Name, S3BucketName,
 S3KeyPrefix,
 @{N="DeliveryFrequency";E={$_.ConfigSnapshotDeliveryProperties.DeliveryFrequency}}
```

Ausgabe:

```
Name    S3BucketName               S3KeyPrefix DeliveryFrequency
----    ------------               ----------- -----------------
default config-bucket-NA my          TwentyFour_Hours
```

- Einzelheiten zur API finden Sie unter DescribeDeliveryChannels AWS -Tools für PowerShellCmdlet-Referenz (V4).

Aktualisieren des Übermittlungskanals

Beim Aktualisieren des Übermittlungskanals können Sie die folgenden Optionen festlegen:

- Der Amazon S3 S3-Bucket, in AWS Config den Konfigurations-Snapshots und Konfigurationsverlaufsdateien gesendet werden.
- Wie oft werden AWS Config Konfigurations-Snapshots an Ihren Amazon S3 S3-Bucket gesendet?
- Das Amazon SNS SNS-Thema, an das Benachrichtigungen über Konfigurationsänderungen AWS Config gesendet werden.

Um den Lieferkanal zu aktualisieren (Konsole)

Sie können die AWS Config Konsole verwenden, um den Amazon S3-Bucket und das Amazon SNS SNS-Thema für Ihren Lieferkanal festzulegen. Die Schritte zum Verwalten dieser Einstellungen finden Sie unter Einrichtung AWS Config mit der Konsole.

Die Konsole bietet keine Optionen zum Umbenennen des Übermittlungskanals, zum Festlegen der Häufigkeit für die Konfiguration von Snapshots oder zum Löschen des Übermittlungskanals. Um diese Aufgaben zu erledigen, müssen Sie die AWS CLI, die AWS Config API oder eine der AWS SDKs verwenden.

So aktualisieren Sie den Übermittlungskanal (AWS SDKs)

Die folgenden Code-Beispiele zeigen, wie `PutDeliveryChannel` verwendet wird.

CLI

AWS CLI

Um einen Lieferkanal zu erstellen

Der folgende Befehl stellt die Einstellungen für den Lieferkanal als JSON-Code bereit:

```
aws configservice put-delivery-channel --delivery-channel file://
deliveryChannel.json
```

Die `deliveryChannel.json` Datei spezifiziert die Attribute des Lieferkanals:

```
{
    "name": "default",
    "s3BucketName": "config-bucket-123456789012",
    "snsTopicARN": "arn:aws:sns:us-east-1:123456789012:config-topic",
    "configSnapshotDeliveryProperties": {
        "deliveryFrequency": "Twelve_Hours"
    }
}
```

In diesem Beispiel werden die folgenden Attribute festgelegt:

`name`- Der Name des Lieferkanals. Standardmäßig weist AWS Config den Namen einem neuen Lieferkanal `default` zu. Sie können den Namen des Lieferkanals nicht mit dem Befehl aktualisieren. `put-delivery-channel` Die Schritte zum Ändern des Namens finden Sie unter Umbenennen des Lieferkanals. `s3BucketName` - Der Name des Amazon S3 S3-Buckets, für den AWS Config Konfigurations-Snapshots und Konfigurationsverlaufsdateien bereitstellt. Wenn Sie einen Bucket angeben, der zu einem anderen AWS Konto gehört, muss dieser Bucket über Richtlinien verfügen, die Config Zugriffsberechtigungen gewähren. AWS Weitere Informationen finden Sie unter Berechtigungen für den Amazon-S3-Bucket.

`snsTopicARN`— Der Amazon-Ressourcenname (ARN) des Amazon SNS-Themas, an das AWS Config Benachrichtigungen über Konfigurationsänderungen sendet. Wenn Sie ein Thema aus einem anderen Konto auswählen, muss das Thema über Richtlinien verfügen, die Config Zugriffsberechtigungen gewähren. AWS Weitere Informationen finden Sie unter Berechtigungen für das Amazon SNS SNS-Thema.

`configSnapshotDeliveryProperties`- Enthält das `deliveryFrequency` Attribut, das festlegt, wie oft AWS Config Konfigurations-Snapshots liefert und wie oft es Evaluierungen für periodische Config-Regeln aufruft.

Wenn der Befehl erfolgreich ist, gibt AWS Config keine Ausgabe zurück. Führen Sie den describe-delivery-channels Befehl aus, um die Einstellungen Ihres Lieferkanals zu überprüfen.

- Einzelheiten zur API finden Sie PutDeliveryChannelin der AWS CLI Befehlsreferenz.

PowerShell

Tools für PowerShell V4

Beispiel 1: In diesem Beispiel wird die DeliveryFrequency-Eigenschaft eines vorhandenen Lieferkanals geändert.

```
Write-CFGDeliveryChannel -ConfigSnapshotDeliveryProperties_DeliveryFrequency
 TwentyFour_Hours -DeliveryChannelName default -DeliveryChannel_S3BucketName
 amzn-s3-demo-bucket -DeliveryChannel_S3KeyPrefix my
```

- Einzelheiten zur API finden Sie unter PutDeliveryChannel AWS -Tools für PowerShellCmdlet-Referenz (V4).

(Optional) Sie können den `describe-delivery-channels`-Befehl verwenden, um zu überprüfen, ob die Einstellungen für den Übermittlungskanal werden:

```
$ aws configservice describe-delivery-channels
{
    "DeliveryChannels": [
        {
            "configSnapshotDeliveryProperties": {
                "deliveryFrequency": "Twelve_Hours"
            },
            "snsTopicARN": "arn:aws:sns:us-east-2:123456789012:config-topic",
            "name": "default",
            "s3BucketName": "config-bucket-123456789012"
        }
    ]
}
```

Die folgenden Code-Beispiele zeigen, wie `DescribeDeliveryChannels` verwendet wird.

CLI

AWS CLI

Um Details zum Lieferkanal zu erhalten

Der folgende Befehl gibt Details zum Lieferkanal zurück:

```
aws configservice describe-delivery-channels
```

Ausgabe:

```
{
    "DeliveryChannels": [
        {
            "snsTopicARN": "arn:aws:sns:us-east-1:123456789012:config-topic",
            "name": "default",
            "s3BucketName": "config-bucket-123456789012"
        }
    ]
}
```

- Einzelheiten zur API finden Sie DescribeDeliveryChannelsin der AWS CLI Befehlsreferenz.

PowerShell

Tools für PowerShell V4

Beispiel 1: In diesem Beispiel wird der Lieferkanal für die Region abgerufen und Details angezeigt.

```
Get-CFGDeliveryChannel -Region eu-west-1 | Select-Object Name, S3BucketName,
 S3KeyPrefix,
 @{N="DeliveryFrequency";E={$_.ConfigSnapshotDeliveryProperties.DeliveryFrequency}}
```

Ausgabe:

```
Name    S3BucketName               S3KeyPrefix DeliveryFrequency
----    ------------               ----------- -----------------
default config-bucket-NA my          TwentyFour_Hours
```

- Einzelheiten zur API finden Sie unter DescribeDeliveryChannels AWS -Tools für PowerShellCmdlet-Referenz (V4).

Umbenennen des Übermittlungskanals

Um den Namen des Lieferkanals zu ändern, müssen Sie ihn löschen und einen neuen Lieferkanal mit dem von Ihnen angegebenen Namen erstellen. Bevor Sie den Übermittlungskanal löschen können, müssen Sie den Configuration Recorder vorübergehend beenden. Die AWS Config Konsole bietet keine Option zum Löschen des Bereitstellungskanals. Sie müssen die AWS CLI, die AWS Config API oder eine der folgenden verwenden AWS SDKs.

Umbenennen des Lieferkanals mithilfe der AWS CLI

1. Verwenden Sie den `stop-configuration-recorder`-Befehl, um den Configuration Recorder zu beenden:

```
$ aws configservice stop-configuration-recorder --configuration-recorder-
name configRecorderName
```

2. Verwenden Sie den `describe-delivery-channels`-Befehl und notieren Sie sich die Attribute des Übermittlungskanals:

```
$ aws configservice describe-delivery-channels
{
    "DeliveryChannels": [
        {
            "configSnapshotDeliveryProperties": {
                "deliveryFrequency": "Twelve_Hours"
            },
            "snsTopicARN": "arn:aws:sns:us-east-2:123456789012:config-topic",
            "name": "default",
            "s3BucketName": "config-bucket-123456789012"
        }
    ]
}
```

3. Verwenden Sie den `delete-delivery-channel`-Befehl zum Löschen des Übermittlungskanals:

```
$ aws configservice delete-delivery-channel --delivery-channel-name default
```

4. Verwenden Sie den `put-delivery-channel`-Befehl zum Erstellen eines Übermittlungskanals mit dem gewünschten Namen:

```
$ aws configservice put-delivery-channel --delivery-channel file://
deliveryChannel.json
```

Die Datei „deliveryChannel.json” gibt die Attribute des Übermittlungskanals an:

```
{
    "name": "myCustomDeliveryChannelName",
    "s3BucketName": "config-bucket-123456789012",
    "snsTopicARN": "arn:aws:sns:us-east-2:123456789012:config-topic",
    "configSnapshotDeliveryProperties": {
        "deliveryFrequency": "Twelve_Hours"
    }
}
```

5. Verwenden Sie den Befehl „`start-configuration-recorder`“, um die Aufzeichnung fortzusetzen:

```
$ aws configservice start-configuration-recorder --configuration-recorder-
name configRecorderName
```

Bereitstellung von Konfigurations-Snapshots an einen Amazon S3 S3-Bucket

Ein Konfigurations-Snapshot ist eine Sammlung der Konfigurationselemente der unterstützten Ressourcen in Ihrem Konto. Dieser Konfigurations-Snapshot liefert ein vollständiges Bild der derzeit aufgezeichneten Ressourcen und deren Konfigurationen. Die Konfigurations-Snapshot ist ein nützliches Tool für die Validierung Ihrer Konfiguration. Sie können beispielsweise den Konfigurations-Snapshot regelmäßig auf falsch konfigurierte Ressourcen oder solche, die potentiell nicht vorhanden sein sollten, hin prüfen. Der Konfigurations-Snapshot ist in mehreren Formaten verfügbar. Der Konfigurations-Snapshot kann an einen von Ihnen angegebenen Amazon Simple Storage Service (Amazon S3)-Bucket übermittelt werden. Darüber hinaus können Sie in der AWS Config Konsole einen Zeitpunkt auswählen und mithilfe der Beziehungen zwischen den Ressourcen durch den Snapshot der Konfigurationselemente navigieren.

Bereitstellung von Konfigurations-Snapshots

AWS Config generiert Konfigurationsschnappschüsse, wenn Sie die DeliverConfigSnapshotAktion aufrufen oder den AWS CLI `deliver-config-snapshot` Befehl ausführen. AWS Config speichert Konfigurations-Snapshots im Amazon S3 S3-Bucket, den Sie bei der Aktivierung AWS Config angegeben haben.

Geben Sie den `deliver-config-snapshot`Befehl ein, indem Sie den Namen angeben, den Sie AWS Config bei der Konfiguration Ihres Lieferkanals zugewiesen haben, zum Beispiel:

```
$ aws configservice deliver-config-snapshot --delivery-channel-name default
{
    "configSnapshotId": "94ccff53-83be-42d9-996f-b4624b3c1a55"
}
```

Überprüfen des Übermittlungsstatus

Geben Sie den `describe-delivery-channel-status`Befehl ein, um zu überprüfen, ob mit der Bereitstellung der Konfigurationen an den angegebenen Lieferkanal begonnen wurde: AWS Config

```
aws configservice describe-delivery-channel-status
```

In der Antwort wird der Status aller drei Bereitstellungsformate aufgeführt, die für die Bereitstellung von Konfigurationen für Ihren Bereich und Ihr Thema AWS Config verwendet werden.

```
{
    "DeliveryChannelsStatus": [
        {
            "configStreamDeliveryInfo": {
                "lastStatusChangeTime": 1415138614.125,
                "lastStatus": "SUCCESS"
            },
            "configHistoryDeliveryInfo": {
                "lastSuccessfulTime": 1415148744.267,
                "lastStatus": "SUCCESS",
                "lastAttemptTime": 1415148744.267
            },
            "configSnapshotDeliveryInfo": {
                "lastSuccessfulTime": 1415333113.4159999,
                "lastStatus": "SUCCESS",
                "lastAttemptTime": 1415333113.4159999
```

```
            },
            "name": "default"
        }
    ]
}
```

Sehen Sie sich das `lastSuccessfulTime` Feld in an`configSnapshotDeliveryInfo`. Die Uhrzeit sollte mit der Uhrzeit der letzten Anforderung der Übermittlung des Konfigurations-Snapshots übereinstimmen.

> **Note**
>
> AWS Config verwendet das UTC-Format (Coordinated Universal Time), um die Uhrzeit aufzuzeichnen.

Konfigurations-Snapshots im Amazon S3 S3-Bucket anzeigen

Ein Konfigurations-Snapshot ist eine Sammlung der Konfigurationselemente der unterstützten Ressourcen in Ihrem Konto. Dieser Konfigurations-Snapshot liefert ein vollständiges Bild der derzeit aufgezeichneten Ressourcen und deren Konfigurationen. Die Konfigurations-Snapshot ist ein nützliches Tool für die Validierung Ihrer Konfiguration. Sie können beispielsweise den Konfigurations-Snapshot regelmäßig auf falsch konfigurierte Ressourcen oder solche, die potentiell nicht vorhanden sein sollten, hin prüfen. Der Konfigurations-Snapshot ist in mehreren Formaten verfügbar. Der Konfigurations-Snapshot kann an einen von Ihnen angegebenen Amazon Simple Storage Service (Amazon S3)-Bucket übermittelt werden. Darüber hinaus können Sie in der AWS Config Konsole einen Zeitpunkt auswählen und mithilfe der Beziehungen zwischen den Ressourcen durch den Snapshot der Konfigurationselemente navigieren.

Konfigurations-Snapshots anzeigen

1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die Amazon S3 S3-Konsole unter https://console.aws.amazon.com/s3/.
2. Wählen Sie in der Liste „Alle Buckets“ der Amazon S3 S3-Konsole den Namen Ihres Amazon S3 S3-Buckets aus.
3. Gehen Sie die verschachtelten Ordner in Ihrem Bucket durch, bis Sie das `ConfigSnapshot` Objekt mit einer Snapshot-ID sehen, die mit der vom Befehl zurückgegebenen ID übereinstimmt. Laden Sie das Objekt herunter und öffnen Sie es, um den Konfigurations-Snapshot anzuzeigen.

Der S3-Bucket enthält auch eine leere Datei mit dem Namen`ConfigWritabilityCheckFile`. AWS Config erstellt diese Datei, um zu überprüfen, ob der Dienst erfolgreich in den S3-Bucket schreiben kann.

Beispiel für einen Konfigurations-Snapshot von AWS Config

Im Folgenden finden Sie ein Beispiel für die Informationen, die in einem Konfigurations-Snapshot AWS Config enthalten sind. Der Snapshot beschreibt die Konfiguration der Ressourcen, die AWS Config in der aktuellen Region für Sie aufgezeichnet werden AWS-Konto, und er beschreibt die Beziehungen zwischen diesen Ressourcen.

> **Note**
>
> Der Konfigurations-Snapshot kann Verweise auf Ressourcentypen und Ressourcen enthaltenIDs , die nicht unterstützt werden.

```
{
    "fileVersion": "1.0",
    "requestId": "asudf8ow-4e34-4f32-afeb-0ace5bf3trye",
    "configurationItems": [
        {
            "configurationItemVersion": "1.0",
            "resourceId": "vol-ce676ccc",
            "arn": "arn:aws:us-west-2b:123456789012:volume/vol-ce676ccc",
            "accountId": "12345678910",
            "configurationItemCaptureTime": "2014-03-07T23:47:08.918Z",
            "configurationStateID": "3e660fdf-4e34-4f32-afeb-0ace5bf3d63a",
            "configurationItemStatus": "OK",
            "relatedEvents": [
                "06c12a39-eb35-11de-ae07-adb69edbb1e4",
                "c376e30d-71a2-4694-89b7-a5a04ad92281"
            ],
            "availibilityZone": "us-west-2b",
            "resourceType": "AWS::EC2::Volume",
            "resourceCreationTime": "2014-02-27T21:43:53.885Z",
            "tags": {},
            "relationships": [
                {
                    "resourceId": "i-344c463d",
```

```
                "resourceType": "AWS::EC2::Instance",
                "name": "Attached to Instance"
            }
        ],
        "configuration": {
            "volumeId": "vol-ce676ccc",
            "size": 1,
            "snapshotId": "",
            "availabilityZone": "us-west-2b",
            "state": "in-use",
            "createTime": "2014-02-27T21:43:53.0885+0000",
            "attachments": [
                {
                    "volumeId": "vol-ce676ccc",
                    "instanceId": "i-344c463d",
                    "device": "/dev/sdf",
                    "state": "attached",
                    "attachTime": "2014-03-07T23:46:28.0000+0000",
                    "deleteOnTermination": false
                }
            ],
            "tags": [
                {
                    "tagName": "environment",
                    "tagValue": "PROD"
                },
                {
                    "tagName": "name",
                    "tagValue": "DataVolume1"
                }
            ],
            "volumeType": "standard"
        }
    },
    {
        "configurationItemVersion": "1.0",
        "resourceId": "i-344c463d",
        "accountId": "12345678910",
        "arn": "arn:aws:ec2:us-west-2b:123456789012:instance/i-344c463d",
        "configurationItemCaptureTime": "2014-03-07T23:47:09.523Z",
        "configurationStateID": "cdb571fa-ce7a-4ec5-8914-0320466a355e",
        "configurationItemStatus": "OK",
        "relatedEvents": [
            "06c12a39-eb35-11de-ae07-adb69edbb1e4",
```

```
                "c376e30d-71a2-4694-89b7-a5a04ad92281"
            ],
            "availibilityZone": "us-west-2b",
            "resourceType": "AWS::EC2::Instance",
            "resourceCreationTime": "2014-02-26T22:56:35.000Z",
            "tags": {
                "Name": "integ-test-1",
                "examplename": "examplevalue"
            },
            "relationships": [
                {
                    "resourceId": "vol-ce676ccc",
                    "resourceType": "AWS::EC2::Volume",
                    "name": "Attached Volume"
                },
                {
                    "resourceId": "vol-ef0e06ed",
                    "resourceType": "AWS::EC2::Volume",
                    "name": "Attached Volume",
                    "direction": "OUT"
                },
                {
                    "resourceId": "subnet-47b4cf2c",
                    "resourceType": "AWS::EC2::SUBNET",
                    "name": "Is contained in Subnet",
                    "direction": "IN"
                }
            ],
            "configuration": {
                "instanceId": "i-344c463d",
                "imageId": "ami-ccf297fc",
                "state": {
                    "code": 16,
                    "name": "running"
                },
                "privateDnsName": "ip-172-31-21-63.us-west-2.compute.internal",
                "publicDnsName": "ec2-54-218-4-189.us-west-2.compute.amazonaws.com",
                "stateTransitionReason": "",
                "keyName": "configDemo",
                "amiLaunchIndex": 0,
                "productCodes": [],
                "instanceType": "t1.micro",
                "launchTime": "2014-02-26T22:56:35.0000+0000",
                "placement": {
```

```
                "availabilityZone": "us-west-2b",
                "groupName": "",
                "tenancy": "default"
            },
            "kernelId": "aki-fc8f11cc",
            "monitoring": {
                "state": "disabled"
            },
            "subnetId": "subnet-47b4cf2c",
            "vpcId": "vpc-41b4cf2a",
            "privateIpAddress": "172.31.21.63",
            "publicIpAddress": "54.218.4.189",
            "architecture": "x86_64",
            "rootDeviceType": "ebs",
            "rootDeviceName": "/dev/sda1",
            "blockDeviceMappings": [
                {
                    "deviceName": "/dev/sda1",
                    "ebs": {
                        "volumeId": "vol-ef0e06ed",
                        "status": "attached",
                        "attachTime": "2014-02-26T22:56:38.0000+0000",
                        "deleteOnTermination": true
                    }
                },
                {
                    "deviceName": "/dev/sdf",
                    "ebs": {
                        "volumeId": "vol-ce676ccc",
                        "status": "attached",
                        "attachTime": "2014-03-07T23:46:28.0000+0000",
                        "deleteOnTermination": false
                    }
                }
            ],
            "virtualizationType": "paravirtual",
            "clientToken": "aBCDe123456",
            "tags": [
                {
                    "key": "Name",
                    "value": "integ-test-1"
                },
                {
                    "key": "examplekey",
```

```
                        "value": "examplevalue"
                    }
                ],
                "securityGroups": [
                    {
                        "groupName": "launch-wizard-2",
                        "groupId": "sg-892adfec"
                    }
                ],
                "sourceDestCheck": true,
                "hypervisor": "xen",
                "networkInterfaces": [
                    {
                        "networkInterfaceId": "eni-55c03d22",
                        "subnetId": "subnet-47b4cf2c",
                        "vpcId": "vpc-41b4cf2a",
                        "description": "",
                        "ownerId": "12345678910",
                        "status": "in-use",
                        "privateIpAddress": "172.31.21.63",
                        "privateDnsName": "ip-172-31-21-63.us-west-2.compute.internal",
                        "sourceDestCheck": true,
                        "groups": [
                            {
                                "groupName": "launch-wizard-2",
                                "groupId": "sg-892adfec"
                            }
                        ],
                        "attachment": {
                            "attachmentId": "eni-attach-bf90c489",
                            "deviceIndex": 0,
                            "status": "attached",
                            "attachTime": "2014-02-26T22:56:35.0000+0000",
                            "deleteOnTermination": true
                        },
                        "association": {
                            "publicIp": "54.218.4.189",
                            "publicDnsName": "ec2-54-218-4-189.us-
west-2.compute.amazonaws.com",
                            "ipOwnerId": "amazon"
                        },
                        "privateIpAddresses": [
                            {
                                "privateIpAddress": "172.31.21.63",
```

```
                                "privateDnsName": "ip-172-31-21-63.us-
west-2.compute.internal",
                                "primary": true,
                                "association": {
                                    "publicIp": "54.218.4.189",
                                    "publicDnsName": "ec2-54-218-4-189.us-
west-2.compute.amazonaws.com",
                                    "ipOwnerId": "amazon"
                                }
                            }
                        ]
                    }
                ],
                "ebsOptimized": false
            }
        }
    ]
}
```

Im nächsten Schritt überprüfen Sie, ob der Konfigurations-Snapshot dem Übermittlungskanal erfolgreich übermittelt wurde.

Benachrichtigungen, die AWS Config an ein Amazon SNS SNS-Thema gesendet werden

> **Note**
>
> Bevor AWS Config Sie Benachrichtigungen an ein Amazon SNS SNS-Thema senden können, müssen Sie zuerst den Konfigurationsrekorder und den Zustellungskanal einrichten. Weitere Informationen finden Sie unter Verwalten vom Configuration Recorder und Verwalten des Übermittlungskanals.

Sie können konfigurieren AWS Config , dass Konfigurationsänderungen und Benachrichtigungen zu einem Amazon SNS SNS-Thema gestreamt werden. Wenn zum Beispiel eine Ressource aktualisiert wird, können Sie eine Benachrichtigung an Ihre E-Mail-Adresse erhalten, damit Sie die Änderungen sehen können. Sie können auch benachrichtigt werden, wenn Ihre benutzerdefinierten oder verwalteten Regeln anhand Ihrer Ressourcen AWS Config bewertet werden. Weitere Informationen finden Sie unter Anmelden und Überwachen. AWS Config

AWS Config sendet Benachrichtigungen für die folgenden Ereignisse:

- Änderung des Konfigurationselements für eine Ressource.
- Konfigurationsverlauf, wenn eine Ressource für Ihr Konto geliefert wurde.
- Konfigurations-Snapshot für aufgezeichnete Ressourcen, die an Ihr Konto gesendet wurden.
- Compliance-Status Ihrer Ressourcen und ob diese mit Ihren Regeln konform sind.
- Bewertung einer Regel anhand Ihrer Ressourcen hat begonnen.
- AWS Config konnte die Benachrichtigung nicht an Ihr Konto senden.

Themen

- Beispiel für Benachrichtigungen bei Änderung eines Konfigurationselements
- Beispiel einer Benachrichtigung über den Konfigurationsverlauf
- Beispiel einer Benachrichtigung über den Beginn der Lieferung eines Konfigurations-Snapshot
- Beispiel einer Benachrichtigung über die Lieferung eines Konfigurations-Snapshots
- Beispiel einer Benachrichtigung über eine Compliance-Änderung
- Beispiel einer Benachrichtigung über den Beginn der Bewertung von Regeln
- Beispiel einer Benachrichtigung über die Änderung eines übergroßen Konfigurationselements
- Beispiel einer Benachrichtigung über eine fehlgeschlagene Sendung

Beispiel für Benachrichtigungen bei Änderung eines Konfigurationselements

AWS Config verwendet Amazon SNS, um Benachrichtigungen an Abonnement-Endpunkte zu senden. Diese Benachrichtigungen enthalten den Lieferstatus von Konfigurations-Snapshots und Konfigurationshistorien sowie jedes Konfigurationselement, das AWS Config erstellt wird, wenn sich die Konfigurationen aufgezeichneter Ressourcen ändern. AWS AWS Config sendet außerdem Benachrichtigungen, aus denen hervorgeht, ob Ihre Ressourcen Ihren Regeln entsprechen. Bei Benachrichtigungen per E-Mail können Sie in Ihrer E-Mail-Client-Anwendung Filter auf Grundlage des Betreffs und des E-Mail-Texts verwenden.

Die folgende Beispielnutzlast für eine Amazon-SNS-Benachrichtigung wird generiert, wenn AWS Config erkennt, dass das Amazon-Elastic-Block-Store-Volume `vol-ce676ccc` an die Instance mit der ID `i-344c463d` angefügt ist. Die Benachrichtigung enthält die Änderungen der Konfigurationselemente für die Ressource.

```
{
    "Type": "Notification",
    "MessageId": "8b945cb0-db34-5b72-b032-1724878af488",
    "TopicArn": "arn:aws:sns:us-west-2:123456789012:example",
    "Message": {
        "MessageVersion": "1.0",
        "NotificationCreateTime": "2014-03-18T10:11:00Z",
        "messageType": "ConfigurationItemChangeNotification",
        "configurationItem": [
            {
                "configurationItemVersion": "1.0",
                "configurationItemCaptureTime": "2014-03-07T23:47:08.918Z",
                "arn": "arn:aws:us-west-2b:123456789012:volume/vol-ce676ccc",
                "resourceId": "vol-ce676ccc",
                "awsAccountId": "123456789012",
                "configurationStateID": "3e660fdf-4e34-4f32-afeb-0ace5bf3d63a",
                "configurationItemStatus": "OK",
                "relatedEvents": [],
                "availabilityZone": "us-west-2b",
                "resourceType": "AWS::EC2::VOLUME",
                "resourceCreationTime": "2014-02-27T21:43:53.885Z",
                "tags": {},
                "relationships": [
                    {
                        "resourceId": "i-344c463d",
                        "resourceType": "AWS::EC2::INSTANCE",
                        "name": "Attached to Instance"
                    }
                ],
                "configuration": {
                    "volumeId": "vol-ce676ccc",
                    "size": 1,
                    "snapshotId": "",
                    "availabilityZone": "us-west-2b",
                    "state": "in-use",
                    "createTime": "2014-02-27T21:43:53.0885+0000",
                    "attachments": [
                        {
                            "volumeId": "vol-ce676ccc",
                            "instanceId": "i-344c463d",
                            "device": "/dev/sdf",
                            "state": "attached",
                            "attachTime": "2014-03-07T23:46:28.0000+0000",
```

```
                            "deleteOnTermination": false
                        }
                    ],
                    "tags": [],
                    "volumeType": "standard"
                }
            }
        ],
        "configurationItemDiff": {
            "changeType": "UPDATE",
            "changedProperties": {
                "Configuration.State": {
                    "previousValue": "available",
                    "updatedValue": "in-use",
                    "changeType": "UPDATE"
                },
                "Configuration.Attachments.0": {
                    "updatedValue": {
                        "VolumeId": "vol-ce676ccc",
                        "InstanceId": "i-344c463d",
                        "Device": "/dev/sdf",
                        "State": "attached",
                        "AttachTime": "FriMar0723: 46: 28UTC2014",
                        "DeleteOnTermination": "false"
                    },
                    "changeType": "CREATE"
                }
            }
        }
    },
    "Timestamp": "2014-03-07T23:47:10.001Z",
    "SignatureVersion": "1",
    "Signature": "LgfJNB5aOk/w3omqsYrv5cUFY8yvIJvO5ZZh46/
KGPApk6HXRTBRlkhjacnxIXJEWsGI9mxvMmoWPLJGYEAR5FF/+/Ro9QTmiTNcEjQ5kB8wGsRWVrk/
whAzT2lVtofc365En2T1Ncd9iSFFXfJchgBmI7EACZ28t
+n2mWFgo57n6eGDvHTedslzC6KxkfWTfXsR6zHXzkB3XuZImktflg3iPKtvBb3Zc9iVbNsBEI4FITFWktSqqomYDjc5h0kg
+qZhMzEbHWpzFlEzvFl55KaZXxDbznBD1ZkqPgno/WufuxszCiMrsmV8pUNUnkU1TA==",
    "SigningCertURL": "https://sns.us-west-2.amazonaws.com/SimpleNotificationService-
e372f8ca30337fdb084e8ac449342c77.pem",
    "UnsubscribeURL": "https://sns.us-west-2.amazonaws.com/?
Action=Unsubscribe&SubscriptionArn=arn:aws:sns:us-
west-2:123456789012:example:a6859fee-3638-407c-907e-879651c9d143"
}
```

Konfigurationselemente für Ressourcen mit Beziehungen

Steht eine Ressource im Zusammenhang mit anderen Ressourcen, kann sich eine Änderung dieser Ressource auf mehrere Konfigurationselemente auswirken. Das folgende Beispiel zeigt, wie Konfigurationselemente für Ressourcen mit Beziehungen AWS Config erstellt werden.

1. Sie haben eine EC2 Amazon-Instance mit der ID von`i-007d374c8912e3e90`, und die Instance ist einer EC2 Amazon-Sicherheitsgruppe zugeordnet,`sg-c8b141b4`.
2. Sie aktualisieren Ihre EC2 Instance, um die Sicherheitsgruppe in eine andere Sicherheitsgruppe zu ändern,`sg-3f1fef43`.
3. Da die EC2 Instanz mit einer anderen Ressource verknüpft ist, werden mehrere Konfigurationselemente wie die folgenden Beispiele AWS Config erstellt:

Diese Benachrichtigung enthält die Änderung des Konfigurationselements für die EC2 Instance, wenn die Sicherheitsgruppe ersetzt wird.

```
{
    "Type": "Notification",
    "MessageId": "faeba85e-ef46-570a-b01c-f8b0faae8d5d",
    "TopicArn": "arn:aws:sns:us-east-2:123456789012:config-topic-ohio",
    "Subject": "[AWS Config:us-east-2] AWS::EC2::Instance i-007d374c8912e3e90 Updated
 in Account 123456789012",
    "Message": {
        "configurationItemDiff": {
            "changedProperties": {
                "Configuration.NetworkInterfaces.0": {
                    "previousValue": {
                        "networkInterfaceId": "eni-fde9493f",
                        "subnetId": "subnet-2372be7b",
                        "vpcId": "vpc-14400670",
                        "description": "",
                        "ownerId": "123456789012",
                        "status": "in-use",
                        "macAddress": "0e:36:a2:2d:c5:e0",
                        "privateIpAddress": "172.31.16.84",
                        "privateDnsName": "ip-172-31-16-84.ec2.internal",
                        "sourceDestCheck": true,
                        "groups": [{
                            "groupName": "example-security-group-1",
                            "groupId": "sg-c8b141b4"
                        }],
```

```
                        "attachment": {
                            "attachmentId": "eni-attach-85bd89d9",
                            "deviceIndex": 0,
                            "status": "attached",
                            "attachTime": "2017-01-09T19:36:02.000Z",
                            "deleteOnTermination": true
                        },
                        "association": {
                            "publicIp": "54.175.43.43",
                            "publicDnsName":
"ec2-54-175-43-43.compute-1.amazonaws.com",
                            "ipOwnerId": "amazon"
                        },
                        "privateIpAddresses": [{
                            "privateIpAddress": "172.31.16.84",
                            "privateDnsName": "ip-172-31-16-84.ec2.internal",
                            "primary": true,
                            "association": {
                                "publicIp": "54.175.43.43",
                                "publicDnsName":
"ec2-54-175-43-43.compute-1.amazonaws.com",
                                "ipOwnerId": "amazon"
                            }
                        }]
                    },
                    "updatedValue": null,
                    "changeType": "DELETE"
                },
                "Relationships.0": {
                    "previousValue": {
                        "resourceId": "sg-c8b141b4",
                        "resourceName": null,
                        "resourceType": "AWS::EC2::SecurityGroup",
                        "name": "Is associated with SecurityGroup"
                    },
                    "updatedValue": null,
                    "changeType": "DELETE"
                },
                "Configuration.NetworkInterfaces.1": {
                    "previousValue": null,
                    "updatedValue": {
                        "networkInterfaceId": "eni-fde9493f",
                        "subnetId": "subnet-2372be7b",
                        "vpcId": "vpc-14400670",
```

```
                        "description": "",
                        "ownerId": "123456789012",
                        "status": "in-use",
                        "macAddress": "0e:36:a2:2d:c5:e0",
                        "privateIpAddress": "172.31.16.84",
                        "privateDnsName": "ip-172-31-16-84.ec2.internal",
                        "sourceDestCheck": true,
                        "groups": [{
                            "groupName": "example-security-group-2",
                            "groupId": "sg-3f1fef43"
                        }],
                        "attachment": {
                            "attachmentId": "eni-attach-85bd89d9",
                            "deviceIndex": 0,
                            "status": "attached",
                            "attachTime": "2017-01-09T19:36:02.000Z",
                            "deleteOnTermination": true
                        },
                        "association": {
                            "publicIp": "54.175.43.43",
                            "publicDnsName":
 "ec2-54-175-43-43.compute-1.amazonaws.com",
                            "ipOwnerId": "amazon"
                        },
                        "privateIpAddresses": [{
                            "privateIpAddress": "172.31.16.84",
                            "privateDnsName": "ip-172-31-16-84.ec2.internal",
                            "primary": true,
                            "association": {
                                "publicIp": "54.175.43.43",
                                "publicDnsName":
 "ec2-54-175-43-43.compute-1.amazonaws.com",
                                "ipOwnerId": "amazon"
                            }
                        }]
                    },
                    "changeType": "CREATE"
                },
                "Relationships.1": {
                    "previousValue": null,
                    "updatedValue": {
                        "resourceId": "sg-3f1fef43",
                        "resourceName": null,
                        "resourceType": "AWS::EC2::SecurityGroup",
```

```
                    "name": "Is associated with SecurityGroup"
                },
                "changeType": "CREATE"
            },
            "Configuration.SecurityGroups.1": {
                "previousValue": null,
                "updatedValue": {
                    "groupName": "example-security-group-2",
                    "groupId": "sg-3f1fef43"
                },
                "changeType": "CREATE"
            },
            "Configuration.SecurityGroups.0": {
                "previousValue": {
                    "groupName": "example-security-group-1",
                    "groupId": "sg-c8b141b4"
                },
                "updatedValue": null,
                "changeType": "DELETE"
            }
        },
        "changeType": "UPDATE"
    },
    "configurationItem": {
        "relatedEvents": [],
        "relationships": [
            {
                "resourceId": "eni-fde9493f",
                "resourceName": null,
                "resourceType": "AWS::EC2::NetworkInterface",
                "name": "Contains NetworkInterface"
            },
            {
                "resourceId": "sg-3f1fef43",
                "resourceName": null,
                "resourceType": "AWS::EC2::SecurityGroup",
                "name": "Is associated with SecurityGroup"
            },
            {
                "resourceId": "subnet-2372be7b",
                "resourceName": null,
                "resourceType": "AWS::EC2::Subnet",
                "name": "Is contained in Subnet"
            },
```

```
                {
                    "resourceId": "vol-0a2d63a256bce35c5",
                    "resourceName": null,
                    "resourceType": "AWS::EC2::Volume",
                    "name": "Is attached to Volume"
                },
                {
                    "resourceId": "vpc-14400670",
                    "resourceName": null,
                    "resourceType": "AWS::EC2::VPC",
                    "name": "Is contained in Vpc"
                }
            ],
            "configuration": {
                "instanceId": "i-007d374c8912e3e90",
                "imageId": "ami-9be6f38c",
                "state": {
                    "code": 16,
                    "name": "running"
                },
                "privateDnsName": "ip-172-31-16-84.ec2.internal",
                "publicDnsName": "ec2-54-175-43-43.compute-1.amazonaws.com",
                "stateTransitionReason": "",
                "keyName": "ec2-micro",
                "amiLaunchIndex": 0,
                "productCodes": [],
                "instanceType": "t2.micro",
                "launchTime": "2017-01-09T20:13:28.000Z",
                "placement": {
                    "availabilityZone": "us-east-2c",
                    "groupName": "",
                    "tenancy": "default",
                    "hostId": null,
                    "affinity": null
                },
                "kernelId": null,
                "ramdiskId": null,
                "platform": null,
                "monitoring": {"state": "disabled"},
                "subnetId": "subnet-2372be7b",
                "vpcId": "vpc-14400670",
                "privateIpAddress": "172.31.16.84",
                "publicIpAddress": "54.175.43.43",
                "stateReason": null,
```

```
                "architecture": "x86_64",
                "rootDeviceType": "ebs",
                "rootDeviceName": "/dev/xvda",
                "blockDeviceMappings": [{
                    "deviceName": "/dev/xvda",
                    "ebs": {
                        "volumeId": "vol-0a2d63a256bce35c5",
                        "status": "attached",
                        "attachTime": "2017-01-09T19:36:03.000Z",
                        "deleteOnTermination": true
                    }
                }],
                "virtualizationType": "hvm",
                "instanceLifecycle": null,
                "spotInstanceRequestId": null,
                "clientToken": "bIYqA1483990561516",
                "tags": [{
                    "key": "Name",
                    "value": "value"
                }],
                "securityGroups": [{
                    "groupName": "example-security-group-2",
                    "groupId": "sg-3f1fef43"
                }],
                "sourceDestCheck": true,
                "hypervisor": "xen",
                "networkInterfaces": [{
                    "networkInterfaceId": "eni-fde9493f",
                    "subnetId": "subnet-2372be7b",
                    "vpcId": "vpc-14400670",
                    "description": "",
                    "ownerId": "123456789012",
                    "status": "in-use",
                    "macAddress": "0e:36:a2:2d:c5:e0",
                    "privateIpAddress": "172.31.16.84",
                    "privateDnsName": "ip-172-31-16-84.ec2.internal",
                    "sourceDestCheck": true,
                    "groups": [{
                        "groupName": "example-security-group-2",
                        "groupId": "sg-3f1fef43"
                    }],
                    "attachment": {
                        "attachmentId": "eni-attach-85bd89d9",
                        "deviceIndex": 0,
```

```
                        "status": "attached",
                        "attachTime": "2017-01-09T19:36:02.000Z",
                        "deleteOnTermination": true
                    },
                    "association": {
                        "publicIp": "54.175.43.43",
                        "publicDnsName": "ec2-54-175-43-43.compute-1.amazonaws.com",
                        "ipOwnerId": "amazon"
                    },
                    "privateIpAddresses": [{
                        "privateIpAddress": "172.31.16.84",
                        "privateDnsName": "ip-172-31-16-84.ec2.internal",
                        "primary": true,
                        "association": {
                            "publicIp": "54.175.43.43",
                            "publicDnsName":
"ec2-54-175-43-43.compute-1.amazonaws.com",
                            "ipOwnerId": "amazon"
                        }
                    }]
                }],
                "iamInstanceProfile": null,
                "ebsOptimized": false,
                "sriovNetSupport": null,
                "enaSupport": true
            },
            "supplementaryConfiguration": {},
            "tags": {"Name": "value"},
            "configurationItemVersion": "1.2",
            "configurationItemCaptureTime": "2017-01-09T22:50:14.328Z",
            "configurationStateId": 1484002214328,
            "awsAccountId": "123456789012",
            "configurationItemStatus": "OK",
            "resourceType": "AWS::EC2::Instance",
            "resourceId": "i-007d374c8912e3e90",
            "resourceName": null,
            "ARN": "arn:aws:ec2:us-east-2:123456789012:instance/i-007d374c8912e3e90",
            "awsRegion": "us-east-2",
            "availabilityZone": "us-east-2c",
            "configurationStateMd5Hash": "8d0f41750f5965e0071ae9be063ba306",
            "resourceCreationTime": "2017-01-09T20:13:28.000Z"
        },
        "notificationCreationTime": "2017-01-09T22:50:15.928Z",
        "messageType": "ConfigurationItemChangeNotification",
```

```
        "recordVersion": "1.2"
    },
    "Timestamp": "2017-01-09T22:50:16.358Z",
    "SignatureVersion": "1",
    "Signature": "lpJTEYOSr8fUbiaaRNw1ECawJFVoD7I67mIeEkfAWJkqvvpak1ULHLlC
+I0sS/01A4P1Yci8GSK/cOEC/O2XBntlw4CAtbMUgTQvb345Z2YZwcpK0kPNi6v6N51DuZ/6DZA8EC
+gVTNTO09xtNIH8aMlvqyvUSXuh278xayExC5yTRXEg+ikdZRd4QzS7obSK1kgRZWI6ipxPNL6rd56/
VvPxyhcbS7Vm40/2+e0nVb3bjNHBxjQTXSs1Xhuc9eP2gEsC4Sl32bGqdeDU1Y4dFGukuzPYoHuEtDPh
+GkLUq3KeiDAQshxAZLmOIRcQ7iJ/bELDJTN9AcX6lqlDZ79w==",
    "SigningCertURL": "https://sns.us-east-2.amazonaws.com/SimpleNotificationService-
b95095beb82e8f6a046b3aafc7f4149a.pem",
    "UnsubscribeURL": "https://sns.us-east-2.amazonaws.com/?
Action=Unsubscribe&SubscriptionArn=arn:aws:sns:us-east-2:123456789012:config-topic-
ohio:956fe658-0ce3-4fb3-b409-a45f22a3c3d4"
}
```


Diese Benachrichtigung enthält die Änderung des Konfigurationselements für die EC2 Sicherheitsgruppe`sg-3f1fef43`, die der Instance zugeordnet ist.


```
{
    "Type": "Notification",
    "MessageId": "564d873e-711e-51a3-b48c-d7d064f65bf4",
    "TopicArn": "arn:aws:sns:us-east-2:123456789012:config-topic-ohio",
    "Subject": "[AWS Config:us-east-2] AWS::EC2::SecurityGroup sg-3f1fef43 Created in
 Account 123456789012",
    "Message": {
        "configurationItemDiff": {
            "changedProperties": {},
            "changeType": "CREATE"
        },
        "configurationItem": {
            "relatedEvents": [],
            "relationships": [{
                "resourceId": "vpc-14400670",
                "resourceName": null,
                "resourceType": "AWS::EC2::VPC",
                "name": "Is contained in Vpc"
            }],
            "configuration": {
                "ownerId": "123456789012",
                "groupName": "example-security-group-2",
                "groupId": "sg-3f1fef43",
                "description": "This is an example security group.",
```

```
                "ipPermissions": [],
                "ipPermissionsEgress": [{
                    "ipProtocol": "-1",
                    "fromPort": null,
                    "toPort": null,
                    "userIdGroupPairs": [],
                    "ipRanges": ["0.0.0.0/0"],
                    "prefixListIds": []
                }],
                "vpcId": "vpc-14400670",
                "tags": []
            },
            "supplementaryConfiguration": {},
            "tags": {},
            "configurationItemVersion": "1.2",
            "configurationItemCaptureTime": "2017-01-09T22:50:15.156Z",
            "configurationStateId": 1484002215156,
            "awsAccountId": "123456789012",
            "configurationItemStatus": "ResourceDiscovered",
            "resourceType": "AWS::EC2::SecurityGroup",
            "resourceId": "sg-3f1fef43",
            "resourceName": null,
            "ARN": "arn:aws:ec2:us-east-2:123456789012:security-group/sg-3f1fef43",
            "awsRegion": "us-east-2",
            "availabilityZone": "Not Applicable",
            "configurationStateMd5Hash": "7399608745296f67f7fe1c9ca56d5205",
            "resourceCreationTime": null
        },
        "notificationCreationTime": "2017-01-09T22:50:16.021Z",
        "messageType": "ConfigurationItemChangeNotification",
        "recordVersion": "1.2"
    },
    "Timestamp": "2017-01-09T22:50:16.413Z",
    "SignatureVersion": "1",
    "Signature": "GocX31Uu/zNFo85hZqzsNy30skwmLnjPjj+UjaJzkih
+dCP6gXYGQ0bK7uMzaLL2C/ibYOOsT7I/XY4NW6Amc5T46ydyHDjFRtQi8UfUQTqLXYRTnpOO/
hyK9lMFfhUNs4NwQpmx3n3mYEMpLuMs8DCgeBmB3AQ+hXPhNuNuR3mJVgo25S8AqphN9O0okZ2MKNUQy8iJm/
CVAx70TdnYsfUMZ24n88bUzAfiHGzc8QTthMdrFVUwXxa1h/7Zl8+A7BwoGmjo7W8CfLDVwaIQv1Uplgk3qd95Z0AXOzXVx
    "SigningCertURL": "https://sns.us-east-2.amazonaws.com/SimpleNotificationService-
b95095beb82e8f6a046b3aafc7f4149a.pem",
    "UnsubscribeURL": "https://sns.us-east-2.amazonaws.com/?
Action=Unsubscribe&SubscriptionArn=arn:aws:sns:us-east-2:123456789012:config-topic-
ohio:956fe658-0ce3-4fb3-b409-a45f22a3c3d4"
```

```
}
```

Grundlagen zum Feld **`configurationItemDiff`** in **`ConfigurationItemChangeNotification`**-Benachrichtungen in Amazon SNS

AWS Config erstellt ein Konfigurationselement, wenn sich die Konfiguration einer Ressource ändert (create/update/delete). Eine Liste der unterstützten Ressourcentypen, die aufgezeichnet werden AWS Config können, finden Sie unterUnterstützte Ressourcentypen für AWS Config. AWS Config verwendet Amazon SNS, um eine Benachrichtigung zu senden, sobald die Änderungen eintreten. Die Amazon SNS SNS-Benachrichtigungs-Payload enthält Felder, mit denen Sie die Ressourcenänderungen in einer bestimmten AWS Region verfolgen können.

Um zu verstehen, warum Sie eine `ConfigurationItemChangeNotification`-Benachrichtigung erhalten, überprüfen Sie die Details von `configurationItemDiff`. Die Felder variieren je nach Art der Änderung und können in unterschiedlichen Kombinationen vorkommen, z. B. UPDATE-UPDATE, UPDATE-CREATE und DELETE-DELETE. Im Folgenden werden einige häufige Kombinationen erläutert.

UPDATE-CREATE und UPDATE-UPDATE

Das folgende Beispiel umfasst Änderungen an den direkten Ressourcenbeziehungen und Ressourcenkonfigurationen. Die `configurationItemDiff`-Details enthalten die folgenden Informationen:

Durchgeführte Aktion: Eine verwaltete Richtlinie, die im Konto vorhanden ist, wurde mit einer AWS Identity and Access Management (IAM-) Rolle verknüpft.

Ausgeführter Basisvorgang: UPDATE (Aktualisierung der Anzahl der Verknüpfungen des Ressourcentyps `AWS::IAM::Policy` in einem Konto).

Kombinationen der Änderungstypen:

1. Änderung der direkten Beziehung zwischen Ressourcen (UPDATE-CREATE). Zwischen einer IAM-Richtlinie und einer IAM-Rolle wurde eine neue Anfügung oder Zuordnung erstellt.
2. Änderung der Ressourcenkonfiguration (UPDATE-UPDATE). Die Anzahl der IAM-Richtlinienzuordnungen ist von 2 auf 3 gestiegen, als die Richtlinie an die IAM-Rolle angefügt wurde.

Beispiel für eine `configurationItemDiff`-Benachrichtigung zu UPDATE-CREATE und UPDATE-UPDATE:

```
{
    "configurationItemDiff": {
        "changedProperties": {
            "Relationships.0": {
                "previousValue": null,
                "updatedValue": {
                    "resourceId": "AROA6D3M4S53*********",
                    "resourceName": "Test1",
                    "resourceType": "AWS::IAM::Role",
                    "name": "Is attached to Role"
                },
                "changeType": "CREATE"                >>>>>>>>>>>>>>>>>>>> 1
            },
            "Configuration.AttachmentCount": {
                "previousValue": 2,
                "updatedValue": 3,
                "changeType": "UPDATE"                >>>>>>>>>>>>>>>>>>>> 2
            }
        },
        "changeType": "UPDATE"
    }
}
```

UPDATE-DELETE

Das folgende Beispiel umfasst Änderungen an den direkten Ressourcenbeziehungen und Ressourcenkonfigurationen. Die `configurationItemDiff`-Details enthalten die folgenden Informationen:

Ausgeführte Aktion: Eine verwaltete Richtlinie, die im Konto vorhanden ist, wurde von einem IAM-Benutzer getrennt.

Ausgeführter Basisvorgang: UPDATE (Aktualisierung der mit dem Ressourcentyp `AWS::IAM::User` verknüpften Berechtigungsrichtlinie).

Kombinationen der Änderungstypen: Änderung der direkten Ressourcenbeziehung (UPDATE-DELETE). Die Verknüpfung zwischen einem IAM-Benutzer und einer IAM-Richtlinie in einem Konto wurde gelöscht.

Beispiel für eine `configurationItemDiff`-Benachrichtigung zu UPDATE-DELETE:

```
{
  "configurationItemDiff": {
    "changedProperties": {
      "Configuration.UserPolicyList.0": {
        "previousValue": {
          "policyName": "Test2",
          "policyDocument": "{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "VisualEditor0",
            "Effect": "Allow",
            "Action": "ec2:RunInstances",
            "Resource": "arn:aws:ec2:*:*:instance/*",
            "Condition": {
                "StringLike": {
                    "aws:RequestTag/VPCId": "*"
                }
            }
        }
    ]
}"
        },
        "updatedValue": null,
        "changeType": "DELETE"                        >>>>>>>>>>>>>>>>>>>> 3
      }
    },
    "changeType": "UPDATE"
  }
}
```

DELETE-DELETE

Das folgende Beispiel umfasst Änderungen an den direkten Ressourcenbeziehungen und Ressourcenkonfigurationen. Die `configurationItemDiff`-Details enthalten die folgenden Informationen:

Ausgeführte Aktion: Eine in einem Konto vorhandene IAM-Rolle wurde gelöscht.

Ausgeführter Basisvorgang: DELETE (Löschen einer Ressource des Ressourcentyps `AWS::IAM::Role`).

Kombinationen der Änderungstypen: Änderung der direkten Ressourcenbeziehung und Änderung der Ressourcenkonfiguration (DELETE-DELETE). Durch das Löschen der IAM-Rolle wurde auch die Zuordnung der IAM-Richtlinie zur IAM-Rolle gelöscht.

Beispiel für eine `configurationItemDiff`-Benachrichtigung zu DELETE-DELETE:

```
{
  "configurationItemDiff": {
    "changedProperties": {
      "Relationships.0": {
        "previousValue": {
          "resourceId": "ANPAIJ5MXUKK*********",
          "resourceName": "AWSCloudTrailAccessPolicy",
          "resourceType": "AWS::IAM::Policy",
          "name": "Is attached to CustomerManagedPolicy"
        },
        "updatedValue": null,
        "changeType": "DELETE"
      },
      "Configuration": {
        "previousValue": {
          "path": "/",
          "roleName": "CloudTrailRole",
          "roleId": "AROAJITJ6YGM*********",
          "arn": "arn:aws:iam::123456789012:role/CloudTrailRole",
          "createDate": "2017-12-06T10:27:51.000Z",
          "assumeRolePolicyDocument": "{"Version":"2012-10-17","Statement":
[{"Sid":"","Effect":"Allow","Principal":
{"AWS":"arn:aws:iam::123456789012:root"},"Action":"sts:AssumeRole","Condition":
{"StringEquals":{"sts:ExternalId":"123456"}}}]}",
          "instanceProfileList": [],
          "rolePolicyList": [],
          "attachedManagedPolicies": [
            {
              "policyName": "AWSCloudTrailAccessPolicy",
              "policyArn": "arn:aws:iam::123456789012:policy/AWSCloudTrailAccessPolicy"
            }
          ],
          "permissionsBoundary": null,
          "tags": [],
          "roleLastUsed": null
        },
        "updatedValue": null,
```

```
        "changeType": "DELETE"
      }
    },
    "changeType": "DELETE"
}
```

Beispiel einer Benachrichtigung über den Konfigurationsverlauf

Ein Konfigurationsverlauf ist die Sammlung der Konfigurationselemente für eine bestimmte Art von Ressource innerhalb eines Zeitraums. Im Folgenden finden Sie ein Beispiel für eine Benachrichtigung, die AWS Config gesendet wird, wenn der Konfigurationsverlauf für eine CloudTrail Trail-Ressource für Ihr Konto zugestellt wird.

```
{
    "Type": "Notification",
    "MessageId": "ce49bf2c-d03a-51b0-8b6a-ef480a8b39fe",
    "TopicArn": "arn:aws:sns:us-east-2:123456789012:config-topic-ohio",
    "Subject": "[AWS Config:us-east-2] Configuration History Delivery Completed for
 Account 123456789012",
    "Message": {
        "s3ObjectKey": "AWSLogs/123456789012/Config/us-east-2/2016/9/27/
ConfigHistory/123456789012_Config_us-
east-2_ConfigHistory_AWS::CloudTrail::Trail_20160927T195818Z_20160927T195818Z_1.json.gz",
        "s3Bucket": "config-bucket-123456789012-ohio",
        "notificationCreationTime": "2016-09-27T20:37:05.217Z",
        "messageType": "ConfigurationHistoryDeliveryCompleted",
        "recordVersion": "1.1"
    },
    "Timestamp": "2016-09-27T20:37:05.315Z",
    "SignatureVersion": "1",
    "Signature": "OuIcS5RAKXTR6chQEJp3if4KJQVlBz2kmXh7QE1/
RJQiCPsCNfG0J0rUZ1rqfKMqpps/Ka+zF0kg4dUCWV9PF0dliuwnjfbtYmDZpP4EBOoGmxcTliUn1AIe/
yeGFDuc6P3EotP3zt02rhmxjezjf3c11urstFZ8rTLVXp0z0xeyk4da0UetLsWZxUFEG0Z5uhk09mBo5dg/4mryIOovidhr
    "SigningCertURL": "https://sns.us-east-2.amazonaws.com/SimpleNotificationService-
b95095beb82e8f6a046b3aafc7f4149a.pem",
    "UnsubscribeURL": "https://sns.us-east-2.amazonaws.com/?
Action=Unsubscribe&SubscriptionArn=arn:aws:sns:us-east-2:123456789012:config-topic-
ohio:956fe658-0ce3-4fb3-b409-a45f22a3c3d4"
}
```

Beispiel einer Benachrichtigung über den Beginn der Lieferung eines Konfigurations-Snapshot

Im Folgenden finden Sie ein Beispiel für eine Benachrichtigung, die AWS Config gesendet wird, wenn AWS Config mit der Bereitstellung des Konfigurations-Snapshots für Ihr Konto begonnen wird.


```
{
    "Type": "Notification",
    "MessageId": "a32d0487-94b1-53f6-b4e6-5407c9c00be6",
    "TopicArn": "arn:aws:sns:us-east-2:123456789012:config-topic-ohio",
    "Subject": "[AWS Config:us-east-2] Configuration Snapshot Delivery Started for
 Account 123456789012",
    "Message": {
        "configSnapshotId": "108e0794-84a7-4cca-a179-76a199ddd11a",
        "notificationCreationTime": "2016-10-18T17:26:09.572Z",
        "messageType": "ConfigurationSnapshotDeliveryStarted",
        "recordVersion": "1.1"
    },
    "Timestamp": "2016-10-18T17:26:09.840Z",
    "SignatureVersion": "1",
    "Signature": "BBA0DeKsfteTpYyZH5HPANpOLmW/jumOMBsghRq/kimY9tjNlkF/
V3BpLG1HVmDQdQzBh6oKE0h0rxcazbyGf5KF5W5r1zKKlEnS9xugFzALPUx//
olSJ4neWalLBKNIq1xvAQgu9qHfDR7dS2aCwe4scQfqOjn1Ev7PlZqxmT+ux3SR/
C54cbfcduDpDsPwdo868+TpZvMtaU30ySnX04fmOgxoiA8AJO/EnjduQ08/zd4SYXhm
+H9wavcwXB9XECelHhRW70Y+wHQixfx40S1SaSRzvnJE+m9mHphFQs64YraRDRv6tMaenTk6CVPO
+81ceAXIg2E1m7hZ7lz4PA==",
    "SigningCertURL": "https://sns.us-east-2.amazonaws.com/SimpleNotificationService-
b95095beb82e8f6a046b3aafc7f4149a.pem",
    "UnsubscribeURL": "https://sns.us-east-2.amazonaws.com/?
Action=Unsubscribe&SubscriptionArn=arn:aws:sns:us-east-2:123456789012:config-topic-
ohio:956fe658-0ce3-4fb3-b409-a45f22a3c3d4"
}
```


Beispiel einer Benachrichtigung über die Lieferung eines Konfigurations-Snapshots

Der Konfigurations-Snapshot ist eine Sammlung von Konfigurationselementen für alle aufgezeichneten Ressourcen und Konfigurationen in Ihrem Konto. Im Folgenden finden Sie ein Beispiel für eine Benachrichtigung, die AWS Config gesendet wird, wenn der Konfigurations-Snapshot für Ihr Konto zugestellt wird.

```
{
    "Type": "Notification",
    "MessageId": "9fc82f4b-397e-5b69-8f55-7f2f86527100",
    "TopicArn": "arn:aws:sns:us-east-2:123456789012:config-topic-ohio",
    "Subject": "[AWS Config:us-east-2] Configuration Snapshot Delivery Completed for
 Account 123456789012",
    "Message": {
        "configSnapshotId": "16da64e4-cb65-4846-b061-e6c3ba43cb96",
        "s3ObjectKey": "AWSLogs/123456789012/Config/us-east-2/2016/9/27/
ConfigSnapshot/123456789012_Config_us-east-2_ConfigSnapshot_20160927T183939Z_16da64e4-
cb65-4846-b061-e6c3ba43cb96.json.gz",
        "s3Bucket": "config-bucket-123456789012-ohio",
        "notificationCreationTime": "2016-09-27T18:39:39.853Z",
        "messageType": "ConfigurationSnapshotDeliveryCompleted",
        "recordVersion": "1.1"
    },
    "Timestamp": "2016-09-27T18:39:40.062Z",
    "SignatureVersion": "1",
    "Signature": "PMkWfUuj/fKIEXA7s2wTDLbZoF/MDsUkPspYghOpwu9n6m+C
+zrm0cEZXPxxJPvhnWozG7SVqkHYf9QgI/diW2twP/HPDn5GQs2rNDc+YlaByEXnKVtHV1Gd4r1kN57E/
oOW5NVLNczk5ymxAW+WGdptZJkCgyVuhJ28s08m3Z3Kqz96PPSnXzYZoCfCn/
yP6CqXoN7olr4YCbYxYwn8zOUYcPmc45yYNSUTKZi+RJQRnDJkL2qb
+s4h9w2fjbBBj8xe830VbFJqbHp7UkSfpc64Y+tRvmMLY5CI1cYrnuPRhTLdUk+R0sshg5G+JMtSLVG/
TvWbjz44CKXJprjIQg==",
    "SigningCertURL": "https://sns.us-east-2.amazonaws.com/SimpleNotificationService-
b95095beb82e8f6a046b3aafc7f4149a.pem",
    "UnsubscribeURL": "https://sns.us-east-2.amazonaws.com/?
Action=Unsubscribe&SubscriptionArn=arn:aws:sns:us-east-2:123456789012:config-topic-
ohio:956fe658-0ce3-4fb3-b409-a45f22a3c3d4"
}
```


Beispiel einer Benachrichtigung über eine Compliance-Änderung

Wenn Ihre Ressourcen anhand einer benutzerdefinierten oder verwalteten Regel AWS Config bewertet werden, wird eine Benachrichtigung AWS Config gesendet, aus der hervorgeht, ob die Ressourcen der Regel entsprechen.

Im Folgenden finden Sie ein Beispiel für eine Benachrichtigung, bei der die CloudTrail Trail-Ressource mit der `cloudtrail-enabled` verwalteten Regel konform ist.


```
{
    "Type": "Notification",
```

```
    "MessageId": "11fd05dd-47e1-5523-bc01-55b988bb9478",
    "TopicArn": "arn:aws:sns:us-east-2:123456789012:config-topic-ohio",
    "Subject": "[AWS Config:us-east-2] AWS::::Account 123456789012 is COMPLIANT with
 cloudtrail-enabled in Accoun...",
    "Message": {
        "awsAccountId": "123456789012",
        "configRuleName": "cloudtrail-enabled",
        "configRuleARN": "arn:aws:config:us-east-2:123456789012:config-rule/config-
rule-9rpvxc",
        "resourceType": "AWS::::Account",
        "resourceId": "123456789012",
        "awsRegion": "us-east-2",
        "newEvaluationResult": {
            "evaluationResultIdentifier": {
                "evaluationResultQualifier": {
                    "configRuleName": "cloudtrail-enabled",
                    "resourceType": "AWS::::Account",
                    "resourceId": "123456789012"
                },
                "orderingTimestamp": "2016-09-27T19:48:40.619Z"
            },
            "complianceType": "COMPLIANT",
            "resultRecordedTime": "2016-09-27T19:48:41.405Z",
            "configRuleInvokedTime": "2016-09-27T19:48:40.914Z",
            "annotation": null,
            "resultToken": null
        },
        "oldEvaluationResult": {
            "evaluationResultIdentifier": {
                "evaluationResultQualifier": {
                    "configRuleName": "cloudtrail-enabled",
                    "resourceType": "AWS::::Account",
                    "resourceId": "123456789012"
                },
                "orderingTimestamp": "2016-09-27T16:30:49.531Z"
            },
            "complianceType": "NON_COMPLIANT",
            "resultRecordedTime": "2016-09-27T16:30:50.717Z",
            "configRuleInvokedTime": "2016-09-27T16:30:50.105Z",
            "annotation": null,
            "resultToken": null
        },
        "notificationCreationTime": "2016-09-27T19:48:42.620Z",
        "messageType": "ComplianceChangeNotification",
```

```
        "recordVersion": "1.0"
    },
    "Timestamp": "2016-09-27T19:48:42.749Z",
    "SignatureVersion": "1",
    "Signature": "XZ9FfLb2ywkW9yj0yBkNtIP5q7Cry6JtCEyUiHmG9gpOZi3seQ41udhtAqCZoiNiizAEi
+6gcttHCRV1hNemzp/
YmBmTfO6azYXt0FJDaEvd86k68VCS9aqRlBBjYlNo7ILi4Pqd5rE4BX2YBQSzcQyERGkUfTZ2BIFyAmb1Q/
y4/6ez8rDyi545FDSlgcGEb4LKLNR6eDi4FbKtMGZHA7Nz8obqs1dHbgWYnp3c80mVLl7ohP4hilcxdywAgXrbsN32ekYr1
+BIZ21ZtkcUtY5B3ImgRlUO7Yhn3L3c6rZxQ==",
    "SigningCertURL": "https://sns.us-east-2.amazonaws.com/SimpleNotificationService-
b95095beb82e8f6a046b3aafc7f4149a.pem",
    "UnsubscribeURL": "https://sns.us-east-2.amazonaws.com/?
Action=Unsubscribe&SubscriptionArn=arn:aws:sns:us-east-2:123456789012:config-topic-
ohio:956fe658-0ce3-4fb3-b409-a45f22a3c3d4"
}
```


Beispiel: Änderung des Konfigurationselements | Amazon EventBridge


```
{
  "version": "0",
  "id": "00bdf13e-1111-b2f5-cef0-e9cbbe7cd533",
  "detail-type": "Config Configuration Item Change",
  "source": "aws.config",
  "account": "123456789012",
  "time": "2022-03-16T01:10:51Z",
  "region": "us-east-1",
  "resources": ["arn:aws:elasticfilesystem:us-east-1:123456789012:file-system/
fs-01f0d526165b57f95"],
  "detail": {
    "recordVersion": "1.3",
    "messageType": "ConfigurationItemChangeNotification",
    "configurationItemDiff": {
      "changedProperties": {
        "Configuration.FileSystemTags.0": {
          "updatedValue": {
            "Key": "test",
            "Value": "me"
          },
          "changeType": "CREATE"
        },
        "Tags.2": {
          "updatedValue": "me",
          "changeType": "CREATE"
```

```
        }
      },
      "changeType": "UPDATE"
    },
    "notificationCreationTime": "2022-03-16T01:10:51.976Z",
    "configurationItem": {
      "relatedEvents": [],
      "relationships": [],
      "configuration": {
        "FileSystemId": "fs-01f0d526165b57f95",
        "Arn": "arn:aws:elasticfilesystem:us-east-1:123456789012:file-system/
fs-01f0d526165b57f95",
        "Encrypted": true,
        "FileSystemTags": [{
          "Key": "Name",
          "Value": "myname"
        }, {
          "Key": "test",
          "Value": "me"
        }],
        "PerformanceMode": "generalPurpose",
        "ThroughputMode": "bursting",
        "LifecyclePolicies": [{
          "TransitionToIA": "AFTER_30_DAYS"
        }, {
          "TransitionToPrimaryStorageClass": "AFTER_1_ACCESS"
        }],
        "BackupPolicy": {
          "Status": "ENABLED"
        },
        "FileSystemPolicy": {},
        "KmsKeyId": "arn:aws:kms:us-east-1:123456789012:key/0e6c91d5-e23b-4ed3-
bd36-1561fbbc0a2d"
      },
      "supplementaryConfiguration": {},
      "tags": {
        "aws:elasticfilesystem:default-backup": "enabled",
        "test": "me",
        "Name": "cloudcontroltest1"
      },
      "configurationItemVersion": "1.3",
      "configurationItemCaptureTime": "2022-03-16T01:10:50.837Z",
      "configurationStateId": 1647393050837,
      "awsAccountId": "123456789012",
```

```
      "configurationItemStatus": "OK",
      "resourceType": "AWS::EFS::FileSystem",
      "resourceId": "fs-01f0d526165b57f95",
      "resourceName": "fs-01f0d526165b57f95",
      "ARN": "arn:aws:elasticfilesystem:us-east-1:123456789012:file-system/
fs-01f0d526165b57f95",
      "awsRegion": "us-east-1",
      "availabilityZone": "Regional",
      "configurationStateMd5Hash": ""
    }
  }
}
```

Beispiel einer Benachrichtigung über den Beginn der Bewertung von Regeln

AWS Config sendet eine Benachrichtigung, wenn damit begonnen wird, Ihre benutzerdefinierte oder verwaltete Regel anhand Ihrer Ressourcen auszuwerten. Im Folgenden finden Sie ein Beispiel für eine Benachrichtigung, wenn AWS Config mit der Auswertung der `iam-password-policy` verwalteten Regel begonnen wird.

```
{
    "Type": "Notification",
    "MessageId": "358c8e65-e27a-594e-82d0-de1fe77393d7",
    "TopicArn": "arn:aws:sns:us-east-2:123456789012:config-topic-ohio",
    "Subject": "[AWS Config:us-east-2] Config Rules Evaluation Started for Account
 123456789012",
    "Message": {
        "awsAccountId": "123456789012",
        "awsRegion": "us-east-2",
        "configRuleNames": ["iam-password-policy"],
        "notificationCreationTime": "2016-10-13T21:55:21.339Z",
        "messageType": "ConfigRulesEvaluationStarted",
        "recordVersion": "1.0"
    },
    "Timestamp": "2016-10-13T21:55:21.575Z",
    "SignatureVersion": "1",
    "Signature": "DE431D+24zzFRboyPY2bPTsznJWe8L6TjDC+ItYlLFkE9jACSBl3sQ1uSjYzEhEbN7Cs
+wBoHnJ/DxOSpyCxt4giqgKd+H2I636BvrQwHDhJwJm7qI6P8IozEliRvRWbM38zDTvHqkmmXQbdDHRsK/
MssMeVTBKuW0x8ivMrj+KpwuF57tE62eXeFhjBeJ0DKQV+aC+i3onsuT7HQvXQDBPdOM
+cSuLrJaMQJ6TcMU5G76qg/
gl494ilb4Vj4udboGWpHSgUvI3guFsc1SsTrlWXQKXabWtsCQPfdOhkKgmViCfMZrLRp8Pjnu
+uspYQELkEfwBchDVVzd15iMrAzQ==",
```

```
    "SigningCertURL": "https://sns.us-east-2.amazonaws.com/SimpleNotificationService-
b95095beb82e8f6a046b3aafc7f4149a.pem",
    "UnsubscribeURL": "https://sns.us-east-2.amazonaws.com/?
Action=Unsubscribe&SubscriptionArn=arn:aws:sns:us-east-2:123456789012:config-topic-
ohio:956fe658-0ce3-4fb3-b409-a45f22a3c3d4"
}
```

Beispiel einer Benachrichtigung über die Änderung eines übergroßen Konfigurationselements

Wenn eine Konfigurationsänderung für eine Ressource AWS Config erkannt wird, sendet sie eine Benachrichtigung über ein Konfigurationselement (CI). Wenn die Benachrichtigung die für Amazon Simple Notification Service (Amazon SNS) maximal zulässige Größe überschreitet, enthält die Benachrichtigung eine kurze Übersicht über das Konfigurationselement.

Sie können sich die vollständige Benachrichtigung an dem im Feld `s3BucketLocation` angegebenen Amazon-S3-Bucket-Speicherort ansehen.

Die folgende Beispielbenachrichtigung zeigt ein CI für eine EC2 Amazon-Instance. Die Benachrichtigung enthält eine Zusammenfassung der Änderungen und den Speicherort der Benachrichtigung im Amazon-S3-Bucket.

```
View the Timeline for this Resource in the Console:
    https://console.aws.amazon.com/config/home?region=us-west-2#/timeline/
AWS::EC2::Instance/resourceId_14b76876-7969-4097-ab8e-a31942b02e80?
time=2016-10-06T16:46:16.261Z

    The full configuration item change notification for this resource exceeded the
 maximum size allowed by Amazon Simple Notification Service (SNS). A summary of the
 configuration item is provided here. You can view the complete notification in the
 specified Amazon S3 bucket location.

    New State Record Summary:
    ----------------------------
    {
      "configurationItemSummary": {
        "changeType": "UPDATE",
        "configurationItemVersion": "1.2",
        "configurationItemCaptureTime": "2016-10-06T16:46:16.261Z",
        "configurationStateId": 0,
        "awsAccountId": "123456789012",
        "configurationItemStatus": "OK",
```

```
        "resourceType": "AWS::EC2::Instance",
        "resourceId": "resourceId_14b76876-7969-4097-ab8e-a31942b02e80",
        "resourceName": null,
        "ARN": "arn:aws:ec2:us-west-2:123456789012:instance/
resourceId_14b76876-7969-4097-ab8e-a31942b02e80",
        "awsRegion": "us-west-2",
        "availabilityZone": null,
        "configurationStateMd5Hash": "8f1ee69b287895a0f8bc5753eca68e96",
        "resourceCreationTime": "2016-10-06T16:46:10.489Z"
      },
      "s3DeliverySummary": {
        "s3BucketLocation": "amzn-s3-demo-bucket/AWSLogs/123456789012/
Config/us-west-2/2016/10/6/OversizedChangeNotification/AWS::EC2::Instance/
resourceId_14b76876-7969-4097-ab8e-a31942b02e80/123456789012_Config_us-
west-2_ChangeNotification_AWS::EC2::Instance_resourceId_14b76876-7969-4097-ab8e-
a31942b02e80_20161006T164616Z_0.json.gz",
        "errorCode": null,
        "errorMessage": null
      },
      "notificationCreationTime": "2016-10-06T16:46:16.261Z",
      "messageType": "OversizedConfigurationItemChangeNotification",
      "recordVersion": "1.0"
    }
```

Wie greife ich auf übergroße Konfigurationselemente zu

Wenn ein Konfigurationselement überdimensioniert ist, wird nur eine Zusammenfassung an Amazon SNS gesendet. Das vollständige Konfigurationselement (CI) ist in Amazon S3 gespeichert

Das folgende Codebeispiel zeigt, wie Sie auf das komplette CI zugreifen können.

```
import boto3
import json

def handle_oversized_configuration_item(event):
    """
    Example of handling an oversized configuration item notification

    When a configuration item is oversized:
    1. AWS Config sends a summary notification through SNS
    2. The complete configuration item is stored in S3
    3. Use get_resource_config_history API to retrieve the complete configuration
    """
```

```
    # Extract information from the summary notification
    if event['messageType'] == 'OversizedConfigurationItemChangeNotification':
        summary = event['configurationItemSummary']
        resource_type = summary['resourceType']
        resource_id = summary['resourceId']

        # Initialize AWS Config client
        config_client = boto3.client('config')

        # Retrieve the complete configuration item
        response = config_client.get_resource_config_history(
            resourceType=resource_type,
            resourceId=resource_id
        )

        if response['configurationItems']:
            config_item = response['configurationItems'][0]

            # For EC2 instances, the configuration contains instance details
            configuration = json.loads(config_item['configuration'])
            print(f"Instance Configuration: {configuration}")

            # Handle supplementary configuration if present
            if 'supplementaryConfiguration' in config_item:
                for key, value in config_item['supplementaryConfiguration'].items():
                    if isinstance(value, str):
                        config_item['supplementaryConfiguration'][key] =
 json.loads(value)
                print(f"Supplementary Configuration:
 {config_item['supplementaryConfiguration']}")

            return config_item

        # If needed, you can also access the complete notification from S3
        s3_location = event['s3DeliverySummary']['s3BucketLocation']
        print(f"Complete notification available in S3: {s3_location}")

    return None
```

Funktionsweise

1. Die Funktion akzeptiert einen Ereignisparameter, der die AWS Config Benachrichtigung enthält.

2. Sie prüft, ob es sich bei dem Nachrichtentyp um eine zu große Konfigurationsbenachrichtigung handelt.
3. Die Funktion extrahiert den Ressourcentyp und die ID aus der Zusammenfassung.
4. Mithilfe des AWS Config Clients wird der vollständige Konfigurationshistorie abgerufen.
5. Die Funktion verarbeitet sowohl Haupt- als auch Zusatzkonfigurationen.
6. Bei Bedarf können Sie vom angegebenen S3-Standort aus auf die vollständige Benachrichtigung zugreifen.

Beispiel einer Benachrichtigung über eine fehlgeschlagene Sendung

AWS Config sendet eine Benachrichtigung über einen fehlgeschlagenen Versand, wenn der Konfigurations-Snapshot oder eine Benachrichtigung über eine Änderung eines zu großen Konfigurationselements nicht an Ihren Amazon S3 S3-Bucket gesendet werden AWS Config kann. Vergewissern Sie sich, dass Sie einen gültigen Amazon-S3-Bucket angegeben haben.

```
View the Timeline for this Resource in the Console:
    https://console.aws.amazon.com/config/home?region=us-west-2#/timeline/
AWS::EC2::Instance/test_resourceId_014b953d-75e3-40ce-96b9-c7240b975457?
time=2016-10-06T16:46:13.749Z

     The full configuration item change notification for this resource exceeded the
 maximum size allowed by Amazon Simple Notification Service (SNS). A summary of the
 configuration item is provided here. You can view the complete notification in the
 specified Amazon S3 bucket location.

    New State Record Summary:
    ----------------------------
    {
      "configurationItemSummary": {
        "changeType": "UPDATE",
        "configurationItemVersion": "1.2",
        "configurationItemCaptureTime": "2016-10-06T16:46:13.749Z",
        "configurationStateId": 0,
        "awsAccountId": "123456789012",
        "configurationItemStatus": "OK",
        "resourceType": "AWS::EC2::Instance",
        "resourceId": "test_resourceId_014b953d-75e3-40ce-96b9-c7240b975457",
        "resourceName": null,
        "ARN": "arn:aws:ec2:us-west-2:123456789012:instance/
test_resourceId_014b953d-75e3-40ce-96b9-c7240b975457",
```

```
        "awsRegion": "us-west-2",
        "availabilityZone": null,
        "configurationStateMd5Hash": "6de64b95eacd30e7b63d4bba7cd80814",
        "resourceCreationTime": "2016-10-06T16:46:10.489Z"
      },
      "s3DeliverySummary": {
        "s3BucketLocation": null,
        "errorCode": "NoSuchBucket",
        "errorMessage": "Failed to deliver notification to bucket: bucket-example for
 account 123456789012 in region us-west-2."
      },
      "notificationCreationTime": "2016-10-06T16:46:13.749Z",
      "messageType": "OversizedConfigurationItemChangeDeliveryFailed",
      "recordVersion": "1.0"
    }
```

Das AWS Config Dashboard anzeigen

Verwenden Sie das Dashboard, um einen Überblick über Ihre Ressourcen, Regeln, Konformitätspakete und deren Konformitätsstatus zu erhalten und Ihre AWS Config Nutzungs- und Erfolgskennzahlen mit Amazon CloudWatch zu visualisieren. Auf dieser Seite finden Sie schnell die wichtigsten Ressourcen in Ihrem AWS Konto, die Konformitätspakete mit der niedrigsten Konformitätsstufe in Ihrem Konto AWS-Konto, welche Regeln oder Ressourcen in Ihrem Konto nicht konform sind AWS-Konto, welcher Traffic Ihre AWS Config Nutzung vorantreibt und welche Kennzahlen für Erfolg und Misserfolg in Ihren Workflows aufgetreten sind.

Um das Dashboard zu verwenden AWS Config

1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die AWS Config Konsole zu https://console.aws.amazon.com/config/Hause.
2. Wählen Sie im linken Navigationsbereich Dashboard aus.

Inhalt

- Compliance und Ressourcenbestand
- AWS Config Nutzungs- und Erfolgsmetriken

Compliance und Ressourcenbestand

AWS Config Beginnt nach der Einrichtung mit der Aufzeichnung Ihrer angegebenen Ressourcen und deren Auswertung anhand Ihrer Regeln. Es kann einige Minuten dauern, AWS Config bis Ihre Ressourcen, Regeln, Konformitätspakete und deren Konformitätsstatus angezeigt werden.

Konformitätspakete nach Compliance-Ergebnis

Der Bereich Konformitätspakete nach Compliance-Ergebnis zeigt bis zu 10 Ihrer Konformitätspakete mit dem schlechtesten Compliance-Ergebnis an. Ein Konformitätspaket ist das Verhältnis (in Prozent) der Anzahl konformer Regel-Ressourcen-Kombinationen in einem Konformitätspaket zur Anzahl aller möglichen Regel-Ressourcen-Kombinationen in einem Konformitätspaket.

Diese Metrik bietet Ihnen einen umfassenden Überblick über den Compliance-Status Ihrer Konformitätspakete und kann verwendet werden, um den Grad der Compliance in Ihren

Konformitätspaketen zu ermitteln, zu untersuchen und zu verstehen. Sie können das Compliance-Ergebnis verwenden, um den Fortschritt der Korrekturen zu verfolgen, Vergleiche zwischen verschiedenen Anforderungssätzen durchzuführen und die Auswirkungen einer bestimmten Änderung oder Bereitstellung auf ein Konformitätspaket zu ermitteln.

Wenn Sie den Bereitstellungsstatus, das Compliance-Ergebnis, die Compliance-Ergebniszeitleiste und die Regeln für ein Konformitätspaket in einer detaillierten Ansicht sehen möchten, wählen Sie unter Konformitätspaket den Namen eines Konformitätspakets aus.

Compliance status (Compliance-Status)

Der Compliance-Status zeigt die Anzahl Ihrer konformen und nicht konformen Regeln und Ressourcen an. Basierend auf einer Bewertung der zugehörigen Regel sind Ressourcen konform oder nicht konform. Wenn eine Ressource nicht den Spezifikationen der Regel entspricht, werden die Ressource und die Regel als nicht konform gekennzeichnet.

Wenn Sie die Liste der nicht konformen Regeln und Ressourcen anzeigen möchten, wählen Sie Nichtkonforme Regel(n) oder Nichtkonforme Ressource(n) aus.

Regeln nach nicht konformen Ressourcen

Unter Regeln nach nicht konformen Ressourcen werden Ihre wichtigsten nicht konformen Regeln in absteigender Reihenfolge nach der Anzahl der Ressourcen angezeigt. Wählen Sie eine Regel aus, um ihre Details und Parameter sowie die Ressourcen im Geltungsbereich dieser speziellen Regel anzuzeigen.

Eine umfassende Liste der nicht konformen Regeln finden Sie unter Alle nicht konformen Regeln anzeigen.

Ressourcenbestand

Im Ressourceninventar wird die Gesamtzahl der Ressourcen, die AWS Config erfasst werden, in absteigender Reihenfolge nach der Anzahl der Ressourcen und der Anzahl der einzelnen Ressourcentypen in Ihrem angezeigt. AWS-Konto Wenn Sie alle Ressourcen für einen Ressourcentyp öffnen möchten, wählen Sie diesen Ressourcentyp aus und rufen Sie die zugehörige Ressourcenbestand-Seite auf.

Sie können die Dropdown-Liste verwenden, um anzugeben, welche Ressourcengesamtwerte Sie anzeigen lassen möchten. Standardmäßig ist es auf Alle Ressourcen anzeigen eingestellt, Sie können es aber auch in AWS Ressourcen, Ressourcen von Drittanbietern oder Benutzerdefinierte Ressourcen ändern.

> **Note**
>
> Die Meldung Evaluate your AWS resource configuration using Config Rules kann aus den folgenden Gründen auf dem Dashboard erscheinen:
>
> - Sie haben keine AWS Config Regeln für Ihre eingerichtet AWS-Konto. Sie können Add rule (Regel hinzufügen) auswählen, um die Seite Rules (Regeln) aufzurufen.
> - AWS Config bewertet Ihre Ressourcen immer noch anhand Ihrer Regeln. Sie können die Seite aktualisieren, um die neuesten Auswertungsergebnisse zu sehen.
> - AWS Config hat Ihre Ressourcen anhand Ihrer Regeln bewertet und keine Ressourcen im Geltungsbereich gefunden. Sie können die Ressourcen, die aufgezeichnet AWS Config werden sollen, auf der Seite Einstellungen angeben. Weitere Informationen finden Sie unter AWS Ressourcen aufzeichnen mit AWS Config.

AWS Config Nutzungs- und Erfolgsmetriken

Sie können CloudWatch Amazon-Dashboards in der AWS Config Konsole verwenden, um Ihre AWS Config Nutzungs- und Erfolgsmetriken zu visualisieren.

Für jedes Dashboard können Sie folgende Schritte durchführen:

- Passen Sie den Zeitbereich des Dashboards so an, dass Daten der letzten 3 Stunden, 1 Tag oder 1 Woche angezeigt werden.
- Wählen Sie das Kalendersymbol, um einen benutzerdefinierten Zeitraum einzugeben: entweder eine relative Zeit für einen bestimmten Zeitraum in der Vergangenheit oder einen absoluten Zeitraum zwischen zwei Daten.
- Sie können das Zeitformat so ändern, dass Dashboard-Daten in UTC (Coordinated Universal Time) oder in der lokalen Zeitzone (die Zeitzone, die im Betriebssystem Ihres Geräts als Ihre lokale Zeitzone angegeben ist) angezeigt werden.
- Verwenden Sie den Drop-Pfeil neben dem Aktualisierungssymbol, um anzugeben, wie oft die Daten in einem Dashboard aktualisiert werden sollen, oder um die automatische Aktualisierung zu deaktivieren. Wählen Sie Aus, 10 Sekunden, 1 Minute, 2 Minuten, 5 Minuten oder 15 Minuten aus, um das Aktualisierungsintervall zu ändern.
- Wählen Sie Weitere Optionen (das vertikale Ellipsenmenü), um die AWS Config Nutzungsmetriken oder AWS Config Erfolgsmetriken, die Sie gerade im AWS Config Dashboard sehen, zur CloudWatch Konsole hinzuzufügen. Dadurch wird eine neue Registerkarte in der CloudWatch

Konsole geöffnet, auf der Sie ein neues benutzerdefiniertes Dashboard CloudWatch mit Informationen erstellen können, die aus Ihren aktuellen AWS Config Nutzungs- oder AWS Config Erfolgsmetriken kopiert wurden.

Wenn Sie zusätzliche Analysen dieser Metriken mit durchführen möchten CloudWatch, wählen Sie im linken Navigationsbereich der CloudWatch Konsole Metriken und dann AWS/Config. Weitere Informationen dazu, was Sie von der CloudWatch Konsole aus tun können, finden Sie unter Verwenden von CloudWatch Amazon-Dashboards und Verwenden von CloudWatch Amazon-Metriken im CloudWatch Benutzerhandbuch.

AWS Config Nutzungsmetriken

Metrik	Beschreibung	Einheit	
`Configuration Items Recorded`	Die Anzahl der Konfigurationselemente, die für jeden Ressourcentyp oder alle Ressourcentypen aufgezeichnet wurden. Ein Konfigurationselement stellt eine point-in-time Ansicht der verschiedenen Attribute einer unterstützten AWS Ressource dar. Weitere Informationen zu Konfigurationselementen oder unterstützten Ressourcentypen finden Sie unter Konfigurationselemente und Unterstützte Ressourcentypen.	Anzahl	

Sie können den Ressourcentyp, den Sie anzeigen möchten, über die Dropdown-Liste auswählen. Standardmäßig werden alle Ressourcentypen angezeigt.

AWS Config Erfolgskennzahlen

Metrik	Beschreibung	Einheit	
`Change Notifications Delivery Failed`	Die Anzahl der fehlgeschlagenen Lieferungen von Änderungsbenachrichtigungen an das Amazon SNS SNS-Thema für Ihren Lieferkanal. Eine Änderungsbenachrichtigung informiert Sie über eine Änderung des Konfigura	Anzahl	

Metrik	Beschreibung	Einheit	
	tionsstatus Ihrer AWS Ressourcen. Sie können die ConfigStreamDeliveryInfoAPI verwenden, um das `lastErrorCode` oder `lastErrorMessage` für den letzten Zustellversuch für eine Änderungsbenachrichtigung abzurufen. Weitere Informationen finden Sie unter Verwalten des Übermittlungskanals.		
`Config History Export Failed`	Die Anzahl der fehlgeschlagenen Exporte des Konfigurationsverlaufs in Ihren Amazon S3 S3-Bucket. Ein Konfigurationsverlauf ist die Sammlung der Konfigurationselemente für eine bestimmte Ressource über einen festgelegten Zeitraum. Weitere Informationen zum Konfigurationsverlauf finden Sie unter Konfigurationsverlauf.	Anzahl	
`Configuration Recorder Insufficient Permissions Failure`	Die Anzahl der fehlgeschlagenen Zugriffsversuche aufgrund der IAM-Rollenrichtlinie für alle Konfigurationsrekorder in Ihrem Konto und aufgrund unzureichender AWS-Region Berechtigungen. Der Konfigurationsrekorder erkennt Änderungen an den Ressourcentypen im Gültigkeitsbereich. Damit der Konfigurationsrekorder Ihre AWS Ressourcenkonfigurationen aufzeichnen kann, benötigter die erforderlichen IAM-Berechtigungen. Weitere Informationen finden Sie unter IAM-Rollenrichtlinie zum Abrufen von Konfigurationsdetails.	Anzahl	

Metrik	Beschreibung	Einheit	
`Config Snapshot Export Failed`	Die Anzahl der fehlgeschlagenen Konfigurations-Snapshot-Exporte in Ihren Amazon S3 S3-Bucket. Ein Konfigurations-Snapshot ist eine Sammlung der Konfigurationselemente der unterstützten Ressourcen in Ihrem Konto. Weitere Informationen zu Konfigurations-Snapshots finden Sie unter Konfigurations-Snapshot.	Anzahl	

Verwaltung und Anzeige von AWS Ressourcenkonfigurationen mit AWS Config

AWS Config ermöglicht es Ihnen, die Konfigurationen von AWS Ressourcen zu bewerten, zu prüfen und zu bewerten.

AWS Ressourcen sind Entitäten, die Sie mit den AWS Management Console Tools AWS Command Line Interface (CLI) AWS SDKs, oder AWS Partnern erstellen und verwalten. Zu den AWS Ressourcen gehören beispielsweise EC2 Amazon-Instances, Sicherheitsgruppen VPCs, Amazon und Amazon Elastic Block Store. AWS Config bezieht sich auf jede Ressource unter Verwendung ihrer eindeutigen Kennung, z. B. der Ressourcen-ID oder eines Amazon-Ressourcennamens (ARN).

Zu den häufigsten Anwendungsfällen gehören:

- Cloud-Administrator: Sie können Ressourcenkonfigurationen verfolgen und verwalten, um die Einhaltung von Vorschriften sicherzustellen, Probleme zu beheben und Ihre AWS Umgebung besser zu verstehen
- Sicherheitsanalyst: Sie können Ressourcenkonfigurationen anhand der gewünschten Zustände bewerten, um Schwachstellen zu identifizieren und den Sicherheitsstatus zu beurteilen.
- Compliance-Beauftragter: Sie können die Ressourcenkonfigurationen kontinuierlich prüfen und überwachen, um sicherzustellen, dass Unternehmensrichtlinien und Industriestandards eingehalten werden.

Themen

- Unterstützte Ressourcentypen für AWS Config
- Ressourcenabdeckung nach regionaler Verfügbarkeit
- AWS Ressourcen aufzeichnen mit AWS Config
- Aufzeichnen von Konfigurationen mit AWS Config für Ressourcen von Drittanbietern mithilfe des AWS CLI
- Aufzeichnen der Softwarekonfiguration für verwaltete Instanzen mit AWS Config
- Suchen nach Ressourcen, die entdeckt wurden von AWS Config
- Compliance-Informationen und Bewertungsergebnisse für Ihre AWS Ressourcen anzeigen mit AWS Config
- Den Compliance-Verlauf für Ihre AWS Ressourcen anzeigen mit AWS Config

- Den Compliance-Verlauf Ihrer Ressourcen abfragen AWS
- Verschlagworten Sie Ihre Ressourcen AWS Config

Unterstützte Ressourcentypen für AWS Config

> **Important**
>
> Diese Seite wird zu Beginn eines jeden Monats monatlich aktualisiert.

AWS Config unterstützt die folgenden AWS Ressourcentypen und Ressourcenbeziehungen.

- Ausführlichere Informationen zu einem Ressourcentyp finden Sie in den zugehörigen Referenzinformationen (wie Syntax, Eigenschaften und Rückgabewerte) in der Referenz zu AWS Ressourcen und Eigenschaftstypen im AWS CloudFormation Benutzerhandbuch.
- Bei der AWS Config Aufzeichnung unterstützen einige AWS Regionen eine Teilmenge dieser Ressourcentypen. Informationen darüber, welche Ressourcentypen in welchen Regionen unterstützt werden, finden Sie unter Ressourcenabdeckung nach regionaler Verfügbarkeit.
- Erweiterte Abfragen für AWS Config unterstützt eine Teilmenge dieser Ressourcentypen. Sie finden diese unterstützten Ressourcentypen in der Liste der unterstützten Ressourcentypen für erweiterte Abfragen.
- Proaktive Evaluierung für AWS Config unterstützt eine Teilmenge dieser Ressourcentypen. Eine Liste der unterstützten Ressourcentypen finden Sie in der Liste der unterstützten Ressourcentypen für die proaktive Auswertung.
- Periodische Regeln werden ausgeführt, ohne dass der Konfigurationsrekorder aktiviert ist, da periodische Regeln nicht von Konfigurationselementen (CIs) abhängen. Weitere Informationen zum Unterschied zwischen durch Änderungen ausgelösten Regeln und periodischen Regeln finden Sie unter Evaluierungsmodus und Triggertypen für AWS Config Regeln.

  Das bedeutet, dass auf der Regelseite kein CI oder keine unterstützte Ressource aufgeführt ist. Wenn Sie die Ressourcen-ID auswählen, wird der folgende Fehler angezeigt:`The provided resource ID and resource type cannot be found`. Dieses Verhalten wird erwartet.

> **Note**
>
> Regionale Verfügbarkeit für Ressourcentypen

Bevor Sie einen Ressourcentyp für AWS Config die Nachverfolgung angeben, überprüfen Sie, ob der Ressourcentyp in der AWS Region, in der Sie ihn eingerichtet haben, unterstützt wird AWS Config. Wenn ein Ressourcentyp AWS Config in mindestens einer Region unterstützt wird, können Sie die Aufzeichnung dieses Ressourcentyps in allen Regionen aktivieren, die von unterstützt werden AWS Config, auch wenn der angegebene Ressourcentyp in der AWS Region, in der Sie ihn eingerichtet haben, nicht unterstützt wird AWS Config.

Tagging-Unterstützung für Ressourcentypen

Wenn ein Ressourcentyp kein Tagging unterstützt oder keine Tag-Informationen in seiner Describe-API-Antwort enthält, AWS Config werden keine Tag-Daten in den Konfigurationselementen (CIs) für diesen Ressourcentyp erfasst. AWS Config zeichnet diese Ressourcen trotzdem auf. Funktionen, die auf Tag-Daten basieren, funktionieren jedoch nicht. Dies wirkt sich auf Tag-basierte Filterung, Gruppierung oder Konformitätsbewertung aus, die auf Tag-Daten basiert.

Amazon AppStream

AWS Bedienung	Ressourcentyp „Value“	Beziehung	Verwandte Ressource
Amazon AppStream	`AWS::AppStream::DirectoryConfig`	N/A	N/A
	`AWS::AppStream::Application`	N/A	N/A
	`AWS::AppStream::Stack`	N/A	N/A
	`AWS::AppStream::Fleet`	N/A	N/A

Amazon AppFlow

AWS Bedienung	Ressourcentyp „Value“	Beziehung	Verwandte Ressource
Amazon AppFlow	`AWS::AppFlow::Flow`	N/A	N/A

AWS Bedienung	Ressourcentyp „Value“	Beziehung	Verwandte Ressource
Amazon AppIntegrations	`AWS::AppIntegrations::EventIntegration`	N/A	N/A
	`AWS::AppIntegrations::Application`	N/A	N/A

Amazon API Gateway

AWS Bedienung	Ressourcentyp „Value“	Beziehung	Verwandte Ressource
API Gateway	`AWS::ApiGateway::Stage`	ist enthalten in	ApiGateway Api ausruhen
		ist zugeordnet zu	WAFRegional WebACL

AWS Bedienung	Ressourcentyp „Value“	Beziehung	Verwandte Ressource
	`AWS::ApiGateway::RestApi`	enthält	ApiGateway Stufe
API Gateway V2	`AWS::ApiGatewayV2::Stage`	ist enthalten in	ApiGatewayV2 Api
	`AWS::ApiGatewayV2::Api`	enthält	ApiGatewayV2-Stufe

Weitere Informationen zur AWS Config Integration mit Amazon API Gateway finden Sie unter Überwachung der API-Gateway-API-Konfiguration mit AWS Config.

Amazon Athena

AWS Dienst	Ressourcentyp „Value“	Beziehung	Verwandte Ressource
Amazon Athena	`AWS::Athena::WorkGroup`	N/A	N/A
	`AWS::Athena::DataCatalog`	N/A	N/A
	`AWS::Athena::PreparedStatement`	N/A	N/A

Amazon Bedrock

AWS Bedienung	Ressourcentyp „Value“	Beziehung	Verwandte Ressource
Amazon Bedrock	`AWS::Bedrock::Guardrail`	N/A	N/A
	`AWS::Bedrock::KnowledgeBase`	N/A	N/A

Amazon CloudFront

AWS Bedienung	Ressourcentyp „Value“	Beziehung	Verwandte Ressource
Amazon CloudFront	`AWS::CloudFront::Distribution`	ist zugeordnet zu	AWS WAF WebACL
			ACM-Zertifikat
			S3 Bucket
			IAM-Serverzertifikat
	`AWS::CloudFront::StreamingDistribution`	ist zugeordnet zu	AWS WAF WebACL
			ACM-Zertifikat
			S3 Bucket
			IAM-Serverzertifikat

Amazon CloudWatch

AWS Bedienung	Ressourcentyp „Value“	Beziehung	Verwandte Ressource
Amazon CloudWatch	`AWS::CloudWatch::Alarm`	N/A	N/A
	`AWS::CloudWatch::MetricStream`	N/A	N/A
CloudWatch Amazon-Protokolle	`AWS::Logs::Destination`	N/A	N/A
Amazon CloudWatch RUM	`AWS::RUM::AppMonitor`	N/A	N/A
Amazon CloudWatch offenbar	`AWS::Evidently::Project`	N/A	N/A
	`AWS::Evidently::Launch`	N/A	N/A
	`AWS::Evidently::Segment`	N/A	N/A

Amazon CodeGuru

AWS Bedienung	Ressourcentyp „Value“	Beziehung	Verwandte Ressource
CodeGuru Amazon-Rezensent	`AWS::CodeGuruReviewer::RepositoryAssociation`	N/A	N/A

AWS Bedienung	Ressourcentyp „Value“	Beziehung	Verwandte Ressource
Amazon CodeGuru Profiler	`AWS::CodeGuruProfiler::ProfilingGroup`	N/A	N/A

Amazon Cognito

AWS Bedienung	Ressourcentyp „Value“	Beziehung	Verwandte Ressource
Amazon Cognito	`AWS::Cognito::UserPool`	N/A	N/A
	`AWS::Cognito::UserPoolClient`	N/A	N/A
	`AWS::Cognito::UserPoolGroup`	N/A	N/A
	`AWS::Cognito::IdentityPool`	N/A	N/A

Amazon Connect

AWS Bedienung	Ressourcentyp „Value“	Beziehung	Verwandte Ressource
Amazon Connect	`AWS::Connect::PhoneNumber`	N/A	N/A
	`AWS::Connect::QuickConnect`	N/A	N/A
	`AWS::Connect::Instance`	N/A	N/A
	`AWS::Connect::Rule`	N/A	N/A
	`AWS::Connect::User`	N/A	N/A
Amazon Connect Customer Profiles	`AWS::CustomerProfiles::Domain`	N/A	N/A
	`AWS::CustomerProfiles::ObjectType`	N/A	N/A

Amazon Detective

AWS Bedienung	Ressourcentyp „Value“	Beziehung	Verwandte Ressource
Amazon Detective	`AWS::Detective::Graph`	N/A	N/A

Amazon-DynamoDB

AWS Bedienung	Ressourcentyp „Value“	Beziehung	Verwandte Ressource
Amazon-DynamoDB	`AWS::DynamoDB::Table`	N/A	N/A

Amazon Elastic Compute Cloud

AWS Bedienung	Ressourcentyp „Value“	Beziehung	Verwandte Ressource
Amazon Elastic Compute Cloud	`AWS::EC2::Host` *	enthält	EC2 Instanz
	`AWS::EC2::EIP`	ist angefügt an	EC2 Instanz
			Netzwerkschnittstelle
	`AWS::EC2::Instance`	enthält	EC2 Netzwerkschnittstelle
		ist zugeordnet zu	EC2 Sicherheitsgruppe
		ist angefügt an	Amazon EBS-Volume

AWS Bedienung	Ressourcentyp „Value“	Beziehung	Verwandte Ressource
			EC2 Elastische IP (EIP)
		ist enthalten in	EC2 Dedizierter Host
			Routing-Tabelle
			Subnetz
			Virtual Private Cloud (VPC)
	`AWS::EC2::NetworkInterface`	ist zugeordnet zu	EC2 Sicherheitsgruppe
		ist angefügt an	EC2 Elastische IP (EIP)
			EC2 Instanz
		ist enthalten in	Routing-Tabelle
			Subnetz
			Virtual Private Cloud (VPC)
	`AWS::EC2::SecurityGroup` *	ist zugeordnet zu	EC2 Instanz
			EC2 Netzwerkschnittstelle
			Virtual Private Cloud (VPC)
	`AWS::EC2::NatGateway`	ist enthalten in	Virtual Private Cloud (VPC)

AWS Bedienung	Ressourcentyp „Value“	Beziehung	Verwandte Ressource
		ist enthalten in	Subnetz
	`AWS::EC2::EgressOnlyInternetGateway`	ist angefügt an	Virtual Private Cloud (VPC)
	`AWS::EC2::EC2Fleet`	N/A	N/A
	`AWS::EC2::SpotFleet`	N/A	N/A
	`AWS::EC2::PrefixList`	N/A	N/A
	`AWS::EC2::FlowLog`	N/A	N/A
	`AWS::EC2::TransitGateway`	N/A	N/A
	`AWS::EC2::TransitGatewayAttachment`	N/A	N/A
	`AWS::EC2::TransitGatewayRouteTable`	N/A	N/A
	`AWS::EC2::VPCEndpoint`	ist enthalten in	Virtual Private Cloud (VPC)

AWS Bedienung	Ressourcentyp „Value“	Beziehung	Verwandte Ressource
		ist angefügt an	Netzwerkschnittstelle
		ist enthalten in	Subnetz
		ist enthalten in	Routing-Tabelle
	`AWS::EC2::VPCEndpointService`	ist zugeordnet zu	ElasticLoadBalancingV2 LoadBalancer
	`AWS::EC2::VPCPeeringConnection`	ist zugeordnet zu	Virtual Private Cloud (VPC)
	`AWS::EC2::RegisteredHAInstance`	ist zugeordnet zu	EC2 Instanz
	`AWS::EC2::SubnetRouteTableAssociation`	N/A	N/A
	`AWS::EC2::LaunchTemplate`	N/A	N/A
	`AWS::EC2::NetworkInsightsAccessScopeAnalysis`	N/A	N/A
	`AWS::EC2::TrafficMirrorTarget`	N/A	N/A

AWS Bedienung	Ressourcentyp „Value“	Beziehung	Verwandte Ressource
	`AWS::EC2::TrafficMirrorSession`	N/A	N/A
	`AWS::EC2::DHCPOptions`	N/A	N/A
	`AWS::EC2::IPAM`	N/A	N/A
	`AWS::EC2::IPAMResourceDiscovery`	N/A	N/A
	`AWS::EC2::IPAMResourceDiscoveryAssociation`	N/A	N/A
	`AWS::EC2::NetworkInsightsPath`	N/A	N/A
	`AWS::EC2::TrafficMirrorFilter`	N/A	N/A
	`AWS::EC2::CapacityReservation`	N/A	N/A
	`AWS::EC2::ClientVpnEndpoint`	N/A	N/A

AWS Bedienung	Ressourcentyp „Value“	Beziehung	Verwandte Ressource
	`AWS::EC2::Customer Gateway`	ist angefügt an	VPN-Verbindung
	`AWS::EC2::Internet Gateway`	ist angefügt an	Virtual Private Cloud (VPC)
	`AWS::EC2::NetworkAcl`	N/A	N/A
	`AWS::EC2::RouteTable`	enthält	EC2 Instanz
			EC2 Netzwerks chnittstelle
			Subnetz
			VPN-Gateway
		ist enthalten in	Virtual Private Cloud (VPC)
	`AWS::EC2::Subnet`	enthält	EC2 Instanz
			EC2 Netzwerks chnittstelle
		ist angefügt an	Netzwerk-ACL
		ist enthalten in	Routing-Tabelle
			Virtual Private Cloud (VPC)
	`AWS::EC2::VPC`	enthält	EC2 Instanz

AWS Bedienung	Ressourcentyp „Value“	Beziehung	Verwandte Ressource
			EC2 Netzwerks chnittstelle
			Netzwerk-ACL
			Routing-Tabelle
			Subnetz
		ist zugeordnet zu	Sicherheitsgruppe
		ist angefügt an	Internet-Gateway
			VPN-Gateway
	`AWS::EC2::VPNConnection`	ist angefügt an	Kunden-Gateway
			VPN-Gateway
	`AWS::EC2::VPNConnectionRoute`	N/A	N/A
	`AWS::EC2::VPNGateway`	ist angefügt an	Virtual Private Cloud (VPC)
			VPN-Verbindung
		ist enthalten in	Routing-Tabelle
	`AWS::EC2::IPAMScope`	N/A	N/A
	`AWS::EC2::CarrierGateway`	N/A	N/A

AWS Bedienung	Ressourcentyp „Value“	Beziehung	Verwandte Ressource
	`AWS::EC2::TransitGatewayConnect`	N/A	N/A
	`AWS::EC2::IPAMPool`	N/A	N/A
	`AWS::EC2::TransitGatewayMulticastDomain`	N/A	N/A
	`AWS::EC2::NetworkInsightsAccessScope`	N/A	N/A
	`AWS::EC2::NetworkInsightsAnalysis`	N/A	N/A
	`AWS::EC2::VPCBlockPublicAccessOptions`	N/A	N/A
	`AWS::EC2::VPCBlockPublicAccessExclusion`	N/A	N/A
	`AWS::EC2::EIPAssociation`	N/A	N/A

AWS Bedienung	Ressourcentyp „Value“	Beziehung	Verwandte Ressource
	`AWS::EC2::InstanceConnectEndpoint`	N/A	N/A
	`AWS::EC2::SnapshotBlockPublicAccess`	N/A	N/A
	`AWS::EC2::VPCEndpointConnectionNotification`	N/A	N/A
Amazon Elastic Block Store	`AWS::EC2::Volume`	ist angefügt an	EC2 Instanz
EC2 Image Builder	`AWS::ImageBuilder::ImagePipeline`	N/A	N/A
	`AWS::ImageBuilder::DistributionConfiguration`	N/A	N/A
	`AWS::ImageBuilder::ContainerRecipe`	N/A	N/A

AWS Bedienung	Ressourcentyp „Value“	Beziehung	Verwandte Ressource
	`AWS::ImageBuilder::InfrastructureConfiguration`	N/A	N/A
	`AWS::ImageBuilder::ImageRecipe`	N/A	N/A

*AWS Config zeichnet die Konfigurationsdetails von Dedicated Hosts und der Instances auf, die Sie auf ihnen starten. Daher können Sie sie AWS Config als Datenquelle verwenden, wenn Sie die Einhaltung Ihrer servergebundenen Softwarelizenzen melden. Sie können beispielsweise die Konfigurationshistorie einer Instance anzeigen und bestimmen, auf welchem Amazon Machine Image (AMI) sie basiert. Sie können dann den Konfigurationsverlauf des Hosts mit Details wie der Anzahl der Sockets und Kerne nachschlagen, um zu überprüfen, ob der Host die Lizenzanforderungen des AMI erfüllt. Weitere Informationen finden Sie unter Verfolgen von Konfigurationsänderungen mit AWS Config im EC2 Amazon-Benutzerhandbuch.

* Die EC2 SecurityGroup Eigenschaftendefinition enthält IP-CIDR-Blöcke, die intern in IP-Bereiche konvertiert werden und bei der Suche nach einem bestimmten IP-Bereich möglicherweise zu unerwarteten Ergebnissen führen. Problemumgehungen für die Suche nach bestimmten IP-Bereichen finden Sie unter Einschränkungen für erweiterte Abfragen.

Amazon Elastic Container Registry

AWS Dienst	Ressourcentyp „Value“	Beziehung	Verwandte Ressource
Amazon Elastic Container Registry	`AWS::ECR::Repository`	N/A	N/A

AWS Dienst	Ressourcentyp „Value“	Beziehung	Verwandte Ressource
	`AWS::ECR::Registry Policy`	N/A	N/A
	`AWS::ECR::PullThroughCacheRule`	N/A	N/A
Amazon Elastic Container Registry Public	`AWS::ECR::PublicRepository`	N/A	N/A

Amazon Elastic Container Service

AWS Bedienung	Ressourcentyp „Value“	Beziehung	Verwandte Ressource
Amazon Elastic Container Service	`AWS::ECS::Cluster`	N/A	N/A
	`AWS::ECS::TaskDefinition`	N/A	N/A
	`AWS::ECS::Service` *	N/A	N/A
	`AWS::ECS::TaskSet`	N/A	N/A
	`AWS::ECS::CapacityProvider`	N/A	N/A

* Dieser Service unterstützt derzeit nur das neue Format für Amazon Ressourcennamen (ARN). Weitere Informationen finden Sie unter Amazon Resource Names (ARNs) und IDs im ECS-Entwicklerhandbuch.

Alt (nicht unterstützt): `arn:aws:ecs:region:aws_account_id:service/service-name`

Neu (unterstützt): `arn:aws:ecs:region:aws_account_id:service/cluster-name/service-name`

Amazon Elastic File System

AWS Service	Ressourcentyp „Value“	Beziehung	Verwandte Ressource
Amazon Elastic File System	`AWS::EFS::FileSystem`	N/A	N/A
	`AWS::EFS::AccessPoint`	N/A	N/A

Amazon Elastic Kubernetes Service

AWS Bedienung	Ressourcentyp „Value“	Beziehung	Verwandte Ressource
Amazon Elastic Kubernetes Service	`AWS::EKS::Cluster`	N/A	N/A
	`AWS::EKS::FargateProfile`	N/A	N/A
	`AWS::EKS::IdentityProviderConfig`	N/A	N/A
	`AWS::EKS::Addon`	N/A	N/A

Amazon EMR

AWS Bedienung	Ressourcentyp „Value“	Beziehung	Verwandte Ressource
Amazon EMR	`AWS::EMR::Security Configuration`	N/A	N/A

Amazon EventBridge

AWS Bedienung	Ressourcentyp „Value“	Beziehung	Verwandte Ressource
Amazon EventBridge	`AWS::Events::EventBus`	N/A	N/A
	`AWS::Events::ApiDestination`	N/A	N/A
	`AWS::Events::Archive`	N/A	N/A
	`AWS::Events::Endpoint`	N/A	N/A
	`AWS::Events::Connection`	N/A	N/A
	`AWS::Events::Rule`	N/A	N/A
EventBridge Amazon-Schemas	`AWS::EventSchemas::Registry Policy`	N/A	N/A

AWS Bedienung	Ressourcentyp „Value“	Beziehung	Verwandte Ressource
	`AWS::EventSchemas::Discoverer`	N/A	N/A
	`AWS::EventSchemas::Schema`	N/A	N/A
	`AWS::EventSchemas::Registry`	N/A	N/A

Amazon Forecast

AWS Bedienung	Ressourcentyp „Value“	Beziehung	Verwandte Ressource
Amazon Forecast	`AWS::Forecast::Dataset`	N/A	N/A
	`AWS::Forecast::DatasetGroup`	N/A	N/A

Amazon Fraud Detector

AWS Bedienung	Ressourcentyp „Value“	Beziehung	Verwandte Ressource
Amazon Fraud Detector	`AWS::FraudDetector::Label`	N/A	N/A

AWS Bedienung	Ressourcentyp „Value“	Beziehung	Verwandte Ressource
	`AWS::FraudDetector::EntityType`	N/A	N/A
	`AWS::FraudDetector::Variable`	N/A	N/A
	`AWS::FraudDetector::Outcome`	N/A	N/A

Amazon GuardDuty

AWS Bedienung	Ressourcentyp „Value“	Beziehung	Verwandte Ressource
Amazon GuardDuty	`AWS::GuardDuty::Detector`	N/A	N/A
	`AWS::GuardDuty::ThreatIntelSet`	N/A	N/A
	`AWS::GuardDuty::IPSet`	N/A	N/A
	`AWS::GuardDuty::Filter`	N/A	N/A

Amazon Inspector

AWS Bedienung	Ressourcentyp „Value“	Beziehung	Verwandte Ressource
Amazon Inspector	`AWS::InspectorV2::Filter`	N/A	N/A
	`AWS::InspectorV2::Activation`	N/A	N/A

Amazon Interactive Video Service

AWS Bedienung	Ressourcentyp „Value“	Beziehung	Verwandte Ressource
Amazon Interactive Video Service	`AWS::IVS::Channel`	N/A	N/A
	`AWS::IVS::RecordingConfiguration`	N/A	N/A
	`AWS::IVS::PlaybackKeyPair`	N/A	N/A

Amazon Keyspaces (für Apache Cassandra)

AWS Bedienung	Ressourcentyp „Value“	Beziehung	Verwandte Ressource
Amazon Keyspaces (für Apache Cassandra)	`AWS::Cassandra::Keyspace`	N/A	N/A

OpenSearch Amazon-Dienst

AWS Bedienung	Ressourcentyp „Value“	Beziehung	Verwandte Ressource
Amazon OpenSearch Service (ältere Version von Elasticsearch)	`AWS::Elasticsearch::Domain`	ist zugeordnet zu	KMS-Schlüssel
			EC2 Sicherheitsgruppe
			EC2 Subnetz
			Virtual Private Cloud (VPC)
OpenSearch Amazon-Dienst	`AWS::OpenSearch::Domain`	N/A	N/A
Amazon OpenSearch Serverlos	`AWS::OpenSearchServerless::VpcEndpoint`	N/A	N/A
	`AWS::OpenSearchServerless::Collection`	N/A	N/A

> **Amazon OpenSearch Service umbenennen**
>
> Am 8. September 2021 wurde Amazon Elasticsearch Service in Amazon OpenSearch Service umbenannt. OpenSearch Der Service unterstützt sowohl ältere Elasticsearch-Betriebssysteme OpenSearch als auch ältere Versionen. Weitere Informationen finden Sie unter Amazon OpenSearch Service — Zusammenfassung der Änderungen. Möglicherweise werden Ihre Daten für mehrere Wochen weiterhin `AWS::OpenSearch::Domain` unter dem vorhandenen `AWS::Elasticsearch::Domain` Ressourcentyp angezeigt, auch wenn Sie ein Upgrade für eine oder mehrere Domains auf durchführen OpenSearch.

Amazon Personalize

AWS Dienst	Ressourcentyp „Value“	Beziehung	Verwandte Ressource
Amazon Personalize	`AWS::Personalize::Dataset`	N/A	N/A
	`AWS::Personalize::Schema`	N/A	N/A
	`AWS::Personalize::Solution`	N/A	N/A
	`AWS::Personalize::DatasetGroup`	N/A	N/A

Amazon Pinpoint

AWS Bedienung	Ressourcentyp „Value“	Beziehung	Verwandte Ressource
Amazon Pinpoint	`AWS::Pinpoint::ApplicationSettings`	N/A	N/A
	`AWS::Pinpoint::Segment`	N/A	N/A
	`AWS::Pinpoint::App`	N/A	N/A
	`AWS::Pinpoint::Campaign`	N/A	N/A
	`AWS::Pinpoint::InAppTemplate`	N/A	N/A
	`AWS::Pinpoint::EmailChannel`	N/A	N/A
	`AWS::Pinpoint::EmailTemplate`	N/A	N/A
	`AWS::Pinpoint::EventStream`	N/A	N/A

Amazon Quantum Ledger Database (Amazon QLDB)

AWS Bedienung	Ressourcentyp „Value“	Beziehung	Verwandte Ressource
Amazon QLDB	`AWS::QLDB::Ledger`	N/A	N/A

Amazon Kendra

AWS Bedienung	Ressourcentyp „Value“	Beziehung	Verwandte Ressource
Amazon Kendra	`AWS::Kendra::Index`	N/A	N/A

Amazon Kinesis

AWS Bedienung	Ressourcentyp „Value“	Beziehung	Verwandte Ressource
Amazon Kinesis	`AWS::Kinesis::Stream`	N/A	N/A
	`AWS::Kinesis::StreamConsumer`	N/A	N/A
Amazon Kinesis Analytics V2	`AWS::KinesisAnalyticsV2::Application`	N/A	N/A
Amazon Data Firehose	`AWS::KinesisFireho`	N/A	N/A

AWS Bedienung	Ressourcentyp „Value“	Beziehung	Verwandte Ressource
	`se::Deliv eryStream`		
Kinesis-Videostream	`AWS::Kine sisVideo: :Signalin gChannel`	N/A	N/A
	`AWS::Kine sisVideo: :Stream`	N/A	N/A

Amazon Lex

AWS Bedienung	Ressourcentyp „Value“	Beziehung	Verwandte Ressource
Amazon Lex	`AWS::Lex: :BotAlias`	N/A	N/A
	`AWS::Lex::Bot`	N/A	N/A

Amazon Lightsail

AWS Bedienung	Ressourcentyp „Value“	Beziehung	Verwandte Ressource
Amazon Lightsail	`AWS::Ligh tsail::Disk`	N/A	N/A
	`AWS::Ligh tsail::Ce rtificate`	N/A	N/A

AWS Bedienung	Ressourcentyp „Value“	Beziehung	Verwandte Ressource
	`AWS::Lightsail::Bucket`	N/A	N/A
	`AWS::Lightsail::StaticIp`	N/A	N/A

Amazon Lookout für Metrics

AWS Bedienung	Ressourcentyp „Value“	Beziehung	Verwandte Ressource
Amazon Lookout für Metrics	`AWS::LookoutMetrics::Alert`	N/A	N/A

Amazon Lookout für Vision

AWS Bedienung	Ressourcentyp „Value“	Beziehung	Verwandte Ressource
Amazon Lookout für Vision	`AWS::LookoutVision::Project`	N/A	N/A

Amazon Macie

AWS Bedienung	Ressourcentyp „Value“	Beziehung	Verwandte Ressource
Amazon Macie	`AWS::Macie::Session`	N/A	N/A

Amazon Managed Grafana

AWS Bedienung	Ressourcentyp „Value“	Beziehung	Verwandte Ressource
Amazon Managed Grafana	`AWS::Grafana::Workspace`	N/A	N/A

Amazon Managed Service für Prometheus

AWS Bedienung	Ressourcentyp „Value“	Beziehung	Verwandte Ressource
Amazon Managed Service für Prometheus	`AWS::APS::RuleGroupsNamespace`	N/A	N/A

Amazon MemoryDB

AWS Bedienung	Ressourcentyp „Value“	Beziehung	Verwandte Ressource
Amazon MemoryDB	`AWS::MemoryDB::SubnetGroup`	N/A	N/A

Amazon MQ

AWS Bedienung	Ressourcentyp „Value“	Beziehung	Verwandte Ressource
Amazon MQ	`AWS::AmazonMQ::Broker`	N/A	N/A

Amazon Managed Streaming für Apache Kafka

AWS Bedienung	Ressourcentyp „Value“	Beziehung	Verwandte Ressource
Amazon Managed Streaming für Apache Kafka	`AWS::MSK::Cluster`	N/A	N/A
	`AWS::MSK::Configuration`	N/A	N/A
	`AWS::MSK::BatchScramSecret`	N/A	N/A
	`AWS::MSK::ClusterPolicy`	N/A	N/A
	`AWS::MSK::VpcConnection`	N/A	N/A
Amazon Managed Streaming für Apache Kafka Connect	`AWS::KafkaConnect::Connector`	N/A	N/A

Amazon QuickSight

AWS Bedienung	Ressourcentyp „Value“	Beziehung	Verwandte Ressource
Amazon QuickSight	`AWS::QuickSight::DataSource`	N/A	N/A
	`AWS::QuickSight::Template`	N/A	N/A
	`AWS::QuickSight::Theme`	N/A	N/A

Amazon Redshift

AWS Bedienung	Ressourcentyp „Value“	Beziehung	Verwandte Ressource
Amazon Redshift	`AWS::Redshift::Cluster`	ist zugeordnet zu	Cluster-Parametergruppe
			Cluster-Sicherheitsgruppe
			Cluster Subnet Group
			Sicherheitsgruppe
			Virtual Private Cloud (VPC)
	`AWS::Redshift::Clu`	N/A	N/A

AWS Bedienung	Ressourcentyp „Value“	Beziehung	Verwandte Ressource
	`sterParameterGroup`		
	`AWS::Redshift::ClusterSecurityGroup`	N/A	N/A
	`AWS::Redshift::ScheduledAction`	N/A	N/A
	`AWS::Redshift::ClusterSnapshot`	ist zugeordnet zu	Cluster
			Virtual Private Cloud (VPC)
	`AWS::Redshift::ClusterSubnetGroup`	ist zugeordnet zu	Subnetz
			Virtual Private Cloud (VPC)
	`AWS::Redshift::EventSubscription`	N/A	N/A
	`AWS::Redshift::EndpointAccess`	N/A	N/A
	`AWS::Redshift::EndpointAuthorization`	N/A	N/A

Amazon Relational Database Service

AWS Bedienung	Ressourcentyp „Value“	Beziehung	Verwandte Ressource
Amazon Relational Database Service	`AWS::RDS::DBInstance`	ist zugeordnet zu	EC2 Sicherheitsgruppe
			RDS-DB-Sicherheitsgruppe
			RDS-DB-Subnet Group
	`AWS::RDS::DBSecurityGroup`	ist zugeordnet zu	EC2 Sicherheitsgruppe
			Virtual Private Cloud (VPC)
	`AWS::RDS::DBSnapshot`	ist zugeordnet zu	Virtual Private Cloud (VPC)
	`AWS::RDS::DBSubnetGroup`	ist zugeordnet zu	EC2 Sicherheitsgruppe
			Virtual Private Cloud (VPC)
	`AWS::RDS::EventSubscription`	N/A	N/A
	`AWS::RDS::DBCluster`	enthält	RDS-DB-Instance
		ist zugeordnet zu	RDS-DB-Subnet Group

AWS Bedienung	Ressourcentyp „Value“	Beziehung	Verwandte Ressource
			EC2 Sicherheitsgruppe
	`AWS::RDS::DBClusterSnapshot`	ist zugeordnet zu	RDS-DB-Cluster
			Virtual Private Cloud (VPC)
	`AWS::RDS::GlobalCluster`	N/A	N/A
	`AWS::RDS::OptionGroup`	N/A	N/A

Amazon Route 53

AWS Dienst	Ressourcentyp „Value“	Beziehung	Verwandte Ressource
Amazon Route 53	`AWS::Route53::HostedZone`	N/A	N/A
	`AWS::Route53::HealthCheck`	N/A	N/A
Amazon-Route-53-Profile	`AWS::Route53Profiles::Profile`	N/A	N/A
Amazon Route 53 Resolver	`AWS::Route53Resolver::ResolverEndpoint`	N/A	N/A
	`AWS::Route53Resolver::ResolverRule`	N/A	N/A
	`AWS::Route53Resolver::ResolverRuleAssociation`	N/A	N/A

AWS Dienst	Ressourcentyp „Value“	Beziehung	Verwandte Ressource
	`AWS::Route53Resolver::FirewallDomainList`	N/A	N/A
	`AWS::Route53Resolver::FirewallRuleGroupAssociation`	N/A	N/A
	`AWS::Route53Resolver::ResolverQueryLoggingConfig`	N/A	N/A
	`AWS::Route53Resolver::ResolverQueryLoggingConfigAssociation`	N/A	N/A
	`AWS::Route53Resolver::FirewallRuleGroup`	N/A	N/A
Amazon Application Recovery Controller (ARC)	`AWS::Route53RecoveryReadiness::Cell`	N/A	N/A
	`AWS::Route53RecoveryReadiness::ReadinessCheck`	N/A	N/A
	`AWS::Route53RecoveryReadiness::RecoveryGroup`	N/A	N/A
	`AWS::Route53RecoveryControl::Cluster`	N/A	N/A
	`AWS::Route53RecoveryControl::ControlPanel`	N/A	N/A
	`AWS::Route53RecoveryControl::RoutingControl`	N/A	N/A
	`AWS::Route53RecoveryControl::SafetyRule`	N/A	N/A
	`AWS::Route53RecoveryReadiness::ResourceSet`	N/A	N/A

Amazon SageMaker KI

AWS Bedienung	Ressourcentyp „Value“	Beziehung	Verwandte Ressource
Amazon SageMaker KI	`AWS::SageMaker::CodeRepository`	N/A	N/A
	`AWS::SageMaker::Domain`	N/A	N/A
	`AWS::SageMaker::AppImageConfig`	N/A	N/A
	`AWS::SageMaker::Image`	N/A	N/A
	`AWS::SageMaker::Model`	N/A	N/A
	`AWS::SageMaker::NotebookInstance`	N/A	N/A
	`AWS::SageMaker::NotebookInstanceLifecycleConfig`	N/A	N/A
	`AWS::SageMaker::EndpointConfig`	N/A	N/A

AWS Bedienung	Ressourcentyp „Value“	Beziehung	Verwandte Ressource
	`AWS::SageMaker::Workteam`	N/A	N/A
	`AWS::SageMaker::FeatureGroup`	N/A	N/A
	`AWS::SageMaker::InferenceExperiment`	N/A	N/A

Amazon Simple Email Service

AWS Bedienung	Ressourcentyp „Value“	Beziehung	Verwandte Ressource
Amazon Simple Email Service	`AWS::SES::ConfigurationSet`	N/A	N/A
	`AWS::SES::ContactList`	N/A	N/A
	`AWS::SES::Template`	N/A	N/A
	`AWS::SES::ReceiptFilter`	N/A	N/A
	`AWS::SES::ReceiptRuleSet`	N/A	N/A

Amazon Simple Notification Service

AWS Bedienung	Ressourcentyp „Value“	Beziehung	Verwandte Ressource
Amazon Simple Notification Service	`AWS::SNS::Topic`	N/A	N/A

Amazon Simple Queue Service

AWS Bedienung	Ressourcentyp „Value“	Beziehung	Verwandte Ressource
Amazon Simple Queue Service	`AWS::SQS::Queue`	N/A	N/A

Amazon Simple Storage Service

AWS Bedienung	Ressourcentyp „Value“	Beziehung	Verwandte Ressource
Amazon Simple Storage Service	`AWS::S3::Bucket` *	N/A	N/A
	`AWS::S3::AccountPublicAccessBlock`	N/A	N/A
	`AWS::S3::MultiRegionAccessPoint`	N/A	N/A
	`AWS::S3::StorageLens`	N/A	N/A

AWS Bedienung	Ressourcentyp „Value“	Beziehung	Verwandte Ressource
	`AWS::S3::AccessPoint`	N/A	N/A
	`AWS::S3::StorageLensGroup`	N/A	N/A
Amazon S3 Express One Zone	`AWS::S3Express::DirectoryBucket`	N/A	N/A
	`AWS::S3Express::BucketPolicy`	N/A	N/A

* Wenn Sie für AWS Config die Aufzeichnung Ihrer S3-Buckets konfiguriert haben und keine Benachrichtigungen über Konfigurationsänderungen erhalten, überprüfen Sie, ob Ihre S3-Bucket-Richtlinien über die erforderlichen Berechtigungen verfügen. Weitere Informationen finden Sie unter Verwaltung von Berechtigungen für die S3-Bucket-Aufzeichnung.

Amazon-S3-Bucket-Attribute

AWS Config zeichnet auch die folgenden Attribute für den Amazon S3 S3-Bucket-Ressourcentyp auf.

Attribute	Beschreibung
AccelerateConfiguration	Transfer Acceleration bei Daten über große Entfernungen zwischen Ihrem Client und einen Bucket.
BucketAcl	Zugriffskontrollliste für die Verwaltung des Bucket- und Objektzugriffs.
BucketPolicy	Richtlinie, mit der die Berechtigungen für den Bucket bestimmt werden.

Attribute	Beschreibung
CrossOriginConfiguration	Lassen Sie Cross-Origin-Anforderungen an die Buckets zu.
LifecycleConfiguration	Regeln, die den Lebenszyklus von Objekten in Ihrem Bucket definieren.
LoggingConfiguration	Protokollierung zur Nachverfolgung der Zugriffsanforderungen für die Buckets.
NotificationConfiguration	Ereignisbenachrichtigungen für das Senden von Warnungs- und Auslöser-Workflows für bestimmte Bucket-Ereignisse.
ReplicationConfiguration	Automatisches, asynchrones Kopieren von Objekten in den Buckets verschiedener AWS -Regionen.
RequestPaymentConfiguration	Zahlung durch den Anforderer ist aktiviert.
TaggingConfiguration	Tags, die dem Bucket zur Kategorisierung hinzugefügt werden. Sie können die Fakturierung auch durch Markierung verfolgen.
WebsiteConfiguration	Statisches Website-Hosting ist für den Bucket aktiviert.
VersioningConfiguration	Versioning ist für Objekte im Bucket aktiviert.

Weitere Informationen zu den Attributen finden Sie unter Optionen für die Bucket-Konfiguration im Benutzerhandbuch für Amazon Simple Storage Service.

Amazon WorkSpaces

AWS Bedienung	Ressourcentyp „Value“	Beziehung	Verwandte Ressource
Amazon WorkSpaces	`AWS::WorkSpaces::ConnectionAlias`	N/A	N/A

AWS Bedienung	Ressourcentyp „Value“	Beziehung	Verwandte Ressource
	`AWS::WorkSpaces::Workspace`	N/A	N/A

AWS Amplify

AWS Bedienung	Ressourcentyp „Value“	Beziehung	Verwandte Ressource
AWS Amplify	`AWS::Amplify::App`	N/A	N/A
	`AWS::Amplify::Branch`	N/A	N/A

AWS AppConfig

AWS Bedienung	Ressourcentyp „Value“	Beziehung	Verwandte Ressource
AWS AppConfig	`AWS::AppConfig::Application`	N/A	N/A
	`AWS::AppConfig::Environment`	N/A	N/A
	`AWS::AppConfig::ConfigurationProfile`	N/A	N/A

AWS Bedienung	Ressourcentyp „Value“	Beziehung	Verwandte Ressource
	`AWS::AppConfig::DeploymentStrategy`	N/A	N/A
	`AWS::AppConfig::HostedConfigurationVersion`	N/A	N/A
	`AWS::AppConfig::ExtensionAssociation`	N/A	N/A

AWS App Runner

AWS Bedienung	Ressourcentyp „Value“	Beziehung	Verwandte Ressource
AWS App Runner	`AWS::AppRunner::VpcConnector`	N/A	N/A
	`AWS::AppRunner::Service`	N/A	N/A

AWS App Mesh

AWS Bedienung	Ressourcentyp „Value“	Beziehung	Verwandte Ressource
AWS App Mesh	`AWS::AppMesh::VirtualNode`	N/A	N/A
	`AWS::AppMesh::VirtualService`	N/A	N/A
	`AWS::AppMesh::VirtualGateway`	N/A	N/A
	`AWS::AppMesh::VirtualRouter`	N/A	N/A
	`AWS::AppMesh::Route`	N/A	N/A
	`AWS::AppMesh::GatewayRoute`	N/A	N/A
	`AWS::AppMesh::Mesh`	N/A	N/A

AWS AppSync

AWS Bedienung	Ressourcentyp „Value“	Beziehung	Verwandte Ressource
AWS AppSync	`AWS::AppSync::GraphQLApi`	N/A	N/A

AWS Audit Manager

AWS Bedienung	Ressourcentyp „Value“	Beziehung	Verwandte Ressource
AWS Audit Manager	`AWS::AuditManager::Assessment`	N/A	N/A

AWS Auto Scaling

AWS Bedienung	Ressourcentyp „Value“	Beziehung	Verwandte Ressource
AWS Auto Scaling	`AWS::AutoScaling::AutoScalingGroup`	enthält	EC2 Amazon-Instanz
		ist zugeordnet zu	Classic Load Balancer
			Auto Scaling-Startkonfiguration
			Subnetz
	`AWS::AutoScaling::`	ist zugeordnet zu	EC2 Amazon-Sicherheitsgruppe

AWS Bedienung	Ressourcentyp „Value“	Beziehung	Verwandte Ressource
	`LaunchConfiguration`		
	`AWS::AutoScaling::ScalingPolicy`	ist zugeordnet zu	Auto Scaling-Gruppe
			Alarm
	`AWS::AutoScaling::ScheduledAction`	ist zugeordnet zu	Auto Scaling-Gruppe
	`AWS::AutoScaling::WarmPool`	N/A	N/A

AWS Backup

AWS Dienst	Ressourcentyp „Value“	Beziehung	Verwandte Ressource
AWS Backup	`AWS::Backup::BackupPlan`	N/A	N/A*
	`AWS::Backup::BackupSelection`	N/A	N/A
	`AWS::Backup::BackupVault`	N/A	N/A*

AWS Dienst	Ressourcentyp „Value“	Beziehung	Verwandte Ressource
	`AWS::Backup::RecoveryPoint`	N/A	N/A
	`AWS::Backup::ReportPlan`	N/A	N/A

Aufgrund der AWS Backup Funktionsweise beziehen sich einige dieser Ressourcentypen auf die anderen AWS Backup Ressourcentypen in dieser Tabelle.

`AWS::Backup::BackupPlan`bezieht sich darauf, `AWS::Backup::BackupSelection` wo ein Backup-Plan viele Auswahlmöglichkeiten hat, und bezieht `AWS::Backup::BackupVault` sich darauf, `AWS::Backup::RecoveryPoint` wo ein AWS Backup Tresor mehrere Wiederherstellungspunkte hat.

Weitere Informationen finden Sie unter Verwaltung von Backups mithilfe von Backup-Plänen und Arbeiten mit Sicherungstresoren.

AWS Batch

AWS Dienst	Ressourcentyp „Value“	Beziehung	Verwandte Ressource
AWS Batch	`AWS::Batch::JobQueue`	N/A	N/A
	`AWS::Batch::ComputeEnvironment`	N/A	N/A
	`AWS::Batch::SchedulingPolicy`	N/A	N/A

AWS Budgets

AWS Bedienung	Ressourcentyp „Value“	Beziehung	Verwandte Ressource
AWS Budgets	`AWS::Budgets::BudgetsAction`	N/A	N/A

AWS Certificate Manager

AWS Bedienung	Ressourcentyp „Value“	Beziehung	Verwandte Ressource
AWS Certificate Manager	`AWS::ACM::Certificate`	N/A	N/A

AWS CloudFormation

AWS Bedienung	Ressourcentyp „Value“	Beziehung	Verwandte Ressource
AWS CloudFormation	`AWS::CloudFormation::Stack` *	enthält	Unterstützte AWS Ressourcentypen

*AWS Config zeichnet Konfigurationsänderungen an AWS CloudFormation Stacks und unterstützte Ressourcentypen in den Stacks auf. AWS Config zeichnet keine Konfigurationsänderungen für Ressourcentypen im Stack auf, die noch nicht unterstützt werden. Nicht unterstützte Ressourcentypen werden im zusätzlichen Konfigurationsbereich des Konfigurationselements für den Stack aufgezeichnet.

AWS CloudTrail

AWS Dienst	Ressourcentyp „Value“	Beziehung	Verwandte Ressource
AWS CloudTrail	`AWS::CloudTrail::Trail`	N/A	N/A

AWS Cloud9

AWS Bedienung	Ressourcentyp „Value“	Beziehung	Verwandte Ressource
AWS Cloud9	`AWS::Cloud9::EnvironmentEC2`	N/A	N/A

> **AWS Cloud9 Zugriff für neue Benutzer nicht mehr verfügbar**
>
> Nach reiflicher Überlegung haben wir beschlossen, den Zugang für Neukunden mit Wirkung zum AWS Cloud9 25. Juli 2024 zu schließen. AWS Cloud9 Bestandskunden können den Service weiterhin wie gewohnt nutzen. AWS investiert weiterhin in Sicherheit, Verfügbarkeit und Leistungsverbesserungen für AWS Cloud9, aber wir haben nicht vor, neue Funktionen einzuführen. Weitere Informationen finden Sie unter So migrieren Sie von AWS Cloud9 zu AWS IDE Toolkits oder AWS CloudShell.

AWS Cloud Map

AWS Dienst	Ressourcentyp „Value“	Beziehung	Verwandte Ressource
Service Discovery	`AWS::ServiceDiscovery::Service`	N/A	N/A
	`AWS::ServiceDiscovery::PublicDnsNamespace`	N/A	N/A
	`AWS::ServiceDiscovery::HttpNamespace`	N/A	N/A
`AWS::ServiceDiscovery::Instance`	N/A	N/A	

AWS CodeArtifact

AWS Bedienung	Ressourcentyp „Value“	Beziehung	Verwandte Ressource
AWS CodeArtifact	`AWS::CodeArtifact::Repository`	N/A	N/A

AWS CodeBuild

AWS Bedienung	Ressourcentyp „Value“	Beziehung	Verwandte Ressource
AWS CodeBuild	`AWS::CodeBuild::Project` *	ist zugeordnet zu	S3-Bucket
			IAM-Rolle
	`AWS::CodeBuild::ReportGroup`	N/A	N/A

* Weitere Informationen zur AWS Config Integration mit finden Sie AWS CodeBuild unter AWS Config Mit AWS CodeBuild Sample verwenden.

AWS CodeDeploy

AWS Dienst	Ressourcentyp „Value“	Beziehung	Verwandte Ressource
AWS CodeDeploy	`AWS::CodeDeploy::Application`	enthält	DeploymentGroup
	`AWS::CodeDeploy::DeploymentConfig`	N/A	N/A
	`AWS::CodeDeploy::DeploymentGroup`	ist enthalten in	Anwendung

AWS CodePipeline

AWS Bedienung	Ressourcentyp „Value“	Beziehung	Verwandte Ressource
AWS CodePipeline	`AWS::CodePipeline::Pipeline` *	ist angefügt an	S3 bucket
		ist zugeordnet zu	IAM-Rolle
			Codeprojekt
			Lambda-Funktion
			CloudFormation-Stack
			ElasticBeanstalk Anwendung

*AWS Config zeichnet Konfigurationsänderungen an CodePipeline Pipelines und unterstützte Ressourcentypen in den Pipelines auf. AWS Config zeichnet keine Konfigurationsänderungen für Ressourcentypen in den Pipelines auf, die noch nicht unterstützt werden. Nicht unterstützte Ressourcentypen wie `CodeCommit repository`, `CodeDeploy application`, `ECS cluster`, und `ECS service` werden im zusätzlichen Konfigurationsbereich des Konfigurationselements für den Stack aufgezeichnet.

AWS Config

AWS Dienst	Ressourcentyp „Value“	Beziehung	Verwandte Ressource
AWS Config	`AWS::Config::ResourceCompliance` *	ist zugeordnet zu	Alle Ressourcen*
	`AWS::Config::Confo`	N/A	N/A

AWS Dienst	Ressourcentyp „Value“	Beziehung	Verwandte Ressource
	`rmancePackCompliance`		
	`AWS::Config::ConfigurationRecorder` *	N/A	N/A

* Die Beziehung zwischen `AWS::Config::ResourceCompliance` und einer zugehörigen Ressource hängt davon ab, wie `AWS::Config::ResourceCompliance` die Compliance dieses spezifischen Ressourcentyps meldet.

* `AWS::Config::ConfigurationRecorder` ist ein Systemressourcentyp von AWS Config und die Aufzeichnung dieses Ressourcentyps ist standardmäßig aktiviert.

> **Note**
>
> Für die Aufzeichnung der Ressourcentypen `AWS::Config::ConformancePackCompliance` und `AWS::Config::ConfigurationRecorder` fallen keine zusätzlichen Kosten an.

AWS Database Migration Service

AWS Dienst	Ressourcentyp „Value“	Beziehung	Verwandte Ressource
AWS Database Migration Service	`AWS::DMS::EventSubscription`	N/A	N/A
	`AWS::DMS::ReplicationSubnetGroup`	N/A	N/A

AWS Dienst	Ressourcentyp „Value“	Beziehung	Verwandte Ressource
	`AWS::DMS::ReplicationInstance`	N/A	N/A
	`AWS::DMS::ReplicationTask`	N/A	N/A
	`AWS::DMS::Certificate`	N/A	N/A
	`AWS::DMS::Endpoint`	N/A	N/A

AWS DataSync

AWS Bedienung	Ressourcentyp „Value“	Beziehung	Verwandte Ressource
AWS DataSync	`AWS::DataSync::LocationSMB`	N/A	N/A
	`AWS::DataSync::LocationFSxLustre`	N/A	N/A
	`AWS::DataSync::LocationFSxWindows`	N/A	N/A

AWS Bedienung	Ressourcentyp „Value“	Beziehung	Verwandte Ressource
	`AWS::DataSync::LocationS3`	N/A	N/A
	`AWS::DataSync::LocationEFS`	N/A	N/A
	`AWS::DataSync::LocationNFS`	N/A	N/A
	`AWS::DataSync::LocationHDFS`	N/A	N/A
	`AWS::DataSync::LocationObjectStorage`	N/A	N/A
	`AWS::DataSync::Task`	N/A	N/A

AWS Device Farm

AWS Bedienung	Ressourcentyp „Value“	Beziehung	Verwandte Ressource
AWS Device Farm	`AWS::DeviceFarm::TestGridProject`	N/A	N/A

AWS Bedienung	Ressourcentyp „Value“	Beziehung	Verwandte Ressource
	`AWS::DeviceFarm::InstanceProfile`	N/A	N/A
	`AWS::DeviceFarm::Project`	N/A	N/A

AWS Elastic Beanstalk

AWS Bedienung	Ressourcentyp „Value“	Beziehung	Verwandte Ressource
AWS Elastic Beanstalk	`AWS::ElasticBeanstalk::Application`	enthält	Elastic Beanstalk-Anwendungsversion
			Elastic Beanstalk-Umgebung
		ist zugeordnet zu	IAM-Rolle
	`AWS::ElasticBeanstalk::ApplicationVersion`	ist enthalten in	Elastic Beanstalk-Anwendung
		ist zugeordnet zu	Elastic Beanstalk-Umgebung
			S3-Bucket
	`AWS::ElasticBeanstalk::Environment`	ist enthalten in	Elastic Beanstalk-Anwendung
		ist zugeordnet zu	Elastic Beanstalk-Anwendungsversion

AWS Bedienung	Ressourcentyp „Value“	Beziehung	Verwandte Ressource
			IAM-Rolle
		enthält	CloudFormation Stapel

AWS Fault Injection Service

AWS Bedienung	Ressourcentyp „Value“	Beziehung	Verwandte Ressource
AWS Fault Injection Service	`AWS::FIS::ExperimentTemplate`	N/A	N/A

AWS Global Accelerator

AWS Bedienung	Ressourcentyp „Value“	Beziehung	Verwandte Ressource
AWS Global Accelerator	`AWS::GlobalAccelerator::Listener`	N/A	N/A
	`AWS::GlobalAccelerator::EndpointGroup`	N/A	N/A
	`AWS::GlobalAccelerator::Accelerator`	N/A	N/A

AWS Glue

AWS Bedienung	Ressourcentyp „Value“	Beziehung	Verwandte Ressource
AWS Glue	`AWS::Glue::Job`	N/A	N/A
	`AWS::Glue::Classifier`	N/A	N/A
	`AWS::Glue::MLTransform`	N/A	N/A

AWS Ground Station

AWS Bedienung	Ressourcentyp „Value“	Beziehung	Verwandte Ressource
AWS Ground Station	`AWS::GroundStation::Config`	N/A	N/A
	`AWS::GroundStation::MissionProfile`	N/A	N/A
	`AWS::GroundStation::DataflowEndpointGroup`	N/A	N/A

AWS HealthLake

AWS Bedienung	Ressourcentyp „Value“	Beziehung	Verwandte Ressource
AWS HealthLake	`AWS::HealthLake::FHIRDatastore`	N/A	N/A

AWS Identity and Access Management (ICH BIN)

AWS Bedienung	Ressourcentyp „Value“	Beziehung	Verwandte Ressource
AWS Identity and Access Management	`AWS::IAM::User`	ist angefügt an	IAM-Gruppe
			Kundenverwaltete IAM-Richtlinie
	`AWS::IAM::Group`	enthält	IAM-Benutzer
		ist angefügt an	Kundenverwaltete IAM-Richtlinie
	`AWS::IAM::Role`	ist angefügt an	Kundenverwaltete IAM-Richtlinie
	`AWS::IAM::Policy`	ist angefügt an	IAM-Benutzer
			IAM-Gruppe
			IAM-Rolle
	`AWS::IAM::SAMLProvider`	N/A	N/A

AWS Bedienung	Ressourcentyp „Value“	Beziehung	Verwandte Ressource
	`AWS::IAM::ServerCertificate`	N/A	N/A
	`AWS::IAM::InstanceProfile`	N/A	N/A
	`AWS::IAM::OIDCProvider`	N/A	N/A
AWS Identity and Access Management Access Analyzer	`AWS::AccessAnalyzer::Analyzer`	N/A	N/A

AWS Config beinhaltet Inline-Richtlinien mit den Konfigurationsdetails, die er aufzeichnet. Weitere Informationen zu Inline-Richtlinien finden Sie unter Verwaltete Richtlinien und Inline-Richtlinien im IAM-Benutzerhandbuch.

AWS IoT

AWS Dienst	Ressourcentyp „Value“	Beziehung	Verwandte Ressource
AWS IoT	`AWS::IoT::Authorizer`	N/A	N/A
	`AWS::IoT::SecurityProfile`	N/A	N/A
	`AWS::IoT::RoleAlias`	N/A	N/A

AWS Dienst	Ressourcentyp „Value“	Beziehung	Verwandte Ressource
	`AWS::IoT::Dimension`	N/A	N/A
	`AWS::IoT::Policy`	N/A	N/A
	`AWS::IoT::MitigationAction`	N/A	N/A
	`AWS::IoT::ScheduledAudit`	N/A	N/A
	`AWS::IoT::AccountAuditConfiguration`	N/A	N/A
	`AWS::IoTSiteWise::Gateway`	N/A	N/A
	`AWS::IoT::CustomMetric`	N/A	N/A
	`AWS::IoT::JobTemplate`	N/A	N/A
	`AWS::IoT::ProvisioningTemplate`	N/A	N/A
	`AWS::IoT::CACertificate`	N/A	N/A

AWS Dienst	Ressourcentyp „Value“	Beziehung	Verwandte Ressource
AWS IoT Wireless	`AWS::IoTWireless::ServiceProfile`	N/A	N/A
	`AWS::IoTWireless::MulticastGroup`	N/A	N/A
	`AWS::IoTWireless::FuotaTask`	N/A	N/A
AWS IoT Core	`AWS::IoT::FleetMetric`	N/A	N/A
AWS IoT Analytics	`AWS::IoTAnalytics::Datastore`	N/A	N/A
	`AWS::IoTAnalytics::Dataset`	N/A	N/A
	`AWS::IoTAnalytics::Pipeline`	N/A	N/A
	`AWS::IoTAnalytics::Channel`	N/A	N/A
AWS IoT Events	`AWS::IoTEvents::Input`	N/A	N/A

AWS Dienst	Ressourcentyp „Value“	Beziehung	Verwandte Ressource
	`AWS::IoTEvents::DetectorModel`	N/A	N/A
	`AWS::IoTEvents::AlarmModel`	N/A	N/A
AWS IoT TwinMaker	`AWS::IoTTwinMaker::Workspace`	N/A	N/A
	`AWS::IoTTwinMaker::Entity`	N/A	N/A
	`AWS::IoTTwinMaker::Scene`	N/A	N/A
	`AWS::IoTTwinMaker::SyncJob`	N/A	N/A
	`AWS::IoTTwinMaker::ComponentType`	N/A	N/A
AWS IoT SiteWise	`AWS::IoTSiteWise::Dashboard`	N/A	N/A
	`AWS::IoTSiteWise::Project`	N/A	N/A

AWS Dienst	Ressourcentyp „Value“	Beziehung	Verwandte Ressource
	`AWS::IoTSiteWise::Portal`	N/A	N/A
	`AWS::IoTSiteWise::AssetModel`	N/A	N/A
AWS IoT Greengrass Version 2	`AWS::GreengrassV2::ComponentVersion`	N/A	N/A

AWS Key Management Service

AWS Bedienung	Ressourcentyp „Value“	Beziehung	Verwandte Ressource
AWS Key Management Service	`AWS::KMS::Key`	N/A	N/A
	`AWS::KMS::Alias`	N/A	N/A

AWS Lambda

AWS Bedienung	Ressourcentyp „Value“	Beziehung	Verwandte Ressource
AWS Lambda	`AWS::Lambda::Function`	ist zugeordnet zu	IAM-Rolle
			EC2 Sicherheitsgruppe
		ist enthalten in	EC2 Subnetz

AWS Bedienung	Ressourcentyp „Value“	Beziehung	Verwandte Ressource
	`AWS::Lambda::CodeSigningConfig`	N/A	N/A

AWS Mainframe Modernization

AWS Dienst	Ressourcentyp „Value“	Beziehung	Verwandte Ressource
AWS Mainframe Modernization	`AWS::M2::Environment`	N/A	N/A

AWS Network Firewall

AWS Bedienung	Ressourcentyp „Value“	Beziehung	Verwandte Ressource
AWS Network Firewall	`AWS::NetworkFirewall::Firewall`	ist angefügt an	EC2 Subnetz
		ist zugeordnet zu	NetworkFirewall FirewallPolicy
	`AWS::NetworkFirewall::FirewallPolicy`	ist zugeordnet zu	NetworkFirewall RuleGroup
	`AWS::NetworkFirewall::RuleGroup`	N/A	N/A
	`AWS::NetworkFirewa`	N/A	N/A

AWS Bedienung	Ressourcentyp „Value“	Beziehung	Verwandte Ressource
	`ll::TLSInspectionConfiguration`		
	`AWS::NetworkFirewall::VpcEndpointAssociation`	N/A	N/A

AWS Network Manager

AWS Dienst	Ressourcentyp „Value“	Beziehung	Verwandte Ressource
AWS Network Manager	`AWS::NetworkManager::TransitGatewayRegistration`	N/A	N/A
	`AWS::NetworkManager::Site`	N/A	N/A
	`AWS::NetworkManager::Device`	N/A	N/A
	`AWS::NetworkManager::Link`	N/A	N/A

AWS Dienst	Ressourcentyp „Value“	Beziehung	Verwandte Ressource
	`AWS::NetworkManager::GlobalNetwork`	N/A	N/A
	`AWS::NetworkManager::CustomerGatewayAssociation`	N/A	N/A
	`AWS::NetworkManager::LinkAssociation`	N/A	N/A
	`AWS::NetworkManager::ConnectPeer`	N/A	N/A

AWS Panorama

AWS Bedienung	Ressourcentyp „Value“	Beziehung	Verwandte Ressource
AWS Panorama	`AWS::Panorama::Package`	N/A	N/A

AWS Private Certificate Authority

AWS Bedienung	Ressourcentyp „Value“	Beziehung	Verwandte Ressource
AWS Private Certificate Authority	`AWS::ACMPCA::CertificateAuthority`	N/A	N/A
	`AWS::ACMPCA::CertificateAuthorityActivation`	N/A	N/A

AWS Resilience Hub

AWS Bedienung	Ressourcentyp „Value“	Beziehung	Verwandte Ressource
AWS Resilience Hub	`AWS::ResilienceHub::ResiliencyPolicy`	N/A	N/A
	`AWS::ResilienceHub::App`	N/A	N/A

AWS Ressourcen Explorer

AWS Bedienung	Ressourcentyp „Value“	Beziehung	Verwandte Ressource
AWS Ressourcen Explorer	`AWS::ResourceExplorer2::Index`	N/A	N/A

AWS RoboMaker

AWS Bedienung	Ressourcentyp „Value“	Beziehung	Verwandte Ressource
AWS RoboMaker	`AWS::RoboMaker::RobotApplicationVersion`	N/A	N/A
	`AWS::RoboMaker::RobotApplication`	N/A	N/A
	`AWS::RoboMaker::SimulationApplication`	N/A	N/A

AWS Signer

AWS Bedienung	Ressourcentyp „Value“	Beziehung	Verwandte Ressource
AWS Signer	`AWS::Signer::SigningProfile`	N/A	N/A

AWS Secrets Manager

AWS Bedienung	Ressourcentyp „Value“	Beziehung	Verwandte Ressource
AWS Secrets Manager	`AWS::SecretsManager::Secret`	ist zugeordnet zu	Lambda-Funktion
		ist zugeordnet zu	KMS-Schlüssel

AWS Security Hub

AWS Bedienung	Ressourcentyp „Value“	Beziehung	Verwandte Ressource
AWS Security Hub	`AWS::SecurityHub::Standard`	N/A	N/A

AWS Service Catalog

AWS Bedienung	Ressourcentyp „Value“	Beziehung	Verwandte Ressource
AWS Service Catalog	`AWS::ServiceCatalo`	ist enthalten in	Portfolio

AWS Bedienung	Ressourcentyp „Value“	Beziehung	Verwandte Ressource
	`g::CloudFormationProduct`	ist zugeordnet zu	CloudFormationProvisionedProduct
	`AWS::ServiceCatalog::CloudFormationProvisionedProduct`	ist zugeordnet zu	Portfolio
			CloudFormationProduct
			CloudFormationStack
	`AWS::ServiceCatalog::Portfolio`	enthält	CloudFormationProduct

AWS Shield

AWS Bedienung	Ressourcentyp „Value“	Beziehung	Verwandte Ressource
AWS Shield	`AWS::Shield::Protection`	ist zugeordnet zu	CloudFront Amazon-Vertrieb
	`AWS::ShieldRegional::Protection`	ist zugeordnet zu	EC2 EIP
		ist zugeordnet zu	ElasticLoadBalancing Balancer
		ist zugeordnet zu	ElasticLoadBalancingV2 LoadBalancer

AWS Step Functions

AWS Bedienung	Ressourcentyp „Value“	Beziehung	Verwandte Ressource
AWS Step Functions	`AWS::StepFunctions::Activity`	N/A	N/A
	`AWS::StepFunctions::StateMachine`	N/A	N/A

AWS Systems Manager

AWS Bedienung	Ressourcentyp „Value“	Beziehung	Verwandte Ressource
AWS Systems Manager	`AWS::SSM::ManagedInstanceInventory` *	ist zugeordnet zu	EC2 Instanz
	`AWS::SSM::PatchCompliance`	ist zugeordnet zu	Verwalteter Instance-Bestand
	`AWS::SSM::AssociationCompliance`	ist zugeordnet zu	Verwalteter Instance-Bestand
	`AWS::SSM::FileData`	ist zugeordnet zu	Verwalteter Instance-Bestand
	`AWS::SSM::Document`	N/A	N/A

*Weitere Informationen zum verwalteten Instance-Bestand finden Sie unter Recording Software Configuration for Managed Instances.

AWS Transfer Family

AWS Dienst	Ressourcentyp „Value“	Beziehung	Verwandte Ressource
AWS Transfer Family	`AWS::Transfer::Agreement`	N/A	N/A
	`AWS::Transfer::Connector`	N/A	N/A
	`AWS::Transfer::Workflow`	N/A	N/A
	`AWS::Transfer::Certificate`	N/A	N/A
	`AWS::Transfer::Profile`	N/A	N/A

AWS WAF

AWS Bedienung	Ressourcentyp „Value“	Beziehung	Verwandte Ressource
AWS WAF	`AWS::WAF::RateBasedRule`	N/A	N/A
	`AWS::WAF::Rule`	N/A	N/A
	`AWS::WAF::WebACL`	ist zugeordnet zu	WAF-Regel

AWS Bedienung	Ressourcentyp „Value“	Beziehung	Verwandte Ressource
			Ratenbasierte WAF-Regel
			WAF-Regelgruppe
	`AWS::WAF::RuleGroup`	ist zugeordnet zu	WAF-Regel
	`AWS::WAFRegional::RateBasedRule`	N/A	N/A
	`AWS::WAFRegional::Rule`	N/A	N/A
	`AWS::WAFRegional::WebACL`	ist zugeordnet zu	ElasticLoadBalancingV2 LoadBalancer
			WAFRegional Regel
			WAFRegional ratenbasierte Regel
			WAFRegional Regelgruppe
	`AWS::WAFRegional::RuleGroup`	ist zugeordnet zu	WAFRegional Regel
AWS WAF V2	`AWS::WAFv2::WebACL`	ist zugeordnet zu	ElasticLoadBalancingV2 LoadBalancer
			ApiGateway Stufe
			WAFv2 IPSet

AWS Bedienung	Ressourcentyp „Value“	Beziehung	Verwandte Ressource
			WAFv2 RegexPatternSet
			WAFv2 RuleGroup
			WAFv2 ManagedRuleSet
	`AWS::WAFv2::RuleGroup`	ist zugeordnet zu	WAFv2 IPSet
			WAFv2 RegexPatternSet
	`AWS::WAFv2::ManagedRuleSet`	ist zugeordnet zu	WAFv2 RuleGroup
	`AWS::WAFv2::IPSet`	N/A	N/A
	`AWS::WAFv2::RegexPatternSet`	N/A	N/A

AWS X-Ray

AWS Bedienung	Ressourcentyp „Value“	Beziehung	Verwandte Ressource
AWS X-Ray	`AWS::XRay::EncryptionConfig`	N/A	N/A

Elastic Load Balancing

AWS Bedienung	Ressourcentyp „Value“	Beziehung	Verwandte Ressource
Elastic Load Balancing	Application Load Balancer `AWS::ElasticLoadBalancingV2::LoadBalancer`	ist zugeordnet zu	EC2 Sicherheitsgruppe
		ist angefügt an	Subnetz
		ist enthalten in	Virtual Private Cloud (VPC)
	Listener für Application Load Balancer `AWS::ElasticLoadBalancingV2::Listener`	N/A	N/A
	Classic Load Balancer `AWS::ElasticLoadBalancing::LoadBalancer`	ist zugeordnet zu	EC2 Sicherheitsgruppe
		ist angefügt an	Subnetz
		ist enthalten in	Virtual Private Cloud (VPC)
	Network Load Balancer `AWS::ElasticLoadBalancingV2::LoadBalancer`	N/A	N/A

AWS Elemental MediaConnect

AWS Dienst	Ressourcentyp „Value“	Beziehung	Verwandte Ressource
AWS Elemental MediaConnect	`AWS::MediaConnect::FlowEntitlement`	N/A	N/A
	`AWS::MediaConnect::FlowVpcInterface`	N/A	N/A
	`AWS::MediaConnect::FlowSource`	N/A	N/A
	`AWS::MediaConnect::Gateway`	N/A	N/A

AWS Elemental MediaPackage

AWS Bedienung	Ressourcentyp „Value“	Beziehung	Verwandte Ressource
AWS Elemental MediaPackage	`AWS::MediaPackage::PackagingGroup`	N/A	N/A
	`AWS::MediaPackage:`	N/A	N/A

AWS Bedienung	Ressourcentyp „Value“	Beziehung	Verwandte Ressource
	`:PackagingConfiguration`		

AWS Elemental MediaTailor

AWS Bedienung	Ressourcentyp „Value“	Beziehung	Verwandte Ressource
AWS Elemental MediaTailor	`AWS::MediaTailor::PlaybackConfiguration`	N/A	N/A

Ressourcenabdeckung nach regionaler Verfügbarkeit

Regionen Nord- und Südamerika

Ressourcentyp	USA West (Nordkalifornien)	USA Ost (Nord-Virginia)	USA West (Oregon)	USA Ost (Ohio)	Kanada West (Calgary)	Kanada (Zentral)	Mexiko (Zentral)	Südamerika (São Paulo)
AWS::ACM::Certificate	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja
AWS::ACMPCA::CertificateAuthority	Ja	Ja	Ja	Ja	Ja	Ja	Nein	Ja
AWS::ACMPCA::CertificateAuthorityAktivierung	Ja	Ja	Ja	Ja	Ja	Ja	Nein	Ja

Ressourcentyp	USA West (Nordkalifornien)	USA Ost (Nord-Virginia)	USA West (Oregon)	USA Ost (Ohio)	Kanada West (Calgary)	Kanada (Zentral)	Mexiko (Zentral)	Südamerika (São Paulo)
AWS::APS::RuleGroupsNamespace	Nein	Ja	Ja	Ja	Nein	Nein	Nein	Ja
AWS::AccessAnalyzer::Analyzer	Ja	Ja	Ja	Ja	Ja	Ja	Nein	Ja
AWS::AmazonMQ::Broker	Ja	Ja	Ja	Ja	Nein	Ja	Nein	Ja
AWS::Amplify::App	Ja	Ja	Ja	Ja	Nein	Ja	Nein	Ja
AWS::Amplify::Branch	Ja	Ja	Ja	Ja	Nein	Ja	Nein	Ja
AWS::ApiGateway::RestApi	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja
AWS::ApiGateway::Stage	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja
AWS::ApiGatewayV2::Api	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja
AWS::ApiGatewayV2::Stage	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja
AWS::AppConfig::Application	Ja	Ja	Ja	Ja	Nein	Ja	Nein	Ja
AWS::AppConfig::ConfigurationProfile	Ja	Ja	Ja	Ja	Nein	Ja	Nein	Ja

Ressourcentyp	USA West (Nordkalifornien)	USA Ost (Nord-Virginia)	USA West (Oregon)	USA Ost (Ohio)	Kanada West (Calgary)	Kanada (Zentral)	Mexiko (Zentral)	Südamerika (São Paulo)
AWS::AppConfig::DeploymentStrategy	Ja	Ja	Ja	Ja	Ja	Ja	Nein	Ja
AWS::AppConfig::Environment	Ja	Ja	Ja	Ja	Nein	Ja	Nein	Ja
AWS::AppConfig::ExtensionAssociation	Ja	Ja	Ja	Ja	Ja	Ja	Nein	Ja
AWS::AppConfig::HostedConfigurationVersion	Ja	Ja	Ja	Ja	Nein	Ja	Nein	Ja
AWS::AppFlow::Flow	Ja	Ja	Ja	Ja	Nein	Ja	Nein	Ja
AWS::AppIntegrations::Application	Nein	Ja	Ja	Nein	Nein	Ja	Nein	Nein
AWS::AppIntegrations::EventIntegration	Nein	Ja	Ja	Nein	Nein	Ja	Nein	Nein
AWS::AppMesh::GatewayRoute	Ja	Ja	Ja	Ja	Nein	Ja	Nein	Ja
AWS::AppMesh::Mesh	Ja	Ja	Ja	Ja	Nein	Ja	Nein	Ja
AWS::AppMesh::Route	Ja	Ja	Ja	Ja	Nein	Ja	Nein	Ja
AWS::AppMesh::VirtualGateway	Ja	Ja	Ja	Ja	Nein	Ja	Nein	Ja

Ressourcentyp	USA West (Nordkalifornien)	USA Ost (Nord-Virginia)	USA West (Oregon)	USA Ost (Ohio)	Kanada West (Calgary)	Kanada (Zentral)	Mexiko (Zentral)	Südamerika (São Paulo)
AWS::AppMesh::VirtualNode	Ja	Ja	Ja	Ja	Nein	Ja	Nein	Ja
AWS::AppMesh::VirtualRouter	Ja	Ja	Ja	Ja	Nein	Ja	Nein	Ja
AWS::AppMesh::VirtualService	Ja	Ja	Ja	Ja	Nein	Ja	Nein	Ja
AWS::AppRunner::Service	Nein	Ja	Ja	Ja	Nein	Nein	Nein	Nein
AWS::AppRunner::VpcConnector	Nein	Ja	Ja	Ja	Nein	Nein	Nein	Nein
AWS::AppStream::Application	Nein	Ja	Ja	Ja	Nein	Ja	Nein	Ja
AWS::AppStream::DirectoryConfig	Nein	Ja	Ja	Ja	Nein	Ja	Nein	Ja
AWS::AppStream::Fleet	Nein	Ja	Ja	Ja	Nein	Ja	Nein	Nein
AWS::AppStream::Stack	Nein	Ja	Ja	Ja	Nein	Ja	Nein	Nein
AWS::AppSync::ApiCache	Ja	Ja	Ja	Ja	Nein	Ja	Nein	Ja
AWS::AppSync::GraphQLApi	Ja	Ja	Ja	Ja	Nein	Ja	Nein	Ja

Ressourcentyp	USA West (Nordkalifornien)	USA Ost (Nord-Virginia)	USA West (Oregon)	USA Ost (Ohio)	Kanada West (Calgary)	Kanada (Zentral)	Mexiko (Zentral)	Südamerika (São Paulo)
AWS::Athena::DataCatalog	Ja	Ja	Ja	Ja	Ja	Ja	Nein	Ja
AWS::Athena::PreparedStatement	Ja	Ja	Ja	Ja	Ja	Ja	Nein	Ja
AWS::Athena::WorkGroup	Ja	Ja	Ja	Ja	Ja	Ja	Nein	Ja
AWS::AuditManager::Assessment	Ja	Ja	Ja	Ja	Nein	Ja	Nein	Nein
AWS::AutoScaling::AutoScalingGruppe	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja
AWS::AutoScaling::LaunchConfiguration	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja
AWS::AutoScaling::ScalingPolicy	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja
AWS::AutoScaling::ScheduledAction	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja
AWS::AutoScaling::WarmPool	Ja	Ja	Ja	Ja	Nein	Ja	Nein	Ja
AWS::Backup::BackupPlan	Ja	Ja	Ja	Ja	Ja	Ja	Nein	Ja
AWS::Backup::BackupSelection	Ja	Ja	Ja	Ja	Ja	Ja	Nein	Ja

Ressourcentyp	USA West (Nordkalifornien)	USA Ost (Nord-Virginia)	USA West (Oregon)	USA Ost (Ohio)	Kanada West (Calgary)	Kanada (Zentral)	Mexiko (Zentral)	Südamerika (São Paulo)
AWS::Backup::BackupVault	Ja	Ja	Ja	Ja	Ja	Ja	Nein	Ja
AWS::Backup::RecoveryPoint	Ja	Ja	Ja	Ja	Ja	Ja	Nein	Ja
AWS::Backup::ReportPlan	Ja	Ja	Ja	Ja	Nein	Ja	Nein	Ja
AWS::Batch::ComputeEnvironment	Ja	Ja	Ja	Ja	Nein	Ja	Nein	Ja
AWS::Batch::JobQueue	Ja	Ja	Ja	Ja	Nein	Ja	Nein	Ja
AWS::Batch::SchedulingPolicy	Ja	Ja	Ja	Ja	Ja	Ja	Nein	Ja
AWS::Bedrock::Guardrail	Nein	Ja	Ja	Ja	Nein	Ja	Nein	Ja
AWS::Bedrock::KnowledgeBase	Nein	Ja	Ja	Ja	Nein	Ja	Nein	Ja
AWS::Budgets::BudgetsAction	Nein	Ja	Nein	Nein	Nein	Nein	Nein	Nein
AWS::Cassandra::Keyspace	Ja	Ja	Ja	Ja	Nein	Ja	Nein	Ja
AWS::Cloud9::EnvironmentEC2	Ja	Ja	Ja	Ja	Nein	Ja	Nein	Ja

Ressourcentyp	USA West (Nordkalifornien)	USA Ost (Nord-Virginia)	USA West (Oregon)	USA Ost (Ohio)	Kanada West (Calgary)	Kanada (Zentral)	Mexiko (Zentral)	Südamerika (São Paulo)
AWS::CloudFormation::Stack	Ja	Ja	Ja	Ja	Nein	Ja	Nein	Ja
AWS::CloudFront::Distribution	Nein	Ja	Nein	Nein	Nein	Nein	Nein	Nein
AWS::CloudFront::StreamingDistribution	Nein	Ja	Nein	Nein	Nein	Nein	Nein	Nein
AWS::CloudTrail::Trail	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja
AWS::CloudWatch::Alarm	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja
AWS::CloudWatch::MetricStream	Ja	Ja	Ja	Ja	Nein	Ja	Nein	Ja
AWS::CodeArtifact::Repository	Nein	Ja	Ja	Ja	Nein	Nein	Nein	Nein
AWS::CodeBuild::Project	Ja	Ja	Ja	Ja	Nein	Ja	Nein	Ja
AWS::CodeBuild::ReportGroup	Ja	Ja	Ja	Ja	Nein	Ja	Nein	Ja
AWS::CodeDeploy::Application	Ja	Ja	Ja	Ja	Nein	Ja	Nein	Ja
AWS::CodeDeploy::DeploymentConfig	Ja	Ja	Ja	Ja	Nein	Ja	Nein	Ja

Ressourcentyp	USA West (Nordkalifornien)	USA Ost (Nord-Virginia)	USA West (Oregon)	USA Ost (Ohio)	Kanada West (Calgary)	Kanada (Zentral)	Mexiko (Zentral)	Südamerika (São Paulo)
AWS::CodeDeploy::DeploymentGroup	Ja	Ja	Ja	Ja	Nein	Ja	Nein	Ja
AWS::CodeGuruProfiler::ProfilingGroup	Nein	Ja	Ja	Ja	Nein	Nein	Nein	Nein
AWS::CodeGuruReviewer::RepositoryAssociation	Nein	Ja	Ja	Ja	Nein	Nein	Nein	Nein
AWS::CodePipeline::Pipeline	Ja	Ja	Ja	Ja	Nein	Ja	Nein	Ja
AWS::Cognito::IdentityPool	Ja	Ja	Ja	Ja	Ja	Ja	Nein	Ja
AWS::Cognito::UserPool	Ja	Ja	Ja	Ja	Ja	Ja	Nein	Ja
AWS::Cognito::UserPoolKlient	Ja	Ja	Ja	Ja	Ja	Ja	Nein	Ja
AWS::Cognito::UserPoolGruppe	Ja	Ja	Ja	Ja	Ja	Ja	Nein	Ja
AWS::Config::ConfigurationRecorder	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja
AWS::Config::ConformancePack-Compliance	Ja	Ja	Ja	Ja	Ja	Ja	Nein	Ja
AWS::Config::ResourceCompliance	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja

Ressourcentyp	USA West (Nordkalifornien)	USA Ost (Nord-Virginia)	USA West (Oregon)	USA Ost (Ohio)	Kanada West (Calgary)	Kanada (Zentral)	Mexiko (Zentral)	Südamerika (São Paulo)
AWS::Connect::Instance	Nein	Ja	Ja	Nein	Nein	Ja	Nein	Nein
AWS::Connect::PhoneNumber	Nein	Ja	Ja	Nein	Nein	Ja	Nein	Nein
AWS::Connect::QuickConnect	Nein	Ja	Ja	Nein	Nein	Ja	Nein	Nein
AWS::Connect::Rule	Nein	Ja	Ja	Nein	Nein	Ja	Nein	Nein
AWS::Connect::User	Nein	Ja	Ja	Nein	Nein	Ja	Nein	Nein
AWS::CustomerProfiles::Domain	Nein	Ja	Ja	Nein	Nein	Ja	Nein	Nein
AWS::CustomerProfiles::ObjectType	Nein	Ja	Ja	Nein	Nein	Ja	Nein	Nein
AWS::DMS::Certificate	Ja	Ja	Ja	Ja	Nein	Ja	Nein	Ja
AWS::DMS::Endpoint	Ja	Ja	Ja	Ja	Nein	Ja	Nein	Ja
AWS::DMS::EventSubscription	Ja	Ja	Ja	Ja	Nein	Ja	Nein	Ja
AWS::DMS::ReplicationInstance	Ja	Ja	Ja	Ja	Nein	Ja	Nein	Ja

Ressourcentyp	USA West (Nordkalifornien)	USA Ost (Nord-Virginia)	USA West (Oregon)	USA Ost (Ohio)	Kanada West (Calgary)	Kanada (Zentral)	Mexiko (Zentral)	Südamerika (São Paulo)
AWS::DMS::ReplicationSubnetGruppe	Ja	Ja	Ja	Ja	Nein	Ja	Nein	Ja
AWS::DMS::ReplicationTask	Ja	Ja	Ja	Ja	Nein	Ja	Nein	Ja
AWS::DataSync::LocationEFS	Ja	Ja	Ja	Ja	Nein	Ja	Nein	Ja
AWS::DataSync::LocationFSxGlanz	Ja	Ja	Ja	Ja	Nein	Ja	Nein	Ja
AWS::DataSync::LocationFSxFenster	Ja	Ja	Ja	Ja	Nein	Ja	Nein	Ja
AWS::DataSync::LocationHDFS	Ja	Ja	Ja	Ja	Nein	Ja	Nein	Ja
AWS::DataSync::LocationNFS	Ja	Ja	Ja	Ja	Nein	Ja	Nein	Ja
AWS::DataSync::LocationObjectSpeicher	Ja	Ja	Ja	Ja	Nein	Ja	Nein	Ja
AWS::DataSync::LocationS 3	Ja	Ja	Ja	Ja	Ja	Ja	Nein	Ja
AWS::DataSync::LocationSMB	Ja	Ja	Ja	Ja	Nein	Ja	Nein	Ja
AWS::DataSync::Task	Ja	Ja	Ja	Ja	Ja	Ja	Nein	Ja

Ressourcentyp	USA West (Nordkalifornien)	USA Ost (Nord-Virginia)	USA West (Oregon)	USA Ost (Ohio)	Kanada West (Calgary)	Kanada (Zentral)	Mexiko (Zentral)	Südamerika (São Paulo)
AWS::Detective::Graph	Ja	Ja	Ja	Ja	Nein	Ja	Nein	Ja
AWS::DeviceFarm::InstanceProfile	Nein	Nein	Ja	Nein	Nein	Nein	Nein	Nein
AWS::DeviceFarm::Project	Nein	Nein	Ja	Nein	Nein	Nein	Nein	Nein
AWS::DeviceFarm::TestGridProjekt	Nein	Nein	Ja	Nein	Nein	Nein	Nein	Nein
AWS::DynamoDB::Table	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja
AWS::EC2::Capacity Reservation	Ja	Ja	Ja	Ja	Ja	Ja	Nein	Ja
AWS::EC2::CarrierGateway	Nein	Ja	Ja	Ja	Nein	Ja	Nein	Nein
AWS::EC2::ClientVpnEndpunkt	Ja	Ja	Ja	Ja	Nein	Ja	Nein	Ja
AWS::EC2::ClientVpnTargetNetworkAssociation	Ja	Ja	Ja	Ja	Nein	Ja	Nein	Ja
AWS::EC2::CustomerGateway	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja
AWS:EC2:: DHCPOptions	Ja	Ja	Ja	Ja	Ja	Ja	Nein	Ja

Ressourcentyp	USA West (Nordkalifornien)	USA Ost (Nord-Virginia)	USA West (Oregon)	USA Ost (Ohio)	Kanada West (Calgary)	Kanada (Zentral)	Mexiko (Zentral)	Südamerika (São Paulo)
AWS:EC2:: EC2 Flotte	Ja	Ja	Ja	Ja	Nein	Ja	Nein	Ja
AWS::EC2: EIP	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja
AWS:EC2:: EIPAssociation	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja
AWS::EC2::EgressOnlyInternetGateway	Ja	Ja	Ja	Ja	Nein	Ja	Nein	Ja
AWS::EC2::FlowLog	Ja	Ja	Ja	Ja	Nein	Ja	Nein	Ja
AWS::EC2::Host	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja
AWS:::EC2: IPAM	Ja	Ja	Ja	Ja	Nein	Ja	Nein	Ja
AWS:EC2:: IPAMPool	Ja	Ja	Ja	Ja	Nein	Ja	Nein	Ja
AWS:EC2:: IPAMResource Entdeckung	Ja	Ja	Ja	Ja	Nein	Ja	Nein	Ja
AWS:EC2:: IPAMResource DiscoveryAssociation	Ja	Ja	Ja	Ja	Nein	Ja	Nein	Ja
AWS:EC2:: IPAMScope	Ja	Ja	Ja	Ja	Nein	Ja	Nein	Ja

Ressourcentyp	USA West (Nordkalifornien)	USA Ost (Nord-Virginia)	USA West (Oregon)	USA Ost (Ohio)	Kanada West (Calgary)	Kanada (Zentral)	Mexiko (Zentral)	Südamerika (São Paulo)
AWS::EC2::Instance	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja
AWS::EC2::Instance ConnectEndpunkt	Ja	Ja	Ja	Ja	Ja	Ja	Nein	Ja
AWS::EC2::InternetGateway	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja
AWS::EC2::LaunchTemplate	Ja	Ja	Ja	Ja	Nein	Ja	Nein	Ja
AWS::EC2::NatGateway	Ja	Ja	Ja	Ja	Nein	Ja	Nein	Ja
AWS::EC2::NetworkAcl	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja
AWS::EC2::NetworkInsightsAccessScope	Ja	Ja	Ja	Ja	Nein	Ja	Nein	Ja
AWS::EC2::NetworkInsightsAccessScopeAnalysis	Ja	Ja	Ja	Ja	Nein	Ja	Nein	Ja
AWS::EC2::NetworkInsightsAnalyse	Ja	Ja	Ja	Ja	Nein	Ja	Nein	Ja
AWS::EC2::NetworkInsightsPfad	Ja	Ja	Ja	Ja	Nein	Ja	Nein	Ja
AWS::EC2::NetworkInterface	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja

Ressourcentyp	USA West (Nordkalifornien)	USA Ost (Nord-Virginia)	USA West (Oregon)	USA Ost (Ohio)	Kanada West (Calgary)	Kanada (Zentral)	Mexiko (Zentral)	Südamerika (São Paulo)
AWS::EC2::PrefixList	Ja	Ja	Ja	Ja	Ja	Ja	Nein	Ja
AWS::EC2::RegisteredHAInstance	Ja	Ja	Ja	Ja	Nein	Ja	Nein	Ja
AWS::EC2::RouteTable	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja
AWS::EC2::SecurityGroup	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja
AWS::EC2::SnapshotBlockPublicAccess	Ja	Ja	Ja	Ja	Ja	Ja	Nein	Ja
AWS::EC2::SpotFleet	Ja	Ja	Ja	Ja	Ja	Ja	Nein	Ja
AWS::EC2::Subnet	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja
AWS::EC2::SubnetRouteTableAssociation	Ja	Ja	Ja	Ja	Nein	Ja	Nein	Ja
AWS::EC2::TrafficMirrorFilter	Ja	Ja	Ja	Ja	Ja	Ja	Nein	Ja
AWS::EC2::TrafficMirrorSitzung	Ja	Ja	Ja	Ja	Nein	Ja	Nein	Ja
AWS::EC2::TrafficMirrorZiel	Ja	Ja	Ja	Ja	Nein	Ja	Nein	Ja

Ressourcentyp	USA West (Nordkalifornien)	USA Ost (Nord-Virginia)	USA West (Oregon)	USA Ost (Ohio)	Kanada West (Calgary)	Kanada (Zentral)	Mexiko (Zentral)	Südamerika (São Paulo)
AWS::EC2::TransitGateway	Ja	Ja	Ja	Ja	Ja	Ja	Nein	Ja
AWS::EC2::TransitGatewayAnlage	Ja	Ja	Ja	Ja	Nein	Ja	Nein	Ja
AWS::EC2::TransitGatewayConnect	Ja	Ja	Ja	Ja	Nein	Ja	Nein	Ja
AWS::EC2::TransitGatewayMulticastDomain	Ja	Ja	Ja	Ja	Ja	Ja	Nein	Ja
AWS::EC2::TransitGatewayRouteTable	Ja	Ja	Ja	Ja	Nein	Ja	Nein	Ja
AWS:EC2: :VPC	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja
AWS:EC2:: VPCBlockPublicAccessExclusion	Ja	Ja	Ja	Ja	Ja	Ja	Nein	Ja
AWS:EC2:: VPCBlockPublicAccessOptions	Ja	Ja	Ja	Ja	Ja	Ja	Nein	Ja
AWS:EC2:: VPCEndpoint	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja
AWS:EC2:: VPCEndpoint ConnectionNotification	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja
AWS:EC2:: VPCEndpoint Dienst	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja

Ressourcentyp	USA West (Nordkalifornien)	USA Ost (Nord-Virginia)	USA West (Oregon)	USA Ost (Ohio)	Kanada West (Calgary)	Kanada (Zentral)	Mexiko (Zentral)	Südamerika (São Paulo)
AWS::EC2:: VPCPeering Verbindung	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja
AWS:EC2:: VPNConnection	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja
AWS::EC2:: VPNConnection Route	Ja	Ja	Ja	Ja	Ja	Ja	Nein	Ja
AWS:EC2:: VPNGateway	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja
AWS::EC2::Volume	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja
AWS::ECR::PublicRepository	Nein	Ja	Nein	Nein	Nein	Nein	Nein	Nein
AWS::ECR::PullThroughCacheRule	Ja	Ja	Ja	Ja	Ja	Ja	Nein	Ja
AWS::ECR::RegistryPolicy	Ja	Ja	Ja	Ja	Ja	Ja	Nein	Ja
AWS::ECR::Repository	Ja	Ja	Ja	Ja	Ja	Ja	Nein	Ja
AWS::ECS::CapacityProvider	Ja	Ja	Ja	Ja	Ja	Ja	Nein	Ja
AWS::ECS::Cluster	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja

Ressourcentyp	USA West (Nordkalifornien)	USA Ost (Nord-Virginia)	USA West (Oregon)	USA Ost (Ohio)	Kanada West (Calgary)	Kanada (Zentral)	Mexiko (Zentral)	Südamerika (São Paulo)
AWS::ECS::Service	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja
AWS::ECS::TaskDefinition	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja
AWS::ECS::TaskSet	Ja	Ja	Ja	Ja	Nein	Ja	Nein	Ja
AWS::EFS::AccessPoint	Ja	Ja	Ja	Ja	Ja	Ja	Nein	Ja
AWS::EFS::FileSystem	Ja	Ja	Ja	Ja	Ja	Ja	Nein	Ja
AWS::EKS::Addon	Ja	Ja	Ja	Ja	Nein	Ja	Nein	Ja
AWS::EKS::Cluster	Ja	Ja	Ja	Ja	Nein	Ja	Nein	Ja
AWS::EKS::FargateProfile	Ja	Ja	Ja	Ja	Nein	Ja	Nein	Ja
AWS::EKS::IdentityProviderConfig	Ja	Ja	Ja	Ja	Nein	Ja	Nein	Ja
AWS::EMR::SecurityConfiguration	Ja	Ja	Ja	Ja	Ja	Ja	Nein	Ja
AWS::ElasticBeanstalk::Application	Ja	Ja	Ja	Ja	Nein	Ja	Nein	Ja

Ressourcentyp	USA West (Nordkalifornien)	USA Ost (Nord-Virginia)	USA West (Oregon)	USA Ost (Ohio)	Kanada West (Calgary)	Kanada (Zentral)	Mexiko (Zentral)	Südamerika (São Paulo)
AWS::ElasticBeanstalk::ApplicationVersion	Ja	Ja	Ja	Ja	Nein	Ja	Nein	Ja
AWS::ElasticBeanstalk::Environment	Ja	Ja	Ja	Ja	Nein	Ja	Nein	Ja
AWS::ElasticLoadBalancing::LoadBalancer	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja
AWS::ElasticLoadBalancingV2::Listener	Ja	Ja	Ja	Ja	Nein	Ja	Nein	Ja
AWS::ElasticLoadBalancingV2::LoadBalancer	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja
AWS::Elasticsearch::Domain	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja
AWS::EventSchemas::Discoverer	Ja	Ja	Ja	Ja	Nein	Ja	Nein	Ja
AWS::EventSchemas::Registry	Ja	Ja	Ja	Ja	Nein	Ja	Nein	Ja
AWS::EventSchemas::RegistryPolicy	Ja	Ja	Ja	Ja	Nein	Ja	Nein	Ja
AWS::EventSchemas::Schema	Ja	Ja	Ja	Ja	Nein	Ja	Nein	Ja
AWS::Events::ApiDestination	Ja	Ja	Ja	Ja	Nein	Ja	Nein	Ja

Ressourcentyp	USA West (Nordkalifornien)	USA Ost (Nord-Virginia)	USA West (Oregon)	USA Ost (Ohio)	Kanada West (Calgary)	Kanada (Zentral)	Mexiko (Zentral)	Südamerika (São Paulo)
AWS::Events::Archive	Ja	Ja	Ja	Ja	Nein	Ja	Nein	Ja
AWS::Events::Connection	Ja	Ja	Ja	Ja	Nein	Ja	Nein	Ja
AWS::Events::Endpoint	Ja	Ja	Ja	Ja	Nein	Ja	Nein	Ja
AWS::Events::EventBus	Ja	Ja	Ja	Ja	Ja	Ja	Nein	Ja
AWS::Events::Rule	Ja	Ja	Ja	Ja	Nein	Ja	Nein	Ja
AWS::Evidently::Launch	Nein	Ja	Ja	Ja	Nein	Nein	Nein	Nein
AWS::Evidently::Project	Nein	Ja	Ja	Ja	Nein	Nein	Nein	Nein
AWS::Evidently::Segment	Nein	Ja	Ja	Ja	Nein	Nein	Nein	Nein
AWS::FIS::ExperimentTemplate	Ja	Ja	Ja	Ja	Nein	Ja	Nein	Ja
AWS::Forecast::Dataset	Nein	Ja	Ja	Ja	Nein	Nein	Nein	Nein
AWS::Forecast::DatasetGroup	Nein	Ja	Ja	Ja	Nein	Nein	Nein	Nein

Ressourcentyp	USA West (Nordkalifornien)	USA Ost (Nord-Virginia)	USA West (Oregon)	USA Ost (Ohio)	Kanada West (Calgary)	Kanada (Zentral)	Mexiko (Zentral)	Südamerika (São Paulo)
AWS::FraudDetector::EntityType	Nein	Ja	Ja	Ja	Nein	Nein	Nein	Nein
AWS::FraudDetector::Label	Nein	Ja	Ja	Ja	Nein	Nein	Nein	Nein
AWS::FraudDetector::Outcome	Nein	Ja	Ja	Ja	Nein	Nein	Nein	Nein
AWS::FraudDetector::Variable	Nein	Ja	Ja	Ja	Nein	Nein	Nein	Nein
AWS::GlobalAccelerator::Accelerator	Nein	Nein	Ja	Nein	Nein	Nein	Nein	Nein
AWS::GlobalAccelerator::EndpointGroup	Nein	Nein	Ja	Nein	Nein	Nein	Nein	Nein
AWS::GlobalAccelerator::Listener	Nein	Nein	Ja	Nein	Nein	Nein	Nein	Nein
AWS::Glue::Classifier	Ja	Ja	Ja	Ja	Ja	Ja	Nein	Ja
AWS::Glue::Job	Ja	Ja	Ja	Ja	Ja	Ja	Nein	Ja
AWS::Glue::MLTransform	Ja	Ja	Ja	Ja	Ja	Ja	Nein	Ja
AWS::Grafana::Workspace	Nein	Ja	Ja	Ja	Nein	Nein	Nein	Nein

Ressourcentyp	USA West (Nordkalifornien)	USA Ost (Nord-Virginia)	USA West (Oregon)	USA Ost (Ohio)	Kanada West (Calgary)	Kanada (Zentral)	Mexiko (Zentral)	Südamerika (São Paulo)
AWS::GreengrassV2::ComponentVersion	Nein	Ja	Ja	Ja	Nein	Ja	Nein	Nein
AWS::GroundStation::Config	Nein	Ja	Ja	Ja	Nein	Nein	Nein	Ja
AWS::GroundStation::DataflowEndpointGruppe	Nein	Ja	Ja	Ja	Nein	Nein	Nein	Ja
AWS::GroundStation::MissionProfile	Nein	Ja	Ja	Ja	Nein	Nein	Nein	Ja
AWS::GuardDuty::Detector	Ja	Ja	Ja	Ja	Ja	Ja	Nein	Ja
AWS::GuardDuty::Filter	Ja	Ja	Ja	Ja	Nein	Ja	Nein	Ja
AWS::GuardPflicht:: IPSet	Ja	Ja	Ja	Ja	Nein	Ja	Nein	Ja
AWS::GuardDuty::ThreatIntelSatz	Ja	Ja	Ja	Ja	Nein	Ja	Nein	Ja
AWS::HealthSee::FHIRDatastore	Nein	Ja	Ja	Ja	Nein	Nein	Nein	Nein
AWS::IAM::Group	Ja	Ja	Ja	Ja	Nein	Ja	Nein	Ja
AWS::IAM::InstanceProfile	Nein	Ja	Nein	Nein	Nein	Nein	Nein	Nein

Ressourcentyp	USA West (Nordkalifornien)	USA Ost (Nord-Virginia)	USA West (Oregon)	USA Ost (Ohio)	Kanada West (Calgary)	Kanada (Zentral)	Mexiko (Zentral)	Südamerika (São Paulo)
AWS: :ICH: OIDCProvider	Nein	Ja	Nein	Nein	Nein	Nein	Nein	Nein
AWS::IAM::Policy	Ja	Ja	Ja	Ja	Nein	Ja	Nein	Ja
AWS::IAM::Role	Ja	Ja	Ja	Ja	Nein	Ja	Nein	Ja
AWS: :ICH: SAMLProvider	Nein	Ja	Nein	Nein	Nein	Nein	Nein	Nein
AWS::IAM: :ServerCertificate	Nein	Ja	Nein	Nein	Nein	Nein	Nein	Nein
AWS::IAM::User	Ja	Ja	Ja	Ja	Nein	Ja	Nein	Ja
AWS::IVS::Channel	Nein	Ja	Ja	Nein	Nein	Nein	Nein	Nein
AWS::IVS: :PlaybackKeyPaar	Nein	Ja	Ja	Nein	Nein	Nein	Nein	Nein
AWS::IVS::RecordingConfiguration	Nein	Ja	Ja	Nein	Nein	Nein	Nein	Nein
AWS::ImageBuilder: :ContainerRecipe	Ja	Ja	Ja	Ja	Ja	Ja	Nein	Ja
AWS::ImageBuilder: :DistributionConfiguration	Ja	Ja	Ja	Ja	Ja	Ja	Nein	Ja

Ressourcentyp	USA West (Nordkalifornien)	USA Ost (Nord-Virginia)	USA West (Oregon)	USA Ost (Ohio)	Kanada West (Calgary)	Kanada (Zentral)	Mexiko (Zentral)	Südamerika (São Paulo)
AWS::ImageBuilder::ImagePipeline	Ja	Ja	Ja	Ja	Ja	Ja	Nein	Ja
AWS::ImageBuilder::ImageRecipe	Ja	Ja	Ja	Ja	Ja	Ja	Nein	Ja
AWS::ImageBuilder::InfrastructureConfiguration	Ja	Ja	Ja	Ja	Nein	Ja	Nein	Ja
AWS::InspectorV2::Activation	Ja	Ja	Ja	Ja	Nein	Ja	Nein	Ja
AWS::InspectorV2::Filter	Ja	Ja	Ja	Ja	Nein	Ja	Nein	Ja
AWS::IoT::AccountAuditKonfiguration	Ja	Ja	Ja	Ja	Nein	Ja	Nein	Nein
AWS::IoT::Authorizer	Ja	Ja	Ja	Ja	Nein	Ja	Nein	Ja
AWS::IoT:: CACertificate	Ja	Ja	Ja	Ja	Nein	Ja	Nein	Ja
AWS::IoT::CustomMetric	Ja	Ja	Ja	Ja	Nein	Ja	Nein	Nein
AWS::IoT::Dimension	Ja	Ja	Ja	Ja	Nein	Ja	Nein	Nein
AWS::IoT::FleetMetric	Ja	Ja	Ja	Ja	Nein	Ja	Nein	Ja

Ressourcentyp	USA West (Nordkalifornien)	USA Ost (Nord-Virginia)	USA West (Oregon)	USA Ost (Ohio)	Kanada West (Calgary)	Kanada (Zentral)	Mexiko (Zentral)	Südamerika (São Paulo)
AWS::IoT::JobTemplate	Ja	Ja	Ja	Ja	Nein	Ja	Nein	Ja
AWS::IoT::MitigationAction	Ja	Ja	Ja	Ja	Nein	Ja	Nein	Nein
AWS::IoT::Policy	Ja	Ja	Ja	Ja	Nein	Ja	Nein	Ja
AWS::IoT::ProvisioningTemplate	Ja	Ja	Ja	Ja	Nein	Ja	Nein	Ja
AWS::IoT::RoleAlias	Ja	Ja	Ja	Ja	Nein	Ja	Nein	Ja
AWS::IoT::ScheduledAudit	Ja	Ja	Ja	Ja	Nein	Ja	Nein	Nein
AWS::IoT::SecurityProfile	Ja	Ja	Ja	Ja	Nein	Ja	Nein	Nein
AWS::IoTAnalytics::Channel	Nein	Ja	Ja	Ja	Nein	Nein	Nein	Nein
AWS::IoTAnalytics::Dataset	Nein	Ja	Ja	Ja	Nein	Nein	Nein	Nein
AWS::IoTAnalytics::Datastore	Nein	Ja	Ja	Ja	Nein	Nein	Nein	Nein
AWS::IoTAnalytics::Pipeline	Nein	Ja	Ja	Ja	Nein	Nein	Nein	Nein

Ressourcentyp	USA West (Nordkalifornien)	USA Ost (Nord-Virginia)	USA West (Oregon)	USA Ost (Ohio)	Kanada West (Calgary)	Kanada (Zentral)	Mexiko (Zentral)	Südamerika (São Paulo)
AWS::IoTEvents::AlarmModel	Nein	Ja	Ja	Ja	Nein	Ja	Nein	Nein
AWS::IoTEvents::DetectorModel	Nein	Ja	Ja	Ja	Nein	Ja	Nein	Nein
AWS::IoTEvents::Input	Nein	Ja	Ja	Ja	Nein	Ja	Nein	Nein
AWS::IoTSiteWise::AssetModel	Nein	Ja	Ja	Ja	Nein	Ja	Nein	Nein
AWS::IoTSiteWise::Dashboard	Nein	Ja	Ja	Ja	Nein	Ja	Nein	Nein
AWS::IoTSiteWise::Gateway	Nein	Ja	Ja	Ja	Nein	Ja	Nein	Nein
AWS::IoTSiteWise::Portal	Nein	Ja	Ja	Ja	Nein	Ja	Nein	Nein
AWS::IoTSiteWise::Project	Nein	Ja	Ja	Ja	Nein	Ja	Nein	Nein
AWS::IoTTwinMaker::ComponentType	Nein	Ja	Ja	Nein	Nein	Nein	Nein	Nein
AWS::IoTTwinMaker::Entity	Nein	Ja	Ja	Nein	Nein	Nein	Nein	Nein
AWS::IoTTwinMaker::Scene	Nein	Ja	Ja	Nein	Nein	Nein	Nein	Nein

Ressourcentyp	USA West (Nordkalifornien)	USA Ost (Nord-Virginia)	USA West (Oregon)	USA Ost (Ohio)	Kanada West (Calgary)	Kanada (Zentral)	Mexiko (Zentral)	Südamerika (São Paulo)
AWS::IoTTwinMaker::SyncJob	Nein	Ja	Ja	Nein	Nein	Nein	Nein	Nein
AWS::IoTTwinMaker::Workspace	Nein	Ja	Ja	Nein	Nein	Nein	Nein	Nein
AWS::IoTWireless::FuotaTask	Nein	Ja	Ja	Nein	Nein	Nein	Nein	Ja
AWS::IoTWireless::MulticastGroup	Nein	Ja	Ja	Nein	Nein	Nein	Nein	Ja
AWS::IoTWireless::ServiceProfile	Nein	Ja	Ja	Nein	Nein	Nein	Nein	Ja
AWS::KMS::Alias	Ja	Ja	Ja	Ja	Nein	Ja	Nein	Ja
AWS::KMS::Key	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja
AWS::KafkaConnect::Connector	Ja	Ja	Ja	Ja	Nein	Ja	Nein	Ja
AWS::Kendra::Index	Nein	Ja	Ja	Ja	Nein	Ja	Nein	Nein
AWS::Kinesis::Stream	Ja	Ja	Ja	Ja	Nein	Ja	Nein	Ja
AWS::Kinesis::StreamConsumer	Ja	Ja	Ja	Ja	Nein	Ja	Nein	Ja

Ressourcentyp	USA West (Nordkalifornien)	USA Ost (Nord-Virginia)	USA West (Oregon)	USA Ost (Ohio)	Kanada West (Calgary)	Kanada (Zentral)	Mexiko (Zentral)	Südamerika (São Paulo)
AWS::KinesisAnalyticsV2::Application	Ja	Ja	Ja	Ja	Ja	Ja	Nein	Ja
AWS::KinesisFirehose::DeliveryStream	Ja	Ja	Ja	Ja	Nein	Ja	Nein	Ja
AWS::KinesisVideo::SignalingChannel	Nein	Ja	Ja	Ja	Nein	Ja	Nein	Ja
AWS::KinesisVideo::Stream	Nein	Ja	Ja	Ja	Nein	Ja	Nein	Ja
AWS::Lambda::CodeSigningConfig	Ja	Ja	Ja	Ja	Nein	Ja	Nein	Ja
AWS::Lambda::Function	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja
AWS::Lex::Bot	Nein	Ja	Ja	Nein	Nein	Ja	Nein	Nein
AWS::Lex::BotAlias	Nein	Ja	Ja	Nein	Nein	Ja	Nein	Nein
AWS::Lightsail::Bucket	Nein	Ja	Ja	Ja	Nein	Ja	Nein	Nein
AWS::Lightsail::Certificate	Nein	Ja	Ja	Ja	Nein	Ja	Nein	Nein
AWS::Lightsail::Disk	Nein	Ja	Ja	Ja	Nein	Ja	Nein	Nein

Ressourcentyp	USA West (Nordkalifornien)	USA Ost (Nord-Virginia)	USA West (Oregon)	USA Ost (Ohio)	Kanada West (Calgary)	Kanada (Zentral)	Mexiko (Zentral)	Südamerika (São Paulo)
AWS::Lightsail::StaticIp	Nein	Ja	Ja	Ja	Nein	Ja	Nein	Nein
AWS::Logs::Destination	Ja	Ja	Ja	Ja	Ja	Ja	Nein	Ja
AWS::LookoutMetrics::Alert	Nein	Ja	Ja	Ja	Nein	Nein	Nein	Nein
AWS::LookoutVision::Project	Nein	Ja	Ja	Ja	Nein	Nein	Nein	Nein
AWS::M2::Environment	Ja	Ja	Ja	Ja	Nein	Ja	Nein	Ja
AWS::MSK::BatchScramGeheim	Ja	Ja	Ja	Ja	Nein	Ja	Nein	Ja
AWS::MSK::Cluster	Ja	Ja	Ja	Ja	Nein	Ja	Nein	Ja
AWS::MSK::ClusterPolicy	Ja	Ja	Ja	Ja	Nein	Ja	Nein	Ja
AWS::MSK::Configuration	Ja	Ja	Ja	Ja	Ja	Ja	Nein	Ja
AWS::MSK::VpcConnection	Ja	Ja	Ja	Ja	Nein	Ja	Nein	Ja
AWS::Macie::Session	Ja	Ja	Ja	Ja	Nein	Ja	Nein	Ja

Ressourcentyp	USA West (Nordkalifornien)	USA Ost (Nord-Virginia)	USA West (Oregon)	USA Ost (Ohio)	Kanada West (Calgary)	Kanada (Zentral)	Mexiko (Zentral)	Südamerika (São Paulo)
AWS::MediaConnect::FlowEntitlement	Ja	Ja	Ja	Ja	Nein	Ja	Nein	Ja
AWS::MediaConnect::FlowSource	Ja	Ja	Ja	Ja	Nein	Ja	Nein	Ja
AWS::MediaConnect::FlowVpcSchnittstelle	Ja	Ja	Ja	Ja	Nein	Ja	Nein	Ja
AWS::MediaConnect::Gateway	Ja	Ja	Ja	Ja	Nein	Ja	Nein	Ja
AWS::MediaPackage::PackagingConfiguration	Ja	Ja	Ja	Ja	Nein	Ja	Nein	Ja
AWS::MediaPackage::PackagingGroup	Ja	Ja	Ja	Ja	Nein	Ja	Nein	Ja
AWS::MediaTailor::PlaybackConfiguration	Nein	Ja	Ja	Ja	Nein	Ja	Nein	Ja
AWS::MemoryDB::SubnetGroup	Ja	Ja	Ja	Ja	Nein	Ja	Nein	Ja
AWS::NetworkFirewall::Firewall	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja
AWS::NetworkFirewall::FirewallPolicy	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja
AWS::NetworkFirewall::RuleGroup	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja

Ressourcentyp	USA West (Nordkalifornien)	USA Ost (Nord-Virginia)	USA West (Oregon)	USA Ost (Ohio)	Kanada West (Calgary)	Kanada (Zentral)	Mexiko (Zentral)	Südamerika (São Paulo)
AWS::NetworkFirewall: TLSInspectionKonfiguration	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja
AWS::NetworkFirewall::VpcEndpointAssoziation	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja
AWS::NetworkManager::ConnectPeer	Nein	Nein	Ja	Nein	Nein	Nein	Nein	Nein
AWS::NetworkManager::CustomerGatewayVerband	Nein	Nein	Ja	Nein	Nein	Nein	Nein	Nein
AWS::NetworkManager::Device	Nein	Nein	Ja	Nein	Nein	Nein	Nein	Nein
AWS::NetworkManager::GlobalNetwork	Nein	Nein	Ja	Nein	Nein	Nein	Nein	Nein
AWS::NetworkManager::Link	Nein	Nein	Ja	Nein	Nein	Nein	Nein	Nein
AWS::NetworkManager::LinkAssociation	Nein	Nein	Ja	Nein	Nein	Nein	Nein	Nein
AWS::NetworkManager::Site	Nein	Nein	Ja	Nein	Nein	Nein	Nein	Nein
AWS::NetworkManager::TransitGatewayRegistrierung	Nein	Nein	Ja	Nein	Nein	Nein	Nein	Nein

Ressourcentyp	USA West (Nordkalifornien)	USA Ost (Nord-Virginia)	USA West (Oregon)	USA Ost (Ohio)	Kanada West (Calgary)	Kanada (Zentral)	Mexiko (Zentral)	Südamerika (São Paulo)
AWS::OpenSearch::Domain	Ja	Ja	Ja	Ja	Nein	Ja	Nein	Ja
AWS::OpenSearchServerless::Collection	Nein	Ja	Ja	Ja	Nein	Ja	Nein	Ja
AWS::OpenSearchServerless::VpcEndpoint	Nein	Ja	Ja	Ja	Nein	Ja	Nein	Ja
AWS::Panorama::Package	Nein	Ja	Ja	Nein	Nein	Ja	Nein	Nein
AWS::Personalize::Dataset	Nein	Ja	Ja	Ja	Nein	Ja	Nein	Nein
AWS::Personalize::DatasetGroup	Nein	Ja	Ja	Ja	Nein	Ja	Nein	Nein
AWS::Personalize::Schema	Nein	Ja	Ja	Ja	Nein	Ja	Nein	Nein
AWS::Personalize::Solution	Nein	Ja	Ja	Ja	Nein	Ja	Nein	Nein
AWS::Pinpoint::App	Nein	Ja	Ja	Nein	Nein	Ja	Nein	Nein
AWS::Pinpoint::ApplicationSettings	Nein	Ja	Ja	Nein	Nein	Ja	Nein	Nein
AWS::Pinpoint::Campaign	Nein	Ja	Ja	Nein	Nein	Ja	Nein	Nein

Ressourcentyp	USA West (Nordkalifornien)	USA Ost (Nord-Virginia)	USA West (Oregon)	USA Ost (Ohio)	Kanada West (Calgary)	Kanada (Zentral)	Mexiko (Zentral)	Südamerika (São Paulo)
AWS::Pinpoint::EmailChannel	Nein	Ja	Ja	Nein	Nein	Ja	Nein	Nein
AWS::Pinpoint::EmailTemplate	Nein	Ja	Ja	Nein	Nein	Ja	Nein	Nein
AWS::Pinpoint::EventStream	Nein	Ja	Ja	Nein	Nein	Ja	Nein	Nein
AWS::Pinpoint::InAppVorlage	Nein	Ja	Ja	Ja	Nein	Ja	Nein	Nein
AWS::Pinpoint::Segment	Nein	Ja	Ja	Nein	Nein	Ja	Nein	Nein
AWS::QLDB::Ledger	Nein	Ja	Ja	Ja	Nein	Ja	Nein	Nein
AWS::QuickSight::DataSource	Nein	Ja	Ja	Ja	Nein	Ja	Nein	Ja
AWS::QuickSight::Template	Nein	Ja	Ja	Ja	Nein	Ja	Nein	Ja
AWS::QuickSight::Theme	Nein	Ja	Ja	Ja	Nein	Ja	Nein	Ja
AWS: :RDS: DBCluster	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja
AWS: :RDS:: Schnappschuss DBCluster	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja

Ressourcentyp	USA West (Nordkalifornien)	USA Ost (Nord-Virginia)	USA West (Oregon)	USA Ost (Ohio)	Kanada West (Calgary)	Kanada (Zentral)	Mexiko (Zentral)	Südamerika (São Paulo)
AWS: :RDS: DBInstance	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja
AWS: :RDS:: Gruppe DBSecurity	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja
AWS: :RDS: DBSnapshot	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja
AWS: :RDS:: Gruppe DBSubnet	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja
AWS::RDS: :EventSubscription	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja
AWS::RDS::GlobalCluster	Ja	Ja	Ja	Ja	Nein	Ja	Nein	Ja
AWS::RDS::OptionGroup	Ja	Ja	Ja	Ja	Ja	Ja	Nein	Ja
AWS::RUM::AppMonitor	Ja	Ja	Ja	Ja	Nein	Ja	Nein	Ja
AWS::Redshift::Cluster	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja
AWS::Redshift::ClusterParameterGruppe	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja
AWS::Redshift::ClusterSecurityGruppe	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja

Ressourcentyp	USA West (Nordkalifornien)	USA Ost (Nord-Virginia)	USA West (Oregon)	USA Ost (Ohio)	Kanada West (Calgary)	Kanada (Zentral)	Mexiko (Zentral)	Südamerika (São Paulo)
AWS::Redshift::ClusterSnapshot	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja
AWS::Redshift::ClusterSubnetGruppe	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja
AWS::Redshift::EndpointAccess	Ja	Ja	Ja	Ja	Nein	Ja	Nein	Ja
AWS::Redshift::EndpointAuthorization	Ja	Ja	Ja	Ja	Nein	Ja	Nein	Ja
AWS::Redshift::EventSubscription	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja
AWS::Redshift::ScheduledAction	Ja	Ja	Ja	Ja	Nein	Ja	Nein	Ja
AWS::ResilienceHub::App	Ja	Ja	Ja	Ja	Nein	Ja	Nein	Ja
AWS::ResilienceHub::ResiliencyPolicy	Ja	Ja	Ja	Ja	Nein	Ja	Nein	Ja
AWS::ResourceExplorer2::Index	Ja	Ja	Ja	Ja	Ja	Ja	Nein	Ja
AWS::RoboMaker::RobotApplication	Nein	Ja	Ja	Ja	Nein	Nein	Nein	Nein
AWS::RoboMaker::RobotApplicationVersion	Nein	Ja	Ja	Ja	Nein	Nein	Nein	Nein

Ressourcentyp	USA West (Nordkalifornien)	USA Ost (Nord-Virginia)	USA West (Oregon)	USA Ost (Ohio)	Kanada West (Calgary)	Kanada (Zentral)	Mexiko (Zentral)	Südamerika (São Paulo)
AWS::RoboMaker::SimulationApplication	Nein	Ja	Ja	Ja	Nein	Nein	Nein	Nein
AWS::Route53::HealthCheck	Nein	Ja	Nein	Nein	Nein	Nein	Nein	Nein
AWS::Route53::HostedZone	Nein	Ja	Nein	Nein	Nein	Nein	Nein	Nein
AWS::Route53Profiles::Profile	Ja	Ja	Ja	Ja	Ja	Ja	Nein	Ja
AWS::Route53RecoveryControl::Cluster	Nein	Nein	Ja	Nein	Nein	Nein	Nein	Nein
AWS::Route53RecoveryControl::ControlPanel	Nein	Nein	Ja	Nein	Nein	Nein	Nein	Nein
AWS::Route53RecoveryControl::RoutingControl	Nein	Nein	Ja	Nein	Nein	Nein	Nein	Nein
AWS::Route53RecoveryControl::SafetyRule	Nein	Nein	Ja	Nein	Nein	Nein	Nein	Nein
AWS::Route53RecoveryReadiness::Cell	Nein	Nein	Ja	Nein	Nein	Nein	Nein	Nein
AWS::Route53RecoveryReadiness::ReadinessCheck	Nein	Nein	Ja	Nein	Nein	Nein	Nein	Nein

Ressourcentyp	USA West (Nordkalifornien)	USA Ost (Nord-Virginia)	USA West (Oregon)	USA Ost (Ohio)	Kanada West (Calgary)	Kanada (Zentral)	Mexiko (Zentral)	Südamerika (São Paulo)
AWS::Route53RecoveryReadiness::RecoveryGroup	Nein	Nein	Ja	Nein	Nein	Nein	Nein	Nein
AWS::Route53RecoveryReadiness::ResourceSet	Nein	Nein	Ja	Nein	Nein	Nein	Nein	Nein
AWS::Route53Resolver::FirewallDomainListe	Ja	Ja	Ja	Ja	Nein	Ja	Nein	Ja
AWS::Route53Resolver::FirewallRuleGruppe	Ja	Ja	Ja	Ja	Nein	Ja	Nein	Ja
AWS::Route53Resolver::FirewallRuleGroupAssociation	Ja	Ja	Ja	Ja	Nein	Ja	Nein	Ja
AWS::Route53Resolver::ResolverEndpoint	Ja	Ja	Ja	Ja	Nein	Ja	Nein	Ja
AWS::Route53Resolver::ResolverQueryLoggingConfig	Ja	Ja	Ja	Ja	Nein	Ja	Nein	Ja
AWS::Route53Resolver::ResolverQueryLoggingConfigAssociation	Ja	Ja	Ja	Ja	Nein	Ja	Nein	Ja
AWS::Route53Resolver::ResolverRule	Ja	Ja	Ja	Ja	Nein	Ja	Nein	Ja
AWS::Route53Resolver::ResolverRuleVerband	Ja	Ja	Ja	Ja	Nein	Ja	Nein	Ja

Ressourcentyp	USA West (Nordkalifornien)	USA Ost (Nord-Virginia)	USA West (Oregon)	USA Ost (Ohio)	Kanada West (Calgary)	Kanada (Zentral)	Mexiko (Zentral)	Südamerika (São Paulo)
AWS::S3::AccessPoint	Ja	Ja	Ja	Ja	Nein	Ja	Nein	Ja
AWS::S3::AccountPublicAccessBlock	Ja	Ja	Ja	Ja	Nein	Ja	Nein	Ja
AWS::S3::Bucket	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja
AWS::S3::MultiRegionAccessPoint	Nein	Nein	Ja	Nein	Nein	Nein	Nein	Nein
AWS::S3::StorageLens	Ja	Ja	Ja	Ja	Nein	Ja	Nein	Ja
AWS::S3::StorageLensGruppe	Ja	Ja	Ja	Ja	Nein	Ja	Nein	Ja
AWS::S3Express::BucketPolicy	Nein	Ja	Ja	Ja	Nein	Nein	Nein	Nein
AWS::S3Express::DirectoryBucket	Nein	Ja	Ja	Ja	Nein	Nein	Nein	Nein
AWS::SES::ConfigurationSet	Ja	Ja	Ja	Ja	Nein	Ja	Nein	Ja
AWS::SES::ContactList	Ja	Ja	Ja	Ja	Nein	Ja	Nein	Ja
AWS::SES::ReceiptFilter	Nein	Ja	Ja	Ja	Nein	Ja	Nein	Nein

Ressourcentyp	USA West (Nordkalifornien)	USA Ost (Nord-Virginia)	USA West (Oregon)	USA Ost (Ohio)	Kanada West (Calgary)	Kanada (Zentral)	Mexiko (Zentral)	Südamerika (São Paulo)
AWS::SES::ReceiptRuleSatz	Nein	Ja	Ja	Ja	Nein	Ja	Nein	Nein
AWS::SES::Template	Ja	Ja	Ja	Ja	Nein	Ja	Nein	Ja
AWS::SNS::Topic	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja
AWS::SQS::Queue	Ja	Ja	Ja	Ja	Nein	Ja	Nein	Ja
AWS::SSM::AssociationCompliance	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja
AWS::SSM::Document	Ja	Ja	Ja	Ja	Ja	Ja	Nein	Ja
AWS::SSM::FileData	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja
AWS::SSM::ManagedInstance-Bestand	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja
AWS::SSM::PatchCompliance	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja
AWS::SageMaker::AppImageConfig	Ja	Ja	Ja	Ja	Nein	Ja	Nein	Ja
AWS::SageMaker::CodeRepository	Ja	Ja	Ja	Ja	Nein	Ja	Nein	Ja

Ressourcentyp	USA West (Nordkalifornien)	USA Ost (Nord-Virginia)	USA West (Oregon)	USA Ost (Ohio)	Kanada West (Calgary)	Kanada (Zentral)	Mexiko (Zentral)	Südamerika (São Paulo)
AWS::SageMaker::Domain	Ja	Ja	Ja	Ja	Nein	Ja	Nein	Ja
AWS::SageMaker::EndpointConfig	Ja	Ja	Ja	Ja	Nein	Ja	Nein	Ja
AWS::SageMaker::FeatureGroup	Ja	Ja	Ja	Ja	Nein	Ja	Nein	Ja
AWS::SageMaker::Image	Ja	Ja	Ja	Ja	Nein	Ja	Nein	Ja
AWS::SageMaker::InferenceExperiment	Ja	Ja	Ja	Ja	Nein	Ja	Nein	Ja
AWS::SageMaker::Model	Ja	Ja	Ja	Ja	Nein	Ja	Nein	Ja
AWS::SageMaker::NotebookInstance	Ja	Ja	Ja	Ja	Nein	Ja	Nein	Ja
AWS::SageMaker::NotebookInstanceLifecycleConfig	Ja	Ja	Ja	Ja	Nein	Ja	Nein	Ja
AWS::SageMaker::Workteam	Nein	Ja	Ja	Ja	Nein	Ja	Nein	Nein
AWS::SecretsManager::Secret	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja
AWS::SecurityHub::Standard	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja

Ressourcentyp	USA West (Nordkalifornien)	USA Ost (Nord-Virginia)	USA West (Oregon)	USA Ost (Ohio)	Kanada West (Calgary)	Kanada (Zentral)	Mexiko (Zentral)	Südamerika (São Paulo)
AWS::ServiceCatalog::CloudFormationProdukt	Ja	Ja	Ja	Ja	Nein	Ja	Nein	Ja
AWS::ServiceCatalog::CloudFormationProvisionedProduct	Ja	Ja	Ja	Ja	Nein	Ja	Nein	Ja
AWS::ServiceCatalog::Portfolio	Ja	Ja	Ja	Ja	Nein	Ja	Nein	Ja
AWS::ServiceDiscovery::HttpNamespace	Ja	Ja	Ja	Ja	Ja	Ja	Nein	Ja
AWS::ServiceDiscovery::Instance	Ja	Ja	Ja	Ja	Nein	Ja	Nein	Ja
AWS::ServiceDiscovery::PublicDnsNamespace	Ja	Ja	Ja	Ja	Ja	Ja	Nein	Ja
AWS::ServiceDiscovery::Service	Ja	Ja	Ja	Ja	Nein	Ja	Nein	Ja
AWS::Shield::Protection	Nein	Ja	Nein	Nein	Nein	Nein	Nein	Nein
AWS::ShieldRegional::Protection	Ja	Ja	Ja	Ja	Nein	Ja	Nein	Ja
AWS::Signer::SigningProfile	Ja	Ja	Ja	Ja	Nein	Ja	Nein	Ja
AWS::StepFunctions::Activity	Ja	Ja	Ja	Ja	Ja	Ja	Nein	Ja

Ressourcentyp	USA West (Nordkalifornien)	USA Ost (Nord-Virginia)	USA West (Oregon)	USA Ost (Ohio)	Kanada West (Calgary)	Kanada (Zentral)	Mexiko (Zentral)	Südamerika (São Paulo)
AWS::StepFunctions::StateMachine	Ja	Ja	Ja	Ja	Ja	Ja	Nein	Ja
AWS::Transfer::Agreement	Ja	Ja	Ja	Ja	Nein	Ja	Nein	Ja
AWS::Transfer::Certificate	Ja	Ja	Ja	Ja	Ja	Ja	Nein	Ja
AWS::Transfer::Connector	Ja	Ja	Ja	Ja	Ja	Ja	Nein	Ja
AWS::Transfer::Profile	Ja	Ja	Ja	Ja	Ja	Ja	Nein	Ja
AWS::Transfer::Workflow	Ja	Ja	Ja	Ja	Ja	Ja	Nein	Ja
AWS::WAF::RateBasedRegel	Nein	Ja	Nein	Nein	Nein	Nein	Nein	Nein
AWS::WAF::Rule	Nein	Ja	Nein	Nein	Nein	Nein	Nein	Nein
AWS::WAF::RuleGroup	Nein	Ja	Nein	Nein	Nein	Nein	Nein	Nein
AWS::WAF::WebACL	Nein	Ja	Nein	Nein	Nein	Nein	Nein	Nein
AWS::WAFRegional::RateBasedRegel	Ja	Ja	Ja	Ja	Nein	Ja	Nein	Ja

Ressourcentyp	USA West (Nordkalifornien)	USA Ost (Nord-Virginia)	USA West (Oregon)	USA Ost (Ohio)	Kanada West (Calgary)	Kanada (Zentral)	Mexiko (Zentral)	Südamerika (São Paulo)
AWS::WAFRegional::Rule	Ja	Ja	Ja	Ja	Nein	Ja	Nein	Ja
AWS::WAFRegional::RuleGroup	Ja	Ja	Ja	Ja	Nein	Ja	Nein	Ja
AWS::WAFRegional::WebACL	Ja	Ja	Ja	Ja	Nein	Ja	Nein	Ja
AWS:WAFv2:: IPSet	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja
AWS::WAFv2::ManagedRuleSatz	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja
AWS::WAFv2::RegexPatternSatz	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja
AWS::WAFv2::RuleGroup	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja
AWS::WAFv2::WebACL	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja
AWS::WorkSpaces::ConnectionAlias	Nein	Ja	Ja	Nein	Nein	Ja	Nein	Ja
AWS::WorkSpaces::Workspace	Nein	Ja	Ja	Nein	Nein	Ja	Nein	Ja
AWS::XRay::EncryptionConfig	Ja	Ja	Ja	Ja	Nein	Ja	Nein	Ja

Regionen in Europa

Ressourcentyp	Europa (Irland)	Europa (Frankfurt)	Europa (London)	Europa (Paris)	Europa (Stockholm)	Europa (Milan)	Europa (Spain)	Europa (Zürich)
AWS::ACM::Certificate	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja
AWS::ACMPCA::CertificateAuthority	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja
AWS::ACMPCA::CertificateAuthorityAktivierung	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja
AWS::APS::RuleGroupsNamespace	Ja	Ja	Ja	Ja	Ja	Nein	Nein	Nein
AWS::AccessAnalyzer::Analyzer	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja
AWS::AmazonMQ::Broker	Ja	Ja	Ja	Ja	Ja	Ja	Nein	Nein
AWS::Amplify::App	Ja	Ja	Ja	Ja	Ja	Ja	Nein	Nein
AWS::Amplify::Branch	Ja	Ja	Ja	Ja	Ja	Ja	Nein	Nein
AWS::ApiGateway::RestApi	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja
AWS::ApiGateway::Stage	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja
AWS::ApiGatewayV2::Api	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja

Ressourcentyp	Europa (Irland)	Europa (Frankfurt)	Europa (London)	Europa (Paris)	Europa (Stockholm)	Europa (Milan)	Europa (Spain)	Europa (Zürich)
AWS::ApiGatewayV2::Stage	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja
AWS::AppConfig::Application	Ja	Ja	Ja	Ja	Ja	Ja	Nein	Nein
AWS::AppConfig::ConfigurationProfile	Ja	Ja	Ja	Ja	Ja	Ja	Nein	Nein
AWS::AppConfig::DeploymentStrategy	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja
AWS::AppConfig::Environment	Ja	Ja	Ja	Ja	Ja	Ja	Nein	Nein
AWS::AppConfig::ExtensionAssociation	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja
AWS::AppConfig::HostedConfigurationVersion	Ja	Ja	Ja	Ja	Ja	Ja	Nein	Nein
AWS::AppFlow::Flow	Ja	Ja	Ja	Ja	Nein	Nein	Nein	Nein
AWS::AppIntegrations::Application	Nein	Ja	Ja	Nein	Nein	Nein	Nein	Nein
AWS::AppIntegrations::EventIntegration	Nein	Ja	Ja	Nein	Nein	Nein	Nein	Nein
AWS::AppMesh::GatewayRoute	Ja	Ja	Ja	Ja	Ja	Ja	Nein	Nein
AWS::AppMesh::Mesh	Ja	Ja	Ja	Ja	Ja	Ja	Nein	Nein

Ressourcentyp	Europa (Irland)	Europa (Frankfurt)	Europa (London)	Europa (Paris)	Europa (Stockholm)	Europa (Milan)	Europa (Spain)	Europa (Zürich)
AWS::AppMesh::Route	Ja	Ja	Ja	Ja	Ja	Ja	Nein	Nein
AWS::AppMesh::VirtualGateway	Ja	Ja	Ja	Ja	Ja	Ja	Nein	Nein
AWS::AppMesh::VirtualNode	Ja	Ja	Ja	Ja	Ja	Ja	Nein	Nein
AWS::AppMesh::VirtualRouter	Ja	Ja	Ja	Ja	Ja	Ja	Nein	Nein
AWS::AppMesh::VirtualService	Ja	Ja	Ja	Ja	Ja	Ja	Nein	Nein
AWS::AppRunner::Service	Ja	Ja	Ja	Ja	Nein	Nein	Nein	Nein
AWS::AppRunner::VpcConnector	Ja	Ja	Nein	Ja	Nein	Nein	Nein	Nein
AWS::AppStream::Application	Ja	Ja	Ja	Nein	Nein	Nein	Nein	Nein
AWS::AppStream::DirectoryConfig	Ja	Ja	Ja	Nein	Nein	Nein	Nein	Nein
AWS::AppStream::Fleet	Ja	Ja	Ja	Nein	Nein	Nein	Nein	Nein
AWS::AppStream::Stack	Ja	Ja	Ja	Nein	Nein	Nein	Nein	Nein
AWS::AppSync::ApiCache	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja

Ressourcentyp	Europa (Irland)	Europa (Frankfurt)	Europa (London)	Europa (Paris)	Europa (Stockholm)	Europa (Milan)	Europa (Spain)	Europa (Zürich)
AWS::AppSync::GraphQLApi	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja
AWS::Athena::DataCatalog	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja
AWS::Athena::PreparedStatement	Ja	Ja	Ja	Ja	Ja	Nein	Ja	Ja
AWS::Athena::WorkGroup	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja
AWS::AuditManager::Assessment	Ja	Ja	Ja	Nein	Nein	Nein	Nein	Nein
AWS::AutoScaling::AutoScalingGruppe	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja
AWS::AutoScaling::LaunchConfiguration	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja
AWS::AutoScaling::ScalingPolicy	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja
AWS::AutoScaling::ScheduledAction	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja
AWS::AutoScaling::WarmPool	Ja	Ja	Ja	Ja	Ja	Ja	Nein	Nein
AWS::Backup::BackupPlan	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja
AWS::Backup::BackupSelection	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja

Ressourcentyp	Europa (Irland)	Europa (Frankfurt)	Europa (London)	Europa (Paris)	Europa (Stockholm)	Europa (Milan)	Europa (Spain)	Europa (Zürich)
AWS::Backup::BackupVault	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja
AWS::Backup::RecoveryPoint	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja
AWS::Backup::ReportPlan	Ja	Ja	Ja	Ja	Ja	Ja	Nein	Nein
AWS::Batch::ComputeEnvironment	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja
AWS::Batch::JobQueue	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja
AWS::Batch::SchedulingPolicy	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja
AWS::Bedrock::Guardrail	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja
AWS::Bedrock::KnowledgeBase	Ja	Ja	Ja	Ja	Ja	Nein	Nein	Ja
AWS::Cassandra::Keyspace	Ja	Ja	Ja	Ja	Ja	Nein	Nein	Nein
AWS::Cloud9::EnvironmentEC2	Ja	Ja	Ja	Ja	Ja	Ja	Nein	Nein
AWS::CloudFormation::Stack	Ja	Ja	Ja	Ja	Ja	Ja	Nein	Nein
AWS::CloudTrail::Trail	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja

Ressourcentyp	Europa (Irland)	Europa (Frankfurt)	Europa (London)	Europa (Paris)	Europa (Stockholm)	Europa (Milan)	Europa (Spain)	Europa (Zürich)
AWS::CloudWatch::Alarm	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja
AWS::CloudWatch::MetricStream	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja
AWS::CodeArtifact::Repository	Ja	Ja	Ja	Ja	Ja	Ja	Nein	Nein
AWS::CodeBuild::Project	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja
AWS::CodeBuild::ReportGroup	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja
AWS::CodeDeploy::Application	Ja	Ja	Ja	Ja	Ja	Ja	Nein	Nein
AWS::CodeDeploy::DeploymentConfig	Ja	Ja	Ja	Ja	Ja	Ja	Nein	Nein
AWS::CodeDeploy::DeploymentGroup	Ja	Ja	Ja	Ja	Ja	Ja	Nein	Nein
AWS::CodeGuruProfiler::ProfilingGroup	Ja	Ja	Ja	Nein	Ja	Nein	Nein	Nein
AWS::CodeGuruReviewer::RepositoryAssociation	Ja	Ja	Ja	Nein	Ja	Nein	Nein	Nein
AWS::CodePipeline::Pipeline	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja
AWS::Cognito::IdentityPool	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja

Ressourcentyp	Europa (Irland)	Europa (Frankfurt)	Europa (London)	Europa (Paris)	Europa (Stockholm)	Europa (Milan)	Europa (Spain)	Europa (Zürich)
AWS::Cognito::UserPool	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja
AWS::Cognito::UserPoolKlient	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja
AWS::Cognito::UserPoolGruppe	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja
AWS::Config::ConfigurationRecorder	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja
AWS::Config::ConformancePack-Compliance	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja
AWS::Config::ResourceCompliance	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja
AWS::Connect::Instance	Nein	Ja	Ja	Nein	Nein	Nein	Nein	Nein
AWS::Connect::PhoneNumber	Nein	Ja	Ja	Nein	Nein	Nein	Nein	Nein
AWS::Connect::QuickConnect	Nein	Ja	Ja	Nein	Nein	Nein	Nein	Nein
AWS::Connect::Rule	Nein	Ja	Ja	Nein	Nein	Nein	Nein	Nein
AWS::Connect::User	Nein	Ja	Ja	Nein	Nein	Nein	Nein	Nein
AWS::CustomerProfiles::Domain	Nein	Ja	Ja	Nein	Nein	Nein	Nein	Nein

Ressourcentyp	Europa (Irland)	Europa (Frankfurt)	Europa (London)	Europa (Paris)	Europa (Stockholm)	Europa (Milan)	Europa (Spain)	Europa (Zürich)
AWS::CustomerProfiles::ObjectType	Nein	Ja	Ja	Nein	Nein	Nein	Nein	Nein
AWS::DMS::Certificate	Ja	Ja	Ja	Ja	Ja	Ja	Nein	Nein
AWS::DMS::Endpoint	Ja	Ja	Ja	Ja	Ja	Ja	Nein	Nein
AWS::DMS::EventSubscription	Ja	Ja	Ja	Ja	Ja	Ja	Nein	Nein
AWS::DMS::ReplicationInstance	Ja	Ja	Ja	Ja	Ja	Ja	Nein	Nein
AWS::DMS::ReplicationSubnetGruppe	Ja	Ja	Ja	Ja	Ja	Ja	Nein	Nein
AWS::DMS::ReplicationTask	Ja	Ja	Ja	Ja	Ja	Ja	Nein	Nein
AWS::DataSync::LocationEFS	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja
AWS::DataSync::LocationFSxGlanz	Ja	Ja	Ja	Ja	Ja	Ja	Nein	Nein
AWS::DataSync::LocationFSxFenster	Ja	Ja	Ja	Ja	Ja	Ja	Nein	Nein
AWS::DataSync::LocationHDFS	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja
AWS::DataSync::LocationNFS	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja

Ressourcentyp	Europa (Irland)	Europa (Frankfurt)	Europa (London)	Europa (Paris)	Europa (Stockholm)	Europa (Milan)	Europa (Spain)	Europa (Zürich)
AWS::DataSync::LocationObjectSpeicher	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja
AWS::DataSync::LocationS 3	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja
AWS::DataSync::LocationSMB	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja
AWS::DataSync::Task	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja
AWS::Detective::Graph	Ja	Ja	Ja	Ja	Ja	Ja	Nein	Nein
AWS::DynamoDB::Table	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja
AWS::EC2::CapacityReservation	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja
AWS::EC2::CarrierGateway	Ja	Ja	Ja	Ja	Nein	Nein	Nein	Nein
AWS::EC2::ClientVpnEndpunkt	Ja	Ja	Ja	Ja	Ja	Ja	Nein	Ja
AWS::EC2::ClientVpnTargetNetworkAssociation	Ja	Ja	Ja	Ja	Ja	Ja	Nein	Ja
AWS::EC2::CustomerGateway	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja
AWS:EC2:: DHCPOptions	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja

Ressourcentyp	Europa (Irland)	Europa (Frankfurt)	Europa (London)	Europa (Paris)	Europa (Stockholm)	Europa (Milan)	Europa (Spain)	Europa (Zürich)
AWS:EC2:: EC2 Flotte	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja
AWS::EC2: EIP	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja
AWS:EC2:: EIPAssociation	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja
AWS::EC2::EgressOnlyInternetGateway	Ja	Ja	Ja	Ja	Ja	Ja	Nein	Ja
AWS::EC2::FlowLog	Ja	Ja	Ja	Ja	Ja	Ja	Nein	Ja
AWS::EC2::Host	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja
AWS:::EC2: IPAM	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja
AWS:EC2:: IPAMPool	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja
AWS:EC2:: IPAMResource Entdeckung	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja
AWS:EC2:: IPAMResource DiscoveryAssociation	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja
AWS:EC2:: IPAMScope	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja
AWS::EC2::Instance	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja

Ressourcentyp	Europa (Irland)	Europa (Frankfurt)	Europa (London)	Europa (Paris)	Europa (Stockholm)	Europa (Milan)	Europa (Spain)	Europa (Zürich)
AWS::EC2::Instance ConnectEndpunkt	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja
AWS::EC2::InternetGateway	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja
AWS::EC2::LaunchTemplate	Ja	Ja	Ja	Ja	Ja	Ja	Nein	Nein
AWS::EC2::NatGateway	Ja	Ja	Ja	Ja	Ja	Ja	Nein	Ja
AWS::EC2::NetworkAcl	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja
AWS::EC2::NetworkInsightsAccessScope	Ja	Ja	Ja	Ja	Ja	Ja	Nein	Nein
AWS::EC2::NetworkInsightsAccessScopeAnalysis	Ja	Ja	Ja	Ja	Ja	Ja	Nein	Nein
AWS::EC2::NetworkInsightsAnalyse	Ja	Ja	Ja	Ja	Ja	Ja	Nein	Nein
AWS::EC2::NetworkInsightsPfad	Ja	Ja	Ja	Ja	Ja	Ja	Nein	Nein
AWS::EC2::NetworkInterface	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja
AWS::EC2::PrefixList	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja

Ressourcentyp	Europa (Irland)	Europa (Frankfurt)	Europa (London)	Europa (Paris)	Europa (Stockholm)	Europa (Milan)	Europa (Spain)	Europa (Zürich)
AWS::EC2::RegisteredHAInstance	Ja	Ja	Ja	Ja	Ja	Nein	Nein	Nein
AWS::EC2::RouteTable	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja
AWS::EC2::SecurityGroup	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja
AWS::EC2::SnapshotBlockPublicAccess	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja
AWS::EC2::SpotFleet	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja
AWS::EC2::Subnet	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja
AWS::EC2::SubnetRouteTableAssociation	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja
AWS::EC2::TrafficMirrorFilter	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja
AWS::EC2::TrafficMirrorSitzung	Ja	Ja	Ja	Ja	Ja	Nein	Nein	Ja
AWS::EC2::TrafficMirrorZiel	Ja	Ja	Ja	Ja	Ja	Ja	Nein	Ja
AWS::EC2::TransitGateway	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja
AWS::EC2::TransitGatewayAnlage	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja

Ressourcentyp	Europa (Irland)	Europa (Frankfurt)	Europa (London)	Europa (Paris)	Europa (Stockholm)	Europa (Milan)	Europa (Spain)	Europa (Zürich)
AWS::EC2::TransitGatewayConnect	Ja	Ja	Ja	Ja	Ja	Ja	Nein	Ja
AWS::EC2::TransitGatewayMulticastDomain	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja
AWS::EC2::TransitGatewayRouteTable	Ja	Ja	Ja	Ja	Ja	Ja	Nein	Ja
AWS:EC2: :VPC	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja
AWS:EC2:: VPCBlockPublicAccessExclusion	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja
AWS:EC2:: VPCBlockPublicAccessOptions	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja
AWS:EC2:: VPCEndpoint	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja
AWS:EC2:: VPCEndpoint ConnectionNotification	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja
AWS:EC2:: VPCEndpoint Dienst	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja
AWS:EC2:: VPCPeering Verbindung	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja
AWS:EC2:: VPNConnection	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja
AWS::EC2:: VPNConnection Route	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja

Ressourcentyp	Europa (Irland)	Europa (Frankfurt)	Europa (London)	Europa (Paris)	Europa (Stockholm)	Europa (Milan)	Europa (Spain)	Europa (Zürich)
AWS:EC2:: VPNGateway	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja
AWS::EC2::Volume	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja
AWS::ECR::PullThroughCacheRule	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja
AWS::ECR::RegistryPolicy	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja
AWS::ECR::Repository	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja
AWS::ECS::CapacityProvider	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja
AWS::ECS::Cluster	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja
AWS::ECS::Service	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja
AWS::ECS::TaskDefinition	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja
AWS::ECS::TaskSet	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja
AWS::EFS::AccessPoint	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja
AWS::EFS::FileSystem	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja

Ressourcentyp	Europa (Irland)	Europa (Frankfurt)	Europa (London)	Europa (Paris)	Europa (Stockholm)	Europa (Milan)	Europa (Spain)	Europa (Zürich)
AWS::EKS::Addon	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja
AWS::EKS::Cluster	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja
AWS::EKS::FargateProfile	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja
AWS::EKS::IdentityProviderConfig	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja
AWS::EMR::SecurityConfiguration	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja
AWS::ElasticBeanstalk::Application	Ja	Ja	Ja	Ja	Ja	Ja	Nein	Nein
AWS::ElasticBeanstalk::ApplicationVersion	Ja	Ja	Ja	Ja	Ja	Ja	Nein	Nein
AWS::ElasticBeanstalk::Environment	Ja	Ja	Ja	Ja	Ja	Ja	Nein	Nein
AWS::ElasticLoadBalancing::LoadBalancer	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja
AWS::ElasticLoadBalancingV2::Listener	Ja	Ja	Ja	Ja	Ja	Ja	Nein	Nein
AWS::ElasticLoadBalancingV2::LoadBalancer	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja
AWS::Elasticsearch::Domain	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja

Ressourcentyp	Europa (Irland)	Europa (Frankfurt)	Europa (London)	Europa (Paris)	Europa (Stockholm)	Europa (Milan)	Europa (Spain)	Europa (Zürich)
AWS::EventSchemas::Discoverer	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja
AWS::EventSchemas::Registry	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja
AWS::EventSchemas::RegistryPolicy	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja
AWS::EventSchemas::Schema	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja
AWS::Events::ApiDestination	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja
AWS::Events::Archive	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja
AWS::Events::Connection	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja
AWS::Events::Endpoint	Ja	Ja	Ja	Ja	Ja	Nein	Nein	Nein
AWS::Events::EventBus	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja
AWS::Events::Rule	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja
AWS::Evidently::Launch	Ja	Ja	Nein	Nein	Ja	Nein	Nein	Nein
AWS::Evidently::Project	Ja	Ja	Nein	Nein	Ja	Nein	Nein	Nein

Ressourcentyp	Europa (Irland)	Europa (Frankfurt)	Europa (London)	Europa (Paris)	Europa (Stockholm)	Europa (Milan)	Europa (Spain)	Europa (Zürich)
AWS::Evidently::Segment	Ja	Ja	Nein	Nein	Ja	Nein	Nein	Nein
AWS::FIS::ExperimentTemplate	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Nein
AWS::Forecast::Dataset	Ja	Ja	Nein	Nein	Nein	Nein	Nein	Nein
AWS::Forecast::DatasetGroup	Ja	Ja	Nein	Nein	Nein	Nein	Nein	Nein
AWS::FraudDetector::EntityType	Ja	Nein	Nein	Nein	Nein	Nein	Nein	Nein
AWS::FraudDetector::Label	Ja	Nein	Nein	Nein	Nein	Nein	Nein	Nein
AWS::FraudDetector::Outcome	Ja	Nein	Nein	Nein	Nein	Nein	Nein	Nein
AWS::FraudDetector::Variable	Ja	Nein	Nein	Nein	Nein	Nein	Nein	Nein
AWS::Glue::Classifier	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja
AWS::Glue::Job	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja
AWS::Glue::MLTransform	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja
AWS::Grafana::Workspace	Ja	Ja	Ja	Nein	Nein	Nein	Nein	Nein

Ressourcentyp	Europa (Irland)	Europa (Frankfurt)	Europa (London)	Europa (Paris)	Europa (Stockholm)	Europa (Milan)	Europa (Spain)	Europa (Zürich)
AWS::GreengrassV2::ComponentVersion	Ja	Ja	Ja	Nein	Nein	Nein	Nein	Nein
AWS::GroundStation::Config	Ja	Ja	Nein	Nein	Ja	Nein	Nein	Nein
AWS::GroundStation::DataflowEndpointGruppe	Ja	Ja	Nein	Nein	Ja	Nein	Nein	Nein
AWS::GroundStation::MissionProfile	Ja	Ja	Nein	Nein	Ja	Nein	Nein	Nein
AWS::GuardDuty::Detector	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja
AWS::GuardDuty::Filter	Ja	Ja	Ja	Ja	Ja	Ja	Nein	Nein
AWS::GuardPflicht: IPSet	Ja	Ja	Ja	Ja	Ja	Ja	Nein	Nein
AWS::GuardDuty::ThreatIntelSatz	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja
AWS::IAM::Group	Ja	Ja	Ja	Ja	Ja	Ja	Nein	Nein
AWS::IAM::Policy	Ja	Ja	Ja	Ja	Ja	Ja	Nein	Nein
AWS::IAM::Role	Ja	Ja	Ja	Ja	Ja	Ja	Nein	Nein
AWS::IAM::User	Ja	Ja	Ja	Ja	Ja	Ja	Nein	Nein

Ressourcentyp	Europa (Irland)	Europa (Frankfurt)	Europa (London)	Europa (Paris)	Europa (Stockholm)	Europa (Milan)	Europa (Spain)	Europa (Zürich)
AWS::IVS::Channel	Ja	Ja	Nein	Nein	Nein	Nein	Nein	Nein
AWS::IVS::PlaybackKeyPaar	Ja	Ja	Nein	Nein	Nein	Nein	Nein	Nein
AWS::IVS::RecordingConfiguration	Ja	Ja	Nein	Nein	Nein	Nein	Nein	Nein
AWS::ImageBuilder::ContainerRecipe	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja
AWS::ImageBuilder::DistributionConfiguration	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja
AWS::ImageBuilder::ImagePipeline	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja
AWS::ImageBuilder::ImageRecipe	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja
AWS::ImageBuilder::InfrastructureConfiguration	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja
AWS::InspectorV2::Activation	Ja	Ja	Ja	Ja	Ja	Ja	Nein	Ja
AWS::InspectorV2::Filter	Ja	Ja	Ja	Ja	Ja	Ja	Nein	Ja
AWS::IoT::AccountAuditKonfiguration	Ja	Ja	Ja	Ja	Ja	Nein	Nein	Nein
AWS::IoT::Authorizer	Ja	Ja	Ja	Ja	Ja	Nein	Nein	Nein

Ressourcentyp	Europa (Irland)	Europa (Frankfurt)	Europa (London)	Europa (Paris)	Europa (Stockholm)	Europa (Milan)	Europa (Spain)	Europa (Zürich)
AWS::IoT: CACertificate	Ja	Ja	Ja	Ja	Ja	Nein	Nein	Nein
AWS::IoT::CustomMetric	Ja	Ja	Ja	Ja	Ja	Nein	Nein	Nein
AWS::IoT::Dimension	Ja	Ja	Ja	Ja	Ja	Nein	Nein	Nein
AWS::IoT::FleetMetric	Ja	Ja	Ja	Ja	Ja	Nein	Nein	Nein
AWS::IoT::JobTemplate	Ja	Ja	Ja	Ja	Ja	Nein	Nein	Nein
AWS::IoT::MitigationAction	Ja	Ja	Ja	Ja	Ja	Nein	Nein	Nein
AWS::IoT::Policy	Ja	Ja	Ja	Ja	Ja	Nein	Nein	Nein
AWS::IoT::ProvisioningTemplate	Ja	Ja	Ja	Ja	Ja	Nein	Nein	Nein
AWS::IoT::RoleAlias	Ja	Ja	Ja	Ja	Ja	Nein	Nein	Nein
AWS::IoT::ScheduledAudit	Ja	Ja	Ja	Ja	Ja	Nein	Nein	Nein
AWS::IoT::SecurityProfile	Ja	Ja	Ja	Ja	Ja	Nein	Nein	Nein
AWS::IoTAnalytics::Channel	Ja	Ja	Nein	Nein	Nein	Nein	Nein	Nein

Ressourcentyp	Europa (Irland)	Europa (Frankfurt)	Europa (London)	Europa (Paris)	Europa (Stockholm)	Europa (Milan)	Europa (Spain)	Europa (Zürich)
AWS::IoTAnalytics::Dataset	Ja	Ja	Nein	Nein	Nein	Nein	Nein	Nein
AWS::IoTAnalytics::Datastore	Ja	Ja	Nein	Nein	Nein	Nein	Nein	Nein
AWS::IoTAnalytics::Pipeline	Ja	Ja	Nein	Nein	Nein	Nein	Nein	Nein
AWS::IoTEvents::AlarmModel	Ja	Ja	Ja	Nein	Nein	Nein	Nein	Nein
AWS::IoTEvents::DetectorModel	Ja	Ja	Ja	Nein	Nein	Nein	Nein	Nein
AWS::IoTEvents::Input	Ja	Ja	Ja	Nein	Nein	Nein	Nein	Nein
AWS::IoTSiteWise::AssetModel	Ja	Ja	Nein	Nein	Nein	Nein	Nein	Nein
AWS::IoTSiteWise::Dashboard	Ja	Ja	Nein	Nein	Nein	Nein	Nein	Nein
AWS::IoTSiteWise::Gateway	Ja	Ja	Nein	Nein	Nein	Nein	Nein	Nein
AWS::IoTSiteWise::Portal	Ja	Ja	Nein	Nein	Nein	Nein	Nein	Nein
AWS::IoTSiteWise::Project	Ja	Ja	Nein	Nein	Nein	Nein	Nein	Nein
AWS::IoTTwinMaker::ComponentType	Ja	Ja	Nein	Nein	Nein	Nein	Nein	Nein

Ressourcentyp	Europa (Irland)	Europa (Frankfurt)	Europa (London)	Europa (Paris)	Europa (Stockholm)	Europa (Milan)	Europa (Spain)	Europa (Zürich)
AWS::IoTTwinMaker::Entity	Ja	Ja	Nein	Nein	Nein	Nein	Nein	Nein
AWS::IoTTwinMaker::Scene	Ja	Ja	Nein	Nein	Nein	Nein	Nein	Nein
AWS::IoTTwinMaker::SyncJob	Ja	Ja	Nein	Nein	Nein	Nein	Nein	Nein
AWS::IoTTwinMaker::Workspace	Ja	Ja	Nein	Nein	Nein	Nein	Nein	Nein
AWS::IoTWireless::FuotaTask	Ja	Ja	Nein	Nein	Nein	Nein	Nein	Nein
AWS::IoTWireless::MulticastGroup	Ja	Ja	Nein	Nein	Nein	Nein	Nein	Nein
AWS::IoTWireless::ServiceProfile	Ja	Ja	Nein	Nein	Nein	Nein	Nein	Nein
AWS::KMS::Alias	Ja	Ja	Ja	Ja	Ja	Ja	Nein	Ja
AWS::KMS::Key	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja
AWS::KafkaConnect::Connector	Ja	Ja	Ja	Ja	Ja	Nein	Nein	Nein
AWS::Kendra::Index	Ja	Nein	Ja	Nein	Nein	Nein	Nein	Nein
AWS::Kinesis::Stream	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja

Ressourcentyp	Europa (Irland)	Europa (Frankfurt)	Europa (London)	Europa (Paris)	Europa (Stockholm)	Europa (Milan)	Europa (Spain)	Europa (Zürich)
AWS::Kinesis::StreamConsumer	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja
AWS::KinesisAnalyticsV2::Application	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja
AWS::KinesisFirehose::DeliveryStream	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja
AWS::KinesisVideo::SignalingChannel	Ja	Ja	Ja	Ja	Nein	Nein	Nein	Nein
AWS::KinesisVideo::Stream	Ja	Ja	Ja	Ja	Nein	Nein	Nein	Nein
AWS::Lambda::CodeSigningConfig	Ja	Ja	Ja	Ja	Ja	Ja	Nein	Nein
AWS::Lambda::Function	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja
AWS::Lex::Bot	Ja	Ja	Ja	Nein	Nein	Nein	Nein	Nein
AWS::Lex::BotAlias	Ja	Ja	Ja	Nein	Nein	Nein	Nein	Nein
AWS::Lightsail::Bucket	Ja	Ja	Ja	Ja	Ja	Nein	Nein	Nein
AWS::Lightsail::Certificate	Ja	Ja	Ja	Ja	Ja	Nein	Nein	Nein
AWS::Lightsail::Disk	Ja	Ja	Ja	Ja	Ja	Nein	Nein	Nein

Ressourcentyp	Europa (Irland)	Europa (Frankfurt)	Europa (London)	Europa (Paris)	Europa (Stockholm)	Europa (Milan)	Europa (Spain)	Europa (Zürich)
AWS::Lightsail::StaticIp	Ja	Ja	Ja	Ja	Ja	Nein	Nein	Nein
AWS::Logs::Destination	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja
AWS::LookoutMetrics::Alert	Ja	Ja	Nein	Nein	Ja	Nein	Nein	Nein
AWS::LookoutVision::Project	Ja	Ja	Nein	Nein	Nein	Nein	Nein	Nein
AWS::M2::Environment	Ja	Ja	Ja	Ja	Ja	Ja	Nein	Nein
AWS::MSK::BatchScramGeheim	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja
AWS::MSK::Cluster	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja
AWS::MSK::ClusterPolicy	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja
AWS::MSK::Configuration	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja
AWS::MSK::VpcConnection	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja
AWS::Macie::Session	Ja	Ja	Ja	Ja	Ja	Ja	Nein	Nein
AWS::MediaConnect::FlowEntitlement	Ja	Ja	Ja	Ja	Ja	Nein	Nein	Nein

Ressourcentyp	Europa (Irland)	Europa (Frankfurt)	Europa (London)	Europa (Paris)	Europa (Stockholm)	Europa (Milan)	Europa (Spain)	Europa (Zürich)
AWS::MediaConnect::FlowSource	Ja	Ja	Ja	Ja	Ja	Nein	Nein	Nein
AWS::MediaConnect::FlowVpcSchnittstelle	Ja	Ja	Ja	Ja	Ja	Nein	Nein	Nein
AWS::MediaConnect::Gateway	Ja	Ja	Ja	Ja	Ja	Nein	Nein	Nein
AWS::MediaPackage::PackagingConfiguration	Ja	Ja	Ja	Ja	Ja	Nein	Nein	Nein
AWS::MediaPackage::PackagingGroup	Ja	Ja	Ja	Ja	Ja	Nein	Nein	Nein
AWS::MediaTailor::PlaybackConfiguration	Ja	Ja	Nein	Ja	Ja	Nein	Nein	Nein
AWS::MemoryDB::SubnetGroup	Ja	Ja	Ja	Nein	Ja	Nein	Nein	Nein
AWS::NetworkFirewall::Firewall	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja
AWS::NetworkFirewall::FirewallPolicy	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja
AWS::NetworkFirewall::RuleGroup	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja
AWS::NetworkFirewall: TLSInspection Konfiguration	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja

Ressourcentyp	Europa (Irland)	Europa (Frankfurt)	Europa (London)	Europa (Paris)	Europa (Stockholm)	Europa (Milan)	Europa (Spain)	Europa (Zürich)
AWS::NetworkFirewall::VpcEndpointAssoziation	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja
AWS::OpenSearch::Domain	Ja	Ja	Ja	Ja	Ja	Ja	Nein	Nein
AWS::OpenSearchServerless::Collection	Ja	Ja	Ja	Ja	Nein	Nein	Nein	Nein
AWS::OpenSearchServerless::VpcEndpoint	Ja	Ja	Ja	Ja	Nein	Nein	Nein	Nein
AWS::Panorama::Package	Ja	Nein	Nein	Nein	Nein	Nein	Nein	Nein
AWS::Personalize::Dataset	Ja	Ja	Nein	Nein	Nein	Nein	Nein	Nein
AWS::Personalize::DatasetGroup	Ja	Ja	Nein	Nein	Nein	Nein	Nein	Nein
AWS::Personalize::Schema	Ja	Ja	Nein	Nein	Nein	Nein	Nein	Nein
AWS::Personalize::Solution	Ja	Ja	Nein	Nein	Nein	Nein	Nein	Nein
AWS::Pinpoint::App	Ja	Ja	Ja	Nein	Nein	Nein	Nein	Nein
AWS::Pinpoint::ApplicationSettings	Ja	Ja	Ja	Nein	Nein	Nein	Nein	Nein
AWS::Pinpoint::Campaign	Ja	Ja	Ja	Nein	Nein	Nein	Nein	Nein

Ressourcentyp	Europa (Irland)	Europa (Frankfurt)	Europa (London)	Europa (Paris)	Europa (Stockholm)	Europa (Milan)	Europa (Spain)	Europa (Zürich)
AWS::Pinpoint::EmailChannel	Ja	Ja	Ja	Nein	Nein	Nein	Nein	Nein
AWS::Pinpoint::EmailTemplate	Ja	Ja	Ja	Nein	Nein	Nein	Nein	Nein
AWS::Pinpoint::EventStream	Ja	Ja	Ja	Nein	Nein	Nein	Nein	Nein
AWS::Pinpoint::InAppVorlage	Ja	Ja	Ja	Nein	Nein	Nein	Nein	Nein
AWS::Pinpoint::Segment	Ja	Ja	Ja	Nein	Nein	Nein	Nein	Nein
AWS::QLDB::Ledger	Ja	Ja	Ja	Nein	Nein	Nein	Nein	Nein
AWS::QuickSight::DataSource	Ja	Ja	Ja	Ja	Ja	Nein	Nein	Nein
AWS::QuickSight::Template	Ja	Ja	Ja	Ja	Ja	Nein	Nein	Nein
AWS::QuickSight::Theme	Ja	Ja	Ja	Ja	Ja	Nein	Nein	Nein
AWS: :RDS:: DBCluster	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja
AWS: :RDS:: Schnappschuss DBCluster	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja
AWS: :RDS:: DBInstance	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja

Ressourcentyp	Europa (Irland)	Europa (Frankfurt)	Europa (London)	Europa (Paris)	Europa (Stockholm)	Europa (Milan)	Europa (Spain)	Europa (Zürich)
AWS: :RDS:: Gruppe DBSecurity	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja
AWS: :RDS:: DBSnapshot	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja
AWS: :RDS:: Gruppe DBSubnet	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja
AWS::RDS: :EventSubscription	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja
AWS::RDS::GlobalCluster	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja
AWS::RDS::OptionGroup	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja
AWS::RUM::AppMonitor	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja
AWS::Redshift::Cluster	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja
AWS::Redshift::ClusterParameterGruppe	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja
AWS::Redshift::ClusterSecurityGruppe	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja
AWS::Redshift::ClusterSnapshot	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja
AWS::Redshift::ClusterSubnetGruppe	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja

Ressourcentyp	Europa (Irland)	Europa (Frankfurt)	Europa (London)	Europa (Paris)	Europa (Stockholm)	Europa (Milan)	Europa (Spain)	Europa (Zürich)
AWS::Redshift::EndpointAccess	Ja	Ja	Ja	Ja	Ja	Nein	Nein	Nein
AWS::Redshift::EndpointAuthorization	Ja	Ja	Ja	Ja	Ja	Nein	Nein	Nein
AWS::Redshift::EventSubscription	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja
AWS::Redshift::ScheduledAction	Ja	Ja	Ja	Ja	Ja	Ja	Nein	Nein
AWS::ResilienceHub::App	Ja	Ja	Ja	Ja	Ja	Ja	Nein	Nein
AWS::ResilienceHub::ResiliencyPolicy	Ja	Ja	Ja	Ja	Ja	Ja	Nein	Nein
AWS::ResourceExplorer2::Index	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja
AWS::RoboMaker::RobotApplication	Ja	Ja	Nein	Nein	Nein	Nein	Nein	Nein
AWS::RoboMaker::RobotApplicationVersion	Ja	Ja	Nein	Nein	Nein	Nein	Nein	Nein
AWS::RoboMaker::SimulationApplication	Ja	Ja	Nein	Nein	Nein	Nein	Nein	Nein
AWS::Route53Profiles::Profile	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja
AWS::Route53Resolver::FirewallDomainListe	Ja	Ja	Ja	Ja	Ja	Ja	Nein	Nein

Ressourcentyp	Europa (Irland)	Europa (Frankfurt)	Europa (London)	Europa (Paris)	Europa (Stockholm)	Europa (Milan)	Europa (Spain)	Europa (Zürich)
AWS::Route53Resolver::FirewallRuleGruppe	Ja	Ja	Ja	Ja	Ja	Ja	Nein	Nein
AWS::Route53Resolver::FirewallRuleGroupAssociation	Ja	Ja	Ja	Ja	Ja	Ja	Nein	Nein
AWS::Route53Resolver::ResolverEndpoint	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja
AWS::Route53Resolver::ResolverQueryLoggingConfig	Ja	Ja	Ja	Ja	Ja	Ja	Nein	Nein
AWS::Route53Resolver::ResolverQueryLoggingConfigAssociation	Ja	Ja	Ja	Ja	Ja	Ja	Nein	Nein
AWS::Route53Resolver::ResolverRule	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja
AWS::Route53Resolver::ResolverRuleVerband	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja
AWS::S3::AccessPoint	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja
AWS::S3::AccountPublicAccessBlock	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja
AWS::S3::Bucket	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja
AWS::S3::StorageLens	Ja	Ja	Ja	Ja	Ja	Nein	Nein	Nein

Ressourcentyp	Europa (Irland)	Europa (Frankfurt)	Europa (London)	Europa (Paris)	Europa (Stockholm)	Europa (Milan)	Europa (Spain)	Europa (Zürich)
AWS::S3::StorageLensGruppe	Ja	Ja	Ja	Ja	Ja	Nein	Nein	Nein
AWS::S3Express::BucketPolicy	Ja	Nein	Nein	Nein	Ja	Nein	Nein	Nein
AWS::S3Express::DirectoryBucket	Ja	Nein	Nein	Nein	Ja	Nein	Nein	Nein
AWS::SES::ConfigurationSet	Ja	Ja	Ja	Ja	Ja	Ja	Nein	Nein
AWS::SES::ContactList	Ja	Ja	Ja	Ja	Ja	Ja	Nein	Nein
AWS::SES::ReceiptFilter	Ja	Ja	Ja	Nein	Nein	Nein	Nein	Nein
AWS::SES::ReceiptRuleSatz	Ja	Ja	Ja	Nein	Nein	Nein	Nein	Nein
AWS::SES::Template	Ja	Ja	Ja	Ja	Ja	Ja	Nein	Nein
AWS::SNS::Topic	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja
AWS::SQS::Queue	Ja	Ja	Ja	Ja	Ja	Ja	Nein	Nein
AWS::SSM::AssociationCompliance	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja
AWS::SSM::Document	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja

Ressourcentyp	Europa (Irland)	Europa (Frankfurt)	Europa (London)	Europa (Paris)	Europa (Stockholm)	Europa (Milan)	Europa (Spain)	Europa (Zürich)
AWS::SSM::FileData	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja
AWS::SSM::ManagedInstance-Bestand	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja
AWS::SSM::PatchCompliance	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja
AWS::SageMaker::AppImageConfig	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Nein
AWS::SageMaker::CodeRepository	Ja	Ja	Ja	Ja	Ja	Ja	Nein	Nein
AWS::SageMaker::Domain	Ja	Ja	Ja	Ja	Ja	Ja	Nein	Nein
AWS::SageMaker::EndpointConfig	Ja	Ja	Ja	Ja	Ja	Ja	Nein	Nein
AWS::SageMaker::FeatureGroup	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Nein
AWS::SageMaker::Image	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Nein
AWS::SageMaker::InferenceExperiment	Ja	Ja	Ja	Ja	Ja	Ja	Nein	Nein
AWS::SageMaker::Model	Ja	Ja	Ja	Ja	Ja	Ja	Nein	Nein
AWS::SageMaker::NotebookInstance	Ja	Ja	Ja	Ja	Ja	Ja	Nein	Nein

Ressourcentyp	Europa (Irland)	Europa (Frankfurt)	Europa (London)	Europa (Paris)	Europa (Stockholm)	Europa (Milan)	Europa (Spain)	Europa (Zürich)
AWS::SageMaker::NotebookInstanceLifecycleConfig	Ja	Ja	Ja	Ja	Ja	Ja	Nein	Nein
AWS::SageMaker::Workteam	Ja	Ja	Ja	Nein	Nein	Nein	Nein	Nein
AWS::SecretsManager::Secret	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja
AWS::SecurityHub::Standard	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja
AWS::ServiceCatalog::CloudFormationProdukt	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja
AWS::ServiceCatalog::CloudFormationProvisionedProduct	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja
AWS::ServiceCatalog::Portfolio	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja
AWS::ServiceDiscovery::HttpNamespace	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja
AWS::ServiceDiscovery::Instance	Ja	Ja	Ja	Ja	Ja	Ja	Nein	Nein
AWS::ServiceDiscovery::PublicDnsNamespace	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja
AWS::ServiceDiscovery::Service	Ja	Ja	Ja	Ja	Ja	Ja	Nein	Nein

Ressourcentyp	Europa (Irland)	Europa (Frankfurt)	Europa (London)	Europa (Paris)	Europa (Stockholm)	Europa (Milan)	Europa (Spain)	Europa (Zürich)
AWS::ShieldRegional::Protection	Ja	Ja	Ja	Ja	Ja	Ja	Nein	Nein
AWS::Signer::SigningProfile	Ja	Ja	Ja	Ja	Ja	Ja	Nein	Nein
AWS::Step Functions::Activity	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja
AWS::StepFunctions::StateMachine	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja
AWS::Transfer::Agreement	Ja	Ja	Ja	Ja	Ja	Ja	Nein	Nein
AWS::Transfer::Certificate	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja
AWS::Transfer::Connector	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja
AWS::Transfer::Profile	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja
AWS::Transfer::Workflow	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja
AWS::WAFRegional::RateBasedRegel	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja
AWS::WAFRegional::Rule	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja
AWS::WAFRegional::RuleGroup	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja

Ressourcentyp	Europa (Irland)	Europa (Frankfurt)	Europa (London)	Europa (Paris)	Europa (Stockholm)	Europa (Milan)	Europa (Spain)	Europa (Zürich)
AWS::WAFRegional::WebACL	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja
AWS:WAFv2:: IPSet	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja
AWS::WAFv2::ManagedRuleSatz	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja
AWS::WAFv2::RegexPatternSatz	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja
AWS::WAFv2::RuleGroup	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja
AWS::WAFv2::WebACL	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja
AWS::WorkSpaces::ConnectionAlias	Ja	Ja	Ja	Nein	Nein	Nein	Nein	Nein
AWS::WorkSpaces::Workspace	Ja	Ja	Ja	Nein	Nein	Nein	Nein	Nein
AWS::XRay::EncryptionConfig	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja

Regionen in Asien-Pazifik

Ressourcentyp	Asien-Pazifik (Hongkong)	Asien-Pazifik (Hyderabad)	Asien-Pazifik (Jakarta)	Asien-Pazifik (Malaysia)	Asien-Pazifik (Melbourne)	Asien-Pazifik (Mumbai)	Asien-Pazifik (Osaka)	Asien-Pazifik (Seoul)	Asien-Pazifik (Singapur)	Asien-Pazifik (Sydney)	Asien-Pazifik (Taipeh)	Asien-Pazifik (Thailand)	Asien-Pazifik (Tokio)
AWS::ACM::Certificate	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja
AWS::ACMPCA::CertificateAuthority	Ja	Ja	Ja	Nein	Ja	Ja	Ja	Ja	Ja	Ja	Nein	Nein	Ja
AWS::ACMPCA::CertificateAuthorityAktivierung	Ja	Ja	Ja	Nein	Ja	Ja	Ja	Ja	Ja	Ja	Nein	Nein	Ja
AWS::APS::RuleGroupsNamespace	Nein	Nein	Nein	Nein	Nein	Ja	Nein	Ja	Ja	Ja	Nein	Nein	Ja
AWS::AccessAnalyzer::Analyzer	Ja	Ja	Ja	Nein	Ja	Ja	Ja	Ja	Ja	Ja	Nein	Nein	Ja
AWS::AmazonMQ::Broker	Ja	Nein	Ja	Nein	Ja	Ja	Ja	Ja	Ja	Ja	Nein	Nein	Ja
AWS::Amplify::App	Ja	Nein	Nein	Nein	Nein	Ja	Ja	Ja	Ja	Ja	Nein	Nein	Ja
AWS::Amplify::Branch	Ja	Nein	Nein	Nein	Nein	Ja	Ja	Ja	Ja	Ja	Nein	Nein	Ja
AWS::ApiGateway::RestApi	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Nein	Ja	Ja

Ressourcentyp	Asien-Pazifik (Hongkong)	Asien-Pazifik (Hyderabad)	Asien-Pazifik (Jakarta)	Asien-Pazifik (Malaysia)	Asien-Pazifik (Melbourne)	Asien-Pazifik (Mumbai)	Asien-Pazifik (Osaka)	Asien-Pazifik (Seoul)	Asien-Pazifik (Singapur)	Asien-Pazifik (Sydney)	Asien-Pazifik (Taipeh)	Asien-Pazifik (Thailand)	Asien-Pazifik (Tokio)
AWS::ApiGateway::Stage	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Nein	Ja	Ja
AWS::ApiGatewayV2::Api	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Nein	Ja	Ja
AWS::ApiGatewayV2::Stage	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Nein	Ja	Ja
AWS::AppConfig::Application	Ja	Nein	Ja	Nein	Ja	Ja	Ja	Ja	Ja	Ja	Nein	Nein	Ja
AWS::AppConfig::ConfigurationProfile	Ja	Nein	Ja	Nein	Ja	Ja	Ja	Ja	Ja	Ja	Nein	Nein	Ja
AWS::AppConfig::DeploymentStrategy	Ja	Ja	Ja	Nein	Ja	Ja	Ja	Ja	Ja	Ja	Nein	Nein	Ja
AWS::AppConfig::Environment	Ja	Nein	Ja	Nein	Ja	Ja	Ja	Ja	Ja	Ja	Nein	Nein	Ja
AWS::AppConfig::ExtensionAssociation	Ja	Ja	Ja	Nein	Ja	Ja	Ja	Ja	Ja	Ja	Nein	Nein	Ja
AWS::AppConfig::HostedConfigurationVersion	Ja	Nein	Ja	Nein	Ja	Ja	Ja	Ja	Ja	Ja	Nein	Nein	Ja

Ressourcentyp	Asien-Pazifik (Hongkong)	Asien-Pazifik (Hyderabad)	Asien-Pazifik (Jakarta)	Asien-Pazifik (Malaysia)	Asien-Pazifik (Melbourne)	Asien-Pazifik (Mumbai)	Asien-Pazifik (Osaka)	Asien-Pazifik (Seoul)	Asien-Pazifik (Singapur)	Asien-Pazifik (Sydney)	Asien-Pazifik (Taipeh)	Asien-Pazifik (Thailand)	Asien-Pazifik (Tokio)
AWS::AppFlow::Flow	Nein	Nein	Nein	Nein	Nein	Ja	Nein	Ja	Ja	Ja	Nein	Nein	Ja
AWS::AppIntegrations::Application	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Ja	Ja	Ja	Nein	Nein	Ja
AWS::AppIntegrations::EventIntegration	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Ja	Ja	Ja	Nein	Nein	Ja
AWS::AppMesh::GatewayRoute	Ja	Nein	Ja	Nein	Nein	Ja	Ja	Ja	Ja	Ja	Nein	Nein	Ja
AWS::AppMesh::Mesh	Ja	Nein	Ja	Nein	Nein	Ja	Ja	Ja	Ja	Ja	Nein	Nein	Ja
AWS::AppMesh::Route	Ja	Nein	Ja	Nein	Nein	Ja	Ja	Ja	Ja	Ja	Nein	Nein	Ja
AWS::AppMesh::VirtualGateway	Ja	Nein	Ja	Nein	Nein	Ja	Ja	Ja	Ja	Ja	Nein	Nein	Ja
AWS::AppMesh::VirtualNode	Ja	Nein	Ja	Nein	Nein	Ja	Ja	Ja	Ja	Ja	Nein	Nein	Ja
AWS::AppMesh::VirtualRouter	Ja	Nein	Ja	Nein	Nein	Ja	Ja	Ja	Ja	Ja	Nein	Nein	Ja

Ressourcentyp	Asien-Pazifik (Hongkong)	Asien-Pazifik (Hyderabad)	Asien-Pazifik (Jakarta)	Asien-Pazifik (Malaysia)	Asien-Pazifik (Melbourne)	Asien-Pazifik (Mumbai)	Asien-Pazifik (Osaka)	Asien-Pazifik (Seoul)	Asien-Pazifik (Singapur)	Asien-Pazifik (Sydney)	Asien-Pazifik (Taipeh)	Asien-Pazifik (Thailand)	Asien-Pazifik (Tokio)
AWS::AppMesh::VirtualService	Ja	Nein	Ja	Nein	Nein	Ja	Ja	Ja	Ja	Ja	Nein	Nein	Ja
AWS::AppRunner::Service	Nein	Nein	Nein	Nein	Nein	Ja	Nein	Nein	Ja	Ja	Nein	Nein	Ja
AWS::AppRunner::VpcConnector	Nein	Nein	Nein	Nein	Nein	Ja	Nein	Nein	Ja	Ja	Nein	Nein	Ja
AWS::AppStream::Application	Nein	Nein	Nein	Nein	Nein	Ja	Nein	Ja	Ja	Ja	Nein	Nein	Ja
AWS::AppStream::DirectoryConfig	Nein	Nein	Nein	Nein	Nein	Ja	Nein	Ja	Ja	Ja	Nein	Nein	Ja
AWS::AppStream::Fleet	Nein	Nein	Nein	Nein	Nein	Ja	Nein	Ja	Ja	Ja	Nein	Nein	Ja
AWS::AppStream::Stack	Nein	Nein	Nein	Nein	Nein	Ja	Nein	Ja	Ja	Ja	Nein	Nein	Ja
AWS::AppSync::ApiCache	Ja	Ja	Ja	Nein	Ja	Ja	Ja	Ja	Ja	Ja	Nein	Nein	Ja
AWS::AppSync::GraphQLApi	Ja	Ja	Ja	Nein	Ja	Ja	Ja	Ja	Ja	Ja	Nein	Nein	Ja
AWS::Athena::DataCatalog	Ja	Ja	Ja	Nein	Ja	Ja	Ja	Ja	Ja	Ja	Nein	Nein	Ja

Ressourcentyp	Asien-Pazifik (Hongkong)	Asien-Pazifik (Hyderabad)	Asien-Pazifik (Jakarta)	Asien-Pazifik (Malaysia)	Asien-Pazifik (Melbourne)	Asien-Pazifik (Mumbai)	Asien-Pazifik (Osaka)	Asien-Pazifik (Seoul)	Asien-Pazifik (Singapur)	Asien-Pazifik (Sydney)	Asien-Pazifik (Taipeh)	Asien-Pazifik (Thailand)	Asien-Pazifik (Tokio)
AWS::Athena::PreparedStatement	Ja	Ja	Ja	Nein	Ja	Ja	Ja	Ja	Ja	Ja	Nein	Nein	Ja
AWS::Athena::WorkGroup	Ja	Ja	Ja	Nein	Ja	Ja	Ja	Ja	Ja	Ja	Nein	Nein	Ja
AWS::AuditManager::Assessment	Nein	Nein	Nein	Nein	Nein	Ja	Nein	Nein	Ja	Ja	Nein	Nein	Ja
AWS::AutoScaling::AutoScalingGruppe	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja
AWS::AutoScaling::LaunchConfiguration	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja
AWS::AutoScaling::ScalingPolicy	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja
AWS::AutoScaling::ScheduledAction	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja
AWS::AutoScaling::WarmPool	Ja	Nein	Ja	Nein	Nein	Ja	Ja	Ja	Ja	Ja	Nein	Nein	Ja

Ressourcentyp	Asien-Pazifik (Hongkong)	Asien-Pazifik (Hyderabad)	Asien-Pazifik (Jakarta)	Asien-Pazifik (Malaysia)	Asien-Pazifik (Melbourne)	Asien-Pazifik (Mumbai)	Asien-Pazifik (Osaka)	Asien-Pazifik (Seoul)	Asien-Pazifik (Singapur)	Asien-Pazifik (Sydney)	Asien-Pazifik (Taipeh)	Asien-Pazifik (Thailand)	Asien-Pazifik (Tokio)
AWS::Backup::BackupPlan	Ja	Ja	Ja	Nein	Ja	Ja	Ja	Ja	Ja	Ja	Nein	Nein	Ja
AWS::Backup::BackupSelection	Ja	Ja	Ja	Nein	Ja	Ja	Ja	Ja	Ja	Ja	Nein	Nein	Ja
AWS::Backup::BackupVault	Ja	Ja	Ja	Nein	Ja	Ja	Ja	Ja	Ja	Ja	Nein	Nein	Ja
AWS::Backup::RecoveryPoint	Ja	Ja	Ja	Nein	Ja	Ja	Ja	Ja	Ja	Ja	Nein	Nein	Ja
AWS::Backup::ReportPlan	Ja	Nein	Nein	Nein	Nein	Ja	Nein	Ja	Ja	Ja	Nein	Nein	Ja
AWS::Batch::ComputeEnvironment	Ja	Ja	Ja	Nein	Nein	Ja	Ja	Ja	Ja	Ja	Nein	Nein	Ja
AWS::Batch::JobQueue	Ja	Ja	Ja	Nein	Nein	Ja	Ja	Ja	Ja	Ja	Nein	Nein	Ja
AWS::Batch::SchedulingPolicy	Ja	Ja	Ja	Nein	Ja	Ja	Ja	Ja	Ja	Ja	Nein	Nein	Ja
AWS::Bedrock::Guardrail	Nein	Ja	Nein	Nein	Nein	Ja	Ja	Ja	Ja	Ja	Ja	Nein	Ja
AWS::Bedrock::KnowledgeBase	Nein	Nein	Nein	Nein	Nein	Ja	Nein	Ja	Ja	Ja	Ja	Nein	Ja

Ressourcentyp	Asien-Pazifik (Hongkong)	Asien-Pazifik (Hyderabad)	Asien-Pazifik (Jakarta)	Asien-Pazifik (Malaysia)	Asien-Pazifik (Melbourne)	Asien-Pazifik (Mumbai)	Asien-Pazifik (Osaka)	Asien-Pazifik (Seoul)	Asien-Pazifik (Singapur)	Asien-Pazifik (Sydney)	Asien-Pazifik (Taipeh)	Asien-Pazifik (Thailand)	Asien-Pazifik (Tokio)
AWS::Cassandra::Keyspace	Ja	Nein	Nein	Nein	Nein	Ja	Nein	Ja	Ja	Ja	Nein	Nein	Ja
AWS::Cloud9::EnvironmentEC2	Ja	Nein	Nein	Nein	Nein	Ja	Ja	Ja	Ja	Ja	Nein	Nein	Ja
AWS::CloudFormation::Stack	Ja	Nein	Nein	Nein	Nein	Ja	Ja	Ja	Ja	Ja	Nein	Nein	Ja
AWS::CloudTrail::Trail	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja
AWS::CloudWatch::Alarm	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja
AWS::CloudWatch::MetricStream	Ja	Ja	Ja	Nein	Ja	Ja	Ja	Ja	Ja	Ja	Nein	Nein	Ja
AWS::CodeArtifact::Repository	Nein	Nein	Nein	Nein	Nein	Ja	Nein	Nein	Ja	Ja	Nein	Nein	Ja
AWS::CodeBuild::Project	Ja	Ja	Nein	Nein	Ja	Ja	Ja	Ja	Ja	Ja	Nein	Nein	Ja
AWS::CodeBuild::ReportGroup	Ja	Ja	Ja	Nein	Ja	Ja	Ja	Ja	Ja	Ja	Nein	Nein	Ja

Ressourcentyp	Asien-Pazifik (Hongkong)	Asien-Pazifik (Hyderabad)	Asien-Pazifik (Jakarta)	Asien-Pazifik (Malaysia)	Asien-Pazifik (Melbourne)	Asien-Pazifik (Mumbai)	Asien-Pazifik (Osaka)	Asien-Pazifik (Seoul)	Asien-Pazifik (Singapur)	Asien-Pazifik (Sydney)	Asien-Pazifik (Taipeh)	Asien-Pazifik (Thailand)	Asien-Pazifik (Tokio)
AWS::CodeDeploy::Application	Ja	Nein	Nein	Nein	Nein	Ja	Ja	Ja	Ja	Ja	Nein	Nein	Ja
AWS::CodeDeploy::DeploymentConfig	Ja	Nein	Nein	Nein	Nein	Ja	Ja	Ja	Ja	Ja	Nein	Nein	Ja
AWS::CodeDeploy::DeploymentGroup	Ja	Nein	Nein	Nein	Nein	Ja	Ja	Ja	Ja	Ja	Nein	Nein	Ja
AWS::CodeGuruProfiler::ProfilingGroup	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Ja	Ja	Nein	Nein	Ja
AWS::CodeGuruReviewer::RepositoryAssociation	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Ja	Ja	Nein	Nein	Ja
AWS::CodePipeline::Pipeline	Ja	Ja	Nein	Nein	Ja	Ja	Nein	Ja	Ja	Ja	Nein	Nein	Ja
AWS::Cognito::IdentityPool	Ja	Ja	Ja	Nein	Ja	Ja	Ja	Ja	Ja	Ja	Nein	Nein	Ja
AWS::Cognito::UserPool	Ja	Ja	Ja	Nein	Ja	Ja	Ja	Ja	Ja	Ja	Nein	Nein	Ja
AWS::Cognito::UserPoolKunde	Ja	Ja	Ja	Nein	Ja	Ja	Ja	Ja	Ja	Ja	Nein	Nein	Ja

Ressourcentyp	Asien-Pazifik (Hongkong)	Asien-Pazifik (Hyderabad)	Asien-Pazifik (Jakarta)	Asien-Pazifik (Malaysia)	Asien-Pazifik (Melbourne)	Asien-Pazifik (Mumbai)	Asien-Pazifik (Osaka)	Asien-Pazifik (Seoul)	Asien-Pazifik (Singapur)	Asien-Pazifik (Sydney)	Asien-Pazifik (Taipeh)	Asien-Pazifik (Thailand)	Asien-Pazifik (Tokio)
AWS::Cognito::UserPoolGruppe	Ja	Ja	Ja	Nein	Ja	Ja	Ja	Ja	Ja	Ja	Nein	Nein	Ja
AWS::Config::ConfigurationRecorder	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja
AWS::Config::ConformancePack-Compliance	Ja	Ja	Ja	Nein	Ja	Ja	Ja	Ja	Ja	Ja	Nein	Nein	Ja
AWS::Config::ResourceCompliance	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja
AWS::Connect::Instance	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Ja	Ja	Ja	Nein	Nein	Ja
AWS::Connect::PhoneNumber	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Ja	Ja	Ja	Nein	Nein	Ja
AWS::Connect::QuickConnect	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Ja	Ja	Ja	Nein	Nein	Ja
AWS::Connect::Rule	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Ja	Ja	Ja	Nein	Nein	Ja
AWS::Connect::User	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Ja	Ja	Ja	Nein	Nein	Ja

Ressourcentyp	Asien-Pazifik (Hongkong)	Asien-Pazifik (Hyderabad)	Asien-Pazifik (Jakarta)	Asien-Pazifik (Malaysia)	Asien-Pazifik (Melbourne)	Asien-Pazifik (Mumbai)	Asien-Pazifik (Osaka)	Asien-Pazifik (Seoul)	Asien-Pazifik (Singapur)	Asien-Pazifik (Sydney)	Asien-Pazifik (Taipeh)	Asien-Pazifik (Thailand)	Asien-Pazifik (Tokio)
AWS::CustomerProfiles::Domain	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Ja	Ja	Ja	Nein	Nein	Ja
AWS::CustomerProfiles::ObjectType	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Ja	Ja	Ja	Nein	Nein	Ja
AWS::DMS::Certificate	Ja	Nein	Nein	Nein	Nein	Ja	Ja	Ja	Ja	Ja	Nein	Nein	Ja
AWS::DMS::Endpoint	Ja	Nein	Nein	Nein	Nein	Ja	Ja	Ja	Ja	Ja	Nein	Nein	Ja
AWS::DMS::EventSubscription	Ja	Nein	Nein	Nein	Nein	Ja	Ja	Ja	Ja	Ja	Nein	Nein	Ja
AWS::DMS::ReplicationInstance	Ja	Nein	Nein	Nein	Nein	Ja	Ja	Ja	Ja	Ja	Nein	Nein	Ja
AWS::DMS::ReplicationSubnetGruppe	Ja	Nein	Nein	Nein	Nein	Ja	Ja	Ja	Ja	Ja	Nein	Nein	Ja
AWS::DMS::ReplicationTask	Ja	Nein	Nein	Nein	Nein	Ja	Ja	Ja	Ja	Ja	Nein	Nein	Ja
AWS::DataSync::LocationEFS	Ja	Nein	Ja	Nein	Ja	Ja	Ja	Ja	Ja	Ja	Nein	Nein	Ja

Ressourcentyp	Asien-Pazifik (Hongkong)	Asien-Pazifik (Hyderabad)	Asien-Pazifik (Jakarta)	Asien-Pazifik (Malaysia)	Asien-Pazifik (Melbourne)	Asien-Pazifik (Mumbai)	Asien-Pazifik (Osaka)	Asien-Pazifik (Seoul)	Asien-Pazifik (Singapur)	Asien-Pazifik (Sydney)	Asien-Pazifik (Taipeh)	Asien-Pazifik (Thailand)	Asien-Pazifik (Tokio)
AWS::DataSync::LocationFSxGlanz	Ja	Nein	Nein	Nein	Ja	Ja	Ja	Ja	Ja	Ja	Nein	Nein	Ja
AWS::DataSync::LocationFSxFenster	Ja	Nein	Nein	Nein	Ja	Ja	Ja	Ja	Ja	Ja	Nein	Nein	Ja
AWS::DataSync::LocationHDFS	Ja	Ja	Ja	Nein	Ja	Ja	Ja	Ja	Ja	Ja	Nein	Nein	Ja
AWS::DataSync::LocationNFS	Ja	Ja	Ja	Nein	Ja	Ja	Ja	Ja	Ja	Ja	Nein	Nein	Ja
AWS::DataSync::LocationObjectSpeicher	Ja	Ja	Ja	Nein	Ja	Ja	Ja	Ja	Ja	Ja	Nein	Nein	Ja
AWS::DataSync::LocationS3	Ja	Ja	Ja	Nein	Ja	Ja	Ja	Ja	Ja	Ja	Nein	Nein	Ja
AWS::DataSync::LocationKMU	Ja	Ja	Ja	Nein	Ja	Ja	Ja	Ja	Ja	Ja	Nein	Nein	Ja
AWS::DataSync::Task	Ja	Ja	Ja	Nein	Ja	Ja	Ja	Ja	Ja	Ja	Nein	Nein	Ja
AWS::Detective::Graph	Ja	Nein	Nein	Nein	Nein	Ja	Nein	Ja	Ja	Ja	Nein	Nein	Ja

Ressourcentyp	Asien-Pazifik (Hongkong)	Asien-Pazifik (Hyderabad)	Asien-Pazifik (Jakarta)	Asien-Pazifik (Malaysia)	Asien-Pazifik (Melbourne)	Asien-Pazifik (Mumbai)	Asien-Pazifik (Osaka)	Asien-Pazifik (Seoul)	Asien-Pazifik (Singapur)	Asien-Pazifik (Sydney)	Asien-Pazifik (Taipeh)	Asien-Pazifik (Thailand)	Asien-Pazifik (Tokio)
AWS::DynamoDB::Table	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja
AWS::EC2::Capacity Reservation	Ja	Ja	Ja	Nein	Ja	Ja	Ja	Ja	Ja	Ja	Nein	Nein	Ja
AWS::EC2::CarrierGateway	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Ja	Nein	Ja	Nein	Nein	Ja
AWS::EC2::ClientVpnEndpunkt	Ja	Nein	Nein	Nein	Ja	Ja	Ja	Ja	Ja	Ja	Nein	Nein	Ja
AWS::EC2::ClientVpnTargetNetworkAssociation	Ja	Nein	Nein	Nein	Ja	Ja	Ja	Ja	Ja	Ja	Nein	Nein	Ja
AWS::EC2::Customer Gateway	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja
AWS:EC2::DHCPOptions	Ja	Ja	Ja	Nein	Ja	Ja	Ja	Ja	Ja	Ja	Nein	Nein	Ja
AWS:EC2::EC2 Flotte	Ja	Ja	Ja	Nein	Ja	Ja	Ja	Ja	Ja	Ja	Nein	Nein	Ja
AWS::EC2: EIP	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja

Ressourcentyp	Asien-Pazifik (Hongkong)	Asien-Pazifik (Hyderabad)	Asien-Pazifik (Jakarta)	Asien-Pazifik (Malaysia)	Asien-Pazifik (Melbourne)	Asien-Pazifik (Mumbai)	Asien-Pazifik (Osaka)	Asien-Pazifik (Seoul)	Asien-Pazifik (Singapur)	Asien-Pazifik (Sydney)	Asien-Pazifik (Taipeh)	Asien-Pazifik (Thailand)	Asien-Pazifik (Tokio)
AWS:EC2::EIPAssociation	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Nein	Ja	Ja
AWS::EC2::EgressOnlyInternetGateway	Ja	Nein	Ja	Nein	Nein	Ja	Ja	Ja	Ja	Ja	Nein	Nein	Ja
AWS::EC2::FlowLog	Ja	Nein	Ja	Nein	Nein	Ja	Ja	Ja	Ja	Ja	Nein	Nein	Ja
AWS::EC2::Host	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja
AWS:EC2: :IPAM	Ja	Ja	Ja	Nein	Ja	Ja	Ja	Ja	Ja	Ja	Nein	Nein	Ja
AWS:EC2::IPAMPool	Ja	Ja	Ja	Nein	Ja	Ja	Ja	Ja	Ja	Ja	Nein	Nein	Ja
AWS:EC2::IPAMResource Entdeckung	Ja	Ja	Ja	Nein	Ja	Ja	Ja	Ja	Ja	Ja	Nein	Nein	Ja
AWS:EC2::IPAMResource Discovery Association	Ja	Ja	Ja	Nein	Ja	Ja	Ja	Ja	Ja	Ja	Nein	Nein	Ja
AWS:EC2::IPAMScope	Ja	Ja	Ja	Nein	Ja	Ja	Ja	Ja	Ja	Ja	Nein	Nein	Ja
AWS::EC2::Instance	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja

Ressourcentyp	Asien-Pazifik (Hongkong)	Asien-Pazifik (Hyderabad)	Asien-Pazifik (Jakarta)	Asien-Pazifik (Malaysia)	Asien-Pazifik (Melbourne)	Asien-Pazifik (Mumbai)	Asien-Pazifik (Osaka)	Asien-Pazifik (Seoul)	Asien-Pazifik (Singapur)	Asien-Pazifik (Sydney)	Asien-Pazifik (Taipeh)	Asien-Pazifik (Thailand)	Asien-Pazifik (Tokio)
AWS::EC2::Instance ConnectEndpunkt	Ja	Ja	Ja	Nein	Ja	Ja	Ja	Ja	Ja	Ja	Nein	Nein	Ja
AWS::EC2::InternetGateway	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja
AWS::EC2::LaunchTemplate	Ja	Nein	Ja	Nein	Nein	Ja	Ja	Ja	Ja	Ja	Nein	Nein	Ja
AWS::EC2::NatGateway	Ja	Nein	Ja	Nein	Nein	Ja	Ja	Ja	Ja	Ja	Nein	Nein	Ja
AWS::EC2::NetworkAcl	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja
AWS::EC2::NetworkInsightsAccessScope	Ja	Nein	Nein	Nein	Nein	Ja	Ja	Ja	Ja	Ja	Nein	Nein	Ja
AWS::EC2::NetworkInsightsAccessScopeAnalysis	Ja	Nein	Nein	Nein	Nein	Ja	Ja	Ja	Ja	Ja	Nein	Nein	Ja
AWS::EC2::NetworkInsightsAnalyse	Ja	Nein	Nein	Nein	Nein	Ja	Nein	Ja	Ja	Ja	Nein	Nein	Ja

Ressourcentyp	Asien-Pazifik (Hongkong)	Asien-Pazifik (Hyderabad)	Asien-Pazifik (Jakarta)	Asien-Pazifik (Malaysia)	Asien-Pazifik (Melbourne)	Asien-Pazifik (Mumbai)	Asien-Pazifik (Osaka)	Asien-Pazifik (Seoul)	Asien-Pazifik (Singapur)	Asien-Pazifik (Sydney)	Asien-Pazifik (Taipeh)	Asien-Pazifik (Thailand)	Asien-Pazifik (Tokio)
AWS::EC2::NetworkInsightsPfad	Ja	Nein	Nein	Nein	Nein	Ja	Ja	Ja	Ja	Ja	Nein	Nein	Ja
AWS::EC2::NetworkInterface	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja
AWS::EC2::PrefixList	Ja	Ja	Ja	Nein	Ja	Ja	Ja	Ja	Ja	Ja	Nein	Nein	Ja
AWS::EC2::RegisteredHAInstance	Nein	Nein	Nein	Nein	Nein	Ja	Nein	Ja	Ja	Ja	Nein	Nein	Ja
AWS::EC2::RouteTable	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja
AWS::EC2::SecurityGroup	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja
AWS::EC2::SnapshotBlockPublicAccess	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Nein	Nein	Ja
AWS::EC2::SpotFleet	Ja	Ja	Ja	Nein	Ja	Ja	Ja	Ja	Ja	Ja	Nein	Nein	Ja
AWS::EC2::Subnet	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja

Ressourcentyp	Asien-Pazifik (Hongkong)	Asien-Pazifik (Hyderabad)	Asien-Pazifik (Jakarta)	Asien-Pazifik (Malaysia)	Asien-Pazifik (Melbourne)	Asien-Pazifik (Mumbai)	Asien-Pazifik (Osaka)	Asien-Pazifik (Seoul)	Asien-Pazifik (Singapur)	Asien-Pazifik (Sydney)	Asien-Pazifik (Taipeh)	Asien-Pazifik (Thailand)	Asien-Pazifik (Tokio)
AWS::EC2::SubnetRouteTableAssociation	Ja	Ja	Ja	Nein	Ja	Ja	Ja	Ja	Ja	Ja	Nein	Nein	Ja
AWS::EC2::TrafficMirrorFilter	Ja	Ja	Ja	Nein	Ja	Ja	Ja	Ja	Ja	Ja	Nein	Nein	Ja
AWS::EC2::TrafficMirrorSitzung	Ja	Nein	Nein	Nein	Ja	Ja	Ja	Ja	Ja	Ja	Nein	Nein	Ja
AWS::EC2::TrafficMirrorZiel	Ja	Nein	Nein	Nein	Ja	Ja	Ja	Ja	Ja	Ja	Nein	Nein	Ja
AWS::EC2::TransitGateway	Ja	Ja	Ja	Nein	Ja	Ja	Ja	Ja	Ja	Ja	Nein	Nein	Ja
AWS::EC2::TransitGatewayAnlage	Ja	Ja	Ja	Nein	Ja	Ja	Ja	Ja	Ja	Ja	Nein	Nein	Ja
AWS::EC2::TransitGatewayConnect	Ja	Nein	Ja	Nein	Ja	Ja	Ja	Ja	Ja	Ja	Nein	Nein	Ja
AWS::EC2::TransitGatewayMulticastDomain	Ja	Ja	Ja	Nein	Ja	Ja	Ja	Ja	Ja	Ja	Nein	Nein	Ja

Ressourcentyp	Asien-Pazifik (Hongkong)	Asien-Pazifik (Hyderabad)	Asien-Pazifik (Jakarta)	Asien-Pazifik (Malaysia)	Asien-Pazifik (Melbourne)	Asien-Pazifik (Mumbai)	Asien-Pazifik (Osaka)	Asien-Pazifik (Seoul)	Asien-Pazifik (Singapur)	Asien-Pazifik (Sydney)	Asien-Pazifik (Taipeh)	Asien-Pazifik (Thailand)	Asien-Pazifik (Tokio)
AWS::EC2::TransitGatewayRouteTable	Ja	Nein	Ja	Nein	Nein	Ja	Ja	Ja	Ja	Ja	Nein	Nein	Ja
AWS:EC2: :VPC	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja
AWS:EC2::VPCBlockPublicAccessExclusion	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Nein	Nein	Ja
AWS:EC2::VPCBlockPublicAccessOptions	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Nein	Nein	Ja
AWS:EC2::VPCEndpoint	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja
AWS:EC2::VPCEndpoint ConnectionNotification	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Nein	Ja	Ja
AWS:EC2::VPCEndpoint Dienst	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja

Ressourcentyp	Asien-Pazifik (Hongkong)	Asien-Pazifik (Hyderabad)	Asien-Pazifik (Jakarta)	Asien-Pazifik (Malaysia)	Asien-Pazifik (Melbourne)	Asien-Pazifik (Mumbai)	Asien-Pazifik (Osaka)	Asien-Pazifik (Seoul)	Asien-Pazifik (Singapur)	Asien-Pazifik (Sydney)	Asien-Pazifik (Taipeh)	Asien-Pazifik (Thailand)	Asien-Pazifik (Tokio)
AWS:EC2::VPCPeeringVerbindung	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja
AWS:EC2::VPNConnection	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja
AWS::EC2::VPNConnection Route	Ja	Ja	Ja	Nein	Ja	Ja	Ja	Ja	Ja	Ja	Nein	Nein	Ja
AWS:EC2::VPNGateway	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja
AWS::EC2::Volume	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja
AWS::ECR::PullThroughCacheRule	Ja	Ja	Ja	Nein	Ja	Ja	Ja	Ja	Ja	Ja	Nein	Nein	Ja
AWS::ECR::RegistryPolicy	Ja	Ja	Ja	Nein	Ja	Ja	Ja	Ja	Ja	Ja	Nein	Nein	Ja
AWS::ECR::Repository	Ja	Ja	Ja	Nein	Ja	Ja	Ja	Ja	Ja	Ja	Nein	Nein	Ja
AWS::ECS::CapacityProvider	Ja	Ja	Ja	Nein	Ja	Ja	Ja	Ja	Ja	Ja	Nein	Nein	Ja
AWS::ECS::Cluster	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja

Ressourcentyp	Asien-Pazifik (Hongkong)	Asien-Pazifik (Hyderabad)	Asien-Pazifik (Jakarta)	Asien-Pazifik (Malaysia)	Asien-Pazifik (Melbourne)	Asien-Pazifik (Mumbai)	Asien-Pazifik (Osaka)	Asien-Pazifik (Seoul)	Asien-Pazifik (Singapur)	Asien-Pazifik (Sydney)	Asien-Pazifik (Taipeh)	Asien-Pazifik (Thailand)	Asien-Pazifik (Tokio)
AWS::ECS::Service	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja
AWS::ECS::TaskDefinition	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja
AWS::ECS::TaskSet	Ja	Ja	Ja	Nein	Ja	Ja	Ja	Ja	Ja	Ja	Nein	Nein	Ja
AWS::EFS::AccessPoint	Ja	Ja	Ja	Nein	Ja	Ja	Ja	Ja	Ja	Ja	Nein	Nein	Ja
AWS::EFS::FileSystem	Ja	Ja	Ja	Nein	Ja	Ja	Ja	Ja	Ja	Ja	Nein	Nein	Ja
AWS::EKS::Addon	Ja	Ja	Ja	Nein	Ja	Ja	Ja	Ja	Ja	Ja	Nein	Nein	Ja
AWS::EKS::Cluster	Ja	Ja	Ja	Nein	Ja	Ja	Ja	Ja	Ja	Ja	Nein	Nein	Ja
AWS::EKS::FargateProfile	Ja	Ja	Ja	Nein	Ja	Ja	Ja	Ja	Ja	Ja	Nein	Nein	Ja
AWS::EKS::IdentityProviderConfig	Ja	Ja	Ja	Nein	Ja	Ja	Ja	Ja	Ja	Ja	Nein	Nein	Ja
AWS::EMR::SecurityConfiguration	Ja	Ja	Ja	Nein	Ja	Ja	Ja	Ja	Ja	Ja	Nein	Nein	Ja

Ressourcentyp	Asien-Pazifik (Hongkong)	Asien-Pazifik (Hyderabad)	Asien-Pazifik (Jakarta)	Asien-Pazifik (Malaysia)	Asien-Pazifik (Melbourne)	Asien-Pazifik (Mumbai)	Asien-Pazifik (Osaka)	Asien-Pazifik (Seoul)	Asien-Pazifik (Singapur)	Asien-Pazifik (Sydney)	Asien-Pazifik (Taipeh)	Asien-Pazifik (Thailand)	Asien-Pazifik (Tokio)
AWS::ElasticBeanstalk::Application	Ja	Nein	Ja	Nein	Nein	Ja	Ja	Ja	Ja	Ja	Nein	Nein	Ja
AWS::ElasticBeanstalk::ApplicationVersion	Ja	Nein	Ja	Nein	Nein	Ja	Ja	Ja	Ja	Ja	Nein	Nein	Ja
AWS::ElasticBeanstalk::Environment	Ja	Nein	Ja	Nein	Nein	Ja	Ja	Ja	Ja	Ja	Nein	Nein	Ja
AWS::ElasticLoadBalancing::LoadBalancer	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja
AWS::ElasticLoadBalancingV2::Listener	Ja	Nein	Nein	Nein	Nein	Ja	Ja	Ja	Ja	Ja	Nein	Nein	Ja
AWS::ElasticLoadBalancingV2::LoadBalancer	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja
AWS::Elasticsearch::Domain	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja
AWS::EventSchemas::Discoverer	Ja	Nein	Ja	Nein	Nein	Ja	Ja	Ja	Ja	Ja	Nein	Nein	Ja

Ressourcentyp	Asien-Pazifik (Hongkong)	Asien-Pazifik (Hyderabad)	Asien-Pazifik (Jakarta)	Asien-Pazifik (Malaysia)	Asien-Pazifik (Melbourne)	Asien-Pazifik (Mumbai)	Asien-Pazifik (Osaka)	Asien-Pazifik (Seoul)	Asien-Pazifik (Singapur)	Asien-Pazifik (Sydney)	Asien-Pazifik (Taipeh)	Asien-Pazifik (Thailand)	Asien-Pazifik (Tokio)
AWS::EventSchemas::Registry	Ja	Nein	Ja	Nein	Nein	Ja	Ja	Ja	Ja	Ja	Nein	Nein	Ja
AWS::EventSchemas::RegistryPolicy	Ja	Nein	Ja	Nein	Nein	Ja	Ja	Ja	Ja	Ja	Nein	Nein	Ja
AWS::EventSchemas::Schema	Ja	Nein	Ja	Nein	Nein	Ja	Ja	Ja	Ja	Ja	Nein	Nein	Ja
AWS::Events::ApiDestination	Ja	Ja	Ja	Nein	Nein	Ja	Ja	Ja	Ja	Ja	Nein	Nein	Ja
AWS::Events::Archive	Ja	Ja	Ja	Nein	Nein	Ja	Ja	Ja	Ja	Ja	Nein	Nein	Ja
AWS::Events::Connection	Ja	Ja	Ja	Nein	Nein	Ja	Ja	Ja	Ja	Ja	Nein	Nein	Ja
AWS::Events::Endpoint	Nein	Nein	Nein	Nein	Nein	Ja	Ja	Ja	Ja	Ja	Nein	Nein	Ja
AWS::Events::EventBus	Ja	Ja	Ja	Nein	Ja	Ja	Ja	Ja	Ja	Ja	Nein	Nein	Ja
AWS::Events::Rule	Ja	Ja	Nein	Nein	Ja	Ja	Ja	Ja	Ja	Ja	Nein	Nein	Ja
AWS::Evidently::Launch	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Ja	Ja	Nein	Nein	Ja

Ressourcentyp	Asien-Pazifik (Hongkong)	Asien-Pazifik (Hyderabad)	Asien-Pazifik (Jakarta)	Asien-Pazifik (Malaysia)	Asien-Pazifik (Melbourne)	Asien-Pazifik (Mumbai)	Asien-Pazifik (Osaka)	Asien-Pazifik (Seoul)	Asien-Pazifik (Singapur)	Asien-Pazifik (Sydney)	Asien-Pazifik (Taipeh)	Asien-Pazifik (Thailand)	Asien-Pazifik (Tokio)
AWS::Evidently::Project	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Ja	Ja	Nein	Nein	Ja
AWS::Evidently::Segment	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Ja	Ja	Nein	Nein	Ja
AWS::FIS::ExperimentTemplate	Ja	Nein	Nein	Nein	Nein	Ja	Nein	Ja	Ja	Ja	Nein	Nein	Ja
AWS::Forecast::Dataset	Nein	Nein	Nein	Nein	Nein	Ja	Nein	Ja	Ja	Ja	Nein	Nein	Ja
AWS::Forecast::DatasetGroup	Nein	Nein	Nein	Nein	Nein	Ja	Nein	Ja	Ja	Ja	Nein	Nein	Ja
AWS::FraudDetector::EntityType	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Ja	Ja	Nein	Nein	Nein
AWS::FraudDetector::Label	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Ja	Ja	Nein	Nein	Nein
AWS::FraudDetector::Outcome	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Ja	Ja	Nein	Nein	Nein
AWS::FraudDetector::Variable	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Ja	Ja	Nein	Nein	Nein

Ressourcentyp	Asien-Pazifik (Hongkong)	Asien-Pazifik (Hyderabad)	Asien-Pazifik (Jakarta)	Asien-Pazifik (Malaysia)	Asien-Pazifik (Melbourne)	Asien-Pazifik (Mumbai)	Asien-Pazifik (Osaka)	Asien-Pazifik (Seoul)	Asien-Pazifik (Singapur)	Asien-Pazifik (Sydney)	Asien-Pazifik (Taipeh)	Asien-Pazifik (Thailand)	Asien-Pazifik (Tokio)
AWS::Glue::Classifier	Ja	Ja	Ja	Nein	Ja	Ja	Ja	Ja	Ja	Ja	Nein	Nein	Ja
AWS::Glue::Job	Ja	Ja	Ja	Nein	Ja	Ja	Ja	Ja	Ja	Ja	Nein	Nein	Ja
AWS::Glue::MLTransform	Ja	Ja	Ja	Nein	Ja	Ja	Ja	Ja	Ja	Ja	Nein	Nein	Ja
AWS::Grafana::Workspace	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Ja	Ja	Ja	Nein	Nein	Ja
AWS::GreengrassV2::ComponentVersion	Nein	Nein	Nein	Nein	Nein	Ja	Nein	Ja	Ja	Ja	Nein	Nein	Ja
AWS::GroundStation::Config	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Ja	Ja	Ja	Nein	Nein	Nein
AWS::GroundStation::DataflowEndpointGruppe	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Ja	Ja	Ja	Nein	Nein	Nein
AWS::GroundStation::MissionProfile	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Ja	Ja	Ja	Nein	Nein	Nein
AWS::GuardDuty::Detector	Ja	Ja	Ja	Nein	Ja	Ja	Ja	Ja	Ja	Ja	Nein	Nein	Ja
AWS::GuardDuty::Filter	Ja	Nein	Nein	Nein	Nein	Ja	Ja	Ja	Ja	Ja	Nein	Nein	Ja

Ressourcentyp	Asien-Pazifik (Hongkong)	Asien-Pazifik (Hyderabad)	Asien-Pazifik (Jakarta)	Asien-Pazifik (Malaysia)	Asien-Pazifik (Melbourne)	Asien-Pazifik (Mumbai)	Asien-Pazifik (Osaka)	Asien-Pazifik (Seoul)	Asien-Pazifik (Singapur)	Asien-Pazifik (Sydney)	Asien-Pazifik (Taipeh)	Asien-Pazifik (Thailand)	Asien-Pazifik (Tokio)
AWS::GuardPflicht: IPSet	Ja	Ja	Ja	Nein	Ja	Ja	Ja	Ja	Ja	Ja	Nein	Nein	Ja
AWS::GuardDuty::ThreatIntelSatz	Ja	Ja	Ja	Nein	Ja	Ja	Ja	Ja	Ja	Ja	Nein	Nein	Ja
AWS::HealthSee::FHIRDatastore	Nein	Nein	Nein	Nein	Nein	Ja	Nein	Nein	Nein	Nein	Nein	Nein	Nein
AWS::IAM::Group	Ja	Nein	Ja	Nein	Nein	Ja	Ja	Ja	Ja	Ja	Nein	Nein	Ja
AWS::IAM::Policy	Ja	Nein	Ja	Nein	Nein	Ja	Ja	Ja	Ja	Ja	Nein	Nein	Ja
AWS::IAM::Role	Ja	Nein	Ja	Nein	Nein	Ja	Ja	Ja	Ja	Ja	Nein	Nein	Ja
AWS::IAM::User	Ja	Nein	Ja	Nein	Nein	Ja	Ja	Ja	Ja	Ja	Nein	Nein	Ja
AWS::IVS::Channel	Nein	Nein	Nein	Nein	Nein	Ja	Nein	Ja	Nein	Nein	Nein	Nein	Ja
AWS::IVS::PlaybackKeyPaar	Nein	Nein	Nein	Nein	Nein	Ja	Nein	Ja	Nein	Nein	Nein	Nein	Ja
AWS::IVS::RecordingConfiguration	Nein	Nein	Nein	Nein	Nein	Ja	Nein	Ja	Nein	Nein	Nein	Nein	Ja

Ressourcentyp	Asien-Pazifik (Hongkong)	Asien-Pazifik (Hyderabad)	Asien-Pazifik (Jakarta)	Asien-Pazifik (Malaysia)	Asien-Pazifik (Melbourne)	Asien-Pazifik (Mumbai)	Asien-Pazifik (Osaka)	Asien-Pazifik (Seoul)	Asien-Pazifik (Singapur)	Asien-Pazifik (Sydney)	Asien-Pazifik (Taipeh)	Asien-Pazifik (Thailand)	Asien-Pazifik (Tokio)
AWS::ImageBuilder::ContainerRecipe	Ja	Ja	Ja	Nein	Ja	Ja	Ja	Ja	Ja	Ja	Nein	Nein	Ja
AWS::ImageBuilder::DistributionConfiguration	Ja	Ja	Ja	Nein	Ja	Ja	Ja	Ja	Ja	Ja	Nein	Nein	Ja
AWS::ImageBuilder::ImagePipeline	Ja	Ja	Ja	Nein	Ja	Ja	Ja	Ja	Ja	Ja	Nein	Nein	Ja
AWS::ImageBuilder::ImageRecipe	Ja	Ja	Ja	Nein	Ja	Ja	Ja	Ja	Ja	Ja	Nein	Nein	Ja
AWS::ImageBuilder::InfrastructureConfiguration	Ja	Ja	Ja	Nein	Ja	Ja	Ja	Ja	Ja	Ja	Nein	Nein	Ja
AWS::InspectorV2::Activation	Ja	Nein	Ja	Nein	Nein	Ja	Ja	Ja	Ja	Ja	Nein	Nein	Ja
AWS::InspectorV2::Filter	Ja	Nein	Ja	Nein	Nein	Ja	Ja	Ja	Ja	Ja	Nein	Nein	Ja
AWS::IoT::AccountAuditKonfiguration	Ja	Nein	Nein	Nein	Nein	Ja	Nein	Ja	Ja	Ja	Nein	Nein	Ja

Ressourcentyp	Asien-Pazifik (Hongkong)	Asien-Pazifik (Hyderabad)	Asien-Pazifik (Jakarta)	Asien-Pazifik (Malaysia)	Asien-Pazifik (Melbourne)	Asien-Pazifik (Mumbai)	Asien-Pazifik (Osaka)	Asien-Pazifik (Seoul)	Asien-Pazifik (Singapur)	Asien-Pazifik (Sydney)	Asien-Pazifik (Taipeh)	Asien-Pazifik (Thailand)	Asien-Pazifik (Tokio)
AWS::IoT::Authorizer	Ja	Nein	Nein	Nein	Nein	Ja	Nein	Ja	Ja	Ja	Nein	Nein	Ja
AWS::IoT::CACertificate	Ja	Nein	Nein	Nein	Nein	Ja	Nein	Ja	Ja	Ja	Nein	Nein	Ja
AWS::IoT::CustomMetric	Ja	Nein	Nein	Nein	Nein	Ja	Nein	Ja	Ja	Ja	Nein	Nein	Ja
AWS::IoT::Dimension	Ja	Nein	Nein	Nein	Nein	Ja	Nein	Ja	Ja	Ja	Nein	Nein	Ja
AWS::IoT::FleetMetric	Ja	Nein	Nein	Nein	Nein	Ja	Nein	Ja	Ja	Ja	Nein	Nein	Ja
AWS::IoT::JobTemplate	Ja	Nein	Nein	Nein	Nein	Ja	Nein	Ja	Ja	Ja	Nein	Nein	Ja
AWS::IoT::MitigationAction	Ja	Nein	Nein	Nein	Nein	Ja	Nein	Ja	Ja	Ja	Nein	Nein	Ja
AWS::IoT::Policy	Ja	Nein	Nein	Nein	Nein	Ja	Nein	Ja	Ja	Ja	Nein	Nein	Ja
AWS::IoT::ProvisioningTemplate	Ja	Nein	Nein	Nein	Nein	Ja	Nein	Ja	Ja	Ja	Nein	Nein	Ja
AWS::IoT::RoleAlias	Ja	Nein	Nein	Nein	Nein	Ja	Nein	Ja	Ja	Ja	Nein	Nein	Ja
AWS::IoT::ScheduledAudit	Ja	Nein	Nein	Nein	Nein	Ja	Nein	Ja	Ja	Ja	Nein	Nein	Ja

Ressourcentyp	Asien-Pazifik (Hongkong)	Asien-Pazifik (Hyderabad)	Asien-Pazifik (Jakarta)	Asien-Pazifik (Malaysia)	Asien-Pazifik (Melbourne)	Asien-Pazifik (Mumbai)	Asien-Pazifik (Osaka)	Asien-Pazifik (Seoul)	Asien-Pazifik (Singapur)	Asien-Pazifik (Sydney)	Asien-Pazifik (Taipeh)	Asien-Pazifik (Thailand)	Asien-Pazifik (Tokio)
AWS::IoT::SecurityProfile	Ja	Nein	Nein	Nein	Nein	Ja	Nein	Ja	Ja	Ja	Nein	Nein	Ja
AWS::IoTAnalytics::Channel	Nein	Nein	Nein	Nein	Nein	Ja	Nein	Nein	Nein	Ja	Nein	Nein	Ja
AWS::IoTAnalytics::Dataset	Nein	Nein	Nein	Nein	Nein	Ja	Nein	Nein	Nein	Ja	Nein	Nein	Ja
AWS::IoTAnalytics::Datastore	Nein	Nein	Nein	Nein	Nein	Ja	Nein	Nein	Nein	Ja	Nein	Nein	Ja
AWS::IoTAnalytics::Pipeline	Nein	Nein	Nein	Nein	Nein	Ja	Nein	Nein	Nein	Ja	Nein	Nein	Ja
AWS::IoTEvents::AlarmModel	Nein	Nein	Nein	Nein	Nein	Ja	Nein	Ja	Ja	Ja	Nein	Nein	Ja
AWS::IoTEvents::DetectorModel	Nein	Nein	Nein	Nein	Nein	Ja	Nein	Ja	Ja	Ja	Nein	Nein	Ja
AWS::IoTEvents::Input	Nein	Nein	Nein	Nein	Nein	Ja	Nein	Ja	Ja	Ja	Nein	Nein	Ja
AWS::IoTSiteWise::AssetModel	Nein	Nein	Nein	Nein	Nein	Ja	Nein	Ja	Ja	Ja	Nein	Nein	Ja
AWS::IoTSiteWise::Dashboard	Nein	Nein	Nein	Nein	Nein	Ja	Nein	Ja	Ja	Ja	Nein	Nein	Ja

Ressourcentyp	Asien-Pazifik (Hongkong)	Asien-Pazifik (Hyderabad)	Asien-Pazifik (Jakarta)	Asien-Pazifik (Malaysia)	Asien-Pazifik (Melbourne)	Asien-Pazifik (Mumbai)	Asien-Pazifik (Osaka)	Asien-Pazifik (Seoul)	Asien-Pazifik (Singapur)	Asien-Pazifik (Sydney)	Asien-Pazifik (Taipeh)	Asien-Pazifik (Thailand)	Asien-Pazifik (Tokio)
AWS::IoTSiteWise::Gateway	Nein	Nein	Nein	Nein	Nein	Ja	Nein	Ja	Ja	Ja	Nein	Nein	Ja
AWS::IoTSiteWise::Portal	Nein	Nein	Nein	Nein	Nein	Ja	Nein	Ja	Ja	Ja	Nein	Nein	Ja
AWS::IoTSiteWise::Project	Nein	Nein	Nein	Nein	Nein	Ja	Nein	Ja	Ja	Ja	Nein	Nein	Ja
AWS::IoTTwinMaker::ComponentType	Nein	Nein	Nein	Nein	Nein	Ja	Nein	Ja	Ja	Ja	Nein	Nein	Ja
AWS::IoTTwinMaker::Entity	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Ja	Ja	Nein	Nein	Nein
AWS::IoTTwinMaker::Scene	Nein	Nein	Nein	Nein	Nein	Ja	Nein	Ja	Ja	Ja	Nein	Nein	Ja
AWS::IoTTwinMaker::SyncJob	Nein	Nein	Nein	Nein	Nein	Ja	Nein	Ja	Ja	Ja	Nein	Nein	Ja
AWS::IoTTwinMaker::Workspace	Nein	Nein	Nein	Nein	Nein	Ja	Nein	Ja	Ja	Ja	Nein	Nein	Ja
AWS::IoTWireless::FuotaTask	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Ja	Nein	Nein	Ja
AWS::IoTWireless::MulticastGroup	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Ja	Nein	Nein	Ja

Ressourcentyp	Asien-Pazifik (Hongkong)	Asien-Pazifik (Hyderabad)	Asien-Pazifik (Jakarta)	Asien-Pazifik (Malaysia)	Asien-Pazifik (Melbourne)	Asien-Pazifik (Mumbai)	Asien-Pazifik (Osaka)	Asien-Pazifik (Seoul)	Asien-Pazifik (Singapur)	Asien-Pazifik (Sydney)	Asien-Pazifik (Taipeh)	Asien-Pazifik (Thailand)	Asien-Pazifik (Tokio)
AWS::IoTWireless::ServiceProfile	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Ja	Nein	Nein	Ja
AWS::KMS::Alias	Ja	Ja	Ja	Nein	Nein	Ja	Ja	Ja	Ja	Ja	Nein	Nein	Ja
AWS::KMS::Key	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja
AWS::KafkaConnect::Connector	Nein	Nein	Nein	Nein	Nein	Ja	Nein	Ja	Ja	Ja	Nein	Nein	Ja
AWS::Kendra::Index	Nein	Nein	Nein	Nein	Nein	Ja	Nein	Nein	Ja	Ja	Nein	Nein	Ja
AWS::Kinesis::Stream	Ja	Ja	Ja	Nein	Ja	Ja	Ja	Ja	Ja	Ja	Nein	Nein	Ja
AWS::Kinesis::StreamConsumer	Ja	Ja	Nein	Nein	Ja	Ja	Ja	Ja	Ja	Ja	Nein	Nein	Ja
AWS::KinesisAnalyticsV2::Application	Ja	Ja	Ja	Nein	Ja	Ja	Ja	Ja	Ja	Ja	Nein	Nein	Ja
AWS::KinesisFirehose::DeliveryStream	Ja	Ja	Ja	Nein	Ja	Ja	Ja	Ja	Ja	Ja	Nein	Nein	Ja

Ressourcentyp	Asien-Pazifik (Hongkong)	Asien-Pazifik (Hyderabad)	Asien-Pazifik (Jakarta)	Asien-Pazifik (Malaysia)	Asien-Pazifik (Melbourne)	Asien-Pazifik (Mumbai)	Asien-Pazifik (Osaka)	Asien-Pazifik (Seoul)	Asien-Pazifik (Singapur)	Asien-Pazifik (Sydney)	Asien-Pazifik (Taipeh)	Asien-Pazifik (Thailand)	Asien-Pazifik (Tokio)
AWS::KinesisVideo::SignalingChannel	Ja	Nein	Nein	Nein	Nein	Ja	Nein	Ja	Ja	Ja	Nein	Nein	Ja
AWS::KinesisVideo::Stream	Ja	Nein	Nein	Nein	Nein	Ja	Nein	Ja	Ja	Ja	Nein	Nein	Ja
AWS::Lambda::CodeSigningConfig	Ja	Nein	Nein	Nein	Nein	Ja	Nein	Ja	Ja	Ja	Nein	Nein	Ja
AWS::Lambda::Function	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja
AWS::Lex::Bot	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Ja	Ja	Ja	Nein	Nein	Ja
AWS::Lex::BotAlias	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Ja	Ja	Ja	Nein	Nein	Ja
AWS::Lightsail::Bucket	Nein	Nein	Nein	Nein	Nein	Ja	Nein	Ja	Ja	Ja	Nein	Nein	Ja
AWS::Lightsail::Certificate	Nein	Nein	Nein	Nein	Nein	Ja	Nein	Ja	Ja	Ja	Nein	Nein	Ja
AWS::Lightsail::Disk	Nein	Nein	Nein	Nein	Nein	Ja	Nein	Ja	Ja	Ja	Nein	Nein	Ja
AWS::Lightsail::StaticIp	Nein	Nein	Nein	Nein	Nein	Ja	Nein	Ja	Ja	Ja	Nein	Nein	Ja

Ressourcentyp	Asien-Pazifik (Hongkong)	Asien-Pazifik (Hyderabad)	Asien-Pazifik (Jakarta)	Asien-Pazifik (Malaysia)	Asien-Pazifik (Melbourne)	Asien-Pazifik (Mumbai)	Asien-Pazifik (Osaka)	Asien-Pazifik (Seoul)	Asien-Pazifik (Singapur)	Asien-Pazifik (Sydney)	Asien-Pazifik (Taipeh)	Asien-Pazifik (Thailand)	Asien-Pazifik (Tokio)
AWS::Logs::Destination	Ja	Ja	Ja	Nein	Ja	Ja	Ja	Ja	Ja	Ja	Nein	Nein	Ja
AWS::LookoutMetrics::Alert	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Ja	Ja	Nein	Nein	Ja
AWS::LookoutVision::Project	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Ja	Nein	Nein	Nein	Nein	Ja
AWS::M2::Environment	Nein	Nein	Nein	Nein	Nein	Ja	Nein	Ja	Ja	Ja	Nein	Nein	Ja
AWS::MSK::BatchScramGeheim	Ja	Ja	Ja	Nein	Ja	Ja	Ja	Ja	Ja	Ja	Nein	Nein	Ja
AWS::MSK::Cluster	Ja	Ja	Ja	Nein	Ja	Ja	Ja	Ja	Ja	Ja	Nein	Nein	Ja
AWS::MSK::ClusterPolicy	Ja	Ja	Ja	Nein	Ja	Ja	Ja	Ja	Ja	Ja	Nein	Nein	Ja
AWS::MSK::Configuration	Ja	Ja	Ja	Nein	Ja	Ja	Ja	Ja	Ja	Ja	Nein	Nein	Ja
AWS::MSK::VpcConnection	Ja	Ja	Ja	Nein	Ja	Ja	Ja	Ja	Ja	Ja	Nein	Nein	Ja
AWS::Macie::Session	Ja	Nein	Nein	Nein	Nein	Ja	Ja	Ja	Ja	Ja	Nein	Nein	Ja

Ressourcentyp	Asien-Pazifik (Hongkong)	Asien-Pazifik (Hyderabad)	Asien-Pazifik (Jakarta)	Asien-Pazifik (Malaysia)	Asien-Pazifik (Melbourne)	Asien-Pazifik (Mumbai)	Asien-Pazifik (Osaka)	Asien-Pazifik (Seoul)	Asien-Pazifik (Singapur)	Asien-Pazifik (Sydney)	Asien-Pazifik (Taipeh)	Asien-Pazifik (Thailand)	Asien-Pazifik (Tokio)
AWS::MediaConnect::FlowEntitlement	Ja	Ja	Nein	Nein	Ja	Ja	Ja	Ja	Ja	Ja	Nein	Nein	Ja
AWS::MediaConnect::FlowSource	Ja	Ja	Nein	Nein	Ja	Ja	Ja	Ja	Ja	Ja	Nein	Nein	Ja
AWS::MediaConnect::FlowVpcSchnittstelle	Ja	Nein	Nein	Nein	Nein	Ja	Ja	Ja	Ja	Ja	Nein	Nein	Ja
AWS::MediaConnect::Gateway	Ja	Nein	Nein	Nein	Nein	Ja	Ja	Ja	Ja	Ja	Nein	Nein	Ja
AWS::MediaPackage::PackagingConfiguration	Nein	Nein	Nein	Nein	Ja	Ja	Ja	Ja	Ja	Ja	Nein	Nein	Ja
AWS::MediaPackage::PackagingGroup	Nein	Nein	Nein	Nein	Ja	Ja	Ja	Ja	Ja	Ja	Nein	Nein	Ja
AWS::MediaTailor::PlaybackConfiguration	Nein	Nein	Nein	Nein	Ja	Ja	Ja	Ja	Ja	Ja	Nein	Nein	Ja

Ressourcentyp	Asien-Pazifik (Hongkong)	Asien-Pazifik (Hyderabad)	Asien-Pazifik (Jakarta)	Asien-Pazifik (Malaysia)	Asien-Pazifik (Melbourne)	Asien-Pazifik (Mumbai)	Asien-Pazifik (Osaka)	Asien-Pazifik (Seoul)	Asien-Pazifik (Singapur)	Asien-Pazifik (Sydney)	Asien-Pazifik (Taipeh)	Asien-Pazifik (Thailand)	Asien-Pazifik (Tokio)
AWS::MemoryDB::SubnetGroup	Ja	Nein	Nein	Nein	Nein	Ja	Nein	Ja	Ja	Ja	Nein	Nein	Ja
AWS::NetworkFirewall::Firewall	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Nein	Ja	Ja
AWS::NetworkFirewall::FirewallPolicy	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Nein	Ja	Ja
AWS::NetworkFirewall::RuleGroup	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Nein	Ja	Ja
AWS::NetworkFirewall::TLSInspectionKonfiguration	Ja	Ja	Nein	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Nein	Ja	Ja
AWS::NetworkFirewall::VpcEndpointAssoziation	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Nein	Ja	Ja
AWS::OpenSearch::Domain	Ja	Nein	Ja	Nein	Nein	Ja	Ja	Ja	Ja	Ja	Nein	Nein	Ja
AWS::OpenSearchServerless::Collection	Nein	Nein	Nein	Nein	Nein	Ja	Nein	Nein	Ja	Ja	Nein	Nein	Ja

Ressourcentyp	Asien-Pazifik (Hongkong)	Asien-Pazifik (Hyderabad)	Asien-Pazifik (Jakarta)	Asien-Pazifik (Malaysia)	Asien-Pazifik (Melbourne)	Asien-Pazifik (Mumbai)	Asien-Pazifik (Osaka)	Asien-Pazifik (Seoul)	Asien-Pazifik (Singapur)	Asien-Pazifik (Sydney)	Asien-Pazifik (Taipeh)	Asien-Pazifik (Thailand)	Asien-Pazifik (Tokio)
AWS::OpenSearchServerless::VpcEndpoint	Nein	Nein	Nein	Nein	Nein	Ja	Nein	Nein	Ja	Ja	Nein	Nein	Ja
AWS::Panorama::Package	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Ja	Ja	Nein	Nein	Nein
AWS::Personalize::Dataset	Nein	Nein	Nein	Nein	Nein	Ja	Nein	Ja	Ja	Ja	Nein	Nein	Ja
AWS::Personalize::DatasetGroup	Nein	Nein	Nein	Nein	Nein	Ja	Nein	Ja	Ja	Ja	Nein	Nein	Ja
AWS::Personalize::Schema	Nein	Nein	Nein	Nein	Nein	Ja	Nein	Ja	Ja	Ja	Nein	Nein	Ja
AWS::Personalize::Solution	Nein	Nein	Nein	Nein	Nein	Ja	Nein	Ja	Ja	Ja	Nein	Nein	Ja
AWS::Pinpoint::App	Nein	Nein	Nein	Nein	Nein	Ja	Nein	Ja	Ja	Ja	Nein	Nein	Ja
AWS::Pinpoint::ApplicationSettings	Nein	Nein	Nein	Nein	Nein	Ja	Nein	Ja	Ja	Ja	Nein	Nein	Ja
AWS::Pinpoint::Campaign	Nein	Nein	Nein	Nein	Nein	Ja	Nein	Ja	Ja	Ja	Nein	Nein	Ja

Ressourcentyp	Asien-Pazifik (Hongkong)	Asien-Pazifik (Hyderabad)	Asien-Pazifik (Jakarta)	Asien-Pazifik (Malaysia)	Asien-Pazifik (Melbourne)	Asien-Pazifik (Mumbai)	Asien-Pazifik (Osaka)	Asien-Pazifik (Seoul)	Asien-Pazifik (Singapur)	Asien-Pazifik (Sydney)	Asien-Pazifik (Taipeh)	Asien-Pazifik (Thailand)	Asien-Pazifik (Tokio)
AWS::Pinpoint::EmailChannel	Nein	Nein	Nein	Nein	Nein	Ja	Nein	Ja	Ja	Ja	Nein	Nein	Ja
AWS::Pinpoint::EmailTemplate	Nein	Nein	Nein	Nein	Nein	Ja	Nein	Ja	Ja	Ja	Nein	Nein	Ja
AWS::Pinpoint::EventStream	Nein	Nein	Nein	Nein	Nein	Ja	Nein	Ja	Ja	Ja	Nein	Nein	Ja
AWS::Pinpoint::InAppVorlage	Nein	Nein	Nein	Nein	Nein	Ja	Nein	Ja	Ja	Ja	Nein	Nein	Ja
AWS::Pinpoint::Segment	Nein	Nein	Nein	Nein	Nein	Ja	Nein	Ja	Ja	Ja	Nein	Nein	Ja
AWS::QLDB::Ledger	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Ja	Ja	Ja	Nein	Nein	Ja
AWS::QuickSight::DataSource	Nein	Nein	Nein	Nein	Nein	Ja	Nein	Ja	Ja	Ja	Nein	Nein	Ja
AWS::QuickSight::Template	Nein	Nein	Nein	Nein	Nein	Ja	Nein	Ja	Ja	Ja	Nein	Nein	Ja
AWS::QuickSight::Theme	Nein	Nein	Nein	Nein	Nein	Ja	Nein	Ja	Ja	Ja	Nein	Nein	Ja
AWS: :RDS: DBCluster	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja

Ressourcentyp	Asien-Pazifik (Hongkong)	Asien-Pazifik (Hyderabad)	Asien-Pazifik (Jakarta)	Asien-Pazifik (Malaysia)	Asien-Pazifik (Melbourne)	Asien-Pazifik (Mumbai)	Asien-Pazifik (Osaka)	Asien-Pazifik (Seoul)	Asien-Pazifik (Singapur)	Asien-Pazifik (Sydney)	Asien-Pazifik (Taipeh)	Asien-Pazifik (Thailand)	Asien-Pazifik (Tokio)
AWS: :RDS:: Schnappschuss DBCluster	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja
AWS: :RDS: DBInstance	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja
AWS: :RDS:: Gruppe DBSecurity	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja
AWS: :RDS: DBSnapshot	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja
AWS: :RDS:: Gruppe DBSubnet	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja
AWS::RDS: :EventSubscription	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja
AWS::RDS: :GlobalCluster	Ja	Ja	Ja	Nein	Ja	Ja	Ja	Ja	Ja	Ja	Nein	Nein	Ja
AWS::RDS: :OptionGroup	Ja	Ja	Ja	Nein	Ja	Ja	Ja	Ja	Ja	Ja	Nein	Nein	Ja
AWS::RUM: :AppMonitor	Nein	Ja	Ja	Nein	Ja	Ja	Ja	Ja	Ja	Ja	Nein	Nein	Ja
AWS::Redshift::Cluster	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja

Ressourcentyp	Asien-Pazifik (Hongkong)	Asien-Pazifik (Hyderabad)	Asien-Pazifik (Jakarta)	Asien-Pazifik (Malaysia)	Asien-Pazifik (Melbourne)	Asien-Pazifik (Mumbai)	Asien-Pazifik (Osaka)	Asien-Pazifik (Seoul)	Asien-Pazifik (Singapur)	Asien-Pazifik (Sydney)	Asien-Pazifik (Taipeh)	Asien-Pazifik (Thailand)	Asien-Pazifik (Tokio)
AWS::Redshift::ClusterParameterGruppe	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja
AWS::Redshift::ClusterSecurityGruppe	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja
AWS::Redshift::ClusterSnapshot	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja
AWS::Redshift::ClusterSubnetGruppe	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja
AWS::Redshift::EndpointAccess	Nein	Nein	Nein	Nein	Nein	Ja	Nein	Ja	Ja	Ja	Nein	Nein	Ja
AWS::Redshift::EndpointAuthorization	Nein	Nein	Nein	Nein	Nein	Ja	Nein	Ja	Ja	Ja	Nein	Nein	Ja
AWS::Redshift::EventSubscription	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja
AWS::Redshift::ScheduledAction	Ja	Nein	Nein	Nein	Nein	Ja	Nein	Ja	Ja	Ja	Nein	Nein	Ja

Ressourcentyp	Asien-Pazifik (Hongkong)	Asien-Pazifik (Hyderabad)	Asien-Pazifik (Jakarta)	Asien-Pazifik (Malaysia)	Asien-Pazifik (Melbourne)	Asien-Pazifik (Mumbai)	Asien-Pazifik (Osaka)	Asien-Pazifik (Seoul)	Asien-Pazifik (Singapur)	Asien-Pazifik (Sydney)	Asien-Pazifik (Taipeh)	Asien-Pazifik (Thailand)	Asien-Pazifik (Tokio)
AWS::ResilienceHub::App	Ja	Nein	Nein	Nein	Nein	Ja	Nein	Ja	Ja	Ja	Nein	Nein	Ja
AWS::ResilienceHub::ResiliencyPolicy	Ja	Nein	Nein	Nein	Nein	Ja	Nein	Ja	Ja	Ja	Nein	Nein	Ja
AWS::ResourceExplorer2::Index	Ja	Ja	Ja	Nein	Ja	Ja	Ja	Ja	Ja	Ja	Nein	Nein	Ja
AWS::RoboMaker::RobotApplication	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Ja	Nein	Nein	Nein	Ja
AWS::RoboMaker::RobotApplicationVersion	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Ja	Nein	Nein	Nein	Ja
AWS::RoboMaker::SimulationApplication	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Ja	Nein	Nein	Nein	Ja
AWS::Route53Profiles::Profile	Ja	Ja	Ja	Nein	Ja	Ja	Ja	Ja	Ja	Ja	Nein	Nein	Ja

Ressourcentyp	Asien-Pazifik (Hongkong)	Asien-Pazifik (Hyderabad)	Asien-Pazifik (Jakarta)	Asien-Pazifik (Malaysia)	Asien-Pazifik (Melbourne)	Asien-Pazifik (Mumbai)	Asien-Pazifik (Osaka)	Asien-Pazifik (Seoul)	Asien-Pazifik (Singapur)	Asien-Pazifik (Sydney)	Asien-Pazifik (Taipeh)	Asien-Pazifik (Thailand)	Asien-Pazifik (Tokio)
AWS::Route53Resolver::FirewallDomainListe	Ja	Nein	Ja	Nein	Nein	Ja	Ja	Ja	Ja	Ja	Nein	Nein	Ja
AWS::Route53Resolver::FirewallRuleGruppe	Ja	Nein	Ja	Nein	Nein	Ja	Ja	Ja	Ja	Ja	Nein	Nein	Ja
AWS::Route53Resolver::FirewallRuleGroupAssociation	Ja	Nein	Ja	Nein	Nein	Ja	Ja	Ja	Ja	Ja	Nein	Nein	Ja
AWS::Route53Resolver::ResolverEndpoint	Ja	Ja	Nein	Nein	Ja	Ja	Ja	Ja	Ja	Ja	Nein	Nein	Ja
AWS::Route53Resolver::ResolverQueryLoggingConfig	Ja	Nein	Nein	Nein	Nein	Ja	Ja	Ja	Ja	Ja	Nein	Nein	Ja
AWS::Route53Resolver::ResolverQueryLoggingConfigAssociation	Ja	Nein	Nein	Nein	Nein	Ja	Ja	Ja	Ja	Ja	Nein	Nein	Ja

Ressourcentyp	Asien-Pazifik (Hongkong)	Asien-Pazifik (Hyderabad)	Asien-Pazifik (Jakarta)	Asien-Pazifik (Malaysia)	Asien-Pazifik (Melbourne)	Asien-Pazifik (Mumbai)	Asien-Pazifik (Osaka)	Asien-Pazifik (Seoul)	Asien-Pazifik (Singapur)	Asien-Pazifik (Sydney)	Asien-Pazifik (Taipeh)	Asien-Pazifik (Thailand)	Asien-Pazifik (Tokio)
AWS::Route53Resolver::ResolverRule	Ja	Ja	Nein	Nein	Ja	Ja	Ja	Ja	Ja	Ja	Nein	Nein	Ja
AWS::Route53Resolver::ResolverRuleVerband	Ja	Ja	Nein	Nein	Ja	Ja	Ja	Ja	Ja	Ja	Nein	Nein	Ja
AWS::S3::AccessPoint	Ja	Ja	Ja	Nein	Ja	Ja	Ja	Ja	Ja	Ja	Nein	Nein	Ja
AWS::S3::AccountPublicAccessBlock	Ja	Ja	Ja	Nein	Ja	Ja	Ja	Ja	Ja	Ja	Nein	Nein	Ja
AWS::S3::Bucket	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja
AWS::S3::StorageLens	Nein	Nein	Nein	Nein	Nein	Ja	Nein	Ja	Ja	Ja	Nein	Nein	Ja
AWS::S3::StorageLensGruppe	Nein	Nein	Nein	Nein	Nein	Ja	Nein	Ja	Ja	Ja	Nein	Nein	Ja
AWS::S3Express::BucketPolicy	Nein	Nein	Nein	Nein	Nein	Ja	Nein	Nein	Nein	Nein	Nein	Nein	Ja
AWS::S3Express::DirectoryBucket	Nein	Nein	Nein	Nein	Nein	Ja	Nein	Nein	Nein	Nein	Nein	Nein	Ja

Ressourcentyp	Asien-Pazifik (Hongkong)	Asien-Pazifik (Hyderabad)	Asien-Pazifik (Jakarta)	Asien-Pazifik (Malaysia)	Asien-Pazifik (Melbourne)	Asien-Pazifik (Mumbai)	Asien-Pazifik (Osaka)	Asien-Pazifik (Seoul)	Asien-Pazifik (Singapur)	Asien-Pazifik (Sydney)	Asien-Pazifik (Taipeh)	Asien-Pazifik (Thailand)	Asien-Pazifik (Tokio)
AWS::SES::ConfigurationSet	Nein	Nein	Ja	Nein	Nein	Ja	Ja	Ja	Ja	Ja	Nein	Nein	Ja
AWS::SES::ContactList	Nein	Nein	Ja	Nein	Nein	Ja	Ja	Ja	Ja	Ja	Nein	Nein	Ja
AWS::SES::ReceiptFilter	Nein	Nein	Ja	Nein	Nein	Nein	Nein	Nein	Ja	Ja	Nein	Nein	Ja
AWS::SES::ReceiptRuleSatz	Nein	Nein	Ja	Nein	Nein	Nein	Nein	Nein	Ja	Ja	Nein	Nein	Ja
AWS::SES::Template	Nein	Nein	Ja	Nein	Nein	Ja	Ja	Ja	Ja	Ja	Nein	Nein	Ja
AWS::SNS::Topic	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja
AWS::SQS::Queue	Ja	Nein	Nein	Nein	Nein	Ja	Ja	Ja	Ja	Ja	Nein	Nein	Ja
AWS::SSM::AssociationCompliance	Ja	Ja	Ja	Ja	Ja	Ja	Nein	Ja	Ja	Ja	Nein	Ja	Ja
AWS::SSM::Document	Ja	Ja	Ja	Nein	Ja	Ja	Ja	Ja	Ja	Ja	Nein	Nein	Ja
AWS::SSM::FileData	Ja	Ja	Ja	Ja	Ja	Ja	Nein	Ja	Ja	Ja	Nein	Ja	Ja

Ressourcentyp	Asien-Pazifik (Hongkong)	Asien-Pazifik (Hyderabad)	Asien-Pazifik (Jakarta)	Asien-Pazifik (Malaysia)	Asien-Pazifik (Melbourne)	Asien-Pazifik (Mumbai)	Asien-Pazifik (Osaka)	Asien-Pazifik (Seoul)	Asien-Pazifik (Singapur)	Asien-Pazifik (Sydney)	Asien-Pazifik (Taipeh)	Asien-Pazifik (Thailand)	Asien-Pazifik (Tokio)
AWS::SSM::ManagedInstance-Bestand	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Nein	Ja	Ja
AWS::SSM::PatchCompliance	Ja	Ja	Ja	Ja	Ja	Ja	Nein	Ja	Ja	Ja	Nein	Ja	Ja
AWS::SageMaker::AppImageConfig	Ja	Nein	Ja	Nein	Nein	Ja	Ja	Ja	Ja	Ja	Nein	Nein	Ja
AWS::SageMaker::CodeRepository	Ja	Nein	Ja	Nein	Nein	Ja	Ja	Ja	Ja	Ja	Nein	Nein	Ja
AWS::SageMaker::Domain	Ja	Nein	Ja	Nein	Nein	Ja	Ja	Ja	Ja	Ja	Nein	Nein	Ja
AWS::SageMaker::EndpointConfig	Ja	Nein	Ja	Nein	Nein	Ja	Ja	Ja	Ja	Ja	Nein	Nein	Ja
AWS::SageMaker::FeatureGroup	Ja	Nein	Ja	Nein	Nein	Ja	Ja	Ja	Ja	Ja	Nein	Nein	Ja
AWS::SageMaker::Image	Ja	Nein	Ja	Nein	Nein	Ja	Ja	Ja	Ja	Ja	Nein	Nein	Ja
AWS::SageMaker::InferenceExperiment	Ja	Nein	Nein	Nein	Nein	Ja	Ja	Ja	Ja	Ja	Nein	Nein	Ja

Ressourcentyp	Asien-Pazifik (Hongkong)	Asien-Pazifik (Hyderabad)	Asien-Pazifik (Jakarta)	Asien-Pazifik (Malaysia)	Asien-Pazifik (Melbourne)	Asien-Pazifik (Mumbai)	Asien-Pazifik (Osaka)	Asien-Pazifik (Seoul)	Asien-Pazifik (Singapur)	Asien-Pazifik (Sydney)	Asien-Pazifik (Taipeh)	Asien-Pazifik (Thailand)	Asien-Pazifik (Tokio)
AWS::SageMaker::Model	Ja	Nein	Ja	Nein	Nein	Ja	Ja	Ja	Ja	Ja	Nein	Nein	Ja
AWS::SageMaker::NotebookInstance	Ja	Nein	Ja	Nein	Nein	Ja	Ja	Ja	Ja	Ja	Nein	Nein	Ja
AWS::SageMaker::NotebookInstanceLifecycleConfig	Ja	Nein	Nein	Nein	Nein	Ja	Ja	Ja	Ja	Ja	Nein	Nein	Ja
AWS::SageMaker::Workteam	Nein	Nein	Nein	Nein	Nein	Ja	Nein	Ja	Ja	Ja	Nein	Nein	Ja
AWS::SecretsManager::Secret	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja
AWS::SecurityHub::Standard	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Nein	Ja	Ja
AWS::ServiceCatalog::CloudFormationProdukt	Ja	Ja	Nein	Nein	Ja	Ja	Ja	Ja	Ja	Ja	Nein	Nein	Ja

Ressourcentyp	Asien-Pazifik (Hongkong)	Asien-Pazifik (Hyderabad)	Asien-Pazifik (Jakarta)	Asien-Pazifik (Malaysia)	Asien-Pazifik (Melbourne)	Asien-Pazifik (Mumbai)	Asien-Pazifik (Osaka)	Asien-Pazifik (Seoul)	Asien-Pazifik (Singapur)	Asien-Pazifik (Sydney)	Asien-Pazifik (Taipeh)	Asien-Pazifik (Thailand)	Asien-Pazifik (Tokio)
AWS::ServiceCatalog::CloudFormationProvisionedProduct	Ja	Ja	Nein	Nein	Ja	Ja	Ja	Ja	Ja	Ja	Nein	Nein	Ja
AWS::ServiceCatalog::Portfolio	Ja	Ja	Nein	Nein	Ja	Ja	Ja	Ja	Ja	Ja	Nein	Nein	Ja
AWS::ServiceDiscovery::HttpNamespace	Ja	Ja	Ja	Nein	Ja	Ja	Ja	Ja	Ja	Ja	Nein	Nein	Ja
AWS::ServiceDiscovery::Instance	Ja	Nein	Nein	Nein	Nein	Ja	Ja	Ja	Ja	Ja	Nein	Nein	Ja
AWS::ServiceDiscovery::PublicDnsNamespace	Ja	Ja	Ja	Nein	Ja	Ja	Ja	Ja	Ja	Ja	Nein	Nein	Ja
AWS::ServiceDiscovery::Service	Ja	Nein	Nein	Nein	Nein	Ja	Nein	Ja	Ja	Ja	Nein	Nein	Ja
AWS::ShieldRegional::Protection	Ja	Nein	Ja	Nein	Nein	Ja	Ja	Ja	Ja	Ja	Nein	Nein	Ja
AWS::Signer::SigningProfile	Ja	Nein	Nein	Nein	Nein	Ja	Nein	Ja	Ja	Ja	Nein	Nein	Ja

Ressourcentyp	Asien-Pazifik (Hongkong)	Asien-Pazifik (Hyderabad)	Asien-Pazifik (Jakarta)	Asien-Pazifik (Malaysia)	Asien-Pazifik (Melbourne)	Asien-Pazifik (Mumbai)	Asien-Pazifik (Osaka)	Asien-Pazifik (Seoul)	Asien-Pazifik (Singapur)	Asien-Pazifik (Sydney)	Asien-Pazifik (Taipeh)	Asien-Pazifik (Thailand)	Asien-Pazifik (Tokio)
AWS::Step Functions::Activity	Ja	Ja	Ja	Nein	Ja	Ja	Ja	Ja	Ja	Ja	Nein	Nein	Ja
AWS::Step Functions ::StateMachine	Ja	Ja	Ja	Nein	Ja	Ja	Ja	Ja	Ja	Ja	Nein	Nein	Ja
AWS::Transfer::Agreement	Ja	Nein	Ja	Nein	Nein	Ja	Ja	Ja	Ja	Ja	Nein	Nein	Ja
AWS::Transfer::Certificate	Ja	Ja	Ja	Nein	Ja	Ja	Ja	Ja	Ja	Ja	Nein	Nein	Ja
AWS::Transfer::Connector	Ja	Ja	Ja	Nein	Ja	Ja	Ja	Ja	Ja	Ja	Nein	Nein	Ja
AWS::Transfer::Profile	Ja	Ja	Ja	Nein	Ja	Ja	Ja	Ja	Ja	Ja	Nein	Nein	Ja
AWS::Transfer::Workflow	Ja	Ja	Ja	Nein	Ja	Ja	Ja	Ja	Ja	Ja	Nein	Nein	Ja
AWS::WAFRegional::RateBasedRegel	Ja	Ja	Ja	Nein	Ja	Ja	Ja	Ja	Ja	Ja	Nein	Nein	Ja
AWS::WAFRegional::Rule	Ja	Ja	Ja	Nein	Ja	Ja	Ja	Ja	Ja	Ja	Nein	Nein	Ja
AWS::WAFRegional::RuleGroup	Ja	Ja	Ja	Nein	Ja	Ja	Ja	Ja	Ja	Ja	Nein	Nein	Ja

Ressourcentyp	Asien-Pazifik (Hongkong)	Asien-Pazifik (Hyderabad)	Asien-Pazifik (Jakarta)	Asien-Pazifik (Malaysia)	Asien-Pazifik (Melbourne)	Asien-Pazifik (Mumbai)	Asien-Pazifik (Osaka)	Asien-Pazifik (Seoul)	Asien-Pazifik (Singapur)	Asien-Pazifik (Sydney)	Asien-Pazifik (Taipeh)	Asien-Pazifik (Thailand)	Asien-Pazifik (Tokio)
AWS::WAFRegional::WebACL	Ja	Ja	Ja	Nein	Ja	Ja	Ja	Ja	Ja	Ja	Nein	Nein	Ja
AWSWAFv2::IPSet	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Nein	Ja	Ja
AWS::WAFv2::ManagedRuleSatz	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Nein	Ja	Ja
AWS::WAFv2::RegexPatternSatz	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Nein	Ja	Ja
AWS::WAFv2::RuleGroup	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Nein	Ja	Ja
AWS::WAFv2::WebACL	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Nein	Ja	Ja
AWS::WorkSpaces::ConnectionAlias	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Ja	Ja	Ja	Nein	Nein	Ja
AWS::WorkSpaces::Workspace	Nein	Nein	Nein	Nein	Nein	Ja	Nein	Ja	Ja	Ja	Nein	Nein	Ja
AWS::XRay::EncryptionConfig	Ja	Ja	Ja	Nein	Ja	Ja	Ja	Ja	Ja	Ja	Nein	Nein	Ja

Regionen in China

Ressourcentyp	China (Peking)	China (Ningxia)
AWS::ACM::Certificate	Ja	Ja
AWS::AmazonMQ::Broker	Ja	Ja
AWS::ApiGateway::RestApi	Ja	Ja
AWS::ApiGateway::Stage	Ja	Ja
AWS::ApiGatewayV2::Api	Ja	Ja
AWS::ApiGatewayV2::Stage	Ja	Ja
AWS::AppConfig::Application	Ja	Ja
AWS::AppConfig::ConfigurationProfile	Ja	Ja
AWS::AppConfig::DeploymentStrategy	Ja	Ja
AWS::AppConfig::Environment	Ja	Ja
AWS::AppConfig::ExtensionAssociation	Ja	Ja
AWS::AppConfig::HostedConfigurationVersion	Ja	Ja

Ressourcentyp	China (Peking)	China (Ningxia)
AWS::AppSync::ApiCache	Ja	Ja
AWS::AppSync::GraphQLApi	Ja	Ja
AWS::Athena::DataCatalog	Ja	Ja
AWS::Athena::PreparedStatement	Ja	Ja
AWS::Athena::WorkGroup	Ja	Ja
AWS::AutoScaling::AutoScalingGruppe	Ja	Ja
AWS::AutoScaling::LaunchConfiguration	Ja	Ja
AWS::AutoScaling::ScalingPolicy	Ja	Ja
AWS::AutoScaling::ScheduledAction	Ja	Ja
AWS::AutoScaling::WarmPool	Ja	Ja
AWS::Backup::BackupPlan	Ja	Ja
AWS::Backup::BackupSelection	Ja	Ja
AWS::Backup::BackupVault	Ja	Ja

Ressourcentyp	China (Peking)	China (Ningxia)
AWS::Backup::RecoveryPoint	Ja	Ja
AWS::Batch::ComputeEnvironment	Ja	Ja
AWS::Batch::JobQueue	Ja	Ja
AWS::Batch::SchedulingPolicy	Ja	Ja
AWS::Cassandra::Keyspace	Ja	Ja
AWS::CloudFormation::Stack	Ja	Ja
AWS::CloudTrail::Trail	Ja	Ja
AWS::CloudWatch::Alarm	Ja	Ja
AWS::CloudWatch::MetricStream	Ja	Ja
AWS::CodeBuild::Project	Ja	Ja
AWS::CodeBuild::ReportGroup	Ja	Ja
AWS::Cognito::IdentityPool	Ja	Nein
AWS::Config::ConfigurationRecorder	Ja	Ja

Ressourcentyp	China (Peking)	China (Ningxia)
AWS::Config::ResourceCompliance	Ja	Ja
AWS::DMS::Certificate	Ja	Ja
AWS::DMS::Endpoint	Ja	Ja
AWS::DMS::EventSubscription	Ja	Ja
AWS::DMS::ReplicationInstance	Ja	Ja
AWS::DMS::ReplicationSubnetGruppe	Ja	Ja
AWS::DMS::ReplicationTask	Ja	Ja
AWS::DataSync::LocationEFS	Ja	Ja
AWS::DataSync::LocationHDFS	Ja	Ja
AWS::DataSync::LocationNFS	Ja	Ja
AWS::DataSync::LocationObjectSpeicher	Ja	Ja
AWS::DataSync::LocationS 3	Ja	Ja
AWS::DataSync::LocationSMB	Ja	Ja

Ressourcentyp	China (Peking)	China (Ningxia)
AWS::DataSync::Task	Ja	Ja
AWS::DynamoDB::Table	Ja	Ja
AWS::EC2::CapacityReservation	Ja	Ja
AWSEC2:: DHCPOptions	Ja	Ja
AWS:EC2:: EC2 Flotte	Ja	Ja
AWS::EC2: EIP	Ja	Ja
AWSEC2:: EIPAssociation	Ja	Ja
AWS::EC2::FlowLog	Ja	Ja
AWS::EC2::Host	Ja	Ja
AWS::EC2::Instance	Ja	Ja
AWS::EC2::InternetGateway	Ja	Ja
AWS::EC2::LaunchTemplate	Ja	Ja
AWS::EC2::NatGateway	Ja	Ja

Ressourcentyp	China (Peking)	China (Ningxia)
AWS::EC2::NetworkAcl	Ja	Ja
AWS::EC2::NetworkInterface	Ja	Ja
AWS::EC2::PrefixList	Ja	Ja
AWS::EC2::RouteTable	Ja	Ja
AWS::EC2::SecurityGroup	Ja	Ja
AWS::EC2::SnapshotBlockPublicAccess	Ja	Ja
AWS::EC2::SpotFleet	Ja	Ja
AWS::EC2::Subnet	Ja	Ja
AWS::EC2::SubnetRouteTableAssociation	Ja	Ja
AWS::EC2::TrafficMirrorFiltern	Ja	Ja
AWS::EC2::TrafficMirrorSitzung	Ja	Ja
AWS::EC2::TrafficMirrorZiel	Ja	Ja
AWS::EC2::TransitGateway	Ja	Ja

Ressourcentyp	China (Peking)	China (Ningxia)
AWS::EC2::TransitGatewayAnlage	Ja	Ja
AWS::EC2::TransitGatewayConnect	Ja	Ja
AWS::EC2::TransitGatewayMulticastDomain	Ja	Ja
AWS::EC2::TransitGatewayRouteTable	Ja	Ja
AWS:EC2: :VPC	Ja	Ja
AWS:EC2:: VPCBlock PublicAccessExclusion	Ja	Ja
AWS:EC2:: VPCBlock PublicAccessOptions	Ja	Ja
AWSEC2:: VPCEndpoint	Ja	Ja
AWS:EC2:: VPCEndpoint ConnectionNotification	Ja	Ja
AWS:EC2:: VPCEndpoint Dienst	Ja	Ja
AWS::EC2:: VPCPeering Verbindung	Ja	Ja
AWSEC2:: VPNGateway	Ja	Nein
AWS::EC2::Volume	Ja	Ja

Ressourcentyp	China (Peking)	China (Ningxia)
AWS::ECR::Repository	Ja	Ja
AWS::ECS::CapacityProvider	Ja	Ja
AWS::ECS::Cluster	Ja	Ja
AWS::ECS::Service	Ja	Ja
AWS::ECS::TaskDefinition	Ja	Ja
AWS::ECS::TaskSet	Ja	Ja
AWS::EFS::AccessPoint	Ja	Ja
AWS::EFS::FileSystem	Ja	Ja
AWS::EKS::Addon	Ja	Ja
AWS::EKS::Cluster	Ja	Ja
AWS::EKS::FargateProfile	Ja	Ja
AWS::EKS::IdentityProviderConfig	Ja	Ja
AWS::EMR::SecurityConfiguration	Ja	Ja

Ressourcentyp	China (Peking)	China (Ningxia)
AWS::ElasticBeanstalk::Application	Ja	Ja
AWS::ElasticBeanstalk::ApplicationVersion	Ja	Ja
AWS::ElasticBeanstalk::Environment	Ja	Ja
AWS::ElasticLoadBalancing::LoadBalancer	Ja	Ja
AWS::ElasticLoadBalancingV2::Listener	Ja	Ja
AWS::ElasticLoadBalancingV2::LoadBalancer	Ja	Ja
AWS::Elasticsearch::Domain	Ja	Ja
AWS::Events::Archive	Ja	Ja
AWS::Events::EventBus	Ja	Ja
AWS::Events::Rule	Ja	Ja
AWS::Glue::Classifier	Ja	Ja
AWS::Glue::Job	Ja	Ja
AWS::Glue::MLTransform	Ja	Nein

Ressourcentyp	China (Peking)	China (Ningxia)
AWS::GreengrassV2::ComponentVersion	Ja	Nein
AWS::GuardDuty::Filter	Ja	Ja
AWS::GuardDuty::ThreatIntelEinstellen	Ja	Ja
AWS::IAM::Group	Ja	Ja
AWS::IAM::InstanceProfile	Ja	Nein
AWS: :ICH: OIDCProvider	Ja	Nein
AWS::IAM::Policy	Ja	Ja
AWS::IAM::Role	Ja	Ja
AWS: :ICH: SAMLProvider	Ja	Nein
AWS::IAM::ServerCertificate	Ja	Nein
AWS::IAM::User	Ja	Ja
AWS::ImageBuilder::ContainerRecipe	Ja	Ja
AWS::ImageBuilder::DistributionConfiguration	Ja	Ja

Ressourcentyp	China (Peking)	China (Ningxia)
AWS::ImageBuilder::ImagePipeline	Ja	Ja
AWS::ImageBuilder::ImageRecipe	Ja	Ja
AWS::ImageBuilder::InfrastructureConfiguration	Ja	Ja
AWS::InspectorV2::Activation	Ja	Ja
AWS::IoT::AccountAuditKonfiguration	Ja	Ja
AWS::IoT::Authorizer	Ja	Ja
AWS::IoT: CACertificate	Ja	Ja
AWS::IoT::CustomMetric	Ja	Ja
AWS::IoT::Dimension	Ja	Ja
AWS::IoT::FleetMetric	Ja	Ja
AWS::IoT::JobTemplate	Ja	Ja
AWS::IoT::MitigationAction	Ja	Ja
AWS::IoT::Policy	Ja	Ja

Ressourcentyp	China (Peking)	China (Ningxia)
AWS::IoT::ProvisioningTemplate	Ja	Ja
AWS::IoT::RoleAlias	Ja	Ja
AWS::IoT::ScheduledAudit	Ja	Ja
AWS::IoT::SecurityProfile	Ja	Ja
AWS::IoTAnalytics::Channel	Ja	Nein
AWS::IoTAnalytics::Dataset	Ja	Nein
AWS::IoTAnalytics::Datastore	Ja	Nein
AWS::IoTAnalytics::Pipeline	Ja	Nein
AWS::IoTEvents::AlarmModel	Ja	Nein
AWS::IoTEvents::DetectorModel	Ja	Nein
AWS::IoTEvents::Input	Ja	Nein
AWS::IoTSiteWise::AssetModel	Ja	Nein
AWS::IoTSiteWise::Dashboard	Ja	Nein

Ressourcentyp	China (Peking)	China (Ningxia)
AWS::IoTSiteWise::Gateway	Ja	Nein
AWS::IoTSiteWise::Portal	Ja	Nein
AWS::IoTSiteWise::Project	Ja	Nein
AWS::KMS::Alias	Ja	Ja
AWS::KMS::Key	Ja	Ja
AWS::Kinesis::Stream	Ja	Ja
AWS::Kinesis::StreamConsumer	Ja	Ja
AWS::KinesisAnalyticsV2::Application	Ja	Ja
AWS::KinesisFirehose::DeliveryStream	Ja	Ja
AWS::Lambda::Function	Ja	Nein
AWS::Logs::Destination	Ja	Ja
AWS::MSK::BatchScramGeheim	Ja	Ja
AWS::MSK::Cluster	Ja	Ja

Ressourcentyp	China (Peking)	China (Ningxia)
AWS::MSK::ClusterPolicy	Ja	Ja
AWS::MSK::Configuration	Ja	Ja
AWS::MSK::VpcConnection	Ja	Ja
AWS::NetworkFirewall::Firewall	Ja	Ja
AWS::NetworkFirewall::FirewallPolicy	Ja	Ja
AWS::NetworkFirewall::RuleGroup	Ja	Ja
AWS::NetworkFirewall: TLSInspection Konfiguration	Ja	Ja
AWS::NetworkFirewall::VpcEndpointAssoziation	Ja	Ja
AWS::OpenSearch::Domain	Ja	Ja
AWS::Personalize::Dataset	Ja	Nein
AWS::Personalize::DatasetGroup	Ja	Nein
AWS::Personalize::Schema	Ja	Nein
AWS::Personalize::Solution	Ja	Nein

Ressourcentyp	China (Peking)	China (Ningxia)
AWS: :RDS: DBCluster	Nein	Ja
AWS: :RDS:: Schnappschuss DBCluster	Ja	Ja
AWS: :RDS: DBInstance	Ja	Ja
AWS: :RDS:: Gruppe DBSecurity	Ja	Ja
AWS: :RDS: DBSnapshot	Ja	Ja
AWS: :RDS:: Gruppe DBSubnet	Ja	Ja
AWS::RDS::EventSubscription	Ja	Ja
AWS::RDS::OptionGroup	Ja	Ja
AWS::Redshift::Cluster	Ja	Ja
AWS::Redshift::ClusterParameterGruppe	Ja	Ja
AWS::Redshift::ClusterSecurityGruppe	Ja	Ja
AWS::Redshift::ClusterSnapshot	Ja	Ja
AWS::Redshift::ClusterSubnetGruppe	Ja	Ja

Ressourcentyp	China (Peking)	China (Ningxia)
AWS::Redshift::EventSubscription	Ja	Ja
AWS::Route53Profiles::Profile	Ja	Ja
AWS::Route53Resolver::FirewallDomainListe	Ja	Ja
AWS::Route53Resolver::FirewallRuleGroupAssociation	Ja	Ja
AWS::Route53Resolver::ResolverEndpoint	Ja	Ja
AWS::Route53Resolver::ResolverQueryLoggingConfig	Ja	Ja
AWS::Route53Resolver::Resol verQueryLoggingConfigAssociation	Ja	Ja
AWS::Route53Resolver::ResolverRule	Ja	Ja
AWS::Route53Resolver::ResolverRuleVerband	Ja	Ja
AWS::S3::AccessPoint	Ja	Ja
AWS::S3::AccountPublicAccessBlock	Ja	Ja
AWS::S3::Bucket	Ja	Ja
AWS::S3::StorageLensGruppe	Ja	Ja

Ressourcentyp	China (Peking)	China (Ningxia)
AWS::SES::ConfigurationSet	Nein	Ja
AWS::SES::ContactList	Nein	Ja
AWS::SES::Template	Nein	Ja
AWS::SNS::Topic	Ja	Ja
AWS::SQS::Queue	Ja	Ja
AWS::SSM::AssociationCompliance	Ja	Ja
AWS::SSM::Document	Ja	Ja
AWS::SSM::FileData	Ja	Ja
AWS::SSM::ManagedInstance-Bestand	Ja	Ja
AWS::SSM::PatchCompliance	Ja	Ja
AWS::SageMaker::AppImageConfig	Ja	Ja
AWS::SageMaker::CodeRepository	Ja	Ja
AWS::SageMaker::Domain	Ja	Ja

Ressourcentyp	China (Peking)	China (Ningxia)
AWS::SageMaker::EndpointConfig	Ja	Ja
AWS::SageMaker::FeatureGroup	Ja	Ja
AWS::SageMaker::Image	Ja	Ja
AWS::SageMaker::Model	Ja	Ja
AWS::SageMaker::NotebookInstance	Ja	Ja
AWS::SageMaker::NotebookInstanceLifecycleConfig	Ja	Ja
AWS::SecretsManager::Secret	Ja	Ja
AWS::SecurityHub::Standard	Ja	Ja
AWS::ServiceCatalog::CloudFormationProdukt	Ja	Ja
AWS::ServiceCatalog::CloudFormationProvisionedProduct	Ja	Ja
AWS::ServiceCatalog::Portfolio	Ja	Ja
AWS::ServiceDiscovery::HttpNamespace	Ja	Ja
AWS::ServiceDiscovery::Instance	Ja	Ja

Ressourcentyp	China (Peking)	China (Ningxia)
AWS::ServiceDiscovery::PublicDnsNamespace	Ja	Ja
AWS::ServiceDiscovery::Service	Ja	Ja
AWS::StepFunctions::Activity	Ja	Nein
AWS::StepFunctions::StateMachine	Ja	Ja
AWS::Transfer::Agreement	Ja	Ja
AWS::Transfer::Certificate	Ja	Ja
AWS::Transfer::Connector	Ja	Ja
AWS::Transfer::Profile	Ja	Ja
AWS::Transfer::Workflow	Ja	Ja
AWS::WAFRegional::RateBasedRegel	Ja	Ja
AWS::WAFRegional::Rule	Ja	Ja
AWS::WAFRegional::RuleGroup	Ja	Ja
AWS::WAFRegional::WebACL	Ja	Ja

Ressourcentyp	China (Peking)	China (Ningxia)
AWSWAFv2:: IPSet	Ja	Ja
AWS::WAFv2::ManagedRuleSatz	Ja	Ja
AWS::WAFv2::RegexPatternSatz	Ja	Ja
AWS::WAFv2::RuleGroup	Ja	Ja
AWS::WAFv2::WebACL	Ja	Ja
AWS::WorkSpaces::Workspace	Nein	Ja

Regionen in Afrika und im Nahen Osten

Ressourcentyp	Afrika (Kapstadt)	Israel (Tel Aviv)	Naher Osten (Bahrain)	Naher Osten (VAE)
AWS::ACM::Certificate	Ja	Ja	Ja	Ja
AWS::ACMPCA::CertificateAuthority	Ja	Ja	Ja	Ja
AWS::ACMPCA::CertificateAuthorityAktivierung	Ja	Ja	Ja	Ja
AWS::AccessAnalyzer::Analyzer	Ja	Ja	Ja	Ja

Ressourcentyp	Afrika (Kapstadt)	Israel (Tel Aviv)	Naher Osten (Bahrain)	Naher Osten (VAE)
AWS::AmazonMQ::Broker	Ja	Nein	Ja	Ja
AWS::Amplify::App	Nein	Nein	Ja	Nein
AWS::Amplify::Branch	Nein	Nein	Ja	Nein
AWS::ApiGateway::RestApi	Ja	Ja	Ja	Ja
AWS::ApiGateway::Stage	Ja	Ja	Ja	Ja
AWS::ApiGatewayV2::Api	Ja	Ja	Ja	Ja
AWS::ApiGatewayV2::Stage	Ja	Ja	Ja	Ja
AWS::AppConfig::Application	Ja	Ja	Ja	Nein
AWS::AppConfig::ConfigurationProfile	Ja	Ja	Ja	Nein
AWS::AppConfig::DeploymentStrategy	Ja	Ja	Ja	Ja
AWS::AppConfig::Environment	Ja	Ja	Ja	Nein
AWS::AppConfig::ExtensionAssociation	Ja	Ja	Ja	Ja

Ressourcentyp	Afrika (Kapstadt)	Israel (Tel Aviv)	Naher Osten (Bahrain)	Naher Osten (VAE)
AWS::AppConfig::HostedConfigurationVersion	Ja	Ja	Ja	Nein
AWS::AppFlow::Flow	Ja	Nein	Nein	Nein
AWS::AppIntegrations::Application	Ja	Nein	Nein	Nein
AWS::AppIntegrations::EventIntegration	Ja	Nein	Nein	Nein
AWS::AppMesh::GatewayRoute	Ja	Ja	Ja	Nein
AWS::AppMesh::Mesh	Ja	Ja	Ja	Nein
AWS::AppMesh::Route	Ja	Ja	Ja	Nein
AWS::AppMesh::VirtualGateway	Ja	Ja	Ja	Nein
AWS::AppMesh::VirtualNode	Ja	Ja	Ja	Nein
AWS::AppMesh::VirtualRouter	Ja	Ja	Ja	Nein
AWS::AppMesh::VirtualService	Ja	Ja	Ja	Nein
AWS::AppSync::ApiCache	Ja	Ja	Ja	Ja

Ressourcentyp	Afrika (Kapstadt)	Israel (Tel Aviv)	Naher Osten (Bahrain)	Naher Osten (VAE)
AWS::AppSync::GraphQLApi	Ja	Ja	Ja	Ja
AWS::Athena::DataCatalog	Ja	Ja	Ja	Ja
AWS::Athena::PreparedStatement	Ja	Ja	Ja	Ja
AWS::Athena::WorkGroup	Ja	Ja	Ja	Ja
AWS::AutoScaling::AutoScalingGruppe	Ja	Ja	Ja	Ja
AWS::AutoScaling::LaunchConfiguration	Ja	Ja	Ja	Ja
AWS::AutoScaling::ScalingPolicy	Ja	Ja	Ja	Ja
AWS::AutoScaling::ScheduledAction	Ja	Ja	Ja	Ja
AWS::AutoScaling::WarmPool	Ja	Nein	Ja	Nein
AWS::Backup::BackupPlan	Ja	Ja	Ja	Ja
AWS::Backup::BackupSelection	Ja	Ja	Ja	Ja
AWS::Backup::BackupVault	Ja	Ja	Ja	Ja

Ressourcentyp	Afrika (Kapstadt)	Israel (Tel Aviv)	Naher Osten (Bahrain)	Naher Osten (VAE)
AWS::Backup::RecoveryPoint	Ja	Ja	Ja	Ja
AWS::Backup::ReportPlan	Ja	Nein	Ja	Nein
AWS::Batch::ComputeEnvironment	Ja	Nein	Ja	Ja
AWS::Batch::JobQueue	Ja	Nein	Ja	Ja
AWS::Batch::SchedulingPolicy	Ja	Ja	Ja	Ja
AWS::Cassandra::Keyspace	Nein	Nein	Ja	Nein
AWS::Cloud9::EnvironmentEC2	Ja	Nein	Ja	Nein
AWS::CloudFormation::Stack	Ja	Nein	Ja	Nein
AWS::CloudTrail::Trail	Ja	Ja	Ja	Ja
AWS::CloudWatch::Alarm	Ja	Ja	Ja	Ja
AWS::CloudWatch::MetricStream	Ja	Ja	Ja	Ja
AWS::CodeBuild::Project	Ja	Ja	Ja	Ja

Ressourcentyp	Afrika (Kapstadt)	Israel (Tel Aviv)	Naher Osten (Bahrain)	Naher Osten (VAE)
AWS::CodeBuild::ReportGroup	Ja	Ja	Ja	Ja
AWS::CodeDeploy::Application	Ja	Nein	Ja	Nein
AWS::CodeDeploy::DeploymentConfig	Ja	Nein	Ja	Nein
AWS::CodeDeploy::DeploymentGroup	Ja	Nein	Ja	Nein
AWS::CodePipeline::Pipeline	Nein	Ja	Nein	Ja
AWS::Cognito::IdentityPool	Ja	Ja	Ja	Ja
AWS::Cognito::UserPool	Ja	Ja	Ja	Ja
AWS::Cognito::UserPoolKlient	Ja	Ja	Ja	Ja
AWS::Cognito::UserPoolGruppe	Ja	Ja	Ja	Ja
AWS::Config::ConfigurationRecorder	Ja	Ja	Ja	Ja
AWS::Config::Confo rmancePack-Compliance	Ja	Ja	Ja	Ja
AWS::Config::ResourceCompliance	Ja	Ja	Ja	Ja

Ressourcentyp	Afrika (Kapstadt)	Israel (Tel Aviv)	Naher Osten (Bahrain)	Naher Osten (VAE)
AWS::Connect::Instance	Ja	Nein	Nein	Nein
AWS::Connect::PhoneNumber	Ja	Nein	Nein	Nein
AWS::Connect::QuickConnect	Ja	Nein	Nein	Nein
AWS::Connect::Rule	Ja	Nein	Nein	Nein
AWS::Connect::User	Ja	Nein	Nein	Nein
AWS::CustomerProfiles::Domain	Ja	Nein	Nein	Nein
AWS::CustomerProfiles::ObjectType	Ja	Nein	Nein	Nein
AWS::DMS::Certificate	Ja	Nein	Ja	Nein
AWS::DMS::Endpoint	Ja	Nein	Ja	Nein
AWS::DMS::EventSubscription	Ja	Nein	Ja	Nein
AWS::DMS::ReplicationInstance	Ja	Nein	Ja	Nein
AWS::DMS::ReplicationSubnetGruppe	Ja	Nein	Ja	Nein

Ressourcentyp	Afrika (Kapstadt)	Israel (Tel Aviv)	Naher Osten (Bahrain)	Naher Osten (VAE)
AWS::DMS::ReplicationTask	Ja	Nein	Ja	Nein
AWS::DataSync::LocationEFS	Ja	Nein	Ja	Ja
AWS::DataSync::LocationFSxGlanz	Ja	Nein	Ja	Nein
AWS::DataSync::LocationFSxFenster	Ja	Nein	Ja	Nein
AWS::DataSync::LocationHDFS	Ja	Nein	Ja	Ja
AWS::DataSync::LocationNFS	Ja	Nein	Ja	Ja
AWS::DataSync::LocationObjectSpeicher	Ja	Nein	Ja	Ja
AWS::DataSync::LocationS 3	Ja	Ja	Ja	Ja
AWS::DataSync::LocationSMB	Ja	Nein	Ja	Ja
AWS::DataSync::Task	Ja	Ja	Ja	Ja
AWS::Detective::Graph	Ja	Ja	Ja	Nein
AWS::DynamoDB::Table	Ja	Ja	Ja	Ja

Ressourcentyp	Afrika (Kapstadt)	Israel (Tel Aviv)	Naher Osten (Bahrain)	Naher Osten (VAE)
AWS::EC2::CapacityReservation	Ja	Ja	Ja	Ja
AWS::EC2::ClientVpnEndpunkt	Ja	Nein	Ja	Nein
AWS::EC2::ClientVpnTargetNetworkAssociation	Ja	Ja	Ja	Nein
AWS::EC2::CustomerGateway	Ja	Ja	Ja	Ja
AWSEC2:: DHCPOptions	Ja	Ja	Ja	Ja
AWS:EC2:: EC2 Flotte	Ja	Nein	Ja	Ja
AWS::EC2: EIP	Ja	Ja	Ja	Ja
AWSEC2:: EIPAssociation	Ja	Ja	Ja	Ja
AWS::EC2::EgressOnlyInternetGateway	Ja	Nein	Ja	Ja
AWS::EC2::FlowLog	Ja	Nein	Ja	Ja
AWS::EC2::Host	Ja	Ja	Ja	Ja
AWS:::EC2: IPAM	Ja	Nein	Ja	Ja

Ressourcentyp	Afrika (Kapstadt)	Israel (Tel Aviv)	Naher Osten (Bahrain)	Naher Osten (VAE)
AWSEC2:: IPAMPool	Ja	Nein	Ja	Ja
AWS:EC2:: IPAMResource Entdeckung	Ja	Ja	Ja	Ja
AWS:EC2:: IPAMResou rce DiscoveryAssociation	Ja	Ja	Ja	Ja
AWSEC2:: IPAMScope	Ja	Nein	Ja	Ja
AWS::EC2::Instance	Ja	Ja	Ja	Ja
AWS::EC2::InstanceConnectEndpunkt	Ja	Ja	Ja	Ja
AWS::EC2::InternetGateway	Ja	Ja	Ja	Ja
AWS::EC2::LaunchTemplate	Ja	Nein	Ja	Nein
AWS::EC2::NatGateway	Ja	Nein	Ja	Ja
AWS::EC2::NetworkAcl	Ja	Ja	Ja	Ja
AWS::EC2::NetworkInsightsAccessScope	Ja	Nein	Ja	Nein
AWS::EC2::NetworkI nsightsAccessScopeAnalysis	Ja	Nein	Ja	Nein

Ressourcentyp	Afrika (Kapstadt)	Israel (Tel Aviv)	Naher Osten (Bahrain)	Naher Osten (VAE)
AWS::EC2::NetworkInsightsAnalyse	Ja	Nein	Ja	Nein
AWS::EC2::NetworkInsightsPfad	Ja	Nein	Ja	Nein
AWS::EC2::NetworkInterface	Ja	Ja	Ja	Ja
AWS::EC2::PrefixList	Ja	Ja	Ja	Ja
AWS::EC2::RouteTable	Ja	Ja	Ja	Ja
AWS::EC2::SecurityGroup	Ja	Ja	Ja	Ja
AWS::EC2::SnapshotBlockPublicAccess	Ja	Ja	Ja	Ja
AWS::EC2::SpotFleet	Ja	Ja	Ja	Ja
AWS::EC2::Subnet	Ja	Ja	Ja	Ja
AWS::EC2::SubnetRouteTableAssociation	Ja	Ja	Ja	Ja
AWS::EC2::TrafficMirrorFilter	Ja	Ja	Ja	Ja
AWS::EC2::TrafficMirrorSitzung	Nein	Nein	Ja	Nein

Ressourcentyp	Afrika (Kapstadt)	Israel (Tel Aviv)	Naher Osten (Bahrain)	Naher Osten (VAE)
AWS::EC2::TrafficMirrorZiel	Nein	Nein	Ja	Nein
AWS::EC2::TransitGateway	Ja	Ja	Ja	Ja
AWS::EC2::TransitGatewayAnlage	Ja	Nein	Ja	Ja
AWS::EC2::TransitGatewayConnect	Ja	Nein	Ja	Ja
AWS::EC2::TransitG atewayMulticastDomain	Ja	Ja	Ja	Ja
AWS::EC2::TransitGatewayRouteTable	Ja	Nein	Ja	Ja
AWS:EC2: :VPC	Ja	Ja	Ja	Ja
AWS:EC2:: VPCBlock PublicAccessExclusion	Ja	Ja	Ja	Ja
AWS:EC2:: VPCBlock PublicAccessOptions	Ja	Ja	Ja	Ja
AWSEC2:: VPCEndpoint	Ja	Ja	Ja	Ja
AWS:EC2:: VPCEndpoi nt ConnectionNotification	Ja	Ja	Ja	Ja
AWS:EC2:: VPCEndpoint Dienst	Ja	Ja	Ja	Ja

Ressourcentyp	Afrika (Kapstadt)	Israel (Tel Aviv)	Naher Osten (Bahrain)	Naher Osten (VAE)
AWS::EC2:: VPCPeering Verbindung	Ja	Ja	Ja	Ja
AWSEC2:: VPNConnection	Ja	Ja	Ja	Ja
AWS::EC2:: VPNConnection Route	Ja	Ja	Ja	Ja
AWSEC2:: VPNGateway	Ja	Ja	Ja	Ja
AWS::EC2::Volume	Ja	Ja	Ja	Ja
AWS::ECR::PullThroughCacheRule	Ja	Ja	Ja	Ja
AWS::ECR::RegistryPolicy	Ja	Ja	Ja	Ja
AWS::ECR::Repository	Ja	Ja	Ja	Ja
AWS::ECS::CapacityProvider	Ja	Ja	Ja	Ja
AWS::ECS::Cluster	Ja	Ja	Ja	Ja
AWS::ECS::Service	Ja	Ja	Ja	Ja
AWS::ECS::TaskDefinition	Ja	Ja	Ja	Ja

Ressourcentyp	Afrika (Kapstadt)	Israel (Tel Aviv)	Naher Osten (Bahrain)	Naher Osten (VAE)
AWS::ECS::TaskSet	Ja	Nein	Ja	Ja
AWS::EFS::AccessPoint	Ja	Ja	Ja	Ja
AWS::EFS::FileSystem	Ja	Ja	Ja	Ja
AWS::EKS::Addon	Ja	Nein	Ja	Ja
AWS::EKS::Cluster	Ja	Nein	Ja	Ja
AWS::EKS::FargateProfile	Ja	Ja	Ja	Ja
AWS::EKS::IdentityProviderConfig	Ja	Nein	Ja	Ja
AWS::EMR::SecurityConfiguration	Ja	Ja	Ja	Ja
AWS::ElasticBeanstalk::Application	Ja	Nein	Ja	Ja
AWS::ElasticBeanstalk::ApplicationVersion	Ja	Nein	Ja	Ja
AWS::ElasticBeanstalk::Environment	Ja	Nein	Ja	Ja
AWS::ElasticLoadBalancing::LoadBalancer	Ja	Ja	Ja	Ja

Ressourcentyp	Afrika (Kapstadt)	Israel (Tel Aviv)	Naher Osten (Bahrain)	Naher Osten (VAE)
AWS::ElasticLoadBalancingV2::Listener	Ja	Nein	Ja	Nein
AWS::ElasticLoadBalancingV2::LoadBalancer	Ja	Ja	Ja	Ja
AWS::Elasticsearch::Domain	Ja	Ja	Ja	Ja
AWS::EventSchemas::Discoverer	Ja	Nein	Ja	Ja
AWS::EventSchemas::Registry	Ja	Nein	Ja	Ja
AWS::EventSchemas::RegistryPolicy	Ja	Nein	Ja	Ja
AWS::EventSchemas::Schema	Ja	Nein	Ja	Ja
AWS::Events::ApiDestination	Ja	Nein	Ja	Ja
AWS::Events::Archive	Ja	Nein	Ja	Ja
AWS::Events::Connection	Ja	Nein	Ja	Ja
AWS::Events::EventBus	Ja	Ja	Ja	Ja
AWS::Events::Rule	Ja	Nein	Ja	Nein

Ressourcentyp	Afrika (Kapstadt)	Israel (Tel Aviv)	Naher Osten (Bahrain)	Naher Osten (VAE)
AWS::FIS::ExperimentTemplate	Ja	Nein	Ja	Nein
AWS::Glue::Classifier	Ja	Ja	Ja	Ja
AWS::Glue::Job	Ja	Ja	Ja	Ja
AWS::Glue::MLTransform	Ja	Ja	Ja	Ja
AWS::GroundStation::Config	Ja	Nein	Ja	Nein
AWS::GroundStation ::DataflowEndpointGruppe	Ja	Nein	Ja	Nein
AWS::GroundStation::MissionProfile	Ja	Nein	Ja	Nein
AWS::GuardDuty::Detector	Ja	Ja	Ja	Ja
AWS::GuardDuty::Filter	Ja	Nein	Ja	Nein
AWS::GuardPflicht: IPSet	Ja	Nein	Ja	Ja
AWS::GuardDuty::ThreatIntelSatz	Ja	Ja	Ja	Ja
AWS::IAM::Group	Ja	Nein	Ja	Nein

Ressourcentyp	Afrika (Kapstadt)	Israel (Tel Aviv)	Naher Osten (Bahrain)	Naher Osten (VAE)
AWS::IAM::Policy	Ja	Nein	Ja	Nein
AWS::IAM::Role	Ja	Nein	Ja	Nein
AWS::IAM::User	Ja	Nein	Ja	Nein
AWS::ImageBuilder::ContainerRecipe	Ja	Ja	Ja	Ja
AWS::ImageBuilder::DistributionConfiguration	Ja	Ja	Ja	Ja
AWS::ImageBuilder::ImagePipeline	Ja	Ja	Ja	Ja
AWS::ImageBuilder::ImageRecipe	Ja	Ja	Ja	Ja
AWS::ImageBuilder::InfrastructureConfiguration	Ja	Ja	Ja	Ja
AWS::InspectorV2::Activation	Ja	Nein	Ja	Nein
AWS::InspectorV2::Filter	Ja	Nein	Ja	Nein
AWS::IoT::AccountAuditKonfiguration	Nein	Nein	Ja	Ja
AWS::IoT::Authorizer	Nein	Nein	Ja	Ja

Ressourcentyp	Afrika (Kapstadt)	Israel (Tel Aviv)	Naher Osten (Bahrain)	Naher Osten (VAE)
AWS::IoT: CACertificate	Nein	Nein	Ja	Ja
AWS::IoT::CustomMetric	Nein	Nein	Ja	Ja
AWS::IoT::Dimension	Nein	Nein	Ja	Ja
AWS::IoT::FleetMetric	Nein	Nein	Ja	Ja
AWS::IoT::JobTemplate	Nein	Nein	Ja	Ja
AWS::IoT::MitigationAction	Nein	Nein	Ja	Ja
AWS::IoT::Policy	Nein	Nein	Ja	Ja
AWS::IoT::ProvisioningTemplate	Nein	Nein	Ja	Ja
AWS::IoT::RoleAlias	Nein	Nein	Ja	Ja
AWS::IoT::ScheduledAudit	Nein	Nein	Ja	Ja
AWS::IoT::SecurityProfile	Nein	Nein	Ja	Ja
AWS::KMS::Alias	Ja	Nein	Ja	Ja

Ressourcentyp	Afrika (Kapstadt)	Israel (Tel Aviv)	Naher Osten (Bahrain)	Naher Osten (VAE)
AWS::KMS::Key	Ja	Ja	Ja	Ja
AWS::Kinesis::Stream	Ja	Nein	Ja	Ja
AWS::Kinesis::StreamConsumer	Ja	Ja	Ja	Ja
AWS::KinesisAnalyticsV2::Application	Ja	Ja	Ja	Ja
AWS::KinesisFirehose::DeliveryStream	Ja	Ja	Ja	Ja
AWS::Lambda::CodeSigningConfig	Ja	Nein	Ja	Nein
AWS::Lambda::Function	Ja	Ja	Ja	Ja
AWS::Lex::Bot	Ja	Nein	Nein	Nein
AWS::Lex::BotAlias	Ja	Nein	Nein	Nein
AWS::Logs::Destination	Ja	Ja	Ja	Ja
AWS::MSK::BatchScramGeheim	Ja	Nein	Ja	Ja
AWS::MSK::Cluster	Ja	Nein	Ja	Ja

Ressourcentyp	Afrika (Kapstadt)	Israel (Tel Aviv)	Naher Osten (Bahrain)	Naher Osten (VAE)
AWS::MSK::ClusterPolicy	Ja	Ja	Ja	Ja
AWS::MSK::Configuration	Ja	Ja	Ja	Ja
AWS::MSK::VpcConnection	Ja	Ja	Ja	Ja
AWS::Macie::Session	Ja	Ja	Ja	Nein
AWS::MediaConnect::FlowEntitlement	Ja	Nein	Nein	Ja
AWS::MediaConnect::FlowSource	Ja	Nein	Nein	Ja
AWS::MediaConnect::FlowVpcSchnittstelle	Ja	Nein	Nein	Nein
AWS::MediaConnect::Gateway	Ja	Nein	Nein	Nein
AWS::MediaTailor::PlaybackConfiguration	Ja	Nein	Nein	Ja
AWS::NetworkFirewall::Firewall	Ja	Ja	Ja	Ja
AWS::NetworkFirewall::FirewallPolicy	Ja	Ja	Ja	Ja
AWS::NetworkFirewall::RuleGroup	Ja	Ja	Ja	Ja

Ressourcentyp	Afrika (Kapstadt)	Israel (Tel Aviv)	Naher Osten (Bahrain)	Naher Osten (VAE)
AWS::NetworkFirewall: TLSInspection Konfiguration	Ja	Ja	Ja	Ja
AWS::NetworkFirewall::VpcEndpointAssoziation	Ja	Ja	Ja	Ja
AWS::OpenSearch::Domain	Ja	Nein	Ja	Nein
AWS: :RDS: DBCluster	Ja	Ja	Ja	Ja
AWS: :RDS:: Schnappschuss DBCluster	Ja	Nein	Ja	Ja
AWS: :RDS: DBInstance	Ja	Ja	Ja	Ja
AWS: :RDS:: Gruppe DBSecurity	Ja	Ja	Ja	Ja
AWS: :RDS: DBSnapshot	Ja	Ja	Ja	Ja
AWS: :RDS:: Gruppe DBSubnet	Ja	Ja	Ja	Ja
AWS::RDS::EventSubscription	Ja	Ja	Ja	Ja
AWS::RDS::GlobalCluster	Ja	Ja	Ja	Ja
AWS::RDS::OptionGroup	Ja	Ja	Ja	Ja

Ressourcentyp	Afrika (Kapstadt)	Israel (Tel Aviv)	Naher Osten (Bahrain)	Naher Osten (VAE)
AWS::RUM::AppMonitor	Nein	Nein	Ja	Ja
AWS::Redshift::Cluster	Ja	Ja	Ja	Ja
AWS::Redshift::ClusterParameterGruppe	Ja	Ja	Ja	Ja
AWS::Redshift::ClusterSecurityGruppe	Ja	Ja	Ja	Ja
AWS::Redshift::ClusterSnapshot	Ja	Ja	Ja	Ja
AWS::Redshift::ClusterSubnetGruppe	Ja	Ja	Ja	Ja
AWS::Redshift::EventSubscription	Ja	Ja	Ja	Ja
AWS::Redshift::ScheduledAction	Nein	Nein	Ja	Nein
AWS::ResilienceHub::App	Ja	Nein	Ja	Nein
AWS::ResilienceHub::ResiliencyPolicy	Ja	Nein	Ja	Nein
AWS::ResourceExplorer2::Index	Nein	Nein	Ja	Ja
AWS::Route53Profiles::Profile	Ja	Ja	Ja	Ja

Ressourcentyp	Afrika (Kapstadt)	Israel (Tel Aviv)	Naher Osten (Bahrain)	Naher Osten (VAE)
AWS::Route53Resolver::FirewallDomainListe	Ja	Nein	Ja	Nein
AWS::Route53Resolver::FirewallRuleGruppe	Ja	Nein	Ja	Nein
AWS::Route53Resolver::FirewallRuleGroupAssociation	Ja	Nein	Ja	Nein
AWS::Route53Resolver::ResolverEndpoint	Ja	Nein	Ja	Ja
AWS::Route53Resolver::ResolverQueryLoggingConfig	Ja	Nein	Ja	Nein
AWS::Route53Resolver::ResolverQueryLoggingConfigAssociation	Ja	Nein	Ja	Nein
AWS::Route53Resolver::ResolverRule	Ja	Nein	Ja	Ja
AWS::Route53Resolver::ResolverRuleVerband	Ja	Nein	Ja	Ja
AWS::S3::AccessPoint	Ja	Ja	Ja	Ja
AWS::S3::AccountPublicAccessBlock	Ja	Nein	Ja	Ja
AWS::S3::Bucket	Ja	Ja	Ja	Ja
AWS::SES::ConfigurationSet	Ja	Ja	Ja	Nein

Ressourcentyp	Afrika (Kapstadt)	Israel (Tel Aviv)	Naher Osten (Bahrain)	Naher Osten (VAE)
AWS::SES::ContactList	Ja	Ja	Ja	Nein
AWS::SES::Template	Ja	Ja	Ja	Nein
AWS::SNS::Topic	Ja	Ja	Ja	Ja
AWS::SQS::Queue	Ja	Nein	Ja	Nein
AWS::SSM::AssociationCompliance	Ja	Ja	Ja	Ja
AWS::SSM::Document	Ja	Ja	Ja	Ja
AWS::SSM::FileData	Ja	Ja	Ja	Ja
AWS::SSM::ManagedInstance-Bestand	Ja	Ja	Ja	Ja
AWS::SSM::PatchCompliance	Ja	Ja	Ja	Ja
AWS::SageMaker::AppImageConfig	Ja	Ja	Ja	Ja
AWS::SageMaker::CodeRepository	Ja	Nein	Ja	Nein
AWS::SageMaker::Domain	Ja	Nein	Ja	Nein

Ressourcentyp	Afrika (Kapstadt)	Israel (Tel Aviv)	Naher Osten (Bahrain)	Naher Osten (VAE)
AWS::SageMaker::EndpointConfig	Ja	Nein	Ja	Nein
AWS::SageMaker::FeatureGroup	Ja	Ja	Ja	Nein
AWS::SageMaker::Image	Ja	Ja	Ja	Ja
AWS::SageMaker::InferenceExperiment	Ja	Nein	Ja	Nein
AWS::SageMaker::Model	Ja	Nein	Ja	Nein
AWS::SageMaker::NotebookInstance	Ja	Nein	Ja	Nein
AWS::SageMaker::NotebookInstanceLifecycleConfig	Ja	Nein	Ja	Nein
AWS::SecretsManager::Secret	Ja	Ja	Ja	Ja
AWS::SecurityHub::Standard	Ja	Ja	Ja	Ja
AWS::ServiceCatalog::CloudFormationProdukt	Ja	Nein	Ja	Ja
AWS::ServiceCatalog::CloudFormationProvisionedProduct	Ja	Nein	Ja	Ja
AWS::ServiceCatalog::Portfolio	Ja	Nein	Ja	Ja

Ressourcentyp	Afrika (Kapstadt)	Israel (Tel Aviv)	Naher Osten (Bahrain)	Naher Osten (VAE)
AWS::ServiceDiscovery::HttpNamespace	Ja	Ja	Ja	Ja
AWS::ServiceDiscovery::Instance	Ja	Nein	Ja	Ja
AWS::ServiceDiscovery::PublicDnsNamespace	Ja	Ja	Ja	Ja
AWS::ServiceDiscovery::Service	Ja	Nein	Ja	Ja
AWS::ShieldRegional::Protection	Ja	Nein	Ja	Ja
AWS::Signer::SigningProfile	Ja	Nein	Ja	Nein
AWS::StepFunctions::Activity	Ja	Ja	Ja	Ja
AWS::StepFunctions::StateMachine	Ja	Ja	Ja	Ja
AWS::Transfer::Agreement	Ja	Nein	Ja	Ja
AWS::Transfer::Certificate	Ja	Ja	Ja	Ja
AWS::Transfer::Connector	Ja	Ja	Ja	Ja
AWS::Transfer::Profile	Ja	Ja	Ja	Ja

Ressourcentyp	Afrika (Kapstadt)	Israel (Tel Aviv)	Naher Osten (Bahrain)	Naher Osten (VAE)
AWS::Transfer::Workflow	Ja	Ja	Ja	Ja
AWS::WAFRegional::RateBasedRegel	Ja	Ja	Ja	Ja
AWS::WAFRegional::Rule	Ja	Ja	Ja	Ja
AWS::WAFRegional::RuleGroup	Ja	Ja	Ja	Ja
AWS::WAFRegional::WebACL	Ja	Ja	Ja	Ja
AWSWAFv2:: IPSet	Ja	Ja	Ja	Ja
AWS::WAFv2::ManagedRuleSatz	Ja	Ja	Ja	Ja
AWS::WAFv2::RegexPatternSatz	Ja	Ja	Ja	Ja
AWS::WAFv2::RuleGroup	Ja	Ja	Ja	Ja
AWS::WAFv2::WebACL	Ja	Ja	Ja	Ja
AWS::WorkSpaces::Workspace	Ja	Nein	Nein	Nein
AWS::XRay::EncryptionConfig	Ja	Ja	Nein	Ja

GovCloud Regionen

Ressourcentyp	AWS GovCloud (US-West)	AWS GovCloud (US-Ost)
AWS::ACM::Certificate	Ja	Ja
AWS::ACMPCA::CertificateAuthority	Ja	Ja
AWS::ACMPCA::CertificateAuthorityAktivierung	Ja	Ja
AWS::AccessAnalyzer::Analyzer	Ja	Ja
AWS::AmazonMQ::Broker	Ja	Ja
AWS::ApiGateway::RestApi	Ja	Ja
AWS::ApiGateway::Stage	Ja	Ja
AWS::ApiGatewayV2::Api	Ja	Ja
AWS::ApiGatewayV2::Stage	Ja	Ja
AWS::AppConfig::Application	Ja	Ja
AWS::AppConfig::ConfigurationProfile	Ja	Ja

Ressourcentyp	AWS GovCloud (US-West)	AWS GovCloud (US-Ost)
AWS::AppConfig::DeploymentStrategy	Ja	Ja
AWS::AppConfig::Environment	Ja	Ja
AWS::AppConfig::ExtensionAssociation	Ja	Ja
AWS::AppConfig::HostedConfigurationVersion	Ja	Ja
AWS::AppStream::Application	Ja	Ja
AWS::AppStream::DirectoryConfig	Ja	Nein
AWS::AppStream::Fleet	Ja	Nein
AWS::AppStream::Stack	Ja	Nein
AWS::Athena::DataCatalog	Ja	Ja
AWS::Athena::WorkGroup	Ja	Ja
AWS::AutoScaling::AutoScalingGruppe	Ja	Ja
AWS::AutoScaling::LaunchConfiguration	Ja	Ja

Ressourcentyp	AWS GovCloud (US-West)	AWS GovCloud (US-Ost)
AWS::AutoScaling::ScalingPolicy	Ja	Ja
AWS::AutoScaling::ScheduledAction	Ja	Ja
AWS::AutoScaling::WarmPool	Ja	Ja
AWS::Backup::BackupPlan	Ja	Ja
AWS::Backup::BackupSelection	Ja	Ja
AWS::Backup::BackupVault	Ja	Ja
AWS::Backup::RecoveryPoint	Ja	Ja
AWS::Batch::ComputeEnvironment	Ja	Ja
AWS::Batch::JobQueue	Ja	Ja
AWS::Batch::SchedulingPolicy	Ja	Ja
AWS::Bedrock::Guardrail	Ja	Ja
AWS::Bedrock::KnowledgeBase	Ja	Ja

Ressourcentyp	AWS GovCloud (US-West)	AWS GovCloud (US-Ost)
AWS::Cassandra::Keyspace	Ja	Ja
AWS::CloudFormation::Stack	Ja	Ja
AWS::CloudTrail::Trail	Ja	Ja
AWS::CloudWatch::Alarm	Ja	Ja
AWS::CodeBuild::Project	Ja	Ja
AWS::CodeBuild::ReportGroup	Ja	Ja
AWS::Cognito::IdentityPool	Ja	Nein
AWS::Cognito::UserPoolGruppe	Ja	Nein
AWS::Config::ConfigurationRecorder	Ja	Ja
AWS::Config::ConformancePack-Compliance	Ja	Ja
AWS::Config::ResourceCompliance	Ja	Ja
AWS::Connect::Instance	Ja	Nein

Ressourcentyp	AWS GovCloud (US-West)	AWS GovCloud (US-Ost)
AWS::Connect::QuickConnect	Ja	Nein
AWS::Connect::User	Ja	Nein
AWS::DMS::Certificate	Ja	Ja
AWS::DMS::Endpoint	Ja	Ja
AWS::DMS::EventSubscription	Ja	Ja
AWS::DMS::ReplicationInstance	Ja	Ja
AWS::DMS::ReplicationSubnetGruppe	Ja	Ja
AWS::DMS::ReplicationTask	Ja	Ja
AWS::DataSync::LocationEFS	Ja	Ja
AWS::DataSync::LocationFSxGlanz	Ja	Ja
AWS::DataSync::LocationFSxFenster	Ja	Ja
AWS::DataSync::LocationHDFS	Ja	Ja

Ressourcentyp	AWS GovCloud (US-West)	AWS GovCloud (US-Ost)
AWS::DataSync::LocationNFS	Ja	Ja
AWS::DataSync::LocationObjectSpeicher	Ja	Ja
AWS::DataSync::LocationS 3	Ja	Ja
AWS::DataSync::LocationSMB	Ja	Ja
AWS::DataSync::Task	Ja	Ja
AWS::Detective::Graph	Ja	Ja
AWS::DynamoDB::Table	Ja	Ja
AWS::EC2::CapacityReservation	Ja	Ja
AWS::EC2::ClientVpnEndpunkt	Ja	Ja
AWS::EC2::ClientVpnTargetNetworkAssociation	Ja	Ja
AWS::EC2::CustomerGateway	Ja	Ja
AWSEC2:: DHCPOptions	Ja	Ja

Ressourcentyp	AWS GovCloud (US-West)	AWS GovCloud (US-Ost)
AWS:EC2:: EC2 Flotte	Ja	Ja
AWS::EC2: EIP	Ja	Ja
AWS::EC2::EgressOnlyInternetGateway	Ja	Ja
AWS::EC2::FlowLog	Ja	Ja
AWS::EC2::Host	Ja	Ja
AWS:::EC2: IPAM	Ja	Ja
AWS:EC2:: IPAMPool	Ja	Ja
AWS:EC2:: IPAMResource Entdeckung	Ja	Ja
AWS:EC2:: IPAMResource DiscoveryAssociation	Ja	Ja
AWS:EC2:: IPAMScope	Ja	Ja
AWS::EC2::Instance	Ja	Ja
AWS::EC2::InstanceConnectEndpunkt	Ja	Ja

Ressourcentyp	AWS GovCloud (US-West)	AWS GovCloud (US-Ost)
AWS::EC2::InternetGateway	Ja	Ja
AWS::EC2::LaunchTemplate	Ja	Ja
AWS::EC2::NatGateway	Ja	Ja
AWS::EC2::NetworkAcl	Ja	Ja
AWS::EC2::NetworkInterface	Ja	Ja
AWS::EC2::PrefixList	Ja	Ja
AWS::EC2::RouteTable	Ja	Ja
AWS::EC2::SecurityGroup	Ja	Ja
AWS::EC2::SnapshotBlockPublicAccess	Ja	Ja
AWS::EC2::SpotFleet	Ja	Ja
AWS::EC2::Subnet	Ja	Ja
AWS::EC2::SubnetRouteTableAssociation	Ja	Ja

Ressourcentyp	AWS GovCloud (US-West)	AWS GovCloud (US-Ost)
AWS::EC2::TrafficMirrorFiltern	Ja	Ja
AWS::EC2::TrafficMirrorSitzung	Ja	Ja
AWS::EC2::TrafficMirrorZiel	Ja	Ja
AWS::EC2::TransitGateway	Ja	Nein
AWS::EC2::TransitGatewayAnlage	Ja	Ja
AWS::EC2::TransitGatewayConnect	Ja	Ja
AWS::EC2::TransitGatewayMulticastDomain	Ja	Ja
AWS::EC2::TransitGatewayRouteTable	Ja	Ja
AWS:EC2: :VPC	Ja	Ja
AWS:EC2:: VPCBlock PublicAccessExclusion	Ja	Ja
AWS:EC2:: VPCBlock PublicAccessOptions	Ja	Ja
AWS:EC2:: VPCEndpoint	Ja	Ja

Ressourcentyp	AWS GovCloud (US-West)	AWS GovCloud (US-Ost)
AWS:EC2:: VPCEndpoint ConnectionNotification	Ja	Ja
AWS:EC2:: VPCEndpoint Dienst	Ja	Nein
AWS::EC2:: VPCPeering Verbindung	Ja	Ja
AWS:EC2:: VPNConnection	Ja	Ja
AWS::EC2:: VPNConnection Route	Ja	Ja
AWS:EC2:: VPNGateway	Ja	Ja
AWS::EC2::Volume	Ja	Ja
AWS::ECR::Repository	Ja	Ja
AWS::ECS::CapacityProvider	Ja	Ja
AWS::ECS::Cluster	Ja	Ja
AWS::ECS::Service	Ja	Ja
AWS::ECS::TaskDefinition	Ja	Ja

Ressourcentyp	AWS GovCloud (US-West)	AWS GovCloud (US-Ost)
AWS::ECS::TaskSet	Ja	Ja
AWS::EFS::AccessPoint	Ja	Ja
AWS::EFS::FileSystem	Ja	Ja
AWS::EKS::Addon	Ja	Ja
AWS::EKS::Cluster	Ja	Ja
AWS::EKS::IdentityProviderConfig	Ja	Ja
AWS::EMR::SecurityConfiguration	Ja	Ja
AWS::ElasticBeanstalk::Application	Ja	Ja
AWS::ElasticBeanstalk::ApplicationVersion	Ja	Ja
AWS::ElasticBeanstalk::Environment	Ja	Ja
AWS::ElasticLoadBalancing::LoadBalancer	Ja	Ja
AWS::ElasticLoadBalancingV2::Listener	Ja	Ja

Ressourcentyp	AWS GovCloud (US-West)	AWS GovCloud (US-Ost)
AWS::ElasticLoadBalancingV2::LoadBalancer	Ja	Ja
AWS::Elasticsearch::Domain	Ja	Ja
AWS::Events::EventBus	Ja	Ja
AWS::Events::Rule	Ja	Ja
AWS::FIS::ExperimentTemplate	Ja	Ja
AWS::Glue::Classifier	Ja	Ja
AWS::Glue::Job	Ja	Ja
AWS::Glue::MLTransform	Ja	Nein
AWS::GreengrassV2::ComponentVersion	Ja	Ja
AWS::GuardDuty::Detector	Ja	Ja
AWS::GuardDuty::Filter	Ja	Ja
AWS::GuardPflicht: IPSet	Ja	Ja

Ressourcentyp	AWS GovCloud (US-West)	AWS GovCloud (US-Ost)
AWS::GuardDuty::ThreatIntelSatz	Ja	Ja
AWS::IAM::Group	Ja	Ja
AWS::IAM::InstanceProfile	Nein	Ja
AWS: :ICH: OIDCProvider	Nein	Ja
AWS::IAM::Policy	Ja	Ja
AWS::IAM::Role	Ja	Ja
AWS: :ICH: SAMLProvider	Nein	Ja
AWS::IAM::ServerCertificate	Nein	Ja
AWS::IAM::User	Ja	Ja
AWS::ImageBuilder::ContainerRecipe	Ja	Ja
AWS::ImageBuilder::DistributionConfiguration	Ja	Ja
AWS::ImageBuilder::ImagePipeline	Ja	Ja

Ressourcentyp	AWS GovCloud (US-West)	AWS GovCloud (US-Ost)
AWS::ImageBuilder::ImageRecipe	Ja	Ja
AWS::ImageBuilder::InfrastructureConfiguration	Ja	Ja
AWS::InspectorV2::Activation	Ja	Ja
AWS::IoT::AccountAuditKonfiguration	Ja	Ja
AWS::IoT::Authorizer	Ja	Ja
AWS::IoT: CACertificate	Ja	Ja
AWS::IoT::CustomMetric	Ja	Ja
AWS::IoT::Dimension	Ja	Ja
AWS::IoT::FleetMetric	Ja	Ja
AWS::IoT::JobTemplate	Ja	Ja
AWS::IoT::MitigationAction	Ja	Ja
AWS::IoT::Policy	Ja	Ja

Ressourcentyp	AWS GovCloud (US-West)	AWS GovCloud (US-Ost)
AWS::IoT::ProvisioningTemplate	Ja	Ja
AWS::IoT::RoleAlias	Ja	Ja
AWS::IoT::ScheduledAudit	Ja	Ja
AWS::IoT::SecurityProfile	Ja	Ja
AWS::IoTEvents::AlarmModel	Ja	Nein
AWS::IoTEvents::DetectorModel	Ja	Nein
AWS::IoTEvents::Input	Ja	Nein
AWS::IoTSiteWise::AssetModel	Ja	Nein
AWS::IoTSiteWise::Gateway	Ja	Nein
AWS::IoTSiteWise::Portal	Ja	Nein
AWS::IoTTwinMaker::ComponentType	Ja	Nein
AWS::IoTTwinMaker::Entity	Ja	Nein

Ressourcentyp	AWS GovCloud (US-West)	AWS GovCloud (US-Ost)
AWS::IoTTwinMaker::Workspace	Ja	Nein
AWS::KMS::Alias	Ja	Ja
AWS::KMS::Key	Ja	Ja
AWS::Kinesis::Stream	Ja	Ja
AWS::Kinesis::StreamConsumer	Ja	Ja
AWS::KinesisAnalyticsV2::Application	Ja	Ja
AWS::KinesisFirehose::DeliveryStream	Ja	Ja
AWS::Lambda::Function	Ja	Ja
AWS::Logs::Destination	Ja	Ja
AWS::MSK::BatchScramGeheim	Ja	Ja
AWS::MSK::Cluster	Ja	Ja
AWS::MSK::ClusterPolicy	Ja	Ja

Ressourcentyp	AWS GovCloud (US-West)	AWS GovCloud (US-Ost)
AWS::MSK::Configuration	Ja	Ja
AWS::MSK::VpcConnection	Ja	Ja
AWS::NetworkFirewall::Firewall	Ja	Ja
AWS::NetworkFirewall::FirewallPolicy	Ja	Ja
AWS::NetworkFirewall::RuleGroup	Ja	Ja
AWS::NetworkFirewall::VpcEndpointAssoziation	Ja	Ja
AWS::NetworkManager::CustomerGatewayAssoziation	Ja	Nein
AWS::NetworkManager::Device	Ja	Nein
AWS::NetworkManager::GlobalNetwork	Ja	Nein
AWS::NetworkManager::Link	Ja	Nein
AWS::NetworkManager::LinkAssociation	Ja	Nein
AWS::NetworkManager::Site	Ja	Nein

Ressourcentyp	AWS GovCloud (US-West)	AWS GovCloud (US-Ost)
AWS::NetworkManager::TransitGatewayRegistrierung	Ja	Nein
AWS::OpenSearch::Domain	Ja	Ja
AWS::Pinpoint::App	Ja	Nein
AWS::Pinpoint::ApplicationSettings	Ja	Nein
AWS::Pinpoint::Campaign	Ja	Nein
AWS::Pinpoint::EmailChannel	Ja	Nein
AWS::Pinpoint::EmailTemplate	Ja	Nein
AWS::Pinpoint::EventStream	Ja	Nein
AWS::Pinpoint::InAppVorlage	Ja	Nein
AWS::Pinpoint::Segment	Ja	Nein
AWS::QuickSight::Template	Ja	Nein
AWS: :RDS: DBCluster	Ja	Ja

Ressourcentyp	AWS GovCloud (US-West)	AWS GovCloud (US-Ost)
AWS: :RDS:: Schnappschuss DBCluster	Ja	Ja
AWS: :RDS: DBInstance	Ja	Ja
AWS: :RDS:: Gruppe DBSecurity	Ja	Ja
AWS: :RDS: DBSnapshot	Ja	Ja
AWS: :RDS:: Gruppe DBSubnet	Ja	Ja
AWS::RDS::EventSubscription	Ja	Ja
AWS::RDS::OptionGroup	Ja	Ja
AWS::Redshift::Cluster	Ja	Ja
AWS::Redshift::ClusterParameterGruppe	Ja	Ja
AWS::Redshift::ClusterSecurityGruppe	Ja	Ja
AWS::Redshift::ClusterSnapshot	Ja	Ja
AWS::Redshift::ClusterSubnetGruppe	Ja	Ja

Ressourcentyp	AWS GovCloud (US-West)	AWS GovCloud (US-Ost)
AWS::Redshift::EventSubscription	Ja	Ja
AWS::Redshift::ScheduledAction	Ja	Ja
AWS::RoboMaker::RobotApplication	Ja	Nein
AWS::RoboMaker::RobotApplicationVersion	Ja	Nein
AWS::RoboMaker::SimulationApplication	Ja	Nein
AWS::Route53Profiles::Profile	Ja	Ja
AWS::Route53Resolver::FirewallDomainListe	Ja	Ja
AWS::Route53Resolver::FirewallRuleGruppe	Ja	Ja
AWS::Route53Resolver::FirewallRuleGroupAssociation	Ja	Ja
AWS::Route53Resolver::ResolverEndpoint	Ja	Ja
AWS::Route53Resolver::ResolverQueryLoggingConfig	Ja	Ja
AWS::Route53Resolver::Resol verQueryLoggingConfigAssociation	Ja	Ja

Ressourcentyp	AWS GovCloud (US-West)	AWS GovCloud (US-Ost)
AWS::Route53Resolver::ResolverRule	Ja	Ja
AWS::Route53Resolver::ResolverRuleVerband	Ja	Ja
AWS::S3::AccessPoint	Ja	Ja
AWS::S3::AccountPublicAccessBlock	Ja	Ja
AWS::S3::Bucket	Ja	Ja
AWS::SES::ConfigurationSet	Ja	Nein
AWS::SES::ContactList	Ja	Nein
AWS::SES::Template	Ja	Nein
AWS::SNS::Topic	Ja	Ja
AWS::SQS::Queue	Ja	Ja
AWS::SSM::AssociationCompliance	Ja	Ja
AWS::SSM::Document	Ja	Ja

Ressourcentyp	AWS GovCloud (US-West)	AWS GovCloud (US-Ost)
AWS::SSM::FileData	Ja	Ja
AWS::SSM::ManagedInstance-Bestand	Ja	Ja
AWS::SSM::PatchCompliance	Ja	Ja
AWS::SageMaker::Model	Ja	Nein
AWS::SageMaker::NotebookInstance	Ja	Nein
AWS::SageMaker::NotebookInstanceLifecycleConfig	Ja	Nein
AWS::SecretsManager::Secret	Ja	Ja
AWS::SecurityHub::Standard	Ja	Ja
AWS::ServiceCatalog::CloudFormationProdukt	Ja	Ja
AWS::ServiceCatalog::CloudFormationProvisionedProduct	Ja	Ja
AWS::ServiceCatalog::Portfolio	Ja	Ja
AWS::ServiceDiscovery::HttpNamespace	Ja	Ja

Ressourcentyp	AWS GovCloud (US-West)	AWS GovCloud (US-Ost)
AWS::ServiceDiscovery::Instance	Ja	Ja
AWS::ServiceDiscovery::Service	Ja	Ja
AWS::StepFunctions::StateMachine	Ja	Ja
AWS::Transfer::Agreement	Ja	Ja
AWS::Transfer::Certificate	Ja	Ja
AWS::Transfer::Connector	Ja	Ja
AWS::Transfer::Profile	Ja	Ja
AWS::Transfer::Workflow	Ja	Ja
AWS::WAFRegional::RateBasedRegel	Ja	Ja
AWS::WAFRegional::Rule	Ja	Ja
AWS::WAFRegional::RuleGroup	Ja	Ja
AWS::WAFRegional::WebACL	Ja	Ja

Ressourcentyp	AWS GovCloud (US-West)	AWS GovCloud (US-Ost)
AWS:WAFv2:: IPSet	Ja	Ja
AWS::WAFv2::ManagedRuleSatz	Ja	Ja
AWS::WAFv2::RegexPatternSatz	Ja	Ja
AWS::WAFv2::RuleGroup	Ja	Ja
AWS::WAFv2::WebACL	Ja	Ja
AWS::WorkSpaces::Workspace	Ja	Nein

AWS Ressourcen aufzeichnen mit AWS Config

AWS Config erkennt kontinuierlich, wenn unterstützte Ressourcentypen erstellt, geändert oder gelöscht werden. AWS Config zeichnet diese Ereignisse als Konfigurationselemente auf (CIs).

Sie können festlegen AWS Config , dass Konfigurationsänderungen für alle unterstützten Ressourcentypen oder nur für die unterstützten Ressourcentypen aufgezeichnet werden, die für Sie relevant sind. Eine Liste der unterstützten Ressourcentypen, die aufgezeichnet werden AWS Config können, finden Sie unterUnterstützte Ressourcentypen für AWS Config.

Themen

- Überlegungen
- Was sind die Unterschiede zwischen regionalen und globalen Ressourcen?
- AWS Config Regeln und globale Ressourcentypen
- Aufnahmefrequenz für AWS Config

- Nicht aufgezeichnete Ressourcen
- Ressourcen in der AWS Config Konsole aufzeichnen
- Ressourcen mit der AWS CLI aufzeichnen
- Ressourcen von der Aufzeichnung ausschließen mit AWS Config
- Die Aufzeichnung mit AWS Config dem vom Kunden verwalteten Konfigurationsrekorder beenden

Überlegungen

Hohe Anzahl von AWS Config Bewertungen

Möglicherweise stellen Sie in Ihrem ersten Monat, in dem Sie mit AWS Config aufgezeichnet haben, eine erhöhte Aktivität in Ihrem Konto im Vergleich zu den Folgemonaten fest. AWS Config Führt während des ersten Bootstrapping-Vorgangs Evaluierungen aller Ressourcen in Ihrem Konto durch, die Sie für AWS Config die Aufzeichnung ausgewählt haben.

Wenn Sie kurzlebige Workloads ausführen, können Sie aufgrund der Aufzeichnung von AWS Config Konfigurationsänderungen im Zusammenhang mit dem Erstellen und Löschen dieser temporären Ressourcen eine erhöhte Aktivität feststellen. Eine flüchtige Workload ist eine vorübergehende Nutzung von Computing-Ressourcen, die bei Bedarf geladen und ausgeführt werden. Beispiele hierfür sind Amazon Elastic Compute Cloud (Amazon EC2) Spot-Instances, Amazon EMR-Jobs und AWS Auto Scaling.

Wenn Sie die erhöhte Aktivität durch die Ausführung kurzlebiger Workloads vermeiden möchten, können Sie den vom Kunden verwalteten Konfigurationsrekorder so einrichten, dass diese Ressourcentypen von der Aufzeichnung ausgeschlossen werden, oder Sie können diese Arten von Workloads in einem separaten Konto ausführen, das AWS Config ausgeschaltet ist, um eine erhöhte Konfigurationsaufzeichnung und Regelauswertung zu vermeiden.

Verfügbarkeit in Regionen

Bevor Sie einen Ressourcentyp angeben, der nachverfolgt werden AWS Config soll, überprüfen Sie, ob der Ressourcentyp in der Region, in der AWS Sie ihn eingerichtet haben, unterstützt wird. AWS Config

Wenn ein Ressourcentyp AWS Config in mindestens einer Region unterstützt wird, können Sie die Aufzeichnung dieses Ressourcentyps in allen Regionen aktivieren, die von unterstützt werden AWS Config, auch wenn der angegebene Ressourcentyp in der AWS Region, in der Sie ihn eingerichtet haben, nicht unterstützt wird AWS Config.

Was sind die Unterschiede zwischen regionalen und globalen Ressourcen?

Regionale Ressourcen

Regionale Ressourcen sind mit einer Region verknüpft und können nur in der jeweiligen Region verwendet werden. Sie erstellen sie in einer bestimmten Region AWS-Region, und dann existieren sie in dieser Region. Um diese Ressourcen aufzurufen oder mit ihnen zu interagieren, müssen Sie Ihre Aktivitäten auf diese Region ausrichten. Um beispielsweise eine EC2 Amazon-Instance mit dem zu erstellen AWS Management Console, wählen Sie die aus AWS-Region, in der Sie die Instance erstellen möchten. Wenn Sie das AWS Command Line Interface (AWS CLI) verwenden, um die Instance zu erstellen, fügen Sie den `--region` Parameter hinzu. Sie verfügen AWS SDKs jeweils über einen eigenen, äquivalenten Mechanismus zur Angabe der Region, die von der Operation verwendet wird.

Es gibt mehrere Gründe für die Nutzung regionaler Ressourcen. Ein Grund besteht darin sicherzustellen, dass sich die Ressourcen und die Service-Endpunkte, über die Sie auf sie zugreifen, so nah wie möglich am Kunden befinden. Dies verbessert die Leistung, indem die Latenz minimiert wird. Ein weiterer Grund ist die Bereitstellung einer Isolationsgrenze. Auf diese Weise können Sie unabhängige Kopien von Ressourcen in mehreren Regionen erstellen, um die Last zu verteilen und die Skalierbarkeit zu verbessern. Gleichzeitig werden die Ressourcen voneinander isoliert, um die Verfügbarkeit zu verbessern.

Wenn Sie AWS-Region in der Konsole oder in einem AWS CLI Befehl eine andere angeben, können Sie die Ressourcen, die Sie in der vorherigen Region sehen konnten, nicht mehr sehen oder mit ihnen interagieren.

Wenn Sie den Amazon-Ressourcennamen (ARN) für eine regionale Ressource betrachten, wird die Region, die die Ressource enthält, als viertes Feld im ARN angegeben. Eine EC2 Amazon-Instance ist beispielsweise eine regionale Ressource. Im Folgenden finden Sie ein Beispiel für einen ARN für eine EC2 Amazon-Instance, die in der `us-east-1` Region existiert.

```
arn:aws:ec2:us-east-1:123456789012:instance/i-0a6f30921424d3eee
```

Globale Ressourcen

Bei einigen AWS Serviceressourcen handelt es sich um globale Ressourcen, was bedeutet, dass Sie die Ressource von überall aus verwenden können. Sie geben in der Konsole eines globalen Service keine AWS-Region an. Um auf eine globale Ressource zuzugreifen, geben Sie bei der

Verwendung der Service AWS CLI - und AWS SDK-Operationen keinen `--region` Parameter an.

Globale Ressourcen sind für Fälle konzipiert, in denen es entscheidend ist, dass jeweils nur eine Instance einer bestimmten Ressource vorhanden sein kann. In diesen Szenarien ist die Replikation oder Synchronisation zwischen Kopien in verschiedenen Regionen nicht ausreichend. Dass auf einen einzigen globalen Endpunkt zugegriffen werden muss und dadurch potenziell die Latenz erhöht wird, wird als akzeptabel angesehen, um sicherzustellen, dass alle Änderungen für die Nutzer der Ressource sofort sichtbar sind.

Beispielsweise sind globale Amazon-Aurora-Cluster (`AWS::RDS::GlobalCluster`) globale Ressourcen und daher nicht an eine Region gebunden. Das bedeutet, dass Sie einen globalen Cluster erstellen können, ohne sich auf einen regionalen Endpunkt verlassen zu müssen. Der Vorteil besteht darin, dass der Amazon Relational Database Service (Amazon RDS) selbst zwar nach Regionen organisiert ist, die spezifische Region, aus der ein globaler Cluster stammt, jedoch keinen Einfluss auf den globalen Cluster hat. Er erscheint als ein einzelner, kontinuierlicher globaler Cluster in allen Regionen.

Der Amazon-Ressourcenname (ARN) für eine globale Ressource enthält keine Region. Das vierte Feld ist leer, wie im folgenden Beispiel für einen ARN für einen globalen Cluster.

```
arn:aws:rds::123456789012:global-cluster:test-global-cluster
```

> **Important**
>
> Globale Ressourcentypen, die AWS Config nach Februar 2022 integriert wurden, werden nur in der Heimatregion des Dienstes für die kommerzielle Partition und AWS GovCloud (US-West) für die Partition aufgezeichnet. GovCloud Sie können die Konfigurationselemente (CIs) für diese neuen globalen Ressourcentypen nur in ihrer Heimatregion und AWS GovCloud (US-West) einsehen.
> Globale Ressourcentypen, die vor Februar 2022 eingeführt wurden (`AWS::IAM::Group`, `AWS::IAM::Policy`, `AWS::IAM::Role` und `AWS::IAM::User`) bleiben unverändert. Sie können die Aufzeichnung dieser globalen IAM-Ressourcen in allen Regionen aktivieren, in denen sie vor Februar 2022 unterstützt AWS Config wurde. Diese globalen IAM-Ressourcen können nicht in Regionen aufgezeichnet werden, die AWS Config nach Februar 2022 unterstützt werden.

Globale Ressourcentypen | IAM-Ressourcen

Die folgenden IAM-Ressourcentypen sind globale Ressourcen: IAM-Benutzer, -Gruppen und -Rollen sowie vom Kunden verwaltete Richtlinien. Diese Ressourcentypen können AWS Config in Regionen aufgezeichnet werden, in denen sie vor Februar 2022 verfügbar AWS Config waren. Diese Liste, in der Sie die globalen IAM-Ressourcentypen nicht aufzeichnen können, umfasst die folgenden Regionen: Asien-Pazifik (Hyderabad), Asien-Pazifik (Malaysia), Asien-Pazifik (Melbourne), Asien-Pazifik (Thailand), Kanada West (Calgary), Europa (Spanien), Europa (Zürich), Israel (Tel Aviv), Mexiko (Zentral) und Naher Osten (VAE).

Um doppelte Konfigurationselemente (CIs) zu vermeiden, sollten Sie erwägen, die globalen IAM-Ressourcentypen nur einmal in einer der unterstützten Regionen aufzuzeichnen. Dies kann Ihnen auch dabei helfen, unnötige Evaluierungen und API-Drosselungen zu vermeiden.

Globale Ressourcentypen | Nur Heimatregion

Globale Ressourcen für die folgenden Dienste werden nur AWS Config in der Heimatregion des globalen Ressourcentyps aufgezeichnet: Amazon Elastic Container Registry Public AWS Global Accelerator, Amazon Route 53 CloudFront, Amazon und AWS WAF. Für diese globalen Ressourcen kann dieselbe Instanz des Ressourcentyps in mehreren AWS Regionen verwendet werden, aber die Konfigurationselemente (CIs) werden nur in der Heimatregion für die kommerzielle Partition oder AWS GovCloud (US-West) für die AWS GovCloud (US) Partition aufgezeichnet.

Heimatregionen für globale Ressourcentypen

AWS Dienst	Ressourcentyp „Value“	Heimatregion
Amazon Elastic Container Registry Public	`AWS::ECR::PublicRepository`	Region USA Ost (Nord-Virginia)
AWS Global Accelerator	`AWS::GlobalAccelerator::Listener`	Region USA West (Oregon)
	`AWS::GlobalAccelerator::EndpointGroup`	Region USA West (Oregon)
	`AWS::GlobalAccelerator::Accelerator`	Region USA West (Oregon)

AWS Dienst	Ressourcentyp „Value“	Heimatregion
Amazon Route 53	`AWS::Route53::HostedZone`	Region USA Ost (Nord-Virginia)
	`AWS::Route53::HealthCheck`	Region USA Ost (Nord-Virginia)
Amazon CloudFront	`AWS::CloudFront::Distribution`	Region USA Ost (Nord-Virginia)
AWS WAF	`AWS::WAFv2::WebACL`	Region USA Ost (Nord-Virginia)

Globale Ressourcentypen | Globale Aurora-Cluster

`AWS::RDS::GlobalCluster`ist eine globale Ressource, die in allen unterstützten AWS Config Regionen aufgezeichnet wird, in denen der vom Kunden verwaltete Konfigurationsrekorder aktiviert ist. Dieser globale Ressourcentyp ist insofern einzigartig, als wenn Sie die Aufzeichnung dieser Ressource in einer Region aktivieren, Konfigurationselemente (CIs) für diesen Ressourcentyp in all Ihren aktivierten Regionen aufgezeichnet AWS Config werden.

Wenn `AWS::RDS::GlobalCluster` nicht in allen aktivierten Regionen aufzeichnen soll, verwenden Sie eine der folgenden Aufzeichnungsstrategien für die AWS Config -Konsole:

- Erfassen Sie alle Ressourcentypen mit anpassbaren Überschreibungen, wählen Sie GlobalCluster „AWS RDS“ und anschließend die Option „Von der Aufzeichnung ausschließen“
- zeichnen Sie bestimmte Ressourcentypen auf.

Wenn `AWS::RDS::GlobalCluster` nicht in allen aktivierten Regionen aufzeichnen soll, verwenden Sie eine der folgenden Aufzeichnungsstrategien für die API/CLI:

- Aufzeichnen aller aktuellen und zukünftigen Ressourcentypen mit Ausnahmen (`EXCLUSION_BY_RESOURCE_TYPES`)
- zeichnen Sie bestimmte Ressourcentypen auf (`INCLUSION_BY_RESOURCE_TYPES`).

AWS Config Regeln und globale Ressourcentypen

Die globalen IAM-Ressourcentypen, die vor Februar 2022 eingeführt wurden (`AWS::IAM::Group`,`AWS::IAM::Policy`, und`AWS::IAM::User`)`AWS::IAM::Role`, können nur AWS Config in Regionen erfasst werden, in denen sie vor Februar 2022 verfügbar AWS Config waren. Diese globalen IAM-Ressourcentypen können nicht in Regionen erfasst werden, die nach Februar 2022 unterstützt werden AWS Config . Eine Liste dieser Regionen finden Sie unter AWS Aufzeichnungsressourcen | Globale Ressourcen.

Wenn Sie einen globalen IAM-Ressourcentyp in mindestens einer Region aufzeichnen, führen periodische Regeln, die die Einhaltung des globalen IAM-Ressourcentyps melden, Bewertungen in allen Regionen durch, in denen die periodische Regel hinzugefügt wurde, auch wenn Sie die Aufzeichnung des globalen IAM-Ressourcentyps in der Region, in der die periodische Regel hinzugefügt wurde, nicht aktiviert haben.

Bewährte Verfahren für die Berichterstattung über die Einhaltung der Vorschriften bei globalen Ressourcen, die vor Februar 2022 eingeführt wurden

Um unnötige Evaluierungen zu vermeiden, sollten Sie AWS Config Regeln und Konformitätspakete, für die diese globalen Ressourcen gelten, nur für eine der unterstützten Regionen bereitstellen. Eine Liste der verwalteten Regeln, die in welchen Regionen unterstützt werden, finden Sie unter Liste der AWS Config verwalteten Regeln nach Verfügbarkeit in Regionen. Dies gilt für AWS Config Regeln, AWS Config Organisationsregeln und auch für Regeln, die von anderen AWS Diensten erstellt wurden, z. B. AWS Security Hub und AWS Control Tower.

Wenn Sie keine globalen Ressourcentypen aufzeichnen, die vor Februar 2022 eingeführt wurden, sollten Sie die folgenden regelmäßig wirkenden Regeln nicht aktivieren, um unnötige Kosten zu vermeiden:

- access-keys-rotated
- account-part-of-organizations
- iam-password-policy
- iam-policy-in-use
- iam-root-access-key-überprüfen
- iam-user-mfa-enabled
- iam-user-unused-credentials-überprüfen

- mfa-enabled-for-iam-Konsolenzugriff
- root-account-hardware-mfa-aktiviert
- root-account-mfa-enabled

Bewährte Verfahren für die Berichterstattung über die Einhaltung von Vorschriften in Bezug auf globale Ressourcen, die nach Februar 2022 eingeführt wurden

Globale Ressourcentypen, die nach Februar 2022 in die AWS Config Aufzeichnung integriert wurden, werden nur in der Heimatregion des Dienstes für die kommerzielle Partition und AWS GovCloud (US-West) für die Partition aufgezeichnet. AWS GovCloud (US) Sie sollten AWS Config Regeln und Konformitätspakete bereitstellen, bei denen diese globalen Ressourcen nur für die Heimatregion des Ressourcentyps gelten. Weitere Informationen finden Sie unter Heimatregionen für globale Ressourcentypen.

Aufnahmefrequenz für AWS Config

AWS Config unterstützt kontinuierliche Aufnahme und tägliche Aufnahme. Mit der kontinuierlichen Aufzeichnung können Sie Konfigurationsänderungen kontinuierlich aufzeichnen, wenn eine Änderung auftritt. Mit der täglichen Aufzeichnung können Sie nur dann ein Konfigurationselement (CI) erhalten, das den neuesten Status Ihrer Ressourcen in den letzten 24 Stunden darstellt, wenn es sich von dem zuvor aufgezeichneten CI unterscheidet. Anweisungen zum Ändern der Aufnahmefrequenz finden Sie unter Ändern der Aufnahmefrequenz.

Kontinuierliche Aufzeichnung

Die kontinuierliche Aufzeichnung bietet unter anderem folgende Vorteile:

- Überwachung in Echtzeit: Durch kontinuierliche Aufzeichnungen können unbefugte Änderungen oder unerwartete Änderungen sofort erkannt werden, wodurch Ihre Sicherheits- und Compliance-Bemühungen verbessert werden können.
- Detaillierte Analyse: Durch die kontinuierliche Aufzeichnung können Sie eingehende Analysen der Konfigurationsänderungen an Ihren Ressourcen durchführen, sobald sie auftreten, so dass Sie Muster und Trends sofort erkennen können.

Tägliche Aufzeichnung

Die tägliche Aufzeichnung bietet unter anderem folgende Vorteile:

- Minimale Unterbrechungen: Durch die tägliche Aufzeichnung erhalten Sie einen Informationsfluss, der sich besser handhaben lässt, wodurch die Häufigkeit von Benachrichtigungen und die Ermüdung durch zu häufige Warnmeldungen reduziert werden können.
- Kosteneffizienz: Die tägliche Aufzeichnung bietet Ihnen die Flexibilität, Änderungen an Ihren Ressourcen mit einer geringeren Frequenz aufzuzeichnen, wodurch die Kosten im Zusammenhang mit der Anzahl der aufgezeichneten Konfigurationsänderungen gesenkt werden können.

> **Note**
>
> AWS Firewall Manager hängt von der kontinuierlichen Aufzeichnung ab, um Ihre Ressourcen zu überwachen. Wenn Sie den Firewall Manager verwenden, wird empfohlen, die Aufzeichnungsfrequenz auf „Kontinuierlich“ einzustellen.

Nicht aufgezeichnete Ressourcen

Wenn eine Ressource nicht aufgezeichnet ist, AWS Config erfasst es nur die Erstellung und Löschung dieser Ressource und keine weiteren Details, ohne dass Ihnen dadurch Kosten entstehen. Wenn eine nicht aufgezeichnete Ressource erstellt oder gelöscht wird, AWS Config sendet eine Benachrichtigung und zeigt das Ereignis auf der Seite mit den Ressourcendetails an. Die Detailseite für eine nicht aufgezeichnete Ressource bietet Nullwerte für die meisten Konfigurationsdetails und keine Informationen zu Beziehungen und Konfigurationsänderungen.

Die Beziehungsinformationen, die für aufgezeichnete Ressourcen zur AWS Config Verfügung stehen, sind aufgrund fehlender Daten für nicht aufgezeichnete Ressourcen nicht eingeschränkt. Wenn eine aufgezeichnete Ressource mit einer nicht aufgezeichneten Ressource in Zusammenhang steht, wird diese Beziehung auf der Detailseite der aufgezeichneten Ressource bereitgestellt.

Überlegungen zum IAM-Ressourcentyp

Die `AWS::IAM::Role` Ressourcentypen `AWS::IAM::User` `AWS::IAM::Policy` `AWS::IAM::Group`,,, erfassen nur dann den Erstellungs- (`ResourceNotRecordedResourceDeletedNotRecorded`) und Löschstatus (), wenn die Ressource als Ressource für die Aufzeichnung im vom Kunden verwalteten Konfigurationsrekorder ausgewählt wurde oder zuvor ausgewählt wurde.

CI-Aufzeichnungsplan für nicht aufgezeichnete Ressourcen

Die Konfigurationselemente (CIs) für `ResourceNotRecorded` und `ResourceDeletedNotRecorded` außerhalb der typischen Aufzeichnungszeit für Ressourcentypen. Diese Ressourcentypen werden nur während des periodischen Baselining-Prozesses für den vom Kunden verwalteten Konfigurationsrekorder aufgezeichnet, der seltener erfolgt als bei den anderen Ressourcentypen. Das bedeutet, dass Erstellungs- und Löschbenachrichtigungen nicht bei der Erstellung oder Löschung, sondern während des Baselining-Prozesses gesendet werden.

CI-Lieferung und Umfang des servicebasierten Rekorders

Bei serviceverknüpften Konfigurationsrekordern bestimmt der Umfang der Aufzeichnung, ob Sie Konfigurationselemente (CIs) im Lieferkanal erhalten. Der Umfang der Aufzeichnung wird durch den Dienst festgelegt, der mit dem Konfigurationsrekorder verknüpft ist. Wenn der Umfang der Aufzeichnung intern ist, erhalten Sie keine Daten CIs im Bereitstellungskanal.

Ressourcen in der AWS Config Konsole aufzeichnen

Sie können die AWS Config Konsole verwenden, um die Ressourcentypen auszuwählen, die mit dem vom Kunden verwalteten Konfigurationsrekorder AWS Config aufgezeichnet werden.

So wählen Sie Ressourcen aus

1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die AWS Config Konsole zu https://console.aws.amazon.com/config/Hause.
2. Wählen Sie im linken Navigationsbereich Einstellungen aus.
3. Wählen Sie auf der Registerkarte Vom Kunden verwalteter Rekorder die Option Bearbeiten aus.
4. Wählen Sie im Abschnitt Aufzeichnungsverfahren eine Aufzeichnungsstrategie aus. Sie können die AWS Ressourcen angeben, die Sie aufzeichnen AWS Config möchten.

   All resource types with customizable overrides

   AWS Config So eingerichtet, dass Konfigurationsänderungen für alle aktuellen und future unterstützten Ressourcentypen in dieser Region aufgezeichnet werden. Sie können die Aufzeichnungsfrequenz für bestimmte Ressourcentypen außer Kraft setzen oder bestimmte Ressourcentypen von der Aufzeichnung ausschließen. Weitere Informationen finden Sie unter Unterstützte Ressourcentypen.

   - Standardeinstellungen

Konfigurieren Sie die Standardaufzeichnungsfrequenz für alle derzeit und zukünftig unterstützten Ressourcentypen. Weitere Informationen finden Sie unter Aufzeichnungsfrequenz.

- Kontinuierliche Aufzeichnung — AWS Config zeichnet Konfigurationsänderungen kontinuierlich auf, wenn eine Änderung auftritt.
- Tägliche Aufzeichnung – Sie erhalten ein Konfigurationselement (CI), das den aktuellen Status Ihrer Ressourcen in den letzten 24 Stunden nur dann darstellt, wenn es sich von dem zuvor aufgezeichneten CI unterscheidet.

> **Note**
>
> AWS Firewall Manager hängt von der kontinuierlichen Aufzeichnung ab, um Ihre Ressourcen zu überwachen. Wenn Sie den Firewall Manager verwenden, wird empfohlen, die Aufzeichnungsfrequenz auf „Kontinuierlich“ einzustellen.

- Überschreibungseinstellungen

  Setzen Sie die Aufzeichnungsfrequenz für bestimmte Ressourcentypen außer Kraft oder schließen Sie bestimmte Ressourcentypen von der Aufzeichnung aus. Wenn Sie die Aufzeichnungsfrequenz für einen Ressourcentyp ändern, bleiben die bereits aufgezeichneten Konfigurationselemente unverändert.

Specific resource types

Richten Sie AWS Config es so ein, dass Konfigurationsänderungen nur für die von Ihnen angegebenen Ressourcentypen aufgezeichnet werden.

- Bestimmte Ressourcentypen

  Wählen Sie einen Ressourcentyp und dessen Aufzeichnungsfrequenz aus. Weitere Informationen finden Sie unter Aufzeichnungsfrequenz.

  - Kontinuierliche Aufzeichnung — AWS Config zeichnet Konfigurationsänderungen kontinuierlich auf, wenn eine Änderung eintritt.
  - Tägliche Aufzeichnung – Sie erhalten ein Konfigurationselement (CI), das den aktuellen Status Ihrer Ressourcen in den letzten 24 Stunden nur dann darstellt, wenn es sich von dem zuvor aufgezeichneten CI unterscheidet.

> **Note**
>
> AWS Firewall Manager hängt von der kontinuierlichen Aufzeichnung ab, um Ihre Ressourcen zu überwachen. Wenn Sie den Firewall Manager verwenden, wird empfohlen, die Aufzeichnungsfrequenz auf „Kontinuierlich“ einzustellen.

Wenn Sie die Aufzeichnungsfrequenz für einen Ressourcentyp ändern, bleiben die bereits aufgezeichneten Konfigurationselemente unverändert.

5. Wählen Sie Speichern, um Ihre Änderungen zu speichern.

Überlegungen beim Aufzeichnen von Ressourcen

Hohe Anzahl von AWS Config Bewertungen

Möglicherweise stellen Sie in Ihrem ersten Monat, in dem Sie mit AWS Config aufgezeichnet haben, eine erhöhte Aktivität in Ihrem Konto im Vergleich zu den Folgemonaten fest. AWS Config Führt während des ersten Bootstrapping-Vorgangs Evaluierungen aller Ressourcen in Ihrem Konto durch, die Sie für AWS Config die Aufzeichnung ausgewählt haben.

Wenn Sie kurzlebige Workloads ausführen, können Sie aufgrund der Aufzeichnung von AWS Config Konfigurationsänderungen im Zusammenhang mit dem Erstellen und Löschen dieser temporären Ressourcen eine erhöhte Aktivität feststellen. Eine flüchtige Workload ist eine vorübergehende Nutzung von Computing-Ressourcen, die bei Bedarf geladen und ausgeführt werden. Beispiele hierfür sind Amazon Elastic Compute Cloud (Amazon EC2) Spot-Instances, Amazon EMR-Jobs und AWS Auto Scaling. Wenn Sie die erhöhte Aktivität durch die Ausführung kurzlebiger Workloads vermeiden möchten, können Sie den vom Kunden verwalteten Konfigurationsrekorder so einrichten, dass diese Ressourcentypen von der Aufzeichnung ausgeschlossen werden, oder Sie können diese Arten von Workloads in einem separaten Konto ausführen, das AWS Config ausgeschaltet ist, um eine erhöhte Konfigurationsaufzeichnung und Regelauswertung zu vermeiden.

Considerations: All resource types with customizable overrides

Global aufgezeichnete Ressourcentypen | Die globalen Aurora-Cluster sind zunächst in der Aufzeichnung enthalten

Der `AWS::RDS::GlobalCluster` Ressourcentyp wird in allen unterstützten AWS Config Regionen aufgezeichnet, in denen der vom Kunden verwaltete Konfigurationsrekorder aktiviert ist.

Wenn Sie `AWS::RDS::GlobalCluster` nicht in allen aktivierten Regionen aufzeichnen möchten, wählen Sie „AWS RDS GlobalCluster“ und dann die Option „Von der Aufzeichnung ausschließen“.

Globale Ressourcentypen | IAM-Ressourcentypen sind zunächst von der Aufzeichnung ausgeschlossen

Die globalen IAM-Ressourcentypen sind zunächst von der Aufzeichnung ausgeschlossen, um Ihnen zu helfen, die Kosten zu senken. Dieses Paket umfasst IAM-Benutzer, -Gruppen, -Rollen und vom Kunden verwaltete Richtlinien. Wählen Sie Entfernen, um die Überschreibung zu entfernen und diese Ressourcen in Ihre Aufzeichnung aufzunehmen.

Darüber hinaus können die globalen IAM-Ressourcentypen (`AWS::IAM::User`, `AWS::IAM::GroupAWS::IAM::Role`, und`AWS::IAM::Policy`) nicht in Regionen aufgezeichnet werden, die AWS Config nach Februar 2022 unterstützt werden. Eine Liste dieser Regionen finden Sie unter AWS Aufzeichnungsressourcen | Globale Ressourcen.

Beschränkungen

Sie können bis zu 100 Frequenzüberschreibungen und 600 Ausschlussüberschreibungen hinzufügen.

Die tägliche Aufzeichnung wird für die folgenden Ressourcentypen nicht unterstützt:

- `AWS::Config::ResourceCompliance`
- `AWS::Config::ConformancePackCompliance`
- `AWS::Config::ConfigurationRecorder`

Considerations: Specific resource types

Verfügbarkeit in Regionen

Bevor Sie einen Ressourcentyp angeben, der nachverfolgt werden AWS Config soll, überprüfen Sie, ob der Ressourcentyp in der AWS Region, in der Sie ihn eingerichtet haben, unterstützt wird AWS Config. Wenn ein Ressourcentyp AWS Config in mindestens einer Region unterstützt wird, können Sie die Aufzeichnung dieses Ressourcentyps in allen Regionen aktivieren, die von unterstützt werden AWS Config, auch wenn der angegebene Ressourcentyp in der AWS Region, in der Sie ihn eingerichtet haben, nicht unterstützt wird AWS Config.

Beschränkungen

Keine Beschränkungen, wenn alle Ressourcentypen dieselbe Frequenz haben. Sie können bis zu 100 Ressourcentypen mit täglicher Aufzeichnungsfrequenz hinzufügen, wenn mindestens ein Ressourcentyp auf „Kontinuierlich“ gesetzt ist.

Die tägliche Frequenz wird für die folgenden Ressourcentypen nicht unterstützt:

- `AWS::Config::ResourceCompliance`
- `AWS::Config::ConformancePackCompliance`
- `AWS::Config::ConfigurationRecorder`

Ressourcen mit der AWS CLI aufzeichnen

Sie können die AWS CLI verwenden, um die Ressourcentypen auszuwählen, die Sie aufzeichnen AWS Config möchten. Dazu erstellen Sie einen vom Kunden verwalteten Konfigurationsrekorder, der die Ressourcentypen aufzeichnet, die Sie in einer Aufzeichnungsgruppe angeben. In der Aufnahmegruppe legen Sie fest, ob Sie alle unterstützten Ressourcentypen aufzeichnen oder bestimmte Ressourcentypen ein- und ausschließen möchten.

Record all current and future supported resource types

AWS Config So eingerichtet, dass Konfigurationsänderungen für alle aktuellen und future unterstützten Ressourcentypen in dieser Region aufgezeichnet werden. Eine Liste der unterstützten Ressourcentypen finden Sie unter Unterstützte Ressourcentypen.

1. Verwenden Sie den -Befehl:`put-configuration-recorder`

   Dieser Befehl verwendet die `---recording-group` Felder `--configuration-recorder` und.

   ```
   $ aws configservice put-configuration-recorder \
   --configuration-recorder file://configurationRecorder.json \
   --recording-group file://recordingGroup.json
   ```

   Das **`configuration-recorder`** Feld

   Die `configurationRecorder.json` Datei spezifiziert `name` und `roleArn` auch die Standardaufzeichnungsfrequenz für den Konfigurationsrekorder (`recordingMode`).

   ```
   {
   ```

```
  "name": "default",
  "roleARN": "arn:aws:iam::123456789012:role/config-role",
  "recordingMode": {
    "recordingFrequency": CONTINUOUS or DAILY,
    "recordingModeOverrides": [
        {
            "description": "Description you provide for the override",
            "recordingFrequency": CONTINUOUS or DAILY,
            "resourceTypes": [ Comma-separated list of resource types to include
 in the override ]
        }
    ]
  }
}
```

Das **`recording-group`** Feld

Die `recordingGroup.json` Datei gibt an, welche Ressourcentypen aufgezeichnet werden.

```
{
    "allSupported": true,
    "recordingStrategy": {
        "useOnly": "ALL_SUPPORTED_RESOURCE_TYPES"
    },
    "includeGlobalResourceTypes": true
}
```

Weitere Informationen zu diesen Feldern finden Sie `put-configuration-recorder`in der AWS CLI Befehlsreferenz.

2. (Optional) Verwenden Sie den folgenden `describe-configuration-recorders`Befehl, um zu überprüfen, ob Ihr vom Kunden verwalteter Konfigurationsrekorder über die gewünschten Einstellungen verfügt.

```
$ aws configservice describe-configuration-recorders
```

Nachfolgend finden Sie eine Beispielantwort.

```
{
    "ConfigurationRecorders": [
        {
```

```
            "name": "default"
            "recordingGroup": {
                "allSupported": true,
                "exclusionByResourceTypes": {
                     "resourceTypes": []
                },
                "includeGlobalResourceTypes": true,
                "recordingStrategy": {
                    "useOnly": "ALL_SUPPORTED_RESOURCE_TYPES"
                },
                "resourceTypes": [],
            },
            "recordingMode": {
                "recordingFrequency": CONTINUOUS or DAILY,
                "recordingModeOverrides": [
                 {
                     "description": "Description you provide for the override,
                     "recordingFrequency": CONTINUOUS or DAILY,
                     "resourceTypes": [ Comma-separated list of resource types
 to include in the override]
                }
              ]
            },
            "roleARN": "arn:aws:iam::123456789012:role/config-role"
        }
    ]
}
```

Record all current and future supported resources types excluding the types you specify

AWS Config So eingerichtet, dass Konfigurationsänderungen für alle aktuellen und future unterstützten Ressourcentypen aufgezeichnet werden, einschließlich globaler Ressourcentypen, mit Ausnahme der Ressourcentypen, die Sie von der Aufzeichnung ausschließen möchten.

Wenn Sie die Aufzeichnung für einen Ressourcentyp beenden, bleiben die bereits aufgezeichneten Konfigurationselemente unverändert. Eine Liste der unterstützten Ressourcentypen finden Sie unter Unterstützte Ressourcentypen.

1. Verwenden Sie den -Befehl:`put-configuration-recorder`

   Dieser Befehl verwendet die `---recording-group` Felder `--configuration-recorder` und.

```
$ aws configservice put-configuration-recorder \
--configuration-recorder file://configurationRecorder.json \
--recording-group file://recordingGroup.json
```

Das **`configuration-recorder`** Feld

Die `configurationRecorder.json` Datei spezifiziert `name` und `roleArn` auch die Standardaufzeichnungsfrequenz für den Konfigurationsrekorder (`recordingMode`).

```
{
  "name": "default",
  "roleARN": "arn:aws:iam::123456789012:role/config-role",
  "recordingMode": {
    "recordingFrequency": CONTINUOUS or DAILY,
    "recordingModeOverrides": [
        {
            "description": "Description you provide for the override",
            "recordingFrequency": CONTINUOUS or DAILY,
            "resourceTypes": [ Comma-separated list of resource types to include
 in the override ]
        }
    ]
  }
}
```

Das **`recording-group`** Feld

Die `recordingGroup.json` Datei gibt an, welche Arten von Ressourcen aufgezeichnet AWS Config werden. Übergeben Sie einen oder mehrere auszuschließende Ressourcentypen im `resourceTypes` Feld von`exclusionByResourceTypes`, wie im folgenden Beispiel gezeigt.

```
{
    "allSupported": false,
    "exclusionByResourceTypes": {
        "resourceTypes": [
            "AWS::Redshift::ClusterSnapshot",
            "AWS::RDS::DBClusterSnapshot",
            "AWS::CloudFront::StreamingDistribution"
        ]
    },
```

```
    "includeGlobalResourceTypes": false,
    "recordingStrategy": {
        "useOnly": "EXCLUSION_BY_RESOURCE_TYPES"
     },

}
```

Weitere Informationen zu diesen Feldern finden Sie put-configuration-recorderin der AWS CLI Befehlsreferenz.

2. (Optional) Verwenden Sie den folgenden describe-configuration-recordersBefehl, um zu überprüfen, ob Ihr vom Kunden verwalteter Konfigurationsrekorder über die gewünschten Einstellungen verfügt.

```
$ aws configservice describe-configuration-recorders
```

Nachfolgend finden Sie eine Beispielantwort.

```
{
    "ConfigurationRecorders": [
        {
            "name": "default",
            "recordingGroup": {
                "allSupported": false,
                "exclusionByResourceTypes": {
                    "resourceTypes": [
                        "AWS::Redshift::ClusterSnapshot",
                        "AWS::RDS::DBClusterSnapshot",
                        "AWS::CloudFront::StreamingDistribution"
                    ]
                },
                "includeGlobalResourceTypes": false,
                "recordingStrategy": {
                    "useOnly": "EXCLUSION_BY_RESOURCE_TYPES"
                },
                "resourceTypes": [],
            },
            "recordingMode": {
                "recordingFrequency": CONTINUOUS or DAILY,
                "recordingModeOverrides": [
                 {
                     "description": "Description you provide for the override,
```

```
                    "recordingFrequency": CONTINUOUS or DAILY,
                    "resourceTypes": [ Comma-separated list of resource types to
 include in the override]
                }
              ]
            },
            "roleARN": "arn:aws:iam::123456789012:role/config-role"
        }
    ]
}
```

Record specific resource types

Richten Sie AWS Config es so ein, dass Konfigurationsänderungen nur für die von Ihnen angegebenen Ressourcentypen aufgezeichnet werden.

Wenn Sie die Aufzeichnung für einen Ressourcentyp beenden, bleiben die bereits aufgezeichneten Konfigurationselemente unverändert. Eine Liste der unterstützten Ressourcentypen finden Sie unter Unterstützte Ressourcentypen.

1. Verwenden Sie den -Befehl:`put-configuration-recorder`

   Dieser Befehl verwendet die `---recording-group` Felder `--configuration-recorder` und.

   ```
   $ aws configservice put-configuration-recorder \
   --configuration-recorder file://configurationRecorder.json \
   --recording-group file://recordingGroup.json
   ```

   Das **`configuration-recorder`** Feld

   Die `configurationRecorder.json` Datei spezifiziert `name` und `roleArn` auch die Standardaufzeichnungsfrequenz für den Konfigurationsrekorder (`recordingMode`).

   ```
   {
     "name": "default",
     "roleARN": "arn:aws:iam::123456789012:role/config-role",
     "recordingMode": {
       "recordingFrequency": CONTINUOUS or DAILY,
       "recordingModeOverrides": [
           {
   ```

```
            "description": "Description you provide for the override",
            "recordingFrequency": CONTINUOUS or DAILY,
            "resourceTypes": [ Comma-separated list of resource types to include
 in the override ]
        }
    ]
  }
}
```

Das **`recording-group`** Feld

Die `recordingGroup.json` Datei gibt an, welche Arten von Ressourcen aufgezeichnet AWS Config werden. Übergeben Sie einen oder mehrere auszuschließende Ressourcentypen in das `resourceTypes` Feld, wie im folgenden Beispiel gezeigt.

```
{
    "allSupported": false,
    "recordingStrategy": {
        "useOnly": "INCLUSION_BY_RESOURCE_TYPES"
    },
    "includeGlobalResourceTypes": false,
    "resourceTypes": [
        "AWS::EC2::EIP",
        "AWS::EC2::Instance",
        "AWS::EC2::NetworkAcl",
        "AWS::EC2::SecurityGroup",
        "AWS::CloudTrail::Trail",
        "AWS::EC2::Volume",
        "AWS::EC2::VPC",
        "AWS::IAM::User",
        "AWS::IAM::Policy"
  ]
}
```

Weitere Informationen zu diesen Feldern finden Sie `put-configuration-recorder`in der AWS CLI Befehlsreferenz.

2. (Optional) Verwenden Sie den folgenden `describe-configuration-recorders`Befehl, um zu überprüfen, ob Ihr vom Kunden verwalteter Konfigurationsrekorder über die gewünschten Einstellungen verfügt.

```
$ aws configservice describe-configuration-recorders
```

Nachfolgend finden Sie eine Beispielantwort.

```
{
    "ConfigurationRecorders": [
        {
            "name": "default",
            "recordingGroup": {
                "allSupported": false,
                "exclusionByResourceTypes": {
                    "resourceTypes": []
                },
                "includeGlobalResourceTypes": false
                "recordingStrategy": {
                    "useOnly": "INCLUSION_BY_RESOURCE_TYPES"
                },
                "resourceTypes": [
                    "AWS::EC2::EIP",
                    "AWS::EC2::Instance",
                    "AWS::EC2::NetworkAcl",
                    "AWS::EC2::SecurityGroup",
                    "AWS::CloudTrail::Trail",
                    "AWS::EC2::Volume",
                    "AWS::EC2::VPC",
                    "AWS::IAM::User",
                    "AWS::IAM::Policy"
                ]
            },
            "recordingMode": {
                "recordingFrequency": CONTINUOUS or DAILY,
                "recordingModeOverrides": [
                 {
                     "description": "Description you provide for the override,
                     "recordingFrequency": CONTINUOUS or DAILY,
                     "resourceTypes": [ Comma-separated list of resource types to
 include in the override]
                }
              ]
            },
            "roleARN": "arn:aws:iam::123456789012:role/config-role"
        }
```

```
    ]
}
```

Ressourcen von der Aufzeichnung ausschließen mit AWS Config

AWS Config ermöglicht es Ihnen, bestimmte AWS Ressourcentypen von der Inventarverfolgung und Konformitätsüberwachung auszuschließen und gleichzeitig alle anderen unterstützten Ressourcentypen zu verfolgen AWS Config, die derzeit verfügbar sind, einschließlich derer, die in future hinzugefügt werden. Mit dieser Funktion können Sie sich auf wichtige Ressourcen konzentrieren, die Ihren Compliance- und Governance-Standards unterliegen.

Excluding resources (Console)

Wenn Sie einen AWS Ressourcentyp nicht aufzeichnen möchten, verwenden Sie eine der folgenden Aufzeichnungsstrategien für die AWS Config Konsole:

- Zeichnen Sie alle Ressourcentypen mit anpassbaren Überschreibungen auf, wählen Sie den Ressourcentyp aus, den Sie ausschließen möchten, und wählen Sie die Überschreibung „Von der Aufzeichnung ausschließen“
- zeichnen Sie bestimmte Ressourcentypen auf.

Ausführlichere Schritte finden Sie unter Ressourcen aufzeichnen (Konsole).

Excluding resources (AWS CLI)

Wenn Sie keinen AWS Ressourcentyp aufzeichnen möchten, verwenden Sie eine der folgenden Aufzeichnungsstrategien für die API/CLI:

- Aufzeichnen aller aktuellen und zukünftigen Ressourcentypen mit Ausnahmen (`EXCLUSION_BY_RESOURCE_TYPES`)
- zeichnen Sie bestimmte Ressourcentypen auf (`INCLUSION_BY_RESOURCE_TYPES`).

Ausführlichere Schritte finden Sie unter Ressourcen aufzeichnen ()AWS CLI.

Die Aufzeichnung mit AWS Config dem vom Kunden verwalteten Konfigurationsrekorder beenden

Sie können die Aufzeichnung mit dem AWS Config vom Kunden verwalteten Konfigurationsrekorder jederzeit beenden. Nach AWS Config dem Beenden der Aufzeichnung einer Ressource werden die zuvor erfassten Konfigurationsinformationen beibehalten, und Sie können weiterhin auf diese Informationen zugreifen.

Anweisungen zum Beenden der Aufzeichnung finden Sie unter Stoppen des vom Kunden verwalteten Konfigurationsrekorders.

Aufzeichnen von Konfigurationen mit AWS Config für Ressourcen von Drittanbietern mithilfe des AWS CLI

Zeichnen Sie Konfigurationen für Ressourcen von Drittanbietern oder benutzerdefinierte Ressourcentypen wie lokale Server, SAAS-Überwachungstools und Versionskontrollsysteme (wie GitHub) auf.

Sie können die Konfigurationsdaten von Drittanbieterressourcen in AWS Config der Konsole veröffentlichen und den Ressourcenbestand und den Konfigurationsverlauf mithilfe der AWS Config Konsole und anzeigen und überwachen APIs. Sie können sie verwenden AWS Config , um all Ihre Ressourcen zu verwalten und anhand von AWS Config Regeln die Ressourcenkonfiguration anhand bewährter Verfahren auf ihre Einhaltung hin zu überprüfen. Sie können auch AWS Config Regeln oder Konformitätspakete erstellen, um diese Ressourcen von Drittanbietern anhand von Best Practices, internen Richtlinien und behördlichen Richtlinien zu bewerten.

> **Note**
>
> Wenn Sie so konfiguriert AWS Config haben, dass alle Ressourcentypen aufgezeichnet werden, werden Ressourcen von Drittanbietern, die über verwaltet (erstellt, aktualisiert oder gelöscht) AWS CloudFormation werden, automatisch AWS Config als Konfigurationselemente protokolliert.

Voraussetzung: Die Drittanbieterressourcen oder der benutzerdefinierte Ressourcentyp müssen mit registriert werden AWS CloudFormation.

Themen

- Ressourcen von Drittanbietern hinzufügen zu AWS Config
- Erfassen Sie Konfigurationselemente AWS Config für Ressourcen von Drittanbietern mithilfe des AWS CLI
- Lesen Sie Konfigurationselemente mit AWS Config für Ressourcen von Drittanbietern mithilfe der AWS CLI
- Löschen Sie Ressourcen von Drittanbietern aus der AWS Config Verwendung von AWS CLI

Ressourcen von Drittanbietern hinzufügen zu AWS Config

Gehen Sie wie folgt vor, um eine Drittanbieter-Ressource hinzuzufügen AWS Config.

Themen

- Schritt 1: Einrichten Ihrer Entwicklungsumgebung
- Schritt 2: Modellieren Ihrer Ressource
- Schritt 3: Generieren von Artefakten
- Schritt 4: Registrieren Ihrer Ressource
- Schritt 5: Veröffentlichen der Ressourcenkonfiguration

Schritt 1: Einrichten Ihrer Entwicklungsumgebung

Installieren und Konfigurieren der AWS CloudFormation AWS CLI. Das AWS CLI ermöglicht Ihnen, Ihre benutzerdefinierten Ressourcen zu modellieren und zu registrieren. Weitere Informationen finden Sie unter Benutzerdefinierte Ressourcen und Was ist die CloudFormation Befehlszeilenschnittstelle? .

Schritt 2: Modellieren Ihrer Ressource

Erstellen Sie ein Ressourcenanbieterschema, das der Konfiguration des Ressourcentyps entspricht und diese validiert.

1. Verwenden Sie den Befehl `init`, um Ihr Ressourcenanbieterprojekt zu erstellen und die erforderlichen Dateien zu generieren.

```
$ cfn init
```

```
Initializing new project
```

2. Mit dem Befehl `init` wird ein Assistent gestartet, der Sie durch die Einrichtung des Projekts einschließlich der Angabe des Ressourcennamens führt. Geben Sie für dieses Walkthrough `MyCustomNamespace::Testing::WordPress` an.

```
Enter resource type identifier (Organization::Service::Resource):
 MyCustomNamespace::Testing::WordPress
```

3. Geben Sie einen Paketnamen für Ihre Ressource ein.

```
Enter a package name (empty for default 'com.custom.testing.wordpress'):
 com.custom.testing.wordpress
Initialized a new project in /workplace/user/custom-testing-wordpress
```

> **Note**
>
> Um sicherzustellen, dass alle Projektabhängigkeiten korrekt aufgelöst werden, können Sie das generierte Projekt in Ihre IDE mit Maven-Unterstützung importieren.
> Wenn Sie beispielsweise IntelliJ IDEA verwenden möchten, müssen Sie folgendermaßen vorgehen:
>
> - Wählen Sie im Menü Datei die Option Neu und dann Projekt von vorhandenen Quellen aus.
> - Navigieren Sie zum Projektverzeichnis.
> - Wählen Sie im Dialogfeld Projekt importieren die Option Projekt aus externem Modell importieren und dann Maven aus.
> - Gehen Sie auf Weiter und akzeptieren Sie alle Standardeinstellungen, um den Import des Projekts abzuschließen.

4. Öffnen Sie die Datei `mycustomnamespace-testing-wordpress.json`, die das Schema für Ihre Ressource enthält. Kopieren Sie das folgende Schema und fügen Sie es in `mycustomnamespace-testing-wordpress.json` ein.

```
{
  "typeName": "MyCustomNamespace::Testing::WordPress",
  "description": "An example resource that creates a website based on WordPress
 5.2.2.",
  "properties": {
```

```
    "Name": {
      "description": "A name associated with the website.",
      "type": "string",
      "pattern": "^[a-zA-Z0-9]{1,219}\\Z",
      "minLength": 1, "maxLength": 219
    },
    "SubnetId": {
      "description": "A subnet in which to host the website.",
      "pattern": "^(subnet-[a-f0-9]{13})|(subnet-[a-f0-9]{8})\\Z",
      "type": "string"
    },
    "InstanceId": {
      "description": "The ID of the instance that backs the WordPress site.",
      "type": "string"
    },
    "PublicIp": {
      "description": "The public IP for the WordPress site.",
      "type": "string"
    }
  },
  "required": [ "Name", "SubnetId" ],
  "primaryIdentifier": [ "/properties/PublicIp", "/properties/InstanceId" ],
  "readOnlyProperties": [ "/properties/PublicIp", "/properties/InstanceId" ],
  "additionalProperties": false
}
```

5. Validieren Sie das Schema.

```
$ cfn validate
```

6. Aktualisieren Sie die automatisch generierten Dateien im Ressourcenanbieterpaket, um die Aktualisierungen im Ressourcenanbieterschema anzuzeigen. Bei der Initiierung des Resource Provider-Projekts AWS CLI generiert der unterstützende Dateien und Code für den Resource Provider. Generieren Sie den Code neu, um das aktualisierte Schema anzuzeigen.

```
$ cfn generate
```

> **Note**
>
> Wenn Sie Maven verwenden, wird der Befehl `generate` als Teil des Build-Prozesses automatisch ausgeführt, bevor der Code kompiliert wird. Ihre Änderungen werden also immer mit dem generierten Code synchronisiert.

Beachten Sie, dass sich die CloudFormation CLI an einem Ort befinden muss, den Maven/das System finden kann. Weitere Informationen finden Sie unter Einrichten Ihrer Umgebung für die Entwicklung von Erweiterungen.

Weitere Informationen finden Sie unter Modellieren von Ressourcenanbietern zur Verwendung in AWS CloudFormation.

Schritt 3: Generieren von Artefakten

Führen Sie den folgenden Befehl aus, um Artefakte für `cfn submit` zu erstellen.

```
$ mvn package
```

Schritt 4: Registrieren Ihrer Ressource

AWS Config benötigt keine Ressourcenanbieter-Handler, um die Konfigurationsverfolgung für Ihre Ressource durchzuführen. Führen Sie den folgenden Befehl aus, um Ihre Ressource zu registrieren.

```
$ cfn submit
```

Weitere Informationen finden Sie unter Registrieren von Ressourcenanbietern für die Verwendung in AWS CloudFormation Vorlagen.

Schritt 5: Veröffentlichen der Ressourcenkonfiguration

Ermitteln Sie die Konfiguration für MyCustomNamespace: :Testing::WordPress.

```
{
  "Name": "MyWordPressSite",
  "SubnetId": "subnet-abcd0123",
  "InstanceId": "i-01234567",
  "PublicIp": "my-wordpress-site.com"
}
```

Ermitteln Sie die Schemaversions-ID von AWS CloudFormation `DescribeType`.

In können Sie sehen AWS Config, ob diese Ressourcenkonfiguration akzeptiert wurde. Um die Einhaltung der Vorschriften zu bewerten, können Sie mithilfe dieser Ressource AWS Config Regeln schreiben.

(Optional) Um die Aufzeichnung der Konfiguration zu automatisieren, sollten Sie regelmäßige oder auf Änderungen basierende Konfigurationssammler implementieren.

Erfassen Sie Konfigurationselemente AWS Config für Ressourcen von Drittanbietern mithilfe des AWS CLI

Zeichnen Sie über das folgende Verfahren ein Konfigurationselement für eine Drittanbieterressource oder einen benutzerdefinierten Ressourcentyp auf:

Stellen Sie sicher, dass Sie den Ressourcentyp `MyCustomNamespace::Testing::WordPress` mit dem entsprechenden Schema registrieren.

1. Öffnen Sie eine Eingabeaufforderung oder ein Terminal-Fenster.
2. Geben Sie den folgenden Befehl ein:

```
aws configservice put-resource-config --resource-type
 MyCustomNamespace::Testing::WordPress --resource-id resource-001 --schema-version-
id 00000001 --configuration  '{
  "Id": "resource-001",
  "Name": "My example custom resource.",
  "PublicAccess": false
}'
```

> **Note**
>
> `writeOnlyProperties`Wird wie im Typschema definiert aus der Konfiguration entfernt, bevor es von aufgezeichnet wird AWS Config. Das bedeutet, dass diese Werte nicht vorhanden sind, wenn die Konfiguration durch Lesen abgerufen wird APIs. Weitere Informationen zu `writeOnlyProperties` finden Sie unter Ressourcentypschema.

Lesen Sie Konfigurationselemente mit AWS Config für Ressourcen von Drittanbietern mithilfe der AWS CLI

Lesen Sie mithilfe des folgenden Verfahrens ein Konfigurationselement für eine Drittanbieterressource oder einen benutzerdefinierten Ressourcentyp:

1. Öffnen Sie eine Eingabeaufforderung oder ein Terminal-Fenster.

2. Geben Sie den folgenden Befehl ein:

```
aws configservice list-discovered-resources --resource-type
 MyCustomNamespace::Testing::WordPress
```

3. Drücken Sie die Eingabetaste.

   Die Ausgabe sollte folgendermaßen oder ähnlich aussehen:

```
{
    "resourceIdentifiers": [
        {
            "resourceType": "MyCustomNamespace::Testing::WordPress",
            "resourceId": "resource-001"
        }
    ]
}
```

4. Geben Sie den folgenden Befehl ein:

```
aws configservice batch-get-resource-config --resource-keys '[ { "resourceType":
 "MyCustomNamespace::Testing::WordPress", "resourceId": "resource-001" } ]'
```

5. Drücken Sie die Eingabetaste.

   Die Ausgabe sollte folgendermaßen oder ähnlich aussehen:

```
{
    "unprocessedResourceKeys": [],
    "baseConfigurationItems": [
        {
            "configurationItemCaptureTime": 1569605832.673,
            "resourceType": "MyCustomNamespace::Testing::WordPress",
            "resourceId": "resource-001",
            "configurationStateId": "1569605832673",
            "awsRegion": "us-west-2",
            "version": "1.3",
            "supplementaryConfiguration": {},
            "configuration": "{\"Id\":\"resource-001\",\"Name\":\"My example custom
 resource.\",\"PublicAccess\":false}",
            "configurationItemStatus": "ResourceDiscovered",
            "accountId": "AccountId"
```

```
        }
    ]
}
```

Löschen Sie Ressourcen von Drittanbietern aus der AWS Config Verwendung von AWS CLI

Geben Sie den folgenden Befehl ein, um eine Drittanbieter-Ressource zu löschen:

```
aws configservice delete-resource-config --resource-type
 MyCustomNamespace::Testing::WordPress --resource-id resource-002
```

Bei einer erfolgreichen Befehlsausführung gibt es keine weitere Ausgabe.

Aufzeichnen der Softwarekonfiguration für verwaltete Instanzen mit AWS Config

Sie können AWS Config es verwenden, um Änderungen des Softwareinventars auf EC2 Amazon-Instances und lokalen Servern aufzuzeichnen. Auf diese Weise können Sie die historischen Änderungen an der Softwarekonfiguration anzeigen. Wenn beispielsweise ein neues Windows-Update auf einer verwalteten Windows-Instance installiert ist, AWS Config zeichnet es die Änderungen auf und sendet die Änderungen dann an Ihren Bereitstellungskanal, sodass Sie über die Änderung informiert werden. Mit können Sie den Verlauf anzeigen AWS Config, wann Windows-Updates für die verwaltete Instanz installiert wurden und wie sie sich im Laufe der Zeit geändert haben.

Themen

- Voraussetzungen
- Softwarekonfigurationen aufzeichnen

Voraussetzungen

Sie müssen folgende Schritte ausführen, um Software-Konfigurationsänderungen aufzuzeichnen:

- Die Aufzeichnung des Ressourcentyps des verwalteten Instance-Bestands in AWS Config aktivieren.
- Konfigurieren Sie EC2 lokale Server als verwaltete Instanzen in AWS Systems Manager. Eine verwaltete Instance ist eine Maschine, die für die Verwendung mit Systems Manager konfiguriert wurde.
- Sie können das Erfassen des Softwarebestands über Ihre verwaltete Instance mit der Funktion „AWS Systems Manager Inventory“ initiieren.

> **Note**
>
> Systems Manager unterstützt jetzt das Erstellen von Konfigurationselementen für nicht verwaltete Instances
> Das Konfigurationselement für nicht verwaltete Instances wird zusätzlich mit `Key: “InstanceStatus”` und `Value: “Unmanaged”` konfiguriert.
> Konfigurationselemente für nicht verwaltete Instances werden nicht zusätzlich aktualisiert
> Um zusätzliche Updates zu erhalten, muss es sich bei dem Konfigurationselement um eine verwaltete Instanz handeln.

Sie können AWS Config Regeln auch verwenden, um Änderungen an der Softwarekonfiguration zu überwachen und sich darüber informieren zu lassen, ob die Änderungen Ihren Regeln entsprechen oder nicht. Wenn Sie beispielsweise eine Regel erstellen, die prüft, ob Ihre verwalteten Instances über eine bestimmte Anwendung verfügen, und die Anwendung bei einer Instance nicht installiert ist, wird diese Instanz von AWS Config als nicht regelkonform gekennzeichnet. Eine Liste der AWS Config verwalteten Regeln finden Sie unterListe der AWS Config verwalteten Regeln.

Softwarekonfigurationen aufzeichnen

So aktivieren Sie die Aufzeichnung von Software-Konfigurationsänderungen in AWS Config:

1. Aktivieren Sie die Aufzeichnung aller unterstützten Ressourcentypen oder zeichnen Sie selektiv den Ressourcentyp für den verwaltete Instance-Bestand in AWS Config auf. Weitere Informationen finden Sie unter AWS Ressourcen aufzeichnen mit AWS Config.
2. Starten Sie eine EC2 Amazon-Instance mit einem Instance-Profil für Systems Manager, das die von Amazon SSMManaged InstanceCore verwaltete Richtlinie enthält. Diese AWS verwaltete Richtlinie ermöglicht einer Instance, Systems Manager-Service-Kernfunktionalität zu verwenden.

Weitere Informationen zu anderen Richtlinien, die Sie dem Instance-Profil für Systems Manager hinzufügen können, finden Sie im Artikel zum Erstellen eines IAM-Instance-Profils für Systems Manager im AWS Systems Manager -Benutzerhandbuch.

> **Important**
>
> Beim SSM-Agent handelt es sich um eine Amazon-Software, die auf einer verwalteten Instance installiert werden muss, um mit Systems Manager in der Cloud kommunizieren zu können. Wenn Ihre EC2 Instance aus einem AMI für eines der folgenden Betriebssysteme erstellt wurde, ist der Agent vorinstalliert:
>
> - Windows Server 2003-2012 R2 wurde im November AMIs 2016 oder später veröffentlicht
> - Windows Server 2016 und 2019 R2
> - Amazon Linux
> - Amazon Linux 2
> - Ubuntu Server
> - Ubuntu Server
>
> Auf EC2 Instances, die nicht über ein AMI mit vorinstalliertem Agent erstellt wurden, müssen Sie den Agenten manuell installieren. Weitere Informationen finden Sie in folgenden Themen im AWS Systems Manager -Benutzerhandbuch:
>
> - Installation und Konfiguration des SSM-Agenten auf EC2 Instanzen für Windows Server
> - Installation und Konfiguration des SSM-Agenten auf EC2 Instanzen für Linux

3. Starten Sie die Bestandserfassung wie unter Konfigurieren der Bestandserfassung im AWS Systems Manager -Benutzerhandbuch beschrieben. Die Vorgehensweisen sind bei Linux- und Windows-Instances gleich.

   AWS Config kann Konfigurationsänderungen für die folgenden Inventartypen aufzeichnen:

   - Anwendungen: Eine Liste der Anwendungen für verwaltete Instances wie Antivirensoftware.
   - AWS Komponenten — Eine Liste von AWS Komponenten für verwaltete Instanzen, wie z. B. AWS CLI und SDKs.

- Instance-Informationen: Instance-Informationen wie Betriebssystemname und -version, Domain- und Firewall-Status.
- Netzwerkkonfiguration: Konfigurationsinformationen wie IP-Adresse, Gateway und Subnetzmaske.
- Windows Updates: Eine Liste der Windows-Updates für verwaltete Instances (nur Windows-Instances).

> **Note**
>
> AWS Config unterstützt derzeit nicht die Aufzeichnung des benutzerdefinierten Inventartyps.

Die Bestandserfassung ist eine der vielen Systems-Manager-Funktionen, die in die Kategorien Betriebsverwaltung, Aktionen und Änderungen, Instances und Knoten und Gemeinsame Ressourcen unterteilt sind. Weitere Informationen finden Sie unter Was ist AWS Systems Manager? und Systems Manager-Funktionen im AWS Systems Manager -Benutzerhandbuch.

Suchen nach Ressourcen, die entdeckt wurden von AWS Config

Sie können die AWS Config Konsole und die AWS Config API verwenden AWS CLI, um nach Ressourcen zu suchen, AWS Config die inventarisiert oder entdeckt wurden, einschließlich gelöschter Ressourcen und Ressourcen, die AWS Config derzeit nicht aufgezeichnet werden. AWS Config erkennt nur unterstützte Ressourcentypen. Weitere Informationen finden Sie unter Unterstützte Ressourcentypen für AWS Config.

Looking Up Resources (Console)

Sie können Ressourcentypen oder Tag-Informationen zum Nachschlagen von Ressourcen in der AWS Config -Konsole verwenden.

1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die AWS Config Konsole zu https://console.aws.amazon.com/config/Hause.
2. Geben Sie auf der Seite Ressourcenbestand die Suchoptionen für die Ressourcen an, die Sie nachschlagen möchten:

- Ressourcenkategorie — Wählen Sie alle Ressourcenkategorien aus oder schränken Sie die Ergebnisse auf AWS Ressourcen ein.
- Ressourcentyp: Wählen Sie alle Ressourcentypen aus oder legen Sie fest, nach welchen Ressourcen gefiltert werden soll.
- Compliance: Wählen Sie aus, ob Sie nach einem beliebigen Compliance-Status, konformen oder nicht konformen Elementen filtern möchten.

3. AWS Config listet die Ressourcen auf, die Ihren Suchoptionen entsprechen. Es werden folgenden Informationen zu den Ressourcen angezeigt:

   - Ressourcen-ID: Bei der Ressourcen-ID kann es sich um eine Ressourcen-ID oder einen Ressourcennamen handeln (sofern zutreffend). Wählen Sie den Link für die Ressourcen-ID aus, um die Detailseite für die Ressource anzuzeigen.
   - Ressourcentyp: Der Typ der Ressource wird angegeben.
   - Konformität — Der Status der Ressource, die AWS Config anhand Ihrer Regel bewertet wurde.

Looking Up Resources (AWS CLI)

Sie können den verwenden AWS CLI , um Ressourcen aufzulisten, die entdeckt AWS Config wurden.

Verwenden Sie den AWS Config service **`list-discovered-resources`**-Befehl:

```
$ aws configservice list-discovered-resources --resource-type "AWS::EC2::Instance"
        {
            "resourceIdentifiers": [
                {
                    "resourceType": "AWS::EC2::Instance",
                    "resourceId": "i-nnnnnnnn"
                }
            ]
        }
```

Sie können die in der Antwort aufgeführten Konfigurationsdetails einer Ressource mit dem Befehl „`get-resource-config-history`“ unter Angabe des Ressourcentyps und der -ID anzeigen Ein Beispiel für diesen Befehl und die Antwort von AWS Config finden Sie unterAnzeigen des Konfigurationsverlaufs.

Looking up Resources (API)

Sie geben einen Ressourcentyp an und geben eine Liste mit Ressourcen-IDs für Ressourcen dieses Typs AWS Config zurück. Weitere Informationen finden Sie unter ResourceIdentifier in der AWS Config -API-Referenz.

Verwenden Sie die Aktion „ListDiscoveredResources“.

Sie können die in der Antwort aufgeführten Konfigurationsdetails einer Ressource mit der Aktion „GetResourceConfigHistory“ unter Angabe des Ressourcentyps und der -ID abrufen.

Compliance-Informationen und Bewertungsergebnisse für Ihre AWS Ressourcen anzeigen mit AWS Config

> **Important**
>
> Für eine genaue Berichterstattung über den Compliance-Status müssen Sie den Ressourcentyp `AWS::Config::ResourceCompliance` aufzeichnen. Weitere Informationen finden Sie unter AWS Ressourcen aufzeichnen.

Sie können die AWS Config Konsole verwenden oder AWS SDKs um die Compliance-Informationen und die Evaluierungsergebnisse Ihrer Ressourcen einzusehen.

Themen

- Anzeigen der Compliance (Konsole)
- Konformität anzeigen (AWS SDKs)

Anzeigen der Compliance (Konsole)

Um die Einhaltung der Vorschriften einzusehen (Konsole)

1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die AWS Config Konsole zu https://console.aws.amazon.com/config/Hause.
2. Vergewissern Sie sich im AWS Management Console Menü, dass die Regionsauswahl auf eine Region eingestellt ist, die AWS Config Regeln unterstützt. Die Liste der unterstützten Regionen

finden Sie unter AWS Config -Regionen und -Endpunkte im Allgemeine Amazon Web Services-Referenz.

3. Wählen Sie im Navigationsbereich Resources aus. Auf der Seite „Ressourcenbestand“ können Sie nach Ressourcenkategorie, Ressourcentyp und Compliance-Status filtern. Wählen Sie gegebenenfalls Gelöschte Ressourcen einschließen aus. In der Tabelle werden die Ressourcen-ID für den Ressourcentyp und der Ressourcen-Compliance-Status für diese Ressource angezeigt. Bei der Ressourcen-ID kann es sich um eine Ressourcen-ID oder einen Ressourcennamen handeln.
4. Wählen Sie eine Ressource aus der Spalte mit Ressourcen-IDs aus.
5. Wählen Sie die Schaltfläche Ressourcen-Zeitachse aus. Sie können nach Konfigurationsereignissen, Konformitätsereignissen oder CloudTrail Ereignissen filtern.

> **Note**
>
> Alternativ können Sie auf der Seite „Ressourcenbestand“ direkt auf den Ressourcennamen klicken. Um von der Seite mit den Ressourcendetails auf die Ressourcen-Zeitachse zuzugreifen, wählen Sie die Schaltfläche Ressourcen-Zeitachse.

Sie können auch die Compliance der Ressourcen anzeigen, indem Sie diese auf der Seite Resource inventory (Ressourcenbestand) suchen. Weitere Informationen finden Sie unter Suchen nach Ressourcen, die entdeckt wurden von AWS Config.

Konformität anzeigen (AWS SDKs)

Um Compliance-Informationen für Ihre AWS Ressourcen zu erhalten

Die folgenden Code-Beispiele zeigen, wie `DescribeComplianceByResource` verwendet wird.

CLI

AWS CLI

Um Compliance-Informationen für Ihre AWS Ressourcen zu erhalten

Der folgende Befehl gibt Konformitätsinformationen für jede EC2 Instanz zurück, die von AWS Config aufgezeichnet wurde und gegen eine oder mehrere Regeln verstößt:

```
aws configservice describe-compliance-by-resource --resource-
type AWS::EC2::Instance --compliance-types NON_COMPLIANT
```

In der Ausgabe gibt der Wert für jedes `CappedCount` Attribut an, gegen wie viele Regeln die Ressource verstößt. Die folgende Ausgabe gibt beispielsweise an, dass die Instanz `i-1a2b3c4d` gegen zwei Regeln verstößt.

Ausgabe:

```
{
    "ComplianceByResources": [
        {
            "ResourceType": "AWS::EC2::Instance",
            "ResourceId": "i-1a2b3c4d",
            "Compliance": {
                "ComplianceContributorCount": {
                    "CappedCount": 2,
                    "CapExceeded": false
                },
                "ComplianceType": "NON_COMPLIANT"
            }
        },
        {
            "ResourceType": "AWS::EC2::Instance",
            "ResourceId": "i-2a2b3c4d ",
            "Compliance": {
                "ComplianceContributorCount": {
                    "CappedCount": 3,
                    "CapExceeded": false
                },
                "ComplianceType": "NON_COMPLIANT"
            }
        }
    ]
}
```

- Einzelheiten zur API finden Sie DescribeComplianceByResourcein der AWS CLI Befehlsreferenz.

PowerShell

Tools für PowerShell V4

Beispiel 1: In diesem Beispiel wird der **`AWS::SSM::ManagedInstanceInventory`** Ressourcentyp auf den Konformitätstyp „COMPLIANT“ geprüft.

```
Get-CFGComplianceByResource -ComplianceType COMPLIANT -ResourceType
 AWS::SSM::ManagedInstanceInventory
```

Ausgabe:

```
Compliance                            ResourceId          ResourceType
----------                            ----------          ------------
Amazon.ConfigService.Model.Compliance i-0123bcf4b567890e3
 AWS::SSM::ManagedInstanceInventory
Amazon.ConfigService.Model.Compliance i-0a1234f6f5d6b78f7
 AWS::SSM::ManagedInstanceInventory
```

- Einzelheiten zur API finden Sie unter DescribeComplianceByResource AWS -Tools für PowerShellCmdlet-Referenz (V4).

Um die Konformitätsübersicht Ihrer Ressourcen abzurufen AWS

Die folgenden Code-Beispiele zeigen, wie `GetComplianceSummaryByResourceType` verwendet wird.

CLI

AWS CLI

Um die Konformitätsübersicht für alle Ressourcentypen abzurufen

Der folgende Befehl gibt die Anzahl der AWS Ressourcen zurück, die nicht konform sind, und die Anzahl, die konform sind:

```
aws configservice get-compliance-summary-by-resource-type
```

In der Ausgabe gibt der Wert für jedes `CappedCount` Attribut an, wie viele Ressourcen konform oder nicht konform sind.

Ausgabe:

```
{
    "ComplianceSummariesByResourceType": [
        {
            "ComplianceSummary": {
                "NonCompliantResourceCount": {
                    "CappedCount": 16,
                    "CapExceeded": false
                },
                "ComplianceSummaryTimestamp": 1453237464.543,
                "CompliantResourceCount": {
                    "CappedCount": 10,
                    "CapExceeded": false
                }
            }
        }
    ]
}
```

Um die Konformitätsübersicht für einen bestimmten Ressourcentyp abzurufen

Der folgende Befehl gibt die Anzahl der EC2 Instanzen zurück, die nicht konform sind, und die Anzahl, die konform sind:

```
aws configservice get-compliance-summary-by-resource-type --resource-
types AWS::EC2::Instance
```

In der Ausgabe gibt der Wert für jedes `CappedCount` Attribut an, wie viele Ressourcen konform oder nicht konform sind.

Ausgabe:

```
{
    "ComplianceSummariesByResourceType": [
        {
            "ResourceType": "AWS::EC2::Instance",
            "ComplianceSummary": {
                "NonCompliantResourceCount": {
                    "CappedCount": 3,
                    "CapExceeded": false
```

```
                },
                "ComplianceSummaryTimestamp": 1452204923.518,
                "CompliantResourceCount": {
                    "CappedCount": 7,
                    "CapExceeded": false
                }
            }
        }
    ]
}
```

- Einzelheiten zur API finden Sie unter GetComplianceSummaryByResourceType AWS CLIBefehlsreferenz.

PowerShell

Tools für PowerShell V4

Beispiel 1: Dieses Beispiel gibt die Anzahl der Ressourcen zurück, die konform oder nicht konform sind, und konvertiert die Ausgabe in JSON.

```
Get-CFGComplianceSummaryByResourceType -Select
 ComplianceSummariesByResourceType.ComplianceSummary | ConvertTo-Json
{
  "ComplianceSummaryTimestamp": "2019-12-14T06:14:49.778Z",
  "CompliantResourceCount": {
    "CapExceeded": false,
    "CappedCount": 2
  },
  "NonCompliantResourceCount": {
    "CapExceeded": true,
    "CappedCount": 100
  }
}
```

- Einzelheiten zur API finden Sie unter GetComplianceSummaryByResourceType AWS -Tools für PowerShellCmdlet-Referenz (V4).

Um die Evaluierungsergebnisse für eine Ressource abzurufen AWS

Die folgenden Code-Beispiele zeigen, wie `GetComplianceDetailsByResource` verwendet wird.

CLI

AWS CLI

Um die Bewertungsergebnisse für eine AWS Ressource abzurufen

Der folgende Befehl gibt die Evaluierungsergebnisse für jede Regel zurück, der die EC2 Instanz `i-1a2b3c4d` nicht entspricht:

```
aws configservice get-compliance-details-by-resource --resource-
type AWS::EC2::Instance --resource-id i-1a2b3c4d --compliance-types NON_COMPLIANT
```

Ausgabe:

```
{
    "EvaluationResults": [
        {
            "EvaluationResultIdentifier": {
                "OrderingTimestamp": 1450314635.065,
                "EvaluationResultQualifier": {
                    "ResourceType": "AWS::EC2::Instance",
                    "ResourceId": "i-1a2b3c4d",
                    "ConfigRuleName": "InstanceTypesAreT2micro"
                }
            },
            "ResultRecordedTime": 1450314643.288,
            "ConfigRuleInvokedTime": 1450314643.034,
            "ComplianceType": "NON_COMPLIANT"
        },
        {
            "EvaluationResultIdentifier": {
                "OrderingTimestamp": 1450314635.065,
                "EvaluationResultQualifier": {
                    "ResourceType": "AWS::EC2::Instance",
                    "ResourceId": "i-1a2b3c4d",
                    "ConfigRuleName": "RequiredTagForEC2Instances"
                }
            },
            "ResultRecordedTime": 1450314645.261,
            "ConfigRuleInvokedTime": 1450314642.948,
            "ComplianceType": "NON_COMPLIANT"
        }
    ]
```

```
}
```

- Einzelheiten zur API finden Sie GetComplianceDetailsByResourceunter AWS CLI Befehlsreferenz.

PowerShell

Tools für PowerShell V4

Beispiel 1: Die Ergebnisse dieser Beispielauswertung für die angegebene Ressource.

```
Get-CFGComplianceDetailsByResource -ResourceId ABCD5STJ4EFGHIVEW6JAH -
ResourceType 'AWS::IAM::User'
```

Ausgabe:

```
Annotation                 :
ComplianceType             : COMPLIANT
ConfigRuleInvokedTime      : 8/25/2019 11:34:56 PM
EvaluationResultIdentifier :
 Amazon.ConfigService.Model.EvaluationResultIdentifier
ResultRecordedTime         : 8/25/2019 11:34:56 PM
ResultToken                :
```

- Einzelheiten zur API finden Sie unter GetComplianceDetailsByResource AWS -Tools für PowerShellCmdlet-Referenz (V4).

Den Compliance-Verlauf für Ihre AWS Ressourcen anzeigen mit AWS Config

> **Important**
>
> Für eine genaue Berichterstattung über den Compliance-Status müssen Sie den Ressourcentyp `AWS::Config::ResourceCompliance` aufzeichnen. Weitere Informationen finden Sie unter AWS Ressourcen aufzeichnen.

Sie können die Konfiguration, die Beziehungen und die Anzahl der an einer Ressource vorgenommenen Änderungen in der AWS Config Konsole anzeigen. Sie können den Konfigurationsverlauf für eine Ressource mithilfe von anzeigen AWS CLI.

Themen

- Konformitätsverlauf anzeigen (Konsole)
- Konformitätsverlauf anzeigen (AWS CLI)
- Zeitleiste des Compliance-Verlaufs für Ressourcen und Regeln anzeigen

Konformitätsverlauf anzeigen (Konsole)

Den Konformitätsverlauf mithilfe der Konsole anzeigen

Wenn Sie Ressourcen auf der Seite Ressourcenbestand suchen, klicken Sie in der Spalte mit Ressourcen-IDs auf den Namen oder die ID der Ressource, um die Detailseite der Ressource anzuzeigen. Die Detailseite bietet Informationen über die Konfiguration, die Beziehungen und die Anzahl der vorgenommenen Änderungen dieser Ressource.

Um von der Seite mit den Ressourcendetails auf die Ressourcen-Zeitachse zuzugreifen, wählen Sie die Schaltfläche Ressourcen-Zeitachse aus. In der Ressourcen-Zeitachse werden Änderungen für eine bestimmte Ressource über einen Zeitraum als `ConfigurationItems` erfasst. Sie können nach Konfigurationsereignissen, Konformitätsereignissen oder CloudTrail Ereignissen filtern.

Konformitätsverlauf anzeigen (AWS CLI)

Den Konformitätsverlauf anzeigen mit dem AWS CLI

Die aufgezeichneten Konfigurationselemente werden bei Bedarf als Konfigurations-Snapshot und als Konfigurationsstream an den angegebenen Bereitstellungskanal übermittelt. AWS Config Sie können das verwenden AWS CLI , um den Verlauf der Konfigurationselemente für jede Ressource anzuzeigen.

Anzeigen des Konfigurationsverlaufs

Geben Sie den `get-resource-config-history`Befehl ein und geben Sie den Ressourcentyp und die Ressourcen-ID an, zum Beispiel:

```
$ aws configservice get-resource-config-history --resource-type AWS::EC2::SecurityGroup
 --resource-id sg-6fbb3807
{
```

```
    "configurationItems": [
        {
            "configurationItemCaptureTime": 1414708529.9219999,
            "relationships": [
                {
                    "resourceType": "AWS::EC2::Instance",
                    "resourceId": "i-7a3b232a",
                    "relationshipName": "Is associated with Instance"
                },
                {
                    "resourceType": "AWS::EC2::Instance",
                    "resourceId": "i-8b6eb2ab",
                    "relationshipName": "Is associated with Instance"
                },
                {
                    "resourceType": "AWS::EC2::Instance",
                    "resourceId": "i-c478efe5",
                    "relationshipName": "Is associated with Instance"
                },
                {
                    "resourceType": "AWS::EC2::Instance",
                    "resourceId": "i-e4cbe38d",
                    "relationshipName": "Is associated with Instance"
                }
            ],
            "availabilityZone": "Not Applicable",
            "tags": {},
            "resourceType": "AWS::EC2::SecurityGroup",
            "resourceId": "sg-6fbb3807",
            "configurationStateId": "1",
            "relatedEvents": [],
            "arn": "arn:aws:ec2:us-east-2:012345678912:security-group/default",
            "version": "1.0",
            "configurationItemMD5Hash": "860aa81fc3869e186b2ee00bc638a01a",
            "configuration": "{\"ownerId\":\"605053316265\",\"groupName\":\"default
\",\"groupId\":\"sg-6fbb3807\",\"description\":\"default group\",\"ipPermissions
\":[{\"ipProtocol\":\"tcp\",\"fromPort\":80,\"toPort\":80,\"userIdGroupPairs\":
[{\"userId\":\"amazon-elb\",\"groupName\":\"amazon-elb-sg\",\"groupId\":\"sg-843f59ed
\"}],\"ipRanges\":[\"0.0.0.0/0\"]},{\"ipProtocol\":\"tcp\",\"fromPort\":0,\"toPort
\":65535,\"userIdGroupPairs\":[{\"userId\":\"605053316265\",\"groupName\":\"default
\",\"groupId\":\"sg-6fbb3807\"}],\"ipRanges\":[]},{\"ipProtocol\":\"udp\",\"fromPort
\":0,\"toPort\":65535,\"userIdGroupPairs\":[{\"userId\":\"605053316265\",\"groupName
\":\"default\",\"groupId\":\"sg-6fbb3807\"}],\"ipRanges\":[]},{\"ipProtocol\":\"icmp
\",\"fromPort\":-1,\"toPort\":-1,\"userIdGroupPairs\":[{\"userId\":\"605053316265\",
```

```
\"groupName\":\"default\",\"groupId\":\"sg-6fbb3807\"}],\"ipRanges\":[]},{\"ipProtocol
\":\"tcp\",\"fromPort\":1433,\"toPort\":1433,\"userIdGroupPairs\":[],\"ipRanges
\":[\"0.0.0.0/0\"]},{\"ipProtocol\":\"tcp\",\"fromPort\":3389,\"toPort\":3389,
\"userIdGroupPairs\":[],\"ipRanges\":[\"207.171.160.0/19\"]}],\"ipPermissionsEgress\":
[],\"vpcId\":null,\"tags\":[]}",
            "configurationItemStatus": "ResourceDiscovered",
            "accountId": "605053316265"
        }
    ],
    "nextToken":
     ..........
```

Eine detaillierte Erläuterung der Antwortfelder finden Sie in Components of a Configuration Item und Unterstützte Ressourcentypen für AWS Config.

Beispiel für einen Amazon-EBS-Konfigurationsverlauf aus AWS Config

AWS Config generiert eine Reihe von Dateien, die jeweils einen Ressourcentyp repräsentieren, und listet alle Konfigurationsänderungen für die Ressourcen dieses Typs auf, die AWS Config aufgezeichnet werden. AWS Config exportiert diesen ressourcenzentrierten Konfigurationsverlauf als Objekt in den Amazon S3 S3-Bucket, den Sie bei der Aktivierung angegeben haben. AWS Config In der Datei des Konfigurationsverlaufs für jeden Ressourcentyp sind die für die Ressourcen dieses Typs erkannten Änderungen seit der letzten Übermittlung der Verlaufsdatei enthalten. Die Verlaufsdateien werden in der Regel alle sechs Stunden übermittelt.

Das Folgende ist ein Beispiel für den Inhalt des Amazon S3 S3-Objekts, das den Konfigurationsverlauf aller Amazon Elastic Block Store-Volumes in der aktuellen Region für Sie beschreibt AWS-Konto. Die Volumes in diesem Konto umfassen `vol-ce676ccc` und `vol-cia007c`. Beim Volume `vol-ce676ccc` gab es seit der Übermittlung der vorherigen Verlaufsdatei zwei Konfigurationsänderungen, und beim Volume `vol-cia007c` eine.

```
{
    "fileVersion": "1.0",
    "requestId": "asudf8ow-4e34-4f32-afeb-0ace5bf3trye",
    "configurationItems": [
        {
            "snapshotVersion": "1.0",
            "resourceId": "vol-ce676ccc",
            "arn": "arn:aws:us-west-2b:123456789012:volume/vol-ce676ccc",
            "accountId": "12345678910",
            "configurationItemCaptureTime": "2014-03-07T23:47:08.918Z",
            "configurationStateID": "3e660fdf-4e34-4f32-afeb-0ace5bf3d63a",
```

```
            "configurationItemStatus": "OK",
            "relatedEvents": [
                "06c12a39-eb35-11de-ae07-adb69edbb1e4",
                "c376e30d-71a2-4694-89b7-a5a04ad92281"
            ],
            "availibilityZone": "us-west-2b",
            "resourceType": "AWS::EC2::Volume",
            "resourceCreationTime": "2014-02-27T21:43:53.885Z",
            "tags": {},
            "relationships": [
                {
                    "resourceId": "i-344c463d",
                    "resourceType": "AWS::EC2::Instance",
                    "name": "Attached to Instance"
                }
            ],
            "configuration": {
                "volumeId": "vol-ce676ccc",
                "size": 1,
                "snapshotId": "",
                "availabilityZone": "us-west-2b",
                "state": "in-use",
                "createTime": "2014-02-27T21:43:53.0885+0000",
                "attachments": [
                    {
                        "volumeId": "vol-ce676ccc",
                        "instanceId": "i-344c463d",
                        "device": "/dev/sdf",
                        "state": "attached",
                        "attachTime": "2014-03-07T23:46:28.0000+0000",
                        "deleteOnTermination": false
                    }
                ],
                "tags": [
                    {
                        "tagName": "environment",
                        "tagValue": "PROD"
                    },
                    {
                        "tagName": "name",
                        "tagValue": "DataVolume1"
                    }
                ],
                "volumeType": "standard"
```

```
            }
        },
        {
            "configurationItemVersion": "1.0",
            "resourceId": "vol-ce676ccc",
            "arn": "arn:aws:us-west-2b:123456789012:volume/vol-ce676ccc",
            "accountId": "12345678910",
            "configurationItemCaptureTime": "2014-03-07T21:47:08.918Z",
            "configurationItemState": "3e660fdf-4e34-4f32-sseb-0ace5bf3d63a",
            "configurationItemStatus": "OK",
            "relatedEvents": [
                "06c12a39-eb35-11de-ae07-ad229edbb1e4",
                "c376e30d-71a2-4694-89b7-a5a04w292281"
            ],
            "availibilityZone": "us-west-2b",
            "resourceType": "AWS::EC2::Volume",
            "resourceCreationTime": "2014-02-27T21:43:53.885Z",
            "tags": {},
            "relationships": [
                {
                    "resourceId": "i-344c463d",
                    "resourceType": "AWS::EC2::Instance",
                    "name": "Attached to Instance"
                }
            ],
            "configuration": {
                "volumeId": "vol-ce676ccc",
                "size": 1,
                "snapshotId": "",
                "availabilityZone": "us-west-2b",
                "state": "in-use",
                "createTime": "2014-02-27T21:43:53.0885+0000",
                "attachments": [
                    {
                        "volumeId": "vol-ce676ccc",
                        "instanceId": "i-344c463d",
                        "device": "/dev/sdf",
                        "state": "attached",
                        "attachTime": "2014-03-07T23:46:28.0000+0000",
                        "deleteOnTermination": false
                    }
                ],
                "tags": [
                    {
```

```
                        "tagName": "environment",
                        "tagValue": "PROD"
                    },
                    {
                        "tagName": "name",
                        "tagValue": "DataVolume1"
                    }
                ],
                "volumeType": "standard"
            }
        },
        {
            "configurationItemVersion": "1.0",
            "resourceId": "vol-cia007c",
            "arn": "arn:aws:us-west-2b:123456789012:volume/vol-cia007c",
            "accountId": "12345678910",
            "configurationItemCaptureTime": "2014-03-07T20:47:08.918Z",
            "configurationItemState": "3e660fdf-4e34-4f88-sseb-0ace5bf3d63a",
            "configurationItemStatus": "OK",
            "relatedEvents": [
                "06c12a39-eb35-11de-ae07-adjhk8edbb1e4",
                "c376e30d-71a2-4694-89b7-a5a67u292281"
            ],
            "availibilityZone": "us-west-2b",
            "resourceType": "AWS::EC2::Volume",
            "resourceCreationTime": "2014-02-27T20:43:53.885Z",
            "tags": {},
            "relationships": [
                {
                    "resourceId": "i-344e563d",
                    "resourceType": "AWS::EC2::Instance",
                    "name": "Attached to Instance"
                }
            ],
            "configuration": {
                "volumeId": "vol-cia007c",
                "size": 1,
                "snapshotId": "",
                "availabilityZone": "us-west-2b",
                "state": "in-use",
                "createTime": "2014-02-27T20:43:53.0885+0000",
                "attachments": [
                    {
                        "volumeId": "vol-cia007c",
```

```
                        "instanceId": "i-344e563d",
                        "device": "/dev/sdf",
                        "state": "attached",
                        "attachTime": "2014-03-07T23:46:28.0000+0000",
                        "deleteOnTermination": false
                    }
                ],
                "tags": [
                    {
                        "tagName": "environment",
                        "tagValue": "PROD"
                    },
                    {
                        "tagName": "name",
                        "tagValue": "DataVolume2"
                    }
                ],
                "volumeType": "standard"
            }
        }
    ]
}
```

Zeitleiste des Compliance-Verlaufs für Ressourcen und Regeln anzeigen

AWS Config unterstützt das Speichern von Konformitätsstatusänderungen von Ressourcen, wie sie von bewertet wurden AWS-Config-Regeln. Der Compliance-Verlauf für Ressourcen wird in Form einer Timeline dargestellt. In der Timeline werden Änderungen für eine bestimmte Ressource über einen Zeitraum als `ConfigurationItems` erfasst. Informationen zum Inhalt von `ConfigurationItem` finden Sie ConfigurationItemin der AWS Config API-Referenz.

Sie können die Aufzeichnung aller Ressourcentypen in AWS Config aktivieren oder deaktivieren. Wenn Sie sich dafür entschieden haben, alle Ressourcentypen aufzuzeichnen, beginnt AWS Config automatisch die Aufzeichnung des Compliance-Verlaufs der Ressourcen, wie von bewertet AWS-Config-Regeln. AWS Config Zeichnet standardmäßig die Konfigurationsänderungen für alle unterstützten Ressourcen auf. Sie können auch nur den spezifischen Ressourcentyp für den Compliance-Verlauf der Ressource auswählen: `AWS::Config::ResourceCompliance`. Weitere Informationen finden Sie unter AWS Aufzeichnungen aufzeichnen.

Viewing Resource Timeline Using Resources

Sie können auf die Ressourcen-Zeitachse zugreifen, indem Sie auf der Seite „Ressourcenbestand“ eine bestimmte Ressource auswählen.

1. Wählen Sie im linken Navigationsbereich die Ressourcen aus.
2. Auf der Seite „Ressourcenbestand“ können Sie nach Ressourcenkategorie, Ressourcentyp und Compliance-Status filtern. Wählen Sie gegebenenfalls Gelöschte Ressourcen einschließen aus.

   In der Tabelle werden die Ressourcen-ID für den Ressourcentyp und der Ressourcen-Compliance-Status für diese Ressource angezeigt. Bei der Ressourcen-ID kann es sich um eine Ressourcen-ID oder einen Ressourcennamen handeln.
3. Wählen Sie eine Ressource aus der Spalte mit Ressourcen-IDs aus.
4. Wählen Sie die Schaltfläche Ressourcen-Zeitachse aus. Sie können nach Konfigurationsereignissen, Konformitätsereignissen oder CloudTrail Ereignissen filtern.

   > **Note**
   >
   > Alternativ können Sie auf der Seite „Ressourcenbestand“ direkt auf den Ressourcennamen klicken. Um von der Seite mit den Ressourcendetails auf die Ressourcen-Zeitachse zuzugreifen, wählen Sie die Schaltfläche Ressourcen-Zeitachse aus.

Viewing Resource Timeline Using Rules

Sie können auf die Ressourcen-Zeitachse zugreifen, indem Sie auf der Seite „Regel“ eine bestimmte Regel auswählen.

1. Wählen Sie im linken Navigationsbereich die Regeln aus.
2. Klicken Sie auf der Seite „Regel“ auf den Namen der Regel, durch die Ihre relevanten Ressourcen ausgewertet werden. Wenn keine Regeln auf dem Bildschirm angezeigt werden, fügen Sie mithilfe der Schaltfläche Add rule (Regel hinzufügen) Regeln hinzu.
3. Wählen Sie auf der Seite "Rule details (Regeldetails)" die Ressourcen aus der Tabelle ausgewerteter Ressourcen aus.
4. Wählen Sie die Schaltfläche Ressourcen-Zeitachse aus. Die Ressourcen-Zeitleiste wird angezeigt.

Den Compliance-Verlauf Ihrer Ressourcen abfragen AWS

Fragen Sie den Compliance-Verlauf der Ressourcen get-resource-config-history mithilfe des Ressourcentyps ab`AWS::Config::ResourceCompliance`.

```
aws configservice get-resource-config-history --resource-type
 AWS::Config::ResourceCompliance --resource-id AWS::S3::Bucket/configrules-bucket
```

Die Ausgabe sollte folgendermaßen oder ähnlich aussehen:

```
{
 "configurationItems": [
  {
   "configurationItemCaptureTime": 1539799966.921,
   "relationships": [
    {
     "resourceType": "AWS::S3::Bucket",
     "resourceId": "configrules-bucket",
     "relationshipName": "Is associated with "
    }
   ]
   "tags": {},
   "resourceType": "AWS::Config::ResourceCompliance",
   "resourceId": "AWS::S3::Bucket/configrules-bucket",
   "ConfigurationStateId": "1539799966921",
   "relatedEvents": [];
   "awsRegion": "us-west-2",
   "version": "1.3",
   "configurationItemMD5Hash": "",
   "supplementaryConfiguration": {},
   "configuration": "{\"complianceType\":\"COMPLIANT\",\"targetResourceId\":
\"configrules-bucket\",\"targetResourceType\":\"AWS::S3::Bucket\",\configRuleList"\":
[{\"configRuleArn\":\"arn:aws:config:us-west-2:AccountID:config-rule/config-rule-w1gogw
\",\"configRuleId\":\"config-rule-w1gogw\",\"configRuleName\":\"s3-bucket-logging-
enabled\",\"complianceType\":\"COMPLIANT\"}]}",

   "configurationItemStatus": "ResourceDiscovered",
   "accountId": "AccountID"
  }
 ]
}
```

Verschlagworten Sie Ihre Ressourcen AWS Config

Ein Tag ist eine Bezeichnung, die Sie einer AWS Ressource zuweisen. Jeder Tag (Markierung) besteht aus einem Schlüssel und einem optionalen Wert, beides können Sie bestimmen. Tags erleichtern die Verwaltung, Suche und Filterung von Ressourcen.

Mithilfe von Tags können Sie Ihre AWS Ressourcen auf unterschiedliche Weise kategorisieren, z. B. nach Zweck, Eigentümer oder Umgebung. Dies ist hilfreich, wenn Sie viele Ressourcen desselben Typs haben. In diesem Fall können Sie basierend auf den zugewiesenen Tags schnell bestimmte Ressourcen identifizieren. Sie können Ihren AWS Ressourcen ein oder mehrere Tags zuweisen. Jedes Tag verfügt über einen zugewiesenen Wert.

Wir empfehlen die Verwendung von Tag (Markierung)-Schlüsseln, die die Anforderungen der jeweiligen Ressourcentypen erfüllen. Die Verwendung einheitlicher Tag-Schlüssel vereinfacht das Verwalten der AWS -Ressourcen. Sie können die Ressourcen auf Grundlage der hinzugefügten Tags (Markierungen) filtern und danach suchen.

Tags werden ausschließlich als Zeichenfolgen interpretiert und nicht automatisch Ihren Ressourcen zugewiesen. Sie können Tag (Markierung)-Schlüssel und -Werte bearbeiten und Tags (Markierungen) jederzeit von einer Ressource entfernen. Sie können den Wert eines Tags (Markierung) zwar auf eine leere Zeichenfolge, jedoch nicht null festlegen. Wenn Sie ein Tag (Markierung) mit demselben Schlüssel wie ein vorhandener Tag (Markierung) für die Ressource hinzufügen, wird der alte Wert mit dem neuen überschrieben. Wenn Sie eine Ressource löschen, werden alle Tags (Markierungen) der Ressource ebenfalls gelöscht.

Sie können mit Tags arbeiten, indem Sie die AWS Command Line Interface (AWS CLI) und die AWS Config API-Referenz verwenden.

Einschränkungen beim Markieren

Die folgenden grundlegenden Einschränkungen gelten für Tags.

Einschränkung	Beschreibung
Maximale Anzahl von Tags pro Ressource	50
Maximale Schlüssellänge	128 Unicode-Zeichen in UTF-8
Maximale Länge des Wertes	256 Unicode-Zeichen in UTF-8

Einschränkung	Beschreibung
Präfixeinschränkung	Verwenden Sie das `aws:` Präfix nicht in Ihren Tagnamen oder -Werten, da es für die AWS Verwendung reserviert ist. Sie können keine Tag-Namen oder Werte mit diesem Präfix bearbeiten oder löschen. Tags mit diesem Präfix werden nicht als Ihre Tags pro Ressourcenlimit angerechnet.
Zeicheneinschränkungen	Tags dürfen nur Unicode-Buchstaben, Ziffern, Leerzeichen oder die folgenden Symbole enthalten: `_ . : / = + - @`.

Verwaltung von Tags mit AWS Config API-Aktionen

Tagbasierte Zugriffskontrollen sind für drei Ressourcen verfügbar: `ConfigurationAggregator`, `AggregationAuthorization` und `ConfigRule`. Mit den folgenden Befehlen können Sie Tags für Ihre Ressourcen hinzufügen, aktualisieren, auflisten und löschen.

- ListTagsForResource
- TagResource
- UntagResource

> **Note**
>
> `TagResource`und `UntagResource` erfordern bestimmte AWS Identity and Access Management (IAM-) Berechtigungen, um den Zugriff zu kontrollieren. Weitere Informationen finden Sie unter Zugriffssteuerung auf der Grundlage von Tag-Schlüsseln im IAM-Benutzerhandbuch.

Ressourcen anhand von AWS Config Regeln auswerten

Wird verwendet AWS Config , um die Konfigurationseinstellungen Ihrer AWS Ressourcen auszuwerten. Dazu erstellen Sie AWS Config Regeln, die Ihren idealen Konfigurationseinstellungen entsprechen. AWS Config bietet anpassbare, vordefinierte Regeln, die als verwaltete Regeln bezeichnet werden, um Ihnen den Einstieg zu erleichtern.

Themen

- Überlegungen
- Unterstützung von Regionen
- Bestandteile einer AWS Config Regel
- AWS Config Verwaltete Regeln
- AWS Config Benutzerdefinierte Regeln
- Serviceverknüpfte Regeln AWS Config
- AWS Config Regeln für alle Konten in Ihrer Organisation verwalten
- AWS Config Regeln hinzufügen
- AWS Config Regeln aktualisieren
- AWS Config Regeln löschen
- Details und Compliance-Informationen zu Ihren AWS Config Regeln anzeigen
- Proaktive Evaluierung für AWS Config Regeln aktivieren
- Senden von Regelauswertungen an Security Hub
- Evaluieren Sie Ihre Ressourcen mit AWS Config Regeln
- Löschen von Bewertungsergebnissen aus AWS Config -Regeln
- Problembehandlung für Regeln AWS Config

Überlegungen

Cost Considerations

> Einzelheiten zu den Kosten im Zusammenhang mit der Erfassung von Ressourcen finden Sie unter AWS Config Preise.

Empfehlung: Erwägen Sie, den **`AWS::Config::ResourceCompliance`** Ressourcentyp aus der Aufzeichnung auszuschließen, bevor Sie Regeln löschen

Durch das Löschen von Regeln werden Konfigurationselemente (CIs) erstelltAWS::Config::ResourceCompliance, die sich auf Ihre Kosten für den Konfigurationsrekorder auswirken können. Wenn Sie Regeln löschen, die eine große Anzahl von Ressourcentypen auswerten, kann dies zu einem Anstieg der Anzahl der CIs aufgezeichneten Ressourcentypen führen.

Um die damit verbundenen Kosten zu vermeiden, können Sie die Aufzeichnung für den AWS::Config::ResourceCompliance Ressourcentyp deaktivieren, bevor Sie Regeln löschen, und die Aufzeichnung erneut aktivieren, nachdem die Regeln gelöscht wurden.

Da das Löschen von Regeln jedoch ein asynchroner Vorgang ist, kann es eine Stunde oder länger dauern, bis er abgeschlossen ist. Während der ZeitAWS::Config::ResourceCompliance, für die die Aufzeichnung deaktiviert ist, werden Regelauswertungen nicht im Verlauf der zugehörigen Ressource aufgezeichnet.

AWS Config empfiehlt, diese Faktoren auf einer bestimmten case-by-case Grundlage abzuwägen, bevor Sie entscheiden, wie mit dem Löschen von Regeln verfahren werden soll.

Empfehlung: Fügen Sie Logik hinzu, um die Auswertung gelöschter Ressourcen für benutzerdefinierte Lambda-Regeln zu handhaben

Beim Erstellen von AWS Config benutzerdefinierten Lambda-Regeln wird dringend empfohlen, Logik für die Auswertung gelöschter Ressourcen hinzuzufügen.

Wenn Auswertungsergebnisse als NOT_APPLICABLE gekennzeichnet sind, werden sie zum Löschen markiert und bereinigt. Wenn sie NICHT als markiert sindNOT_APPLICABLE, bleiben die Evaluierungsergebnisse unverändert, bis die Regel gelöscht wird. Dies kann zu einem unerwarteten Anstieg bei der Erstellung von oder AWS::Config::ResourceCompliance beim Löschen der CIs Regel führen.

Informationen dazu, wie Sie AWS Config benutzerdefinierte Lambda-Regeln so einrichten, dass sie NOT_APPLICABLE für gelöschte Ressourcen zurückgegeben werden, finden Sie unter Gelöschte Ressourcen mit AWS Config benutzerdefinierten Lambda-Regeln verwalten.

Empfehlung: Stellen Sie die Ressourcen bereit, die für benutzerdefinierte Lambda-Regeln gelten

AWS Config Benutzerdefinierte Lambda-Regeln können zu einer hohen Anzahl von Lambda-Funktionsaufrufen führen, wenn die Regel nicht auf einen oder mehrere Ressourcentypen

beschränkt ist. Um eine erhöhte Aktivität im Zusammenhang mit Ihrem Konto zu vermeiden, wird dringend empfohlen, Ressourcen im Rahmen Ihrer benutzerdefinierten Lambda-Regeln bereitzustellen. Wenn keine Ressourcentypen ausgewählt sind, ruft die Regel die Lambda-Funktion für alle Ressourcen im Konto auf.

Other considerations

Standardwerte für verwaltete Regeln

Die für verwaltete Regeln angegebenen Standardwerte sind nur bei Verwendung der AWS Konsole vorab ausgefüllt. Die Standardwerte werden für API, CLI oder SDK nicht bereitgestellt.

Verzögerungen bei der Aufzeichnung des Konfigurationselements

AWS Config In der Regel werden Konfigurationsänderungen an Ihren Ressourcen unmittelbar nach dem Erkennen einer Änderung oder in der von Ihnen angegebenen Häufigkeit aufgezeichnet. Dies erfolgt jedoch nach bestem Wissen und kann manchmal länger dauern. Ein Ressourcentyp mit bekannten Verzögerungen ist beispielsweise`AWS::SecretsManager::Secret`. Dieser Ressourcentyp ist ein Beispiel, und diese Liste erhebt keinen Anspruch auf Vollständigkeit.

Richtlinien und Ergebnisse zur Einhaltung von Vorschriften

IAM-Richtlinien und andere Richtlinien, die in verwaltet werden, AWS Organizations können sich darauf auswirken, ob Sie AWS Config berechtigt sind, Konfigurationsänderungen für Ihre Ressourcen aufzuzeichnen. Darüber hinaus bewerten Regeln direkt die Konfiguration einer Ressource, und Regeln berücksichtigen diese Richtlinien bei der Durchführung von Evaluierungen nicht. Stellen Sie sicher, dass die geltenden Richtlinien mit der Art und Weise übereinstimmen, wie Sie sie verwenden möchten AWS Config.

Tagging-Unterstützung für Ressourcentypen

Wenn ein Ressourcentyp kein Tagging unterstützt oder keine Tag-Informationen in seiner Describe-API-Antwort enthält, AWS Config werden keine Tag-Daten in den Konfigurationselementen (CIs) für diesen Ressourcentyp erfasst. AWS Config zeichnet diese Ressourcen trotzdem auf. Funktionen, die auf Tag-Daten basieren, funktionieren jedoch nicht. Dies wirkt sich auf Tag-basierte Filterung, Gruppierung oder Konformitätsbewertung aus, die auf Tag-Daten basiert.

Directory-Buckets werden nicht unterstützt

Verwaltete Regeln unterstützen nur allgemeine Buckets bei der Bewertung von Amazon Simple Storage Service (Amazon S3) -Ressourcen. Weitere Informationen zu Allzweck-Buckets und Verzeichnis-Buckets finden Sie unter Buckets-Übersicht und Verzeichnis-Buckets im Amazon-S3-Benutzerhandbuch.

Verwaltete Regeln und globale IAM-Ressourcentypen

Die globalen IAM-Ressourcentypen, die vor Februar 2022 eingeführt wurden (`AWS::IAM::Group`,, und`AWS::IAM::User`) `AWS::IAM::Policy``AWS::IAM::Role`, können nur AWS Config in AWS Regionen erfasst werden, in denen sie vor Februar 2022 verfügbar AWS Config waren. Diese Ressourcentypen können nicht in Regionen erfasst werden, die AWS Config nach Februar 2022 unterstützt werden. Eine Liste dieser Regionen finden Sie unter AWS Aufzeichnungsressourcen | Globale Ressourcen.

Wenn Sie einen globalen IAM-Ressourcentyp in mindestens einer Region aufzeichnen, führen periodische Regeln, die die Einhaltung des globalen IAM-Ressourcentyps melden, Bewertungen in allen Regionen durch, in denen die periodische Regel hinzugefügt wurde, auch wenn Sie die Aufzeichnung des globalen IAM-Ressourcentyps in der Region, in der die periodische Regel hinzugefügt wurde, nicht aktiviert haben.

Um unnötige Bewertungen zu vermeiden, sollten Sie nur regelmäßige Regeln einrichten, die die Einhaltung der Vorschriften für einen globalen IAM-Ressourcentyp an eine der unterstützten Regionen melden. Eine Liste der verwalteten Regeln, die in welchen Regionen unterstützt werden, finden Sie unter Liste der AWS Config verwalteten Regeln nach regionaler Verfügbarkeit.

Unterstützung von Regionen

Derzeit wird die AWS Config Regelfunktion in den folgenden AWS Regionen unterstützt. Eine Liste der einzelnen AWS Config Regeln, die in welchen Regionen unterstützt werden, finden Sie unter Liste der AWS Config verwalteten Regeln nach Verfügbarkeit in Regionen.

Name der Region	Region	Endpunkt	Protocol (Protokoll)	
USA Ost (Ohio)	us-east-2	config.us-east-2.amazonaws.com	HTTPS	
		config-fips.us-east-2.amazonaws.com	HTTPS	

Name der Region	Region	Endpunkt	Protocol (Protokoll)
USA Ost (Nord-Virginia)	us-east-1	config.us-east-1.amazonaws.com config-fips.us-east-1.amazonaws.com	HTTPS HTTPS
USA West (Nordkalifornien)	us-west-1	config.us-west-1.amazonaws.com config-fips.us-west-1.amazonaws.com	HTTPS HTTPS
USA West (Oregon)	us-west-2	config.us-west-2.amazonaws.com config-fips.us-west-2.amazonaws.com	HTTPS HTTPS
Afrika (Kapstadt)	af-south-1	config.af-south-1.amazonaws.com	HTTPS
Asien-Pazifik (Hongkong)	ap-east-1	config.ap-east-1.amazonaws.com	HTTPS
Asien-Pazifik (Hyderabad)	ap-south-2	config.ap-south-2.amazonaws.com	HTTPS
Asien-Pazifik (Jakarta)	ap-southeast-3	config.ap-southeast-3.amazonaws.com	HTTPS

Name der Region	Region	Endpunkt	Protocol (Protokoll)
Asien-Pazifik (Malaysia)	ap-southeast-5	config.ap-southeast-5.amazonaws.com	HTTPS
Asien-Pazifik (Melbourne)	ap-southeast-4	config.ap-southeast-4.amazonaws.com	HTTPS
Asien-Pazifik (Mumbai)	ap-south-1	config.ap-south-1.amazonaws.com	HTTPS
Asien-Pazifik (Osaka)	ap-northeast-3	config.ap-northeast-3.amazonaws.com	HTTPS
Asien-Pazifik (Seoul)	ap-northeast-2	config.ap-northeast-2.amazonaws.com	HTTPS
Asien-Pazifik (Singapur)	ap-southeast-1	config.ap-southeast-1.amazonaws.com	HTTPS
Asien-Pazifik (Sydney)	ap-southeast-2	config.ap-southeast-2.amazonaws.com	HTTPS
Asien-Pazifik (Taipeh)	ap-east-2	config.ap-east-2.amazonaws.com	HTTPS

Name der Region	Region	Endpunkt	Protocol (Protokoll)
Asien-Pazifik (Thailand)	ap-southeast-7	config.ap-southeast-7.amazonaws.com	HTTPS
Asien-Pazifik (Tokio)	ap-northeast-1	config.ap-northeast-1.amazonaws.com	HTTPS
Kanada (Zentral)	ca-central-1	config.ca-central-1.amazonaws.com	HTTPS
Kanada West (Calgary)	ca-west-1	config.ca-west-1.amazonaws.com	HTTPS
Europa (Frankfurt)	eu-central-1	config.eu-central-1.amazonaws.com	HTTPS
Europa (Irland)	eu-west-1	config.eu-west-1.amazonaws.com	HTTPS
Europa (London)	eu-west-2	config.eu-west-2.amazonaws.com	HTTPS
Europa (Mailand)	eu-south-1	config.eu-south-1.amazonaws.com	HTTPS
Europa (Paris)	eu-west-3	config.eu-west-3.amazonaws.com	HTTPS
Europa (Spanien)	eu-south-2	config.eu-south-2.amazonaws.com	HTTPS

Name der Region	Region	Endpunkt	Protocol (Protokoll)
Europa (Stockholm)	eu-north-1	config.eu-north-1.amazonaws.com	HTTPS
Europa (Zürich)	eu-central-2	config.eu-central-2.amazonaws.com	HTTPS
Israel (Tel Aviv)	il-central-1	config.il-central-1.amazonaws.com	HTTPS
Mexiko (Zentral)	mx-central-1	config.mx-central-1.amazonaws.com	HTTPS
Naher Osten (Bahrain)	me-south-1	config.me-south-1.amazonaws.com	HTTPS
Naher Osten (VAE)	me-central-1	config.me-central-1.amazonaws.com	HTTPS
Südamerika (São Paulo)	sa-east-1	config.sa-east-1.amazonaws.com	HTTPS
AWS GovCloud (US-Ost)	us-gov-east-1	config.us-gov-east-1.amazonaws.com	HTTPS
AWS GovCloud (US-West)	us-gov-west-1	config.us-gov-west-1.amazonaws.com	HTTPS

Die Bereitstellung von AWS Config Regeln für alle Mitgliedskonten einer AWS Organisation wird in den folgenden Regionen unterstützt.

Name der Region	Region	Endpunkt	Protocol (Protokoll)
USA Ost (Ohio)	us-east-2	config.us-east-2.amazonaws.com	HTTPS
USA Ost (Nord-Virginia)	us-east-1	config.us-east-1.amazonaws.com	HTTPS
USA West (Nordkalifornien)	us-west-1	config.us-west-1.amazonaws.com	HTTPS
USA West (Oregon)	us-west-2	config.us-west-2.amazonaws.com	HTTPS
Afrika (Kapstadt)	af-south-1	config.af-south-1.amazonaws.com	HTTPS
Asien-Pazifik (Hongkong)	ap-east-1	config.ap-east-1.amazonaws.com	HTTPS
Asien-Pazifik (Hyderabad)	ap-south-2	config.ap-south-2.amazonaws.com	HTTPS

Name der Region	Region	Endpunkt	Protocol (Protokoll)
Asien-Pazifik (Jakarta)	ap-southeast-3	config.ap-southeast-3.amazonaws.com	HTTPS
Asien-Pazifik (Melbourne)	ap-southeast-4	config.ap-southeast-4.amazonaws.com	HTTPS
Asien-Pazifik (Mumbai)	ap-south-1	config.ap-south-1.amazonaws.com	HTTPS
Asien-Pazifik (Osaka)	ap-northeast-3	config.ap-northeast-3.amazonaws.com	HTTPS
Asien-Pazifik (Seoul)	ap-northeast-2	config.ap-northeast-2.amazonaws.com	HTTPS
Asien-Pazifik (Singapur)	ap-southeast-1	config.ap-southeast-1.amazonaws.com	HTTPS
Asien-Pazifik (Sydney)	ap-southeast-2	config.ap-southeast-2.amazonaws.com	HTTPS
Asien-Pazifik (Tokio)	ap-northeast-1	config.ap-northeast-1.amazonaws.com	HTTPS

Name der Region	Region	Endpunkt	Protocol (Protokoll)
Kanada (Zentral)	ca-central-1	config.ca-central-1.amazonaws.com	HTTPS
Kanada West (Calgary)	ca-west-1	config.ca-west-1.amazonaws.com	HTTPS
Europa (Frankfurt)	eu-central-1	config.eu-central-1.amazonaws.com	HTTPS
Europa (Irland)	eu-west-1	config.eu-west-1.amazonaws.com	HTTPS
Europa (London)	eu-west-2	config.eu-west-2.amazonaws.com	HTTPS
Europa (Mailand)	eu-south-1	config.eu-south-1.amazonaws.com	HTTPS
Europa (Paris)	eu-west-3	config.eu-west-3.amazonaws.com	HTTPS
Europa (Spanien)	eu-south-2	config.eu-south-2.amazonaws.com	HTTPS
Europa (Stockholm)	eu-north-1	config.eu-north-1.amazonaws.com	HTTPS
Europa (Zürich)	eu-central-2	config.eu-central-2.amazonaws.com	HTTPS
Israel (Tel Aviv)	il-central-1	config.il-central-1.amazonaws.com	HTTPS

Name der Region	Region	Endpunkt	Protocol (Protokoll)
Naher Osten (Bahrain)	me-south-1	config.me-south-1.amazonaws.com	HTTPS
Naher Osten (VAE)	me-central-1	config.me-central-1.amazonaws.com	HTTPS
Südamerika (São Paulo)	sa-east-1	config.sa-east-1.amazonaws.com	HTTPS
AWS GovCloud (US-Ost)	us-gov-east-1	config.us-gov-east-1.amazonaws.com	HTTPS
AWS GovCloud (US-West)	us-gov-west-1	config.us-gov-west-1.amazonaws.com	HTTPS

Bestandteile einer AWS Config Regel

AWS Config Regeln bewerten die Konfigurationseinstellungen Ihrer AWS Ressourcen. Auf dieser Seite werden die Komponenten einer Regel beschrieben.

Themen

- So funktionieren AWS Config Regeln
- Auslösertypen
- Evaluierungsmodi
- AWS Config Regel-Metadaten

So funktionieren AWS Config Regeln

Während AWS Config die Konfigurationsänderungen bei allen Ihren Ressourcen kontinuierlich verfolgt, wird überprüft, ob diese Änderungen nicht den Bedingungen Ihrer Regeln entsprechen. Wenn eine Ressource der Regel nicht entspricht, werden die AWS Config Ressource und die Regel als nicht konform gekennzeichnet.

Es gibt vier mögliche Bewertungsergebnisse für eine AWS Config Regel.

Ergebnis der Bewertung	Beschreibung
`COMPLIANT`	Die Regel erfüllt die Bedingungen der Konformit ätsprüfung.
`NON_COMPLIANT`	Die Regel erfüllt die Bedingungen der Konformit ätsprüfung nicht.
`ERROR`	Einer der erforderlichen/optionalen Parameter ist ungültig, hat nicht den richtigen Typ oder ist falsch formatiert.
`NOT_APPLICABLE`	Wird verwendet, um Ressourcen herauszuf iltern, auf die die Logik der Regel nicht angewendet werden kann. Die alb-desync-mode-checkRegel überprüft beispielsweise nur Application Load Balancer und ignoriert Network Load Balancers und Gateway Load Balancers.

Wenn beispielsweise ein EC2 Volume erstellt wird, AWS Config kann das Volume anhand einer Regel bewertet werden, die vorschreibt, dass Volumes verschlüsselt werden müssen. Wenn das Volume nicht verschlüsselt ist, werden AWS Config das Volume und die Regel als nicht konform gekennzeichnet. AWS Config kann auch alle Ihre Ressourcen auf kontoweite Anforderungen überprüfen. AWS Config Kann beispielsweise überprüfen, ob die Anzahl der EC2 Volumen in einem Konto innerhalb der gewünschten Summe bleibt oder ob ein Konto AWS CloudTrail für die Protokollierung verwendet wird.

Auslösertypen

Nachdem Sie Ihrem Konto eine Regel hinzugefügt haben, werden Ihre Ressourcen mit den Bedingungen der Regel AWS Config verglichen. Nach dieser ersten Evaluierung werden die Evaluierungen jedes Mal, wenn eine ausgelöst wird, AWS Config fortgesetzt. Die Evaluierungsauslöser sind als Teil der Regel definiert und können die folgenden Typen beinhalten.

Typ des Auslösers	Beschreibung
Konfigurationsänderungen	AWS Config führt Evaluierungen für die Regel durch, wenn es eine Ressource gibt, die dem Geltungsbereich der Regel entspricht, und wenn sich die Konfiguration der Ressource ändert. Die Evaluierung wird ausgeführt, nachdem eine Benachrichtigung über eine Änderung des Konfigurationselements AWS Config gesendet wurde. Sie können auswählen, welche Ressource n die Auswertung auslösen, indem Sie den Umfang der Regel definieren. Im Umfang kann Folgendes enthalten sein: • Mindestens ein Ressourcentyp • Eine Kombination aus einem Ressourcentyp und einer Ressourcen-ID • Eine Kombination aus einem Tag-Schlüssel und einem Wert • Wann alle aufgezeichneten Ressourcen erstellt, aktualisiert oder gelöscht wurden AWS Config führt die Evaluierung aus, wenn eine Änderung an einer Ressource erkannt wird, die dem Geltungsbereich der Regel entspricht. Sie können den Umfang verwenden

Typ des Auslösers	Beschreibung
	, um zu definieren, welche Ressourcen Auswertungen auslösen.
Regelmäßig	AWS Config führt Evaluierungen für die Regel in einer von Ihnen festgelegten Häufigkeit durch, z. B. alle 24 Stunden.
Hybrid	Einige Regeln werden sowohl durch Konfigura tionsänderungen als auch nach einem Zeitplan ausgelöst. Bei diesen Regeln werden Ihre Ressourcen AWS Config ausgewertet, wenn eine Konfigurationsänderung erkannt wird, und auch in der von Ihnen angegebenen Häufigkeit.

Evaluierungsmodi

Es gibt zwei Bewertungsmodi für AWS Config Regeln.

Bewertungsmodus	Beschreibung
Proaktiv	Verwenden Sie die proaktive Auswertung, um Ressourcen vor der Bereitstellung auszuwert en. Auf diese Weise können Sie auswerten , ob ein Satz von Ressourceneigenschaften, wenn er zur Definition einer AWS Ressource verwendet würde, angesichts der proaktiven Regeln, die Sie in Ihrem Konto in Ihrer Region haben, als KONFORM oder NICHT KONFORM gelten würde.
Detektivisch	Mit der detektivischen Auswertung können Sie Ressourcen auswerten, die bereits bereitges tellt wurden. Auf diese Weise lassen sich die Konfigurationseinstellungen Ihrer vorhandenen Ressourcen auswerten.

> **Note**
>
> Durch proaktive Regeln werden keine Ressourcen korrigiert, die als NON_COMPLIANT gekennzeichnet sind, und sie verhindern auch nicht, dass diese bereitgestellt werden.

Weitere Informationen finden Sie unter Proaktive Evaluierung für AWS Config Regeln aktivieren.

Liste der verwalteten Regeln mit proaktiver Auswertung

Eine Liste der verwalteten Regeln, die die proaktive Evaluierung unterstützen, finden Sie unter Liste der AWS Config verwalteten Regeln nach Testmodus.

Liste der unterstützten Ressourcentypen für die proaktive Auswertung

Im Folgenden finden Sie eine Liste der Ressourcentypen, die für die proaktive Auswertung unterstützt werden:

- `AWS::ApiGateway::Stage`
- `AWS::AutoScaling::AutoScalingGroup`
- `AWS::EC2::EIP`
- `AWS::EC2::Instance`
- `AWS::EC2::Subnet`
- `AWS::Elasticsearch::Domain`
- `AWS::Lambda::Function`
- `AWS::RDS::DBInstance`
- `AWS::Redshift::Cluster`
- `AWS::S3::Bucket`
- `AWS::SNS::Topic`

AWS Config Regel-Metadaten

AWS Config Regeln können die folgenden veränderbaren Metadaten enthalten:

defaultName

DefaultName ist der Name, den Instances einer Regel standardmäßig erhalten.

description

Die Regelbeschreibung bietet einen Kontext für die Elemente, die die Regel auswertet. Für die AWS Config -Konsole gilt eine Beschränkung von 256 Zeichen. Als bewährte Methode sollte die Regelbeschreibung mit „Prüft ob“ beginnen und eine Beschreibung des NON_COMPLIANT-Szenarios enthalten. Servicenamen sollten vollständig geschrieben werden, beginnend mit AWS oder Amazon, wenn sie in der Regelbeschreibung zum ersten Mal erwähnt werden. Zum Beispiel AWS CloudTrail oder Amazon CloudWatch statt CloudTrail oder CloudWatch für den ersten Gebrauch. Im weiteren Verlauf können Servicenamen abgekürzt werden.

scope

Der Umfang bestimmt, auf welche Ressourcentypen sich die Regel bezieht. Eine Liste der unterstützten Ressourcentypen finden Sie unter Unterstützte Ressourcentypen.

compulsoryInputParameterDetails

Die compulsoryInputParameter Details werden für Parameter verwendet, die für die Auswertung einer Regel erforderlich sind. Die verwaltete Regel `access-keys-rotated` enthält beispielsweise den erforderlichen Parameter `maxAccessKeyAge`. Wenn ein Parameter erforderlich ist, wird er nicht als optional markiert. Für jeden Parameter muss ein Typ angegeben werden. Der Typ kann „String“, „int“, „double“, „CSV“, „boolean“ und "StringMap“ sein.

optionalInputParameterDetails

Die optionalInputParameter Details werden für Parameter verwendet, die für die Auswertung einer Regel optional sind. Die verwaltete Regel `elasticsearch-logs-to-cloudwatch` enthält beispielsweise den optionalen Parameter `logTypes`. Für jeden Parameter muss ein Typ angegeben werden. Der Typ kann „String“, „int“, „double“, „CSV“, „boolean“ und "StringMap“ sein.

supportedEvaluationModes

supportedEvaluationModes Legt fest, wann Ressourcen bewertet werden, entweder bevor eine Ressource bereitgestellt wurde oder nachdem eine Ressource bereitgestellt wurde.

`DETECTIVE` wird verwendet, um Ressourcen zu auszuwerten, die bereits bereitgestellt wurden. Auf diese Weise können Sie die Konfigurationseinstellungen Ihrer vorhandenen Ressourcen auswerten. `PROACTIVE` wird verwendet, um Ressourcen auszuwerten, bevor sie bereitgestellt werden.

Auf diese Weise können Sie beurteilen, ob ein Satz von Ressourceneigenschaften, wenn er zur Definition einer AWS Ressource verwendet würde, angesichts der proaktiven Regeln, die Sie in Ihrem Konto in Ihrer Region haben, als KONFORM oder NON_KONFORM gelten würde.

Sie können „An“`DETECTIVE`, `PROACTIVE` „ supportedEvaluationModes oder beide“ und „beide`DETECTIVE`“ angeben. `PROACTIVE` Sie müssen einen Testmodus angeben und dieses Feld darf nicht leer bleiben.

> **Note**
>
> Durch proaktive Regeln werden keine Ressourcen korrigiert, die als NON_COMPLIANT gekennzeichnet sind, und sie verhindern auch nicht, dass diese bereitgestellt werden.

AWS Config Verwaltete Regeln

AWS Config stellt AWS verwaltete Regeln bereit. Dabei handelt es sich um vordefinierte, anpassbare Regeln, AWS Config anhand derer bewertet wird, ob Ihre AWS Ressourcen den gängigen bewährten Methoden entsprechen. Mithilfe einer verwalteten Regel können Sie beispielsweise schnell ermitteln, ob Ihre Amazon Elastic Block Store (Amazon EBS)-Volumes verschlüsselt sind oder ob spezifische Tags auf Ihre Ressourcen angewendet werden.

Die AWS Config Konsole führt Sie durch den Prozess der Konfiguration und Aktivierung einer verwalteten Regel. Sie können auch die AWS Config API AWS Command Line Interface oder verwenden, um den JSON-Code zu übergeben, der Ihre Konfiguration einer verwalteten Regel definiert.

Sie können das Verhalten einer verwalteten Regel Ihren Anforderungen entsprechend anpassen. Sie können beispielsweise den Geltungsbereich der Regel definieren, um einzuschränken, welche Ressourcen eine Bewertung der Regel auslösen, z. B. EC2 Instanzen oder Volumes.

Sie können die Regelparameter anpassen, um die Attribute zu definieren, über die Ihre Ressourcen verfügen müssen, damit sie regelkonform sind. Sie können beispielsweise einen Parameter anpassen, um anzugeben, dass eingehender Datenverkehr zu einem bestimmten Port von Ihrer Sicherheitsgruppe blockiert wird.

Bevor Sie verwaltete Regeln verwenden, finden Sie weitere Informationen unterÜberlegungen.

Themen

- Liste der AWS Config verwalteten Regeln
- Liste der AWS Config verwalteten Regeln nach Testmodus
- Liste der AWS Config verwalteten Regeln nach Triggertyp

- Liste der AWS Config verwalteten Regeln nach Regionen und Verfügbarkeit
- AWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen

Liste der AWS Config verwalteten Regeln

AWS Config unterstützt derzeit die folgenden verwalteten Regeln. Bevor Sie diese Regeln verwenden, finden Sie weitere Informationen unterÜberlegungen.

Themen

- access-keys-rotated
- account-part-of-organizations
- acmpca-certificate-authority-tagged
- acm-certificate-expiration-check
- acm-certificate-rsa-check
- acm-pca-root-ca-deaktiviert
- active-mq-supported-version
- alb-desync-mode-check
- alb-http-drop-invalid-Header-fähig
- alb-http-to-https-Weiterleitungsprüfung
- alb-internal-scheme-check
- alb-listener-tagged
- alb-waf-enabled
- amplify-app-branch-auto-löschfähig
- amplify-app-description
- amplify-app-tagged
- amplify-branch-performance-mode-aktiviert
- amplify-branch-tagged
- api-gwv2- access-logs-enabled
- api-gwv2- authorization-type-configured
- api-gw-associated-with-WAF
- api-gw-cache-enabled-und-verschlüsselt

- api-gw-endpoint-type-überprüfen
- api-gw-execution-logging-aktiviert
- api-gw-ssl-enabled
- api-gw-xray-enabled
- appconfig-application-description
- appconfig-application-tagged
- appconfig-configuration-profile-tagged
- appconfig-configuration-profile-validators-nicht leer
- appconfig-deployment-strategy-description
- appconfig-deployment-strategy-replicate-zu-ssm
- appconfig-environment-description
- appconfig-environment-tagged
- appconfig-extension-association-tagged
- appconfig-freeform-profile-config-Lagerung
- appconfig-hosted-configuration-version-Beschreibung
- appflow-flow-tagged
- appintegrations-event-integration-description
- appintegrations-event-integration-tagged
- appmesh-gateway-route-tagged
- appmesh-mesh-deny-tcp-spedition
- appmesh-mesh-tagged
- appmesh-route-tagged
- appmesh-virtual-gateway-backend-Standards-tls
- appmesh-virtual-gateway-logging-file-path-exists
- appmesh-virtual-gateway-tagged
- appmesh-virtual-node-backend-defaults-tls-on
- appmesh-virtual-node-logging-file-path-exists
- appmesh-virtual-node-tagged
- appmesh-virtual-router-tagged

- appmesh-virtual-service-tagged
- approved-amis-by-id
- approved-amis-by-tag
- apprunner-service-in-vpc
- apprunner-service-no-public-Zugang
- apprunner-service-observability-enabled
- apprunner-service-tagged
- apprunner-vpc-connector-tagged
- appstream-fleet-in-vpc
- appsync-associated-with-waf
- appsync-authorization-check
- appsync-cache-ct-encryption-im Ruhezustand
- appsync-cache-ct-encryptionim Transit
- appsync-cache-encryption-at-ausruhen
- appsync-logging-enabled
- athena-data-catalog-description
- athena-prepared-statement-description
- athena-workgroup-description
- athena-workgroup-encrypted-at-ausruhen
- athena-workgroup-enforce-workgroup-Konfiguration
- athena-workgroup-engine-version-automatisches Upgrade
- athena-workgroup-logging-enabled
- aurora-last-backup-recovery-Punkt-erstellt
- aurora-meets-restore-time-ziel
- aurora-mysql-backtracking-enabled
- aurora-mysql-cluster-audit-Protokollierung
- aurora-resources-in-logically-air-gapped-vault
- aurora-resources-protected-by-Backup-Plan
- autoscaling-capacity-rebalancing

- autoscaling-group-elb-healthcheck-erforderlich
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-hop-Grenze
- autoscaling-launch-config-public-ip-deaktiviert
- autoscaling-launch-template
- autoscaling-multiple-az
- autoscaling-multiple-instance-types
- backup-plan-min-frequency-and-min-retention-check
- backup-recovery-point-encrypted
- backup-recovery-point-manual-löschen-deaktiviert
- backup-recovery-point-minimum-Aufbewahrungsprüfung
- batch-compute-environment-enabled
- batch-compute-environment-managed
- batch-compute-environment-tagged
- batch-job-queue-enabled
- batch-job-queue-tagged
- batch-managed-compute-environment-using-launch-template
- batch-managed-compute-env-compute-resources-tagged
- batch-scheduling-policy-tagged
- beanstalk-enhanced-health-reporting-aktiviert
- cassandra-keyspace-tagged
- clb-desync-mode-check
- clb-multiple-az
- cloudformation-stack-drift-detection-überprüfen
- cloudformation-stack-notification-check
- cloudfront-accesslogs-enabled
- cloudfront-associated-with-waf
- cloudfront-custom-ssl-certificate
- cloudfront-default-root-object-konfiguriert

- cloudfront-no-deprecated-ssl-protokolle
- cloudfront-origin-access-identity-aktiviert
- cloudfront-origin-failover-enabled
- Wolkenfront - 3 origin-access-control-enabled
- Wolkenfront - 3 origin-non-existent-bucket
- cloudfront-security-policy-check
- cloudfront-sni-enabled
- cloudfront-ssl-policy-check
- cloudfront-traffic-to-origin-verschlüsselt
- cloudfront-viewer-policy-https
- cloudtrail-all-read-s3- data-event-check
- cloudtrail-all-write-s3- data-event-check
- Wolkenspur-S3- bucket-access-logging
- Wolkenspur-S3- bucket-public-access-prohibited
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-action-enabled-überprüfen
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted
- cloud-trail-cloud-watch-logs-aktiviert
- cloudtrail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-validierung aktiviert
- cmk-backing-key-rotation-aktiviert
- codebuild-project-artifact-encryption
- codebuild-project-environment-privileged-überprüfen
- codebuild-project-envvar-awscred-überprüfen

- codebuild-project-logging-enabled
- codebuild-project-s3-log-verschlüsselt
- codebuild-project-source-repo-URL-Prüfung
- codebuild-report-group-encrypted-im Ruhezustand
- codedeploy-auto-rollback-monitor-aktiviert
- codedeploy-deployment-group-auto-Rollback-fähig
- codedeploy-deployment-group-outdated-instanzen-aktualisieren
- codedeploy-ec2- minimum-healthy-hosts-configured
- codedeploy-lambda-allatonce-traffic-shift-deaktiviert
- codeguruprofiler-profiling-group-tagged
- codegururevieweer-repository-association-tagged
- codepipeline-deployment-count-check
- codepipeline-region-fanout-check
- cognito-identity-pool-unauth-Zugriffsprüfung
- cognito-user-pool-advanced-sicherheitsaktiviert
- cognito-user-pool-tagged
- connect-instance-logging-enabled
- customerprofiles-object-type-allow-Profilerstellung
- customerprofiles-object-type-tagged
- custom-eventbus-policy-attached
- custom-schema-registry-policy-angehängt
- cw-loggroup-retention-period-überprüfen
- datasync-task-data-verification-aktiviert
- datasync-task-logging-enabled
- datasync-task-tagged
- dax-encryption-enabled
- dax-tls-endpoint-encryption
- db-instance-backup-enabled
- desired-instance-tenancy

- desired-instance-type
- dms-auto-minor-version-Upgrade-Check
- dms-endpoint-ssl-configured
- dms-endpoint-tagged
- dms-mongo-db-authentication-aktiviert
- dms-neptune-iam-authorization-aktiviert
- dms-redis-tls-enabled
- dms-replication-not-public
- dms-replication-task-sourcedb-Protokollierung
- dms-replication-task-tagged
- dms-replication-task-targetdb-Protokollierung
- docdb-cluster-audit-logging-aktiviert
- docdb-cluster-backup-retention-überprüfen
- docdb-cluster-deletion-protection-aktiviert
- docdb-cluster-encrypted
- docdb-cluster-encrypted-in-Transit
- docdb-cluster-snapshot-public-verboten
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-last-backup-recovery-Punkt-erstellt
- dynamodb-meets-restore-time-ziel
- dynamodb-pitr-enabled
- dynamodb-resources-protected-by-Backup-Plan
- dynamodb-table-deletion-protection-aktiviert
- dynamodb-table-encrypted-kms
- dynamodb-table-encryption-enabled
- dynamodb-throughput-limit-check
- ebs-in-backup-plan
- ebs-last-backup-recovery-Punkt-erstellt

- ebs-meets-restore-time-ziel
- ebs-optimized-instance
- ebs-resources-in-logically-air-gapped-vault
- ebs-resources-protected-by-Backup-Plan
- ebs-snapshot-public-restorable-überprüfen
- ec2- capacity-reservation-tagged
- ec2- carrier-gateway-tagged
- ec2- aktiviert client-vpn-connection-log
- ec2- client-vpn-endpoint-tagged
- ec2- -alle client-vpn-not-authorize
- ec2- dhcp-options-tagged
- ec2- ebs-encryption-by-default
- ec2- aktiviert enis-source-destination-check
- ec2-fleet-markiert
- ec2-imdsv2-check
- ec2- instance-detailed-monitoring-enabled
- ec2-ami instance-launched-with-allowed
- ec2-manager instance-managed-by-systems
- ec2- instance-multiple-eni-check
- ec2- instance-no-public-ip
- ec2- instance-profile-attached
- ec2- erstellt last-backup-recovery-point
- ec2-2-check launch-template-imdsv
- ec2- deaktiviert launch-template-public-ip
- ec2- launch-template-tagged
- ec2- managedinstance-applications-blacklisted
- ec2- managedinstance-applications-required
- ec2-prüfen managedinstance-association-compliance-status
- ec2- managedinstance-inventory-blacklisted

- ec2-prüfen managedinstance-patch-compliance-status
- ec2- managedinstance-platform-check
- ec2- meets-restore-time-target
- ec2-analysis-tagged network-insights-access-scope
- ec2- markiert network-insights-access-scope
- ec2- network-insights-path-tagged
- ec2- no-amazon-key-pair
- ec2- paravirtual-instance-check
- ec2- prefix-list-tagged
- ec2-Gapped-Tresor resources-in-logically-air
- ec2-plan resources-protected-by-backup
- ec2-eni security-group-attached-to
- ec2- security-group-attached-to -einperiodisch
- ec2- - spot-fleet-request-ct encryption-at-rest
- ec2-stopped-instance
- ec2- token-hop-limit-check
- ec2- traffic-mirror-filter-description
- ec2- traffic-mirror-filter-tagged
- ec2- traffic-mirror-session-description
- ec2- traffic-mirror-session-tagged
- ec2- traffic-mirror-target-description
- ec2- traffic-mirror-target-tagged
- ec2- transit-gateway-auto-vpc -attach-deaktiviert
- ec2- markiert transit-gateway-multicast-domain
- ec2- volume-inuse-check
- ec2- vpn-connection-logging-enabled
- ecr-private-image-scanning-aktiviert
- ecr-private-lifecycle-policy-konfiguriert
- ecr-private-tag-immutability-aktiviert

- ecr-repository-cmk-encryption-aktiviert
- ecr-repository-tagged
- ecs-awsvpc-networking-enabled
- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-container-insights-enabled
- ecs-fargate-latest-platform-Ausführung
- ecs-no-environment-secrets
- ecs-task-definition-log-Konfiguration
- ecs-task-definition-memory-hartes Limit
- ecs-task-definition-network-mode-not-host
- ecs-task-definition-nonroot-benutzer
- ecs-task-definition-pid-Modusprüfung
- ecs-task-definition-user-for-host-mode-check
- efs-access-point-enforce-root-Verzeichnis
- efs-access-point-enforce-Benutzeridentität
- efs-automatic-backups-enabled
- efs-encrypted-check
- efs-filesystem-ct-encrypted
- efs-in-backup-plan
- efs-last-backup-recovery-Punkt-erstellt
- efs-meets-restore-time-ziel
- efs-mount-target-public-zugänglich
- efs-resources-in-logically-air-gapped-vault
- efs-resources-protected-by-Backup-Plan
- eip-attached
- eks-cluster-logging-enabled
- eks-cluster-log-enabled
- eks-cluster-oldest-supported-Ausführung

- eks-cluster-secrets-encrypted
- eks-cluster-supported-version
- eks-endpoint-no-public-Zugang
- eks-secrets-encrypted
- elasticache-auto-minor-version-Upgrade-Check
- elasticache-rbac-auth-enabled
- elasticache-redis-cluster-automatic-Backup-Check
- elasticache-repl-grp-auto-Failover-fähig
- elasticache-repl-grp-encrypted-im Ruhezustand
- elasticache-repl-grp-encryptedim Transit
- elasticache-repl-grp-redis-auth-aktiviert
- elasticache-subnet-group-check
- elasticache-supported-engine-version
- elasticbeanstalk-application-description
- elasticbeanstalk-application-version-description
- elasticbeanstalk-environment-description
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch
- elasticsearch-node-to-node-Verschlüsselungsprüfung
- elastic-beanstalk-logs-to-Wolkenbeobachtung
- elastic-beanstalk-managed-updates-aktiviert
- ELV 2- acm-certificate-required
- ELV 2- listener-encryption-in-transit
- elbv2-multiple-az
- elbv2-check predefined-security-policy-ssl
- elb-acm-certificate-required
- elb-cross-zone-load-Balancing aktiviert
- elb-custom-security-policy-ssl-Prüfung

- elb-deletion-protection-enabled
- elb-logging-enabled
- elb-predefined-security-policy-ssl-Prüfung
- elb-tls-https-listeners-nur
- emr-block-public-access
- emr-kerberos-enabled
- emr-master-no-public-ip
- emr-security-configuration-encryption-ausruhen
- emr-security-configuration-encryption-Transit
- encrypted-volumes
- event-data-store-cmk-Verschlüsselung aktiviert
- evidently-launch-description
- evidently-launch-tagged
- evidently-project-description
- evidently-project-tagged
- evidently-segment-description
- evidently-segment-tagged
- fis-experiment-template-log-Konfiguration vorhanden
- fis-experiment-template-tagged
- fms-shield-resource-policy-überprüfen
- fms-webacl-resource-policy-überprüfen
- fms-webacl-rulegroup-association-überprüfen
- frauddetector-entity-type-tagged
- frauddetector-label-tagged
- frauddetector-outcome-tagged
- frauddetector-variable-tagged
- fsx-last-backup-recovery-Punkt-erstellt
- fsx-lustre-copy-tagszu Backups
- fsx-meets-restore-time-ziel

- fsx-ontap-deployment-type-überprüfen
- fsx-openzfs-copy-tags-aktiviert
- fsx-openzfs-deployment-type-überprüfen
- fsx-resources-protected-by-Backup-Plan
- fsx-windows-audit-log-konfiguriert
- fsx-windows-deployment-type-überprüfen
- glb-listener-tagged
- global-endpoint-event-replication-aktiviert
- glue-job-logging-enabled
- glue-ml-transform-encrypted-im Ruhezustand
- glue-spark-job-supported-Ausführung
- Schutzzoll-ec2- protection-runtime-enabled
- guardduty-ecs-protection-runtime-aktiviert
- guardduty-eks-protection-audit-aktiviert
- guardduty-eks-protection-runtime-aktiviert
- guardduty-enabled-centralized
- guardduty-lambda-protection-enabled
- guardduty-malware-protection-enabled
- guardduty-non-archived-findings
- guardduty-rds-protection-enabled
- guardduty-runtime-monitoring-enabled
- GuardDuty-S3-Schutz aktiviert
- iam-customer-policy-blocked-kms-Aktionen
- iam-external-access-analyzer-aktiviert
- iam-group-has-users-überprüfen
- iam-inline-policy-blocked-kms-Aktionen
- iam-no-inline-policy-überprüfen
- iam-oidc-provider-tagged
- iam-password-policy

- iam-policy-blacklisted-check
- iam-policy-in-use
- iam-policy-no-statements-with-admin-access
- iam-policy-no-statements-with-full-access
- iam-role-managed-policy-überprüfen
- iam-root-access-key-überprüfen
- iam-saml-provider-tagged
- iam-server-certificate-expiration-überprüfen
- iam-server-certificate-tagged
- iam-user-group-membership-überprüfen
- iam-user-mfa-enabled
- iam-user-no-policies-überprüfen
- iam-user-unused-credentials-überprüfen
- restricted-ssh
- inspector-ec2-Scan aktiviert
- inspector-ecr-scan-enabled
- inspector-lambda-code-scan-aktiviert
- inspector-lambda-standard-scan-aktiviert
- ec2- instances-in-vpc
- internet-gateway-authorized-vpc-nur
- iotevents-alarm-model-tagged
- iotevents-detector-model-tagged
- iotevents-input-tagged
- iotsitewise-asset-model-tagged
- iotsitewise-dashboard-tagged
- iotsitewise-gateway-tagged
- iotsitewise-portal-tagged
- iotsitewise-project-tagged
- iottwinmaker-component-type-tagged
- iottwinmaker-entity-tagged

- iottwinmaker-scene-tagged
- iottwinmaker-sync-job-tagged
- iottwinmaker-workspace-tagged
- iotwireless-fuota-task-tagged
- iotwireless-multicast-group-tagged
- iotwireless-service-profile-tagged
- iot-authorizer-token-signing-aktiviert
- ivs-channel-playback-authorization-aktiviert
- ivs-channel-tagged
- ivs-playback-key-pair-markiert
- ivs-recording-configuration-tagged
- kinesis-firehose-delivery-stream-verschlüsselt
- kinesis-stream-backup-retention-überprüfen
- kinesis-stream-encrypted
- kms-cmk-not-scheduled-zum Löschen
- kms-key-policy-no-öffentlich zugänglich
- lambda-concurrency-check
- lambda-dlq-check
- lambda-function-public-access-verboten
- lambda-function-settings-check
- lambda-function-xray-enabled
- lambda-inside-vpc
- lambda-vpc-multi-az-überprüfen
- lightsail-bucket-tagged
- lightsail-certificate-tagged
- lightsail-disk-tagged
- macie-auto-sensitive-data-Discovery-Check
- macie-status-check
- mariadb-publish-logs-to-Cloudwatch-Protokolle
- mfa-enabled-for-iam-Konsolenzugriff

- mq-active-broker-ldap-Authentifizierung
- mq-active-deployment-mode
- mq-active-single-instance-broker-storage-type-efs
- mq-automatic-minor-version-upgrade-fähig
- mq-auto-minor-version-upgrade-fähig
- mq-broker-general-logging-aktiviert
- mq-cloudwatch-audit-logging-aktiviert
- mq-cloudwatch-audit-log-aktiviert
- mq-no-public-access
- mq-rabbit-deployment-mode
- msk-cluster-public-access-deaktiviert
- msk-connect-connector-logging-aktiviert
- msk-enhanced-monitoring-enabled
- msk-in-cluster-node-TLS erforderlich
- msk-unrestricted-access-check
- multi-region-cloudtrail-enabled
- nacl-no-unrestricted-ssh-rdp
- neptune-cluster-backup-retention-überprüfen
- neptune-cluster-cloudwatch-log-exportfähig
- neptune-cluster-copy-tags-to-snapshot-enabled
- neptune-cluster-deletion-protection-aktiviert
- neptune-cluster-encrypted
- neptune-cluster-iam-database-Authentifizierung
- neptune-cluster-multi-az-aktiviert
- neptune-cluster-snapshot-encrypted
- neptune-cluster-snapshot-public-verboten
- netfw-deletion-protection-enabled
- netfw-logging-enabled
- netfw-multi-az-enabled
- netfw-policy-default-action-fragment-Pakete

- netfw-policy-default-action-vollständige Pakete
- netfw-policy-rule-group-assoziiert
- netfw-stateless-rule-group-nicht leer
- netfw-subnet-change-protection-aktiviert
- nlb-cross-zone-load-Balancing aktiviert
- nlb-internal-scheme-check
- nlb-listener-tagged
- nlb-logging-enabled
- no-unrestricted-route-to-igw
- opensearch-access-control-enabled
- opensearch-audit-logging-enabled
- opensearch-data-node-fault-Toleranz
- opensearch-encrypted-at-rest
- opensearch-https-required
- opensearch-in-vpc-only
- opensearch-logs-to-cloudwatch
- opensearch-node-to-node-Verschlüsselungsprüfung
- opensearch-primary-node-fault-Toleranz
- opensearch-update-check
- rabbit-mq-supported-version
- rds-aurora-mysql-audit-Protokollierung aktiviert
- rds-aurora-postgresql-logs-zu-Cloud-Watch
- rds-automatic-minor-version-upgrade-fähig
- rds-cluster-auto-minor-version-upgrade-enable
- rds-cluster-default-admin-überprüfen
- rds-cluster-deletion-protection-aktiviert
- rds-cluster-encrypted-at-ausruhen
- rds-cluster-iam-authentication-aktiviert
- rds-cluster-multi-az-aktiviert
- rds-db-security-group-nicht erlaubt

- rds-enhanced-monitoring-enabled
- rds-instance-default-admin-überprüfen
- rds-instance-deletion-protection-aktiviert
- rds-instance-iam-authentication-aktiviert
- rds-instance-public-access-überprüfen
- rds-instance-subnet-igw-überprüfen
- rds-in-backup-plan
- rds-last-backup-recovery-Punkt-erstellt
- rds-logging-enabled
- rds-mariadb-instance-encryptedim Transit
- rds-meets-restore-time-ziel
- rds-multi-az-support
- rds-mysql-instance-encryptedim Transit
- rds-postgresql-logs-to-Wolkenbeobachtung
- rds-postgres-instance-encryptedim Transit
- rds-proxy-tls-encryption
- rds-resources-protected-by-Backup-Plan
- rds-snapshots-public-prohibited
- rds-snapshot-encrypted
- rds-sqlserver-encrypted-in-Transit
- rds-sql-server-logs-zu-Cloud-Watch
- rds-storage-encrypted
- redshift-audit-logging-enabled
- redshift-backup-enabled
- redshift-cluster-configuration-check
- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check
- redshift-cluster-multi-az-aktiviert
- redshift-cluster-parameter-group-markiert
- redshift-cluster-public-access-überprüfen

- redshift-cluster-subnet-group-Multi-AZ
- redshift-default-admin-check
- redshift-default-db-name-überprüfen
- redshift-enhanced-vpc-routing-aktiviert
- redshift-require-tls-ssl
- redshift-serverless-default-admin-überprüfen
- redshift-serverless-default-db-Namenscheck
- redshift-serverless-namespace-cmk-Verschlüsselung
- redshift-serverless-publish-logs-to-cloudwatch
- redshift-serverless-workgroup-encryptedim Transit
- redshift-serverless-workgroup-no-öffentlich zugänglich
- redshift-serverless-workgroup-routes-innerhalb von VPC
- redshift-unrestricted-port-access
- required-tags
- restricted-common-ports
- root-account-hardware-mfa-aktiviert
- root-account-mfa-enabled
- Route 53- query-logging-enabled
- s3 express-dir-bucket-lifecycle -regel-check
- nur s3 access-point-in-vpc -
- access-point-public-accesss3-Blöcke
- account-level-public-accesss3-Blöcke
- account-level-public-accesss3-Blöcke-periodisch
- s-3 bucket-acl-prohibited
- s-3 bucket-blacklisted-actions-prohibited
- bucket-cross-region-replications3-fähig
- s-3 bucket-default-lock-enabled
- s3 bucket-level-public-access - verboten
- s-3 bucket-logging-enabled
- s-3 bucket-mfa-delete-enabled

- s-3 bucket-policy-grantee-check
- bucket-policy-not-mores3-permissiv
- s-3 bucket-public-read-prohibited
- s-3 bucket-public-write-prohibited
- s-3 bucket-replication-enabled
- bucket-server-side-encryptions3-fähig
- s-3 bucket-ssl-requests-only
- s3-bucket-tagged
- s-3 bucket-versioning-enabled
- s-3 default-encryption-kms
- s-3 event-notifications-enabled
- s3 last-backup-recovery-point - erstellt
- s-3 lifecycle-policy-check
- s-3 meets-restore-time-target
- resources-in-logically-airS3-Gapped-Tresor
- resources-protected-by-backups3-plan
- s-3 version-lifecycle-policy-check
- sagemaker-app-image-config-markiert
- sagemaker-domain-in-vpc
- sagemaker-domain-tagged
- sagemaker-endpoint-configuration-kms-schlüsselkonfiguriert
- sagemaker-endpoint-config-prod-Instanzenanzahl
- sagemaker-feature-group-tagged
- sagemaker-image-description
- sagemaker-image-tagged
- sagemaker-model-in-vpc
- sagemaker-model-isolation-enabled
- sagemaker-notebook-instance-inside-vpc
- sagemaker-notebook-instance-kms-schlüsselkonfiguriert
- sagemaker-notebook-instance-platform-Ausführung

- sagemaker-notebook-instance-root-Zugriffsprüfung
- sagemaker-notebook-no-direct-Internetzugang
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-überprüfen
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- securityhub-enabled
- security-account-information-provided
- service-catalog-shared-within-Organisation
- service-vpc-endpoint-enabled
- ses-malware-scanning-enabled
- shield-advanced-enabled-autorenew
- shield-drt-access
- sns-encrypted-kms
- sns-topic-message-delivery-Benachrichtigung aktiviert
- sns-topic-no-public-Zugang
- sqs-queue-no-public-Zugang
- ssm-automation-block-public-teilen
- ssm-automation-logging-enabled
- ssm-document-not-public
- ssm-document-tagged
- step-functions-state-machine-Protokollierung aktiviert
- storagegateway-last-backup-recovery-Punkt-erstellt
- storagegateway-resources-in-logically-air-gapped-vault
- storagegateway-resources-protected-by-Backup-Plan
- subnet-auto-assign-public-ip-deaktiviert
- transfer-agreement-description
- transfer-agreement-tagged
- transfer-certificate-description

- transfer-certificate-tagged
- transfer-connector-logging-enabled
- transfer-connector-tagged
- transfer-family-server-no-ftp
- transfer-profile-tagged
- transfer-workflow-description
- transfer-workflow-tagged
- virtualmachine-last-backup-recovery-Punkt-erstellt
- virtualmachine-resources-in-logically-air-gapped-vault
- virtualmachine-resources-protected-by-Backup-Plan
- vpc-default-security-group-geschlossen
- vpc-endpoint-enabled
- vpc-flow-logs-enabled
- vpc-network-acl-unused-überprüfen
- vpc-peering-dns-resolution-überprüfen
- vpc-sg-open-only-to-authorized-ports
- vpc-sg-port-restriction-überprüfen
- vpc-vpn-2-tunnels-up
- wafv2-logging-enabled
- WAF 2- rulegroup-logging-enabled
- WAF 2- rulegroup-not-empty
- WAF 2- webacl-not-empty
- waf-classic-logging-enabled
- waf-global-rulegroup-not-leer
- waf-global-rule-not-leer
- waf-global-webacl-not-leer
- waf-regional-rulegroup-not-leer
- waf-regional-rule-not-leer
- waf-regional-webacl-not-leer
- workspaces-root-volume-encryption-aktiviert

- workspaces-user-volume-encryption-aktiviert

access-keys-rotated

Prüft, ob aktive IAM-Zugriffsschlüssel innerhalb der in `maxAccessKeyAge` angegebenen Anzahl an Tagen rotiert (gewechselt) werden. Die Regel ist NON_COMPLIANT, wenn die Zugriffsschlüssel nicht innerhalb des angegebenen Zeitraums rotiert werden. Der Standardwert lautet 90 Tage.

> **Warning**
>
> Geben Sie Ihre Zugangsschlüssel nicht an Unbefugte weiter, auch nicht, um Ihre Kontokennungen zu finden. Wenn Sie dies tun, gewähren Sie anderen Personen möglicherweise den permanenten Zugriff auf Ihr Konto. Als bewährte Sicherheitsmethode empfiehlt es sich, Passwörter und Zugriffsschlüssel zu entfernen, wenn die Benutzer diese nicht mehr benötigen.

> **Note**
>
> In der Konsole als nicht konform markierter Ressourcentyp
> Wenn diese Regel feststellt, dass einer Ihrer Zugriffsschlüssel nicht konform ist, wird der `AWS::IAM::User` Ressourcentyp auch in der Konsole als nicht konform markiert. AWS Verwaltete Regeln und globale IAM-Ressourcentypen
> Die globalen IAM-Ressourcentypen, die vor Februar 2022 eingeführt wurden (`AWS::IAM::Group`,, und`AWS::IAM::User`) `AWS::IAM::Policy`AWS::IAM::Role, können nur AWS Config in AWS Regionen erfasst werden, in denen sie vor Februar 2022 verfügbar AWS Config waren. Diese Ressourcentypen können nicht in Regionen erfasst werden, die AWS Config nach Februar 2022 unterstützt werden. Eine Liste dieser Regionen finden Sie unter AWS Aufzeichnungsressourcen | Globale Ressourcen.
> Wenn Sie einen globalen IAM-Ressourcentyp in mindestens einer Region aufzeichnen, führen periodische Regeln, die die Einhaltung des globalen IAM-Ressourcentyps melden, Bewertungen in allen Regionen durch, in denen die periodische Regel hinzugefügt wurde, auch wenn Sie die Aufzeichnung des globalen IAM-Ressourcentyps in der Region, in der die periodische Regel hinzugefügt wurde, nicht aktiviert haben.
> Um unnötige Bewertungen zu vermeiden, sollten Sie nur regelmäßige Regeln einrichten, die die Einhaltung der Vorschriften für einen globalen IAM-Ressourcentyp an eine der unterstützten Regionen melden. Eine Liste der verwalteten Regeln, die in welchen Regionen

unterstützt werden, finden Sie unter Liste der AWS Config verwalteten Regeln nach regionaler Verfügbarkeit.
Einschränkungen
Diese Regel gilt nicht für AWS Root-Benutzerzugriffsschlüssel für Konten. Um Ihre Root-Benutzerzugriffsschlüssel zu löschen oder zu rotieren, melden Sie sich mit Ihren Root-Benutzeranmeldedaten auf der Seite Meine Sicherheitsanmeldedaten AWS Management Console unter anhttps://aws.amazon.com/console/.

ID: ACCESS_KEYS_ROTATED

Ressourcentypen: AWS::IAM::User

Auslösertyp: Regelmäßig

AWS-Region: Alle unterstützten AWS Regionen außer Asien-Pazifik (Thailand), Naher Osten (VAE), Asien-Pazifik (Hyderabad), Asien-Pazifik (Malaysia), Asien-Pazifik (Melbourne), Mexiko (Zentral), Israel (Tel Aviv), Asien-Pazifik (Taipeh), Kanada West (Calgary), Europa (Spanien), Europa (Zürich)

Parameter:

maxAccessKeyAlter, Typ: int, Standard: 90

Maximale Anzahl von Tagen ohne Rotation. Standard: 90.

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

account-part-of-organizations

Prüft, ob ein AWS Konto Teil von AWS Organizations ist. Die Regel lautet NON_COMPLIANT, wenn ein AWS Konto nicht Teil von AWS Organizations ist oder die Masterkonto-ID der AWS Organizations nicht mit dem Regelparameter übereinstimmt. `MasterAccountId`

> **Note**
>
> Verwaltete Regeln und globale IAM-Ressourcentypen

Die globalen IAM-Ressourcentypen, die vor Februar 2022 eingeführt wurden (`AWS::IAM::Group`,, und`AWS::IAM::User`) `AWS::IAM::Policy``AWS::IAM::Role`, können nur AWS Config in AWS Regionen erfasst werden, in denen sie vor Februar 2022 verfügbar AWS Config waren. Diese Ressourcentypen können nicht in Regionen erfasst werden, die AWS Config nach Februar 2022 unterstützt werden. Eine Liste dieser Regionen finden Sie unter AWS Ressourcen für die Aufzeichnung | Globale Ressourcen.
Wenn Sie einen globalen IAM-Ressourcentyp in mindestens einer Region aufzeichnen, führen periodische Regeln, die die Einhaltung des globalen IAM-Ressourcentyps melden, Bewertungen in allen Regionen durch, in denen die periodische Regel hinzugefügt wurde, auch wenn Sie die Aufzeichnung des globalen IAM-Ressourcentyps in der Region, in der die periodische Regel hinzugefügt wurde, nicht aktiviert haben.
Um unnötige Bewertungen zu vermeiden, sollten Sie nur regelmäßige Regeln einrichten, die die Einhaltung der Vorschriften für einen globalen IAM-Ressourcentyp an eine der unterstützten Regionen melden. Eine Liste der verwalteten Regeln, die in welchen Regionen unterstützt werden, finden Sie unter Liste der AWS Config verwalteten Regeln nach Verfügbarkeit in Regionen.

ID: ACCOUNT_PART_OF_ORGANIZATIONS

Auslösertyp: Regelmäßig

AWS-Region: Alle unterstützten AWS Regionen außer China (Peking) und Asien-Pazifik (Taipeh)

Parameter:

MasterAccountId (Fakultativ), Typ: Zeichenfolge

Die Hauptkonto-ID für ein AWS Konto.

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

acmpca-certificate-authority-tagged

Prüft, ob AWS private CA-Zertifizierungsstellen über Tags verfügen. Optional können Sie Tag-Schlüssel angeben. Die Regel lautet NON_COMPLIANT, wenn keine Tags vorhanden sind oder

wenn die angegebenen Tag-Schlüssel nicht vorhanden sind. Die Regel sucht nicht nach Tags, die mit 'aws: 'beginnen.

Kennung: ACMPCA_CERTIFICATE_AUTHORITY_TAGGED

Ressourcentypen: AWS::ACMPCA::CertificateAuthority

Auslösertyp: Konfigurationsänderungen

AWS-Region: Alle unterstützten AWS Regionen außer China (Peking), Asien-Pazifik (Thailand), Asien-Pazifik (Malaysia), AWS GovCloud (USA-Ost), AWS GovCloud (US-West), Mexiko (Zentral), China (Ningxia)

Parameter:

requiredKeyTags (Fakultativ), Typ: CSV

> Durch Kommas getrennte Liste von Tag-Schlüsseln, die von der Regel überprüft werden sollen. Falls angegeben, lautet die Regel NON_COMPLIANT, wenn die ausgewertete Ressource diese Schlüssel nicht enthält. Bei Tag-Schlüsseln wird die Groß- und Kleinschreibung beachtet. Tag-Schlüssel, die mit „aws:“ beginnen, sind nicht erlaubt.

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

acm-certificate-expiration-check

Prüft, ob die AWS Certificate Manager-Zertifikate in Ihrem Konto so gekennzeichnet sind, dass sie innerhalb der angegebenen Anzahl von Tagen ablaufen. Von ACM bereitgestellte Zertifikate werden automatisch verlängert. ACM verlängert von Ihnen importierte Zertifikate nicht automatisch. Die Regel ist NON_COMPLIANT, wenn Ihre Zertifikate bald ablaufen.

ID: ACM_CERTIFICATE_EXPIRATION_CHECK

Ressourcentypen: AWS::ACM::Certificate

Auslösertyp: „Konfigurationsänderungen“ und „Regelmäßig“

AWS-Region: Alle unterstützten AWS Regionen außer der Region Asien-Pazifik (Osaka)

Parameter:

daysToExpiration (Fakultativ), Typ: int, Standard: 14

Geben Sie den Zeitraum in Tagen an, nach dem die Regel des ACM-Zertifikats als nicht konform gekennzeichnet wird.

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

acm-certificate-rsa-check

Überprüft, ob von AWS Certificate Manager (ACM) verwaltete RSA-Zertifikate eine Schlüssellänge von mindestens '2048' Bit haben. Die Regel lautet NON_COMPLIANT, wenn die Mindestschlüssellänge weniger als 2048 Bit beträgt.

ID: ACM_CERTIFICATE_RSA_CHECK

Ressourcentypen: AWS::ACM::Certificate

Auslösertyp: Konfigurationsänderungen

AWS-Region: Alle unterstützten AWS Regionen außer China (Peking), Asien-Pazifik (Thailand), Asien-Pazifik (Malaysia), AWS GovCloud (USA-Ost), AWS GovCloud (US-West), Mexiko (Zentral), Kanada West (Calgary), China (Ningxia)

Parameter:

Keine

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

acm-pca-root-ca-deaktiviert

Prüft, ob die AWS Private Certificate Authority (AWS Private CA) über eine deaktivierte Stammzertifizierungsstelle verfügt. Die Regel ist NON_COMPLIANT für Root-Benutzer CAs mit einem Status, der nicht DEAKTIVIERT ist.

ID: ACM_PCA_ROOT_CA_DISABLED

Ressourcentypen: AWS::ACMPCA::CertificateAuthority

Auslösertyp: Regelmäßig

AWS-Region: Alle unterstützten AWS Regionen außer China (Peking), Asien-Pazifik (Thailand), Asien-Pazifik (Malaysia), AWS GovCloud (USA-Ost), AWS GovCloud (US-West), Mexiko (Zentral), Kanada West (Calgary), China (Ningxia)

Parameter:

ausgenommen (optional) CAArns , Typ: CSV

> Durch Kommata getrennte Liste der Amazon-Ressourcennamen (ARN) der Zertifizierungsstellen, die aktiviert werden können. Dieser Wert kann für andere Zertifizierungsstellen angegeben werden CAs, z. B. für bestimmte Stamm CAs - oder Zwischenzertifizierungsstellen, die aktiviert werden können.

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

active-mq-supported-version

Prüft, ob ein Amazon MQ ActiveMQ-Broker auf einer bestimmten unterstützten Engine-Mindestversion läuft. Die Regel lautet NON_COMPLIANT, wenn der ActiveMQ-Broker nicht auf der von Ihnen angegebenen Mindestversion der unterstützten Engine ausgeführt wird.

Kennung: ACTIVE_MQ_SUPPORTED_VERSION

Ressourcentypen: AWS::AmazonMQ::Broker

Auslösertyp: Konfigurationsänderungen

AWS-Region: Alle unterstützten AWS Regionen außer Asien-Pazifik (Thailand), Asien-Pazifik (Hyderabad), Asien-Pazifik (Malaysia), Asien-Pazifik (Melbourne), Mexiko (Zentral), Israel (Tel Aviv), Kanada West (Calgary), Europa (Spanien), Europa (Zürich)

Parameter:

supportedEngineVersion, Typ: Zeichenfolge

Zeichenkettenwert für die Regel zur Überprüfung der unterstützten Mindestversion der Engine für den ActiveMQ-Broker. ActiveMQ-Broker verwenden eine semantische Versionsspezifikation: X.Y.Z. X bezeichnet die Hauptversion, Y steht für die Nebenversion und Z bezeichnet die Patch-Version.

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

alb-desync-mode-check

Prüft, ob für einen Application Load Balancer (ALB) ein benutzerdefinierter desynchroner Mitigationsmodus konfiguriert ist. Die Regel ist NON_COMPLIANT, wenn der desynchrone Mitigationsmodus der ALBs nicht mit dem benutzerdefinierten desynchronen Mitigationsmodus übereinstimmt.

ID: ALB_DESYNC_MODE_CHECK

Ressourcentypen: AWS::ElasticLoadBalancingV2::LoadBalancer

Auslösertyp: Konfigurationsänderungen

AWS-Region: Alle unterstützten AWS Regionen außer Asien-Pazifik (Thailand), Asien-Pazifik (Malaysia), Mexiko (Zentral) und Kanada West (Calgary)

Parameter:

desyncMode, Typ: CSV

Durch Kommata getrennte Liste, in der Kunden maximal zwei dieser Werte wählen können: „Defensiv“, „Am strengsten“ und „Überwachen“.

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

alb-http-drop-invalid-Header-fähig

Überprüft, ob die Regel AWS Application Load Balancer (ALB) auswertet, um sicherzustellen, dass sie so konfiguriert sind, dass sie HTTP-Header löschen. Die Regel ist NON_COMPLIANT, wenn der Wert für routing.http.drop_invalid_header_fields.enabled auf „False“ festgelegt ist.

ID: ALB_HTTP_DROP_INVALID_HEADER_ENABLED

Ressourcentypen: AWS::ElasticLoadBalancingV2::LoadBalancer

Auslösertyp: Konfigurationsänderungen

AWS-Region: Alle unterstützten AWS Regionen außer der Region Asien-Pazifik (Osaka)

Parameter:

Keine

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

alb-http-to-https-Weiterleitungsprüfung

Prüft, ob auf allen HTTP-Listenern von Application Load Balancers die HTTP-zu-HTTPS-Umleitung konfiguriert ist. Die Regel ist NON_COMPLIANT, wenn für einen oder mehrere HTTP-Listener von Application Load Balancers keine HTTP-zu-HTTPS-Umleitung konfiguriert ist. Die Regel ist auch NON_COMPLIANT, wenn einer oder mehrere HTTP-Listener eine Weiterleitung an einen HTTP-Listener anstelle einer Umleitung verwenden.

ID: ALB_HTTP_TO_HTTPS_REDIRECTION_CHECK

Ressourcentypen: AWS::ElasticLoadBalancingV2::LoadBalancer

Auslösertyp: Regelmäßig

AWS-Region: Alle unterstützten AWS Regionen außer der Region Asien-Pazifik (Osaka)

Parameter:

Keine

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

alb-internal-scheme-check

Prüft, ob ein Application Load Balancer Balancer-Schema intern ist. Die Regel ist NON_COMPLIANT, wenn configuration.scheme nicht auf internal gesetzt ist.

Kennung: ALB_INTERNAL_SCHEME_CHECK

Ressourcentypen: AWS::ElasticLoadBalancingV2::LoadBalancer

Auslösertyp: Konfigurationsänderungen

AWS-Region: Alle unterstützten AWS Regionen außer China (Peking), Asien-Pazifik (Thailand), Asien-Pazifik (Malaysia), AWS GovCloud (USA-Ost), AWS GovCloud (US-West), Mexiko (Zentral), China (Ningxia)

Parameter:

Keine

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

alb-listener-tagged

Prüft, ob Application Load Balancer Balancer-Listener über Tags verfügen. Optional können Sie Tag-Schlüssel angeben. Die Regel lautet NON_COMPLIANT, wenn keine Tags vorhanden sind oder wenn die angegebenen Tag-Schlüssel nicht vorhanden sind. Die Regel sucht nicht nach Tags, die mit 'aws: 'beginnen.

Kennung: ALB_LISTENER_TAGGED

Ressourcentypen: AWS::ElasticLoadBalancingV2::Listener

Auslösertyp: Konfigurationsänderungen

AWS-Region: Alle unterstützten AWS Regionen außer China (Peking), Asien-Pazifik (Thailand), Asien-Pazifik (Jakarta), Naher Osten (VAE), Asien-Pazifik (Hyderabad), Asien-Pazifik (Malaysia), Asien-Pazifik (Melbourne), AWS GovCloud (US-Ost), AWS GovCloud (US-West), Mexiko (Zentral), Israel (Tel Aviv), Kanada West (Calgary), Europa (Spanien), China (Ningxia), Europa (Zürich)

Parameter:

requiredKeyTags (Fakultativ), Typ: CSV

> Durch Kommas getrennte Liste von Tag-Schlüsseln, die von der Regel überprüft werden sollen. Falls angegeben, lautet die Regel NON_COMPLIANT, wenn die ausgewertete Ressource diese Schlüssel nicht enthält. Bei Tag-Schlüsseln wird die Groß- und Kleinschreibung beachtet. Tag-Schlüssel, die mit „aws:“ beginnen, sind nicht erlaubt.

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

alb-waf-enabled

Prüft, ob AWS WAF auf Application Load Balancers () aktiviert ist. ALBs Die Regel ist NON_COMPLIANT, wenn der Schlüssel „waf.enabled“ auf „False“ festgelegt ist.

ID: ALB_WAF_ENABLED

Ressourcentypen: AWS::ElasticLoadBalancingV2::LoadBalancer

Auslösertyp: Konfigurationsänderungen

AWS-Region: Alle unterstützten AWS Regionen außer der Region Asien-Pazifik (Osaka)

Parameter:

wafWebAclIDs (optional), Typ: CSV

> Durch Kommas getrennte Liste von Web-ACL-IDs (für WAF) oder Web-ACL-ARN (für WAFV2) bei der Überprüfung auf ALB-Assoziation.

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

amplify-app-branch-auto-löschfähig

Überprüft, ob AWS Amplify-Apps einen Branch in Amplify Hosting automatisch trennen, wenn Sie einen Branch aus Ihrem Git-Repository löschen. Die Regel ist NON_COMPLIANT, wenn sie konfiguriert ist. EnableBranchAutoDeletion ist falsch.

Kennung: AMPLIFY_APP_BRANCH_AUTO_DELETION_ENABLED

Ressourcentypen: AWS::Amplify::App

Auslösertyp: Konfigurationsänderungen

AWS-Region: Alle unterstützten AWS Regionen außer China (Peking), Asien-Pazifik (Thailand), Asien-Pazifik (Jakarta), Afrika (Kapstadt), Naher Osten (VAE), Asien-Pazifik (Hyderabad), Asien-Pazifik (Malaysia), Asien-Pazifik (Melbourne), AWS GovCloud (US-Ost), AWS GovCloud (US-West), Mexiko (Zentral), Israel (Tel Aviv), Kanada West (Calgary), Europa (Spanien), China (Ningxia), Europa (Region Zürich

Parameter:

Keine

AWS CloudFormation Schablone

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

amplify-app-description

Prüft, ob AWS Amplify-Apps eine Beschreibung haben. Die Regel ist NON_COMPLIANT, wenn Configuration.Description nicht existiert oder eine leere Zeichenfolge ist.

Kennung: AMPLIFY_APP_DESCRIPTION

Ressourcentypen: AWS::Amplify::App

Auslösertyp: Konfigurationsänderungen

AWS-Region: Alle unterstützten AWS Regionen außer China (Peking), Asien-Pazifik (Thailand), Asien-Pazifik (Jakarta), Afrika (Kapstadt), Naher Osten (VAE), Asien-Pazifik (Hyderabad), Asien-Pazifik (Malaysia), Asien-Pazifik (Melbourne), AWS GovCloud (US-Ost), AWS GovCloud (US-West), Mexiko (Zentral), Israel (Tel Aviv), Kanada West (Calgary), Europa (Spanien), China (Ningxia), Europa (Region Zürich)

Parameter:

Keine

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

amplify-app-tagged

Prüft, ob AWS Amplify-Apps Tags haben. Optional können Sie Tag-Schlüssel für die Regel angeben. Die Regel ist NON_COMPLIANT, wenn keine Tags vorhanden sind oder wenn die angegebenen Tag-Schlüssel nicht vorhanden sind. Die Regel sucht nicht nach Tags, die mit 'aws: 'beginnen.

Kennung: AMPLIFY_APP_TAGGED

Ressourcentypen: AWS::Amplify::App

Auslösertyp: Konfigurationsänderungen

AWS-Region: Alle unterstützten AWS Regionen außer China (Peking), Asien-Pazifik (Thailand), Asien-Pazifik (Jakarta), Afrika (Kapstadt), Naher Osten (VAE), Asien-Pazifik (Hyderabad), Asien-Pazifik (Malaysia), Asien-Pazifik (Melbourne), AWS GovCloud (US-Ost), AWS GovCloud (US-West), Mexiko (Zentral), Israel (Tel Aviv), Kanada West (Calgary), Europa (Spanien), China (Ningxia), Europa (Region Zürich)

Parameter:

requiredKeyTags (Fakultativ), Typ: CSV

> Durch Kommas getrennte Liste von Tag-Schlüsseln, die von der Regel überprüft werden sollen. Falls angegeben, lautet die Regel NON_COMPLIANT, wenn die ausgewertete Ressource diese Schlüssel nicht enthält. Bei Tag-Schlüsseln wird die Groß- und Kleinschreibung beachtet. Tag-Schlüssel, die mit „aws:“ beginnen, sind nicht erlaubt.

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

amplify-branch-performance-mode-aktiviert

Prüft, ob AWS Amplify Amplify-Zweigen der Leistungsmodus aktiviert ist. Bei der Konfiguration lautet die Regel NON_COMPLIANT. EnablePerformanceMode ist falsch.

Kennung: AMPLIFY_BRANCH_PERFORMANCE_MODE_ENABLED

Ressourcentypen: AWS::Amplify::Branch

Auslösertyp: Konfigurationsänderungen

AWS-Region: Alle unterstützten AWS Regionen außer China (Peking), Asien-Pazifik (Thailand), Asien-Pazifik (Jakarta), Afrika (Kapstadt), Naher Osten (VAE), Asien-Pazifik (Hyderabad), Asien-Pazifik (Malaysia), Asien-Pazifik (Melbourne), AWS GovCloud (US-Ost), AWS GovCloud (US-West), Mexiko (Zentral), Israel (Tel Aviv), Kanada West (Calgary), Europa (Spanien), China (Ningxia), Europa (Region Zürich)

Parameter:

Keine

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

amplify-branch-tagged

Prüft, ob AWS Amplify-Zweige Tags haben. Optional können Sie Tag-Schlüssel für die Regel angeben. Die Regel ist NON_COMPLIANT, wenn keine Tags vorhanden sind oder wenn die angegebenen Tag-Schlüssel nicht vorhanden sind. Die Regel sucht nicht nach Tags, die mit 'aws: 'beginnen.

Kennung: AMPLIFY_BRANCH_TAGGED

Ressourcentypen: AWS::Amplify::Branch

Auslösertyp: Konfigurationsänderungen

AWS-Region: Alle unterstützten AWS Regionen außer China (Peking), Asien-Pazifik (Thailand), Asien-Pazifik (Jakarta), Afrika (Kapstadt), Naher Osten (VAE), Asien-Pazifik (Hyderabad), Asien-Pazifik (Malaysia), Asien-Pazifik (Melbourne), AWS GovCloud (US-Ost), AWS GovCloud (US-West), Mexiko (Zentral), Israel (Tel Aviv), Kanada West (Calgary), Europa (Spanien), China (Ningxia), Europa (Region Zürich)

Parameter:

requiredKeyTags (Fakultativ), Typ: CSV

> Durch Kommas getrennte Liste von Tag-Schlüsseln, die von der Regel überprüft werden sollen. Falls angegeben, lautet die Regel NON_COMPLIANT, wenn die ausgewertete Ressource diese Schlüssel nicht enthält. Bei Tag-Schlüsseln wird die Groß- und Kleinschreibung beachtet. Tag-Schlüssel, die mit „aws:“ beginnen, sind nicht erlaubt.

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

api-gwv2- access-logs-enabled

Prüft, ob für die V2-Stufen von Amazon API Gateway die Zugriffsprotokollierung aktiviert ist. Die Regel lautet NON_COMPLIANT, wenn 'accessLogSettings' in der Stage-Konfiguration nicht vorhanden ist.

Kennung: 2_ACCESS_LOGS_ENABLED API_GWV

Ressourcentypen: AWS::ApiGatewayV2::Stage

Auslösertyp: Konfigurationsänderungen

AWS-Region: Alle unterstützten AWS Regionen außer Asien-Pazifik (Thailand), Asien-Pazifik (Jakarta), Naher Osten (VAE), Asien-Pazifik (Hyderabad), Asien-Pazifik (Malaysia), Asien-Pazifik (Melbourne), AWS GovCloud (USA-Ost), AWS GovCloud (US-West), Mexiko (Zentral), Israel (Tel Aviv), Kanada West (Calgary), Europa (Spanien), Europa (Zürich)

Parameter:

Keine

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

api-gwv2- authorization-type-configured

Prüft, ob für API-Routen von Amazon API Gatewayv2 ein Autorisierungstyp festgelegt ist. Diese Regel ist NON_COMPLIANT, wenn der Autorisierungstyp NONE ist.

Kennung: 2_AUTHORIZATION_TYPE_CONFIGURED API_GWV

Ressourcentypen: AWS::ApiGatewayV2::Route

Auslösertyp: Regelmäßig

AWS-Region: Alle unterstützten AWS Regionen außer Asien-Pazifik (Thailand), Asien-Pazifik (Jakarta), Naher Osten (VAE), Asien-Pazifik (Hyderabad), Asien-Pazifik (Malaysia), Asien-Pazifik (Melbourne), AWS GovCloud (USA-Ost), AWS GovCloud (US-West), Mexiko (Zentral), Israel (Tel Aviv), Kanada West (Calgary), Europa (Spanien), Europa (Zürich)

Parameter:

authorizationType (optional), Typ: Zeichenfolge

> Parameter, mit dem die Autorisierungstypen von API-Routen verglichen werden sollen. Zeichenkettenparameter, die CUSTOM, AWS_IAM, JWT entsprechen, sind gültig.

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

api-gw-associated-with-WAF

Prüft, ob eine Amazon API Gateway Gateway-API-Stufe eine AWS WAF-Web-Zugriffskontrollliste (Web-ACL) verwendet. Die Regel lautet NON_COMPLIANT, wenn keine AWS WAF-Web-ACL verwendet wird oder wenn eine verwendete AWS Web-ACL nicht mit den Angaben im Regelparameter übereinstimmt.

Kennung: _ASSOCIATED_WITH_WAF API_GW

Ressourcentypen: AWS::ApiGateway::Stage

Auslösertyp: Konfigurationsänderungen

AWS-Region: Alle unterstützten AWS Regionen außer Mexiko (Zentral) und Asien-Pazifik (Taipeh)

Parameter:

WebAclArns (Fakultativ), Typ: CSV

Kommagetrennte Liste der Web-ACL-Amazon-Ressourcennamen ()ARNs.

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

api-gw-cache-enabled-und-verschlüsselt

Prüft, ob für alle Methoden in Amazon-API-Gateway-Stufen der Cache aktiviert und verschlüsselt ist. Die Regel ist NON_COMPLIANT, wenn für eine Methode in einer Amazon-API-Gateway-Stufe der Cache nicht konfiguriert oder nicht verschlüsselt ist.

Kennung: _CACHE_ENABLED_AND_ENCRYPTED API_GW

Ressourcentypen: AWS::ApiGateway::Stage

Auslösertyp: Konfigurationsänderungen

AWS-Region: Alle unterstützten AWS Regionen außer Mexiko (Zentral) und Asien-Pazifik (Taipeh)

Parameter:

Keine

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

api-gw-endpoint-type-überprüfen

Prüft, ob Amazon API Gateway APIs dem im Regelparameter angegebenen Typ entsprichtendpointConfigurationType. Die Regel gibt NON_COMPLIANT zurück, wenn die REST-API nicht mit dem Endpunkttyp übereinstimmt, der im Regelparameter konfiguriert ist.

Kennung: API_GW _ENDPOINT_TYPE_CHECK

Ressourcentypen: AWS::ApiGateway::RestApi

Auslösertyp: Konfigurationsänderungen

AWS-Region: Alle unterstützten AWS Regionen außer Mexiko (Zentral) und Asien-Pazifik (Taipeh)

Parameter:

endpointConfigurationTypes, Typ: Zeichenfolge

> Kommagetrennte Liste der zulässigen Werte. endpointConfigurationTypes Zulässige Werte sind REGIONAL, PRIVATE und EDGE.

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

api-gw-execution-logging-aktiviert

Prüft, ob für alle Methoden in Amazon-API-Gateway-Stufen die Protokollierung aktiviert ist. Die Regel ist NON_COMPLIANT, wenn die Protokollierung nicht aktiviert ist oder `loggingLevel` weder ERROR noch INFO lautet.

Kennung: _EXECUTION_LOGGING_ENABLED API_GW

Ressourcentypen:, AWS::ApiGateway::Stage AWS::ApiGatewayV2::Stage

Auslösertyp: Konfigurationsänderungen

AWS-Region: Alle unterstützten AWS Regionen außer Mexiko (Zentral) und Asien-Pazifik (Taipeh)

Parameter:

loggingLevel (optional), Typ: Zeichenfolge, Standard: ERROR, INFO

> Durch Kommata getrennte Liste bestimmter Protokollierungsebenen (z. B. ERROR, INFO oder ERROR,INFO).

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

api-gw-ssl-enabled

Prüft, ob eine REST-API-Stufe ein SSL-Zertifikat verwendet. Die Regel ist NON_COMPLIANT, wenn der REST-API-Stufe kein SSL-Zertifikat zugeordnet ist.

> **Note**
>
> Diese Regel gibt zurück`NOT_APPLICABLE`, wenn die GetIntegrationAPI `AWS` als Typ zurückkehrt.

Kennung: API_GW _SSL_ENABLED

Ressourcentypen: AWS::ApiGateway::Stage

Auslösertyp: Konfigurationsänderungen

AWS-Region: Alle unterstützten AWS Regionen außer Mexiko (Zentral) und Asien-Pazifik (Taipeh)

Parameter:

Zertifikat IDs (optional), Typ: CSV

Durch Kommas getrennte Liste von Client-Zertifikaten, die auf einer REST-API-Phase IDs konfiguriert wurden.

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

api-gw-xray-enabled

Prüft, ob AWS X-Ray Tracing auf Amazon API Gateway REST APIs aktiviert ist. Die Regel ist COMPLIANT, wenn die X-Ray-Ablaufverfolgung aktiviert ist, andernfalls ist sie NON_COMPLIANT.

Kennung: _XRAY_ENABLED API_GW

Ressourcentypen: AWS::ApiGateway::Stage

Auslösertyp: Konfigurationsänderungen

AWS-Region: Alle unterstützten AWS Regionen außer Mexiko (Zentral) und Asien-Pazifik (Taipeh)

Parameter:

Keine

Proaktive Auswertung

Anweisungen zur Ausführung dieser Regel im proaktiven Modus finden Sie unter Evaluieren Ihrer Ressourcen mithilfe von AWS Config Regeln. Damit diese Regel im proaktiven Modus COMPLIANT zurückgibt, muss das Ressourcenkonfigurationsschema für die StartResourceEvaluationAPI die folgenden Eingaben enthalten, die als Zeichenfolge kodiert sind:

```
"ResourceConfiguration":
...
{
   "TracingEnabled": BOOLEAN,
   "RestApiId": "my-rest-api-Id",
}
...
```

Weitere Informationen zur proaktiven Auswertung finden Sie unter Auswertungsmodus.

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

appconfig-application-description

Prüft, ob AWS AppConfig Anwendungen eine Beschreibung haben. Die Regel ist NON_COMPLIANT, wenn Configuration.Description nicht existiert oder eine leere Zeichenfolge ist.

Kennung: APPCONFIG_APPLICATION_DESCRIPTION

Ressourcentypen: AWS::AppConfig::Application

Auslösertyp: Konfigurationsänderungen

AWS-Region: Alle unterstützten AWS Regionen außer China (Peking), Asien-Pazifik (Thailand), Naher Osten (VAE), Asien-Pazifik (Hyderabad), Asien-Pazifik (Malaysia), AWS GovCloud (USA-Ost), AWS GovCloud (US-West), Mexiko (Zentral), Kanada West (Calgary), Europa (Spanien), China (Ningxia), Europa (Zürich)

Parameter:

Keine

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

appconfig-application-tagged

Prüft, ob AWS AppConfig Anwendungen Tags haben. Optional können Sie Tag-Schlüssel angeben, die von der Regel überprüft werden sollen. Die Regel ist NON_COMPLIANT, wenn keine Tags vorhanden sind oder wenn die angegebenen Tag-Schlüssel nicht vorhanden sind. Die Regel sucht nicht nach Tags, die mit 'aws: 'beginnen.

Kennung: APPCONFIG_APPLICATION_TAGGED

Ressourcentypen: AWS::AppConfig::Application

Auslösertyp: Konfigurationsänderungen

AWS-Region: Alle unterstützten AWS Regionen außer China (Peking), Asien-Pazifik (Thailand), Naher Osten (VAE), Asien-Pazifik (Hyderabad), Asien-Pazifik (Malaysia), AWS GovCloud (USA-Ost), AWS GovCloud (US-West), Mexiko (Zentral), Kanada West (Calgary), Europa (Spanien), China (Ningxia), Europa (Zürich)

Parameter:

requiredKeyTags (Fakultativ), Typ: CSV

Durch Kommas getrennte Liste von Tag-Schlüsseln, die von der Regel überprüft werden sollen. Falls angegeben, lautet die Regel NON_COMPLIANT, wenn die ausgewertete Ressource diese

Schlüssel nicht enthält. Bei Tag-Schlüsseln wird die Groß- und Kleinschreibung beachtet. Tag-Schlüssel, die mit „aws:“ beginnen, sind nicht erlaubt.

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

appconfig-configuration-profile-tagged

Prüft, ob AWS AppConfig Konfigurationsprofile Tags haben. Optional können Sie Tag-Schlüssel angeben. Die Regel lautet NON_COMPLIANT, wenn keine Tags vorhanden sind oder wenn die angegebenen Tag-Schlüssel nicht vorhanden sind. Die Regel sucht nicht nach Tags, die mit 'aws: 'beginnen.

Kennung: APPCONFIG_CONFIGURATION_PROFILE_TAGGED

Ressourcentypen: AWS::AppConfig::ConfigurationProfile

Auslösertyp: Konfigurationsänderungen

AWS-Region: Alle unterstützten AWS Regionen außer China (Peking), Asien-Pazifik (Thailand), Naher Osten (VAE), Asien-Pazifik (Hyderabad), Asien-Pazifik (Malaysia), AWS GovCloud (USA-Ost), AWS GovCloud (US-West), Mexiko (Zentral), Kanada West (Calgary), Europa (Spanien), China (Ningxia), Europa (Zürich)

Parameter:

requiredKeyTags (Fakultativ), Typ: CSV

Durch Kommas getrennte Liste von Tag-Schlüsseln, die von der Regel überprüft werden sollen. Falls angegeben, lautet die Regel NON_COMPLIANT, wenn die ausgewertete Ressource diese Schlüssel nicht enthält. Bei Tag-Schlüsseln wird die Groß- und Kleinschreibung beachtet. Tag-Schlüssel, die mit „aws:“ beginnen, sind nicht erlaubt.

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

appconfig-configuration-profile-validators-nicht leer

Überprüft, ob ein AWS AppConfig Konfigurationsprofil mindestens einen Validator für syntaktische oder semantische Prüfungen enthält, um sicherzustellen, dass die Konfiguration wie vorgesehen funktioniert. Die Regel lautet NON_COMPLIANT, wenn die Eigenschaft Validators ein leeres Array ist.

Kennung: APPCONFIG_CONFIGURATION_PROFILE_VALIDATORS_NOT_EMPTY

Ressourcentypen: AWS::AppConfig::ConfigurationProfile

Auslösertyp: Konfigurationsänderungen

AWS-Region: Alle unterstützten AWS Regionen außer China (Peking), Asien-Pazifik (Thailand), Naher Osten (VAE), Asien-Pazifik (Hyderabad), Asien-Pazifik (Malaysia), AWS GovCloud (USA-Ost), AWS GovCloud (US-West), Mexiko (Zentral), Kanada West (Calgary), Europa (Spanien), China (Ningxia), Europa (Zürich)

Parameter:

Keine

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

appconfig-deployment-strategy-description

Prüft, ob die AWS AppConfig Bereitstellungsstrategien eine Beschreibung haben. Die Regel ist NON_COMPLIANT, wenn Configuration.Description nicht existiert oder eine leere Zeichenfolge ist.

Kennung: APPCONFIG_DEPLOYMENT_STRATEGY_DESCRIPTION

Ressourcentypen: AWS::AppConfig::DeploymentStrategy

Auslösertyp: Konfigurationsänderungen

AWS-Region: Alle unterstützten AWS Regionen außer China (Peking), Asien-Pazifik (Thailand), Asien-Pazifik (Malaysia), AWS GovCloud (USA-Ost), AWS GovCloud (US-West), Mexiko (Zentral), China (Ningxia)

Parameter:

Keine

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

appconfig-deployment-strategy-replicate-zu-ssm

Überprüft, ob AWS AppConfig Bereitstellungsstrategien die Bereitstellungsstrategie in einem AWS Systems Manager (SSM) -Dokument speichern. Bei der Konfiguration lautet die Regel NON_COMPLIANT. ReplicateTo ist nicht 'SSM_DOCUMENT'.

Kennung: APPCONFIG_DEPLOYMENT_STRATEGY_REPLICATE_TO_SSM

Ressourcentypen: AWS::AppConfig::DeploymentStrategy

Auslösertyp: Konfigurationsänderungen

AWS-Region: Alle unterstützten AWS Regionen außer China (Peking), Asien-Pazifik (Thailand), Asien-Pazifik (Malaysia), AWS GovCloud (USA-Ost), AWS GovCloud (US-West), Mexiko (Zentral), China (Ningxia)

Parameter:

Keine

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

appconfig-environment-description

Prüft, ob AWS AppConfig Umgebungen eine Beschreibung haben. Die Regel ist NON_COMPLIANT, wenn Configuration.Description nicht existiert oder eine leere Zeichenfolge ist.

Kennung: APPCONFIG_ENVIRONMENT_DESCRIPTION

Ressourcentypen: AWS::AppConfig::Environment

Auslösertyp: Konfigurationsänderungen

AWS-Region: Alle unterstützten AWS Regionen außer China (Peking), Asien-Pazifik (Thailand), Naher Osten (VAE), Asien-Pazifik (Hyderabad), Asien-Pazifik (Malaysia), AWS GovCloud (USA-Ost), AWS GovCloud (US-West), Mexiko (Zentral), Kanada West (Calgary), Europa (Spanien), China (Ningxia), Europa (Zürich)

Parameter:

Keine

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

appconfig-environment-tagged

Prüft, ob AWS AppConfig Umgebungen Tags haben. Optional können Sie Tag-Schlüssel angeben, die von der Regel überprüft werden sollen. Die Regel ist NON_COMPLIANT, wenn keine Tags vorhanden sind oder wenn die angegebenen Tag-Schlüssel nicht vorhanden sind. Die Regel sucht nicht nach Tags, die mit 'aws: 'beginnen.

Kennung: APPCONFIG_ENVIRONMENT_TAGGED

Ressourcentypen: AWS::AppConfig::Environment

Auslösertyp: Konfigurationsänderungen

AWS-Region: Alle unterstützten AWS Regionen außer China (Peking), Asien-Pazifik (Thailand), Naher Osten (VAE), Asien-Pazifik (Hyderabad), Asien-Pazifik (Malaysia), AWS GovCloud (USA-Ost), AWS GovCloud (US-West), Mexiko (Zentral), Kanada West (Calgary), Europa (Spanien), China (Ningxia), Europa (Zürich)

Parameter:

requiredKeyTags (Fakultativ), Typ: CSV

> Durch Kommas getrennte Liste von Tag-Schlüsseln, die von der Regel überprüft werden sollen. Falls angegeben, lautet die Regel NON_COMPLIANT, wenn die ausgewertete Ressource diese Schlüssel nicht enthält. Bei Tag-Schlüsseln wird die Groß- und Kleinschreibung beachtet. Tag-Schlüssel, die mit „aws:“ beginnen, sind nicht erlaubt.

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

appconfig-extension-association-tagged

Prüft, ob AWS AppConfig Erweiterungszuordnungen Tags haben. Optional können Sie Tag-Schlüssel angeben. Die Regel lautet NON_COMPLIANT, wenn keine Tags vorhanden sind oder wenn die angegebenen Tag-Schlüssel nicht vorhanden sind. Die Regel sucht nicht nach Tags, die mit 'aws: 'beginnen.

Kennung: APPCONFIG_EXTENSION_ASSOCIATION_TAGGED

Ressourcentypen: AWS::AppConfig::ExtensionAssociation

Auslösertyp: Konfigurationsänderungen

AWS-Region: Alle unterstützten AWS Regionen außer China (Peking), Asien-Pazifik (Thailand), Asien-Pazifik (Malaysia), AWS GovCloud (USA-Ost), AWS GovCloud (US-West), Mexiko (Zentral), Kanada West (Calgary), China (Ningxia)

Parameter:

requiredKeyTags (Fakultativ), Typ: CSV

> Durch Kommas getrennte Liste von Tag-Schlüsseln, die von der Regel überprüft werden sollen. Falls angegeben, lautet die Regel NON_COMPLIANT, wenn die ausgewertete Ressource diese Schlüssel nicht enthält. Bei Tag-Schlüsseln wird die Groß- und Kleinschreibung beachtet. Tag-Schlüssel, die mit „aws:“ beginnen, sind nicht erlaubt.

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

appconfig-freeform-profile-config-Lagerung

Überprüft, ob Freiform-Konfigurationsprofile ihre Konfigurationsdaten im AWS Secrets Manager oder im AWS AppConfig gehosteten Konfigurationsspeicher speichern. AWS AppConfig Bei der

Konfiguration lautet die Regel NON_COMPLIANT. LocationUri ist weder SecretsManager noch gehostet.

Kennung: APPCONFIG_FREEFORM_PROFILE_CONFIG_STORAGE

Ressourcentypen: AWS::AppConfig::ConfigurationProfile

Auslösertyp: Konfigurationsänderungen

AWS-Region: Alle unterstützten AWS Regionen außer China (Peking), Asien-Pazifik (Thailand), Naher Osten (VAE), Asien-Pazifik (Hyderabad), Asien-Pazifik (Malaysia), AWS GovCloud (USA-Ost), AWS GovCloud (US-West), Mexiko (Zentral), Kanada West (Calgary), Europa (Spanien), China (Ningxia), Europa (Zürich)

Parameter:

Keine

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

appconfig-hosted-configuration-version-Beschreibung

Prüft, ob AWS AppConfig gehostete Konfigurationsversionen eine Beschreibung haben. Die Regel ist NON_COMPLIANT, wenn Configuration.Description nicht existiert oder eine leere Zeichenfolge ist.

Kennung: APPCONFIG_HOSTED_CONFIGURATION_VERSION_DESCRIPTION

Ressourcentypen: AWS::AppConfig::HostedConfigurationVersion

Auslösertyp: Konfigurationsänderungen

AWS-Region: Alle unterstützten AWS Regionen außer China (Peking), Asien-Pazifik (Thailand), Naher Osten (VAE), Asien-Pazifik (Hyderabad), Asien-Pazifik (Malaysia), AWS GovCloud (USA-Ost), AWS GovCloud (US-West), Mexiko (Zentral), Kanada West (Calgary), Europa (Spanien), China (Ningxia), Europa (Zürich)

Parameter:

Keine

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

appflow-flow-tagged

Prüft, ob AppFlow Amazon-Flows Tags haben. Optional können Sie Tag-Schlüssel angeben. Die Regel lautet NON_COMPLIANT, wenn keine Tags vorhanden sind oder wenn die angegebenen Tag-Schlüssel nicht vorhanden sind. Die Regel sucht nicht nach Tags, die mit 'aws: 'beginnen.

Kennung: APPFLOW_FLOW_TAGGED

Ressourcentypen: AWS::AppFlow::Flow

Auslösertyp: Konfigurationsänderungen

AWS-Region: Nur verfügbar in Asien-Pazifik (Mumbai), Europa (Paris), USA Ost (Ohio), Afrika (Kapstadt), Europa (Irland), Europa (Frankfurt), Südamerika (Sao Paulo), USA Ost (Nord-Virginia), Asien-Pazifik (Seoul), Europa (London), Asien-Pazifik (Tokio), USA West (Oregon), USA West (Nordkalifornien), Asien-Pazifik (Singapur), Asien-Pazifik (Sydney), Kanada (Region (Mitte)

Parameter:

requiredKeyTags (Fakultativ), Typ: CSV

> Durch Kommas getrennte Liste von Tag-Schlüsseln, die von der Regel überprüft werden sollen. Falls angegeben, lautet die Regel NON_COMPLIANT, wenn die ausgewertete Ressource diese Schlüssel nicht enthält. Bei Tag-Schlüsseln wird die Groß- und Kleinschreibung beachtet. Tag-Schlüssel, die mit „aws:“ beginnen, sind nicht erlaubt.

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

appintegrations-event-integration-description

Prüft, ob AppIntegrations Amazon-Eventintegrationen eine Beschreibung haben. Die Regel ist NON_COMPLIANT, wenn Configuration.Description nicht existiert.

Kennung: APPINTEGRATIONS_EVENT_INTEGRATION_DESCRIPTION

Ressourcentypen: AWS::AppIntegrations::EventIntegration

Auslösertyp: Konfigurationsänderungen

AWS-Region: Nur verfügbar in Afrika (Kapstadt), Europa (Frankfurt), USA Ost (Nord-Virginia), Asien-Pazifik (Seoul), Europa (London), Asien-Pazifik (Tokio), USA West (Oregon), Asien-Pazifik (Singapur), Asien-Pazifik (Sydney), Kanada (Zentral)

Parameter:

Keine

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

appintegrations-event-integration-tagged

Prüft, ob AppIntegrations Amazon-Eventintegrationen Tags haben. Optional können Sie Tag-Schlüssel angeben. Die Regel lautet NON_COMPLIANT, wenn keine Tags vorhanden sind oder wenn die angegebenen Tag-Schlüssel nicht vorhanden sind. Die Regel sucht nicht nach Tags, die mit 'aws: 'beginnen.

Kennung: APPINTEGRATIONS_EVENT_INTEGRATION_TAGGED

Ressourcentypen: AWS::AppIntegrations::EventIntegration

Auslösertyp: Konfigurationsänderungen

AWS-Region: Nur verfügbar in Afrika (Kapstadt), Europa (Frankfurt), USA Ost (Nord-Virginia), Asien-Pazifik (Seoul), Europa (London), Asien-Pazifik (Tokio), USA West (Oregon), Asien-Pazifik (Singapur), Asien-Pazifik (Sydney), Kanada (Zentral)

Parameter:

requiredKeyTags (Fakultativ), Typ: CSV

Durch Kommas getrennte Liste von Tag-Schlüsseln, die von der Regel überprüft werden sollen. Falls angegeben, lautet die Regel NON_COMPLIANT, wenn die ausgewertete Ressource diese

Schlüssel nicht enthält. Bei Tag-Schlüsseln wird die Groß- und Kleinschreibung beachtet. Tag-Schlüssel, die mit „aws:“ beginnen, sind nicht erlaubt.

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

appmesh-gateway-route-tagged

Prüft, ob AWS App Mesh Mesh-Gateway-Routen Tags haben. Optional können Sie Tag-Schlüssel für die Regel angeben. Die Regel ist NON_COMPLIANT, wenn keine Tags vorhanden sind oder wenn die angegebenen Tag-Schlüssel nicht vorhanden sind. Die Regel sucht nicht nach Tags, die mit 'aws: 'beginnen.

Kennung: APPMESH_GATEWAY_ROUTE_TAGGED

Ressourcentypen: AWS::AppMesh::GatewayRoute

Auslösertyp: Konfigurationsänderungen

AWS-Region: Alle unterstützten AWS Regionen außer China (Peking), Asien-Pazifik (Thailand), Naher Osten (VAE), Asien-Pazifik (Hyderabad), Asien-Pazifik (Malaysia), Asien-Pazifik (Melbourne), AWS GovCloud (US-Ost), AWS GovCloud (US-West), Mexiko (Zentral), Kanada West (Calgary), Europa (Spanien), China (Ningxia), Europa (Zürich)

Parameter:

requiredKeyTags (Fakultativ), Typ: CSV

Durch Kommas getrennte Liste von Tag-Schlüsseln, die von der Regel überprüft werden sollen. Falls angegeben, lautet die Regel NON_COMPLIANT, wenn die ausgewertete Ressource diese Schlüssel nicht enthält. Bei Tag-Schlüsseln wird die Groß- und Kleinschreibung beachtet. Tag-Schlüssel, die mit „aws:“ beginnen, sind nicht erlaubt.

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

appmesh-mesh-deny-tcp-spedition

Überprüft, ob Proxys für AWS App Mesh-Servicemeshes den TCP-Verkehr nicht direkt an Dienste weiterleiten, die nicht mit einem im Mesh definierten Proxy bereitgestellt werden. Die Regel ist NON_COMPLIANT, wenn Configuration.spec. EgressFilter.Type ist auf 'ALLOW_ALL' gesetzt.

Kennung: APPMESH_MESH_DENY_TCP_FORWARDING

Ressourcentypen: AWS::AppMesh::Mesh

Auslösertyp: Konfigurationsänderungen

AWS-Region: Alle unterstützten AWS Regionen außer China (Peking), Asien-Pazifik (Thailand), Naher Osten (VAE), Asien-Pazifik (Hyderabad), Asien-Pazifik (Malaysia), Asien-Pazifik (Melbourne), AWS GovCloud (US-Ost), AWS GovCloud (US-West), Mexiko (Zentral), Kanada West (Calgary), Europa (Spanien), China (Ningxia), Europa (Zürich)

Parameter:

Keine

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

appmesh-mesh-tagged

Prüft, ob AWS App Mesh Mesh-Netze Tags haben. Optional können Sie Tag-Schlüssel angeben, die von der Regel überprüft werden sollen. Die Regel ist NON_COMPLIANT, wenn keine Tags vorhanden sind oder wenn die angegebenen Tag-Schlüssel nicht vorhanden sind. Die Regel sucht nicht nach Tags, die mit 'aws: 'beginnen.

Kennung: APPMESH_MESH_TAGGED

Ressourcentypen: AWS::AppMesh::Mesh

Auslösertyp: Konfigurationsänderungen

AWS-Region: Alle unterstützten AWS Regionen außer China (Peking), Asien-Pazifik (Thailand), Naher Osten (VAE), Asien-Pazifik (Hyderabad), Asien-Pazifik (Malaysia), Asien-Pazifik (Melbourne),

AWS GovCloud (US-Ost), AWS GovCloud (US-West), Mexiko (Zentral), Kanada West (Calgary), Europa (Spanien), China (Ningxia), Europa (Zürich)

Parameter:

requiredKeyTags (Fakultativ), Typ: CSV

Durch Kommas getrennte Liste von Tag-Schlüsseln, die von der Regel überprüft werden sollen. Falls angegeben, lautet die Regel NON_COMPLIANT, wenn die ausgewertete Ressource diese Schlüssel nicht enthält. Bei Tag-Schlüsseln wird die Groß- und Kleinschreibung beachtet. Tag-Schlüssel, die mit „aws:“ beginnen, sind nicht erlaubt.

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

appmesh-route-tagged

Prüft, ob AWS App Mesh Mesh-Routen Tags haben. Optional können Sie Tag-Schlüssel angeben, die von der Regel überprüft werden sollen. Die Regel ist NON_COMPLIANT, wenn keine Tags vorhanden sind oder wenn die angegebenen Tag-Schlüssel nicht vorhanden sind. Die Regel sucht nicht nach Tags, die mit 'aws: 'beginnen.

Kennung: APPMESH_ROUTE_TAGGED

Ressourcentypen: AWS::AppMesh::Route

Auslösertyp: Konfigurationsänderungen

AWS-Region: Alle unterstützten AWS Regionen außer China (Peking), Asien-Pazifik (Thailand), Naher Osten (VAE), Asien-Pazifik (Hyderabad), Asien-Pazifik (Malaysia), Asien-Pazifik (Melbourne), AWS GovCloud (US-Ost), AWS GovCloud (US-West), Mexiko (Zentral), Kanada West (Calgary), Europa (Spanien), China (Ningxia), Europa (Zürich)

Parameter:

requiredKeyTags (Fakultativ), Typ: CSV

Durch Kommas getrennte Liste von Tag-Schlüsseln, die von der Regel überprüft werden sollen. Falls angegeben, lautet die Regel NON_COMPLIANT, wenn die ausgewertete Ressource diese

Schlüssel nicht enthält. Bei Tag-Schlüsseln wird die Groß- und Kleinschreibung beachtet. Tag-Schlüssel, die mit „aws:“ beginnen, sind nicht erlaubt.

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

appmesh-virtual-gateway-backend-Standards-tls

Überprüft, ob die Backend-Standardeinstellungen für virtuelle AWS App Mesh Mesh-Gateways erfordern, dass die virtuellen Gateways mit allen Ports über TLS kommunizieren. Die Regel ist NON_COMPLIANT, wenn Configuration.spec. BackendDefaults. ClientPolicy.Tls.Enforce ist falsch.

Kennung: APPMESH_VIRTUAL_GATEWAY_BACKEND_DEFAULTS_TLS

Ressourcentypen: AWS::AppMesh::VirtualGateway

Auslösertyp: Konfigurationsänderungen

AWS-Region: Alle unterstützten AWS Regionen außer China (Peking), Asien-Pazifik (Thailand), Naher Osten (VAE), Asien-Pazifik (Hyderabad), Asien-Pazifik (Malaysia), Asien-Pazifik (Melbourne), AWS GovCloud (US-Ost), AWS GovCloud (US-West), Mexiko (Zentral), Kanada West (Calgary), Europa (Spanien), China (Ningxia), Europa (Zürich)

Parameter:

Keine

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

appmesh-virtual-gateway-logging-file-path-exists

Überprüft, ob virtuelle AWS App Mesh Mesh-Gateways über einen Dateipfad verfügen, in den Zugriffsprotokolle geschrieben werden können. Die Regel ist NON_COMPLIANT, wenn Configuration.spec.Logging. AccessLog.File.Path ist nicht vorhanden.

Kennung: APPMESH_VIRTUAL_GATEWAY_LOGGING_FILE_PATH_EXISTS

Ressourcentypen: AWS::AppMesh::VirtualGateway

Auslösertyp: Konfigurationsänderungen

AWS-Region: Alle unterstützten AWS Regionen außer China (Peking), Asien-Pazifik (Thailand), Naher Osten (VAE), Asien-Pazifik (Hyderabad), Asien-Pazifik (Malaysia), Asien-Pazifik (Melbourne), AWS GovCloud (US-Ost), AWS GovCloud (US-West), Mexiko (Zentral), Kanada West (Calgary), Europa (Spanien), China (Ningxia), Europa (Zürich)

Parameter:

Keine

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

appmesh-virtual-gateway-tagged

Überprüft, ob virtuelle AWS App Mesh Mesh-Gateways über Tags verfügen. Optional können Sie Tag-Schlüssel für die Regel angeben. Die Regel ist NON_COMPLIANT, wenn keine Tags vorhanden sind oder wenn die angegebenen Tag-Schlüssel nicht vorhanden sind. Die Regel sucht nicht nach Tags, die mit 'aws: 'beginnen.

Kennung: APPMESH_VIRTUAL_GATEWAY_TAGGED

Ressourcentypen: AWS::AppMesh::VirtualGateway

Auslösertyp: Konfigurationsänderungen

AWS-Region: Alle unterstützten AWS Regionen außer China (Peking), Asien-Pazifik (Thailand), Naher Osten (VAE), Asien-Pazifik (Hyderabad), Asien-Pazifik (Malaysia), Asien-Pazifik (Melbourne), AWS GovCloud (US-Ost), AWS GovCloud (US-West), Mexiko (Zentral), Kanada West (Calgary), Europa (Spanien), China (Ningxia), Europa (Zürich)

Parameter:

requiredKeyTags (Fakultativ), Typ: CSV

Durch Kommas getrennte Liste von Tag-Schlüsseln, die von der Regel überprüft werden sollen. Falls angegeben, lautet die Regel NON_COMPLIANT, wenn die ausgewertete Ressource diese

Schlüssel nicht enthält. Bei Tag-Schlüsseln wird die Groß- und Kleinschreibung beachtet. Tag-Schlüssel, die mit „aws:“ beginnen, sind nicht erlaubt.

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

appmesh-virtual-node-backend-defaults-tls-on

Überprüft, ob die Backend-Standardeinstellungen für virtuelle AWS App Mesh-Knoten erfordern, dass die virtuellen Knoten mit allen Ports über TLS kommunizieren. Die Regel ist NON_COMPLIANT, wenn Configuration.spec. BackendDefaults. ClientPolicy.Tls.Enforce ist falsch.

Kennung: APPMESH_VIRTUAL_NODE_BACKEND_DEFAULTS_TLS_ON

Ressourcentypen: AWS::AppMesh::VirtualNode

Auslösertyp: Konfigurationsänderungen

AWS-Region: Alle unterstützten AWS Regionen außer China (Peking), Asien-Pazifik (Thailand), Naher Osten (VAE), Asien-Pazifik (Hyderabad), Asien-Pazifik (Malaysia), Asien-Pazifik (Melbourne), AWS GovCloud (US-Ost), AWS GovCloud (US-West), Mexiko (Zentral), Kanada West (Calgary), Europa (Spanien), China (Ningxia), Europa (Zürich)

Parameter:

Keine

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

appmesh-virtual-node-logging-file-path-exists

Prüft, ob virtuelle AWS App Mesh-Knoten über einen Dateipfad verfügen, in den Zugriffsprotokolle geschrieben werden können. Die Regel ist NON_COMPLIANT, wenn Configuration.spec.Logging. AccessLog.File.Path ist nicht vorhanden.

Kennung: APPMESH_VIRTUAL_NODE_LOGGING_FILE_PATH_EXISTS

Ressourcentypen: AWS::AppMesh::VirtualNode

Auslösertyp: Konfigurationsänderungen

AWS-Region: Alle unterstützten AWS Regionen außer China (Peking), Asien-Pazifik (Thailand), Naher Osten (VAE), Asien-Pazifik (Hyderabad), Asien-Pazifik (Malaysia), Asien-Pazifik (Melbourne), AWS GovCloud (US-Ost), AWS GovCloud (US-West), Mexiko (Zentral), Kanada West (Calgary), Europa (Spanien), China (Ningxia), Europa (Zürich)

Parameter:

Keine

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

appmesh-virtual-node-tagged

Prüft, ob virtuelle AWS App Mesh-Knoten Tags haben. Optional können Sie Tag-Schlüssel angeben, die von der Regel überprüft werden sollen. Die Regel ist NON_COMPLIANT, wenn keine Tags vorhanden sind oder wenn die angegebenen Tag-Schlüssel nicht vorhanden sind. Die Regel sucht nicht nach Tags, die mit 'aws: 'beginnen.

Kennung: APPMESH_VIRTUAL_NODE_TAGGED

Ressourcentypen: AWS::AppMesh::VirtualNode

Auslösertyp: Konfigurationsänderungen

AWS-Region: Alle unterstützten AWS Regionen außer China (Peking), Asien-Pazifik (Thailand), Naher Osten (VAE), Asien-Pazifik (Hyderabad), Asien-Pazifik (Malaysia), Asien-Pazifik (Melbourne), AWS GovCloud (US-Ost), AWS GovCloud (US-West), Mexiko (Zentral), Kanada West (Calgary), Europa (Spanien), China (Ningxia), Europa (Zürich)

Parameter:

requiredKeyTags (Fakultativ), Typ: CSV

Durch Kommas getrennte Liste von Tag-Schlüsseln, die von der Regel überprüft werden sollen. Falls angegeben, lautet die Regel NON_COMPLIANT, wenn die ausgewertete Ressource diese

Schlüssel nicht enthält. Bei Tag-Schlüsseln wird die Groß- und Kleinschreibung beachtet. Tag-Schlüssel, die mit „aws:“ beginnen, sind nicht erlaubt.

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

appmesh-virtual-router-tagged

Überprüft, ob virtuelle AWS App Mesh Mesh-Router Tags haben. Optional können Sie Tag-Schlüssel für die Regel angeben. Die Regel ist NON_COMPLIANT, wenn keine Tags vorhanden sind oder wenn die angegebenen Tag-Schlüssel nicht vorhanden sind. Die Regel sucht nicht nach Tags, die mit 'aws: 'beginnen.

Kennung: APPMESH_VIRTUAL_ROUTER_TAGGED

Ressourcentypen: AWS::AppMesh::VirtualRouter

Auslösertyp: Konfigurationsänderungen

AWS-Region: Alle unterstützten AWS Regionen außer China (Peking), Asien-Pazifik (Thailand), Naher Osten (VAE), Asien-Pazifik (Hyderabad), Asien-Pazifik (Malaysia), Asien-Pazifik (Melbourne), AWS GovCloud (US-Ost), AWS GovCloud (US-West), Mexiko (Zentral), Kanada West (Calgary), Europa (Spanien), China (Ningxia), Europa (Zürich)

Parameter:

requiredKeyTags (Fakultativ), Typ: CSV

Durch Kommas getrennte Liste von Tag-Schlüsseln, die von der Regel überprüft werden sollen. Falls angegeben, lautet die Regel NON_COMPLIANT, wenn die ausgewertete Ressource diese Schlüssel nicht enthält. Bei Tag-Schlüsseln wird die Groß- und Kleinschreibung beachtet. Tag-Schlüssel, die mit „aws:“ beginnen, sind nicht erlaubt.

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

appmesh-virtual-service-tagged

Prüft, ob virtuelle AWS App Mesh Mesh-Dienste über Tags verfügen. Optional können Sie Tag-Schlüssel für die Regel angeben. Die Regel ist NON_COMPLIANT, wenn keine Tags vorhanden sind oder wenn die angegebenen Tag-Schlüssel nicht vorhanden sind. Die Regel sucht nicht nach Tags, die mit 'aws: 'beginnen.

Kennung: APPMESH_VIRTUAL_SERVICE_TAGGED

Ressourcentypen: AWS::AppMesh::VirtualService

Auslösertyp: Konfigurationsänderungen

AWS-Region: Alle unterstützten AWS Regionen außer China (Peking), Asien-Pazifik (Thailand), Naher Osten (VAE), Asien-Pazifik (Hyderabad), Asien-Pazifik (Malaysia), Asien-Pazifik (Melbourne), AWS GovCloud (US-Ost), AWS GovCloud (US-West), Mexiko (Zentral), Kanada West (Calgary), Europa (Spanien), China (Ningxia), Europa (Zürich)

Parameter:

requiredKeyTags (Fakultativ), Typ: CSV

> Durch Kommas getrennte Liste von Tag-Schlüsseln, die von der Regel überprüft werden sollen. Falls angegeben, lautet die Regel NON_COMPLIANT, wenn die ausgewertete Ressource diese Schlüssel nicht enthält. Bei Tag-Schlüsseln wird die Groß- und Kleinschreibung beachtet. Tag-Schlüssel, die mit „aws:“ beginnen, sind nicht erlaubt.

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

approved-amis-by-id

Prüft, ob EC2 Instances angegebene Amazon Machine Images (AMIs) verwenden. Geben Sie eine Liste der genehmigten AMI an IDs. Laufende Instances AMIs , die nicht auf dieser Liste stehen, sind NON_COMPLIANT.

ID: APPROVED_AMIS_BY_ID

Ressourcentypen: AWS::EC2::Instance

Auslösertyp: Konfigurationsänderungen

AWS-Region: Alle unterstützten AWS Regionen

Parameter:

amiIds, Typ: CSV

Kommagetrennte Liste mit bis zu 21 AMI. IDs Es gibt ein Limit von 1024 Zeichen.

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

approved-amis-by-tag

Prüft, ob EC2 Instances die angegebenen Amazon Machine Images (AMIs) verwenden. Geben Sie die Tags an, die die identifizieren AMIs. Laufende Instanzen AMIs , die nicht mindestens eines der angegebenen Tags haben, sind NON_COMPLIANT.

ID: APPROVED_AMIS_BY_TAG

Ressourcentypen: AWS::EC2::Instance

Auslösertyp: Konfigurationsänderungen

AWS-Region: Alle unterstützten AWS Regionen

Parameter:

amisByTagKeyAndValue, Typ: StringMap, Standard: Tag-Schlüssel:Tag-Wert, other-tag-key

Kommagetrennte Liste mit bis zu 10 Tags (Tag-Schlüssel:Tag-Wert). AMIs Beispiel: tag-key1 entspricht tag-key1; tag-key2:value2 entspricht tag-key2 mit dem Wert 2. AMIs

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

apprunner-service-in-vpc

Prüft, ob AWS App Runner-Dienste ausgehenden Datenverkehr über eine benutzerdefinierte VPC weiterleiten. Die Regel lautet NON_COMPLIANT, wenn sie konfiguriert ist. NetworkConfiguration. EgressConfiguration. EgressType ist gleich DEFAULT.

Kennung: APPRUNNER_SERVICE_IN_VPC

Ressourcentypen: AWS::AppRunner::Service

Auslösertyp: Konfigurationsänderungen

AWS-Region: Nur in der Region Asien-Pazifik (Mumbai), Europa (Paris), USA Ost (Ohio), Europa (Irland), Europa (Frankfurt), USA Ost (Nord-Virginia), Europa (London), Asien-Pazifik (Tokio), USA West (Oregon), Asien-Pazifik (Singapur), Asien-Pazifik (Sydney) verfügbar

Parameter:

Keine

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

apprunner-service-no-public-Zugang

Prüft, ob AWS AppRunner Dienste nicht öffentlich zugänglich sind. Bei service.configuration lautet die Regel NON_COMPLIANT. NetworkConfiguration. IngressConfiguration. IsPubliclyAccessible ist falsch.

Kennung: APPRUNNER_SERVICE_NO_PUBLIC_ACCESS

Ressourcentypen: AWS::AppRunner::Service

Auslösertyp: Konfigurationsänderungen

AWS-Region: Nur in der Region Asien-Pazifik (Mumbai), Europa (Paris), USA Ost (Ohio), Europa (Irland), Europa (Frankfurt), USA Ost (Nord-Virginia), Europa (London), Asien-Pazifik (Tokio), USA West (Oregon), Asien-Pazifik (Singapur), Asien-Pazifik (Sydney) verfügbar

Parameter:

Keine

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

apprunner-service-observability-enabled

Überprüft, ob für AWS App Runner-Dienste Observability aktiviert ist. Bei der Konfiguration lautet die Regel NON_COMPLIANT. ObservabilityConfiguration. ObservabilityEnabled ist falsch'.

Kennung: APPRUNNER_SERVICE_OBSERVABILITY_ENABLED

Ressourcentypen: AWS::AppRunner::Service

Auslösertyp: Konfigurationsänderungen

AWS-Region: Nur in der Region Asien-Pazifik (Mumbai), Europa (Paris), USA Ost (Ohio), Europa (Irland), Europa (Frankfurt), USA Ost (Nord-Virginia), Europa (London), Asien-Pazifik (Tokio), USA West (Oregon), Asien-Pazifik (Singapur), Asien-Pazifik (Sydney) verfügbar

Parameter:

Keine

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

apprunner-service-tagged

Prüft, ob AWS App Runner-Dienste Tags haben. Optional können Sie Tag-Schlüssel angeben. Die Regel lautet NON_COMPLIANT, wenn keine Tags vorhanden sind oder wenn die angegebenen Tag-Schlüssel nicht vorhanden sind. Die Regel sucht nicht nach Tags, die mit 'aws: 'beginnen.

Kennung: APPRUNNER_SERVICE_TAGGED

Ressourcentypen: AWS::AppRunner::Service

Auslösertyp: Konfigurationsänderungen

AWS-Region: Nur in der Region Asien-Pazifik (Mumbai), Europa (Paris), USA Ost (Ohio), Europa (Irland), Europa (Frankfurt), USA Ost (Nord-Virginia), Europa (London), Asien-Pazifik (Tokio), USA West (Oregon), Asien-Pazifik (Singapur), Asien-Pazifik (Sydney) verfügbar

Parameter:

requiredKeyTags (Fakultativ), Typ: CSV

> Durch Kommas getrennte Liste von Tag-Schlüsseln, die von der Regel überprüft werden sollen. Falls angegeben, lautet die Regel NON_COMPLIANT, wenn die ausgewertete Ressource diese Schlüssel nicht enthält. Bei Tag-Schlüsseln wird die Groß- und Kleinschreibung beachtet. Tag-Schlüssel, die mit „aws:“ beginnen, sind nicht erlaubt.

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

apprunner-vpc-connector-tagged

Prüft, ob AWS App Runner VPC-Connectors Tags haben. Optional können Sie Tag-Schlüssel angeben. Die Regel lautet NON_COMPLIANT, wenn keine Tags vorhanden sind oder wenn die angegebenen Tag-Schlüssel nicht vorhanden sind. Die Regel sucht nicht nach Tags, die mit 'aws: 'beginnen.

Kennung: APPRUNNER_VPC_CONNECTOR_TAGGED

Ressourcentypen: AWS::AppRunner::VpcConnector

Auslösertyp: Konfigurationsänderungen

AWS-Region: Nur in der Region Asien-Pazifik (Mumbai), Europa (Paris), USA Ost (Ohio), Europa (Irland), Europa (Frankfurt), USA Ost (Nord-Virginia), Asien-Pazifik (Tokio), USA West (Oregon), Asien-Pazifik (Singapur), Asien-Pazifik (Sydney) verfügbar

Parameter:

requiredKeyTags (Fakultativ), Typ: CSV

> Durch Kommas getrennte Liste von Tag-Schlüsseln, die von der Regel überprüft werden sollen. Falls angegeben, lautet die Regel NON_COMPLIANT, wenn die ausgewertete Ressource diese

Schlüssel nicht enthält. Bei Tag-Schlüsseln wird die Groß- und Kleinschreibung beachtet. Tag-Schlüssel, die mit „aws:“ beginnen, sind nicht erlaubt.

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

appstream-fleet-in-vpc

Prüft, ob Amazon AppStream 2.0-Flotten eine Amazon Virtual Private Cloud (Amazon VPC) verwenden. Bei der Konfiguration lautet die Regel NON_COMPLIANT. VpcConfig ist nicht vorhanden. Die Regel überprüft Elastic Fleets nicht.

Kennung: APPSTREAM_FLEET_IN_VPC

Ressourcentypen: AWS::AppStream::Fleet

Auslösertyp: Konfigurationsänderungen

AWS-Region: Nur in der Region Asien-Pazifik (Mumbai), USA Ost (Ohio), Europa (Irland), Europa (Frankfurt), USA Ost (Nord-Virginia), Asien-Pazifik (Seoul), Europa (London), Asien-Pazifik (Tokio), USA West (Oregon), Asien-Pazifik (Singapur), Asien-Pazifik (Sydney), Kanada (Zentral) verfügbar

Parameter:

Keine

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

appsync-associated-with-waf

Prüft, ob AWS AppSync APIs sie mit AWS WAFv2 Web-Zugriffskontrolllisten () ACLs verknüpft sind. Die Regel ist NON_COMPLIANT für eine AWS AppSync API, wenn sie keiner Web-ACL zugeordnet ist.

ID: APPSYNC_ASSOCIATED_WITH_WAF

Ressourcentypen: AWS::AppSync::GraphQLApi

Auslösertyp: Regelmäßig

AWS-Region: Alle unterstützten AWS Regionen außer Asien-Pazifik (Thailand), Asien-Pazifik (Jakarta), Afrika (Kapstadt), Naher Osten (VAE), Asien-Pazifik (Hyderabad), Asien-Pazifik (Malaysia), Asien-Pazifik (Melbourne), AWS GovCloud (USA-Ost), AWS GovCloud (US-West), Mexiko (Zentral), Israel (Tel Aviv), Kanada West (Calgary), Europa (Spanien), Europa (Zürich)

Parameter:

wafWebAclARNs (Fakultativ), Typ: CSV

Kommagetrennte Liste von Amazon-Ressourcennamen (ARNs) für autorisierte Websites. ACLs

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

appsync-authorization-check

Prüft, ob eine AWS AppSync API zulässige Autorisierungsmechanismen verwendet. Die Regel ist NON_COMPLIANT, wenn ein nicht genehmigter Autorisierungsmechanismus verwendet wird.

ID: APPSYNC_AUTHORIZATION_CHECK

Ressourcentypen: AWS::AppSync::GraphQLApi

Auslösertyp: Konfigurationsänderungen

AWS-Region: Alle unterstützten AWS Regionen außer Asien-Pazifik (Thailand), Asien-Pazifik (Malaysia), Asien-Pazifik (Melbourne), AWS GovCloud (USA-Ost), AWS GovCloud (US-West), Mexiko (Zentral), Israel (Tel Aviv), Kanada West (Calgary)

Parameter:

AllowedAuthorizationTypes, Typ: CSV

Durch Kommas getrennte Liste der zulässigen Autorisierungsmechanismen. AWS AppSync Zulässige Werte sind: '', 'API_KEY AWS_LAMBDA','AWS_IAM ',' OPENID_CONNECT ', 'AMAZON_COGNITO_USER_POOLS'.

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

appsync-cache-ct-encryption-im Ruhezustand

Prüft, ob für einen AWS AppSync API-Cache die Verschlüsselung im Ruhezustand aktiviert ist. Diese Regel ist NON_COMPLIANT, wenn 'AtRestEncryptionEnabled' falsch ist.

Kennung: APPSYNC_CACHE_CT_ENCRYPTION_AT_REST

Ressourcentypen: AWS::AppSync::ApiCache

Auslösertyp: Konfigurationsänderungen

AWS-Region: Nur in den Regionen Naher Osten (Bahrain), Europa (Frankfurt), Südamerika (Sao Paulo), USA Ost (Nord-Virginia) verfügbar

Parameter:

Keine

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

appsync-cache-ct-encryptionim Transit

Prüft, ob für einen AWS AppSync API-Cache die Verschlüsselung bei der Übertragung aktiviert ist. Die Regel ist NON_COMPLIANT, wenn 'TransitEncryptionEnabled' falsch ist.

Kennung: APPSYNC_CACHE_CT_ENCRYPTION_IN_TRANSIT

Ressourcentypen: AWS::AppSync::ApiCache

Auslösertyp: Konfigurationsänderungen

AWS-Region: Nur in den Regionen Naher Osten (Bahrain), Europa (Frankfurt), Südamerika (Sao Paulo), USA Ost (Nord-Virginia) verfügbar

Parameter:

Keine

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

appsync-cache-encryption-at-ausruhen

Prüft, ob für einen AWS AppSync API-Cache die Verschlüsselung im Ruhezustand aktiviert ist. Diese Regel ist NON_COMPLIANT, wenn 'AtRestEncryptionEnabled' falsch ist.

ID: APPSYNC_CACHE_ENCRYPTION_AT_REST

Ressourcentypen: AWS::AppSync::GraphQLApi

Auslösertyp: Regelmäßig

AWS-Region: Alle unterstützten AWS Regionen außer China (Peking), Asien-Pazifik (Thailand), Asien-Pazifik (Jakarta), Afrika (Kapstadt), Naher Osten (VAE), Asien-Pazifik (Hyderabad), Asien-Pazifik (Malaysia), Asien-Pazifik (Melbourne), AWS GovCloud (US-Ost), AWS GovCloud (US-West), Mexiko (Zentral), Israel (Tel Aviv), Kanada West (Calgary), Europa (Spanien), China (Ningxia), Europa (Region Zürich)

Parameter:

Keine

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

appsync-logging-enabled

Prüft, ob für eine AWS AppSync API die Protokollierung aktiviert ist. Die Regel ist NON_COMPLIANT, wenn die Protokollierung nicht aktiviert ist oder wenn die Feldprotokollierungsebenen für die AWS AppSync API nicht den im Regelparameter '`fieldLoggingLevel`' angegebenen Werten entsprechen.

ID: APPSYNC_LOGGING_ENABLED

Ressourcentypen: AWS::AppSync::GraphQLApi

Auslösertyp: Konfigurationsänderungen

AWS-Region: Alle unterstützten AWS Regionen außer Asien-Pazifik (Thailand), Asien-Pazifik (Malaysia), Asien-Pazifik (Melbourne), AWS GovCloud (USA-Ost), AWS GovCloud (US-West), Mexiko (Zentral), Israel (Tel Aviv), Kanada West (Calgary)

Parameter:

fieldLoggingLevel (Fakultativ), Typ: CSV

> Durch Kommas getrennte Liste der Feldprotokollierungsebenen, die von der Regel überprüft werden sollen. Zum Beispiel „ERROR, INFO“.

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

athena-data-catalog-description

Prüft, ob Amazon Athena Athena-Datenkataloge eine Beschreibung haben. Die Regel ist NON_COMPLIANT, wenn Configuration.Description nicht existiert.

Kennung: ATHENA_DATA_CATALOG_DESCRIPTION

Ressourcentypen: AWS::Athena::DataCatalog

Auslösertyp: Konfigurationsänderungen

AWS-Region: Alle unterstützten AWS Regionen außer China (Peking), Asien-Pazifik (Thailand), Asien-Pazifik (Malaysia), AWS GovCloud (USA-Ost), AWS GovCloud (US-West), Mexiko (Zentral), China (Ningxia)

Parameter:

Keine

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

athena-prepared-statement-description

Prüft, ob die von Amazon Athena vorbereiteten Kontoauszüge eine Beschreibung enthalten. Die Regel ist NON_COMPLIANT, wenn Configuration.Description nicht existiert.

Kennung: ATHENA_PREPARED_STATEMENT_DESCRIPTION

Ressourcentypen: AWS::Athena::PreparedStatement

Auslösertyp: Konfigurationsänderungen

AWS-Region: Alle unterstützten AWS Regionen außer China (Peking), Asien-Pazifik (Thailand), Asien-Pazifik (Malaysia), Europa (Mailand), AWS GovCloud (USA-Ost), AWS GovCloud (US-West), Mexiko (Zentral), China (Ningxia)

Parameter:

Keine

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

athena-workgroup-description

Prüft, ob Amazon Athena Athena-Arbeitsgruppen eine Beschreibung haben. Die Regel ist NON_COMPLIANT, wenn Configuration.Description nicht existiert oder eine leere Zeichenfolge ist.

Kennung: ATHENA_WORKGROUP_DESCRIPTION

Ressourcentypen: AWS::Athena::WorkGroup

Auslösertyp: Konfigurationsänderungen

AWS-Region: Alle unterstützten AWS Regionen außer China (Peking), Asien-Pazifik (Thailand), Asien-Pazifik (Malaysia), AWS GovCloud (USA-Ost), AWS GovCloud (US-West), Mexiko (Zentral), China (Ningxia)

Parameter:

Keine

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

athena-workgroup-encrypted-at-ausruhen

Prüft, ob eine Amazon-Athena-Arbeitsgruppe im Ruhezustand verschlüsselt wird. Die Regel ist NON_COMPLIANT, wenn die Verschlüsselung von Daten im Ruhezustand für eine Athena-Arbeitsgruppe nicht aktiviert ist.

ID: ATHENA_WORKGROUP_ENCRYPTED_AT_REST

Ressourcentypen: AWS::Athena::WorkGroup

Auslösertyp: Konfigurationsänderungen

AWS-Region: Alle unterstützten AWS Regionen außer Asien-Pazifik (Thailand), Naher Osten (VAE), Asien-Pazifik (Hyderabad), Asien-Pazifik (Malaysia), Asien-Pazifik (Melbourne), AWS GovCloud (USA-Ost), AWS GovCloud (US-West), Mexiko (Zentral), Israel (Tel Aviv), Kanada West (Calgary), Europa (Spanien), Europa (Zürich)

Parameter:

Keine

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

athena-workgroup-enforce-workgroup-Konfiguration

Prüft, ob Amazon Athena Athena-Arbeitsgruppen, die die Athena-Engine verwenden, erzwingen, dass die Arbeitsgruppenkonfiguration die clientseitigen Einstellungen überschreibt.

Bei der Konfiguration lautet die Regel NON_COMPLIANT. WorkGroupConfiguration. EnforceWorkGroupConfiguration ist falsch.

Kennung: ATHENA_WORKGROUP_ENFORCE_WORKGROUP_CONFIGURATION

Ressourcentypen: AWS::Athena::WorkGroup

Auslösertyp: Konfigurationsänderungen

AWS-Region: Alle unterstützten AWS Regionen außer China (Peking), Asien-Pazifik (Thailand), Asien-Pazifik (Malaysia), AWS GovCloud (USA-Ost), AWS GovCloud (US-West), Mexiko (Zentral), China (Ningxia)

Parameter:

Keine

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

athena-workgroup-engine-version-automatisches Upgrade

Überprüft, ob Amazon Athena Athena-Arbeitsgruppen, die die Athena-Engine verwenden, für ein auto Upgrade konfiguriert sind. Bei der Konfiguration lautet die Regel NON_COMPLIANT. WorkGroupConfiguration. EngineVersion. SelectedEngineVersion ist nicht „AUTO“.

Kennung: ATHENA_WORKGROUP_ENGINE_VERSION_AUTO_UPGRADE

Ressourcentypen: AWS::Athena::WorkGroup

Auslösertyp: Konfigurationsänderungen

AWS-Region: Alle unterstützten AWS Regionen außer China (Peking), Asien-Pazifik (Thailand), Asien-Pazifik (Malaysia), AWS GovCloud (USA-Ost), AWS GovCloud (US-West), Mexiko (Zentral), China (Ningxia)

Parameter:

Keine

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

athena-workgroup-logging-enabled

Prüft, ob Amazon Athena Nutzungsmetriken für Amazon WorkGroup CloudWatch veröffentlicht. Die Regel lautet NON_COMPLIANT, wenn Amazon Athena WorkGroup 'PublishCloudWatchMetricsEnabled' auf False gesetzt ist.

Kennung: ATHENA_WORKGROUP_LOGGING_ENABLED

Ressourcentypen: AWS::Athena::WorkGroup

Auslösertyp: Konfigurationsänderungen

AWS-Region: Alle unterstützten AWS Regionen außer Asien-Pazifik (Thailand), Asien-Pazifik (Malaysia), Mexiko (Zentral) und Kanada West (Calgary)

Parameter:

Keine

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

aurora-last-backup-recovery-Punkt-erstellt

Prüft, ob für DB-Cluster von Amazon Aurora ein Wiederherstellungspunkt erstellt wurde. Die Regel ist NON_COMPLIANT, wenn für den DB-Cluster von Amazon Relational Database Service (Amazon RDS) innerhalb des angegebenen Zeitraums kein entsprechender Wiederherstellungspunkt erstellt wurde.

ID: AURORA_LAST_BACKUP_RECOVERY_POINT_CREATED

Ressourcentypen: AWS::RDS::DBCluster

Auslösertyp: Regelmäßig

AWS-Region: Alle unterstützten AWS Regionen außer China (Peking), Asien-Pazifik (Thailand), Asien-Pazifik (Malaysia), Mexiko (Zentral), Israel (Tel Aviv), Kanada West (Calgary), China (Ningxia)

Parameter:

resourceTags (optional), Typ: Zeichenfolge

Tags von Aurora-DB-Clustern, die von der Regel überprüft werden sollen, im JSON-Format `{"tagkey" : "tagValue"}`.

resourceId (optional), Typ: Zeichenfolge

ID des Aurora-DB-Clusters, den die Regel prüfen soll.

recoveryPointAgeWert (optional), Typ: int, Standard: 1

Numerischer Wert für das zulässige Höchstalter. Nicht mehr als 744 für Stunden oder 31 für Tage.

recoveryPointAgeEinheit (optional), Typ: Zeichenfolge, Standard: days

Zeiteinheit für das zulässige Höchstalter. Zulässige Werte: „Stunden“, „Tage“.

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

aurora-meets-restore-time-ziel

Überprüft, ob die Wiederherstellungszeit von Amazon-Aurora-DB-Clustern der angegebenen Dauer entspricht. Die Regel lautet NON_COMPLIANT, wenn LatestRestoreExecutionTimeMinutes der Wert eines Aurora-DB-Clusters mehr als maxRestoreTime Minuten beträgt.

Kennung: AURORA_MEETS_RESTORE_TIME_TARGET

Ressourcentypen: AWS::RDS::DBCluster

Auslösertyp: Regelmäßig

AWS-Region: Alle unterstützten AWS Regionen außer China (Peking), Asien-Pazifik (Thailand), Asien-Pazifik (Malaysia), AWS GovCloud (USA-Ost), AWS GovCloud (US-West), Mexiko (Zentral), Israel (Tel Aviv), Kanada West (Calgary), China (Ningxia)

Parameter:

maxRestoreTime, Typ: int

Numerischer Wert für die maximal zulässige Wiederherstellungslaufzeit.

resourceTags (optional), Typ: Zeichenfolge

Tags von Aurora-DB-Clustern, die von der Regel überprüft werden sollen, im JSON-Format.

resourceId (optional), Typ: Zeichenfolge

ID des Aurora-DB-Clusters, den die Regel prüfen soll.

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

aurora-mysql-backtracking-enabled

Prüft, ob für einen Amazon-Aurora-MySQL-Cluster die Rückverfolgung aktiviert ist. Die Regel ist NON_COMPLIANT, wenn der Aurora-Cluster MySQL verwendet und die Rückverfolgung nicht aktiviert ist.

ID: AURORA_MYSQL_BACKTRACKING_ENABLED

Ressourcentypen: AWS::RDS::DBCluster

Auslösertyp: Konfigurationsänderungen

AWS-Region: Alle unterstützten AWS Regionen außer Europa (Stockholm), Naher Osten (Bahrain), China (Peking), Asien-Pazifik (Jakarta), Afrika (Kapstadt), Naher Osten (VAE), Südamerika (Sao Paulo), Asien-Pazifik (Hongkong), Asien-Pazifik (Hyderabad), Asien-Pazifik (Melbourne), Europa (Mailand), (US-Ost), AWS GovCloud (US-West), Israel AWS GovCloud (Tel Aviv), Kanada West (Calgary), Region Europa (Spanien)

Parameter:

BacktrackWindowInHours (Fakultativ), Typ: double

Zeitraum in Stunden (bis zu 72) für die Rückverfolgung Ihres Aurora-MySQL-Clusters.

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

aurora-mysql-cluster-audit-Protokollierung

Prüft, ob für Amazon Aurora MySQL-DB-Cluster die Audit-Protokollierung aktiviert ist. Die Regel lautet NON_COMPLIANT, wenn für einen DB-Cluster die Audit-Protokollierung nicht aktiviert ist.

Kennung: AURORA_MYSQL_CLUSTER_AUDIT_LOGGING

Ressourcentypen: AWS::RDS::DBCluster

Auslösertyp: Regelmäßig

AWS-Region: Alle unterstützten AWS Regionen außer Naher Osten (Bahrain), China (Peking), Asien-Pazifik (Thailand), Asien-Pazifik (Malaysia), Mexiko (Zentral), Kanada West (Calgary), China (Ningxia)

Parameter:

Keine

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

aurora-resources-in-logically-air-gapped-vault

Überprüft, ob sich Amazon Aurora Aurora-DB-Cluster in einem Tresor mit logischem Air-Gap befinden. Die Regel lautet NON_COMPLIANT, wenn sich ein Amazon Aurora Aurora-DB-Cluster innerhalb des angegebenen Zeitraums nicht in einem Tresor mit logischem Air-Gap befindet.

Kennung: AURORA_RESOURCES_IN_LOGICALLY_AIR_GAPPED_VAULT

Ressourcentypen: AWS::RDS::DBCluster

Auslösertyp: Regelmäßig

AWS-Region: Alle unterstützten AWS Regionen außer China (Peking), Asien-Pazifik (Thailand), Asien-Pazifik (Malaysia), AWS GovCloud (USA-Ost), AWS GovCloud (US-West), Mexiko (Zentral), Israel (Tel Aviv), Kanada West (Calgary), China (Ningxia)

Parameter:

resourceTags (optional), Typ: Zeichenfolge

Tags von Aurora-DB-Clustern, die von der Regel überprüft werden sollen, im JSON-Format.

resourceId (optional), Typ: Zeichenfolge

ID des Aurora-DB-Clusters, den die Regel prüfen soll.

recoveryPointAgeWert (optional), Typ: int, Standard: 1

Numerischer Wert für das zulässige Höchstalter. Nicht mehr als 2184 für Stunden, 91 für Tage.

recoveryPointAgeEinheit (optional), Typ: Zeichenfolge, Standard: days

Zeiteinheit für das zulässige Höchstalter. Zulässige Werte: „Stunden“, „Tage“.

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

aurora-resources-protected-by-Backup-Plan

Prüft, ob DB-Cluster von Amazon Aurora durch einen Backup-Plan geschützt sind. Die Regel ist NON_COMPLIANT, wenn der Datenbank-Cluster von Amazon Relational Database Service (Amazon RDS) nicht durch einen Backup-Plan geschützt ist.

ID: AURORA_RESOURCES_PROTECTED_BY_BACKUP_PLAN

Ressourcentypen: AWS::RDS::DBCluster

Auslösertyp: Regelmäßig

AWS-Region: Alle unterstützten AWS Regionen außer China (Peking), Asien-Pazifik (Thailand), Asien-Pazifik (Malaysia), Mexiko (Zentral), Israel (Tel Aviv), Kanada West (Calgary), China (Ningxia)

Parameter:

resourceTags (optional), Typ: Zeichenfolge

Tags von Aurora-DB-Clustern, die von der Regel überprüft werden sollen, im JSON-Format `{"tagkey" : "tagValue"}`.

resourceId (optional), Typ: Zeichenfolge

ID des Aurora-DB-Clusters, den die Regel prüfen soll.

crossRegionList (Fakultativ), Typ: Zeichenfolge

Durch Kommata getrennte Liste der Zielregionen, für die die regionsübergreifende Backup-Kopie aufbewahrt werden soll.

crossAccountList (Fakultativ), Typ: Zeichenfolge

Durch Kommata getrennte Liste der Zielkonten, für die die kontoübergreifende Backup-Kopie aufbewahrt werden soll.

maxRetentionDays (Fakultativ), Typ: int

Die maximale Aufbewahrungsdauer in Tagen für die Backup-Tresorsperre.

minRetentionDays (Fakultativ), Typ: int

Die Mindestaufbewahrungsdauer in Tagen für die Backup-Tresorsperre.

backupVaultLockÜberprüfen Sie (fakultativ), Typ: Zeichenfolge

Akzeptierte Werte: „True“ oder „False“. Geben Sie „True“ ein, damit die Regel prüft, ob die Ressource in einem gesperrten Tresor gesichert ist.

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

autoscaling-capacity-rebalancing

Prüft, ob Capacity Rebalancing für Amazon EC2 Auto Scaling Scaling-Gruppen aktiviert ist, die mehrere Instance-Typen verwenden. Die Regel ist NON_COMPLIANT, wenn der Kapazitätsausgleich nicht aktiviert ist.

ID: AUTOSCALING_CAPACITY_REBALANCING

Ressourcentypen: AWS::AutoScaling::AutoScalingGroup

Auslösertyp: Konfigurationsänderungen

AWS-Region: Alle unterstützten AWS Regionen außer China (Peking), Asien-Pazifik (Thailand), Asien-Pazifik (Jakarta), Naher Osten (VAE), Asien-Pazifik (Hyderabad), Asien-Pazifik (Malaysia), Asien-Pazifik (Melbourne), AWS GovCloud (US-Ost), AWS GovCloud (US-West), Mexiko (Zentral), Israel (Tel Aviv), Kanada West (Calgary), Europa (Spanien), China (Ningxia), Europa (Zürich)

Parameter:

Keine

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

autoscaling-group-elb-healthcheck-erforderlich

Überprüft, ob Ihre Amazon EC2 Auto Scaling Scaling-Gruppen, die einem Elastic Load Balancer zugeordnet sind, Elastic Load Balancing Balancing-Zustandsprüfungen verwenden. Die Regel lautet NON_COMPLIANT, wenn die Amazon EC2 Auto Scaling Scaling-Gruppen keine Elastic Load Balancing Balancing-Zustandsprüfungen verwenden.

ID: AUTOSCALING_GROUP_ELB_HEALTHCHECK_REQUIRED

Ressourcentypen: AWS::AutoScaling::AutoScalingGroup

Auslösertyp: Konfigurationsänderungen

AWS-Region: Alle unterstützten AWS Regionen außer Naher Osten (VAE) und Asien-Pazifik (Taipeh)

Parameter:

Keine

Proaktive Auswertung

Anweisungen zur Ausführung dieser Regel im proaktiven Modus finden Sie unter Evaluieren Ihrer Ressourcen mithilfe von AWS Config Regeln. Damit diese Regel im proaktiven Modus COMPLIANT

zurückgibt, muss das Ressourcenkonfigurationsschema für die StartResourceEvaluationAPI die folgenden Eingaben enthalten, die als Zeichenfolge kodiert sind:

```
"ResourceConfiguration":
...
{
   "LoadBalancerNames": "[my-load-balancer-1, my-load-balancer-2, my-load-
balancer-3, ...]",
   "HealthCheckType": HealthCheckType*"
}
...
```

* Die zulässigen Werte sind `EC2` (Standard), `ELB` und `VPC_LATTICE`. Der `VPC_LATTICE`-Zustandsprüfungen von VPC Lattice befindet sich in der Vorversion und kann noch geändert werden. Weitere Informationen finden Sie unter Zustandsprüfungen für Auto Scaling Scaling-Instances im Amazon EC2 Auto Scaling Scaling-Benutzerhandbuch.

Weitere Informationen zur proaktiven Auswertung finden Sie unter Auswertungsmodus.

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

autoscaling-launchconfig-requires-imdsv2

Prüft, ob Only aktiviert IMDSv2 ist. Diese Regel ist NON_COMPLIANT, wenn die Metadaten-Version nicht in der Startkonfiguration enthalten ist oder sowohl Metadaten V1 als auch V2 aktiviert sind.

Kennung: AUTOSCALING_LAUNCHCONFIG_REQUIRES_ IMDSV2

Ressourcentypen: AWS::AutoScaling::LaunchConfiguration

Auslösertyp: Konfigurationsänderungen

AWS-Region: Alle unterstützten AWS Regionen außer Asien-Pazifik (Thailand), Asien-Pazifik (Malaysia), Mexiko (Zentral) und Kanada West (Calgary)

Parameter:

Keine

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

autoscaling-launch-config-hop-Grenze

Prüft die Anzahl der Netzwerk-Hops, die das Metadaten-Token zurücklegen kann. Diese Regel ist NON_COMPLIANT, wenn das Limit für Metadaten-Antwort-Hops größer als 1 ist.

ID: AUTOSCALING_LAUNCH_CONFIG_HOP_LIMIT

Ressourcentypen: AWS::AutoScaling::LaunchConfiguration

Auslösertyp: Konfigurationsänderungen

AWS-Region: Alle unterstützten AWS Regionen außer Asien-Pazifik (Thailand), Asien-Pazifik (Jakarta), Asien-Pazifik (Malaysia), AWS GovCloud (USA-Ost), AWS GovCloud (US-West), Mexiko (Zentral), Kanada West (Calgary)

Parameter:

Keine

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

autoscaling-launch-config-public-ip-deaktiviert

Überprüft, ob für Amazon EC2 Auto Scaling Scaling-Gruppen öffentliche IP-Adressen über Startkonfigurationen aktiviert sind. Die Regel lautet NON_COMPLIANT, wenn die Startkonfiguration für eine Amazon EC2 Auto Scaling Scaling-Gruppe auf „true AssociatePublicIpAddress “ gesetzt ist.

ID: AUTOSCALING_LAUNCH_CONFIG_PUBLIC_IP_DISABLED

Ressourcentypen: AWS::AutoScaling::LaunchConfiguration

Auslösertyp: Konfigurationsänderungen

AWS-Region: Alle unterstützten AWS Regionen außer der Region Asien-Pazifik (Taipeh)

Parameter:

Keine

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

autoscaling-launch-template

Prüft, ob eine Amazon Elastic Compute Cloud (EC2) Auto Scaling Scaling-Gruppe anhand einer EC2 Startvorlage erstellt wurde. Die Regel lautet NON_COMPLIANT, wenn die Skalierungsgruppe nicht anhand einer EC2 Startvorlage erstellt wurde.

ID: AUTOSCALING_LAUNCH_TEMPLATE

Ressourcentypen: AWS::AutoScaling::AutoScalingGroup

Auslösertyp: Konfigurationsänderungen

AWS-Region: Alle unterstützten AWS Regionen außer Asien-Pazifik (Thailand), Asien-Pazifik (Malaysia), AWS GovCloud (USA-Ost), AWS GovCloud (US-West), Mexiko (Zentral), Kanada West (Calgary)

Parameter:

Keine

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

autoscaling-multiple-az

Prüft, ob die Auto-Scaling-Gruppe mehrere Availability Zones umfasst. Die Regel ist NON_COMPLIANT, wenn die Auto-Scaling-Gruppe nicht mehrere Availability Zones umfasst.

ID: AUTOSCALING_MULTIPLE_AZ

Ressourcentypen: AWS::AutoScaling::AutoScalingGroup

Auslösertyp: Konfigurationsänderungen

AWS-Region: Alle unterstützten AWS Regionen außer Asien-Pazifik (Thailand), Asien-Pazifik (Malaysia), AWS GovCloud (USA-Ost), AWS GovCloud (US-West), Mexiko (Zentral), Kanada West (Calgary)

Parameter:

minAvailabilityZones (Fakultativ), Typ: int

Mindestanzahl der erwarteten Availability Zones.

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

autoscaling-multiple-instance-types

Prüft, ob eine Amazon EC2 Auto Scaling Scaling-Gruppe mehrere Instance-Typen verwendet. Die Regel lautet NON_COMPLIANT, wenn für die Amazon EC2 Auto Scaling Scaling-Gruppe nur ein Instance-Typ definiert ist. Diese Regel bewertet keine attributbasierten Instance-Typen.

ID: AUTOSCALING_MULTIPLE_INSTANCE_TYPES

Ressourcentypen: AWS::AutoScaling::AutoScalingGroup

Auslösertyp: Konfigurationsänderungen

AWS-Region: Alle unterstützten AWS Regionen außer Asien-Pazifik (Thailand), Asien-Pazifik (Malaysia), Mexiko (Zentral) und Kanada West (Calgary)

Parameter:

Keine

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

backup-plan-min-frequency-and-min-retention-check

Prüft, ob ein Backup-Plan über eine Backup-Regel mit der erforderlichen Häufigkeit und Aufbewahrungsdauer verfügt. Die Regel ist NON_COMPLIANT, wenn Wiederherstellungspunkte nicht mindestens so oft wie die angegebene Häufigkeit erstellt werden oder vor dem angegebenen Zeitraum ablaufen.

ID: BACKUP_PLAN_MIN_FREQUENCY_AND_MIN_RETENTION_CHECK

Ressourcentypen: AWS::Backup::BackupPlan

Auslösertyp: Konfigurationsänderungen

AWS-Region: Alle unterstützten AWS Regionen außer China (Peking), Asien-Pazifik (Thailand), Asien-Pazifik (Malaysia), Mexiko (Zentral), Israel (Tel Aviv), Kanada West (Calgary), China (Ningxia)

Parameter:

requiredFrequencyValue (Fakultativ), Typ: int, Standard: 1

Numerischer Wert für die erforderliche Backup-Häufigkeit. Höchstens 24 für Stunden, 31 für Tage.

requiredRetentionDays (Fakultativ), Typ: int, Standard: 35

Erforderlicher Aufbewahrungszeitraum in Tagen.

requiredFrequencyUnit (Fakultativ), Typ: Zeichenfolge, Standard: days

Zeiteinheit für die erforderliche Backup-Häufigkeit. Zulässige Werte: „hours“, „days“.

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unter AWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

backup-recovery-point-encrypted

Prüft, ob ein Wiederherstellungspunkt verschlüsselt ist. Die Regel ist NON_COMPLIANT, wenn der Wiederherstellungspunkt nicht verschlüsselt ist.

ID: BACKUP_RECOVERY_POINT_ENCRYPTED

Ressourcentypen: AWS::Backup::RecoveryPoint

Auslösertyp: Konfigurationsänderungen

AWS-Region: Alle unterstützten AWS Regionen außer China (Peking), Asien-Pazifik (Thailand), Asien-Pazifik (Malaysia), Mexiko (Zentral), Israel (Tel Aviv), Kanada West (Calgary), China (Ningxia)

Parameter:

Keine

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

backup-recovery-point-manual-löschen-deaktiviert

Prüft, ob ein Backup-Tresor über eine zugeordnete ressourcenbasierte Richtlinie verfügt, die das Löschen von Wiederherstellungspunkten verhindert. Die Regel lautet NON_COMPLIANT, wenn der Backup-Tresor keine ressourcenbasierten Richtlinien oder Richtlinien ohne eine geeignete „Deny“ -Anweisung (Anweisung mit den Berechtigungen backup:DeleteRecoveryPoint, backup: und backup:UpdateRecoveryPointLifecycle) hat. PutBackupVaultAccessPolicy

> **Note**
>
> Für und für die Deny-Anweisung ist ein Platzhalter erforderlich **`"Resource"`** **`"Principal"`** Die Regel erfordert, dass das `"Resource"` Ende `"Principal"` der Deny-Anweisung in der Tresorzugriffsrichtlinie einen Platzhalter enthalten muss. Andernfalls gibt die Regel NON_COMPLIANT zurück.

ID: BACKUP_RECOVERY_POINT_MANUAL_DELETION_DISABLED

Ressourcentypen: AWS::Backup::BackupVault

Auslösertyp: Konfigurationsänderungen

AWS-Region: Alle unterstützten AWS Regionen außer China (Peking), Asien-Pazifik (Thailand), Asien-Pazifik (Malaysia), Mexiko (Zentral), Israel (Tel Aviv), Kanada West (Calgary), China (Ningxia)

Parameter:

principalArnList (Fakultativ), Typ: CSV

Durch Kommas getrennte Liste der Amazon-Ressourcennamen () für AWS Identity and Access Management (IAM), die von der Regel NICHT geprüft werden sollen. ARNs

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

backup-recovery-point-minimum-Aufbewahrungsprüfung

Prüft, ob ein Wiederherstellungspunkt frühestens nach Ablauf des angegebenen Zeitraums abläuft. Die Regel ist NON_COMPLIANT, wenn der Aufbewahrungszeitraum des Wiederherstellungspunkts kürzer als der erforderliche Aufbewahrungszeitraum ist.

ID: BACKUP_RECOVERY_POINT_MINIMUM_RETENTION_CHECK

Ressourcentypen: AWS::Backup::RecoveryPoint

Auslösertyp: Konfigurationsänderungen

AWS-Region: Alle unterstützten AWS Regionen außer China (Peking), Asien-Pazifik (Thailand), Asien-Pazifik (Malaysia), Mexiko (Zentral), Israel (Tel Aviv), Kanada West (Calgary), China (Ningxia)

Parameter:

requiredRetentionDays (Fakultativ), Typ: int, Standard: 35

Erforderlicher Aufbewahrungszeitraum in Tagen.

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

batch-compute-environment-enabled

Prüft, ob AWS Batch-Computing-Umgebungen aktiviert sind. Die Regel ist NON_COMPLIANT, wenn Configuration.STATE auf 'DISABLED' gesetzt ist.

Kennung: BATCH_COMPUTE_ENVIRONMENT_ENABLED

Ressourcentypen: AWS::Batch::ComputeEnvironment

Auslösertyp: Konfigurationsänderungen

AWS-Region: Alle unterstützten AWS Regionen außer China (Peking), Asien-Pazifik (Thailand), Asien-Pazifik (Malaysia), Asien-Pazifik (Melbourne), AWS GovCloud (USA-Ost), AWS GovCloud (US-West), Mexiko (Zentral), Israel (Tel Aviv), Kanada West (Calgary), China (Ningxia)

Parameter:

Keine

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

batch-compute-environment-managed

Prüft, ob AWS Batch-Computing-Umgebungen verwaltet werden. Die Regel ist NON_COMPLIANT, wenn Configuration.type auf 'UNMANAGED' gesetzt ist.

Kennung: BATCH_COMPUTE_ENVIRONMENT_MANAGED

Ressourcentypen: AWS::Batch::ComputeEnvironment

Auslösertyp: Konfigurationsänderungen

AWS-Region: Alle unterstützten AWS Regionen außer China (Peking), Asien-Pazifik (Thailand), Asien-Pazifik (Malaysia), Asien-Pazifik (Melbourne), AWS GovCloud (USA-Ost), AWS GovCloud (US-West), Mexiko (Zentral), Israel (Tel Aviv), Kanada West (Calgary), China (Ningxia)

Parameter:

Keine

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

batch-compute-environment-tagged

Prüft, ob AWS Batch-Computing-Umgebungen Tags haben. Optional können Sie Tag-Schlüssel angeben. Die Regel lautet NON_COMPLIANT, wenn keine Tags vorhanden sind oder wenn die angegebenen Tag-Schlüssel nicht vorhanden sind. Die Regel sucht nicht nach Tags, die mit 'aws: 'beginnen.

Kennung: BATCH_COMPUTE_ENVIRONMENT_TAGGED

Ressourcentypen: AWS::Batch::ComputeEnvironment

Auslösertyp: Konfigurationsänderungen

AWS-Region: Alle unterstützten AWS Regionen außer China (Peking), Asien-Pazifik (Thailand), Asien-Pazifik (Malaysia), Asien-Pazifik (Melbourne), AWS GovCloud (USA-Ost), AWS GovCloud (US-West), Mexiko (Zentral), Israel (Tel Aviv), Kanada West (Calgary), China (Ningxia)

Parameter:

requiredKeyTags (Fakultativ), Typ: CSV

> Durch Kommas getrennte Liste von Tag-Schlüsseln, die von der Regel überprüft werden sollen. Falls angegeben, lautet die Regel NON_COMPLIANT, wenn die ausgewertete Ressource diese Schlüssel nicht enthält. Bei Tag-Schlüsseln wird die Groß- und Kleinschreibung beachtet. Tag-Schlüssel, die mit „aws:“ beginnen, sind nicht erlaubt.

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

batch-job-queue-enabled

Prüft, ob AWS Batch-Job-Warteschlangen aktiviert sind. Die Regel ist NON_COMPLIANT, wenn Configuration.STATE auf 'DISABLED' gesetzt ist.

Kennung: BATCH_JOB_QUEUE_ENABLED

Ressourcentypen: AWS::Batch::JobQueue

Auslösertyp: Konfigurationsänderungen

AWS-Region: Alle unterstützten AWS Regionen außer China (Peking), Asien-Pazifik (Thailand), Asien-Pazifik (Malaysia), Asien-Pazifik (Melbourne), AWS GovCloud (US-Ost), AWS GovCloud (US-West), Mexiko (Zentral), Israel (Tel Aviv), Kanada West (Calgary), China (Ningxia)

Parameter:

Keine

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

batch-job-queue-tagged

Prüft, ob AWS Batch-Job-Warteschlangen Tags haben. Optional können Sie Tag-Schlüssel angeben. Die Regel lautet NON_COMPLIANT, wenn keine Tags vorhanden sind oder wenn die angegebenen Tag-Schlüssel nicht vorhanden sind. Die Regel sucht nicht nach Tags, die mit 'aws: 'beginnen.

Kennung: BATCH_JOB_QUEUE_TAGGED

Ressourcentypen: AWS::Batch::JobQueue

Auslösertyp: Konfigurationsänderungen

AWS-Region: Alle unterstützten AWS Regionen außer China (Peking), Asien-Pazifik (Thailand), Asien-Pazifik (Malaysia), Asien-Pazifik (Melbourne), AWS GovCloud (USA-Ost), AWS GovCloud (US-West), Mexiko (Zentral), Israel (Tel Aviv), Kanada West (Calgary), China (Ningxia)

Parameter:

requiredKeyTags (Fakultativ), Typ: CSV

> Durch Kommas getrennte Liste von Tag-Schlüsseln, die von der Regel überprüft werden sollen. Falls angegeben, lautet die Regel NON_COMPLIANT, wenn die ausgewertete Ressource diese Schlüssel nicht enthält. Bei Tag-Schlüsseln wird die Groß- und Kleinschreibung beachtet. Tag-Schlüssel, die mit „aws:“ beginnen, sind nicht erlaubt.

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

batch-managed-compute-environment-using-launch-template

Überprüft, ob AWS Batch-verwaltete Rechenumgebungen mithilfe einer Startvorlage konfiguriert sind. Bei der Konfiguration lautet die Regel NON_COMPLIANT. ComputeResources. LaunchTemplate existiert nicht.

Kennung: BATCH_MANAGED_COMPUTE_ENVIRONMENT_USING_LAUNCH_TEMPLATE

Ressourcentypen: AWS::Batch::ComputeEnvironment

Auslösertyp: Konfigurationsänderungen

AWS-Region: Alle unterstützten AWS Regionen außer China (Peking), Asien-Pazifik (Thailand), Asien-Pazifik (Malaysia), Asien-Pazifik (Melbourne), AWS GovCloud (US-Ost), AWS GovCloud (US-West), Mexiko (Zentral), Israel (Tel Aviv), Kanada West (Calgary), China (Ningxia)

Parameter:

Keine

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

batch-managed-compute-env-compute-resources-tagged

Prüft, ob die Rechenressourcen von AWS Batch-verwalteten Rechenumgebungen über Tags verfügen. Optional können Sie Tag-Schlüssel angeben. Die Regel lautet NON_COMPLIANT, wenn keine Tags vorhanden sind oder wenn die angegebenen Tag-Schlüssel nicht vorhanden sind. Tags, die mit 'aws: 'beginnen, werden nicht geprüft.

Kennung: BATCH_MANAGED_COMPUTE_ENV_COMPUTE_RESOURCES_TAGGED

Ressourcentypen: AWS::Batch::ComputeEnvironment

Auslösertyp: Konfigurationsänderungen

AWS-Region: Alle unterstützten AWS Regionen außer China (Peking), Asien-Pazifik (Thailand), Asien-Pazifik (Malaysia), Asien-Pazifik (Melbourne), AWS GovCloud (USA-Ost), AWS GovCloud (US-West), Mexiko (Zentral), Israel (Tel Aviv), Kanada West (Calgary), China (Ningxia)

Parameter:

requiredKeyTags (Fakultativ), Typ: CSV

> Durch Kommas getrennte Liste von Tag-Schlüsseln, die von der Regel überprüft werden sollen. Falls angegeben, lautet die Regel NON_COMPLIANT, wenn die ausgewertete Ressource diese Schlüssel nicht enthält. Bei Tag-Schlüsseln wird die Groß- und Kleinschreibung beachtet. Tag-Schlüssel, die mit „aws:“ beginnen, sind nicht erlaubt.

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

batch-scheduling-policy-tagged

Prüft, ob Richtlinien zur AWS Batch-Planung Tags haben. Optional können Sie Tag-Schlüssel angeben. Die Regel lautet NON_COMPLIANT, wenn keine Tags vorhanden sind oder wenn die angegebenen Tag-Schlüssel nicht vorhanden sind. Die Regel sucht nicht nach Tags, die mit 'aws: 'beginnen.

Kennung: BATCH_SCHEDULING_POLICY_TAGGED

Ressourcentypen: AWS::Batch::SchedulingPolicy

Auslösertyp: Konfigurationsänderungen

AWS-Region: Alle unterstützten AWS Regionen außer China (Peking), Asien-Pazifik (Thailand), Asien-Pazifik (Malaysia), AWS GovCloud (USA-Ost), AWS GovCloud (US-West), Mexiko (Zentral), China (Ningxia)

Parameter:

requiredKeyTags (Fakultativ), Typ: CSV

> Durch Kommas getrennte Liste von Tag-Schlüsseln, die von der Regel überprüft werden sollen. Falls angegeben, lautet die Regel NON_COMPLIANT, wenn die ausgewertete Ressource diese

Schlüssel nicht enthält. Bei Tag-Schlüsseln wird die Groß- und Kleinschreibung beachtet. Tag-Schlüssel, die mit „aws:“ beginnen, sind nicht erlaubt.

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

beanstalk-enhanced-health-reporting-aktiviert

Prüft, ob eine AWS Elastic Beanstalk Beanstalk-Umgebung für erweiterte Statusberichte konfiguriert ist. Die Regel ist COMPLIANT, wenn die Umgebung für erweiterte Zustandsberichte konfiguriert ist. Die Regel ist NON_COMPLIANT, wenn die Umgebung für grundlegende Zustandsberichte konfiguriert ist.

ID: BEANSTALK_ENHANCED_HEALTH_REPORTING_ENABLED

Ressourcentypen: AWS::ElasticBeanstalk::Environment

Auslösertyp: Konfigurationsänderungen

AWS-Region: Alle unterstützten AWS Regionen außer Asien-Pazifik (Thailand), Asien-Pazifik (Jakarta), Naher Osten (VAE), Asien-Pazifik (Hyderabad), Asien-Pazifik (Osaka), Asien-Pazifik (Malaysia), Asien-Pazifik (Melbourne), Mexiko (Zentral), Israel (Tel Aviv), Asien-Pazifik (Taipeh), Kanada West (Calgary), Europa (Spanien), Europa (Zürich)

Parameter:

Keine

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

cassandra-keyspace-tagged

Prüft, ob Amazon Keyspaces (für Apache Cassandra) Tags haben. Optional können Sie Tag-Schlüssel angeben. Die Regel lautet NON_COMPLIANT, wenn keine Tags vorhanden sind oder

wenn die angegebenen Tag-Schlüssel nicht vorhanden sind. Die Regel sucht nicht nach Tags, die mit 'aws: 'beginnen.

Kennung: CASSANDRA_KEYSPACE_TAGGED

Ressourcentypen: AWS::Cassandra::Keyspace

Auslösertyp: Konfigurationsänderungen

AWS-Region: Nur verfügbar in Europa (Stockholm), Naher Osten (Bahrain), Asien-Pazifik (Mumbai), Europa (Paris), USA Ost (Ohio), Europa (Irland), Europa (Frankfurt), Südamerika (Sao Paulo), Asien-Pazifik (Hongkong), USA Ost (Nord-Virginia), Asien-Pazifik (Seoul), Europa (London), Asien-Pazifik (Tokio), USA West (Oregon), USA West (Nordkalifornien), Asien-Pazifik (Tokio), USA West (Oregon), USA West (Nordkalifornien), Asien-Pazifik (Singapur), Asien-Pazifik (Sydney), Region Kanada (Zentral)

Parameter:

requiredKeyTags (Fakultativ), Typ: CSV

> Durch Kommas getrennte Liste von Tag-Schlüsseln, die von der Regel überprüft werden sollen. Falls angegeben, lautet die Regel NON_COMPLIANT, wenn die ausgewertete Ressource diese Schlüssel nicht enthält. Bei Tag-Schlüsseln wird die Groß- und Kleinschreibung beachtet. Tag-Schlüssel, die mit „aws:“ beginnen, sind nicht erlaubt.

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

clb-desync-mode-check

Prüft, ob für Classic Load Balancers (CLB) ein benutzerdefinierter desynchroner Mitigationsmodus konfiguriert ist. Die Regel ist NON_COMPLIANT, wenn der desynchrone Mitigationsmodus der CLBs nicht mit dem benutzerdefinierten desynchronen Mitigationsmodus übereinstimmt.

ID: CLB_DESYNC_MODE_CHECK

Ressourcentypen: AWS::ElasticLoadBalancing::LoadBalancer

Auslösertyp: Konfigurationsänderungen

AWS-Region: Alle unterstützten AWS Regionen außer Asien-Pazifik (Thailand), Naher Osten (VAE), Asien-Pazifik (Hyderabad), Asien-Pazifik (Malaysia), Asien-Pazifik (Melbourne), Mexiko (Zentral), Israel (Tel Aviv), Kanada West (Calgary), Europa (Spanien), Europa (Zürich)

Parameter:

desyncMode, Typ: CSV

> Eine durch Kommata getrennte Liste der Werte. Sie können maximal zwei auswählen. Zu den zulässigen Werten gehören „Defensiv“, „Am strengsten“ und „Überwachen“.

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

clb-multiple-az

Prüft, ob ein Classic Load Balancer mehrere Availability Zones () AZs umfasst. Die Regel lautet NON_COMPLIANT, wenn sich ein Classic Load Balancer über weniger als 2 erstreckt AZs oder nicht die Anzahl der im `minAvailabilityZones` Parameter AZs genannten (falls angegeben) umfasst.

ID: CLB_MULTIPLE_AZ

Ressourcentypen: AWS::ElasticLoadBalancing::LoadBalancer

Auslösertyp: Konfigurationsänderungen

AWS-Region: Alle unterstützten AWS Regionen außer Asien-Pazifik (Thailand), Asien-Pazifik (Malaysia), AWS GovCloud (USA-Ost), AWS GovCloud (US-West), Mexiko (Zentral), Kanada West (Calgary)

Parameter:

minAvailabilityZones (Fakultativ), Typ: int

> Gewünschte Mindestanzahl der erwarteten AZs. Zulässig sind alle Werte zwischen 2 und 10, beide inklusive. Der Standardwert ist 2, falls dieser Parameter nicht angegeben ist.

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

cloudformation-stack-drift-detection-überprüfen

Prüft, ob die tatsächliche Konfiguration eines AWS CloudFormation (AWS CloudFormation) -Stacks von der erwarteten Konfiguration abweicht oder von der erwarteten Konfiguration abweicht. Für einen Stack wird eine Abweichung konstatiert, wenn sich mindestens eine seiner Ressourcen von der erwarteten Konfiguration unterscheidet. Regel und Stack sind COMPLIANT, wenn der Status der Stack-Abweichung IN_SYNC lautet. Die Regel ist NON_COMPLIANT, wenn der Abweichungsstatus des Stacks ABGEWICHEN lautet.

> **Note**
>
> Diese Regel führt den DetectStackDrift Vorgang für jeden Stack in Ihrem Konto aus. Der DetectStackDrift Vorgang kann je nach Anzahl der im Stack enthaltenen Ressourcen bis zu mehreren Minuten dauern. Da die maximale Ausführungszeit dieser Regel auf 15 Minuten begrenzt ist, kann es vorkommen, dass für die Regel eine Zeitüberschreitung auftritt, bevor die Auswertung aller Stacks in Ihrem Konto abgeschlossen ist.
> Wenn Sie auf dieses Problem stoßen, sollten Sie die Anzahl der Stacks, die für die Regel gelten, mithilfe von Tags beschränken. Sie haben die folgenden Möglichkeiten:
>
> 1. Teilen Sie Ihre Stacks in Gruppen ein, jede mit einem anderen Tag.
> 2. Wenden Sie dasselbe Tag auf alle Stacks in dieser Gruppe an.
> 3. Achten Sie darauf, dass Ihr Konto über mehrere Instances dieser Regel verfügt, die jeweils von einem anderen Tag beschränkt sind. Dadurch kann jede Instance der Regel nur die Stacks verarbeiten, deren Gültigkeitsbereich das entsprechende Tag enthält.

ID: CLOUDFORMATION_STACK_DRIFT_DETECTION_CHECK

Ressourcentypen: AWS::CloudFormation::Stack

Auslösertyp: „Konfigurationsänderungen“ und „Regelmäßig“

AWS-Region: Alle unterstützten AWS Regionen außer Asien-Pazifik (Jakarta), Naher Osten (VAE), Asien-Pazifik (Hyderabad), Asien-Pazifik (Melbourne), Israel (Tel Aviv), Kanada West (Calgary), Europa (Spanien), Europa (Zürich)

Parameter:

cloudformationRoleArn, Typ: Zeichenfolge

Der Amazon-Ressourcenname (ARN) der IAM-Rolle mit Richtlinienberechtigungen zur Erkennung von Abweichungen bei AWS CloudFormation Stacks. Informationen zu den erforderlichen IAM-Berechtigungen für die Rolle finden Sie unter Erkennen nicht verwalteter Konfigurationsänderungen an Stacks und Ressourcen | Überlegungen zur Erkennung von Abweichungen im Benutzerhandbuch.AWS CloudFormation

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

cloudformation-stack-notification-check

Überprüft, ob Ihre CloudFormation Stacks Ereignisbenachrichtigungen an ein Amazon SNS SNS-Thema senden. Prüft optional, ob festgelegte Amazon-SNS-Themen verwendet werden. Die Regel lautet NON_COMPLIANT, wenn CloudFormation Stacks keine Benachrichtigungen senden.

ID: CLOUDFORMATION_STACK_NOTIFICATION_CHECK

Ressourcentypen: AWS::CloudFormation::Stack

Auslösertyp: Konfigurationsänderungen

AWS-Region: Alle unterstützten AWS Regionen außer Asien-Pazifik (Thailand), Asien-Pazifik (Jakarta), Naher Osten (VAE), Asien-Pazifik (Hyderabad), Asien-Pazifik (Malaysia), Asien-Pazifik (Melbourne), Mexiko (Zentral), Israel (Tel Aviv), Asien-Pazifik (Taipeh), Kanada West (Calgary), Europa (Spanien), Europa (Zürich)

Parameter:

snsTopic1 (optional), Typ: Zeichenfolge

SNS-Thema-ARN.

snsTopic2 (optional), Typ: Zeichenfolge

SNS-Thema-ARN.

snsTopic3 (optional), Typ: Zeichenfolge

SNS-Thema-ARN.

snsTopic4 (optional), Typ: Zeichenfolge

SNS-Thema-ARN.

snsTopic5 (optional), Typ: Zeichenfolge

SNS-Thema-ARN.

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

cloudfront-accesslogs-enabled

Prüft, ob CloudFront Amazon-Distributionen so konfiguriert sind, dass sie mithilfe der Standardprotokollierung (Legacy) Zugriffsprotokolle an einen Amazon S3-Bucket übermitteln. Die Regel lautet NON_COMPLIANT, wenn für eine CloudFront Distribution keine Legacy-Protokollierung konfiguriert ist.

ID: CLOUDFRONT_ACCESSLOGS_ENABLED

Ressourcentypen: AWS::CloudFront::Distribution

Auslösertyp: Konfigurationsänderungen

AWS-Region: Nur in der Region USA Ost (Nord-Virginia) verfügbar

Parameter:

S3 BucketName (fakultativ), Typ: Zeichenfolge

Der Name des Amazon-S3-Buckets, in dem die Serverzugriffsprotokolle gespeichert werden.

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

cloudfront-associated-with-waf

Prüft, ob CloudFront Amazon-Distributionen entweder mit Web Application Firewall (WAF) oder WAFv2 Web Access Control Lists (ACLs) verknüpft sind. Die Regel lautet NON_COMPLIANT, wenn eine CloudFront Distribution keiner WAF-Web-ACL zugeordnet ist.

ID: CLOUDFRONT_ASSOCIATED_WITH_WAF

Ressourcentypen: AWS::CloudFront::Distribution

Auslösertyp: Konfigurationsänderungen

AWS-Region: Nur in der Region USA Ost (Nord-Virginia) verfügbar

Parameter:

wafWebAclIDs (optional), Typ: CSV

> Durch Kommas getrennte Liste von Web-ACL IDs für WAF oder Web-ACLs Amazon Resource Names () ARNs für. WAFV2

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

cloudfront-custom-ssl-certificate

Prüft, ob das mit einer CloudFront Amazon-Distribution verknüpfte Zertifikat das Standard-SSL-Zertifikat ist. Die Regel lautet NON_COMPLIANT, wenn eine CloudFront Distribution das Standard-SSL-Zertifikat verwendet.

ID: CLOUDFRONT_CUSTOM_SSL_CERTIFICATE

Ressourcentypen: AWS::CloudFront::Distribution

Auslösertyp: Konfigurationsänderungen

AWS-Region: Nur in der Region USA Ost (Nord-Virginia) verfügbar

Parameter:

Keine

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

cloudfront-default-root-object-konfiguriert

Prüft, ob eine CloudFront Amazon-Distribution so konfiguriert ist, dass sie ein bestimmtes Objekt zurückgibt, das das Standard-Root-Objekt ist. Die Regel lautet NON_COMPLIANT, wenn bei Amazon CloudFront Distribution kein Standard-Root-Objekt konfiguriert ist.

ID: CLOUDFRONT_DEFAULT_ROOT_OBJECT_CONFIGURED

Ressourcentypen: AWS::CloudFront::Distribution

Auslösertyp: Konfigurationsänderungen

AWS-Region: Nur in der Region USA Ost (Nord-Virginia) verfügbar

Parameter:

Keine

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

cloudfront-no-deprecated-ssl-protokolle

Überprüft, ob CloudFront Distributionen veraltete SSL-Protokolle für die HTTPS-Kommunikation zwischen CloudFront Edge-Standorten und benutzerdefinierten Ursprüngen verwenden. Diese Regel ist NON_COMPLIANT für eine CloudFront Verteilung, wenn eine " " enthält. OriginSslProtocols SSLv3

ID: CLOUDFRONT_NO_DEPRECATED_SSL_PROTOCOLS

Ressourcentypen: AWS::CloudFront::Distribution

Auslösertyp: Konfigurationsänderungen

AWS-Region: Nur in der Region USA Ost (Nord-Virginia) verfügbar

Parameter:

Keine

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

cloudfront-origin-access-identity-aktiviert

Überprüft, ob für den CloudFront Vertrieb mit dem Origin-Typ Amazon S3 die Ursprungszugriffsidentität konfiguriert ist. Die Regel lautet NON_COMPLIANT, wenn die CloudFront Verteilung von S3 unterstützt wird und ein Quelltyp nicht OAI-konfiguriert ist oder der Ursprung kein S3-Bucket ist.

> **Note**
>
> Die Regel kehrt nicht zurück, `NOT_APPLICABLE` wenn der Ursprung kein S3-Bucket ist.

ID: CLOUDFRONT_ORIGIN_ACCESS_IDENTITY_ENABLED

Ressourcentypen: AWS::CloudFront::Distribution

Auslösertyp: Konfigurationsänderungen

AWS-Region: Nur in der Region USA Ost (Nord-Virginia) verfügbar

Parameter:

Keine

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

cloudfront-origin-failover-enabled

Prüft, ob eine Ursprungsgruppe für die Verteilung von mindestens zwei Ursprüngen in der Ursprungsgruppe für Amazon konfiguriert ist CloudFront. Die Regel ist NON_COMPLIANT, wenn es keine Ursprungsgruppen für die Verteilung gibt.

ID: CLOUDFRONT_ORIGIN_FAILOVER_ENABLED

Ressourcentypen: AWS::CloudFront::Distribution

Auslösertyp: Konfigurationsänderungen

AWS-Region: Nur in der Region USA Ost (Nord-Virginia) verfügbar

Parameter:

Keine

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

Wolkenfront - 3 origin-access-control-enabled

Prüft, ob bei einer CloudFront Amazon-Distribution mit einem Amazon Simple Storage Service (Amazon S3) Origin Access Control (OAC) aktiviert ist. Die Regel lautet NON_COMPLIANT für CloudFront Distributionen mit Amazon S3 S3-Ursprung, für die OAC nicht aktiviert ist.

ID: CLOUDFRONT_S3_ORIGIN_ACCESS_CONTROL_ENABLED

Ressourcentypen: AWS::CloudFront::Distribution

Auslösertyp: Konfigurationsänderungen

AWS-Region: Nur in der Region USA Ost (Nord-Virginia) verfügbar

Parameter:

Keine

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

Wolkenfront - 3 origin-non-existent-bucket

Prüft, ob CloudFront Amazon-Distributionen auf einen nicht existierenden S3-Bucket verweisen. Die Regel lautet NON_COMPLIANT, wenn `S3 OriginConfig `für eine CloudFront Verteilung auf einen nicht existierenden S3-Bucket verweist. Die Regel bewertet keine S3-Buckets mit Hosting für statische Websites.

ID: CLOUDFRONT_S3_ORIGIN_NON_EXISTENT_BUCKET

Ressourcentypen: AWS::CloudFront::Distribution

Auslösertyp: Regelmäßig

AWS-Region: Nur in den Regionen China (Peking) und USA Ost (Nord-Virginia) verfügbar

Parameter:

Keine

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

cloudfront-security-policy-check

Überprüft, ob CloudFront Amazon-Distributionen eine Mindestsicherheitsrichtlinie und eine Verschlüsselungssuite von TLSv1 .2 oder höher für Zuschauerverbindungen verwenden. Diese Regel ist NON_COMPLIANT für eine CloudFront Distribution, deren Wert unter .2_2018 liegt. minimumProtocolVersion TLSv1

ID: CLOUDFRONT_SECURITY_POLICY_CHECK

Ressourcentypen: AWS::CloudFront::Distribution

Auslösertyp: Konfigurationsänderungen

AWS-Region: Nur in der Region USA Ost (Nord-Virginia) verfügbar

Parameter:

Keine

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

cloudfront-sni-enabled

Prüft, ob CloudFront Amazon-Distributionen ein benutzerdefiniertes SSL-Zertifikat verwenden und so konfiguriert sind, dass SNI zur Bearbeitung von HTTPS-Anfragen verwendet wird. Die Regel ist NON_COMPLIANT, wenn ein benutzerdefiniertes SSL-Zertifikat zugeordnet ist, die SSL-Unterstützungsmethode jedoch eine dedizierte IP-Adresse ist.

ID: CLOUDFRONT_SNI_ENABLED

Ressourcentypen: AWS::CloudFront::Distribution

Auslösertyp: Konfigurationsänderungen

AWS-Region: Nur in der Region USA Ost (Nord-Virginia) verfügbar

Parameter:

Keine

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

cloudfront-ssl-policy-check

Überprüft, ob CloudFront Amazon-Distributionen mit den angegebenen Sicherheitsrichtlinien konfiguriert sind. Die Regel lautet NON_COMPLIANT, wenn eine CloudFront Distribution nicht mit den von Ihnen angegebenen Sicherheitsrichtlinien konfiguriert ist.

Kennung: CLOUDFRONT_SSL_POLICY_CHECK

Ressourcentypen: AWS::CloudFront::Distribution

Auslösertyp: Konfigurationsänderungen

AWS-Region: Nur in der Region USA Ost (Nord-Virginia) verfügbar

Parameter:

Sicherheitsrichtlinien, Typ: CSV

> Durch Kommas getrennte Liste von Sicherheitsrichtlinien für die CloudFront Verteilung, die von der Regel überprüft werden sollen. Zum Beispiel: "TLSv1.2_2018, .2_2019, TLSv1 .2_2021". TLSv1 Eine Liste der gültigen Werte finden Sie im Amazon CloudFront Developer Guide.

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

cloudfront-traffic-to-origin-verschlüsselt

Überprüft, ob CloudFront Amazon-Distributionen den Datenverkehr zu benutzerdefinierten Ursprüngen verschlüsseln. Die Regel ist NON_COMPLIANT, wenn '' für 'nurOriginProtocolPolicy' HTTP 'steht oder wenn' 'für' Match-Viewer 'steht und' OriginProtocolPolicy 'für 'Allow-All' steht. ViewerProtocolPolicy

ID: CLOUDFRONT_TRAFFIC_TO_ORIGIN_ENCRYPTED

Ressourcentypen: AWS::CloudFront::Distribution

Auslösertyp: Konfigurationsänderungen

AWS-Region: Nur in der Region USA Ost (Nord-Virginia) verfügbar

Parameter:

Keine

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

cloudfront-viewer-policy-https

Prüft, ob Ihre CloudFront Amazon-Distributionen HTTPS verwenden (direkt oder über eine Umleitung). Die Regel lautet NON_COMPLIANT, wenn der Wert von auf 'allow-all' für oder für gesetzt ViewerProtocolPolicy ist. DefaultCacheBehavior CacheBehaviors

ID: CLOUDFRONT_VIEWER_POLICY_HTTPS

Ressourcentypen: AWS::CloudFront::Distribution

Auslösertyp: Konfigurationsänderungen

AWS-Region: Nur in der Region USA Ost (Nord-Virginia) verfügbar

Parameter:

Keine

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

cloudtrail-all-read-s3- data-event-check

Überprüft, ob ein AWS CloudTrail Multi-Regions-Trail aktiviert ist, und protokolliert alle gelesenen S3-Datenereignisse für Ihre Buckets. Die Regel lautet NON_COMPLIANT, wenn kein Multiregion-Trail alle gelesenen S3-Datenereignistypen für alle aktuellen und future S3-Buckets protokolliert.

Kennung: CLOUDTRAIL_ALL_READ_S3_DATA_EVENT_CHECK

Ressourcentypen: AWS::::Account

Auslösertyp: Regelmäßig

AWS-Region: Alle unterstützten AWS Regionen außer China (Peking), Asien-Pazifik (Thailand), Asien-Pazifik (Malaysia), Mexiko (Zentral) und Kanada West (Calgary)

Parameter:

Keine

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

cloudtrail-all-write-s3- data-event-check

Überprüft, ob ein Trail AWS CloudTrail mit mehreren Regionen aktiviert ist, und protokolliert alle S3-Schreibdatenereignisse für Ihre Buckets. Die Regel lautet NON_COMPLIANT, wenn kein Trail mit mehreren Regionen alle S3-Schreibdatenereignistypen für alle aktuellen und future S3-Buckets protokolliert.

Kennung: CLOUDTRAIL_ALL_WRITE_S3_DATA_EVENT_CHECK

Ressourcentypen: AWS::::Account

Auslösertyp: Regelmäßig

AWS-Region: Alle unterstützten AWS Regionen außer China (Peking), Asien-Pazifik (Thailand), Asien-Pazifik (Malaysia), Mexiko (Zentral) und Kanada West (Calgary)

Parameter:

Keine

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

Wolkenspur-S3- bucket-access-logging

Prüft, ob in den S3-Bucket-Konfigurationen für Ihre AWS CloudTrail Protokolle die Protokollierung des Amazon S3 S3-Serverzugriffs aktiviert ist. Die Regel lautet NON_COMPLIANT, wenn für mindestens einen S3-Bucket für einen CloudTrail Trail die Protokollierung des S3-Serverzugriffs nicht aktiviert ist.

Kennung: CLOUDTRAIL_S3_BUCKET_ACCESS_LOGGING

Ressourcentypen: AWS::CloudTrail::Trail

Auslösertyp: Regelmäßig

AWS-Region: Alle unterstützten AWS Regionen außer Asien-Pazifik (Thailand), Asien-Pazifik (Malaysia), Mexiko (Zentral) und Kanada West (Calgary)

Parameter:

Keine

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

Wolkenspur-S3- bucket-public-access-prohibited

Prüft, ob die S3-Bucket-Konfigurationen für Ihre AWS CloudTrail Logs den öffentlichen Zugriff blockieren. Die Regel lautet NON_COMPLIANT, wenn mindestens ein S3-Bucket für einen CloudTrail Trail öffentlich zugänglich ist.

Kennung: CLOUDTRAIL_S3_BUCKET_PUBLIC_ACCESS_PROHIBITED

Ressourcentypen: AWS::CloudTrail::Trail

Auslösertyp: Regelmäßig

AWS-Region: Alle unterstützten AWS Regionen außer Asien-Pazifik (Thailand), Asien-Pazifik (Malaysia), Mexiko (Zentral) und Kanada West (Calgary)

Parameter:

Keine

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

cloudtrail-s3-dataevents-enabled

Überprüft, ob mindestens ein AWS CloudTrail Trail Amazon Simple Storage Service (Amazon S3) - Datenereignisse für alle S3-Buckets protokolliert. Die Regel ist NON_COMPLIANT, wenn es keine Trails gibt oder wenn keine Trails S3-Datenereignisse aufzeichnen.

ID: CLOUDTRAIL_S3_DATAEVENTS_ENABLED

Auslösertyp: Regelmäßig

AWS-Region: Alle unterstützten AWS Regionen außer der Region Asien-Pazifik (Taipeh)

Parameter:

S3 BucketNames (optional), Typ: Zeichenfolge

Durch Kommata getrennte Liste von S3-Bucket-Namen, für die die Protokollierung von Datenereignissen aktiviert werden soll. Standardverhaltensüberprüfungen für alle S3-Buckets.

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

cloudtrail-security-trail-enabled

Überprüft, ob mindestens ein AWS CloudTrail Pfad mit bewährten Sicherheitsmethoden definiert ist. Diese Regel ist COMPLIANT, wenn es mindestens einen Trail gibt, der alle der folgenden Bedingungen erfüllt:

- Er zeichnet globale Serviceereignisse auf.
- Es ist ein multiregionaler Trail.
- Die Protokolldateivalidierung ist für ihn aktiviert.
- Er ist mit einem KMS-Schlüssel verschlüsselt.
- Er zeichnet Ereignisse für Lese- und Schreibvorgänge auf.
- Er zeichnet Verwaltungsereignisse auf.
- Er schließt keine Verwaltungsereignisse aus.

Diese Regel ist NON_COMPLIANT, wenn kein Trail alle oben genannten Kriterien erfüllt.

ID: CLOUDTRAIL_SECURITY_TRAIL_ENABLED

Auslösertyp: Regelmäßig

AWS-Region: Alle unterstützten AWS Regionen

Parameter:

Keine

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

cloudwatch-alarm-action-check

Prüft, ob für CloudWatch Alarme eine Aktion für den Status ALARM, INSUFFICIENT_DATA oder OK konfiguriert ist. Prüft optional, ob Aktionen mit einem benannten ARN übereinstimmen. Die Regel ist NON_COMPLIANT, wenn für den Alarm oder den optionalen Parameter keine Aktion festgelegt ist.

ID: CLOUDWATCH_ALARM_ACTION_CHECK

Ressourcentypen: AWS::CloudWatch::Alarm

Auslösertyp: Konfigurationsänderungen

AWS-Region: Alle unterstützten AWS Regionen

Parameter:

alarmActionRequired, Typ: Zeichenfolge, Standard: true

Alarme verfügen mindestens über eine Aktion.

insufficientDataActionErforderlich, Typ: Zeichenfolge, Standard: true

Alarme verfügen über mindestens eine Aktion, wenn der Alarm von einem beliebigen anderen Status auf den Status INSUFFICIENT_DATA übergeht.

okActionRequired, Typ: Zeichenfolge, Standard: false

Alarme verfügen über mindestens eine Aktion, wenn der Alarm von einem beliebigen anderen Status auf den Status OK übergeht.

action1 (optional), Typ: Zeichenfolge

Die auszuführende Aktion, die als ARN angegeben ist.

action2 (optional), Typ: Zeichenfolge

Die auszuführende Aktion, die als ARN angegeben ist.

action3 (optional), Typ: Zeichenfolge

Die auszuführende Aktion, die als ARN angegeben ist.

action4 (optional), Typ: Zeichenfolge

Die auszuführende Aktion, die als ARN angegeben ist.

action5 (optional), Typ: Zeichenfolge

Die auszuführende Aktion, die als ARN angegeben ist.

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

cloudwatch-alarm-action-enabled-überprüfen

Prüft, ob die CloudWatch Amazon-Alarmaktionen aktiviert sind. Die Regel lautet NON_COMPLIANT, wenn sich die CloudWatch Alarmaktionen nicht im Status aktiviert befinden.

ID: CLOUDWATCH_ALARM_ACTION_ENABLED_CHECK

Ressourcentypen: AWS::CloudWatch::Alarm

Auslösertyp: Konfigurationsänderungen

AWS-Region: Alle unterstützten AWS Regionen außer Asien-Pazifik (Thailand), Asien-Pazifik (Malaysia), AWS GovCloud (USA-Ost), AWS GovCloud (US-West), Mexiko (Zentral), Kanada West (Calgary)

Parameter:

Keine

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

cloudwatch-alarm-resource-check

Prüft, ob ein Ressourcentyp einen CloudWatch Alarm für die benannte Metrik hat. Als Ressourcentyp können Sie EBS-Volumes, EC2 Instances, Amazon RDS-Cluster oder S3-Buckets angeben. Die Regel ist KONFORM, wenn die benannte Metrik eine Ressourcen-ID und CloudWatch einen Alarm hat.

ID: CLOUDWATCH_ALARM_RESOURCE_CHECK

Ressourcentypen: AWS::EC2::Instance, AWS::RDS::DBCluster, AWS::S3::Bucket, AWS::EC2::Volume

Auslösertyp: Regelmäßig

AWS-Region: Alle unterstützten AWS Regionen

Parameter:

RessourcenTyp, Typ: Zeichenfolge

AWS Ressourcentyp. Der Wert kann einer der folgenden sein: AWS::EC2::Volume AWS::EC2::Instance, AWS::RDS::DBCluster, oder AWS::S3::Bucket.

metricName, Typ: Zeichenfolge

Der Name der Metrik, die dem Alarm zugeordnet ist (z. B. 'CPUUtilization' für EC2 Instanzen).

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

cloudwatch-alarm-settings-check

Überprüft, ob CloudWatch Alarme mit dem angegebenen Metriknamen die angegebenen Einstellungen haben.

ID: CLOUDWATCH_ALARM_SETTINGS_CHECK

Ressourcentypen: AWS::CloudWatch::Alarm

Auslösertyp: Konfigurationsänderungen

AWS-Region: Alle unterstützten AWS Regionen

Parameter:

metricName, Typ: Zeichenfolge

Der Name für die dem Alarm zugehörige Metrik.

threshold (optional), Typ: int

Der Wert, mit dem die angegebene Statistik verglichen wird.

evaluationPeriods (optional), Typ: int

Die Anzahl der Zeiträume, über die Daten mit dem angegebenen Schwellenwert verglichen werden.

period (optional), Typ: int, Standard: 300

Der Zeitraum in Sekunden, in dem die angegebene Statistik angewendet wird.

comparisonOperator (optional), Typ: Zeichenfolge

Die Operation zum Vergleichen der angegebenen Statistik und des angegebenen Schwellenwerts (z. B. 'GreaterThanThreshold').

statistic (optional), Typ: Zeichenfolge

Die Statistik für die Metrik, die dem Alarm zugewiesen ist (z. B. „Average“ oder „Sum“).

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

cloudwatch-log-group-encrypted

Prüft, ob Amazon CloudWatch Log Groups mit einem beliebigen AWS KMS-Schlüssel oder einer angegebenen AWS KMS-Schlüssel-ID verschlüsselt sind. Die Regel lautet NON_COMPLIANT, wenn eine CloudWatch Protokollgruppe nicht mit einem KMS-Schlüssel oder mit einem KMS-Schlüssel verschlüsselt ist, der nicht im Regelparameter angegeben ist.

ID: CLOUDWATCH_LOG_GROUP_ENCRYPTED

Ressourcentypen: AWS::Logs::LogGroup

Auslösertyp: Regelmäßig

AWS-Region: Alle unterstützten AWS Regionen außer Naher Osten (VAE) und Asien-Pazifik (Taipeh)

Parameter:

KmsKeyId (Fakultativ), Typ: Zeichenfolge

> Amazon-Ressourcenname (ARN) der ID für den KMS-Schlüssel, der zum Verschlüsseln der Protokollgruppe verwendet wird.

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

cloud-trail-cloud-watch-logs-aktiviert

Prüft, ob AWS CloudTrail Trails so konfiguriert sind, dass sie Logs an CloudWatch Logs senden. Der Trail ist NON_COMPLIANT, wenn die CloudWatchLogsLogGroupArn Eigenschaft des Trails leer ist.

ID: CLOUD_TRAIL_CLOUD_WATCH_LOGS_ENABLED

Ressourcentypen: AWS::CloudTrail::Trail

Auslösertyp: Regelmäßig

AWS-Region: Alle unterstützten AWS Regionen

Parameter:

expectedDeliveryWindowAlter (fakultativ), Typ: int

> Höchstalter in Stunden ab der letzten Übermittlung von CloudWatch Protokollen, die den Vorschriften entsprechen.

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

cloudtrail-enabled

> **Important**
>
> Bei dieser Regel unterscheiden sich die Regel-ID (CLOUD_TRAIL_ENABLED) und der Regelname (cloudtrail-enabled).

Prüft, ob in Ihrem AWS Konto ein AWS CloudTrail Trail aktiviert ist. Die Regel ist NON_COMPLIANT, wenn ein Trail nicht aktiviert ist. Optional überprüft die Regel einen bestimmten S3-Bucket, ein Amazon Simple Notification Service (Amazon SNS) -Thema und eine CloudWatch Protokollgruppe.

ID: CLOUD_TRAIL_ENABLED

Auslösertyp: Regelmäßig

AWS-Region: Alle unterstützten Regionen AWS

Parameter:

s3 BucketName (fakultativ), Typ: Zeichenfolge

Name des S3-Buckets CloudTrail , an den Protokolldateien gesendet werden sollen.

snsTopicArn (Fakultativ), Typ: Zeichenfolge

SNS-Thema ARN CloudTrail zur Verwendung für Benachrichtigungen.

cloudWatchLogsLogGroupArn (Fakultativ), Typ: Zeichenfolge

CloudWatch Loggruppen-ARN CloudTrail , an die Daten gesendet werden sollen.

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

cloud-trail-encryption-enabled

AWS CloudTrail Überprüft, ob für die Verwendung der serverseitigen Verschlüsselung (SSE) AWS Key Management Service (AWS KMS) konfiguriert ist. Die Regel ist KONFORM, wenn die definiert KmsKeyId ist.

ID: CLOUD_TRAIL_ENCRYPTION_ENABLED

Ressourcentypen: AWS::CloudTrail::Trail

Auslösertyp: Regelmäßig

AWS-Region: Alle unterstützten AWS Regionen

Parameter:

Keine

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

cloud-trail-log-file-validierung aktiviert

Überprüft, ob eine signierte Digest-Datei mit Protokollen AWS CloudTrail erstellt wird. AWS empfiehlt, dass die Dateiüberprüfung auf allen Pfaden aktiviert sein muss. Die Regel ist NON_COMPLIANT, wenn die Validierung nicht aktiviert ist.

ID: CLOUD_TRAIL_LOG_FILE_VALIDATION_ENABLED

Ressourcentypen: AWS::CloudTrail::Trail

Auslösertyp: Regelmäßig

AWS-Region: Alle unterstützten AWS Regionen

Parameter:

Keine

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

cmk-backing-key-rotation-aktiviert

Überprüft, ob die automatische Schlüsselrotation für jeden Schlüssel aktiviert ist, und stimmt mit der Schlüssel-ID des vom Kunden erstellten AWS KMS-Schlüssels überein. Die Regel lautet NON_COMPLIANT, wenn die AWS Config-Recorder-Rolle für eine Ressource nicht über die kms: DescribeKey entsprechende Berechtigung verfügt.

> **Note**
>
> Die automatische Schlüsselrotation wird für asymmetrische KMS-Schlüssel, HMAC-KMS-Schlüssel, KMS-Schlüssel mit importiertem Schlüsselmaterial oder KMS-Schlüssel in benutzerdefinierten Schlüsselspeichern nicht unterstützt.

ID: CMK_BACKING_KEY_ROTATION_ENABLED

Ressourcentypen: AWS::KMS::Key

Auslösertyp: Regelmäßig

AWS-Region: Alle unterstützten AWS Regionen außer der Region Naher Osten (VAE)

Parameter:

Keine

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

codebuild-project-artifact-encryption

Prüft, ob in einem AWS CodeBuild Projekt die Verschlüsselung für alle Artefakte aktiviert ist. Die Regel ist NON_COMPLIANT, wenn „encryptionDisabled“ für alle primären oder sekundären (falls vorhanden) Artefaktkonfigurationen auf „True“ festgelegt ist.

ID: CODEBUILD_PROJECT_ARTIFACT_ENCRYPTION

Ressourcentypen: AWS::CodeBuild::Project

Auslösertyp: Konfigurationsänderungen

AWS-Region: Alle unterstützten AWS Regionen außer China (Peking), Asien-Pazifik (Thailand), Asien-Pazifik (Jakarta), Naher Osten (VAE), Asien-Pazifik (Hyderabad), Asien-Pazifik (Osaka), Asien-Pazifik (Malaysia), Asien-Pazifik (Melbourne), AWS GovCloud (USA-Ost), AWS GovCloud (US-West), Mexiko (Zentral), Israel (Tel Aviv), Kanada West (Calgary), Europa (Spanien), China (Ningxia), Europa (Region Zürich)

Parameter:

Keine

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

codebuild-project-environment-privileged-überprüfen

Prüft, ob in einer Projektumgebung der privilegierte Modus aktiviert ist AWS CodeBuild . Die Regel lautet NON_COMPLIANT für ein CodeBuild Projekt, wenn 'PrivilegedMode' auf 'true' gesetzt ist.

ID: CODEBUILD_PROJECT_ENVIRONMENT_PRIVILEGED_CHECK

Ressourcentypen: AWS::CodeBuild::Project

Auslösertyp: Konfigurationsänderungen

AWS-Region: Alle unterstützten AWS Regionen außer Asien-Pazifik (Thailand), Asien-Pazifik (Jakarta), Naher Osten (VAE), Asien-Pazifik (Hyderabad), Asien-Pazifik (Osaka), Asien-Pazifik (Malaysia), Asien-Pazifik (Melbourne), Mexiko (Zentral), Israel (Tel Aviv), Kanada West (Calgary), Europa (Spanien), Europa (Zürich)

Parameter:

exemptedProjects (optional), Typ: CSV

> Durch Kommas getrennte Liste von CodeBuild Projektnamen, die 'PrivilegedMode' mit dem Wert 'true' haben dürfen.

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

codebuild-project-envvar-awscred-überprüfen

Prüft, ob das Projekt die Umgebungsvariablen _ACCESS_KEY_ID und _SECRET_ACCESS_KEY enthält. AWS AWS Die Regel ist NON_COMPLIANT, wenn die Projekt-Umgebungsvariablen Klartext-Anmeldeinformationen enthalten.

Kennung: CODEBUILD_PROJECT_ENVVAR_ AWSCRED_CHECK

Ressourcentypen: AWS::CodeBuild::Project

Auslösertyp: Konfigurationsänderungen

AWS-Region: Alle unterstützten AWS Regionen außer Asien-Pazifik (Thailand), Asien-Pazifik (Jakarta), Asien-Pazifik (Malaysia), Mexiko (Zentral), Asien-Pazifik (Taipeh) und Kanada West (Calgary)

Parameter:

Keine

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

codebuild-project-logging-enabled

Prüft, ob in einer AWS CodeBuild Projektumgebung mindestens eine Protokolloption aktiviert ist. Die Regel ist NON_COMPLIANT, wenn der Status aller vorhandenen Protokollkonfigurationen auf DEAKTIVIERT gesetzt ist.

ID: CODEBUILD_PROJECT_LOGGING_ENABLED

Ressourcentypen: AWS::CodeBuild::Project

Auslösertyp: Konfigurationsänderungen

AWS-Region: Alle unterstützten AWS Regionen außer Asien-Pazifik (Thailand), Asien-Pazifik (Jakarta), Asien-Pazifik (Malaysia), Mexiko (Zentral) und Kanada West (Calgary)

Parameter:

s3 BucketNames (fakultativ), Typ: Zeichenfolge

Durch Kommata getrennte Liste der Namen von Amazon-S3-Buckets, an die Protokolle gesendet werden sollen, wenn S3-Protokolle konfiguriert sind.

cloudWatchGroupNamen (optional), Typ: Zeichenfolge

Durch Kommas getrennte Liste von CloudWatch Amazon-Protokollgruppennamen, an die Protokolle gesendet werden sollen, wenn CloudWatch Protokolle konfiguriert sind.

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

codebuild-project-s3-log-verschlüsselt

Prüft, ob bei einem mit Amazon S3 Logs konfigurierten AWS CodeBuild Projekt die Verschlüsselung für seine Protokolle aktiviert ist. Die Regel lautet NON_COMPLIANT, wenn 'EncryptionDisabled' in einem LogsConfig S3-Projekt auf 'true' gesetzt ist. CodeBuild

ID: CODEBUILD_PROJECT_S3_LOGS_ENCRYPTED

Ressourcentypen: AWS::CodeBuild::Project

Auslösertyp: Konfigurationsänderungen

AWS-Region: Alle unterstützten AWS Regionen außer Asien-Pazifik (Thailand), Asien-Pazifik (Jakarta), Asien-Pazifik (Malaysia), Mexiko (Zentral) und Kanada West (Calgary)

Parameter:

exemptedProjects (optional), Typ: CSV

Durch Kommas getrennte Liste von CodeBuild Projektnamen, die unverschlüsselte Protokolle ausgeben dürfen.

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

codebuild-project-source-repo-URL-Prüfung

Prüft, ob die URL des Bitbucket-Quell-Repositorys Anmeldeinformationen enthält oder nicht. Die Regel ist NON_COMPLIANT, wenn die URL Anmeldeinformationen enthält, und COMPLIANT, falls dies nicht der Fall ist.

ID: CODEBUILD_PROJECT_SOURCE_REPO_URL_CHECK

Ressourcentypen: AWS::CodeBuild::Project

Auslösertyp: Konfigurationsänderungen

AWS-Region: Alle unterstützten AWS Regionen außer Asien-Pazifik (Thailand), Asien-Pazifik (Jakarta), Asien-Pazifik (Malaysia), Mexiko (Zentral), Asien-Pazifik (Taipeh) und Kanada West (Calgary)

Parameter:

Keine

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

codebuild-report-group-encrypted-im Ruhezustand

Prüft, ob für eine AWS CodeBuild Berichtsgruppe die Einstellung Verschlüsselung im Ruhezustand aktiviert ist. Die Regel ist NON_COMPLIANT, wenn " " den Wert 'EncryptionDisabledtrue' hat.

Kennung: CODEBUILD_REPORT_GROUP_ENCRYPTED_AT_REST

Ressourcentypen: AWS::CodeBuild::ReportGroup

Auslösertyp: Konfigurationsänderungen

AWS-Region: Alle unterstützten AWS Regionen außer Asien-Pazifik (Thailand), Asien-Pazifik (Malaysia), Mexiko (Zentral) und Kanada West (Calgary)

Parameter:

Keine

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

codedeploy-auto-rollback-monitor-aktiviert

Überprüft, ob die Bereitstellungsgruppe mit automatischem Rollback und automatischer Überwachung der Bereitstellung mit angehängten Alarmen konfiguriert ist. Die Regel ist NON_COMPLIANT, wenn sie konfiguriert AlarmConfiguration wurde AutoRollbackConfiguration oder nicht aktiviert ist.

ID: CODEDEPLOY_AUTO_ROLLBACK_MONITOR_ENABLED

Ressourcentypen: AWS::CodeDeploy::DeploymentGroup

Auslösertyp: Konfigurationsänderungen

AWS-Region: Alle unterstützten AWS Regionen außer China (Peking), Asien-Pazifik (Thailand), Asien-Pazifik (Jakarta), Naher Osten (VAE), Asien-Pazifik (Hyderabad), Asien-Pazifik (Malaysia), Asien-Pazifik (Melbourne), AWS GovCloud (US-Ost), AWS GovCloud (US-West), Mexiko (Zentral), Israel (Tel Aviv), Kanada West (Calgary), Europa (Spanien), China (Ningxia), Europa (Zürich)

Parameter:

Keine

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

codedeploy-deployment-group-auto-Rollback-fähig

Überprüft, ob AWS CodeDeploy für Bereitstellungsgruppen die auto Rollback-Konfiguration aktiviert ist. Bei der Konfiguration lautet die Regel NON_COMPLIANT. autoRollbackConfiguration.enabled ist falsch oder existiert nicht.

Kennung: CODEDEPLOY_DEPLOYMENT_GROUP_AUTO_ROLLBACK_ENABLED

Ressourcentypen: AWS::CodeDeploy::DeploymentGroup

Auslösertyp: Konfigurationsänderungen

AWS-Region: Alle unterstützten AWS Regionen außer China (Peking), Asien-Pazifik (Thailand), Asien-Pazifik (Jakarta), Naher Osten (VAE), Asien-Pazifik (Hyderabad), Asien-Pazifik (Malaysia), Asien-Pazifik (Melbourne), AWS GovCloud (US-Ost), AWS GovCloud (US-West), Mexiko (Zentral), Israel (Tel Aviv), Kanada West (Calgary), Europa (Spanien), China (Ningxia), Europa (Zürich)

Parameter:

Keine

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

codedeploy-deployment-group-outdated-instanzen-aktualisieren

Überprüft, ob AWS CodeDeploy Bereitstellungsgruppen veraltete Instanzen automatisch aktualisieren. Bei der Konfiguration lautet die Regel NON_COMPLIANT. outdatedInstancesStrategy ist 'IGNORE'.

Kennung: CODEDEPLOY_DEPLOYMENT_GROUP_OUTDATED_INSTANCES_UPDATE

Ressourcentypen: AWS::CodeDeploy::DeploymentGroup

Auslösertyp: Konfigurationsänderungen

AWS-Region: Alle unterstützten AWS Regionen außer China (Peking), Asien-Pazifik (Thailand), Asien-Pazifik (Jakarta), Naher Osten (VAE), Asien-Pazifik (Hyderabad), Asien-Pazifik (Malaysia), Asien-Pazifik (Melbourne), AWS GovCloud (US-Ost), AWS GovCloud (US-West), Mexiko (Zentral), Israel (Tel Aviv), Kanada West (Calgary), Europa (Spanien), China (Ningxia), Europa (Zürich)

Parameter:

Keine

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

codedeploy-ec2- minimum-healthy-hosts-configured

Überprüft, ob die Bereitstellungsgruppe für EC2 /On-Premises Compute Platform so konfiguriert ist, dass ein Mindestprozentsatz für eine fehlerfreie Hostflotte oder eine Hostanzahl größer oder gleich dem Eingabeschwellenwert ist. Die Regel ist NON_COMPLIANT, wenn einer der Werte unter dem Schwellenwert liegt.

Kennung: CODEDEPLOY_ _MINIMUM_HEALTHY_HOSTS_CONFIGURED EC2

Ressourcentypen: AWS::CodeDeploy::DeploymentGroup

Auslösertyp: Konfigurationsänderungen

AWS-Region: Alle unterstützten AWS Regionen außer China (Peking), Asien-Pazifik (Thailand), Asien-Pazifik (Jakarta), Naher Osten (VAE), Asien-Pazifik (Hyderabad), Asien-Pazifik (Malaysia), Asien-Pazifik (Melbourne), AWS GovCloud (US-Ost), AWS GovCloud (US-West), Mexiko (Zentral), Israel (Tel Aviv), Kanada West (Calgary), Europa (Spanien), China (Ningxia), Europa (Zürich)

Parameter:

minimumHealthyHostsFleetPercent (Fakultativ), Typ: int, Standard: 66

Mindestprozentsatz fehlerfreier Hosts in der Flotte während der Bereitstellung. Der Wert ist standardmäßig auf 66 Prozent festgelegt.

minimumHealthyHostsHostCount (Fakultativ), Typ: int, Standard: 1

Mindestanzahl fehlerfreier Hosts in der Flotte während der Bereitstellung. Der Wert ist standardmäßig auf 1 festgelegt.

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

codedeploy-lambda-allatonce-traffic-shift-deaktiviert

Prüft, ob die Bereitstellungsgruppe für die Lambda-Computing-Plattform nicht die Standard-Bereitstellungskonfiguration verwendet. Die Regel lautet NON_COMPLIANT, wenn die Bereitstellungsgruppe die Bereitstellungskonfiguration 'verwendet. CodeDeployDefault LambdaAllAtOnce'.

ID: CODEDEPLOY_LAMBDA_ALLATONCE_TRAFFIC_SHIFT_DISABLED

Ressourcentypen: AWS::CodeDeploy::DeploymentGroup

Auslösertyp: Konfigurationsänderungen

AWS-Region: Alle unterstützten AWS Regionen außer China (Peking), Asien-Pazifik (Thailand), Asien-Pazifik (Jakarta), Naher Osten (VAE), Asien-Pazifik (Hyderabad), Asien-Pazifik (Malaysia), Asien-Pazifik (Melbourne), AWS GovCloud (US-Ost), AWS GovCloud (US-West), Mexiko (Zentral), Israel (Tel Aviv), Kanada West (Calgary), Europa (Spanien), China (Ningxia), Europa (Zürich)

Parameter:

Keine

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

codeguruprofiler-profiling-group-tagged

Überprüft, ob Amazon CodeGuru Profiler-Profiling-Gruppen Tags haben. Optional können Sie Tag-Schlüssel angeben. Die Regel lautet NON_COMPLIANT, wenn keine Tags vorhanden sind oder wenn die angegebenen Tag-Schlüssel nicht vorhanden sind. Die Regel sucht nicht nach Tags, die mit 'aws: 'beginnen.

Kennung: CODEGURUPROFILER_PROFILING_GROUP_TAGGED

Ressourcentypen: AWS::CodeGuruProfiler::ProfilingGroup

Auslösertyp: Konfigurationsänderungen

AWS-Region: Nur in der Region Europa (Stockholm), USA Ost (Ohio), Europa (Irland), Europa (Frankfurt), USA Ost (Nord-Virginia), Europa (London), Asien-Pazifik (Tokio), USA West (Oregon), Asien-Pazifik (Singapur), Asien-Pazifik (Sydney) verfügbar

Parameter:

requiredKeyTags (Fakultativ), Typ: CSV

> Durch Kommas getrennte Liste von Tag-Schlüsseln, die von der Regel überprüft werden sollen. Falls angegeben, lautet die Regel NON_COMPLIANT, wenn die ausgewertete Ressource diese Schlüssel nicht enthält. Bei Tag-Schlüsseln wird die Groß- und Kleinschreibung beachtet. Tag-Schlüssel, die mit „aws:“ beginnen, sind nicht erlaubt.

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

codegurureviewer-repository-association-tagged

Prüft, ob Amazon CodeGuru Reviewer-Repository-Verknüpfungen Tags haben. Optional können Sie Tag-Schlüssel angeben. Die Regel lautet NON_COMPLIANT, wenn keine Tags vorhanden sind oder wenn die angegebenen Tag-Schlüssel nicht vorhanden sind. Die Regel sucht nicht nach Tags, die mit 'aws: 'beginnen.

Kennung: CODEGURUREVIEWER_REPOSITORY_ASSOCIATION_TAGGED

Ressourcentypen: AWS::CodeGuruReviewer::RepositoryAssociation

Auslösertyp: Konfigurationsänderungen

AWS-Region: Nur in der Region Europa (Stockholm), USA Ost (Ohio), Europa (Irland), Europa (Frankfurt), USA Ost (Nord-Virginia), Europa (London), Asien-Pazifik (Tokio), USA West (Oregon), Asien-Pazifik (Singapur), Asien-Pazifik (Sydney) verfügbar

Parameter:

requiredKeyTags (Fakultativ), Typ: CSV

> Durch Kommas getrennte Liste von Tag-Schlüsseln, die von der Regel überprüft werden sollen. Falls angegeben, lautet die Regel NON_COMPLIANT, wenn die ausgewertete Ressource diese

Schlüssel nicht enthält. Bei Tag-Schlüsseln wird die Groß- und Kleinschreibung beachtet. Tag-Schlüssel, die mit „aws:“ beginnen, sind nicht erlaubt.

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

codepipeline-deployment-count-check

Überprüft, ob in der ersten Bereitstellungsphase AWS CodePipeline von mehr als eine Bereitstellung durchgeführt wird. Prüft optional, ob jede der nachfolgenden verbleibenden Stufen mehr als die angegebene Anzahl von Bereitstellungen (`deploymentLimit`) bereitstellt.

ID: CODEPIPELINE_DEPLOYMENT_COUNT_CHECK

Ressourcentypen: AWS::CodePipeline::Pipeline

Auslösertyp: Konfigurationsänderungen

AWS-Region: Alle unterstützten AWS Regionen außer Naher Osten (Bahrain), China (Peking), Asien-Pazifik (Thailand), Asien-Pazifik (Jakarta), Afrika (Kapstadt), Asien-Pazifik (Osaka), Asien-Pazifik (Malaysia), Asien-Pazifik (Melbourne), (USA-Ost), AWS GovCloud (US-West), Mexiko AWS GovCloud (Zentral), Asien-Pazifik (Taipeh), Kanada West (Calgary), Europa (Spanien), China (Ningxia), Europa (Zürich)) Region

Parameter:

deploymentLimit (optional), Typ: int

Die maximale Anzahl an Bereitstellungen, die jede Stufe durchführen kann.

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

codepipeline-region-fanout-check

Überprüft, ob jede Phase der AWS CodePipeline Bereitstellung mehr als das N-fache der Anzahl der Regionen umfasst, die sie in allen vorherigen kombinierten Phasen bereitgestellt AWS CodePipeline

hat, wobei N die Fanout-Nummer der Region ist. Die erste Bereitstellungsstufe kann höchstens für eine Region erfolgen und die zweite Bereitstellungsstufe kann für eine in `regionFanoutFactor` angegebene maximale Anzahl an Regionen erfolgen. Wenn Sie für `regionFanoutFactor` keinen Wert angeben, wird standardmäßig der Wert 3 verwendet. Beispiel: Wenn die erste Bereitstellungsstufe für eine Region und die zweite Bereitstellungsstufe für drei Regionen erfolgt, kann die dritte Bereitstellungsstufe für 12 Regionen, also der Summe der vorherigen Stufen multipliziert mit der Fanout-Anzahl der Region (3), erfolgen. Die Regel ist NON_COMPLIANT, wenn die Bereitstellung in der ersten Stufe für mehr als eine Region oder in der zweiten Stufe für mehr als drei Regionen oder in der dritten Stufe für mehr als 12 Regionen erfolgt.

ID: CODEPIPELINE_REGION_FANOUT_CHECK

Ressourcentypen: AWS::CodePipeline::Pipeline

Auslösertyp: Konfigurationsänderungen

AWS-Region: Nur verfügbar in Asien-Pazifik (Mumbai), Europa (Paris), USA Ost (Ohio), Europa (Irland), Naher Osten (VAE), Europa (Frankfurt), Südamerika (Sao Paulo), Asien-Pazifik (Hyderabad), USA Ost (Nord-Virginia), Asien-Pazifik (Seoul), Europa (London), Asien-Pazifik (Tokio), USA West (Oregon), USA West (Nordkalifornien), Asien-Pazifik (Singapur), Asien Pazifik (Sydney), Israel (Tel Aviv), Region Kanada (Zentral)

Parameter:

regionFanoutFactor (Fakultativ), Typ: int, Standard: 3

> Die Anzahl der Regionen, in denen die Bereitstellung in allen vorherigen Phasen durchgeführt AWS CodePipeline wurde, entspricht der akzeptablen Anzahl von Regionen, in denen eine Phase bereitgestellt werden kann.

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

cognito-identity-pool-unauth-Zugriffsprüfung

Überprüft, ob Amazon Cognito Identity Pool nicht authentifizierte Identitäten zulässt. Die Regel lautet NON_COMPLIANT, wenn der Identity Pool so konfiguriert ist, dass er nicht authentifizierte Identitäten zulässt.

Kennung: COGNITO_IDENTITY_POOL_UNAUTH_ACCESS_CHECK

Ressourcentypen: AWS::Cognito::IdentityPool

Auslösertyp: Konfigurationsänderungen

AWS-Region: Alle unterstützten AWS Regionen außer China (Peking), Asien-Pazifik (Thailand), Naher Osten (VAE), Asien-Pazifik (Hyderabad), Asien-Pazifik (Seoul), Asien-Pazifik (Malaysia), AWS GovCloud (US-Ost), Mexiko (Zentral), Israel (Tel Aviv), Kanada West (Calgary), Europa (Spanien), China (Ningxia), Europa (Zürich)

Parameter:

Keine

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

cognito-user-pool-advanced-sicherheitsaktiviert

Prüft, ob für einen Amazon Cognito Cognito-Benutzerpool erweiterte Sicherheitsfunktionen für die Standardauthentifizierung aktiviert sind. Die Regel lautet NON_COMPLIANT, wenn Advanced Security nicht aktiviert ist. Optional können Sie einen erweiterten Sicherheitsmodus angeben, den die Regel überprüfen soll.

Kennung: COGNITO_USER_POOL_ADVANCED_SECURITY_ENABLED

Ressourcentypen: AWS::Cognito::UserPool

Auslösertyp: Konfigurationsänderungen

AWS-Region: Alle unterstützten AWS Regionen außer China (Peking), Asien-Pazifik (Thailand), Asien-Pazifik (Jakarta), Afrika (Kapstadt), Naher Osten (VAE), Asien-Pazifik (Hongkong), Asien-Pazifik (Hyderabad), Asien-Pazifik (Malaysia), Asien-Pazifik (Melbourne), AWS GovCloud (USA-Ost), AWS GovCloud (US-West), Mexiko (Zentral), Kanada West (Calgary), Europa (Spanien), China (Ningxia), Europa Region (Zürich)

Parameter:

SecurityMode (Fakultativ), Typ: Zeichenfolge

Zeichenkettenwert des erweiterten Sicherheitsmodus, den die Regel überprüfen soll. Falls angegeben, lautet die Regel NON_COMPLIANT, wenn der erweiterte Sicherheitsmodus für Benutzerpools diesem Parameterwert nicht entspricht. Gültige Werte sind AUDIT und ENFORCED

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

cognito-user-pool-tagged

Prüft, ob Amazon Cognito Cognito-Benutzerpools Tags haben. Optional können Sie Tag-Schlüssel angeben. Die Regel lautet NON_COMPLIANT, wenn keine Tags vorhanden sind oder wenn die angegebenen Tag-Schlüssel nicht vorhanden sind. Die Regel sucht nicht nach Tags, die mit 'aws: 'beginnen.

Kennung: COGNITO_USER_POOL_TAGGED

Ressourcentypen: AWS::Cognito::UserPool

Auslösertyp: Konfigurationsänderungen

AWS-Region: Alle unterstützten AWS Regionen außer China (Peking), Asien-Pazifik (Thailand), Asien-Pazifik (Malaysia), AWS GovCloud (USA-Ost), AWS GovCloud (US-West), Mexiko (Zentral), China (Ningxia)

Parameter:

requiredKeyTags (Fakultativ), Typ: CSV

Durch Kommas getrennte Liste von Tag-Schlüsseln, die von der Regel überprüft werden sollen. Falls angegeben, lautet die Regel NON_COMPLIANT, wenn die ausgewertete Ressource diese Schlüssel nicht enthält. Bei Tag-Schlüsseln wird die Groß- und Kleinschreibung beachtet. Tag-Schlüssel, die mit „aws:“ beginnen, sind nicht erlaubt.

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

connect-instance-logging-enabled

Prüft, ob für Amazon Connect Connect-Instances Flow-Logs in einer CloudWatch Amazon-Protokollgruppe aktiviert sind. Die Regel lautet NON_COMPLIANT, wenn für eine Amazon Connect Connect-Instance keine Flow-Logs aktiviert sind.

Kennung: CONNECT_INSTANCE_LOGGING_ENABLED

Ressourcentypen: AWS::Connect::Instance

Auslösertyp: Konfigurationsänderungen

AWS-Region: Nur verfügbar in Afrika (Kapstadt), Europa (Frankfurt), USA Ost (Nord-Virginia), Asien-Pazifik (Seoul), Europa (London), Asien-Pazifik (Tokio), USA West (Oregon), Asien-Pazifik (Singapur), Asien-Pazifik (Sydney), Kanada (Zentral)

Parameter:

Keine

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

customerprofiles-object-type-allow-Profilerstellung

Prüft, ob die Objekttypen von Amazon Connect Customer Profiles die Erstellung eines neuen Standardprofils ermöglichen, falls noch keines vorhanden ist. Die Regel ist NON_COMPLIANT, wenn sie konfiguriert ist. AllowProfileCreation ist falsch.

Kennung: CUSTOMERPROFILES_OBJECT_TYPE_ALLOW_PROFILE_CREATION

Ressourcentypen: AWS::CustomerProfiles::ObjectType

Auslösertyp: Konfigurationsänderungen

AWS-Region: Nur verfügbar in Afrika (Kapstadt), Europa (Frankfurt), USA Ost (Nord-Virginia), Asien-Pazifik (Seoul), Europa (London), Asien-Pazifik (Tokio), USA West (Oregon), Asien-Pazifik (Singapur), Asien-Pazifik (Sydney), Kanada (Zentral)

Parameter:

Keine

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

customerprofiles-object-type-tagged

Überprüft, ob die Objekttypen von Amazon Connect Customer Profiles Tags haben. Optional können Sie Tag-Schlüssel angeben. Die Regel lautet NON_COMPLIANT, wenn keine Tags vorhanden sind oder wenn die angegebenen Tag-Schlüssel nicht vorhanden sind. Die Regel sucht nicht nach Tags, die mit 'aws: 'beginnen.

Kennung: CUSTOMERPROFILES_OBJECT_TYPE_TAGGED

Ressourcentypen: AWS::CustomerProfiles::ObjectType

Auslösertyp: Konfigurationsänderungen

AWS-Region: Nur verfügbar in Afrika (Kapstadt), Europa (Frankfurt), USA Ost (Nord-Virginia), Asien-Pazifik (Seoul), Europa (London), Asien-Pazifik (Tokio), USA West (Oregon), Asien-Pazifik (Singapur), Asien-Pazifik (Sydney), Kanada (Zentral)

Parameter:

requiredKeyTags (Fakultativ), Typ: CSV

> Durch Kommas getrennte Liste von Tag-Schlüsseln, die von der Regel überprüft werden sollen. Falls angegeben, lautet die Regel NON_COMPLIANT, wenn die ausgewertete Ressource diese Schlüssel nicht enthält. Bei Tag-Schlüsseln wird die Groß- und Kleinschreibung beachtet. Tag-Schlüssel, die mit „aws:“ beginnen, sind nicht erlaubt.

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

custom-eventbus-policy-attached

Überprüft, ob Amazon EventBridge Custom Event Buses eine ressourcenbasierte Richtlinie angehängt haben. Die Regel ist NON_COMPLIANT, wenn an eine benutzerdefinierte Event-Bus-Richtlinie keine ressourcenbasierte Richtlinie angefügt ist.

ID: CUSTOM_EVENTBUS_POLICY_ATTACHED

Ressourcentypen: AWS::Events::EventBus

Auslösertyp: Konfigurationsänderungen

AWS-Region: Alle unterstützten AWS Regionen außer Asien-Pazifik (Thailand), Asien-Pazifik (Malaysia), AWS GovCloud (USA-Ost), AWS GovCloud (US-West), Mexiko (Zentral), Kanada West (Calgary)

Parameter:

Keine

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

custom-schema-registry-policy-angehängt

Prüft, ob an benutzerdefinierte EventBridge Amazon-Schemaregister eine Ressourcenrichtlinie angehängt ist. Die Regel ist für benutzerdefinierte Schemaregistrierungen NON_COMPLIANT, wenn keine Ressourcenrichtlinie angefügt ist.

ID: CUSTOM_SCHEMA_REGISTRY_POLICY_ATTACHED

Ressourcentypen: AWS::EventSchemas::Registry

Auslösertyp: Regelmäßig

AWS-Region: Nur in Europa (Stockholm), Asien-Pazifik (Mumbai), Europa (Paris), USA Ost (Ohio), Europa (Irland), Europa (Frankfurt), Südamerika (Sao Paulo), Asien-Pazifik (Hongkong), USA Ost (Nord-Virginia), Asien-Pazifik (Seoul), Europa (London), Asien-Pazifik (Tokio), USA West (Oregon), USA West (Nordkalifornien), Asien-Pazifik (Singapur), Asien-Pazifik (Singapur), Asien-Pazifik (Asien-Pazifik), Asien-Pazifik (Tokio), USA West (Oregon), USA West (Nordkalifornien), Asien-Pazifik (Singapur), Asien-Pazifik (Singapur), Asien-Pazifik (Sydney), Region Kanada (Zentral)

Parameter:

Keine

AWS CloudFormation Schablone

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

cw-loggroup-retention-period-überprüfen

Prüft, ob eine CloudWatch LogGroup Amazon-Aufbewahrungsfrist auf mehr als 365 Tage oder eine bestimmte Aufbewahrungsfrist festgelegt ist. Die Regel lautet NON_COMPLIANT, wenn die Aufbewahrungsfrist weniger als`MinRetentionTime`, falls angegeben, oder andernfalls 365 Tage beträgt.

> **Note**
>
> Wenn die Aufbewahrungseinstellung für eine Protokollgruppe „Läuft nie ab“ lautet, wird die Regel als COMPLIANT markiert.

ID: CW_LOGGROUP_RETENTION_PERIOD_CHECK

Ressourcentypen: AWS::Logs::LogGroup

Auslösertyp: Regelmäßig

AWS-Region: Alle unterstützten AWS Regionen außer der Region Naher Osten (VAE)

Parameter:

LogGroupNames (Fakultativ), Typ: CSV

Eine durch Kommata getrennte Liste von Namen der Protokollgruppen, für die der Aufbewahrungszeitraum geprüft werden soll.

MinRetentionTime (Fakultativ), Typ: int

Geben Sie die Aufbewahrungszeit in Tagen an. Mögliche Werte sind: 1, 3, 5, 7, 14, 30, 60, 90, 120, 150, 180, 365, 400, 545, 731, 1827 und 3653. Der Standardaufbewahrungszeitraum beträgt 365 Tage.

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

datasync-task-data-verification-aktiviert

Prüft, ob für AWS DataSync Aufgaben die Datenüberprüfung aktiviert ist, um am Ende Ihrer Übertragung eine zusätzliche Überprüfung durchzuführen. Die Regel ist NON_COMPLIANT, wenn Configuration.OPTIONS angegeben ist. VerifyMode ist 'NONE'.

Kennung: DATASYNC_TASK_DATA_VERIFICATION_ENABLED

Ressourcentypen: AWS::DataSync::Task

Auslösertyp: Konfigurationsänderungen

AWS-Region: Alle unterstützten AWS Regionen außer China (Peking), Asien-Pazifik (Thailand), Asien-Pazifik (Malaysia), AWS GovCloud (USA-Ost), AWS GovCloud (US-West), Mexiko (Zentral), China (Ningxia)

Parameter:

Keine

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

datasync-task-logging-enabled

Prüft, ob für eine AWS DataSync Aufgabe die CloudWatch Amazon-Protokollierung aktiviert ist. Die Regel lautet NON_COMPLIANT, wenn für eine AWS DataSync Aufgabe die CloudWatch Amazon-Protokollierung nicht aktiviert ist oder wenn die Protokollierungsebene nicht der von Ihnen angegebenen Protokollierungsebene entspricht.

Kennung: DATASYNC_TASK_LOGGING_ENABLED

Ressourcentypen: AWS::DataSync::Task

Auslösertyp: Konfigurationsänderungen

AWS-Region: Alle unterstützten AWS Regionen außer Asien-Pazifik (Thailand), Asien-Pazifik (Malaysia), Mexiko (Zentral) und Kanada West (Calgary)

Parameter:

logLevel (optional), Typ: Zeichenfolge

> Zeichenkettenwert für die Protokollierungsebene. Zu den gültigen Werten gehören: 'BASIC' und 'TRANSFER'. Wenn nicht angegeben, ist der Standardwert „BASIC“.

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

datasync-task-tagged

Prüft, ob AWS DataSync Aufgaben Tags haben. Optional können Sie Tag-Schlüssel für die Regel angeben. Die Regel ist NON_COMPLIANT, wenn keine Tags vorhanden sind oder wenn die angegebenen Tag-Schlüssel nicht vorhanden sind. Die Regel sucht nicht nach Tags, die mit 'aws: 'beginnen.

Kennung: DATASYNC_TASK_TAGGED

Ressourcentypen: AWS::DataSync::Task

Auslösertyp: Konfigurationsänderungen

AWS-Region: Alle unterstützten AWS Regionen außer China (Peking), Asien-Pazifik (Thailand), Asien-Pazifik (Malaysia), AWS GovCloud (USA-Ost), AWS GovCloud (US-West), Mexiko (Zentral), China (Ningxia)

Parameter:

requiredKeyTags (Fakultativ), Typ: CSV

> Durch Kommas getrennte Liste von Tag-Schlüsseln, die von der Regel überprüft werden sollen. Falls angegeben, lautet die Regel NON_COMPLIANT, wenn die ausgewertete Ressource diese Schlüssel nicht enthält. Bei Tag-Schlüsseln wird die Groß- und Kleinschreibung beachtet. Tag-Schlüssel, die mit „aws:“ beginnen, sind nicht erlaubt.

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

dax-encryption-enabled

Prüft, ob Amazon DynamoDB Accelerator (DAX)-Cluster verschlüsselt sind. Die Regel ist NON_COMPLIANT, wenn ein DAX-Cluster nicht verschlüsselt ist.

ID: DAX_ENCRYPTION_ENABLED

Ressourcentypen: AWS::DAX::Cluster

Auslösertyp: Regelmäßig

AWS-Region: Nur verfügbar in Europa (Stockholm), China (Peking), Asien-Pazifik (Mumbai), Europa (Paris), USA Ost (Ohio), Europa (Irland), Europa (Frankfurt), Südamerika (Sao Paulo), USA Ost (Nord-Virginia), Europa (London), Asien-Pazifik (Tokio), USA West (Oregon), USA West (Nordkalifornien), Asien-Pazifik (Singapur), Asien-Pazifik (Sydney), Europa (Spanien), Region China (Ningxia)

Parameter:

Keine

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

dax-tls-endpoint-encryption

Prüft, ob Ihr Amazon DynamoDB Accelerator (DAX) -Cluster auf TLS ClusterEndpointEncryptionType eingestellt ist. Die Regel lautet NON_COMPLIANT, wenn ein DAX-Cluster nicht mit Transport Layer Security (TLS) verschlüsselt ist.

Kennung: DAX_TLS_ENDPOINT_ENCRYPTION

Ressourcentypen: AWS::DAX::Cluster

Auslösertyp: Regelmäßig

AWS-Region: Nur verfügbar in den Regionen Asien-Pazifik (Mumbai), Europa (Paris), USA Ost (Ohio), Europa (Irland), Europa (Frankfurt), Südamerika (São Paulo), USA Ost (Nord-Virginia), Europa (London), Asien-Pazifik (Tokio), USA West (Oregon); USA West (Nordkalifornien); Asien-Pazifik (Singapur) und Asien-Pazifik (Sydney)

Parameter:

Keine

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

db-instance-backup-enabled

Prüft, ob bei RDS-DB-Instances Sicherungen aktiviert sind. Optional wird von der Regel auch der Aufbewahrungszeitraum für Backups und das Sicherungsfenster überprüft.

ID: DB_INSTANCE_BACKUP_ENABLED

Ressourcentypen: AWS::RDS::DBInstance

Auslösertyp: Konfigurationsänderungen

AWS-Region: Alle unterstützten AWS Regionen

Parameter:

backupRetentionPeriod (Fakultativ), Typ: int

Der Aufbewahrungszeitraum für Backups.

backupRetentionMinimum (Fakultativ), Typ: int

Der minimale Aufbewahrungszeitraum für Backups.

preferredBackupWindow (Fakultativ), Typ: Zeichenfolge

Zeitraum, in dem Sicherungen erstellt werden.

checkReadReplicas (Fakultativ), Typ: Boolesch

Prüft, ob bei RDS-DB-Instances Sicherungen für Read Replicas aktiviert sind.

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

desired-instance-tenancy

Überprüft EC2 Instances auf einen „Tenancy“ -Wert. Überprüft auch, ob AMI so spezifiziert IDs sind, dass sie von diesen aus gestartet werden, AMIs oder ob Hosts auf diesen Dedicated Hosts gestartet IDs werden. Die Regel ist COMPLIANT, wenn die Instance einem Host und einem AMI, falls angegeben, in einer Liste entspricht.

ID: DESIRED_INSTANCE_TENANCY

Ressourcentypen: AWS::EC2::Instance

Auslösertyp: Konfigurationsänderungen

AWS-Region: Alle unterstützten AWS Regionen

Parameter:

tenancy, Typ: Zeichenfolge

Die gewünschte Tenancy der Instances. Gültige Werte sind DEDIZIERT, HOST und STANDARD.

imageId (optional), Typ: CSV

Die Regel bewertet Instanzen, die nur AMIs mit den angegebenen IDs Instances gestartet wurden. Trennen Sie mehrere AMI IDs durch Kommas.

hostId (optional), Typ: CSV

Der IDs der EC2 Dedicated Hosts, auf denen die Instances gestartet werden sollen. Trennen Sie mehrere Hosts IDs durch Kommas.

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

desired-instance-type

Prüft, ob Ihre EC2 Instances einem bestimmten Instance-Typ angehören. Die Regel lautet NON_COMPLIANT, wenn eine EC2 Instanz nicht in der Parameterliste angegeben ist. Eine Liste der unterstützten EC2 Instanztypen finden Sie unter Instanztypen im EC2 Benutzerhandbuch für Linux-Instances.

ID: DESIRED_INSTANCE_TYPE

Ressourcentypen: AWS::EC2::Instance

Auslösertyp: Konfigurationsänderungen

AWS-Region: Alle unterstützten AWS Regionen

Parameter:

instanceType, Typ: CSV

Durch Kommas getrennte Liste von EC2 Instance-Typen (z. B. „t2.small, m4.large, i2.xlarge“).

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

dms-auto-minor-version-Upgrade-Check

Prüft, ob für eine Replikationsinstanz des AWS Database Migration Service (AWS DMS) automatische Upgrades für Nebenversionen aktiviert sind. Die Regel lautet NON_COMPLIANT, wenn eine AWS DMS-Replikationsinstanz nicht mit automatischen Upgrades für Nebenversionen konfiguriert ist.

ID: DMS_AUTO_MINOR_VERSION_UPGRADE_CHECK

Ressourcentypen: AWS::DMS::ReplicationInstance

Auslösertyp: Konfigurationsänderungen

AWS-Region: Alle unterstützten AWS Regionen außer Asien-Pazifik (Thailand), Asien-Pazifik (Jakarta), Naher Osten (VAE), Asien-Pazifik (Hyderabad), Asien-Pazifik (Malaysia), Asien-Pazifik (Melbourne), AWS GovCloud (USA-Ost), AWS GovCloud (US-West), Mexiko (Zentral), Israel (Tel Aviv), Kanada West (Calgary), Europa (Spanien), Europa (Zürich)

Parameter:

Keine

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

dms-endpoint-ssl-configured

Überprüft, ob die Endpunkte des AWS Database Migration Service (AWS DMS) mit einer SSL-Verbindung konfiguriert sind. Die Regel lautet NON_COMPLIANT, wenn für AWS DMS keine SSL-Verbindung konfiguriert ist.

Kontext: SSL/TLS-Verbindungen bieten eine Sicherheitsebene, indem sie Daten verschlüsseln, die zwischen Ihrem Client und einer DB-Instance übertragen werden. Die Verwendung eines Serverzertifikats bietet eine zusätzliche Sicherheitsebene, indem bestätigt wird, dass die Verbindung zu einer Amazon RDS-DB-Instance hergestellt wird. Dazu wird das Serverzertifikat überprüft, das automatisch auf allen von Ihnen bereitgestellten DB-Instances installiert wird. Indem Sie die SSL-Verbindung aktivieren AWS DMS, schützen Sie die Vertraulichkeit der Daten während der Migration.

Informationen zur Konfiguration der SSL-Verbindung finden Sie unter Verwenden AWS DMS, SSL/TLS um eine Verbindung zu einer DB-Instance oder einem Cluster zu verschlüsseln im Amazon Relational Database Service Service-Benutzerhandbuch.

ID: DMS_ENDPOINT_SSL_CONFIGURED

Ressourcentypen: AWS::DMS::Endpoint

Auslösertyp: Konfigurationsänderungen

AWS-Region: Alle unterstützten AWS Regionen außer Asien-Pazifik (Thailand), Asien-Pazifik (Jakarta), Naher Osten (VAE), Asien-Pazifik (Hyderabad), Asien-Pazifik (Malaysia), Asien-Pazifik (Melbourne), AWS GovCloud (USA-Ost), AWS GovCloud (US-West), Mexiko (Zentral), Israel (Tel Aviv), Kanada West (Calgary), Europa (Spanien), Europa (Zürich)

Parameter:

Keine

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

dms-endpoint-tagged

Prüft, ob AWS DMS-Endpunkte Tags haben. Optional können Sie Tag-Schlüssel angeben. Die Regel lautet NON_COMPLIANT, wenn keine Tags vorhanden sind oder wenn die angegebenen Tag-Schlüssel nicht vorhanden sind. Die Regel sucht nicht nach Tags, die mit 'aws: 'beginnen.

Kennung: DMS_ENDPOINT_TAGGED

Ressourcentypen: AWS::DMS::Endpoint

Auslösertyp: Konfigurationsänderungen

AWS-Region: Alle unterstützten AWS Regionen außer China (Peking), Asien-Pazifik (Thailand), Asien-Pazifik (Jakarta), Naher Osten (VAE), Asien-Pazifik (Hyderabad), Asien-Pazifik (Malaysia), Asien-Pazifik (Melbourne), AWS GovCloud (US-Ost), AWS GovCloud (US-West), Mexiko (Zentral), Israel (Tel Aviv), Kanada West (Calgary), Europa (Spanien), China (Ningxia), Europa (Zürich)

Parameter:

requiredKeyTags (Fakultativ), Typ: CSV

Durch Kommas getrennte Liste von Tag-Schlüsseln, die von der Regel überprüft werden sollen. Falls angegeben, lautet die Regel NON_COMPLIANT, wenn die ausgewertete Ressource diese Schlüssel nicht enthält. Bei Tag-Schlüsseln wird die Groß- und Kleinschreibung beachtet. Tag-Schlüssel, die mit „aws:“ beginnen, sind nicht erlaubt.

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

dms-mongo-db-authentication-aktiviert

Überprüft, ob die Endpunkte des AWS Database Migration Service (AWS DMS) für MongoDb Datenspeicher für kennwortbasierte Authentifizierung und Zugriffskontrolle aktiviert sind. Die Regel lautet NON_COMPLIANT, wenn die kennwortbasierte Authentifizierung und Zugriffskontrolle nicht aktiviert ist.

Kennung: DMS_MONGO_DB_AUTHENTICATION_ENABLED

Ressourcentypen: AWS::DMS::Endpoint

Auslösertyp: Konfigurationsänderungen

AWS-Region: Alle unterstützten AWS Regionen außer China (Peking), Asien-Pazifik (Thailand), Asien-Pazifik (Jakarta), Naher Osten (VAE), Asien-Pazifik (Hyderabad), Asien-Pazifik (Malaysia), Asien-Pazifik (Melbourne), Mexiko (Zentral), Israel (Tel Aviv), Kanada West (Calgary), Europa (Spanien), China (Ningxia), Europa (Zürich)

Parameter:

Keine

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

dms-neptune-iam-authorization-aktiviert

Überprüft, ob ein AWS DMS-Endpunkt (AWS Database Migration Service) für Amazon Neptune Neptune-Datenbanken mit IAM-Autorisierung konfiguriert ist. Die Regel lautet NON_COMPLIANT, wenn ein AWS DMS-Endpunkt, an dem Neptune das Ziel ist, auf False gesetzt wurde. IamAuthEnabled

Kennung: DMS_NEPTUNE_IAM_AUTHORIZATION_ENABLED

Ressourcentypen: AWS::DMS::Endpoint

Auslösertyp: Konfigurationsänderungen

AWS-Region: Alle unterstützten AWS Regionen außer China (Peking), Asien-Pazifik (Thailand), Asien-Pazifik (Jakarta), Afrika (Kapstadt), Naher Osten (VAE), Asien-Pazifik (Hyderabad), Asien-Pazifik (Osaka), Asien-Pazifik (Malaysia), Asien-Pazifik (Melbourne), Europa (Mailand), Mexiko (Zentral), Israel (Tel Aviv), Kanada West (Calgary), Europa (Spanien), China (Ningxia), Europa Region (Zürich)

Parameter:

Keine

AWS CloudFormation Schablone

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

dms-redis-tls-enabled

Überprüft, ob die AWS DMS-Endpunkte (AWS Database Migration Service) für Redis-Datenspeicher für die TLS/SSL Verschlüsselung von Daten aktiviert sind, die mit anderen Endpunkten übertragen werden. Die Regel lautet NON_COMPLIANT, wenn die Verschlüsselung nicht aktiviert ist. TLS/SSL

Kennung: DMS_REDIS_TLS_ENABLED

Ressourcentypen: AWS::DMS::Endpoint

Auslösertyp: Konfigurationsänderungen

AWS-Region: Alle unterstützten AWS Regionen außer China (Peking), Asien-Pazifik (Thailand), Asien-Pazifik (Jakarta), Naher Osten (VAE), Asien-Pazifik (Hyderabad), Asien-Pazifik (Malaysia),

Asien-Pazifik (Melbourne), Mexiko (Zentral), Israel (Tel Aviv), Kanada West (Calgary), Europa (Spanien), China (Ningxia), Europa (Zürich)

Parameter:

Keine

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

dms-replication-not-public

Überprüft, ob Replikationsinstanzen des AWS Database Migration Service (AWS DMS) öffentlich sind. Die Regel lautet NON_COMPLIANT, wenn PubliclyAccessible das Feld auf true gesetzt ist.

ID: DMS_REPLICATION_NOT_PUBLIC

Ressourcentypen: AWS::DMS::ReplicationInstance

Auslösertyp: Regelmäßig

AWS-Region: Alle unterstützten AWS Regionen außer der Region Asien-Pazifik (Taipeh)

Parameter:

Keine

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

dms-replication-task-sourcedb-Protokollierung

Prüft, ob die Protokollierung mit einem gültigen Schweregrad für AWS DMS-Replikationsaufgaben einer Quelldatenbank aktiviert ist. Die Regel ist NON_COMPLIANT, wenn die Protokollierung nicht aktiviert ist oder Protokolle für DMS-Replikationsaufgaben einer Quelldatenbank einen ungültigen Schweregrad haben.

ID: DMS_REPLICATION_TASK_SOURCEDB_LOGGING

Ressourcentypen: AWS::DMS::ReplicationTask

Auslösertyp: Konfigurationsänderungen

AWS-Region: Alle unterstützten AWS Regionen außer Asien-Pazifik (Thailand), Asien-Pazifik (Jakarta), Naher Osten (VAE), Asien-Pazifik (Hyderabad), Asien-Pazifik (Osaka), Asien-Pazifik (Malaysia), Asien-Pazifik (Melbourne), AWS GovCloud (USA-Ost), AWS GovCloud (US-West), Mexiko (Zentral), Israel (Tel Aviv), Kanada West (Calgary), Europa (Spanien), Europa (Zürich)

Parameter:

Keine

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

dms-replication-task-tagged

Prüft, ob AWS DMS-Replikationsaufgaben Tags haben. Optional können Sie Tag-Schlüssel angeben. Die Regel lautet NON_COMPLIANT, wenn keine Tags vorhanden sind oder wenn die angegebenen Tag-Schlüssel nicht vorhanden sind. Die Regel sucht nicht nach Tags, die mit 'aws: 'beginnen.

Kennung: DMS_REPLICATION_TASK_TAGGED

Ressourcentypen: AWS::DMS::ReplicationTask

Auslösertyp: Konfigurationsänderungen

AWS-Region: Alle unterstützten AWS Regionen außer China (Peking), Asien-Pazifik (Thailand), Asien-Pazifik (Jakarta), Naher Osten (VAE), Asien-Pazifik (Hyderabad), Asien-Pazifik (Malaysia), Asien-Pazifik (Melbourne), AWS GovCloud (US-Ost), AWS GovCloud (US-West), Mexiko (Zentral), Israel (Tel Aviv), Kanada West (Calgary), Europa (Spanien), China (Ningxia), Europa (Zürich)

Parameter:

requiredKeyTags (Fakultativ), Typ: CSV

> Durch Kommas getrennte Liste von Tag-Schlüsseln, die von der Regel überprüft werden sollen. Falls angegeben, lautet die Regel NON_COMPLIANT, wenn die ausgewertete Ressource diese

Schlüssel nicht enthält. Bei Tag-Schlüsseln wird die Groß- und Kleinschreibung beachtet. Tag-Schlüssel, die mit „aws:“ beginnen, sind nicht erlaubt.

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

dms-replication-task-targetdb-Protokollierung

Prüft, ob die Protokollierung mit einem gültigen Schweregrad für AWS DMS-Replikationsaufgabenereignisse einer Zieldatenbank aktiviert ist. Die Regel ist NON_COMPLIANT, wenn die Protokollierung nicht aktiviert ist oder die Protokollierung von Replikationsaufgaben einer Zieldatenbank einen ungültigen Schweregrad hat.

ID: DMS_REPLICATION_TASK_TARGETDB_LOGGING

Ressourcentypen: AWS::DMS::ReplicationTask

Auslösertyp: Konfigurationsänderungen

AWS-Region: Alle unterstützten AWS Regionen außer Asien-Pazifik (Thailand), Asien-Pazifik (Jakarta), Naher Osten (VAE), Asien-Pazifik (Hyderabad), Asien-Pazifik (Osaka), Asien-Pazifik (Malaysia), Asien-Pazifik (Melbourne), AWS GovCloud (USA-Ost), AWS GovCloud (US-West), Mexiko (Zentral), Israel (Tel Aviv), Kanada West (Calgary), Europa (Spanien), Europa (Zürich)

Parameter:

Keine

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

docdb-cluster-audit-logging-aktiviert

Prüft, ob in einem Amazon DocumentDB DocumentDB-Instance-Cluster (mit MongoDB-Kompatibilität) der Protokollexport für CloudWatch Audit-Logs aktiviert ist. Die Regel lautet NON_COMPLIANT, wenn in einem Amazon DocumentDB DocumentDB-Instance-Cluster kein CloudWatch Protokollexport für Audit-Logs aktiviert ist.

ID: DOCDB_CLUSTER_AUDIT_LOGGING_ENABLED

Ressourcentypen: AWS::RDS::DBCluster

Auslösertyp: Konfigurationsänderungen

AWS-Region: Alle unterstützten AWS Regionen außer Europa (Stockholm), Naher Osten (Bahrain), China (Peking), Asien-Pazifik (Thailand), Asien-Pazifik (Jakarta), Afrika (Kapstadt), Asien-Pazifik (Osaka), Asien-Pazifik (Malaysia), Asien-Pazifik (Melbourne), AWS GovCloud (USA-Ost), AWS GovCloud (US-West), Mexiko (Zentral), USA West (Nordkalifornien), Israel (Tel Aviv), Kanada West (Calgary), Europa (Spanien), Region Europa (Zürich)

Parameter:

Keine

AWS CloudFormation Schablone

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

docdb-cluster-backup-retention-überprüfen

Prüft, ob ein Aufbewahrungszeitraum für Cluster von Amazon DocumentDB auf eine bestimmte Anzahl von Tagen festgelegt ist. Die Regel ist NON_COMPLIANT, wenn der Aufbewahrungszeitraum kürzer ist als durch den Parameter angegeben.

ID: DOCDB_CLUSTER_BACKUP_RETENTION_CHECK

Ressourcentypen: AWS::RDS::DBCluster

Auslösertyp: Konfigurationsänderungen

AWS-Region: Alle unterstützten AWS Regionen außer Europa (Stockholm), Naher Osten (Bahrain), China (Peking), Asien-Pazifik (Thailand), Asien-Pazifik (Jakarta), Afrika (Kapstadt), Asien-Pazifik (Osaka), Asien-Pazifik (Malaysia), Asien-Pazifik (Melbourne), AWS GovCloud (USA-Ost), AWS GovCloud (US-West), Mexiko (Zentral), USA West (Nordkalifornien), Israel (Tel Aviv), Kanada West (Calgary), Europa (Spanien), Region Europa (Zürich)

Parameter:

minimumBackupRetentionZeitraum (optional), Typ: int

Mindestaufbewahrungszeitraum für Backups. Gültige Werte: 1 bis 35; Standardwert: 7. Diese Regel ist NON_COMPLIANT, wenn der Wert größer als " backupRetentionPeriod ist.

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

docdb-cluster-deletion-protection-aktiviert

Prüft, ob für einen Amazon DocumentDB-Cluster (mit MongoDB-Kompatibilität) der Löschschutz aktiviert ist. Die Regel ist NON_COMPLIANT, wenn in einem Amazon DocumentDB-Cluster das Feld DeletionProtection auf „False“ festgelegt ist.

ID: DOCDB_CLUSTER_DELETION_PROTECTION_ENABLED

Ressourcentypen: AWS::RDS::DBCluster

Auslösertyp: Konfigurationsänderungen

AWS-Region: Alle unterstützten AWS Regionen außer Europa (Stockholm), Naher Osten (Bahrain), China (Peking), Asien-Pazifik (Thailand), Asien-Pazifik (Jakarta), Afrika (Kapstadt), Asien-Pazifik (Osaka), Asien-Pazifik (Malaysia), Asien-Pazifik (Melbourne), AWS GovCloud (USA-Ost), AWS GovCloud (US-West), Mexiko (Zentral), USA West (Nordkalifornien), Israel (Tel Aviv), Kanada West (Calgary), Europa (Spanien), Region Europa (Zürich)

Parameter:

Keine

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

docdb-cluster-encrypted

Prüft, ob die Speicherverschlüsselung für Ihre Amazon DocumentDB-Cluster (mit MongoDB-Kompatibilität) aktiviert ist. Die Regel ist NON_COMPLIANT, wenn die Speicherverschlüsselung nicht aktiviert ist.

ID: DOCDB_CLUSTER_ENCRYPTED

Ressourcentypen: AWS::RDS::DBCluster

Auslösertyp: Konfigurationsänderungen

AWS-Region: Alle unterstützten AWS Regionen außer Europa (Stockholm), Naher Osten (Bahrain), China (Peking), Asien-Pazifik (Thailand), Asien-Pazifik (Jakarta), Afrika (Kapstadt), Asien-Pazifik (Osaka), Asien-Pazifik (Malaysia), Asien-Pazifik (Melbourne), AWS GovCloud (USA-Ost), AWS GovCloud (US-West), Mexiko (Zentral), USA West (Nordkalifornien), Israel (Tel Aviv), Kanada West (Calgary), Europa (Spanien), Region Europa (Zürich)

Parameter:

kmsKeyArns (Fakultativ), Typ: CSV

> Eine durch Kommas getrennte Liste von KMS-Schlüsseln ARNs , die mit der KmsKey ID des verschlüsselten Clusters verglichen werden sollen.

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

docdb-cluster-encrypted-in-Transit

Prüft, ob Verbindungen zu Amazon DocumentDB-Clustern so konfiguriert sind, dass sie Verschlüsselung bei der Übertragung verwenden. Die Regel lautet NON_COMPLIANT, wenn die Parametergruppe nicht „synchron“ ist oder der TLS-Parameter entweder auf „deaktiviert“ oder auf einen Wert in gesetzt ist. `excludeTlsParameters`

Kennung: DOCDB_CLUSTER_ENCRYPTED_IN_TRANSIT

Ressourcentypen: AWS::RDS::DBCluster

Auslösertyp: Regelmäßig

AWS-Region: Alle unterstützten AWS Regionen außer Europa (Stockholm), Naher Osten (Bahrain), Asien-Pazifik (Thailand), Asien-Pazifik (Jakarta), Afrika (Kapstadt), Asien-Pazifik (Osaka), Asien-Pazifik (Malaysia), Asien-Pazifik (Melbourne), Mexiko (Zentral), USA West (Nordkalifornien), Israel (Tel Aviv), Kanada West (Calgary), Europa (Spanien), Europa (Zürich)

Parameter:

excludeTlsParameters (Fakultativ), Typ: CSV

> Durch Kommas getrennte Liste von TLS-Clusterparametern, die von der Regel NICHT geprüft werden sollen. Standardwert: 'deaktiviert'.

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

docdb-cluster-snapshot-public-verboten

Prüft, ob manuelle Cluster-Snapshots von Amazon DocumentDB öffentlich sind. Die Regel ist NON_COMPLIANT, wenn manuelle Cluster-Snapshots von Amazon DocumentDB öffentlich sind.

ID: DOCDB_CLUSTER_SNAPSHOT_PUBLIC_PROHIBITED

Ressourcentypen: AWS::RDS::DBClusterSnapshot

Auslösertyp: Konfigurationsänderungen

AWS-Region: Nur verfügbar in Asien-Pazifik (Mumbai), Europa (Paris), USA Ost (Ohio), Europa (Irland), Naher Osten (VAE), Europa (Frankfurt), Südamerika (Sao Paulo), Asien-Pazifik (Hongkong), Asien-Pazifik (Hyderabad), USA Ost (Nord-Virginia), Asien-Pazifik (Seoul), Europa (London), Europa (Mailand), Asien-Pazifik (Tokio), USA West (Oregon), Asien-Pazifik (Oregon), Asien-Pazifik (Singapur), Asien-Pazifik (Sydney), Region Kanada (Zentral)

Parameter:

Keine

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

dynamodb-autoscaling-enabled

Prüft, ob Amazon DynamoDB-Tabellen oder globale sekundäre Indizes Lese-/Schreibkapazität im On-Demand-Modus oder im Bereitstellungsmodus mit aktiviertem Auto Scaling verarbeiten können. Die Regel ist NON_COMPLIANT, wenn einer der Modi ohne aktiviertes Auto Scaling verwendet wird.

ID: DYNAMODB_AUTOSCALING_ENABLED

Ressourcentypen: AWS::DynamoDB::Table

Auslösertyp: Regelmäßig

AWS-Region: Alle unterstützten AWS Regionen

Parameter:

minProvisionedReadKapazität (optional), Typ: int

Die Mindestanzahl der Einheiten, die für die Lesekapazität in der Auto-Scaling-Gruppe bereitgestellt werden sollte.

maxProvisionedReadKapazität (optional), Typ: int

Die maximale Anzahl der Einheiten, die für die Lesekapazität in der Auto-Scaling-Gruppe bereitgestellt werden sollte.

targetReadUtilization (Fakultativ), Typ: double

Der Zielauslastungsprozentsatz für die Lesekapazität. Die Zielauslastung wird als das Verhältnis der verbrauchten Kapazitätseinheiten zu den bereitgestellten Kapazitätseinheiten ausgedrückt.

minProvisionedWriteKapazität (optional), Typ: int

Die Mindestanzahl der Einheiten, die für die Schreibkapazität in der Auto-Scaling-Gruppe bereitgestellt werden sollte.

maxProvisionedWriteKapazität (optional), Typ: int

Die maximale Anzahl der Einheiten, die für die Schreibkapazität in der Auto-Scaling-Gruppe bereitgestellt werden sollte.

targetWriteUtilization (Fakultativ), Typ: double

Der Zielauslastungsprozentsatz für die Schreibkapazität. Die Zielauslastung wird als das Verhältnis der verbrauchten Kapazitätseinheiten zu den bereitgestellten Kapazitätseinheiten ausgedrückt.

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

dynamodb-in-backup-plan

Prüft, ob die Amazon DynamoDB-Tabelle in AWS Backup-Plänen vorhanden ist. Die Regel lautet NON_COMPLIANT, wenn Amazon DynamoDB-Tabellen in keinem Backup-Plan enthalten sind. AWS

ID: DYNAMODB_IN_BACKUP_PLAN

Ressourcentypen: AWS::DynamoDB::Table

Auslösertyp: Regelmäßig

AWS-Region: Alle unterstützten AWS Regionen außer der Region Asien-Pazifik (Taipeh)

Parameter:

Keine

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

dynamodb-last-backup-recovery-Punkt-erstellt

Prüft, ob innerhalb des angegebenen Zeitraums ein Wiederherstellungspunkt für Amazon DynamoDB-Tabellen erstellt wurde. Die Regel ist NON_COMPLIANT, wenn innerhalb des angegebenen Zeitraums kein entsprechender Wiederherstellungspunkt für die DynamoDB-Tabelle erstellt wurde.

ID: DYNAMODB_LAST_BACKUP_RECOVERY_POINT_CREATED

Ressourcentypen: AWS::DynamoDB::Table

Auslösertyp: Regelmäßig

AWS-Region: Alle unterstützten AWS Regionen außer China (Peking), Asien-Pazifik (Thailand), Asien-Pazifik (Malaysia), Mexiko (Zentral), Israel (Tel Aviv), Kanada West (Calgary), China (Ningxia)

Parameter:

resourceTags (optional), Typ: Zeichenfolge

Tags der DynamoDB-Tabellen, die von der Regel geprüft werden sollen, im JSON-Format `{"tagkey" : "tagValue"}`.

resourceId (optional), Typ: Zeichenfolge

Name der DynamoDB-Tabelle, die von der Regel geprüft werden soll.

recoveryPointAgeWert (optional), Typ: int, Standard: 1

Numerischer Wert für das zulässige Höchstalter. Nicht mehr als 744 für Stunden oder 31 für Tage.

recoveryPointAgeEinheit (optional), Typ: Zeichenfolge, Standard: days

Zeiteinheit für das zulässige Höchstalter. Zulässige Werte: „Stunden“, „Tage“.

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

dynamodb-meets-restore-time-ziel

Überprüft, ob die Wiederherstellungszeit von Amazon-DynamoDB-Tabellen der angegebenen Dauer entspricht. Die Regel lautet NON_COMPLIANT, wenn LatestRestoreExecutionTimeMinutes der Wert einer DynamoDB-Tabelle länger als Minuten ist. maxRestoreTime

Kennung: DYNAMODB_MEETS_RESTORE_TIME_TARGET

Ressourcentypen: AWS::DynamoDB::Table

Auslösertyp: Regelmäßig

AWS-Region: Alle unterstützten AWS Regionen außer China (Peking), Asien-Pazifik (Thailand), Asien-Pazifik (Malaysia), AWS GovCloud (USA-Ost), AWS GovCloud (US-West), Mexiko (Zentral), Israel (Tel Aviv), Kanada West (Calgary), China (Ningxia)

Parameter:

maxRestoreTime, Typ: int

Numerischer Wert für die maximal zulässige Wiederherstellungslaufzeit.

resourceTags (optional), Typ: Zeichenfolge

Tags der DynamoDB-Tabellen, die von der Regel geprüft werden sollen, im JSON-Format.

resourceId (optional), Typ: Zeichenfolge

Name der DynamoDB-Tabelle, die von der Regel geprüft werden soll.

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

dynamodb-pitr-enabled

Prüft, ob point-in-time Recovery (PITR) für Amazon DynamoDB-Tabellen aktiviert ist. Die Regel ist NON_COMPLIANT, wenn PITR für DynamoDB-Tabellen nicht aktiviert ist.

Kennung: DYNAMODB_PITR_ENABLED

Ressourcentypen: AWS::DynamoDB::Table

Auslösertyp: Konfigurationsänderungen

AWS-Region: Alle unterstützten AWS Regionen

Parameter:

Keine

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

dynamodb-resources-protected-by-Backup-Plan

Prüft, ob Amazon-DynamoDB-Tabellen durch einen Backup-Plan geschützt sind. Die Regel ist NON_COMPLIANT, wenn die DynamoDB-Tabelle nicht durch einen Backup-Plan gedeckt ist.

ID: DYNAMODB_RESOURCES_PROTECTED_BY_BACKUP_PLAN

Ressourcentypen: AWS::DynamoDB::Table

Auslösertyp: Regelmäßig

AWS-Region: Alle unterstützten AWS Regionen außer China (Peking), Asien-Pazifik (Thailand), Asien-Pazifik (Malaysia), Mexiko (Zentral), Israel (Tel Aviv), Kanada West (Calgary), China (Ningxia)

Parameter:

resourceTags (optional), Typ: Zeichenfolge

Tags für DynamoDB-Tabellen, die von der Regel geprüft werden sollen, im JSON-Format `{"tagkey" : "tagValue"}`.

resourceId (optional), Typ: Zeichenfolge

Name der DynamoDB-Tabelle, die von der Regel geprüft werden soll.

crossRegionList (Fakultativ), Typ: Zeichenfolge

Durch Kommata getrennte Liste der Zielregionen, für die die regionsübergreifende Backup-Kopie aufbewahrt werden soll.

crossAccountList (Fakultativ), Typ: Zeichenfolge

Durch Kommata getrennte Liste der Zielkonten, für die die kontoübergreifende Backup-Kopie aufbewahrt werden soll.

maxRetentionDays (Fakultativ), Typ: int

Die maximale Aufbewahrungsdauer in Tagen für die Backup-Tresorsperre.

minRetentionDays (Fakultativ), Typ: int

Die Mindestaufbewahrungsdauer in Tagen für die Backup-Tresorsperre.

backupVaultLockÜberprüfen Sie (fakultativ), Typ: Zeichenfolge

Akzeptierte Werte: „True“ oder „False“. Geben Sie „True“ ein, damit die Regel prüft, ob die Ressource in einem gesperrten Tresor gesichert ist.

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

dynamodb-table-deletion-protection-aktiviert

Prüft, ob für eine Amazon DynamoDB-Tabelle der Löschschutz aktiviert ist. Die Regel ist NON_COMPLIANT, wenn für die Tabelle der Löschschutz deaktiviert ist.

ID: DYNAMODB_TABLE_DELETION_PROTECTION_ENABLED

Ressourcentypen: AWS::DynamoDB::Table

Auslösertyp: Konfigurationsänderungen

AWS-Region: Alle unterstützten AWS Regionen außer Asien-Pazifik (Thailand), Asien-Pazifik (Malaysia), Mexiko (Zentral) und Kanada West (Calgary)

Parameter:

Keine

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

dynamodb-table-encrypted-kms

Prüft, ob die Amazon DynamoDB-Tabelle mit dem AWS Key Management Service (KMS) verschlüsselt ist. Die Regel lautet NON_COMPLIANT, wenn die Amazon DynamoDB-Tabelle nicht mit KMS verschlüsselt ist. AWS Die Regel ist auch NON_COMPLIANT, wenn der verschlüsselte AWS KMS-Schlüssel nicht im Eingabeparameter vorhanden ist. `kmsKeyArns`

Kennung: DYNAMODB_TABLE_ENCRYPTED_KMS

Ressourcentypen: AWS::DynamoDB::Table

Auslösertyp: Konfigurationsänderungen

AWS-Region: Alle unterstützten AWS Regionen außer der Region Asien-Pazifik (Taipeh)

Parameter:

kmsKeyArns (Fakultativ), Typ: CSV

Kommagetrennte Liste der AWS KMS-Schlüssel, die für die Verschlüsselung von Amazon DynamoDB-Tabellen ARNs zulässig sind.

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

dynamodb-table-encryption-enabled

Prüft, ob die Amazon-DynamoDB-Tabellen verschlüsselt sind, und überprüft ihren Status. Die Regel ist COMPLIANT, wenn der Status "Aktiviert" oder "Wird aktiviert" lautet.

ID: DYNAMODB_TABLE_ENCRYPTION_ENABLED

Ressourcentypen: AWS::DynamoDB::Table

Auslösertyp: Konfigurationsänderungen

AWS-Region: Alle unterstützten AWS Regionen außer Europa (Stockholm), Naher Osten (Bahrain), Asien-Pazifik (Jakarta), Afrika (Kapstadt), Asien-Pazifik (Hongkong), Asien-Pazifik (Hyderabad), Asien-Pazifik (Osaka), Europa (Mailand), Europa (Spanien), China (Ningxia)

Parameter:

Keine

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

dynamodb-throughput-limit-check

Prüft, ob der bereitgestellte DynamoDB-Durchsatz das Maximallimit für Ihr Konto erreicht. Standardmäßig wird von der Regel geprüft, ob ein bereitgestellter Durchsatz einen Schwellenwert von 80 Prozent Ihres Kontolimits überschreitet.

ID: DYNAMODB_THROUGHPUT_LIMIT_CHECK

Auslösertyp: Regelmäßig

AWS-Region: Alle unterstützten AWS Regionen außer der Region Asien-Pazifik (Taipeh)

Parameter:

RCUThresholdProzentsatz des Kontos (optional), Typ: int, Standard: 80

Prozentsatz der bereitgestellten Lesekapazitätseinheiten für Ihr Konto. Wenn dieser Wert erreicht ist, wird die Regel als nicht konform gekennzeichnet.

WCUThresholdProzentsatz des Kontos (optional), Typ: int, Standard: 80

Prozentsatz der bereitgestellten Schreibkapazitätseinheiten für Ihr Konto. Wenn dieser Wert erreicht ist, wird die Regel als nicht konform gekennzeichnet.

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

ebs-in-backup-plan

Prüfen Sie, ob Amazon Elastic Block Store (Amazon EBS) -Volumes zu den Backup-Plänen von AWS Backup hinzugefügt wurden. Die Regel ist NON_COMPLIANT, wenn Amazon-EBS-Volumes nicht in den Backup-Plänen enthalten sind.

ID: EBS_IN_BACKUP_PLAN

Ressourcentypen: AWS::EC2::Volume

Auslösertyp: Regelmäßig

AWS-Region: Alle unterstützten AWS Regionen außer Asien-Pazifik (Melbourne), Asien-Pazifik (Taipeh) und Kanada West (Calgary)

Parameter:

Keine

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

ebs-last-backup-recovery-Punkt-erstellt

Prüft, ob für Amazon Elastic Block Store (Amazon EBS) ein Wiederherstellungspunkt erstellt wurde. Die Regel ist NON_COMPLIANT, wenn innerhalb des angegebenen Zeitraums kein entsprechender Wiederherstellungspunkt für das Amazon-EBS-Volume erstellt wurde.

ID: EBS_LAST_BACKUP_RECOVERY_POINT_CREATED

Ressourcentypen: AWS::EC2::Volume

Auslösertyp: Regelmäßig

AWS-Region: Alle unterstützten AWS Regionen außer China (Peking), Asien-Pazifik (Thailand), Asien-Pazifik (Malaysia), Mexiko (Zentral), Israel (Tel Aviv), Kanada West (Calgary), China (Ningxia)

Parameter:

resourceTags (optional), Typ: Zeichenfolge

Tags der Amazon-EBS-Volumes, die von der Regel geprüft werden sollen, im JSON-Format `{"tagkey" : "tagValue"}`.

resourceId (optional), Typ: Zeichenfolge

ID des Amazon-EBS-Volumes, das von der Regel geprüft werden soll.

recoveryPointAgeWert (optional), Typ: int, Standard: 1

Numerischer Wert für das zulässige Höchstalter. Nicht mehr als 744 für Stunden oder 31 für Tage.

recoveryPointAgeEinheit (optional), Typ: Zeichenfolge, Standard: days

Zeiteinheit für das zulässige Höchstalter. Zulässige Werte: „Stunden“, „Tage“.

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

ebs-meets-restore-time-ziel

Prüft, ob die Wiederherstellungszeit von Amazon Elastic Block Store (Amazon EBS)-Instances der angegebenen Dauer entspricht. Die Regel lautet NON_COMPLIANT, wenn LatestRestoreExecutionTimeMinutes der Wert eines Amazon EBS-Volumes mehr als Minuten beträgt. maxRestoreTime

Kennung: EBS_MEETS_RESTORE_TIME_TARGET

Ressourcentypen: AWS::EC2::Volume

Auslösertyp: Regelmäßig

AWS-Region: Alle unterstützten AWS Regionen außer China (Peking), Asien-Pazifik (Thailand), Asien-Pazifik (Malaysia), AWS GovCloud (USA-Ost), AWS GovCloud (US-West), Mexiko (Zentral), Israel (Tel Aviv), Kanada West (Calgary), China (Ningxia)

Parameter:

maxRestoreTime, Typ: int

Numerischer Wert für die maximal zulässige Wiederherstellungslaufzeit.

resourceTags (optional), Typ: Zeichenfolge

Tags für Amazon-EBS-Volumes, die von der Regel geprüft werden sollen, im JSON-Format.

resourceId (optional), Typ: Zeichenfolge

ID des Amazon-EBS-Volumes, das von der Regel geprüft werden soll.

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

ebs-optimized-instance

Prüft, ob die Amazon EBS-Optimierung für Ihre Amazon Elastic Compute Cloud (Amazon EC2) -Instances aktiviert ist, die Amazon EBS-optimiert werden können. Die Regel lautet NON_COMPLIANT, wenn die EBS-Optimierung für eine EC2 Amazon-Instance, die EBS-optimiert werden kann, nicht aktiviert ist.

> **Note**
>
> EC2 Instances, die standardmäßig EBS-optimiert sind, führen immer dazu, dass Regelauswertungen zurückgegeben werden. `COMPLIANT`

ID: EBS_OPTIMIZED_INSTANCE

Ressourcentypen: AWS::EC2::Instance

Auslösertyp: Konfigurationsänderungen

AWS-Region: Alle unterstützten AWS Regionen außer Asien-Pazifik (Thailand), Asien-Pazifik (Malaysia), Mexiko (Zentral), Asien-Pazifik (Taipeh) und Kanada West (Calgary)

Parameter:

Keine

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

ebs-resources-in-logically-air-gapped-vault

Überprüft, ob sich Amazon Elastic Block Store (Amazon EBS) -Volumes in einem Tresor mit logischem Air-Gap befinden. Die Regel lautet NON_COMPLIANT, wenn sich ein Amazon EBS-Volume innerhalb des angegebenen Zeitraums nicht in einem Tresor mit logischem Air-Gap befindet.

Kennung: EBS_RESOURCES_IN_LOGICALLY_AIR_GAPPED_VAULT

Ressourcentypen: AWS::EC2::Volume

Auslösertyp: Regelmäßig

AWS-Region: Alle unterstützten AWS Regionen außer China (Peking), Asien-Pazifik (Thailand), Asien-Pazifik (Malaysia), AWS GovCloud (USA-Ost), AWS GovCloud (US-West), Mexiko (Zentral), Israel (Tel Aviv), Kanada West (Calgary), China (Ningxia)

Parameter:

resourceTags (optional), Typ: Zeichenfolge

Tags von Amazon EBS-Volumes, die von der Regel überprüft werden sollen, im JSON-Format.

resourceId (optional), Typ: Zeichenfolge

ID des Amazon-EBS-Volumes, das von der Regel geprüft werden soll.

recoveryPointAgeWert (optional), Typ: int, Standard: 1

Numerischer Wert für das zulässige Höchstalter. Nicht mehr als 2184 für Stunden, 91 für Tage.

recoveryPointAgeEinheit (optional), Typ: Zeichenfolge, Standard: days

Zeiteinheit für das zulässige Höchstalter. Zulässige Werte: „Stunden“, „Tage“.

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

ebs-resources-protected-by-Backup-Plan

Prüft, ob Amazon Elastic Block Store (Amazon EBS)-Volumes durch einen Backup-Plan geschützt sind. Die Regel ist NON_COMPLIANT, wenn das Amazon-EBS-Volume nicht durch einen Backup-Plan gedeckt ist.

ID: EBS_RESOURCES_PROTECTED_BY_BACKUP_PLAN

Ressourcentypen: AWS::EC2::Volume

Auslösertyp: Regelmäßig

AWS-Region: Alle unterstützten AWS Regionen außer China (Peking), Asien-Pazifik (Thailand), Asien-Pazifik (Malaysia), Mexiko (Zentral), Israel (Tel Aviv), Kanada West (Calgary), China (Ningxia)

Parameter:

resourceTags (optional), Typ: Zeichenfolge

Tags für Amazon-EBS-Volumes, die von der Regel geprüft werden sollen, im JSON-Format `{"tagkey" : "tagValue"}`.

resourceId (optional), Typ: Zeichenfolge

ID des Amazon-EBS-Volumes, das von der Regel geprüft werden soll.

crossRegionList (Fakultativ), Typ: Zeichenfolge

Durch Kommata getrennte Liste der Zielregionen, für die die regionsübergreifende Backup-Kopie aufbewahrt werden soll.

crossAccountList (Fakultativ), Typ: Zeichenfolge

Durch Kommata getrennte Liste der Zielkonten, für die die kontoübergreifende Backup-Kopie aufbewahrt werden soll.

maxRetentionDays (Fakultativ), Typ: int

Die maximale Aufbewahrungsdauer in Tagen für die Backup-Tresorsperre.

minRetentionDays (Fakultativ), Typ: int

Die Mindestaufbewahrungsdauer in Tagen für die Backup-Tresorsperre.

backupVaultLockÜberprüfen Sie (fakultativ), Typ: Zeichenfolge

Akzeptierte Werte: „True“ oder „False“. Geben Sie „True“ ein, damit die Regel prüft, ob die Ressource in einem gesperrten Tresor gesichert ist.

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

ebs-snapshot-public-restorable-überprüfen

Prüft, ob Amazon Elastic Block Store (Amazon EBS)-Snapshots nicht öffentlich wiederherstellbar sind. Die Regel lautet NON_COMPLIANT, wenn ein oder mehrere Snapshots mit RestorableByUserIds Feld auf all gesetzt sind, d. h. Amazon EBS-Snapshots sind öffentlich.

ID: EBS_SNAPSHOT_PUBLIC_RESTORABLE_CHECK

Auslösertyp: Regelmäßig

AWS-Region: Alle unterstützten AWS Regionen außer der Region Europa (Spanien)

Parameter:

Keine

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

ec2- capacity-reservation-tagged

Prüft, ob EC2 Amazon-Kapazitätsreservierungen mit Tags versehen sind. Optional können Sie Tag-Schlüssel für die Regel angeben. Die Regel ist NON_COMPLIANT, wenn keine Tags vorhanden sind oder wenn die angegebenen Tag-Schlüssel nicht vorhanden sind. Die Regel sucht nicht nach Tags, die mit 'aws: 'beginnen.

Kennung: EC2 _CAPACITY_RESERVATION_TAGGED

Ressourcentypen: AWS::EC2::CapacityReservation

Auslösertyp: Konfigurationsänderungen

AWS-Region: Alle unterstützten AWS Regionen außer China (Peking), Asien-Pazifik (Thailand), Asien-Pazifik (Malaysia), AWS GovCloud (USA-Ost), AWS GovCloud (US-West), Mexiko (Zentral), China (Ningxia)

Parameter:

requiredKeyTags (Fakultativ), Typ: CSV

> Durch Kommas getrennte Liste von Tag-Schlüsseln, die von der Regel überprüft werden sollen. Falls angegeben, lautet die Regel NON_COMPLIANT, wenn die ausgewertete Ressource diese Schlüssel nicht enthält. Bei Tag-Schlüsseln wird die Groß- und Kleinschreibung beachtet. Tag-Schlüssel, die mit „aws:“ beginnen, sind nicht erlaubt.

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

ec2- carrier-gateway-tagged

Überprüft, ob die Gateways von Amazon EC2 Carrier Tags haben. Optional können Sie Tag-Schlüssel für die Regel angeben. Die Regel ist NON_COMPLIANT, wenn keine Tags vorhanden sind oder wenn die angegebenen Tag-Schlüssel nicht vorhanden sind. Die Regel sucht nicht nach Tags, die mit 'aws: 'beginnen.

Kennung: EC2 _CARRIER_GATEWAY_TAGGED

Ressourcentypen: AWS::EC2::CarrierGateway

Auslösertyp: Konfigurationsänderungen

AWS-Region: Nur in Europa (Paris), USA Ost (Ohio), Europa (Irland), Europa (Frankfurt), USA Ost (Nord-Virginia), Asien-Pazifik (Seoul), Europa (London), Asien-Pazifik (Tokio), USA West (Oregon), Asien-Pazifik (Sydney), Kanada (Zentral) verfügbar

Parameter:

requiredKeyTags (Fakultativ), Typ: CSV

> Durch Kommas getrennte Liste von Tag-Schlüsseln, die von der Regel überprüft werden sollen. Falls angegeben, lautet die Regel NON_COMPLIANT, wenn die ausgewertete Ressource diese Schlüssel nicht enthält. Bei Tag-Schlüsseln wird die Groß- und Kleinschreibung beachtet. Tag-Schlüssel, die mit „aws:“ beginnen, sind nicht erlaubt.

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

ec2- aktiviert client-vpn-connection-log

Prüft, ob für den AWS Client-VPN-Endpunkt die Client-Verbindungsprotokollierung aktiviert ist. Die Regel ist NON_COMPLIANT, wenn es sich um „Konfiguration“ handelt. ConnectionLogOptions.Enabled' ist auf false gesetzt.

Kennung: _CLIENT_VPN_CONNECTION_LOG_ENABLED EC2

Ressourcentypen: AWS::EC2::ClientVpnEndpoint

Auslösertyp: Konfigurationsänderungen

AWS-Region: Alle unterstützten AWS Regionen außer China (Peking), Asien-Pazifik (Thailand), Asien-Pazifik (Jakarta), Naher Osten (VAE), Asien-Pazifik (Hyderabad), Asien-Pazifik (Malaysia), Mexiko (Zentral), Israel (Tel Aviv), Kanada West (Calgary), Europa (Spanien), China (Ningxia)

Parameter:

Keine

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

ec2- client-vpn-endpoint-tagged

Überprüft, ob EC2 Amazon-Client-VPN-Endpunkte Tags haben. Optional können Sie Tag-Schlüssel für die Regel angeben. Die Regel ist NON_COMPLIANT, wenn keine Tags vorhanden sind oder wenn die angegebenen Tag-Schlüssel nicht vorhanden sind. Die Regel sucht nicht nach Tags, die mit 'aws: 'beginnen.

Kennung: EC2 _CLIENT_VPN_ENDPOINT_TAGGED

Ressourcentypen: AWS::EC2::ClientVpnEndpoint

Auslösertyp: Konfigurationsänderungen

AWS-Region: Alle unterstützten AWS Regionen außer China (Peking), Asien-Pazifik (Thailand), Asien-Pazifik (Jakarta), Naher Osten (VAE), Asien-Pazifik (Hyderabad), Asien-Pazifik (Malaysia), AWS GovCloud (USA-Ost), AWS GovCloud (US-West), Mexiko (Zentral), Israel (Tel Aviv), Kanada West (Calgary), Europa (Spanien), China (Ningxia)

Parameter:

requiredKeyTags (Fakultativ), Typ: CSV

> Durch Kommas getrennte Liste von Tag-Schlüsseln, die von der Regel überprüft werden sollen. Falls angegeben, lautet die Regel NON_COMPLIANT, wenn die ausgewertete Ressource diese Schlüssel nicht enthält. Bei Tag-Schlüsseln wird die Groß- und Kleinschreibung beachtet. Tag-Schlüssel, die mit „aws:“ beginnen, sind nicht erlaubt.

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

ec2- -alle client-vpn-not-authorize

Prüft, ob die AWS Client-VPN-Autorisierungsregeln den Verbindungszugriff für alle Clients autorisieren. Die Regel ist NON_COMPLIANT, wenn 'AccessAll' vorhanden und auf true gesetzt ist.

Kennung: _CLIENT_VPN_NOT_AUTHORIZE_ALL EC2

Ressourcentypen: AWS::EC2::ClientVpnEndpoint

Auslösertyp: Regelmäßig

AWS-Region: Alle unterstützten AWS Regionen außer China (Peking), Asien-Pazifik (Thailand), Asien-Pazifik (Jakarta), Naher Osten (VAE), Asien-Pazifik (Hyderabad), Asien-Pazifik (Osaka), Asien-Pazifik (Malaysia), Asien-Pazifik (Melbourne), AWS GovCloud (USA-Ost), AWS GovCloud (US-West), Mexiko (Zentral), Israel (Tel Aviv), Kanada West (Calgary), Europa (Spanien), China (Ningxia), Europa (Region Zürich)

Parameter:

Keine

AWS CloudFormation Schablone

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

ec2- dhcp-options-tagged

Prüft, ob Amazon EC2 DHCP-Optionen Tags haben. Optional können Sie Tag-Schlüssel für die Regel angeben. Die Regel ist NON_COMPLIANT, wenn keine Tags vorhanden sind oder wenn die angegebenen Tag-Schlüssel nicht vorhanden sind. Die Regel sucht nicht nach Tags, die mit 'aws: 'beginnen.

Kennung: EC2 _DHCP_OPTIONS_TAGGED

Ressourcentypen: AWS::EC2::DHCPOptions

Auslösertyp: Konfigurationsänderungen

AWS-Region: Alle unterstützten AWS Regionen außer China (Peking), Asien-Pazifik (Thailand), Asien-Pazifik (Malaysia), AWS GovCloud (USA-Ost), AWS GovCloud (US-West), Mexiko (Zentral), China (Ningxia)

Parameter:

requiredKeyTags (Fakultativ), Typ: CSV

> Durch Kommas getrennte Liste von Tag-Schlüsseln, die von der Regel überprüft werden sollen. Falls angegeben, lautet die Regel NON_COMPLIANT, wenn die ausgewertete Ressource diese Schlüssel nicht enthält. Bei Tag-Schlüsseln wird die Groß- und Kleinschreibung beachtet. Tag-Schlüssel, die mit „aws:“ beginnen, sind nicht erlaubt.

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

ec2- ebs-encryption-by-default

Prüft, ob die Amazon-EBS-Verschlüsselung (Amazon Elastic Block Store) standardmäßig aktiviert ist. Die Regel ist NON_COMPLIANT, wenn die Verschlüsselung nicht aktiviert ist.

Kennung: _EBS_ENCRYPTION_BY_DEFAULT EC2

Auslösertyp: Regelmäßig

AWS-Region: Alle unterstützten Regionen AWS

Parameter:

Keine

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

ec2- aktiviert enis-source-destination-check

EC2 ENIs source/destination Prüft, ob bei der Verwaltung durch Benutzer die Option „Prüfung“ aktiviert ist. Die Regel lautet NON_COMPLIANT, wenn die source/destination Prüfung ENIs für diese Optionen für 'Lambda', 'aws_codestar_connections_managed', 'branch', 'efa', 'interface' und 'quicksight' deaktiviert ist.

Kennung EC2: _ENIS_SOURCE_DESTINATION_CHECK_ENABLED

Ressourcentypen: AWS::EC2::NetworkInterface

Auslösertyp: Konfigurationsänderungen

AWS-Region: Alle unterstützten AWS Regionen außer China (Peking), Asien-Pazifik (Thailand), Naher Osten (VAE), Asien-Pazifik (Hyderabad), Asien-Pazifik (Seoul), Asien-Pazifik (Malaysia), Mexiko (Zentral), Israel (Tel Aviv), Kanada West (Calgary), Europa (Spanien), Europa (Zürich)

Parameter:

Keine

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

ec2-fleet-markiert

Prüft, ob EC2 Amazon-Flotten Tags haben. Optional können Sie Tag-Schlüssel angeben. Die Regel lautet NON_COMPLIANT, wenn keine Tags vorhanden sind oder wenn die angegebenen Tag-Schlüssel nicht vorhanden sind. Die Regel sucht nicht nach Tags, die mit 'aws: 'beginnen.

Kennung: EC2 _FLEET_TAGGED

Ressourcentypen: 2Fleet AWS::EC2::EC

Auslösertyp: Konfigurationsänderungen

AWS-Region: Alle unterstützten AWS Regionen außer China (Peking), Asien-Pazifik (Thailand), Asien-Pazifik (Malaysia), AWS GovCloud (USA-Ost), AWS GovCloud (US-West), Mexiko (Zentral), Israel (Tel Aviv), Kanada West (Calgary), China (Ningxia)

Parameter:

requiredKeyTags (Fakultativ), Typ: CSV

Durch Kommas getrennte Liste von Tag-Schlüsseln, die von der Regel überprüft werden sollen. Falls angegeben, lautet die Regel NON_COMPLIANT, wenn die ausgewertete Ressource diese Schlüssel nicht enthält. Bei Tag-Schlüsseln wird die Groß- und Kleinschreibung beachtet. Tag-Schlüssel, die mit „aws:“ beginnen, sind nicht erlaubt.

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

ec2-imdsv2-check

Prüft, ob die Metadatenversion Ihrer Amazon Elastic Compute Cloud (Amazon EC2) -Instance mit Instance Metadata Service Version 2 (IMDSv2) konfiguriert ist. Die Regel ist NON_COMPLIANT, wenn sie auf HttpTokens optional gesetzt ist.

Kennung: _ _CHECK EC2 IMDSV2

Ressourcentypen: AWS::EC2::Instance

Auslösertyp: Konfigurationsänderungen

AWS-Region: Alle unterstützten AWS Regionen

Parameter:

Keine

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

ec2- instance-detailed-monitoring-enabled

Prüft, ob die detaillierte Überwachung für EC2 Instanzen aktiviert ist. Die Regel ist NON_COMPLIANT, wenn keine detaillierte Überwachung aktiviert ist.

Kennung: EC2 _INSTANCE_DETAILED_MONITORING_ENABLED

Ressourcentypen: AWS::EC2::Instance

Auslösertyp: Konfigurationsänderungen

AWS-Region: Alle unterstützten AWS Regionen

Parameter:

Keine

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

ec2-ami instance-launched-with-allowed

Prüft, ob laufende oder gestoppte EC2 Instances mit Amazon Machine Images (AMIs) gestartet wurden, die Ihren AMIs Zulassungskriterien entsprechen. Die Regel lautet NON_COMPLIANT, wenn ein AMI die AMIs Kriterien „Zulässig“ nicht erfüllt und die AMIs Einstellungen „Zulässig“ nicht deaktiviert sind.

Kennung: _INSTANCE_LAUNCHED_WITH_ALLOWED_AMI EC2

Ressourcentypen: AWS::EC2::Instance

Auslösertyp: „Konfigurationsänderungen“ und „Regelmäßig“

AWS-Region: Alle unterstützten AWS Regionen

Parameter:

InstanceStateNameList (Fakultativ), Typ: CSV

> Durch Kommas getrennte Liste der EC2 Amazon-Instance-Staaten, die von der Regel überprüft werden sollen. Gültige Werte sind „running“ und „stopped“.

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

ec2-manager instance-managed-by-systems

> **Important**
>
> Bei dieser Regel unterscheiden sich die Regel-ID (EC2_INSTANCE_MANAGED_BY_SSM) und der Regelname (ec2- -manager). instance-managed-by-systems

Überprüft, ob Ihre EC2 Amazon-Instances von einem AWS Systems Manager Agenten (SSM-Agent) verwaltet werden. Die Regel lautet NON_COMPLIANT, wenn eine EC2 Instance läuft und der SSM-Agent gestoppt ist oder wenn eine EC2 Instance läuft und der SSM-Agent beendet ist.

> **Note**
>
> Die Regel gibt nicht NON_COMPLIANT zurück, wenn eine EC2 Instanz gestoppt ist und der SSM-Agent läuft.

Kennung: _INSTANCE_MANAGED_BY_SSM EC2

Ressourcentypen:, AWS::EC2::Instance AWS::SSM::ManagedInstanceInventory

Auslösertyp: Konfigurationsänderungen

AWS-Region: Alle unterstützten AWS Regionen außer Naher Osten (VAE) und Asien-Pazifik (Taipeh)

Parameter:

Keine

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

ec2- instance-multiple-eni-check

Prüft, ob Amazon Elastic Compute Cloud (Amazon EC2) mehrere Elastic Network Interfaces (ENIs) oder Elastic Fabric Adapter (EFAs) verwendet. Die Regel lautet NON_COMPLIANT. Eine EC2 Amazon-Instance verwendet mehrere Netzwerkschnittstellen.

Kennung: _INSTANCE_MULTIPLE_ENI_CHECK EC2

Ressourcentypen: AWS::EC2::Instance

Auslösertyp: Konfigurationsänderungen

AWS-Region: Alle unterstützten AWS Regionen

Parameter:

NetworkInterfaceIds (Fakultativ), Typ: CSV

Durch Kommas getrennte Liste der Netzwerkinstanzen IDs

Proaktive Auswertung

Anweisungen zur Ausführung dieser Regel im proaktiven Modus finden Sie unter Evaluieren Ihrer Ressourcen mithilfe AWS Config von Regeln. Damit diese Regel im proaktiven Modus COMPLIANT zurückgibt, muss das Ressourcenkonfigurationsschema für die StartResourceEvaluationAPI die folgenden Eingaben enthalten, die als Zeichenfolge kodiert sind:

```
"ResourceConfiguration":
...
{
   "NetworkInterfaces": "[NetworkInterfaceId-1, NetworkInterfaceId-2,
 NetworkInterfaceId-3, ...]"
}
...
```

Weitere Informationen zur proaktiven Auswertung finden Sie unter Auswertungsmodus.

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

ec2- instance-no-public-ip

Prüft, ob EC2 Instances eine öffentliche IP-Zuordnung haben. Die Regel lautet NON_COMPLIANT, wenn das Feld publicIP im Instanzkonfigurationselement vorhanden ist. EC2 Die Regel gilt nur für. IPv4

Kontext: Öffentliche IP-Adressen können den direkten Zugriff auf EC2 Instanzen über das Internet ermöglichen, was unter Sicherheits- oder Compliance-Gesichtspunkten möglicherweise nicht immer wünschenswert ist:

- Sicherheit: In vielen Fällen möchten Sie möglicherweise nicht, dass Ihre EC2 Instances öffentliche IP-Adressen haben, es sei denn, sie müssen öffentlich zugänglich sein. Eine öffentliche IP-Adresse kann Ihre EC2 Instance potenziellen Sicherheitsrisiken wie unbefugtem Zugriff oder Angriffen aussetzen.
- Compliance: Verschiedene Compliance-Standards wie PCI, DSS oder HIPAA haben spezifische Anforderungen in Bezug auf Netzwerksegmentierung und Zugriffskontrollen. Wenn Sie sicherstellen, dass EC2 Instances keine unnötigen öffentlichen IP-Adressen haben, können Sie die Einhaltung dieser Anforderungen sicherstellen.
- Kostenmanagement: Öffentliche IP-Adressen können zusätzliche Kosten verursachen, insbesondere wenn ihnen ständig EC2 Instanzen zugeordnet sind. Indem Sie öffentliche EC2 Instanzen identifizieren IPs , die diese nicht benötigen, können Sie potenziell die Kosten senken.

Kennung: EC2 _INSTANCE_NO_PUBLIC_IP

Ressourcentypen: AWS::EC2::Instance

Auslösertyp: Konfigurationsänderungen

AWS-Region: Alle unterstützten AWS Regionen

Parameter:

Keine

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

ec2- instance-profile-attached

Prüft, ob an eine EC2 Instanz ein AWS Identity and Access Management (IAM) -Profil angehängt ist. Die Regel lautet NON_COMPLIANT, wenn der Instanz kein IAM-Profil angehängt ist. EC2

Kennung: _INSTANCE_PROFILE_ATTACHED EC2

Ressourcentypen: AWS::EC2::Instance

Auslösertyp: Konfigurationsänderungen

AWS-Region: Alle unterstützten AWS Regionen außer Asien-Pazifik (Taipeh) und Kanada West (Calgary)

Parameter:

IamInstanceProfileArnList (Fakultativ), Typ: CSV

> Durch Kommas getrennte Liste von Amazon Resource Names (ARNs) für das IAM-Profil, die Amazon-Instances angehängt werden können. EC2

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

ec2- erstellt last-backup-recovery-point

Prüft, ob ein Erholungspunkt für Amazon Elastic Compute Cloud (Amazon EC2) -Instances erstellt wurde. Die Regel lautet NON_COMPLIANT, wenn für die EC2 Amazon-Instance innerhalb des angegebenen Zeitraums kein entsprechender Wiederherstellungspunkt erstellt wurde.

Kennung: _LAST_BACKUP_RECOVERY_POINT_CREATED EC2

Ressourcentypen: AWS::EC2::Instance

Auslösertyp: Regelmäßig

AWS-Region: Alle unterstützten AWS Regionen außer China (Peking), Asien-Pazifik (Thailand), Asien-Pazifik (Malaysia), Mexiko (Zentral), Israel (Tel Aviv), Kanada West (Calgary), China (Ningxia)

Parameter:

resourceTags (optional), Typ: Zeichenfolge

> Tags von EC2 Amazon-Instances, die von der Regel überprüft werden sollen, im JSON-Format`{"tagkey" : "tagValue"}`.

resourceId (optional), Typ: Zeichenfolge

ID der EC2 Amazon-Instance, für die die Regel überprüft werden soll.

recoveryPointAgeWert (optional), Typ: int, Standard: 1

Numerischer Wert für das zulässige Höchstalter. Nicht mehr als 744 für Stunden oder 31 für Tage.

recoveryPointAgeEinheit (optional), Typ: Zeichenfolge, Standard: days

Zeiteinheit für das zulässige Höchstalter. Zulässige Werte: „Stunden“, „Tage“.

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

ec2-2-check launch-template-imdsv

Prüft, ob die aktuell festgelegte Standardversion einer Amazon EC2 Launch Template erfordert, dass neu gestartete Instances Version 2 des Amazon EC2 Instance Metadata Service (IMDSv2) verwenden. Die Regel lautet NON_COMPLIANT, wenn für „Metadaten-Version“ nicht V2 () angegeben ist. IMDSv2

Kennung: _LAUNCH_TEMPLATE_ _CHECK EC2 IMDSV2

Ressourcentypen: AWS::EC2::LaunchTemplate

Auslösertyp: Konfigurationsänderungen

AWS-Region: Alle unterstützten AWS Regionen außer Asien-Pazifik (Thailand), Naher Osten (VAE), Asien-Pazifik (Hyderabad), Asien-Pazifik (Malaysia), Asien-Pazifik (Melbourne), AWS GovCloud (USA-Ost), AWS GovCloud (US-West), Mexiko (Zentral), Israel (Tel Aviv), Kanada West (Calgary), Europa (Spanien), Europa (Zürich)

Parameter:

Keine

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

ec2- deaktiviert launch-template-public-ip

Prüft, ob Amazon EC2 Launch Templates so eingestellt sind, dass Netzwerkschnittstellen öffentliche IP-Adressen zugewiesen werden. Die Regel lautet NON_COMPLIANT, wenn die Standardversion einer EC2 Startvorlage mindestens eine Netzwerkschnittstelle hat, bei der '' auf 'trueAssociatePublicIpAddress' gesetzt ist.

Kennung EC2: _LAUNCH_TEMPLATE_PUBLIC_IP_DISABLED

Ressourcentypen: AWS::EC2::LaunchTemplate

Auslösertyp: Konfigurationsänderungen

AWS-Region: Alle unterstützten AWS Regionen außer Asien-Pazifik (Thailand), Naher Osten (VAE), Asien-Pazifik (Hyderabad), Asien-Pazifik (Malaysia), Asien-Pazifik (Melbourne), AWS GovCloud (USA-Ost), AWS GovCloud (US-West), Mexiko (Zentral), Israel (Tel Aviv), Kanada West (Calgary), Europa (Spanien), Europa (Zürich)

Parameter:

exemptedLaunchTemplates (Fakultativ), Typ: CSV

> Durch Kommas getrennte Liste der ausgenommenen EC2 Startvorlagen IDs , für die Netzwerkschnittstellen verwendet werden dürfen, deren AssociatePublicIpAddress Wert auf „true“ gesetzt ist.

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

ec2- launch-template-tagged

Prüft, ob EC2 Amazon-Startvorlagen Tags haben. Optional können Sie Tag-Schlüssel für die Regel angeben. Die Regel ist NON_COMPLIANT, wenn keine Tags vorhanden sind oder wenn die angegebenen Tag-Schlüssel nicht vorhanden sind. Die Regel sucht nicht nach Tags, die mit 'aws: 'beginnen.

Kennung: EC2 _LAUNCH_TEMPLATE_TAGGED

Ressourcentypen: AWS::EC2::LaunchTemplate

Auslösertyp: Konfigurationsänderungen

AWS-Region: Alle unterstützten AWS Regionen außer China (Peking), Asien-Pazifik (Thailand), Naher Osten (VAE), Asien-Pazifik (Hyderabad), Asien-Pazifik (Malaysia), Asien-Pazifik (Melbourne), AWS GovCloud (USA-Ost), AWS GovCloud (US-West), Mexiko (Zentral), Israel (Tel Aviv), Kanada West (Calgary), Europa (Spanien), China (Ningxia), Europa (Zürich)

Parameter:

requiredKeyTags (Fakultativ), Typ: CSV

> Durch Kommas getrennte Liste von Tag-Schlüsseln, die von der Regel überprüft werden sollen. Falls angegeben, lautet die Regel NON_COMPLIANT, wenn die ausgewertete Ressource diese Schlüssel nicht enthält. Bei Tag-Schlüsseln wird die Groß- und Kleinschreibung beachtet. Tag-Schlüssel, die mit „aws:“ beginnen, sind nicht erlaubt.

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

ec2- managedinstance-applications-blacklisted

Prüft, ob keine der angegebenen Anwendungen auf der Instance installiert ist. Legen Sie optional die Version fest. Neuere Versionen werden in der Liste aufgeführt. Geben Sie optional die Plattform an, um die Regel nur für Instances anzuwenden, auf denen die Plattform ausgeführt wird.

Kennung: EC2 _MANAGEDINSTANCE_APPLICATIONS_BLACKLISTED

Ressourcentypen: AWS::SSM::ManagedInstanceInventory

Auslösertyp: Konfigurationsänderungen

AWS-Region: Alle unterstützten AWS Regionen außer Asien-Pazifik (Taipeh) und Kanada West (Calgary)

Parameter:

applicationNames, Typ: CSV

> Durch Komma getrennte Liste der Anwendungsnamen. Geben Sie Versionen optional mit angehängtem „:“ an (z. B. „Chrome: 0.5.3, FireFox“).

> **Note**
>
> Die Anwendungsnamen müssen genau übereinstimmen. Verwenden Sie beispielsweise **`firefox`** unter Linux oder **`firefox-compat`** unter Amazon Linux. Außerdem werden derzeit AWS Config keine Platzhalter für den ApplicationNames-Parameter unterstützt (z. B.**`firefox*`**).

platformType (optional), Typ: Zeichenfolge

Plattformtyp (z. B. „Linux“ oder „Windows“).

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

ec2- managedinstance-applications-required

Prüft, ob alle der angegebenen Anwendungen auf der Instance installiert sind. Geben Sie optional die akzeptable Mindestversion an. Sie können optional die Plattform angeben, um die Regel nur für Instances anzuwenden, auf denen die Plattform ausgeführt wird.

> **Note**
>
> Stellen Sie sicher, dass der SSM-Agent auf der EC2 Instance ausgeführt wird und eine Verknüpfung zur Erfassung des Anwendungssoftwareinventars erstellt wurde. Die Regel kehrt zurück`NOT_APPLICABLE`, wenn der SSM-Agent nicht installiert ist oder noch keine Zuordnung erstellt wurde oder ausgeführt wird.

Kennung: EC2 _MANAGEDINSTANCE_APPLICATIONS_REQUIRED

Ressourcentypen: AWS::SSM::ManagedInstanceInventory

Auslösertyp: Konfigurationsänderungen

AWS-Region: Alle unterstützten AWS Regionen außer Asien-Pazifik (Taipeh) und Kanada West (Calgary)

Parameter:

applicationNames, Typ: CSV

Durch Komma getrennte Liste der Anwendungsnamen. Geben Sie Versionen optional mit angehängtem „:“ an (z. B. „Chrome: 0.5.3, FireFox“).

> **Note**
>
> Die Anwendungsnamen müssen genau übereinstimmen. Verwenden Sie beispielsweise **`firefox`** unter Linux oder **`firefox-compat`** unter Amazon Linux. Außerdem werden derzeit AWS Config keine Platzhalter für den ApplicationNames-Parameter unterstützt (z. B.**`firefox*`**).

platformType (optional), Typ: Zeichenfolge

Plattformtyp (z. B. „Linux“ oder „Windows“).

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

ec2-prüfen managedinstance-association-compliance-status

Überprüft, ob der Status der AWS Systems Manager Manager-Zuordnungs-Konformität nach der Ausführung der Zuordnung auf der Instanz COMPLIANT oder NON_COMPLIANT lautet. Die Regel ist konform, wenn das Feldstatus COMPLIANT lautet. Weitere Informationen zu Zuordnungen finden Sie unter Was ist eine Zuordnung?.

Kennung: _MANAGEDINSTANCE_ASSOCIATION_COMPLIANCE_STATUS_CHECK EC2

Ressourcentypen: AWS::SSM::AssociationCompliance

Auslösertyp: Konfigurationsänderungen

AWS-Region: Alle unterstützten AWS Regionen außer Asien-Pazifik (Thailand), Asien-Pazifik (Jakarta), Afrika (Kapstadt), Asien-Pazifik (Hyderabad), Asien-Pazifik (Osaka), Asien-Pazifik

(Malaysia), Asien-Pazifik (Melbourne), Europa (Mailand), Mexiko (Zentral), Israel (Tel Aviv), Asien-Pazifik (Taipeh), Kanada West (Calgary), Europa (Spanien), Europa (Zürich)

Parameter:

Keine

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

ec2- managedinstance-inventory-blacklisted

Überprüft, ob von Amazon EC2 Systems Manager verwaltete Instances so konfiguriert sind, dass sie Inventartypen erfassen, die auf der schwarzen Liste stehen.

Kennung: EC2 _MANAGEDINSTANCE_INVENTORY_BLACKLISTED

Ressourcentypen: AWS::SSM::ManagedInstanceInventory

Auslösertyp: Konfigurationsänderungen

AWS-Region: Alle unterstützten AWS Regionen außer Asien-Pazifik (Taipeh) und Kanada West (Calgary)

Parameter:

inventoryNames, Typ: CSV

Kommagetrennte Liste der Systems Manager Manager-Inventartypen (z. B. ':Network AWS,: AWS'). WindowsUpdate

platformType (optional), Typ: Zeichenfolge

Plattformtyp (z. B. „Linux“).

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

ec2-prüfen managedinstance-patch-compliance-status

Überprüft, ob der Kompatibilitätsstatus der AWS Systems Manager Manager-Patch-Konformität nach der Patch-Installation auf der Instanz COMPLIANT oder NON_COMPLIANT lautet. Die Regel ist konform, wenn das Feldstatus COMPLIANT lautet.

Kennung: _MANAGEDINSTANCE_PATCH_COMPLIANCE_STATUS_CHECK EC2

Ressourcentypen: AWS::SSM::PatchCompliance

Auslösertyp: Konfigurationsänderungen

AWS-Region: Alle unterstützten AWS Regionen außer Asien-Pazifik (Osaka), Europa (Mailand), Asien-Pazifik (Taipeh) und Kanada West (Calgary)

Parameter:

Keine

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

ec2- managedinstance-platform-check

Prüft, ob EC2 verwaltete Instanzen die gewünschten Konfigurationen haben.

Kennung: EC2 _MANAGEDINSTANCE_PLATFORM_CHECK

Ressourcentypen: AWS::SSM::ManagedInstanceInventory

Auslösertyp: Konfigurationsänderungen

AWS-Region: Alle unterstützten AWS Regionen außer Asien-Pazifik (Taipeh) und Kanada West (Calgary)

Parameter:

platformType, Typ: Zeichenfolge

Plattformtyp (z. B. „Linux“).

platformVersion (optional), Typ: Zeichenfolge

Plattformversion (z. B. „2016.09“).

agentVersion (optional), Typ: Zeichenfolge

Agent-Version (z. B. „2.0.433.0“).

platformName (optional), Typ: Zeichenfolge

Die Version der Plattform (z. B. „2016.09“)

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

ec2- meets-restore-time-target

Überprüft, ob die Wiederherstellungszeit von Amazon Elastic Compute Cloud (Amazon EC2) -Instances der angegebenen Dauer entspricht. Die Regel lautet NON_COMPLIANT, wenn LatestRestoreExecutionTimeMinutes die Anzahl einer EC2 Amazon-Instance länger als maxRestoreTime Minuten ist.

Kennung: _MEETS_RESTORE_TIME_TARGET EC2

Ressourcentypen: AWS::EC2::Instance

Auslösertyp: Regelmäßig

AWS-Region: Alle unterstützten AWS Regionen außer China (Peking), Asien-Pazifik (Thailand), Asien-Pazifik (Malaysia), AWS GovCloud (USA-Ost), AWS GovCloud (US-West), Mexiko (Zentral), Israel (Tel Aviv), Kanada West (Calgary), China (Ningxia)

Parameter:

maxRestoreTime, Typ: int

Numerischer Wert für die maximal zulässige Wiederherstellungslaufzeit.

resourceTags (optional), Typ: Zeichenfolge

Tags von EC2 Amazon-Instances, die von der Regel überprüft werden sollen, im JSON-Format.

resourceId (optional), Typ: Zeichenfolge

ID der EC2 Amazon-Instance, für die die Regel überprüft werden soll.

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

ec2-analysis-tagged network-insights-access-scope

Überprüft, ob die Zugriffsumfangsanalysen von Amazon EC2 Network Insights mit Tags versehen sind. Optional können Sie Tag-Schlüssel angeben. Die Regel lautet NON_COMPLIANT, wenn keine Tags vorhanden sind oder wenn die angegebenen Tag-Schlüssel nicht vorhanden sind. Die Regel sucht nicht nach Tags, die mit 'aws: 'beginnen.

Kennung: EC2 _NETWORK_INSIGHTS_ACCESS_SCOPE_ANALYSIS_TAGGED

Ressourcentypen: AWS::EC2::NetworkInsightsAccessScopeAnalysis

Auslösertyp: Konfigurationsänderungen

AWS-Region: Alle unterstützten AWS Regionen außer China (Peking), Asien-Pazifik (Thailand), Asien-Pazifik (Jakarta), Naher Osten (VAE), Asien-Pazifik (Hyderabad), Asien-Pazifik (Malaysia), Asien-Pazifik (Melbourne), AWS GovCloud (US-Ost), AWS GovCloud (US-West), Mexiko (Zentral), Israel (Tel Aviv), Kanada West (Calgary), Europa (Spanien), China (Ningxia), Europa (Zürich)

Parameter:

requiredKeyTags (Fakultativ), Typ: CSV

Durch Kommas getrennte Liste von Tag-Schlüsseln, die von der Regel überprüft werden sollen. Falls angegeben, lautet die Regel NON_COMPLIANT, wenn die ausgewertete Ressource diese Schlüssel nicht enthält. Bei Tag-Schlüsseln wird die Groß- und Kleinschreibung beachtet. Tag-Schlüssel, die mit „aws:“ beginnen, sind nicht erlaubt.

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

ec2- markiert network-insights-access-scope

Prüft, ob die Zugriffsbereiche von Amazon EC2 Network Insights Tags haben. Optional können Sie Tag-Schlüssel angeben. Die Regel lautet NON_COMPLIANT, wenn keine Tags vorhanden sind oder wenn die angegebenen Tag-Schlüssel nicht vorhanden sind. Die Regel sucht nicht nach Tags, die mit 'aws: 'beginnen.

Kennung: EC2 _NETWORK_INSIGHTS_ACCESS_SCOPE_TAGGED

Ressourcentypen: AWS::EC2::NetworkInsightsAccessScope

Auslösertyp: Konfigurationsänderungen

AWS-Region: Alle unterstützten AWS Regionen außer China (Peking), Asien-Pazifik (Thailand), Asien-Pazifik (Jakarta), Naher Osten (VAE), Asien-Pazifik (Hyderabad), Asien-Pazifik (Malaysia), Asien-Pazifik (Melbourne), AWS GovCloud (US-Ost), AWS GovCloud (US-West), Mexiko (Zentral), Israel (Tel Aviv), Kanada West (Calgary), Europa (Spanien), China (Ningxia), Europa (Zürich)

Parameter:

requiredKeyTags (Fakultativ), Typ: CSV

> Durch Kommas getrennte Liste von Tag-Schlüsseln, die von der Regel überprüft werden sollen. Falls angegeben, lautet die Regel NON_COMPLIANT, wenn die ausgewertete Ressource diese Schlüssel nicht enthält. Bei Tag-Schlüsseln wird die Groß- und Kleinschreibung beachtet. Tag-Schlüssel, die mit „aws:“ beginnen, sind nicht erlaubt.

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

ec2- network-insights-path-tagged

Prüft, ob Amazon EC2 Network Insights-Pfade Tags haben. Optional können Sie Tag-Schlüssel angeben. Die Regel lautet NON_COMPLIANT, wenn keine Tags vorhanden sind oder wenn die angegebenen Tag-Schlüssel nicht vorhanden sind. Die Regel sucht nicht nach Tags, die mit 'aws: 'beginnen.

Kennung: EC2 _NETWORK_INSIGHTS_PATH_TAGGED

Ressourcentypen: AWS::EC2::NetworkInsightsPath

Auslösertyp: Konfigurationsänderungen

AWS-Region: Alle unterstützten AWS Regionen außer China (Peking), Asien-Pazifik (Thailand), Asien-Pazifik (Jakarta), Naher Osten (VAE), Asien-Pazifik (Hyderabad), Asien-Pazifik (Malaysia), Asien-Pazifik (Melbourne), AWS GovCloud (US-Ost), AWS GovCloud (US-West), Mexiko (Zentral), Israel (Tel Aviv), Kanada West (Calgary), Europa (Spanien), China (Ningxia), Europa (Zürich)

Parameter:

requiredKeyTags (Fakultativ), Typ: CSV

> Durch Kommas getrennte Liste von Tag-Schlüsseln, die von der Regel überprüft werden sollen. Falls angegeben, lautet die Regel NON_COMPLIANT, wenn die ausgewertete Ressource diese Schlüssel nicht enthält. Bei Tag-Schlüsseln wird die Groß- und Kleinschreibung beachtet. Tag-Schlüssel, die mit „aws:“ beginnen, sind nicht erlaubt.

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

ec2- no-amazon-key-pair

Prüft, ob laufende Amazon Elastic Compute Cloud (EC2) -Instances mit Amazon-Schlüsselpaaren gestartet werden. Die Regel lautet NON_COMPLIANT, wenn eine laufende EC2 Instance mit einem key pair gestartet wird.

Kennung: _NO_AMAZON_KEY_PAIR EC2

Ressourcentypen: AWS::EC2::Instance

Auslösertyp: Konfigurationsänderungen

AWS-Region: Alle unterstützten AWS Regionen außer China (Peking), Asien-Pazifik (Thailand), Asien-Pazifik (Jakarta), Naher Osten (VAE), Asien-Pazifik (Hyderabad), Asien-Pazifik (Malaysia), Asien-Pazifik (Melbourne), AWS GovCloud (US-Ost), AWS GovCloud (US-West), Mexiko (Zentral), Israel (Tel Aviv), Kanada West (Calgary), Europa (Spanien), China (Ningxia), Europa (Zürich)

Parameter:

Keine

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

ec2- paravirtual-instance-check

Prüft, ob der Virtualisierungstyp einer Instanz paravirtual ist. EC2 Diese Regel ist NON_COMPLIANT für eine EC2 Instanz, wenn 'VirtualizationType' auf 'paravirtual' gesetzt ist.

Kennung EC2: _PARAVIRTUAL_INSTANCE_CHECK

Ressourcentypen: AWS::EC2::Instance

Auslösertyp: Konfigurationsänderungen

AWS-Region: Nur verfügbar in China (Peking), Europa (Irland), Europa (Frankfurt), Südamerika (São Paulo), USA Ost (Nord-Virginia), Asien-Pazifik (Tokio), USA West (Oregon), USA West (Nordkalifornien), Asien-Pazifik (Singapur) und Asien-Pazifik (Sydney)

Parameter:

Keine

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

ec2- prefix-list-tagged

Prüft, ob von Amazon EC2 verwaltete Präfixlisten Tags enthalten. Optional können Sie Tag-Schlüssel für die Regel angeben. Die Regel ist NON_COMPLIANT, wenn keine Tags vorhanden sind oder wenn die angegebenen Tag-Schlüssel nicht vorhanden sind. Die Regel sucht nicht nach Tags, die mit 'aws: 'beginnen.

Kennung: EC2 _PREFIX_LIST_TAGGED

Ressourcentypen: AWS::EC2::PrefixList

Auslösertyp: Konfigurationsänderungen

AWS-Region: Alle unterstützten AWS Regionen außer China (Peking), Asien-Pazifik (Thailand), Asien-Pazifik (Malaysia), AWS GovCloud (USA-Ost), AWS GovCloud (US-West), Mexiko (Zentral), China (Ningxia)

Parameter:

requiredKeyTags (Fakultativ), Typ: CSV

Durch Kommas getrennte Liste von Tag-Schlüsseln, die von der Regel überprüft werden sollen. Falls angegeben, lautet die Regel NON_COMPLIANT, wenn die ausgewertete Ressource diese Schlüssel nicht enthält. Bei Tag-Schlüsseln wird die Groß- und Kleinschreibung beachtet. Tag-Schlüssel, die mit „aws:“ beginnen, sind nicht erlaubt.

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

ec2-Gapped-Tresor resources-in-logically-air

Prüft, ob sich Amazon Elastic Compute Cloud (Amazon EC2) -Instances in einem Tresor mit logischem Air-Gap befinden. Die Regel lautet NON_COMPLIANT, wenn sich eine EC2 Amazon-Instance innerhalb des angegebenen Zeitraums nicht in einem Tresor mit logischem Air-Gap befindet.

Kennung: EC2 _RESOURCES_IN_LOGICALLY_AIR_GAPPED_VAULT

Ressourcentypen: AWS::EC2::Instance

Auslösertyp: Regelmäßig

AWS-Region: Alle unterstützten AWS Regionen außer China (Peking), Asien-Pazifik (Thailand), Asien-Pazifik (Malaysia), AWS GovCloud (USA-Ost), AWS GovCloud (US-West), Mexiko (Zentral), Israel (Tel Aviv), Kanada West (Calgary), China (Ningxia)

Parameter:

resourceTags (optional), Typ: Zeichenfolge

Tags von EC2 Amazon-Instances, die von der Regel überprüft werden sollen, im JSON-Format.

resourceId (optional), Typ: Zeichenfolge

ID der EC2 Amazon-Instance, für die die Regel überprüft werden soll.

recoveryPointAgeWert (optional), Typ: int, Standard: 1

Numerischer Wert für das zulässige Höchstalter. Nicht mehr als 2184 für Stunden, 91 für Tage.

recoveryPointAgeEinheit (optional), Typ: Zeichenfolge, Standard: days

Zeiteinheit für das zulässige Höchstalter. Zulässige Werte: „Stunden“, „Tage“.

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

ec2-plan resources-protected-by-backup

Prüft, ob Amazon Elastic Compute Cloud (Amazon EC2) -Instances durch einen Backup-Plan geschützt sind. Die Regel lautet NON_COMPLIANT, wenn die EC2 Amazon-Instance nicht durch einen Backup-Plan abgedeckt ist.

> **Note**
>
> Diese Regel gilt nur für laufende EC2 Amazon-Instances und nicht für heruntergefahrene Instances.

Kennung: EC2 _RESOURCES_PROTECTED_BY_BACKUP_PLAN

Ressourcentypen: AWS::EC2::Instance

Auslösertyp: Regelmäßig

AWS-Region: Alle unterstützten AWS Regionen außer China (Peking), Asien-Pazifik (Thailand), Asien-Pazifik (Malaysia), Mexiko (Zentral), Israel (Tel Aviv), Kanada West (Calgary), China (Ningxia)

Parameter:

resourceTags (optional), Typ: Zeichenfolge

Tags für EC2 Amazon-Instances, die von der Regel überprüft werden sollen, im JSON-Format`{"tagkey" : "tagValue"}`.

resourceId (optional), Typ: Zeichenfolge

ID der EC2 Amazon-Instance, für die die Regel überprüft werden soll.

crossRegionList (Fakultativ), Typ: Zeichenfolge

Durch Kommata getrennte Liste der Zielregionen, für die die regionsübergreifende Backup-Kopie aufbewahrt werden soll.

crossAccountList (Fakultativ), Typ: Zeichenfolge

Durch Kommata getrennte Liste der Zielkonten, für die die kontoübergreifende Backup-Kopie aufbewahrt werden soll.

maxRetentionDays (Fakultativ), Typ: int

Die maximale Aufbewahrungsdauer in Tagen für die Backup-Tresorsperre.

minRetentionDays (Fakultativ), Typ: int

Die Mindestaufbewahrungsdauer in Tagen für die Backup-Tresorsperre.

backupVaultLockÜberprüfen Sie (fakultativ), Typ: Zeichenfolge

Akzeptierte Werte: „True“ oder „False“. Geben Sie „True“ ein, damit die Regel prüft, ob die Ressource in einem gesperrten Tresor gesichert ist.

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

ec2-eni security-group-attached-to

Prüft, ob Elastic-Network-Schnittstellen nicht standardmäßigen Sicherheitsgruppen zugeordnet sind. Die Regel ist NON_COMPLIANT, wenn die Sicherheitsgruppe keiner Network-Schnittstelle zugeordnet ist.

Kennung: _SECURITY_GROUP_ATTACHED_TO_ENI EC2

Ressourcentypen: AWS::EC2::SecurityGroup

Auslösertyp: Konfigurationsänderungen

AWS-Region: Alle unterstützten AWS Regionen außer Naher Osten (VAE), Asien-Pazifik (Taipeh) und Kanada West (Calgary)

Parameter:

Keine

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

ec2- security-group-attached-to -einperiodisch

Prüft, ob nicht standardmäßige Sicherheitsgruppen an Elastic Network Interfaces () ENIs angehängt sind. Die Regel ist NON_COMPLIANT, wenn die Sicherheitsgruppe keiner ENI zugeordnet ist. Sicherheitsgruppen, die nicht zu dem aufrufenden Konto gehören, werden als NOT_APPLICABLE bewertet.

> **Note**
>
> Diese Regel berichtet über den `AWS::EC2::SecurityGroup`-Ressourcentyp. Damit die Regel jedoch effektiv ausgeführt werden kann, müssen Sie die Aufzeichnung des `AWS::EC2::NetworkInterface`-Ressourcentyps aktivieren.

Kennung: _SECURITY_GROUP_ATTACHED_TO_ENI_PERIODIC EC2

Ressourcentypen: AWS::EC2::SecurityGroup

Auslösertyp: Regelmäßig

AWS-Region: Alle unterstützten AWS Regionen außer China (Peking), Asien-Pazifik (Thailand), Asien-Pazifik (Jakarta), Naher Osten (VAE), Asien-Pazifik (Hyderabad), Asien-Pazifik (Osaka), Asien-Pazifik (Malaysia), Asien-Pazifik (Melbourne), AWS GovCloud (USA-Ost), AWS GovCloud (US-West), Mexiko (Zentral), Israel (Tel Aviv), Kanada West (Calgary), Europa (Spanien), China (Ningxia), Europa (Region Zürich)

Parameter:

Keine

AWS CloudFormation Schablone

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

ec2- - spot-fleet-request-ct encryption-at-rest

Überprüft, ob Amazon EC2 Spot Fleet-Anfragen verschlüsselte Amazon Elastic Block Store (Amazon EBS) -Volumes für alle gestarteten EC2 Instances enthalten. Die Regel lautet NON_COMPLIANT, wenn eines der EBS-Volumes im Ruhezustand nicht verschlüsselt ist.

Kennung: _SPOT_FLEET_REQUEST_CT_ENCRYPTION_AT_REST EC2

Ressourcentypen: AWS::EC2::SpotFleet

Auslösertyp: Konfigurationsänderungen

AWS-Region: Nur in der Region Europa (Irland), USA Ost (Nord-Virginia), Asien-Pazifik (Seoul), USA West (Oregon), China (Ningxia), Europa (Zürich) verfügbar

Parameter:

Keine

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

ec2-stopped-instance

Überprüft, ob Amazon Elastic Compute Cloud (Amazon EC2) -Instances länger als die zulässige Anzahl von Tagen gestoppt wurden. Die Regel lautet NON_COMPLIANT, wenn der Status einer EC2 Amazon-Instance länger als die zulässige Anzahl von Tagen gestoppt wurde oder wenn der Zeitraum nicht bestimmt werden kann.

Kennung: _STOPPED_INSTANCE EC2

Ressourcentypen: AWS::EC2::Instance

Auslösertyp: Regelmäßig

AWS-Region: Alle unterstützten AWS Regionen außer Afrika (Kapstadt), Naher Osten (VAE), Asien-Pazifik (Osaka), Asien-Pazifik (Melbourne), Europa (Mailand), Kanada West (Calgary)

Parameter:

AllowedDays (Fakultativ), Typ: int, Standard: 30

Die Anzahl der Tage, an denen eine EC2 Amazon-Instance gestoppt werden kann, bevor die Regel NON_COMPLIANT ist. Die Standardanzahl von Tagen ist 30.

> **Note**
>
> Die ausgewählte Anzahl von Tagen muss unter der Anzahl von Tagen liegen, die als Aufbewahrungszeitraum konfiguriert ist, da diese Regel auf den erfassten Verlaufsdaten beruht. Weitere Informationen zur Aufbewahrung historischer Daten finden Sie unter Löschen von AWS Config Daten.

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

ec2- token-hop-limit-check

Prüft, ob die Metadaten einer Amazon Elastic Compute Cloud (EC2) -Instance über ein bestimmtes Token-Hop-Limit verfügen, das unter dem gewünschten Limit liegt. Die Regel ist für eine Instance NON_COMPLIANT, wenn ihr Hop-Limit-Wert über dem vorgesehenen Limit liegt.

Kennung: EC2 _TOKEN_HOP_LIMIT_CHECK

Ressourcentypen: AWS::EC2::Instance

Auslösertyp: Konfigurationsänderungen

AWS-Region: Alle unterstützten AWS Regionen außer China (Peking), Asien-Pazifik (Thailand), Asien-Pazifik (Jakarta), Naher Osten (VAE), Asien-Pazifik (Hyderabad), Asien-Pazifik (Malaysia), Asien-Pazifik (Melbourne), AWS GovCloud (US-Ost), AWS GovCloud (US-West), Mexiko (Zentral), Israel (Tel Aviv), Kanada West (Calgary), Europa (Spanien), China (Ningxia), Europa (Zürich)

Parameter:

tokenHopLimit (Fakultativ), Typ: int

Das gewünschte Token-Hop-Limit. Zulässig sind alle Werte zwischen 1 und 64, beide inklusive. Der Standardwert ist 1, falls dieser Parameter nicht angegeben ist.

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

ec2- traffic-mirror-filter-description

Prüft, ob Amazon EC2 Traffic Mirror-Filter eine Beschreibung haben. Die Regel ist NON_COMPLIANT, wenn Configuration.Description nicht existiert.

Kennung: EC2 _TRAFFIC_MIRROR_FILTER_DESCRIPTION

Ressourcentypen: AWS::EC2::TrafficMirrorFilter

Auslösertyp: Konfigurationsänderungen

AWS-Region: Alle unterstützten AWS Regionen außer China (Peking), Asien-Pazifik (Thailand), Asien-Pazifik (Malaysia), AWS GovCloud (USA-Ost), AWS GovCloud (US-West), Mexiko (Zentral), China (Ningxia)

Parameter:

Keine

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

ec2- traffic-mirror-filter-tagged

Prüft, ob Amazon EC2 Traffic Mirror-Filter Tags haben. Optional können Sie Tag-Schlüssel für die Regel angeben. Die Regel ist NON_COMPLIANT, wenn keine Tags vorhanden sind oder wenn die

angegebenen Tag-Schlüssel nicht vorhanden sind. Die Regel sucht nicht nach Tags, die mit 'aws: 'beginnen.

Kennung: EC2 _TRAFFIC_MIRROR_FILTER_TAGGED

Ressourcentypen: AWS::EC2::TrafficMirrorFilter

Auslösertyp: Konfigurationsänderungen

AWS-Region: Alle unterstützten AWS Regionen außer China (Peking), Asien-Pazifik (Thailand), Asien-Pazifik (Malaysia), AWS GovCloud (USA-Ost), AWS GovCloud (US-West), Mexiko (Zentral), China (Ningxia)

Parameter:

requiredKeyTags (Fakultativ), Typ: CSV

> Durch Kommas getrennte Liste von Tag-Schlüsseln, die von der Regel überprüft werden sollen. Falls angegeben, lautet die Regel NON_COMPLIANT, wenn die ausgewertete Ressource diese Schlüssel nicht enthält. Bei Tag-Schlüsseln wird die Groß- und Kleinschreibung beachtet. Tag-Schlüssel, die mit „aws:“ beginnen, sind nicht erlaubt.

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

ec2- traffic-mirror-session-description

Prüft, ob Amazon EC2 Traffic Mirror-Sitzungen eine Beschreibung haben. Die Regel ist NON_COMPLIANT, wenn Configuration.Description nicht existiert.

Kennung: EC2 _TRAFFIC_MIRROR_SESSION_DESCRIPTION

Ressourcentypen: AWS::EC2::TrafficMirrorSession

Auslösertyp: Konfigurationsänderungen

AWS-Region: Alle unterstützten AWS Regionen außer China (Peking), Asien-Pazifik (Thailand), Asien-Pazifik (Jakarta), Afrika (Kapstadt), Naher Osten (VAE), Asien-Pazifik (Hyderabad), Asien-Pazifik (Malaysia), Europa (Mailand), AWS GovCloud (USA-Ost), AWS GovCloud (US-West), Mexiko (Zentral), Israel (Tel Aviv), Kanada West (Calgary), Europa (Spanien), China (Ningxia)

Parameter:

Keine

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

ec2- traffic-mirror-session-tagged

Prüft, ob Amazon EC2 Traffic Mirror-Sitzungen Tags haben. Optional können Sie Tag-Schlüssel für die Regel angeben. Die Regel ist NON_COMPLIANT, wenn keine Tags vorhanden sind oder wenn die angegebenen Tag-Schlüssel nicht vorhanden sind. Die Regel sucht nicht nach Tags, die mit 'aws: 'beginnen.

Kennung: EC2 _TRAFFIC_MIRROR_SESSION_TAGGED

Ressourcentypen: AWS::EC2::TrafficMirrorSession

Auslösertyp: Konfigurationsänderungen

AWS-Region: Alle unterstützten AWS Regionen außer China (Peking), Asien-Pazifik (Thailand), Asien-Pazifik (Jakarta), Afrika (Kapstadt), Naher Osten (VAE), Asien-Pazifik (Hyderabad), Asien-Pazifik (Malaysia), Europa (Mailand), AWS GovCloud (USA-Ost), AWS GovCloud (US-West), Mexiko (Zentral), Israel (Tel Aviv), Kanada West (Calgary), Europa (Spanien), China (Ningxia)

Parameter:

requiredKeyTags (Fakultativ), Typ: CSV

> Durch Kommas getrennte Liste von Tag-Schlüsseln, die von der Regel überprüft werden sollen. Falls angegeben, lautet die Regel NON_COMPLIANT, wenn die ausgewertete Ressource diese Schlüssel nicht enthält. Bei Tag-Schlüsseln wird die Groß- und Kleinschreibung beachtet. Tag-Schlüssel, die mit „aws:“ beginnen, sind nicht erlaubt.

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

ec2- traffic-mirror-target-description

Prüft, ob Amazon EC2 Traffic Mirror-Ziele eine Beschreibung haben. Die Regel ist NON_COMPLIANT, wenn Configuration.Description nicht existiert.

Kennung: EC2 _TRAFFIC_MIRROR_TARGET_DESCRIPTION

Ressourcentypen: AWS::EC2::TrafficMirrorTarget

Auslösertyp: Konfigurationsänderungen

AWS-Region: Alle unterstützten AWS Regionen außer China (Peking), Asien-Pazifik (Thailand), Asien-Pazifik (Jakarta), Afrika (Kapstadt), Naher Osten (VAE), Asien-Pazifik (Hyderabad), Asien-Pazifik (Malaysia), AWS GovCloud (US-Ost), AWS GovCloud (US-West), Mexiko (Zentral), Israel (Tel Aviv), Kanada West (Calgary), Europa (Spanien), China (Ningxia)

Parameter:

Keine

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

ec2- traffic-mirror-target-tagged

Prüft, ob Amazon EC2 Traffic Mirror-Ziele Tags haben. Optional können Sie Tag-Schlüssel für die Regel angeben. Die Regel ist NON_COMPLIANT, wenn keine Tags vorhanden sind oder wenn die angegebenen Tag-Schlüssel nicht vorhanden sind. Die Regel sucht nicht nach Tags, die mit 'aws: 'beginnen.

Kennung: EC2 _TRAFFIC_MIRROR_TARGET_TAGGED

Ressourcentypen: AWS::EC2::TrafficMirrorTarget

Auslösertyp: Konfigurationsänderungen

AWS-Region: Alle unterstützten AWS Regionen außer China (Peking), Asien-Pazifik (Thailand), Asien-Pazifik (Jakarta), Afrika (Kapstadt), Naher Osten (VAE), Asien-Pazifik (Hyderabad), Asien-Pazifik (Malaysia), AWS GovCloud (US-Ost), AWS GovCloud (US-West), Mexiko (Zentral), Israel (Tel Aviv), Kanada West (Calgary), Europa (Spanien), China (Ningxia)

Parameter:

requiredKeyTags (Fakultativ), Typ: CSV

Durch Kommas getrennte Liste von Tag-Schlüsseln, die von der Regel überprüft werden sollen. Falls angegeben, lautet die Regel NON_COMPLIANT, wenn die ausgewertete Ressource diese Schlüssel nicht enthält. Bei Tag-Schlüsseln wird die Groß- und Kleinschreibung beachtet. Tag-Schlüssel, die mit „aws:“ beginnen, sind nicht erlaubt.

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

ec2- transit-gateway-auto-vpc -attach-deaktiviert

Prüft, ob Amazon Elastic Compute Cloud (Amazon EC2) Transit Gateways 'AutoAcceptSharedAttachments' aktiviert sind. Die Regel ist NON_COMPLIANT für ein Transit Gateway, wenn '' auf AutoAcceptSharedAttachments 'aktiviert' gesetzt ist.

Kennung: EC2 _TRANSIT_GATEWAY_AUTO_VPC_ATTACH_DISABLED

Ressourcentypen: AWS::EC2::TransitGateway

Auslösertyp: Konfigurationsänderungen

AWS-Region: Alle unterstützten AWS Regionen außer China (Peking), Asien-Pazifik (Thailand), Asien-Pazifik (Osaka), Asien-Pazifik (Malaysia), Asien-Pazifik (Melbourne), AWS GovCloud (USA-Ost), AWS GovCloud (US-West), Mexiko (Zentral), Israel (Tel Aviv), Kanada West (Calgary), China (Ningxia)

Parameter:

Keine

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

ec2- markiert transit-gateway-multicast-domain

Überprüft, ob Amazon EC2 Transit Gateway-Multicast-Domains Tags haben. Optional können Sie Tag-Schlüssel angeben. Die Regel lautet NON_COMPLIANT, wenn keine Tags vorhanden sind oder wenn die angegebenen Tag-Schlüssel nicht vorhanden sind. Die Regel sucht nicht nach Tags, die mit 'aws: 'beginnen.

Kennung: EC2 _TRANSIT_GATEWAY_MULTICAST_DOMAIN_TAGGED

Ressourcentypen: AWS::EC2::TransitGatewayMulticastDomain

Auslösertyp: Konfigurationsänderungen

AWS-Region: Alle unterstützten AWS Regionen außer China (Peking), Asien-Pazifik (Thailand), Asien-Pazifik (Malaysia), AWS GovCloud (USA-Ost), AWS GovCloud (US-West), Mexiko (Zentral), China (Ningxia)

Parameter:

requiredKeyTags (Fakultativ), Typ: CSV

> Durch Kommas getrennte Liste von Tag-Schlüsseln, die von der Regel überprüft werden sollen. Falls angegeben, lautet die Regel NON_COMPLIANT, wenn die ausgewertete Ressource diese Schlüssel nicht enthält. Bei Tag-Schlüsseln wird die Groß- und Kleinschreibung beachtet. Tag-Schlüssel, die mit „aws:“ beginnen, sind nicht erlaubt.

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

ec2- volume-inuse-check

Prüft, ob EBS-Volumes an Instances angehängt sind. EC2 Optional wird überprüft, ob EBS-Volumes zum Löschen gekennzeichnet werden, wenn eine Instance beendet wurde.

Die Regel ist KONFORM, wenn ein EBS-Volume an eine laufende EC2 Instance angehängt ist. In diesem Fall ist sie KONFORM, wenn das EBS-Volume aktiv von einer EC2 Instance verwendet wird.

Die Regel lautet NON_COMPLIANT, wenn ein EBS-Volume keiner EC2 Instance oder einer gestoppten oder beendeten Instance angehängt ist. EC2 In diesem Fall lautet sie NON_COMPLIANT, wenn das EBS-Volume nicht aktiv von einer Instance verwendet wird. EC2

Kennung: _VOLUME_INUSE_CHECK EC2

Ressourcentypen: AWS::EC2::Volume

Auslösertyp: Konfigurationsänderungen

AWS-Region: Alle unterstützten AWS Regionen außer Asien-Pazifik (Taipeh) und Kanada West (Calgary)

Parameter:

deleteOnTermination (Fakultativ), Typ: Boolesch

> EBS-Volumes werden zum Löschen gekennzeichnet, wenn eine Instance beendet wurde. Mögliche Werte: „True“ oder „False“ (andere Eingabewerte werden als NON_COMPLIANT gekennzeichnet). Bei `True` ist die Regel NON_COMPLIANT, wenn ein beendetes EBS-Volume nicht zum Löschen markiert ist.

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

ec2- vpn-connection-logging-enabled

Prüft, ob bei AWS Site-to-Site VPN-Verbindungen die CloudWatch Amazon-Protokollierung für beide Tunnel aktiviert ist. Die Regel lautet NON_COMPLIANT, wenn bei einer Site-to-Site VPN-Verbindung die CloudWatch Protokollierung nicht für einen oder beide Tunnel aktiviert ist.

Kennung: _VPN_CONNECTION_LOGGING_ENABLED EC2

Ressourcentypen: AWS::EC2::VPNConnection

Auslösertyp: Konfigurationsänderungen

AWS-Region: Alle unterstützten AWS Regionen außer China (Peking), Asien-Pazifik (Thailand), Asien-Pazifik (Malaysia), Mexiko (Zentral), Kanada West (Calgary), China (Ningxia)

Parameter:

Keine

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

ecr-private-image-scanning-aktiviert

Prüft, ob in einem privaten Amazon Elastic Container Registry (Amazon ECR)-Repository das Scannen von Images aktiviert ist. Die Regel ist NON_COMPLIANT, wenn die Scan-Frequenz des privaten Amazon-ECR-Repositorys nicht auf „Push-Scan“ oder „Kontinuierlicher Scan“ eingestellt ist. Weitere Informationen zur Aktivierung des Bildscannens finden Sie unter Scannen von Bildern im Amazon ECR-Benutzerhandbuch.

ID: ECR_PRIVATE_IMAGE_SCANNING_ENABLED

Ressourcentypen: AWS::ECR::Repository

Auslösertyp: Regelmäßig

AWS-Region: Alle unterstützten AWS Regionen außer China (Peking), Asien-Pazifik (Thailand), Asien-Pazifik (Malaysia), Mexiko (Zentral), Kanada West (Calgary), China (Ningxia)

Parameter:

Keine

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

ecr-private-lifecycle-policy-konfiguriert

Prüft, ob für ein privates Amazon Elastic Container Registry (ECR)-Repository mindestens eine Lebenszyklus-Richtlinie konfiguriert wurde. Die Regel ist NON_COMPLIANT, wenn keine Lebenszyklus-Richtlinie für das private ECR-Repository konfiguriert ist.

ID: ECR_PRIVATE_LIFECYCLE_POLICY_CONFIGURED

Ressourcentypen: AWS::ECR::Repository

Auslösertyp: Konfigurationsänderungen

AWS-Region: Alle unterstützten AWS Regionen außer Asien-Pazifik (Thailand), Asien-Pazifik (Malaysia), Mexiko (Zentral), Israel (Tel Aviv) und Kanada West (Calgary)

Parameter:

Keine

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

ecr-private-tag-immutability-aktiviert

Prüft, ob für ein privates Amazon Elastic Container Registry (ECR)-Repository die Unveränderlichkeit von Tags aktiviert ist. Diese Regel ist NON_COMPLIANT, wenn die Unveränderlichkeit von Tags für das private ECR-Repository nicht aktiviert ist.

ID: ECR_PRIVATE_TAG_IMMUTABILITY_ENABLED

Ressourcentypen: AWS::ECR::Repository

Auslösertyp: Konfigurationsänderungen

AWS-Region: Alle unterstützten AWS Regionen außer Asien-Pazifik (Thailand), Asien-Pazifik (Malaysia), Mexiko (Zentral), Israel (Tel Aviv) und Kanada West (Calgary)

Parameter:

Keine

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

ecr-repository-cmk-encryption-aktiviert

Überprüft, ob das ECR-Repository im Ruhezustand mit einem vom Kunden verwalteten KMS-Schlüssel verschlüsselt ist. Diese Regel ist NON_COMPLIANT, wenn das Repository mit AES256 oder dem Standard-KMS-Schlüssel ('aws/ecr') verschlüsselt ist.

Kennung: ECR_REPOSITORY_CMK_ENCRYPTION_ENABLED

Ressourcentypen: AWS::ECR::Repository

Auslösertyp: Konfigurationsänderungen

AWS-Region: Alle unterstützten AWS Regionen außer Naher Osten (Bahrain), Asien-Pazifik (Thailand), Asien-Pazifik (Malaysia), Mexiko (Zentral), Israel (Tel Aviv) und Kanada West (Calgary)

Parameter:

kmsKeyArns (Fakultativ), Typ: CSV

Durch Kommas getrennte Liste der KMS-Schlüssel Amazon Resource Names (ARNs), die das ECR-Repository verschlüsseln sollen.

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

ecr-repository-tagged

Prüft, ob Amazon ECR-Repositorys Tags haben. Optional können Sie Tag-Schlüssel angeben. Die Regel lautet NON_COMPLIANT, wenn keine Tags vorhanden sind oder wenn die angegebenen Tag-Schlüssel nicht vorhanden sind. Die Regel sucht nicht nach Tags, die mit 'aws: 'beginnen.

Kennung: ECR_REPOSITORY_TAGGED

Ressourcentypen: AWS::ECR::Repository

Auslösertyp: Konfigurationsänderungen

AWS-Region: Alle unterstützten AWS Regionen außer China (Peking), Asien-Pazifik (Thailand), Asien-Pazifik (Malaysia), AWS GovCloud (USA-Ost), AWS GovCloud (US-West), Mexiko (Zentral), China (Ningxia)

Parameter:

requiredKeyTags (Fakultativ), Typ: CSV

Durch Kommas getrennte Liste von Tag-Schlüsseln, die von der Regel überprüft werden sollen. Falls angegeben, lautet die Regel NON_COMPLIANT, wenn die ausgewertete Ressource diese

Schlüssel nicht enthält. Bei Tag-Schlüsseln wird die Groß- und Kleinschreibung beachtet. Tag-Schlüssel, die mit „aws:“ beginnen, sind nicht erlaubt.

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

ecs-awsvpc-networking-enabled

Prüft, ob der Netzwerkmodus für aktive ECSTask Definitionen auf 'awsvpc' gesetzt ist. Diese Regel ist NON_COMPLIANT, wenn aktive ECSTask Definitionen nicht auf 'awsvpc' gesetzt sind.

> **Note**
>
> Diese Regel bewertet nur die letzte aktive Revision einer Amazon-ECS-Aufgabendefinition.

KennungAWSVPC_NETWORKING: ECS_ _ENABLED

Ressourcentypen: AWS::ECS::TaskDefinition

Auslösertyp: Konfigurationsänderungen

AWS-Region: Alle unterstützten AWS Regionen außer China (Peking), Asien-Pazifik (Thailand), Asien-Pazifik (Jakarta), Naher Osten (VAE), Asien-Pazifik (Hyderabad), Asien-Pazifik (Osaka), Asien-Pazifik (Malaysia), Asien-Pazifik (Melbourne), AWS GovCloud (USA-Ost), AWS GovCloud (US-West), Mexiko (Zentral), Israel (Tel Aviv), Kanada West (Calgary), Europa (Spanien), China (Ningxia), Europa (Region Zürich)

Parameter:

Keine

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

ecs-containers-nonprivileged

Prüft, ob der privilegierte Parameter in der Containerdefinition von ECSTask Definitions auf „true“ gesetzt ist. Die Regel ist NON_COMPLIANT, wenn der privilegierte Parameter „True“ ist.

> **Note**
>
> Diese Regel bewertet nur die letzte aktive Revision einer Amazon-ECS-Aufgabendefinition.

ID: ECS_CONTAINERS_NONPRIVILEGED

Ressourcentypen: AWS::ECS::TaskDefinition

Auslösertyp: Konfigurationsänderungen

AWS-Region: Alle unterstützten AWS Regionen außer Asien-Pazifik (Thailand), Asien-Pazifik (Malaysia), Mexiko (Zentral) und Kanada West (Calgary)

Parameter:

Keine

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

ecs-containers-readonly-access

Prüft, ob Amazon Elastic Container Service (Amazon ECS)-Container nur Lesezugriff auf ihre Root-Dateisysteme haben. Die Regel ist NON_COMPLIANT, wenn der readonlyRootFilesystem Parameter in der Containerdefinition von Definitions auf 'false' gesetzt ist. ECSTask

> **Note**
>
> Diese Regel bewertet nur die letzte aktive Revision einer Amazon-ECS-Aufgabendefinition.

ID: ECS_CONTAINERS_READONLY_ACCESS

Ressourcentypen: AWS::ECS::TaskDefinition

Auslösertyp: Konfigurationsänderungen

AWS-Region: Alle unterstützten AWS Regionen außer Asien-Pazifik (Thailand), Asien-Pazifik (Malaysia), Mexiko (Zentral) und Kanada West (Calgary)

Parameter:

Keine

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

ecs-container-insights-enabled

Prüft, ob Container Insights für Amazon Elastic Container Service-Cluster aktiviert sind. Die Regel ist NON_COMPLIANT, wenn Container Insights nicht aktiviert sind.

ID: ECS_CONTAINER_INSIGHTS_ENABLED

Ressourcentypen: AWS::ECS::Cluster

Auslösertyp: Konfigurationsänderungen

AWS-Region: Alle unterstützten AWS Regionen außer Asien-Pazifik (Thailand), Asien-Pazifik (Malaysia), Mexiko (Zentral) und Kanada West (Calgary)

Parameter:

Keine

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

ecs-fargate-latest-platform-Ausführung

Prüft, ob die ECS-Fargate-Services auf die neueste Plattformversion festgelegt sind. Die Regel lautet NON_COMPLIANT, wenn der Starttyp PlatformVersion für Fargate nicht auf LATEST

gesetzt ist oder wenn latestLinuxVersion weder der Starttyp noch als Parameter angegeben `latestWindowsVersion` wurden.

ID: ECS_FARGATE_LATEST_PLATFORM_VERSION

Ressourcentypen: AWS::ECS::Service

Auslösertyp: Konfigurationsänderungen

AWS-Region: Alle unterstützten AWS Regionen außer Asien-Pazifik (Thailand), Asien-Pazifik (Malaysia), Mexiko (Zentral) und Kanada West (Calgary)

Parameter:

latestLinuxVersion (Fakultativ), Typ: Zeichenfolge

> Die neueste Version von Linux unterstützt PlatformVersion " im Format Semantic Versioning (SemVer). Der Parameter ist möglicherweise erforderlich, wenn Fargate bereitgestellt wurde und das PlatformVersion " explizit angegeben wurde oder als " DeploymentController verwendet CodeDeploy wird

latestWindowsVersion (Fakultativ), Typ: Zeichenfolge

> Die neueste Version von Windows unterstützt PlatformVersion " im Format Semantic Versioning (SemVer). Der Parameter ist möglicherweise erforderlich, wenn Fargate bereitgestellt wurde und das PlatformVersion " explizit angegeben wurde oder als " DeploymentController verwendet CodeDeploy wird

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

ecs-no-environment-secrets

Prüft, ob Geheimnisse als Container-Umgebungsvariablen übergeben werden. Die Regel ist NON_COMPLIANT, wenn ein oder mehrere Umgebungsvariablenschlüssel mit einem Schlüssel übereinstimmen, der im Parameter „`secretKeys`“ aufgeführt ist (ausgenommen Umgebungsvariablen von anderen Speicherorten wie Amazon S3).

> **Note**
>
> Diese Regel bewertet nur die letzte aktive Revision einer Amazon-ECS-Aufgabendefinition.

ID: ECS_NO_ENVIRONMENT_SECRETS

Ressourcentypen: AWS::ECS::TaskDefinition

Auslösertyp: Konfigurationsänderungen

AWS-Region: Alle unterstützten AWS Regionen außer Asien-Pazifik (Thailand), Asien-Pazifik (Malaysia), AWS GovCloud (USA-Ost), AWS GovCloud (US-West), Mexiko (Zentral), Kanada West (Calgary)

Parameter:

secretKeys, Typ: CSV

Durch Kommata getrennte Liste von Schlüsselnamen, nach denen in den Umgebungsvariablen von Containerdefinitionen innerhalb von Aufgabendefinitionen gesucht werden soll. Zusätzliche Leerzeichen werden entfernt.

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

ecs-task-definition-log-Konfiguration

Prüft, ob die Protokollkonfiguration für aktive ECS-Aufgabendefinitionen festgelegt ist. Diese Regel ist NON_COMPLIANT, wenn für eine aktive ECSTask Definition die LogConfiguration-Ressource nicht definiert ist oder der Wert für LogConfiguration in mindestens einer Containerdefinition Null ist.

> **Note**
>
> Diese Regel bewertet nur die letzte aktive Revision einer Amazon-ECS-Aufgabendefinition.

ID: ECS_TASK_DEFINITION_LOG_CONFIGURATION

Ressourcentypen: AWS::ECS::TaskDefinition

Auslösertyp: Konfigurationsänderungen

AWS-Region: Alle unterstützten AWS Regionen außer Asien-Pazifik (Thailand), Asien-Pazifik (Malaysia), AWS GovCloud (USA-Ost), AWS GovCloud (US-West), Mexiko (Zentral), Kanada West (Calgary)

Parameter:

Keine

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

ecs-task-definition-memory-hartes Limit

Überprüft, ob Amazon Elastic Container Service (ECS)-Aufgabendefinitionen ein festgelegtes Speicherlimit für ihre Containerdefinitionen haben. Die Regel ist NON_COMPLIANT für eine Aufgabendefinition, wenn der Parameter „Arbeitsspeicher“ für eine Containerdefinition fehlt.

> **Note**
>
> Diese Regel bewertet nur die letzte aktive Revision einer Amazon-ECS-Aufgabendefinition.

ID: ECS_TASK_DEFINITION_MEMORY_HARD_LIMIT

Ressourcentypen: AWS::ECS::TaskDefinition

Auslösertyp: Konfigurationsänderungen

AWS-Region: Alle unterstützten AWS Regionen außer China (Peking), Asien-Pazifik (Thailand), Asien-Pazifik (Jakarta), Naher Osten (VAE), Asien-Pazifik (Hyderabad), Asien-Pazifik (Osaka), Asien-Pazifik (Malaysia), Asien-Pazifik (Melbourne), AWS GovCloud (USA-Ost), AWS GovCloud (US-West), Mexiko (Zentral), Israel (Tel Aviv), Kanada West (Calgary), Europa (Spanien), China (Ningxia), Europa (Region Zürich)

Parameter:

Keine

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

ecs-task-definition-network-mode-not-host

Prüft, ob die neueste aktive Version der Amazon ECS-Aufgabendefinitionen den Host-Netzwerkmodus verwendet. Die Regel lautet NON_COMPLIANT, wenn die letzte aktive Revision der ECS-Aufgabendefinition den Host-Netzwerkmodus verwendet.

Kennung: ECS_TASK_DEFINITION_NETWORK_MODE_NOT_HOST

Ressourcentypen: AWS::ECS::TaskDefinition

Auslösertyp: Konfigurationsänderungen

AWS-Region: Alle unterstützten AWS Regionen außer Naher Osten (Bahrain), Asien-Pazifik (Thailand) und Mexiko (Zentral)

Parameter:

Keine

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

ecs-task-definition-nonroot-benutzer

Prüft, ob ECSTask Definitionen einen Benutzer angeben, auf dem Container vom EC2 Starttyp Amazon Elastic Container Service (Amazon ECS) ausgeführt werden sollen. Die Regel ist NON_COMPLIANT, wenn der Parameter „Benutzer“ nicht vorhanden oder auf „Stamm“ festgelegt ist.

> **Note**
>
> Diese Regel bewertet nur die letzte aktive Revision einer Amazon-ECS-Aufgabendefinition.

ID: ECS_TASK_DEFINITION_NONROOT_USER

Ressourcentypen: AWS::ECS::TaskDefinition

Auslösertyp: Konfigurationsänderungen

AWS-Region: Alle unterstützten AWS Regionen außer China (Peking), Asien-Pazifik (Thailand), Asien-Pazifik (Jakarta), Naher Osten (VAE), Asien-Pazifik (Hyderabad), Asien-Pazifik (Osaka), Asien-Pazifik (Malaysia), Asien-Pazifik (Melbourne), AWS GovCloud (USA-Ost), AWS GovCloud (US-West), Mexiko (Zentral), Israel (Tel Aviv), Kanada West (Calgary), Europa (Spanien), China (Ningxia), Europa (Region Zürich)

Parameter:

Keine

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

ecs-task-definition-pid-Modusprüfung

Prüft, ob ECSTask Definitionen so konfiguriert sind, dass sie den Prozess-Namespace eines Hosts mit seinen Amazon Elastic Container Service (Amazon ECS) -Containern gemeinsam nutzen. Die Regel lautet NON_COMPLIANT, wenn der Parameter „pidMode“ auf „host“ festgelegt ist.

> **Note**
>
> Diese Regel bewertet nur die letzte aktive Revision einer Amazon-ECS-Aufgabendefinition.

ID: ECS_TASK_DEFINITION_PID_MODE_CHECK

Ressourcentypen: AWS::ECS::TaskDefinition

Auslösertyp: Konfigurationsänderungen

AWS-Region: Alle unterstützten AWS Regionen außer Asien-Pazifik (Thailand), Asien-Pazifik (Malaysia), AWS GovCloud (USA-Ost), AWS GovCloud (US-West), Mexiko (Zentral), Kanada West (Calgary)

Parameter:

Keine

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

ecs-task-definition-user-for-host-mode-check

Prüft, ob Amazon ECS-Aufgabendefinitionen mit Host-Netzwerkmodus in der Container-Definition privilegiert ODER non-root enthalten. Die Regel lautet NON_COMPLIANT, wenn die letzte aktive Revision einer Aufgabendefinition den Wert privileged=false (oder null) UND user=root (oder null) hat.

> **Important**
>
> Es muss nur eine Bedingung erfüllt sein, damit die Regel wieder konform ist
> Die Regel ist in jedem der folgenden Szenarien KONFORM:
>
> - Wenn der Netzwerkmodus nicht auf Host eingestellt ist,
> - Wenn die letzte aktive Revision einer Aufgabendefinition den Wert privileged=true hat,
> - Wenn die letzte aktive Version einer Aufgabendefinition einen Benutzer hat, der nicht der Stammbenutzer ist.
>
> Das bedeutet, dass nur eine dieser Bedingungen erfüllt sein muss, damit die Regel wieder konform ist. Um genau zu überprüfen, ob eine Aufgabendefinition den Wert privileged=true hat, finden Sie unter. ecs-containers-nonprivileged Um genau zu überprüfen, ob eine Aufgabendefinition einen Benutzer hat, der nicht der Root-Benutzer ist, finden Sie unter -user. ecs-task-definition-nonroot

ID: ECS_TASK_DEFINITION_USER_FOR_HOST_MODE_CHECK

Ressourcentypen: AWS::ECS::TaskDefinition

Auslösertyp: Konfigurationsänderungen

AWS-Region: Alle unterstützten AWS Regionen außer Naher Osten (VAE) und Asien-Pazifik (Taipeh)

Parameter:

SkipInactiveTaskDefinitions (Fakultativ), Typ: Boolesch

Boolesche Markierung, um INAKTIVE EC2 Amazon-Aufgabendefinitionen nicht zu überprüfen. Wenn sie auf „true“ gesetzt ist, bewertet die Regel keine INAKTIVEN EC2 Amazon-Aufgabendefinitionen. Wenn der Wert auf „falsch“ gesetzt ist, bewertet die Regel die neueste Version der INAKTIVEN EC2 Amazon-Aufgabendefinitionen.

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

efs-access-point-enforce-root-Verzeichnis

Prüft, ob Amazon Elastic File System (Amazon EFS)-Zugriffspunkte so konfiguriert sind, dass ein Stammverzeichnis erzwungen wird. Die Regel ist NON_COMPLIANT, wenn der Wert für „Pfad“ auf „/“ (Standard-Stammverzeichnis des Dateisystems) festgelegt ist.

ID: EFS_ACCESS_POINT_ENFORCE_ROOT_DIRECTORY

Ressourcentypen: AWS::EFS::AccessPoint

Auslösertyp: Konfigurationsänderungen

AWS-Region: Alle unterstützten AWS Regionen außer Asien-Pazifik (Thailand), Asien-Pazifik (Malaysia), AWS GovCloud (USA-Ost), AWS GovCloud (US-West), Mexiko (Zentral), Israel (Tel Aviv), Kanada West (Calgary), China (Ningxia)

Parameter:

approvedDirectories (optional), Typ: CSV

Durch Kommata getrennte Liste der Unterverzeichnispfade, die für die Durchsetzung des Stammverzeichnisses von Amazon-EFS-Zugriffspunkten zugelassen sind.

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

efs-access-point-enforce-Benutzeridentität

Prüft, ob Amazon Elastic File System (Amazon EFS)-Zugriffspunkte so konfiguriert sind, dass eine Benutzeridentität erzwungen wird. Die Regel ist NON_COMPLIANT, wenn PosixUser " nicht definiert ist oder wenn Parameter angegeben werden und der entsprechende Parameter keine Übereinstimmung enthält.

ID: EFS_ACCESS_POINT_ENFORCE_USER_IDENTITY

Ressourcentypen: AWS::EFS::AccessPoint

Auslösertyp: Konfigurationsänderungen

AWS-Region: Alle unterstützten AWS Regionen außer Asien-Pazifik (Thailand), Asien-Pazifik (Malaysia), Mexiko (Zentral), Israel (Tel Aviv), Kanada West (Calgary), China (Ningxia)

Parameter:

approvedUids (optional), Typ: CSV

Durch Kommata getrennte Liste der POSIX-Benutzer-IDs, die für die Durchsetzung von EFS-Zugriffspunkt-Benutzern zugelassen sind.

approvedGids (optional), Typ: CSV

Durch Kommas getrennte Liste von POSIX-Gruppen IDs , die für die Benutzerdurchsetzung von EFS Access Points zugelassen sind.

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

efs-automatic-backups-enabled

Prüft, ob für ein Amazon Elastic File System (Amazon EFS) -Dateisystem automatische Backups aktiviert sind. Die Regel ist NON_COMPLIANT, wenn `BackupPolicy.Status` auf DISABLED gesetzt ist.

Kennung: EFS_AUTOMATIC_BACKUPS_ENABLED

Ressourcentypen: AWS::EFS::FileSystem

Auslösertyp: Konfigurationsänderungen

AWS-Region: Alle unterstützten AWS Regionen außer Asien-Pazifik (Thailand), Asien-Pazifik (Malaysia), Mexiko (Zentral) und Kanada West (Calgary)

Parameter:

Keine

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

efs-encrypted-check

Prüft, ob Amazon Elastic File System (Amazon EFS) so konfiguriert ist, dass es die Dateidaten mit AWS Key Management Service (AWS KMS) verschlüsselt. Die Regel ist NON_COMPLIANT, wenn der verschlüsselte Schlüssel für `DescribeFileSystems` auf „false“ festgelegt ist, oder wenn der `KmsKeyId`-Schlüssel in `DescribeFileSystems` nicht mit dem `KmsKeyId`-Parameter übereinstimmt.

ID: EFS_ENCRYPTED_CHECK

Ressourcentypen: AWS::EFS::FileSystem

Auslösertyp: Regelmäßig

AWS-Region: Alle unterstützten AWS Regionen außer der Region Asien-Pazifik (Taipeh)

Parameter:

KmsKeyId (Fakultativ), Typ: Zeichenfolge

> Amazon-Ressourcenname (ARN) des KMS-Schlüssels, mit dem das EFS-Dateisystem verschlüsselt wird.

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

efs-filesystem-ct-encrypted

Überprüft, ob Amazon Elastic File System (Amazon EFS) Daten mit AWS Key Management Service (AWS KMS) verschlüsselt. Die Regel lautet NON_COMPLIANT, wenn ein Dateisystem nicht verschlüsselt ist. Optional können Sie überprüfen, ob ein Dateisystem nicht mit bestimmten KMS-Schlüsseln verschlüsselt ist.

Kennung: EFS_FILESYSTEM_CT_ENCRYPTED

Ressourcentypen: AWS::EFS::FileSystem

Auslösertyp: Konfigurationsänderungen

AWS-Region: Alle unterstützten AWS Regionen außer Asien-Pazifik (Thailand), Asien-Pazifik (Malaysia), Mexiko (Zentral), Israel (Tel Aviv) und Kanada West (Calgary)

Parameter:

kmsKeyArns (Fakultativ), Typ: Zeichenfolge

> (Optional) Durch Kommas getrennte Liste von Amazon-Ressourcennamen (ARNs) für AWS KMS-Schlüssel. Falls angegeben, prüft die Regel, ob die angegebenen KMS-Schlüssel ein Amazon EFS-Dateisystem nicht verschlüsseln.

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

efs-in-backup-plan

Prüft, ob Amazon Elastic File System (Amazon EFS) -Dateisysteme zu den Backup-Plänen von AWS Backup hinzugefügt wurden. Die Regel ist NON_COMPLIANT, wenn EFS-Dateisysteme nicht in den Backup-Plänen enthalten sind.

ID: EFS_IN_BACKUP_PLAN

Ressourcentypen: AWS::EFS::FileSystem

Auslösertyp: Regelmäßig

AWS-Region: Alle unterstützten AWS Regionen außer der Region Asien-Pazifik (Taipeh)

Parameter:

Keine

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

efs-last-backup-recovery-Punkt-erstellt

Prüft, ob für Amazon Elastic File System (Amazon EFS)-Dateisysteme ein Wiederherstellungspunkt erstellt wurde. Die Regel ist NON_COMPLIANT, wenn für das Amazon-EFS-Dateisystem innerhalb des angegebenen Zeitraums kein entsprechender Wiederherstellungspunkt erstellt wurde.

ID: EFS_LAST_BACKUP_RECOVERY_POINT_CREATED

Ressourcentypen: AWS::EFS::FileSystem

Auslösertyp: Regelmäßig

AWS-Region: Alle unterstützten AWS Regionen außer China (Peking), Asien-Pazifik (Thailand), Asien-Pazifik (Malaysia), Mexiko (Zentral), Israel (Tel Aviv), Kanada West (Calgary), China (Ningxia)

Parameter:

resourceTags (optional), Typ: Zeichenfolge

Tags von Amazon-EFS-Dateisystemen, die von der Regel geprüft werden sollen, im JSON-Format `{"tagkey" : "tagValue"}`.

resourceId (optional), Typ: Zeichenfolge

ID des EFS-Dateisystems, das von der Regel geprüft werden soll.

recoveryPointAgeWert (optional), Typ: int, Standard: 1

Numerischer Wert für das zulässige Höchstalter. Nicht mehr als 744 für Stunden oder 31 für Tage.

recoveryPointAgeEinheit (optional), Typ: Zeichenfolge, Standard: days

Zeiteinheit für das zulässige Höchstalter. Zulässige Werte: „Stunden“, „Tage“.

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

efs-meets-restore-time-ziel

Prüft, ob die Wiederherstellungszeit von Amazon Elastic File System (Amazon EFS)-Dateisystemen der angegebenen Dauer entspricht. Die Regel lautet NON_COMPLIANT, wenn LatestRestoreExecutionTimeMinutes ein Amazon EFS-Dateisystem länger als maxRestoreTime Minuten ist.

Kennung: EFS_MEETS_RESTORE_TIME_TARGET

Ressourcentypen: AWS::EFS::FileSystem

Auslösertyp: Regelmäßig

AWS-Region: Alle unterstützten AWS Regionen außer China (Peking), Asien-Pazifik (Thailand), Asien-Pazifik (Malaysia), AWS GovCloud (USA-Ost), AWS GovCloud (US-West), Mexiko (Zentral), Israel (Tel Aviv), Kanada West (Calgary), China (Ningxia)

Parameter:

maxRestoreTime, Typ: int

Numerischer Wert für die maximal zulässige Wiederherstellungslaufzeit.

resourceTags (optional), Typ: Zeichenfolge

Tags von Amazon-EFS-Dateisystemen, die von der Regel geprüft werden sollen, im JSON-Format.

resourceId (optional), Typ: Zeichenfolge

ID des EFS-Dateisystems, das von der Regel geprüft werden soll.

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

efs-mount-target-public-zugänglich

Überprüft, ob ein Amazon Elastic File System (Amazon EFS) -Mount-Ziel keinem öffentlichen Subnetz zugeordnet ist. Die Regel ist NICHT KONFORM, wenn das Amazon EFS-Mount-Ziel einem öffentlichen Subnetz zugeordnet ist.

Kennung: EFS_MOUNT_TARGET_PUBLIC_ACCESSIBLE

Ressourcentypen: AWS::EFS::FileSystem

Auslösertyp: Regelmäßig

AWS-Region: Alle unterstützten AWS Regionen außer China (Peking), Asien-Pazifik (Thailand), Asien-Pazifik (Malaysia), Mexiko (Zentral), Kanada West (Calgary), China (Ningxia)

Parameter:

Keine

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

efs-resources-in-logically-air-gapped-vault

Überprüft, ob sich die Dateisysteme von Amazon Elastic File System (Amazon EFS) in einem Tresor mit logischem Air-Gap befinden. Die Regel lautet NON_COMPLIANT, wenn sich ein Amazon EFS-Dateisystem innerhalb des angegebenen Zeitraums nicht in einem Tresor mit logischem Air-Gap befindet.

Kennung: EFS_RESOURCES_IN_LOGICALLY_AIR_GAPPED_VAULT

Ressourcentypen: AWS::EFS::FileSystem

Auslösertyp: Regelmäßig

AWS-Region: Alle unterstützten AWS Regionen außer China (Peking), Asien-Pazifik (Thailand), Asien-Pazifik (Malaysia), AWS GovCloud (USA-Ost), AWS GovCloud (US-West), Mexiko (Zentral), Israel (Tel Aviv), Kanada West (Calgary), China (Ningxia)

Parameter:

resourceTags (optional), Typ: Zeichenfolge

Tags von Amazon-EFS-Dateisystemen, die von der Regel geprüft werden sollen, im JSON-Format.

resourceId (optional), Typ: Zeichenfolge

ID des EFS-Dateisystems, das von der Regel geprüft werden soll.

recoveryPointAgeWert (optional), Typ: int, Standard: 1

Numerischer Wert für das zulässige Höchstalter. Nicht mehr als 2184 für Stunden, 91 für Tage.

recoveryPointAgeEinheit (optional), Typ: Zeichenfolge, Standard: days

Zeiteinheit für das zulässige Höchstalter. Zulässige Werte: „Stunden“, „Tage“.

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

efs-resources-protected-by-Backup-Plan

Prüft, ob Amazon Elastic File System (Amazon EFS)-Dateisysteme durch einen Backup-Plan geschützt sind. Die Regel ist NON_COMPLIANT, wenn das EFS-Dateisystem nicht durch einen Backup-Plan gedeckt ist.

ID: EFS_RESOURCES_PROTECTED_BY_BACKUP_PLAN

Ressourcentypen: AWS::EFS::FileSystem

Auslösertyp: Regelmäßig

AWS-Region: Alle unterstützten AWS Regionen außer China (Peking), Asien-Pazifik (Thailand), Asien-Pazifik (Malaysia), Mexiko (Zentral), Israel (Tel Aviv), Kanada West (Calgary), China (Ningxia)

Parameter:

resourceTags (optional), Typ: Zeichenfolge

Tags von EFS-Dateisystemen, die von der Regel geprüft werden sollen, im JSON-Format `{"tagkey" : "tagValue"}`.

resourceId (optional), Typ: Zeichenfolge

ID des EFS-Dateisystems, das von der Regel geprüft werden soll.

crossRegionList (Fakultativ), Typ: Zeichenfolge

Durch Kommata getrennte Liste der Zielregionen, für die die regionsübergreifende Backup-Kopie aufbewahrt werden soll.

crossAccountList (Fakultativ), Typ: Zeichenfolge

Durch Kommata getrennte Liste der Zielkonten, für die die kontoübergreifende Backup-Kopie aufbewahrt werden soll.

maxRetentionDays (Fakultativ), Typ: int

Die maximale Aufbewahrungsdauer in Tagen für die Backup-Tresorsperre.

minRetentionDays (Fakultativ), Typ: int

Die Mindestaufbewahrungsdauer in Tagen für die Backup-Tresorsperre.

backupVaultLockÜberprüfen Sie (fakultativ), Typ: Zeichenfolge

Akzeptierte Werte: „True“ oder „False“. Geben Sie „True“ ein, damit die Regel prüft, ob die Ressource in einem gesperrten Tresor gesichert ist.

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

eip-attached

Überprüft, ob alle Elastic IP-Adressen, die einem AWS Konto zugewiesen sind, mit EC2 Instances oder verwendeten Elastic Network-Schnittstellen verknüpft sind. Die Regel lautet NON_COMPLIANT, wenn 'AssociationId' für die Elastic IP-Adresse Null ist.

> **Note**
>
> Es kann nach erfolgter Auswertung bis zu 6 Stunden dauern, bis Ergebnisse verfügbar sind.

ID: EIP_ATTACHED

Ressourcentypen: AWS::EC2::EIP

Auslösertyp: Konfigurationsänderungen

AWS-Region: Alle unterstützten AWS Regionen außer der Region Naher Osten (VAE)

Parameter:

Keine

Proaktive Auswertung

Anweisungen zur Ausführung dieser Regel im proaktiven Modus finden Sie unter Evaluieren Ihrer Ressourcen mithilfe von AWS Config Regeln. Damit diese Regel im proaktiven Modus COMPLIANT zurückgibt, muss das Ressourcenkonfigurationsschema für die StartResourceEvaluationAPI die folgenden Eingaben enthalten, die als Zeichenfolge kodiert sind:

```
"ResourceConfiguration":
...
{
   "InstanceId": "my-instance-Id"
}
...
```

Weitere Informationen zur proaktiven Auswertung finden Sie unter Auswertungsmodus.

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

eks-cluster-logging-enabled

Prüft, ob ein Amazon Elastic Kubernetes Service (Amazon EKS)-Cluster mit aktivierter Protokollierung konfiguriert ist. Die Regel ist NON_COMPLIANT, wenn die Protokollierung für Amazon-EKS-Cluster nicht für alle Protokolltypen aktiviert ist.

ID: EKS_CLUSTER_LOGGING_ENABLED

Ressourcentypen: AWS::EKS::Cluster

Auslösertyp: Regelmäßig

AWS-Region: Alle unterstützten AWS Regionen außer China (Peking), Asien-Pazifik (Thailand), Naher Osten (VAE), Asien-Pazifik (Hyderabad), Asien-Pazifik (Malaysia), Asien-Pazifik (Melbourne), AWS GovCloud (USA-Ost), AWS GovCloud (US-West), Mexiko (Zentral), Israel (Tel Aviv), Kanada West (Calgary), Europa (Spanien), China (Ningxia), Europa (Zürich)

Parameter:

Keine

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

eks-cluster-log-enabled

Prüft, ob ein Amazon Elastic Kubernetes Service (Amazon EKS)-Cluster mit aktivierter Protokollierung konfiguriert ist. Die Regel ist NON_COMPLIANT, wenn die Protokollierung für Amazon-EKS-Cluster nicht aktiviert ist oder wenn die Protokollierung nicht mit dem genannten Protokolltyp aktiviert ist.

ID: EKS_CLUSTER_LOG_ENABLED

Ressourcentypen: AWS::EKS::Cluster

Auslösertyp: Konfigurationsänderungen

AWS-Region: Alle unterstützten AWS Regionen außer Asien-Pazifik (Thailand), Asien-Pazifik (Malaysia), AWS GovCloud (USA-Ost), AWS GovCloud (US-West), Mexiko (Zentral), Israel (Tel Aviv), Kanada West (Calgary)

Parameter:

logTypes (optional), Typ: CSV

> Durch Kommas getrennte Liste der Protokolltypen der EKS-Cluster-Steuerungsebene, die von der Regel überprüft werden sollen. Gültige Werte: „api“, „audit“, „authenticator“, „ControllerManager“, „scheduler

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

eks-cluster-oldest-supported-Ausführung

Prüft, ob auf einem Amazon Elastic Kubernetes Service (EKS)-Cluster die älteste unterstützte Version ausgeführt wird. Die Regel ist NON_COMPLIANT, wenn auf einem EKS-Cluster die älteste unterstützte Version (gleich dem Parameter `oldestVersionSupported`) ausgeführt wird.

ID: EKS_CLUSTER_OLDEST_SUPPORTED_VERSION

Ressourcentypen: AWS::EKS::Cluster

Auslösertyp: Konfigurationsänderungen

AWS-Region: Alle unterstützten AWS Regionen außer China (Peking), Asien-Pazifik (Thailand), Asien-Pazifik (Jakarta), Naher Osten (VAE), Asien-Pazifik (Hyderabad), Asien-Pazifik (Osaka), Asien-Pazifik (Malaysia), Asien-Pazifik (Melbourne), AWS GovCloud (USA-Ost), AWS GovCloud (US-West), Mexiko (Zentral), Israel (Tel Aviv), Kanada West (Calgary), Europa (Spanien), China (Ningxia), Europa (Region Zürich

Parameter:

oldestVersionSupported, Typ: Zeichenfolge

Wert der ältesten Kubernetes-Version, die auf AWS unterstützt wird.

AWS CloudFormation Schablone

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

eks-cluster-secrets-encrypted

Prüft, ob Amazon EKS-Cluster so konfiguriert sind, dass Kubernetes-Geheimnisse mit KMS verschlüsselt AWS werden. Die Regel lautet NON_COMPLIANT, wenn ein EKS-Cluster keine EncryptionConfig-Ressource hat oder wenn EncryptionConfig Geheimnisse nicht als Ressource benennt.

Kennung: EKS_CLUSTER_SECRETS_ENCRYPTED

Ressourcentypen: AWS::EKS::Cluster

Auslösertyp: Regelmäßig

AWS-Region: Alle unterstützten AWS Regionen außer China (Peking), Asien-Pazifik (Thailand), Asien-Pazifik (Malaysia), Mexiko (Zentral), Kanada West (Calgary), China (Ningxia)

Parameter:

kmsKeyArns (Fakultativ), Typ: CSV

Durch Kommas getrennte Liste der KMS-Schlüssel Amazon Resource Names (ARNs), die für die Verwendung von EKS zugelassen sind.

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

eks-cluster-supported-version

Prüft, ob auf einem Amazon Elastic Kubernetes Service (EKS)-Cluster eine unterstützte Kubernetes-Version ausgeführt wird. Diese Regel ist NON_COMPLIANT, wenn auf einem EKS-Cluster eine nicht unterstützte Version ausgeführt wird (älter als Parameter „`oldestVersionSupported`“).

ID: EKS_CLUSTER_SUPPORTED_VERSION

Ressourcentypen: AWS::EKS::Cluster

Auslösertyp: Konfigurationsänderungen

AWS-Region: Alle unterstützten AWS Regionen außer Asien-Pazifik (Thailand), Asien-Pazifik (Malaysia), Mexiko (Zentral), Israel (Tel Aviv) und Kanada West (Calgary)

Parameter:

oldestVersionSupported, Typ: Zeichenfolge

Wert der ältesten Kubernetes-Version, die auf AWS unterstützt wird.

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

eks-endpoint-no-public-Zugang

Prüft, ob der Amazon Elastic Kubernetes Service (Amazon EKS)-Endpunkt nicht öffentlich zugänglich ist. Die Regel ist NON_COMPLIANT, wenn der Endpunkt öffentlich zugänglich ist.

ID: EKS_ENDPOINT_NO_PUBLIC_ACCESS

Ressourcentypen: AWS::EKS::Cluster

Auslösertyp: Regelmäßig

AWS-Region: Alle unterstützten AWS Regionen außer der Region Asien-Pazifik (Taipeh)

Parameter:

Keine

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

eks-secrets-encrypted

Prüft, ob Amazon Elastic Kubernetes Service Service-Cluster so konfiguriert sind, dass Kubernetes-Secrets mit AWS Key Management Service (KMS) -Schlüsseln verschlüsselt werden.

- Diese Regel ist COMPLIANT, wenn ein EKS-Cluster eine Verschlüsselungskonfiguration mit Secrets als eine der Ressourcen hat.
- Diese Regel ist auch COMPLIANT, wenn der zur Verschlüsselung von EKS-Secrets verwendete Schlüssel mit dem Parameter übereinstimmt.
- Diese Regel ist NON_COMPLIANT, wenn ein EKS-Cluster keine Verschlüsselungskonfiguration hat oder wenn die Ressourcen der Verschlüsselungskonfiguration keine Secrets enthalten.
- Diese Regel ist auch NON_COMPLIANT, wenn der zur Verschlüsselung von EKS-Secrets verwendete Schlüssel nicht mit dem Parameter übereinstimmt.

ID: EKS_SECRETS_ENCRYPTED

Ressourcentypen: AWS::EKS::Cluster

Auslösertyp: Regelmäßig

AWS-Region: Alle unterstützten AWS Regionen außer der Region Asien-Pazifik (Taipeh)

Parameter:

kmsKeyArns (Fakultativ), Typ: CSV

> Durch Kommata getrennte Liste der Amazon-Ressourcennamen (ARN) des KMS-Schlüssels, der für verschlüsselte Secrets in einem EKS-Cluster verwendet werden soll.

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

elasticache-auto-minor-version-Upgrade-Check

Prüft, ob Amazon ElastiCache Amazon-Clustern auto Nebenversions-Upgrades aktiviert sind. Die Regel lautet NON_COMPLIANT für einen ElastiCache Cluster, wenn er die Redis- oder Valkey-Engine verwendet und '' nicht auf 'trueAutoMinorVersionUpgrade' gesetzt ist.

ID: ELASTICACHE_AUTO_MINOR_VERSION_UPGRADE_CHECK

Ressourcentypen: AWS::ElastiCache::CacheCluster

Auslösertyp: Regelmäßig

AWS-Region: Alle unterstützten AWS Regionen außer Asien-Pazifik (Thailand), Naher Osten (VAE), Asien-Pazifik (Malaysia), Asien-Pazifik (Melbourne), AWS GovCloud (USA-Ost), AWS GovCloud (US-West), Mexiko (Zentral), Israel (Tel Aviv), Kanada West (Calgary)

Parameter:

Keine

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

elasticache-rbac-auth-enabled

Prüft, ob für ElastiCache Amazon-Replikationsgruppen die RBAC-Authentifizierung aktiviert ist. Die Regel lautet NON_COMPLIANT, wenn die Redis-Version 6 oder höher ist und 'UserGroupIds' fehlt, leer ist oder nicht mit einem durch den Parameter '' bereitgestellten Eintrag übereinstimmt. `allowedUserGroupIDs`

ID: ELASTICACHE_RBAC_AUTH_ENABLED

Ressourcentypen: AWS::ElastiCache::ReplicationGroup

Auslösertyp: Regelmäßig

AWS-Region: Alle unterstützten AWS Regionen außer China (Peking), Asien-Pazifik (Thailand), Asien-Pazifik (Jakarta), Naher Osten (VAE), Asien-Pazifik (Hyderabad), Asien-Pazifik (Malaysia), Asien-Pazifik (Melbourne), AWS GovCloud (US-Ost), AWS GovCloud (US-West), Mexiko (Zentral), Israel (Tel Aviv), Kanada West (Calgary), Europa (Spanien), China (Ningxia), Europa (Zürich)

Parameter:

allowedUserGroupIDs (Fakultativ), Typ: CSV

> Eine durch Kommas getrennte Liste von Benutzergruppen IDs , die für den Zugriff auf ElastiCache Replikationsgruppen zugelassen sind.

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

elasticache-redis-cluster-automatic-Backup-Check

Prüfen Sie, ob die Amazon ElastiCache Redis-Cluster die automatische Sicherung aktiviert haben. Die Regel lautet NON_COMPLIANT, wenn der SnapshotRetentionLimit For-Redis-Cluster kleiner als der Parameter ist. SnapshotRetentionPeriod Beispiel: Wenn der Parameter 15 ist, ist die Regel nicht konform, wenn der snapshotRetentionPeriod zwischen 0 und 15 liegt.

ID: ELASTICACHE_REDIS_CLUSTER_AUTOMATIC_BACKUP_CHECK

Ressourcentypen:, AWS::ElastiCache::CacheCluster AWS::ElastiCache::ReplicationGroup

Auslösertyp: Regelmäßig

AWS-Region: Alle unterstützten AWS Regionen außer der Region Asien-Pazifik (Taipeh)

Parameter:

snapshotRetentionPeriod (Fakultativ), Typ: int, Standard: 15

> Minimaler Snapshot-Aufbewahrungszeitraum in Tagen für Redis-Cluster. Der Standardwert beträgt 15 Tage.

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

elasticache-repl-grp-auto-Failover-fähig

Prüft, ob für Amazon ElastiCache Redis-Replikationsgruppen das automatische Failover aktiviert ist. Die Regel lautet NON_COMPLIANT für eine ElastiCache Replikationsgruppe, wenn '' nicht auf 'AutomaticFailoveraktiviert' gesetzt ist.

ID: ELASTICACHE_REPL_GRP_AUTO_FAILOVER_ENABLED

Ressourcentypen: AWS::ElastiCache::ReplicationGroup

Auslösertyp: Regelmäßig

AWS-Region: Alle unterstützten AWS Regionen außer Asien-Pazifik (Thailand), Naher Osten (VAE), Asien-Pazifik (Malaysia), Asien-Pazifik (Melbourne), AWS GovCloud (USA-Ost), AWS GovCloud (US-West), Mexiko (Zentral), Israel (Tel Aviv), Kanada West (Calgary)

Parameter:

Keine

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

elasticache-repl-grp-encrypted-im Ruhezustand

Prüft, ob ElastiCache Amazon-Replikationsgruppen encryption-at-rest aktiviert wurden. Die Regel ist NON_COMPLIANT für eine ElastiCache Replikationsgruppe, wenn 'AtRestEncryptionEnabled' deaktiviert ist oder wenn der KMS-Schlüssel-ARN nicht mit dem genehmigten KMSKey Arns-Parameter übereinstimmt.

ID: ELASTICACHE_REPL_GRP_ENCRYPTED_AT_REST

Ressourcentypen: AWS::ElastiCache::ReplicationGroup

Auslösertyp: Regelmäßig

AWS-Region: Alle unterstützten AWS Regionen außer Asien-Pazifik (Thailand), Naher Osten (VAE), Asien-Pazifik (Malaysia), Asien-Pazifik (Melbourne), AWS GovCloud (USA-Ost), AWS GovCloud (US-West), Mexiko (Zentral), Israel (Tel Aviv), Kanada West (Calgary)

Parameter:

zugelassene KMSKey Ausweise (optional), Typ: CSV

> Durch Kommas getrennte Liste von KMS-Schlüsseln IDs , die zur ElastiCache Verwendung zugelassen sind.

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

elasticache-repl-grp-encryptedim Transit

Prüft, ob ElastiCache Amazon-Replikationsgruppen encryption-in-transit aktiviert wurden. Die Regel lautet NON_COMPLIANT für eine ElastiCache Replikationsgruppe, wenn '' auf TransitEncryptionEnabled 'false' gesetzt ist.

ID: ELASTICACHE_REPL_GRP_ENCRYPTED_IN_TRANSIT

Ressourcentypen: AWS::ElastiCache::ReplicationGroup

Auslösertyp: Regelmäßig

AWS-Region: Alle unterstützten AWS Regionen außer Asien-Pazifik (Thailand), Naher Osten (VAE), Asien-Pazifik (Malaysia), Asien-Pazifik (Melbourne), AWS GovCloud (USA-Ost), AWS GovCloud (US-West), Mexiko (Zentral), Israel (Tel Aviv), Kanada West (Calgary)

Parameter:

Keine

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

elasticache-repl-grp-redis-auth-aktiviert

Prüft, ob Redis AUTH für ElastiCache Amazon-Replikationsgruppen aktiviert ist. Die Regel lautet NON_COMPLIANT für eine ElastiCache Replikationsgruppe, wenn die Redis-Version ihrer Knoten unter 6 liegt (Version 6+ verwenden Sie Redis ACLs) und '' AuthToken fehlt oder leer/null ist.

ID: ELASTICACHE_REPL_GRP_REDIS_AUTH_ENABLED

Ressourcentypen: AWS::ElastiCache::ReplicationGroup

Auslösertyp: Regelmäßig

AWS-Region: Alle unterstützten AWS Regionen außer Asien-Pazifik (Thailand), Asien-Pazifik (Jakarta), Naher Osten (VAE), Asien-Pazifik (Hyderabad), Asien-Pazifik (Malaysia), Asien-Pazifik (Melbourne), AWS GovCloud (USA-Ost), AWS GovCloud (US-West), Mexiko (Zentral), Israel (Tel Aviv), Kanada West (Calgary), Europa (Spanien), Europa (Zürich)

Parameter:

Keine

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

elasticache-subnet-group-check

Prüft, ob ElastiCache Amazon-Cluster mit einer benutzerdefinierten Subnetzgruppe konfiguriert sind. Die Regel lautet NON_COMPLIANT für einen ElastiCache Cluster, wenn dieser eine Standard-Subnetzgruppe verwendet.

ID: ELASTICACHE_SUBNET_GROUP_CHECK

Ressourcentypen: AWS::ElastiCache::CacheCluster

Auslösertyp: Regelmäßig

AWS-Region: Alle unterstützten AWS Regionen außer Asien-Pazifik (Thailand), Asien-Pazifik (Jakarta), Naher Osten (VAE), Asien-Pazifik (Hyderabad), Asien-Pazifik (Osaka), Asien-Pazifik (Malaysia), Asien-Pazifik (Melbourne), AWS GovCloud (USA-Ost), AWS GovCloud (US-West), Mexiko (Zentral), Israel (Tel Aviv), Kanada West (Calgary), Europa (Spanien), Europa (Zürich)

Parameter:

Keine

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

elasticache-supported-engine-version

Überprüft, ob auf ElastiCache Clustern eine Version ausgeführt wird, die höher oder gleich der empfohlenen Engine-Version ist. Die Regel lautet NON_COMPLIANT, wenn der EngineVersion Wert " für einen ElastiCache Cluster unter der angegebenen empfohlenen Version für die angegebene Engine liegt.

ID: ELASTICACHE_SUPPORTED_ENGINE_VERSION

Ressourcentypen: AWS::ElastiCache::CacheCluster

Auslösertyp: Regelmäßig

AWS-Region: Alle unterstützten AWS Regionen außer China (Peking), Asien-Pazifik (Thailand), Naher Osten (VAE), Asien-Pazifik (Hyderabad), Asien-Pazifik (Malaysia), Asien-Pazifik (Melbourne),

AWS GovCloud (USA-Ost), AWS GovCloud (US-West), Mexiko (Zentral), Israel (Tel Aviv), Kanada West (Calgary), Europa (Spanien), China (Ningxia), Europa (Zürich)

Parameter:

latestMemcachedVersion, Typ: Zeichenfolge

Die neueste empfohlene Engine-Version für Memcached. Gültige Werte sind im Format Semantic Versioning (SemVer) mit einer 3-Komponenten-Nummer für Haupt-, Neben- und Patch-Versionen (z. B. 1.6.6, nicht 1.6).

latestRedisVersion, Typ: Zeichenfolge

Die neueste empfohlene Engine-Version für Redis. Gültige Werte liegen im Format Semantic Versioning (SemVer) mit einer 3-Komponenten-Nummer für Haupt-, Neben- und Patch-Versionen vor (z. B. 7.0.5, nicht 7.0).

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

elasticbeanstalk-application-description

Prüft, ob AWS Elastic Beanstalk Beanstalk-Anwendungen eine Beschreibung haben. Die Regel lautet NON_COMPLIANT, wenn configuration.description nicht existiert oder eine leere Zeichenfolge ist.

Kennung: ELASTICBEANSTALK_APPLICATION_DESCRIPTION

Ressourcentypen: AWS::ElasticBeanstalk::Application

Auslösertyp: Konfigurationsänderungen

AWS-Region: Alle unterstützten AWS Regionen außer China (Peking), Asien-Pazifik (Thailand), Naher Osten (VAE), Asien-Pazifik (Hyderabad), Asien-Pazifik (Malaysia), Asien-Pazifik (Melbourne), AWS GovCloud (USA-Ost), AWS GovCloud (US-West), Mexiko (Zentral), Israel (Tel Aviv), Kanada West (Calgary), Europa (Spanien), China (Ningxia), Europa (Zürich)

Parameter:

Keine

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

elasticbeanstalk-application-version-description

Prüft, ob die AWS Elastic Beanstalk Beanstalk-Anwendungsversionen eine Beschreibung haben. Die Regel lautet NON_COMPLIANT, wenn configuration.description nicht existiert oder eine leere Zeichenfolge ist.

Kennung: ELASTICBEANSTALK_APPLICATION_VERSION_DESCRIPTION

Ressourcentypen: AWS::ElasticBeanstalk::ApplicationVersion

Auslösertyp: Konfigurationsänderungen

AWS-Region: Alle unterstützten AWS Regionen außer China (Peking), Asien-Pazifik (Thailand), Naher Osten (VAE), Asien-Pazifik (Hyderabad), Asien-Pazifik (Malaysia), Asien-Pazifik (Melbourne), AWS GovCloud (USA-Ost), AWS GovCloud (US-West), Mexiko (Zentral), Israel (Tel Aviv), Kanada West (Calgary), Europa (Spanien), China (Ningxia), Europa (Zürich)

Parameter:

Keine

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

elasticbeanstalk-environment-description

Prüft, ob AWS Elastic Beanstalk Beanstalk-Umgebungen eine Beschreibung haben. Die Regel lautet NON_COMPLIANT, wenn configuration.description nicht existiert oder eine leere Zeichenfolge ist.

Kennung: ELASTICBEANSTALK_ENVIRONMENT_DESCRIPTION

Ressourcentypen: AWS::ElasticBeanstalk::Environment

Auslösertyp: Konfigurationsänderungen

AWS-Region: Alle unterstützten AWS Regionen außer China (Peking), Asien-Pazifik (Thailand), Naher Osten (VAE), Asien-Pazifik (Hyderabad), Asien-Pazifik (Malaysia), Asien-Pazifik (Melbourne), AWS GovCloud (USA-Ost), AWS GovCloud (US-West), Mexiko (Zentral), Israel (Tel Aviv), Kanada West (Calgary), Europa (Spanien), China (Ningxia), Europa (Zürich)

Parameter:

Keine

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

elasticsearch-encrypted-at-rest

Überprüft, ob für Amazon OpenSearch Service-Domains (früher Elasticsearch genannt) die Konfiguration „Verschlüsselung im Ruhezustand“ aktiviert ist. Die Regel lautet NON_COMPLIANT, wenn das EncryptionAtRestOptions Feld nicht aktiviert ist.

ID: ELASTICSEARCH_ENCRYPTED_AT_REST

Ressourcentypen: AWS::Elasticsearch::Domain

Auslösertyp: Regelmäßig

AWS-Region: Alle unterstützten AWS Regionen außer der Region Asien-Pazifik (Taipeh)

Parameter:

Keine

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

elasticsearch-in-vpc-only

Überprüft, ob sich Amazon OpenSearch Service-Domains (früher Elasticsearch genannt) in Amazon Virtual Private Cloud (Amazon VPC) befinden. Die Regel lautet NON_COMPLIANT, wenn ein OpenSearch Service-Domain-Endpunkt öffentlich ist.

ID: ELASTICSEARCH_IN_VPC_ONLY

Ressourcentypen: AWS::Elasticsearch::Domain

Auslösertyp: Regelmäßig

AWS-Region: Alle unterstützten AWS Regionen außer der Region Asien-Pazifik (Taipeh)

Parameter:

Keine

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

elasticsearch-logs-to-cloudwatch

Prüft, ob Amazon OpenSearch Service-Domains so konfiguriert sind, dass sie Protokolle an Amazon CloudWatch Logs senden. Die Regel ist COMPLIANT, wenn ein Protokoll für eine Amazon-ES-Domäne aktiviert ist. Diese Regel ist NON_COMPLIANT, wenn die Protokollierung nicht konfiguriert ist.

ID: ELASTICSEARCH_LOGS_TO_CLOUDWATCH

Ressourcentypen: AWS::Elasticsearch::Domain

Auslösertyp: Konfigurationsänderungen

AWS-Region: Alle unterstützten AWS Regionen außer der Region Asien-Pazifik (Taipeh)

Parameter:

logTypes (optional), Typ: CSV

> Durch Kommata getrennte Liste der Protokolle, die aktiviert sind. Zulässige Werte sind „Such“, „Index“ und „Fehler“.

Proaktive Auswertung

Anweisungen zur Ausführung dieser Regel im proaktiven Modus finden Sie unter Evaluieren Ihrer Ressourcen mithilfe von AWS Config Regeln. Damit diese Regel im proaktiven Modus COMPLIANT

zurückgibt, muss das Ressourcenkonfigurationsschema für die StartResourceEvaluationAPI die folgenden Eingaben enthalten, die als Zeichenfolge kodiert sind:

```
"ResourceConfiguration":
...
{
   "LogPublishingOptions": "{Key : Value, ...}"*
}
...
```

*Ein Objekt mit einem oder mehreren der folgenden Schlüssel: `SEARCH_SLOW_LOGS`, `ES_APPLICATION_LOGS`, `INDEX_SLOW_LOGS`, `AUDIT_LOGS`, abhängig von den Protokolltypen, die Sie veröffentlichen möchten. Jeder Schlüssel benötigt einen gültigen `LogPublishingOption`-Wert.

Weitere Informationen zur proaktiven Auswertung finden Sie unter Auswertungsmodus.

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

elasticsearch-node-to-node-Verschlüsselungsprüfung

Prüfen Sie, ob OpenSearch Service-Knoten (früher Elasticsearch genannt) durchgehend verschlüsselt sind. Die Regel lautet NON_COMPLIANT, wenn die node-to-node Verschlüsselung in der Domain nicht aktiviert ist.

ID: ELASTICSEARCH_NODE_TO_NODE_ENCRYPTION_CHECK

Ressourcentypen: AWS::Elasticsearch::Domain

Auslösertyp: Konfigurationsänderungen

AWS-Region: Alle unterstützten AWS Regionen außer der Region Asien-Pazifik (Taipeh)

Parameter:

Keine

Proaktive Auswertung

Anweisungen zur Ausführung dieser Regel im proaktiven Modus finden Sie unter Evaluieren Ihrer Ressourcen mithilfe von AWS Config Regeln. Damit diese Regel im proaktiven Modus COMPLIANT

zurückgibt, muss das Ressourcenkonfigurationsschema für die StartResourceEvaluationAPI die folgenden Eingaben enthalten, die als Zeichenfolge kodiert sind:

```
"ResourceConfiguration":
...
{
   "NodeToNodeEncryptionOptions": BOOLEAN
}
...
```

Weitere Informationen zur proaktiven Auswertung finden Sie unter Auswertungsmodus.

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

elastic-beanstalk-logs-to-Wolkenbeobachtung

Prüft, ob AWS Elastic Beanstalk Beanstalk-Umgebungen so konfiguriert sind, dass sie Protokolle an Amazon CloudWatch Logs senden. Die Regel lautet NON_COMPLIANT, wenn der Wert von `` StreamLogs falsch ist.

ID: ELASTIC_BEANSTALK_LOGS_TO_CLOUDWATCH

Ressourcentypen: AWS::ElasticBeanstalk::Environment

Auslösertyp: Konfigurationsänderungen

AWS-Region: Alle unterstützten AWS Regionen außer China (Peking), Asien-Pazifik (Thailand), Naher Osten (VAE), Asien-Pazifik (Hyderabad), Asien-Pazifik (Malaysia), Asien-Pazifik (Melbourne), AWS GovCloud (USA-Ost), AWS GovCloud (US-West), Mexiko (Zentral), Israel (Tel Aviv), Kanada West (Calgary), Europa (Spanien), China (Ningxia), Europa (Zürich)

Parameter:

RetentionInDays (Fakultativ), Typ: Zeichenfolge

> Prüft die Anzahl der Tage, die Protokollereignisse gespeichert werden, bevor sie ablaufen. Mögliche Werte sind: 1, 3, 5, 7, 14, 30, 60, 90, 120, 150, 180, 365, 400, 545, 731, 1827 und 3653. Die Regel ist NON_COMPLIANT, wenn der Wert `logs lautet. RetentionInDays`entspricht nicht diesem Parameter.

DeleteOnTerminate (Fakultativ), Typ: Zeichenfolge

Prüft, ob Protokolle so konfiguriert sind, dass sie beim Beenden der Umgebung gelöscht werden. Gültige Werte sind „True“ oder „False“. Die Regel ist NON_COMPLIANT, wenn der Wert `logs lautet. DeleteOnTerminate`entspricht nicht diesem Parameter.

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

elastic-beanstalk-managed-updates-aktiviert

Prüft, ob verwaltete Plattformupdates in einer AWS Elastic Beanstalk Umgebung aktiviert sind. Die Regel ist COMPLIANT, wenn der Wert für `ManagedActionsEnabled` auf „True“ festgelegt ist. Die Regel ist NON_COMPLIANT, wenn der Wert für `ManagedActionsEnabled` auf „False“ festgelegt oder ein Parameter angegeben ist, dessen Wert nicht mit den vorhandenen Konfigurationen übereinstimmt.

ID: ELASTIC_BEANSTALK_MANAGED_UPDATES_ENABLED

Ressourcentypen: AWS::ElasticBeanstalk::Environment

Auslösertyp: Konfigurationsänderungen

AWS-Region: Alle unterstützten AWS Regionen außer Asien-Pazifik (Thailand), Asien-Pazifik (Jakarta), Naher Osten (VAE), Asien-Pazifik (Hyderabad), Asien-Pazifik (Osaka), Asien-Pazifik (Malaysia), Asien-Pazifik (Melbourne), Mexiko (Zentral), Israel (Tel Aviv), Asien-Pazifik (Taipeh), Kanada West (Calgary), Europa (Spanien), Europa (Zürich)

Parameter:

UpdateLevel (Fakultativ), Typ: Zeichenfolge

Gibt an, ob die Aktualisierungsebenen auf „kleinere“ Versionsupdates oder „Patch“-Versionsupdates eingestellt sind.

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

ELV 2- acm-certificate-required

Überprüft, ob Application Load Balancer und Network Load Balancer über Listener verfügen, die für die Verwendung von Zertifikaten von (ACM) konfiguriert sind. AWS Certificate Manager Diese Regel ist NON_COMPLIANT, wenn mindestens ein Load Balancer über mindestens einen Listener verfügt, der ohne ein Zertifikat von ACM oder mit einem anderen als einem ACM-Zertifikat konfiguriert ist.

Kennung ELBV2: _ACM_CERTIFICATE_REQUIRED

Ressourcentypen: AWS::ElasticLoadBalancingV2::LoadBalancer

Auslösertyp: Regelmäßig

AWS-Region: Alle unterstützten AWS Regionen außer Asien-Pazifik (Thailand), Asien-Pazifik (Jakarta), Naher Osten (VAE), Asien-Pazifik (Hyderabad), Asien-Pazifik (Osaka), Asien-Pazifik (Malaysia), Asien-Pazifik (Melbourne), AWS GovCloud (US-Ost), AWS GovCloud (US-West), Mexiko (Zentral), Israel (Tel Aviv), Asien-Pazifik (Taipeh), Kanada West (Calgary), Europa (Spanien), Europa (Zürich)

Parameter:

AcmCertificatesAllowed (Fakultativ), Typ: CSV

Kommagetrennte Liste von Zertifikaten Amazon Resource Names ()ARNs.

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unter[AWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen](#).

ELV 2- listener-encryption-in-transit

Überprüft, ob die Listener für die Load Balancer mit HTTPS- oder TLS-Terminierung konfiguriert sind. Die Regel lautet NON_COMPLIANT, wenn Listener nicht mit HTTPS- oder TLS-Terminierung konfiguriert sind.

Kennung: _LISTENER_ENCRYPTION_IN_TRANSIT ELBV2

Ressourcentypen: AWS::ElasticLoadBalancingV2::Listener

Auslösertyp: Konfigurationsänderungen

AWS-Region: Alle unterstützten AWS Regionen außer Asien-Pazifik (Thailand), Asien-Pazifik (Jakarta), Naher Osten (VAE), Asien-Pazifik (Hyderabad), Asien-Pazifik (Seoul), Asien-Pazifik (Malaysia), Asien-Pazifik (Melbourne), Mexiko (Zentral), Israel (Tel Aviv), Kanada West (Calgary), Europa (Spanien), Europa (Zürich)

Parameter:

Keine

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

elbv2-multiple-az

Prüft, ob ein Elastic Load Balancer V2 (Application, Network oder Gateway Load Balancer) mehreren Availability Zones () zugeordnet ist. AZs Die Regel lautet NON_COMPLIANT, wenn einem Elastic Load Balancer V2 weniger als 2 zugeordnet ist. AZs Weitere Informationen finden Sie unter Availability Zones für Ihren Application Load Balancer.

ELBV2Kennung: _MULTIPLE_AZ

Ressourcentypen: AWS::ElasticLoadBalancingV2::LoadBalancer

Auslösertyp: Konfigurationsänderungen

AWS-Region: Alle unterstützten AWS Regionen außer Asien-Pazifik (Thailand), Asien-Pazifik (Malaysia), AWS GovCloud (USA-Ost), AWS GovCloud (US-West), Mexiko (Zentral), Kanada West (Calgary)

Parameter:

minAvailabilityZones (Fakultativ), Typ: int

Mindestanzahl erwarteter AZs Personen (zwischen 2 und einschließlich 10).

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

elbv2-check predefined-security-policy-ssl

Überprüft, ob Listener für Application Load Balancers (ALBs) oder Network Load Balancers () bestimmte Sicherheitsrichtlinien verwenden. NLBs Die Regel lautet NON_COMPLIANT, wenn ein HTTPS-Listener für einen ALB oder ein TLS-Listener für einen NLB die von Ihnen angegebenen Sicherheitsrichtlinien nicht verwendet.

Kennung ELBV2: _PREDEFINED_SECURITY_POLICY_SSL_CHECK

Ressourcentypen: AWS::ElasticLoadBalancingV2::Listener

Auslösertyp: Konfigurationsänderungen

AWS-Region: Alle unterstützten AWS Regionen außer Naher Osten (Bahrain), Asien-Pazifik (Thailand), Asien-Pazifik (Jakarta), Naher Osten (VAE), Asien-Pazifik (Hyderabad), Asien-Pazifik (Malaysia), Asien-Pazifik (Melbourne), Mexiko (Zentral), Israel (Tel Aviv), Kanada West (Calgary), Europa (Spanien), China (Ningxia), Europa (Zürich)

Parameter:

SSL-Richtlinien, Typ: CSV

> Durch Kommas getrennte Liste von SSL-Sicherheitsrichtlinien, die von der Regel überprüft werden sollen. Zum Beispiel "ELBSecurityPolicy- TLS13 -1-2-2021-06".

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

elb-acm-certificate-required

Prüft, ob die Classic Load Balancer SSL-Zertifikate verwenden, die von bereitgestellt werden. AWS Certificate Manager Verwenden Sie zur Nutzung dieser Regel mit Ihrem Classic Load Balancer einen SSL- oder HTTPS-Listener. Diese Regel trifft nur auf Classic Load Balancer zu. Mit dieser Regel werden keine Application Load Balancer oder Network Load Balancer geprüft.

ID: ELB_ACM_CERTIFICATE_REQUIRED

Ressourcentypen: AWS::ElasticLoadBalancing::LoadBalancer

Auslösertyp: Konfigurationsänderungen

AWS-Region: Alle unterstützten AWS Regionen außer Afrika (Kapstadt), Asien-Pazifik (Osaka), Europa (Mailand), Israel (Tel Aviv), Kanada West (Calgary), Europa (Spanien), Europa (Zürich)

Parameter:

Keine

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

elb-cross-zone-load-Balancing aktiviert

Prüft, ob zonenübergreifendes Load Balancing für Classic Load Balancer aktiviert ist. Die Regel ist NON_COMPLIANT, wenn zonenübergreifendes Load Balancing für Classic Load Balancers nicht aktiviert ist.

ID: ELB_CROSS_ZONE_LOAD_BALANCING_ENABLED

Ressourcentypen: AWS::ElasticLoadBalancing::LoadBalancer

Auslösertyp: Konfigurationsänderungen

AWS-Region: Alle unterstützten AWS Regionen

Parameter:

Keine

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

elb-custom-security-policy-ssl-Prüfung

Prüft, ob die SSL-Listener Ihres Classic Load Balancers eine benutzerdefinierte Richtlinie verwenden. Die Regel ist nur anwendbar, wenn für den Classic Load Balancer SSL-Listener vorhanden sind.

ID: ELB_CUSTOM_SECURITY_POLICY_SSL_CHECK

Ressourcentypen: AWS::ElasticLoadBalancing::LoadBalancer

Auslösertyp: Konfigurationsänderungen

AWS-Region: Alle unterstützten AWS Regionen außer Asien-Pazifik (Jakarta), Asien-Pazifik (Osaka), Asien-Pazifik (Melbourne) und Asien-Pazifik (Taipeh)

Parameter:

sslProtocolsAndChiffren, Typ: Zeichenfolge

Eine durch Kommata getrennte Liste der Verschlüsselungsverfahren und Protokolle.

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

elb-deletion-protection-enabled

Prüft, ob der Löschschutz für einen Elastic Load Balancer aktiviert ist. Die Regel ist NON_COMPLIANT, wenn „Löschschutz aktiviert“ den Wert „False“ hat.

ID: ELB_DELETION_PROTECTION_ENABLED

Ressourcentypen: AWS::ElasticLoadBalancingV2::LoadBalancer

Auslösertyp: Konfigurationsänderungen

AWS-Region: Alle unterstützten AWS Regionen außer der Region Asien-Pazifik (Osaka)

Parameter:

Keine

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

elb-logging-enabled

Prüft, ob für den Application Load Balancer und den Classic Load Balancer die Protokollierung aktiviert ist. Die Regel ist NON_COMPLIANT, wenn der falsch `access_logs.s3.enabled` `access_logs.S3.bucket` ist oder nicht dem von Ihnen angegebenen s3 BucketName entspricht.

> **Note**
>
> Die Regel gilt nicht für Network Load Balancer oder Gateway Load Balancer.

ID: ELB_LOGGING_ENABLED

Ressourcentypen:, AWS::ElasticLoadBalancing::LoadBalancer AWS::ElasticLoadBalancingV2::LoadBalancer

Auslösertyp: Konfigurationsänderungen

AWS-Region: Alle unterstützten AWS Regionen

Parameter:

s3 BucketNames (fakultativ), Typ: CSV

> Eine durch Kommata getrennte Liste mit Namen von Amazon-S3-Buckets zur Bereitstellung der Protokolldateien durch Amazon ELB.

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

elb-predefined-security-policy-ssl-Prüfung

Prüft, ob Ihre SSL-Listener von Classic Load Balancer eine vordefinierte Richtlinie verwenden. Die Regel lautet NON_COMPLIANT, wenn die Richtlinie des Classic Load Balancer HTTPS/SSL Balancer-Listeners nicht dem Wert des Parameters " entspricht. `predefinedPolicyName`

ID: ELB_PREDEFINED_SECURITY_POLICY_SSL_CHECK

Ressourcentypen: AWS::ElasticLoadBalancing::LoadBalancer

Auslösertyp: Konfigurationsänderungen

AWS-Region: Alle unterstützten AWS Regionen außer der Region Asien-Pazifik (Osaka)

Parameter:

predefinedPolicyName, Typ: Zeichenfolge

Der Name der vordefinierten Richtlinie.

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

elb-tls-https-listeners-nur

Prüft, ob Ihr Classic Load Balancer mit SSL- oder HTTPS-Listenern konfiguriert ist. Die Regel lautet NON_COMPLIANT, wenn ein Listener nicht mit SSL oder HTTPS konfiguriert ist.

- Wenn für den Classic Load Balancer kein Listener konfiguriert ist, kehrt die Regel zurück. `NOT_APPLICABLE`
- Die Regel ist COMPLIANT, wenn die Classic Load Balancer-Listener mit SSL oder HTTPS konfiguriert sind.
- Die Regel lautet NON_COMPLIANT, wenn ein Listener nicht mit SSL oder HTTPS konfiguriert ist.

ID: ELB_TLS_HTTPS_LISTENERS_ONLY

Ressourcentypen: AWS::ElasticLoadBalancing::LoadBalancer

Auslösertyp: Konfigurationsänderungen

AWS-Region: Alle unterstützten AWS Regionen außer Naher Osten (VAE) und Asien-Pazifik (Osaka)

Parameter:

Keine

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

emr-block-public-access

Prüft, ob für ein Konto mit Amazon EMR die Einstellung „Öffentlichen Zugriff blockieren“ aktiviert ist. Die Regel ist NON_COMPLIANT, wenn sie falsch BlockPublicSecurityGroupRules ist, oder wenn sie wahr ist, sind andere Ports als Port 22 aufgeführt. PermittedPublicSecurityGroupRuleRanges

ID: EMR_BLOCK_PUBLIC_ACCESS

Ressourcentypen: AWS::::Account

Auslösertyp: Regelmäßig

AWS-Region: Alle unterstützten AWS Regionen außer China (Peking), Asien-Pazifik (Thailand), Asien-Pazifik (Malaysia), AWS GovCloud (USA-Ost), AWS GovCloud (US-West), Mexiko (Zentral), Kanada West (Calgary), China (Ningxia)

Parameter:

Keine

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

emr-kerberos-enabled

Prüft, ob Kerberos in Amazon-EMR-Clustern aktiviert ist. Die Regel ist NON_COMPLIANT, wenn keine Sicherheitskonfiguration an den Cluster angefügt ist oder die Sicherheitskonfiguration nicht den angegebenen Regelparametern entspricht.

ID: EMR_KERBEROS_ENABLED

Ressourcentypen: AWS::EMR::Cluster

Auslösertyp: Regelmäßig

AWS-Region: Alle unterstützten AWS Regionen außer Asien-Pazifik (Taipeh) und Kanada West (Calgary)

Parameter:

TicketLifetimeInHours (Fakultativ), Typ: int

Der Zeitraum, für den das vom KDC des Clusters ausgestellte Kerberos-Ticket gültig ist.

Realm (optional), Typ: Zeichenfolge

Der Kerberos-Bereichsname des anderen Bereichs in der Vertrauensstellung.

Domain (optional), Typ: Zeichenfolge

Der Domänenname des anderen Bereichs in der Vertrauensstellung.

AdminServer (Fakultativ), Typ: Zeichenfolge

Der vollständig qualifizierte Domänenname (FQDN, Fully Qualified Domain Name) des Admin-Servers im anderen Bereich der Vertrauensstellung.

KdcServer (Fakultativ), Typ: Zeichenfolge

Der vollständig qualifizierte Domänenname (FQDN) des KDC-Servers im anderen Bereich der Vertrauensstellung.

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

emr-master-no-public-ip

Prüft, ob die Master-Knoten der Amazon EMR-Cluster öffentlich sind. IPs Die Regel ist NON_COMPLIANT, wenn der Master-Knoten über eine öffentliche IP verfügt.

> **Note**
>
> Diese Regel überprüft Cluster, die sich im Status RUNNING oder WAITING befinden. Diese Regel erfordert, dass Sie die Aufzeichnung für den Ressourcentyp `AWS::EC2::Instance` aktivieren, um eine genaue Bewertung zu erhalten.

Bezeichner: EMR_MASTER_NO_PUBLIC_IP

Ressourcentypen:, AWS::EMR::Cluster AWS::EC2::Instance

Auslösertyp: Regelmäßig

AWS-Region: Alle unterstützten AWS Regionen außer Asien-Pazifik (Osaka), Asien-Pazifik (Melbourne), Israel (Tel Aviv), Asien-Pazifik (Taipeh) und Kanada West (Calgary)

Parameter:

Keine

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

emr-security-configuration-encryption-ausruhen

Überprüft, ob für eine Amazon EMR-Sicherheitskonfiguration die Verschlüsselung im Ruhezustand aktiviert ist. Bei der Konfiguration lautet die Regel NON_COMPLIANT. SecurityConfiguration. EncryptionConfiguration. EnableAtRestEncryption ist falsch.

Kennung: EMR_SECURITY_CONFIGURATION_ENCRYPTION_REST

Ressourcentypen: AWS::EMR::SecurityConfiguration

Auslösertyp: Konfigurationsänderungen

AWS-Region: Alle unterstützten AWS Regionen außer China (Peking), Asien-Pazifik (Thailand), Asien-Pazifik (Malaysia), AWS GovCloud (USA-Ost), AWS GovCloud (US-West), Mexiko (Zentral), China (Ningxia)

Parameter:

Keine

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

emr-security-configuration-encryption-Transit

Prüft, ob für eine Amazon EMR-Sicherheitskonfiguration die Verschlüsselung bei der Übertragung aktiviert ist. Bei der Konfiguration lautet die Regel NON_COMPLIANT. SecurityConfiguration. EncryptionConfiguration. EnableInTransitEncryption ist falsch.

Kennung: EMR_SECURITY_CONFIGURATION_ENCRYPTION_TRANSIT

Ressourcentypen: AWS::EMR::SecurityConfiguration

Auslösertyp: Konfigurationsänderungen

AWS-Region: Alle unterstützten AWS Regionen außer China (Peking), Asien-Pazifik (Thailand), Asien-Pazifik (Malaysia), AWS GovCloud (USA-Ost), AWS GovCloud (US-West), Mexiko (Zentral), China (Ningxia)

Parameter:

Keine

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

encrypted-volumes

Prüft, ob angehängte Amazon-EBS-Volumes verschlüsselt sind, und optional, ob sie mit einem festgelegten KMS-Schlüssel verschlüsselt sind. Die Regel ist NON_COMPLIANT, wenn angehängte EBS-Volumes nicht verschlüsselt oder mit einem KMS-Schlüssel verschlüsselt sind, der nicht in den angegebenen Parametern enthalten ist.

ID: ENCRYPTED_VOLUMES

Ressourcentypen: AWS::EC2::Volume

Auslösertyp: Konfigurationsänderungen

AWS-Region: Alle unterstützten AWS Regionen

Parameter:

kmsId (optional), Typ: Zeichenfolge

ID oder ARN des KMS-Schlüssels zum Verschlüsseln des Volumes.

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

event-data-store-cmk-Verschlüsselung aktiviert

Prüft, ob in AWS Cloud Trail-Ereignisdatenspeichern vom Kunden verwaltete AWS KMS-Schlüssel aktiviert sind. Die Regel lautet NON_COMPLIANT, wenn ein Ereignisdatenspeicher vom Kunden verwaltete KMS-Schlüssel deaktiviert hat. Optional können Sie eine Liste von KMS-Schlüsseln angeben, die von der Regel überprüft werden sollen.

Kennung: EVENT_DATA_STORE_CMK_ENCRYPTION_ENABLED

Ressourcentypen: AWS::CloudTrail::EventDataStore

Auslösertyp: Regelmäßig

AWS-Region: Alle unterstützten AWS Regionen außer Naher Osten (Bahrain), China (Peking), Asien-Pazifik (Thailand), Asien-Pazifik (Malaysia), Mexiko (Zentral), Kanada West (Calgary), China (Ningxia)

Parameter:

kmsKeyArns (Fakultativ), Typ: CSV

Durch Kommas getrennte Liste der Amazon-Ressourcennamen (ARNs) von AWS KMS-Schlüsseln, die von der Regel überprüft werden sollen. Falls angegeben, lautet die Regel NON_COMPLIANT, wenn ein AWS Cloud Trail-Ereignisdatenspeicher nicht mit einem dieser KMS-Schlüssel verschlüsselt ist.

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

evidently-launch-description

Überprüft, ob die Produkteinführungen von CloudWatch Amazon Evidently eine Beschreibung haben. Die Regel ist NON_COMPLIANT, wenn Configuration.Description nicht existiert oder eine leere Zeichenfolge ist.

Kennung: EVIDENTLY_LAUNCH_DESCRIPTION

Ressourcentypen: AWS::Evidently::Launch

Auslösertyp: Konfigurationsänderungen

AWS-Region: Nur in den Regionen Europa (Stockholm), USA Ost (Ohio), Europa (Irland), Europa (Frankfurt), USA Ost (Nord-Virginia), Asien-Pazifik (Tokio), USA West (Oregon), Asien-Pazifik (Singapur), Asien-Pazifik (Sydney) verfügbar

Parameter:

Keine

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

evidently-launch-tagged

Überprüft, ob die Starts von Amazon CloudWatch Evidently Tags haben. Optional können Sie Tag-Schlüssel angeben. Die Regel lautet NON_COMPLIANT, wenn keine Tags vorhanden sind oder wenn die angegebenen Tag-Schlüssel nicht vorhanden sind. Die Regel sucht nicht nach Tags, die mit 'aws: 'beginnen.

Kennung: EVIDENTLY_LAUNCH_TAGGED

Ressourcentypen: AWS::Evidently::Launch

Auslösertyp: Konfigurationsänderungen

AWS-Region: Nur in den Regionen Europa (Stockholm), USA Ost (Ohio), Europa (Irland), Europa (Frankfurt), USA Ost (Nord-Virginia), Asien-Pazifik (Tokio), USA West (Oregon), Asien-Pazifik (Singapur), Asien-Pazifik (Sydney) verfügbar

Parameter:

requiredKeyTags (Fakultativ), Typ: CSV

Durch Kommas getrennte Liste von Tag-Schlüsseln, die von der Regel überprüft werden sollen. Falls angegeben, lautet die Regel NON_COMPLIANT, wenn die ausgewertete Ressource diese Schlüssel nicht enthält. Bei Tag-Schlüsseln wird die Groß- und Kleinschreibung beachtet. Tag-Schlüssel, die mit „aws:“ beginnen, sind nicht erlaubt.

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

evidently-project-description

Prüft, ob Amazon CloudWatch Evidenly-Projekte eine Beschreibung haben. Die Regel ist NON_COMPLIANT, wenn Configuration.Description nicht existiert oder eine leere Zeichenfolge ist.

Kennung: EVIDENTLY_PROJECT_DESCRIPTION

Ressourcentypen: AWS::Evidently::Project

Auslösertyp: Konfigurationsänderungen

AWS-Region: Nur in den Regionen Europa (Stockholm), USA Ost (Ohio), Europa (Irland), Europa (Frankfurt), USA Ost (Nord-Virginia), Asien-Pazifik (Tokio), USA West (Oregon), Asien-Pazifik (Singapur), Asien-Pazifik (Sydney) verfügbar

Parameter:

Keine

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

evidently-project-tagged

Prüft, ob Amazon CloudWatch Evidenly-Projekte Tags haben. Optional können Sie Tag-Schlüssel angeben. Die Regel lautet NON_COMPLIANT, wenn keine Tags vorhanden sind oder wenn die

angegebenen Tag-Schlüssel nicht vorhanden sind. Die Regel sucht nicht nach Tags, die mit 'aws: 'beginnen.

Kennung: EVIDENTLY_PROJECT_TAGGED

Ressourcentypen: AWS::Evidently::Project

Auslösertyp: Konfigurationsänderungen

AWS-Region: Nur in den Regionen Europa (Stockholm), USA Ost (Ohio), Europa (Irland), Europa (Frankfurt), USA Ost (Nord-Virginia), Asien-Pazifik (Tokio), USA West (Oregon), Asien-Pazifik (Singapur), Asien-Pazifik (Sydney) verfügbar

Parameter:

requiredKeyTags (Fakultativ), Typ: CSV

> Durch Kommas getrennte Liste von Tag-Schlüsseln, die von der Regel überprüft werden sollen. Falls angegeben, lautet die Regel NON_COMPLIANT, wenn die ausgewertete Ressource diese Schlüssel nicht enthält. Bei Tag-Schlüsseln wird die Groß- und Kleinschreibung beachtet. Tag-Schlüssel, die mit „aws:“ beginnen, sind nicht erlaubt.

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

evidently-segment-description

Prüft, ob CloudWatch Amazon-Evidenly-Segmente eine Beschreibung haben. Die Regel ist NON_COMPLIANT, wenn Configuration.Description nicht existiert oder eine leere Zeichenfolge ist.

Kennung: EVIDENTLY_SEGMENT_DESCRIPTION

Ressourcentypen: AWS::Evidently::Segment

Auslösertyp: Konfigurationsänderungen

AWS-Region: Nur in den Regionen Europa (Stockholm), USA Ost (Ohio), Europa (Irland), Europa (Frankfurt), USA Ost (Nord-Virginia), Asien-Pazifik (Tokio), USA West (Oregon), Asien-Pazifik (Singapur), Asien-Pazifik (Sydney) verfügbar

Parameter:

Keine

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

evidently-segment-tagged

Prüft, ob CloudWatch Amazon-Evidenly-Segmente Tags haben. Optional können Sie Tag-Schlüssel angeben. Die Regel lautet NON_COMPLIANT, wenn keine Tags vorhanden sind oder wenn die angegebenen Tag-Schlüssel nicht vorhanden sind. Die Regel sucht nicht nach Tags, die mit 'aws: 'beginnen.

Kennung: EVIDENTLY_SEGMENT_TAGGED

Ressourcentypen: AWS::Evidently::Segment

Auslösertyp: Konfigurationsänderungen

AWS-Region: Nur in den Regionen Europa (Stockholm), USA Ost (Ohio), Europa (Irland), Europa (Frankfurt), USA Ost (Nord-Virginia), Asien-Pazifik (Tokio), USA West (Oregon), Asien-Pazifik (Singapur), Asien-Pazifik (Sydney) verfügbar

Parameter:

requiredKeyTags (Fakultativ), Typ: CSV

> Durch Kommas getrennte Liste von Tag-Schlüsseln, die von der Regel überprüft werden sollen. Falls angegeben, lautet die Regel NON_COMPLIANT, wenn die ausgewertete Ressource diese Schlüssel nicht enthält. Bei Tag-Schlüsseln wird die Groß- und Kleinschreibung beachtet. Tag-Schlüssel, die mit „aws:“ beginnen, sind nicht erlaubt.

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

fis-experiment-template-log-Konfiguration vorhanden

Prüft, ob in den AWS FIS-Versuchsvorlagen die Protokollierung von Experimenten konfiguriert ist. Bei der Konfiguration lautet die Regel NON_COMPLIANT. LogConfiguration ist nicht vorhanden.

Kennung: FIS_EXPERIMENT_TEMPLATE_LOG_CONFIGURATION_EXISTS

Ressourcentypen: AWS::FIS::ExperimentTemplate

Auslösertyp: Konfigurationsänderungen

AWS-Region: Alle unterstützten AWS Regionen außer China (Peking), Asien-Pazifik (Thailand), Asien-Pazifik (Jakarta), Naher Osten (VAE), Asien-Pazifik (Hyderabad), Asien-Pazifik (Osaka), Asien-Pazifik (Malaysia), Asien-Pazifik (Melbourne), AWS GovCloud (USA-Ost), AWS GovCloud (US-West), Mexiko (Zentral), Israel (Tel Aviv), Kanada West (Calgary), China (Ningxia), Europa (Zürich)

Parameter:

Keine

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

fis-experiment-template-tagged

Prüft, ob AWS FIS-Versuchsvorlagen Tags enthalten. Optional können Sie Tag-Schlüssel angeben. Die Regel lautet NON_COMPLIANT, wenn keine Tags vorhanden sind oder wenn die angegebenen Tag-Schlüssel nicht vorhanden sind. Die Regel sucht nicht nach Tags, die mit 'aws: 'beginnen.

Kennung: FIS_EXPERIMENT_TEMPLATE_TAGGED

Ressourcentypen: AWS::FIS::ExperimentTemplate

Auslösertyp: Konfigurationsänderungen

AWS-Region: Alle unterstützten AWS Regionen außer China (Peking), Asien-Pazifik (Thailand), Asien-Pazifik (Jakarta), Naher Osten (VAE), Asien-Pazifik (Hyderabad), Asien-Pazifik (Osaka), Asien-Pazifik (Malaysia), Asien-Pazifik (Melbourne), AWS GovCloud (USA-Ost), AWS GovCloud (US-West), Mexiko (Zentral), Israel (Tel Aviv), Kanada West (Calgary), China (Ningxia), Europa (Zürich)

Parameter:

requiredKeyTags (Fakultativ), Typ: CSV

Durch Kommas getrennte Liste von Tag-Schlüsseln, die von der Regel überprüft werden sollen. Falls angegeben, lautet die Regel NON_COMPLIANT, wenn die ausgewertete Ressource diese Schlüssel nicht enthält. Bei Tag-Schlüsseln wird die Groß- und Kleinschreibung beachtet. Tag-Schlüssel, die mit „aws:“ beginnen, sind nicht erlaubt.

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

fms-shield-resource-policy-überprüfen

Überprüft, ob Ressourcen, die AWS Shield Advanced schützen kann, durch Shield Advanced geschützt sind. Die Regel lautet NON_COMPLIANT, wenn eine angegebene Ressource nicht geschützt ist.

ID: FMS_SHIELD_RESOURCE_POLICY_CHECK

Ressourcentypen: AWS::CloudFront::Distribution, AWS::ElasticLoadBalancingV2::LoadBalancer, AWS::WAFRegional::WebACL,, AWS::EC2::EIP, AWS::ElasticLoadBalancing::LoadBalancer AWS::ShieldRegional::Protection AWS::Shield::Protection

Auslösertyp: Konfigurationsänderungen

AWS-Region: Alle unterstützten AWS Regionen außer China (Peking), Asien-Pazifik (Thailand), Asien-Pazifik (Jakarta), Asien-Pazifik (Malaysia), Mexiko (Zentral), Asien-Pazifik (Taipeh), Kanada West (Calgary), China (Ningxia)

Parameter:

Web ACLId, Typ: Zeichenfolge

Eine eindeutige Kennung für eine Web-ACL.

resourceTypes, Typ: Zeichenfolge

Die Ressourcentypen, die Sie für die zu prüfende Regel angeben.

resourceTags (optional), Typ: Zeichenfolge

Die Ressourcen-Tags, die Sie für die zu prüfende Regel angeben. Zum Beispiel {„tagKey1": [" tagValue1"], „tagKey2": [" tagValue2", „tagValue3"]}.

excludeResourceTags (Fakultativ), Typ: Boolesch

Falls wahr, schließt die Regel die in resourceTags angegebenen Ressourcen aus. Wenn der Wert falsch ist, umfasst die Regel alle in resourceTags Ressourcen.

fmsManagedToken (Fakultativ), Typ: Zeichenfolge

Ein Token, das von AWS Firewall Manager bei der Erstellung der Regel in Ihrem Konto generiert wurde. AWS Config ignoriert diesen Parameter, wenn Sie diese Regel erstellen.

fmsRemediationEnabled (Fakultativ), Typ: Boolesch

Falls wahr, aktualisiert AWS Firewall Manager die NON_COMPLIANT-Ressourcen gemäß der FMS-Richtlinie. AWS Config ignoriert diesen Parameter, wenn Sie diese Regel erstellen.

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

fms-webacl-resource-policy-überprüfen

Prüft, ob die Web-ACL mit einem Application Load Balancer, einer API Gateway Gateway-Stufe oder CloudFront Amazon-Distributionen verknüpft ist. Bei der AWS Firewall Manager Erstellung dieser Regel gibt der Eigentümer der FMS-Richtlinie das `WebACLId` in der FMS-Richtlinie an und kann optional die Problembehebung aktivieren.

ID: FMS_WEBACL_RESOURCE_POLICY_CHECK

Ressourcentypen: AWS::CloudFront::Distribution,,, AWS::ApiGateway::Stage AWS::ElasticLoadBalancingV2::LoadBalancer AWS::WAFRegional::WebACL

Auslösertyp: Konfigurationsänderungen

AWS-Region: Alle unterstützten AWS Regionen außer Asien-Pazifik (Thailand), Asien-Pazifik (Malaysia), Mexiko (Zentral), Asien-Pazifik (Taipeh) und Kanada West (Calgary)

Parameter:

Netz ACLId, Typ: Zeichenfolge

Das Web ACLId des Web-ACL.

resourceTags (optional), Typ: Zeichenfolge

Die Ressourcen-Tags (ApplicationLoadBalancer ApiGatewayStage und CloudFront Distributionen), denen die Regel zugeordnet werden soll. (zum Beispiel {„tagKey1": [" tagValue1"], „tagKey2": [" tagValue2", „tagValue3"]})

excludeResourceTags (Fakultativ), Typ: Boolesch

Wenn der Wert „true“ lautet, werden Ressourcen ausgeschlossen, die mit „resourceTags“ übereinstimmen.

fmsManagedToken (Fakultativ), Typ: Zeichenfolge

Ein Token, das von AWS Firewall Manager bei der Erstellung der Regel im Kundenkonto generiert wurde. AWS Config ignoriert diesen Parameter, wenn der Kunde diese Regel erstellt.

fmsRemediationEnabled (Fakultativ), Typ: Boolesch

Falls wahr, aktualisiert AWS Firewall Manager nicht konforme Ressourcen gemäß der FMS-Richtlinie. AWS Config ignoriert diesen Parameter, wenn der Kunde diese Regel erstellt.

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

fms-webacl-rulegroup-association-überprüfen

Prüft, ob die Regelgruppen der Web-ACL auf der richtigen Priorität zugeordnet werden. Die richtige Priorität wird über den Rang der Regelgruppen im Parameter "ruleGroups" bestimmt. Bei AWS Firewall Manager der Erstellung dieser Regel wird der höchsten Priorität 0 zugewiesen, gefolgt von 1, 2 usw. Der FMS-Richtlinienbesitzer gibt den `ruleGroups`-Rang in der FMS-Richtlinie an und kann optional Korrekturmaßnahmen ermöglichen.

ID: FMS_WEBACL_RULEGROUP_ASSOCIATION_CHECK

Ressourcentypen: AWS::WAF::WebACL, AWS::WAFRegional::WebACL

Auslösertyp: Konfigurationsänderungen

AWS-Region: Alle unterstützten AWS Regionen außer Asien-Pazifik (Thailand), Asien-Pazifik (Malaysia), Mexiko (Zentral), Asien-Pazifik (Taipeh) und Kanada West (Calgary)

Parameter:

ruleGroups, Typ: Zeichenfolge

Kommagetrennte Liste von und-Paaren. RuleGroupIds WafOverrideAction (zum Beispiel ruleGroupId -1:NONE, 2:COUNT) ruleGroupId

fmsManagedToken (Fakultativ), Typ: Zeichenfolge

Ein Token, das von AWS Firewall Manager bei der Erstellung der Regel im Kundenkonto generiert wurde. AWS Config ignoriert diesen Parameter, wenn der Kunde diese Regel erstellt.

fmsRemediationEnabled (Fakultativ), Typ: Boolesch

Falls wahr, aktualisiert AWS Firewall Manager nicht konforme Ressourcen gemäß der FMS-Richtlinie. AWS Config ignoriert diesen Parameter, wenn der Kunde diese Regel erstellt.

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

frauddetector-entity-type-tagged

Überprüft, ob die Entitätstypen von Amazon Fraud Detector Tags haben. Optional können Sie Tag-Schlüssel für die Regel angeben. Die Regel ist NON_COMPLIANT, wenn keine Tags vorhanden sind oder wenn die angegebenen Tag-Schlüssel nicht vorhanden sind. Die Regel sucht nicht nach Tags, die mit 'aws: 'beginnen.

Kennung: FRAUDDETECTOR_ENTITY_TYPE_TAGGED

Ressourcentypen: AWS::FraudDetector::EntityType

Auslösertyp: Konfigurationsänderungen

AWS-Region: Nur in den Regionen USA Ost (Ohio), Europa (Irland), USA Ost (Nord-Virginia), USA West (Oregon), Asien-Pazifik (Singapur), Asien-Pazifik (Sydney) verfügbar

Parameter:

requiredKeyTags (Fakultativ), Typ: CSV

Durch Kommas getrennte Liste von Tag-Schlüsseln, die von der Regel überprüft werden sollen. Falls angegeben, lautet die Regel NON_COMPLIANT, wenn die ausgewertete Ressource diese Schlüssel nicht enthält. Bei Tag-Schlüsseln wird die Groß- und Kleinschreibung beachtet. Tag-Schlüssel, die mit „aws:“ beginnen, sind nicht erlaubt.

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

frauddetector-label-tagged

Überprüft, ob die Labels von Amazon Fraud Detector Tags haben. Optional können Sie Tag-Schlüssel für die Regel angeben. Die Regel ist NON_COMPLIANT, wenn keine Tags vorhanden sind oder wenn die angegebenen Tag-Schlüssel nicht vorhanden sind. Die Regel sucht nicht nach Tags, die mit 'aws: 'beginnen.

Kennung: FRAUDDETECTOR_LABEL_TAGGED

Ressourcentypen: AWS::FraudDetector::Label

Auslösertyp: Konfigurationsänderungen

AWS-Region: Nur in den Regionen USA Ost (Ohio), Europa (Irland), USA Ost (Nord-Virginia), USA West (Oregon), Asien-Pazifik (Singapur), Asien-Pazifik (Sydney) verfügbar

Parameter:

requiredKeyTags (Fakultativ), Typ: CSV

> Durch Kommas getrennte Liste von Tag-Schlüsseln, die von der Regel überprüft werden sollen. Falls angegeben, lautet die Regel NON_COMPLIANT, wenn die ausgewertete Ressource diese Schlüssel nicht enthält. Bei Tag-Schlüsseln wird die Groß- und Kleinschreibung beachtet. Tag-Schlüssel, die mit „aws:“ beginnen, sind nicht erlaubt.

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

frauddetector-outcome-tagged

Überprüft, ob die Ergebnisse von Amazon Fraud Detector mit Tags versehen sind. Optional können Sie Tag-Schlüssel für die Regel angeben. Die Regel ist NON_COMPLIANT, wenn keine Tags vorhanden sind oder wenn die angegebenen Tag-Schlüssel nicht vorhanden sind. Die Regel sucht nicht nach Tags, die mit 'aws: 'beginnen.

Kennung: FRAUDDETECTOR_OUTCOME_TAGGED

Ressourcentypen: AWS::FraudDetector::Outcome

Auslösertyp: Konfigurationsänderungen

AWS-Region: Nur in den Regionen USA Ost (Ohio), Europa (Irland), USA Ost (Nord-Virginia), USA West (Oregon), Asien-Pazifik (Singapur), Asien-Pazifik (Sydney) verfügbar

Parameter:

requiredKeyTags (Fakultativ), Typ: CSV

> Durch Kommas getrennte Liste von Tag-Schlüsseln, die von der Regel überprüft werden sollen. Falls angegeben, lautet die Regel NON_COMPLIANT, wenn die ausgewertete Ressource diese Schlüssel nicht enthält. Bei Tag-Schlüsseln wird die Groß- und Kleinschreibung beachtet. Tag-Schlüssel, die mit „aws:“ beginnen, sind nicht erlaubt.

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

frauddetector-variable-tagged

Überprüft, ob die Variablen von Amazon Fraud Detector Tags haben. Optional können Sie Tag-Schlüssel für die Regel angeben. Die Regel ist NON_COMPLIANT, wenn keine Tags vorhanden sind oder wenn die angegebenen Tag-Schlüssel nicht vorhanden sind. Die Regel sucht nicht nach Tags, die mit 'aws: 'beginnen.

Kennung: FRAUDDETECTOR_VARIABLE_TAGGED

Ressourcentypen: AWS::FraudDetector::Variable

Auslösertyp: Konfigurationsänderungen

AWS-Region: Nur in den Regionen USA Ost (Ohio), Europa (Irland), USA Ost (Nord-Virginia), USA West (Oregon), Asien-Pazifik (Singapur), Asien-Pazifik (Sydney) verfügbar

Parameter:

requiredKeyTags (Fakultativ), Typ: CSV

Durch Kommas getrennte Liste von Tag-Schlüsseln, die von der Regel überprüft werden sollen. Falls angegeben, lautet die Regel NON_COMPLIANT, wenn die ausgewertete Ressource diese Schlüssel nicht enthält. Bei Tag-Schlüsseln wird die Groß- und Kleinschreibung beachtet. Tag-Schlüssel, die mit „aws:“ beginnen, sind nicht erlaubt.

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

fsx-last-backup-recovery-Punkt-erstellt

Prüft, ob ein Wiederherstellungspunkt für Amazon FSx File Systems erstellt wurde. Die Regel lautet NON_COMPLIANT, wenn für das FSx Amazon-Dateisystem innerhalb des angegebenen Zeitraums kein entsprechender Wiederherstellungspunkt erstellt wurde.

ID: FSX_LAST_BACKUP_RECOVERY_POINT_CREATED

Ressourcentypen: AWS::FSx::FileSystem

Auslösertyp: Regelmäßig

AWS-Region: Alle unterstützten AWS Regionen außer China (Peking), Asien-Pazifik (Thailand), Asien-Pazifik (Malaysia), Mexiko (Zentral), Israel (Tel Aviv), Kanada West (Calgary), China (Ningxia)

Parameter:

resourceTags (optional), Typ: Zeichenfolge

Tags von Amazon FSx File Systems für die zu prüfende Regel im JSON-Format`{"tagkey" : "tagValue"}`.

resourceId (optional), Typ: Zeichenfolge

ID des FSx Amazon-Dateisystems für die zu prüfende Regel.

recoveryPointAgeWert (optional), Typ: int, Standard: 1

Numerischer Wert für das zulässige Höchstalter. Nicht mehr als 744 für Stunden oder 31 für Tage.

recoveryPointAgeEinheit (optional), Typ: Zeichenfolge, Standard: days

Zeiteinheit für das zulässige Höchstalter. Zulässige Werte: „Stunden“, „Tage“.

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

fsx-lustre-copy-tagszu Backups

Prüft, ob die Amazon FSx for Lustre-Dateisysteme so konfiguriert sind, dass sie Tags in Backups kopieren. Die Regel ist NON_COMPLIANT, wenn Lustre-Dateisysteme nicht so konfiguriert sind, dass sie Tags in Backups kopieren.

ID: FSX_LUSTRE_COPY_TAGS_TO_BACKUPS

Ressourcentypen: AWS::FSx::FileSystem

Auslösertyp: Regelmäßig

AWS-Region: Alle unterstützten AWS Regionen außer China (Peking), Asien-Pazifik (Thailand), Asien-Pazifik (Malaysia), AWS GovCloud (USA-Ost), AWS GovCloud (US-West), Mexiko (Zentral), Kanada West (Calgary), China (Ningxia)

Parameter:

Keine

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

fsx-meets-restore-time-ziel

Prüft, ob die Wiederherstellungszeit von Amazon FSx File Systems der angegebenen Dauer entspricht. Die Regel lautet NON_COMPLIANT, wenn LatestRestoreExecutionTimeMinutes der Wert eines FSx Amazon-Dateisystems länger als maxRestoreTime Minuten ist.

Kennung: FSX_MEETS_RESTORE_TIME_TARGET

Ressourcentypen: AWS::FSx::FileSystem

Auslösertyp: Regelmäßig

AWS-Region: Alle unterstützten AWS Regionen außer China (Peking), Asien-Pazifik (Thailand), Asien-Pazifik (Malaysia), AWS GovCloud (USA-Ost), AWS GovCloud (US-West), Mexiko (Zentral), Israel (Tel Aviv), Kanada West (Calgary), China (Ningxia)

Parameter:

maxRestoreTime, Typ: int

Numerischer Wert für die maximal zulässige Wiederherstellungslaufzeit.

resourceTags (optional), Typ: Zeichenfolge

Tags von Amazon FSx File Systems für die zu prüfende Regel im JSON-Format.

resourceId (optional), Typ: Zeichenfolge

ID des FSx Amazon-Dateisystems für die zu prüfende Regel.

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

fsx-ontap-deployment-type-überprüfen

Überprüft, ob Amazon FSx for NetApp ONTAP-Dateisysteme mit bestimmten Bereitstellungstypen konfiguriert sind. Die Regel lautet NON_COMPLIANT, wenn die Amazon FSx for NetApp ONTAP-Dateisysteme nicht mit den von Ihnen angegebenen Bereitstellungstypen konfiguriert sind.

Kennung: FSX_ONTAP_DEPLOYMENT_TYPE_CHECK

Ressourcentypen: AWS::FSx::FileSystem

Auslösertyp: Regelmäßig

AWS-Region: Alle unterstützten AWS Regionen außer Naher Osten (Bahrain), Asien-Pazifik (Thailand), Asien-Pazifik (Malaysia), Mexiko (Zentral) und Kanada West (Calgary)

Parameter:

Bereitstellungstypen, Typ: CSV

Durch Kommas getrennte Liste der zulässigen Bereitstellungstypen, die von der Regel überprüft werden sollen.

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

fsx-openzfs-copy-tags-aktiviert

Überprüft, ob die Amazon FSx for OpenZFS-Dateisysteme so konfiguriert sind, dass sie Tags auf Backups und Volumes kopieren. Die Regel lautet NON_COMPLIANT, wenn die Dateisysteme FSx für OpenZFS nicht so konfiguriert sind, dass sie Tags auf Backups und Volumes kopieren.

ID: FSX_OPENZFS_COPY_TAGS_ENABLED

Ressourcentypen: AWS::FSx::FileSystem

Auslösertyp: Regelmäßig

AWS-Region: Alle unterstützten AWS Regionen außer China (Peking), Asien-Pazifik (Thailand), Asien-Pazifik (Malaysia), Asien-Pazifik (Melbourne), AWS GovCloud (USA Ost), AWS GovCloud (USA West), Mexiko (Zentral), Kanada West (Calgary), China (Ningxia)

Parameter:

Keine

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

fsx-openzfs-deployment-type-überprüfen

Überprüft, ob die Amazon FSx for OpenZFS-Dateisysteme mit bestimmten Bereitstellungstypen konfiguriert sind. Die Regel lautet NON_COMPLIANT, wenn die Dateisysteme FSx für OpenZFS nicht mit den von Ihnen angegebenen Bereitstellungstypen konfiguriert sind.

Kennung: FSX_OPENZFS_DEPLOYMENT_TYPE_CHECK

Ressourcentypen: AWS::FSx::FileSystem

Auslösertyp: Regelmäßig

AWS-Region: Alle unterstützten AWS Regionen außer Naher Osten (Bahrain), Asien-Pazifik (Thailand), Asien-Pazifik (Malaysia), Asien-Pazifik (Melbourne), Mexiko (Zentral) und Kanada West (Calgary)

Parameter:

Bereitstellungstypen, Typ: CSV

Durch Kommas getrennte Liste der zulässigen Bereitstellungstypen, die von der Regel überprüft werden sollen.

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

fsx-resources-protected-by-Backup-Plan

Prüft, ob Amazon FSx File Systems durch einen Backup-Plan geschützt sind. Die Regel lautet NON_COMPLIANT, wenn das FSx Amazon-Dateisystem nicht durch einen Backup-Plan abgedeckt ist.

ID: FSX_RESOURCES_PROTECTED_BY_BACKUP_PLAN

Ressourcentypen: AWS::FSx::FileSystem

Auslösertyp: Regelmäßig

AWS-Region: Alle unterstützten AWS Regionen außer China (Peking), Asien-Pazifik (Thailand), Asien-Pazifik (Malaysia), Mexiko (Zentral), Israel (Tel Aviv), Kanada West (Calgary), China (Ningxia)

Parameter:

resourceTags (optional), Typ: Zeichenfolge

Tags von Amazon FSx File Systems für die zu prüfende Regel im JSON-Format`{"tagkey" : "tagValue"}`.

resourceId (optional), Typ: Zeichenfolge

ID des FSx Amazon-Dateisystems, für das die Regel überprüft werden soll.

crossRegionList (Fakultativ), Typ: Zeichenfolge

Durch Kommata getrennte Liste der Zielregionen, für die die regionsübergreifende Backup-Kopie aufbewahrt werden soll.

crossAccountList (Fakultativ), Typ: Zeichenfolge

Durch Kommata getrennte Liste der Zielkonten, für die die kontoübergreifende Backup-Kopie aufbewahrt werden soll.

maxRetentionDays (Fakultativ), Typ: int

Die maximale Aufbewahrungsdauer in Tagen für die Backup-Tresorsperre.

minRetentionDays (Fakultativ), Typ: int

Die Mindestaufbewahrungsdauer in Tagen für die Backup-Tresorsperre.

backupVaultLockÜberprüfen Sie (fakultativ), Typ: Zeichenfolge

Akzeptierte Werte: „True“ oder „False“. Geben Sie „True“ ein, damit die Regel prüft, ob die Ressource in einem gesperrten Tresor gesichert ist.

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

fsx-windows-audit-log-konfiguriert

Prüft, ob in den Dateisystemen von Amazon FSx for Windows File Server die Dateizugriffsprüfung aktiviert ist. Die Regel lautet NON_COMPLIANT, wenn FSx für die Dateisysteme für Windows File Server keine Dateizugriffsüberwachung aktiviert ist.

ID: FSX_WINDOWS_AUDIT_LOG_CONFIGURED

Ressourcentypen: AWS::FSx::FileSystem

Auslösertyp: Regelmäßig

AWS-Region: Alle unterstützten AWS Regionen außer China (Peking), Asien-Pazifik (Thailand), Asien-Pazifik (Malaysia), Asien-Pazifik (Melbourne), AWS GovCloud (USA-Ost), AWS GovCloud (US-West), Mexiko (Zentral), Israel (Tel Aviv), Kanada West (Calgary), China (Ningxia)

Parameter:

Keine

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

fsx-windows-deployment-type-überprüfen

Überprüft, ob die Dateisysteme von Amazon FSx für WINDOWS mit bestimmten Bereitstellungstypen konfiguriert sind. Die Regel lautet NON_COMPLIANT, wenn Dateisysteme FSx für WINDOWS nicht mit den von Ihnen angegebenen Bereitstellungstypen konfiguriert sind.

Kennung: FSX_WINDOWS_DEPLOYMENT_TYPE_CHECK

Ressourcentypen: AWS::FSx::FileSystem

Auslösertyp: Regelmäßig

AWS-Region: Alle unterstützten AWS Regionen außer Naher Osten (Bahrain), China (Peking), Asien-Pazifik (Thailand), Europa (Paris), Asien-Pazifik (Malaysia), Mexiko (Zentral), Kanada West (Calgary), China (Ningxia)

Parameter:

Bereitstellungstypen, Typ: CSV

> Durch Kommas getrennte Liste der zulässigen Bereitstellungstypen, die von der Regel überprüft werden sollen.

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

glb-listener-tagged

Überprüft, ob Gateway Load Balancer-Listener Tags haben. Optional können Sie Tag-Schlüssel angeben. Die Regel lautet NON_COMPLIANT, wenn keine Tags vorhanden sind oder wenn die

angegebenen Tag-Schlüssel nicht vorhanden sind. Die Regel sucht nicht nach Tags, die mit 'aws: 'beginnen.

Kennung: GLB_LISTENER_TAGGED

Ressourcentypen: AWS::ElasticLoadBalancingV2::Listener

Auslösertyp: Konfigurationsänderungen

AWS-Region: Alle unterstützten AWS Regionen außer China (Peking), Asien-Pazifik (Thailand), Asien-Pazifik (Jakarta), Naher Osten (VAE), Asien-Pazifik (Hyderabad), Asien-Pazifik (Malaysia), Asien-Pazifik (Melbourne), AWS GovCloud (US-Ost), AWS GovCloud (US-West), Mexiko (Zentral), Israel (Tel Aviv), Kanada West (Calgary), Europa (Spanien), China (Ningxia), Europa (Zürich)

Parameter:

requiredKeyTags (Fakultativ), Typ: CSV

> Durch Kommas getrennte Liste von Tag-Schlüsseln, die von der Regel überprüft werden sollen. Falls angegeben, lautet die Regel NON_COMPLIANT, wenn die ausgewertete Ressource diese Schlüssel nicht enthält. Bei Tag-Schlüsseln wird die Groß- und Kleinschreibung beachtet. Tag-Schlüssel, die mit „aws:“ beginnen, sind nicht erlaubt.

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

global-endpoint-event-replication-aktiviert

Prüft, ob die Ereignisreplikation für EventBridge globale Amazon-Endpunkte aktiviert ist. Die Regel ist NON_COMPLIANT, wenn die Ereignisreplikation nicht aktiviert ist.

ID: GLOBAL_ENDPOINT_EVENT_REPLICATION_ENABLED

Ressourcentypen: AWS::Events::Endpoint

Auslösertyp: Konfigurationsänderungen

AWS-Region: Nur verfügbar in Europa (Stockholm), Asien-Pazifik (Mumbai), Europa (Paris), USA Ost (Ohio), Europa (Irland), Europa (Frankfurt), Südamerika (Sao Paulo), USA Ost (Nord-Virginia), Asien-Pazifik (Seoul), Asien-Pazifik (Osaka), Europa (London), Asien-Pazifik (Tokio), USA West (Oregon),

USA West (Nordkalifornien), Asien-Pazifik (Singapur), Asien-Pazifik (Asien-Pazifik) (Asien-Pazifik) Sydney), Region Kanada (Zentral)

Parameter:

Keine

AWS CloudFormation Schablone

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

glue-job-logging-enabled

Prüft, ob für einen AWS Glue-Job die Protokollierung aktiviert ist. Die Regel lautet NON_COMPLIANT, wenn für einen AWS Glue-Job keine CloudWatch Amazon-Logs aktiviert sind.

Kennung: GLUE_JOB_LOGGING_ENABLED

Ressourcentypen: AWS::Glue::Job

Auslösertyp: Konfigurationsänderungen

AWS-Region: Alle unterstützten AWS Regionen außer Asien-Pazifik (Thailand), Asien-Pazifik (Malaysia), Mexiko (Zentral) und Kanada West (Calgary)

Parameter:

Keine

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

glue-ml-transform-encrypted-im Ruhezustand

Prüft, ob für eine AWS Glue ML-Transformation die Verschlüsselung im Ruhezustand aktiviert ist. Die Regel ist NON_COMPLIANT, wenn `` auf MLUser DataEncryptionMode `DISABLED` gesetzt ist.

Kennung: GLUE_ML_TRANSFORM_ENCRYPTED_AT_REST

Ressourcentypen: AWS::Glue::MLTransform

Auslösertyp: Konfigurationsänderungen

AWS-Region: Alle unterstützten AWS Regionen außer Asien-Pazifik (Thailand), Asien-Pazifik (Malaysia), AWS GovCloud (USA-Ost), Mexiko (Zentral), Kanada West (Calgary), China (Ningxia)

Parameter:

Keine

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

glue-spark-job-supported-Ausführung

Prüft, ob ein AWS Glue Spark-Job auf der angegebenen unterstützten Mindestversion von AWS Glue ausgeführt wird. Die Regel lautet NON_COMPLIANT, wenn der AWS Glue Spark-Job nicht auf der von Ihnen angegebenen Mindestversion von AWS Glue ausgeführt wird.

Kennung: GLUE_SPARK_JOB_SUPPORTED_VERSION

Ressourcentypen: AWS::Glue::Job

Auslösertyp: Konfigurationsänderungen

AWS-Region: Alle unterstützten AWS Regionen außer Naher Osten (Bahrain), Asien-Pazifik (Thailand), Asien-Pazifik (Malaysia), Mexiko (Zentral) und Kanada West (Calgary)

Parameter:

minimumSupportedGlueAusführung, Typ: Zeichenfolge

> Zeichenkettenwert, den Sie für die unterstützte Mindestversion von AWS Glue angeben müssen, damit die Regel überprüft werden kann.

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

Schutzzoll-ec2- protection-runtime-enabled

Prüft, ob ECS Runtime Monitoring mit automatisierter Agentenverwaltung für Amazon GuardDuty Detector aktiviert ist. Die Regel lautet NON_COMPLIANT, wenn die Funktion für Ihr Konto oder mindestens ein Mitgliedskonto in Ihrer Organisation nicht aktiviert ist.

Kennung: GUARDDUTY_ _PROTECTION_RUNTIME_ENABLED EC2

Ressourcentypen: AWS::GuardDuty::Detector

Auslösertyp: Regelmäßig

AWS-Region: Alle unterstützten AWS Regionen außer Naher Osten (Bahrain), China (Peking), Asien-Pazifik (Thailand), Asien-Pazifik (Malaysia), AWS GovCloud (USA-Ost), AWS GovCloud (US-West), Mexiko (Zentral), Kanada West (Calgary), China (Ningxia)

Parameter:

Keine

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

guardduty-ecs-protection-runtime-aktiviert

Prüft, ob ECS Runtime Monitoring mit automatisierter Agentenverwaltung für Amazon GuardDuty Detector aktiviert ist. Die Regel lautet NON_COMPLIANT, wenn die Funktion für Ihr Konto oder mindestens ein Mitgliedskonto in Ihrer Organisation nicht aktiviert ist.

Kennung: GUARDDUTY_ECS_PROTECTION_RUNTIME_ENABLED

Ressourcentypen: AWS::GuardDuty::Detector

Auslösertyp: Regelmäßig

AWS-Region: Alle unterstützten AWS Regionen außer Naher Osten (Bahrain), China (Peking), Asien-Pazifik (Thailand), Asien-Pazifik (Malaysia), AWS GovCloud (USA-Ost), AWS GovCloud (US-West), Mexiko (Zentral), Kanada West (Calgary), China (Ningxia)

Parameter:

Keine

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

guardduty-eks-protection-audit-aktiviert

Prüft, ob Audit Log Monitoring für Amazon Elastic Kubernetes Service (Amazon EKS) für einen Amazon GuardDuty Detector in Ihrem Konto aktiviert ist. Die Regel lautet NON_COMPLIANT, wenn die EKS-Funktion Audit Log Monitoring für Ihr Konto nicht aktiviert ist.

Kennung: GUARDDUTY_EKS_PROTECTION_AUDIT_ENABLED

Ressourcentypen: AWS::GuardDuty::Detector

Auslösertyp: Regelmäßig

AWS-Region: Alle unterstützten AWS Regionen außer China (Peking), Asien-Pazifik (Thailand), Asien-Pazifik (Malaysia), Mexiko (Zentral), Kanada West (Calgary), China (Ningxia)

Parameter:

Keine

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

guardduty-eks-protection-runtime-aktiviert

Prüft, ob Amazon EKS Runtime Monitoring mit automatisierter Agentenverwaltung für GuardDuty Detektor in Ihrem Konto aktiviert ist. Die Regel lautet NON_COMPLIANT, wenn EKS Runtime Monitoring mit aktivierter automatisierter Agentenverwaltung für Ihr Konto nicht aktiviert GuardDuty ist.

Kennung: GUARDDUTY_EKS_PROTECTION_RUNTIME_ENABLED

Ressourcentypen: AWS::GuardDuty::Detector

Auslösertyp: Regelmäßig

AWS-Region: Alle unterstützten AWS Regionen außer China (Peking), Asien-Pazifik (Thailand), Asien-Pazifik (Malaysia), AWS GovCloud (USA-Ost), AWS GovCloud (US-West), Mexiko (Zentral), Kanada West (Calgary), China (Ningxia)

Parameter:

Keine

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

guardduty-enabled-centralized

Prüft, ob Amazon in Ihrem AWS Konto und Ihrer AWS Region aktiviert GuardDuty ist. Wenn Sie ein AWS Konto für die Zentralisierung angeben, wertet die Regel die GuardDuty Ergebnisse im zentralisierten Konto aus. Die Regel ist KONFORM, wenn sie aktiviert GuardDuty ist.

ID: GUARDDUTY_ENABLED_CENTRALIZED

Auslösertyp: Regelmäßig

AWS-Region: Alle unterstützten AWS Regionen außer Asien-Pazifik (Thailand), Mexiko (Zentral) und Asien-Pazifik (Taipeh)

Parameter:

CentralMonitoringAccount (Fakultativ), Typ: Zeichenfolge

> Durch Kommas getrennte Liste von AWS Konten (12-stellig), für die GuardDuty Amazon-Ergebnisse zentralisiert werden dürfen.

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

guardduty-lambda-protection-enabled

Prüft, ob Lambda Protection für einen GuardDuty Amazon-Detektor in Ihrem Konto aktiviert ist. Die Regel lautet NON_COMPLIANT, wenn die Lambda Protection-Funktion in Amazon für GuardDuty Ihr Konto nicht aktiviert ist.

Kennung: GUARDDUTY_LAMBDA_PROTECTION_ENABLED

Ressourcentypen: AWS::GuardDuty::Detector

Auslösertyp: Regelmäßig

AWS-Region: Alle unterstützten AWS Regionen außer China (Peking), Asien-Pazifik (Thailand), Asien-Pazifik (Malaysia), Mexiko (Zentral), Kanada West (Calgary), China (Ningxia)

Parameter:

Keine

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

guardduty-malware-protection-enabled

Prüft, ob der Malware-Schutz für einen GuardDuty Amazon-Detektor in Ihrem Konto aktiviert ist. Die Regel lautet NON_COMPLIANT, wenn die Malware-Schutzfunktion von Amazon für Ihr Konto nicht aktiviert GuardDuty ist.

Kennung: GUARDDUTY_MALWARE_PROTECTION_ENABLED

Ressourcentypen: AWS::GuardDuty::Detector

Auslösertyp: Regelmäßig

AWS-Region: Alle unterstützten AWS Regionen außer China (Peking), Asien-Pazifik (Thailand), Asien-Pazifik (Malaysia), AWS GovCloud (USA-Ost), AWS GovCloud (US-West), Mexiko (Zentral), Kanada West (Calgary), China (Ningxia)

Parameter:

Keine

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

guardduty-non-archived-findings

Prüft, ob Amazon GuardDuty über Ergebnisse verfügt, die nicht archiviert sind. Die Regel lautet NON_COMPLIANT, wenn der Parameter „/“ nicht GuardDuty low/medium/high severity findings older than the specified number in the daysLowSev/daysMediumSev archiviert ist. `daysHighSev`

Bezeichner: GUARDDUTY_NON_ARCHIVED_FINDINGS

Auslösertyp: Regelmäßig

AWS-Region: Alle unterstützten AWS Regionen außer Asien-Pazifik (Thailand), Mexiko (Zentral) und Asien-Pazifik (Taipeh)

Parameter:

daysLowSev (Fakultativ), Typ: int, Standard: 30

Die Anzahl der Tage, an denen Amazon-Ergebnisse mit GuardDuty geringem Schweregrad nicht archiviert werden dürfen. Der Standardwert ist 30 Tage.

daysMediumSev (Fakultativ), Typ: int, Standard: 7

Die Anzahl der Tage, an denen Amazon-Ergebnisse mit GuardDuty mittlerem Schweregrad nicht archiviert werden dürfen. Der Standardwert ist 7 Tage.

daysHighSev (Fakultativ), Typ: int, Standard: 1

Die Anzahl der Tage, an denen Amazon-Ergebnisse mit GuardDuty hohem Schweregrad nicht archiviert werden dürfen. Der Standardwert ist 1 Tag.

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

guardduty-rds-protection-enabled

Überprüft, ob der Amazon Relational Database Service (Amazon RDS) -Schutz für einen GuardDuty Amazon-Detektor in Ihrem Konto aktiviert ist. Die Regel lautet NON_COMPLIANT, wenn die Amazon RDS-Schutzfunktion in Amazon für Ihr Konto nicht aktiviert GuardDuty ist.

Kennung: GUARDDUTY_RDS_PROTECTION_ENABLED

Ressourcentypen: AWS::GuardDuty::Detector

Auslösertyp: Regelmäßig

AWS-Region: Alle unterstützten AWS Regionen außer China (Peking), Asien-Pazifik (Thailand), Asien-Pazifik (Malaysia), AWS GovCloud (USA-Ost), AWS GovCloud (US-West), Mexiko (Zentral), Kanada West (Calgary), China (Ningxia)

Parameter:

Keine

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

guardduty-runtime-monitoring-enabled

Prüft, ob Runtime Monitoring für Amazon GuardDuty Detector in Ihrem Konto oder Ihrer Organisation aktiviert ist. Die Regel lautet NON_COMPLIANT, wenn Runtime Monitoring in für Ihr Konto oder mindestens ein Mitgliedskonto in Ihrer Organisation nicht aktiviert GuardDuty ist.

Kennung: GUARDDUTY_RUNTIME_MONITORING_ENABLED

Ressourcentypen: AWS::GuardDuty::Detector

Auslösertyp: Regelmäßig

AWS-Region: Alle unterstützten AWS Regionen außer Naher Osten (Bahrain), China (Peking), Asien-Pazifik (Thailand), Asien-Pazifik (Malaysia), AWS GovCloud (USA-Ost), AWS GovCloud (US-West), Mexiko (Zentral), Kanada West (Calgary), China (Ningxia)

Parameter:

Keine

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

GuardDuty-S3-Schutz aktiviert

Prüft, ob S3 Protection für einen Amazon GuardDuty Detector in Ihrem Konto aktiviert ist. Die Regel lautet NON_COMPLIANT, wenn die S3-Schutzfunktion in Amazon für Ihr Konto nicht aktiviert GuardDuty ist.

Kennung: GUARDDUTY_S3_PROTECTION_ENABLED

Ressourcentypen: AWS::GuardDuty::Detector

Auslösertyp: Regelmäßig

AWS-Region: Alle unterstützten AWS Regionen außer China (Peking), Asien-Pazifik (Thailand), Asien-Pazifik (Malaysia), Mexiko (Zentral), Kanada West (Calgary), China (Ningxia)

Parameter:

Keine

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

iam-customer-policy-blocked-kms-Aktionen

Überprüft, ob die verwalteten AWS Identity and Access Management (IAM) -Richtlinien, die Sie erstellen, keine blockierten KMS-Aktionen für alle AWS KMS-Schlüsselressourcen zulassen. Die Regel lautet NON_COMPLIANT, wenn eine blockierte Aktion gemäß der verwalteten IAM-Richtlinie für alle AWS KMS-Schlüssel zulässig ist.

> **Note**
>
> Um als nicht öffentlich zu gelten, darf eine IAM-Richtlinie nur Zugriff auf feste Werte gewähren. Das bedeutet Werte, die keinen Platzhalter oder das folgende IAM-Richtlinienelement enthalten: Variablen.

ID: IAM_CUSTOMER_POLICY_BLOCKED_KMS_ACTIONS

Ressourcentypen: AWS::IAM::Policy

Auslösertyp: Konfigurationsänderungen

AWS-Region: Alle unterstützten AWS Regionen außer Asien-Pazifik (Thailand), Naher Osten (VAE), Asien-Pazifik (Hyderabad), Asien-Pazifik (Malaysia), Asien-Pazifik (Melbourne), Mexiko (Zentral), Israel (Tel Aviv), Asien-Pazifik (Taipeh), Kanada West (Calgary), Europa (Spanien), Europa (Zürich)

Parameter:

blockedActionsPatterns, Typ: CSV

Durch Kommas getrennte Liste blockierter KMS-Aktionsmuster, die von der Regel überprüft werden sollen. Die Regel lautet NON_COMPLIANT, wenn vom Kunden verwaltete IAM-Richtlinien Platzhalterzugriff auf alle Ressourcen für die von Ihnen angegebenen Aktionen zulassen.

excludePermissionBoundaryRichtlinie (optional), Typ: Boolesch

Boolesche Markierung, um die Auswertung von IAM-Richtlinien auszuschließen, die als Berechtigungsgrenzen verwendet werden. Wenn dieser Wert auf „True“ festgelegt ist, bezieht die Regel keine Berechtigungsgrenzen in die Auswertung mit ein. Andernfalls werden alle IAM-Richtlinien im Gültigkeitsbereich ausgewertet, wenn der Wert auf „False“ gesetzt ist. Der Standardwert ist „False“.

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

iam-external-access-analyzer-aktiviert

Prüft pro Region, ob in Ihrem Konto ein IAM Access Analyzer für externen Zugriff aktiviert ist. Die Regel lautet NON_COMPLIANT, wenn es in der Region keine Analysatoren für externen Zugriff gibt oder wenn das Attribut 'status' nicht auf 'ACTIVE' gesetzt ist.

Kennung: IAM_EXTERNAL_ACCESS_ANALYZER_ENABLED

Ressourcentypen: AWS::::Account

Auslösertyp: Regelmäßig

AWS-Region: Alle unterstützten AWS Regionen außer China (Peking), Asien-Pazifik (Thailand), Asien-Pazifik (Malaysia), AWS GovCloud (USA-Ost), AWS GovCloud (US-West), Mexiko (Zentral), Israel (Tel Aviv), Kanada West (Calgary), China (Ningxia)

Parameter:

Keine

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

iam-group-has-users-überprüfen

Prüft, ob IAM-Gruppen über mindestens einen IAM-Benutzer verfügen.

ID: IAM_GROUP_HAS_USERS_CHECK

Ressourcentypen: AWS::IAM::Group

Auslösertyp: Konfigurationsänderungen

AWS-Region: Alle unterstützten AWS Regionen außer Asien-Pazifik (Thailand), Naher Osten (VAE), Asien-Pazifik (Hyderabad), Asien-Pazifik (Malaysia), Asien-Pazifik (Melbourne), Mexiko (Zentral), Israel (Tel Aviv), Asien-Pazifik (Taipeh), Kanada West (Calgary), Europa (Spanien), Europa (Zürich)

Parameter:

Keine

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

iam-inline-policy-blocked-kms-Aktionen

Überprüft, ob die Ihren IAM-Benutzern, -Rollen und -Gruppen zugewiesenen Inline-Richtlinien keine blockierten Aktionen für alle AWS KMS-Schlüssel zulassen. Die Regel lautet NON_COMPLIANT, wenn eine blockierte Aktion für alle AWS KMS-Schlüssel in einer Inline-Richtlinie zulässig ist.

ID: IAM_INLINE_POLICY_BLOCKED_KMS_ACTIONS

Ressourcentypen: AWS::IAM::Group,, AWS::IAM::Role AWS::IAM::User

Auslösertyp: Konfigurationsänderungen

AWS-Region: Alle unterstützten AWS Regionen außer Asien-Pazifik (Thailand), Naher Osten (VAE), Asien-Pazifik (Hyderabad), Asien-Pazifik (Malaysia), Asien-Pazifik (Melbourne), Mexiko (Zentral), Israel (Tel Aviv), Asien-Pazifik (Taipeh), Kanada West (Calgary), Europa (Spanien), Europa (Zürich)

Parameter:

blockedActionsPatterns, Typ: CSV

Durch Kommas getrennte Liste blockierter KMS-Aktionsmuster, z. B. *, Decrypt, kms: kms: *. kms: ReEncrypt

excludeRoleByManagementAccount (Fakultativ), Typ: Boolesch

Schließt eine Rolle aus, wenn sie nur vom Verwaltungskonto der Organisation übernommen werden kann.

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

iam-no-inline-policy-überprüfen

Prüft, ob die Funktion der eingebundenen Richtlinien nicht in Gebrauch ist. Die Regel lautet NON_COMPLIANT, wenn ein AWS Identity and Access Management (IAM) -Benutzer, eine IAM-Rolle oder eine IAM-Gruppe über eine Inline-Richtlinie verfügt.

ID: IAM_NO_INLINE_POLICY_CHECK

Ressourcentypen:,, AWS::IAM::User AWS::IAM::Role AWS::IAM::Group

Auslösertyp: Konfigurationsänderungen

AWS-Region: Alle unterstützten AWS Regionen außer Asien-Pazifik (Thailand), Naher Osten (VAE), Asien-Pazifik (Hyderabad), Asien-Pazifik (Malaysia), Asien-Pazifik (Melbourne), Mexiko (Zentral), Israel (Tel Aviv), Asien-Pazifik (Taipeh), Kanada West (Calgary), Europa (Spanien), Europa (Zürich)

Parameter:

Keine

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

iam-oidc-provider-tagged

Prüft, ob AWS IAM-OIDC-Anbieter über Tags verfügen. Optional können Sie Tag-Schlüssel angeben. Die Regel lautet NON_COMPLIANT, wenn keine Tags vorhanden sind oder wenn die angegebenen Tag-Schlüssel nicht vorhanden sind. Die Regel sucht nicht nach Tags, die mit 'aws: 'beginnen.

Kennung: IAM_OIDC_PROVIDER_TAGGED

Ressourcentypen: AWS::IAM::OIDCProvider

Auslösertyp: Konfigurationsänderungen

AWS-Region: Nur in der Region USA Ost (Nord-Virginia) verfügbar

Parameter:

requiredKeyTags (Fakultativ), Typ: CSV

> Durch Kommas getrennte Liste von Tag-Schlüsseln, die von der Regel überprüft werden sollen. Falls angegeben, lautet die Regel NON_COMPLIANT, wenn die ausgewertete Ressource diese Schlüssel nicht enthält. Bei Tag-Schlüsseln wird die Groß- und Kleinschreibung beachtet. Tag-Schlüssel, die mit „aws:“ beginnen, sind nicht erlaubt.

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

iam-password-policy

Überprüft, ob die Kontokennwortrichtlinie für AWS Identity and Access Management (IAM) -Benutzer die in den Parametern angegebenen Anforderungen erfüllt. Die Regel ist NON_COMPLIANT, wenn die Kontokennwortrichtlinie die angegebenen Anforderungen nicht erfüllt.

> **Important**
>
> Bei den Werten `true` und `false` für die Regelparameter wird zwischen Groß- und Kleinschreibung unterschieden. Wenn `true` nicht in Kleinbuchstaben angegeben wird, wird es wie `false.` behandelt.

> **Note**
>
> Ergebnis der Evaluierung der Standard-IAM-Passwortrichtlinie
> Diese Regel wird als NON_COMPLIANT markiert, wenn die standardmäßige IAM-Passwortrichtlinie verwendet wird.
> Verwaltete Regeln und globale IAM-Ressourcentypen
> Die globalen IAM-Ressourcentypen, die vor Februar 2022 eingeführt wurden (`AWS::IAM::Group`,, und`AWS::IAM::User`) `AWS::IAM::Policy`AWS::IAM::Role, können nur AWS Config in AWS Regionen erfasst werden, in denen sie vor Februar 2022 verfügbar AWS Config waren. Diese Ressourcentypen können nicht in Regionen erfasst werden, die AWS Config nach Februar 2022 unterstützt werden. Eine Liste dieser Regionen finden Sie unter AWS Aufzeichnungsressourcen | Globale Ressourcen.
> Wenn Sie einen globalen IAM-Ressourcentyp in mindestens einer Region aufzeichnen, führen periodische Regeln, die die Einhaltung des globalen IAM-Ressourcentyps melden, Bewertungen in allen Regionen durch, in denen die periodische Regel hinzugefügt wurde, auch wenn Sie die Aufzeichnung des globalen IAM-Ressourcentyps in der Region, in der die periodische Regel hinzugefügt wurde, nicht aktiviert haben.
> Um unnötige Bewertungen zu vermeiden, sollten Sie nur regelmäßige Regeln einrichten, die die Einhaltung der Vorschriften für einen globalen IAM-Ressourcentyp an eine der unterstützten Regionen melden. Eine Liste der verwalteten Regeln, die in welchen Regionen

unterstützt werden, finden Sie unter Liste der AWS Config verwalteten Regeln nach regionaler Verfügbarkeit.

ID: IAM_PASSWORD_POLICY

Auslösertyp: Regelmäßig

AWS-Region: Alle unterstützten AWS Regionen außer Israel (Tel Aviv), Asien-Pazifik (Taipeh) und Kanada West (Calgary)

Parameter:

RequireUppercaseCharacters (Fakultativ), Typ: Boolesch, Standard: true

Verlangen Sie mindestens einen Großbuchstaben im Passwort.

RequireLowercaseCharacters (Fakultativ), Typ: Boolesch, Standard: true

Verlangen Sie mindestens einen Kleinbuchstaben im Passwort.

RequireSymbols (Fakultativ), Typ: Boolesch, Standard: true

Verlangen Sie mindestens ein Symbol im Passwort.

RequireNumbers (Fakultativ), Typ: Boolesch, Standard: true

Verlangen Sie mindestens eine Zahl im Passwort.

MinimumPasswordLength (Fakultativ), Typ: int, Standard: 14

Mindestpasswortlänge.

PasswordReusePrevention (Fakultativ), Typ: int, Standard: 24

Anzahl der Passwörter vor der Wiederverwendung.

MaxPasswordAge (Fakultativ), Typ: int, Standard: 90

Anzahl der Tage vor Ablauf des Passworts.

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

iam-policy-blacklisted-check

Prüft jede AWS Identity and Access Management (IAM) -Ressource, ob der IAM-Ressource eine Richtlinie mit dem Amazon Resource Name (ARN) im Eingabeparameter zugewiesen ist. Die Regel ist NON_COMPLIANT, wenn der Richtlinien-ARN an die IAM-Ressource angehängt ist.

ID: IAM_POLICY_BLACKLISTED_CHECK

Ressourcentypen: AWS::IAM::User,, AWS::IAM::Group AWS::IAM::Role

Auslösertyp: Konfigurationsänderungen

AWS-Region: Alle unterstützten AWS Regionen außer Asien-Pazifik (Thailand), Naher Osten (VAE), Asien-Pazifik (Hyderabad), Asien-Pazifik (Malaysia), Asien-Pazifik (Melbourne), Mexiko (Zentral), Israel (Tel Aviv), Asien-Pazifik (Taipeh), Kanada West (Calgary), Europa (Spanien), Europa (Zürich)

Parameter:

policyArns, Typ: CSV, Standard: arn:aws:iam: :aws:policy/ AdministratorAccess

Durch Kommata getrennte Liste der IAM-Richtlinien-ARN, die keiner IAM-Entität angehängt werden sollen.

exceptionList (optional), Typ: CSV

Durch Kommas getrennte Liste von Ressourcentypen und Liste von Ressourcennamenpaaren. Beispiel: "Benutzer:[user1;user2], Gruppen:[group1;group2], Rollen:[role1;role2;role3]".

> **Note**
>
> Geben Sie für die Ausnahmeliste den Namen der Ressource und nicht den vollständigen ARN an. Nicht gültig:`arn:aws:iam::444455556666:role/Admin`. Gültig:`Admin`.

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

iam-policy-in-use

Prüft, ob der IAM-Richtlinien-ARN einem IAM-Benutzer oder einer IAM-Gruppe mit einem oder mehreren IAM-Benutzern oder einer IAM-Rolle mit einer oder mehreren vertrauenswürdigen Entitäten zugeordnet ist.

> **Note**
>
> Verwaltete Regeln und globale IAM-Ressourcentypen
> Die globalen IAM-Ressourcentypen, die vor Februar 2022 eingeführt wurden (`AWS::IAM::Group`,, und`AWS::IAM::User`) `AWS::IAM::Policy``AWS::IAM::Role`, können nur AWS Config in AWS Regionen erfasst werden, in denen sie vor Februar 2022 verfügbar AWS Config waren. Diese Ressourcentypen können nicht in Regionen erfasst werden, die AWS Config nach Februar 2022 unterstützt werden. Eine Liste dieser Regionen finden Sie unter AWS Aufzeichnungsressourcen | Globale Ressourcen.
> Wenn Sie einen globalen IAM-Ressourcentyp in mindestens einer Region aufzeichnen, führen periodische Regeln, die die Einhaltung des globalen IAM-Ressourcentyps melden, Bewertungen in allen Regionen durch, in denen die periodische Regel hinzugefügt wurde, auch wenn Sie die Aufzeichnung des globalen IAM-Ressourcentyps in der Region, in der die periodische Regel hinzugefügt wurde, nicht aktiviert haben.
> Um unnötige Bewertungen zu vermeiden, sollten Sie nur regelmäßige Regeln einrichten, die die Einhaltung der Vorschriften für einen globalen IAM-Ressourcentyp an eine der unterstützten Regionen melden. Eine Liste der verwalteten Regeln, die in welchen Regionen unterstützt werden, finden Sie unter Liste der AWS Config verwalteten Regeln nach regionaler Verfügbarkeit.

Kennung: IAM_POLICY_IN_USE

Ressourcentypen: AWS::IAM::Policy

Auslösertyp: Regelmäßig

AWS-Region: Alle unterstützten AWS Regionen außer Asien-Pazifik (Thailand), Naher Osten (VAE), Asien-Pazifik (Hyderabad), Asien-Pazifik (Malaysia), Asien-Pazifik (Melbourne), Mexiko (Zentral), Israel (Tel Aviv), Asien-Pazifik (Taipeh), Kanada West (Calgary), Europa (Spanien), Europa (Zürich)

Parameter:

policyARN, Typ: Zeichenfolge

Ein zu überprüfender ARN einer IAM-Richtlinie.

policyUsageType (Fakultativ), Typ: Zeichenfolge

Geben Sie an, ob die Richtlinie einem IAM-Benutzer, einer IAM-Gruppe oder einer IAM-Rolle angefügt werden soll. Gültige Werte sind IAM_USER, IAM_GROUP, IAM_ROLE oder ANY. Der Standardwert ist ANY.

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

iam-policy-no-statements-with-admin-access

Überprüft, ob die von Ihnen erstellten AWS Identity and Access Management (IAM) -Richtlinien über Zulassungsanweisungen verfügen, die Berechtigungen für alle Aktionen auf allen Ressourcen gewähren. Die Regel ist NON_COMPLIANT, wenn eine vom Kunden verwaltete IAM-Richtlinienanweisung „Effekt“: „Erlauben“ mit „Aktion“: „*“ über „Ressource“: „*“ enthält.

> **Note**
>
> Diese Regel bewertet nur vom Kunden verwaltete Richtlinien. Diese Regel bewertet KEINE Inline-Richtlinien oder AWS verwalteten Richtlinien. Weitere Informationen zum Unterschied finden Sie unter Verwaltete Richtlinien und Inline-Richtlinien im IAM-Benutzerhandbuch.

Die folgende Richtlinie ist NON_COMPLIANT:

```
"Statement": [
{
"Sid": "VisualEditor",
"Effect": "Allow",
"Action": "*",
"Resource": "*"
}
```

Die folgende Richtlinie ist COMPLIANT:

```
"Statement": [
{
"Sid": "VisualEditor",
"Effect": "Allow",
"Action": "service:*",
"Resource": "*"
}
```

ID: IAM_POLICY_NO_STATEMENTS_WITH_ADMIN_ACCESS

Ressourcentypen: AWS::IAM::Policy

Auslösertyp: Konfigurationsänderungen

AWS-Region: Alle unterstützten AWS Regionen außer Asien-Pazifik (Thailand), Naher Osten (VAE), Asien-Pazifik (Hyderabad), Asien-Pazifik (Malaysia), Asien-Pazifik (Melbourne), Mexiko (Zentral), Israel (Tel Aviv), Asien-Pazifik (Taipeh), Kanada West (Calgary), Europa (Spanien), Europa (Zürich)

Parameter:

excludePermissionBoundaryRichtlinie (optional), Typ: Boolesch

> Boolesche Markierung, um die Auswertung von IAM-Richtlinien auszuschließen, die als Berechtigungsgrenzen verwendet werden. Wenn dieser Wert auf „True“ festgelegt ist, bezieht die Regel keine Berechtigungsgrenzen in die Auswertung mit ein. Andernfalls werden alle IAM-Richtlinien im Gültigkeitsbereich ausgewertet, wenn der Wert auf „False“ gesetzt ist. Der Standardwert ist „False“.

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

iam-policy-no-statements-with-full-access

Überprüft, ob von Ihnen erstellte AWS Identity and Access Management (IAM) -Richtlinien Berechtigungen für alle Aktionen auf einzelnen AWS Ressourcen gewähren. Die Regel lautet NON_COMPLIANT, wenn eine vom Kunden verwaltete IAM-Richtlinie vollen Zugriff auf mindestens einen Dienst gewährt. AWS

Kontext: Gemäß dem Prinzip der geringsten Rechte wird empfohlen, bei der Erteilung von Berechtigungen für Dienste die zulässigen Aktionen in Ihren IAM-Richtlinien einzuschränken. AWS Mit diesem Ansatz können Sie sicherstellen, dass Sie nur die erforderlichen Berechtigungen gewähren, indem Sie genau die erforderlichen Aktionen angeben und so die Verwendung uneingeschränkter Platzhalter für einen Dienst vermeiden, wie z. `ec2:*`

In einigen Fällen möchten Sie möglicherweise mehrere Aktionen mit einem ähnlichen Präfix zulassen, z. B. DescribeFlowLogsund. DescribeAvailabilityZones In diesen Fällen können Sie dem gemeinsamen Präfix einen Platzhalter mit Suffix hinzufügen (z. B.). `ec2:Describe*` Durch das Gruppieren verwandter Aktionen kann verhindert werden, dass die Größenbeschränkungen der IAM-Richtlinie überschritten werden.

Diese Regel gibt COMPLIANT zurück, wenn Sie Aktionen mit einem Platzhalter als Präfix verwenden (z. B.). `ec2:Describe*` Diese Regel gibt nur dann NON_COMPLIANT zurück, wenn Sie uneingeschränkte Platzhalter verwenden (z. B.). `ec2:*`

> **Note**
>
> Diese Regel bewertet nur vom Kunden verwaltete Richtlinien. Diese Regel bewertet KEINE Inline-Richtlinien oder verwalteten Richtlinien. AWS Weitere Informationen zum Unterschied finden Sie unter Verwaltete Richtlinien und Inline-Richtlinien im IAM-Benutzerhandbuch.

ID: IAM_POLICY_NO_STATEMENTS_WITH_FULL_ACCESS

Ressourcentypen: AWS::IAM::Policy

Auslösertyp: Konfigurationsänderungen

AWS-Region: Alle unterstützten AWS Regionen außer Asien-Pazifik (Thailand), Naher Osten (VAE), Asien-Pazifik (Hyderabad), Asien-Pazifik (Malaysia), Asien-Pazifik (Melbourne), Mexiko (Zentral), Israel (Tel Aviv), Asien-Pazifik (Taipeh), Kanada West (Calgary), Europa (Spanien), Europa (Zürich)

Parameter:

excludePermissionBoundaryRichtlinie (optional), Typ: Boolesch

> Boolesche Markierung, um die Auswertung von IAM-Richtlinien auszuschließen, die als Berechtigungsgrenzen verwendet werden. Wenn dieser Wert auf „True“ festgelegt ist, bezieht die Regel keine Berechtigungsgrenzen in die Auswertung mit ein. Andernfalls werden alle

IAM-Richtlinien im Gültigkeitsbereich ausgewertet, wenn der Wert auf „False“ gesetzt ist. Der Standardwert ist „False“.

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

iam-role-managed-policy-überprüfen

Überprüft, ob alle in der Liste der verwalteten Richtlinien angegebenen verwalteten Richtlinien der Rolle AWS Identity and Access Management (IAM) zugeordnet sind. Die Regel ist NON_COMPLIANT, wenn eine verwaltete Richtlinie nicht an die IAM-Rolle angefügt ist.

ID: IAM_ROLE_MANAGED_POLICY_CHECK

Ressourcentypen: AWS::IAM::Role

Auslösertyp: Konfigurationsänderungen

AWS-Region: Alle unterstützten AWS Regionen außer Asien-Pazifik (Thailand), Naher Osten (VAE), Asien-Pazifik (Hyderabad), Asien-Pazifik (Malaysia), Asien-Pazifik (Melbourne), Mexiko (Zentral), Israel (Tel Aviv), Asien-Pazifik (Taipeh), Kanada West (Calgary), Europa (Spanien), Europa (Zürich)

Parameter:

managedPolicyArns, Typ: CSV

Durch Kommas getrennte Liste AWS verwalteter Richtlinien Amazon Resource Names ()ARNs. Weitere Informationen finden Sie unter Amazon Resource Names (ARNs) und AWS verwaltete Richtlinien im IAM-Benutzerhandbuch.

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

iam-root-access-key-überprüfen

Prüft, ob der Zugriffsschlüssel des Root-Benutzers verfügbar ist. Die Regel ist COMPLIANT, wenn der Benutzer-Zugriffsschlüssel nicht vorhanden ist. Andernfalls ist sie NON_COMPLIANT.

> **Note**
>
> Verwaltete Regeln und globale IAM-Ressourcentypen
>
> Die globalen IAM-Ressourcentypen, die vor Februar 2022 eingeführt wurden (`AWS::IAM::Group`,, und`AWS::IAM::User`) `AWS::IAM::Policy``AWS::IAM::Role`, können nur AWS Config in AWS Regionen erfasst werden, in denen sie vor Februar 2022 verfügbar AWS Config waren. Diese Ressourcentypen können nicht in Regionen erfasst werden, die AWS Config nach Februar 2022 unterstützt werden. Eine Liste dieser Regionen finden Sie unter AWS Ressourcen für die Aufzeichnung | Globale Ressourcen.
>
> Wenn Sie einen globalen IAM-Ressourcentyp in mindestens einer Region aufzeichnen, führen periodische Regeln, die die Einhaltung des globalen IAM-Ressourcentyps melden, Bewertungen in allen Regionen durch, in denen die periodische Regel hinzugefügt wurde, auch wenn Sie die Aufzeichnung des globalen IAM-Ressourcentyps in der Region, in der die periodische Regel hinzugefügt wurde, nicht aktiviert haben.
>
> Um unnötige Bewertungen zu vermeiden, sollten Sie nur regelmäßige Regeln einrichten, die die Einhaltung der Vorschriften für einen globalen IAM-Ressourcentyp an eine der unterstützten Regionen melden. Eine Liste der verwalteten Regeln, die in welchen Regionen unterstützt werden, finden Sie unter Liste der AWS Config verwalteten Regeln nach Verfügbarkeit in Regionen.

ID: IAM_ROOT_ACCESS_KEY_CHECK

Auslösertyp: Regelmäßig

AWS-Region: Alle unterstützten AWS Regionen außer Asien-Pazifik (Thailand), Naher Osten (VAE), Asien-Pazifik (Malaysia), Mexiko (Zentral), Israel (Tel Aviv), Asien-Pazifik (Taipeh), Kanada West (Calgary), Europa (Spanien), Europa (Zürich)

Parameter:

Keine

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

iam-saml-provider-tagged

Prüft, ob AWS IAM-SAML-Anbieter über Tags verfügen. Optional können Sie Tag-Schlüssel angeben. Die Regel lautet NON_COMPLIANT, wenn keine Tags vorhanden sind oder wenn die angegebenen Tag-Schlüssel nicht vorhanden sind. Die Regel sucht nicht nach Tags, die mit 'aws: 'beginnen.

Kennung: IAM_SAML_PROVIDER_TAGGED

Ressourcentypen: AWS::IAM::SAMLProvider

Auslösertyp: Konfigurationsänderungen

AWS-Region: Nur in der Region USA Ost (Nord-Virginia) verfügbar

Parameter:

requiredKeyTags (Fakultativ), Typ: CSV

> Durch Kommas getrennte Liste von Tag-Schlüsseln, die von der Regel überprüft werden sollen. Falls angegeben, lautet die Regel NON_COMPLIANT, wenn die ausgewertete Ressource diese Schlüssel nicht enthält. Bei Tag-Schlüsseln wird die Groß- und Kleinschreibung beachtet. Tag-Schlüssel, die mit „aws:“ beginnen, sind nicht erlaubt.

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

iam-server-certificate-expiration-überprüfen

Überprüft, ob die in AWS IAM gespeicherten SSL/TLS IAM-Serverzertifikate abgelaufen sind. Die Regel lautet NON_COMPLIANT, wenn ein IAM-Serverzertifikat abgelaufen ist.

Kennung: IAM_SERVER_CERTIFICATE_EXPIRATION_CHECK

Ressourcentypen: AWS::IAM::ServerCertificate

Auslösertyp: Regelmäßig

AWS-Region: Nur in der Region USA Ost (Nord-Virginia) verfügbar

Parameter:

Keine

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

iam-server-certificate-tagged

Prüft, ob AWS IAM-Serverzertifikate Tags haben. Optional können Sie Tag-Schlüssel angeben. Die Regel lautet NON_COMPLIANT, wenn keine Tags vorhanden sind oder wenn die angegebenen Tag-Schlüssel nicht vorhanden sind. Die Regel sucht nicht nach Tags, die mit 'aws: 'beginnen.

Kennung: IAM_SERVER_CERTIFICATE_TAGGED

Ressourcentypen: AWS::IAM::ServerCertificate

Auslösertyp: Konfigurationsänderungen

AWS-Region: Nur in der Region USA Ost (Nord-Virginia) verfügbar

Parameter:

requiredKeyTags (Fakultativ), Typ: CSV

> Durch Kommas getrennte Liste von Tag-Schlüsseln, die von der Regel überprüft werden sollen. Falls angegeben, lautet die Regel NON_COMPLIANT, wenn die ausgewertete Ressource diese Schlüssel nicht enthält. Bei Tag-Schlüsseln wird die Groß- und Kleinschreibung beachtet. Tag-Schlüssel, die mit „aws:“ beginnen, sind nicht erlaubt.

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

iam-user-group-membership-überprüfen

Prüft, ob IAM-Benutzer Mitglieder mindestens einer IAM-Gruppe sind.

ID: IAM_USER_GROUP_MEMBERSHIP_CHECK

Ressourcentypen: AWS::IAM::User

Auslösertyp: Konfigurationsänderungen

AWS-Region: Alle unterstützten AWS Regionen außer Asien-Pazifik (Thailand), Naher Osten (VAE), Asien-Pazifik (Hyderabad), Asien-Pazifik (Malaysia), Asien-Pazifik (Melbourne), Mexiko (Zentral), Israel (Tel Aviv), Asien-Pazifik (Taipeh), Kanada West (Calgary), Europa (Spanien), Europa (Zürich)

Parameter:

groupNames (optional), Typ: Zeichenfolge

Durch Kommata getrennte Liste der IAM-Gruppen, in denen IAM-Benutzer Mitglieder sein müssen.

> **Note**
>
> Diese Regel unterstützt keine Gruppennamen mit Kommas.

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

iam-user-mfa-enabled

Überprüft, ob die Benutzer von AWS Identity and Access Management (IAM) die Multi-Faktor-Authentifizierung (MFA) aktiviert haben. Die Regel ist NON_COMPLIANT, wenn die MFA nicht für mindestens einen IAM-Benutzer aktiviert ist.

> **Note**
>
> Verwaltete Regeln und globale IAM-Ressourcentypen
> Die globalen IAM-Ressourcentypen, die vor Februar 2022 eingeführt wurden (`AWS::IAM::Group`,, und`AWS::IAM::User`) `AWS::IAM::Policy`AWS::IAM::Role, können nur AWS Config in AWS Regionen erfasst werden, in denen sie vor Februar 2022 verfügbar AWS Config waren. Diese Ressourcentypen können nicht in Regionen erfasst werden, die AWS Config nach Februar 2022 unterstützt werden. Eine Liste dieser Regionen finden Sie unter AWS Aufzeichnungsressourcen | Globale Ressourcen.
> Wenn Sie einen globalen IAM-Ressourcentyp in mindestens einer Region aufzeichnen, führen periodische Regeln, die die Einhaltung des globalen IAM-Ressourcentyps melden,

Bewertungen in allen Regionen durch, in denen die periodische Regel hinzugefügt wurde, auch wenn Sie die Aufzeichnung des globalen IAM-Ressourcentyps in der Region, in der die periodische Regel hinzugefügt wurde, nicht aktiviert haben.
Um unnötige Bewertungen zu vermeiden, sollten Sie nur regelmäßige Regeln einrichten, die die Einhaltung der Vorschriften für einen globalen IAM-Ressourcentyp an eine der unterstützten Regionen melden. Eine Liste der verwalteten Regeln, die in welchen Regionen unterstützt werden, finden Sie unter Liste der AWS Config verwalteten Regeln nach Verfügbarkeit in Regionen.

ID: IAM_USER_MFA_ENABLED

Ressourcentypen: AWS::IAM::User

Auslösertyp: Regelmäßig

AWS-Region: Alle unterstützten AWS Regionen außer Asien-Pazifik (Thailand), Naher Osten (VAE), Asien-Pazifik (Hyderabad), Asien-Pazifik (Malaysia), Asien-Pazifik (Melbourne), Mexiko (Zentral), Israel (Tel Aviv), Asien-Pazifik (Taipeh), Kanada West (Calgary), Europa (Spanien), Europa (Zürich)

Parameter:

Keine

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

iam-user-no-policies-überprüfen

Überprüft, ob an keinen Ihrer AWS Identity and Access Management (IAM) -Benutzer Richtlinien angehängt sind. IAM-Benutzer müssen die Berechtigungen von IAM-Gruppen oder -Rollen erben. Die Regel lautet NON_COMPLIANT, wenn dem IAM-Benutzer mindestens eine Richtlinie zugewiesen ist.

ID: IAM_USER_NO_POLICIES_CHECK

Ressourcentypen: AWS::IAM::User

Auslösertyp: Konfigurationsänderungen

AWS-Region: Alle unterstützten AWS Regionen außer Asien-Pazifik (Thailand), Naher Osten (VAE), Asien-Pazifik (Hyderabad), Asien-Pazifik (Malaysia), Asien-Pazifik (Melbourne), Mexiko (Zentral), Israel (Tel Aviv), Asien-Pazifik (Taipeh), Kanada West (Calgary), Europa (Spanien), Europa (Zürich)

Parameter:

Keine

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

iam-user-unused-credentials-überprüfen

Prüft, ob Ihre AWS Identity and Access Management (IAM-) Benutzer über Passwörter oder aktive Zugriffsschlüssel verfügen, die innerhalb der von Ihnen angegebenen Anzahl von Tagen nicht verwendet wurden. Die Regel ist NON_COMPLIANT, wenn es inaktive Konten gibt, die in letzter Zeit nicht verwendet wurden.

> **Note**
>
> Zeitplan für die Neubewertung
> Ein erneute Auswertung dieser Regel innerhalb von 4 Stunden hat keine Auswirkungen auf die Ergebnisse.
> Verwaltete Regeln und globale IAM-Ressourcentypen
> Die globalen IAM-Ressourcentypen, die vor Februar 2022 eingeführt wurden (`AWS::IAM::Group`,, und`AWS::IAM::User`) `AWS::IAM::Policy`AWS::IAM::Role, können nur AWS Config in AWS Regionen erfasst werden, in denen sie vor Februar 2022 verfügbar AWS Config waren. Diese Ressourcentypen können nicht in Regionen erfasst werden, die AWS Config nach Februar 2022 unterstützt werden. Eine Liste dieser Regionen finden Sie unter AWS Aufzeichnungsressourcen | Globale Ressourcen.
> Wenn Sie einen globalen IAM-Ressourcentyp in mindestens einer Region aufzeichnen, führen periodische Regeln, die die Einhaltung des globalen IAM-Ressourcentyps melden, Bewertungen in allen Regionen durch, in denen die periodische Regel hinzugefügt wurde, auch wenn Sie die Aufzeichnung des globalen IAM-Ressourcentyps in der Region, in der die periodische Regel hinzugefügt wurde, nicht aktiviert haben.
> Um unnötige Bewertungen zu vermeiden, sollten Sie nur regelmäßige Regeln einrichten, die die Einhaltung der Vorschriften für einen globalen IAM-Ressourcentyp an eine der

unterstützten Regionen melden. Eine Liste der verwalteten Regeln, die in welchen Regionen unterstützt werden, finden Sie unter Liste der AWS Config verwalteten Regeln nach Verfügbarkeit in Regionen.

ID: IAM_USER_UNUSED_CREDENTIALS_CHECK

Ressourcentypen: AWS::IAM::User

Auslösertyp: Regelmäßig

AWS-Region: Alle unterstützten AWS Regionen außer Asien-Pazifik (Thailand), Naher Osten (VAE), Asien-Pazifik (Hyderabad), Asien-Pazifik (Malaysia), Asien-Pazifik (Melbourne), Mexiko (Zentral), Israel (Tel Aviv), Asien-Pazifik (Taipeh), Kanada West (Calgary), Europa (Spanien), Europa (Zürich)

Parameter:

maxCredentialUsageAlter, Typ: int, Standard: 90

Maximale Anzahl der Tage, innerhalb derer Anmeldeinformation nicht verwendet werden können. Der Standardwert lautet 90 Tage.

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

restricted-ssh

Important

Bei dieser Regel unterscheidet sich die Regel-ID (INCOMING_SSH_DISABLED) vom Regelnamen (restricted-ssh).

Prüft, ob der eingehende SSH-Datenverkehr für die Sicherheitsgruppen zugänglich ist. Die Regel ist COMPLIANT, wenn die IP-Adressen des eingehenden SSH-Datenverkehrs in den Sicherheitsgruppen eingeschränkt sind (CIDR ungleich 0.0.0.0/0 oder ::/0). Andernfalls ist sie NON_COMPLIANT.

ID: INCOMING_SSH_DISABLED

Ressourcentypen: AWS::EC2::SecurityGroup

Auslösertyp: „Konfigurationsänderungen“ und „Regelmäßig“

AWS-Region: Alle unterstützten AWS Regionen

Parameter:

Keine

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

inspector-ec2-Scan aktiviert

Überprüft, ob der Amazon Inspector EC2 V2-Scan für Ihre Umgebung mit einem oder mehreren Konten aktiviert ist, um potenzielle Sicherheitslücken und Probleme mit der Netzwerkerreichbarkeit auf Ihren Instances zu erkennen. EC2 Die Regel lautet NON_COMPLIANT, wenn EC2 das Scannen nicht aktiviert ist.

Kennung: INSPECTOR_ _SCAN_ENABLED EC2

Ressourcentypen: AWS::::Account

Auslösertyp: Regelmäßig

AWS-Region: Alle unterstützten AWS Regionen außer China (Peking), Asien-Pazifik (Thailand), Naher Osten (VAE), Asien-Pazifik (Hyderabad), Asien-Pazifik (Malaysia), Asien-Pazifik (Melbourne), Mexiko (Zentral), Israel (Tel Aviv), Kanada West (Calgary), Europa (Spanien), China (Ningxia)

Parameter:

Keine

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

inspector-ecr-scan-enabled

Überprüft, ob der Amazon Inspector V2 ECR-Scan für Ihre Umgebung mit einem oder mehreren Konten aktiviert ist, um potenzielle Softwareschwachstellen in Ihren Container-Images zu erkennen. Die Regel lautet NON_COMPLIANT, wenn der ECR-Scan nicht aktiviert ist.

Kennung: INSPECTOR_ECR_SCAN_ENABLED

Ressourcentypen: AWS::::Account

Auslösertyp: Regelmäßig

AWS-Region: Alle unterstützten AWS Regionen außer China (Peking), Asien-Pazifik (Thailand), Naher Osten (VAE), Asien-Pazifik (Hyderabad), Asien-Pazifik (Malaysia), Asien-Pazifik (Melbourne), Mexiko (Zentral), Israel (Tel Aviv), Kanada West (Calgary), Europa (Spanien), China (Ningxia)

Parameter:

Keine

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

inspector-lambda-code-scan-aktiviert

Überprüft, ob das Amazon Inspector V2 Lambda-Code-Scanning für Ihre Umgebung mit einem oder mehreren Konten aktiviert ist, um potenzielle Code-Schwachstellen zu erkennen. Die Regel lautet NON_COMPLIANT, wenn der Lambda-Code-Scan nicht aktiviert ist.

Kennung: INSPECTOR_LAMBDA_CODE_SCAN_ENABLED

Ressourcentypen: AWS::::Account

Auslösertyp: Regelmäßig

AWS-Region: Nur in der Region Europa (Stockholm), USA Ost (Ohio), Europa (Irland), Europa (Frankfurt), USA Ost (Nord-Virginia), Europa (London), Asien-Pazifik (Tokio), USA West (Oregon), Asien-Pazifik (Singapur), Asien-Pazifik (Sydney) verfügbar

Parameter:

Keine

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

inspector-lambda-standard-scan-aktiviert

Überprüft, ob der Amazon Inspector V2 Lambda-Standardscan für Ihre Umgebung mit einem oder mehreren Konten aktiviert ist, um potenzielle Softwareschwachstellen zu erkennen. Die Regel lautet NON_COMPLIANT, wenn das Lambda-Standardscannen nicht aktiviert ist.

Kennung: INSPECTOR_LAMBDA_STANDARD_SCAN_ENABLED

Ressourcentypen: AWS::::Account

Auslösertyp: Regelmäßig

AWS-Region: Alle unterstützten AWS Regionen außer China (Peking), Asien-Pazifik (Thailand), Naher Osten (VAE), Asien-Pazifik (Hyderabad), Asien-Pazifik (Malaysia), Asien-Pazifik (Melbourne), Mexiko (Zentral), Israel (Tel Aviv), Kanada West (Calgary), Europa (Spanien), China (Ningxia)

Parameter:

Keine

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

ec2- instances-in-vpc

> **Important**
>
> Bei dieser Regel unterscheiden sich die Regel-ID (INSTANCES_IN_VPC) und der Regelname (ec2-). instances-in-vpc

Prüft, ob Ihre EC2 Instanzen zu einer Virtual Private Cloud (VPC) gehören. Optional können Sie die Ihren Instances zuzuordnende VPC-ID angeben.

ID: INSTANCES_IN_VPC

Ressourcentypen: AWS::EC2::Instance

Auslösertyp: Konfigurationsänderungen

AWS-Region: Alle unterstützten AWS Regionen

Parameter:

vpcId (optional), Typ: Zeichenfolge

VPC-ID, die diese EC2 Instances enthält.

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

internet-gateway-authorized-vpc-nur

Prüft, ob Internet-Gateways an eine autorisierte Virtual Private Cloud (Amazon VPC) angehängt sind. Die Regel ist NON_COMPLIANT, wenn Internet-Gateways an eine nicht autorisierte VPC angehängt sind.

Identifier (Kennung): INTERNET_GATEWAY_AUTHORIZED_VPC_ONLY

Ressourcentypen: AWS::EC2::InternetGateway

Auslösertyp: Konfigurationsänderungen

AWS-Region: Alle unterstützten AWS Regionen außer Asien-Pazifik (Thailand), Asien-Pazifik (Taipeh) und Kanada West (Calgary)

Parameter:

AuthorizedVpcIds (Fakultativ), Typ: Zeichenfolge

Kommagetrennte Liste der autorisierten VPC IDs mit angehängtem. IGWs Wenn der Parameter nicht angegeben wird, sind alle angehängten Dateien IGWs NON_COMPLIANT.

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

iotevents-alarm-model-tagged

Überprüft, ob AWS IoT-Ereignis-Alarmmodelle Tags haben. Optional können Sie Tag-Schlüssel angeben. Die Regel lautet NON_COMPLIANT, wenn keine Tags vorhanden sind oder wenn die angegebenen Tag-Schlüssel nicht vorhanden sind. Die Regel sucht nicht nach Tags, die mit 'aws: 'beginnen.

Kennung: IOTEVENTS_ALARM_MODEL_TAGGED

Ressourcentypen: AWS::IoTEvents::AlarmModel

Auslösertyp: Konfigurationsänderungen

AWS-Region: Nur in der Region Asien-Pazifik (Mumbai), USA Ost (Ohio), Europa (Irland), Europa (Frankfurt), USA Ost (Nord-Virginia), Asien-Pazifik (Seoul), Europa (London), Asien-Pazifik (Tokio), USA West (Oregon), Asien-Pazifik (Singapur), Asien-Pazifik (Sydney), Kanada (Zentral) verfügbar

Parameter:

requiredKeyTags (Fakultativ), Typ: CSV

> Durch Kommas getrennte Liste von Tag-Schlüsseln, die von der Regel überprüft werden sollen. Falls angegeben, lautet die Regel NON_COMPLIANT, wenn die ausgewertete Ressource diese Schlüssel nicht enthält. Bei Tag-Schlüsseln wird die Groß- und Kleinschreibung beachtet. Tag-Schlüssel, die mit „aws:“ beginnen, sind nicht erlaubt.

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

iotevents-detector-model-tagged

Überprüft, ob Modelle mit AWS IoT-Ereignisdetektoren Tags haben. Optional können Sie Tag-Schlüssel angeben. Die Regel lautet NON_COMPLIANT, wenn keine Tags vorhanden sind oder wenn die angegebenen Tag-Schlüssel nicht vorhanden sind. Die Regel sucht nicht nach Tags, die mit 'aws: 'beginnen.

Kennung: IOTEVENTS_DETECTOR_MODEL_TAGGED

Ressourcentypen: AWS::IoTEvents::DetectorModel

Auslösertyp: Konfigurationsänderungen

AWS-Region: Nur in der Region Asien-Pazifik (Mumbai), USA Ost (Ohio), Europa (Irland), Europa (Frankfurt), USA Ost (Nord-Virginia), Asien-Pazifik (Seoul), Europa (London), Asien-Pazifik (Tokio), USA West (Oregon), Asien-Pazifik (Singapur), Asien-Pazifik (Sydney), Kanada (Zentral) verfügbar

Parameter:

requiredKeyTags (Fakultativ), Typ: CSV

> Durch Kommas getrennte Liste von Tag-Schlüsseln, die von der Regel überprüft werden sollen. Falls angegeben, lautet die Regel NON_COMPLIANT, wenn die ausgewertete Ressource diese Schlüssel nicht enthält. Bei Tag-Schlüsseln wird die Groß- und Kleinschreibung beachtet. Tag-Schlüssel, die mit „aws:“ beginnen, sind nicht erlaubt.

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

iotevents-input-tagged

Prüft, ob AWS IoT-Events-Eingaben Tags haben. Optional können Sie Tag-Schlüssel angeben. Die Regel lautet NON_COMPLIANT, wenn keine Tags vorhanden sind oder wenn die angegebenen Tag-Schlüssel nicht vorhanden sind. Die Regel sucht nicht nach Tags, die mit 'aws: 'beginnen.

Kennung: IOTEVENTS_INPUT_TAGGED

Ressourcentypen: AWS::IoTEvents::Input

Auslösertyp: Konfigurationsänderungen

AWS-Region: Nur in der Region Asien-Pazifik (Mumbai), USA Ost (Ohio), Europa (Irland), Europa (Frankfurt), USA Ost (Nord-Virginia), Asien-Pazifik (Seoul), Europa (London), Asien-Pazifik (Tokio), USA West (Oregon), Asien-Pazifik (Singapur), Asien-Pazifik (Sydney), Kanada (Zentral) verfügbar

Parameter:

requiredKeyTags (Fakultativ), Typ: CSV

Durch Kommas getrennte Liste von Tag-Schlüsseln, die von der Regel überprüft werden sollen. Falls angegeben, lautet die Regel NON_COMPLIANT, wenn die ausgewertete Ressource diese Schlüssel nicht enthält. Bei Tag-Schlüsseln wird die Groß- und Kleinschreibung beachtet. Tag-Schlüssel, die mit „aws:“ beginnen, sind nicht erlaubt.

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

iotsitewise-asset-model-tagged

Prüft, ob AWS SiteWise IoT-Assetmodelle Tags haben. Optional können Sie Tag-Schlüssel für die Regel angeben. Die Regel ist NON_COMPLIANT, wenn keine Tags vorhanden sind oder wenn die angegebenen Tag-Schlüssel nicht vorhanden sind. Die Regel sucht nicht nach Tags, die mit 'aws: 'beginnen.

Kennung: IOTSITEWISE_ASSET_MODEL_TAGGED

Ressourcentypen: AWS::IoTSiteWise::AssetModel

Auslösertyp: Konfigurationsänderungen

AWS-Region: Nur in der Region Asien-Pazifik (Mumbai), USA Ost (Ohio), Europa (Irland), Europa (Frankfurt), USA Ost (Nord-Virginia), Asien-Pazifik (Seoul), Asien-Pazifik (Tokio), USA West (Oregon), Asien-Pazifik (Singapur), Asien-Pazifik (Sydney), Kanada (Zentral) verfügbar

Parameter:

requiredKeyTags (Fakultativ), Typ: CSV

Durch Kommas getrennte Liste von Tag-Schlüsseln, die von der Regel überprüft werden sollen. Falls angegeben, lautet die Regel NON_COMPLIANT, wenn die ausgewertete Ressource diese Schlüssel nicht enthält. Bei Tag-Schlüsseln wird die Groß- und Kleinschreibung beachtet. Tag-Schlüssel, die mit „aws:“ beginnen, sind nicht erlaubt.

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

iotsitewise-dashboard-tagged

Prüft, ob AWS SiteWise IoT-Dashboards Tags haben. Optional können Sie Tag-Schlüssel für die Regel angeben. Die Regel ist NON_COMPLIANT, wenn keine Tags vorhanden sind oder wenn die angegebenen Tag-Schlüssel nicht vorhanden sind. Die Regel sucht nicht nach Tags, die mit 'aws: 'beginnen.

Kennung: IOTSITEWISE_DASHBOARD_TAGGED

Ressourcentypen: AWS::IoTSiteWise::Dashboard

Auslösertyp: Konfigurationsänderungen

AWS-Region: Nur in der Region Asien-Pazifik (Mumbai), USA Ost (Ohio), Europa (Irland), Europa (Frankfurt), USA Ost (Nord-Virginia), Asien-Pazifik (Seoul), Asien-Pazifik (Tokio), USA West (Oregon), Asien-Pazifik (Singapur), Asien-Pazifik (Sydney), Kanada (Zentral) verfügbar

Parameter:

requiredKeyTags (Fakultativ), Typ: CSV

> Durch Kommas getrennte Liste von Tag-Schlüsseln, die von der Regel überprüft werden sollen. Falls angegeben, lautet die Regel NON_COMPLIANT, wenn die ausgewertete Ressource diese Schlüssel nicht enthält. Bei Tag-Schlüsseln wird die Groß- und Kleinschreibung beachtet. Tag-Schlüssel, die mit „aws:“ beginnen, sind nicht erlaubt.

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

iotsitewise-gateway-tagged

Prüft, ob AWS SiteWise IoT-Gateways Tags haben. Optional können Sie Tag-Schlüssel für die Regel angeben. Die Regel ist NON_COMPLIANT, wenn keine Tags vorhanden sind oder wenn die angegebenen Tag-Schlüssel nicht vorhanden sind. Die Regel sucht nicht nach Tags, die mit 'aws: 'beginnen.

Kennung: IOTSITEWISE_GATEWAY_TAGGED

Ressourcentypen: AWS::IoTSiteWise::Gateway

Auslösertyp: Konfigurationsänderungen

AWS-Region: Nur in der Region Asien-Pazifik (Mumbai), USA Ost (Ohio), Europa (Irland), Europa (Frankfurt), USA Ost (Nord-Virginia), Asien-Pazifik (Seoul), Asien-Pazifik (Tokio), USA West (Oregon), Asien-Pazifik (Singapur), Asien-Pazifik (Sydney), Kanada (Zentral) verfügbar

Parameter:

requiredKeyTags (Fakultativ), Typ: CSV

> Durch Kommas getrennte Liste von Tag-Schlüsseln, die von der Regel überprüft werden sollen. Falls angegeben, lautet die Regel NON_COMPLIANT, wenn die ausgewertete Ressource diese Schlüssel nicht enthält. Bei Tag-Schlüsseln wird die Groß- und Kleinschreibung beachtet. Tag-Schlüssel, die mit „aws:“ beginnen, sind nicht erlaubt.

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

iotsitewise-portal-tagged

Prüft, ob AWS SiteWise IoT-Portale Tags haben. Optional können Sie Tag-Schlüssel für die Regel angeben. Die Regel ist NON_COMPLIANT, wenn keine Tags vorhanden sind oder wenn die angegebenen Tag-Schlüssel nicht vorhanden sind. Die Regel sucht nicht nach Tags, die mit 'aws: 'beginnen.

Kennung: IOTSITEWISE_PORTAL_TAGGED

Ressourcentypen: AWS::IoTSiteWise::Portal

Auslösertyp: Konfigurationsänderungen

AWS-Region: Nur in der Region Asien-Pazifik (Mumbai), USA Ost (Ohio), Europa (Irland), Europa (Frankfurt), USA Ost (Nord-Virginia), Asien-Pazifik (Seoul), Asien-Pazifik (Tokio), USA West (Oregon), Asien-Pazifik (Singapur), Asien-Pazifik (Sydney), Kanada (Zentral) verfügbar

Parameter:

requiredKeyTags (Fakultativ), Typ: CSV

Durch Kommas getrennte Liste von Tag-Schlüsseln, die von der Regel überprüft werden sollen. Falls angegeben, lautet die Regel NON_COMPLIANT, wenn die ausgewertete Ressource diese Schlüssel nicht enthält. Bei Tag-Schlüsseln wird die Groß- und Kleinschreibung beachtet. Tag-Schlüssel, die mit „aws:“ beginnen, sind nicht erlaubt.

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

iotsitewise-project-tagged

Prüft, ob AWS SiteWise IoT-Projekte Tags haben. Optional können Sie Tag-Schlüssel für die Regel angeben. Die Regel ist NON_COMPLIANT, wenn keine Tags vorhanden sind oder wenn die angegebenen Tag-Schlüssel nicht vorhanden sind. Die Regel sucht nicht nach Tags, die mit 'aws: 'beginnen.

Kennung: IOTSITEWISE_PROJECT_TAGGED

Ressourcentypen: AWS::IoTSiteWise::Project

Auslösertyp: Konfigurationsänderungen

AWS-Region: Nur in der Region Asien-Pazifik (Mumbai), USA Ost (Ohio), Europa (Irland), Europa (Frankfurt), USA Ost (Nord-Virginia), Asien-Pazifik (Seoul), Asien-Pazifik (Tokio), USA West (Oregon), Asien-Pazifik (Singapur), Asien-Pazifik (Sydney), Kanada (Zentral) verfügbar

Parameter:

requiredKeyTags (Fakultativ), Typ: CSV

Durch Kommas getrennte Liste von Tag-Schlüsseln, die von der Regel überprüft werden sollen. Falls angegeben, lautet die Regel NON_COMPLIANT, wenn die ausgewertete Ressource diese Schlüssel nicht enthält. Bei Tag-Schlüsseln wird die Groß- und Kleinschreibung beachtet. Tag-Schlüssel, die mit „aws:“ beginnen, sind nicht erlaubt.

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

iottwinmaker-component-type-tagged

Prüft, ob AWS TwinMaker IoT-Komponententypen Tags haben. Optional können Sie Tag-Schlüssel angeben. Die Regel lautet NON_COMPLIANT, wenn keine Tags vorhanden sind oder wenn die angegebenen Tag-Schlüssel nicht vorhanden sind. Die Regel sucht nicht nach Tags, die mit 'aws: 'beginnen.

Kennung: IOTTWINMAKER_COMPONENT_TYPE_TAGGED

Ressourcentypen: AWS::IoTTwinMaker::ComponentType

Auslösertyp: Konfigurationsänderungen

AWS-Region: Nur in der Region Asien-Pazifik (Mumbai), Europa (Irland), Europa (Frankfurt), USA Ost (Nord-Virginia), Asien-Pazifik (Seoul), Asien-Pazifik (Tokio), USA West (Oregon), Asien-Pazifik (Singapur), Asien-Pazifik (Sydney) verfügbar

Parameter:

requiredKeyTags (Fakultativ), Typ: CSV

> Durch Kommas getrennte Liste von Tag-Schlüsseln, die von der Regel überprüft werden sollen. Falls angegeben, lautet die Regel NON_COMPLIANT, wenn die ausgewertete Ressource diese Schlüssel nicht enthält. Bei Tag-Schlüsseln wird die Groß- und Kleinschreibung beachtet. Tag-Schlüssel, die mit „aws:“ beginnen, sind nicht erlaubt.

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

iottwinmaker-entity-tagged

Prüft, ob AWS TwinMaker IoT-Entitäten Tags haben. Optional können Sie Tag-Schlüssel angeben. Die Regel lautet NON_COMPLIANT, wenn keine Tags vorhanden sind oder wenn die angegebenen Tag-Schlüssel nicht vorhanden sind. Die Regel sucht nicht nach Tags, die mit 'aws: 'beginnen.

Kennung: IOTTWINMAKER_ENTITY_TAGGED

Ressourcentypen: AWS::IoTTwinMaker::Entity

Auslösertyp: Konfigurationsänderungen

AWS-Region: Nur in den Regionen Europa (Irland), Europa (Frankfurt), USA Ost (Nord-Virginia), USA West (Oregon), Asien-Pazifik (Singapur), Asien-Pazifik (Sydney) verfügbar

Parameter:

requiredKeyTags (Fakultativ), Typ: CSV

> Durch Kommas getrennte Liste von Tag-Schlüsseln, die von der Regel überprüft werden sollen. Falls angegeben, lautet die Regel NON_COMPLIANT, wenn die ausgewertete Ressource diese Schlüssel nicht enthält. Bei Tag-Schlüsseln wird die Groß- und Kleinschreibung beachtet. Tag-Schlüssel, die mit „aws:“ beginnen, sind nicht erlaubt.

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

iottwinmaker-scene-tagged

Prüft, ob AWS TwinMaker IoT-Szenen Tags haben. Optional können Sie Tag-Schlüssel angeben. Die Regel lautet NON_COMPLIANT, wenn keine Tags vorhanden sind oder wenn die angegebenen Tag-Schlüssel nicht vorhanden sind. Die Regel sucht nicht nach Tags, die mit 'aws: 'beginnen.

Kennung: IOTTWINMAKER_SCENE_TAGGED

Ressourcentypen: AWS::IoTTwinMaker::Scene

Auslösertyp: Konfigurationsänderungen

AWS-Region: Nur in der Region Asien-Pazifik (Mumbai), Europa (Irland), Europa (Frankfurt), USA Ost (Nord-Virginia), Asien-Pazifik (Seoul), Asien-Pazifik (Tokio), USA West (Oregon), Asien-Pazifik (Singapur), Asien-Pazifik (Sydney) verfügbar

Parameter:

requiredKeyTags (Fakultativ), Typ: CSV

Durch Kommas getrennte Liste von Tag-Schlüsseln, die von der Regel überprüft werden sollen. Falls angegeben, lautet die Regel NON_COMPLIANT, wenn die ausgewertete Ressource diese Schlüssel nicht enthält. Bei Tag-Schlüsseln wird die Groß- und Kleinschreibung beachtet. Tag-Schlüssel, die mit „aws:“ beginnen, sind nicht erlaubt.

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

iottwinmaker-sync-job-tagged

Prüft, ob AWS TwinMaker IoT-Synchronisierungsjobs Tags haben. Optional können Sie Tag-Schlüssel angeben. Die Regel lautet NON_COMPLIANT, wenn keine Tags vorhanden sind oder wenn die angegebenen Tag-Schlüssel nicht vorhanden sind. Die Regel sucht nicht nach Tags, die mit 'aws: 'beginnen.

Kennung: IOTTWINMAKER_SYNC_JOB_TAGGED

Ressourcentypen: AWS::IoTTwinMaker::SyncJob

Auslösertyp: Konfigurationsänderungen

AWS-Region: Nur in der Region Asien-Pazifik (Mumbai), Europa (Irland), Europa (Frankfurt), USA Ost (Nord-Virginia), Asien-Pazifik (Seoul), Asien-Pazifik (Tokio), USA West (Oregon), Asien-Pazifik (Singapur), Asien-Pazifik (Sydney) verfügbar

Parameter:

requiredKeyTags (Fakultativ), Typ: CSV

Durch Kommas getrennte Liste von Tag-Schlüsseln, die von der Regel überprüft werden sollen. Falls angegeben, lautet die Regel NON_COMPLIANT, wenn die ausgewertete Ressource diese Schlüssel nicht enthält. Bei Tag-Schlüsseln wird die Groß- und Kleinschreibung beachtet. Tag-Schlüssel, die mit „aws:“ beginnen, sind nicht erlaubt.

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

iottwinmaker-workspace-tagged

Prüft, ob AWS TwinMaker IoT-Workspaces Tags haben. Optional können Sie Tag-Schlüssel angeben. Die Regel lautet NON_COMPLIANT, wenn keine Tags vorhanden sind oder wenn die angegebenen Tag-Schlüssel nicht vorhanden sind. Die Regel sucht nicht nach Tags, die mit 'aws: 'beginnen.

Kennung: IOTTWINMAKER_WORKSPACE_TAGGED

Ressourcentypen: AWS::IoTTwinMaker::Workspace

Auslösertyp: Konfigurationsänderungen

AWS-Region: Nur in der Region Asien-Pazifik (Mumbai), Europa (Irland), Europa (Frankfurt), USA Ost (Nord-Virginia), Asien-Pazifik (Seoul), Asien-Pazifik (Tokio), USA West (Oregon), Asien-Pazifik (Singapur), Asien-Pazifik (Sydney) verfügbar

Parameter:

requiredKeyTags (Fakultativ), Typ: CSV

> Durch Kommas getrennte Liste von Tag-Schlüsseln, die von der Regel überprüft werden sollen. Falls angegeben, lautet die Regel NON_COMPLIANT, wenn die ausgewertete Ressource diese Schlüssel nicht enthält. Bei Tag-Schlüsseln wird die Groß- und Kleinschreibung beachtet. Tag-Schlüssel, die mit „aws:“ beginnen, sind nicht erlaubt.

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

iotwireless-fuota-task-tagged

Prüft, ob AWS IoT Wireless FUOTA-Aufgaben Tags haben. Optional können Sie Tag-Schlüssel angeben. Die Regel lautet NON_COMPLIANT, wenn keine Tags vorhanden sind oder wenn die

angegebenen Tag-Schlüssel nicht vorhanden sind. Die Regel sucht nicht nach Tags, die mit 'aws: 'beginnen.

Kennung: IOTWIRELESS_FUOTA_TASK_TAGGED

Ressourcentypen: AWS::IoTWireless::FuotaTask

Auslösertyp: Konfigurationsänderungen

AWS-Region: Nur in den Regionen Europa (Irland), Europa (Frankfurt), Südamerika (Sao Paulo), USA Ost (Nord-Virginia), Asien-Pazifik (Tokio), USA West (Oregon), Asien-Pazifik (Sydney) verfügbar

Parameter:

requiredKeyTags (Fakultativ), Typ: CSV

> Durch Kommas getrennte Liste von Tag-Schlüsseln, die von der Regel überprüft werden sollen. Falls angegeben, lautet die Regel NON_COMPLIANT, wenn die ausgewertete Ressource diese Schlüssel nicht enthält. Bei Tag-Schlüsseln wird die Groß- und Kleinschreibung beachtet. Tag-Schlüssel, die mit „aws:“ beginnen, sind nicht erlaubt.

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

iotwireless-multicast-group-tagged

Überprüft, ob AWS IoT Wireless Wireless-Multicast-Gruppen Tags haben. Optional können Sie Tag-Schlüssel angeben. Die Regel lautet NON_COMPLIANT, wenn keine Tags vorhanden sind oder wenn die angegebenen Tag-Schlüssel nicht vorhanden sind. Die Regel sucht nicht nach Tags, die mit 'aws: 'beginnen.

Kennung: IOTWIRELESS_MULTICAST_GROUP_TAGGED

Ressourcentypen: AWS::IoTWireless::MulticastGroup

Auslösertyp: Konfigurationsänderungen

AWS-Region: Nur in den Regionen Europa (Irland), Europa (Frankfurt), Südamerika (Sao Paulo), USA Ost (Nord-Virginia), Asien-Pazifik (Tokio), USA West (Oregon), Asien-Pazifik (Sydney) verfügbar

Parameter:

requiredKeyTags (Fakultativ), Typ: CSV

Durch Kommas getrennte Liste von Tag-Schlüsseln, die von der Regel überprüft werden sollen. Falls angegeben, lautet die Regel NON_COMPLIANT, wenn die ausgewertete Ressource diese Schlüssel nicht enthält. Bei Tag-Schlüsseln wird die Groß- und Kleinschreibung beachtet. Tag-Schlüssel, die mit „aws:“ beginnen, sind nicht erlaubt.

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

iotwireless-service-profile-tagged

Überprüft, ob AWS IoT Wireless Wireless-Dienstprofile Tags haben. Optional können Sie Tag-Schlüssel angeben. Die Regel lautet NON_COMPLIANT, wenn keine Tags vorhanden sind oder wenn die angegebenen Tag-Schlüssel nicht vorhanden sind. Die Regel sucht nicht nach Tags, die mit 'aws: 'beginnen.

Kennung: IOTWIRELESS_SERVICE_PROFILE_TAGGED

Ressourcentypen: AWS::IoTWireless::ServiceProfile

Auslösertyp: Konfigurationsänderungen

AWS-Region: Nur in den Regionen Europa (Irland), Europa (Frankfurt), Südamerika (Sao Paulo), USA Ost (Nord-Virginia), Asien-Pazifik (Tokio), USA West (Oregon), Asien-Pazifik (Sydney) verfügbar

Parameter:

requiredKeyTags (Fakultativ), Typ: CSV

Durch Kommas getrennte Liste von Tag-Schlüsseln, die von der Regel überprüft werden sollen. Falls angegeben, lautet die Regel NON_COMPLIANT, wenn die ausgewertete Ressource diese Schlüssel nicht enthält. Bei Tag-Schlüsseln wird die Groß- und Kleinschreibung beachtet. Tag-Schlüssel, die mit „aws:“ beginnen, sind nicht erlaubt.

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

iot-authorizer-token-signing-aktiviert

Überprüft, ob ein AWS IoT Core-Autorisierer die Signaturanforderungen für die Validierung der Tokensignatur in einer Autorisierungsanfrage nicht deaktiviert hat. Die Regel lautet NON_COMPLIANT, wenn der Autorisierer über eine Konfiguration verfügt. SigningDisabled auf True gesetzt.

Kennung: IOT_AUTHORIZER_TOKEN_SIGNING_ENABLED

Ressourcentypen: AWS::IoT::Authorizer

Auslösertyp: Konfigurationsänderungen

AWS-Region: Alle unterstützten AWS Regionen außer China (Peking), Asien-Pazifik (Thailand), Asien-Pazifik (Jakarta), Afrika (Kapstadt), Asien-Pazifik (Hyderabad), Asien-Pazifik (Osaka), Asien-Pazifik (Malaysia), Asien-Pazifik (Melbourne), Europa (Mailand), (USA-Ost), AWS GovCloud (US-West), Mexiko AWS GovCloud (Zentral), Israel (Tel Aviv), Kanada West (Calgary), Europa (Spanien), China (Ningan) Xia), Region Europa (Zürich)

Parameter:

Keine

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

ivs-channel-playback-authorization-aktiviert

Prüft, ob für Amazon IVS Kanäle die Wiedergabeautorisierung aktiviert ist. Die Regel ist NON_COMPLIANT, wenn Configuration.AUTHORIZED den Wert false hat.

Kennung: IVS_CHANNEL_PLAYBACK_AUTHORIZATION_ENABLED

Ressourcentypen: AWS::IVS::Channel

Auslösertyp: Konfigurationsänderungen

AWS-Region: Nur in der Region Asien-Pazifik (Mumbai), Europa (Irland), Europa (Frankfurt), USA Ost (Nord-Virginia), Asien-Pazifik (Seoul), Asien-Pazifik (Tokio), USA West (Oregon) verfügbar

Parameter:

Keine

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

ivs-channel-tagged

Prüft, ob Amazon IVS Kanäle Tags haben. Optional können Sie Tag-Schlüssel angeben. Die Regel lautet NON_COMPLIANT, wenn keine Tags vorhanden sind oder wenn die angegebenen Tag-Schlüssel nicht vorhanden sind. Die Regel sucht nicht nach Tags, die mit 'aws: 'beginnen.

Kennung: IVS_CHANNEL_TAGGED

Ressourcentypen: AWS::IVS::Channel

Auslösertyp: Konfigurationsänderungen

AWS-Region: Nur in der Region Asien-Pazifik (Mumbai), Europa (Irland), Europa (Frankfurt), USA Ost (Nord-Virginia), Asien-Pazifik (Seoul), Asien-Pazifik (Tokio), USA West (Oregon) verfügbar

Parameter:

requiredKeyTags (Fakultativ), Typ: CSV

> Durch Kommas getrennte Liste von Tag-Schlüsseln, die von der Regel überprüft werden sollen. Falls angegeben, lautet die Regel NON_COMPLIANT, wenn die ausgewertete Ressource diese Schlüssel nicht enthält. Bei Tag-Schlüsseln wird die Groß- und Kleinschreibung beachtet. Tag-Schlüssel, die mit „aws:“ beginnen, sind nicht erlaubt.

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

ivs-playback-key-pair-markiert

Prüft, ob Amazon IVS-Wiedergabeschlüsselpaare Tags haben. Optional können Sie Tag-Schlüssel angeben. Die Regel lautet NON_COMPLIANT, wenn keine Tags vorhanden sind oder wenn die

angegebenen Tag-Schlüssel nicht vorhanden sind. Die Regel sucht nicht nach Tags, die mit 'aws: 'beginnen.

Kennung: IVS_PLAYBACK_KEY_PAIR_TAGGED

Ressourcentypen: AWS::IVS::PlaybackKeyPair

Auslösertyp: Konfigurationsänderungen

AWS-Region: Nur in der Region Asien-Pazifik (Mumbai), Europa (Irland), Europa (Frankfurt), USA Ost (Nord-Virginia), Asien-Pazifik (Seoul), Asien-Pazifik (Tokio), USA West (Oregon) verfügbar

Parameter:

requiredKeyTags (Fakultativ), Typ: CSV

> Durch Kommas getrennte Liste von Tag-Schlüsseln, die von der Regel überprüft werden sollen. Falls angegeben, lautet die Regel NON_COMPLIANT, wenn die ausgewertete Ressource diese Schlüssel nicht enthält. Bei Tag-Schlüsseln wird die Groß- und Kleinschreibung beachtet. Tag-Schlüssel, die mit „aws:“ beginnen, sind nicht erlaubt.

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

ivs-recording-configuration-tagged

Prüft, ob Amazon IVS-Aufzeichnungskonfigurationen Tags haben. Optional können Sie Tag-Schlüssel angeben. Die Regel lautet NON_COMPLIANT, wenn keine Tags vorhanden sind oder wenn die angegebenen Tag-Schlüssel nicht vorhanden sind. Die Regel sucht nicht nach Tags, die mit 'aws: 'beginnen.

Kennung: IVS_RECORDING_CONFIGURATION_TAGGED

Ressourcentypen: AWS::IVS::RecordingConfiguration

Auslösertyp: Konfigurationsänderungen

AWS-Region: Nur in der Region Asien-Pazifik (Mumbai), Europa (Irland), Europa (Frankfurt), USA Ost (Nord-Virginia), Asien-Pazifik (Seoul), Asien-Pazifik (Tokio), USA West (Oregon) verfügbar

Parameter:

requiredKeyTags (Fakultativ), Typ: CSV

Durch Kommas getrennte Liste von Tag-Schlüsseln, die von der Regel überprüft werden sollen. Falls angegeben, lautet die Regel NON_COMPLIANT, wenn die ausgewertete Ressource diese Schlüssel nicht enthält. Bei Tag-Schlüsseln wird die Groß- und Kleinschreibung beachtet. Tag-Schlüssel, die mit „aws:“ beginnen, sind nicht erlaubt.

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

kinesis-firehose-delivery-stream-verschlüsselt

Überprüft, ob Amazon Kinesis Data Firehose Firehose-Lieferstreams im Ruhezustand mit serverseitiger Verschlüsselung verschlüsselt sind. Die Regel lautet NON_COMPLIANT, wenn ein Kinesis Data Firehose Firehose-Lieferstream im Ruhezustand nicht mit serverseitiger Verschlüsselung verschlüsselt ist.

Kennung: KINESIS_FIREHOSE_DELIVERY_STREAM_ENCRYPTED

Ressourcentypen: AWS::KinesisFirehose::DeliveryStream

Auslösertyp: Regelmäßig

AWS-Region: Alle unterstützten AWS Regionen außer China (Peking), Asien-Pazifik (Thailand), Asien-Pazifik (Malaysia), Mexiko (Zentral), Kanada West (Calgary), China (Ningxia)

Parameter:

kmsKeyArns (Fakultativ), Typ: CSV

Durch Kommas getrennte Liste von KMS Key Arns, die für die Verwendung mit Kinesis Firehose zugelassen sind.

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

kinesis-stream-backup-retention-überprüfen

Prüft, ob für einen Amazon Kinesis Data Stream die Aufbewahrungsfrist für Datensätze auf eine bestimmte Anzahl von Stunden festgelegt ist. Die Regel lautet NON_COMPLIANT, wenn die Eigenschaft `RetentionPeriodHours` auf einen Wert gesetzt ist, der unter dem durch den Parameter angegebenen Wert liegt.

Kennung: KINESIS_STREAM_BACKUP_RETENTION_CHECK

Ressourcentypen: AWS::Kinesis::Stream

Auslösertyp: Konfigurationsänderungen

AWS-Region: Alle unterstützten AWS Regionen außer Asien-Pazifik (Thailand), Asien-Pazifik (Malaysia), Mexiko (Zentral), Israel (Tel Aviv) und Kanada West (Calgary)

Parameter:

minimumBackupRetentionZeitraum (optional), Typ: Zeichenfolge

> Datensätze sollten mindestens Stunden aufbewahrt werden. Gültige Werte liegen zwischen 24 und 8760, der Standardwert ist 168.

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

kinesis-stream-encrypted

Prüft, ob Amazon-Kinesis-Streams im Ruhezustand mit serverseitiger Verschlüsselung verschlüsselt sind. Die Regel lautet NON_COMPLIANT für einen Kinesis-Stream, wenn 'StreamEncryption' nicht vorhanden ist.

Kontext: Die serverseitige Verschlüsselung ist eine Funktion in Amazon Kinesis Data Streams, die Daten mithilfe eines AWS KMS-Schlüssels automatisch verschlüsselt, bevor sie gespeichert werden. Die Daten werden verschlüsselt, bevor sie in die Speicherschicht des Kinesis-Streams geschrieben werden. Nach Abruf aus dem Speicher werden sie entschlüsselt. Dadurch sind Ihre ruhenden Daten innerhalb des Services Kinesis Data Streams verschlüsselt. Sie erfüllen so die regulatorischen Anforderungen und erhöhen die Sicherheit Ihrer Daten. Weitere Informationen finden Sie unter Datenschutz in Amazon Kinesis Data Streams.

ID: KINESIS_STREAM_ENCRYPTED

Ressourcentypen: AWS::Kinesis::Stream

Auslösertyp: Konfigurationsänderungen

AWS-Region: Alle unterstützten AWS Regionen außer Asien-Pazifik (Thailand), Asien-Pazifik (Malaysia), Mexiko (Zentral), Israel (Tel Aviv) und Kanada West (Calgary)

Parameter:

Keine

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

kms-cmk-not-scheduled-zum Löschen

Prüft, ob die AWS Schlüssel des Key Management Service (AWS KMS) nicht für das Löschen in AWS KMS geplant sind. Die Regel lautet NON_COMPLIANT, wenn das Löschen von KMS-Schlüsseln geplant ist.

Identifier (Kennung): KMS_CMK_NOT_SCHEDULED_FOR_DELETION

Ressourcentypen: AWS::KMS::Key

Auslösertyp: Regelmäßig

AWS-Region: Alle unterstützten AWS Regionen außer Europa (Mailand) und Asien-Pazifik (Taipeh)

Parameter:

kmsKeyIds (Fakultativ), Typ: Zeichenfolge

> (Optional) Durch Kommas getrennte Liste bestimmter kundenverwalteter Schlüssel, IDs deren Löschung nicht geplant ist. Wenn Sie keine Schlüssel angeben, überprüft die Regel alle Schlüssel.

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

kms-key-policy-no-öffentlich zugänglich

Überprüft, ob die AWS KMS-Schlüsselrichtlinie öffentlichen Zugriff zulässt. Die Regel lautet NON_COMPLIANT, wenn die KMS-Schlüsselrichtlinie öffentlichen Zugriff auf den KMS-Schlüssel zulässt.

> **Note**
>
> Um als nicht öffentlich zu gelten, muss eine KMS-Schlüsselrichtlinie nur Zugriff auf feste Werte gewähren. Das bedeutet Werte, die keinen Platzhalter oder das folgende IAM-Richtlinienelement enthalten: Variablen.

Kennung: KMS_KEY_POLICY_NO_PUBLIC_ACCESS

Ressourcentypen: AWS::KMS::Key

Auslösertyp: Konfigurationsänderungen

AWS-Region: Alle unterstützten AWS Regionen außer Asien-Pazifik (Thailand), Asien-Pazifik (Malaysia), AWS GovCloud (USA-Ost), AWS GovCloud (US-West), Mexiko (Zentral), Kanada West (Calgary)

Parameter:

Keine

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

lambda-concurrency-check

Prüft, ob die Lambda-Funktion mit dem Limit für die gleichzeitige Ausführung auf Funktionsebene konfiguriert ist. Die Regel ist NON_COMPLIANT, wenn die Lambda-Funktion nicht mit dem Limit für die gleichzeitige Ausführung auf Funktionsebene konfiguriert ist.

ID: LAMBDA_CONCURRENCY_CHECK

Ressourcentypen: AWS::Lambda::Function

Auslösertyp: Konfigurationsänderungen

AWS-Region: Alle unterstützten AWS Regionen außer Asien-Pazifik (Taipeh) und China (Ningxia)

Parameter:

ConcurrencyLimitLow (Fakultativ), Typ: Zeichenfolge

Minimales Limit für die gleichzeitige Ausführung

ConcurrencyLimitHigh (Fakultativ), Typ: Zeichenfolge

Maximales Limit für die gleichzeitige Ausführung

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

lambda-dlq-check

Prüft, ob eine Lambda-Funktion mit einer Warteschlange für unzustellbare Nachrichten konfiguriert ist. Die Regel ist NON_COMPLIANT, wenn die Lambda-Funktion nicht mit einer Warteschlange für unzustellbare Nachrichten konfiguriert ist.

ID: LAMBDA_DLQ_CHECK

Ressourcentypen: AWS::Lambda::Function

Auslösertyp: Konfigurationsänderungen

AWS-Region: Alle unterstützten AWS Regionen außer Asien-Pazifik (Taipeh) und China (Ningxia)

Parameter:

dlqArns (optional), Typ: Zeichenfolge

Durch Kommas getrennte Liste von Amazon SQS und Amazon SNS, die als Warteschlangenziel für ARNs Dead-Letter-Warteschlangen der Lambda-Funktion konfiguriert werden müssen.

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

lambda-function-public-access-verboten

Prüft, ob die an die Lambda-Ressource angehängte AWS Lambda Funktionsrichtlinie den öffentlichen Zugriff verbietet. Wenn die Lambda-Funktionsrichtlinie öffentlichen Zugriff zulässt, ist sie NON_COMPLIANT.

Kontext: Es wird davon ausgegangen, dass eine Lambda-Funktionsrichtlinie den öffentlichen Zugriff ermöglicht, wenn das Hauptelement leer ist oder einen Platzhalter enthält. Zum Beispiel, wenn das Hauptelement oder ist`“”`. `{“AWS”: “”}` Die Gewährung eines öffentlichen Zugangs wird aus Sicherheitsgründen nicht empfohlen. Durch die Beschränkung des öffentlichen Zugriffs können Sie verhindern, dass Ihre Lambda-Funktionen unbefugt aufgerufen werden, die Ihre Daten gefährden oder unerwünschte Kosten verursachen könnten.

Um den Zugriff auf Ihre Lambda-Funktionen einzuschränken, geben Sie das AWS Konto IDs oder die Amazon-Ressourcennamen (ARNs) der IAM-Benutzer, -Rollen oder -Services an, die die Funktionen aufrufen können. Weitere Informationen finden Sie im Entwicklerhandbuch unter Gewähren von Funktionszugriff auf andere Konten.AWS Lambda

Die Regel gilt auch, `NON_COMPLIANT` wenn eine Lambda-Funktion von Amazon S3 aus aufgerufen wird und die Richtlinie keine Bedingung zur Beschränkung des öffentlichen Zugriffs enthält, wie z. `AWS:SourceAccount` Wir empfehlen, andere S3-Bedingungen zusammen mit `AWS:SourceAccount` in Ihrer Bucket-Richtlinie zu verwenden, um den Zugriff zu verfeinern.

> **Note**
>
> Um als nicht öffentlich zu gelten, darf eine auf Lambda-Ressourcen basierende Richtlinie nur Zugriff auf feste Werte gewähren. Das bedeutet Werte, die keinen Platzhalter oder das folgende IAM-Richtlinienelement enthalten: Variablen.

ID: LAMBDA_FUNCTION_PUBLIC_ACCESS_PROHIBITED

Ressourcentypen: AWS::Lambda::Function

Auslösertyp: Konfigurationsänderungen

AWS-Region: Alle unterstützten AWS Regionen außer Europa (Spanien) und China (Ningxia)

Parameter:

Keine

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

lambda-function-settings-check

Überprüft, ob die AWS Lambda-Funktionseinstellungen für Laufzeit, Rolle, Timeout und Speichergröße den erwarteten Werten entsprechen. Die Regel ignoriert Funktionen mit dem Pakettyp „Image“ und Funktionen, deren Laufzeit auf „Nur Betriebssystem-Laufzeit“ gesetzt ist. Die Regel ist NON_COMPLIANT, wenn die Einstellungen der Lambda-Funktion nicht den erwarteten Werten entsprechen.

ID: LAMBDA_FUNCTION_SETTINGS_CHECK

Ressourcentypen: AWS::Lambda::Function

Auslösertyp: Konfigurationsänderungen

AWS-Region: Alle unterstützten AWS Regionen außer der Region China (Ningxia)

Parameter:

runtime, Typ: CSV

Kommagetrennte Liste von AWS Lambda-Laufzeitwerten

role (optional), Typ: Zeichenfolge

Name oder ARN der AWS Lambda-Ausführungsrolle

timeout (optional), Typ: int, Standard: 3

AWS Timeout für Lambda-Funktionen in Sekunden

memorySize (optional), Typ: int, Standard: 128

AWS Größe der Lambda-Funktion in Megabyte

Proaktive Auswertung

Anweisungen zur Ausführung dieser Regel im proaktiven Modus finden Sie unter Evaluieren Ihrer Ressourcen mithilfe von Regeln. AWS Config Damit diese Regel im proaktiven Modus COMPLIANT zurückgibt, muss das Ressourcenkonfigurationsschema für die StartResourceEvaluationAPI die folgenden Eingaben enthalten, die als Zeichenfolge kodiert sind:

```
"ResourceConfiguration":
...
{
    "MemorySize": Integer*,
    "Role": String*,
    "Runtime": String*,
    "Timeout": Integer*
}
...
```

* Weitere Informationen zu gültigen Werten für diese Eingaben finden Sie unter Rolle MemorySize, Laufzeit und Timeout im AWS CloudFormation Benutzerhandbuch.

Weitere Informationen zur proaktiven Auswertung finden Sie unter Auswertungsmodus.

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

lambda-function-xray-enabled

Prüft, ob AWS X-Ray für AWS Lambda-Funktionen aktiviert ist. Die Regel lautet NON_COMPLIANT, wenn X-Ray Tracing für eine Lambda-Funktion deaktiviert ist.

Kennung: LAMBDA_FUNCTION_XRAY_ENABLED

Ressourcentypen: AWS::Lambda::Function

Auslösertyp: Konfigurationsänderungen

AWS-Region: Alle unterstützten AWS Regionen außer Asien-Pazifik (Thailand), Naher Osten (VAE), Asien-Pazifik (Hyderabad), Asien-Pazifik (Seoul), Asien-Pazifik (Malaysia), Mexiko (Zentral), Israel (Tel Aviv), Kanada West (Calgary), Europa (Spanien), China (Ningxia), Europa (Zürich)

Parameter:

Keine

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

lambda-inside-vpc

Prüft, ob einer Lambda-Funktion der Zugriff auf eine Virtual Private Cloud (VPC) gestattet ist. Die Regel ist NON_COMPLIANT, wenn die Lambda-Funktion nicht VPC-fähig ist.

ID: LAMBDA_INSIDE_VPC

Ressourcentypen: AWS::Lambda::Function

Auslösertyp: Konfigurationsänderungen

AWS-Region: Alle unterstützten AWS Regionen außer der Region China (Ningxia)

Parameter:

subnetIds (optional), Typ: Zeichenfolge

> Durch Kommas getrennte Liste von Subnetzen IDs , denen Lambda-Funktionen zugeordnet werden können.

Proaktive Auswertung

Anweisungen zur Ausführung dieser Regel im proaktiven Modus finden Sie unter Evaluieren Ihrer Ressourcen mithilfe von Regeln. AWS Config Damit diese Regel im proaktiven Modus COMPLIANT zurückgibt, muss das Ressourcenkonfigurationsschema für die StartResourceEvaluationAPI die folgenden Eingaben enthalten, die als Zeichenfolge kodiert sind:

```
"ResourceConfiguration":
...
{
   "VpcConfig": {
         "SubnetIds": "[SubnetId-1, SubnetId-2, SubnetId-3, ...]"
   }
}
...
```

Weitere Informationen zur proaktiven Auswertung finden Sie unter Auswertungsmodus.

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

lambda-vpc-multi-az-überprüfen

Prüft, ob Lambda mehr als eine Availability Zone zugeordnet ist. Die Regel ist NON_COMPLIANT, wenn Lambda nur eine Availability Zone zugeordnet ist oder die Anzahl der verknüpften Availability Zones geringer ist als die im optionalen Parameter angegebene Zahl.

ID: LAMBDA_VPC_MULTI_AZ_CHECK

Ressourcentypen: AWS::Lambda::Function

Auslösertyp: Konfigurationsänderungen

AWS-Region: Alle unterstützten AWS Regionen außer Asien-Pazifik (Thailand), Asien-Pazifik (Malaysia), AWS GovCloud (USA-Ost), AWS GovCloud (US-West), Mexiko (Zentral), Israel (Tel Aviv), Kanada West (Calgary), China (Ningxia)

Parameter:

availabilityZones (optional), Typ: int

Anzahl der erwarteten Availability Zones.

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

lightsail-bucket-tagged

Prüft, ob Amazon Lightsail-Buckets Tags haben. Optional können Sie Tag-Schlüssel angeben. Die Regel lautet NON_COMPLIANT, wenn keine Tags vorhanden sind oder wenn die angegebenen Tag-Schlüssel nicht vorhanden sind. Die Regel sucht nicht nach Tags, die mit 'aws: 'beginnen.

Kennung: LIGHTSAIL_BUCKET_TAGGED

Ressourcentypen: AWS::Lightsail::Bucket

Auslösertyp: Konfigurationsänderungen

AWS-Region: Nur verfügbar in Europa (Stockholm), Asien-Pazifik (Mumbai), Europa (Paris), USA Ost (Ohio), Europa (Irland), Europa (Frankfurt), USA Ost (Nord-Virginia), Asien-Pazifik (Seoul), Europa (London), Asien-Pazifik (Tokio), USA West (Oregon), Asien-Pazifik (Singapur), Asien-Pazifik (Sydney), Kanada (Zentral)

Parameter:

requiredKeyTags (Fakultativ), Typ: CSV

> Durch Kommas getrennte Liste von Tag-Schlüsseln, die von der Regel überprüft werden sollen. Falls angegeben, lautet die Regel NON_COMPLIANT, wenn die ausgewertete Ressource diese Schlüssel nicht enthält. Bei Tag-Schlüsseln wird die Groß- und Kleinschreibung beachtet. Tag-Schlüssel, die mit „aws:“ beginnen, sind nicht erlaubt.

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

lightsail-certificate-tagged

Prüft, ob Amazon Lightsail-Zertifikate Tags haben. Optional können Sie Tag-Schlüssel angeben. Die Regel lautet NON_COMPLIANT, wenn keine Tags vorhanden sind oder wenn die angegebenen Tag-Schlüssel nicht vorhanden sind. Die Regel sucht nicht nach Tags, die mit 'aws: 'beginnen.

Kennung: LIGHTSAIL_CERTIFICATE_TAGGED

Ressourcentypen: AWS::Lightsail::Certificate

Auslösertyp: Konfigurationsänderungen

AWS-Region: Nur verfügbar in Europa (Stockholm), Asien-Pazifik (Mumbai), Europa (Paris), USA Ost (Ohio), Europa (Irland), Europa (Frankfurt), USA Ost (Nord-Virginia), Asien-Pazifik (Seoul), Europa (London), Asien-Pazifik (Tokio), USA West (Oregon), Asien-Pazifik (Singapur), Asien-Pazifik (Sydney), Kanada (Zentral)

Parameter:

requiredKeyTags (Fakultativ), Typ: CSV

> Durch Kommas getrennte Liste von Tag-Schlüsseln, die von der Regel überprüft werden sollen. Falls angegeben, lautet die Regel NON_COMPLIANT, wenn die ausgewertete Ressource diese Schlüssel nicht enthält. Bei Tag-Schlüsseln wird die Groß- und Kleinschreibung beachtet. Tag-Schlüssel, die mit „aws:“ beginnen, sind nicht erlaubt.

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

lightsail-disk-tagged

Prüft, ob Amazon Lightsail-Festplatten Tags haben. Optional können Sie Tag-Schlüssel angeben. Die Regel lautet NON_COMPLIANT, wenn keine Tags vorhanden sind oder wenn die angegebenen Tag-Schlüssel nicht vorhanden sind. Die Regel sucht nicht nach Tags, die mit 'aws: 'beginnen.

Kennung: LIGHTSAIL_DISK_TAGGED

Ressourcentypen: AWS::Lightsail::Disk

Auslösertyp: Konfigurationsänderungen

AWS-Region: Nur verfügbar in Europa (Stockholm), Asien-Pazifik (Mumbai), Europa (Paris), USA Ost (Ohio), Europa (Irland), Europa (Frankfurt), USA Ost (Nord-Virginia), Asien-Pazifik (Seoul), Europa (London), Asien-Pazifik (Tokio), USA West (Oregon), Asien-Pazifik (Singapur), Asien-Pazifik (Sydney), Kanada (Zentral)

Parameter:

requiredKeyTags (Fakultativ), Typ: CSV

> Durch Kommas getrennte Liste von Tag-Schlüsseln, die von der Regel überprüft werden sollen. Falls angegeben, lautet die Regel NON_COMPLIANT, wenn die ausgewertete Ressource diese

Schlüssel nicht enthält. Bei Tag-Schlüsseln wird die Groß- und Kleinschreibung beachtet. Tag-Schlüssel, die mit „aws:“ beginnen, sind nicht erlaubt.

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

macie-auto-sensitive-data-Discovery-Check

Prüft, ob die automatische Erkennung sensibler Daten für Amazon Macie aktiviert ist. Die Regel lautet NON_COMPLIANT, wenn die automatische Erkennung sensibler Daten deaktiviert ist. Die Regel gilt für Administratorkonten und NOT_APPLICABLE für Mitgliedskonten.

Kennung: MACIE_AUTO_SENSITIVE_DATA_DISCOVERY_CHECK

Ressourcentypen: AWS::::Account

Auslösertyp: Regelmäßig

AWS-Region: Alle unterstützten AWS Regionen außer China (Peking), Asien-Pazifik (Thailand), Asien-Pazifik (Jakarta), Naher Osten (VAE), Asien-Pazifik (Hyderabad), Asien-Pazifik (Malaysia), Asien-Pazifik (Melbourne), AWS GovCloud (US-Ost), AWS GovCloud (US-West), Mexiko (Zentral), Kanada West (Calgary), Europa (Spanien), China (Ningxia), Europa (Zürich)

Parameter:

Keine

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

macie-status-check

Prüft pro Region, ob Amazon Macie in Ihrem Konto aktiviert ist. Die Regel ist NON_COMPLIANT, wenn das Attribut „status“ nicht auf „ENABLED“ festgelegt ist.

ID: MACIE_STATUS_CHECK

Ressourcentypen: AWS::::Account

Auslösertyp: Regelmäßig

AWS-Region: Alle unterstützten AWS Regionen außer China (Peking), Asien-Pazifik (Thailand), Asien-Pazifik (Jakarta), Naher Osten (VAE), Asien-Pazifik (Hyderabad), Asien-Pazifik (Malaysia), Asien-Pazifik (Melbourne), AWS GovCloud (US-Ost), AWS GovCloud (US-West), Mexiko (Zentral), Israel (Tel Aviv), Kanada West (Calgary), Europa (Spanien), China (Ningxia), Europa (Zürich)

Parameter:

Keine

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

mariadb-publish-logs-to-Cloudwatch-Protokolle

Prüft, ob Amazon MariaDB-Datenbank-Instances so konfiguriert sind, dass sie Protokolle in Amazon CloudWatch Logs veröffentlichen. Die Regel lautet NON_COMPLIANT, wenn eine Datenbank-Instance nicht für die Veröffentlichung von Protokollen in Logs konfiguriert ist. CloudWatch

Kennung: MARIADB_PUBLISH_LOGS_TO_CLOUDWATCH_LOGS

Ressourcentypen: AWS::RDS::DBInstance

Auslösertyp: Regelmäßig

AWS-Region: Alle unterstützten AWS Regionen außer Naher Osten (Bahrain), China (Peking), Asien-Pazifik (Thailand), Asien-Pazifik (Malaysia), Mexiko (Zentral), Kanada West (Calgary), China (Ningxia)

Parameter:

logTypes (optional), Typ: Zeichenfolge

> Durch Kommas getrennte Liste der Protokolltypen, die von der Regel überprüft werden sollen. Falls nicht angegeben, sucht die Regel nach den Standard-Protokolltypen: „Fehler“ und „Prüfung“.

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

mfa-enabled-for-iam-Konsolenzugriff

Überprüft, ob die AWS Multi-Faktor-Authentifizierung (MFA) für alle AWS Identity and Access Management (IAM) -Benutzer aktiviert ist, die ein Konsolenkennwort verwenden. Die Regel ist COMPLIANT, wenn MFA aktiviert ist.

> **Note**
>
> Zeitplan für die Neubewertung
> Ein erneute Auswertung dieser Regel innerhalb von 4 Stunden hat keine Auswirkungen auf die Ergebnisse.
> Verwaltete Regeln und globale IAM-Ressourcentypen
> Die globalen IAM-Ressourcentypen, die vor Februar 2022 eingeführt wurden (`AWS::IAM::Group`,, und`AWS::IAM::User`) `AWS::IAM::Policy`AWS::IAM::Role, können nur AWS Config in AWS Regionen erfasst werden, in denen sie vor Februar 2022 verfügbar AWS Config waren. Diese Ressourcentypen können nicht in Regionen erfasst werden, die AWS Config nach Februar 2022 unterstützt werden. Eine Liste dieser Regionen finden Sie unter AWS Aufzeichnungsressourcen | Globale Ressourcen.
> Wenn Sie einen globalen IAM-Ressourcentyp in mindestens einer Region aufzeichnen, führen periodische Regeln, die die Einhaltung des globalen IAM-Ressourcentyps melden, Bewertungen in allen Regionen durch, in denen die periodische Regel hinzugefügt wurde, auch wenn Sie die Aufzeichnung des globalen IAM-Ressourcentyps in der Region, in der die periodische Regel hinzugefügt wurde, nicht aktiviert haben.
> Um unnötige Bewertungen zu vermeiden, sollten Sie nur regelmäßige Regeln einrichten, die die Einhaltung der Vorschriften für einen globalen IAM-Ressourcentyp an eine der unterstützten Regionen melden. Eine Liste der verwalteten Regeln, die in welchen Regionen unterstützt werden, finden Sie unter Liste der AWS Config verwalteten Regeln nach regionaler Verfügbarkeit.

ID: MFA_ENABLED_FOR_IAM_CONSOLE_ACCESS

Ressourcentypen: AWS::IAM::User

Auslösertyp: Regelmäßig

AWS-Region: Alle unterstützten AWS Regionen außer Asien-Pazifik (Thailand), Naher Osten (VAE), Asien-Pazifik (Hyderabad), Asien-Pazifik (Malaysia), Asien-Pazifik (Melbourne), Mexiko (Zentral), Israel (Tel Aviv), Asien-Pazifik (Taipeh), Kanada West (Calgary), Europa (Spanien), Europa (Zürich)

Parameter:

Keine

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

mq-active-broker-ldap-Authentifizierung

Überprüft, ob Amazon MQ ActiveMQ-Broker die LDAP-Authentifizierungsstrategie verwenden, um den Broker zu schützen. Die Regel lautet NON_COMPLIANT, wenn sie konfiguriert ist. AuthenticationStrategy ist nicht 'ldap'.

Kennung: MQ_ACTIVE_BROKER_LDAP_AUTHENTICATION

Ressourcentypen: AWS::AmazonMQ::Broker

Auslösertyp: Konfigurationsänderungen

AWS-Region: Alle unterstützten AWS Regionen außer China (Peking), Asien-Pazifik (Thailand), Asien-Pazifik (Hyderabad), Asien-Pazifik (Malaysia), AWS GovCloud (USA-Ost), AWS GovCloud (US-West), Mexiko (Zentral), Israel (Tel Aviv), Kanada West (Calgary), Europa (Spanien), China (Ningxia), Europa (Zürich)

Parameter:

Keine

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

mq-active-deployment-mode

Prüft den für die Broker-Engine von Amazon MQ ActiveMQ konfigurierten Bereitstellungsmodus. Die Regel ist NON_COMPLIANT, wenn der standardmäßige Modus „Single-Instance-Broker“ verwendet wird.

ID: MQ_ACTIVE_DEPLOYMENT_MODE

Ressourcentypen: AWS::AmazonMQ::Broker

Auslösertyp: Konfigurationsänderungen

AWS-Region: Alle unterstützten AWS Regionen außer Asien-Pazifik (Thailand), Asien-Pazifik (Hyderabad), Asien-Pazifik (Malaysia), AWS GovCloud (USA-Ost), AWS GovCloud (US-West), Mexiko (Zentral), Israel (Tel Aviv), Kanada West (Calgary), Europa (Spanien), Europa (Zürich)

Parameter:

Keine

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

mq-active-single-instance-broker-storage-type-efs

Überprüft, ob ein Einzelinstanz-Broker von Amazon MQ for ActiveMQ, der die Instance-Typfamilie mq.m5 verwendet, mit Amazon Elastic File System (EFS) für Broker-Speicher konfiguriert ist. Bei der Konfiguration lautet die Regel NON_COMPLIANT. StorageType ist nicht 'efs'.

Kennung: MQ_ACTIVE_SINGLE_INSTANCE_BROKER_STORAGE_TYPE_EFS

Ressourcentypen: AWS::AmazonMQ::Broker

Auslösertyp: Konfigurationsänderungen

AWS-Region: Alle unterstützten AWS Regionen außer China (Peking), Asien-Pazifik (Thailand), Asien-Pazifik (Hyderabad), Asien-Pazifik (Malaysia), AWS GovCloud (USA-Ost), AWS GovCloud (US-West), Mexiko (Zentral), Israel (Tel Aviv), Kanada West (Calgary), Europa (Spanien), China (Ningxia), Europa (Zürich)

Parameter:

Keine

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

mq-automatic-minor-version-upgrade-fähig

Prüft, ob für Amazon-MQ-Broker automatische Unterversions-Upgrades aktiviert sind. Die Regel lautet NON_COMPLIANT, wenn das Feld 'AutoMinorVersionUpgrade' nicht für einen Amazon MQ-Broker aktiviert ist.

ID: MQ_AUTOMATIC_MINOR_VERSION_UPGRADE_ENABLED

Ressourcentypen: AWS::AmazonMQ::Broker

Auslösertyp: Regelmäßig

AWS-Region: Alle unterstützten AWS Regionen außer China (Peking), Asien-Pazifik (Thailand), Asien-Pazifik (Jakarta), Afrika (Kapstadt), Naher Osten (VAE), Asien-Pazifik (Hyderabad), Asien-Pazifik (Malaysia), Asien-Pazifik (Melbourne), AWS GovCloud (US-Ost), AWS GovCloud (US-West), Mexiko (Zentral), Israel (Tel Aviv), Kanada West (Calgary), Europa (Spanien), China (Ningxia), Europa (Region Zürich

Parameter:

Keine

AWS CloudFormation Schablone

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

mq-auto-minor-version-upgrade-fähig

Prüft, ob für Amazon-MQ-Broker automatische Unterversions-Upgrades aktiviert sind. Die Regel lautet NON_COMPLIANT, wenn das Feld 'AutoMinorVersionUpgrade' nicht für einen Amazon MQ-Broker aktiviert ist.

ID: MQ_AUTO_MINOR_VERSION_UPGRADE_ENABLED

Ressourcentypen: AWS::AmazonMQ::Broker

Auslösertyp: Konfigurationsänderungen

AWS-Region: Alle unterstützten AWS Regionen außer Asien-Pazifik (Thailand), Asien-Pazifik (Hyderabad), Asien-Pazifik (Malaysia), AWS GovCloud (USA-Ost), AWS GovCloud (US-West), Mexiko (Zentral), Israel (Tel Aviv), Kanada West (Calgary), Europa (Spanien), Europa (Zürich)

Parameter:

Keine

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

mq-broker-general-logging-aktiviert

Prüft, ob Amazon MQ-Broker die allgemeine Protokollierung aktiviert haben. Die Regel ist NON_COMPLIANT, wenn configuration.logs.GENERAL den Wert false hat.

Kennung: MQ_BROKER_GENERAL_LOGGING_ENABLED

Ressourcentypen: AWS::AmazonMQ::Broker

Auslösertyp: Konfigurationsänderungen

AWS-Region: Alle unterstützten AWS Regionen außer China (Peking), Asien-Pazifik (Thailand), Asien-Pazifik (Hyderabad), Asien-Pazifik (Malaysia), AWS GovCloud (USA-Ost), AWS GovCloud (US-West), Mexiko (Zentral), Israel (Tel Aviv), Kanada West (Calgary), Europa (Spanien), China (Ningxia), Europa (Zürich)

Parameter:

Keine

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

mq-cloudwatch-audit-logging-aktiviert

Prüft, ob Amazon MQ-Broker die CloudWatch Amazon-Auditprotokollierung aktiviert haben. Die Regel ist NON_COMPLIANT, wenn für einen Broker die Audit-Protokollierung nicht aktiviert ist.

ID: MQ_CLOUDWATCH_AUDIT_LOGGING_ENABLED

Ressourcentypen: AWS::AmazonMQ::Broker

Auslösertyp: Regelmäßig

AWS-Region: Alle unterstützten AWS Regionen außer China (Peking), Asien-Pazifik (Thailand), Asien-Pazifik (Jakarta), Afrika (Kapstadt), Naher Osten (VAE), Asien-Pazifik (Hyderabad), Asien-Pazifik (Malaysia), Asien-Pazifik (Melbourne), AWS GovCloud (US-Ost), AWS GovCloud (US-West), Mexiko (Zentral), Israel (Tel Aviv), Kanada West (Calgary), Europa (Spanien), China (Ningxia), Europa (Region Zürich)

Parameter:

Keine

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

mq-cloudwatch-audit-log-aktiviert

Prüft, ob bei einem Amazon MQ-Broker die CloudWatch Auditprotokollierung aktiviert ist. Die Regel lautet NON_COMPLIANT, wenn für den Broker die Audit-Protokollierung nicht aktiviert ist.

Kennung: MQ_CLOUDWATCH_AUDIT_LOG_ENABLED

Ressourcentypen: AWS::AmazonMQ::Broker

Auslösertyp: Konfigurationsänderungen

AWS-Region: Alle unterstützten AWS Regionen außer China (Peking), Asien-Pazifik (Thailand), Asien-Pazifik (Hyderabad), Asien-Pazifik (Malaysia), Mexiko (Zentral), Israel (Tel Aviv), Kanada West (Calgary), Europa (Spanien), China (Ningxia), Europa (Zürich)

Parameter:

Keine

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

mq-no-public-access

Prüft, ob Amazon-MQ-Broker nicht öffentlich zugänglich sind. Die Regel lautet NON_COMPLIANT, wenn das Feld 'PubliclyAccessible' für einen Amazon MQ-Broker auf true gesetzt ist.

ID: MQ_NO_PUBLIC_ACCESS

Ressourcentypen: AWS::AmazonMQ::Broker

Auslösertyp: Regelmäßig

AWS-Region: Alle unterstützten AWS Regionen außer China (Peking), Asien-Pazifik (Thailand), Asien-Pazifik (Jakarta), Afrika (Kapstadt), Naher Osten (VAE), Asien-Pazifik (Hyderabad), Asien-Pazifik (Malaysia), Asien-Pazifik (Melbourne), AWS GovCloud (US-Ost), AWS GovCloud (US-West), Mexiko (Zentral), Israel (Tel Aviv), Kanada West (Calgary), Europa (Spanien), China (Ningxia), Europa (Region Zürich)

Parameter:

Keine

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

mq-rabbit-deployment-mode

Prüft den für die Broker-Engine von Amazon MQ RabbitMQ konfigurierten Bereitstellungsmodus. Die Regel ist NON_COMPLIANT, wenn der standardmäßige Modus „Single-Instance-Broker“ verwendet wird.

ID: MQ_RABBIT_DEPLOYMENT_MODE

Ressourcentypen: AWS::AmazonMQ::Broker

Auslösertyp: Konfigurationsänderungen

AWS-Region: Alle unterstützten AWS Regionen außer Asien-Pazifik (Thailand), Asien-Pazifik (Hyderabad), Asien-Pazifik (Malaysia), Asien-Pazifik (Melbourne), AWS GovCloud (USA-Ost), AWS GovCloud (US-West), Mexiko (Zentral), Israel (Tel Aviv), Kanada West (Calgary), Europa (Spanien), Europa (Zürich)

Parameter:

Keine

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

msk-cluster-public-access-deaktiviert

Prüft, ob der öffentliche Zugriff auf Amazon MSK-Clustern deaktiviert ist. Die Regel lautet NON_COMPLIANT, wenn der öffentliche Zugriff auf einem Amazon MSK-Cluster nicht deaktiviert ist.

Kennung: MSK_CLUSTER_PUBLIC_ACCESS_DISABLED

Ressourcentypen: AWS::MSK::Cluster

Auslösertyp: Konfigurationsänderungen

AWS-Region: Alle unterstützten AWS Regionen außer Asien-Pazifik (Thailand), Naher Osten (VAE), Asien-Pazifik (Hyderabad), Asien-Pazifik (Seoul), Asien-Pazifik (Malaysia), Mexiko (Zentral), Israel (Tel Aviv), Kanada West (Calgary), Europa (Spanien), Europa (Zürich)

Parameter:

Keine

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

msk-connect-connector-logging-aktiviert

Prüft, ob Amazon MSK Connector die Protokollierung für eines der Protokollziele aktiviert hat. Die Regel lautet NON_COMPLIANT, wenn Amazon MSK Connector die Protokollierung nicht aktiviert hat.

Kennung: MSK_CONNECT_CONNECTOR_LOGGING_ENABLED

Ressourcentypen: AWS::KafkaConnect::Connector

Auslösertyp: Konfigurationsänderungen

AWS-Region: Nur verfügbar in Europa (Stockholm), Asien-Pazifik (Mumbai), Europa (Paris), USA Ost (Ohio), Europa (Irland), Europa (Frankfurt), Südamerika (Sao Paulo), USA Ost (Nord-Virginia), Europa (London), Asien-Pazifik (Tokio), USA West (Oregon), USA West (Nordkalifornien), Asien-Pazifik (Singapur), Asien-Pazifik (Sydney), Kanada (Zentral)

Parameter:

Keine

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

msk-enhanced-monitoring-enabled

Prüft, ob die erweiterte Überwachung für einen Amazon-MSK-Cluster aktiviert ist, der auf PER_TOPIC_PER_BROKER oder PER_TOPIC_PER_PARTITION festgelegt ist. Die Regel ist NON_COMPLIANT, wenn die erweiterte Überwachung aktiviert und auf DEFAULT oder PER_BROKER festgelegt ist.

ID: MSK_ENHANCED_MONITORING_ENABLED

Ressourcentypen: AWS::MSK::Cluster

Auslösertyp: Konfigurationsänderungen

AWS-Region: Alle unterstützten AWS Regionen außer Asien-Pazifik (Thailand), Asien-Pazifik (Malaysia), AWS GovCloud (USA-Ost), AWS GovCloud (US-West), Mexiko (Zentral), Israel (Tel Aviv), Kanada West (Calgary)

Parameter:

Keine

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

msk-in-cluster-node-TLS erforderlich

Prüft, ob ein Amazon-MSK-Cluster die Verschlüsselung bei der Übertragung erzwingt, indem er für die Broker-Knoten des Clusters HTTPS (TLS) verwendet. Die Regel ist NON_COMPLIANT, wenn Klartextkommunikation für Broker-Knotenverbindungen in Clustern aktiviert ist.

ID: MSK_IN_CLUSTER_NODE_REQUIRE_TLS

Ressourcentypen: AWS::MSK::Cluster

Auslösertyp: Konfigurationsänderungen

AWS-Region: Alle unterstützten AWS Regionen außer Asien-Pazifik (Thailand), Asien-Pazifik (Malaysia), AWS GovCloud (USA-Ost), AWS GovCloud (US-West), Mexiko (Zentral), Israel (Tel Aviv), Kanada West (Calgary)

Parameter:

Keine

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

msk-unrestricted-access-check

Prüft, ob für einen Amazon MSK-Cluster der unauthentifizierte Zugriff deaktiviert ist. Die Regel lautet NON_COMPLIANT, wenn für Amazon MSK Cluster der unauthentifizierte Zugriff aktiviert ist.

Kennung: MSK_UNRESTRICTED_ACCESS_CHECK

Ressourcentypen: AWS::MSK::Cluster

Auslösertyp: Konfigurationsänderungen

AWS-Region: Alle unterstützten AWS Regionen außer Asien-Pazifik (Thailand), Naher Osten (VAE), Asien-Pazifik (Hyderabad), Asien-Pazifik (Seoul), Asien-Pazifik (Malaysia), Mexiko (Zentral), Israel (Tel Aviv), Kanada West (Calgary), Europa (Spanien), Europa (Zürich)

Parameter:

Keine

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

multi-region-cloudtrail-enabled

> **Important**
>
> Bei dieser Regel unterscheiden sich die Regel-ID (MULTI_REGION_CLOUD_TRAIL_ENABLED) und der Regelname (). multi-region-cloudtrail-enabled

Prüft, ob es mindestens eine Multiregion gibt. AWS CloudTrail Die Regel ist NON_COMPLIANT, wenn die Trails nicht mit den Eingabeparametern übereinstimmen. Die Regel lautet NON_COMPLIANT, wenn das `ExcludeManagementEventSources` Feld nicht leer ist oder wenn sie so konfiguriert AWS CloudTrail ist, dass Verwaltungsereignisse wie AWS KMS Ereignisse oder Amazon RDS Data API-Ereignisse ausgeschlossen werden.

ID: MULTI_REGION_CLOUD_TRAIL_ENABLED

Auslösertyp: Regelmäßig

AWS-Region: Alle unterstützten Regionen AWS

Parameter:

s3 BucketName (fakultativ), Typ: Zeichenfolge

> Name des Amazon S3 S3-Buckets AWS CloudTrail , an den Protokolldateien gesendet werden sollen.

snsTopicArn (Fakultativ), Typ: Zeichenfolge

Amazon SNS SNS-Thema ARN AWS CloudTrail zur Verwendung für Benachrichtigungen.

cloudWatchLogsLogGroupArn (Fakultativ), Typ: Zeichenfolge

CloudWatch Amazon-Protokollgruppen-ARN AWS CloudTrail , an die Daten gesendet werden sollen.

includeManagementEvents (Fakultativ), Typ: Boolesch

Ereignisauswahl für die Aufnahme von Verwaltungsereignissen für den AWS CloudTrail.

readWriteType (Fakultativ), Typ: Zeichenfolge

Typ der Ereignisse, die aufgezeichnet werden sollen. Gültige Werte sind ReadOnly, WriteOnly und ALL.

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

nacl-no-unrestricted-ssh-rdp

Überprüft, ob die Standardports für SSH/RDP eingehenden Datenverkehr für Netzwerkzugriffskontrolllisten (NACLs) uneingeschränkt sind. Die Regel ist NON_COMPLIANT, wenn ein eingehender NACL-Eintrag für die Ports 22 oder 3389 einen CIDR-Block des Typs Quell-TCP oder -UDP zulässt.

ID: NACL_NO_UNRESTRICTED_SSH_RDP

Ressourcentypen: AWS::EC2::NetworkAcl

Auslösertyp: Konfigurationsänderungen

AWS-Region: Alle unterstützten AWS Regionen außer Asien-Pazifik (Thailand), Asien-Pazifik (Malaysia), Mexiko (Zentral) und Kanada West (Calgary)

Parameter:

Keine

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

neptune-cluster-backup-retention-überprüfen

Prüft, ob ein Aufbewahrungszeitraum für Cluster der Amazon Neptune-DB auf eine bestimmte Anzahl von Tagen festgelegt ist. Die Regel ist NON_COMPLIANT, wenn der Aufbewahrungszeitraum kürzer ist als durch den Parameter angegeben.

ID: NEPTUNE_CLUSTER_BACKUP_RETENTION_CHECK

Ressourcentypen: AWS::RDS::DBCluster

Auslösertyp: Konfigurationsänderungen

AWS-Region: Alle unterstützten AWS Regionen außer China (Peking), Asien-Pazifik (Thailand), Asien-Pazifik (Jakarta), Asien-Pazifik (Hyderabad), Asien-Pazifik (Malaysia), Asien-Pazifik (Melbourne), Europa (Mailand), AWS GovCloud (USA-Ost), AWS GovCloud (US-West), Mexiko (Zentral), Kanada West (Calgary), Europa (Spanien), Europa (Zürich)

Parameter:

minimumBackupRetentionZeitraum (optional), Typ: int

> Mindestaufbewahrungszeitraum für Backups. Gültige Werte: 1 bis 35; Standardwert: 7. Die Regel lautet NON_COMPLIANT, wenn der Wert größer als " backupRetentionPeriod ist. Die Regel ist KONFORM, wenn der Wert kleiner oder gleich " backupRetentionPeriod ist.

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

neptune-cluster-cloudwatch-log-exportfähig

Prüft, ob für einen Amazon Neptune Neptune-Cluster der Protokollexport für CloudWatch Audit-Logs aktiviert ist. Die Regel lautet NON_COMPLIANT, wenn für einen Neptune-Cluster der Protokollexport für CloudWatch Audit-Logs nicht aktiviert ist.

ID: NEPTUNE_CLUSTER_CLOUDWATCH_LOG_EXPORT_ENABLED

Ressourcentypen: AWS::RDS::DBCluster

Auslösertyp: Konfigurationsänderungen

AWS-Region: Alle unterstützten AWS Regionen außer China (Peking), Asien-Pazifik (Thailand), Asien-Pazifik (Jakarta), Asien-Pazifik (Hyderabad), Asien-Pazifik (Malaysia), Asien-Pazifik (Melbourne), Europa (Mailand), AWS GovCloud (USA-Ost), AWS GovCloud (US-West), Mexiko (Zentral), Kanada West (Calgary), Europa (Spanien), Europa (Zürich)

Parameter:

Keine

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

neptune-cluster-copy-tags-to-snapshot-enabled

Prüft, ob ein Amazon Neptune-Cluster so konfiguriert ist, dass er bei der Erstellung der Snapshots alle Tags nach Snapshots kopiert. Die Regel ist NON_COMPLIANT, wenn 'Snapshot' copyTagsTo auf False gesetzt ist.

ID: NEPTUNE_CLUSTER_COPY_TAGS_TO_SNAPSHOT_ENABLED

Ressourcentypen: AWS::RDS::DBCluster

Auslösertyp: Konfigurationsänderungen

AWS-Region: Alle unterstützten AWS Regionen außer China (Peking), Asien-Pazifik (Thailand), Asien-Pazifik (Jakarta), Asien-Pazifik (Hyderabad), Asien-Pazifik (Malaysia), Asien-Pazifik (Melbourne), Europa (Mailand), AWS GovCloud (USA-Ost), AWS GovCloud (US-West), Mexiko (Zentral), Kanada West (Calgary), Europa (Spanien), Europa (Zürich)

Parameter:

Keine

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

neptune-cluster-deletion-protection-aktiviert

Prüft, ob für einen Cluster der Amazon-Neptune-DB der Löschschutz aktiviert ist. Die Regel ist NON_COMPLIANT, wenn bei einem Amazon Neptune-Cluster das Feld „Schutz vor Löschung“ auf „False“ festgelegt ist.

ID: NEPTUNE_CLUSTER_DELETION_PROTECTION_ENABLED

Ressourcentypen: AWS::RDS::DBCluster

Auslösertyp: Konfigurationsänderungen

AWS-Region: Alle unterstützten AWS Regionen außer China (Peking), Asien-Pazifik (Thailand), Asien-Pazifik (Jakarta), Asien-Pazifik (Hyderabad), Asien-Pazifik (Malaysia), Asien-Pazifik (Melbourne), Europa (Mailand), AWS GovCloud (USA-Ost), AWS GovCloud (US-West), Mexiko (Zentral), Kanada West (Calgary), Europa (Spanien), Europa (Zürich)

Parameter:

Keine

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

neptune-cluster-encrypted

Prüft, ob die Speicherverschlüsselung für Ihre Cluster der Amazon-Neptune-DB aktiviert ist. Die Regel ist NON_COMPLIANT, wenn die Speicherverschlüsselung nicht aktiviert ist.

ID: NEPTUNE_CLUSTER_ENCRYPTED

Ressourcentypen: AWS::RDS::DBCluster

Auslösertyp: Konfigurationsänderungen

AWS-Region: Alle unterstützten AWS Regionen außer China (Peking), Asien-Pazifik (Thailand), Asien-Pazifik (Jakarta), Asien-Pazifik (Hyderabad), Asien-Pazifik (Malaysia), Asien-Pazifik (Melbourne), Europa (Mailand), AWS GovCloud (USA-Ost), AWS GovCloud (US-West), Mexiko (Zentral), Kanada West (Calgary), Europa (Spanien), Europa (Zürich)

Parameter:

KmsKeyArns (Fakultativ), Typ: CSV

> Eine durch Kommas getrennte Liste von KMS-Schlüsseln ARNs , die mit denen KmsKeyId des verschlüsselten Clusters verglichen werden sollen.

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

neptune-cluster-iam-database-Authentifizierung

Prüft, ob für einen Amazon Neptune Neptune-Cluster die AWS Identity and Access Management (IAM) -Datenbankauthentifizierung aktiviert ist. Die Regel ist NON_COMPLIANT, wenn für einen Amazon-Neptune-Cluster die IAM-Datenbankauthentifizierung nicht aktiviert ist.

ID: NEPTUNE_CLUSTER_IAM_DATABASE_AUTHENTICATION

Ressourcentypen: AWS::RDS::DBCluster

Auslösertyp: Konfigurationsänderungen

AWS-Region: Alle unterstützten AWS Regionen außer China (Peking), Asien-Pazifik (Thailand), Asien-Pazifik (Jakarta), Asien-Pazifik (Hyderabad), Asien-Pazifik (Malaysia), Asien-Pazifik (Melbourne), Europa (Mailand), AWS GovCloud (USA-Ost), AWS GovCloud (US-West), Mexiko (Zentral), Kanada West (Calgary), Europa (Spanien), Europa (Zürich)

Parameter:

Keine

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

neptune-cluster-multi-az-aktiviert

Prüft, ob für einen Amazon-Neptune-Cluster die Multi-AZ-Replikation von Amazon RDS konfiguriert ist. Die Regel ist NON_COMPLIANT, wenn die Multi-AZ-Replikation nicht aktiviert ist.

ID: NEPTUNE_CLUSTER_MULTI_AZ_ENABLED

Ressourcentypen: AWS::RDS::DBCluster

Auslösertyp: Konfigurationsänderungen

AWS-Region: Alle unterstützten AWS Regionen außer China (Peking), Asien-Pazifik (Thailand), Asien-Pazifik (Jakarta), Asien-Pazifik (Hyderabad), Asien-Pazifik (Malaysia), Asien-Pazifik (Melbourne), Europa (Mailand), AWS GovCloud (USA-Ost), AWS GovCloud (US-West), Mexiko (Zentral), Kanada West (Calgary), Europa (Spanien), Europa (Zürich)

Parameter:

Keine

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

neptune-cluster-snapshot-encrypted

Überprüft, ob der Cluster einer Amazon-Neptune-DB verschlüsselte Snapshots enthält. Die Regel ist NON_COMPLIANT, wenn ein Neptune-Cluster keine verschlüsselten Snapshots enthält.

ID: NEPTUNE_CLUSTER_SNAPSHOT_ENCRYPTED

Ressourcentypen: AWS::RDS::DBClusterSnapshot

Auslösertyp: Konfigurationsänderungen

AWS-Region: Alle unterstützten AWS Regionen außer China (Peking), Asien-Pazifik (Thailand), Asien-Pazifik (Jakarta), Asien-Pazifik (Hyderabad), Asien-Pazifik (Malaysia), Asien-Pazifik (Melbourne), Europa (Mailand), AWS GovCloud (USA-Ost), AWS GovCloud (US-West), Mexiko (Zentral), Israel (Tel Aviv), Kanada West (Calgary), Europa (Spanien), Europa (Zürich)

Parameter:

Keine

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

neptune-cluster-snapshot-public-verboten

Prüft, ob ein manueller DB-Cluster-Snapshot von Amazon Neptune öffentlich ist. Die Regel ist NON_COMPLIANT, wenn es vorhandene und neue Neptune-Cluster-Snapshots gibt, die öffentlich zugänglich sind.

ID: NEPTUNE_CLUSTER_SNAPSHOT_PUBLIC_PROHIBITED

Ressourcentypen: AWS::RDS::DBClusterSnapshot

Auslösertyp: Konfigurationsänderungen

AWS-Region: Alle unterstützten AWS Regionen außer China (Peking), Asien-Pazifik (Thailand), Asien-Pazifik (Jakarta), Asien-Pazifik (Hyderabad), Asien-Pazifik (Malaysia), Asien-Pazifik (Melbourne), Europa (Mailand), AWS GovCloud (US-Ost), AWS GovCloud (US-West), Mexiko (Zentral), Israel (Tel Aviv), Kanada West (Calgary), Europa (Spanien), China (Ningxia), Europa (Zürich)

Parameter:

Keine

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

netfw-deletion-protection-enabled

Prüft, ob die AWS Network Firewall den Löschschutz aktiviert hat. Die Regel ist NON_COMPLIANT, wenn für Network Firewall kein Löschschutz aktiviert ist.

ID: NETFW_DELETION_PROTECTION_ENABLED

Ressourcentypen: AWS::NetworkFirewall::Firewall

Auslösertyp: Konfigurationsänderungen

AWS-Region: Alle unterstützten AWS Regionen außer China (Peking), Asien-Pazifik (Thailand), Asien-Pazifik (Malaysia), AWS GovCloud (USA-Ost), AWS GovCloud (US-West), Mexiko (Zentral), Kanada West (Calgary), China (Ningxia)

Parameter:

Keine

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

netfw-logging-enabled

Überprüft, ob bei AWS Netzwerk-Firewall-Firewalls die Protokollierung aktiviert ist. Die Regel ist NON_COMPLIANT, wenn kein Protokollierungstyp konfiguriert ist. Sie können angeben, welchen Protokollierungstyp die Regel prüfen soll.

ID: NETFW_LOGGING_ENABLED

Ressourcentypen: AWS::NetworkFirewall::LoggingConfiguration

Auslösertyp: Regelmäßig

AWS-Region: Alle unterstützten AWS Regionen außer China (Peking), Asien-Pazifik (Thailand), Asien-Pazifik (Malaysia), AWS GovCloud (USA-Ost), AWS GovCloud (US-West), Mexiko (Zentral), Kanada West (Calgary), China (Ningxia)

Parameter:

logType (optional), Typ: Zeichenfolge

logType (optional): Protokolltyp für die Regel, die nach Firewalls suchen soll: „alert“, „flow“ oder „both“.

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

netfw-multi-az-enabled

Überprüft, ob AWS Netzwerk-Firewall-Firewalls in mehreren Availability Zones eingesetzt werden. Die Regel ist NON_COMPLIANT, wenn Firewalls nur in einer Availability Zone oder in weniger Zones bereitgestellt wurden als im optionalen Parameter angegeben.

ID: NETFW_MULTI_AZ_ENABLED

Ressourcentypen: AWS::NetworkFirewall::Firewall

Auslösertyp: Konfigurationsänderungen

AWS-Region: Alle unterstützten AWS Regionen außer China (Peking), Asien-Pazifik (Thailand), Asien-Pazifik (Malaysia), AWS GovCloud (USA-Ost), AWS GovCloud (US-West), Mexiko (Zentral), Kanada West (Calgary), China (Ningxia)

Parameter:

availabilityZones (optional), Typ: int

Die Anzahl der erwarteten Availability Zones.

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

netfw-policy-default-action-fragment-Pakete

Prüft, ob eine AWS Netzwerk-Firewall-Richtlinie mit einer benutzerdefinierten statusfreien Standardaktion für fragmentierte Pakete konfiguriert ist. Die Regel ist NON_COMPLIANT, wenn

die zustandslose Standardaktion für fragmentierte Pakete nicht mit der benutzerdefinierten Standardaktion übereinstimmt.

ID: NETFW_POLICY_DEFAULT_ACTION_FRAGMENT_PACKETS

Ressourcentypen: AWS::NetworkFirewall::FirewallPolicy

Auslösertyp: Konfigurationsänderungen

AWS-Region: Alle unterstützten AWS Regionen außer China (Peking), Asien-Pazifik (Thailand), Asien-Pazifik (Malaysia), AWS GovCloud (USA-Ost), AWS GovCloud (US-West), Mexiko (Zentral), Kanada West (Calgary), China (Ningxia)

Parameter:

statelessFragmentDefaultAktionen, Typ: CSV

> Eine durch Kommata getrennte Liste der Werte. Sie können maximal zwei auswählen. Zu den zulässigen Werten gehören „aws:pass“, „aws:drop“ und „aws:forward_to_sfe“.

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

netfw-policy-default-action-vollständige Pakete

Prüft, ob eine AWS Netzwerk-Firewall-Richtlinie mit einer benutzerdefinierten statusfreien Standardaktion für vollständige Pakete konfiguriert ist. Diese Regel ist NON_COMPLIANT, wenn die zustandslose Standardaktion für vollständige Pakete nicht mit der benutzerdefinierten statuslosen Standardaktion übereinstimmt.

ID: NETFW_POLICY_DEFAULT_ACTION_FULL_PACKETS

Ressourcentypen: AWS::NetworkFirewall::FirewallPolicy

Auslösertyp: Konfigurationsänderungen

AWS-Region: Alle unterstützten AWS Regionen außer China (Peking), Asien-Pazifik (Thailand), Asien-Pazifik (Malaysia), AWS GovCloud (USA-Ost), AWS GovCloud (US-West), Mexiko (Zentral), Kanada West (Calgary), China (Ningxia)

Parameter:

statelessDefaultActions, Typ: CSV

Eine durch Kommata getrennte Liste der Werte. Sie können maximal zwei auswählen. Zu den zulässigen Werten gehören „aws:pass“, „aws:drop“ und „aws:forward_to_sfe“.

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

netfw-policy-rule-group-assoziiert

Prüfen Sie, ob die AWS Netzwerk-Firewall-Richtlinie statusbehafteten ODER statusfreien Regelgruppen zugeordnet ist. Diese Regel ist NON_COMPLIANT, wenn der Network-Firewall-Richtlinie keine zustandsbehafteten oder zustandslosen Regelgruppen zugeordnet sind, und COMPLIANT, wenn eine der Regelgruppen existiert.

ID: NETFW_POLICY_RULE_GROUP_ASSOCIATED

Ressourcentypen: AWS::NetworkFirewall::FirewallPolicy

Auslösertyp: Konfigurationsänderungen

AWS-Region: Alle unterstützten AWS Regionen außer China (Peking), Asien-Pazifik (Thailand), Asien-Pazifik (Malaysia), Mexiko (Zentral), Kanada West (Calgary), China (Ningxia)

Parameter:

Keine

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

netfw-stateless-rule-group-nicht leer

Prüft, ob eine zustandslose Firewall-Regelgruppe von Network Firewall Regeln enthält. Die Regel ist NON_COMPLIANT, wenn eine zustandslose Regelgruppe von Network Firewall keine Regeln enthält.

ID: NETFW_STATELESS_RULE_GROUP_NOT_EMPTY

Ressourcentypen: AWS::NetworkFirewall::RuleGroup

Auslösertyp: Konfigurationsänderungen

AWS-Region: Alle unterstützten AWS Regionen außer China (Peking), Asien-Pazifik (Thailand), Asien-Pazifik (Malaysia), Mexiko (Zentral), Kanada West (Calgary), China (Ningxia)

Parameter:

Keine

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

netfw-subnet-change-protection-aktiviert

Überprüft, ob bei der AWS Network Firewall der Subnetzänderungsschutz aktiviert ist. Die Regel lautet NON_COMPLIANT, wenn der Subnetzänderungsschutz nicht aktiviert ist.

Kennung: NETFW_SUBNET_CHANGE_PROTECTION_ENABLED

Ressourcentypen: AWS::NetworkFirewall::Firewall

Auslösertyp: Konfigurationsänderungen

AWS-Region: Alle unterstützten AWS Regionen außer Naher Osten (Bahrain), China (Peking), Asien-Pazifik (Thailand), Asien-Pazifik (Malaysia), Mexiko (Zentral), Kanada West (Calgary), China (Ningxia)

Parameter:

Keine

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

nlb-cross-zone-load-Balancing aktiviert

Überprüft, ob der zonenübergreifende Load Balancing auf Network Load Balancers () aktiviert ist. NLBs Die Regel ist NON_COMPLIANT, wenn für einen NLB kein zonenübergreifendes Load Balancing aktiviert ist.

ID: NLB_CROSS_ZONE_LOAD_BALANCING_ENABLED

Ressourcentypen: AWS::ElasticLoadBalancingV2::LoadBalancer

Auslösertyp: Konfigurationsänderungen

AWS-Region: Alle unterstützten AWS Regionen außer China (Peking), Asien-Pazifik (Thailand), Asien-Pazifik (Jakarta), Naher Osten (VAE), Asien-Pazifik (Hyderabad), Asien-Pazifik (Malaysia), Asien-Pazifik (Melbourne), AWS GovCloud (US-Ost), AWS GovCloud (US-West), Mexiko (Zentral), Israel (Tel Aviv), Kanada West (Calgary), Europa (Spanien), China (Ningxia), Europa (Zürich)

Parameter:

Keine

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

nlb-internal-scheme-check

Prüft, ob ein Network Load Balancer Balancer-Schema intern ist. Die Regel ist NON_COMPLIANT, wenn configuration.scheme nicht auf internal gesetzt ist.

Kennung: NLB_INTERNAL_SCHEME_CHECK

Ressourcentypen: AWS::ElasticLoadBalancingV2::LoadBalancer

Auslösertyp: Konfigurationsänderungen

AWS-Region: Alle unterstützten AWS Regionen außer China (Peking), Asien-Pazifik (Thailand), Asien-Pazifik (Malaysia), AWS GovCloud (USA-Ost), AWS GovCloud (US-West), Mexiko (Zentral), China (Ningxia)

Parameter:

Keine

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

nlb-listener-tagged

Überprüft, ob Network Load Balancer Balancer-Listener Tags haben. Optional können Sie Tag-Schlüssel angeben. Die Regel lautet NON_COMPLIANT, wenn keine Tags vorhanden sind oder wenn die angegebenen Tag-Schlüssel nicht vorhanden sind. Die Regel sucht nicht nach Tags, die mit 'aws: 'beginnen.

Kennung: NLB_LISTENER_TAGGED

Ressourcentypen: AWS::ElasticLoadBalancingV2::Listener

Auslösertyp: Konfigurationsänderungen

AWS-Region: Alle unterstützten AWS Regionen außer China (Peking), Asien-Pazifik (Thailand), Asien-Pazifik (Jakarta), Naher Osten (VAE), Asien-Pazifik (Hyderabad), Asien-Pazifik (Malaysia), Asien-Pazifik (Melbourne), AWS GovCloud (US-Ost), AWS GovCloud (US-West), Mexiko (Zentral), Israel (Tel Aviv), Kanada West (Calgary), Europa (Spanien), China (Ningxia), Europa (Zürich)

Parameter:

requiredKeyTags (Fakultativ), Typ: CSV

> Durch Kommas getrennte Liste von Tag-Schlüsseln, die von der Regel überprüft werden sollen. Falls angegeben, lautet die Regel NON_COMPLIANT, wenn die ausgewertete Ressource diese Schlüssel nicht enthält. Bei Tag-Schlüsseln wird die Groß- und Kleinschreibung beachtet. Tag-Schlüssel, die mit „aws:“ beginnen, sind nicht erlaubt.

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

nlb-logging-enabled

Prüft, ob die Zugriffsprotokollierung für Network Load Balancer aktiviert ist. Die Regel lautet NON_COMPLIANT, wenn die Zugriffsprotokollierung für einen Network Load Balancer nicht aktiviert ist.

Kennung: NLB_LOGGING_ENABLED

Ressourcentypen: AWS::ElasticLoadBalancingV2::LoadBalancer

Auslösertyp: Regelmäßig

AWS-Region: Alle unterstützten AWS Regionen außer Asien-Pazifik (Thailand), Asien-Pazifik (Malaysia), Mexiko (Zentral), Kanada West (Calgary), China (Ningxia)

Parameter:

Keine

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

no-unrestricted-route-to-igw

Prüft, ob die Routentabelle öffentliche Routen zu einem Internet-Gateway (IGW) enthält. Die Regel ist NON_COMPLIANT, wenn eine Route zu einem IGW den Ziel-CIDR-Block „0.0.0.0/0“ oder „::/0“ hat oder wenn ein CIDR-Zielblock nicht mit dem Regelparameter übereinstimmt.

ID: NO_UNRESTRICTED_ROUTE_TO_IGW

Ressourcentypen: AWS::EC2::RouteTable

Auslösertyp: Konfigurationsänderungen

AWS-Region: Alle unterstützten AWS Regionen außer Asien-Pazifik (Taipeh) und Kanada West (Calgary)

Parameter:

routeTableIds (Fakultativ), Typ: CSV

Durch Kommas getrennte Liste von Routentabellen IDs , die Routen zu einem Internet Gateway mit einem CIDR-Zielblock von '0.0.0.0/0' oder ': :/0' enthalten können.

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

opensearch-access-control-enabled

Überprüft, ob für Amazon OpenSearch Service-Domains eine differenzierte Zugriffskontrolle aktiviert ist. Die Regel lautet NON_COMPLIANT, wenn sie für die AdvancedSecurityOptions Service-Domain nicht aktiviert ist. OpenSearch

ID: OPENSEARCH_ACCESS_CONTROL_ENABLED

Ressourcentypen: AWS::OpenSearch::Domain

Auslösertyp: Konfigurationsänderungen

AWS-Region: Alle unterstützten AWS Regionen außer China (Peking), Asien-Pazifik (Thailand), Naher Osten (VAE), Asien-Pazifik (Hyderabad), Asien-Pazifik (Malaysia), Asien-Pazifik (Melbourne), AWS GovCloud (USA-Ost), AWS GovCloud (US-West), Mexiko (Zentral), Israel (Tel Aviv), Kanada West (Calgary), Europa (Spanien), China (Ningxia), Europa (Zürich)

Parameter:

Keine

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

opensearch-audit-logging-enabled

Prüft, ob für Amazon OpenSearch Service-Domains die Audit-Protokollierung aktiviert ist. Die Regel lautet NON_COMPLIANT, wenn für eine OpenSearch Service-Domain die Audit-Protokollierung nicht aktiviert ist.

ID: OPENSEARCH_AUDIT_LOGGING_ENABLED

Ressourcentypen: AWS::OpenSearch::Domain

Auslösertyp: Konfigurationsänderungen

AWS-Region: Alle unterstützten AWS Regionen außer China (Peking), Asien-Pazifik (Thailand), Naher Osten (VAE), Asien-Pazifik (Hyderabad), Asien-Pazifik (Malaysia), Asien-Pazifik (Melbourne), AWS GovCloud (USA-Ost), AWS GovCloud (US-West), Mexiko (Zentral), Israel (Tel Aviv), Kanada West (Calgary), Europa (Spanien), China (Ningxia), Europa (Zürich)

Parameter:

cloudWatchLogsLogGroupArnList (Fakultativ), Typ: CSV

> Kommagetrennte Liste von Amazon-Ressourcennamen (ARNs) für Amazon CloudWatch Logs-Protokollgruppen. Die Regel prüft, ob die angegebenen Protokollgruppen für Audit-Logs konfiguriert sind.
>
> Gültige Werte sind `arn:aws:logs:region:account-id:log-group:log_group_name:*` und `arn:aws:logs:region:account-id:log-group:log_group_name`.

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

opensearch-data-node-fault-Toleranz

Überprüft, ob Amazon OpenSearch Service-Domains mit mindestens drei Datenknoten konfiguriert sind und zoneAwarenessEnabled ist wahr. Die Regel ist NON_COMPLIANT für eine OpenSearch Domain, wenn 'instanceCount' kleiner als 3 ist oder '' auf 'falsezoneAwarenessEnabled' gesetzt ist.

ID: OPENSEARCH_DATA_NODE_FAULT_TOLERANCE

Ressourcentypen: AWS::OpenSearch::Domain

Auslösertyp: Konfigurationsänderungen

AWS-Region: Alle unterstützten AWS Regionen außer China (Peking), Asien-Pazifik (Thailand), Naher Osten (VAE), Asien-Pazifik (Hyderabad), Asien-Pazifik (Malaysia), Asien-Pazifik (Melbourne),

AWS GovCloud (USA-Ost), AWS GovCloud (US-West), Mexiko (Zentral), Israel (Tel Aviv), Kanada West (Calgary), Europa (Spanien), China (Ningxia), Europa (Zürich)

Parameter:

Keine

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

opensearch-encrypted-at-rest

Prüft, ob für Amazon OpenSearch Service-Domains die Konfiguration „Verschlüsselung im Ruhezustand“ aktiviert ist. Die Regel ist NON_COMPLIANT, wenn das Feld „`EncryptionAtRestOptions`“ nicht aktiviert ist.

> **Note**
>
> Die Regel bewertet keine Elasticsearch-Domains.

ID: OPENSEARCH_ENCRYPTED_AT_REST

Ressourcentypen: AWS::OpenSearch::Domain

Auslösertyp: Konfigurationsänderungen

AWS-Region: Alle unterstützten AWS Regionen außer China (Peking), Asien-Pazifik (Thailand), Naher Osten (VAE), Asien-Pazifik (Hyderabad), Asien-Pazifik (Malaysia), Asien-Pazifik (Melbourne), AWS GovCloud (USA-Ost), AWS GovCloud (US-West), Mexiko (Zentral), Israel (Tel Aviv), Kanada West (Calgary), Europa (Spanien), China (Ningxia), Europa (Zürich)

Parameter:

Keine

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

opensearch-https-required

Überprüft, ob Verbindungen zu Domains HTTPS verwenden. OpenSearch Die Regel lautet NON_COMPLIANT, wenn die OpenSearch Amazon-Domain 'EnforceHTTPS' nicht 'true' oder 'true' ist und 'TLSSecurityPolicy' nicht in '' enthalten ist. `tlsPolicies`

ID: OPENSEARCH_HTTPS_REQUIRED

Ressourcentypen: AWS::OpenSearch::Domain

Auslösertyp: Konfigurationsänderungen

AWS-Region: Alle unterstützten AWS Regionen außer China (Peking), Asien-Pazifik (Thailand), Naher Osten (VAE), Asien-Pazifik (Hyderabad), Asien-Pazifik (Malaysia), Asien-Pazifik (Melbourne), AWS GovCloud (USA-Ost), AWS GovCloud (US-West), Mexiko (Zentral), Israel (Tel Aviv), Kanada West (Calgary), Europa (Spanien), China (Ningxia), Europa (Zürich)

Parameter:

tlsPolicies (optional), Typ: CSV

> Durch Kommas getrennte Liste von TLS-Sicherheitsrichtlinien, die mit der OpensSearch Amazon-Domain verglichen werden sollen.

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

opensearch-in-vpc-only

Prüft, ob sich Amazon OpenSearch Service-Domains in einer Amazon Virtual Private Cloud (VPC) befinden. Die Regel lautet NON_COMPLIANT, wenn ein OpenSearch Service-Domain-Endpunkt öffentlich ist.

> **Note**
>
> Die Regel bewertet keine Elasticsearch-Domains.

ID: OPENSEARCH_IN_VPC_ONLY

Ressourcentypen: AWS::OpenSearch::Domain

Auslösertyp: Konfigurationsänderungen

AWS-Region: Alle unterstützten AWS Regionen außer China (Peking), Asien-Pazifik (Thailand), Naher Osten (VAE), Asien-Pazifik (Hyderabad), Asien-Pazifik (Malaysia), Asien-Pazifik (Melbourne), AWS GovCloud (USA-Ost), AWS GovCloud (US-West), Mexiko (Zentral), Israel (Tel Aviv), Kanada West (Calgary), Europa (Spanien), China (Ningxia), Europa (Zürich)

Parameter:

Keine

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

opensearch-logs-to-cloudwatch

Prüft, ob Amazon OpenSearch Service-Domains so konfiguriert sind, dass sie Protokolle an Amazon CloudWatch Logs senden. Die Regel ist NON_COMPLIANT, wenn die Protokollierung nicht konfiguriert ist.

> **Note**
>
> Die Regel bewertet keine Elasticsearch-Domains.

ID: OPENSEARCH_LOGS_TO_CLOUDWATCH

Ressourcentypen: AWS::OpenSearch::Domain

Auslösertyp: Konfigurationsänderungen

AWS-Region: Alle unterstützten AWS Regionen außer China (Peking), Asien-Pazifik (Thailand), Naher Osten (VAE), Asien-Pazifik (Hyderabad), Asien-Pazifik (Malaysia), Asien-Pazifik (Melbourne), AWS GovCloud (USA-Ost), AWS GovCloud (US-West), Mexiko (Zentral), Israel (Tel Aviv), Kanada West (Calgary), Europa (Spanien), China (Ningxia), Europa (Zürich)

Parameter:

logTypes (optional), Typ: CSV

Durch Kommata getrennte Liste der Protokolle, die aktiviert sind. Zulässige Werte sind „Such“, „Index“ und „Fehler“.

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

opensearch-node-to-node-Verschlüsselungsprüfung

Prüfen Sie, ob Amazon OpenSearch Service-Knoten von Ende zu Ende verschlüsselt sind. Die Regel lautet NON_COMPLIANT, wenn die node-to-node Verschlüsselung auf der Domain nicht aktiviert ist

> **Note**
> Die Regel bewertet keine Elasticsearch-Domains.

ID: OPENSEARCH_NODE_TO_NODE_ENCRYPTION_CHECK

Ressourcentypen: AWS::OpenSearch::Domain

Auslösertyp: Konfigurationsänderungen

AWS-Region: Alle unterstützten AWS Regionen außer China (Peking), Asien-Pazifik (Thailand), Naher Osten (VAE), Asien-Pazifik (Hyderabad), Asien-Pazifik (Malaysia), Asien-Pazifik (Melbourne), AWS GovCloud (USA-Ost), AWS GovCloud (US-West), Mexiko (Zentral), Israel (Tel Aviv), Kanada West (Calgary), Europa (Spanien), China (Ningxia), Europa (Zürich)

Parameter:

Keine

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

opensearch-primary-node-fault-Toleranz

Prüft, ob Amazon OpenSearch Service-Domains mit mindestens drei dedizierten Primärknoten konfiguriert sind. Die Regel lautet NON_COMPLIANT für eine OpenSearch Service-Domain, wenn DedicatedMasterEnabled '' auf 'false' gesetzt ist oder 'DedicatedMasterCount' weniger als 3 ist.

Kennung: OPENSEARCH_PRIMARY_NODE_FAULT_TOLERANCE

Ressourcentypen: AWS::OpenSearch::Domain

Auslösertyp: Konfigurationsänderungen

AWS-Region: Alle unterstützten AWS Regionen außer China (Peking), Asien-Pazifik (Thailand), Naher Osten (VAE), Asien-Pazifik (Hyderabad), Asien-Pazifik (Malaysia), Asien-Pazifik (Melbourne), Mexiko (Zentral), Israel (Tel Aviv), Kanada West (Calgary), Europa (Spanien), China (Ningxia), Region Europa (Zürich)

Parameter:

Keine

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

opensearch-update-check

Prüft, ob Amazon OpenSearch Service-Versionsupdates verfügbar, aber nicht installiert sind. Die Regel lautet NON_COMPLIANT für eine OpenSearch Domain, wenn die neuesten Softwareupdates nicht installiert sind.

ID: OPENSEARCH_UPDATE_CHECK

Ressourcentypen: AWS::OpenSearch::Domain

Auslösertyp: Konfigurationsänderungen

AWS-Region: Alle unterstützten AWS Regionen außer Asien-Pazifik (Thailand), Naher Osten (VAE), Asien-Pazifik (Hyderabad), Asien-Pazifik (Malaysia), Asien-Pazifik (Melbourne), Mexiko (Zentral), Israel (Tel Aviv), Kanada West (Calgary), Europa (Spanien), Europa (Zürich)

Parameter:

Keine

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

rabbit-mq-supported-version

Prüft, ob ein Amazon MQ RabbitMQ-Broker auf einer bestimmten unterstützten Engine-Mindestversion läuft. Die Regel lautet NON_COMPLIANT, wenn der RabbitMQ-Broker nicht auf der von Ihnen angegebenen Mindestversion der unterstützten Engine läuft.

Kennung: RABBIT_MQ_SUPPORTED_VERSION

Ressourcentypen: AWS::AmazonMQ::Broker

Auslösertyp: Konfigurationsänderungen

AWS-Region: Alle unterstützten AWS Regionen außer Asien-Pazifik (Thailand), Asien-Pazifik (Hyderabad), Asien-Pazifik (Malaysia), Asien-Pazifik (Melbourne), Mexiko (Zentral), Israel (Tel Aviv), Kanada West (Calgary), Europa (Spanien), Europa (Zürich)

Parameter:

supportedEngineVersion, Typ: Zeichenfolge

> Zeichenkettenwert für die Regel zur Überprüfung der mindestens unterstützten Engine-Version für den RabbitMQ-Broker. RabbitMQ-Broker verwenden eine semantische Versionsspezifikation: X.Y.Z. X steht für die Hauptversion, Y für die Nebenversion und Z für die Patch-Version.

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

rds-aurora-mysql-audit-Protokollierung aktiviert

Prüft, ob Amazon Aurora MySQL-Compatible Edition-Cluster so konfiguriert sind, dass sie Audit-Logs in Amazon Logs veröffentlichen. CloudWatch Die Regel ist NON_COMPLIANT, wenn bei Clustern von Aurora MySQL-Compatible Edition die Veröffentlichung von Prüfprotokollen nicht aktiviert ist.

ID: RDS_AURORA_MYSQL_AUDIT_LOGGING_ENABLED

Ressourcentypen: AWS::RDS::DBCluster

Auslösertyp: Konfigurationsänderungen

AWS-Region: Alle unterstützten AWS Regionen außer China (Peking), Asien-Pazifik (Thailand), Asien-Pazifik (Malaysia), AWS GovCloud (USA-Ost), AWS GovCloud (US-West), Mexiko (Zentral), Kanada West (Calgary)

Parameter:

Keine

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

rds-aurora-postgresql-logs-zu-Cloud-Watch

Prüft, ob ein Amazon Aurora PostgreSQL-DB-Cluster für die Veröffentlichung von PostgreSQL-Protokollen in Amazon Logs konfiguriert ist. CloudWatch Diese Regel ist NON_COMPLIANT, wenn der DB-Cluster nicht für die Veröffentlichung von PostgreSQL-Protokollen in Amazon Logs konfiguriert ist. CloudWatch

Kennung: RDS_AURORA_POSTGRESQL_LOGS_TO_CLOUDWATCH

Ressourcentypen: AWS::RDS::DBCluster

Auslösertyp: Konfigurationsänderungen

AWS-Region: Alle unterstützten AWS Regionen außer China (Peking), Asien-Pazifik (Thailand), Asien-Pazifik (Hyderabad), Asien-Pazifik (Malaysia), Asien-Pazifik (Melbourne), Mexiko (Zentral), Israel (Tel Aviv), Kanada West (Calgary), Europa (Spanien)

Parameter:

Keine

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

rds-automatic-minor-version-upgrade-fähig

Prüft, ob für Datenbank-Instances von Amazon Relational Database Service (Amazon RDS) automatische Unterversion-Upgrades konfiguriert sind. Die Regel ist NON_COMPLIANT, wenn der Wert von 'Upgrade' falsch ist. autoMinorVersion

ID: RDS_AUTOMATIC_MINOR_VERSION_UPGRADE_ENABLED

Ressourcentypen: AWS::RDS::DBInstance

Auslösertyp: Konfigurationsänderungen

AWS-Region: Alle unterstützten AWS Regionen

Parameter:

Keine

Proaktive Auswertung

Anweisungen zur Ausführung dieser Regel im proaktiven Modus finden Sie unter Evaluieren Ihrer Ressourcen mithilfe von AWS Config Regeln. Damit diese Regel im proaktiven Modus COMPLIANT zurückgibt, muss das Ressourcenkonfigurationsschema für die StartResourceEvaluationAPI die folgenden Eingaben enthalten, die als Zeichenfolge kodiert sind:

```
"ResourceConfiguration":
...
{
    "AutoMinorVersionUpgrade": BOOLEAN*,
    "Engine": String*
}
...
```

* Weitere Informationen zu gültigen Werten für diese Eingaben finden Sie unter AutoMinorVersionUpgrade und Engine im AWS CloudFormation Benutzerhandbuch.

Weitere Informationen zur proaktiven Auswertung finden Sie unter Auswertungsmodus.

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

rds-cluster-auto-minor-version-upgrade-enable

Prüft, ob automatische Unterversion-Upgrades für Clusterbereitstellungen von Amazon RDS Multi-AZ aktiviert sind. Die Regel ist NON_COMPLIANT, wenn autoMinorVersion Upgrade auf False gesetzt ist.

ID: RDS_CLUSTER_AUTO_MINOR_VERSION_UPGRADE_ENABLE

Ressourcentypen: AWS::RDS::DBCluster

Auslösertyp: Konfigurationsänderungen

AWS-Region: Alle unterstützten AWS Regionen außer China (Peking), Asien-Pazifik (Thailand), Naher Osten (VAE), Asien-Pazifik (Hyderabad), Asien-Pazifik (Malaysia), Asien-Pazifik (Melbourne), AWS GovCloud (USA-Ost), AWS GovCloud (US-West), Mexiko (Zentral), USA West (Nordkalifornien), Israel (Tel Aviv), Kanada West (Calgary), Europa (Spanien), Europa (Zürich)

Parameter:

Keine

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

rds-cluster-default-admin-überprüfen

Prüft, ob ein Datenbankcluster von Amazon Relational Database Service (Amazon RDS) den Standardwert des Admin-Benutzernamens geändert hat. Die Regel ist NON_COMPLIANT, wenn der Admin-Benutzername auf den Standardwert festgelegt ist.

ID: RDS_CLUSTER_DEFAULT_ADMIN_CHECK

Ressourcentypen: AWS::RDS::DBCluster

Auslösertyp: Konfigurationsänderungen

AWS-Region: Alle unterstützten AWS Regionen außer China (Peking), Asien-Pazifik (Thailand), Asien-Pazifik (Malaysia), AWS GovCloud (USA-Ost), AWS GovCloud (US-West), Mexiko (Zentral), Kanada West (Calgary), China (Ningxia)

Parameter:

validAdminUserNamen (optional), Typ: CSV

> Durch Kommata getrennte Liste der Namen von Administrator-Benutzern, die Amazon-RDS-Cluster verwenden können. „Postgres“ oder „admin“ dürfen darin nicht als zulässige Benutzernamen enthalten sein, da es sich um Standardwerte handelt.

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

rds-cluster-deletion-protection-aktiviert

Prüft, ob für einen Cluster von Amazon Relational Database Service (Amazon RDS) der Löschschutz aktiviert ist. Die Regel ist NON_COMPLIANT, wenn für einen Amazon-RDS-Cluster kein Löschschutz aktiviert ist.

ID: RDS_CLUSTER_DELETION_PROTECTION_ENABLED

Ressourcentypen: AWS::RDS::DBCluster

Auslösertyp: Konfigurationsänderungen

AWS-Region: Alle unterstützten AWS Regionen außer der Region China (Peking)

Parameter:

Keine

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

rds-cluster-encrypted-at-ausruhen

Prüft, ob ein Cluster von Amazon Relational Database Service (Amazon RDS) im Ruhezustand verschlüsselt ist. Die Regel ist NON_COMPLIANT, wenn ein Amazon-RDS-Cluster im Ruhezustand nicht verschlüsselt ist.

ID: RDS_CLUSTER_ENCRYPTED_AT_REST

Ressourcentypen: AWS::RDS::DBCluster

Auslösertyp: Konfigurationsänderungen

AWS-Region: Alle unterstützten AWS Regionen außer China (Peking), Asien-Pazifik (Thailand), Asien-Pazifik (Malaysia), AWS GovCloud (USA-Ost), AWS GovCloud (US-West), Mexiko (Zentral), Kanada West (Calgary)

Parameter:

Keine

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

rds-cluster-iam-authentication-aktiviert

Prüft, ob für einen Amazon Relational Database Service (Amazon RDS) -Cluster die AWS Identity and Access Management (IAM) -Authentifizierung aktiviert ist. Die Regel ist NON_COMPLIANT, wenn für einen Amazon-RDS-Cluster die IAM-Authentifizierung nicht aktiviert ist.

ID: RDS_CLUSTER_IAM_AUTHENTICATION_ENABLED

Ressourcentypen: AWS::RDS::DBCluster

Auslösertyp: Konfigurationsänderungen

AWS-Region: Alle unterstützten AWS Regionen außer der Region China (Peking)

Parameter:

Keine

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

rds-cluster-multi-az-aktiviert

Prüft, ob die Multi-Availability Zone (Multi-AZ) -Replikation auf Amazon Aurora- und Multi-AZ-DB-Clustern aktiviert ist, die von Amazon Relational Database Service (Amazon RDS) verwaltet werden. Die Regel ist NON_COMPLIANT, wenn für eine Amazon-RDS-Instance keine Multi-AZ konfiguriert ist.

ID: RDS_CLUSTER_MULTI_AZ_ENABLED

Ressourcentypen: AWS::RDS::DBCluster

Auslösertyp: Konfigurationsänderungen

AWS-Region: Alle unterstützten AWS Regionen außer China (Peking) und Asien-Pazifik (Melbourne)

Parameter:

Keine

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

rds-db-security-group-nicht erlaubt

Prüft, ob es DB-Sicherheitsgruppen von Amazon Relational Database Service (Amazon RDS) gibt, die nicht die standardmäßige DB-Sicherheitsgruppe sind. Die Regel ist NON_COMPLIANT, wenn es DB-Sicherheitsgruppen gibt, die nicht die standardmäßige DB-Sicherheitsgruppe sind.

ID: RDS_DB_SECURITY_GROUP_NOT_ALLOWED

Ressourcentypen: AWS::RDS::DBSecurityGroup

Auslösertyp: Konfigurationsänderungen

AWS-Region: Nur verfügbar in Europa (Irland), Südamerika (São Paulo), USA Ost (Nord-Virginia), Asien-Pazifik (Tokio), USA West (Oregon), USA West (Nordkalifornien), Asien-Pazifik (Singapur) und Asien-Pazifik (Sydney)

Parameter:

Keine

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

rds-enhanced-monitoring-enabled

Prüft, ob die erweiterte Überwachung für Amazon-RDS-Instances aktiviert ist. Diese Regel ist NON_COMPLIANT, wenn `monitoringInterval` im Konfigurationselement der RDS-Instance „0“ ist oder wenn `monitoringInterval` nicht mit dem Regelparameterwert übereinstimmt.

Bezeichner: RDS_ENHANCED_MONITORING_ENABLED

Ressourcentypen: AWS::RDS::DBInstance

Auslösertyp: Konfigurationsänderungen

AWS-Region: Alle unterstützten AWS Regionen

Parameter:

monitoringInterval (optional), Typ: int

> Ein ganzzahliger Wert in Sekunden zwischen Punkten, wenn erweiterte Überwachungsmetriken für die Datenbank-Instance erfasst werden. Die gültigen Werte sind 1, 5, 10, 15, 30 und 60.

Proaktive Auswertung

Anweisungen zur Ausführung dieser Regel im proaktiven Modus finden Sie unter Evaluieren Ihrer Ressourcen mithilfe von AWS Config Regeln. Damit diese Regel im proaktiven Modus COMPLIANT zurückgibt, muss das Ressourcenkonfigurationsschema für die StartResourceEvaluationAPI die folgenden Eingaben enthalten, die als Zeichenfolge kodiert sind:

```
"ResourceConfiguration":
...
{
    "MonitoringInterval": Integer*,
    "Engine": String*
}
...
```

* Weitere Informationen zu gültigen Werten für diese Eingaben finden Sie unter MonitoringIntervalund Engine im AWS CloudFormation Benutzerhandbuch.

Weitere Informationen zur proaktiven Auswertung finden Sie unter Auswertungsmodus.

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

rds-instance-default-admin-überprüfen

Prüft, ob eine Datenbank von Amazon Relational Database Service (Amazon RDS) den Standardwert des Admin-Benutzernamens geändert hat. Diese Regel wird nur auf RDS-Datenbank-Instances ausgeführt. Die Regel ist NON_COMPLIANT, wenn der Admin-Benutzername auf den Standardwert festgelegt ist.

ID: RDS_INSTANCE_DEFAULT_ADMIN_CHECK

Ressourcentypen: AWS::RDS::DBInstance

Auslösertyp: Konfigurationsänderungen

AWS-Region: Alle unterstützten AWS Regionen außer China (Peking), Asien-Pazifik (Thailand), Asien-Pazifik (Malaysia), Mexiko (Zentral), Kanada West (Calgary), China (Ningxia)

Parameter:

validAdminUserNamen (optional), Typ: CSV

> Durch Kommata getrennte Liste der Namen von Administrator-Benutzern, die Amazon-RDS-Instances verwenden können. („Postgres“ oder „admin“ dürfen darin nicht als zulässige Benutzernamen enthalten sein, da es sich um Standardwerte handelt.)

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

rds-instance-deletion-protection-aktiviert

Prüft, ob für eine Instance von Amazon Relational Database Service (Amazon RDS) der Löschschutz aktiviert ist. Die Regel ist NON_COMPLIANT, wenn für eine Amazon-RDS-Instance kein Löschschutz aktiviert ist („DeletionProtection“ ist beispielsweise auf „False“ gesetzt).

> **Warning**
>
> Einige RDS-DB-Instances innerhalb eines Clusters (Aurora/DocumentDB) werden als nicht konform angezeigt.

ID: RDS_INSTANCE_DELETION_PROTECTION_ENABLED

Ressourcentypen: AWS::RDS::DBInstance

Auslösertyp: Konfigurationsänderungen

AWS-Region: Alle unterstützten AWS Regionen

Parameter:

databaseEngines (optional), Typ: CSV

Durch Kommata getrennte Liste der RDS-Datenbank-Engines, die in die Auswertung der Regel aufgenommen werden sollen. Zum Beispiel „mysql, postgres, mariadb“.

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

rds-instance-iam-authentication-aktiviert

Prüft, ob für eine Amazon Relational Database Service (Amazon RDS) -Instance die AWS Identity and Access Management (IAM) -Authentifizierung aktiviert ist. Die Regel ist NON_COMPLIANT, wenn für eine Amazon-RDS-Instance die IAM-Authentifizierung nicht aktiviert ist.

> **Note**
>
> Die DB-Engine sollte „mysql“, „postgres“, „aurora“, „aurora-mysql“ oder „aurora-postgresql“ lauten. Der DB-Instance-Status sollte entweder „available“, „backing-up“, „storage-optimization“ oder „storage-full“ lauten.

ID: RDS_INSTANCE_IAM_AUTHENTICATION_ENABLED

Ressourcentypen: AWS::RDS::DBInstance

Auslösertyp: Konfigurationsänderungen

AWS-Region: Alle unterstützten AWS Regionen

Parameter:

Keine

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

rds-instance-public-access-überprüfen

Prüft, ob Amazon Relational Database Service (Amazon RDS)-Instances nicht öffentlich zugänglich sind. Die Regel ist NON_COMPLIANT, wenn das Feld „Öffentlich zugänglich“ im Konfigurationselement der Instance auf „True“ gesetzt ist.

ID: RDS_INSTANCE_PUBLIC_ACCESS_CHECK

Ressourcentypen: AWS::RDS::DBInstance

Auslösertyp: Konfigurationsänderungen

AWS-Region: Alle unterstützten AWS Regionen

Parameter:

Keine

Proaktive Auswertung

Anweisungen zur Ausführung dieser Regel im proaktiven Modus finden Sie unter Evaluieren Ihrer Ressourcen mithilfe von AWS Config Regeln. Damit diese Regel im proaktiven Modus COMPLIANT zurückgibt, muss das Ressourcenkonfigurationsschema für die StartResourceEvaluationAPI die folgenden Eingaben enthalten, die als Zeichenfolge kodiert sind:

```
"ResourceConfiguration":
...
{
   "PubliclyAccessible": BOOLEAN
}
...
```

Weitere Informationen zur proaktiven Auswertung finden Sie unter Auswertungsmodus.

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

rds-instance-subnet-igw-überprüfen

Überprüft, ob RDS-DB-Instances in einem öffentlichen Subnetz mit einer Route zum Internet-Gateway bereitgestellt werden. Die Regel lautet NON_COMPLIANT, wenn RDS-DB-Instances in einem öffentlichen Subnetz bereitgestellt werden

Kennung: RDS_INSTANCE_SUBNET_IGW_CHECK

Ressourcentypen: AWS::RDS::DBInstance

Auslösertyp: Regelmäßig

AWS-Region: Alle unterstützten AWS Regionen außer Naher Osten (Bahrain), Asien-Pazifik (Thailand), Asien-Pazifik (Malaysia), Mexiko (Zentral) und Kanada West (Calgary)

Parameter:

Keine

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

rds-in-backup-plan

Prüft, ob Amazon Relational Database Service (Amazon RDS) -Datenbanken in AWS Backup-Plänen vorhanden sind. Die Regel lautet NON_COMPLIANT, wenn Amazon RDS-Datenbanken in keinem AWS Backup-Plan enthalten sind.

> **Note**
>
> Die Regel bezieht sich nur auf Amazon-Aurora-DB-Instances. DB-Cluster werden nicht unterstützt.

ID: RDS_IN_BACKUP_PLAN

Ressourcentypen: AWS::RDS::DBInstance

Auslösertyp: Regelmäßig

AWS-Region: Alle unterstützten AWS Regionen außer Asien-Pazifik (Taipeh) und Kanada West (Calgary)

Parameter:

Keine

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

rds-last-backup-recovery-Punkt-erstellt

Überprüft, ob für Amazon Relational Database Service (Amazon RDS) ein Wiederherstellungspunkt erstellt wurde. Die Regel ist NON_COMPLIANT, wenn innerhalb des angegebenen Zeitraums kein entsprechender Wiederherstellungspunkt für die Amazon-RDS-Instance erstellt wurde.

ID: RDS_LAST_BACKUP_RECOVERY_POINT_CREATED

Ressourcentypen: AWS::RDS::DBInstance

Auslösertyp: Regelmäßig

AWS-Region: Alle unterstützten AWS Regionen außer China (Peking), Asien-Pazifik (Thailand), Asien-Pazifik (Malaysia), Mexiko (Zentral), Israel (Tel Aviv), Kanada West (Calgary), China (Ningxia)

Parameter:

resourceTags (optional), Typ: Zeichenfolge

Tags von Amazon-RDS-Instances, die von der Regel geprüft werden sollen, im JSON-Format `{"tagkey" : "tagValue"}`.

resourceId (optional), Typ: Zeichenfolge

ID der Amazon-RDS-Instance; die von der Regel geprüft werden soll.

recoveryPointAgeWert (optional), Typ: int, Standard: 1

Numerischer Wert für das zulässige Höchstalter. Nicht mehr als 744 für Stunden oder 31 für Tage.

recoveryPointAgeEinheit (optional), Typ: Zeichenfolge, Standard: days

Zeiteinheit für das zulässige Höchstalter. Zulässige Werte: „Stunden“, „Tage“.

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

rds-logging-enabled

Prüft, ob die entsprechenden Protokolle von Amazon Relational Database Service (Amazon RDS) aktiviert sind. Die Regel ist NON_COMPLIANT, wenn nicht alle Protokolltypen aktiviert sind.

> **Note**
>
> DB-Instances, die sich nicht im Status „available“, „backing-up“, „storage-optimization“ oder „storage-full“ befinden, werden als `NOT_APPLICABLE` bewertet.

ID: RDS_LOGGING_ENABLED

Ressourcentypen: AWS::RDS::DBInstance

Auslösertyp: Konfigurationsänderungen

AWS-Region: Alle unterstützten AWS Regionen

Parameter:

additionalLogs (optional), Typ: StringMap

> Durch Kommata getrennte Liste der Engine- und Protokolltypnamen. Zum Beispiel „additionalLogs“: „oracle: general, slowquery ; aurora: alert, slowquery“

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

rds-mariadb-instance-encryptedim Transit

Überprüft, ob Verbindungen zu Amazon RDS for MariaDB MariaDB-DB-Instances mit einer Engine-Version größer oder gleich 10.5 Verschlüsselung bei der Übertragung verwenden. Die Regel lautet NON_COMPLIANT, wenn die DB-Parametergruppe nicht synchron ist oder wenn require_secure_transport nicht auf ON gesetzt ist.

Kennung: RDS_MARIADB_INSTANCE_ENCRYPTED_IN_TRANSIT

Ressourcentypen: AWS::RDS::DBInstance

Auslösertyp: Regelmäßig

AWS-Region: Alle unterstützten AWS Regionen außer Naher Osten (Bahrain), China (Peking), Asien-Pazifik (Thailand), Asien-Pazifik (Malaysia), Mexiko (Zentral), Kanada West (Calgary), China (Ningxia)

Parameter:

Keine

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

rds-meets-restore-time-ziel

Überprüft, ob die Wiederherstellungszeit von Amazon Relational Database Service (Amazon RDS)-Instances die angegebene Dauer einhält. Die Regel lautet NON_COMPLIANT, wenn LatestRestoreExecutionTimeMinutes die Anzahl einer Amazon RDS-Instance länger als maxRestoreTime Minuten ist.

Kennung: RDS_MEETS_RESTORE_TIME_TARGET

Ressourcentypen: AWS::RDS::DBInstance

Auslösertyp: Regelmäßig

AWS-Region: Alle unterstützten AWS Regionen außer China (Peking), Asien-Pazifik (Thailand), Asien-Pazifik (Malaysia), AWS GovCloud (USA-Ost), AWS GovCloud (US-West), Mexiko (Zentral), Israel (Tel Aviv), Kanada West (Calgary), China (Ningxia)

Parameter:

maxRestoreTime, Typ: int

Numerischer Wert für die maximal zulässige Wiederherstellungslaufzeit.

resourceTags (optional), Typ: Zeichenfolge

Tags von Amazon-RDS-Instances, die von der Regel geprüft werden sollen, im JSON-Format.

resourceId (optional), Typ: Zeichenfolge

ID der Amazon-RDS-Instance; die von der Regel geprüft werden soll.

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

rds-multi-az-support

Prüft, ob hohe Verfügbarkeit für Ihre RDS-DB-Instances aktiviert ist.

Bei einer Multi-AZ-Bereitstellung sorgt Amazon RDS für eine automatische Bereitstellung und Verwaltung eines synchronen Standby-Replikats in einer anderen Availability Zone. Weitere Informationen finden Sie unter Hohe Verfügbarkeit (Multi-AZ) im Amazon-RDS-Benutzerhandbuch.

> **Note**
>
> Diese Regel bewertet Instances von Amazon Aurora DB, Amazon DocumentDB und Amazon Neptune DB nicht.

ID: RDS_MULTI_AZ_SUPPORT

Ressourcentypen: AWS::RDS::DBInstance

Auslösertyp: Konfigurationsänderungen

AWS-Region: Alle unterstützten AWS Regionen

Parameter:

Keine

Proaktive Auswertung

Anweisungen zur Ausführung dieser Regel im proaktiven Modus finden Sie unter Evaluieren Ihrer Ressourcen mithilfe von AWS Config Regeln. Damit diese Regel im proaktiven Modus COMPLIANT zurückgibt, muss das Ressourcenkonfigurationsschema für die StartResourceEvaluationAPI die folgenden Eingaben enthalten, die als Zeichenfolge kodiert sind:

```
"ResourceConfiguration":
...
{
    "MultiAZ": BOOLEAN*,
    "Engine": String*
}
...
```

* Weitere Informationen zu gültigen Werten für diese Eingaben finden Sie unter MultiAZ und Engine im AWS CloudFormation Benutzerhandbuch.

Weitere Informationen zur proaktiven Auswertung finden Sie unter Auswertungsmodus.

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

rds-mysql-instance-encryptedim Transit

Prüft, ob Verbindungen zu Amazon RDS for MySQL MySQL-Datenbank-Instances so konfiguriert sind, dass sie Verschlüsselung bei der Übertragung verwenden. Die Regel lautet NON_COMPLIANT, wenn die zugehörige Datenbankparametergruppe nicht synchron ist oder wenn der Parameter require_secure_transport nicht auf 1 gesetzt ist.

> **Note**
>
> Die Regel gibt zurück`NOT_APPLICABLE`, wenn die Amazon RDS-Instance Teil eines RDS-Clusters ist.

Kennung: RDS_MYSQL_INSTANCE_ENCRYPTED_IN_TRANSIT

Ressourcentypen: AWS::RDS::DBInstance

Auslösertyp: Regelmäßig

AWS-Region: Alle unterstützten AWS Regionen außer Asien-Pazifik (Thailand), Asien-Pazifik (Malaysia), Mexiko (Zentral) und Kanada West (Calgary)

Parameter:

Keine

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

rds-postgresql-logs-to-Wolkenbeobachtung

Prüft, ob eine Amazon PostgreSQL-DB-Instance für die Veröffentlichung von Protokollen in Amazon CloudWatch Logs konfiguriert ist. Die Regel lautet NON_COMPLIANT, wenn die DB-Instance nicht für die Veröffentlichung von Protokollen in Amazon CloudWatch Logs konfiguriert ist.

Kennung: RDS_POSTGRESQL_LOGS_TO_CLOUDWATCH

Ressourcentypen: AWS::RDS::DBInstance

Auslösertyp: Konfigurationsänderungen

AWS-Region: Alle unterstützten AWS Regionen außer Asien-Pazifik (Thailand), Asien-Pazifik (Malaysia), Mexiko (Zentral) und Kanada West (Calgary)

Parameter:

logTypes (optional), Typ: CSV

> Durch Kommas getrennte Liste der Protokolltypen, die in Logs veröffentlicht werden sollen. CloudWatch Gültige Werte sind: 'postgresql', 'upgrade'. Der Standardwert ist 'postgresql'.

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

rds-postgres-instance-encryptedim Transit

Prüft, ob Verbindungen zu Amazon RDS PostgreSQL-Datenbank-Instances so konfiguriert sind, dass sie Verschlüsselung bei der Übertragung verwenden. Die Regel lautet NON_COMPLIANT, wenn die zugehörige Datenbankparametergruppe nicht synchron ist oder wenn der rds.force_ssl-Parameter nicht auf 1 gesetzt ist.

> **Note**
>
> Die Regel gibt zurück`NOT_APPLICABLE`, wenn die Amazon RDS-Instance Teil eines RDS-Clusters ist.

Kennung: RDS_POSTGRES_INSTANCE_ENCRYPTED_IN_TRANSIT

Ressourcentypen: AWS::RDS::DBInstance

Auslösertyp: Regelmäßig

AWS-Region: Alle unterstützten AWS Regionen außer Asien-Pazifik (Thailand), Asien-Pazifik (Malaysia), Mexiko (Zentral) und Kanada West (Calgary)

Parameter:

Keine

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

rds-proxy-tls-encryption

Überprüft, ob Amazon RDS-Proxys TLS für alle Verbindungen erzwingen. Die Regel lautet NON_COMPLIANT, wenn bei einem Amazon RDS-Proxy TLS nicht für alle Verbindungen durchgesetzt wird.

Kennung: RDS_PROXY_TLS_ENCRYPTION

Ressourcentypen: AWS::RDS::DBProxy

Auslösertyp: Regelmäßig

AWS-Region: Alle unterstützten AWS Regionen außer Naher Osten (Bahrain), China (Peking), Asien-Pazifik (Thailand), Asien-Pazifik (Malaysia), AWS GovCloud (USA-Ost), AWS GovCloud (US-West), Mexiko (Zentral), Kanada West (Calgary), China (Ningxia)

Parameter:

Keine

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

rds-resources-protected-by-Backup-Plan

Prüft, ob Instances von Amazon Relational Database Service (Amazon RDS) durch einen Backup-Plan geschützt sind. Die Regel ist NON_COMPLIANT, wenn die Instance der Amazon-RDS-Datenbank nicht durch einen Backup-Plan gedeckt ist.

ID: RDS_RESOURCES_PROTECTED_BY_BACKUP_PLAN

Ressourcentypen: AWS::RDS::DBInstance

Auslösertyp: Regelmäßig

AWS-Region: Alle unterstützten AWS Regionen außer China (Peking), Asien-Pazifik (Thailand), Asien-Pazifik (Malaysia), Mexiko (Zentral), Israel (Tel Aviv), Kanada West (Calgary), China (Ningxia)

Parameter:

resourceTags (optional), Typ: Zeichenfolge

Tags für Amazon-RDS-Instances, die von der Regel geprüft werden sollen, im JSON-Format `{"tagkey" : "tagValue"}`.

resourceId (optional), Typ: Zeichenfolge

ID der Amazon-RDS-Instance; die von der Regel geprüft werden soll.

crossRegionList (Fakultativ), Typ: Zeichenfolge

Durch Kommata getrennte Liste der Zielregionen, für die die regionsübergreifende Backup-Kopie aufbewahrt werden soll.

crossAccountList (Fakultativ), Typ: Zeichenfolge

Durch Kommata getrennte Liste der Zielkonten, für die die kontoübergreifende Backup-Kopie aufbewahrt werden soll.

maxRetentionDays (Fakultativ), Typ: int

Die maximale Aufbewahrungsdauer in Tagen für die Backup-Tresorsperre.

minRetentionDays (Fakultativ), Typ: int

Die Mindestaufbewahrungsdauer in Tagen für die Backup-Tresorsperre.

backupVaultLockÜberprüfen Sie (fakultativ), Typ: Zeichenfolge

Akzeptierte Werte: „True“ oder „False“. Geben Sie „True“ ein, damit die Regel prüft, ob die Ressource in einem gesperrten Tresor gesichert ist.

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

rds-snapshots-public-prohibited

Prüft, ob Snapshots von Amazon Relational Database Service (Amazon RDS) öffentlich sind. Die Regel ist NON_COMPLIANT, wenn alle bestehenden und neuen Amazon-RDS-Snapshots öffentlich zugänglich sind.

> **Note**
>
> Es kann bis zu 12 Stunden dauern, bis die Compliance-Ergebnisse erfasst werden.

ID: RDS_SNAPSHOTS_PUBLIC_PROHIBITED

Ressourcentypen: AWS::RDS::DBSnapshot, AWS::RDS::DBClusterSnapshot

Auslösertyp: Konfigurationsänderungen

AWS-Region: Alle unterstützten AWS Regionen außer Afrika (Kapstadt), Asien-Pazifik (Melbourne), Europa (Mailand), Israel (Tel Aviv), Europa (Spanien), Europa (Zürich)

Parameter:

Keine

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

rds-snapshot-encrypted

Prüft, ob DB-Snapshots von Amazon Relational Database Service (Amazon RDS) verschlüsselt sind. Die Regel ist NON_COMPLIANT, wenn die Snapshots der Amazon-RDS-Datenbank nicht verschlüsselt sind.

Kennung: RDS_SNAPSHOT_ENCRYPTED

Ressourcentypen: AWS::RDS::DBSnapshot, AWS::RDS::DBClusterSnapshot

Auslösertyp: Konfigurationsänderungen

AWS-Region: Alle unterstützten AWS Regionen

Parameter:

Keine

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

rds-sqlserver-encrypted-in-Transit

Prüft, ob Verbindungen zu Amazon RDS-SQL-Server-Datenbank-Instances so konfiguriert sind, dass sie Verschlüsselung bei der Übertragung verwenden. Die Regel lautet NON_COMPLIANT, wenn der DB-Parameter force_ssl für die Parametergruppe nicht auf 1 gesetzt ist oder der ApplyStatus Parameter nicht „synchron“ ist.

Kennung: RDS_SQLSERVER_ENCRYPTED_IN_TRANSIT

Ressourcentypen: AWS::RDS::DBInstance

Auslösertyp: Regelmäßig

AWS-Region: Alle unterstützten AWS Regionen außer Naher Osten (Bahrain), Asien-Pazifik (Thailand), Asien-Pazifik (Malaysia), Mexiko (Zentral) und Kanada West (Calgary)

Parameter:

Keine

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

rds-sql-server-logs-zu-Cloud-Watch

Prüft, ob eine Amazon SQL Server-DB-Instance für die Veröffentlichung von Protokollen in Amazon CloudWatch Logs konfiguriert ist. Diese Regel ist NON_COMPLIANT, wenn die DB-Instance nicht für die Veröffentlichung von Protokollen in Amazon CloudWatch Logs konfiguriert ist.

Kennung: RDS_SQL_SERVER_LOGS_TO_CLOUDWATCH

Ressourcentypen: AWS::RDS::DBInstance

Auslösertyp: Konfigurationsänderungen

AWS-Region: Alle unterstützten AWS Regionen außer Asien-Pazifik (Thailand), Asien-Pazifik (Malaysia), Mexiko (Zentral) und Kanada West (Calgary)

Parameter:

logTypes (optional), Typ: CSV

> LogTypes — (Optional): Durch Kommas getrennte Liste von Protokolltypen, die in Logs veröffentlicht werden sollen. CloudWatch Gültige Werte sind: 'error', 'agent'. Der Standardwert ist 'error', 'agent'.

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

rds-storage-encrypted

Prüft, ob die Speicherverschlüsselung für die DB-Instances von Amazon Relational Database Service (Amazon RDS) aktiviert ist. Die Regel ist NON_COMPLIANT, wenn die Speicherverschlüsselung nicht aktiviert ist.

ID: RDS_STORAGE_ENCRYPTED

Ressourcentypen: AWS::RDS::DBInstance

Auslösertyp: Konfigurationsänderungen

AWS-Region: Alle unterstützten AWS Regionen

Parameter:

kmsKeyId (Fakultativ), Typ: Zeichenfolge

> KMS-Schlüssel-ID oder Amazon-Ressourcenname (ARN) zur Verschlüsselung des Speichers.

Proaktive Auswertung

Anweisungen zur Ausführung dieser Regel im proaktiven Modus finden Sie unter Evaluieren Ihrer Ressourcen mithilfe von AWS Config Regeln. Damit diese Regel im proaktiven Modus COMPLIANT zurückgibt, muss das Ressourcenkonfigurationsschema für die StartResourceEvaluationAPI die folgenden Eingaben enthalten, die als Zeichenfolge kodiert sind:

```
"ResourceConfiguration":
...
{
   "StorageEncrypted": BOOLEAN
}
...
```

Weitere Informationen zur proaktiven Auswertung finden Sie unter Auswertungsmodus.

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

redshift-audit-logging-enabled

Prüft, ob Amazon-Redshift-Cluster Prüfungen in einem bestimmten Bucket protokollieren. Die Regel ist NON_COMPLIANT, wenn die Prüfungsprotokollierung für einen Redshift-Cluster nicht aktiviert ist oder der Parameter `bucketNames` angegeben ist, aber das Ziel der Prüfungsprotokollierung nicht übereinstimmt.

ID: REDSHIFT_AUDIT_LOGGING_ENABLED

Ressourcentypen: AWS::Redshift::Cluster

Auslösertyp: Konfigurationsänderungen

AWS-Region: Alle unterstützten AWS Regionen außer China (Peking), Asien-Pazifik (Thailand), Asien-Pazifik (Jakarta), Naher Osten (VAE), Asien-Pazifik (Hyderabad), Asien-Pazifik (Malaysia), Asien-Pazifik (Melbourne), AWS GovCloud (US-Ost), AWS GovCloud (US-West), Mexiko (Zentral), Israel (Tel Aviv), Kanada West (Calgary), Europa (Spanien), China (Ningxia), Europa (Zürich)

Parameter:

bucketNames (optional), Typ: CSV

Durch Kommata getrennte Liste der Namen von Amazon-S3-Buckets zum Speichern von Prüfungsprotokollen.

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

redshift-backup-enabled

Prüft, ob automatisierte Amazon-Redshift-Snapshots für Cluster aktiviert sind. Die Regel ist NON_COMPLIANT, wenn der Wert für `automatedSnapshotRetentionPeriod` größer als `MaxRetentionPeriod`, kleiner als `MinRetentionPeriod` oder gleich 0 ist.

ID: REDSHIFT_BACKUP_ENABLED

Ressourcentypen: AWS::Redshift::Cluster

Auslösertyp: Konfigurationsänderungen

AWS-Region: Alle unterstützten AWS Regionen außer Asien-Pazifik (Thailand), Asien-Pazifik (Malaysia), Mexiko (Zentral), Israel (Tel Aviv), Asien-Pazifik (Taipeh) und Kanada West (Calgary)

Parameter:

MinRetentionPeriod (Fakultativ), Typ: int

Mindestwert für den Aufbewahrungszeitraum. Der Mindestwert ist 1.

MaxRetentionPeriod (Fakultativ), Typ: int

Höchstwert für den Aufbewahrungszeitraum. Der Höchstwert ist 35.

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

redshift-cluster-configuration-check

Prüft, ob die Amazon-Redshift-Cluster über die angegebenen Einstellungen verfügen. Die Regel ist NON_COMPLIANT, wenn der Amazon-Redshift-Cluster nicht oder mit einem anderen Schlüssel verschlüsselt ist oder für einen Cluster die Prüfungsprotokollierung nicht aktiviert ist.

ID: REDSHIFT_CLUSTER_CONFIGURATION_CHECK

Ressourcentypen: AWS::Redshift::Cluster

Auslösertyp: Konfigurationsänderungen

AWS-Region: Alle unterstützten AWS Regionen außer Asien-Pazifik (Thailand), Naher Osten (VAE), Asien-Pazifik (Hyderabad), Asien-Pazifik (Malaysia), Mexiko (Zentral), Asien-Pazifik (Taipeh), Kanada West (Calgary), Europa (Spanien)

Parameter:

clusterDbEncrypted, Typ: Boolesch, Standard: true

Datenbankverschlüsselung ist aktiviert.

loggingEnabled, Typ: Boolesch, Standard: true

Audit-Protokollierung ist aktiviert.

nodeTypes (optional), Typ: CSV, Standard: dc1.large

Knotentyp angeben.

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

redshift-cluster-kms-enabled

Prüft, ob Amazon Redshift Redshift-Cluster einen angegebenen AWS Key Management Service (AWS KMS) Schlüssel für die Verschlüsselung verwenden. Die Regel ist COMPLIANT, wenn die Verschlüsselung aktiviert ist und der Cluster mit dem im Parameter `kmsKeyArn` angegebenen Schlüssel verschlüsselt ist. Die Regel ist NON_COMPLIANT, wenn der Cluster nicht oder mit einem anderen Schlüssel verschlüsselt ist.

ID: REDSHIFT_CLUSTER_KMS_ENABLED

Ressourcentypen: AWS::Redshift::Cluster

Auslösertyp: Konfigurationsänderungen

AWS-Region: Alle unterstützten AWS Regionen außer Asien-Pazifik (Thailand), Mexiko (Zentral) und Asien-Pazifik (Taipeh)

Parameter:

kmsKeyArns (Fakultativ), Typ: CSV

Durch Kommas getrennte Liste der AWS KMS wichtigsten Amazon-Ressourcennamen (ARNs), die in Amazon Redshift-Clustern zur Verschlüsselung verwendet werden.

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

redshift-cluster-maintenancesettings-check

Prüft, ob die Amazon-Redshift-Cluster über die angegebenen Wartungseinstellungen verfügen. Die Regel ist NON_COMPLIANT, wenn automatische Upgrades auf die Hauptversion deaktiviert sind.

ID: REDSHIFT_CLUSTER_MAINTENANCESETTINGS_CHECK

Ressourcentypen: AWS::Redshift::Cluster

Auslösertyp: Konfigurationsänderungen

AWS-Region: Alle unterstützten AWS Regionen außer Asien-Pazifik (Thailand), Mexiko (Zentral) und Asien-Pazifik (Taipeh)

Parameter:

allowVersionUpgrade, Typ: Boolesch, Standard: true

Erlaubnis für Versions-Upgrades ist aktiviert.

preferredMaintenanceWindow (Fakultativ), Typ: Zeichenfolge

Das geplante Wartungsfenster für Cluster (z. B. Mo: 09:30 Uhr bis Mo: 10:00 Uhr).

automatedSnapshotRetentionZeitraum (fakultativ), Typ: int, Standard: 1

Anzahl der Tage für die Aufbewahrung automatischer Snapshots.

Proaktive Auswertung

Anweisungen zur Ausführung dieser Regel im proaktiven Modus finden Sie unter Evaluieren Ihrer Ressourcen mithilfe von AWS Config Regeln. Damit diese Regel im proaktiven Modus COMPLIANT zurückgibt, muss das Ressourcenkonfigurationsschema für die StartResourceEvaluationAPI die folgenden Eingaben enthalten, die als Zeichenfolge kodiert sind:

```
"ResourceConfiguration":
...
{
    "AutomatedSnapshotRetentionPeriod": Integer*,
    "PreferredMaintenanceWindow": String*,
    "AllowVersionUpgrade": BOOLEAN*
}
...
```

* Weitere Informationen zu gültigen Werten für diese Eingaben finden Sie unter AutomatedSnapshotRetentionPeriodPreferredMaintenanceWindow, und AllowVersionUpgradeim AWS CloudFormation Benutzerhandbuch.

Weitere Informationen zur proaktiven Auswertung finden Sie unter Auswertungsmodus.

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

redshift-cluster-multi-az-aktiviert

Prüft, ob für einen Amazon Redshift Redshift-Cluster mehrere Availability Zones-Bereitstellungen aktiviert sind. Diese Regel ist NON_COMPLIANT, wenn für den Amazon Redshift Redshift-Cluster nicht mehrere Availability Zones-Bereitstellungen aktiviert sind.

Kennung: REDSHIFT_CLUSTER_MULTI_AZ_ENABLED

Ressourcentypen: AWS::Redshift::Cluster

Auslösertyp: Konfigurationsänderungen

AWS-Region: Alle unterstützten AWS Regionen außer Asien-Pazifik (Thailand), Naher Osten (VAE), Asien-Pazifik (Hyderabad), Asien-Pazifik (Seoul), Asien-Pazifik (Malaysia), Mexiko (Zentral), USA West (Nordkalifornien), Israel (Tel Aviv), Kanada West (Calgary), Europa (Spanien), Europa (Zürich)

Parameter:

Keine

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

redshift-cluster-parameter-group-markiert

Prüft, ob Amazon Redshift Redshift-Cluster-Parametergruppen Tags haben. Optional können Sie Tag-Schlüssel angeben. Die Regel lautet NON_COMPLIANT, wenn keine Tags vorhanden sind oder wenn die angegebenen Tag-Schlüssel nicht vorhanden sind. Die Regel sucht nicht nach Tags, die mit 'aws: 'beginnen.

Kennung: REDSHIFT_CLUSTER_PARAMETER_GROUP_TAGGED

Ressourcentypen: AWS::Redshift::ClusterParameterGroup

Auslösertyp: Konfigurationsänderungen

AWS-Region: Alle unterstützten AWS Regionen außer China (Peking), Asien-Pazifik (Thailand), Asien-Pazifik (Malaysia), AWS GovCloud (USA-Ost), AWS GovCloud (US-West), Mexiko (Zentral), China (Ningxia)

Parameter:

requiredKeyTags (Fakultativ), Typ: CSV

Durch Kommas getrennte Liste von Tag-Schlüsseln, die von der Regel überprüft werden sollen. Falls angegeben, lautet die Regel NON_COMPLIANT, wenn die ausgewertete Ressource diese

Schlüssel nicht enthält. Bei Tag-Schlüsseln wird die Groß- und Kleinschreibung beachtet. Tag-Schlüssel, die mit „aws:“ beginnen, sind nicht erlaubt.

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

redshift-cluster-public-access-überprüfen

Prüft, ob Amazon-Redshift-Cluster nicht öffentlich zugänglich sind. Die Regel ist NON_COMPLIANT, wenn das Feld „Öffentlich zugänglich“ im Konfigurationselement des Clusters auf „True“ gesetzt ist.

ID: REDSHIFT_CLUSTER_PUBLIC_ACCESS_CHECK

Ressourcentypen: AWS::Redshift::Cluster

Auslösertyp: Konfigurationsänderungen

AWS-Region: Alle unterstützten AWS Regionen außer Asien-Pazifik (Thailand), Mexiko (Zentral) und Asien-Pazifik (Taipeh)

Parameter:

Keine

Proaktive Auswertung

Anweisungen zur Ausführung dieser Regel im proaktiven Modus finden Sie unter Evaluieren Ihrer Ressourcen mithilfe von AWS Config Regeln. Damit diese Regel im proaktiven Modus COMPLIANT zurückgibt, muss das Ressourcenkonfigurationsschema für die StartResourceEvaluationAPI die folgenden Eingaben enthalten, die als Zeichenfolge kodiert sind:

```
"ResourceConfiguration":
...
{
   "PubliclyAccessible": BOOLEAN
}
...
```

Weitere Informationen zur proaktiven Auswertung finden Sie unter Auswertungsmodus.

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

redshift-cluster-subnet-group-Multi-AZ

Prüft, ob Amazon Redshift Redshift-Subnetzgruppen Subnetze aus mehr als einer Availability Zone enthalten. Die Regel lautet NON_COMPLIANT, wenn eine Amazon Redshift Redshift-Subnetzgruppe keine Subnetze aus mindestens zwei verschiedenen Availability Zones enthält.

Kennung: REDSHIFT_CLUSTER_SUBNET_GROUP_MULTI_AZ

Ressourcentypen: AWS::Redshift::ClusterSubnetGroup

Auslösertyp: Konfigurationsänderungen

AWS-Region: Alle unterstützten AWS Regionen außer Asien-Pazifik (Thailand), Asien-Pazifik (Malaysia), Mexiko (Zentral) und Kanada West (Calgary)

Parameter:

Keine

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

redshift-default-admin-check

Prüft, ob ein Amazon-Redshift-Cluster den Standardwert des Benutzernamens des Administrators geändert hat. Die Regel ist NON_COMPLIANT, wenn der Benutzername des Administrators für einen Redshift-Cluster auf „awsuser“ festgelegt ist oder der Benutzername nicht mit dem Inhalt des Parameters übereinstimmt.

ID: REDSHIFT_DEFAULT_ADMIN_CHECK

Ressourcentypen: AWS::Redshift::Cluster

Auslösertyp: Konfigurationsänderungen

AWS-Region: Alle unterstützten AWS Regionen außer Asien-Pazifik (Thailand), Asien-Pazifik (Malaysia), Mexiko (Zentral), Israel (Tel Aviv) und Kanada West (Calgary)

Parameter:

validAdminUserNamen (optional), Typ: CSV

Durch Kommata getrennte Liste der Benutzernamen von Administratoren, die von Redshift-Clustern verwendet werden sollen. Hinweis: „awsuser“ ist die Standardeinstellung und wird nicht akzeptiert.

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

redshift-default-db-name-überprüfen

Prüft, ob ein Redshift-Cluster den Standardwert seines Datenbanknamens geändert hat. Die Regel ist NON_COMPLIANT, wenn der Datenbankname für einen Redshift-Cluster auf „dev“ festgelegt oder der optionale Parameter angegeben ist und der Datenbankname nicht mit ihm übereinstimmt.

ID: REDSHIFT_DEFAULT_DB_NAME_CHECK

Ressourcentypen: AWS::Redshift::Cluster

Auslösertyp: Konfigurationsänderungen

AWS-Region: Alle unterstützten AWS Regionen außer Asien-Pazifik (Thailand), Asien-Pazifik (Malaysia), AWS GovCloud (USA-Ost), AWS GovCloud (US-West), Mexiko (Zentral), Israel (Tel Aviv), Kanada West (Calgary)

Parameter:

validDatabaseNames (Fakultativ), Typ: CSV

Durch Kommata getrennte Liste von Datenbanknamen für Redshift-Cluster.

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

redshift-enhanced-vpc-routing-aktiviert

Prüft, ob der Amazon Redshift Redshift-Cluster 'enhancedVpcRouting' aktiviert ist. Die Regel ist NON_COMPLIANT, wenn 'enhancedVpcRouting' nicht aktiviert ist oder wenn die Konfiguration nicht aktiviert ist. enhancedVpcRouting Feld ist 'falsch'.

ID: REDSHIFT_ENHANCED_VPC_ROUTING_ENABLED

Ressourcentypen: AWS::Redshift::Cluster

Auslösertyp: Konfigurationsänderungen

AWS-Region: Alle unterstützten AWS Regionen außer Asien-Pazifik (Thailand), Mexiko (Zentral) und Asien-Pazifik (Taipeh)

Parameter:

Keine

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

redshift-require-tls-ssl

Prüft, ob Amazon Redshift Redshift-Cluster für die Verbindung mit SQL-Clients TLS/SSL verschlüsselt werden müssen. Die Regel ist NON_COMPLIANT, wenn für einen Amazon-Redshift-Cluster der Parameter „require_SSL“ nicht auf „True“ festgelegt ist.

ID: REDSHIFT_REQUIRE_TLS_SSL

Ressourcentypen: AWS::Redshift::Cluster, AWS::Redshift::ClusterParameterGroup

Auslösertyp: Konfigurationsänderungen

AWS-Region: Alle unterstützten AWS Regionen außer Asien-Pazifik (Thailand), Mexiko (Zentral) und Asien-Pazifik (Taipeh)

Parameter:

Keine

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

redshift-serverless-default-admin-überprüfen

Prüft, ob ein Amazon Redshift Serverless Namespace den Standardwert des Admin-Benutzernamens geändert hat. Die Regel lautet NON_COMPLIANT, wenn der Admin-Benutzername für einen Redshift Serverless Namespace auf „admin“ gesetzt ist.

Kennung: REDSHIFT_SERVERLESS_DEFAULT_ADMIN_CHECK

Ressourcentypen: AWS::RedshiftServerless::Namespace

Auslösertyp: Regelmäßig

AWS-Region: Alle unterstützten AWS Regionen außer Naher Osten (Bahrain), Asien-Pazifik (Thailand), Afrika (Kapstadt), Asien-Pazifik (Hyderabad), Asien-Pazifik (Osaka), Asien-Pazifik (Malaysia), Asien-Pazifik (Melbourne), Europa (Mailand), Mexiko (Zentral), Kanada West (Calgary)

Parameter:

Keine

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

redshift-serverless-default-db-Namenscheck

Prüft, ob ein Amazon Redshift Serverless-Namespace seinen Datenbanknamen gegenüber dem Standardwert geändert hat. Die Regel lautet NON_COMPLIANT, wenn der Datenbankname für einen Amazon Redshift Serverless Namespace auf `dev` gesetzt ist.

Kennung: REDSHIFT_SERVERLESS_DEFAULT_DB_NAME_CHECK

Ressourcentypen: AWS::RedshiftServerless::Namespace

Auslösertyp: Regelmäßig

AWS-Region: Alle unterstützten AWS Regionen außer Naher Osten (Bahrain), Asien-Pazifik (Thailand), Afrika (Kapstadt), Asien-Pazifik (Hyderabad), Asien-Pazifik (Osaka), Asien-Pazifik (Malaysia), Asien-Pazifik (Melbourne), Europa (Mailand), Mexiko (Zentral), Kanada West (Calgary)

Parameter:

Keine

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

redshift-serverless-namespace-cmk-Verschlüsselung

Überprüft, ob Amazon Redshift Serverless-Namespaces durch vom Kunden verwaltete KMS-Schlüssel verschlüsselt sind. AWS Die Regel lautet NON_COMPLIANT, wenn ein Namespace nicht durch einen vom Kunden verwalteten Schlüssel verschlüsselt ist. Optional können Sie eine Liste von KMS-Schlüsseln angeben, die von der Regel überprüft werden sollen.

Kennung: REDSHIFT_SERVERLESS_NAMESPACE_CMK_ENCRYPTION

Ressourcentypen: AWS::RedshiftServerless::Namespace

Auslösertyp: Regelmäßig

AWS-Region: Alle unterstützten AWS Regionen außer Naher Osten (Bahrain), Asien-Pazifik (Thailand), Afrika (Kapstadt), Asien-Pazifik (Hyderabad), Asien-Pazifik (Osaka), Asien-Pazifik (Malaysia), Asien-Pazifik (Melbourne), Europa (Mailand), Mexiko (Zentral), Kanada West (Calgary)

Parameter:

kmsKeyArns (Fakultativ), Typ: CSV

> Durch Kommas getrennte Liste der Amazon-Ressourcennamen (ARNs) der vom Kunden verwalteten Schlüssel, die von der Regel überprüft werden sollen. Falls angegeben, lautet die Regel NON_COMPLIANT, wenn ein Amazon Redshift Serverless-Namespace nicht mit einem dieser KMS-Schlüssel verschlüsselt ist.

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

redshift-serverless-publish-logs-to-cloudwatch

Prüft, ob Amazon Redshift Serverless Namespace so konfiguriert ist, dass die folgenden Protokolle in Amazon Logs veröffentlicht werden. CloudWatch Diese Regel ist NON_COMPLIANT, wenn der Namespace nicht so konfiguriert ist, dass er die folgenden Protokolle in Amazon Logs veröffentlicht. CloudWatch

Kennung: REDSHIFT_SERVERLESS_PUBLISH_LOGS_TO_CLOUDWATCH

Ressourcentypen: AWS::RedshiftServerless::Namespace

Auslösertyp: Regelmäßig

AWS-Region: Alle unterstützten AWS Regionen außer Naher Osten (Bahrain), Asien-Pazifik (Thailand), Afrika (Kapstadt), Asien-Pazifik (Hyderabad), Asien-Pazifik (Osaka), Asien-Pazifik (Malaysia), Asien-Pazifik (Melbourne), Europa (Mailand), AWS GovCloud (USA-Ost), AWS GovCloud (US-West), Mexiko (Zentral), Kanada West (Calgary)

Parameter:

logType (optional), Typ: CSV

> Durch Kommas getrennte Liste der Protokolltypen, die in Logs veröffentlicht werden sollen. CloudWatch Gültige Werte sind 'connectionlog', 'userlog'. Der Standardwert ist 'connectionlog', 'userlog'.

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

redshift-serverless-workgroup-encryptedim Transit

Überprüft, ob bei AWS Redshift Serverless-Arbeitsgruppen der Konfigurationsparameter require_ssl auf true gesetzt ist. Die Regel lautet NON_COMPLIANT, wenn require_ssl auf false gesetzt ist.

Kennung: REDSHIFT_SERVERLESS_WORKGROUP_ENCRYPTED_IN_TRANSIT

Ressourcentypen: AWS::RedshiftServerless::Workgroup

Auslösertyp: Regelmäßig

AWS-Region: Nur verfügbar in Europa (Stockholm), Asien-Pazifik (Mumbai), Europa (Paris), USA Ost (Ohio), Europa (Irland), Europa (Frankfurt), USA Ost (Nord-Virginia), Asien-Pazifik (Seoul), Europa (London), Asien-Pazifik (Tokio), USA West (Oregon), USA West (Nordkalifornien), Asien-Pazifik (Singapur), Asien-Pazifik (Sydney), Kanada (Zentral), Europa (Spanien), Region Europa (Zürich)

Parameter:

Keine

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

redshift-serverless-workgroup-no-öffentlich zugänglich

Prüft, ob Amazon Redshift Serverless-Arbeitsgruppen keinen öffentlichen Zugriff zulassen. Die Regel lautet NON_COMPLIANT, wenn für eine Arbeitsgruppe die Option „Public Accessible aktivieren“ aktiviert ist.

Kennung: REDSHIFT_SERVERLESS_WORKGROUP_NO_PUBLIC_ACCESS

Ressourcentypen: AWS::RedshiftServerless::Workgroup

Auslösertyp: Regelmäßig

AWS-Region: Alle unterstützten AWS Regionen außer Naher Osten (Bahrain), China (Peking), Asien-Pazifik (Thailand), Afrika (Kapstadt), Asien-Pazifik (Hyderabad), Asien-Pazifik (Osaka), Asien-Pazifik (Malaysia), Asien-Pazifik (Melbourne), Europa (Mailand), AWS GovCloud (USA-Ost), AWS GovCloud (US-West), Mexiko (Zentral), Kanada West (Calgary), China (Ningxia)

Parameter:

Keine

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

redshift-serverless-workgroup-routes-innerhalb von VPC

Prüft, ob Amazon Redshift Serverless-Arbeitsgruppen den Netzwerkverkehr über eine VPC weiterleiten. Die Regel lautet NON_COMPLIANT, wenn für Arbeitsgruppen „Erweitertes VPC-Routing aktivieren“ deaktiviert ist.

Kennung: REDSHIFT_SERVERLESS_WORKGROUP_ROUTES_WITHIN_VPC

Ressourcentypen: AWS::RedshiftServerless::Workgroup

Auslösertyp: Regelmäßig

AWS-Region: Nur verfügbar in Europa (Stockholm), Asien-Pazifik (Mumbai), Europa (Paris), USA Ost (Ohio), Europa (Irland), Europa (Frankfurt), USA Ost (Nord-Virginia), Asien-Pazifik (Seoul), Europa (London), Asien-Pazifik (Tokio), USA West (Oregon), USA West (Nordkalifornien), Asien-Pazifik (Singapur), Asien-Pazifik (Sydney), Kanada (Zentral), Europa (Spanien), Region Europa (Zürich)

Parameter:

Keine

AWS CloudFormation Schablone

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

redshift-unrestricted-port-access

Überprüft, ob Sicherheitsgruppen, die einem Amazon Redshift Redshift-Cluster zugeordnet sind, Regeln für eingehenden Datenverkehr haben, die uneingeschränkten eingehenden Datenverkehr zulassen. Die Regel lautet NON_COMPLIANT, wenn es Regeln für eingehenden Datenverkehr gibt, die uneingeschränkten eingehenden Datenverkehr zum Redshift-Cluster-Port zulassen.

Kennung: REDSHIFT_UNRESTRICTED_PORT_ACCESS

Ressourcentypen: AWS::Redshift::Cluster

Auslösertyp: Regelmäßig

AWS-Region: Alle unterstützten AWS Regionen außer China (Peking), Asien-Pazifik (Thailand), Asien-Pazifik (Malaysia), Mexiko (Zentral), Kanada West (Calgary), China (Ningxia)

Parameter:

Keine

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

required-tags

Prüft, ob Ihre Ressourcen über die angegebenen Tags verfügen. Sie können beispielsweise überprüfen, ob Ihre EC2 Amazon-Instances das `CostCenter` Tag haben, und gleichzeitig prüfen, ob alle Ihre RDS-Instances über einen Satz Keys-Tags verfügen. Trennen Sie mehrere Werte durch Kommas. Sie können bis zu 6 Tags gleichzeitig prüfen.

Das AWS Dokument zur verwalteten AWS Systems Manager Automatisierung `AWS-SetRequiredTags` eignet sich nicht als Problembehebung bei dieser Regel. Zur Problembehebung müssen Sie Ihre eigene benutzerdefinierte Automatisierungsdokumentation für Systems Manager erstellen.

Kontext: AWS ermöglicht es Ihnen, AWS Ressourcen Metadaten in Form von Tags zuzuweisen. Jedes Tag ist ein Label, das aus einem Schlüssel und einem optionalen Wert besteht, der zum Speichern von Informationen über die Ressource oder die in dieser Ressource gespeicherten Daten dient. Weitere Informationen finden Sie unter Entwickeln einer eigenen Tagging-Strategie.

Sie können diese Regel verwenden, um Ressourcen in Ihrem Konto zu finden, die nicht mit den gewünschten Konfigurationen gestartet wurden, indem Sie angeben, welche Ressourcen Tags haben sollten und wie der erwartete Wert für jedes Tag lautet. Sie können auch Korrekturmaßnahmen ergreifen, um Markierungsfehler zu beheben. Diese Regel verhindert jedoch nicht, dass Sie Ressourcen mit falschen Tags erstellen.

> **Note**
>
> AWS Config unterstützt nicht das Aufzeichnen von zugehörigen Tags für alle Ressourcentypen. So überprüfen Sie, ob Tags im Konfigurationselement (CI) für einen bestimmten Ressourcentyp AWS Config aufgezeichnet werden:

- Stellen Sie sicher, dass die aktuelle Konfiguration für die Ressource AWS Config korrekt aufgezeichnet wird, mit Ausnahme von Tags.
- Stellen Sie sicher, dass AWS Config die aufgezeichnete Konfiguration aktualisiert wird, wenn eine Änderung an der Ressource vorgenommen wird.

ID: REQUIRED_TAGS

Ressourcentypen: AWS::ACM::Certificate AWS::AutoScaling::AutoScalingGroup AWS::CloudFormation::Stack AWS::CodeBuild::Project AWS::DynamoDB::Table, AWS::EC2::CustomerGateway, AWS::EC2::Instance, AWS::EC2::InternetGateway AWS::EC2::NetworkAcl, AWS::EC2::NetworkInterface, AWS::EC2::RouteTable, AWS::EC2::SecurityGroup AWS::EC2::Subnet, AWS::EC2::Volume, AWS::EC2::VPC, AWS::EC2::VPNConnection AWS::EC2::VPNGateway, AWS::ElasticLoadBalancing::LoadBalancer, AWS::ElasticLoadBalancingV2::LoadBalancer, AWS::RDS::DBInstance, AWS::RDS::DBSecurityGroup AWS::RDS::DBSnapshot, AWS::RDS::DBSubnetGroup, AWS::RDS::EventSubscription, AWS::Redshift::Cluster AWS::Redshift::ClusterParameterGroup, AWS::Redshift::ClusterSecurityGroup, AWS::Redshift::ClusterSnapshot, AWS::Redshift::ClusterSubnetGroup AWS::S3::Bucket

Auslösertyp: Konfigurationsänderungen

AWS-Region: Alle unterstützten AWS Regionen

Parameter:

tag1Key, Typ: Zeichenfolge, Standard: CostCenter

Schlüssel des erforderlichen Tags.

tag1Value (optional), Typ: CSV

Optionaler Wert des erforderlichen Tags. Trennen Sie mehrere Werte durch Kommas.

tag2Key (optional), Typ: Zeichenfolge

Schlüssel eines zweiten erforderlichen Tags.

tag2Value (optional), Typ: CSV

Optionaler Wert des zweiten erforderlichen Tags. Trennen Sie mehrere Werte durch Kommas.

tag3Key (optional), Typ: Zeichenfolge

Schlüssel eines dritten erforderlichen Tags.

tag3Value (optional), Typ: CSV

Optionaler Wert des dritten erforderlichen Tags. Trennen Sie mehrere Werte durch Kommas.

tag4Key (optional), Typ: Zeichenfolge

Schlüssel eines vierten erforderlichen Tags.

tag4Value (optional), Typ: CSV

Optionaler Wert des vierten erforderlichen Tags. Trennen Sie mehrere Werte durch Kommas.

tag5Key (optional), Typ: Zeichenfolge

Schlüssel eines fünften erforderlichen Tags.

tag5Value (optional), Typ: CSV

Optionaler Wert des fünften erforderlichen Tags. Trennen Sie mehrere Werte durch Kommas.

tag6Key (optional), Typ: Zeichenfolge

Schlüssel eines sechsten erforderlichen Tags.

tag6Value (optional), Typ: CSV

Optionaler Wert des sechsten erforderlichen Tags. Trennen Sie mehrere Werte durch Kommas.

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

restricted-common-ports

> **Important**
>
> Bei dieser Regel unterscheiden sich die Regel-ID (RESTRICTED_INCOMING_TRAFFIC) und der Regelname (). restricted-common-ports

Prüft, ob die verwendeten Sicherheitsgruppen keinen uneingeschränkten eingehenden Datenverkehr des Transmission Control Protocol (TCP) an die festgelegten Ports zulassen. Die Regel ist COMPLIANT, wenn folgende Kriterien erfüllt sind:

- Der Portzugriff ist für den gesamten TCP-Verkehr gesperrt.
- Der Portzugriff steht TCP-Verkehr über Regeln für eingehenden Datenverkehr offen, wobei die Quelle entweder eine einzelne IPv4 Adresse oder ein Adressbereich in CIDR-Notation ist, der nicht alle IPv4 Adressen abdeckt („0.0.0.0/0"). IPv4
- Der Portzugriff steht TCP-Verkehr über Regeln für eingehenden Datenverkehr offen, wobei die Quelle entweder eine einzelne IPv6 Adresse oder ein Adressbereich in CIDR-Notation ist, der nicht alle IPv6 IPv6 Adressen abdeckt („:: /0)“).

Die Regel ist NON_COMPLIANT, wenn IP-Adressen für eingehende TCP-Verbindungen nicht auf bestimmte Ports beschränkt sind.

ID: RESTRICTED_INCOMING_TRAFFIC

Ressourcentypen: AWS::EC2::SecurityGroup

Auslösertyp: „Konfigurationsänderungen“ und „Regelmäßig“

AWS-Region: Alle unterstützten AWS Regionen

Parameter:

blockedPort1 (optional), Typ: int, Standard: 20

Blockierte TCP-Port-Nummer. Der Standardwert 20 entspricht der FTP-Datenübertragung (File Transfer Protocol).

blockedPort2 (optional), Typ: int, Standard: 21

Blockierte TCP-Port-Nummer. Der Standardwert 21 entspricht der FTP-Befehlssteuerung (File Transfer Protocol).

blockedPort3 (optional), Typ: int, Standard: 3389

Blockierte TCP-Port-Nummer. Der Standardwert 3389 entspricht dem Remote Desktop Protocol (RDP).

blockedPort4 (optional), Typ: int, Standard: 3306

Blockierte TCP-Port-Nummer. Der Standardwert 3306 entspricht dem MySQL-Protokoll.

blockedPort5 (optional), Typ: int, Standard: 4333

Blockierte TCP-Port-Nummer. Der Standardwert 4333 entspricht dem MySQL-Protokoll.

blockedPorts (optional), Typ: CSV

Durch Kommata getrennte Liste der blockierten TCP-Portnummern. Zum Beispiel 20, 21, 3306, 3389 und 4333.

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

root-account-hardware-mfa-aktiviert

Überprüft, ob Ihr AWS Konto für die Verwendung eines Hardwaregeräts mit Multi-Faktor-Authentifizierung (MFA) aktiviert ist, um sich mit Root-Anmeldeinformationen anzumelden. Die Regel ist NON_COMPLIANT, wenn die Anmeldung mit Root-Anmeldeinformationen über virtuelle MFA-Geräte zulässig ist.

> **Note**
>
> Gilt nicht für Konten ohne Root-Benutzeranmeldedaten
> Diese Regel kehrt zurück`NOT_APPLICABLE`, wenn keine Root-Benutzeranmeldedaten vorhanden sind.
> Verwaltete Regeln und globale IAM-Ressourcentypen
> Die globalen IAM-Ressourcentypen, die vor Februar 2022 eingeführt wurden (`AWS::IAM::Group`,, und`AWS::IAM::User`) `AWS::IAM::Policy`AWS::IAM::Role, können nur AWS Config in AWS Regionen erfasst werden, in denen sie vor Februar 2022 verfügbar AWS Config waren. Diese Ressourcentypen können nicht in Regionen erfasst werden, die AWS Config nach Februar 2022 unterstützt werden. Eine Liste dieser Regionen finden Sie unter AWS Aufzeichnungsressourcen | Globale Ressourcen.
> Wenn Sie einen globalen IAM-Ressourcentyp in mindestens einer Region aufzeichnen, führen periodische Regeln, die die Einhaltung des globalen IAM-Ressourcentyps melden, Bewertungen in allen Regionen durch, in denen die periodische Regel hinzugefügt wurde, auch wenn Sie die Aufzeichnung des globalen IAM-Ressourcentyps in der Region, in der die periodische Regel hinzugefügt wurde, nicht aktiviert haben.
> Um unnötige Bewertungen zu vermeiden, sollten Sie nur regelmäßige Regeln einrichten, die die Einhaltung der Vorschriften für einen globalen IAM-Ressourcentyp an eine der

unterstützten Regionen melden. Eine Liste der verwalteten Regeln, die in welchen Regionen unterstützt werden, finden Sie unter Liste der AWS Config verwalteten Regeln nach regionaler Verfügbarkeit.

ID: ROOT_ACCOUNT_HARDWARE_MFA_ENABLED

Auslösertyp: Regelmäßig

AWS-Region: Alle unterstützten AWS Regionen außer China (Peking), Asien-Pazifik (Thailand), Naher Osten (VAE), Asien-Pazifik (Malaysia), AWS GovCloud (USA-Ost), AWS GovCloud (US-West), Mexiko (Zentral), Israel (Tel Aviv), Asien-Pazifik (Taipeh), Kanada West (Calgary), China (Ningxia)

Parameter:

Keine

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

root-account-mfa-enabled

Überprüft, ob der Root-Benutzer Ihres AWS Kontos eine Multi-Faktor-Authentifizierung für die Konsolenanmeldung benötigt. Die Regel lautet NON_COMPLIANT, wenn für den Root-Kontobenutzer von AWS Identity and Access Management (IAM) keine Multi-Faktor-Authentifizierung (MFA) aktiviert ist.

> **Note**
>
> Gilt nicht für Konten ohne Root-Benutzeranmeldedaten
> Diese Regel kehrt zurück`NOT_APPLICABLE`, wenn keine Root-Benutzeranmeldedaten vorhanden sind.
> Verwaltete Regeln und globale IAM-Ressourcentypen
> Die globalen IAM-Ressourcentypen, die vor Februar 2022 eingeführt wurden (`AWS::IAM::Group`,, und`AWS::IAM::User`) `AWS::IAM::Policy`AWS::IAM::Role, können nur AWS Config in AWS Regionen erfasst werden, in denen sie vor Februar 2022 verfügbar AWS Config waren. Diese Ressourcentypen können nicht in Regionen erfasst

werden, die AWS Config nach Februar 2022 unterstützt werden. Eine Liste dieser Regionen finden Sie unter AWS Aufzeichnungsressourcen | Globale Ressourcen.
Wenn Sie einen globalen IAM-Ressourcentyp in mindestens einer Region aufzeichnen, führen periodische Regeln, die die Einhaltung des globalen IAM-Ressourcentyps melden, Bewertungen in allen Regionen durch, in denen die periodische Regel hinzugefügt wurde, auch wenn Sie die Aufzeichnung des globalen IAM-Ressourcentyps in der Region, in der die periodische Regel hinzugefügt wurde, nicht aktiviert haben.
Um unnötige Bewertungen zu vermeiden, sollten Sie nur regelmäßige Regeln einrichten, die die Einhaltung der Vorschriften für einen globalen IAM-Ressourcentyp an eine der unterstützten Regionen melden. Eine Liste der verwalteten Regeln, die in welchen Regionen unterstützt werden, finden Sie unter Liste der AWS Config verwalteten Regeln nach regionaler Verfügbarkeit.

ID: ROOT_ACCOUNT_MFA_ENABLED

Auslösertyp: Regelmäßig

AWS-Region: Alle unterstützten AWS Regionen außer China (Peking), Asien-Pazifik (Thailand), Naher Osten (VAE), Asien-Pazifik (Malaysia), AWS GovCloud (USA-Ost), AWS GovCloud (US-West), Mexiko (Zentral), Israel (Tel Aviv), Asien-Pazifik (Taipeh), Kanada West (Calgary), China (Ningxia)

Parameter:

Keine

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

Route 53- query-logging-enabled

Überprüft, ob die DNS-Abfrageprotokollierung für Ihre öffentlichen gehosteten Zonen von Amazon Route 53 aktiviert ist. Die Regel ist NON_COMPLIANT, wenn die DNS-Abfrageprotokollierung für Ihre öffentlichen gehosteten Zonen von Amazon Route 53 nicht aktiviert ist.

Kennung: _QUERY_LOGGING_ENABLED ROUTE53

Ressourcentypen: AWS::Route53::HostedZone

Auslösertyp: Konfigurationsänderungen

AWS-Region: Nur in der Region USA Ost (Nord-Virginia) verfügbar

Parameter:

Keine

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

s3 express-dir-bucket-lifecycle -regel-check

Prüft, ob Lebenszyklusregeln für einen Amazon S3 Express-Verzeichnis-Bucket konfiguriert sind. Die Regel ist NON_COMPLIANT, wenn es keine aktiven Konfigurationsregeln für den Lebenszyklus gibt oder wenn die Konfiguration nicht mit den Parameterwerten übereinstimmt.

Kennung: S3EXPRESS_DIR_BUCKET_LIFECYCLE_RULES_CHECK

Ressourcentypen: AWS::S3Express::DirectoryBucket

Auslösertyp: Konfigurationsänderungen

AWS-Region: Nur in den Regionen Europa (Stockholm), Asien-Pazifik (Mumbai), USA Ost (Ohio), Europa (Irland), USA Ost (Nord-Virginia), Asien-Pazifik (Tokio), USA West (Oregon) verfügbar

Parameter:

targetExpirationDays (Fakultativ), Typ: int

> Anzahl der Tage nach der Erstellung, an denen Objekte aus Amazon S3 Express-Verzeichnis-Buckets gelöscht werden.

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

nur s3 access-point-in-vpc -

Prüft, ob ein Amazon S3 S3-Zugriffspunkt keinen Zugriff über das Internet zulässt (NetworkOrigin ist VPC). Die Regel ist NON_COMPLIANT, wenn NetworkOrigin es sich um Internet handelt.

ID: S3_ACCESS_POINT_IN_VPC_ONLY

Ressourcentypen: AWS::S3::AccessPoint

Auslösertyp: Konfigurationsänderungen

AWS-Region: Alle unterstützten AWS Regionen außer Asien-Pazifik (Thailand), Asien-Pazifik (Malaysia), Mexiko (Zentral) und Kanada West (Calgary)

Parameter:

Keine

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

access-point-public-accesss3-Blöcke

Prüft, ob für Amazon-S3-Zugangspunkte die Einstellung „Öffentlichen Zugriff blockieren“ aktiviert ist. Die Regel ist NON_COMPLIANT, wenn die Einstellung zum Blockieren des öffentlichen Zugriffs für S3-Zugangspunkte nicht aktiviert ist.

ID: S3_ACCESS_POINT_PUBLIC_ACCESS_BLOCKS

Ressourcentypen: AWS::S3::AccessPoint

Auslösertyp: Konfigurationsänderungen

AWS-Region: Alle unterstützten AWS Regionen außer Asien-Pazifik (Thailand), Asien-Pazifik (Malaysia), Mexiko (Zentral) und Kanada West (Calgary)

Parameter:

excludedAccessPoints (Fakultativ), Typ: CSV

Durch Kommata getrennte Liste der Namen für zulässige öffentliche Amazon-S3-Zugangspunkte.

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

account-level-public-accesss3-Blöcke

Prüft, ob die erforderliche Einstellung zum Blockieren des öffentlichen Zugriffs auf Kontoebene konfiguriert ist. Die Regel ist nur NON_COMPLIANT, wenn die unten festgelegten Felder nicht mit den entsprechenden Feldern im Konfigurationselement übereinstimmen.

> **Note**
>
> Wenn Sie diese Regel verwenden, stellen Sie sicher, dass „Öffentlichen Zugriff blockieren“ für S3 aktiviert ist. Die Regel wird durch Änderungen ausgelöst, weshalb sie erst aufgerufen wird, wenn „Öffentlichen Zugriff blockieren“ für S3 aktiviert wird. Wenn „Öffentlichen Zugriff blockieren“ für S3 nicht aktiviert ist, gibt die Regel INSUFFICIENT_DATA zurück. Das bedeutet, dass Sie möglicherweise immer noch einige öffentliche Buckets haben. Weitere Informationen zum Blockieren des öffentlichen Zugriffs auf S3 finden Sie unter Blockieren des öffentlichen Zugriffs auf Ihren Amazon-S3-Speicher.

ID: S3_ACCOUNT_LEVEL_PUBLIC_ACCESS_BLOCKS

Ressourcentypen: AWS::S3::AccountPublicAccessBlock

Auslösertyp: Konfigurationsänderungen (aktueller Status wird nicht geprüft, nur ausgewertet, wenn Änderungen neue Ereignisse generieren)

> **Note**
>
> Diese Regel wird nur durch Konfigurationsänderungen für die spezifische Region ausgelöst, in der sich der S3-Endpunkt befindet. In allen anderen Regionen wird die Regel regelmäßig geprüft. Wenn in einer anderen Region eine Änderung vorgenommen wurde, kann es zu einer Verzögerung kommen, bis die Regel NON_COMPLIANT zurückgibt.

AWS-Region: Alle unterstützten AWS Regionen außer Asien-Pazifik (Thailand), Asien-Pazifik (Malaysia), Mexiko (Zentral), Israel (Tel Aviv), Asien-Pazifik (Taipeh) und Kanada West (Calgary)

Parameter:

IgnorePublicAcls (Fakultativ), Typ: Zeichenfolge, Standard: True

IgnorePublicAcls ist erzwungen oder nicht, Standardeinstellung True

BlockPublicPolicy (Fakultativ), Typ: Zeichenfolge, Standard: True

BlockPublicPolicy ist erzwungen oder nicht, Standardeinstellung True

BlockPublicAcls (Fakultativ), Typ: Zeichenfolge, Standard: True

BlockPublicAcls ist erzwungen oder nicht, Standardeinstellung True

RestrictPublicBuckets (Fakultativ), Typ: Zeichenfolge, Standard: True

RestrictPublicBuckets ist erzwungen oder nicht, Standardeinstellung True

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

account-level-public-accesss3-Blöcke-periodisch

Prüft, ob die erforderliche Einstellung zum Blockieren des öffentlichen Zugriffs auf Kontoebene konfiguriert ist. Die Regel ist NON_COMPLIANT, wenn das Konfigurationselement nicht mit einer oder mehreren Einstellungen aus Parametern (oder der Standardeinstellung) übereinstimmt.

ID: S3_ACCOUNT_LEVEL_PUBLIC_ACCESS_BLOCKS_PERIODIC

Ressourcentypen: AWS::::Account

Auslösertyp: Regelmäßig

AWS-Region: Alle unterstützten Regionen AWS

Parameter:

IgnorePublicAcls (Fakultativ), Typ: Zeichenfolge

IgnorePublicAcls ist erzwungen oder nicht, Standardeinstellung True

BlockPublicPolicy (Fakultativ), Typ: Zeichenfolge

BlockPublicPolicy ist erzwungen oder nicht, Standardeinstellung True

BlockPublicAcls (Fakultativ), Typ: Zeichenfolge

BlockPublicAcls ist erzwungen oder nicht, Standardeinstellung True

RestrictPublicBuckets (Fakultativ), Typ: Zeichenfolge

RestrictPublicBuckets ist erzwungen oder nicht, Standardeinstellung True

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

s-3 bucket-acl-prohibited

Prüft, ob Amazon Simple Storage Service (Amazon S3) -Buckets Benutzerberechtigungen über Zugriffskontrolllisten zulassen (ACLs). Die Regel lautet NON_COMPLIANT, wenn sie für den Benutzerzugriff in Amazon S3 S3-Buckets konfiguriert ACLs sind.

ID: S3_BUCKET_ACL_PROHIBITED

Ressourcentypen: AWS::S3::Bucket

Auslösertyp: Konfigurationsänderungen

AWS-Region: Alle unterstützten AWS Regionen außer Asien-Pazifik (Thailand), Asien-Pazifik (Malaysia), Mexiko (Zentral) und Kanada West (Calgary)

Parameter:

Keine

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

s-3 bucket-blacklisted-actions-prohibited

Prüft, ob eine Bucket-Richtlinie von Amazon Simple Storage Service (Amazon S3) keine Aktionen auf Bucket-Ebene und Objektebene auf Blocklisten für Ressourcen im Bucket für Prinzipale anderer

Konten zulässt. AWS Die Regel überprüft beispielsweise, ob die Amazon S3 S3-Bucket-Richtlinie einem anderen AWS Konto nicht erlaubt, `s3:GetBucket*` Aktionen und `s3:DeleteObject` für Objekte im Bucket auszuführen. Die Regel ist NON_COMPLIANT, wenn gesperrte Aktionen gemäß der Bucket-Richtlinie von Amazon S3 zulässig sind.

> **Note**
>
> Die Regel sucht nur in der Eigenschaft „Prinzipal“ nach Entitäten und berücksichtigt in einer Richtlinie keine Bedingungen unter der Eigenschaft „Bedingung“.

ID: S3_BUCKET_BLACKLISTED_ACTIONS_PROHIBITED

Ressourcentypen: AWS::S3::Bucket

Auslösertyp: Konfigurationsänderungen

AWS-Region: Alle unterstützten AWS Regionen außer Asien-Pazifik (Hyderabad) und Europa (Spanien)

Parameter:

blacklistedActionPattern, Typ: CSV

Durch Kommas getrennte Liste von Aktionsmustern auf der schwarzen Liste, z. B. s3: GetBucket * und s3:. DeleteObject

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

bucket-cross-region-replications3-fähig

Überprüft, ob Sie die regionsübergreifende S3-Replikation für Ihre Amazon S3 S3-Buckets aktiviert haben. Die Regel lautet NON_COMPLIANT, wenn keine Replikationsregeln für die regionsübergreifende Replikation aktiviert sind.

Kennung: S3_BUCKET_CROSS_REGION_REPLICATION_ENABLED

Ressourcentypen: AWS::S3::Bucket

Auslösertyp: Konfigurationsänderungen

AWS-Region: Alle unterstützten AWS Regionen außer Asien-Pazifik (Thailand), Asien-Pazifik (Malaysia), Mexiko (Zentral) und Kanada West (Calgary)

Parameter:

Keine

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

s-3 bucket-default-lock-enabled

Überprüft, ob für den S3-Bucket die Sperre standardmäßig aktiviert ist. Die Regel ist NON_COMPLIANT, wenn die Sperre nicht aktiviert ist.

ID: S3_BUCKET_DEFAULT_LOCK_ENABLED

Ressourcentypen: AWS::S3::Bucket

Auslösertyp: Konfigurationsänderungen

AWS-Region: Alle unterstützten AWS Regionen

Parameter:

mode (optional), Typ: Zeichenfolge

> mode: (optional): Ein Modusparameter mit den gültigen Werten GOVERNANCE oder COMPLIANCE.

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

s3 bucket-level-public-access - verboten

Prüft, ob S3-Buckets öffentlich zugänglich sind. Die Regel ist NON_COMPLIANT, wenn ein S3-Bucket nicht im Parameter `excludedPublicBuckets` aufgeführt ist und die Einstellungen auf Bucket-Ebene öffentlich sind.

ID: S3_BUCKET_LEVEL_PUBLIC_ACCESS_PROHIBITED

Ressourcentypen: AWS::S3::Bucket

Auslösertyp: Konfigurationsänderungen

AWS-Region: Alle unterstützten AWS Regionen

Parameter:

excludedPublicBuckets (Fakultativ), Typ: CSV

> Durch Kommata getrennte Liste bekannter zulässiger öffentlicher Namen von Amazon-S3-Buckets.

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

s-3 bucket-logging-enabled

Prüft, ob die Protokollierung für Ihre S3-Buckets aktiviert ist. Die Regel ist NON_COMPLIANT, wenn die Protokollierung nicht aktiviert ist.

ID: S3_BUCKET_LOGGING_ENABLED

Ressourcentypen: AWS::S3::Bucket

Auslösertyp: Konfigurationsänderungen

AWS-Region: Alle unterstützten AWS Regionen

Parameter:

targetBucket (optional), Typ: Zeichenfolge

S3-Ziel-Bucket zum Speichern von Serverzugriffsprotokollen.

targetPrefix (optional), Typ: Zeichenfolge

Präfix des S3-Buckets zum Speichern von Serverzugriffsprotokollen.

Proaktive Auswertung

Anweisungen zur Ausführung dieser Regel im proaktiven Modus finden Sie unter Evaluieren Ihrer Ressourcen mithilfe von AWS Config Regeln. Damit diese Regel im proaktiven Modus COMPLIANT zurückgibt, muss das Ressourcenkonfigurationsschema für die StartResourceEvaluationAPI die folgenden Eingaben enthalten, die als Zeichenfolge kodiert sind:

```
"ResourceConfiguration":
...
{
   "BucketName": "amzn-s3-demo-bucket",
   "LoggingConfiguration": {
         "DestinationBucketName": "amzn-s3-demo-destination-bucket",
         "LogFilePrefix":"my-log"
   }
}
...
```

Weitere Informationen zur proaktiven Auswertung finden Sie unter Auswertungsmodus.

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

s-3 bucket-mfa-delete-enabled

Prüft, ob MFA Delete in der Konfiguration der Versionsverwaltung des Amazon Simple Storage Service (Amazon S3)-Buckets aktiviert ist. Die Regel ist NON_COMPLIANT, wenn MFA Delete nicht aktiviert ist.

ID: S3_BUCKET_MFA_DELETE_ENABLED

Ressourcentypen: AWS::S3::Bucket

Auslösertyp: Konfigurationsänderungen

AWS-Region: Alle unterstützten AWS Regionen außer Asien-Pazifik (Thailand), Asien-Pazifik (Malaysia), Mexiko (Zentral) und Kanada West (Calgary)

Parameter:

Keine

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

s-3 bucket-policy-grantee-check

Überprüft, ob der vom Amazon S3 S3-Bucket gewährte Zugriff durch die von Ihnen AWS angegebenen Principals, Verbundbenutzer, Service-Principals, IP-Adressen oder VPCs IP-Adressen eingeschränkt ist. Die Regel ist COMPLIANT, wenn keine Bucket-Richtlinie vorhanden ist.

Wenn beispielsweise der Eingabeparameter für die Regel aus einer Liste mit den zwei Prinzipalen `111122223333` und `444455556666` besteht und die Bucket-Richtlinie angibt, dass nur `111122223333` auf den Bucket zugreifen kann, ist die Regel COMPLIANT. Mit denselben Eingabeparametern: Wenn die Bucket-Richtlinie dies festlegt `111122223333` und auf den Bucket zugreifen `444455556666` kann, ist sie ebenfalls KONFORM.

Wenn die Bucket-Richtlinie jedoch angibt, dass auf den Bucket zugegriffen `999900009999` werden kann, lautet die Regel NON_COMPLIANT.

> **Note**
>
> Wenn eine Bucket-Richtlinie mehr als eine Anweisung enthält, wird jede Anweisung in der Bucket-Richtlinie anhand dieser Regel ausgewertet.

ID: S3_BUCKET_POLICY_GRANTEE_CHECK

Ressourcentypen: AWS::S3::Bucket

Auslösertyp: Konfigurationsänderungen

AWS-Region: Alle unterstützten AWS Regionen außer der Region Asien-Pazifik (Taipeh)

Parameter:

awsPrincipals (optional), Typ: CSV

Durch Kommas getrennte Liste mit Prinzipalen wie IAM-Benutzer ARNs, IAM-Rolle und Konten. ARNs AWS Sie müssen den vollständigen ARN angeben oder einen teilweisen Abgleich verwenden. Zum Beispiel „arn:aws:iam: :role/" oder „arn:aws:iam: :role/*`AccountID`“. `role_name` `AccountID` Wenn der angegebene Wert nicht exakt mit dem in der Bucket-Richtlinie angegebenen Prinzipal-ARN übereinstimmt, lautet die Regel NON_COMPLIANT.

servicePrincipals (optional), Typ: CSV

Durch Kommata getrennte Liste von Service-Prinzipalen, zum Beispiel „cloudtrail.amazonaws.com, lambda.amazonaws.com“.

federatedUsers (optional), Typ: CSV

Durch Kommata getrennte Liste der Anbieter von Web-Identitätsverbunden wie Amazon Cognito und SAML. Zum Beispiel „cognito-identity.amazonaws.com, arn:aws:iam::111122223333:saml-provider/my-provider“.

ipAddresses (optional), Typ: CSV

Durch Kommata getrennte Liste von IP-Adressen im CIDR-Format, zum Beispiel „10.0.0.1, 192.168.1.0/24, 2001:db8: :/32“.

vpcIds (optional), Typ: CSV

Durch Kommas getrennte Liste von Amazon Virtual Private Clouds (Amazon VPC) IDs, zum Beispiel 'vpc-1234abc0, vpc-ab1234c0'.

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

bucket-policy-not-mores3-permissiv

Prüft, ob Ihre Bucket-Richtlinien für Amazon Simple Storage Service keine anderen Berechtigungen zwischen Konten als die von Ihnen angegebene Bucket-Richtlinie zur Steuerung des Zugriffs auf Amazon S3 erlauben.

> **Note**
>
> Wenn Sie einen ungültigen Parameterwert angeben, wird die folgende Fehlermeldung angezeigt: Der Wert für den controlPolicy-Parameter muss eine Bucket-Richtlinie für Amazon S3 sein.

ID: S3_BUCKET_POLICY_NOT_MORE_PERMISSIVE

Ressourcentypen: AWS::S3::Bucket

Auslösertyp: Konfigurationsänderungen

AWS-Region: Alle unterstützten AWS Regionen außer der Region Asien-Pazifik (Taipeh)

Parameter:

controlPolicy, Typ: Zeichenfolge

> Bucket-Richtlinie für Amazon S3, die eine Obergrenze für die Berechtigungen Ihrer S3-Buckets festlegt. Die Richtlinie darf maximal 1 024 Zeichen lang sein.

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

s-3 bucket-public-read-prohibited

Prüft, ob Ihre S3-Buckets keinen öffentlichen Lesezugriff zulassen. Mit dieser Regel werden die Einstellungen für „Block Public Access“ (Blockieren des öffentlichen Zugriffs), die Bucket-Richtlinie und die Bucket-Zugriffskontrollliste (ACL) überprüft.

Die Regel ist konform, wenn die beiden folgenden Punkte erfüllt sind:

- Die Einstellung „Block Public Access“ schränkt die öffentlichen Richtlinien ein oder die Bucket-Richtlinie erlaubt keinen öffentlichen Lesezugriff.
- Die Einstellung „Öffentlichen Zugriff blockieren“ schränkt den öffentlichen Lesezugriff ein, ACLs oder die Bucket-ACL erlaubt keinen öffentlichen Lesezugriff.

Die Regel ist nicht konform, wenn:

- Wenn die Einstellung „Öffentlichen Zugriff blockieren“ öffentliche Richtlinien nicht einschränkt, wird AWS Config geprüft, ob die Richtlinie öffentlichen Lesezugriff zulässt. Wenn die Richtlinie den öffentlichen Lesezugriff erlaubt, ist die Regel nicht konform.
- Wenn die Einstellung „Öffentlichen Zugriff blockieren“ den öffentlichen Bucket nicht einschränkt ACLs, wird AWS Config geprüft, ob die Bucket-ACL öffentlichen Lesezugriff zulässt. Wenn die Bucket-ACL den öffentlichen Lesezugriff erlaubt, ist die Regel nicht konform.

> **Note**
>
> Um als nicht öffentlich zu gelten, muss eine S3-Bucket-Richtlinie nur Zugriff auf feste Werte gewähren. Das bedeutet Werte, die keinen Platzhalter oder das folgende IAM-Richtlinienelement enthalten: Variablen.

ID: S3_BUCKET_PUBLIC_READ_PROHIBITED

Ressourcentypen: AWS::S3::Bucket

Auslösertyp: „Konfigurationsänderungen“ und „Regelmäßig“

AWS-Region: Alle unterstützten AWS Regionen

Parameter:

Keine

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

s-3 bucket-public-write-prohibited

Prüft, ob Ihre Amazon-S3-Buckets keinen öffentlichen Schreibzugriff zulassen. Mit dieser Regel werden die Einstellungen für „Block Public Access“ (Blockieren des öffentlichen Zugriffs), die Bucket-Richtlinie und die Bucket-Zugriffskontrollliste (ACL) überprüft.

Die Regel ist konform, wenn die beiden folgenden Punkte erfüllt sind:

- Die Einstellung „Block Public Access“ schränkt die öffentlichen Richtlinien ein oder die Bucket-Richtlinie erlaubt keinen öffentlichen Schreibzugriff.
- Die Einstellung „Öffentlichen Zugriff blockieren“ schränkt den öffentlichen Schreibzugriff ein, ACLs oder die Bucket-ACL erlaubt keinen öffentlichen Schreibzugriff.

Die Regel ist nicht konform, wenn:

- Wenn die Einstellung „Öffentlichen Zugriff blockieren“ öffentliche Richtlinien nicht einschränkt, wird AWS Config geprüft, ob die Richtlinie öffentlichen Schreibzugriff zulässt. Wenn die Richtlinie öffentlichen Schreibzugriff erlaubt, ist die Regel nicht konform.
- Wenn die Einstellung „Öffentlichen Zugriff blockieren“ den öffentlichen Bucket nicht einschränkt ACLs, wird AWS Config geprüft, ob die Bucket-ACL öffentlichen Schreibzugriff zulässt. Wenn die Bucket-ACL öffentlichen Schreibzugriff erlaubt, ist die Regel nicht konform.

> **Note**
>
> Diese Regel wertet keine Änderungen an der Einstellung zum Blockieren des öffentlichen Zugriffs auf Kontoebene aus. Um zu überprüfen, ob die erforderlichen Blockeinstellungen für öffentlichen Zugriff auf Kontoebene konfiguriert sind, siehe s3- account-level-public-access -blocks und s3- account-level-public-access -blocks-periodic.

> **Note**
>
> Um als nicht öffentlich zu gelten, muss eine S3-Bucket-Richtlinie nur Zugriff auf feste Werte gewähren. Das bedeutet Werte, die keinen Platzhalter oder das folgende IAM-Richtlinienelement enthalten: Variablen.

ID: S3_BUCKET_PUBLIC_WRITE_PROHIBITED

Ressourcentypen: AWS::S3::Bucket

Auslösertyp: „Konfigurationsänderungen“ und „Regelmäßig“

AWS-Region: Alle unterstützten AWS Regionen

Parameter:

Keine

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

s-3 bucket-replication-enabled

Prüft, ob für S3-Buckets Replikationsregeln aktiviert sind. Die Regel ist NON_COMPLIANT, wenn ein S3-Bucket keine Replikationsregel hat oder eine Replikationsregel hat, die nicht aktiviert ist.

ID: S3_BUCKET_REPLICATION_ENABLED

Ressourcentypen: AWS::S3::Bucket

Auslösertyp: Konfigurationsänderungen

AWS-Region: Alle unterstützten AWS Regionen

Parameter:

ReplicationType (Fakultativ), Typ: Zeichenfolge

> Zulässige Werte: CROSS-REGION und SAME-REGION. Geben Sie CROSS-REGION ein, damit die Regel prüft, ob für alle Buckets nur die regionsübergreifende Replikation aktiviert ist. Geben Sie SAME-REGION ein, damit die Regel prüft, ob für alle Buckets nur die Replikation in der gleichen Region aktiviert ist.

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

bucket-server-side-encryptions3-fähig

Prüft, ob für Ihren Amazon-S3-Bucket entweder die Amazon-S3-Standardverschlüsselung aktiviert ist oder die Richtlinie von Amazon-S3-Bucket `put-object`-Anfragen ohne serverseitige

Verschlüsselung, die AES-256 oder AWS Key Management Service verwendet, explizit ausschließt. Die Regel ist NON_COMPLIANT, wenn Ihr Amazon-S3-Bucket nicht standardmäßig verschlüsselt ist.

ID: S3_BUCKET_SERVER_SIDE_ENCRYPTION_ENABLED

Ressourcentypen: AWS::S3::Bucket

Auslösertyp: Konfigurationsänderungen

AWS-Region: Alle unterstützten AWS Regionen außer der Region Europa (Spanien)

Parameter:

Keine

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

s-3 bucket-ssl-requests-only

Prüft, ob S3-Buckets über Richtlinien verfügen, die bei Anfragen die Verwendung von SSL/TLS erfordern. Die Regel ist NON_COMPLIANT, wenn ein S3-Bucket über Richtlinien verfügt, die HTTP-Anfragen zulassen.

ID: S3_BUCKET_SSL_REQUESTS_ONLY

Ressourcentypen: AWS::S3::Bucket

Auslösertyp: Konfigurationsänderungen

AWS-Region: Alle unterstützten AWS Regionen

Parameter:

Keine

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

s3-bucket-tagged

Prüft, ob Amazon S3 S3-Buckets Tags haben. Optional können Sie Tag-Schlüssel angeben. Die Regel lautet NON_COMPLIANT, wenn keine Tags vorhanden sind oder wenn die angegebenen Tag-Schlüssel nicht vorhanden sind. Die Regel sucht nicht nach Tags, die mit 'aws: 'beginnen.

Kennung: S3_BUCKET_TAGGED

Ressourcentypen: AWS::S3::Bucket

Auslösertyp: Konfigurationsänderungen

AWS-Region: Alle unterstützten AWS Regionen außer China (Peking), Asien-Pazifik (Thailand), Asien-Pazifik (Malaysia), AWS GovCloud (USA-Ost), AWS GovCloud (US-West), Mexiko (Zentral), China (Ningxia)

Parameter:

requiredKeyTags (Fakultativ), Typ: CSV

> Durch Kommas getrennte Liste von Tag-Schlüsseln, die von der Regel überprüft werden sollen. Falls angegeben, lautet die Regel NON_COMPLIANT, wenn die ausgewertete Ressource diese Schlüssel nicht enthält. Bei Tag-Schlüsseln wird die Groß- und Kleinschreibung beachtet. Tag-Schlüssel, die mit „aws:“ beginnen, sind nicht erlaubt.

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

s-3 bucket-versioning-enabled

Prüft, ob die Versionsverwaltung für Ihre S3-Buckets aktiviert ist. Optional wird von der Regel überprüft, ob die MFA-Löschung für Ihre S3-Buckets aktiviert ist.

ID: S3_BUCKET_VERSIONING_ENABLED

Ressourcentypen: AWS::S3::Bucket

Auslösertyp: Konfigurationsänderungen

AWS-Region: Alle unterstützten AWS Regionen

Parameter:

isMfaDeleteAktiviert (optional), Typ: Zeichenfolge

MFA-Löschung ist für Ihre S3-Buckets aktiviert.

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

s-3 default-encryption-kms

Überprüft, ob die S3-Buckets mit dem AWS Key Management Service (AWS KMS) verschlüsselt sind. Die Regel lautet NON_COMPLIANT, wenn der S3-Bucket nicht mit einem AWS KMS-Schlüssel verschlüsselt ist.

ID: S3_DEFAULT_ENCRYPTION_KMS

Ressourcentypen:, AWS::S3::Bucket AWS::KMS::Key

Auslösertyp: Konfigurationsänderungen

AWS-Region: Alle unterstützten AWS Regionen außer der Region Asien-Pazifik (Taipeh)

Parameter:

kmsKeyArns (Fakultativ), Typ: CSV

Durch Kommas getrennte Liste der AWS KMS-Schlüssel, die für die Verschlüsselung von Amazon S3 S3-Buckets ARNs zulässig sind.

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

s-3 event-notifications-enabled

Prüft, ob Amazon-S3-Ereignisbenachrichtigungen in einem S3-Bucket aktiviert sind. Die Regel ist NON_COMPLIANT, wenn für einen Bucket keine S3-Ereignisbenachrichtigungen festgelegt

sind oder der Ereignistyp oder das Ziel nicht mit den Parametern `eventTypes` und destinationArn übereinstimmen.

ID: S3_EVENT_NOTIFICATIONS_ENABLED

Ressourcentypen: AWS::S3::Bucket

Auslösertyp: Konfigurationsänderungen

AWS-Region: Alle unterstützten AWS Regionen außer Asien-Pazifik (Thailand), Asien-Pazifik (Jakarta), Asien-Pazifik (Malaysia), Mexiko (Zentral) und Kanada West (Calgary)

Parameter:

destinationArn (optional), Typ: Zeichenfolge

Der Amazon-Ressourcenname (ARN) des Ziels für die Ereignisbenachrichtigung (Amazon SNS-Thema, AWS Lambda, Amazon SQS SQS-Warteschlange).

eventTypes (optional), Typ: CSV

Durch Kommata getrennte Liste der bevorzugten Amazon-S3-Ereignistypen

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

s3 last-backup-recovery-point - erstellt

Prüft, ob für Amazon Simple Storage Service (Amazon S3) ein Wiederherstellungspunkt erstellt wurde. Die Regel ist NON_COMPLIANT, wenn innerhalb des angegebenen Zeitraums kein entsprechender Wiederherstellungspunkt für den Amazon-S3-Bucket erstellt wurde.

ID: S3_LAST_BACKUP_RECOVERY_POINT_CREATED

Ressourcentypen: AWS::S3::Bucket

Auslösertyp: Regelmäßig

AWS-Region: Alle unterstützten AWS Regionen außer China (Peking), Asien-Pazifik (Thailand), Asien-Pazifik (Malaysia), Mexiko (Zentral), Israel (Tel Aviv), Kanada West (Calgary), China (Ningxia)

Parameter:

resourceTags (optional), Typ: Zeichenfolge

Tags des Amazon-S3-Buckets, der von der Regel geprüft werden soll, im JSON-Format `{"tagkey" : "tagValue"}`.

resourceId (optional), Typ: Zeichenfolge

Name des Amazon-S3-Buckets, den die Regel überprüfen soll.

recoveryPointAgeWert (optional), Typ: int, Standard: 1

Numerischer Wert für das zulässige Höchstalter. Nicht mehr als 744 für Stunden oder 31 für Tage.

recoveryPointAgeEinheit (optional), Typ: Zeichenfolge, Standard: days

Zeiteinheit für das zulässige Höchstalter. Zulässige Werte: „Stunden“, „Tage“.

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

s-3 lifecycle-policy-check

Prüft, ob für einen Amazon Simple Storage Service (Amazon S3)-Bucket eine Lebenszyklusregel konfiguriert ist. Die Regel ist NON_COMPLIANT, wenn es keine aktiven Konfigurationsregeln für den Lebenszyklus gibt oder wenn die Konfiguration nicht mit den Parameterwerten übereinstimmt.

ID: S3_LIFECYCLE_POLICY_CHECK

Ressourcentypen: AWS::S3::Bucket

Auslösertyp: Konfigurationsänderungen

AWS-Region: Alle unterstützten AWS Regionen außer Asien-Pazifik (Thailand), Asien-Pazifik (Malaysia), Mexiko (Zentral) und Kanada West (Calgary)

Parameter:

targetTransitionDays (Fakultativ), Typ: int

Anzahl der Tage nach der Objekterstellung, nach denen Objekte in die angegebene Speicherklasse übergehen (z. B. 30 Tage)

targetExpirationDays (Fakultativ), Typ: int

Anzahl der Tage nach der Objekterstellung, nach denen Objekte gelöscht werden (z. B. 395 Tage)

targetTransitionStorageKlasse (fakultativ), Typ: Zeichenfolge

Typ der Zielspeicherklasse. Zum Beispiel Amazon S3 Standard-Infrequent Access (S3 Standard-IA). Weitere Informationen finden Sie unter Amazon S3 S3-Speicherklassen verstehen und verwalten.

targetPrefix (optional), Typ: Zeichenfolge

Amazon-S3-Objektpräfix zur Identifizierung eines oder mehrerer Objekte.

bucketNames (optional), Typ: CSV

Durch Kommata getrennte Liste der Namen von Amazon-S3-Buckets, für die die Lebenszyklusrichtlinie aktiviert ist.

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

s-3 meets-restore-time-target

Überprüft, ob die Wiederherstellungszeit von Amazon Simple Storage Service (Amazon S3)-Buckets die angegebene Dauer einhält. Die Regel lautet NON_COMPLIANT, wenn LatestRestoreExecutionTimeMinutes der Wert eines Amazon S3 S3-Buckets mehr als maxRestoreTime Minuten beträgt.

Kennung: S3_MEETS_RESTORE_TIME_TARGET

Ressourcentypen: AWS::S3::Bucket

Auslösertyp: Regelmäßig

AWS-Region: Alle unterstützten AWS Regionen außer China (Peking), Asien-Pazifik (Thailand), Asien-Pazifik (Malaysia), AWS GovCloud (USA-Ost), AWS GovCloud (US-West), Mexiko (Zentral), Israel (Tel Aviv), Kanada West (Calgary), China (Ningxia)

Parameter:

maxRestoreTime, Typ: int

Numerischer Wert für die maximal zulässige Wiederherstellungslaufzeit.

resourceTags (optional), Typ: Zeichenfolge

Tags des Amazon-S3-Buckets, der von der Regel geprüft werden soll, im JSON-Format .

resourceId (optional), Typ: Zeichenfolge

Name des Amazon-S3-Buckets, den die Regel überprüfen soll.

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

resources-in-logically-airS3-Gapped-Tresor

Überprüft, ob sich Amazon Simple Storage Service (Amazon S3) -Buckets in einem Tresor mit logischem Air-Gap befinden. Die Regel lautet NON_COMPLIANT, wenn sich ein Amazon S3 S3-Bucket innerhalb des angegebenen Zeitraums nicht in einem Tresor mit logischem Air-Gap befindet.

Kennung: S3_RESOURCES_IN_LOGICALLY_AIR_GAPPED_VAULT

Ressourcentypen: AWS::S3::Bucket

Auslösertyp: Regelmäßig

AWS-Region: Nur verfügbar in Europa (Stockholm), Naher Osten (Bahrain), Asien-Pazifik (Mumbai), Europa (Paris), USA Ost (Ohio), Europa (Irland), Europa (Frankfurt), Südamerika (Sao Paulo), USA Ost (Nord-Virginia), Asien-Pazifik (Seoul), Asien-Pazifik (Osaka), Europa (London), Asien-Pazifik (Tokio), USA West (Oregon), USA West (Nordkalifornien), Asien-Pazifik (Singapur), Asien-Pazifik (Sydney), Region Kanada (Zentral)

Parameter:

resourceTags (optional), Typ: Zeichenfolge

Tags des Amazon-S3-Buckets, der von der Regel geprüft werden soll, im JSON-Format .

resourceId (optional), Typ: Zeichenfolge

Name des Amazon-S3-Buckets, den die Regel überprüfen soll.

recoveryPointAgeWert (optional), Typ: int, Standard: 1

Numerischer Wert für das zulässige Höchstalter. Nicht mehr als 2184 für Stunden, 91 für Tage.

recoveryPointAgeEinheit (optional), Typ: Zeichenfolge, Standard: days

Zeiteinheit für das zulässige Höchstalter. Zulässige Werte: „Stunden“, „Tage“.

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

resources-protected-by-backups3-plan

Prüft, ob Amazon Simple Storage Service (Amazon S3)-Buckets durch einen Backup-Plan geschützt sind. Die Regel ist NON_COMPLIANT, wenn der Amazon-S3-Bucket nicht durch einen Backup-Plan gedeckt ist.

ID: S3_RESOURCES_PROTECTED_BY_BACKUP_PLAN

Ressourcentypen: AWS::S3::Bucket

Auslösertyp: Regelmäßig

AWS-Region: Alle unterstützten AWS Regionen außer China (Peking), Asien-Pazifik (Thailand), Asien-Pazifik (Malaysia), Mexiko (Zentral), Israel (Tel Aviv), Kanada West (Calgary), China (Ningxia)

Parameter:

resourceTags (optional), Typ: Zeichenfolge

Tags für Amazon-S3-Buckets, die von der Regel geprüft werden sollen, im JSON-Format `{"tagkey" : "tagValue"}`.

resourceId (optional), Typ: Zeichenfolge

Name des Amazon-S3-Buckets, den die Regel überprüfen soll.

crossRegionList (Fakultativ), Typ: Zeichenfolge

Durch Kommata getrennte Liste der Zielregionen, für die die regionsübergreifende Backup-Kopie aufbewahrt werden soll.

crossAccountList (Fakultativ), Typ: Zeichenfolge

Durch Kommata getrennte Liste der Zielkonten, für die die kontoübergreifende Backup-Kopie aufbewahrt werden soll.

maxRetentionDays (Fakultativ), Typ: int

Die maximale Aufbewahrungsdauer in Tagen für die Backup-Tresorsperre.

minRetentionDays (Fakultativ), Typ: int

Die Mindestaufbewahrungsdauer in Tagen für die Backup-Tresorsperre.

backupVaultLockÜberprüfen Sie (optional), Typ: Zeichenfolge

Akzeptierte Werte: „True“ oder „False“. Geben Sie „True“ ein, damit die Regel prüft, ob die Ressource in einem gesperrten Tresor gesichert ist.

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

s-3 version-lifecycle-policy-check

Prüft, ob für Buckets, die Amazon Simple Storage Service (Amazon S3) ausführen können, eine Lebenszyklusrichtlinie konfiguriert ist. Die Regel ist NON_COMPLIANT, wenn die Lebenszyklusrichtlinie für Amazon S3 nicht aktiviert ist.

ID: S3_VERSION_LIFECYCLE_POLICY_CHECK

Ressourcentypen: AWS::S3::Bucket

Auslösertyp: Konfigurationsänderungen

AWS-Region: Alle unterstützten AWS Regionen außer Asien-Pazifik (Thailand), Asien-Pazifik (Malaysia), Mexiko (Zentral) und Kanada West (Calgary)

Parameter:

bucketNames (optional), Typ: CSV

Durch Kommata getrennte Liste der Namen von Amazon-S3-Buckets, für die die Lebenszyklusrichtlinie aktiviert ist.

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

sagemaker-app-image-config-markiert

Prüft, ob SageMaker Amazon-App-Image-Konfigurationen Tags haben. Optional können Sie Tag-Schlüssel angeben. Die Regel lautet NON_COMPLIANT, wenn keine Tags vorhanden sind oder wenn die angegebenen Tag-Schlüssel nicht vorhanden sind. Die Regel sucht nicht nach Tags, die mit 'aws: 'beginnen.

Kennung: SAGEMAKER_APP_IMAGE_CONFIG_TAGGED

Ressourcentypen: AWS::SageMaker::AppImageConfig

Auslösertyp: Konfigurationsänderungen

AWS-Region: Alle unterstützten AWS Regionen außer China (Peking), Asien-Pazifik (Thailand), Asien-Pazifik (Hyderabad), Asien-Pazifik (Malaysia), Asien-Pazifik (Melbourne), AWS GovCloud (USA-Ost), AWS GovCloud (US-West), Mexiko (Zentral), Kanada West (Calgary), China (Ningxia), Europa (Zürich)

Parameter:

requiredKeyTags (Fakultativ), Typ: CSV

> Durch Kommas getrennte Liste von Tag-Schlüsseln, die von der Regel überprüft werden sollen. Falls angegeben, lautet die Regel NON_COMPLIANT, wenn die ausgewertete Ressource diese Schlüssel nicht enthält. Bei Tag-Schlüsseln wird die Groß- und Kleinschreibung beachtet. Tag-Schlüssel, die mit „aws:“ beginnen, sind nicht erlaubt.

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

sagemaker-domain-in-vpc

Prüft, ob eine SageMaker Amazon-Domain eine kundeneigene Amazon Virtual Private Cloud (VPC) für Nicht-EFS-Verkehr verwendet. Bei der Konfiguration lautet die Regel NON_COMPLIANT. AppNetworkAccessType ist nicht auf gesetzt. VpcOnly

Kennung: SAGEMAKER_DOMAIN_IN_VPC

Ressourcentypen: AWS::SageMaker::Domain

Auslösertyp: Konfigurationsänderungen

AWS-Region: Alle unterstützten AWS Regionen außer China (Peking), Asien-Pazifik (Thailand), Naher Osten (VAE), Asien-Pazifik (Hyderabad), Asien-Pazifik (Malaysia), Asien-Pazifik (Melbourne), AWS GovCloud (USA-Ost), AWS GovCloud (US-West), Mexiko (Zentral), Israel (Tel Aviv), Kanada West (Calgary), Europa (Spanien), China (Ningxia), Europa (Zürich)

Parameter:

Keine

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

sagemaker-domain-tagged

Prüft, ob SageMaker Amazon-Domains Tags haben. Optional können Sie Tag-Schlüssel angeben. Die Regel lautet NON_COMPLIANT, wenn keine Tags vorhanden sind oder wenn die angegebenen Tag-Schlüssel nicht vorhanden sind. Die Regel sucht nicht nach Tags, die mit 'aws: 'beginnen.

Kennung: SAGEMAKER_DOMAIN_TAGGED

Ressourcentypen: AWS::SageMaker::Domain

Auslösertyp: Konfigurationsänderungen

AWS-Region: Alle unterstützten AWS Regionen außer China (Peking), Asien-Pazifik (Thailand), Naher Osten (VAE), Asien-Pazifik (Hyderabad), Asien-Pazifik (Malaysia), Asien-Pazifik (Melbourne), AWS GovCloud (USA-Ost), AWS GovCloud (US-West), Mexiko (Zentral), Israel (Tel Aviv), Kanada West (Calgary), Europa (Spanien), China (Ningxia), Europa (Zürich)

Parameter:

requiredKeyTags (Fakultativ), Typ: CSV

Durch Kommas getrennte Liste von Tag-Schlüsseln, die von der Regel überprüft werden sollen. Falls angegeben, lautet die Regel NON_COMPLIANT, wenn die ausgewertete Ressource diese

Schlüssel nicht enthält. Bei Tag-Schlüsseln wird die Groß- und Kleinschreibung beachtet. Tag-Schlüssel, die mit „aws:“ beginnen, sind nicht erlaubt.

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

sagemaker-endpoint-configuration-kms-schlüsselkonfiguriert

Prüft, ob der AWS Key Management Service (AWS KMS) -Schlüssel für eine SageMaker Amazon-Endpunktkonfiguration konfiguriert ist. Die Regel lautet NON_COMPLIANT, wenn 'KmsKeyId' nicht für die SageMaker Amazon-Endpunktkonfiguration angegeben ist.

ID: SAGEMAKER_ENDPOINT_CONFIGURATION_KMS_KEY_CONFIGURED

Ressourcentypen: AWS::SageMaker::EndpointConfig

Auslösertyp: Regelmäßig

AWS-Region: Alle unterstützten AWS Regionen außer Asien-Pazifik (Thailand), Asien-Pazifik (Malaysia), Asien-Pazifik (Melbourne), Mexiko (Zentral), Asien-Pazifik (Taipeh)

Parameter:

kmsKeyArns (Fakultativ), Typ: Zeichenfolge

Durch Kommas getrennte Liste bestimmter AWS KMS-Schlüssel, die für eine SageMaker Amazon-Endpunktkonfiguration ARNs zulässig sind.

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

sagemaker-endpoint-config-prod-Instanzenanzahl

Prüft, ob Amazon SageMaker Amazon-Endpunktkonfigurationen die Produktionsvarianten InitialInstanceCount `` auf einen Wert größer als 1 gesetzt sind. Die Regel lautet NON_COMPLIANT, wenn die Produktionsvariante `InitialInstanceCount` gleich 1 ist.

Kennung: SAGEMAKER_ENDPOINT_CONFIG_PROD_INSTANCE_COUNT

Ressourcentypen: AWS::SageMaker::EndpointConfig

Auslösertyp: Regelmäßig

AWS-Region: Alle unterstützten AWS Regionen außer China (Peking), Asien-Pazifik (Thailand), Asien-Pazifik (Malaysia), Mexiko (Zentral), Kanada West (Calgary), China (Ningxia)

Parameter:

Keine

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

sagemaker-feature-group-tagged

Prüft, ob SageMaker Amazon-Feature-Gruppen Tags haben. Optional können Sie Tag-Schlüssel angeben. Die Regel lautet NON_COMPLIANT, wenn keine Tags vorhanden sind oder wenn die angegebenen Tag-Schlüssel nicht vorhanden sind. Die Regel sucht nicht nach Tags, die mit 'aws: 'beginnen.

Kennung: SAGEMAKER_FEATURE_GROUP_TAGGED

Ressourcentypen: AWS::SageMaker::FeatureGroup

Auslösertyp: Konfigurationsänderungen

AWS-Region: Alle unterstützten AWS Regionen außer China (Peking), Asien-Pazifik (Thailand), Naher Osten (VAE), Asien-Pazifik (Hyderabad), Asien-Pazifik (Malaysia), Asien-Pazifik (Melbourne), AWS GovCloud (USA-Ost), AWS GovCloud (US-West), Mexiko (Zentral), Kanada West (Calgary), China (Ningxia), Europa (Zürich)

Parameter:

requiredKeyTags (Fakultativ), Typ: CSV

> Durch Kommas getrennte Liste von Tag-Schlüsseln, die von der Regel überprüft werden sollen. Falls angegeben, lautet die Regel NON_COMPLIANT, wenn die ausgewertete Ressource diese

Schlüssel nicht enthält. Bei Tag-Schlüsseln wird die Groß- und Kleinschreibung beachtet. Tag-Schlüssel, die mit „aws:“ beginnen, sind nicht erlaubt.

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

sagemaker-image-description

Prüft, ob SageMaker Amazon-Bilder eine Beschreibung haben. Die Regel lautet NON_COMPLIANT, wenn sie konfiguriert ist. ImageDescription ist nicht vorhanden.

Kennung: SAGEMAKER_IMAGE_DESCRIPTION

Ressourcentypen: AWS::SageMaker::Image

Auslösertyp: Konfigurationsänderungen

AWS-Region: Alle unterstützten AWS Regionen außer China (Peking), Asien-Pazifik (Thailand), Asien-Pazifik (Hyderabad), Asien-Pazifik (Malaysia), Asien-Pazifik (Melbourne), AWS GovCloud (USA-Ost), AWS GovCloud (US-West), Mexiko (Zentral), Kanada West (Calgary), China (Ningxia), Europa (Zürich)

Parameter:

Keine

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

sagemaker-image-tagged

Prüft, ob SageMaker Amazon-Bilder Tags haben. Optional können Sie Tag-Schlüssel angeben. Die Regel lautet NON_COMPLIANT, wenn keine Tags vorhanden sind oder wenn die angegebenen Tag-Schlüssel nicht vorhanden sind. Die Regel sucht nicht nach Tags, die mit 'aws: 'beginnen.

Kennung: SAGEMAKER_IMAGE_TAGGED

Ressourcentypen: AWS::SageMaker::Image

Auslösertyp: Konfigurationsänderungen

AWS-Region: Alle unterstützten AWS Regionen außer China (Peking), Asien-Pazifik (Thailand), Asien-Pazifik (Hyderabad), Asien-Pazifik (Malaysia), Asien-Pazifik (Melbourne), AWS GovCloud (USA-Ost), AWS GovCloud (US-West), Mexiko (Zentral), Kanada West (Calgary), China (Ningxia), Europa (Zürich)

Parameter:

requiredKeyTags (Fakultativ), Typ: CSV

> Durch Kommas getrennte Liste von Tag-Schlüsseln, die von der Regel überprüft werden sollen. Falls angegeben, lautet die Regel NON_COMPLIANT, wenn die ausgewertete Ressource diese Schlüssel nicht enthält. Bei Tag-Schlüsseln wird die Groß- und Kleinschreibung beachtet. Tag-Schlüssel, die mit „aws:“ beginnen, sind nicht erlaubt.

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

sagemaker-model-in-vpc

Prüft, ob ein SageMaker Amazon-Modell eine Amazon Virtual Private Cloud (Amazon VPC) für den Containerverkehr verwendet. Die Regel lautet NON_COMPLIANT, wenn sie konfiguriert ist. VpcConfig existiert nicht.

Kennung: SAGEMAKER_MODEL_IN_VPC

Ressourcentypen: AWS::SageMaker::Model

Auslösertyp: Konfigurationsänderungen

AWS-Region: Alle unterstützten AWS Regionen außer China (Peking), Asien-Pazifik (Thailand), Naher Osten (VAE), Asien-Pazifik (Hyderabad), Asien-Pazifik (Malaysia), Asien-Pazifik (Melbourne), AWS GovCloud (USA-Ost), AWS GovCloud (US-West), Mexiko (Zentral), Israel (Tel Aviv), Kanada West (Calgary), Europa (Spanien), China (Ningxia), Europa (Zürich)

Parameter:

Keine

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

sagemaker-model-isolation-enabled

Prüft, ob bei einem SageMaker Amazon-Modell die Netzwerkisolierung aktiviert ist. Bei der Konfiguration lautet die Regel NON_COMPLIANT. EnableNetworkIsolation ist falsch.

Kennung: SAGEMAKER_MODEL_ISOLATION_ENABLED

Ressourcentypen: AWS::SageMaker::Model

Auslösertyp: Konfigurationsänderungen

AWS-Region: Alle unterstützten AWS Regionen außer China (Peking), Asien-Pazifik (Thailand), Naher Osten (VAE), Asien-Pazifik (Hyderabad), Asien-Pazifik (Malaysia), Asien-Pazifik (Melbourne), AWS GovCloud (USA-Ost), AWS GovCloud (US-West), Mexiko (Zentral), Israel (Tel Aviv), Kanada West (Calgary), Europa (Spanien), China (Ningxia), Europa (Zürich)

Parameter:

Keine

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

sagemaker-notebook-instance-inside-vpc

Prüft, ob eine SageMaker Amazon-Notebook-Instance innerhalb einer VPC oder innerhalb einer Liste zugelassener Subnetze gestartet wird. Die Regel ist NON_COMPLIANT, wenn eine Notebook-Instance nicht innerhalb einer VPC gestartet wird oder wenn ihre Subnetz-ID nicht in der Parameterliste enthalten ist.

ID: SAGEMAKER_NOTEBOOK_INSTANCE_INSIDE_VPC

Ressourcentypen: AWS::SageMaker::NotebookInstance

Auslösertyp: Konfigurationsänderungen

AWS-Region: Alle unterstützten AWS Regionen außer Asien-Pazifik (Thailand), Naher Osten (VAE), Asien-Pazifik (Hyderabad), Asien-Pazifik (Malaysia), Asien-Pazifik (Melbourne), AWS GovCloud (USA-Ost), AWS GovCloud (US-West), Mexiko (Zentral), Israel (Tel Aviv), Kanada West (Calgary), Europa (Spanien), Europa (Zürich)

Parameter:

SubnetIds (Fakultativ), Typ: CSV

> Durch Kommas getrennte Liste der Subnetze IDs , in denen Notebook-Instances gestartet werden können.

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

sagemaker-notebook-instance-kms-schlüsselkonfiguriert

Prüft, ob ein AWS Key Management Service (AWS KMS) -Schlüssel für eine SageMaker Amazon-Notebook-Instance konfiguriert ist. Die Regel lautet NON_COMPLIANT, wenn 'KmsKeyId' nicht für die SageMaker Notebook-Instance angegeben ist.

ID: SAGEMAKER_NOTEBOOK_INSTANCE_KMS_KEY_CONFIGURED

Ressourcentypen: AWS::SageMaker::NotebookInstance

Auslösertyp: Regelmäßig

AWS-Region: Alle unterstützten AWS Regionen außer Asien-Pazifik (Thailand), Asien-Pazifik (Malaysia), Asien-Pazifik (Melbourne), Mexiko (Zentral), Asien-Pazifik (Taipeh)

Parameter:

kmsKeyArns (Fakultativ), Typ: Zeichenfolge

> Durch Kommas getrennte Liste der AWS KMS-Schlüssel, die für eine SageMaker Amazon-Notebook-Instance ARNs zulässig sind.

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

sagemaker-notebook-instance-platform-Ausführung

Prüft, ob eine Sagemaker Notebook-Instanz für die Verwendung einer unterstützten Platform Identifier-Version konfiguriert ist. Die Regel lautet NON_COMPLIANT, wenn eine Notebook-Instanz nicht die angegebene unterstützte Platform Identifier-Version verwendet, wie im Parameter angegeben.

Kennung: SAGEMAKER_NOTEBOOK_INSTANCE_PLATFORM_VERSION

Ressourcentypen: AWS::SageMaker::NotebookInstance

Auslösertyp: Regelmäßig

AWS-Region: Alle unterstützten AWS Regionen außer Naher Osten (Bahrain), Asien-Pazifik (Thailand), Asien-Pazifik (Malaysia), Asien-Pazifik (Melbourne), Mexiko (Zentral) und Kanada West (Calgary)

Parameter:

supportedPlatformIdentifierVersionen, Typ: CSV

> Durch Kommas getrennte Liste der unterstützten Plattformkenner-Versionen, die von der Regel überprüft werden soll.

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

sagemaker-notebook-instance-root-Zugriffsprüfung

Prüft, ob die SageMaker RootAccess Amazon-Einstellung für SageMaker Amazon-Notebook-Instances aktiviert ist. Die Regel lautet NON_COMPLIANT, wenn die RootAccess Einstellung für eine SageMaker Amazon-Notebook-Instance auf „Aktiviert“ gesetzt ist.

ID: SAGEMAKER_NOTEBOOK_INSTANCE_ROOT_ACCESS_CHECK

Ressourcentypen: AWS::SageMaker::NotebookInstance

Auslösertyp: Konfigurationsänderungen

AWS-Region: Alle unterstützten AWS Regionen außer Asien-Pazifik (Thailand), Naher Osten (VAE), Asien-Pazifik (Hyderabad), Asien-Pazifik (Malaysia), Asien-Pazifik (Melbourne), AWS GovCloud (USA-Ost), AWS GovCloud (US-West), Mexiko (Zentral), Israel (Tel Aviv), Kanada West (Calgary), Europa (Spanien), Europa (Zürich)

Parameter:

Keine

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

sagemaker-notebook-no-direct-Internetzugang

Prüft, ob der direkte Internetzugang für eine Amazon SageMaker Notebook-Instance deaktiviert ist. Die Regel lautet NON_COMPLIANT, wenn eine SageMaker Notebook-Instance internetfähig ist.

ID: SAGEMAKER_NOTEBOOK_NO_DIRECT_INTERNET_ACCESS

Ressourcentypen: AWS::SageMaker::NotebookInstance

Auslösertyp: Regelmäßig

AWS-Region: Alle unterstützten AWS Regionen außer Asien-Pazifik (Thailand), Asien-Pazifik (Malaysia), Asien-Pazifik (Melbourne), Mexiko (Zentral), Asien-Pazifik (Taipeh)

Parameter:

Keine

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

secretsmanager-rotation-enabled-check

Prüft, ob für AWS Secrets Manager Secret die Rotation aktiviert ist. Die Regel prüft auch einen optionalen `maximumAllowedRotationFrequency`-Parameter. Wenn der Parameter angegeben wird, wird die Rotationshäufigkeit des Secrets mit der maximal zulässigen Häufigkeit verglichen. Die Regel ist „NON_COMPLIANT“, wenn das Secret nicht für die Rotation vorgesehen ist. Die Regel ist auch NON_COMPLIANT, wenn die Rotationsfrequenz höher als die im Parameter maximumAllowedRotation Frequenz angegebene Zahl ist.

> **Note**
>
> Ein erneute Auswertung dieser Regel innerhalb von 4 Stunden hat keine Auswirkungen auf die Ergebnisse.

ID: SECRETSMANAGER_ROTATION_ENABLED_CHECK

Ressourcentypen: AWS::SecretsManager::Secret

Auslösertyp: Konfigurationsänderungen

AWS-Region: Alle unterstützten AWS Regionen außer Mexiko (Zentral) und Asien-Pazifik (Taipeh)

Parameter:

maximumAllowedRotationFrequenz (optional), Typ: int

Maximal zulässige Rotationshäufigkeit des Secrets in Tagen.

maximumAllowedRotationFrequencyInHours (Fakultativ), Typ: int

Maximal zulässige Rotationshäufigkeit des Secrets in Stunden.

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unter AWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

secretsmanager-scheduled-rotation-success-überprüfen

Überprüft, ob AWS Secrets Manager Manager-Geheimnisse gemäß dem Rotationsplan erfolgreich rotiert wurden. Secrets Manager berechnet das Datum, an dem die Rotation stattfinden soll. Die Regel ist NON_COMPLIANT, wenn das Datum verstrichen ist und das Secret nicht rotiert wurde.

> **Note**
>
> Verzögerungen bei der Aufnahme
> Die Evaluierungsergebnisse für diese Regel können sich um bis zu 2 Tage verzögern, wenn der Rotationstermin nicht eingehalten wird. Eine direktere Überwachung finden Sie unter Monitor AWS Secrets Manager with Amazon CloudWatch im Secrets Manager Manager-Benutzerhandbuch.
> Geheimnisse ohne Rotation
> Die Regel kehrt `NOT_APPLICABLE` für Geheimnisse zurück, die nicht für die Rotation konfiguriert sind.

Identifier (Kennung): SECRETSMANAGER_SCHEDULED_ROTATION_SUCCESS_CHECK

Ressourcentypen: AWS::SecretsManager::Secret

Auslösertyp: Konfigurationsänderungen

AWS-Region: Alle unterstützten AWS Regionen außer Mexiko (Zentral) und Asien-Pazifik (Taipeh)

Parameter:

Keine

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

secretsmanager-secret-periodic-rotation

Prüft, ob AWS Secrets Manager-Geheimnisse in der letzten angegebenen Anzahl von Tagen rotiert wurden. Die Regel lautet NON_COMPLIANT, wenn ein Secret länger als die Anzahl der maxDaysSince Rotationstage nicht gewechselt wurde. Der Standardwert lautet 90 Tage.

ID: SECRETSMANAGER_SECRET_PERIODIC_ROTATION

Ressourcentypen: AWS::SecretsManager::Secret

Auslösertyp: Regelmäßig

AWS-Region: Alle unterstützten AWS Regionen außer Mexiko (Zentral) und Asien-Pazifik (Taipeh)

Parameter:

maxDaysSinceRotation (optional), Typ: int

Maximale Anzahl von Tagen, die ein Secret unverändert bleiben kann. Der Standardwert lautet 90 Tage.

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

secretsmanager-secret-unused

Prüft, ob innerhalb einer bestimmten Anzahl von Tagen auf AWS Secrets Manager-Geheimnisse zugegriffen wurde. Die Regel lautet NON_COMPLIANT, wenn innerhalb von 'unusedForDays' Tagen nicht auf ein Geheimnis zugegriffen wurde. Der Standardwert lautet 90 Tage.

Kontext: Es wird empfohlen, ungenutzte Secrets routinemäßig zu löschen. Unbenutzte Secrets können von ehemaligen Benutzern missbraucht werden, die keinen Zugriff mehr auf diese Geheimnisse benötigen. Je mehr Benutzer Zugriff auf ein Secret erhalten, desto wahrscheinlicher wird es außerdem, dass jemand ein Secret missbraucht oder einer nicht autorisierten Entität Zugriff gewährt hat. Durch das Löschen ungenutzter Secrets können Sie Benutzern, die sie nicht mehr benötigen, den Zugriff auf die Secrets entziehen und Ihre Kosten für die Nutzung von AWS Secrets Manager senken.

ID: SECRETSMANAGER_SECRET_UNUSED

Ressourcentypen: AWS::SecretsManager::Secret

Auslösertyp: Regelmäßig

AWS-Region: Alle unterstützten AWS Regionen außer Mexiko (Zentral) und Asien-Pazifik (Taipeh)

Parameter:

unusedForDays (Fakultativ), Typ: int

Anzahl von Tagen, die ein Secret ungenutzt bleiben kann. Der Standardwert lautet 90 Tage.

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

secretsmanager-using-cmk

Überprüft, ob alle Secrets in mit dem Von AWS verwalteter Schlüssel (`aws/secretsmanager`) oder einem vom Kunden verwalteten Schlüssel, der in AWS Key Management Service (AWS KMS) erstellt wurde, verschlüsselt AWS Secrets Manager sind. Die Regel ist COMPLIANT, wenn ein Secret mit einem kundenverwalteten Schlüssel verschlüsselt ist. Diese Regel ist NON_COMPLIANT, wenn ein Secret mit `aws/secretsmanager` verschlüsselt ist.

> **Note**
>
> Diese Regel hat keinen Zugriff auf kontoübergreifende, kundenverwaltete Schlüssel und bewertet Secrets als NON_COMPLIANT, wenn ein kontoübergreifender Schlüssel verwendet wird.

ID: SECRETSMANAGER_USING_CMK

Ressourcentypen: AWS::SecretsManager::Secret

Auslösertyp: Konfigurationsänderungen

AWS-Region: Alle unterstützten AWS Regionen außer der Region Asien-Pazifik (Taipeh)

Parameter:

kmsKeyArns (Fakultativ), Typ: CSV

Durch Kommas getrennte Liste der KMS-Schlüssel Amazon Resource Names (ARNs), um zu überprüfen, ob die Schlüssel bei der Verschlüsselung verwendet werden.

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

securityhub-enabled

Prüft, ob AWS Security Hub für ein AWS Konto aktiviert ist. Die Regel lautet NON_COMPLIANT, wenn AWS Security Hub nicht aktiviert ist.

Kennung: SECURITYHUB_ENABLED

Auslösertyp: Regelmäßig

AWS-Region: Alle unterstützten AWS Regionen außer der Region Asien-Pazifik (Taipeh)

Parameter:

Keine

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

security-account-information-provided

Überprüft, ob Sie Sicherheitskontaktinformationen für Ihre AWS Kontokontakte angegeben haben. Die Regel ist NON_COMPLIANT, wenn keine Sicherheitskontaktinformationen innerhalb des Kontos angegeben wurden.

ID: SECURITY_ACCOUNT_INFORMATION_PROVIDED

Ressourcentypen: AWS::::Account

Auslösertyp: Regelmäßig

AWS-Region: Alle unterstützten AWS Regionen außer Asien-Pazifik (Thailand), Asien-Pazifik (Malaysia), AWS GovCloud (USA-Ost), AWS GovCloud (US-West), Mexiko (Zentral), Kanada West (Calgary)

Parameter:

Keine

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

service-catalog-shared-within-Organisation

Prüft, ob AWS Service Catalog Portfolios an eine Organisation weitergibt (eine Sammlung von AWS Konten, die als eine Einheit behandelt werden), wenn die Integration mit AWS Organizations aktiviert ist. Die Regel ist NON_COMPLIANT, wenn der Wert `Type` einer Aktie `ACCOUNT` ist.

Kennung: SERVICE_CATALOG_SHARED_WITHIN_ORGANIZATION

Ressourcentypen: AWS::ServiceCatalog::Portfolio

Auslösertyp: Konfigurationsänderungen

AWS-Region: Alle unterstützten AWS Regionen außer China (Peking), Asien-Pazifik (Thailand), Asien-Pazifik (Jakarta), Asien-Pazifik (Malaysia), Mexiko (Zentral), Israel (Tel Aviv), Kanada West (Calgary), China (Ningxia)

Parameter:

Keine

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

service-vpc-endpoint-enabled

Prüft, ob für jede Amazon Virtual Private Cloud (Amazon VPC) ein Service-Endpunkt für den im Regelparameter angegebenen Service erstellt wurde. Die Regel ist NON_COMPLIANT, wenn für eine Amazon VPC kein Amazon-VPC-Endpunkt für den Service erstellt wurde.

Bezeichner: SERVICE_VPC_ENDPOINT_ENABLED

Ressourcentypen: AWS::EC2::VPC

Auslösertyp: Regelmäßig

AWS-Region: Alle unterstützten AWS Regionen

Parameter:

serviceName, Typ: Zeichenfolge

> Der Kurzname oder das Suffix für den Service. Hinweis: Um eine Liste verfügbarer Dienstnamen oder eine Liste gültiger Suffixe zu erhalten, verwenden Sie DescribeVpcEndpointServices.

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

ses-malware-scanning-enabled

Prüft, ob für Amazon Simple Email Service (Amazon SES) der Malware- und Spam-Scan für eingehende Nachrichten aktiviert ist. Die Regel ist NON_COMPLIANT, wenn der Malware- und Spam-Scan nicht aktiviert ist.

ID: SES_MALWARE_SCANNING_ENABLED

Ressourcentypen: AWS::SES::ReceiptRule

Auslösertyp: Regelmäßig

AWS-Region: Nur verfügbar in den Regionen Europa (Irland), USA Ost (Nord-Virginia) und USA West (Oregon)

Parameter:

Keine

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

shield-advanced-enabled-autorenew

Prüft, ob AWS Shield Advanced in Ihrem AWS Konto aktiviert ist und ob dieses Abonnement so eingestellt ist, dass es sich automatisch verlängert. Die Regel ist COMPLIANT, wenn Shield Advanced und die automatische Verlängerung aktiviert sind.

> **Note**
>
> Der API-Endpunkt von AWS Shield Advanced ist nur in der Region USA Ost (Nord-Virginia) verfügbar. Diese Regel sollte nur für die Ausführung in der Region USA Ost (Nord-Virginia) geplant werden.

ID: SHIELD_ADVANCED_ENABLED_AUTORENEW

Auslösertyp: Regelmäßig

AWS-Region: Nur in der Region USA Ost (Nord-Virginia) verfügbar

Parameter:

Keine

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

shield-drt-access

Prüft, ob das Shield Response Team (SRT) auf Ihr AWS Konto zugreifen kann. Die Regel ist NON_COMPLIANT, wenn sie aktiviert AWS Shield Advanced ist, aber die Rolle für den SRT-Zugriff nicht konfiguriert ist.

Identifier (Kennung): SHIELD_DRT_ACCESS

Auslösertyp: Regelmäßig

AWS-Region: Nur in der Region USA Ost (Nord-Virginia) verfügbar

Parameter:

Keine

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

sns-encrypted-kms

Überprüft, ob SNS-Themen mit dem AWS Key Management Service (AWS KMS) verschlüsselt sind. Die Regel lautet NON_COMPLIANT, wenn ein SNS-Thema nicht mit KMS verschlüsselt ist. AWS Geben Sie optional den Schlüssel ARNs, den Alias ARNs, den Aliasnamen oder den Schlüssel an, den die Regel IDs überprüfen soll.

Kennung: SNS_ENCRYPTED_KMS

Ressourcentypen: AWS::SNS::Topic

Auslösertyp: Konfigurationsänderungen

AWS-Region: Alle unterstützten AWS Regionen

Parameter:

kmsKeyIds (Fakultativ), Typ: CSV

> Durch Kommas getrennte Liste von AWS KMS-Schlüsseln, Amazon Resource Names (ARNs), KMS-Aliasnamen ARNs, KMS-Aliasnamen oder KMS-Schlüsseln IDs , die von der Regel überprüft werden sollen.

Proaktive Auswertung

Anweisungen zur Ausführung dieser Regel im proaktiven Modus finden Sie unter Evaluieren Ihrer Ressourcen mithilfe AWS Config von Regeln. Damit diese Regel im proaktiven Modus COMPLIANT zurückgibt, muss das Ressourcenkonfigurationsschema für die StartResourceEvaluationAPI die folgenden Eingaben enthalten, die als Zeichenfolge kodiert sind:

```
"ResourceConfiguration":
...
{
   "KmsMasterKeyId": "my-kms-key-Id"
```

```
}
...
```

Weitere Informationen zur proaktiven Auswertung finden Sie unter Auswertungsmodus.

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

sns-topic-message-delivery-Benachrichtigung aktiviert

Prüft, ob die Amazon Simple Notification Service (SNS)-Protokollierung des Status der Zustellung von Benachrichtigungen aktiviert ist, die an ein Thema für die Endpunkte gesendet werden. Die Regel ist NON_COMPLIANT, wenn die Benachrichtigung über den Status der Zustellung von Nachrichten nicht aktiviert ist.

ID: SNS_TOPIC_MESSAGE_DELIVERY_NOTIFICATION_ENABLED

Ressourcentypen: AWS::SNS::Topic

Auslösertyp: Konfigurationsänderungen

AWS-Region: Alle unterstützten AWS Regionen außer Asien-Pazifik (Thailand), Asien-Pazifik (Jakarta), Naher Osten (VAE), Asien-Pazifik (Hyderabad), Asien-Pazifik (Malaysia), Asien-Pazifik (Melbourne), AWS GovCloud (USA-Ost), AWS GovCloud (US-West), Mexiko (Zentral), Israel (Tel Aviv), Kanada West (Calgary), Europa (Spanien), Europa (Zürich)

Parameter:

Keine

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

sns-topic-no-public-Zugang

Prüft, ob die Richtlinie für den Zugriff auf SNS-Themen öffentlichen Zugriff zulässt. Die Regel lautet NON_COMPLIANT, wenn die Richtlinie für den Zugriff auf SNS-Themen öffentlichen Zugriff zulässt.

> **Note**
>
> Um als nicht öffentlich zu gelten, muss eine SNS-Richtlinie nur Zugriff auf feste Werte gewähren. Das bedeutet Werte, die keinen Platzhalter oder das folgende IAM-Richtlinienelement enthalten: Variablen.

Kennung: SNS_TOPIC_NO_PUBLIC_ACCESS

Ressourcentypen: AWS::SNS::Topic

Auslösertyp: Konfigurationsänderungen

AWS-Region: Alle unterstützten AWS Regionen außer Asien-Pazifik (Thailand), Asien-Pazifik (Malaysia), AWS GovCloud (USA-Ost), AWS GovCloud (US-West), Mexiko (Zentral), Kanada West (Calgary)

Parameter:

Keine

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

sqs-queue-no-public-Zugang

Prüft, ob die SQS-Warteschlangenzugriffsrichtlinie öffentlichen Zugriff zulässt. Die Regel lautet NON_COMPLIANT, wenn die SQS-Warteschlangenzugriffsrichtlinie öffentlichen Zugriff zulässt.

> **Note**
>
> Um als nicht öffentlich zu gelten, muss eine SQS-Richtlinie nur Zugriff auf feste Werte gewähren. Das bedeutet Werte, die keinen Platzhalter oder das folgende IAM-Richtlinienelement enthalten: Variablen.

Kennung: SQS_QUEUE_NO_PUBLIC_ACCESS

Ressourcentypen: AWS::SQS::Queue

Auslösertyp: Konfigurationsänderungen

AWS-Region: Alle unterstützten AWS Regionen außer Naher Osten (Bahrain), Asien-Pazifik (Thailand), Asien-Pazifik (Jakarta), Naher Osten (VAE), Asien-Pazifik (Hyderabad), Asien-Pazifik (Malaysia), Asien-Pazifik (Melbourne), AWS GovCloud (USA-Ost), AWS GovCloud (US-West), Mexiko (Zentral), Israel (Tel Aviv), Kanada West (Calgary), Europa (Spanien), Europa (Zürich)

Parameter:

Keine

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

ssm-automation-block-public-teilen

Überprüft, ob AWS Systems Manager Automation die Option Öffentliche Freigabe blockieren aktiviert hat. Die Regel lautet NON_COMPLIANT, wenn Systems Manager Automation die öffentliche Freigabe blockieren deaktiviert hat.

Kennung: SSM_AUTOMATION_BLOCK_PUBLIC_SHARING

Ressourcentypen: AWS::::Account

Auslösertyp: Regelmäßig

AWS-Region: Alle unterstützten AWS Regionen außer Asien-Pazifik (Thailand), Naher Osten (VAE), Asien-Pazifik (Hyderabad), Asien-Pazifik (Seoul), Asien-Pazifik (Malaysia), Asien-Pazifik (Melbourne), Mexiko (Zentral), Israel (Tel Aviv), Kanada West (Calgary), Europa (Spanien), Europa (Zürich)

Parameter:

Keine

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

ssm-automation-logging-enabled

Prüft, ob AWS Systems Manager Automation die CloudWatch Amazon-Protokollierung aktiviert hat. Die Regel gibt NON_COMPLIANT zurück, wenn Systems Manager Automation die CloudWatch Protokollierung nicht aktiviert hat.

Kennung: SSM_AUTOMATION_LOGGING_ENABLED

Ressourcentypen: AWS::::Account

Auslösertyp: Regelmäßig

AWS-Region: Alle unterstützten AWS Regionen außer Asien-Pazifik (Thailand), Naher Osten (VAE), Asien-Pazifik (Hyderabad), Asien-Pazifik (Seoul), Asien-Pazifik (Malaysia), Mexiko (Zentral), Israel (Tel Aviv), Kanada West (Calgary), Europa (Spanien), Europa (Zürich)

Parameter:

Keine

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

ssm-document-not-public

Überprüft, ob AWS Systems Manager Manager-Dokumente, die dem Konto gehören, öffentlich sind. Die Regel ist NON_COMPLIANT, wenn Systems-Manager-Dokumente mit dem Besitzertyp „Selbst“ öffentlich sind.

ID: SSM_DOCUMENT_NOT_PUBLIC

Ressourcentypen: AWS::SSM::Document

Auslösertyp: Regelmäßig

AWS-Region: Alle unterstützten AWS Regionen außer Asien-Pazifik (Taipeh) und Kanada West (Calgary)

Parameter:

Keine

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

ssm-document-tagged

Überprüft, ob AWS Systems Manager Manager-Dokumente Tags haben. Optional können Sie Tag-Schlüssel angeben. Die Regel lautet NON_COMPLIANT, wenn keine Tags vorhanden sind oder wenn die angegebenen Tag-Schlüssel nicht vorhanden sind. Die Regel sucht nicht nach Tags, die mit 'aws: 'beginnen.

Kennung: SSM_DOCUMENT_TAGGED

Ressourcentypen: AWS::SSM::Document

Auslösertyp: Konfigurationsänderungen

AWS-Region: Alle unterstützten AWS Regionen außer China (Peking), Asien-Pazifik (Thailand), Asien-Pazifik (Malaysia), AWS GovCloud (USA-Ost), AWS GovCloud (US-West), Mexiko (Zentral), China (Ningxia)

Parameter:

requiredKeyTags (Fakultativ), Typ: CSV

> Durch Kommas getrennte Liste von Tag-Schlüsseln, die von der Regel überprüft werden sollen. Falls angegeben, lautet die Regel NON_COMPLIANT, wenn die ausgewertete Ressource diese Schlüssel nicht enthält. Bei Tag-Schlüsseln wird die Groß- und Kleinschreibung beachtet. Tag-Schlüssel, die mit „aws:“ beginnen, sind nicht erlaubt.

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

step-functions-state-machine-Protokollierung aktiviert

Prüft, ob auf der AWS Step Functions Functions-Maschine die Protokollierung aktiviert ist. Die Regel ist NON_COMPLIANT, wenn für eine Zustandsmaschine die Protokollierung nicht aktiviert ist oder die Protokollierungskonfiguration nicht auf dem angegebenen Mindestniveau liegt.

ID: STEP_FUNCTIONS_STATE_MACHINE_LOGGING_ENABLED

Ressourcentypen: AWS::StepFunctions::StateMachine

Auslösertyp: Konfigurationsänderungen

AWS-Region: Alle unterstützten AWS Regionen außer Asien-Pazifik (Thailand), Asien-Pazifik (Malaysia), Asien-Pazifik (Melbourne), AWS GovCloud (USA-Ost), AWS GovCloud (US-West), Mexiko (Zentral), Israel (Tel Aviv), Kanada West (Calgary)

Parameter:

cloudWatchLogGroupArns (Fakultativ), Typ: CSV

Durch Kommas getrennte Liste von Amazon-Ressourcennamen (ARNs) für Amazon CloudWatch Logs-Protokollgruppen. Die Regel prüft, ob die angegebenen Protokollgruppen für die Protokolle Ihrer Zustandsmaschine konfiguriert sind.

logLevel (optional), Typ: Zeichenfolge

Die Mindestprotokollebene für Ihre Zustandsmaschine. Zu den zulässigen Werten gehören: ALL, ERROR, FATAL.

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

storagegateway-last-backup-recovery-Punkt-erstellt

Überprüft, ob ein Wiederherstellungspunkt für AWS Storage Gateway Gateway-Volumes erstellt wurde. Die Regel ist NON_COMPLIANT, wenn innerhalb des angegebenen Zeitraums kein entsprechender Wiederherstellungspunkt für das Storage Gateway erstellt wurde.

ID: STORAGEGATEWAY_LAST_BACKUP_RECOVERY_POINT_CREATED

Ressourcentypen: AWS::StorageGateway::Volume

Auslösertyp: Regelmäßig

AWS-Region: Alle unterstützten AWS Regionen außer China (Peking), Asien-Pazifik (Thailand), Asien-Pazifik (Malaysia), Mexiko (Zentral), Israel (Tel Aviv), Kanada West (Calgary), China (Ningxia)

Parameter:

resourceTags (optional), Typ: Zeichenfolge

Tags von Storage-Gateway-Volumes, die von der Regel geprüft werden sollen, im JSON-Format `{"tagkey" : "tagValue"}`.

resourceId (optional), Typ: Zeichenfolge

ID des Storage-Gateway-Volumes, das von der Regel geprüft werden soll.

recoveryPointAgeWert (optional), Typ: int, Standard: 1

Numerischer Wert für das zulässige Höchstalter. Nicht mehr als 744 für Stunden oder 31 für Tage.

recoveryPointAgeEinheit (optional), Typ: Zeichenfolge, Standard: days

Zeiteinheit für das zulässige Höchstalter. Zulässige Werte: „Stunden“, „Tage“.

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

storagegateway-resources-in-logically-air-gapped-vault

Überprüft, ob sich AWS Storage Gateway Gateway-Volumes in einem Tresor mit logischem Air-Gap befinden. Die Regel lautet NON_COMPLIANT, wenn sich ein AWS Storage Gateway Gateway-Volume innerhalb des angegebenen Zeitraums nicht in einem Tresor mit logischem Air-Gap befindet.

Kennung: STORAGEGATEWAY_RESOURCES_IN_LOGICALLY_AIR_GAPPED_VAULT

Ressourcentypen: AWS::StorageGateway::Volume

Auslösertyp: Regelmäßig

AWS-Region: Alle unterstützten AWS Regionen außer China (Peking), Asien-Pazifik (Thailand), Asien-Pazifik (Malaysia), AWS GovCloud (USA-Ost), AWS GovCloud (US-West), Mexiko (Zentral), Israel (Tel Aviv), Kanada West (Calgary), China (Ningxia)

Parameter:

resourceTags (optional), Typ: Zeichenfolge

Tags von Storage Gateway Gateway-Volumes, die von der Regel überprüft werden sollen, im JSON-Format.

resourceId (optional), Typ: Zeichenfolge

ID des Storage-Gateway-Volumes, das von der Regel geprüft werden soll.

recoveryPointAgeWert (optional), Typ: int, Standard: 1

Numerischer Wert für das zulässige Höchstalter. Nicht mehr als 2184 für Stunden, 91 für Tage.

recoveryPointAgeEinheit (optional), Typ: Zeichenfolge, Standard: days

Zeiteinheit für das zulässige Höchstalter. Zulässige Werte: „Stunden“, „Tage“.

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

storagegateway-resources-protected-by-Backup-Plan

Überprüft, ob AWS Storage Gateway Gateway-Volumes durch einen Backup-Plan geschützt sind. Die Regel ist NON_COMPLIANT, wenn das Storage-Gateway-Volume nicht durch einen Backup-Plan gedeckt ist.

ID: STORAGEGATEWAY_RESOURCES_PROTECTED_BY_BACKUP_PLAN

Ressourcentypen: AWS::StorageGateway::Volume

Auslösertyp: Regelmäßig

AWS-Region: Alle unterstützten AWS Regionen außer China (Peking), Asien-Pazifik (Thailand), Asien-Pazifik (Malaysia), Mexiko (Zentral), Israel (Tel Aviv), Kanada West (Calgary), China (Ningxia)

Parameter:

resourceTags (optional), Typ: Zeichenfolge

Tags für Storage-Gateway-Volumes, die von der Regel überprüft werden sollen, im JSON-Format.

resourceId (optional), Typ: Zeichenfolge

ID des Storage-Gateway-Volumes, das von der Regel geprüft werden soll.

crossRegionList (Fakultativ), Typ: Zeichenfolge

Durch Kommata getrennte Liste der Zielregionen, für die die regionsübergreifende Backup-Kopie aufbewahrt werden soll.

crossAccountList (Fakultativ), Typ: Zeichenfolge

Durch Kommata getrennte Liste der Zielkonten, für die die kontoübergreifende Backup-Kopie aufbewahrt werden soll.

maxRetentionDays (Fakultativ), Typ: int

Die maximale Aufbewahrungsdauer in Tagen für die Backup-Tresorsperre.

minRetentionDays (Fakultativ), Typ: int

Die Mindestaufbewahrungsdauer in Tagen für die Backup-Tresorsperre.

backupVaultLockÜberprüfen Sie (fakultativ), Typ: Zeichenfolge

Akzeptierte Werte: „True“ oder „False“. Geben Sie „True“ ein, damit die Regel prüft, ob die Ressource in einem gesperrten Tresor gesichert ist.

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

subnet-auto-assign-public-ip-deaktiviert

Prüft, ob den Subnetzen von Amazon Virtual Private Cloud (Amazon VPC) eine öffentliche IP-Adresse zugewiesen wurde. Die Regel ist COMPLIANT, wenn Amazon VPC keine Subnetze hat, denen eine öffentliche IP-Adresse zugewiesen wurde. Die Regel ist NON_COMPLIANT, wenn Amazon VPC Subnetze hat, denen eine öffentliche IP-Adresse zugewiesen wurde.

ID: SUBNET_AUTO_ASSIGN_PUBLIC_IP_DISABLED

Ressourcentypen: AWS::EC2::Subnet

Auslösertyp: Konfigurationsänderungen

AWS-Region: Alle unterstützten AWS Regionen

Parameter:

Keine

Proaktive Auswertung

Anweisungen zur Ausführung dieser Regel im proaktiven Modus finden Sie unter Evaluieren Ihrer Ressourcen mithilfe von AWS Config Regeln. Damit diese Regel im proaktiven Modus COMPLIANT zurückgibt, muss das Ressourcenkonfigurationsschema für die StartResourceEvaluationAPI die folgenden Eingaben enthalten, die als Zeichenfolge kodiert sind:

```
"ResourceConfiguration":
...
{
   "MapPublicIpOnLaunch": BOOLEAN
}
...
```

Weitere Informationen zur proaktiven Auswertung finden Sie unter Auswertungsmodus.

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

transfer-agreement-description

Prüft, ob AWS Transfer Family Agreements eine Beschreibung haben. Die Regel ist NON_COMPLIANT, wenn Configuration.Description nicht existiert.

Kennung: TRANSFER_AGREEMENT_DESCRIPTION

Ressourcentypen: AWS::Transfer::Agreement

Auslösertyp: Konfigurationsänderungen

AWS-Region: Alle unterstützten AWS Regionen außer China (Peking), Asien-Pazifik (Thailand), Asien-Pazifik (Hyderabad), Asien-Pazifik (Malaysia), Asien-Pazifik (Melbourne), AWS GovCloud (USA-Ost), AWS GovCloud (US-West), Mexiko (Zentral), Israel (Tel Aviv), Kanada West (Calgary), Europa (Spanien), China (Ningxia), Europa (Zürich)

Parameter:

Keine

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

transfer-agreement-tagged

Prüft, ob AWS Transfer Family Family-Verträge mit Tags versehen sind. Optional können Sie Tag-Schlüssel angeben. Die Regel lautet NON_COMPLIANT, wenn keine Tags vorhanden sind oder wenn die angegebenen Tag-Schlüssel nicht vorhanden sind. Die Regel sucht nicht nach Tags, die mit 'aws: 'beginnen.

Kennung: TRANSFER_AGREEMENT_TAGGED

Ressourcentypen: AWS::Transfer::Agreement

Auslösertyp: Konfigurationsänderungen

AWS-Region: Alle unterstützten AWS Regionen außer China (Peking), Asien-Pazifik (Thailand), Asien-Pazifik (Hyderabad), Asien-Pazifik (Malaysia), Asien-Pazifik (Melbourne), AWS GovCloud (USA-Ost), AWS GovCloud (US-West), Mexiko (Zentral), Israel (Tel Aviv), Kanada West (Calgary), Europa (Spanien), China (Ningxia), Europa (Zürich)

Parameter:

requiredKeyTags (Fakultativ), Typ: CSV

> Durch Kommas getrennte Liste von Tag-Schlüsseln, die von der Regel überprüft werden sollen. Falls angegeben, lautet die Regel NON_COMPLIANT, wenn die ausgewertete Ressource diese Schlüssel nicht enthält. Bei Tag-Schlüsseln wird die Groß- und Kleinschreibung beachtet. Tag-Schlüssel, die mit „aws:“ beginnen, sind nicht erlaubt.

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

transfer-certificate-description

Prüft, ob AWS Transfer Family Family-Zertifikate eine Beschreibung haben. Die Regel ist NON_COMPLIANT, wenn Configuration.Description nicht existiert.

Kennung: TRANSFER_CERTIFICATE_DESCRIPTION

Ressourcentypen: AWS::Transfer::Certificate

Auslösertyp: Konfigurationsänderungen

AWS-Region: Alle unterstützten AWS Regionen außer China (Peking), Asien-Pazifik (Thailand), Asien-Pazifik (Malaysia), AWS GovCloud (USA-Ost), AWS GovCloud (US-West), Mexiko (Zentral), China (Ningxia)

Parameter:

Keine

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

transfer-certificate-tagged

Überprüft, ob AWS Transfer Family Family-Zertifikate Tags haben. Optional können Sie Tag-Schlüssel angeben. Die Regel lautet NON_COMPLIANT, wenn keine Tags vorhanden sind oder wenn die angegebenen Tag-Schlüssel nicht vorhanden sind. Die Regel sucht nicht nach Tags, die mit 'aws: 'beginnen.

Kennung: TRANSFER_CERTIFICATE_TAGGED

Ressourcentypen: AWS::Transfer::Certificate

Auslösertyp: Konfigurationsänderungen

AWS-Region: Alle unterstützten AWS Regionen außer China (Peking), Asien-Pazifik (Thailand), Asien-Pazifik (Malaysia), AWS GovCloud (USA-Ost), AWS GovCloud (US-West), Mexiko (Zentral), China (Ningxia)

Parameter:

requiredKeyTags (Fakultativ), Typ: CSV

Durch Kommas getrennte Liste von Tag-Schlüsseln, die von der Regel überprüft werden sollen. Falls angegeben, lautet die Regel NON_COMPLIANT, wenn die ausgewertete Ressource diese

Schlüssel nicht enthält. Bei Tag-Schlüsseln wird die Groß- und Kleinschreibung beachtet. Tag-Schlüssel, die mit „aws:“ beginnen, sind nicht erlaubt.

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

transfer-connector-logging-enabled

Überprüft, ob AWS Transfer Family Connector Protokolle an Amazon veröffentlicht CloudWatch. Die Regel lautet NON_COMPLIANT, wenn einem Connector kein Connector zugewiesen wurde. LoggingRole

Kennung: TRANSFER_CONNECTOR_LOGGING_ENABLED

Ressourcentypen: AWS::Transfer::Connector

Auslösertyp: Konfigurationsänderungen

AWS-Region: Alle unterstützten AWS Regionen außer Naher Osten (Bahrain), Asien-Pazifik (Thailand), Asien-Pazifik (Hyderabad), Asien-Pazifik (Malaysia), Asien-Pazifik (Melbourne), Mexiko (Zentral), Israel (Tel Aviv), Kanada West (Calgary), Europa (Spanien), Europa (Zürich)

Parameter:

Keine

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

transfer-connector-tagged

Überprüft, ob die Steckverbinder der AWS Transfer Family über Tags verfügen. Optional können Sie Tag-Schlüssel angeben. Die Regel lautet NON_COMPLIANT, wenn keine Tags vorhanden sind oder wenn die angegebenen Tag-Schlüssel nicht vorhanden sind. Die Regel sucht nicht nach Tags, die mit 'aws: 'beginnen.

Kennung: TRANSFER_CONNECTOR_TAGGED

Ressourcentypen: AWS::Transfer::Connector

Auslösertyp: Konfigurationsänderungen

AWS-Region: Alle unterstützten AWS Regionen außer China (Peking), Asien-Pazifik (Thailand), Asien-Pazifik (Malaysia), AWS GovCloud (USA-Ost), AWS GovCloud (US-West), Mexiko (Zentral), China (Ningxia)

Parameter:

requiredKeyTags (Fakultativ), Typ: CSV

> Durch Kommas getrennte Liste von Tag-Schlüsseln, die von der Regel überprüft werden sollen. Falls angegeben, lautet die Regel NON_COMPLIANT, wenn die ausgewertete Ressource diese Schlüssel nicht enthält. Bei Tag-Schlüsseln wird die Groß- und Kleinschreibung beachtet. Tag-Schlüssel, die mit „aws:“ beginnen, sind nicht erlaubt.

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

transfer-family-server-no-ftp

Überprüft, ob ein mit AWS Transfer Family erstellter Server FTP für die Endpunktverbindung verwendet. Die Regel lautet NON_COMPLIANT, wenn das Serverprotokoll für die Endpunktverbindung FTP-fähig ist.

Kennung: TRANSFER_FAMILY_SERVER_NO_FTP

Ressourcentypen: AWS::Transfer::Server

Auslösertyp: Regelmäßig

AWS-Region: Alle unterstützten AWS Regionen außer China (Peking), Asien-Pazifik (Thailand), Asien-Pazifik (Malaysia), Mexiko (Zentral), Kanada West (Calgary), China (Ningxia)

Parameter:

Keine

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

transfer-profile-tagged

Prüft, ob die Profile von AWS Transfer Family Tags haben. Optional können Sie Tag-Schlüssel angeben. Die Regel lautet NON_COMPLIANT, wenn keine Tags vorhanden sind oder wenn die angegebenen Tag-Schlüssel nicht vorhanden sind. Die Regel sucht nicht nach Tags, die mit 'aws: 'beginnen.

Kennung: TRANSFER_PROFILE_TAGGED

Ressourcentypen: AWS::Transfer::Profile

Auslösertyp: Konfigurationsänderungen

AWS-Region: Alle unterstützten AWS Regionen außer China (Peking), Asien-Pazifik (Thailand), Asien-Pazifik (Malaysia), AWS GovCloud (USA-Ost), AWS GovCloud (US-West), Mexiko (Zentral), China (Ningxia)

Parameter:

requiredKeyTags (Fakultativ), Typ: CSV

> Durch Kommas getrennte Liste von Tag-Schlüsseln, die von der Regel überprüft werden sollen. Falls angegeben, lautet die Regel NON_COMPLIANT, wenn die ausgewertete Ressource diese Schlüssel nicht enthält. Bei Tag-Schlüsseln wird die Groß- und Kleinschreibung beachtet. Tag-Schlüssel, die mit „aws:“ beginnen, sind nicht erlaubt.

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

transfer-workflow-description

Prüft, ob die Workflows zum AWS Transfer Family eine Beschreibung haben. Die Regel ist NON_COMPLIANT, wenn Configuration.Description nicht existiert oder eine leere Zeichenfolge ist.

Kennung: TRANSFER_WORKFLOW_DESCRIPTION

Ressourcentypen: AWS::Transfer::Workflow

Auslösertyp: Konfigurationsänderungen

AWS-Region: Alle unterstützten AWS Regionen außer China (Peking), Asien-Pazifik (Thailand), Asien-Pazifik (Malaysia), AWS GovCloud (USA-Ost), AWS GovCloud (US-West), Mexiko (Zentral), China (Ningxia)

Parameter:

Keine

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

transfer-workflow-tagged

Überprüft, ob die Workflows zum AWS Transfer Family Tags enthalten. Optional können Sie Tag-Schlüssel angeben. Die Regel lautet NON_COMPLIANT, wenn keine Tags vorhanden sind oder wenn die angegebenen Tag-Schlüssel nicht vorhanden sind. Die Regel sucht nicht nach Tags, die mit 'aws: 'beginnen.

Kennung: TRANSFER_WORKFLOW_TAGGED

Ressourcentypen: AWS::Transfer::Workflow

Auslösertyp: Konfigurationsänderungen

AWS-Region: Alle unterstützten AWS Regionen außer China (Peking), Asien-Pazifik (Thailand), Asien-Pazifik (Malaysia), AWS GovCloud (USA-Ost), AWS GovCloud (US-West), Mexiko (Zentral), China (Ningxia)

Parameter:

requiredKeyTags (Fakultativ), Typ: CSV

> Durch Kommas getrennte Liste von Tag-Schlüsseln, die von der Regel überprüft werden sollen. Falls angegeben, lautet die Regel NON_COMPLIANT, wenn die ausgewertete Ressource diese Schlüssel nicht enthält. Bei Tag-Schlüsseln wird die Groß- und Kleinschreibung beachtet. Tag-Schlüssel, die mit „aws:“ beginnen, sind nicht erlaubt.

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

virtualmachine-last-backup-recovery-Punkt-erstellt

Prüft, ob ein Recovery Point für AWS VirtualMachines Backup-Gateway erstellt wurde. Die Regel lautet NON_COMPLIANT, wenn für ein AWS Backup-Gateway innerhalb des angegebenen Zeitraums VirtualMachines kein entsprechender Recovery Point erstellt wurde.

ID: VIRTUALMACHINE_LAST_BACKUP_RECOVERY_POINT_CREATED

Ressourcentypen: AWS::BackupGateway::VirtualMachine

Auslösertyp: Regelmäßig

AWS-Region: Alle unterstützten AWS Regionen außer China (Peking), Asien-Pazifik (Thailand), Asien-Pazifik (Jakarta), Naher Osten (VAE), Asien-Pazifik (Hyderabad), Asien-Pazifik (Malaysia), Asien-Pazifik (Melbourne), Mexiko (Zentral), Israel (Tel Aviv), Kanada West (Calgary), Europa (Spanien), China (Ningxia), Europa (Zürich)

Parameter:

resourceTags (optional), Typ: Zeichenfolge

Tags des AWS Backup-Gateways VirtualMachines für die zu prüfende Regel im JSON-Format. `{"tagkey" : "tagValue"}`

resourceId (optional), Typ: Zeichenfolge

ID des AWS Backup-Gateways VirtualMachine für die zu prüfende Regel.

recoveryPointAgeWert (optional), Typ: int, Standard: 1

Numerischer Wert für das zulässige Höchstalter. Nicht mehr als 744 für Stunden oder 31 für Tage.

recoveryPointAgeEinheit (optional), Typ: Zeichenfolge, Standard: days

Zeiteinheit für das zulässige Höchstalter. Zulässige Werte: „Stunden“, „Tage“.

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

virtualmachine-resources-in-logically-air-gapped-vault

Prüft, ob sich das AWS Backup-Gateway in einem VirtualMachines Tresor mit logischem Air-Gap befindet. Die Regel lautet NON_COMPLIANT, wenn sich ein AWS Backup-Gateway innerhalb des angegebenen VirtualMachines Zeitraums nicht in einem Tresor mit logischem Air-Gap befindet.

Kennung: VIRTUALMACHINE_RESOURCES_IN_LOGICALLY_AIR_GAPPED_VAULT

Ressourcentypen: AWS::BackupGateway::VirtualMachine

Auslösertyp: Regelmäßig

AWS-Region: Alle unterstützten AWS Regionen außer China (Peking), Asien-Pazifik (Thailand), Asien-Pazifik (Jakarta), Naher Osten (VAE), Asien-Pazifik (Hyderabad), Asien-Pazifik (Malaysia), Asien-Pazifik (Melbourne), AWS GovCloud (US-Ost), AWS GovCloud (US-West), Mexiko (Zentral), Israel (Tel Aviv), Kanada West (Calgary), Europa (Spanien), China (Ningxia), Europa (Zürich)

Parameter:

resourceTags (optional), Typ: Zeichenfolge

Tags des AWS Backup-Gateways VirtualMachines für die zu prüfende Regel im JSON-Format.

resourceId (optional), Typ: Zeichenfolge

ID des AWS Backup-Gateways VirtualMachine für die zu prüfende Regel.

recoveryPointAgeWert (optional), Typ: int, Standard: 1

Numerischer Wert für das zulässige Höchstalter. Nicht mehr als 2184 für Stunden, 91 für Tage.

recoveryPointAgeEinheit (optional), Typ: Zeichenfolge, Standard: days

Zeiteinheit für das zulässige Höchstalter. Zulässige Werte: „Stunden“, „Tage“.

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

virtualmachine-resources-protected-by-Backup-Plan

Prüft, ob AWS Backup-Gateway VirtualMachines durch einen Backup-Plan geschützt ist. Die Regel lautet NON_COMPLIANT, wenn das Backup-Gateway nicht durch einen Backup-Plan abgedeckt VirtualMachine ist.

ID: VIRTUALMACHINE_RESOURCES_PROTECTED_BY_BACKUP_PLAN

Ressourcentypen: AWS::BackupGateway::VirtualMachine

Auslösertyp: Regelmäßig

AWS-Region: Alle unterstützten AWS Regionen außer China (Peking), Asien-Pazifik (Thailand), Asien-Pazifik (Jakarta), Naher Osten (VAE), Asien-Pazifik (Hyderabad), Asien-Pazifik (Malaysia), Asien-Pazifik (Melbourne), Mexiko (Zentral), Israel (Tel Aviv), Kanada West (Calgary), Europa (Spanien), China (Ningxia), Europa (Zürich)

Parameter:

resourceTags (optional), Typ: Zeichenfolge

Tags für AWS Backup-Gateway VirtualMachines für die zu prüfende Regel, im JSON-Format. `{"tagkey" : "tagValue"}`

resourceId (optional), Typ: Zeichenfolge

ID des AWS Backup-Gateways VirtualMachine für die zu prüfende Regel.

crossRegionList (Fakultativ), Typ: Zeichenfolge

Durch Kommata getrennte Liste der Zielregionen, für die die regionsübergreifende Backup-Kopie aufbewahrt werden soll.

crossAccountList (Fakultativ), Typ: Zeichenfolge

Durch Kommata getrennte Liste der Zielkonten, für die die kontoübergreifende Backup-Kopie aufbewahrt werden soll.

maxRetentionDays (Fakultativ), Typ: int

Die maximale Aufbewahrungsdauer in Tagen für die Backup-Tresorsperre.

minRetentionDays (Fakultativ), Typ: int

Die Mindestaufbewahrungsdauer in Tagen für die Backup-Tresorsperre.

backupVaultLockÜberprüfen Sie (fakultativ), Typ: Zeichenfolge

Akzeptierte Werte: „True“ oder „False“. Geben Sie „True“ ein, damit die Regel prüft, ob die Ressource in einem gesperrten Tresor gesichert ist.

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

vpc-default-security-group-geschlossen

Prüft, ob die standardmäßige Sicherheitsgruppe einer beliebigen Amazon Virtual Private Cloud (Amazon VPC) eingehenden oder ausgehenden Datenverkehr unterbindet. Die Regel ist NON_COMPLIANT, wenn bei der standardmäßigen Sicherheitsgruppe einer oder mehrere Regeln für eingehenden oder ausgehenden Datenverkehr erkannt werden.

> **Note**
>
> Zwischen dem Zeitpunkt, an dem das Löschen verwandter Ressourcen AWS Config aufgezeichnet wird, wie z. B. Standardsicherheitsgruppen, die im Rahmen der Amazon VPC-Löschung gelöscht werden, kann es zu einer Verzögerung kommen. Daher ist es möglich, dass die Regel, selbst wenn alle Standardsicherheitsgruppen oder andere zugehörige Ressourcen gelöscht oder korrigiert wurden, bis zum nächsten Konto-Baselining-Prozess den Wert NON_COMPLIANT meldet.

ID: VPC_DEFAULT_SECURITY_GROUP_CLOSED

Ressourcentypen: AWS::EC2::SecurityGroup

Auslösertyp: Konfigurationsänderungen

AWS-Region: Alle unterstützten AWS Regionen

Parameter:

Keine

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

vpc-endpoint-enabled

Prüft, ob jeder im Parameter angegebene Service über einen Amazon VPC-Endpunkt verfügt. Die Regel lautet NON_COMPLIANT, wenn Amazon VPC nicht über einen VPC-Endpunkt verfügt, der für jeden angegebenen Service erstellt wurde. Optional können Sie bestimmte VPCs Werte angeben, die von der Regel überprüft werden sollen.

Kennung: VPC_ENDPOINT_ENABLED

Ressourcentypen: AWS::EC2::VPC

Auslösertyp: Regelmäßig

AWS-Region: Alle unterstützten AWS Regionen außer Asien-Pazifik (Thailand), Asien-Pazifik (Osaka), Asien-Pazifik (Malaysia), Mexiko (Zentral), Israel (Tel Aviv) und Kanada West (Calgary)

Parameter:

Namen der Dienste, Typ: CSV

Durch Kommas getrennte Liste von Dienstnamen oder Endpunkten. Beispiel: „access-analyzer, appconfig, cloudtrail“ oder „com.amazonaws.region.access-analyzer“. DescribeVpcEndpointServices Für verfügbare Namen verwenden.

vpcIds (optional), Typ: CSV

Durch Kommas getrennte Liste von Amazon VPC IDs für VPC-Endpoints. Falls angegeben, lautet die Regel NON_COMPLIANT, wenn die im Parameter ServiceName angegebenen Dienste keinen dieser VPC-Endpunkte haben.

scopeConfigResourceTypen (optional), Typ: CSV

Durch Kommas getrennte Liste der AWS Config-Ressourcentypen, die von der Regel überprüft werden sollen. Falls angegeben, gibt die Regel nur dann einen Konformitätsstatus zurück, wenn mindestens eine angegebene Ressource im Konto erfasst ist. Zum Beispiel: "AWS::SNS::Topic“.

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

vpc-flow-logs-enabled

Überprüft, ob Amazon Virtual Private Cloud (Amazon VPC) Flow-Logs gefunden und für alle Amazon VPCs aktiviert wurden. Die Regel ist NON_COMPLIANT, wenn nicht für mindestens eine Amazon VPC Flow-Logs aktiviert sind.

ID: VPC_FLOW_LOGS_ENABLED

Ressourcentypen: AWS::EC2::VPC

Auslösertyp: Regelmäßig

AWS-Region: Alle unterstützten AWS Regionen

Parameter:

trafficType (optional), Typ: Zeichenfolge

TrafficType von Flow-Logs

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

vpc-network-acl-unused-überprüfen

Prüft, ob unbenutzte Netzwerkzugriffskontrolllisten (Netzwerk ACLs) vorhanden sind. Die Regel ist COMPLIANT, wenn jeder Netzwerk-ACL einem Subnetz zugeordnet ist. Die Regel ist NON_COMPLIANT, wenn eine Netzwerk-ACL keinem Subnetz zugeordnet ist.

ID: VPC_NETWORK_ACL_UNUSED_CHECK

Ressourcentypen: AWS::EC2::NetworkAcl

Auslösertyp: Konfigurationsänderungen

AWS-Region: Alle unterstützten AWS Regionen

Parameter:

Keine

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

vpc-peering-dns-resolution-überprüfen

Überprüft, ob die DNS-Auflösung von accepter/requester VPC zu privater IP aktiviert ist. Die Regel lautet NON_COMPLIANT, wenn die DNS-Auflösung von accepter/requester VPC zu privater IP nicht aktiviert ist.

ID: VPC_PEERING_DNS_RESOLUTION_CHECK

Ressourcentypen: AWS::EC2::VPCPeeringConnection

Auslösertyp: Konfigurationsänderungen

AWS-Region: Alle unterstützten AWS Regionen außer China (Peking), Asien-Pazifik (Thailand), Asien-Pazifik (Jakarta), Naher Osten (VAE), Asien-Pazifik (Hyderabad), Asien-Pazifik (Malaysia), Asien-Pazifik (Melbourne), AWS GovCloud (US-Ost), AWS GovCloud (US-West), Mexiko (Zentral), Israel (Tel Aviv), Kanada West (Calgary), Europa (Spanien), China (Ningxia), Europa (Zürich)

Parameter:

vpcIds (optional), Typ: CSV

Kommagetrennte Liste der IDs zu prüfenden VPC.

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

vpc-sg-open-only-to-authorized-ports

Prüft, ob Sicherheitsgruppen, die uneingeschränkten eingehenden Datenverkehr zulassen („0.0.0.0/0“ oder „::/0“), nur eingehende TCP- oder UDP-Verbindungen an autorisierten Ports zulassen. Die Regel ist NON_COMPLIANT, wenn für solche Sicherheitsgruppen keine Ports in den Regelparametern angegeben sind.

> **Note**
>
> Diese Regel wertet EC2 Amazon-Sicherheitsgruppen aus, deren Eingangsregel auf IPv4 ='0.0.0.0/0' oder =': :/' gesetzt ist. IPv6 Wenn die Sicherheitsgruppe keines dieser Ziele hat, gibt diese Regel den Wert `NOT_APPLICABLE` zurück.

Identifier (ID): VPC_SG_OPEN_ONLY_TO_AUTHORIZED_PORTS

Ressourcentypen: AWS::EC2::SecurityGroup

Auslösertyp: „Konfigurationsänderungen“ und „Regelmäßig“

AWS-Region: Alle unterstützten AWS Regionen außer der Region Asien-Pazifik (Melbourne)

Parameter:

authorizedTcpPorts (Fakultativ), Typ: Zeichenfolge

Durch Komma getrennte Liste der TCP-Ports, die autorisiert sind, für „0.0.0.0/0“ oder „::/0“ offen zu sein. Bereiche werden durch Bindestrich definiert, z. B. „443.1020-1025“.

authorizedUdpPorts (Fakultativ), Typ: Zeichenfolge

Durch Komma getrennte Liste der UDP-Ports, die autorisiert sind, für „0.0.0.0/0“ oder „::/0“ offen zu sein. Bereiche werden durch Bindestrich definiert, z. B. „500,1020-1025“.

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

vpc-sg-port-restriction-überprüfen

Überprüft, ob Sicherheitsgruppen den eingehenden Datenverkehr explizit auf eingeschränkte Ports von 0.0.0.0/0 oder: :/0 beschränken. Die Regel lautet NON_COMPLIANT, wenn Sicherheitsgruppen eingehenden Verkehr von 0.0.0.0/0 oder: :/0 über die Ports 22/3389 oder wie in den Parametern angegeben zulassen. TCP/UDP

Kennung: VPC_SG_PORT_RESTRICTION_CHECK

Ressourcentypen: AWS::EC2::SecurityGroup

Auslösertyp: Regelmäßig

AWS-Region: Alle unterstützten AWS Regionen außer China (Peking), Asien-Pazifik (Thailand), Asien-Pazifik (Malaysia), Mexiko (Zentral) und Kanada West (Calgary)

Parameter:

Anschlüsse einschränken (optional), Typ: CSV

Durch Kommas getrennte Liste von Ports, die nicht für eingehenden Datenverkehr über den gesamten IP-Bereich geöffnet sein sollten. Gültige Portnummern reichen von 0 bis 65535. Wenn nicht angegeben, sucht die Regel standardmäßig nach 22 und 3389.

Protokolltyp (optional), Typ: Zeichenfolge

Der Übertragungsprotokolltyp für die zu prüfende Regel. Zu den gültigen Werten gehören „TCP“, „UDP“ und „ALL“ (Groß- und Kleinschreibung wird nicht beachtet). Wenn der Wert auf 'ALL' gesetzt ist, sucht die Regel nach Regeln, die entweder das Protokoll 'TCP', 'UDP' oder 'ALL' (-1) verwenden. Der Standardwert ist 'ALL'.

excludeExternalSecurityGruppen (optional), Typ: Boolesch

Boolesches Flag, um die Bewertung externer Sicherheitsgruppen auszuschließen. Wenn der Wert auf „true“ gesetzt ist, bezieht die Regel keine externen Sicherheitsgruppen in die Bewertung mit ein. Andernfalls werden alle Sicherheitsgruppen ausgewertet, wenn der Wert auf „Falsch“ gesetzt ist. Der Standardwert ist „wahr“.

IPType (optional), Typ: Zeichenfolge

Die Version des Internetprotokolls (IP), für die die Regel überprüft werden soll. Zu den gültigen Werten gehören 'IPv4', '' und IPv6 'ALL' (Groß-/Kleinschreibung wird nicht beachtet). Wenn nicht angegeben, sucht die Regel standardmäßig nach „ALL“.

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

vpc-vpn-2-tunnels-up

Überprüft, ob sich beide von VPN bereitgestellten AWS Site-to-Site VPN-Tunnel (Virtual Private Network) im UP-Status befinden. Die Regel ist NON_COMPLIANT, wenn ein oder beide Tunnel den Status „DOWN“ aufweisen.

ID: VPC_VPN_2_TUNNELS_UP

Ressourcentypen: AWS::EC2::VPNConnection

Auslösertyp: Konfigurationsänderungen

AWS-Region: Alle unterstützten AWS Regionen außer Naher Osten (Bahrain), China (Peking), Asien-Pazifik (Osaka), Israel (Tel Aviv), China (Ningxia)

Parameter:

Keine

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

wafv2-logging-enabled

Prüft, ob die Protokollierung für AWS WAFv2 regionale und globale Web-Zugriffskontrolllisten (Web ACLs) aktiviert ist. Die Regel ist NON_COMPLIANT, wenn die Protokollierung aktiviert ist, das Protokollierungsziel jedoch nicht mit dem Wert des Parameters übereinstimmt.

> **Note**
>
> Amazon Security Lake-Ausnahme
> Diese Regel überprüft nicht die Protokollierung, die mit Security Lake for AWS WAFV2 Web durchgeführt wurde ACLs.

Kennung: WAFV2 _LOGGING_ENABLED

Ressourcentypen: AWS::WAFv2::WebACL

Auslösertyp: Regelmäßig

AWS-Region: Alle unterstützten AWS Regionen außer Asien-Pazifik (Thailand), Mexiko (Zentral) und Asien-Pazifik (Taipeh)

Parameter:

KinesisFirehoseDeliveryStreamArns (Fakultativ), Typ: CSV

Kommagetrennte Liste des Kinesis Firehose-Lieferstreams ARNs

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

WAF 2- rulegroup-logging-enabled

Überprüft, ob die Erfassung von CloudWatch Amazon-Sicherheitsmetriken für AWS WAFv2 Regelgruppen aktiviert ist. Die Regel ist NON_COMPLIANT, wenn '. VisibilityConfig CloudWatchMetricsEnabledDas Feld 'ist auf falsch gesetzt.

Kontext: AWS WAFV2 (Web Application Firewall Version 2) ermöglicht es Ihnen, AWS WAF Regeln zu erstellen, um Ihre Webanwendungen vor häufigen Web-Exploits und Sicherheitslücken zu schützen. Eine AWS WAF Regelgruppe ist eine Sammlung von AWS WAF Regeln, die Sie einer Web-ACL (Access Control List) zuordnen können, um das gewünschte Verhalten für den Datenverkehr Ihrer Webanwendung zu definieren. Weitere Informationen finden Sie unter AWS WAF Regeln und Regelgruppen im AWS WAF Entwicklerhandbuch.

Indem Sie die Erfassung von CloudWatch Sicherheitsmetriken für eine AWS WAFV2 Regelgruppe konfigurieren, können Sie Sicherheitsmetriken wie erfolgreiche oder fehlgeschlagene Distributed-Denial-of-Service- (DDoS) -Angriffe, SQL-Injection-Angriffe und Cross-Site Scripting (XSS) -Angriffe überwachen. Die gesammelten Sicherheitsmetriken können Ihnen helfen, Ihre Untersuchungen zu vereinfachen.

> **Note**
>
> Wenn die Regelgruppe keine AWS WAF Regeln enthält, die AWS WAFV2 von der AWS Config verwalteten Regel überprüft werden könnten, kehrt die AWS Config verwaltete Regel zurück`NOT_APPLICABLE`.

ID: WAFV2 _RULEGROUP_LOGGING_ENABLED

Ressourcentypen: AWS::WAFv2::RuleGroup

Auslösertyp: Konfigurationsänderungen

AWS-Region: Alle unterstützten AWS Regionen außer Asien-Pazifik (Thailand), Asien-Pazifik (Malaysia), AWS GovCloud (USA-Ost), AWS GovCloud (US-West), Mexiko (Zentral), Kanada West (Calgary)

Parameter:

Keine

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

WAF 2- rulegroup-not-empty

Prüft, ob WAFv2 Regelgruppen Regeln enthalten. Die Regel ist NON_COMPLIANT, wenn eine WAFv2 Regelgruppe keine Regeln enthält.

Kennung: _RULEGROUP_NOT_EMPTY WAFV2

Ressourcentypen: AWS::WAFv2::RuleGroup

Auslösertyp: Konfigurationsänderungen

AWS-Region: Alle unterstützten AWS Regionen außer China (Peking), Asien-Pazifik (Thailand), Asien-Pazifik (Jakarta), Naher Osten (VAE), Asien-Pazifik (Hyderabad), Asien-Pazifik (Malaysia), Asien-Pazifik (Melbourne), AWS GovCloud (US-Ost), AWS GovCloud (US-West), Mexiko (Zentral), Israel (Tel Aviv), Kanada West (Calgary), Europa (Spanien), China (Ningxia), Europa (Zürich)

Parameter:

Keine

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

WAF 2- webacl-not-empty

Prüft, ob eine WAFv2 Web-ACL WAF-Regeln oder WAF-Regelgruppen enthält. Diese Regel ist NON_COMPLIANT, wenn eine Web-ACL keine WAF-Regeln oder WAF-Regelgruppen enthält.

Kennung: _WEBACL_NOT_EMPTY WAFV2

Ressourcentypen: AWS::WAFv2::WebACL

Auslösertyp: Konfigurationsänderungen

AWS-Region: Alle unterstützten AWS Regionen außer Asien-Pazifik (Thailand), Asien-Pazifik (Jakarta), Naher Osten (VAE), Asien-Pazifik (Hyderabad), Asien-Pazifik (Malaysia), AWS GovCloud (USA-Ost), AWS GovCloud (US-West), Mexiko (Zentral), Kanada West (Calgary), Europa (Spanien), Europa (Zürich)

Parameter:

Keine

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

waf-classic-logging-enabled

Prüft, ob die Protokollierung in den AWS WAF Classic Global Web Access Control Lists (Web ACLs) aktiviert ist. Die Regel ist NON_COMPLIANT für eine globale Web-ACL, wenn die Protokollierung nicht aktiviert ist.

ID: WAF_CLASSIC_LOGGING_ENABLED

Ressourcentypen: AWS::WAF::WebACL

Auslösertyp: Regelmäßig

AWS-Region: Nur in der Region USA Ost (Nord-Virginia) verfügbar

Parameter:

KinesisFirehoseDeliveryStreamArns (Fakultativ), Typ: CSV

Kommagetrennte Liste der Amazon Kinesis Kinesis-Stream-ARN für AWS WAF-Protokolle.

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

waf-global-rulegroup-not-leer

Prüft, ob eine AWS WAF Classic-Regelgruppe Regeln enthält. Die Regel ist NON_COMPLIANT, wenn innerhalb einer Regelgruppe keine Regeln vorhanden sind.

ID: WAF_GLOBAL_RULEGROUP_NOT_EMPTY

Ressourcentypen: AWS::WAF::RuleGroup

Auslösertyp: Konfigurationsänderungen

AWS-Region: Nur in der Region USA Ost (Nord-Virginia) verfügbar

Parameter:

Keine

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

waf-global-rule-not-leer

Prüft, ob eine globale AWS WAF-Regel Bedingungen enthält. Die Regel ist NON_COMPLIANT, wenn in der globalen WAF-Regel keine Bedingungen vorhanden sind.

ID: WAF_GLOBAL_RULE_NOT_EMPTY

Ressourcentypen: AWS::WAF::Rule

Auslösertyp: Konfigurationsänderungen

AWS-Region: Nur in der Region USA Ost (Nord-Virginia) verfügbar

Parameter:

Keine

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

waf-global-webacl-not-leer

Prüft, ob eine globale WAF-Web-ACL WAF-Regeln oder -Regelgruppen enthält. Diese Regel ist NON_COMPLIANT, wenn eine globale Web-ACL keine WAF-Regel oder -Regelgruppe enthält.

ID: WAF_GLOBAL_WEBACL_NOT_EMPTY

Ressourcentypen: AWS::WAF::WebACL

Auslösertyp: Konfigurationsänderungen

AWS-Region: Nur in der Region USA Ost (Nord-Virginia) verfügbar

Parameter:

Keine

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

waf-regional-rulegroup-not-leer

Prüft, ob regionale WAF-Regelgruppen Regeln enthalten. Die Regel ist NON_COMPLIANT, wenn innerhalb einer regionalen WAF-Regelgruppe keine Regeln vorhanden sind.

ID: WAF_REGIONAL_RULEGROUP_NOT_EMPTY

Ressourcentypen: AWS::WAFRegional::RuleGroup

Auslösertyp: Konfigurationsänderungen

AWS-Region: Alle unterstützten AWS Regionen außer China (Peking), Asien-Pazifik (Thailand), Asien-Pazifik (Jakarta), Naher Osten (VAE), Asien-Pazifik (Hyderabad), Asien-Pazifik (Osaka), Asien-Pazifik (Malaysia), AWS GovCloud (US-Ost), AWS GovCloud (US-West), Mexiko (Zentral), Israel (Tel Aviv), Kanada West (Calgary), Europa (Spanien), China (Ningxia), Europa (Zürich)

Parameter:

Keine

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

waf-regional-rule-not-leer

Prüft, ob die regionale WAF-Regel Bedingungen enthält. Diese Regel ist COMPLIANT, wenn die regionale Regel mindestens eine Bedingung enthält, andernfalls ist sie NON_COMPLIANT.

ID: WAF_REGIONAL_RULE_NOT_EMPTY

Ressourcentypen: AWS::WAFRegional::Rule

Auslösertyp: Konfigurationsänderungen

AWS-Region: Alle unterstützten AWS Regionen außer Asien-Pazifik (Thailand), Asien-Pazifik (Malaysia), AWS GovCloud (USA-Ost), AWS GovCloud (US-West), Mexiko (Zentral), Kanada West (Calgary)

Parameter:

Keine

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

waf-regional-webacl-not-leer

Prüft, ob eine regionale WAF-Web-ACL WAF-Regeln oder -Regelgruppen enthält. Die Regel ist NON_COMPLIANT, wenn in einer Web-ACL keine WAF-Regeln oder -Regelgruppen vorhanden sind.

ID: WAF_REGIONAL_WEBACL_NOT_EMPTY

Ressourcentypen: AWS::WAFRegional::WebACL

Auslösertyp: Konfigurationsänderungen

AWS-Region: Alle unterstützten AWS Regionen außer Asien-Pazifik (Thailand), Asien-Pazifik (Malaysia), AWS GovCloud (USA-Ost), AWS GovCloud (US-West), Mexiko (Zentral), Kanada West (Calgary)

Parameter:

Keine

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

workspaces-root-volume-encryption-aktiviert

Prüft, ob bei einem WorkSpace Amazon-Volume die Verschlüsselungseinstellungen für das Root-Volume aktiviert sind. Diese Regel ist NON_COMPLIANT, wenn die Verschlüsselungseinstellung für das Root-Volume nicht aktiviert ist.

Kennung: WORKSPACES_ROOT_VOLUME_ENCRYPTION_ENABLED

Ressourcentypen: AWS::WorkSpaces::Workspace

Auslösertyp: Konfigurationsänderungen

AWS-Region: Nur in der Region Asien-Pazifik (Mumbai), Afrika (Kapstadt), Europa (Irland), Europa (Frankfurt), Südamerika (Sao Paulo), USA Ost (Nord-Virginia), Asien-Pazifik (Seoul), Europa (London), Asien-Pazifik (Tokio), USA West (Oregon), Asien-Pazifik (Singapur), Asien-Pazifik (Sydney), Kanada (Zentral), China (Ningxia) verfügbar

Parameter:

Keine

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

workspaces-user-volume-encryption-aktiviert

Prüft, ob bei einem WorkSpace Amazon-Volume die Verschlüsselungseinstellungen für Benutzervolumes aktiviert sind. Diese Regel ist NON_COMPLIANT, wenn die Verschlüsselungseinstellung für das Benutzervolume nicht aktiviert ist.

Kennung: WORKSPACES_USER_VOLUME_ENCRYPTION_ENABLED

Ressourcentypen: AWS::WorkSpaces::Workspace

Auslösertyp: Konfigurationsänderungen

AWS-Region: Nur in der Region Asien-Pazifik (Mumbai), Afrika (Kapstadt), Europa (Irland), Europa (Frankfurt), Südamerika (Sao Paulo), USA Ost (Nord-Virginia), Asien-Pazifik (Seoul), Europa (London), Asien-Pazifik (Tokio), USA West (Oregon), Asien-Pazifik (Singapur), Asien-Pazifik (Sydney), Kanada (Zentral), China (Ningxia) verfügbar

Parameter:

Keine

AWS CloudFormation Vorlage

Informationen zum Erstellen AWS Config verwalteter Regeln mit AWS CloudFormation Vorlagen finden Sie unterAWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.

Liste der AWS Config verwalteten Regeln nach Testmodus

AWS Config unterstützt derzeit die folgenden verwalteten Regeln. Bevor Sie diese Regeln verwenden, finden Sie weitere Informationen unterÜberlegungen.

Proaktive Auswertung

Proaktive Regeln sind Regeln, die den proaktiven Auswertungsmodus für Ressourcen unterstützen, die nicht bereitgestellt wurden. Auf diese Weise können Sie auswerten, ob ein Satz von Ressourceneigenschaften, wenn er zur Definition einer AWS Ressource verwendet würde, angesichts der proaktiven Regeln, die Sie in Ihrem Konto in Ihrer Region haben, als COMPLIANT oder NON_COMPLIANT gelten würde. Weitere Informationen finden Sie unter Auswertungsmodi.

> **Note**
>
> Durch proaktive Regeln werden keine Ressourcen korrigiert, die als NON_COMPLIANT gekennzeichnet sind, und sie verhindern auch nicht, dass diese bereitgestellt werden.

Proaktive Auswertung

- api-gw-xray-enabled
- autoscaling-group-elb-healthcheck-erforderlich
- ec2- instance-multiple-eni-check
- eip-attached
- elasticsearch-node-to-node-Verschlüsselungsprüfung
- lambda-function-settings-check
- lambda-inside-vpc
- rds-automatic-minor-version-Upgrade aktiviert
- rds-enhanced-monitoring-enabled
- rds-instance-public-access-überprüfen
- rds-multi-az-support
- rds-storage-encrypted
- redshift-cluster-maintenancesettings-check
- redshift-cluster-public-access-überprüfen
- s3- bucket-logging-enabled
- sns-encrypted-kms
- subnet-auto-assign-public-ip-deaktiviert

Detektivische Auswertung

Detektivische Regeln sind Regeln, die den detektivischen Auswertungsmodus für Ressourcen unterstützen, die bereits bereitgestellt wurden. Auf diese Weise lassen sich die Konfigurationseinstellungen Ihrer vorhandenen Ressourcen auswerten.

> **Note**
>
> Derzeit unterstützen alle AWS Config Regeln die detektivische Bewertung.

Detektivische Auswertung

- access-keys-rotated
- account-part-of-organizations
- acmpca-certificate-authority-tagged
- acm-certificate-expiration-check
- acm-certificate-rsa-check
- acm-pca-root-ca-deaktiviert
- active-mq-supported-version
- alb-desync-mode-check
- alb-http-drop-invalid-Header-fähig
- alb-http-to-https-Umleitungsprüfung
- alb-internal-scheme-check
- alb-listener-tagged
- alb-waf-enabled
- amplify-app-branch-auto-löschung aktiviert
- amplify-app-description
- amplify-app-tagged
- amplify-branch-performance-mode-aktiviert
- amplify-branch-tagged
- api-gwv2- access-logs-enabled
- api-gwv2- authorization-type-configured
- api-gw-associated-with-WAF

- api-gw-cache-enabled-und-verschlüsselt
- api-gw-endpoint-type-überprüfen
- api-gw-execution-logging-aktiviert
- api-gw-ssl-enabled
- api-gw-xray-enabled
- appconfig-application-description
- appconfig-application-tagged
- appconfig-configuration-profile-tagged
- appconfig-configuration-profile-validators-nicht leer
- appconfig-deployment-strategy-description
- appconfig-deployment-strategy-replicate-zu-ssm
- appconfig-environment-description
- appconfig-environment-tagged
- appconfig-extension-association-tagged
- appconfig-freeform-profile-config-Speicher
- appconfig-hosted-configuration-version-Beschreibung
- appflow-flow-tagged
- appintegrations-event-integration-description
- appintegrations-event-integration-tagged
- appmesh-gateway-route-tagged
- appmesh-mesh-deny-tcp-Weiterleitung
- appmesh-mesh-tagged
- appmesh-route-tagged
- appmesh-virtual-gateway-backend-Standardeinstellungen-TLS
- appmesh-virtual-gateway-logging-file-path-exists
- appmesh-virtual-gateway-tagged
- appmesh-virtual-node-backend-defaults-tls-on
- appmesh-virtual-node-logging-file-path-exists
- appmesh-virtual-node-tagged
- appmesh-virtual-router-tagged

- appmesh-virtual-service-tagged
- approved-amis-by-id
- approved-amis-by-tag
- apprunner-service-in-vpc
- apprunner-service-no-public-Zugang
- apprunner-service-observability-enabled
- apprunner-service-tagged
- apprunner-vpc-connector-tagged
- appstream-fleet-in-vpc
- appsync-associated-with-waf
- appsync-authorization-check
- appsync-cache-ct-encryption-im Ruhezustand
- appsync-cache-ct-encryptionim Transit
- appsync-cache-encryption-at-ausruhen
- appsync-logging-enabled
- athena-data-catalog-description
- athena-prepared-statement-description
- athena-workgroup-description
- athena-workgroup-encrypted-at-ausruhen
- athena-workgroup-enforce-workgroup-Konfiguration
- athena-workgroup-engine-version-automatisches Upgrade
- athena-workgroup-logging-enabled
- aurora-last-backup-recovery-Punkt erstellt
- aurora-meets-restore-time-Ziel
- aurora-mysql-backtracking-enabled
- aurora-mysql-cluster-audit-Protokollierung
- aurora-resources-in-logically-air-gapped-vault
- aurora-resources-protected-by-Backup-Plan
- autoscaling-capacity-rebalancing
- autoscaling-group-elb-healthcheck-erforderlich

- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-hop-Grenze
- autoscaling-launch-config-public-ip-deaktiviert
- autoscaling-launch-template
- autoscaling-multiple-az
- autoscaling-multiple-instance-types
- backup-plan-min-frequency-and-min-retention-check
- backup-recovery-point-encrypted
- backup-recovery-point-manual-Löschen-deaktiviert
- backup-recovery-point-minimum-Aufbewahrungsprüfung
- batch-compute-environment-enabled
- batch-compute-environment-managed
- batch-compute-environment-tagged
- batch-job-queue-enabled
- batch-job-queue-tagged
- batch-managed-compute-environment-using-launch-template
- batch-managed-compute-env-compute-resources-tagged
- batch-scheduling-policy-tagged
- beanstalk-enhanced-health-reporting-aktiviert
- cassandra-keyspace-tagged
- clb-desync-mode-check
- clb-multiple-az
- cloudformation-stack-drift-detection-überprüfen
- cloudformation-stack-notification-check
- cloudfront-accesslogs-enabled
- cloudfront-associated-with-waf
- cloudfront-custom-ssl-certificate
- cloudfront-default-root-object-konfiguriert
- cloudfront-no-deprecated-ssl-Protokolle
- cloudfront-origin-access-identity-aktiviert

- cloudfront-origin-failover-enabled
- Cloudfront-S3- origin-access-control-enabled
- Wolkenfront - 3 origin-non-existent-bucket
- cloudfront-security-policy-check
- cloudfront-sni-enabled
- cloudfront-ssl-policy-check
- cloudfront-traffic-to-origin-verschlüsselt
- cloudfront-viewer-policy-https
- cloudtrail-all-read-s3- data-event-check
- cloudtrail-all-write-s3- data-event-check
- Wolkenspur-S3- bucket-access-logging
- CloudTrail-S3- bucket-public-access-prohibited
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-action-enabled-überprüfen
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted
- cloud-trail-cloud-watch-logs-aktiviert
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-Validierung aktiviert
- cmk-backing-key-rotation-aktiviert
- codebuild-project-artifact-encryption
- codebuild-project-environment-privileged-überprüfen
- codebuild-project-envvar-awscred-überprüfen
- codebuild-project-logging-enabled
- codebuild-project-s3-log-verschlüsselt
- codebuild-project-source-repo-URL-Prüfung

- codebuild-report-group-encrypted-im Ruhezustand
- codedeploy-auto-rollback-monitor-aktiviert
- codedeploy-deployment-group-auto-rollback-aktiviert
- codedeploy-deployment-group-outdated-instanzen-aktualisieren
- Codedeploy-ec2- minimum-healthy-hosts-configured
- codedeploy-lambda-allatonce-traffic-shift-deaktiviert
- codeguruprofiler-profiling-group-tagged
- codegururevieweer-repository-association-tagged
- codepipeline-deployment-count-check
- codepipeline-region-fanout-check
- cognito-identity-pool-unauth-Zugriffsprüfung
- cognito-user-pool-advanced-sicherheitsaktiviert
- cognito-user-pool-tagged
- connect-instance-logging-enabled
- customerprofiles-object-type-allow-Profilerstellung
- customerprofiles-object-type-tagged
- custom-eventbus-policy-attached
- custom-schema-registry-policy-beigefügt
- cw-loggroup-retention-period-überprüfen
- datasync-task-data-verification-aktiviert
- datasync-task-logging-enabled
- datasync-task-tagged
- dax-encryption-enabled
- dax-tls-endpoint-encryption
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- dms-auto-minor-version-aktualisieren-Prüfung
- dms-endpoint-ssl-configured
- dms-endpoint-tagged

- dms-mongo-db-authentication-aktiviert
- dms-neptune-iam-authorization-aktiviert
- dms-redis-tls-enabled
- dms-replication-not-public
- dms-replication-task-sourcedb-Protokollierung
- dms-replication-task-tagged
- dms-replication-task-targetdb-Protokollierung
- docdb-cluster-audit-logging-aktiviert
- docdb-cluster-backup-retention-überprüfen
- docdb-cluster-deletion-protection-aktiviert
- docdb-cluster-encrypted
- docdb-cluster-encrypted-in-transit
- docdb-cluster-snapshot-public-verboten
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-last-backup-recovery-Punkt erstellt
- dynamodb-meets-restore-time-Ziel
- dynamodb-pitr-enabled
- dynamodb-resources-protected-by-Backup-Plan
- dynamodb-table-deletion-protection-aktiviert
- dynamodb-table-encrypted-kms
- dynamodb-table-encryption-enabled
- dynamodb-throughput-limit-check
- ebs-in-backup-plan
- ebs-last-backup-recovery-punkt-erstellt
- ebs-meets-restore-time-Ziel
- ebs-optimized-instance
- ebs-resources-in-logically-air-gapped-vault
- ebs-resources-protected-by-Backup-Plan
- ebs-snapshot-public-restorable-überprüfen

- ec2- capacity-reservation-tagged
- ec2- carrier-gateway-tagged
- ec2- aktiviert client-vpn-connection-log
- ec2- client-vpn-endpoint-tagged
- ec2- -alle client-vpn-not-authorize
- ec2- dhcp-options-tagged
- ec2- ebs-encryption-by-default
- ec2- aktiviert enis-source-destination-check
- ec2-fleet-markiert
- ec2-imdsv2-check
- ec2- instance-detailed-monitoring-enabled
- ec2-ami instance-launched-with-allowed
- ec2- instance-managed-by-ssm
- ec2- instance-multiple-eni-check
- ec2- instance-no-public-ip
- ec2- instance-profile-attached
- ec2- erstellt last-backup-recovery-point
- ec2-2-prüfen launch-template-imdsv
- ec2- -deaktiviert launch-template-public-ip
- ec2- launch-template-tagged
- ec2- managedinstance-applications-blacklisted
- ec2- managedinstance-applications-required
- ec2- prüfen managedinstance-association-compliance-status
- ec2- managedinstance-inventory-blacklisted
- ec2- prüfen managedinstance-patch-compliance-status
- ec2- managedinstance-platform-check
- ec2- meets-restore-time-target
- ec2- Analyse mit Schlagwörtern network-insights-access-scope
- ec2 network-insights-access-scope - markiert
- ec2- network-insights-path-tagged

- ec2- no-amazon-key-pair
- ec2- paravirtual-instance-check
- ec2- prefix-list-tagged
- ec2- -Tresor mit Lücken resources-in-logically-air
- ec2- resources-protected-by-backup -plan
- ec2- -eni security-group-attached-to
- ec2- -eni-periodisch security-group-attached-to
- ec2 spot-fleet-request-ct - - encryption-at-rest
- ec2-stopped-instance
- ec2- token-hop-limit-check
- ec2- traffic-mirror-filter-description
- ec2- traffic-mirror-filter-tagged
- ec2- traffic-mirror-session-description
- ec2- traffic-mirror-session-tagged
- ec2- traffic-mirror-target-description
- ec2- traffic-mirror-target-tagged
- ec2- -attach-deaktiviert transit-gateway-auto-vpc
- ec2 transit-gateway-multicast-domain - markiert
- ec2- volume-inuse-check
- ec2- vpn-connection-logging-enabled
- ecr-private-image-scanning-aktiviert
- ecr-private-lifecycle-policy-konfiguriert
- ecr-private-tag-immutability-aktiviert
- ecr-repository-cmk-encryption-aktiviert
- ecr-repository-tagged
- ecs-awsvpc-networking-enabled
- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-container-insights-enabled
- ecs-fargate-latest-platform-Version

- ecs-no-environment-secrets
- ecs-task-definition-log-Konfiguration
- ecs-task-definition-memory-hartes Limit
- ecs-task-definition-network-mode-not-host
- ecs-task-definition-nonroot-Benutzer
- ecs-task-definition-pid-Modus-Check
- ecs-task-definition-user-for-host-mode-check
- efs-access-point-enforce-Stammverzeichnis
- efs-access-point-enforce-Benutzeridentität
- efs-automatic-backups-enabled
- efs-encrypted-check
- efs-filesystem-ct-encrypted
- efs-in-backup-plan
- efs-last-backup-recovery-Punkt erstellt
- efs-meets-restore-time-Ziel
- efs-mount-target-public-zugänglich
- efs-resources-in-logically-air-gapped-vault
- efs-resources-protected-by-Ersatzplan
- eip-attached
- eks-cluster-logging-enabled
- eks-cluster-log-enabled
- eks-cluster-oldest-supported-Ausführung
- eks-cluster-secrets-encrypted
- eks-cluster-supported-version
- eks-endpoint-no-public-Zugang
- eks-secrets-encrypted
- elasticache-auto-minor-version-aktualisieren-Prüfung
- elasticache-rbac-auth-enabled
- elasticache-redis-cluster-automatic-Backup-Check
- elasticache-repl-grp-auto-failover-fähig

- elasticache-repl-grp-encrypted-im Ruhezustand
- elasticache-repl-grp-encryptedauf der Durchreise
- elasticache-repl-grp-redis-auth-aktiviert
- elasticache-subnet-group-check
- elasticache-supported-engine-version
- elasticbeanstalk-application-description
- elasticbeanstalk-application-version-description
- elasticbeanstalk-environment-description
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch
- elasticsearch-node-to-node-Verschlüsselungsprüfung
- elastic-beanstalk-logs-to- Cloudwatch
- elastic-beanstalk-managed-updates-aktiviert
- elbv2- acm-certificate-required
- elv 2- listener-encryption-in-transit
- elbv2-multiple-az
- elbv2- prüfen predefined-security-policy-ssl
- elb-acm-certificate-required
- elb-cross-zone-load-Balancing aktiviert
- elb-custom-security-policy-ssl-Prüfung
- elb-deletion-protection-enabled
- elb-logging-enabled
- elb-predefined-security-policy-ssl-Überprüfung
- elb-tls-https-listeners-nur
- emr-block-public-access
- emr-kerberos-enabled
- emr-master-no-public-ip
- emr-security-configuration-encryption-ruh dich aus
- emr-security-configuration-encryption-Transit

- encrypted-volumes
- event-data-store-cmk-Verschlüsselung aktiviert
- evidently-launch-description
- evidently-launch-tagged
- evidently-project-description
- evidently-project-tagged
- evidently-segment-description
- evidently-segment-tagged
- fis-experiment-template-log-Konfiguration vorhanden
- fis-experiment-template-tagged
- fms-shield-resource-policy-überprüfen
- fms-webacl-resource-policy-überprüfen
- fms-webacl-rulegroup-association-überprüfen
- frauddetector-entity-type-tagged
- frauddetector-label-tagged
- frauddetector-outcome-tagged
- frauddetector-variable-tagged
- fsx-last-backup-recovery-Punkt erstellt
- fsx-lustre-copy-tagszu Backups
- fsx-meets-restore-time-Ziel
- fsx-ontap-deployment-type-überprüfen
- fsx-openzfs-copy-tags-aktiviert
- fsx-openzfs-deployment-type-überprüfen
- fsx-resources-protected-by-Backup-Plan
- fsx-windows-audit-log-konfiguriert
- fsx-windows-deployment-type-überprüfen
- glb-listener-tagged
- global-endpoint-event-replication-aktiviert
- glue-job-logging-enabled
- glue-ml-transform-encrypted-im Ruhezustand

- glue-spark-job-supported-Ausführung
- GuardDuty-EC2- protection-runtime-enabled
- guardduty-ecs-protection-runtime-aktiviert
- guardduty-eks-protection-audit-aktiviert
- guardduty-eks-protection-runtime-aktiviert
- guardduty-enabled-centralized
- guardduty-lambda-protection-enabled
- guardduty-malware-protection-enabled
- guardduty-non-archived-findings
- guardduty-rds-protection-enabled
- guardduty-runtime-monitoring-enabled
- GuardDuty-S3-Schutz aktiviert
- iam-customer-policy-blocked-kms-Aktionen
- iam-external-access-analyzer-aktiviert
- iam-group-has-users-überprüfen
- iam-inline-policy-blocked-kms-Aktionen
- iam-no-inline-policy-überprüfen
- iam-oidc-provider-tagged
- iam-password-policy
- iam-policy-blacklisted-check
- iam-policy-in-use
- iam-policy-no-statements-with-admin-access
- iam-policy-no-statements-with-full-access
- iam-role-managed-policy-überprüfen
- iam-root-access-key-überprüfen
- iam-saml-provider-tagged
- iam-server-certificate-expiration-überprüfen
- iam-server-certificate-tagged
- iam-user-group-membership-überprüfen
- iam-user-mfa-enabled

- iam-user-no-policies-überprüfen
- iam-user-unused-credentials-überprüfen
- incoming-ssh-disabled
- inspector-ec2-Scan aktiviert
- inspector-ecr-scan-enabled
- inspector-lambda-code-scan-aktiviert
- inspector-lambda-standard-scan-aktiviert
- instances-in-vpc
- internet-gateway-authorized-vpc-nur
- iotevents-alarm-model-tagged
- iotevents-detector-model-tagged
- iotevents-input-tagged
- iotsitewise-asset-model-tagged
- iotsitewise-dashboard-tagged
- iotsitewise-gateway-tagged
- iotsitewise-portal-tagged
- iotsitewise-project-tagged
- iottwinmaker-component-type-tagged
- iottwinmaker-entity-tagged
- iottwinmaker-scene-tagged
- iottwinmaker-sync-job-tagged
- iottwinmaker-workspace-tagged
- iotwireless-fuota-task-tagged
- iotwireless-multicast-group-tagged
- iotwireless-service-profile-tagged
- iot-authorizer-token-signing-aktiviert
- ivs-channel-playback-authorization-aktiviert
- ivs-channel-tagged
- ivs-playback-key-pair-markiert
- ivs-recording-configuration-tagged

- kinesis-firehose-delivery-stream-verschlüsselt
- kinesis-stream-backup-retention-überprüfen
- kinesis-stream-encrypted
- kms-cmk-not-scheduled-zum Löschen
- kms-key-policy-no-öffentlicher Zugang
- lambda-concurrency-check
- lambda-dlq-check
- lambda-function-public-access-verboten
- lambda-function-settings-check
- lambda-function-xray-enabled
- lambda-inside-vpc
- lambda-vpc-multi-az-überprüfen
- lightsail-bucket-tagged
- lightsail-certificate-tagged
- lightsail-disk-tagged
- macie-auto-sensitive-data-Discovery-Check
- macie-status-check
- mariadb-publish-logs-to-Cloudwatch-Protokolle
- mfa-enabled-for-iam-Konsolenzugriff
- mq-active-broker-ldap-Authentifizierung
- mq-active-deployment-mode
- mq-active-single-instance-broker-storage-type-efs
- mq-automatic-minor-version-Upgrade aktiviert
- mq-auto-minor-version-upgrade-fähig
- mq-broker-general-logging-aktiviert
- mq-cloudwatch-audit-logging-aktiviert
- mq-cloudwatch-audit-log-aktiviert
- mq-no-public-access
- mq-rabbit-deployment-mode
- msk-cluster-public-access-deaktiviert

- msk-connect-connector-logging-aktiviert
- msk-enhanced-monitoring-enabled
- msk-in-cluster-node-require-tls
- msk-unrestricted-access-check
- multi-region-cloud-trail-aktiviert
- nacl-no-unrestricted-ssh-rdp
- neptune-cluster-backup-retention-überprüfen
- neptune-cluster-cloudwatch-log-exportfähig
- neptune-cluster-copy-tags-to-snapshot-enabled
- neptune-cluster-deletion-protection-aktiviert
- neptune-cluster-encrypted
- neptune-cluster-iam-database-Authentifizierung
- neptune-cluster-multi-az-aktiviert
- neptune-cluster-snapshot-encrypted
- neptune-cluster-snapshot-public-verboten
- netfw-deletion-protection-enabled
- netfw-logging-enabled
- netfw-multi-az-enabled
- netfw-policy-default-action-fragment-Pakete
- netfw-policy-default-action-vollständige Pakete
- netfw-policy-rule-group-assoziiert
- netfw-stateless-rule-group-nicht leer
- netfw-subnet-change-protection-aktiviert
- nlb-cross-zone-load-Balancing aktiviert
- nlb-internal-scheme-check
- nlb-listener-tagged
- nlb-logging-enabled
- no-unrestricted-route-to-igw
- opensearch-access-control-enabled
- opensearch-audit-logging-enabled

- opensearch-data-node-fault-Toleranz
- opensearch-encrypted-at-rest
- opensearch-https-required
- opensearch-in-vpc-only
- opensearch-logs-to-cloudwatch
- opensearch-node-to-node-Verschlüsselungsprüfung
- opensearch-primary-node-fault-Toleranz
- opensearch-update-check
- rabbit-mq-supported-version
- rds-aurora-mysql-audit-Protokollierung aktiviert
- rds-aurora-postgresql-logs-zu-Cloud-Watch
- rds-automatic-minor-version-upgrade-fähig
- rds-cluster-auto-minor-version-upgrade-enable
- rds-cluster-default-admin-überprüfen
- rds-cluster-deletion-protection-aktiviert
- rds-cluster-encrypted-at-ausruhen
- rds-cluster-iam-authentication-aktiviert
- rds-cluster-multi-az-aktiviert
- rds-db-security-group-nicht erlaubt
- rds-enhanced-monitoring-enabled
- rds-instance-default-admin-überprüfen
- rds-instance-deletion-protection-aktiviert
- rds-instance-iam-authentication-aktiviert
- rds-instance-public-access-überprüfen
- rds-instance-subnet-igw-überprüfen
- rds-in-backup-plan
- rds-last-backup-recovery-Punkt erstellt
- rds-logging-enabled
- rds-mariadb-instance-encryptedwährend des Transports
- rds-meets-restore-time-Ziel

- rds-multi-az-support
- rds-mysql-instance-encryptedim Transit
- rds-postgresql-logs-to- Cloudwatch
- rds-postgres-instance-encryptedim Transit
- rds-proxy-tls-encryption
- rds-resources-protected-by-Ersatzplan
- rds-snapshots-public-prohibited
- rds-snapshot-encrypted
- rds-sqlserver-encrypted-in-Transit
- rds-sql-server-logs-zu-Cloud-Uhr
- rds-storage-encrypted
- redshift-audit-logging-enabled
- redshift-backup-enabled
- redshift-cluster-configuration-check
- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check
- redshift-cluster-multi-az-aktiviert
- redshift-cluster-parameter-group-markiert
- redshift-cluster-public-access-überprüfen
- redshift-cluster-subnet-group-Multi-Az
- redshift-default-admin-check
- redshift-default-db-name-überprüfen
- redshift-enhanced-vpc-routing-aktiviert
- redshift-require-tls-ssl
- redshift-serverless-default-admin-überprüfen
- redshift-serverless-default-db-Namenscheck
- redshift-serverless-namespace-cmk-Verschlüsselung
- redshift-serverless-publish-logs-zu-Cloud-Watch
- redshift-serverless-workgroup-encryptedunterwegs
- redshift-serverless-workgroup-no-öffentlich zugänglich

- redshift-serverless-workgroup-routes-innerhalb von VPC
- redshift-unrestricted-port-access
- required-tags
- restricted-incoming-traffic
- root-account-hardware-mfa-aktiviert
- root-account-mfa-enabled
- Route 53- query-logging-enabled
- s3 -regel-check express-dir-bucket-lifecycle
- nur s3- access-point-in-vpc
- s3- -Blöcke access-point-public-access
- s3- -Blöcke account-level-public-access
- s3- -Blocke-periodisch account-level-public-access
- s 3- bucket-acl-prohibited
- s-3 bucket-blacklisted-actions-prohibited
- s3- bucket-cross-region-replication -aktiviert
- s-3 bucket-default-lock-enabled
- s3 bucket-level-public-access - verboten
- s3- bucket-logging-enabled
- s-3 bucket-mfa-delete-enabled
- s-3 bucket-policy-grantee-check
- s3- bucket-policy-not-more -freizügig
- s 3- bucket-public-read-prohibited
- s-3 bucket-public-write-prohibited
- s-3 bucket-replication-enabled
- s3- bucket-server-side-encryption -aktiviert
- s-3 bucket-ssl-requests-only
- s3-Bucket-Tagged
- s-3 bucket-versioning-enabled
- s-3 default-encryption-kms
- s-3 event-notifications-enabled

- s3 last-backup-recovery-point - erstellt
- s3- lifecycle-policy-check
- s-3 meets-restore-time-target
- s3- resources-in-logically-air -Tresor mit Lücken
- s3 resources-protected-by-backup - -Plan
- s 3- version-lifecycle-policy-check
- sagemaker-app-image-config-markiert
- sagemaker-domain-in-vpc
- sagemaker-domain-tagged
- sagemaker-endpoint-configuration-kms-schlüsselkonfiguriert
- sagemaker-endpoint-config-prod-Anzahl der Instanzen
- sagemaker-feature-group-tagged
- sagemaker-image-description
- sagemaker-image-tagged
- sagemaker-model-in-vpc
- sagemaker-model-isolation-enabled
- sagemaker-notebook-instance-inside-vpc
- sagemaker-notebook-instance-kms-key-konfiguriert
- sagemaker-notebook-instance-platform-Version
- sagemaker-notebook-instance-root-Zugriffsprüfung
- sagemaker-notebook-no-direct-Internetzugang
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-überprüfen
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- securityhub-enabled
- security-account-information-provided
- service-catalog-shared-within-Organisation
- service-vpc-endpoint-enabled

- ses-malware-scanning-enabled
- shield-advanced-enabled-autorenew
- shield-drt-access
- sns-encrypted-kms
- sns-topic-message-delivery-Benachrichtigung aktiviert
- sns-topic-no-public-Zugriff
- sqs-queue-no-public-Zugang
- ssm-automation-block-public-teilen
- ssm-automation-logging-enabled
- ssm-document-not-public
- ssm-document-tagged
- step-functions-state-machine-Protokollierung aktiviert
- storagegateway-last-backup-recovery-punkt-erstellt
- storagegateway-resources-in-logically-air-gapped-vault
- storagegateway-resources-protected-by-Ersatzplan
- subnet-auto-assign-public-ip-deaktiviert
- transfer-agreement-description
- transfer-agreement-tagged
- transfer-certificate-description
- transfer-certificate-tagged
- transfer-connector-logging-enabled
- transfer-connector-tagged
- transfer-family-server-no-ftp
- transfer-profile-tagged
- transfer-workflow-description
- transfer-workflow-tagged
- virtualmachine-last-backup-recovery-punkt-erstellt
- virtualmachine-resources-in-logically-air-gapped-vault
- virtualmachine-resources-protected-by-Ersatzplan
- vpc-default-security-group-geschlossen

- vpc-endpoint-enabled
- vpc-flow-logs-enabled
- vpc-network-acl-unused-überprüfen
- vpc-peering-dns-resolution-überprüfen
- vpc-sg-open-only-to-authorized-ports
- vpc-sg-port-restriction-überprüfen
- vpc-vpn-2-tunnels-up
- wafv2-logging-enabled
- WAF 2- rulegroup-logging-enabled
- WAF 2- rulegroup-not-empty
- WAF 2- webacl-not-empty
- waf-classic-logging-enabled
- waf-global-rulegroup-not-leer
- waf-global-rule-not-leer
- waf-global-webacl-not-leer
- waf-regional-rulegroup-not-leer
- waf-regional-rule-not-leer
- waf-regional-webacl-not-leer
- workspaces-root-volume-encryption-aktiviert
- workspaces-user-volume-encryption-aktiviert

Liste der AWS Config verwalteten Regeln nach Triggertyp

AWS Config unterstützt derzeit die folgenden verwalteten Regeln. Bevor Sie diese Regeln verwenden, finden Sie weitere Informationen unterÜberlegungen.

Konfigurationsänderungen

Durch Änderungen ausgelöste Regeln sind Regeln, die als Reaktion auf AWS Config Konfigurationsänderungen ausgewertet werden.

Konfigurationsänderungen

- acmpca-certificate-authority-tagged

- acm-certificate-rsa-check
- active-mq-supported-version
- alb-desync-mode-check
- alb-http-drop-invalid-header aktiviert
- alb-internal-scheme-check
- alb-listener-tagged
- alb-waf-enabled
- amplify-app-branch-auto-löschfähig
- amplify-app-description
- amplify-app-tagged
- amplify-branch-performance-mode-aktiviert
- amplify-branch-tagged
- api-gwv2- access-logs-enabled
- api-gw-associated-with-WAF
- api-gw-cache-enabled-und-verschlüsselt
- api-gw-endpoint-type-überprüfen
- api-gw-execution-logging-aktiviert
- api-gw-ssl-enabled
- api-gw-xray-enabled
- appconfig-application-description
- appconfig-application-tagged
- appconfig-configuration-profile-tagged
- appconfig-configuration-profile-validators-nicht leer
- appconfig-deployment-strategy-description
- appconfig-deployment-strategy-replicate-zu-ssm
- appconfig-environment-description
- appconfig-environment-tagged
- appconfig-extension-association-tagged
- appconfig-freeform-profile-config-Speicher
- appconfig-hosted-configuration-version-Beschreibung

- appflow-flow-tagged
- appintegrations-event-integration-description
- appintegrations-event-integration-tagged
- appmesh-gateway-route-tagged
- appmesh-mesh-deny-tcp-Weiterleitung
- appmesh-mesh-tagged
- appmesh-route-tagged
- appmesh-virtual-gateway-backend-Standardeinstellungen-TLS
- appmesh-virtual-gateway-logging-file-path-exists
- appmesh-virtual-gateway-tagged
- appmesh-virtual-node-backend-defaults-tls-on
- appmesh-virtual-node-logging-file-path-exists
- appmesh-virtual-node-tagged
- appmesh-virtual-router-tagged
- appmesh-virtual-service-tagged
- approved-amis-by-id
- approved-amis-by-tag
- apprunner-service-in-vpc
- apprunner-service-no-public-Zugang
- apprunner-service-observability-enabled
- apprunner-service-tagged
- apprunner-vpc-connector-tagged
- appstream-fleet-in-vpc
- appsync-authorization-check
- appsync-cache-ct-encryption-im Ruhezustand
- appsync-cache-ct-encryptionunterwegs
- appsync-logging-enabled
- athena-data-catalog-description
- athena-prepared-statement-description
- athena-workgroup-description

- athena-workgroup-encrypted-at-ausruhen
- athena-workgroup-enforce-workgroup-Konfiguration
- athena-workgroup-engine-version-automatisches Upgrade
- athena-workgroup-logging-enabled
- aurora-mysql-backtracking-enabled
- autoscaling-capacity-rebalancing
- autoscaling-group-elb-healthcheck-erforderlich
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-hop-Grenze
- autoscaling-launch-config-public-ip-deaktiviert
- autoscaling-launch-template
- autoscaling-multiple-az
- autoscaling-multiple-instance-types
- backup-plan-min-frequency-and-min-retention-check
- backup-recovery-point-encrypted
- backup-recovery-point-manual-Löschen-deaktiviert
- backup-recovery-point-minimum-Aufbewahrungsprüfung
- batch-compute-environment-enabled
- batch-compute-environment-managed
- batch-compute-environment-tagged
- batch-job-queue-enabled
- batch-job-queue-tagged
- batch-managed-compute-environment-using-launch-template
- batch-managed-compute-env-compute-resources-tagged
- batch-scheduling-policy-tagged
- beanstalk-enhanced-health-reporting-aktiviert
- cassandra-keyspace-tagged
- clb-desync-mode-check
- clb-multiple-az
- cloudformation-stack-notification-check

- cloudfront-accesslogs-enabled
- cloudfront-associated-with-waf
- cloudfront-custom-ssl-certificate
- cloudfront-default-root-object-konfiguriert
- cloudfront-no-deprecated-ssl-Protokolle
- cloudfront-origin-access-identity-aktiviert
- cloudfront-origin-failover-enabled
- Cloudfront-S3- origin-access-control-enabled
- cloudfront-security-policy-check
- cloudfront-sni-enabled
- cloudfront-ssl-policy-check
- cloudfront-traffic-to-origin-verschlüsselt
- cloudfront-viewer-policy-https
- cloudwatch-alarm-action-check
- cloudwatch-alarm-action-enabled-überprüfen
- cloudwatch-alarm-settings-check
- codebuild-project-artifact-encryption
- codebuild-project-environment-privileged-überprüfen
- codebuild-project-envvar-awscred-überprüfen
- codebuild-project-logging-enabled
- codebuild-project-s3-log-verschlüsselt
- codebuild-project-source-repo-URL-Prüfung
- codebuild-report-group-encrypted-im Ruhezustand
- codedeploy-auto-rollback-monitor-aktiviert
- codedeploy-deployment-group-auto-rollback-aktiviert
- codedeploy-deployment-group-outdated-instanzen-aktualisieren
- Codedeploy-ec2- minimum-healthy-hosts-configured
- codedeploy-lambda-allatonce-traffic-shift-deaktiviert
- codeguruprofiler-profiling-group-tagged
- codegururevieweer-repository-association-tagged

- codepipeline-deployment-count-check
- codepipeline-region-fanout-check
- cognito-identity-pool-unauth-Zugriffsprüfung
- cognito-user-pool-advanced-sicherheitsaktiviert
- cognito-user-pool-tagged
- connect-instance-logging-enabled
- customerprofiles-object-type-allow-Profilerstellung
- customerprofiles-object-type-tagged
- custom-eventbus-policy-attached
- datasync-task-data-verification-aktiviert
- datasync-task-logging-enabled
- datasync-task-tagged
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- dms-auto-minor-version-aktualisieren-Prüfung
- dms-endpoint-ssl-configured
- dms-endpoint-tagged
- dms-mongo-db-authentication-aktiviert
- dms-neptune-iam-authorization-aktiviert
- dms-redis-tls-enabled
- dms-replication-task-sourcedb-Protokollierung
- dms-replication-task-tagged
- dms-replication-task-targetdb-Protokollierung
- docdb-cluster-audit-logging-aktiviert
- docdb-cluster-backup-retention-überprüfen
- docdb-cluster-deletion-protection-aktiviert
- docdb-cluster-encrypted
- docdb-cluster-snapshot-public-verboten
- dynamodb-pitr-enabled

- dynamodb-table-deletion-protection-aktiviert
- dynamodb-table-encrypted-kms
- dynamodb-table-encryption-enabled
- ebs-optimized-instance
- ec2- capacity-reservation-tagged
- ec2- carrier-gateway-tagged
- ec2- aktiviert client-vpn-connection-log
- ec2- client-vpn-endpoint-tagged
- ec2- dhcp-options-tagged
- ec2- aktiviert enis-source-destination-check
- ec2-fleet-markiert
- ec2-imdsv2-check
- ec2- instance-detailed-monitoring-enabled
- ec2- instance-managed-by-ssm
- ec2- instance-multiple-eni-check
- ec2- instance-no-public-ip
- ec2- instance-profile-attached
- ec2-2-prüfen launch-template-imdsv
- ec2- -deaktiviert launch-template-public-ip
- ec2- launch-template-tagged
- ec2- managedinstance-applications-blacklisted
- ec2- managedinstance-applications-required
- ec2- prüfen managedinstance-association-compliance-status
- ec2- managedinstance-inventory-blacklisted
- ec2- prüfen managedinstance-patch-compliance-status
- ec2- managedinstance-platform-check
- ec2- Analyse mit Schlagwörtern network-insights-access-scope
- ec2 network-insights-access-scope - markiert
- ec2- network-insights-path-tagged
- ec2- no-amazon-key-pair

- ec2- paravirtual-instance-check
- ec2- prefix-list-tagged
- ec2-eni security-group-attached-to
- ec2- - spot-fleet-request-ct encryption-at-rest
- ec2- token-hop-limit-check
- ec2- traffic-mirror-filter-description
- ec2- traffic-mirror-filter-tagged
- ec2- traffic-mirror-session-description
- ec2- traffic-mirror-session-tagged
- ec2- traffic-mirror-target-description
- ec2- traffic-mirror-target-tagged
- ec2- -attach-deaktiviert transit-gateway-auto-vpc
- ec2 transit-gateway-multicast-domain - markiert
- ec2- volume-inuse-check
- ec2- vpn-connection-logging-enabled
- ecr-private-lifecycle-policy-konfiguriert
- ecr-private-tag-immutability-aktiviert
- ecr-repository-cmk-encryption-aktiviert
- ecr-repository-tagged
- ecs-awsvpc-networking-enabled
- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-container-insights-enabled
- ecs-fargate-latest-platform-Version
- ecs-no-environment-secrets
- ecs-task-definition-log-Konfiguration
- ecs-task-definition-memory-hartes Limit
- ecs-task-definition-network-mode-not-host
- ecs-task-definition-nonroot-Benutzer
- ecs-task-definition-pid-Modus-Check

- ecs-task-definition-user-for-host-mode-check
- efs-access-point-enforce-Stammverzeichnis
- efs-access-point-enforce-Benutzeridentität
- efs-automatic-backups-enabled
- efs-filesystem-ct-encrypted
- eip-attached
- eks-cluster-log-enabled
- eks-cluster-oldest-supported-Version
- eks-cluster-supported-version
- elasticbeanstalk-application-description
- elasticbeanstalk-application-version-description
- elasticbeanstalk-environment-description
- elasticsearch-logs-to-cloudwatch
- elasticsearch-node-to-node-Verschlüsselungsprüfung
- elastic-beanstalk-logs-to- Cloudwatch
- elastic-beanstalk-managed-updates-aktiviert
- elbv2- listener-encryption-in-transit
- elbv2-multiple-az
- elbv2- prüfen predefined-security-policy-ssl
- elb-acm-certificate-required
- elb-cross-zone-load-Balancing aktiviert
- elb-custom-security-policy-ssl-Prüfung
- elb-deletion-protection-enabled
- elb-logging-enabled
- elb-predefined-security-policy-ssl-Überprüfung
- elb-tls-https-listeners-nur
- emr-security-configuration-encryption-ruh dich aus
- emr-security-configuration-encryption-Transit
- encrypted-volumes
- evidently-launch-description

- evidently-launch-tagged
- evidently-project-description
- evidently-project-tagged
- evidently-segment-description
- evidently-segment-tagged
- fis-experiment-template-log-Konfiguration vorhanden
- fis-experiment-template-tagged
- fms-shield-resource-policy-überprüfen
- fms-webacl-resource-policy-überprüfen
- fms-webacl-rulegroup-association-überprüfen
- frauddetector-entity-type-tagged
- frauddetector-label-tagged
- frauddetector-outcome-tagged
- frauddetector-variable-tagged
- glb-listener-tagged
- global-endpoint-event-replication-aktiviert
- glue-job-logging-enabled
- glue-ml-transform-encrypted-im Ruhezustand
- glue-spark-job-supported-Ausführung
- iam-customer-policy-blocked-kms-Aktionen
- iam-group-has-users-überprüfen
- iam-inline-policy-blocked-KMS-Aktionen
- iam-no-inline-policy-überprüfen
- iam-oidc-provider-tagged
- iam-policy-blacklisted-check
- iam-policy-no-statements-with-admin-access
- iam-policy-no-statements-with-full-access
- iam-role-managed-policy-überprüfen
- iam-saml-provider-tagged
- iam-server-certificate-tagged

- iam-user-group-membership-überprüfen
- iam-user-no-policies-überprüfen
- instances-in-vpc
- internet-gateway-authorized-vpc-nur
- iotevents-alarm-model-tagged
- iotevents-detector-model-tagged
- iotevents-input-tagged
- iotsitewise-asset-model-tagged
- iotsitewise-dashboard-tagged
- iotsitewise-gateway-tagged
- iotsitewise-portal-tagged
- iotsitewise-project-tagged
- iottwinmaker-component-type-tagged
- iottwinmaker-entity-tagged
- iottwinmaker-scene-tagged
- iottwinmaker-sync-job-tagged
- iottwinmaker-workspace-tagged
- iotwireless-fuota-task-tagged
- iotwireless-multicast-group-tagged
- iotwireless-service-profile-tagged
- iot-authorizer-token-signing-aktiviert
- ivs-channel-playback-authorization-aktiviert
- ivs-channel-tagged
- ivs-playback-key-pair-markiert
- ivs-recording-configuration-tagged
- kinesis-stream-backup-retention-überprüfen
- kinesis-stream-encrypted
- kms-key-policy-no-öffentlich zugänglich
- lambda-concurrency-check
- lambda-dlq-check

- lambda-function-public-access-verboten
- lambda-function-settings-check
- lambda-function-xray-enabled
- lambda-inside-vpc
- lambda-vpc-multi-az-überprüfen
- lightsail-bucket-tagged
- lightsail-certificate-tagged
- lightsail-disk-tagged
- mq-active-broker-ldap-Authentifizierung
- mq-active-deployment-mode
- mq-active-single-instance-broker-storage-type-efs
- mq-auto-minor-version-Upgrade aktiviert
- mq-broker-general-logging-aktiviert
- mq-cloudwatch-audit-log-aktiviert
- mq-rabbit-deployment-mode
- msk-cluster-public-access-deaktiviert
- msk-connect-connector-logging-aktiviert
- msk-enhanced-monitoring-enabled
- msk-in-cluster-node-require-tls
- msk-unrestricted-access-check
- nacl-no-unrestricted-ssh-rdp
- neptune-cluster-backup-retention-überprüfen
- neptune-cluster-cloudwatch-log-exportfähig
- neptune-cluster-copy-tags-to-snapshot-enabled
- neptune-cluster-deletion-protection-aktiviert
- neptune-cluster-encrypted
- neptune-cluster-iam-database-Authentifizierung
- neptune-cluster-multi-az-aktiviert
- neptune-cluster-snapshot-encrypted
- neptune-cluster-snapshot-public-verboten

- netfw-deletion-protection-enabled
- netfw-multi-az-enabled
- netfw-policy-default-action-fragment-Pakete
- netfw-policy-default-action-vollständige Pakete
- netfw-policy-rule-group-assoziiert
- netfw-stateless-rule-group-nicht leer
- netfw-subnet-change-protection-aktiviert
- nlb-cross-zone-load-Balancing aktiviert
- nlb-internal-scheme-check
- nlb-listener-tagged
- no-unrestricted-route-to-igw
- opensearch-access-control-enabled
- opensearch-audit-logging-enabled
- opensearch-data-node-fault-Toleranz
- opensearch-encrypted-at-rest
- opensearch-https-required
- opensearch-in-vpc-only
- opensearch-logs-to-cloudwatch
- opensearch-node-to-node-Verschlüsselungsprüfung
- opensearch-primary-node-fault-Toleranz
- opensearch-update-check
- rabbit-mq-supported-version
- rds-aurora-mysql-audit-Protokollierung aktiviert
- rds-aurora-postgresql-logs-zu-Cloud-Watch
- rds-automatic-minor-version-upgrade-fähig
- rds-cluster-auto-minor-version-upgrade-enable
- rds-cluster-default-admin-überprüfen
- rds-cluster-deletion-protection-aktiviert
- rds-cluster-encrypted-at-ausruhen
- rds-cluster-iam-authentication-aktiviert

- rds-cluster-multi-az-aktiviert
- rds-db-security-group-nicht erlaubt
- rds-enhanced-monitoring-enabled
- rds-instance-default-admin-überprüfen
- rds-instance-deletion-protection-aktiviert
- rds-instance-iam-authentication-aktiviert
- rds-instance-public-access-überprüfen
- rds-logging-enabled
- rds-multi-az-support
- rds-postgresql-logs-to- Cloudwatch
- rds-snapshots-public-prohibited
- rds-snapshot-encrypted
- rds-sql-server-logs-zu-Cloud-Watch
- rds-storage-encrypted
- redshift-audit-logging-enabled
- redshift-backup-enabled
- redshift-cluster-configuration-check
- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check
- redshift-cluster-multi-az-aktiviert
- redshift-cluster-parameter-group-markiert
- redshift-cluster-public-access-überprüfen
- redshift-cluster-subnet-group-Multi-Az
- redshift-default-admin-check
- redshift-default-db-name-überprüfen
- redshift-enhanced-vpc-routing-aktiviert
- redshift-require-tls-ssl
- required-tags
- Route 53- query-logging-enabled
- s3 -regel-check express-dir-bucket-lifecycle

- nur s3- access-point-in-vpc
- s3- -Blöcke access-point-public-access
- s3- -Blöcke account-level-public-access
- s-3 bucket-acl-prohibited
- s-3 bucket-blacklisted-actions-prohibited
- s3- bucket-cross-region-replication -aktiviert
- s-3 bucket-default-lock-enabled
- s3 bucket-level-public-access - verboten
- s3- bucket-logging-enabled
- s-3 bucket-mfa-delete-enabled
- s-3 bucket-policy-grantee-check
- s3- bucket-policy-not-more -freizügig
- s 3- bucket-replication-enabled
- s3- bucket-server-side-encryption -aktiviert
- s-3 bucket-ssl-requests-only
- s3-Bucket-Tagged
- s-3 bucket-versioning-enabled
- s-3 default-encryption-kms
- s-3 event-notifications-enabled
- s-3 lifecycle-policy-check
- s-3 version-lifecycle-policy-check
- sagemaker-app-image-config-markiert
- sagemaker-domain-in-vpc
- sagemaker-domain-tagged
- sagemaker-feature-group-tagged
- sagemaker-image-description
- sagemaker-image-tagged
- sagemaker-model-in-vpc
- sagemaker-model-isolation-enabled
- sagemaker-notebook-instance-inside-vpc

- sagemaker-notebook-instance-root-Zugriffsprüfung
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-prüfen
- secretsmanager-using-cmk
- service-catalog-shared-within-Organisation
- sns-encrypted-kms
- sns-topic-message-delivery-Benachrichtigung aktiviert
- sns-topic-no-public-Zugriff
- sqs-queue-no-public-Zugang
- ssm-document-tagged
- step-functions-state-machine-Protokollierung aktiviert
- subnet-auto-assign-public-ip-deaktiviert
- transfer-agreement-description
- transfer-agreement-tagged
- transfer-certificate-description
- transfer-certificate-tagged
- transfer-connector-logging-enabled
- transfer-connector-tagged
- transfer-profile-tagged
- transfer-workflow-description
- transfer-workflow-tagged
- vpc-default-security-group-geschlossen
- vpc-network-acl-unused-überprüfen
- vpc-peering-dns-resolution-überprüfen
- vpc-vpn-2-tunnels-up
- WAF 2- rulegroup-logging-enabled
- WAF 2- rulegroup-not-empty
- WAF 2- webacl-not-empty
- waf-global-rulegroup-not-leer
- waf-global-rule-not-leer

- waf-global-webacl-not-leer
- waf-regional-rulegroup-not-leer
- waf-regional-rule-not-leer
- waf-regional-webacl-not-leer
- workspaces-root-volume-encryption-aktiviert
- workspaces-user-volume-encryption-aktiviert

Regelmäßig

Periodische Regeln sind Regeln, die in regelmäßigen Abständen mit einer von Ihnen festgelegten Häufigkeit AWS Config ausgewertet werden, z. B. alle 24 Stunden.

Regelmäßig

- access-keys-rotated
- account-part-of-organizations
- acm-pca-root-ca-deaktiviert
- alb-http-to-https-Umleitungsprüfung
- api-gwv2- authorization-type-configured
- appsync-associated-with-waf
- appsync-cache-encryption-at-ausruhen
- aurora-last-backup-recovery-Punkt erstellt
- aurora-meets-restore-time-Ziel
- aurora-mysql-cluster-audit-Protokollierung
- aurora-resources-in-logically-air-gapped-vault
- aurora-resources-protected-by-Backup-Plan
- Cloudfront-S3- origin-non-existent-bucket
- cloudtrail-all-read-s3- data-event-check
- cloudtrail-all-write-s3- data-event-check
- Wolkenspur-S3- bucket-access-logging
- CloudTrail-S3- bucket-public-access-prohibited
- cloudtrail-s3-dataevents-enabled

- cloudtrail-security-trail-enabled
- cloudwatch-alarm-resource-check
- cloudwatch-log-group-encrypted
- cloud-trail-cloud-watch-logs-aktiviert
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-Validierung aktiviert
- cmk-backing-key-rotation-aktiviert
- custom-schema-registry-policy-angehängt
- cw-loggroup-retention-period-überprüfen
- dax-encryption-enabled
- dax-tls-endpoint-encryption
- dms-replication-not-public
- docdb-cluster-encrypted-in-Durchreise
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-last-backup-recovery-Punkt erstellt
- dynamodb-meets-restore-time-Ziel
- dynamodb-resources-protected-by-Backup-Plan
- dynamodb-throughput-limit-check
- ebs-in-backup-plan
- ebs-last-backup-recovery-Punkt erstellt
- ebs-meets-restore-time-Ziel
- ebs-resources-in-logically-air-gapped-vault
- ebs-resources-protected-by-Backup-Plan
- ebs-snapshot-public-restorable-überprüfen
- ec2- -alle client-vpn-not-authorize
- ec2- ebs-encryption-by-default
- ec2- erstellt last-backup-recovery-point
- ec2- meets-restore-time-target

- ec2- -Tresor mit Lücken resources-in-logically-air
- ec2- resources-protected-by-backup -plan
- ec2- -einperiodisch security-group-attached-to
- ec2-stopped-instance
- ecr-private-image-scanning-aktiviert
- efs-encrypted-check
- efs-in-backup-plan
- efs-last-backup-recovery-punkt-erstellt
- efs-meets-restore-time-Ziel
- efs-mount-target-public-zugänglich
- efs-resources-in-logically-air-gapped-vault
- efs-resources-protected-by-Backup-Plan
- eks-cluster-logging-enabled
- eks-cluster-secrets-encrypted
- eks-endpoint-no-public-Zugang
- eks-secrets-encrypted
- elasticache-auto-minor-version-Upgrade-Check
- elasticache-rbac-auth-enabled
- elasticache-redis-cluster-automatic-Backup-Check
- elasticache-repl-grp-auto-failover-fähig
- elasticache-repl-grp-encrypted-im Ruhezustand
- elasticache-repl-grp-encryptedim Transit
- elasticache-repl-grp-redis-auth-aktiviert
- elasticache-subnet-group-check
- elasticache-supported-engine-version
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elbv2- acm-certificate-required
- emr-block-public-access
- emr-kerberos-enabled

- emr-master-no-public-ip
- event-data-store-cmk-Verschlüsselung aktiviert
- fsx-last-backup-recovery-punkt-erstellt
- fsx-lustre-copy-tagszu Backups
- fsx-meets-restore-time-Ziel
- fsx-ontap-deployment-type-überprüfen
- fsx-openzfs-copy-tags-aktiviert
- fsx-openzfs-deployment-type-überprüfen
- fsx-resources-protected-by-Ersatzplan
- fsx-windows-audit-log-konfiguriert
- fsx-windows-deployment-type-überprüfen
- GuardDuty-EC2- protection-runtime-enabled
- guardduty-ecs-protection-runtime-aktiviert
- guardduty-eks-protection-audit-aktiviert
- guardduty-eks-protection-runtime-aktiviert
- guardduty-enabled-centralized
- guardduty-lambda-protection-enabled
- guardduty-malware-protection-enabled
- guardduty-non-archived-findings
- guardduty-rds-protection-enabled
- guardduty-runtime-monitoring-enabled
- GuardDuty-S3-Schutz aktiviert
- iam-external-access-analyzer-aktiviert
- iam-password-policy
- iam-policy-in-use
- iam-root-access-key-überprüfen
- iam-server-certificate-expiration-überprüfen
- iam-user-mfa-enabled
- iam-user-unused-credentials-überprüfen
- inspector-ec2-Scan aktiviert

- inspector-ecr-scan-enabled
- inspector-lambda-code-scan-aktiviert
- inspector-lambda-standard-scan-aktiviert
- kinesis-firehose-delivery-stream-verschlüsselt
- kms-cmk-not-scheduled-zum Löschen
- macie-auto-sensitive-data-Discovery-Check
- macie-status-check
- mariadb-publish-logs-to-Cloudwatch-Protokolle
- mfa-enabled-for-iam-Konsolenzugriff
- mq-automatic-minor-version-Upgrade aktiviert
- mq-cloudwatch-audit-logging-aktiviert
- mq-no-public-access
- multi-region-cloud-trail-aktiviert
- netfw-logging-enabled
- nlb-logging-enabled
- rds-instance-subnet-igw-überprüfen
- rds-in-backup-plan
- rds-last-backup-recovery-Punkt erstellt
- rds-mariadb-instance-encryptedim Transit
- rds-meets-restore-time-Ziel
- rds-mysql-instance-encryptedunterwegs
- rds-postgres-instance-encryptedim Transit
- rds-proxy-tls-encryption
- rds-resources-protected-by-Backup-Plan
- rds-sqlserver-encrypted-in-Transit
- redshift-serverless-default-admin-überprüfen
- redshift-serverless-default-db-Namenscheck
- redshift-serverless-namespace-cmk-Verschlüsselung
- redshift-serverless-publish-logs-zu-Cloud-Watch
- redshift-serverless-workgroup-encryptedauf dem Weg

- redshift-serverless-workgroup-no-öffentlich zugänglich
- redshift-serverless-workgroup-routes-innerhalb von VPC
- redshift-unrestricted-port-access
- root-account-hardware-mfa-aktiviert
- root-account-mfa-enabled
- s3- -Blocke-periodisch account-level-public-access
- s3- -erstellt last-backup-recovery-point
- s3- meets-restore-time-target
- s3- resources-in-logically-air -Tresor mit Lücken
- s3 resources-protected-by-backup - -Plan
- sagemaker-endpoint-configuration-kms-Schlüssel konfiguriert
- sagemaker-endpoint-config-prod-Anzahl der Instanzen
- sagemaker-notebook-instance-kms-key-konfiguriert
- sagemaker-notebook-instance-platform-Version
- sagemaker-notebook-no-direct-Internetzugang
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- securityhub-enabled
- security-account-information-provided
- service-vpc-endpoint-enabled
- ses-malware-scanning-enabled
- shield-advanced-enabled-autorenew
- shield-drt-access
- ssm-automation-block-public-teilen
- ssm-automation-logging-enabled
- ssm-document-not-public
- storagegateway-last-backup-recovery-Punkt erstellt
- storagegateway-resources-in-logically-air-gapped-vault
- storagegateway-resources-protected-by-Ersatzplan
- transfer-family-server-no-ftp

- virtualmachine-last-backup-recovery-Punkt erstellt
- virtualmachine-resources-in-logically-air-gapped-vault
- virtualmachine-resources-protected-by-Ersatzplan
- vpc-endpoint-enabled
- vpc-flow-logs-enabled
- vpc-sg-port-restriction-überprüfen
- wafv2-logging-enabled
- waf-classic-logging-enabled

Hybrid

Hybridregeln sind Regeln, die sowohl als Reaktion auf Konfigurationsänderungen als auch in regelmäßigen Abständen AWS Config ausgewertet werden.

Hybrid

- acm-certificate-expiration-check
- cloudformation-stack-drift-detection-überprüfen
- ec2- -ami instance-launched-with-allowed
- incoming-ssh-disabled
- restricted-incoming-traffic
- s-3 bucket-public-read-prohibited
- s-3 bucket-public-write-prohibited
- vpc-sg-open-only-to-authorized-ports

Liste der AWS Config verwalteten Regeln nach Regionen und Verfügbarkeit

AWS Config unterstützt derzeit die folgenden verwalteten Regeln. Bevor Sie diese Regeln verwenden, finden Sie weitere Informationen unterÜberlegungen.

Region USA Ost (Ohio)

USA Ost (Ohio)

- access-keys-rotated

- account-part-of-organizations
- acmpca-certificate-authority-tagged
- acm-certificate-expiration-check
- acm-certificate-rsa-check
- acm-pca-root-ca-deaktiviert
- active-mq-supported-version
- alb-desync-mode-check
- alb-http-drop-invalid-Header-fähig
- alb-http-to-https-Umleitungsprüfung
- alb-internal-scheme-check
- alb-listener-tagged
- alb-waf-enabled
- amplify-app-branch-auto-löschung aktiviert
- amplify-app-description
- amplify-app-tagged
- amplify-branch-performance-mode-aktiviert
- amplify-branch-tagged
- api-gwv2- access-logs-enabled
- api-gwv2- authorization-type-configured
- api-gw-associated-with-WAF
- api-gw-cache-enabled-und-verschlüsselt
- api-gw-endpoint-type-überprüfen
- api-gw-execution-logging-aktiviert
- api-gw-ssl-enabled
- api-gw-xray-enabled
- appconfig-application-description
- appconfig-application-tagged
- appconfig-configuration-profile-tagged
- appconfig-configuration-profile-validators-nicht leer
- appconfig-deployment-strategy-description

- appconfig-deployment-strategy-replicate-zu-ssm
- appconfig-environment-description
- appconfig-environment-tagged
- appconfig-extension-association-tagged
- appconfig-freeform-profile-config-Speicher
- appconfig-hosted-configuration-version-Beschreibung
- appflow-flow-tagged
- appmesh-gateway-route-tagged
- appmesh-mesh-deny-tcp-Weiterleitung
- appmesh-mesh-tagged
- appmesh-route-tagged
- appmesh-virtual-gateway-backend-Standardeinstellungen-TLS
- appmesh-virtual-gateway-logging-file-path-exists
- appmesh-virtual-gateway-tagged
- appmesh-virtual-node-backend-defaults-tls-on
- appmesh-virtual-node-logging-file-path-exists
- appmesh-virtual-node-tagged
- appmesh-virtual-router-tagged
- appmesh-virtual-service-tagged
- approved-amis-by-id
- approved-amis-by-tag
- apprunner-service-in-vpc
- apprunner-service-no-public-Zugang
- apprunner-service-observability-enabled
- apprunner-service-tagged
- apprunner-vpc-connector-tagged
- appstream-fleet-in-vpc
- appsync-associated-with-waf
- appsync-authorization-check
- appsync-cache-encryption-at-ausruhen

- appsync-logging-enabled
- athena-data-catalog-description
- athena-prepared-statement-description
- athena-workgroup-description
- athena-workgroup-encrypted-at-ausruhen
- athena-workgroup-enforce-workgroup-Konfiguration
- athena-workgroup-engine-version-automatisches Upgrade
- athena-workgroup-logging-enabled
- aurora-last-backup-recovery-punkt-erstellt
- aurora-meets-restore-time-Ziel
- aurora-mysql-backtracking-enabled
- aurora-mysql-cluster-audit-Protokollierung
- aurora-resources-in-logically-air-gapped-vault
- aurora-resources-protected-by-Backup-Plan
- autoscaling-capacity-rebalancing
- autoscaling-group-elb-healthcheck-erforderlich
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-hop-Grenze
- autoscaling-launch-config-public-ip-deaktiviert
- autoscaling-launch-template
- autoscaling-multiple-az
- autoscaling-multiple-instance-types
- backup-plan-min-frequency-and-min-retention-check
- backup-recovery-point-encrypted
- backup-recovery-point-manual-Löschen-deaktiviert
- backup-recovery-point-minimum-Aufbewahrungsprüfung
- batch-compute-environment-enabled
- batch-compute-environment-managed
- batch-compute-environment-tagged
- batch-job-queue-enabled

- batch-job-queue-tagged
- batch-managed-compute-environment-using-launch-template
- batch-managed-compute-env-compute-resources-tagged
- batch-scheduling-policy-tagged
- beanstalk-enhanced-health-reporting-aktiviert
- cassandra-keyspace-tagged
- clb-desync-mode-check
- clb-multiple-az
- cloudformation-stack-drift-detection-überprüfen
- cloudformation-stack-notification-check
- cloudtrail-all-read-s3- data-event-check
- cloudtrail-all-write-s3- data-event-check
- Wolkenspur-S3- bucket-access-logging
- cloudtrail-s3- bucket-public-access-prohibited
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-action-enabled-überprüfen
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted
- cloud-trail-cloud-watch-logs-aktiviert
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-Validierung aktiviert
- cmk-backing-key-rotation-aktiviert
- codebuild-project-artifact-encryption
- codebuild-project-environment-privileged-überprüfen
- codebuild-project-envvar-awscred-überprüfen
- codebuild-project-logging-enabled

- codebuild-project-s3-log-verschlüsselt
- codebuild-project-source-repo-URL-Prüfung
- codebuild-report-group-encrypted-im Ruhezustand
- codedeploy-auto-rollback-monitor-aktiviert
- codedeploy-deployment-group-auto-rollback-aktiviert
- codedeploy-deployment-group-outdated-instanzen-aktualisieren
- Codedeploy-ec2- minimum-healthy-hosts-configured
- codedeploy-lambda-allatonce-traffic-shift-deaktiviert
- codeguruprofiler-profiling-group-tagged
- codegururevieweer-repository-association-tagged
- codepipeline-deployment-count-check
- codepipeline-region-fanout-check
- cognito-identity-pool-unauth-Zugriffsprüfung
- cognito-user-pool-advanced-sicherheitsaktiviert
- cognito-user-pool-tagged
- custom-eventbus-policy-attached
- custom-schema-registry-policy-angehängt
- cw-loggroup-retention-period-überprüfen
- datasync-task-data-verification-aktiviert
- datasync-task-logging-enabled
- datasync-task-tagged
- dax-encryption-enabled
- dax-tls-endpoint-encryption
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- dms-auto-minor-version-aktualisieren-Prüfung
- dms-endpoint-ssl-configured
- dms-endpoint-tagged
- dms-mongo-db-authentication-aktiviert

- dms-neptune-iam-authorization-aktiviert
- dms-redis-tls-enabled
- dms-replication-not-public
- dms-replication-task-sourcedb-Protokollierung
- dms-replication-task-tagged
- dms-replication-task-targetdb-Protokollierung
- docdb-cluster-audit-logging-aktiviert
- docdb-cluster-backup-retention-überprüfen
- docdb-cluster-deletion-protection-aktiviert
- docdb-cluster-encrypted
- docdb-cluster-encrypted-in-transit
- docdb-cluster-snapshot-public-verboten
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-last-backup-recovery-Punkt erstellt
- dynamodb-meets-restore-time-Ziel
- dynamodb-pitr-enabled
- dynamodb-resources-protected-by-Backup-Plan
- dynamodb-table-deletion-protection-aktiviert
- dynamodb-table-encrypted-kms
- dynamodb-table-encryption-enabled
- dynamodb-throughput-limit-check
- ebs-in-backup-plan
- ebs-last-backup-recovery-punkt-erstellt
- ebs-meets-restore-time-Ziel
- ebs-optimized-instance
- ebs-resources-in-logically-air-gapped-vault
- ebs-resources-protected-by-Backup-Plan
- ebs-snapshot-public-restorable-überprüfen
- ec2- capacity-reservation-tagged

- ec2- carrier-gateway-tagged
- ec2- aktiviert client-vpn-connection-log
- ec2- client-vpn-endpoint-tagged
- ec2- -alle client-vpn-not-authorize
- ec2- dhcp-options-tagged
- ec2- ebs-encryption-by-default
- ec2- aktiviert enis-source-destination-check
- ec2-fleet-markiert
- ec2-imdsv2-check
- ec2- instance-detailed-monitoring-enabled
- ec2-ami instance-launched-with-allowed
- ec2- instance-managed-by-ssm
- ec2- instance-multiple-eni-check
- ec2- instance-no-public-ip
- ec2- instance-profile-attached
- ec2- erstellt last-backup-recovery-point
- ec2-2-prüfen launch-template-imdsv
- ec2- -deaktiviert launch-template-public-ip
- ec2- launch-template-tagged
- ec2- managedinstance-applications-blacklisted
- ec2- managedinstance-applications-required
- ec2- prüfen managedinstance-association-compliance-status
- ec2- managedinstance-inventory-blacklisted
- ec2- prüfen managedinstance-patch-compliance-status
- ec2- managedinstance-platform-check
- ec2- meets-restore-time-target
- ec2- Analyse mit Schlagwörtern network-insights-access-scope
- ec2 network-insights-access-scope - markiert
- ec2- network-insights-path-tagged
- ec2- no-amazon-key-pair

- ec2- prefix-list-tagged
- ec2- -Tresor mit Lücken resources-in-logically-air
- ec2- resources-protected-by-backup -plan
- ec2-eni security-group-attached-to
- ec2- -eni-periodisch security-group-attached-to
- ec2-stopped-instance
- ec2- token-hop-limit-check
- ec2- traffic-mirror-filter-description
- ec2- traffic-mirror-filter-tagged
- ec2- traffic-mirror-session-description
- ec2- traffic-mirror-session-tagged
- ec2- traffic-mirror-target-description
- ec2- traffic-mirror-target-tagged
- ec2- -attach-deaktiviert transit-gateway-auto-vpc
- ec2 transit-gateway-multicast-domain - markiert
- ec2- volume-inuse-check
- ec2- vpn-connection-logging-enabled
- ecr-private-image-scanning-aktiviert
- ecr-private-lifecycle-policy-konfiguriert
- ecr-private-tag-immutability-aktiviert
- ecr-repository-cmk-encryption-aktiviert
- ecr-repository-tagged
- ecs-awsvpc-networking-enabled
- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-container-insights-enabled
- ecs-fargate-latest-platform-Version
- ecs-no-environment-secrets
- ecs-task-definition-log-Konfiguration
- ecs-task-definition-memory-hartes Limit

- ecs-task-definition-network-mode-not-host
- ecs-task-definition-nonroot-Benutzer
- ecs-task-definition-pid-Modus-Check
- ecs-task-definition-user-for-host-mode-check
- efs-access-point-enforce-Stammverzeichnis
- efs-access-point-enforce-Benutzeridentität
- efs-automatic-backups-enabled
- efs-encrypted-check
- efs-filesystem-ct-encrypted
- efs-in-backup-plan
- efs-last-backup-recovery-Punkt erstellt
- efs-meets-restore-time-Ziel
- efs-mount-target-public-zugänglich
- efs-resources-in-logically-air-gapped-vault
- efs-resources-protected-by-Backup-Plan
- eip-attached
- eks-cluster-logging-enabled
- eks-cluster-log-enabled
- eks-cluster-oldest-supported-Ausführung
- eks-cluster-secrets-encrypted
- eks-cluster-supported-version
- eks-endpoint-no-public-Zugang
- eks-secrets-encrypted
- elasticache-auto-minor-version-Upgrade-Check
- elasticache-rbac-auth-enabled
- elasticache-redis-cluster-automatic-Backup-Check
- elasticache-repl-grp-auto-failover-fähig
- elasticache-repl-grp-encrypted-im Ruhezustand
- elasticache-repl-grp-encryptedunterwegs
- elasticache-repl-grp-redis-auth-aktiviert

- elasticache-subnet-group-check
- elasticache-supported-engine-version
- elasticbeanstalk-application-description
- elasticbeanstalk-application-version-description
- elasticbeanstalk-environment-description
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch
- elasticsearch-node-to-node-Verschlüsselungsprüfung
- elastic-beanstalk-logs-to- Cloudwatch
- elastic-beanstalk-managed-updates-aktiviert
- elbv2- acm-certificate-required
- elv 2- listener-encryption-in-transit
- elbv2-multiple-az
- elbv2- prüfen predefined-security-policy-ssl
- elb-acm-certificate-required
- elb-cross-zone-load-Balancing aktiviert
- elb-custom-security-policy-ssl-Überprüfung
- elb-deletion-protection-enabled
- elb-logging-enabled
- elb-predefined-security-policy-SSL-Überprüfung
- elb-tls-https-listeners-nur
- emr-block-public-access
- emr-kerberos-enabled
- emr-master-no-public-ip
- emr-security-configuration-encryption-ruh dich aus
- emr-security-configuration-encryption-Transit
- encrypted-volumes
- event-data-store-cmk-Verschlüsselung aktiviert
- evidently-launch-description

- evidently-launch-tagged
- evidently-project-description
- evidently-project-tagged
- evidently-segment-description
- evidently-segment-tagged
- fis-experiment-template-log-Konfiguration ist vorhanden
- fis-experiment-template-tagged
- fms-shield-resource-policy-überprüfen
- fms-webacl-resource-policy-überprüfen
- fms-webacl-rulegroup-association-überprüfen
- frauddetector-entity-type-tagged
- frauddetector-label-tagged
- frauddetector-outcome-tagged
- frauddetector-variable-tagged
- fsx-last-backup-recovery-Punkt erstellt
- fsx-lustre-copy-tagszu Backups
- fsx-meets-restore-time-Ziel
- fsx-ontap-deployment-type-überprüfen
- fsx-openzfs-copy-tags-aktiviert
- fsx-openzfs-deployment-type-überprüfen
- fsx-resources-protected-by-Ersatzplan
- fsx-windows-audit-log-konfiguriert
- fsx-windows-deployment-type-überprüfen
- glb-listener-tagged
- global-endpoint-event-replication-aktiviert
- glue-job-logging-enabled
- glue-ml-transform-encrypted-im Ruhezustand
- glue-spark-job-supported-Ausführung
- GuardDuty-EC2- protection-runtime-enabled
- guardduty-ecs-protection-runtime-aktiviert

- guardduty-eks-protection-audit-aktiviert
- guardduty-eks-protection-runtime-aktiviert
- guardduty-enabled-centralized
- guardduty-lambda-protection-enabled
- guardduty-malware-protection-enabled
- guardduty-non-archived-findings
- guardduty-rds-protection-enabled
- guardduty-runtime-monitoring-enabled
- GuardDuty-S3-Schutz aktiviert
- iam-customer-policy-blocked-kms-Aktionen
- iam-external-access-analyzer-aktiviert
- iam-group-has-users-überprüfen
- iam-inline-policy-blocked-kms-Aktionen
- iam-no-inline-policy-überprüfen
- iam-password-policy
- iam-policy-blacklisted-check
- iam-policy-in-use
- iam-policy-no-statements-with-admin-access
- iam-policy-no-statements-with-full-access
- iam-role-managed-policy-überprüfen
- iam-root-access-key-überprüfen
- iam-user-group-membership-überprüfen
- iam-user-mfa-enabled
- iam-user-no-policies-überprüfen
- iam-user-unused-credentials-überprüfen
- incoming-ssh-disabled
- inspector-ec2-Scan aktiviert
- inspector-ecr-scan-enabled
- inspector-lambda-code-scan-aktiviert
- inspector-lambda-standard-scan-aktiviert

- instances-in-vpc
- internet-gateway-authorized-vpc-nur
- iotevents-alarm-model-tagged
- iotevents-detector-model-tagged
- iotevents-input-tagged
- iotsitewise-asset-model-tagged
- iotsitewise-dashboard-tagged
- iotsitewise-gateway-tagged
- iotsitewise-portal-tagged
- iotsitewise-project-tagged
- iot-authorizer-token-signing-aktiviert
- kinesis-firehose-delivery-stream-verschlüsselt
- kinesis-stream-backup-retention-überprüfen
- kinesis-stream-encrypted
- kms-cmk-not-scheduled-zum Löschen
- kms-key-policy-no-öffentlicher Zugang
- lambda-concurrency-check
- lambda-dlq-check
- lambda-function-public-access-verboten
- lambda-function-settings-check
- lambda-function-xray-enabled
- lambda-inside-vpc
- lambda-vpc-multi-az-überprüfen
- lightsail-bucket-tagged
- lightsail-certificate-tagged
- lightsail-disk-tagged
- macie-auto-sensitive-data-Discovery-Check
- macie-status-check
- mariadb-publish-logs-to-Cloudwatch-Protokolle
- mfa-enabled-for-iam-Konsolenzugriff

- mq-active-broker-ldap-Authentifizierung
- mq-active-deployment-mode
- mq-active-single-instance-broker-storage-type-efs
- mq-automatic-minor-version-Upgrade aktiviert
- mq-auto-minor-version-upgrade-fähig
- mq-broker-general-logging-aktiviert
- mq-cloudwatch-audit-logging-aktiviert
- mq-cloudwatch-audit-log-aktiviert
- mq-no-public-access
- mq-rabbit-deployment-mode
- msk-cluster-public-access-deaktiviert
- msk-connect-connector-logging-aktiviert
- msk-enhanced-monitoring-enabled
- msk-in-cluster-node-require-tls
- msk-unrestricted-access-check
- multi-region-cloud-trail-aktiviert
- nacl-no-unrestricted-ssh-rdp
- neptune-cluster-backup-retention-überprüfen
- neptune-cluster-cloudwatch-log-exportfähig
- neptune-cluster-copy-tags-to-snapshot-enabled
- neptune-cluster-deletion-protection-aktiviert
- neptune-cluster-encrypted
- neptune-cluster-iam-database-Authentifizierung
- neptune-cluster-multi-az-aktiviert
- neptune-cluster-snapshot-encrypted
- neptune-cluster-snapshot-public-verboten
- netfw-deletion-protection-enabled
- netfw-logging-enabled
- netfw-multi-az-enabled
- netfw-policy-default-action-fragment-Pakete

- netfw-policy-default-action-vollständige Pakete
- netfw-policy-rule-group-assoziiert
- netfw-stateless-rule-group-nicht leer
- netfw-subnet-change-protection-aktiviert
- nlb-cross-zone-load-Balancing aktiviert
- nlb-internal-scheme-check
- nlb-listener-tagged
- nlb-logging-enabled
- no-unrestricted-route-to-igw
- opensearch-access-control-enabled
- opensearch-audit-logging-enabled
- opensearch-data-node-fault-Toleranz
- opensearch-encrypted-at-rest
- opensearch-https-required
- opensearch-in-vpc-only
- opensearch-logs-to-cloudwatch
- opensearch-node-to-node-Verschlüsselungsprüfung
- opensearch-primary-node-fault-Toleranz
- opensearch-update-check
- rabbit-mq-supported-version
- rds-aurora-mysql-audit-Protokollierung aktiviert
- rds-aurora-postgresql-logs-zu-Cloud-Watch
- rds-automatic-minor-version-upgrade-fähig
- rds-cluster-auto-minor-version-upgrade-enable
- rds-cluster-default-admin-überprüfen
- rds-cluster-deletion-protection-aktiviert
- rds-cluster-encrypted-at-ausruhen
- rds-cluster-iam-authentication-aktiviert
- rds-cluster-multi-az-aktiviert
- rds-enhanced-monitoring-enabled

- rds-instance-default-admin-überprüfen
- rds-instance-deletion-protection-aktiviert
- rds-instance-iam-authentication-aktiviert
- rds-instance-public-access-überprüfen
- rds-instance-subnet-igw-überprüfen
- rds-in-backup-plan
- rds-last-backup-recovery-Punkt erstellt
- rds-logging-enabled
- rds-mariadb-instance-encryptedim Transit
- rds-meets-restore-time-Ziel
- rds-multi-az-support
- rds-mysql-instance-encryptedunterwegs
- rds-postgresql-logs-to- Cloudwatch
- rds-postgres-instance-encryptedunterwegs
- rds-proxy-tls-encryption
- rds-resources-protected-by-Backup-Plan
- rds-snapshots-public-prohibited
- rds-snapshot-encrypted
- rds-sqlserver-encrypted-in-Transit
- rds-sql-server-logszur Cloud-Überwachung
- rds-storage-encrypted
- redshift-audit-logging-enabled
- redshift-backup-enabled
- redshift-cluster-configuration-check
- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check
- redshift-cluster-multi-az-aktiviert
- redshift-cluster-parameter-group-markiert
- redshift-cluster-public-access-überprüfen
- redshift-cluster-subnet-group-Multi-Az

- redshift-default-admin-check
- redshift-default-db-name-überprüfen
- redshift-enhanced-vpc-routing-aktiviert
- redshift-require-tls-ssl
- redshift-serverless-default-admin-überprüfen
- redshift-serverless-default-db-Namenscheck
- redshift-serverless-namespace-cmk-Verschlüsselung
- redshift-serverless-publish-logs-zu-Cloud-Watch
- redshift-serverless-workgroup-encryptedauf dem Weg
- redshift-serverless-workgroup-no-öffentlich zugänglich
- redshift-serverless-workgroup-routes-innerhalb von VPC
- redshift-unrestricted-port-access
- required-tags
- restricted-incoming-traffic
- root-account-hardware-mfa-aktiviert
- root-account-mfa-enabled
- s3 -regel-check express-dir-bucket-lifecycle
- nur s3- access-point-in-vpc
- s3- -Blöcke access-point-public-access
- s3- -Blöcke account-level-public-access
- s3- -Blocke-periodisch account-level-public-access
- s 3- bucket-acl-prohibited
- s-3 bucket-blacklisted-actions-prohibited
- s3- bucket-cross-region-replication -aktiviert
- s-3 bucket-default-lock-enabled
- s3 bucket-level-public-access - verboten
- s3- bucket-logging-enabled
- s-3 bucket-mfa-delete-enabled
- s-3 bucket-policy-grantee-check
- s3- bucket-policy-not-more -freizügig

- s 3- bucket-public-read-prohibited
- s-3 bucket-public-write-prohibited
- s-3 bucket-replication-enabled
- s3- bucket-server-side-encryption -aktiviert
- s-3 bucket-ssl-requests-only
- s3-Bucket-Tagged
- s-3 bucket-versioning-enabled
- s-3 default-encryption-kms
- s-3 event-notifications-enabled
- s3 last-backup-recovery-point - erstellt
- s3- lifecycle-policy-check
- s-3 meets-restore-time-target
- s3- resources-in-logically-air -Tresor mit Lücken
- s3 resources-protected-by-backup - -Plan
- s 3- version-lifecycle-policy-check
- sagemaker-app-image-config-markiert
- sagemaker-domain-in-vpc
- sagemaker-domain-tagged
- sagemaker-endpoint-configuration-kms-schlüsselkonfiguriert
- sagemaker-endpoint-config-prod-Anzahl der Instanzen
- sagemaker-feature-group-tagged
- sagemaker-image-description
- sagemaker-image-tagged
- sagemaker-model-in-vpc
- sagemaker-model-isolation-enabled
- sagemaker-notebook-instance-inside-vpc
- sagemaker-notebook-instance-kms-key-konfiguriert
- sagemaker-notebook-instance-platform-Version
- sagemaker-notebook-instance-root-Zugriffsprüfung
- sagemaker-notebook-no-direct-Internetzugang

- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-überprüfen
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- securityhub-enabled
- security-account-information-provided
- service-catalog-shared-within-Organisation
- service-vpc-endpoint-enabled
- sns-encrypted-kms
- sns-topic-message-delivery-Benachrichtigung aktiviert
- sns-topic-no-public-Zugriff
- sqs-queue-no-public-Zugang
- ssm-automation-block-public-teilen
- ssm-automation-logging-enabled
- ssm-document-not-public
- ssm-document-tagged
- step-functions-state-machine-Protokollierung aktiviert
- storagegateway-last-backup-recovery-punkt-erstellt
- storagegateway-resources-in-logically-air-gapped-vault
- storagegateway-resources-protected-by-Ersatzplan
- subnet-auto-assign-public-ip-deaktiviert
- transfer-agreement-description
- transfer-agreement-tagged
- transfer-certificate-description
- transfer-certificate-tagged
- transfer-connector-logging-enabled
- transfer-connector-tagged
- transfer-family-server-no-ftp
- transfer-profile-tagged

- transfer-workflow-description
- transfer-workflow-tagged
- virtualmachine-last-backup-recovery-punkt-erstellt
- virtualmachine-resources-in-logically-air-gapped-vault
- virtualmachine-resources-protected-by-Ersatzplan
- vpc-default-security-group-geschlossen
- vpc-endpoint-enabled
- vpc-flow-logs-enabled
- vpc-network-acl-unused-überprüfen
- vpc-peering-dns-resolution-überprüfen
- vpc-sg-open-only-to-authorized-ports
- vpc-sg-port-restriction-überprüfen
- vpc-vpn-2-tunnels-up
- wafv2-logging-enabled
- WAF 2- rulegroup-logging-enabled
- WAF 2- rulegroup-not-empty
- WAF 2- webacl-not-empty
- waf-regional-rulegroup-not-leer
- waf-regional-rule-not-leer
- waf-regional-webacl-not-leer

Region USA Ost (Nord-Virginia)

USA Ost (Nord-Virginia)

- access-keys-rotated
- account-part-of-organizations
- acmpca-certificate-authority-tagged
- acm-certificate-expiration-check
- acm-certificate-rsa-check
- acm-pca-root-ca-deaktiviert
- active-mq-supported-version

- alb-desync-mode-check
- alb-http-drop-invalid-Header-fähig
- alb-http-to-https-Umleitungsprüfung
- alb-internal-scheme-check
- alb-listener-tagged
- alb-waf-enabled
- amplify-app-branch-auto-löschung aktiviert
- amplify-app-description
- amplify-app-tagged
- amplify-branch-performance-mode-aktiviert
- amplify-branch-tagged
- api-gwv2- access-logs-enabled
- api-gwv2- authorization-type-configured
- api-gw-associated-with-WAF
- api-gw-cache-enabled-und-verschlüsselt
- api-gw-endpoint-type-überprüfen
- api-gw-execution-logging-aktiviert
- api-gw-ssl-enabled
- api-gw-xray-enabled
- appconfig-application-description
- appconfig-application-tagged
- appconfig-configuration-profile-tagged
- appconfig-configuration-profile-validators-nicht leer
- appconfig-deployment-strategy-description
- appconfig-deployment-strategy-replicate-zu-ssm
- appconfig-environment-description
- appconfig-environment-tagged
- appconfig-extension-association-tagged
- appconfig-freeform-profile-config-Speicher
- appconfig-hosted-configuration-version-Beschreibung

- appflow-flow-tagged
- appintegrations-event-integration-description
- appintegrations-event-integration-tagged
- appmesh-gateway-route-tagged
- appmesh-mesh-deny-tcp-Weiterleitung
- appmesh-mesh-tagged
- appmesh-route-tagged
- appmesh-virtual-gateway-backend-Standardeinstellungen-TLS
- appmesh-virtual-gateway-logging-file-path-exists
- appmesh-virtual-gateway-tagged
- appmesh-virtual-node-backend-defaults-tls-on
- appmesh-virtual-node-logging-file-path-exists
- appmesh-virtual-node-tagged
- appmesh-virtual-router-tagged
- appmesh-virtual-service-tagged
- approved-amis-by-id
- approved-amis-by-tag
- apprunner-service-in-vpc
- apprunner-service-no-public-Zugang
- apprunner-service-observability-enabled
- apprunner-service-tagged
- apprunner-vpc-connector-tagged
- appstream-fleet-in-vpc
- appsync-associated-with-waf
- appsync-authorization-check
- appsync-cache-ct-encryption-im Ruhezustand
- appsync-cache-ct-encryptionunterwegs
- appsync-cache-encryption-at-ausruhen
- appsync-logging-enabled
- athena-data-catalog-description

- athena-prepared-statement-description
- athena-workgroup-description
- athena-workgroup-encrypted-at-ausruhen
- athena-workgroup-enforce-workgroup-Konfiguration
- athena-workgroup-engine-version-automatisches Upgrade
- athena-workgroup-logging-enabled
- aurora-last-backup-recovery-punkt-erstellt
- aurora-meets-restore-time-Ziel
- aurora-mysql-backtracking-enabled
- aurora-mysql-cluster-audit-Protokollierung
- aurora-resources-in-logically-air-gapped-vault
- aurora-resources-protected-by-Backup-Plan
- autoscaling-capacity-rebalancing
- autoscaling-group-elb-healthcheck-erforderlich
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-hop-Grenze
- autoscaling-launch-config-public-ip-deaktiviert
- autoscaling-launch-template
- autoscaling-multiple-az
- autoscaling-multiple-instance-types
- backup-plan-min-frequency-and-min-retention-check
- backup-recovery-point-encrypted
- backup-recovery-point-manual-Löschen-deaktiviert
- backup-recovery-point-minimum-Aufbewahrungsprüfung
- batch-compute-environment-enabled
- batch-compute-environment-managed
- batch-compute-environment-tagged
- batch-job-queue-enabled
- batch-job-queue-tagged
- batch-managed-compute-environment-using-launch-template

- batch-managed-compute-env-compute-resources-tagged
- batch-scheduling-policy-tagged
- beanstalk-enhanced-health-reporting-aktiviert
- cassandra-keyspace-tagged
- clb-desync-mode-check
- clb-multiple-az
- cloudformation-stack-drift-detection-überprüfen
- cloudformation-stack-notification-check
- cloudfront-accesslogs-enabled
- cloudfront-associated-with-waf
- cloudfront-custom-ssl-certificate
- cloudfront-default-root-object-konfiguriert
- cloudfront-no-deprecated-ssl-Protokolle
- cloudfront-origin-access-identity-aktiviert
- cloudfront-origin-failover-enabled
- cloudfront-s3- origin-access-control-enabled
- Wolkenfront - 3 origin-non-existent-bucket
- cloudfront-security-policy-check
- cloudfront-sni-enabled
- cloudfront-ssl-policy-check
- cloudfront-traffic-to-origin-verschlüsselt
- cloudfront-viewer-policy-https
- cloudtrail-all-read-s3- data-event-check
- cloudtrail-all-write-s3- data-event-check
- Wolkenspur-S3- bucket-access-logging
- CloudTrail-S3- bucket-public-access-prohibited
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-action-enabled-überprüfen

- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted
- cloud-trail-cloud-watch-logs-aktiviert
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-Validierung aktiviert
- cmk-backing-key-rotation-aktiviert
- codebuild-project-artifact-encryption
- codebuild-project-environment-privileged-überprüfen
- codebuild-project-envvar-awscred-überprüfen
- codebuild-project-logging-enabled
- codebuild-project-s3-log-verschlüsselt
- codebuild-project-source-repo-URL-Prüfung
- codebuild-report-group-encrypted-im Ruhezustand
- codedeploy-auto-rollback-monitor-aktiviert
- codedeploy-deployment-group-auto-rollback-aktiviert
- codedeploy-deployment-group-outdated-instanzen-aktualisieren
- Codedeploy-ec2- minimum-healthy-hosts-configured
- codedeploy-lambda-allatonce-traffic-shift-deaktiviert
- codeguruprofiler-profiling-group-tagged
- codegururevieweer-repository-association-tagged
- codepipeline-deployment-count-check
- codepipeline-region-fanout-check
- cognito-identity-pool-unauth-Zugriffsprüfung
- cognito-user-pool-advanced-sicherheitsaktiviert
- cognito-user-pool-tagged
- connect-instance-logging-enabled
- customerprofiles-object-type-allow-Profilerstellung
- customerprofiles-object-type-tagged

- custom-eventbus-policy-attached
- custom-schema-registry-policy-beigefügt
- cw-loggroup-retention-period-überprüfen
- datasync-task-data-verification-aktiviert
- datasync-task-logging-enabled
- datasync-task-tagged
- dax-encryption-enabled
- dax-tls-endpoint-encryption
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- dms-auto-minor-version-upgrade-check
- dms-endpoint-ssl-configured
- dms-endpoint-tagged
- dms-mongo-db-authentication-aktiviert
- dms-neptune-iam-authorization-aktiviert
- dms-redis-tls-enabled
- dms-replication-not-public
- dms-replication-task-sourcedb-Protokollierung
- dms-replication-task-tagged
- dms-replication-task-targetdb-Protokollierung
- docdb-cluster-audit-logging-aktiviert
- docdb-cluster-backup-retention-überprüfen
- docdb-cluster-deletion-protection-aktiviert
- docdb-cluster-encrypted
- docdb-cluster-encrypted-in-transit
- docdb-cluster-snapshot-public-verboten
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-last-backup-recovery-Punkt erstellt

- dynamodb-meets-restore-time-Ziel
- dynamodb-pitr-enabled
- dynamodb-resources-protected-by-Backup-Plan
- dynamodb-table-deletion-protection-aktiviert
- dynamodb-table-encrypted-kms
- dynamodb-table-encryption-enabled
- dynamodb-throughput-limit-check
- ebs-in-backup-plan
- ebs-last-backup-recovery-punkt-erstellt
- ebs-meets-restore-time-Ziel
- ebs-optimized-instance
- ebs-resources-in-logically-air-gapped-vault
- ebs-resources-protected-by-Backup-Plan
- ebs-snapshot-public-restorable-überprüfen
- ec2- capacity-reservation-tagged
- ec2- carrier-gateway-tagged
- ec2- aktiviert client-vpn-connection-log
- ec2- client-vpn-endpoint-tagged
- ec2- -alle client-vpn-not-authorize
- ec2- dhcp-options-tagged
- ec2- ebs-encryption-by-default
- ec2- aktiviert enis-source-destination-check
- ec2-fleet-markiert
- ec2-imdsv2-check
- ec2- instance-detailed-monitoring-enabled
- ec2-ami instance-launched-with-allowed
- ec2- instance-managed-by-ssm
- ec2- instance-multiple-eni-check
- ec2- instance-no-public-ip
- ec2- instance-profile-attached

- ec2- erstellt last-backup-recovery-point
- ec2-2-prüfen launch-template-imdsv
- ec2- -deaktiviert launch-template-public-ip
- ec2- launch-template-tagged
- ec2- managedinstance-applications-blacklisted
- ec2- managedinstance-applications-required
- ec2- prüfen managedinstance-association-compliance-status
- ec2- managedinstance-inventory-blacklisted
- ec2- prüfen managedinstance-patch-compliance-status
- ec2- managedinstance-platform-check
- ec2- meets-restore-time-target
- ec2- Analyse mit Schlagwörtern network-insights-access-scope
- ec2 network-insights-access-scope - markiert
- ec2- network-insights-path-tagged
- ec2- no-amazon-key-pair
- ec2- paravirtual-instance-check
- ec2- prefix-list-tagged
- ec2- -Tresor mit Lücken resources-in-logically-air
- ec2- resources-protected-by-backup -plan
- ec2-eni security-group-attached-to
- ec2- -eni-periodisch security-group-attached-to
- ec2 spot-fleet-request-ct - - encryption-at-rest
- ec2-stopped-instance
- ec2- token-hop-limit-check
- ec2- traffic-mirror-filter-description
- ec2- traffic-mirror-filter-tagged
- ec2- traffic-mirror-session-description
- ec2- traffic-mirror-session-tagged
- ec2- traffic-mirror-target-description
- ec2- traffic-mirror-target-tagged

- ec2- -attach-deaktiviert transit-gateway-auto-vpc
- ec2 transit-gateway-multicast-domain - markiert
- ec2- volume-inuse-check
- ec2- vpn-connection-logging-enabled
- ecr-private-image-scanning-aktiviert
- ecr-private-lifecycle-policy-konfiguriert
- ecr-private-tag-immutability-aktiviert
- ecr-repository-cmk-encryption-aktiviert
- ecr-repository-tagged
- ecs-awsvpc-networking-enabled
- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-container-insights-enabled
- ecs-fargate-latest-platform-Version
- ecs-no-environment-secrets
- ecs-task-definition-log-Konfiguration
- ecs-task-definition-memory-hartes Limit
- ecs-task-definition-network-mode-not-host
- ecs-task-definition-nonroot-Benutzer
- ecs-task-definition-pid-Modus-Check
- ecs-task-definition-user-for-host-mode-check
- efs-access-point-enforce-Stammverzeichnis
- efs-access-point-enforce-Benutzeridentität
- efs-automatic-backups-enabled
- efs-encrypted-check
- efs-filesystem-ct-encrypted
- efs-in-backup-plan
- efs-last-backup-recovery-Punkt erstellt
- efs-meets-restore-time-Ziel
- efs-mount-target-public-zugänglich

- efs-resources-in-logically-air-gapped-vault
- efs-resources-protected-by-Backup-Plan
- eip-attached
- eks-cluster-logging-enabled
- eks-cluster-log-enabled
- eks-cluster-oldest-supported-Ausführung
- eks-cluster-secrets-encrypted
- eks-cluster-supported-version
- eks-endpoint-no-public-Zugang
- eks-secrets-encrypted
- elasticache-auto-minor-version-Upgrade-Check
- elasticache-rbac-auth-enabled
- elasticache-redis-cluster-automatic-Backup-Check
- elasticache-repl-grp-auto-failover-fähig
- elasticache-repl-grp-encrypted-im Ruhezustand
- elasticache-repl-grp-encryptedunterwegs
- elasticache-repl-grp-redis-auth-aktiviert
- elasticache-subnet-group-check
- elasticache-supported-engine-version
- elasticbeanstalk-application-description
- elasticbeanstalk-application-version-description
- elasticbeanstalk-environment-description
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch
- elasticsearch-node-to-node-Verschlüsselungsprüfung
- elastic-beanstalk-logs-to- Cloudwatch
- elastic-beanstalk-managed-updates-aktiviert
- elbv2- acm-certificate-required
- elv 2- listener-encryption-in-transit

- elbv2-multiple-az
- elbv2- prüfen predefined-security-policy-ssl
- elb-acm-certificate-required
- elb-cross-zone-load-Balancing aktiviert
- elb-custom-security-policy-ssl-Prüfung
- elb-deletion-protection-enabled
- elb-logging-enabled
- elb-predefined-security-policy-ssl-Überprüfung
- elb-tls-https-listeners-nur
- emr-block-public-access
- emr-kerberos-enabled
- emr-master-no-public-ip
- emr-security-configuration-encryption-ruh dich aus
- emr-security-configuration-encryption-Transit
- encrypted-volumes
- event-data-store-cmk-Verschlüsselung aktiviert
- evidently-launch-description
- evidently-launch-tagged
- evidently-project-description
- evidently-project-tagged
- evidently-segment-description
- evidently-segment-tagged
- fis-experiment-template-log-Konfiguration ist vorhanden
- fis-experiment-template-tagged
- fms-shield-resource-policy-überprüfen
- fms-webacl-resource-policy-überprüfen
- fms-webacl-rulegroup-association-überprüfen
- frauddetector-entity-type-tagged
- frauddetector-label-tagged
- frauddetector-outcome-tagged

- frauddetector-variable-tagged
- fsx-last-backup-recovery-Punkt erstellt
- fsx-lustre-copy-tagszu Backups
- fsx-meets-restore-time-Ziel
- fsx-ontap-deployment-type-überprüfen
- fsx-openzfs-copy-tags-aktiviert
- fsx-openzfs-deployment-type-überprüfen
- fsx-resources-protected-by-Ersatzplan
- fsx-windows-audit-log-konfiguriert
- fsx-windows-deployment-type-überprüfen
- glb-listener-tagged
- global-endpoint-event-replication-aktiviert
- glue-job-logging-enabled
- glue-ml-transform-encrypted-im Ruhezustand
- glue-spark-job-supported-Ausführung
- GuardDuty-EC2- protection-runtime-enabled
- guardduty-ecs-protection-runtime-aktiviert
- guardduty-eks-protection-audit-aktiviert
- guardduty-eks-protection-runtime-aktiviert
- guardduty-enabled-centralized
- guardduty-lambda-protection-enabled
- guardduty-malware-protection-enabled
- guardduty-non-archived-findings
- guardduty-rds-protection-enabled
- guardduty-runtime-monitoring-enabled
- GuardDuty-S3-Schutz aktiviert
- iam-customer-policy-blocked-kms-Aktionen
- iam-external-access-analyzer-aktiviert
- iam-group-has-users-überprüfen
- iam-inline-policy-blocked-kms-Aktionen

- iam-no-inline-policy-überprüfen
- iam-oidc-provider-tagged
- iam-password-policy
- iam-policy-blacklisted-check
- iam-policy-in-use
- iam-policy-no-statements-with-admin-access
- iam-policy-no-statements-with-full-access
- iam-role-managed-policy-überprüfen
- iam-root-access-key-überprüfen
- iam-saml-provider-tagged
- iam-server-certificate-expiration-überprüfen
- iam-server-certificate-tagged
- iam-user-group-membership-überprüfen
- iam-user-mfa-enabled
- iam-user-no-policies-überprüfen
- iam-user-unused-credentials-überprüfen
- incoming-ssh-disabled
- inspector-ec2-Scan aktiviert
- inspector-ecr-scan-enabled
- inspector-lambda-code-scan-aktiviert
- inspector-lambda-standard-scan-aktiviert
- instances-in-vpc
- internet-gateway-authorized-vpc-nur
- iotevents-alarm-model-tagged
- iotevents-detector-model-tagged
- iotevents-input-tagged
- iotsitewise-asset-model-tagged
- iotsitewise-dashboard-tagged
- iotsitewise-gateway-tagged
- iotsitewise-portal-tagged

- iotsitewise-project-tagged
- iottwinmaker-component-type-tagged
- iottwinmaker-entity-tagged
- iottwinmaker-scene-tagged
- iottwinmaker-sync-job-tagged
- iottwinmaker-workspace-tagged
- iotwireless-fuota-task-tagged
- iotwireless-multicast-group-tagged
- iotwireless-service-profile-tagged
- iot-authorizer-token-signing-aktiviert
- ivs-channel-playback-authorization-aktiviert
- ivs-channel-tagged
- ivs-playback-key-pair-markiert
- ivs-recording-configuration-tagged
- kinesis-firehose-delivery-stream-verschlüsselt
- kinesis-stream-backup-retention-überprüfen
- kinesis-stream-encrypted
- kms-cmk-not-scheduled-zum Löschen
- kms-key-policy-no-öffentlicher Zugang
- lambda-concurrency-check
- lambda-dlq-check
- lambda-function-public-access-verboten
- lambda-function-settings-check
- lambda-function-xray-enabled
- lambda-inside-vpc
- lambda-vpc-multi-az-überprüfen
- lightsail-bucket-tagged
- lightsail-certificate-tagged
- lightsail-disk-tagged
- macie-auto-sensitive-data-Discovery-Check

- macie-status-check
- mariadb-publish-logs-to-Cloudwatch-Protokolle
- mfa-enabled-for-iam-Konsolenzugriff
- mq-active-broker-ldap-Authentifizierung
- mq-active-deployment-mode
- mq-active-single-instance-broker-storage-type-efs
- mq-automatic-minor-version-Upgrade aktiviert
- mq-auto-minor-version-upgrade-fähig
- mq-broker-general-logging-aktiviert
- mq-cloudwatch-audit-logging-aktiviert
- mq-cloudwatch-audit-log-aktiviert
- mq-no-public-access
- mq-rabbit-deployment-mode
- msk-cluster-public-access-deaktiviert
- msk-connect-connector-logging-aktiviert
- msk-enhanced-monitoring-enabled
- msk-in-cluster-node-require-tls
- msk-unrestricted-access-check
- multi-region-cloud-trail-aktiviert
- nacl-no-unrestricted-ssh-rdp
- neptune-cluster-backup-retention-überprüfen
- neptune-cluster-cloudwatch-log-exportfähig
- neptune-cluster-copy-tags-to-snapshot-enabled
- neptune-cluster-deletion-protection-aktiviert
- neptune-cluster-encrypted
- neptune-cluster-iam-database-Authentifizierung
- neptune-cluster-multi-az-aktiviert
- neptune-cluster-snapshot-encrypted
- neptune-cluster-snapshot-public-verboten
- netfw-deletion-protection-enabled

- netfw-logging-enabled
- netfw-multi-az-enabled
- netfw-policy-default-action-fragment-Pakete
- netfw-policy-default-action-vollständige Pakete
- netfw-policy-rule-group-assoziiert
- netfw-stateless-rule-group-nicht leer
- netfw-subnet-change-protection-aktiviert
- nlb-cross-zone-load-Balancing aktiviert
- nlb-internal-scheme-check
- nlb-listener-tagged
- nlb-logging-enabled
- no-unrestricted-route-to-igw
- opensearch-access-control-enabled
- opensearch-audit-logging-enabled
- opensearch-data-node-fault-Toleranz
- opensearch-encrypted-at-rest
- opensearch-https-required
- opensearch-in-vpc-only
- opensearch-logs-to-cloudwatch
- opensearch-node-to-node-Verschlüsselungsprüfung
- opensearch-primary-node-fault-Toleranz
- opensearch-update-check
- rabbit-mq-supported-version
- rds-aurora-mysql-audit-Protokollierung aktiviert
- rds-aurora-postgresql-logs-zu-Cloud-Watch
- rds-automatic-minor-version-upgrade-fähig
- rds-cluster-auto-minor-version-upgrade-enable
- rds-cluster-default-admin-überprüfen
- rds-cluster-deletion-protection-aktiviert
- rds-cluster-encrypted-at-ausruhen

- rds-cluster-iam-authentication-aktiviert
- rds-cluster-multi-az-aktiviert
- rds-db-security-group-nicht erlaubt
- rds-enhanced-monitoring-enabled
- rds-instance-default-admin-überprüfen
- rds-instance-deletion-protection-aktiviert
- rds-instance-iam-authentication-aktiviert
- rds-instance-public-access-überprüfen
- rds-instance-subnet-igw-überprüfen
- rds-in-backup-plan
- rds-last-backup-recovery-Punkt erstellt
- rds-logging-enabled
- rds-mariadb-instance-encryptedim Transit
- rds-meets-restore-time-Ziel
- rds-multi-az-support
- rds-mysql-instance-encryptedunterwegs
- rds-postgresql-logs-to- Cloudwatch
- rds-postgres-instance-encryptedunterwegs
- rds-proxy-tls-encryption
- rds-resources-protected-by-Backup-Plan
- rds-snapshots-public-prohibited
- rds-snapshot-encrypted
- rds-sqlserver-encrypted-in-Transit
- rds-sql-server-logszur Cloud-Überwachung
- rds-storage-encrypted
- redshift-audit-logging-enabled
- redshift-backup-enabled
- redshift-cluster-configuration-check
- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check

- redshift-cluster-multi-az-aktiviert
- redshift-cluster-parameter-group-markiert
- redshift-cluster-public-access-überprüfen
- redshift-cluster-subnet-group-Multi-Az
- redshift-default-admin-check
- redshift-default-db-name-überprüfen
- redshift-enhanced-vpc-routing-aktiviert
- redshift-require-tls-ssl
- redshift-serverless-default-admin-überprüfen
- redshift-serverless-default-db-Namenscheck
- redshift-serverless-namespace-cmk-Verschlüsselung
- redshift-serverless-publish-logs-zu-Cloud-Watch
- redshift-serverless-workgroup-encryptedauf dem Weg
- redshift-serverless-workgroup-no-öffentlich zugänglich
- redshift-serverless-workgroup-routes-innerhalb von VPC
- redshift-unrestricted-port-access
- required-tags
- restricted-incoming-traffic
- root-account-hardware-mfa-aktiviert
- root-account-mfa-enabled
- Route 53- query-logging-enabled
- s3 -regel-check express-dir-bucket-lifecycle
- nur s3- access-point-in-vpc
- s3- -Blöcke access-point-public-access
- s3- -Blöcke account-level-public-access
- s3- -Blocke-periodisch account-level-public-access
- s 3- bucket-acl-prohibited
- s-3 bucket-blacklisted-actions-prohibited
- s3- bucket-cross-region-replication -aktiviert
- s-3 bucket-default-lock-enabled

- s3 bucket-level-public-access - verboten
- s3- bucket-logging-enabled
- s-3 bucket-mfa-delete-enabled
- s-3 bucket-policy-grantee-check
- s3- bucket-policy-not-more -freizügig
- s 3- bucket-public-read-prohibited
- s-3 bucket-public-write-prohibited
- s-3 bucket-replication-enabled
- s3- bucket-server-side-encryption -aktiviert
- s-3 bucket-ssl-requests-only
- s3-Bucket-Tagged
- s-3 bucket-versioning-enabled
- s-3 default-encryption-kms
- s-3 event-notifications-enabled
- s3 last-backup-recovery-point - erstellt
- s3- lifecycle-policy-check
- s-3 meets-restore-time-target
- s3- resources-in-logically-air -Tresor mit Lücken
- s3 resources-protected-by-backup - -Plan
- s 3- version-lifecycle-policy-check
- sagemaker-app-image-config-markiert
- sagemaker-domain-in-vpc
- sagemaker-domain-tagged
- sagemaker-endpoint-configuration-kms-schlüsselkonfiguriert
- sagemaker-endpoint-config-prod-Anzahl der Instanzen
- sagemaker-feature-group-tagged
- sagemaker-image-description
- sagemaker-image-tagged
- sagemaker-model-in-vpc
- sagemaker-model-isolation-enabled

- sagemaker-notebook-instance-inside-vpc
- sagemaker-notebook-instance-kms-key-konfiguriert
- sagemaker-notebook-instance-platform-Version
- sagemaker-notebook-instance-root-Zugriffsprüfung
- sagemaker-notebook-no-direct-Internetzugang
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-überprüfen
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- securityhub-enabled
- security-account-information-provided
- service-catalog-shared-within-Organisation
- service-vpc-endpoint-enabled
- ses-malware-scanning-enabled
- shield-advanced-enabled-autorenew
- shield-drt-access
- sns-encrypted-kms
- sns-topic-message-delivery-Benachrichtigung aktiviert
- sns-topic-no-public-Zugriff
- sqs-queue-no-public-Zugang
- ssm-automation-block-public-teilen
- ssm-automation-logging-enabled
- ssm-document-not-public
- ssm-document-tagged
- step-functions-state-machine-Protokollierung aktiviert
- storagegateway-last-backup-recovery-punkt-erstellt
- storagegateway-resources-in-logically-air-gapped-vault
- storagegateway-resources-protected-by-Ersatzplan
- subnet-auto-assign-public-ip-deaktiviert

- transfer-agreement-description
- transfer-agreement-tagged
- transfer-certificate-description
- transfer-certificate-tagged
- transfer-connector-logging-enabled
- transfer-connector-tagged
- transfer-family-server-no-ftp
- transfer-profile-tagged
- transfer-workflow-description
- transfer-workflow-tagged
- virtualmachine-last-backup-recovery-punkt-erstellt
- virtualmachine-resources-in-logically-air-gapped-vault
- virtualmachine-resources-protected-by-Ersatzplan
- vpc-default-security-group-geschlossen
- vpc-endpoint-enabled
- vpc-flow-logs-enabled
- vpc-network-acl-unused-überprüfen
- vpc-peering-dns-resolution-überprüfen
- vpc-sg-open-only-to-authorized-ports
- vpc-sg-port-restriction-überprüfen
- vpc-vpn-2-tunnels-up
- wafv2-logging-enabled
- WAF 2- rulegroup-logging-enabled
- WAF 2- rulegroup-not-empty
- WAF 2- webacl-not-empty
- waf-classic-logging-enabled
- waf-global-rulegroup-not-leer
- waf-global-rule-not-leer
- waf-global-webacl-not-leer
- waf-regional-rulegroup-not-leer

- waf-regional-rule-not-leer
- waf-regional-webacl-not-leer
- workspaces-root-volume-encryption-aktiviert
- workspaces-user-volume-encryption-aktiviert

Region USA West (Nordkalifornien)

USA West (Nordkalifornien)

- access-keys-rotated
- account-part-of-organizations
- acmpca-certificate-authority-tagged
- acm-certificate-expiration-check
- acm-certificate-rsa-check
- acm-pca-root-ca-deaktiviert
- active-mq-supported-version
- alb-desync-mode-check
- alb-http-drop-invalid-Header-fähig
- alb-http-to-https-Umleitungsprüfung
- alb-internal-scheme-check
- alb-listener-tagged
- alb-waf-enabled
- amplify-app-branch-auto-löschung aktiviert
- amplify-app-description
- amplify-app-tagged
- amplify-branch-performance-mode-aktiviert
- amplify-branch-tagged
- api-gwv2- access-logs-enabled
- api-gwv2- authorization-type-configured
- api-gw-associated-with-WAF
- api-gw-cache-enabled-und-verschlüsselt
- api-gw-endpoint-type-überprüfen

- api-gw-execution-logging-aktiviert
- api-gw-ssl-enabled
- api-gw-xray-enabled
- appconfig-application-description
- appconfig-application-tagged
- appconfig-configuration-profile-tagged
- appconfig-configuration-profile-validators-nicht leer
- appconfig-deployment-strategy-description
- appconfig-deployment-strategy-replicate-zu-ssm
- appconfig-environment-description
- appconfig-environment-tagged
- appconfig-extension-association-tagged
- appconfig-freeform-profile-config-Speicher
- appconfig-hosted-configuration-version-Beschreibung
- appflow-flow-tagged
- appmesh-gateway-route-tagged
- appmesh-mesh-deny-tcp-Weiterleitung
- appmesh-mesh-tagged
- appmesh-route-tagged
- appmesh-virtual-gateway-backend-Standardeinstellungen-TLS
- appmesh-virtual-gateway-logging-file-path-exists
- appmesh-virtual-gateway-tagged
- appmesh-virtual-node-backend-defaults-tls-on
- appmesh-virtual-node-logging-file-path-exists
- appmesh-virtual-node-tagged
- appmesh-virtual-router-tagged
- appmesh-virtual-service-tagged
- approved-amis-by-id
- approved-amis-by-tag
- appsync-associated-with-waf

- appsync-authorization-check
- appsync-cache-encryption-at-ausruhen
- appsync-logging-enabled
- athena-data-catalog-description
- athena-prepared-statement-description
- athena-workgroup-description
- athena-workgroup-encrypted-at-ausruhen
- athena-workgroup-enforce-workgroup-Konfiguration
- athena-workgroup-engine-version-automatisches Upgrade
- athena-workgroup-logging-enabled
- aurora-last-backup-recovery-Punkt erstellt
- aurora-meets-restore-time-Ziel
- aurora-mysql-backtracking-enabled
- aurora-mysql-cluster-audit-Protokollierung
- aurora-resources-in-logically-air-gapped-vault
- aurora-resources-protected-by-Backup-Plan
- autoscaling-capacity-rebalancing
- autoscaling-group-elb-healthcheck-erforderlich
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-hop-Grenze
- autoscaling-launch-config-public-ip-deaktiviert
- autoscaling-launch-template
- autoscaling-multiple-az
- autoscaling-multiple-instance-types
- backup-plan-min-frequency-and-min-retention-check
- backup-recovery-point-encrypted
- backup-recovery-point-manual-Löschen-deaktiviert
- backup-recovery-point-minimum-Aufbewahrungsprüfung
- batch-compute-environment-enabled
- batch-compute-environment-managed

- batch-compute-environment-tagged
- batch-job-queue-enabled
- batch-job-queue-tagged
- batch-managed-compute-environment-using-launch-template
- batch-managed-compute-env-compute-resources-tagged
- batch-scheduling-policy-tagged
- beanstalk-enhanced-health-reporting-aktiviert
- cassandra-keyspace-tagged
- clb-desync-mode-check
- clb-multiple-az
- cloudformation-stack-drift-detection-überprüfen
- cloudformation-stack-notification-check
- cloudtrail-all-read-s3- data-event-check
- cloudtrail-all-write-s3- data-event-check
- Wolkenspur-S3- bucket-access-logging
- CloudTrail-S3- bucket-public-access-prohibited
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-action-enabled-überprüfen
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted
- cloud-trail-cloud-watch-logs-aktiviert
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-Validierung aktiviert
- cmk-backing-key-rotation-aktiviert
- codebuild-project-artifact-encryption
- codebuild-project-environment-privileged-überprüfen

- codebuild-project-envvar-awscred-überprüfen
- codebuild-project-logging-enabled
- codebuild-project-s3-log-verschlüsselt
- codebuild-project-source-repo-URL-Prüfung
- codebuild-report-group-encrypted-im Ruhezustand
- codedeploy-auto-rollback-monitor-aktiviert
- codedeploy-deployment-group-auto-rollback-aktiviert
- codedeploy-deployment-group-outdated-instanzen-aktualisieren
- Codedeploy-ec2- minimum-healthy-hosts-configured
- codedeploy-lambda-allatonce-traffic-shift-deaktiviert
- codepipeline-deployment-count-check
- codepipeline-region-fanout-check
- cognito-identity-pool-unauth-Zugriffsprüfung
- cognito-user-pool-advanced-sicherheitsaktiviert
- cognito-user-pool-tagged
- custom-eventbus-policy-attached
- custom-schema-registry-policy-angehängt
- cw-loggroup-retention-period-überprüfen
- datasync-task-data-verification-aktiviert
- datasync-task-logging-enabled
- datasync-task-tagged
- dax-encryption-enabled
- dax-tls-endpoint-encryption
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- dms-auto-minor-version-upgrade-check
- dms-endpoint-ssl-configured
- dms-endpoint-tagged
- dms-mongo-db-authentication-aktiviert

- dms-neptune-iam-authorization-aktiviert
- dms-redis-tls-enabled
- dms-replication-not-public
- dms-replication-task-sourcedb-Protokollierung
- dms-replication-task-tagged
- dms-replication-task-targetdb-Protokollierung
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-last-backup-recovery-Punkt erstellt
- dynamodb-meets-restore-time-Ziel
- dynamodb-pitr-enabled
- dynamodb-resources-protected-by-Backup-Plan
- dynamodb-table-deletion-protection-aktiviert
- dynamodb-table-encrypted-kms
- dynamodb-table-encryption-enabled
- dynamodb-throughput-limit-check
- ebs-in-backup-plan
- ebs-last-backup-recovery-punkt-erstellt
- ebs-meets-restore-time-Ziel
- ebs-optimized-instance
- ebs-resources-in-logically-air-gapped-vault
- ebs-resources-protected-by-Backup-Plan
- ebs-snapshot-public-restorable-überprüfen
- ec2- capacity-reservation-tagged
- ec2- aktiviert client-vpn-connection-log
- ec2- client-vpn-endpoint-tagged
- ec2- -alle client-vpn-not-authorize
- ec2- dhcp-options-tagged
- ec2- ebs-encryption-by-default
- ec2- aktiviert enis-source-destination-check

- ec2-fleet-markiert
- ec2-imdsv2-check
- ec2- instance-detailed-monitoring-enabled
- ec2-ami instance-launched-with-allowed
- ec2- instance-managed-by-ssm
- ec2- instance-multiple-eni-check
- ec2- instance-no-public-ip
- ec2- instance-profile-attached
- ec2- erstellt last-backup-recovery-point
- ec2-2-prüfen launch-template-imdsv
- ec2- -deaktiviert launch-template-public-ip
- ec2- launch-template-tagged
- ec2- managedinstance-applications-blacklisted
- ec2- managedinstance-applications-required
- ec2- prüfen managedinstance-association-compliance-status
- ec2- managedinstance-inventory-blacklisted
- ec2- prüfen managedinstance-patch-compliance-status
- ec2- managedinstance-platform-check
- ec2- meets-restore-time-target
- ec2- Analyse mit Schlagwörtern network-insights-access-scope
- ec2 network-insights-access-scope - markiert
- ec2- network-insights-path-tagged
- ec2- no-amazon-key-pair
- ec2- paravirtual-instance-check
- ec2- prefix-list-tagged
- ec2- -Tresor mit Lücken resources-in-logically-air
- ec2- resources-protected-by-backup -plan
- ec2- -eni security-group-attached-to
- ec2- -eni-periodisch security-group-attached-to
- ec2-stopped-instance

- ec2- token-hop-limit-check
- ec2- traffic-mirror-filter-description
- ec2- traffic-mirror-filter-tagged
- ec2- traffic-mirror-session-description
- ec2- traffic-mirror-session-tagged
- ec2- traffic-mirror-target-description
- ec2- traffic-mirror-target-tagged
- ec2- -attach-deaktiviert transit-gateway-auto-vpc
- ec2 transit-gateway-multicast-domain - markiert
- ec2- volume-inuse-check
- ec2- vpn-connection-logging-enabled
- ecr-private-image-scanning-aktiviert
- ecr-private-lifecycle-policy-konfiguriert
- ecr-private-tag-immutability-aktiviert
- ecr-repository-cmk-encryption-aktiviert
- ecr-repository-tagged
- ecs-awsvpc-networking-enabled
- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-container-insights-enabled
- ecs-fargate-latest-platform-Version
- ecs-no-environment-secrets
- ecs-task-definition-log-Konfiguration
- ecs-task-definition-memory-hartes Limit
- ecs-task-definition-network-mode-not-host
- ecs-task-definition-nonroot-Benutzer
- ecs-task-definition-pid-Modus-Check
- ecs-task-definition-user-for-host-mode-check
- efs-access-point-enforce-Stammverzeichnis
- efs-access-point-enforce-Benutzeridentität

- efs-automatic-backups-enabled
- efs-encrypted-check
- efs-filesystem-ct-encrypted
- efs-in-backup-plan
- efs-last-backup-recovery-Punkt erstellt
- efs-meets-restore-time-Ziel
- efs-mount-target-public-zugänglich
- efs-resources-in-logically-air-gapped-vault
- efs-resources-protected-by-Backup-Plan
- eip-attached
- eks-cluster-logging-enabled
- eks-cluster-log-enabled
- eks-cluster-oldest-supported-Ausführung
- eks-cluster-secrets-encrypted
- eks-cluster-supported-version
- eks-endpoint-no-public-Zugang
- eks-secrets-encrypted
- elasticache-auto-minor-version-Upgrade-Check
- elasticache-rbac-auth-enabled
- elasticache-redis-cluster-automatic-Backup-Check
- elasticache-repl-grp-auto-failover-fähig
- elasticache-repl-grp-encrypted-im Ruhezustand
- elasticache-repl-grp-encryptedunterwegs
- elasticache-repl-grp-redis-auth-aktiviert
- elasticache-subnet-group-check
- elasticache-supported-engine-version
- elasticbeanstalk-application-description
- elasticbeanstalk-application-version-description
- elasticbeanstalk-environment-description
- elasticsearch-encrypted-at-rest

- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch
- elasticsearch-node-to-node-Verschlüsselungsprüfung
- elastic-beanstalk-logs-to- Cloudwatch
- elastic-beanstalk-managed-updates-aktiviert
- elbv2- acm-certificate-required
- elv 2- listener-encryption-in-transit
- elbv2-multiple-az
- elbv2- prüfen predefined-security-policy-ssl
- elb-acm-certificate-required
- elb-cross-zone-load-Balancing aktiviert
- elb-custom-security-policy-ssl-Prüfung
- elb-deletion-protection-enabled
- elb-logging-enabled
- elb-predefined-security-policy-ssl-Überprüfung
- elb-tls-https-listeners-nur
- emr-block-public-access
- emr-kerberos-enabled
- emr-master-no-public-ip
- emr-security-configuration-encryption-ruh dich aus
- emr-security-configuration-encryption-Transit
- encrypted-volumes
- event-data-store-cmk-Verschlüsselung aktiviert
- fis-experiment-template-log-Konfiguration ist vorhanden
- fis-experiment-template-tagged
- fms-shield-resource-policy-überprüfen
- fms-webacl-resource-policy-überprüfen
- fms-webacl-rulegroup-association-überprüfen
- fsx-last-backup-recovery-Punkt erstellt
- fsx-lustre-copy-tagszu Backups

- fsx-meets-restore-time-Ziel
- fsx-ontap-deployment-type-überprüfen
- fsx-openzfs-copy-tags-aktiviert
- fsx-openzfs-deployment-type-überprüfen
- fsx-resources-protected-by-Ersatzplan
- fsx-windows-audit-log-konfiguriert
- fsx-windows-deployment-type-überprüfen
- glb-listener-tagged
- global-endpoint-event-replication-aktiviert
- glue-job-logging-enabled
- glue-ml-transform-encrypted-im Ruhezustand
- glue-spark-job-supported-Ausführung
- GuardDuty-EC2- protection-runtime-enabled
- guardduty-ecs-protection-runtime-aktiviert
- guardduty-eks-protection-audit-aktiviert
- guardduty-eks-protection-runtime-aktiviert
- guardduty-enabled-centralized
- guardduty-lambda-protection-enabled
- guardduty-malware-protection-enabled
- guardduty-non-archived-findings
- guardduty-rds-protection-enabled
- guardduty-runtime-monitoring-enabled
- GuardDuty-S3-Schutz aktiviert
- iam-customer-policy-blocked-kms-Aktionen
- iam-external-access-analyzer-aktiviert
- iam-group-has-users-überprüfen
- iam-inline-policy-blocked-KMS-Aktionen
- iam-no-inline-policy-überprüfen
- iam-password-policy
- iam-policy-blacklisted-check

- iam-policy-in-use
- iam-policy-no-statements-with-admin-access
- iam-policy-no-statements-with-full-access
- iam-role-managed-policy-überprüfen
- iam-root-access-key-überprüfen
- iam-user-group-membership-überprüfen
- iam-user-mfa-enabled
- iam-user-no-policies-überprüfen
- iam-user-unused-credentials-überprüfen
- incoming-ssh-disabled
- inspector-ec2-Scan aktiviert
- inspector-ecr-scan-enabled
- inspector-lambda-standard-scan-aktiviert
- instances-in-vpc
- internet-gateway-authorized-vpc-nur
- iot-authorizer-token-signing-aktiviert
- kinesis-firehose-delivery-stream-verschlüsselt
- kinesis-stream-backup-retention-überprüfen
- kinesis-stream-encrypted
- kms-cmk-not-scheduled-zum Löschen
- kms-key-policy-no-öffentlicher Zugang
- lambda-concurrency-check
- lambda-dlq-check
- lambda-function-public-access-verboten
- lambda-function-settings-check
- lambda-function-xray-enabled
- lambda-inside-vpc
- lambda-vpc-multi-az-überprüfen
- macie-auto-sensitive-data-Discovery-Check
- macie-status-check

- mariadb-publish-logs-to-Cloudwatch-Protokolle
- mfa-enabled-for-iam-Konsolenzugriff
- mq-active-broker-ldap-Authentifizierung
- mq-active-deployment-mode
- mq-active-single-instance-broker-storage-type-efs
- mq-automatic-minor-version-Upgrade aktiviert
- mq-auto-minor-version-upgrade-fähig
- mq-broker-general-logging-aktiviert
- mq-cloudwatch-audit-logging-aktiviert
- mq-cloudwatch-audit-log-aktiviert
- mq-no-public-access
- mq-rabbit-deployment-mode
- msk-cluster-public-access-deaktiviert
- msk-connect-connector-logging-aktiviert
- msk-enhanced-monitoring-enabled
- msk-in-cluster-node-require-tls
- msk-unrestricted-access-check
- multi-region-cloud-trail-aktiviert
- nacl-no-unrestricted-ssh-rdp
- neptune-cluster-backup-retention-überprüfen
- neptune-cluster-cloudwatch-log-exportfähig
- neptune-cluster-copy-tags-to-snapshot-enabled
- neptune-cluster-deletion-protection-aktiviert
- neptune-cluster-encrypted
- neptune-cluster-iam-database-Authentifizierung
- neptune-cluster-multi-az-aktiviert
- neptune-cluster-snapshot-encrypted
- neptune-cluster-snapshot-public-verboten
- netfw-deletion-protection-enabled
- netfw-logging-enabled

- netfw-multi-az-enabled
- netfw-policy-default-action-fragment-Pakete
- netfw-policy-default-action-vollständige Pakete
- netfw-policy-rule-group-assoziiert
- netfw-stateless-rule-group-nicht leer
- netfw-subnet-change-protection-aktiviert
- nlb-cross-zone-load-Balancing aktiviert
- nlb-internal-scheme-check
- nlb-listener-tagged
- nlb-logging-enabled
- no-unrestricted-route-to-igw
- opensearch-access-control-enabled
- opensearch-audit-logging-enabled
- opensearch-data-node-fault-Toleranz
- opensearch-encrypted-at-rest
- opensearch-https-required
- opensearch-in-vpc-only
- opensearch-logs-to-cloudwatch
- opensearch-node-to-node-Verschlüsselungsprüfung
- opensearch-primary-node-fault-Toleranz
- opensearch-update-check
- rabbit-mq-supported-version
- rds-aurora-mysql-audit-Protokollierung aktiviert
- rds-aurora-postgresql-logs-zu-Cloud-Watch
- rds-automatic-minor-version-upgrade-fähig
- rds-cluster-default-admin-überprüfen
- rds-cluster-deletion-protection-aktiviert
- rds-cluster-encrypted-at-ausruhen
- rds-cluster-iam-authentication-aktiviert
- rds-cluster-multi-az-aktiviert

- rds-db-security-group-nicht erlaubt
- rds-enhanced-monitoring-enabled
- rds-instance-default-admin-überprüfen
- rds-instance-deletion-protection-aktiviert
- rds-instance-iam-authentication-aktiviert
- rds-instance-public-access-überprüfen
- rds-instance-subnet-igw-überprüfen
- rds-in-backup-plan
- rds-last-backup-recovery-Punkt erstellt
- rds-logging-enabled
- rds-mariadb-instance-encryptedim Transit
- rds-meets-restore-time-Ziel
- rds-multi-az-support
- rds-mysql-instance-encryptedunterwegs
- rds-postgresql-logs-to- Cloudwatch
- rds-postgres-instance-encryptedunterwegs
- rds-proxy-tls-encryption
- rds-resources-protected-by-Backup-Plan
- rds-snapshots-public-prohibited
- rds-snapshot-encrypted
- rds-sqlserver-encrypted-in-Transit
- rds-sql-server-logszur Cloud-Überwachung
- rds-storage-encrypted
- redshift-audit-logging-enabled
- redshift-backup-enabled
- redshift-cluster-configuration-check
- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check
- redshift-cluster-parameter-group-markiert
- redshift-cluster-public-access-überprüfen

- redshift-cluster-subnet-group-Multi-Az
- redshift-default-admin-check
- redshift-default-db-name-überprüfen
- redshift-enhanced-vpc-routing-aktiviert
- redshift-require-tls-ssl
- redshift-serverless-default-admin-überprüfen
- redshift-serverless-default-db-Namenscheck
- redshift-serverless-namespace-cmk-Verschlüsselung
- redshift-serverless-publish-logs-zu-Cloud-Watch
- redshift-serverless-workgroup-encryptedauf dem Weg
- redshift-serverless-workgroup-no-öffentlich zugänglich
- redshift-serverless-workgroup-routes-innerhalb von VPC
- redshift-unrestricted-port-access
- required-tags
- restricted-incoming-traffic
- root-account-hardware-mfa-aktiviert
- root-account-mfa-enabled
- nur s3- access-point-in-vpc
- s3- -Blöcke access-point-public-access
- s3- -Blöcke account-level-public-access
- s3- -Blocke-periodisch account-level-public-access
- s 3- bucket-acl-prohibited
- s-3 bucket-blacklisted-actions-prohibited
- s3- bucket-cross-region-replication -aktiviert
- s-3 bucket-default-lock-enabled
- s3 bucket-level-public-access - verboten
- s3- bucket-logging-enabled
- s-3 bucket-mfa-delete-enabled
- s-3 bucket-policy-grantee-check
- s3- bucket-policy-not-more -freizügig

- s 3- bucket-public-read-prohibited
- s-3 bucket-public-write-prohibited
- s-3 bucket-replication-enabled
- s3- bucket-server-side-encryption -aktiviert
- s-3 bucket-ssl-requests-only
- s3-Bucket-Tagged
- s-3 bucket-versioning-enabled
- s-3 default-encryption-kms
- s-3 event-notifications-enabled
- s3 last-backup-recovery-point - erstellt
- s3- lifecycle-policy-check
- s-3 meets-restore-time-target
- s3- resources-in-logically-air -Tresor mit Lücken
- s3 resources-protected-by-backup - -Plan
- s 3- version-lifecycle-policy-check
- sagemaker-app-image-config-markiert
- sagemaker-domain-in-vpc
- sagemaker-domain-tagged
- sagemaker-endpoint-configuration-kms-schlüsselkonfiguriert
- sagemaker-endpoint-config-prod-Anzahl der Instanzen
- sagemaker-feature-group-tagged
- sagemaker-image-description
- sagemaker-image-tagged
- sagemaker-model-in-vpc
- sagemaker-model-isolation-enabled
- sagemaker-notebook-instance-inside-vpc
- sagemaker-notebook-instance-kms-key-konfiguriert
- sagemaker-notebook-instance-platform-Version
- sagemaker-notebook-instance-root-Zugriffsprüfung
- sagemaker-notebook-no-direct-Internetzugang

- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-überprüfen
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- securityhub-enabled
- security-account-information-provided
- service-catalog-shared-within-Organisation
- service-vpc-endpoint-enabled
- sns-encrypted-kms
- sns-topic-message-delivery-Benachrichtigung aktiviert
- sns-topic-no-public-Zugriff
- sqs-queue-no-public-Zugang
- ssm-automation-block-public-teilen
- ssm-automation-logging-enabled
- ssm-document-not-public
- ssm-document-tagged
- step-functions-state-machine-Protokollierung aktiviert
- storagegateway-last-backup-recovery-punkt-erstellt
- storagegateway-resources-in-logically-air-gapped-vault
- storagegateway-resources-protected-by-Ersatzplan
- subnet-auto-assign-public-ip-deaktiviert
- transfer-agreement-description
- transfer-agreement-tagged
- transfer-certificate-description
- transfer-certificate-tagged
- transfer-connector-logging-enabled
- transfer-connector-tagged
- transfer-family-server-no-ftp
- transfer-profile-tagged

- transfer-workflow-description
- transfer-workflow-tagged
- virtualmachine-last-backup-recovery-Punkt erstellt
- virtualmachine-resources-in-logically-air-gapped-vault
- virtualmachine-resources-protected-by-Ersatzplan
- vpc-default-security-group-geschlossen
- vpc-endpoint-enabled
- vpc-flow-logs-enabled
- vpc-network-acl-unused-überprüfen
- vpc-peering-dns-resolution-überprüfen
- vpc-sg-open-only-to-authorized-ports
- vpc-sg-port-restriction-überprüfen
- vpc-vpn-2-tunnels-up
- wafv2-logging-enabled
- WAF 2- rulegroup-logging-enabled
- WAF 2- rulegroup-not-empty
- WAF 2- webacl-not-empty
- waf-regional-rulegroup-not-leer
- waf-regional-rule-not-leer
- waf-regional-webacl-not-leer

Region USA West (Oregon)

USA West (Oregon)

- access-keys-rotated
- account-part-of-organizations
- acmpca-certificate-authority-tagged
- acm-certificate-expiration-check
- acm-certificate-rsa-check
- acm-pca-root-ca-deaktiviert
- active-mq-supported-version

- alb-desync-mode-check
- alb-http-drop-invalid-Header-fähig
- alb-http-to-https-Umleitungsprüfung
- alb-internal-scheme-check
- alb-listener-tagged
- alb-waf-enabled
- amplify-app-branch-auto-löschung aktiviert
- amplify-app-description
- amplify-app-tagged
- amplify-branch-performance-mode-aktiviert
- amplify-branch-tagged
- api-gwv2- access-logs-enabled
- api-gwv2- authorization-type-configured
- api-gw-associated-with-WAF
- api-gw-cache-enabled-und-verschlüsselt
- api-gw-endpoint-type-überprüfen
- api-gw-execution-logging-aktiviert
- api-gw-ssl-enabled
- api-gw-xray-enabled
- appconfig-application-description
- appconfig-application-tagged
- appconfig-configuration-profile-tagged
- appconfig-configuration-profile-validators-nicht leer
- appconfig-deployment-strategy-description
- appconfig-deployment-strategy-replicate-zu-ssm
- appconfig-environment-description
- appconfig-environment-tagged
- appconfig-extension-association-tagged
- appconfig-freeform-profile-config-Speicher
- appconfig-hosted-configuration-version-Beschreibung

- appflow-flow-tagged
- appintegrations-event-integration-description
- appintegrations-event-integration-tagged
- appmesh-gateway-route-tagged
- appmesh-mesh-deny-tcp-Weiterleitung
- appmesh-mesh-tagged
- appmesh-route-tagged
- appmesh-virtual-gateway-backend-Standardeinstellungen-TLS
- appmesh-virtual-gateway-logging-file-path-exists
- appmesh-virtual-gateway-tagged
- appmesh-virtual-node-backend-defaults-tls-on
- appmesh-virtual-node-logging-file-path-exists
- appmesh-virtual-node-tagged
- appmesh-virtual-router-tagged
- appmesh-virtual-service-tagged
- approved-amis-by-id
- approved-amis-by-tag
- apprunner-service-in-vpc
- apprunner-service-no-public-Zugang
- apprunner-service-observability-enabled
- apprunner-service-tagged
- apprunner-vpc-connector-tagged
- appstream-fleet-in-vpc
- appsync-associated-with-waf
- appsync-authorization-check
- appsync-cache-encryption-at-ausruhen
- appsync-logging-enabled
- athena-data-catalog-description
- athena-prepared-statement-description
- athena-workgroup-description

- athena-workgroup-encrypted-at-ausruhen
- athena-workgroup-enforce-workgroup-Konfiguration
- athena-workgroup-engine-version-automatisches Upgrade
- athena-workgroup-logging-enabled
- aurora-last-backup-recovery-Punkt erstellt
- aurora-meets-restore-time-Ziel
- aurora-mysql-backtracking-enabled
- aurora-mysql-cluster-audit-Protokollierung
- aurora-resources-in-logically-air-gapped-vault
- aurora-resources-protected-by-Backup-Plan
- autoscaling-capacity-rebalancing
- autoscaling-group-elb-healthcheck-erforderlich
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-hop-Grenze
- autoscaling-launch-config-public-ip-deaktiviert
- autoscaling-launch-template
- autoscaling-multiple-az
- autoscaling-multiple-instance-types
- backup-plan-min-frequency-and-min-retention-check
- backup-recovery-point-encrypted
- backup-recovery-point-manual-Löschen-deaktiviert
- backup-recovery-point-minimum-Aufbewahrungsprüfung
- batch-compute-environment-enabled
- batch-compute-environment-managed
- batch-compute-environment-tagged
- batch-job-queue-enabled
- batch-job-queue-tagged
- batch-managed-compute-environment-using-launch-template
- batch-managed-compute-env-compute-resources-tagged
- batch-scheduling-policy-tagged

- beanstalk-enhanced-health-reporting-aktiviert
- cassandra-keyspace-tagged
- clb-desync-mode-check
- clb-multiple-az
- cloudformation-stack-drift-detection-überprüfen
- cloudformation-stack-notification-check
- cloudtrail-all-read-s3- data-event-check
- cloudtrail-all-write-s3- data-event-check
- Wolkenspur-S3- bucket-access-logging
- CloudTrail-S3- bucket-public-access-prohibited
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-action-enabled-überprüfen
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted
- cloud-trail-cloud-watch-logs-aktiviert
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-Validierung aktiviert
- cmk-backing-key-rotation-aktiviert
- codebuild-project-artifact-encryption
- codebuild-project-environment-privileged-überprüfen
- codebuild-project-envvar-awscred-überprüfen
- codebuild-project-logging-enabled
- codebuild-project-s3-log-verschlüsselt
- codebuild-project-source-repo-URL-Prüfung
- codebuild-report-group-encrypted-im Ruhezustand
- codedeploy-auto-rollback-monitor-aktiviert

- codedeploy-deployment-group-auto-rollback-aktiviert
- codedeploy-deployment-group-outdated-instanzen-aktualisieren
- Codedeploy-ec2- minimum-healthy-hosts-configured
- codedeploy-lambda-allatonce-traffic-shift-deaktiviert
- codeguruprofiler-profiling-group-tagged
- codegururevieweer-repository-association-tagged
- codepipeline-deployment-count-check
- codepipeline-region-fanout-check
- cognito-identity-pool-unauth-Zugriffsprüfung
- cognito-user-pool-advanced-sicherheitsaktiviert
- cognito-user-pool-tagged
- connect-instance-logging-enabled
- customerprofiles-object-type-allow-Profilerstellung
- customerprofiles-object-type-tagged
- custom-eventbus-policy-attached
- custom-schema-registry-policy-beigefügt
- cw-loggroup-retention-period-überprüfen
- datasync-task-data-verification-aktiviert
- datasync-task-logging-enabled
- datasync-task-tagged
- dax-encryption-enabled
- dax-tls-endpoint-encryption
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- dms-auto-minor-version-upgrade-check
- dms-endpoint-ssl-configured
- dms-endpoint-tagged
- dms-mongo-db-authentication-aktiviert
- dms-neptune-iam-authorization-aktiviert

- dms-redis-tls-enabled
- dms-replication-not-public
- dms-replication-task-sourcedb-Protokollierung
- dms-replication-task-tagged
- dms-replication-task-targetdb-Protokollierung
- docdb-cluster-audit-logging-aktiviert
- docdb-cluster-backup-retention-überprüfen
- docdb-cluster-deletion-protection-aktiviert
- docdb-cluster-encrypted
- docdb-cluster-encrypted-in-Transit
- docdb-cluster-snapshot-public-verboten
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-last-backup-recovery-Punkt erstellt
- dynamodb-meets-restore-time-Ziel
- dynamodb-pitr-enabled
- dynamodb-resources-protected-by-Backup-Plan
- dynamodb-table-deletion-protection-aktiviert
- dynamodb-table-encrypted-kms
- dynamodb-table-encryption-enabled
- dynamodb-throughput-limit-check
- ebs-in-backup-plan
- ebs-last-backup-recovery-punkt-erstellt
- ebs-meets-restore-time-Ziel
- ebs-optimized-instance
- ebs-resources-in-logically-air-gapped-vault
- ebs-resources-protected-by-Backup-Plan
- ebs-snapshot-public-restorable-überprüfen
- ec2- capacity-reservation-tagged
- ec2- carrier-gateway-tagged

- ec2- aktiviert client-vpn-connection-log
- ec2- client-vpn-endpoint-tagged
- ec2- -alle client-vpn-not-authorize
- ec2- dhcp-options-tagged
- ec2- ebs-encryption-by-default
- ec2- aktiviert enis-source-destination-check
- ec2-fleet-markiert
- ec2-imdsv2-check
- ec2- instance-detailed-monitoring-enabled
- ec2-ami instance-launched-with-allowed
- ec2- instance-managed-by-ssm
- ec2- instance-multiple-eni-check
- ec2- instance-no-public-ip
- ec2- instance-profile-attached
- ec2- erstellt last-backup-recovery-point
- ec2-2-prüfen launch-template-imdsv
- ec2- -deaktiviert launch-template-public-ip
- ec2- launch-template-tagged
- ec2- managedinstance-applications-blacklisted
- ec2- managedinstance-applications-required
- ec2- prüfen managedinstance-association-compliance-status
- ec2- managedinstance-inventory-blacklisted
- ec2- prüfen managedinstance-patch-compliance-status
- ec2- managedinstance-platform-check
- ec2- meets-restore-time-target
- ec2- Analyse mit Schlagwörtern network-insights-access-scope
- ec2 network-insights-access-scope - markiert
- ec2- network-insights-path-tagged
- ec2- no-amazon-key-pair
- ec2- paravirtual-instance-check

- ec2- prefix-list-tagged
- ec2- -Tresor mit Lücken resources-in-logically-air
- ec2- resources-protected-by-backup -plan
- ec2- -eni security-group-attached-to
- ec2- -eni-periodisch security-group-attached-to
- ec2 spot-fleet-request-ct - - encryption-at-rest
- ec2-stopped-instance
- ec2- token-hop-limit-check
- ec2- traffic-mirror-filter-description
- ec2- traffic-mirror-filter-tagged
- ec2- traffic-mirror-session-description
- ec2- traffic-mirror-session-tagged
- ec2- traffic-mirror-target-description
- ec2- traffic-mirror-target-tagged
- ec2- -attach-deaktiviert transit-gateway-auto-vpc
- ec2 transit-gateway-multicast-domain - markiert
- ec2- volume-inuse-check
- ec2- vpn-connection-logging-enabled
- ecr-private-image-scanning-aktiviert
- ecr-private-lifecycle-policy-konfiguriert
- ecr-private-tag-immutability-aktiviert
- ecr-repository-cmk-encryption-aktiviert
- ecr-repository-tagged
- ecs-awsvpc-networking-enabled
- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-container-insights-enabled
- ecs-fargate-latest-platform-Version
- ecs-no-environment-secrets
- ecs-task-definition-log-Konfiguration

- ecs-task-definition-memory-hartes Limit
- ecs-task-definition-network-mode-not-host
- ecs-task-definition-nonroot-Benutzer
- ecs-task-definition-pid-Modus-Check
- ecs-task-definition-user-for-host-mode-check
- efs-access-point-enforce-Stammverzeichnis
- efs-access-point-enforce-Benutzeridentität
- efs-automatic-backups-enabled
- efs-encrypted-check
- efs-filesystem-ct-encrypted
- efs-in-backup-plan
- efs-last-backup-recovery-Punkt erstellt
- efs-meets-restore-time-Ziel
- efs-mount-target-public-zugänglich
- efs-resources-in-logically-air-gapped-vault
- efs-resources-protected-by-Backup-Plan
- eip-attached
- eks-cluster-logging-enabled
- eks-cluster-log-enabled
- eks-cluster-oldest-supported-Ausführung
- eks-cluster-secrets-encrypted
- eks-cluster-supported-version
- eks-endpoint-no-public-Zugang
- eks-secrets-encrypted
- elasticache-auto-minor-version-Upgrade-Check
- elasticache-rbac-auth-enabled
- elasticache-redis-cluster-automatic-Backup-Check
- elasticache-repl-grp-auto-failover-fähig
- elasticache-repl-grp-encrypted-im Ruhezustand
- elasticache-repl-grp-encryptedim Transit

- elasticache-repl-grp-redis-auth-aktiviert
- elasticache-subnet-group-check
- elasticache-supported-engine-version
- elasticbeanstalk-application-description
- elasticbeanstalk-application-version-description
- elasticbeanstalk-environment-description
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch
- elasticsearch-node-to-node-Verschlüsselungsprüfung
- elastic-beanstalk-logs-to- Cloudwatch
- elastic-beanstalk-managed-updates-aktiviert
- elbv2- acm-certificate-required
- elv 2- listener-encryption-in-transit
- elbv2-multiple-az
- elbv2- prüfen predefined-security-policy-ssl
- elb-acm-certificate-required
- elb-cross-zone-load-Balancing aktiviert
- elb-custom-security-policy-ssl-Prüfung
- elb-deletion-protection-enabled
- elb-logging-enabled
- elb-predefined-security-policy-ssl-Überprüfung
- elb-tls-https-listeners-nur
- emr-block-public-access
- emr-kerberos-enabled
- emr-master-no-public-ip
- emr-security-configuration-encryption-ruh dich aus
- emr-security-configuration-encryption-Transit
- encrypted-volumes
- event-data-store-cmk-Verschlüsselung aktiviert

- evidently-launch-description
- evidently-launch-tagged
- evidently-project-description
- evidently-project-tagged
- evidently-segment-description
- evidently-segment-tagged
- fis-experiment-template-log-Konfiguration ist vorhanden
- fis-experiment-template-tagged
- fms-shield-resource-policy-überprüfen
- fms-webacl-resource-policy-überprüfen
- fms-webacl-rulegroup-association-überprüfen
- frauddetector-entity-type-tagged
- frauddetector-label-tagged
- frauddetector-outcome-tagged
- frauddetector-variable-tagged
- fsx-last-backup-recovery-Punkt erstellt
- fsx-lustre-copy-tagszu Backups
- fsx-meets-restore-time-Ziel
- fsx-ontap-deployment-type-überprüfen
- fsx-openzfs-copy-tags-aktiviert
- fsx-openzfs-deployment-type-überprüfen
- fsx-resources-protected-by-Ersatzplan
- fsx-windows-audit-log-konfiguriert
- fsx-windows-deployment-type-überprüfen
- glb-listener-tagged
- global-endpoint-event-replication-aktiviert
- glue-job-logging-enabled
- glue-ml-transform-encrypted-im Ruhezustand
- glue-spark-job-supported-Ausführung
- GuardDuty-EC2- protection-runtime-enabled

- guardduty-ecs-protection-runtime-aktiviert
- guardduty-eks-protection-audit-aktiviert
- guardduty-eks-protection-runtime-aktiviert
- guardduty-enabled-centralized
- guardduty-lambda-protection-enabled
- guardduty-malware-protection-enabled
- guardduty-non-archived-findings
- guardduty-rds-protection-enabled
- guardduty-runtime-monitoring-enabled
- GuardDuty-S3-Schutz aktiviert
- iam-customer-policy-blocked-kms-Aktionen
- iam-external-access-analyzer-aktiviert
- iam-group-has-users-überprüfen
- iam-inline-policy-blocked-KMS-Aktionen
- iam-no-inline-policy-überprüfen
- iam-password-policy
- iam-policy-blacklisted-check
- iam-policy-in-use
- iam-policy-no-statements-with-admin-access
- iam-policy-no-statements-with-full-access
- iam-role-managed-policy-überprüfen
- iam-root-access-key-überprüfen
- iam-user-group-membership-überprüfen
- iam-user-mfa-enabled
- iam-user-no-policies-überprüfen
- iam-user-unused-credentials-überprüfen
- incoming-ssh-disabled
- inspector-ec2-Scan aktiviert
- inspector-ecr-scan-enabled
- inspector-lambda-code-scan-aktiviert

- inspector-lambda-standard-scan-aktiviert
- instances-in-vpc
- internet-gateway-authorized-vpc-nur
- iotevents-alarm-model-tagged
- iotevents-detector-model-tagged
- iotevents-input-tagged
- iotsitewise-asset-model-tagged
- iotsitewise-dashboard-tagged
- iotsitewise-gateway-tagged
- iotsitewise-portal-tagged
- iotsitewise-project-tagged
- iottwinmaker-component-type-tagged
- iottwinmaker-entity-tagged
- iottwinmaker-scene-tagged
- iottwinmaker-sync-job-tagged
- iottwinmaker-workspace-tagged
- iotwireless-fuota-task-tagged
- iotwireless-multicast-group-tagged
- iotwireless-service-profile-tagged
- iot-authorizer-token-signing-aktiviert
- ivs-channel-playback-authorization-aktiviert
- ivs-channel-tagged
- ivs-playback-key-pair-markiert
- ivs-recording-configuration-tagged
- kinesis-firehose-delivery-stream-verschlüsselt
- kinesis-stream-backup-retention-überprüfen
- kinesis-stream-encrypted
- kms-cmk-not-scheduled-zum Löschen
- kms-key-policy-no-öffentlicher Zugang
- lambda-concurrency-check

- lambda-dlq-check
- lambda-function-public-access-verboten
- lambda-function-settings-check
- lambda-function-xray-enabled
- lambda-inside-vpc
- lambda-vpc-multi-az-überprüfen
- lightsail-bucket-tagged
- lightsail-certificate-tagged
- lightsail-disk-tagged
- macie-auto-sensitive-data-Discovery-Check
- macie-status-check
- mariadb-publish-logs-to-Cloudwatch-Protokolle
- mfa-enabled-for-iam-Konsolenzugriff
- mq-active-broker-ldap-Authentifizierung
- mq-active-deployment-mode
- mq-active-single-instance-broker-storage-type-efs
- mq-automatic-minor-version-Upgrade aktiviert
- mq-auto-minor-version-upgrade-fähig
- mq-broker-general-logging-aktiviert
- mq-cloudwatch-audit-logging-aktiviert
- mq-cloudwatch-audit-log-aktiviert
- mq-no-public-access
- mq-rabbit-deployment-mode
- msk-cluster-public-access-deaktiviert
- msk-connect-connector-logging-aktiviert
- msk-enhanced-monitoring-enabled
- msk-in-cluster-node-require-tls
- msk-unrestricted-access-check
- multi-region-cloud-trail-aktiviert
- nacl-no-unrestricted-ssh-rdp

- neptune-cluster-backup-retention-überprüfen
- neptune-cluster-cloudwatch-log-exportfähig
- neptune-cluster-copy-tags-to-snapshot-enabled
- neptune-cluster-deletion-protection-aktiviert
- neptune-cluster-encrypted
- neptune-cluster-iam-database-Authentifizierung
- neptune-cluster-multi-az-aktiviert
- neptune-cluster-snapshot-encrypted
- neptune-cluster-snapshot-public-verboten
- netfw-deletion-protection-enabled
- netfw-logging-enabled
- netfw-multi-az-enabled
- netfw-policy-default-action-fragment-Pakete
- netfw-policy-default-action-vollständige Pakete
- netfw-policy-rule-group-assoziiert
- netfw-stateless-rule-group-nicht leer
- netfw-subnet-change-protection-aktiviert
- nlb-cross-zone-load-Balancing aktiviert
- nlb-internal-scheme-check
- nlb-listener-tagged
- nlb-logging-enabled
- no-unrestricted-route-to-igw
- opensearch-access-control-enabled
- opensearch-audit-logging-enabled
- opensearch-data-node-fault-Toleranz
- opensearch-encrypted-at-rest
- opensearch-https-required
- opensearch-in-vpc-only
- opensearch-logs-to-cloudwatch
- opensearch-node-to-node-Verschlüsselungsprüfung

- opensearch-primary-node-fault-Toleranz
- opensearch-update-check
- rabbit-mq-supported-version
- rds-aurora-mysql-audit-Protokollierung aktiviert
- rds-aurora-postgresql-logs-zu-Cloud-Watch
- rds-automatic-minor-version-upgrade-fähig
- rds-cluster-auto-minor-version-upgrade-enable
- rds-cluster-default-admin-überprüfen
- rds-cluster-deletion-protection-aktiviert
- rds-cluster-encrypted-at-ausruhen
- rds-cluster-iam-authentication-aktiviert
- rds-cluster-multi-az-aktiviert
- rds-db-security-group-nicht erlaubt
- rds-enhanced-monitoring-enabled
- rds-instance-default-admin-überprüfen
- rds-instance-deletion-protection-aktiviert
- rds-instance-iam-authentication-aktiviert
- rds-instance-public-access-überprüfen
- rds-instance-subnet-igw-überprüfen
- rds-in-backup-plan
- rds-last-backup-recovery-Punkt erstellt
- rds-logging-enabled
- rds-mariadb-instance-encryptedim Transit
- rds-meets-restore-time-Ziel
- rds-multi-az-support
- rds-mysql-instance-encryptedunterwegs
- rds-postgresql-logs-to- Cloudwatch
- rds-postgres-instance-encryptedunterwegs
- rds-proxy-tls-encryption
- rds-resources-protected-by-Backup-Plan

- rds-snapshots-public-prohibited
- rds-snapshot-encrypted
- rds-sqlserver-encrypted-in-Transit
- rds-sql-server-logszur Cloud-Überwachung
- rds-storage-encrypted
- redshift-audit-logging-enabled
- redshift-backup-enabled
- redshift-cluster-configuration-check
- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check
- redshift-cluster-multi-az-aktiviert
- redshift-cluster-parameter-group-markiert
- redshift-cluster-public-access-überprüfen
- redshift-cluster-subnet-group-Multi-Az
- redshift-default-admin-check
- redshift-default-db-name-überprüfen
- redshift-enhanced-vpc-routing-aktiviert
- redshift-require-tls-ssl
- redshift-serverless-default-admin-überprüfen
- redshift-serverless-default-db-Namenscheck
- redshift-serverless-namespace-cmk-Verschlüsselung
- redshift-serverless-publish-logs-zu-Cloud-Watch
- redshift-serverless-workgroup-encryptedauf dem Weg
- redshift-serverless-workgroup-no-öffentlich zugänglich
- redshift-serverless-workgroup-routes-innerhalb von VPC
- redshift-unrestricted-port-access
- required-tags
- restricted-incoming-traffic
- root-account-hardware-mfa-aktiviert
- root-account-mfa-enabled

- s3 -regelprüfung express-dir-bucket-lifecycle
- nur s3- access-point-in-vpc
- s3- -Blöcke access-point-public-access
- s3- -Blöcke account-level-public-access
- s3- -Blocke-periodisch account-level-public-access
- s 3- bucket-acl-prohibited
- s-3 bucket-blacklisted-actions-prohibited
- s3- bucket-cross-region-replication -aktiviert
- s-3 bucket-default-lock-enabled
- s3 bucket-level-public-access - verboten
- s3- bucket-logging-enabled
- s-3 bucket-mfa-delete-enabled
- s-3 bucket-policy-grantee-check
- s3- bucket-policy-not-more -freizügig
- s 3- bucket-public-read-prohibited
- s-3 bucket-public-write-prohibited
- s-3 bucket-replication-enabled
- s3- bucket-server-side-encryption -aktiviert
- s-3 bucket-ssl-requests-only
- s3-Bucket-Tagged
- s-3 bucket-versioning-enabled
- s-3 default-encryption-kms
- s-3 event-notifications-enabled
- s3 last-backup-recovery-point - erstellt
- s3- lifecycle-policy-check
- s-3 meets-restore-time-target
- s3- resources-in-logically-air -Tresor mit Lücken
- s3 resources-protected-by-backup - -Plan
- s 3- version-lifecycle-policy-check
- sagemaker-app-image-config-markiert

- sagemaker-domain-in-vpc
- sagemaker-domain-tagged
- sagemaker-endpoint-configuration-kms-schlüsselkonfiguriert
- sagemaker-endpoint-config-prod-Anzahl der Instanzen
- sagemaker-feature-group-tagged
- sagemaker-image-description
- sagemaker-image-tagged
- sagemaker-model-in-vpc
- sagemaker-model-isolation-enabled
- sagemaker-notebook-instance-inside-vpc
- sagemaker-notebook-instance-kms-key-konfiguriert
- sagemaker-notebook-instance-platform-Version
- sagemaker-notebook-instance-root-Zugriffsprüfung
- sagemaker-notebook-no-direct-Internetzugang
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-überprüfen
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- securityhub-enabled
- security-account-information-provided
- service-catalog-shared-within-Organisation
- service-vpc-endpoint-enabled
- ses-malware-scanning-enabled
- sns-encrypted-kms
- sns-topic-message-delivery-Benachrichtigung aktiviert
- sns-topic-no-public-Zugriff
- sqs-queue-no-public-Zugang
- ssm-automation-block-public-teilen
- ssm-automation-logging-enabled

- ssm-document-not-public
- ssm-document-tagged
- step-functions-state-machine-Protokollierung aktiviert
- storagegateway-last-backup-recovery-punkt-erstellt
- storagegateway-resources-in-logically-air-gapped-vault
- storagegateway-resources-protected-by-Ersatzplan
- subnet-auto-assign-public-ip-deaktiviert
- transfer-agreement-description
- transfer-agreement-tagged
- transfer-certificate-description
- transfer-certificate-tagged
- transfer-connector-logging-enabled
- transfer-connector-tagged
- transfer-family-server-no-ftp
- transfer-profile-tagged
- transfer-workflow-description
- transfer-workflow-tagged
- virtualmachine-last-backup-recovery-Punkt erstellt
- virtualmachine-resources-in-logically-air-gapped-vault
- virtualmachine-resources-protected-by-Ersatzplan
- vpc-default-security-group-geschlossen
- vpc-endpoint-enabled
- vpc-flow-logs-enabled
- vpc-network-acl-unused-überprüfen
- vpc-peering-dns-resolution-überprüfen
- vpc-sg-open-only-to-authorized-ports
- vpc-sg-port-restriction-überprüfen
- vpc-vpn-2-tunnels-up
- wafv2-logging-enabled
- WAF 2- rulegroup-logging-enabled

- WAF 2- rulegroup-not-empty
- WAF 2- webacl-not-empty
- waf-regional-rulegroup-not-leer
- waf-regional-rule-not-leer
- waf-regional-webacl-not-leer
- workspaces-root-volume-encryption-aktiviert
- workspaces-user-volume-encryption-aktiviert

Region Afrika (Kapstadt)

Afrika (Kapstadt)

- access-keys-rotated
- account-part-of-organizations
- acmpca-certificate-authority-tagged
- acm-certificate-expiration-check
- acm-certificate-rsa-check
- acm-pca-root-ca-deaktiviert
- active-mq-supported-version
- alb-desync-mode-check
- alb-http-drop-invalid-Header-fähig
- alb-http-to-https-Umleitungsprüfung
- alb-internal-scheme-check
- alb-listener-tagged
- alb-waf-enabled
- api-gwv2- access-logs-enabled
- api-gwv2- authorization-type-configured
- api-gw-associated-with-WAF
- api-gw-cache-enabled-und-verschlüsselt
- api-gw-endpoint-type-überprüfen
- api-gw-execution-logging-aktiviert
- api-gw-ssl-enabled

- api-gw-xray-enabled
- appconfig-application-description
- appconfig-application-tagged
- appconfig-configuration-profile-tagged
- appconfig-configuration-profile-validators-nicht leer
- appconfig-deployment-strategy-description
- appconfig-deployment-strategy-replicate-zu-ssm
- appconfig-environment-description
- appconfig-environment-tagged
- appconfig-extension-association-tagged
- appconfig-freeform-profile-config-Speicher
- appconfig-hosted-configuration-version-Beschreibung
- appflow-flow-tagged
- appintegrations-event-integration-description
- appintegrations-event-integration-tagged
- appmesh-gateway-route-tagged
- appmesh-mesh-deny-tcp-Weiterleitung
- appmesh-mesh-tagged
- appmesh-route-tagged
- appmesh-virtual-gateway-backend-Standardeinstellungen-TLS
- appmesh-virtual-gateway-logging-file-path-exists
- appmesh-virtual-gateway-tagged
- appmesh-virtual-node-backend-defaults-tls-on
- appmesh-virtual-node-logging-file-path-exists
- appmesh-virtual-node-tagged
- appmesh-virtual-router-tagged
- appmesh-virtual-service-tagged
- approved-amis-by-id
- approved-amis-by-tag
- appsync-authorization-check

- appsync-logging-enabled
- athena-data-catalog-description
- athena-prepared-statement-description
- athena-workgroup-description
- athena-workgroup-encrypted-at-ausruhen
- athena-workgroup-enforce-workgroup-Konfiguration
- athena-workgroup-engine-version-automatisches Upgrade
- athena-workgroup-logging-enabled
- aurora-last-backup-recovery-Punkt erstellt
- aurora-meets-restore-time-Ziel
- aurora-mysql-cluster-audit-Protokollierung
- aurora-resources-in-logically-air-gapped-vault
- aurora-resources-protected-by-Backup-Plan
- autoscaling-capacity-rebalancing
- autoscaling-group-elb-healthcheck-erforderlich
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-hop-Grenze
- autoscaling-launch-config-public-ip-deaktiviert
- autoscaling-launch-template
- autoscaling-multiple-az
- autoscaling-multiple-instance-types
- backup-plan-min-frequency-and-min-retention-check
- backup-recovery-point-encrypted
- backup-recovery-point-manual-Löschen-deaktiviert
- backup-recovery-point-minimum-Aufbewahrungsprüfung
- batch-compute-environment-enabled
- batch-compute-environment-managed
- batch-compute-environment-tagged
- batch-job-queue-enabled
- batch-job-queue-tagged

- batch-managed-compute-environment-using-launch-template
- batch-managed-compute-env-compute-resources-tagged
- batch-scheduling-policy-tagged
- beanstalk-enhanced-health-reporting-aktiviert
- clb-desync-mode-check
- clb-multiple-az
- cloudformation-stack-drift-detection-überprüfen
- cloudformation-stack-notification-check
- cloudtrail-all-read-s3- data-event-check
- cloudtrail-all-write-s3- data-event-check
- Wolkenspur-S3- bucket-access-logging
- CloudTrail-S3- bucket-public-access-prohibited
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-action-enabled-überprüfen
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted
- cloud-trail-cloud-watch-logs-aktiviert
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-Validierung aktiviert
- cmk-backing-key-rotation-aktiviert
- codebuild-project-artifact-encryption
- codebuild-project-environment-privileged-überprüfen
- codebuild-project-envvar-awscred-überprüfen
- codebuild-project-logging-enabled
- codebuild-project-s3-log-verschlüsselt
- codebuild-project-source-repo-URL-Prüfung

- codebuild-report-group-encrypted-im Ruhezustand
- codedeploy-auto-rollback-monitor-aktiviert
- codedeploy-deployment-group-auto-rollback-aktiviert
- codedeploy-deployment-group-outdated-instanzen-aktualisieren
- Codedeploy-ec2- minimum-healthy-hosts-configured
- codedeploy-lambda-allatonce-traffic-shift-deaktiviert
- cognito-identity-pool-unauth-Zugriffsprüfung
- cognito-user-pool-tagged
- connect-instance-logging-enabled
- customerprofiles-object-type-allow-Profilerstellung
- customerprofiles-object-type-tagged
- custom-eventbus-policy-attached
- cw-loggroup-retention-period-überprüfen
- datasync-task-data-verification-aktiviert
- datasync-task-logging-enabled
- datasync-task-tagged
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- dms-auto-minor-version-upgrade-check
- dms-endpoint-ssl-configured
- dms-endpoint-tagged
- dms-mongo-db-authentication-aktiviert
- dms-redis-tls-enabled
- dms-replication-not-public
- dms-replication-task-sourcedb-Protokollierung
- dms-replication-task-tagged
- dms-replication-task-targetdb-Protokollierung
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan

- dynamodb-last-backup-recovery-Punkt erstellt
- dynamodb-meets-restore-time-Ziel
- dynamodb-pitr-enabled
- dynamodb-resources-protected-by-Backup-Plan
- dynamodb-table-deletion-protection-aktiviert
- dynamodb-table-encrypted-kms
- dynamodb-throughput-limit-check
- ebs-in-backup-plan
- ebs-last-backup-recovery-punkt-erstellt
- ebs-meets-restore-time-Ziel
- ebs-optimized-instance
- ebs-resources-in-logically-air-gapped-vault
- ebs-resources-protected-by-Backup-Plan
- ebs-snapshot-public-restorable-überprüfen
- ec2- capacity-reservation-tagged
- ec2- aktiviert client-vpn-connection-log
- ec2- client-vpn-endpoint-tagged
- ec2- -alle client-vpn-not-authorize
- ec2- dhcp-options-tagged
- ec2- ebs-encryption-by-default
- ec2- aktiviert enis-source-destination-check
- ec2-fleet-markiert
- ec2-imdsv2-check
- ec2- instance-detailed-monitoring-enabled
- ec2-ami instance-launched-with-allowed
- ec2- instance-managed-by-ssm
- ec2- instance-multiple-eni-check
- ec2- instance-no-public-ip
- ec2- instance-profile-attached
- ec2- erstellt last-backup-recovery-point

- ec2-2-prüfen launch-template-imdsv
- ec2- -deaktiviert launch-template-public-ip
- ec2- launch-template-tagged
- ec2- managedinstance-applications-blacklisted
- ec2- managedinstance-applications-required
- ec2- managedinstance-inventory-blacklisted
- ec2- prüfen managedinstance-patch-compliance-status
- ec2- managedinstance-platform-check
- ec2- meets-restore-time-target
- ec2- Analyse mit Schlagwörtern network-insights-access-scope
- ec2 network-insights-access-scope - markiert
- ec2- network-insights-path-tagged
- ec2- no-amazon-key-pair
- ec2- prefix-list-tagged
- ec2- -Tresor mit Lücken resources-in-logically-air
- ec2- resources-protected-by-backup -plan
- ec2- -eni security-group-attached-to
- ec2- -eni-periodisch security-group-attached-to
- ec2- token-hop-limit-check
- ec2- traffic-mirror-filter-description
- ec2- traffic-mirror-filter-tagged
- ec2- -attach-deaktiviert transit-gateway-auto-vpc
- ec2 transit-gateway-multicast-domain - markiert
- ec2- volume-inuse-check
- ec2- vpn-connection-logging-enabled
- ecr-private-image-scanning-aktiviert
- ecr-private-lifecycle-policy-konfiguriert
- ecr-private-tag-immutability-aktiviert
- ecr-repository-cmk-encryption-aktiviert
- ecr-repository-tagged

- ecs-awsvpc-networking-enabled
- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-container-insights-enabled
- ecs-fargate-latest-platform-Version
- ecs-no-environment-secrets
- ecs-task-definition-log-Konfiguration
- ecs-task-definition-memory-hartes Limit
- ecs-task-definition-network-mode-not-host
- ecs-task-definition-nonroot-Benutzer
- ecs-task-definition-pid-Modus-Check
- ecs-task-definition-user-for-host-mode-check
- efs-access-point-enforce-Stammverzeichnis
- efs-access-point-enforce-Benutzeridentität
- efs-automatic-backups-enabled
- efs-encrypted-check
- efs-filesystem-ct-encrypted
- efs-in-backup-plan
- efs-last-backup-recovery-Punkt erstellt
- efs-meets-restore-time-Ziel
- efs-mount-target-public-zugänglich
- efs-resources-in-logically-air-gapped-vault
- efs-resources-protected-by-Backup-Plan
- eip-attached
- eks-cluster-logging-enabled
- eks-cluster-log-enabled
- eks-cluster-oldest-supported-Ausführung
- eks-cluster-secrets-encrypted
- eks-cluster-supported-version
- eks-endpoint-no-public-Zugang

- eks-secrets-encrypted
- elasticache-auto-minor-version-Upgrade-Check
- elasticache-rbac-auth-enabled
- elasticache-redis-cluster-automatic-Backup-Check
- elasticache-repl-grp-auto-failover-fähig
- elasticache-repl-grp-encrypted-im Ruhezustand
- elasticache-repl-grp-encryptedim Transit
- elasticache-repl-grp-redis-auth-aktiviert
- elasticache-subnet-group-check
- elasticache-supported-engine-version
- elasticbeanstalk-application-description
- elasticbeanstalk-application-version-description
- elasticbeanstalk-environment-description
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch
- elasticsearch-node-to-node-Verschlüsselungsprüfung
- elastic-beanstalk-logs-to- Cloudwatch
- elastic-beanstalk-managed-updates-aktiviert
- elbv2- acm-certificate-required
- elv 2- listener-encryption-in-transit
- elbv2-multiple-az
- elbv2- prüfen predefined-security-policy-ssl
- elb-cross-zone-load-Balancing aktiviert
- elb-custom-security-policy-ssl-Prüfung
- elb-deletion-protection-enabled
- elb-logging-enabled
- elb-predefined-security-policy-ssl-Überprüfung
- elb-tls-https-listeners-nur
- emr-block-public-access

- emr-kerberos-enabled
- emr-master-no-public-ip
- emr-security-configuration-encryption-ruh dich aus
- emr-security-configuration-encryption-Transit
- encrypted-volumes
- event-data-store-cmk-Verschlüsselung aktiviert
- fis-experiment-template-log-Konfiguration ist vorhanden
- fis-experiment-template-tagged
- fms-shield-resource-policy-überprüfen
- fms-webacl-resource-policy-überprüfen
- fms-webacl-rulegroup-association-überprüfen
- fsx-last-backup-recovery-Punkt erstellt
- fsx-lustre-copy-tagszu Backups
- fsx-meets-restore-time-Ziel
- fsx-ontap-deployment-type-überprüfen
- fsx-openzfs-copy-tags-aktiviert
- fsx-openzfs-deployment-type-überprüfen
- fsx-resources-protected-by-Ersatzplan
- fsx-windows-audit-log-konfiguriert
- fsx-windows-deployment-type-überprüfen
- glb-listener-tagged
- glue-job-logging-enabled
- glue-ml-transform-encrypted-im Ruhezustand
- glue-spark-job-supported-Ausführung
- GuardDuty-EC2- protection-runtime-enabled
- guardduty-ecs-protection-runtime-aktiviert
- guardduty-eks-protection-audit-aktiviert
- guardduty-eks-protection-runtime-aktiviert
- guardduty-enabled-centralized
- guardduty-lambda-protection-enabled

- guardduty-malware-protection-enabled
- guardduty-non-archived-findings
- guardduty-rds-protection-enabled
- guardduty-runtime-monitoring-enabled
- GuardDuty-S3-Schutz aktiviert
- iam-customer-policy-blocked-kms-Aktionen
- iam-external-access-analyzer-aktiviert
- iam-group-has-users-überprüfen
- iam-inline-policy-blocked-KMS-Aktionen
- iam-no-inline-policy-überprüfen
- iam-password-policy
- iam-policy-blacklisted-check
- iam-policy-in-use
- iam-policy-no-statements-with-admin-access
- iam-policy-no-statements-with-full-access
- iam-role-managed-policy-überprüfen
- iam-root-access-key-überprüfen
- iam-user-group-membership-überprüfen
- iam-user-mfa-enabled
- iam-user-no-policies-überprüfen
- iam-user-unused-credentials-überprüfen
- incoming-ssh-disabled
- inspector-ec2-Scan aktiviert
- inspector-ecr-scan-enabled
- inspector-lambda-standard-scan-aktiviert
- instances-in-vpc
- internet-gateway-authorized-vpc-nur
- kinesis-firehose-delivery-stream-verschlüsselt
- kinesis-stream-backup-retention-überprüfen
- kinesis-stream-encrypted

- kms-cmk-not-scheduled-zum Löschen
- kms-key-policy-no-öffentlicher Zugang
- lambda-concurrency-check
- lambda-dlq-check
- lambda-function-public-access-verboten
- lambda-function-settings-check
- lambda-function-xray-enabled
- lambda-inside-vpc
- lambda-vpc-multi-az-überprüfen
- macie-auto-sensitive-data-Discovery-Check
- macie-status-check
- mariadb-publish-logs-to-Cloudwatch-Protokolle
- mfa-enabled-for-iam-Konsolenzugriff
- mq-active-broker-ldap-Authentifizierung
- mq-active-deployment-mode
- mq-active-single-instance-broker-storage-type-efs
- mq-auto-minor-version-Upgrade aktiviert
- mq-broker-general-logging-aktiviert
- mq-cloudwatch-audit-log-aktiviert
- mq-rabbit-deployment-mode
- msk-cluster-public-access-deaktiviert
- msk-enhanced-monitoring-enabled
- msk-in-cluster-node-require-tls
- msk-unrestricted-access-check
- multi-region-cloud-trail-aktiviert
- nacl-no-unrestricted-ssh-rdp
- neptune-cluster-backup-retention-überprüfen
- neptune-cluster-cloudwatch-log-exportfähig
- neptune-cluster-copy-tags-to-snapshot-enabled
- neptune-cluster-deletion-protection-aktiviert

- neptune-cluster-encrypted
- neptune-cluster-iam-database-Authentifizierung
- neptune-cluster-multi-az-aktiviert
- neptune-cluster-snapshot-encrypted
- neptune-cluster-snapshot-public-verboten
- netfw-deletion-protection-enabled
- netfw-logging-enabled
- netfw-multi-az-enabled
- netfw-policy-default-action-fragment-Pakete
- netfw-policy-default-action-vollständige Pakete
- netfw-policy-rule-group-assoziiert
- netfw-stateless-rule-group-nicht leer
- netfw-subnet-change-protection-aktiviert
- nlb-cross-zone-load-Balancing aktiviert
- nlb-internal-scheme-check
- nlb-listener-tagged
- nlb-logging-enabled
- no-unrestricted-route-to-igw
- opensearch-access-control-enabled
- opensearch-audit-logging-enabled
- opensearch-data-node-fault-Toleranz
- opensearch-encrypted-at-rest
- opensearch-https-required
- opensearch-in-vpc-only
- opensearch-logs-to-cloudwatch
- opensearch-node-to-node-Verschlüsselungsprüfung
- opensearch-primary-node-fault-Toleranz
- opensearch-update-check
- rabbit-mq-supported-version
- rds-aurora-mysql-audit-Protokollierung aktiviert

- rds-aurora-postgresql-logs-zu-Cloud-Watch
- rds-automatic-minor-version-upgrade-fähig
- rds-cluster-auto-minor-version-upgrade-enable
- rds-cluster-default-admin-überprüfen
- rds-cluster-deletion-protection-aktiviert
- rds-cluster-encrypted-at-ausruhen
- rds-cluster-iam-authentication-aktiviert
- rds-cluster-multi-az-aktiviert
- rds-enhanced-monitoring-enabled
- rds-instance-default-admin-überprüfen
- rds-instance-deletion-protection-aktiviert
- rds-instance-iam-authentication-aktiviert
- rds-instance-public-access-überprüfen
- rds-instance-subnet-igw-überprüfen
- rds-in-backup-plan
- rds-last-backup-recovery-Punkt erstellt
- rds-logging-enabled
- rds-mariadb-instance-encryptedim Transit
- rds-meets-restore-time-Ziel
- rds-multi-az-support
- rds-mysql-instance-encryptedunterwegs
- rds-postgresql-logs-to- Cloudwatch
- rds-postgres-instance-encryptedunterwegs
- rds-proxy-tls-encryption
- rds-resources-protected-by-Backup-Plan
- rds-snapshot-encrypted
- rds-sqlserver-encrypted-in-Transit
- rds-sql-server-logszur Cloud-Überwachung
- rds-storage-encrypted
- redshift-audit-logging-enabled

- redshift-backup-enabled
- redshift-cluster-configuration-check
- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check
- redshift-cluster-multi-az-aktiviert
- redshift-cluster-parameter-group-markiert
- redshift-cluster-public-access-überprüfen
- redshift-cluster-subnet-group-Multi-Az
- redshift-default-admin-check
- redshift-default-db-name-überprüfen
- redshift-enhanced-vpc-routing-aktiviert
- redshift-require-tls-ssl
- redshift-unrestricted-port-access
- required-tags
- restricted-incoming-traffic
- root-account-hardware-mfa-aktiviert
- root-account-mfa-enabled
- nur s3- access-point-in-vpc
- s3- -Blöcke access-point-public-access
- s3- -Blöcke account-level-public-access
- s3- -Blocke-periodisch account-level-public-access
- s 3- bucket-acl-prohibited
- s-3 bucket-blacklisted-actions-prohibited
- s3- bucket-cross-region-replication -aktiviert
- s-3 bucket-default-lock-enabled
- s3 bucket-level-public-access - verboten
- s3- bucket-logging-enabled
- s-3 bucket-mfa-delete-enabled
- s-3 bucket-policy-grantee-check
- s3- bucket-policy-not-more -freizügig

- s 3- bucket-public-read-prohibited
- s-3 bucket-public-write-prohibited
- s-3 bucket-replication-enabled
- s3- bucket-server-side-encryption -aktiviert
- s-3 bucket-ssl-requests-only
- s3-Bucket-Tagged
- s-3 bucket-versioning-enabled
- s-3 default-encryption-kms
- s-3 event-notifications-enabled
- s3 last-backup-recovery-point - erstellt
- s3- lifecycle-policy-check
- s-3 meets-restore-time-target
- resources-protected-by-backups3-plan
- s 3- version-lifecycle-policy-check
- sagemaker-app-image-config-markiert
- sagemaker-domain-in-vpc
- sagemaker-domain-tagged
- sagemaker-endpoint-configuration-kms-schlüsselkonfiguriert
- sagemaker-endpoint-config-prod-Anzahl der Instanzen
- sagemaker-feature-group-tagged
- sagemaker-image-description
- sagemaker-image-tagged
- sagemaker-model-in-vpc
- sagemaker-model-isolation-enabled
- sagemaker-notebook-instance-inside-vpc
- sagemaker-notebook-instance-kms-key-konfiguriert
- sagemaker-notebook-instance-platform-Version
- sagemaker-notebook-instance-root-Zugriffsprüfung
- sagemaker-notebook-no-direct-Internetzugang
- secretsmanager-rotation-enabled-check

- secretsmanager-scheduled-rotation-success-überprüfen
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- securityhub-enabled
- security-account-information-provided
- service-catalog-shared-within-Organisation
- service-vpc-endpoint-enabled
- sns-encrypted-kms
- sns-topic-message-delivery-Benachrichtigung aktiviert
- sns-topic-no-public-Zugriff
- sqs-queue-no-public-Zugang
- ssm-automation-block-public-teilen
- ssm-automation-logging-enabled
- ssm-document-not-public
- ssm-document-tagged
- step-functions-state-machine-Protokollierung aktiviert
- storagegateway-last-backup-recovery-punkt-erstellt
- storagegateway-resources-in-logically-air-gapped-vault
- storagegateway-resources-protected-by-Ersatzplan
- subnet-auto-assign-public-ip-deaktiviert
- transfer-agreement-description
- transfer-agreement-tagged
- transfer-certificate-description
- transfer-certificate-tagged
- transfer-connector-logging-enabled
- transfer-connector-tagged
- transfer-family-server-no-ftp
- transfer-profile-tagged
- transfer-workflow-description

- transfer-workflow-tagged
- virtualmachine-last-backup-recovery-Punkt erstellt
- virtualmachine-resources-in-logically-air-gapped-vault
- virtualmachine-resources-protected-by-Ersatzplan
- vpc-default-security-group-geschlossen
- vpc-endpoint-enabled
- vpc-flow-logs-enabled
- vpc-network-acl-unused-überprüfen
- vpc-peering-dns-resolution-überprüfen
- vpc-sg-open-only-to-authorized-ports
- vpc-sg-port-restriction-überprüfen
- vpc-vpn-2-tunnels-up
- wafv2-logging-enabled
- WAF 2- rulegroup-logging-enabled
- WAF 2- rulegroup-not-empty
- WAF 2- webacl-not-empty
- waf-regional-rulegroup-not-leer
- waf-regional-rule-not-leer
- waf-regional-webacl-not-leer
- workspaces-root-volume-encryption-aktiviert
- workspaces-user-volume-encryption-aktiviert

Region Asien-Pazifik (Hongkong)

Asien-Pazifik (Hongkong)

- access-keys-rotated
- account-part-of-organizations
- acmpca-certificate-authority-tagged
- acm-certificate-expiration-check
- acm-certificate-rsa-check
- acm-pca-root-ca-deaktiviert

- active-mq-supported-version
- alb-desync-mode-check
- alb-http-drop-invalid-Header-fähig
- alb-http-to-https-Umleitungsprüfung
- alb-internal-scheme-check
- alb-listener-tagged
- alb-waf-enabled
- amplify-app-branch-auto-löschung aktiviert
- amplify-app-description
- amplify-app-tagged
- amplify-branch-performance-mode-aktiviert
- amplify-branch-tagged
- api-gwv2- access-logs-enabled
- api-gwv2- authorization-type-configured
- api-gw-associated-with-WAF
- api-gw-cache-enabled-und-verschlüsselt
- api-gw-endpoint-type-überprüfen
- api-gw-execution-logging-aktiviert
- api-gw-ssl-enabled
- api-gw-xray-enabled
- appconfig-application-description
- appconfig-application-tagged
- appconfig-configuration-profile-tagged
- appconfig-configuration-profile-validators-nicht leer
- appconfig-deployment-strategy-description
- appconfig-deployment-strategy-replicate-zu-ssm
- appconfig-environment-description
- appconfig-environment-tagged
- appconfig-extension-association-tagged
- appconfig-freeform-profile-config-Speicher

- appconfig-hosted-configuration-version-Beschreibung
- appmesh-gateway-route-tagged
- appmesh-mesh-deny-tcp-Weiterleitung
- appmesh-mesh-tagged
- appmesh-route-tagged
- appmesh-virtual-gateway-backend-Standardeinstellungen-TLS
- appmesh-virtual-gateway-logging-file-path-exists
- appmesh-virtual-gateway-tagged
- appmesh-virtual-node-backend-defaults-tls-on
- appmesh-virtual-node-logging-file-path-exists
- appmesh-virtual-node-tagged
- appmesh-virtual-router-tagged
- appmesh-virtual-service-tagged
- approved-amis-by-id
- approved-amis-by-tag
- appsync-associated-with-waf
- appsync-authorization-check
- appsync-cache-encryption-at-ausruhen
- appsync-logging-enabled
- athena-data-catalog-description
- athena-prepared-statement-description
- athena-workgroup-description
- athena-workgroup-encrypted-at-ausruhen
- athena-workgroup-enforce-workgroup-Konfiguration
- athena-workgroup-engine-version-automatisches Upgrade
- athena-workgroup-logging-enabled
- aurora-last-backup-recovery-Punkt erstellt
- aurora-meets-restore-time-Ziel
- aurora-mysql-cluster-audit-Protokollierung
- aurora-resources-in-logically-air-gapped-vault

- aurora-resources-protected-by-Backup-Plan
- autoscaling-capacity-rebalancing
- autoscaling-group-elb-healthcheck-erforderlich
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-hop-Grenze
- autoscaling-launch-config-public-ip-deaktiviert
- autoscaling-launch-template
- autoscaling-multiple-az
- autoscaling-multiple-instance-types
- backup-plan-min-frequency-and-min-retention-check
- backup-recovery-point-encrypted
- backup-recovery-point-manual-Löschen-deaktiviert
- backup-recovery-point-minimum-Aufbewahrungsprüfung
- batch-compute-environment-enabled
- batch-compute-environment-managed
- batch-compute-environment-tagged
- batch-job-queue-enabled
- batch-job-queue-tagged
- batch-managed-compute-environment-using-launch-template
- batch-managed-compute-env-compute-resources-tagged
- batch-scheduling-policy-tagged
- beanstalk-enhanced-health-reporting-aktiviert
- cassandra-keyspace-tagged
- clb-desync-mode-check
- clb-multiple-az
- cloudformation-stack-drift-detection-überprüfen
- cloudformation-stack-notification-check
- cloudtrail-all-read-s3- data-event-check
- cloudtrail-all-write-s3- data-event-check
- Wolkenspur-S3- bucket-access-logging

- CloudTrail-S3- bucket-public-access-prohibited
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-action-enabled-überprüfen
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted
- cloud-trail-cloud-watch-logs-aktiviert
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-Validierung aktiviert
- cmk-backing-key-rotation-aktiviert
- codebuild-project-artifact-encryption
- codebuild-project-environment-privileged-überprüfen
- codebuild-project-envvar-awscred-überprüfen
- codebuild-project-logging-enabled
- codebuild-project-s3-log-verschlüsselt
- codebuild-project-source-repo-URL-Prüfung
- codebuild-report-group-encrypted-im Ruhezustand
- codedeploy-auto-rollback-monitor-aktiviert
- codedeploy-deployment-group-auto-rollback-aktiviert
- codedeploy-deployment-group-outdated-instanzen-aktualisieren
- Codedeploy-ec2- minimum-healthy-hosts-configured
- codedeploy-lambda-allatonce-traffic-shift-deaktiviert
- codepipeline-deployment-count-check
- cognito-identity-pool-unauth-Zugriffsprüfung
- cognito-user-pool-tagged
- custom-eventbus-policy-attached
- custom-schema-registry-policy-beigefügt

- cw-loggroup-retention-period-überprüfen
- datasync-task-data-verification-aktiviert
- datasync-task-logging-enabled
- datasync-task-tagged
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- dms-auto-minor-version-aktualisieren-Prüfung
- dms-endpoint-ssl-configured
- dms-endpoint-tagged
- dms-mongo-db-authentication-aktiviert
- dms-neptune-iam-authorization-aktiviert
- dms-redis-tls-enabled
- dms-replication-not-public
- dms-replication-task-sourcedb-Protokollierung
- dms-replication-task-tagged
- dms-replication-task-targetdb-Protokollierung
- docdb-cluster-audit-logging-aktiviert
- docdb-cluster-backup-retention-überprüfen
- docdb-cluster-deletion-protection-aktiviert
- docdb-cluster-encrypted
- docdb-cluster-encrypted-in-Transit
- docdb-cluster-snapshot-public-verboten
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-last-backup-recovery-Punkt erstellt
- dynamodb-meets-restore-time-Ziel
- dynamodb-pitr-enabled
- dynamodb-resources-protected-by-Backup-Plan
- dynamodb-table-deletion-protection-aktiviert

- dynamodb-table-encrypted-kms
- dynamodb-throughput-limit-check
- ebs-in-backup-plan
- ebs-last-backup-recovery-punkt-erstellt
- ebs-meets-restore-time-Ziel
- ebs-optimized-instance
- ebs-resources-in-logically-air-gapped-vault
- ebs-resources-protected-by-Backup-Plan
- ebs-snapshot-public-restorable-überprüfen
- ec2- capacity-reservation-tagged
- ec2- aktiviert client-vpn-connection-log
- ec2- client-vpn-endpoint-tagged
- ec2- -alle client-vpn-not-authorize
- ec2- dhcp-options-tagged
- ec2- ebs-encryption-by-default
- ec2- aktiviert enis-source-destination-check
- ec2-fleet-markiert
- ec2-imdsv2-check
- ec2- instance-detailed-monitoring-enabled
- ec2-ami instance-launched-with-allowed
- ec2- instance-managed-by-ssm
- ec2- instance-multiple-eni-check
- ec2- instance-no-public-ip
- ec2- instance-profile-attached
- ec2- erstellt last-backup-recovery-point
- ec2-2-prüfen launch-template-imdsv
- ec2- -deaktiviert launch-template-public-ip
- ec2- launch-template-tagged
- ec2- managedinstance-applications-blacklisted
- ec2- managedinstance-applications-required

- ec2- prüfen managedinstance-association-compliance-status
- ec2- managedinstance-inventory-blacklisted
- ec2- prüfen managedinstance-patch-compliance-status
- ec2- managedinstance-platform-check
- ec2- meets-restore-time-target
- ec2- Analyse mit Schlagwörtern network-insights-access-scope
- ec2 network-insights-access-scope - markiert
- ec2- network-insights-path-tagged
- ec2- no-amazon-key-pair
- ec2- prefix-list-tagged
- ec2- -Tresor mit Lücken resources-in-logically-air
- ec2- resources-protected-by-backup -plan
- ec2- -eni security-group-attached-to
- ec2- -eni-periodisch security-group-attached-to
- ec2-stopped-instance
- ec2- token-hop-limit-check
- ec2- traffic-mirror-filter-description
- ec2- traffic-mirror-filter-tagged
- ec2- traffic-mirror-session-description
- ec2- traffic-mirror-session-tagged
- ec2- traffic-mirror-target-description
- ec2- traffic-mirror-target-tagged
- ec2- -attach-deaktiviert transit-gateway-auto-vpc
- ec2 transit-gateway-multicast-domain - markiert
- ec2- volume-inuse-check
- ec2- vpn-connection-logging-enabled
- ecr-private-image-scanning-aktiviert
- ecr-private-lifecycle-policy-konfiguriert
- ecr-private-tag-immutability-aktiviert
- ecr-repository-cmk-encryption-aktiviert

- ecr-repository-tagged
- ecs-awsvpc-networking-enabled
- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-container-insights-enabled
- ecs-fargate-latest-platform-Version
- ecs-no-environment-secrets
- ecs-task-definition-log-Konfiguration
- ecs-task-definition-memory-hartes Limit
- ecs-task-definition-network-mode-not-host
- ecs-task-definition-nonroot-Benutzer
- ecs-task-definition-pid-Modus-Check
- ecs-task-definition-user-for-host-mode-check
- efs-access-point-enforce-Stammverzeichnis
- efs-access-point-enforce-Benutzeridentität
- efs-automatic-backups-enabled
- efs-encrypted-check
- efs-filesystem-ct-encrypted
- efs-in-backup-plan
- efs-last-backup-recovery-Punkt erstellt
- efs-meets-restore-time-Ziel
- efs-mount-target-public-zugänglich
- efs-resources-in-logically-air-gapped-vault
- efs-resources-protected-by-Backup-Plan
- eip-attached
- eks-cluster-logging-enabled
- eks-cluster-log-enabled
- eks-cluster-oldest-supported-Ausführung
- eks-cluster-secrets-encrypted
- eks-cluster-supported-version

- eks-endpoint-no-public-Zugang
- eks-secrets-encrypted
- elasticache-auto-minor-version-Upgrade-Check
- elasticache-rbac-auth-enabled
- elasticache-redis-cluster-automatic-Backup-Check
- elasticache-repl-grp-auto-failover-fähig
- elasticache-repl-grp-encrypted-im Ruhezustand
- elasticache-repl-grp-encryptedim Transit
- elasticache-repl-grp-redis-auth-aktiviert
- elasticache-subnet-group-check
- elasticache-supported-engine-version
- elasticbeanstalk-application-description
- elasticbeanstalk-application-version-description
- elasticbeanstalk-environment-description
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch
- elasticsearch-node-to-node-Verschlüsselungsprüfung
- elastic-beanstalk-logs-to- Cloudwatch
- elastic-beanstalk-managed-updates-aktiviert
- elbv2- acm-certificate-required
- elv 2- listener-encryption-in-transit
- elbv2-multiple-az
- elbv2- -prüfen predefined-security-policy-ssl
- elb-acm-certificate-required
- elb-cross-zone-load-Balancing aktiviert
- elb-custom-security-policy-ssl-Prüfung
- elb-deletion-protection-enabled
- elb-logging-enabled
- elb-predefined-security-policy-ssl-Überprüfung

- elb-tls-https-listeners-nur
- emr-block-public-access
- emr-kerberos-enabled
- emr-master-no-public-ip
- emr-security-configuration-encryption-ruh dich aus
- emr-security-configuration-encryption-Transit
- encrypted-volumes
- event-data-store-cmk-Verschlüsselung aktiviert
- fis-experiment-template-log-Konfiguration ist vorhanden
- fis-experiment-template-tagged
- fms-shield-resource-policy-überprüfen
- fms-webacl-resource-policy-überprüfen
- fms-webacl-rulegroup-association-überprüfen
- fsx-last-backup-recovery-Punkt erstellt
- fsx-lustre-copy-tagszu Backups
- fsx-meets-restore-time-Ziel
- fsx-ontap-deployment-type-überprüfen
- fsx-openzfs-copy-tags-aktiviert
- fsx-openzfs-deployment-type-überprüfen
- fsx-resources-protected-by-Backup-Plan
- fsx-windows-audit-log-konfiguriert
- fsx-windows-deployment-type-überprüfen
- glb-listener-tagged
- glue-job-logging-enabled
- glue-ml-transform-encrypted-im Ruhezustand
- glue-spark-job-supported-Ausführung
- GuardDuty-EC2- protection-runtime-enabled
- guardduty-ecs-protection-runtime-aktiviert
- guardduty-eks-protection-audit-aktiviert
- guardduty-eks-protection-runtime-aktiviert

- guardduty-enabled-centralized
- guardduty-lambda-protection-enabled
- guardduty-malware-protection-enabled
- guardduty-non-archived-findings
- guardduty-rds-protection-enabled
- guardduty-runtime-monitoring-enabled
- GuardDuty-S3-Schutz aktiviert
- iam-customer-policy-blocked-kms-Aktionen
- iam-external-access-analyzer-aktiviert
- iam-group-has-users-überprüfen
- iam-inline-policy-blocked-kms-Aktionen
- iam-no-inline-policy-überprüfen
- iam-password-policy
- iam-policy-blacklisted-check
- iam-policy-in-use
- iam-policy-no-statements-with-admin-access
- iam-policy-no-statements-with-full-access
- iam-role-managed-policy-überprüfen
- iam-root-access-key-überprüfen
- iam-user-group-membership-überprüfen
- iam-user-mfa-enabled
- iam-user-no-policies-überprüfen
- iam-user-unused-credentials-überprüfen
- incoming-ssh-disabled
- inspector-ec2-Scan aktiviert
- inspector-ecr-scan-enabled
- inspector-lambda-standard-scan-aktiviert
- instances-in-vpc
- internet-gateway-authorized-vpc-nur
- iot-authorizer-token-signing-aktiviert

- kinesis-firehose-delivery-stream-verschlüsselt
- kinesis-stream-backup-retention-überprüfen
- kinesis-stream-encrypted
- kms-cmk-not-scheduled-zum Löschen
- kms-key-policy-no-öffentlicher Zugang
- lambda-concurrency-check
- lambda-dlq-check
- lambda-function-public-access-verboten
- lambda-function-settings-check
- lambda-function-xray-enabled
- lambda-inside-vpc
- lambda-vpc-multi-az-überprüfen
- macie-auto-sensitive-data-Discovery-Check
- macie-status-check
- mariadb-publish-logs-to-Cloudwatch-Protokolle
- mfa-enabled-for-iam-Konsolenzugriff
- mq-active-broker-ldap-Authentifizierung
- mq-active-deployment-mode
- mq-active-single-instance-broker-storage-type-efs
- mq-automatic-minor-version-Upgrade aktiviert
- mq-auto-minor-version-upgrade-fähig
- mq-broker-general-logging-aktiviert
- mq-cloudwatch-audit-logging-aktiviert
- mq-cloudwatch-audit-log-aktiviert
- mq-no-public-access
- mq-rabbit-deployment-mode
- msk-cluster-public-access-deaktiviert
- msk-enhanced-monitoring-enabled
- msk-in-cluster-node-require-tls
- msk-unrestricted-access-check

- multi-region-cloud-trail-aktiviert
- nacl-no-unrestricted-ssh-rdp
- neptune-cluster-backup-retention-überprüfen
- neptune-cluster-cloudwatch-log-exportfähig
- neptune-cluster-copy-tags-to-snapshot-enabled
- neptune-cluster-deletion-protection-aktiviert
- neptune-cluster-encrypted
- neptune-cluster-iam-database-Authentifizierung
- neptune-cluster-multi-az-aktiviert
- neptune-cluster-snapshot-encrypted
- neptune-cluster-snapshot-public-verboten
- netfw-deletion-protection-enabled
- netfw-logging-enabled
- netfw-multi-az-enabled
- netfw-policy-default-action-fragment-Pakete
- netfw-policy-default-action-vollständige Pakete
- netfw-policy-rule-group-assoziiert
- netfw-stateless-rule-group-nicht leer
- netfw-subnet-change-protection-aktiviert
- nlb-cross-zone-load-Balancing aktiviert
- nlb-internal-scheme-check
- nlb-listener-tagged
- nlb-logging-enabled
- no-unrestricted-route-to-igw
- opensearch-access-control-enabled
- opensearch-audit-logging-enabled
- opensearch-data-node-fault-Toleranz
- opensearch-encrypted-at-rest
- opensearch-https-required
- opensearch-in-vpc-only

- opensearch-logs-to-cloudwatch
- opensearch-node-to-node-Verschlüsselungsprüfung
- opensearch-primary-node-fault-Toleranz
- opensearch-update-check
- rabbit-mq-supported-version
- rds-aurora-mysql-audit-Protokollierung aktiviert
- rds-aurora-postgresql-logs-zu-Cloud-Watch
- rds-automatic-minor-version-upgrade-fähig
- rds-cluster-auto-minor-version-upgrade-enable
- rds-cluster-default-admin-überprüfen
- rds-cluster-deletion-protection-aktiviert
- rds-cluster-encrypted-at-ausruhen
- rds-cluster-iam-authentication-aktiviert
- rds-cluster-multi-az-aktiviert
- rds-enhanced-monitoring-enabled
- rds-instance-default-admin-überprüfen
- rds-instance-deletion-protection-aktiviert
- rds-instance-iam-authentication-aktiviert
- rds-instance-public-access-überprüfen
- rds-instance-subnet-igw-überprüfen
- rds-in-backup-plan
- rds-last-backup-recovery-Punkt erstellt
- rds-logging-enabled
- rds-mariadb-instance-encryptedim Transit
- rds-meets-restore-time-Ziel
- rds-multi-az-support
- rds-mysql-instance-encryptedim Transit
- rds-postgresql-logs-to- Cloudwatch
- rds-postgres-instance-encryptedunterwegs
- rds-proxy-tls-encryption

- rds-resources-protected-by-Backup-Plan
- rds-snapshots-public-prohibited
- rds-snapshot-encrypted
- rds-sqlserver-encrypted-in-Transit
- rds-sql-server-logszur Cloud-Überwachung
- rds-storage-encrypted
- redshift-audit-logging-enabled
- redshift-backup-enabled
- redshift-cluster-configuration-check
- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check
- redshift-cluster-multi-az-aktiviert
- redshift-cluster-parameter-group-markiert
- redshift-cluster-public-access-überprüfen
- redshift-cluster-subnet-group-Multi-Az
- redshift-default-admin-check
- redshift-default-db-name-überprüfen
- redshift-enhanced-vpc-routing-aktiviert
- redshift-require-tls-ssl
- redshift-serverless-default-admin-überprüfen
- redshift-serverless-default-db-Namenscheck
- redshift-serverless-namespace-cmk-Verschlüsselung
- redshift-serverless-publish-logs-zu-Cloud-Watch
- redshift-serverless-workgroup-no-öffentlicher Zugang
- redshift-unrestricted-port-access
- required-tags
- restricted-incoming-traffic
- root-account-hardware-mfa-aktiviert
- root-account-mfa-enabled
- nur s3- access-point-in-vpc

- s3- -Blöcke access-point-public-access
- s3- -Blöcke account-level-public-access
- s3- -Blocke-periodisch account-level-public-access
- s 3- bucket-acl-prohibited
- s-3 bucket-blacklisted-actions-prohibited
- s3- bucket-cross-region-replication -aktiviert
- s-3 bucket-default-lock-enabled
- s3 bucket-level-public-access - verboten
- s3- bucket-logging-enabled
- s-3 bucket-mfa-delete-enabled
- s-3 bucket-policy-grantee-check
- s3- bucket-policy-not-more -freizügig
- s 3- bucket-public-read-prohibited
- s-3 bucket-public-write-prohibited
- s-3 bucket-replication-enabled
- s3- bucket-server-side-encryption -aktiviert
- s-3 bucket-ssl-requests-only
- s3-Bucket-Tagged
- s-3 bucket-versioning-enabled
- s-3 default-encryption-kms
- s-3 event-notifications-enabled
- s3 last-backup-recovery-point - erstellt
- s3- lifecycle-policy-check
- s-3 meets-restore-time-target
- resources-protected-by-backups3-plan
- s 3- version-lifecycle-policy-check
- sagemaker-app-image-config-markiert
- sagemaker-domain-in-vpc
- sagemaker-domain-tagged
- sagemaker-endpoint-configuration-kms-schlüsselkonfiguriert

- sagemaker-endpoint-config-prod-Anzahl der Instanzen
- sagemaker-feature-group-tagged
- sagemaker-image-description
- sagemaker-image-tagged
- sagemaker-model-in-vpc
- sagemaker-model-isolation-enabled
- sagemaker-notebook-instance-inside-vpc
- sagemaker-notebook-instance-kms-key-konfiguriert
- sagemaker-notebook-instance-platform-Version
- sagemaker-notebook-instance-root-Zugriffsprüfung
- sagemaker-notebook-no-direct-Internetzugang
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-überprüfen
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- securityhub-enabled
- security-account-information-provided
- service-catalog-shared-within-Organisation
- service-vpc-endpoint-enabled
- sns-encrypted-kms
- sns-topic-message-delivery-Benachrichtigung aktiviert
- sns-topic-no-public-Zugriff
- sqs-queue-no-public-Zugang
- ssm-automation-block-public-teilen
- ssm-automation-logging-enabled
- ssm-document-not-public
- ssm-document-tagged
- step-functions-state-machine-Protokollierung aktiviert
- storagegateway-last-backup-recovery-punkt-erstellt

- storagegateway-resources-in-logically-air-gapped-vault
- storagegateway-resources-protected-by-Ersatzplan
- subnet-auto-assign-public-ip-deaktiviert
- transfer-agreement-description
- transfer-agreement-tagged
- transfer-certificate-description
- transfer-certificate-tagged
- transfer-connector-logging-enabled
- transfer-connector-tagged
- transfer-family-server-no-ftp
- transfer-profile-tagged
- transfer-workflow-description
- transfer-workflow-tagged
- virtualmachine-last-backup-recovery-punkt-erstellt
- virtualmachine-resources-in-logically-air-gapped-vault
- virtualmachine-resources-protected-by-Ersatzplan
- vpc-default-security-group-geschlossen
- vpc-endpoint-enabled
- vpc-flow-logs-enabled
- vpc-network-acl-unused-überprüfen
- vpc-peering-dns-resolution-überprüfen
- vpc-sg-open-only-to-authorized-ports
- vpc-sg-port-restriction-überprüfen
- vpc-vpn-2-tunnels-up
- wafv2-logging-enabled
- WAF 2- rulegroup-logging-enabled
- WAF 2- rulegroup-not-empty
- WAF 2- webacl-not-empty
- waf-regional-rulegroup-not-leer
- waf-regional-rule-not-leer

- waf-regional-webacl-not-leer

Region Asien-Pazifik (Hyderabad)

Asien-Pazifik (Hyderabad)

- account-part-of-organizations
- acmpca-certificate-authority-tagged
- acm-certificate-expiration-check
- acm-certificate-rsa-check
- acm-pca-root-ca-deaktiviert
- alb-desync-mode-check
- alb-http-drop-invalid-Header-fähig
- alb-http-to-https-Umleitungsprüfung
- alb-internal-scheme-check
- alb-waf-enabled
- api-gw-associated-with-WAF
- api-gw-cache-enabled-und-verschlüsselt
- api-gw-endpoint-type-überprüfen
- api-gw-execution-logging-aktiviert
- api-gw-ssl-enabled
- api-gw-xray-enabled
- appconfig-deployment-strategy-description
- appconfig-deployment-strategy-replicate-zu-ssm
- appconfig-extension-association-tagged
- approved-amis-by-id
- approved-amis-by-tag
- appsync-authorization-check
- appsync-logging-enabled
- athena-data-catalog-description
- athena-prepared-statement-description
- athena-workgroup-description

- athena-workgroup-enforce-workgroup-Konfiguration
- athena-workgroup-engine-version-automatisches Upgrade
- athena-workgroup-logging-enabled
- aurora-last-backup-recovery-Punkt erstellt
- aurora-meets-restore-time-Ziel
- aurora-mysql-cluster-audit-Protokollierung
- aurora-resources-in-logically-air-gapped-vault
- aurora-resources-protected-by-Backup-Plan
- autoscaling-group-elb-healthcheck-erforderlich
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-hop-Grenze
- autoscaling-launch-config-public-ip-deaktiviert
- autoscaling-launch-template
- autoscaling-multiple-az
- autoscaling-multiple-instance-types
- backup-plan-min-frequency-and-min-retention-check
- backup-recovery-point-encrypted
- backup-recovery-point-manual-Löschen-deaktiviert
- backup-recovery-point-minimum-Aufbewahrungsprüfung
- batch-compute-environment-enabled
- batch-compute-environment-managed
- batch-compute-environment-tagged
- batch-job-queue-enabled
- batch-job-queue-tagged
- batch-managed-compute-environment-using-launch-template
- batch-managed-compute-env-compute-resources-tagged
- batch-scheduling-policy-tagged
- clb-multiple-az
- cloudtrail-all-read-s3- data-event-check
- cloudtrail-all-write-s3- data-event-check

- Wolkenspur-S3- bucket-access-logging
- CloudTrail-S3- bucket-public-access-prohibited
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-action-enabled-überprüfen
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted
- cloud-trail-cloud-watch-logs-aktiviert
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-Validierung aktiviert
- cmk-backing-key-rotation-aktiviert
- codebuild-project-envvar-awscred-überprüfen
- codebuild-project-logging-enabled
- codebuild-project-s3-log-verschlüsselt
- codebuild-project-source-repo-URL-Prüfung
- codebuild-report-group-encrypted-im Ruhezustand
- codepipeline-deployment-count-check
- codepipeline-region-fanout-check
- cognito-user-pool-tagged
- custom-eventbus-policy-attached
- cw-loggroup-retention-period-überprüfen
- datasync-task-data-verification-aktiviert
- datasync-task-logging-enabled
- datasync-task-tagged
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type

- dms-replication-not-public
- docdb-cluster-audit-logging-aktiviert
- docdb-cluster-backup-retention-überprüfen
- docdb-cluster-deletion-protection-aktiviert
- docdb-cluster-encrypted
- docdb-cluster-encrypted-in-Transit
- docdb-cluster-snapshot-public-verboten
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-last-backup-recovery-Punkt erstellt
- dynamodb-meets-restore-time-Ziel
- dynamodb-pitr-enabled
- dynamodb-resources-protected-by-Backup-Plan
- dynamodb-table-deletion-protection-aktiviert
- dynamodb-table-encrypted-kms
- dynamodb-throughput-limit-check
- ebs-in-backup-plan
- ebs-last-backup-recovery-punkt-erstellt
- ebs-meets-restore-time-Ziel
- ebs-optimized-instance
- ebs-resources-in-logically-air-gapped-vault
- ebs-resources-protected-by-Backup-Plan
- ebs-snapshot-public-restorable-überprüfen
- ec2- capacity-reservation-tagged
- ec2- dhcp-options-tagged
- ec2- ebs-encryption-by-default
- ec2-Fleet-markiert
- ec2-imdsv2-check
- ec2- instance-detailed-monitoring-enabled
- ec2-ami instance-launched-with-allowed

- ec2- instance-managed-by-ssm
- ec2- instance-multiple-eni-check
- ec2- instance-no-public-ip
- ec2- instance-profile-attached
- ec2- erstellt last-backup-recovery-point
- ec2- managedinstance-applications-blacklisted
- ec2- managedinstance-applications-required
- ec2- managedinstance-inventory-blacklisted
- ec2- prüfen managedinstance-patch-compliance-status
- ec2- managedinstance-platform-check
- ec2- meets-restore-time-target
- ec2- prefix-list-tagged
- ec2- -Tresor mit Lücken resources-in-logically-air
- ec2- resources-protected-by-backup -plan
- ec2- -eni security-group-attached-to
- ec2-stopped-instance
- ec2- traffic-mirror-filter-description
- ec2- traffic-mirror-filter-tagged
- ec2- -attach-deaktiviert transit-gateway-auto-vpc
- ec2 transit-gateway-multicast-domain - markiert
- ec2- volume-inuse-check
- ec2- vpn-connection-logging-enabled
- ecr-private-image-scanning-aktiviert
- ecr-private-lifecycle-policy-konfiguriert
- ecr-private-tag-immutability-aktiviert
- ecr-repository-cmk-encryption-aktiviert
- ecr-repository-tagged
- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-container-insights-enabled

- ecs-fargate-latest-platform-Version
- ecs-no-environment-secrets
- ecs-task-definition-log-Konfiguration
- ecs-task-definition-network-mode-not-host
- ecs-task-definition-pid-Modus-Überprüfung
- ecs-task-definition-user-for-host-mode-check
- efs-access-point-enforce-Stammverzeichnis
- efs-access-point-enforce-Benutzeridentität
- efs-automatic-backups-enabled
- efs-encrypted-check
- efs-filesystem-ct-encrypted
- efs-in-backup-plan
- efs-last-backup-recovery-Punkt erstellt
- efs-meets-restore-time-Ziel
- efs-mount-target-public-zugänglich
- efs-resources-in-logically-air-gapped-vault
- efs-resources-protected-by-Backup-Plan
- eip-attached
- eks-cluster-log-enabled
- eks-cluster-secrets-encrypted
- eks-cluster-supported-version
- eks-endpoint-no-public-Zugang
- eks-secrets-encrypted
- elasticache-auto-minor-version-Upgrade-Check
- elasticache-redis-cluster-automatic-Backup-Check
- elasticache-repl-grp-auto-failover-fähig
- elasticache-repl-grp-encrypted-im Ruhezustand
- elasticache-repl-grp-encryptedim Transit
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only

- elasticsearch-logs-to-cloudwatch
- elasticsearch-node-to-node-Verschlüsselungsprüfung
- elbv2-multiple-az
- elb-acm-certificate-required
- elb-cross-zone-load-Balancing aktiviert
- elb-custom-security-policy-ssl-Prüfung
- elb-deletion-protection-enabled
- elb-logging-enabled
- elb-predefined-security-policy-ssl-Überprüfung
- elb-tls-https-listeners-nur
- emr-block-public-access
- emr-kerberos-enabled
- emr-master-no-public-ip
- emr-security-configuration-encryption-ruh dich aus
- emr-security-configuration-encryption-Transit
- encrypted-volumes
- event-data-store-cmk-Verschlüsselung aktiviert
- fms-shield-resource-policy-überprüfen
- fms-webacl-resource-policy-überprüfen
- fms-webacl-rulegroup-association-überprüfen
- fsx-last-backup-recovery-Punkt erstellt
- fsx-lustre-copy-tagszu Backups
- fsx-meets-restore-time-Ziel
- fsx-ontap-deployment-type-überprüfen
- fsx-openzfs-copy-tags-aktiviert
- fsx-openzfs-deployment-type-überprüfen
- fsx-resources-protected-by-Backup-Plan
- fsx-windows-audit-log-konfiguriert
- fsx-windows-deployment-type-überprüfen
- glue-job-logging-enabled

- glue-ml-transform-encrypted-im Ruhezustand
- glue-spark-job-supported-Ausführung
- GuardDuty-EC2- protection-runtime-enabled
- guardduty-ecs-protection-runtime-aktiviert
- guardduty-eks-protection-audit-aktiviert
- guardduty-eks-protection-runtime-aktiviert
- guardduty-enabled-centralized
- guardduty-lambda-protection-enabled
- guardduty-malware-protection-enabled
- guardduty-non-archived-findings
- guardduty-rds-protection-enabled
- guardduty-runtime-monitoring-enabled
- GuardDuty-S3-Schutz aktiviert
- iam-external-access-analyzer-aktiviert
- iam-password-policy
- iam-root-access-key-überprüfen
- incoming-ssh-disabled
- instances-in-vpc
- internet-gateway-authorized-vpc-nur
- kinesis-firehose-delivery-stream-verschlüsselt
- kinesis-stream-backup-retention-überprüfen
- kinesis-stream-encrypted
- kms-cmk-not-scheduled-zum Löschen
- kms-key-policy-no-öffentlicher Zugang
- lambda-concurrency-check
- lambda-dlq-check
- lambda-function-public-access-verboten
- lambda-function-settings-check
- lambda-inside-vpc
- lambda-vpc-multi-az-überprüfen

- mariadb-publish-logs-to-cloudwatch-Protokolle
- msk-enhanced-monitoring-enabled
- msk-in-cluster-node-benötigt-tls
- multi-region-cloud-trail-aktiviert
- nacl-no-unrestricted-ssh-rdp
- netfw-deletion-protection-enabled
- netfw-logging-enabled
- netfw-multi-az-enabled
- netfw-policy-default-action-fragment-Pakete
- netfw-policy-default-action-vollständige Pakete
- netfw-policy-rule-group-assoziiert
- netfw-stateless-rule-group-nicht leer
- netfw-subnet-change-protection-aktiviert
- nlb-internal-scheme-check
- nlb-logging-enabled
- no-unrestricted-route-to-igw
- rds-aurora-mysql-audit-Protokollierung aktiviert
- rds-automatic-minor-version-upgrade-fähig
- rds-cluster-default-admin-überprüfen
- rds-cluster-deletion-protection-aktiviert
- rds-cluster-encrypted-at-ausruhen
- rds-cluster-iam-authentication-aktiviert
- rds-cluster-multi-az-aktiviert
- rds-enhanced-monitoring-enabled
- rds-instance-default-admin-überprüfen
- rds-instance-deletion-protection-aktiviert
- rds-instance-iam-authentication-aktiviert
- rds-instance-public-access-überprüfen
- rds-instance-subnet-igw-überprüfen
- rds-in-backup-plan

- rds-last-backup-recovery-Punkt erstellt
- rds-logging-enabled
- rds-mariadb-instance-encryptedim Transit
- rds-meets-restore-time-Ziel
- rds-multi-az-support
- rds-mysql-instance-encryptedim Transit
- rds-postgresql-logs-to- Cloudwatch
- rds-postgres-instance-encryptedunterwegs
- rds-proxy-tls-encryption
- rds-resources-protected-by-Backup-Plan
- rds-snapshots-public-prohibited
- rds-snapshot-encrypted
- rds-sqlserver-encrypted-in-Transit
- rds-sql-server-logszur Cloud-Überwachung
- rds-storage-encrypted
- redshift-backup-enabled
- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check
- redshift-cluster-parameter-group-markiert
- redshift-cluster-public-access-überprüfen
- redshift-cluster-subnet-group-Multi-Az
- redshift-default-admin-check
- redshift-default-db-name-überprüfen
- redshift-enhanced-vpc-routing-aktiviert
- redshift-require-tls-ssl
- redshift-unrestricted-port-access
- required-tags
- restricted-incoming-traffic
- root-account-hardware-mfa-aktiviert
- root-account-mfa-enabled

- nur s3- access-point-in-vpc
- s3- -Blöcke access-point-public-access
- s3- -Blöcke account-level-public-access
- s3- -Blocke-periodisch account-level-public-access
- s 3- bucket-acl-prohibited
- s3- bucket-cross-region-replication -aktiviert
- s-3 bucket-default-lock-enabled
- s3 bucket-level-public-access - verboten
- s3- bucket-logging-enabled
- s-3 bucket-mfa-delete-enabled
- s-3 bucket-policy-grantee-check
- s3- bucket-policy-not-more -freizügig
- s 3- bucket-public-read-prohibited
- s-3 bucket-public-write-prohibited
- s-3 bucket-replication-enabled
- s3- bucket-server-side-encryption -aktiviert
- s-3 bucket-ssl-requests-only
- s3-Bucket-Tagged
- s-3 bucket-versioning-enabled
- s-3 default-encryption-kms
- s-3 event-notifications-enabled
- s3 last-backup-recovery-point - erstellt
- s3- lifecycle-policy-check
- s-3 meets-restore-time-target
- resources-protected-by-backups3-plan
- s 3- version-lifecycle-policy-check
- sagemaker-endpoint-configuration-kms-key-konfiguriert
- sagemaker-endpoint-config-prod-Anzahl der Instanzen
- sagemaker-notebook-instance-kms-key-konfiguriert
- sagemaker-notebook-instance-platform-Version

- sagemaker-notebook-no-direct-Internetzugang
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-überprüfen
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- securityhub-enabled
- security-account-information-provided
- service-catalog-shared-within-Organisation
- service-vpc-endpoint-enabled
- sns-encrypted-kms
- sns-topic-no-public-Zugang
- ssm-document-not-public
- ssm-document-tagged
- step-functions-state-machine-Protokollierung aktiviert
- storagegateway-last-backup-recovery-punkt-erstellt
- storagegateway-resources-in-logically-air-gapped-vault
- storagegateway-resources-protected-by-Ersatzplan
- subnet-auto-assign-public-ip-deaktiviert
- transfer-certificate-description
- transfer-certificate-tagged
- transfer-connector-tagged
- transfer-family-server-no-ftp
- transfer-profile-tagged
- transfer-workflow-description
- transfer-workflow-tagged
- vpc-default-security-group-geschlossen
- vpc-endpoint-enabled
- vpc-flow-logs-enabled
- vpc-network-acl-unused-überprüfen

- vpc-sg-open-only-to-authorized-ports
- vpc-sg-port-restriction-überprüfen
- vpc-vpn-2-tunnels-up
- wafv2-logging-enabled
- WAF 2- rulegroup-logging-enabled
- waf-regional-rule-not-leer
- waf-regional-webacl-not-leer

Region Asien-Pazifik (Jakarta)

Asien-Pazifik (Jakarta)

- access-keys-rotated
- account-part-of-organizations
- acmpca-certificate-authority-tagged
- acm-certificate-expiration-check
- acm-certificate-rsa-check
- acm-pca-root-ca-deaktiviert
- active-mq-supported-version
- alb-desync-mode-check
- alb-http-drop-invalid-Header-fähig
- alb-http-to-https-Umleitungsprüfung
- alb-internal-scheme-check
- alb-waf-enabled
- api-gw-associated-with-WAF
- api-gw-cache-enabled-und-verschlüsselt
- api-gw-endpoint-type-überprüfen
- api-gw-execution-logging-aktiviert
- api-gw-ssl-enabled
- api-gw-xray-enabled
- appconfig-application-description
- appconfig-application-tagged

- appconfig-configuration-profile-tagged
- appconfig-configuration-profile-validators-nicht leer
- appconfig-deployment-strategy-description
- appconfig-deployment-strategy-replicate-zu-ssm
- appconfig-environment-description
- appconfig-environment-tagged
- appconfig-extension-association-tagged
- appconfig-freeform-profile-config-Speicher
- appconfig-hosted-configuration-version-Beschreibung
- appmesh-gateway-route-tagged
- appmesh-mesh-deny-tcp-Weiterleitung
- appmesh-mesh-tagged
- appmesh-route-tagged
- appmesh-virtual-gateway-backend-Standardeinstellungen-TLS
- appmesh-virtual-gateway-logging-file-path-exists
- appmesh-virtual-gateway-tagged
- appmesh-virtual-node-backend-defaults-tls-on
- appmesh-virtual-node-logging-file-path-exists
- appmesh-virtual-node-tagged
- appmesh-virtual-router-tagged
- appmesh-virtual-service-tagged
- approved-amis-by-id
- approved-amis-by-tag
- appsync-authorization-check
- appsync-logging-enabled
- athena-data-catalog-description
- athena-prepared-statement-description
- athena-workgroup-description
- athena-workgroup-encrypted-at-ausruhen
- athena-workgroup-enforce-workgroup-Konfiguration

- athena-workgroup-engine-version-automatisches Upgrade
- athena-workgroup-logging-enabled
- aurora-last-backup-recovery-Punkt erstellt
- aurora-meets-restore-time-Ziel
- aurora-mysql-cluster-audit-Protokollierung
- aurora-resources-in-logically-air-gapped-vault
- aurora-resources-protected-by-Backup-Plan
- autoscaling-group-elb-healthcheck-erforderlich
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-public-ip-deaktiviert
- autoscaling-launch-template
- autoscaling-multiple-az
- autoscaling-multiple-instance-types
- backup-plan-min-frequency-and-min-retention-check
- backup-recovery-point-encrypted
- backup-recovery-point-manual-Löschen-deaktiviert
- backup-recovery-point-minimum-Aufbewahrungsprüfung
- batch-compute-environment-enabled
- batch-compute-environment-managed
- batch-compute-environment-tagged
- batch-job-queue-enabled
- batch-job-queue-tagged
- batch-managed-compute-environment-using-launch-template
- batch-managed-compute-env-compute-resources-tagged
- batch-scheduling-policy-tagged
- clb-desync-mode-check
- clb-multiple-az
- cloudtrail-all-read-s3- data-event-check
- cloudtrail-all-write-s3- data-event-check
- Wolkenspur-S3- bucket-access-logging

- CloudTrail-S3- bucket-public-access-prohibited
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-action-enabled-überprüfen
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted
- cloud-trail-cloud-watch-logs-aktiviert
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-Validierung aktiviert
- cmk-backing-key-rotation-aktiviert
- codebuild-report-group-encrypted-im Ruhezustand
- cognito-identity-pool-unauth-Zugriffsprüfung
- cognito-user-pool-tagged
- custom-eventbus-policy-attached
- cw-loggroup-retention-period-prüfen
- datasync-task-data-verification-aktiviert
- datasync-task-logging-enabled
- datasync-task-tagged
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- dms-replication-not-public
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-last-backup-recovery-punkt-erstellt
- dynamodb-meets-restore-time-Ziel
- dynamodb-pitr-enabled

- dynamodb-resources-protected-by-Backup-Plan
- dynamodb-table-deletion-protection-aktiviert
- dynamodb-table-encrypted-kms
- dynamodb-throughput-limit-check
- ebs-in-backup-plan
- ebs-last-backup-recovery-punkt-erstellt
- ebs-meets-restore-time-Ziel
- ebs-optimized-instance
- ebs-resources-in-logically-air-gapped-vault
- ebs-resources-protected-by-Backup-Plan
- ebs-snapshot-public-restorable-überprüfen
- ec2- capacity-reservation-tagged
- ec2- dhcp-options-tagged
- ec2- ebs-encryption-by-default
- ec2- aktiviert enis-source-destination-check
- ec2-fleet-markiert
- ec2-imdsv2-check
- ec2- instance-detailed-monitoring-enabled
- ec2-ami instance-launched-with-allowed
- ec2- instance-managed-by-ssm
- ec2- instance-multiple-eni-check
- ec2- instance-no-public-ip
- ec2- instance-profile-attached
- ec2- erstellt last-backup-recovery-point
- ec2-2-prüfen launch-template-imdsv
- ec2- -deaktiviert launch-template-public-ip
- ec2- launch-template-tagged
- ec2- managedinstance-applications-blacklisted
- ec2- managedinstance-applications-required
- ec2- managedinstance-inventory-blacklisted

- ec2- prüfen managedinstance-patch-compliance-status
- ec2- managedinstance-platform-check
- ec2- meets-restore-time-target
- ec2- prefix-list-tagged
- ec2- -Tresor mit Lücken resources-in-logically-air
- ec2- resources-protected-by-backup -plan
- ec2- -eni security-group-attached-to
- ec2-stopped-instance
- ec2- traffic-mirror-filter-description
- ec2- traffic-mirror-filter-tagged
- ec2- -attach-deaktiviert transit-gateway-auto-vpc
- ec2 transit-gateway-multicast-domain - markiert
- ec2- volume-inuse-check
- ec2- vpn-connection-logging-enabled
- ecr-private-image-scanning-aktiviert
- ecr-private-lifecycle-policy-konfiguriert
- ecr-private-tag-immutability-aktiviert
- ecr-repository-cmk-encryption-aktiviert
- ecr-repository-tagged
- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-container-insights-enabled
- ecs-fargate-latest-platform-Version
- ecs-no-environment-secrets
- ecs-task-definition-log-Konfiguration
- ecs-task-definition-network-mode-not-host
- ecs-task-definition-pid-Modus-Überprüfung
- ecs-task-definition-user-for-host-mode-check
- efs-access-point-enforce-Stammverzeichnis
- efs-access-point-enforce-Benutzeridentität

- efs-automatic-backups-enabled
- efs-encrypted-check
- efs-filesystem-ct-encrypted
- efs-in-backup-plan
- efs-last-backup-recovery-Punkt erstellt
- efs-meets-restore-time-Ziel
- efs-mount-target-public-zugänglich
- efs-resources-in-logically-air-gapped-vault
- efs-resources-protected-by-Backup-Plan
- eip-attached
- eks-cluster-logging-enabled
- eks-cluster-log-enabled
- eks-cluster-secrets-encrypted
- eks-cluster-supported-version
- eks-endpoint-no-public-Zugang
- eks-secrets-encrypted
- elasticache-auto-minor-version-Upgrade-Check
- elasticache-redis-cluster-automatic-Backup-Check
- elasticache-repl-grp-auto-failover-fähig
- elasticache-repl-grp-encrypted-im Ruhezustand
- elasticache-repl-grp-encryptedim Transit
- elasticache-supported-engine-version
- elasticbeanstalk-application-description
- elasticbeanstalk-application-version-description
- elasticbeanstalk-environment-description
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch
- elasticsearch-node-to-node-Verschlüsselungsprüfung
- elastic-beanstalk-logs-to- Cloudwatch

- elbv2-multiple-az
- elb-acm-certificate-required
- elb-cross-zone-load-Balancing aktiviert
- elb-deletion-protection-enabled
- elb-logging-enabled
- elb-predefined-security-policy-ssl-Prüfung
- elb-tls-https-listeners-nur
- emr-block-public-access
- emr-kerberos-enabled
- emr-master-no-public-ip
- emr-security-configuration-encryption-ruh dich aus
- emr-security-configuration-encryption-Transit
- encrypted-volumes
- event-data-store-cmk-Verschlüsselung aktiviert
- fms-webacl-resource-policy-überprüfen
- fms-webacl-rulegroup-association-überprüfen
- fsx-last-backup-recovery-Punkt erstellt
- fsx-lustre-copy-tagszu Backups
- fsx-meets-restore-time-Ziel
- fsx-ontap-deployment-type-überprüfen
- fsx-openzfs-copy-tags-aktiviert
- fsx-openzfs-deployment-type-überprüfen
- fsx-resources-protected-by-Backup-Plan
- fsx-windows-audit-log-konfiguriert
- fsx-windows-deployment-type-überprüfen
- glue-job-logging-enabled
- glue-ml-transform-encrypted-im Ruhezustand
- glue-spark-job-supported-Ausführung
- GuardDuty-EC2- protection-runtime-enabled
- guardduty-ecs-protection-runtime-aktiviert

- guardduty-eks-protection-audit-aktiviert
- guardduty-eks-protection-runtime-aktiviert
- guardduty-enabled-centralized
- guardduty-lambda-protection-enabled
- guardduty-malware-protection-enabled
- guardduty-non-archived-findings
- guardduty-rds-protection-enabled
- guardduty-runtime-monitoring-enabled
- GuardDuty-S3-Schutz aktiviert
- iam-customer-policy-blocked-kms-Aktionen
- iam-external-access-analyzer-aktiviert
- iam-group-has-users-überprüfen
- iam-inline-policy-blocked-kms-Aktionen
- iam-no-inline-policy-überprüfen
- iam-password-policy
- iam-policy-blacklisted-check
- iam-policy-in-use
- iam-policy-no-statements-with-admin-access
- iam-policy-no-statements-with-full-access
- iam-role-managed-policy-überprüfen
- iam-root-access-key-überprüfen
- iam-user-group-membership-überprüfen
- iam-user-mfa-enabled
- iam-user-no-policies-überprüfen
- iam-user-unused-credentials-überprüfen
- incoming-ssh-disabled
- inspector-ec2-Scan aktiviert
- inspector-ecr-scan-enabled
- inspector-lambda-standard-scan-aktiviert
- instances-in-vpc

- internet-gateway-authorized-vpc-nur
- kinesis-firehose-delivery-stream-verschlüsselt
- kinesis-stream-backup-retention-überprüfen
- kinesis-stream-encrypted
- kms-cmk-not-scheduled-zum Löschen
- kms-key-policy-no-öffentlicher Zugang
- lambda-concurrency-check
- lambda-dlq-check
- lambda-function-public-access-verboten
- lambda-function-settings-check
- lambda-function-xray-enabled
- lambda-inside-vpc
- lambda-vpc-multi-az-überprüfen
- mariadb-publish-logs-to-cloudwatch-Protokolle
- mfa-enabled-for-iam-Konsolenzugriff
- mq-active-broker-ldap-Authentifizierung
- mq-active-deployment-mode
- mq-active-single-instance-broker-storage-type-efs
- mq-auto-minor-version-Upgrade aktiviert
- mq-broker-general-logging-aktiviert
- mq-cloudwatch-audit-log-aktiviert
- mq-rabbit-deployment-mode
- msk-cluster-public-access-deaktiviert
- msk-enhanced-monitoring-enabled
- msk-in-cluster-node-require-tls
- msk-unrestricted-access-check
- multi-region-cloud-trail-aktiviert
- nacl-no-unrestricted-ssh-rdp
- netfw-deletion-protection-enabled
- netfw-logging-enabled

- netfw-multi-az-enabled
- netfw-policy-default-action-fragment-Pakete
- netfw-policy-default-action-vollständige Pakete
- netfw-policy-rule-group-assoziiert
- netfw-stateless-rule-group-nicht leer
- netfw-subnet-change-protection-aktiviert
- nlb-internal-scheme-check
- nlb-logging-enabled
- no-unrestricted-route-to-igw
- opensearch-access-control-enabled
- opensearch-audit-logging-enabled
- opensearch-data-node-fault-Toleranz
- opensearch-encrypted-at-rest
- opensearch-https-required
- opensearch-in-vpc-only
- opensearch-logs-to-cloudwatch
- opensearch-node-to-node-Verschlüsselungsprüfung
- opensearch-primary-node-fault-Toleranz
- opensearch-update-check
- rabbit-mq-supported-version
- rds-aurora-mysql-audit-Protokollierung aktiviert
- rds-aurora-postgresql-logs-zu-Cloud-Watch
- rds-automatic-minor-version-upgrade-fähig
- rds-cluster-auto-minor-version-upgrade-enable
- rds-cluster-default-admin-überprüfen
- rds-cluster-deletion-protection-aktiviert
- rds-cluster-encrypted-at-ausruhen
- rds-cluster-iam-authentication-aktiviert
- rds-cluster-multi-az-aktiviert
- rds-enhanced-monitoring-enabled

- rds-instance-default-admin-überprüfen
- rds-instance-deletion-protection-aktiviert
- rds-instance-iam-authentication-aktiviert
- rds-instance-public-access-überprüfen
- rds-instance-subnet-igw-überprüfen
- rds-in-backup-plan
- rds-last-backup-recovery-Punkt erstellt
- rds-logging-enabled
- rds-mariadb-instance-encryptedim Transit
- rds-meets-restore-time-Ziel
- rds-multi-az-support
- rds-mysql-instance-encryptedim Transit
- rds-postgresql-logs-to- Cloudwatch
- rds-postgres-instance-encryptedunterwegs
- rds-proxy-tls-encryption
- rds-resources-protected-by-Backup-Plan
- rds-snapshots-public-prohibited
- rds-snapshot-encrypted
- rds-sqlserver-encrypted-in-Transit
- rds-sql-server-logszur Cloud-Überwachung
- rds-storage-encrypted
- redshift-backup-enabled
- redshift-cluster-configuration-check
- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check
- redshift-cluster-multi-az-aktiviert
- redshift-cluster-parameter-group-markiert
- redshift-cluster-public-access-überprüfen
- redshift-cluster-subnet-group-Multi-Az
- redshift-default-admin-check

- redshift-default-db-name-überprüfen
- redshift-enhanced-vpc-routing-aktiviert
- redshift-require-tls-ssl
- redshift-serverless-default-admin-überprüfen
- redshift-serverless-default-db-Namenscheck
- redshift-serverless-namespace-cmk-Verschlüsselung
- redshift-serverless-publish-logs-zu-Cloud-Watch
- redshift-serverless-workgroup-no-öffentlicher Zugang
- redshift-unrestricted-port-access
- required-tags
- restricted-incoming-traffic
- root-account-hardware-mfa-aktiviert
- root-account-mfa-enabled
- nur s3- access-point-in-vpc
- s3- -Blöcke access-point-public-access
- s3- -Blöcke account-level-public-access
- s3- -Blocke-periodisch account-level-public-access
- s 3- bucket-acl-prohibited
- s-3 bucket-blacklisted-actions-prohibited
- s3- bucket-cross-region-replication -aktiviert
- s-3 bucket-default-lock-enabled
- s3 bucket-level-public-access - verboten
- s3- bucket-logging-enabled
- s-3 bucket-mfa-delete-enabled
- s-3 bucket-policy-grantee-check
- s3- bucket-policy-not-more -freizügig
- s 3- bucket-public-read-prohibited
- s-3 bucket-public-write-prohibited
- s-3 bucket-replication-enabled
- s3- bucket-server-side-encryption -aktiviert

- s-3 bucket-ssl-requests-only
- s3-Bucket-Tagged
- s-3 bucket-versioning-enabled
- s-3 default-encryption-kms
- s3 last-backup-recovery-point - erstellt
- s3- lifecycle-policy-check
- s-3 meets-restore-time-target
- resources-protected-by-backups3-plan
- s 3- version-lifecycle-policy-check
- sagemaker-app-image-config-markiert
- sagemaker-domain-in-vpc
- sagemaker-domain-tagged
- sagemaker-endpoint-configuration-kms-schlüsselkonfiguriert
- sagemaker-endpoint-config-prod-Anzahl der Instanzen
- sagemaker-feature-group-tagged
- sagemaker-image-description
- sagemaker-image-tagged
- sagemaker-model-in-vpc
- sagemaker-model-isolation-enabled
- sagemaker-notebook-instance-inside-vpc
- sagemaker-notebook-instance-kms-key-konfiguriert
- sagemaker-notebook-instance-platform-Version
- sagemaker-notebook-instance-root-Zugriffsprüfung
- sagemaker-notebook-no-direct-Internetzugang
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-überprüfen
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- securityhub-enabled

- security-account-information-provided
- service-vpc-endpoint-enabled
- sns-encrypted-kms
- sns-topic-no-public-Zugang
- ssm-automation-block-public-teilen
- ssm-automation-logging-enabled
- ssm-document-not-public
- ssm-document-tagged
- step-functions-state-machine-Protokollierung aktiviert
- storagegateway-last-backup-recovery-punkt-erstellt
- storagegateway-resources-in-logically-air-gapped-vault
- storagegateway-resources-protected-by-Ersatzplan
- subnet-auto-assign-public-ip-deaktiviert
- transfer-agreement-description
- transfer-agreement-tagged
- transfer-certificate-description
- transfer-certificate-tagged
- transfer-connector-logging-enabled
- transfer-connector-tagged
- transfer-family-server-no-ftp
- transfer-profile-tagged
- transfer-workflow-description
- transfer-workflow-tagged
- vpc-default-security-group-geschlossen
- vpc-endpoint-enabled
- vpc-flow-logs-enabled
- vpc-network-acl-unused-überprüfen
- vpc-sg-open-only-to-authorized-ports
- vpc-sg-port-restriction-überprüfen
- vpc-vpn-2-tunnels-up

- wafv2-logging-enabled
- WAF 2- rulegroup-logging-enabled
- waf-regional-rule-not-leer
- waf-regional-webacl-not-leer

Region Asien-Pazifik (Malaysia)

Asien-Pazifik (Malaysia)

- account-part-of-organizations
- acm-certificate-expiration-check
- alb-http-drop-invalid-Header-fähig
- alb-http-to-https-Umleitungsprüfung
- alb-waf-enabled
- api-gw-associated-with-WAF
- api-gw-cache-enabled-und-verschlüsselt
- api-gw-endpoint-type-überprüfen
- api-gw-execution-logging-aktiviert
- api-gw-ssl-enabled
- api-gw-xray-enabled
- approved-amis-by-id
- approved-amis-by-tag
- aurora-mysql-backtracking-enabled
- autoscaling-group-elb-healthcheck-erforderlich
- autoscaling-launch-config-public-ip-deaktiviert
- cloudformation-stack-drift-detection-überprüfen
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted

- cloud-trail-cloud-watch-logs-aktiviert
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-Validierung aktiviert
- cmk-backing-key-rotation-aktiviert
- cw-loggroup-retention-period-überprüfen
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- dms-replication-not-public
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-pitr-enabled
- dynamodb-table-encrypted-kms
- dynamodb-table-encryption-enabled
- dynamodb-throughput-limit-check
- ebs-in-backup-plan
- ebs-snapshot-public-restorable-überprüfen
- ec2- ebs-encryption-by-default
- ec2-imdsv2-check
- ec2- instance-detailed-monitoring-enabled
- ec2-ami instance-launched-with-allowed
- ec2- instance-managed-by-ssm
- ec2- instance-multiple-eni-check
- ec2- instance-no-public-ip
- ec2- instance-profile-attached
- ec2- managedinstance-applications-blacklisted
- ec2- managedinstance-applications-required
- ec2- managedinstance-inventory-blacklisted
- ec2- prüfen managedinstance-patch-compliance-status

- ec2- managedinstance-platform-check
- ec2-eni security-group-attached-to
- ec2-stopped-instance
- ec2- volume-inuse-check
- ecs-task-definition-network-mode-not-host
- ecs-task-definition-user-for-host-mode-check
- efs-encrypted-check
- efs-in-backup-plan
- eip-attached
- eks-endpoint-no-public-Zugang
- eks-secrets-encrypted
- elasticache-redis-cluster-automatic-Backup-Check
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch
- elasticsearch-node-to-node-Verschlüsselungsprüfung
- elb-acm-certificate-required
- elb-cross-zone-load-Balancing aktiviert
- elb-custom-security-policy-ssl-Prüfung
- elb-deletion-protection-enabled
- elb-logging-enabled
- elb-predefined-security-policy-ssl-Überprüfung
- elb-tls-https-listeners-nur
- emr-kerberos-enabled
- emr-master-no-public-ip
- encrypted-volumes
- guardduty-enabled-centralized
- guardduty-non-archived-findings
- iam-password-policy
- incoming-ssh-disabled

- instances-in-vpc
- internet-gateway-authorized-vpc-nur
- kms-cmk-not-scheduled-zum Löschen
- lambda-concurrency-check
- lambda-dlq-check
- lambda-function-public-access-verboten
- lambda-function-settings-check
- lambda-inside-vpc
- multi-region-cloud-trail-aktiviert
- no-unrestricted-route-to-igw
- rds-automatic-minor-version-Upgrade aktiviert
- rds-cluster-deletion-protection-aktiviert
- rds-cluster-iam-authentication-aktiviert
- rds-cluster-multi-az-aktiviert
- rds-enhanced-monitoring-enabled
- rds-instance-deletion-protection-aktiviert
- rds-instance-iam-authentication-aktiviert
- rds-instance-public-access-überprüfen
- rds-in-backup-plan
- rds-logging-enabled
- rds-multi-az-support
- rds-snapshots-public-prohibited
- rds-snapshot-encrypted
- rds-storage-encrypted
- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check
- redshift-cluster-public-access-überprüfen
- redshift-enhanced-vpc-routing-aktiviert
- redshift-require-tls-ssl
- required-tags

- restricted-incoming-traffic
- s3- -Blocke-periodisch account-level-public-access
- s 3- bucket-blacklisted-actions-prohibited
- s-3 bucket-default-lock-enabled
- s3 bucket-level-public-access - verboten
- s3- bucket-logging-enabled
- s-3 bucket-policy-grantee-check
- s3- bucket-policy-not-more -freizügig
- s 3- bucket-public-read-prohibited
- s-3 bucket-public-write-prohibited
- s-3 bucket-replication-enabled
- s3- bucket-server-side-encryption -aktiviert
- s-3 bucket-ssl-requests-only
- s-3 bucket-versioning-enabled
- s-3 default-encryption-kms
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-überprüfen
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- securityhub-enabled
- service-vpc-endpoint-enabled
- sns-encrypted-kms
- ssm-document-not-public
- subnet-auto-assign-public-ip-deaktiviert
- vpc-default-security-group-geschlossen
- vpc-flow-logs-enabled
- vpc-network-acl-unused-überprüfen
- vpc-sg-open-only-to-authorized-ports
- vpc-vpn-2-tunnels-up

- wafv2-logging-enabled

Region Asien-Pazifik (Melbourne)

Asien-Pazifik (Melbourne)

- account-part-of-organizations
- acmpca-certificate-authority-tagged
- acm-certificate-expiration-check
- acm-certificate-rsa-check
- acm-pca-root-ca-deaktiviert
- alb-desync-mode-check
- alb-http-drop-invalid-Header-fähig
- alb-http-to-https-Umleitungsprüfung
- alb-internal-scheme-check
- alb-waf-enabled
- api-gw-associated-with-WAF
- api-gw-cache-enabled-und-verschlüsselt
- api-gw-endpoint-type-überprüfen
- api-gw-execution-logging-aktiviert
- api-gw-ssl-enabled
- api-gw-xray-enabled
- appconfig-application-description
- appconfig-application-tagged
- appconfig-configuration-profile-tagged
- appconfig-configuration-profile-validators-nicht leer
- appconfig-deployment-strategy-description
- appconfig-deployment-strategy-replicate-zu-ssm
- appconfig-environment-description
- appconfig-environment-tagged
- appconfig-extension-association-tagged
- appconfig-freeform-profile-config-Speicher

- appconfig-hosted-configuration-version-Beschreibung
- approved-amis-by-id
- approved-amis-by-tag
- athena-data-catalog-description
- athena-prepared-statement-description
- athena-workgroup-description
- athena-workgroup-enforce-workgroup-Konfiguration
- athena-workgroup-engine-version-automatisches Upgrade
- athena-workgroup-logging-enabled
- aurora-last-backup-recovery-Punkt erstellt
- aurora-meets-restore-time-Ziel
- aurora-mysql-cluster-audit-Protokollierung
- aurora-resources-in-logically-air-gapped-vault
- aurora-resources-protected-by-Backup-Plan
- autoscaling-group-elb-healthcheck-erforderlich
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-hop-Grenze
- autoscaling-launch-config-public-ip-deaktiviert
- autoscaling-launch-template
- autoscaling-multiple-az
- autoscaling-multiple-instance-types
- backup-plan-min-frequency-and-min-retention-check
- backup-recovery-point-encrypted
- backup-recovery-point-manual-Löschen-deaktiviert
- backup-recovery-point-minimum-Aufbewahrungsprüfung
- batch-scheduling-policy-tagged
- clb-multiple-az
- cloudtrail-all-read-s3- data-event-check
- cloudtrail-all-write-s3- data-event-check
- Wolkenspur-S3- bucket-access-logging

- CloudTrail-S3- bucket-public-access-prohibited
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-action-enabled-überprüfen
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted
- cloud-trail-cloud-watch-logs-aktiviert
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-Validierung aktiviert
- cmk-backing-key-rotation-aktiviert
- codebuild-project-envvar-awscred-überprüfen
- codebuild-project-logging-enabled
- codebuild-project-s3-log-verschlüsselt
- codebuild-project-source-repo-URL-Prüfung
- codebuild-report-group-encrypted-im Ruhezustand
- cognito-identity-pool-unauth-Zugriffsprüfung
- cognito-user-pool-tagged
- custom-eventbus-policy-attached
- cw-loggroup-retention-period-prüfen
- datasync-task-data-verification-aktiviert
- datasync-task-logging-enabled
- datasync-task-tagged
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- dms-replication-not-public
- dynamodb-autoscaling-enabled

- dynamodb-in-backup-plan
- dynamodb-last-backup-recovery-punkt-erstellt
- dynamodb-meets-restore-time-Ziel
- dynamodb-pitr-enabled
- dynamodb-resources-protected-by-Backup-Plan
- dynamodb-table-deletion-protection-aktiviert
- dynamodb-table-encrypted-kms
- dynamodb-table-encryption-enabled
- dynamodb-throughput-limit-check
- ebs-last-backup-recovery-punkt-erstellt
- ebs-meets-restore-time-Ziel
- ebs-optimized-instance
- ebs-resources-in-logically-air-gapped-vault
- ebs-resources-protected-by-Backup-Plan
- ebs-snapshot-public-restorable-überprüfen
- ec2- capacity-reservation-tagged
- ec2- aktiviert client-vpn-connection-log
- ec2- client-vpn-endpoint-tagged
- ec2- dhcp-options-tagged
- ec2- ebs-encryption-by-default
- ec2- aktiviert enis-source-destination-check
- ec2-fleet-markiert
- ec2-imdsv2-check
- ec2- instance-detailed-monitoring-enabled
- ec2-ami instance-launched-with-allowed
- ec2- instance-managed-by-ssm
- ec2- instance-multiple-eni-check
- ec2- instance-no-public-ip
- ec2- instance-profile-attached
- ec2- erstellt last-backup-recovery-point

- ec2- managedinstance-applications-blacklisted
- ec2- managedinstance-applications-required
- ec2- managedinstance-inventory-blacklisted
- ec2- prüfen managedinstance-patch-compliance-status
- ec2- managedinstance-platform-check
- ec2- meets-restore-time-target
- ec2- prefix-list-tagged
- ec2- -Tresor mit Lücken resources-in-logically-air
- ec2- resources-protected-by-backup -plan
- ec2- -eni security-group-attached-to
- ec2- traffic-mirror-filter-description
- ec2- traffic-mirror-filter-tagged
- ec2- traffic-mirror-session-description
- ec2- traffic-mirror-session-tagged
- ec2- traffic-mirror-target-description
- ec2- traffic-mirror-target-tagged
- ec2- markiert transit-gateway-multicast-domain
- ec2- volume-inuse-check
- ec2- vpn-connection-logging-enabled
- ecr-private-image-scanning-aktiviert
- ecr-private-lifecycle-policy-konfiguriert
- ecr-private-tag-immutability-aktiviert
- ecr-repository-cmk-encryption-aktiviert
- ecr-repository-tagged
- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-container-insights-enabled
- ecs-fargate-latest-platform-Version
- ecs-no-environment-secrets
- ecs-task-definition-log-Konfiguration

- ecs-task-definition-network-mode-not-host
- ecs-task-definition-pid-Modus-Überprüfung
- ecs-task-definition-user-for-host-mode-check
- efs-access-point-enforce-Stammverzeichnis
- efs-access-point-enforce-Benutzeridentität
- efs-automatic-backups-enabled
- efs-encrypted-check
- efs-filesystem-ct-encrypted
- efs-in-backup-plan
- efs-last-backup-recovery-Punkt erstellt
- efs-meets-restore-time-Ziel
- efs-mount-target-public-zugänglich
- efs-resources-in-logically-air-gapped-vault
- efs-resources-protected-by-Backup-Plan
- eip-attached
- eks-cluster-log-enabled
- eks-cluster-secrets-encrypted
- eks-cluster-supported-version
- eks-endpoint-no-public-Zugang
- eks-secrets-encrypted
- elasticache-redis-cluster-automatic-Backup-Check
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch
- elasticsearch-node-to-node-Verschlüsselungsprüfung
- elbv2-multiple-az
- elb-acm-certificate-required
- elb-cross-zone-load-Balancing aktiviert
- elb-deletion-protection-enabled
- elb-logging-enabled

- elb-predefined-security-policy-ssl-Prüfung
- elb-tls-https-listeners-nur
- emr-block-public-access
- emr-kerberos-enabled
- emr-security-configuration-encryption-ausruhen
- emr-security-configuration-encryption-Transit
- encrypted-volumes
- event-data-store-cmk-Verschlüsselung aktiviert
- fms-shield-resource-policy-überprüfen
- fms-webacl-resource-policy-überprüfen
- fms-webacl-rulegroup-association-überprüfen
- fsx-last-backup-recovery-Punkt erstellt
- fsx-lustre-copy-tagszu Backups
- fsx-meets-restore-time-Ziel
- fsx-ontap-deployment-type-überprüfen
- fsx-resources-protected-by-Backup-Plan
- fsx-windows-deployment-type-überprüfen
- glue-job-logging-enabled
- glue-ml-transform-encrypted-im Ruhezustand
- glue-spark-job-supported-Ausführung
- GuardDuty-EC2- protection-runtime-enabled
- guardduty-ecs-protection-runtime-aktiviert
- guardduty-eks-protection-audit-aktiviert
- guardduty-eks-protection-runtime-aktiviert
- guardduty-enabled-centralized
- guardduty-lambda-protection-enabled
- guardduty-malware-protection-enabled
- guardduty-non-archived-findings
- guardduty-rds-protection-enabled
- guardduty-runtime-monitoring-enabled

- GuardDuty-S3-Schutz aktiviert
- iam-external-access-analyzer-aktiviert
- iam-password-policy
- iam-root-access-key-überprüfen
- incoming-ssh-disabled
- instances-in-vpc
- internet-gateway-authorized-vpc-nur
- kinesis-firehose-delivery-stream-verschlüsselt
- kinesis-stream-backup-retention-überprüfen
- kinesis-stream-encrypted
- kms-cmk-not-scheduled-zum Löschen
- kms-key-policy-no-öffentlicher Zugang
- lambda-concurrency-check
- lambda-dlq-check
- lambda-function-public-access-verboten
- lambda-function-settings-check
- lambda-function-xray-enabled
- lambda-inside-vpc
- lambda-vpc-multi-az-überprüfen
- mariadb-publish-logs-to-cloudwatch-Protokolle
- mq-active-broker-ldap-Authentifizierung
- mq-active-deployment-mode
- mq-active-single-instance-broker-storage-type-efs
- mq-auto-minor-version-Upgrade aktiviert
- mq-broker-general-logging-aktiviert
- mq-cloudwatch-audit-log-aktiviert
- msk-cluster-public-access-deaktiviert
- msk-enhanced-monitoring-enabled
- msk-in-cluster-node-require-tls
- msk-unrestricted-access-check

- multi-region-cloud-trail-aktiviert
- nacl-no-unrestricted-ssh-rdp
- netfw-deletion-protection-enabled
- netfw-logging-enabled
- netfw-multi-az-enabled
- netfw-policy-default-action-fragment-Pakete
- netfw-policy-default-action-vollständige Pakete
- netfw-policy-rule-group-assoziiert
- netfw-stateless-rule-group-nicht leer
- netfw-subnet-change-protection-aktiviert
- nlb-internal-scheme-check
- nlb-logging-enabled
- no-unrestricted-route-to-igw
- rds-aurora-mysql-audit-Protokollierung aktiviert
- rds-automatic-minor-version-upgrade-fähig
- rds-cluster-default-admin-überprüfen
- rds-cluster-deletion-protection-aktiviert
- rds-cluster-encrypted-at-ausruhen
- rds-cluster-iam-authentication-aktiviert
- rds-enhanced-monitoring-enabled
- rds-instance-default-admin-überprüfen
- rds-instance-deletion-protection-aktiviert
- rds-instance-iam-authentication-aktiviert
- rds-instance-public-access-überprüfen
- rds-instance-subnet-igw-überprüfen
- rds-in-backup-plan
- rds-last-backup-recovery-Punkt erstellt
- rds-logging-enabled
- rds-mariadb-instance-encryptedim Transit
- rds-meets-restore-time-Ziel

- rds-multi-az-support
- rds-mysql-instance-encryptedim Transit
- rds-postgresql-logs-to- Cloudwatch
- rds-postgres-instance-encryptedunterwegs
- rds-proxy-tls-encryption
- rds-resources-protected-by-Backup-Plan
- rds-snapshot-encrypted
- rds-sqlserver-encrypted-in-Transit
- rds-sql-server-logszur Cloud-Überwachung
- rds-storage-encrypted
- redshift-backup-enabled
- redshift-cluster-configuration-check
- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check
- redshift-cluster-multi-az-aktiviert
- redshift-cluster-parameter-group-markiert
- redshift-cluster-public-access-überprüfen
- redshift-cluster-subnet-group-Multi-Az
- redshift-default-admin-check
- redshift-default-db-name-überprüfen
- redshift-enhanced-vpc-routing-aktiviert
- redshift-require-tls-ssl
- redshift-unrestricted-port-access
- required-tags
- restricted-incoming-traffic
- root-account-hardware-mfa-aktiviert
- root-account-mfa-enabled
- nur s3- access-point-in-vpc
- s3- -Blöcke access-point-public-access
- s3- -Blöcke account-level-public-access

- s3- -Blocke-periodisch account-level-public-access
- s 3- bucket-acl-prohibited
- s-3 bucket-blacklisted-actions-prohibited
- s3- bucket-cross-region-replication -aktiviert
- s-3 bucket-default-lock-enabled
- s3 bucket-level-public-access - verboten
- s3- bucket-logging-enabled
- s-3 bucket-mfa-delete-enabled
- s-3 bucket-policy-grantee-check
- s3- bucket-policy-not-more -freizügig
- s 3- bucket-public-read-prohibited
- s-3 bucket-public-write-prohibited
- s-3 bucket-replication-enabled
- s3- bucket-server-side-encryption -aktiviert
- s-3 bucket-ssl-requests-only
- s3-Bucket-Tagged
- s-3 bucket-versioning-enabled
- s-3 default-encryption-kms
- s-3 event-notifications-enabled
- s3 last-backup-recovery-point - erstellt
- s3- lifecycle-policy-check
- s-3 meets-restore-time-target
- resources-protected-by-backups3-plan
- s 3- version-lifecycle-policy-check
- sagemaker-endpoint-config-prod-Anzahl der Instanzen
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-überprüfen
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk

- securityhub-enabled
- security-account-information-provided
- service-catalog-shared-within-Organisation
- service-vpc-endpoint-enabled
- sns-encrypted-kms
- sns-topic-no-public-Zugang
- ssm-automation-logging-enabled
- ssm-document-not-public
- ssm-document-tagged
- storagegateway-last-backup-recovery-Punkt erstellt
- storagegateway-resources-in-logically-air-gapped-vault
- storagegateway-resources-protected-by-Ersatzplan
- subnet-auto-assign-public-ip-deaktiviert
- transfer-certificate-description
- transfer-certificate-tagged
- transfer-connector-tagged
- transfer-family-server-no-ftp
- transfer-profile-tagged
- transfer-workflow-description
- transfer-workflow-tagged
- vpc-default-security-group-geschlossen
- vpc-endpoint-enabled
- vpc-flow-logs-enabled
- vpc-network-acl-unused-überprüfen
- vpc-sg-port-restriction-überprüfen
- vpc-vpn-2-tunnels-up
- wafv2-logging-enabled
- WAF 2- rulegroup-logging-enabled
- WAF 2- webacl-not-empty
- waf-regional-rulegroup-not-leer

- waf-regional-rule-not-leer
- waf-regional-webacl-not-leer

Region Asien-Pazifik (Mumbai)

Asien-Pazifik (Mumbai)

- access-keys-rotated
- account-part-of-organizations
- acmpca-certificate-authority-tagged
- acm-certificate-expiration-check
- acm-certificate-rsa-check
- acm-pca-root-ca-deaktiviert
- active-mq-supported-version
- alb-desync-mode-check
- alb-http-drop-invalid-Header-fähig
- alb-http-to-https-Umleitungsprüfung
- alb-internal-scheme-check
- alb-listener-tagged
- alb-waf-enabled
- amplify-app-branch-auto-löschung aktiviert
- amplify-app-description
- amplify-app-tagged
- amplify-branch-performance-mode-aktiviert
- amplify-branch-tagged
- api-gwv2- access-logs-enabled
- api-gwv2- authorization-type-configured
- api-gw-associated-with-WAF
- api-gw-cache-enabled-und-verschlüsselt
- api-gw-endpoint-type-überprüfen
- api-gw-execution-logging-aktiviert
- api-gw-ssl-enabled

- api-gw-xray-enabled
- appconfig-application-description
- appconfig-application-tagged
- appconfig-configuration-profile-tagged
- appconfig-configuration-profile-validators-nicht leer
- appconfig-deployment-strategy-description
- appconfig-deployment-strategy-replicate-zu-ssm
- appconfig-environment-description
- appconfig-environment-tagged
- appconfig-extension-association-tagged
- appconfig-freeform-profile-config-Speicher
- appconfig-hosted-configuration-version-Beschreibung
- appflow-flow-tagged
- appmesh-gateway-route-tagged
- appmesh-mesh-deny-tcp-Weiterleitung
- appmesh-mesh-tagged
- appmesh-route-tagged
- appmesh-virtual-gateway-backend-Standardeinstellungen-TLS
- appmesh-virtual-gateway-logging-file-path-exists
- appmesh-virtual-gateway-tagged
- appmesh-virtual-node-backend-defaults-tls-on
- appmesh-virtual-node-logging-file-path-exists
- appmesh-virtual-node-tagged
- appmesh-virtual-router-tagged
- appmesh-virtual-service-tagged
- approved-amis-by-id
- approved-amis-by-tag
- apprunner-service-in-vpc
- apprunner-service-no-public-Zugang
- apprunner-service-observability-enabled

- apprunner-service-tagged
- apprunner-vpc-connector-tagged
- appstream-fleet-in-vpc
- appsync-associated-with-waf
- appsync-authorization-check
- appsync-cache-encryption-at-ausruhen
- appsync-logging-enabled
- athena-data-catalog-description
- athena-prepared-statement-description
- athena-workgroup-description
- athena-workgroup-encrypted-at-ausruhen
- athena-workgroup-enforce-workgroup-Konfiguration
- athena-workgroup-engine-version-automatisches Upgrade
- athena-workgroup-logging-enabled
- aurora-last-backup-recovery-Punkt erstellt
- aurora-meets-restore-time-Ziel
- aurora-mysql-backtracking-enabled
- aurora-mysql-cluster-audit-Protokollierung
- aurora-resources-in-logically-air-gapped-vault
- aurora-resources-protected-by-Backup-Plan
- autoscaling-capacity-rebalancing
- autoscaling-group-elb-healthcheck-erforderlich
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-hop-Grenze
- autoscaling-launch-config-public-ip-deaktiviert
- autoscaling-launch-template
- autoscaling-multiple-az
- autoscaling-multiple-instance-types
- backup-plan-min-frequency-and-min-retention-check
- backup-recovery-point-encrypted

- backup-recovery-point-manual-Löschen-deaktiviert
- backup-recovery-point-minimum-Aufbewahrungsprüfung
- batch-compute-environment-enabled
- batch-compute-environment-managed
- batch-compute-environment-tagged
- batch-job-queue-enabled
- batch-job-queue-tagged
- batch-managed-compute-environment-using-launch-template
- batch-managed-compute-env-compute-resources-tagged
- batch-scheduling-policy-tagged
- beanstalk-enhanced-health-reporting-aktiviert
- cassandra-keyspace-tagged
- clb-desync-mode-check
- clb-multiple-az
- cloudformation-stack-drift-detection-überprüfen
- cloudformation-stack-notification-check
- cloudtrail-all-read-s3- data-event-check
- cloudtrail-all-write-s3- data-event-check
- Wolkenspur-S3- bucket-access-logging
- CloudTrail-S3- bucket-public-access-prohibited
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-action-enabled-überprüfen
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted
- cloud-trail-cloud-watch-logs-aktiviert
- cloud-trail-enabled
- cloud-trail-encryption-enabled

- cloud-trail-log-file-Validierung aktiviert
- cmk-backing-key-rotation-aktiviert
- codebuild-project-artifact-encryption
- codebuild-project-environment-privileged-überprüfen
- codebuild-project-envvar-awscred-überprüfen
- codebuild-project-logging-enabled
- codebuild-project-s3-log-verschlüsselt
- codebuild-project-source-repo-URL-Prüfung
- codebuild-report-group-encrypted-im Ruhezustand
- codedeploy-auto-rollback-monitor-aktiviert
- codedeploy-deployment-group-auto-rollback-aktiviert
- codedeploy-deployment-group-outdated-instanzen-aktualisieren
- Codedeploy-ec2- minimum-healthy-hosts-configured
- codedeploy-lambda-allatonce-traffic-shift-deaktiviert
- codepipeline-deployment-count-check
- codepipeline-region-fanout-check
- cognito-identity-pool-unauth-Zugriffsprüfung
- cognito-user-pool-advanced-sicherheitsaktiviert
- cognito-user-pool-tagged
- custom-eventbus-policy-attached
- custom-schema-registry-policy-angehängt
- cw-loggroup-retention-period-überprüfen
- datasync-task-data-verification-aktiviert
- datasync-task-logging-enabled
- datasync-task-tagged
- dax-encryption-enabled
- dax-tls-endpoint-encryption
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type

- dms-auto-minor-version-aktualisieren-Prüfung
- dms-endpoint-ssl-configured
- dms-endpoint-tagged
- dms-mongo-db-authentication-aktiviert
- dms-neptune-iam-authorization-aktiviert
- dms-redis-tls-enabled
- dms-replication-not-public
- dms-replication-task-sourcedb-Protokollierung
- dms-replication-task-tagged
- dms-replication-task-targetdb-Protokollierung
- docdb-cluster-audit-logging-aktiviert
- docdb-cluster-backup-retention-überprüfen
- docdb-cluster-deletion-protection-aktiviert
- docdb-cluster-encrypted
- docdb-cluster-encrypted-in-Transit
- docdb-cluster-snapshot-public-verboten
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-last-backup-recovery-Punkt erstellt
- dynamodb-meets-restore-time-Ziel
- dynamodb-pitr-enabled
- dynamodb-resources-protected-by-Backup-Plan
- dynamodb-table-deletion-protection-aktiviert
- dynamodb-table-encrypted-kms
- dynamodb-table-encryption-enabled
- dynamodb-throughput-limit-check
- ebs-in-backup-plan
- ebs-last-backup-recovery-punkt-erstellt
- ebs-meets-restore-time-Ziel
- ebs-optimized-instance

- ebs-resources-in-logically-air-gapped-vault
- ebs-resources-protected-by-Backup-Plan
- ebs-snapshot-public-restorable-überprüfen
- ec2- capacity-reservation-tagged
- ec2- aktiviert client-vpn-connection-log
- ec2- client-vpn-endpoint-tagged
- ec2- -alle client-vpn-not-authorize
- ec2- dhcp-options-tagged
- ec2- ebs-encryption-by-default
- ec2- aktiviert enis-source-destination-check
- ec2-fleet-markiert
- ec2-imdsv2-check
- ec2- instance-detailed-monitoring-enabled
- ec2-ami instance-launched-with-allowed
- ec2- instance-managed-by-ssm
- ec2- instance-multiple-eni-check
- ec2- instance-no-public-ip
- ec2- instance-profile-attached
- ec2- erstellt last-backup-recovery-point
- ec2-2-prüfen launch-template-imdsv
- ec2- -deaktiviert launch-template-public-ip
- ec2- launch-template-tagged
- ec2- managedinstance-applications-blacklisted
- ec2- managedinstance-applications-required
- ec2- prüfen managedinstance-association-compliance-status
- ec2- managedinstance-inventory-blacklisted
- ec2- prüfen managedinstance-patch-compliance-status
- ec2- managedinstance-platform-check
- ec2- meets-restore-time-target
- ec2- Analyse mit Schlagwörtern network-insights-access-scope

- ec2 network-insights-access-scope - markiert
- ec2- network-insights-path-tagged
- ec2- no-amazon-key-pair
- ec2- prefix-list-tagged
- ec2- -Tresor mit Lücken resources-in-logically-air
- ec2- resources-protected-by-backup -plan
- ec2- -eni security-group-attached-to
- ec2- -eni-periodisch security-group-attached-to
- ec2-stopped-instance
- ec2- token-hop-limit-check
- ec2- traffic-mirror-filter-description
- ec2- traffic-mirror-filter-tagged
- ec2- traffic-mirror-session-description
- ec2- traffic-mirror-session-tagged
- ec2- traffic-mirror-target-description
- ec2- traffic-mirror-target-tagged
- ec2- -attach-deaktiviert transit-gateway-auto-vpc
- ec2 transit-gateway-multicast-domain - markiert
- ec2- volume-inuse-check
- ec2- vpn-connection-logging-enabled
- ecr-private-image-scanning-aktiviert
- ecr-private-lifecycle-policy-konfiguriert
- ecr-private-tag-immutability-aktiviert
- ecr-repository-cmk-encryption-aktiviert
- ecr-repository-tagged
- ecs-awsvpc-networking-enabled
- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-container-insights-enabled
- ecs-fargate-latest-platform-Version

- ecs-no-environment-secrets
- ecs-task-definition-log-Konfiguration
- ecs-task-definition-memory-hartes Limit
- ecs-task-definition-network-mode-not-host
- ecs-task-definition-nonroot-Benutzer
- ecs-task-definition-pid-Modus-Check
- ecs-task-definition-user-for-host-mode-check
- efs-access-point-enforce-Stammverzeichnis
- efs-access-point-enforce-Benutzeridentität
- efs-automatic-backups-enabled
- efs-encrypted-check
- efs-filesystem-ct-encrypted
- efs-in-backup-plan
- efs-last-backup-recovery-Punkt erstellt
- efs-meets-restore-time-Ziel
- efs-mount-target-public-zugänglich
- efs-resources-in-logically-air-gapped-vault
- efs-resources-protected-by-Backup-Plan
- eip-attached
- eks-cluster-logging-enabled
- eks-cluster-log-enabled
- eks-cluster-oldest-supported-Ausführung
- eks-cluster-secrets-encrypted
- eks-cluster-supported-version
- eks-endpoint-no-public-Zugang
- eks-secrets-encrypted
- elasticache-auto-minor-version-Upgrade-Check
- elasticache-rbac-auth-enabled
- elasticache-redis-cluster-automatic-Backup-Check
- elasticache-repl-grp-auto-failover-fähig

- elasticache-repl-grp-encrypted-im Ruhezustand
- elasticache-repl-grp-encryptedim Transit
- elasticache-repl-grp-redis-auth-aktiviert
- elasticache-subnet-group-check
- elasticache-supported-engine-version
- elasticbeanstalk-application-description
- elasticbeanstalk-application-version-description
- elasticbeanstalk-environment-description
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch
- elasticsearch-node-to-node-Verschlüsselungsprüfung
- elastic-beanstalk-logs-to- Cloudwatch
- elastic-beanstalk-managed-updates-aktiviert
- elbv2- acm-certificate-required
- elv 2- listener-encryption-in-transit
- elbv2-multiple-az
- elbv2- -prüfen predefined-security-policy-ssl
- elb-acm-certificate-required
- elb-cross-zone-load-Balancing aktiviert
- elb-custom-security-policy-ssl-Prüfung
- elb-deletion-protection-enabled
- elb-logging-enabled
- elb-predefined-security-policy-ssl-Überprüfung
- elb-tls-https-listeners-nur
- emr-block-public-access
- emr-kerberos-enabled
- emr-master-no-public-ip
- emr-security-configuration-encryption-ruh dich aus
- emr-security-configuration-encryption-Transit

- encrypted-volumes
- event-data-store-cmk-Verschlüsselung aktiviert
- fis-experiment-template-log-Konfiguration ist vorhanden
- fis-experiment-template-tagged
- fms-shield-resource-policy-überprüfen
- fms-webacl-resource-policy-überprüfen
- fms-webacl-rulegroup-association-überprüfen
- fsx-last-backup-recovery-Punkt erstellt
- fsx-lustre-copy-tagszu Backups
- fsx-meets-restore-time-Ziel
- fsx-ontap-deployment-type-überprüfen
- fsx-openzfs-copy-tags-aktiviert
- fsx-openzfs-deployment-type-überprüfen
- fsx-resources-protected-by-Backup-Plan
- fsx-windows-audit-log-konfiguriert
- fsx-windows-deployment-type-überprüfen
- glb-listener-tagged
- global-endpoint-event-replication-aktiviert
- glue-job-logging-enabled
- glue-ml-transform-encrypted-im Ruhezustand
- glue-spark-job-supported-Ausführung
- GuardDuty-EC2- protection-runtime-enabled
- guardduty-ecs-protection-runtime-aktiviert
- guardduty-eks-protection-audit-aktiviert
- guardduty-eks-protection-runtime-aktiviert
- guardduty-enabled-centralized
- guardduty-lambda-protection-enabled
- guardduty-malware-protection-enabled
- guardduty-non-archived-findings
- guardduty-rds-protection-enabled

- guardduty-runtime-monitoring-enabled
- GuardDuty-S3-Schutz aktiviert
- iam-customer-policy-blocked-kms-Aktionen
- iam-external-access-analyzer-aktiviert
- iam-group-has-users-überprüfen
- iam-inline-policy-blocked-KMS-Aktionen
- iam-no-inline-policy-überprüfen
- iam-password-policy
- iam-policy-blacklisted-check
- iam-policy-in-use
- iam-policy-no-statements-with-admin-access
- iam-policy-no-statements-with-full-access
- iam-role-managed-policy-überprüfen
- iam-root-access-key-überprüfen
- iam-user-group-membership-überprüfen
- iam-user-mfa-enabled
- iam-user-no-policies-überprüfen
- iam-user-unused-credentials-überprüfen
- incoming-ssh-disabled
- inspector-ec2-Scan aktiviert
- inspector-ecr-scan-enabled
- inspector-lambda-standard-scan-aktiviert
- instances-in-vpc
- internet-gateway-authorized-vpc-nur
- iotevents-alarm-model-tagged
- iotevents-detector-model-tagged
- iotevents-input-tagged
- iotsitewise-asset-model-tagged
- iotsitewise-dashboard-tagged
- iotsitewise-gateway-tagged

- iotsitewise-portal-tagged
- iotsitewise-project-tagged
- iottwinmaker-component-type-tagged
- iottwinmaker-scene-tagged
- iottwinmaker-sync-job-tagged
- iottwinmaker-workspace-tagged
- iot-authorizer-token-signing-aktiviert
- ivs-channel-playback-authorization-aktiviert
- ivs-channel-tagged
- ivs-playback-key-pair-markiert
- ivs-recording-configuration-tagged
- kinesis-firehose-delivery-stream-verschlüsselt
- kinesis-stream-backup-retention-überprüfen
- kinesis-stream-encrypted
- kms-cmk-not-scheduled-zum Löschen
- kms-key-policy-no-öffentlicher Zugang
- lambda-concurrency-check
- lambda-dlq-check
- lambda-function-public-access-verboten
- lambda-function-settings-check
- lambda-function-xray-enabled
- lambda-inside-vpc
- lambda-vpc-multi-az-überprüfen
- lightsail-bucket-tagged
- lightsail-certificate-tagged
- lightsail-disk-tagged
- macie-auto-sensitive-data-Discovery-Check
- macie-status-check
- mariadb-publish-logs-to-Cloudwatch-Protokolle
- mfa-enabled-for-iam-Konsolenzugriff

- mq-active-broker-ldap-Authentifizierung
- mq-active-deployment-mode
- mq-active-single-instance-broker-storage-type-efs
- mq-automatic-minor-version-Upgrade aktiviert
- mq-auto-minor-version-upgrade-fähig
- mq-broker-general-logging-aktiviert
- mq-cloudwatch-audit-logging-aktiviert
- mq-cloudwatch-audit-log-aktiviert
- mq-no-public-access
- mq-rabbit-deployment-mode
- msk-cluster-public-access-deaktiviert
- msk-connect-connector-logging-aktiviert
- msk-enhanced-monitoring-enabled
- msk-in-cluster-node-require-tls
- msk-unrestricted-access-check
- multi-region-cloud-trail-aktiviert
- nacl-no-unrestricted-ssh-rdp
- neptune-cluster-backup-retention-überprüfen
- neptune-cluster-cloudwatch-log-exportfähig
- neptune-cluster-copy-tags-to-snapshot-enabled
- neptune-cluster-deletion-protection-aktiviert
- neptune-cluster-encrypted
- neptune-cluster-iam-database-Authentifizierung
- neptune-cluster-multi-az-aktiviert
- neptune-cluster-snapshot-encrypted
- neptune-cluster-snapshot-public-verboten
- netfw-deletion-protection-enabled
- netfw-logging-enabled
- netfw-multi-az-enabled
- netfw-policy-default-action-fragment-Pakete

- netfw-policy-default-action-vollständige Pakete
- netfw-policy-rule-group-assoziiert
- netfw-stateless-rule-group-nicht leer
- netfw-subnet-change-protection-aktiviert
- nlb-cross-zone-load-Balancing aktiviert
- nlb-internal-scheme-check
- nlb-listener-tagged
- nlb-logging-enabled
- no-unrestricted-route-to-igw
- opensearch-access-control-enabled
- opensearch-audit-logging-enabled
- opensearch-data-node-fault-Toleranz
- opensearch-encrypted-at-rest
- opensearch-https-required
- opensearch-in-vpc-only
- opensearch-logs-to-cloudwatch
- opensearch-node-to-node-Verschlüsselungsprüfung
- opensearch-primary-node-fault-Toleranz
- opensearch-update-check
- rabbit-mq-supported-version
- rds-aurora-mysql-audit-Protokollierung aktiviert
- rds-aurora-postgresql-logs-zu-Cloud-Watch
- rds-automatic-minor-version-upgrade-fähig
- rds-cluster-auto-minor-version-upgrade-enable
- rds-cluster-default-admin-überprüfen
- rds-cluster-deletion-protection-aktiviert
- rds-cluster-encrypted-at-ausruhen
- rds-cluster-iam-authentication-aktiviert
- rds-cluster-multi-az-aktiviert
- rds-enhanced-monitoring-enabled

- rds-instance-default-admin-überprüfen
- rds-instance-deletion-protection-aktiviert
- rds-instance-iam-authentication-aktiviert
- rds-instance-public-access-überprüfen
- rds-instance-subnet-igw-überprüfen
- rds-in-backup-plan
- rds-last-backup-recovery-Punkt erstellt
- rds-logging-enabled
- rds-mariadb-instance-encryptedim Transit
- rds-meets-restore-time-Ziel
- rds-multi-az-support
- rds-mysql-instance-encryptedunterwegs
- rds-postgresql-logs-to- Cloudwatch
- rds-postgres-instance-encryptedunterwegs
- rds-proxy-tls-encryption
- rds-resources-protected-by-Backup-Plan
- rds-snapshots-public-prohibited
- rds-snapshot-encrypted
- rds-sqlserver-encrypted-in-Transit
- rds-sql-server-logszur Cloud-Überwachung
- rds-storage-encrypted
- redshift-audit-logging-enabled
- redshift-backup-enabled
- redshift-cluster-configuration-check
- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check
- redshift-cluster-multi-az-aktiviert
- redshift-cluster-parameter-group-markiert
- redshift-cluster-public-access-überprüfen
- redshift-cluster-subnet-group-Multi-Az

- redshift-default-admin-check
- redshift-default-db-name-überprüfen
- redshift-enhanced-vpc-routing-aktiviert
- redshift-require-tls-ssl
- redshift-serverless-default-admin-überprüfen
- redshift-serverless-default-db-Namenscheck
- redshift-serverless-namespace-cmk-Verschlüsselung
- redshift-serverless-publish-logs-zu-Cloud-Watch
- redshift-serverless-workgroup-encryptedauf dem Weg
- redshift-serverless-workgroup-no-öffentlich zugänglich
- redshift-serverless-workgroup-routes-innerhalb von VPC
- redshift-unrestricted-port-access
- required-tags
- restricted-incoming-traffic
- root-account-hardware-mfa-aktiviert
- root-account-mfa-enabled
- s3 -regel-check express-dir-bucket-lifecycle
- nur s3- access-point-in-vpc
- s3- -Blöcke access-point-public-access
- s3- -Blöcke account-level-public-access
- s3- -Blocke-periodisch account-level-public-access
- s 3- bucket-acl-prohibited
- s-3 bucket-blacklisted-actions-prohibited
- s3- bucket-cross-region-replication -aktiviert
- s-3 bucket-default-lock-enabled
- s3 bucket-level-public-access - verboten
- s3- bucket-logging-enabled
- s-3 bucket-mfa-delete-enabled
- s-3 bucket-policy-grantee-check
- s3- bucket-policy-not-more -freizügig

- s 3- bucket-public-read-prohibited
- s-3 bucket-public-write-prohibited
- s-3 bucket-replication-enabled
- s3- bucket-server-side-encryption -aktiviert
- s-3 bucket-ssl-requests-only
- s3-Bucket-Tagged
- s-3 bucket-versioning-enabled
- s-3 default-encryption-kms
- s-3 event-notifications-enabled
- s3 last-backup-recovery-point - erstellt
- s3- lifecycle-policy-check
- s-3 meets-restore-time-target
- s3- resources-in-logically-air -Tresor mit Lücken
- s3 resources-protected-by-backup - -Plan
- s 3- version-lifecycle-policy-check
- sagemaker-app-image-config-markiert
- sagemaker-domain-in-vpc
- sagemaker-domain-tagged
- sagemaker-endpoint-configuration-kms-schlüsselkonfiguriert
- sagemaker-endpoint-config-prod-Anzahl der Instanzen
- sagemaker-feature-group-tagged
- sagemaker-image-description
- sagemaker-image-tagged
- sagemaker-model-in-vpc
- sagemaker-model-isolation-enabled
- sagemaker-notebook-instance-inside-vpc
- sagemaker-notebook-instance-kms-key-konfiguriert
- sagemaker-notebook-instance-platform-Version
- sagemaker-notebook-instance-root-Zugriffsprüfung
- sagemaker-notebook-no-direct-Internetzugang

- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-überprüfen
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- securityhub-enabled
- security-account-information-provided
- service-catalog-shared-within-Organisation
- service-vpc-endpoint-enabled
- sns-encrypted-kms
- sns-topic-message-delivery-Benachrichtigung aktiviert
- sns-topic-no-public-Zugriff
- sqs-queue-no-public-Zugang
- ssm-automation-block-public-teilen
- ssm-automation-logging-enabled
- ssm-document-not-public
- ssm-document-tagged
- step-functions-state-machine-Protokollierung aktiviert
- storagegateway-last-backup-recovery-punkt-erstellt
- storagegateway-resources-in-logically-air-gapped-vault
- storagegateway-resources-protected-by-Ersatzplan
- subnet-auto-assign-public-ip-deaktiviert
- transfer-agreement-description
- transfer-agreement-tagged
- transfer-certificate-description
- transfer-certificate-tagged
- transfer-connector-logging-enabled
- transfer-connector-tagged
- transfer-family-server-no-ftp
- transfer-profile-tagged

- transfer-workflow-description
- transfer-workflow-tagged
- virtualmachine-last-backup-recovery-Punkt erstellt
- virtualmachine-resources-in-logically-air-gapped-vault
- virtualmachine-resources-protected-by-Ersatzplan
- vpc-default-security-group-geschlossen
- vpc-endpoint-enabled
- vpc-flow-logs-enabled
- vpc-network-acl-unused-überprüfen
- vpc-peering-dns-resolution-überprüfen
- vpc-sg-open-only-to-authorized-ports
- vpc-sg-port-restriction-überprüfen
- vpc-vpn-2-tunnels-up
- wafv2-logging-enabled
- WAF 2- rulegroup-logging-enabled
- WAF 2- rulegroup-not-empty
- WAF 2- webacl-not-empty
- waf-regional-rulegroup-not-leer
- waf-regional-rule-not-leer
- waf-regional-webacl-not-leer
- workspaces-root-volume-encryption-aktiviert
- workspaces-user-volume-encryption-aktiviert

Region Asien-Pazifik (Osaka)

Asien-Pazifik (Osaka)

- access-keys-rotated
- account-part-of-organizations
- acmpca-certificate-authority-tagged
- acm-certificate-rsa-check
- acm-pca-root-ca-deaktiviert

- active-mq-supported-version
- alb-desync-mode-check
- alb-internal-scheme-check
- alb-listener-tagged
- amplify-app-branch-auto-löschung aktiviert
- amplify-app-description
- amplify-app-tagged
- amplify-branch-performance-mode-aktiviert
- amplify-branch-tagged
- api-gwv2- access-logs-enabled
- api-gwv2- authorization-type-configured
- api-gw-associated-with-WAF
- api-gw-cache-enabled-und-verschlüsselt
- api-gw-endpoint-type-überprüfen
- api-gw-execution-logging-aktiviert
- api-gw-ssl-enabled
- api-gw-xray-enabled
- appconfig-application-description
- appconfig-application-tagged
- appconfig-configuration-profile-tagged
- appconfig-configuration-profile-validators-nicht leer
- appconfig-deployment-strategy-description
- appconfig-deployment-strategy-replicate-zu-ssm
- appconfig-environment-description
- appconfig-environment-tagged
- appconfig-extension-association-tagged
- appconfig-freeform-profile-config-Speicher
- appconfig-hosted-configuration-version-Beschreibung
- appmesh-gateway-route-tagged
- appmesh-mesh-deny-tcp-Weiterleitung

- appmesh-mesh-tagged
- appmesh-route-tagged
- appmesh-virtual-gateway-backend-Standardeinstellungen-TLS
- appmesh-virtual-gateway-logging-file-path-exists
- appmesh-virtual-gateway-tagged
- appmesh-virtual-node-backend-defaults-tls-on
- appmesh-virtual-node-logging-file-path-exists
- appmesh-virtual-node-tagged
- appmesh-virtual-router-tagged
- appmesh-virtual-service-tagged
- approved-amis-by-id
- approved-amis-by-tag
- appsync-associated-with-waf
- appsync-authorization-check
- appsync-cache-encryption-at-ausruhen
- appsync-logging-enabled
- athena-data-catalog-description
- athena-prepared-statement-description
- athena-workgroup-description
- athena-workgroup-encrypted-at-ausruhen
- athena-workgroup-enforce-workgroup-Konfiguration
- athena-workgroup-engine-version-automatisches Upgrade
- athena-workgroup-logging-enabled
- aurora-last-backup-recovery-Punkt erstellt
- aurora-meets-restore-time-Ziel
- aurora-mysql-backtracking-enabled
- aurora-mysql-cluster-audit-Protokollierung
- aurora-resources-in-logically-air-gapped-vault
- aurora-resources-protected-by-Backup-Plan
- autoscaling-capacity-rebalancing

- autoscaling-group-elb-healthcheck-erforderlich
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-hop-Grenze
- autoscaling-launch-config-public-ip-deaktiviert
- autoscaling-launch-template
- autoscaling-multiple-az
- autoscaling-multiple-instance-types
- backup-plan-min-frequency-and-min-retention-check
- backup-recovery-point-encrypted
- backup-recovery-point-manual-Löschen-deaktiviert
- backup-recovery-point-minimum-Aufbewahrungsprüfung
- batch-compute-environment-enabled
- batch-compute-environment-managed
- batch-compute-environment-tagged
- batch-job-queue-enabled
- batch-job-queue-tagged
- batch-managed-compute-environment-using-launch-template
- batch-managed-compute-env-compute-resources-tagged
- batch-scheduling-policy-tagged
- clb-desync-mode-check
- clb-multiple-az
- cloudformation-stack-drift-detection-überprüfen
- cloudformation-stack-notification-check
- cloudtrail-all-read-s3- data-event-check
- cloudtrail-all-write-s3- data-event-check
- Wolkenspur-S3- bucket-access-logging
- CloudTrail-S3- bucket-public-access-prohibited
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check

- cloudwatch-alarm-action-enabled-überprüfen
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted
- cloud-trail-cloud-watch-logs-aktiviert
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-Validierung aktiviert
- cmk-backing-key-rotation-aktiviert
- codebuild-project-envvar-awscred-überprüfen
- codebuild-project-logging-enabled
- codebuild-project-s3-log-verschlüsselt
- codebuild-project-source-repo-URL-Prüfung
- codebuild-report-group-encrypted-im Ruhezustand
- codedeploy-auto-rollback-monitor-aktiviert
- codedeploy-deployment-group-auto-rollback-aktiviert
- codedeploy-deployment-group-outdated-instanzen-aktualisieren
- Codedeploy-ec2- minimum-healthy-hosts-configured
- codedeploy-lambda-allatonce-traffic-shift-deaktiviert
- cognito-identity-pool-unauth-Zugriffsprüfung
- cognito-user-pool-advanced-sicherheitsaktiviert
- cognito-user-pool-tagged
- custom-eventbus-policy-attached
- cw-loggroup-retention-period-überprüfen
- datasync-task-data-verification-aktiviert
- datasync-task-logging-enabled
- datasync-task-tagged
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type

- dms-auto-minor-version-aktualisieren-Prüfung
- dms-endpoint-ssl-configured
- dms-endpoint-tagged
- dms-mongo-db-authentication-aktiviert
- dms-redis-tls-enabled
- dms-replication-not-public
- dms-replication-task-tagged
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-last-backup-recovery-punkt-erstellt
- dynamodb-meets-restore-time-Ziel
- dynamodb-pitr-enabled
- dynamodb-resources-protected-by-Backup-Plan
- dynamodb-table-deletion-protection-aktiviert
- dynamodb-table-encrypted-kms
- dynamodb-throughput-limit-check
- ebs-in-backup-plan
- ebs-last-backup-recovery-punkt-erstellt
- ebs-meets-restore-time-Ziel
- ebs-optimized-instance
- ebs-resources-in-logically-air-gapped-vault
- ebs-resources-protected-by-Backup-Plan
- ebs-snapshot-public-restorable-überprüfen
- ec2- capacity-reservation-tagged
- ec2- aktiviert client-vpn-connection-log
- ec2- client-vpn-endpoint-tagged
- ec2- dhcp-options-tagged
- ec2- ebs-encryption-by-default
- ec2- aktiviert enis-source-destination-check
- ec2-fleet-markiert

- ec2-imdsv2-check
- ec2- instance-detailed-monitoring-enabled
- ec2-ami instance-launched-with-allowed
- ec2- instance-managed-by-ssm
- ec2- instance-multiple-eni-check
- ec2- instance-no-public-ip
- ec2- instance-profile-attached
- ec2- erstellt last-backup-recovery-point
- ec2-2-prüfen launch-template-imdsv
- ec2- -deaktiviert launch-template-public-ip
- ec2- launch-template-tagged
- ec2- managedinstance-applications-blacklisted
- ec2- managedinstance-applications-required
- ec2- managedinstance-inventory-blacklisted
- ec2- managedinstance-platform-check
- ec2- meets-restore-time-target
- ec2- Analyse mit Schlagwörtern network-insights-access-scope
- ec2 network-insights-access-scope - markiert
- ec2- network-insights-path-tagged
- ec2- no-amazon-key-pair
- ec2- prefix-list-tagged
- ec2- -Tresor mit Lücken resources-in-logically-air
- ec2- resources-protected-by-backup -plan
- ec2- -eni security-group-attached-to
- ec2- token-hop-limit-check
- ec2- traffic-mirror-filter-description
- ec2- traffic-mirror-filter-tagged
- ec2- traffic-mirror-session-description
- ec2- traffic-mirror-session-tagged
- ec2- traffic-mirror-target-description

- ec2- traffic-mirror-target-tagged
- ec2- markiert transit-gateway-multicast-domain
- ec2- volume-inuse-check
- ec2- vpn-connection-logging-enabled
- ecr-private-image-scanning-aktiviert
- ecr-private-lifecycle-policy-konfiguriert
- ecr-private-tag-immutability-aktiviert
- ecr-repository-cmk-encryption-aktiviert
- ecr-repository-tagged
- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-container-insights-enabled
- ecs-fargate-latest-platform-Version
- ecs-no-environment-secrets
- ecs-task-definition-log-Konfiguration
- ecs-task-definition-network-mode-not-host
- ecs-task-definition-pid-Modus-Überprüfung
- ecs-task-definition-user-for-host-mode-check
- efs-access-point-enforce-Stammverzeichnis
- efs-access-point-enforce-Benutzeridentität
- efs-automatic-backups-enabled
- efs-encrypted-check
- efs-filesystem-ct-encrypted
- efs-in-backup-plan
- efs-last-backup-recovery-Punkt erstellt
- efs-meets-restore-time-Ziel
- efs-mount-target-public-zugänglich
- efs-resources-in-logically-air-gapped-vault
- efs-resources-protected-by-Backup-Plan
- eip-attached

- eks-cluster-logging-enabled
- eks-cluster-log-enabled
- eks-cluster-secrets-encrypted
- eks-cluster-supported-version
- eks-endpoint-no-public-Zugang
- eks-secrets-encrypted
- elasticache-auto-minor-version-aktualisieren-Prüfung
- elasticache-rbac-auth-enabled
- elasticache-redis-cluster-automatic-Backup-Check
- elasticache-repl-grp-auto-failover-fähig
- elasticache-repl-grp-encrypted-im Ruhezustand
- elasticache-repl-grp-encryptedim Transit
- elasticache-repl-grp-redis-auth-aktiviert
- elasticache-supported-engine-version
- elasticbeanstalk-application-description
- elasticbeanstalk-application-version-description
- elasticbeanstalk-environment-description
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch
- elasticsearch-node-to-node-Verschlüsselungsprüfung
- elastic-beanstalk-logs-to- Cloudwatch
- Elb V2- listener-encryption-in-transit
- elbv2-multiple-az
- elbv2- prüfen predefined-security-policy-ssl
- elb-cross-zone-load-Balancing aktiviert
- elb-logging-enabled
- emr-block-public-access
- emr-kerberos-enabled
- emr-security-configuration-encryption-ausruhen

- emr-security-configuration-encryption-Transit
- encrypted-volumes
- event-data-store-cmk-Verschlüsselung aktiviert
- fms-shield-resource-policy-überprüfen
- fms-webacl-resource-policy-überprüfen
- fms-webacl-rulegroup-association-überprüfen
- fsx-last-backup-recovery-Punkt erstellt
- fsx-lustre-copy-tagszu Backups
- fsx-meets-restore-time-Ziel
- fsx-ontap-deployment-type-überprüfen
- fsx-openzfs-copy-tags-aktiviert
- fsx-openzfs-deployment-type-überprüfen
- fsx-resources-protected-by-Ersatzplan
- fsx-windows-audit-log-konfiguriert
- fsx-windows-deployment-type-überprüfen
- glb-listener-tagged
- global-endpoint-event-replication-aktiviert
- glue-job-logging-enabled
- glue-ml-transform-encrypted-im Ruhezustand
- glue-spark-job-supported-Ausführung
- GuardDuty-EC2- protection-runtime-enabled
- guardduty-ecs-protection-runtime-aktiviert
- guardduty-eks-protection-audit-aktiviert
- guardduty-eks-protection-runtime-aktiviert
- guardduty-enabled-centralized
- guardduty-lambda-protection-enabled
- guardduty-malware-protection-enabled
- guardduty-non-archived-findings
- guardduty-rds-protection-enabled
- guardduty-runtime-monitoring-enabled

- GuardDuty-S3-Schutz aktiviert
- iam-customer-policy-blocked-kms-Aktionen
- iam-external-access-analyzer-aktiviert
- iam-group-has-users-überprüfen
- iam-inline-policy-blocked-KMS-Aktionen
- iam-no-inline-policy-überprüfen
- iam-password-policy
- iam-policy-blacklisted-check
- iam-policy-in-use
- iam-policy-no-statements-with-admin-access
- iam-policy-no-statements-with-full-access
- iam-role-managed-policy-überprüfen
- iam-root-access-key-überprüfen
- iam-user-group-membership-überprüfen
- iam-user-mfa-enabled
- iam-user-no-policies-überprüfen
- iam-user-unused-credentials-überprüfen
- incoming-ssh-disabled
- inspector-ec2-Scan aktiviert
- inspector-ecr-scan-enabled
- inspector-lambda-standard-scan-aktiviert
- instances-in-vpc
- internet-gateway-authorized-vpc-nur
- kinesis-firehose-delivery-stream-verschlüsselt
- kinesis-stream-backup-retention-überprüfen
- kinesis-stream-encrypted
- kms-cmk-not-scheduled-zum Löschen
- kms-key-policy-no-öffentlicher Zugang
- lambda-concurrency-check
- lambda-dlq-check

- lambda-function-public-access-verboten
- lambda-function-settings-check
- lambda-function-xray-enabled
- lambda-inside-vpc
- lambda-vpc-multi-az-überprüfen
- macie-auto-sensitive-data-Discovery-Check
- macie-status-check
- mariadb-publish-logs-to-Cloudwatch-Protokolle
- mfa-enabled-for-iam-Konsolenzugriff
- mq-active-broker-ldap-Authentifizierung
- mq-active-deployment-mode
- mq-active-single-instance-broker-storage-type-efs
- mq-automatic-minor-version-Upgrade aktiviert
- mq-auto-minor-version-upgrade-fähig
- mq-broker-general-logging-aktiviert
- mq-cloudwatch-audit-logging-aktiviert
- mq-cloudwatch-audit-log-aktiviert
- mq-no-public-access
- mq-rabbit-deployment-mode
- msk-cluster-public-access-deaktiviert
- msk-enhanced-monitoring-enabled
- msk-in-cluster-node-require-tls
- msk-unrestricted-access-check
- multi-region-cloud-trail-aktiviert
- nacl-no-unrestricted-ssh-rdp
- neptune-cluster-backup-retention-überprüfen
- neptune-cluster-cloudwatch-log-exportfähig
- neptune-cluster-copy-tags-to-snapshot-enabled
- neptune-cluster-deletion-protection-aktiviert
- neptune-cluster-encrypted

- neptune-cluster-iam-database-Authentifizierung
- neptune-cluster-multi-az-aktiviert
- neptune-cluster-snapshot-encrypted
- neptune-cluster-snapshot-public-verboten
- netfw-deletion-protection-enabled
- netfw-logging-enabled
- netfw-multi-az-enabled
- netfw-policy-default-action-fragment-Pakete
- netfw-policy-default-action-vollständige Pakete
- netfw-policy-rule-group-assoziiert
- netfw-stateless-rule-group-nicht leer
- netfw-subnet-change-protection-aktiviert
- nlb-cross-zone-load-Balancing aktiviert
- nlb-internal-scheme-check
- nlb-listener-tagged
- nlb-logging-enabled
- no-unrestricted-route-to-igw
- opensearch-access-control-enabled
- opensearch-audit-logging-enabled
- opensearch-data-node-fault-Toleranz
- opensearch-encrypted-at-rest
- opensearch-https-required
- opensearch-in-vpc-only
- opensearch-logs-to-cloudwatch
- opensearch-node-to-node-Verschlüsselungsprüfung
- opensearch-primary-node-fault-Toleranz
- opensearch-update-check
- rabbit-mq-supported-version
- rds-aurora-mysql-audit-Protokollierung aktiviert
- rds-aurora-postgresql-logs-zu-Cloud-Watch

- rds-automatic-minor-version-upgrade-fähig
- rds-cluster-auto-minor-version-upgrade-enable
- rds-cluster-default-admin-überprüfen
- rds-cluster-deletion-protection-aktiviert
- rds-cluster-encrypted-at-ausruhen
- rds-cluster-iam-authentication-aktiviert
- rds-cluster-multi-az-aktiviert
- rds-enhanced-monitoring-enabled
- rds-instance-default-admin-überprüfen
- rds-instance-deletion-protection-aktiviert
- rds-instance-iam-authentication-aktiviert
- rds-instance-public-access-überprüfen
- rds-instance-subnet-igw-überprüfen
- rds-in-backup-plan
- rds-last-backup-recovery-Punkt erstellt
- rds-logging-enabled
- rds-mariadb-instance-encryptedim Transit
- rds-meets-restore-time-Ziel
- rds-multi-az-support
- rds-mysql-instance-encryptedunterwegs
- rds-postgresql-logs-to- Cloudwatch
- rds-postgres-instance-encryptedunterwegs
- rds-proxy-tls-encryption
- rds-resources-protected-by-Backup-Plan
- rds-snapshots-public-prohibited
- rds-snapshot-encrypted
- rds-sqlserver-encrypted-in-Transit
- rds-sql-server-logszur Cloud-Überwachung
- rds-storage-encrypted
- redshift-audit-logging-enabled

- redshift-backup-enabled
- redshift-cluster-configuration-check
- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check
- redshift-cluster-multi-az-aktiviert
- redshift-cluster-parameter-group-markiert
- redshift-cluster-public-access-überprüfen
- redshift-cluster-subnet-group-Multi-Az
- redshift-default-admin-check
- redshift-default-db-name-überprüfen
- redshift-enhanced-vpc-routing-aktiviert
- redshift-require-tls-ssl
- redshift-unrestricted-port-access
- required-tags
- restricted-incoming-traffic
- root-account-hardware-mfa-aktiviert
- root-account-mfa-enabled
- nur s3- access-point-in-vpc
- s3- -Blöcke access-point-public-access
- s3- -Blöcke account-level-public-access
- s3- -Blocke-periodisch account-level-public-access
- s 3- bucket-acl-prohibited
- s-3 bucket-blacklisted-actions-prohibited
- s3- bucket-cross-region-replication -aktiviert
- s-3 bucket-default-lock-enabled
- s3 bucket-level-public-access - verboten
- s3- bucket-logging-enabled
- s-3 bucket-mfa-delete-enabled
- s-3 bucket-policy-grantee-check
- s3- bucket-policy-not-more -freizügig

- s 3- bucket-public-read-prohibited
- s-3 bucket-public-write-prohibited
- s-3 bucket-replication-enabled
- s3- bucket-server-side-encryption -aktiviert
- s-3 bucket-ssl-requests-only
- s3-Bucket-Tagged
- s-3 bucket-versioning-enabled
- s-3 default-encryption-kms
- s-3 event-notifications-enabled
- s3 last-backup-recovery-point - erstellt
- s3- lifecycle-policy-check
- s-3 meets-restore-time-target
- s3- resources-in-logically-air -Tresor mit Lücken
- s3 resources-protected-by-backup - -Plan
- s 3- version-lifecycle-policy-check
- sagemaker-app-image-config-markiert
- sagemaker-domain-in-vpc
- sagemaker-domain-tagged
- sagemaker-endpoint-configuration-kms-schlüsselkonfiguriert
- sagemaker-endpoint-config-prod-Anzahl der Instanzen
- sagemaker-feature-group-tagged
- sagemaker-image-description
- sagemaker-image-tagged
- sagemaker-model-in-vpc
- sagemaker-model-isolation-enabled
- sagemaker-notebook-instance-inside-vpc
- sagemaker-notebook-instance-kms-key-konfiguriert
- sagemaker-notebook-instance-platform-Version
- sagemaker-notebook-instance-root-Zugriffsprüfung
- sagemaker-notebook-no-direct-Internetzugang

- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-überprüfen
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- securityhub-enabled
- security-account-information-provided
- service-catalog-shared-within-Organisation
- service-vpc-endpoint-enabled
- sns-encrypted-kms
- sns-topic-message-delivery-Benachrichtigung aktiviert
- sns-topic-no-public-Zugriff
- sqs-queue-no-public-Zugang
- ssm-automation-block-public-teilen
- ssm-automation-logging-enabled
- ssm-document-not-public
- ssm-document-tagged
- step-functions-state-machine-Protokollierung aktiviert
- storagegateway-last-backup-recovery-punkt-erstellt
- storagegateway-resources-in-logically-air-gapped-vault
- storagegateway-resources-protected-by-Ersatzplan
- subnet-auto-assign-public-ip-deaktiviert
- transfer-agreement-description
- transfer-agreement-tagged
- transfer-certificate-description
- transfer-certificate-tagged
- transfer-connector-logging-enabled
- transfer-connector-tagged
- transfer-family-server-no-ftp
- transfer-profile-tagged

- transfer-workflow-description
- transfer-workflow-tagged
- virtualmachine-last-backup-recovery-Punkt erstellt
- virtualmachine-resources-in-logically-air-gapped-vault
- virtualmachine-resources-protected-by-Ersatzplan
- vpc-default-security-group-geschlossen
- vpc-flow-logs-enabled
- vpc-network-acl-unused-überprüfen
- vpc-peering-dns-resolution-überprüfen
- vpc-sg-open-only-to-authorized-ports
- vpc-sg-port-restriction-überprüfen
- wafv2-logging-enabled
- WAF 2- rulegroup-logging-enabled
- WAF 2- rulegroup-not-empty
- WAF 2- webacl-not-empty
- waf-regional-rule-not-leer
- waf-regional-webacl-not-leer

Region Asien-Pazifik (Seoul)

Asien-Pazifik (Seoul)

- access-keys-rotated
- account-part-of-organizations
- acmpca-certificate-authority-tagged
- acm-certificate-expiration-check
- acm-certificate-rsa-check
- acm-pca-root-ca-deaktiviert
- active-mq-supported-version
- alb-desync-mode-check
- alb-http-drop-invalid-Header-fähig
- alb-http-to-https-Umleitungsprüfung

- alb-internal-scheme-check
- alb-listener-tagged
- alb-waf-enabled
- amplify-app-branch-auto-löschung aktiviert
- amplify-app-description
- amplify-app-tagged
- amplify-branch-performance-mode-aktiviert
- amplify-branch-tagged
- api-gwv2- access-logs-enabled
- api-gwv2- authorization-type-configured
- api-gw-associated-with-WAF
- api-gw-cache-enabled-und-verschlüsselt
- api-gw-endpoint-type-überprüfen
- api-gw-execution-logging-aktiviert
- api-gw-ssl-enabled
- api-gw-xray-enabled
- appconfig-application-description
- appconfig-application-tagged
- appconfig-configuration-profile-tagged
- appconfig-configuration-profile-validators-nicht leer
- appconfig-deployment-strategy-description
- appconfig-deployment-strategy-replicate-zu-ssm
- appconfig-environment-description
- appconfig-environment-tagged
- appconfig-extension-association-tagged
- appconfig-freeform-profile-config-Speicher
- appconfig-hosted-configuration-version-Beschreibung
- appflow-flow-tagged
- appintegrations-event-integration-description
- appintegrations-event-integration-tagged

- appmesh-gateway-route-tagged
- appmesh-mesh-deny-tcp-Weiterleitung
- appmesh-mesh-tagged
- appmesh-route-tagged
- appmesh-virtual-gateway-backend-Standardeinstellungen-TLS
- appmesh-virtual-gateway-logging-file-path-exists
- appmesh-virtual-gateway-tagged
- appmesh-virtual-node-backend-defaults-tls-on
- appmesh-virtual-node-logging-file-path-exists
- appmesh-virtual-node-tagged
- appmesh-virtual-router-tagged
- appmesh-virtual-service-tagged
- approved-amis-by-id
- approved-amis-by-tag
- appstream-fleet-in-vpc
- appsync-associated-with-waf
- appsync-authorization-check
- appsync-cache-encryption-at-ausruhen
- appsync-logging-enabled
- athena-data-catalog-description
- athena-prepared-statement-description
- athena-workgroup-description
- athena-workgroup-encrypted-at-ausruhen
- athena-workgroup-enforce-workgroup-Konfiguration
- athena-workgroup-engine-version-automatisches Upgrade
- athena-workgroup-logging-enabled
- aurora-last-backup-recovery-Punkt erstellt
- aurora-meets-restore-time-Ziel
- aurora-mysql-backtracking-enabled
- aurora-mysql-cluster-audit-Protokollierung

- aurora-resources-in-logically-air-gapped-vault
- aurora-resources-protected-by-Backup-Plan
- autoscaling-capacity-rebalancing
- autoscaling-group-elb-healthcheck-erforderlich
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-hop-Grenze
- autoscaling-launch-config-public-ip-deaktiviert
- autoscaling-launch-template
- autoscaling-multiple-az
- autoscaling-multiple-instance-types
- backup-plan-min-frequency-and-min-retention-check
- backup-recovery-point-encrypted
- backup-recovery-point-manual-Löschen-deaktiviert
- backup-recovery-point-minimum-Aufbewahrungsprüfung
- batch-compute-environment-enabled
- batch-compute-environment-managed
- batch-compute-environment-tagged
- batch-job-queue-enabled
- batch-job-queue-tagged
- batch-managed-compute-environment-using-launch-template
- batch-managed-compute-env-compute-resources-tagged
- batch-scheduling-policy-tagged
- beanstalk-enhanced-health-reporting-aktiviert
- cassandra-keyspace-tagged
- clb-desync-mode-check
- clb-multiple-az
- cloudformation-stack-drift-detection-überprüfen
- cloudformation-stack-notification-check
- cloudtrail-all-read-s3- data-event-check
- cloudtrail-all-write-s3- data-event-check

- Wolkenspur-S3- bucket-access-logging
- CloudTrail-S3- bucket-public-access-prohibited
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-action-enabled-überprüfen
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted
- cloud-trail-cloud-watch-logs-aktiviert
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-Validierung aktiviert
- cmk-backing-key-rotation-aktiviert
- codebuild-project-artifact-encryption
- codebuild-project-environment-privileged-überprüfen
- codebuild-project-envvar-awscred-überprüfen
- codebuild-project-logging-enabled
- codebuild-project-s3-log-verschlüsselt
- codebuild-project-source-repo-URL-Prüfung
- codebuild-report-group-encrypted-im Ruhezustand
- codedeploy-auto-rollback-monitor-aktiviert
- codedeploy-deployment-group-auto-rollback-aktiviert
- codedeploy-deployment-group-outdated-instanzen-aktualisieren
- Codedeploy-ec2- minimum-healthy-hosts-configured
- codedeploy-lambda-allatonce-traffic-shift-deaktiviert
- codepipeline-deployment-count-check
- codepipeline-region-fanout-check
- cognito-user-pool-advanced-sicherheitsaktiviert
- cognito-user-pool-tagged

- connect-instance-logging-enabled
- customerprofiles-object-type-allow-Profilerstellung
- customerprofiles-object-type-tagged
- custom-eventbus-policy-attached
- custom-schema-registry-policy-beigefügt
- cw-loggroup-retention-period-überprüfen
- datasync-task-data-verification-aktiviert
- datasync-task-logging-enabled
- datasync-task-tagged
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- dms-auto-minor-version-aktualisieren-Prüfung
- dms-endpoint-ssl-configured
- dms-endpoint-tagged
- dms-mongo-db-authentication-aktiviert
- dms-neptune-iam-authorization-aktiviert
- dms-redis-tls-enabled
- dms-replication-not-public
- dms-replication-task-sourcedb-Protokollierung
- dms-replication-task-tagged
- dms-replication-task-targetdb-Protokollierung
- docdb-cluster-audit-logging-aktiviert
- docdb-cluster-backup-retention-überprüfen
- docdb-cluster-deletion-protection-aktiviert
- docdb-cluster-encrypted
- docdb-cluster-encrypted-in-Transit
- docdb-cluster-snapshot-public-verboten
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan

- dynamodb-last-backup-recovery-Punkt erstellt
- dynamodb-meets-restore-time-Ziel
- dynamodb-pitr-enabled
- dynamodb-resources-protected-by-Backup-Plan
- dynamodb-table-deletion-protection-aktiviert
- dynamodb-table-encrypted-kms
- dynamodb-table-encryption-enabled
- dynamodb-throughput-limit-check
- ebs-in-backup-plan
- ebs-last-backup-recovery-punkt-erstellt
- ebs-meets-restore-time-Ziel
- ebs-optimized-instance
- ebs-resources-in-logically-air-gapped-vault
- ebs-resources-protected-by-Backup-Plan
- ebs-snapshot-public-restorable-überprüfen
- ec2- capacity-reservation-tagged
- ec2- carrier-gateway-tagged
- ec2- aktiviert client-vpn-connection-log
- ec2- client-vpn-endpoint-tagged
- ec2- -alle client-vpn-not-authorize
- ec2- dhcp-options-tagged
- ec2- ebs-encryption-by-default
- ec2-Fleet-markiert
- ec2-imdsv2-check
- ec2- instance-detailed-monitoring-enabled
- ec2-ami instance-launched-with-allowed
- ec2- instance-managed-by-ssm
- ec2- instance-multiple-eni-check
- ec2- instance-no-public-ip
- ec2- instance-profile-attached

- ec2- erstellt last-backup-recovery-point
- ec2-2-prüfen launch-template-imdsv
- ec2- -deaktiviert launch-template-public-ip
- ec2- launch-template-tagged
- ec2- managedinstance-applications-blacklisted
- ec2- managedinstance-applications-required
- ec2- prüfen managedinstance-association-compliance-status
- ec2- managedinstance-inventory-blacklisted
- ec2- prüfen managedinstance-patch-compliance-status
- ec2- managedinstance-platform-check
- ec2- meets-restore-time-target
- ec2- Analyse mit Schlagwörtern network-insights-access-scope
- ec2 network-insights-access-scope - markiert
- ec2- network-insights-path-tagged
- ec2- no-amazon-key-pair
- ec2- prefix-list-tagged
- ec2- -Tresor mit Lücken resources-in-logically-air
- ec2- resources-protected-by-backup -plan
- ec2- -eni security-group-attached-to
- ec2- -eni-periodisch security-group-attached-to
- ec2 spot-fleet-request-ct - - encryption-at-rest
- ec2-stopped-instance
- ec2- token-hop-limit-check
- ec2- traffic-mirror-filter-description
- ec2- traffic-mirror-filter-tagged
- ec2- traffic-mirror-session-description
- ec2- traffic-mirror-session-tagged
- ec2- traffic-mirror-target-description
- ec2- traffic-mirror-target-tagged
- ec2- -attach-deaktiviert transit-gateway-auto-vpc

- ec2 transit-gateway-multicast-domain - markiert
- ec2- volume-inuse-check
- ec2- vpn-connection-logging-enabled
- ecr-private-image-scanning-aktiviert
- ecr-private-lifecycle-policy-konfiguriert
- ecr-private-tag-immutability-aktiviert
- ecr-repository-cmk-encryption-aktiviert
- ecr-repository-tagged
- ecs-awsvpc-networking-enabled
- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-container-insights-enabled
- ecs-fargate-latest-platform-Version
- ecs-no-environment-secrets
- ecs-task-definition-log-Konfiguration
- ecs-task-definition-memory-hartes Limit
- ecs-task-definition-network-mode-not-host
- ecs-task-definition-nonroot-Benutzer
- ecs-task-definition-pid-Modus-Check
- ecs-task-definition-user-for-host-mode-check
- efs-access-point-enforce-Stammverzeichnis
- efs-access-point-enforce-Benutzeridentität
- efs-automatic-backups-enabled
- efs-encrypted-check
- efs-filesystem-ct-encrypted
- efs-in-backup-plan
- efs-last-backup-recovery-Punkt erstellt
- efs-meets-restore-time-Ziel
- efs-mount-target-public-zugänglich
- efs-resources-in-logically-air-gapped-vault

- efs-resources-protected-by-Ersatzplan
- eip-attached
- eks-cluster-logging-enabled
- eks-cluster-log-enabled
- eks-cluster-oldest-supported-Ausführung
- eks-cluster-secrets-encrypted
- eks-cluster-supported-version
- eks-endpoint-no-public-Zugang
- eks-secrets-encrypted
- elasticache-auto-minor-version-aktualisieren-Prüfung
- elasticache-rbac-auth-enabled
- elasticache-redis-cluster-automatic-Backup-Check
- elasticache-repl-grp-auto-failover-fähig
- elasticache-repl-grp-encrypted-im Ruhezustand
- elasticache-repl-grp-encryptedim Transit
- elasticache-repl-grp-redis-auth-aktiviert
- elasticache-subnet-group-check
- elasticache-supported-engine-version
- elasticbeanstalk-application-description
- elasticbeanstalk-application-version-description
- elasticbeanstalk-environment-description
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch
- elasticsearch-node-to-node-Verschlüsselungsprüfung
- elastic-beanstalk-logs-to- Cloudwatch
- elastic-beanstalk-managed-updates-aktiviert
- elbv2- acm-certificate-required
- elbv2-multiple-az
- elbv2- prüfen predefined-security-policy-ssl

- elb-acm-certificate-required
- elb-cross-zone-load-Balancing aktiviert
- elb-custom-security-policy-ssl-Prüfung
- elb-deletion-protection-enabled
- elb-logging-enabled
- elb-predefined-security-policy-ssl-Überprüfung
- elb-tls-https-listeners-nur
- emr-block-public-access
- emr-kerberos-enabled
- emr-master-no-public-ip
- emr-security-configuration-encryption-ruh dich aus
- emr-security-configuration-encryption-Transit
- encrypted-volumes
- event-data-store-cmk-Verschlüsselung aktiviert
- fis-experiment-template-log-Konfiguration ist vorhanden
- fis-experiment-template-tagged
- fms-shield-resource-policy-überprüfen
- fms-webacl-resource-policy-überprüfen
- fms-webacl-rulegroup-association-überprüfen
- fsx-last-backup-recovery-Punkt erstellt
- fsx-lustre-copy-tagszu Backups
- fsx-meets-restore-time-Ziel
- fsx-ontap-deployment-type-überprüfen
- fsx-openzfs-copy-tags-aktiviert
- fsx-openzfs-deployment-type-überprüfen
- fsx-resources-protected-by-Ersatzplan
- fsx-windows-audit-log-konfiguriert
- fsx-windows-deployment-type-überprüfen
- glb-listener-tagged
- global-endpoint-event-replication-aktiviert

- glue-job-logging-enabled
- glue-ml-transform-encrypted-im Ruhezustand
- glue-spark-job-supported-Ausführung
- GuardDuty-EC2- protection-runtime-enabled
- guardduty-ecs-protection-runtime-aktiviert
- guardduty-eks-protection-audit-aktiviert
- guardduty-eks-protection-runtime-aktiviert
- guardduty-enabled-centralized
- guardduty-lambda-protection-enabled
- guardduty-malware-protection-enabled
- guardduty-non-archived-findings
- guardduty-rds-protection-enabled
- guardduty-runtime-monitoring-enabled
- GuardDuty-S3-Schutz aktiviert
- iam-customer-policy-blocked-kms-Aktionen
- iam-external-access-analyzer-aktiviert
- iam-group-has-users-überprüfen
- iam-inline-policy-blocked-KMS-Aktionen
- iam-no-inline-policy-überprüfen
- iam-password-policy
- iam-policy-blacklisted-check
- iam-policy-in-use
- iam-policy-no-statements-with-admin-access
- iam-policy-no-statements-with-full-access
- iam-role-managed-policy-überprüfen
- iam-root-access-key-überprüfen
- iam-user-group-membership-überprüfen
- iam-user-mfa-enabled
- iam-user-no-policies-überprüfen
- iam-user-unused-credentials-überprüfen

- incoming-ssh-disabled
- inspector-ec2-Scan aktiviert
- inspector-ecr-scan-enabled
- inspector-lambda-standard-scan-aktiviert
- instances-in-vpc
- internet-gateway-authorized-vpc-nur
- iotevents-alarm-model-tagged
- iotevents-detector-model-tagged
- iotevents-input-tagged
- iotsitewise-asset-model-tagged
- iotsitewise-dashboard-tagged
- iotsitewise-gateway-tagged
- iotsitewise-portal-tagged
- iotsitewise-project-tagged
- iottwinmaker-component-type-tagged
- iottwinmaker-scene-tagged
- iottwinmaker-sync-job-tagged
- iottwinmaker-workspace-tagged
- iot-authorizer-token-signing-aktiviert
- ivs-channel-playback-authorization-aktiviert
- ivs-channel-tagged
- ivs-playback-key-pair-markiert
- ivs-recording-configuration-tagged
- kinesis-firehose-delivery-stream-verschlüsselt
- kinesis-stream-backup-retention-überprüfen
- kinesis-stream-encrypted
- kms-cmk-not-scheduled-zum Löschen
- kms-key-policy-no-öffentlicher Zugang
- lambda-concurrency-check
- lambda-dlq-check

- lambda-function-public-access-verboten
- lambda-function-settings-check
- lambda-inside-vpc
- lambda-vpc-multi-az-überprüfen
- lightsail-bucket-tagged
- lightsail-certificate-tagged
- lightsail-disk-tagged
- macie-auto-sensitive-data-Discovery-Check
- macie-status-check
- mariadb-publish-logs-to-Cloudwatch-Protokolle
- mfa-enabled-for-iam-Konsolenzugriff
- mq-active-broker-ldap-Authentifizierung
- mq-active-deployment-mode
- mq-active-single-instance-broker-storage-type-efs
- mq-automatic-minor-version-Upgrade aktiviert
- mq-auto-minor-version-upgrade-fähig
- mq-broker-general-logging-aktiviert
- mq-cloudwatch-audit-logging-aktiviert
- mq-cloudwatch-audit-log-aktiviert
- mq-no-public-access
- mq-rabbit-deployment-mode
- msk-enhanced-monitoring-enabled
- msk-in-cluster-node-require-tls
- multi-region-cloud-trail-aktiviert
- nacl-no-unrestricted-ssh-rdp
- neptune-cluster-backup-retention-überprüfen
- neptune-cluster-cloudwatch-log-exportfähig
- neptune-cluster-copy-tags-to-snapshot-enabled
- neptune-cluster-deletion-protection-aktiviert
- neptune-cluster-encrypted

- neptune-cluster-iam-database-Authentifizierung
- neptune-cluster-multi-az-aktiviert
- neptune-cluster-snapshot-encrypted
- neptune-cluster-snapshot-public-verboten
- netfw-deletion-protection-enabled
- netfw-logging-enabled
- netfw-multi-az-enabled
- netfw-policy-default-action-fragment-Pakete
- netfw-policy-default-action-vollständige Pakete
- netfw-policy-rule-group-assoziiert
- netfw-stateless-rule-group-nicht leer
- netfw-subnet-change-protection-aktiviert
- nlb-cross-zone-load-Balancing aktiviert
- nlb-internal-scheme-check
- nlb-listener-tagged
- nlb-logging-enabled
- no-unrestricted-route-to-igw
- opensearch-access-control-enabled
- opensearch-audit-logging-enabled
- opensearch-data-node-fault-Toleranz
- opensearch-encrypted-at-rest
- opensearch-https-required
- opensearch-in-vpc-only
- opensearch-logs-to-cloudwatch
- opensearch-node-to-node-Verschlüsselungsprüfung
- opensearch-primary-node-fault-Toleranz
- opensearch-update-check
- rabbit-mq-supported-version
- rds-aurora-mysql-audit-Protokollierung aktiviert
- rds-aurora-postgresql-logs-zu-Cloud-Watch

- rds-automatic-minor-version-upgrade-fähig
- rds-cluster-auto-minor-version-upgrade-enable
- rds-cluster-default-admin-überprüfen
- rds-cluster-deletion-protection-aktiviert
- rds-cluster-encrypted-at-ausruhen
- rds-cluster-iam-authentication-aktiviert
- rds-cluster-multi-az-aktiviert
- rds-enhanced-monitoring-enabled
- rds-instance-default-admin-überprüfen
- rds-instance-deletion-protection-aktiviert
- rds-instance-iam-authentication-aktiviert
- rds-instance-public-access-überprüfen
- rds-instance-subnet-igw-überprüfen
- rds-in-backup-plan
- rds-last-backup-recovery-Punkt erstellt
- rds-logging-enabled
- rds-mariadb-instance-encryptedim Transit
- rds-meets-restore-time-Ziel
- rds-multi-az-support
- rds-mysql-instance-encryptedunterwegs
- rds-postgresql-logs-to- Cloudwatch
- rds-postgres-instance-encryptedunterwegs
- rds-proxy-tls-encryption
- rds-resources-protected-by-Ersatzplan
- rds-snapshots-public-prohibited
- rds-snapshot-encrypted
- rds-sqlserver-encrypted-in-Transit
- rds-sql-server-logszur Cloud-Überwachung
- rds-storage-encrypted
- redshift-audit-logging-enabled

- redshift-backup-enabled
- redshift-cluster-configuration-check
- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check
- redshift-cluster-parameter-group-markiert
- redshift-cluster-public-access-überprüfen
- redshift-cluster-subnet-group-Multi-Az
- redshift-default-admin-check
- redshift-default-db-name-überprüfen
- redshift-enhanced-vpc-routing-aktiviert
- redshift-require-tls-ssl
- redshift-serverless-default-admin-überprüfen
- redshift-serverless-default-db-Namenscheck
- redshift-serverless-namespace-cmk-Verschlüsselung
- redshift-serverless-publish-logs-zu-Cloud-Watch
- redshift-serverless-workgroup-encryptedauf dem Weg
- redshift-serverless-workgroup-no-öffentlich zugänglich
- redshift-serverless-workgroup-routes-innerhalb von VPC
- redshift-unrestricted-port-access
- required-tags
- restricted-incoming-traffic
- root-account-hardware-mfa-aktiviert
- root-account-mfa-enabled
- nur s3- access-point-in-vpc
- s3- -Blöcke access-point-public-access
- s3- -Blöcke account-level-public-access
- s3- -Blocke-periodisch account-level-public-access
- s 3- bucket-acl-prohibited
- s-3 bucket-blacklisted-actions-prohibited
- s3- bucket-cross-region-replication -aktiviert

- s-3 bucket-default-lock-enabled
- s3 bucket-level-public-access - verboten
- s3- bucket-logging-enabled
- s-3 bucket-mfa-delete-enabled
- s-3 bucket-policy-grantee-check
- s3- bucket-policy-not-more -freizügig
- s 3- bucket-public-read-prohibited
- s-3 bucket-public-write-prohibited
- s-3 bucket-replication-enabled
- s3- bucket-server-side-encryption -aktiviert
- s-3 bucket-ssl-requests-only
- s3-Bucket-Tagged
- s-3 bucket-versioning-enabled
- s-3 default-encryption-kms
- s-3 event-notifications-enabled
- s3 last-backup-recovery-point - erstellt
- s3- lifecycle-policy-check
- s-3 meets-restore-time-target
- s3- resources-in-logically-air -Tresor mit Lücken
- s3 resources-protected-by-backup - -Plan
- s 3- version-lifecycle-policy-check
- sagemaker-app-image-config-markiert
- sagemaker-domain-in-vpc
- sagemaker-domain-tagged
- sagemaker-endpoint-configuration-kms-schlüsselkonfiguriert
- sagemaker-endpoint-config-prod-Anzahl der Instanzen
- sagemaker-feature-group-tagged
- sagemaker-image-description
- sagemaker-image-tagged
- sagemaker-model-in-vpc

- sagemaker-model-isolation-enabled
- sagemaker-notebook-instance-inside-vpc
- sagemaker-notebook-instance-kms-key-konfiguriert
- sagemaker-notebook-instance-platform-Version
- sagemaker-notebook-instance-root-Zugriffsprüfung
- sagemaker-notebook-no-direct-Internetzugang
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-überprüfen
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- securityhub-enabled
- security-account-information-provided
- service-catalog-shared-within-Organisation
- service-vpc-endpoint-enabled
- sns-encrypted-kms
- sns-topic-message-delivery-Benachrichtigung aktiviert
- sns-topic-no-public-Zugriff
- sqs-queue-no-public-Zugang
- ssm-document-not-public
- ssm-document-tagged
- step-functions-state-machine-Protokollierung aktiviert
- storagegateway-last-backup-recovery-punkt-erstellt
- storagegateway-resources-in-logically-air-gapped-vault
- storagegateway-resources-protected-by-Ersatzplan
- subnet-auto-assign-public-ip-deaktiviert
- transfer-agreement-description
- transfer-agreement-tagged
- transfer-certificate-description
- transfer-certificate-tagged

- transfer-connector-logging-enabled
- transfer-connector-tagged
- transfer-family-server-no-ftp
- transfer-profile-tagged
- transfer-workflow-description
- transfer-workflow-tagged
- virtualmachine-last-backup-recovery-Punkt erstellt
- virtualmachine-resources-in-logically-air-gapped-vault
- virtualmachine-resources-protected-by-Ersatzplan
- vpc-default-security-group-geschlossen
- vpc-endpoint-enabled
- vpc-flow-logs-enabled
- vpc-network-acl-unused-überprüfen
- vpc-peering-dns-resolution-überprüfen
- vpc-sg-open-only-to-authorized-ports
- vpc-sg-port-restriction-überprüfen
- vpc-vpn-2-tunnels-up
- wafv2-logging-enabled
- WAF 2- rulegroup-logging-enabled
- WAF 2- rulegroup-not-empty
- WAF 2- webacl-not-empty
- waf-regional-rulegroup-not-leer
- waf-regional-rule-not-leer
- waf-regional-webacl-not-leer
- workspaces-root-volume-encryption-aktiviert
- workspaces-user-volume-encryption-aktiviert

Region Asien-Pazifik (Singapur)

Asien-Pazifik (Singapur)

- access-keys-rotated

- account-part-of-organizations
- acmpca-certificate-authority-tagged
- acm-certificate-expiration-check
- acm-certificate-rsa-check
- acm-pca-root-ca-deaktiviert
- active-mq-supported-version
- alb-desync-mode-check
- alb-http-drop-invalid-Header-fähig
- alb-http-to-https-Umleitungsprüfung
- alb-internal-scheme-check
- alb-listener-tagged
- alb-waf-enabled
- amplify-app-branch-auto-löschung aktiviert
- amplify-app-description
- amplify-app-tagged
- amplify-branch-performance-mode-aktiviert
- amplify-branch-tagged
- api-gwv2- access-logs-enabled
- api-gwv2- authorization-type-configured
- api-gw-associated-with-WAF
- api-gw-cache-enabled-und-verschlüsselt
- api-gw-endpoint-type-überprüfen
- api-gw-execution-logging-aktiviert
- api-gw-ssl-enabled
- api-gw-xray-enabled
- appconfig-application-description
- appconfig-application-tagged
- appconfig-configuration-profile-tagged
- appconfig-configuration-profile-validators-nicht leer
- appconfig-deployment-strategy-description

- appconfig-deployment-strategy-replicate-zu-ssm
- appconfig-environment-description
- appconfig-environment-tagged
- appconfig-extension-association-tagged
- appconfig-freeform-profile-config-Speicher
- appconfig-hosted-configuration-version-Beschreibung
- appflow-flow-tagged
- appintegrations-event-integration-description
- appintegrations-event-integration-tagged
- appmesh-gateway-route-tagged
- appmesh-mesh-deny-tcp-Weiterleitung
- appmesh-mesh-tagged
- appmesh-route-tagged
- appmesh-virtual-gateway-backend-Standardeinstellungen-TLS
- appmesh-virtual-gateway-logging-file-path-exists
- appmesh-virtual-gateway-tagged
- appmesh-virtual-node-backend-defaults-tls-on
- appmesh-virtual-node-logging-file-path-exists
- appmesh-virtual-node-tagged
- appmesh-virtual-router-tagged
- appmesh-virtual-service-tagged
- approved-amis-by-id
- approved-amis-by-tag
- apprunner-service-in-vpc
- apprunner-service-no-public-Zugang
- apprunner-service-observability-enabled
- apprunner-service-tagged
- apprunner-vpc-connector-tagged
- appstream-fleet-in-vpc
- appsync-associated-with-waf

- appsync-authorization-check
- appsync-cache-encryption-at-ausruhen
- appsync-logging-enabled
- athena-data-catalog-description
- athena-prepared-statement-description
- athena-workgroup-description
- athena-workgroup-encrypted-at-ausruhen
- athena-workgroup-enforce-workgroup-Konfiguration
- athena-workgroup-engine-version-automatisches Upgrade
- athena-workgroup-logging-enabled
- aurora-last-backup-recovery-Punkt erstellt
- aurora-meets-restore-time-Ziel
- aurora-mysql-backtracking-enabled
- aurora-mysql-cluster-audit-Protokollierung
- aurora-resources-in-logically-air-gapped-vault
- aurora-resources-protected-by-Backup-Plan
- autoscaling-capacity-rebalancing
- autoscaling-group-elb-healthcheck-erforderlich
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-hop-Grenze
- autoscaling-launch-config-public-ip-deaktiviert
- autoscaling-launch-template
- autoscaling-multiple-az
- autoscaling-multiple-instance-types
- backup-plan-min-frequency-and-min-retention-check
- backup-recovery-point-encrypted
- backup-recovery-point-manual-Löschen-deaktiviert
- backup-recovery-point-minimum-Aufbewahrungsprüfung
- batch-compute-environment-enabled
- batch-compute-environment-managed

- batch-compute-environment-tagged
- batch-job-queue-enabled
- batch-job-queue-tagged
- batch-managed-compute-environment-using-launch-template
- batch-managed-compute-env-compute-resources-tagged
- batch-scheduling-policy-tagged
- beanstalk-enhanced-health-reporting-aktiviert
- cassandra-keyspace-tagged
- clb-desync-mode-check
- clb-multiple-az
- cloudformation-stack-drift-detection-überprüfen
- cloudformation-stack-notification-check
- cloudtrail-all-read-s3- data-event-check
- cloudtrail-all-write-s3- data-event-check
- Wolkenspur-S3- bucket-access-logging
- CloudTrail-S3- bucket-public-access-prohibited
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-action-enabled-überprüfen
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted
- cloud-trail-cloud-watch-logs-aktiviert
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-Validierung aktiviert
- cmk-backing-key-rotation-aktiviert
- codebuild-project-artifact-encryption
- codebuild-project-environment-privileged-überprüfen

- codebuild-project-envvar-awscred-überprüfen
- codebuild-project-logging-enabled
- codebuild-project-s3-log-verschlüsselt
- codebuild-project-source-repo-URL-Prüfung
- codebuild-report-group-encrypted-im Ruhezustand
- codedeploy-auto-rollback-monitor-aktiviert
- codedeploy-deployment-group-auto-rollback-aktiviert
- codedeploy-deployment-group-outdated-instanzen-aktualisieren
- Codedeploy-ec2- minimum-healthy-hosts-configured
- codedeploy-lambda-allatonce-traffic-shift-deaktiviert
- codeguruprofiler-profiling-group-tagged
- codegururevieweer-repository-association-tagged
- codepipeline-deployment-count-check
- codepipeline-region-fanout-check
- cognito-identity-pool-unauth-Zugriffsprüfung
- cognito-user-pool-advanced-sicherheitsaktiviert
- cognito-user-pool-tagged
- connect-instance-logging-enabled
- customerprofiles-object-type-allow-Profilerstellung
- customerprofiles-object-type-tagged
- custom-eventbus-policy-attached
- custom-schema-registry-policy-beigefügt
- cw-loggroup-retention-period-überprüfen
- datasync-task-data-verification-aktiviert
- datasync-task-logging-enabled
- datasync-task-tagged
- dax-encryption-enabled
- dax-tls-endpoint-encryption
- db-instance-backup-enabled
- desired-instance-tenancy

- desired-instance-type
- dms-auto-minor-version-aktualisieren-Prüfung
- dms-endpoint-ssl-configured
- dms-endpoint-tagged
- dms-mongo-db-authentication-aktiviert
- dms-neptune-iam-authorization-aktiviert
- dms-redis-tls-enabled
- dms-replication-not-public
- dms-replication-task-sourcedb-Protokollierung
- dms-replication-task-tagged
- dms-replication-task-targetdb-Protokollierung
- docdb-cluster-audit-logging-aktiviert
- docdb-cluster-backup-retention-überprüfen
- docdb-cluster-deletion-protection-aktiviert
- docdb-cluster-encrypted
- docdb-cluster-encrypted-in-Transit
- docdb-cluster-snapshot-public-verboten
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-last-backup-recovery-Punkt erstellt
- dynamodb-meets-restore-time-Ziel
- dynamodb-pitr-enabled
- dynamodb-resources-protected-by-Backup-Plan
- dynamodb-table-deletion-protection-aktiviert
- dynamodb-table-encrypted-kms
- dynamodb-table-encryption-enabled
- dynamodb-throughput-limit-check
- ebs-in-backup-plan
- ebs-last-backup-recovery-punkt-erstellt
- ebs-meets-restore-time-Ziel

- ebs-optimized-instance
- ebs-resources-in-logically-air-gapped-vault
- ebs-resources-protected-by-Backup-Plan
- ebs-snapshot-public-restorable-überprüfen
- ec2- capacity-reservation-tagged
- ec2- aktiviert client-vpn-connection-log
- ec2- client-vpn-endpoint-tagged
- ec2- -alle client-vpn-not-authorize
- ec2- dhcp-options-tagged
- ec2- ebs-encryption-by-default
- ec2- aktiviert enis-source-destination-check
- ec2-fleet-markiert
- ec2-imdsv2-check
- ec2- instance-detailed-monitoring-enabled
- ec2-ami instance-launched-with-allowed
- ec2- instance-managed-by-ssm
- ec2- instance-multiple-eni-check
- ec2- instance-no-public-ip
- ec2- instance-profile-attached
- ec2- erstellt last-backup-recovery-point
- ec2-2-prüfen launch-template-imdsv
- ec2- -deaktiviert launch-template-public-ip
- ec2- launch-template-tagged
- ec2- managedinstance-applications-blacklisted
- ec2- managedinstance-applications-required
- ec2- prüfen managedinstance-association-compliance-status
- ec2- managedinstance-inventory-blacklisted
- ec2- prüfen managedinstance-patch-compliance-status
- ec2- managedinstance-platform-check
- ec2- meets-restore-time-target

- ec2- Analyse mit Schlagwörtern network-insights-access-scope
- ec2 network-insights-access-scope - markiert
- ec2- network-insights-path-tagged
- ec2- no-amazon-key-pair
- ec2- paravirtual-instance-check
- ec2- prefix-list-tagged
- ec2- -Tresor mit Lücken resources-in-logically-air
- ec2- resources-protected-by-backup -plan
- ec2- -eni security-group-attached-to
- ec2- -eni-periodisch security-group-attached-to
- ec2-stopped-instance
- ec2- token-hop-limit-check
- ec2- traffic-mirror-filter-description
- ec2- traffic-mirror-filter-tagged
- ec2- traffic-mirror-session-description
- ec2- traffic-mirror-session-tagged
- ec2- traffic-mirror-target-description
- ec2- traffic-mirror-target-tagged
- ec2- -attach-deaktiviert transit-gateway-auto-vpc
- ec2 transit-gateway-multicast-domain - markiert
- ec2- volume-inuse-check
- ec2- vpn-connection-logging-enabled
- ecr-private-image-scanning-aktiviert
- ecr-private-lifecycle-policy-konfiguriert
- ecr-private-tag-immutability-aktiviert
- ecr-repository-cmk-encryption-aktiviert
- ecr-repository-tagged
- ecs-awsvpc-networking-enabled
- ecs-containers-nonprivileged
- ecs-containers-readonly-access

- ecs-container-insights-enabled
- ecs-fargate-latest-platform-Version
- ecs-no-environment-secrets
- ecs-task-definition-log-Konfiguration
- ecs-task-definition-memory-hartes Limit
- ecs-task-definition-network-mode-not-host
- ecs-task-definition-nonroot-Benutzer
- ecs-task-definition-pid-Modus-Check
- ecs-task-definition-user-for-host-mode-check
- efs-access-point-enforce-Stammverzeichnis
- efs-access-point-enforce-Benutzeridentität
- efs-automatic-backups-enabled
- efs-encrypted-check
- efs-filesystem-ct-encrypted
- efs-in-backup-plan
- efs-last-backup-recovery-Punkt erstellt
- efs-meets-restore-time-Ziel
- efs-mount-target-public-zugänglich
- efs-resources-in-logically-air-gapped-vault
- efs-resources-protected-by-Ersatzplan
- eip-attached
- eks-cluster-logging-enabled
- eks-cluster-log-enabled
- eks-cluster-oldest-supported-Ausführung
- eks-cluster-secrets-encrypted
- eks-cluster-supported-version
- eks-endpoint-no-public-Zugang
- eks-secrets-encrypted
- elasticache-auto-minor-version-aktualisieren-Prüfung
- elasticache-rbac-auth-enabled

- elasticache-redis-cluster-automatic-Backup-Check
- elasticache-repl-grp-auto-failover-fähig
- elasticache-repl-grp-encrypted-im Ruhezustand
- elasticache-repl-grp-encryptedim Transit
- elasticache-repl-grp-redis-auth-aktiviert
- elasticache-subnet-group-check
- elasticache-supported-engine-version
- elasticbeanstalk-application-description
- elasticbeanstalk-application-version-description
- elasticbeanstalk-environment-description
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch
- elasticsearch-node-to-node-Verschlüsselungsprüfung
- elastic-beanstalk-logs-to- Cloudwatch
- elastic-beanstalk-managed-updates-aktiviert
- elbv2- acm-certificate-required
- elv 2- listener-encryption-in-transit
- elbv2-multiple-az
- elbv2- prüfen predefined-security-policy-ssl
- elb-acm-certificate-required
- elb-cross-zone-load-Balancing aktiviert
- elb-custom-security-policy-ssl-Prüfung
- elb-deletion-protection-enabled
- elb-logging-enabled
- elb-predefined-security-policy-ssl-Überprüfung
- elb-tls-https-listeners-nur
- emr-block-public-access
- emr-kerberos-enabled
- emr-master-no-public-ip

- emr-security-configuration-encryption-ruh dich aus
- emr-security-configuration-encryption-Transit
- encrypted-volumes
- event-data-store-cmk-Verschlüsselung aktiviert
- evidently-launch-description
- evidently-launch-tagged
- evidently-project-description
- evidently-project-tagged
- evidently-segment-description
- evidently-segment-tagged
- fis-experiment-template-log-Konfiguration ist vorhanden
- fis-experiment-template-tagged
- fms-shield-resource-policy-überprüfen
- fms-webacl-resource-policy-überprüfen
- fms-webacl-rulegroup-association-überprüfen
- frauddetector-entity-type-tagged
- frauddetector-label-tagged
- frauddetector-outcome-tagged
- frauddetector-variable-tagged
- fsx-last-backup-recovery-Punkt erstellt
- fsx-lustre-copy-tagszu Backups
- fsx-meets-restore-time-Ziel
- fsx-ontap-deployment-type-überprüfen
- fsx-openzfs-copy-tags-aktiviert
- fsx-openzfs-deployment-type-überprüfen
- fsx-resources-protected-by-Ersatzplan
- fsx-windows-audit-log-konfiguriert
- fsx-windows-deployment-type-überprüfen
- glb-listener-tagged
- global-endpoint-event-replication-aktiviert

- glue-job-logging-enabled
- glue-ml-transform-encrypted-im Ruhezustand
- glue-spark-job-supported-Ausführung
- GuardDuty-EC2- protection-runtime-enabled
- guardduty-ecs-protection-runtime-aktiviert
- guardduty-eks-protection-audit-aktiviert
- guardduty-eks-protection-runtime-aktiviert
- guardduty-enabled-centralized
- guardduty-lambda-protection-enabled
- guardduty-malware-protection-enabled
- guardduty-non-archived-findings
- guardduty-rds-protection-enabled
- guardduty-runtime-monitoring-enabled
- GuardDuty-S3-Schutz aktiviert
- iam-customer-policy-blocked-kms-Aktionen
- iam-external-access-analyzer-aktiviert
- iam-group-has-users-überprüfen
- iam-inline-policy-blocked-KMS-Aktionen
- iam-no-inline-policy-überprüfen
- iam-password-policy
- iam-policy-blacklisted-check
- iam-policy-in-use
- iam-policy-no-statements-with-admin-access
- iam-policy-no-statements-with-full-access
- iam-role-managed-policy-überprüfen
- iam-root-access-key-überprüfen
- iam-user-group-membership-überprüfen
- iam-user-mfa-enabled
- iam-user-no-policies-überprüfen
- iam-user-unused-credentials-überprüfen

- incoming-ssh-disabled
- inspector-ec2-Scan aktiviert
- inspector-ecr-scan-enabled
- inspector-lambda-code-scan-aktiviert
- inspector-lambda-standard-scan-aktiviert
- instances-in-vpc
- internet-gateway-authorized-vpc-nur
- iotevents-alarm-model-tagged
- iotevents-detector-model-tagged
- iotevents-input-tagged
- iotsitewise-asset-model-tagged
- iotsitewise-dashboard-tagged
- iotsitewise-gateway-tagged
- iotsitewise-portal-tagged
- iotsitewise-project-tagged
- iottwinmaker-component-type-tagged
- iottwinmaker-entity-tagged
- iottwinmaker-scene-tagged
- iottwinmaker-sync-job-tagged
- iottwinmaker-workspace-tagged
- iot-authorizer-token-signing-aktiviert
- kinesis-firehose-delivery-stream-verschlüsselt
- kinesis-stream-backup-retention-überprüfen
- kinesis-stream-encrypted
- kms-cmk-not-scheduled-zum Löschen
- kms-key-policy-no-öffentlicher Zugang
- lambda-concurrency-check
- lambda-dlq-check
- lambda-function-public-access-verboten
- lambda-function-settings-check

- lambda-function-xray-enabled
- lambda-inside-vpc
- lambda-vpc-multi-az-überprüfen
- lightsail-bucket-tagged
- lightsail-certificate-tagged
- lightsail-disk-tagged
- macie-auto-sensitive-data-Discovery-Check
- macie-status-check
- mariadb-publish-logs-to-Cloudwatch-Protokolle
- mfa-enabled-for-iam-Konsolenzugriff
- mq-active-broker-ldap-Authentifizierung
- mq-active-deployment-mode
- mq-active-single-instance-broker-storage-type-efs
- mq-automatic-minor-version-Upgrade aktiviert
- mq-auto-minor-version-upgrade-fähig
- mq-broker-general-logging-aktiviert
- mq-cloudwatch-audit-logging-aktiviert
- mq-cloudwatch-audit-log-aktiviert
- mq-no-public-access
- mq-rabbit-deployment-mode
- msk-cluster-public-access-deaktiviert
- msk-connect-connector-logging-aktiviert
- msk-enhanced-monitoring-enabled
- msk-in-cluster-node-require-tls
- msk-unrestricted-access-check
- multi-region-cloud-trail-aktiviert
- nacl-no-unrestricted-ssh-rdp
- neptune-cluster-backup-retention-überprüfen
- neptune-cluster-cloudwatch-log-exportfähig
- neptune-cluster-copy-tags-to-snapshot-enabled

- neptune-cluster-deletion-protection-aktiviert
- neptune-cluster-encrypted
- neptune-cluster-iam-database-Authentifizierung
- neptune-cluster-multi-az-aktiviert
- neptune-cluster-snapshot-encrypted
- neptune-cluster-snapshot-public-verboten
- netfw-deletion-protection-enabled
- netfw-logging-enabled
- netfw-multi-az-enabled
- netfw-policy-default-action-fragment-Pakete
- netfw-policy-default-action-vollständige Pakete
- netfw-policy-rule-group-assoziiert
- netfw-stateless-rule-group-nicht leer
- netfw-subnet-change-protection-aktiviert
- nlb-cross-zone-load-Balancing aktiviert
- nlb-internal-scheme-check
- nlb-listener-tagged
- nlb-logging-enabled
- no-unrestricted-route-to-igw
- opensearch-access-control-enabled
- opensearch-audit-logging-enabled
- opensearch-data-node-fault-Toleranz
- opensearch-encrypted-at-rest
- opensearch-https-required
- opensearch-in-vpc-only
- opensearch-logs-to-cloudwatch
- opensearch-node-to-node-Verschlüsselungsprüfung
- opensearch-primary-node-fault-Toleranz
- opensearch-update-check
- rabbit-mq-supported-version

- rds-aurora-mysql-audit-Protokollierung aktiviert
- rds-aurora-postgresql-logs-zu-Cloud-Watch
- rds-automatic-minor-version-upgrade-fähig
- rds-cluster-auto-minor-version-upgrade-enable
- rds-cluster-default-admin-überprüfen
- rds-cluster-deletion-protection-aktiviert
- rds-cluster-encrypted-at-ausruhen
- rds-cluster-iam-authentication-aktiviert
- rds-cluster-multi-az-aktiviert
- rds-db-security-group-nicht erlaubt
- rds-enhanced-monitoring-enabled
- rds-instance-default-admin-überprüfen
- rds-instance-deletion-protection-aktiviert
- rds-instance-iam-authentication-aktiviert
- rds-instance-public-access-überprüfen
- rds-instance-subnet-igw-überprüfen
- rds-in-backup-plan
- rds-last-backup-recovery-Punkt erstellt
- rds-logging-enabled
- rds-mariadb-instance-encryptedim Transit
- rds-meets-restore-time-Ziel
- rds-multi-az-support
- rds-mysql-instance-encryptedunterwegs
- rds-postgresql-logs-to- Cloudwatch
- rds-postgres-instance-encryptedunterwegs
- rds-proxy-tls-encryption
- rds-resources-protected-by-Ersatzplan
- rds-snapshots-public-prohibited
- rds-snapshot-encrypted
- rds-sqlserver-encrypted-in-Transit

- rds-sql-server-logszur Cloud-Überwachung
- rds-storage-encrypted
- redshift-audit-logging-enabled
- redshift-backup-enabled
- redshift-cluster-configuration-check
- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check
- redshift-cluster-multi-az-aktiviert
- redshift-cluster-parameter-group-markiert
- redshift-cluster-public-access-überprüfen
- redshift-cluster-subnet-group-Multi-Az
- redshift-default-admin-check
- redshift-default-db-name-überprüfen
- redshift-enhanced-vpc-routing-aktiviert
- redshift-require-tls-ssl
- redshift-serverless-default-admin-überprüfen
- redshift-serverless-default-db-Namenscheck
- redshift-serverless-namespace-cmk-Verschlüsselung
- redshift-serverless-publish-logs-zu-Cloud-Watch
- redshift-serverless-workgroup-encryptedauf dem Weg
- redshift-serverless-workgroup-no-öffentlich zugänglich
- redshift-serverless-workgroup-routes-innerhalb von VPC
- redshift-unrestricted-port-access
- required-tags
- restricted-incoming-traffic
- root-account-hardware-mfa-aktiviert
- root-account-mfa-enabled
- nur s3- access-point-in-vpc
- s3- -Blöcke access-point-public-access
- s3- -Blöcke account-level-public-access

- s3- -Blocke-periodisch account-level-public-access
- s 3- bucket-acl-prohibited
- s-3 bucket-blacklisted-actions-prohibited
- s3- bucket-cross-region-replication -aktiviert
- s-3 bucket-default-lock-enabled
- s3 bucket-level-public-access - verboten
- s3- bucket-logging-enabled
- s-3 bucket-mfa-delete-enabled
- s-3 bucket-policy-grantee-check
- s3- bucket-policy-not-more -freizügig
- s 3- bucket-public-read-prohibited
- s-3 bucket-public-write-prohibited
- s-3 bucket-replication-enabled
- s3- bucket-server-side-encryption -aktiviert
- s-3 bucket-ssl-requests-only
- s3-Bucket-Tagged
- s-3 bucket-versioning-enabled
- s-3 default-encryption-kms
- s-3 event-notifications-enabled
- s3 last-backup-recovery-point - erstellt
- s3- lifecycle-policy-check
- s-3 meets-restore-time-target
- s3- resources-in-logically-air -Tresor mit Lücken
- s3 resources-protected-by-backup - -Plan
- s 3- version-lifecycle-policy-check
- sagemaker-app-image-config-markiert
- sagemaker-domain-in-vpc
- sagemaker-domain-tagged
- sagemaker-endpoint-configuration-kms-schlüsselkonfiguriert
- sagemaker-endpoint-config-prod-Anzahl der Instanzen

- sagemaker-feature-group-tagged
- sagemaker-image-description
- sagemaker-image-tagged
- sagemaker-model-in-vpc
- sagemaker-model-isolation-enabled
- sagemaker-notebook-instance-inside-vpc
- sagemaker-notebook-instance-kms-key-konfiguriert
- sagemaker-notebook-instance-platform-Version
- sagemaker-notebook-instance-root-Zugriffsprüfung
- sagemaker-notebook-no-direct-Internetzugang
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-überprüfen
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- securityhub-enabled
- security-account-information-provided
- service-catalog-shared-within-Organisation
- service-vpc-endpoint-enabled
- sns-encrypted-kms
- sns-topic-message-delivery-Benachrichtigung aktiviert
- sns-topic-no-public-Zugriff
- sqs-queue-no-public-Zugang
- ssm-automation-block-public-teilen
- ssm-automation-logging-enabled
- ssm-document-not-public
- ssm-document-tagged
- step-functions-state-machine-Protokollierung aktiviert
- storagegateway-last-backup-recovery-punkt-erstellt
- storagegateway-resources-in-logically-air-gapped-vault

- storagegateway-resources-protected-by-Ersatzplan
- subnet-auto-assign-public-ip-deaktiviert
- transfer-agreement-description
- transfer-agreement-tagged
- transfer-certificate-description
- transfer-certificate-tagged
- transfer-connector-logging-enabled
- transfer-connector-tagged
- transfer-family-server-no-ftp
- transfer-profile-tagged
- transfer-workflow-description
- transfer-workflow-tagged
- virtualmachine-last-backup-recovery-Punkt erstellt
- virtualmachine-resources-in-logically-air-gapped-vault
- virtualmachine-resources-protected-by-Ersatzplan
- vpc-default-security-group-geschlossen
- vpc-endpoint-enabled
- vpc-flow-logs-enabled
- vpc-network-acl-unused-überprüfen
- vpc-peering-dns-resolution-überprüfen
- vpc-sg-open-only-to-authorized-ports
- vpc-sg-port-restriction-überprüfen
- vpc-vpn-2-tunnels-up
- wafv2-logging-enabled
- WAF 2- rulegroup-logging-enabled
- WAF 2- rulegroup-not-empty
- WAF 2- webacl-not-empty
- waf-regional-rulegroup-not-leer
- waf-regional-rule-not-leer
- waf-regional-webacl-not-leer

- workspaces-root-volume-encryption-aktiviert
- workspaces-user-volume-encryption-aktiviert

Region Asien-Pazifik (Sydney)

Asien-Pazifik (Sydney)

- access-keys-rotated
- account-part-of-organizations
- acmpca-certificate-authority-tagged
- acm-certificate-expiration-check
- acm-certificate-rsa-check
- acm-pca-root-ca-deaktiviert
- active-mq-supported-version
- alb-desync-mode-check
- alb-http-drop-invalid-Header-fähig
- alb-http-to-https-Umleitungsprüfung
- alb-internal-scheme-check
- alb-listener-tagged
- alb-waf-enabled
- amplify-app-branch-auto-löschung aktiviert
- amplify-app-description
- amplify-app-tagged
- amplify-branch-performance-mode-aktiviert
- amplify-branch-tagged
- api-gwv2- access-logs-enabled
- api-gwv2- authorization-type-configured
- api-gw-associated-with-WAF
- api-gw-cache-enabled-und-verschlüsselt
- api-gw-endpoint-type-überprüfen
- api-gw-execution-logging-aktiviert

- api-gw-ssl-enabled
- api-gw-xray-enabled
- appconfig-application-description
- appconfig-application-tagged
- appconfig-configuration-profile-tagged
- appconfig-configuration-profile-validators-nicht leer
- appconfig-deployment-strategy-description
- appconfig-deployment-strategy-replicate-zu-ssm
- appconfig-environment-description
- appconfig-environment-tagged
- appconfig-extension-association-tagged
- appconfig-freeform-profile-config-Speicher
- appconfig-hosted-configuration-version-Beschreibung
- appflow-flow-tagged
- appintegrations-event-integration-description
- appintegrations-event-integration-tagged
- appmesh-gateway-route-tagged
- appmesh-mesh-deny-tcp-Weiterleitung
- appmesh-mesh-tagged
- appmesh-route-tagged
- appmesh-virtual-gateway-backend-Standardeinstellungen-TLS
- appmesh-virtual-gateway-logging-file-path-exists
- appmesh-virtual-gateway-tagged
- appmesh-virtual-node-backend-defaults-tls-on
- appmesh-virtual-node-logging-file-path-exists
- appmesh-virtual-node-tagged
- appmesh-virtual-router-tagged
- appmesh-virtual-service-tagged
- approved-amis-by-id
- approved-amis-by-tag

- apprunner-service-in-vpc
- apprunner-service-no-public-Zugang
- apprunner-service-observability-enabled
- apprunner-service-tagged
- apprunner-vpc-connector-tagged
- appstream-fleet-in-vpc
- appsync-associated-with-waf
- appsync-authorization-check
- appsync-cache-encryption-at-ausruhen
- appsync-logging-enabled
- athena-data-catalog-description
- athena-prepared-statement-description
- athena-workgroup-description
- athena-workgroup-encrypted-at-ausruhen
- athena-workgroup-enforce-workgroup-Konfiguration
- athena-workgroup-engine-version-automatisches Upgrade
- athena-workgroup-logging-enabled
- aurora-last-backup-recovery-Punkt erstellt
- aurora-meets-restore-time-Ziel
- aurora-mysql-backtracking-enabled
- aurora-mysql-cluster-audit-Protokollierung
- aurora-resources-in-logically-air-gapped-vault
- aurora-resources-protected-by-Backup-Plan
- autoscaling-capacity-rebalancing
- autoscaling-group-elb-healthcheck-erforderlich
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-hop-Grenze
- autoscaling-launch-config-public-ip-deaktiviert
- autoscaling-launch-template
- autoscaling-multiple-az

- autoscaling-multiple-instance-types
- backup-plan-min-frequency-and-min-retention-check
- backup-recovery-point-encrypted
- backup-recovery-point-manual-Löschen-deaktiviert
- backup-recovery-point-minimum-Aufbewahrungsprüfung
- batch-compute-environment-enabled
- batch-compute-environment-managed
- batch-compute-environment-tagged
- batch-job-queue-enabled
- batch-job-queue-tagged
- batch-managed-compute-environment-using-launch-template
- batch-managed-compute-env-compute-resources-tagged
- batch-scheduling-policy-tagged
- beanstalk-enhanced-health-reporting-aktiviert
- cassandra-keyspace-tagged
- clb-desync-mode-check
- clb-multiple-az
- cloudformation-stack-drift-detection-überprüfen
- cloudformation-stack-notification-check
- cloudtrail-all-read-s3- data-event-check
- cloudtrail-all-write-s3- data-event-check
- Wolkenspur-S3- bucket-access-logging
- CloudTrail-S3- bucket-public-access-prohibited
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-action-enabled-überprüfen
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted

- cloud-trail-cloud-watch-logs-aktiviert
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-Validierung aktiviert
- cmk-backing-key-rotation-aktiviert
- codebuild-project-artifact-encryption
- codebuild-project-environment-privileged-überprüfen
- codebuild-project-envvar-awscred-überprüfen
- codebuild-project-logging-enabled
- codebuild-project-s3-log-verschlüsselt
- codebuild-project-source-repo-URL-Prüfung
- codebuild-report-group-encrypted-im Ruhezustand
- codedeploy-auto-rollback-monitor-aktiviert
- codedeploy-deployment-group-auto-rollback-aktiviert
- codedeploy-deployment-group-outdated-instanzen-aktualisieren
- Codedeploy-ec2- minimum-healthy-hosts-configured
- codedeploy-lambda-allatonce-traffic-shift-deaktiviert
- codeguruprofiler-profiling-group-tagged
- codegururevieweer-repository-association-tagged
- codepipeline-deployment-count-check
- codepipeline-region-fanout-check
- cognito-identity-pool-unauth-Zugriffsprüfung
- cognito-user-pool-advanced-sicherheitsaktiviert
- cognito-user-pool-tagged
- connect-instance-logging-enabled
- customerprofiles-object-type-allow-Profilerstellung
- customerprofiles-object-type-tagged
- custom-eventbus-policy-attached
- custom-schema-registry-policy-beigefügt
- cw-loggroup-retention-period-überprüfen

- datasync-task-data-verification-aktiviert
- datasync-task-logging-enabled
- datasync-task-tagged
- dax-encryption-enabled
- dax-tls-endpoint-encryption
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- dms-auto-minor-version-aktualisieren-Prüfung
- dms-endpoint-ssl-configured
- dms-endpoint-tagged
- dms-mongo-db-authentication-aktiviert
- dms-neptune-iam-authorization-aktiviert
- dms-redis-tls-enabled
- dms-replication-not-public
- dms-replication-task-sourcedb-Protokollierung
- dms-replication-task-tagged
- dms-replication-task-targetdb-Protokollierung
- docdb-cluster-audit-logging-aktiviert
- docdb-cluster-backup-retention-überprüfen
- docdb-cluster-deletion-protection-aktiviert
- docdb-cluster-encrypted
- docdb-cluster-encrypted-in-Transit
- docdb-cluster-snapshot-public-verboten
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-last-backup-recovery-Punkt erstellt
- dynamodb-meets-restore-time-Ziel
- dynamodb-pitr-enabled
- dynamodb-resources-protected-by-Backup-Plan

- dynamodb-table-deletion-protection-aktiviert
- dynamodb-table-encrypted-kms
- dynamodb-table-encryption-enabled
- dynamodb-throughput-limit-check
- ebs-in-backup-plan
- ebs-last-backup-recovery-punkt-erstellt
- ebs-meets-restore-time-Ziel
- ebs-optimized-instance
- ebs-resources-in-logically-air-gapped-vault
- ebs-resources-protected-by-Backup-Plan
- ebs-snapshot-public-restorable-überprüfen
- ec2- capacity-reservation-tagged
- ec2- carrier-gateway-tagged
- ec2- aktiviert client-vpn-connection-log
- ec2- client-vpn-endpoint-tagged
- ec2- -alle client-vpn-not-authorize
- ec2- dhcp-options-tagged
- ec2- ebs-encryption-by-default
- ec2- aktiviert enis-source-destination-check
- ec2-fleet-markiert
- ec2-imdsv2-check
- ec2- instance-detailed-monitoring-enabled
- ec2-ami instance-launched-with-allowed
- ec2- instance-managed-by-ssm
- ec2- instance-multiple-eni-check
- ec2- instance-no-public-ip
- ec2- instance-profile-attached
- ec2- erstellt last-backup-recovery-point
- ec2-2-prüfen launch-template-imdsv
- ec2- -deaktiviert launch-template-public-ip

- ec2- launch-template-tagged
- ec2- managedinstance-applications-blacklisted
- ec2- managedinstance-applications-required
- ec2- prüfen managedinstance-association-compliance-status
- ec2- managedinstance-inventory-blacklisted
- ec2- prüfen managedinstance-patch-compliance-status
- ec2- managedinstance-platform-check
- ec2- meets-restore-time-target
- ec2- Analyse mit Schlagwörtern network-insights-access-scope
- ec2 network-insights-access-scope - markiert
- ec2- network-insights-path-tagged
- ec2- no-amazon-key-pair
- ec2- paravirtual-instance-check
- ec2- prefix-list-tagged
- ec2- -Tresor mit Lücken resources-in-logically-air
- ec2- resources-protected-by-backup -plan
- ec2- -eni security-group-attached-to
- ec2- -eni-periodisch security-group-attached-to
- ec2-stopped-instance
- ec2- token-hop-limit-check
- ec2- traffic-mirror-filter-description
- ec2- traffic-mirror-filter-tagged
- ec2- traffic-mirror-session-description
- ec2- traffic-mirror-session-tagged
- ec2- traffic-mirror-target-description
- ec2- traffic-mirror-target-tagged
- ec2- -attach-deaktiviert transit-gateway-auto-vpc
- ec2 transit-gateway-multicast-domain - markiert
- ec2- volume-inuse-check
- ec2- vpn-connection-logging-enabled

- ecr-private-image-scanning-aktiviert
- ecr-private-lifecycle-policy-konfiguriert
- ecr-private-tag-immutability-aktiviert
- ecr-repository-cmk-encryption-aktiviert
- ecr-repository-tagged
- ecs-awsvpc-networking-enabled
- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-container-insights-enabled
- ecs-fargate-latest-platform-Version
- ecs-no-environment-secrets
- ecs-task-definition-log-Konfiguration
- ecs-task-definition-memory-hartes Limit
- ecs-task-definition-network-mode-not-host
- ecs-task-definition-nonroot-Benutzer
- ecs-task-definition-pid-Modus-Check
- ecs-task-definition-user-for-host-mode-check
- efs-access-point-enforce-Stammverzeichnis
- efs-access-point-enforce-Benutzeridentität
- efs-automatic-backups-enabled
- efs-encrypted-check
- efs-filesystem-ct-encrypted
- efs-in-backup-plan
- efs-last-backup-recovery-Punkt erstellt
- efs-meets-restore-time-Ziel
- efs-mount-target-public-zugänglich
- efs-resources-in-logically-air-gapped-vault
- efs-resources-protected-by-Ersatzplan
- eip-attached
- eks-cluster-logging-enabled

- eks-cluster-log-enabled
- eks-cluster-oldest-supported-Ausführung
- eks-cluster-secrets-encrypted
- eks-cluster-supported-version
- eks-endpoint-no-public-Zugang
- eks-secrets-encrypted
- elasticache-auto-minor-version-aktualisieren-Prüfung
- elasticache-rbac-auth-enabled
- elasticache-redis-cluster-automatic-Backup-Check
- elasticache-repl-grp-auto-failover-fähig
- elasticache-repl-grp-encrypted-im Ruhezustand
- elasticache-repl-grp-encryptedim Transit
- elasticache-repl-grp-redis-auth-aktiviert
- elasticache-subnet-group-check
- elasticache-supported-engine-version
- elasticbeanstalk-application-description
- elasticbeanstalk-application-version-description
- elasticbeanstalk-environment-description
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch
- elasticsearch-node-to-node-Verschlüsselungsprüfung
- elastic-beanstalk-logs-to- Cloudwatch
- elastic-beanstalk-managed-updates-aktiviert
- elbv2- acm-certificate-required
- elv 2- listener-encryption-in-transit
- elbv2-multiple-az
- elbv2- prüfen predefined-security-policy-ssl
- elb-acm-certificate-required
- elb-cross-zone-load-Balancing aktiviert

- elb-custom-security-policy-ssl-Prüfung
- elb-deletion-protection-enabled
- elb-logging-enabled
- elb-predefined-security-policy-ssl-Überprüfung
- elb-tls-https-listeners-nur
- emr-block-public-access
- emr-kerberos-enabled
- emr-master-no-public-ip
- emr-security-configuration-encryption-ruh dich aus
- emr-security-configuration-encryption-Transit
- encrypted-volumes
- event-data-store-cmk-Verschlüsselung aktiviert
- evidently-launch-description
- evidently-launch-tagged
- evidently-project-description
- evidently-project-tagged
- evidently-segment-description
- evidently-segment-tagged
- fis-experiment-template-log-Konfiguration ist vorhanden
- fis-experiment-template-tagged
- fms-shield-resource-policy-überprüfen
- fms-webacl-resource-policy-überprüfen
- fms-webacl-rulegroup-association-überprüfen
- frauddetector-entity-type-tagged
- frauddetector-label-tagged
- frauddetector-outcome-tagged
- frauddetector-variable-tagged
- fsx-last-backup-recovery-Punkt erstellt
- fsx-lustre-copy-tagszu Backups
- fsx-meets-restore-time-Ziel

- fsx-ontap-deployment-type-überprüfen
- fsx-openzfs-copy-tags-aktiviert
- fsx-openzfs-deployment-type-überprüfen
- fsx-resources-protected-by-Ersatzplan
- fsx-windows-audit-log-konfiguriert
- fsx-windows-deployment-type-überprüfen
- glb-listener-tagged
- global-endpoint-event-replication-aktiviert
- glue-job-logging-enabled
- glue-ml-transform-encrypted-im Ruhezustand
- glue-spark-job-supported-Ausführung
- GuardDuty-EC2- protection-runtime-enabled
- guardduty-ecs-protection-runtime-aktiviert
- guardduty-eks-protection-audit-aktiviert
- guardduty-eks-protection-runtime-aktiviert
- guardduty-enabled-centralized
- guardduty-lambda-protection-enabled
- guardduty-malware-protection-enabled
- guardduty-non-archived-findings
- guardduty-rds-protection-enabled
- guardduty-runtime-monitoring-enabled
- GuardDuty-S3-Schutz aktiviert
- iam-customer-policy-blocked-kms-Aktionen
- iam-external-access-analyzer-aktiviert
- iam-group-has-users-überprüfen
- iam-inline-policy-blocked-KMS-Aktionen
- iam-no-inline-policy-überprüfen
- iam-password-policy
- iam-policy-blacklisted-check
- iam-policy-in-use

- iam-policy-no-statements-with-admin-access
- iam-policy-no-statements-with-full-access
- iam-role-managed-policy-überprüfen
- iam-root-access-key-überprüfen
- iam-user-group-membership-überprüfen
- iam-user-mfa-enabled
- iam-user-no-policies-überprüfen
- iam-user-unused-credentials-überprüfen
- incoming-ssh-disabled
- inspector-ec2-Scan aktiviert
- inspector-ecr-scan-enabled
- inspector-lambda-code-scan-aktiviert
- inspector-lambda-standard-scan-aktiviert
- instances-in-vpc
- internet-gateway-authorized-vpc-nur
- iotevents-alarm-model-tagged
- iotevents-detector-model-tagged
- iotevents-input-tagged
- iotsitewise-asset-model-tagged
- iotsitewise-dashboard-tagged
- iotsitewise-gateway-tagged
- iotsitewise-portal-tagged
- iotsitewise-project-tagged
- iottwinmaker-component-type-tagged
- iottwinmaker-entity-tagged
- iottwinmaker-scene-tagged
- iottwinmaker-sync-job-tagged
- iottwinmaker-workspace-tagged
- iotwireless-fuota-task-tagged
- iotwireless-multicast-group-tagged

- iotwireless-service-profile-tagged
- iot-authorizer-token-signing-aktiviert
- kinesis-firehose-delivery-stream-verschlüsselt
- kinesis-stream-backup-retention-überprüfen
- kinesis-stream-encrypted
- kms-cmk-not-scheduled-zum Löschen
- kms-key-policy-no-öffentlicher Zugang
- lambda-concurrency-check
- lambda-dlq-check
- lambda-function-public-access-verboten
- lambda-function-settings-check
- lambda-function-xray-enabled
- lambda-inside-vpc
- lambda-vpc-multi-az-überprüfen
- lightsail-bucket-tagged
- lightsail-certificate-tagged
- lightsail-disk-tagged
- macie-auto-sensitive-data-Discovery-Check
- macie-status-check
- mariadb-publish-logs-to-Cloudwatch-Protokolle
- mfa-enabled-for-iam-Konsolenzugriff
- mq-active-broker-ldap-Authentifizierung
- mq-active-deployment-mode
- mq-active-single-instance-broker-storage-type-efs
- mq-automatic-minor-version-Upgrade aktiviert
- mq-auto-minor-version-upgrade-fähig
- mq-broker-general-logging-aktiviert
- mq-cloudwatch-audit-logging-aktiviert
- mq-cloudwatch-audit-log-aktiviert
- mq-no-public-access

- mq-rabbit-deployment-mode
- msk-cluster-public-access-deaktiviert
- msk-connect-connector-logging-aktiviert
- msk-enhanced-monitoring-enabled
- msk-in-cluster-node-require-tls
- msk-unrestricted-access-check
- multi-region-cloud-trail-aktiviert
- nacl-no-unrestricted-ssh-rdp
- neptune-cluster-backup-retention-überprüfen
- neptune-cluster-cloudwatch-log-exportfähig
- neptune-cluster-copy-tags-to-snapshot-enabled
- neptune-cluster-deletion-protection-aktiviert
- neptune-cluster-encrypted
- neptune-cluster-iam-database-Authentifizierung
- neptune-cluster-multi-az-aktiviert
- neptune-cluster-snapshot-encrypted
- neptune-cluster-snapshot-public-verboten
- netfw-deletion-protection-enabled
- netfw-logging-enabled
- netfw-multi-az-enabled
- netfw-policy-default-action-fragment-Pakete
- netfw-policy-default-action-vollständige Pakete
- netfw-policy-rule-group-assoziiert
- netfw-stateless-rule-group-nicht leer
- netfw-subnet-change-protection-aktiviert
- nlb-cross-zone-load-Balancing aktiviert
- nlb-internal-scheme-check
- nlb-listener-tagged
- nlb-logging-enabled
- no-unrestricted-route-to-igw

- opensearch-access-control-enabled
- opensearch-audit-logging-enabled
- opensearch-data-node-fault-Toleranz
- opensearch-encrypted-at-rest
- opensearch-https-required
- opensearch-in-vpc-only
- opensearch-logs-to-cloudwatch
- opensearch-node-to-node-Verschlüsselungsprüfung
- opensearch-primary-node-fault-Toleranz
- opensearch-update-check
- rabbit-mq-supported-version
- rds-aurora-mysql-audit-Protokollierung aktiviert
- rds-aurora-postgresql-logs-zu-Cloud-Watch
- rds-automatic-minor-version-upgrade-fähig
- rds-cluster-auto-minor-version-upgrade-enable
- rds-cluster-default-admin-überprüfen
- rds-cluster-deletion-protection-aktiviert
- rds-cluster-encrypted-at-ausruhen
- rds-cluster-iam-authentication-aktiviert
- rds-cluster-multi-az-aktiviert
- rds-db-security-group-nicht erlaubt
- rds-enhanced-monitoring-enabled
- rds-instance-default-admin-überprüfen
- rds-instance-deletion-protection-aktiviert
- rds-instance-iam-authentication-aktiviert
- rds-instance-public-access-überprüfen
- rds-instance-subnet-igw-überprüfen
- rds-in-backup-plan
- rds-last-backup-recovery-Punkt erstellt
- rds-logging-enabled

- rds-mariadb-instance-encryptedim Transit
- rds-meets-restore-time-Ziel
- rds-multi-az-support
- rds-mysql-instance-encryptedunterwegs
- rds-postgresql-logs-to- Cloudwatch
- rds-postgres-instance-encryptedunterwegs
- rds-proxy-tls-encryption
- rds-resources-protected-by-Ersatzplan
- rds-snapshots-public-prohibited
- rds-snapshot-encrypted
- rds-sqlserver-encrypted-in-Transit
- rds-sql-server-logszur Cloud-Überwachung
- rds-storage-encrypted
- redshift-audit-logging-enabled
- redshift-backup-enabled
- redshift-cluster-configuration-check
- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check
- redshift-cluster-multi-az-aktiviert
- redshift-cluster-parameter-group-markiert
- redshift-cluster-public-access-überprüfen
- redshift-cluster-subnet-group-Multi-Az
- redshift-default-admin-check
- redshift-default-db-name-überprüfen
- redshift-enhanced-vpc-routing-aktiviert
- redshift-require-tls-ssl
- redshift-serverless-default-admin-überprüfen
- redshift-serverless-default-db-Namenscheck
- redshift-serverless-namespace-cmk-Verschlüsselung
- redshift-serverless-publish-logs-zu-Cloud-Watch

- redshift-serverless-workgroup-encryptedauf dem Weg
- redshift-serverless-workgroup-no-öffentlich zugänglich
- redshift-serverless-workgroup-routes-innerhalb von VPC
- redshift-unrestricted-port-access
- required-tags
- restricted-incoming-traffic
- root-account-hardware-mfa-aktiviert
- root-account-mfa-enabled
- nur s3- access-point-in-vpc
- s3- -Blöcke access-point-public-access
- s3- -Blöcke account-level-public-access
- s3- -Blocke-periodisch account-level-public-access
- s 3- bucket-acl-prohibited
- s-3 bucket-blacklisted-actions-prohibited
- s3- bucket-cross-region-replication -aktiviert
- s-3 bucket-default-lock-enabled
- s3 bucket-level-public-access - verboten
- s3- bucket-logging-enabled
- s-3 bucket-mfa-delete-enabled
- s-3 bucket-policy-grantee-check
- s3- bucket-policy-not-more -freizügig
- s 3- bucket-public-read-prohibited
- s-3 bucket-public-write-prohibited
- s-3 bucket-replication-enabled
- s3- bucket-server-side-encryption -aktiviert
- s-3 bucket-ssl-requests-only
- s3-Bucket-Tagged
- s-3 bucket-versioning-enabled
- s-3 default-encryption-kms
- s-3 event-notifications-enabled

- s3 last-backup-recovery-point - erstellt
- s3- lifecycle-policy-check
- s-3 meets-restore-time-target
- s3- resources-in-logically-air -Tresor mit Lücken
- s3 resources-protected-by-backup - -Plan
- s 3- version-lifecycle-policy-check
- sagemaker-app-image-config-markiert
- sagemaker-domain-in-vpc
- sagemaker-domain-tagged
- sagemaker-endpoint-configuration-kms-schlüsselkonfiguriert
- sagemaker-endpoint-config-prod-Anzahl der Instanzen
- sagemaker-feature-group-tagged
- sagemaker-image-description
- sagemaker-image-tagged
- sagemaker-model-in-vpc
- sagemaker-model-isolation-enabled
- sagemaker-notebook-instance-inside-vpc
- sagemaker-notebook-instance-kms-key-konfiguriert
- sagemaker-notebook-instance-platform-Version
- sagemaker-notebook-instance-root-Zugriffsprüfung
- sagemaker-notebook-no-direct-Internetzugang
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-überprüfen
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- securityhub-enabled
- security-account-information-provided
- service-catalog-shared-within-Organisation
- service-vpc-endpoint-enabled

- sns-encrypted-kms
- sns-topic-message-delivery-Benachrichtigung aktiviert
- sns-topic-no-public-Zugriff
- sqs-queue-no-public-Zugang
- ssm-automation-block-public-teilen
- ssm-automation-logging-enabled
- ssm-document-not-public
- ssm-document-tagged
- step-functions-state-machine-Protokollierung aktiviert
- storagegateway-last-backup-recovery-punkt-erstellt
- storagegateway-resources-in-logically-air-gapped-vault
- storagegateway-resources-protected-by-Ersatzplan
- subnet-auto-assign-public-ip-deaktiviert
- transfer-agreement-description
- transfer-agreement-tagged
- transfer-certificate-description
- transfer-certificate-tagged
- transfer-connector-logging-enabled
- transfer-connector-tagged
- transfer-family-server-no-ftp
- transfer-profile-tagged
- transfer-workflow-description
- transfer-workflow-tagged
- virtualmachine-last-backup-recovery-Punkt erstellt
- virtualmachine-resources-in-logically-air-gapped-vault
- virtualmachine-resources-protected-by-Ersatzplan
- vpc-default-security-group-geschlossen
- vpc-endpoint-enabled
- vpc-flow-logs-enabled
- vpc-network-acl-unused-überprüfen

- vpc-peering-dns-resolution-überprüfen
- vpc-sg-open-only-to-authorized-ports
- vpc-sg-port-restriction-überprüfen
- vpc-vpn-2-tunnels-up
- wafv2-logging-enabled
- WAF 2- rulegroup-logging-enabled
- WAF 2- rulegroup-not-empty
- WAF 2- webacl-not-empty
- waf-regional-rulegroup-not-leer
- waf-regional-rule-not-leer
- waf-regional-webacl-not-leer
- workspaces-root-volume-encryption-aktiviert
- workspaces-user-volume-encryption-aktiviert

Region Asien-Pazifik (Taipeh)

Asien-Pazifik (Taipeh)

- acm-certificate-expiration-check
- alb-http-drop-invalid-Header-fähig
- alb-http-to-https-Umleitungsprüfung
- alb-waf-enabled
- approved-amis-by-id
- approved-amis-by-tag
- aurora-mysql-backtracking-enabled
- cloudformation-stack-drift-detection-überprüfen
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloud-trail-cloud-watch-logs-aktiviert
- cloud-trail-enabled

- cloud-trail-encryption-enabled
- cloud-trail-log-file-Validierung aktiviert
- cmk-backing-key-rotation-aktiviert
- cw-loggroup-retention-period-überprüfen
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- dynamodb-autoscaling-enabled
- dynamodb-pitr-enabled
- dynamodb-table-encryption-enabled
- ebs-snapshot-public-restorable-überprüfen
- ec2- ebs-encryption-by-default
- ec2-imdsv2-check
- ec2- instance-detailed-monitoring-enabled
- ec2- instance-multiple-eni-check
- ec2- instance-no-public-ip
- ec2-stopped-instance
- eip-attached
- elb-acm-certificate-required
- elb-cross-zone-load-Balancing aktiviert
- elb-deletion-protection-enabled
- elb-logging-enabled
- elb-predefined-security-policy-ssl-Prüfung
- elb-tls-https-listeners-nur
- encrypted-volumes
- incoming-ssh-disabled
- instances-in-vpc
- lambda-function-public-access-verboten
- lambda-function-settings-check
- lambda-inside-vpc

- multi-region-cloud-trail-aktiviert
- rds-automatic-minor-version-upgrade-fähig
- rds-cluster-deletion-protection-aktiviert
- rds-cluster-iam-authentication-aktiviert
- rds-cluster-multi-az-aktiviert
- rds-enhanced-monitoring-enabled
- rds-instance-deletion-protection-aktiviert
- rds-instance-iam-authentication-aktiviert
- rds-instance-public-access-überprüfen
- rds-logging-enabled
- rds-multi-az-support
- rds-snapshots-public-prohibited
- rds-snapshot-encrypted
- rds-storage-encrypted
- required-tags
- restricted-incoming-traffic
- s3- -Blocke-periodisch account-level-public-access
- s 3- bucket-blacklisted-actions-prohibited
- s-3 bucket-default-lock-enabled
- s3 bucket-level-public-access - verboten
- s3- bucket-logging-enabled
- s-3 bucket-public-read-prohibited
- s-3 bucket-public-write-prohibited
- s-3 bucket-replication-enabled
- s3- bucket-server-side-encryption -aktiviert
- s-3 bucket-ssl-requests-only
- s-3 bucket-versioning-enabled
- service-vpc-endpoint-enabled
- sns-encrypted-kms
- subnet-auto-assign-public-ip-deaktiviert

- vpc-default-security-group-geschlossen
- vpc-flow-logs-enabled
- vpc-network-acl-unused-überprüfen
- vpc-sg-open-only-to-authorized-ports
- vpc-vpn-2-tunnels-up

Region Asien-Pazifik (Thailand)

Asien-Pazifik (Thailand)

- account-part-of-organizations
- acm-certificate-expiration-check
- alb-http-drop-invalid-Header-fähig
- alb-http-to-https-Umleitungsprüfung
- alb-waf-enabled
- api-gw-associated-with-WAF
- api-gw-cache-enabled-und-verschlüsselt
- api-gw-endpoint-type-überprüfen
- api-gw-execution-logging-aktiviert
- api-gw-ssl-enabled
- api-gw-xray-enabled
- approved-amis-by-id
- approved-amis-by-tag
- aurora-mysql-backtracking-enabled
- autoscaling-group-elb-healthcheck-erforderlich
- autoscaling-launch-config-public-ip-deaktiviert
- cloudformation-stack-drift-detection-überprüfen
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check

- cloudwatch-log-group-encrypted
- cloud-trail-cloud-watch-logs-aktiviert
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-Validierung aktiviert
- cmk-backing-key-rotation-aktiviert
- cw-loggroup-retention-period-überprüfen
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- dms-replication-not-public
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-pitr-enabled
- dynamodb-table-encrypted-kms
- dynamodb-table-encryption-enabled
- dynamodb-throughput-limit-check
- ebs-in-backup-plan
- ebs-snapshot-public-restorable-überprüfen
- ec2- ebs-encryption-by-default
- ec2-imdsv2-check
- ec2- instance-detailed-monitoring-enabled
- ec2-ami instance-launched-with-allowed
- ec2- instance-managed-by-ssm
- ec2- instance-multiple-eni-check
- ec2- instance-no-public-ip
- ec2- instance-profile-attached
- ec2- managedinstance-applications-blacklisted
- ec2- managedinstance-applications-required
- ec2- managedinstance-inventory-blacklisted

- ec2- prüfen managedinstance-patch-compliance-status
- ec2- managedinstance-platform-check
- ec2-eni security-group-attached-to
- ec2-stopped-instance
- ec2- volume-inuse-check
- ecs-task-definition-user-for-host-mode-check
- efs-encrypted-check
- efs-in-backup-plan
- eip-attached
- eks-endpoint-no-public-Zugang
- eks-secrets-encrypted
- elasticache-redis-cluster-automatic-Backup-Check
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch
- elasticsearch-node-to-node-Verschlüsselungsprüfung
- elb-acm-certificate-required
- elb-cross-zone-load-Balancing aktiviert
- elb-custom-security-policy-ssl-Prüfung
- elb-deletion-protection-enabled
- elb-logging-enabled
- elb-predefined-security-policy-SSL-Überprüfung
- elb-tls-https-listeners-nur
- emr-kerberos-enabled
- emr-master-no-public-ip
- encrypted-volumes
- iam-password-policy
- incoming-ssh-disabled
- instances-in-vpc
- kms-cmk-not-scheduled-zum Löschen

- lambda-concurrency-check
- lambda-dlq-check
- lambda-function-public-access-verboten
- lambda-function-settings-check
- lambda-inside-vpc
- multi-region-cloud-trail-aktiviert
- no-unrestricted-route-to-igw
- rds-automatic-minor-version-Upgrade aktiviert
- rds-cluster-deletion-protection-aktiviert
- rds-cluster-iam-authentication-aktiviert
- rds-cluster-multi-az-aktiviert
- rds-enhanced-monitoring-enabled
- rds-instance-deletion-protection-aktiviert
- rds-instance-iam-authentication-aktiviert
- rds-instance-public-access-überprüfen
- rds-in-backup-plan
- rds-logging-enabled
- rds-multi-az-support
- rds-snapshots-public-prohibited
- rds-snapshot-encrypted
- rds-storage-encrypted
- required-tags
- restricted-incoming-traffic
- s3- -Blocke-periodisch account-level-public-access
- s 3- bucket-blacklisted-actions-prohibited
- s-3 bucket-default-lock-enabled
- s3 bucket-level-public-access - verboten
- s3- bucket-logging-enabled
- s-3 bucket-policy-grantee-check
- s3- bucket-policy-not-more -freizügig

- s 3- bucket-public-read-prohibited
- s-3 bucket-public-write-prohibited
- s-3 bucket-replication-enabled
- s3- bucket-server-side-encryption -aktiviert
- s-3 bucket-ssl-requests-only
- s-3 bucket-versioning-enabled
- s-3 default-encryption-kms
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-überprüfen
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- securityhub-enabled
- service-vpc-endpoint-enabled
- sns-encrypted-kms
- ssm-document-not-public
- subnet-auto-assign-public-ip-deaktiviert
- vpc-default-security-group-geschlossen
- vpc-flow-logs-enabled
- vpc-network-acl-unused-überprüfen
- vpc-sg-open-only-to-authorized-ports
- vpc-vpn-2-tunnels-up

Region Asien-Pazifik (Tokio)

Asien-Pazifik (Tokio)

- access-keys-rotated
- account-part-of-organizations
- acmpca-certificate-authority-tagged
- acm-certificate-expiration-check
- acm-certificate-rsa-check

- acm-pca-root-ca-deaktiviert
- active-mq-supported-version
- alb-desync-mode-check
- alb-http-drop-invalid-Header-fähig
- alb-http-to-https-Umleitungsprüfung
- alb-internal-scheme-check
- alb-listener-tagged
- alb-waf-enabled
- amplify-app-branch-auto-löschung aktiviert
- amplify-app-description
- amplify-app-tagged
- amplify-branch-performance-mode-aktiviert
- amplify-branch-tagged
- api-gwv2- access-logs-enabled
- api-gwv2- authorization-type-configured
- api-gw-associated-with-WAF
- api-gw-cache-enabled-und-verschlüsselt
- api-gw-endpoint-type-überprüfen
- api-gw-execution-logging-aktiviert
- api-gw-ssl-enabled
- api-gw-xray-enabled
- appconfig-application-description
- appconfig-application-tagged
- appconfig-configuration-profile-tagged
- appconfig-configuration-profile-validators-nicht leer
- appconfig-deployment-strategy-description
- appconfig-deployment-strategy-replicate-zu-ssm
- appconfig-environment-description
- appconfig-environment-tagged
- appconfig-extension-association-tagged

- appconfig-freeform-profile-config-Speicher
- appconfig-hosted-configuration-version-Beschreibung
- appflow-flow-tagged
- appintegrations-event-integration-description
- appintegrations-event-integration-tagged
- appmesh-gateway-route-tagged
- appmesh-mesh-deny-tcp-Weiterleitung
- appmesh-mesh-tagged
- appmesh-route-tagged
- appmesh-virtual-gateway-backend-Standardeinstellungen-TLS
- appmesh-virtual-gateway-logging-file-path-exists
- appmesh-virtual-gateway-tagged
- appmesh-virtual-node-backend-defaults-tls-on
- appmesh-virtual-node-logging-file-path-exists
- appmesh-virtual-node-tagged
- appmesh-virtual-router-tagged
- appmesh-virtual-service-tagged
- approved-amis-by-id
- approved-amis-by-tag
- apprunner-service-in-vpc
- apprunner-service-no-public-Zugang
- apprunner-service-observability-enabled
- apprunner-service-tagged
- apprunner-vpc-connector-tagged
- appstream-fleet-in-vpc
- appsync-associated-with-waf
- appsync-authorization-check
- appsync-cache-encryption-at-ausruhen
- appsync-logging-enabled
- athena-data-catalog-description

- athena-prepared-statement-description
- athena-workgroup-description
- athena-workgroup-encrypted-at-ausruhen
- athena-workgroup-enforce-workgroup-Konfiguration
- athena-workgroup-engine-version-automatisches Upgrade
- athena-workgroup-logging-enabled
- aurora-last-backup-recovery-Punkt erstellt
- aurora-meets-restore-time-Ziel
- aurora-mysql-backtracking-enabled
- aurora-mysql-cluster-audit-Protokollierung
- aurora-resources-in-logically-air-gapped-vault
- aurora-resources-protected-by-Backup-Plan
- autoscaling-capacity-rebalancing
- autoscaling-group-elb-healthcheck-erforderlich
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-hop-Grenze
- autoscaling-launch-config-public-ip-deaktiviert
- autoscaling-launch-template
- autoscaling-multiple-az
- autoscaling-multiple-instance-types
- backup-plan-min-frequency-and-min-retention-check
- backup-recovery-point-encrypted
- backup-recovery-point-manual-Löschen-deaktiviert
- backup-recovery-point-minimum-Aufbewahrungsprüfung
- batch-compute-environment-enabled
- batch-compute-environment-managed
- batch-compute-environment-tagged
- batch-job-queue-enabled
- batch-job-queue-tagged
- batch-managed-compute-environment-using-launch-template

- batch-managed-compute-env-compute-resources-tagged
- batch-scheduling-policy-tagged
- beanstalk-enhanced-health-reporting-aktiviert
- cassandra-keyspace-tagged
- clb-desync-mode-check
- clb-multiple-az
- cloudformation-stack-drift-detection-überprüfen
- cloudformation-stack-notification-check
- cloudtrail-all-read-s3- data-event-check
- cloudtrail-all-write-s3- data-event-check
- Wolkenspur-S3- bucket-access-logging
- CloudTrail-S3- bucket-public-access-prohibited
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-action-enabled-überprüfen
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted
- cloud-trail-cloud-watch-logs-aktiviert
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-Validierung aktiviert
- cmk-backing-key-rotation-aktiviert
- codebuild-project-artifact-encryption
- codebuild-project-environment-privileged-überprüfen
- codebuild-project-envvar-awscred-überprüfen
- codebuild-project-logging-enabled
- codebuild-project-s3-log-verschlüsselt
- codebuild-project-source-repo-URL-Prüfung

- codebuild-report-group-encrypted-im Ruhezustand
- codedeploy-auto-rollback-monitor-aktiviert
- codedeploy-deployment-group-auto-rollback-aktiviert
- codedeploy-deployment-group-outdated-instanzen-aktualisieren
- Codedeploy-ec2- minimum-healthy-hosts-configured
- codedeploy-lambda-allatonce-traffic-shift-deaktiviert
- codeguruprofiler-profiling-group-tagged
- codegururevieweer-repository-association-tagged
- codepipeline-deployment-count-check
- codepipeline-region-fanout-check
- cognito-identity-pool-unauth-Zugriffsprüfung
- cognito-user-pool-advanced-sicherheitsaktiviert
- cognito-user-pool-tagged
- connect-instance-logging-enabled
- customerprofiles-object-type-allow-Profilerstellung
- customerprofiles-object-type-tagged
- custom-eventbus-policy-attached
- custom-schema-registry-policy-beigefügt
- cw-loggroup-retention-period-überprüfen
- datasync-task-data-verification-aktiviert
- datasync-task-logging-enabled
- datasync-task-tagged
- dax-encryption-enabled
- dax-tls-endpoint-encryption
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- dms-auto-minor-version-aktualisieren-Prüfung
- dms-endpoint-ssl-configured
- dms-endpoint-tagged

- dms-mongo-db-authentication-aktiviert
- dms-neptune-iam-authorization-aktiviert
- dms-redis-tls-enabled
- dms-replication-not-public
- dms-replication-task-sourcedb-Protokollierung
- dms-replication-task-tagged
- dms-replication-task-targetdb-Protokollierung
- docdb-cluster-audit-logging-aktiviert
- docdb-cluster-backup-retention-überprüfen
- docdb-cluster-deletion-protection-aktiviert
- docdb-cluster-encrypted
- docdb-cluster-encrypted-in-transit
- docdb-cluster-snapshot-public-verboten
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-last-backup-recovery-Punkt erstellt
- dynamodb-meets-restore-time-Ziel
- dynamodb-pitr-enabled
- dynamodb-resources-protected-by-Backup-Plan
- dynamodb-table-deletion-protection-aktiviert
- dynamodb-table-encrypted-kms
- dynamodb-table-encryption-enabled
- dynamodb-throughput-limit-check
- ebs-in-backup-plan
- ebs-last-backup-recovery-punkt-erstellt
- ebs-meets-restore-time-Ziel
- ebs-optimized-instance
- ebs-resources-in-logically-air-gapped-vault
- ebs-resources-protected-by-Backup-Plan
- ebs-snapshot-public-restorable-überprüfen

- ec2- capacity-reservation-tagged
- ec2- carrier-gateway-tagged
- ec2- aktiviert client-vpn-connection-log
- ec2- client-vpn-endpoint-tagged
- ec2- -alle client-vpn-not-authorize
- ec2- dhcp-options-tagged
- ec2- ebs-encryption-by-default
- ec2- aktiviert enis-source-destination-check
- ec2-fleet-markiert
- ec2-imdsv2-check
- ec2- instance-detailed-monitoring-enabled
- ec2-ami instance-launched-with-allowed
- ec2- instance-managed-by-ssm
- ec2- instance-multiple-eni-check
- ec2- instance-no-public-ip
- ec2- instance-profile-attached
- ec2- erstellt last-backup-recovery-point
- ec2-2-prüfen launch-template-imdsv
- ec2- -deaktiviert launch-template-public-ip
- ec2- launch-template-tagged
- ec2- managedinstance-applications-blacklisted
- ec2- managedinstance-applications-required
- ec2- prüfen managedinstance-association-compliance-status
- ec2- managedinstance-inventory-blacklisted
- ec2- prüfen managedinstance-patch-compliance-status
- ec2- managedinstance-platform-check
- ec2- meets-restore-time-target
- ec2- Analyse mit Schlagwörtern network-insights-access-scope
- ec2 network-insights-access-scope - markiert
- ec2- network-insights-path-tagged

- ec2- no-amazon-key-pair
- ec2- paravirtual-instance-check
- ec2- prefix-list-tagged
- ec2- -Tresor mit Lücken resources-in-logically-air
- ec2- resources-protected-by-backup -plan
- ec2- -eni security-group-attached-to
- ec2- -eni-periodisch security-group-attached-to
- ec2-stopped-instance
- ec2- token-hop-limit-check
- ec2- traffic-mirror-filter-description
- ec2- traffic-mirror-filter-tagged
- ec2- traffic-mirror-session-description
- ec2- traffic-mirror-session-tagged
- ec2- traffic-mirror-target-description
- ec2- traffic-mirror-target-tagged
- ec2- -attach-deaktiviert transit-gateway-auto-vpc
- ec2 transit-gateway-multicast-domain - markiert
- ec2- volume-inuse-check
- ec2- vpn-connection-logging-enabled
- ecr-private-image-scanning-aktiviert
- ecr-private-lifecycle-policy-konfiguriert
- ecr-private-tag-immutability-aktiviert
- ecr-repository-cmk-encryption-aktiviert
- ecr-repository-tagged
- ecs-awsvpc-networking-enabled
- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-container-insights-enabled
- ecs-fargate-latest-platform-Version
- ecs-no-environment-secrets

- ecs-task-definition-log-Konfiguration
- ecs-task-definition-memory-hartes Limit
- ecs-task-definition-network-mode-not-host
- ecs-task-definition-nonroot-Benutzer
- ecs-task-definition-pid-Modus-Check
- ecs-task-definition-user-for-host-mode-check
- efs-access-point-enforce-Stammverzeichnis
- efs-access-point-enforce-Benutzeridentität
- efs-automatic-backups-enabled
- efs-encrypted-check
- efs-filesystem-ct-encrypted
- efs-in-backup-plan
- efs-last-backup-recovery-Punkt erstellt
- efs-meets-restore-time-Ziel
- efs-mount-target-public-zugänglich
- efs-resources-in-logically-air-gapped-vault
- efs-resources-protected-by-Ersatzplan
- eip-attached
- eks-cluster-logging-enabled
- eks-cluster-log-enabled
- eks-cluster-oldest-supported-Ausführung
- eks-cluster-secrets-encrypted
- eks-cluster-supported-version
- eks-endpoint-no-public-Zugang
- eks-secrets-encrypted
- elasticache-auto-minor-version-aktualisieren-Prüfung
- elasticache-rbac-auth-enabled
- elasticache-redis-cluster-automatic-Backup-Check
- elasticache-repl-grp-auto-failover-fähig
- elasticache-repl-grp-encrypted-im Ruhezustand

- elasticache-repl-grp-encryptedim Transit
- elasticache-repl-grp-redis-auth-aktiviert
- elasticache-subnet-group-check
- elasticache-supported-engine-version
- elasticbeanstalk-application-description
- elasticbeanstalk-application-version-description
- elasticbeanstalk-environment-description
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch
- elasticsearch-node-to-node-Verschlüsselungsprüfung
- elastic-beanstalk-logs-to- Cloudwatch
- elastic-beanstalk-managed-updates-aktiviert
- elbv2- acm-certificate-required
- elv 2- listener-encryption-in-transit
- elbv2-multiple-az
- elbv2- prüfen predefined-security-policy-ssl
- elb-acm-certificate-required
- elb-cross-zone-load-Balancing aktiviert
- elb-custom-security-policy-ssl-Prüfung
- elb-deletion-protection-enabled
- elb-logging-enabled
- elb-predefined-security-policy-SSL-Überprüfung
- elb-tls-https-listeners-nur
- emr-block-public-access
- emr-kerberos-enabled
- emr-master-no-public-ip
- emr-security-configuration-encryption-ausruhen
- emr-security-configuration-encryption-Transit
- encrypted-volumes

- event-data-store-cmk-Verschlüsselung aktiviert
- evidently-launch-description
- evidently-launch-tagged
- evidently-project-description
- evidently-project-tagged
- evidently-segment-description
- evidently-segment-tagged
- fis-experiment-template-log-Konfiguration ist vorhanden
- fis-experiment-template-tagged
- fms-shield-resource-policy-überprüfen
- fms-webacl-resource-policy-überprüfen
- fms-webacl-rulegroup-association-überprüfen
- fsx-last-backup-recovery-Punkt erstellt
- fsx-lustre-copy-tagszu Backups
- fsx-meets-restore-time-Ziel
- fsx-ontap-deployment-type-überprüfen
- fsx-openzfs-copy-tags-aktiviert
- fsx-openzfs-deployment-type-überprüfen
- fsx-resources-protected-by-Ersatzplan
- fsx-windows-audit-log-konfiguriert
- fsx-windows-deployment-type-überprüfen
- glb-listener-tagged
- global-endpoint-event-replication-aktiviert
- glue-job-logging-enabled
- glue-ml-transform-encrypted-im Ruhezustand
- glue-spark-job-supported-Ausführung
- GuardDuty-EC2- protection-runtime-enabled
- guardduty-ecs-protection-runtime-aktiviert
- guardduty-eks-protection-audit-aktiviert
- guardduty-eks-protection-runtime-aktiviert

- guardduty-enabled-centralized
- guardduty-lambda-protection-enabled
- guardduty-malware-protection-enabled
- guardduty-non-archived-findings
- guardduty-rds-protection-enabled
- guardduty-runtime-monitoring-enabled
- GuardDuty-S3-Schutz aktiviert
- iam-customer-policy-blocked-kms-Aktionen
- iam-external-access-analyzer-aktiviert
- iam-group-has-users-überprüfen
- iam-inline-policy-blocked-KMS-Aktionen
- iam-no-inline-policy-überprüfen
- iam-password-policy
- iam-policy-blacklisted-check
- iam-policy-in-use
- iam-policy-no-statements-with-admin-access
- iam-policy-no-statements-with-full-access
- iam-role-managed-policy-überprüfen
- iam-root-access-key-überprüfen
- iam-user-group-membership-überprüfen
- iam-user-mfa-enabled
- iam-user-no-policies-überprüfen
- iam-user-unused-credentials-überprüfen
- incoming-ssh-disabled
- inspector-ec2-Scan aktiviert
- inspector-ecr-scan-enabled
- inspector-lambda-code-scan-aktiviert
- inspector-lambda-standard-scan-aktiviert
- instances-in-vpc
- internet-gateway-authorized-vpc-nur

- iotevents-alarm-model-tagged
- iotevents-detector-model-tagged
- iotevents-input-tagged
- iotsitewise-asset-model-tagged
- iotsitewise-dashboard-tagged
- iotsitewise-gateway-tagged
- iotsitewise-portal-tagged
- iotsitewise-project-tagged
- iottwinmaker-component-type-tagged
- iottwinmaker-scene-tagged
- iottwinmaker-sync-job-tagged
- iottwinmaker-workspace-tagged
- iotwireless-fuota-task-tagged
- iotwireless-multicast-group-tagged
- iotwireless-service-profile-tagged
- iot-authorizer-token-signing-aktiviert
- ivs-channel-playback-authorization-aktiviert
- ivs-channel-tagged
- ivs-playback-key-pair-markiert
- ivs-recording-configuration-tagged
- kinesis-firehose-delivery-stream-verschlüsselt
- kinesis-stream-backup-retention-überprüfen
- kinesis-stream-encrypted
- kms-cmk-not-scheduled-zum Löschen
- kms-key-policy-no-öffentlicher Zugang
- lambda-concurrency-check
- lambda-dlq-check
- lambda-function-public-access-verboten
- lambda-function-settings-check
- lambda-function-xray-enabled

- lambda-inside-vpc
- lambda-vpc-multi-az-überprüfen
- lightsail-bucket-tagged
- lightsail-certificate-tagged
- lightsail-disk-tagged
- macie-auto-sensitive-data-Discovery-Check
- macie-status-check
- mariadb-publish-logs-to-Cloudwatch-Protokolle
- mfa-enabled-for-iam-Konsolenzugriff
- mq-active-broker-ldap-Authentifizierung
- mq-active-deployment-mode
- mq-active-single-instance-broker-storage-type-efs
- mq-automatic-minor-version-Upgrade aktiviert
- mq-auto-minor-version-upgrade-fähig
- mq-broker-general-logging-aktiviert
- mq-cloudwatch-audit-logging-aktiviert
- mq-cloudwatch-audit-log-aktiviert
- mq-no-public-access
- mq-rabbit-deployment-mode
- msk-cluster-public-access-deaktiviert
- msk-connect-connector-logging-aktiviert
- msk-enhanced-monitoring-enabled
- msk-in-cluster-node-require-tls
- msk-unrestricted-access-check
- multi-region-cloud-trail-aktiviert
- nacl-no-unrestricted-ssh-rdp
- neptune-cluster-backup-retention-überprüfen
- neptune-cluster-cloudwatch-log-exportfähig
- neptune-cluster-copy-tags-to-snapshot-enabled
- neptune-cluster-deletion-protection-aktiviert

- neptune-cluster-encrypted
- neptune-cluster-iam-database-Authentifizierung
- neptune-cluster-multi-az-aktiviert
- neptune-cluster-snapshot-encrypted
- neptune-cluster-snapshot-public-verboten
- netfw-deletion-protection-enabled
- netfw-logging-enabled
- netfw-multi-az-enabled
- netfw-policy-default-action-fragment-Pakete
- netfw-policy-default-action-vollständige Pakete
- netfw-policy-rule-group-assoziiert
- netfw-stateless-rule-group-nicht leer
- netfw-subnet-change-protection-aktiviert
- nlb-cross-zone-load-Balancing aktiviert
- nlb-internal-scheme-check
- nlb-listener-tagged
- nlb-logging-enabled
- no-unrestricted-route-to-igw
- opensearch-access-control-enabled
- opensearch-audit-logging-enabled
- opensearch-data-node-fault-Toleranz
- opensearch-encrypted-at-rest
- opensearch-https-required
- opensearch-in-vpc-only
- opensearch-logs-to-cloudwatch
- opensearch-node-to-node-Verschlüsselungsprüfung
- opensearch-primary-node-fault-Toleranz
- opensearch-update-check
- rabbit-mq-supported-version
- rds-aurora-mysql-audit-Protokollierung aktiviert

- rds-aurora-postgresql-logs-zu-Cloud-Watch
- rds-automatic-minor-version-upgrade-fähig
- rds-cluster-auto-minor-version-upgrade-enable
- rds-cluster-default-admin-überprüfen
- rds-cluster-deletion-protection-aktiviert
- rds-cluster-encrypted-at-ausruhen
- rds-cluster-iam-authentication-aktiviert
- rds-cluster-multi-az-aktiviert
- rds-db-security-group-nicht erlaubt
- rds-enhanced-monitoring-enabled
- rds-instance-default-admin-überprüfen
- rds-instance-deletion-protection-aktiviert
- rds-instance-iam-authentication-aktiviert
- rds-instance-public-access-überprüfen
- rds-instance-subnet-igw-überprüfen
- rds-in-backup-plan
- rds-last-backup-recovery-Punkt erstellt
- rds-logging-enabled
- rds-mariadb-instance-encryptedim Transit
- rds-meets-restore-time-Ziel
- rds-multi-az-support
- rds-mysql-instance-encryptedunterwegs
- rds-postgresql-logs-to- Cloudwatch
- rds-postgres-instance-encryptedunterwegs
- rds-proxy-tls-encryption
- rds-resources-protected-by-Ersatzplan
- rds-snapshots-public-prohibited
- rds-snapshot-encrypted
- rds-sqlserver-encrypted-in-Transit
- rds-sql-server-logszur Cloud-Überwachung

- rds-storage-encrypted
- redshift-audit-logging-enabled
- redshift-backup-enabled
- redshift-cluster-configuration-check
- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check
- redshift-cluster-multi-az-aktiviert
- redshift-cluster-parameter-group-markiert
- redshift-cluster-public-access-überprüfen
- redshift-cluster-subnet-group-Multi-Az
- redshift-default-admin-check
- redshift-default-db-name-überprüfen
- redshift-enhanced-vpc-routing-aktiviert
- redshift-require-tls-ssl
- redshift-serverless-default-admin-überprüfen
- redshift-serverless-default-db-Namenscheck
- redshift-serverless-namespace-cmk-Verschlüsselung
- redshift-serverless-publish-logs-zu-Cloud-Watch
- redshift-serverless-workgroup-encryptedauf dem Weg
- redshift-serverless-workgroup-no-öffentlich zugänglich
- redshift-serverless-workgroup-routes-innerhalb von VPC
- redshift-unrestricted-port-access
- required-tags
- restricted-incoming-traffic
- root-account-hardware-mfa-aktiviert
- root-account-mfa-enabled
- s3 -regel-check express-dir-bucket-lifecycle
- nur s3- access-point-in-vpc
- s3- -Blöcke access-point-public-access
- s3- -Blöcke account-level-public-access

- s3- -Blocke-periodisch account-level-public-access
- s 3- bucket-acl-prohibited
- s-3 bucket-blacklisted-actions-prohibited
- s3- bucket-cross-region-replication -aktiviert
- s-3 bucket-default-lock-enabled
- s3 bucket-level-public-access - verboten
- s3- bucket-logging-enabled
- s-3 bucket-mfa-delete-enabled
- s-3 bucket-policy-grantee-check
- s3- bucket-policy-not-more -freizügig
- s 3- bucket-public-read-prohibited
- s-3 bucket-public-write-prohibited
- s-3 bucket-replication-enabled
- s3- bucket-server-side-encryption -aktiviert
- s-3 bucket-ssl-requests-only
- s3-Bucket-Tag
- s-3 bucket-versioning-enabled
- s-3 default-encryption-kms
- s-3 event-notifications-enabled
- s3 last-backup-recovery-point - erstellt
- s3- lifecycle-policy-check
- s-3 meets-restore-time-target
- s3- resources-in-logically-air -Tresor mit Lücken
- s3 resources-protected-by-backup - -Plan
- s 3- version-lifecycle-policy-check
- sagemaker-app-image-config-markiert
- sagemaker-domain-in-vpc
- sagemaker-domain-tagged
- sagemaker-endpoint-configuration-kms-schlüsselkonfiguriert
- sagemaker-endpoint-config-prod-Anzahl der Instanzen

- sagemaker-feature-group-tagged
- sagemaker-image-description
- sagemaker-image-tagged
- sagemaker-model-in-vpc
- sagemaker-model-isolation-enabled
- sagemaker-notebook-instance-inside-vpc
- sagemaker-notebook-instance-kms-key-konfiguriert
- sagemaker-notebook-instance-platform-Version
- sagemaker-notebook-instance-root-Zugriffsprüfung
- sagemaker-notebook-no-direct-Internetzugang
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-überprüfen
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- securityhub-enabled
- security-account-information-provided
- service-catalog-shared-within-Organisation
- service-vpc-endpoint-enabled
- sns-encrypted-kms
- sns-topic-message-delivery-Benachrichtigung aktiviert
- sns-topic-no-public-Zugriff
- sqs-queue-no-public-Zugang
- ssm-automation-block-public-teilen
- ssm-automation-logging-enabled
- ssm-document-not-public
- ssm-document-tagged
- step-functions-state-machine-Protokollierung aktiviert
- storagegateway-last-backup-recovery-punkt-erstellt
- storagegateway-resources-in-logically-air-gapped-vault

- storagegateway-resources-protected-by-Ersatzplan
- subnet-auto-assign-public-ip-deaktiviert
- transfer-agreement-description
- transfer-agreement-tagged
- transfer-certificate-description
- transfer-certificate-tagged
- transfer-connector-logging-enabled
- transfer-connector-tagged
- transfer-family-server-no-ftp
- transfer-profile-tagged
- transfer-workflow-description
- transfer-workflow-tagged
- virtualmachine-last-backup-recovery-Punkt erstellt
- virtualmachine-resources-in-logically-air-gapped-vault
- virtualmachine-resources-protected-by-Ersatzplan
- vpc-default-security-group-geschlossen
- vpc-endpoint-enabled
- vpc-flow-logs-enabled
- vpc-network-acl-unused-überprüfen
- vpc-peering-dns-resolution-überprüfen
- vpc-sg-open-only-to-authorized-ports
- vpc-sg-port-restriction-überprüfen
- vpc-vpn-2-tunnels-up
- wafv2-logging-enabled
- WAF 2- rulegroup-logging-enabled
- WAF 2- rulegroup-not-empty
- WAF 2- webacl-not-empty
- waf-regional-rulegroup-not-leer
- waf-regional-rule-not-leer
- waf-regional-webacl-not-leer

- workspaces-root-volume-encryption-aktiviert
- workspaces-user-volume-encryption-aktiviert

Region Kanada (Zentral)

Kanada (Zentral)

- access-keys-rotated
- account-part-of-organizations
- acmpca-certificate-authority-tagged
- acm-certificate-expiration-check
- acm-certificate-rsa-check
- acm-pca-root-ca-deaktiviert
- active-mq-supported-version
- alb-desync-mode-check
- alb-http-drop-invalid-Header-fähig
- alb-http-to-https-Umleitungsprüfung
- alb-internal-scheme-check
- alb-listener-tagged
- alb-waf-enabled
- amplify-app-branch-auto-löschung aktiviert
- amplify-app-description
- amplify-app-tagged
- amplify-branch-performance-mode-aktiviert
- amplify-branch-tagged
- api-gwv2- access-logs-enabled
- api-gwv2- authorization-type-configured
- api-gw-associated-with-WAF
- api-gw-cache-enabled-und-verschlüsselt
- api-gw-endpoint-type-überprüfen
- api-gw-execution-logging-aktiviert
- api-gw-ssl-enabled

- api-gw-xray-enabled
- appconfig-application-description
- appconfig-application-tagged
- appconfig-configuration-profile-tagged
- appconfig-configuration-profile-validators-nicht leer
- appconfig-deployment-strategy-description
- appconfig-deployment-strategy-replicate-zu-ssm
- appconfig-environment-description
- appconfig-environment-tagged
- appconfig-extension-association-tagged
- appconfig-freeform-profile-config-Speicher
- appconfig-hosted-configuration-version-Beschreibung
- appflow-flow-tagged
- appintegrations-event-integration-description
- appintegrations-event-integration-tagged
- appmesh-gateway-route-tagged
- appmesh-mesh-deny-tcp-Weiterleitung
- appmesh-mesh-tagged
- appmesh-route-tagged
- appmesh-virtual-gateway-backend-Standardeinstellungen-TLS
- appmesh-virtual-gateway-logging-file-path-exists
- appmesh-virtual-gateway-tagged
- appmesh-virtual-node-backend-defaults-tls-on
- appmesh-virtual-node-logging-file-path-exists
- appmesh-virtual-node-tagged
- appmesh-virtual-router-tagged
- appmesh-virtual-service-tagged
- approved-amis-by-id
- approved-amis-by-tag
- appstream-fleet-in-vpc

- appsync-associated-with-waf
- appsync-authorization-check
- appsync-cache-encryption-at-ausruhen
- appsync-logging-enabled
- athena-data-catalog-description
- athena-prepared-statement-description
- athena-workgroup-description
- athena-workgroup-encrypted-at-ausruhen
- athena-workgroup-enforce-workgroup-Konfiguration
- athena-workgroup-engine-version-automatisches Upgrade
- athena-workgroup-logging-enabled
- aurora-last-backup-recovery-Punkt erstellt
- aurora-meets-restore-time-Ziel
- aurora-mysql-backtracking-enabled
- aurora-mysql-cluster-audit-Protokollierung
- aurora-resources-in-logically-air-gapped-vault
- aurora-resources-protected-by-Backup-Plan
- autoscaling-capacity-rebalancing
- autoscaling-group-elb-healthcheck-erforderlich
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-hop-Grenze
- autoscaling-launch-config-public-ip-deaktiviert
- autoscaling-launch-template
- autoscaling-multiple-az
- autoscaling-multiple-instance-types
- backup-plan-min-frequency-and-min-retention-check
- backup-recovery-point-encrypted
- backup-recovery-point-manual-Löschen-deaktiviert
- backup-recovery-point-minimum-Aufbewahrungsprüfung
- batch-compute-environment-enabled

- batch-compute-environment-managed
- batch-compute-environment-tagged
- batch-job-queue-enabled
- batch-job-queue-tagged
- batch-managed-compute-environment-using-launch-template
- batch-managed-compute-env-compute-resources-tagged
- batch-scheduling-policy-tagged
- beanstalk-enhanced-health-reporting-aktiviert
- cassandra-keyspace-tagged
- clb-desync-mode-check
- clb-multiple-az
- cloudformation-stack-drift-detection-überprüfen
- cloudformation-stack-notification-check
- cloudtrail-all-read-s3- data-event-check
- cloudtrail-all-write-s3- data-event-check
- Wolkenspur-S3- bucket-access-logging
- CloudTrail-S3- bucket-public-access-prohibited
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-action-enabled-überprüfen
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted
- cloud-trail-cloud-watch-logs-aktiviert
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-Validierung aktiviert
- cmk-backing-key-rotation-aktiviert
- codebuild-project-artifact-encryption

- codebuild-project-environment-privileged-überprüfen
- codebuild-project-envvar-awscred-überprüfen
- codebuild-project-logging-enabled
- codebuild-project-s3-log-verschlüsselt
- codebuild-project-source-repo-URL-Prüfung
- codebuild-report-group-encrypted-im Ruhezustand
- codedeploy-auto-rollback-monitor-aktiviert
- codedeploy-deployment-group-auto-rollback-aktiviert
- codedeploy-deployment-group-outdated-instanzen-aktualisieren
- Codedeploy-ec2- minimum-healthy-hosts-configured
- codedeploy-lambda-allatonce-traffic-shift-deaktiviert
- codepipeline-deployment-count-check
- codepipeline-region-fanout-check
- cognito-identity-pool-unauth-Zugriffsprüfung
- cognito-user-pool-advanced-sicherheitsaktiviert
- cognito-user-pool-tagged
- connect-instance-logging-enabled
- customerprofiles-object-type-allow-Profilerstellung
- customerprofiles-object-type-tagged
- custom-eventbus-policy-attached
- custom-schema-registry-policy-beigefügt
- cw-loggroup-retention-period-überprüfen
- datasync-task-data-verification-aktiviert
- datasync-task-logging-enabled
- datasync-task-tagged
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- dms-auto-minor-version-aktualisieren-Prüfung
- dms-endpoint-ssl-configured

- dms-endpoint-tagged
- dms-mongo-db-authentication-aktiviert
- dms-neptune-iam-authorization-aktiviert
- dms-redis-tls-enabled
- dms-replication-not-public
- dms-replication-task-sourcedb-Protokollierung
- dms-replication-task-tagged
- dms-replication-task-targetdb-Protokollierung
- docdb-cluster-audit-logging-aktiviert
- docdb-cluster-backup-retention-überprüfen
- docdb-cluster-deletion-protection-aktiviert
- docdb-cluster-encrypted
- docdb-cluster-encrypted-in-transit
- docdb-cluster-snapshot-public-verboten
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-last-backup-recovery-Punkt erstellt
- dynamodb-meets-restore-time-Ziel
- dynamodb-pitr-enabled
- dynamodb-resources-protected-by-Backup-Plan
- dynamodb-table-deletion-protection-aktiviert
- dynamodb-table-encrypted-kms
- dynamodb-table-encryption-enabled
- dynamodb-throughput-limit-check
- ebs-in-backup-plan
- ebs-last-backup-recovery-punkt-erstellt
- ebs-meets-restore-time-Ziel
- ebs-optimized-instance
- ebs-resources-in-logically-air-gapped-vault
- ebs-resources-protected-by-Backup-Plan

- ebs-snapshot-public-restorable-überprüfen
- ec2- capacity-reservation-tagged
- ec2- carrier-gateway-tagged
- ec2- aktiviert client-vpn-connection-log
- ec2- client-vpn-endpoint-tagged
- ec2- -alle client-vpn-not-authorize
- ec2- dhcp-options-tagged
- ec2- ebs-encryption-by-default
- ec2- aktiviert enis-source-destination-check
- ec2-fleet-markiert
- ec2-imdsv2-check
- ec2- instance-detailed-monitoring-enabled
- ec2-ami instance-launched-with-allowed
- ec2- instance-managed-by-ssm
- ec2- instance-multiple-eni-check
- ec2- instance-no-public-ip
- ec2- instance-profile-attached
- ec2- erstellt last-backup-recovery-point
- ec2-2-prüfen launch-template-imdsv
- ec2- -deaktiviert launch-template-public-ip
- ec2- launch-template-tagged
- ec2- managedinstance-applications-blacklisted
- ec2- managedinstance-applications-required
- ec2- prüfen managedinstance-association-compliance-status
- ec2- managedinstance-inventory-blacklisted
- ec2- prüfen managedinstance-patch-compliance-status
- ec2- managedinstance-platform-check
- ec2- meets-restore-time-target
- ec2- Analyse mit Schlagwörtern network-insights-access-scope
- ec2 network-insights-access-scope - markiert

- ec2- network-insights-path-tagged
- ec2- no-amazon-key-pair
- ec2- prefix-list-tagged
- ec2- -Tresor mit Lücken resources-in-logically-air
- ec2- resources-protected-by-backup -plan
- ec2- -eni security-group-attached-to
- ec2- -eni-periodisch security-group-attached-to
- ec2-stopped-instance
- ec2- token-hop-limit-check
- ec2- traffic-mirror-filter-description
- ec2- traffic-mirror-filter-tagged
- ec2- traffic-mirror-session-description
- ec2- traffic-mirror-session-tagged
- ec2- traffic-mirror-target-description
- ec2- traffic-mirror-target-tagged
- ec2- -attach-deaktiviert transit-gateway-auto-vpc
- ec2 transit-gateway-multicast-domain - markiert
- ec2- volume-inuse-check
- ec2- vpn-connection-logging-enabled
- ecr-private-image-scanning-aktiviert
- ecr-private-lifecycle-policy-konfiguriert
- ecr-private-tag-immutability-aktiviert
- ecr-repository-cmk-encryption-aktiviert
- ecr-repository-tagged
- ecs-awsvpc-networking-enabled
- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-container-insights-enabled
- ecs-fargate-latest-platform-Version
- ecs-no-environment-secrets

- ecs-task-definition-log-Konfiguration
- ecs-task-definition-memory-hartes Limit
- ecs-task-definition-network-mode-not-host
- ecs-task-definition-nonroot-Benutzer
- ecs-task-definition-pid-Modus-Check
- ecs-task-definition-user-for-host-mode-check
- efs-access-point-enforce-Stammverzeichnis
- efs-access-point-enforce-Benutzeridentität
- efs-automatic-backups-enabled
- efs-encrypted-check
- efs-filesystem-ct-encrypted
- efs-in-backup-plan
- efs-last-backup-recovery-Punkt erstellt
- efs-meets-restore-time-Ziel
- efs-mount-target-public-zugänglich
- efs-resources-in-logically-air-gapped-vault
- efs-resources-protected-by-Ersatzplan
- eip-attached
- eks-cluster-logging-enabled
- eks-cluster-log-enabled
- eks-cluster-oldest-supported-Ausführung
- eks-cluster-secrets-encrypted
- eks-cluster-supported-version
- eks-endpoint-no-public-Zugang
- eks-secrets-encrypted
- elasticache-auto-minor-version-aktualisieren-Prüfung
- elasticache-rbac-auth-enabled
- elasticache-redis-cluster-automatic-Backup-Check
- elasticache-repl-grp-auto-failover-fähig
- elasticache-repl-grp-encrypted-im Ruhezustand

- elasticache-repl-grp-encryptedim Transit
- elasticache-repl-grp-redis-auth-aktiviert
- elasticache-subnet-group-check
- elasticache-supported-engine-version
- elasticbeanstalk-application-description
- elasticbeanstalk-application-version-description
- elasticbeanstalk-environment-description
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch
- elasticsearch-node-to-node-Verschlüsselungsprüfung
- elastic-beanstalk-logs-to- Cloudwatch
- elastic-beanstalk-managed-updates-aktiviert
- elbv2- acm-certificate-required
- elv 2- listener-encryption-in-transit
- elbv2-multiple-az
- elbv2- prüfen predefined-security-policy-ssl
- elb-acm-certificate-required
- elb-cross-zone-load-Balancing aktiviert
- elb-custom-security-policy-ssl-Prüfung
- elb-deletion-protection-enabled
- elb-logging-enabled
- elb-predefined-security-policy-SSL-Überprüfung
- elb-tls-https-listeners-nur
- emr-block-public-access
- emr-kerberos-enabled
- emr-master-no-public-ip
- emr-security-configuration-encryption-ausruhen
- emr-security-configuration-encryption-Transit
- encrypted-volumes

- event-data-store-cmk-Verschlüsselung aktiviert
- fis-experiment-template-log-Konfiguration ist vorhanden
- fis-experiment-template-tagged
- fms-shield-resource-policy-überprüfen
- fms-webacl-resource-policy-überprüfen
- fms-webacl-rulegroup-association-überprüfen
- fsx-last-backup-recovery-Punkt erstellt
- fsx-lustre-copy-tagszu Backups
- fsx-meets-restore-time-Ziel
- fsx-ontap-deployment-type-überprüfen
- fsx-openzfs-copy-tags-aktiviert
- fsx-openzfs-deployment-type-überprüfen
- fsx-resources-protected-by-Ersatzplan
- fsx-windows-audit-log-konfiguriert
- fsx-windows-deployment-type-überprüfen
- glb-listener-tagged
- global-endpoint-event-replication-aktiviert
- glue-job-logging-enabled
- glue-ml-transform-encrypted-im Ruhezustand
- glue-spark-job-supported-Ausführung
- GuardDuty-EC2- protection-runtime-enabled
- guardduty-ecs-protection-runtime-aktiviert
- guardduty-eks-protection-audit-aktiviert
- guardduty-eks-protection-runtime-aktiviert
- guardduty-enabled-centralized
- guardduty-lambda-protection-enabled
- guardduty-malware-protection-enabled
- guardduty-non-archived-findings
- guardduty-rds-protection-enabled
- guardduty-runtime-monitoring-enabled

- GuardDuty-S3-Schutz aktiviert
- iam-customer-policy-blocked-kms-Aktionen
- iam-external-access-analyzer-aktiviert
- iam-group-has-users-überprüfen
- iam-inline-policy-blocked-KMS-Aktionen
- iam-no-inline-policy-überprüfen
- iam-password-policy
- iam-policy-blacklisted-check
- iam-policy-in-use
- iam-policy-no-statements-with-admin-access
- iam-policy-no-statements-with-full-access
- iam-role-managed-policy-überprüfen
- iam-root-access-key-überprüfen
- iam-user-group-membership-überprüfen
- iam-user-mfa-enabled
- iam-user-no-policies-überprüfen
- iam-user-unused-credentials-überprüfen
- incoming-ssh-disabled
- inspector-ec2-Scan aktiviert
- inspector-ecr-scan-enabled
- inspector-lambda-standard-scan-aktiviert
- instances-in-vpc
- internet-gateway-authorized-vpc-nur
- iotevents-alarm-model-tagged
- iotevents-detector-model-tagged
- iotevents-input-tagged
- iotsitewise-asset-model-tagged
- iotsitewise-dashboard-tagged
- iotsitewise-gateway-tagged
- iotsitewise-portal-tagged

- iotsitewise-project-tagged
- iot-authorizer-token-signing-aktiviert
- kinesis-firehose-delivery-stream-verschlüsselt
- kinesis-stream-backup-retention-überprüfen
- kinesis-stream-encrypted
- kms-cmk-not-scheduled-zum Löschen
- kms-key-policy-no-öffentlicher Zugang
- lambda-concurrency-check
- lambda-dlq-check
- lambda-function-public-access-verboten
- lambda-function-settings-check
- lambda-function-xray-enabled
- lambda-inside-vpc
- lambda-vpc-multi-az-überprüfen
- lightsail-bucket-tagged
- lightsail-certificate-tagged
- lightsail-disk-tagged
- macie-auto-sensitive-data-Discovery-Check
- macie-status-check
- mariadb-publish-logs-to-Cloudwatch-Protokolle
- mfa-enabled-for-iam-Konsolenzugriff
- mq-active-broker-ldap-Authentifizierung
- mq-active-deployment-mode
- mq-active-single-instance-broker-storage-type-efs
- mq-automatic-minor-version-Upgrade aktiviert
- mq-auto-minor-version-upgrade-fähig
- mq-broker-general-logging-aktiviert
- mq-cloudwatch-audit-logging-aktiviert
- mq-cloudwatch-audit-log-aktiviert
- mq-no-public-access

- mq-rabbit-deployment-mode
- msk-cluster-public-access-deaktiviert
- msk-connect-connector-logging-aktiviert
- msk-enhanced-monitoring-enabled
- msk-in-cluster-node-require-tls
- msk-unrestricted-access-check
- multi-region-cloud-trail-aktiviert
- nacl-no-unrestricted-ssh-rdp
- neptune-cluster-backup-retention-überprüfen
- neptune-cluster-cloudwatch-log-exportfähig
- neptune-cluster-copy-tags-to-snapshot-enabled
- neptune-cluster-deletion-protection-aktiviert
- neptune-cluster-encrypted
- neptune-cluster-iam-database-Authentifizierung
- neptune-cluster-multi-az-aktiviert
- neptune-cluster-snapshot-encrypted
- neptune-cluster-snapshot-public-verboten
- netfw-deletion-protection-enabled
- netfw-logging-enabled
- netfw-multi-az-enabled
- netfw-policy-default-action-fragment-Pakete
- netfw-policy-default-action-vollständige Pakete
- netfw-policy-rule-group-assoziiert
- netfw-stateless-rule-group-nicht leer
- netfw-subnet-change-protection-aktiviert
- nlb-cross-zone-load-Balancing aktiviert
- nlb-internal-scheme-check
- nlb-listener-tagged
- nlb-logging-enabled
- no-unrestricted-route-to-igw

- opensearch-access-control-enabled
- opensearch-audit-logging-enabled
- opensearch-data-node-fault-Toleranz
- opensearch-encrypted-at-rest
- opensearch-https-required
- opensearch-in-vpc-only
- opensearch-logs-to-cloudwatch
- opensearch-node-to-node-Verschlüsselungsprüfung
- opensearch-primary-node-fault-Toleranz
- opensearch-update-check
- rabbit-mq-supported-version
- rds-aurora-mysql-audit-Protokollierung aktiviert
- rds-aurora-postgresql-logs-zu-Cloud-Watch
- rds-automatic-minor-version-upgrade-fähig
- rds-cluster-auto-minor-version-upgrade-enable
- rds-cluster-default-admin-überprüfen
- rds-cluster-deletion-protection-aktiviert
- rds-cluster-encrypted-at-ausruhen
- rds-cluster-iam-authentication-aktiviert
- rds-cluster-multi-az-aktiviert
- rds-enhanced-monitoring-enabled
- rds-instance-default-admin-überprüfen
- rds-instance-deletion-protection-aktiviert
- rds-instance-iam-authentication-aktiviert
- rds-instance-public-access-überprüfen
- rds-instance-subnet-igw-überprüfen
- rds-in-backup-plan
- rds-last-backup-recovery-Punkt erstellt
- rds-logging-enabled
- rds-mariadb-instance-encryptedim Transit

- rds-meets-restore-time-Ziel
- rds-multi-az-support
- rds-mysql-instance-encryptedunterwegs
- rds-postgresql-logs-to- Cloudwatch
- rds-postgres-instance-encryptedunterwegs
- rds-proxy-tls-encryption
- rds-resources-protected-by-Ersatzplan
- rds-snapshots-public-prohibited
- rds-snapshot-encrypted
- rds-sqlserver-encrypted-in-Transit
- rds-sql-server-logszur Cloud-Überwachung
- rds-storage-encrypted
- redshift-audit-logging-enabled
- redshift-backup-enabled
- redshift-cluster-configuration-check
- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check
- redshift-cluster-multi-az-aktiviert
- redshift-cluster-parameter-group-markiert
- redshift-cluster-public-access-überprüfen
- redshift-cluster-subnet-group-Multi-Az
- redshift-default-admin-check
- redshift-default-db-name-überprüfen
- redshift-enhanced-vpc-routing-aktiviert
- redshift-require-tls-ssl
- redshift-serverless-default-admin-überprüfen
- redshift-serverless-default-db-Namenscheck
- redshift-serverless-namespace-cmk-Verschlüsselung
- redshift-serverless-publish-logs-zu-Cloud-Watch
- redshift-serverless-workgroup-encryptedauf dem Weg

- redshift-serverless-workgroup-no-öffentlich zugänglich
- redshift-serverless-workgroup-routes-innerhalb von VPC
- redshift-unrestricted-port-access
- required-tags
- restricted-incoming-traffic
- root-account-hardware-mfa-aktiviert
- root-account-mfa-enabled
- nur s3- access-point-in-vpc
- s3- -Blöcke access-point-public-access
- s3- -Blöcke account-level-public-access
- s3- -Blocke-periodisch account-level-public-access
- s 3- bucket-acl-prohibited
- s-3 bucket-blacklisted-actions-prohibited
- s3- bucket-cross-region-replication -aktiviert
- s-3 bucket-default-lock-enabled
- s3 bucket-level-public-access - verboten
- s3- bucket-logging-enabled
- s-3 bucket-mfa-delete-enabled
- s-3 bucket-policy-grantee-check
- s3- bucket-policy-not-more -freizügig
- s 3- bucket-public-read-prohibited
- s-3 bucket-public-write-prohibited
- s-3 bucket-replication-enabled
- s3- bucket-server-side-encryption -aktiviert
- s-3 bucket-ssl-requests-only
- s3-Bucket-Tag
- s-3 bucket-versioning-enabled
- s-3 default-encryption-kms
- s-3 event-notifications-enabled
- s3 last-backup-recovery-point - erstellt

- s3- lifecycle-policy-check
- s-3 meets-restore-time-target
- s3- resources-in-logically-air -Tresor mit Lücken
- s3 resources-protected-by-backup - -Plan
- s 3- version-lifecycle-policy-check
- sagemaker-app-image-config-markiert
- sagemaker-domain-in-vpc
- sagemaker-domain-tagged
- sagemaker-endpoint-configuration-kms-schlüsselkonfiguriert
- sagemaker-endpoint-config-prod-Anzahl der Instanzen
- sagemaker-feature-group-tagged
- sagemaker-image-description
- sagemaker-image-tagged
- sagemaker-model-in-vpc
- sagemaker-model-isolation-enabled
- sagemaker-notebook-instance-inside-vpc
- sagemaker-notebook-instance-kms-key-konfiguriert
- sagemaker-notebook-instance-platform-Version
- sagemaker-notebook-instance-root-Zugriffsprüfung
- sagemaker-notebook-no-direct-Internetzugang
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-überprüfen
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- securityhub-enabled
- security-account-information-provided
- service-catalog-shared-within-Organisation
- service-vpc-endpoint-enabled
- sns-encrypted-kms

- sns-topic-message-delivery-Benachrichtigung aktiviert
- sns-topic-no-public-Zugriff
- sqs-queue-no-public-Zugang
- ssm-automation-block-public-teilen
- ssm-automation-logging-enabled
- ssm-document-not-public
- ssm-document-tagged
- step-functions-state-machine-Protokollierung aktiviert
- storagegateway-last-backup-recovery-punkt-erstellt
- storagegateway-resources-in-logically-air-gapped-vault
- storagegateway-resources-protected-by-Ersatzplan
- subnet-auto-assign-public-ip-deaktiviert
- transfer-agreement-description
- transfer-agreement-tagged
- transfer-certificate-description
- transfer-certificate-tagged
- transfer-connector-logging-enabled
- transfer-connector-tagged
- transfer-family-server-no-ftp
- transfer-profile-tagged
- transfer-workflow-description
- transfer-workflow-tagged
- virtualmachine-last-backup-recovery-Punkt erstellt
- virtualmachine-resources-in-logically-air-gapped-vault
- virtualmachine-resources-protected-by-Ersatzplan
- vpc-default-security-group-geschlossen
- vpc-endpoint-enabled
- vpc-flow-logs-enabled
- vpc-network-acl-unused-überprüfen
- vpc-peering-dns-resolution-überprüfen

- vpc-sg-open-only-to-authorized-ports
- vpc-sg-port-restriction-überprüfen
- vpc-vpn-2-tunnels-up
- wafv2-logging-enabled
- WAF 2- rulegroup-logging-enabled
- WAF 2- rulegroup-not-empty
- WAF 2- webacl-not-empty
- waf-regional-rulegroup-not-leer
- waf-regional-rule-not-leer
- waf-regional-webacl-not-leer
- workspaces-root-volume-encryption-aktiviert
- workspaces-user-volume-encryption-aktiviert

Region Kanada West (Calgary)

Kanada West (Calgary)

- account-part-of-organizations
- acmpca-certificate-authority-tagged
- acm-certificate-expiration-check
- alb-http-drop-invalid-Header-fähig
- alb-http-to-https-Umleitungsprüfung
- alb-internal-scheme-check
- alb-waf-enabled
- api-gw-associated-with-WAF
- api-gw-cache-enabled-und-verschlüsselt
- api-gw-endpoint-type-überprüfen
- api-gw-execution-logging-aktiviert
- api-gw-ssl-enabled
- api-gw-xray-enabled
- appconfig-deployment-strategy-description
- appconfig-deployment-strategy-replicate-zu-ssm

- approved-amis-by-id
- approved-amis-by-tag
- athena-data-catalog-description
- athena-prepared-statement-description
- athena-workgroup-description
- athena-workgroup-enforce-workgroup-Konfiguration
- athena-workgroup-engine-version-automatisches Upgrade
- autoscaling-group-elb-healthcheck-erforderlich
- autoscaling-launch-config-public-ip-deaktiviert
- batch-scheduling-policy-tagged
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted
- cloud-trail-cloud-watch-logs-aktiviert
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-Validierung aktiviert
- cmk-backing-key-rotation-aktiviert
- cognito-user-pool-tagged
- cw-loggroup-retention-period-überprüfen
- datasync-task-data-verification-aktiviert
- datasync-task-tagged
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- dms-replication-not-public
- dynamodb-autoscaling-enabled

- dynamodb-in-backup-plan
- dynamodb-pitr-enabled
- dynamodb-table-encrypted-kms
- dynamodb-table-encryption-enabled
- dynamodb-throughput-limit-check
- ebs-snapshot-public-restorable-überprüfen
- ec2- capacity-reservation-tagged
- ec2- dhcp-options-tagged
- ec2- ebs-encryption-by-default
- ec2-imdsv2-check
- ec2- instance-detailed-monitoring-enabled
- ec2-ami instance-launched-with-allowed
- ec2- instance-managed-by-ssm
- ec2- instance-multiple-eni-check
- ec2- instance-no-public-ip
- ec2- prefix-list-tagged
- ec2- traffic-mirror-filter-description
- ec2- traffic-mirror-filter-tagged
- ec2- markiert transit-gateway-multicast-domain
- ecr-repository-tagged
- ecs-task-definition-network-mode-not-host
- ecs-task-definition-user-for-host-mode-check
- efs-encrypted-check
- efs-in-backup-plan
- eip-attached
- eks-endpoint-no-public-Zugang
- eks-secrets-encrypted
- elasticache-redis-cluster-automatic-Backup-Check
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only

- elasticsearch-logs-to-cloudwatch
- elasticsearch-node-to-node-Verschlüsselungsprüfung
- elb-cross-zone-load-Balancing aktiviert
- elb-custom-security-policy-ssl-Prüfung
- elb-deletion-protection-enabled
- elb-logging-enabled
- elb-predefined-security-policy-SSL-Überprüfung
- elb-tls-https-listeners-nur
- emr-security-configuration-encryption-ausruhen
- emr-security-configuration-encryption-Transit
- encrypted-volumes
- guardduty-enabled-centralized
- guardduty-non-archived-findings
- incoming-ssh-disabled
- instances-in-vpc
- kms-cmk-not-scheduled-zum Löschen
- lambda-concurrency-check
- lambda-dlq-check
- lambda-function-public-access-verboten
- lambda-function-settings-check
- lambda-inside-vpc
- multi-region-cloud-trail-aktiviert
- nlb-internal-scheme-check
- rds-automatic-minor-version-upgrade-fähig
- rds-cluster-deletion-protection-aktiviert
- rds-cluster-iam-authentication-aktiviert
- rds-cluster-multi-az-aktiviert
- rds-enhanced-monitoring-enabled
- rds-instance-deletion-protection-aktiviert
- rds-instance-iam-authentication-aktiviert

- rds-instance-public-access-überprüfen
- rds-logging-enabled
- rds-multi-az-support
- rds-snapshots-public-prohibited
- rds-snapshot-encrypted
- rds-storage-encrypted
- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check
- redshift-cluster-parameter-group-markiert
- redshift-cluster-public-access-überprüfen
- redshift-enhanced-vpc-routing-aktiviert
- redshift-require-tls-ssl
- required-tags
- restricted-incoming-traffic
- s3- -Blocke-periodisch account-level-public-access
- s 3- bucket-blacklisted-actions-prohibited
- s-3 bucket-default-lock-enabled
- s3 bucket-level-public-access - verboten
- s3- bucket-logging-enabled
- s-3 bucket-policy-grantee-check
- s3- bucket-policy-not-more -freizügig
- s 3- bucket-public-read-prohibited
- s-3 bucket-public-write-prohibited
- s-3 bucket-replication-enabled
- s3- bucket-server-side-encryption -aktiviert
- s-3 bucket-ssl-requests-only
- s3-Bucket-Tag
- s-3 bucket-versioning-enabled
- s-3 default-encryption-kms
- sagemaker-endpoint-configuration-kms-key-konfiguriert

- sagemaker-notebook-instance-kms-key-konfiguriert
- sagemaker-notebook-no-direct-Internetzugang
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-überprüfen
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- securityhub-enabled
- service-vpc-endpoint-enabled
- sns-encrypted-kms
- ssm-document-tagged
- subnet-auto-assign-public-ip-deaktiviert
- transfer-certificate-description
- transfer-certificate-tagged
- transfer-connector-tagged
- transfer-profile-tagged
- transfer-workflow-description
- transfer-workflow-tagged
- vpc-default-security-group-geschlossen
- vpc-flow-logs-enabled
- vpc-network-acl-unused-überprüfen
- vpc-sg-open-only-to-authorized-ports
- vpc-vpn-2-tunnels-up
- wafv2-logging-enabled

Region China (Peking)

China (Peking)

- access-keys-rotated
- acm-certificate-expiration-check
- active-mq-supported-version

- alb-desync-mode-check
- alb-http-drop-invalid-Header-fähig
- alb-http-to-https-Umleitungsprüfung
- alb-waf-enabled
- api-gwv2- access-logs-enabled
- api-gwv2- authorization-type-configured
- api-gw-associated-with-WAF
- api-gw-cache-enabled-und-verschlüsselt
- api-gw-endpoint-type-überprüfen
- api-gw-execution-logging-aktiviert
- api-gw-ssl-enabled
- api-gw-xray-enabled
- approved-amis-by-id
- approved-amis-by-tag
- appsync-associated-with-waf
- appsync-authorization-check
- appsync-logging-enabled
- athena-workgroup-encrypted-at-ausruhen
- athena-workgroup-logging-enabled
- autoscaling-group-elb-healthcheck-erforderlich
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-hop-Grenze
- autoscaling-launch-config-public-ip-deaktiviert
- autoscaling-launch-template
- autoscaling-multiple-az
- autoscaling-multiple-instance-types
- beanstalk-enhanced-health-reporting-aktiviert
- clb-desync-mode-check
- clb-multiple-az
- cloudformation-stack-drift-detection-überprüfen

- cloudformation-stack-notification-check
- Cloudfront - 3- origin-non-existent-bucket
- CloudTrail-S3- bucket-access-logging
- CloudTrail-S3- bucket-public-access-prohibited
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-action-enabled-überprüfen
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted
- cloud-trail-cloud-watch-logs-aktiviert
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-Validierung aktiviert
- cmk-backing-key-rotation-aktiviert
- codebuild-project-environment-privileged-überprüfen
- codebuild-project-envvar-awscred-überprüfen
- codebuild-project-logging-enabled
- codebuild-project-s3-log-verschlüsselt
- codebuild-project-source-repo-URL-Prüfung
- codebuild-report-group-encrypted-im Ruhezustand
- custom-eventbus-policy-attached
- cw-loggroup-retention-period-überprüfen
- datasync-task-logging-enabled
- dax-encryption-enabled
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- dms-auto-minor-version-aktualisieren-Prüfung

- dms-endpoint-ssl-configured
- dms-replication-not-public
- dms-replication-task-sourcedb-Protokollierung
- dms-replication-task-targetdb-Protokollierung
- docdb-cluster-encrypted-in-Transit
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-pitr-enabled
- dynamodb-table-deletion-protection-aktiviert
- dynamodb-table-encrypted-kms
- dynamodb-table-encryption-enabled
- dynamodb-throughput-limit-check
- ebs-in-backup-plan
- ebs-optimized-instance
- ebs-snapshot-public-restorable-überprüfen
- ec2- ebs-encryption-by-default
- ec2-imdsv2-check
- ec2- instance-detailed-monitoring-enabled
- ec2-ami instance-launched-with-allowed
- ec2- instance-managed-by-ssm
- ec2- instance-multiple-eni-check
- ec2- instance-no-public-ip
- ec2- instance-profile-attached
- ec2-2-prüfen launch-template-imdsv
- ec2- -deaktiviert launch-template-public-ip
- ec2- managedinstance-applications-blacklisted
- ec2- managedinstance-applications-required
- ec2- prüfen managedinstance-association-compliance-status
- ec2- managedinstance-inventory-blacklisted
- ec2- prüfen managedinstance-patch-compliance-status

- ec2- managedinstance-platform-check
- ec2- paravirtual-instance-check
- ec2-eni security-group-attached-to
- ec2-stopped-instance
- ec2- volume-inuse-check
- ecr-private-lifecycle-policy-konfiguriert
- ecr-private-tag-immutability-aktiviert
- ecr-repository-cmk-encryption-aktiviert
- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-container-insights-enabled
- ecs-fargate-latest-platform-Version
- ecs-no-environment-secrets
- ecs-task-definition-log-Konfiguration
- ecs-task-definition-network-mode-not-host
- ecs-task-definition-pid-Modus-Überprüfung
- ecs-task-definition-user-for-host-mode-check
- efs-access-point-enforce-Stammverzeichnis
- efs-access-point-enforce-Benutzeridentität
- efs-automatic-backups-enabled
- efs-encrypted-check
- efs-filesystem-ct-encrypted
- efs-in-backup-plan
- eip-attached
- eks-cluster-log-enabled
- eks-cluster-supported-version
- eks-endpoint-no-public-Zugang
- eks-secrets-encrypted
- elasticache-auto-minor-version-aktualisieren-Prüfung
- elasticache-redis-cluster-automatic-Backup-Check

- elasticache-repl-grp-auto-failover-fähig
- elasticache-repl-grp-encrypted-im Ruhezustand
- elasticache-repl-grp-encryptedim Transit
- elasticache-repl-grp-redis-auth-aktiviert
- elasticache-subnet-group-check
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch
- elasticsearch-node-to-node-Verschlüsselungsprüfung
- elastic-beanstalk-managed-updates-aktiviert
- elbv2- acm-certificate-required
- elv 2- listener-encryption-in-transit
- elbv2-multiple-az
- elbv2- prüfen predefined-security-policy-ssl
- elb-acm-certificate-required
- elb-cross-zone-load-Balancing aktiviert
- elb-custom-security-policy-ssl-Prüfung
- elb-deletion-protection-enabled
- elb-logging-enabled
- elb-predefined-security-policy-SSL-Überprüfung
- elb-tls-https-listeners-nur
- emr-kerberos-enabled
- emr-master-no-public-ip
- encrypted-volumes
- fms-webacl-resource-policy-überprüfen
- fms-webacl-rulegroup-association-überprüfen
- fsx-ontap-deployment-type-überprüfen
- fsx-openzfs-deployment-type-überprüfen
- glue-job-logging-enabled
- glue-ml-transform-encrypted-im Ruhezustand

- glue-spark-job-supported-Ausführung
- guardduty-enabled-centralized
- guardduty-non-archived-findings
- iam-customer-policy-blocked-kms-Aktionen
- iam-group-has-users-überprüfen
- iam-inline-policy-blocked-kms-Aktionen
- iam-no-inline-policy-überprüfen
- iam-password-policy
- iam-policy-blacklisted-check
- iam-policy-in-use
- iam-policy-no-statements-with-admin-access
- iam-policy-no-statements-with-full-access
- iam-role-managed-policy-überprüfen
- iam-root-access-key-überprüfen
- iam-user-group-membership-überprüfen
- iam-user-mfa-enabled
- iam-user-no-policies-überprüfen
- iam-user-unused-credentials-überprüfen
- incoming-ssh-disabled
- instances-in-vpc
- internet-gateway-authorized-vpc-nur
- kinesis-stream-backup-retention-überprüfen
- kinesis-stream-encrypted
- kms-cmk-not-scheduled-zum Löschen
- kms-key-policy-no-öffentlicher Zugang
- lambda-concurrency-check
- lambda-dlq-check
- lambda-function-public-access-verboten
- lambda-function-settings-check
- lambda-function-xray-enabled

- lambda-inside-vpc
- lambda-vpc-multi-az-überprüfen
- mfa-enabled-for-iam-Konsolenzugriff
- mq-active-deployment-mode
- mq-auto-minor-version-Upgrade aktiviert
- mq-rabbit-deployment-mode
- msk-cluster-public-access-deaktiviert
- msk-enhanced-monitoring-enabled
- msk-in-cluster-node-require-tls
- msk-unrestricted-access-check
- multi-region-cloud-trail-aktiviert
- nacl-no-unrestricted-ssh-rdp
- nlb-logging-enabled
- no-unrestricted-route-to-igw
- opensearch-update-check
- rabbit-mq-supported-version
- rds-automatic-minor-version-Upgrade aktiviert
- rds-enhanced-monitoring-enabled
- rds-instance-deletion-protection-aktiviert
- rds-instance-iam-authentication-aktiviert
- rds-instance-public-access-überprüfen
- rds-instance-subnet-igw-überprüfen
- rds-in-backup-plan
- rds-logging-enabled
- rds-multi-az-support
- rds-mysql-instance-encryptedunterwegs
- rds-postgresql-logs-to- Cloudwatch
- rds-postgres-instance-encryptedunterwegs
- rds-snapshots-public-prohibited
- rds-snapshot-encrypted

- rds-sqlserver-encrypted-in-im Transit
- rds-sql-server-logszur Cloud-Überwachung
- rds-storage-encrypted
- redshift-backup-enabled
- redshift-cluster-configuration-check
- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check
- redshift-cluster-multi-az-aktiviert
- redshift-cluster-public-access-überprüfen
- redshift-cluster-subnet-group-Multi-Az
- redshift-default-admin-check
- redshift-default-db-name-überprüfen
- redshift-enhanced-vpc-routing-aktiviert
- redshift-require-tls-ssl
- redshift-serverless-default-admin-überprüfen
- redshift-serverless-default-db-Namenscheck
- redshift-serverless-namespace-cmk-Verschlüsselung
- redshift-serverless-publish-logs-zu-Cloud-Watch
- required-tags
- restricted-incoming-traffic
- nur s3- access-point-in-vpc
- s3- -Blöcke access-point-public-access
- s3- -Blöcke account-level-public-access
- s3- -Blocke-periodisch account-level-public-access
- s 3- bucket-acl-prohibited
- s-3 bucket-blacklisted-actions-prohibited
- s3- bucket-cross-region-replication -aktiviert
- s-3 bucket-default-lock-enabled
- s3 bucket-level-public-access - verboten
- s3- bucket-logging-enabled

- s-3 bucket-mfa-delete-enabled
- s-3 bucket-policy-grantee-check
- s3- bucket-policy-not-more -freizügig
- s 3- bucket-public-read-prohibited
- s-3 bucket-public-write-prohibited
- s-3 bucket-replication-enabled
- s3- bucket-server-side-encryption -aktiviert
- s-3 bucket-ssl-requests-only
- s-3 bucket-versioning-enabled
- s-3 default-encryption-kms
- s-3 event-notifications-enabled
- s-3 lifecycle-policy-check
- s-3 version-lifecycle-policy-check
- sagemaker-endpoint-configuration-kms-key-konfiguriert
- sagemaker-notebook-instance-inside-vpc
- sagemaker-notebook-instance-kms-key-konfiguriert
- sagemaker-notebook-instance-platform-Version
- sagemaker-notebook-instance-root-Zugriffsprüfung
- sagemaker-notebook-no-direct-Internetzugang
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-überprüfen
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- securityhub-enabled
- security-account-information-provided
- service-vpc-endpoint-enabled
- sns-encrypted-kms
- sns-topic-message-delivery-Benachrichtigung aktiviert
- sns-topic-no-public-Zugriff

- sqs-queue-no-public-Zugang
- ssm-automation-block-public-teilen
- ssm-automation-logging-enabled
- ssm-document-not-public
- step-functions-state-machine-Protokollierung aktiviert
- subnet-auto-assign-public-ip-deaktiviert
- transfer-connector-logging-enabled
- vpc-default-security-group-geschlossen
- vpc-endpoint-enabled
- vpc-flow-logs-enabled
- vpc-network-acl-unused-überprüfen
- vpc-sg-open-only-to-authorized-ports
- wafv2-logging-enabled
- WAF 2- rulegroup-logging-enabled
- WAF 2- webacl-not-empty
- waf-regional-rule-not-leer
- waf-regional-webacl-not-leer

Region China (Ningxia)

China (Ningxia)

- access-keys-rotated
- account-part-of-organizations
- acm-certificate-expiration-check
- active-mq-supported-version
- alb-desync-mode-check
- alb-http-drop-invalid-Header-fähig
- alb-http-to-https-Umleitungsprüfung
- alb-waf-enabled
- api-gwv2- access-logs-enabled
- api-gwv2- authorization-type-configured

- api-gw-associated-with-WAF
- api-gw-cache-enabled-und-verschlüsselt
- api-gw-endpoint-type-überprüfen
- api-gw-execution-logging-aktiviert
- api-gw-ssl-enabled
- api-gw-xray-enabled
- approved-amis-by-id
- approved-amis-by-tag
- appsync-associated-with-waf
- appsync-authorization-check
- appsync-logging-enabled
- athena-workgroup-encrypted-at-ausruhen
- athena-workgroup-logging-enabled
- aurora-mysql-backtracking-enabled
- autoscaling-group-elb-healthcheck-erforderlich
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-hop-Grenze
- autoscaling-launch-config-public-ip-deaktiviert
- autoscaling-launch-template
- autoscaling-multiple-az
- autoscaling-multiple-instance-types
- beanstalk-enhanced-health-reporting-aktiviert
- clb-desync-mode-check
- clb-multiple-az
- cloudformation-stack-drift-detection-überprüfen
- cloudformation-stack-notification-check
- cloudtrail-all-read-s3- data-event-check
- cloudtrail-all-write-s3- data-event-check
- Wolkenspur-S3- bucket-access-logging
- CloudTrail-S3- bucket-public-access-prohibited

- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-action-enabled-überprüfen
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted
- cloud-trail-cloud-watch-logs-aktiviert
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-Validierung aktiviert
- cmk-backing-key-rotation-aktiviert
- codebuild-project-environment-privileged-überprüfen
- codebuild-project-envvar-awscred-überprüfen
- codebuild-project-logging-enabled
- codebuild-project-s3-log-verschlüsselt
- codebuild-project-source-repo-URL-Prüfung
- codebuild-report-group-encrypted-im Ruhezustand
- custom-eventbus-policy-attached
- cw-loggroup-retention-period-überprüfen
- datasync-task-logging-enabled
- dax-encryption-enabled
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- dms-auto-minor-version-aktualisieren-Prüfung
- dms-endpoint-ssl-configured
- dms-replication-not-public
- dms-replication-task-sourcedb-Protokollierung
- dms-replication-task-targetdb-Protokollierung

- docdb-cluster-audit-logging-aktiviert
- docdb-cluster-backup-retention-überprüfen
- docdb-cluster-deletion-protection-aktiviert
- docdb-cluster-encrypted
- docdb-cluster-encrypted-in-Transit
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-pitr-enabled
- dynamodb-table-deletion-protection-aktiviert
- dynamodb-table-encrypted-kms
- dynamodb-throughput-limit-check
- ebs-in-backup-plan
- ebs-optimized-instance
- ebs-snapshot-public-restorable-überprüfen
- ec2- ebs-encryption-by-default
- ec2- aktiviert enis-source-destination-check
- ec2-imdsv2-check
- ec2- instance-detailed-monitoring-enabled
- ec2-ami instance-launched-with-allowed
- ec2- instance-managed-by-ssm
- ec2- instance-multiple-eni-check
- ec2- instance-no-public-ip
- ec2- instance-profile-attached
- ec2-2-prüfen launch-template-imdsv
- ec2- -deaktiviert launch-template-public-ip
- ec2- managedinstance-applications-blacklisted
- ec2- managedinstance-applications-required
- ec2- prüfen managedinstance-association-compliance-status
- ec2- managedinstance-inventory-blacklisted
- ec2- prüfen managedinstance-patch-compliance-status

- ec2- managedinstance-platform-check
- ec2-eni security-group-attached-to
- ec2- - spot-fleet-request-ct encryption-at-rest
- ec2-stopped-instance
- ec2- volume-inuse-check
- ecr-private-lifecycle-policy-konfiguriert
- ecr-private-tag-immutability-aktiviert
- ecr-repository-cmk-encryption-aktiviert
- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-container-insights-enabled
- ecs-fargate-latest-platform-Version
- ecs-no-environment-secrets
- ecs-task-definition-log-Konfiguration
- ecs-task-definition-network-mode-not-host
- ecs-task-definition-pid-Modus-Überprüfung
- ecs-task-definition-user-for-host-mode-check
- efs-automatic-backups-enabled
- efs-encrypted-check
- efs-filesystem-ct-encrypted
- efs-in-backup-plan
- eip-attached
- eks-cluster-log-enabled
- eks-cluster-supported-version
- eks-endpoint-no-public-Zugang
- eks-secrets-encrypted
- elasticache-auto-minor-version-aktualisieren-Prüfung
- elasticache-redis-cluster-automatic-Backup-Check
- elasticache-repl-grp-auto-failover-fähig
- elasticache-repl-grp-encrypted-im Ruhezustand

- elasticache-repl-grp-encryptedim Transit
- elasticache-repl-grp-redis-auth-aktiviert
- elasticache-subnet-group-check
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch
- elasticsearch-node-to-node-Verschlüsselungsprüfung
- elastic-beanstalk-managed-updates-aktiviert
- elbv2- acm-certificate-required
- elv 2- listener-encryption-in-transit
- elbv2-multiple-az
- elb-acm-certificate-required
- elb-cross-zone-load-Balancing aktiviert
- elb-custom-security-policy-ssl-Prüfung
- elb-deletion-protection-enabled
- elb-logging-enabled
- elb-predefined-security-policy-SSL-Überprüfung
- elb-tls-https-listeners-nur
- emr-kerberos-enabled
- emr-master-no-public-ip
- encrypted-volumes
- fms-webacl-resource-policy-überprüfen
- fms-webacl-rulegroup-association-überprüfen
- fsx-ontap-deployment-type-überprüfen
- fsx-openzfs-deployment-type-überprüfen
- glue-job-logging-enabled
- glue-spark-job-supported-Ausführung
- guardduty-enabled-centralized
- guardduty-non-archived-findings
- iam-customer-policy-blocked-kms-Aktionen

- iam-group-has-users-überprüfen
- iam-inline-policy-blocked-kms-Aktionen
- iam-no-inline-policy-überprüfen
- iam-password-policy
- iam-policy-blacklisted-check
- iam-policy-in-use
- iam-policy-no-statements-with-admin-access
- iam-policy-no-statements-with-full-access
- iam-role-managed-policy-überprüfen
- iam-root-access-key-überprüfen
- iam-user-group-membership-überprüfen
- iam-user-mfa-enabled
- iam-user-no-policies-überprüfen
- iam-user-unused-credentials-überprüfen
- incoming-ssh-disabled
- instances-in-vpc
- internet-gateway-authorized-vpc-nur
- kinesis-stream-backup-retention-überprüfen
- kinesis-stream-encrypted
- kms-cmk-not-scheduled-zum Löschen
- kms-key-policy-no-öffentlicher Zugang
- mfa-enabled-for-iam-Konsolenzugriff
- mq-active-deployment-mode
- mq-auto-minor-version-Upgrade aktiviert
- mq-rabbit-deployment-mode
- msk-cluster-public-access-deaktiviert
- msk-enhanced-monitoring-enabled
- msk-in-cluster-node-require-tls
- msk-unrestricted-access-check
- multi-region-cloud-trail-aktiviert

- nacl-no-unrestricted-ssh-rdp
- neptune-cluster-backup-retention-überprüfen
- neptune-cluster-cloudwatch-log-exportfähig
- neptune-cluster-copy-tags-to-snapshot-enabled
- neptune-cluster-deletion-protection-aktiviert
- neptune-cluster-encrypted
- neptune-cluster-iam-database-Authentifizierung
- neptune-cluster-multi-az-aktiviert
- neptune-cluster-snapshot-encrypted
- no-unrestricted-route-to-igw
- opensearch-update-check
- rabbit-mq-supported-version
- rds-aurora-mysql-audit-Protokollierung aktiviert
- rds-aurora-postgresql-logs-zu-Cloud-Watch
- rds-automatic-minor-version-upgrade-fähig
- rds-cluster-auto-minor-version-upgrade-enable
- rds-cluster-deletion-protection-aktiviert
- rds-cluster-encrypted-at-ausruhen
- rds-cluster-iam-authentication-aktiviert
- rds-cluster-multi-az-aktiviert
- rds-enhanced-monitoring-enabled
- rds-instance-deletion-protection-aktiviert
- rds-instance-iam-authentication-aktiviert
- rds-instance-public-access-überprüfen
- rds-instance-subnet-igw-überprüfen
- rds-in-backup-plan
- rds-logging-enabled
- rds-multi-az-support
- rds-mysql-instance-encryptedunterwegs
- rds-postgresql-logs-to- Cloudwatch

- rds-postgres-instance-encryptedunterwegs
- rds-snapshots-public-prohibited
- rds-snapshot-encrypted
- rds-sqlserver-encrypted-in-im Transit
- rds-sql-server-logszur Cloud-Überwachung
- rds-storage-encrypted
- redshift-backup-enabled
- redshift-cluster-configuration-check
- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check
- redshift-cluster-multi-az-aktiviert
- redshift-cluster-public-access-überprüfen
- redshift-cluster-subnet-group-Multi-Az
- redshift-default-admin-check
- redshift-default-db-name-überprüfen
- redshift-enhanced-vpc-routing-aktiviert
- redshift-require-tls-ssl
- redshift-serverless-default-admin-überprüfen
- redshift-serverless-default-db-Namenscheck
- redshift-serverless-namespace-cmk-Verschlüsselung
- redshift-serverless-publish-logs-zu-Cloud-Watch
- required-tags
- restricted-incoming-traffic
- nur s3- access-point-in-vpc
- s3- -Blöcke access-point-public-access
- s3- -Blöcke account-level-public-access
- s3- -Blocke-periodisch account-level-public-access
- s 3- bucket-acl-prohibited
- s-3 bucket-blacklisted-actions-prohibited
- s3- bucket-cross-region-replication -aktiviert

- s-3 bucket-default-lock-enabled
- s3 bucket-level-public-access - verboten
- s3- bucket-logging-enabled
- s-3 bucket-mfa-delete-enabled
- s-3 bucket-policy-grantee-check
- s3- bucket-policy-not-more -freizügig
- s 3- bucket-public-read-prohibited
- s-3 bucket-public-write-prohibited
- s-3 bucket-replication-enabled
- s3- bucket-server-side-encryption -aktiviert
- s-3 bucket-ssl-requests-only
- s-3 bucket-versioning-enabled
- s-3 default-encryption-kms
- s-3 event-notifications-enabled
- s-3 lifecycle-policy-check
- s-3 version-lifecycle-policy-check
- sagemaker-endpoint-configuration-kms-key-konfiguriert
- sagemaker-notebook-instance-inside-vpc
- sagemaker-notebook-instance-kms-key-konfiguriert
- sagemaker-notebook-instance-platform-Version
- sagemaker-notebook-instance-root-Zugriffsprüfung
- sagemaker-notebook-no-direct-Internetzugang
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-überprüfen
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- securityhub-enabled
- security-account-information-provided
- service-vpc-endpoint-enabled

- sns-encrypted-kms
- sns-topic-message-delivery-Benachrichtigung aktiviert
- sns-topic-no-public-Zugriff
- sqs-queue-no-public-Zugang
- ssm-automation-block-public-teilen
- ssm-automation-logging-enabled
- ssm-document-not-public
- step-functions-state-machine-Protokollierung aktiviert
- subnet-auto-assign-public-ip-deaktiviert
- transfer-connector-logging-enabled
- vpc-default-security-group-geschlossen
- vpc-endpoint-enabled
- vpc-flow-logs-enabled
- vpc-network-acl-unused-überprüfen
- vpc-sg-open-only-to-authorized-ports
- vpc-sg-port-restriction-überprüfen
- wafv2-logging-enabled
- WAF 2- rulegroup-logging-enabled
- WAF 2- webacl-not-empty
- waf-regional-rule-not-leer
- waf-regional-webacl-not-leer
- workspaces-root-volume-encryption-aktiviert
- workspaces-user-volume-encryption-aktiviert

Region Europa (Frankfurt)

Europa (Frankfurt)

- access-keys-rotated
- account-part-of-organizations
- acmpca-certificate-authority-tagged
- acm-certificate-expiration-check

- acm-certificate-rsa-check
- acm-pca-root-ca-deaktiviert
- active-mq-supported-version
- alb-desync-mode-check
- alb-http-drop-invalid-Header-fähig
- alb-http-to-https-Umleitungsprüfung
- alb-internal-scheme-check
- alb-listener-tagged
- alb-waf-enabled
- amplify-app-branch-auto-löschung aktiviert
- amplify-app-description
- amplify-app-tagged
- amplify-branch-performance-mode-aktiviert
- amplify-branch-tagged
- api-gwv2- access-logs-enabled
- api-gwv2- authorization-type-configured
- api-gw-associated-with-WAF
- api-gw-cache-enabled-und-verschlüsselt
- api-gw-endpoint-type-überprüfen
- api-gw-execution-logging-aktiviert
- api-gw-ssl-enabled
- api-gw-xray-enabled
- appconfig-application-description
- appconfig-application-tagged
- appconfig-configuration-profile-tagged
- appconfig-configuration-profile-validators-nicht leer
- appconfig-deployment-strategy-description
- appconfig-deployment-strategy-replicate-zu-ssm
- appconfig-environment-description
- appconfig-environment-tagged

- appconfig-extension-association-tagged
- appconfig-freeform-profile-config-Speicher
- appconfig-hosted-configuration-version-Beschreibung
- appflow-flow-tagged
- appintegrations-event-integration-description
- appintegrations-event-integration-tagged
- appmesh-gateway-route-tagged
- appmesh-mesh-deny-tcp-Weiterleitung
- appmesh-mesh-tagged
- appmesh-route-tagged
- appmesh-virtual-gateway-backend-Standardeinstellungen-TLS
- appmesh-virtual-gateway-logging-file-path-exists
- appmesh-virtual-gateway-tagged
- appmesh-virtual-node-backend-defaults-tls-on
- appmesh-virtual-node-logging-file-path-exists
- appmesh-virtual-node-tagged
- appmesh-virtual-router-tagged
- appmesh-virtual-service-tagged
- approved-amis-by-id
- approved-amis-by-tag
- apprunner-service-in-vpc
- apprunner-service-no-public-Zugang
- apprunner-service-observability-enabled
- apprunner-service-tagged
- apprunner-vpc-connector-tagged
- appstream-fleet-in-vpc
- appsync-associated-with-waf
- appsync-authorization-check
- appsync-cache-ct-encryption-im Ruhezustand
- appsync-cache-ct-encryptionim Transit

- appsync-cache-encryption-at-ausruhen
- appsync-logging-enabled
- athena-data-catalog-description
- athena-prepared-statement-description
- athena-workgroup-description
- athena-workgroup-encrypted-at-ausruhen
- athena-workgroup-enforce-workgroup-Konfiguration
- athena-workgroup-engine-version-automatisches Upgrade
- athena-workgroup-logging-enabled
- aurora-last-backup-recovery-Punkt erstellt
- aurora-meets-restore-time-Ziel
- aurora-mysql-backtracking-enabled
- aurora-mysql-cluster-audit-Protokollierung
- aurora-resources-in-logically-air-gapped-vault
- aurora-resources-protected-by-Backup-Plan
- autoscaling-capacity-rebalancing
- autoscaling-group-elb-healthcheck-erforderlich
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-hop-Grenze
- autoscaling-launch-config-public-ip-deaktiviert
- autoscaling-launch-template
- autoscaling-multiple-az
- autoscaling-multiple-instance-types
- backup-plan-min-frequency-and-min-retention-check
- backup-recovery-point-encrypted
- backup-recovery-point-manual-Löschen-deaktiviert
- backup-recovery-point-minimum-Aufbewahrungsprüfung
- batch-compute-environment-enabled
- batch-compute-environment-managed
- batch-compute-environment-tagged

- batch-job-queue-enabled
- batch-job-queue-tagged
- batch-managed-compute-environment-using-launch-template
- batch-managed-compute-env-compute-resources-tagged
- batch-scheduling-policy-tagged
- beanstalk-enhanced-health-reporting-aktiviert
- cassandra-keyspace-tagged
- clb-desync-mode-check
- clb-multiple-az
- cloudformation-stack-drift-detection-überprüfen
- cloudformation-stack-notification-check
- cloudtrail-all-read-s3- data-event-check
- cloudtrail-all-write-s3- data-event-check
- Wolkenspur-S3- bucket-access-logging
- CloudTrail-S3- bucket-public-access-prohibited
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-action-enabled-überprüfen
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted
- cloud-trail-cloud-watch-logs-aktiviert
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-Validierung aktiviert
- cmk-backing-key-rotation-aktiviert
- codebuild-project-artifact-encryption
- codebuild-project-environment-privileged-überprüfen
- codebuild-project-envvar-awscred-überprüfen

- codebuild-project-logging-enabled
- codebuild-project-s3-log-verschlüsselt
- codebuild-project-source-repo-URL-Prüfung
- codebuild-report-group-encrypted-im Ruhezustand
- codedeploy-auto-rollback-monitor-aktiviert
- codedeploy-deployment-group-auto-rollback-aktiviert
- codedeploy-deployment-group-outdated-instanzen-aktualisieren
- Codedeploy-ec2- minimum-healthy-hosts-configured
- codedeploy-lambda-allatonce-traffic-shift-deaktiviert
- codeguruprofiler-profiling-group-tagged
- codegururevieweer-repository-association-tagged
- codepipeline-deployment-count-check
- codepipeline-region-fanout-check
- cognito-identity-pool-unauth-Zugriffsprüfung
- cognito-user-pool-advanced-sicherheitsaktiviert
- cognito-user-pool-tagged
- connect-instance-logging-enabled
- customerprofiles-object-type-allow-Profilerstellung
- customerprofiles-object-type-tagged
- custom-eventbus-policy-attached
- custom-schema-registry-policy-beigefügt
- cw-loggroup-retention-period-überprüfen
- datasync-task-data-verification-aktiviert
- datasync-task-logging-enabled
- datasync-task-tagged
- dax-encryption-enabled
- dax-tls-endpoint-encryption
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type

- dms-auto-minor-version-upgrade-check
- dms-endpoint-ssl-configured
- dms-endpoint-tagged
- dms-mongo-db-authentication-aktiviert
- dms-neptune-iam-authorization-aktiviert
- dms-redis-tls-enabled
- dms-replication-not-public
- dms-replication-task-sourcedb-Protokollierung
- dms-replication-task-tagged
- dms-replication-task-targetdb-Protokollierung
- docdb-cluster-audit-logging-aktiviert
- docdb-cluster-backup-retention-überprüfen
- docdb-cluster-deletion-protection-aktiviert
- docdb-cluster-encrypted
- docdb-cluster-encrypted-in-Transit
- docdb-cluster-snapshot-public-verboten
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-last-backup-recovery-Punkt erstellt
- dynamodb-meets-restore-time-Ziel
- dynamodb-pitr-enabled
- dynamodb-resources-protected-by-Backup-Plan
- dynamodb-table-deletion-protection-aktiviert
- dynamodb-table-encrypted-kms
- dynamodb-table-encryption-enabled
- dynamodb-throughput-limit-check
- ebs-in-backup-plan
- ebs-last-backup-recovery-punkt-erstellt
- ebs-meets-restore-time-Ziel
- ebs-optimized-instance

- ebs-resources-in-logically-air-gapped-vault
- ebs-resources-protected-by-Backup-Plan
- ebs-snapshot-public-restorable-überprüfen
- ec2- capacity-reservation-tagged
- ec2- carrier-gateway-tagged
- ec2- aktiviert client-vpn-connection-log
- ec2- client-vpn-endpoint-tagged
- ec2- -alle client-vpn-not-authorize
- ec2- dhcp-options-tagged
- ec2- ebs-encryption-by-default
- ec2- aktiviert enis-source-destination-check
- ec2-fleet-markiert
- ec2-imdsv2-check
- ec2- instance-detailed-monitoring-enabled
- ec2-ami instance-launched-with-allowed
- ec2- instance-managed-by-ssm
- ec2- instance-multiple-eni-check
- ec2- instance-no-public-ip
- ec2- instance-profile-attached
- ec2- erstellt last-backup-recovery-point
- ec2-2-prüfen launch-template-imdsv
- ec2- -deaktiviert launch-template-public-ip
- ec2- launch-template-tagged
- ec2- managedinstance-applications-blacklisted
- ec2- managedinstance-applications-required
- ec2- prüfen managedinstance-association-compliance-status
- ec2- managedinstance-inventory-blacklisted
- ec2- prüfen managedinstance-patch-compliance-status
- ec2- managedinstance-platform-check
- ec2- meets-restore-time-target

- ec2- Analyse mit Schlagwörtern network-insights-access-scope
- ec2 network-insights-access-scope - markiert
- ec2- network-insights-path-tagged
- ec2- no-amazon-key-pair
- ec2- paravirtual-instance-check
- ec2- prefix-list-tagged
- ec2- -Tresor mit Lücken resources-in-logically-air
- ec2- resources-protected-by-backup -plan
- ec2- -eni security-group-attached-to
- ec2- -eni-periodisch security-group-attached-to
- ec2-stopped-instance
- ec2- token-hop-limit-check
- ec2- traffic-mirror-filter-description
- ec2- traffic-mirror-filter-tagged
- ec2- traffic-mirror-session-description
- ec2- traffic-mirror-session-tagged
- ec2- traffic-mirror-target-description
- ec2- traffic-mirror-target-tagged
- ec2- -attach-deaktiviert transit-gateway-auto-vpc
- ec2 transit-gateway-multicast-domain - markiert
- ec2- volume-inuse-check
- ec2- vpn-connection-logging-enabled
- ecr-private-image-scanning-aktiviert
- ecr-private-lifecycle-policy-konfiguriert
- ecr-private-tag-immutability-aktiviert
- ecr-repository-cmk-encryption-aktiviert
- ecr-repository-tagged
- ecs-awsvpc-networking-enabled
- ecs-containers-nonprivileged
- ecs-containers-readonly-access

- ecs-container-insights-enabled
- ecs-fargate-latest-platform-Version
- ecs-no-environment-secrets
- ecs-task-definition-log-Konfiguration
- ecs-task-definition-memory-hartes Limit
- ecs-task-definition-network-mode-not-host
- ecs-task-definition-nonroot-Benutzer
- ecs-task-definition-pid-Modus-Check
- ecs-task-definition-user-for-host-mode-check
- efs-access-point-enforce-Stammverzeichnis
- efs-access-point-enforce-Benutzeridentität
- efs-automatic-backups-enabled
- efs-encrypted-check
- efs-filesystem-ct-encrypted
- efs-in-backup-plan
- efs-last-backup-recovery-Punkt erstellt
- efs-meets-restore-time-Ziel
- efs-mount-target-public-zugänglich
- efs-resources-in-logically-air-gapped-vault
- efs-resources-protected-by-Ersatzplan
- eip-attached
- eks-cluster-logging-enabled
- eks-cluster-log-enabled
- eks-cluster-oldest-supported-Ausführung
- eks-cluster-secrets-encrypted
- eks-cluster-supported-version
- eks-endpoint-no-public-Zugang
- eks-secrets-encrypted
- elasticache-auto-minor-version-aktualisieren-Prüfung
- elasticache-rbac-auth-enabled

- elasticache-redis-cluster-automatic-Backup-Check
- elasticache-repl-grp-auto-failover-fähig
- elasticache-repl-grp-encrypted-im Ruhezustand
- elasticache-repl-grp-encryptedim Transit
- elasticache-repl-grp-redis-auth-aktiviert
- elasticache-subnet-group-check
- elasticache-supported-engine-version
- elasticbeanstalk-application-description
- elasticbeanstalk-application-version-description
- elasticbeanstalk-environment-description
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch
- elasticsearch-node-to-node-Verschlüsselungsprüfung
- elastic-beanstalk-logs-to- Cloudwatch
- elastic-beanstalk-managed-updates-aktiviert
- elbv2- acm-certificate-required
- elv 2- listener-encryption-in-transit
- elbv2-multiple-az
- elbv2- prüfen predefined-security-policy-ssl
- elb-acm-certificate-required
- elb-cross-zone-load-Balancing aktiviert
- elb-custom-security-policy-ssl-Prüfung
- elb-deletion-protection-enabled
- elb-logging-enabled
- elb-predefined-security-policy-ssl-Überprüfung
- elb-tls-https-listeners-nur
- emr-block-public-access
- emr-kerberos-enabled
- emr-master-no-public-ip

- emr-security-configuration-encryption-ruh dich aus
- emr-security-configuration-encryption-Transit
- encrypted-volumes
- event-data-store-cmk-Verschlüsselung aktiviert
- evidently-launch-description
- evidently-launch-tagged
- evidently-project-description
- evidently-project-tagged
- evidently-segment-description
- evidently-segment-tagged
- fis-experiment-template-log-Konfiguration ist vorhanden
- fis-experiment-template-tagged
- fms-shield-resource-policy-überprüfen
- fms-webacl-resource-policy-überprüfen
- fms-webacl-rulegroup-association-überprüfen
- fsx-last-backup-recovery-Punkt erstellt
- fsx-lustre-copy-tagszu Backups
- fsx-meets-restore-time-Ziel
- fsx-ontap-deployment-type-überprüfen
- fsx-openzfs-copy-tags-aktiviert
- fsx-openzfs-deployment-type-überprüfen
- fsx-resources-protected-by-Backup-Plan
- fsx-windows-audit-log-konfiguriert
- fsx-windows-deployment-type-überprüfen
- glb-listener-tagged
- global-endpoint-event-replication-aktiviert
- glue-job-logging-enabled
- glue-ml-transform-encrypted-im Ruhezustand
- glue-spark-job-supported-Ausführung
- GuardDuty-EC2- protection-runtime-enabled

- guardduty-ecs-protection-runtime-aktiviert
- guardduty-eks-protection-audit-aktiviert
- guardduty-eks-protection-runtime-aktiviert
- guardduty-enabled-centralized
- guardduty-lambda-protection-enabled
- guardduty-malware-protection-enabled
- guardduty-non-archived-findings
- guardduty-rds-protection-enabled
- guardduty-runtime-monitoring-enabled
- GuardDuty-S3-Schutz aktiviert
- iam-customer-policy-blocked-kms-Aktionen
- iam-external-access-analyzer-aktiviert
- iam-group-has-users-überprüfen
- iam-inline-policy-blocked-kms-Aktionen
- iam-no-inline-policy-überprüfen
- iam-password-policy
- iam-policy-blacklisted-check
- iam-policy-in-use
- iam-policy-no-statements-with-admin-access
- iam-policy-no-statements-with-full-access
- iam-role-managed-policy-überprüfen
- iam-root-access-key-überprüfen
- iam-user-group-membership-überprüfen
- iam-user-mfa-enabled
- iam-user-no-policies-überprüfen
- iam-user-unused-credentials-überprüfen
- incoming-ssh-disabled
- inspector-ec2-Scan aktiviert
- inspector-ecr-scan-enabled
- inspector-lambda-code-scan-aktiviert

- inspector-lambda-standard-scan-aktiviert
- instances-in-vpc
- internet-gateway-authorized-vpc-nur
- iotevents-alarm-model-tagged
- iotevents-detector-model-tagged
- iotevents-input-tagged
- iotsitewise-asset-model-tagged
- iotsitewise-dashboard-tagged
- iotsitewise-gateway-tagged
- iotsitewise-portal-tagged
- iotsitewise-project-tagged
- iottwinmaker-component-type-tagged
- iottwinmaker-entity-tagged
- iottwinmaker-scene-tagged
- iottwinmaker-sync-job-tagged
- iottwinmaker-workspace-tagged
- iotwireless-fuota-task-tagged
- iotwireless-multicast-group-tagged
- iotwireless-service-profile-tagged
- iot-authorizer-token-signing-aktiviert
- ivs-channel-playback-authorization-aktiviert
- ivs-channel-tagged
- ivs-playback-key-pair-markiert
- ivs-recording-configuration-tagged
- kinesis-firehose-delivery-stream-verschlüsselt
- kinesis-stream-backup-retention-überprüfen
- kinesis-stream-encrypted
- kms-cmk-not-scheduled-zum Löschen
- kms-key-policy-no-öffentlicher Zugang
- lambda-concurrency-check

- lambda-dlq-check
- lambda-function-public-access-verboten
- lambda-function-settings-check
- lambda-function-xray-enabled
- lambda-inside-vpc
- lambda-vpc-multi-az-überprüfen
- lightsail-bucket-tagged
- lightsail-certificate-tagged
- lightsail-disk-tagged
- macie-auto-sensitive-data-Discovery-Check
- macie-status-check
- mariadb-publish-logs-to-Cloudwatch-Protokolle
- mfa-enabled-for-iam-Konsolenzugriff
- mq-active-broker-ldap-Authentifizierung
- mq-active-deployment-mode
- mq-active-single-instance-broker-storage-type-efs
- mq-automatic-minor-version-Upgrade aktiviert
- mq-auto-minor-version-upgrade-fähig
- mq-broker-general-logging-aktiviert
- mq-cloudwatch-audit-logging-aktiviert
- mq-cloudwatch-audit-log-aktiviert
- mq-no-public-access
- mq-rabbit-deployment-mode
- msk-cluster-public-access-deaktiviert
- msk-connect-connector-logging-aktiviert
- msk-enhanced-monitoring-enabled
- msk-in-cluster-node-require-tls
- msk-unrestricted-access-check
- multi-region-cloud-trail-aktiviert
- nacl-no-unrestricted-ssh-rdp

- neptune-cluster-backup-retention-überprüfen
- neptune-cluster-cloudwatch-log-exportfähig
- neptune-cluster-copy-tags-to-snapshot-enabled
- neptune-cluster-deletion-protection-aktiviert
- neptune-cluster-encrypted
- neptune-cluster-iam-database-Authentifizierung
- neptune-cluster-multi-az-aktiviert
- neptune-cluster-snapshot-encrypted
- neptune-cluster-snapshot-public-verboten
- netfw-deletion-protection-enabled
- netfw-logging-enabled
- netfw-multi-az-enabled
- netfw-policy-default-action-fragment-Pakete
- netfw-policy-default-action-vollständige Pakete
- netfw-policy-rule-group-assoziiert
- netfw-stateless-rule-group-nicht leer
- netfw-subnet-change-protection-aktiviert
- nlb-cross-zone-load-Balancing aktiviert
- nlb-internal-scheme-check
- nlb-listener-tagged
- nlb-logging-enabled
- no-unrestricted-route-to-igw
- opensearch-access-control-enabled
- opensearch-audit-logging-enabled
- opensearch-data-node-fault-Toleranz
- opensearch-encrypted-at-rest
- opensearch-https-required
- opensearch-in-vpc-only
- opensearch-logs-to-cloudwatch
- opensearch-node-to-node-Verschlüsselungsprüfung

- opensearch-primary-node-fault-Toleranz
- opensearch-update-check
- rabbit-mq-supported-version
- rds-aurora-mysql-audit-Protokollierung aktiviert
- rds-aurora-postgresql-logs-zu-Cloud-Watch
- rds-automatic-minor-version-upgrade-fähig
- rds-cluster-auto-minor-version-upgrade-enable
- rds-cluster-default-admin-überprüfen
- rds-cluster-deletion-protection-aktiviert
- rds-cluster-encrypted-at-ausruhen
- rds-cluster-iam-authentication-aktiviert
- rds-cluster-multi-az-aktiviert
- rds-enhanced-monitoring-enabled
- rds-instance-default-admin-überprüfen
- rds-instance-deletion-protection-aktiviert
- rds-instance-iam-authentication-aktiviert
- rds-instance-public-access-überprüfen
- rds-instance-subnet-igw-überprüfen
- rds-in-backup-plan
- rds-last-backup-recovery-Punkt erstellt
- rds-logging-enabled
- rds-mariadb-instance-encryptedwährend des Transports
- rds-meets-restore-time-Ziel
- rds-multi-az-support
- rds-mysql-instance-encryptedim Transit
- rds-postgresql-logs-to- Cloudwatch
- rds-postgres-instance-encryptedunterwegs
- rds-proxy-tls-encryption
- rds-resources-protected-by-Backup-Plan
- rds-snapshots-public-prohibited

- rds-snapshot-encrypted
- rds-sqlserver-encrypted-in-Transit
- rds-sql-server-logszur Cloud-Überwachung
- rds-storage-encrypted
- redshift-audit-logging-enabled
- redshift-backup-enabled
- redshift-cluster-configuration-check
- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check
- redshift-cluster-multi-az-aktiviert
- redshift-cluster-parameter-group-markiert
- redshift-cluster-public-access-überprüfen
- redshift-cluster-subnet-group-Multi-Az
- redshift-default-admin-check
- redshift-default-db-name-überprüfen
- redshift-enhanced-vpc-routing-aktiviert
- redshift-require-tls-ssl
- redshift-serverless-default-admin-überprüfen
- redshift-serverless-default-db-Namenscheck
- redshift-serverless-namespace-cmk-Verschlüsselung
- redshift-serverless-publish-logs-zu-Cloud-Watch
- redshift-serverless-workgroup-encryptedauf dem Weg
- redshift-serverless-workgroup-no-öffentlich zugänglich
- redshift-serverless-workgroup-routes-innerhalb von VPC
- redshift-unrestricted-port-access
- required-tags
- restricted-incoming-traffic
- root-account-hardware-mfa-aktiviert
- root-account-mfa-enabled
- nur s3- access-point-in-vpc

- s3- -Blöcke access-point-public-access
- s3- -Blöcke account-level-public-access
- s3- -Blocke-periodisch account-level-public-access
- s 3- bucket-acl-prohibited
- s-3 bucket-blacklisted-actions-prohibited
- s3- bucket-cross-region-replication -aktiviert
- s-3 bucket-default-lock-enabled
- s3 bucket-level-public-access - verboten
- s3- bucket-logging-enabled
- s-3 bucket-mfa-delete-enabled
- s-3 bucket-policy-grantee-check
- s3- bucket-policy-not-more -freizügig
- s 3- bucket-public-read-prohibited
- s-3 bucket-public-write-prohibited
- s-3 bucket-replication-enabled
- s3- bucket-server-side-encryption -aktiviert
- s-3 bucket-ssl-requests-only
- s3-Bucket-Tagged
- s-3 bucket-versioning-enabled
- s-3 default-encryption-kms
- s-3 event-notifications-enabled
- s3 last-backup-recovery-point - erstellt
- s3- lifecycle-policy-check
- s-3 meets-restore-time-target
- s3- resources-in-logically-air -Tresor mit Lücken
- s3 resources-protected-by-backup - -Plan
- s 3- version-lifecycle-policy-check
- sagemaker-app-image-config-markiert
- sagemaker-domain-in-vpc
- sagemaker-domain-tagged

- sagemaker-endpoint-configuration-kms-schlüsselkonfiguriert
- sagemaker-endpoint-config-prod-Anzahl der Instanzen
- sagemaker-feature-group-tagged
- sagemaker-image-description
- sagemaker-image-tagged
- sagemaker-model-in-vpc
- sagemaker-model-isolation-enabled
- sagemaker-notebook-instance-inside-vpc
- sagemaker-notebook-instance-kms-key-konfiguriert
- sagemaker-notebook-instance-platform-Version
- sagemaker-notebook-instance-root-Zugriffsprüfung
- sagemaker-notebook-no-direct-Internetzugang
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-überprüfen
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- securityhub-enabled
- security-account-information-provided
- service-catalog-shared-within-Organisation
- service-vpc-endpoint-enabled
- sns-encrypted-kms
- sns-topic-message-delivery-Benachrichtigung aktiviert
- sns-topic-no-public-Zugriff
- sqs-queue-no-public-Zugang
- ssm-automation-block-public-teilen
- ssm-automation-logging-enabled
- ssm-document-not-public
- ssm-document-tagged
- step-functions-state-machine-Protokollierung aktiviert

- storagegateway-last-backup-recovery-punkt-erstellt
- storagegateway-resources-in-logically-air-gapped-vault
- storagegateway-resources-protected-by-Ersatzplan
- subnet-auto-assign-public-ip-deaktiviert
- transfer-agreement-description
- transfer-agreement-tagged
- transfer-certificate-description
- transfer-certificate-tagged
- transfer-connector-logging-enabled
- transfer-connector-tagged
- transfer-family-server-no-ftp
- transfer-profile-tagged
- transfer-workflow-description
- transfer-workflow-tagged
- virtualmachine-last-backup-recovery-punkt-erstellt
- virtualmachine-resources-in-logically-air-gapped-vault
- virtualmachine-resources-protected-by-Ersatzplan
- vpc-default-security-group-geschlossen
- vpc-endpoint-enabled
- vpc-flow-logs-enabled
- vpc-network-acl-unused-überprüfen
- vpc-peering-dns-resolution-überprüfen
- vpc-sg-open-only-to-authorized-ports
- vpc-sg-port-restriction-überprüfen
- vpc-vpn-2-tunnels-up
- wafv2-logging-enabled
- WAF 2- rulegroup-logging-enabled
- WAF 2- rulegroup-not-empty
- WAF 2- webacl-not-empty
- waf-regional-rulegroup-not-leer

- waf-regional-rule-not-leer
- waf-regional-webacl-not-leer
- workspaces-root-volume-encryption-aktiviert
- workspaces-user-volume-encryption-aktiviert

Region Europa (Irland)

Europa (Irland)

- access-keys-rotated
- account-part-of-organizations
- acmpca-certificate-authority-tagged
- acm-certificate-expiration-check
- acm-certificate-rsa-check
- acm-pca-root-ca-deaktiviert
- active-mq-supported-version
- alb-desync-mode-check
- alb-http-drop-invalid-Header-fähig
- alb-http-to-https-Umleitungsprüfung
- alb-internal-scheme-check
- alb-listener-tagged
- alb-waf-enabled
- amplify-app-branch-auto-löschung aktiviert
- amplify-app-description
- amplify-app-tagged
- amplify-branch-performance-mode-aktiviert
- amplify-branch-tagged
- api-gwv2- access-logs-enabled
- api-gwv2- authorization-type-configured
- api-gw-associated-with-WAF
- api-gw-cache-enabled-und-verschlüsselt
- api-gw-endpoint-type-überprüfen

- api-gw-execution-logging-aktiviert
- api-gw-ssl-enabled
- api-gw-xray-enabled
- appconfig-application-description
- appconfig-application-tagged
- appconfig-configuration-profile-tagged
- appconfig-configuration-profile-validators-nicht leer
- appconfig-deployment-strategy-description
- appconfig-deployment-strategy-replicate-zu-ssm
- appconfig-environment-description
- appconfig-environment-tagged
- appconfig-extension-association-tagged
- appconfig-freeform-profile-config-Speicher
- appconfig-hosted-configuration-version-Beschreibung
- appflow-flow-tagged
- appmesh-gateway-route-tagged
- appmesh-mesh-deny-tcp-Weiterleitung
- appmesh-mesh-tagged
- appmesh-route-tagged
- appmesh-virtual-gateway-backend-Standardeinstellungen-TLS
- appmesh-virtual-gateway-logging-file-path-exists
- appmesh-virtual-gateway-tagged
- appmesh-virtual-node-backend-defaults-tls-on
- appmesh-virtual-node-logging-file-path-exists
- appmesh-virtual-node-tagged
- appmesh-virtual-router-tagged
- appmesh-virtual-service-tagged
- approved-amis-by-id
- approved-amis-by-tag
- apprunner-service-in-vpc

- apprunner-service-no-public-Zugang
- apprunner-service-observability-enabled
- apprunner-service-tagged
- apprunner-vpc-connector-tagged
- appstream-fleet-in-vpc
- appsync-associated-with-waf
- appsync-authorization-check
- appsync-cache-encryption-at-ausruhen
- appsync-logging-enabled
- athena-data-catalog-description
- athena-prepared-statement-description
- athena-workgroup-description
- athena-workgroup-encrypted-at-ausruhen
- athena-workgroup-enforce-workgroup-Konfiguration
- athena-workgroup-engine-version-automatisches Upgrade
- athena-workgroup-logging-enabled
- aurora-last-backup-recovery-Punkt erstellt
- aurora-meets-restore-time-Ziel
- aurora-mysql-backtracking-enabled
- aurora-mysql-cluster-audit-Protokollierung
- aurora-resources-in-logically-air-gapped-vault
- aurora-resources-protected-by-Backup-Plan
- autoscaling-capacity-rebalancing
- autoscaling-group-elb-healthcheck-erforderlich
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-hop-Grenze
- autoscaling-launch-config-public-ip-deaktiviert
- autoscaling-launch-template
- autoscaling-multiple-az
- autoscaling-multiple-instance-types

- backup-plan-min-frequency-and-min-retention-check
- backup-recovery-point-encrypted
- backup-recovery-point-manual-Löschen-deaktiviert
- backup-recovery-point-minimum-Aufbewahrungsprüfung
- batch-compute-environment-enabled
- batch-compute-environment-managed
- batch-compute-environment-tagged
- batch-job-queue-enabled
- batch-job-queue-tagged
- batch-managed-compute-environment-using-launch-template
- batch-managed-compute-env-compute-resources-tagged
- batch-scheduling-policy-tagged
- beanstalk-enhanced-health-reporting-aktiviert
- cassandra-keyspace-tagged
- clb-desync-mode-check
- clb-multiple-az
- cloudformation-stack-drift-detection-überprüfen
- cloudformation-stack-notification-check
- cloudtrail-all-read-s3- data-event-check
- cloudtrail-all-write-s3- data-event-check
- Wolkenspur-S3- bucket-access-logging
- CloudTrail-S3- bucket-public-access-prohibited
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-action-enabled-überprüfen
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted
- cloud-trail-cloud-watch-logs-aktiviert

- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-Validierung aktiviert
- cmk-backing-key-rotation-aktiviert
- codebuild-project-artifact-encryption
- codebuild-project-environment-privileged-überprüfen
- codebuild-project-envvar-awscred-überprüfen
- codebuild-project-logging-enabled
- codebuild-project-s3-log-verschlüsselt
- codebuild-project-source-repo-URL-Prüfung
- codebuild-report-group-encrypted-im Ruhezustand
- codedeploy-auto-rollback-monitor-aktiviert
- codedeploy-deployment-group-auto-rollback-aktiviert
- codedeploy-deployment-group-outdated-instanzen-aktualisieren
- Codedeploy-ec2- minimum-healthy-hosts-configured
- codedeploy-lambda-allatonce-traffic-shift-deaktiviert
- codeguruprofiler-profiling-group-tagged
- codegururevieweer-repository-association-tagged
- codepipeline-deployment-count-check
- codepipeline-region-fanout-check
- cognito-identity-pool-unauth-Zugriffsprüfung
- cognito-user-pool-advanced-sicherheitsaktiviert
- cognito-user-pool-tagged
- custom-eventbus-policy-attached
- custom-schema-registry-policy-angehängt
- cw-loggroup-retention-period-überprüfen
- datasync-task-data-verification-aktiviert
- datasync-task-logging-enabled
- datasync-task-tagged
- dax-encryption-enabled

- dax-tls-endpoint-encryption
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- dms-auto-minor-version-upgrade-check
- dms-endpoint-ssl-configured
- dms-endpoint-tagged
- dms-mongo-db-authentication-aktiviert
- dms-neptune-iam-authorization-aktiviert
- dms-redis-tls-enabled
- dms-replication-not-public
- dms-replication-task-sourcedb-Protokollierung
- dms-replication-task-tagged
- dms-replication-task-targetdb-Protokollierung
- docdb-cluster-audit-logging-aktiviert
- docdb-cluster-backup-retention-überprüfen
- docdb-cluster-deletion-protection-aktiviert
- docdb-cluster-encrypted
- docdb-cluster-encrypted-in-Transit
- docdb-cluster-snapshot-public-verboten
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-last-backup-recovery-Punkt erstellt
- dynamodb-meets-restore-time-Ziel
- dynamodb-pitr-enabled
- dynamodb-resources-protected-by-Backup-Plan
- dynamodb-table-deletion-protection-aktiviert
- dynamodb-table-encrypted-kms
- dynamodb-table-encryption-enabled
- dynamodb-throughput-limit-check

- ebs-in-backup-plan
- ebs-last-backup-recovery-punkt-erstellt
- ebs-meets-restore-time-Ziel
- ebs-optimized-instance
- ebs-resources-in-logically-air-gapped-vault
- ebs-resources-protected-by-Backup-Plan
- ebs-snapshot-public-restorable-überprüfen
- ec2- capacity-reservation-tagged
- ec2- carrier-gateway-tagged
- ec2- aktiviert client-vpn-connection-log
- ec2- client-vpn-endpoint-tagged
- ec2- -alle client-vpn-not-authorize
- ec2- dhcp-options-tagged
- ec2- ebs-encryption-by-default
- ec2- aktiviert enis-source-destination-check
- ec2-fleet-markiert
- ec2-imdsv2-check
- ec2- instance-detailed-monitoring-enabled
- ec2-ami instance-launched-with-allowed
- ec2- instance-managed-by-ssm
- ec2- instance-multiple-eni-check
- ec2- instance-no-public-ip
- ec2- instance-profile-attached
- ec2- erstellt last-backup-recovery-point
- ec2-2-prüfen launch-template-imdsv
- ec2- -deaktiviert launch-template-public-ip
- ec2- launch-template-tagged
- ec2- managedinstance-applications-blacklisted
- ec2- managedinstance-applications-required
- ec2- prüfen managedinstance-association-compliance-status

- ec2- managedinstance-inventory-blacklisted
- ec2- prüfen managedinstance-patch-compliance-status
- ec2- managedinstance-platform-check
- ec2- meets-restore-time-target
- ec2- Analyse mit Schlagwörtern network-insights-access-scope
- ec2 network-insights-access-scope - markiert
- ec2- network-insights-path-tagged
- ec2- no-amazon-key-pair
- ec2- paravirtual-instance-check
- ec2- prefix-list-tagged
- ec2- -Tresor mit Lücken resources-in-logically-air
- ec2- resources-protected-by-backup -plan
- ec2- -eni security-group-attached-to
- ec2- -eni-periodisch security-group-attached-to
- ec2 spot-fleet-request-ct - - encryption-at-rest
- ec2-stopped-instance
- ec2- token-hop-limit-check
- ec2- traffic-mirror-filter-description
- ec2- traffic-mirror-filter-tagged
- ec2- traffic-mirror-session-description
- ec2- traffic-mirror-session-tagged
- ec2- traffic-mirror-target-description
- ec2- traffic-mirror-target-tagged
- ec2- -attach-deaktiviert transit-gateway-auto-vpc
- ec2 transit-gateway-multicast-domain - markiert
- ec2- volume-inuse-check
- ec2- vpn-connection-logging-enabled
- ecr-private-image-scanning-aktiviert
- ecr-private-lifecycle-policy-konfiguriert
- ecr-private-tag-immutability-aktiviert

- ecr-repository-cmk-encryption-aktiviert
- ecr-repository-tagged
- ecs-awsvpc-networking-enabled
- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-container-insights-enabled
- ecs-fargate-latest-platform-Version
- ecs-no-environment-secrets
- ecs-task-definition-log-Konfiguration
- ecs-task-definition-memory-hartes Limit
- ecs-task-definition-network-mode-not-host
- ecs-task-definition-nonroot-Benutzer
- ecs-task-definition-pid-Modus-Check
- ecs-task-definition-user-for-host-mode-check
- efs-access-point-enforce-Stammverzeichnis
- efs-access-point-enforce-Benutzeridentität
- efs-automatic-backups-enabled
- efs-encrypted-check
- efs-filesystem-ct-encrypted
- efs-in-backup-plan
- efs-last-backup-recovery-Punkt erstellt
- efs-meets-restore-time-Ziel
- efs-mount-target-public-zugänglich
- efs-resources-in-logically-air-gapped-vault
- efs-resources-protected-by-Backup-Plan
- eip-attached
- eks-cluster-logging-enabled
- eks-cluster-log-enabled
- eks-cluster-oldest-supported-Ausführung
- eks-cluster-secrets-encrypted

- eks-cluster-supported-version
- eks-endpoint-no-public-Zugang
- eks-secrets-encrypted
- elasticache-auto-minor-version-aktualisieren-Prüfung
- elasticache-rbac-auth-enabled
- elasticache-redis-cluster-automatic-Backup-Check
- elasticache-repl-grp-auto-failover-fähig
- elasticache-repl-grp-encrypted-im Ruhezustand
- elasticache-repl-grp-encryptedim Transit
- elasticache-repl-grp-redis-auth-aktiviert
- elasticache-subnet-group-check
- elasticache-supported-engine-version
- elasticbeanstalk-application-description
- elasticbeanstalk-application-version-description
- elasticbeanstalk-environment-description
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch
- elasticsearch-node-to-node-Verschlüsselungsprüfung
- elastic-beanstalk-logs-to- Cloudwatch
- elastic-beanstalk-managed-updates-aktiviert
- elbv2- acm-certificate-required
- elv 2- listener-encryption-in-transit
- elbv2-multiple-az
- elbv2- prüfen predefined-security-policy-ssl
- elb-acm-certificate-required
- elb-cross-zone-load-Balancing aktiviert
- elb-custom-security-policy-ssl-Prüfung
- elb-deletion-protection-enabled
- elb-logging-enabled

- elb-predefined-security-policy-ssl-Überprüfung
- elb-tls-https-listeners-nur
- emr-block-public-access
- emr-kerberos-enabled
- emr-master-no-public-ip
- emr-security-configuration-encryption-ruh dich aus
- emr-security-configuration-encryption-Transit
- encrypted-volumes
- event-data-store-cmk-Verschlüsselung aktiviert
- evidently-launch-description
- evidently-launch-tagged
- evidently-project-description
- evidently-project-tagged
- evidently-segment-description
- evidently-segment-tagged
- fis-experiment-template-log-Konfiguration ist vorhanden
- fis-experiment-template-tagged
- fms-shield-resource-policy-überprüfen
- fms-webacl-resource-policy-überprüfen
- fms-webacl-rulegroup-association-überprüfen
- frauddetector-entity-type-tagged
- frauddetector-label-tagged
- frauddetector-outcome-tagged
- frauddetector-variable-tagged
- fsx-last-backup-recovery-Punkt erstellt
- fsx-lustre-copy-tagszu Backups
- fsx-meets-restore-time-Ziel
- fsx-ontap-deployment-type-überprüfen
- fsx-openzfs-copy-tags-aktiviert
- fsx-openzfs-deployment-type-überprüfen

- fsx-resources-protected-by-Backup-Plan
- fsx-windows-audit-log-konfiguriert
- fsx-windows-deployment-type-überprüfen
- glb-listener-tagged
- global-endpoint-event-replication-aktiviert
- glue-job-logging-enabled
- glue-ml-transform-encrypted-im Ruhezustand
- glue-spark-job-supported-Ausführung
- GuardDuty-EC2- protection-runtime-enabled
- guardduty-ecs-protection-runtime-aktiviert
- guardduty-eks-protection-audit-aktiviert
- guardduty-eks-protection-runtime-aktiviert
- guardduty-enabled-centralized
- guardduty-lambda-protection-enabled
- guardduty-malware-protection-enabled
- guardduty-non-archived-findings
- guardduty-rds-protection-enabled
- guardduty-runtime-monitoring-enabled
- GuardDuty-S3-Schutz aktiviert
- iam-customer-policy-blocked-kms-Aktionen
- iam-external-access-analyzer-aktiviert
- iam-group-has-users-überprüfen
- iam-inline-policy-blocked-kms-Aktionen
- iam-no-inline-policy-überprüfen
- iam-password-policy
- iam-policy-blacklisted-check
- iam-policy-in-use
- iam-policy-no-statements-with-admin-access
- iam-policy-no-statements-with-full-access
- iam-role-managed-policy-überprüfen

- iam-root-access-key-überprüfen
- iam-user-group-membership-überprüfen
- iam-user-mfa-enabled
- iam-user-no-policies-überprüfen
- iam-user-unused-credentials-überprüfen
- incoming-ssh-disabled
- inspector-ec2-Scan aktiviert
- inspector-ecr-scan-enabled
- inspector-lambda-code-scan-aktiviert
- inspector-lambda-standard-scan-aktiviert
- instances-in-vpc
- internet-gateway-authorized-vpc-nur
- iotevents-alarm-model-tagged
- iotevents-detector-model-tagged
- iotevents-input-tagged
- iotsitewise-asset-model-tagged
- iotsitewise-dashboard-tagged
- iotsitewise-gateway-tagged
- iotsitewise-portal-tagged
- iotsitewise-project-tagged
- iottwinmaker-component-type-tagged
- iottwinmaker-entity-tagged
- iottwinmaker-scene-tagged
- iottwinmaker-sync-job-tagged
- iottwinmaker-workspace-tagged
- iotwireless-fuota-task-tagged
- iotwireless-multicast-group-tagged
- iotwireless-service-profile-tagged
- iot-authorizer-token-signing-aktiviert
- ivs-channel-playback-authorization-aktiviert

- ivs-channel-tagged
- ivs-playback-key-pair-markiert
- ivs-recording-configuration-tagged
- kinesis-firehose-delivery-stream-verschlüsselt
- kinesis-stream-backup-retention-überprüfen
- kinesis-stream-encrypted
- kms-cmk-not-scheduled-zum Löschen
- kms-key-policy-no-öffentlicher Zugang
- lambda-concurrency-check
- lambda-dlq-check
- lambda-function-public-access-verboten
- lambda-function-settings-check
- lambda-function-xray-enabled
- lambda-inside-vpc
- lambda-vpc-multi-az-überprüfen
- lightsail-bucket-tagged
- lightsail-certificate-tagged
- lightsail-disk-tagged
- macie-auto-sensitive-data-Discovery-Check
- macie-status-check
- mariadb-publish-logs-to-Cloudwatch-Protokolle
- mfa-enabled-for-iam-Konsolenzugriff
- mq-active-broker-ldap-Authentifizierung
- mq-active-deployment-mode
- mq-active-single-instance-broker-storage-type-efs
- mq-automatic-minor-version-Upgrade aktiviert
- mq-auto-minor-version-upgrade-fähig
- mq-broker-general-logging-aktiviert
- mq-cloudwatch-audit-logging-aktiviert
- mq-cloudwatch-audit-log-aktiviert

- mq-no-public-access
- mq-rabbit-deployment-mode
- msk-cluster-public-access-deaktiviert
- msk-connect-connector-logging-aktiviert
- msk-enhanced-monitoring-enabled
- msk-in-cluster-node-require-tls
- msk-unrestricted-access-check
- multi-region-cloud-trail-aktiviert
- nacl-no-unrestricted-ssh-rdp
- neptune-cluster-backup-retention-überprüfen
- neptune-cluster-cloudwatch-log-exportfähig
- neptune-cluster-copy-tags-to-snapshot-enabled
- neptune-cluster-deletion-protection-aktiviert
- neptune-cluster-encrypted
- neptune-cluster-iam-database-Authentifizierung
- neptune-cluster-multi-az-aktiviert
- neptune-cluster-snapshot-encrypted
- neptune-cluster-snapshot-public-verboten
- netfw-deletion-protection-enabled
- netfw-logging-enabled
- netfw-multi-az-enabled
- netfw-policy-default-action-fragment-Pakete
- netfw-policy-default-action-vollständige Pakete
- netfw-policy-rule-group-assoziiert
- netfw-stateless-rule-group-nicht leer
- netfw-subnet-change-protection-aktiviert
- nlb-cross-zone-load-Balancing aktiviert
- nlb-internal-scheme-check
- nlb-listener-tagged
- nlb-logging-enabled

- no-unrestricted-route-to-igw
- opensearch-access-control-enabled
- opensearch-audit-logging-enabled
- opensearch-data-node-fault-Toleranz
- opensearch-encrypted-at-rest
- opensearch-https-required
- opensearch-in-vpc-only
- opensearch-logs-to-cloudwatch
- opensearch-node-to-node-Verschlüsselungsprüfung
- opensearch-primary-node-fault-Toleranz
- opensearch-update-check
- rabbit-mq-supported-version
- rds-aurora-mysql-audit-Protokollierung aktiviert
- rds-aurora-postgresql-logs-zu-Cloud-Watch
- rds-automatic-minor-version-upgrade-fähig
- rds-cluster-auto-minor-version-upgrade-enable
- rds-cluster-default-admin-überprüfen
- rds-cluster-deletion-protection-aktiviert
- rds-cluster-encrypted-at-ausruhen
- rds-cluster-iam-authentication-aktiviert
- rds-cluster-multi-az-aktiviert
- rds-db-security-group-nicht erlaubt
- rds-enhanced-monitoring-enabled
- rds-instance-default-admin-überprüfen
- rds-instance-deletion-protection-aktiviert
- rds-instance-iam-authentication-aktiviert
- rds-instance-public-access-überprüfen
- rds-instance-subnet-igw-überprüfen
- rds-in-backup-plan
- rds-last-backup-recovery-Punkt erstellt

- rds-logging-enabled
- rds-mariadb-instance-encryptedwährend des Transports
- rds-meets-restore-time-Ziel
- rds-multi-az-support
- rds-mysql-instance-encryptedim Transit
- rds-postgresql-logs-to- Cloudwatch
- rds-postgres-instance-encryptedunterwegs
- rds-proxy-tls-encryption
- rds-resources-protected-by-Backup-Plan
- rds-snapshots-public-prohibited
- rds-snapshot-encrypted
- rds-sqlserver-encrypted-in-Transit
- rds-sql-server-logszur Cloud-Überwachung
- rds-storage-encrypted
- redshift-audit-logging-enabled
- redshift-backup-enabled
- redshift-cluster-configuration-check
- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check
- redshift-cluster-multi-az-aktiviert
- redshift-cluster-parameter-group-markiert
- redshift-cluster-public-access-überprüfen
- redshift-cluster-subnet-group-Multi-Az
- redshift-default-admin-check
- redshift-default-db-name-überprüfen
- redshift-enhanced-vpc-routing-aktiviert
- redshift-require-tls-ssl
- redshift-serverless-default-admin-überprüfen
- redshift-serverless-default-db-Namenscheck
- redshift-serverless-namespace-cmk-Verschlüsselung

- redshift-serverless-publish-logs-zu-Cloud-Watch
- redshift-serverless-workgroup-encryptedauf dem Weg
- redshift-serverless-workgroup-no-öffentlich zugänglich
- redshift-serverless-workgroup-routes-innerhalb von VPC
- redshift-unrestricted-port-access
- required-tags
- restricted-incoming-traffic
- root-account-hardware-mfa-aktiviert
- root-account-mfa-enabled
- s3 -regel-check express-dir-bucket-lifecycle
- nur s3- access-point-in-vpc
- s3- -Blöcke access-point-public-access
- s3- -Blöcke account-level-public-access
- s3- -Blocke-periodisch account-level-public-access
- s 3- bucket-acl-prohibited
- s-3 bucket-blacklisted-actions-prohibited
- s3- bucket-cross-region-replication -aktiviert
- s-3 bucket-default-lock-enabled
- s3 bucket-level-public-access - verboten
- s3- bucket-logging-enabled
- s-3 bucket-mfa-delete-enabled
- s-3 bucket-policy-grantee-check
- s3- bucket-policy-not-more -freizügig
- s 3- bucket-public-read-prohibited
- s-3 bucket-public-write-prohibited
- s-3 bucket-replication-enabled
- s3- bucket-server-side-encryption -aktiviert
- s-3 bucket-ssl-requests-only
- s3-Bucket-Tagged
- s-3 bucket-versioning-enabled

- s-3 default-encryption-kms
- s-3 event-notifications-enabled
- s3 last-backup-recovery-point - erstellt
- s3- lifecycle-policy-check
- s-3 meets-restore-time-target
- s3- resources-in-logically-air -Tresor mit Lücken
- s3 resources-protected-by-backup - -Plan
- s 3- version-lifecycle-policy-check
- sagemaker-app-image-config-markiert
- sagemaker-domain-in-vpc
- sagemaker-domain-tagged
- sagemaker-endpoint-configuration-kms-schlüsselkonfiguriert
- sagemaker-endpoint-config-prod-Anzahl der Instanzen
- sagemaker-feature-group-tagged
- sagemaker-image-description
- sagemaker-image-tagged
- sagemaker-model-in-vpc
- sagemaker-model-isolation-enabled
- sagemaker-notebook-instance-inside-vpc
- sagemaker-notebook-instance-kms-key-konfiguriert
- sagemaker-notebook-instance-platform-Version
- sagemaker-notebook-instance-root-Zugriffsprüfung
- sagemaker-notebook-no-direct-Internetzugang
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-überprüfen
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- securityhub-enabled
- security-account-information-provided

- service-catalog-shared-within-Organisation
- service-vpc-endpoint-enabled
- ses-malware-scanning-enabled
- sns-encrypted-kms
- sns-topic-message-delivery-Benachrichtigung aktiviert
- sns-topic-no-public-Zugriff
- sqs-queue-no-public-Zugang
- ssm-automation-block-public-teilen
- ssm-automation-logging-enabled
- ssm-document-not-public
- ssm-document-tagged
- step-functions-state-machine-Protokollierung aktiviert
- storagegateway-last-backup-recovery-punkt-erstellt
- storagegateway-resources-in-logically-air-gapped-vault
- storagegateway-resources-protected-by-Ersatzplan
- subnet-auto-assign-public-ip-deaktiviert
- transfer-agreement-description
- transfer-agreement-tagged
- transfer-certificate-description
- transfer-certificate-tagged
- transfer-connector-logging-enabled
- transfer-connector-tagged
- transfer-family-server-no-ftp
- transfer-profile-tagged
- transfer-workflow-description
- transfer-workflow-tagged
- virtualmachine-last-backup-recovery-punkt-erstellt
- virtualmachine-resources-in-logically-air-gapped-vault
- virtualmachine-resources-protected-by-Ersatzplan
- vpc-default-security-group-geschlossen

- vpc-endpoint-enabled
- vpc-flow-logs-enabled
- vpc-network-acl-unused-überprüfen
- vpc-peering-dns-resolution-überprüfen
- vpc-sg-open-only-to-authorized-ports
- vpc-sg-port-restriction-überprüfen
- vpc-vpn-2-tunnels-up
- wafv2-logging-enabled
- WAF 2- rulegroup-logging-enabled
- WAF 2- rulegroup-not-empty
- WAF 2- webacl-not-empty
- waf-regional-rulegroup-not-leer
- waf-regional-rule-not-leer
- waf-regional-webacl-not-leer
- workspaces-root-volume-encryption-aktiviert
- workspaces-user-volume-encryption-aktiviert

Region Europa (London)

Europa (London)

- access-keys-rotated
- account-part-of-organizations
- acmpca-certificate-authority-tagged
- acm-certificate-expiration-check
- acm-certificate-rsa-check
- acm-pca-root-ca-deaktiviert
- active-mq-supported-version
- alb-desync-mode-check
- alb-http-drop-invalid-Header-fähig
- alb-http-to-https-Umleitungsprüfung
- alb-internal-scheme-check

- alb-listener-tagged
- alb-waf-enabled
- amplify-app-branch-auto-löschung aktiviert
- amplify-app-description
- amplify-app-tagged
- amplify-branch-performance-mode-aktiviert
- amplify-branch-tagged
- api-gwv2- access-logs-enabled
- api-gwv2- authorization-type-configured
- api-gw-associated-with-WAF
- api-gw-cache-enabled-und-verschlüsselt
- api-gw-endpoint-type-überprüfen
- api-gw-execution-logging-aktiviert
- api-gw-ssl-enabled
- api-gw-xray-enabled
- appconfig-application-description
- appconfig-application-tagged
- appconfig-configuration-profile-tagged
- appconfig-configuration-profile-validators-nicht leer
- appconfig-deployment-strategy-description
- appconfig-deployment-strategy-replicate-zu-ssm
- appconfig-environment-description
- appconfig-environment-tagged
- appconfig-extension-association-tagged
- appconfig-freeform-profile-config-Speicher
- appconfig-hosted-configuration-version-Beschreibung
- appflow-flow-tagged
- appintegrations-event-integration-description
- appintegrations-event-integration-tagged
- appmesh-gateway-route-tagged

- appmesh-mesh-deny-tcp-Weiterleitung
- appmesh-mesh-tagged
- appmesh-route-tagged
- appmesh-virtual-gateway-backend-Standardeinstellungen-TLS
- appmesh-virtual-gateway-logging-file-path-exists
- appmesh-virtual-gateway-tagged
- appmesh-virtual-node-backend-defaults-tls-on
- appmesh-virtual-node-logging-file-path-exists
- appmesh-virtual-node-tagged
- appmesh-virtual-router-tagged
- appmesh-virtual-service-tagged
- approved-amis-by-id
- approved-amis-by-tag
- apprunner-service-in-vpc
- apprunner-service-no-public-Zugang
- apprunner-service-observability-enabled
- apprunner-service-tagged
- appstream-fleet-in-vpc
- appsync-associated-with-waf
- appsync-authorization-check
- appsync-cache-encryption-at-ausruhen
- appsync-logging-enabled
- athena-data-catalog-description
- athena-prepared-statement-description
- athena-workgroup-description
- athena-workgroup-encrypted-at-ausruhen
- athena-workgroup-enforce-workgroup-Konfiguration
- athena-workgroup-engine-version-automatisches Upgrade
- athena-workgroup-logging-enabled
- aurora-last-backup-recovery-Punkt erstellt

- aurora-meets-restore-time-Ziel
- aurora-mysql-backtracking-enabled
- aurora-mysql-cluster-audit-Protokollierung
- aurora-resources-in-logically-air-gapped-vault
- aurora-resources-protected-by-Backup-Plan
- autoscaling-capacity-rebalancing
- autoscaling-group-elb-healthcheck-erforderlich
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-hop-Grenze
- autoscaling-launch-config-public-ip-deaktiviert
- autoscaling-launch-template
- autoscaling-multiple-az
- autoscaling-multiple-instance-types
- backup-plan-min-frequency-and-min-retention-check
- backup-recovery-point-encrypted
- backup-recovery-point-manual-Löschen-deaktiviert
- backup-recovery-point-minimum-Aufbewahrungsprüfung
- batch-compute-environment-enabled
- batch-compute-environment-managed
- batch-compute-environment-tagged
- batch-job-queue-enabled
- batch-job-queue-tagged
- batch-managed-compute-environment-using-launch-template
- batch-managed-compute-env-compute-resources-tagged
- batch-scheduling-policy-tagged
- beanstalk-enhanced-health-reporting-aktiviert
- cassandra-keyspace-tagged
- clb-desync-mode-check
- clb-multiple-az
- cloudformation-stack-drift-detection-überprüfen

- cloudformation-stack-notification-check
- cloudtrail-all-read-s3- data-event-check
- cloudtrail-all-write-s3- data-event-check
- Wolkenspur-S3- bucket-access-logging
- CloudTrail-S3- bucket-public-access-prohibited
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-action-enabled-überprüfen
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted
- cloud-trail-cloud-watch-logs-aktiviert
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-Validierung aktiviert
- cmk-backing-key-rotation-aktiviert
- codebuild-project-artifact-encryption
- codebuild-project-environment-privileged-überprüfen
- codebuild-project-envvar-awscred-überprüfen
- codebuild-project-logging-enabled
- codebuild-project-s3-log-verschlüsselt
- codebuild-project-source-repo-URL-Prüfung
- codebuild-report-group-encrypted-im Ruhezustand
- codedeploy-auto-rollback-monitor-aktiviert
- codedeploy-deployment-group-auto-rollback-aktiviert
- codedeploy-deployment-group-outdated-instanzen-aktualisieren
- Codedeploy-ec2- minimum-healthy-hosts-configured
- codedeploy-lambda-allatonce-traffic-shift-deaktiviert
- codeguruprofiler-profiling-group-tagged

- codegurureviewer-repository-association-tagged
- codepipeline-deployment-count-check
- codepipeline-region-fanout-check
- cognito-identity-pool-unauth-Zugriffsprüfung
- cognito-user-pool-advanced-sicherheitsaktiviert
- cognito-user-pool-tagged
- connect-instance-logging-enabled
- customerprofiles-object-type-allow-Profilerstellung
- customerprofiles-object-type-tagged
- custom-eventbus-policy-attached
- custom-schema-registry-policy-beigefügt
- cw-loggroup-retention-period-überprüfen
- datasync-task-data-verification-aktiviert
- datasync-task-logging-enabled
- datasync-task-tagged
- dax-encryption-enabled
- dax-tls-endpoint-encryption
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- dms-auto-minor-version-aktualisieren-Prüfung
- dms-endpoint-ssl-configured
- dms-endpoint-tagged
- dms-mongo-db-authentication-aktiviert
- dms-neptune-iam-authorization-aktiviert
- dms-redis-tls-enabled
- dms-replication-not-public
- dms-replication-task-sourcedb-Protokollierung
- dms-replication-task-tagged
- dms-replication-task-targetdb-Protokollierung

- docdb-cluster-audit-logging-aktiviert
- docdb-cluster-backup-retention-überprüfen
- docdb-cluster-deletion-protection-aktiviert
- docdb-cluster-encrypted
- docdb-cluster-encrypted-in-Transit
- docdb-cluster-snapshot-public-verboten
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-last-backup-recovery-Punkt erstellt
- dynamodb-meets-restore-time-Ziel
- dynamodb-pitr-enabled
- dynamodb-resources-protected-by-Backup-Plan
- dynamodb-table-deletion-protection-aktiviert
- dynamodb-table-encrypted-kms
- dynamodb-table-encryption-enabled
- dynamodb-throughput-limit-check
- ebs-in-backup-plan
- ebs-last-backup-recovery-punkt-erstellt
- ebs-meets-restore-time-Ziel
- ebs-optimized-instance
- ebs-resources-in-logically-air-gapped-vault
- ebs-resources-protected-by-Backup-Plan
- ebs-snapshot-public-restorable-überprüfen
- ec2- capacity-reservation-tagged
- ec2- carrier-gateway-tagged
- ec2- aktiviert client-vpn-connection-log
- ec2- client-vpn-endpoint-tagged
- ec2- -alle client-vpn-not-authorize
- ec2- dhcp-options-tagged
- ec2- ebs-encryption-by-default

- ec2- aktiviert enis-source-destination-check
- ec2-fleet-markiert
- ec2-imdsv2-check
- ec2- instance-detailed-monitoring-enabled
- ec2-ami instance-launched-with-allowed
- ec2- instance-managed-by-ssm
- ec2- instance-multiple-eni-check
- ec2- instance-no-public-ip
- ec2- instance-profile-attached
- ec2- erstellt last-backup-recovery-point
- ec2-2-prüfen launch-template-imdsv
- ec2- -deaktiviert launch-template-public-ip
- ec2- launch-template-tagged
- ec2- managedinstance-applications-blacklisted
- ec2- managedinstance-applications-required
- ec2- prüfen managedinstance-association-compliance-status
- ec2- managedinstance-inventory-blacklisted
- ec2- prüfen managedinstance-patch-compliance-status
- ec2- managedinstance-platform-check
- ec2- meets-restore-time-target
- ec2- Analyse mit Schlagwörtern network-insights-access-scope
- ec2 network-insights-access-scope - markiert
- ec2- network-insights-path-tagged
- ec2- no-amazon-key-pair
- ec2- prefix-list-tagged
- ec2- -Tresor mit Lücken resources-in-logically-air
- ec2- resources-protected-by-backup -plan
- ec2- -eni security-group-attached-to
- ec2- -eni-periodisch security-group-attached-to
- ec2-stopped-instance

- ec2- token-hop-limit-check
- ec2- traffic-mirror-filter-description
- ec2- traffic-mirror-filter-tagged
- ec2- traffic-mirror-session-description
- ec2- traffic-mirror-session-tagged
- ec2- traffic-mirror-target-description
- ec2- traffic-mirror-target-tagged
- ec2- -attach-deaktiviert transit-gateway-auto-vpc
- ec2 transit-gateway-multicast-domain - markiert
- ec2- volume-inuse-check
- ec2- vpn-connection-logging-enabled
- ecr-private-image-scanning-aktiviert
- ecr-private-lifecycle-policy-konfiguriert
- ecr-private-tag-immutability-aktiviert
- ecr-repository-cmk-encryption-aktiviert
- ecr-repository-tagged
- ecs-awsvpc-networking-enabled
- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-container-insights-enabled
- ecs-fargate-latest-platform-Version
- ecs-no-environment-secrets
- ecs-task-definition-log-Konfiguration
- ecs-task-definition-memory-hartes Limit
- ecs-task-definition-network-mode-not-host
- ecs-task-definition-nonroot-Benutzer
- ecs-task-definition-pid-Modus-Check
- ecs-task-definition-user-for-host-mode-check
- efs-access-point-enforce-Stammverzeichnis
- efs-access-point-enforce-Benutzeridentität

- efs-automatic-backups-enabled
- efs-encrypted-check
- efs-filesystem-ct-encrypted
- efs-in-backup-plan
- efs-last-backup-recovery-Punkt erstellt
- efs-meets-restore-time-Ziel
- efs-mount-target-public-zugänglich
- efs-resources-in-logically-air-gapped-vault
- efs-resources-protected-by-Backup-Plan
- eip-attached
- eks-cluster-logging-enabled
- eks-cluster-log-enabled
- eks-cluster-oldest-supported-Ausführung
- eks-cluster-secrets-encrypted
- eks-cluster-supported-version
- eks-endpoint-no-public-Zugang
- eks-secrets-encrypted
- elasticache-auto-minor-version-aktualisieren-Prüfung
- elasticache-rbac-auth-enabled
- elasticache-redis-cluster-automatic-Backup-Check
- elasticache-repl-grp-auto-failover-fähig
- elasticache-repl-grp-encrypted-im Ruhezustand
- elasticache-repl-grp-encryptedunterwegs
- elasticache-repl-grp-redis-auth-aktiviert
- elasticache-subnet-group-check
- elasticache-supported-engine-version
- elasticbeanstalk-application-description
- elasticbeanstalk-application-version-description
- elasticbeanstalk-environment-description
- elasticsearch-encrypted-at-rest

- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch
- elasticsearch-node-to-node-Verschlüsselungsprüfung
- elastic-beanstalk-logs-to- Cloudwatch
- elastic-beanstalk-managed-updates-aktiviert
- elbv2- acm-certificate-required
- elv 2- listener-encryption-in-transit
- elbv2-multiple-az
- elbv2- prüfen predefined-security-policy-ssl
- elb-acm-certificate-required
- elb-cross-zone-load-Balancing aktiviert
- elb-custom-security-policy-ssl-Prüfung
- elb-deletion-protection-enabled
- elb-logging-enabled
- elb-predefined-security-policy-ssl-Überprüfung
- elb-tls-https-listeners-nur
- emr-block-public-access
- emr-kerberos-enabled
- emr-master-no-public-ip
- emr-security-configuration-encryption-ruh dich aus
- emr-security-configuration-encryption-Transit
- encrypted-volumes
- event-data-store-cmk-Verschlüsselung aktiviert
- fis-experiment-template-log-Konfiguration ist vorhanden
- fis-experiment-template-tagged
- fms-shield-resource-policy-überprüfen
- fms-webacl-resource-policy-überprüfen
- fms-webacl-rulegroup-association-überprüfen
- fsx-last-backup-recovery-Punkt erstellt
- fsx-lustre-copy-tagszu Backups

- fsx-meets-restore-time-Ziel
- fsx-ontap-deployment-type-überprüfen
- fsx-openzfs-copy-tags-aktiviert
- fsx-openzfs-deployment-type-überprüfen
- fsx-resources-protected-by-Backup-Plan
- fsx-windows-audit-log-konfiguriert
- fsx-windows-deployment-type-überprüfen
- glb-listener-tagged
- global-endpoint-event-replication-aktiviert
- glue-job-logging-enabled
- glue-ml-transform-encrypted-im Ruhezustand
- glue-spark-job-supported-Ausführung
- GuardDuty-EC2- protection-runtime-enabled
- guardduty-ecs-protection-runtime-aktiviert
- guardduty-eks-protection-audit-aktiviert
- guardduty-eks-protection-runtime-aktiviert
- guardduty-enabled-centralized
- guardduty-lambda-protection-enabled
- guardduty-malware-protection-enabled
- guardduty-non-archived-findings
- guardduty-rds-protection-enabled
- guardduty-runtime-monitoring-enabled
- GuardDuty-S3-Schutz aktiviert
- iam-customer-policy-blocked-kms-Aktionen
- iam-external-access-analyzer-aktiviert
- iam-group-has-users-überprüfen
- iam-inline-policy-blocked-kms-Aktionen
- iam-no-inline-policy-überprüfen
- iam-password-policy
- iam-policy-blacklisted-check

- iam-policy-in-use
- iam-policy-no-statements-with-admin-access
- iam-policy-no-statements-with-full-access
- iam-role-managed-policy-überprüfen
- iam-root-access-key-überprüfen
- iam-user-group-membership-überprüfen
- iam-user-mfa-enabled
- iam-user-no-policies-überprüfen
- iam-user-unused-credentials-überprüfen
- incoming-ssh-disabled
- inspector-ec2-Scan aktiviert
- inspector-ecr-scan-enabled
- inspector-lambda-code-scan-aktiviert
- inspector-lambda-standard-scan-aktiviert
- instances-in-vpc
- internet-gateway-authorized-vpc-nur
- iotevents-alarm-model-tagged
- iotevents-detector-model-tagged
- iotevents-input-tagged
- iot-authorizer-token-signing-aktiviert
- kinesis-firehose-delivery-stream-verschlüsselt
- kinesis-stream-backup-retention-überprüfen
- kinesis-stream-encrypted
- kms-cmk-not-scheduled-zum Löschen
- kms-key-policy-no-öffentlicher Zugang
- lambda-concurrency-check
- lambda-dlq-check
- lambda-function-public-access-verboten
- lambda-function-settings-check
- lambda-function-xray-enabled

- lambda-inside-vpc
- lambda-vpc-multi-az-überprüfen
- lightsail-bucket-tagged
- lightsail-certificate-tagged
- lightsail-disk-tagged
- macie-auto-sensitive-data-Discovery-Check
- macie-status-check
- mariadb-publish-logs-to-Cloudwatch-Protokolle
- mfa-enabled-for-iam-Konsolenzugriff
- mq-active-broker-ldap-Authentifizierung
- mq-active-deployment-mode
- mq-active-single-instance-broker-storage-type-efs
- mq-automatic-minor-version-Upgrade aktiviert
- mq-auto-minor-version-upgrade-fähig
- mq-broker-general-logging-aktiviert
- mq-cloudwatch-audit-logging-aktiviert
- mq-cloudwatch-audit-log-aktiviert
- mq-no-public-access
- mq-rabbit-deployment-mode
- msk-cluster-public-access-deaktiviert
- msk-connect-connector-logging-aktiviert
- msk-enhanced-monitoring-enabled
- msk-in-cluster-node-require-tls
- msk-unrestricted-access-check
- multi-region-cloud-trail-aktiviert
- nacl-no-unrestricted-ssh-rdp
- neptune-cluster-backup-retention-überprüfen
- neptune-cluster-cloudwatch-log-exportfähig
- neptune-cluster-copy-tags-to-snapshot-enabled
- neptune-cluster-deletion-protection-aktiviert

- neptune-cluster-encrypted
- neptune-cluster-iam-database-Authentifizierung
- neptune-cluster-multi-az-aktiviert
- neptune-cluster-snapshot-encrypted
- neptune-cluster-snapshot-public-verboten
- netfw-deletion-protection-enabled
- netfw-logging-enabled
- netfw-multi-az-enabled
- netfw-policy-default-action-fragment-Pakete
- netfw-policy-default-action-vollständige Pakete
- netfw-policy-rule-group-assoziiert
- netfw-stateless-rule-group-nicht leer
- netfw-subnet-change-protection-aktiviert
- nlb-cross-zone-load-Balancing aktiviert
- nlb-internal-scheme-check
- nlb-listener-tagged
- nlb-logging-enabled
- no-unrestricted-route-to-igw
- opensearch-access-control-enabled
- opensearch-audit-logging-enabled
- opensearch-data-node-fault-Toleranz
- opensearch-encrypted-at-rest
- opensearch-https-required
- opensearch-in-vpc-only
- opensearch-logs-to-cloudwatch
- opensearch-node-to-node-Verschlüsselungsprüfung
- opensearch-primary-node-fault-Toleranz
- opensearch-update-check
- rabbit-mq-supported-version
- rds-aurora-mysql-audit-Protokollierung aktiviert

- rds-aurora-postgresql-logs-zu-Cloud-Watch
- rds-automatic-minor-version-upgrade-fähig
- rds-cluster-auto-minor-version-upgrade-enable
- rds-cluster-default-admin-überprüfen
- rds-cluster-deletion-protection-aktiviert
- rds-cluster-encrypted-at-ausruhen
- rds-cluster-iam-authentication-aktiviert
- rds-cluster-multi-az-aktiviert
- rds-enhanced-monitoring-enabled
- rds-instance-default-admin-überprüfen
- rds-instance-deletion-protection-aktiviert
- rds-instance-iam-authentication-aktiviert
- rds-instance-public-access-überprüfen
- rds-instance-subnet-igw-überprüfen
- rds-in-backup-plan
- rds-last-backup-recovery-Punkt erstellt
- rds-logging-enabled
- rds-mariadb-instance-encryptedwährend des Transports
- rds-meets-restore-time-Ziel
- rds-multi-az-support
- rds-mysql-instance-encryptedunterwegs
- rds-postgresql-logs-to- Cloudwatch
- rds-postgres-instance-encryptedunterwegs
- rds-proxy-tls-encryption
- rds-resources-protected-by-Backup-Plan
- rds-snapshots-public-prohibited
- rds-snapshot-encrypted
- rds-sqlserver-encrypted-in-Transit
- rds-sql-server-logszur Cloud-Überwachung
- rds-storage-encrypted

- redshift-audit-logging-enabled
- redshift-backup-enabled
- redshift-cluster-configuration-check
- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check
- redshift-cluster-multi-az-aktiviert
- redshift-cluster-parameter-group-markiert
- redshift-cluster-public-access-überprüfen
- redshift-cluster-subnet-group-Multi-Az
- redshift-default-admin-check
- redshift-default-db-name-überprüfen
- redshift-enhanced-vpc-routing-aktiviert
- redshift-require-tls-ssl
- redshift-serverless-default-admin-überprüfen
- redshift-serverless-default-db-Namenscheck
- redshift-serverless-namespace-cmk-Verschlüsselung
- redshift-serverless-publish-logs-zu-Cloud-Watch
- redshift-serverless-workgroup-encryptedauf dem Weg
- redshift-serverless-workgroup-no-öffentlich zugänglich
- redshift-serverless-workgroup-routes-innerhalb von VPC
- redshift-unrestricted-port-access
- required-tags
- restricted-incoming-traffic
- root-account-hardware-mfa-aktiviert
- root-account-mfa-enabled
- nur s3- access-point-in-vpc
- s3- -Blöcke access-point-public-access
- s3- -Blöcke account-level-public-access
- s3- -Blocke-periodisch account-level-public-access
- s 3- bucket-acl-prohibited

- s-3 bucket-blacklisted-actions-prohibited
- s3- bucket-cross-region-replication -aktiviert
- s-3 bucket-default-lock-enabled
- s3 bucket-level-public-access - verboten
- s3- bucket-logging-enabled
- s-3 bucket-mfa-delete-enabled
- s-3 bucket-policy-grantee-check
- s3- bucket-policy-not-more -freizügig
- s 3- bucket-public-read-prohibited
- s-3 bucket-public-write-prohibited
- s-3 bucket-replication-enabled
- s3- bucket-server-side-encryption -aktiviert
- s-3 bucket-ssl-requests-only
- s3-Bucket-Tagged
- s-3 bucket-versioning-enabled
- s-3 default-encryption-kms
- s-3 event-notifications-enabled
- s3 last-backup-recovery-point - erstellt
- s3- lifecycle-policy-check
- s-3 meets-restore-time-target
- s3- resources-in-logically-air -Tresor mit Lücken
- s3 resources-protected-by-backup - -Plan
- s 3- version-lifecycle-policy-check
- sagemaker-app-image-config-markiert
- sagemaker-domain-in-vpc
- sagemaker-domain-tagged
- sagemaker-endpoint-configuration-kms-schlüsselkonfiguriert
- sagemaker-endpoint-config-prod-Anzahl der Instanzen
- sagemaker-feature-group-tagged
- sagemaker-image-description

- sagemaker-image-tagged
- sagemaker-model-in-vpc
- sagemaker-model-isolation-enabled
- sagemaker-notebook-instance-inside-vpc
- sagemaker-notebook-instance-kms-key-konfiguriert
- sagemaker-notebook-instance-platform-Version
- sagemaker-notebook-instance-root-Zugriffsprüfung
- sagemaker-notebook-no-direct-Internetzugang
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-überprüfen
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- securityhub-enabled
- security-account-information-provided
- service-catalog-shared-within-Organisation
- service-vpc-endpoint-enabled
- sns-encrypted-kms
- sns-topic-message-delivery-Benachrichtigung aktiviert
- sns-topic-no-public-Zugriff
- sqs-queue-no-public-Zugang
- ssm-automation-block-public-teilen
- ssm-automation-logging-enabled
- ssm-document-not-public
- ssm-document-tagged
- step-functions-state-machine-Protokollierung aktiviert
- storagegateway-last-backup-recovery-punkt-erstellt
- storagegateway-resources-in-logically-air-gapped-vault
- storagegateway-resources-protected-by-Ersatzplan
- subnet-auto-assign-public-ip-deaktiviert

- transfer-agreement-description
- transfer-agreement-tagged
- transfer-certificate-description
- transfer-certificate-tagged
- transfer-connector-logging-enabled
- transfer-connector-tagged
- transfer-family-server-no-ftp
- transfer-profile-tagged
- transfer-workflow-description
- transfer-workflow-tagged
- virtualmachine-last-backup-recovery-Punkt erstellt
- virtualmachine-resources-in-logically-air-gapped-vault
- virtualmachine-resources-protected-by-Ersatzplan
- vpc-default-security-group-geschlossen
- vpc-endpoint-enabled
- vpc-flow-logs-enabled
- vpc-network-acl-unused-überprüfen
- vpc-peering-dns-resolution-überprüfen
- vpc-sg-open-only-to-authorized-ports
- vpc-sg-port-restriction-überprüfen
- vpc-vpn-2-tunnels-up
- wafv2-logging-enabled
- WAF 2- rulegroup-logging-enabled
- WAF 2- rulegroup-not-empty
- WAF 2- webacl-not-empty
- waf-regional-rulegroup-not-leer
- waf-regional-rule-not-leer
- waf-regional-webacl-not-leer
- workspaces-root-volume-encryption-aktiviert
- workspaces-user-volume-encryption-aktiviert

Region Europa (Mailand)

Europa (Milan)

- access-keys-rotated
- account-part-of-organizations
- acmpca-certificate-authority-tagged
- acm-certificate-expiration-check
- acm-certificate-rsa-check
- acm-pca-root-ca-deaktiviert
- active-mq-supported-version
- alb-desync-mode-check
- alb-http-drop-invalid-Header-fähig
- alb-http-to-https-Umleitungsprüfung
- alb-internal-scheme-check
- alb-listener-tagged
- alb-waf-enabled
- amplify-app-branch-auto-löschung aktiviert
- amplify-app-description
- amplify-app-tagged
- amplify-branch-performance-mode-aktiviert
- amplify-branch-tagged
- api-gwv2- access-logs-enabled
- api-gwv2- authorization-type-configured
- api-gw-associated-with-WAF
- api-gw-cache-enabled-und-verschlüsselt
- api-gw-endpoint-type-überprüfen
- api-gw-execution-logging-aktiviert
- api-gw-ssl-enabled
- api-gw-xray-enabled
- appconfig-application-description
- appconfig-application-tagged

- appconfig-configuration-profile-tagged
- appconfig-configuration-profile-validators-nicht leer
- appconfig-deployment-strategy-description
- appconfig-deployment-strategy-replicate-zu-ssm
- appconfig-environment-description
- appconfig-environment-tagged
- appconfig-extension-association-tagged
- appconfig-freeform-profile-config-Speicher
- appconfig-hosted-configuration-version-Beschreibung
- appmesh-gateway-route-tagged
- appmesh-mesh-deny-tcp-Weiterleitung
- appmesh-mesh-tagged
- appmesh-route-tagged
- appmesh-virtual-gateway-backend-Standardeinstellungen-TLS
- appmesh-virtual-gateway-logging-file-path-exists
- appmesh-virtual-gateway-tagged
- appmesh-virtual-node-backend-defaults-tls-on
- appmesh-virtual-node-logging-file-path-exists
- appmesh-virtual-node-tagged
- appmesh-virtual-router-tagged
- appmesh-virtual-service-tagged
- approved-amis-by-id
- approved-amis-by-tag
- appsync-associated-with-waf
- appsync-authorization-check
- appsync-cache-encryption-at-ausruhen
- appsync-logging-enabled
- athena-data-catalog-description
- athena-workgroup-description
- athena-workgroup-encrypted-at-ausruhen

- athena-workgroup-enforce-workgroup-Konfiguration
- athena-workgroup-engine-version-automatisches Upgrade
- athena-workgroup-logging-enabled
- aurora-last-backup-recovery-Punkt erstellt
- aurora-meets-restore-time-Ziel
- aurora-mysql-cluster-audit-Protokollierung
- aurora-resources-in-logically-air-gapped-vault
- aurora-resources-protected-by-Backup-Plan
- autoscaling-capacity-rebalancing
- autoscaling-group-elb-healthcheck-erforderlich
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-hop-Grenze
- autoscaling-launch-config-public-ip-deaktiviert
- autoscaling-launch-template
- autoscaling-multiple-az
- autoscaling-multiple-instance-types
- backup-plan-min-frequency-and-min-retention-check
- backup-recovery-point-encrypted
- backup-recovery-point-manual-Löschen-deaktiviert
- backup-recovery-point-minimum-Aufbewahrungsprüfung
- batch-compute-environment-enabled
- batch-compute-environment-managed
- batch-compute-environment-tagged
- batch-job-queue-enabled
- batch-job-queue-tagged
- batch-managed-compute-environment-using-launch-template
- batch-managed-compute-env-compute-resources-tagged
- batch-scheduling-policy-tagged
- beanstalk-enhanced-health-reporting-aktiviert
- clb-desync-mode-check

- clb-multiple-az
- cloudformation-stack-drift-detection-überprüfen
- cloudformation-stack-notification-check
- cloudtrail-all-read-s3- data-event-check
- cloudtrail-all-write-s3- data-event-check
- Wolkenspur-S3- bucket-access-logging
- CloudTrail-S3- bucket-public-access-prohibited
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-action-enabled-überprüfen
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted
- cloud-trail-cloud-watch-logs-aktiviert
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-Validierung aktiviert
- cmk-backing-key-rotation-aktiviert
- codebuild-project-artifact-encryption
- codebuild-project-environment-privileged-überprüfen
- codebuild-project-envvar-awscred-überprüfen
- codebuild-project-logging-enabled
- codebuild-project-s3-log-verschlüsselt
- codebuild-project-source-repo-URL-Prüfung
- codebuild-report-group-encrypted-im Ruhezustand
- codedeploy-auto-rollback-monitor-aktiviert
- codedeploy-deployment-group-auto-rollback-aktiviert
- codedeploy-deployment-group-outdated-instanzen-aktualisieren
- Codedeploy-ec2- minimum-healthy-hosts-configured

- codedeploy-lambda-allatonce-traffic-shift-deaktiviert
- codepipeline-deployment-count-check
- cognito-identity-pool-unauth-Zugriffsprüfung
- cognito-user-pool-advanced-sicherheitsaktiviert
- cognito-user-pool-tagged
- custom-eventbus-policy-attached
- cw-loggroup-retention-period-überprüfen
- datasync-task-data-verification-aktiviert
- datasync-task-logging-enabled
- datasync-task-tagged
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- dms-auto-minor-version-aktualisieren-Prüfung
- dms-endpoint-ssl-configured
- dms-endpoint-tagged
- dms-mongo-db-authentication-aktiviert
- dms-redis-tls-enabled
- dms-replication-not-public
- dms-replication-task-sourcedb-Protokollierung
- dms-replication-task-tagged
- dms-replication-task-targetdb-Protokollierung
- docdb-cluster-audit-logging-aktiviert
- docdb-cluster-backup-retention-überprüfen
- docdb-cluster-deletion-protection-aktiviert
- docdb-cluster-encrypted
- docdb-cluster-encrypted-in-Transit
- docdb-cluster-snapshot-public-verboten
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan

- dynamodb-last-backup-recovery-Punkt erstellt
- dynamodb-meets-restore-time-Ziel
- dynamodb-pitr-enabled
- dynamodb-resources-protected-by-Backup-Plan
- dynamodb-table-deletion-protection-aktiviert
- dynamodb-table-encrypted-kms
- dynamodb-throughput-limit-check
- ebs-in-backup-plan
- ebs-last-backup-recovery-punkt-erstellt
- ebs-meets-restore-time-Ziel
- ebs-optimized-instance
- ebs-resources-in-logically-air-gapped-vault
- ebs-resources-protected-by-Backup-Plan
- ebs-snapshot-public-restorable-überprüfen
- ec2- capacity-reservation-tagged
- ec2- aktiviert client-vpn-connection-log
- ec2- client-vpn-endpoint-tagged
- ec2- -alle client-vpn-not-authorize
- ec2- dhcp-options-tagged
- ec2- ebs-encryption-by-default
- ec2- aktiviert enis-source-destination-check
- ec2-fleet-markiert
- ec2-imdsv2-check
- ec2- instance-detailed-monitoring-enabled
- ec2-ami instance-launched-with-allowed
- ec2- instance-managed-by-ssm
- ec2- instance-multiple-eni-check
- ec2- instance-no-public-ip
- ec2- instance-profile-attached
- ec2- erstellt last-backup-recovery-point

- ec2-2-prüfen launch-template-imdsv
- ec2- -deaktiviert launch-template-public-ip
- ec2- launch-template-tagged
- ec2- managedinstance-applications-blacklisted
- ec2- managedinstance-applications-required
- ec2- managedinstance-inventory-blacklisted
- ec2- managedinstance-platform-check
- ec2- meets-restore-time-target
- ec2- Analyse mit Schlagwörtern network-insights-access-scope
- ec2 network-insights-access-scope - markiert
- ec2- network-insights-path-tagged
- ec2- no-amazon-key-pair
- ec2- prefix-list-tagged
- ec2- -Tresor mit Lücken resources-in-logically-air
- ec2- resources-protected-by-backup -plan
- ec2-eni security-group-attached-to
- ec2- -eni-periodisch security-group-attached-to
- ec2- token-hop-limit-check
- ec2- traffic-mirror-filter-description
- ec2- traffic-mirror-filter-tagged
- ec2- traffic-mirror-target-description
- ec2- traffic-mirror-target-tagged
- ec2- -attach-deaktiviert transit-gateway-auto-vpc
- ec2 transit-gateway-multicast-domain - markiert
- ec2- volume-inuse-check
- ec2- vpn-connection-logging-enabled
- ecr-private-image-scanning-aktiviert
- ecr-private-lifecycle-policy-konfiguriert
- ecr-private-tag-immutability-aktiviert
- ecr-repository-cmk-encryption-aktiviert

- ecr-repository-tagged
- ecs-awsvpc-networking-enabled
- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-container-insights-enabled
- ecs-fargate-latest-platform-Version
- ecs-no-environment-secrets
- ecs-task-definition-log-Konfiguration
- ecs-task-definition-memory-hartes Limit
- ecs-task-definition-network-mode-not-host
- ecs-task-definition-nonroot-Benutzer
- ecs-task-definition-pid-Modus-Check
- ecs-task-definition-user-for-host-mode-check
- efs-access-point-enforce-Stammverzeichnis
- efs-access-point-enforce-Benutzeridentität
- efs-automatic-backups-enabled
- efs-encrypted-check
- efs-filesystem-ct-encrypted
- efs-in-backup-plan
- efs-last-backup-recovery-Punkt erstellt
- efs-meets-restore-time-Ziel
- efs-mount-target-public-zugänglich
- efs-resources-in-logically-air-gapped-vault
- efs-resources-protected-by-Backup-Plan
- eip-attached
- eks-cluster-logging-enabled
- eks-cluster-log-enabled
- eks-cluster-oldest-supported-Ausführung
- eks-cluster-secrets-encrypted
- eks-cluster-supported-version

- eks-endpoint-no-public-Zugang
- eks-secrets-encrypted
- elasticache-auto-minor-version-aktualisieren-Prüfung
- elasticache-rbac-auth-enabled
- elasticache-redis-cluster-automatic-Backup-Check
- elasticache-repl-grp-auto-failover-fähig
- elasticache-repl-grp-encrypted-im Ruhezustand
- elasticache-repl-grp-encryptedunterwegs
- elasticache-repl-grp-redis-auth-aktiviert
- elasticache-subnet-group-check
- elasticache-supported-engine-version
- elasticbeanstalk-application-description
- elasticbeanstalk-application-version-description
- elasticbeanstalk-environment-description
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch
- elasticsearch-node-to-node-Verschlüsselungsprüfung
- elastic-beanstalk-logs-to- Cloudwatch
- elastic-beanstalk-managed-updates-aktiviert
- elbv2- acm-certificate-required
- elv 2- listener-encryption-in-transit
- elbv2-multiple-az
- elbv2- prüfen predefined-security-policy-ssl
- elb-cross-zone-load-Balancing aktiviert
- elb-custom-security-policy-ssl-Prüfung
- elb-deletion-protection-enabled
- elb-logging-enabled
- elb-predefined-security-policy-ssl-Überprüfung
- elb-tls-https-listeners-nur

- emr-block-public-access
- emr-kerberos-enabled
- emr-master-no-public-ip
- emr-security-configuration-encryption-ruh dich aus
- emr-security-configuration-encryption-Transit
- encrypted-volumes
- event-data-store-cmk-Verschlüsselung aktiviert
- fis-experiment-template-log-Konfiguration ist vorhanden
- fis-experiment-template-tagged
- fms-shield-resource-policy-überprüfen
- fms-webacl-resource-policy-überprüfen
- fms-webacl-rulegroup-association-überprüfen
- fsx-last-backup-recovery-Punkt erstellt
- fsx-lustre-copy-tagszu Backups
- fsx-meets-restore-time-Ziel
- fsx-ontap-deployment-type-überprüfen
- fsx-openzfs-copy-tags-aktiviert
- fsx-openzfs-deployment-type-überprüfen
- fsx-resources-protected-by-Ersatzplan
- fsx-windows-audit-log-konfiguriert
- fsx-windows-deployment-type-überprüfen
- glb-listener-tagged
- glue-job-logging-enabled
- glue-ml-transform-encrypted-im Ruhezustand
- glue-spark-job-supported-Ausführung
- GuardDuty-EC2- protection-runtime-enabled
- guardduty-ecs-protection-runtime-aktiviert
- guardduty-eks-protection-audit-aktiviert
- guardduty-eks-protection-runtime-aktiviert
- guardduty-enabled-centralized

- guardduty-lambda-protection-enabled
- guardduty-malware-protection-enabled
- guardduty-non-archived-findings
- guardduty-rds-protection-enabled
- guardduty-runtime-monitoring-enabled
- GuardDuty-S3-Schutz aktiviert
- iam-customer-policy-blocked-kms-Aktionen
- iam-external-access-analyzer-aktiviert
- iam-group-has-users-überprüfen
- iam-inline-policy-blocked-KMS-Aktionen
- iam-no-inline-policy-überprüfen
- iam-password-policy
- iam-policy-blacklisted-check
- iam-policy-in-use
- iam-policy-no-statements-with-admin-access
- iam-policy-no-statements-with-full-access
- iam-role-managed-policy-überprüfen
- iam-root-access-key-überprüfen
- iam-user-group-membership-überprüfen
- iam-user-mfa-enabled
- iam-user-no-policies-überprüfen
- iam-user-unused-credentials-überprüfen
- incoming-ssh-disabled
- inspector-ec2-Scan aktiviert
- inspector-ecr-scan-enabled
- inspector-lambda-standard-scan-aktiviert
- instances-in-vpc
- internet-gateway-authorized-vpc-nur
- kinesis-firehose-delivery-stream-verschlüsselt
- kinesis-stream-backup-retention-überprüfen

- kinesis-stream-encrypted
- kms-key-policy-no-öffentlich zugänglich
- lambda-concurrency-check
- lambda-dlq-check
- lambda-function-public-access-verboten
- lambda-function-settings-check
- lambda-function-xray-enabled
- lambda-inside-vpc
- lambda-vpc-multi-az-überprüfen
- macie-auto-sensitive-data-Discovery-Check
- macie-status-check
- mariadb-publish-logs-to-Cloudwatch-Protokolle
- mfa-enabled-for-iam-Konsolenzugriff
- mq-active-broker-ldap-Authentifizierung
- mq-active-deployment-mode
- mq-active-single-instance-broker-storage-type-efs
- mq-automatic-minor-version-Upgrade aktiviert
- mq-auto-minor-version-upgrade-fähig
- mq-broker-general-logging-aktiviert
- mq-cloudwatch-audit-logging-aktiviert
- mq-cloudwatch-audit-log-aktiviert
- mq-no-public-access
- mq-rabbit-deployment-mode
- msk-cluster-public-access-deaktiviert
- msk-enhanced-monitoring-enabled
- msk-in-cluster-node-require-tls
- msk-unrestricted-access-check
- multi-region-cloud-trail-aktiviert
- nacl-no-unrestricted-ssh-rdp
- netfw-deletion-protection-enabled

- netfw-logging-enabled
- netfw-multi-az-enabled
- netfw-policy-default-action-fragment-Pakete
- netfw-policy-default-action-vollständige Pakete
- netfw-policy-rule-group-assoziiert
- netfw-stateless-rule-group-nicht leer
- netfw-subnet-change-protection-aktiviert
- nlb-cross-zone-load-Balancing aktiviert
- nlb-internal-scheme-check
- nlb-listener-tagged
- nlb-logging-enabled
- no-unrestricted-route-to-igw
- opensearch-access-control-enabled
- opensearch-audit-logging-enabled
- opensearch-data-node-fault-Toleranz
- opensearch-encrypted-at-rest
- opensearch-https-required
- opensearch-in-vpc-only
- opensearch-logs-to-cloudwatch
- opensearch-node-to-node-Verschlüsselungsprüfung
- opensearch-primary-node-fault-Toleranz
- opensearch-update-check
- rabbit-mq-supported-version
- rds-aurora-mysql-audit-Protokollierung aktiviert
- rds-aurora-postgresql-logs-zu-Cloud-Watch
- rds-automatic-minor-version-upgrade-fähig
- rds-cluster-auto-minor-version-upgrade-enable
- rds-cluster-default-admin-überprüfen
- rds-cluster-deletion-protection-aktiviert
- rds-cluster-encrypted-at-ausruhen

- rds-cluster-iam-authentication-aktiviert
- rds-cluster-multi-az-aktiviert
- rds-enhanced-monitoring-enabled
- rds-instance-default-admin-überprüfen
- rds-instance-deletion-protection-aktiviert
- rds-instance-iam-authentication-aktiviert
- rds-instance-public-access-überprüfen
- rds-instance-subnet-igw-überprüfen
- rds-in-backup-plan
- rds-last-backup-recovery-Punkt erstellt
- rds-logging-enabled
- rds-mariadb-instance-encryptedwährend des Transports
- rds-meets-restore-time-Ziel
- rds-multi-az-support
- rds-mysql-instance-encryptedunterwegs
- rds-postgresql-logs-to- Cloudwatch
- rds-postgres-instance-encryptedunterwegs
- rds-proxy-tls-encryption
- rds-resources-protected-by-Backup-Plan
- rds-snapshot-encrypted
- rds-sqlserver-encrypted-in-Transit
- rds-sql-server-logszur Cloud-Überwachung
- rds-storage-encrypted
- redshift-audit-logging-enabled
- redshift-backup-enabled
- redshift-cluster-configuration-check
- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check
- redshift-cluster-multi-az-aktiviert
- redshift-cluster-parameter-group-markiert

- redshift-cluster-public-access-überprüfen
- redshift-cluster-subnet-group-Multi-Az
- redshift-default-admin-check
- redshift-default-db-name-überprüfen
- redshift-enhanced-vpc-routing-aktiviert
- redshift-require-tls-ssl
- redshift-unrestricted-port-access
- required-tags
- restricted-incoming-traffic
- root-account-hardware-mfa-aktiviert
- root-account-mfa-enabled
- nur s3- access-point-in-vpc
- s3- -Blöcke access-point-public-access
- s3- -Blöcke account-level-public-access
- s3- -Blocke-periodisch account-level-public-access
- s 3- bucket-acl-prohibited
- s-3 bucket-blacklisted-actions-prohibited
- s3- bucket-cross-region-replication -aktiviert
- s-3 bucket-default-lock-enabled
- s3 bucket-level-public-access - verboten
- s3- bucket-logging-enabled
- s-3 bucket-mfa-delete-enabled
- s-3 bucket-policy-grantee-check
- s3- bucket-policy-not-more -freizügig
- s 3- bucket-public-read-prohibited
- s-3 bucket-public-write-prohibited
- s-3 bucket-replication-enabled
- s3- bucket-server-side-encryption -aktiviert
- s-3 bucket-ssl-requests-only
- s3-Bucket-Tagged

- s-3 bucket-versioning-enabled
- s-3 default-encryption-kms
- s-3 event-notifications-enabled
- s3 last-backup-recovery-point - erstellt
- s3- lifecycle-policy-check
- s-3 meets-restore-time-target
- resources-protected-by-backups3-plan
- s 3- version-lifecycle-policy-check
- sagemaker-app-image-config-markiert
- sagemaker-domain-in-vpc
- sagemaker-domain-tagged
- sagemaker-endpoint-configuration-kms-schlüsselkonfiguriert
- sagemaker-endpoint-config-prod-Anzahl der Instanzen
- sagemaker-feature-group-tagged
- sagemaker-image-description
- sagemaker-image-tagged
- sagemaker-model-in-vpc
- sagemaker-model-isolation-enabled
- sagemaker-notebook-instance-inside-vpc
- sagemaker-notebook-instance-kms-key-konfiguriert
- sagemaker-notebook-instance-platform-Version
- sagemaker-notebook-instance-root-Zugriffsprüfung
- sagemaker-notebook-no-direct-Internetzugang
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-überprüfen
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- securityhub-enabled
- security-account-information-provided

- service-catalog-shared-within-Organisation
- service-vpc-endpoint-enabled
- sns-encrypted-kms
- sns-topic-message-delivery-Benachrichtigung aktiviert
- sns-topic-no-public-Zugriff
- sqs-queue-no-public-Zugang
- ssm-automation-block-public-teilen
- ssm-automation-logging-enabled
- ssm-document-not-public
- ssm-document-tagged
- step-functions-state-machine-Protokollierung aktiviert
- storagegateway-last-backup-recovery-punkt-erstellt
- storagegateway-resources-in-logically-air-gapped-vault
- storagegateway-resources-protected-by-Ersatzplan
- subnet-auto-assign-public-ip-deaktiviert
- transfer-agreement-description
- transfer-agreement-tagged
- transfer-certificate-description
- transfer-certificate-tagged
- transfer-connector-logging-enabled
- transfer-connector-tagged
- transfer-family-server-no-ftp
- transfer-profile-tagged
- transfer-workflow-description
- transfer-workflow-tagged
- virtualmachine-last-backup-recovery-Punkt erstellt
- virtualmachine-resources-in-logically-air-gapped-vault
- virtualmachine-resources-protected-by-Ersatzplan
- vpc-default-security-group-geschlossen
- vpc-endpoint-enabled

- vpc-flow-logs-enabled
- vpc-network-acl-unused-überprüfen
- vpc-peering-dns-resolution-überprüfen
- vpc-sg-open-only-to-authorized-ports
- vpc-sg-port-restriction-überprüfen
- vpc-vpn-2-tunnels-up
- wafv2-logging-enabled
- WAF 2- rulegroup-logging-enabled
- WAF 2- rulegroup-not-empty
- WAF 2- webacl-not-empty
- waf-regional-rulegroup-not-leer
- waf-regional-rule-not-leer
- waf-regional-webacl-not-leer

Region Europa (Paris)

Europa (Paris)

- access-keys-rotated
- account-part-of-organizations
- acmpca-certificate-authority-tagged
- acm-certificate-expiration-check
- acm-certificate-rsa-check
- acm-pca-root-ca-deaktiviert
- active-mq-supported-version
- alb-desync-mode-check
- alb-http-drop-invalid-Header-fähig
- alb-http-to-https-Umleitungsprüfung
- alb-internal-scheme-check
- alb-listener-tagged
- alb-waf-enabled
- amplify-app-branch-auto-löschung aktiviert

- amplify-app-description
- amplify-app-tagged
- amplify-branch-performance-mode-aktiviert
- amplify-branch-tagged
- api-gwv2- access-logs-enabled
- api-gwv2- authorization-type-configured
- api-gw-associated-with-WAF
- api-gw-cache-enabled-und-verschlüsselt
- api-gw-endpoint-type-überprüfen
- api-gw-execution-logging-aktiviert
- api-gw-ssl-enabled
- api-gw-xray-enabled
- appconfig-application-description
- appconfig-application-tagged
- appconfig-configuration-profile-tagged
- appconfig-configuration-profile-validators-nicht leer
- appconfig-deployment-strategy-description
- appconfig-deployment-strategy-replicate-zu-ssm
- appconfig-environment-description
- appconfig-environment-tagged
- appconfig-extension-association-tagged
- appconfig-freeform-profile-config-Speicher
- appconfig-hosted-configuration-version-Beschreibung
- appflow-flow-tagged
- appmesh-gateway-route-tagged
- appmesh-mesh-deny-tcp-Weiterleitung
- appmesh-mesh-tagged
- appmesh-route-tagged
- appmesh-virtual-gateway-backend-Standardeinstellungen-TLS
- appmesh-virtual-gateway-logging-file-path-exists

- appmesh-virtual-gateway-tagged
- appmesh-virtual-node-backend-defaults-tls-on
- appmesh-virtual-node-logging-file-path-exists
- appmesh-virtual-node-tagged
- appmesh-virtual-router-tagged
- appmesh-virtual-service-tagged
- approved-amis-by-id
- approved-amis-by-tag
- apprunner-service-in-vpc
- apprunner-service-no-public-Zugang
- apprunner-service-observability-enabled
- apprunner-service-tagged
- apprunner-vpc-connector-tagged
- appsync-associated-with-waf
- appsync-authorization-check
- appsync-cache-encryption-at-ausruhen
- appsync-logging-enabled
- athena-data-catalog-description
- athena-prepared-statement-description
- athena-workgroup-description
- athena-workgroup-encrypted-at-ausruhen
- athena-workgroup-enforce-workgroup-Konfiguration
- athena-workgroup-engine-version-automatisches Upgrade
- athena-workgroup-logging-enabled
- aurora-last-backup-recovery-Punkt erstellt
- aurora-meets-restore-time-Ziel
- aurora-mysql-backtracking-enabled
- aurora-mysql-cluster-audit-Protokollierung
- aurora-resources-in-logically-air-gapped-vault
- aurora-resources-protected-by-Backup-Plan

- autoscaling-capacity-rebalancing
- autoscaling-group-elb-healthcheck-erforderlich
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-hop-Grenze
- autoscaling-launch-config-public-ip-deaktiviert
- autoscaling-launch-template
- autoscaling-multiple-az
- autoscaling-multiple-instance-types
- backup-plan-min-frequency-and-min-retention-check
- backup-recovery-point-encrypted
- backup-recovery-point-manual-Löschen-deaktiviert
- backup-recovery-point-minimum-Aufbewahrungsprüfung
- batch-compute-environment-enabled
- batch-compute-environment-managed
- batch-compute-environment-tagged
- batch-job-queue-enabled
- batch-job-queue-tagged
- batch-managed-compute-environment-using-launch-template
- batch-managed-compute-env-compute-resources-tagged
- batch-scheduling-policy-tagged
- beanstalk-enhanced-health-reporting-aktiviert
- cassandra-keyspace-tagged
- clb-desync-mode-check
- clb-multiple-az
- cloudformation-stack-drift-detection-überprüfen
- cloudformation-stack-notification-check
- cloudtrail-all-read-s3- data-event-check
- cloudtrail-all-write-s3- data-event-check
- Wolkenspur-S3- bucket-access-logging
- CloudTrail-S3- bucket-public-access-prohibited

- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-action-enabled-überprüfen
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted
- cloud-trail-cloud-watch-logs-aktiviert
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-Validierung aktiviert
- cmk-backing-key-rotation-aktiviert
- codebuild-project-artifact-encryption
- codebuild-project-environment-privileged-überprüfen
- codebuild-project-envvar-awscred-überprüfen
- codebuild-project-logging-enabled
- codebuild-project-s3-log-verschlüsselt
- codebuild-project-source-repo-URL-Prüfung
- codebuild-report-group-encrypted-im Ruhezustand
- codedeploy-auto-rollback-monitor-aktiviert
- codedeploy-deployment-group-auto-rollback-aktiviert
- codedeploy-deployment-group-outdated-instanzen-aktualisieren
- Codedeploy-ec2- minimum-healthy-hosts-configured
- codedeploy-lambda-allatonce-traffic-shift-deaktiviert
- codepipeline-deployment-count-check
- codepipeline-region-fanout-check
- cognito-identity-pool-unauth-Zugriffsprüfung
- cognito-user-pool-advanced-sicherheitsaktiviert
- cognito-user-pool-tagged
- custom-eventbus-policy-attached

- custom-schema-registry-policy-angehängt
- cw-loggroup-retention-period-überprüfen
- datasync-task-data-verification-aktiviert
- datasync-task-logging-enabled
- datasync-task-tagged
- dax-encryption-enabled
- dax-tls-endpoint-encryption
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- dms-auto-minor-version-aktualisieren-Prüfung
- dms-endpoint-ssl-configured
- dms-endpoint-tagged
- dms-mongo-db-authentication-aktiviert
- dms-neptune-iam-authorization-aktiviert
- dms-redis-tls-enabled
- dms-replication-not-public
- dms-replication-task-sourcedb-Protokollierung
- dms-replication-task-tagged
- dms-replication-task-targetdb-Protokollierung
- docdb-cluster-audit-logging-aktiviert
- docdb-cluster-backup-retention-überprüfen
- docdb-cluster-deletion-protection-aktiviert
- docdb-cluster-encrypted
- docdb-cluster-encrypted-in-Transit
- docdb-cluster-snapshot-public-verboten
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-last-backup-recovery-Punkt erstellt
- dynamodb-meets-restore-time-Ziel

- dynamodb-pitr-enabled
- dynamodb-resources-protected-by-Backup-Plan
- dynamodb-table-deletion-protection-aktiviert
- dynamodb-table-encrypted-kms
- dynamodb-table-encryption-enabled
- dynamodb-throughput-limit-check
- ebs-in-backup-plan
- ebs-last-backup-recovery-punkt-erstellt
- ebs-meets-restore-time-Ziel
- ebs-optimized-instance
- ebs-resources-in-logically-air-gapped-vault
- ebs-resources-protected-by-Backup-Plan
- ebs-snapshot-public-restorable-überprüfen
- ec2- capacity-reservation-tagged
- ec2- carrier-gateway-tagged
- ec2- aktiviert client-vpn-connection-log
- ec2- client-vpn-endpoint-tagged
- ec2- -alle client-vpn-not-authorize
- ec2- dhcp-options-tagged
- ec2- ebs-encryption-by-default
- ec2- aktiviert enis-source-destination-check
- ec2-fleet-markiert
- ec2-imdsv2-check
- ec2- instance-detailed-monitoring-enabled
- ec2-ami instance-launched-with-allowed
- ec2- instance-managed-by-ssm
- ec2- instance-multiple-eni-check
- ec2- instance-no-public-ip
- ec2- instance-profile-attached
- ec2- erstellt last-backup-recovery-point

- ec2-2-prüfen launch-template-imdsv
- ec2- -deaktiviert launch-template-public-ip
- ec2- launch-template-tagged
- ec2- managedinstance-applications-blacklisted
- ec2- managedinstance-applications-required
- ec2- prüfen managedinstance-association-compliance-status
- ec2- managedinstance-inventory-blacklisted
- ec2- prüfen managedinstance-patch-compliance-status
- ec2- managedinstance-platform-check
- ec2- meets-restore-time-target
- ec2- Analyse mit Schlagwörtern network-insights-access-scope
- ec2 network-insights-access-scope - markiert
- ec2- network-insights-path-tagged
- ec2- no-amazon-key-pair
- ec2- prefix-list-tagged
- ec2- -Tresor mit Lücken resources-in-logically-air
- ec2- resources-protected-by-backup -plan
- ec2-eni security-group-attached-to
- ec2- -eni-periodisch security-group-attached-to
- ec2-stopped-instance
- ec2- token-hop-limit-check
- ec2- traffic-mirror-filter-description
- ec2- traffic-mirror-filter-tagged
- ec2- traffic-mirror-session-description
- ec2- traffic-mirror-session-tagged
- ec2- traffic-mirror-target-description
- ec2- traffic-mirror-target-tagged
- ec2- -attach-deaktiviert transit-gateway-auto-vpc
- ec2 transit-gateway-multicast-domain - markiert
- ec2- volume-inuse-check

- ec2- vpn-connection-logging-enabled
- ecr-private-image-scanning-aktiviert
- ecr-private-lifecycle-policy-konfiguriert
- ecr-private-tag-immutability-aktiviert
- ecr-repository-cmk-encryption-aktiviert
- ecr-repository-tagged
- ecs-awsvpc-networking-enabled
- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-container-insights-enabled
- ecs-fargate-latest-platform-Version
- ecs-no-environment-secrets
- ecs-task-definition-log-Konfiguration
- ecs-task-definition-memory-hartes Limit
- ecs-task-definition-network-mode-not-host
- ecs-task-definition-nonroot-Benutzer
- ecs-task-definition-pid-Modus-Check
- ecs-task-definition-user-for-host-mode-check
- efs-access-point-enforce-Stammverzeichnis
- efs-access-point-enforce-Benutzeridentität
- efs-automatic-backups-enabled
- efs-encrypted-check
- efs-filesystem-ct-encrypted
- efs-in-backup-plan
- efs-last-backup-recovery-Punkt erstellt
- efs-meets-restore-time-Ziel
- efs-mount-target-public-zugänglich
- efs-resources-in-logically-air-gapped-vault
- efs-resources-protected-by-Backup-Plan
- eip-attached

- eks-cluster-logging-enabled
- eks-cluster-log-enabled
- eks-cluster-oldest-supported-Ausführung
- eks-cluster-secrets-encrypted
- eks-cluster-supported-version
- eks-endpoint-no-public-Zugang
- eks-secrets-encrypted
- elasticache-auto-minor-version-Upgrade-Check
- elasticache-rbac-auth-enabled
- elasticache-redis-cluster-automatic-Backup-Check
- elasticache-repl-grp-auto-failover-fähig
- elasticache-repl-grp-encrypted-im Ruhezustand
- elasticache-repl-grp-encryptedunterwegs
- elasticache-repl-grp-redis-auth-aktiviert
- elasticache-subnet-group-check
- elasticache-supported-engine-version
- elasticbeanstalk-application-description
- elasticbeanstalk-application-version-description
- elasticbeanstalk-environment-description
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch
- elasticsearch-node-to-node-Verschlüsselungsprüfung
- elastic-beanstalk-logs-to- Cloudwatch
- elastic-beanstalk-managed-updates-aktiviert
- elbv2- acm-certificate-required
- elv 2- listener-encryption-in-transit
- elbv2-multiple-az
- elbv2- prüfen predefined-security-policy-ssl
- elb-acm-certificate-required

- elb-cross-zone-load-Balancing aktiviert
- elb-custom-security-policy-ssl-Prüfung
- elb-deletion-protection-enabled
- elb-logging-enabled
- elb-predefined-security-policy-ssl-Überprüfung
- elb-tls-https-listeners-nur
- emr-block-public-access
- emr-kerberos-enabled
- emr-master-no-public-ip
- emr-security-configuration-encryption-ruh dich aus
- emr-security-configuration-encryption-Transit
- encrypted-volumes
- event-data-store-cmk-Verschlüsselung aktiviert
- fis-experiment-template-log-Konfiguration ist vorhanden
- fis-experiment-template-tagged
- fms-shield-resource-policy-überprüfen
- fms-webacl-resource-policy-überprüfen
- fms-webacl-rulegroup-association-überprüfen
- fsx-last-backup-recovery-Punkt erstellt
- fsx-lustre-copy-tagszu Backups
- fsx-meets-restore-time-Ziel
- fsx-ontap-deployment-type-überprüfen
- fsx-openzfs-copy-tags-aktiviert
- fsx-openzfs-deployment-type-überprüfen
- fsx-resources-protected-by-Ersatzplan
- fsx-windows-audit-log-konfiguriert
- glb-listener-tagged
- global-endpoint-event-replication-aktiviert
- glue-job-logging-enabled
- glue-ml-transform-encrypted-im Ruhezustand

- glue-spark-job-supported-Ausführung
- GuardDuty-EC2- protection-runtime-enabled
- guardduty-ecs-protection-runtime-aktiviert
- guardduty-eks-protection-audit-aktiviert
- guardduty-eks-protection-runtime-aktiviert
- guardduty-enabled-centralized
- guardduty-lambda-protection-enabled
- guardduty-malware-protection-enabled
- guardduty-non-archived-findings
- guardduty-rds-protection-enabled
- guardduty-runtime-monitoring-enabled
- GuardDuty-S3-Schutz aktiviert
- iam-customer-policy-blocked-kms-Aktionen
- iam-external-access-analyzer-aktiviert
- iam-group-has-users-überprüfen
- iam-inline-policy-blocked-KMS-Aktionen
- iam-no-inline-policy-überprüfen
- iam-password-policy
- iam-policy-blacklisted-check
- iam-policy-in-use
- iam-policy-no-statements-with-admin-access
- iam-policy-no-statements-with-full-access
- iam-role-managed-policy-überprüfen
- iam-root-access-key-überprüfen
- iam-user-group-membership-überprüfen
- iam-user-mfa-enabled
- iam-user-no-policies-überprüfen
- iam-user-unused-credentials-überprüfen
- incoming-ssh-disabled
- inspector-ec2-Scan aktiviert

- inspector-ecr-scan-enabled
- inspector-lambda-standard-scan-aktiviert
- instances-in-vpc
- internet-gateway-authorized-vpc-nur
- iot-authorizer-token-signing-aktiviert
- kinesis-firehose-delivery-stream-verschlüsselt
- kinesis-stream-backup-retention-überprüfen
- kinesis-stream-encrypted
- kms-cmk-not-scheduled-zum Löschen
- kms-key-policy-no-öffentlicher Zugang
- lambda-concurrency-check
- lambda-dlq-check
- lambda-function-public-access-verboten
- lambda-function-settings-check
- lambda-function-xray-enabled
- lambda-inside-vpc
- lambda-vpc-multi-az-überprüfen
- lightsail-bucket-tagged
- lightsail-certificate-tagged
- lightsail-disk-tagged
- macie-auto-sensitive-data-Discovery-Check
- macie-status-check
- mariadb-publish-logs-to-Cloudwatch-Protokolle
- mfa-enabled-for-iam-Konsolenzugriff
- mq-active-broker-ldap-Authentifizierung
- mq-active-deployment-mode
- mq-active-single-instance-broker-storage-type-efs
- mq-automatic-minor-version-Upgrade aktiviert
- mq-auto-minor-version-upgrade-fähig
- mq-broker-general-logging-aktiviert

- mq-cloudwatch-audit-logging-aktiviert
- mq-cloudwatch-audit-log-aktiviert
- mq-no-public-access
- mq-rabbit-deployment-mode
- msk-cluster-public-access-deaktiviert
- msk-connect-connector-logging-aktiviert
- msk-enhanced-monitoring-enabled
- msk-in-cluster-node-require-tls
- msk-unrestricted-access-check
- multi-region-cloud-trail-aktiviert
- nacl-no-unrestricted-ssh-rdp
- neptune-cluster-backup-retention-überprüfen
- neptune-cluster-cloudwatch-log-exportfähig
- neptune-cluster-copy-tags-to-snapshot-enabled
- neptune-cluster-deletion-protection-aktiviert
- neptune-cluster-encrypted
- neptune-cluster-iam-database-Authentifizierung
- neptune-cluster-multi-az-aktiviert
- neptune-cluster-snapshot-encrypted
- neptune-cluster-snapshot-public-verboten
- netfw-deletion-protection-enabled
- netfw-logging-enabled
- netfw-multi-az-enabled
- netfw-policy-default-action-fragment-Pakete
- netfw-policy-default-action-vollständige Pakete
- netfw-policy-rule-group-assoziiert
- netfw-stateless-rule-group-nicht leer
- netfw-subnet-change-protection-aktiviert
- nlb-cross-zone-load-Balancing aktiviert
- nlb-internal-scheme-check

- nlb-listener-tagged
- nlb-logging-enabled
- no-unrestricted-route-to-igw
- opensearch-access-control-enabled
- opensearch-audit-logging-enabled
- opensearch-data-node-fault-Toleranz
- opensearch-encrypted-at-rest
- opensearch-https-required
- opensearch-in-vpc-only
- opensearch-logs-to-cloudwatch
- opensearch-node-to-node-Verschlüsselungsprüfung
- opensearch-primary-node-fault-Toleranz
- opensearch-update-check
- rabbit-mq-supported-version
- rds-aurora-mysql-audit-Protokollierung aktiviert
- rds-aurora-postgresql-logs-zu-Cloud-Watch
- rds-automatic-minor-version-upgrade-fähig
- rds-cluster-auto-minor-version-upgrade-enable
- rds-cluster-default-admin-überprüfen
- rds-cluster-deletion-protection-aktiviert
- rds-cluster-encrypted-at-ausruhen
- rds-cluster-iam-authentication-aktiviert
- rds-cluster-multi-az-aktiviert
- rds-enhanced-monitoring-enabled
- rds-instance-default-admin-überprüfen
- rds-instance-deletion-protection-aktiviert
- rds-instance-iam-authentication-aktiviert
- rds-instance-public-access-überprüfen
- rds-instance-subnet-igw-überprüfen
- rds-in-backup-plan

- rds-last-backup-recovery-Punkt erstellt
- rds-logging-enabled
- rds-mariadb-instance-encryptedwährend des Transports
- rds-meets-restore-time-Ziel
- rds-multi-az-support
- rds-mysql-instance-encryptedunterwegs
- rds-postgresql-logs-to- Cloudwatch
- rds-postgres-instance-encryptedunterwegs
- rds-proxy-tls-encryption
- rds-resources-protected-by-Backup-Plan
- rds-snapshots-public-prohibited
- rds-snapshot-encrypted
- rds-sqlserver-encrypted-in-Transit
- rds-sql-server-logszur Cloud-Überwachung
- rds-storage-encrypted
- redshift-audit-logging-enabled
- redshift-backup-enabled
- redshift-cluster-configuration-check
- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check
- redshift-cluster-multi-az-aktiviert
- redshift-cluster-parameter-group-markiert
- redshift-cluster-public-access-überprüfen
- redshift-cluster-subnet-group-Multi-Az
- redshift-default-admin-check
- redshift-default-db-name-überprüfen
- redshift-enhanced-vpc-routing-aktiviert
- redshift-require-tls-ssl
- redshift-serverless-default-admin-überprüfen
- redshift-serverless-default-db-Namenscheck

- redshift-serverless-namespace-cmk-Verschlüsselung
- redshift-serverless-publish-logs-zu-Cloud-Watch
- redshift-serverless-workgroup-encryptedauf dem Weg
- redshift-serverless-workgroup-no-öffentlich zugänglich
- redshift-serverless-workgroup-routes-innerhalb von VPC
- redshift-unrestricted-port-access
- required-tags
- restricted-incoming-traffic
- root-account-hardware-mfa-aktiviert
- root-account-mfa-enabled
- nur s3- access-point-in-vpc
- s3- -Blöcke access-point-public-access
- s3- -Blöcke account-level-public-access
- s3- -Blocke-periodisch account-level-public-access
- s 3- bucket-acl-prohibited
- s-3 bucket-blacklisted-actions-prohibited
- s3- bucket-cross-region-replication -aktiviert
- s-3 bucket-default-lock-enabled
- s3 bucket-level-public-access - verboten
- s3- bucket-logging-enabled
- s-3 bucket-mfa-delete-enabled
- s-3 bucket-policy-grantee-check
- s3- bucket-policy-not-more -freizügig
- s 3- bucket-public-read-prohibited
- s-3 bucket-public-write-prohibited
- s-3 bucket-replication-enabled
- s3- bucket-server-side-encryption -aktiviert
- s-3 bucket-ssl-requests-only
- s3-Bucket-Tagged
- s-3 bucket-versioning-enabled

- s-3 default-encryption-kms
- s-3 event-notifications-enabled
- s3 last-backup-recovery-point - erstellt
- s3- lifecycle-policy-check
- s-3 meets-restore-time-target
- s3- resources-in-logically-air -Tresor mit Lücken
- s3 resources-protected-by-backup - -Plan
- s 3- version-lifecycle-policy-check
- sagemaker-app-image-config-markiert
- sagemaker-domain-in-vpc
- sagemaker-domain-tagged
- sagemaker-endpoint-configuration-kms-schlüsselkonfiguriert
- sagemaker-endpoint-config-prod-Anzahl der Instanzen
- sagemaker-feature-group-tagged
- sagemaker-image-description
- sagemaker-image-tagged
- sagemaker-model-in-vpc
- sagemaker-model-isolation-enabled
- sagemaker-notebook-instance-inside-vpc
- sagemaker-notebook-instance-kms-key-konfiguriert
- sagemaker-notebook-instance-platform-Version
- sagemaker-notebook-instance-root-Zugriffsprüfung
- sagemaker-notebook-no-direct-Internetzugang
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-überprüfen
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- securityhub-enabled
- security-account-information-provided

- service-catalog-shared-within-Organisation
- service-vpc-endpoint-enabled
- sns-encrypted-kms
- sns-topic-message-delivery-Benachrichtigung aktiviert
- sns-topic-no-public-Zugriff
- sqs-queue-no-public-Zugang
- ssm-automation-block-public-teilen
- ssm-automation-logging-enabled
- ssm-document-not-public
- ssm-document-tagged
- step-functions-state-machine-Protokollierung aktiviert
- storagegateway-last-backup-recovery-punkt-erstellt
- storagegateway-resources-in-logically-air-gapped-vault
- storagegateway-resources-protected-by-Ersatzplan
- subnet-auto-assign-public-ip-deaktiviert
- transfer-agreement-description
- transfer-agreement-tagged
- transfer-certificate-description
- transfer-certificate-tagged
- transfer-connector-logging-enabled
- transfer-connector-tagged
- transfer-family-server-no-ftp
- transfer-profile-tagged
- transfer-workflow-description
- transfer-workflow-tagged
- virtualmachine-last-backup-recovery-Punkt erstellt
- virtualmachine-resources-in-logically-air-gapped-vault
- virtualmachine-resources-protected-by-Ersatzplan
- vpc-default-security-group-geschlossen
- vpc-endpoint-enabled

- vpc-flow-logs-enabled
- vpc-network-acl-unused-überprüfen
- vpc-peering-dns-resolution-überprüfen
- vpc-sg-open-only-to-authorized-ports
- vpc-sg-port-restriction-überprüfen
- vpc-vpn-2-tunnels-up
- wafv2-logging-enabled
- WAF 2- rulegroup-logging-enabled
- WAF 2- rulegroup-not-empty
- WAF 2- webacl-not-empty
- waf-regional-rulegroup-not-leer
- waf-regional-rule-not-leer
- waf-regional-webacl-not-leer

Region Europa (Spanien)

Europa (Spain)

- account-part-of-organizations
- acmpca-certificate-authority-tagged
- acm-certificate-expiration-check
- acm-certificate-rsa-check
- acm-pca-root-ca-deaktiviert
- alb-desync-mode-check
- alb-http-drop-invalid-Header-fähig
- alb-http-to-https-Umleitungsprüfung
- alb-internal-scheme-check
- alb-waf-enabled
- api-gw-associated-with-WAF
- api-gw-cache-enabled-und-verschlüsselt
- api-gw-endpoint-type-überprüfen
- api-gw-execution-logging-aktiviert

- api-gw-ssl-enabled
- api-gw-xray-enabled
- appconfig-deployment-strategy-description
- appconfig-deployment-strategy-replicate-zu-ssm
- appconfig-extension-association-tagged
- approved-amis-by-id
- approved-amis-by-tag
- appsync-authorization-check
- appsync-logging-enabled
- athena-data-catalog-description
- athena-prepared-statement-description
- athena-workgroup-description
- athena-workgroup-enforce-workgroup-Konfiguration
- athena-workgroup-engine-version-automatisches Upgrade
- athena-workgroup-logging-enabled
- aurora-last-backup-recovery-Punkt erstellt
- aurora-meets-restore-time-Ziel
- aurora-mysql-cluster-audit-Protokollierung
- aurora-resources-in-logically-air-gapped-vault
- aurora-resources-protected-by-Backup-Plan
- autoscaling-group-elb-healthcheck-erforderlich
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-hop-Grenze
- autoscaling-launch-config-public-ip-deaktiviert
- autoscaling-launch-template
- autoscaling-multiple-az
- autoscaling-multiple-instance-types
- backup-plan-min-frequency-and-min-retention-check
- backup-recovery-point-encrypted
- backup-recovery-point-manual-Löschen-deaktiviert

- backup-recovery-point-minimum-Aufbewahrungsprüfung
- batch-compute-environment-enabled
- batch-compute-environment-managed
- batch-compute-environment-tagged
- batch-job-queue-enabled
- batch-job-queue-tagged
- batch-managed-compute-environment-using-launch-template
- batch-managed-compute-env-compute-resources-tagged
- batch-scheduling-policy-tagged
- clb-multiple-az
- cloudtrail-all-read-s3- data-event-check
- cloudtrail-all-write-s3- data-event-check
- Wolkenspur-S3- bucket-access-logging
- CloudTrail-S3- bucket-public-access-prohibited
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-action-enabled-überprüfen
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted
- cloud-trail-cloud-watch-logs-aktiviert
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-Validierung aktiviert
- cmk-backing-key-rotation-aktiviert
- codebuild-project-envvar-awscred-überprüfen
- codebuild-project-logging-enabled
- codebuild-project-s3-log-verschlüsselt
- codebuild-project-source-repo-URL-Prüfung

- codebuild-report-group-encrypted-im Ruhezustand
- cognito-user-pool-tagged
- custom-eventbus-policy-attached
- cw-loggroup-retention-period-überprüfen
- datasync-task-data-verification-aktiviert
- datasync-task-logging-enabled
- datasync-task-tagged
- dax-encryption-enabled
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- dms-replication-not-public
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-last-backup-recovery-punkt-erstellt
- dynamodb-meets-restore-time-Ziel
- dynamodb-pitr-enabled
- dynamodb-resources-protected-by-Backup-Plan
- dynamodb-table-deletion-protection-aktiviert
- dynamodb-table-encrypted-kms
- dynamodb-throughput-limit-check
- ebs-in-backup-plan
- ebs-last-backup-recovery-punkt-erstellt
- ebs-meets-restore-time-Ziel
- ebs-optimized-instance
- ebs-resources-in-logically-air-gapped-vault
- ebs-resources-protected-by-Backup-Plan
- ec2- capacity-reservation-tagged
- ec2- dhcp-options-tagged
- ec2- ebs-encryption-by-default

- ec2-Fleet-markiert
- ec2-imdsv2-check
- ec2- instance-detailed-monitoring-enabled
- ec2-ami instance-launched-with-allowed
- ec2- instance-managed-by-ssm
- ec2- instance-multiple-eni-check
- ec2- instance-no-public-ip
- ec2- instance-profile-attached
- ec2- erstellt last-backup-recovery-point
- ec2- managedinstance-applications-blacklisted
- ec2- managedinstance-applications-required
- ec2- managedinstance-inventory-blacklisted
- ec2- prüfen managedinstance-patch-compliance-status
- ec2- managedinstance-platform-check
- ec2- meets-restore-time-target
- ec2- prefix-list-tagged
- ec2- -Tresor mit Lücken resources-in-logically-air
- ec2- resources-protected-by-backup -plan
- ec2-eni security-group-attached-to
- ec2-stopped-instance
- ec2- traffic-mirror-filter-description
- ec2- traffic-mirror-filter-tagged
- ec2- -attach-deaktiviert transit-gateway-auto-vpc
- ec2 transit-gateway-multicast-domain - markiert
- ec2- volume-inuse-check
- ec2- vpn-connection-logging-enabled
- ecr-private-image-scanning-aktiviert
- ecr-private-lifecycle-policy-konfiguriert
- ecr-private-tag-immutability-aktiviert
- ecr-repository-cmk-encryption-aktiviert

- ecr-repository-tagged
- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-container-insights-enabled
- ecs-fargate-latest-platform-Version
- ecs-no-environment-secrets
- ecs-task-definition-log-Konfiguration
- ecs-task-definition-network-mode-not-host
- ecs-task-definition-pid-Modus-Überprüfung
- ecs-task-definition-user-for-host-mode-check
- efs-access-point-enforce-Stammverzeichnis
- efs-access-point-enforce-Benutzeridentität
- efs-automatic-backups-enabled
- efs-encrypted-check
- efs-filesystem-ct-encrypted
- efs-in-backup-plan
- efs-last-backup-recovery-Punkt erstellt
- efs-meets-restore-time-Ziel
- efs-mount-target-public-zugänglich
- efs-resources-in-logically-air-gapped-vault
- efs-resources-protected-by-Backup-Plan
- eip-attached
- eks-cluster-log-enabled
- eks-cluster-secrets-encrypted
- eks-cluster-supported-version
- eks-endpoint-no-public-Zugang
- eks-secrets-encrypted
- elasticache-auto-minor-version-Upgrade-Check
- elasticache-redis-cluster-automatic-Backup-Check
- elasticache-repl-grp-auto-failover-fähig

- elasticache-repl-grp-encrypted-im Ruhezustand
- elasticache-repl-grp-encryptedunterwegs
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch
- elasticsearch-node-to-node-Verschlüsselungsprüfung
- elbv2-multiple-az
- elb-cross-zone-load-Balancing aktiviert
- elb-custom-security-policy-ssl-Prüfung
- elb-deletion-protection-enabled
- elb-logging-enabled
- elb-predefined-security-policy-ssl-Überprüfung
- elb-tls-https-listeners-nur
- emr-block-public-access
- emr-kerberos-enabled
- emr-master-no-public-ip
- emr-security-configuration-encryption-ruh dich aus
- emr-security-configuration-encryption-Transit
- encrypted-volumes
- event-data-store-cmk-Verschlüsselung aktiviert
- fis-experiment-template-log-Konfiguration ist vorhanden
- fis-experiment-template-tagged
- fms-shield-resource-policy-überprüfen
- fms-webacl-resource-policy-überprüfen
- fms-webacl-rulegroup-association-überprüfen
- fsx-last-backup-recovery-Punkt erstellt
- fsx-lustre-copy-tagszu Backups
- fsx-meets-restore-time-Ziel
- fsx-ontap-deployment-type-überprüfen
- fsx-openzfs-copy-tags-aktiviert

- fsx-openzfs-deployment-type-überprüfen
- fsx-resources-protected-by-Ersatzplan
- fsx-windows-audit-log-konfiguriert
- fsx-windows-deployment-type-überprüfen
- glue-job-logging-enabled
- glue-ml-transform-encrypted-im Ruhezustand
- glue-spark-job-supported-Ausführung
- GuardDuty-EC2- protection-runtime-enabled
- guardduty-ecs-protection-runtime-aktiviert
- guardduty-eks-protection-audit-aktiviert
- guardduty-eks-protection-runtime-aktiviert
- guardduty-enabled-centralized
- guardduty-lambda-protection-enabled
- guardduty-malware-protection-enabled
- guardduty-non-archived-findings
- guardduty-rds-protection-enabled
- guardduty-runtime-monitoring-enabled
- GuardDuty-S3-Schutz aktiviert
- iam-external-access-analyzer-aktiviert
- iam-password-policy
- incoming-ssh-disabled
- instances-in-vpc
- internet-gateway-authorized-vpc-nur
- kinesis-firehose-delivery-stream-verschlüsselt
- kinesis-stream-backup-retention-überprüfen
- kinesis-stream-encrypted
- kms-cmk-not-scheduled-zum Löschen
- kms-key-policy-no-öffentlicher Zugang
- lambda-concurrency-check
- lambda-dlq-check

- lambda-function-settings-check
- lambda-inside-vpc
- lambda-vpc-multi-az-überprüfen
- mariadb-publish-logs-to-cloudwatch-Protokolle
- msk-enhanced-monitoring-enabled
- msk-in-cluster-node-benötigt-tls
- multi-region-cloud-trail-aktiviert
- nacl-no-unrestricted-ssh-rdp
- netfw-deletion-protection-enabled
- netfw-logging-enabled
- netfw-multi-az-enabled
- netfw-policy-default-action-fragment-Pakete
- netfw-policy-default-action-vollständige Pakete
- netfw-policy-rule-group-assoziiert
- netfw-stateless-rule-group-nicht leer
- netfw-subnet-change-protection-aktiviert
- nlb-internal-scheme-check
- nlb-logging-enabled
- no-unrestricted-route-to-igw
- rds-aurora-mysql-audit-Protokollierung aktiviert
- rds-automatic-minor-version-upgrade-fähig
- rds-cluster-default-admin-überprüfen
- rds-cluster-deletion-protection-aktiviert
- rds-cluster-encrypted-at-ausruhen
- rds-cluster-iam-authentication-aktiviert
- rds-cluster-multi-az-aktiviert
- rds-enhanced-monitoring-enabled
- rds-instance-default-admin-überprüfen
- rds-instance-deletion-protection-aktiviert
- rds-instance-iam-authentication-aktiviert

- rds-instance-public-access-überprüfen
- rds-instance-subnet-igw-überprüfen
- rds-in-backup-plan
- rds-last-backup-recovery-Punkt erstellt
- rds-logging-enabled
- rds-mariadb-instance-encryptedwährend des Transports
- rds-meets-restore-time-Ziel
- rds-multi-az-support
- rds-mysql-instance-encryptedunterwegs
- rds-postgresql-logs-to- Cloudwatch
- rds-postgres-instance-encryptedunterwegs
- rds-proxy-tls-encryption
- rds-resources-protected-by-Backup-Plan
- rds-snapshot-encrypted
- rds-sqlserver-encrypted-in-Transit
- rds-sql-server-logszur Cloud-Überwachung
- rds-storage-encrypted
- redshift-backup-enabled
- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check
- redshift-cluster-parameter-group-markiert
- redshift-cluster-public-access-überprüfen
- redshift-cluster-subnet-group-Multi-Az
- redshift-default-admin-check
- redshift-default-db-name-überprüfen
- redshift-enhanced-vpc-routing-aktiviert
- redshift-require-tls-ssl
- redshift-serverless-default-admin-überprüfen
- redshift-serverless-default-db-Namenscheck
- redshift-serverless-namespace-cmk-Verschlüsselung

- redshift-serverless-publish-logs-zu-Cloud-Watch
- redshift-serverless-workgroup-encryptedauf dem Weg
- redshift-serverless-workgroup-no-öffentlich zugänglich
- redshift-serverless-workgroup-routes-innerhalb von VPC
- redshift-unrestricted-port-access
- required-tags
- restricted-incoming-traffic
- root-account-hardware-mfa-aktiviert
- root-account-mfa-enabled
- nur s3- access-point-in-vpc
- s3- -Blöcke access-point-public-access
- s3- -Blöcke account-level-public-access
- s3- -Blocke-periodisch account-level-public-access
- s 3- bucket-acl-prohibited
- s3- bucket-cross-region-replication -aktiviert
- s-3 bucket-default-lock-enabled
- s3 bucket-level-public-access - verboten
- s3- bucket-logging-enabled
- s-3 bucket-mfa-delete-enabled
- s-3 bucket-policy-grantee-check
- s3- bucket-policy-not-more -freizügig
- s 3- bucket-public-read-prohibited
- s-3 bucket-public-write-prohibited
- s-3 bucket-replication-enabled
- s-3 bucket-ssl-requests-only
- s3-Bucket-Tagged
- s-3 bucket-versioning-enabled
- s-3 default-encryption-kms
- s-3 event-notifications-enabled
- s3 last-backup-recovery-point - erstellt

- s3- lifecycle-policy-check
- s-3 meets-restore-time-target
- resources-protected-by-backups3-plan
- s 3- version-lifecycle-policy-check
- sagemaker-app-image-config-markiert
- sagemaker-endpoint-configuration-kms-schlüsselkonfiguriert
- sagemaker-endpoint-config-prod-Anzahl der Instanzen
- sagemaker-feature-group-tagged
- sagemaker-image-description
- sagemaker-image-tagged
- sagemaker-notebook-instance-kms-key-konfiguriert
- sagemaker-notebook-instance-platform-Version
- sagemaker-notebook-no-direct-Internetzugang
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-überprüfen
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- securityhub-enabled
- security-account-information-provided
- service-catalog-shared-within-Organisation
- service-vpc-endpoint-enabled
- sns-encrypted-kms
- sns-topic-no-public-Zugang
- ssm-document-not-public
- ssm-document-tagged
- step-functions-state-machine-Protokollierung aktiviert
- storagegateway-last-backup-recovery-punkt-erstellt
- storagegateway-resources-in-logically-air-gapped-vault
- storagegateway-resources-protected-by-Ersatzplan

- subnet-auto-assign-public-ip-deaktiviert
- transfer-certificate-description
- transfer-certificate-tagged
- transfer-connector-tagged
- transfer-family-server-no-ftp
- transfer-profile-tagged
- transfer-workflow-description
- transfer-workflow-tagged
- vpc-default-security-group-geschlossen
- vpc-endpoint-enabled
- vpc-flow-logs-enabled
- vpc-network-acl-unused-überprüfen
- vpc-sg-open-only-to-authorized-ports
- vpc-sg-port-restriction-überprüfen
- vpc-vpn-2-tunnels-up
- wafv2-logging-enabled
- WAF 2- rulegroup-logging-enabled
- waf-regional-rule-not-leer
- waf-regional-webacl-not-leer

Region Europa (Stockholm)

Europa (Stockholm)

- access-keys-rotated
- account-part-of-organizations
- acmpca-certificate-authority-tagged
- acm-certificate-expiration-check
- acm-certificate-rsa-check
- acm-pca-root-ca-deaktiviert
- active-mq-supported-version
- alb-desync-mode-check

- alb-http-drop-invalid-Header-fähig
- alb-http-to-https-Umleitungsprüfung
- alb-internal-scheme-check
- alb-listener-tagged
- alb-waf-enabled
- amplify-app-branch-auto-löschung aktiviert
- amplify-app-description
- amplify-app-tagged
- amplify-branch-performance-mode-aktiviert
- amplify-branch-tagged
- api-gwv2- access-logs-enabled
- api-gwv2- authorization-type-configured
- api-gw-associated-with-WAF
- api-gw-cache-enabled-und-verschlüsselt
- api-gw-endpoint-type-überprüfen
- api-gw-execution-logging-aktiviert
- api-gw-ssl-enabled
- api-gw-xray-enabled
- appconfig-application-description
- appconfig-application-tagged
- appconfig-configuration-profile-tagged
- appconfig-configuration-profile-validators-nicht leer
- appconfig-deployment-strategy-description
- appconfig-deployment-strategy-replicate-zu-ssm
- appconfig-environment-description
- appconfig-environment-tagged
- appconfig-extension-association-tagged
- appconfig-freeform-profile-config-Speicher
- appconfig-hosted-configuration-version-Beschreibung
- appmesh-gateway-route-tagged

- appmesh-mesh-deny-tcp-Weiterleitung
- appmesh-mesh-tagged
- appmesh-route-tagged
- appmesh-virtual-gateway-backend-Standardeinstellungen-TLS
- appmesh-virtual-gateway-logging-file-path-exists
- appmesh-virtual-gateway-tagged
- appmesh-virtual-node-backend-defaults-tls-on
- appmesh-virtual-node-logging-file-path-exists
- appmesh-virtual-node-tagged
- appmesh-virtual-router-tagged
- appmesh-virtual-service-tagged
- approved-amis-by-id
- approved-amis-by-tag
- appsync-associated-with-waf
- appsync-authorization-check
- appsync-cache-encryption-at-ausruhen
- appsync-logging-enabled
- athena-data-catalog-description
- athena-prepared-statement-description
- athena-workgroup-description
- athena-workgroup-encrypted-at-ausruhen
- athena-workgroup-enforce-workgroup-Konfiguration
- athena-workgroup-engine-version-automatisches Upgrade
- athena-workgroup-logging-enabled
- aurora-last-backup-recovery-Punkt erstellt
- aurora-meets-restore-time-Ziel
- aurora-mysql-cluster-audit-Protokollierung
- aurora-resources-in-logically-air-gapped-vault
- aurora-resources-protected-by-Backup-Plan
- autoscaling-capacity-rebalancing

- autoscaling-group-elb-healthcheck-erforderlich
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-hop-Grenze
- autoscaling-launch-config-public-ip-deaktiviert
- autoscaling-launch-template
- autoscaling-multiple-az
- autoscaling-multiple-instance-types
- backup-plan-min-frequency-and-min-retention-check
- backup-recovery-point-encrypted
- backup-recovery-point-manual-Löschen-deaktiviert
- backup-recovery-point-minimum-Aufbewahrungsprüfung
- batch-compute-environment-enabled
- batch-compute-environment-managed
- batch-compute-environment-tagged
- batch-job-queue-enabled
- batch-job-queue-tagged
- batch-managed-compute-environment-using-launch-template
- batch-managed-compute-env-compute-resources-tagged
- batch-scheduling-policy-tagged
- beanstalk-enhanced-health-reporting-aktiviert
- cassandra-keyspace-tagged
- clb-desync-mode-check
- clb-multiple-az
- cloudformation-stack-drift-detection-überprüfen
- cloudformation-stack-notification-check
- cloudtrail-all-read-s3- data-event-check
- cloudtrail-all-write-s3- data-event-check
- Wolkenspur-S3- bucket-access-logging
- CloudTrail-S3- bucket-public-access-prohibited
- cloudtrail-s3-dataevents-enabled

- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-action-enabled-überprüfen
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted
- cloud-trail-cloud-watch-logs-aktiviert
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-Validierung aktiviert
- cmk-backing-key-rotation-aktiviert
- codebuild-project-artifact-encryption
- codebuild-project-environment-privileged-überprüfen
- codebuild-project-envvar-awscred-überprüfen
- codebuild-project-logging-enabled
- codebuild-project-s3-log-verschlüsselt
- codebuild-project-source-repo-URL-Prüfung
- codebuild-report-group-encrypted-im Ruhezustand
- codedeploy-auto-rollback-monitor-aktiviert
- codedeploy-deployment-group-auto-rollback-aktiviert
- codedeploy-deployment-group-outdated-instanzen-aktualisieren
- Codedeploy-ec2- minimum-healthy-hosts-configured
- codedeploy-lambda-allatonce-traffic-shift-deaktiviert
- codeguruprofiler-profiling-group-tagged
- codegururevieweer-repository-association-tagged
- codepipeline-deployment-count-check
- cognito-identity-pool-unauth-Zugriffsprüfung
- cognito-user-pool-advanced-sicherheitsaktiviert
- cognito-user-pool-tagged
- custom-eventbus-policy-attached

- custom-schema-registry-policy-angehängt
- cw-loggroup-retention-period-überprüfen
- datasync-task-data-verification-aktiviert
- datasync-task-logging-enabled
- datasync-task-tagged
- dax-encryption-enabled
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- dms-auto-minor-version-aktualisieren-Prüfung
- dms-endpoint-ssl-configured
- dms-endpoint-tagged
- dms-mongo-db-authentication-aktiviert
- dms-neptune-iam-authorization-aktiviert
- dms-redis-tls-enabled
- dms-replication-not-public
- dms-replication-task-sourcedb-Protokollierung
- dms-replication-task-tagged
- dms-replication-task-targetdb-Protokollierung
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-last-backup-recovery-Punkt erstellt
- dynamodb-meets-restore-time-Ziel
- dynamodb-pitr-enabled
- dynamodb-resources-protected-by-Backup-Plan
- dynamodb-table-deletion-protection-aktiviert
- dynamodb-table-encrypted-kms
- dynamodb-throughput-limit-check
- ebs-in-backup-plan
- ebs-last-backup-recovery-punkt-erstellt

- ebs-meets-restore-time-Ziel
- ebs-optimized-instance
- ebs-resources-in-logically-air-gapped-vault
- ebs-resources-protected-by-Backup-Plan
- ebs-snapshot-public-restorable-überprüfen
- ec2- capacity-reservation-tagged
- ec2- aktiviert client-vpn-connection-log
- ec2- client-vpn-endpoint-tagged
- ec2- -alle client-vpn-not-authorize
- ec2- dhcp-options-tagged
- ec2- ebs-encryption-by-default
- ec2- aktiviert enis-source-destination-check
- ec2-fleet-markiert
- ec2-imdsv2-check
- ec2- instance-detailed-monitoring-enabled
- ec2-ami instance-launched-with-allowed
- ec2- instance-managed-by-ssm
- ec2- instance-multiple-eni-check
- ec2- instance-no-public-ip
- ec2- instance-profile-attached
- ec2- erstellt last-backup-recovery-point
- ec2-2-prüfen launch-template-imdsv
- ec2- -deaktiviert launch-template-public-ip
- ec2- launch-template-tagged
- ec2- managedinstance-applications-blacklisted
- ec2- managedinstance-applications-required
- ec2- prüfen managedinstance-association-compliance-status
- ec2- managedinstance-inventory-blacklisted
- ec2- prüfen managedinstance-patch-compliance-status
- ec2- managedinstance-platform-check

- ec2- meets-restore-time-target
- ec2- Analyse mit Schlagwörtern network-insights-access-scope
- ec2 network-insights-access-scope - markiert
- ec2- network-insights-path-tagged
- ec2- no-amazon-key-pair
- ec2- prefix-list-tagged
- ec2- -Tresor mit Lücken resources-in-logically-air
- ec2- resources-protected-by-backup -plan
- ec2-eni security-group-attached-to
- ec2- -eni-periodisch security-group-attached-to
- ec2-stopped-instance
- ec2- token-hop-limit-check
- ec2- traffic-mirror-filter-description
- ec2- traffic-mirror-filter-tagged
- ec2- traffic-mirror-session-description
- ec2- traffic-mirror-session-tagged
- ec2- traffic-mirror-target-description
- ec2- traffic-mirror-target-tagged
- ec2- -attach-deaktiviert transit-gateway-auto-vpc
- ec2 transit-gateway-multicast-domain - markiert
- ec2- volume-inuse-check
- ec2- vpn-connection-logging-enabled
- ecr-private-image-scanning-aktiviert
- ecr-private-lifecycle-policy-konfiguriert
- ecr-private-tag-immutability-aktiviert
- ecr-repository-cmk-encryption-aktiviert
- ecr-repository-tagged
- ecs-awsvpc-networking-enabled
- ecs-containers-nonprivileged
- ecs-containers-readonly-access

- ecs-container-insights-enabled
- ecs-fargate-latest-platform-Version
- ecs-no-environment-secrets
- ecs-task-definition-log-Konfiguration
- ecs-task-definition-memory-hartes Limit
- ecs-task-definition-network-mode-not-host
- ecs-task-definition-nonroot-Benutzer
- ecs-task-definition-pid-Modus-Check
- ecs-task-definition-user-for-host-mode-check
- efs-access-point-enforce-Stammverzeichnis
- efs-access-point-enforce-Benutzeridentität
- efs-automatic-backups-enabled
- efs-encrypted-check
- efs-filesystem-ct-encrypted
- efs-in-backup-plan
- efs-last-backup-recovery-Punkt erstellt
- efs-meets-restore-time-Ziel
- efs-mount-target-public-zugänglich
- efs-resources-in-logically-air-gapped-vault
- efs-resources-protected-by-Backup-Plan
- eip-attached
- eks-cluster-logging-enabled
- eks-cluster-log-enabled
- eks-cluster-oldest-supported-Ausführung
- eks-cluster-secrets-encrypted
- eks-cluster-supported-version
- eks-endpoint-no-public-Zugang
- eks-secrets-encrypted
- elasticache-auto-minor-version-Upgrade-Check
- elasticache-rbac-auth-enabled

- elasticache-redis-cluster-automatic-Backup-Check
- elasticache-repl-grp-auto-failover-fähig
- elasticache-repl-grp-encrypted-im Ruhezustand
- elasticache-repl-grp-encryptedim Transit
- elasticache-repl-grp-redis-auth-aktiviert
- elasticache-subnet-group-check
- elasticache-supported-engine-version
- elasticbeanstalk-application-description
- elasticbeanstalk-application-version-description
- elasticbeanstalk-environment-description
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch
- elasticsearch-node-to-node-Verschlüsselungsprüfung
- elastic-beanstalk-logs-to- Cloudwatch
- elastic-beanstalk-managed-updates-aktiviert
- elbv2- acm-certificate-required
- elv 2- listener-encryption-in-transit
- elbv2-multiple-az
- elbv2- prüfen predefined-security-policy-ssl
- elb-acm-certificate-required
- elb-cross-zone-load-Balancing aktiviert
- elb-custom-security-policy-ssl-Prüfung
- elb-deletion-protection-enabled
- elb-logging-enabled
- elb-predefined-security-policy-ssl-Überprüfung
- elb-tls-https-listeners-nur
- emr-block-public-access
- emr-kerberos-enabled
- emr-master-no-public-ip

- emr-security-configuration-encryption-ruh dich aus
- emr-security-configuration-encryption-Transit
- encrypted-volumes
- event-data-store-cmk-Verschlüsselung aktiviert
- evidently-launch-description
- evidently-launch-tagged
- evidently-project-description
- evidently-project-tagged
- evidently-segment-description
- evidently-segment-tagged
- fis-experiment-template-log-Konfiguration ist vorhanden
- fis-experiment-template-tagged
- fms-shield-resource-policy-überprüfen
- fms-webacl-resource-policy-überprüfen
- fms-webacl-rulegroup-association-überprüfen
- fsx-last-backup-recovery-Punkt erstellt
- fsx-lustre-copy-tagszu Backups
- fsx-meets-restore-time-Ziel
- fsx-ontap-deployment-type-überprüfen
- fsx-openzfs-copy-tags-aktiviert
- fsx-openzfs-deployment-type-überprüfen
- fsx-resources-protected-by-Ersatzplan
- fsx-windows-audit-log-konfiguriert
- fsx-windows-deployment-type-überprüfen
- glb-listener-tagged
- global-endpoint-event-replication-aktiviert
- glue-job-logging-enabled
- glue-ml-transform-encrypted-im Ruhezustand
- glue-spark-job-supported-Ausführung
- GuardDuty-EC2- protection-runtime-enabled

- guardduty-ecs-protection-runtime-aktiviert
- guardduty-eks-protection-audit-aktiviert
- guardduty-eks-protection-runtime-aktiviert
- guardduty-enabled-centralized
- guardduty-lambda-protection-enabled
- guardduty-malware-protection-enabled
- guardduty-non-archived-findings
- guardduty-rds-protection-enabled
- guardduty-runtime-monitoring-enabled
- GuardDuty-S3-Schutz aktiviert
- iam-customer-policy-blocked-kms-Aktionen
- iam-external-access-analyzer-aktiviert
- iam-group-has-users-überprüfen
- iam-inline-policy-blocked-kms-Aktionen
- iam-no-inline-policy-überprüfen
- iam-password-policy
- iam-policy-blacklisted-check
- iam-policy-in-use
- iam-policy-no-statements-with-admin-access
- iam-policy-no-statements-with-full-access
- iam-role-managed-policy-überprüfen
- iam-root-access-key-überprüfen
- iam-user-group-membership-überprüfen
- iam-user-mfa-enabled
- iam-user-no-policies-überprüfen
- iam-user-unused-credentials-überprüfen
- incoming-ssh-disabled
- inspector-ec2-Scan aktiviert
- inspector-ecr-scan-enabled
- inspector-lambda-code-scan-aktiviert

- inspector-lambda-standard-scan-aktiviert
- instances-in-vpc
- internet-gateway-authorized-vpc-nur
- iot-authorizer-token-signing-aktiviert
- kinesis-firehose-delivery-stream-verschlüsselt
- kinesis-stream-backup-retention-überprüfen
- kinesis-stream-encrypted
- kms-cmk-not-scheduled-zum Löschen
- kms-key-policy-no-öffentlicher Zugang
- lambda-concurrency-check
- lambda-dlq-check
- lambda-function-public-access-verboten
- lambda-function-settings-check
- lambda-function-xray-enabled
- lambda-inside-vpc
- lambda-vpc-multi-az-überprüfen
- lightsail-bucket-tagged
- lightsail-certificate-tagged
- lightsail-disk-tagged
- macie-auto-sensitive-data-Discovery-Check
- macie-status-check
- mariadb-publish-logs-to-Cloudwatch-Protokolle
- mfa-enabled-for-iam-Konsolenzugriff
- mq-active-broker-ldap-Authentifizierung
- mq-active-deployment-mode
- mq-active-single-instance-broker-storage-type-efs
- mq-automatic-minor-version-Upgrade aktiviert
- mq-auto-minor-version-upgrade-fähig
- mq-broker-general-logging-aktiviert
- mq-cloudwatch-audit-logging-aktiviert

- mq-cloudwatch-audit-log-aktiviert
- mq-no-public-access
- mq-rabbit-deployment-mode
- msk-cluster-public-access-deaktiviert
- msk-connect-connector-logging-aktiviert
- msk-enhanced-monitoring-enabled
- msk-in-cluster-node-require-tls
- msk-unrestricted-access-check
- multi-region-cloud-trail-aktiviert
- nacl-no-unrestricted-ssh-rdp
- neptune-cluster-backup-retention-überprüfen
- neptune-cluster-cloudwatch-log-exportfähig
- neptune-cluster-copy-tags-to-snapshot-enabled
- neptune-cluster-deletion-protection-aktiviert
- neptune-cluster-encrypted
- neptune-cluster-iam-database-Authentifizierung
- neptune-cluster-multi-az-aktiviert
- neptune-cluster-snapshot-encrypted
- neptune-cluster-snapshot-public-verboten
- netfw-deletion-protection-enabled
- netfw-logging-enabled
- netfw-multi-az-enabled
- netfw-policy-default-action-fragment-Pakete
- netfw-policy-default-action-vollständige Pakete
- netfw-policy-rule-group-assoziiert
- netfw-stateless-rule-group-nicht leer
- netfw-subnet-change-protection-aktiviert
- nlb-cross-zone-load-Balancing aktiviert
- nlb-internal-scheme-check
- nlb-listener-tagged

- nlb-logging-enabled
- no-unrestricted-route-to-igw
- opensearch-access-control-enabled
- opensearch-audit-logging-enabled
- opensearch-data-node-fault-Toleranz
- opensearch-encrypted-at-rest
- opensearch-https-required
- opensearch-in-vpc-only
- opensearch-logs-to-cloudwatch
- opensearch-node-to-node-Verschlüsselungsprüfung
- opensearch-primary-node-fault-Toleranz
- opensearch-update-check
- rabbit-mq-supported-version
- rds-aurora-mysql-audit-Protokollierung aktiviert
- rds-aurora-postgresql-logs-zu-Cloud-Watch
- rds-automatic-minor-version-upgrade-fähig
- rds-cluster-auto-minor-version-upgrade-enable
- rds-cluster-default-admin-überprüfen
- rds-cluster-deletion-protection-aktiviert
- rds-cluster-encrypted-at-ausruhen
- rds-cluster-iam-authentication-aktiviert
- rds-cluster-multi-az-aktiviert
- rds-enhanced-monitoring-enabled
- rds-instance-default-admin-überprüfen
- rds-instance-deletion-protection-aktiviert
- rds-instance-iam-authentication-aktiviert
- rds-instance-public-access-überprüfen
- rds-instance-subnet-igw-überprüfen
- rds-in-backup-plan
- rds-last-backup-recovery-Punkt erstellt

- rds-logging-enabled
- rds-mariadb-instance-encryptedim Transit
- rds-meets-restore-time-Ziel
- rds-multi-az-support
- rds-mysql-instance-encryptedunterwegs
- rds-postgresql-logs-to- Cloudwatch
- rds-postgres-instance-encryptedunterwegs
- rds-proxy-tls-encryption
- rds-resources-protected-by-Backup-Plan
- rds-snapshots-public-prohibited
- rds-snapshot-encrypted
- rds-sqlserver-encrypted-in-Transit
- rds-sql-server-logszur Cloud-Überwachung
- rds-storage-encrypted
- redshift-audit-logging-enabled
- redshift-backup-enabled
- redshift-cluster-configuration-check
- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check
- redshift-cluster-multi-az-aktiviert
- redshift-cluster-parameter-group-markiert
- redshift-cluster-public-access-überprüfen
- redshift-cluster-subnet-group-Multi-Az
- redshift-default-admin-check
- redshift-default-db-name-überprüfen
- redshift-enhanced-vpc-routing-aktiviert
- redshift-require-tls-ssl
- redshift-serverless-default-admin-überprüfen
- redshift-serverless-default-db-Namenscheck
- redshift-serverless-namespace-cmk-Verschlüsselung

- redshift-serverless-publish-logs-zu-Cloud-Watch
- redshift-serverless-workgroup-encryptedauf dem Weg
- redshift-serverless-workgroup-no-öffentlich zugänglich
- redshift-serverless-workgroup-routes-innerhalb von VPC
- redshift-unrestricted-port-access
- required-tags
- restricted-incoming-traffic
- root-account-hardware-mfa-aktiviert
- root-account-mfa-enabled
- s3 -regel-check express-dir-bucket-lifecycle
- nur s3- access-point-in-vpc
- s3- -Blöcke access-point-public-access
- s3- -Blöcke account-level-public-access
- s3- -Blocke-periodisch account-level-public-access
- s 3- bucket-acl-prohibited
- s-3 bucket-blacklisted-actions-prohibited
- s3- bucket-cross-region-replication -aktiviert
- s-3 bucket-default-lock-enabled
- s3 bucket-level-public-access - verboten
- s3- bucket-logging-enabled
- s-3 bucket-mfa-delete-enabled
- s-3 bucket-policy-grantee-check
- s3- bucket-policy-not-more -freizügig
- s 3- bucket-public-read-prohibited
- s-3 bucket-public-write-prohibited
- s-3 bucket-replication-enabled
- s3- bucket-server-side-encryption -aktiviert
- s-3 bucket-ssl-requests-only
- s3-Bucket-Tagged
- s-3 bucket-versioning-enabled

- s-3 default-encryption-kms
- s-3 event-notifications-enabled
- s3 last-backup-recovery-point - erstellt
- s3- lifecycle-policy-check
- s-3 meets-restore-time-target
- s3- resources-in-logically-air -Tresor mit Lücken
- s3 resources-protected-by-backup - -Plan
- s 3- version-lifecycle-policy-check
- sagemaker-app-image-config-markiert
- sagemaker-domain-in-vpc
- sagemaker-domain-tagged
- sagemaker-endpoint-configuration-kms-schlüsselkonfiguriert
- sagemaker-endpoint-config-prod-Anzahl der Instanzen
- sagemaker-feature-group-tagged
- sagemaker-image-description
- sagemaker-image-tagged
- sagemaker-model-in-vpc
- sagemaker-model-isolation-enabled
- sagemaker-notebook-instance-inside-vpc
- sagemaker-notebook-instance-kms-key-konfiguriert
- sagemaker-notebook-instance-platform-Version
- sagemaker-notebook-instance-root-Zugriffsprüfung
- sagemaker-notebook-no-direct-Internetzugang
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-überprüfen
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- securityhub-enabled
- security-account-information-provided

- service-catalog-shared-within-Organisation
- service-vpc-endpoint-enabled
- sns-encrypted-kms
- sns-topic-message-delivery-Benachrichtigung aktiviert
- sns-topic-no-public-Zugriff
- sqs-queue-no-public-Zugang
- ssm-automation-block-public-teilen
- ssm-automation-logging-enabled
- ssm-document-not-public
- ssm-document-tagged
- step-functions-state-machine-Protokollierung aktiviert
- storagegateway-last-backup-recovery-punkt-erstellt
- storagegateway-resources-in-logically-air-gapped-vault
- storagegateway-resources-protected-by-Ersatzplan
- subnet-auto-assign-public-ip-deaktiviert
- transfer-agreement-description
- transfer-agreement-tagged
- transfer-certificate-description
- transfer-certificate-tagged
- transfer-connector-logging-enabled
- transfer-connector-tagged
- transfer-family-server-no-ftp
- transfer-profile-tagged
- transfer-workflow-description
- transfer-workflow-tagged
- virtualmachine-last-backup-recovery-Punkt erstellt
- virtualmachine-resources-in-logically-air-gapped-vault
- virtualmachine-resources-protected-by-Ersatzplan
- vpc-default-security-group-geschlossen
- vpc-endpoint-enabled

- vpc-flow-logs-enabled
- vpc-network-acl-unused-überprüfen
- vpc-peering-dns-resolution-überprüfen
- vpc-sg-open-only-to-authorized-ports
- vpc-sg-port-restriction-überprüfen
- vpc-vpn-2-tunnels-up
- wafv2-logging-enabled
- WAF 2- rulegroup-logging-enabled
- WAF 2- rulegroup-not-empty
- WAF 2- webacl-not-empty
- waf-regional-rulegroup-not-leer
- waf-regional-rule-not-leer
- waf-regional-webacl-not-leer

Region Europa (Zürich)

Europa (Zürich)

- account-part-of-organizations
- acmpca-certificate-authority-tagged
- acm-certificate-expiration-check
- acm-certificate-rsa-check
- acm-pca-root-ca-deaktiviert
- alb-desync-mode-check
- alb-http-drop-invalid-Header-fähig
- alb-http-to-https-Umleitungsprüfung
- alb-internal-scheme-check
- alb-waf-enabled
- api-gw-associated-with-WAF
- api-gw-cache-enabled-und-verschlüsselt
- api-gw-endpoint-type-überprüfen
- api-gw-execution-logging-aktiviert

- api-gw-ssl-enabled
- api-gw-xray-enabled
- appconfig-deployment-strategy-description
- appconfig-deployment-strategy-replicate-zu-ssm
- appconfig-extension-association-tagged
- approved-amis-by-id
- approved-amis-by-tag
- appsync-authorization-check
- appsync-logging-enabled
- athena-data-catalog-description
- athena-prepared-statement-description
- athena-workgroup-description
- athena-workgroup-enforce-workgroup-Konfiguration
- athena-workgroup-engine-version-automatisches Upgrade
- athena-workgroup-logging-enabled
- aurora-last-backup-recovery-Punkt erstellt
- aurora-meets-restore-time-Ziel
- aurora-mysql-backtracking-enabled
- aurora-mysql-cluster-audit-Protokollierung
- aurora-resources-in-logically-air-gapped-vault
- aurora-resources-protected-by-Backup-Plan
- autoscaling-group-elb-healthcheck-erforderlich
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-hop-Grenze
- autoscaling-launch-config-public-ip-deaktiviert
- autoscaling-launch-template
- autoscaling-multiple-az
- autoscaling-multiple-instance-types
- backup-plan-min-frequency-and-min-retention-check
- backup-recovery-point-encrypted

- backup-recovery-point-manual-Löschen-deaktiviert
- backup-recovery-point-minimum-Aufbewahrungsprüfung
- batch-compute-environment-enabled
- batch-compute-environment-managed
- batch-compute-environment-tagged
- batch-job-queue-enabled
- batch-job-queue-tagged
- batch-managed-compute-environment-using-launch-template
- batch-managed-compute-env-compute-resources-tagged
- batch-scheduling-policy-tagged
- clb-multiple-az
- cloudtrail-all-read-s3- data-event-check
- cloudtrail-all-write-s3- data-event-check
- Wolkenspur-S3- bucket-access-logging
- CloudTrail-S3- bucket-public-access-prohibited
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-action-enabled-überprüfen
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted
- cloud-trail-cloud-watch-logs-aktiviert
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-Validierung aktiviert
- cmk-backing-key-rotation-aktiviert
- codebuild-project-envvar-awscred-überprüfen
- codebuild-project-logging-enabled
- codebuild-project-s3-log-verschlüsselt

- codebuild-project-source-repo-URL-Prüfung
- codebuild-report-group-encrypted-im Ruhezustand
- cognito-user-pool-tagged
- custom-eventbus-policy-attached
- cw-loggroup-retention-period-überprüfen
- datasync-task-data-verification-aktiviert
- datasync-task-logging-enabled
- datasync-task-tagged
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- dms-replication-not-public
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-last-backup-recovery-punkt-erstellt
- dynamodb-meets-restore-time-Ziel
- dynamodb-pitr-enabled
- dynamodb-resources-protected-by-Backup-Plan
- dynamodb-table-deletion-protection-aktiviert
- dynamodb-table-encrypted-kms
- dynamodb-table-encryption-enabled
- dynamodb-throughput-limit-check
- ebs-in-backup-plan
- ebs-last-backup-recovery-punkt-erstellt
- ebs-meets-restore-time-Ziel
- ebs-optimized-instance
- ebs-resources-in-logically-air-gapped-vault
- ebs-resources-protected-by-Backup-Plan
- ebs-snapshot-public-restorable-überprüfen
- ec2- capacity-reservation-tagged

- ec2- aktiviert client-vpn-connection-log
- ec2- client-vpn-endpoint-tagged
- ec2- dhcp-options-tagged
- ec2- ebs-encryption-by-default
- ec2-Fleet-markiert
- ec2-imdsv2-check
- ec2- instance-detailed-monitoring-enabled
- ec2-ami instance-launched-with-allowed
- ec2- instance-managed-by-ssm
- ec2- instance-multiple-eni-check
- ec2- instance-no-public-ip
- ec2- instance-profile-attached
- ec2- erstellt last-backup-recovery-point
- ec2- managedinstance-applications-blacklisted
- ec2- managedinstance-applications-required
- ec2- managedinstance-inventory-blacklisted
- ec2- prüfen managedinstance-patch-compliance-status
- ec2- managedinstance-platform-check
- ec2- meets-restore-time-target
- ec2- prefix-list-tagged
- ec2- -Tresor mit Lücken resources-in-logically-air
- ec2- resources-protected-by-backup -plan
- ec2-eni security-group-attached-to
- ec2- - spot-fleet-request-ct encryption-at-rest
- ec2-stopped-instance
- ec2- traffic-mirror-filter-description
- ec2- traffic-mirror-filter-tagged
- ec2- traffic-mirror-session-description
- ec2- traffic-mirror-session-tagged
- ec2- traffic-mirror-target-description

- ec2- traffic-mirror-target-tagged
- ec2- -attach-deaktiviert transit-gateway-auto-vpc
- ec2 transit-gateway-multicast-domain - markiert
- ec2- volume-inuse-check
- ec2- vpn-connection-logging-enabled
- ecr-private-image-scanning-aktiviert
- ecr-private-lifecycle-policy-konfiguriert
- ecr-private-tag-immutability-aktiviert
- ecr-repository-cmk-encryption-aktiviert
- ecr-repository-tagged
- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-container-insights-enabled
- ecs-fargate-latest-platform-Version
- ecs-no-environment-secrets
- ecs-task-definition-log-Konfiguration
- ecs-task-definition-network-mode-not-host
- ecs-task-definition-pid-Modus-Überprüfung
- ecs-task-definition-user-for-host-mode-check
- efs-access-point-enforce-Stammverzeichnis
- efs-access-point-enforce-Benutzeridentität
- efs-automatic-backups-enabled
- efs-encrypted-check
- efs-filesystem-ct-encrypted
- efs-in-backup-plan
- efs-last-backup-recovery-Punkt erstellt
- efs-meets-restore-time-Ziel
- efs-mount-target-public-zugänglich
- efs-resources-in-logically-air-gapped-vault
- efs-resources-protected-by-Backup-Plan

- eip-attached
- eks-cluster-log-enabled
- eks-cluster-secrets-encrypted
- eks-cluster-supported-version
- eks-endpoint-no-public-Zugang
- eks-secrets-encrypted
- elasticache-auto-minor-version-Upgrade-Check
- elasticache-redis-cluster-automatic-Backup-Check
- elasticache-repl-grp-auto-failover-fähig
- elasticache-repl-grp-encrypted-im Ruhezustand
- elasticache-repl-grp-encryptedim Transit
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch
- elasticsearch-node-to-node-Verschlüsselungsprüfung
- elbv2-multiple-az
- elb-cross-zone-load-Balancing aktiviert
- elb-custom-security-policy-ssl-Prüfung
- elb-deletion-protection-enabled
- elb-logging-enabled
- elb-predefined-security-policy-ssl-Überprüfung
- elb-tls-https-listeners-nur
- emr-block-public-access
- emr-kerberos-enabled
- emr-master-no-public-ip
- emr-security-configuration-encryption-ruh dich aus
- emr-security-configuration-encryption-Transit
- encrypted-volumes
- event-data-store-cmk-Verschlüsselung aktiviert
- fms-shield-resource-policy-überprüfen

- fms-webacl-resource-policy-überprüfen
- fms-webacl-rulegroup-association-überprüfen
- fsx-last-backup-recovery-Punkt erstellt
- fsx-lustre-copy-tagszu Backups
- fsx-meets-restore-time-Ziel
- fsx-ontap-deployment-type-überprüfen
- fsx-openzfs-copy-tags-aktiviert
- fsx-openzfs-deployment-type-überprüfen
- fsx-resources-protected-by-Ersatzplan
- fsx-windows-audit-log-konfiguriert
- fsx-windows-deployment-type-überprüfen
- glue-job-logging-enabled
- glue-ml-transform-encrypted-im Ruhezustand
- glue-spark-job-supported-Ausführung
- GuardDuty-EC2- protection-runtime-enabled
- guardduty-ecs-protection-runtime-aktiviert
- guardduty-eks-protection-audit-aktiviert
- guardduty-eks-protection-runtime-aktiviert
- guardduty-enabled-centralized
- guardduty-lambda-protection-enabled
- guardduty-malware-protection-enabled
- guardduty-non-archived-findings
- guardduty-rds-protection-enabled
- guardduty-runtime-monitoring-enabled
- GuardDuty-S3-Schutz aktiviert
- iam-external-access-analyzer-aktiviert
- iam-password-policy
- incoming-ssh-disabled
- inspector-ec2-Scan aktiviert
- inspector-ecr-scan-enabled

- inspector-lambda-standard-scan-aktiviert
- instances-in-vpc
- internet-gateway-authorized-vpc-nur
- kinesis-firehose-delivery-stream-verschlüsselt
- kinesis-stream-backup-retention-überprüfen
- kinesis-stream-encrypted
- kms-cmk-not-scheduled-zum Löschen
- kms-key-policy-no-öffentlicher Zugang
- lambda-concurrency-check
- lambda-dlq-check
- lambda-function-public-access-verboten
- lambda-function-settings-check
- lambda-inside-vpc
- lambda-vpc-multi-az-überprüfen
- mariadb-publish-logs-to-cloudwatch-Protokolle
- msk-enhanced-monitoring-enabled
- msk-in-cluster-node-benötigt-tls
- multi-region-cloud-trail-aktiviert
- nacl-no-unrestricted-ssh-rdp
- netfw-deletion-protection-enabled
- netfw-logging-enabled
- netfw-multi-az-enabled
- netfw-policy-default-action-fragment-Pakete
- netfw-policy-default-action-vollständige Pakete
- netfw-policy-rule-group-assoziiert
- netfw-stateless-rule-group-nicht leer
- netfw-subnet-change-protection-aktiviert
- nlb-internal-scheme-check
- nlb-logging-enabled
- no-unrestricted-route-to-igw

- rds-aurora-mysql-audit-Protokollierung aktiviert
- rds-aurora-postgresql-logs-zu-Cloud-Watch
- rds-automatic-minor-version-upgrade-fähig
- rds-cluster-default-admin-überprüfen
- rds-cluster-deletion-protection-aktiviert
- rds-cluster-encrypted-at-ausruhen
- rds-cluster-iam-authentication-aktiviert
- rds-cluster-multi-az-aktiviert
- rds-enhanced-monitoring-enabled
- rds-instance-default-admin-überprüfen
- rds-instance-deletion-protection-aktiviert
- rds-instance-iam-authentication-aktiviert
- rds-instance-public-access-überprüfen
- rds-instance-subnet-igw-überprüfen
- rds-in-backup-plan
- rds-last-backup-recovery-Punkt erstellt
- rds-logging-enabled
- rds-mariadb-instance-encryptedim Transit
- rds-meets-restore-time-Ziel
- rds-multi-az-support
- rds-mysql-instance-encryptedunterwegs
- rds-postgresql-logs-to- Cloudwatch
- rds-postgres-instance-encryptedunterwegs
- rds-proxy-tls-encryption
- rds-resources-protected-by-Backup-Plan
- rds-snapshot-encrypted
- rds-sqlserver-encrypted-in-Transit
- rds-sql-server-logszur Cloud-Überwachung
- rds-storage-encrypted
- redshift-backup-enabled

- redshift-cluster-configuration-check
- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check
- redshift-cluster-parameter-group-markiert
- redshift-cluster-public-access-überprüfen
- redshift-cluster-subnet-group-Multi-Az
- redshift-default-admin-check
- redshift-default-db-name-überprüfen
- redshift-enhanced-vpc-routing-aktiviert
- redshift-require-tls-ssl
- redshift-serverless-default-admin-überprüfen
- redshift-serverless-default-db-Namenscheck
- redshift-serverless-namespace-cmk-Verschlüsselung
- redshift-serverless-publish-logs-zu-Cloud-Watch
- redshift-serverless-workgroup-encryptedauf dem Weg
- redshift-serverless-workgroup-no-öffentlich zugänglich
- redshift-serverless-workgroup-routes-innerhalb von VPC
- redshift-unrestricted-port-access
- required-tags
- restricted-incoming-traffic
- root-account-hardware-mfa-aktiviert
- root-account-mfa-enabled
- nur s3- access-point-in-vpc
- s3- -Blöcke access-point-public-access
- s3- -Blöcke account-level-public-access
- s3- -Blocke-periodisch account-level-public-access
- s 3- bucket-acl-prohibited
- s-3 bucket-blacklisted-actions-prohibited
- s3- bucket-cross-region-replication -aktiviert
- s-3 bucket-default-lock-enabled

- s3 bucket-level-public-access - verboten
- s3- bucket-logging-enabled
- s-3 bucket-mfa-delete-enabled
- s-3 bucket-policy-grantee-check
- s3- bucket-policy-not-more -freizügig
- s 3- bucket-public-read-prohibited
- s-3 bucket-public-write-prohibited
- s-3 bucket-replication-enabled
- s3- bucket-server-side-encryption -aktiviert
- s-3 bucket-ssl-requests-only
- s3-Bucket-Tagged
- s-3 bucket-versioning-enabled
- s-3 default-encryption-kms
- s-3 event-notifications-enabled
- s3 last-backup-recovery-point - erstellt
- s3- lifecycle-policy-check
- s-3 meets-restore-time-target
- resources-protected-by-backups3-plan
- s 3- version-lifecycle-policy-check
- sagemaker-endpoint-configuration-kms-key-konfiguriert
- sagemaker-endpoint-config-prod-Anzahl der Instanzen
- sagemaker-notebook-instance-kms-key-konfiguriert
- sagemaker-notebook-instance-platform-Version
- sagemaker-notebook-no-direct-Internetzugang
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-überprüfen
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- securityhub-enabled

- security-account-information-provided
- service-catalog-shared-within-Organisation
- service-vpc-endpoint-enabled
- sns-encrypted-kms
- sns-topic-no-public-Zugang
- ssm-document-not-public
- ssm-document-tagged
- step-functions-state-machine-Protokollierung aktiviert
- storagegateway-last-backup-recovery-punkt-erstellt
- storagegateway-resources-in-logically-air-gapped-vault
- storagegateway-resources-protected-by-Ersatzplan
- subnet-auto-assign-public-ip-deaktiviert
- transfer-certificate-description
- transfer-certificate-tagged
- transfer-connector-tagged
- transfer-family-server-no-ftp
- transfer-profile-tagged
- transfer-workflow-description
- transfer-workflow-tagged
- vpc-default-security-group-geschlossen
- vpc-endpoint-enabled
- vpc-flow-logs-enabled
- vpc-network-acl-unused-überprüfen
- vpc-sg-open-only-to-authorized-ports
- vpc-sg-port-restriction-überprüfen
- vpc-vpn-2-tunnels-up
- wafv2-logging-enabled
- WAF 2- rulegroup-logging-enabled
- waf-regional-rule-not-leer
- waf-regional-webacl-not-leer

Region Israel (Tel Aviv)

Israel (Tel Aviv)

- account-part-of-organizations
- acmpca-certificate-authority-tagged
- acm-certificate-expiration-check
- acm-certificate-rsa-check
- acm-pca-root-ca-deaktiviert
- alb-desync-mode-check
- alb-http-drop-invalid-Header-fähig
- alb-http-to-https-Umleitungsprüfung
- alb-internal-scheme-check
- alb-waf-enabled
- api-gw-associated-with-WAF
- api-gw-cache-enabled-und-verschlüsselt
- api-gw-endpoint-type-überprüfen
- api-gw-execution-logging-aktiviert
- api-gw-ssl-enabled
- api-gw-xray-enabled
- appconfig-application-description
- appconfig-application-tagged
- appconfig-configuration-profile-tagged
- appconfig-configuration-profile-validators-nicht leer
- appconfig-deployment-strategy-description
- appconfig-deployment-strategy-replicate-zu-ssm
- appconfig-environment-description
- appconfig-environment-tagged
- appconfig-extension-association-tagged
- appconfig-freeform-profile-config-Speicher
- appconfig-hosted-configuration-version-Beschreibung

- appmesh-gateway-route-tagged
- appmesh-mesh-deny-tcp-Weiterleitung
- appmesh-mesh-tagged
- appmesh-route-tagged
- appmesh-virtual-gateway-backend-Standardeinstellungen-TLS
- appmesh-virtual-gateway-logging-file-path-exists
- appmesh-virtual-gateway-tagged
- appmesh-virtual-node-backend-defaults-tls-on
- appmesh-virtual-node-logging-file-path-exists
- appmesh-virtual-node-tagged
- appmesh-virtual-router-tagged
- appmesh-virtual-service-tagged
- approved-amis-by-id
- approved-amis-by-tag
- athena-data-catalog-description
- athena-prepared-statement-description
- athena-workgroup-description
- athena-workgroup-enforce-workgroup-Konfiguration
- athena-workgroup-engine-version-automatisches Upgrade
- athena-workgroup-logging-enabled
- aurora-mysql-cluster-audit-Protokollierung
- autoscaling-group-elb-healthcheck-erforderlich
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-hop-Grenze
- autoscaling-launch-config-public-ip-deaktiviert
- autoscaling-launch-template
- autoscaling-multiple-az
- autoscaling-multiple-instance-types
- batch-scheduling-policy-tagged
- clb-multiple-az

- cloudtrail-all-read-s3- data-event-check
- cloudtrail-all-write-s3- data-event-check
- Wolkenspur-S3- bucket-access-logging
- cloudtrail-s3- bucket-public-access-prohibited
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-action-enabled-überprüfen
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted
- cloud-trail-cloud-watch-logs-aktiviert
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-Validierung aktiviert
- cmk-backing-key-rotation-aktiviert
- codebuild-project-envvar-awscred-überprüfen
- codebuild-project-logging-enabled
- codebuild-project-s3-log-verschlüsselt
- codebuild-project-source-repo-URL-Prüfung
- codebuild-report-group-encrypted-im Ruhezustand
- codepipeline-deployment-count-check
- codepipeline-region-fanout-check
- cognito-user-pool-advanced-sicherheitsaktiviert
- cognito-user-pool-tagged
- custom-eventbus-policy-attached
- cw-loggroup-retention-period-überprüfen
- datasync-task-data-verification-aktiviert
- datasync-task-logging-enabled
- datasync-task-tagged

- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- dms-replication-not-public
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-pitr-enabled
- dynamodb-table-deletion-protection-aktiviert
- dynamodb-table-encrypted-kms
- dynamodb-table-encryption-enabled
- dynamodb-throughput-limit-check
- ebs-in-backup-plan
- ebs-optimized-instance
- ebs-snapshot-public-restorable-überprüfen
- ec2- capacity-reservation-tagged
- ec2- dhcp-options-tagged
- ec2- ebs-encryption-by-default
- ec2-imdsv2-check
- ec2- instance-detailed-monitoring-enabled
- ec2-ami instance-launched-with-allowed
- ec2- instance-managed-by-ssm
- ec2- instance-multiple-eni-check
- ec2- instance-no-public-ip
- ec2- instance-profile-attached
- ec2- managedinstance-applications-blacklisted
- ec2- managedinstance-applications-required
- ec2- managedinstance-inventory-blacklisted
- ec2- prüfen managedinstance-patch-compliance-status
- ec2- managedinstance-platform-check
- ec2- prefix-list-tagged

- ec2-eni security-group-attached-to
- ec2-stopped-instance
- ec2- traffic-mirror-filter-description
- ec2- traffic-mirror-filter-tagged
- ec2- markiert transit-gateway-multicast-domain
- ec2- volume-inuse-check
- ec2- vpn-connection-logging-enabled
- ecr-private-image-scanning-aktiviert
- ecr-repository-tagged
- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-container-insights-enabled
- ecs-fargate-latest-platform-Version
- ecs-no-environment-secrets
- ecs-task-definition-log-Konfiguration
- ecs-task-definition-network-mode-not-host
- ecs-task-definition-pid-Modus-Überprüfung
- ecs-task-definition-user-for-host-mode-check
- efs-automatic-backups-enabled
- efs-encrypted-check
- efs-in-backup-plan
- efs-mount-target-public-zugänglich
- eip-attached
- eks-cluster-secrets-encrypted
- eks-endpoint-no-public-Zugang
- eks-secrets-encrypted
- elasticache-redis-cluster-automatic-Backup-Check
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch

- elasticsearch-node-to-node-Verschlüsselungsprüfung
- elbv2-multiple-az
- elb-cross-zone-load-Balancing aktiviert
- elb-custom-security-policy-ssl-Prüfung
- elb-deletion-protection-enabled
- elb-logging-enabled
- elb-predefined-security-policy-ssl-Überprüfung
- elb-tls-https-listeners-nur
- emr-block-public-access
- emr-kerberos-enabled
- emr-security-configuration-encryption-ausruhen
- emr-security-configuration-encryption-Transit
- encrypted-volumes
- event-data-store-cmk-Verschlüsselung aktiviert
- fms-shield-resource-policy-überprüfen
- fms-webacl-resource-policy-überprüfen
- fms-webacl-rulegroup-association-überprüfen
- fsx-lustre-copy-tagszu Backups
- fsx-ontap-deployment-type-überprüfen
- fsx-openzfs-copy-tags-aktiviert
- fsx-openzfs-deployment-type-überprüfen
- fsx-windows-deployment-type-überprüfen
- glue-job-logging-enabled
- glue-ml-transform-encrypted-im Ruhezustand
- glue-spark-job-supported-Ausführung
- GuardDuty-EC2- protection-runtime-enabled
- guardduty-ecs-protection-runtime-aktiviert
- guardduty-eks-protection-audit-aktiviert
- guardduty-eks-protection-runtime-aktiviert
- guardduty-enabled-centralized

- guardduty-lambda-protection-enabled
- guardduty-malware-protection-enabled
- guardduty-non-archived-findings
- guardduty-rds-protection-enabled
- guardduty-runtime-monitoring-enabled
- GuardDuty-S3-Schutz aktiviert
- incoming-ssh-disabled
- instances-in-vpc
- internet-gateway-authorized-vpc-nur
- kinesis-firehose-delivery-stream-verschlüsselt
- kms-cmk-not-scheduled-zum Löschen
- kms-key-policy-no-öffentlicher Zugang
- lambda-concurrency-check
- lambda-dlq-check
- lambda-function-public-access-verboten
- lambda-function-settings-check
- lambda-inside-vpc
- macie-auto-sensitive-data-Discovery-Check
- mariadb-publish-logs-to-Cloudwatch-Protokolle
- multi-region-cloud-trail-aktiviert
- nacl-no-unrestricted-ssh-rdp
- neptune-cluster-backup-retention-überprüfen
- neptune-cluster-cloudwatch-log-exportfähig
- neptune-cluster-copy-tags-to-snapshot-enabled
- neptune-cluster-deletion-protection-aktiviert
- neptune-cluster-encrypted
- neptune-cluster-iam-database-Authentifizierung
- neptune-cluster-multi-az-aktiviert
- netfw-deletion-protection-enabled
- netfw-logging-enabled

- netfw-multi-az-enabled
- netfw-policy-default-action-fragment-Pakete
- netfw-policy-default-action-vollständige Pakete
- netfw-policy-rule-group-assoziiert
- netfw-stateless-rule-group-nicht leer
- netfw-subnet-change-protection-aktiviert
- nlb-internal-scheme-check
- nlb-logging-enabled
- no-unrestricted-route-to-igw
- rds-aurora-mysql-audit-Protokollierung aktiviert
- rds-automatic-minor-version-upgrade-fähig
- rds-cluster-default-admin-überprüfen
- rds-cluster-deletion-protection-aktiviert
- rds-cluster-encrypted-at-ausruhen
- rds-cluster-iam-authentication-aktiviert
- rds-cluster-multi-az-aktiviert
- rds-enhanced-monitoring-enabled
- rds-instance-default-admin-überprüfen
- rds-instance-deletion-protection-aktiviert
- rds-instance-iam-authentication-aktiviert
- rds-instance-public-access-überprüfen
- rds-instance-subnet-igw-überprüfen
- rds-in-backup-plan
- rds-logging-enabled
- rds-mariadb-instance-encryptedauf dem Weg
- rds-multi-az-support
- rds-mysql-instance-encryptedim Transit
- rds-postgresql-logs-to- Cloudwatch
- rds-postgres-instance-encryptedunterwegs
- rds-proxy-tls-encryption

- rds-snapshot-encrypted
- rds-sqlserver-encrypted-in-im Transit
- rds-sql-server-logszur Cloud-Überwachung
- rds-storage-encrypted
- redshift-cluster-configuration-check
- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check
- redshift-cluster-parameter-group-markiert
- redshift-cluster-public-access-überprüfen
- redshift-cluster-subnet-group-Multi-Az
- redshift-enhanced-vpc-routing-aktiviert
- redshift-require-tls-ssl
- redshift-serverless-default-admin-überprüfen
- redshift-serverless-default-db-Namenscheck
- redshift-serverless-namespace-cmk-Verschlüsselung
- redshift-serverless-publish-logs-zu-Cloud-Watch
- redshift-serverless-workgroup-no-öffentlicher Zugang
- redshift-unrestricted-port-access
- required-tags
- restricted-incoming-traffic
- nur s3- access-point-in-vpc
- s3- -Blöcke access-point-public-access
- s3- -Blocke-periodisch account-level-public-access
- s 3- bucket-acl-prohibited
- s-3 bucket-blacklisted-actions-prohibited
- s3- bucket-cross-region-replication -aktiviert
- s-3 bucket-default-lock-enabled
- s3 bucket-level-public-access - verboten
- s3- bucket-logging-enabled
- s-3 bucket-mfa-delete-enabled

- s-3 bucket-policy-grantee-check
- s3- bucket-policy-not-more -freizügig
- s 3- bucket-public-read-prohibited
- s-3 bucket-public-write-prohibited
- s-3 bucket-replication-enabled
- s3- bucket-server-side-encryption -aktiviert
- s-3 bucket-ssl-requests-only
- s3-Bucket-Tagged
- s-3 bucket-versioning-enabled
- s-3 default-encryption-kms
- s-3 event-notifications-enabled
- s-3 lifecycle-policy-check
- s-3 version-lifecycle-policy-check
- sagemaker-app-image-config-markiert
- sagemaker-endpoint-configuration-kms-schlüsselkonfiguriert
- sagemaker-endpoint-config-prod-Anzahl der Instanzen
- sagemaker-feature-group-tagged
- sagemaker-image-description
- sagemaker-image-tagged
- sagemaker-notebook-instance-kms-key-konfiguriert
- sagemaker-notebook-instance-platform-Version
- sagemaker-notebook-no-direct-Internetzugang
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-überprüfen
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- securityhub-enabled
- security-account-information-provided
- service-vpc-endpoint-enabled

- sns-encrypted-kms
- sns-topic-no-public-Zugang
- ssm-document-not-public
- ssm-document-tagged
- subnet-auto-assign-public-ip-deaktiviert
- transfer-certificate-description
- transfer-certificate-tagged
- transfer-connector-tagged
- transfer-family-server-no-ftp
- transfer-profile-tagged
- transfer-workflow-description
- transfer-workflow-tagged
- vpc-default-security-group-geschlossen
- vpc-flow-logs-enabled
- vpc-network-acl-unused-überprüfen
- vpc-sg-open-only-to-authorized-ports
- vpc-sg-port-restriction-überprüfen
- wafv2-logging-enabled
- WAF 2- rulegroup-logging-enabled
- WAF 2- webacl-not-empty
- waf-regional-rule-not-leer
- waf-regional-webacl-not-leer

Region Mexiko (Zentral)

Mexiko (Zentral)

- account-part-of-organizations
- acm-certificate-expiration-check
- alb-http-drop-invalid-Header-fähig
- alb-http-to-https-Umleitungsprüfung
- alb-waf-enabled

- approved-amis-by-id
- approved-amis-by-tag
- aurora-mysql-backtracking-enabled
- autoscaling-group-elb-healthcheck-erforderlich
- autoscaling-launch-config-public-ip-deaktiviert
- cloudformation-stack-drift-detection-überprüfen
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted
- cloud-trail-cloud-watch-logs-aktiviert
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-Validierung aktiviert
- cmk-backing-key-rotation-aktiviert
- cw-loggroup-retention-period-überprüfen
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- dms-replication-not-public
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-pitr-enabled
- dynamodb-table-encrypted-kms
- dynamodb-table-encryption-enabled
- dynamodb-throughput-limit-check
- ebs-in-backup-plan
- ebs-snapshot-public-restorable-überprüfen

- ec2- ebs-encryption-by-default
- ec2-imdsv2-check
- ec2- instance-detailed-monitoring-enabled
- ec2-ami instance-launched-with-allowed
- ec2- instance-managed-by-ssm
- ec2- instance-multiple-eni-check
- ec2- instance-no-public-ip
- ec2- instance-profile-attached
- ec2- managedinstance-applications-blacklisted
- ec2- managedinstance-applications-required
- ec2- managedinstance-inventory-blacklisted
- ec2- prüfen managedinstance-patch-compliance-status
- ec2- managedinstance-platform-check
- ec2-eni security-group-attached-to
- ec2-stopped-instance
- ec2- volume-inuse-check
- ecs-task-definition-user-for-host-mode-check
- efs-encrypted-check
- efs-in-backup-plan
- eip-attached
- eks-endpoint-no-public-Zugang
- eks-secrets-encrypted
- elasticache-redis-cluster-automatic-Backup-Check
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch
- elasticsearch-node-to-node-Verschlüsselungsprüfung
- elb-acm-certificate-required
- elb-cross-zone-load-Balancing aktiviert
- elb-custom-security-policy-ssl-Prüfung

- elb-deletion-protection-enabled
- elb-logging-enabled
- elb-predefined-security-policy-ssl-Überprüfung
- elb-tls-https-listeners-nur
- emr-kerberos-enabled
- emr-master-no-public-ip
- encrypted-volumes
- iam-password-policy
- incoming-ssh-disabled
- instances-in-vpc
- internet-gateway-authorized-vpc-nur
- kms-cmk-not-scheduled-zum Löschen
- lambda-concurrency-check
- lambda-dlq-check
- lambda-function-public-access-verboten
- lambda-function-settings-check
- lambda-inside-vpc
- multi-region-cloud-trail-aktiviert
- no-unrestricted-route-to-igw
- rds-automatic-minor-version-Upgrade aktiviert
- rds-cluster-deletion-protection-aktiviert
- rds-cluster-iam-authentication-aktiviert
- rds-cluster-multi-az-aktiviert
- rds-enhanced-monitoring-enabled
- rds-instance-deletion-protection-aktiviert
- rds-instance-iam-authentication-aktiviert
- rds-instance-public-access-überprüfen
- rds-in-backup-plan
- rds-logging-enabled
- rds-multi-az-support

- rds-snapshots-public-prohibited
- rds-snapshot-encrypted
- rds-storage-encrypted
- required-tags
- restricted-incoming-traffic
- s3- -Blocke-periodisch account-level-public-access
- s 3- bucket-blacklisted-actions-prohibited
- s-3 bucket-default-lock-enabled
- s3 bucket-level-public-access - verboten
- s3- bucket-logging-enabled
- s-3 bucket-policy-grantee-check
- s3- bucket-policy-not-more -freizügig
- s 3- bucket-public-read-prohibited
- s-3 bucket-public-write-prohibited
- s-3 bucket-replication-enabled
- s3- bucket-server-side-encryption -aktiviert
- s-3 bucket-ssl-requests-only
- s-3 bucket-versioning-enabled
- s-3 default-encryption-kms
- secretsmanager-using-cmk
- securityhub-enabled
- service-vpc-endpoint-enabled
- sns-encrypted-kms
- ssm-document-not-public
- subnet-auto-assign-public-ip-deaktiviert
- vpc-default-security-group-geschlossen
- vpc-flow-logs-enabled
- vpc-network-acl-unused-überprüfen
- vpc-sg-open-only-to-authorized-ports
- vpc-vpn-2-tunnels-up

Region Naher Osten (Bahrain)

Naher Osten (Bahrain)

- access-keys-rotated
- account-part-of-organizations
- acmpca-certificate-authority-tagged
- acm-certificate-expiration-check
- acm-certificate-rsa-check
- acm-pca-root-ca-deaktiviert
- active-mq-supported-version
- alb-desync-mode-check
- alb-http-drop-invalid-Header-fähig
- alb-http-to-https-Umleitungsprüfung
- alb-internal-scheme-check
- alb-listener-tagged
- alb-waf-enabled
- amplify-app-branch-auto-löschung aktiviert
- amplify-app-description
- amplify-app-tagged
- amplify-branch-performance-mode-aktiviert
- amplify-branch-tagged
- api-gwv2- access-logs-enabled
- api-gwv2- authorization-type-configured
- api-gw-associated-with-WAF
- api-gw-cache-enabled-und-verschlüsselt
- api-gw-endpoint-type-überprüfen
- api-gw-execution-logging-aktiviert
- api-gw-ssl-enabled
- api-gw-xray-enabled
- appconfig-application-description

- appconfig-application-tagged
- appconfig-configuration-profile-tagged
- appconfig-configuration-profile-validators-nicht leer
- appconfig-deployment-strategy-description
- appconfig-deployment-strategy-replicate-zu-ssm
- appconfig-environment-description
- appconfig-environment-tagged
- appconfig-extension-association-tagged
- appconfig-freeform-profile-config-Speicher
- appconfig-hosted-configuration-version-Beschreibung
- appmesh-gateway-route-tagged
- appmesh-mesh-deny-tcp-Weiterleitung
- appmesh-mesh-tagged
- appmesh-route-tagged
- appmesh-virtual-gateway-backend-Standardeinstellungen-TLS
- appmesh-virtual-gateway-logging-file-path-exists
- appmesh-virtual-gateway-tagged
- appmesh-virtual-node-backend-defaults-tls-on
- appmesh-virtual-node-logging-file-path-exists
- appmesh-virtual-node-tagged
- appmesh-virtual-router-tagged
- appmesh-virtual-service-tagged
- approved-amis-by-id
- approved-amis-by-tag
- appsync-associated-with-waf
- appsync-authorization-check
- appsync-cache-ct-encryption-im Ruhezustand
- appsync-cache-ct-encryptionim Transit
- appsync-cache-encryption-at-ausruhen
- appsync-logging-enabled

- athena-data-catalog-description
- athena-prepared-statement-description
- athena-workgroup-description
- athena-workgroup-encrypted-at-ausruhen
- athena-workgroup-enforce-workgroup-Konfiguration
- athena-workgroup-engine-version-automatisches Upgrade
- athena-workgroup-logging-enabled
- aurora-last-backup-recovery-Punkt erstellt
- aurora-meets-restore-time-Ziel
- aurora-resources-in-logically-air-gapped-vault
- aurora-resources-protected-by-Backup-Plan
- autoscaling-capacity-rebalancing
- autoscaling-group-elb-healthcheck-erforderlich
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-hop-Grenze
- autoscaling-launch-config-public-ip-deaktiviert
- autoscaling-launch-template
- autoscaling-multiple-az
- autoscaling-multiple-instance-types
- backup-plan-min-frequency-and-min-retention-check
- backup-recovery-point-encrypted
- backup-recovery-point-manual-Löschen-deaktiviert
- backup-recovery-point-minimum-Aufbewahrungsprüfung
- batch-compute-environment-enabled
- batch-compute-environment-managed
- batch-compute-environment-tagged
- batch-job-queue-enabled
- batch-job-queue-tagged
- batch-managed-compute-environment-using-launch-template
- batch-managed-compute-env-compute-resources-tagged

- batch-scheduling-policy-tagged
- beanstalk-enhanced-health-reporting-aktiviert
- cassandra-keyspace-tagged
- clb-desync-mode-check
- clb-multiple-az
- cloudformation-stack-drift-detection-überprüfen
- cloudformation-stack-notification-check
- cloudtrail-all-read-s3- data-event-check
- cloudtrail-all-write-s3- data-event-check
- Wolkenspur-S3- bucket-access-logging
- cloudtrail-s3- bucket-public-access-prohibited
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-action-enabled-überprüfen
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted
- cloud-trail-cloud-watch-logs-aktiviert
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-Validierung aktiviert
- cmk-backing-key-rotation-aktiviert
- codebuild-project-artifact-encryption
- codebuild-project-environment-privileged-überprüfen
- codebuild-project-envvar-awscred-überprüfen
- codebuild-project-logging-enabled
- codebuild-project-s3-log-verschlüsselt
- codebuild-project-source-repo-URL-Prüfung
- codebuild-report-group-encrypted-im Ruhezustand

- codedeploy-auto-rollback-monitor-aktiviert
- codedeploy-deployment-group-auto-rollback-aktiviert
- codedeploy-deployment-group-outdated-instanzen-aktualisieren
- Codedeploy-ec2- minimum-healthy-hosts-configured
- codedeploy-lambda-allatonce-traffic-shift-deaktiviert
- cognito-identity-pool-unauth-Zugriffsprüfung
- cognito-user-pool-advanced-sicherheitsaktiviert
- cognito-user-pool-tagged
- custom-eventbus-policy-attached
- cw-loggroup-retention-period-überprüfen
- datasync-task-data-verification-aktiviert
- datasync-task-logging-enabled
- datasync-task-tagged
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- dms-auto-minor-version-aktualisieren-Prüfung
- dms-endpoint-ssl-configured
- dms-endpoint-tagged
- dms-mongo-db-authentication-aktiviert
- dms-neptune-iam-authorization-aktiviert
- dms-redis-tls-enabled
- dms-replication-not-public
- dms-replication-task-sourcedb-Protokollierung
- dms-replication-task-tagged
- dms-replication-task-targetdb-Protokollierung
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-last-backup-recovery-Punkt erstellt
- dynamodb-meets-restore-time-Ziel

- dynamodb-pitr-enabled
- dynamodb-resources-protected-by-Backup-Plan
- dynamodb-table-deletion-protection-aktiviert
- dynamodb-table-encrypted-kms
- dynamodb-throughput-limit-check
- ebs-in-backup-plan
- ebs-last-backup-recovery-punkt-erstellt
- ebs-meets-restore-time-Ziel
- ebs-optimized-instance
- ebs-resources-in-logically-air-gapped-vault
- ebs-resources-protected-by-Backup-Plan
- ebs-snapshot-public-restorable-überprüfen
- ec2- capacity-reservation-tagged
- ec2- aktiviert client-vpn-connection-log
- ec2- client-vpn-endpoint-tagged
- ec2- -alle client-vpn-not-authorize
- ec2- dhcp-options-tagged
- ec2- ebs-encryption-by-default
- ec2- aktiviert enis-source-destination-check
- ec2-fleet-markiert
- ec2-imdsv2-check
- ec2- instance-detailed-monitoring-enabled
- ec2-ami instance-launched-with-allowed
- ec2- instance-managed-by-ssm
- ec2- instance-multiple-eni-check
- ec2- instance-no-public-ip
- ec2- instance-profile-attached
- ec2- erstellt last-backup-recovery-point
- ec2-2-prüfen launch-template-imdsv
- ec2- -deaktiviert launch-template-public-ip

- ec2- launch-template-tagged
- ec2- managedinstance-applications-blacklisted
- ec2- managedinstance-applications-required
- ec2- prüfen managedinstance-association-compliance-status
- ec2- managedinstance-inventory-blacklisted
- ec2- prüfen managedinstance-patch-compliance-status
- ec2- managedinstance-platform-check
- ec2- meets-restore-time-target
- ec2- Analyse mit Schlagwörtern network-insights-access-scope
- ec2 network-insights-access-scope - markiert
- ec2- network-insights-path-tagged
- ec2- no-amazon-key-pair
- ec2- prefix-list-tagged
- ec2- -Tresor mit Lücken resources-in-logically-air
- ec2- resources-protected-by-backup -plan
- ec2- -eni security-group-attached-to
- ec2- -eni-periodisch security-group-attached-to
- ec2-stopped-instance
- ec2- token-hop-limit-check
- ec2- traffic-mirror-filter-description
- ec2- traffic-mirror-filter-tagged
- ec2- traffic-mirror-session-description
- ec2- traffic-mirror-session-tagged
- ec2- traffic-mirror-target-description
- ec2- traffic-mirror-target-tagged
- ec2- -attach-deaktiviert transit-gateway-auto-vpc
- ec2 transit-gateway-multicast-domain - markiert
- ec2- volume-inuse-check
- ec2- vpn-connection-logging-enabled
- ecr-private-image-scanning-aktiviert

- ecr-private-lifecycle-policy-konfiguriert
- ecr-private-tag-immutability-aktiviert
- ecr-repository-tagged
- ecs-awsvpc-networking-enabled
- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-container-insights-enabled
- ecs-fargate-latest-platform-Version
- ecs-no-environment-secrets
- ecs-task-definition-log-Konfiguration
- ecs-task-definition-memory-hartes Limit
- ecs-task-definition-nonroot-Benutzer
- ecs-task-definition-pid-Modus-Check
- ecs-task-definition-user-for-host-mode-check
- efs-access-point-enforce-Stammverzeichnis
- efs-access-point-enforce-Benutzeridentität
- efs-automatic-backups-enabled
- efs-encrypted-check
- efs-filesystem-ct-encrypted
- efs-in-backup-plan
- efs-last-backup-recovery-Punkt erstellt
- efs-meets-restore-time-Ziel
- efs-mount-target-public-zugänglich
- efs-resources-in-logically-air-gapped-vault
- efs-resources-protected-by-Ersatzplan
- eip-attached
- eks-cluster-logging-enabled
- eks-cluster-log-enabled
- eks-cluster-oldest-supported-Ausführung
- eks-cluster-secrets-encrypted

- eks-cluster-supported-version
- eks-endpoint-no-public-Zugang
- eks-secrets-encrypted
- elasticache-auto-minor-version-Upgrade-Check
- elasticache-rbac-auth-enabled
- elasticache-redis-cluster-automatic-Backup-Check
- elasticache-repl-grp-auto-failover-fähig
- elasticache-repl-grp-encrypted-im Ruhezustand
- elasticache-repl-grp-encryptedim Transit
- elasticache-repl-grp-redis-auth-aktiviert
- elasticache-subnet-group-check
- elasticache-supported-engine-version
- elasticbeanstalk-application-description
- elasticbeanstalk-application-version-description
- elasticbeanstalk-environment-description
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch
- elasticsearch-node-to-node-Verschlüsselungsprüfung
- elastic-beanstalk-logs-to- Cloudwatch
- elastic-beanstalk-managed-updates-aktiviert
- elbv2- acm-certificate-required
- elv 2- listener-encryption-in-transit
- elbv2-multiple-az
- elb-acm-certificate-required
- elb-cross-zone-load-Balancing aktiviert
- elb-custom-security-policy-ssl-Prüfung
- elb-deletion-protection-enabled
- elb-logging-enabled
- elb-predefined-security-policy-ssl-Überprüfung

- elb-tls-https-listeners-nur
- emr-block-public-access
- emr-kerberos-enabled
- emr-master-no-public-ip
- emr-security-configuration-encryption-ausruhen
- emr-security-configuration-encryption-Transit
- encrypted-volumes
- fis-experiment-template-log-Konfiguration vorhanden
- fis-experiment-template-tagged
- fms-shield-resource-policy-überprüfen
- fms-webacl-resource-policy-überprüfen
- fms-webacl-rulegroup-association-überprüfen
- fsx-last-backup-recovery-Punkt erstellt
- fsx-lustre-copy-tagszu Backups
- fsx-meets-restore-time-Ziel
- fsx-openzfs-copy-tags-aktiviert
- fsx-resources-protected-by-Backup-Plan
- fsx-windows-audit-log-konfiguriert
- glb-listener-tagged
- glue-job-logging-enabled
- glue-ml-transform-encrypted-im Ruhezustand
- guardduty-eks-protection-audit-aktiviert
- guardduty-eks-protection-runtime-aktiviert
- guardduty-enabled-centralized
- guardduty-lambda-protection-enabled
- guardduty-malware-protection-enabled
- guardduty-non-archived-findings
- guardduty-rds-protection-enabled
- GuardDuty-S3-Schutz aktiviert
- iam-customer-policy-blocked-kms-Aktionen

- iam-external-access-analyzer-aktiviert
- iam-group-has-users-überprüfen
- iam-inline-policy-blocked-kms-Aktionen
- iam-no-inline-policy-überprüfen
- iam-password-policy
- iam-policy-blacklisted-check
- iam-policy-in-use
- iam-policy-no-statements-with-admin-access
- iam-policy-no-statements-with-full-access
- iam-role-managed-policy-überprüfen
- iam-root-access-key-überprüfen
- iam-user-group-membership-überprüfen
- iam-user-mfa-enabled
- iam-user-no-policies-überprüfen
- iam-user-unused-credentials-überprüfen
- incoming-ssh-disabled
- inspector-ec2-Scan aktiviert
- inspector-ecr-scan-enabled
- inspector-lambda-standard-scan-aktiviert
- instances-in-vpc
- internet-gateway-authorized-vpc-nur
- iot-authorizer-token-signing-aktiviert
- kinesis-firehose-delivery-stream-verschlüsselt
- kinesis-stream-backup-retention-überprüfen
- kinesis-stream-encrypted
- kms-cmk-not-scheduled-zum Löschen
- kms-key-policy-no-öffentlicher Zugang
- lambda-concurrency-check
- lambda-dlq-check
- lambda-function-public-access-verboten

- lambda-function-settings-check
- lambda-function-xray-enabled
- lambda-inside-vpc
- lambda-vpc-multi-az-überprüfen
- macie-auto-sensitive-data-Discovery-Check
- macie-status-check
- mfa-enabled-for-iam-Konsolenzugriff
- mq-active-broker-ldap-Authentifizierung
- mq-active-deployment-mode
- mq-active-single-instance-broker-storage-type-efs
- mq-automatic-minor-version-Upgrade aktiviert
- mq-auto-minor-version-upgrade-fähig
- mq-broker-general-logging-aktiviert
- mq-cloudwatch-audit-logging-aktiviert
- mq-cloudwatch-audit-log-aktiviert
- mq-no-public-access
- mq-rabbit-deployment-mode
- msk-cluster-public-access-deaktiviert
- msk-enhanced-monitoring-enabled
- msk-in-cluster-node-require-tls
- msk-unrestricted-access-check
- multi-region-cloud-trail-aktiviert
- nacl-no-unrestricted-ssh-rdp
- neptune-cluster-backup-retention-überprüfen
- neptune-cluster-cloudwatch-log-exportfähig
- neptune-cluster-copy-tags-to-snapshot-enabled
- neptune-cluster-deletion-protection-aktiviert
- neptune-cluster-encrypted
- neptune-cluster-iam-database-Authentifizierung
- neptune-cluster-multi-az-aktiviert

- neptune-cluster-snapshot-encrypted
- neptune-cluster-snapshot-public-verboten
- netfw-deletion-protection-enabled
- netfw-logging-enabled
- netfw-multi-az-enabled
- netfw-policy-default-action-fragment-Pakete
- netfw-policy-default-action-vollständige Pakete
- netfw-policy-rule-group-assoziiert
- netfw-stateless-rule-group-nicht leer
- nlb-cross-zone-load-Balancing aktiviert
- nlb-internal-scheme-check
- nlb-listener-tagged
- nlb-logging-enabled
- no-unrestricted-route-to-igw
- opensearch-access-control-enabled
- opensearch-audit-logging-enabled
- opensearch-data-node-fault-Toleranz
- opensearch-encrypted-at-rest
- opensearch-https-required
- opensearch-in-vpc-only
- opensearch-logs-to-cloudwatch
- opensearch-node-to-node-Verschlüsselungsprüfung
- opensearch-primary-node-fault-Toleranz
- opensearch-update-check
- rabbit-mq-supported-version
- rds-aurora-mysql-audit-Protokollierung aktiviert
- rds-aurora-postgresql-logs-zu-Cloud-Watch
- rds-automatic-minor-version-upgrade-fähig
- rds-cluster-auto-minor-version-upgrade-enable
- rds-cluster-default-admin-überprüfen

- rds-cluster-deletion-protection-aktiviert
- rds-cluster-encrypted-at-ausruhen
- rds-cluster-iam-authentication-aktiviert
- rds-cluster-multi-az-aktiviert
- rds-enhanced-monitoring-enabled
- rds-instance-default-admin-überprüfen
- rds-instance-deletion-protection-aktiviert
- rds-instance-iam-authentication-aktiviert
- rds-instance-public-access-überprüfen
- rds-in-backup-plan
- rds-last-backup-recovery-Punkt erstellt
- rds-logging-enabled
- rds-meets-restore-time-Ziel
- rds-multi-az-support
- rds-mysql-instance-encryptedunterwegs
- rds-postgresql-logs-to- Cloudwatch
- rds-postgres-instance-encryptedauf dem Weg
- rds-resources-protected-by-Ersatzplan
- rds-snapshots-public-prohibited
- rds-snapshot-encrypted
- rds-sql-server-logszur Cloud-Überwachung
- rds-storage-encrypted
- redshift-audit-logging-enabled
- redshift-backup-enabled
- redshift-cluster-configuration-check
- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check
- redshift-cluster-multi-az-aktiviert
- redshift-cluster-parameter-group-markiert
- redshift-cluster-public-access-überprüfen

- redshift-cluster-subnet-group-Multi-Az
- redshift-default-admin-check
- redshift-default-db-name-überprüfen
- redshift-enhanced-vpc-routing-aktiviert
- redshift-require-tls-ssl
- redshift-unrestricted-port-access
- required-tags
- restricted-incoming-traffic
- root-account-hardware-mfa-aktiviert
- root-account-mfa-enabled
- nur s3- access-point-in-vpc
- s3- -Blöcke access-point-public-access
- s3- -Blöcke account-level-public-access
- s3- -Blocke-periodisch account-level-public-access
- s 3- bucket-acl-prohibited
- s-3 bucket-blacklisted-actions-prohibited
- s3- bucket-cross-region-replication -aktiviert
- s-3 bucket-default-lock-enabled
- s3 bucket-level-public-access - verboten
- s3- bucket-logging-enabled
- s-3 bucket-mfa-delete-enabled
- s-3 bucket-policy-grantee-check
- s3- bucket-policy-not-more -freizügig
- s 3- bucket-public-read-prohibited
- s-3 bucket-public-write-prohibited
- s-3 bucket-replication-enabled
- s3- bucket-server-side-encryption -aktiviert
- s-3 bucket-ssl-requests-only
- s3-Bucket-Tag
- s-3 bucket-versioning-enabled

- s-3 default-encryption-kms
- s-3 event-notifications-enabled
- s3 last-backup-recovery-point - erstellt
- s3- lifecycle-policy-check
- s-3 meets-restore-time-target
- s3- resources-in-logically-air -Tresor mit Lücken
- s3 resources-protected-by-backup - -Plan
- s 3- version-lifecycle-policy-check
- sagemaker-app-image-config-markiert
- sagemaker-domain-in-vpc
- sagemaker-domain-tagged
- sagemaker-endpoint-configuration-kms-schlüsselkonfiguriert
- sagemaker-endpoint-config-prod-Anzahl der Instanzen
- sagemaker-feature-group-tagged
- sagemaker-image-description
- sagemaker-image-tagged
- sagemaker-model-in-vpc
- sagemaker-model-isolation-enabled
- sagemaker-notebook-instance-inside-vpc
- sagemaker-notebook-instance-kms-key-konfiguriert
- sagemaker-notebook-instance-root-Zugriffsprüfung
- sagemaker-notebook-no-direct-Internetzugang
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-überprüfen
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- securityhub-enabled
- security-account-information-provided
- service-catalog-shared-within-Organisation

- service-vpc-endpoint-enabled
- sns-encrypted-kms
- sns-topic-message-delivery-Benachrichtigung aktiviert
- sns-topic-no-public-Zugriff
- ssm-automation-block-public-teilen
- ssm-automation-logging-enabled
- ssm-document-not-public
- ssm-document-tagged
- step-functions-state-machine-Protokollierung aktiviert
- storagegateway-last-backup-recovery-punkt-erstellt
- storagegateway-resources-in-logically-air-gapped-vault
- storagegateway-resources-protected-by-Ersatzplan
- subnet-auto-assign-public-ip-deaktiviert
- transfer-agreement-description
- transfer-agreement-tagged
- transfer-certificate-description
- transfer-certificate-tagged
- transfer-connector-tagged
- transfer-family-server-no-ftp
- transfer-profile-tagged
- transfer-workflow-description
- transfer-workflow-tagged
- virtualmachine-last-backup-recovery-Punkt erstellt
- virtualmachine-resources-in-logically-air-gapped-vault
- virtualmachine-resources-protected-by-Ersatzplan
- vpc-default-security-group-geschlossen
- vpc-endpoint-enabled
- vpc-flow-logs-enabled
- vpc-network-acl-unused-überprüfen
- vpc-peering-dns-resolution-überprüfen

- vpc-sg-open-only-to-authorized-ports
- vpc-sg-port-restriction-überprüfen
- wafv2-logging-enabled
- WAF 2- rulegroup-logging-enabled
- WAF 2- rulegroup-not-empty
- WAF 2- webacl-not-empty
- waf-regional-rulegroup-not-leer
- waf-regional-rule-not-leer
- waf-regional-webacl-not-leer

Region Naher Osten (UAE)

Naher Osten (VAE)

- account-part-of-organizations
- acmpca-certificate-authority-tagged
- acm-certificate-expiration-check
- acm-certificate-rsa-check
- acm-pca-root-ca-deaktiviert
- active-mq-supported-version
- alb-desync-mode-check
- alb-http-drop-invalid-Header-fähig
- alb-http-to-https-Umleitungsprüfung
- alb-internal-scheme-check
- alb-waf-enabled
- api-gw-associated-with-WAF
- api-gw-cache-enabled-und-verschlüsselt
- api-gw-endpoint-type-überprüfen
- api-gw-execution-logging-aktiviert
- api-gw-ssl-enabled
- api-gw-xray-enabled
- appconfig-deployment-strategy-description

- appconfig-deployment-strategy-replicate-zu-ssm
- appconfig-extension-association-tagged
- approved-amis-by-id
- approved-amis-by-tag
- appsync-authorization-check
- appsync-logging-enabled
- athena-data-catalog-description
- athena-prepared-statement-description
- athena-workgroup-description
- athena-workgroup-enforce-workgroup-Konfiguration
- athena-workgroup-engine-version-automatisches Upgrade
- athena-workgroup-logging-enabled
- aurora-last-backup-recovery-Punkt erstellt
- aurora-meets-restore-time-Ziel
- aurora-mysql-cluster-audit-Protokollierung
- aurora-resources-in-logically-air-gapped-vault
- aurora-resources-protected-by-Backup-Plan
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-hop-Grenze
- autoscaling-launch-config-public-ip-deaktiviert
- autoscaling-launch-template
- autoscaling-multiple-az
- autoscaling-multiple-instance-types
- backup-plan-min-frequency-and-min-retention-check
- backup-recovery-point-encrypted
- backup-recovery-point-manual-Löschen-deaktiviert
- backup-recovery-point-minimum-Aufbewahrungsprüfung
- batch-compute-environment-enabled
- batch-compute-environment-managed
- batch-compute-environment-tagged

- batch-job-queue-enabled
- batch-job-queue-tagged
- batch-managed-compute-environment-using-launch-template
- batch-managed-compute-env-compute-resources-tagged
- batch-scheduling-policy-tagged
- clb-multiple-az
- cloudtrail-all-read-s3- data-event-check
- cloudtrail-all-write-s3- data-event-check
- Wolkenspur-S3- bucket-access-logging
- cloudtrail-s3- bucket-public-access-prohibited
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-action-enabled-überprüfen
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloud-trail-cloud-watch-logs-aktiviert
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-Validierung aktiviert
- codebuild-project-envvar-awscred-überprüfen
- codebuild-project-logging-enabled
- codebuild-project-s3-log-verschlüsselt
- codebuild-project-source-repo-URL-Prüfung
- codebuild-report-group-encrypted-im Ruhezustand
- codepipeline-deployment-count-check
- codepipeline-region-fanout-check
- cognito-user-pool-tagged
- custom-eventbus-policy-attached
- datasync-task-data-verification-aktiviert

- datasync-task-logging-enabled
- datasync-task-tagged
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- dms-replication-not-public
- docdb-cluster-audit-logging-aktiviert
- docdb-cluster-backup-retention-überprüfen
- docdb-cluster-deletion-protection-aktiviert
- docdb-cluster-encrypted
- docdb-cluster-encrypted-in-Transit
- docdb-cluster-snapshot-public-verboten
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-last-backup-recovery-Punkt erstellt
- dynamodb-meets-restore-time-Ziel
- dynamodb-pitr-enabled
- dynamodb-resources-protected-by-Backup-Plan
- dynamodb-table-deletion-protection-aktiviert
- dynamodb-table-encrypted-kms
- dynamodb-table-encryption-enabled
- dynamodb-throughput-limit-check
- ebs-in-backup-plan
- ebs-last-backup-recovery-punkt-erstellt
- ebs-meets-restore-time-Ziel
- ebs-optimized-instance
- ebs-resources-in-logically-air-gapped-vault
- ebs-resources-protected-by-Backup-Plan
- ebs-snapshot-public-restorable-überprüfen
- ec2- capacity-reservation-tagged

- ec2- dhcp-options-tagged
- ec2- ebs-encryption-by-default
- ec2-Fleet-markiert
- ec2-imdsv2-check
- ec2- instance-detailed-monitoring-enabled
- ec2-ami instance-launched-with-allowed
- ec2- instance-multiple-eni-check
- ec2- instance-no-public-ip
- ec2- instance-profile-attached
- ec2- erstellt last-backup-recovery-point
- ec2- managedinstance-applications-blacklisted
- ec2- managedinstance-applications-required
- ec2- prüfen managedinstance-association-compliance-status
- ec2- managedinstance-inventory-blacklisted
- ec2- prüfen managedinstance-patch-compliance-status
- ec2- managedinstance-platform-check
- ec2- meets-restore-time-target
- ec2- prefix-list-tagged
- ec2- -Tresor mit Lücken resources-in-logically-air
- ec2- resources-protected-by-backup -plan
- ec2- traffic-mirror-filter-description
- ec2- traffic-mirror-filter-tagged
- ec2- -attach-deaktiviert transit-gateway-auto-vpc
- ec2 transit-gateway-multicast-domain - markiert
- ec2- volume-inuse-check
- ec2- vpn-connection-logging-enabled
- ecr-private-image-scanning-aktiviert
- ecr-private-lifecycle-policy-konfiguriert
- ecr-private-tag-immutability-aktiviert
- ecr-repository-cmk-encryption-aktiviert

- ecr-repository-tagged
- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-container-insights-enabled
- ecs-fargate-latest-platform-Version
- ecs-no-environment-secrets
- ecs-task-definition-log-Konfiguration
- ecs-task-definition-network-mode-not-host
- ecs-task-definition-pid-Modus-Überprüfung
- efs-access-point-enforce-Stammverzeichnis
- efs-access-point-enforce-Benutzeridentität
- efs-automatic-backups-enabled
- efs-encrypted-check
- efs-filesystem-ct-encrypted
- efs-in-backup-plan
- efs-last-backup-recovery-Punkt erstellt
- efs-meets-restore-time-Ziel
- efs-mount-target-public-zugänglich
- efs-resources-in-logically-air-gapped-vault
- efs-resources-protected-by-Ersatzplan
- eks-cluster-log-enabled
- eks-cluster-secrets-encrypted
- eks-cluster-supported-version
- eks-endpoint-no-public-Zugang
- eks-secrets-encrypted
- elasticache-redis-cluster-automatic-Backup-Check
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch
- elasticsearch-node-to-node-Verschlüsselungsprüfung

- elbv2-multiple-az
- elb-acm-certificate-required
- elb-cross-zone-load-Balancing aktiviert
- elb-custom-security-policy-ssl-Prüfung
- elb-deletion-protection-enabled
- elb-logging-enabled
- elb-predefined-security-policy-ssl-Überprüfung
- emr-block-public-access
- emr-kerberos-enabled
- emr-master-no-public-ip
- emr-security-configuration-encryption-ausruhen
- emr-security-configuration-encryption-Transit
- encrypted-volumes
- event-data-store-cmk-Verschlüsselung aktiviert
- fms-shield-resource-policy-überprüfen
- fms-webacl-resource-policy-überprüfen
- fms-webacl-rulegroup-association-überprüfen
- fsx-last-backup-recovery-Punkt erstellt
- fsx-lustre-copy-tagszu Backups
- fsx-meets-restore-time-Ziel
- fsx-ontap-deployment-type-überprüfen
- fsx-openzfs-copy-tags-aktiviert
- fsx-openzfs-deployment-type-überprüfen
- fsx-resources-protected-by-Ersatzplan
- fsx-windows-audit-log-konfiguriert
- fsx-windows-deployment-type-überprüfen
- glue-job-logging-enabled
- glue-ml-transform-encrypted-im Ruhezustand
- glue-spark-job-supported-Ausführung
- GuardDuty-EC2- protection-runtime-enabled

- guardduty-ecs-protection-runtime-aktiviert
- guardduty-eks-protection-audit-aktiviert
- guardduty-eks-protection-runtime-aktiviert
- guardduty-enabled-centralized
- guardduty-lambda-protection-enabled
- guardduty-malware-protection-enabled
- guardduty-non-archived-findings
- guardduty-rds-protection-enabled
- guardduty-runtime-monitoring-enabled
- GuardDuty-S3-Schutz aktiviert
- iam-external-access-analyzer-aktiviert
- iam-password-policy
- incoming-ssh-disabled
- instances-in-vpc
- internet-gateway-authorized-vpc-nur
- iot-authorizer-token-signing-aktiviert
- kinesis-firehose-delivery-stream-verschlüsselt
- kinesis-stream-backup-retention-überprüfen
- kinesis-stream-encrypted
- kms-cmk-not-scheduled-zum Löschen
- kms-key-policy-no-öffentlicher Zugang
- lambda-concurrency-check
- lambda-dlq-check
- lambda-function-public-access-verboten
- lambda-function-settings-check
- lambda-inside-vpc
- lambda-vpc-multi-az-überprüfen
- mariadb-publish-logs-to-cloudwatch-Protokolle
- mq-active-broker-ldap-Authentifizierung
- mq-active-deployment-mode

- mq-active-single-instance-broker-storage-type-efs
- mq-auto-minor-version-Upgrade aktiviert
- mq-broker-general-logging-aktiviert
- mq-cloudwatch-audit-log-aktiviert
- mq-rabbit-deployment-mode
- msk-enhanced-monitoring-enabled
- msk-in-cluster-node-require-tls
- multi-region-cloud-trail-aktiviert
- nacl-no-unrestricted-ssh-rdp
- neptune-cluster-backup-retention-überprüfen
- neptune-cluster-cloudwatch-log-exportfähig
- neptune-cluster-copy-tags-to-snapshot-enabled
- neptune-cluster-deletion-protection-aktiviert
- neptune-cluster-encrypted
- neptune-cluster-iam-database-Authentifizierung
- neptune-cluster-multi-az-aktiviert
- neptune-cluster-snapshot-encrypted
- neptune-cluster-snapshot-public-verboten
- netfw-deletion-protection-enabled
- netfw-logging-enabled
- netfw-multi-az-enabled
- netfw-policy-default-action-fragment-Pakete
- netfw-policy-default-action-vollständige Pakete
- netfw-policy-rule-group-assoziiert
- netfw-stateless-rule-group-nicht leer
- netfw-subnet-change-protection-aktiviert
- nlb-internal-scheme-check
- nlb-logging-enabled
- no-unrestricted-route-to-igw
- rabbit-mq-supported-version

- rds-aurora-mysql-audit-Protokollierung aktiviert
- rds-aurora-postgresql-logs-zu-Cloud-Watch
- rds-automatic-minor-version-upgrade-fähig
- rds-cluster-default-admin-überprüfen
- rds-cluster-deletion-protection-aktiviert
- rds-cluster-encrypted-at-ausruhen
- rds-cluster-iam-authentication-aktiviert
- rds-cluster-multi-az-aktiviert
- rds-enhanced-monitoring-enabled
- rds-instance-default-admin-überprüfen
- rds-instance-deletion-protection-aktiviert
- rds-instance-iam-authentication-aktiviert
- rds-instance-public-access-überprüfen
- rds-instance-subnet-igw-überprüfen
- rds-in-backup-plan
- rds-last-backup-recovery-Punkt erstellt
- rds-logging-enabled
- rds-mariadb-instance-encryptedim Transit
- rds-meets-restore-time-Ziel
- rds-multi-az-support
- rds-mysql-instance-encryptedunterwegs
- rds-postgresql-logs-to- Cloudwatch
- rds-postgres-instance-encryptedauf dem Weg
- rds-proxy-tls-encryption
- rds-resources-protected-by-Ersatzplan
- rds-snapshots-public-prohibited
- rds-snapshot-encrypted
- rds-sqlserver-encrypted-in-Transit
- rds-sql-server-logszur Cloud-Überwachung
- rds-storage-encrypted

- redshift-backup-enabled
- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check
- redshift-cluster-parameter-group-markiert
- redshift-cluster-public-access-überprüfen
- redshift-cluster-subnet-group-Multi-Az
- redshift-default-admin-check
- redshift-default-db-name-überprüfen
- redshift-enhanced-vpc-routing-aktiviert
- redshift-require-tls-ssl
- redshift-serverless-default-admin-überprüfen
- redshift-serverless-default-db-Namenscheck
- redshift-serverless-namespace-cmk-Verschlüsselung
- redshift-serverless-publish-logs-zu-Cloud-Watch
- redshift-serverless-workgroup-no-öffentlicher Zugang
- redshift-unrestricted-port-access
- required-tags
- restricted-incoming-traffic
- nur s3- access-point-in-vpc
- s3- -Blöcke access-point-public-access
- s3- -Blöcke account-level-public-access
- s3- -Blocke-periodisch account-level-public-access
- s 3- bucket-acl-prohibited
- s-3 bucket-blacklisted-actions-prohibited
- s3- bucket-cross-region-replication -aktiviert
- s-3 bucket-default-lock-enabled
- s3 bucket-level-public-access - verboten
- s3- bucket-logging-enabled
- s-3 bucket-mfa-delete-enabled
- s-3 bucket-policy-grantee-check

- s3- bucket-policy-not-more -freizügig
- s 3- bucket-public-read-prohibited
- s-3 bucket-public-write-prohibited
- s-3 bucket-replication-enabled
- s3- bucket-server-side-encryption -aktiviert
- s-3 bucket-ssl-requests-only
- s3-Bucket-Tag
- s-3 bucket-versioning-enabled
- s-3 default-encryption-kms
- s-3 event-notifications-enabled
- s3 last-backup-recovery-point - erstellt
- s3- lifecycle-policy-check
- s-3 meets-restore-time-target
- resources-protected-by-backups3-plan
- s 3- version-lifecycle-policy-check
- sagemaker-app-image-config-markiert
- sagemaker-endpoint-configuration-kms-schlüsselkonfiguriert
- sagemaker-endpoint-config-prod-Anzahl der Instanzen
- sagemaker-image-description
- sagemaker-image-tagged
- sagemaker-notebook-instance-kms-key-konfiguriert
- sagemaker-notebook-instance-platform-Version
- sagemaker-notebook-no-direct-Internetzugang
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-überprüfen
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- securityhub-enabled
- security-account-information-provided

- service-catalog-shared-within-Organisation
- service-vpc-endpoint-enabled
- sns-encrypted-kms
- sns-topic-no-public-Zugang
- ssm-document-not-public
- ssm-document-tagged
- step-functions-state-machine-Protokollierung aktiviert
- storagegateway-last-backup-recovery-punkt-erstellt
- storagegateway-resources-in-logically-air-gapped-vault
- storagegateway-resources-protected-by-Ersatzplan
- subnet-auto-assign-public-ip-deaktiviert
- transfer-agreement-description
- transfer-agreement-tagged
- transfer-certificate-description
- transfer-certificate-tagged
- transfer-connector-logging-enabled
- transfer-connector-tagged
- transfer-family-server-no-ftp
- transfer-profile-tagged
- transfer-workflow-description
- transfer-workflow-tagged
- vpc-default-security-group-geschlossen
- vpc-endpoint-enabled
- vpc-flow-logs-enabled
- vpc-network-acl-unused-überprüfen
- vpc-sg-open-only-to-authorized-ports
- vpc-sg-port-restriction-überprüfen
- vpc-vpn-2-tunnels-up
- wafv2-logging-enabled
- WAF 2- rulegroup-logging-enabled

- waf-regional-rule-not-leer
- waf-regional-webacl-not-leer

Region Südamerika (São Paulo)

Südamerika (São Paulo)

- access-keys-rotated
- account-part-of-organizations
- acmpca-certificate-authority-tagged
- acm-certificate-expiration-check
- acm-certificate-rsa-check
- acm-pca-root-ca-deaktiviert
- active-mq-supported-version
- alb-desync-mode-check
- alb-http-drop-invalid-Header-fähig
- alb-http-to-https-Umleitungsprüfung
- alb-internal-scheme-check
- alb-listener-tagged
- alb-waf-enabled
- amplify-app-branch-auto-löschung aktiviert
- amplify-app-description
- amplify-app-tagged
- amplify-branch-performance-mode-aktiviert
- amplify-branch-tagged
- api-gwv2- access-logs-enabled
- api-gwv2- authorization-type-configured
- api-gw-associated-with-WAF
- api-gw-cache-enabled-und-verschlüsselt
- api-gw-endpoint-type-überprüfen
- api-gw-execution-logging-aktiviert
- api-gw-ssl-enabled

- api-gw-xray-enabled
- appconfig-application-description
- appconfig-application-tagged
- appconfig-configuration-profile-tagged
- appconfig-configuration-profile-validators-nicht leer
- appconfig-deployment-strategy-description
- appconfig-deployment-strategy-replicate-zu-ssm
- appconfig-environment-description
- appconfig-environment-tagged
- appconfig-extension-association-tagged
- appconfig-freeform-profile-config-Speicher
- appconfig-hosted-configuration-version-Beschreibung
- appflow-flow-tagged
- appmesh-gateway-route-tagged
- appmesh-mesh-deny-tcp-Weiterleitung
- appmesh-mesh-tagged
- appmesh-route-tagged
- appmesh-virtual-gateway-backend-Standardeinstellungen-TLS
- appmesh-virtual-gateway-logging-file-path-exists
- appmesh-virtual-gateway-tagged
- appmesh-virtual-node-backend-defaults-tls-on
- appmesh-virtual-node-logging-file-path-exists
- appmesh-virtual-node-tagged
- appmesh-virtual-router-tagged
- appmesh-virtual-service-tagged
- approved-amis-by-id
- approved-amis-by-tag
- appsync-associated-with-waf
- appsync-authorization-check
- appsync-cache-ct-encryption-im Ruhezustand

- appsync-cache-ct-encryptionunterwegs
- appsync-cache-encryption-at-ausruhen
- appsync-logging-enabled
- athena-data-catalog-description
- athena-prepared-statement-description
- athena-workgroup-description
- athena-workgroup-encrypted-at-ausruhen
- athena-workgroup-enforce-workgroup-Konfiguration
- athena-workgroup-engine-version-automatisches Upgrade
- athena-workgroup-logging-enabled
- aurora-last-backup-recovery-Punkt erstellt
- aurora-meets-restore-time-Ziel
- aurora-mysql-cluster-audit-Protokollierung
- aurora-resources-in-logically-air-gapped-vault
- aurora-resources-protected-by-Backup-Plan
- autoscaling-capacity-rebalancing
- autoscaling-group-elb-healthcheck-erforderlich
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-hop-Grenze
- autoscaling-launch-config-public-ip-deaktiviert
- autoscaling-launch-template
- autoscaling-multiple-az
- autoscaling-multiple-instance-types
- backup-plan-min-frequency-and-min-retention-check
- backup-recovery-point-encrypted
- backup-recovery-point-manual-Löschen-deaktiviert
- backup-recovery-point-minimum-Aufbewahrungsprüfung
- batch-compute-environment-enabled
- batch-compute-environment-managed
- batch-compute-environment-tagged

- batch-job-queue-enabled
- batch-job-queue-tagged
- batch-managed-compute-environment-using-launch-template
- batch-managed-compute-env-compute-resources-tagged
- batch-scheduling-policy-tagged
- beanstalk-enhanced-health-reporting-aktiviert
- cassandra-keyspace-tagged
- clb-desync-mode-check
- clb-multiple-az
- cloudformation-stack-drift-detection-überprüfen
- cloudformation-stack-notification-check
- cloudtrail-all-read-s3- data-event-check
- cloudtrail-all-write-s3- data-event-check
- Wolkenspur-S3- bucket-access-logging
- cloudtrail-s3- bucket-public-access-prohibited
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-action-enabled-überprüfen
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted
- cloud-trail-cloud-watch-logs-aktiviert
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-Validierung aktiviert
- cmk-backing-key-rotation-aktiviert
- codebuild-project-artifact-encryption
- codebuild-project-environment-privileged-überprüfen
- codebuild-project-envvar-awscred-überprüfen

- codebuild-project-logging-enabled
- codebuild-project-s3-log-verschlüsselt
- codebuild-project-source-repo-URL-Prüfung
- codebuild-report-group-encrypted-im Ruhezustand
- codedeploy-auto-rollback-monitor-aktiviert
- codedeploy-deployment-group-auto-rollback-aktiviert
- codedeploy-deployment-group-outdated-instanzen-aktualisieren
- Codedeploy-ec2- minimum-healthy-hosts-configured
- codedeploy-lambda-allatonce-traffic-shift-deaktiviert
- codepipeline-deployment-count-check
- codepipeline-region-fanout-check
- cognito-identity-pool-unauth-Zugriffsprüfung
- cognito-user-pool-advanced-sicherheitsaktiviert
- cognito-user-pool-tagged
- custom-eventbus-policy-attached
- custom-schema-registry-policy-angehängt
- cw-loggroup-retention-period-überprüfen
- datasync-task-data-verification-aktiviert
- datasync-task-logging-enabled
- datasync-task-tagged
- dax-encryption-enabled
- dax-tls-endpoint-encryption
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- dms-auto-minor-version-aktualisieren-Prüfung
- dms-endpoint-ssl-configured
- dms-endpoint-tagged
- dms-mongo-db-authentication-aktiviert
- dms-neptune-iam-authorization-aktiviert

- dms-redis-tls-enabled
- dms-replication-not-public
- dms-replication-task-sourcedb-Protokollierung
- dms-replication-task-tagged
- dms-replication-task-targetdb-Protokollierung
- docdb-cluster-audit-logging-aktiviert
- docdb-cluster-backup-retention-überprüfen
- docdb-cluster-deletion-protection-aktiviert
- docdb-cluster-encrypted
- docdb-cluster-encrypted-in-Transit
- docdb-cluster-snapshot-public-verboten
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-last-backup-recovery-Punkt erstellt
- dynamodb-meets-restore-time-Ziel
- dynamodb-pitr-enabled
- dynamodb-resources-protected-by-Ersatzplan
- dynamodb-table-deletion-protection-aktiviert
- dynamodb-table-encrypted-kms
- dynamodb-table-encryption-enabled
- dynamodb-throughput-limit-check
- ebs-in-backup-plan
- ebs-last-backup-recovery-punkt-erstellt
- ebs-meets-restore-time-Ziel
- ebs-optimized-instance
- ebs-resources-in-logically-air-gapped-vault
- ebs-resources-protected-by-Ersatzplan
- ebs-snapshot-public-restorable-überprüfen
- ec2- capacity-reservation-tagged
- ec2- aktiviert client-vpn-connection-log

- ec2- client-vpn-endpoint-tagged
- ec2- -alle client-vpn-not-authorize
- ec2- dhcp-options-tagged
- ec2- ebs-encryption-by-default
- ec2- aktiviert enis-source-destination-check
- ec2-fleet-markiert
- ec2-imdsv2-check
- ec2- instance-detailed-monitoring-enabled
- ec2-ami instance-launched-with-allowed
- ec2- instance-managed-by-ssm
- ec2- instance-multiple-eni-check
- ec2- instance-no-public-ip
- ec2- instance-profile-attached
- ec2- erstellt last-backup-recovery-point
- ec2-2-prüfen launch-template-imdsv
- ec2- -deaktiviert launch-template-public-ip
- ec2- launch-template-tagged
- ec2- managedinstance-applications-blacklisted
- ec2- managedinstance-applications-required
- ec2- prüfen managedinstance-association-compliance-status
- ec2- managedinstance-inventory-blacklisted
- ec2- prüfen managedinstance-patch-compliance-status
- ec2- managedinstance-platform-check
- ec2- meets-restore-time-target
- ec2- Analyse mit Schlagwörtern network-insights-access-scope
- ec2 network-insights-access-scope - markiert
- ec2- network-insights-path-tagged
- ec2- no-amazon-key-pair
- ec2- paravirtual-instance-check
- ec2- prefix-list-tagged

- ec2- -Tresor mit Lücken resources-in-logically-air
- ec2- resources-protected-by-backup -plan
- ec2- -eni security-group-attached-to
- ec2- -eni-periodisch security-group-attached-to
- ec2-stopped-instance
- ec2- token-hop-limit-check
- ec2- traffic-mirror-filter-description
- ec2- traffic-mirror-filter-tagged
- ec2- traffic-mirror-session-description
- ec2- traffic-mirror-session-tagged
- ec2- traffic-mirror-target-description
- ec2- traffic-mirror-target-tagged
- ec2- -attach-deaktiviert transit-gateway-auto-vpc
- ec2 transit-gateway-multicast-domain - markiert
- ec2- volume-inuse-check
- ec2- vpn-connection-logging-enabled
- ecr-private-image-scanning-aktiviert
- ecr-private-lifecycle-policy-konfiguriert
- ecr-private-tag-immutability-aktiviert
- ecr-repository-cmk-encryption-aktiviert
- ecr-repository-tagged
- ecs-awsvpc-networking-enabled
- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-container-insights-enabled
- ecs-fargate-latest-platform-Version
- ecs-no-environment-secrets
- ecs-task-definition-log-Konfiguration
- ecs-task-definition-memory-hartes Limit
- ecs-task-definition-network-mode-not-host

- ecs-task-definition-nonroot-Benutzer
- ecs-task-definition-pid-Modus-Check
- ecs-task-definition-user-for-host-mode-check
- efs-access-point-enforce-Stammverzeichnis
- efs-access-point-enforce-Benutzeridentität
- efs-automatic-backups-enabled
- efs-encrypted-check
- efs-filesystem-ct-encrypted
- efs-in-backup-plan
- efs-last-backup-recovery-Punkt erstellt
- efs-meets-restore-time-Ziel
- efs-mount-target-public-zugänglich
- efs-resources-in-logically-air-gapped-vault
- efs-resources-protected-by-Ersatzplan
- eip-attached
- eks-cluster-logging-enabled
- eks-cluster-log-enabled
- eks-cluster-oldest-supported-Ausführung
- eks-cluster-secrets-encrypted
- eks-cluster-supported-version
- eks-endpoint-no-public-Zugang
- eks-secrets-encrypted
- elasticache-auto-minor-version-Upgrade-Check
- elasticache-rbac-auth-enabled
- elasticache-redis-cluster-automatic-Backup-Check
- elasticache-repl-grp-auto-failover-fähig
- elasticache-repl-grp-encrypted-im Ruhezustand
- elasticache-repl-grp-encryptedunterwegs
- elasticache-repl-grp-redis-auth-aktiviert
- elasticache-subnet-group-check

- elasticache-supported-engine-version
- elasticbeanstalk-application-description
- elasticbeanstalk-application-version-description
- elasticbeanstalk-environment-description
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch
- elasticsearch-node-to-node-Verschlüsselungsprüfung
- elastic-beanstalk-logs-to- Cloudwatch
- elastic-beanstalk-managed-updates-aktiviert
- elbv2- acm-certificate-required
- elv 2- listener-encryption-in-transit
- elbv2-multiple-az
- elbv2- prüfen predefined-security-policy-ssl
- elb-acm-certificate-required
- elb-cross-zone-load-Balancing aktiviert
- elb-custom-security-policy-ssl-Prüfung
- elb-deletion-protection-enabled
- elb-logging-enabled
- elb-predefined-security-policy-ssl-Überprüfung
- elb-tls-https-listeners-nur
- emr-block-public-access
- emr-kerberos-enabled
- emr-master-no-public-ip
- emr-security-configuration-encryption-ausruhen
- emr-security-configuration-encryption-Transit
- encrypted-volumes
- event-data-store-cmk-Verschlüsselung aktiviert
- fis-experiment-template-log-Konfiguration ist vorhanden
- fis-experiment-template-tagged

- fms-shield-resource-policy-überprüfen
- fms-webacl-resource-policy-überprüfen
- fms-webacl-rulegroup-association-überprüfen
- fsx-last-backup-recovery-Punkt erstellt
- fsx-lustre-copy-tagszu Backups
- fsx-meets-restore-time-Ziel
- fsx-ontap-deployment-type-überprüfen
- fsx-openzfs-copy-tags-aktiviert
- fsx-openzfs-deployment-type-überprüfen
- fsx-resources-protected-by-Backup-Plan
- fsx-windows-audit-log-konfiguriert
- fsx-windows-deployment-type-überprüfen
- glb-listener-tagged
- global-endpoint-event-replication-aktiviert
- glue-job-logging-enabled
- glue-ml-transform-encrypted-im Ruhezustand
- glue-spark-job-supported-Ausführung
- GuardDuty-EC2- protection-runtime-enabled
- guardduty-ecs-protection-runtime-aktiviert
- guardduty-eks-protection-audit-aktiviert
- guardduty-eks-protection-runtime-aktiviert
- guardduty-enabled-centralized
- guardduty-lambda-protection-enabled
- guardduty-malware-protection-enabled
- guardduty-non-archived-findings
- guardduty-rds-protection-enabled
- guardduty-runtime-monitoring-enabled
- GuardDuty-S3-Schutz aktiviert
- iam-customer-policy-blocked-kms-Aktionen
- iam-external-access-analyzer-aktiviert

- iam-group-has-users-überprüfen
- iam-inline-policy-blocked-kms-Aktionen
- iam-no-inline-policy-überprüfen
- iam-password-policy
- iam-policy-blacklisted-check
- iam-policy-in-use
- iam-policy-no-statements-with-admin-access
- iam-policy-no-statements-with-full-access
- iam-role-managed-policy-überprüfen
- iam-root-access-key-überprüfen
- iam-user-group-membership-überprüfen
- iam-user-mfa-enabled
- iam-user-no-policies-überprüfen
- iam-user-unused-credentials-überprüfen
- incoming-ssh-disabled
- inspector-ec2-Scan aktiviert
- inspector-ecr-scan-enabled
- inspector-lambda-standard-scan-aktiviert
- instances-in-vpc
- internet-gateway-authorized-vpc-nur
- iotwireless-fuota-task-tagged
- iotwireless-multicast-group-tagged
- iotwireless-service-profile-tagged
- iot-authorizer-token-signing-aktiviert
- kinesis-firehose-delivery-stream-verschlüsselt
- kinesis-stream-backup-retention-überprüfen
- kinesis-stream-encrypted
- kms-cmk-not-scheduled-zum Löschen
- kms-key-policy-no-öffentlicher Zugang
- lambda-concurrency-check

- lambda-dlq-check
- lambda-function-public-access-verboten
- lambda-function-settings-check
- lambda-function-xray-enabled
- lambda-inside-vpc
- lambda-vpc-multi-az-überprüfen
- macie-auto-sensitive-data-Discovery-Check
- macie-status-check
- mariadb-publish-logs-to-Cloudwatch-Protokolle
- mfa-enabled-for-iam-Konsolenzugriff
- mq-active-broker-ldap-Authentifizierung
- mq-active-deployment-mode
- mq-active-single-instance-broker-storage-type-efs
- mq-automatic-minor-version-Upgrade aktiviert
- mq-auto-minor-version-upgrade-fähig
- mq-broker-general-logging-aktiviert
- mq-cloudwatch-audit-logging-aktiviert
- mq-cloudwatch-audit-log-aktiviert
- mq-no-public-access
- mq-rabbit-deployment-mode
- msk-cluster-public-access-deaktiviert
- msk-connect-connector-logging-aktiviert
- msk-enhanced-monitoring-enabled
- msk-in-cluster-node-require-tls
- msk-unrestricted-access-check
- multi-region-cloud-trail-aktiviert
- nacl-no-unrestricted-ssh-rdp
- neptune-cluster-backup-retention-überprüfen
- neptune-cluster-cloudwatch-log-exportfähig
- neptune-cluster-copy-tags-to-snapshot-enabled

- neptune-cluster-deletion-protection-aktiviert
- neptune-cluster-encrypted
- neptune-cluster-iam-database-Authentifizierung
- neptune-cluster-multi-az-aktiviert
- neptune-cluster-snapshot-encrypted
- neptune-cluster-snapshot-public-verboten
- netfw-deletion-protection-enabled
- netfw-logging-enabled
- netfw-multi-az-enabled
- netfw-policy-default-action-fragment-Pakete
- netfw-policy-default-action-vollständige Pakete
- netfw-policy-rule-group-assoziiert
- netfw-stateless-rule-group-nicht leer
- netfw-subnet-change-protection-aktiviert
- nlb-cross-zone-load-Balancing aktiviert
- nlb-internal-scheme-check
- nlb-listener-tagged
- nlb-logging-enabled
- no-unrestricted-route-to-igw
- opensearch-access-control-enabled
- opensearch-audit-logging-enabled
- opensearch-data-node-fault-Toleranz
- opensearch-encrypted-at-rest
- opensearch-https-required
- opensearch-in-vpc-only
- opensearch-logs-to-cloudwatch
- opensearch-node-to-node-Verschlüsselungsprüfung
- opensearch-primary-node-fault-Toleranz
- opensearch-update-check
- rabbit-mq-supported-version

- rds-aurora-mysql-audit-Protokollierung aktiviert
- rds-aurora-postgresql-logs-zu-Cloud-Watch
- rds-automatic-minor-version-upgrade-fähig
- rds-cluster-auto-minor-version-upgrade-enable
- rds-cluster-default-admin-überprüfen
- rds-cluster-deletion-protection-aktiviert
- rds-cluster-encrypted-at-ausruhen
- rds-cluster-iam-authentication-aktiviert
- rds-cluster-multi-az-aktiviert
- rds-db-security-group-nicht erlaubt
- rds-enhanced-monitoring-enabled
- rds-instance-default-admin-überprüfen
- rds-instance-deletion-protection-aktiviert
- rds-instance-iam-authentication-aktiviert
- rds-instance-public-access-überprüfen
- rds-instance-subnet-igw-überprüfen
- rds-in-backup-plan
- rds-last-backup-recovery-Punkt erstellt
- rds-logging-enabled
- rds-mariadb-instance-encryptedim Transit
- rds-meets-restore-time-Ziel
- rds-multi-az-support
- rds-mysql-instance-encryptedim Transit
- rds-postgresql-logs-to- Cloudwatch
- rds-postgres-instance-encryptedauf dem Weg
- rds-proxy-tls-encryption
- rds-resources-protected-by-Ersatzplan
- rds-snapshots-public-prohibited
- rds-snapshot-encrypted
- rds-sqlserver-encrypted-in-Transit

- rds-sql-server-logszur Cloud-Überwachung
- rds-storage-encrypted
- redshift-audit-logging-enabled
- redshift-backup-enabled
- redshift-cluster-configuration-check
- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check
- redshift-cluster-multi-az-aktiviert
- redshift-cluster-parameter-group-markiert
- redshift-cluster-public-access-überprüfen
- redshift-cluster-subnet-group-Multi-Az
- redshift-default-admin-check
- redshift-default-db-name-überprüfen
- redshift-enhanced-vpc-routing-aktiviert
- redshift-require-tls-ssl
- redshift-serverless-default-admin-überprüfen
- redshift-serverless-default-db-Namenscheck
- redshift-serverless-namespace-cmk-Verschlüsselung
- redshift-serverless-publish-logs-zu-Cloud-Watch
- redshift-serverless-workgroup-no-öffentlicher Zugang
- redshift-unrestricted-port-access
- required-tags
- restricted-incoming-traffic
- root-account-hardware-mfa-aktiviert
- root-account-mfa-enabled
- nur s3- access-point-in-vpc
- s3- -Blöcke access-point-public-access
- s3- -Blöcke account-level-public-access
- s3- -Blocke-periodisch account-level-public-access
- s 3- bucket-acl-prohibited

- s-3 bucket-blacklisted-actions-prohibited
- s3- bucket-cross-region-replication -aktiviert
- s-3 bucket-default-lock-enabled
- s3 bucket-level-public-access - verboten
- s3- bucket-logging-enabled
- s-3 bucket-mfa-delete-enabled
- s-3 bucket-policy-grantee-check
- s3- bucket-policy-not-more -freizügig
- s 3- bucket-public-read-prohibited
- s-3 bucket-public-write-prohibited
- s-3 bucket-replication-enabled
- s3- bucket-server-side-encryption -aktiviert
- s-3 bucket-ssl-requests-only
- s3-Bucket-Tag
- s-3 bucket-versioning-enabled
- s-3 default-encryption-kms
- s-3 event-notifications-enabled
- s3 last-backup-recovery-point - erstellt
- s3- lifecycle-policy-check
- s-3 meets-restore-time-target
- s3- resources-in-logically-air -Tresor mit Lücken
- s3 resources-protected-by-backup - -Plan
- s 3- version-lifecycle-policy-check
- sagemaker-app-image-config-markiert
- sagemaker-domain-in-vpc
- sagemaker-domain-tagged
- sagemaker-endpoint-configuration-kms-schlüsselkonfiguriert
- sagemaker-endpoint-config-prod-Anzahl der Instanzen
- sagemaker-feature-group-tagged
- sagemaker-image-description

- sagemaker-image-tagged
- sagemaker-model-in-vpc
- sagemaker-model-isolation-enabled
- sagemaker-notebook-instance-inside-vpc
- sagemaker-notebook-instance-kms-key-konfiguriert
- sagemaker-notebook-instance-platform-Version
- sagemaker-notebook-instance-root-Zugriffsprüfung
- sagemaker-notebook-no-direct-Internetzugang
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-überprüfen
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- securityhub-enabled
- security-account-information-provided
- service-catalog-shared-within-Organisation
- service-vpc-endpoint-enabled
- sns-encrypted-kms
- sns-topic-message-delivery-Benachrichtigung aktiviert
- sns-topic-no-public-Zugriff
- sqs-queue-no-public-Zugang
- ssm-automation-block-public-teilen
- ssm-automation-logging-enabled
- ssm-document-not-public
- ssm-document-tagged
- step-functions-state-machine-Protokollierung aktiviert
- storagegateway-last-backup-recovery-punkt-erstellt
- storagegateway-resources-in-logically-air-gapped-vault
- storagegateway-resources-protected-by-Ersatzplan
- subnet-auto-assign-public-ip-deaktiviert

- transfer-agreement-description
- transfer-agreement-tagged
- transfer-certificate-description
- transfer-certificate-tagged
- transfer-connector-logging-enabled
- transfer-connector-tagged
- transfer-family-server-no-ftp
- transfer-profile-tagged
- transfer-workflow-description
- transfer-workflow-tagged
- virtualmachine-last-backup-recovery-punkt-erstellt
- virtualmachine-resources-in-logically-air-gapped-vault
- virtualmachine-resources-protected-by-Ersatzplan
- vpc-default-security-group-geschlossen
- vpc-endpoint-enabled
- vpc-flow-logs-enabled
- vpc-network-acl-unused-überprüfen
- vpc-peering-dns-resolution-überprüfen
- vpc-sg-open-only-to-authorized-ports
- vpc-sg-port-restriction-überprüfen
- vpc-vpn-2-tunnels-up
- wafv2-logging-enabled
- WAF 2- rulegroup-logging-enabled
- WAF 2- rulegroup-not-empty
- WAF 2- webacl-not-empty
- waf-regional-rulegroup-not-leer
- waf-regional-rule-not-leer
- waf-regional-webacl-not-leer
- workspaces-root-volume-encryption-aktiviert
- workspaces-user-volume-encryption-aktiviert

AWS GovCloud Region (USA-Ost)

AWS GovCloud (US-Ost)

- access-keys-rotated
- account-part-of-organizations
- acm-certificate-expiration-check
- active-mq-supported-version
- alb-desync-mode-check
- alb-http-drop-invalid-Header-fähig
- alb-http-to-https-Umleitungsprüfung
- alb-waf-enabled
- api-gw-associated-with-WAF
- api-gw-cache-enabled-und-verschlüsselt
- api-gw-endpoint-type-überprüfen
- api-gw-execution-logging-aktiviert
- api-gw-ssl-enabled
- api-gw-xray-enabled
- approved-amis-by-id
- approved-amis-by-tag
- athena-workgroup-logging-enabled
- aurora-last-backup-recovery-punkt-erstellt
- aurora-mysql-cluster-audit-Protokollierung
- aurora-resources-protected-by-Backup-Plan
- autoscaling-group-elb-healthcheck-erforderlich
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-public-ip-deaktiviert
- autoscaling-multiple-instance-types
- backup-plan-min-frequency-and-min-retention-check
- backup-recovery-point-encrypted
- backup-recovery-point-manual-Löschen-deaktiviert
- backup-recovery-point-minimum-Aufbewahrungsprüfung

- beanstalk-enhanced-health-reporting-aktiviert
- clb-desync-mode-check
- cloudformation-stack-drift-detection-überprüfen
- cloudformation-stack-notification-check
- cloudtrail-all-read-s3- data-event-check
- cloudtrail-all-write-s3- data-event-check
- Wolkenspur-S3- bucket-access-logging
- cloudtrail-s3- bucket-public-access-prohibited
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted
- cloud-trail-cloud-watch-logs-aktiviert
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-Validierung aktiviert
- cmk-backing-key-rotation-aktiviert
- codebuild-project-environment-privileged-überprüfen
- codebuild-project-envvar-awscred-überprüfen
- codebuild-project-logging-enabled
- codebuild-project-s3-log-verschlüsselt
- codebuild-project-source-repo-URL-Prüfung
- codebuild-report-group-encrypted-im Ruhezustand
- cw-loggroup-retention-period-überprüfen
- datasync-task-logging-enabled
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type

- dms-mongo-db-authentication-aktiviert
- dms-neptune-iam-authorization-aktiviert
- dms-redis-tls-enabled
- dms-replication-not-public
- docdb-cluster-encrypted-in-Transit
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-last-backup-recovery-Punkt erstellt
- dynamodb-pitr-enabled
- dynamodb-resources-protected-by-Ersatzplan
- dynamodb-table-deletion-protection-aktiviert
- dynamodb-table-encrypted-kms
- dynamodb-table-encryption-enabled
- dynamodb-throughput-limit-check
- ebs-in-backup-plan
- ebs-last-backup-recovery-punkt-erstellt
- ebs-optimized-instance
- ebs-resources-protected-by-Ersatzplan
- ebs-snapshot-public-restorable-überprüfen
- ec2- aktiviert client-vpn-connection-log
- ec2- ebs-encryption-by-default
- ec2- aktiviert enis-source-destination-check
- ec2-imdsv2-check
- ec2- instance-detailed-monitoring-enabled
- ec2-ami instance-launched-with-allowed
- ec2- instance-managed-by-ssm
- ec2- instance-multiple-eni-check
- ec2- instance-no-public-ip
- ec2- instance-profile-attached
- ec2- erstellt last-backup-recovery-point

- ec2- managedinstance-applications-blacklisted
- ec2- managedinstance-applications-required
- ec2- prüfen managedinstance-association-compliance-status
- ec2- managedinstance-inventory-blacklisted
- ec2- prüfen managedinstance-patch-compliance-status
- ec2- managedinstance-platform-check
- ec2-plan resources-protected-by-backup
- ec2- -eni security-group-attached-to
- ec2-stopped-instance
- ec2- volume-inuse-check
- ec2- vpn-connection-logging-enabled
- ecr-private-image-scanning-aktiviert
- ecr-private-lifecycle-policy-konfiguriert
- ecr-private-tag-immutability-aktiviert
- ecr-repository-cmk-encryption-aktiviert
- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-container-insights-enabled
- ecs-fargate-latest-platform-Version
- ecs-task-definition-network-mode-not-host
- ecs-task-definition-user-for-host-mode-check
- efs-access-point-enforce-Benutzeridentität
- efs-automatic-backups-enabled
- efs-encrypted-check
- efs-filesystem-ct-encrypted
- efs-in-backup-plan
- efs-last-backup-recovery-Punkt erstellt
- efs-mount-target-public-zugänglich
- efs-resources-protected-by-Ersatzplan
- eip-attached

- eks-cluster-secrets-encrypted
- eks-cluster-supported-version
- eks-endpoint-no-public-Zugang
- eks-secrets-encrypted
- elasticache-redis-cluster-automatic-Backup-Check
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch
- elasticsearch-node-to-node-Verschlüsselungsprüfung
- elastic-beanstalk-managed-updates-aktiviert
- elbv2- listener-encryption-in-transit
- elbv2- -prüfen predefined-security-policy-ssl
- elb-acm-certificate-required
- elb-cross-zone-load-Balancing aktiviert
- elb-custom-security-policy-ssl-Prüfung
- elb-deletion-protection-enabled
- elb-logging-enabled
- elb-predefined-security-policy-ssl-Überprüfung
- elb-tls-https-listeners-nur
- emr-kerberos-enabled
- emr-master-no-public-ip
- encrypted-volumes
- event-data-store-cmk-Verschlüsselung aktiviert
- fms-shield-resource-policy-überprüfen
- fms-webacl-resource-policy-überprüfen
- fms-webacl-rulegroup-association-überprüfen
- fsx-last-backup-recovery-Punkt erstellt
- fsx-ontap-deployment-type-überprüfen
- fsx-openzfs-deployment-type-überprüfen
- fsx-resources-protected-by-Backup-Plan

- fsx-windows-deployment-type-überprüfen
- glue-job-logging-enabled
- glue-spark-job-supported-Ausführung
- guardduty-eks-protection-audit-aktiviert
- guardduty-enabled-centralized
- guardduty-lambda-protection-enabled
- guardduty-non-archived-findings
- GuardDuty-S3-Schutz aktiviert
- iam-customer-policy-blocked-kms-Aktionen
- iam-group-has-users-überprüfen
- iam-inline-policy-blocked-kms-Aktionen
- iam-no-inline-policy-überprüfen
- iam-password-policy
- iam-policy-blacklisted-check
- iam-policy-in-use
- iam-policy-no-statements-with-admin-access
- iam-policy-no-statements-with-full-access
- iam-role-managed-policy-überprüfen
- iam-root-access-key-überprüfen
- iam-user-group-membership-überprüfen
- iam-user-mfa-enabled
- iam-user-no-policies-überprüfen
- iam-user-unused-credentials-überprüfen
- incoming-ssh-disabled
- inspector-ec2-Scan aktiviert
- inspector-ecr-scan-enabled
- inspector-lambda-standard-scan-aktiviert
- instances-in-vpc
- internet-gateway-authorized-vpc-nur
- kinesis-firehose-delivery-stream-verschlüsselt

- kinesis-stream-backup-retention-überprüfen
- kinesis-stream-encrypted
- kms-cmk-not-scheduled-zum Löschen
- lambda-concurrency-check
- lambda-dlq-check
- lambda-function-public-access-verboten
- lambda-function-settings-check
- lambda-function-xray-enabled
- lambda-inside-vpc
- mariadb-publish-logs-to-cloudwatch-Protokolle
- mfa-enabled-for-iam-Konsolenzugriff
- mq-cloudwatch-audit-log-aktiviert
- msk-cluster-public-access-deaktiviert
- msk-unrestricted-access-check
- multi-region-cloud-trail-aktiviert
- nacl-no-unrestricted-ssh-rdp
- netfw-policy-rule-group-assoziiert
- netfw-stateless-rule-group-nicht leer
- netfw-subnet-change-protection-aktiviert
- nlb-logging-enabled
- no-unrestricted-route-to-igw
- opensearch-primary-node-fault-Toleranz
- opensearch-update-check
- rabbit-mq-supported-version
- rds-aurora-postgresql-logs-zu-Cloud-Uhr
- rds-automatic-minor-version-upgrade-fähig
- rds-cluster-deletion-protection-aktiviert
- rds-cluster-iam-authentication-aktiviert
- rds-cluster-multi-az-aktiviert
- rds-enhanced-monitoring-enabled

- rds-instance-default-admin-überprüfen
- rds-instance-deletion-protection-aktiviert
- rds-instance-iam-authentication-aktiviert
- rds-instance-public-access-überprüfen
- rds-instance-subnet-igw-überprüfen
- rds-in-backup-plan
- rds-last-backup-recovery-Punkt erstellt
- rds-logging-enabled
- rds-mariadb-instance-encryptedim Transit
- rds-multi-az-support
- rds-mysql-instance-encryptedim Transit
- rds-postgresql-logs-to- Cloudwatch
- rds-postgres-instance-encryptedauf dem Weg
- rds-resources-protected-by-Ersatzplan
- rds-snapshots-public-prohibited
- rds-snapshot-encrypted
- rds-sqlserver-encrypted-in-Transit
- rds-sql-server-logszur Cloud-Überwachung
- rds-storage-encrypted
- redshift-backup-enabled
- redshift-cluster-configuration-check
- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check
- redshift-cluster-multi-az-aktiviert
- redshift-cluster-public-access-überprüfen
- redshift-cluster-subnet-group-Multi-Az
- redshift-default-admin-check
- redshift-enhanced-vpc-routing-aktiviert
- redshift-require-tls-ssl
- redshift-serverless-default-admin-überprüfen

- redshift-serverless-default-db-Namenscheck
- redshift-serverless-namespace-cmk-Verschlüsselung
- redshift-unrestricted-port-access
- required-tags
- restricted-incoming-traffic
- nur s3- access-point-in-vpc
- s3- -Blöcke access-point-public-access
- s3- -Blöcke account-level-public-access
- s3- -Blocke-periodisch account-level-public-access
- s 3- bucket-acl-prohibited
- s-3 bucket-blacklisted-actions-prohibited
- s3- bucket-cross-region-replication -aktiviert
- s-3 bucket-default-lock-enabled
- s3 bucket-level-public-access - verboten
- s3- bucket-logging-enabled
- s-3 bucket-mfa-delete-enabled
- s-3 bucket-policy-grantee-check
- s3- bucket-policy-not-more -freizügig
- s 3- bucket-public-read-prohibited
- s-3 bucket-public-write-prohibited
- s-3 bucket-replication-enabled
- s3- bucket-server-side-encryption -aktiviert
- s-3 bucket-ssl-requests-only
- s-3 bucket-versioning-enabled
- s-3 default-encryption-kms
- s-3 event-notifications-enabled
- s3 last-backup-recovery-point - erstellt
- s3- lifecycle-policy-check
- resources-protected-by-backups3-plan
- s 3- version-lifecycle-policy-check

- sagemaker-endpoint-configuration-kms-key-konfiguriert
- sagemaker-endpoint-config-prod-Anzahl der Instanzen
- sagemaker-notebook-instance-kms-key-konfiguriert
- sagemaker-notebook-instance-platform-Version
- sagemaker-notebook-no-direct-Internetzugang
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-überprüfen
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- securityhub-enabled
- service-catalog-shared-within-Organisation
- service-vpc-endpoint-enabled
- sns-encrypted-kms
- ssm-automation-block-public-teilen
- ssm-automation-logging-enabled
- ssm-document-not-public
- storagegateway-last-backup-recovery-Punkt erstellt
- storagegateway-resources-protected-by-Ersatzplan
- subnet-auto-assign-public-ip-deaktiviert
- transfer-connector-logging-enabled
- transfer-family-server-no-ftp
- virtualmachine-last-backup-recovery-punkt-erstellt
- virtualmachine-resources-protected-by-Ersatzplan
- vpc-default-security-group-geschlossen
- vpc-endpoint-enabled
- vpc-flow-logs-enabled
- vpc-network-acl-unused-überprüfen
- vpc-sg-open-only-to-authorized-ports
- vpc-sg-port-restriction-überprüfen

- vpc-vpn-2-tunnels-up
- wafv2-logging-enabled

AWS GovCloud Region (USA West)

AWS GovCloud (US-West)

- access-keys-rotated
- account-part-of-organizations
- acm-certificate-expiration-check
- active-mq-supported-version
- alb-desync-mode-check
- alb-http-drop-invalid-Header-fähig
- alb-http-to-https-Umleitungsprüfung
- alb-waf-enabled
- api-gw-associated-with-WAF
- api-gw-cache-enabled-und-verschlüsselt
- api-gw-endpoint-type-überprüfen
- api-gw-execution-logging-aktiviert
- api-gw-ssl-enabled
- api-gw-xray-enabled
- approved-amis-by-id
- approved-amis-by-tag
- athena-workgroup-logging-enabled
- aurora-last-backup-recovery-punkt-erstellt
- aurora-mysql-cluster-audit-Protokollierung
- aurora-resources-protected-by-Backup-Plan
- autoscaling-group-elb-healthcheck-erforderlich
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-public-ip-deaktiviert
- autoscaling-multiple-instance-types
- backup-plan-min-frequency-and-min-retention-check

- backup-recovery-point-encrypted
- backup-recovery-point-manual-Löschen-deaktiviert
- backup-recovery-point-minimum-Aufbewahrungsprüfung
- beanstalk-enhanced-health-reporting-aktiviert
- clb-desync-mode-check
- cloudformation-stack-drift-detection-überprüfen
- cloudformation-stack-notification-check
- cloudtrail-all-read-s3- data-event-check
- cloudtrail-all-write-s3- data-event-check
- Wolkenspur-S3- bucket-access-logging
- cloudtrail-s3- bucket-public-access-prohibited
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted
- cloud-trail-cloud-watch-logs-aktiviert
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-Validierung aktiviert
- cmk-backing-key-rotation-aktiviert
- codebuild-project-environment-privileged-überprüfen
- codebuild-project-envvar-awscred-überprüfen
- codebuild-project-logging-enabled
- codebuild-project-s3-log-verschlüsselt
- codebuild-project-source-repo-URL-Prüfung
- codebuild-report-group-encrypted-im Ruhezustand
- cognito-identity-pool-unauth-Zugriffsprüfung
- connect-instance-logging-enabled

- cw-loggroup-retention-period-prüfen
- datasync-task-logging-enabled
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- dms-mongo-db-authentication-aktiviert
- dms-neptune-iam-authorization-aktiviert
- dms-redis-tls-enabled
- dms-replication-not-public
- docdb-cluster-encrypted-in-Transit
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-last-backup-recovery-Punkt erstellt
- dynamodb-pitr-enabled
- dynamodb-resources-protected-by-Ersatzplan
- dynamodb-table-deletion-protection-aktiviert
- dynamodb-table-encrypted-kms
- dynamodb-table-encryption-enabled
- dynamodb-throughput-limit-check
- ebs-in-backup-plan
- ebs-last-backup-recovery-punkt-erstellt
- ebs-optimized-instance
- ebs-resources-protected-by-Ersatzplan
- ebs-snapshot-public-restorable-überprüfen
- ec2- aktiviert client-vpn-connection-log
- ec2- ebs-encryption-by-default
- ec2- aktiviert enis-source-destination-check
- ec2-imdsv2-check
- ec2- instance-detailed-monitoring-enabled
- ec2-ami instance-launched-with-allowed

- ec2- instance-managed-by-ssm
- ec2- instance-multiple-eni-check
- ec2- instance-no-public-ip
- ec2- instance-profile-attached
- ec2- erstellt last-backup-recovery-point
- ec2- managedinstance-applications-blacklisted
- ec2- managedinstance-applications-required
- ec2- prüfen managedinstance-association-compliance-status
- ec2- managedinstance-inventory-blacklisted
- ec2- prüfen managedinstance-patch-compliance-status
- ec2- managedinstance-platform-check
- ec2-plan resources-protected-by-backup
- ec2- -eni security-group-attached-to
- ec2-stopped-instance
- ec2- volume-inuse-check
- ec2- vpn-connection-logging-enabled
- ecr-private-image-scanning-aktiviert
- ecr-private-lifecycle-policy-konfiguriert
- ecr-private-tag-immutability-aktiviert
- ecr-repository-cmk-encryption-aktiviert
- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-container-insights-enabled
- ecs-fargate-latest-platform-Version
- ecs-task-definition-network-mode-not-host
- ecs-task-definition-user-for-host-mode-check
- efs-access-point-enforce-Benutzeridentität
- efs-automatic-backups-enabled
- efs-encrypted-check
- efs-filesystem-ct-encrypted

- efs-in-backup-plan
- efs-last-backup-recovery-Punkt erstellt
- efs-mount-target-public-zugänglich
- efs-resources-protected-by-Ersatzplan
- eip-attached
- eks-cluster-secrets-encrypted
- eks-cluster-supported-version
- eks-endpoint-no-public-Zugang
- eks-secrets-encrypted
- elasticache-redis-cluster-automatic-Backup-Check
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch
- elasticsearch-node-to-node-Verschlüsselungsprüfung
- elastic-beanstalk-managed-updates-aktiviert
- elbv2- listener-encryption-in-transit
- elbv2- -prüfen predefined-security-policy-ssl
- elb-acm-certificate-required
- elb-cross-zone-load-Balancing aktiviert
- elb-custom-security-policy-ssl-Prüfung
- elb-deletion-protection-enabled
- elb-logging-enabled
- elb-predefined-security-policy-ssl-Überprüfung
- elb-tls-https-listeners-nur
- emr-kerberos-enabled
- emr-master-no-public-ip
- encrypted-volumes
- event-data-store-cmk-Verschlüsselung aktiviert
- fms-shield-resource-policy-überprüfen
- fms-webacl-resource-policy-überprüfen

- fms-webacl-rulegroup-association-überprüfen
- fsx-last-backup-recovery-Punkt erstellt
- fsx-ontap-deployment-type-überprüfen
- fsx-openzfs-deployment-type-überprüfen
- fsx-resources-protected-by-Backup-Plan
- fsx-windows-deployment-type-überprüfen
- glue-job-logging-enabled
- glue-ml-transform-encrypted-im Ruhezustand
- glue-spark-job-supported-Ausführung
- guardduty-eks-protection-audit-aktiviert
- guardduty-enabled-centralized
- guardduty-lambda-protection-enabled
- guardduty-non-archived-findings
- GuardDuty-S3-Schutz aktiviert
- iam-customer-policy-blocked-kms-Aktionen
- iam-group-has-users-überprüfen
- iam-inline-policy-blocked-kms-Aktionen
- iam-no-inline-policy-überprüfen
- iam-password-policy
- iam-policy-blacklisted-check
- iam-policy-in-use
- iam-policy-no-statements-with-admin-access
- iam-policy-no-statements-with-full-access
- iam-role-managed-policy-überprüfen
- iam-root-access-key-überprüfen
- iam-server-certificate-expiration-überprüfen
- iam-user-group-membership-überprüfen
- iam-user-mfa-enabled
- iam-user-no-policies-überprüfen
- iam-user-unused-credentials-überprüfen

- incoming-ssh-disabled
- inspector-ec2-Scan aktiviert
- inspector-ecr-scan-enabled
- inspector-lambda-standard-scan-aktiviert
- instances-in-vpc
- internet-gateway-authorized-vpc-nur
- kinesis-firehose-delivery-stream-verschlüsselt
- kinesis-stream-backup-retention-überprüfen
- kinesis-stream-encrypted
- kms-cmk-not-scheduled-zum Löschen
- lambda-concurrency-check
- lambda-dlq-check
- lambda-function-public-access-verboten
- lambda-function-settings-check
- lambda-function-xray-enabled
- lambda-inside-vpc
- mariadb-publish-logs-to-cloudwatch-Protokolle
- mfa-enabled-for-iam-Konsolenzugriff
- mq-cloudwatch-audit-log-aktiviert
- msk-cluster-public-access-deaktiviert
- msk-unrestricted-access-check
- multi-region-cloud-trail-aktiviert
- nacl-no-unrestricted-ssh-rdp
- netfw-policy-rule-group-assoziiert
- netfw-stateless-rule-group-nicht leer
- netfw-subnet-change-protection-aktiviert
- nlb-logging-enabled
- no-unrestricted-route-to-igw
- opensearch-primary-node-fault-Toleranz
- opensearch-update-check

- rabbit-mq-supported-version
- rds-aurora-postgresql-logs-zu-Cloud-Uhr
- rds-automatic-minor-version-upgrade-fähig
- rds-cluster-deletion-protection-aktiviert
- rds-cluster-iam-authentication-aktiviert
- rds-cluster-multi-az-aktiviert
- rds-enhanced-monitoring-enabled
- rds-instance-default-admin-überprüfen
- rds-instance-deletion-protection-aktiviert
- rds-instance-iam-authentication-aktiviert
- rds-instance-public-access-überprüfen
- rds-instance-subnet-igw-überprüfen
- rds-in-backup-plan
- rds-last-backup-recovery-Punkt erstellt
- rds-logging-enabled
- rds-mariadb-instance-encryptedim Transit
- rds-multi-az-support
- rds-mysql-instance-encryptedim Transit
- rds-postgresql-logs-to- Cloudwatch
- rds-postgres-instance-encryptedim Transit
- rds-resources-protected-by-Ersatzplan
- rds-snapshots-public-prohibited
- rds-snapshot-encrypted
- rds-sqlserver-encrypted-in-Transit
- rds-sql-server-logs-zu-Cloud-Uhr
- rds-storage-encrypted
- redshift-backup-enabled
- redshift-cluster-configuration-check
- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check

- redshift-cluster-multi-az-aktiviert
- redshift-cluster-public-access-überprüfen
- redshift-cluster-subnet-group-Multi-Az
- redshift-default-admin-check
- redshift-enhanced-vpc-routing-aktiviert
- redshift-require-tls-ssl
- redshift-serverless-default-admin-überprüfen
- redshift-serverless-default-db-Namenscheck
- redshift-serverless-namespace-cmk-Verschlüsselung
- redshift-unrestricted-port-access
- required-tags
- restricted-incoming-traffic
- nur s3- access-point-in-vpc
- s3- -Blöcke access-point-public-access
- s3- -Blöcke account-level-public-access
- s3- -Blocke-periodisch account-level-public-access
- s 3- bucket-acl-prohibited
- s-3 bucket-blacklisted-actions-prohibited
- s3- bucket-cross-region-replication -aktiviert
- s-3 bucket-default-lock-enabled
- s3 bucket-level-public-access - verboten
- s3- bucket-logging-enabled
- s-3 bucket-mfa-delete-enabled
- s-3 bucket-policy-grantee-check
- s3- bucket-policy-not-more -freizügig
- s 3- bucket-public-read-prohibited
- s-3 bucket-public-write-prohibited
- s-3 bucket-replication-enabled
- s3- bucket-server-side-encryption -aktiviert
- s-3 bucket-ssl-requests-only

- s-3 bucket-versioning-enabled
- s-3 default-encryption-kms
- s-3 event-notifications-enabled
- s3 last-backup-recovery-point - erstellt
- s3- lifecycle-policy-check
- resources-protected-by-backups3-plan
- s 3- version-lifecycle-policy-check
- sagemaker-endpoint-configuration-kms-key-konfiguriert
- sagemaker-endpoint-config-prod-Anzahl der Instanzen
- sagemaker-notebook-instance-kms-key-konfiguriert
- sagemaker-notebook-instance-platform-Version
- sagemaker-notebook-no-direct-Internetzugang
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-überprüfen
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- securityhub-enabled
- service-catalog-shared-within-Organisation
- service-vpc-endpoint-enabled
- sns-encrypted-kms
- ssm-automation-block-public-teilen
- ssm-automation-logging-enabled
- ssm-document-not-public
- storagegateway-last-backup-recovery-Punkt erstellt
- storagegateway-resources-protected-by-Ersatzplan
- subnet-auto-assign-public-ip-deaktiviert
- transfer-connector-logging-enabled
- transfer-family-server-no-ftp
- virtualmachine-last-backup-recovery-punkt-erstellt

- virtualmachine-resources-protected-by-Ersatzplan
- vpc-default-security-group-geschlossen
- vpc-endpoint-enabled
- vpc-flow-logs-enabled
- vpc-network-acl-unused-überprüfen
- vpc-sg-open-only-to-authorized-ports
- vpc-sg-port-restriction-überprüfen
- vpc-vpn-2-tunnels-up
- wafv2-logging-enabled
- workspaces-root-volume-encryption-aktiviert
- workspaces-user-volume-encryption-aktiviert

AWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen

> **Important**
>
> Sie müssen zuerst den AWS Config Konfigurationsrekorder erstellen und starten, um AWS Config verwaltete Regeln mit zu erstellen AWS CloudFormation. Weitere Informationen finden Sie unter Verwalten von Configuration Recorder.

Für unterstützte AWS Config verwaltete Regeln können Sie die AWS CloudFormation Vorlagen verwenden, um die Regel für Ihr Konto zu erstellen oder einen vorhandenen AWS CloudFormation Stack zu aktualisieren. Ein Stack ist eine Sammlung von verwandten Ressourcen, die Sie als Einheit bereitstellen und aktualisieren. Wenn Sie einem Stack mit einer Vorlage starten, wird die verwaltete AWS Config -Regel für Sie erstellt. Die Vorlagen erstellen nur die Regel und keine zusätzlichen AWS Ressourcen.

> **Note**
>
> Wenn AWS Config verwaltete Regeln aktualisiert werden, werden die Vorlagen mit den neuesten Änderungen aktualisiert. Wenn Sie eine bestimmte Version einer Vorlage für eine Regel speichern möchten, laden Sie die Vorlage herunter und zu Ihrem S3-Bucket hoch.

Weitere Informationen zum Arbeiten mit AWS CloudFormation Vorlagen finden Sie unter Erste Schritte mit AWS CloudFormation im AWS CloudFormation Benutzerhandbuch.

Um einen AWS CloudFormation Stack für eine AWS Config verwaltete Regel zu starten

1. Gehen Sie zur CloudFormationKonsole und erstellen Sie einen neuen Stack.
2. Für Specify template (Vorlage angeben):
   - Wenn Sie die Vorlage heruntergeladen haben, wählen Sie Upload a template file (Vorlagendatei hochladen) aus und klicken Sie dann auf Choose file (Datei auswählen), um die Vorlage hochzuladen.
   - Sie können auch Amazon-S3-URL auswählen und die Vorlagen-URL `http://s3.amazonaws.com/aws-configservice-us-east-1/cloudformation-templates-for-managed-rules/THE_RULE_IDENTIFIER.template` eingeben.

   > **Note**
   >
   > Die Regel-ID sollte im Format ALL_CAPS_WITH_UNDERSCORES geschrieben werden. Zum Beispiel CLOUDWATCH_LOG_GROUP_ENCRYPTED statt. cloudwatch-log-group-encrypted
   > Bei einigen Regeln unterscheidet sich die Regel-ID vom Regelnamen. Stellen Sie sicher, dass Sie die Regel-ID verwenden. Die Regel-ID für restricted-ssh ist beispielsweise INCOMING_SSH_DISABLED.

3. Wählen Sie Weiter.
4. Geben Sie unter Stackdetails angeben einen Stacknamen und Parameterwerte für die Regel ein. AWS Config Wenn Sie beispielsweise die verwaltete Regelvorlage `DESIRED_INSTANCE_TYPE` verwenden, können Sie den Instance-Typ angeben (z. B. "m4.large").
5. Wählen Sie Weiter.
6. In Options können Sie Tags erstellen oder andere erweiterte Optionen konfigurieren. Diese sind nicht erforderlich.
7. Wählen Sie Weiter.
8. Bestätigen Sie bei Review (Prüfen), dass die Vorlage, Parameter und andere Optionen richtig sind.
9. Wählen Sie Create (Erstellen) aus. Der Stack wird in wenigen Minuten erstellt. Sie können die erstellte Regel in der AWS Config -Konsole anzeigen.

Sie können die Vorlagen verwenden, um einen einzelnen Stack für AWS Config verwaltete Regeln zu erstellen oder einen vorhandenen Stack in Ihrem Konto zu aktualisieren. Wenn Sie einen Stack löschen, werden die aus diesem Stack erstellten verwalteten Regeln ebenfalls gelöscht. Weitere Informationen finden Sie unter Arbeiten mit Stacks im Benutzerhandbuch von AWS CloudFormation .

AWS Config Benutzerdefinierte Regeln

AWS Config Benutzerdefinierte Regeln sind Regeln, die Sie von Grund auf neu erstellen. Es gibt zwei Möglichkeiten, AWS Config benutzerdefinierte Regeln zu erstellen: mit Lambda-Funktionen (AWS Lambda Developer Guide) und mit Guard (Guard GitHub Repository), einer policy-as-code Sprache.

AWS Config Mit Lambda erstellte benutzerdefinierte Regeln werden als AWS Config benutzerdefinierte Lambda-Regeln bezeichnet, und mit Guard erstellte AWS Config benutzerdefinierte Regeln werden als AWS Config benutzerdefinierte Richtlinienregeln bezeichnet.

Bevor Sie benutzerdefinierte Regeln verwenden, finden Sie weitere Informationen unter. Überlegungen

AWS Config Benutzerdefinierte Richtlinienregeln

Mit Guard geschriebene Regeln können von der AWS Config Konsole aus oder mithilfe der AWS Config Regel erstellt werden APIs. AWS Config Mit benutzerdefinierten Richtlinienregeln können Sie AWS Config benutzerdefinierte Regeln erstellen, ohne Java oder Python verwenden zu müssen, um Lambda-Funktionen zur Verwaltung Ihrer benutzerdefinierten Regeln zu entwickeln. AWS Config Benutzerdefinierte Richtlinienregeln werden durch Konfigurationsänderungen initiiert. Weitere Informationen zu Guard finden Sie im GitHubGuard-Repository.

AWS Config Benutzerdefinierte Lambda-Regeln

Benutzerdefinierte Lambda-Regeln bieten Ihnen die Möglichkeit, Java oder Python zu verwenden, um eine Lambda-Funktion für eine AWS Config benutzerdefinierte Regel zu erstellen. Eine Lambda-Funktion ist benutzerdefinierter Code AWS Lambda, in den Sie hochladen und der durch Ereignisse aufgerufen wird, die von einer Ereignisquelle in ihr veröffentlicht werden. Wenn die Lambda-Funktion mit einer AWS Config Regel verknüpft ist, wird sie AWS Config aufgerufen, wenn die Regel initiiert wird. Die Lambda-Funktion wertet dann die von AWS Config gesendeten Konfigurationsinformationen aus und gibt die Auswertungsergebnisse zurück. Weitere Informationen zu Lambda-Funktionen finden Sie in den Erläuterungen zu Funktions- und Ereignisquellen im AWS Lambda -Entwicklerhandbuch.

Formatunterschiede für benutzerdefinierte Regeln AWS Config

In der folgenden Tabelle werden die Formatunterschiede in den Feldern für den ConfigurationItemDatentyp und für AWS Config benutzerdefinierte Regeln angezeigt.

ConfigurationItem	AWS Config Benutzerdefinierte Regel
`version`	`configurationItemVersion`
`accountId`	`awsAccountId`
`arn`	`ARN`
`configurationItemMD5Hash`	`configurationStateMd5Hash`

Themen

- AWS Config Benutzerdefinierte Richtlinienregeln erstellen
- AWS Config Benutzerdefinierte Lambda-Regeln erstellen
- Gelöschte Ressourcen für AWS Config benutzerdefinierte Lambda-Regeln verwalten

AWS Config Benutzerdefinierte Richtlinienregeln erstellen

Sie können AWS Config benutzerdefinierte Richtlinienregeln über die AWS Management Console AWS CLI, oder AWS Config API erstellen.

AWS Config Benutzerdefinierte Richtlinienregeln hinzufügen

Using the console

1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die AWS Config Konsole zu https://console.aws.amazon.com/config/Hause.
2. Vergewissern Sie sich im AWS Management Console Menü, dass die Regionsauswahl auf eine AWS Region eingestellt ist, die AWS Config Regeln unterstützt. Die Liste der unterstützten Regionen finden Sie unter AWS Config -Regionen und -Endpunkte im Allgemeine Amazon Web Services-Referenz.
3. Klicken Sie im linken Navigationsbereich auf die Option Regeln.

4. Wählen Sie auf der Seite Rules (Regeln) die Option Add Rule (Regel hinzufügen) aus.
5. Wählen Sie auf der Seite Regeltyp angeben die Option Benutzerdefinierte Regel mit Guard erstellen aus.
6. Auf der Seite Regel konfigurieren konfigurieren Sie die Regel, indem Sie die folgenden Schritte ausführen:

   a. Geben Sie unter Regelname einen eindeutigen Namen für die Regel ein.

   b. Geben Sie unter Beschreibung eine Beschreibung für die Regel ein.

   c. Wählen Sie für die Guard-Runtime-Version das Laufzeitsystem für Ihre AWS Config benutzerdefinierte Richtlinienregel aus.

   d. Unter Regelinhalt können Sie die benutzerdefinierte Guard-Richtlinie für Ihre Regel angeben.

   e. Wählen Sie für den Testmodus aus, wann Sie im Prozess der Ressourcenerstellung und -verwaltung Ihre Ressourcen bewerten AWS Config möchten. Je nach Regel AWS Config können Sie Ihre Ressourcenkonfigurationen auswerten, bevor eine Ressource bereitgestellt wurde, nachdem eine Ressource bereitgestellt wurde oder beides.

      i. Wählen Sie Proaktive Auswertung einschalten aus, damit Auswertungen der Konfigurationseinstellungen Ihrer Ressourcen ausgeführt werden können, bevor diese bereitgestellt werden.

         Nachdem Sie die proaktive Evaluierung aktiviert haben, können Sie mithilfe der StartResourceEvaluationAPI und GetResourceEvaluationSummaryder API überprüfen, ob die Ressourcen, die Sie in diesen Befehlen angeben, durch die proaktiven Regeln in Ihrem Konto in Ihrer Region als NON_COMPLIANT gekennzeichnet werden.

         Weitere Informationen zur Verwendung dieser Befehle finden Sie unter Evaluieren Ihrer Ressourcen mithilfe von Regeln. AWS Config Eine Liste der verwalteten Regeln, die die proaktive Evaluierung unterstützen, finden Sie unter Liste der AWS Config verwalteten Regeln nach Testmodus.

      ii. Wählen Sie Detektivische Auswertung einschalten aus, um die Konfigurationseinstellungen Ihrer vorhandenen Ressourcen auszuwerten.

         Bei der detektiven Evaluierung werden AWS Config benutzerdefinierte Richtlinienregeln durch Konfigurationsänderungen initiiert. Diese Option ist vorab ausgewählt.

- Ressourcen: Wenn eine Ressource, die dem angegebenen Ressourcentyp oder dem Typ und dem Bezeichner entspricht, erstellt, geändert oder gelöscht wird
- Tags: Wenn eine Ressource mit einem bestimmten angegebenen Tag erstellt, geändert oder gelöscht wird
- Alle Änderungen — Wenn eine von aufgezeichnete Ressource erstellt, geändert oder gelöscht AWS Config wird.

AWS Config führt die Auswertung aus, wenn eine Änderung an einer Ressource erkannt wird, die dem Geltungsbereich der Regel entspricht. Sie können den Umfang verwenden, um zu beschränken, welche Ressourcen Auswertungen initiieren. Andernfalls werden Auswertungen initiiert, wenn eine nach der Bereitstellung bereitgestellte Ressource geändert wird.

f. Unter Parameter können Sie die Werte für die bereitgestellten Schlüssel anpassen, falls Ihre Regel Parameter enthält. Ein Parameter ist ein Attribut, über das Ihre Ressourcen verfügen müssen, damit sie als regelkonform gelten.

7. Überprüfen Sie auf der Seite Überprüfen und erstellen alle Ihre Auswahlen, bevor Sie die Regel zu Ihrer AWS-Konto hinzufügen.
8. Wenn Sie mit der Überprüfung Ihrer Regeln fertig sind, wählen Sie Regel hinzufügen aus.

Using the AWS CLI

Verwenden Sie den `put-config-rule`-Befehl.

Das `Owner`-Feld sollte den Wert `CUSTOM_POLICY` aufweisen. Die folgenden zusätzlichen Felder sind für AWS Config benutzerdefinierte Richtlinienregeln erforderlich:

- `Runtime`: Das Laufzeitsystem für Ihre AWS Config benutzerdefinierten Policy-Regeln.
- `PolicyText`: Die Richtliniendefinition, die die Logik für Ihre benutzerdefinierten AWS Config - Richtlinienregeln enthält.
- `EnableDebugLogDelivery`: Der boolesche Ausdruck zur Aktivierung der Debug-Protokollierung für Ihre AWS Config benutzerdefinierte Policy-Regel. Der Standardwert ist `false`.

Using the API Reference

Verwenden Sie die Aktion „PutConfigRule“.

Das `Owner`-Feld sollte den Wert `CUSTOM_POLICY` aufweisen. Die folgenden zusätzlichen Felder sind für AWS Config benutzerdefinierte Richtlinienregeln erforderlich:

- `Runtime`: Das Laufzeitsystem für Ihre AWS Config benutzerdefinierten Policy-Regeln.
- `PolicyText`: Die Richtliniendefinition, die die Logik für Ihre benutzerdefinierten AWS Config - Richtlinienregeln enthält.
- `EnableDebugLogDelivery`: Der boolesche Ausdruck zur Aktivierung der Debug-Protokollierung für Ihre AWS Config benutzerdefinierte Policy-Regel. Der Standardwert ist `false`.

Regelinhalt für AWS Config benutzerdefinierte Richtlinienregeln schreiben

Mit AWS Config benutzerdefinierten Richtlinienregeln können Sie die domänenspezifische Sprache (DSL) von AWS CloudFormation Guard verwenden, um Ressourcenkonfigurationen zu bewerten. Dieses Thema enthält Muster und bewährte Methoden für das Schreiben benutzerdefinierter Richtlinienregeln.

Weitere Informationen zum Schreiben von Regeln mit Guard finden Sie unter Writing Guard-Regeln im AWS CloudFormation Guard-Benutzerhandbuch und unter den Betriebsmodi von AWS CloudFormation Guard 2.0 im GitHub Guard-Repository.

Grundlegende Regelstruktur

Verwenden Sie das folgende Basisformat, um Regeln zu erstellen:

```
# Basic rule format
rule <rule_name> when
    resourceType == "<AWS::Service::Resource>" {
    # Evaluation clauses
}

# Example with filtering
let resources_of_type = Resources.*[ Type == 'AWS::Service::Resource' ]
rule check_resources when %resources_of_type !empty {
    %resources_of_type.configuration.property == expected_value
```

```
}
```

Zentrale Komponenten

Konfiguration

Enthält den Inhalt für die Ressourcenkonfiguration.

supplementaryConfiguration

Enthält zusätzliche Inhalte für die Ressourcenkonfiguration. AWS Config gibt dieses Feld für bestimmte Ressourcentypen zurück, um die für das Konfigurationsfeld zurückgegebenen Informationen zu ergänzen.

RessourcenTyp

AWS Ressourcentyp wird ausgewertet.

resourceId

Die ID der Ressource (zum Beispiel`sg-xxxxxx`).

accountId

Die 12-stellige AWS-Konto ID, die der Ressource zugeordnet ist.

Allgemeine Muster

Status checks

```
let allowed_status = ['ACTIVE', 'RUNNING']
rule check_resource_status when
    resourceType == "AWS::Service::Resource" {
    configuration.status IN %allowed_status
}
```

Required properties

```
rule check_required_properties when
    resourceType == "AWS::Service::Resource" {
    configuration.propertyName exists
    configuration.propertyName is_string  # or is_list, is_struct
}
```

Query blocks

```
configuration.Properties {
    property1 exists
    property2 is_string
    property3 IN [allowed_value1, allowed_value2]
}
```

Conditional evaluation

```
when configuration.feature_enabled == true {
    configuration.feature_settings exists
    configuration.feature_settings is_struct
}
```

Custom messages

```
rule check_compliance when
    resourceType == "AWS::Service::Resource" {
    configuration.property == expected_value <<Custom error message explaining the
 requirement>>
}}
```

Erweiterte Funktionen

Range checks

```
rule check_numeric_limits {
    # Inclusive range (lower_limit <= value <= upper_limit)
    configuration.value IN r[minimum_value, maximum_value]

    # Exclusive range (lower_limit < value < upper_limit)
    configuration.value IN r(exclusive_min, exclusive_max)

    # Left inclusive, right exclusive (lower_limit <= value < upper_limit)
    configuration.value IN r[minimum_value, exclusive_max)

    # Left exclusive, right inclusive (lower_limit < value <= upper_limit)
    configuration.value IN r(exclusive_min, maximum_value]
}
```

Combining conditions

```
# AND conditions (implicit through new lines)
condition_1
condition_2

# OR conditions (explicit)
condition_3 OR
condition_4
```

Chaining rules

```
rule check_prerequisites {
    configuration.required_setting exists
}

rule check_details when check_prerequisites {
    configuration.required_setting == expected_value
}
```

Bewährte Methoden

- Verwenden Sie Variablen mit `let` Anweisungen, um die Lesbarkeit zu verbessern.
- Gruppenbezogene Prüfungen mithilfe benannter Regelblöcke.
- Fügen Sie beschreibende Kommentare hinzu.
- Verwenden Sie die entsprechenden Operatoren (`exists`,`is_string`,`is_list`).
- Verwenden Sie Regex-Muster ohne Berücksichtigung der Groß-/Kleinschreibung.

Beispiel: dynamodb-pitr-enabled

Das folgende Beispiel zeigt die Richtliniendefinition für eine AWS Config benutzerdefinierte Richtlinienregelversion der verwalteten Regel. AWS Config dynamodb-pitr-enabled Diese Regel prüft, ob für DynamoDB-Tabellen Point-in-Time Recovery aktiviert ist.

```
# Check if DynamoDB tables have Point-in-Time Recovery enabled
let status = ['ACTIVE']

rule tableisactive when
```

```
    resourceType == "AWS::DynamoDB::Table" {
    configuration.tableStatus == %status
}

rule checkcompliance when
    resourceType == "AWS::DynamoDB::Table"
    tableisactive {
    let pitr =
 supplementaryConfiguration.ContinuousBackupsDescription.pointInTimeRecoveryDescription.pointIn
    %pitr == "ENABLED" <<DynamoDB tables must have Point-in-Time Recovery enabled>>
}
```

AWS Config Benutzerdefinierte Lambda-Regeln erstellen

Sie können benutzerdefinierte Regeln entwickeln und diese AWS Config mit AWS Lambda Funktionen ergänzen.

Sie verknüpfen jede benutzerdefinierte Regel mit einer Lambda-Funktion, die die Logik enthält, die bewertet, ob Ihre AWS Ressourcen der Regel entsprechen. Sie ordnen diese Funktion Ihrer Regel zu und die Regel ruft die Funktion entweder als Reaktion auf Änderungen an der Konfiguration oder in regelmäßigen Abständen ab. Die Funktion bewertet dann, ob Ihre Ressourcen Ihrer Regel entsprechen, und sendet ihre Bewertungsergebnisse an. AWS Config

AWS Regelentwicklungskit (RDK)

Das AWS Rule Development Kit (RDK) wurde entwickelt, um einen intuitiven und produktiven Compliance-as-Code-Workflow zu unterstützen. Es abstrahiert einen Großteil der undifferenzierten Arbeit, die mit der Bereitstellung von AWS Config Regeln verbunden ist, die durch benutzerdefinierte Lambda-Funktionen unterstützt werden, und bietet einen optimierten develop-deploy-monitor iterativen Prozess.

Eine step-by-step Anleitung finden Sie in der Dokumentation zum AWS Rule Development Kit (RDK).

AWS Lambda Beispielfunktionen für AWS Config Regeln (Node.js)

AWS Lambda führt Funktionen als Reaktion auf Ereignisse aus, die von AWS Diensten veröffentlicht werden. Die Funktion für eine AWS Config benutzerdefinierte Lambda-Regel empfängt ein Ereignis, das von veröffentlicht wurde AWS Config, und die Funktion verwendet dann Daten, die sie von dem Ereignis empfängt und die sie von der AWS Config API abruft, um die Einhaltung der Regel zu bewerten. Die Operationen in einer Funktion für eine Config-Regel unterscheiden sich darin, ob eine durch Konfigurationsänderungen ausgelöste oder regelmäßige Auswertung durchgeführt wird.

Informationen zu häufig verwendeten Mustern innerhalb von AWS Lambda Funktionen finden Sie unter Programmiermodell im AWS Lambda Entwicklerhandbuch.

Example Function for Evaluations Triggered by Configuration Changes

AWS Config ruft eine Funktion wie das folgende Beispiel auf, wenn sie eine Konfigurationsänderung für eine Ressource erkennt, die im Geltungsbereich einer benutzerdefinierten Regel liegt.

Wenn Sie die AWS Config Konsole verwenden, um eine Regel zu erstellen, die mit einer Funktion wie diesem Beispiel verknüpft ist, wählen Sie Configuration changes als Triggertyp aus. Wenn Sie die AWS Config API verwenden oder AWS CLI die Regel erstellen, legen Sie das `MessageType` Attribut auf `ConfigurationItemChangeNotification` und fest`OversizedConfigurationItemChangeNotification`. Mit diesen Einstellungen kann Ihre Regel immer dann ausgelöst werden, wenn aufgrund einer Ressourcenänderung ein Konfigurationselement oder ein zu großes Konfigurationselement AWS Config generiert wird.

In diesem Beispiel werden Ihre Ressourcen ausgewertet und es wird geprüft, ob die Instances dem Ressourcentyp `AWS::EC2::Instance` entsprechen. Die Regel wird ausgelöst, wenn AWS Config eine Benachrichtigung über ein Konfigurationselement oder ein übergroßes Konfigurationselement generiert.

```
'use strict';

import { ConfigServiceClient, GetResourceConfigHistoryCommand,
 PutEvaluationsCommand } from "@aws-sdk/client-config-service";

const configClient = new ConfigServiceClient({});

// Helper function used to validate input
function checkDefined(reference, referenceName) {
    if (!reference) {
        throw new Error(`Error: ${referenceName} is not defined`);
    }
    return reference;
}

// Check whether the message type is OversizedConfigurationItemChangeNotification,
function isOverSizedChangeNotification(messageType) {
    checkDefined(messageType, 'messageType');
    return messageType === 'OversizedConfigurationItemChangeNotification';
}
```

```
// Get the configurationItem for the resource using the getResourceConfigHistory
 API.
async function getConfiguration(resourceType, resourceId, configurationCaptureTime,
 callback) {
    const input = { resourceType, resourceId, laterTime: new
 Date(configurationCaptureTime), limit: 1 };
    const command = new GetResourceConfigHistoryCommand(input);
    await configClient.send(command).then(
        (data) => {
            callback(null, data.configurationItems[0]);
        },
        (error) => {
            callback(error, null);
        }
    );

}

// Convert the oversized configuration item from the API model to the original
 invocation model.
function convertApiConfiguration(apiConfiguration) {
    apiConfiguration.awsAccountId = apiConfiguration.accountId;
    apiConfiguration.ARN = apiConfiguration.arn;
    apiConfiguration.configurationStateMd5Hash =
 apiConfiguration.configurationItemMD5Hash;
    apiConfiguration.configurationItemVersion = apiConfiguration.version;
    apiConfiguration.configuration = JSON.parse(apiConfiguration.configuration);
    if ({}.hasOwnProperty.call(apiConfiguration, 'relationships')) {
        for (let i = 0; i < apiConfiguration.relationships.length; i++) {
            apiConfiguration.relationships[i].name =
 apiConfiguration.relationships[i].relationshipName;
        }
    }
    return apiConfiguration;
}

// Based on the message type, get the configuration item either from the
 configurationItem object in the invoking event or with the getResourceConfigHistory
 API in the getConfiguration function.
async function getConfigurationItem(invokingEvent, callback) {
    checkDefined(invokingEvent, 'invokingEvent');
    if (isOverSizedChangeNotification(invokingEvent.messageType)) {
```

```
        const configurationItemSummary =
 checkDefined(invokingEvent.configurationItemSummary, 'configurationItemSummary');
        await getConfiguration(configurationItemSummary.resourceType,
 configurationItemSummary.resourceId,
 configurationItemSummary.configurationItemCaptureTime, (err, apiConfigurationItem)
 => {
            if (err) {
                callback(err);
            }
            const configurationItem = convertApiConfiguration(apiConfigurationItem);
            callback(null, configurationItem);
        });
    } else {
        checkDefined(invokingEvent.configurationItem, 'configurationItem');
        callback(null, invokingEvent.configurationItem);
    }
}

// Check whether the resource has been deleted. If the resource was deleted, then
 the evaluation returns not applicable.
function isApplicable(configurationItem, event) {
    checkDefined(configurationItem, 'configurationItem');
    checkDefined(event, 'event');
    const status = configurationItem.configurationItemStatus;
    const eventLeftScope = event.eventLeftScope;
    return (status === 'OK' || status === 'ResourceDiscovered') && eventLeftScope
 === false;
}

// In this example, the resource is compliant if it is an instance and its type
 matches the type specified as the desired type.
// If the resource is not an instance, then this resource is not applicable.
function evaluateChangeNotificationCompliance(configurationItem, ruleParameters) {
    checkDefined(configurationItem, 'configurationItem');
    checkDefined(configurationItem.configuration,
 'configurationItem.configuration');
    checkDefined(ruleParameters, 'ruleParameters');

    if (configurationItem.resourceType !== 'AWS::EC2::Instance') {
        return 'NOT_APPLICABLE';
    } else if (ruleParameters.desiredInstanceType ===
 configurationItem.configuration.instanceType) {
        return 'COMPLIANT';
    }
```

```
    return 'NON_COMPLIANT';
}

// Receives the event and context from AWS Lambda.
export const handler = async (event, context) => {
    checkDefined(event, 'event');
    const invokingEvent = JSON.parse(event.invokingEvent);
    const ruleParameters = JSON.parse(event.ruleParameters);
    await getConfigurationItem(invokingEvent, async (err, configurationItem) => {

        let compliance = 'NOT_APPLICABLE';
        let annotation = '';
        const putEvaluationsRequest = {};
        if (isApplicable(configurationItem, event)) {
            // Invoke the compliance checking function.
            compliance = evaluateChangeNotificationCompliance(configurationItem,
 ruleParameters);
            if (compliance === "NON_COMPLIANT") {
                annotation = "This is an annotation describing why the resource is
 not compliant.";
            }
        }
        // Initializes the request that contains the evaluation results.
        if (annotation) {
            putEvaluationsRequest.Evaluations = [
                {
                    ComplianceResourceType: configurationItem.resourceType,
                    ComplianceResourceId: configurationItem.resourceId,
                    ComplianceType: compliance,
                    OrderingTimestamp: new
 Date(configurationItem.configurationItemCaptureTime),
                    Annotation: annotation
                },
            ];
        } else {
            putEvaluationsRequest.Evaluations = [
                {
                    ComplianceResourceType: configurationItem.resourceType,
                    ComplianceResourceId: configurationItem.resourceId,
                    ComplianceType: compliance,
                    OrderingTimestamp: new
 Date(configurationItem.configurationItemCaptureTime),
                },
            ];
```

```
        }
        putEvaluationsRequest.ResultToken = event.resultToken;

        // Sends the evaluation results to AWS Config.
        await configClient.send(new PutEvaluationsCommand(putEvaluationsRequest));
    });
};
```

Funktionsoperationen

Die Funktion führt die folgenden Operationen zur Laufzeit aus:

1. Die Funktion wird ausgeführt, wenn AWS Lambda das `event` Objekt an die `handler` Funktion übergeben wird. In diesem Beispiel akzeptiert die Funktion den optionalen `callback` Parameter, mit dem sie Informationen an den Aufrufer zurückgibt. AWS Lambda übergibt außerdem ein `context` Objekt, das Informationen und Methoden enthält, die die Funktion während ihrer Ausführung verwenden kann. Beachten Sie, dass in neueren Versionen von Lambda „context“ nicht mehr verwendet wird.
2. Die Funktion prüft, ob `messageType` für das Ereignis ein Konfigurationselement oder ein übergroßes Konfigurationselement ist, und gibt anschließend das Konfigurationselement zurück.
3. Der Handler ruft die `isApplicable`-Funktion auf, um zu ermitteln, ob die Ressource gelöscht wurde.

   > **Note**
   >
   > Regeln, die gelöschte Ressourcen melden, sollten das Auswertungsergebnis `NOT_APPLICABLE` zurückgeben, um unnötige Regelauswertungen zu vermeiden.

4. Der Handler ruft die `evaluateChangeNotificationCompliance` Funktion auf und übergibt die `ruleParameters` Objekte `configurationItem` und, die im Ereignis AWS Config veröffentlicht wurden.

   Die Funktion bewertet zunächst, ob es sich bei der Ressource um eine EC2 Instanz handelt. Wenn die Ressource keine EC2 Instanz ist, gibt die Funktion den Konformitätswert von `NOT_APPLICABLE` zurück.

   Anschließend wertet die Funktion aus, ob das `instanceType`-Attribut im Konfigurationselement dem `desiredInstanceType`-Parameterwert gleicht. Wenn die Werte

identisch sind, gibt die Funktion `COMPLIANT` zurück. Wenn die Werte nicht identisch sind, gibt die Funktion `NON_COMPLIANT` zurück.

5. Der Handler bereitet das Senden der Auswertungsergebnisse vor, AWS Config indem er das `putEvaluationsRequest` Objekt initialisiert. Dieses Objekt enthält die `Evaluations`-Parameter, die das Compliance-Ergebnis, den Ressourcentyp und die ID der ausgewerteten Ressource identifizieren. Das `putEvaluationsRequest` Objekt enthält auch das Ergebnis-Token des Ereignisses, das die Regel und das Ereignis für AWS Config identifiziert.
6. Der Handler sendet die Auswertungsergebnisse an, AWS Config indem er das Objekt an die `putEvaluations` Methode des `config` Clients übergibt.

Example Function for Periodic Evaluations

AWS Config ruft eine Funktion wie das folgende Beispiel für regelmäßige Auswertungen auf. Regelmäßige Auswertungen werden mit der von Ihnen bei der Definition der Regel in AWS Config angegebenen Häufigkeit ausgeführt.

Wenn Sie die AWS Config Konsole verwenden, um eine Regel zu erstellen, die mit einer Funktion wie diesem Beispiel verknüpft ist, wählen Sie Periodisch als Triggertyp. Wenn Sie die AWS Config API verwenden oder AWS CLI die Regel erstellen, setzen Sie das `MessageType` Attribut auf`ScheduledNotification`.

In diesem Beispiel wird überprüft, ob die Gesamtanzahl einer bestimmten Ressource einen bestimmten Höchstwert überschreitet.

```
'use strict';
import { ConfigServiceClient, ListDiscoveredResourcesCommand,
 PutEvaluationsCommand } from "@aws-sdk/client-config-service";

const configClient = new ConfigServiceClient({});

// Receives the event and context from AWS Lambda.
export const handler = async (event, context, callback) => {
    // Parses the invokingEvent and ruleParameters values, which contain JSON
 objects passed as strings.
    var invokingEvent = JSON.parse(event.invokingEvent),
        ruleParameters = JSON.parse(event.ruleParameters),
        numberOfResources = 0;

    if (isScheduledNotification(invokingEvent) &&
 hasValidRuleParameters(ruleParameters, callback)) {
```

```
        await countResourceTypes(ruleParameters.applicableResourceType, "",
numberOfResources, async function (err, count) {
            if (err === null) {
                var putEvaluationsRequest;
                const compliance = evaluateCompliance(ruleParameters.maxCount,
count);
                var annotation = '';
                if (compliance === "NON_COMPLIANT") {
                    annotation = "Description of why the resource is not
compliant.";
                }
                // Initializes the request that contains the evaluation results.
                if (annotation) {
                    putEvaluationsRequest = {
                        Evaluations: [{
                            // Applies the evaluation result to the AWS account
published in the event.
                            ComplianceResourceType: 'AWS::::Account',
                            ComplianceResourceId: event.accountId,
                            ComplianceType: compliance,
                            OrderingTimestamp: new Date(),
                            Annotation: annotation
                        }],
                        ResultToken: event.resultToken
                    };
                } else {
                    putEvaluationsRequest = {
                        Evaluations: [{
                            // Applies the evaluation result to the AWS account
published in the event.
                            ComplianceResourceType: 'AWS::::Account',
                            ComplianceResourceId: event.accountId,
                            ComplianceType: compliance,
                            OrderingTimestamp: new Date()
                        }],
                        ResultToken: event.resultToken
                    };
                }

                // Sends the evaluation results to AWS Config.
                try {
                    await configClient.send(new
PutEvaluationsCommand(putEvaluationsRequest));
                }
```

```
                catch (e) {
                    callback(e, null);
                }
            } else {
                callback(err, null);
            }
        });
    } else {
        console.log("Invoked for a notification other than Scheduled Notification...
 Ignoring.");
    }
};

// Checks whether the invoking event is ScheduledNotification.
function isScheduledNotification(invokingEvent) {
    return (invokingEvent.messageType === 'ScheduledNotification');
}

// Checks the rule parameters to see if they are valid
function hasValidRuleParameters(ruleParameters, callback) {
    // Regular express to verify that applicable resource given is a resource type
    const awsResourcePattern = /^AWS::(\w*)::(\w*)$/;
    const isApplicableResourceType =
 awsResourcePattern.test(ruleParameters.applicableResourceType);
    // Check to make sure the maxCount in the parameters is an integer
    const maxCountIsInt = !isNaN(ruleParameters.maxCount) &&
 parseInt(Number(ruleParameters.maxCount)) == ruleParameters.maxCount && !
isNaN(parseInt(ruleParameters.maxCount, 10));
    if (!isApplicableResourceType) {
        callback("The applicableResourceType parameter is not a valid resource
 type.", null);
    }
    if (!maxCountIsInt) {
        callback("The maxCount parameter is not a valid integer.", null);
    }
    return isApplicableResourceType && maxCountIsInt;
}

// Checks whether the compliance conditions for the rule are violated.
function evaluateCompliance(maxCount, actualCount) {
    if (actualCount > maxCount) {
        return "NON_COMPLIANT";
    } else {
        return "COMPLIANT";
```

```
    }
}

// Counts the applicable resources that belong to the AWS account.
async function countResourceTypes(applicableResourceType, nextToken, count,
 callback) {
    const input = { resourceType: applicableResourceType, nextToken: nextToken };
    const command = new ListDiscoveredResourcesCommand(input);
    try {
        const response = await configClient.send(command);
        count = count + response.resourceIdentifiers.length;
        if (response.nextToken !== undefined && response.nextToken != null) {
            countResourceTypes(applicableResourceType, response.nextToken, count,
 callback);
        }
        callback(null, count);
    } catch (e) {
        callback(e, null);
    }
    return count;
}
```

Funktionsoperationen

Die Funktion führt die folgenden Operationen zur Laufzeit aus:

1. Die Funktion wird ausgeführt, wenn AWS Lambda das `event` Objekt an die `handler` Funktion übergeben wird. In diesem Beispiel akzeptiert die Funktion den optionalen `callback` Parameter, mit dem sie Informationen an den Aufrufer zurückgibt. AWS Lambda übergibt außerdem ein `context` Objekt, das Informationen und Methoden enthält, die die Funktion während ihrer Ausführung verwenden kann. Beachten Sie, dass in neueren Versionen von Lambda „context“ nicht mehr verwendet wird.
2. Der Handler ruft die `countResourceTypes`-Funktion auf, um die Ressourcen des angegebenen Typs zu zählen, und die Funktion übergibt den `applicableResourceType`-Parameter, den sie vom Ereignis erhalten hat. Die `countResourceTypes`-Funktion ruft die `listDiscoveredResources`-Methode des `config`-Clients auf. Dieser gibt eine Liste der Kennungen für die entsprechenden Ressourcen zurück. Die Funktion verwendet die Länge dieser Liste, um die Anzahl der anwendbaren Ressourcen zu bestimmen, und gibt diese Anzahl an den Handler zurück.

3. Der Handler bereitet das Senden der Auswertungsergebnisse vor, AWS Config indem er das `putEvaluationsRequest` Objekt initialisiert. Dieses Objekt enthält den `Evaluations` Parameter, der das Konformitätsergebnis und das Ergebnis identifiziert AWS-Konto , das bei dem Ereignis veröffentlicht wurde. Sie können das Ergebnis mithilfe des `Evaluations`-Parameters auf jeden von AWS Config unterstützten Ressourcentyp anwenden. Das `putEvaluationsRequest` Objekt enthält auch das Ergebnis-Token des Ereignisses, das die Regel und das Ereignis für identifiziert AWS Config.
4. Innerhalb des `putEvaluationsRequest`-Objekts ruft der Handler die `evaluateCompliance`-Funktion auf. Diese Funktion prüft, ob die Anzahl der anwendbaren Ressourcen das Maximum überschreitet, das dem vom Ereignis bereitgestellten `maxCount`-Parameter zugewiesene wurde. Wenn die Anzahl der Ressourcen das Maximum überschreitet, gibt die Funktion `NON_COMPLIANT` zurück. Wenn die Anzahl der Ressourcen das Maximum nicht überschreitet, gibt die Funktion `COMPLIANT` zurück.
5. Der Handler sendet die Auswertungsergebnisse an, AWS Config indem er das Objekt an die `putEvaluations` Methode des `config` Clients übergibt.

AWS Lambda Beispielfunktionen für AWS Config Regeln (Python)

AWS Lambda führt Funktionen als Reaktion auf Ereignisse aus, die von AWS Diensten veröffentlicht werden. Die Funktion für eine AWS Config benutzerdefinierte Lambda-Regel empfängt ein Ereignis, das von veröffentlicht wurde AWS Config, und die Funktion verwendet dann Daten, die sie von dem Ereignis empfängt und die sie von der AWS Config API abruft, um die Einhaltung der Regel zu bewerten. Die Operationen in einer Funktion für eine Config-Regel unterscheiden sich darin, ob eine durch Konfigurationsänderungen ausgelöste oder regelmäßige Auswertung durchgeführt wird.

Informationen zu häufig verwendeten Mustern innerhalb von AWS Lambda Funktionen finden Sie unter Programmiermodell im AWS Lambda Entwicklerhandbuch.

Example Function for Evaluations Triggered by Configuration Changes

AWS Config ruft eine Funktion wie das folgende Beispiel auf, wenn sie eine Konfigurationsänderung für eine Ressource erkennt, die im Geltungsbereich einer benutzerdefinierten Regel liegt.

Wenn Sie die AWS Config Konsole verwenden, um eine Regel zu erstellen, die mit einer Funktion wie diesem Beispiel verknüpft ist, wählen Sie Configuration changes als Triggertyp aus. Wenn Sie die AWS Config API verwenden oder AWS CLI die Regel erstellen, legen Sie das `MessageType` Attribut auf `ConfigurationItemChangeNotification` und

fest`OversizedConfigurationItemChangeNotification`. Mit diesen Einstellungen kann Ihre Regel immer dann ausgelöst werden, wenn aufgrund einer Ressourcenänderung ein Konfigurationselement oder ein zu großes Konfigurationselement AWS Config generiert wird.

```
import botocore
import boto3
import json
import datetime

# Set to True to get the lambda to assume the Role attached on the Config Service
 (useful for cross-account).
ASSUME_ROLE_MODE = False

# This gets the client after assuming the Config service role
# either in the same AWS account or cross-account.
def get_client(service, event):
    """Return the service boto client. It should be used instead of directly calling
 the client.
    Keyword arguments:
    service -- the service name used for calling the boto.client()
    event -- the event variable given in the lambda handler
    """
    if not ASSUME_ROLE_MODE:
        return boto3.client(service)
    credentials = get_assume_role_credentials(event["executionRoleArn"])
    return boto3.client(service, aws_access_key_id=credentials['AccessKeyId'],
                        aws_secret_access_key=credentials['SecretAccessKey'],
                        aws_session_token=credentials['SessionToken']
                       )

# Helper function used to validate input
def check_defined(reference, reference_name):
    if not reference:
        raise Exception('Error: ', reference_name, 'is not defined')
    return reference

# Check whether the message is OversizedConfigurationItemChangeNotification or not
def is_oversized_changed_notification(message_type):
    check_defined(message_type, 'messageType')
    return message_type == 'OversizedConfigurationItemChangeNotification'

# Get configurationItem using getResourceConfigHistory API
# in case of OversizedConfigurationItemChangeNotification
```

```
def get_configuration(resource_type, resource_id, configuration_capture_time):
    result = AWS_CONFIG_CLIENT.get_resource_config_history(
        resourceType=resource_type,
        resourceId=resource_id,
        laterTime=configuration_capture_time,
        limit=1)
    configurationItem = result['configurationItems'][0]
    return convert_api_configuration(configurationItem)

# Convert from the API model to the original invocation model
def convert_api_configuration(configurationItem):
    for k, v in configurationItem.items():
        if isinstance(v, datetime.datetime):
            configurationItem[k] = str(v)
    configurationItem['awsAccountId'] = configurationItem['accountId']
    configurationItem['ARN'] = configurationItem['arn']
    configurationItem['configurationStateMd5Hash'] =
 configurationItem['configurationItemMD5Hash']
    configurationItem['configurationItemVersion'] = configurationItem['version']
    configurationItem['configuration'] =
 json.loads(configurationItem['configuration'])
    if 'relationships' in configurationItem:
        for i in range(len(configurationItem['relationships'])):
            configurationItem['relationships'][i]['name'] =
 configurationItem['relationships'][i]['relationshipName']
    return configurationItem

# Based on the type of message get the configuration item
# either from configurationItem in the invoking event
# or using the getResourceConfigHistory API in getConfiguration function.
def get_configuration_item(invokingEvent):
    check_defined(invokingEvent, 'invokingEvent')
    if is_oversized_changed_notification(invokingEvent['messageType']):
        configurationItemSummary =
 check_defined(invokingEvent['configurationItemSummary'],
 'configurationItemSummary')
        return get_configuration(configurationItemSummary['resourceType'],
 configurationItemSummary['resourceId'],
 configurationItemSummary['configurationItemCaptureTime'])
    return check_defined(invokingEvent['configurationItem'], 'configurationItem')

# Check whether the resource has been deleted. If it has, then the evaluation is
 unnecessary.
def is_applicable(configurationItem, event):
```

```
    try:
        check_defined(configurationItem, 'configurationItem')
        check_defined(event, 'event')
    except:
        return True
    status = configurationItem['configurationItemStatus']
    eventLeftScope = event['eventLeftScope']
    if status == 'ResourceDeleted':
        print("Resource Deleted, setting Compliance Status to NOT_APPLICABLE.")
    return (status == 'OK' or status == 'ResourceDiscovered') and not eventLeftScope

def get_assume_role_credentials(role_arn):
    sts_client = boto3.client('sts')
    try:
        assume_role_response = sts_client.assume_role(RoleArn=role_arn,
 RoleSessionName="configLambdaExecution")
        return assume_role_response['Credentials']
    except botocore.exceptions.ClientError as ex:
        # Scrub error message for any internal account info leaks
        if 'AccessDenied' in ex.response['Error']['Code']:
            ex.response['Error']['Message'] = "AWS Config does not have permission
 to assume the IAM role."
        else:
            ex.response['Error']['Message'] = "InternalError"
            ex.response['Error']['Code'] = "InternalError"
        raise ex

def evaluate_change_notification_compliance(configuration_item, rule_parameters):
    check_defined(configuration_item, 'configuration_item')
    check_defined(configuration_item['configuration'],
 'configuration_item[\'configuration\']')
    if rule_parameters:
        check_defined(rule_parameters, 'rule_parameters')

    if (configuration_item['resourceType'] != 'AWS::EC2::Instance'):
        return 'NOT_APPLICABLE'

    elif rule_parameters.get('desiredInstanceType'):
        if (configuration_item['configuration']['instanceType'] in
 rule_parameters['desiredInstanceType']):
            return 'COMPLIANT'
    return 'NON_COMPLIANT'

def lambda_handler(event, context):
```

```
    global AWS_CONFIG_CLIENT

    check_defined(event, 'event')
    invoking_event = json.loads(event['invokingEvent'])
    rule_parameters = {}
    if 'ruleParameters' in event:
        rule_parameters = json.loads(event['ruleParameters'])

    compliance_value = 'NOT_APPLICABLE'

    AWS_CONFIG_CLIENT = get_client('config', event)
    configuration_item = get_configuration_item(invoking_event)
    if is_applicable(configuration_item, event):
        compliance_value = evaluate_change_notification_compliance(
                configuration_item, rule_parameters)

    response = AWS_CONFIG_CLIENT.put_evaluations(
       Evaluations=[
           {
               'ComplianceResourceType': invoking_event['configurationItem']
['resourceType'],
               'ComplianceResourceId': invoking_event['configurationItem']
['resourceId'],
               'ComplianceType': compliance_value,
               'OrderingTimestamp': invoking_event['configurationItem']
['configurationItemCaptureTime']
           },
       ],
       ResultToken=event['resultToken'])
```

Funktionsoperationen

Die Funktion führt die folgenden Operationen zur Laufzeit aus:

1. Die Funktion wird ausgeführt, wenn AWS Lambda das `event` Objekt an die `handler` Funktion übergeben wird. In diesem Beispiel akzeptiert die Funktion den optionalen `callback` Parameter, mit dem sie Informationen an den Aufrufer zurückgibt. AWS Lambda übergibt außerdem ein `context` Objekt, das Informationen und Methoden enthält, die die Funktion während ihrer Ausführung verwenden kann. Beachten Sie, dass in neueren Versionen von Lambda „context“ nicht mehr verwendet wird.

2. Die Funktion prüft, ob `messageType` für das Ereignis ein Konfigurationselement oder ein übergroßes Konfigurationselement ist, und gibt anschließend das Konfigurationselement zurück.
3. Der Handler ruft die `isApplicable`-Funktion auf, um zu ermitteln, ob die Ressource gelöscht wurde.

> **Note**
>
> Regeln, die gelöschte Ressourcen melden, sollten das Auswertungsergebnis `NOT_APPLICABLE` zurückgeben, um unnötige Regelauswertungen zu vermeiden.

4. Der Handler ruft die `evaluateChangeNotificationCompliance` Funktion auf und übergibt die `ruleParameters` Objekte `configurationItem` und, die im Ereignis AWS Config veröffentlicht wurden.

   Die Funktion bewertet zunächst, ob es sich bei der Ressource um eine EC2 Instanz handelt. Wenn die Ressource keine EC2 Instanz ist, gibt die Funktion den Konformitätswert von `NOT_APPLICABLE` zurück.

   Anschließend wertet die Funktion aus, ob das `instanceType`-Attribut im Konfigurationselement dem `desiredInstanceType`-Parameterwert gleicht. Wenn die Werte identisch sind, gibt die Funktion `COMPLIANT` zurück. Wenn die Werte nicht identisch sind, gibt die Funktion `NON_COMPLIANT` zurück.
5. Der Handler bereitet das Senden der Auswertungsergebnisse vor, AWS Config indem er das `putEvaluationsRequest` Objekt initialisiert. Dieses Objekt enthält die `Evaluations`-Parameter, die das Compliance-Ergebnis, den Ressourcentyp und die ID der ausgewerteten Ressource identifizieren. Das `putEvaluationsRequest` Objekt enthält auch das Ergebnis-Token des Ereignisses, das die Regel und das Ereignis für AWS Config identifiziert.
6. Der Handler sendet die Auswertungsergebnisse an, AWS Config indem er das Objekt an die `putEvaluations` Methode des `config` Clients übergibt.

Example Function for Periodic Evaluations

AWS Config ruft eine Funktion wie das folgende Beispiel für regelmäßige Auswertungen auf. Regelmäßige Auswertungen werden mit der von Ihnen bei der Definition der Regel in AWS Config angegebenen Häufigkeit ausgeführt.

Wenn Sie die AWS Config Konsole verwenden, um eine Regel zu erstellen, die mit einer Funktion wie diesem Beispiel verknüpft ist, wählen Sie Periodisch als Triggertyp. Wenn Sie die AWS Config API verwenden oder AWS CLI die Regel erstellen, setzen Sie das `MessageType` Attribut auf`ScheduledNotification`.

```
import botocore
import boto3
import json
import datetime

# Set to True to get the lambda to assume the Role attached on the Config Service
 (useful for cross-account).
ASSUME_ROLE_MODE = False
DEFAULT_RESOURCE_TYPE = 'AWS::::Account'

# This gets the client after assuming the Config service role
# either in the same AWS account or cross-account.
def get_client(service, event):
    """Return the service boto client. It should be used instead of directly calling
 the client.
    Keyword arguments:
    service -- the service name used for calling the boto.client()
    event -- the event variable given in the lambda handler
    """
    if not ASSUME_ROLE_MODE:
        return boto3.client(service)
    credentials = get_assume_role_credentials(event["executionRoleArn"])
    return boto3.client(service, aws_access_key_id=credentials['AccessKeyId'],
                        aws_secret_access_key=credentials['SecretAccessKey'],
                        aws_session_token=credentials['SessionToken']
                       )

def get_assume_role_credentials(role_arn):
    sts_client = boto3.client('sts')
    try:
        assume_role_response = sts_client.assume_role(RoleArn=role_arn,
 RoleSessionName="configLambdaExecution")
        return assume_role_response['Credentials']
    except botocore.exceptions.ClientError as ex:
        # Scrub error message for any internal account info leaks
        if 'AccessDenied' in ex.response['Error']['Code']:
            ex.response['Error']['Message'] = "AWS Config does not have permission
 to assume the IAM role."
```

```
        else:
            ex.response['Error']['Message'] = "InternalError"
            ex.response['Error']['Code'] = "InternalError"
        raise ex

# Check whether the message is a ScheduledNotification or not.
def is_scheduled_notification(message_type):
    return message_type == 'ScheduledNotification'

def count_resource_types(applicable_resource_type, next_token, count):
    resource_identifier =
 AWS_CONFIG_CLIENT.list_discovered_resources(resourceType=applicable_resource_type,
 nextToken=next_token)
    updated = count + len(resource_identifier['resourceIdentifiers']);
    return updated

# Evaluates the configuration items in the snapshot and returns the compliance value
 to the handler.
def evaluate_compliance(max_count, actual_count):
    return 'NON_COMPLIANT' if int(actual_count) > int(max_count) else 'COMPLIANT'

def evaluate_parameters(rule_parameters):
    if 'applicableResourceType' not in rule_parameters:
        raise ValueError('The parameter with "applicableResourceType" as key must be
 defined.')
    if not rule_parameters['applicableResourceType']:
        raise ValueError('The parameter "applicableResourceType" must have a defined
 value.')
    return rule_parameters

# This generate an evaluation for config
def build_evaluation(resource_id, compliance_type, event,
 resource_type=DEFAULT_RESOURCE_TYPE, annotation=None):
    """Form an evaluation as a dictionary. Usually suited to report on scheduled
 rules.
    Keyword arguments:
    resource_id -- the unique id of the resource to report
    compliance_type -- either COMPLIANT, NON_COMPLIANT or NOT_APPLICABLE
    event -- the event variable given in the lambda handler
    resource_type -- the CloudFormation resource type (or AWS:::Account) to report
 on the rule (default DEFAULT_RESOURCE_TYPE)
    annotation -- an annotation to be added to the evaluation (default None)
    """
    eval_cc = {}
```

```
    if annotation:
        eval_cc['Annotation'] = annotation
    eval_cc['ComplianceResourceType'] = resource_type
    eval_cc['ComplianceResourceId'] = resource_id
    eval_cc['ComplianceType'] = compliance_type
    eval_cc['OrderingTimestamp'] = str(json.loads(event['invokingEvent'])
['notificationCreationTime'])
    return eval_cc

def lambda_handler(event, context):

    global AWS_CONFIG_CLIENT

    evaluations = []
    rule_parameters = {}
    resource_count = 0
    max_count = 0

    invoking_event = json.loads(event['invokingEvent'])
    if 'ruleParameters' in event:
        rule_parameters = json.loads(event['ruleParameters'])
        valid_rule_parameters = evaluate_parameters(rule_parameters)

    compliance_value = 'NOT_APPLICABLE'

    AWS_CONFIG_CLIENT = get_client('config', event)
    if is_scheduled_notification(invoking_event['messageType']):
        result_resource_count =
 count_resource_types(valid_rule_parameters['applicableResourceType'], '',
 resource_count)

    if valid_rule_parameters.get('maxCount'):
        max_count = valid_rule_parameters['maxCount']

    compliance_value = evaluate_compliance(max_count, result_resource_count)
    evaluations.append(build_evaluation(event['accountId'], compliance_value, event,
 resource_type=DEFAULT_RESOURCE_TYPE))
    response = AWS_CONFIG_CLIENT.put_evaluations(Evaluations=evaluations,
 ResultToken=event['resultToken'])
```

Funktionsoperationen

Die Funktion führt die folgenden Operationen zur Laufzeit aus:

1. Die Funktion wird ausgeführt, wenn AWS Lambda das `event` Objekt an die `handler` Funktion übergeben wird. In diesem Beispiel akzeptiert die Funktion den optionalen `callback` Parameter, mit dem sie Informationen an den Aufrufer zurückgibt. AWS Lambda übergibt außerdem ein `context` Objekt, das Informationen und Methoden enthält, die die Funktion während ihrer Ausführung verwenden kann. Beachten Sie, dass in neueren Versionen von Lambda „context“ nicht mehr verwendet wird.
2. Der Handler ruft die `countResourceTypes`-Funktion auf, um die Ressourcen des angegebenen Typs zu zählen, und die Funktion übergibt den `applicableResourceType`-Parameter, den sie vom Ereignis erhalten hat. Die `countResourceTypes`-Funktion ruft die `listDiscoveredResources`-Methode des `config`-Clients auf. Dieser gibt eine Liste der Kennungen für die entsprechenden Ressourcen zurück. Die Funktion verwendet die Länge dieser Liste, um die Anzahl der anwendbaren Ressourcen zu bestimmen, und gibt diese Anzahl an den Handler zurück.
3. Der Handler bereitet das Senden der Auswertungsergebnisse vor, AWS Config indem er das `putEvaluationsRequest` Objekt initialisiert. Dieses Objekt enthält den `Evaluations` Parameter, der das Konformitätsergebnis und das Ergebnis identifiziert AWS-Konto , das bei dem Ereignis veröffentlicht wurde. Sie können das Ergebnis mithilfe des `Evaluations`-Parameters auf jeden von AWS Config unterstützten Ressourcentyp anwenden. Das `putEvaluationsRequest` Objekt enthält auch das Ergebnis-Token des Ereignisses, das die Regel und das Ereignis für identifiziert AWS Config.
4. Innerhalb des `putEvaluationsRequest`-Objekts ruft der Handler die `evaluateCompliance`-Funktion auf. Diese Funktion prüft, ob die Anzahl der anwendbaren Ressourcen das Maximum überschreitet, das dem vom Ereignis bereitgestellten `maxCount`-Parameter zugewiesene wurde. Wenn die Anzahl der Ressourcen das Maximum überschreitet, gibt die Funktion `NON_COMPLIANT` zurück. Wenn die Anzahl der Ressourcen das Maximum nicht überschreitet, gibt die Funktion `COMPLIANT` zurück.
5. Der Handler sendet die Auswertungsergebnisse an, AWS Config indem er das Objekt an die `putEvaluations` Methode des `config` Clients übergibt.

Beispielereignisse für AWS Config Regeln

Wenn der Auslöser für eine Regel eintritt, AWS Config ruft die AWS Lambda Funktion der Regel auf, indem ein Ereignis veröffentlicht wird. AWS Lambda Führt dann die Funktion aus, indem das Ereignis an den Handler der Funktion übergeben wird.

Example Event for Evaluations Triggered by Configuration Changes

AWS Config veröffentlicht ein Ereignis, wenn eine Konfigurationsänderung für eine Ressource erkannt wird, die im Geltungsbereich einer Regel liegt. Das folgende Beispielereignis zeigt, dass die Regel durch eine Konfigurationsänderung für eine EC2 Instanz ausgelöst wurde.

```
{
    "invokingEvent": "{\"configurationItem\":{\"configurationItemCaptureTime
\":\"2016-02-17T01:36:34.043Z\",\"awsAccountId\":\"123456789012\",
\"configurationItemStatus\":\"OK\",\"resourceId\":\"i-00000000\",\"ARN
\":\"arn:aws:ec2:us-east-2:123456789012:instance/i-00000000\",\"awsRegion
\":\"us-east-2\",\"availabilityZone\":\"us-east-2a\",\"resourceType\":
\"AWS::EC2::Instance\",\"tags\":{\"Foo\":\"Bar\"},\"relationships\":[{\"resourceId
\":\"eipalloc-00000000\",\"resourceType\":\"AWS::EC2::EIP\",\"name\":\"Is
 attached to ElasticIp\"}],\"configuration\":{\"foo\":\"bar\"}},\"messageType\":
\"ConfigurationItemChangeNotification\"}",
    "ruleParameters": "{\"myParameterKey\":\"myParameterValue\"}",
    "resultToken": "myResultToken",
    "eventLeftScope": false,
    "executionRoleArn": "arn:aws:iam::123456789012:role/config-role",
    "configRuleArn": "arn:aws:config:us-east-2:123456789012:config-rule/config-
rule-0123456",
    "configRuleName": "change-triggered-config-rule",
    "configRuleId": "config-rule-0123456",
    "accountId": "123456789012",
    "version": "1.0"
}
```

Example Event for Evaluations Triggered by Oversized Configuration Changes

Einige Änderungen an der Ressource erzeugen übergroße Konfigurationselemente. Das folgende Beispielereignis zeigt, dass die Regel durch eine übergroße Konfigurationsänderung für eine EC2 Instanz ausgelöst wurde.

```
{
        "invokingEvent": "{\"configurationItemSummary\": {\"changeType\":
 \"UPDATE\",\"configurationItemVersion\": \"1.2\",\"configurationItemCaptureTime
\":\"2016-10-06T16:46:16.261Z\",\"configurationStateId\": 0,\"awsAccountId
\":\"123456789012\",\"configurationItemStatus\": \"OK\",\"resourceType
\": \"AWS::EC2::Instance\",\"resourceId\":\"i-00000000\",\"resourceName
\":null,\"ARN\":\"arn:aws:ec2:us-west-2:123456789012:instance/i-00000000\",
\"awsRegion\": \"us-west-2\",\"availabilityZone\":\"us-west-2a\",
```

```
\"configurationStateMd5Hash\":\"8f1ee69b287895a0f8bc5753eca68e96\",
\"resourceCreationTime\":\"2016-10-06T16:46:10.489Z\"},\"messageType\":
\"OversizedConfigurationItemChangeNotification\"}",
        "ruleParameters": "{\"myParameterKey\":\"myParameterValue\"}",
        "resultToken": "myResultToken",
        "eventLeftScope": false,
        "executionRoleArn": "arn:aws:iam::123456789012:role/config-role",
        "configRuleArn": "arn:aws:config:us-east-2:123456789012:config-rule/config-
rule-ec2-managed-instance-inventory",
        "configRuleName": "change-triggered-config-rule",
        "configRuleId": "config-rule-0123456",
        "accountId": "123456789012",
        "version": "1.0"
    }
```

Example Event for Evaluations Triggered by Periodic Frequency

AWS Config veröffentlicht ein Ereignis, wenn Ihre Ressourcen mit einer von Ihnen festgelegten Häufigkeit bewertet werden (z. B. alle 24 Stunden). Im folgenden Beispielereignis wird gezeigt, dass die Regel von einer periodischen Häufigkeit ausgelöst wurde.

```
{
    "invokingEvent": "{\"awsAccountId\":\"123456789012\",\"notificationCreationTime
\":\"2016-07-13T21:50:00.373Z\",\"messageType\":\"ScheduledNotification\",
\"recordVersion\":\"1.0\"}",
    "ruleParameters": "{\"myParameterKey\":\"myParameterValue\"}",
    "resultToken": "myResultToken",
    "eventLeftScope": false,
    "executionRoleArn": "arn:aws:iam::123456789012:role/config-role",
    "configRuleArn": "arn:aws:config:us-east-2:123456789012:config-rule/config-
rule-0123456",
    "configRuleName": "periodic-config-rule",
    "configRuleId": "config-rule-6543210",
    "accountId": "123456789012",
    "version": "1.0"
}
```

Ereignisattribute

Das JSON-Objekt für ein AWS Config Ereignis enthält die folgenden Attribute:

`invokingEvent`

Das Ereignis, das die Bewertung für eine Regel auslöst. Wenn das Ereignis als Antwort auf die Änderung einer Ressourcenkonfigurationsänderung veröffentlicht wird, handelt es sich bei dem Wert für dieses Attribut um eine Zeichenfolge mit einem JSON-`configurationItem` oder einer `configurationItemSummary` (für übergroße große Konfigurationselemente). Das Konfigurationselement stellt den Status der Ressource zu dem Zeitpunkt dar, in dem die Änderung AWS Config erkannt wurde. Ein Beispiel für ein Konfigurationselement finden Sie in der Ausgabe des `get-resource-config-history` AWS CLI Befehls in Anzeigen des Konfigurationsverlaufs.

Wenn das Ereignis für eine regelmäßige Bewertung veröffentlicht wird, handelt es sich bei dem Wert um eine Zeichenfolge mit einem JSON-Objekt. Das Objekt enthält Informationen über die Bewertung, die ausgelöst wurde.

Für jeden Ereignistyp, muss eine Funktion die Zeichenfolge mit einem JSON-Parser analysieren, um die Inhalte zu bewerten, wie im folgenden Node.js-Beispiel:

```
var invokingEvent = JSON.parse(event.invokingEvent);
```

`ruleParameters`

Schlüssel/Wert-Paare, die die Funktion als Teil seiner Bewertungslogik verarbeitet. Sie definieren Parameter, wenn Sie die AWS Config Konsole verwenden, um eine benutzerdefinierte Lambda-Regel zu erstellen. Sie können Parameter auch mit dem `InputParameters` Attribut in der `PutConfigRule` AWS Config API-Anfrage oder im `put-config-rule` AWS CLI Befehl definieren.

Der JSON-Code für die Parameter ist in einer Zeichenfolge enthalten, sodass eine Funktion die Zeichenfolge mit einem JSON-Parser analysieren muss, um die Inhalte wie im folgenden Node.js-Beispiel bewerten zu können:

```
var ruleParameters = JSON.parse(event.ruleParameters);
```

`resultToken`

Ein Token, an das die Funktion AWS Config beim `PutEvaluations` Aufruf übergeben muss.

`eventLeftScope`

Ein boolescher Wert, der angibt, ob die auszuwertende AWS Ressource aus dem Geltungsbereich der Regel entfernt wurde. Wenn der Wert `true` ist, gibt die Funktion an, dass die Bewertung ignoriert werden kann, indem Sie `NOT_APPLICABLE` als Wert für das `ComplianceType`-Attribut im `PutEvaluations`-Aufruf übergibt.

`executionRoleArn`

Der ARN der IAM-Rolle, der zugewiesen AWS Config ist.

`configRuleArn`

Der ARN, AWS Config der der Regel zugewiesen wurde.

`configRuleName`

Der Name, den Sie der Regel zugewiesen haben, die AWS Config zur Veröffentlichung des Ereignisses und zum Aufrufen der Funktion geführt hat.

`configRuleId`

Die ID, die AWS Config der Regel zugewiesen wurde.

`accountId`

Die ID desjenigen AWS-Konto , dem die Regel gehört.

`version`

Eine Versionsnummer, die von zugewiesen wurde AWS. Die Version wird erhöht, wenn AWS Config Ereignissen Attribute AWS hinzugefügt werden. Wenn eine Funktion ein Attribut erfordert, das nur in Ereignissen vorhanden ist, die gleich oder größer als eine bestimmte Version sind, überprüft diese Funktion den Wert für dieses Attribut.

Die aktuelle Version für AWS Config Ereignisse ist 1.0.

Gelöschte Ressourcen für AWS Config benutzerdefinierte Lambda-Regeln verwalten

Regeln, die gelöschte Ressourcen melden, sollten das Auswertungsergebnis `NOT_APPLICABLE` zurückgeben, um unnötige Regelauswertungen zu vermeiden.

Wenn Sie eine Ressource löschen, AWS Config erstellt ein `configurationItem` mit `ResourceDeleted` für`configurationItemStatus`. Sie können diese Metadaten verwenden,

um zu überprüfen, ob eine Regel einen Bericht über eine gelöschte Ressource sendet. Weitere Informationen zu Konfigurationselementen finden Sie unter Konzepte | Konfigurationselemente.

Fügen Sie die folgenden Codefragmente ein, um nach gelöschten Ressourcen zu suchen, und legen Sie als Auswertungsergebnis einer AWS Config benutzerdefinierten Lambda-Regel fest, `NOT_APPLICABLE` ob sie über eine gelöschte Ressource berichtet:

Custom Lambda Rules (Node.js)

```
// Check whether the resource has been deleted. If the resource was deleted, then
 the evaluation returns not applicable.
function isApplicable(configurationItem, event) {
    checkDefined(configurationItem, 'configurationItem');
    checkDefined(event, 'event');
    const status = configurationItem.configurationItemStatus;
    const eventLeftScope = event.eventLeftScope;
    return (status === 'OK' || status === 'ResourceDiscovered') && eventLeftScope
 === false;
}
```

Custom Lambda Rules (Python)

```
# Check whether the resource has been deleted. If the resource was deleted, then the
 evaluation returns not applicable.
def is_applicable(configurationItem, event):
    try:
        check_defined(configurationItem, 'configurationItem')
        check_defined(event, 'event')
    except:
        return True
    status = configurationItem['configurationItemStatus']
    eventLeftScope = event['eventLeftScope']
    if status == 'ResourceDeleted':
        print("Resource Deleted, setting Compliance Status to NOT_APPLICABLE.")
    return (status == 'OK' or status == 'ResourceDiscovered') and not eventLeftScope
```

> **Note**
>
> AWS Config Verwaltete Regeln und AWS Config benutzerdefinierte Richtlinienregeln behandeln dieses Verhalten standardmäßig.

Wenn Sie mit Python mithilfe des AWS Config Development Kit (RDK) und der AWS Config Development Kit Library (RDKlib) eine AWS Config benutzerdefinierte Lambd-Regel erstellen, überprüft die importierte Evaluator-Klasse dieses Verhalten. Informationen zum Schreiben von Regeln mit dem RDK und RDKlib finden Sie unter Regeln mit dem RDK schreiben und. RDKlib

Serviceverknüpfte Regeln AWS Config

Eine serviceverknüpfte AWS Config Regel ist ein einzigartiger Typ AWS Config verwalteter Regeln, der andere AWS Dienste bei der Erstellung von AWS Config Regeln in Ihrem Konto unterstützt. Servicebezogene Regeln sind so vordefiniert, dass sie alle Berechtigungen enthalten, die erforderlich sind, um andere AWS Dienste in Ihrem Namen aufzurufen. Diese Regeln ähneln den Standards, die ein AWS Dienst Ihnen AWS-Konto zur Überprüfung der Einhaltung der Vorschriften empfiehlt.

Diese dienstbezogenen AWS Config Regeln sind Eigentum der AWS Serviceteams. Das AWS Serviceteam erstellt diese Regeln in Ihrem AWS-Konto. Sie haben schreibgeschützten Zugriff auf die Regeln. Sie können diese Regeln nicht bearbeiten oder löschen, wenn Sie AWS einen Dienst abonniert haben, mit dem diese Regeln verknüpft sind.

Mit Diensten verknüpfte Regeln und die AWS Command Line Interface

Der AWS CLI, PutConfigRuleDeleteConfigRule, und der DeleteEvaluationResults APIs Rückzugriff wurde mit der folgenden Fehlermeldung verweigert:

```
INSUFFICIENT_SLCR_PERMISSIONS = "An AWS service owns
ServiceLinkedConfigRule. You do not have permissions to take action on this
rule."
```

Regeln und die Konsole, die mit dem AWS Config Dienst verknüpft sind

In der AWS Config Konsole sind die mit dem Dienst verknüpften AWS Config Regeln auf der Seite Regeln sichtbar. Die Schaltflächen „Ergebnisse bearbeiten“ und „Ergebnisse löschen“ sind in der Konsole ausgegraut, sodass Sie die Regel nicht bearbeiten können. Sie können Details zur Regel ansehen, indem Sie sie auswählen.

Servicebezogene Regeln, Behebungsmaßnahmen und Konformitätspakete

Um einer serviceverknüpften Regel in einem Conformance Pack Behebungsmaßnahmen hinzuzufügen, müssen Sie die Behebungsaktion der Conformance Pack-Vorlage selbst hinzufügen

und dann das Conformance Pack mit Ihrer aktualisierten Vorlage aktualisieren. Informationen zur Aktualisierung von Conformance Packs finden Sie unter Bereitstellen eines Conformance Packs (Konsole), Bereitstellen eines Conformance Packs () und Verwalten von Organizational Conformance Packs.AWS CLI

Serviceverknüpfte Regeln bearbeiten und löschen

Um eine serviceverknüpfte Regel zu bearbeiten oder zu löschen, wenden Sie sich an den AWS Dienst, der die Regel erstellt hat. Bei serviceverknüpften Regeln, die von erstellt wurden AWS Security Hub, können Sie beispielsweise eine dienstverknüpfte Regel entfernen, indem Sie die folgenden Schritte im AWS Security Hub Benutzerhandbuch: Deaktivieren eines Sicherheitsstandards ausführen.

AWS Config Regeln für alle Konten in Ihrer Organisation verwalten

> **Important**
>
> Organisationsregeln können nur über die API oder CLI erstellt werden. Dieser Vorgang wird in der AWS Config Konsole nicht unterstützt.

AWS Config ermöglicht es Ihnen, AWS Config Regeln für alle AWS-Konten innerhalb einer Organisation zu verwalten. Sie haben folgende Möglichkeiten:

- AWS Config Regeln für alle Konten in Ihrer Organisation zentral erstellen, aktualisieren und löschen.
- Stellen Sie ein einheitliches AWS Config Regelwerk für alle Konten bereit und geben Sie Konten an, AWS Config für die keine Regeln erstellt werden sollen.
- Verwenden Sie das APIs From the Management Account in AWS Organizations , um die Steuerung durchzusetzen, indem Sie sicherstellen, dass die zugrunde liegenden AWS Config Regeln nicht durch die Mitgliedskonten Ihrer Organisation geändert werden können.

Überlegungen

Für Bereitstellungen in verschiedenen Regionen

Der API-Aufruf zur kontenübergreifenden Bereitstellung von Regeln und Konformitätspaketen ist AWS regionsspezifisch. Auf Organisationsebene müssen Sie den Kontext Ihres API-Aufrufs auf eine

andere Region ändern, wenn Sie Regeln in anderen Regionen bereitstellen möchten. Wenn Sie beispielsweise eine Regel in USA Ost (Nord-Virginia) bereitstellen möchten, ändern Sie die Region auf USA Ost (Nord-Virginia) und rufen Sie dann `PutOrganizationConfigRule` auf.

Für Konten innerhalb einer Organisation

Wenn ein neues Konto einer Organisation beitritt, wird die Regel oder das Konformitätspaket für dieses Konto bereitgestellt. Wenn ein Konto eine Organisation verlässt, wird die Regel oder das Konformitätspaket entfernt.

Wenn Sie eine Organisationsregel oder ein Konformitätspaket im Konto eines Organisationsadministrators bereitstellen und dann einen delegierten Administrator einrichten und eine Organisationsregel oder ein Konformitätspaket im delegierten Administratorkonto bereitstellen, können Sie die Organisationsregel oder das Konformitätspaket im Konto des Organisationsadministrators nicht vom delegierten Administratorkonto aus sehen. Sie können auch die Organisationsregel oder das Konformitätspaket nicht vom delegierten Administratorkonto des Kontos eines Organisationsadministrators aus sehen. Die DescribeOrganizationConfigRulesund DescribeOrganizationConformancePacks APIs können nur die organisationsbezogenen Ressourcen sehen und mit ihnen interagieren, die von dem Konto aus bereitgestellt wurden, das sie aufruft. APIs

Wiederholungsmechanismus für neue Konten, die einer Organisation hinzugefügt wurden

Wenn kein Recorder verfügbar ist, wird die Bereitstellung vorhandener Organisationsregeln und Konformitätspakete nur 7 Stunden lang wiederholt, nachdem ein Konto zu Ihrer Organisation hinzugefügt wurde. Es wird erwartet, dass Sie innerhalb von 7 Stunden nach dem Hinzufügen eines Kontos zu Ihrer Organisation einen Recorder erstellen, falls noch keiner vorhanden ist.

Konten für die Organisationsverwaltung, delegierte Administratoren und dienstbezogene Rollen

Wenn Sie ein Organisationsverwaltungskonto verwenden und beabsichtigen, einen delegierten Administrator für die organisatorische Bereitstellung zu verwenden, beachten Sie, dass dadurch die serviceverknüpfte Rolle (SLR) AWS Config nicht automatisch erstellt wird. Sie müssen die serviceverknüpfte Rolle (SLR) mithilfe von IAM separat manuell erstellen.

Wenn Sie keine Spiegelreflexkamera für Ihr Verwaltungskonto haben, können Sie von einem delegierten Administratorkonto aus keine Ressourcen für dieses Konto bereitstellen. Sie können weiterhin AWS Config Regeln für Mitgliedskonten von Verwaltungs- und delegierten Administratorkonten aus bereitstellen. Weitere Informationen finden Sie unter Verwenden von serviceverknüpften Rollen im AWS Identity and Access Management (IAM-) Benutzerhandbuch.

Bereitstellung

Informationen zur Integration AWS Config mit finden Sie AWS Organizations unter AWS Config und AWS Organizations im AWS Organizations Benutzerhandbuch. Stellen Sie sicher, dass die AWS Config Aufzeichnung aktiviert ist, bevor Sie die folgenden Methoden verwenden APIs , um AWS Config Regeln AWS-Konten innerhalb einer Organisation zu verwalten:

- PutOrganizationConfigRule, fügt eine Regel zur Organisationskonfiguration für Ihre gesamte Organisation hinzu oder aktualisiert sie. Dabei wird bewertet, ob Ihre AWS Ressourcen den gewünschten Konfigurationen entsprechen.
- DescribeOrganizationConfigRules, gibt eine Liste von Organisationskonfigurationsregeln zurück.
- GetOrganizationConfigRuleDetailedStatus, gibt einen detaillierten Status für jedes Mitgliedskonto innerhalb einer Organisation für eine bestimmte Organisationskonfigurationsregel zurück.
- GetOrganizationCustomRulePolicy, gibt die Richtliniendefinition zurück, die die Logik für die benutzerdefinierte Richtlinienregel Ihrer Organisationskonfiguration enthält.
- DescribeOrganizationConfigRuleStatuses, gibt den Bereitstellungsstatus der Organisationskonfigurationsregel für eine Organisation an.
- DeleteOrganizationConfigRule, löscht die angegebene Organisationskonfigurationsregel und alle zugehörigen Bewertungsergebnisse aus allen Mitgliedskonten in dieser Organisation.

Unterstützung von Regionen

Die Bereitstellung von AWS Config Regeln für alle Mitgliedskonten einer AWS Organisation wird in den folgenden Regionen unterstützt.

Name der Region	Region	Endpunkt	Protocol (Protokoll)
USA Ost (Ohio)	us-east-2	config.us-east-2.amazonaws.com	HTTPS
USA Ost (Nord-Virginia)	us-east-1	config.us-east-1.amazonaws.com	HTTPS

Name der Region	Region	Endpunkt	Protocol (Protokoll)	
USA West (Nordkalifornien)	us-west-1	config.us-west-1.amazonaws.com	HTTPS	
USA West (Oregon)	us-west-2	config.us-west-2.amazonaws.com	HTTPS	
Afrika (Kapstadt)	af-south-1	config.af-south-1.amazonaws.com	HTTPS	
Asien-Pazifik (Hongkong)	ap-east-1	config.ap-east-1.amazonaws.com	HTTPS	
Asien-Pazifik (Hyderabad)	ap-south-2	config.ap-south-2.amazonaws.com	HTTPS	
Asien-Pazifik (Jakarta)	ap-southeast-3	config.ap-southeast-3.amazonaws.com	HTTPS	
Asien-Pazifik (Melbourne)	ap-southeast-4	config.ap-southeast-4.amazonaws.com	HTTPS	

Name der Region	Region	Endpunkt	Protocol (Protokoll)
Asien-Pazifik (Mumbai)	ap-south-1	config.ap-south-1.amazonaws.com	HTTPS
Asien-Pazifik (Osaka)	ap-northeast-3	config.ap-northeast-3.amazonaws.com	HTTPS
Asien-Pazifik (Seoul)	ap-northeast-2	config.ap-northeast-2.amazonaws.com	HTTPS
Asien-Pazifik (Singapur)	ap-southeast-1	config.ap-southeast-1.amazonaws.com	HTTPS
Asien-Pazifik (Sydney)	ap-southeast-2	config.ap-southeast-2.amazonaws.com	HTTPS
Asien-Pazifik (Tokio)	ap-northeast-1	config.ap-northeast-1.amazonaws.com	HTTPS
Kanada (Zentral)	ca-central-1	config.ca-central-1.amazonaws.com	HTTPS
Kanada West (Calgary)	ca-west-1	config.ca-west-1.amazonaws.com	HTTPS
Europa (Frankfurt)	eu-central-1	config.eu-central-1.amazonaws.com	HTTPS

Name der Region	Region	Endpunkt	Protocol (Protokoll)
Europa (Irland)	eu-west-1	config.eu-west-1.amazonaws.com	HTTPS
Europa (London)	eu-west-2	config.eu-west-2.amazonaws.com	HTTPS
Europa (Mailand)	eu-south-1	config.eu-south-1.amazonaws.com	HTTPS
Europa (Paris)	eu-west-3	config.eu-west-3.amazonaws.com	HTTPS
Europa (Spanien)	eu-south-2	config.eu-south-2.amazonaws.com	HTTPS
Europa (Stockholm)	eu-north-1	config.eu-north-1.amazonaws.com	HTTPS
Europa (Zürich)	eu-central-2	config.eu-central-2.amazonaws.com	HTTPS
Israel (Tel Aviv)	il-central-1	config.il-central-1.amazonaws.com	HTTPS
Naher Osten (Bahrain)	me-south-1	config.me-south-1.amazonaws.com	HTTPS
Naher Osten (VAE)	me-central-1	config.me-central-1.amazonaws.com	HTTPS

Name der Region	Region	Endpunkt	Protocol (Protokoll)
Südamerika (São Paulo)	sa-east-1	config.sa-east-1.amazonaws.com	HTTPS
AWS GovCloud (US-Ost)	us-gov-east-1	config.us-gov-east-1.amazonaws.com	HTTPS
AWS GovCloud (US-West)	us-gov-west-1	config.us-gov-west-1.amazonaws.com	HTTPS

AWS Config Regeln hinzufügen

Sie können die AWS Config Konsole oder die verwenden AWS SDKs , um Regeln hinzuzufügen.

Themen

- Regeln hinzufügen (Konsole)
- Regeln hinzufügen (AWS SDKs)

Regeln hinzufügen (Konsole)

Auf der Seite Regeln werden Ihre Regeln und deren aktuelle Compliance-Ergebnisse in einer Tabelle dargestellt. Das Ergebnis für jede Regel lautet Evaluierung... bis die Bewertung Ihrer Ressourcen anhand der Regel AWS Config abgeschlossen ist. Sie können die Ergebnisse über die Aktualisieren-Schaltfläche aktualisieren. Wenn die AWS Config Evaluierungen abgeschlossen sind, können Sie sehen, welche Regeln und Ressourcentypen den Anforderungen entsprechen oder nicht. Weitere Informationen finden Sie unter Compliance-Informationen und Bewertungsergebnisse für Ihre AWS Ressourcen anzeigen mit AWS Config.

> **Note**
>
> Wenn Sie eine neue Regel hinzufügen, werden die entsprechenden Ressourcen in Ihrem Ressourceninventar AWS Config bewertet, einschließlich der zuvor erfassten Ressourcen. Wenn Sie beispielsweise `AWS::IoT::Policy` Ressourcen aufgezeichnet, sie aber später von der Aufzeichnung ausgeschlossen haben, werden die ursprünglichen Konfigurationselemente (CIs) in Ihrem Inventar AWS Config beibehalten. Diese werden zwar nicht AWS Config mehr aktualisiert, CIs wenn die ihnen zugewiesenen Ressourcentypen von der Aufzeichnung ausgeschlossen werden, ihr zuletzt aufgezeichneter Status wird jedoch beibehalten und sie ausgewertet, wenn Sie entsprechende Regeln hinzufügen.
> AWS Config bewertet keine Ressourcen, die nicht im Ressourceninventar enthalten sind. Wenn Sie beispielsweise die amplify-branch-tagged Regel hinzufügen, aber keine `AWS::Amplify::Branch` Ressourcen aufzeichnen und auch nie erfasst haben, AWS Config kann nicht bewertet werden, ob die AWS Amplify Filialen in Ihrem Konto den Vorschriften entsprechen oder nicht.
> Weitere Informationen finden Sie unter AWS Ressourcen aufzeichnen mit AWS Config.

Hinzufügen von Regeln

So fügen Sie eine Regel hinzu

1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die AWS Config Konsole zu https://console.aws.amazon.com/config/Hause.
2. Vergewissern Sie sich im AWS Management Console Menü, dass die Regionsauswahl auf eine Region eingestellt ist, die AWS Config Regeln unterstützt. Die Liste der unterstützten Regionen finden Sie unter AWS Config -Regionen und -Endpunkte im Allgemeine Amazon Web Services-Referenz.
3. Klicken Sie im linken Navigationsbereich auf die Option Regeln.
4. Wählen Sie auf der Seite Rules (Regeln) die Option Add Rule (Regel hinzufügen) aus.
5. Geben Sie auf der Seite Regeltyp angeben den Regeltyp an, indem Sie die folgenden Schritte ausführen:

    a. Geben Sie einen Begriff in das Suchfeld ein, um die Liste der verwalteten Regeln nach Regelname, Beschreibung und Bezeichnung zu filtern. Geben Sie beispielsweise Regeln ein, EC2die EC2 Ressourcentypen auswerten, oder geben Sie Periodisch ein, um Regeln zurückzugeben, die regelmäßig ausgelöst werden.

b. Zudem können Sie Ihre eigene benutzerdefinierte Regel erstellen. Wählen Sie Benutzerdefinierte Regel mithilfe von Lambda erstellen oder Benutzerdefinierte Regel mithilfe von Guard erstellen und folgen Sie den Anweisungen unter AWS Config Benutzerdefinierte Lambda-Regeln erstellen oder AWS Config Benutzerdefinierte Richtlinienregeln erstellen.

6. Auf der Seite Regel konfigurieren konfigurieren Sie die Regel, indem Sie die folgenden Schritte ausführen:

   a. Geben Sie unter Name einen eindeutigen Namen für die Regel ein.

   b. Geben Sie unter Beschreibung eine Beschreibung für die Regel ein.

   c. Wählen Sie für den Testmodus aus, wann Sie im Prozess der Ressourcenerstellung und -verwaltung Ihre Ressourcen bewerten AWS Config möchten. Je nach Regel AWS Config können Sie Ihre Ressourcenkonfigurationen auswerten, bevor eine Ressource bereitgestellt wurde, nachdem eine Ressource bereitgestellt wurde oder beides.

      i. Wählen Sie Proaktive Auswertung einschalten aus, damit Auswertungen der Konfigurationseinstellungen Ihrer Ressourcen ausgeführt werden können, bevor diese bereitgestellt werden.

         Nachdem Sie die proaktive Evaluierung aktiviert haben, können Sie mithilfe der StartResourceEvaluationAPI und GetResourceEvaluationSummaryder API überprüfen, ob die Ressourcen, die Sie in diesen Befehlen angeben, durch die proaktiven Regeln in Ihrem Konto in Ihrer Region als NON_COMPLIANT gekennzeichnet werden.

         Weitere Informationen zur Verwendung dieser Befehle finden Sie unter Evaluieren Ihrer Ressourcen mithilfe von Regeln. AWS Config Eine Liste der verwalteten Regeln, die die proaktive Evaluierung unterstützen, finden Sie unter Liste der AWS Config verwalteten Regeln nach Testmodus.

      ii. Wählen Sie Detektivische Auswertung einschalten aus, um die Konfigurationseinstellungen Ihrer vorhandenen Ressourcen auszuwerten.

         Für die detektivische Auswertung gibt es zwei Arten von Auslösern: Wenn sich die Konfiguration ändert und Regelmäßig.

         A. Wenn die Triggertypen für Ihre Regel Konfigurationsänderungen beinhalten, geben Sie eine der folgenden Optionen für Umfang der Änderungen an, mit denen Ihre Lambda-Funktion AWS Config aufgerufen wird:

- Ressourcen: Wenn eine Ressource, die dem angegebenen Ressourcentyp oder dem Typ und dem Bezeichner entspricht, erstellt, geändert oder gelöscht wird
- Tags: Wenn eine Ressource mit einem bestimmten angegebenen Tag erstellt, geändert oder gelöscht wird
- Alle Änderungen — Wenn eine von aufgezeichnete Ressource erstellt, geändert oder gelöscht AWS Config wird.

AWS Config führt die Auswertung aus, wenn eine Änderung an einer Ressource erkannt wird, die dem Geltungsbereich der Regel entspricht. Sie können den Umfang verwenden, um zu definieren, welche Ressourcen Auswertungen auslösen.

B. Wenn die Triggertypen für Ihre Regel Periodisch beinhalten, geben Sie die Frequenz an, mit der Ihre Lambda-Funktion AWS Config aufgerufen wird.

d. Unter Parameter können Sie die Werte für die bereitgestellten Schlüssel anpassen, falls Ihre Regel Parameter enthält. Ein Parameter ist ein Attribut, über das Ihre Ressourcen verfügen müssen, damit sie als regelkonform gelten.

7. Überprüfen Sie auf der Seite Überprüfen und erstellen alle Ihre Auswahlen, bevor Sie die Regel zu Ihrer hinzufügen. AWS-Konto Wenn die Regel oder Funktion nicht wie erwartet funktioniert, wird eine der folgenden Meldungen bei Compliance angezeigt:

   - Keine Ergebnisse gemeldet — Ihre Ressourcen wurden anhand der Regel AWS Config bewertet. Die Regel galt nicht für die AWS Ressourcen in ihrem Geltungsbereich, die angegebenen Ressourcen wurden gelöscht oder die Bewertungsergebnisse wurden gelöscht. Wenn Sie die Auswertungsergebnisse abrufen möchten, aktualisieren Sie die Regel, ändern Sie Ihren Umfang oder wählen Sie Re-evaluate (Erneut bewerten) aus.

     Diese Meldung wird ggf. auch dann angezeigt, wenn die Regel keine Auswertungsergebnisse gemeldet hat.
   - Keine Ressourcen im Gültigkeitsbereich — Ihre aufgezeichneten AWS Ressourcen AWS Config können nicht anhand dieser Regel bewertet werden, da sich keine Ihrer Ressourcen innerhalb des Gültigkeitsbereichs der Regel befindet. Um Bewertungsergebnisse zu erhalten, bearbeiten Sie die Regel und ändern Sie ihren Geltungsbereich, oder fügen Sie mithilfe der Einstellungsseite Ressourcen für AWS Config die Aufzeichnung hinzu.

- Evaluations failed (Auswertungen fehlgeschlagen) – Weitere Informationen, mit denen Sie das Problem bestimmen können, finden Sie, indem Sie den Regelnamen auswählen und die Detailseite öffnen, um die Fehlermeldung anzuzeigen.

Regeln hinzufügen (AWS SDKs)

Hinzufügen von Regeln

Die folgenden Code-Beispiele zeigen, wie `PutConfigRule` verwendet wird.

CLI

AWS CLI

So fügen Sie eine AWS verwaltete Konfigurationsregel hinzu

Der folgende Befehl stellt JSON-Code zum Hinzufügen einer AWS verwalteten Config-Regel bereit:

```
aws configservice put-config-rule --config-rule file://
RequiredTagsForEC2Instances.json
```

`RequiredTagsForEC2Instances.jsonist` eine JSON-Datei, die die Regelkonfiguration enthält:

```
{
  "ConfigRuleName": "RequiredTagsForEC2Instances",
  "Description": "Checks whether the CostCenter and Owner tags are applied to EC2
 instances.",
  "Scope": {
    "ComplianceResourceTypes": [
      "AWS::EC2::Instance"
    ]
  },
  "Source": {
    "Owner": "AWS",
    "SourceIdentifier": "REQUIRED_TAGS"
  },
  "InputParameters": "{\"tag1Key\":\"CostCenter\",\"tag2Key\":\"Owner\"}"
}
```

Für das `ComplianceResourceTypes` Attribut beschränkt dieser JSON-Code den Bereich auf Ressourcen des `AWS::EC2::Instance` Typs, sodass AWS Config nur EC2 Instanzen anhand der Regel auswertet. Da es sich bei der Regel um eine verwaltete Regel handelt, ist das `Owner` Attribut auf festgelegt`AWS`, und das `SourceIdentifier` Attribut ist auf den Regelbezeichner, festgelegt`REQUIRED_TAGS`. Für das `InputParameters` Attribut werden die Tag-Schlüssel, die die Regel benötigt`Owner`, `CostCenter` und, angegeben.

Wenn der Befehl erfolgreich ist, gibt AWS Config keine Ausgabe zurück. Um die Regelkonfiguration zu überprüfen, führen Sie den describe-config-rules Befehl aus und geben Sie den Regelnamen an.

So fügen Sie eine vom Kunden verwaltete Konfigurationsregel hinzu

Der folgende Befehl stellt JSON-Code zum Hinzufügen einer vom Kunden verwalteten Konfigurationsregel bereit:

```
aws configservice put-config-rule --config-rule file://
InstanceTypesAreT2micro.json
```

`InstanceTypesAreT2micro.jsonist` eine JSON-Datei, die die Regelkonfiguration enthält:

```
{
  "ConfigRuleName": "InstanceTypesAreT2micro",
  "Description": "Evaluates whether EC2 instances are the t2.micro type.",
  "Scope": {
    "ComplianceResourceTypes": [
      "AWS::EC2::Instance"
    ]
  },
  "Source": {
    "Owner": "CUSTOM_LAMBDA",
    "SourceIdentifier": "arn:aws:lambda:us-
east-1:123456789012:function:InstanceTypeCheck",
    "SourceDetails": [
      {
        "EventSource": "aws.config",
        "MessageType": "ConfigurationItemChangeNotification"
      }
    ]
  },
  "InputParameters": "{\"desiredInstanceType\":\"t2.micro\"}"
```

```
}
```

Für das `ComplianceResourceTypes` Attribut beschränkt dieser JSON-Code den Bereich auf Ressourcen des `AWS::EC2::Instance` Typs, sodass AWS Config nur EC2 Instanzen anhand der Regel auswertet. Da es sich bei dieser Regel um eine vom Kunden verwaltete Regel handelt`CUSTOM_LAMBDA`, ist das `Owner` Attribut auf und das `SourceIdentifier` Attribut auf den ARN der AWS Lambda-Funktion gesetzt. Das `SourceDetails` Objekt ist erforderlich. Die für das `InputParameters` Attribut angegebenen Parameter werden an die AWS Lambda-Funktion übergeben, wenn AWS Config sie aufruft, um Ressourcen anhand der Regel auszuwerten.

Wenn der Befehl erfolgreich ist, gibt AWS Config keine Ausgabe zurück. Um die Regelkonfiguration zu überprüfen, führen Sie den describe-config-rules Befehl aus und geben Sie den Regelnamen an.

- Einzelheiten zur API finden Sie PutConfigRuleunter AWS CLI Befehlsreferenz.

Python

SDK für Python (Boto3)

> **Note**
>
> Es gibt noch mehr dazu GitHub. Hier finden Sie das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel- einrichten und ausführen.

```
class ConfigWrapper:
    """
    Encapsulates AWS Config functions.
    """

    def __init__(self, config_client):
        """
        :param config_client: A Boto3 AWS Config client.
        """
        self.config_client = config_client


    def put_config_rule(self, rule_name):
```

```
        """
        Sets a configuration rule that prohibits making Amazon S3 buckets
publicly
        readable.

        :param rule_name: The name to give the rule.
        """
        try:
            self.config_client.put_config_rule(
                ConfigRule={
                    "ConfigRuleName": rule_name,
                    "Description": "S3 Public Read Prohibited Bucket Rule",
                    "Scope": {
                        "ComplianceResourceTypes": [
                            "AWS::S3::Bucket",
                        ],
                    },
                    "Source": {
                        "Owner": "AWS",
                        "SourceIdentifier": "S3_BUCKET_PUBLIC_READ_PROHIBITED",
                    },
                    "InputParameters": "{}",
                    "ConfigRuleState": "ACTIVE",
                }
            )
            logger.info("Created configuration rule %s.", rule_name)
        except ClientError:
            logger.exception("Couldn't create configuration rule %s.", rule_name)
            raise
```

- Einzelheiten zur API finden Sie PutConfigRulein AWS SDK for Python (Boto3) API Reference.

AWS Config Regeln aktualisieren

Sie können die AWS Config Konsole oder die verwenden AWS SDKs , um Ihre Regeln zu aktualisieren.

Themen

- Regeln aktualisieren (Konsole)
- Regeln aktualisieren ()AWS SDKs

Regeln aktualisieren (Konsole)

Auf der Seite Regeln werden Ihre Regeln und deren aktuelle Compliance-Ergebnisse in einer Tabelle dargestellt. Das Ergebnis für jede Regel lautet Evaluierung... bis die Bewertung Ihrer Ressourcen anhand der Regel AWS Config abgeschlossen ist. Sie können die Ergebnisse über die Aktualisieren-Schaltfläche aktualisieren. Wenn die AWS Config Evaluierungen abgeschlossen sind, können Sie sehen, welche Regeln und Ressourcentypen den Anforderungen entsprechen oder nicht. Weitere Informationen finden Sie unter Compliance-Informationen und Bewertungsergebnisse für Ihre AWS Ressourcen anzeigen mit AWS Config.

Aktualisieren von Regeln

So aktualisieren Sie eine Regel

1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die AWS Config Konsole zu https://console.aws.amazon.com/config/Hause.
2. Vergewissern Sie sich im AWS Management Console Menü, dass die Regionsauswahl auf eine Region eingestellt ist, die AWS Config Regeln unterstützt. Die Liste der unterstützten Regionen finden Sie unter AWS Config -Regionen und -Endpunkte im Allgemeine Amazon Web Services-Referenz.
3. Klicken Sie im linken Navigationsbereich auf die Option Regeln.
4. Wählen Sie eine Regel aus und klicken Sie auf Regel bearbeiten für die Regel, die aktualisiert werden soll.
5. Bearbeiten Sie die Einstellungen auf der Seite Regel bearbeiten, um Ihre Regel nach Bedarf zu ändern.
6. Wählen Sie Speichern.

Regeln aktualisieren ()AWS SDKs

Aktualisieren von Regeln

Wenn Sie eine Regel aktualisieren, die Sie zuvor hinzugefügt haben, können Sie die Regel mit `ConfigRuleName`, `ConfigRuleId` oder `ConfigRuleArn` im `ConfigRule`-Datentyp angeben, den

Sie in dieser Anforderung verwenden. Sie verwenden denselben `PutConfigRule` Befehl, den Sie beim Hinzufügen einer Regel verwenden.

Die folgenden Code-Beispiele zeigen, wie `PutConfigRule` verwendet wird.

CLI

AWS CLI

So fügen Sie eine AWS verwaltete Konfigurationsregel hinzu

Der folgende Befehl stellt JSON-Code zum Hinzufügen einer AWS verwalteten Config-Regel bereit:

```
aws configservice put-config-rule --config-rule file://
RequiredTagsForEC2Instances.json
```

`RequiredTagsForEC2Instances.jsonist` eine JSON-Datei, die die Regelkonfiguration enthält:

```
{
  "ConfigRuleName": "RequiredTagsForEC2Instances",
  "Description": "Checks whether the CostCenter and Owner tags are applied to EC2
 instances.",
  "Scope": {
    "ComplianceResourceTypes": [
      "AWS::EC2::Instance"
    ]
  },
  "Source": {
    "Owner": "AWS",
    "SourceIdentifier": "REQUIRED_TAGS"
  },
  "InputParameters": "{\"tag1Key\":\"CostCenter\",\"tag2Key\":\"Owner\"}"
}
```

Für das `ComplianceResourceTypes` Attribut beschränkt dieser JSON-Code den Bereich auf Ressourcen des `AWS::EC2::Instance` Typs, sodass AWS Config nur EC2 Instanzen anhand der Regel auswertet. Da es sich bei der Regel um eine verwaltete Regel handelt, ist das `Owner` Attribut auf festgelegt`AWS`, und das `SourceIdentifier` Attribut ist auf den Regelbezeichner, festgelegt`REQUIRED_TAGS`. Für das `InputParameters` Attribut werden die Tag-Schlüssel, die die Regel benötigt`Owner`, `CostCenter` und, angegeben.

Wenn der Befehl erfolgreich ist, gibt AWS Config keine Ausgabe zurück. Um die Regelkonfiguration zu überprüfen, führen Sie den describe-config-rules Befehl aus und geben Sie den Regelnamen an.

So fügen Sie eine vom Kunden verwaltete Konfigurationsregel hinzu

Der folgende Befehl stellt JSON-Code zum Hinzufügen einer vom Kunden verwalteten Konfigurationsregel bereit:

```
aws configservice put-config-rule --config-rule file://
InstanceTypesAreT2micro.json
```

`InstanceTypesAreT2micro.jsonist` eine JSON-Datei, die die Regelkonfiguration enthält:

```
{
  "ConfigRuleName": "InstanceTypesAreT2micro",
  "Description": "Evaluates whether EC2 instances are the t2.micro type.",
  "Scope": {
    "ComplianceResourceTypes": [
      "AWS::EC2::Instance"
    ]
  },
  "Source": {
    "Owner": "CUSTOM_LAMBDA",
    "SourceIdentifier": "arn:aws:lambda:us-
east-1:123456789012:function:InstanceTypeCheck",
    "SourceDetails": [
      {
        "EventSource": "aws.config",
        "MessageType": "ConfigurationItemChangeNotification"
      }
    ]
  },
  "InputParameters": "{\"desiredInstanceType\":\"t2.micro\"}"
}
```

Für das `ComplianceResourceTypes` Attribut beschränkt dieser JSON-Code den Bereich auf Ressourcen des `AWS::EC2::Instance` Typs, sodass AWS Config nur EC2 Instanzen anhand der Regel auswertet. Da es sich bei dieser Regel um eine vom Kunden verwaltete Regel handelt`CUSTOM_LAMBDA`, ist das `Owner` Attribut auf und das `SourceIdentifier` Attribut auf den ARN der AWS Lambda-Funktion gesetzt. Das `SourceDetails` Objekt ist

erforderlich. Die für das `InputParameters` Attribut angegebenen Parameter werden an die AWS Lambda-Funktion übergeben, wenn AWS Config sie aufruft, um Ressourcen anhand der Regel auszuwerten.

Wenn der Befehl erfolgreich ist, gibt AWS Config keine Ausgabe zurück. Um die Regelkonfiguration zu überprüfen, führen Sie den describe-config-rules Befehl aus und geben Sie den Regelnamen an.

- Einzelheiten zur API finden Sie PutConfigRuleunter AWS CLI Befehlsreferenz.

Python

SDK für Python (Boto3)

> **Note**
>
> Es gibt noch mehr dazu GitHub. Hier finden Sie das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel- einrichten und ausführen.

```
class ConfigWrapper:
    """
    Encapsulates AWS Config functions.
    """

    def __init__(self, config_client):
        """
        :param config_client: A Boto3 AWS Config client.
        """
        self.config_client = config_client


    def put_config_rule(self, rule_name):
        """
        Sets a configuration rule that prohibits making Amazon S3 buckets
 publicly
        readable.

        :param rule_name: The name to give the rule.
        """
        try:
            self.config_client.put_config_rule(
```

```
                ConfigRule={
                    "ConfigRuleName": rule_name,
                    "Description": "S3 Public Read Prohibited Bucket Rule",
                    "Scope": {
                        "ComplianceResourceTypes": [
                            "AWS::S3::Bucket",
                        ],
                    },
                    "Source": {
                        "Owner": "AWS",
                        "SourceIdentifier": "S3_BUCKET_PUBLIC_READ_PROHIBITED",
                    },
                    "InputParameters": "{}",
                    "ConfigRuleState": "ACTIVE",
                }
            )
            logger.info("Created configuration rule %s.", rule_name)
        except ClientError:
            logger.exception("Couldn't create configuration rule %s.", rule_name)
            raise
```

- Einzelheiten zur API finden Sie PutConfigRulein AWS SDK for Python (Boto3) API Reference.

AWS Config Regeln löschen

Sie können die AWS Config Konsole oder die verwenden AWS SDKs , um Ihre Regeln zu löschen.

Themen

- Überlegungen
- Regeln löschen (Konsole)
- Regeln löschen ()AWS SDKs

Überlegungen

Empfehlung: Erwägen Sie, den **`AWS::Config::ResourceCompliance`** Ressourcentyp aus der Aufzeichnung auszuschließen, bevor Sie Regeln löschen

Durch das Löschen von Regeln werden Konfigurationselemente (CIs) erstelltAWS::Config::ResourceCompliance, die sich auf Ihre Kosten für den Konfigurationsrekorder auswirken können. Wenn Sie Regeln löschen, die eine große Anzahl von Ressourcentypen auswerten, kann dies zu einem Anstieg der Anzahl der CIs aufgezeichneten Ressourcentypen führen.

Um die damit verbundenen Kosten zu vermeiden, können Sie die Aufzeichnung für den AWS::Config::ResourceCompliance Ressourcentyp deaktivieren, bevor Sie Regeln löschen, und die Aufzeichnung erneut aktivieren, nachdem die Regeln gelöscht wurden.

Da das Löschen von Regeln jedoch ein asynchroner Vorgang ist, kann es eine Stunde oder länger dauern, bis er abgeschlossen ist. Während der ZeitAWS::Config::ResourceCompliance, für die die Aufzeichnung deaktiviert ist, werden Regelauswertungen nicht im Verlauf der zugehörigen Ressource aufgezeichnet.

Regeln löschen (Konsole)

Auf der Seite Regeln werden Ihre Regeln und deren aktuelle Compliance-Ergebnisse in einer Tabelle dargestellt. Das Ergebnis für jede Regel lautet Evaluierung... bis die Bewertung Ihrer Ressourcen anhand der Regel AWS Config abgeschlossen ist. Sie können die Ergebnisse über die Aktualisieren-Schaltfläche aktualisieren. Wenn die AWS Config Evaluierungen abgeschlossen sind, können Sie sehen, welche Regeln und Ressourcentypen den Anforderungen entsprechen oder nicht. Weitere Informationen finden Sie unter Compliance-Informationen und Bewertungsergebnisse für Ihre AWS Ressourcen anzeigen mit AWS Config.

> **Note**
>
> AWS Config wertet nur die Ressourcentypen aus, die gerade aufgezeichnet werden. Wenn Sie beispielsweise die cloudtrail-aktivierte Regel hinzufügen, aber den CloudTrail Trail-Ressourcentyp nicht aufzeichnen, AWS Config kann nicht bewertet werden, ob die Trails in Ihrem Konto konform sind oder nicht. Weitere Informationen finden Sie unter AWS Ressourcen aufzeichnen mit AWS Config.

Löschen von Regeln

So löschen Sie eine Regel

1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die AWS Config Konsole zu Hause. https://console.aws.amazon.com/config/
2. Vergewissern Sie sich im AWS Management Console Menü, dass die Regionsauswahl auf eine Region eingestellt ist, die AWS Config Regeln unterstützt. Die Liste der unterstützten Regionen finden Sie unter AWS Config -Regionen und -Endpunkte im Allgemeine Amazon Web Services-Referenz.
3. Klicken Sie im linken Navigationsbereich auf die Option Regeln.
4. Wählen Sie in der Tabelle die Regel aus, die Sie löschen möchten.
5. Wählen Sie in der Dropdown-Liste Aktionen die Option Regel löschen aus.
6. Wenn Sie dazu aufgefordert werden, geben Sie „Delete“ ein (Groß- und Kleinschreibung beachten) und wählen Sie dann Löschen aus.

Regeln löschen ()AWS SDKs

Löschen von Regeln

Die folgenden Code-Beispiele zeigen, wie `DeleteConfigRule` verwendet wird.

CLI

AWS CLI

Um eine AWS Config-Regel zu löschen

Der folgende Befehl löscht eine AWS Config-Regel mit dem Namen`MyConfigRule`:

```
aws configservice delete-config-rule --config-rule-name MyConfigRule
```

- Einzelheiten zur API finden Sie DeleteConfigRulein der AWS CLI Befehlsreferenz.

Python

SDK für Python (Boto3)

> **Note**
>
> Es gibt noch mehr dazu GitHub. Hier finden Sie das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel- einrichten und ausführen.

```
class ConfigWrapper:
    """
    Encapsulates AWS Config functions.
    """

    def __init__(self, config_client):
        """
        :param config_client: A Boto3 AWS Config client.
        """
        self.config_client = config_client


    def delete_config_rule(self, rule_name):
        """
        Delete the specified rule.

        :param rule_name: The name of the rule to delete.
        """
        try:
            self.config_client.delete_config_rule(ConfigRuleName=rule_name)
            logger.info("Deleted rule %s.", rule_name)
        except ClientError:
            logger.exception("Couldn't delete rule %s.", rule_name)
            raise
```

- Einzelheiten zur API finden Sie DeleteConfigRulein AWS SDK for Python (Boto3) API Reference.

Details und Compliance-Informationen zu Ihren AWS Config Regeln anzeigen

> **Important**
>
> Für eine genaue Berichterstattung über den Compliance-Status müssen Sie den Ressourcentyp `AWS::Config::ResourceCompliance` aufzeichnen. Weitere Informationen finden Sie unter AWS Aufzeichnungsressourcen.

Sie können die AWS Config Konsole oder die verwenden AWS SDKs , um Ihre Regeln einzusehen.

Themen

- Regeln anzeigen (Konsole)
- Regeln anzeigen (AWS SDKs)

Regeln anzeigen (Konsole)

Auf der Seite Regeln werden Ihre Regeln und deren aktuelle Compliance-Ergebnisse in einer Tabelle dargestellt. Das Ergebnis für jede Regel lautet Evaluierung... bis die Bewertung Ihrer Ressourcen anhand der Regel AWS Config abgeschlossen ist. Sie können die Ergebnisse über die Aktualisieren-Schaltfläche aktualisieren. Wenn die AWS Config Evaluierungen abgeschlossen sind, können Sie sehen, welche Regeln und Ressourcentypen den Anforderungen entsprechen oder nicht. Weitere Informationen finden Sie unter Compliance-Informationen und Bewertungsergebnisse für Ihre AWS Ressourcen anzeigen mit AWS Config.

> **Note**
>
> AWS Config wertet nur die Ressourcentypen aus, die gerade aufgezeichnet werden. Wenn Sie beispielsweise die cloudtrail-aktivierte Regel hinzufügen, aber den CloudTrail Trail-Ressourcentyp nicht aufzeichnen, AWS Config kann nicht bewertet werden, ob die Trails in Ihrem Konto konform sind oder nicht. Weitere Informationen finden Sie unter AWS Ressourcen aufzeichnen mit AWS Config.

Anzeigen von Regeln

So zeigen Sie Ihre Regeln an

1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die AWS Config Konsole zu Hause. https://console.aws.amazon.com/config/
2. Vergewissern Sie sich im AWS Management Console Menü, dass die Regionsauswahl auf eine Region eingestellt ist, die AWS Config Regeln unterstützt. Die Liste der unterstützten Regionen finden Sie unter AWS Config -Regionen und -Endpunkte im Allgemeine Amazon Web Services-Referenz.
3. Klicken Sie im linken Navigationsbereich auf die Option Regeln.
4. Auf der Seite Regeln werden alle Regeln angezeigt, die sich derzeit in Ihrem AWS-Konto befinden. Es werden der Name, die zugehörigen Korrekturmaßnahmen und der Compliance-Status jeder Regel aufgeführt.
   - Klicken Sie auf Add Rule (Regel hinzufügen), um mit der Regelerstellung zu beginnen.
   - Wählen Sie eine Regel aus, um ihre Einstellungen zu sehen, oder wählen Sie eine Regel aus und klicken Sie auf Details anzeigen.
   - Zeigen Sie die Compliance-Status der Regel bei der Auswertung Ihrer Ressourcen an.
   - Wählen Sie eine Regel aus und klicken Sie auf Regel bearbeiten, um die Konfigurationseinstellungen der Regel zu ändern und eine Korrekturmaßnahme für eine nicht konforme Regel festzulegen.

Regeln anzeigen (AWS SDKs)

Details zu Ihren Regeln anzeigen

Die folgenden Code-Beispiele zeigen, wie `DescribeConfigRules` verwendet wird.

CLI

AWS CLI

Um Details für eine AWS Config-Regel abzurufen

Der folgende Befehl gibt Details für eine AWS Config-Regel mit dem Namen zurück`InstanceTypesAreT2micro`:

```
aws configservice describe-config-rules --config-rule-
names InstanceTypesAreT2micro
```

Ausgabe:

```
{
    "ConfigRules": [
        {
            "ConfigRuleState": "ACTIVE",
            "Description": "Evaluates whether EC2 instances are the t2.micro
 type.",
            "ConfigRuleName": "InstanceTypesAreT2micro",
            "ConfigRuleArn": "arn:aws:config:us-east-1:123456789012:config-rule/
config-rule-abcdef",
            "Source": {
                "Owner": "CUSTOM_LAMBDA",
                "SourceIdentifier": "arn:aws:lambda:us-
east-1:123456789012:function:InstanceTypeCheck",
                "SourceDetails": [
                    {
                        "EventSource": "aws.config",
                        "MessageType": "ConfigurationItemChangeNotification"
                    }
                ]
            },
            "InputParameters": "{\"desiredInstanceType\":\"t2.micro\"}",
            "Scope": {
                "ComplianceResourceTypes": [
                    "AWS::EC2::Instance"
                ]
            },
            "ConfigRuleId": "config-rule-abcdef"
        }
    ]
}
```

- Einzelheiten zur API finden Sie DescribeConfigRulesin der AWS CLI Befehlsreferenz.

PowerShell

Tools für PowerShell V4

Beispiel 1: In diesem Beispiel werden die Konfigurationsregeln für das Konto mit ausgewählten Eigenschaften aufgeführt.

```
Get-CFGConfigRule | Select-Object ConfigRuleName, ConfigRuleId, ConfigRuleArn,
 ConfigRuleState
```

Ausgabe:

```
ConfigRuleName                                     ConfigRuleId
 ConfigRuleArn
 ConfigRuleState
--------------                                     ------------
 -------------
 ---------------
ALB_REDIRECTION_CHECK                              config-rule-12iyn3
 arn:aws:config-service:eu-west-1:123456789012:config-rule/config-rule-12iyn3
 ACTIVE
access-keys-rotated                                config-rule-aospfr
 arn:aws:config-service:eu-west-1:123456789012:config-rule/config-rule-aospfr
 ACTIVE
autoscaling-group-elb-healthcheck-required         config-rule-cn1f2x
 arn:aws:config-service:eu-west-1:123456789012:config-rule/config-rule-cn1f2x
 ACTIVE
```

- Einzelheiten zur API finden Sie unter DescribeConfigRules AWS -Tools für PowerShellCmdlet-Referenz (V4).

Python

SDK für Python (Boto3)

> **Note**
>
> Es gibt noch mehr dazu. GitHub Hier finden Sie das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel- einrichten und ausführen.

```
class ConfigWrapper:
    """
    Encapsulates AWS Config functions.
    """

    def __init__(self, config_client):
        """
        :param config_client: A Boto3 AWS Config client.
        """
        self.config_client = config_client


    def describe_config_rule(self, rule_name):
        """
        Gets data for the specified rule.

        :param rule_name: The name of the rule to retrieve.
        :return: The rule data.
        """
        try:
            response = self.config_client.describe_config_rules(
                ConfigRuleNames=[rule_name]
            )
            rule = response["ConfigRules"]
            logger.info("Got data for rule %s.", rule_name)
        except ClientError:
            logger.exception("Couldn't get data for rule %s.", rule_name)
            raise
        else:
            return rule
```

- Einzelheiten zur API finden Sie DescribeConfigRulesin AWS SDK for Python (Boto3) API Reference.

Konformitätsinformationen für Ihre Regeln anzeigen

Die folgenden Code-Beispiele zeigen, wie `DescribeComplianceByConfigRule` verwendet wird.

CLI

AWS CLI

Um Compliance-Informationen für Ihre AWS Config-Regeln zu erhalten

Der folgende Befehl gibt Konformitätsinformationen für jede AWS Config-Regel zurück, gegen die eine oder mehrere AWS Ressourcen verstoßen:

```
aws configservice describe-compliance-by-config-rule --compliance-
types NON_COMPLIANT
```

In der Ausgabe gibt der Wert für jedes `CappedCount` Attribut an, wie viele Ressourcen der zugehörigen Regel nicht entsprechen. Die folgende Ausgabe gibt beispielsweise an, dass 3 Ressourcen der genannten Regel nicht entsprechen`InstanceTypesAreT2micro`.

Ausgabe:

```
{
    "ComplianceByConfigRules": [
        {
            "Compliance": {
                "ComplianceContributorCount": {
                    "CappedCount": 3,
                    "CapExceeded": false
                },
                "ComplianceType": "NON_COMPLIANT"
            },
            "ConfigRuleName": "InstanceTypesAreT2micro"
        },
        {
            "Compliance": {
                "ComplianceContributorCount": {
                    "CappedCount": 10,
                    "CapExceeded": false
                },
                "ComplianceType": "NON_COMPLIANT"
            },
            "ConfigRuleName": "RequiredTagsForVolumes"
        }
    ]
}
```

- Einzelheiten zur API finden Sie DescribeComplianceByConfigRuleunter AWS CLI Befehlsreferenz.

PowerShell

Tools für PowerShell V4

Beispiel 1: In diesem Beispiel werden Konformitätsdetails für die Regel abgerufen ebs-optimized-instance, für die es keine aktuellen Bewertungsergebnisse für die Regel gibt. Daher wird INSUFFICIENT_DATA zurückgegeben

```
(Get-CFGComplianceByConfigRule -ConfigRuleName ebs-optimized-instance).Compliance
```

Ausgabe:

```
ComplianceContributorCount ComplianceType
-------------------------- --------------
                           INSUFFICIENT_DATA
```

Beispiel 2: Dieses Beispiel gibt die Anzahl der nicht konformen Ressourcen für die Regel ALB_HTTP_TO_HTTPS_REDIRECTION_CHECK zurück.

```
(Get-CFGComplianceByConfigRule -ConfigRuleName
 ALB_HTTP_TO_HTTPS_REDIRECTION_CHECK -ComplianceType
 NON_COMPLIANT).Compliance.ComplianceContributorCount
```

Ausgabe:

```
CapExceeded CappedCount
----------- -----------
False       2
```

- Einzelheiten AWS -Tools für PowerShell zur DescribeComplianceByConfigRuleAPI finden Sie unter Cmdlet-Referenz (V4).

Die Konformitätsübersicht für Ihre Regeln anzeigen

Die folgenden Code-Beispiele zeigen, wie `GetComplianceSummaryByConfigRule` verwendet wird.

CLI

AWS CLI

Um die Konformitätsübersicht für Ihre AWS Config-Regeln abzurufen

Der folgende Befehl gibt die Anzahl der Regeln zurück, die konform sind, und die Anzahl der Regeln, die nicht konform sind:

```
aws configservice get-compliance-summary-by-config-rule
```

In der Ausgabe gibt der Wert für jedes `CappedCount` Attribut an, wie viele Regeln konform oder nicht konform sind.

Ausgabe:

```
{
    "ComplianceSummary": {
        "NonCompliantResourceCount": {
            "CappedCount": 3,
            "CapExceeded": false
        },
        "ComplianceSummaryTimestamp": 1452204131.493,
        "CompliantResourceCount": {
            "CappedCount": 2,
            "CapExceeded": false
        }
    }
}
```

- Einzelheiten zur API finden Sie unter GetComplianceSummaryByConfigRule AWS CLIBefehlsreferenz.

PowerShell

Tools für PowerShell V4

Beispiel 1: Dieses Beispiel gibt die Anzahl der Config-Regeln zurück, die nicht konform sind.

```
Get-CFGComplianceSummaryByConfigRule -Select
 ComplianceSummary.NonCompliantResourceCount
```

Ausgabe:

```
CapExceeded CappedCount
----------- -----------
False       9
```

- Einzelheiten zur API finden Sie unter GetComplianceSummaryByConfigRule AWS -Tools für PowerShellCmdlet-Referenz (V4).

Die Evaluierungsergebnisse für Ihre Regeln anzeigen

Die folgenden Code-Beispiele zeigen, wie `GetComplianceDetailsByConfigRule` verwendet wird.

CLI

AWS CLI

Um die Auswertungsergebnisse für eine AWS Config-Regel abzurufen

Der folgende Befehl gibt die Auswertungsergebnisse für alle Ressourcen zurück, die nicht einer AWS Config-Regel mit dem Namen entsprechen`InstanceTypesAreT2micro`:

```
aws configservice get-compliance-details-by-config-rule --config-rule-
name InstanceTypesAreT2micro --compliance-types NON_COMPLIANT
```

Ausgabe:

```
{
    "EvaluationResults": [
        {
            "EvaluationResultIdentifier": {
                "OrderingTimestamp": 1450314635.065,
                "EvaluationResultQualifier": {
                    "ResourceType": "AWS::EC2::Instance",
                    "ResourceId": "i-1a2b3c4d",
                    "ConfigRuleName": "InstanceTypesAreT2micro"
                }
            },
            "ResultRecordedTime": 1450314645.261,
            "ConfigRuleInvokedTime": 1450314642.948,
            "ComplianceType": "NON_COMPLIANT"
```

```
        },
        {
            "EvaluationResultIdentifier": {
                "OrderingTimestamp": 1450314635.065,
                "EvaluationResultQualifier": {
                    "ResourceType": "AWS::EC2::Instance",
                    "ResourceId": "i-2a2b3c4d",
                    "ConfigRuleName": "InstanceTypesAreT2micro"
                }
            },
            "ResultRecordedTime": 1450314645.18,
            "ConfigRuleInvokedTime": 1450314642.902,
            "ComplianceType": "NON_COMPLIANT"
        },
        {
            "EvaluationResultIdentifier": {
                "OrderingTimestamp": 1450314635.065,
                "EvaluationResultQualifier": {
                    "ResourceType": "AWS::EC2::Instance",
                    "ResourceId": "i-3a2b3c4d",
                    "ConfigRuleName": "InstanceTypesAreT2micro"
                }
            },
            "ResultRecordedTime": 1450314643.346,
            "ConfigRuleInvokedTime": 1450314643.124,
            "ComplianceType": "NON_COMPLIANT"
        }
    ]
}
```

- Einzelheiten zur API finden Sie GetComplianceDetailsByConfigRulein der AWS CLI Befehlsreferenz.

PowerShell

Tools für PowerShell V4

Beispiel 1: In diesem Beispiel werden die Auswertungsergebnisse für die Regel abgerufen access-keys-rotated und die Ausgabe nach Konformitätstyp gruppiert zurückgegeben

```
Get-CFGComplianceDetailsByConfigRule -ConfigRuleName access-keys-rotated | Group-
Object ComplianceType
```

Ausgabe:

```
Count Name                      Group
----- ----                      -----
    2 COMPLIANT                 {Amazon.ConfigService.Model.EvaluationResult,
 Amazon.ConfigService.Model.EvaluationResult}
    5 NON_COMPLIANT             {Amazon.ConfigService.Model.EvaluationResult,
 Amazon.ConfigService.Model.EvaluationResult,
 Amazon.ConfigService.Model.EvaluationRes...
```

Beispiel 2: In diesem Beispiel werden Konformitätsdetails für die Regel access-keys-rotated für COMPLIANT-Ressourcen abgefragt.

```
Get-CFGComplianceDetailsByConfigRule -ConfigRuleName access-
keys-rotated -ComplianceType COMPLIANT | ForEach-Object
 {$_.EvaluationResultIdentifier.EvaluationResultQualifier}
```

Ausgabe:

```
ConfigRuleName      ResourceId            ResourceType
--------------      ----------            ------------
access-keys-rotated BCAB1CDJ2LITAPVEW3JAH AWS::IAM::User
access-keys-rotated BCAB1CDJ2LITL3EHREM4Q AWS::IAM::User
```

- Einzelheiten zur API finden Sie unter GetComplianceDetailsByConfigRule AWS -Tools für PowerShellCmdlet-Referenz (V4).

Proaktive Evaluierung für AWS Config Regeln aktivieren

Sie können die AWS Config Konsole oder die verwenden AWS SDKs , um proaktive Bewertungsregeln zu aktivieren. Eine Liste der Ressourcentypen und verwalteten Regeln, die die proaktive Evaluierung unterstützen, finden Sie unter Komponenten einer Regel | Evaluierungsmodi.

Themen

- Proaktive Evaluierung aktivieren (Konsole)
- Proaktive Evaluierung aktivieren ()AWS SDKs

Proaktive Evaluierung aktivieren (Konsole)

Auf der Seite Regeln werden Ihre Regeln und deren aktuelle Compliance-Ergebnisse in einer Tabelle dargestellt. Das Ergebnis für jede Regel lautet Evaluierung... bis die Bewertung Ihrer Ressourcen anhand der Regel AWS Config abgeschlossen ist. Sie können die Ergebnisse über die Aktualisieren-Schaltfläche aktualisieren.

Wenn die AWS Config Evaluierungen abgeschlossen sind, können Sie sehen, welche Regeln und Ressourcentypen den Anforderungen entsprechen oder nicht. Weitere Informationen finden Sie unter Compliance-Informationen und Bewertungsergebnisse für Ihre AWS Ressourcen anzeigen mit AWS Config.

> **Note**
>
> AWS Config wertet nur die Ressourcentypen aus, die gerade aufgezeichnet werden. Wenn Sie beispielsweise die cloudtrail-aktivierte Regel hinzufügen, aber den CloudTrail Trail-Ressourcentyp nicht aufzeichnen, AWS Config kann nicht bewertet werden, ob die Trails in Ihrem Konto konform sind oder nicht. Weitere Informationen finden Sie unter AWS Ressourcen aufzeichnen mit AWS Config.

Aktivieren der proaktiven Auswertung

Verwenden Sie die proaktive Auswertung, um Ressourcen vor der Bereitstellung auszuwerten. Auf diese Weise können Sie beurteilen, ob ein Satz von Ressourceneigenschaften, wenn er zur Definition einer AWS Ressource verwendet würde, angesichts der proaktiven Regeln, die Sie in Ihrem Konto in Ihrer Region haben, als KONFORM oder NICHT KONFORM gelten würde.

Das Ressourcentypschema gibt die Eigenschaften einer Ressource an. Sie finden das Ressourcentypschema in "AWS public extensions" in der AWS CloudFormation Registrierung oder mit dem folgenden CLI-Befehl:

```
aws cloudformation describe-type --type-name "AWS::S3::Bucket" --type RESOURCE
```

Weitere Informationen finden Sie unter Verwaltung von Erweiterungen über die AWS CloudFormation Registrierung und Referenz zu AWS Ressourcen- und Eigenschaftstypen im AWS CloudFormation Benutzerhandbuch.

> **Note**
>
> Durch proaktive Regeln werden keine Ressourcen korrigiert, die als NON_COMPLIANT gekennzeichnet sind, und sie verhindern auch nicht, dass diese bereitgestellt werden.

So aktivieren Sie die proaktive Auswertung

1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die AWS Config Konsole zu https://console.aws.amazon.com/config/Hause.
2. Vergewissern Sie sich im AWS Management Console Menü, dass die Regionsauswahl auf eine Region eingestellt ist, die AWS Config Regeln unterstützt. Die Liste der unterstützten AWS - Regionen finden Sie unter AWS Config Regionen und -Endpunkte im Allgemeine Amazon Web Services-Referenz.
3. Klicken Sie im linken Navigationsbereich auf die Option Regeln. Eine Liste der verwalteten Regeln, die eine proaktive Evaluierung unterstützen, finden Sie unter Liste der AWS Config verwalteten Regeln nach Testmodus.
4. Wählen Sie eine Regel aus und klicken Sie auf Regel bearbeiten für die Regel, die aktualisiert werden soll.
5. Wählen Sie unter Auswertungsmodus die Option Proaktive Auswertung einschalten aus, damit Auswertungen der Konfigurationseinstellungen Ihrer Ressourcen ausgeführt werden können, bevor diese bereitgestellt werden.
6. Wählen Sie Speichern.

Nachdem Sie die proaktive Evaluierung aktiviert haben, können Sie mithilfe der StartResourceEvaluationAPI und GetResourceEvaluationSummaryder API überprüfen, ob die Ressourcen, die Sie in diesen Befehlen angeben, durch die proaktiven Regeln in Ihrem Konto in Ihrer Region als NON_COMPLIANT gekennzeichnet werden.

Beginnen Sie beispielsweise mit der API: StartResourceEvaluation

```
aws configservice start-resource-evaluation --evaluation-mode PROACTIVE
                --resource-details '{"ResourceId":"MY_RESOURCE_ID",
                                     "ResourceType":"AWS::RESOURCE::TYPE",

 "ResourceConfiguration":"RESOURCE_DEFINITION_AS_PER_THE_RESOURCE_CONFIGURATION_SCHEMA",
```

```
 "ResourceConfigurationSchemaType":"CFN_RESOURCE_SCHEMA"}'
```

Sie sollten die `ResourceEvaluationId` in der Ausgabe erhalten:

```
{
    "ResourceEvaluationId": "MY_RESOURCE_EVALUATION_ID"
}
```

Verwenden Sie dann `ResourceEvaluationId` zusammen mit der GetResourceEvaluationSummary API das, um das Evaluierungsergebnis zu überprüfen:

```
aws configservice get-resource-evaluation-summary
    --resource-evaluation-id MY_RESOURCE_EVALUATION_ID
```

Die Ausgabe sollte folgendermaßen oder ähnlich aussehen:

```
{
    "ResourceEvaluationId": "MY_RESOURCE_EVALUATION_ID",
    "EvaluationMode": "PROACTIVE",
    "EvaluationStatus": {
        "Status": "SUCCEEDED"
    },
    "EvaluationStartTimestamp": "2022-11-15T19:13:46.029000+00:00",
    "Compliance": "COMPLIANT",
    "ResourceDetails": {
        "ResourceId": "MY_RESOURCE_ID",
        "ResourceType": "AWS::RESOURCE::TYPE",
        "ResourceConfiguration":
 "RESOURCE_DEFINITION_AS_PER_THE_RESOURCE_CONFIGURATION_SCHEMA"
    }
}
```

Verwenden Sie die API, um zusätzliche Informationen zum Evaluierungsergebnis zu erhalten, z. B. welche Regel eine Ressource als NON_COMPLIANT gekennzeichnet hat. GetComplianceDetailsByResource

Proaktive Evaluierung aktivieren ()AWS SDKs

Aktivierung der proaktiven Bewertung (AWS CLI)

Verwenden Sie die proaktive Auswertung, um Ressourcen vor der Bereitstellung auszuwerten. Auf diese Weise können Sie auswerten, ob eine Reihe von Ressourceneigenschaften, wenn sie zur Definition einer AWS Ressource verwendet würden, angesichts der proaktiven Regeln, die Sie in Ihrem Konto in Ihrer Region haben, als KONFORM oder NICHT KONFORM gelten würde.

Das Ressourcentypschema gibt die Eigenschaften einer Ressource an. Sie finden das Ressourcentypschema in "AWS public extensions" in der AWS CloudFormation Registrierung oder mit dem folgenden CLI-Befehl:

```
aws cloudformation describe-type --type-name "AWS::S3::Bucket" --type RESOURCE
```

Weitere Informationen finden Sie unter Verwaltung von Erweiterungen über die AWS CloudFormation Registrierung und Referenz zu AWS Ressourcen- und Eigenschaftstypen im AWS CloudFormation Benutzerhandbuch.

> **Note**
>
> Durch proaktive Regeln werden keine Ressourcen korrigiert, die als NON_COMPLIANT gekennzeichnet sind, und sie verhindern auch nicht, dass diese bereitgestellt werden.

Aktivieren Sie die proaktive Auswertung wie folgt:

Verwenden Sie den `put-config-rule`-Befehl und aktivieren Sie `PROACTIVE` für`EvaluationModes`.

Nachdem Sie die proaktive Evaluierung aktiviert haben, können Sie mit dem start-resource-evaluationCLI-Befehl und dem get-resource-evaluation-summaryCLI-Befehl überprüfen, ob die Ressourcen, die Sie in diesen Befehlen angeben, durch die proaktiven Regeln in Ihrem Konto in Ihrer Region als NON_COMPLIANT gekennzeichnet werden.

Beginnen Sie z. B. mit dem start-resource-evaluation-Befehl:

```
aws configservice start-resource-evaluation --evaluation-mode PROACTIVE
```

```
                --resource-details '{"ResourceId":"MY_RESOURCE_ID",
                                     "ResourceType":"AWS::RESOURCE::TYPE",

 "ResourceConfiguration":"RESOURCE_DEFINITION_AS_PER_THE_RESOURCE_CONFIGURATION_SCHEMA",

 "ResourceConfigurationSchemaType":"CFN_RESOURCE_SCHEMA"}'
```

Sie sollten die `ResourceEvaluationId` in der Ausgabe erhalten:

```
{
    "ResourceEvaluationId": "MY_RESOURCE_EVALUATION_ID"
}
```

Verwenden Sie dann die `ResourceEvaluationId` mit get-resource-evaluation-summary, um das Auswertungsergebnis zu überprüfen:

```
aws configservice get-resource-evaluation-summary
    --resource-evaluation-id MY_RESOURCE_EVALUATION_ID
```

Die Ausgabe sollte folgendermaßen oder ähnlich aussehen:

```
{
    "ResourceEvaluationId": "MY_RESOURCE_EVALUATION_ID",
    "EvaluationMode": "PROACTIVE",
    "EvaluationStatus": {
        "Status": "SUCCEEDED"
    },
    "EvaluationStartTimestamp": "2022-11-15T19:13:46.029000+00:00",
    "Compliance": "COMPLIANT",
    "ResourceDetails": {
        "ResourceId": "MY_RESOURCE_ID",
        "ResourceType": "AWS::RESOURCE::TYPE",
        "ResourceConfiguration":
 "RESOURCE_DEFINITION_AS_PER_THE_RESOURCE_CONFIGURATION_SCHEMA"
    }
}
```

Verwenden Sie den CLI-Befehl get-compliance-details-by-resource, um zusätzliche Informationen zum Evaluierungsergebnis anzuzeigen, z. B. welche Regel eine Ressource als NON_COMPLIANT gekennzeichnet hat.

> **Note**
>
> Eine Liste der verwalteten Regeln, die die proaktive Evaluierung unterstützen, finden Sie unter Liste der AWS Config verwalteten Regeln nach Testmodus.

Aktivierung der proaktiven Evaluierung (API)

Verwenden Sie die proaktive Auswertung, um Ressourcen vor der Bereitstellung auszuwerten. Auf diese Weise können Sie beurteilen, ob eine Reihe von Ressourceneigenschaften, wenn sie zur Definition einer AWS Ressource verwendet würden, angesichts der proaktiven Regeln, die Sie in Ihrem Konto in Ihrer Region haben, als KONFORM oder NON_KONFORM gelten würde.

Das Ressourcentypschema gibt die Eigenschaften einer Ressource an. Sie finden das Ressourcentypschema in "AWS public extensions" in der AWS CloudFormation Registrierung oder mit dem folgenden CLI-Befehl:

```
aws cloudformation describe-type --type-name "AWS::S3::Bucket" --type RESOURCE
```

Weitere Informationen finden Sie unter Verwaltung von Erweiterungen über die AWS CloudFormation Registrierung und Referenz zu AWS Ressourcen- und Eigenschaftstypen im AWS CloudFormation Benutzerhandbuch.

> **Note**
>
> Durch proaktive Regeln werden keine Ressourcen korrigiert, die als NON_COMPLIANT gekennzeichnet sind, und sie verhindern auch nicht, dass diese bereitgestellt werden.

Aktivieren Sie die proaktive Auswertung für eine Regel wie folgt:

Verwenden Sie die PutConfigRuleAktion und aktivieren Sie sie `PROACTIVE` für`EvaluationModes`.

Nachdem Sie die proaktive Evaluierung aktiviert haben, können Sie mithilfe der StartResourceEvaluationAPI und GetResourceEvaluationSummaryder API überprüfen, ob die Ressourcen, die Sie in diesen Befehlen angeben, durch die proaktiven Regeln in Ihrem Konto in Ihrer Region als NON_COMPLIANT gekennzeichnet werden. Beginnen Sie beispielsweise mit der API: StartResourceEvaluation

```
aws configservice start-resource-evaluation --evaluation-mode PROACTIVE
```

```
                --resource-details '{"ResourceId":"MY_RESOURCE_ID",
                                     "ResourceType":"AWS::RESOURCE::TYPE",

 "ResourceConfiguration":"RESOURCE_DEFINITION_AS_PER_THE_RESOURCE_CONFIGURATION_SCHEMA",

 "ResourceConfigurationSchemaType":"CFN_RESOURCE_SCHEMA"}'
```

Sie sollten die `ResourceEvaluationId` in der Ausgabe erhalten:

```
{
    "ResourceEvaluationId": "MY_RESOURCE_EVALUATION_ID"
}
```

Verwenden Sie dann `ResourceEvaluationId` zusammen mit der GetResourceEvaluationSummary API das, um das Evaluierungsergebnis zu überprüfen:

```
aws configservice get-resource-evaluation-summary
    --resource-evaluation-id MY_RESOURCE_EVALUATION_ID
```

Die Ausgabe sollte folgendermaßen oder ähnlich aussehen:

```
{
    "ResourceEvaluationId": "MY_RESOURCE_EVALUATION_ID",
    "EvaluationMode": "PROACTIVE",
    "EvaluationStatus": {
        "Status": "SUCCEEDED"
    },
    "EvaluationStartTimestamp": "2022-11-15T19:13:46.029000+00:00",
    "Compliance": "COMPLIANT",
    "ResourceDetails": {
        "ResourceId": "MY_RESOURCE_ID",
        "ResourceType": "AWS::RESOURCE::TYPE",
        "ResourceConfiguration":
 "RESOURCE_DEFINITION_AS_PER_THE_RESOURCE_CONFIGURATION_SCHEMA"
    }
}
```

Verwenden Sie die API, um zusätzliche Informationen zum Evaluierungsergebnis zu erhalten, z. B. welche Regel eine Ressource als NON_COMPLIANT gekennzeichnet hat. GetComplianceDetailsByResource

> **Note**
>
> Eine Liste der verwalteten Regeln, die die proaktive Bewertung unterstützen, finden Sie unter Liste der AWS Config verwalteten Regeln nach Testmodus.

Senden von Regelauswertungen an Security Hub

Nachdem Sie eine AWS Config Regel hinzugefügt haben, können Sie Regelauswertungen auch an senden AWS Security Hub. Die Integration zwischen AWS Config und Security Hub ermöglicht es Ihnen, Regelauswertungen sowie andere Fehlkonfigurationen und Sicherheitsprobleme zu überprüfen und zu beheben.

Senden von Regelauswertungen an Security Hub

Um Regelauswertungen an Security Hub zu senden, müssen Sie zuerst eine AWS Config verwaltete oder benutzerdefinierte Regel einrichten AWS Security Hub und AWS Config dann hinzufügen. Danach beginnt AWS Config sofort das Senden von Regelauswertungen an Security Hub. Security Hub ergänzt die Regelauswertungen und wandelt sie in Security Hub-Ergebnisse um.

Weitere Informationen zu dieser Integration finden Sie unter Verfügbare AWS Serviceintegrationen im AWS Security Hub Benutzerhandbuch.

Evaluieren Sie Ihre Ressourcen mit AWS Config Regeln

Wenn Sie benutzerdefinierte Regeln erstellen oder verwaltete Regeln verwenden, werden Ihre Ressourcen anhand dieser Regeln AWS Config bewertet. Sie können Auswertungen für Ressourcen anhand Ihrer Regeln bei Bedarf durchführen. Dies ist beispielsweise hilfreich, wenn Sie eine benutzerdefinierte Regel erstellen und überprüfen möchten, ob Ihre Ressourcen AWS Config korrekt ausgewertet werden, oder wenn Sie feststellen möchten, ob ein Problem mit der Bewertungslogik Ihrer AWS Lambda Funktion vorliegt.

Beispiel

1. Sie erstellen eine benutzerdefinierte Regel, die auswertet, ob Ihre IAM-Benutzer über aktive Zugriffsschlüssel verfügen.
2. AWS Config bewertet Ihre Ressourcen anhand Ihrer benutzerdefinierten Regel.

3. In Ihrem Konto ist ein IAM-Benutzer vorhanden, der über keinen aktiven Zugriffsschlüssel verfügt. Ihre Regel kennzeichnet diese Ressource nicht korrekt als NON_COMPLIANT.
4. Beheben Sie die Regel und starten Sie die Auswertung erneut.
5. Da Sie Ihre Regel korrigiert haben, wertet sie Ihre Ressourcen richtig aus und kennzeichnet den IAM-Benutzer als NON_COMPLIANT.

Wenn Sie Ihrem Konto eine Regel hinzufügen, können Sie angeben, zu welchem Zeitpunkt im Prozess der Ressourcenerstellung und -verwaltung Sie Ihre Ressourcen bewerten AWS Config möchten. Der Prozess der Ressourcenerstellung und -verwaltung wird als Ressourcenbereitstellung bezeichnet. Sie wählen den Bewertungsmodus, um anzugeben, wann Sie in diesem Prozess Ihre Ressourcen bewerten AWS Config möchten.

Je nach Regel AWS Config können Sie Ihre Ressourcenkonfigurationen auswerten, bevor eine Ressource bereitgestellt wurde, nachdem eine Ressource bereitgestellt wurde, oder beides. Die Auswertung einer Ressource vor ihrer Bereitstellung ist eine proaktive Auswertung. Die Auswertung einer Ressource nach der Bereitstellung ist eine detektivische Auswertung.

Proaktiver Modus

Verwenden Sie die proaktive Auswertung, um Ressourcen vor der Bereitstellung auszuwerten. Auf diese Weise können Sie auswerten, ob eine Reihe von Ressourceneigenschaften, wenn sie zur Definition einer AWS Ressource verwendet würden, angesichts der proaktiven Regeln, die Sie in Ihrem Konto in Ihrer Region haben, als COMPLIANT oder NON_COMPLIANT gelten würde.

Das Ressourcentypschema gibt die Eigenschaften einer Ressource an. Sie finden das Ressourcentypschema in "AWS public extensions" in der AWS CloudFormation Registrierung oder mit dem folgenden CLI-Befehl:

```
aws cloudformation describe-type --type-name "AWS::S3::Bucket" --type RESOURCE
```

Weitere Informationen finden Sie unter Verwaltung von Erweiterungen über die AWS CloudFormation Registrierung und Referenz zu AWS Ressourcen- und Eigenschaftstypen im AWS CloudFormation Benutzerhandbuch.

> **Note**
>
> Durch proaktive Regeln werden keine Ressourcen korrigiert, die als NON_COMPLIANT gekennzeichnet sind, und sie verhindern auch nicht, dass diese bereitgestellt werden.

Auswerten Ihrer Ressourcen

So aktivieren Sie die proaktive Auswertung

1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die AWS Config Konsole zu https://console.aws.amazon.com/config/Hause.
2. Vergewissern Sie sich im AWS Management Console Menü, dass die Regionsauswahl auf eine Region eingestellt ist, die AWS Config Regeln unterstützt. Die Liste der unterstützten AWS - Regionen finden Sie unter AWS Config Regionen und -Endpunkte im Allgemeine Amazon Web Services-Referenz.
3. Klicken Sie im linken Navigationsbereich auf die Option Regeln. Eine Liste der verwalteten Regeln, die eine proaktive Evaluierung unterstützen, finden Sie unter Liste der AWS Config verwalteten Regeln nach Testmodus.
4. Wählen Sie eine Regel aus und klicken Sie auf Regel bearbeiten für die Regel, die aktualisiert werden soll.
5. Wählen Sie unter Auswertungsmodus die Option Proaktive Auswertung einschalten aus, damit Auswertungen der Konfigurationseinstellungen Ihrer Ressourcen ausgeführt werden können, bevor diese bereitgestellt werden.
6. Wählen Sie Speichern.

> **Note**
>
> Sie können die proaktive Evaluierung auch aktivieren, indem Sie den `put-config-rule`Befehl und die Aktivierung `PROACTIVE` für `EvaluationModes` oder die PutConfigRuleAktion und Aktivierung `PROACTIVE` für verwenden`EvaluationModes`.

Nachdem Sie die proaktive Evaluierung aktiviert haben, können Sie mithilfe der StartResourceEvaluationAPI und GetResourceEvaluationSummaryder API überprüfen, ob die Ressourcen, die Sie in diesen Befehlen angeben, durch die proaktiven Regeln in Ihrem Konto in Ihrer Region als NON_COMPLIANT gekennzeichnet werden.

Beginnen Sie beispielsweise mit der API: StartResourceEvaluation

```
aws configservice start-resource-evaluation --evaluation-mode PROACTIVE
                --resource-details '{"ResourceId":"MY_RESOURCE_ID",
```

```
                                        "ResourceType":"AWS::RESOURCE::TYPE",

 "ResourceConfiguration":"RESOURCE_DEFINITION_AS_PER_THE_RESOURCE_CONFIGURATION_SCHEMA",

 "ResourceConfigurationSchemaType":"CFN_RESOURCE_SCHEMA"}'
```

Sie sollten die `ResourceEvaluationId` in der Ausgabe erhalten:

```
{
    "ResourceEvaluationId": "MY_RESOURCE_EVALUATION_ID"
}
```

Verwenden Sie dann `ResourceEvaluationId` mit der GetResourceEvaluationSummary API das, um das Evaluierungsergebnis zu überprüfen:

```
aws configservice get-resource-evaluation-summary
    --resource-evaluation-id MY_RESOURCE_EVALUATION_ID
```

Die Ausgabe sollte folgendermaßen oder ähnlich aussehen:

```
{
    "ResourceEvaluationId": "MY_RESOURCE_EVALUATION_ID",
    "EvaluationMode": "PROACTIVE",
    "EvaluationStatus": {
        "Status": "SUCCEEDED"
    },
    "EvaluationStartTimestamp": "2022-11-15T19:13:46.029000+00:00",
    "Compliance": "COMPLIANT",
    "ResourceDetails": {
        "ResourceId": "MY_RESOURCE_ID",
        "ResourceType": "AWS::RESOURCE::TYPE",
        "ResourceConfiguration":
 "RESOURCE_DEFINITION_AS_PER_THE_RESOURCE_CONFIGURATION_SCHEMA"
    }
}
```

Verwenden Sie die API, um zusätzliche Informationen zum Evaluierungsergebnis zu erhalten, z. B. welche Regel eine Ressource als NON_COMPLIANT gekennzeichnet hat. GetComplianceDetailsByResource

Detektivischer Modus

Mit der detektivischen Auswertung können Sie Ressourcen auswerten, die bereits bereitgestellt wurden. Auf diese Weise lassen sich die Konfigurationseinstellungen Ihrer vorhandenen Ressourcen auswerten.

Auswerten Ihrer Ressourcen (Konsole)

1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die AWS Config Konsole zu Hause. https://console.aws.amazon.com/config/
2. Vergewissern Sie sich im AWS Management Console Menü, dass die Regionsauswahl auf eine Region eingestellt ist, die AWS Config Regeln unterstützt. Die Liste der unterstützten Regionen finden Sie unter AWS Config -Regionen und -Endpunkte im Allgemeine Amazon Web Services-Referenz.
3. Wählen Sie im Navigationsbereich Regeln aus. Auf der Seite Regeln werden der Name, die zugehörigen Korrekturmaßnahmen und der Compliance-Status jeder Regel aufgeführt.
4. Wählen Sie eine Regel aus der Tabelle aus.
5. Wählen Sie in der Dropdown-Liste Aktionen die Option Erneut bewerten aus.
6. AWS Config beginnt mit der Bewertung der Ressourcen anhand Ihrer Regel.

> **Note**
>
> Sie können eine Regel einmal pro Minute neu bewerten. Sie müssen warten AWS Config , bis die Bewertung Ihrer Regel abgeschlossen ist, bevor Sie eine weitere Bewertung starten können. Es können keine Auswertung ausgeführt werden, wenn gleichzeitig die Regel aktualisiert oder gelöscht wird.

Auswerten Ihrer Ressourcen (CLI)

- Verwenden Sie den start-config-rules-evaluation-Befehl:

```
$ aws configservice start-config-rules-evaluation --config-rule-
names ConfigRuleName
```

  AWS Config beginnt mit der Auswertung der aufgezeichneten Ressourcenkonfigurationen anhand Ihrer Regel. Sie können auch mehrere Regeln in Ihrer Anforderung angeben:

```
$ aws configservice start-config-rules-evaluation --config-rule-
names ConfigRuleName1 ConfigRuleName2 ConfigRuleName3
```

Auswerten Ihrer Ressourcen (API)

Verwenden Sie die Aktion „StartConfigRulesEvaluation“.

Löschen von Bewertungsergebnissen aus AWS Config -Regeln

Nach der AWS Config Auswertung Ihrer Regel können Sie die Evaluierungsergebnisse auf der Seite Regeln oder auf der Seite mit den Regeldetails für die Regel sehen. Wenn die Auswertungsergebnisse nicht korrekt sind oder wenn Sie eine erneute Auswertung durchführen möchten, können Sie die aktuellen Auswertungsergebnisse für die Regel löschen. Wenn Ihre Regel beispielsweise Ihre Ressourcen oder die kürzlich von Ihrem Konto gelöschten Ressourcen falsch auswertet, können Sie die Auswertungsergebnisse löschen und eine neue Auswertung durchführen.

Deleting Evaluation Results (Console)

1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die AWS Config Konsole zu https://console.aws.amazon.com/config/Hause.
2. Vergewissern Sie sich im AWS Management Console Menü, dass die Regionsauswahl auf eine AWS Region eingestellt ist, die AWS Config Regeln unterstützt. Die Liste der unterstützten Regionen finden Sie unter AWS Config -Regionen und -Endpunkte im Allgemeine Amazon Web Services-Referenz.
3. Wählen Sie im Navigationsbereich Regeln aus. Auf der Seite Regeln werden der Name, die zugehörigen Korrekturmaßnahmen und der Compliance-Status jeder Regel aufgeführt.
4. Wählen Sie eine Regel aus der Tabelle aus.
5. Wählen Sie in der Dropdown-Liste Aktionen die Option Ergebnisse löschen aus.
6. Wenn Sie dazu aufgefordert werden, geben Sie Delete ein (Groß- und Kleinschreibung beachten) und wählen Sie dann Löschen aus. Nachdem Sie eine Bewertung gelöscht haben, können Sie sie nicht mehr abrufen.
7. Nach der Löschung die Auswertungsergebnisse können Sie eine neue Auswertung manuell starten.

Deleting Evaluation Results (CLI)

- Verwenden Sie den delete-evaluation-results-Befehl.

```
$ aws configservice delete-evaluation-results --config-rule-name ConfigRuleName
```

  AWS Config löscht die Auswertungsergebnisse für die Regel.

Deleting Evaluation Results (API)

Verwenden Sie die Aktion „DeleteEvaluationResults“.

Problembehandlung für Regeln AWS Config

Überprüfen Sie die folgenden Probleme, um zu beheben, wenn Sie eine AWS Config Regel nicht löschen können oder wenn Sie eine Fehlermeldung erhalten, die der folgenden ähnelt: „Ein Fehler ist aufgetreten bei AWS Config.“

Die AWS Identity and Access Management (IAM-) Entität hat Berechtigungen für die API DeleteConfigRule

1. Öffnen Sie unter https://console.aws.amazon.com/iam/ die IAM-Konsole.
2. Wählen Sie im Navigationsbereich Benutzer oder Rollen aus.
3. Wählen Sie den Benutzer oder die Rolle aus, den Sie zum Löschen der AWS Config Regel verwendet haben, und erweitern Sie den Bereich Berechtigungsrichtlinien.
4. Wählen Sie auf der Registerkarte „Berechtigungen“ die Option JSON aus.
5. Vergewissern Sie sich im JSON-Vorschaufenster, dass die IAM-Richtlinie Berechtigungen für die DeleteConfigRuleAPI zulässt.

Die Berechtigungsgrenze der IAM-Entität erlaubt die API DeleteConfigRule

Wenn die IAM-Entität über eine Berechtigungsgrenze verfügt, stellen Sie sicher, dass sie Berechtigungen für die DeleteConfigRule API zulässt.

1. Öffnen Sie unter https://console.aws.amazon.com/iam/ die IAM-Konsole.
2. Wählen Sie im Navigationsbereich Benutzer oder Rollen aus.

3. Wählen Sie den Benutzer oder die Rolle aus, den Sie zum Löschen der AWS Config Regel verwendet haben, erweitern Sie die Rechtegrenze und wählen Sie dann JSON aus.
4. Vergewissern Sie sich im JSON-Vorschaufenster, dass die IAM-Richtlinie Berechtigungen für die DeleteConfigRuleAPI zulässt.

> **Warning**
>
> IAM-Benutzer verfügen über langfristige Anmeldeinformationen, was ein Sicherheitsrisiko darstellt. Um dieses Risiko zu minimieren, empfehlen wir, diesen Benutzern nur die Berechtigungen zu gewähren, die sie für die Ausführung der Aufgabe benötigen, und diese Benutzer zu entfernen, wenn sie nicht mehr benötigt werden.

Die Service Control Policy (SCP) erlaubt die API DeleteConfigRule

1. Öffnen Sie die AWS Organizations Konsole unter https://console.aws.amazon.com/organizations/ Verwendung des Verwaltungskontos für die Organisation.
2. Wählen Sie unter Kontoname die AWS-Konto.
3. Erweitern Sie unter Richtlinien den Eintrag Richtlinien zur Dienststeuerung und notieren Sie sich die angehängten SCP-Richtlinien.
4. Wählen Sie oben auf der Seite Richtlinien aus.
5. Wählen Sie die Richtlinie und dann Details anzeigen aus.
6. Vergewissern Sie sich im JSON-Vorschaufenster, dass die Richtlinie die DeleteConfigRuleAPI zulässt.

Bei der Regel handelt es sich nicht um eine serviceverknüpfte Regel

Wenn Sie einen Sicherheitsstandard aktivieren, AWS Security Hub erstellt servicebezogene Regeln für Sie. Sie können diese dienstbezogenen Regeln nicht mithilfe von löschen AWS Config, und die Schaltfläche Löschen ist ausgegraut. Informationen zum Entfernen einer serviceverknüpften Regel finden Sie unter Deaktivieren eines Sicherheitsstandards im Security Hub Hub-Benutzerhandbuch.

Derzeit werden keine Abhilfemaßnahmen durchgeführt

Sie können keine AWS Config Regeln löschen, für die derzeit Behebungsmaßnahmen durchgeführt werden. Folgen Sie den Schritten, um die mit dieser Regel verknüpfte Behebungsaktion zu löschen. Versuchen Sie dann erneut, die Regel zu löschen.

> **Important**
>
> Löschen Sie nur Behebungsaktionen, die sich im Status „Fehlgeschlagen“ oder „Erfolgreich“ befinden.

Konformitätspakete für AWS Config

Ein Konformitätspaket ist eine Sammlung von AWS Config Regeln und Abhilfemaßnahmen, die einfach als einzelne Einheit in einem Konto und einer Region oder unternehmensweit in einem Unternehmen eingesetzt werden können. AWS Organizations

Conformance Packs werden erstellt, indem eine YAML-Vorlage erstellt wird, die die Liste der von AWS Config verwalteten oder benutzerdefinierten Regeln und Korrekturmaßnahmen enthält. Sie können auch AWS Systems Manager Dokumente (SSM-Dokumente) verwenden, um Ihre Conformance Pack-Vorlagen zu speichern AWS und Conformance Packs mithilfe von SSM-Dokumentnamen direkt bereitzustellen. Sie können die Vorlage mithilfe der AWS Config -Konsole oder der AWS CLI bereitstellen.

Verwenden Sie eine der Beispielvorlagen für Conformance Packs, um schnell loszulegen und Ihre AWS Umgebung zu evaluieren. Sie können auch eine YAML-Datei für ein Konformitätspaket von Grund auf neu erstellen. Weitere Informationen finden Sie unter Benutzerdefiniertes Konformitätspaket.

Themen

- Compliance-Daten im Conformance Packs-Dashboard anzeigen für AWS Config
- Voraussetzung für Conformance Packs für AWS Config
- Unterstützung von Regionen
- AWS Config Prozessprüfungen innerhalb eines Konformitätspakets für AWS Config
- Conformance Pack-Beispielvorlagen für AWS Config
- Erstellen von Vorlagen für benutzerdefinierte Conformance Packs für AWS Config
- Bereitstellung von Conformance Packs für AWS Config
- Conformance Packs bearbeiten für AWS Config
- Löschen von Conformance Packs für AWS Config
- Details und Compliance-Informationen für Ihre Conformance Packs anzeigen für AWS Config
- Zeitleiste des Compliance-Verlaufs für Conformance Packs anzeigen für AWS Config
- Abfragen des Compliance-Verlaufs für Conformance Packs für AWS Config
- Verwaltung von Conformance Packs AWS Config für alle Konten in Ihrem Unternehmen
- Problembehandlung für Conformance Packs für AWS Config

Compliance-Daten im Conformance Packs-Dashboard anzeigen für AWS Config

Auf der zentralen Seite für Konformitätspakete werden alle Konformitätspakete angezeigt, die derzeit in Ihrem AWS-Konto vorhanden sind. Die Seite enthält auch den Namen, den Bereitstellungsstatus und die Konformitätsbewertung der einzelnen Konformitätspakete. Ein Konformitätspaket ist das Verhältnis (in Prozent) der Anzahl konformer Regel-Ressourcen-Kombinationen in einem Konformitätspaket zur Anzahl aller möglichen Regel-Ressourcen-Kombinationen in einem Konformitätspaket.

Auf diesem Dashboard können Sie den Grad der Konformität Ihrer Konformitätspakete nachvollziehen und anhand der Konformitätsbewertung den Fortschritt der Korrekturen verfolgen, Vergleiche zwischen verschiedenen Anforderungssätzen durchführen und die Auswirkungen einer bestimmten Änderung oder Bereitstellung auf ein Konformitätspaket ermitteln.

Navigieren auf der zentralen Seite für Konformitätspakete

1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die AWS Config Konsole zu https://console.aws.amazon.com/config/Hause.
2. Navigieren Sie zur Seite für Konformitätspakete. Überprüfen Sie Ihre Konformitätspakete und deren Compliance-Bewertung. Sie können zudem Folgendes durchführen:
   - Wählen Sie Konformitätspaket bereitstellen, um ein neues Konformitätspaket hinzuzufügen und zu konfigurieren.
   - Wenn Sie ein Konformitätspaket und seine Daten löschen möchten, die Konfigurationseinstellungen ändern oder zusätzliche Details wie den Lieferort oder die Parameter anzeigen möchten, wählen Sie ein Konformitätspaket aus und klicken Sie auf Aktionen.

> **Note**
>
> Sie können ein bereitgestelltes Konformitätspaket nicht bearbeiten. Sie können die restlichen Einstellungen jederzeit ändern, indem Sie in der Dropdownliste Aktionen den Namen des Konformitätspakets und dann Bearbeiten auswählen.

- Wenn Sie den Verlauf der Änderungen des Compliance-Status sehen möchten, wählen Sie ein Konformitätspaket und dann Konformitätspaketzeitplan aus. Weitere Informationen finden Sie unter Anzeigen einer Zeitleiste des Compliance-Verlaufs für Konformitätspakete.
- Wenn Sie den Bereitstellungsstatus, die Compliance-Bewertung, die Compliance-Ergebniszeitleiste und die Regeln für ein Konformitätspaket in einer detaillierten Ansicht sehen möchten, wählen Sie ein Konformitätspaket aus und klicken Sie auf Anzeigen.

Voraussetzung für Conformance Packs für AWS Config

Bevor Sie Ihr Conformance Pack bereitstellen, schalten AWS Config Sie die Aufzeichnung ein.

Themen

- Schritt 1: AWS Config Aufnahme starten (für alle Conformance Packs erforderlich)
- Schritt 2: Zusätzliche Voraussetzungen je nach Conformance Pack-Typ

Schritt 1: AWS Config Aufnahme starten (für alle Conformance Packs erforderlich)

1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die AWS Config Konsole zu https://console.aws.amazon.com/config/Hause.
2. Wählen Sie im Navigationsbereich Settings (Einstellungen) aus.
3. Wählen Sie unter Recording is off (Aufzeichnung ist aus) die Option Turn on (Einschalten), um die Aufzeichnung zu starten. Wenn Sie dazu aufgefordert werden, klicken Sie auf Weiter.

Schritt 2: Zusätzliche Voraussetzungen je nach Conformance Pack-Typ

A. Voraussetzungen für die Verwendung eines Conformance Packs mit Remediation

Bevor Sie Conformance Packs mithilfe von Beispielvorlagen mit Problembehebung bereitstellen, müssen Sie auf der Grundlage Ihres Behebungsziels entsprechende Ressourcen wie Automatisierung, Übernahme der Rolle und andere AWS Ressourcen einrichten.

Wenn Sie bereits über eine Automatisierungsrolle verfügen, die Sie für Korrekturmaßnahen mithilfe von SSM-Dokumenten verwenden, können Sie den ARN dieser Rolle direkt angeben. Wenn Sie über Ressourcen verfügen, können Sie diese in der Vorlage angeben.

> **Note**
>
> Bei der Bereitstellung eines Konformitätspakets mit Korrekturen für eine Organisation muss die Verwaltungskonto-ID der Organisation angegeben sein. Andernfalls ersetzt AWS Config bei der Bereitstellung des Konformitätspakets für die Organisation die Verwaltungskonto-ID automatisch durch die Mitgliedskonto-ID.

AWS Config unterstützt keine AWS CloudFormation systemeigenen Funktionen für die Automatisierungsausführungsrolle oder die. `ConfigRuleName` Sie müssen den genauen ARN der Rolle als Zeichenfolge angeben, und Sie müssen den vollständigen Regelnamen ohne systeminterne Funktionen verwenden.

Weitere Informationen zum Angeben des genauen ARN finden Sie unter Conformance Pack-Beispielvorlagen für AWS Config. Aktualisieren Sie Ihre Konto-ID und die Verwaltungskonto-ID für die Organisation, wenn Sie Beispielvorlagen verwenden.

B. Voraussetzungen für die Verwendung eines Conformance Packs mit einer oder mehreren benutzerdefinierten Regeln AWS Config

Bevor Sie ein Conformance Pack mit einer oder mehreren benutzerdefinierten AWS Config Regeln bereitstellen, erstellen Sie entsprechende Ressourcen wie AWS Lambda Funktion und die entsprechende Ausführungsrolle.

Wenn Sie bereits über eine benutzerdefinierte AWS Config Regel verfügen, können Sie die AWS Lambda Funktion `ARN` of direkt bereitstellen, um eine weitere Instanz dieser benutzerdefinierten Regel als Teil des Pakets zu erstellen.

Wenn Sie noch keine benutzerdefinierte AWS Config Regel haben, können Sie eine AWS Lambda Funktion erstellen und den ARN der Lambda-Funktion verwenden. Weitere Informationen finden Sie unter AWS Config Benutzerdefinierte Regeln.

Wenn Ihre AWS Lambda Funktion in einer anderen Version vorhanden ist AWS-Konto, können Sie AWS Config Regeln mit entsprechender kontoübergreifender AWS Lambda Funktionsautorisierung erstellen. Weitere Informationen finden Sie im AWS-Konten Blogbeitrag So verwalten Sie AWS Config Regeln für mehrere Personen zentral.

Same account bucket policy

AWS Config Um Conformance Pack-Artefakte speichern zu können, müssen Sie einen Amazon S3 S3-Bucket bereitstellen und die folgenden Berechtigungen hinzufügen. Weitere Informationen zur Benennung von Buckets finden Sie unter Regeln für die Benennung von Buckets.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AWSConfigConformsBucketPermissionsCheck",
      "Effect": "Allow",
      "Principal": {
        "AWS": [
            "arn:aws:iam::AccountId:role/aws-service-role/config-
conforms.amazonaws.com/AWSServiceRoleForConfigConforms"
        ]
      },
      "Action": "s3:GetBucketAcl",
      "Resource": "arn:aws:s3:::delivery-bucket-name"
    },
    {
      "Sid": "AWSConfigConformsBucketDelivery",
      "Effect": "Allow",
      "Principal": {
        "AWS": [
            "arn:aws:iam::AccountId:role/aws-service-role/config-
conforms.amazonaws.com/AWSServiceRoleForConfigConforms"
        ]
      },
      "Action": "s3:PutObject",
      "Resource": "arn:aws:s3:::delivery-bucket-name/[optional] prefix/
AWSLogs/AccountId/Config/*",
      "Condition": {
        "StringEquals": {
          "s3:x-amz-acl": "bucket-owner-full-control"
        }
      }
    }
  ]
}
```

Cross-account bucket policy

AWS Config Um Conformance Pack-Artefakte speichern zu können, müssen Sie einen Amazon S3 S3-Bucket bereitstellen und die folgenden Berechtigungen hinzufügen. Weitere Informationen zur Benennung von Buckets finden Sie unter Regeln für die Benennung von Buckets.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AWSConfigConformsBucketPermissionsCheck",
      "Effect": "Allow",
      "Principal": {
        "AWS": [
            "arn:aws:iam::SourceAccountId:role/aws-service-role/config-
conforms.amazonaws.com/AWSServiceRoleForConfigConforms",
            "PutConformancePack API caller user principal like
 arn:aws:iam::SourceAccountId:user/userName "
        ]
      },
      "Action": "s3:GetBucketAcl",
      "Resource": "arn:aws:s3:::awsconfigconforms-suffix in bucket name"
    },
    {
      "Sid": "AWSConfigConformsBucketDelivery",
      "Effect": "Allow",
      "Principal": {
        "AWS": [
            "arn:aws:iam::SourceAccountId:role/aws-service-role/config-
conforms.amazonaws.com/AWSServiceRoleForConfigConforms"
        ]
      },
      "Action": "s3:PutObject",
      "Resource": "arn:aws:s3:::awsconfigconforms-suffix in bucket name/[optional]
 prefix/AWSLogs/AccountID/Config/*",
      "Condition": {
        "StringEquals": {
          "s3:x-amz-acl": "bucket-owner-full-control"
        }
      }
    },
    {
      "Sid": " AWSConfigConformsBucketReadAccess",
```

```
      "Effect": "Allow",
      "Principal": {
        "AWS": [
            "arn:aws:iam::SourceAccountId:role/aws-service-role/config-
conforms.amazonaws.com/AWSServiceRoleForConfigConforms"
        ]
      },
      "Action": "s3:GetObject",
      "Resource": "arn:aws:s3:::awsconfigconforms-suffix in bucket name/[optional]
 prefix/AWSLogs/AccountID/Config/*"
    }
  ]
}
```

> **Note**
>
> Bei der Bereitstellung kontoübergreifender Konformitätspakete sollte der Name des Amazon-S3-Buckets für die Übermittlung mit `awsconfigconforms` beginnen.

C. Voraussetzungen für Organization Conformance Packs

Geben Sie einen ARN für die Automatisierungsausführungsrolle für diese Korrekturmaßnahme in der Vorlage an, wenn die Eingabevorlage über eine Konfiguration für die automatische Korrektur verfügt. Stellen Sie sicher, dass in allen Konten (Verwaltung und Mitglied) einer Organisation eine Rolle mit dem angegebenen Namen vorhanden ist. Sie müssen diese Rolle in allen Konten erstellen, bevor Sie `PutOrganizationConformancePack` aufrufen. Sie können diese Rolle manuell erstellen oder die AWS CloudFormation Stack-Sets verwenden, um sie in jedem Konto zu erstellen.

Wenn Ihre Vorlage eine AWS CloudFormation systeminterne Funktion verwendet, `Fn::ImportValue` um eine bestimmte Variable zu importieren, muss diese Variable `Export Value` in allen Mitgliedskonten dieser Organisation als eine definiert werden.

Informationen zu benutzerdefinierten AWS Config Regeln finden Sie im Blog So verwalten Sie AWS Config Regeln zentral in mehreren AWS-Konten Blogs, um die richtigen Berechtigungen einzurichten.

Bucket-Richtlinie der Organisation:

AWS Config Um Conformance Pack-Artefakte speichern zu können, müssen Sie einen Amazon S3 S3-Bucket bereitstellen und die folgenden Berechtigungen hinzufügen. Weitere Informationen zur Benennung von Buckets finden Sie unter Regeln für die Benennung von Buckets.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowGetObject",
            "Effect": "Allow",
            "Principal": "*",
            "Action": [
                 "s3:GetObject",
                 "s3:PutObject"
            ],
            "Resource": "arn:aws:s3:::awsconfigconforms-suffix in bucket name/*",
            "Condition": {
                "StringEquals": {
                    "aws:PrincipalOrgID": "customer_org_id"
                },
                "ArnLike": {
                    "aws:PrincipalArn": "arn:aws:iam::*:role/aws-service-role/config-
conforms.amazonaws.com/AWSServiceRoleForConfigConforms"
                }
            }
        },
        {
            "Sid": "AllowGetBucketAcl",
            "Effect": "Allow",
            "Principal": "*",
            "Action": "s3:GetBucketAcl",
            "Resource": "arn:aws:s3:::awsconfigconforms-suffix in bucket name",
            "Condition": {
                "StringEquals": {
                    "aws:PrincipalOrgID": "customer_org_id"
                },
                "ArnLike": {
                    "aws:PrincipalArn": "arn:aws:iam::*:role/aws-service-role/config-
conforms.amazonaws.com/AWSServiceRoleForConfigConforms"
                }
            }
        }
    ]
}
```

> **Note**
>
> Wenn Sie Konformitätspakete für eine Organisation bereitstellen, sollte der Name des Amazon-S3-Buckets für die Übermittlung mit `awsconfigconforms` beginnen.

Unterstützung von Regionen

Conformance Packs werden in den folgenden Regionen unterstützt.

Name der Region	Region	Endpunkt	Protocol (Protokoll)
USA Ost (Ohio)	us-east-2	config.us-east-2.amazonaws.com	HTTPS
USA Ost (Nord-Virginia)	us-east-1	config.us-east-1.amazonaws.com	HTTPS
USA West (Nordkalifornien)	us-west-1	config.us-west-1.amazonaws.com	HTTPS
USA West (Oregon)	us-west-2	config.us-west-2.amazonaws.com	HTTPS
Afrika (Kapstadt)	af-south-1	config.af-south-1.amazonaws.com	HTTPS
Asien-Pazifik (Hongkong)	ap-east-1	config.ap-east-1.amazonaws.com	HTTPS

Name der Region	Region	Endpunkt	Protocol (Protokoll)
Asien-Pazifik (Hyderabad)	ap-south-2	config.ap-south-2.amazonaws.com	HTTPS
Asien-Pazifik (Jakarta)	ap-southeast-3	config.ap-southeast-3.amazonaws.com	HTTPS
Asien-Pazifik (Melbourne)	ap-southeast-4	config.ap-southeast-4.amazonaws.com	HTTPS
Asien-Pazifik (Mumbai)	ap-south-1	config.ap-south-1.amazonaws.com	HTTPS
Asien-Pazifik (Osaka)	ap-northeast-3	config.ap-northeast-3.amazonaws.com	HTTPS
Asien-Pazifik (Seoul)	ap-northeast-2	config.ap-northeast-2.amazonaws.com	HTTPS
Asien-Pazifik (Singapur)	ap-southeast-1	config.ap-southeast-1.amazonaws.com	HTTPS
Asien-Pazifik (Sydney)	ap-southeast-2	config.ap-southeast-2.amazonaws.com	HTTPS

Name der Region	Region	Endpunkt	Protocol (Protokoll)
Asien-Pazifik (Tokio)	ap-northeast-1	config.ap-northeast-1.amazonaws.com	HTTPS
Kanada (Zentral)	ca-central-1	config.ca-central-1.amazonaws.com	HTTPS
Kanada West (Calgary)	ca-west-1	config.ca-west-1.amazonaws.com	HTTPS
Europa (Frankfurt)	eu-central-1	config.eu-central-1.amazonaws.com	HTTPS
Europa (Irland)	eu-west-1	config.eu-west-1.amazonaws.com	HTTPS
Europa (London)	eu-west-2	config.eu-west-2.amazonaws.com	HTTPS
Europa (Mailand)	eu-south-1	config.eu-south-1.amazonaws.com	HTTPS
Europa (Paris)	eu-west-3	config.eu-west-3.amazonaws.com	HTTPS
Europa (Spanien)	eu-south-2	config.eu-south-2.amazonaws.com	HTTPS
Europa (Stockholm)	eu-north-1	config.eu-north-1.amazonaws.com	HTTPS

Name der Region	Region	Endpunkt	Protocol (Protokoll)
Europa (Zürich)	eu-central-2	config.eu-central-2.amazonaws.com	HTTPS
Israel (Tel Aviv)	il-central-1	config.il-central-1.amazonaws.com	HTTPS
Naher Osten (Bahrain)	me-south-1	config.me-south-1.amazonaws.com	HTTPS
Naher Osten (VAE)	me-central-1	config.me-central-1.amazonaws.com	HTTPS
Südamerika (São Paulo)	sa-east-1	config.sa-east-1.amazonaws.com	HTTPS
AWS GovCloud (US-Ost)	us-gov-east-1	config.us-gov-east-1.amazonaws.com	HTTPS
AWS GovCloud (US-West)	us-gov-west-1	config.us-gov-west-1.amazonaws.com	HTTPS

Die Bereitstellung von Conformance Packs für alle Mitgliedskonten einer AWS Organisation wird in den folgenden Regionen unterstützt.

Name der Region	Region	Endpunkt	Protocol (Protokoll)
USA Ost (Ohio)	us-east-2	config.us-east-2.amazonaws.com	HTTPS
USA Ost (Nord-Virginia)	us-east-1	config.us-east-1.amazonaws.com	HTTPS
USA West (Nordkalifornien)	us-west-1	config.us-west-1.amazonaws.com	HTTPS
USA West (Oregon)	us-west-2	config.us-west-2.amazonaws.com	HTTPS
Afrika (Kapstadt)	af-south-1	config.af-south-1.amazonaws.com	HTTPS
Asien-Pazifik (Hongkong)	ap-east-1	config.ap-east-1.amazonaws.com	HTTPS
Asien-Pazifik (Hyderabad)	ap-south-2	config.ap-south-2.amazonaws.com	HTTPS
Asien-Pazifik (Jakarta)	ap-southeast-3	config.ap-southeast-3.amazonaws.com	HTTPS

Name der Region	Region	Endpunkt	Protocol (Protokoll)	
Asien-Pazifik (Melbourne)	ap-southeast-4	config.ap-southeast-4.amazonaws.com	HTTPS	
Asien-Pazifik (Mumbai)	ap-south-1	config.ap-south-1.amazonaws.com	HTTPS	
Asien-Pazifik (Osaka)	ap-northeast-3	config.ap-northeast-3.amazonaws.com	HTTPS	
Asien-Pazifik (Seoul)	ap-northeast-2	config.ap-northeast-2.amazonaws.com	HTTPS	
Asien-Pazifik (Singapur)	ap-southeast-1	config.ap-southeast-1.amazonaws.com	HTTPS	
Asien-Pazifik (Sydney)	ap-southeast-2	config.ap-southeast-2.amazonaws.com	HTTPS	
Asien-Pazifik (Tokio)	ap-northeast-1	config.ap-northeast-1.amazonaws.com	HTTPS	
Kanada (Zentral)	ca-central-1	config.ca-central-1.amazonaws.com	HTTPS	

Name der Region	Region	Endpunkt	Protocol (Protokoll)
Kanada West (Calgary)	ca-west-1	config.ca-west-1.amazonaws.com	HTTPS
Europa (Frankfurt)	eu-central-1	config.eu-central-1.amazonaws.com	HTTPS
Europa (Irland)	eu-west-1	config.eu-west-1.amazonaws.com	HTTPS
Europa (London)	eu-west-2	config.eu-west-2.amazonaws.com	HTTPS
Europa (Mailand)	eu-south-1	config.eu-south-1.amazonaws.com	HTTPS
Europa (Paris)	eu-west-3	config.eu-west-3.amazonaws.com	HTTPS
Europa (Spanien)	eu-south-2	config.eu-south-2.amazonaws.com	HTTPS
Europa (Stockholm)	eu-north-1	config.eu-north-1.amazonaws.com	HTTPS
Europa (Zürich)	eu-central-2	config.eu-central-2.amazonaws.com	HTTPS
Israel (Tel Aviv)	il-central-1	config.il-central-1.amazonaws.com	HTTPS

Name der Region	Region	Endpunkt	Protocol (Protokoll)
Naher Osten (Bahrain)	me-south-1	config.me-south-1.amazonaws.com	HTTPS
Naher Osten (VAE)	me-central-1	config.me-central-1.amazonaws.com	HTTPS
Südamerika (São Paulo)	sa-east-1	config.sa-east-1.amazonaws.com	HTTPS
AWS GovCloud (US-Ost)	us-gov-east-1	config.us-gov-east-1.amazonaws.com	HTTPS
AWS GovCloud (US-West)	us-gov-west-1	config.us-gov-west-1.amazonaws.com	HTTPS

AWS Config Prozessprüfungen innerhalb eines Konformitätspakets für AWS Config

Bei Prozessüberprüfungen handelt es sich um eine Art von AWS Config Regel, mit der Sie Ihre externen und internen Aufgaben, für die eine Überprüfung im Rahmen der Konformitätspakete erforderlich ist, nachverfolgen können. Diese Prüfungen können einem vorhandenen Conformance Pack oder einem neuen Conformance Pack hinzugefügt werden. Sie können die gesamte Einhaltung der Vorschriften, einschließlich AWS Config der Dauer und manueller Prüfungen, an einem einzigen Ort nachverfolgen.

Mithilfe von Prozessprüfungen können Sie die Compliance von Anforderungen und Maßnahmen an einem Ort auflisten. Diese Prozessprüfungen tragen dazu bei, den Umfang der Conformance

Packs zu vergrößern, die auf Compliance-Regelungen basieren. Sie können das Conformance Pack erweitern, indem Sie neue Prozessprüfungen hinzufügen, mit denen Prozesse und Aktionen verfolgt werden, die manuell überprüft und nachverfolgt werden müssen. Auf diese Weise kann das Konformitätspaket zur Vorlage werden, die Einzelheiten zu den AWS Config Fristen und manuellen Prozessen für ein Compliance-Regime enthält.

Sie können die Compliance von Prozessen, die nicht mit Änderungen der Ressourcenkonfiguration in Zusammenhang stehen, innerhalb eines Conformance Packs im Rahmen von Prozessprüfungen nachverfolgen und verwalten. Sie können beispielsweise eine Prozessprüfung hinzufügen, um die PCI-DSS-Compliance-Anforderungen für die Aufbewahrung von Medien-Backups an einem externen Standort nachzuverfolgen. Sie werten die Compliance anhand der PCI-DSS-Richtlinien oder gemäß den Richtlinien Ihres Unternehmens manuell aus.

Verfügbarkeit in der Region: Prozessprüfungen mit den Conformance Packs sind überall verfügbar, AWS-Regionen wo AWS Config Konformitätspakete verfügbar sind. Weitere Informationen finden Sie unter Unterstützung von Regionen.

Themen

- Beispielvorlage für ein Conformance Pack zum Erstellen von Prozessprüfungen
- Einschließen von Prozessprüfungen in ein Conformance Pack
- Ändern des Compliance-Status einer Prozessprüfung
- Anzeigen und Bearbeiten von Prozessprüfungen (Konsole)

Beispielvorlage für ein Conformance Pack zum Erstellen von Prozessprüfungen

```
################################################################################
#
#  Conformance Pack template for process check
#
################################################################################
Resources:
  AWSConfigProcessCheck:
    Properties:
      ConfigRuleName: RuleName
      Description: Description of Rule
      Source:
        Owner: AWS
```

```
        SourceIdentifier: AWS_CONFIG_PROCESS_CHECK
    Type: AWS::Config::ConfigRule
```

Sehen Sie sich zwei Beispielvorlagen an: Best Practices für den Betrieb von CIS AWS Foundations Benchmark v1.4 Level 1 und Best Practices für den Betrieb von CIS AWS Foundations Benchmark v1.4 Level 2 .

Einschließen von Prozessprüfungen in ein Conformance Pack

1. Fügen Sie der Vorlage für das Conformance Pack eine Prozessprüfung hinzu. Weitere Informationen finden Sie unter Beispielvorlage für ein Conformance Pack zum Erstellen von Prozessprüfungen.

   ```
   Resources:
     ConfigEnabledAllRegions:
       Properties:
         ConfigRuleName: Config-Enabled-All-Regions
         Description: Ensure AWS Config is enabled in all Regions.
         Source:
           Owner: AWS
           SourceIdentifier: AWS_CONFIG_PROCESS_CHECK
       Type: AWS::Config::ConfigRule
   ```

2. Geben Sie einen Namen für die Prozessprüfung ein.
3. Geben Sie eine Beschreibung für die Prozessprüfung ein.
4. Stellen Sie das Conformance Pack bereit. Weitere Informationen finden Sie unter Bereitstellung von Conformance Packs für AWS Config.

Ändern des Compliance-Status einer Prozessprüfung

Sie können den Konformitätsstatus einer Prozessprüfung mithilfe der AWS Config Konsole AWS CLI, der Taste und ändern APIs.

Change Compliance Status for Process Checks (Console)

1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die AWS Config Konsole zu https://console.aws.amazon.com/config/Hause.
2. Navigieren Sie zur Seite mit den AWS Config Regeln.

3. Wählen Sie den Namen der Prozessprüfung aus, die Sie in der Vorlage angegeben haben, sowie die ID im Conformance Pack.

> **Note**
>
> Alle Prozessprüfungen aus demselben Conformance Pack haben dasselbe Suffix.

4. Auf der Seite mit den Regeldetails können Sie die Regel nicht bearbeiten, aber Sie können die Compliance der Regel bearbeiten. Wählen Sie im Abschnitt „Manuelle Compliance“ die Option Compliance bearbeiten aus.
5. Wählen Sie die entsprechende Compliance aus der Dropdown-Liste aus.
6. (Optional) Geben Sie eine Beschreibung für den Compliance-Status ein.
7. Wählen Sie Speichern.

Change the Compliance Status for Process Checks (AWS CLI)

Sie können die Konformität von Prozessprüfungen innerhalb eines Conformance Packs mithilfe von AWS Command Line Interface (AWS CLI) aktualisieren.

Informationen zur Installation von AWS CLI auf Ihrem lokalen Computer finden Sie unter Installation von AWS CLI im AWS CLI Benutzerhandbuch.

Geben Sie bei Bedarf ein, `AWS Config ure` um das so zu konfigurieren, AWS CLI dass es eine AWS Region verwendet, in der AWS Config Konformitätspakete verfügbar sind.

1. Öffnen Sie eine Eingabeaufforderung oder ein Terminal-Fenster.
2. Geben Sie den folgenden Befehl ein, um die Konformität einer Prozessprüfung zu aktualisieren, bei der Sie `ComplianceResourceId` sich `Account ID` befinden, und geben Sie den Namen Ihrer Regel an.

```
aws configservice put-external-evaluation --config-rule-
name process-check-rule-name  --external-evaluation
 ComplianceResourceType=AWS::::Account,ComplianceResourceId=Account
 ID,ComplianceType=NON_COMPLIANT,OrderingTimestamp=2020-12-17T00:10:00.000Z
```

3. Drücken Sie die Eingabetaste, um den Befehl auszuführen.

Change the Compliance Status for Process Checks (API)

Verwenden Sie nach Abschluss der Bereitstellung die `PutExternalEvaluation`-API, um die Auswertungen und Compliance der Prozessprüfungen zu aktualisieren. Weitere Informationen finden Sie unter PutExternalEvaluation.

Anzeigen und Bearbeiten von Prozessprüfungen (Konsole)

Sie können Prozessprüfungen erst anzeigen, nachdem den Prozessprüfungen ein Compliance-Status hinzugefügt wurde. Wählen Sie ein bestimmtes Conformance Pack aus, um alle Prozessprüfungen in diesem Conformance Pack anzuzeigen. Hier finden Sie eine Liste der Prozessprüfungen, die den Status „konform“ und „nicht konform“ aufweisen.

Da es sich um eine serviceverknüpfte Regel handelt, können Sie die Prozessprüfung nicht auf der Seite mit den Regeldetails bearbeiten.

> **Note**
>
> Sie können jedoch die Konformität der Prozessprüfung aktualisieren, indem Sie „Konformität bearbeiten“ wählen und den entsprechenden Wert unter „Konform“, „Nicht konform“ oder „Nicht zutreffend“ auswählen.

Sie können eine Prozessprüfung aus dem Conformance Pack, dem Sie Prozessprüfungen hinzugefügt haben, bearbeiten oder löschen.

Conformance Pack-Beispielvorlagen für AWS Config

Hier sind die YAML-Vorlagen für das Conformance Pack, die Sie in der Konsole sehen. AWS Config In jeder Conformance Pack-Vorlage können Sie eine oder mehrere AWS Config Regeln und Behebungsmaßnahmen verwenden. Bei den im Conformance Pack aufgeführten AWS Config Regeln kann AWS Config es sich um verwaltete Regeln und/oder AWS Config um benutzerdefinierte Regeln handeln. Sie können alle Conformance Pack-Vorlagen von herunterladen. GitHub

> **Important**
>
> Conformance Packs bieten ein allgemeines Compliance-Framework, mit dem Sie mithilfe verwalteter oder benutzerdefinierter AWS Config Regeln und Abhilfemaßnahmen

Kontrollen zur Sicherheits-, Betriebs- oder Kostenoptimierung durchführen können. AWS Config AWS Mustervorlagen für Conformance Packs sollen Ihnen helfen, Ihre eigenen Conformance Packs mit unterschiedlichen oder zusätzlichen Regeln, Eingabeparametern und Abhilfemaßnahmen zu erstellen, die zu Ihrer Umgebung passen. Die Beispielvorlagen, einschließlich derjenigen, die sich auf Compliance-Standards und Branchen-Benchmarks beziehen, sind nicht darauf ausgelegt, Ihre Compliance mit einem bestimmten Governance-Standard zu gewährleisten. Sie können weder interne Maßnahmen ersetzen noch garantieren, dass Sie eine Compliance-Bewertung bestehen.

Note

Es wird empfohlen, vor der Bereitstellung die Regeln zu überprüfen, die in der Region verfügbar sind, in der Sie ein Conformance Pack bereitstellen (Liste der AWS Config verwalteten Regeln nach Verfügbarkeit in der Region) und die Vorlage für Regeln zu ändern, die in dieser Region noch nicht verfügbar sind.

Themen

- AWS Control Tower Detective Guardrails Konformitätspaket
- Bewährte Methoden für den Betrieb von ABS CCIG 2.0 Material Workloads
- Bewährte Methoden für den Betrieb von ABS CCIG 2.0 Standard Workloads
- Bewährte Methoden für die Implementierung von ACSC Essential 8
- Bewährte Methoden für die Implementierung von ACSC ISM
- Bewährte Methoden für die Ausführung von KI und ML
- Bewährte Methoden für die Implementierung von Amazon API Gateway
- Bewährte Betriebspraktiken für Amazon CloudWatch
- Bewährte Methoden für die Ausführung von Amazon DynamoDB
- Bewährte Methoden für die Ausführung von Amazon S3
- Bewährte Methoden für die Implementierung von APRA CPG 234
- Bewährte Methoden für die Ausführung des Asset-Managements
- Bewährte Methoden für die Ausführung von AWS Backup
- Operative Best Practices für AWS Identitäts- und Zugriffsmanagement

- Operative Best Practices für die AWS Zuverlässigkeit eines gut konzipierten Frameworks
- Bewährte betriebliche Verfahren für die AWS Sicherheitssäule eines Well-Architected Frameworks
- Bewährte Methoden für die Ausführung von BCP und DR
- Bewährte Betriebspraktiken für BNM T RMi
- Bewährte Methoden für das Canadian Centre for Cyber Security (CCCS)-Medium-Cloud-Kontrollprofil
- Best Practices für den Betrieb von CIS AWS Foundations Benchmark v1.4 Level 1
- Best Practices für den Betrieb von CIS AWS Foundations Benchmark v1.4 Level 2
- Bewährte Betriebspraktiken für kritische Sicherheitskontrollen der GUS v8 IG1
- Bewährte Betriebspraktiken für kritische Sicherheitskontrollen der GUS v8 IG2
- Bewährte Betriebspraktiken für kritische Sicherheitskontrollen der GUS v8 IG3
- Bewährte Methoden für die Ausführung von CIS Top 20
- Bewährte Methoden für die Ausführung von CISA Cyber Essentials
- Bewährte Methoden für die Ausführung von Criminal Justice Information Services (CJIS)
- Bewährte Methoden für die Ausführung von CMMC 2.0 Level 1
- Bewährte Methoden für die Ausführung von CMMC 2.0 Level 2
- Bewährte Methoden für die Ausführung von Datenverarbeitungsservices
- Bewährte Methoden für die Erreichung von Ausfallsicherheit
- Bewährte Methoden für die Ausführung von Datenbankservices
- Bewährte Methoden für die Ausführung von Data Lakes und Analyseservices
- Bewährte Methoden für die Ausführung von DevOps
- Bewährte Methoden für die Ausführung von EC2
- Bewährte Methoden für die Verwendung von Verschlüsselung und Schlüsselverwaltung
- Leitfaden für bewährte Betriebspraktiken für die ENISA-Cybersicherheit für SMEs
- Bewährte Methoden für die Implementierung des Esquema Nacional de Seguridad (ENS) Low
- Bewährte Methoden für die Implementierung des Esquema Nacional de Seguridad (ENS) Medium
- Bewährte Methoden für die Implementierung des Esquema Nacional de Seguridad (ENS) High
- Betriebliche bewährte Methoden für FDA Titel 21 CFR Teil 11
- Bewährte Methoden zur Implementierung von FedRAMP(Low)
- Bewährte Methoden für die Ausführung von FedRAMP(Moderate)

- Bewährte Betriebspraktiken für FedRAMP (High Part 1)
- Bewährte Betriebspraktiken für FedRAMP (High Part 2)
- Betriebliche bewährte Methoden für FFIEC
- Bewährte Methoden für die Implementierung des deutschen Kriterienkatalogs C5 (Cloud Computing Compliance Criteria Catalogue)
- Bewährte Methoden für die Implementierung des Gramm Leach Bliley Act (GLBA)
- Bewährte Methoden für die Implementierung Anhang 11 zum EG-Leitfaden der Guten Herstellungspraxis
- Betriebliche bewährte Methoden für die HIPAA-Sicherheit
- Bewährte Methoden für die Ausführung von IRS 1075
- Bewährte Methoden zur Ausführung von K-ISMS
- Bewährte Methoden für die Ausführung von Load Balancing
- Betriebliche bewährte Methoden für die Protokollierung
- Bewährte Methoden für die Ausführung von Management- und Governance-Services
- Bewährte Methoden für die Verwendung der MAS Notice 655
- Bewährte Methoden für die Ausführung von MAS TRMG
- Bewährte Methoden für die Überwachung
- Bewährte Methoden für die Implementierung von NBC TRMG
- Bewährte Methoden für die Ausführung von NERC CIP BCSI
- Bewährte Methoden für die Ausführung von NCSC-Cloud-Sicherheitsprinzipien
- Bewährte Methoden für die Implementierung des Cyber Assessment Framework des NCSC
- Bewährte Methoden für die Ausführung von Services für Netzwerke und zur Bereitstellung von Inhalten
- Bewährte Methoden für die Implementierung von NIST 800-53 Rev. 4
- Bewährte Methoden für die Ausführung von NIST 800-53 Rev. 5
- Bewährte Methoden für die Ausführung von NIST 800 171
- Bewährte Methoden für die Ausführung von NIST 800 172
- Bewährte Methoden für die Ausführung von NIST 800 181
- Bewährte Methoden für die Ausführung von NIST 1800 25
- Bewährte Methoden für die Ausführung von NIST CSF

- Bewährte Betriebspraktiken für NIST Privacy Framework v1.0
- Bewährte Methoden für die Ausführung von NYDFS 23
- Bewährte Betriebspraktiken für NZISM 3.8
- Bewährte Methoden für die Ausführung von PCI DSS 3.2.1
- Operative Best Practices für PCI DSS 4.0 (ohne globale Ressourcentypen)
- Operative Best Practices für PCI DSS 4.0 (einschließlich globaler Ressourcentypen)
- Bewährte Methoden für die Ausführung von öffentlich zugänglichen Ressourcen
- Operative Best Practices für das RBI Cyber Security Framework für UCBs
- Bewährte Methoden für die Ausführung von RBI MD-ITF
- Bewährte Methoden für Sicherheits-, Identitäts- und Compliance-Services
- Bewährte Methoden für die Ausführung von Serverless
- Bewährte Methoden für die Ausführung von Speicherservices
- Bewährte Methoden für die Ausführung von SWIFT-CSP
- Bewährte Methoden für die Sicherheit in Amazon Elastic Container Service (Amazon ECS)
- Bewährte Methoden für die Sicherheit in Amazon Elastic File System (Amazon EFS)
- Bewährte Methoden für die Sicherheit in Amazon Elastic Kubernetes Service (Amazon EKS)
- Bewährte Sicherheitsmethoden für Amazon CloudFront
- Bewährte Sicherheitsmethoden für Amazon OpenSearch Service
- Bewährte Methoden für die Sicherheit in Amazon Redshift
- Bewährte Methoden für die Sicherheit in Amazon Relational Database Service (Amazon RDS)
- Bewährte Sicherheitsmethoden für AWS Auto Scaling
- Bewährte Sicherheitsmethoden für AWS CloudTrail
- Bewährte Sicherheitsmethoden für AWS CodeBuild
- Bewährte Methoden für die Sicherheit in Amazon ECR
- Bewährte Sicherheitsmethoden für AWS Lambda
- Bewährte Sicherheitsmethoden für AWS Network Firewall
- Bewährte Sicherheitsmethoden für Amazon SageMaker AI
- Bewährte Sicherheitsmethoden für AWS Secrets Manager
- Bewährte Sicherheitsmethoden für AWS WAF
- Beispielvorlagen mit Korrekturmaßnahmen

AWS Control Tower Detective Guardrails Konformitätspaket

Dieses Konformitätspaket enthält AWS Config Regeln, die auf AWS Control Tower Detective Guardrails basieren. Eine Liste aller verwalteten Regeln, die von unterstützt werden AWS Config, finden Sie unter Liste der AWS Config verwalteten Regeln.

Die Namen und Beschreibungen der erforderlichen Parameter finden Sie im `Parameters` Abschnitt der folgenden Vorlage.

Die Vorlage ist verfügbar auf GitHub: AWS Control Tower Detective Guardrails Conformance Pack.

Bewährte Methoden für den Betrieb von ABS CCIG 2.0 Material Workloads

Konformitätspakete bieten ein allgemeines Compliance-Framework, das es Ihnen ermöglicht, mithilfe verwalteter oder benutzerdefinierter Regeln und Abhilfemaßnahmen Kontrollen zur Sicherheits-, Betriebs- oder Kostenoptimierung durchzuführen. AWS Config AWS Config Conformance Packs dienen als Beispielvorlagen nicht dazu, die vollständige Einhaltung eines bestimmten Governance- oder Compliance-Standards sicherzustellen. Sie sind dafür verantwortlich, selbst zu beurteilen, ob Ihre Nutzung der Services den geltenden gesetzlichen und behördlichen Anforderungen entspricht.

Im Folgenden finden Sie ein Beispiel für eine Zuordnung zwischen dem ABS Cloud Computing Implementation Guide 2.0 — Material Workloads und AWS Managed Config Rules. Jede Config-Regel gilt für eine bestimmte AWS Ressource und bezieht sich auf eine oder mehrere Steuerelemente des ABS Cloud Computing Implementation Guide. Eine Kontrolle des ABS Cloud Computing Implementation Guide kann sich auf mehrere Konfigurationsregeln beziehen. In der folgenden Tabelle finden Sie weitere Informationen und Anleitungen zu diesen Zuordnungen.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 a-govern-the-cloud — 2 — materielle Arbeitsla sten	guardduty-enabled-centralized	Amazon GuardDuty kann mithilfe von Threat Intellige nce Feeds helfen, potenzielle Cybersicherheitsereignisse zu überwachen und zu erkennen. Dazu gehören Listen mit bösartigen IPs und maschinel len Lernmethoden zur Identifiz ierung unerwarteter, nicht

Kontroll-ID	AWS Config	Empfehlungen
		autorisierter und bösartige r Aktivitäten in Ihrer AWS Cloud-Umgebung.
Abschnitt 4 a-govern-the-cloud — 2 — materielle Arbeitsla sten	securityhub-enabled	AWS Security Hub hilft bei der Überwachung von unbefugte m Personal, Verbindungen, Geräten und Software. AWS Security Hub aggregiert, organisiert und priorisiert die Sicherheitswarnungen oder Ergebnisse mehrerer Dienste. AWS Einige dieser Dienste sind Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer und AWS Firewall Manager sowie AWS Partnerlösungen.
Abschnitt 4 - 2 - Standard-Workloads a-govern-the-cloud	account-part-of-organizations	Durch die zentrale Verwaltun g AWS-Konten innerhalb von AWS Organizations wird sichergestellt, dass die Konten den Vorschriften entsprech en. Eine fehlende zentrale Kontoverwaltung kann zu inkonsistenten Kontokonf igurationen führen, wodurch Ressourcen und sensible Daten offengelegt werden können.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 a-govern-the-cloud — 2 — Standard-Workloads	cloudtrail-s3-dataevents-enabled	Die Erfassung von Simple Storage Service (Amazon S3)-Datenereignissen unterstützt die Erkennung von ungewöhnlichen Aktivitäten. Zu den Details gehören Informationen zu dem AWS -Konto, das auf einen Amazon-S3-Bucket zugegriffen hat, die IP-Adresse und die Uhrzeit des Ereignisses.
Abschnitt 4 - a-govern-the-cloud 2 - Standard-Workloads	cloudtrail-security-trail-enabled	Diese Regel hilft sicherzustellen, dass die AWS empfohlenen bewährten Sicherheitsmethoden für verwendet werden AWS CloudTrail, indem geprüft wird, ob mehrere Einstellungen aktiviert sind. Dazu gehören die Verwendung von Protokollverschlüsselung, Protokollvalidierung und Aktivierung AWS CloudTrail in mehreren Regionen.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 a-govern-the-cloud — 2 — Standard-Workloads	cloudwatch-alarm-action-check	Amazon CloudWatch alarmiert , wenn eine Metrik den Schwellenwert für eine bestimmte Anzahl von Bewertungszeiträumen überschreitet. Der Alarm führt eine oder mehrere Aktionen durch, die vom Wert der Metrik oder des Ausdrucks im Vergleich zu einem Schwellenwert in einer Reihe von Zeiträumen abhängt. Diese Regel erfordert einen Wert für alarmActionRequired (Config Default: True), insufficientDataActionRequired (Config Default: True), okActionRequired (Config Default: False). Der tatsächliche Wert muss die Alarmaktionen für Ihre Umgebung widerspiegeln.
Abschnitt 4 a-govern-the-cloud — 2 — Standard-Workloads	cloud-trail-cloud-watch-logs-aktiviert	Verwenden Sie Amazon CloudWatch , um Protokoll ereignisaktivitäten zentral zu sammeln und zu verwalten . Die Aufnahme von AWS CloudTrail Daten liefert Einzelheiten zu den API-Aufrufaktivitäten in Ihrem AWS-Konto.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 a-govern-the-cloud — 2 — Standard-Workloads	ec2-manager instance-managed-by-systems	Eine Bestandsaufnahme der Softwareplattformen und Anwendungen innerhalb des Unternehmens ist möglich, indem Amazon Elastic Compute Cloud (Amazon EC2) -Instances mit AWS Systems Manager verwaltet werden. Verwenden Sie AWS Systems Manager, um detaillierte Systemkonfigurationen, Betriebssystem-Patch-Levels, Namen und Typ der Dienste, Softwareinstallationen, Anwendungsname, Herausgeber und Version sowie andere Details zu Ihrer Umgebung bereitzustellen.
Abschnitt 4 a-govern-the-cloud - 2 - Standard-Workloads	guardduty-enabled-centralized	Amazon GuardDuty kann mithilfe von Threat Intelligence Feeds helfen, potenzielle Cybersicherheitsereignisse zu überwachen und zu erkennen. Dazu gehören Listen mit bösartigen IPs und maschinellen Lernmethoden zur Identifizierung unerwarteter, nicht autorisierter und bösartiger Aktivitäten in Ihrer AWS Cloud-Umgebung.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 a-govern-the-cloud — 2 — Standard-Workloads	securityhub-enabled	AWS Security Hub hilft bei der Überwachung von unbefugte m Personal, Verbindungen, Geräten und Software. AWS Security Hub aggregiert, organisiert und priorisiert die Sicherheitswarnungen oder Ergebnisse mehrerer Dienste. AWS Einige dieser Dienste sind Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer und AWS Firewall Manager sowie AWS Partnerlösungen.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4-3-materielle Arbeitslasten a-govern-the-cloud	dynamodb-throughput-limit-check	Aktivieren Sie diese Regel, um sicherzustellen, dass die bereitgestellte Durchsatz kapazität in Ihren Amazon-DynamoDB-Tabellen überprüft wird. Dies ist der Umfang der Lese- und Schreibaktivitäten, der von den jeweiligen Tabellen unterstützt werden kann. DynamoDB verwendet diese Informationen für das Reservieren ausreichender Systemressourcen, um Ihren Durchsatzanforderungen gerecht zu werden. Diese Regel generiert eine Warnung, wenn sich der Durchsatz dem Höchstlimit für ein Kundenkonto nähert. Mit dieser Regel können Sie optional die Parameter RCUThreshold Kontoprozentsatz (Konfigurationsstandard: 80) und WCUThreshold Kontoprozentsatz (Konfigurationsstandard: 80) festlegen. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 a-govern-the-cloud — 3 — materielle Arbeitsbelastungen	lambda-concurrency-check	Diese Regel stellt sicher, dass die Höchst- und Untergrenzen für die Gleichzeitigkeit einer Lambda-Funktion festgelegt werden. Dies kann Sie beim Baselining für die Anzahl der Anforderungen unterstützen, die Ihre Funktion zu einem bestimmten Zeitpunkt verarbeitet.
Abschnitt 4 a-govern-the-cloud -3-Standard-Workloads	ec2-manager instance-managed-by-systems	Eine Bestandsaufnahme der Softwareplattformen und Anwendungen innerhalb des Unternehmens ist möglich, indem Amazon Elastic Compute Cloud (Amazon EC2) -Instances mit AWS Systems Manager verwaltet werden. Verwenden Sie AWS Systems Manager, um detaillierte Systemkonfigurationen, Betriebssystem-Patch-Levels, Namen und Typ der Dienste, Softwareinstallationen, Anwendungsname, Herausgeber und Version sowie andere Details zu Ihrer Umgebung bereitzustellen.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 a-govern-the-cloud — 3-Standard-Workloads	ec2-stopped-instance	Aktivieren Sie diese Regel, um bei der Basiskonfiguration von Amazon Elastic Compute Cloud (Amazon EC2) - Instances zu helfen, indem Sie überprüfen, ob EC2 Amazon-Instances gemäß den Standards Ihrer Organisat ion für mehr als die zulässige Anzahl von Tagen gestoppt wurden.
Abschnitt 4 a-govern-the-cloud — 3-Standard-Workloads	ec2- volume-inuse-check	Diese Regel stellt sicher, dass Amazon Elastic Block Store-Volumes, die an Amazon Elastic Compute Cloud (Amazon EC2) -Instances angehängt sind, zum Löschen markiert werden, wenn eine Instance beendet wird. Wenn ein Amazon-EBS-Volume nicht gelöscht wird, wenn die Instance, an die es angehängt ist, beendet wird, kann dies gegen das Konzept der geringsten Funktionalität verstoßen.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 a-govern-the-cloud — 3-Standard-Workloads	eip-attached	Diese Regel stellt sicher, dass Elastic, die einer Amazon Virtual Private Cloud (Amazon VPC) IPs zugewiesen sind, an Amazon Elastic Compute Cloud (Amazon EC2) - Instances oder verwendete Elastic Network Interfaces angehängt sind. Diese Regel hilft bei der Überwachung ungenutzter Inhalte EIPs in Ihrer Umgebung.
Abschnitt 4 a-govern-the-cloud -3-Standard-Workloads	vpc-network-acl-unused-überprüfen	Diese Regel stellt sicher, dass Amazon Virtual Private Cloud (VPC)-Netzwerkzugriffskontrolllisten verwendet werden. Die Überwachung ungenutzter Netzwerkzugriffskontrolllisten kann zu einer genauen Inventarisierung und Verwaltung Ihrer Umgebung beitragen.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 b-design-and-secure — Die Cloud-1-Standard-Workloads	autoscaling-launch-config-public-ip-deaktiviert	Wenn Sie Ihre Netzwerkschnittstellen mit einer öffentlichen IP-Adresse konfigurieren, sind die diesen Netzwerkschnittstellen zugehörigen Ressourcen über das Internet erreichbar. EC2 Ressourcen sollten nicht öffentlich zugänglich sein, da dies einen unbeabsichtigten Zugriff auf Ihre Anwendungen oder Server ermöglichen kann.
Abschnitt 4 b-design-and-secure — Die Cloud-1-Standard-Workloads	dms-replication-not-public	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass auf DMS-Replikationsinstanzen nicht öffentlich zugegriffen werden kann. DMS-Replikations-Instances können vertrauliche Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.
Abschnitt 4 b-design-and-secure — Die Cloud-1-Standard-Workloads	ebs-snapshot-public-restorable-überprüfen	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass EBS-Snapshots nicht öffentlich wiederherstellbar sind. EBS-Volume-Snapshots können vertrauliche Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	AWS Config	Empfehlungen
b-design-and-secureAbschnitt 4 — Die Cloud-1-Standard-Workloads	ec2- instance-no-public-ip	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon Elastic Compute Cloud (Amazon EC2) -Instances nicht öffentlich zugänglich sind. EC2Amazon-Instances können vertrauliche Informationen enthalten, und für solche Konten ist eine Zugriffskontrolle erforderlich.
Abschnitt 4 b-design-and-secure — Die Cloud-1-Standard-Workloads	ec2- instance-profile-attached	EC2 Instanzprofile übergeben eine IAM-Rolle an eine EC2 Instance. Das Anhängen eines Instance-Profils an Ihre Instances kann bei der Implementierung von geringsten Berechtigungen und der Berechtigungsverwaltung helfen.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 b-design-and-secure — Die Cloud-1-Standard-Workloads	ecs-task-definition-user-for-host-mode-check	Wenn für eine Aufgabendefinition erhöhte Berechtigungen gelten, liegt das daran, dass der Kunde diesen Konfigurationen ausdrücklich zugestimmt hat. Diese Kontrolle prüft, ob eine unerwartete Berechtigungseskalation vorliegt, wenn für eine Aufgabendefinition das Host-Netzwerk aktiviert ist, die Kunden aber keine erhöhten Berechtigungen aktiviert haben.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 — b-design-and-secure Cloud-1-Standard-Workloads	emr-kerberos-enabled	Die Zugriffsberechtigungen und -autorisierungen können verwaltet und nach den Prinzipien der geringsten Berechtigung und Aufgabentrennung integriert werden, indem Kerberos für Amazon-EMR-Cluster aktiviert wird. In Kerberos werden Services und Benutzer, die sich authentifizieren müssen, als Prinzipale bezeichnet. Prinzipale befinden sich in einem Kerberos-Bereich. Innerhalb dieses Bereichs wird ein Kerberos-Server als Key Distribution Center (KDC) bezeichnet. Über diesen Server können sich Prinzipale authentifizieren. Die Authentifizierung im KDC erfolgt durch die Ausstellung von Authentifizierungstickets. Das KDC unterhält eine Datenbank der Prinzipale in seinem Bereich mit ihren Passwörtern und anderen administrativen Informationen zu jedem Prinzipal.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 — b-design-and-secure Cloud-1-Standard-Workloads	emr-master-no-public-ip	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon EMR-Cluster-Masterknoten nicht öffentlich zugänglich sind. Amazon-EMR-Cluster-Hauptknoten können vertrauliche Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 b-design-and-secure — Die Cloud-1-Standard-Workloads	iam-customer-policy-blocked-kms-Aktionen	AWS Identity and Access Management (IAM) kann Ihnen dabei helfen, die Prinzipien der geringsten Rechte und der Aufgabentrennung in Zugriffsberechtigungen und Autorisierungen zu integrieren und so zu verhindern, dass Richtlinien blockierte Aktionen für alle AWS Schlüssel des Key Management Service enthalten. Wenn Benutzer mehr Rechte haben, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und Aufgabentrennung verstoßen. Mit dieser Regel können Sie den Parameter festlegen. blockedActionsPatterns (Wert „AWS Bewährte grundlegende Sicherheitsmethoden“: kms: Decrypt, kms:ReEncryptFrom). Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 — Die Cloud-1-Standard-Workloads b-design-and-secure	iam-group-has-users-überprüfen	AWS Identity and Access Management (IAM) kann Ihnen helfen, die Prinzipien der geringsten Rechte und der Aufgabentrennung mit Zugriffsberechtigungen und Autorisierungen zu integrieren, indem sichergestellt wird, dass IAM-Gruppen mindestens einen Benutzer haben. Die Einteilung von Benutzern in Gruppen auf der Grundlage der ihnen zugewiesenen Berechtigungen oder ihrer Funktion ist eine Möglichkeit, das Prinzip der geringsten Berechtigung zu implementieren.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 — Die Cloud-1-Standard-Workloads b-design-and-secure	iam-inline-policy-blocked-kms-Aktionen	Stellen Sie sicher, dass ein Benutzer, eine IAM-Rolle oder eine IAM-Gruppe (AWS Identity and Access Management) nicht über eine Inline-Richtlinie verfügt, die blockierte Aktionen für alle AWS Schlüssel des Key Management Service zulässt. AWS empfiehlt, verwaltete Richtlinien anstelle von Inline-Richtlinien zu verwenden. Verwaltete Richtlinien ermöglichen Wiederverwendbarkeit, Versionsverwaltung, Rollback und Delegierung der Berechtigungsverwaltung. Mit dieser Regel können Sie den blockedActionsPatterns Parameter festlegen. (Wert „AWS Bewährte grundlegende Sicherheitsmethoden“: kms: Decrypt, kms:ReEncryptFrom). Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 — Die Cloud-1-Standard-Workloads b-design-and-secure	iam-no-inline-policy-überprüfen	Stellen Sie sicher, dass ein Benutzer, eine IAM-Rolle oder eine IAM-Gruppe (AWS Identity and Access Management) nicht über eine Inline-Richtlinie zur Zugriffskontrolle auf Systeme und Ressourcen verfügt. AWS empfiehlt, verwaltete Richtlinien anstelle von Inline-Richtlinien zu verwenden . Verwaltete Richtlinien ermöglichen Wiederverwendbarkeit, Versionsverwaltung, Rollback und Delegierung der Berechtigungsverwaltung.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 b-design-and-secure — Die Cloud-1-Standard-Workloads	iam-password-policy	Die Identitäten und Anmeldeinformationen werden auf der Grundlage einer organisatorischen IAM-Passwortrichtlinie ausgestellt, verwaltet und verifiziert. Sie erfüllen oder übertreffen die Anforderungen von NIST SP 800-63 und dem Standard „Best Practices“ von Foundational Security für die Passwortstärke. AWS Mit dieser Regel können Sie optional RequireUppercaseCharacters (Wert für AWS grundlegende Sicherheitsbewährte Methoden: wahr), RequireLowercaseCharacters (Wert für bewährte Methoden für AWS grundlegende Sicherheit: wahr), RequireSymbols (Wert für bewährte Methoden für AWS grundlegende Sicherheit: wahr), RequireNumbers (Wert für bewährte Methoden für AWS grundlegende Sicherheit: wahr), MinimumPasswordLength (Wert für bewährte Methoden für AWS grundlegende Sicherheit: 14), PasswordReusePrevention (Wert für bewährte Methoden für AWS grundlegende Sicherheit: 24) und

Kontroll-ID	AWS Config	Empfehlungen
		MaxPasswordAge (Wert für bewährte Methoden für AWS grundlegende Sicherheit: 90) für Ihr IAM festlegen Kennwortrichtlinie. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.
Abschnitt 4 b-design-and-secure — Die Cloud-1-Standard-Workloads	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) kann Ihnen dabei helfen, die Prinzipien der geringsten Rechte und der Aufgabentrennung in Zugriffsberechtigungen und Autorisierungen zu integrieren und so zu verhindern, dass Richtlinien „Effect“: „Allow“ mit „Action“: „*“ anstelle von „Resource“: „*“ enthalten. Wenn Benutzern mehr Rechte eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und der Aufgabentrennung verstoßen.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt b-design-and-secure 4 — Die Cloud-1-Standard-Workloads	iam-policy-no-statements-with-full-access	Stellen Sie sicher, dass IAM-Aktionen nur auf die benötigten Aktionen beschränkt sind. Wenn Benutzern mehr Rechte eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und der Aufgabentrennung verstoßen.
Abschnitt 4 — b-design-and-secure Cloud-1-Standard-Workloads	iam-root-access-key-überprüfen	Der Zugriff auf Systeme und Ressourcen kann gesteuert werden, indem überprüft wird, ob der Root-Benutzer keine Zugriffsschlüssel mit seiner AWS Identity and Access Management (IAM) -Rolle verknüpft hat. Stellen Sie sicher, dass die Root-Zugriffsschlüssel gelöscht werden. Erstellen und verwenden Sie stattdessen rollenbasierte Funktionen, AWS-Konten um das Prinzip der geringsten Funktionalität zu berücksichtigen.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 — Die Cloud-1-Standard-Workloads b-design-and-secure	iam-user-group-membership-überprüfen	AWS Identity and Access Management (IAM) kann Ihnen helfen, Zugriffsberechtigungen und Autorisierungen einzuschränken, indem sichergestellt wird, dass Benutzer Mitglieder mindestens einer Gruppe sind. Wenn Benutzern mehr Berechtigungen eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und Aufgabentrennung verstoßen.
Abschnitt 4 — Die Cloud-1-Standard-Workloads b-design-and-secure	iam-user-mfa-enabled	Aktivieren Sie diese Regel, um den Zugriff auf Ressourcen in der AWS -Cloud einzuschränken. Diese Regel stellt sicher, dass die Multi-Faktor-Authentifizierung (MFA) für alle Benutzer aktiviert ist. MFA bietet eine weitere Schutzebene zusätzlich zum Benutzernamen und Passwort. Reduzieren Sie Fälle von kompromittierten Konten, indem Sie MFA für Benutzer vorschreiben.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 — b-design-and-secure Cloud-1-Standard-Workloads	iam-user-no-policies-überprüfen	Diese Regel stellt sicher, dass AWS Identity and Access Management (IAM) -Richtlinien nur Gruppen oder Rollen zugewiesen werden, um den Zugriff auf Systeme und Ressourcen zu kontrollieren. Die Zuweisung von Berechtigungen auf Gruppen- oder Rollenebene trägt dazu bei, die Wahrscheinlichkeit zu verringern, dass eine Identität übermäßige Berechtigungen erhält oder beibehält.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 b-design-and-secure — Die Cloud-1-Standard-Workloads	iam-user-unused-credentials-überprüfen	AWS Identity and Access Management (IAM) kann Ihnen bei Zugriffsberechtigungen und Autorisierungen helfen, indem es nach IAM-Passwörtern und Zugriffsschlüsseln sucht, die für einen bestimmten Zeitraum nicht verwendet wurden. Wenn ungenutzte Anmeldeinformationen identifiziert werden, müssen Sie sie deaktivieren und/oder entfernen, da dies gegen das Prinzip der geringsten Berechtigung verstoßen könnte. Für diese Regel müssen Sie einen Wert für das maxCredentialUsage Alter festlegen (Standardkonfiguration: 90). Der tatsächliche Wert muss den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 b-design-and-secure — Die Cloud-1-Standard-Workloads	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) Security Groups können bei der Verwaltung des Netzwerkzugriffs helfen, indem sie eine statusbehaftete Filterung des ein- und ausgehenden Netzwerkverkehrs zu Ressourcen bereitstellen. AWS Wenn Sie eingehenden (oder entfernten) Datenverkehr von 0.0.0.0/0 bis Port 22 auf Ihren Ressourcen nicht zulassen, können Sie den Remote-Zugriff einschränken.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 — Die Cloud-1-Standard-Workloads b-design-and-secure	ec2- instances-in-vpc	Stellen Sie Amazon Elastic Compute Cloud (Amazon EC2) -Instances innerhalb einer Amazon Virtual Private Cloud (Amazon VPC) bereit, um eine sichere Kommunikation zwischen einer Instance und anderen Services innerhalb der Amazon VPC zu ermöglichen, ohne dass ein Internet-Gateway, ein NAT-Gerät oder eine VPN-Verbindung erforderlich ist. Der gesamte Datenverkehr bleibt sicher in der AWS Cloud. Domains, die sich innerhalb einer VPC befinden, verfügen aufgrund ihrer logischen Isolierung im Vergleich zu Domains mit öffentlichen Endpunkten über eine zusätzliche Sicherheitsebene. Weisen Sie EC2 Amazon-Instances einer Amazon-VPC zu, um den Zugriff ordnungsgemäß zu verwalten.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 b-design-and-secure — Cloud-1-Standard-Workloads	internet-gateway-authorized-vpc-nur	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Internet-Gateways nur mit autorisierter Amazon Virtual Private Cloud (Amazon VPC) verbunden sind. Internet-Gateways ermöglichen den bidirekti onalen Internetzugang zur und von der Amazon VPC, was möglicherweise zu einem unbefugten Zugriff auf Amazon-VPC-Ressourcen führen kann.
Abschnitt 4 — Die Cloud-1-S tandard-Workloads b-design-and-secure	lambda-function-public-acce ss-verboten	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherste llen, dass AWS Lambda-Funktionen nicht öffentlich zugänglich sind. Der öffentlic he Zugriff kann möglicher weise die Verfügbarkeit von Ressourcen beeinträchtigen.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 b-design-and-secure — Die Cloud-1-Standard-Workloads	lambda-inside-vpc	Stellen Sie AWS Lambda-Funktionen in einer Amazon Virtual Private Cloud (Amazon VPC) bereit, um eine sichere Kommunikation zwischen einer Funktion und anderen Diensten innerhalb der Amazon VPC zu gewährleisten. Bei dieser Konfiguration sind kein Internet-Gateway, kein NAT-Gerät und keine VPN-Verbindung erforderlich. Der gesamte Datenverkehr bleibt sicher in der Cloud. AWS Domains, die sich innerhalb einer VPC befinden, verfügen aufgrund ihrer logischen Isolierung im Vergleich zu Domains mit öffentlichen Endpunkten über eine zusätzliche Sicherheitsebene. Um den Zugriff ordnungsgemäß zu verwalten, sollten AWS Lambda-Funktionen einer VPC zugewiesen werden.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 — Die Cloud-1-Standard-Workloads b-design-and-secure	mfa-enabled-for-iam-Konsolenzugriff	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass MFA für alle AWS Identity and Access Management (IAM) -Benutzer aktiviert ist, die über ein Konsolenkennwort verfügen. MFA sorgt für eine weitere Schutzebene zusätzlich zu den Anmeldeinformationen. Indem Sie MFA für Benutzer vorschreiben, können Sie Fälle kompromittierter Konten reduzieren und verhindern, dass unbefugte Benutzer auf vertrauliche Daten zugreifen.
Abschnitt 4 — Die Cloud-1-Standard-Workloads b-design-and-secure	no-unrestricted-route-to-igw	Stellen Sie sicher, dass EC2 Amazon-Routentabellen keine uneingeschränkten Routen zu einem Internet-Gateway enthalten. Durch das Entfernen oder Beschränken des Internetzugangs für Workloads innerhalb von Amazon VPCs können unbeabsichtigte Zugriffe in Ihrer Umgebung reduziert werden.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 — Die Cloud-1-Standard-Workloads b-design-and-secure	rds-instance-public-access-überprüfen	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Relational Database Service (Amazon RDS) -Instances nicht öffentlich sind. Amazon-RDS-Datenbank-Instances können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.
Abschnitt 4 b-design-and-secure — Die Cloud-1-Standard-Workloads	redshift-cluster-public-access-überprüfen	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Redshift Redshift-Cluster nicht öffentlich sind. Amazon-Redshift-Cluster können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 b-design-and-secure — Die Cloud-1-Standard-Workloads	redshift-enhanced-vpc-routing-aktiviert	Mit Enhanced-VPC-Routing wird erzwungen, dass der gesamte COPY- und UNLOAD-Datenverkehr zwischen Ihrem Cluster und Datenrepositorys über Ihre Amazon VPC erfolgt. Anschließend können Sie VPC-Features wie Sicherheitsgruppen und Netzwerkzugriffskontrollisten verwenden, um den Netzwerkverkehr zu schützen. Sie können auch VPC-Flow-Protokolle verwenden, um den Netzwerkverkehr zu überwachen.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 b-design-and-secure — Die Cloud-1-Standard-Workloads	restricted-common-ports	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass gemeinsame Ports für Amazon Elastic Compute Cloud (Amazon EC2) - Sicherheitsgruppen eingeschränkt sind. Wenn der Zugriff auf Ports nicht auf vertrauenswürdige Quellen beschränkt wird, kann dies zu Angriffen auf die Verfügbarkeit, Integrität und Vertraulichkeit von Systemen führen. Mit dieser Regel können Sie optional die Parameter blockedPort1–blockedPort5 festlegen (Standardkonfigurationen: 20, 21, 3389, 3306, 4333). Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 b-design-and-secure — Die Cloud-1-Standard-Workloads	root-account-hardware-mfa-aktiviert	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Hardware-MFA für den Root-Benutzer aktiviert ist. Der Stammbenutzer ist der AWS-Konto-Benutzer mit den meisten Berechtigungen. MFA sorgt für eine weitere Schutzebene zusätzlich zu den Anmeldeinformationen. Indem Sie MFA für den Root-Benutzer vorschreiben, können Sie die Anzahl AWS-Konten kompromittierter Benutzer reduzieren.
Abschnitt 4 — Die Cloud-1-Standard-Workloads b-design-and-secure	root-account-mfa-enabled	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass MFA für den Root-Benutzer aktiviert ist. Der Stammbenutzer ist der AWS-Konto-Benutzer mit den meisten Berechtigungen. MFA bietet eine weitere Schutzebene zusätzlich zum Benutzernamen und Passwort. Indem Sie MFA für den Root-Benutzer vorschreiben, können Sie die Anzahl AWS-Konten kompromittierter Benutzer reduzieren.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 — Die Cloud-1-Standard-Workloads b-design-and-secure	s3- -Blöcke — periodisch account-level-public-access	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Simple Storage Service (Amazon S3) -Buckets nicht öffentlich zugänglich sind. Diese Regel trägt dazu bei, sensible Daten vor unbefugten Remote-Benutzern zu schützen, indem sie den öffentlichen Zugriff verhindert. Mit dieser Regel können Sie optional die Parameter ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) und restrictPublicBuckets Parameter (Config Default: True) festlegen. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 b-design-and-secure — Die Cloud-1-Standard-Workloads	s3- bucket-public-read-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie nur autorisierten Benutzern, Prozessen und Geräten Zugriff auf Amazon Simple Storage Service (Amazon S3) -Buckets gewähren. Die Verwaltung des Zugriffs sollte mit der Klassifizierung der Daten übereinstimmen.
Abschnitt 4 b-design-and-secure — Die Cloud-1-Standard-Workloads	s3- bucket-public-write-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie nur autorisierten Benutzern, Prozessen und Geräten Zugriff auf Amazon Simple Storage Service (Amazon S3) -Buckets gewähren. Die Verwaltung des Zugriffs sollte mit der Klassifizierung der Daten übereinstimmen.
Abschnitt 4 b-design-and-secure — Die Cloud-1-Standard-Workloads	sagemaker-notebook-no-direct-Internetzugang	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass SageMaker Amazon-Notebooks keinen direkten Internetzugang zulassen. Indem Sie direkten Internetzugang blockieren, vermeiden Sie, dass unbefugte Benutzer auf sensible Daten zugreifen.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 b-design-and-secure — Die Cloud-1-Standard-Workloads	ssm-document-not-public	Stellen Sie sicher, dass AWS Systems Manager (SSM) - Dokumente nicht öffentlich sind, da dies einen unbeabsichtigten Zugriff auf Ihre SSM-Dokumente ermöglichen kann. Ein öffentliches SSM-Dokument kann Informationen über Ihr Konto, Ihre Ressourcen und internen Prozesse preisgeben.
b-design-and-secureAbschnitt 4 — Die Cloud-1-Standard-Workloads	vpc-default-security-group-geschlossen	Sicherheitsgruppen von Amazon Elastic Compute Cloud (Amazon EC2) können bei der Verwaltung des Netzwerkzugriffs helfen, indem sie eine statusbehaftete Filterung des ein- und ausgehenden Netzwerkverkehrs zu Ressourcen bereitstellen. AWS Die Beschränkung des gesamten Datenverkehrs auf die Standardsicherheitsgruppe hilft dabei, den Fernzugriff auf Ihre Ressourcen einzuschränken. AWS

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 — Die Cloud-1-Standard-Workloads b-design-and-secure	vpc-sg-open-only-to-authorized-ports	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass gemeinsame Ports für Amazon Elastic Compute Cloud (Amazon EC2) - Sicherheitsgruppen eingeschränkt sind. Wenn der Zugriff auf Ports nicht auf vertrauenswürdige Quellen beschränkt wird, kann dies zu Angriffen auf die Verfügbarkeit, Integrität und Vertraulichkeit von Systemen führen. Durch die Beschränkung des Zugriffs auf Ressourcen innerhalb einer Sicherheitsgruppe aus dem Internet (0.0.0.0/0) kann der Remote-Zugriff auf interne Systeme gesteuert werden.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 b-design-and-secure — Die Cloud-1-Standard-Workloads	ecs-containers-nonprivileged	Um die Implementierung des Prinzips der geringsten Berechtigung zu unterstützen, dürfen in Amazon Elastic Container Service (Amazon ECS)-Aufgabendefinitionen keine erhöhten Berechtigungen aktiviert sein. Wenn dieser Parameter den Wert „true“ aufweist, erhält der Container erhöhte Berechtigungen auf der Host-Container-Instance (ähnlich wie der Root-Benutzer).
Abschnitt 4 — b-design-and-secure Cloud-1-Standard-Workloads	s3- verboten bucket-level-public-access	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Simple Storage Service (Amazon S3) -Buckets nicht öffentlich zugänglich sind. Diese Regel trägt dazu bei, sensible Daten vor unbefugten Remote-Benutzern zu schützen, indem sie den öffentlichen Zugriff auf Bucket-Ebene verhindert.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 b-design-and-secure — Die Cloud-1-Standard-Workloads	subnet-auto-assign-public-ip-deaktiviert	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon Virtual Private Cloud (VPC) -Subnetzen nicht automatisch eine öffentliche IP-Adresse zugewiesen wird. Amazon Elastic Compute Cloud (EC2) -Instances, die in Subnetzen gestartet werden, in denen dieses Attribut aktiviert ist, haben ihrer primären Netzwerkschnittstelle eine öffentliche IP-Adresse zugewiesen.
Abschnitt 4 b-design-and-secure — Die Cloud-2-Standard-Workloads	cloudtrail-security-trail-enabled	Diese Regel trägt dazu bei, die Verwendung der AWS empfohlenen bewährten Sicherheitsmethoden für sicherzustellen, indem geprüft wird AWS CloudTrail, ob mehrere Einstellungen aktiviert sind. Dazu gehören die Verwendung von Protokoll verschlüsselung, Protokoll validierung und Aktivierung AWS CloudTrail in mehreren Regionen.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 b-design-and-secure — Die Cloud — 2 — Standard-Workloads	ec2-manager instance-managed-by-systems	Eine Bestandsaufnahme der Softwareplattformen und Anwendungen innerhalb des Unternehmens ist möglich, indem Amazon Elastic Compute Cloud (Amazon EC2) -Instances mit AWS Systems Manager verwaltet werden. Verwenden Sie AWS Systems Manager, um detaillierte Systemkonfigurationen, Betriebssystem-Patch-Levels, Namen und Typ der Dienste, Softwareinstallationen, Anwendungsname, Herausgeber und Version sowie andere Details zu Ihrer Umgebung bereitzustellen.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 b-design-and-secure — Die Cloud-2-Standard-Workloads	ec2-prüfen managedinstance-association-compliance-status	Verwenden Sie AWS Systems Manager Associations, um bei der Inventarisierung von Softwareplattformen und Anwendungen innerhalb eines Unternehmens zu helfen. AWS Systems Manager weist Ihren verwalteten Instances einen Konfigurationsstatus zu und ermöglicht es Ihnen, Basiswerte für Betriebssystem-Patch-Levels, Softwareinstallationen, Anwendungskonfigurationen und andere Details zu Ihrer Umgebung festzulegen.
Abschnitt 4 b-design-and-secure — Die Cloud — 2 — Standard-Workloads	ec2-prüfen managedinstance-patch-compliance-status	Aktivieren Sie diese Regel, um bei der Identifizierung und Dokumentation von Sicherheitslücken in Amazon Elastic Compute Cloud (Amazon EC2) zu helfen. Die Regel prüft, ob die EC2 Amazon-Instance die Patch-Konformität im AWS Systems Manager gemäß den Richtlinien und Verfahren Ihrer Organisation einhält.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 b-design-and-secure — Cloud-2-Standard-Workloads	redshift-cluster-maintenancesettings-check	Diese Regel stellt sicher, dass Amazon-Redshift-Cluster die bevorzugten Einstellungen für Ihre Organisation haben. Insbesondere sorgt sie dafür, dass Cluster bevorzugte Wartungsfenster und automatisierte Aufbewahrungsfristen für Snapshots für die Datenbank haben. Für diese Regel müssen Sie die festlegen. allowVersionUpgrade Der Standardwert ist „true“. Außerdem können Sie optional den Zeitraum preferredMaintenanceWindow (der Standardwert ist sa: 16:00 -sa: 16:30) und den automatedSnapshotRetention Zeitraum (der Standardwert ist 1) festlegen. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 — Die Cloud — 3 — materielle Workloads b-design-and-secure	dynamodb-autoscaling-enabled	Amazon DynamoDB Auto Scaling verwendet den AWS Application Auto Scaling-Service, um die bereitgestellte Durchsatzkapazität so anzupassen, dass sie automatisch auf tatsächliche Verkehrsmuster reagiert. Auf diese Weise kann eine Tabelle oder ein globaler sekundärer Index die bereitgestellte Lese-/Schreibkapazität erhöhen, um plötzliche Erhöhungen des Datenverkehrs ohne Drosselung zu bewältigen.
b-design-and-secureAbschnitt 4 — Die Cloud — 3 — materielle Workloads	elb-cross-zone-load-Balancing aktiviert	Aktivieren Sie zonenübergreifendes Load Balancing für Ihre Elastic Load Balancer (ELBs), um eine angemessene Kapazität und Verfügbarkeit aufrechtzuerhalten. Zonenübergreifendes Load Balancing reduziert die Notwendigkeit, die gleiche Anzahl von Instances in jeder aktivierten Availability Zone aufrechtzuerhalten. Es verbessert auch die Fähigkeit Ihrer Anwendung, den Verlust einer oder mehrerer Instances zu bewältigen.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 — Die Cloud — 3 — materielle Workloads b-design-and-secure	elb-deletion-protection-enabled	Diese Regel sorgt dafür, dass der Löschschutz für Elastic Load Balancing aktiviert ist. Verwenden Sie diese Funktion, um zu verhindern, dass Ihr Load Balancer versehentlich oder böswillig gelöscht wird, was zum Verlust der Verfügbarkeit Ihrer Anwendungen führen kann.
Abschnitt 4 — Die Wolke b-design-and-secure — 3 — materielle Workloads	rds-instance-deletion-protection-aktiviert	Stellen Sie sicher, dass Amazon Relational Database Service (Amazon RDS)-Instances den Löschschutz aktiviert haben. Verwenden Sie den Löschschutz, um zu verhindern, dass Ihre Amazon-RDS-Instances versehentlich oder böswillig gelöscht werden, was zum Verlust der Verfügbarkeit Ihrer Anwendungen führen kann.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 b-design-and-secure — Die Cloud — 3 — materielle Workloads	rds-multi-az-support	Die Multi-AZ-Unterstützung in Amazon Relational Database Service (Amazon RDS) bietet eine verbesserte Verfügbar keit und Beständigkeit von Datenbank-Instances. Wenn Sie eine Multi-AZ-Datenbank-Instance bereitstellen, erstellt Amazon RDS automatisch eine primäre Datenbank-Instance und repliziert die Daten synchron auf eine Standby-Instance in einer anderen Availability Zone. Jede Availability Zone läuft auf einer eigenen, physisch getrennten, unabhängigen Infrastruktur und ist auf eine hohe Verfügbarkeit ausgelegt . Im Falle eines Infrastru kturausfalls führt Amazon RDS einen automatischen Failover zum Standby-Modus durch, sodass Sie den Datenbank betrieb wieder aufnehmen können, sobald der Failover abgeschlossen ist.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 — Die Wolke b-design-and-secure — 3 — materielle Workloads	rds-cluster-multi-az-aktiviert	Die Multi-AZ-Unterstützung in Amazon Relational Database Service (Amazon RDS) bietet eine verbesserte Verfügbar keit und Beständigkeit von Datenbank-Instances. Wenn Sie eine Multi-AZ-Datenbank-Instance bereitstellen, erstellt Amazon RDS automatisch eine primäre Datenbank-Instance und repliziert die Daten synchron auf eine Standby-Instance in einer anderen Availability Zone. Jede Availability Zone läuft auf einer eigenen, physisch getrennten, unabhängigen Infrastruktur und ist auf eine hohe Verfügbarkeit ausgelegt . Im Falle eines Infrastru kturausfalls führt Amazon RDS einen automatischen Failover zum Standby-Modus durch, sodass Sie den Datenbank betrieb wieder aufnehmen können, sobald der Failover abgeschlossen ist.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 b-design-and-secure — Die Cloud — 3 — materielle Workloads	s3- bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) unterstützt die Aufrechte rhaltung einer angemessenen Kapazität und Verfügbarkeit. CRR ermöglicht das automatis che, asynchrone Kopieren von Objekten in Amazon-S3 -Buckets, um die Datenverf ügbarkeit sicherzustellen.
Abschnitt 4 b-design-and-secure — die Cloud-3-S tandard-Workloads	autoscaling-group-elb-healt hcheck-erforderlich	Die Elastic Load Balancer (ELB) -Zustandsprüfungen für Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling Scaling-Gruppen unterstützen die Aufrechte rhaltung einer angemessenen Kapazität und Verfügbarkeit. Der Load Balancer sendet regelmäßig Pings, versucht Verbindungen herzustellen oder sendet Anfragen, um den Zustand der EC2 Amazon-In stances in einer Gruppe mit auto-scaling zu testen. Wenn eine Instance nicht zurückmel det, wird der Traffic an eine neue EC2 Amazon-Instance gesendet.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 b-design-and-secure — Die Cloud-3-Standard-Workloads	dynamodb-autoscaling-enabled	Amazon DynamoDB Auto Scaling verwendet den AWS Application Auto Scaling-Service, um die bereitgestellte Durchsatzkapazität so anzupassen, dass sie automatisch auf tatsächliche Verkehrsmuster reagiert. Auf diese Weise kann eine Tabelle oder ein globaler sekundärer Index die bereitgestellte Lese-/Schreibkapazität erhöhen, um plötzliche Erhöhungen des Datenverkehrs ohne Drosselung zu bewältigen.
b-design-and-secureAbschnitt 4 — Die Cloud-3-Standard-Workloads	ec2- instance-detailed-monitoring-enabled	Aktivieren Sie diese Regel, um die Amazon Elastic Compute Cloud (Amazon EC2) -Instance-Überwachung auf der EC2 Amazon-Konsole zu verbessern, in der Monitoring-Diagramme mit einem Zeitraum von 1 Minute für die Instance angezeigt werden.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 b-design-and-secure — Die Cloud-3-Standard-Workloads	elb-cross-zone-load-Balancing aktiviert	Aktivieren Sie zonenüber greifendes Load Balancing für Ihre Elastic Load Balancer (ELBs), um eine angemessene Kapazität und Verfügbarkeit aufrechtzuerhalten. Zonenübergreifendes Load Balancing reduziert die Notwendigkeit, die gleiche Anzahl von Instances in jeder aktivierten Availability Zone aufrechtzuerhalten. Es verbessert auch die Fähigkeit Ihrer Anwendung, den Verlust einer oder mehrerer Instances zu bewältigen.
Abschnitt 4 — Die Cloud-3-Standard-Workloads b-design-and-secure	elb-deletion-protection-enabled	Diese Regel sorgt dafür, dass der Löschschutz für Elastic Load Balancing aktiviert ist. Verwenden Sie diese Funktion, um zu verhindern, dass Ihr Load Balancer versehentlich oder böswillig gelöscht wird, was zum Verlust der Verfügbarkeit Ihrer Anwendungen führen kann.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 — Die b-design-and-secure Cloud-3-Standard-Workloads	rds-enhanced-monitoring-enabled	Aktivieren Sie Amazon Relational Database Service (Amazon RDS), um die Verfügbarkeit von Amazon RDS zu überwachen. Dies bietet einen detaillierten Einblick in den Zustand Ihrer Amazon-RDS-Datenbank-Instances. Wenn der Amazon-RDS-Speicher mehr als ein zugrunde liegendes physisches Gerät verwendet, erfasst Enhanced Monitoring die Daten für jedes Gerät. Wenn die Datenbank-Instance von Amazon RDS in einer Multi-AZ-Bereitstellung ausgeführt wird, werden außerdem die Daten für jedes Gerät auf dem sekundären Host sowie die Metriken des sekundären Hosts erfasst.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 — Die b-design-and-secure Cloud-3-Standard-Workloads	rds-multi-az-support	Die Multi-AZ-Unterstützung in Amazon Relational Database Service (Amazon RDS) bietet eine verbesserte Verfügbar keit und Beständigkeit von Datenbank-Instances. Wenn Sie eine Multi-AZ-Datenbank-Instance bereitstellen, erstellt Amazon RDS automatisch eine primäre Datenbank-Instance und repliziert die Daten synchron auf eine Standby-Instance in einer anderen Availability Zone. Jede Availability Zone läuft auf einer eigenen, physisch getrennten, unabhängigen Infrastruktur und ist auf eine hohe Verfügbarkeit ausgelegt . Im Falle eines Infrastru kturausfalls führt Amazon RDS einen automatischen Failover zum Standby-Modus durch, sodass Sie den Datenbank betrieb wieder aufnehmen können, sobald der Failover abgeschlossen ist.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 — Die b-design-and-secure Cloud-3-Standard-Workloads	rds-cluster-multi-az-aktiviert	Die Multi-AZ-Unterstützung in Amazon Relational Database Service (Amazon RDS) bietet eine verbesserte Verfügbar keit und Beständigkeit von Datenbank-Instances. Wenn Sie eine Multi-AZ-Datenbank-Instance bereitstellen, erstellt Amazon RDS automatisch eine primäre Datenbank-Instance und repliziert die Daten synchron auf eine Standby-Instance in einer anderen Availability Zone. Jede Availability Zone läuft auf einer eigenen, physisch getrennten, unabhängigen Infrastruktur und ist auf eine hohe Verfügbarkeit ausgelegt . Im Falle eines Infrastru kturausfalls führt Amazon RDS einen automatischen Failover zum Standby-Modus durch, sodass Sie den Datenbank betrieb wieder aufnehmen können, sobald der Failover abgeschlossen ist.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 b-design-and-secure — die Cloud-3-Standard-Workloads	beanstalk-enhanced-health-reporting-aktiviert	AWS Die verbesserte Zustandsberichterstattung von Elastic Beanstalk ermöglicht eine schnellere Reaktion auf Veränderungen im Zustand der zugrunde liegenden Infrastruktur. Diese Änderungen könnten zu einer mangelnden Verfügbarkeit der Anwendung führen. Die erweiterten Zustandsberichte von Elastic Beanstalk bieten eine Statusbeschreibung, um den Schweregrad der identifizierten Probleme einzuschätzen und mögliche Ursachen zu identifizieren, die untersucht werden müssen.
Abschnitt 4 — Die Cloud — 4 — materielle Workloads b-design-and-secure	alb-waf-enabled	Stellen Sie sicher, dass AWS WAF auf Elastic Load Balancers (ELB) aktiviert ist, um Webanwendungen zu schützen. Eine WAF trägt zum Schutz Ihrer Webanwendungen oder APIs vor gängigen Web-Exploits bei. Diese Web-Exploits können sich auf die Verfügbarkeit auswirken, die Sicherheit gefährden oder übermäßige Ressourcen in Ihrer Umgebung verbrauchen.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 — Die Cloud — 4 — materielle Workloads b-design-and-secure	api-gw-associated-with-WAF	AWS Mit WAF können Sie eine Reihe von Regeln (als Web Access Control List (Web ACL) bezeichnet) konfiguri eren, die Webanfragen auf der Grundlage von anpassbar en Websicherheitsregeln und -bedingungen, die Sie definieren, zulassen, blockiere n oder zählen. Stellen Sie sicher, dass Ihre Amazon-API-Gateway-Stufe mit einer WAF-Web-ACL verknüpft ist, um sie vor böswilligen Angriffen zu schützen.
Abschnitt 4 b-design-and-secure — Die Cloud — 4 — materielle Workloads	autoscaling-launch-config-public-ip-deaktiviert	Wenn Sie Ihre Netzwerks chnittstellen mit einer öffentlic hen IP-Adresse konfigurieren, sind die diesen Netzwerks chnittstellen zugehörigen Ressourcen über das Internet erreichbar. EC2 Ressource n sollten nicht öffentlich zugänglich sein, da dies einen unbeabsichtigten Zugriff auf Ihre Anwendungen oder Server ermöglichen kann.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 b-design-and-secure — Die Cloud-4-Material-Workloads	dms-replication-not-public	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass auf DMS-Replikationsinstanzen nicht öffentlich zugegriffen werden kann. DMS-Replikations-Instances können vertrauliche Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.
Abschnitt 4 b-design-and-secure — Die Cloud — 4 — materielle Workloads	ec2- instance-no-public-ip	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon Elastic Compute Cloud (Amazon EC2) -Instances nicht öffentlich zugänglich sind. EC2Amazon-Instances können vertrauliche Informationen enthalten, und für solche Konten ist eine Zugriffskontrolle erforderlich.
Abschnitt 4 b-design-and-secure — Die Cloud — 4 — materielle Workloads	emr-master-no-public-ip	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon EMR-Cluster-Masterknoten nicht öffentlich zugänglich sind. Amazon-EMR-Cluster-Hauptknoten können vertrauliche Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 b-design-and-secure — Die Cloud — 4 — materielle Workloads	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) Security Groups können bei der Verwaltung des Netzwerkz ugriffs helfen, indem sie eine statusbehaftete Filterung des ein- und ausgehend en Netzwerkverkehrs zu Ressourcen bereitstellen. AWS Wenn Sie eingehenden (oder entfernten) Datenverk ehr von 0.0.0.0/0 bis Port 22 auf Ihren Ressourcen nicht zulassen, können Sie den Remote-Zugriff einschränken.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 — Die Cloud — 4 — materielle Workloads b-design-and-secure	ec2- instances-in-vpc	Stellen Sie Amazon Elastic Compute Cloud (Amazon EC2) -Instances innerhalb einer Amazon Virtual Private Cloud (Amazon VPC) bereit, um eine sichere Kommunika tion zwischen einer Instance und anderen Services innerhalb der Amazon VPC zu ermöglichen, ohne dass ein Internet-Gateway, ein NAT-Gerät oder eine VPN-Verbi ndung erforderlich ist. Der gesamte Datenverkehr bleibt sicher in der AWS Cloud. Domains, die sich innerhalb einer VPC befinden, verfügen aufgrund ihrer logischen Isolierung im Vergleich zu Domains mit öffentlic hen Endpunkten über eine zusätzliche Sicherheitsebene. Weisen Sie EC2 Amazon-In stances einer Amazon-VPC zu, um den Zugriff ordnungsg emäß zu verwalten.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 b-design-and-secure — Die Cloud-4-Material-Workloads	internet-gateway-authorized-vpc-nur	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Internet-Gateways nur mit autorisierter Amazon Virtual Private Cloud (Amazon VPC) verbunden sind. Internet-Gateways ermöglichen den bidirektionalen Internetzugang zur und von der Amazon VPC, was möglicherweise zu einem unbefugten Zugriff auf Amazon-VPC-Ressourcen führen kann.
Abschnitt 4 — Die Cloud-4-materiellen Workloads b-design-and-secure	lambda-function-public-access-verboten	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass AWS Lambda-Funktionen nicht öffentlich zugänglich sind. Der öffentliche Zugriff kann möglicherweise die Verfügbarkeit von Ressourcen beeinträchtigen.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 b-design-and-secure — Die Cloud — 4 — materielle Workloads	lambda-inside-vpc	Stellen Sie AWS Lambda-Funktionen in einer Amazon Virtual Private Cloud (Amazon VPC) bereit, um eine sichere Kommunikation zwischen einer Funktion und anderen Diensten innerhalb der Amazon VPC zu gewährleisten. Bei dieser Konfiguration sind kein Internet-Gateway, kein NAT-Gerät und keine VPN-Verbindung erforderlich. Der gesamte Datenverkehr bleibt sicher in der Cloud. AWS Domains, die sich innerhalb einer VPC befinden, verfügen aufgrund ihrer logischen Isolierung im Vergleich zu Domains mit öffentlichen Endpunkten über eine zusätzliche Sicherheitsebene. Um den Zugriff ordnungsgemäß zu verwalten, sollten AWS Lambda-Funktionen einer VPC zugewiesen werden.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 — Die Cloud — 4 — materielle Workloads b-design-and-secure	no-unrestricted-route-to-igw	Stellen Sie sicher, dass EC2 Amazon-Routentabellen keine uneingeschränkten Routen zu einem Internet-Gateway enthalten. Durch das Entfernen oder Beschränken des Internetzugangs für Workloads innerhalb von Amazon VPCs können unbeabsichtigte Zugriffe in Ihrer Umgebung reduziert werden.
Abschnitt 4 — Die Cloud-4-Material-Workloads b-design-and-secure	opensearch-in-vpc-only	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass sich Amazon OpenSearch Service-Domains innerhalb einer Amazon Virtual Private Cloud (Amazon VPC) befinden. Eine Amazon OpenSearch Service-Domain innerhalb einer Amazon VPC ermöglicht die sichere Kommunikation zwischen Amazon OpenSearch Service und anderen Services innerhalb der Amazon VPC, ohne dass ein Internet-Gateway, ein NAT-Gerät oder eine VPN-Verbindung erforderlich ist.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 — Die Cloud-4-Material-Workloads b-design-and-secure	rds-instance-public-access-überprüfen	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Relational Database Service (Amazon RDS) -Instances nicht öffentlich sind. Amazon-RDS-Datenbank-Instances können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.
Abschnitt 4 b-design-and-secure — Die Cloud — 4 — materielle Workloads	redshift-cluster-public-access-überprüfen	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Redshift Redshift-Cluster nicht öffentlich sind. Amazon-Redshift-Cluster können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 b-design-and-secure — Die Cloud — 4 — materielle Workloads	restricted-common-ports	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass gemeinsame Ports für Amazon Elastic Compute Cloud (Amazon EC2) - Sicherheitsgruppen eingeschränkt sind. Wenn der Zugriff auf Ports nicht auf vertrauenswürdige Quellen beschränkt wird, kann dies zu Angriffen auf die Verfügbarkeit, Integrität und Vertraulichkeit von Systemen führen. Mit dieser Regel können Sie optional die Parameter blockedPort1–blockedPort5 festlegen (Standardkonfigurationen: 20, 21, 3389, 3306, 4333). Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 b-design-and-secure — Die Cloud — 4 — materielle Workloads	s3- -Blöcke — periodisch account-level-public-access	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Simple Storage Service (Amazon S3) -Buckets nicht öffentlich zugänglich sind. Diese Regel trägt dazu bei, sensible Daten vor unbefugten Remote-Benutzern zu schützen, indem sie den öffentlichen Zugriff verhindert. Mit dieser Regel können Sie optional die Parameter ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) und restrictPublicBuckets Parameter (Config Default: True) festlegen. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 b-design-and-secure — Die Cloud-4-Material-Workloads	sagemaker-notebook-no-direct-Internetzugang	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass SageMaker Amazon-Notebooks keinen direkten Internetzugang zulassen. Indem Sie direkten Internetzugang blockieren, vermeiden Sie, dass unbefugte Benutzer auf sensible Daten zugreifen.
Abschnitt 4 b-design-and-secure — Die Cloud — 4 — materielle Workloads	ssm-document-not-public	Stellen Sie sicher, dass AWS Systems Manager (SSM) - Dokumente nicht öffentlich sind, da dies einen unbeabsichtigten Zugriff auf Ihre SSM-Dokumente ermöglichen kann. Ein öffentliches SSM-Dokument kann Informationen über Ihr Konto, Ihre Ressourcen und internen Prozesse preisgeben.

Kontroll-ID	AWS Config	Empfehlungen
b-design-and-secureAbschnitt 4 — Die Cloud-4-Material-Workloads	vpc-default-security-group-geschlossen	Sicherheitsgruppen von Amazon Elastic Compute Cloud (Amazon EC2) können bei der Verwaltung des Netzwerkzugriffs helfen, indem sie eine statusbehaftete Filterung des ein- und ausgehenden Netzwerkverkehrs zu Ressourcen bereitstellen. AWS Die Beschränkung des gesamten Datenverkehrs auf die Standardsicherheitsgruppe hilft dabei, den Fernzugriff auf Ihre Ressourcen einzuschränken. AWS

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 — Die Cloud-4-materiellen Workloads b-design-and-secure	vpc-sg-open-only-to-authorized-ports	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass gemeinsame Ports für Amazon Elastic Compute Cloud (Amazon EC2) - Sicherheitsgruppen eingeschränkt sind. Wenn der Zugriff auf Ports nicht auf vertrauenswürdige Quellen beschränkt wird, kann dies zu Angriffen auf die Verfügbarkeit, Integrität und Vertraulichkeit von Systemen führen. Durch die Beschränkung des Zugriffs auf Ressourcen innerhalb einer Sicherheitsgruppe aus dem Internet (0.0.0.0/0) kann der Remote-Zugriff auf interne Systeme gesteuert werden.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 b-design-and-secure — Die Cloud — 4 — materielle Workloads	vpc-vpn-2-tunnels-up	Redundante Site-to-Site VPN-Tunnel können implement iert werden, um die Anforderu ngen an die Ausfallsicherheit zu erfüllen. Es verwendet zwei Tunnel, um die Konnektiv ität sicherzustellen, falls eine der Site-to-Site VPN-Verbi ndungen nicht verfügbar ist. Um sich vor einem Verbindun gsverlust zu schützen, können Sie für den Fall, dass Ihr Kunden-Gateway nicht verfügbar ist, eine zweite Site-to-Site VPN-Verbindung zu Ihrer Amazon Virtual Private Cloud (Amazon VPC) und Ihrem Virtual Private Gateway einrichten, indem Sie ein zweites Kunden-Gateway verwenden.
Abschnitt 4 b-design-and-secure — Die Cloud — 4 — materielle Workloads	s3- verboten bucket-level-publi c-access	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherste llen, dass Amazon Simple Storage Service (Amazon S3) -Buckets nicht öffentlich zugänglich sind. Diese Regel trägt dazu bei, sensible Daten vor unbefugten Remote-Be nutzern zu schützen, indem sie den öffentlichen Zugriff auf Bucket-Ebene verhindert.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 b-design-and-secure — Die Cloud-4-Material-Workloads	subnet-auto-assign-public-ip-deaktiviert	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon Virtual Private Cloud (VPC) -Subnetzen nicht automatisch eine öffentliche IP-Adresse zugewiesen wird. Amazon Elastic Compute Cloud (EC2) -Instances, die in Subnetzen gestartet werden, in denen dieses Attribut aktiviert ist, haben ihrer primären Netzwerkschnittstelle eine öffentliche IP-Adresse zugewiesen.
Abschnitt 4 b-design-and-secure — Die Cloud-4-Standard-Workloads	alb-waf-enabled	Stellen Sie sicher, dass AWS WAF auf Elastic Load Balancers (ELB) aktiviert ist, um Webanwendungen zu schützen. Eine WAF trägt zum Schutz Ihrer Webanwendungen oder APIs vor gängigen Web-Exploits bei. Diese Web-Exploits können sich auf die Verfügbarkeit auswirken, die Sicherheit gefährden oder übermäßige Ressourcen in Ihrer Umgebung verbrauchen.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 — Die Cloud — 4-Standard-Workloads b-design-and-secure	api-gw-associated-with-WAF	AWS Mit WAF können Sie eine Reihe von Regeln (als Web Access Control List (Web ACL) bezeichnet) konfiguri eren, die Webanfragen auf der Grundlage von anpassbar en Websicherheitsregeln und -bedingungen, die Sie definieren, zulassen, blockiere n oder zählen. Stellen Sie sicher, dass Ihre Amazon-API-Gateway-Stufe mit einer WAF-Web-ACL verknüpft ist, um sie vor böswilligen Angriffen zu schützen.
Abschnitt 4 b-design-and-secure — Cloud-4-Standard-Workloads	autoscaling-launch-config-public-ip-deaktiviert	Wenn Sie Ihre Netzwerks chnittstellen mit einer öffentlic hen IP-Adresse konfigurieren, sind die diesen Netzwerks chnittstellen zugehörigen Ressourcen über das Internet erreichbar. EC2 Ressource n sollten nicht öffentlich zugänglich sein, da dies einen unbeabsichtigten Zugriff auf Ihre Anwendungen oder Server ermöglichen kann.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 b-design-and-secure — Die Cloud-4-S tandard-Workloads	ec2- instance-no-public-ip	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon Elastic Compute Cloud (Amazon EC2) -Instances nicht öffentlich zugänglich sind. EC2Amazon-Instances können vertrauliche Informati onen enthalten, und für solche Konten ist eine Zugriffsk ontrolle erforderlich.
Abschnitt 4 b-design-and-secure — Die Cloud-4-S tandard-Workloads	ec2- instance-profile-attached	EC2 Instanzprofile übergeben eine IAM-Rolle an eine EC2 Instance. Das Anhängen eines Instance-Profils an Ihre Instances kann bei der Implementierung von geringsten Berechtigungen und der Berechtigungsverwa ltung helfen.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 b-design-and-secure — Cloud-4-Standard-Workloads	ecs-task-definition-user-for-host-mode-check	Wenn für eine Aufgabend efinition erhöhte Berechtig ungen gelten, liegt das daran, dass der Kunde diesen Konfigurationen ausdrücklich zugestimmt hat. Diese Kontrolle prüft, ob eine unerwartete Berechtig ungseskalation vorliegt, wenn für eine Aufgabendefinition das Host-Netzwerk aktiviert ist, die Kunden aber keine erhöhten Berechtigungen aktiviert haben.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 — Die b-design-and-secure Cloud-4-Standard-Workloads	emr-kerberos-enabled	Die Zugriffsberechtigungen und -autorisierungen können verwaltet und nach den Prinzipien der geringsten Berechtigung und Aufgabent rennung integriert werden, indem Kerberos für Amazon-EMR-Cluster aktiviert wird. In Kerberos werden Services und Benutzer, die sich authentifizieren müssen, als Prinzipale bezeichnet. Prinzipale befinden sich in einem Kerberos-Bereich. Innerhalb dieses Bereichs wird ein Kerberos-Server als Key Distribution Center (KDC) bezeichnet. Über diesen Server können sich Prinzipale authentifizieren. Die Authentifizierung im KDC erfolgt durch die Ausstellu ng von Authentifizierungs tickets. Das KDC unterhält eine Datenbank der Prinzipal e in seinem Bereich mit ihren Passwörtern und anderen administrativen Informationen zu jedem Prinzipal.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 — Die b-design-and-secure Cloud-4-Standard-Workloads	emr-master-no-public-ip	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon EMR-Cluster-Masterknoten nicht öffentlich zugänglich sind. Amazon-EMR-Cluster-Hauptknoten können vertrauliche Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.
Abschnitt 4 b-design-and-secure — Cloud-4-Standard-Workloads	guardduty-enabled-centralized	Amazon GuardDuty kann mithilfe von Threat Intelligence Feeds helfen, potenzielle Cybersicherheitsereignisse zu überwachen und zu erkennen. Dazu gehören Listen mit bösartigen IPs und maschinellen Lernmethoden zur Identifizierung unerwarteter, nicht autorisierter und bösartiger Aktivitäten in Ihrer AWS Cloud-Umgebung.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 b-design-and-secure — Die Cloud-4-S tandard-Workloads	iam-customer-policy-blocked-kms-Aktionen	AWS Identity and Access Management (IAM) kann Ihnen dabei helfen, die Prinzipien der geringsten Rechte und der Aufgabent rennung in Zugriffsberechtigu ngen und Autorisierungen zu integrieren und so zu verhindern, dass Richtlini en blockierte Aktionen für alle AWS Schlüssel des Key Management Service enthalten. Wenn Benutzer mehr Rechte haben, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtig ung und Aufgabentrennung verstoßen. Mit dieser Regel können Sie den Parameter festlegen. blockedActionsPatt erns (Wert „AWS Bewährte grundlegende Sicherhei tsmethoden“: kms: Decrypt, kms:ReEncryptFrom). Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisat ion entsprechen.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 — Cloud-4-Standard-Workloads b-design-and-secure	iam-group-has-users-überprüfen	AWS Identity and Access Management (IAM) kann Ihnen helfen, die Prinzipien der geringsten Rechte und der Aufgabentrennung mit Zugriffsberechtigungen und Autorisierungen zu integrieren, indem sichergestellt wird, dass IAM-Gruppen mindestens einen Benutzer haben. Die Einteilung von Benutzern in Gruppen auf der Grundlage der ihnen zugewiesenen Berechtigungen oder ihrer Funktion ist eine Möglichkeit, das Prinzip der geringsten Berechtigung zu implementieren.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 — Die Cloud-4-Standard-Workloads b-design-and-secure	iam-inline-policy-blocked-kms-Aktionen	Stellen Sie sicher, dass ein Benutzer, eine IAM-Rolle oder eine IAM-Gruppe (AWS Identity and Access Management) nicht über eine Inline-Richtlinie verfügt, die blockierte Aktionen für alle AWS Schlüssel des Key Management Service zulässt. AWS empfiehlt, verwaltete Richtlinien anstelle von Inline-Richtlinien zu verwenden . Verwaltete Richtlinien ermöglichen Wiederverwendbarkeit, Versionsverwaltung, Rollback und Delegierung der Berechtigungsverwaltung. Mit dieser Regel können Sie den blockedActionsPatterns Parameter festlegen. (Wert „AWS Bewährte grundlegende Sicherheitsmethoden“: kms: Decrypt, kms:ReEncryptFrom). Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 — Cloud-4-Standard-Workloads b-design-and-secure	iam-password-policy	Die Identitäten und Anmeldeinformationen werden auf der Grundlage einer organisatorischen IAM-Passwortrichtlinie ausgestellt, verwaltet und verifiziert. Sie erfüllen oder übertreffen die Anforderungen von NIST SP 800-63 und dem Standard „Best Practices“ von Foundational Security für die Passwortstärke. AWS Mit dieser Regel können Sie optional RequireUppercaseCharacters (Wert für AWS grundlegende Sicherheitsbewährte Methoden: wahr), RequireLowercaseCharacters (Wert für bewährte Methoden für AWS grundlegende Sicherheit: wahr), RequireSymbols (Wert für bewährte Methoden für AWS grundlegende Sicherheit: wahr), RequireNumbers (Wert für bewährte Methoden für AWS grundlegende Sicherheit: wahr), MinimumPasswordLength (Wert für bewährte Methoden für AWS grundlegende Sicherheit: 14), PasswordReusePrevention (Wert für bewährte Methoden für AWS grundlegende Sicherheit: 24) und

Kontroll-ID	AWS Config	Empfehlungen
		MaxPasswordAge (Wert für bewährte Methoden für AWS grundlegende Sicherheit: 90) für Ihr IAM festlegen Kennwortrichtlinie. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.
Abschnitt 4 b-design-and-secure — Die Cloud — 4-Standard-Workloads	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) kann Ihnen dabei helfen, die Prinzipien der geringsten Rechte und der Aufgabentrennung in Zugriffsberechtigungen und Autorisierungen zu integrieren und so zu verhindern, dass Richtlinien „Effect“: „Allow“ mit „Action“: „*“ anstelle von „Resource“: „*“ enthalten. Wenn Benutzern mehr Rechte eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und der Aufgabentrennung verstoßen.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt b-design-and-secure 4 — Die Cloud-4-Standard-Workloads	iam-policy-no-statements-with-full-access	Stellen Sie sicher, dass IAM-Aktionen nur auf die benötigten Aktionen beschränkt sind. Wenn Benutzern mehr Rechte eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und der Aufgabentrennung verstoßen.
Abschnitt 4 — Die b-design-and-secure Cloud-4-Standard-Workloads	iam-root-access-key-überprüfen	Der Zugriff auf Systeme und Ressourcen kann gesteuert werden, indem überprüft wird, ob der Root-Benutzer keine Zugriffsschlüssel mit seiner AWS Identity and Access Management (IAM) -Rolle verknüpft hat. Stellen Sie sicher, dass die Root-Zugriffsschlüssel gelöscht werden. Erstellen und verwenden Sie stattdessen rollenbasierte Funktionen, AWS-Konten um das Prinzip der geringsten Funktionalität zu berücksichtigen.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 — Cloud-4-Standard-Workloads b-design-and-secure	iam-user-group-membership-überprüfen	AWS Identity and Access Management (IAM) kann Ihnen helfen, Zugriffsberechtigungen und Autorisierungen einzuschränken, indem sichergestellt wird, dass Benutzer Mitglieder mindestens einer Gruppe sind. Wenn Benutzern mehr Berechtigungen eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und Aufgabentrennung verstoßen.
Abschnitt 4 — Die Cloud-4-Standard-Workloads b-design-and-secure	iam-user-mfa-enabled	Aktivieren Sie diese Regel, um den Zugriff auf Ressourcen in der AWS -Cloud einzuschränken. Diese Regel stellt sicher, dass die Multi-Faktor-Authentifizierung (MFA) für alle Benutzer aktiviert ist. MFA bietet eine weitere Schutzebene zusätzlich zum Benutzernamen und Passwort. Reduzieren Sie Fälle von kompromittierten Konten, indem Sie MFA für Benutzer vorschreiben.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 — Die b-design-and-secure Cloud-4-Standard-Workloads	iam-user-no-policies-überprüfen	Diese Regel stellt sicher, dass AWS Identity and Access Management (IAM) -Richtlinien nur Gruppen oder Rollen zugewiesen werden, um den Zugriff auf Systeme und Ressourcen zu kontrollieren. Die Zuweisung von Berechtigungen auf Gruppen- oder Rollenebene trägt dazu bei, die Wahrscheinlichkeit zu verringern, dass eine Identität übermäßige Berechtigungen erhält oder beibehält.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 b-design-and-secure — Cloud-4-Standard-Workloads	iam-user-unused-credentials-überprüfen	AWS Identity and Access Management (IAM) kann Ihnen bei Zugriffsberechtigungen und Autorisierungen helfen, indem es nach IAM-Passwörtern und Zugriffsschlüsseln sucht, die für einen bestimmten Zeitraum nicht verwendet wurden. Wenn ungenutzte Anmeldeinformationen identifiziert werden, müssen Sie sie deaktivieren und/oder entfernen, da dies gegen das Prinzip der geringsten Berechtigung verstoßen könnte. Für diese Regel müssen Sie einen Wert für das maxCredentialUsage Alter festlegen (Standardkonfiguration: 90). Der tatsächliche Wert muss den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 b-design-and-secure — Die Cloud-4-S tandard-Workloads	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) Security Groups können bei der Verwaltung des Netzwerkz ugriffs helfen, indem sie eine statusbehaftete Filterung des ein- und ausgehend en Netzwerkverkehrs zu Ressourcen bereitstellen. AWS Wenn Sie eingehenden (oder entfernten) Datenverk ehr von 0.0.0.0/0 bis Port 22 auf Ihren Ressourcen nicht zulassen, können Sie den Remote-Zugriff einschränken.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 — Die Cloud-4-Standard-Workloads b-design-and-secure	ec2- instances-in-vpc	Stellen Sie Amazon Elastic Compute Cloud (Amazon EC2) -Instances innerhalb einer Amazon Virtual Private Cloud (Amazon VPC) bereit, um eine sichere Kommunikation zwischen einer Instance und anderen Services innerhalb der Amazon VPC zu ermöglichen, ohne dass ein Internet-Gateway, ein NAT-Gerät oder eine VPN-Verbindung erforderlich ist. Der gesamte Datenverkehr bleibt sicher in der AWS Cloud. Domains, die sich innerhalb einer VPC befinden, verfügen aufgrund ihrer logischen Isolierung im Vergleich zu Domains mit öffentlichen Endpunkten über eine zusätzliche Sicherheitsebene. Weisen Sie EC2 Amazon-Instances einer Amazon-VPC zu, um den Zugriff ordnungsgemäß zu verwalten.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 b-design-and-secure — Cloud-4-Standard-Workloads	internet-gateway-authorized-vpc-nur	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Internet-Gateways nur mit autorisierter Amazon Virtual Private Cloud (Amazon VPC) verbunden sind. Internet-Gateways ermöglichen den bidirekti onalen Internetzugang zur und von der Amazon VPC, was möglicherweise zu einem unbefugten Zugriff auf Amazon-VPC-Ressourcen führen kann.
Abschnitt 4 — Die Cloud-4-S tandard-Workloads b-design-and-secure	lambda-function-public-acce ss-verboten	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherste llen, dass AWS Lambda-Funktionen nicht öffentlich zugänglich sind. Der öffentlic he Zugriff kann möglicher weise die Verfügbarkeit von Ressourcen beeinträchtigen.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 b-design-and-secure — Die Cloud-4-S tandard-Workloads	lambda-inside-vpc	Stellen Sie AWS Lambda-Funktionen in einer Amazon Virtual Private Cloud (Amazon VPC) bereit, um eine sichere Kommunikation zwischen einer Funktion und anderen Diensten innerhalb der Amazon VPC zu gewährlei sten. Bei dieser Konfigura tion sind kein Internet-Gateway, kein NAT-Gerät und keine VPN-Verbindung erforderlich. Der gesamte Datenverkehr bleibt sicher in der Cloud. AWS Domains, die sich innerhalb einer VPC befinden, verfügen aufgrund ihrer logischen Isolierung im Vergleich zu Domains mit öffentlichen Endpunkten über eine zusätzliche Sicherhei tsebene. Um den Zugriff ordnungsgemäß zu verwalten , sollten AWS Lambda-Fu nktionen einer VPC zugewiese n werden.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 — Die Cloud-4-Standard-Workloads b-design-and-secure	mfa-enabled-for-iam-Konsolenzugriff	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass MFA für alle AWS Identity and Access Management (IAM) -Benutzer aktiviert ist, die über ein Konsolenkennwort verfügen. MFA sorgt für eine weitere Schutzebene zusätzlich zu den Anmeldeinformationen. Indem Sie MFA für Benutzer vorschreiben, können Sie Fälle kompromittierter Konten reduzieren und verhindern, dass unbefugte Benutzer auf vertrauliche Daten zugreifen.
Abschnitt 4 — Die Cloud-4-Standard-Workloads b-design-and-secure	no-unrestricted-route-to-igw	Stellen Sie sicher, dass EC2 Amazon-Routentabellen keine uneingeschränkten Routen zu einem Internet-Gateway enthalten. Durch das Entfernen oder Beschränken des Internetzugangs für Workloads innerhalb von Amazon VPCs können unbeabsichtigte Zugriffe in Ihrer Umgebung reduziert werden.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 — Cloud-4-S tandard-Workloads b-design-and-secure	opensearch-in-vpc-only	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass sich Amazon OpenSearch Service-Domains innerhalb einer Amazon Virtual Private Cloud (Amazon VPC) befinden. Eine Amazon OpenSearch Service-Domain innerhalb einer Amazon VPC ermöglich t die sichere Kommunika tion zwischen Amazon OpenSearch Service und anderen Services innerhalb der Amazon VPC, ohne dass ein Internet-Gateway, ein NAT-Gerät oder eine VPN-Verbindung erforderlich ist.
Abschnitt 4 — Die Cloud-4-S tandard-Workloads b-design-and-secure	rds-instance-public-access-überprüfen	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherste llen, dass Amazon Relationa l Database Service (Amazon RDS) -Instances nicht öffentlic h sind. Amazon-RDS-Datenba nk-Instances können vertrauli che Informationen enthalten und für solche Konten sind Prinzipien und Zugriffsk ontrollen erforderlich.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 b-design-and-secure — Cloud-4-Standard-Workloads	redshift-cluster-public-access-überprüfen	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Redshift Redshift-Cluster nicht öffentlich sind. Amazon-Redshift-Cluster können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.
Abschnitt 4 b-design-and-secure — Die Cloud-4-Standard-Workloads	restricted-common-ports	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass gemeinsame Ports für Amazon Elastic Compute Cloud (Amazon EC2) - Sicherheitsgruppen eingeschränkt sind. Wenn der Zugriff auf Ports nicht auf vertrauenswürdige Quellen beschränkt wird, kann dies zu Angriffen auf die Verfügbarkeit, Integrität und Vertraulichkeit von Systemen führen. Mit dieser Regel können Sie optional die Parameter blockedPort1–blockedPort5 festlegen (Standardkonfigurationen: 20, 21, 3389, 3306, 4333). Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 b-design-and-secure — Die Cloud-4-Standard-Workloads	root-account-hardware-mfa-aktiviert	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Hardware-MFA für den Root-Benutzer aktiviert ist. Der Stammbenutzer ist der AWS-Konto-Benutzer mit den meisten Berechtigungen. MFA sorgt für eine weitere Schutzebene zusätzlich zu den Anmeldeinformationen. Indem Sie MFA für den Root-Benutzer vorschreiben, können Sie die Anzahl AWS-Konten kompromittierter Benutzer reduzieren.
Abschnitt 4 — Cloud-4-Standard-Workloads b-design-and-secure	root-account-mfa-enabled	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass MFA für den Root-Benutzer aktiviert ist. Der Stammbenutzer ist der AWS-Konto-Benutzer mit den meisten Berechtigungen. MFA bietet eine weitere Schutzebene zusätzlich zum Benutzernamen und Passwort. Indem Sie MFA für den Root-Benutzer vorschreiben, können Sie die Anzahl AWS-Konten kompromittierter Benutzer reduzieren.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 — Cloud-4-S tandard-Workloads b-design-and-secure	s3- -Blöcke — periodisch account-level-public-access	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherste llen, dass Amazon Simple Storage Service (Amazon S3) -Buckets nicht öffentlich zugänglich sind. Diese Regel trägt dazu bei, sensible Daten vor unbefugten Remote-Benutzern zu schützen, indem sie den öffentlichen Zugriff verhindert. Mit dieser Regel können Sie optional die Parameter ignorePub licAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPubl icAcls (Config Default: True) und restrictPublicBuckets Parameter (Config Default: True) festlegen. Die tatsächli chen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 b-design-and-secure — Die Cloud-4-S tandard-Workloads	sagemaker-notebook-no-direct-Internetzugang	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass SageMaker Amazon-Notebooks keinen direkten Internetzugang zulassen. Indem Sie direkten Internetzugang blockieren, vermeiden Sie, dass unbefugte Benutzer auf sensible Daten zugreifen.
Abschnitt 4 b-design-and-secure — Die Cloud-4-S tandard-Workloads	securityhub-enabled	AWS Security Hub hilft bei der Überwachung von unbefugtem Personal, Verbindungen, Geräten und Software. AWS Security Hub aggregiert, organisiert und priorisiert die Sicherheitswarnungen oder Ergebnisse mehrerer Dienste. AWS Einige dieser Dienste sind Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer und AWS Firewall Manager sowie AWS Partnerlösungen.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 — Die Cloud-4-Standard-Workloads b-design-and-secure	vpc-default-security-group-geschlossen	Sicherheitsgruppen von Amazon Elastic Compute Cloud (Amazon EC2) können bei der Verwaltung des Netzwerkzugriffs helfen, indem sie eine statusbehaftete Filterung des ein- und ausgehenden Netzwerkverkehrs zu Ressourcen bereitstellen. AWS Die Beschränkung des gesamten Datenverkehrs auf die Standardsicherheitsgruppe hilft dabei, den Fernzugriff auf Ihre Ressourcen einzuschränken. AWS

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 — Die Cloud-4-Standard-Workloads b-design-and-secure	vpc-sg-open-only-to-authorized-ports	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass gemeinsame Ports für Amazon Elastic Compute Cloud (Amazon EC2) - Sicherheitsgruppen eingeschränkt sind. Wenn der Zugriff auf Ports nicht auf vertrauenswürdige Quellen beschränkt wird, kann dies zu Angriffen auf die Verfügbarkeit, Integrität und Vertraulichkeit von Systemen führen. Durch die Beschränkung des Zugriffs auf Ressourcen innerhalb einer Sicherheitsgruppe aus dem Internet (0.0.0.0/0) kann der Remote-Zugriff auf interne Systeme gesteuert werden.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 b-design-and-secure — Die Cloud-4-S tandard-Workloads	vpc-vpn-2-tunnels-up	Redundante Site-to-Site VPN-Tunnel können implement iert werden, um die Anforderu ngen an die Ausfallsicherheit zu erfüllen. Es verwendet zwei Tunnel, um die Konnektiv ität sicherzustellen, falls eine der Site-to-Site VPN-Verbi ndungen nicht verfügbar ist. Um sich vor einem Verbindun gsverlust zu schützen, können Sie für den Fall, dass Ihr Kunden-Gateway nicht verfügbar ist, eine zweite Site-to-Site VPN-Verbindung zu Ihrer Amazon Virtual Private Cloud (Amazon VPC) und Ihrem Virtual Private Gateway einrichten, indem Sie ein zweites Kunden-Gateway verwenden.
Abschnitt 4 b-design-and-secure — Die Cloud-4-S tandard-Workloads	s3- verboten bucket-level-publi c-access	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherste llen, dass Amazon Simple Storage Service (Amazon S3) -Buckets nicht öffentlich zugänglich sind. Diese Regel trägt dazu bei, sensible Daten vor unbefugten Remote-Be nutzern zu schützen, indem sie den öffentlichen Zugriff auf Bucket-Ebene verhindert.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 b-design-and-secure — Cloud-4-Standard-Workloads	subnet-auto-assign-public-ip-deaktiviert	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon Virtual Private Cloud (VPC) -Subnetzen nicht automatis ch eine öffentliche IP-Adress e zugewiesen wird. Amazon Elastic Compute Cloud (EC2) -Instances, die in Subnetzen gestartet werden, in denen dieses Attribut aktiviert ist, haben ihrer primären Netzwerkschnittste lle eine öffentliche IP-Adresse zugewiesen.
Abschnitt 4 b-design-and-secure — Die Cloud — 5 — materielle Workloads	cmk-backing-key-rotation-ak tiviert	Aktivieren Sie die Schlüssel rotation, um sicherzustellen, dass Schlüssel rotiert werden, sobald sie das Ende ihrer Kryptoperiode erreicht haben.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 b-design-and-secure — Die Cloud — 5 — materielle Workloads	iam-root-access-key-überprüfen	Der Zugriff auf Systeme und Ressourcen kann gesteuert werden, indem überprüft wird, ob der Root-Benutzer keine Zugriffsschlüssel mit seiner AWS Identity and Access Management (IAM) -Rolle verknüpft hat. Stellen Sie sicher, dass die Root-Zugriffsschlüssel gelöscht werden. Erstellen und verwenden Sie stattdessen rollenbasierte Funktionen, AWS-Konten um das Prinzip der geringsten Funktionalität zu berücksichtigen.
Abschnitt 4 — Die Cloud — 5 materielle Workloads b-design-and-secure	iam-user-mfa-enabled	Aktivieren Sie diese Regel, um den Zugriff auf Ressourcen in der AWS -Cloud einzuschränken. Diese Regel stellt sicher, dass die Multi-Faktor-Authentifizierung (MFA) für alle Benutzer aktiviert ist. MFA bietet eine weitere Schutzebene zusätzlich zum Benutzernamen und Passwort. Reduzieren Sie Fälle von kompromittierten Konten, indem Sie MFA für Benutzer vorschreiben.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 — Die Wolke b-design-and-secure — 5 — materielle Workloads	mfa-enabled-for-iam-Konsolenzugriff	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass MFA für alle AWS Identity and Access Management (IAM) -Benutzer aktiviert ist, die über ein Konsolenkennwort verfügen. MFA sorgt für eine weitere Schutzebene zusätzlich zu den Anmeldeinformationen. Indem Sie MFA für Benutzer vorschreiben, können Sie Fälle kompromittierter Konten reduzieren und verhindern, dass unbefugte Benutzer auf vertrauliche Daten zugreifen.
Abschnitt 4 — Die Cloud — 5 — materielle Workloads b-design-and-secure	root-account-hardware-mfa-aktiviert	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Hardware-MFA für den Root-Benutzer aktiviert ist. Der Stammbenutzer ist der AWS-Konto-Benutzer mit den meisten Berechtigungen. MFA sorgt für eine weitere Schutzebene zusätzlich zu den Anmeldeinformationen. Indem Sie MFA für den Root-Benutzer vorschreiben, können Sie die Anzahl AWS-Konten kompromittierter Benutzer reduzieren.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 — Die Cloud-5-Standard-Workloads b-design-and-secure	acm-certificate-expiration-check	Stellen Sie sicher, dass die Netzwerkintegrität geschützt ist, indem Sie sicherstellen, dass X509-Zertifikate von ACM ausgestellt werden. AWS Diese Zertifikate müssen gültig und dürfen nicht abgelaufen sein. Für diese Regel ist ein Wert für erforderlich daysToExpiration (Wert für bewährte AWS Grundregeln für Sicherheit: 90). Der tatsächliche Wert muss den Richtlinien Ihrer Organisation entsprechen.
Abschnitt 4 b-design-and-secure — Die Cloud — 5 Standard-Workloads	cmk-backing-key-rotation-aktiviert	Aktivieren Sie die Schlüsselrotation, um sicherzustellen, dass Schlüssel rotiert werden, sobald sie das Ende ihrer Kryptoperiode erreicht haben.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 b-design-and-secure — Die Cloud-5-S tandard-Workloads	iam-customer-policy-blocked-kms-Aktionen	AWS Identity and Access Management (IAM) kann Ihnen dabei helfen, die Prinzipien der geringsten Rechte und der Aufgabent rennung in Zugriffsberechtigu ngen und Autorisierungen zu integrieren und so zu verhindern, dass Richtlini en blockierte Aktionen für alle AWS Schlüssel des Key Management Service enthalten. Wenn Benutzer mehr Rechte haben, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtig ung und Aufgabentrennung verstoßen. Mit dieser Regel können Sie den Parameter festlegen. blockedActionsPatt erns (Wert „AWS Bewährte grundlegende Sicherhei tsmethoden“: kms: Decrypt, kms:ReEncryptFrom). Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisat ion entsprechen.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 — Die Cloud-5-Standard-Workloads b-design-and-secure	iam-inline-policy-blocked-kms-Aktionen	Stellen Sie sicher, dass ein Benutzer, eine IAM-Rolle oder eine IAM-Gruppe (AWS Identity and Access Management) nicht über eine Inline-Richtlinie verfügt, die blockierte Aktionen für alle AWS Schlüssel des Key Management Service zulässt. AWS empfiehlt, verwaltete Richtlinien anstelle von Inline-Richtlinien zu verwenden . Verwaltete Richtlinien ermöglichen Wiederverwendbarkeit, Versionsverwaltung, Rollback und Delegierung der Berechtigungsverwaltung. Mit dieser Regel können Sie den blockedActionsPatterns Parameter festlegen. (Wert „AWS Bewährte grundlegende Sicherheitsmethoden“: kms: Decrypt, kms:ReEncryptFrom). Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 — Die Cloud-5-Standard-Workloads b-design-and-secure	iam-policy-no-statements-with-full-access	Stellen Sie sicher, dass IAM-Aktionen nur auf die benötigten Aktionen beschränkt sind. Wenn Benutzern mehr Rechte eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und der Aufgabentrennung verstoßen.
Abschnitt 4 — Die b-design-and-secure Cloud-5-Standard-Workloads	kms-cmk-not-scheduled-zum Löschen	Um Daten im Ruhezustand zu schützen, sollten Sie sicherstellen, dass die für den Kunden erforderlichen Masterschlüssel (CMKs) nicht für das Löschen im AWS Key Management Service (AWS KMS) vorgesehen sind. Da Schlüssel manchmal gelöscht werden müssen, können Sie mit dieser Regel alle zu löschenden Schlüssel überprüfen, falls ein Schlüssel versehentlich zur Löschung vorgemerkt wurde.
Abschnitt 4 b-design-and-secure — Die Cloud — sechs materielle Workloads	cmk-backing-key-rotation-aktiviert	Aktivieren Sie die Schlüssel rotation, um sicherzustellen, dass Schlüssel rotiert werden, sobald sie das Ende ihrer Kryptoperiode erreicht haben.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 b-design-and-secure — Die Cloud — 6 — materielle Workloads	iam-customer-policy-blocked-kms-Aktionen	AWS Identity and Access Management (IAM) kann Ihnen dabei helfen, die Prinzipien der geringsten Rechte und der Aufgabent rennung in Zugriffsberechtigu ngen und Autorisierungen zu integrieren und so zu verhindern, dass Richtlini en blockierte Aktionen für alle AWS Schlüssel des Key Management Service enthalten. Wenn Benutzer mehr Rechte haben, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtig ung und Aufgabentrennung verstoßen. Mit dieser Regel können Sie den Parameter festlegen. blockedActionsPatt erns (Wert „AWS Bewährte grundlegende Sicherhei tsmethoden“: kms: Decrypt, kms:ReEncryptFrom). Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisat ion entsprechen.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 — Die Cloud — sechs materielle Workloads b-design-and-secure	iam-inline-policy-blocked-kms-Aktionen	Stellen Sie sicher, dass ein Benutzer, eine IAM-Rolle oder eine IAM-Grupp e (AWS Identity and Access Management) nicht über eine Inline-Richtlinie verfügt, die blockierte Aktionen für alle AWS Schlüssel des Key Management Service zulässt. AWS empfiehlt, verwaltete Richtlinien anstelle von Inline-Richtlinien zu verwenden . Verwaltete Richtlinien ermöglichen Wiederver wendbarkeit, Versionsv erwaltung, Rollback und Delegierung der Berechtig ungsverwaltung. Mit dieser Regel können Sie den blockedActionsPatterns Parameter festlegen. (Wert „AWS Bewährte grundlege nde Sicherheitsmethoden“: kms: Decrypt, kms:ReEnc ryptFrom). Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprech en.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 — Die Cloud — sechs materielle Workloads b-design-and-secure	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) kann Ihnen dabei helfen, die Prinzipien der geringsten Rechte und der Aufgabent rennung in Zugriffsberechtigu ngen und Autorisierungen zu integrieren und so zu verhindern, dass Richtlinien „Effect“: „Allow“ mit „Action“: „*“ anstelle von „Resource“: „*“ enthalten. Wenn Benutzern mehr Rechte eingeräumt werden, als für die Ausführun g einer Aufgabe erforderl ich sind, kann dies gegen das Prinzip der geringste n Berechtigung und der Aufgabentrennung verstoßen.
Abschnitt 4 — Die b-design-and-secure Cloud-6-Material-Workloads	iam-policy-no-statements-with-full-access	Stellen Sie sicher, dass IAM-Aktionen nur auf die benötigte n Aktionen beschränkt sind. Wenn Benutzern mehr Rechte eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und der Aufgabentrennung verstoßen.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 — Die Cloud b-design-and-secure — sechs materielle Workloads	kms-cmk-not-scheduled-zum Löschen	Um Daten im Ruhezustand zu schützen, sollten Sie sicherstellen, dass die für den Kunden erforderlichen Masterschlüssel (CMKs) nicht für das Löschen im AWS Key Management Service (AWS KMS) vorgesehen sind. Da Schlüssel manchmal gelöscht werden müssen, können Sie mit dieser Regel alle zu löschenden Schlüssel überprüfen, falls ein Schlüssel versehentlich zur Löschung vorgemerkt wurde.
Abschnitt 4 b-design-and-secure — Cloud-6-Standard-Workloads	alb-http-drop-invalid-Header-fähig	Stellen Sie sicher, dass Ihre Elastic Load Balancers (ELB) so konfiguriert sind, dass sie HTTP-Header löschen. Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 — Die Cloud — 6-Standard-Workloads b-design-and-secure	alb-http-to-https-Umleitung sprüfung	Um Daten während der Übertragung zu schützen, stellen Sie sicher, dass Ihr Application Load Balancer unverschlüsselte HTTP-Anfragen automatisch an HTTPS umleitet. Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.
Abschnitt 4 — Die Cloud — 6 Standard-Workloads b-design-and-secure	api-gw-cache-enabled-und verschlüsselt	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass die Verschlüsselung für den Cache Ihrer API-Gatew ay-Stufe aktiviert ist. Da für die API-Methode sensible Daten erfasst werden können, sollten Sie die Verschlüsselung von Daten im Ruhezustand aktivieren, um diese Daten zu schützen.
Abschnitt 4 — Die Cloud — 6-Standard-Workloads b-design-and-secure	cloudwatch-log-group-encryp ted	Um sensible Daten im Ruhezustand zu schützen, stellen Sie sicher, dass die Verschlüsselung für Ihre Amazon CloudWatch Log Groups aktiviert ist.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 b-design-and-secure — Die Cloud — 6-Standard-Workloads	cloud-trail-encryption-enabled	Zum Schutz von eventuell vorhandenen sensiblen Daten sowie Daten im Ruhezusta nd müssen Sie sicherstellen, dass die Verschlüsselung für Ihre AWS CloudTrail aktiviert ist.
Abschnitt 4 — Die Cloud — 6 b-design-and-secure Standard-Workloads	dynamodb-table-encrypted-kms	Stellen Sie sicher, dass die Verschlüsselung für Ihre Amazon-DynamoDB-Tabellen aktiviert ist. Um eventuell vorhandene sensible Daten im Ruhezustand in diesen Tabellen zu schützen, müssen Sie die Verschlüsselung von Daten im Ruhezustand aktivieren. Standardmäßig werden DynamoDB-Tabellen mit einem AWS eigenen Kundenhauptschlüssel (CMK) verschlüsselt.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 — b-design-and-secure Cloud-6-Standard-Workloads	ec2- ebs-encryption-by-default	Zum Schutz von Daten im Ruhezustand müssen Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon Elastic Block Store (Amazon EBS)-Volumes aktiviert ist. Da sensible Daten auch im Ruhezustand vorhanden sein können, sollten Sie die Verschlüsselung im Ruhezustand aktivieren, um diese Daten zu schützen.
Abschnitt 4 b-design-and-secure — Die Cloud — 6 — Standard-Workloads	efs-encrypted-check	Aktivieren Sie die Verschlüsselung für Ihr Amazon Elastic File System (EFS), um eventuell vorhandene sensible Daten sowie Daten im Ruhezustand zu schützen.
Abschnitt 4 — Die Cloud — 6 b-design-and-secure Standard-Workloads	elasticsearch-encrypted-at-rest	Da sensible Daten vorhanden sein können und um Daten im Ruhezustand zu schützen, sollten Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon OpenSearch Service (OpenSearch Service) -Domains aktiviert ist.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 b-design-and-secure — Cloud-6-Standard-Workloads	elasticsearch-node-to-node-Verschlüsselungsprüfung	Stellen Sie sicher, dass die node-to-node Verschlüsselung für Amazon OpenSearch Service aktiviert ist. Node-to-nodeVerschlüsselung ermöglicht die TLS 1.2-Versc hlüsselung für die gesamte Kommunikation innerhalb der Amazon Virtual Private Cloud (Amazon VPC). Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.
Abschnitt 4 b-design-and-secure — Cloud-6-Standard-Workloads	elv 2- acm-certificate-required	Zum Schutz von eventuell vorhandenen sensiblen Daten sowie von Daten während der Übertragung muss die Verschlüsselung für Ihr Elastic Load Balancing aktiviert sein. Verwenden Sie AWS Certifica te Manager, um öffentlic he und private SSL/TLS-Z ertifikate mit AWS Diensten und internen Ressourcen zu verwalten, bereitzustellen und bereitzustellen.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 — Cloud-6-S tandard-Workloads b-design-and-secure	elb-acm-certificate-required	Zum Schutz von eventuell vorhandenen sensiblen Daten sowie von Daten während der Übertragung muss die Verschlüsselung für Ihr Elastic Load Balancing aktiviert sein. Verwenden Sie AWS Certifica te Manager, um öffentlic he und private SSL/TLS-Z ertifikate mit AWS Diensten und internen Ressourcen zu verwalten, bereitzustellen und bereitzustellen.
Abschnitt 4 — Cloud-6-S tandard-Workloads b-design-and-secure	elb-tls-https-listeners-nur	Stellen Sie sicher, dass Ihre Elastic Load Balancer (ELBs) mit SSL- oder HTTPS-Lis tenern konfiguriert sind. Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.
Abschnitt 4 — Die Cloud — 6-Standard-Workloads b-design-and-secure	encrypted-volumes	Aktivieren Sie die Verschlüs selung für Ihre Amazon-El astic-Block-Store (Amazon-EBS)-Volumes, um eventuell vorhandene sensible Daten sowie Daten im Ruhezustand zu schützen.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 — Die Cloud — 6 b-design-and-secure Standard-Workloads	opensearch-encrypted-at-rest	Da sensible Daten vorhanden sein können und um Daten im Ruhezustand zu schützen, sollten Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon OpenSearch Service-Domains aktiviert ist.
Abschnitt 4 b-design-and-secure — Die Cloud — 6-Standard-Workloads	rds-snapshot-encrypted	Stellen Sie sicher, dass die Verschlüsselung für Ihre Amazon Relational Database Service (Amazon RDS)-Snapshots aktiviert ist. Da sensible Daten auch im Ruhezustand vorhanden sein können, sollten Sie die Verschlüsselung von Daten im Ruhezustand aktivieren, um diese Daten zu schützen.
Abschnitt 4 — Die Cloud — 6 b-design-and-secure Standard-Workloads	rds-storage-encrypted	Zum Schutz von Daten im Ruhezustand müssen Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon Relational Database Service (Amazon RDS)-Instances aktiviert ist. Um eventuell vorhandene sensible Daten im Ruhezustand in Amazon-RDS-Instanc es zu schützen, muss die Verschlüsselung von Daten im Ruhezustand aktiviert sein.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 — Die Cloud — 6 b-design-and-secure Standard-Workloads	redshift-cluster-configuration-check	Um Daten im Ruhezustand zu schützen, muss die Verschlüs selung für Ihre Amazon-Re dshift-Cluster aktiviert sein. Sie müssen auch sicherste llen, dass die erforderlichen Konfigurationen auf Amazon-Redshift-Clustern bereitgestellt werden. Die Prüfungsprotokolli erung muss aktiviert sein, um Informationen zu Verbindun gen und Benutzeraktivitäten in der Datenbank bereitzus tellen. Diese Regel erfordert , dass ein Wert für clusterDb Encrypted (Config Default: TRUE) und LoggingEnabled (Config Default: TRUE) gesetzt ist. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprech en.
b-design-and-secureAbschnitt 4 — Die Cloud-6-Standard-W orkloads	redshift-require-tls-ssl	Stellen Sie sicher, dass Ihre Amazon-Redshift-Cluster eine TLS/SSL-Verschlüsselung erfordern, um eine Verbindun g zu SQL-Clients herzustel len. Um eventuell vorhanden e sensible Daten zu schützen, sollten Sie die Verschlüs selung bei der Übertragung aktivieren.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 — Die Cloud — 6 b-design-and-secure Standard-Workloads	s3- aktiviert bucket-server-side -encryption	Zum Schutz von Daten im Ruhezustand müssen Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon Simple Storage Service (Amazon S3)-Bucke ts aktiviert ist. Um eventuell vorhandene sensible Daten im Ruhezustand in Amazon-S3 -Buckets zu schützen, muss die Verschlüsselung aktiviert sein.
Abschnitt 4 b-design-and-secure — Die Cloud — 6-Standard-Workloads	s3- bucket-ssl-requests-only	Um Daten während der Übertragung zu schützen, stellen Sie sicher, dass Ihre Amazon Simple Storage Service (Amazon S3)-Buckets Anfragen zur Verwendung von Secure Socket Layer (SSL)-Buckets erfordern. Da sensible Daten vorhanden sein können, sollten Sie die Verschlüs selung bei der Übertragung aktivieren, um diese Daten zu schützen.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 b-design-and-secure — Die Cloud — 6 — Standard-Workloads	s3- default-encryption-kms	Stellen Sie sicher, dass die Verschlüsselung für Ihre Amazon Simple Storage Service (Amazon S3)-Buckets aktiviert ist. Um eventuell vorhandene sensible Daten im Ruhezustand in einem Amazon-S3-Bucket zu schützen, muss die Verschlüsselung aktiviert sein.
Abschnitt 4 b-design-and-secure — Die Cloud — 6 — Standard-Workloads	sagemaker-endpoint-configuration-kms-schlüsselkonfiguriert	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass die Verschlüsselung mit dem AWS Key Management Service (AWS KMS) für Ihren Endpunkt aktiviert ist. SageMaker Da sensible Daten auf dem SageMaker Endgerät gespeichert werden können, sollten Sie die Verschlüsselung im Ruhezustand aktivieren, um diese Daten zu schützen.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 b-design-and-secure — Die Cloud — 6 Standard-Workloads	sagemaker-notebook-instance-kms-schlüsselkonfiguriert	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass die Verschlüsselung mit dem AWS Key Management Service (AWS KMS) für Ihr Notebook aktiviert ist. SageMaker Da vertrauliche Daten im SageMaker Notebook gespeichert werden können, sollten Sie die Verschlüsselung im Ruhezustand aktivieren, um diese Daten zu schützen.
Abschnitt 4 b-design-and-secure — Die Cloud — 6 Standard-Workloads	sns-encrypted-kms	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass Ihre Amazon Simple Notification Service (Amazon SNS) -Themen mit dem AWS Key Management Service (AWS KMS) verschlüsselt werden müssen. Um eventuell vorhandene sensible Daten im Ruhezustand in veröffentlichten Nachrichten zu schützen, muss die Verschlüsselung von Daten im Ruhezustand aktiviert sein.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 b-design-and-secure — Die Cloud — 6 Standard-Workloads	api-gw-ssl-enabled	Stellen Sie sicher, dass die REST-API-Stufen von Amazon API Gateway mit SSL-Zertifikaten konfiguriert sind, damit Backend-Systeme überprüfen können, ob Anforderungen von API Gateway stammen.
Abschnitt 4 — Die Cloud — 6 b-design-and-secure Standard-Workloads	redshift-cluster-kms-enabled	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass die Verschlüsselung mit AWS Key Management Service (AWS KMS) für Ihren Amazon Redshift Redshift-Cluster aktiviert ist. Um eventuell vorhandene sensible Daten im Ruhezustand in Redshift-Clustern zu schützen, muss die Verschlüsselung von Daten im Ruhezustand aktiviert sein.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 b-design-and-secure — Die Cloud — 8 materielle Workloads	iam-root-access-key-überprüfen	Der Zugriff auf Systeme und Ressourcen kann gesteuert werden, indem überprüft wird, ob der Root-Benutzer keine Zugriffsschlüssel mit seiner AWS Identity and Access Management (IAM) -Rolle verknüpft hat. Stellen Sie sicher, dass die Root-Zugriffsschlüssel gelöscht werden. Erstellen und verwenden Sie stattdessen rollenbasierte Funktionen, AWS-Konten um das Prinzip der geringsten Funktionalität zu berücksichtigen.
Abschnitt 4 — Die Cloud — 8 materielle Workloads b-design-and-secure	iam-user-mfa-enabled	Aktivieren Sie diese Regel, um den Zugriff auf Ressourcen in der AWS -Cloud einzuschränken. Diese Regel stellt sicher, dass die Multi-Faktor-Authentifizierung (MFA) für alle Benutzer aktiviert ist. MFA bietet eine weitere Schutzebene zusätzlich zum Benutzernamen und Passwort. Reduzieren Sie Fälle von kompromittierten Konten, indem Sie MFA für Benutzer vorschreiben.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 — Die Cloud b-design-and-secure — 8 materielle Workloads	mfa-enabled-for-iam-Konsolenzugriff	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass MFA für alle AWS Identity and Access Management (IAM) -Benutzer aktiviert ist, die über ein Konsolenkennwort verfügen. MFA sorgt für eine weitere Schutzebene zusätzlich zu den Anmeldeinformationen. Indem Sie MFA für Benutzer vorschreiben, können Sie Fälle kompromittierter Konten reduzieren und verhindern, dass unbefugte Benutzer auf vertrauliche Daten zugreifen.
Abschnitt 4 — Die Cloud — 8 materielle Workloads b-design-and-secure	root-account-hardware-mfa-aktiviert	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Hardware-MFA für den Root-Benutzer aktiviert ist. Der Stammbenutzer ist der AWS-Konto-Benutzer mit den meisten Berechtigungen. MFA sorgt für eine weitere Schutzebene zusätzlich zu den Anmeldeinformationen. Indem Sie MFA für den Root-Benutzer vorschreiben, können Sie die Anzahl AWS-Konten kompromittierter Benutzer reduzieren.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 — Die Cloud — 8 materielle Workloads b-design-and-secure	root-account-mfa-enabled	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass MFA für den Root-Benutzer aktiviert ist. Der Stammbenutzer ist der AWS-Konto-Benutzer mit den meisten Berechtigungen. MFA bietet eine weitere Schutzebene zusätzlich zum Benutzernamen und Passwort. Indem Sie MFA für den Root-Benutzer vorschreiben, können Sie die Anzahl AWS-Konten kompromittierter Benutzer reduzieren.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 — Die Cloud — 8 Standard-Workloads b-design-and-secure	access-keys-rotated	Die Anmeldeinformationen für autorisierte Geräte, Benutzer und Prozesse werden geprüft, indem sichergestellt wird, dass die IAM-Zugriffsschlüssel entsprechend den Vorgaben der Unternehmensrichtlinie rotiert werden. Das regelmäßi ge Ändern der Zugriffss chlüssel ist eine bewährte Sicherheitsmethode. Es verkürzt den Zeitraum, in dem ein Zugriffsschlüssel aktiv ist, und reduziert die Auswirkun gen auf das Unternehmen, wenn die Schlüssel kompromit tiert werden. Diese Regel erfordert einen Wert für die Zugriffsschlüssel-Rotation (Standardkonfiguration: 90). Der tatsächliche Wert muss den Richtlinien Ihrer Organisat ion entsprechen.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 — Die Cloud-8-Standard-Workloads b-design-and-secure	account-part-of-organizations	Durch die zentrale Verwaltung AWS-Konten innerhalb von AWS Organizations wird sichergestellt, dass die Konten den Vorschriften entsprechen. Eine fehlende zentrale Kontoverwaltung kann zu inkonsistenten Kontokonfigurationen führen, wodurch Ressourcen und sensible Daten offengelegt werden können.
Abschnitt 4 b-design-and-secure — Die Cloud — 8 Standard-Workloads	cloudtrail-security-trail-enabled	Diese Regel trägt dazu bei, die Verwendung der AWS empfohlenen bewährten Sicherheitsmethoden für sicherzustellen, indem geprüft wird AWS CloudTrail, ob mehrere Einstellungen aktiviert sind. Dazu gehören die Verwendung von Protokollverschlüsselung, Protokollvalidierung und Aktivierung AWS CloudTrail in mehreren Regionen.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 b-design-and-secure — Die Cloud — 8 Standard-Workloads	emr-kerberos-enabled	Die Zugriffsberechtigungen und -autorisierungen können verwaltet und nach den Prinzipien der geringsten Berechtigung und Aufgabent rennung integriert werden, indem Kerberos für Amazon-EMR-Cluster aktiviert wird. In Kerberos werden Services und Benutzer, die sich authentifizieren müssen, als Prinzipale bezeichnet. Prinzipale befinden sich in einem Kerberos-Bereich. Innerhalb dieses Bereichs wird ein Kerberos-Server als Key Distribution Center (KDC) bezeichnet. Über diesen Server können sich Prinzipale authentifizieren. Die Authentifizierung im KDC erfolgt durch die Ausstellu ng von Authentifizierungs tickets. Das KDC unterhält eine Datenbank der Prinzipal e in seinem Bereich mit ihren Passwörtern und anderen administrativen Informationen zu jedem Prinzipal.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 — Die Cloud mit 8 b-design-and-secure Standard-Workloads	iam-customer-policy-blocked-kms-Aktionen	AWS Identity and Access Management (IAM) kann Ihnen dabei helfen, die Prinzipien der geringsten Rechte und der Aufgabent rennung in Zugriffsberechtigu ngen und Autorisierungen zu integrieren und so zu verhindern, dass Richtlini en blockierte Aktionen für alle AWS Schlüssel des Key Management Service enthalten. Wenn Benutzer mehr Rechte haben, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtig ung und Aufgabentrennung verstoßen. Mit dieser Regel können Sie den Parameter festlegen. blockedActionsPatt erns (Wert „AWS Bewährte grundlegende Sicherhei tsmethoden“: kms: Decrypt, kms:ReEncryptFrom). Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisat ion entsprechen.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 — Die Cloud — 8 Standard-Workloads b-design-and-secure	iam-group-has-users-überprüfen	AWS Identity and Access Management (IAM) kann Ihnen helfen, die Prinzipien der geringsten Rechte und der Aufgabentrennung mit Zugriffsberechtigungen und Autorisierungen zu integrieren, indem sichergestellt wird, dass IAM-Gruppen mindestens einen Benutzer haben. Die Einteilung von Benutzern in Gruppen auf der Grundlage der ihnen zugewiesenen Berechtigungen oder ihrer Funktion ist eine Möglichkeit, das Prinzip der geringsten Berechtigung zu implementieren.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 — Die Cloud-8-Standard-Workloads b-design-and-secure	iam-inline-policy-blocked-kms-Aktionen	Stellen Sie sicher, dass ein Benutzer, eine IAM-Rolle oder eine IAM-Gruppe (AWS Identity and Access Management) nicht über eine Inline-Richtlinie verfügt, die blockierte Aktionen für alle AWS Schlüssel des Key Management Service zulässt. AWS empfiehlt, verwaltete Richtlinien anstelle von Inline-Richtlinien zu verwenden . Verwaltete Richtlinien ermöglichen Wiederverwendbarkeit, Versionsverwaltung, Rollback und Delegierung der Berechtigungsverwaltung. Mit dieser Regel können Sie den blockedActionsPatterns Parameter festlegen. (Wert „AWS Bewährte grundlegende Sicherheitsmethoden“: kms: Decrypt, kms:ReEncryptFrom). Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 — Die Cloud — 8 Standard-Workloads b-design-and-secure	iam-no-inline-policy-überprüfen	Stellen Sie sicher, dass ein Benutzer, eine IAM-Rolle oder eine IAM-Gruppe (AWS Identity and Access Management) nicht über eine Inline-Richtlinie zur Zugriffskontrolle auf Systeme und Ressourcen verfügt. AWS empfiehlt, verwaltete Richtlinien anstelle von Inline-Richtlinien zu verwenden . Verwaltete Richtlinien ermöglichen Wiederverwendbarkeit, Versionsverwaltung, Rollback und Delegierung der Berechtigungsverwaltung.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 b-design-and-secure — Die Cloud — 8 Standard-Workloads	iam-password-policy	Die Identitäten und Anmeldein formationen werden auf der Grundlage einer organisat orischen IAM-Passwortrichtl inie ausgestellt, verwaltet und verifiziert. Sie erfüllen oder übertreffen die Anforderu ngen von NIST SP 800-63 und dem Standard „Best Practices“ von Foundational Security für die Passworts tärke. AWS Mit dieser Regel können Sie optional RequireUppercaseCharacters (Wert für AWS grundlege nde Sicherheitsbewährte Methoden: wahr), RequireLo wercaseCharacters (Wert für bewährte Methoden für AWS grundlegende Sicherheit: wahr), RequireSymbols (Wert für bewährte Methoden für AWS grundlegende Sicherhei t: wahr), RequireNumbers (Wert für bewährte Methoden für AWS grundlegende Sicherheit: wahr), MinimumPa sswordLength (Wert für bewährte Methoden für AWS grundlegende Sicherheit: 14), PasswordReusePreve ntion (Wert für bewährte Methoden für AWS grundlege nde Sicherheit: 24) und

Kontroll-ID	AWS Config	Empfehlungen
		MaxPasswordAge (Wert für bewährte Methoden für AWS grundlegende Sicherheit: 90) für Ihr IAM festlegen Kennwortrichtlinie. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.
Abschnitt 4 b-design-and-secure — Die Cloud — 8-Standard-Workloads	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) kann Ihnen dabei helfen, die Prinzipien der geringsten Rechte und der Aufgabentrennung in Zugriffsberechtigungen und Autorisierungen zu integrieren und so zu verhindern, dass Richtlinien „Effect“: „Allow“ mit „Action“: „*“ anstelle von „Resource“: „*“ enthalten. Wenn Benutzern mehr Rechte eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und der Aufgabentrennung verstoßen.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt b-design-and-secure 4 — Die Cloud-8-Standard-Workloads	iam-policy-no-statements-with-full-access	Stellen Sie sicher, dass IAM-Aktionen nur auf die benötigten Aktionen beschränkt sind. Wenn Benutzern mehr Rechte eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und der Aufgabentrennung verstoßen.
Abschnitt 4 — Die Cloud mit 8 b-design-and-secure Standard-Workloads	iam-root-access-key-überprüfen	Der Zugriff auf Systeme und Ressourcen kann gesteuert werden, indem überprüft wird, ob der Root-Benutzer keine Zugriffsschlüssel mit seiner AWS Identity and Access Management (IAM) -Rolle verknüpft hat. Stellen Sie sicher, dass die Root-Zugriffsschlüssel gelöscht werden. Erstellen und verwenden Sie stattdessen rollenbasierte Funktionen, AWS-Konten um das Prinzip der geringsten Funktionalität zu berücksichtigen.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 — Die Cloud — 8 Standard-Workloads b-design-and-secure	iam-user-group-membership-überprüfen	AWS Identity and Access Management (IAM) kann Ihnen helfen, Zugriffsberechtigungen und Autorisierungen einzuschränken, indem sichergestellt wird, dass Benutzer Mitglieder mindestens einer Gruppe sind. Wenn Benutzern mehr Berechtigungen eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und Aufgabentrennung verstoßen.
Abschnitt 4 — Die Cloud — 8 Standard-Workloads b-design-and-secure	iam-user-mfa-enabled	Aktivieren Sie diese Regel, um den Zugriff auf Ressourcen in der AWS -Cloud einzuschränken. Diese Regel stellt sicher, dass die Multi-Faktor-Authentifizierung (MFA) für alle Benutzer aktiviert ist. MFA bietet eine weitere Schutzebene zusätzlich zum Benutzernamen und Passwort. Reduzieren Sie Fälle von kompromittierten Konten, indem Sie MFA für Benutzer vorschreiben.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 — Die Cloud mit 8 b-design-and-secure Standard-Workloads	iam-user-no-policies-überprüfen	Diese Regel stellt sicher, dass AWS Identity and Access Management (IAM) -Richtlinien nur Gruppen oder Rollen zugewiesen werden, um den Zugriff auf Systeme und Ressourcen zu kontrollieren. Die Zuweisung von Berechtigungen auf Gruppen- oder Rollenebene trägt dazu bei, die Wahrscheinlichkeit zu verringern, dass eine Identität übermäßige Berechtigungen erhält oder beibehält.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 b-design-and-secure — Cloud-8-Standard-Workloads	iam-user-unused-credentials-überprüfen	AWS Identity and Access Management (IAM) kann Ihnen bei Zugriffsberechtigungen und Autorisierungen helfen, indem es nach IAM-Passwörtern und Zugriffsschlüsseln sucht, die für einen bestimmten Zeitraum nicht verwendet wurden. Wenn ungenutzte Anmeldeinformationen identifiziert werden, müssen Sie sie deaktivieren und/oder entfernen, da dies gegen das Prinzip der geringsten Berechtigung verstoßen könnte. Für diese Regel müssen Sie einen Wert für das maxCredentialUsage Alter festlegen (Standardkonfiguration: 90). Der tatsächliche Wert muss den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 b-design-and-secure — Die Cloud — 8-Standard-Workloads	mfa-enabled-for-iam-Konsolenzugriff	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass MFA für alle AWS Identity and Access Management (IAM) -Benutzer aktiviert ist, die über ein Konsolenkennwort verfügen. MFA sorgt für eine weitere Schutzebene zusätzlich zu den Anmeldeinformationen. Indem Sie MFA für Benutzer vorschreiben, können Sie Fälle kompromittierter Konten reduzieren und verhindern, dass unbefugte Benutzer auf vertrauliche Daten zugreifen.
Abschnitt 4 — Die Cloud — 8 Standard-Workloads b-design-and-secure	root-account-hardware-mfa-aktiviert	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Hardware-MFA für den Root-Benutzer aktiviert ist. Der Stammbenutzer ist der AWS-Konto-Benutzer mit den meisten Berechtigungen. MFA sorgt für eine weitere Schutzebene zusätzlich zu den Anmeldeinformationen. Indem Sie MFA für den Root-Benutzer vorschreiben, können Sie die Anzahl AWS-Konten kompromittierter Benutzer reduzieren.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 — Die Cloud — 8 Standard-Workloads b-design-and-secure	root-account-mfa-enabled	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass MFA für den Root-Benutzer aktiviert ist. Der Stammbenutzer ist der AWS-Konto-Benutzer mit den meisten Berechtigungen. MFA bietet eine weitere Schutzebene zusätzlich zum Benutzernamen und Passwort. Indem Sie MFA für den Root-Benutzer vorschreiben, können Sie die Anzahl AWS-Konten kompromittierter Benutzer reduzieren.
Abschnitt 4 — Die Cloud — 9 materielle Workloads b-design-and-secure	cloudtrail-security-trail-enabled	Diese Regel trägt dazu bei, die Verwendung der AWS empfohlenen bewährten Sicherheitsmethoden für sicherzustellen, indem geprüft wird AWS CloudTrail, ob mehrere Einstellungen aktiviert sind. Dazu gehören die Verwendung von Protokoll verschlüsselung, Protokoll validierung und Aktivierung AWS CloudTrail in mehreren Regionen.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 b-design-and-secure — Die Cloud — 9 materielle Workloads	guardduty-enabled-centralized	Amazon GuardDuty kann mithilfe von Threat Intelligence Feeds helfen, potenzielle Cybersicherheitsereignisse zu überwachen und zu erkennen. Dazu gehören Listen mit bösartigen IPs und maschinellen Lernmethoden zur Identifizierung unerwarteter, nicht autorisierter und bösartiger Aktivitäten in Ihrer AWS Cloud-Umgebung.
Abschnitt 4 b-design-and-secure — Die Cloud — 9 — materielle Workloads	iam-root-access-key-überprüfen	Der Zugriff auf Systeme und Ressourcen kann gesteuert werden, indem überprüft wird, ob der Root-Benutzer keine Zugriffsschlüssel mit seiner AWS Identity and Access Management (IAM) -Rolle verknüpft hat. Stellen Sie sicher, dass die Root-Zugriffsschlüssel gelöscht werden. Erstellen und verwenden Sie stattdessen rollenbasierte Funktionen, AWS-Konten um das Prinzip der geringsten Funktionalität zu berücksichtigen.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 — Die Cloud — 9 materielle Workloads b-design-and-secure	iam-user-mfa-enabled	Aktivieren Sie diese Regel, um den Zugriff auf Ressourcen in der AWS -Cloud einzuschränken. Diese Regel stellt sicher, dass die Multi-Faktor-Authentifizierung (MFA) für alle Benutzer aktiviert ist. MFA bietet eine weitere Schutzebene zusätzlich zum Benutzernamen und Passwort. Reduzieren Sie Fälle von kompromittierten Konten, indem Sie MFA für Benutzer vorschreiben.
Abschnitt 4 — Die Cloud b-design-and-secure — 9 — materielle Workloads	mfa-enabled-for-iam-Konsolenzugriff	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass MFA für alle AWS Identity and Access Management (IAM) -Benutzer aktiviert ist, die über ein Konsolenkennwort verfügen. MFA sorgt für eine weitere Schutzebene zusätzlich zu den Anmeldeinformationen. Indem Sie MFA für Benutzer vorschreiben, können Sie Fälle kompromittierter Konten reduzieren und verhindern, dass unbefugte Benutzer auf vertrauliche Daten zugreifen.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 — Die Cloud — 9 — materielle Workloads b-design-and-secure	root-account-hardware-mfa-aktiviert	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Hardware-MFA für den Root-Benutzer aktiviert ist. Der Stammbenutzer ist der AWS-Konto-Benutzer mit den meisten Berechtigungen. MFA sorgt für eine weitere Schutzebene zusätzlich zu den Anmeldeinformationen. Indem Sie MFA für den Root-Benutzer vorschreiben, können Sie die Anzahl AWS-Konten kompromittierter Benutzer reduzieren.
Abschnitt 4 — Die Cloud — 9 materielle Workloads b-design-and-secure	root-account-mfa-enabled	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass MFA für den Root-Benutzer aktiviert ist. Der Stammbenutzer ist der AWS-Konto-Benutzer mit den meisten Berechtigungen. MFA bietet eine weitere Schutzebene zusätzlich zum Benutzernamen und Passwort. Indem Sie MFA für den Root-Benutzer vorschreiben, können Sie die Anzahl AWS-Konten kompromittierter Benutzer reduzieren.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 — Cloud-9-S tandard-Workloads b-design-and-secure	cloudtrail-enabled	AWS CloudTrail kann durch die Aufzeichnung von Aktionen und API-Aufrufen in der Management Console bei der Nichtabstreitbarkeit helfen. AWS Sie können die Benutzer und die Benutzer AWS-Konten , die einen AWS Dienst aufgerufen haben, die Quell-IP-Adresse, über die die Aufrufe generiert wurden, und den Zeitpunkt der Anrufe identifizieren. Einzelheiten zu den erfassten Daten finden Sie in den AWS CloudTrail Datensatzinhalten.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 b-design-and-secure — Cloud-9-Standard-Workloads	iam-group-has-users-überprüfen	AWS Identity and Access Management (IAM) kann Ihnen helfen, die Prinzipien der geringsten Rechte und der Aufgabentrennung mit Zugriffsberechtigungen und Autorisierungen zu integrieren, indem sichergestellt wird, dass IAM-Gruppen mindestens einen Benutzer haben. Die Einteilung von Benutzern in Gruppen auf der Grundlage der ihnen zugewiesenen Berechtigungen oder ihrer Funktion ist eine Möglichkeit, das Prinzip der geringsten Berechtigung zu implementieren.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 — Cloud-9-Standard-Workloads b-design-and-secure	iam-no-inline-policy-überprüfen	Stellen Sie sicher, dass ein Benutzer, eine IAM-Rolle oder eine IAM-Gruppe (AWS Identity and Access Management) nicht über eine Inline-Richtlinie zur Zugriffskontrolle auf Systeme und Ressourcen verfügt. AWS empfiehlt, verwaltete Richtlinien anstelle von Inline-Richtlinien zu verwenden . Verwaltete Richtlinien ermöglichen Wiederverwendbarkeit, Versionsverwaltung, Rollback und Delegierung der Berechtigungsverwaltung.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 b-design-and-secure — Die Cloud — 9-Standard-Workloads	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) kann Ihnen dabei helfen, die Prinzipien der geringsten Rechte und der Aufgabent rennung in Zugriffsberechtigu ngen und Autorisierungen zu integrieren und so zu verhindern, dass Richtlinien „Effect“: „Allow“ mit „Action“: „*“ anstelle von „Resource“: „*“ enthalten. Wenn Benutzern mehr Rechte eingeräumt werden, als für die Ausführun g einer Aufgabe erforderl ich sind, kann dies gegen das Prinzip der geringste n Berechtigung und der Aufgabentrennung verstoßen.
Abschnitt b-design-and-secure 4 — Die Cloud-9-Standard-W orkloads	iam-policy-no-statements-with-full-access	Stellen Sie sicher, dass IAM-Aktionen nur auf die benötigte n Aktionen beschränkt sind. Wenn Benutzern mehr Rechte eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und der Aufgabentrennung verstoßen.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 — Die b-design-and-secure Cloud-9-Standard-Workloads	iam-root-access-key-überprüfen	Der Zugriff auf Systeme und Ressourcen kann gesteuert werden, indem überprüft wird, ob der Root-Benutzer keine Zugriffsschlüssel mit seiner AWS Identity and Access Management (IAM) -Rolle verknüpft hat. Stellen Sie sicher, dass die Root-Zugriffsschlüssel gelöscht werden. Erstellen und verwenden Sie stattdessen rollenbasierte Funktionen, AWS-Konten um das Prinzip der geringsten Funktionalität zu berücksichtigen.
Abschnitt 4 — Cloud-9-Standard-Workloads b-design-and-secure	iam-user-group-membership-überprüfen	AWS Identity and Access Management (IAM) kann Ihnen helfen, Zugriffsberechtigungen und Autorisierungen einzuschränken, indem sichergestellt wird, dass Benutzer Mitglieder mindestens einer Gruppe sind. Wenn Benutzern mehr Berechtigungen eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und Aufgabentrennung verstoßen.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 — Die Cloud-9-Standard-Workloads b-design-and-secure	iam-user-mfa-enabled	Aktivieren Sie diese Regel, um den Zugriff auf Ressourcen in der AWS -Cloud einzuschränken. Diese Regel stellt sicher, dass die Multi-Faktor-Authentifizierung (MFA) für alle Benutzer aktiviert ist. MFA bietet eine weitere Schutzebene zusätzlich zum Benutzernamen und Passwort. Reduzieren Sie Fälle von kompromittierten Konten, indem Sie MFA für Benutzer vorschreiben.
Abschnitt 4 — Die b-design-and-secure Cloud-9-Standard-Workloads	iam-user-no-policies-überprüfen	Diese Regel stellt sicher, dass AWS Identity and Access Management (IAM) -Richtlinien nur Gruppen oder Rollen zugewiesen werden, um den Zugriff auf Systeme und Ressourcen zu kontrollieren. Die Zuweisung von Berechtigungen auf Gruppen- oder Rollenebene trägt dazu bei, die Wahrscheinlichkeit zu verringern, dass eine Identität übermäßige Berechtigungen erhält oder beibehält.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 b-design-and-secure — Cloud-9-Standard-Workloads	iam-user-unused-credentials-überprüfen	AWS Identity and Access Management (IAM) kann Ihnen bei Zugriffsberechtigungen und Autorisierungen helfen, indem es nach IAM-Passwörtern und Zugriffsschlüsseln sucht, die für einen bestimmten Zeitraum nicht verwendet wurden. Wenn ungenutzte Anmeldeinformationen identifiziert werden, müssen Sie sie deaktivieren und/oder entfernen, da dies gegen das Prinzip der geringsten Berechtigung verstoßen könnte. Für diese Regel müssen Sie einen Wert für das maxCredentialUsage Alter festlegen (Standardkonfiguration: 90). Der tatsächliche Wert muss den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 b-design-and-secure — Die Cloud-9-Standard-Workloads	mfa-enabled-for-iam-Konsolenzugriff	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass MFA für alle AWS Identity and Access Management (IAM) -Benutzer aktiviert ist, die über ein Konsolenkennwort verfügen. MFA sorgt für eine weitere Schutzebene zusätzlich zu den Anmeldeinformationen. Indem Sie MFA für Benutzer vorschreiben, können Sie Fälle kompromittierter Konten reduzieren und verhindern, dass unbefugte Benutzer auf vertrauliche Daten zugreifen.
Abschnitt 4 — Die Cloud-9-Standard-Workloads b-design-and-secure	root-account-hardware-mfa-aktiviert	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Hardware-MFA für den Root-Benutzer aktiviert ist. Der Stammbenutzer ist der AWS-Konto-Benutzer mit den meisten Berechtigungen. MFA sorgt für eine weitere Schutzebene zusätzlich zu den Anmeldeinformationen. Indem Sie MFA für den Root-Benutzer vorschreiben, können Sie die Anzahl AWS-Konten kompromittierter Benutzer reduzieren.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 — Cloud-9-S tandard-Workloads b-design-and-secure	root-account-mfa-enabled	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherste llen, dass MFA für den Root-Benutzer aktiviert ist. Der Stammbenutzer ist der AWS-Konto-Benutzer mit den meisten Berechtigungen. MFA bietet eine weitere Schutzebe ne zusätzlich zum Benutzern amen und Passwort. Indem Sie MFA für den Root-Benu tzer vorschreiben, können Sie die Anzahl AWS-Konte n kompromittierter Benutzer reduzieren.
Abschnitt 4 — Cloud-9-S tandard-Workloads b-design-and-secure	securityhub-enabled	AWS Security Hub hilft bei der Überwachung von unbefugte m Personal, Verbindungen, Geräten und Software. AWS Security Hub aggregiert, organisiert und priorisiert die Sicherheitswarnungen oder Ergebnisse mehrerer Dienste. AWS Einige dieser Dienste sind Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer und AWS Firewall Manager sowie AWS Partnerlösungen.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 — Die Cloud — 10 materielle Workloads b-design-and-secure	autoscaling-launch-config-public-ip-deaktiviert	Wenn Sie Ihre Netzwerkschnittstellen mit einer öffentlichen IP-Adresse konfigurieren, sind die diesen Netzwerkschnittstellen zugehörigen Ressourcen über das Internet erreichbar. EC2 Ressourcen sollten nicht öffentlich zugänglich sein, da dies einen unbeabsichtigten Zugriff auf Ihre Anwendungen oder Server ermöglichen kann.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 b-design-and-secure — Die Cloud — 10 materielle Workloads	cloudwatch-alarm-action-check	Amazon CloudWatch alarmiert, wenn eine Metrik den Schwellenwert für eine bestimmte Anzahl von Bewertungszeiträumen überschreitet. Der Alarm führt eine oder mehrere Aktionen durch, die vom Wert der Metrik oder des Ausdrucks im Vergleich zu einem Schwellenwert in einer Reihe von Zeiträumen abhängt. Diese Regel erfordert einen Wert für alarmActionRequired (Config Default: True), insufficientDataActionRequired (Config Default: True), okActionRequired (Config Default: False). Der tatsächliche Wert muss die Alarmaktionen für Ihre Umgebung widerspiegeln.
Abschnitt 4 b-design-and-secure — Die Cloud-10-Material-Workloads	dms-replication-not-public	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass auf DMS-Replikationsinstanzen nicht öffentlich zugegriffen werden kann. DMS-Replikations-Instances können vertrauliche Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 b-design-and-secure — Die Cloud — 10 materielle Workloads	ec2-manager instance-managed-by-systems	Eine Bestandsaufnahme der Softwareplattformen und Anwendungen innerhalb des Unternehmens ist möglich, indem Amazon Elastic Compute Cloud (Amazon EC2) -Instances mit AWS Systems Manager verwaltet werden. Verwenden Sie AWS Systems Manager, um detaillierte Systemkonfiguratio nen, Betriebssystem-Patch-Levels, Namen und Typ der Dienste, Softwareinstallati onen, Anwendungsname, Herausgeber und Version sowie andere Details zu Ihrer Umgebung bereitzustellen.
Abschnitt 4 b-design-and-secure — Die Cloud — 10 materielle Workloads	ec2- instance-no-public-ip	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon Elastic Compute Cloud (Amazon EC2) -Instances nicht öffentlich zugänglich sind. EC2Amazon-Instances können vertrauliche Informati onen enthalten, und für solche Konten ist eine Zugriffsk ontrolle erforderlich.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 b-design-and-secure — Die Cloud — 10 materielle Workloads	emr-master-no-public-ip	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon EMR-Cluster-Masterknoten nicht öffentlich zugänglich sind. Amazon-EMR-Cluster-Hauptknoten können vertrauliche Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.
Abschnitt 4 b-design-and-secure — Die Cloud — 10 materielle Workloads	guardduty-enabled-centralized	Amazon GuardDuty kann mithilfe von Threat Intelligence Feeds helfen, potenzielle Cybersicherheitsereignisse zu überwachen und zu erkennen. Dazu gehören Listen mit bösartigen IPs und maschinellen Lernmethoden zur Identifizierung unerwarteter, nicht autorisierter und bösartiger Aktivitäten in Ihrer AWS Cloud-Umgebung.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 b-design-and-secure — Die Cloud — 10 materielle Workloads	iam-password-policy	Die Identitäten und Anmeldein formationen werden auf der Grundlage einer organisat orischen IAM-Passwortrichtl inie ausgestellt, verwaltet und verifiziert. Sie erfüllen oder übertreffen die Anforderu ngen von NIST SP 800-63 und dem Standard „Best Practices“ von Foundational Security für die Passworts tärke. AWS Mit dieser Regel können Sie optional RequireUppercaseCharacters (Wert für AWS grundlege nde Sicherheitsbewährte Methoden: wahr), RequireLo wercaseCharacters (Wert für bewährte Methoden für AWS grundlegende Sicherheit: wahr), RequireSymbols (Wert für bewährte Methoden für AWS grundlegende Sicherhei t: wahr), RequireNumbers (Wert für bewährte Methoden für AWS grundlegende Sicherheit: wahr), MinimumPa sswordLength (Wert für bewährte Methoden für AWS grundlegende Sicherheit: 14), PasswordReusePreve ntion (Wert für bewährte Methoden für AWS grundlege nde Sicherheit: 24) und

Kontroll-ID	AWS Config	Empfehlungen
		MaxPasswordAge (Wert für bewährte Methoden für AWS grundlegende Sicherhei t: 90) für Ihr IAM festlegen Kennwortrichtlinie. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisat ion entsprechen.
Abschnitt 4 b-design-and-secure — Die Cloud — 10 materielle Workloads	iam-root-access-key-überprü fen	Der Zugriff auf Systeme und Ressourcen kann gesteuert werden, indem überprüft wird, ob der Root-Benutzer keine Zugriffsschlüssel mit seiner AWS Identity and Access Management (IAM) -Rolle verknüpft hat. Stellen Sie sicher, dass die Root-Zugr iffsschlüssel gelöscht werden. Erstellen und verwenden Sie stattdessen rollenbasierte Funktionen, AWS-Konten um das Prinzip der geringsten Funktionalität zu berücksic htigen.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 — Die Cloud — 10 materielle Workloads b-design-and-secure	iam-user-mfa-enabled	Aktivieren Sie diese Regel, um den Zugriff auf Ressourcen in der AWS -Cloud einzuschränken. Diese Regel stellt sicher, dass die Multi-Faktor-Authentifizierung (MFA) für alle Benutzer aktiviert ist. MFA bietet eine weitere Schutzebene zusätzlich zum Benutzernamen und Passwort. Reduzieren Sie Fälle von kompromittierten Konten, indem Sie MFA für Benutzer vorschreiben.
Abschnitt 4 — Die Cloud b-design-and-secure — 10 materielle Workloads	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) Security Groups können bei der Verwaltung des Netzwerkzugriffs helfen, indem sie eine statusbehaftete Filterung des ein- und ausgehenden Netzwerkverkehrs zu Ressourcen bereitstellen. AWS Wenn Sie eingehenden (oder entfernten) Datenverkehr von 0.0.0.0/0 bis Port 22 auf Ihren Ressourcen nicht zulassen, können Sie den Remote-Zugriff einschränken.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 — Die Cloud — 10 materielle Workloads b-design-and-secure	internet-gateway-authorized-vpc-nur	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Internet-Gateways nur mit autorisierter Amazon Virtual Private Cloud (Amazon VPC) verbunden sind. Internet-Gateways ermöglichen den bidirekti onalen Internetzugang zur und von der Amazon VPC, was möglicherweise zu einem unbefugten Zugriff auf Amazon-VPC-Ressourcen führen kann.
Abschnitt 4 — Die Cloud — 10 materielle Workloads b-design-and-secure	lambda-function-public-acce ss-verboten	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherste llen, dass AWS Lambda-Funktionen nicht öffentlich zugänglich sind. Der öffentlic he Zugriff kann möglicher weise die Verfügbarkeit von Ressourcen beeinträchtigen.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 b-design-and-secure — Die Cloud — 10 materielle Workloads	mfa-enabled-for-iam-Konsolenzugriff	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass MFA für alle AWS Identity and Access Management (IAM) -Benutzer aktiviert ist, die über ein Konsolenkennwort verfügen. MFA sorgt für eine weitere Schutzebene zusätzlich zu den Anmeldeinformationen. Indem Sie MFA für Benutzer vorschreiben, können Sie Fälle kompromittierter Konten reduzieren und verhindern, dass unbefugte Benutzer auf vertrauliche Daten zugreifen.
Abschnitt 4 — Die Cloud — 10 materielle Workloads b-design-and-secure	no-unrestricted-route-to-igw	Stellen Sie sicher, dass EC2 Amazon-Routentabellen keine uneingeschränkten Routen zu einem Internet-Gateway enthalten. Durch das Entfernen oder Beschränken des Internetzugangs für Workloads innerhalb von Amazon VPCs können unbeabsichtigte Zugriffe in Ihrer Umgebung reduziert werden.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 — Die Cloud — 10-Material-Workloads b-design-and-secure	opensearch-in-vpc-only	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass sich Amazon OpenSearch Service-Domains innerhalb einer Amazon Virtual Private Cloud (Amazon VPC) befinden. Eine Amazon OpenSearch Service-Domain innerhalb einer Amazon VPC ermöglich t die sichere Kommunika tion zwischen Amazon OpenSearch Service und anderen Services innerhalb der Amazon VPC, ohne dass ein Internet-Gateway, ein NAT-Gerät oder eine VPN-Verbindung erforderlich ist.
Abschnitt 4 — Die Cloud — 10 materielle Workloads b-design-and-secure	rds-instance-public-access-überprüfen	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherste llen, dass Amazon Relationa l Database Service (Amazon RDS) -Instances nicht öffentlic h sind. Amazon-RDS-Datenba nk-Instances können vertrauli che Informationen enthalten und für solche Konten sind Prinzipien und Zugriffsk ontrollen erforderlich.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 b-design-and-secure — Die Cloud — 10 materielle Workloads	redshift-cluster-public-access-überprüfen	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Redshift Redshift-Cluster nicht öffentlich sind. Amazon-Redshift-Cluster können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.
Abschnitt 4 b-design-and-secure — Die Cloud — 10 materielle Workloads	redshift-enhanced-vpc-routing-aktiviert	Mit Enhanced-VPC-Routing wird erzwungen, dass der gesamte COPY- und UNLOAD-Datenverkehr zwischen Ihrem Cluster und Datenrepositorys über Ihre Amazon VPC erfolgt. Anschließend können Sie VPC-Features wie Sicherheitsgruppen und Netzwerkzugriffskontrollisten verwenden, um den Netzwerkverkehr zu schützen. Sie können auch VPC-Flow-Protokolle verwenden, um den Netzwerkverkehr zu überwachen.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 b-design-and-secure — Die Cloud — 10 materielle Workloads	restricted-common-ports	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass gemeinsame Ports für Amazon Elastic Compute Cloud (Amazon EC2) - Sicherheitsgruppen eingeschränkt sind. Wenn der Zugriff auf Ports nicht auf vertrauenswürdige Quellen beschränkt wird, kann dies zu Angriffen auf die Verfügbarkeit, Integrität und Vertraulichkeit von Systemen führen. Mit dieser Regel können Sie optional die Parameter blockedPort1–blockedPort5 festlegen (Standardkonfigurationen: 20, 21, 3389, 3306, 4333). Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 b-design-and-secure — Die Cloud — 10 materielle Workloads	root-account-hardware-mfa-aktiviert	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Hardware-MFA für den Root-Benutzer aktiviert ist. Der Stammbenutzer ist der AWS-Konto-Benutzer mit den meisten Berechtigungen. MFA sorgt für eine weitere Schutzebene zusätzlich zu den Anmeldeinformationen. Indem Sie MFA für den Root-Benutzer vorschreiben, können Sie die Anzahl AWS-Konten kompromittierter Benutzer reduzieren.
Abschnitt 4 — Die Cloud — 10 materielle Workloads b-design-and-secure	root-account-mfa-enabled	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass MFA für den Root-Benutzer aktiviert ist. Der Stammbenutzer ist der AWS-Konto-Benutzer mit den meisten Berechtigungen. MFA bietet eine weitere Schutzebene zusätzlich zum Benutzernamen und Passwort. Indem Sie MFA für den Root-Benutzer vorschreiben, können Sie die Anzahl AWS-Konten kompromittierter Benutzer reduzieren.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 — Die Cloud — 10 materielle Workloads b-design-and-secure	s3- -Blöcke — periodisch account-level-public-access	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Simple Storage Service (Amazon S3) -Buckets nicht öffentlich zugänglich sind. Diese Regel trägt dazu bei, sensible Daten vor unbefugten Remote-Benutzern zu schützen, indem sie den öffentlichen Zugriff verhindert. Mit dieser Regel können Sie optional die Parameter ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) und restrictPublicBuckets Parameter (Config Default: True) festlegen. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 b-design-and-secure — Die Cloud — 10 materielle Workloads	sagemaker-notebook-no-direct-Internetzugang	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass SageMaker Amazon-Notebooks keinen direkten Internetzugang zulassen. Indem Sie direkten Internetzugang blockieren, vermeiden Sie, dass unbefugte Benutzer auf sensible Daten zugreifen.
Abschnitt 4 b-design-and-secure — Die Cloud — 10 materielle Workloads	ssm-document-not-public	Stellen Sie sicher, dass AWS Systems Manager (SSM) - Dokumente nicht öffentlich sind, da dies einen unbeabsichtigten Zugriff auf Ihre SSM-Dokumente ermöglichen kann. Ein öffentliches SSM-Dokument kann Informationen über Ihr Konto, Ihre Ressourcen und internen Prozesse preisgeben.

Kontroll-ID	AWS Config	Empfehlungen
b-design-and-secureAbschnitt 4 — Die Cloud — 10 materielle Workloads	vpc-default-security-group-geschlossen	Sicherheitsgruppen von Amazon Elastic Compute Cloud (Amazon EC2) können bei der Verwaltung des Netzwerkzugriffs helfen, indem sie eine statusbehaftete Filterung des ein- und ausgehenden Netzwerkverkehrs zu Ressourcen bereitstellen. AWS Die Beschränkung des gesamten Datenverkehrs auf die Standardsicherheitsgruppe hilft dabei, den Fernzugriff auf Ihre Ressourcen einzuschränken. AWS

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 — Die Cloud — 10 materielle Workloads b-design-and-secure	vpc-sg-open-only-to-authorized-ports	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass gemeinsame Ports für Amazon Elastic Compute Cloud (Amazon EC2) - Sicherheitsgruppen eingeschränkt sind. Wenn der Zugriff auf Ports nicht auf vertrauenswürdige Quellen beschränkt wird, kann dies zu Angriffen auf die Verfügbarkeit, Integrität und Vertraulichkeit von Systemen führen. Durch die Beschränkung des Zugriffs auf Ressourcen innerhalb einer Sicherheitsgruppe aus dem Internet (0.0.0.0/0) kann der Remote-Zugriff auf interne Systeme gesteuert werden.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 b-design-and-secure — Die Cloud — 10 materielle Workloads	vpc-vpn-2-tunnels-up	Redundante Site-to-Site VPN-Tunnel können implement iert werden, um die Anforderu ngen an die Ausfallsicherheit zu erfüllen. Es verwendet zwei Tunnel, um die Konnektiv ität sicherzustellen, falls eine der Site-to-Site VPN-Verbi ndungen nicht verfügbar ist. Um sich vor einem Verbindun gsverlust zu schützen, können Sie für den Fall, dass Ihr Kunden-Gateway nicht verfügbar ist, eine zweite Site-to-Site VPN-Verbindung zu Ihrer Amazon Virtual Private Cloud (Amazon VPC) und Ihrem Virtual Private Gateway einrichten, indem Sie ein zweites Kunden-Gateway verwenden.
Abschnitt 4 b-design-and-secure — Die Cloud — 10 materielle Workloads	s3- verboten bucket-level-publi c-access	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherste llen, dass Amazon Simple Storage Service (Amazon S3) -Buckets nicht öffentlich zugänglich sind. Diese Regel trägt dazu bei, sensible Daten vor unbefugten Remote-Be nutzern zu schützen, indem sie den öffentlichen Zugriff auf Bucket-Ebene verhindert.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 b-design-and-secure — Die Cloud — 10 materielle Workloads	subnet-auto-assign-public-ip-deaktiviert	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon Virtual Private Cloud (VPC) -Subnetzen nicht automatisch eine öffentliche IP-Adresse zugewiesen wird. Amazon Elastic Compute Cloud (EC2) -Instances, die in Subnetzen gestartet werden, in denen dieses Attribut aktiviert ist, haben ihrer primären Netzwerkschnittstelle eine öffentliche IP-Adresse zugewiesen.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 b-design-and-secure — Die Cloud-10-Standard-Workloads	access-keys-rotated	Die Anmeldeinformationen für autorisierte Geräte, Benutzer und Prozesse werden geprüft, indem sichergestellt wird, dass die IAM-Zugriffsschlüssel entsprechend den Vorgaben der Unternehmensrichtlinie rotiert werden. Das regelmäßige Ändern der Zugriffsschlüssel ist eine bewährte Sicherheitsmethode. Es verkürzt den Zeitraum, in dem ein Zugriffsschlüssel aktiv ist, und reduziert die Auswirkungen auf das Unternehmen, wenn die Schlüssel kompromittiert werden. Diese Regel erfordert einen Wert für die Zugriffsschlüssel-Rotation (Standardkonfiguration: 90). Der tatsächliche Wert muss den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 — Die Cloud-10-Standard-Workloads b-design-and-secure	autoscaling-launch-config-public-ip-deaktiviert	Wenn Sie Ihre Netzwerkschnittstellen mit einer öffentlichen IP-Adresse konfigurieren, sind die diesen Netzwerkschnittstellen zugehörigen Ressourcen über das Internet erreichbar. EC2 Ressourcen sollten nicht öffentlich zugänglich sein, da dies einen unbeabsichtigten Zugriff auf Ihre Anwendungen oder Server ermöglichen kann.
Abschnitt 4 b-design-and-secure — Die Cloud-10-Standard-Workloads	emr-master-no-public-ip	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon EMR-Cluster-Masterknoten nicht öffentlich zugänglich sind. Amazon-EMR-Cluster-Hauptknoten können vertrauliche Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 b-design-and-secure — Die Cloud-10-Standard-Workloads	iam-no-inline-policy-überprüfen	Stellen Sie sicher, dass ein Benutzer, eine IAM-Rolle oder eine IAM-Gruppe (AWS Identity and Access Management) nicht über eine Inline-Richtlinie zur Zugriffskontrolle auf Systeme und Ressourcen verfügt. AWS empfiehlt, verwaltete Richtlinien anstelle von Inline-Richtlinien zu verwenden . Verwaltete Richtlinien ermöglichen Wiederverwendbarkeit, Versionsverwaltung, Rollback und Delegierung der Berechtigungsverwaltung.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 b-design-and-secure — Die Cloud — 10-Standard-Workloads	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) kann Ihnen dabei helfen, die Prinzipien der geringsten Rechte und der Aufgabent rennung in Zugriffsberechtigu ngen und Autorisierungen zu integrieren und so zu verhindern, dass Richtlinien „Effect“: „Allow“ mit „Action“: „*“ anstelle von „Resource“: „*“ enthalten. Wenn Benutzern mehr Rechte eingeräumt werden, als für die Ausführun g einer Aufgabe erforderl ich sind, kann dies gegen das Prinzip der geringste n Berechtigung und der Aufgabentrennung verstoßen.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt b-design-and-secure 4 — Die Cloud-10-Standard-Workloads	iam-root-access-key-überprüfen	Der Zugriff auf Systeme und Ressourcen kann gesteuert werden, indem überprüft wird, ob der Root-Benutzer keine Zugriffsschlüssel mit seiner AWS Identity and Access Management (IAM) -Rolle verknüpft hat. Stellen Sie sicher, dass die Root-Zugriffsschlüssel gelöscht werden. Erstellen und verwenden Sie stattdessen rollenbasierte Funktionen, AWS-Konten um das Prinzip der geringsten Funktionalität zu berücksichtigen.
Abschnitt 4 — Die Cloud — 10-Standard-Workloads b-design-and-secure	iam-user-mfa-enabled	Aktivieren Sie diese Regel, um den Zugriff auf Ressourcen in der AWS -Cloud einzuschränken. Diese Regel stellt sicher, dass die Multi-Faktor-Authentifizierung (MFA) für alle Benutzer aktiviert ist. MFA bietet eine weitere Schutzebene zusätzlich zum Benutzernamen und Passwort. Reduzieren Sie Fälle von kompromittierten Konten, indem Sie MFA für Benutzer vorschreiben.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 — Die b-design-and-secure Cloud-10-Standard-Workloads	iam-user-no-policies-überprüfen	Diese Regel stellt sicher, dass AWS Identity and Access Management (IAM) -Richtlinien nur Gruppen oder Rollen zugewiesen werden, um den Zugriff auf Systeme und Ressourcen zu kontrollieren. Die Zuweisung von Berechtigungen auf Gruppen- oder Rollenebene trägt dazu bei, die Wahrscheinlichkeit zu verringern, dass eine Identität übermäßige Berechtigungen erhält oder beibehält.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 b-design-and-secure — Die Cloud-10-Standard-Workloads	iam-user-unused-credentials-überprüfen	AWS Identity and Access Management (IAM) kann Ihnen bei Zugriffsberechtigungen und Autorisierungen helfen, indem es nach IAM-Passwörtern und Zugriffsschlüsseln sucht, die für einen bestimmten Zeitraum nicht verwendet wurden. Wenn ungenutzte Anmeldeinformationen identifiziert werden, müssen Sie sie deaktivieren und/oder entfernen, da dies gegen das Prinzip der geringsten Berechtigung verstoßen könnte. Für diese Regel müssen Sie einen Wert für das maxCredentialUsage Alter festlegen (Standardkonfiguration: 90). Der tatsächliche Wert muss den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 b-design-and-secure — Die Cloud-10-Standard-Workloads	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) Security Groups können bei der Verwaltung des Netzwerkz ugriffs helfen, indem sie eine statusbehaftete Filterung des ein- und ausgehend en Netzwerkverkehrs zu Ressourcen bereitstellen. AWS Wenn Sie eingehenden (oder entfernten) Datenverk ehr von 0.0.0.0/0 bis Port 22 auf Ihren Ressourcen nicht zulassen, können Sie den Remote-Zugriff einschränken.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 — Die Cloud-10-Standard-Workloads b-design-and-secure	ec2- instances-in-vpc	Stellen Sie Amazon Elastic Compute Cloud (Amazon EC2) -Instances innerhalb einer Amazon Virtual Private Cloud (Amazon VPC) bereit, um eine sichere Kommunika tion zwischen einer Instance und anderen Services innerhalb der Amazon VPC zu ermöglichen, ohne dass ein Internet-Gateway, ein NAT-Gerät oder eine VPN-Verbi ndung erforderlich ist. Der gesamte Datenverkehr bleibt sicher in der AWS Cloud. Domains, die sich innerhalb einer VPC befinden, verfügen aufgrund ihrer logischen Isolierung im Vergleich zu Domains mit öffentlic hen Endpunkten über eine zusätzliche Sicherheitsebene. Weisen Sie EC2 Amazon-In stances einer Amazon-VPC zu, um den Zugriff ordnungsg emäß zu verwalten.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 b-design-and-secure — Die Cloud-10-Standard-Workloads	internet-gateway-authorized-vpc-nur	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Internet-Gateways nur mit autorisierter Amazon Virtual Private Cloud (Amazon VPC) verbunden sind. Internet-Gateways ermöglichen den bidirekti onalen Internetzugang zur und von der Amazon VPC, was möglicherweise zu einem unbefugten Zugriff auf Amazon-VPC-Ressourcen führen kann.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 — Die Cloud-10-Standard-Workloads b-design-and-secure	lambda-inside-vpc	Stellen Sie AWS Lambda-Funktionen in einer Amazon Virtual Private Cloud (Amazon VPC) bereit, um eine sichere Kommunikation zwischen einer Funktion und anderen Diensten innerhalb der Amazon VPC zu gewährleisten. Bei dieser Konfiguration sind kein Internet-Gateway, kein NAT-Gerät und keine VPN-Verbindung erforderlich. Der gesamte Datenverkehr bleibt sicher in der Cloud. AWS Domains, die sich innerhalb einer VPC befinden, verfügen aufgrund ihrer logischen Isolierung im Vergleich zu Domains mit öffentlichen Endpunkten über eine zusätzliche Sicherheitsebene. Um den Zugriff ordnungsgemäß zu verwalten, sollten AWS Lambda-Funktionen einer VPC zugewiesen werden.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 — Die Cloud-10-Standard-Workloads b-design-and-secure	mfa-enabled-for-iam-Konsolenzugriff	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass MFA für alle AWS Identity and Access Management (IAM) -Benutzer aktiviert ist, die über ein Konsolenkennwort verfügen. MFA sorgt für eine weitere Schutzebene zusätzlich zu den Anmeldeinformationen. Indem Sie MFA für Benutzer vorschreiben, können Sie Fälle kompromittierter Konten reduzieren und verhindern, dass unbefugte Benutzer auf vertrauliche Daten zugreifen.
Abschnitt 4 — Die Cloud-10-Standard-Workloads b-design-and-secure	no-unrestricted-route-to-igw	Stellen Sie sicher, dass EC2 Amazon-Routentabellen keine uneingeschränkten Routen zu einem Internet-Gateway enthalten. Durch das Entfernen oder Beschränken des Internetzugangs für Workloads innerhalb von Amazon VPCs können unbeabsichtigte Zugriffe in Ihrer Umgebung reduziert werden.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 — Die Cloud-10-Standard-Workloads b-design-and-secure	opensearch-in-vpc-only	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass sich Amazon OpenSearch Service-Domains innerhalb einer Amazon Virtual Private Cloud (Amazon VPC) befinden. Eine Amazon OpenSearch Service-Domain innerhalb einer Amazon VPC ermöglich t die sichere Kommunika tion zwischen Amazon OpenSearch Service und anderen Services innerhalb der Amazon VPC, ohne dass ein Internet-Gateway, ein NAT-Gerät oder eine VPN-Verbindung erforderlich ist.
Abschnitt 4 — Die Cloud-10-Standard-Workloads b-design-and-secure	rds-instance-public-access-überprüfen	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherste llen, dass Amazon Relationa l Database Service (Amazon RDS) -Instances nicht öffentlic h sind. Amazon-RDS-Datenba nk-Instances können vertrauli che Informationen enthalten und für solche Konten sind Prinzipien und Zugriffsk ontrollen erforderlich.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 b-design-and-secure — Die Cloud-10-Standard-Workloads	redshift-cluster-public-access-überprüfen	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Redshift Redshift-Cluster nicht öffentlich sind. Amazon-Redshift-Cluster können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.
Abschnitt 4 b-design-and-secure — Die Cloud — 10-Standard-Workloads	restricted-common-ports	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass gemeinsame Ports für Amazon Elastic Compute Cloud (Amazon EC2) - Sicherheitsgruppen eingeschränkt sind. Wenn der Zugriff auf Ports nicht auf vertrauenswürdige Quellen beschränkt wird, kann dies zu Angriffen auf die Verfügbarkeit, Integrität und Vertraulichkeit von Systemen führen. Mit dieser Regel können Sie optional die Parameter blockedPort1–blockedPort5 festlegen (Standardkonfigurationen: 20, 21, 3389, 3306, 4333). Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 b-design-and-secure — Die Cloud-10-Standard-Workloads	root-account-hardware-mfa-aktiviert	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Hardware-MFA für den Root-Benutzer aktiviert ist. Der Stammbenutzer ist der AWS-Konto-Benutzer mit den meisten Berechtigungen. MFA sorgt für eine weitere Schutzebene zusätzlich zu den Anmeldeinformationen. Indem Sie MFA für den Root-Benutzer vorschreiben, können Sie die Anzahl AWS-Konten kompromittierter Benutzer reduzieren.
Abschnitt 4 — Die Cloud-10-Standard-Workloads b-design-and-secure	root-account-mfa-enabled	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass MFA für den Root-Benutzer aktiviert ist. Der Stammbenutzer ist der AWS-Konto-Benutzer mit den meisten Berechtigungen. MFA bietet eine weitere Schutzebene zusätzlich zum Benutzernamen und Passwort. Indem Sie MFA für den Root-Benutzer vorschreiben, können Sie die Anzahl AWS-Konten kompromittierter Benutzer reduzieren.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 — Die Cloud-10-Standard-Workloads b-design-and-secure	s3- -Blöcke — periodisch account-level-public-access	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Simple Storage Service (Amazon S3) -Buckets nicht öffentlich zugänglich sind. Diese Regel trägt dazu bei, sensible Daten vor unbefugten Remote-Benutzern zu schützen, indem sie den öffentlichen Zugriff verhindert. Mit dieser Regel können Sie optional die Parameter ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) und restrictPublicBuckets Parameter (Config Default: True) festlegen. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 b-design-and-secure — Die Cloud-10-Standard-Workloads	sagemaker-notebook-no-direct-Internetzugang	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass SageMaker Amazon-Notebooks keinen direkten Internetzugang zulassen. Indem Sie direkten Internetzugang blockieren, vermeiden Sie, dass unbefugte Benutzer auf sensible Daten zugreifen.
Abschnitt 4 b-design-and-secure — Die Cloud-10-Standard-Workloads	ssm-document-not-public	Stellen Sie sicher, dass AWS Systems Manager (SSM) -Dokumente nicht öffentlich sind, da dies einen unbeabsichtigten Zugriff auf Ihre SSM-Dokumente ermöglichen kann. Ein öffentliches SSM-Dokument kann Informationen über Ihr Konto, Ihre Ressourcen und internen Prozesse preisgeben.

Kontroll-ID	AWS Config	Empfehlungen
b-design-and-secureAbschnitt 4 — Die Cloud-10-Standard-Workloads	vpc-default-security-group-geschlossen	Sicherheitsgruppen von Amazon Elastic Compute Cloud (Amazon EC2) können bei der Verwaltung des Netzwerkzugriffs helfen, indem sie eine statusbeh aftete Filterung des ein- und ausgehenden Netzwerkv erkehrs zu Ressourcen bereitstellen. AWS Die Beschränkung des gesamten Datenverkehrs auf die Standardsicherheitsgruppe hilft dabei, den Fernzugriff auf Ihre Ressourcen einzuschr änken. AWS

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 — Die Cloud-10-Standard-Workloads b-design-and-secure	vpc-sg-open-only-to-authorized-ports	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass gemeinsame Ports für Amazon Elastic Compute Cloud (Amazon EC2) -Sicherheitsgruppen eingeschränkt sind. Wenn der Zugriff auf Ports nicht auf vertrauenswürdige Quellen beschränkt wird, kann dies zu Angriffen auf die Verfügbarkeit, Integrität und Vertraulichkeit von Systemen führen. Durch die Beschränkung des Zugriffs auf Ressourcen innerhalb einer Sicherheitsgruppe aus dem Internet (0.0.0.0/0) kann der Remote-Zugriff auf interne Systeme gesteuert werden.
Abschnitt 4 b-design-and-secure — Die Cloud-10-Standard-Workloads	s3- verboten bucket-level-public-access	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Simple Storage Service (Amazon S3) -Buckets nicht öffentlich zugänglich sind. Diese Regel trägt dazu bei, sensible Daten vor unbefugten Remote-Benutzern zu schützen, indem sie den öffentlichen Zugriff auf Bucket-Ebene verhindert.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 b-design-and-secure — Die Cloud-10-Standard-Workloads	subnet-auto-assign-public-ip-deaktiviert	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon Virtual Private Cloud (VPC) -Subnetzen nicht automatis ch eine öffentliche IP-Adress e zugewiesen wird. Amazon Elastic Compute Cloud (EC2) -Instances, die in Subnetzen gestartet werden, in denen dieses Attribut aktiviert ist, haben ihrer primären Netzwerkschnittste lle eine öffentliche IP-Adresse zugewiesen.
Abschnitt 4 b-design-and-secure — Materielle Workloads in der Cloud 11	api-gw-execution-logging-ak tiviert	Die API-Gateway-Protok ollierung zeigt detaillierte Ansichten der Benutzer, die auf die API zugegriffen haben, und wie diese Benutzer auf die API zugegriffen haben. Diese Einblicke ermöglichen die Transparenz von Benutzera ktivitäten.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 b-design-and-secure — Die Cloud 11 — materielle Workloads	cloudtrail-s3-dataevents-enabled	Die Erfassung von Simple Storage Service (Amazon S3)-Datenereignissen unterstützt die Erkennung von ungewöhnlichen Aktivitäten. Zu den Details gehören Informationen zu dem AWS -Konto, das auf einen Amazon-S3-Bucket zugegriffen hat, die IP-Adresse und die Uhrzeit des Ereignisses.
Abschnitt 4 — Materielle b-design-and-secure Workloads in der Cloud	cloudtrail-security-trail-enabled	Diese Regel trägt dazu bei, die Verwendung der AWS empfohlenen bewährten Sicherheitsmethoden für sicherzustellen, indem geprüft wird AWS CloudTrail, ob mehrere Einstellungen aktiviert sind. Dazu gehören die Verwendung von Protokoll verschlüsselung, Protokoll validierung und Aktivierung AWS CloudTrail in mehreren Regionen.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 b-design-and-secure — Die Cloud 11 — materielle Workloads	cloudwatch-alarm-action-check	Amazon CloudWatch alarmiert , wenn eine Metrik den Schwellenwert für eine bestimmte Anzahl von Bewertungszeiträumen überschreitet. Der Alarm führt eine oder mehrere Aktionen durch, die vom Wert der Metrik oder des Ausdrucks im Vergleich zu einem Schwellenwert in einer Reihe von Zeiträumen abhängt. Diese Regel erfordert einen Wert für alarmActionRequired (Config Default: True), insufficientDataActionRequired (Config Default: True), okActionRequired (Config Default: False). Der tatsächliche Wert muss die Alarmaktionen für Ihre Umgebung widerspiegeln.
Abschnitt 4 b-design-and-secure — Materielle Workloads in der Cloud 11	cloud-trail-cloud-watch-logs-aktiviert	Verwenden Sie Amazon CloudWatch , um Protokoll ereignisaktivitäten zentral zu sammeln und zu verwalten . Die Aufnahme von AWS CloudTrail Daten liefert Einzelheiten zu den API-Aufrufaktivitäten in Ihrem AWS-Konto.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 b-design-and-secure — Die Cloud 11 — materielle Workloads	elasticsearch-logs-to-cloudwatch	Stellen Sie sicher, dass für Amazon OpenSearch Service-Domains Fehlerprotokolle aktiviert und zur Aufbewahrung und Beantwortung an Amazon CloudWatch Logs gestreamt werden. Domain-Fehlerprotokolle sind bei Sicherheits- und Zugriffsprüfungen sowie bei der Diagnose von Verfügbarkeitsproblemen nützlich.
Abschnitt 4 b-design-and-secure — Die Cloud 11 — materielle Workloads	elb-logging-enabled	Die Elastic-Load-Balancing-Aktivität ist ein zentraler Kommunikationspunkt innerhalb einer Umgebung. Stellen Sie sicher, dass die ELB-Protokollierung aktiviert ist. Die gesammelten Daten enthalten detaillierte Informationen zu Anfragen, die an den ELB gesendet wurden. Jedes Protokoll enthält Informationen wie die Zeit, zu der die Anforderung einging, die Client-IP-Adresse, Latenzen, Anforderungspfade und Serverantworten.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 — Materielle b-design-and-secure Workloads in der Cloud	guardduty-enabled-centralized	Amazon GuardDuty kann mithilfe von Threat Intellige nce Feeds helfen, potenzielle Cybersicherheitsereignisse zu überwachen und zu erkennen. Dazu gehören Listen mit bösartigen IPs und maschinel len Lernmethoden zur Identifiz ierung unerwarteter, nicht autorisierter und bösartige r Aktivitäten in Ihrer AWS Cloud-Umgebung.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 b-design-and-secure — Die Cloud 11 — materielle Workloads	iam-user-unused-credentials-überprüfen	AWS Identity and Access Management (IAM) kann Ihnen bei Zugriffsberechtigungen und Autorisierungen helfen, indem es nach IAM-Passwörtern und Zugriffsschlüsseln sucht, die für einen bestimmten Zeitraum nicht verwendet wurden. Wenn ungenutzte Anmeldeinformationen identifiziert werden, müssen Sie sie deaktivieren und/oder entfernen, da dies gegen das Prinzip der geringsten Berechtigung verstoßen könnte. Für diese Regel müssen Sie einen Wert für das maxCredentialUsage Alter festlegen (Standardkonfiguration: 90). Der tatsächliche Wert muss den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 b-design-and-secure — materielle Workloads in der Cloud 11	rds-logging-enabled	Um die Protokollierung und Überwachung in Ihrer Umgebung zu erleichtern, stellen Sie sicher, dass die Amazon Relational Database Service (Amazon RDS)-Protokollierung aktiviert ist. Mit der Amazon-RDS-Protokollierung können Sie Ereignisse wie Verbindungen, Verbindungsabbrüche, Abfragen oder abgefragte Tabellen erfassen.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 — Materielle b-design-and-secure Workloads in der Cloud	redshift-cluster-configuration-check	Um Daten im Ruhezustand zu schützen, muss die Verschlüsselung für Ihre Amazon-Redshift-Cluster aktiviert sein. Sie müssen auch sicherstellen, dass die erforderlichen Konfigurationen auf Amazon-Redshift-Clustern bereitgestellt werden. Die Prüfungsprotokollierung muss aktiviert sein, um Informationen zu Verbindungen und Benutzeraktivitäten in der Datenbank bereitzustellen. Diese Regel erfordert, dass ein Wert für clusterDbEncrypted (Config Default: TRUE) und LoggingEnabled (Config Default: TRUE) gesetzt ist. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	AWS Config	Empfehlungen
b-design-and-secureAbschnitt 4 — Materielle Workloads in der Cloud 11	s3- bucket-logging-enabled	Die Amazon Simple Storage Service (Amazon S3)-Serverzugriffsprotokollierung bietet eine Methode zur Überwachung des Netzwerks im Hinblick auf potenzielle Cybersicherheitsereignisse. Die Ereignisse werden überwacht, indem detaillierte Aufzeichnungen über die Anfragen erfasst werden, die an einen Amazon-S3-Bucket gestellt wurden. Jeder Zugriffsprotokolleintrag enthält Details zu einer einzelnen Zugriffsanfrage. Zu den Details gehören Anforderer, Bucket-Name, Anforderungszeit, Anforderungsaktion, Antwortstatus und Fehlercode, falls relevant.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 b-design-and-secure — Die Cloud 11 — materielle Arbeitslasten	securityhub-enabled	AWS Security Hub hilft bei der Überwachung von unbefugte m Personal, Verbindungen, Geräten und Software. AWS Security Hub aggregiert, organisiert und priorisiert die Sicherheitswarnungen oder Ergebnisse mehrerer Dienste. AWS Einige dieser Dienste sind Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer und AWS Firewall Manager sowie AWS Partnerlösungen.
Abschnitt 4 — Die Cloud 11 — materielle Workloads b-design-and-secure	vpc-flow-logs-enabled	VPC-Flow-Protokolle erfassen detaillierte Informationsdatens ätze über den IP-Datenv erkehr, der zu und von Netzwerkschnittstellen in Ihrer Amazon Virtual Private Cloud (Amazon VPC) fließt. Standardmäßig enthalten Flow-Protokolldatensätze Werte für die verschiedenen Komponenten des IP-Flows, einschließlich Quelle, Ziel und Protokoll.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 — Materielle b-design-and-secure Workloads in der Cloud	wafv2-logging-enabled	Um die Protokollierung und Überwachung in Ihrer Umgebung zu erleichte rn, aktivieren Sie die AWS WAF (V2) -Protokollierung im regionalen und globalen Web. ACLs AWS Die WAF-Protokollierung bietet detaillie rte Informationen über den Datenverkehr, der von Ihrer Web-ACL analysiert wird. In den Protokollen werden die Uhrzeit aufgezeichnet, zu der die AWS WAF die Anfrage von Ihrer AWS Ressource erhalten hat, Informationen über die Anfrage und eine Aktion für die Regel, der jede Anfrage entsprach.
Abschnitt 4 b-design-and-secure — Die Cloud-12-Standard-Workloads	api-gw-cache-enabled-und verschlüsselt	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass die Verschlüsselung für den Cache Ihrer API-Gatew ay-Stufe aktiviert ist. Da für die API-Methode sensible Daten erfasst werden können, sollten Sie die Verschlüsselung von Daten im Ruhezustand aktivieren, um diese Daten zu schützen.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 — Die Cloud-12-Standard-Workloads b-design-and-secure	cloudwatch-log-group-encrypted	Um sensible Daten im Ruhezustand zu schützen, stellen Sie sicher, dass die Verschlüsselung für Ihre Amazon CloudWatch Log Groups aktiviert ist.
Abschnitt 4 b-design-and-secure — Die Cloud-12-Standard-Workloads	cloud-trail-encryption-enabled	Zum Schutz von eventuell vorhandenen sensiblen Daten sowie Daten im Ruhezustand müssen Sie sicherstellen, dass die Verschlüsselung für Ihre AWS CloudTrail aktiviert ist.
Abschnitt 4 — Die b-design-and-secure Cloud-12-Standard-Workloads	codebuild-project-envvar-awscred-überprüfen	Stellen Sie sicher, dass die Anmeldeinformationen AWS_ACCESS_KEY_ID AWS_SECRET_ACCESS_KEY nicht in AWS Codebuild -Projektumgebungen vorhanden sind. Speichern Sie diese Variablen nicht als Klartext. Das Speichern dieser Variablen als Klartext bewirkt eine unbeabsichtigte Offenlegung von Daten sowie unberechtigte Zugriffe.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 b-design-and-secure — Die Cloud-12-Standard-Workloads	codebuild-project-source-repo-URL-Prüfung	Stellen Sie sicher, dass die URL des Quell-Repositorys GitHub oder des Bitbucket -Quell-Repositorys keine persönlichen Zugriffstoken oder Anmeldeinformationen in Codebuild-Projektumgebungen enthält. AWS Verwende OAuth anstelle von persönlichen Zugriffstoken oder Anmeldedaten die Autorisierung für den Zugriff auf GitHub Bitbucket-Repositorys.
b-design-and-secureAbschnitt 4 — Die Cloud-12-Standard-Workloads	dynamodb-table-encrypted-kms	Stellen Sie sicher, dass die Verschlüsselung für Ihre Amazon-DynamoDB-Tabellen aktiviert ist. Um eventuell vorhandene sensible Daten im Ruhezustand in diesen Tabellen zu schützen, müssen Sie die Verschlüsselung von Daten im Ruhezustand aktivieren. Standardmäßig werden DynamoDB-Tabellen mit einem AWS eigenen Kundenhauptschlüssel (CMK) verschlüsselt.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 — Die b-design-and-secure Cloud-12-Standard-Workloads	ec2- ebs-encryption-by-default	Zum Schutz von Daten im Ruhezustand müssen Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon Elastic Block Store (Amazon EBS)-Volumes aktiviert ist. Da sensible Daten auch im Ruhezusta nd vorhanden sein können, sollten Sie die Verschlüs selung im Ruhezustand aktivieren, um diese Daten zu schützen.
Abschnitt 4 b-design-and-secure — Die Cloud-12-Standard-Workloads	efs-encrypted-check	Aktivieren Sie die Verschlüs selung für Ihr Amazon Elastic File System (EFS), um eventuell vorhandene sensible Daten sowie Daten im Ruhezustand zu schützen.
Abschnitt 4 — Die b-design-and-secure Cloud-12-Standard-Workloads	elasticsearch-encrypted-at-rest	Da sensible Daten vorhanden sein können und um Daten im Ruhezustand zu schützen, sollten Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon OpenSearch Service (OpenSearch Service) -Domains aktiviert ist.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 b-design-and-secure — Die Cloud-12-Standard-Workloads	encrypted-volumes	Aktivieren Sie die Verschlüs selung für Ihre Amazon-El astic-Block-Store (Amazon-EBS)-Volumes, um eventuell vorhandene sensible Daten sowie Daten im Ruhezustand zu schützen.
Abschnitt 4 — Die b-design-and-secure Cloud-12-Standard-Workloads	iam-no-inline-policy-überpr üfen	Stellen Sie sicher, dass ein Benutzer, eine IAM-Rolle oder eine IAM-Grupp e (AWS Identity and Access Management) nicht über eine Inline-Richtlinie zur Zugriffskontrolle auf Systeme und Ressourcen verfügt. AWS empfiehlt, verwaltete Richtlinien anstelle von Inline-Richtlinien zu verwenden . Verwaltete Richtlinien ermöglichen Wiederver wendbarkeit, Versionsv erwaltung, Rollback und Delegierung der Berechtig ungsverwaltung.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 b-design-and-secure — Die Cloud — 12 Standard-Workloads	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) kann Ihnen dabei helfen, die Prinzipien der geringsten Rechte und der Aufgabent rennung in Zugriffsberechtigu ngen und Autorisierungen zu integrieren und so zu verhindern, dass Richtlinien „Effect“: „Allow“ mit „Action“: „*“ anstelle von „Resource“: „*“ enthalten. Wenn Benutzern mehr Rechte eingeräumt werden, als für die Ausführun g einer Aufgabe erforderl ich sind, kann dies gegen das Prinzip der geringste n Berechtigung und der Aufgabentrennung verstoßen.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt b-design-and-secure 4 — Die Cloud-12-Standard-Workloads	iam-user-group-membership-überprüfen	AWS Identity and Access Management (IAM) kann Ihnen helfen, Zugriffsberechtigungen und Autorisierungen einzuschränken, indem sichergestellt wird, dass Benutzer Mitglieder mindestens einer Gruppe sind. Wenn Benutzern mehr Berechtigungen eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und Aufgabentrennung verstoßen.
Abschnitt 4 — Die Cloud-12-Standard-Workloads b-design-and-secure	iam-user-no-policies-überprüfen	Diese Regel stellt sicher, dass AWS Identity and Access Management (IAM) -Richtlinien nur Gruppen oder Rollen zugewiesen werden, um den Zugriff auf Systeme und Ressourcen zu kontrollieren. Die Zuweisung von Berechtigungen auf Gruppen- oder Rollenebene trägt dazu bei, die Wahrscheinlichkeit zu verringern, dass eine Identität übermäßige Berechtigungen erhält oder beibehält.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 b-design-and-secure — Die Cloud-12-Standard-Workloads	opensearch-encrypted-at-rest	Da sensible Daten vorhanden sein können und um Daten im Ruhezustand zu schützen, sollten Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon OpenSearch Service-Domains aktiviert ist.
Abschnitt 4 b-design-and-secure — Die Cloud-12-Standard-Workloads	rds-snapshot-encrypted	Stellen Sie sicher, dass die Verschlüsselung für Ihre Amazon Relational Database Service (Amazon RDS)-Snapshots aktiviert ist. Da sensible Daten auch im Ruhezustand vorhanden sein können, sollten Sie die Verschlüsselung von Daten im Ruhezustand aktivieren, um diese Daten zu schützen.
Abschnitt 4 — Die b-design-and-secure Cloud-12-Standard-Workloads	rds-storage-encrypted	Zum Schutz von Daten im Ruhezustand müssen Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon Relational Database Service (Amazon RDS)-Instances aktiviert ist. Um eventuell vorhandene sensible Daten im Ruhezustand in Amazon-RDS-Instanc es zu schützen, muss die Verschlüsselung von Daten im Ruhezustand aktiviert sein.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 — Die b-design-and-secure Cloud-12-Standard-Workloads	redshift-cluster-configuration-check	Um Daten im Ruhezustand zu schützen, muss die Verschlüsselung für Ihre Amazon-Redshift-Cluster aktiviert sein. Sie müssen auch sicherstellen, dass die erforderlichen Konfigurationen auf Amazon-Redshift-Clustern bereitgestellt werden. Die Prüfungsprotokollierung muss aktiviert sein, um Informationen zu Verbindungen und Benutzeraktivitäten in der Datenbank bereitzustellen. Diese Regel erfordert, dass ein Wert für clusterDbEncrypted (Config Default: TRUE) und LoggingEnabled (Config Default: TRUE) gesetzt ist. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	AWS Config	Empfehlungen
b-design-and-secureAbschnitt 4 — Die Cloud-12-Standard-Workloads	s3-aktiviert bucket-server-side-encryption	Zum Schutz von Daten im Ruhezustand müssen Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon Simple Storage Service (Amazon S3)-Buckets aktiviert ist. Um eventuell vorhandene sensible Daten im Ruhezustand in Amazon-S3-Buckets zu schützen, muss die Verschlüsselung aktiviert sein.
Abschnitt 4 b-design-and-secure — Die Cloud-12-Standard-Workloads	sagemaker-endpoint-configuration-kms-schlüsselkonfiguriert	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass die Verschlüsselung mit dem AWS Key Management Service (AWS KMS) für Ihren Endpunkt aktiviert ist. SageMaker Da sensible Daten auf dem SageMaker Endgerät gespeichert werden können, sollten Sie die Verschlüsselung im Ruhezustand aktivieren, um diese Daten zu schützen.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 b-design-and-secure — Die Cloud-12-Standard-Workloads	sagemaker-notebook-instance-kms-schlüsselkonfiguriert	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass die Verschlüsselung mit dem AWS Key Management Service (AWS KMS) für Ihr Notebook aktiviert ist. SageMaker Da vertrauliche Daten im SageMaker Notebook gespeichert werden können, sollten Sie die Verschlüsselung im Ruhezustand aktivieren, um diese Daten zu schützen.
Abschnitt 4 b-design-and-secure — Die Cloud-12-Standard-Workloads	sns-encrypted-kms	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass Ihre Amazon Simple Notification Service (Amazon SNS) -Themen mit dem AWS Key Management Service (AWS KMS) verschlüsselt werden müssen. Um eventuell vorhandene sensible Daten im Ruhezustand in veröffentlichten Nachrichten zu schützen, muss die Verschlüsselung von Daten im Ruhezustand aktiviert sein.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 b-design-and-secure — Die Cloud — 14 — materielle Workloads	cloudtrail-s3-dataevents-enabled	Die Erfassung von Simple Storage Service (Amazon S3)-Datenereignissen unterstützt die Erkennung von ungewöhnlichen Aktivitäten. Zu den Details gehören Informationen zu dem AWS -Konto, das auf einen Amazon-S3-Bucket zugegriffen hat, die IP-Adresse und die Uhrzeit des Ereignisses.
Abschnitt 4 — Die Cloud b-design-and-secure — 14 — materielle Workloads	cloudtrail-security-trail-enabled	Diese Regel trägt dazu bei, die Verwendung der AWS empfohlenen bewährten Sicherheitsmethoden für sicherzustellen, indem geprüft wird AWS CloudTrail, ob mehrere Einstellungen aktiviert sind. Dazu gehören die Verwendung von Protokoll verschlüsselung, Protokoll validierung und Aktivierung AWS CloudTrail in mehreren Regionen.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 b-design-and-secure — Die Cloud — 14 — materielle Workloads	cloudwatch-alarm-action-check	Amazon CloudWatch alarmiert , wenn eine Metrik den Schwellenwert für eine bestimmte Anzahl von Bewertungszeiträumen überschreitet. Der Alarm führt eine oder mehrere Aktionen durch, die vom Wert der Metrik oder des Ausdrucks im Vergleich zu einem Schwellenwert in einer Reihe von Zeiträumen abhängt. Diese Regel erfordert einen Wert für alarmActionRequired (Config Default: True), insufficientDataActionRequired (Config Default: True), okActionRequired (Config Default: False). Der tatsächliche Wert muss die Alarmaktionen für Ihre Umgebung widerspiegeln.
Abschnitt 4 b-design-and-secure — Die Cloud-14-Material-Workloads	cloud-trail-cloud-watch-logs-aktiviert	Verwenden Sie Amazon CloudWatch , um Protokoll ereignisaktivitäten zentral zu sammeln und zu verwalten . Die Aufnahme von AWS CloudTrail Daten liefert Einzelheiten zu den API-Aufrufaktivitäten in Ihrem AWS-Konto.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 b-design-and-secure — Die Cloud — 14 materielle Workloads	cw-loggroup-retention-period-überprüfen	Stellen Sie sicher, dass die Ereignisprotokolldaten für Ihre Protokollgruppen über eine Mindestdauer aufbewahrt werden, um die Fehlerbehebung und forensische Untersuch ungen zu unterstützen. Fehlende frühere Ereignisp rotokolldaten erschweren die Rekonstruierung und Identifiz ierung potenziell schädlicher Ereignisse.
Abschnitt 4 b-design-and-secure — Die Cloud — 14 — materielle Workloads	db-instance-backup-enabled	Die Sicherungsfunktion von Amazon RDS erstellt Sicherungen Ihrer Datenbank en und Transaktionsprotokolle. Amazon RDS erstellt einen Snapshot für das Speicherv olume Ihrer DB-Instance, sodass die gesamte DB-Instance gesichert wird. Sie können im System spezifisc he Aufbewahrungsfristen festlegen, um Ihre Ausfallsi cherheitsanforderungen zu erfüllen.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 — Die Cloud b-design-and-secure — 14 — materielle Workloads	dynamodb-in-backup-plan	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon DynamoDB-Tabellen Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.
Abschnitt 4 — Die Cloud — 14 — materielle Workloads b-design-and-secure	guardduty-enabled-centralized	Amazon GuardDuty kann mithilfe von Threat Intelligence Feeds helfen, potenzielle Cybersicherheitsereignisse zu überwachen und zu erkennen. Dazu gehören Listen mit bösartigen IPs und maschinellen Lernmethoden zur Identifizierung unerwarteter, nicht autorisierter und bösartiger Aktivitäten in Ihrer AWS Cloud-Umgebung.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 b-design-and-secure — Die Cloud — 14 — materielle Workloads	rds-in-backup-plan	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon Relational Database Service (Amazon RDS) -Instances Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 — Die Cloud — 14 — materielle Workloads b-design-and-secure	redshift-backup-enabled	Stellen Sie zur Unterstützung der Datensicherungsprozesse sicher, dass Ihre Amazon-Redshift-Cluster über automatisierte Snapshots verfügen. Wenn automatisierte Snapshots für einen Cluster aktiviert sind, erstellt Redshift in regelmäßigen Abständen Snapshots dieses Clusters. Standardmäßig erstellt Redshift alle acht Stunden oder alle 5 GB einen Snapshot für jeden Knoten mit Datenänderungen oder je nachdem, was zuerst eintritt.
Abschnitt 4 — Die Cloud — 14 materielle Workloads b-design-and-secure	securityhub-enabled	AWS Security Hub hilft bei der Überwachung von unbefugtem Personal, Verbindungen, Geräten und Software. AWS Security Hub aggregiert, organisiert und priorisiert die Sicherheitswarnungen oder Ergebnisse mehrerer Dienste. AWS Einige dieser Dienste sind Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer und AWS Firewall Manager sowie AWS Partnerlösungen.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 — Cloud-14-Standard-Workloads b-design-and-secure	api-gw-execution-logging-aktiviert	Die API-Gateway-Protokollierung zeigt detaillierte Ansichten der Benutzer, die auf die API zugegriffen haben, und wie diese Benutzer auf die API zugegriffen haben. Diese Einblicke ermöglichen die Transparenz von Benutzeraktivitäten.
Abschnitt 4 b-design-and-secure — Cloud-14-Standard-Workloads	cloudtrail-s3-dataevents-enabled	Die Erfassung von Simple Storage Service (Amazon S3)-Datenereignissen unterstützt die Erkennung von ungewöhnlichen Aktivitäten. Zu den Details gehören Informationen zu dem AWS -Konto, das auf einen Amazon-S3-Bucket zugegriffen hat, die IP-Adresse und die Uhrzeit des Ereignisses.
Abschnitt 4 — b-design-and-secure Cloud-14-Standard-Workloads	cloudtrail-security-trail-enabled	Diese Regel trägt dazu bei, die Verwendung der AWS empfohlenen bewährten Sicherheitsmethoden für sicherzustellen, indem geprüft wird AWS CloudTrail, ob mehrere Einstellungen aktiviert sind. Dazu gehören die Verwendung von Protokoll verschlüsselung, Protokoll validierung und Aktivierung AWS CloudTrail in mehreren Regionen.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 b-design-and-secure — Cloud-14-Standard-Workloads	cloudwatch-log-group-encrypted	Um sensible Daten im Ruhezustand zu schützen, stellen Sie sicher, dass die Verschlüsselung für Ihre Amazon CloudWatch Log Groups aktiviert ist.
Abschnitt 4 b-design-and-secure — Cloud-14-Standard-Workloads	cloud-trail-cloud-watch-Logs aktiviert	Verwenden Sie Amazon CloudWatch , um Protokoll ereignisaktivitäten zentral zu sammeln und zu verwalten . Die Aufnahme von AWS CloudTrail Daten liefert Einzelheiten zu den API-Aufrufaktivitäten in Ihrem AWS-Konto.
Abschnitt 4 b-design-and-secure — Die Cloud — 14-Standard-Workloads	cloud-trail-encryption-enabled	Zum Schutz von eventuell vorhandenen sensiblen Daten sowie Daten im Ruhezustand müssen Sie sicherstellen, dass die Verschlüsselung für Ihre AWS CloudTrail aktiviert ist.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 — b-design-and-secure Cloud-14-Standard-Workloads	cloud-trail-log-file-Validierung aktiviert	Verwenden Sie die AWS CloudTrail Protokolldateivalidierung, um die Integrität von Protokollen zu überprüfen. CloudTrail Mithilfe der Protokolldateivalidierung kann festgestellt werden, ob eine Protokolldatei geändert oder gelöscht wurde oder ob sie nach der Übermittlung CloudTrail unverändert geblieben ist. Dieses Feature wurde mit dem Branchenstandard entsprechenden Algorithmen entwickelt: SHA-256 für die Hashfunktion und SHA-256 mit RSA für digitale Signaturen. Aus diesem Grund ist es rechnerisch unmöglich, CloudTrail Protokolldateien unbemerkt zu ändern, zu löschen oder zu fälschen.

Kontroll-ID	AWS Config	Empfehlungen
b-design-and-secureAbschnitt 4 — Die Cloud-14-Standard-Workloads	cw-loggroup-retention-period-überprüfen	Stellen Sie sicher, dass die Ereignisprotokolldaten für Ihre Protokollgruppen über eine Mindestdauer aufbewahrt werden, um die Fehlerbehebung und forensische Untersuchungen zu unterstützen. Fehlende frühere Ereignisprotokolldaten erschweren die Rekonstruierung und Identifizierung potenziell schädlicher Ereignisse.
Abschnitt 4 b-design-and-secure — Die Cloud-14-Standard-Workloads	elasticsearch-logs-to-cloudwatch	Stellen Sie sicher, dass für Amazon OpenSearch Service-Domains Fehlerprotokolle aktiviert und zur Aufbewahrung und Beantwortung an Amazon CloudWatch Logs gestreamt werden. Domain-Fehlerprotokolle sind bei Sicherheits- und Zugriffsprüfungen sowie bei der Diagnose von Verfügbarkeitsproblemen nützlich.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 b-design-and-secure — Cloud-14-Standard-Workloads	elb-logging-enabled	Die Elastic-Load-Balancing-Aktivität ist ein zentraler Kommunikationspunkt innerhalb einer Umgebung. Stellen Sie sicher, dass die ELB-Protokollierung aktiviert ist. Die gesammelten Daten enthalten detaillierte Informati onen zu Anfragen, die an den ELB gesendet wurden. Jedes Protokoll enthält Informati onen wie die Zeit, zu der die Anforderung einging, die Client-IP-Adresse, Latenzen, Anforderungspfade und Serverantworten.
Abschnitt 4 — b-design-and-secure Cloud-14-Standard-Workloads	guardduty-enabled-centralized	Amazon GuardDuty kann mithilfe von Threat Intellige nce Feeds helfen, potenzielle Cybersicherheitsereignisse zu überwachen und zu erkennen. Dazu gehören Listen mit bösartigen IPs und maschinel len Lernmethoden zur Identifiz ierung unerwarteter, nicht autorisierter und bösartige r Aktivitäten in Ihrer AWS Cloud-Umgebung.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 b-design-and-secure — Cloud-14-Standard-Workloads	iam-no-inline-policy-überprüfen	Stellen Sie sicher, dass ein Benutzer, eine IAM-Rolle oder eine IAM-Gruppe (AWS Identity and Access Management) nicht über eine Inline-Richtlinie zur Zugriffskontrolle auf Systeme und Ressourcen verfügt. AWS empfiehlt, verwaltete Richtlinien anstelle von Inline-Richtlinien zu verwenden . Verwaltete Richtlinien ermöglichen Wiederverwendbarkeit, Versionsverwaltung, Rollback und Delegierung der Berechtigungsverwaltung.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 b-design-and-secure — Die Cloud — 14-Standard-Workloads	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) kann Ihnen dabei helfen, die Prinzipien der geringsten Rechte und der Aufgabent rennung in Zugriffsberechtigu ngen und Autorisierungen zu integrieren und so zu verhindern, dass Richtlinien „Effect“: „Allow“ mit „Action“: „*“ anstelle von „Resource“: „*“ enthalten. Wenn Benutzern mehr Rechte eingeräumt werden, als für die Ausführun g einer Aufgabe erforderl ich sind, kann dies gegen das Prinzip der geringste n Berechtigung und der Aufgabentrennung verstoßen.
Abschnitt b-design-and-secur e 4 — Die Cloud-14-Standard-Workloads	iam-user-no-policies-überpr üfen	Diese Regel stellt sicher, dass AWS Identity and Access Management (IAM) -Richtlin ien nur Gruppen oder Rollen zugewiesen werden, um den Zugriff auf Systeme und Ressourcen zu kontrollieren. Die Zuweisung von Berechtig ungen auf Gruppen- oder Rollenebene trägt dazu bei, die Wahrscheinlichkeit zu verringern, dass eine Identität übermäßige Berechtigungen erhält oder beibehält.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 b-design-and-secure — Cloud-14-Standard-Workloads	multi-region-cloudtrail-enabled	AWS CloudTrail zeichnet Aktionen und AWS API-Aufrufe der Management Console auf. Sie können feststellen, welche Benutzer und Konten angerufen wurden AWS, von welcher Quell-IP-Adresse aus die Anrufe getätigt wurden und wann die Anrufe erfolgten. CloudTrail übermittelt Protokolldateien aus allen AWS Regionen an Ihren S3-Bucket, wenn MULTI_REGION_CLOUD_TRAIL_ENABLED aktiviert ist. Außerdem wird beim AWS Start einer neuen Region derselbe Trail in der neuen Region erstellt. CloudTrail Dadurch erhalten Sie automatisch Protokoll dateien mit API-Aktivitäten für die neue Region.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 b-design-and-secure — Die Cloud — 14-Standard-Workloads	rds-logging-enabled	Um die Protokollierung und Überwachung in Ihrer Umgebung zu erleichtern, stellen Sie sicher, dass die Amazon Relational Database Service (Amazon RDS)-Protokollierung aktiviert ist. Mit der Amazon-RDS-Protokollierung können Sie Ereignisse wie Verbindungen, Verbindungsabbrüche, Abfragen oder abgefragte Tabellen erfassen.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 — b-design-and-secure Cloud-14-Standard-Workloads	redshift-cluster-configuration-check	Um Daten im Ruhezustand zu schützen, muss die Verschlüsselung für Ihre Amazon-Redshift-Cluster aktiviert sein. Sie müssen auch sicherstellen, dass die erforderlichen Konfigurationen auf Amazon-Redshift-Clustern bereitgestellt werden. Die Prüfungsprotokollierung muss aktiviert sein, um Informationen zu Verbindungen und Benutzeraktivitäten in der Datenbank bereitzustellen. Diese Regel erfordert, dass ein Wert für clusterDbEncrypted (Config Default: TRUE) und LoggingEnabled (Config Default: TRUE) gesetzt ist. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	AWS Config	Empfehlungen
b-design-and-secureAbschnitt 4 — Die Cloud-14-Standard-Workloads	s3- -Blöcke — periodisch account-level-public-access	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Simple Storage Service (Amazon S3) -Buckets nicht öffentlich zugänglich sind. Diese Regel trägt dazu bei, sensible Daten vor unbefugten Remote-Benutzern zu schützen, indem sie den öffentlichen Zugriff verhindert. Mit dieser Regel können Sie optional die Parameter ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) und restrictPublicBuckets Parameter (Config Default: True) festlegen. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 b-design-and-secure — Die Cloud-14-Standard-Workloads	s3- bucket-default-lock-enabled	Stellen Sie sicher, dass für Ihren Amazon Simple Storage Service (Amazon S3)-Bucket standardmäßig eine Sperre aktiviert ist. Zum Schutz eventuell vorhandener sensibler Daten in S3-Bucket s müssen Sie Objektsperren für Daten im Ruhezustand erzwingen.
Abschnitt 4 b-design-and-secure — die Cloud-14-Standard-Workloads	s3- bucket-logging-enabled	Die Amazon Simple Storage Service (Amazon S3)-Serve rzugriffsprotokollierung bietet eine Methode zur Überwachung des Netzwerks im Hinblick auf potenzielle Cybersicherheitsereignisse. Die Ereignisse werden überwacht, indem detaillie rte Aufzeichnungen über die Anfragen erfasst werden, die an einen Amazon-S3-Bucket gestellt wurden. Jeder Zugriffsprotokolleintrag enthält Details zu einer einzelnen Zugriffsanfrage. Zu den Details gehören Anfordere r, Bucket-Name, Anforderu ngszeit, Anforderungsaktion, Antwortstatus und Fehlercode, falls relevant.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 b-design-and-secure — die Cloud-14-Standard-Workloads	s3- bucket-policy-grantee-check	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie s3_bucket_policy_grantee_check aktivieren. Diese Regel prüft, ob der vom Amazon S3 S3-Bucket gewährte Zugriff durch die von Ihnen bereitgestellten AWS Principals, Verbundbenutzer, Service Principals, IP-Adressen oder Amazon Virtual Private Cloud (Amazon VPC) IDs eingeschränkt ist.
Abschnitt 4 — Die Cloud-14-Standard-Workloads b-design-and-secure	s3-aktiviert bucket-server-side-encryption	Zum Schutz von Daten im Ruhezustand müssen Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon Simple Storage Service (Amazon S3)-Buckets aktiviert ist. Um eventuell vorhandene sensible Daten im Ruhezustand in Amazon-S3-Buckets zu schützen, muss die Verschlüsselung aktiviert sein.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 b-design-and-secure — Cloud-14-Standard-Workloads	s3- bucket-versioning-enabled	Die Versionsverwaltung von Amazon Simple Storage Service (Amazon S3)-Buckets hilft dabei, mehrere Varianten eines Objekts im selben Amazon-S3-Bucket zu speichern. Verwenden Sie die Versionsverwaltung, um sämtliche Versionen aller Objekte in Ihrem Amazon-S3-Bucket zu speichern, abzurufen oder wiederher zustellen. Mit der Versionsv erwaltung können Sie Versionen sowohl nach unbeabsichtigten Benutzera ktionen als auch nach Anwendungsfehlern problemlo s wiederherstellen.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 b-design-and-secure — die Cloud-14-Standard-Workloads	securityhub-enabled	AWS Security Hub hilft bei der Überwachung von unbefugte m Personal, Verbindungen, Geräten und Software. AWS Security Hub aggregiert, organisiert und priorisiert die Sicherheitswarnungen oder Ergebnisse mehrerer Dienste. AWS Einige dieser Dienste sind Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer und AWS Firewall Manager sowie AWS Partnerlösungen.
Abschnitt 4 — Cloud-14-Standard-Workloads b-design-and-secure	vpc-flow-logs-enabled	VPC-Flow-Protokolle erfassen detaillierte Informationsdatens ätze über den IP-Datenv erkehr, der zu und von Netzwerkschnittstellen in Ihrer Amazon Virtual Private Cloud (Amazon VPC) fließt. Standardmäßig enthalten Flow-Protokolldatensätze Werte für die verschiedenen Komponenten des IP-Flows, einschließlich Quelle, Ziel und Protokoll.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 — b-design-and-secure Cloud-14-Standard-Workloads	wafv2-logging-enabled	Um die Protokollierung und Überwachung in Ihrer Umgebung zu erleichte rn, aktivieren Sie die AWS WAF (V2) -Protokollierung im regionalen und globalen Web. ACLs AWS Die WAF-Protokollierung bietet detaillie rte Informationen über den Datenverkehr, der von Ihrer Web-ACL analysiert wird. In den Protokollen werden die Uhrzeit aufgezeichnet, zu der die AWS WAF die Anfrage von Ihrer AWS Ressource erhalten hat, Informationen über die Anfrage und eine Aktion für die Regel, der jede Anfrage entsprach.
Abschnitt 4 b-design-and-secure — Die Cloud — 15 materielle Workloads	db-instance-backup-enabled	Die Sicherungsfunktion von Amazon RDS erstellt Sicherungen Ihrer Datenbank en und Transaktionsprotokolle. Amazon RDS erstellt einen Snapshot für das Speicherv olume Ihrer DB-Instance, sodass die gesamte DB-Instance gesichert wird. Sie können im System spezifisc he Aufbewahrungsfristen festlegen, um Ihre Ausfallsi cherheitsanforderungen zu erfüllen.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 — Die Cloud-15 b-design-and-secure — materielle Workloads	dynamodb-in-backup-plan	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon DynamoDB-Tabellen Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 — Die Cloud — 15 — materielle Workloads b-design-and-secure	rds-in-backup-plan	Um Sie bei Datensich erungsprozessen zu unterstüt zen, stellen Sie sicher, dass Ihre Amazon Relational Database Service (Amazon RDS) -Instances Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherung smanagement und erleichte rt Ihnen die Erfüllung von geschäftlichen und behördlic hen Compliance-Anforde rungen hinsichtlich Datensich erungen.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 — Die Cloud — 15 — materielle Workloads b-design-and-secure	redshift-backup-enabled	Stellen Sie zur Unterstützung der Datensicherungsprozesse sicher, dass Ihre Amazon-Redshift-Cluster über automatisierte Snapshots verfügen. Wenn automatisierte Snapshots für einen Cluster aktiviert sind, erstellt Redshift in regelmäßigen Abständen Snapshots dieses Clusters. Standardmäßig erstellt Redshift alle acht Stunden oder alle 5 GB einen Snapshot für jeden Knoten mit Datenänderungen oder je nachdem, was zuerst eintritt.
Abschnitt 4 — Cloud-15-Standard-Workloads b-design-and-secure	cmk-backing-key-rotation-aktiviert	Aktivieren Sie die Schlüsselrotation, um sicherzustellen, dass Schlüssel rotiert werden, sobald sie das Ende ihrer Kryptoperiode erreicht haben.
Abschnitt 4 b-design-and-secure — Die Cloud-15-Standard-Workloads	dms-replication-not-public	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass auf DMS-Replikationsinstanzen nicht öffentlich zugegriffen werden kann. DMS-Replikations-Instances können vertrauliche Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 b-design-and-secure — Die Cloud-15-Standard-Workloads	ebs-snapshot-public-restorable-überprüfen	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass EBS-Snapshots nicht öffentlich wiederherstellbar sind. EBS-Volume-Snapshots können vertrauliche Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.
b-design-and-secureAbschnitt 4 — Cloud-15-Standard-Workloads	ec2- ebs-encryption-by-default	Zum Schutz von Daten im Ruhezustand müssen Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon Elastic Block Store (Amazon EBS)-Volumes aktiviert ist. Da sensible Daten auch im Ruhezustand vorhanden sein können, sollten Sie die Verschlüsselung im Ruhezustand aktivieren, um diese Daten zu schützen.
Abschnitt 4 b-design-and-secure — Die Cloud-15-Standard-Workloads	efs-encrypted-check	Aktivieren Sie die Verschlüsselung für Ihr Amazon Elastic File System (EFS), um eventuell vorhandene sensible Daten sowie Daten im Ruhezustand zu schützen.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 — b-design-and-secure Cloud-15-Standard-Workloads	encrypted-volumes	Aktivieren Sie die Verschlüs selung für Ihre Amazon-El astic-Block-Store (Amazon-EBS)-Volumes, um eventuell vorhandene sensible Daten sowie Daten im Ruhezustand zu schützen.
Abschnitt 4 — b-design-and-secure Cloud-15-Standard-Workloads	kms-cmk-not-scheduled-zum Löschen	Um Daten im Ruhezusta nd zu schützen, sollten Sie sicherstellen, dass die für den Kunden erforderlichen Masterschlüssel (CMKs) nicht für das Löschen im AWS Key Management Service (AWS KMS) vorgesehen sind. Da Schlüssel manchmal gelöscht werden müssen, können Sie mit dieser Regel alle zu löschenden Schlüssel überprüfen, falls ein Schlüssel versehentlich zur Löschung vorgemerkt wurde.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 b-design-and-secure — Cloud-15-Standard-Workloads	opensearch-in-vpc-only	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass sich Amazon OpenSearch Service-Domains innerhalb einer Amazon Virtual Private Cloud (Amazon VPC) befinden. Eine Amazon OpenSearch Service-Domain innerhalb einer Amazon VPC ermöglich t die sichere Kommunika tion zwischen Amazon OpenSearch Service und anderen Services innerhalb der Amazon VPC, ohne dass ein Internet-Gateway, ein NAT-Gerät oder eine VPN-Verbindung erforderlich ist.
Abschnitt 4 — Die Cloud-15-Standard-Workloads b-design-and-secure	rds-snapshots-public-prohib ited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherste llen, dass Amazon Relationa l Database Service (Amazon RDS) -Instances nicht öffentlic h sind. Amazon-RDS-Datenba nk-Instances können vertrauli che Informationen enthalten und für solche Konten sind Prinzipien und Zugriffsk ontrollen erforderlich.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 b-design-and-secure — Cloud-15-Standard-Workloads	rds-snapshot-encrypted	Stellen Sie sicher, dass die Verschlüsselung für Ihre Amazon Relational Database Service (Amazon RDS)-Snapshots aktiviert ist. Da sensible Daten auch im Ruhezustand vorhanden sein können, sollten Sie die Verschlüsselung von Daten im Ruhezustand aktivieren, um diese Daten zu schützen.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 — b-design-and-secure Cloud-15-Standard-Workloads	s3- -Blöcke — periodisch account-level-public-access	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Simple Storage Service (Amazon S3) -Buckets nicht öffentlich zugänglich sind. Diese Regel trägt dazu bei, sensible Daten vor unbefugten Remote-Benutzern zu schützen, indem sie den öffentlichen Zugriff verhindert. Mit dieser Regel können Sie optional die Parameter ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) und restrictPublicBuckets Parameter (Config Default: True) festlegen. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 b-design-and-secure — Die Cloud-15-Standard-Workloads	s3- bucket-default-lock-enabled	Stellen Sie sicher, dass für Ihren Amazon Simple Storage Service (Amazon S3)-Bucket standardmäßig eine Sperre aktiviert ist. Zum Schutz eventuell vorhandener sensibler Daten in S3-Bucket s müssen Sie Objektsperren für Daten im Ruhezustand erzwingen.
Abschnitt 4 b-design-and-secure — Die Cloud-15-Standard-Workloads	s3- bucket-policy-grantee-check	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie s3_bucket_policy_grantee_check aktivieren. Diese Regel prüft, ob der vom Amazon S3 S3-Bucket gewährte Zugriff durch die von Ihnen bereitgestellten AWS Principals, Verbundbe nutzer, Service Principals, IP-Adressen oder Amazon Virtual Private Cloud (Amazon VPC) IDs eingeschränkt ist.
Abschnitt 4 — Die Cloud-15-Standard-Workloads b-design-and-secure	s3- bucket-public-read-prohibit ed	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie nur autorisie rten Benutzern, Prozessen und Geräten Zugriff auf Amazon Simple Storage Service (Amazon S3) -Buckets gewähren. Die Verwaltung des Zugriffs sollte mit der Klassifiz ierung der Daten übereinst immen.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 b-design-and-secure — Die Cloud-15-Standard-Workloads	s3- bucket-public-write-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie nur autorisierten Benutzern, Prozessen und Geräten Zugriff auf Amazon Simple Storage Service (Amazon S3) -Buckets gewähren. Die Verwaltung des Zugriffs sollte mit der Klassifizierung der Daten übereinstimmen.
Abschnitt 4 b-design-and-secure — Die Cloud-15-Standard-Workloads	s3-aktiviert bucket-server-side-encryption	Zum Schutz von Daten im Ruhezustand müssen Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon Simple Storage Service (Amazon S3)-Buckets aktiviert ist. Um eventuell vorhandene sensible Daten im Ruhezustand in Amazon-S3 -Buckets zu schützen, muss die Verschlüsselung aktiviert sein.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 b-design-and-secure — Die Cloud-15-Standard-Workloads	s3- bucket-versioning-enabled	Die Versionsverwaltung von Amazon Simple Storage Service (Amazon S3)-Buckets hilft dabei, mehrere Varianten eines Objekts im selben Amazon-S3-Bucket zu speichern. Verwenden Sie die Versionsverwaltung, um sämtliche Versionen aller Objekte in Ihrem Amazon-S3-Bucket zu speichern, abzurufen oder wiederher zustellen. Mit der Versionsv erwaltung können Sie Versionen sowohl nach unbeabsichtigten Benutzera ktionen als auch nach Anwendungsfehlern problemlo s wiederherstellen.
Abschnitt 4 b-design-and-secure — Die Cloud-15-Standard-Workloads	s3- default-encryption-kms	Stellen Sie sicher, dass die Verschlüsselung für Ihre Amazon Simple Storage Service (Amazon S3)-Bucke ts aktiviert ist. Um eventuell vorhandene sensible Daten im Ruhezustand in einem Amazon-S3-Bucket zu schützen, muss die Verschlüs selung aktiviert sein.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 -1- Standard-Workloads c-run-the-cloud	cloudtrail-enabled	AWS CloudTrail kann durch die Aufzeichnung von Aktionen und API-Aufrufen in der Management Console bei der Nichtabstreitbarkeit helfen. AWS Sie können die Benutzer und die Benutzer AWS-Konten , die einen AWS Dienst aufgerufen haben, die Quell-IP-Adresse, über die die Aufrufe generiert wurden, und den Zeitpunkt der Anrufe identifizieren. Einzelheiten zu den erfassten Daten finden Sie in den AWS CloudTrail Datensatzinhalten.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 c-run-the-cloud — 2 — materielle Arbeitslasten	ec2-manager instance-managed-by-systems	Eine Bestandsaufnahme der Softwareplattformen und Anwendungen innerhalb des Unternehmens ist möglich, indem Amazon Elastic Compute Cloud (Amazon EC2) -Instances mit AWS Systems Manager verwaltet werden. Verwenden Sie AWS Systems Manager, um detaillierte Systemkonfigurationen, Betriebssystem-Patch-Levels, Namen und Typ der Dienste, Softwareinstallationen, Anwendungsname, Herausgeber und Version sowie andere Details zu Ihrer Umgebung bereitzustellen.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 c-run-the-cloud — 2 — materielle Arbeitslasten	ec2- prüfen managedinstance-association-compliance-status	Verwenden Sie AWS Systems Manager Associations, um bei der Inventarisierung von Softwareplattformen und Anwendungen innerhalb eines Unternehmens zu helfen. AWS Systems Manager weist Ihren verwalteten Instances einen Konfigurationsstatus zu und ermöglicht es Ihnen, Basiswerte für Betriebss ystem-Patch-Levels, Softwarei nstallationen, Anwendung skonfigurationen und andere Details zu Ihrer Umgebung festzulegen.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 c-run-the-cloud - 2 - Standard-Workloads	cloudwatch-alarm-action-check	Amazon CloudWatch alarmiert, wenn eine Metrik den Schwellenwert für eine bestimmte Anzahl von Bewertungszeiträumen überschreitet. Der Alarm führt eine oder mehrere Aktionen durch, die vom Wert der Metrik oder des Ausdrucks im Vergleich zu einem Schwellenwert in einer Reihe von Zeiträumen abhängt. Diese Regel erfordert einen Wert für alarmActionRequired (Config Default: True), insufficientDataActionRequired (Config Default: True), okActionRequired (Config Default: False). Der tatsächliche Wert muss die Alarmaktionen für Ihre Umgebung widerspiegeln.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 c-run-the-cloud — 2 — Standard-Workloads	guardduty-enabled-centralized	Amazon GuardDuty kann mithilfe von Threat Intellige nce Feeds helfen, potenzielle Cybersicherheitsereignisse zu überwachen und zu erkennen. Dazu gehören Listen mit bösartigen IPs und maschinel len Lernmethoden zur Identifiz ierung unerwarteter, nicht autorisierter und bösartige r Aktivitäten in Ihrer AWS Cloud-Umgebung.
Abschnitt 4 c-run-the-cloud — 2 — Standard-Workloads	iam-group-has-users-überprü fen	AWS Identity and Access Management (IAM) kann Ihnen helfen, die Prinzipien der geringsten Rechte und der Aufgabentrennung mit Zugriffsberechtigungen und Autorisierungen zu integrier en, indem sichergestellt wird, dass IAM-Gruppen mindesten s einen Benutzer haben. Die Einteilung von Benutzern in Gruppen auf der Grundlage der ihnen zugewiesenen Berechtigungen oder ihrer Funktion ist eine Möglichke it, das Prinzip der geringste n Berechtigung zu implement ieren.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 — 2 — Standard-Workloads c-run-the-cloud	iam-no-inline-policy-überprüfen	Stellen Sie sicher, dass ein Benutzer, eine IAM-Rolle oder eine IAM-Gruppe (AWS Identity and Access Management) nicht über eine Inline-Richtlinie zur Zugriffskontrolle auf Systeme und Ressourcen verfügt. AWS empfiehlt, verwaltete Richtlinien anstelle von Inline-Richtlinien zu verwenden . Verwaltete Richtlinien ermöglichen Wiederverwendbarkeit, Versionsverwaltung, Rollback und Delegierung der Berechtigungsverwaltung.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 c-run-the-cloud — 2 — Standard-Workloads	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) kann Ihnen dabei helfen, die Prinzipien der geringsten Rechte und der Aufgabent rennung in Zugriffsberechtigu ngen und Autorisierungen zu integrieren und so zu verhindern, dass Richtlinien „Effect“: „Allow“ mit „Action“: „*“ anstelle von „Resource“: „*“ enthalten. Wenn Benutzern mehr Rechte eingeräumt werden, als für die Ausführun g einer Aufgabe erforderl ich sind, kann dies gegen das Prinzip der geringste n Berechtigung und der Aufgabentrennung verstoßen.
Abschnitt c-run-the-cloud 4 -2 Standard-Workloads	iam-policy-no-statements-with-full-access	Stellen Sie sicher, dass IAM-Aktionen nur auf die benötigte n Aktionen beschränkt sind. Wenn Benutzern mehr Rechte eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und der Aufgabentrennung verstoßen.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 - c-run-the-cloud 2 - Standard-Workloads	iam-root-access-key-überprüfen	Der Zugriff auf Systeme und Ressourcen kann gesteuert werden, indem überprüft wird, ob der Root-Benutzer keine Zugriffsschlüssel mit seiner AWS Identity and Access Management (IAM) -Rolle verknüpft hat. Stellen Sie sicher, dass die Root-Zugriffsschlüssel gelöscht werden. Erstellen und verwenden Sie stattdessen rollenbasierte Funktionen, AWS-Konten um das Prinzip der geringsten Funktionalität zu berücksichtigen.
Abschnitt 4 — 2 — Standard-Workloads c-run-the-cloud	iam-user-group-membership-überprüfen	AWS Identity and Access Management (IAM) kann Ihnen helfen, Zugriffsberechtigungen und Autorisierungen einzuschränken, indem sichergestellt wird, dass Benutzer Mitglieder mindestens einer Gruppe sind. Wenn Benutzern mehr Berechtigungen eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und Aufgabentrennung verstoßen.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 — 2 — Standard-Workloads c-run-the-cloud	iam-user-no-policies-überprüfen	Diese Regel stellt sicher, dass AWS Identity and Access Management (IAM) -Richtlinien nur Gruppen oder Rollen zugewiesen werden, um den Zugriff auf Systeme und Ressourcen zu kontrollieren. Die Zuweisung von Berechtigungen auf Gruppen- oder Rollenebene trägt dazu bei, die Wahrscheinlichkeit zu verringern, dass eine Identität übermäßige Berechtigungen erhält oder beibehält.
Abschnitt 4 c-run-the-cloud — 2 — Standard-Workloads	securityhub-enabled	AWS Security Hub hilft bei der Überwachung von unbefugtem Personal, Verbindungen, Geräten und Software. AWS Security Hub aggregiert, organisiert und priorisiert die Sicherheitswarnungen oder Ergebnisse mehrerer Dienste. AWS Einige dieser Dienste sind Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer und AWS Firewall Manager sowie AWS Partnerlösungen.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 — 3-Standard-Workloads c-run-the-cloud	api-gw-execution-logging-aktiviert	Die API-Gateway-Protokollierung zeigt detaillierte Ansichten der Benutzer, die auf die API zugegriffen haben, und wie diese Benutzer auf die API zugegriffen haben. Diese Einblicke ermöglichen die Transparenz von Benutzeraktivitäten.
Abschnitt 4 c-run-the-cloud -3-Standard-Workloads	cloudtrail-s3-dataevents-enabled	Die Erfassung von Simple Storage Service (Amazon S3)-Datenereignissen unterstützt die Erkennung von ungewöhnlichen Aktivitäten. Zu den Details gehören Informationen zu dem AWS -Konto, das auf einen Amazon-S3-Bucket zugegriffen hat, die IP-Adresse und die Uhrzeit des Ereignisses.
Abschnitt 4 c-run-the-cloud -3-Standard-Workloads	cloudtrail-security-trail-enabled	Diese Regel trägt dazu bei, die Verwendung der AWS empfohlenen bewährten Sicherheitsmethoden für sicherzustellen AWS CloudTrail, indem geprüft wird, ob mehrere Einstellungen aktiviert sind. Dazu gehören die Verwendung von Protokollverschlüsselung, Protokollvalidierung und Aktivierung AWS CloudTrail in mehreren Regionen.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 c-run-the-cloud -3-Standard-Workloads	cloudwatch-alarm-action-check	Amazon CloudWatch alarmiert , wenn eine Metrik den Schwellenwert für eine bestimmte Anzahl von Bewertungszeiträumen überschreitet. Der Alarm führt eine oder mehrere Aktionen durch, die vom Wert der Metrik oder des Ausdrucks im Vergleich zu einem Schwellenwert in einer Reihe von Zeiträumen abhängt. Diese Regel erfordert einen Wert für alarmActionRequired (Config Default: True), insufficientDataActionRequired (Config Default: True), okActionRequired (Config Default: False). Der tatsächliche Wert muss die Alarmaktionen für Ihre Umgebung widerspiegeln.
Abschnitt 4 c-run-the-cloud — 3-Standard-Workloads	cloud-trail-cloud-watch-logs-aktiviert	Verwenden Sie Amazon CloudWatch , um Protokoll ereignisaktivitäten zentral zu sammeln und zu verwalten . Die Aufnahme von AWS CloudTrail Daten liefert Einzelheiten zu den API-Aufrufaktivitäten in Ihrem AWS-Konto.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 c-run-the-cloud -3-Standard-Workloads	cloudtrail-enabled	AWS CloudTrail kann durch die Aufzeichnung von Aktionen und API-Aufrufen in der Management Console bei der Nichtabstreitbarkeit helfen. AWS Sie können die Benutzer und die Benutzer AWS-Konten , die einen AWS Dienst aufgerufen haben, die Quell-IP-Adresse, über die die Aufrufe generiert wurden, und den Zeitpunkt der Anrufe identifizieren. Einzelheiten zu den erfassten Daten finden Sie in den AWS CloudTrail Datensatzinhalten.
Abschnitt 4 c-run-the-cloud -3-Standard-Workloads	cloud-trail-encryption-enabled	Zum Schutz von eventuell vorhandenen sensiblen Daten sowie Daten im Ruhezusta nd müssen Sie sicherstellen, dass die Verschlüsselung für Ihre AWS CloudTrail aktiviert ist.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 c-run-the-cloud -3-Standard-Workloads	cloud-trail-log-file-Validierung aktiviert	Verwenden Sie die AWS CloudTrail Protokolldateivalidierung, um die Integrität von Protokollen zu überprüfen. CloudTrail Mithilfe der Protokolldateivalidierung kann festgestellt werden, ob eine Protokolldatei geändert oder gelöscht wurde oder ob sie nach der Übermittlung CloudTrail unverändert geblieben ist. Dieses Feature wurde mit dem Branchenstandard entsprechenden Algorithmen entwickelt: SHA-256 für die Hashfunktion und SHA-256 mit RSA für digitale Signaturen. Aus diesem Grund ist es rechnerisch unmöglich, CloudTrail Protokolldateien unbemerkt zu ändern, zu löschen oder zu fälschen.

Kontroll-ID	AWS Config	Empfehlungen
c-run-the-cloudAbschnitt 4-3-Standard-Workloads	elasticsearch-logs-to-cloudwatch	Stellen Sie sicher, dass für Amazon OpenSearch Service-Domains Fehlerprotokolle aktiviert und zur Aufbewahrung und Beantwortung an Amazon CloudWatch Logs gestreamt werden. Domain-Fehlerprotokolle sind bei Sicherheits- und Zugriffsprüfungen sowie bei der Diagnose von Verfügbarkeitsproblemen nützlich.
Abschnitt 4-3-Standard-Workloads c-run-the-cloud	elb-logging-enabled	Die Elastic-Load-Balancing-Aktivität ist ein zentraler Kommunikationspunkt innerhalb einer Umgebung. Stellen Sie sicher, dass die ELB-Protokollierung aktiviert ist. Die gesammelten Daten enthalten detaillierte Informationen zu Anfragen, die an den ELB gesendet wurden. Jedes Protokoll enthält Informationen wie die Zeit, zu der die Anforderung einging, die Client-IP-Adresse, Latenzen, Anforderungspfade und Serverantworten.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 c-run-the-cloud -3-Standard-Workloads	guardduty-enabled-centralized	Amazon GuardDuty kann mithilfe von Threat Intellige nce Feeds helfen, potenzielle Cybersicherheitsereignisse zu überwachen und zu erkennen. Dazu gehören Listen mit bösartigen IPs und maschinel len Lernmethoden zur Identifiz ierung unerwarteter, nicht autorisierter und bösartige r Aktivitäten in Ihrer AWS Cloud-Umgebung.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4-3-Standard-Workloads c-run-the-cloud	multi-region-cloudtrail-enabled	AWS CloudTrail zeichnet Aktionen AWS und API-Aufrufe der Management Console auf. Sie können feststellen, welche Benutzer und Konten angerufen wurden AWS, von welcher Quell-IP-Adresse aus die Anrufe getätigt wurden und wann die Anrufe erfolgten. CloudTrail übermittelt Protokolldateien aus allen AWS Regionen an Ihren S3-Bucket, wenn MULTI_REGION_CLOUD_TRAIL_ENABLED aktiviert ist. Außerdem wird beim AWS Start einer neuen Region derselbe Trail in der neuen Region erstellt. CloudTrail Dadurch erhalten Sie automatisch Protokoll dateien mit API-Aktivitäten für die neue Region.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4-3-Standard-Workloads c-run-the-cloud	rds-logging-enabled	Um die Protokollierung und Überwachung in Ihrer Umgebung zu erleichtern, stellen Sie sicher, dass die Amazon Relational Database Service (Amazon RDS)-Protokollierung aktiviert ist. Mit der Amazon-RDS-Protokollierung können Sie Ereignisse wie Verbindungen, Verbindungsabbrüche, Abfragen oder abgefragte Tabellen erfassen.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 c-run-the-cloud -3-Standard-Workloads	redshift-cluster-configuration-check	Um Daten im Ruhezustand zu schützen, muss die Verschlüsselung für Ihre Amazon-Redshift-Cluster aktiviert sein. Sie müssen auch sicherstellen, dass die erforderlichen Konfigurationen auf Amazon-Redshift-Clustern bereitgestellt werden. Die Prüfungsprotokollierung muss aktiviert sein, um Informationen zu Verbindungen und Benutzeraktivitäten in der Datenbank bereitzustellen. Diese Regel erfordert, dass ein Wert für clusterDbEncrypted (Config Default: TRUE) und LoggingEnabled (Config Default: TRUE) gesetzt ist. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 — 3-Standard-Workloads c-run-the-cloud	s-3 bucket-logging-enabled	Die Amazon Simple Storage Service (Amazon S3)-Serverzugriffsprotokollierung bietet eine Methode zur Überwachung des Netzwerks im Hinblick auf potenzielle Cybersicherheitsereignisse. Die Ereignisse werden überwacht, indem detaillierte Aufzeichnungen über die Anfragen erfasst werden, die an einen Amazon-S3-Bucket gestellt wurden. Jeder Zugriffsprotokolleintrag enthält Details zu einer einzelnen Zugriffsanfrage. Zu den Details gehören Anforderer, Bucket-Name, Anforderungszeit, Anforderungsaktion, Antwortstatus und Fehlercode, falls relevant.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 c-run-the-cloud -3-Standard-Workloads	securityhub-enabled	AWS Security Hub hilft bei der Überwachung von unbefugte m Personal, Verbindungen, Geräten und Software. AWS Security Hub aggregiert, organisiert und priorisiert die Sicherheitswarnungen oder Ergebnisse mehrerer Dienste. AWS Einige dieser Dienste sind Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer und AWS Firewall Manager sowie AWS Partnerlösungen.
Abschnitt 4 — 3-Standard-Workloads c-run-the-cloud	vpc-flow-logs-enabled	VPC-Flow-Protokolle erfassen detaillierte Informationsdatens ätze über den IP-Datenv erkehr, der zu und von Netzwerkschnittstellen in Ihrer Amazon Virtual Private Cloud (Amazon VPC) fließt. Standardmäßig enthalten Flow-Protokolldatensätze Werte für die verschiedenen Komponenten des IP-Flows, einschließlich Quelle, Ziel und Protokoll.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 c-run-the-cloud -3-Standard-Workloads	wafv2-logging-enabled	Um die Protokollierung und Überwachung in Ihrer Umgebung zu erleichte rn, aktivieren Sie die AWS WAF (V2) -Protokollierung im regionalen und globalen Web. ACLs AWS Die WAF-Protokollierung bietet detaillie rte Informationen über den Datenverkehr, der von Ihrer Web-ACL analysiert wird. In den Protokollen werden die Uhrzeit aufgezeichnet, zu der die AWS WAF die Anfrage von Ihrer AWS Ressource erhalten hat, Informationen über die Anfrage und eine Aktion für die Regel, der jede Anfrage entsprach.
Abschnitt 4 c-run-the-cloud — 4-Standard-Workloads	response-plan-exists-mainta ined (Prozessüberprüfung)	Stellen Sie sicher, dass Vorfallreaktionspläne erstellt, verwaltet und an das verantwortliche Personal verteilt werden.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4-4-materielle Arbeitsbelastungen c-run-the-cloud	alb-waf-enabled	Stellen Sie sicher, dass AWS WAF auf Elastic Load Balancers (ELB) aktiviert ist, um Webanwendungen zu schützen. Eine WAF trägt zum Schutz Ihrer Webanwendungen oder APIs vor gängigen Web-Exploits bei. Diese Web-Exploits können sich auf die Verfügbarkeit auswirken, die Sicherheit gefährden oder übermäßige Ressourcen in Ihrer Umgebung verbrauchen.
Abschnitt 4 — 4 — materielle Arbeitslasten c-run-the-cloud	api-gw-associated-with-WAF	AWS Mit WAF können Sie eine Reihe von Regeln (als Web Access Control List (Web ACL) bezeichnet) konfigurieren, die Webanfragen auf der Grundlage von anpassbaren Websicherheitsregeln und -bedingungen, die Sie definieren, zulassen, blockieren oder zählen. Stellen Sie sicher, dass Ihre Amazon-API-Gateway-Stufe mit einer WAF-Web-ACL verknüpft ist, um sie vor böswilligen Angriffen zu schützen.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 c-run-the-cloud — 4 — materielle Arbeitslasten	guardduty-enabled-centralized	Amazon GuardDuty kann mithilfe von Threat Intellige nce Feeds helfen, potenzielle Cybersicherheitsereignisse zu überwachen und zu erkennen. Dazu gehören Listen mit bösartigen IPs und maschinel len Lernmethoden zur Identifiz ierung unerwarteter, nicht autorisierter und bösartige r Aktivitäten in Ihrer AWS Cloud-Umgebung.
Abschnitt 4 c-run-the-cloud — 4 — materielle Arbeitslasten	securityhub-enabled	AWS Security Hub hilft bei der Überwachung von unbefugte m Personal, Verbindungen, Geräten und Software. AWS Security Hub aggregiert, organisiert und priorisiert die Sicherheitswarnungen oder Ergebnisse mehrerer Dienste. AWS Einige dieser Dienste sind Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer und AWS Firewall Manager sowie AWS Partnerlösungen.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 — 5 — Standard-Workloads c-run-the-cloud	autoscaling-group-elb-healthcheck-erforderlich	Die Elastic Load Balancer (ELB) -Zustandsprüfungen für Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling Scaling-Gruppen unterstützen die Aufrechterhaltung einer angemessenen Kapazität und Verfügbarkeit. Der Load Balancer sendet regelmäßig Pings, versucht Verbindungen herzustellen oder sendet Anfragen, um den Zustand der EC2 Amazon-Instances in einer Gruppe mit auto-scaling zu testen. Wenn eine Instance nicht zurückmeldet, wird der Traffic an eine neue EC2 Amazon-Instance gesendet.
Abschnitt 4 c-run-the-cloud — 5 — Standard-Workloads	cloud-trail-cloud-watch-logs-aktiviert	Verwenden Sie Amazon CloudWatch , um Protokollereignisaktivitäten zentral zu sammeln und zu verwalten . Die Aufnahme von AWS CloudTrail Daten liefert Einzelheiten zu den API-Aufrufaktivitäten in Ihrem AWS-Konto.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 c-run-the-cloud — 5 — Standard-Workloads	dynamodb-autoscaling-enabled	Amazon DynamoDB Auto Scaling verwendet den AWS Application Auto Scaling-Service, um die bereitgestellte Durchsatzkapazität so anzupassen, dass sie automatisch auf tatsächliche Verkehrsmuster reagiert. Auf diese Weise kann eine Tabelle oder ein globaler sekundärer Index die bereitgestellte Lese-/Schreibkapazität erhöhen, um plötzliche Erhöhungen des Datenverkehrs ohne Drosselung zu bewältigen.

Kontroll-ID	AWS Config	Empfehlungen
c-run-the-cloudAbschnitt 4 — 5 — Standard-Workloads	dynamodb-throughput-limit-check	Aktivieren Sie diese Regel, um sicherzustellen, dass die bereitgestellte Durchsatz kapazität in Ihren Amazon-DynamoDB-Tabellen überprüft wird. Dies ist der Umfang der Lese- und Schreibak tivitäten, der von den jeweilige n Tabellen unterstützt werden kann. DynamoDB verwendet diese Informationen für das Reservieren ausreichender Systemressourcen, um Ihren Durchsatzanforderungen gerecht zu werden. Diese Regel generiert eine Warnung, wenn sich der Durchsatz dem Höchstlimit für ein Kundenkon to nähert. Mit dieser Regel können Sie optional die Parameter RCUThreshold Kontoprozentsatz (Konfigur ationsstandard: 80) und WCUThreshold Kontoproz entsatz (Konfigurationssta ndard: 80) festlegen. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisat ion entsprechen.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 c-run-the-cloud — 5 — Standard-Workloads	ec2- instance-detailed-monitoring-enabled	Aktivieren Sie diese Regel, um die Amazon Elastic Compute Cloud (Amazon EC2) -Instance-Überwachung auf der EC2 Amazon-Konsole zu verbessern, in der Monitoring-Diagramme mit einem Zeitraum von 1 Minute für die Instance angezeigt werden.
Abschnitt 4 c-run-the-cloud — 5 — Standard-Workloads	lambda-concurrency-check	Diese Regel stellt sicher, dass die Höchst- und Untergrenzen für die Gleichzeitigkeit einer Lambda-Funktion festgelegt werden. Dies kann Sie beim Baselining für die Anzahl der Anforderungen unterstützen, die Ihre Funktion zu einem bestimmten Zeitpunkt verarbeitet.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 — c-run-the-cloud 5 — Standard-Workloads	rds-enhanced-monitoring-enabled	Aktivieren Sie Amazon Relational Database Service (Amazon RDS), um die Verfügbarkeit von Amazon RDS zu überwachen. Dies bietet einen detaillierten Einblick in den Zustand Ihrer Amazon-RDS-Datenbank-Instances. Wenn der Amazon-RDS-Speicher mehr als ein zugrunde liegendes physisches Gerät verwendet, erfasst Enhanced Monitoring die Daten für jedes Gerät. Wenn die Datenbank-Instance von Amazon RDS in einer Multi-AZ-Bereitstellung ausgeführt wird, werden außerdem die Daten für jedes Gerät auf dem sekundären Host sowie die Metriken des sekundären Hosts erfasst.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 — c-run-the-cloud 5 — Standard-Workloads	beanstalk-enhanced-health-reporting-aktiviert	AWS Die verbesserte Zustandsberichterstattung von Elastic Beanstalk ermöglicht eine schnellere Reaktion auf Veränderungen im Zustand der zugrunde liegenden Infrastruktur. Diese Änderungen könnten zu einer mangelnden Verfügbarkeit der Anwendung führen. Die erweiterten Zustandsberichte von Elastic Beanstalk bieten eine Statusbeschreibung, um den Schweregrad der identifizierten Probleme einzuschätzen und mögliche Ursachen zu identifizieren, die untersucht werden müssen.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 — 6 — materielle Arbeitslasten c-run-the-cloud	ec2-manager instance-managed-by-systems	Eine Bestandsaufnahme der Softwareplattformen und Anwendungen innerhalb des Unternehmens ist möglich, indem Amazon Elastic Compute Cloud (Amazon EC2) -Instances mit AWS Systems Manager verwaltet werden. Verwenden Sie AWS Systems Manager, um detaillierte Systemkonfigurationen, Betriebssystem-Patch-Levels, Namen und Typ der Dienste, Softwareinstallationen, Anwendungsname, Herausgeber und Version sowie andere Details zu Ihrer Umgebung bereitzustellen.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 c-run-the-cloud — 6 — materielle Arbeitslasten	ec2- prüfen managedinstance-association-compliance-status	Verwenden Sie AWS Systems Manager Associations, um bei der Inventarisierung von Softwareplattformen und Anwendungen innerhalb eines Unternehmens zu helfen. AWS Systems Manager weist Ihren verwalteten Instances einen Konfigurationsstatus zu und ermöglicht es Ihnen, Basiswerte für Betriebss ystem-Patch-Levels, Softwarei nstallationen, Anwendung skonfigurationen und andere Details zu Ihrer Umgebung festzulegen.
Abschnitt 4 c-run-the-cloud — 6 — materielle Arbeitsbe lastungen	ec2- prüfen managedinstance-patch-compliance-status	Aktivieren Sie diese Regel, um bei der Identifizierung und Dokumentation von Sicherhei tslücken in Amazon Elastic Compute Cloud (Amazon EC2) zu helfen. Die Regel prüft, ob die EC2 Amazon-In stance die Patch-Konformität im AWS Systems Manager gemäß den Richtlinien und Verfahren Ihrer Organisation einhält.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 c-run-the-cloud — 6 — materielle Arbeitslasten	guardduty-enabled-centralized	Amazon GuardDuty kann mithilfe von Threat Intellige nce Feeds helfen, potenzielle Cybersicherheitsereignisse zu überwachen und zu erkennen. Dazu gehören Listen mit bösartigen IPs und maschinel len Lernmethoden zur Identifiz ierung unerwarteter, nicht autorisierter und bösartige r Aktivitäten in Ihrer AWS Cloud-Umgebung.
Abschnitt 4 c-run-the-cloud — 6 — materielle Arbeitslasten	guardduty-non-archived-find ings	Amazon GuardDuty hilft Ihnen dabei, die Auswirkungen eines Vorfalls zu verstehen, indem es die Ergebnisse nach Schweregrad klassifiziert: niedrig, mittel und hoch. Diese Klassifizierungen können Sie zur Festlegung von entsprech enden Strategien und Priorität en zur Behebung solcher Vorfälle verwenden. Mit dieser Regel können Sie optional daysLowSev (Config Default: 30), daysMediu mSev (Config Default: 7) und daysHighSev (Config Default: 1) für nicht archivierte Ergebnisse festlegen, wie es die Richtlinien Ihrer Organisat ion erfordern.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 c-run-the-cloud — 6 — Standard-Workloads	ec2-manager instance-managed-by-systems	Eine Bestandsaufnahme der Softwareplattformen und Anwendungen innerhalb des Unternehmens ist möglich, indem Amazon Elastic Compute Cloud (Amazon EC2) -Instances mit AWS Systems Manager verwaltet werden. Verwenden Sie AWS Systems Manager, um detaillierte Systemkonfiguratio nen, Betriebssystem-Patch-Levels, Namen und Typ der Dienste, Softwareinstallati onen, Anwendungsname, Herausgeber und Version sowie andere Details zu Ihrer Umgebung bereitzustellen.
Abschnitt 4 c-run-the-cloud — 6 — Standard-Workloads	ec2- prüfen managedinstance-patch-compliance-status	Aktivieren Sie diese Regel, um bei der Identifizierung und Dokumentation von Sicherhei tslücken in Amazon Elastic Compute Cloud (Amazon EC2) zu helfen. Die Regel prüft, ob die EC2 Amazon-In stance die Patch-Konformität im AWS Systems Manager gemäß den Richtlinien und Verfahren Ihrer Organisation einhält.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 c-run-the-cloud — 6 — Standard-Workloads	redshift-cluster-maintenancesettings-check	Diese Regel stellt sicher, dass Amazon-Redshift-Cluster die bevorzugten Einstellungen für Ihre Organisation haben. Insbesondere sorgt sie dafür, dass Cluster bevorzugte Wartungsfenster und automatisierte Aufbewahrungsfristen für Snapshots für die Datenbank haben. Für diese Regel müssen Sie die festlegen. allowVersionUpgrade Der Standardwert ist „true“. Außerdem können Sie optional den Zeitraum preferredMaintenanceWindow (der Standardwert ist sa: 16:00 -sa: 16:30) und den automatedSnapshotRetention Zeitraum (der Standardwert ist 1) festlegen. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 — 6 — Standard-Workloads c-run-the-cloud	elastic-beanstalk-managed-updates-aktiviert	Durch die Aktivierung verwalteter Plattformupdates für eine Amazon-Elastic-Beanstalk-Umgebung wird sichergestellt, dass die aktuellen verfügbaren Plattform-Fixes, -Updates und -Features für die Umgebung installiert sind. Eine bewährte Methode zur Sicherung von Systemen besteht darin, stets die aktuellen Patches zu installieren.

Vorlage

Die Vorlage ist verfügbar unter GitHub: Operational Best Practices for ABS CCIG 2.0 Material Workloads.

Bewährte Methoden für den Betrieb von ABS CCIG 2.0 Standard Workloads

Konformitätspakete bieten ein allgemeines Compliance-Framework, das es Ihnen ermöglicht, mithilfe verwalteter oder benutzerdefinierter Regeln und Abhilfemaßnahmen Kontrollen zur Sicherheits-, Betriebs- oder Kostenoptimierung durchzuführen. AWS Config AWS Config Conformance Packs dienen als Beispielvorlagen nicht dazu, die vollständige Einhaltung eines bestimmten Governance- oder Compliance-Standards sicherzustellen. Sie sind dafür verantwortlich, selbst zu beurteilen, ob Ihre Nutzung der Services den geltenden gesetzlichen und behördlichen Anforderungen entspricht.

Im Folgenden finden Sie ein Beispiel für eine Zuordnung zwischen dem ABS Cloud Computing Implementation Guide 2.0 — Standard Workloads und AWS Managed Config Rules. Jede Config-Regel gilt für eine bestimmte AWS Ressource und bezieht sich auf eine oder mehrere Steuerelemente des ABS Cloud Computing Implementation Guide. Eine Kontrolle des ABS Cloud Computing Implementation Guide kann sich auf mehrere Konfigurationsregeln beziehen. In der folgenden Tabelle finden Sie weitere Informationen und Anleitungen zu diesen Zuordnungen.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 a-govern-the-cloud - 2 - Standard-Workloads	account-part-of-organizations	Durch die zentrale Verwaltun g AWS-Konten innerhalb von AWS Organizations wird sichergestellt, dass die Konten den Vorschriften entsprech en. Eine fehlende zentrale Kontoverwaltung kann zu inkonsistenten Kontokonf igurationen führen, wodurch Ressourcen und sensible Daten offengelegt werden können.
Abschnitt 4 a-govern-the-cloud — 2 — Standard-Workloads	cloudtrail-s3-dataevents-en abled	Die Erfassung von Simple Storage Service (Amazon S3)-Datenereignissen unterstützt die Erkennung von ungewöhnl ichen Aktivitäten. Zu den Details gehören Informati onen zu dem AWS -Konto, das auf einen Amazon-S3-Bucket zugegriffen hat, die IP-Adresse und die Uhrzeit des Ereignisses.
Abschnitt 4 - a-govern-the-cloud 2 - Standard-Workloads	cloudtrail-security-trail-enabled	Diese Regel hilft sicherzus tellen, dass die AWS empfohlenen bewährten Sicherheitsmethoden für verwendet werden AWS CloudTrail, indem geprüft wird, ob mehrere Einstellungen aktiviert sind. Dazu gehören die Verwendung von Protokoll verschlüsselung, Protokoll

Kontroll-ID	AWS Config	Empfehlungen
		validierung und Aktivierung AWS CloudTrail in mehreren Regionen.
Abschnitt 4 a-govern-the-cloud — 2 — Standard-Workloads	cloudwatch-alarm-action-check	Amazon CloudWatch alarmiert, wenn eine Metrik den Schwellenwert für eine bestimmte Anzahl von Bewertungszeiträumen überschreitet. Der Alarm führt eine oder mehrere Aktionen durch, die vom Wert der Metrik oder des Ausdrucks im Vergleich zu einem Schwellenwert in einer Reihe von Zeiträumen abhängt. Diese Regel erfordert einen Wert für alarmActionRequired (Config Default: True), insufficientDataActionRequired (Config Default: True), okActionRequired (Config Default: False). Der tatsächliche Wert muss die Alarmaktionen für Ihre Umgebung widerspiegeln.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 a-govern-the-cloud — 2 — Standard-Workloads	cloud-trail-cloud-watch-logs-aktiviert	Verwenden Sie Amazon CloudWatch , um Protokoll ereignisaktivitäten zentral zu sammeln und zu verwalten . Die Aufnahme von AWS CloudTrail Daten liefert Einzelheiten zu den API-Aufru faktivitäten in Ihrem AWS-Konto.
Abschnitt 4 a-govern-the-cloud — 2 — Standard-Workloads	ec2-manager instance-managed-by-systems	Eine Bestandsaufnahme der Softwareplattformen und Anwendungen innerhalb des Unternehmens ist möglich, indem Amazon Elastic Compute Cloud (Amazon EC2) -Instances mit AWS Systems Manager verwaltet werden. Verwenden Sie AWS Systems Manager, um detaillierte Systemkonfiguratio nen, Betriebssystem-Patch-Levels, Namen und Typ der Dienste, Softwareinstallati onen, Anwendungsname, Herausgeber und Version sowie andere Details zu Ihrer Umgebung bereitzustellen.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 a-govern-the-cloud - 2 - Standard-Workloads	guardduty-enabled-centralized	Amazon GuardDuty kann mithilfe von Threat Intellige nce Feeds helfen, potenzielle Cybersicherheitsereignisse zu überwachen und zu erkennen. Dazu gehören Listen mit bösartigen IPs und maschinel len Lernmethoden zur Identifiz ierung unerwarteter, nicht autorisierter und bösartige r Aktivitäten in Ihrer AWS Cloud-Umgebung.
Abschnitt 4 a-govern-the-cloud — 2 — Standard-Workloads	securityhub-enabled	AWS Security Hub hilft bei der Überwachung von unbefugte m Personal, Verbindungen, Geräten und Software. AWS Security Hub aggregiert, organisiert und priorisiert die Sicherheitswarnungen oder Ergebnisse mehrerer Dienste. AWS Einige dieser Dienste sind Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer und AWS Firewall Manager sowie AWS Partnerlösungen.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 — 3-Standard-Workloads a-govern-the-cloud	ec2-manager instance-managed-by-systems	Eine Bestandsaufnahme der Softwareplattformen und Anwendungen innerhalb des Unternehmens ist möglich, indem Amazon Elastic Compute Cloud (Amazon EC2) -Instances mit AWS Systems Manager verwaltet werden. Verwenden Sie AWS Systems Manager, um detaillierte Systemkonfigurationen, Betriebssystem-Patch-Levels, Namen und Typ der Dienste, Softwareinstallationen, Anwendungsname, Herausgeber und Version sowie andere Details zu Ihrer Umgebung bereitzustellen.
Abschnitt 4 a-govern-the-cloud — 3-Standard-Workloads	ec2-stopped-instance	Aktivieren Sie diese Regel, um bei der Basiskonfiguration von Amazon Elastic Compute Cloud (Amazon EC2) -Instances zu helfen, indem Sie überprüfen, ob EC2 Amazon-Instances gemäß den Standards Ihrer Organisation für mehr als die zulässige Anzahl von Tagen gestoppt wurden.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 a-govern-the-cloud — 3-Standard-Workloads	ec2- volume-inuse-check	Diese Regel stellt sicher, dass Amazon Elastic Block Store-Volumes, die an Amazon Elastic Compute Cloud (Amazon EC2) -Instances angehängt sind, zum Löschen markiert werden, wenn eine Instance beendet wird. Wenn ein Amazon-EBS-Volume nicht gelöscht wird, wenn die Instance, an die es angehängt ist, beendet wird, kann dies gegen das Konzept der geringsten Funktionalität verstoßen.
Abschnitt 4 a-govern-the-cloud — 3-Standard-Workloads	eip-attached	Diese Regel stellt sicher, dass Elastic, die einer Amazon Virtual Private Cloud (Amazon VPC) IPs zugewiesen sind, an Amazon Elastic Compute Cloud (Amazon EC2) - Instances oder verwendete Elastic Network Interfaces angehängt sind. Diese Regel hilft bei der Überwachung ungenutzter Inhalte EIPs in Ihrer Umgebung.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 a-govern-the-cloud -3-Standard-Workloads	vpc-network-acl-unused-überprüfen	Diese Regel stellt sicher, dass Amazon Virtual Private Cloud (VPC)-Netzwerkzugriffskontrolllisten verwendet werden. Die Überwachung ungenutzter Netzwerkzugriffskontrolllisten kann zu einer genauen Inventarisierung und Verwaltung Ihrer Umgebung beitragen.
Abschnitt 4 b-design-and-secure — Die Cloud-1-Standard-Workloads	autoscaling-launch-config-public-ip-deaktiviert	Wenn Sie Ihre Netzwerkschnittstellen mit einer öffentlichen IP-Adresse konfigurieren, sind die diesen Netzwerkschnittstellen zugehörigen Ressourcen über das Internet erreichbar. EC2 Ressourcen sollten nicht öffentlich zugänglich sein, da dies einen unbeabsichtigten Zugriff auf Ihre Anwendungen oder Server ermöglichen kann.
Abschnitt 4 b-design-and-secure — Die Cloud-1-Standard-Workloads	dms-replication-not-public	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass auf DMS-Replikationsinstanzen nicht öffentlich zugegriffen werden kann. DMS-Replikations-Instances können vertrauliche Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 b-design-and-secure — Die Cloud-1-Standard-Workloads	ebs-snapshot-public-restorable-überprüfen	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass EBS-Snapshots nicht öffentlich wiederherstellbar sind. EBS-Volume-Snapshots können vertrauliche Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.
b-design-and-secureAbschnitt 4 — Die Cloud-1-Standard-Workloads	ec2- instance-no-public-ip	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon Elastic Compute Cloud (Amazon EC2) -Instances nicht öffentlich zugänglich sind. EC2Amazon-Instances können vertrauliche Informationen enthalten, und für solche Konten ist eine Zugriffskontrolle erforderlich.
Abschnitt 4 b-design-and-secure — Die Cloud-1-Standard-Workloads	ec2- instance-profile-attached	EC2 Instanzprofile übergeben eine IAM-Rolle an eine Instanz EC2 . Das Anhängen eines Instance-Profils an Ihre Instances kann bei der Implementierung von geringsten Berechtigungen und der Berechtigungsverwaltung helfen.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 b-design-and-secure — Die Cloud-1-Standard-Workloads	ecs-task-definition-user-for-host-mode-check	Wenn für eine Aufgabendefinition erhöhte Berechtigungen gelten, liegt das daran, dass der Kunde diesen Konfigurationen ausdrücklich zugestimmt hat. Diese Kontrolle prüft, ob eine unerwartete Berechtigungseskalation vorliegt, wenn für eine Aufgabendefinition das Host-Netzwerk aktiviert ist, die Kunden aber keine erhöhten Berechtigungen aktiviert haben.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 — b-design-and-secure Cloud-1-Standard-Workloads	emr-kerberos-enabled	Die Zugriffsberechtigungen und -autorisierungen können verwaltet und nach den Prinzipien der geringsten Berechtigung und Aufgabentrennung integriert werden, indem Kerberos für Amazon-EMR-Cluster aktiviert wird. In Kerberos werden Services und Benutzer, die sich authentifizieren müssen, als Prinzipale bezeichnet. Prinzipale befinden sich in einem Kerberos-Bereich. Innerhalb dieses Bereichs wird ein Kerberos-Server als Key Distribution Center (KDC) bezeichnet. Über diesen Server können sich Prinzipale authentifizieren. Die Authentifizierung im KDC erfolgt durch die Ausstellung von Authentifizierungstickets. Das KDC unterhält eine Datenbank der Prinzipale in seinem Bereich mit ihren Passwörtern und anderen administrativen Informationen zu jedem Prinzipal.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 — b-design-and-secure Cloud-1-Standard-Workloads	emr-master-no-public-ip	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon EMR-Cluster-Masterknoten nicht öffentlich zugänglich sind. Amazon-EMR-Cluster-Hauptknoten können vertrauliche Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 b-design-and-secure — Die Cloud-1-Standard-Workloads	iam-customer-policy-blocked-kms-Aktionen	AWS Identity and Access Management (IAM) kann Ihnen helfen, die Prinzipien der geringsten Rechte und der Aufgabentrennung in Zugriffsberechtigungen und Autorisierungen zu integrieren und so zu verhindern, dass Richtlinien blockierte Aktionen für alle AWS Schlüssel des Key Management Service enthalten. Wenn Benutzer mehr Rechte haben, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und Aufgabentrennung verstoßen. Mit dieser Regel können Sie den Parameter festlegen. blockedActionsPatterns (Wert „AWS Bewährte grundlegende Sicherheitsmethoden“: kms:Entschlüsseln, kms:ReEncryptFrom). Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 — Die Cloud-1-Standard-Workloads b-design-and-secure	iam-group-has-users-überprüfen	AWS Identity and Access Management (IAM) kann Ihnen helfen, die Prinzipien der geringsten Rechte und der Aufgabentrennung mit Zugriffsberechtigungen und Autorisierungen zu integrieren, indem sichergestellt wird, dass IAM-Gruppen mindestens einen Benutzer haben. Die Einteilung von Benutzern in Gruppen auf der Grundlage der ihnen zugewiesenen Berechtigungen oder ihrer Funktion ist eine Möglichkeit, das Prinzip der geringsten Berechtigung zu implementieren.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 — Die Cloud-1-Standard-Workloads b-design-and-secure	iam-inline-policy-blocked-kms-Aktionen	Stellen Sie sicher, dass ein Benutzer, eine IAM-Rolle oder eine IAM-Gruppe (AWS Identity and Access Management) nicht über eine Inline-Richtlinie verfügt, die blockierte Aktionen für alle AWS Schlüssel des Key Management Service zulässt. AWS empfiehlt, verwaltete Richtlinien anstelle von Inline-Richtlinien zu verwenden. Verwaltete Richtlinien ermöglichen Wiederverwendbarkeit, Versionsverwaltung, Rollback und Delegierung der Berechtigungsverwaltung. Mit dieser Regel können Sie den blockedActionsPatterns Parameter festlegen. (Wert „AWS Bewährte grundlegende Sicherheitsmethoden“: kms:Entschlüsseln, kms:ReEncryptFrom). Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 — Die Cloud-1-Standard-Workloads b-design-and-secure	iam-no-inline-policy-überprüfen	Stellen Sie sicher, dass ein Benutzer, eine IAM-Rolle oder eine IAM-Gruppe (AWS Identity and Access Management) nicht über eine Inline-Richtlinie zur Zugriffskontrolle auf Systeme und Ressourcen verfügt. AWS empfiehlt, verwaltete Richtlinien anstelle von Inline-Richtlinien zu verwenden . Verwaltete Richtlinien ermöglichen Wiederverwendbarkeit, Versionsverwaltung, Rollback und Delegierung der Berechtigungsverwaltung.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 b-design-and-secure — Die Cloud-1-Standard-Workloads	iam-password-policy	Die Identitäten und Anmeldeinformationen werden auf der Grundlage einer organisatorischen IAM-Passwortrichtlinie ausgestellt, verwaltet und verifiziert. Sie erfüllen oder übertreffen die Anforderungen von NIST SP 800-63 und dem Standard „Best Practices“ von Foundational Security für die Passwortstärke. AWS Mit dieser Regel können Sie optional RequireUppercaseCharacters (Wert für AWS grundlegende Sicherheitsbewährte Verfahren: wahr), RequireLowercaseCharacters (Wert für bewährte Methoden für AWS grundlegende Sicherheit: wahr), RequireSymbols (Wert für bewährte Methoden für AWS grundlegende Sicherheit: wahr), RequireNumbers (Wert für bewährte Methoden für AWS grundlegende Sicherheit: wahr), MinimumPasswordLength (Wert für bewährte Methoden für AWS grundlegende Sicherheit: 14), PasswordReusePrevention (Wert für bewährte Methoden für AWS grundlegende Sicherheit: 24) und

Kontroll-ID	AWS Config	Empfehlungen
		MaxPasswordAge (Wert für bewährte Methoden für AWS grundlegende Sicherhei t: 90) für Ihr IAM festlegen Kennwortrichtlinie. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisat ion entsprechen.
Abschnitt 4 b-design-and-secure — Die Cloud-1-S tandard-Workloads	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) kann Ihnen dabei helfen, die Prinzipien der geringsten Rechte und der Aufgabent rennung in Zugriffsberechtigu ngen und Autorisierungen zu integrieren und so zu verhindern, dass Richtlinien „Effect“: „Allow“ mit „Action“: „*“ anstelle von „Resource“: „*“ enthalten. Wenn Benutzern mehr Rechte eingeräumt werden, als für die Ausführun g einer Aufgabe erforderl ich sind, kann dies gegen das Prinzip der geringste n Berechtigung und der Aufgabentrennung verstoßen.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt b-design-and-secure 4 — Die Cloud-1-Standard-Workloads	iam-policy-no-statements-with-full-access	Stellen Sie sicher, dass IAM-Aktionen nur auf die benötigten Aktionen beschränkt sind. Wenn Benutzern mehr Rechte eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und der Aufgabentrennung verstoßen.
Abschnitt 4 — b-design-and-secure Cloud-1-Standard-Workloads	iam-root-access-key-überprüfen	Der Zugriff auf Systeme und Ressourcen kann gesteuert werden, indem überprüft wird, ob der Root-Benutzer keine Zugriffsschlüssel mit seiner AWS Identity and Access Management (IAM) -Rolle verknüpft hat. Stellen Sie sicher, dass die Root-Zugriffsschlüssel gelöscht werden. Erstellen und verwenden Sie stattdessen rollenbasierte Funktionen, AWS-Konten um das Prinzip der geringsten Funktionalität zu berücksichtigen.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 — Die Cloud-1-Standard-Workloads b-design-and-secure	iam-user-group-membership-überprüfen	AWS Identity and Access Management (IAM) kann Ihnen helfen, Zugriffsberechtigungen und Autorisierungen einzuschränken, indem sichergestellt wird, dass Benutzer Mitglieder mindestens einer Gruppe sind. Wenn Benutzern mehr Berechtigungen eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und Aufgabentrennung verstoßen.
Abschnitt 4 — Die Cloud-1-Standard-Workloads b-design-and-secure	iam-user-mfa-enabled	Aktivieren Sie diese Regel, um den Zugriff auf Ressourcen in der AWS -Cloud einzuschränken. Diese Regel stellt sicher, dass die Multi-Faktor-Authentifizierung (MFA) für alle Benutzer aktiviert ist. MFA bietet eine weitere Schutzebene zusätzlich zum Benutzernamen und Passwort. Reduzieren Sie Fälle von kompromittierten Konten, indem Sie MFA für Benutzer vorschreiben.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 — b-design-and-secure Cloud-1-Standard-Workloads	iam-user-no-policies-überprüfen	Diese Regel stellt sicher, dass AWS Identity and Access Management (IAM) -Richtlinien nur Gruppen oder Rollen zugewiesen werden, um den Zugriff auf Systeme und Ressourcen zu kontrollieren. Die Zuweisung von Berechtigungen auf Gruppen- oder Rollenebene trägt dazu bei, die Wahrscheinlichkeit zu verringern, dass eine Identität übermäßige Berechtigungen erhält oder beibehält.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 b-design-and-secure — Die Cloud-1-Standard-Workloads	iam-user-unused-credentials-überprüfen	AWS Identity and Access Management (IAM) kann Ihnen bei Zugriffsberechtigungen und Autorisierungen helfen, indem es nach IAM-Passwörtern und Zugriffsschlüsseln sucht, die für einen bestimmten Zeitraum nicht verwendet wurden. Wenn ungenutzte Anmeldeinformationen identifiziert werden, müssen Sie sie deaktivieren und/oder entfernen, da dies gegen das Prinzip der geringsten Berechtigung verstoßen könnte. Für diese Regel müssen Sie einen Wert für das maxCredentialUsage Alter festlegen (Standardkonfiguration: 90). Der tatsächliche Wert muss den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 b-design-and-secure — Die Cloud-1-Standard-Workloads	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) Security Groups können bei der Verwaltung des Netzwerkzugriffs helfen, indem sie eine statusbehaftete Filterung von eingehendem und ausgehendem Netzwerkverkehr zu Ressourcen bereitstellen. AWS Wenn Sie eingehenden (oder entfernten) Datenverkehr von 0.0.0.0/0 bis Port 22 auf Ihren Ressourcen nicht zulassen, können Sie den Remote-Zugriff einschränken.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 — Die Cloud-1-Standard-Workloads b-design-and-secure	ec2- instances-in-vpc	Stellen Sie Amazon Elastic Compute Cloud (Amazon EC2) -Instances innerhalb einer Amazon Virtual Private Cloud (Amazon VPC) bereit, um eine sichere Kommunikation zwischen einer Instance und anderen Services innerhalb der Amazon VPC zu ermöglichen, ohne dass ein Internet-Gateway, ein NAT-Gerät oder eine VPN-Verbindung erforderlich ist. Der gesamte Datenverkehr bleibt sicher in der AWS Cloud. Domains, die sich innerhalb einer VPC befinden, verfügen aufgrund ihrer logischen Isolierung im Vergleich zu Domains mit öffentlichen Endpunkten über eine zusätzliche Sicherheitsebene. Weisen Sie EC2 Amazon-Instances einer Amazon-VPC zu, um den Zugriff ordnungsgemäß zu verwalten.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 b-design-and-secure — Cloud-1-Standard-Workloads	internet-gateway-authorized-vpc-nur	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Internet-Gateways nur mit autorisierter Amazon Virtual Private Cloud (Amazon VPC) verbunden sind. Internet-Gateways ermöglichen den bidirekti onalen Internetzugang zur und von der Amazon VPC, was möglicherweise zu einem unbefugten Zugriff auf Amazon-VPC-Ressourcen führen kann.
Abschnitt 4 — Die Cloud-1-S tandard-Workloads b-design-and-secure	lambda-function-public-acce ss-verboten	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherste llen, dass AWS Lambda-Funktionen nicht öffentlich zugänglich sind. Der öffentlic he Zugriff kann möglicher weise die Verfügbarkeit von Ressourcen beeinträchtigen.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 b-design-and-secure — Die Cloud-1-Standard-Workloads	lambda-inside-vpc	Stellen Sie AWS Lambda-Funktionen in einer Amazon Virtual Private Cloud (Amazon VPC) bereit, um eine sichere Kommunikation zwischen einer Funktion und anderen Diensten innerhalb der Amazon VPC zu gewährleisten. Bei dieser Konfiguration sind kein Internet-Gateway, kein NAT-Gerät und keine VPN-Verbindung erforderlich. Der gesamte Datenverkehr bleibt sicher in der Cloud. AWS Domains, die sich innerhalb einer VPC befinden, verfügen aufgrund ihrer logischen Isolierung im Vergleich zu Domains mit öffentlichen Endpunkten über eine zusätzliche Sicherheitsebene. Um den Zugriff ordnungsgemäß zu verwalten, sollten AWS Lambda-Funktionen einer VPC zugewiesen werden.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 — Die Cloud-1-Standard-Workloads b-design-and-secure	mfa-enabled-for-iam-Konsolenzugriff	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass MFA für alle AWS Identity and Access Management (IAM) -Benutzer aktiviert ist, die über ein Konsolenkennwort verfügen. MFA sorgt für eine weitere Schutzebene zusätzlich zu den Anmeldeinformationen. Indem Sie MFA für Benutzer vorschreiben, können Sie Fälle kompromittierter Konten reduzieren und verhindern, dass unbefugte Benutzer auf vertrauliche Daten zugreifen.
Abschnitt 4 — Die Cloud-1-Standard-Workloads b-design-and-secure	no-unrestricted-route-to-igw	Stellen Sie sicher, dass EC2 Amazon-Routentabellen keine uneingeschränkten Routen zu einem Internet-Gateway enthalten. Durch das Entfernen oder Beschränken des Internetzugangs für Workloads innerhalb von Amazon VPCs können unbeabsichtigte Zugriffe in Ihrer Umgebung reduziert werden.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 — Die Cloud-1-Standard-Workloads b-design-and-secure	rds-instance-public-access-überprüfen	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Relational Database Service (Amazon RDS) -Instances nicht öffentlich sind. Amazon-RDS-Datenbank-Instances können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.
Abschnitt 4 b-design-and-secure — Cloud-1-Standard-Workloads	redshift-cluster-public-access-überprüfen	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Redshift Redshift-Cluster nicht öffentlich sind. Amazon-Redshift-Cluster können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 b-design-and-secure — Die Cloud-1-Standard-Workloads	redshift-enhanced-vpc-routing-aktiviert	Mit Enhanced-VPC-Routing wird erzwungen, dass der gesamte COPY- und UNLOAD-Datenverkehr zwischen Ihrem Cluster und Datenrepositorys über Ihre Amazon VPC erfolgt. Anschließend können Sie VPC-Features wie Sicherheitsgruppen und Netzwerkzugriffskontrollisten verwenden, um den Netzwerkverkehr zu schützen. Sie können auch VPC-Flow-Protokolle verwenden, um den Netzwerkverkehr zu überwachen.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 b-design-and-secure — Die Cloud-1-Standard-Workloads	restricted-common-ports	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass gemeinsame Ports für Amazon Elastic Compute Cloud (Amazon EC2) - Sicherheitsgruppen eingeschränkt sind. Wenn der Zugriff auf Ports nicht auf vertrauenswürdige Quellen beschränkt wird, kann dies zu Angriffen auf die Verfügbarkeit, Integrität und Vertraulichkeit von Systemen führen. Mit dieser Regel können Sie optional die Parameter blockedPort1–blockedPort5 festlegen (Standardkonfigurationen: 20, 21, 3389, 3306, 4333). Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 b-design-and-secure — Die Cloud-1-Standard-Workloads	root-account-hardware-mfa-aktiviert	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Hardware-MFA für den Root-Benutzer aktiviert ist. Der Stammbenutzer ist der AWS-Konto-Benutzer mit den meisten Berechtigungen. MFA sorgt für eine weitere Schutzebene zusätzlich zu den Anmeldeinformationen. Indem Sie MFA für den Root-Benutzer vorschreiben, können Sie die Anzahl AWS-Konten kompromittierter Benutzer reduzieren.
Abschnitt 4 — Die Cloud-1-Standard-Workloads b-design-and-secure	root-account-mfa-enabled	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass MFA für den Root-Benutzer aktiviert ist. Der Stammbenutzer ist der AWS-Konto-Benutzer mit den meisten Berechtigungen. MFA bietet eine weitere Schutzebene zusätzlich zum Benutzernamen und Passwort. Indem Sie MFA für den Root-Benutzer vorschreiben, können Sie die Anzahl AWS-Konten kompromittierter Benutzer reduzieren.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 — Die Cloud-1-Standard-Workloads b-design-and-secure	s3- -Blöcke — periodisch account-level-public-access	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Simple Storage Service (Amazon S3) -Buckets nicht öffentlich zugänglich sind. Diese Regel trägt dazu bei, sensible Daten vor unbefugten Remote-Benutzern zu schützen, indem sie den öffentlichen Zugriff verhindert. Mit dieser Regel können Sie optional die Parameter ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) und restrictPublicBuckets Parameter (Config Default: True) festlegen. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 b-design-and-secure — Die Cloud-1-Standard-Workloads	s3- bucket-public-read-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie nur autorisierten Benutzern, Prozessen und Geräten Zugriff auf Amazon Simple Storage Service (Amazon S3) -Buckets gewähren. Die Verwaltung des Zugriffs sollte mit der Klassifizierung der Daten übereinstimmen.
Abschnitt 4 b-design-and-secure — Die Cloud-1-Standard-Workloads	s3- bucket-public-write-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie nur autorisierten Benutzern, Prozessen und Geräten Zugriff auf Amazon Simple Storage Service (Amazon S3) -Buckets gewähren. Die Verwaltung des Zugriffs sollte mit der Klassifizierung der Daten übereinstimmen.
Abschnitt 4 b-design-and-secure — Die Cloud-1-Standard-Workloads	sagemaker-notebook-no-direct-Internetzugang	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass SageMaker Amazon-Notebooks keinen direkten Internetzugang zulassen. Indem Sie direkten Internetzugang blockieren, vermeiden Sie, dass unbefugte Benutzer auf sensible Daten zugreifen.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 b-design-and-secure — Die Cloud-1-Standard-Workloads	ssm-document-not-public	Stellen Sie sicher, dass AWS Systems Manager (SSM) - Dokumente nicht öffentlich sind, da dies einen unbeabsichtigten Zugriff auf Ihre SSM-Dokumente ermöglichen kann. Ein öffentliches SSM-Dokument kann Informationen über Ihr Konto, Ihre Ressourcen und internen Prozesse preisgeben.
b-design-and-secureAbschnitt 4 — Die Cloud-1-Standard-Workloads	vpc-default-security-group-geschlossen	Sicherheitsgruppen von Amazon Elastic Compute Cloud (Amazon EC2) können bei der Verwaltung des Netzwerkzugriffs helfen, indem sie eine statusbehaftete Filterung des ein- und ausgehenden Netzwerkverkehrs zu Ressourcen bereitstellen. AWS Die Beschränkung des gesamten Datenverkehrs auf die Standardsicherheitsgruppe hilft dabei, den Fernzugriff auf Ihre Ressourcen einzuschränken. AWS

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 — Die Cloud-1-Standard-Workloads b-design-and-secure	vpc-sg-open-only-to-authorized-ports	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass gemeinsame Ports für Amazon Elastic Compute Cloud (Amazon EC2) - Sicherheitsgruppen eingeschränkt sind. Wenn der Zugriff auf Ports nicht auf vertrauenswürdige Quellen beschränkt wird, kann dies zu Angriffen auf die Verfügbarkeit, Integrität und Vertraulichkeit von Systemen führen. Durch die Beschränkung des Zugriffs auf Ressourcen innerhalb einer Sicherheitsgruppe aus dem Internet (0.0.0.0/0) kann der Remote-Zugriff auf interne Systeme gesteuert werden.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 b-design-and-secure — Die Cloud-1-Standard-Workloads	ecs-containers-nonprivileged	Um die Implementierung des Prinzips der geringsten Berechtigung zu unterstützen, dürfen in Amazon Elastic Container Service (Amazon ECS)-Aufgabendefinitionen keine erhöhten Berechtigungen aktiviert sein. Wenn dieser Parameter den Wert „true“ aufweist, erhält der Container erhöhte Berechtigungen auf der Host-Container-Instance (ähnlich wie der Root-Benutzer).
Abschnitt 4 — b-design-and-secure Cloud-1-Standard-Workloads	ecs-containers-readonly-access	Die Aktivierung des schreibgeschützten Zugriffs auf Amazon Elastic Container Service (ECS)-Container kann dazu beitragen, das Prinzip der geringsten Berechtigung einzuhalten. Diese Option kann Angriffsvektoren reduzieren, da das Dateisystem der Container-Instance nur geändert werden kann, wenn es über ausdrückliche Lese- und Schreibberechtigungen verfügt.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 — b-design-and-secure Cloud-1-Standard-Workloads	opensearch-access-control-enabled	Stellen Sie sicher, dass eine differenzierte Zugriffskontrolle für Ihre Amazon OpenSearch Service-Domains aktiviert ist. Eine differenzierte Zugriffskontrolle bietet erweiterte Autorisierungsmechanismen, um den Zugriff auf Amazon Service-Domains mit den geringsten Rechten zu erreichen. OpenSearch Es ermöglicht eine rollenbasierte Zugriffskontrolle auf die Domain sowie Sicherheit auf Index-, Dokument- und Feldebene, Unterstützung für OpenSearch Service-Dashboards, Mehrmandantenfähigkeit und HTTP-Basisauthentifizierung für Service und Kibana. OpenSearch
Abschnitt 4 — Die Cloud-1-Standard-Workloads b-design-and-secure	s3- verboten bucket-level-public-access	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Simple Storage Service (Amazon S3) -Buckets nicht öffentlich zugänglich sind. Diese Regel trägt dazu bei, sensible Daten vor unbefugten Remote-Benutzern zu schützen, indem sie den öffentlichen Zugriff auf Bucket-Ebene verhindert.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 b-design-and-secure — Die Cloud-1-Standard-Workloads	subnet-auto-assign-public-ip-deaktiviert	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon Virtual Private Cloud (VPC) -Subnetzen nicht automatisch eine öffentliche IP-Adresse zugewiesen wird. Amazon Elastic Compute Cloud (EC2) -Instances, die in Subnetzen gestartet werden, in denen dieses Attribut aktiviert ist, haben ihrer primären Netzwerkschnittstelle eine öffentliche IP-Adresse zugewiesen.
Abschnitt 4 b-design-and-secure — Die Cloud-2-Standard-Workloads	cloudtrail-security-trail-enabled	Diese Regel trägt dazu bei, die Verwendung der AWS empfohlenen bewährten Sicherheitsmethoden für sicherzustellen, indem geprüft wird AWS CloudTrail, ob mehrere Einstellungen aktiviert sind. Dazu gehören die Verwendung von Protokoll verschlüsselung, Protokoll validierung und Aktivierung AWS CloudTrail in mehreren Regionen.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 b-design-and-secure — Die Cloud — 2 — Standard-Workloads	ec2-manager instance-managed-by-systems	Eine Bestandsaufnahme der Softwareplattformen und Anwendungen innerhalb des Unternehmens ist möglich, indem Amazon Elastic Compute Cloud (Amazon EC2) -Instances mit AWS Systems Manager verwaltet werden. Verwenden Sie AWS Systems Manager, um detaillierte Systemkonfigurationen, Betriebssystem-Patch-Levels, Namen und Typ der Dienste, Softwareinstallationen, Anwendungsname, Herausgeber und Version sowie andere Details zu Ihrer Umgebung bereitzustellen.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 b-design-and-secure — Die Cloud-2-Standard-Workloads	ec2-prüfen managedinstance-association-compliance-status	Verwenden Sie AWS Systems Manager Associations, um bei der Inventarisierung von Softwareplattformen und Anwendungen innerhalb eines Unternehmens zu helfen. AWS Systems Manager weist Ihren verwalteten Instances einen Konfigurationsstatus zu und ermöglicht es Ihnen, Basiswerte für Betriebssystem-Patch-Levels, Softwareinstallationen, Anwendungskonfigurationen und andere Details zu Ihrer Umgebung festzulegen.
Abschnitt 4 b-design-and-secure — Die Cloud — 2 — Standard-Workloads	ec2-prüfen managedinstance-patch-compliance-status	Aktivieren Sie diese Regel, um bei der Identifizierung und Dokumentation von Sicherheitslücken in Amazon Elastic Compute Cloud (Amazon EC2) zu helfen. Die Regel prüft, ob die EC2 Amazon-Instance die Patch-Konformität im AWS Systems Manager gemäß den Richtlinien und Verfahren Ihrer Organisation einhält.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 b-design-and-secure — Cloud-2-Standard-Workloads	redshift-cluster-maintenancesettings-check	Diese Regel stellt sicher, dass Amazon-Redshift-Cluster die bevorzugten Einstellungen für Ihre Organisation haben. Insbesondere sorgt sie dafür, dass Cluster bevorzugte Wartungsfenster und automatisierte Aufbewahrungsfristen für Snapshots für die Datenbank haben. Für diese Regel müssen Sie die festlegen. allowVersionUpgrade Der Standardwert ist „true“. Außerdem können Sie optional den Zeitraum preferredMaintenanceWindow (der Standardwert ist sa: 16:00 -sa: 16:30) und den automatedSnapshotRetention Zeitraum (der Standardwert ist 1) festlegen. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 — Die Cloud-3-Standard-Workloads b-design-and-secure	autoscaling-group-elb-healthcheck-erforderlich	Die Elastic Load Balancer (ELB) -Zustandsprüfungen für Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling Scaling-Gruppen unterstützen die Aufrechterhaltung einer angemessenen Kapazität und Verfügbarkeit. Der Load Balancer sendet regelmäßig Pings, versucht Verbindungen herzustellen oder sendet Anfragen, um den Zustand der EC2 Amazon-Instances in einer Gruppe mit auto-scaling zu testen. Wenn eine Instance nicht zurückmeldet, wird der Traffic an eine neue EC2 Amazon-Instance gesendet.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 b-design-and-secure — Die Cloud-3-Standard-Workloads	dynamodb-autoscaling-enabled	Amazon DynamoDB Auto Scaling verwendet den AWS Application Auto Scaling-Service, um die bereitgestellte Durchsatzkapazität so anzupassen, dass sie automatisch auf tatsächliche Verkehrsmuster reagiert. Auf diese Weise kann eine Tabelle oder ein globaler sekundärer Index die bereitgestellte Lese-/Schreibkapazität erhöhen, um plötzliche Erhöhungen des Datenverkehrs ohne Drosselung zu bewältigen.
b-design-and-secureAbschnitt 4 — Die Cloud-3-Standard-Workloads	ec2- instance-detailed-monitoring-enabled	Aktivieren Sie diese Regel, um die Amazon Elastic Compute Cloud (Amazon EC2) -Instance-Überwachung auf der EC2 Amazon-Konsole zu verbessern, in der Monitoring-Diagramme mit einem Zeitraum von 1 Minute für die Instance angezeigt werden.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 b-design-and-secure — Die Cloud-3-S tandard-Workloads	elb-cross-zone-load-Balancing aktiviert	Aktivieren Sie zonenüber greifendes Load Balancing für Ihre Elastic Load Balancer (ELBs), um eine angemesse ne Kapazität und Verfügbar keit aufrechtzuerhalten. Zonenübergreifendes Load Balancing reduziert die Notwendigkeit, die gleiche Anzahl von Instances in jeder aktivierten Availability Zone aufrechtzuerhalten. Es verbessert auch die Fähigkeit Ihrer Anwendung, den Verlust einer oder mehrerer Instances zu bewältigen.
Abschnitt 4 — Die Cloud-3-S tandard-Workloads b-design-and-secure	elb-deletion-protection-ena bled	Diese Regel sorgt dafür, dass der Löschschutz für Elastic Load Balancing aktiviert ist. Verwenden Sie diese Funktion, um zu verhinder n, dass Ihr Load Balancer versehentlich oder böswillig gelöscht wird, was zum Verlust der Verfügbarkeit Ihrer Anwendungen führen kann.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 — Die b-design-and-secure Cloud-3-Standard-Workloads	rds-enhanced-monitoring-enabled	Aktivieren Sie Amazon Relational Database Service (Amazon RDS), um die Verfügbarkeit von Amazon RDS zu überwachen. Dies bietet einen detaillierten Einblick in den Zustand Ihrer Amazon-RDS-Datenbank-Instances. Wenn der Amazon-RDS-Speicher mehr als ein zugrunde liegendes physisches Gerät verwendet, erfasst Enhanced Monitoring die Daten für jedes Gerät. Wenn die Datenbank-Instance von Amazon RDS in einer Multi-AZ-Bereitstellung ausgeführt wird, werden außerdem die Daten für jedes Gerät auf dem sekundären Host sowie die Metriken des sekundären Hosts erfasst.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 — Die b-design-and-secure Cloud-3-Standard-Workloads	rds-multi-az-support	Die Multi-AZ-Unterstützung in Amazon Relational Database Service (Amazon RDS) bietet eine verbesserte Verfügbar keit und Beständigkeit von Datenbank-Instances. Wenn Sie eine Multi-AZ-Datenbank-Instance bereitstellen, erstellt Amazon RDS automatisch eine primäre Datenbank-Instance und repliziert die Daten synchron auf eine Standby-Instance in einer anderen Availability Zone. Jede Availability Zone läuft auf einer eigenen, physisch getrennten, unabhängigen Infrastruktur und ist auf eine hohe Verfügbarkeit ausgelegt . Im Falle eines Infrastru kturausfalls führt Amazon RDS einen automatischen Failover zum Standby-Modus durch, sodass Sie den Datenbank betrieb wieder aufnehmen können, sobald der Failover abgeschlossen ist.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 — Die b-design-and-secure Cloud-3-Standard-Workloads	rds-cluster-multi-az-aktiviert	Die Multi-AZ-Unterstützung in Amazon Relational Database Service (Amazon RDS) bietet eine verbesserte Verfügbar keit und Beständigkeit von Datenbank-Instances. Wenn Sie eine Multi-AZ-Datenbank-Instance bereitstellen, erstellt Amazon RDS automatisch eine primäre Datenbank-Instance und repliziert die Daten synchron auf eine Standby-Instance in einer anderen Availability Zone. Jede Availability Zone läuft auf einer eigenen, physisch getrennten, unabhängigen Infrastruktur und ist auf eine hohe Verfügbarkeit ausgelegt . Im Falle eines Infrastru kturausfalls führt Amazon RDS einen automatischen Failover zum Standby-Modus durch, sodass Sie den Datenbank betrieb wieder aufnehmen können, sobald der Failover abgeschlossen ist.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 b-design-and-secure — die Cloud-3-Standard-Workloads	beanstalk-enhanced-health-reporting-aktiviert	AWS Die verbesserte Zustandsberichterstattung von Elastic Beanstalk ermöglicht eine schnellere Reaktion auf Veränderungen im Zustand der zugrunde liegenden Infrastruktur. Diese Änderungen könnten zu einer mangelnden Verfügbarkeit der Anwendung führen. Die erweiterten Zustandsberichte von Elastic Beanstalk bieten eine Statusbeschreibung, um den Schweregrad der identifizierten Probleme einzuschätzen und mögliche Ursachen zu identifizieren, die untersucht werden müssen.
Abschnitt 4 — Cloud-4-Standard-Workloads b-design-and-secure	alb-waf-enabled	Stellen Sie sicher, dass AWS WAF auf Elastic Load Balancers (ELB) aktiviert ist, um Webanwendungen zu schützen. Eine WAF trägt zum Schutz Ihrer Webanwendungen oder APIs vor gängigen Web-Exploits bei. Diese Web-Exploits können sich auf die Verfügbarkeit auswirken, die Sicherheit gefährden oder übermäßige Ressourcen in Ihrer Umgebung verbrauchen.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 — Die Cloud-4-Standard-Workloads b-design-and-secure	api-gw-associated-with-WAF	AWS Mit WAF können Sie eine Reihe von Regeln (als Web Access Control List (Web ACL) bezeichnet) konfigurieren, die Webanfragen auf der Grundlage von anpassbaren Websicherheitsregeln und -bedingungen, die Sie definieren, zulassen, blockieren oder zählen. Stellen Sie sicher, dass Ihre Amazon-API-Gateway-Stufe mit einer WAF-Web-ACL verknüpft ist, um sie vor böswilligen Angriffen zu schützen.
Abschnitt 4 b-design-and-secure — Cloud-4-Standard-Workloads	autoscaling-launch-config-public-ip-deaktiviert	Wenn Sie Ihre Netzwerkschnittstellen mit einer öffentlichen IP-Adresse konfigurieren, sind die diesen Netzwerkschnittstellen zugehörigen Ressourcen über das Internet erreichbar. EC2 Ressourcen sollten nicht öffentlich zugänglich sein, da dies einen unbeabsichtigten Zugriff auf Ihre Anwendungen oder Server ermöglichen kann.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 b-design-and-secure — Die Cloud-4-S tandard-Workloads	ec2- instance-no-public-ip	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon Elastic Compute Cloud (Amazon EC2) -Instances nicht öffentlich zugänglich sind. EC2Amazon-Instances können vertrauliche Informati onen enthalten, und für solche Konten ist eine Zugriffsk ontrolle erforderlich.
Abschnitt 4 b-design-and-secure — Cloud-4-Standard-Workloads	ec2- instance-profile-attached	EC2 Instanzprofile übergeben eine IAM-Rolle an eine Instanz EC2 . Das Anhängen eines Instance-Profils an Ihre Instances kann bei der Implementierung von geringsten Berechtigungen und der Berechtigungsverwa ltung helfen.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 b-design-and-secure — Cloud-4-Standard-Workloads	ecs-task-definition-user-for-host-mode-check	Wenn für eine Aufgabend efinition erhöhte Berechtig ungen gelten, liegt das daran, dass der Kunde diesen Konfigurationen ausdrücklich zugestimmt hat. Diese Kontrolle prüft, ob eine unerwartete Berechtig ungseskalation vorliegt, wenn für eine Aufgabendefinition das Host-Netzwerk aktiviert ist, die Kunden aber keine erhöhten Berechtigungen aktiviert haben.
Abschnitt 4 — Die b-design-and-secure Cloud-4-Standard-Workloads	elasticsearch-in-vpc-only	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass sich Amazon OpenSearch OpenSearch Service (Service) -Domains innerhalb einer Amazon Virtual Private Cloud (Amazon VPC) befinden. Eine OpenSearch Service-D omain innerhalb einer Amazon VPC ermöglicht die sichere Kommunikation zwischen OpenSearch Service und anderen Services innerhalb der Amazon VPC, ohne dass ein Internet-Gateway, ein NAT-Gerät oder eine VPN-Verbindung erforderlich ist.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 — Die Cloud-4-Standard-Workloads b-design-and-secure	emr-kerberos-enabled	Die Zugriffsberechtigungen und -autorisierungen können verwaltet und nach den Prinzipien der geringsten Berechtigung und Aufgabentrennung integriert werden, indem Kerberos für Amazon-EMR-Cluster aktiviert wird. In Kerberos werden Services und Benutzer, die sich authentifizieren müssen, als Prinzipale bezeichnet. Prinzipale befinden sich in einem Kerberos-Bereich. Innerhalb dieses Bereichs wird ein Kerberos-Server als Key Distribution Center (KDC) bezeichnet. Über diesen Server können sich Prinzipale authentifizieren. Die Authentifizierung im KDC erfolgt durch die Ausstellung von Authentifizierungstickets. Das KDC unterhält eine Datenbank der Prinzipale in seinem Bereich mit ihren Passwörtern und anderen administrativen Informationen zu jedem Prinzipal.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 — Die b-design-and-secure Cloud-4-Standard-Workloads	emr-master-no-public-ip	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon EMR-Cluster-Masterknoten nicht öffentlich zugänglich sind. Amazon-EMR-Cluster-Hauptknoten können vertrauliche Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.
Abschnitt 4 b-design-and-secure — Cloud-4-Standard-Workloads	guardduty-enabled-centralized	Amazon GuardDuty kann mithilfe von Threat Intelligence Feeds helfen, potenzielle Cybersicherheitsereignisse zu überwachen und zu erkennen. Dazu gehören Listen mit bösartigen IPs und maschinellen Lernmethoden zur Identifizierung unerwarteter, nicht autorisierter und bösartiger Aktivitäten in Ihrer AWS Cloud-Umgebung.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 b-design-and-secure — Die Cloud-4-S tandard-Workloads	iam-customer-policy-blocked-kms-Aktionen	AWS Identity and Access Management (IAM) kann Ihnen helfen, die Prinzipien der geringsten Rechte und der Aufgabentrennung in Zugriffsberechtigungen und Autorisierungen zu integrier en und so zu verhindern, dass Richtlinien blockierte Aktionen für alle AWS Schlüssel des Key Management Service enthalten. Wenn Benutzer mehr Rechte haben, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und Aufgabentrennung verstoßen . Mit dieser Regel können Sie den Parameter festlegen. blockedActionsPatterns (Wert „AWS Bewährte grundlegende Sicherheitsmethoden“: kms: Entschlüsseln, kms:ReEnc ryptFrom). Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprech en.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 — Cloud-4-Standard-Workloads b-design-and-secure	iam-group-has-users-überprüfen	AWS Identity and Access Management (IAM) kann Ihnen helfen, die Prinzipien der geringsten Rechte und der Aufgabentrennung mit Zugriffsberechtigungen und Autorisierungen zu integrieren, indem sichergestellt wird, dass IAM-Gruppen mindestens einen Benutzer haben. Die Einteilung von Benutzern in Gruppen auf der Grundlage der ihnen zugewiesenen Berechtigungen oder ihrer Funktion ist eine Möglichkeit, das Prinzip der geringsten Berechtigung zu implementieren.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 — Die Cloud-4-Standard-Workloads b-design-and-secure	iam-inline-policy-blocked-kms-Aktionen	Stellen Sie sicher, dass ein Benutzer, eine IAM-Rolle oder eine IAM-Gruppe (AWS Identity and Access Management) nicht über eine Inline-Richtlinie verfügt, die blockierte Aktionen für alle AWS Schlüssel des Key Management Service zulässt. AWS empfiehlt, verwaltete Richtlinien anstelle von Inline-Richtlinien zu verwenden. Verwaltete Richtlinien ermöglichen Wiederverwendbarkeit, Versionsverwaltung, Rollback und Delegierung der Berechtigungsverwaltung. Mit dieser Regel können Sie den blockedActionsPatterns Parameter festlegen. (Wert „AWS Bewährte grundlegende Sicherheitsmethoden“: kms:Entschlüsseln, kms:ReEncryptFrom). Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 — Cloud-4-Standard-Workloads b-design-and-secure	iam-password-policy	Die Identitäten und Anmeldeinformationen werden auf der Grundlage einer organisatorischen IAM-Passwortrichtlinie ausgestellt, verwaltet und verifiziert. Sie erfüllen oder übertreffen die Anforderungen von NIST SP 800-63 und dem Standard „Best Practices“ von Foundational Security für die Passwortstärke. AWS Mit dieser Regel können Sie optional RequireUppercaseCharacters (Wert für AWS grundlegende Sicherheitsbewährte Verfahren: wahr), RequireLowercaseCharacters (Wert für bewährte Methoden für AWS grundlegende Sicherheit: wahr), RequireSymbols (Wert für bewährte Methoden für AWS grundlegende Sicherheit: wahr), RequireNumbers (Wert für bewährte Methoden für AWS grundlegende Sicherheit: wahr), MinimumPasswordLength (Wert für bewährte Methoden für AWS grundlegende Sicherheit: 14), PasswordReusePrevention (Wert für bewährte Methoden für AWS grundlegende Sicherheit: 24) und

Kontroll-ID	AWS Config	Empfehlungen
		MaxPasswordAge (Wert für bewährte Methoden für AWS grundlegende Sicherhei t: 90) für Ihr IAM festlegen Kennwortrichtlinie. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisat ion entsprechen.
Abschnitt 4 b-design-and-secure — Die Cloud — 4-Standard-Workloads	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) kann Ihnen dabei helfen, die Prinzipien der geringsten Rechte und der Aufgabent rennung in Zugriffsberechtigu ngen und Autorisierungen zu integrieren und so zu verhindern, dass Richtlinien „Effect“: „Allow“ mit „Action“: „*“ anstelle von „Resource“: „*“ enthalten. Wenn Benutzern mehr Rechte eingeräumt werden, als für die Ausführun g einer Aufgabe erforderl ich sind, kann dies gegen das Prinzip der geringste n Berechtigung und der Aufgabentrennung verstoßen.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt b-design-and-secure 4 — Die Cloud-4-Standard-Workloads	iam-policy-no-statements-with-full-access	Stellen Sie sicher, dass IAM-Aktionen nur auf die benötigten Aktionen beschränkt sind. Wenn Benutzern mehr Rechte eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und der Aufgabentrennung verstoßen.
Abschnitt 4 — Die b-design-and-secure Cloud-4-Standard-Workloads	iam-root-access-key-überprüfen	Der Zugriff auf Systeme und Ressourcen kann gesteuert werden, indem überprüft wird, ob der Root-Benutzer keine Zugriffsschlüssel mit seiner AWS Identity and Access Management (IAM) -Rolle verknüpft hat. Stellen Sie sicher, dass die Root-Zugriffsschlüssel gelöscht werden. Erstellen und verwenden Sie stattdessen rollenbasierte Funktionen, AWS-Konten um das Prinzip der geringsten Funktionalität zu berücksichtigen.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 — Cloud-4-Standard-Workloads b-design-and-secure	iam-user-group-membership-überprüfen	AWS Identity and Access Management (IAM) kann Ihnen helfen, Zugriffsberechtigungen und Autorisierungen einzuschränken, indem sichergestellt wird, dass Benutzer Mitglieder mindestens einer Gruppe sind. Wenn Benutzern mehr Berechtigungen eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und Aufgabentrennung verstoßen.
Abschnitt 4 — Die Cloud-4-Standard-Workloads b-design-and-secure	iam-user-mfa-enabled	Aktivieren Sie diese Regel, um den Zugriff auf Ressourcen in der AWS -Cloud einzuschränken. Diese Regel stellt sicher, dass die Multi-Faktor-Authentifizierung (MFA) für alle Benutzer aktiviert ist. MFA bietet eine weitere Schutzebene zusätzlich zum Benutzernamen und Passwort. Reduzieren Sie Fälle von kompromittierten Konten, indem Sie MFA für Benutzer vorschreiben.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 — Die b-design-and-secure Cloud-4-Standard-Workloads	iam-user-no-policies-überprüfen	Diese Regel stellt sicher, dass AWS Identity and Access Management (IAM) -Richtlinien nur Gruppen oder Rollen zugewiesen werden, um den Zugriff auf Systeme und Ressourcen zu kontrollieren. Die Zuweisung von Berechtigungen auf Gruppen- oder Rollenebene trägt dazu bei, die Wahrscheinlichkeit zu verringern, dass eine Identität übermäßige Berechtigungen erhält oder beibehält.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 b-design-and-secure — Cloud-4-Standard-Workloads	iam-user-unused-credentials-überprüfen	AWS Identity and Access Management (IAM) kann Ihnen bei Zugriffsberechtigungen und Autorisierungen helfen, indem es nach IAM-Passwörtern und Zugriffsschlüsseln sucht, die für einen bestimmten Zeitraum nicht verwendet wurden. Wenn ungenutzte Anmeldeinformationen identifiziert werden, müssen Sie sie deaktivieren und/oder entfernen, da dies gegen das Prinzip der geringsten Berechtigung verstoßen könnte. Für diese Regel müssen Sie einen Wert für das maxCredentialUsage Alter festlegen (Standardkonfiguration: 90). Der tatsächliche Wert muss den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 b-design-and-secure — Die Cloud-4-S tandard-Workloads	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) Security Groups können bei der Verwaltung des Netzwerkz ugriffs helfen, indem sie eine statusbehaftete Filterung von eingehendem und ausgehend em Netzwerkverkehr zu Ressourcen bereitstellen. AWS Wenn Sie eingehenden (oder entfernten) Datenverk ehr von 0.0.0.0/0 bis Port 22 auf Ihren Ressourcen nicht zulassen, können Sie den Remote-Zugriff einschränken.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 — Die Cloud-4-Standard-Workloads b-design-and-secure	ec2- instances-in-vpc	Stellen Sie Amazon Elastic Compute Cloud (Amazon EC2) -Instances innerhalb einer Amazon Virtual Private Cloud (Amazon VPC) bereit, um eine sichere Kommunikation zwischen einer Instance und anderen Services innerhalb der Amazon VPC zu ermöglichen, ohne dass ein Internet-Gateway, ein NAT-Gerät oder eine VPN-Verbindung erforderlich ist. Der gesamte Datenverkehr bleibt sicher in der AWS Cloud. Domains, die sich innerhalb einer VPC befinden, verfügen aufgrund ihrer logischen Isolierung im Vergleich zu Domains mit öffentlichen Endpunkten über eine zusätzliche Sicherheitsebene. Weisen Sie EC2 Amazon-Instances einer Amazon-VPC zu, um den Zugriff ordnungsgemäß zu verwalten.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 b-design-and-secure — Cloud-4-Standard-Workloads	internet-gateway-authorized-vpc-nur	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Internet-Gateways nur mit autorisierter Amazon Virtual Private Cloud (Amazon VPC) verbunden sind. Internet-Gateways ermöglichen den bidirekti onalen Internetzugang zur und von der Amazon VPC, was möglicherweise zu einem unbefugten Zugriff auf Amazon-VPC-Ressourcen führen kann.
Abschnitt 4 — Die Cloud-4-S tandard-Workloads b-design-and-secure	lambda-function-public-acce ss-verboten	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherste llen, dass AWS Lambda-Funktionen nicht öffentlich zugänglich sind. Der öffentlic he Zugriff kann möglicher weise die Verfügbarkeit von Ressourcen beeinträchtigen.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 b-design-and-secure — Die Cloud-4-S tandard-Workloads	lambda-inside-vpc	Stellen Sie AWS Lambda-Funktionen in einer Amazon Virtual Private Cloud (Amazon VPC) bereit, um eine sichere Kommunikation zwischen einer Funktion und anderen Diensten innerhalb der Amazon VPC zu gewährlei sten. Bei dieser Konfigura tion sind kein Internet-Gateway, kein NAT-Gerät und keine VPN-Verbindung erforderlich. Der gesamte Datenverkehr bleibt sicher in der Cloud. AWS Domains, die sich innerhalb einer VPC befinden, verfügen aufgrund ihrer logischen Isolierung im Vergleich zu Domains mit öffentlichen Endpunkten über eine zusätzliche Sicherhei tsebene. Um den Zugriff ordnungsgemäß zu verwalten , sollten AWS Lambda-Fu nktionen einer VPC zugewiese n werden.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 — Die Cloud-4-Standard-Workloads b-design-and-secure	mfa-enabled-for-iam-Konsolenzugriff	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass MFA für alle AWS Identity and Access Management (IAM) -Benutzer aktiviert ist, die über ein Konsolenkennwort verfügen. MFA sorgt für eine weitere Schutzebene zusätzlich zu den Anmeldeinformationen. Indem Sie MFA für Benutzer vorschreiben, können Sie Fälle kompromittierter Konten reduzieren und verhindern, dass unbefugte Benutzer auf vertrauliche Daten zugreifen.
Abschnitt 4 — Die Cloud-4-Standard-Workloads b-design-and-secure	no-unrestricted-route-to-igw	Stellen Sie sicher, dass EC2 Amazon-Routentabellen keine uneingeschränkten Routen zu einem Internet-Gateway enthalten. Durch das Entfernen oder Beschränken des Internetzugangs für Workloads innerhalb von Amazon VPCs können unbeabsichtigte Zugriffe in Ihrer Umgebung reduziert werden.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 — Cloud-4-S tandard-Workloads b-design-and-secure	opensearch-in-vpc-only	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass sich Amazon OpenSearch Service-Domains innerhalb einer Amazon Virtual Private Cloud (Amazon VPC) befinden. Eine Amazon OpenSearch Service-Domain innerhalb einer Amazon VPC ermöglich t die sichere Kommunika tion zwischen Amazon OpenSearch Service und anderen Services innerhalb der Amazon VPC, ohne dass ein Internet-Gateway, ein NAT-Gerät oder eine VPN-Verbindung erforderlich ist.
Abschnitt 4 — Die Cloud-4-S tandard-Workloads b-design-and-secure	rds-instance-public-access-überprüfen	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherste llen, dass Amazon Relationa l Database Service (Amazon RDS) -Instances nicht öffentlic h sind. Amazon-RDS-Datenba nk-Instances können vertrauli che Informationen enthalten und für solche Konten sind Prinzipien und Zugriffsk ontrollen erforderlich.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 b-design-and-secure — Cloud-4-Standard-Workloads	redshift-cluster-public-access-überprüfen	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Redshift Redshift-Cluster nicht öffentlich sind. Amazon-Redshift-Cluster können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.
Abschnitt 4 b-design-and-secure — Cloud-4-Standard-Workloads	restricted-common-ports	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass gemeinsame Ports für Amazon Elastic Compute Cloud (Amazon EC2) - Sicherheitsgruppen eingeschränkt sind. Wenn der Zugriff auf Ports nicht auf vertrauenswürdige Quellen beschränkt wird, kann dies zu Angriffen auf die Verfügbarkeit, Integrität und Vertraulichkeit von Systemen führen. Mit dieser Regel können Sie optional die Parameter blockedPort1–blockedPort5 festlegen (Standardkonfigurationen: 20, 21, 3389, 3306, 4333). Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 b-design-and-secure — Die Cloud-4-Standard-Workloads	root-account-hardware-mfa-aktiviert	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Hardware-MFA für den Root-Benutzer aktiviert ist. Der Stammbenutzer ist der AWS-Konto-Benutzer mit den meisten Berechtigungen. MFA sorgt für eine weitere Schutzebene zusätzlich zu den Anmeldeinformationen. Indem Sie MFA für den Root-Benutzer vorschreiben, können Sie die Anzahl AWS-Konten kompromittierter Benutzer reduzieren.
Abschnitt 4 — Cloud-4-Standard-Workloads b-design-and-secure	root-account-mfa-enabled	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass MFA für den Root-Benutzer aktiviert ist. Der Stammbenutzer ist der AWS-Konto-Benutzer mit den meisten Berechtigungen. MFA bietet eine weitere Schutzebene zusätzlich zum Benutzernamen und Passwort. Indem Sie MFA für den Root-Benutzer vorschreiben, können Sie die Anzahl AWS-Konten kompromittierter Benutzer reduzieren.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 — Cloud-4-S tandard-Workloads b-design-and-secure	s3- -Blöcke — periodisch account-level-public-access	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherste llen, dass Amazon Simple Storage Service (Amazon S3) -Buckets nicht öffentlich zugänglich sind. Diese Regel trägt dazu bei, sensible Daten vor unbefugten Remote-Benutzern zu schützen, indem sie den öffentlichen Zugriff verhindert. Mit dieser Regel können Sie optional die Parameter ignorePub licAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPubl icAcls (Config Default: True) und restrictPublicBuckets Parameter (Config Default: True) festlegen. Die tatsächli chen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 b-design-and-secure — Die Cloud-4-S tandard-Workloads	sagemaker-notebook-no-direct-Internetzugang	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass SageMaker Amazon-Notebooks keinen direkten Internetzugang zulassen. Indem Sie direkten Internetzugang blockieren, vermeiden Sie, dass unbefugte Benutzer auf sensible Daten zugreifen.
Abschnitt 4 b-design-and-secure — Die Cloud-4-S tandard-Workloads	securityhub-enabled	AWS Security Hub hilft bei der Überwachung von unbefugtem Personal, Verbindungen, Geräten und Software. AWS Security Hub aggregiert, organisiert und priorisiert die Sicherheitswarnungen oder Ergebnisse mehrerer Dienste. AWS Einige dieser Dienste sind Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer und AWS Firewall Manager sowie AWS Partnerlösungen.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 — Die Cloud-4-Standard-Workloads b-design-and-secure	vpc-default-security-group-geschlossen	Sicherheitsgruppen von Amazon Elastic Compute Cloud (Amazon EC2) können bei der Verwaltung des Netzwerkzugriffs helfen, indem sie eine statusbehaftete Filterung des ein- und ausgehenden Netzwerkverkehrs zu Ressourcen bereitstellen. AWS Die Beschränkung des gesamten Datenverkehrs auf die Standardsicherheitsgruppe hilft dabei, den Fernzugriff auf Ihre Ressourcen einzuschränken. AWS

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 — Die Cloud-4-Standard-Workloads b-design-and-secure	vpc-sg-open-only-to-authorized-ports	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass gemeinsame Ports für Amazon Elastic Compute Cloud (Amazon EC2) - Sicherheitsgruppen eingeschränkt sind. Wenn der Zugriff auf Ports nicht auf vertrauenswürdige Quellen beschränkt wird, kann dies zu Angriffen auf die Verfügbarkeit, Integrität und Vertraulichkeit von Systemen führen. Durch die Beschränkung des Zugriffs auf Ressourcen innerhalb einer Sicherheitsgruppe aus dem Internet (0.0.0.0/0) kann der Remote-Zugriff auf interne Systeme gesteuert werden.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 b-design-and-secure — Die Cloud-4-S tandard-Workloads	vpc-vpn-2-tunnels-up	Redundante Site-to-Site VPN-Tunnel können implement iert werden, um die Anforderu ngen an die Ausfallsicherheit zu erfüllen. Es verwendet zwei Tunnel, um die Konnektiv ität sicherzustellen, falls eine der Site-to-Site VPN-Verbi ndungen nicht verfügbar ist. Um sich vor einem Verbindun gsverlust zu schützen, können Sie für den Fall, dass Ihr Kunden-Gateway nicht verfügbar ist, eine zweite Site-to-Site VPN-Verbindung zu Ihrer Amazon Virtual Private Cloud (Amazon VPC) und Ihrem Virtual Private Gateway einrichten, indem Sie ein zweites Kunden-Gateway verwenden.
Abschnitt 4 b-design-and-secure — Die Cloud-4-S tandard-Workloads	s3- verboten bucket-level-publi c-access	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherste llen, dass Amazon Simple Storage Service (Amazon S3) -Buckets nicht öffentlich zugänglich sind. Diese Regel trägt dazu bei, sensible Daten vor unbefugten Remote-Be nutzern zu schützen, indem sie den öffentlichen Zugriff auf Bucket-Ebene verhindert.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 b-design-and-secure — Cloud-4-Standard-Workloads	subnet-auto-assign-public-ip-deaktiviert	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon Virtual Private Cloud (VPC) -Subnetzen nicht automatis ch eine öffentliche IP-Adress e zugewiesen wird. Amazon Elastic Compute Cloud (EC2) -Instances, die in Subnetzen gestartet werden, in denen dieses Attribut aktiviert ist, haben ihrer primären Netzwerkschnittste lle eine öffentliche IP-Adresse zugewiesen.
Abschnitt 4 b-design-and-secure — Die Cloud-5-S tandard-Workloads	acm-certificate-expiration-check	Stellen Sie sicher, dass die Netzwerkintegrität geschützt ist, indem Sie sicherstellen, dass X509-Zertifikate von ACM ausgestellt werden. AWS Diese Zertifikate müssen gültig und dürfen nicht abgelaufe n sein. Für diese Regel ist ein Wert für erforderlich daysToExpiration (Wert für bewährte AWS Grundrege ln für Sicherheit: 90). Der tatsächliche Wert muss den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 b-design-and-secure — Die Cloud — 5 Standard-Workloads	cmk-backing-key-rotation-aktiviert	Aktivieren Sie die Schlüssel rotation, um sicherzustellen, dass Schlüssel rotiert werden, sobald sie das Ende ihrer Kryptoperiode erreicht haben.
Abschnitt 4 b-design-and-secure — Die Cloud-5-Standard-Workloads	iam-customer-policy-blocked-kms-Aktionen	AWS Identity and Access Management (IAM) kann Ihnen helfen, die Prinzipien der geringsten Rechte und der Aufgabentrennung in Zugriffsberechtigungen und Autorisierungen zu integrieren und so zu verhindern, dass Richtlinien blockierte Aktionen für alle AWS Schlüssel des Key Management Service enthalten. Wenn Benutzer mehr Rechte haben, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und Aufgabentrennung verstoßen. Mit dieser Regel können Sie den Parameter festlegen. blockedActionsPatterns (Wert „AWS Bewährte grundlegende Sicherheitsmethoden“: kms: Entschlüsseln, kms:ReEncryptFrom). Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 — Die Cloud-5-Standard-Workloads b-design-and-secure	iam-inline-policy-blocked-kms-Aktionen	Stellen Sie sicher, dass ein Benutzer, eine IAM-Rolle oder eine IAM-Gruppe (AWS Identity and Access Management) nicht über eine Inline-Richtlinie verfügt, die blockierte Aktionen für alle AWS Schlüssel des Key Management Service zulässt. AWS empfiehlt, verwaltete Richtlinien anstelle von Inline-Richtlinien zu verwenden. Verwaltete Richtlinien ermöglichen Wiederverwendbarkeit, Versionsverwaltung, Rollback und Delegierung der Berechtigungsverwaltung. Mit dieser Regel können Sie den blockedActionsPatterns Parameter festlegen. (Wert „AWS Bewährte grundlegende Sicherheitsmethoden“: kms:Entschlüsseln, kms:ReEncryptFrom). Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 — Die Cloud-5-Standard-Workloads b-design-and-secure	iam-policy-no-statements-with-full-access	Stellen Sie sicher, dass IAM-Aktionen nur auf die benötigten Aktionen beschränkt sind. Wenn Benutzern mehr Rechte eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und der Aufgabentrennung verstoßen.
Abschnitt 4 — Die b-design-and-secure Cloud-5-Standard-Workloads	kms-cmk-not-scheduled-zum Löschen	Um Daten im Ruhezustand zu schützen, sollten Sie sicherstellen, dass die für den Kunden erforderlichen Masterschlüssel (CMKs) nicht im AWS Key Management Service (AWS KMS) gelöscht werden. Da Schlüssel manchmal gelöscht werden müssen, können Sie mit dieser Regel alle zu löschenden Schlüssel überprüfen, falls ein Schlüssel versehentlich zur Löschung vorgemerkt wurde.
Abschnitt 4 b-design-and-secure — Cloud-6-Standard-Workloads	alb-http-drop-invalid-Header-fähig	Stellen Sie sicher, dass Ihre Elastic Load Balancers (ELB) so konfiguriert sind, dass sie HTTP-Header löschen. Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 — Die Cloud — 6-Standard-Workloads b-design-and-secure	alb-http-to-https-Umleitung sprüfung	Um Daten während der Übertragung zu schützen, stellen Sie sicher, dass Ihr Application Load Balancer unverschlüsselte HTTP-Anfragen automatisch an HTTPS umleitet. Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.
Abschnitt 4 — Die Cloud — 6 Standard-Workloads b-design-and-secure	api-gw-cache-enabled-und verschlüsselt	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass die Verschlüsselung für den Cache Ihrer API-Gatew ay-Stufe aktiviert ist. Da für die API-Methode sensible Daten erfasst werden können, sollten Sie die Verschlüsselung von Daten im Ruhezustand aktivieren, um diese Daten zu schützen.
Abschnitt 4 — Die Cloud — 6-Standard-Workloads b-design-and-secure	cloudwatch-log-group-encryp ted	Um sensible Daten im Speicher zu schützen, stellen Sie sicher, dass die Verschlüs selung für Ihre Amazon CloudWatch Log Groups aktiviert ist.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 b-design-and-secure — Die Cloud — 6-Standard-Workloads	cloud-trail-encryption-enabled	Zum Schutz von eventuell vorhandenen sensiblen Daten sowie Daten im Ruhezusta nd müssen Sie sicherstellen, dass die Verschlüsselung für Ihre AWS CloudTrail aktiviert ist.
Abschnitt 4 — Die Cloud — 6 b-design-and-secure Standard-Workloads	dynamodb-table-encrypted-kms	Stellen Sie sicher, dass die Verschlüsselung für Ihre Amazon-DynamoDB-Tabellen aktiviert ist. Um eventuell vorhandene sensible Daten im Ruhezustand in diesen Tabellen zu schützen, müssen Sie die Verschlüsselung von Daten im Ruhezustand aktivieren. Standardmäßig werden DynamoDB-Tabellen mit einem AWS eigenen Kundenhauptschlüssel (CMK) verschlüsselt.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 — b-design-and-secure Cloud-6-Standard-Workloads	ec2- ebs-encryption-by-default	Zum Schutz von Daten im Ruhezustand müssen Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon Elastic Block Store (Amazon EBS)-Volumes aktiviert ist. Da sensible Daten auch im Ruhezustand vorhanden sein können, sollten Sie die Verschlüsselung im Ruhezustand aktivieren, um diese Daten zu schützen.
Abschnitt 4 b-design-and-secure — Die Cloud — 6 — Standard-Workloads	efs-encrypted-check	Aktivieren Sie die Verschlüsselung für Ihr Amazon Elastic File System (EFS), um eventuell vorhandene sensible Daten sowie Daten im Ruhezustand zu schützen.
Abschnitt 4 — Die Cloud — 6 b-design-and-secure Standard-Workloads	elasticsearch-encrypted-at-rest	Da sensible Daten vorhanden sein können und um Daten im Ruhezustand zu schützen, sollten Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon OpenSearch Service (OpenSearch Service) -Domains aktiviert ist.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 b-design-and-secure — Cloud-6-Standard-Workloads	elasticsearch-node-to-node-Verschlüsselungsprüfung	Stellen Sie sicher, dass die node-to-node Verschlüsselung für Amazon OpenSearch Service aktiviert ist. Node-to-nodeVerschlüsselung ermöglicht die TLS 1.2-Versc hlüsselung für die gesamte Kommunikation innerhalb der Amazon Virtual Private Cloud (Amazon VPC). Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.
Abschnitt 4 b-design-and-secure — Cloud-6-Standard-Workloads	elasticsearch-node-to-node-Verschlüsselungsprüfung	Stellen Sie sicher, dass die node-to-node Verschlüsselung für Amazon OpenSearch Service aktiviert ist. Node-to-nodeVerschlüsselung ermöglicht die TLS 1.2-Versc hlüsselung für die gesamte Kommunikation innerhalb der Amazon Virtual Private Cloud (Amazon VPC). Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 b-design-and-secure — Cloud-6-Standard-Workloads	elv 2- acm-certificate-required	Zum Schutz von eventuell vorhandenen sensiblen Daten sowie von Daten während der Übertragung muss die Verschlüsselung für Ihr Elastic Load Balancing aktiviert sein. Verwenden Sie AWS Certifica te Manager, um öffentlic he und private SSL/TLS-Z ertifikate mit AWS Diensten und internen Ressourcen zu verwalten, bereitzustellen und bereitzustellen.
Abschnitt 4 — Cloud-6-S tandard-Workloads b-design-and-secure	elb-acm-certificate-required	Zum Schutz von eventuell vorhandenen sensiblen Daten sowie von Daten während der Übertragung muss die Verschlüsselung für Ihr Elastic Load Balancing aktiviert sein. Verwenden Sie AWS Certifica te Manager, um öffentlic he und private SSL/TLS-Z ertifikate mit AWS Diensten und internen Ressourcen zu verwalten, bereitzustellen und bereitzustellen.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 — Cloud-6-Standard-Workloads b-design-and-secure	elb-tls-https-listeners-nur	Stellen Sie sicher, dass Ihre Elastic Load Balancer (ELBs) mit SSL- oder HTTPS-Listenern konfiguriert sind. Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.
Abschnitt 4 — Die Cloud — 6-Standard-Workloads b-design-and-secure	encrypted-volumes	Aktivieren Sie die Verschlüsselung für Ihre Amazon-Elastic-Block-Store (Amazon-EBS)-Volumes, um eventuell vorhandene sensible Daten sowie Daten im Ruhezustand zu schützen.
Abschnitt 4 — Die Cloud — 6 b-design-and-secure Standard-Workloads	kinesis-stream-encrypted	Aktivieren Sie die Verschlüsselung für Ihre Amazon-Kinesis-Streams, um eventuell vorhandene sensible Daten sowie Daten im Ruhezustand zu schützen.
Abschnitt 4 — Die Cloud — 6 b-design-and-secure Standard-Workloads	kinesis-stream-encrypted	Aktivieren Sie die Verschlüsselung für Ihre Amazon-Kinesis-Streams, um eventuell vorhandene sensible Daten sowie Daten im Ruhezustand zu schützen.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 — Die Cloud — 6 b-design-and-secure Standard-Workloads	opensearch-encrypted-at-rest	Da sensible Daten vorhanden sein können und um Daten im Ruhezustand zu schützen, sollten Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon OpenSearch Service-Domains aktiviert ist.
Abschnitt 4 b-design-and-secure — Cloud-6-Standard-Workloads	opensearch-node-to-node-Verschlüsselungsprüfung	Stellen Sie sicher, dass die node-to-node Verschlüsselung für Amazon OpenSearch Service aktiviert ist. Node-to-nodeVerschlüsselung ermöglicht die TLS 1.2-Verschlüsselung für die gesamte Kommunikation innerhalb der Amazon Virtual Private Cloud (Amazon VPC). Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.
Abschnitt 4 b-design-and-secure — Cloud-6-Standard-Workloads	rds-snapshot-encrypted	Stellen Sie sicher, dass die Verschlüsselung für Ihre Amazon Relational Database Service (Amazon RDS)-Snapshots aktiviert ist. Da sensible Daten auch im Ruhezustand vorhanden sein können, sollten Sie die Verschlüsselung von Daten im Ruhezustand aktivieren, um diese Daten zu schützen.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 — Die Cloud — 6 b-design-and-secure Standard-Workloads	rds-storage-encrypted	Zum Schutz von Daten im Ruhezustand müssen Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon Relational Database Service (Amazon RDS)-Instances aktiviert ist. Um eventuell vorhandene sensible Daten im Ruhezustand in Amazon-RDS-Instanc es zu schützen, muss die Verschlüsselung von Daten im Ruhezustand aktiviert sein.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 — Die Cloud — 6 b-design-and-secure Standard-Workloads	redshift-cluster-configuration-check	Um Daten im Ruhezustand zu schützen, muss die Verschlüs selung für Ihre Amazon-Re dshift-Cluster aktiviert sein. Sie müssen auch sicherste llen, dass die erforderlichen Konfigurationen auf Amazon-Redshift-Clustern bereitgestellt werden. Die Prüfungsprotokolli erung muss aktiviert sein, um Informationen zu Verbindun gen und Benutzeraktivitäten in der Datenbank bereitzus tellen. Diese Regel erfordert , dass ein Wert für clusterDb Encrypted (Config Default: TRUE) und LoggingEnabled (Config Default: TRUE) gesetzt ist. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprech en.
b-design-and-secureAbschnitt 4 — Die Cloud-6-Standard-W orkloads	redshift-require-tls-ssl	Stellen Sie sicher, dass Ihre Amazon-Redshift-Cluster eine TLS/SSL-Verschlüsselung erfordern, um eine Verbindun g zu SQL-Clients herzustel len. Um eventuell vorhanden e sensible Daten zu schützen, sollten Sie die Verschlüs selung bei der Übertragung aktivieren.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 — Die Cloud — 6 b-design-and-secure Standard-Workloads	s3- aktiviert bucket-server-side -encryption	Zum Schutz von Daten im Ruhezustand müssen Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon Simple Storage Service (Amazon S3)-Bucke ts aktiviert ist. Um eventuell vorhandene sensible Daten im Ruhezustand in Amazon-S3 -Buckets zu schützen, muss die Verschlüsselung aktiviert sein.
Abschnitt 4 b-design-and-secure — Die Cloud — 6-Standard-Workloads	s3- bucket-ssl-requests-only	Um Daten während der Übertragung zu schützen, stellen Sie sicher, dass Ihre Amazon Simple Storage Service (Amazon S3)-Buckets Anfragen zur Verwendung von Secure Socket Layer (SSL)-Buckets erfordern. Da sensible Daten vorhanden sein können, sollten Sie die Verschlüs selung bei der Übertragung aktivieren, um diese Daten zu schützen.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 b-design-and-secure — Die Cloud — 6 — Standard-Workloads	s3- default-encryption-kms	Stellen Sie sicher, dass die Verschlüsselung für Ihre Amazon Simple Storage Service (Amazon S3)-Buckets aktiviert ist. Um eventuell vorhandene sensible Daten im Ruhezustand in einem Amazon-S3-Bucket zu schützen, muss die Verschlüsselung aktiviert sein.
Abschnitt 4 b-design-and-secure — Die Cloud — 6 — Standard-Workloads	sagemaker-endpoint-configuration-kms-schlüsselkonfiguriert	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass die Verschlüsselung mit dem AWS Key Management Service (AWS KMS) für Ihren Endpunkt aktiviert ist. SageMaker Da sensible Daten auf dem SageMaker Endgerät gespeichert werden können, sollten Sie die Verschlüsselung im Ruhezustand aktivieren, um diese Daten zu schützen.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 b-design-and-secure — Die Cloud — 6 Standard-Workloads	sagemaker-notebook-instance-kms-schlüsselkonfiguriert	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass die Verschlüsselung mit dem AWS Key Management Service (AWS KMS) für Ihr Notebook aktiviert ist. SageMaker Da vertrauliche Daten im SageMaker Notebook gespeichert werden können, sollten Sie die Verschlüsselung im Ruhezustand aktivieren, um diese Daten zu schützen.
Abschnitt 4 b-design-and-secure — Die Cloud — 6 Standard-Workloads	sns-encrypted-kms	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass Ihre Amazon Simple Notification Service (Amazon SNS) -Themen mit dem AWS Key Management Service (AWS KMS) verschlüsselt werden müssen. Um eventuell vorhandene sensible Daten im Ruhezustand in veröffentlichten Nachrichten zu schützen, muss die Verschlüsselung von Daten im Ruhezustand aktiviert sein.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 b-design-and-secure — Die Cloud — 6 Standard-Workloads	api-gw-ssl-enabled	Stellen Sie sicher, dass die REST-API-Stufen von Amazon API Gateway mit SSL-Zertifikaten konfiguriert sind, damit Backend-Systeme überprüfen können, ob Anforderungen von API Gateway stammen.
Abschnitt 4 — Die Cloud — 6 b-design-and-secure Standard-Workloads	redshift-cluster-kms-enabled	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass die Verschlüsselung mit AWS Key Management Service (AWS KMS) für Ihren Amazon Redshift Redshift-Cluster aktiviert ist. Um eventuell vorhandene sensible Daten im Ruhezustand in Redshift-Clustern zu schützen, muss die Verschlüsselung von Daten im Ruhezustand aktiviert sein.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 b-design-and-secure — Die Cloud — 8 Standard-Workloads	access-keys-rotated	Die Anmeldeinformationen für autorisierte Geräte, Benutzer und Prozesse werden geprüft, indem sichergestellt wird, dass die IAM-Zugriffsschlüssel entsprechend den Vorgaben der Unternehmensrichtlinie rotiert werden. Das regelmäßige Ändern der Zugriffsschlüssel ist eine bewährte Sicherheitsmethode. Es verkürzt den Zeitraum, in dem ein Zugriffsschlüssel aktiv ist, und reduziert die Auswirkungen auf das Unternehmen, wenn die Schlüssel kompromittiert werden. Diese Regel erfordert einen Wert für die Zugriffsschlüssel-Rotation (Standardkonfiguration: 90). Der tatsächliche Wert muss den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 — Die Cloud-8-Standard-Workloads b-design-and-secure	account-part-of-organizations	Durch die zentrale Verwaltung AWS-Konten innerhalb von AWS Organizations wird sichergestellt, dass die Konten den Vorschriften entsprechen. Eine fehlende zentrale Kontoverwaltung kann zu inkonsistenten Kontokonfigurationen führen, wodurch Ressourcen und sensible Daten offengelegt werden können.
Abschnitt 4 b-design-and-secure — Die Cloud — 8 Standard-Workloads	cloudtrail-security-trail-enabled	Diese Regel trägt dazu bei, die Verwendung der AWS empfohlenen bewährten Sicherheitsmethoden für sicherzustellen, indem geprüft wird AWS CloudTrail, ob mehrere Einstellungen aktiviert sind. Dazu gehören die Verwendung von Protokollverschlüsselung, Protokollvalidierung und Aktivierung AWS CloudTrail in mehreren Regionen.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 b-design-and-secure — Die Cloud — 8 Standard-Workloads	emr-kerberos-enabled	Die Zugriffsberechtigungen und -autorisierungen können verwaltet und nach den Prinzipien der geringsten Berechtigung und Aufgabent rennung integriert werden, indem Kerberos für Amazon-EMR-Cluster aktiviert wird. In Kerberos werden Services und Benutzer, die sich authentifizieren müssen, als Prinzipale bezeichnet. Prinzipale befinden sich in einem Kerberos-Bereich. Innerhalb dieses Bereichs wird ein Kerberos-Server als Key Distribution Center (KDC) bezeichnet. Über diesen Server können sich Prinzipale authentifizieren. Die Authentifizierung im KDC erfolgt durch die Ausstellu ng von Authentifizierungs tickets. Das KDC unterhält eine Datenbank der Prinzipal e in seinem Bereich mit ihren Passwörtern und anderen administrativen Informationen zu jedem Prinzipal.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 — Die Cloud mit 8 b-design-and-secure Standard-Workloads	iam-customer-policy-blocked-kms-Aktionen	AWS Identity and Access Management (IAM) kann Ihnen helfen, die Prinzipien der geringsten Rechte und der Aufgabentrennung in Zugriffsberechtigungen und Autorisierungen zu integrier en und so zu verhindern, dass Richtlinien blockierte Aktionen für alle AWS Schlüssel des Key Management Service enthalten. Wenn Benutzer mehr Rechte haben, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und Aufgabentrennung verstoßen . Mit dieser Regel können Sie den Parameter festlegen. blockedActionsPatterns (Wert „AWS Bewährte grundlegende Sicherheitsmethoden“: kms: Entschlüsseln, kms:ReEnc ryptFrom). Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprech en.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 — Die Cloud — 8 Standard-Workloads b-design-and-secure	iam-group-has-users-überprüfen	AWS Identity and Access Management (IAM) kann Ihnen helfen, die Prinzipien der geringsten Rechte und der Aufgabentrennung mit Zugriffsberechtigungen und Autorisierungen zu integrieren, indem sichergestellt wird, dass IAM-Gruppen mindestens einen Benutzer haben. Die Einteilung von Benutzern in Gruppen auf der Grundlage der ihnen zugewiesenen Berechtigungen oder ihrer Funktion ist eine Möglichkeit, das Prinzip der geringsten Berechtigung zu implementieren.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 — Die Cloud-8-Standard-Workloads b-design-and-secure	iam-inline-policy-blocked-kms-Aktionen	Stellen Sie sicher, dass ein Benutzer, eine IAM-Rolle oder eine IAM-Gruppe (AWS Identity and Access Management) nicht über eine Inline-Richtlinie verfügt, die blockierte Aktionen für alle AWS Schlüssel des Key Management Service zulässt. AWS empfiehlt, verwaltete Richtlinien anstelle von Inline-Richtlinien zu verwenden. Verwaltete Richtlinien ermöglichen Wiederverwendbarkeit, Versionsverwaltung, Rollback und Delegierung der Berechtigungsverwaltung. Mit dieser Regel können Sie den blockedActionsPatterns Parameter festlegen. (Wert „AWS Bewährte grundlegende Sicherheitsmethoden“: kms:Entschlüsseln, kms:ReEncryptFrom). Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 — Die Cloud — 8 Standard-Workloads b-design-and-secure	iam-no-inline-policy-überprüfen	Stellen Sie sicher, dass ein Benutzer, eine IAM-Rolle oder eine IAM-Gruppe (AWS Identity and Access Management) nicht über eine Inline-Richtlinie zur Zugriffskontrolle auf Systeme und Ressourcen verfügt. AWS empfiehlt, verwaltete Richtlinien anstelle von Inline-Richtlinien zu verwenden . Verwaltete Richtlinien ermöglichen Wiederverwendbarkeit, Versionsverwaltung, Rollback und Delegierung der Berechtigungsverwaltung.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 b-design-and-secure — Die Cloud — 8 Standard-Workloads	iam-password-policy	Die Identitäten und Anmeldein formationen werden auf der Grundlage einer organisat orischen IAM-Passwortrichtl inie ausgestellt, verwaltet und verifiziert. Sie erfüllen oder übertreffen die Anforderu ngen von NIST SP 800-63 und dem Standard „Best Practices“ von Foundational Security für die Passworts tärke. AWS Mit dieser Regel können Sie optional RequireUppercaseCharacters (Wert für AWS grundlege nde Sicherheitsbewährte Verfahren: wahr), RequireLo wercaseCharacters (Wert für bewährte Methoden für AWS grundlegende Sicherheit: wahr), RequireSymbols (Wert für bewährte Methoden für AWS grundlegende Sicherhei t: wahr), RequireNumbers (Wert für bewährte Methoden für AWS grundlegende Sicherheit: wahr), MinimumPa sswordLength (Wert für bewährte Methoden für AWS grundlegende Sicherheit: 14), PasswordReusePreve ntion (Wert für bewährte Methoden für AWS grundlege nde Sicherheit: 24) und

Kontroll-ID	AWS Config	Empfehlungen
		MaxPasswordAge (Wert für bewährte Methoden für AWS grundlegende Sicherhei t: 90) für Ihr IAM festlegen Kennwortrichtlinie. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisat ion entsprechen.
Abschnitt 4 b-design-and-secure — Die Cloud — 8-Standard-Workloads	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) kann Ihnen dabei helfen, die Prinzipien der geringsten Rechte und der Aufgabent rennung in Zugriffsberechtigu ngen und Autorisierungen zu integrieren und so zu verhindern, dass Richtlinien „Effect“: „Allow“ mit „Action“: „*“ anstelle von „Resource“: „*“ enthalten. Wenn Benutzern mehr Rechte eingeräumt werden, als für die Ausführun g einer Aufgabe erforderl ich sind, kann dies gegen das Prinzip der geringste n Berechtigung und der Aufgabentrennung verstoßen.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt b-design-and-secure 4 — Die Cloud-8-Standard-Workloads	iam-policy-no-statements-with-full-access	Stellen Sie sicher, dass IAM-Aktionen nur auf die benötigten Aktionen beschränkt sind. Wenn Benutzern mehr Rechte eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und der Aufgabentrennung verstoßen.
Abschnitt 4 — Die Cloud mit 8 b-design-and-secure Standard-Workloads	iam-root-access-key-überprüfen	Der Zugriff auf Systeme und Ressourcen kann gesteuert werden, indem überprüft wird, ob der Root-Benutzer keine Zugriffsschlüssel mit seiner AWS Identity and Access Management (IAM) -Rolle verknüpft hat. Stellen Sie sicher, dass die Root-Zugriffsschlüssel gelöscht werden. Erstellen und verwenden Sie stattdessen rollenbasierte Funktionen, AWS-Konten um das Prinzip der geringsten Funktionalität zu berücksichtigen.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 — Die Cloud — 8 Standard-Workloads b-design-and-secure	iam-user-group-membership-überprüfen	AWS Identity and Access Management (IAM) kann Ihnen helfen, Zugriffsberechtigungen und Autorisierungen einzuschränken, indem sichergestellt wird, dass Benutzer Mitglieder mindestens einer Gruppe sind. Wenn Benutzern mehr Berechtigungen eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und Aufgabentrennung verstoßen.
Abschnitt 4 — Die Cloud — 8 Standard-Workloads b-design-and-secure	iam-user-mfa-enabled	Aktivieren Sie diese Regel, um den Zugriff auf Ressourcen in der AWS -Cloud einzuschränken. Diese Regel stellt sicher, dass die Multi-Faktor-Authentifizierung (MFA) für alle Benutzer aktiviert ist. MFA bietet eine weitere Schutzebene zusätzlich zum Benutzernamen und Passwort. Reduzieren Sie Fälle von kompromittierten Konten, indem Sie MFA für Benutzer vorschreiben.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 — Die Cloud mit 8 b-design-and-secure Standard-Workloads	iam-user-no-policies-überprüfen	Diese Regel stellt sicher, dass AWS Identity and Access Management (IAM) -Richtlinien nur Gruppen oder Rollen zugewiesen werden, um den Zugriff auf Systeme und Ressourcen zu kontrollieren. Die Zuweisung von Berechtigungen auf Gruppen- oder Rollenebene trägt dazu bei, die Wahrscheinlichkeit zu verringern, dass eine Identität übermäßige Berechtigungen erhält oder beibehält.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 b-design-and-secure — Cloud-8-Standard-Workloads	iam-user-unused-credentials-überprüfen	AWS Identity and Access Management (IAM) kann Ihnen bei Zugriffsberechtigungen und Autorisierungen helfen, indem es nach IAM-Passwörtern und Zugriffsschlüsseln sucht, die für einen bestimmten Zeitraum nicht verwendet wurden. Wenn ungenutzte Anmeldeinformationen identifiziert werden, müssen Sie sie deaktivieren und/oder entfernen, da dies gegen das Prinzip der geringsten Berechtigung verstoßen könnte. Für diese Regel müssen Sie einen Wert für das maxCredentialUsage Alter festlegen (Standardkonfiguration: 90). Der tatsächliche Wert muss den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 b-design-and-secure — Die Cloud — 8-Standard-Workloads	mfa-enabled-for-iam-Konsolenzugriff	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass MFA für alle AWS Identity and Access Management (IAM) -Benutzer aktiviert ist, die über ein Konsolenkennwort verfügen. MFA sorgt für eine weitere Schutzebene zusätzlich zu den Anmeldeinformationen. Indem Sie MFA für Benutzer vorschreiben, können Sie Fälle kompromittierter Konten reduzieren und verhindern, dass unbefugte Benutzer auf vertrauliche Daten zugreifen.
Abschnitt 4 — Die Cloud — 8 Standard-Workloads b-design-and-secure	root-account-hardware-mfa-aktiviert	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Hardware-MFA für den Root-Benutzer aktiviert ist. Der Stammbenutzer ist der AWS-Konto-Benutzer mit den meisten Berechtigungen. MFA sorgt für eine weitere Schutzebene zusätzlich zu den Anmeldeinformationen. Indem Sie MFA für den Root-Benutzer vorschreiben, können Sie die Anzahl AWS-Konten kompromittierter Benutzer reduzieren.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 — Die Cloud — 8 Standard-Workloads b-design-and-secure	root-account-mfa-enabled	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass MFA für den Root-Benutzer aktiviert ist. Der Stammbenutzer ist der AWS-Konto-Benutzer mit den meisten Berechtigungen. MFA bietet eine weitere Schutzebene zusätzlich zum Benutzernamen und Passwort. Indem Sie MFA für den Root-Benutzer vorschreiben, können Sie die Anzahl AWS-Konten kompromittierter Benutzer reduzieren.
Abschnitt 4 — Cloud-9-Standard-Workloads b-design-and-secure	cloudtrail-enabled	AWS CloudTrail kann durch die Aufzeichnung von Aktionen und API-Aufrufen in der Management Console bei der Nichtabstreitbarkeit helfen. AWS Sie können die Benutzer und die Benutzer AWS-Konten , die einen AWS Dienst aufgerufen haben, die Quell-IP-Adresse, über die die Aufrufe generiert wurden, und den Zeitpunkt der Anrufe identifizieren. Einzelheiten zu den erfassten Daten finden Sie unter Inhalt des AWS CloudTrail Datensatzes.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 b-design-and-secure — Cloud-9-Standard-Workloads	iam-group-has-users-überprüfen	AWS Identity and Access Management (IAM) kann Ihnen helfen, die Prinzipien der geringsten Rechte und der Aufgabentrennung mit Zugriffsberechtigungen und Autorisierungen zu integrieren, indem sichergestellt wird, dass IAM-Gruppen mindestens einen Benutzer haben. Die Einteilung von Benutzern in Gruppen auf der Grundlage der ihnen zugewiesenen Berechtigungen oder ihrer Funktion ist eine Möglichkeit, das Prinzip der geringsten Berechtigung zu implementieren.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 — Cloud-9-Standard-Workloads b-design-and-secure	iam-no-inline-policy-überprüfen	Stellen Sie sicher, dass ein Benutzer, eine IAM-Rolle oder eine IAM-Gruppe (AWS Identity and Access Management) nicht über eine Inline-Richtlinie zur Zugriffskontrolle auf Systeme und Ressourcen verfügt. AWS empfiehlt, verwaltete Richtlinien anstelle von Inline-Richtlinien zu verwenden . Verwaltete Richtlinien ermöglichen Wiederverwendbarkeit, Versionsverwaltung, Rollback und Delegierung der Berechtigungsverwaltung.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 b-design-and-secure — Die Cloud — 9-Standard-Workloads	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) kann Ihnen dabei helfen, die Prinzipien der geringsten Rechte und der Aufgabent rennung in Zugriffsberechtigu ngen und Autorisierungen zu integrieren und so zu verhindern, dass Richtlinien „Effect“: „Allow“ mit „Action“: „*“ anstelle von „Resource“: „*“ enthalten. Wenn Benutzern mehr Rechte eingeräumt werden, als für die Ausführun g einer Aufgabe erforderl ich sind, kann dies gegen das Prinzip der geringste n Berechtigung und der Aufgabentrennung verstoßen.
Abschnitt b-design-and-secure 4 — Die Cloud-9-Standard-W orkloads	iam-policy-no-statements-with-full-access	Stellen Sie sicher, dass IAM-Aktionen nur auf die benötigte n Aktionen beschränkt sind. Wenn Benutzern mehr Rechte eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und der Aufgabentrennung verstoßen.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 — b-design-and-secure Cloud-9-Standard-Workloads	iam-root-access-key-überprüfen	Der Zugriff auf Systeme und Ressourcen kann gesteuert werden, indem überprüft wird, ob der Root-Benutzer keine Zugriffsschlüssel mit seiner AWS Identity and Access Management (IAM) -Rolle verknüpft hat. Stellen Sie sicher, dass die Root-Zugriffsschlüssel gelöscht werden. Erstellen und verwenden Sie stattdessen rollenbasierte Funktionen, AWS-Konten um das Prinzip der geringsten Funktionalität zu berücksichtigen.
Abschnitt 4 — Cloud-9-Standard-Workloads b-design-and-secure	iam-user-group-membership-überprüfen	AWS Identity and Access Management (IAM) kann Ihnen helfen, Zugriffsberechtigungen und Autorisierungen einzuschränken, indem sichergestellt wird, dass Benutzer Mitglieder mindestens einer Gruppe sind. Wenn Benutzern mehr Berechtigungen eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und Aufgabentrennung verstoßen.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 — Die Cloud-9-Standard-Workloads b-design-and-secure	iam-user-mfa-enabled	Aktivieren Sie diese Regel, um den Zugriff auf Ressourcen in der AWS -Cloud einzuschränken. Diese Regel stellt sicher, dass die Multi-Faktor-Authentifizierung (MFA) für alle Benutzer aktiviert ist. MFA bietet eine weitere Schutzebene zusätzlich zum Benutzernamen und Passwort. Reduzieren Sie Fälle von kompromittierten Konten, indem Sie MFA für Benutzer vorschreiben.
Abschnitt 4 — b-design-and-secure Cloud-9-Standard-Workloads	iam-user-no-policies-überprüfen	Diese Regel stellt sicher, dass AWS Identity and Access Management (IAM) -Richtlinien nur Gruppen oder Rollen zugewiesen werden, um den Zugriff auf Systeme und Ressourcen zu kontrollieren. Die Zuweisung von Berechtigungen auf Gruppen- oder Rollenebene trägt dazu bei, die Wahrscheinlichkeit zu verringern, dass eine Identität übermäßige Berechtigungen erhält oder beibehält.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 b-design-and-secure — Cloud-9-Standard-Workloads	iam-user-unused-credentials-überprüfen	AWS Identity and Access Management (IAM) kann Ihnen bei Zugriffsberechtigungen und Autorisierungen helfen, indem es nach IAM-Passwörtern und Zugriffsschlüsseln sucht, die für einen bestimmten Zeitraum nicht verwendet wurden. Wenn ungenutzte Anmeldeinformationen identifiziert werden, müssen Sie sie deaktivieren und/oder entfernen, da dies gegen das Prinzip der geringsten Berechtigung verstoßen könnte. Für diese Regel müssen Sie einen Wert für das maxCredentialUsage Alter festlegen (Standardkonfiguration: 90). Der tatsächliche Wert muss den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 b-design-and-secure — Die Cloud-9-Standard-Workloads	mfa-enabled-for-iam-Konsolenzugriff	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass MFA für alle AWS Identity and Access Management (IAM) -Benutzer aktiviert ist, die über ein Konsolenkennwort verfügen. MFA sorgt für eine weitere Schutzebene zusätzlich zu den Anmeldeinformationen. Indem Sie MFA für Benutzer vorschreiben, können Sie Fälle kompromittierter Konten reduzieren und verhindern, dass unbefugte Benutzer auf vertrauliche Daten zugreifen.
Abschnitt 4 — Die Cloud-9-Standard-Workloads b-design-and-secure	root-account-hardware-mfa-aktiviert	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Hardware-MFA für den Root-Benutzer aktiviert ist. Der Stammbenutzer ist der AWS-Konto-Benutzer mit den meisten Berechtigungen. MFA sorgt für eine weitere Schutzebene zusätzlich zu den Anmeldeinformationen. Indem Sie MFA für den Root-Benutzer vorschreiben, können Sie die Anzahl AWS-Konten kompromittierter Benutzer reduzieren.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 — Cloud-9-S tandard-Workloads b-design-and-secure	root-account-mfa-enabled	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherste llen, dass MFA für den Root-Benutzer aktiviert ist. Der Stammbenutzer ist der AWS-Konto-Benutzer mit den meisten Berechtigungen. MFA bietet eine weitere Schutzebe ne zusätzlich zum Benutzern amen und Passwort. Indem Sie MFA für den Root-Benu tzer vorschreiben, können Sie die Anzahl AWS-Konte n kompromittierter Benutzer reduzieren.
Abschnitt 4 — Cloud-9-S tandard-Workloads b-design-and-secure	securityhub-enabled	AWS Security Hub hilft bei der Überwachung von unbefugte m Personal, Verbindungen, Geräten und Software. AWS Security Hub aggregiert, organisiert und priorisiert die Sicherheitswarnungen oder Ergebnisse mehrerer Dienste. AWS Einige dieser Dienste sind Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer und AWS Firewall Manager sowie AWS Partnerlösungen.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 — Die Cloud-10-Standard-Workloads b-design-and-secure	access-keys-rotated	Die Anmeldeinformationen für autorisierte Geräte, Benutzer und Prozesse werden geprüft, indem sichergestellt wird, dass die IAM-Zugriffsschlüssel entsprechend den Vorgaben der Unternehmensrichtlinie rotiert werden. Das regelmäßi ge Ändern der Zugriffss chlüssel ist eine bewährte Sicherheitsmethode. Es verkürzt den Zeitraum, in dem ein Zugriffsschlüssel aktiv ist, und reduziert die Auswirkun gen auf das Unternehmen, wenn die Schlüssel kompromit tiert werden. Diese Regel erfordert einen Wert für die Zugriffsschlüssel-Rotation (Standardkonfiguration: 90). Der tatsächliche Wert muss den Richtlinien Ihrer Organisat ion entsprechen.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 — Die Cloud-10-Standard-Workloads b-design-and-secure	autoscaling-launch-config-public-ip-deaktiviert	Wenn Sie Ihre Netzwerkschnittstellen mit einer öffentlichen IP-Adresse konfigurieren, sind die diesen Netzwerkschnittstellen zugehörigen Ressourcen über das Internet erreichbar. EC2 Ressourcen sollten nicht öffentlich zugänglich sein, da dies einen unbeabsichtigten Zugriff auf Ihre Anwendungen oder Server ermöglichen kann.
Abschnitt 4 b-design-and-secure — Die Cloud-10-Standard-Workloads	elasticsearch-in-vpc-only	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass sich Amazon OpenSearch OpenSearch Service (Service)-Domains innerhalb einer Amazon Virtual Private Cloud (Amazon VPC) befinden. Eine OpenSearch Service-Domain innerhalb einer Amazon VPC ermöglicht die sichere Kommunikation zwischen OpenSearch Service und anderen Services innerhalb der Amazon VPC, ohne dass ein Internet-Gateway, ein NAT-Gerät oder eine VPN-Verbindung erforderlich ist.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 — Die Cloud-10-Standard-Workloads b-design-and-secure	emr-master-no-public-ip	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon EMR-Cluster-Masterknoten nicht öffentlich zugänglich sind. Amazon-EMR-Cluster-Hauptknoten können vertrauliche Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.
Abschnitt 4 b-design-and-secure — Die Cloud-10-Standard-Workloads	iam-no-inline-policy-überprüfen	Stellen Sie sicher, dass ein Benutzer, eine IAM-Rolle oder eine IAM-Gruppe (AWS Identity and Access Management) nicht über eine Inline-Richtlinie zur Zugriffskontrolle auf Systeme und Ressourcen verfügt. AWS empfiehlt, verwaltete Richtlinien anstelle von Inline-Richtlinien zu verwenden . Verwaltete Richtlinien ermöglichen Wiederverwendbarkeit, Versionsverwaltung, Rollback und Delegierung der Berechtigungsverwaltung.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 b-design-and-secure — Die Cloud — 10 Standard-Workloads	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) kann Ihnen dabei helfen, die Prinzipien der geringsten Rechte und der Aufgabent rennung in Zugriffsberechtigu ngen und Autorisierungen zu integrieren und so zu verhindern, dass Richtlinien „Effect“: „Allow“ mit „Action“: „*“ anstelle von „Resource“: „*“ enthalten. Wenn Benutzern mehr Rechte eingeräumt werden, als für die Ausführun g einer Aufgabe erforderl ich sind, kann dies gegen das Prinzip der geringste n Berechtigung und der Aufgabentrennung verstoßen.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt b-design-and-secure 4 — Die Cloud-10-Standard-Workloads	iam-root-access-key-überprüfen	Der Zugriff auf Systeme und Ressourcen kann gesteuert werden, indem überprüft wird, ob der Root-Benutzer keine Zugriffsschlüssel mit seiner AWS Identity and Access Management (IAM) -Rolle verknüpft hat. Stellen Sie sicher, dass die Root-Zugriffsschlüssel gelöscht werden. Erstellen und verwenden Sie stattdessen rollenbasierte Funktionen, AWS-Konten um das Prinzip der geringsten Funktionalität zu berücksichtigen.
Abschnitt 4 — Die Cloud-10-Standard-Workloads b-design-and-secure	iam-user-mfa-enabled	Aktivieren Sie diese Regel, um den Zugriff auf Ressourcen in der AWS -Cloud einzuschränken. Diese Regel stellt sicher, dass die Multi-Faktor-Authentifizierung (MFA) für alle Benutzer aktiviert ist. MFA bietet eine weitere Schutzebene zusätzlich zum Benutzernamen und Passwort. Reduzieren Sie Fälle von kompromittierten Konten, indem Sie MFA für Benutzer vorschreiben.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 — Die b-design-and-secure Cloud-10-Standard-Workloads	iam-user-no-policies-überprüfen	Diese Regel stellt sicher, dass AWS Identity and Access Management (IAM) -Richtlinien nur Gruppen oder Rollen zugewiesen werden, um den Zugriff auf Systeme und Ressourcen zu kontrollieren. Die Zuweisung von Berechtigungen auf Gruppen- oder Rollenebene trägt dazu bei, die Wahrscheinlichkeit zu verringern, dass eine Identität übermäßige Berechtigungen erhält oder beibehält.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 b-design-and-secure — Die Cloud-10-Standard-Workloads	iam-user-unused-credentials-überprüfen	AWS Identity and Access Management (IAM) kann Ihnen bei Zugriffsberechtigungen und Autorisierungen helfen, indem es nach IAM-Passwörtern und Zugriffsschlüsseln sucht, die für einen bestimmten Zeitraum nicht verwendet wurden. Wenn ungenutzte Anmeldeinformationen identifiziert werden, müssen Sie sie deaktivieren und/oder entfernen, da dies gegen das Prinzip der geringsten Berechtigung verstoßen könnte. Für diese Regel müssen Sie einen Wert für das maxCredentialUsage Alter festlegen (Standardkonfiguration: 90). Der tatsächliche Wert muss den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 b-design-and-secure — Die Cloud-10-Standard-Workloads	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) Security Groups können bei der Verwaltung des Netzwerkz ugriffs helfen, indem sie eine statusbehaftete Filterung von eingehendem und ausgehend em Netzwerkverkehr zu Ressourcen bereitstellen. AWS Wenn Sie eingehenden (oder entfernten) Datenverk ehr von 0.0.0.0/0 bis Port 22 auf Ihren Ressourcen nicht zulassen, können Sie den Remote-Zugriff einschränken.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 — Die Cloud-10-Standard-Workloads b-design-and-secure	ec2- instances-in-vpc	Stellen Sie Amazon Elastic Compute Cloud (Amazon EC2) -Instances innerhalb einer Amazon Virtual Private Cloud (Amazon VPC) bereit, um eine sichere Kommunika tion zwischen einer Instance und anderen Services innerhalb der Amazon VPC zu ermöglichen, ohne dass ein Internet-Gateway, ein NAT-Gerät oder eine VPN-Verbi ndung erforderlich ist. Der gesamte Datenverkehr bleibt sicher in der AWS Cloud. Domains, die sich innerhalb einer VPC befinden, verfügen aufgrund ihrer logischen Isolierung im Vergleich zu Domains mit öffentlic hen Endpunkten über eine zusätzliche Sicherheitsebene. Weisen Sie EC2 Amazon-In stances einer Amazon-VPC zu, um den Zugriff ordnungsg emäß zu verwalten.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 b-design-and-secure — Die Cloud-10-Standard-Workloads	internet-gateway-authorized-vpc-nur	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Internet-Gateways nur mit autorisierter Amazon Virtual Private Cloud (Amazon VPC) verbunden sind. Internet-Gateways ermöglichen den bidirekti onalen Internetzugang zur und von der Amazon VPC, was möglicherweise zu einem unbefugten Zugriff auf Amazon-VPC-Ressourcen führen kann.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 — Die Cloud-10-Standard-Workloads b-design-and-secure	lambda-inside-vpc	Stellen Sie AWS Lambda-Funktionen in einer Amazon Virtual Private Cloud (Amazon VPC) bereit, um eine sichere Kommunikation zwischen einer Funktion und anderen Diensten innerhalb der Amazon VPC zu gewährleisten. Bei dieser Konfiguration sind kein Internet-Gateway, kein NAT-Gerät und keine VPN-Verbindung erforderlich. Der gesamte Datenverkehr bleibt sicher in der Cloud. AWS Domains, die sich innerhalb einer VPC befinden, verfügen aufgrund ihrer logischen Isolierung im Vergleich zu Domains mit öffentlichen Endpunkten über eine zusätzliche Sicherheitsebene. Um den Zugriff ordnungsgemäß zu verwalten, sollten AWS Lambda-Funktionen einer VPC zugewiesen werden.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 — Die Cloud-10-Standard-Workloads b-design-and-secure	mfa-enabled-for-iam-Konsolenzugriff	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass MFA für alle AWS Identity and Access Management (IAM) -Benutzer aktiviert ist, die über ein Konsolenkennwort verfügen. MFA sorgt für eine weitere Schutzebene zusätzlich zu den Anmeldeinformationen. Indem Sie MFA für Benutzer vorschreiben, können Sie Fälle kompromittierter Konten reduzieren und verhindern, dass unbefugte Benutzer auf vertrauliche Daten zugreifen.
Abschnitt 4 — Die Cloud-10-Standard-Workloads b-design-and-secure	no-unrestricted-route-to-igw	Stellen Sie sicher, dass EC2 Amazon-Routentabellen keine uneingeschränkten Routen zu einem Internet-Gateway enthalten. Durch das Entfernen oder Beschränken des Internetzugangs für Workloads innerhalb von Amazon VPCs können unbeabsichtigte Zugriffe in Ihrer Umgebung reduziert werden.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 — Die Cloud-10-Standard-Workloads b-design-and-secure	opensearch-in-vpc-only	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass sich Amazon OpenSearch Service-Domains innerhalb einer Amazon Virtual Private Cloud (Amazon VPC) befinden. Eine Amazon OpenSearch Service-Domain innerhalb einer Amazon VPC ermöglich t die sichere Kommunika tion zwischen Amazon OpenSearch Service und anderen Services innerhalb der Amazon VPC, ohne dass ein Internet-Gateway, ein NAT-Gerät oder eine VPN-Verbindung erforderlich ist.
Abschnitt 4 — Die Cloud-10-Standard-Workloads b-design-and-secure	rds-instance-public-access-überprüfen	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherste llen, dass Amazon Relationa l Database Service (Amazon RDS) -Instances nicht öffentlic h sind. Amazon-RDS-Datenba nk-Instances können vertrauli che Informationen enthalten und für solche Konten sind Prinzipien und Zugriffsk ontrollen erforderlich.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 b-design-and-secure — Die Cloud-10-Standard-Workloads	redshift-cluster-public-access-überprüfen	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Redshift Redshift-Cluster nicht öffentlich sind. Amazon-Redshift-Cluster können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.
Abschnitt 4 b-design-and-secure — Die Cloud — 10-Standard-Workloads	restricted-common-ports	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass gemeinsame Ports für Amazon Elastic Compute Cloud (Amazon EC2) - Sicherheitsgruppen eingeschränkt sind. Wenn der Zugriff auf Ports nicht auf vertrauenswürdige Quellen beschränkt wird, kann dies zu Angriffen auf die Verfügbarkeit, Integrität und Vertraulichkeit von Systemen führen. Mit dieser Regel können Sie optional die Parameter blockedPort1–blockedPort5 festlegen (Standardkonfigurationen: 20, 21, 3389, 3306, 4333). Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 b-design-and-secure — Die Cloud-10-Standard-Workloads	root-account-hardware-mfa-aktiviert	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Hardware-MFA für den Root-Benutzer aktiviert ist. Der Stammbenutzer ist der AWS-Konto-Benutzer mit den meisten Berechtigungen. MFA sorgt für eine weitere Schutzebene zusätzlich zu den Anmeldeinformationen. Indem Sie MFA für den Root-Benutzer vorschreiben, können Sie die Anzahl AWS-Konten kompromittierter Benutzer reduzieren.
Abschnitt 4 — Die Cloud-10-Standard-Workloads b-design-and-secure	root-account-mfa-enabled	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass MFA für den Root-Benutzer aktiviert ist. Der Stammbenutzer ist der AWS-Konto-Benutzer mit den meisten Berechtigungen. MFA bietet eine weitere Schutzebene zusätzlich zum Benutzernamen und Passwort. Indem Sie MFA für den Root-Benutzer vorschreiben, können Sie die Anzahl AWS-Konten kompromittierter Benutzer reduzieren.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 — Die Cloud-10-Standard-Workloads b-design-and-secure	s3- -Blöcke — periodisch account-level-public-access	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Simple Storage Service (Amazon S3) -Buckets nicht öffentlich zugänglich sind. Diese Regel trägt dazu bei, sensible Daten vor unbefugten Remote-Benutzern zu schützen, indem sie den öffentlichen Zugriff verhindert. Mit dieser Regel können Sie optional die Parameter ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) und restrictPublicBuckets Parameter (Config Default: True) festlegen. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 b-design-and-secure — Die Cloud-10-Standard-Workloads	sagemaker-notebook-no-direct-Internetzugang	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass SageMaker Amazon-Notebooks keinen direkten Internetzugang zulassen. Indem Sie direkten Internetzugang blockieren, vermeiden Sie, dass unbefugte Benutzer auf sensible Daten zugreifen.
Abschnitt 4 b-design-and-secure — Die Cloud-10-Standard-Workloads	ssm-document-not-public	Stellen Sie sicher, dass AWS Systems Manager (SSM) -Dokumente nicht öffentlich sind, da dies einen unbeabsichtigten Zugriff auf Ihre SSM-Dokumente ermöglichen kann. Ein öffentliches SSM-Dokument kann Informationen über Ihr Konto, Ihre Ressourcen und internen Prozesse preisgeben.

Kontroll-ID	AWS Config	Empfehlungen
b-design-and-secureAbschnitt 4 — Die Cloud-10-Standard-Workloads	vpc-default-security-group-geschlossen	Sicherheitsgruppen von Amazon Elastic Compute Cloud (Amazon EC2) können bei der Verwaltung des Netzwerkzugriffs helfen, indem sie eine statusbeh aftete Filterung des ein- und ausgehenden Netzwerkv erkehrs zu Ressourcen bereitstellen. AWS Die Beschränkung des gesamten Datenverkehrs auf die Standardsicherheitsgruppe hilft dabei, den Fernzugriff auf Ihre Ressourcen einzuschr änken. AWS

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 — Die Cloud-10-Standard-Workloads b-design-and-secure	vpc-sg-open-only-to-authorized-ports	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass gemeinsame Ports für Amazon Elastic Compute Cloud (Amazon EC2) -Sicherheitsgruppen eingeschränkt sind. Wenn der Zugriff auf Ports nicht auf vertrauenswürdige Quellen beschränkt wird, kann dies zu Angriffen auf die Verfügbarkeit, Integrität und Vertraulichkeit von Systemen führen. Durch die Beschränkung des Zugriffs auf Ressourcen innerhalb einer Sicherheitsgruppe aus dem Internet (0.0.0.0/0) kann der Remote-Zugriff auf interne Systeme gesteuert werden.
Abschnitt 4 b-design-and-secure — Die Cloud-10-Standard-Workloads	s3- verboten bucket-level-public-access	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Simple Storage Service (Amazon S3) -Buckets nicht öffentlich zugänglich sind. Diese Regel trägt dazu bei, sensible Daten vor unbefugten Remote-Benutzern zu schützen, indem sie den öffentlichen Zugriff auf Bucket-Ebene verhindert.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 b-design-and-secure — Die Cloud-10-Standard-Workloads	subnet-auto-assign-public-ip-deaktiviert	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon Virtual Private Cloud (VPC) -Subnetzen nicht automatis ch eine öffentliche IP-Adress e zugewiesen wird. Amazon Elastic Compute Cloud (EC2) -Instances, die in Subnetzen gestartet werden, in denen dieses Attribut aktiviert ist, haben ihrer primären Netzwerkschnittste lle eine öffentliche IP-Adresse zugewiesen.
Abschnitt 4 b-design-and-secure — Die Cloud-12-Standard-Workloads	api-gw-cache-enabled-und verschlüsselt	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass die Verschlüsselung für den Cache Ihrer API-Gatew ay-Stufe aktiviert ist. Da für die API-Methode sensible Daten erfasst werden können, sollten Sie die Verschlüsselung von Daten im Ruhezustand aktivieren, um diese Daten zu schützen.
Abschnitt 4 — Die Cloud-12-Standard-Workloads b-design-and-secure	cloudwatch-log-group-encryp ted	Um sensible Daten im Speicher zu schützen, stellen Sie sicher, dass die Verschlüs selung für Ihre Amazon CloudWatch Log Groups aktiviert ist.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 b-design-and-secure — Die Cloud-12-Standard-Workloads	cloud-trail-encryption-enabled	Zum Schutz von eventuell vorhandenen sensiblen Daten sowie Daten im Ruhezusta nd müssen Sie sicherstellen, dass die Verschlüsselung für Ihre AWS CloudTrail aktiviert ist.
Abschnitt 4 — Die b-design-and-secure Cloud-12-Standard-Workloads	codebuild-project-envvar-aw scred-überprüfen	Stellen Sie sicher, dass die Anmeldeinformationen AWS_ACCESS_KEY_ID AWS_SECRET_ACCESS_ KEY nicht in AWS Codebuild -Projektumgebungen vorhanden sind. Speichern Sie diese Variablen nicht als Klartext. Das Speichern dieser Variablen als Klartext bewirkt eine unbeabsichtigte Offenlegung von Daten sowie unberechtigte Zugriffe.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 b-design-and-secure — Die Cloud-12-Standard-Workloads	codebuild-project-source-repo-URL-Prüfung	Stellen Sie sicher, dass die URL des Quell-Repositorys GitHub oder des Bitbucket -Quell-Repositorys keine persönlichen Zugriffstoken oder Anmeldeinformationen in Codebuild-Projektumgebungen enthält. AWS Verwende OAuth anstelle von persönlichen Zugriffstoken oder Anmeldedaten die Autorisierung für den Zugriff auf GitHub Bitbucket-Repositorys.
b-design-and-secureAbschnitt 4 — Die Cloud-12-Standard-Workloads	dynamodb-table-encrypted-kms	Stellen Sie sicher, dass die Verschlüsselung für Ihre Amazon-DynamoDB-Tabellen aktiviert ist. Um eventuell vorhandene sensible Daten im Ruhezustand in diesen Tabellen zu schützen, müssen Sie die Verschlüsselung von Daten im Ruhezustand aktivieren. Standardmäßig werden DynamoDB-Tabellen mit einem AWS eigenen Kundenhauptschlüssel (CMK) verschlüsselt.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 — Die b-design-and-secure Cloud-12-Standard-Workloads	ec2- ebs-encryption-by-default	Zum Schutz von Daten im Ruhezustand müssen Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon Elastic Block Store (Amazon EBS)-Volumes aktiviert ist. Da sensible Daten auch im Ruhezusta nd vorhanden sein können, sollten Sie die Verschlüs selung im Ruhezustand aktivieren, um diese Daten zu schützen.
Abschnitt 4 b-design-and-secure — Die Cloud-12-Standard-Workloads	efs-encrypted-check	Aktivieren Sie die Verschlüs selung für Ihr Amazon Elastic File System (EFS), um eventuell vorhandene sensible Daten sowie Daten im Ruhezustand zu schützen.
Abschnitt 4 — Die b-design-and-secure Cloud-12-Standard-Workloads	elasticsearch-encrypted-at-rest	Da sensible Daten vorhanden sein können und um Daten im Ruhezustand zu schützen, sollten Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon OpenSearch Service (OpenSearch Service) -Domains aktiviert ist.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 b-design-and-secure — Die Cloud-12-Standard-Workloads	encrypted-volumes	Aktivieren Sie die Verschlüs selung für Ihre Amazon-El astic-Block-Store (Amazon-EBS)-Volumes, um eventuell vorhandene sensible Daten sowie Daten im Ruhezustand zu schützen.
Abschnitt 4 — Die b-design-and-secure Cloud-12-Standard-Workloads	iam-no-inline-policy-überpr üfen	Stellen Sie sicher, dass ein Benutzer, eine IAM-Rolle oder eine IAM-Grupp e (AWS Identity and Access Management) nicht über eine Inline-Richtlinie zur Zugriffskontrolle auf Systeme und Ressourcen verfügt. AWS empfiehlt, verwaltete Richtlinien anstelle von Inline-Richtlinien zu verwenden . Verwaltete Richtlinien ermöglichen Wiederver wendbarkeit, Versionsv erwaltung, Rollback und Delegierung der Berechtig ungsverwaltung.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 b-design-and-secure — Die Cloud — 12 Standard-Workloads	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) kann Ihnen dabei helfen, die Prinzipien der geringsten Rechte und der Aufgabent rennung in Zugriffsberechtigu ngen und Autorisierungen zu integrieren und so zu verhindern, dass Richtlinien „Effect“: „Allow“ mit „Action“: „*“ anstelle von „Resource“: „*“ enthalten. Wenn Benutzern mehr Rechte eingeräumt werden, als für die Ausführun g einer Aufgabe erforderl ich sind, kann dies gegen das Prinzip der geringste n Berechtigung und der Aufgabentrennung verstoßen.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt b-design-and-secure 4 — Die Cloud-12-Standard-Workloads	iam-user-group-membership-überprüfen	AWS Identity and Access Management (IAM) kann Ihnen helfen, Zugriffsberechtigungen und Autorisierungen einzuschränken, indem sichergestellt wird, dass Benutzer Mitglieder mindestens einer Gruppe sind. Wenn Benutzern mehr Berechtigungen eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und Aufgabentrennung verstoßen.
Abschnitt 4 — Die Cloud-12-Standard-Workloads b-design-and-secure	iam-user-no-policies-überprüfen	Diese Regel stellt sicher, dass AWS Identity and Access Management (IAM) -Richtlinien nur Gruppen oder Rollen zugewiesen werden, um den Zugriff auf Systeme und Ressourcen zu kontrollieren. Die Zuweisung von Berechtigungen auf Gruppen- oder Rollenebene trägt dazu bei, die Wahrscheinlichkeit zu verringern, dass eine Identität übermäßige Berechtigungen erhält oder beibehält.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 b-design-and-secure — Die Cloud-12-Standard-Workloads	kinesis-stream-encrypted	Aktivieren Sie die Verschlüs selung für Ihre Amazon-Ki nesis-Streams, um eventuell vorhandene sensible Daten sowie Daten im Ruhezustand zu schützen.
Abschnitt 4 — Die b-design-and-secure Cloud-12-Standard-Workloads	opensearch-encrypted-at-rest	Da sensible Daten vorhanden sein können und um Daten im Ruhezustand zu schützen, sollten Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon OpenSearch Service-Domains aktiviert ist.
Abschnitt 4 b-design-and-secure — Die Cloud-12-Standard-Workloads	rds-snapshot-encrypted	Stellen Sie sicher, dass die Verschlüsselung für Ihre Amazon Relational Database Service (Amazon RDS)-Snapshots aktiviert ist. Da sensible Daten auch im Ruhezustand vorhanden sein können, sollten Sie die Verschlüsselung von Daten im Ruhezustand aktivieren, um diese Daten zu schützen.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 — Die b-design-and-secure Cloud-12-Standard-Workloads	rds-storage-encrypted	Zum Schutz von Daten im Ruhezustand müssen Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon Relational Database Service (Amazon RDS)-Instances aktiviert ist. Um eventuell vorhandene sensible Daten im Ruhezustand in Amazon-RDS-Instanc es zu schützen, muss die Verschlüsselung von Daten im Ruhezustand aktiviert sein.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 — Die b-design-and-secure Cloud-12-Standard-Workloads	redshift-cluster-configuration-check	Um Daten im Ruhezustand zu schützen, muss die Verschlüsselung für Ihre Amazon-Redshift-Cluster aktiviert sein. Sie müssen auch sicherstellen, dass die erforderlichen Konfigurationen auf Amazon-Redshift-Clustern bereitgestellt werden. Die Prüfungsprotokollierung muss aktiviert sein, um Informationen zu Verbindungen und Benutzeraktivitäten in der Datenbank bereitzustellen. Diese Regel erfordert, dass ein Wert für clusterDbEncrypted (Config Default: TRUE) und LoggingEnabled (Config Default: TRUE) gesetzt ist. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	AWS Config	Empfehlungen
b-design-and-secureAbschnitt 4 — Die Cloud-12-Standard-Workloads	s3-aktiviert bucket-server-side-encryption	Zum Schutz von Daten im Ruhezustand müssen Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon Simple Storage Service (Amazon S3)-Buckets aktiviert ist. Um eventuell vorhandene sensible Daten im Ruhezustand in Amazon-S3-Buckets zu schützen, muss die Verschlüsselung aktiviert sein.
Abschnitt 4 b-design-and-secure — Die Cloud-12-Standard-Workloads	sagemaker-endpoint-configuration-kms-schlüsselkonfiguriert	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass die Verschlüsselung mit dem AWS Key Management Service (AWS KMS) für Ihren Endpunkt aktiviert ist. SageMaker Da sensible Daten auf dem SageMaker Endgerät gespeichert werden können, sollten Sie die Verschlüsselung im Ruhezustand aktivieren, um diese Daten zu schützen.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 b-design-and-secure — Die Cloud-12-Standard-Workloads	sagemaker-notebook-instance-kms-schlüsselkonfiguriert	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass die Verschlüsselung mit dem AWS Key Management Service (AWS KMS) für Ihr Notebook aktiviert ist. SageMaker Da vertrauliche Daten im SageMaker Notebook gespeichert werden können, sollten Sie die Verschlüsselung im Ruhezustand aktivieren, um diese Daten zu schützen.
Abschnitt 4 b-design-and-secure — Die Cloud-12-Standard-Workloads	sns-encrypted-kms	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass Ihre Amazon Simple Notification Service (Amazon SNS) -Themen mit dem AWS Key Management Service (AWS KMS) verschlüsselt werden müssen. Um eventuell vorhandene sensible Daten im Ruhezustand in veröffentlichten Nachrichten zu schützen, muss die Verschlüsselung von Daten im Ruhezustand aktiviert sein.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 b-design-and-secure — Cloud-14-Standard-Workloads	api-gw-execution-logging-aktiviert	Die API-Gateway-Protokollierung zeigt detaillierte Ansichten der Benutzer, die auf die API zugegriffen haben, und wie diese Benutzer auf die API zugegriffen haben. Diese Einblicke ermöglichen die Transparenz von Benutzeraktivitäten.
Abschnitt 4 b-design-and-secure — Cloud-14-Standard-Workloads	cloudtrail-s3-dataevents-enabled	Die Erfassung von Simple Storage Service (Amazon S3)-Datenereignissen unterstützt die Erkennung von ungewöhnlichen Aktivitäten. Zu den Details gehören Informationen zu dem AWS -Konto, das auf einen Amazon-S3-Bucket zugegriffen hat, die IP-Adresse und die Uhrzeit des Ereignisses.
Abschnitt 4 — b-design-and-secure Cloud-14-Standard-Workloads	cloudtrail-security-trail-enabled	Diese Regel trägt dazu bei, die Verwendung der AWS empfohlenen bewährten Sicherheitsmethoden für sicherzustellen, indem geprüft wird AWS CloudTrail, ob mehrere Einstellungen aktiviert sind. Dazu gehören die Verwendung von Protokollverschlüsselung, Protokollvalidierung und Aktivierung AWS CloudTrail in mehreren Regionen.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 b-design-and-secure — Cloud-14-Standard-Workloads	cloudwatch-log-group-encrypted	Um sensible Daten im Speicher zu schützen, stellen Sie sicher, dass die Verschlüsselung für Ihre Amazon CloudWatch Log Groups aktiviert ist.
Abschnitt 4 b-design-and-secure — Cloud-14-Standard-Workloads	cloud-trail-cloud-watch-Logs aktiviert	Verwenden Sie Amazon CloudWatch , um Protokoll ereignisaktivitäten zentral zu sammeln und zu verwalten . Die Aufnahme von AWS CloudTrail Daten liefert Einzelheiten zu den API-Aufrufaktivitäten in Ihrem AWS-Konto.
Abschnitt 4 b-design-and-secure — Cloud-14-Standard-Workloads	cloud-trail-encryption-enabled	Zum Schutz von eventuell vorhandenen sensiblen Daten sowie Daten im Ruhezustand müssen Sie sicherstellen, dass die Verschlüsselung für Ihre AWS CloudTrail aktiviert ist.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 — b-design-and-secure Cloud-14-Standard-Workloads	cloud-trail-log-file-Validierung aktiviert	Verwenden Sie die AWS CloudTrail Protokolldateivalidierung, um die Integrität von Protokollen zu überprüfen. CloudTrail Mithilfe der Protokolldateivalidierung kann festgestellt werden, ob eine Protokolldatei geändert oder gelöscht wurde oder ob sie nach der Übermittlung CloudTrail unverändert geblieben ist. Dieses Feature wurde mit dem Branchenstandard entsprechenden Algorithmen entwickelt: SHA-256 für die Hashfunktion und SHA-256 mit RSA für digitale Signaturen. Aus diesem Grund ist es rechnerisch unmöglich, CloudTrail Protokolldateien unbemerkt zu ändern, zu löschen oder zu fälschen.

Kontroll-ID	AWS Config	Empfehlungen
b-design-and-secureAbschnitt 4 — Die Cloud-14-Standard-Workloads	cw-loggroup-retention-period-überprüfen	Stellen Sie sicher, dass die Ereignisprotokolldaten für Ihre Protokollgruppen über eine Mindestdauer aufbewahrt werden, um die Fehlerbehebung und forensische Untersuchungen zu unterstützen. Fehlende frühere Ereignisprotokolldaten erschweren die Rekonstruierung und Identifizierung potenziell schädlicher Ereignisse.
Abschnitt 4 b-design-and-secure — Die Cloud-14-Standard-Workloads	elasticsearch-logs-to-cloudwatch	Stellen Sie sicher, dass für Amazon OpenSearch Service-Domains Fehlerprotokolle aktiviert und zur Aufbewahrung und Beantwortung an Amazon CloudWatch Logs gestreamt werden. Domain-Fehlerprotokolle sind bei Sicherheits- und Zugriffsprüfungen sowie bei der Diagnose von Verfügbarkeitsproblemen nützlich.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 b-design-and-secure — Die Cloud-14-Standard-Workloads	elb-logging-enabled	Die Elastic-Load-Balancing-Aktivität ist ein zentraler Kommunikationspunkt innerhalb einer Umgebung. Stellen Sie sicher, dass die ELB-Protokollierung aktiviert ist. Die gesammelten Daten enthalten detaillierte Informationen zu Anfragen, die an den ELB gesendet wurden. Jedes Protokoll enthält Informationen wie die Zeit, zu der die Anforderung einging, die Client-IP-Adresse, Latenzen, Anforderungspfade und Serverantworten.
Abschnitt 4 — b-design-and-secure Cloud-14-Standard-Workloads	guardduty-enabled-centralized	Amazon GuardDuty kann mithilfe von Threat Intelligence Feeds helfen, potenzielle Cybersicherheitsereignisse zu überwachen und zu erkennen. Dazu gehören Listen mit bösartigen IPs und maschinellen Lernmethoden zur Identifizierung unerwarteter, nicht autorisierter und bösartiger Aktivitäten in Ihrer AWS Cloud-Umgebung.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 b-design-and-secure — Cloud-14-Standard-Workloads	iam-no-inline-policy-überprüfen	Stellen Sie sicher, dass ein Benutzer, eine IAM-Rolle oder eine IAM-Gruppe (AWS Identity and Access Management) nicht über eine Inline-Richtlinie zur Zugriffskontrolle auf Systeme und Ressourcen verfügt. AWS empfiehlt, verwaltete Richtlinien anstelle von Inline-Richtlinien zu verwenden . Verwaltete Richtlinien ermöglichen Wiederverwendbarkeit, Versionsverwaltung, Rollback und Delegierung der Berechtigungsverwaltung.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 b-design-and-secure — Die Cloud — 14-Standard-Workloads	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) kann Ihnen dabei helfen, die Prinzipien der geringsten Rechte und der Aufgabent rennung in Zugriffsberechtigu ngen und Autorisierungen zu integrieren und so zu verhindern, dass Richtlinien „Effect“: „Allow“ mit „Action“: „*“ anstelle von „Resource“: „*“ enthalten. Wenn Benutzern mehr Rechte eingeräumt werden, als für die Ausführun g einer Aufgabe erforderl ich sind, kann dies gegen das Prinzip der geringste n Berechtigung und der Aufgabentrennung verstoßen.
Abschnitt b-design-and-secur e 4 — Die Cloud-14-Standard-Workloads	iam-user-no-policies-überpr üfen	Diese Regel stellt sicher, dass AWS Identity and Access Management (IAM) -Richtlin ien nur Gruppen oder Rollen zugewiesen werden, um den Zugriff auf Systeme und Ressourcen zu kontrollieren. Die Zuweisung von Berechtig ungen auf Gruppen- oder Rollenebene trägt dazu bei, die Wahrscheinlichkeit zu verringern, dass eine Identität übermäßige Berechtigungen erhält oder beibehält.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 b-design-and-secure — Cloud-14-Standard-Workloads	multi-region-cloudtrail-enabled	AWS CloudTrail zeichnet Aktionen und AWS API-Aufrufe der Management Console auf. Sie können feststellen, welche Benutzer und Konten angerufen wurden AWS, von welcher Quell-IP-Adresse aus die Anrufe getätigt wurden und wann die Anrufe erfolgten. CloudTrail übermittelt Protokolldateien aus allen AWS Regionen an Ihren S3-Bucket, wenn MULTI_REGION_CLOUD_TRAIL_ENABLED aktiviert ist. Außerdem wird beim AWS Start einer neuen Region derselbe Trail in der neuen Region erstellt. CloudTrail Dadurch erhalten Sie automatisch Protokoll dateien mit API-Aktivitäten für die neue Region.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 b-design-and-secure — Cloud-14-Standard-Workloads	opensearch-logs-to-cloudwatch	Stellen Sie sicher, dass für Amazon OpenSearch Service-Domains Fehlerprotokolle aktiviert und zur Aufbewahrung und Beantwortung an Amazon CloudWatch Logs gestreamt werden. OpenSearch Service-Fehlerprotokolle können bei Sicherheits- und Zugriffsprüfungen helfen und bei der Diagnose von Verfügbarkeitsproblemen helfen.
Abschnitt 4 b-design-and-secure — Cloud-14-Standard-Workloads	rds-logging-enabled	Um die Protokollierung und Überwachung in Ihrer Umgebung zu erleichtern, stellen Sie sicher, dass die Amazon Relational Database Service (Amazon RDS)-Protokollierung aktiviert ist. Mit der Amazon-RDS-Protokollierung können Sie Ereignisse wie Verbindungen, Verbindungsabbrüche, Abfragen oder abgefragte Tabellen erfassen.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 — b-design-and-secure Cloud-14-Standard-Workloads	redshift-cluster-configuration-check	Um Daten im Ruhezustand zu schützen, muss die Verschlüsselung für Ihre Amazon-Redshift-Cluster aktiviert sein. Sie müssen auch sicherstellen, dass die erforderlichen Konfigurationen auf Amazon-Redshift-Clustern bereitgestellt werden. Die Prüfungsprotokollierung muss aktiviert sein, um Informationen zu Verbindungen und Benutzeraktivitäten in der Datenbank bereitzustellen. Diese Regel erfordert, dass ein Wert für clusterDbEncrypted (Config Default: TRUE) und LoggingEnabled (Config Default: TRUE) gesetzt ist. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	AWS Config	Empfehlungen
b-design-and-secureAbschnitt 4 — Die Cloud-14-Standard-Workloads	s3- -Blöcke — periodisch account-level-public-access	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Simple Storage Service (Amazon S3) -Buckets nicht öffentlich zugänglich sind. Diese Regel trägt dazu bei, sensible Daten vor unbefugten Remote-Benutzern zu schützen, indem sie den öffentlichen Zugriff verhindert. Mit dieser Regel können Sie optional die Parameter ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) und restrictPublicBuckets Parameter (Config Default: True) festlegen. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 b-design-and-secure — Die Cloud-14-Standard-Workloads	s3- bucket-default-lock-enabled	Stellen Sie sicher, dass für Ihren Amazon Simple Storage Service (Amazon S3)-Bucket standardmäßig eine Sperre aktiviert ist. Zum Schutz eventuell vorhandener sensibler Daten in S3-Bucket s müssen Sie Objektsperren für Daten im Ruhezustand erzwingen.
Abschnitt 4 b-design-and-secure — die Cloud-14-Standard-Workloads	s3- bucket-logging-enabled	Die Amazon Simple Storage Service (Amazon S3)-Serve rzugriffsprotokollierung bietet eine Methode zur Überwachung des Netzwerks im Hinblick auf potenzielle Cybersicherheitsereignisse. Die Ereignisse werden überwacht, indem detaillie rte Aufzeichnungen über die Anfragen erfasst werden, die an einen Amazon-S3-Bucket gestellt wurden. Jeder Zugriffsprotokolleintrag enthält Details zu einer einzelnen Zugriffsanfrage. Zu den Details gehören Anfordere r, Bucket-Name, Anforderu ngszeit, Anforderungsaktion, Antwortstatus und Fehlercode, falls relevant.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 b-design-and-secure — die Cloud-14-Standard-Workloads	s3- bucket-policy-grantee-check	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie s3_bucket_policy_grantee_check aktivieren. Diese Regel prüft, ob der vom Amazon S3 S3-Bucket gewährte Zugriff durch die von Ihnen bereitgestellten AWS Principals, Verbundbenutzer, Service Principals, IP-Adressen oder Amazon Virtual Private Cloud (Amazon VPC) IDs eingeschränkt ist.
Abschnitt 4 — Die Cloud-14-Standard-Workloads b-design-and-secure	s3-aktiviert bucket-server-side-encryption	Zum Schutz von Daten im Ruhezustand müssen Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon Simple Storage Service (Amazon S3)-Buckets aktiviert ist. Um eventuell vorhandene sensible Daten im Ruhezustand in Amazon-S3-Buckets zu schützen, muss die Verschlüsselung aktiviert sein.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 b-design-and-secure — Cloud-14-Standard-Workloads	s3- bucket-versioning-enabled	Die Versionsverwaltung von Amazon Simple Storage Service (Amazon S3)-Buckets hilft dabei, mehrere Varianten eines Objekts im selben Amazon-S3-Bucket zu speichern. Verwenden Sie die Versionsverwaltung, um sämtliche Versionen aller Objekte in Ihrem Amazon-S3-Bucket zu speichern, abzurufen oder wiederher zustellen. Mit der Versionsv erwaltung können Sie Versionen sowohl nach unbeabsichtigten Benutzera ktionen als auch nach Anwendungsfehlern problemlo s wiederherstellen.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 b-design-and-secure — die Cloud-14-Standard-Workloads	securityhub-enabled	AWS Security Hub hilft bei der Überwachung von unbefugte m Personal, Verbindungen, Geräten und Software. AWS Security Hub aggregiert, organisiert und priorisiert die Sicherheitswarnungen oder Ergebnisse mehrerer Dienste. AWS Einige dieser Dienste sind Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer und AWS Firewall Manager sowie AWS Partnerlösungen.
Abschnitt 4 — Cloud-14-Standard-Workloads b-design-and-secure	vpc-flow-logs-enabled	VPC-Flow-Protokolle erfassen detaillierte Informationsdatens ätze über den IP-Datenv erkehr, der zu und von Netzwerkschnittstellen in Ihrer Amazon Virtual Private Cloud (Amazon VPC) fließt. Standardmäßig enthalten Flow-Protokolldatensätze Werte für die verschiedenen Komponenten des IP-Flows, einschließlich Quelle, Ziel und Protokoll.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 — b-design-and-secure Cloud-14-Standard-Workloads	wafv2-logging-enabled	Um die Protokollierung und Überwachung in Ihrer Umgebung zu erleichte rn, aktivieren Sie die AWS WAF (V2) -Protokollierung im regionalen und globalen Web. ACLs AWS Die WAF-Protokollierung bietet detaillie rte Informationen über den Datenverkehr, der von Ihrer Web-ACL analysiert wird. In den Protokollen werden die Uhrzeit aufgezeichnet, zu der die AWS WAF die Anfrage von Ihrer AWS Ressource erhalten hat, Informationen über die Anfrage und eine Aktion für die Regel, der jede Anfrage entsprach.
Abschnitt 4 b-design-and-secure — Die Cloud-14-Standard-Workloads	opensearch-audit-logging-en abled	Stellen Sie sicher, dass die Audit-Protokollierung für Ihre Amazon OpenSearch Service-Domains aktiviert ist. Mit der Audit-Protokollierung können Sie Benutzeraktivitäten auf Ihren OpenSearch Domains verfolgen, einschließlich erfolgreicher und fehlgesch lagener Authentifizierunge n OpenSearch, Anfragen an, Indexänderungen und eingehende Suchanfragen.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 b-design-and-secure — Die Cloud-15-Standard-Workloads	cmk-backing-key-rotation-aktiviert	Aktivieren Sie die Schlüssel rotation, um sicherzustellen, dass Schlüssel rotiert werden, sobald sie das Ende ihrer Kryptoperiode erreicht haben.
Abschnitt 4 b-design-and-secure — Die Cloud-15-Standard-Workloads	dms-replication-not-public	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass auf DMS-Replikationsinstanzen nicht öffentlich zugegriffen werden kann. DMS-Replikations-Instances können vertrauliche Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.
Abschnitt 4 b-design-and-secure — Cloud-15-Standard-Workloads	ebs-snapshot-public-restorable-überprüfen	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass EBS-Snapshots nicht öffentlich wiederherstellbar sind. EBS-Volume-Snapshots können vertrauliche Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	AWS Config	Empfehlungen
b-design-and-secureAbschnitt 4 — Cloud-15-Standard-Workloads	ec2- ebs-encryption-by-default	Zum Schutz von Daten im Ruhezustand müssen Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon Elastic Block Store (Amazon EBS)-Volumes aktiviert ist. Da sensible Daten auch im Ruhezustand vorhanden sein können, sollten Sie die Verschlüsselung im Ruhezustand aktivieren, um diese Daten zu schützen.
Abschnitt 4 b-design-and-secure — Die Cloud-15-Standard-Workloads	efs-encrypted-check	Aktivieren Sie die Verschlüsselung für Ihr Amazon Elastic File System (EFS), um eventuell vorhandene sensible Daten sowie Daten im Ruhezustand zu schützen.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 — b-design-and-secure Cloud-15-Standard-Workloads	elasticsearch-in-vpc-only	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass sich Amazon OpenSearch OpenSearch Service (Service) -Domains innerhalb einer Amazon Virtual Private Cloud (Amazon VPC) befinden. Eine OpenSearch Service-Domain innerhalb einer Amazon VPC ermöglicht die sichere Kommunikation zwischen OpenSearch Service und anderen Services innerhalb der Amazon VPC, ohne dass ein Internet-Gateway, ein NAT-Gerät oder eine VPN-Verbindung erforderlich ist.
Abschnitt 4 — Die Cloud-15-Standard-Workloads b-design-and-secure	encrypted-volumes	Aktivieren Sie die Verschlüsselung für Ihre Amazon-Elastic-Block-Store (Amazon-EBS)-Volumes, um eventuell vorhandene sensible Daten sowie Daten im Ruhezustand zu schützen.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 — b-design-and-secure Cloud-15-Standard-Workloads	kms-cmk-not-scheduled-zum Löschen	Um Daten im Ruhezustand zu schützen, sollten Sie sicherstellen, dass die für den Kunden erforderlichen Masterschlüssel (CMKs) nicht im AWS Key Management Service (AWS KMS) gelöscht werden. Da Schlüssel manchmal gelöscht werden müssen, können Sie mit dieser Regel alle zu löschenden Schlüssel überprüfen, falls ein Schlüssel versehentlich zur Löschung vorgemerkt wurde.
Abschnitt 4 b-design-and-secure — Cloud-15-Standard-Workloads	opensearch-in-vpc-only	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass sich Amazon OpenSearch Service-Domains innerhalb einer Amazon Virtual Private Cloud (Amazon VPC) befinden. Eine Amazon OpenSearch Service-Domain innerhalb einer Amazon VPC ermöglicht die sichere Kommunikation zwischen Amazon OpenSearch Service und anderen Services innerhalb der Amazon VPC, ohne dass ein Internet-Gateway, ein NAT-Gerät oder eine VPN-Verbindung erforderlich ist.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 — Die Cloud-15-Standard-Workloads b-design-and-secure	rds-snapshots-public-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Relational Database Service (Amazon RDS) -Instances nicht öffentlich sind. Amazon-RDS-Datenbank-Instances können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.
Abschnitt 4 b-design-and-secure — Cloud-15-Standard-Workloads	rds-snapshot-encrypted	Stellen Sie sicher, dass die Verschlüsselung für Ihre Amazon Relational Database Service (Amazon RDS)-Snapshots aktiviert ist. Da sensible Daten auch im Ruhezustand vorhanden sein können, sollten Sie die Verschlüsselung von Daten im Ruhezustand aktivieren, um diese Daten zu schützen.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 — b-design-and-secure Cloud-15-Standard-Workloads	s3- -Blöcke — periodisch account-level-public-access	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Simple Storage Service (Amazon S3) -Buckets nicht öffentlich zugänglich sind. Diese Regel trägt dazu bei, sensible Daten vor unbefugten Remote-Benutzern zu schützen, indem sie den öffentlichen Zugriff verhindert. Mit dieser Regel können Sie optional die Parameter ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) und restrictPublicBuckets Parameter (Config Default: True) festlegen. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 b-design-and-secure — Die Cloud-15-Standard-Workloads	s3- bucket-default-lock-enabled	Stellen Sie sicher, dass für Ihren Amazon Simple Storage Service (Amazon S3)-Bucket standardmäßig eine Sperre aktiviert ist. Zum Schutz eventuell vorhandener sensibler Daten in S3-Bucket s müssen Sie Objektsperren für Daten im Ruhezustand erzwingen.
Abschnitt 4 b-design-and-secure — Die Cloud-15-Standard-Workloads	s3- bucket-policy-grantee-check	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie s3_bucket_policy_grantee_check aktivieren. Diese Regel prüft, ob der vom Amazon S3 S3-Bucket gewährte Zugriff durch die von Ihnen bereitgestellten AWS Principals, Verbundbe nutzer, Service Principals, IP-Adressen oder Amazon Virtual Private Cloud (Amazon VPC) IDs eingeschränkt ist.
Abschnitt 4 — Die Cloud-15-Standard-Workloads b-design-and-secure	s3- bucket-public-read-prohibit ed	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie nur autorisie rten Benutzern, Prozessen und Geräten Zugriff auf Amazon Simple Storage Service (Amazon S3) -Buckets gewähren. Die Verwaltung des Zugriffs sollte mit der Klassifiz ierung der Daten übereinst immen.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 b-design-and-secure — Die Cloud-15-Standard-Workloads	s3- bucket-public-write-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie nur autorisierten Benutzern, Prozessen und Geräten Zugriff auf Amazon Simple Storage Service (Amazon S3) -Buckets gewähren. Die Verwaltung des Zugriffs sollte mit der Klassifizierung der Daten übereinstimmen.
Abschnitt 4 b-design-and-secure — Die Cloud-15-Standard-Workloads	s3-aktiviert bucket-server-side-encryption	Zum Schutz von Daten im Ruhezustand müssen Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon Simple Storage Service (Amazon S3)-Buckets aktiviert ist. Um eventuell vorhandene sensible Daten im Ruhezustand in Amazon-S3 -Buckets zu schützen, muss die Verschlüsselung aktiviert sein.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 b-design-and-secure — Die Cloud-15-Standard-Workloads	s3- bucket-versioning-enabled	Die Versionsverwaltung von Amazon Simple Storage Service (Amazon S3)-Buckets hilft dabei, mehrere Varianten eines Objekts im selben Amazon-S3-Bucket zu speichern. Verwenden Sie die Versionsverwaltung, um sämtliche Versionen aller Objekte in Ihrem Amazon-S3-Bucket zu speichern, abzurufen oder wiederher zustellen. Mit der Versionsv erwaltung können Sie Versionen sowohl nach unbeabsichtigten Benutzera ktionen als auch nach Anwendungsfehlern problemlo s wiederherstellen.
Abschnitt 4 b-design-and-secure — Die Cloud-15-Standard-Workloads	s3- default-encryption-kms	Stellen Sie sicher, dass die Verschlüsselung für Ihre Amazon Simple Storage Service (Amazon S3)-Bucke ts aktiviert ist. Um eventuell vorhandene sensible Daten im Ruhezustand in einem Amazon-S3-Bucket zu schützen, muss die Verschlüs selung aktiviert sein.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 -1- Standard-Workloads c-run-the-cloud	cloudtrail-enabled	AWS CloudTrail kann durch die Aufzeichnung von Aktionen und API-Aufrufen der Management Console bei der Nichtabstreitbarkeit helfen. AWS Sie können die Benutzer und die Benutzer AWS-Konten , die einen AWS Dienst aufgerufen haben, die Quell-IP-Adresse, über die die Aufrufe generiert wurden, und den Zeitpunkt der Anrufe identifizieren. Einzelheiten zu den erfassten Daten finden Sie unter Inhalt des AWS CloudTrail Datensatzes.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 c-run-the-cloud — 2 — Standard-Workloads	cloudwatch-alarm-action-check	Amazon CloudWatch alarmiert, wenn eine Metrik den Schwellenwert für eine bestimmte Anzahl von Bewertungszeiträumen überschreitet. Der Alarm führt eine oder mehrere Aktionen durch, die vom Wert der Metrik oder des Ausdrucks im Vergleich zu einem Schwellenwert in einer Reihe von Zeiträumen abhängt. Diese Regel erfordert einen Wert für alarmActionRequired (Config Default: True), insufficientDataActionRequired (Config Default: True), okActionRequired (Config Default: False). Der tatsächliche Wert muss die Alarmaktionen für Ihre Umgebung widerspiegeln.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 c-run-the-cloud — 2 — Standard-Workloads	guardduty-enabled-centralized	Amazon GuardDuty kann mithilfe von Threat Intellige nce Feeds helfen, potenzielle Cybersicherheitsereignisse zu überwachen und zu erkennen. Dazu gehören Listen mit bösartigen IPs und maschinel len Lernmethoden zur Identifiz ierung unerwarteter, nicht autorisierter und bösartige r Aktivitäten in Ihrer AWS Cloud-Umgebung.
Abschnitt 4 c-run-the-cloud — 2 — Standard-Workloads	iam-group-has-users-überprü fen	AWS Identity and Access Management (IAM) kann Ihnen helfen, die Prinzipien der geringsten Rechte und der Aufgabentrennung mit Zugriffsberechtigungen und Autorisierungen zu integrier en, indem sichergestellt wird, dass IAM-Gruppen mindesten s einen Benutzer haben. Die Einteilung von Benutzern in Gruppen auf der Grundlage der ihnen zugewiesenen Berechtigungen oder ihrer Funktion ist eine Möglichke it, das Prinzip der geringste n Berechtigung zu implement ieren.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 — 2 — Standard-Workloads c-run-the-cloud	iam-no-inline-policy-überprüfen	Stellen Sie sicher, dass ein Benutzer, eine IAM-Rolle oder eine IAM-Gruppe (AWS Identity and Access Management) nicht über eine Inline-Richtlinie zur Zugriffskontrolle auf Systeme und Ressourcen verfügt. AWS empfiehlt, verwaltete Richtlinien anstelle von Inline-Richtlinien zu verwenden . Verwaltete Richtlinien ermöglichen Wiederverwendbarkeit, Versionsverwaltung, Rollback und Delegierung der Berechtigungsverwaltung.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 c-run-the-cloud — 2 — Standard-Workloads	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) kann Ihnen dabei helfen, die Prinzipien der geringsten Rechte und der Aufgabent rennung in Zugriffsberechtigu ngen und Autorisierungen zu integrieren und so zu verhindern, dass Richtlinien „Effect“: „Allow“ mit „Action“: „*“ anstelle von „Resource“: „*“ enthalten. Wenn Benutzern mehr Rechte eingeräumt werden, als für die Ausführun g einer Aufgabe erforderl ich sind, kann dies gegen das Prinzip der geringste n Berechtigung und der Aufgabentrennung verstoßen.
Abschnitt c-run-the-cloud 4 -2 Standard-Workloads	iam-policy-no-statements-with-full-access	Stellen Sie sicher, dass IAM-Aktionen nur auf die benötigte n Aktionen beschränkt sind. Wenn Benutzern mehr Rechte eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und der Aufgabentrennung verstoßen.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 - c-run-the-cloud 2 - Standard-Workloads	iam-root-access-key-überprüfen	Der Zugriff auf Systeme und Ressourcen kann gesteuert werden, indem überprüft wird, ob der Root-Benutzer keine Zugriffsschlüssel mit seiner AWS Identity and Access Management (IAM) -Rolle verknüpft hat. Stellen Sie sicher, dass die Root-Zugriffsschlüssel gelöscht werden. Erstellen und verwenden Sie stattdessen rollenbasierte Funktionen, AWS-Konten um das Prinzip der geringsten Funktionalität zu berücksichtigen.
Abschnitt 4 — 2 — Standard-Workloads c-run-the-cloud	iam-user-group-membership-überprüfen	AWS Identity and Access Management (IAM) kann Ihnen helfen, Zugriffsberechtigungen und Autorisierungen einzuschränken, indem sichergestellt wird, dass Benutzer Mitglieder mindestens einer Gruppe sind. Wenn Benutzern mehr Berechtigungen eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und Aufgabentrennung verstoßen.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 — 2 — Standard-Workloads c-run-the-cloud	iam-user-no-policies-überprüfen	Diese Regel stellt sicher, dass AWS Identity and Access Management (IAM) -Richtlinien nur Gruppen oder Rollen zugewiesen werden, um den Zugriff auf Systeme und Ressourcen zu kontrollieren. Die Zuweisung von Berechtigungen auf Gruppen- oder Rollenebene trägt dazu bei, die Wahrscheinlichkeit zu verringern, dass eine Identität übermäßige Berechtigungen erhält oder beibehält.
Abschnitt 4 c-run-the-cloud — 2 — Standard-Workloads	securityhub-enabled	AWS Security Hub hilft bei der Überwachung von unbefugtem Personal, Verbindungen, Geräten und Software. AWS Security Hub aggregiert, organisiert und priorisiert die Sicherheitswarnungen oder Ergebnisse mehrerer Dienste. AWS Einige dieser Dienste sind Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer und AWS Firewall Manager sowie AWS Partnerlösungen.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 — 3-Standard-Workloads c-run-the-cloud	api-gw-execution-logging-aktiviert	Die API-Gateway-Protokollierung zeigt detaillierte Ansichten der Benutzer, die auf die API zugegriffen haben, und wie diese Benutzer auf die API zugegriffen haben. Diese Einblicke ermöglichen die Transparenz von Benutzeraktivitäten.
Abschnitt 4 c-run-the-cloud -3-Standard-Workloads	cloudtrail-s3-dataevents-enabled	Die Erfassung von Simple Storage Service (Amazon S3)-Datenereignissen unterstützt die Erkennung von ungewöhnlichen Aktivitäten. Zu den Details gehören Informationen zu dem AWS -Konto, das auf einen Amazon-S3-Bucket zugegriffen hat, die IP-Adresse und die Uhrzeit des Ereignisses.
Abschnitt 4 c-run-the-cloud -3-Standard-Workloads	cloudtrail-security-trail-enabled	Diese Regel hilft sicherzustellen, dass die AWS empfohlenen bewährten Sicherheitsmethoden für verwendet werden AWS CloudTrail, indem geprüft wird, ob mehrere Einstellungen aktiviert sind. Dazu gehören die Verwendung von Protokollverschlüsselung, Protokollvalidierung und Aktivierung AWS CloudTrail in mehreren Regionen.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 c-run-the-cloud -3-Standard-Workloads	cloudwatch-alarm-action-check	Amazon CloudWatch alarmiert , wenn eine Metrik den Schwellenwert für eine bestimmte Anzahl von Bewertungszeiträumen überschreitet. Der Alarm führt eine oder mehrere Aktionen durch, die vom Wert der Metrik oder des Ausdrucks im Vergleich zu einem Schwellenwert in einer Reihe von Zeiträumen abhängt. Diese Regel erfordert einen Wert für alarmActionRequired (Config Default: True), insufficientDataActionRequired (Config Default: True), okActionRequired (Config Default: False). Der tatsächliche Wert muss die Alarmaktionen für Ihre Umgebung widerspiegeln.
Abschnitt 4 c-run-the-cloud — 3-Standard-Workloads	cloud-trail-cloud-watch-logs-aktiviert	Verwenden Sie Amazon CloudWatch , um Protokoll ereignisaktivitäten zentral zu sammeln und zu verwalten . Die Aufnahme von AWS CloudTrail Daten liefert Einzelheiten zu den API-Aufrufaktivitäten in Ihrem AWS-Konto.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 c-run-the-cloud -3-Standard-Workloads	cloudtrail-enabled	AWS CloudTrail kann durch die Aufzeichnung von Aktionen und API-Aufrufen in der Management Console bei der Nichtabstreitbarkeit helfen. AWS Sie können die Benutzer und die Benutzer AWS-Konten , die einen AWS Dienst aufgerufen haben, die Quell-IP-Adresse, über die die Aufrufe generiert wurden, und den Zeitpunkt der Anrufe identifizieren. Einzelheiten zu den erfassten Daten finden Sie unter Inhalt des AWS CloudTrail Datensatzes.
Abschnitt 4 c-run-the-cloud -3-Standard-Workloads	cloud-trail-encryption-enabled	Zum Schutz von eventuell vorhandenen sensiblen Daten sowie Daten im Ruhezusta nd müssen Sie sicherstellen, dass die Verschlüsselung für Ihre AWS CloudTrail aktiviert ist.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 c-run-the-cloud -3-Standard-Workloads	cloud-trail-log-file-Validierung aktiviert	Verwenden Sie die AWS CloudTrail Protokolldateivalidierung, um die Integrität von Protokollen zu überprüfen. CloudTrail Mithilfe der Protokolldateivalidierung kann festgestellt werden, ob eine Protokolldatei geändert oder gelöscht wurde oder ob sie nach der Übermittlung CloudTrail unverändert geblieben ist. Dieses Feature wurde mit dem Branchenstandard entsprechenden Algorithmen entwickelt: SHA-256 für die Hashfunktion und SHA-256 mit RSA für digitale Signaturen. Aus diesem Grund ist es rechnerisch unmöglich, CloudTrail Protokolldateien unbemerkt zu ändern, zu löschen oder zu fälschen.

Kontroll-ID	AWS Config	Empfehlungen
c-run-the-cloudAbschnitt 4-3-Standard-Workloads	elasticsearch-logs-to-cloudwatch	Stellen Sie sicher, dass für Amazon OpenSearch Service-Domains Fehlerprotokolle aktiviert und zur Aufbewahrung und Beantwortung an Amazon CloudWatch Logs gestreamt werden. Domain-Fehlerprotokolle sind bei Sicherheits- und Zugriffsprüfungen sowie bei der Diagnose von Verfügbarkeitsproblemen nützlich.
Abschnitt 4 c-run-the-cloud — 3 — Standard-Workloads	elb-logging-enabled	Die Elastic-Load-Balancing-Aktivität ist ein zentraler Kommunikationspunkt innerhalb einer Umgebung. Stellen Sie sicher, dass die ELB-Protokollierung aktiviert ist. Die gesammelten Daten enthalten detaillierte Informationen zu Anfragen, die an den ELB gesendet wurden. Jedes Protokoll enthält Informationen wie die Zeit, zu der die Anforderung einging, die Client-IP-Adresse, Latenzen, Anforderungspfade und Serverantworten.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 c-run-the-cloud -3-Standard-Workloads	guardduty-enabled-centralized	Amazon GuardDuty kann mithilfe von Threat Intellige nce Feeds helfen, potenzielle Cybersicherheitsereignisse zu überwachen und zu erkennen. Dazu gehören Listen mit bösartigen IPs und maschinel len Lernmethoden zur Identifiz ierung unerwarteter, nicht autorisierter und bösartige r Aktivitäten in Ihrer AWS Cloud-Umgebung.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4-3-Standard-Workloads c-run-the-cloud	multi-region-cloudtrail-enabled	AWS CloudTrail zeichnet Aktionen AWS und API-Aufrufe der Management Console auf. Sie können feststellen, welche Benutzer und Konten angerufen wurden AWS, von welcher Quell-IP-Adresse aus die Anrufe getätigt wurden und wann die Anrufe erfolgten. CloudTrail übermittelt Protokolldateien aus allen AWS Regionen an Ihren S3-Bucket, wenn MULTI_REGION_CLOUD_TRAIL_ENABLED aktiviert ist. Außerdem wird beim AWS Start einer neuen Region derselbe Trail in der neuen Region erstellt. CloudTrail Dadurch erhalten Sie automatisch Protokoll dateien mit API-Aktivitäten für die neue Region.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4-3-Standard-Workloads c-run-the-cloud	opensearch-logs-to-cloudwatch	Stellen Sie sicher, dass für Amazon OpenSearch Service-Domains Fehlerprotokolle aktiviert und zur Aufbewahrung und Beantwortung an Amazon CloudWatch Logs gestreamt werden. OpenSearch Service-Fehlerprotokolle können bei Sicherheits- und Zugriffsprüfungen helfen und bei der Diagnose von Verfügbarkeitsproblemen helfen.
Abschnitt 4-3-Standard-Workloads c-run-the-cloud	rds-logging-enabled	Um die Protokollierung und Überwachung in Ihrer Umgebung zu erleichtern, stellen Sie sicher, dass die Amazon Relational Database Service (Amazon RDS)-Protokollierung aktiviert ist. Mit der Amazon-RDS-Protokollierung können Sie Ereignisse wie Verbindungen, Verbindungsabbrüche, Abfragen oder abgefragte Tabellen erfassen.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 c-run-the-cloud -3-Standard-Workloads	redshift-cluster-configuration-check	Um Daten im Ruhezustand zu schützen, muss die Verschlüsselung für Ihre Amazon-Redshift-Cluster aktiviert sein. Sie müssen auch sicherstellen, dass die erforderlichen Konfigurationen auf Amazon-Redshift-Clustern bereitgestellt werden. Die Prüfungsprotokollierung muss aktiviert sein, um Informationen zu Verbindungen und Benutzeraktivitäten in der Datenbank bereitzustellen. Diese Regel erfordert, dass ein Wert für clusterDbEncrypted (Config Default: TRUE) und LoggingEnabled (Config Default: TRUE) gesetzt ist. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 — 3-Standard-Workloads c-run-the-cloud	s-3 bucket-logging-enabled	Die Amazon Simple Storage Service (Amazon S3)-Serverzugriffsprotokollierung bietet eine Methode zur Überwachung des Netzwerks im Hinblick auf potenzielle Cybersicherheitsereignisse. Die Ereignisse werden überwacht, indem detaillierte Aufzeichnungen über die Anfragen erfasst werden, die an einen Amazon-S3-Bucket gestellt wurden. Jeder Zugriffsprotokolleintrag enthält Details zu einer einzelnen Zugriffsanfrage. Zu den Details gehören Anforderer, Bucket-Name, Anforderungszeit, Anforderungsaktion, Antwortstatus und Fehlercode, falls relevant.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 c-run-the-cloud -3-Standard-Workloads	securityhub-enabled	AWS Security Hub hilft bei der Überwachung von unbefugte m Personal, Verbindungen, Geräten und Software. AWS Security Hub aggregiert, organisiert und priorisiert die Sicherheitswarnungen oder Ergebnisse mehrerer Dienste. AWS Einige dieser Dienste sind Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer und AWS Firewall Manager sowie AWS Partnerlösungen.
Abschnitt 4 — 3-Standard-Workloads c-run-the-cloud	vpc-flow-logs-enabled	VPC-Flow-Protokolle erfassen detaillierte Informationsdatens ätze über den IP-Datenv erkehr, der zu und von Netzwerkschnittstellen in Ihrer Amazon Virtual Private Cloud (Amazon VPC) fließt. Standardmäßig enthalten Flow-Protokolldatensätze Werte für die verschiedenen Komponenten des IP-Flows, einschließlich Quelle, Ziel und Protokoll.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 c-run-the-cloud -3-Standard-Workloads	wafv2-logging-enabled	Um Ihnen bei der Protokoll ierung und Überwachung in Ihrer Umgebung zu helfen, aktivieren Sie die AWS WAF (V2) -Protokollierung im regionalen und globalen Web. ACLs AWS Die WAF-Protokollierung bietet detaillie rte Informationen über den Datenverkehr, der von Ihrer Web-ACL analysiert wird. In den Protokollen werden die Uhrzeit aufgezeichnet, zu der die AWS WAF die Anfrage von Ihrer AWS Ressource erhalten hat, Informationen über die Anfrage und eine Aktion für die Regel, der jede Anfrage entsprach.
Abschnitt 4-3-Standard-Workl oads c-run-the-cloud	opensearch-audit-logging-en abled	Stellen Sie sicher, dass die Audit-Protokollierung für Ihre Amazon OpenSearch Service-Domains aktiviert ist. Mit der Audit-Protokollierung können Sie Benutzeraktivitäten auf Ihren OpenSearch Domains verfolgen, einschließlich erfolgreicher und fehlgesch lagener Authentifizierunge n OpenSearch, Anfragen an, Indexänderungen und eingehende Suchanfragen.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 c-run-the-cloud — 4-Standard-Workloads	response-plan-exists-maintained (Prozessüberprüfung)	Stellen Sie sicher, dass Vorfallreaktionspläne erstellt, verwaltet und an das verantwortliche Personal verteilt werden.
Abschnitt 4 c-run-the-cloud — 5 — Standard-Workloads	autoscaling-group-elb-healthcheck-erforderlich	Die Elastic Load Balancer (ELB) -Zustandsprüfungen für Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling Scaling-Gruppen unterstützen die Aufrechterhaltung einer angemessenen Kapazität und Verfügbarkeit. Der Load Balancer sendet regelmäßig Pings, versucht Verbindungen herzustellen oder sendet Anfragen, um den Zustand der EC2 Amazon-Instances in einer Gruppe mit auto-scaling zu testen. Wenn eine Instance nicht zurückmeldet, wird der Traffic an eine neue EC2 Amazon-Instance gesendet.
Abschnitt 4 c-run-the-cloud — 5 — Standard-Workloads	cloud-trail-cloud-watch-logs-aktiviert	Verwenden Sie Amazon CloudWatch , um Protokoll ereignisaktivitäten zentral zu sammeln und zu verwalten . Die Aufnahme von AWS CloudTrail Daten liefert Einzelheiten zu den API-Aufrufaktivitäten in Ihrem AWS-Konto.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 c-run-the-cloud — 5 — Standard-Workloads	dynamodb-autoscaling-enabled	Amazon DynamoDB Auto Scaling verwendet den AWS Application Auto Scaling-Service, um die bereitgestellte Durchsatzkapazität so anzupassen, dass sie automatisch auf tatsächliche Verkehrsmuster reagiert. Auf diese Weise kann eine Tabelle oder ein globaler sekundärer Index die bereitgestellte Lese-/Schreibkapazität erhöhen, um plötzliche Erhöhungen des Datenverkehrs ohne Drosselung zu bewältigen.

Kontroll-ID	AWS Config	Empfehlungen
c-run-the-cloudAbschnitt 4 — 5 — Standard-Workloads	dynamodb-throughput-limit-check	Aktivieren Sie diese Regel, um sicherzustellen, dass die bereitgestellte Durchsatz kapazität in Ihren Amazon-DynamoDB-Tabellen überprüft wird. Dies ist der Umfang der Lese- und Schreibaktivitäten, der von den jeweiligen Tabellen unterstützt werden kann. DynamoDB verwendet diese Informationen für das Reservieren ausreichender Systemressourcen, um Ihren Durchsatzanforderungen gerecht zu werden. Diese Regel generiert eine Warnung, wenn sich der Durchsatz dem Höchstlimit für ein Kundenkonto nähert. Mit dieser Regel können Sie optional die Parameter RCUThreshold Kontoprozentsatz (Konfigurationsstandard: 80) und WCUThreshold Kontoprozentsatz (Konfigurationsstandard: 80) festlegen. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 c-run-the-cloud — 5 — Standard-Workloads	ec2- instance-detailed-monitoring-enabled	Aktivieren Sie diese Regel, um die Amazon Elastic Compute Cloud (Amazon EC2) -Instance-Überwachung auf der EC2 Amazon-Konsole zu verbessern, in der Monitoring-Diagramme mit einem Zeitraum von 1 Minute für die Instance angezeigt werden.
Abschnitt 4 c-run-the-cloud — 5 — Standard-Workloads	lambda-concurrency-check	Diese Regel stellt sicher, dass die Höchst- und Untergrenzen für die Gleichzeitigkeit einer Lambda-Funktion festgelegt werden. Dies kann Sie beim Baselining für die Anzahl der Anforderungen unterstützen, die Ihre Funktion zu einem bestimmten Zeitpunkt verarbeitet.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 — c-run-the-cloud 5 — Standard-Workloads	rds-enhanced-monitoring-enabled	Aktivieren Sie Amazon Relational Database Service (Amazon RDS), um die Verfügbarkeit von Amazon RDS zu überwachen. Dies bietet einen detaillierten Einblick in den Zustand Ihrer Amazon-RDS-Datenbank-Instances. Wenn der Amazon-RDS-Speicher mehr als ein zugrunde liegendes physisches Gerät verwendet, erfasst Enhanced Monitoring die Daten für jedes Gerät. Wenn die Datenbank-Instance von Amazon RDS in einer Multi-AZ-Bereitstellung ausgeführt wird, werden außerdem die Daten für jedes Gerät auf dem sekundären Host sowie die Metriken des sekundären Hosts erfasst.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 — c-run-the-cloud 5 — Standard-Workloads	beanstalk-enhanced-health-reporting-aktiviert	AWS Die verbesserte Zustandsberichterstattung von Elastic Beanstalk ermöglicht eine schnellere Reaktion auf Veränderungen im Zustand der zugrunde liegenden Infrastruktur. Diese Änderungen könnten zu einer mangelnden Verfügbarkeit der Anwendung führen. Die erweiterten Zustandsberichte von Elastic Beanstalk bieten eine Statusbeschreibung, um den Schweregrad der identifizierten Probleme einzuschätzen und mögliche Ursachen zu identifizieren, die untersucht werden müssen.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 — 6 — Standard-Workloads c-run-the-cloud	ec2-manager instance-managed-by-systems	Eine Bestandsaufnahme der Softwareplattformen und Anwendungen innerhalb des Unternehmens ist möglich, indem Amazon Elastic Compute Cloud (Amazon EC2) -Instances mit AWS Systems Manager verwaltet werden. Verwenden Sie AWS Systems Manager, um detaillierte Systemkonfigurationen, Betriebssystem-Patch-Levels, Namen und Typ der Dienste, Softwareinstallationen, Anwendungsname, Herausgeber und Version sowie andere Details zu Ihrer Umgebung bereitzustellen.
Abschnitt 4 c-run-the-cloud — 6 — Standard-Workloads	ec2- prüfen managedinstance-patch-compliance-status	Aktivieren Sie diese Regel, um bei der Identifizierung und Dokumentation von Sicherheitslücken in Amazon Elastic Compute Cloud (Amazon EC2) zu helfen. Die Regel prüft, ob die EC2 Amazon-Instance die Patch-Konformität im AWS Systems Manager gemäß den Richtlinien und Verfahren Ihrer Organisation einhält.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 c-run-the-cloud — 6 — Standard-Workloads	redshift-cluster-maintenancesettings-check	Diese Regel stellt sicher, dass Amazon-Redshift-Cluster die bevorzugten Einstellungen für Ihre Organisation haben. Insbesondere sorgt sie dafür, dass Cluster bevorzugte Wartungsfenster und automatisierte Aufbewahrungsfristen für Snapshots für die Datenbank haben. Für diese Regel müssen Sie die festlegen. allowVersionUpgrade Der Standardwert ist „true“. Außerdem können Sie optional den Zeitraum preferredMaintenanceWindow (der Standardwert ist sa: 16:00 -sa: 16:30) und den automatedSnapshotRetention Zeitraum (der Standardwert ist 1) festlegen. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	AWS Config	Empfehlungen
Abschnitt 4 — 6 — Standard-Workloads c-run-the-cloud	elastic-beanstalk-managed-updates-aktiviert	Durch die Aktivierung verwalteter Plattformupdates für eine Amazon-Elastic-Beanstalk-Umgebung wird sichergestellt, dass die aktuellen verfügbaren Plattform-Fixes, -Updates und -Features für die Umgebung installiert sind. Eine bewährte Methode zur Sicherung von Systemen besteht darin, stets die aktuellen Patches zu installieren.

Vorlage

Die Vorlage ist verfügbar unter GitHub: Operational Best Practices for ABS CCIG 2.0 Standard Workloads.

Bewährte Methoden für die Implementierung von ACSC Essential 8

Konformitätspakete bieten ein allgemeines Compliance-Framework, das es Ihnen ermöglicht, mithilfe verwalteter oder benutzerdefinierter AWS Config Regeln und Abhilfemaßnahmen Kontrollen zur Sicherheits-, Betriebs- oder Kostenoptimierung durchzuführen. AWS Config Conformance Packs dienen als Beispielvorlagen nicht dazu, die vollständige Einhaltung eines bestimmten Governance- oder Compliance-Standards sicherzustellen. Sie sind dafür verantwortlich, selbst zu beurteilen, ob Ihre Nutzung der Services den geltenden gesetzlichen und behördlichen Anforderungen entspricht.

Im Folgenden finden Sie ein Beispiel für eine Zuordnung zwischen dem Essential Eight Maturity Model des Australian Cyber Security Centre (ACSC) und AWS verwalteten Konfigurationsregeln. Jede Config-Regel gilt für eine bestimmte AWS Ressource und bezieht sich auf eine oder mehrere ACSC Essential Eight-Kontrollen. Eine ACSC-Essential-Eight-Kontrolle kann mehreren Konfigurationsregeln zugeordnet werden. In der folgenden Tabelle finden Sie weitere Informationen und Anleitungen zu diesen Zuordnungen. Einige der Zuordnungen zu Konfigurationsregeln beziehen

sich auf den Abschnitt höherer Ordnung (z. B. Abhilfemaßnahmen zur Begrenzung des Ausmaßes von Cybersicherheitsvorfällen) im Gegensatz zu den stärker präskriptiven Abschnitten.

Diese Vorlage für ein Konformitätspaket enthält Zuordnungen zu Kontrollen innerhalb von ACSC Essential 8, das vom Commonwealth of Australia erstellt wurde und unter ACSC | Essential Eight zu finden ist. Die Lizenzierung des Frameworks unter der Creative Commons Namensnennung 4.0 Internationale öffentliche Lizenz und Informationen zum Urheberrecht für das Framework (einschließlich eines Gewährleistungsausschlusses) finden Sie unter ACSC | Copyright.

Kontroll-ID	AWS Config	Empfehlungen
Application_control	alb-waf-enabled	Stellen Sie sicher, dass AWS WAF auf Elastic Load Balancers (ELB) aktiviert ist, um Webanwendungen zu schützen. Eine WAF trägt zum Schutz Ihrer Webanwend ungen oder APIs vor gängigen Web-Exploits bei. Diese Web-Exploits können sich auf die Verfügbarkeit auswirken, die Sicherheit gefährden oder übermäßige Ressourcen in Ihrer Umgebung verbrauchen.
Application_control	api-gw-associated-with-WAF	AWS Mit WAF können Sie eine Reihe von Regeln (als Web Access Control List (Web ACL) bezeichnet) konfiguri eren, die Webanfragen auf der Grundlage von anpassbar en Websicherheitsregeln und -bedingungen, die Sie definieren, zulassen, blockiere n oder zählen. Stellen Sie sicher, dass Ihre Amazon-API-Gateway-Stufe mit einer WAF-

Kontroll-ID	AWS Config	Empfehlungen
		Web-ACL verknüpft ist, um sie vor böswilligen Angriffen zu schützen.
Application_control	ec2-manager instance-managed-by-systems	Eine Bestandsaufnahme der Softwareplattformen und Anwendungen innerhalb des Unternehmens ist möglich, indem Amazon Elastic Compute Cloud (Amazon EC2) -Instances mit AWS Systems Manager verwaltet werden. Verwenden Sie AWS Systems Manager, um detaillierte Systemkonfigurationen, Betriebssystem-Patch-Levels, Namen und Typ der Dienste, Softwareinstallationen, Anwendungsname, Herausgeber und Version sowie andere Details zu Ihrer Umgebung bereitzustellen.
Application_control	waf-regional-rule-not-leer	Stellen Sie sicher, dass Ihre AWS WAF eine Regel hat, die nicht leer ist. Eine Regel ohne Bedingungen kann zu unbeabsichtigtem Verhalten führen.

Kontroll-ID	AWS Config	Empfehlungen
Application_control	waf-regional-rulegroup-not-leer	Stellen Sie sicher, dass Ihre AWS WAF eine Regelgrup pe hat, die nicht leer ist. Eine leere Regelgruppe kann zu unbeabsichtigtem Verhalten führen.
Application_control	waf-regional-webacl-not-leer	Eine an eine AWS WAF angehängte Web-ACL kann eine Sammlung von Regeln und Regelgruppen zur Überprüfung und Steuerung von Webanfragen enthalten . Wenn eine Web-ACL leer ist, wird der Webdatenverkehr weitergeleitet, ohne von der WAF erkannt oder bearbeitet zu werden.
Application_control	ec2-check managedinstance-association-compliance-status	Verwenden Sie AWS Systems Manager Associations, um bei der Inventarisierung von Softwareplattformen und Anwendungen innerhalb eines Unternehmens zu helfen. AWS Systems Manager weist Ihren verwalteten Instances einen Konfigurationsstatus zu und ermöglicht es Ihnen, Basiswerte für Betriebss ystem-Patch-Levels, Softwarei nstallationen, Anwendung skonfigurationen und andere Details zu Ihrer Umgebung festzulegen.

Kontroll-ID	AWS Config	Empfehlungen
Patch_applications	ec2-imdsv2-check	Stellen Sie sicher, dass die Methode Instance Metadata Service Version 2 (IMDSv2) aktiviert ist, um den Zugriff auf und die Kontrolle der Amazon Elastic Compute Cloud (Amazon EC2) -Instance-Metadaten zu schützen. Die IMDSv2 Methode verwendet sitzungsbasierte Kontrolle n. Mit können Kontrollen implementiert werden IMDSv2, um Änderungen an Instanzme tadaten einzuschränken.
Patch_applications	ec2-manager instance-managed-by-systems	Eine Bestandsaufnahme der Softwareplattformen und Anwendungen innerhalb des Unternehmens ist möglich, indem Amazon Elastic Compute Cloud (Amazon EC2) -Instances mit AWS Systems Manager verwaltet werden. Verwenden Sie AWS Systems Manager, um detaillierte Systemkonfiguratio nen, Betriebssystem-Patch-Levels, Namen und Typ der Dienste, Softwareinstallati onen, Anwendungsname, Herausgeber und Version sowie andere Details zu Ihrer Umgebung bereitzustellen.

Kontroll-ID	AWS Config	Empfehlungen
Patch_applications	ecs-fargate-latest-platform-Version	Sicherheitsupdates und Patches werden automatis ch für Ihre AWS Fargate-Aufgaben bereitgestellt. Wenn ein Sicherheitsproblem gefunden wird, das eine AWS Fargate-Plattformversion betrifft, AWS wird die Plattform version gepatcht. Um Sie bei der Patchverwaltung Ihrer Amazon Elastic Container Service (ECS) -Aufgaben zu unterstützen, auf denen AWS Fargate ausgeführt wird, aktualisieren Sie Ihre eigenständigen Service-Aufgaben, sodass sie die neueste Plattformversion verwenden.
Patch_applications	elastic-beanstalk-managed-updates-aktiviert	Durch die Aktivierung verwalteter Plattformupdates für eine Amazon-Elastic-Beanstalk-Umgebung wird sichergestellt, dass die aktuellen verfügbaren Plattform-Fixes, -Updates und -Features für die Umgebung installiert sind. Eine bewährte Methode zur Sicherung von Systemen besteht darin, stets die aktuellen Patches zu installieren.

Kontroll-ID	AWS Config	Empfehlungen
Patch_applications	rds-automatic-minor-version-upgrade-fähig	Aktivieren Sie automatische Unterversions-Upgrades auf Ihren Amazon-Relational-Database-Service (RDS)-Instances, um sicherzustellen, dass die aktuellen Updates für Unterversionen des Relational Database Management System (RDBMS) installiert sind, die Sicherheitspatches und Bugfixes enthalten können.
Patch_applications	ec2- prüfen managedinstance-association-compliance-status	Verwenden Sie AWS Systems Manager Associations, um bei der Inventarisierung von Softwareplattformen und Anwendungen innerhalb eines Unternehmens zu helfen. AWS Systems Manager weist Ihren verwalteten Instances einen Konfigurationsstatus zu und ermöglicht es Ihnen, Basiswerte für Betriebssystem-Patch-Levels, Softwareinstallationen, Anwendungskonfigurationen und andere Details zu Ihrer Umgebung festzulegen.

Kontroll-ID	AWS Config	Empfehlungen
Patch_applications	redshift-cluster-maintenancesettings-check	Diese Regel stellt sicher, dass Amazon-Redshift-Cluster die bevorzugten Einstellungen für Ihre Organisation haben. Insbesondere sorgt sie dafür, dass Cluster bevorzugte Wartungsfenster und automatisierte Aufbewahrungsfristen für Snapshots für die Datenbank haben. Für diese Regel müssen Sie die festlegen allowVersionUpgrade. Der Standardwert ist „true“. Außerdem können Sie optional den Zeitraum preferredMaintenanceWindow (der Standardwert ist sa: 16:00 -sa: 16:30) und den automatedSnapshotRetention Zeitraum (der Standardwert ist 1) festlegen. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	AWS Config	Empfehlungen
Restrict_administrative_privileges	iam-no-inline-policy-überprüfen	Stellen Sie sicher, dass ein Benutzer, eine IAM-Rolle oder eine IAM-Gruppe (AWS Identity and Access Management) nicht über eine Inline-Richtlinie zur Zugriffskontrolle auf Systeme und Ressourcen verfügt. AWS empfiehlt, verwaltete Richtlinien anstelle von Inline-Richtlinien zu verwenden . Verwaltete Richtlinien ermöglichen Wiederverwendbarkeit, Versionsverwaltung, Rollback und Delegierung der Berechtigungsverwaltung.

Kontroll-ID	AWS Config	Empfehlungen
Restrict_administrative_privileges	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) kann Ihnen dabei helfen, die Prinzipien der geringsten Rechte und der Aufgabentrennung in Zugriffsberechtigungen und Autorisierungen zu integrieren und so zu verhindern, dass Richtlinien „Effect“: „Allow“ mit „Action“: „*“ anstelle von „Resource“: „*“ enthalten. Wenn Benutzern mehr Rechte eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und der Aufgabentrennung verstoßen.

Kontroll-ID	AWS Config	Empfehlungen
Restrict_administrative_privileges	iam-root-access-key-überprüfen	Der Zugriff auf Systeme und Ressourcen kann gesteuert werden, indem überprüft wird, ob der Root-Benutzer keine Zugriffsschlüssel mit seiner AWS Identity and Access Management (IAM) -Rolle verknüpft hat. Stellen Sie sicher, dass die Root-Zugriffsschlüssel gelöscht werden. Erstellen und verwenden Sie stattdessen rollenbasierte Funktionen, AWS-Konten um das Prinzip der geringsten Funktionalität zu berücksichtigen.
Restrict_administrative_privileges	codebuild-project-environment-privileged-überprüfen	Um Sie bei der Implementierung des Prinzips der geringsten Rechte zu unterstützen, stellen Sie sicher, dass in Ihrer CodeBuild Amazon-Projektumgebung der privilegierte Modus nicht aktiviert ist. Diese Einstellung sollte deaktiviert werden, um unbeabsichtigten Zugriff auf Docker APIs sowie auf die dem Container zugrundeliegende Hardware zu verhindern.

Kontroll-ID	AWS Config	Empfehlungen
Restrict_administrative_privileges	ecs-containers-nonprivileged	Um die Implementierung des Prinzips der geringsten Berechtigung zu unterstützen, dürfen in Amazon Elastic Container Service (Amazon ECS)-Aufgabendefinitionen keine erhöhten Berechtigungen aktiviert sein. Wenn dieser Parameter den Wert „true“ aufweist, erhält der Container erhöhte Berechtigungen auf der Host-Container-Instance (ähnlich wie der Root-Benutzer).
Restrict_administrative_privileges	ecs-containers-readonly-access	Die Aktivierung des schreibgeschützten Zugriffs auf Amazon Elastic Container Service (ECS)-Container kann dazu beitragen, das Prinzip der geringsten Berechtigung einzuhalten. Diese Option kann Angriffsvektoren reduzieren, da das Dateisystem der Container-Instance nur geändert werden kann, wenn es über ausdrückliche Lese- und Schreibberechtigungen verfügt.

Kontroll-ID	AWS Config	Empfehlungen
Restrict_administrative_privileges	ecs-task-definition-nonroot-Benutzer	Sie bestimmen einen Nicht-Root-Benutzer für den Zugriff auf Ihre Aufgabendefinitionen von Amazon Elastic Container Service (Amazon ECS), um die Implementierung des Prinzips der geringsten Berechtigung zu unterstützen.
Restrict_administrative_privileges	efs-access-point-enforce-Benutzeridentität	Um die Implementierung des Prinzips der geringsten Rechte zu unterstützen, stellen Sie sicher, dass die Benutzerdurchsetzung für Ihr Amazon Elastic File System (Amazon EFS) aktiviert ist. Wenn diese Option aktiviert ist, ersetzt Amazon EFS den Benutzer und die Gruppe IDs des NFS-Clients durch die Identität, die auf dem Access Point für alle Dateisystemoperationen konfiguriert ist, und gewährt nur Zugriff auf diese erzwungene Benutzeridentität.

Kontroll-ID	AWS Config	Empfehlungen
Restrict_administrative_privileges	iam-user-group-membership-überprüfen	AWS Identity and Access Management (IAM) kann Ihnen helfen, Zugriffsberechtigungen und Autorisierungen einzuschränken, indem sichergestellt wird, dass Benutzer Mitglieder mindestens einer Gruppe sind. Wenn Benutzern mehr Berechtigungen eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und Aufgabentrennung verstoßen.

Kontroll-ID	AWS Config	Empfehlungen
Restrict_administrative_privileges	iam-user-unused-credentials-überprüfen	AWS Identity and Access Management (IAM) kann Ihnen bei Zugriffsberechtigungen und Autorisierungen helfen, indem es nach IAM-Passwörtern und Zugriffsschlüsseln sucht, die für einen bestimmten Zeitraum nicht verwendet wurden. Wenn ungenutzte Anmeldeinformationen identifiziert werden, müssen Sie sie deaktivieren und/oder entfernen, da dies gegen das Prinzip der geringsten Berechtigung verstoßen könnte. Für diese Regel müssen Sie einen Wert für das maxCredentialUsage Alter festlegen (Standardkonfiguration: 90). Der tatsächliche Wert muss den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	AWS Config	Empfehlungen
Restrict_administrative_privileges	rds-instance-iam-authentication-aktiviert	Stellen Sie sicher, dass eine AWS Identity and Access Management (IAM) - Authentifizierung auf Amazon Relational Database Service (Amazon RDS) -Instances aktiviert ist, um den Zugriff auf Systeme und Ressourcen zu kontrollieren. Dadurch wird die Verschlüsselung von ausgehendem und eingehendem Netzwerkverkehr von und zur Datenbank anhand von Secure Sockets Layer (SSL) durchgesetzt. Da die Authentifizierung extern verwaltet wird, ist es nicht erforderlich, Benutzeranmeldeinformationen in der Datenbank zu speichern.
Restrict_administrative_privileges	ec2- instance-profile-attached	EC2 Instanzprofile übergeben eine IAM-Rolle an eine EC2 Instance. Das Anhängen eines Instance-Profils an Ihre Instances kann bei der Implementierung von geringsten Berechtigungen und der Berechtigungsverwaltung helfen.

Kontroll-ID	AWS Config	Empfehlungen
Restrict_administrative_privileges	ecs-task-definition-user-for-host-mode-check	Wenn für eine Aufgabendefinition erhöhte Berechtigungen gelten, liegt das daran, dass der Kunde diesen Konfigurationen ausdrücklich zugestimmt hat. Diese Kontrolle prüft, ob eine unerwartete Berechtigungseskalation vorliegt, wenn für eine Aufgabendefinition das Host-Netzwerk aktiviert ist, die Kunden aber keine erhöhten Berechtigungen aktiviert haben.

Kontroll-ID	AWS Config	Empfehlungen
Restrict_administrative_privileges	iam-customer-policy-blocked-kms-Aktionen	AWS Identity and Access Management (IAM) kann Ihnen helfen, die Prinzipien der geringsten Rechte und der Aufgabentrennung in Zugriffsberechtigungen und Autorisierungen zu integrieren und so zu verhindern, dass Richtlinien blockierte Aktionen für alle AWS Schlüssel des Key Management Service enthalten. Wenn Benutzer mehr Rechte haben, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und Aufgabentrennung verstoßen. Mit dieser Regel können Sie den Parameter festlegen. blockedActionsPatterns (Wert „AWS Bewährte grundlegende Sicherheitsmethoden“: kms: Decrypt, kms:ReEncryptFrom). Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	AWS Config	Empfehlungen
Restrict_administrative_privileges	iam-inline-policy-blocked-kms-Aktionen	Stellen Sie sicher, dass ein Benutzer, eine IAM-Rolle oder eine IAM-Gruppe (AWS Identity and Access Management) nicht über eine Inline-Richtlinie verfügt, die blockierte Aktionen für alle AWS Schlüssel des Key Management Service zulässt. AWS empfiehlt, verwaltete Richtlinien anstelle von Inline-Richtlinien zu verwenden . Verwaltete Richtlinien ermöglichen Wiederverwendbarkeit, Versionsverwaltung, Rollback und Delegierung der Berechtigungsverwaltung. Mit dieser Regel können Sie den blockedActionsPatterns Parameter festlegen. (Wert „AWS Bewährte grundlegende Sicherheitsmethoden“: kms: Decrypt, kms:ReEncryptFrom). Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	AWS Config	Empfehlungen
Restrict_administrative_privileges	iam-policy-no-statements-with-full-access	Stellen Sie sicher, dass IAM-Aktionen nur auf die benötigten Aktionen beschränkt sind. Wenn Benutzern mehr Rechte eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und der Aufgabentrennung verstoßen.
Patch_operating_systems	ec2-check managedinstance-patch-compliance-status	Aktivieren Sie diese Regel, um bei der Identifizierung und Dokumentation von Sicherheitslücken in Amazon Elastic Compute Cloud (Amazon EC2) zu helfen. Die Regel prüft, ob die EC2 Amazon-Instance die Patch-Konformität im AWS Systems Manager gemäß den Richtlinien und Verfahren Ihrer Organisation einhält.

Kontroll-ID	AWS Config	Empfehlungen
Multi-factor_authentication	iam-root-access-key-überprüfen	Der Zugriff auf Systeme und Ressourcen kann gesteuert werden, indem überprüft wird, ob der Root-Benutzer keine Zugriffsschlüssel mit seiner AWS Identity and Access Management (IAM) -Rolle verknüpft hat. Stellen Sie sicher, dass die Root-Zugriffsschlüssel gelöscht werden. Erstellen und verwenden Sie stattdessen rollenbasierte Funktionen, AWS-Konten um das Prinzip der geringsten Funktionalität zu berücksichtigen.
Multi-factor_authentication	iam-user-mfa-enabled	Aktivieren Sie diese Regel, um den Zugriff auf Ressourcen in der AWS -Cloud einzuschränken. Diese Regel stellt sicher, dass die Multi-Faktor-Authentifizierung (MFA) für alle Benutzer aktiviert ist. MFA bietet eine weitere Schutzebene zusätzlich zum Benutzernamen und Passwort. Reduzieren Sie Fälle von kompromittierten Konten, indem Sie MFA für Benutzer vorschreiben.

Kontroll-ID	AWS Config	Empfehlungen
Multi-factor_authentication	mfa-enabled-for-iam-Konsolenzugriff	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass MFA für alle AWS Identity and Access Management (IAM) -Benutzer aktiviert ist, die über ein Konsolenkennwort verfügen. MFA sorgt für eine weitere Schutzebene zusätzlich zu den Anmeldeinformationen. Indem Sie MFA für Benutzer vorschreiben, können Sie Fälle kompromittierter Konten reduzieren und verhindern, dass unbefugte Benutzer auf vertrauliche Daten zugreifen.
Multi-factor_authentication	root-account-hardware-mfa-aktiviert	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Hardware-MFA für den Root-Benutzer aktiviert ist. Der Stammbenutzer ist der AWS-Konto-Benutzer mit den meisten Berechtigungen. MFA sorgt für eine weitere Schutzebene zusätzlich zu den Anmeldeinformationen. Indem Sie MFA für den Root-Benutzer vorschreiben, können Sie die Anzahl AWS-Konten kompromittierter Benutzer reduzieren.

Kontroll-ID	AWS Config	Empfehlungen
Multi-factor_authentication	root-account-mfa-enabled	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass MFA für den Root-Benutzer aktiviert ist. Der Stammbenutzer ist der AWS-Konto-Benutzer mit den meisten Berechtigungen. MFA bietet eine weitere Schutzebene zusätzlich zum Benutzernamen und Passwort. Indem Sie MFA für den Root-Benutzer vorschreiben, können Sie die Anzahl AWS-Konten kompromittierter Benutzer reduzieren.
Regular_backups	db-instance-backup-enabled	Die Sicherungsfunktion von Amazon RDS erstellt Sicherungen Ihrer Datenbanken und Transaktionsprotokolle. Amazon RDS erstellt einen Snapshot für das Speichervolume Ihrer DB-Instance, sodass die gesamte DB-Instance gesichert wird. Sie können im System spezifische Aufbewahrungsfristen festlegen, um Ihre Ausfallsicherheitsanforderungen zu erfüllen.

Kontroll-ID	AWS Config	Empfehlungen
Regular_backups	dynamodb-in-backup-plan	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon DynamoDB-Tabellen Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.
Regular_backups	ebs-in-backup-plan	Stellen Sie zur Unterstützung der Datensicherungsprozesse sicher, dass Ihre Amazon Elastic Block Store (Amazon EBS) -Volumes Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihre Backup-Verwaltung und ermöglicht es Ihnen, Ihre geschäftlichen und behördlichen Anforderungen bezüglich Backups zu erfüllen.

Kontroll-ID	AWS Config	Empfehlungen
Regular_backups	efs-in-backup-plan	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon Elastic File System (Amazon EFS) - Dateisysteme Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.
Regular_backups	elasticache-redis-cluster-automatic-Backup-Check	Wenn automatische Backups aktiviert sind, ElastiCache erstellt Amazon täglich ein Backup des Clusters. Die Sicherung kann für eine von Ihrer Organisation festgelegte Anzahl von Tagen aufbewahrt werden. Automatische Backups schützen vor Datenverlust. Bei einem Ausfall können Sie einen neuen Cluster erstellen, der Ihre Daten aus dem aktuellen Backup wiederherstellt.

Kontroll-ID	AWS Config	Empfehlungen
Regular_backups	rds-in-backup-plan	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon Relational Database Service (Amazon RDS) -Instances Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.
Regular_backups	s-3 bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) unterstützt die Aufrechterhaltung einer angemessenen Kapazität und Verfügbarkeit. CRR ermöglicht das automatische, asynchrone Kopieren von Objekten in Amazon-S3 -Buckets, um die Datenverfügbarkeit sicherzustellen.

Kontroll-ID	AWS Config	Empfehlungen
Regular_backups	s-3 bucket-versioning-enabled	Die Versionsverwaltung von Amazon Simple Storage Service (Amazon S3)-Buckets hilft dabei, mehrere Varianten eines Objekts im selben Amazon-S3-Bucket zu speichern. Verwenden Sie die Versionsverwaltung, um sämtliche Versionen aller Objekte in Ihrem Amazon-S3-Bucket zu speichern, abzurufen oder wiederher zustellen. Mit der Versionsv erwaltung können Sie Versionen sowohl nach unbeabsichtigten Benutzera ktionen als auch nach Anwendungsfehlern problemlo s wiederherstellen.

Kontroll-ID	AWS Config	Empfehlungen
Regular_backups	aurora-resources-protected-by-Backup-Plan	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon Aurora Aurora-Ressourcen Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	AWS Config	Empfehlungen
Regular_backups	backup-plan-min-frequency-and-min-retention-check	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihr AWS Backup-Plan auf eine Mindestfrequenz und Aufbewahrung festgelegt ist. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen. Mit dieser Regel können Sie die Parameter requiredFrequencyValue (Config default: 1), requiredRetentionDays (Config default: 35) und requiredFrequencyUnit (Config default: days) festlegen. Der tatsächliche Wert muss den Anforderungen Ihrer Organisation entsprechen.

Kontroll-ID	AWS Config	Empfehlungen
Regular_backups	backup-recovery-point-manual-löschen-deaktiviert	Stellen Sie sicher, dass Ihren AWS Backup-Wiederherstellungspunkten eine ressourcenbasierte Richtlinie zugeordnet ist, die das Löschen von Wiederherstellungspunkten verhindert. Die Verwendung einer ressourcenbasierten Richtlinie zur Verhinderung des Löschens von Wiederherstellungspunkten kann dazu beitragen, ein versehentliches oder absichtliches Löschen zu unterbinden.
Regular_backups	ec2--Plan resources-protected-by-backup	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon Elastic Compute Cloud (Amazon EC2) - Ressourcen Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	AWS Config	Empfehlungen
Regular_backups	redshift-backup-enabled	Stellen Sie zur Unterstützung der Datensicherungsprozesse sicher, dass Ihre Amazon-Redshift-Cluster über automatisierte Snapshots verfügen. Wenn automatisierte Snapshots für einen Cluster aktiviert sind, erstellt Redshift in regelmäßigen Abständen Snapshots dieses Clusters. Standardmäßig erstellt Redshift alle acht Stunden oder alle 5 GB einen Snapshot für jeden Knoten mit Datenänderungen oder je nachdem, was zuerst eintritt.

Vorlage

Die Vorlage ist verfügbar unter GitHub: Operational Best Practices for ACSC Essential 8.

Bewährte Methoden für die Implementierung von ACSC ISM

Konformitätspakete bieten ein allgemeines Compliance-Framework, das es Ihnen ermöglicht, mithilfe verwalteter oder benutzerdefinierter AWS Config Regeln und Abhilfemaßnahmen Kontrollen zur Sicherheits-, Betriebs- oder Kostenoptimierung durchzuführen. AWS Config Conformance Packs dienen als Beispielvorlagen nicht dazu, die vollständige Einhaltung eines bestimmten Governance- oder Compliance-Standards sicherzustellen. Sie sind dafür verantwortlich, selbst zu beurteilen, ob Ihre Nutzung der Services den geltenden gesetzlichen und behördlichen Anforderungen entspricht.

Im Folgenden finden Sie ein Beispiel für eine Zuordnung zwischen dem Information Security Manual (ISM) 2020-06 des Australian Cyber Security Centre (ACSC) und AWS verwalteten Konfigurationsregeln. Jede Config-Regel gilt für eine bestimmte AWS Ressource und bezieht sich auf eine oder mehrere ISM-Steuerelemente. Eine ISM-Kontrolle kann mehreren Konfigurationsregeln

zugeordnet werden. In der folgenden Tabelle finden Sie weitere Informationen und Anleitungen zu diesen Zuordnungen.

Diese Vorlage für ein Konformitätspaket enthält Zuordnungen zu Kontrollen innerhalb des ISM-Frameworks, das vom Commonwealth of Australia erstellt wurde und im Australian Government Information Security Manual zu finden ist. Die Lizenzierung des Frameworks unter der Creative Commons Namensnennung 4.0 Internationale öffentliche Lizenz und Informationen zum Urheberrecht für das Framework (einschließlich eines Gewährleistungsausschlusses) finden Sie unter ACSC | Copyright.

Kontroll-ID	AWS Config	Empfehlungen
43	response-plan-exists-maintained (Prozessüberprüfung)	Stellen Sie sicher, dass Vorfallreaktionspläne erstellt, verwaltet und an das verantwortliche Personal verteilt werden.
252	security-awareness-program-exists (Prozessprüfung)	Etablieren und pflegen Sie ein Programm zur Förderung des Sicherheitsbewusstseins in Ihrer Organisation. Programme zur Förderung des Sicherheitsbewusstseins der Mitarbeiter vermitteln ihnen, wie sie die Organisation vor diversen Sicherheitsverletzungen oder Sicherheitsvorfällen schützen können.
261	api-gw-execution-logging-aktiviert	Die API-Gateway-Protokollierung zeigt detaillierte Ansichten der Benutzer, die auf die API zugegriffen haben, und wie diese Benutzer auf die API zugegriffen haben. Diese Einblicke ermöglichen die

Kontroll-ID	AWS Config	Empfehlungen
		Transparenz von Benutzera ktivitäten.
261	elb-logging-enabled	Die Elastic-Load-Balancing-Aktivität ist ein zentraler Kommunikationspunkt innerhalb einer Umgebung. Stellen Sie sicher, dass die ELB-Protokollierung aktiviert ist. Die gesammelten Daten enthalten detaillierte Informati onen zu Anfragen, die an den ELB gesendet wurden. Jedes Protokoll enthält Informati onen wie die Zeit, zu der die Anforderung einging, die Client-IP-Adresse, Latenzen, Anforderungspfade und Serverantworten.

Kontroll-ID	AWS Config	Empfehlungen
261	wafv2-logging-enabled	Um die Protokollierung und Überwachung in Ihrer Umgebung zu erleichte rn, aktivieren Sie die AWS WAF (V2) -Protokollierung im regionalen und globalen Web. ACLs AWS Die WAF-Protokollierung bietet detaillie rte Informationen über den Datenverkehr, der von Ihrer Web-ACL analysiert wird. In den Protokollen werden die Uhrzeit aufgezeichnet, zu der die AWS WAF die Anfrage von Ihrer AWS Ressource erhalten hat, Informationen über die Anfrage und eine Aktion für die Regel, der jede Anfrage entsprach.
298	ec2-prüfen managedinstance-patch-compliance-status	Aktivieren Sie diese Regel, um bei der Identifizierung und Dokumentation von Sicherhei tslücken in Amazon Elastic Compute Cloud (Amazon EC2) zu helfen. Die Regel prüft, ob die EC2 Amazon-In stance die Patch-Konformität im AWS Systems Manager gemäß den Richtlinien und Verfahren Ihrer Organisation einhält.

Kontroll-ID	AWS Config	Empfehlungen
298	redshift-cluster-maintenancesettings-check	Diese Regel stellt sicher, dass Amazon-Redshift-Cluster die bevorzugten Einstellungen für Ihre Organisation haben. Insbesondere sorgt sie dafür, dass Cluster bevorzugte Wartungsfenster und automatisierte Aufbewahrungsfristen für Snapshots für die Datenbank haben. Für diese Regel müssen Sie die festlegen allowVersionUpgrade. Der Standardwert ist „true“. Außerdem können Sie optional den Zeitraum preferredMaintenanceWindow (der Standardwert ist sa: 16:00 -sa: 16:30) und den automatedSnapshotRetention Zeitraum (der Standardwert ist 1) festlegen. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	AWS Config	Empfehlungen
298	elastic-beanstalk-managed-updates-aktiviert	Durch die Aktivierung verwalteter Plattformupdates für eine Amazon-Elastic-Beanstalk-Umgebung wird sichergestellt, dass die aktuellen verfügbaren Plattform-Fixes, -Updates und -Features für die Umgebung installiert sind. Eine bewährte Methode zur Sicherung von Systemen besteht darin, stets die aktuellen Patches zu installieren.
298	rds-automatic-minor-version-upgrade-fähig	Aktivieren Sie automatische Unterversions-Upgrades auf Ihren Amazon-Relational-Database-Service (RDS)-Instances, um sicherzustellen, dass die aktuellen Updates für Unterversionen des Relational Database Management System (RDBMS) installiert sind, die Sicherheitspatches und Bugfixes enthalten können.

Kontroll-ID	AWS Config	Empfehlungen
380	iam-group-has-users-überprüfen	AWS Identity and Access Management (IAM) kann Ihnen helfen, die Prinzipien der geringsten Rechte und der Aufgabentrennung mit Zugriffsberechtigungen und Autorisierungen zu integrieren, indem sichergestellt wird, dass IAM-Gruppen mindestens einen Benutzer haben. Die Einteilung von Benutzern in Gruppen auf der Grundlage der ihnen zugewiesenen Berechtigungen oder ihrer Funktion ist eine Möglichkeit, das Prinzip der geringsten Berechtigung zu implementieren.
459	api-gw-cache-enabled-und verschlüsselt	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass die Verschlüsselung für den Cache Ihrer API-Gateway-Stufe aktiviert ist. Da für die API-Methode sensible Daten erfasst werden können, sollten Sie die Verschlüsselung von Daten im Ruhezustand aktivieren, um diese Daten zu schützen.

Kontroll-ID	AWS Config	Empfehlungen
459	cloud-trail-encryption-enabled	Zum Schutz von eventuell vorhandenen sensiblen Daten sowie Daten im Ruhezusta nd müssen Sie sicherstellen, dass die Verschlüsselung für Ihre AWS CloudTrail aktiviert ist.
459	ec-2 ebs-encryption-by-default	Zum Schutz von Daten im Ruhezustand müssen Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon Elastic Block Store (Amazon EBS)-Volumes aktiviert ist. Aktivieren Sie die Verschlüsselung von Daten im Ruhezustand, um eventuell in diesen Volumes vorhandene sensible Daten im Ruhezusta nd zu schützen.
459	efs-encrypted-check	Aktivieren Sie die Verschlüs selung für Ihr Amazon Elastic File System (EFS), um eventuell vorhandene sensible Daten sowie Daten im Ruhezustand zu schützen.
459	encrypted-volumes	Aktivieren Sie die Verschlüs selung für Ihre Volumes von Amazon Elastic Block Store (Amazon EBS), um eventuell vorhandene sensible Daten sowie Daten im Ruhezustand zu schützen.

Kontroll-ID	AWS Config	Empfehlungen
459	bucket-server-side-encryption s3-fähig	Zum Schutz von Daten im Ruhezustand müssen Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon Simple Storage Service (Amazon S3)-Buckets aktiviert ist. Da sensible Daten in Amazon-S3-Buckets gespeichert werden können, sollten Sie die Verschlüsselung aktivieren, um diese Daten zu schützen.
459	s-3 default-encryption-kms	Stellen Sie sicher, dass die Verschlüsselung für Ihre Amazon Simple Storage Service (Amazon S3)-Buckets aktiviert ist. Da sensible Daten in einem Amazon-S3-Bucket gespeichert werden können, sollten Sie die Verschlüsselung im Ruhezustand aktivieren, um diese Daten zu schützen.

Kontroll-ID	AWS Config	Empfehlungen
459	redshift-cluster-kms-enabled	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass die Verschlüsselung mit AWS Key Management Service (AWS KMS) für Ihren Amazon Redshift Redshift-Cluster aktiviert ist. Um eventuell vorhandene sensible Daten im Ruhezustand in Redshift-Clustern zu schützen, muss die Verschlüsselung von Daten im Ruhezustand aktiviert sein.
459	elasticsearch-encrypted-at-rest	Da sensible Daten vorhanden sein können und um Daten im Ruhezustand zu schützen, sollten Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon OpenSearch Service (OpenSearch Service) -Domains aktiviert ist.
459	opensearch-encrypted-at-rest	Da sensible Daten vorhanden sein können und um Daten im Ruhezustand zu schützen, sollten Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon OpenSearch Service-Domains aktiviert ist.

Kontroll-ID	AWS Config	Empfehlungen
459	sagemaker-endpoint-configuration-kms-schlüsselkonfiguriert	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass die Verschlüsselung mit dem AWS Key Management Service (AWS KMS) für Ihren Endpunkt aktiviert ist. SageMaker Da sensible Daten auf dem SageMaker Endgerät gespeichert werden können, sollten Sie die Verschlüsselung im Ruhezustand aktivieren, um diese Daten zu schützen.
459	sagemaker-notebook-instance-kms-schlüsselkonfiguriert	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass die Verschlüsselung mit dem AWS Key Management Service (AWS KMS) für Ihr Notebook aktiviert ist. SageMaker Da vertrauliche Daten im SageMaker Notebook gespeichert werden können, sollten Sie die Verschlüsselung im Ruhezustand aktivieren, um diese Daten zu schützen.

Kontroll-ID	AWS Config	Empfehlungen
459	backup-recovery-point-encrypted	Stellen Sie sicher, dass die Verschlüsselung für Ihre AWS Backup-Wiederherstellungspunkte aktiviert ist. Da sensible Daten auch im Ruhezustand vorhanden sein können, sollten Sie die Verschlüsselung im Ruhezustand aktivieren, um diese Daten zu schützen.
459	codebuild-project-artifact-encryption	Um sensible Daten im Speicher zu schützen, stellen Sie sicher, dass die Verschlüsselung für Ihre AWS CodeBuild Artefakte aktiviert ist.
459	codebuild-project-s3-Log-verschlüsselt	Um sensible Daten im Speicher zu schützen, stellen Sie sicher, dass die Verschlüsselung für Ihre in Amazon S3 gespeicherten AWS CodeBuild Protokolle aktiviert ist.

Kontroll-ID	AWS Config	Empfehlungen
459	dynamodb-table-encrypted-kms	Stellen Sie sicher, dass die Verschlüsselung für Ihre Amazon-DynamoDB-Tabellen aktiviert ist. Um eventuell vorhandene sensible Daten im Ruhezustand in diesen Tabellen zu schützen, müssen Sie die Verschlüsselung von Daten im Ruhezustand aktivieren. Standardmäßig werden DynamoDB-Tabellen mit einem AWS eigenen Kundenhauptschlüssel (CMK) verschlüsselt.
459	kinesis-stream-encrypted	Aktivieren Sie die Verschlüsselung für Ihre Amazon-Kinesis-Streams, um eventuell vorhandene sensible Daten sowie Daten im Ruhezustand zu schützen.
459	rds-snapshot-encrypted	Stellen Sie sicher, dass die Verschlüsselung für Ihre Amazon Relational Database Service (Amazon RDS)-Snapshots aktiviert ist. Da sensible Daten auch im Ruhezustand vorhanden sein können, sollten Sie die Verschlüsselung von Daten im Ruhezustand aktivieren, um diese Daten zu schützen.

Kontroll-ID	AWS Config	Empfehlungen
459	rds-storage-encrypted	Zum Schutz von Daten im Ruhezustand müssen Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon Relational Database Service (Amazon RDS)-Instances aktiviert ist. Da sensible Daten in Amazon-RDS-Instances gespeichert werden können, sollten Sie die Verschlüsselung von Daten im Ruhezustand aktivieren, um diese Daten zu schützen.
459	sns-encrypted-kms	Um Daten im Ruhezusta nd zu schützen, stellen Sie sicher, dass Ihre Amazon Simple Notification Service (Amazon SNS) -Themen mit dem AWS Key Management Service (AWS KMS) verschlüs selt werden müssen. Um eventuell vorhandene sensible Daten im Ruhezustand in veröffentlichten Nachricht en zu schützen, muss die Verschlüsselung von Daten im Ruhezustand aktiviert sein.

Kontroll-ID	AWS Config	Empfehlungen
580	audit-log-policy-exists (Prozessüberprüfung)	Richten Sie eine Richtlinie zur Verwaltung von Prüfprotokollen ein, in der die Protokollierungsanforderungen Ihres Unternehmens definiert sind, und pflegen Sie diese Richtlinie. Dies beinhaltet, ist aber nicht beschränkt auf die Überprüfung und Aufbewahrung von Prüfprotokollen.
634	vpc-flow-logs-enabled	VPC-Flow-Protokolle erfassen detaillierte Informationsdatensätze über den IP-Datenverkehr, der zu und von Netzwerkschnittstellen in Ihrer Amazon Virtual Private Cloud (Amazon VPC) fließt. Standardmäßig enthalten Flow-Protokolldatensätze Werte für die verschiedenen Komponenten des IP-Flows, einschließlich Quelle, Ziel und Protokoll.

Kontroll-ID	AWS Config	Empfehlungen
859	cw-loggroup-retention-period-überprüfen	Stellen Sie sicher, dass die Ereignisprotokolldaten für Ihre Protokollgruppen über eine Mindestdauer aufbewahrt werden, um die Fehlerbehebung und forensische Untersuch ungen zu unterstützen. Fehlende frühere Ereignisp rotokolldaten erschweren die Rekonstruierung und Identifiz ierung potenziell schädlicher Ereignisse.
974	iam-user-mfa-enabled	Aktivieren Sie diese Regel, um den Zugriff auf Ressourcen in der AWS -Cloud einzuschr änken. Diese Regel stellt sicher, dass die Multi-Fak tor-Authentifizierung (MFA) für alle Benutzer aktiviert ist. MFA bietet eine weitere Schutzebene zusätzlich zum Benutzernamen und Passwort. Reduzieren Sie Fälle von kompromittierten Konten, indem Sie MFA für Benutzer vorschreiben.

Kontroll-ID	AWS Config	Empfehlungen
974	mfa-enabled-for-iam-Konsolenzugriff	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass MFA für alle AWS Identity and Access Management (IAM) -Benutzer aktiviert ist, die über ein Konsolenkennwort verfügen. MFA sorgt für eine weitere Schutzebene zusätzlich zu den Anmeldeinformationen. Indem Sie MFA für Benutzer vorschreiben, können Sie Fälle kompromittierter Konten reduzieren und verhindern, dass unbefugte Benutzer auf vertrauliche Daten zugreifen.

Kontroll-ID	AWS Config	Empfehlungen
1139	elb-predefined-security-policy-SSL-Überprüfung	Stellen Sie sicher, dass Ihre SSL-Listener von Classic Elastic Load Balancing eine vordefinierte Sicherheitsrichtlinie verwenden, um Daten während der Übertragung zu schützen. Elastic Load Balancing bietet vordefinierte Aushandlungskonfigurationen, die für die SSL-Aushandlung verwendet werden, wenn eine Verbindung zwischen einem Client und Ihrem Load Balancer hergestellt wurde. Die SSL-Aushandlungskonfigurationen sind mit einer breiten Palette von Clients kompatibel und verwenden hochfeste kryptografische Algorithmen. Diese Regel verlangt, dass Sie eine vordefinierte Sicherheitsrichtlinie für Ihre SSL-Listener festlegen. Die Standard-Sicherheitsrichtlinie lautet: Policy-TLS-1-2-2017-0. ELBSecurity Der tatsächliche Wert muss den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	AWS Config	Empfehlungen
1173	root-account-hardware-mfa-aktiviert	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Hardware-MFA für den Root-Benutzer aktiviert ist. Der Stammbenutzer ist der AWS-Konto-Benutzer mit den meisten Berechtigungen. MFA sorgt für eine weitere Schutzebene zusätzlich zu den Anmeldeinformationen. Indem Sie MFA für den Root-Benutzer vorschreiben, können Sie die Anzahl AWS-Konten kompromittierter Benutzer reduzieren.
1173	root-account-mfa-enabled	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass MFA für den Root-Benutzer aktiviert ist. Der Stammbenutzer ist der AWS-Konto-Benutzer mit den meisten Berechtigungen. MFA bietet eine weitere Schutzebene zusätzlich zum Benutzernamen und Passwort. Indem Sie MFA für den Root-Benutzer vorschreiben, können Sie die Anzahl AWS-Konten kompromittierter Benutzer reduzieren.

Kontroll-ID	AWS Config	Empfehlungen
1173	iam-root-access-key-überprüfen	Der Zugriff auf Systeme und Ressourcen kann gesteuert werden, indem überprüft wird, ob der Root-Benutzer keine Zugriffsschlüssel mit seiner AWS Identity and Access Management (IAM) -Rolle verknüpft hat. Stellen Sie sicher, dass die Root-Zugriffsschlüssel gelöscht werden. Erstellen und verwenden Sie stattdessen rollenbasierte Funktionen, AWS-Konten um das Prinzip der geringsten Funktionalität zu berücksichtigen.
1173	iam-user-mfa-enabled	Aktivieren Sie diese Regel, um den Zugriff auf Ressourcen in der AWS -Cloud einzuschränken. Diese Regel stellt sicher, dass die Multi-Faktor-Authentifizierung (MFA) für alle Benutzer aktiviert ist. MFA bietet eine weitere Schutzebene zusätzlich zum Benutzernamen und Passwort. Reduzieren Sie Fälle von kompromittierten Konten, indem Sie MFA für Benutzer vorschreiben.

Kontroll-ID	AWS Config	Empfehlungen
1173	mfa-enabled-for-iam-Konsolenzugriff	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass MFA für alle AWS Identity and Access Management (IAM) -Benutzer aktiviert ist, die über ein Konsolenkennwort verfügen. MFA sorgt für eine weitere Schutzebene zusätzlich zu den Anmeldeinformationen. Indem Sie MFA für Benutzer vorschreiben, können Sie Fälle kompromittierter Konten reduzieren und verhindern, dass unbefugte Benutzer auf vertrauliche Daten zugreifen.
1228	guardduty-enabled-centralized	Amazon GuardDuty kann mithilfe von Threat Intelligence Feeds helfen, potenzielle Cybersicherheitsereignisse zu überwachen und zu erkennen. Dazu gehören Listen mit bösartigen IPs und maschinellen Lernmethoden zur Identifizierung unerwarteter, nicht autorisierter und bösartiger Aktivitäten in Ihrer AWS Cloud-Umgebung.

Kontroll-ID	AWS Config	Empfehlungen
1240	alb-waf-enabled	Stellen Sie sicher, dass AWS WAF auf Elastic Load Balancers (ELB) aktiviert ist, um Webanwendungen zu schützen. Eine WAF trägt zum Schutz Ihrer Webanwend ungen oder APIs vor gängigen Web-Exploits bei. Diese Web-Exploits können sich auf die Verfügbarkeit auswirken, die Sicherheit gefährden oder übermäßige Ressourcen in Ihrer Umgebung verbrauchen.
1240	api-gw-associated-with-WAF	AWS Mit WAF können Sie eine Reihe von Regeln (als Web Access Control List (Web ACL) bezeichnet) konfiguri eren, die Webanfragen auf der Grundlage von anpassbar en Websicherheitsregeln und -bedingungen, die Sie definieren, zulassen, blockiere n oder zählen. Stellen Sie sicher, dass Ihre Amazon-API-Gateway-Stufe mit einer WAF-Web-ACL verknüpft ist, um sie vor böswilligen Angriffen zu schützen.

Kontroll-ID	AWS Config	Empfehlungen
1271	rds-instance-public-access-überprüfen	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Relational Database Service (Amazon RDS) -Instances nicht öffentlich sind. Amazon-RDS-Datenbank-Instances können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.
1271	redshift-enhanced-vpc-routing-aktiviert	Mit Enhanced-VPC-Routing wird erzwungen, dass der gesamte COPY- und UNLOAD-Datenverkehr zwischen Ihrem Cluster und Datenrepositorys über Ihre Amazon VPC erfolgt. Anschließend können Sie VPC-Features wie Sicherheitsgruppen und Netzwerkzugriffskontrollllisten verwenden, um den Netzwerkverkehr zu schützen. Sie können auch VPC-Flow-Protokolle verwenden, um den Netzwerkverkehr zu überwachen.

Kontroll-ID	AWS Config	Empfehlungen
1277	redshift-require-tls-ssl	Stellen Sie sicher, dass Ihre Amazon-Redshift-Cluster eine TLS/SSL-Verschlüsselung erfordern, um eine Verbindun g zu SQL-Clients herzustellen. Da sensible Daten vorhanden sein können, sollten Sie die Verschlüsselung bei der Übertragung aktivieren, um diese Daten zu schützen.
1277	rds-instance-iam-authentica tion-aktiviert	Stellen Sie sicher, dass eine AWS Identity and Access Management (IAM) - Authentifizierung auf Amazon Relational Database Service (Amazon RDS) -Instances aktiviert ist, um den Zugriff auf Systeme und Ressource n zu kontrollieren. Dadurch wird die Verschlüsselung von ausgehendem und eingehend em Netzwerkverkehr von und zur Datenbank anhand von Secure Sockets Layer (SSL) durchgesetzt. Da die Authentif izierung extern verwaltet wird, ist es nicht erforderl ich, Benutzeranmeldeinf ormationen in der Datenbank zu speichern.

Kontroll-ID	AWS Config	Empfehlungen
1277	api-gw-ssl-enabled	Stellen Sie sicher, dass die REST-API-Stufen von Amazon API Gateway mit SSL-Zerti fikaten konfiguriert sind, damit Backend-Systeme überprüfe n können, ob Anforderungen von API Gateway stammen.
1380	ec2-imdsv2-check	Stellen Sie sicher, dass die Methode Instance Metadata Service Version 2 (IMDSv2) aktiviert ist, um den Zugriff auf und die Kontrolle der Amazon Elastic Compute Cloud (Amazon EC2) -Instance-Metadaten zu schützen. Die IMDSv2 Methode verwendet sitzungsbasierte Kontrolle n. Mit können Kontrollen implementiert werden IMDSv2, um Änderungen an Instanzme tadaten einzuschränken.

Kontroll-ID	AWS Config	Empfehlungen
1380	ec2-manager instance-managed-by-systems	Eine Bestandsaufnahme der Softwareplattformen und Anwendungen innerhalb des Unternehmens ist möglich, indem Amazon Elastic Compute Cloud (Amazon EC2) -Instances mit AWS Systems Manager verwaltet werden. Verwenden Sie AWS Systems Manager, um detaillierte Systemkonfigurationen, Betriebssystem-Patch-Levels, Namen und Typ der Dienste, Softwareinstallationen, Anwendungsname, Herausgeber und Version sowie andere Details zu Ihrer Umgebung bereitzustellen.

Kontroll-ID	AWS Config	Empfehlungen
1380	ecs-fargate-latest-platform-Ausführung	Sicherheitsupdates und Patches werden automatis ch für Ihre AWS Fargate-Aufgaben bereitgestellt. Wenn ein Sicherheitsproblem gefunden wird, das eine AWS Fargate-Plattformversion betrifft, AWS wird die Plattform version gepatcht. Um Sie bei der Patchverwaltung Ihrer Amazon Elastic Container Service (ECS) -Aufgaben zu unterstützen, auf denen AWS Fargate ausgeführt wird, aktualisieren Sie Ihre eigenständigen Service-Aufgaben, sodass sie die neueste Plattformversion verwenden.
1380	elastic-beanstalk-managed-updates-aktiviert	Durch die Aktivierung verwalteter Plattformupdates für eine Amazon-Elastic-Beanstalk-Umgebung wird sichergestellt, dass die aktuellen verfügbaren Plattform-Fixes, -Updates und -Features für die Umgebung installiert sind. Eine bewährte Methode zur Sicherung von Systemen besteht darin, stets die aktuellen Patches zu installieren.

Kontroll-ID	AWS Config	Empfehlungen
1380	rds-automatic-minor-version-Upgrade aktiviert	Aktivieren Sie automatische Unterversions-Upgrades auf Ihren Amazon-Relational-Database-Service (RDS)-Instances, um sicherzustellen, dass die aktuellen Updates für Unterversionen des Relational Database Management System (RDBMS) installiert sind, die Sicherheitspatches und Bugfixes enthalten können.
1380	ec2-prüfen managedinstance-association-compliance-status	Verwenden Sie AWS Systems Manager Associations, um bei der Inventarisierung von Softwareplattformen und Anwendungen innerhalb eines Unternehmens zu helfen. AWS Systems Manager weist Ihren verwalteten Instances einen Konfigurationsstatus zu und ermöglicht es Ihnen, Basiswerte für Betriebssystem-Patch-Levels, Softwareinstallationen, Anwendungskonfigurationen und andere Details zu Ihrer Umgebung festzulegen.

Kontroll-ID	AWS Config	Empfehlungen
1380	redshift-cluster-maintenancesettings-check	Diese Regel stellt sicher, dass Amazon-Redshift-Cluster die bevorzugten Einstellungen für Ihre Organisation haben. Insbesondere sorgt sie dafür, dass Cluster bevorzugte Wartungsfenster und automatisierte Aufbewahrungsfristen für Snapshots für die Datenbank haben. Für diese Regel müssen Sie die allowVersionUpgrade festlegen. Der Standardwert ist „true“. Außerdem können Sie optional den Zeitraum preferredMaintenanceWindow (der Standardwert ist sa: 16:00 -sa: 16:30) und den automatedSnapshotRetention Zeitraum (der Standardwert ist 1) festlegen. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	AWS Config	Empfehlungen
1380	iam-no-inline-policy-überprüfen	Stellen Sie sicher, dass ein Benutzer, eine IAM-Rolle oder eine IAM-Gruppe (AWS Identity and Access Management) nicht über eine Inline-Richtlinie zur Zugriffskontrolle auf Systeme und Ressourcen verfügt. AWS empfiehlt, verwaltete Richtlinien anstelle von Inline-Richtlinien zu verwenden . Verwaltete Richtlinien ermöglichen Wiederverwendbarkeit, Versionsverwaltung, Rollback und Delegierung der Berechtigungsverwaltung.

Kontroll-ID	AWS Config	Empfehlungen
1380	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) kann Ihnen dabei helfen, die Prinzipien der geringsten Rechte und der Aufgabent rennung in Zugriffsberechtigu ngen und Autorisierungen zu integrieren und so zu verhindern, dass Richtlinien „Effect“: „Allow“ mit „Action“: „*“ anstelle von „Resource“: „*“ enthalten. Wenn Benutzern mehr Rechte eingeräumt werden, als für die Ausführun g einer Aufgabe erforderl ich sind, kann dies gegen das Prinzip der geringste n Berechtigung und der Aufgabentrennung verstoßen.

Kontroll-ID	AWS Config	Empfehlungen
1380	iam-root-access-key-überprüfen	Der Zugriff auf Systeme und Ressourcen kann gesteuert werden, indem überprüft wird, ob der Root-Benutzer keine Zugriffsschlüssel mit seiner AWS Identity and Access Management (IAM) -Rolle verknüpft hat. Stellen Sie sicher, dass die Root-Zugriffsschlüssel gelöscht werden. Erstellen und verwenden Sie stattdessen rollenbasierte Funktionen, AWS-Konten um das Prinzip der geringsten Funktionalität zu berücksichtigen.
1380	codebuild-project-environment-privileged-überprüfen	Um die Implementierung des Prinzips der geringsten Rechte zu unterstützen, stellen Sie sicher, dass in Ihrer CodeBuild Amazon-Projektumgebung der privilegierte Modus nicht aktiviert ist. Diese Einstellung sollte deaktiviert werden, um einen unbeabsichtigten Zugriff auf Docker APIs sowie auf die dem Container zugrunde liegende Hardware zu verhindern.

Kontroll-ID	AWS Config	Empfehlungen
1380	ecs-containers-nonprivileged	Um die Implementierung des Prinzips der geringsten Berechtigung zu unterstützen, dürfen in Amazon Elastic Container Service (Amazon ECS)-Aufgabendefinitionen keine erhöhten Berechtigungen aktiviert sein. Wenn dieser Parameter den Wert „true“ aufweist, erhält der Container erhöhte Berechtigungen auf der Host-Container-Instance (ähnlich wie der Root-Benutzer).
1380	ecs-containers-readonly-access	Die Aktivierung des schreibgeschützten Zugriffs auf Amazon Elastic Container Service (ECS)-Container kann dazu beitragen, das Prinzip der geringsten Berechtigung einzuhalten. Diese Option kann Angriffsvektoren reduzieren, da das Dateisystem der Container-Instance nur geändert werden kann, wenn es über ausdrückliche Lese- und Schreibberechtigungen verfügt.

Kontroll-ID	AWS Config	Empfehlungen
1380	ecs-task-definition-nonroot-Benutzer	Sie bestimmen einen Nicht-Root-Benutzer für den Zugriff auf Ihre Aufgabendefinitionen des Amazon Elastic Container Service (Amazon ECS), um die Implementierung des Prinzips der geringsten Berechtigung zu unterstützen.
1380	efs-access-point-enforce-Benutzeridentität	Um die Implementierung des Prinzips der geringsten Rechte zu unterstützen, stellen Sie sicher, dass die Benutzerd urchsetzung für Ihr Amazon Elastic File System (Amazon EFS) aktiviert ist. Wenn diese Option aktiviert ist, ersetzt Amazon EFS den Benutzer und die Gruppe IDs des NFS-Clients durch die Identität , die auf dem Access Point für alle Dateisystemoperati onen konfiguriert ist, und gewährt nur Zugriff auf diese erzwungene Benutzeridentität.

Kontroll-ID	AWS Config	Empfehlungen
1380	iam-user-group-membership-überprüfen	AWS Identity and Access Management (IAM) kann Ihnen helfen, Zugriffsberechtigungen und Autorisierungen einzuschränken, indem sichergestellt wird, dass Benutzer Mitglieder mindestens einer Gruppe sind. Wenn Benutzern mehr Berechtigungen eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und Aufgabentrennung verstoßen.

Kontroll-ID	AWS Config	Empfehlungen
1380	rds-instance-iam-authentication-aktiviert	Stellen Sie sicher, dass eine AWS Identity and Access Management (IAM) - Authentifizierung auf Amazon Relational Database Service (Amazon RDS) -Instances aktiviert ist, um den Zugriff auf Systeme und Ressourcen zu kontrollieren. Dadurch wird die Verschlüsselung von ausgehendem und eingehendem Netzwerkverkehr von und zur Datenbank anhand von Secure Sockets Layer (SSL) durchgesetzt. Da die Authentifizierung extern verwaltet wird, ist es nicht erforderlich, Benutzeranmeldeinformationen in der Datenbank zu speichern.
1380	ec-2 instance-profile-attached	EC2 Instanzprofile übergeben eine IAM-Rolle an eine EC2 Instance. Das Anhängen eines Instance-Profils an Ihre Instances kann bei der Implementierung von geringsten Berechtigungen und der Berechtigungsverwaltung helfen.

Kontroll-ID	AWS Config	Empfehlungen
1380	ecs-task-definition-user-for-host-mode-check	Wenn für eine Aufgabend efinition erhöhte Berechtig ungen gelten, liegt das daran, dass der Kunde diesen Konfigurationen ausdrücklich zugestimmt hat. Diese Kontrolle prüft, ob eine unerwartete Berechtig ungseskalation vorliegt, wenn für eine Aufgabendefinition das Host-Netzwerk aktiviert ist, die Kunden aber keine erhöhten Berechtigungen aktiviert haben.

Kontroll-ID	AWS Config	Empfehlungen
1380	iam-customer-policy-blocked-KMS-Aktionen	AWS Identity and Access Management (IAM) kann Ihnen helfen, die Prinzipien der geringsten Rechte und der Aufgabentrennung in Zugriffsberechtigungen und Autorisierungen zu integrier en und so zu verhindern, dass Richtlinien blockierte Aktionen für alle AWS Schlüssel des Key Management Service enthalten. Wenn Benutzer mehr Rechte haben, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und Aufgabentrennung verstoßen . Mit dieser Regel können Sie den Parameter festlegen. blockedActionsPatterns (Wert „AWS Bewährte grundlegende Sicherheitsmethoden“: kms: Entschlüsseln, kms:ReEnc ryptFrom). Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprech en.

Kontroll-ID	AWS Config	Empfehlungen
1380	iam-inline-policy-blocked-KMS-Aktionen	Stellen Sie sicher, dass ein Benutzer, eine IAM-Rolle oder eine IAM-Gruppe (AWS Identity and Access Management) nicht über eine Inline-Richtlinie verfügt, die blockierte Aktionen für alle AWS Schlüssel des Key Management Service zulässt. AWS empfiehlt, verwaltete Richtlinien anstelle von Inline-Richtlinien zu verwenden . Verwaltete Richtlinien ermöglichen Wiederverwendbarkeit, Versionsverwaltung, Rollback und Delegierung der Berechtigungsverwaltung. Mit dieser Regel können Sie den blockedActionsPatterns Parameter festlegen. (Wert „AWS Bewährte grundlegende Sicherheitsmethoden“: kms:Entschlüsseln, kms:ReEncryptFrom). Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	AWS Config	Empfehlungen
1380	iam-policy-no-statements-with-full-access	Stellen Sie sicher, dass IAM-Aktionen nur auf die benötigte n Aktionen beschränkt sind. Wenn Benutzern mehr Rechte eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und der Aufgabentrennung verstoßen.
1388	restricted-common-ports	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherste llen, dass gemeinsame Ports für Amazon Elastic Compute Cloud (Amazon EC2) - Sicherheitsgruppen eingeschr änkt sind. Wenn der Zugriff auf Ports nicht auf vertrauen swürdige Quellen beschränk t wird, kann dies zu Angriffen auf die Verfügbarkeit, Integritä t und Vertraulichkeit von Systemen führen. Mit dieser Regel können Sie optional die Parameter blockedPort1–block edPort5 festlegen (Standard konfigurationen: 20, 21, 3389, 3306, 4333). Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprech en.

Kontroll-ID	AWS Config	Empfehlungen
1388	vpc-sg-open-only-to-authorized-ports	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass gemeinsame Ports für Amazon Elastic Compute Cloud (Amazon EC2) - Sicherheitsgruppen eingeschränkt sind. Wenn der Zugriff auf Ports nicht auf vertrauenswürdige Quellen beschränkt wird, kann dies zu Angriffen auf die Verfügbarkeit, Integrität und Vertraulichkeit von Systemen führen. Durch die Beschränkung des Zugriffs auf Ressourcen innerhalb einer Sicherheitsgruppe aus dem Internet (0.0.0.0/0) kann der Fernzugriff auf interne Systeme gesteuert werden.

Kontroll-ID	AWS Config	Empfehlungen
1401	iam-root-access-key-überprüfen	Der Zugriff auf Systeme und Ressourcen kann gesteuert werden, indem überprüft wird, ob der Root-Benutzer keine Zugriffsschlüssel mit seiner AWS Identity and Access Management (IAM) -Rolle verknüpft hat. Stellen Sie sicher, dass die Root-Zugriffsschlüssel gelöscht werden. Erstellen und verwenden Sie stattdessen rollenbasierte Funktionen, AWS-Konten um das Prinzip der geringsten Funktionalität zu berücksichtigen.
1401	iam-user-mfa-enabled	Aktivieren Sie diese Regel, um den Zugriff auf Ressourcen in der AWS -Cloud einzuschränken. Diese Regel stellt sicher, dass die Multi-Faktor-Authentifizierung (MFA) für alle Benutzer aktiviert ist. MFA bietet eine weitere Schutzebene zusätzlich zum Benutzernamen und Passwort. Reduzieren Sie Fälle von kompromittierten Konten, indem Sie MFA für Benutzer vorschreiben.

Kontroll-ID	AWS Config	Empfehlungen
1401	mfa-enabled-for-iam-Konsolenzugriff	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass MFA für alle AWS Identity and Access Management (IAM) -Benutzer aktiviert ist, die über ein Konsolenkennwort verfügen. MFA sorgt für eine weitere Schutzebene zusätzlich zu den Anmeldeinformationen. Indem Sie MFA für Benutzer vorschreiben, können Sie Fälle kompromittierter Konten reduzieren und verhindern, dass unbefugte Benutzer auf vertrauliche Daten zugreifen.
1401	root-account-hardware-mfa-aktiviert	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Hardware-MFA für den Root-Benutzer aktiviert ist. Der Stammbenutzer ist der AWS-Konto-Benutzer mit den meisten Berechtigungen. MFA sorgt für eine weitere Schutzebene zusätzlich zu den Anmeldeinformationen. Indem Sie MFA für den Root-Benutzer vorschreiben, können Sie die Anzahl AWS-Konten kompromittierter Benutzer reduzieren.

Kontroll-ID	AWS Config	Empfehlungen
1401	root-account-mfa-enabled	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass MFA für den Root-Benutzer aktiviert ist. Der Stammbenutzer ist der AWS-Konto-Benutzer mit den meisten Berechtigungen. MFA bietet eine weitere Schutzebene zusätzlich zum Benutzernamen und Passwort. Indem Sie MFA für den Root-Benutzer vorschreiben, können Sie die Anzahl AWS-Konten kompromittierter Benutzer reduzieren.

Kontroll-ID	AWS Config	Empfehlungen
1402	iam-password-policy	Die Identitäten und Anmeldein formationen werden auf der Grundlage einer organisat orischen IAM-Passwortrichtl inie ausgestellt, verwaltet und verifiziert. Sie erfüllen oder übertreffen die Anforderungen von NIST SP 800-63 und dem Standard „Best Practices“ von AWS Foundational Security für die Passwortstärke. Mit dieser Regel können Sie optional RequireUppercaseCharacters (Wert für AWS grundlege nde Sicherheitsbewährte Methoden: wahr), RequireLo wercaseCharacters (Wert für bewährte Methoden für AWS grundlegende Sicherheit: wahr), RequireSymbols (Wert für bewährte Methoden für AWS grundlegende Sicherhei t: wahr), RequireNumbers (Wert für bewährte Methoden für AWS grundlegende Sicherheit: wahr), MinimumPa sswordLength (Wert für bewährte Methoden für AWS grundlegende Sicherheit: 14), PasswordReusePreve ntion (Wert für bewährte Methoden für AWS grundlege nde Sicherheit: 24) und MaxPasswordAge (Wert

Kontroll-ID	AWS Config	Empfehlungen
		für bewährte Methoden für AWS grundlegende Sicherhei t: 90) für Ihr IAM festlegen Kennwortrichtlinie. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisat ion entsprechen.
1404	iam-user-unused-credentials-überprüfen	AWS Identity and Access Management (IAM) kann Ihnen bei Zugriffsberechtigu ngen und Autorisierungen helfen, indem es nach IAM-Passwörtern und Zugriffss chlüsseln sucht, die für einen bestimmten Zeitraum nicht verwendet wurden. Wenn ungenutzte Anmeldein formationen identifiziert werden, müssen Sie sie deaktivieren und/oder entfernen, da dies gegen das Prinzip der geringste n Berechtigung verstoßen könnte. Für diese Regel müssen Sie einen Wert für das maxCredentialUsage Alter festlegen (Standardkonfigura tion: 90). Der tatsächliche Wert muss den Richtlinien Ihrer Organisation entsprech en.

Kontroll-ID	AWS Config	Empfehlungen
1405	cloud-trail-cloud-watch-logs-aktiviert	Verwenden Sie Amazon CloudWatch , um Protokoll ereignisaktivitäten zentral zu sammeln und zu verwalten . Die Aufnahme von AWS CloudTrail Daten liefert Einzelheiten zu den API-Aufru faktivitäten in Ihrem AWS-Konto.
1405	cloudtrail-enabled	AWS CloudTrail kann durch die Aufzeichnung von Aktionen und API-Aufrufen in der AWS Management Console bei der Nichtabst reitbarkeit helfen. Sie können die Benutzer und die Benutzer AWS-Konten , die einen AWS Dienst aufgerufen haben, die Quell-IP-Adresse, über die die Aufrufe generiert wurden, und den Zeitpunkt der Anrufe identifizieren. Einzelheiten zu den erfassten Daten finden Sie in den AWS CloudTrail Datensatzinhalten.
1405	multi-region-cloudtrail-enabled	MULTI_REGION_CLOUD _TRAIL_ENABLED

Kontroll-ID	AWS Config	Empfehlungen
1405	cloudtrail-security-trail-enabled	Diese Regel trägt dazu bei, die Verwendung der AWS empfohlenen bewährten Sicherheitsmethoden für sicherzustellen AWS CloudTrail, indem geprüft wird, ob mehrere Einstellungen aktiviert sind. Dazu gehören die Verwendung von Protokoll verschlüsselung, Protokoll validierung und Aktivierung AWS CloudTrail in mehreren Regionen.
1405	elasticsearch-logs-to-cloud watch	Stellen Sie sicher, dass für Amazon OpenSearch Service-Domains Fehlerprotokolle aktiviert und zur Aufbewahr ung und Beantwortung an Amazon CloudWatch Logs gestreamt werden. Domain-Fehlerprotokolle sind bei Sicherheits- und Zugriffsp rüfungen sowie bei der Diagnose von Verfügbar keitsproblemen nützlich.

Kontroll-ID	AWS Config	Empfehlungen
1405	api-gw-execution-logging-aktiviert	Die API-Gateway-Protokollierung zeigt detaillierte Ansichten der Benutzer, die auf die API zugegriffen haben, und wie diese Benutzer auf die API zugegriffen haben. Diese Einblicke ermöglichen die Transparenz von Benutzeraktivitäten.
1405	cloudtrail-s3-dataevents-enabled	Die Erfassung von Simple Storage Service (Amazon S3)-Datenereignissen unterstützt die Erkennung von ungewöhnlichen Aktivitäten. Zu den Details gehören Informationen zu dem AWS -Konto, das auf einen Amazon-S3-Bucket zugegriffen hat, die IP-Adresse und die Uhrzeit des Ereignisses.
1405	rds-logging-enabled	Um die Protokollierung und Überwachung in Ihrer Umgebung zu erleichtern, stellen Sie sicher, dass die Amazon Relational Database Service (Amazon RDS)-Protokollierung aktiviert ist. Mit der Amazon-RDS-Protokollierung können Sie Ereignisse wie Verbindungen, Verbindungsabbrüche, Abfragen oder abgefragte Tabellen erfassen.

Kontroll-ID	AWS Config	Empfehlungen
1405	redshift-cluster-configuration-check	Um Daten im Ruhezustand zu schützen, muss die Verschlüsselung für Ihre Amazon-Redshift-Cluster aktiviert sein. Sie müssen auch sicherstellen, dass die erforderlichen Konfigurationen auf Amazon-Redshift-Clustern bereitgestellt werden. Die Prüfungsprotokollierung muss aktiviert sein, um Informationen zu Verbindungen und Benutzeraktivitäten in der Datenbank bereitzustellen. Diese Regel erfordert, dass ein Wert für clusterDbEncrypted (Config Default: TRUE) und LoggingEnabled (Config Default: TRUE) gesetzt ist. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	AWS Config	Empfehlungen
1405	s-3 bucket-logging-enabled	Die Amazon Simple Storage Service (Amazon S3)-Serverzugriffsprotokollierung bietet eine Methode zur Überwachung des Netzwerks im Hinblick auf potenzielle Cybersicherheitsereignisse. Die Ereignisse werden überwacht, indem detaillierte Aufzeichnungen über die Anfragen erfasst werden, die an einen Amazon-S3-Bucket gestellt wurden. Jeder Zugriffsprotokolleintrag enthält Details zu einer einzelnen Zugriffsanfrage. Zu den Details gehören Auftraggeber, Bucket-Name, Anforderungszeit, Anforderungsaktion, Antwortstatus und Fehlercode, falls relevant.

Kontroll-ID	AWS Config	Empfehlungen
1405	vpc-flow-logs-enabled	VPC-Flow-Protokolle erfassen detaillierte Informationsdatensätze über den IP-Datenverkehr, der zu und von Netzwerkschnittstellen in Ihrer Amazon Virtual Private Cloud (Amazon VPC) fließt. Standardmäßig enthalten Flow-Protokolldatensätze Werte für die verschiedenen Komponenten des IP-Flows, einschließlich Quelle, Ziel und Protokoll.
1405	wafv2-logging-enabled	Um die Protokollierung und Überwachung in Ihrer Umgebung zu erleichtern, aktivieren Sie die AWS WAF (V2) -Protokollierung im regionalen und globalen Web. ACLs AWS Die WAF-Protokollierung bietet detaillierte Informationen über den Datenverkehr, der von Ihrer Web-ACL analysiert wird. In den Protokollen werden die Uhrzeit aufgezeichnet, zu der die AWS WAF die Anfrage von Ihrer AWS Ressource erhalten hat, Informationen über die Anfrage und eine Aktion für die Regel, der jede Anfrage entsprach.

Kontroll-ID	AWS Config	Empfehlungen
1405	elb-logging-enabled	Die Elastic-Load-Balancing-Aktivität ist ein zentraler Kommunikationspunkt innerhalb einer Umgebung. Stellen Sie sicher, dass die ELB-Protokollierung aktiviert ist. Die gesammelten Daten enthalten detaillierte Informationen zu Anfragen, die an den ELB gesendet wurden. Jedes Protokoll enthält Informationen wie die Zeit, zu der die Anforderung einging, die Client-IP-Adresse, Latenzen, Anforderungspfade und Serverantworten.
1405	codebuild-project-logging-enabled	Stellen Sie sicher, dass die AWS CodeBuild Projektprotokollierung aktiviert ist, damit Ihre Build-Ausgabeprotokolle entweder an Amazon CloudWatch oder Amazon Simple Storage Service (Amazon S3) gesendet werden. Build-Ausgabeprotokolle enthalten detaillierte Informationen zu Ihrem Build-Projekt.

Kontroll-ID	AWS Config	Empfehlungen
1405	redshift-audit-logging-enabled	Aktivieren Sie die Prüfungsprotokollierung, um Informationen über Verbindungen und Benutzeraktivitäten in Ihrem Amazon-Redshift-Cluster zu erfassen.
1405	opensearch-audit-logging-enabled	Stellen Sie sicher, dass die Audit-Protokollierung für Ihre Amazon OpenSearch Service-Domains aktiviert ist. Mit der Audit-Protokollierung können Sie Benutzeraktivitäten auf Ihren OpenSearch Domains verfolgen, einschließlich erfolgreicher und fehlgeschlagener Authentifizierungen OpenSearch, Anfragen an, Indexänderungen und eingehende Suchanfragen.
1405	opensearch-logs-to-cloudwatch	Stellen Sie sicher, dass für Amazon OpenSearch Service-Domains Fehlerprotokolle aktiviert und zur Aufbewahrung und Beantwortung an Amazon CloudWatch Logs gestreamt werden. OpenSearch Service-Fehlerprotokolle können bei Sicherheits- und Zugriffsprüfungen helfen und bei der Diagnose von Verfügbarkeitsproblemen helfen.

Kontroll-ID	AWS Config	Empfehlungen
1490	alb-waf-enabled	Stellen Sie sicher, dass AWS WAF auf Elastic Load Balancers (ELB) aktiviert ist, um Webanwendungen zu schützen. Eine WAF trägt zum Schutz Ihrer Webanwendungen oder APIs vor gängigen Web-Exploits bei. Diese Web-Exploits können sich auf die Verfügbarkeit auswirken, die Sicherheit gefährden oder übermäßige Ressourcen in Ihrer Umgebung verbrauchen.
1490	api-gw-associated-with-WAF	AWS Mit WAF können Sie eine Reihe von Regeln (als Web Access Control List (Web ACL) bezeichnet) konfigurieren, die Webanfragen auf der Grundlage von anpassbaren Websicherheitsregeln und -bedingungen, die Sie definieren, zulassen, blockieren oder zählen. Stellen Sie sicher, dass Ihre Amazon-API-Gateway-Stufe mit einer WAF-Web-ACL verknüpft ist, um sie vor böswilligen Angriffen zu schützen.

Kontroll-ID	AWS Config	Empfehlungen
1490	waf-regional-rule-not-leer	Stellen Sie sicher, dass Ihre AWS WAF eine Regel hat, die nicht leer ist. Eine Regel ohne Bedingungen kann zu unbeabsichtigtem Verhalten führen.
1490	waf-regional-rulegroup-not-leer	Stellen Sie sicher, dass Ihre AWS WAF eine Regelgrup pe hat, die nicht leer ist. Eine leere Regelgruppe kann zu unbeabsichtigtem Verhalten führen.
1490	waf-regional-webacl-not-leer	Eine an eine AWS WAF angehängte Web-ACL kann eine Sammlung von Regeln und Regelgruppen zur Überprüfung und Steuerung von Webanfragen enthalten . Wenn eine Web-ACL leer ist, wird der Webdatenverkehr weitergeleitet, ohne von der WAF erkannt oder bearbeitet zu werden.

Kontroll-ID	AWS Config	Empfehlungen
1490	ec2-prüfen managedinstance-association-compliance-status	Verwenden Sie AWS Systems Manager Associations, um bei der Inventarisierung von Softwareplattformen und Anwendungen innerhalb eines Unternehmens zu helfen. AWS Systems Manager weist Ihren verwalteten Instances einen Konfigurationsstatus zu und ermöglicht es Ihnen, Basiswerte für Betriebss ystem-Patch-Levels, Softwarei nstallationen, Anwendung skonfigurationen und andere Details zu Ihrer Umgebung festzulegen.
1501	ec2-prüfen managedinstance-patch-compliance-status	Aktivieren Sie diese Regel, um bei der Identifizierung und Dokumentation von Sicherhei tslücken in Amazon Elastic Compute Cloud (Amazon EC2) zu helfen. Die Regel prüft, ob die EC2 Amazon-In stance die Patch-Konformität im AWS Systems Manager gemäß den Richtlinien und Verfahren Ihrer Organisation einhält.

Kontroll-ID	AWS Config	Empfehlungen
1504	iam-root-access-key-überprüfen	Der Zugriff auf Systeme und Ressourcen kann gesteuert werden, indem überprüft wird, ob der Root-Benutzer keine Zugriffsschlüssel mit seiner AWS Identity and Access Management (IAM) -Rolle verknüpft hat. Stellen Sie sicher, dass die Root-Zugriffsschlüssel gelöscht werden. Erstellen und verwenden Sie stattdessen rollenbasierte Funktionen, AWS-Konten um das Prinzip der geringsten Funktionalität zu berücksichtigen.
1504	iam-user-mfa-enabled	Aktivieren Sie diese Regel, um den Zugriff auf Ressourcen in der AWS -Cloud einzuschränken. Diese Regel stellt sicher, dass die Multi-Faktor-Authentifizierung (MFA) für alle Benutzer aktiviert ist. MFA bietet eine weitere Schutzebene zusätzlich zum Benutzernamen und Passwort. Reduzieren Sie Fälle von kompromittierten Konten, indem Sie MFA für Benutzer vorschreiben.

Kontroll-ID	AWS Config	Empfehlungen
1504	mfa-enabled-for-iam-Konsolenzugriff	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass MFA für alle AWS Identity and Access Management (IAM) -Benutzer aktiviert ist, die über ein Konsolenkennwort verfügen. MFA sorgt für eine weitere Schutzebene zusätzlich zu den Anmeldeinformationen. Indem Sie MFA für Benutzer vorschreiben, können Sie Fälle kompromittierter Konten reduzieren und verhindern, dass unbefugte Benutzer auf vertrauliche Daten zugreifen.
1504	root-account-hardware-mfa-aktiviert	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Hardware-MFA für den Root-Benutzer aktiviert ist. Der Stammbenutzer ist der AWS-Konto-Benutzer mit den meisten Berechtigungen. MFA sorgt für eine weitere Schutzebene zusätzlich zu den Anmeldeinformationen. Indem Sie MFA für den Root-Benutzer vorschreiben, können Sie die Anzahl AWS-Konten kompromittierter Benutzer reduzieren.

Kontroll-ID	AWS Config	Empfehlungen
1504	root-account-mfa-enabled	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass MFA für den Root-Benutzer aktiviert ist. Der Stammbenutzer ist der AWS-Konto-Benutzer mit den meisten Berechtigungen. MFA bietet eine weitere Schutzebene zusätzlich zum Benutzernamen und Passwort. Indem Sie MFA für den Root-Benutzer vorschreiben, können Sie die Anzahl AWS-Konten kompromittierter Benutzer reduzieren.
1509	cloud-trail-cloud-watch-logs-aktiviert	Verwenden Sie Amazon CloudWatch , um Protokollereignisaktivitäten zentral zu sammeln und zu verwalten . Die Aufnahme von AWS CloudTrail Daten liefert Einzelheiten zu den API-Aufrufaktivitäten in Ihrem AWS-Konto.

Kontroll-ID	AWS Config	Empfehlungen
1509	cloudtrail-enabled	AWS CloudTrail kann durch die Aufzeichnung von Aktionen und API-Aufrufen in der AWS Management Console bei der Nichtabst reitbarkeit helfen. Sie können die Benutzer und die Benutzer AWS-Konten , die einen AWS Dienst aufgerufen haben, die Quell-IP-Adresse, über die die Aufrufe generiert wurden, und den Zeitpunkt der Anrufe identifizieren. Einzelheiten zu den erfassten Daten finden Sie in den AWS CloudTrail Datensatzinhalten.

Kontroll-ID	AWS Config	Empfehlungen
1509	multi-region-cloudtrail-enabled	AWS CloudTrail zeichnet Aktionen und API-Aufrufe der AWS Management Console auf. Sie können feststellen, welche Benutzer und Konten angerufen wurden AWS, von welcher Quell-IP-Adresse aus die Anrufe getätigt wurden und wann die Anrufe erfolgten . CloudTrail übermittelt Protokolldateien aus allen AWS Regionen an Ihren S3-Bucket, wenn MULTI_REG ION_CLOUD_TRAIL_EN ABLED aktiviert ist. Außerdem wird beim AWS Start einer neuen Region derselbe Trail in der neuen Region erstellt. CloudTrail Dadurch erhalten Sie automatisch Protokoll dateien mit API-Aktivitäten für die neue Region.

Kontroll-ID	AWS Config	Empfehlungen
1509	cloudtrail-security-trail-enabled	Diese Regel trägt dazu bei, die Verwendung der AWS empfohlenen bewährten Sicherheitsmethoden für sicherzustellen AWS CloudTrail, indem geprüft wird, ob mehrere Einstellungen aktiviert sind. Dazu gehören die Verwendung von Protokoll verschlüsselung, Protokoll validierung und Aktivierung AWS CloudTrail in mehreren Regionen.
1509	elasticsearch-logs-to-cloud watch	Stellen Sie sicher, dass für Amazon OpenSearch Service-Domains Fehlerprotokolle aktiviert und zur Aufbewahr ung und Beantwortung an Amazon CloudWatch Logs gestreamt werden. Domain-Fehlerprotokolle sind bei Sicherheits- und Zugriffsp rüfungen sowie bei der Diagnose von Verfügbar keitsproblemen nützlich.

Kontroll-ID	AWS Config	Empfehlungen
1509	api-gw-execution-logging-aktiviert	Die API-Gateway-Protokollierung zeigt detaillierte Ansichten der Benutzer, die auf die API zugegriffen haben, und wie diese Benutzer auf die API zugegriffen haben. Diese Einblicke ermöglichen die Transparenz von Benutzeraktivitäten.
1509	cloudtrail-s3-dataevents-enabled	Die Erfassung von Simple Storage Service (Amazon S3)-Datenereignissen unterstützt die Erkennung von ungewöhnlichen Aktivitäten. Zu den Details gehören Informationen zu dem AWS -Konto, das auf einen Amazon-S3-Bucket zugegriffen hat, die IP-Adresse und die Uhrzeit des Ereignisses.
1509	rds-logging-enabled	Um die Protokollierung und Überwachung in Ihrer Umgebung zu erleichtern, stellen Sie sicher, dass die Amazon Relational Database Service (Amazon RDS)-Protokollierung aktiviert ist. Mit der Amazon-RDS-Protokollierung können Sie Ereignisse wie Verbindungen, Verbindungsabbrüche, Abfragen oder abgefragte Tabellen erfassen.

Kontroll-ID	AWS Config	Empfehlungen
1509	redshift-cluster-configuration-check	Um Daten im Ruhezustand zu schützen, muss die Verschlüsselung für Ihre Amazon-Redshift-Cluster aktiviert sein. Sie müssen auch sicherstellen, dass die erforderlichen Konfigurationen auf Amazon-Redshift-Clustern bereitgestellt werden. Die Prüfungsprotokollierung muss aktiviert sein, um Informationen zu Verbindungen und Benutzeraktivitäten in der Datenbank bereitzustellen. Diese Regel erfordert, dass ein Wert für clusterDbEncrypted (Config Default: TRUE) und LoggingEnabled (Config Default: TRUE) gesetzt ist. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	AWS Config	Empfehlungen
1509	s-3 bucket-logging-enabled	Die Amazon Simple Storage Service (Amazon S3)-Serverzugriffsprotokollierung bietet eine Methode zur Überwachung des Netzwerks im Hinblick auf potenzielle Cybersicherheitsereignisse. Die Ereignisse werden überwacht, indem detaillierte Aufzeichnungen über die Anfragen erfasst werden, die an einen Amazon-S3-Bucket gestellt wurden. Jeder Zugriffsprotokolleintrag enthält Details zu einer einzelnen Zugriffsanfrage. Zu den Details gehören Auftraggeber, Bucket-Name, Anforderungszeit, Anforderungsaktion, Antwortstatus und Fehlercode, falls relevant.

Kontroll-ID	AWS Config	Empfehlungen
1509	vpc-flow-logs-enabled	VPC-Flow-Protokolle erfassen detaillierte Informationsdatensätze über den IP-Datenverkehr, der zu und von Netzwerkschnittstellen in Ihrer Amazon Virtual Private Cloud (Amazon VPC) fließt. Standardmäßig enthalten Flow-Protokolldatensätze Werte für die verschiedenen Komponenten des IP-Flows, einschließlich Quelle, Ziel und Protokoll.
1509	wafv2-logging-enabled	Um die Protokollierung und Überwachung in Ihrer Umgebung zu erleichtern, aktivieren Sie die AWS WAF (V2) -Protokollierung im regionalen und globalen Web. ACLs AWS Die WAF-Protokollierung bietet detaillierte Informationen über den Datenverkehr, der von Ihrer Web-ACL analysiert wird. In den Protokollen werden die Uhrzeit aufgezeichnet, zu der die AWS WAF die Anfrage von Ihrer AWS Ressource erhalten hat, Informationen über die Anfrage und eine Aktion für die Regel, der jede Anfrage entsprach.

Kontroll-ID	AWS Config	Empfehlungen
1509	elb-logging-enabled	Die Elastic-Load-Balancing-Aktivität ist ein zentraler Kommunikationspunkt innerhalb einer Umgebung. Stellen Sie sicher, dass die ELB-Protokollierung aktiviert ist. Die gesammelten Daten enthalten detaillierte Informati onen zu Anfragen, die an den ELB gesendet wurden. Jedes Protokoll enthält Informati onen wie die Zeit, zu der die Anforderung einging, die Client-IP-Adresse, Latenzen, Anforderungspfade und Serverantworten.
1509	codebuild-project-logging-e nabled	Stellen Sie sicher, dass die AWS CodeBuild Projektpr otokollierung aktiviert ist, damit Ihre Build-Ausgabeproto kolle entweder an Amazon CloudWatch oder Amazon Simple Storage Service (Amazon S3) gesendet werden. Build-Ausgabeproto kolle enthalten detaillierte Informationen zu Ihrem Build-Projekt.

Kontroll-ID	AWS Config	Empfehlungen
1509	redshift-audit-logging-enabled	Aktivieren Sie die Prüfungsprotokollierung, um Informationen über Verbindungen und Benutzeraktivitäten in Ihrem Amazon-Redshift-Cluster zu erfassen.
1509	opensearch-audit-logging-enabled	Stellen Sie sicher, dass die Audit-Protokollierung für Ihre Amazon OpenSearch Service-Domains aktiviert ist. Mit der Audit-Protokollierung können Sie Benutzeraktivitäten auf Ihren OpenSearch Domains verfolgen, einschließlich erfolgreicher und fehlgeschlagener Authentifizierungen OpenSearch, Anfragen an, Indexänderungen und eingehende Suchanfragen.
1509	opensearch-logs-to-cloudwatch	Stellen Sie sicher, dass für Amazon OpenSearch Service-Domains Fehlerprotokolle aktiviert und zur Aufbewahrung und Beantwortung an Amazon CloudWatch Logs gestreamt werden. OpenSearch Service-Fehlerprotokolle können bei Sicherheits- und Zugriffsprüfungen helfen und bei der Diagnose von Verfügbarkeitsproblemen helfen.

Kontroll-ID	AWS Config	Empfehlungen
1511	db-instance-backup-enabled	Die Sicherungsfunktion von Amazon RDS erstellt Sicherungen Ihrer Datenbank en und Transaktionsprotokolle. Amazon RDS erstellt einen Snapshot für das Speicherv olume Ihrer DB-Instance, sodass die gesamte DB-Instance gesichert wird. Sie können im System spezifisc he Aufbewahrungsfristen festlegen, um Ihre Ausfallsi cherheitsanforderungen zu erfüllen.
1511	dynamodb-in-backup-plan	Um Sie bei Datensich erungsprozessen zu unterstüt zen, stellen Sie sicher, dass Ihre Amazon DynamoDB-Tabellen Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherung smanagement und erleichte rt Ihnen die Erfüllung von geschäftlichen und behördlic hen Compliance-Anforde rungen hinsichtlich Datensich erungen.

Kontroll-ID	AWS Config	Empfehlungen
1511	dynamodb-pitr-enabled	Aktivieren Sie diese Regel, um zu überprüfen, ob die Informationen gesichert wurden. Es verwaltet auch die Backups, indem es sicherste llt, dass die point-in-time Wiederherstellung in Amazon DynamoDB aktiviert ist. Bei der Wiederherstellung werden fortlaufende Backups Ihrer Tabelle für die letzten 35 Tage gespeichert.
1511	ebs-in-backup-plan	Stellen Sie zur Unterstützung der Datensicherungsprozesse sicher, dass Ihre Amazon Elastic Block Store (Amazon EBS) -Volumes Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihre Backup-Ve rwaltung und ermöglicht es Ihnen, Ihre geschäftlichen und behördlichen Anforderungen bezüglich Backups zu erfüllen.

Kontroll-ID	AWS Config	Empfehlungen
1511	efs-in-backup-plan	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon Elastic File System (Amazon EFS) - Dateisysteme Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.
1511	elasticache-redis-cluster-automatic-Backup-Check	Wenn automatische Backups aktiviert sind, ElastiCache erstellt Amazon täglich ein Backup des Clusters. Die Sicherung kann für eine von Ihrer Organisation festgelegte Anzahl von Tagen aufbewahrt werden. Automatische Backups schützen vor Datenverlust. Bei einem Ausfall können Sie einen neuen Cluster erstellen, der Ihre Daten aus dem aktuellen Backup wiederherstellt.

Kontroll-ID	AWS Config	Empfehlungen
1511	rds-in-backup-plan	Um Sie bei Datensich erungsprozessen zu unterstüt zen, stellen Sie sicher, dass Ihre Amazon Relational Database Service (Amazon RDS) -Instances Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherung smanagement und erleichte rt Ihnen die Erfüllung von geschäftlichen und behördlic hen Compliance-Anforde rungen hinsichtlich Datensich erungen.

Kontroll-ID	AWS Config	Empfehlungen
1511	s-3 bucket-versioning-enabled	Die Versionsverwaltung von Amazon Simple Storage Service (Amazon S3)-Buckets hilft dabei, mehrere Varianten eines Objekts im selben Amazon-S3-Bucket zu speichern. Verwenden Sie die Versionsverwaltung, um sämtliche Versionen aller Objekte in Ihrem Amazon-S3-Bucket zu speichern, abzurufen oder wiederher zustellen. Mit der Versionsv erwaltung können Sie Versionen sowohl nach unbeabsichtigten Benutzera ktionen als auch nach Anwendungsfehlern problemlo s wiederherstellen.

Kontroll-ID	AWS Config	Empfehlungen
1511	redshift-backup-enabled	Stellen Sie zur Unterstützung der Datensicherungsprozesse sicher, dass Ihre Amazon-Redshift-Cluster über automatisierte Snapshots verfügen. Wenn automatisierte Snapshots für einen Cluster aktiviert sind, erstellt Redshift in regelmäßigen Abständen Snapshots dieses Clusters. Standardmäßig erstellt Redshift alle acht Stunden oder alle 5 GB einen Snapshot für jeden Knoten mit Datenänderungen oder je nachdem, was zuerst eintritt.
1511	aurora-resources-protected-by-Ersatzplan	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon Aurora Aurora-Ressourcen Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	AWS Config	Empfehlungen
1511	backup-plan-min-frequency-and-min-retention-check	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihr AWS Backup-Plan auf eine Mindestfrequenz und Aufbewahrung festgelegt ist. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen. Mit dieser Regel können Sie die Parameter requiredFrequencyValue (Config default: 1), requiredRetentionDays (Config default: 35) und requiredFrequencyUnit (Config default: days) festlegen. Der tatsächliche Wert muss den Anforderungen Ihrer Organisation entsprechen.

Kontroll-ID	AWS Config	Empfehlungen
1511	backup-recovery-point-minimum-Aufbewahrungsprüfung	Um bei Datensicherungsprozessen zu helfen, stellen Sie sicher, dass für Ihre AWS Backup-Wiederherstellungspunkte eine Mindestaufbewahrungsdauer festgelegt ist. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen. Mit dieser Regel können Sie den Parameter requiredRetentionDays (Config Default: 35) festlegen. Der tatsächliche Wert muss den Anforderungen Ihrer Organisation entsprechen.

Kontroll-ID	AWS Config	Empfehlungen
1511	ec2--Plan resources-protected-by-backup	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon Elastic Compute Cloud (Amazon EC2) - Ressourcen Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	AWS Config	Empfehlungen
1511	fsx-resources-protected-by-Ersatzplan	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre FSx Amazon-Dateisysteme Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.
1511	s-3 bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) unterstützt die Aufrechterhaltung einer angemessenen Kapazität und Verfügbarkeit. CRR ermöglicht das automatische, asynchrone Kopieren von Objekten in Amazon-S3-Buckets, um die Datenverfügbarkeit sicherzustellen.

Kontroll-ID	AWS Config	Empfehlungen
1511	backup-plan-min-frequency-and-min-retention-check	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihr AWS Backup-Plan auf eine Mindestfrequenz und Aufbewahrung festgelegt ist. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen. Mit dieser Regel können Sie die Parameter requiredFrequencyValue (Config default: 1), requiredRetentionDays (Config default: 35) und requiredFrequencyUnit (Config default: days) festlegen. Der tatsächliche Wert muss den Anforderungen Ihrer Organisation entsprechen.

Kontroll-ID	AWS Config	Empfehlungen
1511	backup-recovery-point-manual-Löschen-deaktiviert	Stellen Sie sicher, dass Ihren AWS Backup-Wiederherstellungspunkten eine ressourcenbasierte Richtlinie zugeordnet ist, die das Löschen von Wiederherstellungspunkten verhindert. Die Verwendung einer ressourcenbasierten Richtlinie zur Verhinderung des Löschens von Wiederherstellungspunkten kann dazu beitragen, ein versehentliches oder absichtliches Löschen zu unterbinden.
1515	db-instance-backup-enabled	Die Sicherungsfunktion von Amazon RDS erstellt Sicherungen Ihrer Datenbanken und Transaktionsprotokolle. Amazon RDS erstellt einen Snapshot für das Speichervolume Ihrer DB-Instance, sodass die gesamte DB-Instance gesichert wird. Sie können im System spezifische Aufbewahrungsfristen festlegen, um Ihre Ausfallsicherheitsanforderungen zu erfüllen.

Kontroll-ID	AWS Config	Empfehlungen
1515	dynamodb-in-backup-plan	Um Sie bei Datensich erungsprozessen zu unterstüt zen, stellen Sie sicher, dass Ihre Amazon DynamoDB-Tabellen Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherung smanagement und erleichte rt Ihnen die Erfüllung von geschäftlichen und behördlic hen Compliance-Anforde rungen hinsichtlich Datensich erungen.
1515	ebs-in-backup-plan	Stellen Sie zur Unterstützung der Datensicherungsprozesse sicher, dass Ihre Amazon Elastic Block Store (Amazon EBS) -Volumes Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihre Backup-Ve rwaltung und ermöglicht es Ihnen, Ihre geschäftlichen und behördlichen Anforderungen bezüglich Backups zu erfüllen.

Kontroll-ID	AWS Config	Empfehlungen
1515	efs-in-backup-plan	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon Elastic File System (Amazon EFS) - Dateisysteme Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.
1515	elasticache-redis-cluster-automatic-Backup-Check	Wenn automatische Backups aktiviert sind, ElastiCache erstellt Amazon täglich ein Backup des Clusters. Die Sicherung kann für eine von Ihrer Organisation festgelegte Anzahl von Tagen aufbewahrt werden. Automatische Backups schützen vor Datenverlust. Bei einem Ausfall können Sie einen neuen Cluster erstellen, der Ihre Daten aus dem aktuellen Backup wiederherstellt.

Kontroll-ID	AWS Config	Empfehlungen
1515	rds-in-backup-plan	Um Sie bei Datensich erungsprozessen zu unterstüt zen, stellen Sie sicher, dass Ihre Amazon Relational Database Service (Amazon RDS) -Instances Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherung smanagement und erleichte rt Ihnen die Erfüllung von geschäftlichen und behördlic hen Compliance-Anforde rungen hinsichtlich Datensich erungen.
1515	s-3 bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) unterstützt die Aufrechte rhaltung einer angemessenen Kapazität und Verfügbarkeit. CRR ermöglicht das automatis che, asynchrone Kopieren von Objekten in Amazon-S3 -Buckets, um die Datenverf ügbarkeit sicherzustellen.

Kontroll-ID	AWS Config	Empfehlungen
1515	s-3 bucket-versioning-enabled	Die Versionsverwaltung von Amazon Simple Storage Service (Amazon S3)-Buckets hilft dabei, mehrere Varianten eines Objekts im selben Amazon-S3-Bucket zu speichern. Verwenden Sie die Versionsverwaltung, um sämtliche Versionen aller Objekte in Ihrem Amazon-S3-Bucket zu speichern, abzurufen oder wiederher zustellen. Mit der Versionsv erwaltung können Sie Versionen sowohl nach unbeabsichtigten Benutzera ktionen als auch nach Anwendungsfehlern problemlo s wiederherstellen.

Kontroll-ID	AWS Config	Empfehlungen
1515	aurora-resources-protected-by-Backup-Plan	Um Sie bei Datensich erungsprozessen zu unterstüt zen, stellen Sie sicher, dass Ihre Amazon Aurora Aurora-Ressourcen Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherung smanagement und erleichte rt Ihnen die Erfüllung von geschäftlichen und behördlic hen Compliance-Anforde rungen hinsichtlich Datensich erungen.

Kontroll-ID	AWS Config	Empfehlungen
1515	backup-plan-min-frequency-and-min-retention-check	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihr AWS Backup-Plan auf eine Mindestfrequenz und Aufbewahrung festgelegt ist. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen. Mit dieser Regel können Sie die Parameter requiredFrequencyValue (Config default: 1), requiredRetentionDays (Config default: 35) und requiredFrequencyUnit (Config default: days) festlegen. Der tatsächliche Wert muss den Anforderungen Ihrer Organisation entsprechen.

Kontroll-ID	AWS Config	Empfehlungen
1515	backup-recovery-point-manual-löschen-deaktiviert	Stellen Sie sicher, dass Ihren AWS Backup-Wiederherstellungspunkten eine ressourcenbasierte Richtlinie zugeordnet ist, die das Löschen von Wiederherstellungspunkten verhindert. Die Verwendung einer ressourcenbasierten Richtlinie zur Verhinderung des Löschens von Wiederherstellungspunkten kann dazu beitragen, ein versehentliches oder absichtliches Löschen zu unterbinden.
1515	ec2--Plan resources-protected-by-backup	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon Elastic Compute Cloud (Amazon EC2) - Ressourcen Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	AWS Config	Empfehlungen
1515	redshift-backup-enabled	Stellen Sie zur Unterstützung der Datensicherungsprozesse sicher, dass Ihre Amazon-Redshift-Cluster über automatisierte Snapshots verfügen. Wenn automatisierte Snapshots für einen Cluster aktiviert sind, erstellt Redshift in regelmäßigen Abständen Snapshots dieses Clusters. Standardmäßig erstellt Redshift alle acht Stunden oder alle 5 GB einen Snapshot für jeden Knoten mit Datenänderungen oder je nachdem, was zuerst eintritt.
1536	cloudtrail-s3-dataevents-enabled	Die Erfassung von Simple Storage Service (Amazon S3)-Datenereignissen unterstützt die Erkennung von ungewöhnlichen Aktivitäten. Zu den Details gehören Informationen zu dem AWS -Konto, das auf einen Amazon-S3-Bucket zugegriffen hat, die IP-Adresse und die Uhrzeit des Ereignisses.

Kontroll-ID	AWS Config	Empfehlungen
1537	rds-logging-enabled	Um die Protokollierung und Überwachung in Ihrer Umgebung zu erleichtern, stellen Sie sicher, dass die Amazon Relational Database Service (Amazon RDS)-Protokollierung aktiviert ist. Mit der Amazon-RDS-Protokollierung können Sie Ereignisse wie Verbindungen, Verbindungsabbrüche, Abfragen oder abgefragte Tabellen erfassen.

Kontroll-ID	AWS Config	Empfehlungen
1537	redshift-cluster-configuration-check	Um Daten im Ruhezustand zu schützen, muss die Verschlüsselung für Ihre Amazon-Redshift-Cluster aktiviert sein. Sie müssen auch sicherstellen, dass die erforderlichen Konfigurationen auf Amazon-Redshift-Clustern bereitgestellt werden. Die Prüfungsprotokollierung muss aktiviert sein, um Informationen zu Verbindungen und Benutzeraktivitäten in der Datenbank bereitzustellen. Diese Regel erfordert, dass ein Wert für clusterDbEncrypted (Config Default: TRUE) und LoggingEnabled (Config Default: TRUE) gesetzt ist. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	AWS Config	Empfehlungen
1552	acm-certificate-expiration-check	Stellen Sie sicher, dass die Netzwerkintegrität geschützt ist, indem Sie sicherstellen, dass X509-Zertifikate von AWS ACM ausgestellt werden. Diese Zertifikate müssen gültig und dürfen nicht abgelaufe n sein. Für diese Regel ist ein Wert für erforderlich daysToExpiration (Wert für bewährte AWS Grundrege ln für Sicherheit: 90). Der tatsächliche Wert muss den Richtlinien Ihrer Organisation entsprechen.
1552	alb-http-to-https-Umleitung sprüfung	Um Daten während der Übertragung zu schützen, stellen Sie sicher, dass Ihr Application Load Balancer unverschlüsselte HTTP-Anfr agen automatisch an HTTPS umleitet. Da sensible Daten vorhanden sein können, sollten Sie die Verschlüs selung bei der Übertragung aktivieren, um diese Daten zu schützen.

Kontroll-ID	AWS Config	Empfehlungen
1552	elb-acm-certificate-required	Zum Schutz von eventuell vorhandenen sensiblen Daten sowie von Daten während der Übertragung muss die Verschlüsselung für Ihr Elastic Load Balancing aktiviert sein. Verwenden Sie AWS Certifica te Manager, um öffentlic he und private SSL/TLS-Z ertifikate mit AWS Diensten und internen Ressourcen zu verwalten, bereitzustellen und bereitzustellen.
1552	elb-tls-https-listeners-nur	Stellen Sie sicher, dass Ihre Elastic Load Balancer (ELBs) mit SSL- oder HTTPS-Lis tenern konfiguriert sind. Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	AWS Config	Empfehlungen
1552	Elb v 2 acm-certificate-required	Zum Schutz von eventuell vorhandenen sensiblen Daten sowie von Daten während der Übertragung muss die Verschlüsselung für Ihr Elastic Load Balancing aktiviert sein. Verwenden Sie AWS Certificate Manager, um öffentliche und private SSL/TLS-Zertifikate mit AWS Diensten und internen Ressourcen zu verwalten, bereitzustellen und bereitzustellen.
1579	dynamodb-autoscaling-enabled	Amazon DynamoDB Auto Scaling verwendet den AWS Application Auto Scaling-Service, um die bereitgestellte Durchsatzkapazität so anzupassen, dass sie automatisch auf tatsächliche Verkehrsmuster reagiert. Auf diese Weise kann eine Tabelle oder ein globaler sekundärer Index die bereitgestellte Lese-/Schreibkapazität erhöhen, um plötzliche Erhöhungen des Datenverkehrs ohne Drosselung zu bewältigen.

Kontroll-ID	AWS Config	Empfehlungen
1580	elb-cross-zone-load-Balancing aktiviert	Aktivieren Sie zonenüber greifendes Load Balancing für Ihre Elastic Load Balancer (ELBs), um eine angemesse ne Kapazität und Verfügbar keit aufrechtzuerhalten. Zonenübergreifendes Load Balancing reduziert die Notwendigkeit, die gleiche Anzahl von Instances in jeder aktivierten Availability Zone aufrechtzuerhalten. Dadurch wird auch die Fähigkeit Ihrer Anwendung verbessert, den Verlust einer oder mehrerer Instances zu bewältigen.

Kontroll-ID	AWS Config	Empfehlungen
1580	rds-multi-az-support	Die Multi-AZ-Unterstützung in Amazon Relational Database Service (Amazon RDS) bietet eine verbesserte Verfügbar keit und Beständigkeit von Datenbank-Instances. Wenn Sie eine Multi-AZ-Datenbank-Instance bereitstellen, erstellt Amazon RDS automatisch eine primäre Datenbank-Instance und repliziert die Daten synchron auf eine Standby-Instance in einer anderen Availability Zone. Jede Availability Zone läuft auf einer eigenen, physisch getrennten, unabhängigen Infrastruktur und ist auf eine hohe Verfügbarkeit ausgelegt . Im Falle eines Infrastru kturausfalls führt Amazon RDS einen automatischen Failover zum Standby-Modus durch, sodass Sie den Datenbank betrieb wieder aufnehmen können, sobald der Failover abgeschlossen ist.

Kontroll-ID	AWS Config	Empfehlungen
1580	rds-cluster-multi-az-aktiviert	Für Cluster von Amazon Relational Database Service (Amazon RDS) sollte die Multi-AZ-Replikation aktiviert sein, um die Verfügbar keit der gespeicherten Daten zu gewährleisten. Availability Zones werden auf einer physisch getrennte n, unabhängigen Infrastru ktur ausgeführt und sind auf höchste Zuverlässigkeit ausgelegt. Im Falle eines Infrastrukturausfalls führt Amazon RDS einen automatis chen Failover zum Standby-Modus durch, sodass Sie den Datenbankbetrieb wieder aufnehmen können, sobald der Failover abgeschlossen ist.
1650	cloud-trail-cloud-watch-logs-aktiviert	Verwenden Sie Amazon CloudWatch , um Protokoll ereignisaktivitäten zentral zu sammeln und zu verwalten . Die Aufnahme von AWS CloudTrail Daten liefert Einzelheiten zu den API-Aufru faktivitäten in Ihrem AWS-Konto.

Kontroll-ID	AWS Config	Empfehlungen
1650	cloudtrail-enabled	AWS CloudTrail kann durch die Aufzeichnung von Aktionen und API-Aufrufen in der AWS Management Console bei der Nichtabst reitbarkeit helfen. Sie können die Benutzer und die Benutzer AWS-Konten , die einen AWS Dienst aufgerufen haben, die Quell-IP-Adresse, über die die Aufrufe generiert wurden, und den Zeitpunkt der Anrufe identifizieren. Einzelheiten zu den erfassten Daten finden Sie in den AWS CloudTrail Datensatzinhalten.

Kontroll-ID	AWS Config	Empfehlungen
1650	multi-region-cloudtrail-enabled	AWS CloudTrail zeichnet Aktionen und API-Aufrufe der AWS Management Console auf. Sie können feststellen, welche Benutzer und Konten angerufen wurden AWS, von welcher Quell-IP-Adresse aus die Anrufe getätigt wurden und wann die Anrufe erfolgten . CloudTrail übermittelt Protokolldateien aus allen AWS Regionen an Ihren S3-Bucket, wenn MULTI_REG ION_CLOUD_TRAIL_EN ABLED aktiviert ist. Außerdem wird beim AWS Start einer neuen Region derselbe Trail in der neuen Region erstellt. CloudTrail Dadurch erhalten Sie automatisch Protokoll dateien mit API-Aktivitäten für die neue Region.

Kontroll-ID	AWS Config	Empfehlungen
1650	cloudtrail-security-trail-enabled	Diese Regel trägt dazu bei, die Verwendung der AWS empfohlenen bewährten Sicherheitsmethoden für sicherzustellen AWS CloudTrail, indem geprüft wird, ob mehrere Einstellungen aktiviert sind. Dazu gehören die Verwendung von Protokoll verschlüsselung, Protokoll validierung und Aktivierung AWS CloudTrail in mehreren Regionen.
1650	elasticsearch-logs-to-cloud watch	Stellen Sie sicher, dass für Amazon OpenSearch Service-Domains Fehlerprotokolle aktiviert und zur Aufbewahr ung und Beantwortung an Amazon CloudWatch Logs gestreamt werden. Domain-Fehlerprotokolle sind bei Sicherheits- und Zugriffsp rüfungen sowie bei der Diagnose von Verfügbar keitsproblemen nützlich.

Kontroll-ID	AWS Config	Empfehlungen
1650	api-gw-execution-logging-aktiviert	Die API-Gateway-Protokollierung zeigt detaillierte Ansichten der Benutzer, die auf die API zugegriffen haben, und wie diese Benutzer auf die API zugegriffen haben. Diese Einblicke ermöglichen die Transparenz von Benutzeraktivitäten.
1650	cloudtrail-s3-dataevents-enabled	Die Erfassung von Simple Storage Service (Amazon S3)-Datenereignissen unterstützt die Erkennung von ungewöhnlichen Aktivitäten. Zu den Details gehören Informationen zu dem AWS -Konto, das auf einen Amazon-S3-Bucket zugegriffen hat, die IP-Adresse und die Uhrzeit des Ereignisses.
1650	rds-logging-enabled	Um die Protokollierung und Überwachung in Ihrer Umgebung zu erleichtern, stellen Sie sicher, dass die Amazon Relational Database Service (Amazon RDS)-Protokollierung aktiviert ist. Mit der Amazon-RDS-Protokollierung können Sie Ereignisse wie Verbindungen, Verbindungsabbrüche, Abfragen oder abgefragte Tabellen erfassen.

Kontroll-ID	AWS Config	Empfehlungen
1650	redshift-cluster-configuration-check	Um Daten im Ruhezustand zu schützen, muss die Verschlüsselung für Ihre Amazon-Redshift-Cluster aktiviert sein. Sie müssen auch sicherstellen, dass die erforderlichen Konfigurationen auf Amazon-Redshift-Clustern bereitgestellt werden. Die Prüfungsprotokollierung muss aktiviert sein, um Informationen zu Verbindungen und Benutzeraktivitäten in der Datenbank bereitzustellen. Diese Regel erfordert, dass ein Wert für clusterDbEncrypted (Config Default: TRUE) und LoggingEnabled (Config Default: TRUE) gesetzt ist. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	AWS Config	Empfehlungen
1650	s-3 bucket-logging-enabled	Die Amazon Simple Storage Service (Amazon S3)-Serverzugriffsprotokollierung bietet eine Methode zur Überwachung des Netzwerks im Hinblick auf potenzielle Cybersicherheitsereignisse. Die Ereignisse werden überwacht, indem detaillierte Aufzeichnungen über die Anfragen erfasst werden, die an einen Amazon-S3-Bucket gestellt wurden. Jeder Zugriffsprotokolleintrag enthält Details zu einer einzelnen Zugriffsanfrage. Zu den Details gehören Auftraggeber, Bucket-Name, Anforderungszeit, Anforderungsaktion, Antwortstatus und Fehlercode, falls relevant.

Kontroll-ID	AWS Config	Empfehlungen
1650	vpc-flow-logs-enabled	VPC-Flow-Protokolle erfassen detaillierte Informationsdatensätze über den IP-Datenverkehr, der zu und von Netzwerkschnittstellen in Ihrer Amazon Virtual Private Cloud (Amazon VPC) fließt. Standardmäßig enthalten Flow-Protokolldatensätze Werte für die verschiedenen Komponenten des IP-Flows, einschließlich Quelle, Ziel und Protokoll.
1650	wafv2-logging-enabled	Um die Protokollierung und Überwachung in Ihrer Umgebung zu erleichtern, aktivieren Sie die AWS WAF (V2) -Protokollierung im regionalen und globalen Web. ACLs AWS Die WAF-Protokollierung bietet detaillierte Informationen über den Datenverkehr, der von Ihrer Web-ACL analysiert wird. In den Protokollen werden die Uhrzeit aufgezeichnet, zu der die AWS WAF die Anfrage von Ihrer AWS Ressource erhalten hat, Informationen über die Anfrage und eine Aktion für die Regel, der jede Anfrage entsprach.

Kontroll-ID	AWS Config	Empfehlungen
1650	elb-logging-enabled	Die Elastic-Load-Balancing-Aktivität ist ein zentraler Kommunikationspunkt innerhalb einer Umgebung. Stellen Sie sicher, dass die ELB-Protokollierung aktiviert ist. Die gesammelten Daten enthalten detaillierte Informationen zu Anfragen, die an den ELB gesendet wurden. Jedes Protokoll enthält Informationen wie die Zeit, zu der die Anforderung einging, die Client-IP-Adresse, Latenzen, Anforderungspfade und Serverantworten.
1650	codebuild-project-logging-enabled	Stellen Sie sicher, dass die AWS CodeBuild Projektprotokollierung aktiviert ist, damit Ihre Build-Ausgabeprotokolle entweder an Amazon CloudWatch oder Amazon Simple Storage Service (Amazon S3) gesendet werden. Build-Ausgabeprotokolle enthalten detaillierte Informationen zu Ihrem Build-Projekt.

Kontroll-ID	AWS Config	Empfehlungen
1650	redshift-audit-logging-enabled	Aktivieren Sie die Prüfungsprotokollierung, um Informationen über Verbindungen und Benutzeraktivitäten in Ihrem Amazon-Redshift-Cluster zu erfassen.
1650	opensearch-audit-logging-enabled	Stellen Sie sicher, dass die Audit-Protokollierung für Ihre Amazon OpenSearch Service-Domains aktiviert ist. Mit der Audit-Protokollierung können Sie Benutzeraktivitäten auf Ihren OpenSearch Domains verfolgen, einschließlich erfolgreicher und fehlgeschlagener Authentifizierungen OpenSearch, Anfragen an, Indexänderungen und eingehende Suchanfragen.
1650	opensearch-logs-to-cloudwatch	Stellen Sie sicher, dass für Amazon OpenSearch Service-Domains Fehlerprotokolle aktiviert und zur Aufbewahrung und Beantwortung an Amazon CloudWatch Logs gestreamt werden. OpenSearch Service-Fehlerprotokolle können bei Sicherheits- und Zugriffsprüfungen helfen und bei der Diagnose von Verfügbarkeitsproblemen helfen.

Kontroll-ID	AWS Config	Empfehlungen
1657	alb-waf-enabled	Stellen Sie sicher, dass AWS WAF auf Elastic Load Balancers (ELB) aktiviert ist, um Webanwendungen zu schützen. Eine WAF trägt zum Schutz Ihrer Webanwendungen oder APIs vor gängigen Web-Exploits bei. Diese Web-Exploits können sich auf die Verfügbarkeit auswirken, die Sicherheit gefährden oder übermäßige Ressourcen in Ihrer Umgebung verbrauchen.
1657	api-gw-associated-with-WAF	AWS Mit WAF können Sie eine Reihe von Regeln (als Web Access Control List (Web ACL) bezeichnet) konfigurieren, die Webanfragen auf der Grundlage von anpassbaren Websicherheitsregeln und -bedingungen, die Sie definieren, zulassen, blockieren oder zählen. Stellen Sie sicher, dass Ihre Amazon-API-Gateway-Stufe mit einer WAF-Web-ACL verknüpft ist, um sie vor böswilligen Angriffen zu schützen.

Kontroll-ID	AWS Config	Empfehlungen
1657	ec2-manager instance-managed-by-systems	Eine Bestandsaufnahme der Softwareplattformen und Anwendungen innerhalb des Unternehmens ist möglich, indem Amazon Elastic Compute Cloud (Amazon EC2) -Instances mit AWS Systems Manager verwaltet werden. Verwenden Sie AWS Systems Manager, um detaillierte Systemkonfigurationen, Betriebssystem-Patch-Levels, Namen und Typ der Dienste, Softwareinstallationen, Anwendungsname, Herausgeber und Version sowie andere Details zu Ihrer Umgebung bereitzustellen.
1657	waf-regional-rule-not-leer	Stellen Sie sicher, dass Ihre AWS WAF eine Regel hat, die nicht leer ist. Eine Regel ohne Bedingungen kann zu unbeabsichtigtem Verhalten führen.
1657	waf-regional-rulegroup-not-leer	Stellen Sie sicher, dass Ihre AWS WAF eine Regelgruppe hat, die nicht leer ist. Eine leere Regelgruppe kann zu unbeabsichtigtem Verhalten führen.

Kontroll-ID	AWS Config	Empfehlungen
1657	waf-regional-webacl-not-leer	Eine an eine AWS WAF angehängte Web-ACL kann eine Sammlung von Regeln und Regelgruppen zur Überprüfung und Steuerung von Webanfragen enthalten . Wenn eine Web-ACL leer ist, wird der Webdatenverkehr weitergeleitet, ohne von der WAF erkannt oder bearbeitet zu werden.
1657	ec2-prüfen managedinstance-association-compliance-status	Verwenden Sie AWS Systems Manager Associations, um bei der Inventarisierung von Softwareplattformen und Anwendungen innerhalb eines Unternehmens zu helfen. AWS Systems Manager weist Ihren verwalteten Instances einen Konfigurationsstatus zu und ermöglicht es Ihnen, Basiswerte für Betriebss ystem-Patch-Levels, Softwarei nstallationen, Anwendung skonfigurationen und andere Details zu Ihrer Umgebung festzulegen.

Kontroll-ID	AWS Config	Empfehlungen
1661	cloud-trail-cloud-watch-logs-aktiviert	Verwenden Sie Amazon CloudWatch , um Protokoll ereignisaktivitäten zentral zu sammeln und zu verwalten . Die Aufnahme von AWS CloudTrail Daten liefert Einzelheiten zu den API-Aufru faktivitäten in Ihrem AWS-Konto.
1661	cloudtrail-enabled	AWS CloudTrail kann durch die Aufzeichnung von Aktionen und API-Aufrufen in der AWS Management Console bei der Nichtabst reitbarkeit helfen. Sie können die Benutzer und die Benutzer AWS-Konten , die einen AWS Dienst aufgerufen haben, die Quell-IP-Adresse, über die die Aufrufe generiert wurden, und den Zeitpunkt der Anrufe identifizieren. Einzelheiten zu den erfassten Daten finden Sie in den AWS CloudTrail Datensatzinhalten.

Kontroll-ID	AWS Config	Empfehlungen
1661	multi-region-cloudtrail-enabled	AWS CloudTrail zeichnet Aktionen und API-Aufrufe der AWS Management Console auf. Sie können feststellen, welche Benutzer und Konten angerufen wurden AWS, von welcher Quell-IP-Adresse aus die Anrufe getätigt wurden und wann die Anrufe erfolgten . CloudTrail übermittelt Protokolldateien aus allen AWS Regionen an Ihren S3-Bucket, wenn MULTI_REG ION_CLOUD_TRAIL_EN ABLED aktiviert ist. Außerdem wird beim AWS Start einer neuen Region derselbe Trail in der neuen Region erstellt. CloudTrail Dadurch erhalten Sie automatisch Protokoll dateien mit API-Aktivitäten für die neue Region.

Kontroll-ID	AWS Config	Empfehlungen
1661	cloudtrail-security-trail-enabled	Diese Regel trägt dazu bei, die Verwendung der AWS empfohlenen bewährten Sicherheitsmethoden für sicherzustellen AWS CloudTrail, indem geprüft wird, ob mehrere Einstellungen aktiviert sind. Dazu gehören die Verwendung von Protokoll verschlüsselung, Protokoll validierung und Aktivierung AWS CloudTrail in mehreren Regionen.
1661	elasticsearch-logs-to-cloud watch	Stellen Sie sicher, dass für Amazon OpenSearch Service-Domains Fehlerprotokolle aktiviert und zur Aufbewahr ung und Beantwortung an Amazon CloudWatch Logs gestreamt werden. Domain-Fehlerprotokolle sind bei Sicherheits- und Zugriffsp rüfungen sowie bei der Diagnose von Verfügbar keitsproblemen nützlich.

Kontroll-ID	AWS Config	Empfehlungen
1661	api-gw-execution-logging-aktiviert	Die API-Gateway-Protokollierung zeigt detaillierte Ansichten der Benutzer, die auf die API zugegriffen haben, und wie diese Benutzer auf die API zugegriffen haben. Diese Einblicke ermöglichen die Transparenz von Benutzeraktivitäten.
161	cloudtrail-s3-dataevents-enabled	Die Erfassung von Simple Storage Service (Amazon S3)-Datenereignissen unterstützt die Erkennung von ungewöhnlichen Aktivitäten. Zu den Details gehören Informationen zu dem AWS -Konto, das auf einen Amazon-S3-Bucket zugegriffen hat, die IP-Adresse und die Uhrzeit des Ereignisses.
1661	rds-logging-enabled	Um die Protokollierung und Überwachung in Ihrer Umgebung zu erleichtern, stellen Sie sicher, dass die Amazon Relational Database Service (Amazon RDS)-Protokollierung aktiviert ist. Mit der Amazon-RDS-Protokollierung können Sie Ereignisse wie Verbindungen, Verbindungsabbrüche, Abfragen oder abgefragte Tabellen erfassen.

Kontroll-ID	AWS Config	Empfehlungen
1661	redshift-cluster-configuration-check	Um Daten im Ruhezustand zu schützen, muss die Verschlüsselung für Ihre Amazon-Redshift-Cluster aktiviert sein. Sie müssen auch sicherstellen, dass die erforderlichen Konfigurationen auf Amazon-Redshift-Clustern bereitgestellt werden. Die Prüfungsprotokollierung muss aktiviert sein, um Informationen zu Verbindungen und Benutzeraktivitäten in der Datenbank bereitzustellen. Diese Regel erfordert, dass ein Wert für clusterDbEncrypted (Config Default: TRUE) und LoggingEnabled (Config Default: TRUE) gesetzt ist. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	AWS Config	Empfehlungen
1661	s-3 bucket-logging-enabled	Die Amazon Simple Storage Service (Amazon S3)-Serverzugriffsprotokollierung bietet eine Methode zur Überwachung des Netzwerks im Hinblick auf potenzielle Cybersicherheitsereignisse. Die Ereignisse werden überwacht, indem detaillierte Aufzeichnungen über die Anfragen erfasst werden, die an einen Amazon-S3-Bucket gestellt wurden. Jeder Zugriffsprotokolleintrag enthält Details zu einer einzelnen Zugriffsanfrage. Zu den Details gehören Auftraggeber, Bucket-Name, Anforderungszeit, Anforderungsaktion, Antwortstatus und Fehlercode, falls relevant.

Kontroll-ID	AWS Config	Empfehlungen
161	vpc-flow-logs-enabled	VPC-Flow-Protokolle erfassen detaillierte Informationsdatensätze über den IP-Datenverkehr, der zu und von Netzwerkschnittstellen in Ihrer Amazon Virtual Private Cloud (Amazon VPC) fließt. Standardmäßig enthalten Flow-Protokolldatensätze Werte für die verschiedenen Komponenten des IP-Flows, einschließlich Quelle, Ziel und Protokoll.
1661	wafv2-logging-enabled	Um die Protokollierung und Überwachung in Ihrer Umgebung zu erleichtern, aktivieren Sie die AWS WAF (V2) -Protokollierung im regionalen und globalen Web. ACLs AWS Die WAF-Protokollierung bietet detaillierte Informationen über den Datenverkehr, der von Ihrer Web-ACL analysiert wird. In den Protokollen werden die Uhrzeit aufgezeichnet, zu der die AWS WAF die Anfrage von Ihrer AWS Ressource erhalten hat, Informationen über die Anfrage und eine Aktion für die Regel, der jede Anfrage entsprach.

Kontroll-ID	AWS Config	Empfehlungen
1661	elb-logging-enabled	Die Elastic-Load-Balancing-Aktivität ist ein zentraler Kommunikationspunkt innerhalb einer Umgebung. Stellen Sie sicher, dass die ELB-Protokollierung aktiviert ist. Die gesammelten Daten enthalten detaillierte Informationen zu Anfragen, die an den ELB gesendet wurden. Jedes Protokoll enthält Informationen wie die Zeit, zu der die Anforderung einging, die Client-IP-Adresse, Latenzen, Anforderungspfade und Serverantworten.
1661	opensearch-logs-to-cloudwatch	Stellen Sie sicher, dass für Amazon OpenSearch Service-Domains Fehlerprotokolle aktiviert und zur Aufbewahrung und Beantwortung an Amazon CloudWatch Logs gestreamt werden. OpenSearch Service-Fehlerprotokolle können bei Sicherheits- und Zugriffsprüfungen helfen und bei der Diagnose von Verfügbarkeitsproblemen helfen.

Kontroll-ID	AWS Config	Empfehlungen
1679	iam-root-access-key-überprüfen	Der Zugriff auf Systeme und Ressourcen kann gesteuert werden, indem überprüft wird, ob der Root-Benutzer keine Zugriffsschlüssel mit seiner AWS Identity and Access Management (IAM) -Rolle verknüpft hat. Stellen Sie sicher, dass die Root-Zugriffsschlüssel gelöscht werden. Erstellen und verwenden Sie stattdessen rollenbasierte Funktionen, AWS-Konten um das Prinzip der geringsten Funktionalität zu berücksichtigen.
1679	iam-user-mfa-enabled	Aktivieren Sie diese Regel, um den Zugriff auf Ressourcen in der AWS -Cloud einzuschränken. Diese Regel stellt sicher, dass die Multi-Faktor-Authentifizierung (MFA) für alle Benutzer aktiviert ist. MFA bietet eine weitere Schutzebene zusätzlich zum Benutzernamen und Passwort. Reduzieren Sie Fälle von kompromittierten Konten, indem Sie MFA für Benutzer vorschreiben.

Kontroll-ID	AWS Config	Empfehlungen
1679	mfa-enabled-for-iam-Konsolenzugriff	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass MFA für alle AWS Identity and Access Management (IAM) -Benutzer aktiviert ist, die über ein Konsolenkennwort verfügen. MFA sorgt für eine weitere Schutzebene zusätzlich zu den Anmeldeinformationen. Indem Sie MFA für Benutzer vorschreiben, können Sie Fälle kompromittierter Konten reduzieren und verhindern, dass unbefugte Benutzer auf vertrauliche Daten zugreifen.
1679	root-account-hardware-mfa-aktiviert	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Hardware-MFA für den Root-Benutzer aktiviert ist. Der Stammbenutzer ist der AWS-Konto-Benutzer mit den meisten Berechtigungen. MFA sorgt für eine weitere Schutzebene zusätzlich zu den Anmeldeinformationen. Indem Sie MFA für den Root-Benutzer vorschreiben, können Sie die Anzahl AWS-Konten kompromittierter Benutzer reduzieren.

Kontroll-ID	AWS Config	Empfehlungen
1679	root-account-mfa-enabled	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass MFA für den Root-Benutzer aktiviert ist. Der Stammbenutzer ist der AWS-Konto-Benutzer mit den meisten Berechtigungen. MFA bietet eine weitere Schutzebene zusätzlich zum Benutzernamen und Passwort. Indem Sie MFA für den Root-Benutzer vorschreiben, können Sie die Anzahl AWS-Konten kompromittierter Benutzer reduzieren.
1680	iam-root-access-key-überprüfen	Der Zugriff auf Systeme und Ressourcen kann gesteuert werden, indem überprüft wird, ob der Root-Benutzer keine Zugriffsschlüssel mit seiner AWS Identity and Access Management (IAM) -Rolle verknüpft hat. Stellen Sie sicher, dass die Root-Zugriffsschlüssel gelöscht werden. Erstellen und verwenden Sie stattdessen rollenbasierte Funktionen, AWS-Konten um das Prinzip der geringsten Funktionalität zu berücksichtigen.

Kontroll-ID	AWS Config	Empfehlungen
1680	iam-user-mfa-enabled	Aktivieren Sie diese Regel, um den Zugriff auf Ressourcen in der AWS -Cloud einzuschränken. Diese Regel stellt sicher, dass die Multi-Faktor-Authentifizierung (MFA) für alle Benutzer aktiviert ist. MFA bietet eine weitere Schutzebene zusätzlich zum Benutzernamen und Passwort. Reduzieren Sie Fälle von kompromittierten Konten, indem Sie MFA für Benutzer vorschreiben.
1680	mfa-enabled-for-iam-Konsolenzugriff	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass MFA für alle AWS Identity and Access Management (IAM) -Benutzer aktiviert ist, die über ein Konsolenkennwort verfügen. MFA sorgt für eine weitere Schutzebene zusätzlich zu den Anmeldeinformationen. Indem Sie MFA für Benutzer vorschreiben, können Sie Fälle kompromittierter Konten reduzieren und verhindern, dass unbefugte Benutzer auf vertrauliche Daten zugreifen.

Kontroll-ID	AWS Config	Empfehlungen
1680	root-account-hardware-mfa-aktiviert	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Hardware-MFA für den Root-Benutzer aktiviert ist. Der Stammbenutzer ist der AWS-Konto-Benutzer mit den meisten Berechtigungen. MFA sorgt für eine weitere Schutzebene zusätzlich zu den Anmeldeinformationen. Indem Sie MFA für den Root-Benutzer vorschreiben, können Sie die Anzahl AWS-Konten kompromittierter Benutzer reduzieren.
1680	root-account-mfa-enabled	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass MFA für den Root-Benutzer aktiviert ist. Der Stammbenutzer ist der AWS-Konto-Benutzer mit den meisten Berechtigungen. MFA bietet eine weitere Schutzebene zusätzlich zum Benutzernamen und Passwort. Indem Sie MFA für den Root-Benutzer vorschreiben, können Sie die Anzahl AWS-Konten kompromittierter Benutzer reduzieren.

Kontroll-ID	AWS Config	Empfehlungen
1681	iam-root-access-key-überprüfen	Der Zugriff auf Systeme und Ressourcen kann gesteuert werden, indem überprüft wird, ob der Root-Benutzer keine Zugriffsschlüssel mit seiner AWS Identity and Access Management (IAM) -Rolle verknüpft hat. Stellen Sie sicher, dass die Root-Zugriffsschlüssel gelöscht werden. Erstellen und verwenden Sie stattdessen rollenbasierte Funktionen, AWS-Konten um das Prinzip der geringsten Funktionalität zu berücksichtigen.
1681	iam-user-mfa-enabled	Aktivieren Sie diese Regel, um den Zugriff auf Ressourcen in der AWS -Cloud einzuschränken. Diese Regel stellt sicher, dass die Multi-Faktor-Authentifizierung (MFA) für alle Benutzer aktiviert ist. MFA bietet eine weitere Schutzebene zusätzlich zum Benutzernamen und Passwort. Reduzieren Sie Fälle von kompromittierten Konten, indem Sie MFA für Benutzer vorschreiben.

Kontroll-ID	AWS Config	Empfehlungen
1681	mfa-enabled-for-iam-Konsolenzugriff	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass MFA für alle AWS Identity and Access Management (IAM) -Benutzer aktiviert ist, die über ein Konsolenkennwort verfügen. MFA sorgt für eine weitere Schutzebene zusätzlich zu den Anmeldeinformationen. Indem Sie MFA für Benutzer vorschreiben, können Sie Fälle kompromittierter Konten reduzieren und verhindern, dass unbefugte Benutzer auf vertrauliche Daten zugreifen.
1681	root-account-hardware-mfa-aktiviert	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Hardware-MFA für den Root-Benutzer aktiviert ist. Der Stammbenutzer ist der AWS-Konto-Benutzer mit den meisten Berechtigungen. MFA sorgt für eine weitere Schutzebene zusätzlich zu den Anmeldeinformationen. Indem Sie MFA für den Root-Benutzer vorschreiben, können Sie die Anzahl AWS-Konten kompromittierter Benutzer reduzieren.

Kontroll-ID	AWS Config	Empfehlungen
1681	root-account-mfa-enabled	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass MFA für den Root-Benutzer aktiviert ist. Der Stammbenutzer ist der AWS-Konto-Benutzer mit den meisten Berechtigungen. MFA bietet eine weitere Schutzebene zusätzlich zum Benutzernamen und Passwort. Indem Sie MFA für den Root-Benutzer vorschreiben, können Sie die Anzahl AWS-Konten kompromittierter Benutzer reduzieren.
1683	cloudtrail-enabled	AWS CloudTrail kann durch die Aufzeichnung von Aktionen und API-Aufrufen in der AWS Management Console bei der Nichtabstreitbarkeit helfen. Sie können die Benutzer und die Benutzer AWS-Konten , die einen AWS Dienst aufgerufen haben, die Quell-IP-Adresse, über die die Aufrufe generiert wurden, und den Zeitpunkt der Anrufe identifizieren. Einzelheiten zu den erfassten Daten finden Sie in den AWS CloudTrail Datensatzinhalten.

Kontroll-ID	AWS Config	Empfehlungen
1683	s-3 bucket-logging-enabled	Die Amazon Simple Storage Service (Amazon S3)-Serverzugriffsprotokollierung bietet eine Methode zur Überwachung des Netzwerks im Hinblick auf potenzielle Cybersicherheitsereignisse. Die Ereignisse werden überwacht, indem detaillierte Aufzeichnungen über die Anfragen erfasst werden, die an einen Amazon-S3-Bucket gestellt wurden. Jeder Zugriffsprotokolleintrag enthält Details zu einer einzelnen Zugriffsanfrage. Zu den Details gehören Auftraggeber, Bucket-Name, Anforderungszeit, Anforderungsaktion, Antwortstatus und Fehlercode, falls relevant.

Kontroll-ID	AWS Config	Empfehlungen
1690	ec2-imdsv2-check	Stellen Sie sicher, dass die Methode Instance Metadata Service Version 2 (IMDSv2) aktiviert ist, um den Zugriff auf und die Kontrolle der Amazon Elastic Compute Cloud (Amazon EC2) -Instance-Metadaten zu schützen. Die IMDSv2 Methode verwendet sitzungsbasierte Kontrolle n. Mit können Kontrollen implementiert werden IMDSv2, um Änderungen an Instanzme tadaten einzuschränken.
1690	ec2-manager instance-managed-by-systems	Eine Bestandsaufnahme der Softwareplattformen und Anwendungen innerhalb des Unternehmens ist möglich, indem Amazon Elastic Compute Cloud (Amazon EC2) -Instances mit AWS Systems Manager verwaltet werden. Verwenden Sie AWS Systems Manager, um detaillierte Systemkonfiguratio nen, Betriebssystem-Patch-Levels, Namen und Typ der Dienste, Softwareinstallati onen, Anwendungsname, Herausgeber und Version sowie andere Details zu Ihrer Umgebung bereitzustellen.

Kontroll-ID	AWS Config	Empfehlungen
1690	ecs-fargate-latest-platform-Ausführung	Sicherheitsupdates und Patches werden automatis ch für Ihre AWS Fargate-Aufgaben bereitgestellt. Wenn ein Sicherheitsproblem gefunden wird, das eine AWS Fargate-Plattformversion betrifft, AWS wird die Plattform version gepatcht. Um Sie bei der Patchverwaltung Ihrer Amazon Elastic Container Service (ECS) -Aufgaben zu unterstützen, auf denen AWS Fargate ausgeführt wird, aktualisieren Sie Ihre eigenständigen Service-Aufgaben, sodass sie die neueste Plattformversion verwenden.
1690	elastic-beanstalk-managed-updates-aktiviert	Durch die Aktivierung verwalteter Plattformupdates für eine Amazon-Elastic-Beanstalk-Umgebung wird sichergestellt, dass die aktuellen verfügbaren Plattform-Fixes, -Updates und -Features für die Umgebung installiert sind. Eine bewährte Methode zur Sicherung von Systemen besteht darin, stets die aktuellen Patches zu installieren.

Kontroll-ID	AWS Config	Empfehlungen
1690	rds-automatic-minor-version-Upgrade-fähig	Aktivieren Sie automatische Unterversions-Upgrades auf Ihren Amazon-Relational-Database-Service (RDS)-Instances, um sicherzustellen, dass die aktuellen Updates für Unterversionen des Relational Database Management System (RDBMS) installiert sind, die Sicherheitspatches und Bugfixes enthalten können.
1690	ec2-prüfen managedinstance-association-compliance-status	Verwenden Sie AWS Systems Manager Associations, um bei der Inventarisierung von Softwareplattformen und Anwendungen innerhalb eines Unternehmens zu helfen. AWS Systems Manager weist Ihren verwalteten Instances einen Konfigurationsstatus zu und ermöglicht es Ihnen, Basiswerte für Betriebssystem-Patch-Levels, Softwareinstallationen, Anwendungskonfigurationen und andere Details zu Ihrer Umgebung festzulegen.

Kontroll-ID	AWS Config	Empfehlungen
1690	redshift-cluster-maintenancesettings-check	Diese Regel stellt sicher, dass Amazon-Redshift-Cluster die bevorzugten Einstellungen für Ihre Organisation haben. Insbesondere sorgt sie dafür, dass Cluster bevorzugte Wartungsfenster und automatisierte Aufbewahrungsfristen für Snapshots für die Datenbank haben. Für diese Regel müssen Sie die allowVersionUpgrade festlegen. Der Standardwert ist „true“. Außerdem können Sie optional den Zeitraum preferredMaintenanceWindow (der Standardwert ist sa: 16:00 -sa: 16:30) und den automatedSnapshotRetention Zeitraum (der Standardwert ist 1) festlegen. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	AWS Config	Empfehlungen
1691	ec2-imdsv2-check	Stellen Sie sicher, dass die Methode Instance Metadata Service Version 2 (IMDSv2) aktiviert ist, um den Zugriff auf und die Kontrolle der Amazon Elastic Compute Cloud (Amazon EC2) -Instance-Metadaten zu schützen. Die IMDSv2 Methode verwendet sitzungsbasierte Kontrolle n. Mit können Kontrollen implementiert werden IMDSv2, um Änderungen an Instanzme tadaten einzuschränken.
1691	ec2-manager instance-managed-by-systems	Eine Bestandsaufnahme der Softwareplattformen und Anwendungen innerhalb des Unternehmens ist möglich, indem Amazon Elastic Compute Cloud (Amazon EC2) -Instances mit AWS Systems Manager verwaltet werden. Verwenden Sie AWS Systems Manager, um detaillierte Systemkonfiguratio nen, Betriebssystem-Patch-Levels, Namen und Typ der Dienste, Softwareinstallati onen, Anwendungsname, Herausgeber und Version sowie andere Details zu Ihrer Umgebung bereitzustellen.

Kontroll-ID	AWS Config	Empfehlungen
1691	ecs-fargate-latest-platform-Ausführung	Sicherheitsupdates und Patches werden automatis ch für Ihre AWS Fargate-Aufgaben bereitgestellt. Wenn ein Sicherheitsproblem gefunden wird, das eine AWS Fargate-Plattformversion betrifft, AWS wird die Plattform version gepatcht. Um Sie bei der Patchverwaltung Ihrer Amazon Elastic Container Service (ECS) -Aufgaben zu unterstützen, auf denen AWS Fargate ausgeführt wird, aktualisieren Sie Ihre eigenständigen Service-Aufgaben, sodass sie die neueste Plattformversion verwenden.
1691	elastic-beanstalk-managed-updates-aktiviert	Durch die Aktivierung verwalteter Plattformupdates für eine Amazon-Elastic-Beanstalk-Umgebung wird sichergestellt, dass die aktuellen verfügbaren Plattform-Fixes, -Updates und -Features für die Umgebung installiert sind. Eine bewährte Methode zur Sicherung von Systemen besteht darin, stets die aktuellen Patches zu installieren.

Kontroll-ID	AWS Config	Empfehlungen
1691	rds-automatic-minor-version-Upgrade aktiviert	Aktivieren Sie automatische Unterversions-Upgrades auf Ihren Amazon-Relational-Database-Service (RDS)-Instances, um sicherzustellen, dass die aktuellen Updates für Unterversionen des Relational Database Management System (RDBMS) installiert sind, die Sicherheitspatches und Bugfixes enthalten können.
1691	ec2-prüfen managedinstance-association-compliance-status	Verwenden Sie AWS Systems Manager Associations, um bei der Inventarisierung von Softwareplattformen und Anwendungen innerhalb eines Unternehmens zu helfen. AWS Systems Manager weist Ihren verwalteten Instances einen Konfigurationsstatus zu und ermöglicht es Ihnen, Basiswerte für Betriebssystem-Patch-Levels, Softwareinstallationen, Anwendungskonfigurationen und andere Details zu Ihrer Umgebung festzulegen.

Kontroll-ID	AWS Config	Empfehlungen
1691	redshift-cluster-maintenancesettings-check	Diese Regel stellt sicher, dass Amazon-Redshift-Cluster die bevorzugten Einstellungen für Ihre Organisation haben. Insbesondere sorgt sie dafür, dass Cluster bevorzugte Wartungsfenster und automatisierte Aufbewahrungsfristen für Snapshots für die Datenbank haben. Für diese Regel müssen Sie die allowVersionUpgrade festlegen. Der Standardwert ist „true“. Außerdem können Sie optional den Zeitraum preferredMaintenanceWindow (der Standardwert ist sa: 16:00 -sa: 16:30) und den automatedSnapshotRetention Zeitraum (der Standardwert ist 1) festlegen. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	AWS Config	Empfehlungen
1693	ec2-imdsv2-check	Stellen Sie sicher, dass die Methode Instance Metadata Service Version 2 (IMDSv2) aktiviert ist, um den Zugriff auf und die Kontrolle der Amazon Elastic Compute Cloud (Amazon EC2) -Instance-Metadaten zu schützen. Die IMDSv2 Methode verwendet sitzungsbasierte Kontrolle n. Mit können Kontrollen implementiert werden IMDSv2, um Änderungen an Instanzme tadaten einzuschränken.
1693	ec2-manager instance-managed-by-systems	Eine Bestandsaufnahme der Softwareplattformen und Anwendungen innerhalb des Unternehmens ist möglich, indem Amazon Elastic Compute Cloud (Amazon EC2) -Instances mit AWS Systems Manager verwaltet werden. Verwenden Sie AWS Systems Manager, um detaillierte Systemkonfiguratio nen, Betriebssystem-Patch-Levels, Namen und Typ der Dienste, Softwareinstallati onen, Anwendungsname, Herausgeber und Version sowie andere Details zu Ihrer Umgebung bereitzustellen.

Kontroll-ID	AWS Config	Empfehlungen
1693	ecs-fargate-latest-platform-Ausführung	Sicherheitsupdates und Patches werden automatis ch für Ihre AWS Fargate-Aufgaben bereitgestellt. Wenn ein Sicherheitsproblem gefunden wird, das eine AWS Fargate-Plattformversion betrifft, AWS wird die Plattform version gepatcht. Um Sie bei der Patchverwaltung Ihrer Amazon Elastic Container Service (ECS) -Aufgaben zu unterstützen, auf denen AWS Fargate ausgeführt wird, aktualisieren Sie Ihre eigenständigen Service-Aufgaben, sodass sie die neueste Plattformversion verwenden.
1693	elastic-beanstalk-managed-updates-aktiviert	Durch die Aktivierung verwalteter Plattformupdates für eine Amazon-Elastic-Beanstalk-Umgebung wird sichergestellt, dass die aktuellen verfügbaren Plattform-Fixes, -Updates und -Features für die Umgebung installiert sind. Eine bewährte Methode zur Sicherung von Systemen besteht darin, stets die aktuellen Patches zu installieren.

Kontroll-ID	AWS Config	Empfehlungen
1693	rds-automatic-minor-version-Upgrade aktiviert	Aktivieren Sie automatische Unterversions-Upgrades auf Ihren Amazon-Relational-Database-Service (RDS)-Instances, um sicherzustellen, dass die aktuellen Updates für Unterversionen des Relational Database Management System (RDBMS) installiert sind, die Sicherheitspatches und Bugfixes enthalten können.
1693	ec2-prüfen managedinstance-association-compliance-status	Verwenden Sie AWS Systems Manager Associations, um bei der Inventarisierung von Softwareplattformen und Anwendungen innerhalb eines Unternehmens zu helfen. AWS Systems Manager weist Ihren verwalteten Instances einen Konfigurationsstatus zu und ermöglicht es Ihnen, Basiswerte für Betriebssystem-Patch-Levels, Softwareinstallationen, Anwendungskonfigurationen und andere Details zu Ihrer Umgebung festzulegen.

Kontroll-ID	AWS Config	Empfehlungen
1693	redshift-cluster-maintenancesettings-check	Diese Regel stellt sicher, dass Amazon-Redshift-Cluster die bevorzugten Einstellungen für Ihre Organisation haben. Insbesondere sorgt sie dafür, dass Cluster bevorzugte Wartungsfenster und automatisierte Aufbewahrungsfristen für Snapshots für die Datenbank haben. Für diese Regel müssen Sie die allowVersionUpgrade festlegen. Der Standardwert ist „true“. Außerdem können Sie optional den Zeitraum preferredMaintenanceWindow (der Standardwert ist sa: 16:00 -sa: 16:30) und den automatedSnapshotRetention Zeitraum (der Standardwert ist 1) festlegen. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	AWS Config	Empfehlungen
1694	ec2-prüfen managedinstance-patch-compliance-status	Aktivieren Sie diese Regel, um bei der Identifizierung und Dokumentation von Sicherheitslücken in Amazon Elastic Compute Cloud (Amazon EC2) zu helfen. Die Regel prüft, ob die EC2 Amazon-Instance die Patch-Konformität im AWS Systems Manager gemäß den Richtlinien und Verfahren Ihrer Organisation einhält.
1695	ec2-prüfen managedinstance-patch-compliance-status	Aktivieren Sie diese Regel, um bei der Identifizierung und Dokumentation von Sicherheitslücken in Amazon Elastic Compute Cloud (Amazon EC2) zu helfen. Die Regel prüft, ob die EC2 Amazon-Instance die Patch-Konformität im AWS Systems Manager gemäß den Richtlinien und Verfahren Ihrer Organisation einhält.

Kontroll-ID	AWS Config	Empfehlungen
1707	backup-recovery-point-manual-Löschen-deaktiviert	Stellen Sie sicher, dass Ihren AWS Backup-Wiederherstellungspunkten eine ressourcenbasierte Richtlinie zugeordnet ist, die das Löschen von Wiederherstellungspunkten verhindert. Die Verwendung einer ressourcenbasierten Richtlinie zur Verhinderung des Löschens von Wiederherstellungspunkten kann dazu beitragen, ein versehentliches oder absichtliches Löschen zu unterbinden.
P1	rds-cluster-deletion-protection-aktiviert	Stellen Sie sicher, dass Amazon Relational Database Service (Amazon RDS)-Instances den Löschschutz aktiviert haben. Verwenden Sie den Löschschutz, um zu verhindern, dass Ihre Amazon-RDS-Instances versehentlich oder böswillig gelöscht werden, was zum Verlust der Verfügbarkeit Ihrer Anwendungen führen kann.

Kontroll-ID	AWS Config	Empfehlungen
P1	rds-instance-deletion-protection-aktiviert	Stellen Sie sicher, dass Amazon Relational Database Service (Amazon RDS)-Instances den Löschschutz aktiviert haben. Verwenden Sie den Löschschutz, um zu verhindern, dass Ihre Amazon-RDS-Instances versehentlich oder böswillig gelöscht werden, was zum Verlust der Verfügbarkeit Ihrer Anwendungen führen kann.
P3	ec2-imdsv2-check	Stellen Sie sicher, dass die Methode Instance Metadata Service Version 2 (IMDSv2) aktiviert ist, um den Zugriff auf und die Kontrolle der Amazon Elastic Compute Cloud (Amazon EC2) -Instance-Metadaten zu schützen. Die IMDSv2 Methode verwendet sitzungsbasierte Kontrolle n. Mit können Kontrollen implementiert werden IMDSv2, um Änderungen an Instanzme tadaten einzuschränken.

Kontroll-ID	AWS Config	Empfehlungen
P5	securityhub-enabled	AWS Security Hub hilft bei der Überwachung von unbefugte m Personal, Verbindungen, Geräten und Software. AWS Security Hub aggregiert, organisiert und priorisiert die Sicherheitswarnungen oder Ergebnisse mehrerer Dienste. AWS Einige dieser Dienste sind Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer und AWS Firewall Manager sowie AWS Partnerlösungen.
P7	elasticsearch-node-to-node-Verschlüsselungsprüfung	Stellen Sie sicher, dass die node-to-node Verschlüsselung für Amazon OpenSearch Service aktiviert ist. Node-to-nodeVerschlüsselung ermöglicht die TLS 1.2-Versc hlüsselung für die gesamte Kommunikation innerhalb der Amazon Virtual Private Cloud (Amazon VPC). Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	AWS Config	Empfehlungen
P7	s-3 bucket-ssl-requests-only	Um Daten während der Übertragung zu schützen, stellen Sie sicher, dass Ihre Amazon Simple Storage Service (Amazon S3)-Buckets Anfragen zur Verwendung von Secure Socket Layer (SSL)-Buckets erfordern. Da sensible Daten vorhanden sein können, sollten Sie die Verschlüs selung bei der Übertragung aktivieren, um diese Daten zu schützen.
P7	opensearch-node-to-node-Verschlüsselungsprüfung	Stellen Sie sicher, dass die node-to-node Verschlüsselung für Amazon OpenSearch Service aktiviert ist. Node-to-nodeVerschlüsselung ermöglicht die TLS 1.2-Versc hlüsselung für die gesamte Kommunikation innerhalb der Amazon Virtual Private Cloud (Amazon VPC). Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	AWS Config	Empfehlungen
P7	opensearch-https-required	Da sensible Daten existieren können und um Daten während der Übertragung zu schützen, sollten Sie sicherstellen, dass HTTPS für Verbindungen zu Ihren Amazon OpenSearch Service-Domains aktiviert ist.
P8	s3- bucket-logging-enabled	Die Amazon Simple Storage Service (Amazon S3)-Serverzugriffsprotokollierung bietet eine Methode zur Überwachung des Netzwerks im Hinblick auf potenzielle Cybersicherheitsereignisse. Die Ereignisse werden überwacht, indem detaillierte Aufzeichnungen über die Anfragen erfasst werden, die an einen Amazon-S3-Bucket gestellt wurden. Jeder Zugriffsprotokolleintrag enthält Details zu einer einzelnen Zugriffsanfrage. Zu den Details gehören Auftraggeber, Bucket-Name, Anforderungszeit, Anforderungsaktion, Antwortstatus und Fehlercode, falls relevant.

Kontroll-ID	AWS Config	Empfehlungen
P9	aurora-resources-protected-by-Backup-Plan	Um Sie bei Datensich erungsprozessen zu unterstüt zen, stellen Sie sicher, dass Ihre Amazon Aurora Aurora-Ressourcen Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherung smanagement und erleichte rt Ihnen die Erfüllung von geschäftlichen und behördlic hen Compliance-Anforde rungen hinsichtlich Datensich erungen.

Kontroll-ID	AWS Config	Empfehlungen
P9	backup-plan-min-frequency-and-min-retention-check	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihr AWS Backup-Plan auf eine Mindestfrequenz und Aufbewahrung festgelegt ist. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen. Mit dieser Regel können Sie die Parameter requiredFrequencyValue (Config default: 1), requiredRetentionDays (Config default: 35) und requiredFrequencyUnit (Config default: days) festlegen. Der tatsächliche Wert muss den Anforderungen Ihrer Organisation entsprechen.

Kontroll-ID	AWS Config	Empfehlungen
P9	backup-recovery-point-encrypted	Stellen Sie sicher, dass die Verschlüsselung für Ihre AWS Backup-Wiederherstellungspunkte aktiviert ist. Da sensible Daten auch im Ruhezustand vorhanden sein können, sollten Sie die Verschlüsselung im Ruhezustand aktivieren, um diese Daten zu schützen.
P9	backup-recovery-point-manual-Löschen-deaktiviert	Stellen Sie sicher, dass Ihren AWS Backup-Wiederherstellungspunkten eine ressourcenbasierte Richtlinie zugeordnet ist, die das Löschen von Wiederherstellungspunkten verhindert. Die Verwendung einer ressourcenbasierten Richtlinie zur Verhinderung des Löschens von Wiederherstellungspunkten kann dazu beitragen, ein versehentliches oder absichtliches Löschen zu unterbinden.

Kontroll-ID	AWS Config	Empfehlungen
P9	backup-recovery-point-minimum-Aufbewahrungsprüfung	Um bei Datensicherungsprozessen zu helfen, stellen Sie sicher, dass für Ihre AWS Backup-Wiederherstellungspunkte eine Mindestaufbewahrungsdauer festgelegt ist. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen. Mit dieser Regel können Sie den Parameter requiredRetentionDays (Config Default: 35) festlegen. Der tatsächliche Wert muss den Anforderungen Ihrer Organisation entsprechen.

Kontroll-ID	AWS Config	Empfehlungen
P9	db-instance-backup-enabled	Die Sicherungsfunktion von Amazon RDS erstellt Sicherungen Ihrer Datenbank en und Transaktionsprotokolle. Amazon RDS erstellt einen Snapshot für das Speicherv olume Ihrer DB-Instance, sodass die gesamte DB-Instance gesichert wird. Sie können im System spezifisc he Aufbewahrungsfristen festlegen, um Ihre Ausfallsi cherheitsanforderungen zu erfüllen.
P9	dynamodb-in-backup-plan	Um Sie bei Datensich erungsprozessen zu unterstüt zen, stellen Sie sicher, dass Ihre Amazon DynamoDB-Tabellen Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherung smanagement und erleichte rt Ihnen die Erfüllung von geschäftlichen und behördlic hen Compliance-Anforde rungen hinsichtlich Datensich erungen.

Kontroll-ID	AWS Config	Empfehlungen
P9	ebs-in-backup-plan	Stellen Sie zur Unterstützung der Datensicherungsprozesse sicher, dass Ihre Amazon Elastic Block Store (Amazon EBS) -Volumes Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihre Backup-Verwaltung und ermöglicht es Ihnen, Ihre geschäftlichen und behördlichen Anforderungen bezüglich Backups zu erfüllen.
P9	ec2--Plan resources-protected-by-backup	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon Elastic Compute Cloud (Amazon EC2) -Ressourcen Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	AWS Config	Empfehlungen
P9	efs-in-backup-plan	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon Elastic File System (Amazon EFS) - Dateisysteme Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.
P9	elasticache-redis-cluster-automatic-Backup-Check	Wenn automatische Backups aktiviert sind, ElastiCache erstellt Amazon täglich ein Backup des Clusters. Die Sicherung kann für eine von Ihrer Organisation festgelegte Anzahl von Tagen aufbewahrt werden. Automatische Backups schützen vor Datenverlust. Bei einem Ausfall können Sie einen neuen Cluster erstellen, der Ihre Daten aus dem aktuellen Backup wiederherstellt.

Kontroll-ID	AWS Config	Empfehlungen
P9	fsx-resources-protected-by-Backup-Plan	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre FSx Amazon-Dateisysteme Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	AWS Config	Empfehlungen
P9	rds-in-backup-plan	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon Relational Database Service (Amazon RDS) -Instances Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	AWS Config	Empfehlungen
P9	redshift-backup-enabled	Stellen Sie zur Unterstützung der Datensicherungsprozesse sicher, dass Ihre Amazon-Redshift-Cluster über automatisierte Snapshots verfügen. Wenn automatisierte Snapshots für einen Cluster aktiviert sind, erstellt Redshift in regelmäßigen Abständen Snapshots dieses Clusters. Standardmäßig erstellt Redshift alle acht Stunden oder alle 5 GB einen Snapshot für jeden Knoten mit Datenänderungen oder je nachdem, was zuerst eintritt.

Kontroll-ID	AWS Config	Empfehlungen
P10	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) kann Ihnen dabei helfen, die Prinzipien der geringsten Rechte und der Aufgabent rennung in Zugriffsberechtigu ngen und Autorisierungen zu integrieren und so zu verhindern, dass Richtlinien „Effect“: „Allow“ mit „Action“: „*“ anstelle von „Resource“: „*“ enthalten. Wenn Benutzern mehr Rechte eingeräumt werden, als für die Ausführun g einer Aufgabe erforderl ich sind, kann dies gegen das Prinzip der geringste n Berechtigung und der Aufgabentrennung verstoßen.

Kontroll-ID	AWS Config	Empfehlungen
P10	iam-no-inline-policy-überprüfen	Stellen Sie sicher, dass ein Benutzer, eine IAM-Rolle oder eine IAM-Gruppe (AWS Identity and Access Management) nicht über eine Inline-Richtlinie zur Zugriffskontrolle auf Systeme und Ressourcen verfügt. AWS empfiehlt, verwaltete Richtlinien anstelle von Inline-Richtlinien zu verwenden . Verwaltete Richtlinien ermöglichen Wiederverwendbarkeit, Versionsverwaltung, Rollback und Delegierung der Berechtigungsverwaltung.

Kontroll-ID	AWS Config	Empfehlungen
P10	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) kann Ihnen helfen, die Prinzipien der geringsten Rechte und der Aufgabentrennung in Zugriffsberechtigungen und Autorisierungen zu integrier en und so zu verhindern, dass Richtlinien blockierte Aktionen für alle AWS Schlüssel des Key Management Service enthalten. Wenn Benutzer mehr Rechte haben, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und Aufgabentrennung verstoßen . Mit dieser Regel können Sie den Parameter festlegen. blockedActionsPatterns (Wert „AWS Bewährte grundlegende Sicherheitsmethoden“: kms: Entschlüsseln, kms:ReEnc ryptFrom). Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprech en.

Kontroll-ID	AWS Config	Empfehlungen
P10	iam-inline-policy-blocked-kms-Aktionen	Stellen Sie sicher, dass ein Benutzer, eine IAM-Rolle oder eine IAM-Gruppe (AWS Identity and Access Management) nicht über eine Inline-Richtlinie verfügt, die blockierte Aktionen für alle AWS Schlüssel des Key Management Service zulässt. AWS empfiehlt, verwaltete Richtlinien anstelle von Inline-Richtlinien zu verwenden. Verwaltete Richtlinien ermöglichen Wiederverwendbarkeit, Versionsverwaltung, Rollback und Delegierung der Berechtigungsverwaltung. Mit dieser Regel können Sie den blockedActionsPatterns Parameter festlegen. (Wert „AWS Bewährte grundlegende Sicherheitsmethoden“: kms:Entschlüsseln, kms:ReEncryptFrom). Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	AWS Config	Empfehlungen
P10	iam-policy-no-statements-with-full-access	Stellen Sie sicher, dass IAM-Aktionen nur auf die benötigte n Aktionen beschränkt sind. Wenn Benutzern mehr Rechte eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und der Aufgabentrennung verstoßen.
P11	iam-user-group-membership-überprüfen	AWS Identity and Access Management (IAM) kann Ihnen helfen, Zugriffsb erechtigungen und Autorisie rungen einzuschränken, indem sichergestellt wird, dass Benutzer Mitglieder mindesten s einer Gruppe sind. Wenn Benutzern mehr Berechtig ungen eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtig ung und Aufgabentrennung verstoßen.

Vorlage

Die Vorlage ist verfügbar unter GitHub: Operational Best Practices for ACSC ISM.

Bewährte Methoden für die Ausführung von KI und ML

Dieses Konformitätspaket enthält AWS Config Regeln, die auf KI und ML basieren. Eine Liste aller verwalteten Regeln, die von unterstützt werden AWS Config, finden Sie unter Liste der AWS Config verwalteten Regeln.

Die Namen und Beschreibungen der erforderlichen Parameter finden Sie im `Parameters` Abschnitt der folgenden Vorlage.

Die Vorlage ist verfügbar unter GitHub: Operationelle Best Practices für KI und ML.

Bewährte Methoden für die Implementierung von Amazon API Gateway

Dieses Konformitätspaket enthält AWS Config Regeln, die auf der Nutzung von Amazon API Gateway innerhalb AWS von Amazon API Gateway basieren. Eine Liste aller verwalteten Regeln, die von unterstützt werden AWS Config, finden Sie unter Liste der AWS Config verwalteten Regeln.

Die Namen und Beschreibungen der erforderlichen Parameter finden Sie im `Parameters` Abschnitt der folgenden Vorlage.

Die Vorlage ist verfügbar unter GitHub: Operational Best Practices for Amazon API Gateway.

Bewährte Betriebspraktiken für Amazon CloudWatch

Dieses Konformitätspaket enthält AWS Config Regeln, die auf der Nutzung von Amazon CloudWatch innerhalb AWS von Amazon basieren. Eine Liste aller verwalteten Regeln, die von unterstützt werden AWS Config, finden Sie unter Liste der AWS Config verwalteten Regeln.

Die Namen und Beschreibungen der erforderlichen Parameter finden Sie im `Parameters` Abschnitt der folgenden Vorlage.

Die Vorlage ist verfügbar unter GitHub: Operational Best Practices for Amazon CloudWatch.

Bewährte Methoden für die Ausführung von Amazon DynamoDB

Die Vorlage ist verfügbar unter GitHub: Operational Best Practices for Amazon DynamoDB.

Bewährte Methoden für die Ausführung von Amazon S3

Die Vorlage ist verfügbar unter GitHub: Operational Best Practices for Amazon S3.

Bewährte Methoden für die Implementierung von APRA CPG 234

Konformitätspakete bieten ein allgemeines Compliance-Framework, das es Ihnen ermöglicht, mithilfe verwalteter oder benutzerdefinierter Regeln und Abhilfemaßnahmen Kontrollen zur Sicherheits-, Betriebs- oder Kostenoptimierung durchzuführen. AWS Config AWS Config Conformance Packs dienen als Beispielvorlagen nicht dazu, die vollständige Einhaltung eines bestimmten Governance- oder Compliance-Standards sicherzustellen. Sie sind dafür verantwortlich, selbst zu beurteilen, ob Ihre Nutzung der Services den geltenden gesetzlichen und behördlichen Anforderungen entspricht.

Im Folgenden finden Sie ein Beispiel für eine Zuordnung zwischen CPG 234 der Australian Prudential Regulation Authority (APRA) und AWS verwalteten Konfigurationsregeln. Jede Config-Regel gilt für eine bestimmte AWS Ressource und bezieht sich auf eine oder mehrere APRA CPG 234-Steuerelemente. Eine Kontrolle nach APRA CPG 234 kann mehreren Konfigurationsregeln zugeordnet werden. In der folgenden Tabelle finden Sie weitere Informationen und Anleitungen zu diesen Zuordnungen.

Diese Vorlage für ein Konformitätspaket enthält Zuordnungen zu Kontrollen innerhalb des Frameworks APRA CPG 234 2019, das vom Commonwealth of Australia erstellt wurde und unter Prudential Practice Guide: CPG 234 Information Security zu finden ist. Die Lizenzierung des Frameworks unter der Creative Commons Australia Namensnennung 3.0 Lizenz und Informationen zum Urheberrecht für das Framework (einschließlich eines Gewährleistungsausschlusses) finden Sie unter APRA | Copyright.

Kontroll-ID	AWS Config	Empfehlungen
36a	ec2-manager instance-managed-by-systems	Eine Bestandsaufnahme der Softwareplattformen und Anwendungen innerhalb des Unternehmens ist möglich, indem Amazon Elastic Compute Cloud (Amazon EC2) -Instances mit AWS Systems Manager verwaltet werden. Verwenden Sie AWS Systems Manager, um detaillierte Systemkonfiguratio nen, Betriebssystem-Patch-Levels, Namen und Typ der

Kontroll-ID	AWS Config	Empfehlungen
		Dienste, Softwareinstallationen, Anwendungsname, Herausgeber und Version sowie andere Details zu Ihrer Umgebung bereitzustellen.
36a	ec2-check managedinstance-association-compliance-status	Verwenden Sie AWS Systems Manager Associations, um bei der Inventarisierung von Softwareplattformen und Anwendungen innerhalb eines Unternehmens zu helfen. AWS Systems Manager weist Ihren verwalteten Instances einen Konfigurationsstatus zu und ermöglicht es Ihnen, Basiswerte für Betriebssystem-Patch-Levels, Softwareinstallationen, Anwendungskonfigurationen und andere Details zu Ihrer Umgebung festzulegen.
36a	ec2-prüfen managedinstance-patch-compliance-status	Aktivieren Sie diese Regel, um bei der Identifizierung und Dokumentation von Sicherheitslücken in Amazon Elastic Compute Cloud (Amazon EC2) zu helfen. Die Regel prüft, ob die EC2 Amazon-Instance die Patch-Konformität im AWS Systems Manager gemäß den Richtlinien und Verfahren Ihrer Organisation einhält.

Kontroll-ID	AWS Config	Empfehlungen
36b	ec2-manager instance-managed-by-systems	Eine Bestandsaufnahme der Softwareplattformen und Anwendungen innerhalb des Unternehmens ist möglich, indem Amazon Elastic Compute Cloud (Amazon EC2) -Instances mit AWS Systems Manager verwaltet werden. Verwenden Sie AWS Systems Manager, um detaillierte Systemkonfigurationen, Betriebssystem-Patch-Levels, Namen und Typ der Dienste, Softwareinstallationen, Anwendungsname, Herausgeber und Version sowie andere Details zu Ihrer Umgebung bereitzustellen.

Kontroll-ID	AWS Config	Empfehlungen
36b	ec2-check managedinstance-association-compliance-status	Verwenden Sie AWS Systems Manager Associations, um bei der Inventarisierung von Softwareplattformen und Anwendungen innerhalb eines Unternehmens zu helfen. AWS Systems Manager weist Ihren verwalteten Instances einen Konfigurationsstatus zu und ermöglicht es Ihnen, Basiswerte für Betriebss ystem-Patch-Levels, Softwarei nstallationen, Anwendung skonfigurationen und andere Details zu Ihrer Umgebung festzulegen.
36b	ec2-prüfen managedinstance-patch-compliance-status	Aktivieren Sie diese Regel, um bei der Identifizierung und Dokumentation von Sicherhei tslücken in Amazon Elastic Compute Cloud (Amazon EC2) zu helfen. Die Regel prüft, ob die EC2 Amazon-In stance die Patch-Konformität im AWS Systems Manager gemäß den Richtlinien und Verfahren Ihrer Organisation einhält.

Kontroll-ID	AWS Config	Empfehlungen
36b	cloudtrail-security-trail-enabled	Diese Regel trägt dazu bei, die Verwendung der AWS empfohlenen bewährten Sicherheitsmethoden für sicherzustellen AWS CloudTrail, indem geprüft wird, ob mehrere Einstellungen aktiviert sind. Dazu gehören die Verwendung von Protokoll verschlüsselung, Protokoll validierung und Aktivierung AWS CloudTrail in mehreren Regionen.

Kontroll-ID	AWS Config	Empfehlungen
36b	redshift-cluster-maintenancesettings-check	Diese Regel stellt sicher, dass Amazon-Redshift-Cluster die bevorzugten Einstellungen für Ihre Organisation haben. Insbesondere sorgt sie dafür, dass Cluster bevorzugte Wartungsfenster und automatisierte Aufbewahrungsfristen für Snapshots für die Datenbank haben. Für diese Regel müssen Sie die festlegen allowVersionUpgrade. Der Standardwert ist „true“. Außerdem können Sie optional den Zeitraum preferredMaintenanceWindow (der Standardwert ist sa: 16:00 -sa: 16:30) und den automatedSnapshotRetention Zeitraum (der Standardwert ist 1) festlegen. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	AWS Config	Empfehlungen
36b	elastic-beanstalk-managed-updates-aktiviert	Durch die Aktivierung verwalteter Plattformupdates für eine Amazon-Elastic-Beanstalk-Umgebung wird sichergestellt, dass die aktuellen verfügbaren Plattform-Fixes, -Updates und -Features für die Umgebung installiert sind. Eine bewährte Methode zur Sicherung von Systemen besteht darin, stets die aktuellen Patches zu installieren.
36b	rds-automatic-minor-version-upgrade-fähig	Aktivieren Sie automatische Unterversions-Upgrades auf Ihren Amazon-Relational-Database-Service (RDS)-Instances, um sicherzustellen, dass die aktuellen Updates für Unterversionen des Relational Database Management System (RDBMS) installiert sind, die Sicherheitspatches und Bugfixes enthalten können.

Kontroll-ID	AWS Config	Empfehlungen
36c	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) kann Ihnen dabei helfen, die Prinzipien der geringsten Rechte und der Aufgabent rennung in Zugriffsberechtigu ngen und Autorisierungen zu integrieren und so zu verhindern, dass Richtlinien „Effect“: „Allow“ mit „Action“: „*“ anstelle von „Resource“: „*“ enthalten. Wenn Benutzern mehr Rechte eingeräumt werden, als für die Ausführun g einer Aufgabe erforderl ich sind, kann dies gegen das Prinzip der geringste n Berechtigung und der Aufgabentrennung verstoßen.

Kontroll-ID	AWS Config	Empfehlungen
36c	iam-user-group-membership-überprüfen	AWS Identity and Access Management (IAM) kann Ihnen helfen, Zugriffsberechtigungen und Autorisierungen einzuschränken, indem sichergestellt wird, dass Benutzer Mitglieder mindestens einer Gruppe sind. Wenn Benutzern mehr Berechtigungen eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und Aufgabentrennung verstoßen.
36c	iam-no-inline-policy-überprüfen	Stellen Sie sicher, dass ein Benutzer, eine IAM-Rolle oder eine IAM-Gruppe (AWS Identity and Access Management) nicht über eine Inline-Richtlinie zur Zugriffskontrolle auf Systeme und Ressourcen verfügt. AWS empfiehlt, verwaltete Richtlinien anstelle von Inline-Richtlinien zu verwenden . Verwaltete Richtlinien ermöglichen Wiederverwendbarkeit, Versionsverwaltung, Rollback und Delegierung der Berechtigungsverwaltung.

Kontroll-ID	AWS Config	Empfehlungen
36c	restricted-common-ports	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass gemeinsame Ports für Amazon Elastic Compute Cloud (Amazon EC2) - Sicherheitsgruppen eingeschränkt sind. Wenn der Zugriff auf Ports nicht auf vertrauenswürdige Quellen beschränkt wird, kann dies zu Angriffen auf die Verfügbarkeit, Integrität und Vertraulichkeit von Systemen führen. Mit dieser Regel können Sie optional die Parameter blockedPort1–blockedPort5 festlegen (Standardkonfigurationen: 20, 21, 3389, 3306, 4333). Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	AWS Config	Empfehlungen
36c	vpc-sg-open-only-to-authorized-ports	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass gemeinsame Ports für Amazon Elastic Compute Cloud (Amazon EC2) - Sicherheitsgruppen eingeschränkt sind. Wenn der Zugriff auf Ports nicht auf vertrauenswürdige Quellen beschränkt wird, kann dies zu Angriffen auf die Verfügbarkeit, Integrität und Vertraulichkeit von Systemen führen. Durch die Beschränkung des Zugriffs auf Ressourcen innerhalb einer Sicherheitsgruppe aus dem Internet (0.0.0.0/0) kann der Fernzugriff auf interne Systeme gesteuert werden.

Kontroll-ID	AWS Config	Empfehlungen
36c	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) Security Groups können bei der Verwaltung des Netzwerkz ugriffs helfen, indem sie eine statusbehaftete Filterung von eingehendem und ausgehend em Netzwerkverkehr zu Ressourcen bereitstellen. AWS Wenn Sie eingehenden (oder entfernten) Datenverk ehr von 0.0.0.0/0 bis Port 22 auf Ihren Ressourcen nicht zulassen, können Sie den Remote-Zugriff einschränken.
36c	ec-2 instance-profile-attached	EC2 Instanzprofile übergeben eine IAM-Rolle an eine EC2 Instance. Das Anhängen eines Instance-Profils an Ihre Instances kann bei der Implementierung von geringsten Berechtigungen und der Berechtigungsverwa ltung helfen.

Kontroll-ID	AWS Config	Empfehlungen
36c	iam-policy-no-statements-with-full-access	Stellen Sie sicher, dass IAM-Aktionen nur auf die benötigte n Aktionen beschränkt sind. Wenn Benutzern mehr Rechte eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und der Aufgabentrennung verstoßen.
36c	ecs-task-definition-user-for-host-mode-check	Wenn für eine Aufgabend efinition erhöhte Berechtig ungen gelten, liegt das daran, dass der Kunde diesen Konfigurationen ausdrücklich zugestimmt hat. Diese Kontrolle prüft, ob eine unerwartete Berechtig ungseskalation vorliegt, wenn für eine Aufgabendefinition das Host-Netzwerk aktiviert ist, die Kunden aber keine erhöhten Berechtigungen aktiviert haben.

Kontroll-ID	AWS Config	Empfehlungen
36d	dms-replication-not-public	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass auf DMS-Replikationsinstanzen nicht öffentlich zugegriffen werden kann. DMS-Replikations-I nstances können vertrauli che Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.
36d	ebs-snapshot-public-restora ble-überprüfen	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass EBS-Snaps hots nicht öffentlich wiederher stellbar sind. EBS-Volume-Snapshots können vertrauli che Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.
36d	ec-2 instance-no-public-ip	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon Elastic Compute Cloud (Amazon EC2) -Instances nicht öffentlich zugänglich sind. EC2Amazon-Instances können vertrauliche Informati onen enthalten, und für solche Konten ist eine Zugriffsk ontrolle erforderlich.

Kontroll-ID	AWS Config	Empfehlungen
36d	elasticsearch-in-vpc-only	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass sich Amazon OpenSearch OpenSearch Service (Service) -Domains innerhalb einer Amazon Virtual Private Cloud (Amazon VPC) befinden. Eine OpenSearch Service-Domain innerhalb einer Amazon VPC ermöglicht die sichere Kommunikation zwischen OpenSearch Service und anderen Services innerhalb der Amazon VPC, ohne dass ein Internet-Gateway, ein NAT-Gerät oder eine VPN-Verbindung erforderlich ist.
36d	emr-master-no-public-ip	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon EMR-Cluster-Masterknoten nicht öffentlich zugänglich sind. Amazon-EMR-Cluster-Hauptknoten können vertrauliche Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	AWS Config	Empfehlungen
36d	ec-2 instances-in-vpc	Stellen Sie Amazon Elastic Compute Cloud (Amazon EC2) -Instances innerhalb einer Amazon Virtual Private Cloud (Amazon VPC) bereit, um eine sichere Kommunika tion zwischen einer Instance und anderen Services innerhalb der Amazon VPC zu ermöglichen, ohne dass ein Internet-Gateway, ein NAT-Gerät oder eine VPN-Verbi ndung erforderlich ist. Der gesamte Datenverkehr bleibt sicher in der AWS Cloud. Domains, die sich innerhalb einer VPC befinden, verfügen aufgrund ihrer logischen Isolierung im Vergleich zu Domains mit öffentlic hen Endpunkten über eine zusätzliche Sicherheitsebene. Weisen Sie EC2 Amazon-In stances einer Amazon-VPC zu, um den Zugriff ordnungsg emäß zu verwalten.

Kontroll-ID	AWS Config	Empfehlungen
36d	internet-gateway-authorized-vpc-nur	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Internet-Gateways nur mit autorisierter Amazon Virtual Private Cloud (Amazon VPC) verbunden sind. Internet-Gateways ermöglichen den bidirekti onalen Internetzugang zur und von der Amazon VPC, was möglicherweise zu einem unbefugten Zugriff auf Amazon-VPC-Ressourcen führen kann.
36d	lambda-function-public-acce ss-verboten	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherste llen, dass AWS Lambda-Funktionen nicht öffentlich zugänglich sind. Der öffentlic he Zugriff kann möglicher weise die Verfügbarkeit von Ressourcen beeinträchtigen.

Kontroll-ID	AWS Config	Empfehlungen
36d	lambda-inside-vpc	Stellen Sie AWS Lambda-Funktionen in einer Amazon Virtual Private Cloud (Amazon VPC) bereit, um eine sichere Kommunikation zwischen einer Funktion und anderen Diensten innerhalb der Amazon VPC zu gewährleisten. Bei dieser Konfiguration sind kein Internet-Gateway, kein NAT-Gerät und keine VPN-Verbindung erforderlich. Der gesamte Datenverkehr bleibt sicher in der Cloud. AWS Domains, die sich innerhalb einer VPC befinden, verfügen aufgrund ihrer logischen Isolierung im Vergleich zu Domains mit öffentlichen Endpunkten über eine zusätzliche Sicherheitsebene. Um den Zugriff ordnungsgemäß zu verwalten, sollten AWS Lambda-Funktionen einer VPC zugewiesen werden.

Kontroll-ID	AWS Config	Empfehlungen
36d	rds-instance-public-access-überprüfen	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Relational Database Service (Amazon RDS) -Instances nicht öffentlich sind. Amazon-RDS-Datenbank-Instances können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.
36d	rds-snapshots-public-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Relational Database Service (Amazon RDS) -Instances nicht öffentlich sind. Amazon-RDS-Datenbank-Instances können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	AWS Config	Empfehlungen
36d	redshift-cluster-public-access-überprüfen	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Redshift Redshift-Cluster nicht öffentlich sind. Amazon-Redshift-Cluster können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.
36d	s-3 bucket-public-read-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie nur autorisierten Benutzern, Prozessen und Geräten Zugriff auf Amazon Simple Storage Service (Amazon S3) -Buckets gewähren. Die Verwaltung des Zugriffs sollte mit der Klassifizierung der Daten übereinstimmen.
36d	s3- bucket-public-write-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie nur autorisierten Benutzern, Prozessen und Geräten Zugriff auf Amazon Simple Storage Service (Amazon S3) -Buckets gewähren. Die Verwaltung des Zugriffs sollte mit der Klassifizierung der Daten übereinstimmen.

Kontroll-ID	AWS Config	Empfehlungen
36d	sagemaker-notebook-no-direct-Internetzugang	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass SageMaker Amazon-Notebooks keinen direkten Internetzugang zulassen. Indem Sie direkten Internetzugang blockieren, vermeiden Sie, dass unbefugte Benutzer auf sensible Daten zugreifen.

Kontroll-ID	AWS Config	Empfehlungen
36d	access-keys-rotated	Die Anmeldeinformationen für autorisierte Geräte, Benutzer und Prozesse werden geprüft, indem sichergestellt wird, dass die IAM-Zugriffsschlüssel entsprechend den Vorgaben der Unternehmensrichtlinie rotiert werden. Das regelmäßi ge Ändern der Zugriffss chlüssel ist eine bewährte Sicherheitsmethode. Es verkürzt den Zeitraum, in dem ein Zugriffsschlüssel aktiv ist, und reduziert die Auswirkun gen auf das Unternehmen, wenn die Schlüssel kompromit tiert werden. Diese Regel erfordert einen Wert für die Zugriffsschlüssel-Rotation (Standardkonfiguration: 90). Der tatsächliche Wert muss den Richtlinien Ihrer Organisat ion entsprechen.

Kontroll-ID	AWS Config	Empfehlungen
36d	emr-kerberos-enabled	Die Zugriffsberechtigungen und -autorisierungen können verwaltet und nach den Prinzipien der geringsten Berechtigung und Aufgabent rennung integriert werden, indem Kerberos für Amazon-EMR-Cluster aktiviert wird. In Kerberos werden Services und Benutzer, die sich authentifizieren müssen, als Prinzipale bezeichnet. Prinzipale befinden sich in einem Kerberos-Bereich. Innerhalb dieses Bereichs wird ein Kerberos-Server als Key Distribution Center (KDC) bezeichnet. Über diesen Server können sich Prinzipale authentifizieren. Die Authentifizierung im KDC erfolgt durch die Ausstellu ng von Authentifizierungs tickets. Das KDC unterhält eine Datenbank der Prinzipal e in seinem Bereich mit ihren Passwörtern und anderen administrativen Informationen zu jedem Prinzipal.

Kontroll-ID	AWS Config	Empfehlungen
36d	iam-password-policy	Die Identitäten und Anmeldein formationen werden auf der Grundlage einer organisat orischen IAM-Passwortrichtl inie ausgestellt, verwaltet und verifiziert. Sie erfüllen oder übertreffen die Anforderu ngen von NIST SP 800-63 und dem Standard „Best Practices“ von AWS Foundatio nal Security in Bezug auf die Passwortstärke. Mit dieser Regel können Sie optional RequireUppercaseCharacters (Wert für AWS grundlege nde Sicherheitsbewährte Methoden: wahr), RequireLo wercaseCharacters (Wert für bewährte Methoden für AWS grundlegende Sicherheit: wahr), RequireSymbols (Wert für bewährte Methoden für AWS grundlegende Sicherhei t: wahr), RequireNumbers (Wert für bewährte Methoden für AWS grundlegende Sicherheit: wahr), MinimumPa sswordLength (Wert für bewährte Methoden für AWS grundlegende Sicherheit: 14), PasswordReusePreve ntion (Wert für bewährte Methoden für AWS grundlege nde Sicherheit: 24) und

Kontroll-ID	AWS Config	Empfehlungen
		MaxPasswordAge (Wert für bewährte Methoden für AWS grundlegende Sicherhei t: 90) für Ihr IAM festlegen . Kennwortrichtlinie. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisat ion entsprechen.
36d	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) kann Ihnen dabei helfen, die Prinzipien der geringsten Rechte und der Aufgabent rennung in Zugriffsberechtigu ngen und Autorisierungen zu integrieren und so zu verhindern, dass Richtlinien „Effect“: „Allow“ mit „Action“: „*“ anstelle von „Resource“: „*“ enthalten. Wenn Benutzern mehr Rechte eingeräumt werden, als für die Ausführun g einer Aufgabe erforderl ich sind, kann dies gegen das Prinzip der geringste n Berechtigung und der Aufgabentrennung verstoßen.

Kontroll-ID	AWS Config	Empfehlungen
36d	iam-root-access-key-überprüfen	Der Zugriff auf Systeme und Ressourcen kann gesteuert werden, indem überprüft wird, ob der Root-Benutzer keine Zugriffsschlüssel mit seiner AWS Identity and Access Management (IAM) -Rolle verknüpft hat. Stellen Sie sicher, dass die Root-Zugriffsschlüssel gelöscht werden. Erstellen und verwenden Sie stattdessen rollenbasierte Funktionen, AWS-Konten um das Prinzip der geringsten Funktionalität zu berücksichtigen.
36d	iam-user-group-membership-überprüfen	AWS Identity and Access Management (IAM) kann Ihnen helfen, Zugriffsberechtigungen und Autorisierungen einzuschränken, indem sichergestellt wird, dass Benutzer Mitglieder mindestens einer Gruppe sind. Wenn Benutzern mehr Berechtigungen eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und Aufgabentrennung verstoßen.

Kontroll-ID	AWS Config	Empfehlungen
36d	iam-user-mfa-enabled	Aktivieren Sie diese Regel, um den Zugriff auf Ressourcen in der AWS -Cloud einzuschränken. Diese Regel stellt sicher, dass die Multi-Faktor-Authentifizierung (MFA) für alle Benutzer aktiviert ist. MFA bietet eine weitere Schutzebene zusätzlich zum Benutzernamen und Passwort. Reduzieren Sie Fälle von kompromittierten Konten, indem Sie MFA für Benutzer vorschreiben.
36d	iam-user-no-policies-überprüfen	Diese Regel stellt sicher, dass AWS Identity and Access Management (IAM) -Richtlinien nur Gruppen oder Rollen zugewiesen werden, um den Zugriff auf Systeme und Ressourcen zu kontrollieren. Die Zuweisung von Berechtigungen auf Gruppen- oder Rollenebene trägt dazu bei, die Wahrscheinlichkeit zu verringern, dass eine Identität übermäßige Berechtigungen erhält oder beibehält.

Kontroll-ID	AWS Config	Empfehlungen
36d	iam-user-unused-credentials-überprüfen	AWS Identity and Access Management (IAM) kann Ihnen bei Zugriffsberechtigungen und Autorisierungen helfen, indem es nach IAM-Passwörtern und Zugriffsschlüsseln sucht, die für einen bestimmten Zeitraum nicht verwendet wurden. Wenn ungenutzte Anmeldeinformationen identifiziert werden, müssen Sie sie deaktivieren und/oder entfernen, da dies gegen das Prinzip der geringsten Berechtigung verstoßen könnte. Für diese Regel müssen Sie einen Wert für das maxCredentialUsage Alter festlegen (Standardkonfiguration: 90). Der tatsächliche Wert muss den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	AWS Config	Empfehlungen
36d	mfa-enabled-for-iam-Konsolenzugriff	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass MFA für alle AWS Identity and Access Management (IAM) -Benutzer aktiviert ist, die über ein Konsolenkennwort verfügen. MFA sorgt für eine weitere Schutzebene zusätzlich zu den Anmeldeinformationen. Indem Sie MFA für Benutzer vorschreiben, können Sie Fälle kompromittierter Konten reduzieren und verhindern, dass unbefugte Benutzer auf vertrauliche Daten zugreifen.
36d	root-account-hardware-mfa-aktiviert	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Hardware-MFA für den Root-Benutzer aktiviert ist. Der Stammbenutzer ist der AWS-Konto-Benutzer mit den meisten Berechtigungen. MFA sorgt für eine weitere Schutzebene zusätzlich zu den Anmeldeinformationen. Indem Sie MFA für den Root-Benutzer vorschreiben, können Sie die Anzahl AWS-Konten kompromittierter Benutzer reduzieren.

Kontroll-ID	AWS Config	Empfehlungen
36d	root-account-mfa-enabled	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass MFA für den Root-Benutzer aktiviert ist. Der Stammbenutzer ist der AWS-Konto-Benutzer mit den meisten Berechtigungen. MFA bietet eine weitere Schutzebene zusätzlich zum Benutzernamen und Passwort. Indem Sie MFA für den Root-Benutzer vorschreiben, können Sie die Anzahl AWS-Konten kompromittierter Benutzer reduzieren.
36d	ec2-imdsv2-check	Stellen Sie sicher, dass die Methode Instance Metadata Service Version 2 (IMDSv2) aktiviert ist, um den Zugriff auf und die Kontrolle der Amazon Elastic Compute Cloud (Amazon EC2) -Instance-Metadaten zu schützen. Die IMDSv2 Methode verwendet sitzungsbasierte Kontrollen. Mit können Kontrollen implementiert werden IMDSv2, um Änderungen an Instanzmetadaten einzuschränken.

Kontroll-ID	AWS Config	Empfehlungen
36d	iam-no-inline-policy-überprüfen	Stellen Sie sicher, dass ein Benutzer, eine IAM-Rolle oder eine IAM-Gruppe (AWS Identity and Access Management) nicht über eine Inline-Richtlinie zur Zugriffskontrolle auf Systeme und Ressourcen verfügt. AWS empfiehlt, verwaltete Richtlinien anstelle von Inline-Richtlinien zu verwenden . Verwaltete Richtlinien ermöglichen Wiederverwendbarkeit, Versionsverwaltung, Rollback und Delegierung der Berechtigungsverwaltung.

Kontroll-ID	AWS Config	Empfehlungen
36d	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) kann Ihnen helfen, die Prinzipien der geringsten Rechte und der Aufgabentrennung in Zugriffsberechtigungen und Autorisierungen zu integrier en und so zu verhindern, dass Richtlinien blockierte Aktionen für alle AWS Schlüssel des Key Management Service enthalten. Wenn Benutzer mehr Rechte haben, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtig ung und Aufgabentrennung verstoßen. Mit dieser Regel können Sie den Parameter festlegen. blockedActionsPatt erns (Wert „AWS Bewährte grundlegende Sicherhei tsmethoden“: kms: Decrypt, kms:ReEncryptFrom). Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisat ion entsprechen.

Kontroll-ID	AWS Config	Empfehlungen
36d	iam-inline-policy-blocked-kms-Aktionen	Stellen Sie sicher, dass ein Benutzer, eine IAM-Rolle oder eine IAM-Grupp e (AWS Identity and Access Management) nicht über eine Inline-Richtlinie verfügt, die blockierte Aktionen für alle AWS Schlüssel des Key Management Service zulässt. AWS empfiehlt, verwaltete Richtlinien anstelle von Inline-Richtlinien zu verwenden . Verwaltete Richtlinien ermöglichen Wiederver wendbarkeit, Versionsv erwaltung, Rollback und Delegierung der Berechtig ungsverwaltung. Mit dieser Regel können Sie den blockedActionsPatterns Parameter festlegen. (Wert „AWS Bewährte grundlege nde Sicherheitsmethoden“: kms: Decrypt, kms:ReEnc ryptFrom). Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprech en.

Kontroll-ID	AWS Config	Empfehlungen
36d	ec-2 instance-profile-attached	EC2 Instanzprofile übergeben eine IAM-Rolle an eine EC2 Instance. Das Anhängen eines Instance-Profils an Ihre Instances kann bei der Implementierung von geringsten Berechtigungen und der Berechtigungsverwa ltung helfen.
36d	iam-policy-no-statements-with-full-access	Stellen Sie sicher, dass IAM-Aktionen nur auf die benötigte n Aktionen beschränkt sind. Wenn Benutzern mehr Rechte eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und der Aufgabentrennung verstoßen.

Kontroll-ID	AWS Config	Empfehlungen
36d	ecs-task-definition-user-for-host-mode-check	Wenn für eine Aufgabend efinition erhöhte Berechtig ungen gelten, liegt das daran, dass der Kunde diesen Konfigurationen ausdrücklich zugestimmt hat. Diese Kontrolle prüft, ob eine unerwartete Berechtig ungseskalation vorliegt, wenn für eine Aufgabendefinition das Host-Netzwerk aktiviert ist, die Kunden aber keine erhöhten Berechtigungen aktiviert haben.
36d	no-unrestricted-route-to-igw	Stellen Sie sicher, dass EC2 Amazon-Routentabellen keine uneingeschränkten Routen zu einem Internet-Gateway enthalten. Durch das Entfernen oder Beschränk en des Internetzugangs für Workloads innerhalb von Amazon VPCs können unbeabsichtigte Zugriffe in Ihrer Umgebung reduziert werden.

Kontroll-ID	AWS Config	Empfehlungen
36d	s3- verboten bucket-level-public-access	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Simple Storage Service (Amazon S3) -Buckets nicht öffentlich zugänglich sind. Diese Regel trägt dazu bei, sensible Daten vor unbefugten Remote-Benutzern zu schützen, indem sie den öffentlichen Zugriff auf Bucket-Ebene verhindert.
36d	subnet-auto-assign-public-ip-deaktiviert	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon Virtual Private Cloud (VPC) -Subnetzen nicht automatisch eine öffentliche IP-Adresse zugewiesen wird. Amazon Elastic Compute Cloud (EC2) -Instances, die in Subnetzen gestartet werden, in denen dieses Attribut aktiviert ist, haben ihrer primären Netzwerkschnittstelle eine öffentliche IP-Adresse zugewiesen.

Kontroll-ID	AWS Config	Empfehlungen
36d	autoscaling-launch-config-public-ip-deaktiviert	Wenn Sie Ihre Netzwerkschnittstellen mit einer öffentlichen IP-Adresse konfigurieren, sind die diesen Netzwerkschnittstellen zugehörigen Ressourcen über das Internet erreichbar. EC2 Ressourcen sollten nicht öffentlich zugänglich sein, da dies einen unbeabsichtigten Zugriff auf Ihre Anwendungen oder Server ermöglichen kann.
36d	redshift-enhanced-vpc-routing-aktiviert	Mit Enhanced-VPC-Routing wird erzwungen, dass der gesamte COPY- und UNLOAD-Datenverkehr zwischen Ihrem Cluster und Datenrepositorys über Ihre Amazon VPC erfolgt. Anschließend können Sie VPC-Features wie Sicherheitsgruppen und Netzwerkzugriffskontrollllisten verwenden, um den Netzwerkverkehr zu schützen. Sie können auch VPC-Flow-Protokolle verwenden, um den Netzwerkverkehr zu überwachen.

Kontroll-ID	AWS Config	Empfehlungen
36d	s3- -Blocke-periodisch account-level-public-access	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Simple Storage Service (Amazon S3) -Buckets nicht öffentlich zugänglich sind. Diese Regel trägt dazu bei, sensible Daten vor unbefugten Remote-Benutzern zu schützen, indem sie den öffentlichen Zugriff verhindert. Mit dieser Regel können Sie optional die Parameter ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) und restrictPublicBuckets Parameter (Config Default: True) festlegen. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	AWS Config	Empfehlungen
36d	ssm-document-not-public	Stellen Sie sicher, dass AWS Systems Manager (SSM) - Dokumente nicht öffentlich sind, da dies einen unbeabsichtigten Zugriff auf Ihre SSM-Dokumente ermöglichen kann. Ein öffentliches SSM-Dokument kann Informationen über Ihr Konto, Ihre Ressourcen und internen Prozesse preisgeben.
36d	opensearch-in-vpc-only	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass sich Amazon OpenSearch Service-Domains innerhalb einer Amazon Virtual Private Cloud (Amazon VPC) befinden. Eine Amazon OpenSearch Service-Domain innerhalb einer Amazon VPC ermöglicht die sichere Kommunikation zwischen Amazon OpenSearch Service und anderen Services innerhalb der Amazon VPC, ohne dass ein Internet-Gateway, ein NAT-Gerät oder eine VPN-Verbindung erforderlich ist.

Kontroll-ID	AWS Config	Empfehlungen
36e	secretsmanager-rotation-enabled-check	Diese Regel stellt sicher, dass bei AWS Secrets Manager Manager-Geheimnissen die Rotation aktiviert ist. Die regelmäßige Rotation von Secrets kann den Zeitraum verkürzen, in dem ein Secret aktiv ist, und möglicherweise die Auswirkungen auf das Unternehmen verringern, falls das Secret kompromittiert wird.
36e	secretsmanager-scheduled-rotation-success-überprüfen	Diese Regel stellt sicher, dass AWS Secrets Manager Manager-Geheimnisse gemäß dem Rotationsplan erfolgreich rotiert wurden. Die regelmäßige Rotation von Secrets kann den Zeitraum verkürzen, in dem ein Secret aktiv ist, und möglicherweise die Auswirkungen auf das Unternehmen verringern, falls es kompromittiert wird.

Kontroll-ID	AWS Config	Empfehlungen
36e	dms-replication-not-public	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass auf DMS-Replikationsinstanzen nicht öffentlich zugegriffen werden kann. DMS-Replikations-I nstances können vertrauli che Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.
36e	ebs-snapshot-public-restora ble-überprüfen	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass EBS-Snaps hots nicht öffentlich wiederher stellbar sind. EBS-Volume-Snapshots können vertrauli che Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.
36e	ec-2 instance-no-public-ip	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon Elastic Compute Cloud (Amazon EC2) -Instances nicht öffentlich zugänglich sind. EC2Amazon-Instances können vertrauliche Informati onen enthalten, und für solche Konten ist eine Zugriffsk ontrolle erforderlich.

Kontroll-ID	AWS Config	Empfehlungen
36e	elasticsearch-in-vpc-only	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass sich Amazon OpenSearch OpenSearch Service (Service) -Domains innerhalb einer Amazon Virtual Private Cloud (Amazon VPC) befinden. Eine OpenSearch Service-Domain innerhalb einer Amazon VPC ermöglicht die sichere Kommunikation zwischen OpenSearch Service und anderen Services innerhalb der Amazon VPC, ohne dass ein Internet-Gateway, ein NAT-Gerät oder eine VPN-Verbindung erforderlich ist.
36e	emr-master-no-public-ip	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon EMR-Cluster-Masterknoten nicht öffentlich zugänglich sind. Amazon-EMR-Cluster-Hauptknoten können vertrauliche Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	AWS Config	Empfehlungen
36e	ec-2 instances-in-vpc	Stellen Sie Amazon Elastic Compute Cloud (Amazon EC2) -Instances innerhalb einer Amazon Virtual Private Cloud (Amazon VPC) bereit, um eine sichere Kommunika tion zwischen einer Instance und anderen Services innerhalb der Amazon VPC zu ermöglichen, ohne dass ein Internet-Gateway, ein NAT-Gerät oder eine VPN-Verbi ndung erforderlich ist. Der gesamte Datenverkehr bleibt sicher in der AWS Cloud. Domains, die sich innerhalb einer VPC befinden, verfügen aufgrund ihrer logischen Isolierung im Vergleich zu Domains mit öffentlic hen Endpunkten über eine zusätzliche Sicherheitsebene. Weisen Sie EC2 Amazon-In stances einer Amazon-VPC zu, um den Zugriff ordnungsg emäß zu verwalten.

Kontroll-ID	AWS Config	Empfehlungen
36e	internet-gateway-authorized-vpc-nur	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Internet-Gateways nur mit autorisierter Amazon Virtual Private Cloud (Amazon VPC) verbunden sind. Internet-Gateways ermöglichen den bidirekti onalen Internetzugang zur und von der Amazon VPC, was möglicherweise zu einem unbefugten Zugriff auf Amazon-VPC-Ressourcen führen kann.
36e	lambda-function-public-acce ss-verboten	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherste llen, dass AWS Lambda-Funktionen nicht öffentlich zugänglich sind. Der öffentlic he Zugriff kann möglicher weise die Verfügbarkeit von Ressourcen beeinträchtigen.

Kontroll-ID	AWS Config	Empfehlungen
36e	lambda-inside-vpc	Stellen Sie AWS Lambda-Funktionen in einer Amazon Virtual Private Cloud (Amazon VPC) bereit, um eine sichere Kommunikation zwischen einer Funktion und anderen Diensten innerhalb der Amazon VPC zu gewährleisten. Bei dieser Konfiguration sind kein Internet-Gateway, kein NAT-Gerät und keine VPN-Verbindung erforderlich. Der gesamte Datenverkehr bleibt sicher in der Cloud. AWS Domains, die sich innerhalb einer VPC befinden, verfügen aufgrund ihrer logischen Isolierung im Vergleich zu Domains mit öffentlichen Endpunkten über eine zusätzliche Sicherheitsebene. Um den Zugriff ordnungsgemäß zu verwalten, sollten AWS Lambda-Funktionen einer VPC zugewiesen werden.

Kontroll-ID	AWS Config	Empfehlungen
36e	rds-instance-public-access-überprüfen	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Relational Database Service (Amazon RDS) -Instances nicht öffentlich sind. Amazon-RDS-Datenbank-Instances können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.
36e	rds-snapshots-public-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Relational Database Service (Amazon RDS) -Instances nicht öffentlich sind. Amazon-RDS-Datenbank-Instances können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	AWS Config	Empfehlungen
36e	redshift-cluster-public-access-überprüfen	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Redshift Redshift-Cluster nicht öffentlich sind. Amazon-Redshift-Cluster können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.
36e	s-3 bucket-public-read-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie nur autorisierten Benutzern, Prozessen und Geräten Zugriff auf Amazon Simple Storage Service (Amazon S3) -Buckets gewähren. Die Verwaltung des Zugriffs sollte mit der Klassifizierung der Daten übereinstimmen.
36e	s3- bucket-public-write-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie nur autorisierten Benutzern, Prozessen und Geräten Zugriff auf Amazon Simple Storage Service (Amazon S3) -Buckets gewähren. Die Verwaltung des Zugriffs sollte mit der Klassifizierung der Daten übereinstimmen.

Kontroll-ID	AWS Config	Empfehlungen
36e	sagemaker-notebook-no-direct-Internetzugang	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass SageMaker Amazon-Notebooks keinen direkten Internetzugang zulassen. Indem Sie direkten Internetzugang blockieren, vermeiden Sie, dass unbefugte Benutzer auf sensible Daten zugreifen.
36e	ec-2 instance-profile-attached	EC2 Instanzprofile übergeben eine IAM-Rolle an eine EC2 Instance. Das Anhängen eines Instance-Profils an Ihre Instances kann bei der Implementierung von geringsten Berechtigungen und der Berechtigungsverwaltung helfen.
36e	no-unrestricted-route-to-igw	Stellen Sie sicher, dass EC2 Amazon-Routentabellen keine uneingeschränkten Routen zu einem Internet-Gateway enthalten. Durch das Entfernen oder Beschränken des Internetzugangs für Workloads innerhalb von Amazon VPCs können unbeabsichtigte Zugriffe in Ihrer Umgebung reduziert werden.

Kontroll-ID	AWS Config	Empfehlungen
36e	s3- verboten bucket-level-public-access	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Simple Storage Service (Amazon S3) -Buckets nicht öffentlich zugänglich sind. Diese Regel trägt dazu bei, sensible Daten vor unbefugten Remote-Benutzern zu schützen, indem sie den öffentlichen Zugriff auf Bucket-Ebene verhindert.
36e	subnet-auto-assign-public-ip-deaktiviert	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon Virtual Private Cloud (VPC) -Subnetzen nicht automatisch eine öffentliche IP-Adresse zugewiesen wird. Amazon Elastic Compute Cloud (EC2) -Instances, die in Subnetzen gestartet werden, in denen dieses Attribut aktiviert ist, haben ihrer primären Netzwerkschnittstelle eine öffentliche IP-Adresse zugewiesen.

Kontroll-ID	AWS Config	Empfehlungen
36e	autoscaling-launch-config-public-ip-deaktiviert	Wenn Sie Ihre Netzwerkschnittstellen mit einer öffentlichen IP-Adresse konfigurieren, sind die diesen Netzwerkschnittstellen zugehörigen Ressourcen über das Internet erreichbar. EC2 Ressourcen sollten nicht öffentlich zugänglich sein, da dies einen unbeabsichtigten Zugriff auf Ihre Anwendungen oder Server ermöglichen kann.
36e	redshift-enhanced-vpc-routing-aktiviert	Mit Enhanced-VPC-Routing wird erzwungen, dass der gesamte COPY- und UNLOAD-Datenverkehr zwischen Ihrem Cluster und Datenrepositorys über Ihre Amazon VPC erfolgt. Anschließend können Sie VPC-Features wie Sicherheitsgruppen und Netzwerkzugriffskontrollllisten verwenden, um den Netzwerkverkehr zu schützen. Sie können auch VPC-Flow-Protokolle verwenden, um den Netzwerkverkehr zu überwachen.

Kontroll-ID	AWS Config	Empfehlungen
36e	api-gw-associated-with-WAF	AWS Mit WAF können Sie eine Reihe von Regeln (als Web Access Control List (Web ACL) bezeichnet) konfiguri eren, die Webanfragen auf der Grundlage von anpassbar en Websicherheitsregeln und -bedingungen, die Sie definieren, zulassen, blockiere n oder zählen. Stellen Sie sicher, dass Ihre Amazon-API-Gateway-Stufe mit einer WAF-Web-ACL verknüpft ist, um sie vor böswilligen Angriffen zu schützen.

Kontroll-ID	AWS Config	Empfehlungen
36e	s3- -blöcke-periodisch account-level-public-access	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Simple Storage Service (Amazon S3) -Buckets nicht öffentlich zugänglich sind. Diese Regel trägt dazu bei, sensible Daten vor unbefugten Remote-Benutzern zu schützen, indem sie den öffentlichen Zugriff verhindert. Mit dieser Regel können Sie optional die Parameter ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) und restrictPublicBuckets Parameter (Config Default: True) festlegen. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	AWS Config	Empfehlungen
36e	ssm-document-not-public	Stellen Sie sicher, dass AWS Systems Manager (SSM) - Dokumente nicht öffentlich sind, da dies einen unbeabsichtigten Zugriff auf Ihre SSM-Dokumente ermöglichen kann. Ein öffentliches SSM-Dokument kann Informationen über Ihr Konto, Ihre Ressourcen und internen Prozesse preisgeben.
36e	opensearch-in-vpc-only	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass sich Amazon OpenSearch Service-Domains innerhalb einer Amazon Virtual Private Cloud (Amazon VPC) befinden. Eine Amazon OpenSearch Service-Domain innerhalb einer Amazon VPC ermöglicht die sichere Kommunikation zwischen Amazon OpenSearch Service und anderen Services innerhalb der Amazon VPC, ohne dass ein Internet-Gateway, ein NAT-Gerät oder eine VPN-Verbindung erforderlich ist.

Kontroll-ID	AWS Config	Empfehlungen
36f	dms-replication-not-public	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass auf DMS-Replikationsinstanzen nicht öffentlich zugegriffen werden kann. DMS-Replikations-I nstances können vertrauli che Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.
36f	ebs-snapshot-public-restora ble-überprüfen	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass EBS-Snaps hots nicht öffentlich wiederher stellbar sind. EBS-Volume-Snapshots können vertrauli che Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.
36f	ec-2 instance-no-public-ip	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon Elastic Compute Cloud (Amazon EC2) -Instances nicht öffentlich zugänglich sind. EC2Amazon-Instances können vertrauliche Informati onen enthalten, und für solche Konten ist eine Zugriffsk ontrolle erforderlich.

Kontroll-ID	AWS Config	Empfehlungen
36f	elasticsearch-in-vpc-only	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass sich Amazon OpenSearch OpenSearch Service (Service) -Domains innerhalb einer Amazon Virtual Private Cloud (Amazon VPC) befinden. Eine OpenSearch Service-Domain innerhalb einer Amazon VPC ermöglicht die sichere Kommunikation zwischen OpenSearch Service und anderen Services innerhalb der Amazon VPC, ohne dass ein Internet-Gateway, ein NAT-Gerät oder eine VPN-Verbindung erforderlich ist.
36f	emr-master-no-public-ip	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon EMR-Cluster-Masterknoten nicht öffentlich zugänglich sind. Amazon-EMR-Cluster-Hauptknoten können vertrauliche Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	AWS Config	Empfehlungen
36f	ec-2 instances-in-vpc	Stellen Sie Amazon Elastic Compute Cloud (Amazon EC2) -Instances innerhalb einer Amazon Virtual Private Cloud (Amazon VPC) bereit, um eine sichere Kommunika tion zwischen einer Instance und anderen Services innerhalb der Amazon VPC zu ermöglichen, ohne dass ein Internet-Gateway, ein NAT-Gerät oder eine VPN-Verbi ndung erforderlich ist. Der gesamte Datenverkehr bleibt sicher in der AWS Cloud. Domains, die sich innerhalb einer VPC befinden, verfügen aufgrund ihrer logischen Isolierung im Vergleich zu Domains mit öffentlic hen Endpunkten über eine zusätzliche Sicherheitsebene. Weisen Sie EC2 Amazon-In stances einer Amazon-VPC zu, um den Zugriff ordnungsg emäß zu verwalten.

Kontroll-ID	AWS Config	Empfehlungen
36f	internet-gateway-authorized-vpc-nur	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Internet-Gateways nur mit autorisierter Amazon Virtual Private Cloud (Amazon VPC) verbunden sind. Internet-Gateways ermöglichen den bidirekti onalen Internetzugang zur und von der Amazon VPC, was möglicherweise zu einem unbefugten Zugriff auf Amazon-VPC-Ressourcen führen kann.
36f	lambda-function-public-acce ss-verboten	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherste llen, dass AWS Lambda-Funktionen nicht öffentlich zugänglich sind. Der öffentlic he Zugriff kann möglicher weise die Verfügbarkeit von Ressourcen beeinträchtigen.

Kontroll-ID	AWS Config	Empfehlungen
36f	lambda-inside-vpc	Stellen Sie AWS Lambda-Funktionen in einer Amazon Virtual Private Cloud (Amazon VPC) bereit, um eine sichere Kommunikation zwischen einer Funktion und anderen Diensten innerhalb der Amazon VPC zu gewährleisten. Bei dieser Konfiguration sind kein Internet-Gateway, kein NAT-Gerät und keine VPN-Verbindung erforderlich. Der gesamte Datenverkehr bleibt sicher in der Cloud. AWS Domains, die sich innerhalb einer VPC befinden, verfügen aufgrund ihrer logischen Isolierung im Vergleich zu Domains mit öffentlichen Endpunkten über eine zusätzliche Sicherheitsebene. Um den Zugriff ordnungsgemäß zu verwalten, sollten AWS Lambda-Funktionen einer VPC zugewiesen werden.

Kontroll-ID	AWS Config	Empfehlungen
36f	rds-instance-public-access-überprüfen	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Relational Database Service (Amazon RDS) -Instances nicht öffentlich sind. Amazon-RDS-Datenbank-Instances können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.
36f	rds-snapshots-public-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Relational Database Service (Amazon RDS) -Instances nicht öffentlich sind. Amazon-RDS-Datenbank-Instances können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	AWS Config	Empfehlungen
36f	redshift-cluster-public-access-überprüfen	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Redshift Redshift-Cluster nicht öffentlich sind. Amazon-Redshift-Cluster können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.
36f	s-3 bucket-public-read-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie nur autorisierten Benutzern, Prozessen und Geräten Zugriff auf Amazon Simple Storage Service (Amazon S3) -Buckets gewähren. Die Verwaltung des Zugriffs sollte mit der Klassifizierung der Daten übereinstimmen.
36f	s3- bucket-public-write-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie nur autorisierten Benutzern, Prozessen und Geräten Zugriff auf Amazon Simple Storage Service (Amazon S3) -Buckets gewähren. Die Verwaltung des Zugriffs sollte mit der Klassifizierung der Daten übereinstimmen.

Kontroll-ID	AWS Config	Empfehlungen
36f	sagemaker-notebook-no-direct-Internetzugang	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass SageMaker Amazon-Notebooks keinen direkten Internetzugang zulassen. Indem Sie direkten Internetzugang blockieren, vermeiden Sie, dass unbefugte Benutzer auf sensible Daten zugreifen.
36f	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) Security Groups können bei der Verwaltung des Netzwerkzugriffs helfen, indem sie eine statusbehaftete Filterung von eingehendem und ausgehendem Netzwerkverkehr zu Ressourcen bereitstellen. AWS Wenn Sie eingehenden (oder entfernten) Datenverkehr von 0.0.0.0/0 bis Port 22 auf Ihren Ressourcen nicht zulassen, können Sie den Remote-Zugriff einschränken.

Kontroll-ID	AWS Config	Empfehlungen
36f	restricted-common-ports	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass gemeinsame Ports für Amazon Elastic Compute Cloud (Amazon EC2) - Sicherheitsgruppen eingeschränkt sind. Wenn der Zugriff auf Ports nicht auf vertrauenswürdige Quellen beschränkt wird, kann dies zu Angriffen auf die Verfügbarkeit, Integrität und Vertraulichkeit von Systemen führen. Mit dieser Regel können Sie optional die Parameter blockedPort1–blockedPort5 festlegen (Standardkonfigurationen: 20, 21, 3389, 3306, 4333). Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	AWS Config	Empfehlungen
36f	vpc-default-security-group-geschlossen	Sicherheitsgruppen von Amazon Elastic Compute Cloud (Amazon EC2) können bei der Verwaltung des Netzwerkzugriffs helfen, indem sie eine statusbeh aftete Filterung des ein- und ausgehenden Netzwerkv erkehrs zu Ressourcen bereitstellen. AWS Die Beschränkung des gesamten Datenverkehrs auf die Standardsicherheitsgruppe hilft dabei, den Fernzugriff auf Ihre Ressourcen einzuschr änken. AWS

Kontroll-ID	AWS Config	Empfehlungen
36f	vpc-sg-open-only-to-authorized-ports	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass gemeinsame Ports für Amazon Elastic Compute Cloud (Amazon EC2) - Sicherheitsgruppen eingeschränkt sind. Wenn der Zugriff auf Ports nicht auf vertrauenswürdige Quellen beschränkt wird, kann dies zu Angriffen auf die Verfügbarkeit, Integrität und Vertraulichkeit von Systemen führen. Durch die Beschränkung des Zugriffs auf Ressourcen innerhalb einer Sicherheitsgruppe aus dem Internet (0.0.0.0/0) kann der Fernzugriff auf interne Systeme gesteuert werden.
36f	alb-waf-enabled	Stellen Sie sicher, dass AWS WAF auf Elastic Load Balancers (ELB) aktiviert ist, um Webanwendungen zu schützen. Eine WAF trägt zum Schutz Ihrer Webanwendungen oder APIs vor gängigen Web-Exploits bei. Diese Web-Exploits können sich auf die Verfügbarkeit auswirken, die Sicherheit gefährden oder übermäßige Ressourcen in Ihrer Umgebung verbrauchen.

Kontroll-ID	AWS Config	Empfehlungen
36f	no-unrestricted-route-to-igw	Stellen Sie sicher, dass EC2 Amazon-Routentabellen keine uneingeschränkten Routen zu einem Internet-Gateway enthalten. Durch das Entfernen oder Beschränken des Internetzugangs für Workloads innerhalb von Amazon VPCs können unbeabsichtigte Zugriffe in Ihrer Umgebung reduziert werden.
36f	s3- verboten bucket-level-public-access	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Simple Storage Service (Amazon S3) -Buckets nicht öffentlich zugänglich sind. Diese Regel trägt dazu bei, sensible Daten vor unbefugten Remote-Benutzern zu schützen, indem sie den öffentlichen Zugriff auf Bucket-Ebene verhindert.

Kontroll-ID	AWS Config	Empfehlungen
36f	subnet-auto-assign-public-ip-deaktiviert	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon Virtual Private Cloud (VPC) -Subnetzen nicht automatis ch eine öffentliche IP-Adress e zugewiesen wird. Amazon Elastic Compute Cloud (EC2) -Instances, die in Subnetzen gestartet werden, in denen dieses Attribut aktiviert ist, haben ihrer primären Netzwerkschnittste lle eine öffentliche IP-Adresse zugewiesen.
36f	autoscaling-launch-config-public-ip-deaktiviert	Wenn Sie Ihre Netzwerks chnittstellen mit einer öffentlic hen IP-Adresse konfigurieren, sind die diesen Netzwerks chnittstellen zugehörigen Ressourcen über das Internet erreichbar. EC2 Ressource n sollten nicht öffentlich zugänglich sein, da dies einen unbeabsichtigten Zugriff auf Ihre Anwendungen oder Server ermöglichen kann.

Kontroll-ID	AWS Config	Empfehlungen
36f	redshift-enhanced-vpc-routing-aktiviert	Mit Enhanced-VPC-Routing wird erzwungen, dass der gesamte COPY- und UNLOAD-Datenverkehr zwischen Ihrem Cluster und Datenrepositorys über Ihre Amazon VPC erfolgt. Anschließend können Sie VPC-Features wie Sicherheitsgruppen und Netzwerkzugriffskontrolllisten verwenden, um den Netzwerkverkehr zu schützen. Sie können auch VPC-Flow-Protokolle verwenden, um den Netzwerkverkehr zu überwachen.
36f	api-gw-associated-with-WAF	AWS Mit WAF können Sie eine Reihe von Regeln (als Web Access Control List (Web ACL) bezeichnet) konfigurieren, die Webanfragen auf der Grundlage von anpassbaren Websicherheitsregeln und -bedingungen, die Sie definieren, zulassen, blockieren oder zählen. Stellen Sie sicher, dass Ihre Amazon-API-Gateway-Stufe mit einer WAF-Web-ACL verknüpft ist, um sie vor böswilligen Angriffen zu schützen.

Kontroll-ID	AWS Config	Empfehlungen
36f	s3- -blöcke-periodisch account-level-public-access	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Simple Storage Service (Amazon S3) -Buckets nicht öffentlich zugänglich sind. Diese Regel trägt dazu bei, sensible Daten vor unbefugten Remote-Benutzern zu schützen, indem sie den öffentlichen Zugriff verhindert. Mit dieser Regel können Sie optional die Parameter ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) und restrictPublicBuckets Parameter (Config Default: True) festlegen. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	AWS Config	Empfehlungen
36f	ssm-document-not-public	Stellen Sie sicher, dass AWS Systems Manager (SSM) - Dokumente nicht öffentlich sind, da dies einen unbeabsichtigten Zugriff auf Ihre SSM-Dokumente ermöglichen kann. Ein öffentliches SSM-Dokument kann Informationen über Ihr Konto, Ihre Ressourcen und internen Prozesse preisgeben.
36f	opensearch-in-vpc-only	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass sich Amazon OpenSearch Service-Domains innerhalb einer Amazon Virtual Private Cloud (Amazon VPC) befinden. Eine Amazon OpenSearch Service-Domain innerhalb einer Amazon VPC ermöglicht die sichere Kommunikation zwischen Amazon OpenSearch Service und anderen Services innerhalb der Amazon VPC, ohne dass ein Internet-Gateway, ein NAT-Gerät oder eine VPN-Verbindung erforderlich ist.

Kontroll-ID	AWS Config	Empfehlungen
36g	securityhub-enabled	AWS Security Hub hilft bei der Überwachung von unbefugte m Personal, Verbindungen, Geräten und Software. AWS Security Hub aggregiert, organisiert und priorisiert die Sicherheitswarnungen oder Ergebnisse mehrerer Dienste. AWS Einige dieser Dienste sind Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer und AWS Firewall Manager sowie AWS Partnerlösungen.
36g	guardduty-enabled-centralized	Amazon GuardDuty kann mithilfe von Threat Intellige nce Feeds helfen, potenzielle Cybersicherheitsereignisse zu überwachen und zu erkennen. Dazu gehören Listen mit bösartigen IPs und maschinel len Lernmethoden zur Identifiz ierung unerwarteter, nicht autorisierter und bösartige r Aktivitäten in Ihrer AWS Cloud-Umgebung.

Kontroll-ID	AWS Config	Empfehlungen
36g	guardduty-non-archived-findings	Amazon GuardDuty hilft Ihnen dabei, die Auswirkungen eines Vorfalls zu verstehen, indem es die Ergebnisse nach Schweregrad klassifiziert: niedrig, mittel und hoch. Diese Klassifizierungen können Sie zur Festlegung von entsprechenden Strategien und Prioritäten zur Behebung solcher Vorfälle verwenden. Mit dieser Regel können Sie optional daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7) und daysHighSev (Config Default: 1) für nicht archivierte Ergebnisse festlegen, wie es die Richtlinien Ihrer Organisation erfordern.

Kontroll-ID	AWS Config	Empfehlungen
36h	securityhub-enabled	AWS Security Hub hilft bei der Überwachung von unbefugte m Personal, Verbindungen, Geräten und Software. AWS Security Hub aggregiert, organisiert und priorisiert die Sicherheitswarnungen oder Ergebnisse mehrerer Dienste. AWS Einige dieser Dienste sind Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer und AWS Firewall Manager sowie AWS Partnerlösungen.
36h	guardduty-enabled-centralized	Amazon GuardDuty kann mithilfe von Threat Intellige nce Feeds helfen, potenzielle Cybersicherheitsereignisse zu überwachen und zu erkennen. Dazu gehören Listen mit bösartigen IPs und maschinel len Lernmethoden zur Identifiz ierung unerwarteter, nicht autorisierter und bösartige r Aktivitäten in Ihrer AWS Cloud-Umgebung.

Kontroll-ID	AWS Config	Empfehlungen
36h	guardduty-non-archived-findings	Amazon GuardDuty hilft Ihnen dabei, die Auswirkungen eines Vorfalls zu verstehen, indem es die Ergebnisse nach Schweregrad klassifiziert: niedrig, mittel und hoch. Diese Klassifizierungen können Sie zur Festlegung von entsprechenden Strategien und Prioritäten zur Behebung solcher Vorfälle verwenden. Mit dieser Regel können Sie optional daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7) und daysHighSev (Config Default: 1) für nicht archivierte Ergebnisse festlegen, wie es die Richtlinien Ihrer Organisation erfordern.

Kontroll-ID	AWS Config	Empfehlungen
36h	ec2-manager instance-managed-by-systems	Eine Bestandsaufnahme der Softwareplattformen und Anwendungen innerhalb des Unternehmens ist möglich, indem Amazon Elastic Compute Cloud (Amazon EC2) -Instances mit AWS Systems Manager verwaltet werden. Verwenden Sie AWS Systems Manager, um detaillierte Systemkonfigurationen, Betriebssystem-Patch-Levels, Namen und Typ der Dienste, Softwareinstallationen, Anwendungsname, Herausgeber und Version sowie andere Details zu Ihrer Umgebung bereitzustellen.

Kontroll-ID	AWS Config	Empfehlungen
36h	ec2-check managedinstance-association-compliance-status	Verwenden Sie AWS Systems Manager Associations, um bei der Inventarisierung von Softwareplattformen und Anwendungen innerhalb eines Unternehmens zu helfen. AWS Systems Manager weist Ihren verwalteten Instances einen Konfigurationsstatus zu und ermöglicht es Ihnen, Basiswerte für Betriebss ystem-Patch-Levels, Softwarei nstallationen, Anwendung skonfigurationen und andere Details zu Ihrer Umgebung festzulegen.
36h	ec2-prüfen managedinstance-patch-compliance-status	Aktivieren Sie diese Regel, um bei der Identifizierung und Dokumentation von Sicherhei tslücken in Amazon Elastic Compute Cloud (Amazon EC2) zu helfen. Die Regel prüft, ob die EC2 Amazon-In stance die Patch-Konformität im AWS Systems Manager gemäß den Richtlinien und Verfahren Ihrer Organisation einhält.

Kontroll-ID	AWS Config	Empfehlungen
36h	redshift-cluster-maintenancesettings-check	Diese Regel stellt sicher, dass Amazon-Redshift-Cluster die bevorzugten Einstellungen für Ihre Organisation haben. Insbesondere sorgt sie dafür, dass Cluster bevorzugte Wartungsfenster und automatisierte Aufbewahrungsfristen für Snapshots für die Datenbank haben. Für diese Regel müssen Sie die festlegen allowVersionUpgrade. Der Standardwert ist „true“. Außerdem können Sie optional den Zeitraum preferredMaintenanceWindow (der Standardwert ist sa: 16:00 -sa: 16:30) und den automatedSnapshotRetention Zeitraum (der Standardwert ist 1) festlegen. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	AWS Config	Empfehlungen
36h	elastic-beanstalk-managed-updates-aktiviert	Durch die Aktivierung verwalteter Plattformupdates für eine Amazon-Elastic-Beanstalk-Umgebung wird sichergestellt, dass die aktuellen verfügbaren Plattform-Fixes, -Updates und -Features für die Umgebung installiert sind. Eine bewährte Methode zur Sicherung von Systemen besteht darin, stets die aktuellen Patches zu installieren.
36i	autoscaling-group-elb-healthcheck-erforderlich	Die Elastic Load Balancer (ELB) -Zustandsprüfungen für Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling Scaling-Gruppen unterstützen die Aufrechterhaltung einer angemessenen Kapazität und Verfügbarkeit. Der Load Balancer sendet regelmäßig Pings, versucht Verbindungen herzustellen oder sendet Anfragen, um den Zustand der EC2 Amazon-Instances in einer Gruppe mit auto-scaling zu testen. Wenn eine Instance nicht zurückmeldet, wird der Traffic an eine neue EC2 Amazon-Instance gesendet.

Kontroll-ID	AWS Config	Empfehlungen
36i	cloudwatch-alarm-action-check	Amazon CloudWatch alarmiert, wenn eine Metrik den Schwellenwert für eine bestimmte Anzahl von Bewertungszeiträumen überschreitet. Der Alarm führt eine oder mehrere Aktionen durch, die vom Wert der Metrik oder des Ausdrucks im Vergleich zu einem Schwellenwert in einer Reihe von Zeiträumen abhängt. Diese Regel erfordert einen Wert für alarmActionRequired (Config Default: True), insufficientDataActionRequired (Config Default: True), okActionRequired (Config Default: False). Der tatsächliche Wert muss die Alarmaktionen für Ihre Umgebung widerspiegeln.

Kontroll-ID	AWS Config	Empfehlungen
36i	dynamodb-throughput-limit-check	Aktivieren Sie diese Regel, um sicherzustellen, dass die bereitgestellte Durchsatz kapazität in Ihren Amazon-DynamoDB-Tabellen überprüft wird. Dies ist der Umfang der Lese- und Schreibaktivitäten, der von den jeweiligen Tabellen unterstützt werden kann. DynamoDB verwendet diese Informationen für das Reservieren ausreichender Systemressourcen, um Ihren Durchsatzanforderungen gerecht zu werden. Diese Regel generiert eine Warnung, wenn sich der Durchsatz dem Höchstlimit für ein Kundenkonto nähert. Mit dieser Regel können Sie optional die Parameter RCUThreshold Kontoprozentsatz (Konfigurationsstandard: 80) und WCUThreshold Kontoprozentsatz (Konfigurationsstandard: 80) festlegen. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	AWS Config	Empfehlungen
36i	guardduty-enabled-centralized	Amazon GuardDuty kann mithilfe von Threat Intellige nce Feeds helfen, potenzielle Cybersicherheitsereignisse zu überwachen und zu erkennen. Dazu gehören Listen mit bösartigen IPs und maschinel len Lernmethoden zur Identifiz ierung unerwarteter, nicht autorisierter und bösartige r Aktivitäten in Ihrer AWS Cloud-Umgebung.
36i	lambda-concurrency-check	Diese Regel stellt sicher, dass die Höchst- und Untergrenzen für die Gleichzeitigkeit einer Lambda-Funktion festgelegt werden. Dies kann Sie beim Baselining für die Anzahl der Anforderungen unterstüt zen, die Ihre Funktion zu einem bestimmten Zeitpunkt verarbeitet.
36i	lambda-dlq-check	Aktivieren Sie diese Regel, um das entsprechende Personal über Amazon Simple Queue Service (Amazon SQS) oder Amazon Simple Notification Service (Amazon SNS) zu benachrichtigen, wenn eine Funktion ausgefallen ist.

Kontroll-ID	AWS Config	Empfehlungen
36i	rds-enhanced-monitoring-enabled	Aktivieren Sie Amazon Relational Database Service (Amazon RDS), um die Verfügbarkeit von Amazon RDS zu überwachen. Dies bietet einen detaillierten Einblick in den Zustand Ihrer Amazon-RDS-Datenbank-Instances. Wenn der Amazon-RDS-Speicher mehr als ein zugrunde liegendes physisches Gerät verwendet, erfasst Enhanced Monitoring die Daten für jedes Gerät. Wenn die Datenbank-Instance von Amazon RDS in einer Multi-AZ-Bereitstellung ausgeführt wird, werden außerdem die Daten für jedes Gerät auf dem sekundären Host sowie die Metriken des sekundären Hosts erfasst.

Kontroll-ID	AWS Config	Empfehlungen
36i	opensearch-logs-to-cloudwatch	Stellen Sie sicher, dass für Amazon OpenSearch Service-Domains Fehlerprotokolle aktiviert und zur Aufbewahrung und Beantwortung an Amazon CloudWatch Logs gestreamt werden. OpenSearch Service-Fehlerprotokolle können bei Sicherheits- und Zugriffsprüfungen helfen und bei der Diagnose von Verfügbarkeitsproblemen helfen.
36i	securityhub-enabled	AWS Security Hub hilft bei der Überwachung von unbefugtem Personal, Verbindungen, Geräten und Software. AWS Security Hub aggregiert, organisiert und priorisiert die Sicherheitswarnungen oder Ergebnisse mehrerer Dienste. AWS Einige dieser Dienste sind Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer und AWS Firewall Manager sowie AWS Partnerlösungen.

Kontroll-ID	AWS Config	Empfehlungen
36i	beanstalk-enhanced-health-reporting-aktiviert	AWS Die verbesserte Zustandsberichterstattung von Elastic Beanstalk ermöglicht eine schnellere Reaktion auf Veränderungen im Zustand der zugrunde liegenden Infrastruktur. Diese Änderungen könnten zu einer mangelnden Verfügbarkeit der Anwendung führen. Die erweiterten Zustandsberichte von Elastic Beanstalk bieten eine Statusbeschreibung, um den Schweregrad der identifizierten Probleme einzuschätzen und mögliche Ursachen zu identifizieren, die untersucht werden müssen.
36i	elasticsearch-logs-to-cloudwatch	Stellen Sie sicher, dass für Amazon OpenSearch Service-Domains Fehlerprotokolle aktiviert und zur Aufbewahrung und Beantwortung an Amazon CloudWatch Logs gestreamt werden. Domain-Fehlerprotokolle sind bei Sicherheits- und Zugriffsprüfungen sowie bei der Diagnose von Verfügbarkeitsproblemen nützlich.

Kontroll-ID	AWS Config	Empfehlungen
36j	securityhub-enabled	AWS Security Hub hilft bei der Überwachung von unbefugte m Personal, Verbindungen, Geräten und Software. AWS Security Hub aggregiert, organisiert und priorisiert die Sicherheitswarnungen oder Ergebnisse mehrerer Dienste. AWS Einige dieser Dienste sind Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer und AWS Firewall Manager sowie AWS Partnerlösungen.
36j	guardduty-enabled-centralized	Amazon GuardDuty kann mithilfe von Threat Intellige nce Feeds helfen, potenzielle Cybersicherheitsereignisse zu überwachen und zu erkennen. Dazu gehören Listen mit bösartigen IPs und maschinel len Lernmethoden zur Identifiz ierung unerwarteter, nicht autorisierter und bösartige r Aktivitäten in Ihrer AWS Cloud-Umgebung.

Kontroll-ID	AWS Config	Empfehlungen
36j	guardduty-non-archived-findings	Amazon GuardDuty hilft Ihnen dabei, die Auswirkungen eines Vorfalls zu verstehen, indem es die Ergebnisse nach Schweregrad klassifiziert: niedrig, mittel und hoch. Diese Klassifizierungen können Sie zur Festlegung von entsprechenden Strategien und Prioritäten zur Behebung solcher Vorfälle verwenden. Mit dieser Regel können Sie optional daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7) und daysHighSev (Config Default: 1) für nicht archivierte Ergebnisse festlegen, wie es die Richtlinien Ihrer Organisation erfordern.
36j	opensearch-logs-to-cloudwatch	Stellen Sie sicher, dass für Amazon OpenSearch Service-Domains Fehlerprotokolle aktiviert und zur Aufbewahrung und Beantwortung an Amazon CloudWatch Logs gestreamt werden. OpenSearch Service-Fehlerprotokolle können bei Sicherheits- und Zugriffsprüfungen helfen und bei der Diagnose von Verfügbarkeitsproblemen helfen.

Kontroll-ID	AWS Config	Empfehlungen
36j	autoscaling-group-elb-healthcheck-erforderlich	Die Elastic Load Balancer (ELB) -Zustandsprüfungen für Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling Scaling-Gruppen unterstützen die Aufrechterhaltung einer angemessenen Kapazität und Verfügbarkeit. Der Load Balancer sendet regelmäßig Pings, versucht Verbindungen herzustellen oder sendet Anfragen, um den Zustand der EC2 Amazon-Instances in einer Gruppe mit auto-scaling zu testen. Wenn eine Instance nicht zurückmeldet, wird der Traffic an eine neue EC2 Amazon-Instance gesendet.

Kontroll-ID	AWS Config	Empfehlungen
36j	cloudwatch-alarm-action-check	Amazon CloudWatch alarmiert, wenn eine Metrik den Schwellenwert für eine bestimmte Anzahl von Bewertungszeiträumen überschreitet. Der Alarm führt eine oder mehrere Aktionen durch, die vom Wert der Metrik oder des Ausdrucks im Vergleich zu einem Schwellenwert in einer Reihe von Zeiträumen abhängt. Diese Regel erfordert einen Wert für alarmActionRequired (Config Default: True), insufficientDataActionRequired (Config Default: True), okActionRequired (Config Default: False). Der tatsächliche Wert muss die Alarmaktionen für Ihre Umgebung widerspiegeln.

Kontroll-ID	AWS Config	Empfehlungen
36j	dynamodb-throughput-limit-check	Aktivieren Sie diese Regel, um sicherzustellen, dass die bereitgestellte Durchsatz kapazität in Ihren Amazon-DynamoDB-Tabellen überprüft wird. Dies ist der Umfang der Lese- und Schreibaktivitäten, der von den jeweiligen Tabellen unterstützt werden kann. DynamoDB verwendet diese Informationen für das Reservieren ausreichender Systemressourcen, um Ihren Durchsatzanforderungen gerecht zu werden. Diese Regel generiert eine Warnung, wenn sich der Durchsatz dem Höchstlimit für ein Kundenkonto nähert. Mit dieser Regel können Sie optional die Parameter RCUThreshold Kontoprozentsatz (Konfigurationsstandard: 80) und WCUThreshold Kontoprozentsatz (Konfigurationsstandard: 80) festlegen. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	AWS Config	Empfehlungen
36j	lambda-dlq-check	Aktivieren Sie diese Regel, um das entsprechende Personal über Amazon Simple Queue Service (Amazon SQS) oder Amazon Simple Notification Service (Amazon SNS) zu benachrichtigen, wenn eine Funktion ausgefallen ist.
36j	rds-enhanced-monitoring-enabled	Aktivieren Sie Amazon Relational Database Service (Amazon RDS), um die Verfügbarkeit von Amazon RDS zu überwachen. Dies bietet einen detaillierten Einblick in den Zustand Ihrer Amazon-RDS-Datenbank-Instances. Wenn der Amazon-RDS-Speicher mehr als ein zugrunde liegendes physisches Gerät verwendet, erfasst Enhanced Monitoring die Daten für jedes Gerät. Wenn die Datenbank-Instance von Amazon RDS in einer Multi-AZ-Bereitstellung ausgeführt wird, werden außerdem die Daten für jedes Gerät auf dem sekundären Host sowie die Metriken des sekundären Hosts erfasst.

Kontroll-ID	AWS Config	Empfehlungen
36j	beanstalk-enhanced-health-reporting-aktiviert	AWS Die verbesserte Zustandsberichterstattung von Elastic Beanstalk ermöglicht eine schnellere Reaktion auf Veränderungen im Zustand der zugrunde liegenden Infrastruktur. Diese Änderungen könnten zu einer mangelnden Verfügbarkeit der Anwendung führen. Die erweiterten Zustandsberichte von Elastic Beanstalk bieten eine Statusbeschreibung, um den Schweregrad der identifizierten Probleme einzuschätzen und mögliche Ursachen zu identifizieren, die untersucht werden müssen.
36j	elasticsearch-logs-to-cloudwatch	Stellen Sie sicher, dass für Amazon OpenSearch Service-Domains Fehlerprotokolle aktiviert und zur Aufbewahrung und Beantwortung an Amazon CloudWatch Logs gestreamt werden. Domain-Fehlerprotokolle sind bei Sicherheits- und Zugriffsprüfungen sowie bei der Diagnose von Verfügbarkeitsproblemen nützlich.

Kontroll-ID	AWS Config	Empfehlungen
36l	db-instance-backup-enabled	Die Sicherungsfunktion von Amazon RDS erstellt Sicherungen Ihrer Datenbanken und Transaktionsprotokolle. Amazon RDS erstellt einen Snapshot für das Speichervolume Ihrer DB-Instance, sodass die gesamte DB-Instance gesichert wird. Sie können im System spezifische Aufbewahrungsfristen festlegen, um Ihre Ausfallsicherheitsanforderungen zu erfüllen.
36l	dynamodb-autoscaling-enabled	Amazon DynamoDB Auto Scaling verwendet den AWS Application Auto Scaling-Service, um die bereitgestellte Durchsatzkapazität so anzupassen, dass sie automatisch auf tatsächliche Verkehrsmuster reagiert. Auf diese Weise kann eine Tabelle oder ein globaler sekundärer Index die bereitgestellte Lese-/Schreibkapazität erhöhen, um plötzliche Erhöhungen des Datenverkehrs ohne Drosselung zu bewältigen.

Kontroll-ID	AWS Config	Empfehlungen
36l	dynamodb-pitr-enabled	Aktivieren Sie diese Regel, um zu überprüfen, ob die Informationen gesichert wurden. Es verwaltet auch die Backups, indem es sicherstellt, dass die point-in-time Wiederherstellung in Amazon DynamoDB aktiviert ist. Bei der Wiederherstellung werden fortlaufende Backups Ihrer Tabelle für die letzten 35 Tage gespeichert.
36l	elasticache-redis-cluster-automatic-Backup-Prüfung	Wenn automatische Backups aktiviert sind, ElastiCache erstellt Amazon täglich ein Backup des Clusters. Die Sicherung kann für eine von Ihrer Organisation festgelegte Anzahl von Tagen aufbewahrt werden. Automatische Backups schützen vor Datenverlust. Bei einem Ausfall können Sie einen neuen Cluster erstellen, der Ihre Daten aus dem aktuellen Backup wiederherstellt.

Kontroll-ID	AWS Config	Empfehlungen
36l	elb-deletion-protection-enabled	Diese Regel sorgt dafür, dass der Löschschutz für Elastic Load Balancing aktiviert ist. Verwenden Sie diese Funktion, um zu verhindern, dass Ihr Load Balancer versehentlich oder böswillig gelöscht wird, was zum Verlust der Verfügbarkeit Ihrer Anwendungen führen kann.

Kontroll-ID	AWS Config	Empfehlungen
36l	rds-multi-az-support	Die Multi-AZ-Unterstützung in Amazon Relational Database Service (Amazon RDS) bietet eine verbesserte Verfügbar keit und Beständigkeit von Datenbank-Instances. Wenn Sie eine Multi-AZ-Datenbank-Instance bereitstellen, erstellt Amazon RDS automatisch eine primäre Datenbank-Instance und repliziert die Daten synchron auf eine Standby-Instance in einer anderen Availability Zone. Jede Availability Zone läuft auf einer eigenen, physisch getrennten, unabhängigen Infrastruktur und ist auf eine hohe Verfügbarkeit ausgelegt . Im Falle eines Infrastru kturausfalls führt Amazon RDS einen automatischen Failover zum Standby-Modus durch, sodass Sie den Datenbank betrieb wieder aufnehmen können, sobald der Failover abgeschlossen ist.

Kontroll-ID	AWS Config	Empfehlungen
36l	rds-cluster-multi-az-aktiviert	Die Multi-AZ-Unterstützung in Amazon Relational Database Service (Amazon RDS) bietet eine verbesserte Verfügbar keit und Beständigkeit von Datenbank-Instances. Wenn Sie eine Multi-AZ-Datenbank-Instance bereitstellen, erstellt Amazon RDS automatisch eine primäre Datenbank-Instance und repliziert die Daten synchron auf eine Standby-Instance in einer anderen Availability Zone. Jede Availability Zone läuft auf einer eigenen, physisch getrennten, unabhängigen Infrastruktur und ist auf eine hohe Verfügbarkeit ausgelegt . Im Falle eines Infrastru kturausfalls führt Amazon RDS einen automatischen Failover zum Standby-Modus durch, sodass Sie den Datenbank betrieb wieder aufnehmen können, sobald der Failover abgeschlossen ist.

Kontroll-ID	AWS Config	Empfehlungen
36l	s3- bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) unterstützt die Aufrechte rhaltung einer angemessenen Kapazität und Verfügbarkeit. CRR ermöglicht das automatis che, asynchrone Kopieren von Objekten in Amazon-S3 -Buckets, um die Datenverf ügbarkeit sicherzustellen.
36l	vpc-vpn-2-tunnels-up	Redundante Site-to-Site VPN-Tunnel können implement iert werden, um die Anforderu ngen an die Ausfallsicherheit zu erfüllen. Es verwendet zwei Tunnel, um die Konnektiv ität sicherzustellen, falls eine der Site-to-Site VPN-Verbi ndungen nicht verfügbar ist. Um sich vor einem Verbindun gsverlust zu schützen, können Sie für den Fall, dass Ihr Kunden-Gateway nicht verfügbar ist, eine zweite Site-to-Site VPN-Verbindung zu Ihrer Amazon Virtual Private Cloud (Amazon VPC) und Ihrem Virtual Private Gateway einrichten, indem Sie ein zweites Kunden-Gateway verwenden.

Kontroll-ID	AWS Config	Empfehlungen
36l	dynamodb-in-backup-plan	Um Sie bei Datensich erungsprozessen zu unterstüt zen, stellen Sie sicher, dass Ihre Amazon DynamoDB-Tabellen Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherung smanagement und erleichte rt Ihnen die Erfüllung von geschäftlichen und behördlic hen Compliance-Anforde rungen hinsichtlich Datensich erungen.
36l	ebs-in-backup-plan	Stellen Sie zur Unterstützung der Datensicherungsprozesse sicher, dass Ihre Amazon Elastic Block Store (Amazon EBS) -Volumes Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihre Backup-Ve rwaltung und ermöglicht es Ihnen, Ihre geschäftlichen und behördlichen Anforderungen bezüglich Backups zu erfüllen.

Kontroll-ID	AWS Config	Empfehlungen
36l	efs-in-backup-plan	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon Elastic File System (Amazon EFS) - Dateisysteme Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	AWS Config	Empfehlungen
36l	elb-cross-zone-load-Balancing aktiviert	Aktivieren Sie zonenüber greifendes Load Balancing für Ihre Elastic Load Balancer (ELBs), um eine angemesse ne Kapazität und Verfügbar keit aufrechtzuerhalten. Zonenübergreifendes Load Balancing reduziert die Notwendigkeit, die gleiche Anzahl von Instances in jeder aktivierten Availability Zone aufrechtzuerhalten. Dadurch wird auch die Fähigkeit Ihrer Anwendung verbessert, den Verlust einer oder mehrerer Instances zu bewältigen.
36l	rds-instance-deletion-prote ction-aktiviert	Stellen Sie sicher, dass Amazon Relational Database Service (Amazon RDS)-Instances den Löschschutz aktiviert haben. Verwenden Sie den Löschschutz, um zu verhindern, dass Ihre Amazon-RDS-Instances versehentlich oder böswillig gelöscht werden, was zum Verlust der Verfügbarkeit Ihrer Anwendungen führen kann.

Kontroll-ID	AWS Config	Empfehlungen
36l	rds-in-backup-plan	Um Sie bei Datensich erungsprozessen zu unterstüt zen, stellen Sie sicher, dass Ihre Amazon Relational Database Service (Amazon RDS) -Instances Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherung smanagement und erleichte rt Ihnen die Erfüllung von geschäftlichen und behördlic hen Compliance-Anforde rungen hinsichtlich Datensich erungen.

Kontroll-ID	AWS Config	Empfehlungen
36l	redshift-backup-enabled	Stellen Sie zur Unterstützung der Datensicherungsprozesse sicher, dass Ihre Amazon-Redshift-Cluster über automatisierte Snapshots verfügen. Wenn automatisierte Snapshots für einen Cluster aktiviert sind, erstellt Redshift in regelmäßigen Abständen Snapshots dieses Clusters. Standardmäßig erstellt Redshift alle acht Stunden oder alle 5 GB einen Snapshot für jeden Knoten mit Datenänderungen oder je nachdem, was zuerst eintritt.

Kontroll-ID	AWS Config	Empfehlungen
36l	beanstalk-enhanced-health-reporting-aktiviert	AWS Die verbesserte Zustandsberichterstattung von Elastic Beanstalk ermöglicht eine schnellere Reaktion auf Veränderungen im Zustand der zugrunde liegenden Infrastruktur. Diese Änderungen könnten zu einer mangelnden Verfügbarkeit der Anwendung führen. Die erweiterten Zustandsberichte von Elastic Beanstalk bieten eine Statusbeschreibung, um den Schweregrad der identifizierten Probleme einzuschätzen und mögliche Ursachen zu identifizieren, die untersucht werden müssen.
39(a)(b)(d)	guardduty-enabled-centralized	Amazon GuardDuty kann mithilfe von Threat Intelligence Feeds helfen, potenzielle Cybersicherheitsereignisse zu überwachen und zu erkennen. Dazu gehören Listen mit bösartigen IPs und maschinellen Lernmethoden zur Identifizierung unerwarteter, nicht autorisierter und bösartiger Aktivitäten in Ihrer AWS Cloud-Umgebung.

Kontroll-ID	AWS Config	Empfehlungen
39(a)(b)(d)	guardduty-non-archived-findings	Amazon GuardDuty hilft Ihnen dabei, die Auswirkungen eines Vorfalls zu verstehen, indem es die Ergebnisse nach Schweregrad klassifiziert: niedrig, mittel und hoch. Diese Klassifizierungen können Sie zur Festlegung von entsprechenden Strategien und Prioritäten zur Behebung solcher Vorfälle verwenden. Mit dieser Regel können Sie optional daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7) und daysHighSev (Config Default: 1) für nicht archivierte Ergebnisse festlegen, wie es die Richtlinien Ihrer Organisation erfordern.

Kontroll-ID	AWS Config	Empfehlungen
39(a)(b)(d)	securityhub-enabled	AWS Security Hub hilft bei der Überwachung von unbefugte m Personal, Verbindungen, Geräten und Software. AWS Security Hub aggregiert, organisiert und priorisiert die Sicherheitswarnungen oder Ergebnisse mehrerer Dienste. AWS Einige dieser Dienste sind Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer und AWS Firewall Manager sowie AWS Partnerlösungen.
40	ec2-prüfen managedinstance-patch-compliance-status	Aktivieren Sie diese Regel, um bei der Identifizierung und Dokumentation von Sicherhei tslücken in Amazon Elastic Compute Cloud (Amazon EC2) zu helfen. Die Regel prüft, ob die EC2 Amazon-In stance die Patch-Konformität im AWS Systems Manager gemäß den Richtlinien und Verfahren Ihrer Organisation einhält.

Kontroll-ID	AWS Config	Empfehlungen
40	redshift-cluster-maintenancesettings-check	Diese Regel stellt sicher, dass Amazon-Redshift-Cluster die bevorzugten Einstellungen für Ihre Organisation haben. Insbesondere sorgt sie dafür, dass Cluster bevorzugte Wartungsfenster und automatisierte Aufbewahrungsfristen für Snapshots für die Datenbank haben. Für diese Regel müssen Sie die festlegen allowVersionUpgrade. Der Standardwert ist „true“. Außerdem können Sie optional den Zeitraum preferredMaintenanceWindow (der Standardwert ist sa: 16:00 -sa: 16:30) und den automatedSnapshotRetention Zeitraum (der Standardwert ist 1) festlegen. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	AWS Config	Empfehlungen
40	elastic-beanstalk-managed-updates-aktiviert	Durch die Aktivierung verwalteter Plattformupdates für eine Amazon-Elastic-Beanstalk-Umgebung wird sichergestellt, dass die aktuellen verfügbaren Plattform-Fixes, -Updates und -Features für die Umgebung installiert sind. Eine bewährte Methode zur Sicherung von Systemen besteht darin, stets die aktuellen Patches zu installieren.
40	rds-automatic-minor-version-upgrade-fähig	Aktivieren Sie automatische Unterversions-Upgrades auf Ihren Amazon Relational Database Service (RDS)-Instances, um sicherzustellen, dass die aktuellen Updates für Unterversionen von Relational Database Management System (RDBMS) installiert sind, die Sicherheitspatches und Bugfixes enthalten können.

Kontroll-ID	AWS Config	Empfehlungen
44a	iam-root-access-key-überprüfen	Der Zugriff auf Systeme und Ressourcen kann gesteuert werden, indem überprüft wird, ob der Root-Benutzer keine Zugriffsschlüssel mit seiner AWS Identity and Access Management (IAM) -Rolle verknüpft hat. Stellen Sie sicher, dass die Root-Zugriffsschlüssel gelöscht werden. Erstellen und verwenden Sie stattdessen rollenbasierte Funktionen, AWS-Konten um das Prinzip der geringsten Funktionalität zu berücksichtigen.
44a	root-account-hardware-mfa-aktiviert	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Hardware-MFA für den Root-Benutzer aktiviert ist. Der Stammbenutzer ist der AWS-Konto-Benutzer mit den meisten Berechtigungen. MFA sorgt für eine weitere Schutzebene zusätzlich zu den Anmeldeinformationen. Indem Sie MFA für den Root-Benutzer vorschreiben, können Sie die Anzahl AWS-Konten kompromittierter Benutzer reduzieren.

Kontroll-ID	AWS Config	Empfehlungen
44a	root-account-mfa-enabled	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass MFA für den Root-Benutzer aktiviert ist. Der Stammbenutzer ist der AWS-Konto-Benutzer mit den meisten Berechtigungen. MFA bietet eine weitere Schutzebene zusätzlich zum Benutzernamen und Passwort. Indem Sie MFA für den Root-Benutzer vorschreiben, können Sie die Anzahl AWS-Konten kompromittierter Benutzer reduzieren.
44b	rds-instance-deletion-protection-aktiviert	Stellen Sie sicher, dass Amazon Relational Database Service (Amazon RDS)-Instances den Löschschutz aktiviert haben. Verwenden Sie den Löschschutz, um zu verhindern, dass Ihre Amazon-RDS-Instances versehentlich oder böswillig gelöscht werden, was zum Verlust der Verfügbarkeit Ihrer Anwendungen führen kann.

Kontroll-ID	AWS Config	Empfehlungen
44b	s3- bucket-versioning-enabled	Die Versionsverwaltung von Amazon Simple Storage Service (Amazon S3)-Buckets hilft dabei, mehrere Varianten eines Objekts im selben Amazon-S3-Bucket zu speichern. Verwenden Sie die Versionsverwaltung, um sämtliche Versionen aller Objekte in Ihrem Amazon-S3-Bucket zu speichern, abzurufen oder wiederher zustellen. Mit der Versionsv erwaltung können Sie Versionen sowohl nach unbeabsichtigten Benutzera ktionen als auch nach Anwendungsfehlern problemlo s wiederherstellen.
44b	elb-deletion-protection-ena bled	Diese Regel sorgt dafür, dass der Löschschutz für Elastic Load Balancing aktiviert ist. Verwenden Sie diese Funktion, um zu verhinder n, dass Ihr Load Balancer versehentlich oder böswillig gelöscht wird, was zum Verlust der Verfügbarkeit Ihrer Anwendungen führen kann.

Kontroll-ID	AWS Config	Empfehlungen
44c	kms-cmk-not-scheduled-zum Löschen	Um Daten im Ruhezustand zu schützen, sollten Sie sicherstellen, dass die für den Kunden erforderlichen Masterschlüssel (CMKs) nicht für das Löschen im AWS Key Management Service (AWS KMS) vorgesehen sind. Da Schlüssel manchmal gelöscht werden müssen, können Sie mit dieser Regel alle zu löschenden Schlüssel überprüfen, falls ein Schlüssel versehentlich zur Löschung vorgemerkt wurde.
44c	iam-root-access-key-überprüfen	Der Zugriff auf Systeme und Ressourcen kann gesteuert werden, indem überprüft wird, ob der Root-Benutzer keine Zugriffsschlüssel mit seiner AWS Identity and Access Management (IAM) -Rolle verknüpft hat. Stellen Sie sicher, dass die Root-Zugriffsschlüssel gelöscht werden. Erstellen und verwenden Sie stattdessen rollenbasierte Funktionen, AWS-Konten um das Prinzip der geringsten Funktionalität zu berücksichtigen.

Kontroll-ID	AWS Config	Empfehlungen
44c	iam-customer-policy-blocked-kms-Aktionen	AWS Identity and Access Management (IAM) kann Ihnen helfen, die Prinzipien der geringsten Rechte und der Aufgabentrennung in Zugriffsberechtigungen und Autorisierungen zu integrier en und so zu verhindern, dass Richtlinien blockierte Aktionen für alle AWS Schlüssel des Key Management Service enthalten. Wenn Benutzer mehr Rechte haben, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtig ung und Aufgabentrennung verstoßen. Mit dieser Regel können Sie den Parameter festlegen. blockedActionsPatt erns (Wert „AWS Bewährte grundlegende Sicherhei tsmethoden“: kms: Decrypt, kms:ReEncryptFrom). Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisat ion entsprechen.

Kontroll-ID	AWS Config	Empfehlungen
44c	iam-inline-policy-blocked-kms-Aktionen	Stellen Sie sicher, dass ein Benutzer, eine IAM-Rolle oder eine IAM-Grupp e (AWS Identity and Access Management) nicht über eine Inline-Richtlinie verfügt, die blockierte Aktionen für alle AWS Schlüssel des Key Management Service zulässt. AWS empfiehlt, verwaltete Richtlinien anstelle von Inline-Richtlinien zu verwenden . Verwaltete Richtlinien ermöglichen Wiederver wendbarkeit, Versionsv erwaltung, Rollback und Delegierung der Berechtig ungsverwaltung. Mit dieser Regel können Sie den blockedActionsPatterns Parameter festlegen. (Wert „AWS Bewährte grundlege nde Sicherheitsmethoden“: kms: Decrypt, kms:ReEnc ryptFrom). Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprech en.

Kontroll-ID	AWS Config	Empfehlungen
45	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) kann Ihnen dabei helfen, die Prinzipien der geringsten Rechte und der Aufgabent rennung in Zugriffsberechtigu ngen und Autorisierungen zu integrieren und so zu verhindern, dass Richtlinien „Effect“: „Allow“ mit „Action“: „*“ anstelle von „Resource“: „*“ enthalten. Wenn Benutzern mehr Rechte eingeräumt werden, als für die Ausführun g einer Aufgabe erforderl ich sind, kann dies gegen das Prinzip der geringste n Berechtigung und der Aufgabentrennung verstoßen.

Kontroll-ID	AWS Config	Empfehlungen
45	iam-root-access-key-überprüfen	Der Zugriff auf Systeme und Ressourcen kann gesteuert werden, indem überprüft wird, ob der Root-Benutzer keine Zugriffsschlüssel mit seiner AWS Identity and Access Management (IAM) -Rolle verknüpft hat. Stellen Sie sicher, dass die Root-Zugriffsschlüssel gelöscht werden. Erstellen und verwenden Sie stattdessen rollenbasierte Funktionen, AWS-Konten um das Prinzip der geringsten Funktionalität zu berücksichtigen.
45	iam-user-group-membership-überprüfen	AWS Identity and Access Management (IAM) kann Ihnen helfen, Zugriffsberechtigungen und Autorisierungen einzuschränken, indem sichergestellt wird, dass Benutzer Mitglieder mindestens einer Gruppe sind. Wenn Benutzern mehr Berechtigungen eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und Aufgabentrennung verstoßen.

Kontroll-ID	AWS Config	Empfehlungen
45	iam-user-mfa-enabled	Aktivieren Sie diese Regel, um den Zugriff auf Ressourcen in der AWS -Cloud einzuschränken. Diese Regel stellt sicher, dass die Multi-Faktor-Authentifizierung (MFA) für alle Benutzer aktiviert ist. MFA bietet eine weitere Schutzebene zusätzlich zum Benutzernamen und Passwort. Reduzieren Sie Fälle von kompromittierten Konten, indem Sie MFA für Benutzer vorschreiben.
45	iam-user-no-policies-überprüfen	Diese Regel stellt sicher, dass AWS Identity and Access Management (IAM) -Richtlinien nur Gruppen oder Rollen zugewiesen werden, um den Zugriff auf Systeme und Ressourcen zu kontrollieren. Die Zuweisung von Berechtigungen auf Gruppen- oder Rollenebene trägt dazu bei, die Wahrscheinlichkeit zu verringern, dass eine Identität übermäßige Berechtigungen erhält oder beibehält.

Kontroll-ID	AWS Config	Empfehlungen
45	iam-user-unused-credentials-überprüfen	AWS Identity and Access Management (IAM) kann Ihnen bei Zugriffsberechtigungen und Autorisierungen helfen, indem es nach IAM-Passwörtern und Zugriffsschlüsseln sucht, die für einen bestimmten Zeitraum nicht verwendet wurden. Wenn ungenutzte Anmeldeinformationen identifiziert werden, müssen Sie sie deaktivieren und/oder entfernen, da dies gegen das Prinzip der geringsten Berechtigung verstoßen könnte. Für diese Regel müssen Sie einen Wert für das maxCredentialUsage Alter festlegen (Standardkonfiguration: 90). Der tatsächliche Wert muss den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	AWS Config	Empfehlungen
45	mfa-enabled-for-iam-Konsolenzugriff	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass MFA für alle AWS Identity and Access Management (IAM) -Benutzer aktiviert ist, die über ein Konsolenkennwort verfügen. MFA sorgt für eine weitere Schutzebene zusätzlich zu den Anmeldeinformationen. Indem Sie MFA für Benutzer vorschreiben, können Sie Fälle kompromittierter Konten reduzieren und verhindern, dass unbefugte Benutzer auf vertrauliche Daten zugreifen.
45	root-account-hardware-mfa-aktiviert	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Hardware-MFA für den Root-Benutzer aktiviert ist. Der Stammbenutzer ist der AWS-Konto-Benutzer mit den meisten Berechtigungen. MFA sorgt für eine weitere Schutzebene zusätzlich zu den Anmeldeinformationen. Indem Sie MFA für den Root-Benutzer vorschreiben, können Sie die Anzahl AWS-Konten kompromittierter Benutzer reduzieren.

Kontroll-ID	AWS Config	Empfehlungen
45	root-account-mfa-enabled	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass MFA für den Root-Benutzer aktiviert ist. Der Stammbenutzer ist der AWS-Konto-Benutzer mit den meisten Berechtigungen. MFA bietet eine weitere Schutzebene zusätzlich zum Benutzernamen und Passwort. Indem Sie MFA für den Root-Benutzer vorschreiben, können Sie die Anzahl AWS-Konten kompromittierter Benutzer reduzieren.

Kontroll-ID	AWS Config	Empfehlungen
45	emr-kerberos-enabled	Die Zugriffsberechtigungen und -autorisierungen können verwaltet und nach den Prinzipien der geringsten Berechtigung und Aufgabent rennung integriert werden, indem Kerberos für Amazon-EMR-Cluster aktiviert wird. In Kerberos werden Services und Benutzer, die sich authentifizieren müssen, als Prinzipale bezeichnet. Prinzipale befinden sich in einem Kerberos-Bereich. Innerhalb dieses Bereichs wird ein Kerberos-Server als Key Distribution Center (KDC) bezeichnet. Über diesen Server können sich Prinzipale authentifizieren. Die Authentifizierung im KDC erfolgt durch die Ausstellu ng von Authentifizierungs tickets. Das KDC unterhält eine Datenbank der Prinzipal e in seinem Bereich mit ihren Passwörtern und anderen administrativen Informationen zu jedem Prinzipal.

Kontroll-ID	AWS Config	Empfehlungen
45	iam-no-inline-policy-überprüfen	Stellen Sie sicher, dass ein Benutzer, eine IAM-Rolle oder eine IAM-Gruppe (AWS Identity and Access Management) nicht über eine Inline-Richtlinie zur Zugriffskontrolle auf Systeme und Ressourcen verfügt. AWS empfiehlt, verwaltete Richtlinien anstelle von Inline-Richtlinien zu verwenden . Verwaltete Richtlinien ermöglichen Wiederverwendbarkeit, Versionsverwaltung, Rollback und Delegierung der Berechtigungsverwaltung.
45	dms-replication-not-public	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass auf DMS-Replikationsinstanzen nicht öffentlich zugegriffen werden kann. DMS-Replikations-Instances können vertrauliche Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	AWS Config	Empfehlungen
45	ebs-snapshot-public-restorable-überprüfen	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass EBS-Snapshots nicht öffentlich wiederherstellbar sind. EBS-Volume-Snapshots können vertrauliche Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.
45	ec-2 instance-no-public-ip	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon Elastic Compute Cloud (Amazon EC2) -Instances nicht öffentlich zugänglich sind. EC2Amazon-Instances können vertrauliche Informationen enthalten, und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	AWS Config	Empfehlungen
45	elasticsearch-in-vpc-only	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass sich Amazon OpenSearch OpenSearch Service (Service) -Domains innerhalb einer Amazon Virtual Private Cloud (Amazon VPC) befinden. Eine OpenSearch Service-Domain innerhalb einer Amazon VPC ermöglicht die sichere Kommunikation zwischen OpenSearch Service und anderen Services innerhalb der Amazon VPC, ohne dass ein Internet-Gateway, ein NAT-Gerät oder eine VPN-Verbindung erforderlich ist.
45	emr-master-no-public-ip	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon EMR-Cluster-Masterknoten nicht öffentlich zugänglich sind. Amazon-EMR-Cluster-Hauptknoten können vertrauliche Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	AWS Config	Empfehlungen
45	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) Security Groups können bei der Verwaltung des Netzwerkz ugriffs helfen, indem sie eine statusbehaftete Filterung von eingehendem und ausgehend em Netzwerkverkehr zu Ressourcen bereitstellen. AWS Wenn Sie eingehenden (oder entfernten) Datenverk ehr von 0.0.0.0/0 bis Port 22 auf Ihren Ressourcen nicht zulassen, können Sie den Remote-Zugriff einschränken.

Kontroll-ID	AWS Config	Empfehlungen
45	ec-2 instances-in-vpc	Stellen Sie Amazon Elastic Compute Cloud (Amazon EC2) -Instances innerhalb einer Amazon Virtual Private Cloud (Amazon VPC) bereit, um eine sichere Kommunika tion zwischen einer Instance und anderen Services innerhalb der Amazon VPC zu ermöglichen, ohne dass ein Internet-Gateway, ein NAT-Gerät oder eine VPN-Verbi ndung erforderlich ist. Der gesamte Datenverkehr bleibt sicher in der AWS Cloud. Domains, die sich innerhalb einer VPC befinden, verfügen aufgrund ihrer logischen Isolierung im Vergleich zu Domains mit öffentlic hen Endpunkten über eine zusätzliche Sicherheitsebene. Weisen Sie EC2 Amazon-In stances einer Amazon-VPC zu, um den Zugriff ordnungsg emäß zu verwalten.

Kontroll-ID	AWS Config	Empfehlungen
45	internet-gateway-authorized-vpc-nur	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Internet-Gateways nur mit autorisierter Amazon Virtual Private Cloud (Amazon VPC) verbunden sind. Internet-Gateways ermöglichen den bidirekti onalen Internetzugang zur und von der Amazon VPC, was möglicherweise zu einem unbefugten Zugriff auf Amazon-VPC-Ressourcen führen kann.
45	lambda-function-public-acce ss-verboten	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherste llen, dass AWS Lambda-Funktionen nicht öffentlich zugänglich sind. Der öffentlic he Zugriff kann möglicher weise die Verfügbarkeit von Ressourcen beeinträchtigen.

Kontroll-ID	AWS Config	Empfehlungen
45	lambda-inside-vpc	Stellen Sie AWS Lambda-Funktionen in einer Amazon Virtual Private Cloud (Amazon VPC) bereit, um eine sichere Kommunikation zwischen einer Funktion und anderen Diensten innerhalb der Amazon VPC zu gewährleisten. Bei dieser Konfiguration sind kein Internet-Gateway, kein NAT-Gerät und keine VPN-Verbindung erforderlich. Der gesamte Datenverkehr bleibt sicher in der Cloud. AWS Domains, die sich innerhalb einer VPC befinden, verfügen aufgrund ihrer logischen Isolierung im Vergleich zu Domains mit öffentlichen Endpunkten über eine zusätzliche Sicherheitsebene. Um den Zugriff ordnungsgemäß zu verwalten, sollten AWS Lambda-Funktionen einer VPC zugewiesen werden.

Kontroll-ID	AWS Config	Empfehlungen
45	rds-instance-public-access-überprüfen	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Relational Database Service (Amazon RDS) -Instances nicht öffentlich sind. Amazon-RDS-Datenbank-Instances können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.
45	rds-snapshots-public-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Relational Database Service (Amazon RDS) -Instances nicht öffentlich sind. Amazon-RDS-Datenbank-Instances können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	AWS Config	Empfehlungen
45	redshift-cluster-public-access-überprüfen	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Redshift Redshift-Cluster nicht öffentlich sind. Amazon-Redshift-Cluster können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.
45	restricted-common-ports	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass gemeinsame Ports für Amazon Elastic Compute Cloud (Amazon EC2) - Sicherheitsgruppen eingeschränkt sind. Wenn der Zugriff auf Ports nicht auf vertrauenswürdige Quellen beschränkt wird, kann dies zu Angriffen auf die Verfügbarkeit, Integrität und Vertraulichkeit von Systemen führen. Mit dieser Regel können Sie optional die Parameter blockedPort1–blockedPort5 festlegen (Standardkonfigurationen: 20, 21, 3389, 3306, 4333). Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	AWS Config	Empfehlungen
45	s-3 bucket-public-read-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie nur autorisierten Benutzern, Prozessen und Geräten Zugriff auf Amazon Simple Storage Service (Amazon S3) -Buckets gewähren. Die Verwaltung des Zugriffs sollte mit der Klassifizierung der Daten übereinstimmen.
45	s3- bucket-public-write-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie nur autorisierten Benutzern, Prozessen und Geräten Zugriff auf Amazon Simple Storage Service (Amazon S3) -Buckets gewähren. Die Verwaltung des Zugriffs sollte mit der Klassifizierung der Daten übereinstimmen.
45	sagemaker-notebook-no-direct-Internetzugang	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass SageMaker Amazon-Notebooks keinen direkten Internetzugang zulassen. Indem Sie direkten Internetzugang blockieren, vermeiden Sie, dass unbefugte Benutzer auf sensible Daten zugreifen.

Kontroll-ID	AWS Config	Empfehlungen
45	vpc-default-security-group-geschlossen	Sicherheitsgruppen von Amazon Elastic Compute Cloud (Amazon EC2) können bei der Verwaltung des Netzwerkzugriffs helfen, indem sie eine statusbeh aftete Filterung des ein- und ausgehenden Netzwerkv erkehrs zu Ressourcen bereitstellen. AWS Die Beschränkung des gesamten Datenverkehrs auf die Standardsicherheitsgruppe hilft dabei, den Fernzugriff auf Ihre Ressourcen einzuschr änken. AWS

Kontroll-ID	AWS Config	Empfehlungen
45	vpc-sg-open-only-to-authorized-ports	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass gemeinsame Ports für Amazon Elastic Compute Cloud (Amazon EC2) - Sicherheitsgruppen eingeschränkt sind. Wenn der Zugriff auf Ports nicht auf vertrauenswürdige Quellen beschränkt wird, kann dies zu Angriffen auf die Verfügbarkeit, Integrität und Vertraulichkeit von Systemen führen. Durch die Beschränkung des Zugriffs auf Ressourcen innerhalb einer Sicherheitsgruppe aus dem Internet (0.0.0.0/0) kann der Fernzugriff auf interne Systeme gesteuert werden.
45	account-part-of-organizations	Durch die zentrale Verwaltung AWS-Konten innerhalb von AWS Organizations wird sichergestellt, dass die Konten den Vorschriften entsprechen. Eine fehlende zentrale Kontoverwaltung kann zu inkonsistenten Kontokonfigurationen führen, wodurch Ressourcen und sensible Daten offengelegt werden können.

Kontroll-ID	AWS Config	Empfehlungen
45	iam-customer-policy-blocked-kms-Aktionen	AWS Identity and Access Management (IAM) kann Ihnen helfen, die Prinzipien der geringsten Rechte und der Aufgabentrennung in Zugriffsberechtigungen und Autorisierungen zu integrier en und so zu verhindern, dass Richtlinien blockierte Aktionen für alle AWS Schlüssel des Key Management Service enthalten. Wenn Benutzer mehr Rechte haben, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtig ung und Aufgabentrennung verstoßen. Mit dieser Regel können Sie den Parameter festlegen. blockedActionsPatt erns (Wert „AWS Bewährte grundlegende Sicherhei tsmethoden“: kms: Decrypt, kms:ReEncryptFrom). Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisat ion entsprechen.

Kontroll-ID	AWS Config	Empfehlungen
45	iam-inline-policy-blocked-kms-Aktionen	Stellen Sie sicher, dass ein Benutzer, eine IAM-Rolle oder eine IAM-Grupp e (AWS Identity and Access Management) nicht über eine Inline-Richtlinie verfügt, die blockierte Aktionen für alle AWS Schlüssel des Key Management Service zulässt. AWS empfiehlt, verwaltete Richtlinien anstelle von Inline-Richtlinien zu verwenden . Verwaltete Richtlinien ermöglichen Wiederver wendbarkeit, Versionsv erwaltung, Rollback und Delegierung der Berechtig ungsverwaltung. Mit dieser Regel können Sie den blockedActionsPatterns Parameter festlegen. (Wert „AWS Bewährte grundlege nde Sicherheitsmethoden“: kms: Decrypt, kms:ReEnc ryptFrom). Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprech en.

Kontroll-ID	AWS Config	Empfehlungen
45	ec-2 instance-profile-attached	EC2 Instanzprofile übergeben eine IAM-Rolle an eine EC2 Instance. Das Anhängen eines Instance-Profils an Ihre Instances kann bei der Implementierung von geringsten Berechtigungen und der Berechtigungsverwa ltung helfen.
45	iam-policy-no-statements-with-full-access	Stellen Sie sicher, dass IAM-Aktionen nur auf die benötigte n Aktionen beschränkt sind. Wenn Benutzern mehr Rechte eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und der Aufgabentrennung verstoßen.
45	no-unrestricted-route-to-igw	Stellen Sie sicher, dass EC2 Amazon-Routentabellen keine uneingeschränkten Routen zu einem Internet-Gateway enthalten. Durch das Entfernen oder Beschränk en des Internetzugangs für Workloads innerhalb von Amazon VPCs können unbeabsichtigte Zugriffe in Ihrer Umgebung reduziert werden.

Kontroll-ID	AWS Config	Empfehlungen
45	s3- verboten bucket-level-public-access	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Simple Storage Service (Amazon S3) -Buckets nicht öffentlich zugänglich sind. Diese Regel trägt dazu bei, sensible Daten vor unbefugten Remote-Benutzern zu schützen, indem sie den öffentlichen Zugriff auf Bucket-Ebene verhindert.
45	subnet-auto-assign-public-ip-deaktiviert	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon Virtual Private Cloud (VPC) -Subnetzen nicht automatisch eine öffentliche IP-Adresse zugewiesen wird. Amazon Elastic Compute Cloud (EC2) -Instances, die in Subnetzen gestartet werden, in denen dieses Attribut aktiviert ist, haben ihrer primären Netzwerkschnittstelle eine öffentliche IP-Adresse zugewiesen.

Kontroll-ID	AWS Config	Empfehlungen
45	autoscaling-launch-config-public-ip-deaktiviert	Wenn Sie Ihre Netzwerkschnittstellen mit einer öffentlichen IP-Adresse konfigurieren, sind die diesen Netzwerkschnittstellen zugehörigen Ressourcen über das Internet erreichbar. EC2 Ressourcen sollten nicht öffentlich zugänglich sein, da dies einen unbeabsichtigten Zugriff auf Ihre Anwendungen oder Server ermöglichen kann.
45	redshift-enhanced-vpc-routing-aktiviert	Mit Enhanced-VPC-Routing wird erzwungen, dass der gesamte COPY- und UNLOAD-Datenverkehr zwischen Ihrem Cluster und Datenrepositorys über Ihre Amazon VPC erfolgt. Anschließend können Sie VPC-Features wie Sicherheitsgruppen und Netzwerkzugriffskontrollllisten verwenden, um den Netzwerkverkehr zu schützen. Sie können auch VPC-Flow-Protokolle verwenden, um den Netzwerkverkehr zu überwachen.

Kontroll-ID	AWS Config	Empfehlungen
45	opensearch-in-vpc-only	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass sich Amazon OpenSearch Service-Domains innerhalb einer Amazon Virtual Private Cloud (Amazon VPC) befinden. Eine Amazon OpenSearch Service-Domain innerhalb einer Amazon VPC ermöglich t die sichere Kommunika tion zwischen Amazon OpenSearch Service und anderen Services innerhalb der Amazon VPC, ohne dass ein Internet-Gateway, ein NAT-Gerät oder eine VPN-Verbindung erforderlich ist.

Kontroll-ID	AWS Config	Empfehlungen
45	S3- Blöcke — periodisch account-level-public-access	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Simple Storage Service (Amazon S3) -Buckets nicht öffentlich zugänglich sind. Diese Regel trägt dazu bei, sensible Daten vor unbefugten Remote-Benutzern zu schützen, indem sie den öffentlichen Zugriff verhindert. Mit dieser Regel können Sie optional die Parameter ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) und restrictPublicBuckets Parameter (Config Default: True) festlegen. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	AWS Config	Empfehlungen
45	ssm-document-not-public	Stellen Sie sicher, dass AWS Systems Manager (SSM) - Dokumente nicht öffentlich sind, da dies einen unbeabsichtigten Zugriff auf Ihre SSM-Dokumente ermöglichen kann. Ein öffentliches SSM-Dokument kann Informationen über Ihr Konto, Ihre Ressourcen und internen Prozesse preisgeben.

Kontroll-ID	AWS Config	Empfehlungen
47c	emr-kerberos-enabled	Die Zugriffsberechtigungen und -autorisierungen können verwaltet und nach den Prinzipien der geringsten Berechtigung und Aufgabent rennung integriert werden, indem Kerberos für Amazon-EMR-Cluster aktiviert wird. In Kerberos werden Services und Benutzer, die sich authentifizieren müssen, als Prinzipale bezeichnet. Prinzipale befinden sich in einem Kerberos-Bereich. Innerhalb dieses Bereichs wird ein Kerberos-Server als Key Distribution Center (KDC) bezeichnet. Über diesen Server können sich Prinzipale authentifizieren. Die Authentifizierung im KDC erfolgt durch die Ausstellu ng von Authentifizierungs tickets. Das KDC unterhält eine Datenbank der Prinzipal e in seinem Bereich mit ihren Passwörtern und anderen administrativen Informationen zu jedem Prinzipal.

Kontroll-ID	AWS Config	Empfehlungen
47c	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) kann Ihnen dabei helfen, die Prinzipien der geringsten Rechte und der Aufgabent rennung in Zugriffsberechtigu ngen und Autorisierungen zu integrieren und so zu verhindern, dass Richtlinien „Effect“: „Allow“ mit „Action“: „*“ anstelle von „Resource“: „*“ enthalten. Wenn Benutzern mehr Rechte eingeräumt werden, als für die Ausführun g einer Aufgabe erforderl ich sind, kann dies gegen das Prinzip der geringste n Berechtigung und der Aufgabentrennung verstoßen.

Kontroll-ID	AWS Config	Empfehlungen
47c	iam-root-access-key-überprüfen	Der Zugriff auf Systeme und Ressourcen kann gesteuert werden, indem überprüft wird, ob der Root-Benutzer keine Zugriffsschlüssel mit seiner AWS Identity and Access Management (IAM) -Rolle verknüpft hat. Stellen Sie sicher, dass die Root-Zugriffsschlüssel gelöscht werden. Erstellen und verwenden Sie stattdessen rollenbasierte Funktionen, AWS-Konten um das Prinzip der geringsten Funktionalität zu berücksichtigen.
47c	iam-user-group-membership-überprüfen	AWS Identity and Access Management (IAM) kann Ihnen helfen, Zugriffsberechtigungen und Autorisierungen einzuschränken, indem sichergestellt wird, dass Benutzer Mitglieder mindestens einer Gruppe sind. Wenn Benutzern mehr Berechtigungen eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und Aufgabentrennung verstoßen.

Kontroll-ID	AWS Config	Empfehlungen
47c	iam-user-no-policies-überprüfen	Diese Regel stellt sicher, dass AWS Identity and Access Management (IAM) -Richtlinien nur Gruppen oder Rollen zugewiesen werden, um den Zugriff auf Systeme und Ressourcen zu kontrollieren. Die Zuweisung von Berechtigungen auf Gruppen- oder Rollenebene trägt dazu bei, die Wahrscheinlichkeit zu verringern, dass eine Identität übermäßige Berechtigungen erhält oder beibehält.
47c	iam-no-inline-policy-überprüfen	Stellen Sie sicher, dass ein Benutzer, eine IAM-Rolle oder eine IAM-Gruppe (AWS Identity and Access Management) nicht über eine Inline-Richtlinie zur Zugriffskontrolle auf Systeme und Ressourcen verfügt. AWS empfiehlt, verwaltete Richtlinien anstelle von Inline-Richtlinien zu verwenden . Verwaltete Richtlinien ermöglichen Wiederverwendbarkeit, Versionsverwaltung, Rollback und Delegierung der Berechtigungsverwaltung.

Kontroll-ID	AWS Config	Empfehlungen
47c	iam-policy-no-statements-with-full-access	Stellen Sie sicher, dass IAM-Aktionen nur auf die benötigten Aktionen beschränkt sind. Wenn Benutzern mehr Rechte eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und der Aufgabentrennung verstoßen.
52c	api-gw-cache-enabled-und-verschlüsselt	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass die Verschlüsselung für den Cache Ihrer API-Gateway-Stufe aktiviert ist. Da für die API-Methode sensible Daten erfasst werden können, sollten Sie die Verschlüsselung von Daten im Ruhezustand aktivieren, um diese Daten zu schützen.
52c	cloud-trail-encryption-enabled	Zum Schutz von eventuell vorhandenen sensiblen Daten sowie Daten im Ruhezustand müssen Sie sicherstellen, dass die Verschlüsselung für Ihre AWS CloudTrail aktiviert ist.

Kontroll-ID	AWS Config	Empfehlungen
52c	cloudwatch-log-group-encrypted	Um sensible Daten im Speicher zu schützen, stellen Sie sicher, dass die Verschlüsselung für Ihre Amazon CloudWatch Log Groups aktiviert ist.
52c	efs-encrypted-check	Aktivieren Sie die Verschlüsselung für Ihr Amazon Elastic File System (EFS), um eventuell vorhandene sensible Daten sowie Daten im Ruhezustand zu schützen.
52c	elasticsearch-encrypted-at-rest	Da sensible Daten vorhanden sein können und um Daten im Ruhezustand zu schützen, sollten Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon OpenSearch Service (OpenSearch Service) -Domains aktiviert ist.
52c	encrypted-volumes	Aktivieren Sie die Verschlüsselung für Ihre Volumes von Amazon Elastic Block Store (Amazon EBS), um eventuell vorhandene sensible Daten sowie Daten im Ruhezustand zu schützen.

Kontroll-ID	AWS Config	Empfehlungen
52c	rds-storage-encrypted	Zum Schutz von Daten im Ruhezustand müssen Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon Relational Database Service (Amazon RDS)-Instances aktiviert ist. Da sensible Daten in Amazon-RDS-Instances gespeichert werden können, sollten Sie die Verschlüsselung von Daten im Ruhezustand aktivieren, um diese Daten zu schützen.

Kontroll-ID	AWS Config	Empfehlungen
52c	redshift-cluster-configuration-check	Um Daten im Ruhezustand zu schützen, muss die Verschlüsselung für Ihre Amazon-Redshift-Cluster aktiviert sein. Sie müssen auch sicherstellen, dass die erforderlichen Konfigurationen auf Amazon-Redshift-Clustern bereitgestellt werden. Die Prüfungsprotokollierung muss aktiviert sein, um Informationen zu Verbindungen und Benutzeraktivitäten in der Datenbank bereitzustellen. Diese Regel erfordert, dass ein Wert für clusterDbEncrypted (Config Default: TRUE) und LoggingEnabled (Config Default: TRUE) gesetzt ist. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	AWS Config	Empfehlungen
52c	s3-aktiviert bucket-server-side-encryption	Zum Schutz von Daten im Ruhezustand müssen Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon Simple Storage Service (Amazon S3)-Buckets aktiviert ist. Da sensible Daten in Amazon-S3-Buckets gespeichert werden können, sollten Sie die Verschlüsselung aktivieren, um diese Daten zu schützen.
52c	sagemaker-endpoint-configuration-kms-key-konfiguriert	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass die Verschlüsselung mit dem AWS Key Management Service (AWS KMS) für Ihren Endpunkt aktiviert ist. SageMaker Da sensible Daten auf dem SageMaker Endgerät gespeichert werden können, sollten Sie die Verschlüsselung im Ruhezustand aktivieren, um diese Daten zu schützen.

Kontroll-ID	AWS Config	Empfehlungen
52c	sagemaker-notebook-instance-kms-schlüsselkonfiguriert	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass die Verschlüsselung mit dem AWS Key Management Service (AWS KMS) für Ihr Notebook aktiviert ist. SageMaker Da vertrauliche Daten im SageMaker Notebook gespeichert werden können, sollten Sie die Verschlüsselung im Ruhezustand aktivieren, um diese Daten zu schützen.
52c	sns-encrypted-kms	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass Ihre Amazon Simple Notification Service (Amazon SNS) -Themen mit dem AWS Key Management Service (AWS KMS) verschlüsselt werden müssen. Um eventuell vorhandene sensible Daten im Ruhezustand in veröffentlichten Nachrichten zu schützen, muss die Verschlüsselung von Daten im Ruhezustand aktiviert sein.

Kontroll-ID	AWS Config	Empfehlungen
52c	ec2- ebs-encryption-by-default	Zum Schutz von Daten im Ruhezustand müssen Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon Elastic Block Store (Amazon EBS)-Volumes aktiviert ist. Aktivieren Sie die Verschlüsselung von Daten im Ruhezustand, um eventuell in diesen Volumes vorhandene sensible Daten im Ruhezusta nd zu schützen.
52c	dynamodb-table-encrypted-km s	Stellen Sie sicher, dass die Verschlüsselung für Ihre Amazon-DynamoDB-Tabellen aktiviert ist. Um eventuell vorhandene sensible Daten im Ruhezustand in diesen Tabellen zu schützen, müssen Sie die Verschlüsselung von Daten im Ruhezustand aktivieren. Standardmäßig werden DynamoDB-Tabellen mit einem AWS eigenen Kundenhauptschlüssel (CMK) verschlüsselt.

Kontroll-ID	AWS Config	Empfehlungen
52c	rds-snapshot-encrypted	Stellen Sie sicher, dass die Verschlüsselung für Ihre Amazon Relational Database Service (Amazon RDS)-Snapshots aktiviert ist. Da sensible Daten auch im Ruhezustand vorhanden sein können, sollten Sie die Verschlüsselung von Daten im Ruhezustand aktivieren, um diese Daten zu schützen.
52c	s-3 default-encryption-kms	Stellen Sie sicher, dass die Verschlüsselung für Ihre Amazon Simple Storage Service (Amazon S3)-Buckets aktiviert ist. Da sensible Daten in einem Amazon-S3-Bucket gespeichert werden können, sollten Sie die Verschlüs selung im Ruhezustand aktivieren, um diese Daten zu schützen.

Kontroll-ID	AWS Config	Empfehlungen
52c	redshift-cluster-kms-enabled	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass die Verschlüsselung mit AWS Key Management Service (AWS KMS) für Ihren Amazon Redshift Redshift-Cluster aktiviert ist. Um eventuell vorhandene sensible Daten im Ruhezustand in Redshift-Clustern zu schützen, muss die Verschlüsselung von Daten im Ruhezustand aktiviert sein.
52c	opensearch-encrypted-at-rest	Da sensible Daten vorhanden sein können und um Daten im Ruhezustand zu schützen, sollten Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon OpenSearch Service-Domains aktiviert ist.
52d	s-3 bucket-public-read-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie nur autorisierten Benutzern, Prozessen und Geräten Zugriff auf Amazon Simple Storage Service (Amazon S3) -Buckets gewähren. Die Verwaltung des Zugriffs sollte mit der Klassifizierung der Daten übereinstimmen.

Kontroll-ID	AWS Config	Empfehlungen
52d	s3- bucket-public-write-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie nur autorisierten Benutzern, Prozessen und Geräten Zugriff auf Amazon Simple Storage Service (Amazon S3) -Buckets gewähren. Die Verwaltung des Zugriffs sollte mit der Klassifizierung der Daten übereinstimmen.
52d	sagemaker-notebook-no-direct-Internetzugang	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass SageMaker Amazon-Notebooks keinen direkten Internetzugang zulassen. Indem Sie direkten Internetzugang blockieren, vermeiden Sie, dass unbefugte Benutzer auf sensible Daten zugreifen.
52d	dms-replication-not-public	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass auf DMS-Replikationsinstanzen nicht öffentlich zugegriffen werden kann. DMS-Replikations-Instances können vertrauliche Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	AWS Config	Empfehlungen
52d	ebs-snapshot-public-restorable-überprüfen	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass EBS-Snapshots nicht öffentlich wiederherstellbar sind. EBS-Volume-Snapshots können vertrauliche Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.
52d	ec-2 instance-no-public-ip	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon Elastic Compute Cloud (Amazon EC2) -Instances nicht öffentlich zugänglich sind. EC2Amazon-Instances können vertrauliche Informationen enthalten, und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	AWS Config	Empfehlungen
52d	elasticsearch-in-vpc-only	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass sich Amazon OpenSearch OpenSearch Service (Service) -Domains innerhalb einer Amazon Virtual Private Cloud (Amazon VPC) befinden. Eine OpenSearch Service-Domain innerhalb einer Amazon VPC ermöglicht die sichere Kommunikation zwischen OpenSearch Service und anderen Services innerhalb der Amazon VPC, ohne dass ein Internet-Gateway, ein NAT-Gerät oder eine VPN-Verbindung erforderlich ist.
52d	emr-master-no-public-ip	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon EMR-Cluster-Masterknoten nicht öffentlich zugänglich sind. Amazon-EMR-Cluster-Hauptknoten können vertrauliche Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	AWS Config	Empfehlungen
52d	ec-2 instances-in-vpc	Stellen Sie Amazon Elastic Compute Cloud (Amazon EC2) -Instances innerhalb einer Amazon Virtual Private Cloud (Amazon VPC) bereit, um eine sichere Kommunika tion zwischen einer Instance und anderen Services innerhalb der Amazon VPC zu ermöglichen, ohne dass ein Internet-Gateway, ein NAT-Gerät oder eine VPN-Verbi ndung erforderlich ist. Der gesamte Datenverkehr bleibt sicher in der AWS Cloud. Domains, die sich innerhalb einer VPC befinden, verfügen aufgrund ihrer logischen Isolierung im Vergleich zu Domains mit öffentlic hen Endpunkten über eine zusätzliche Sicherheitsebene. Weisen Sie EC2 Amazon-In stances einer Amazon-VPC zu, um den Zugriff ordnungsg emäß zu verwalten.

Kontroll-ID	AWS Config	Empfehlungen
52d	internet-gateway-authorized-vpc-nur	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Internet-Gateways nur mit autorisierter Amazon Virtual Private Cloud (Amazon VPC) verbunden sind. Internet-Gateways ermöglichen den bidirekti onalen Internetzugang zur und von der Amazon VPC, was möglicherweise zu einem unbefugten Zugriff auf Amazon-VPC-Ressourcen führen kann.
52d	lambda-function-public-acce ss-verboten	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherste llen, dass AWS Lambda-Funktionen nicht öffentlich zugänglich sind. Der öffentlic he Zugriff kann möglicher weise die Verfügbarkeit von Ressourcen beeinträchtigen.

Kontroll-ID	AWS Config	Empfehlungen
52d	lambda-inside-vpc	Stellen Sie AWS Lambda-Funktionen in einer Amazon Virtual Private Cloud (Amazon VPC) bereit, um eine sichere Kommunikation zwischen einer Funktion und anderen Diensten innerhalb der Amazon VPC zu gewährleisten. Bei dieser Konfiguration sind kein Internet-Gateway, kein NAT-Gerät und keine VPN-Verbindung erforderlich. Der gesamte Datenverkehr bleibt sicher in der Cloud. AWS Domains, die sich innerhalb einer VPC befinden, verfügen aufgrund ihrer logischen Isolierung im Vergleich zu Domains mit öffentlichen Endpunkten über eine zusätzliche Sicherheitsebene. Um den Zugriff ordnungsgemäß zu verwalten, sollten AWS Lambda-Funktionen einer VPC zugewiesen werden.

Kontroll-ID	AWS Config	Empfehlungen
52d	rds-instance-public-access-überprüfen	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Relational Database Service (Amazon RDS) -Instances nicht öffentlich sind. Amazon-RDS-Datenbank-Instances können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.
52d	rds-snapshots-public-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Relational Database Service (Amazon RDS) -Instances nicht öffentlich sind. Amazon-RDS-Datenbank-Instances können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	AWS Config	Empfehlungen
52d	redshift-cluster-public-access-überprüfen	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Redshift Redshift-Cluster nicht öffentlich sind. Amazon-Redshift-Cluster können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.
52d	no-unrestricted-route-to-igw	Stellen Sie sicher, dass EC2 Amazon-Routentabellen keine uneingeschränkten Routen zu einem Internet-Gateway enthalten. Durch das Entfernen oder Beschränken des Internetzugangs für Workloads innerhalb von Amazon VPCs können unbeabsichtigte Zugriffe in Ihrer Umgebung reduziert werden.

Kontroll-ID	AWS Config	Empfehlungen
52d	subnet-auto-assign-public-ip-deaktiviert	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon Virtual Private Cloud (VPC) -Subnetzen nicht automatis ch eine öffentliche IP-Adress e zugewiesen wird. Amazon Elastic Compute Cloud (EC2) -Instances, die in Subnetzen gestartet werden, in denen dieses Attribut aktiviert ist, haben ihrer primären Netzwerkschnittste lle eine öffentliche IP-Adresse zugewiesen.
52d	autoscaling-launch-config-public-ip-deaktiviert	Wenn Sie Ihre Netzwerks chnittstellen mit einer öffentlic hen IP-Adresse konfigurieren, sind die diesen Netzwerks chnittstellen zugehörigen Ressourcen über das Internet erreichbar. EC2 Ressource n sollten nicht öffentlich zugänglich sein, da dies einen unbeabsichtigten Zugriff auf Ihre Anwendungen oder Server ermöglichen kann.

Kontroll-ID	AWS Config	Empfehlungen
52d	redshift-enhanced-vpc-routing-aktiviert	Mit Enhanced-VPC-Routing wird erzwungen, dass der gesamte COPY- und UNLOAD-Datenverkehr zwischen Ihrem Cluster und Datenrepositorys über Ihre Amazon VPC erfolgt. Anschließend können Sie VPC-Features wie Sicherheitsgruppen und Netzwerkzugriffskontrollllisten verwenden, um den Netzwerkverkehr zu schützen. Sie können auch VPC-Flow-Protokolle verwenden, um den Netzwerkverkehr zu überwachen.
52d	ssm-document-not-public	Stellen Sie sicher, dass AWS Systems Manager (SSM) - Dokumente nicht öffentlich sind, da dies einen unbeabsichtigten Zugriff auf Ihre SSM-Dokumente ermöglichen kann. Ein öffentliches SSM-Dokument kann Informationen über Ihr Konto, Ihre Ressourcen und internen Prozesse preisgeben.

Kontroll-ID	AWS Config	Empfehlungen
52d	s3- verboten bucket-level-public-access	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Simple Storage Service (Amazon S3) -Buckets nicht öffentlich zugänglich sind. Diese Regel trägt dazu bei, sensible Daten vor unbefugten Remote-Benutzern zu schützen, indem sie den öffentlichen Zugriff auf Bucket-Ebene verhindert.
52d	opensearch-in-vpc-only	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass sich Amazon OpenSearch Service-Domains innerhalb einer Amazon Virtual Private Cloud (Amazon VPC) befinden. Eine Amazon OpenSearch Service-Domain innerhalb einer Amazon VPC ermöglicht die sichere Kommunikation zwischen Amazon OpenSearch Service und anderen Services innerhalb der Amazon VPC, ohne dass ein Internet-Gateway, ein NAT-Gerät oder eine VPN-Verbindung erforderlich ist.

Kontroll-ID	AWS Config	Empfehlungen
52d	S3- Blöcke — periodisch account-level-public-access	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Simple Storage Service (Amazon S3) -Buckets nicht öffentlich zugänglich sind. Diese Regel trägt dazu bei, sensible Daten vor unbefugten Remote-Benutzern zu schützen, indem sie den öffentlichen Zugriff verhindert. Mit dieser Regel können Sie optional die Parameter ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) und restrictPublicBuckets Parameter (Config Default: True) festlegen. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	AWS Config	Empfehlungen
52e	securityhub-enabled	AWS Security Hub hilft bei der Überwachung von unbefugte m Personal, Verbindungen, Geräten und Software. AWS Security Hub aggregiert, organisiert und priorisiert die Sicherheitswarnungen oder Ergebnisse mehrerer Dienste. AWS Einige dieser Dienste sind Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer und AWS Firewall Manager sowie AWS Partnerlösungen.
52e	guardduty-enabled-centralized	Amazon GuardDuty kann mithilfe von Threat Intellige nce Feeds helfen, potenzielle Cybersicherheitsereignisse zu überwachen und zu erkennen. Dazu gehören Listen mit bösartigen IPs und maschinel len Lernmethoden zur Identifiz ierung unerwarteter, nicht autorisierter und bösartige r Aktivitäten in Ihrer AWS Cloud-Umgebung.

Kontroll-ID	AWS Config	Empfehlungen
53	s-3 bucket-public-read-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie nur autorisierten Benutzern, Prozessen und Geräten Zugriff auf Amazon Simple Storage Service (Amazon S3) -Buckets gewähren. Die Verwaltung des Zugriffs sollte mit der Klassifizierung der Daten übereinstimmen.
53	s3- bucket-public-write-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie nur autorisierten Benutzern, Prozessen und Geräten Zugriff auf Amazon Simple Storage Service (Amazon S3) -Buckets gewähren. Die Verwaltung des Zugriffs sollte mit der Klassifizierung der Daten übereinstimmen.

Kontroll-ID	AWS Config	Empfehlungen
53	opensearch-in-vpc-only	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass sich Amazon OpenSearch Service-Domains innerhalb einer Amazon Virtual Private Cloud (Amazon VPC) befinden. Eine Amazon OpenSearch Service-Domain innerhalb einer Amazon VPC ermöglich t die sichere Kommunika tion zwischen Amazon OpenSearch Service und anderen Services innerhalb der Amazon VPC, ohne dass ein Internet-Gateway, ein NAT-Gerät oder eine VPN-Verbindung erforderlich ist.
53	sagemaker-notebook-no-direc t-Internetzugang	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherste llen, dass SageMaker Amazon-Notebooks keinen direkten Internetzugang zulassen. Indem Sie direkten Internetzugang blockiere n, vermeiden Sie, dass unbefugte Benutzer auf sensible Daten zugreifen.

Kontroll-ID	AWS Config	Empfehlungen
53	dms-replication-not-public	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass auf DMS-Replikationsinstanzen nicht öffentlich zugegriffen werden kann. DMS-Replikations-I nstances können vertrauli che Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.
53	ebs-snapshot-public-restora ble-überprüfen	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass EBS-Snaps hots nicht öffentlich wiederher stellbar sind. EBS-Volume-Snapshots können vertrauli che Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.
53	ec-2 instance-no-public-ip	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon Elastic Compute Cloud (Amazon EC2) -Instances nicht öffentlich zugänglich sind. EC2Amazon-Instances können vertrauliche Informati onen enthalten, und für solche Konten ist eine Zugriffsk ontrolle erforderlich.

Kontroll-ID	AWS Config	Empfehlungen
53	elasticsearch-in-vpc-only	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass sich Amazon OpenSearch OpenSearch Service (Service) -Domains innerhalb einer Amazon Virtual Private Cloud (Amazon VPC) befinden. Eine OpenSearch Service-Domain innerhalb einer Amazon VPC ermöglicht die sichere Kommunikation zwischen OpenSearch Service und anderen Services innerhalb der Amazon VPC, ohne dass ein Internet-Gateway, ein NAT-Gerät oder eine VPN-Verbindung erforderlich ist.
53	emr-master-no-public-ip	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon EMR-Cluster-Masterknoten nicht öffentlich zugänglich sind. Amazon-EMR-Cluster-Hauptknoten können vertrauliche Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	AWS Config	Empfehlungen
53	ec-2 instances-in-vpc	Stellen Sie Amazon Elastic Compute Cloud (Amazon EC2) -Instances innerhalb einer Amazon Virtual Private Cloud (Amazon VPC) bereit, um eine sichere Kommunika tion zwischen einer Instance und anderen Services innerhalb der Amazon VPC zu ermöglichen, ohne dass ein Internet-Gateway, ein NAT-Gerät oder eine VPN-Verbi ndung erforderlich ist. Der gesamte Datenverkehr bleibt sicher in der AWS Cloud. Domains, die sich innerhalb einer VPC befinden, verfügen aufgrund ihrer logischen Isolierung im Vergleich zu Domains mit öffentlic hen Endpunkten über eine zusätzliche Sicherheitsebene. Weisen Sie EC2 Amazon-In stances einer Amazon-VPC zu, um den Zugriff ordnungsg emäß zu verwalten.

Kontroll-ID	AWS Config	Empfehlungen
53	internet-gateway-authorized-vpc-nur	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Internet-Gateways nur mit autorisierter Amazon Virtual Private Cloud (Amazon VPC) verbunden sind. Internet-Gateways ermöglichen den bidirekti onalen Internetzugang zur und von der Amazon VPC, was möglicherweise zu einem unbefugten Zugriff auf Amazon-VPC-Ressourcen führen kann.
53	lambda-function-public-acce ss-verboten	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherste llen, dass AWS Lambda-Funktionen nicht öffentlich zugänglich sind. Der öffentlic he Zugriff kann möglicher weise die Verfügbarkeit von Ressourcen beeinträchtigen.

Kontroll-ID	AWS Config	Empfehlungen
53	lambda-inside-vpc	Stellen Sie AWS Lambda-Funktionen in einer Amazon Virtual Private Cloud (Amazon VPC) bereit, um eine sichere Kommunikation zwischen einer Funktion und anderen Diensten innerhalb der Amazon VPC zu gewährleisten. Bei dieser Konfiguration sind kein Internet-Gateway, kein NAT-Gerät und keine VPN-Verbindung erforderlich. Der gesamte Datenverkehr bleibt sicher in der Cloud. AWS Domains, die sich innerhalb einer VPC befinden, verfügen aufgrund ihrer logischen Isolierung im Vergleich zu Domains mit öffentlichen Endpunkten über eine zusätzliche Sicherheitsebene. Um den Zugriff ordnungsgemäß zu verwalten, sollten AWS Lambda-Funktionen einer VPC zugewiesen werden.

Kontroll-ID	AWS Config	Empfehlungen
53	rds-instance-public-access-überprüfen	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Relational Database Service (Amazon RDS) -Instances nicht öffentlich sind. Amazon-RDS-Datenbank-Instances können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.
53	rds-snapshots-public-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Relational Database Service (Amazon RDS) -Instances nicht öffentlich sind. Amazon-RDS-Datenbank-Instances können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	AWS Config	Empfehlungen
53	redshift-cluster-public-access-überprüfen	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Redshift Redshift-Cluster nicht öffentlich sind. Amazon-Redshift-Cluster können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.
53	no-unrestricted-route-to-igw	Stellen Sie sicher, dass EC2 Amazon-Routentabellen keine uneingeschränkten Routen zu einem Internet-Gateway enthalten. Durch das Entfernen oder Beschränken des Internetzugangs für Workloads innerhalb von Amazon VPCs können unbeabsichtigte Zugriffe in Ihrer Umgebung reduziert werden.

Kontroll-ID	AWS Config	Empfehlungen
53	s3- verboten bucket-level-public-access	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Simple Storage Service (Amazon S3) -Buckets nicht öffentlich zugänglich sind. Diese Regel trägt dazu bei, sensible Daten vor unbefugten Remote-Benutzern zu schützen, indem sie den öffentlichen Zugriff auf Bucket-Ebene verhindert.
53	subnet-auto-assign-public-ip-deaktiviert	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon Virtual Private Cloud (VPC) -Subnetzen nicht automatisch eine öffentliche IP-Adresse zugewiesen wird. Amazon Elastic Compute Cloud (EC2) -Instances, die in Subnetzen gestartet werden, in denen dieses Attribut aktiviert ist, haben ihrer primären Netzwerkschnittstelle eine öffentliche IP-Adresse zugewiesen.

Kontroll-ID	AWS Config	Empfehlungen
53	autoscaling-launch-config-public-ip-deaktiviert	Wenn Sie Ihre Netzwerkschnittstellen mit einer öffentlichen IP-Adresse konfigurieren, sind die diesen Netzwerkschnittstellen zugehörigen Ressourcen über das Internet erreichbar. EC2 Ressourcen sollten nicht öffentlich zugänglich sein, da dies einen unbeabsichtigten Zugriff auf Ihre Anwendungen oder Server ermöglichen kann.
53	redshift-enhanced-vpc-routing-aktiviert	Mit Enhanced-VPC-Routing wird erzwungen, dass der gesamte COPY- und UNLOAD-Datenverkehr zwischen Ihrem Cluster und Datenrepositorys über Ihre Amazon VPC erfolgt. Anschließend können Sie VPC-Features wie Sicherheitsgruppen und Netzwerkzugriffskontrollllisten verwenden, um den Netzwerkverkehr zu schützen. Sie können auch VPC-Flow-Protokolle verwenden, um den Netzwerkverkehr zu überwachen.

Kontroll-ID	AWS Config	Empfehlungen
53	s3- -Blocke-periodisch account-level-public-access	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Simple Storage Service (Amazon S3) -Buckets nicht öffentlich zugänglich sind. Diese Regel trägt dazu bei, sensible Daten vor unbefugten Remote-Benutzern zu schützen, indem sie den öffentlichen Zugriff verhindert. Mit dieser Regel können Sie optional die Parameter ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) und restrictPublicBuckets Parameter (Config Default: True) festlegen. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	AWS Config	Empfehlungen
53	ssm-document-not-public	Stellen Sie sicher, dass AWS Systems Manager (SSM) - Dokumente nicht öffentlich sind, da dies einen unbeabsichtigten Zugriff auf Ihre SSM-Dokumente ermöglichen kann. Ein öffentliches SSM-Dokument kann Informationen über Ihr Konto, Ihre Ressourcen und internen Prozesse preisgeben.
54	opensearch-encrypted-at-rest	Da sensible Daten vorhanden sein können und um Daten im Ruhezustand zu schützen, sollten Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon OpenSearch Service-Domains aktiviert ist.
54	acm-certificate-expiration-check	Stellen Sie sicher, dass die Netzwerkintegrität geschützt ist, indem Sie sicherstellen, dass X509-Zertifikate von AWS ACM ausgestellt werden. Diese Zertifikate müssen gültig und dürfen nicht abgelaufen sein. Für diese Regel ist ein Wert für erforderlich daysToExpiration (Wert für bewährte AWS Grundregeln für Sicherheit: 90). Der tatsächliche Wert muss den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	AWS Config	Empfehlungen
54	alb-http-to-https-Umleitung sprüfung	Um Daten während der Übertragung zu schützen, stellen Sie sicher, dass Ihr Application Load Balancer unverschlüsselte HTTP-Anfr agen automatisch an HTTPS umleitet. Da sensible Daten vorhanden sein können, sollten Sie die Verschlüs selung bei der Übertragung aktivieren, um diese Daten zu schützen.
54	api-gw-cache-enabled-und-ve rschlüsselt	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass die Verschlüsselung für den Cache Ihrer API-Gatew ay-Stufe aktiviert ist. Da für die API-Methode sensible Daten erfasst werden können, sollten Sie die Verschlüsselung von Daten im Ruhezustand aktivieren, um diese Daten zu schützen.
54	cloud-trail-encryption-enabled	Zum Schutz von eventuell vorhandenen sensiblen Daten sowie Daten im Ruhezusta nd müssen Sie sicherstellen, dass die Verschlüsselung für Ihre AWS CloudTrail aktiviert ist.

Kontroll-ID	AWS Config	Empfehlungen
54	cloudwatch-log-group-encrypted	Um sensible Daten im Speicher zu schützen, stellen Sie sicher, dass die Verschlüsselung für Ihre Amazon CloudWatch Log Groups aktiviert ist.
54	efs-encrypted-check	Aktivieren Sie die Verschlüsselung für Ihr Amazon Elastic File System (EFS), um eventuell vorhandene sensible Daten sowie Daten im Ruhezustand zu schützen.
54	elasticsearch-encrypted-at-rest	Da sensible Daten vorhanden sein können und um Daten im Ruhezustand zu schützen, sollten Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon OpenSearch Service (OpenSearch Service) -Domains aktiviert ist.

Kontroll-ID	AWS Config	Empfehlungen
54	elb-acm-certificate-required	Zum Schutz von eventuell vorhandenen sensiblen Daten sowie von Daten während der Übertragung muss die Verschlüsselung für Ihr Elastic Load Balancing aktiviert sein. Verwenden Sie AWS Certifica te Manager, um öffentlic he und private SSL/TLS-Z ertifikate mit AWS Diensten und internen Ressourcen zu verwalten, bereitzustellen und bereitzustellen.
54	encrypted-volumes	Aktivieren Sie die Verschlüs selung für Ihre Volumes von Amazon Elastic Block Store (Amazon EBS), um eventuell vorhandene sensible Daten sowie Daten im Ruhezustand zu schützen.
54	rds-storage-encrypted	Zum Schutz von Daten im Ruhezustand müssen Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon Relational Database Service (Amazon RDS)-Instances aktiviert ist. Da sensible Daten in Amazon-RDS-Instances gespeichert werden können, sollten Sie die Verschlüsselung von Daten im Ruhezustand aktivieren, um diese Daten zu schützen.

Kontroll-ID	AWS Config	Empfehlungen
54	redshift-cluster-configuration-check	Um Daten im Ruhezustand zu schützen, muss die Verschlüsselung für Ihre Amazon-Redshift-Cluster aktiviert sein. Sie müssen auch sicherstellen, dass die erforderlichen Konfigurationen auf Amazon-Redshift-Clustern bereitgestellt werden. Die Prüfungsprotokollierung muss aktiviert sein, um Informationen zu Verbindungen und Benutzeraktivitäten in der Datenbank bereitzustellen. Diese Regel erfordert, dass ein Wert für clusterDbEncrypted (Config Default: TRUE) und LoggingEnabled (Config Default: TRUE) gesetzt ist. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	AWS Config	Empfehlungen
54	opensearch-node-to-node-Verschlüsselungsprüfung	Stellen Sie sicher, dass die node-to-node Verschlüsselung für Amazon OpenSearch Service aktiviert ist. Node-to-nodeVerschlüsselung ermöglicht die TLS 1.2-Verschlüsselung für die gesamte Kommunikation innerhalb der Amazon Virtual Private Cloud (Amazon VPC). Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.
54	redshift-require-tls-ssl	Stellen Sie sicher, dass Ihre Amazon-Redshift-Cluster eine TLS/SSL-Verschlüsselung erfordern, um eine Verbindung zu SQL-Clients herzustellen. Da sensible Daten vorhanden sein können, sollten Sie die Verschlüsselung bei der Übertragung aktivieren, um diese Daten zu schützen.

Kontroll-ID	AWS Config	Empfehlungen
54	s3-fähig bucket-server-side-encryption	Zum Schutz von Daten im Ruhezustand müssen Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon Simple Storage Service (Amazon S3)-Bucke ts aktiviert ist. Da sensible Daten in Amazon-S3-Buckets gespeichert werden können, sollten Sie die Verschlüs selung aktivieren, um diese Daten zu schützen.
54	s-3 bucket-ssl-requests-only	Um Daten während der Übertragung zu schützen, stellen Sie sicher, dass Ihre Amazon Simple Storage Service (Amazon S3)-Buckets Anfragen zur Verwendung von Secure Socket Layer (SSL)-Buckets erfordern. Da sensible Daten vorhanden sein können, sollten Sie die Verschlüs selung bei der Übertragung aktivieren, um diese Daten zu schützen.

Kontroll-ID	AWS Config	Empfehlungen
54	sagemaker-endpoint-configuration-kms-key-konfiguriert	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass die Verschlüsselung mit dem AWS Key Management Service (AWS KMS) für Ihren Endpunkt aktiviert ist. SageMaker Da sensible Daten auf dem SageMaker Endgerät gespeichert werden können, sollten Sie die Verschlüsselung im Ruhezustand aktivieren, um diese Daten zu schützen.
54	sagemaker-notebook-instance-kms-schlüsselkonfiguriert	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass die Verschlüsselung mit dem AWS Key Management Service (AWS KMS) für Ihr Notebook aktiviert ist. SageMaker Da vertrauliche Daten im SageMaker Notebook gespeichert werden können, sollten Sie die Verschlüsselung im Ruhezustand aktivieren, um diese Daten zu schützen.

Kontroll-ID	AWS Config	Empfehlungen
54	sns-encrypted-kms	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass Ihre Amazon Simple Notification Service (Amazon SNS) -Themen mit dem AWS Key Management Service (AWS KMS) verschlüsselt werden müssen. Um eventuell vorhandene sensible Daten im Ruhezustand in veröffentlichten Nachrichten zu schützen, muss die Verschlüsselung von Daten im Ruhezustand aktiviert sein.
54	ec2- ebs-encryption-by-default	Zum Schutz von Daten im Ruhezustand müssen Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon Elastic Block Store (Amazon EBS)-Volumes aktiviert ist. Aktivieren Sie die Verschlüsselung von Daten im Ruhezustand, um eventuell in diesen Volumes vorhandene sensible Daten im Ruhezustand zu schützen.

Kontroll-ID	AWS Config	Empfehlungen
54	rds-snapshot-encrypted	Stellen Sie sicher, dass die Verschlüsselung für Ihre Amazon Relational Database Service (Amazon RDS)-Snapshots aktiviert ist. Da sensible Daten auch im Ruhezustand vorhanden sein können, sollten Sie die Verschlüsselung von Daten im Ruhezustand aktivieren, um diese Daten zu schützen.
54	elasticsearch-node-to-node-Verschlüsselungsprüfung	Stellen Sie sicher, dass die node-to-node Verschlüsselung für Amazon OpenSearch Service aktiviert ist. Node-to-nodeVerschlüsselung ermöglicht die TLS 1.2-Versc hlüsselung für die gesamte Kommunikation innerhalb der Amazon Virtual Private Cloud (Amazon VPC). Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.
54	elb-tls-https-listeners-nur	Stellen Sie sicher, dass Ihre Elastic Load Balancer (ELBs) mit SSL- oder HTTPS-Lis tenern konfiguriert sind. Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	AWS Config	Empfehlungen
54	redshift-cluster-kms-enabled	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass die Verschlüsselung mit AWS Key Management Service (AWS KMS) für Ihren Amazon Redshift Redshift-Cluster aktiviert ist. Um eventuell vorhandene sensible Daten im Ruhezustand in Redshift-Clustern zu schützen, muss die Verschlüsselung von Daten im Ruhezustand aktiviert sein.
54	api-gw-ssl-enabled	Stellen Sie sicher, dass die REST-API-Stufen von Amazon API Gateway mit SSL-Zerti fikaten konfiguriert sind, damit Backend-Systeme überprüfe n können, ob Anforderungen von API Gateway stammen.
54	elbv-2 acm-certificate-required	Zum Schutz von eventuell vorhandenen sensiblen Daten sowie von Daten während der Übertragung muss die Verschlüsselung für Ihr Elastic Load Balancing aktiviert sein. Verwenden Sie AWS Certifica te Manager, um öffentlic he und private SSL/TLS-Z ertifikate mit AWS Diensten und internen Ressourcen zu verwalten, bereitzustellen und bereitzustellen.

Kontroll-ID	AWS Config	Empfehlungen
55	elasticsearch-node-to-node-Verschlüsselungsprüfung	Stellen Sie sicher, dass die node-to-node Verschlüsselung für Amazon OpenSearch Service aktiviert ist. Node-to-nodeVerschlüsselung ermöglicht die TLS 1.2-Versc hlüsselung für die gesamte Kommunikation innerhalb der Amazon Virtual Private Cloud (Amazon VPC). Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.
55	opensearch-node-to-node-Verschlüsselungsprüfung	Stellen Sie sicher, dass die node-to-node Verschlüsselung für Amazon OpenSearch Service aktiviert ist. Node-to-nodeVerschlüsselung ermöglicht die TLS 1.2-Versc hlüsselung für die gesamte Kommunikation innerhalb der Amazon Virtual Private Cloud (Amazon VPC). Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	AWS Config	Empfehlungen
67	api-gw-execution-logging-aktiviert	Die API-Gateway-Protokollierung zeigt detaillierte Ansichten der Benutzer, die auf die API zugegriffen haben, und wie diese Benutzer auf die API zugegriffen haben. Diese Einblicke ermöglichen die Transparenz von Benutzeraktivitäten.
67	cloud-trail-cloud-watch-logs-aktiviert	Verwenden Sie Amazon CloudWatch , um Protokollereignisaktivitäten zentral zu sammeln und zu verwalten . Die Aufnahme von AWS CloudTrail Daten liefert Einzelheiten zu den API-Aufrufaktivitäten in Ihrem AWS-Konto.

Kontroll-ID	AWS Config	Empfehlungen
67	cloudtrail-enabled	AWS CloudTrail kann durch die Aufzeichnung von Aktionen und API-Aufrufen in der AWS Management Console bei der Nichtabst reitbarkeit helfen. Sie können die Benutzer und die Benutzer AWS-Konten , die einen AWS Dienst aufgerufen haben, die Quell-IP-Adresse, über die die Aufrufe generiert wurden, und den Zeitpunkt der Anrufe identifizieren. Einzelheiten zu den erfassten Daten finden Sie in den AWS CloudTrail Datensatzinhalten.
67	cloudtrail-s3-dataevents-en abled	Die Erfassung von Simple Storage Service (Amazon S3)-Datenereignissen unterstützt die Erkennung von ungewöhnl ichen Aktivitäten. Zu den Details gehören Informati onen zu dem AWS -Konto, das auf einen Amazon-S3-Bucket zugegriffen hat, die IP-Adresse und die Uhrzeit des Ereignisses.

Kontroll-ID	AWS Config	Empfehlungen
67	elb-logging-enabled	Die Elastic-Load-Balancing-Aktivität ist ein zentraler Kommunikationspunkt innerhalb einer Umgebung. Stellen Sie sicher, dass die ELB-Protokollierung aktiviert ist. Die gesammelten Daten enthalten detaillierte Informati onen zu Anfragen, die an den ELB gesendet wurden. Jedes Protokoll enthält Informati onen wie die Zeit, zu der die Anforderung einging, die Client-IP-Adresse, Latenzen, Anforderungspfade und Serverantworten.

Kontroll-ID	AWS Config	Empfehlungen
67	multi-region-cloudtrail-enabled	AWS CloudTrail zeichnet Aktionen und API-Aufrufe der AWS Management Console auf. Sie können feststellen, welche Benutzer und Konten angerufen wurden AWS, von welcher Quell-IP-Adresse aus die Anrufe getätigt wurden und wann die Anrufe erfolgten . CloudTrail übermittelt Protokolldateien aus allen AWS Regionen an Ihren S3-Bucket, wenn MULTI_REGION_CLOUD_TRAIL_ENABLED aktiviert ist. Außerdem wird beim AWS Start einer neuen Region derselbe Trail in der neuen Region erstellt. CloudTrail Dadurch erhalten Sie automatisch Protokoll dateien mit API-Aktivitäten für die neue Region.

Kontroll-ID	AWS Config	Empfehlungen
67	s-3 bucket-logging-enabled	Die Amazon Simple Storage Service (Amazon S3)-Serverzugriffsprotokollierung bietet eine Methode zur Überwachung des Netzwerks im Hinblick auf potenzielle Cybersicherheitsereignisse. Die Ereignisse werden überwacht, indem detaillierte Aufzeichnungen über die Anfragen erfasst werden, die an einen Amazon-S3-Bucket gestellt wurden. Jeder Zugriffsprotokolleintrag enthält Details zu einer einzelnen Zugriffsanfrage. Zu den Details gehören Auftraggeber, Bucket-Name, Anforderungszeit, Anforderungsaktion, Antwortstatus und Fehlercode, falls relevant.

Kontroll-ID	AWS Config	Empfehlungen
67	vpc-flow-logs-enabled	VPC-Flow-Protokolle erfassen detaillierte Informationsdatensätze über den IP-Datenverkehr, der zu und von Netzwerkschnittstellen in Ihrer Amazon Virtual Private Cloud (Amazon VPC) fließt. Standardmäßig enthalten Flow-Protokolldatensätze Werte für die verschiedenen Komponenten des IP-Flows, einschließlich Quelle, Ziel und Protokoll.
67	rds-logging-enabled	Um die Protokollierung und Überwachung in Ihrer Umgebung zu erleichtern, stellen Sie sicher, dass die Amazon Relational Database Service (Amazon RDS)-Protokollierung aktiviert ist. Mit der Amazon-RDS-Protokollierung können Sie Ereignisse wie Verbindungen, Verbindungsabbrüche, Abfragen oder abgefragte Tabellen erfassen.

Kontroll-ID	AWS Config	Empfehlungen
67	wafv2-logging-enabled	Um die Protokollierung und Überwachung in Ihrer Umgebung zu erleichte rn, aktivieren Sie die AWS WAF (V2) -Protokollierung im regionalen und globalen Web ACLs. AWS Die WAF-Protokollierung bietet detaillie rte Informationen über den Datenverkehr, der von Ihrer Web-ACL analysiert wird. In den Protokollen werden die Uhrzeit aufgezeichnet, zu der die AWS WAF die Anfrage von Ihrer AWS Ressource erhalten hat, Informationen über die Anfrage und eine Aktion für die Regel, der jede Anfrage entsprach.

Kontroll-ID	AWS Config	Empfehlungen
67	cloudwatch-alarm-action-check	Amazon CloudWatch alarmiert, wenn eine Metrik den Schwellenwert für eine bestimmte Anzahl von Bewertungszeiträumen überschreitet. Der Alarm führt eine oder mehrere Aktionen durch, die vom Wert der Metrik oder des Ausdrucks im Vergleich zu einem Schwellenwert in einer Reihe von Zeiträumen abhängt. Diese Regel erfordert einen Wert für alarmActionRequired (Config Default: True), insufficientDataActionRequired (Config Default: True), okActionRequired (Config Default: False). Der tatsächliche Wert muss die Alarmaktionen für Ihre Umgebung widerspiegeln.

Kontroll-ID	AWS Config	Empfehlungen
67	guardduty-enabled-centralized	Amazon GuardDuty kann mithilfe von Threat Intellige nce Feeds helfen, potenzielle Cybersicherheitsereignisse zu überwachen und zu erkennen. Dazu gehören Listen mit bösartigen IPs und maschinel len Lernmethoden zur Identifiz ierung unerwarteter, nicht autorisierter und bösartige r Aktivitäten in Ihrer AWS Cloud-Umgebung.
67	securityhub-enabled	AWS Security Hub hilft bei der Überwachung von unbefugte m Personal, Verbindungen, Geräten und Software. AWS Security Hub aggregiert, organisiert und priorisiert die Sicherheitswarnungen oder Ergebnisse mehrerer Dienste. AWS Einige dieser Dienste sind Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer und AWS Firewall Manager sowie AWS Partnerlösungen.

Kontroll-ID	AWS Config	Empfehlungen
67	opensearch-logs-to-cloudwatch	Stellen Sie sicher, dass für Amazon OpenSearch Service-Domains Fehlerprotokolle aktiviert und zur Aufbewahrung und Beantwortung an Amazon CloudWatch Logs gestreamt werden. OpenSearch Service-Fehlerprotokolle können bei Sicherheits- und Zugriffsprüfungen helfen und bei der Diagnose von Verfügbarkeitsproblemen helfen.
67	ec2-scheck managedinstance-patch-compliance-status	Aktivieren Sie diese Regel, um bei der Identifizierung und Dokumentation von Sicherheitslücken in Amazon Elastic Compute Cloud (Amazon EC2) zu helfen. Die Regel prüft, ob die EC2 Amazon-Instance die Patch-Konformität im AWS Systems Manager gemäß den Richtlinien und Verfahren Ihrer Organisation einhält.

Kontroll-ID	AWS Config	Empfehlungen
67	ec2-scheck managedinstance-association-compliance-status	Verwenden Sie AWS Systems Manager Associations, um bei der Inventarisierung von Softwareplattformen und Anwendungen innerhalb eines Unternehmens zu helfen. AWS Systems Manager weist Ihren verwalteten Instances einen Konfigurationsstatus zu und ermöglicht es Ihnen, Basiswerte für Betriebss ystem-Patch-Levels, Softwarei nstallationen, Anwendung skonfigurationen und andere Details zu Ihrer Umgebung festzulegen.

Kontroll-ID	AWS Config	Empfehlungen
67	redshift-cluster-configuration-check	Um Daten im Ruhezustand zu schützen, muss die Verschlüsselung für Ihre Amazon-Redshift-Cluster aktiviert sein. Sie müssen auch sicherstellen, dass die erforderlichen Konfigurationen auf Amazon-Redshift-Clustern bereitgestellt werden. Die Prüfungsprotokollierung muss aktiviert sein, um Informationen zu Verbindungen und Benutzeraktivitäten in der Datenbank bereitzustellen. Diese Regel erfordert, dass ein Wert für clusterDbEncrypted (Config Default: TRUE) und LoggingEnabled (Config Default: TRUE) gesetzt ist. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	AWS Config	Empfehlungen
67	elasticsearch-logs-to-cloudwatch	Stellen Sie sicher, dass für Amazon OpenSearch Service-Domains Fehlerprotokolle aktiviert und zur Aufbewahrung und Beantwortung an Amazon CloudWatch Logs gestreamt werden. Domain-Fehlerprotokolle sind bei Sicherheits- und Zugriffsprüfungen sowie bei der Diagnose von Verfügbarkeitsproblemen nützlich.
68	guardduty-enabled-centralized	Amazon GuardDuty kann mithilfe von Threat Intelligence Feeds helfen, potenzielle Cybersicherheitsereignisse zu überwachen und zu erkennen. Dazu gehören Listen mit bösartigen IPs und maschinellen Lernmethoden zur Identifizierung unerwarteter, nicht autorisierter und bösartiger Aktivitäten in Ihrer AWS Cloud-Umgebung.

Kontroll-ID	AWS Config	Empfehlungen
68	securityhub-enabled	AWS Security Hub hilft bei der Überwachung von unbefugte m Personal, Verbindungen, Geräten und Software. AWS Security Hub aggregiert, organisiert und priorisiert die Sicherheitswarnungen oder Ergebnisse mehrerer Dienste. AWS Einige dieser Dienste sind Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer und AWS Firewall Manager sowie AWS Partnerlösungen.
73	guardduty-enabled-centralized	Amazon GuardDuty kann mithilfe von Threat Intellige nce Feeds helfen, potenzielle Cybersicherheitsereignisse zu überwachen und zu erkennen. Dazu gehören Listen mit bösartigen IPs und maschinel len Lernmethoden zur Identifiz ierung unerwarteter, nicht autorisierter und bösartige r Aktivitäten in Ihrer AWS Cloud-Umgebung.

Kontroll-ID	AWS Config	Empfehlungen
73	securityhub-enabled	AWS Security Hub hilft bei der Überwachung von unbefugte m Personal, Verbindungen, Geräten und Software. AWS Security Hub aggregiert, organisiert und priorisiert die Sicherheitswarnungen oder Ergebnisse mehrerer Dienste. AWS Einige dieser Dienste sind Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer und AWS Firewall Manager sowie AWS Partnerlösungen.

Kontroll-ID	AWS Config	Empfehlungen
AttachmentA_1(b)(h)	emr-kerberos-enabled	Die Zugriffsberechtigungen und -autorisierungen können verwaltet und nach den Prinzipien der geringsten Berechtigung und Aufgabent rennung integriert werden, indem Kerberos für Amazon-EMR-Cluster aktiviert wird. In Kerberos werden Services und Benutzer, die sich authentifizieren müssen, als Prinzipale bezeichnet. Prinzipale befinden sich in einem Kerberos-Bereich. Innerhalb dieses Bereichs wird ein Kerberos-Server als Key Distribution Center (KDC) bezeichnet. Über diesen Server können sich Prinzipale authentifizieren. Die Authentifizierung im KDC erfolgt durch die Ausstellu ng von Authentifizierungs tickets. Das KDC unterhält eine Datenbank der Prinzipal e in seinem Bereich mit ihren Passwörtern und anderen administrativen Informationen zu jedem Prinzipal.

Kontroll-ID	AWS Config	Empfehlungen
AttachmentA_1(b)(h)	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) kann Ihnen dabei helfen, die Prinzipien der geringsten Rechte und der Aufgabent rennung in Zugriffsberechtigu ngen und Autorisierungen zu integrieren und so zu verhindern, dass Richtlinien „Effect“: „Allow“ mit „Action“: „*“ anstelle von „Resource“: „*“ enthalten. Wenn Benutzern mehr Rechte eingeräumt werden, als für die Ausführun g einer Aufgabe erforderl ich sind, kann dies gegen das Prinzip der geringste n Berechtigung und der Aufgabentrennung verstoßen.

Kontroll-ID	AWS Config	Empfehlungen
AttachmentA_1(b)(h)	iam-root-access-key-überprüfen	Der Zugriff auf Systeme und Ressourcen kann gesteuert werden, indem überprüft wird, ob der Root-Benutzer keine Zugriffsschlüssel mit seiner AWS Identity and Access Management (IAM) -Rolle verknüpft hat. Stellen Sie sicher, dass die Root-Zugriffsschlüssel gelöscht werden. Erstellen und verwenden Sie stattdessen rollenbasierte Funktionen, AWS-Konten um das Prinzip der geringsten Funktionalität zu berücksichtigen.
AttachmentA_1(b)(h)	iam-user-group-membership-überprüfen	AWS Identity and Access Management (IAM) kann Ihnen helfen, Zugriffsberechtigungen und Autorisierungen einzuschränken, indem sichergestellt wird, dass Benutzer Mitglieder mindestens einer Gruppe sind. Wenn Benutzern mehr Berechtigungen eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und Aufgabentrennung verstoßen.

Kontroll-ID	AWS Config	Empfehlungen
AttachmentA_1(b)(h)	iam-user-unused-credentials-überprüfen	AWS Identity and Access Management (IAM) kann Ihnen bei Zugriffsberechtigungen und Autorisierungen helfen, indem es nach IAM-Passwörtern und Zugriffsschlüsseln sucht, die für einen bestimmten Zeitraum nicht verwendet wurden. Wenn ungenutzte Anmeldeinformationen identifiziert werden, müssen Sie sie deaktivieren und/oder entfernen, da dies gegen das Prinzip der geringsten Berechtigung verstoßen könnte. Für diese Regel müssen Sie einen Wert für das maxCredentialUsage Alter festlegen (Standardkonfiguration: 90). Der tatsächliche Wert muss den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	AWS Config	Empfehlungen
AttachmentA_1(b)(h)	iam-no-inline-policy-überprüfen	Stellen Sie sicher, dass ein Benutzer, eine IAM-Rolle oder eine IAM-Gruppe (AWS Identity and Access Management) nicht über eine Inline-Richtlinie zur Zugriffskontrolle auf Systeme und Ressourcen verfügt. AWS empfiehlt, verwaltete Richtlinien anstelle von Inline-Richtlinien zu verwenden . Verwaltete Richtlinien ermöglichen Wiederverwendbarkeit, Versionsverwaltung, Rollback und Delegierung der Berechtigungsverwaltung.

Kontroll-ID	AWS Config	Empfehlungen
AttachmentA_1(b)(h)	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) kann Ihnen helfen, die Prinzipien der geringsten Rechte und der Aufgabentrennung in Zugriffsberechtigungen und Autorisierungen zu integrier en und so zu verhindern, dass Richtlinien blockierte Aktionen für alle AWS Schlüssel des Key Management Service enthalten. Wenn Benutzer mehr Rechte haben, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtig ung und Aufgabentrennung verstoßen. Mit dieser Regel können Sie den Parameter festlegen. blockedActionsPatt erns (Wert „AWS Bewährte grundlegende Sicherhei tsmethoden“: kms: Decrypt, kms:ReEncryptFrom). Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisat ion entsprechen.

Kontroll-ID	AWS Config	Empfehlungen
AttachmentA_1(b)(h)	iam-inline-policy-blocked-kms-Aktionen	Stellen Sie sicher, dass ein Benutzer, eine IAM-Rolle oder eine IAM-Grupp e (AWS Identity and Access Management) nicht über eine Inline-Richtlinie verfügt, die blockierte Aktionen für alle AWS Schlüssel des Key Management Service zulässt. AWS empfiehlt, verwaltete Richtlinien anstelle von Inline-Richtlinien zu verwenden . Verwaltete Richtlinien ermöglichen Wiederver wendbarkeit, Versionsv erwaltung, Rollback und Delegierung der Berechtig ungsverwaltung. Mit dieser Regel können Sie den blockedActionsPatterns Parameter festlegen. (Wert „AWS Bewährte grundlege nde Sicherheitsmethoden“: kms: Decrypt, kms:ReEnc ryptFrom). Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprech en.

Kontroll-ID	AWS Config	Empfehlungen
AttachmentA_1(b)(h)	iam-policy-no-statements-with-full-access	Stellen Sie sicher, dass IAM-Aktionen nur auf die benötigte n Aktionen beschränkt sind. Wenn Benutzern mehr Rechte eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und der Aufgabentrennung verstoßen.
AttachmentA_1(b)(h)	ec-2 instance-profile-attached	EC2 Instanzprofile übergeben eine IAM-Rolle an eine EC2 Instance. Das Anhängen eines Instance-Profils an Ihre Instances kann bei der Implementierung von geringsten Berechtigungen und der Berechtigungsverwa ltung helfen.

Kontroll-ID	AWS Config	Empfehlungen
AttachmentA_1(c)	securityhub-enabled	AWS Security Hub hilft bei der Überwachung von unbefugte m Personal, Verbindungen, Geräten und Software. AWS Security Hub aggregiert, organisiert und priorisiert die Sicherheitswarnungen oder Ergebnisse mehrerer Dienste. AWS Einige dieser Dienste sind Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer und AWS Firewall Manager sowie AWS Partnerlösungen.
AttachmentA_1(c)	guardduty-enabled-centralized	Amazon GuardDuty kann mithilfe von Threat Intellige nce Feeds helfen, potenzielle Cybersicherheitsereignisse zu überwachen und zu erkennen. Dazu gehören Listen mit bösartigen IPs und maschinel len Lernmethoden zur Identifiz ierung unerwarteter, nicht autorisierter und bösartige r Aktivitäten in Ihrer AWS Cloud-Umgebung.

Kontroll-ID	AWS Config	Empfehlungen
AttachmentA_1(e)	securityhub-enabled	AWS Security Hub hilft bei der Überwachung von unbefugte m Personal, Verbindungen, Geräten und Software. AWS Security Hub aggregiert, organisiert und priorisiert die Sicherheitswarnungen oder Ergebnisse mehrerer Dienste. AWS Einige dieser Dienste sind Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer und AWS Firewall Manager sowie AWS Partnerlösungen.
AttachmentA_1(e)	guardduty-enabled-centralized	Amazon GuardDuty kann mithilfe von Threat Intellige nce Feeds helfen, potenzielle Cybersicherheitsereignisse zu überwachen und zu erkennen. Dazu gehören Listen mit bösartigen IPs und maschinel len Lernmethoden zur Identifiz ierung unerwarteter, nicht autorisierter und bösartige r Aktivitäten in Ihrer AWS Cloud-Umgebung.

Kontroll-ID	AWS Config	Empfehlungen
AttachmentA_1(e)	cloudwatch-alarm-action-check	Amazon CloudWatch alarmiert, wenn eine Metrik den Schwellenwert für eine bestimmte Anzahl von Bewertungszeiträumen überschreitet. Der Alarm führt eine oder mehrere Aktionen durch, die vom Wert der Metrik oder des Ausdrucks im Vergleich zu einem Schwellenwert in einer Reihe von Zeiträumen abhängt. Diese Regel erfordert einen Wert für alarmActionRequired (Config Default: True), insufficientDataActionRequired (Config Default: True), okActionRequired (Config Default: False). Der tatsächliche Wert muss die Alarmaktionen für Ihre Umgebung widerspiegeln.
AttachmentA_1(e)	api-gw-execution-logging-aktiviert	Die API-Gateway-Protokollierung zeigt detaillierte Ansichten der Benutzer, die auf die API zugegriffen haben, und wie diese Benutzer auf die API zugegriffen haben. Diese Einblicke ermöglichen die Transparenz von Benutzeraktivitäten.

Kontroll-ID	AWS Config	Empfehlungen
AttachmentA_1(e)	cloud-trail-cloud-watch-logs-aktiviert	Verwenden Sie Amazon CloudWatch , um Protokoll ereignisaktivitäten zentral zu sammeln und zu verwalten . Die Aufnahme von AWS CloudTrail Daten liefert Einzelheiten zu den API-Aufru faktivitäten in Ihrem AWS-Konto.
AttachmentA_1(e)	cloudtrail-enabled	AWS CloudTrail kann bei der Nichtabstreitbarkeit helfen, indem Aktionen und API-Aufrufe der AWS Managemen t Console aufgezeichnet werden. Sie können die Benutzer und die Benutzer AWS-Konten , die einen AWS Dienst aufgerufen haben, die Quell-IP-Adresse, über die die Aufrufe generiert wurden, und den Zeitpunkt der Anrufe identifizieren. Einzelheiten zu den erfassten Daten finden Sie in den AWS CloudTrail Datensatzinhalten.

Kontroll-ID	AWS Config	Empfehlungen
AttachmentA_1(e)	cloudtrail-s3-dataevents-enabled	Die Erfassung von Simple Storage Service (Amazon S3)-Datenereignissen unterstützt die Erkennung von ungewöhnlichen Aktivitäten. Zu den Details gehören Informationen zu dem AWS -Konto, das auf einen Amazon-S3-Bucket zugegriffen hat, die IP-Adresse und die Uhrzeit des Ereignisses.
AttachmentA_1(e)	elb-logging-enabled	Die Elastic-Load-Balancing-Aktivität ist ein zentraler Kommunikationspunkt innerhalb einer Umgebung. Stellen Sie sicher, dass die ELB-Protokollierung aktiviert ist. Die gesammelten Daten enthalten detaillierte Informationen zu Anfragen, die an den ELB gesendet wurden. Jedes Protokoll enthält Informationen wie die Zeit, zu der die Anforderung einging, die Client-IP-Adresse, Latenzen, Anforderungspfade und Serverantworten.

Kontroll-ID	AWS Config	Empfehlungen
AttachmentA_1(e)	multi-region-cloudtrail-enabled	AWS CloudTrail zeichnet Aktionen und API-Aufrufe der AWS Management Console auf. Sie können feststellen, welche Benutzer und Konten angerufen wurden AWS, von welcher Quell-IP-Adresse aus die Anrufe getätigt wurden und wann die Anrufe erfolgten . CloudTrail übermittelt Protokolldateien aus allen AWS Regionen an Ihren S3-Bucket, wenn MULTI_REG ION_CLOUD_TRAIL_EN ABLED aktiviert ist. Außerdem wird beim AWS Start einer neuen Region derselbe Trail in der neuen Region erstellt. CloudTrail Dadurch erhalten Sie automatisch Protokoll dateien mit API-Aktivitäten für die neue Region.

Kontroll-ID	AWS Config	Empfehlungen
AttachmentA_1(e)	s-3 bucket-logging-enabled	Die Amazon Simple Storage Service (Amazon S3)-Serverzugriffsprotokollierung bietet eine Methode zur Überwachung des Netzwerks im Hinblick auf potenzielle Cybersicherheitsereignisse. Die Ereignisse werden überwacht, indem detaillierte Aufzeichnungen über die Anfragen erfasst werden, die an einen Amazon-S3-Bucket gestellt wurden. Jeder Zugriffsprotokolleintrag enthält Details zu einer einzelnen Zugriffsanfrage. Zu den Details gehören Auftraggeber, Bucket-Name, Anforderungszeit, Anforderungsaktion, Antwortstatus und Fehlercode, falls relevant.

Kontroll-ID	AWS Config	Empfehlungen
AttachmentA_1(e)	vpc-flow-logs-enabled	VPC-Flow-Protokolle erfassen detaillierte Informationsdatensätze über den IP-Datenverkehr, der zu und von Netzwerkschnittstellen in Ihrer Amazon Virtual Private Cloud (Amazon VPC) fließt. Standardmäßig enthalten Flow-Protokolldatensätze Werte für die verschiedenen Komponenten des IP-Flows, einschließlich Quelle, Ziel und Protokoll.
AttachmentA_1(e)	rds-logging-enabled	Um die Protokollierung und Überwachung in Ihrer Umgebung zu erleichtern, stellen Sie sicher, dass die Amazon Relational Database Service (Amazon RDS)-Protokollierung aktiviert ist. Mit der Amazon-RDS-Protokollierung können Sie Ereignisse wie Verbindungen, Verbindungsabbrüche, Abfragen oder abgefragte Tabellen erfassen.

Kontroll-ID	AWS Config	Empfehlungen
AttachmentA_1(e)	wafv2-logging-enabled	Um die Protokollierung und Überwachung in Ihrer Umgebung zu erleichte rn, aktivieren Sie die AWS WAF (V2) -Protokollierung im regionalen und globalen Web ACLs. AWS Die WAF-Protokollierung bietet detaillie rte Informationen über den Datenverkehr, der von Ihrer Web-ACL analysiert wird. In den Protokollen werden die Uhrzeit aufgezeichnet, zu der die AWS WAF die Anfrage von Ihrer AWS Ressource erhalten hat, Informationen über die Anfrage und eine Aktion für die Regel, der jede Anfrage entsprach.
AttachmentA_1(e)	elasticsearch-logs-to-cloud watch	Stellen Sie sicher, dass für Amazon OpenSearch Service-Domains Fehlerprotokolle aktiviert und zur Aufbewahr ung und Beantwortung an Amazon CloudWatch Logs gestreamt werden. Domain-Fehlerprotokolle sind bei Sicherheits- und Zugriffsp rüfungen sowie bei der Diagnose von Verfügbar keitsproblemen nützlich.

Kontroll-ID	AWS Config	Empfehlungen
AttachmentA_1(e)	opensearch-logs-to-cloudwatch	Stellen Sie sicher, dass für Amazon OpenSearch Service-Domains Fehlerprotokolle aktiviert und zur Aufbewahrung und Beantwortung an Amazon CloudWatch Logs gestreamt werden. OpenSearch Service-Fehlerprotokolle können bei Sicherheits- und Zugriffsprüfungen helfen und bei der Diagnose von Verfügbarkeitsproblemen helfen.
AttachmentB_1	security-awareness-program-exists (Prozessüberprüfung)	Etablieren und pflegen Sie ein Programm zur Förderung des Sicherheitsbewusstseins in Ihrer Organisation. Programme zur Förderung des Sicherheitsbewusstseins der Mitarbeiter vermitteln ihnen, wie sie die Organisation vor diversen Sicherheitsverletzungen oder Sicherheitsvorfällen schützen können.

Kontroll-ID	AWS Config	Empfehlungen
AttachmentC_4	access-keys-rotated	Die Anmeldeinformationen für autorisierte Geräte, Benutzer und Prozesse werden geprüft, indem sichergestellt wird, dass die IAM-Zugriffsschlüssel gemäß den Vorgaben der Unternehmensrichtlinie rotiert werden. Das regelmäßige Ändern der Zugriffsschlüssel ist eine bewährte Sicherheitsmethode. Es verkürzt den Zeitraum, in dem ein Zugriffsschlüssel aktiv ist, und reduziert die Auswirkungen auf das Unternehmen, wenn die Schlüssel kompromittiert werden. Diese Regel erfordert einen Wert für die Zugriffsschlüssel-Rotation (Standardkonfiguration: 90). Der tatsächliche Wert muss den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	AWS Config	Empfehlungen
AttachmentC_4	emr-kerberos-enabled	Die Zugriffsberechtigungen und -autorisierungen können verwaltet und nach den Prinzipien der geringsten Berechtigung und Aufgabent rennung integriert werden, indem Kerberos für Amazon-EMR-Cluster aktiviert wird. In Kerberos werden Services und Benutzer, die sich authentifizieren müssen, als Prinzipale bezeichnet. Prinzipale befinden sich in einem Kerberos-Bereich. Innerhalb dieses Bereichs wird ein Kerberos-Server als Key Distribution Center (KDC) bezeichnet. Über diesen Server können sich Prinzipale authentifizieren. Die Authentifizierung im KDC erfolgt durch die Ausstellu ng von Authentifizierungs tickets. Das KDC unterhält eine Datenbank der Prinzipal e in seinem Bereich mit ihren Passwörtern und anderen administrativen Informationen zu jedem Prinzipal.

Kontroll-ID	AWS Config	Empfehlungen
AttachmentC_4	iam-password-policy	Die Identitäten und Anmeldein formationen werden auf der Grundlage einer organisat orischen IAM-Passwortrichtl inie ausgestellt, verwaltet und verifiziert. Sie erfüllen oder übertreffen die Anforderu ngen von NIST SP 800-63 und dem Standard „Best Practices“ von AWS Foundatio nal Security in Bezug auf die Passwortstärke. Mit dieser Regel können Sie optional RequireUppercaseCharacters (Wert für AWS grundlege nde Sicherheitsbewährte Verfahren: wahr), RequireLo wercaseCharacters (Wert für bewährte Methoden für AWS grundlegende Sicherheit: wahr), RequireSymbols (Wert für bewährte Methoden für AWS grundlegende Sicherhei t: wahr), RequireNumbers (Wert für bewährte Methoden für AWS grundlegende Sicherheit: wahr), MinimumPa sswordLength (Wert für bewährte Methoden für AWS grundlegende Sicherheit: 14), PasswordReusePreve ntion (Wert für bewährte Methoden für AWS grundlege nde Sicherheit: 24) und

Kontroll-ID	AWS Config	Empfehlungen
		MaxPasswordAge (Wert für bewährte Methoden für AWS grundlegende Sicherheit: 90) für Ihr IAM festlegen Kennwortrichtlinie. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.
AttachmentC_4	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) kann Ihnen dabei helfen, die Prinzipien der geringsten Rechte und der Aufgabentrennung in Zugriffsberechtigungen und Autorisierungen zu integrieren und so zu verhindern, dass Richtlinien „Effect“: „Allow“ mit „Action“: „*“ anstelle von „Resource“: „*“ enthalten. Wenn Benutzern mehr Rechte eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und der Aufgabentrennung verstoßen.

Kontroll-ID	AWS Config	Empfehlungen
AttachmentC_4	iam-root-access-key-überprüfen	Der Zugriff auf Systeme und Ressourcen kann gesteuert werden, indem überprüft wird, ob der Root-Benutzer keine Zugriffsschlüssel mit seiner AWS Identity and Access Management (IAM) -Rolle verknüpft hat. Stellen Sie sicher, dass die Root-Zugriffsschlüssel gelöscht werden. Erstellen und verwenden Sie stattdessen rollenbasierte Funktionen, AWS-Konten um das Prinzip der geringsten Funktionalität zu berücksichtigen.
AttachmentC_4	iam-user-group-membership-überprüfen	AWS Identity and Access Management (IAM) kann Ihnen helfen, Zugriffsberechtigungen und Autorisierungen einzuschränken, indem sichergestellt wird, dass Benutzer Mitglieder mindestens einer Gruppe sind. Wenn Benutzern mehr Berechtigungen eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und Aufgabentrennung verstoßen.

Kontroll-ID	AWS Config	Empfehlungen
AttachmentC_4	iam-user-mfa-enabled	Aktivieren Sie diese Regel, um den Zugriff auf Ressourcen in der AWS -Cloud einzuschränken. Diese Regel stellt sicher, dass die Multi-Faktor-Authentifizierung (MFA) für alle Benutzer aktiviert ist. MFA bietet eine weitere Schutzebene zusätzlich zum Benutzernamen und Passwort. Reduzieren Sie Fälle von kompromittierten Konten, indem Sie MFA für Benutzer vorschreiben.
AttachmentC_4	iam-user-no-policies-überprüfen	Diese Regel stellt sicher, dass AWS Identity and Access Management (IAM) -Richtlinien nur Gruppen oder Rollen zugewiesen werden, um den Zugriff auf Systeme und Ressourcen zu kontrollieren. Die Zuweisung von Berechtigungen auf Gruppen- oder Rollenebene trägt dazu bei, die Wahrscheinlichkeit zu verringern, dass eine Identität übermäßige Berechtigungen erhält oder beibehält.

Kontroll-ID	AWS Config	Empfehlungen
AttachmentC_4	iam-user-unused-credentials-überprüfen	AWS Identity and Access Management (IAM) kann Ihnen bei Zugriffsberechtigungen und Autorisierungen helfen, indem es nach IAM-Passwörtern und Zugriffsschlüsseln sucht, die für einen bestimmten Zeitraum nicht verwendet wurden. Wenn ungenutzte Anmeldeinformationen identifiziert werden, müssen Sie sie deaktivieren und/oder entfernen, da dies gegen das Prinzip der geringsten Berechtigung verstoßen könnte. Für diese Regel müssen Sie einen Wert für das maxCredentialUsage Alter festlegen (Standardkonfiguration: 90). Der tatsächliche Wert muss den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	AWS Config	Empfehlungen
AttachmentC_4	mfa-enabled-for-iam-Konsolenzugriff	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass MFA für alle AWS Identity and Access Management (IAM) -Benutzer aktiviert ist, die über ein Konsolenkennwort verfügen. MFA sorgt für eine weitere Schutzebene zusätzlich zu den Anmeldeinformationen. Indem Sie MFA für Benutzer vorschreiben, können Sie Fälle kompromittierter Konten reduzieren und verhindern, dass unbefugte Benutzer auf vertrauliche Daten zugreifen.
AttachmentC_4	root-account-hardware-mfa-aktiviert	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Hardware-MFA für den Root-Benutzer aktiviert ist. Der Stammbenutzer ist der AWS-Konto-Benutzer mit den meisten Berechtigungen. MFA sorgt für eine weitere Schutzebene zusätzlich zu den Anmeldeinformationen. Indem Sie MFA für den Root-Benutzer vorschreiben, können Sie die Anzahl AWS-Konten kompromittierter Benutzer reduzieren.

Kontroll-ID	AWS Config	Empfehlungen
AttachmentC_4	root-account-mfa-enabled	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass MFA für den Root-Benutzer aktiviert ist. Der Stammbenutzer ist der AWS-Konto-Benutzer mit den meisten Berechtigungen. MFA bietet eine weitere Schutzebene zusätzlich zum Benutzernamen und Passwort. Indem Sie MFA für den Root-Benutzer vorschreiben, können Sie die Anzahl AWS-Konten kompromittierter Benutzer reduzieren.
AttachmentC_4	secretsmanager-rotation-enabled-check	Diese Regel stellt sicher, dass bei AWS Secrets Manager Manager-Geheimnissen die Rotation aktiviert ist. Die regelmäßige Rotation von Secrets kann den Zeitraum verkürzen, in dem ein Secret aktiv ist, und möglicherweise die Auswirkungen auf das Unternehmen verringern, falls das Secret kompromittiert wird.

Kontroll-ID	AWS Config	Empfehlungen
AttachmentC_4	secretsmanager-scheduled-rotation-success-überprüfen	Diese Regel stellt sicher, dass AWS Secrets Manager Manager-Geheimnisse gemäß dem Rotationsplan erfolgreich rotiert wurden. Die regelmäßige Rotation von Secrets kann den Zeitraum verkürzen, in dem ein Secret aktiv ist, und möglicherweise die Auswirkungen auf das Unternehmen verringern, falls es kompromittiert wird.
AttachmentC_4	iam-no-inline-policy-überprüfen	Stellen Sie sicher, dass ein Benutzer, eine IAM-Rolle oder eine IAM-Gruppe (AWS Identity and Access Management) nicht über eine Inline-Richtlinie zur Zugriffskontrolle auf Systeme und Ressourcen verfügt. AWS empfiehlt, verwaltete Richtlinien anstelle von Inline-Richtlinien zu verwenden . Verwaltete Richtlinien ermöglichen Wiederverwendbarkeit, Versionsverwaltung, Rollback und Delegierung der Berechtigungsverwaltung.

Kontroll-ID	AWS Config	Empfehlungen
AttachmentC_4	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) kann Ihnen helfen, die Prinzipien der geringsten Rechte und der Aufgabentrennung in Zugriffsberechtigungen und Autorisierungen zu integrier en und so zu verhindern, dass Richtlinien blockierte Aktionen für alle AWS Schlüssel des Key Management Service enthalten. Wenn Benutzer mehr Rechte haben, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtig ung und Aufgabentrennung verstoßen. Mit dieser Regel können Sie den Parameter festlegen. blockedActionsPatt erns (Wert „AWS Bewährte grundlegende Sicherhei tsmethoden“: kms: Decrypt, kms:ReEncryptFrom). Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisat ion entsprechen.

Kontroll-ID	AWS Config	Empfehlungen
AttachmentC_4	iam-inline-policy-blocked-kms-Aktionen	Stellen Sie sicher, dass ein Benutzer, eine IAM-Rolle oder eine IAM-Grupp e (AWS Identity and Access Management) nicht über eine Inline-Richtlinie verfügt, die blockierte Aktionen für alle AWS Schlüssel des Key Management Service zulässt. AWS empfiehlt, verwaltete Richtlinien anstelle von Inline-Richtlinien zu verwenden . Verwaltete Richtlinien ermöglichen Wiederver wendbarkeit, Versionsv erwaltung, Rollback und Delegierung der Berechtig ungsverwaltung. Mit dieser Regel können Sie den blockedActionsPatterns Parameter festlegen. (Wert „AWS Bewährte grundlege nde Sicherheitsmethoden“: kms: Decrypt, kms:ReEnc ryptFrom). Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprech en.

Kontroll-ID	AWS Config	Empfehlungen
AttachmentC_4	ec-2 instance-profile-attached	EC2 Instanzprofile übergeben eine IAM-Rolle an eine EC2 Instance. Das Anhängen eines Instance-Profils an Ihre Instances kann bei der Implementierung von geringsten Berechtigungen und der Berechtigungsverwa ltung helfen.
AttachmentC_4	iam-policy-no-statements-with-full-access	Stellen Sie sicher, dass IAM-Aktionen nur auf die benötigte n Aktionen beschränkt sind. Wenn Benutzern mehr Rechte eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und der Aufgabentrennung verstoßen.

Kontroll-ID	AWS Config	Empfehlungen
AttachmentC_5	mfa-enabled-for-iam-Konsolenzugriff	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass MFA für alle AWS Identity and Access Management (IAM) -Benutzer aktiviert ist, die über ein Konsolenkennwort verfügen. MFA sorgt für eine weitere Schutzebene zusätzlich zu den Anmeldeinformationen. Indem Sie MFA für Benutzer vorschreiben, können Sie Fälle kompromittierter Konten reduzieren und verhindern, dass unbefugte Benutzer auf vertrauliche Daten zugreifen.
AttachmentC_5	root-account-hardware-mfa-aktiviert	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Hardware-MFA für den Root-Benutzer aktiviert ist. Der Stammbenutzer ist der AWS-Konto-Benutzer mit den meisten Berechtigungen. MFA sorgt für eine weitere Schutzebene zusätzlich zu den Anmeldeinformationen. Indem Sie MFA für den Root-Benutzer vorschreiben, können Sie die Anzahl AWS-Konten kompromittierter Benutzer reduzieren.

Kontroll-ID	AWS Config	Empfehlungen
AttachmentC_5	root-account-mfa-enabled	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass MFA für den Root-Benutzer aktiviert ist. Der Stammbenutzer ist der AWS-Konto-Benutzer mit den meisten Berechtigungen. MFA bietet eine weitere Schutzebene zusätzlich zum Benutzernamen und Passwort. Indem Sie MFA für den Root-Benutzer vorschreiben, können Sie die Anzahl AWS-Konten kompromittierter Benutzer reduzieren.
AttachmentC_5	iam-user-no-policies-überprüfen	Diese Regel stellt sicher, dass AWS Identity and Access Management (IAM) -Richtlinien nur Gruppen oder Rollen zugewiesen werden, um den Zugriff auf Systeme und Ressourcen zu kontrollieren. Die Zuweisung von Berechtigungen auf Gruppen- oder Rollenebene trägt dazu bei, die Wahrscheinlichkeit zu verringern, dass eine Identität übermäßige Berechtigungen erhält oder beibehält.

Kontroll-ID	AWS Config	Empfehlungen
AttachmentC_5	iam-password-policy	Die Identitäten und Anmeldein formationen werden auf der Grundlage einer organisat orischen IAM-Passwortrichtl inie ausgestellt, verwaltet und verifiziert. Sie erfüllen oder übertreffen die Anforderungen von NIST SP 800-63 und dem Standard „Best Practices“ von AWS Foundational Security für die Passwortstärke. Mit dieser Regel können Sie optional RequireUppercaseCharacters (Wert für AWS grundlege nde Sicherheitsbewährte Verfahren: wahr), RequireLo wercaseCharacters (Wert für bewährte Methoden für AWS grundlegende Sicherheit: wahr), RequireSymbols (Wert für bewährte Methoden für AWS grundlegende Sicherhei t: wahr), RequireNumbers (Wert für bewährte Methoden für AWS grundlegende Sicherheit: wahr), MinimumPa sswordLength (Wert für bewährte Methoden für AWS grundlegende Sicherheit: 14), PasswordReusePreve ntion (Wert für bewährte Methoden für AWS grundlege nde Sicherheit: 24) und MaxPasswordAge (Wert

Kontroll-ID	AWS Config	Empfehlungen
		für bewährte Methoden für AWS grundlegende Sicherhei t: 90) für Ihr IAM festlegen Kennwortrichtlinie. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisat ion entsprechen.
AttachmentC_6	root-account-hardware-mfa-a ktiviert	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherste llen, dass Hardware-MFA für den Root-Benutzer aktiviert ist. Der Stammbenutzer ist der AWS-Konto-Benutzer mit den meisten Berechtig ungen. MFA sorgt für eine weitere Schutzebene zusätzlic h zu den Anmeldeinformation en. Indem Sie MFA für den Root-Benutzer vorschrei ben, können Sie die Anzahl AWS-Konten kompromittierter Benutzer reduzieren.

Kontroll-ID	AWS Config	Empfehlungen
AttachmentC_6	root-account-mfa-enabled	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass MFA für den Root-Benutzer aktiviert ist. Der Stammbenutzer ist der AWS-Konto-Benutzer mit den meisten Berechtigungen. MFA bietet eine weitere Schutzebene zusätzlich zum Benutzernamen und Passwort. Indem Sie MFA für den Root-Benutzer vorschreiben, können Sie die Anzahl AWS-Konten kompromittierter Benutzer reduzieren.
AttachmentC_6	iam-root-access-key-überprüfen	Der Zugriff auf Systeme und Ressourcen kann gesteuert werden, indem überprüft wird, ob der Root-Benutzer keine Zugriffsschlüssel mit seiner AWS Identity and Access Management (IAM) -Rolle verknüpft hat. Stellen Sie sicher, dass die Root-Zugriffsschlüssel gelöscht werden. Erstellen und verwenden Sie stattdessen rollenbasierte Funktionen, AWS-Konten um das Prinzip der geringsten Funktionalität zu berücksichtigen.

Kontroll-ID	AWS Config	Empfehlungen
AttachmentC_7(c)	iam-root-access-key-überprüfen	Der Zugriff auf Systeme und Ressourcen kann gesteuert werden, indem überprüft wird, ob der Root-Benutzer keine Zugriffsschlüssel mit seiner AWS Identity and Access Management (IAM) -Rolle verknüpft hat. Stellen Sie sicher, dass die Root-Zugriffsschlüssel gelöscht werden. Erstellen und verwenden Sie stattdessen rollenbasierte Funktionen, AWS-Konten um das Prinzip der geringsten Funktionalität zu berücksichtigen.
AttachmentC_7(h)	api-gw-execution-logging-aktiviert	Die API-Gateway-Protokollierung zeigt detaillierte Ansichten der Benutzer, die auf die API zugegriffen haben, und wie diese Benutzer auf die API zugegriffen haben. Diese Einblicke ermöglichen die Transparenz von Benutzeraktivitäten.

Kontroll-ID	AWS Config	Empfehlungen
AttachmentC_7(h)	cloud-trail-cloud-watch-logs-aktiviert	Verwenden Sie Amazon CloudWatch , um Protokoll ereignisaktivitäten zentral zu sammeln und zu verwalten . Die Aufnahme von AWS CloudTrail Daten liefert Einzelheiten zu den API-Aufru faktivitäten in Ihrem AWS-Konto.
AttachmentC_7(h)	cloudtrail-enabled	AWS CloudTrail kann bei der Nichtabstreitbarkeit helfen, indem Aktionen und API-Aufrufe der AWS Managemen t Console aufgezeichnet werden. Sie können die Benutzer und die Benutzer AWS-Konten , die einen AWS Dienst aufgerufen haben, die Quell-IP-Adresse, über die die Aufrufe generiert wurden, und den Zeitpunkt der Anrufe identifizieren. Einzelheiten zu den erfassten Daten finden Sie in den AWS CloudTrail Datensatzinhalten.

Kontroll-ID	AWS Config	Empfehlungen
AttachmentC_7(h)	cloudtrail-s3-dataevents-enabled	Die Erfassung von Simple Storage Service (Amazon S3)-Datenereignissen unterstützt die Erkennung von ungewöhnlichen Aktivitäten. Zu den Details gehören Informationen zu dem AWS -Konto, das auf einen Amazon-S3-Bucket zugegriffen hat, die IP-Adresse und die Uhrzeit des Ereignisses.
AttachmentC_7(h)	cloudwatch-alarm-action-check	Amazon CloudWatch alarmiert, wenn eine Metrik den Schwellenwert für eine bestimmte Anzahl von Bewertungszeiträumen überschreitet. Der Alarm führt eine oder mehrere Aktionen durch, die vom Wert der Metrik oder des Ausdrucks im Vergleich zu einem Schwellenwert in einer Reihe von Zeiträumen abhängt. Diese Regel erfordert einen Wert für alarmActionRequired (Config Default: True), insufficientDataActionRequired (Config Default: True), okActionRequired (Config Default: False). Der tatsächliche Wert muss die Alarmaktionen für Ihre Umgebung widerspiegeln.

Kontroll-ID	AWS Config	Empfehlungen
AttachmentC_7(h)	elb-logging-enabled	Die Elastic-Load-Balancing-Aktivität ist ein zentraler Kommunikationspunkt innerhalb einer Umgebung. Stellen Sie sicher, dass die ELB-Protokollierung aktiviert ist. Die gesammelten Daten enthalten detaillierte Informati onen zu Anfragen, die an den ELB gesendet wurden. Jedes Protokoll enthält Informati onen wie die Zeit, zu der die Anforderung einging, die Client-IP-Adresse, Latenzen, Anforderungspfade und Serverantworten.
AttachmentC_7(h)	guardduty-enabled-centralized	Amazon GuardDuty kann mithilfe von Threat Intellige nce Feeds helfen, potenzielle Cybersicherheitsereignisse zu überwachen und zu erkennen. Dazu gehören Listen mit bösartigen IPs und maschinel len Lernmethoden zur Identifiz ierung unerwarteter, nicht autorisierter und bösartige r Aktivitäten in Ihrer AWS Cloud-Umgebung.

Kontroll-ID	AWS Config	Empfehlungen
AttachmentC_7(h)	multi-region-cloudtrail-enabled	AWS CloudTrail zeichnet Aktionen und API-Aufrufe der AWS Management Console auf. Sie können feststellen, welche Benutzer und Konten angerufen wurden AWS, von welcher Quell-IP-Adresse aus die Anrufe getätigt wurden und wann die Anrufe erfolgten . CloudTrail übermittelt Protokolldateien aus allen AWS Regionen an Ihren S3-Bucket, wenn MULTI_REGION_CLOUD_TRAIL_ENABLED aktiviert ist. Außerdem wird beim AWS Start einer neuen Region derselbe Trail in der neuen Region erstellt. CloudTrail Dadurch erhalten Sie automatisch Protokoll dateien mit API-Aktivitäten für die neue Region.

Kontroll-ID	AWS Config	Empfehlungen
AttachmentC_7(h)	s-3 bucket-logging-enabled	Die Amazon Simple Storage Service (Amazon S3)-Serverzugriffsprotokollierung bietet eine Methode zur Überwachung des Netzwerks im Hinblick auf potenzielle Cybersicherheitsereignisse. Die Ereignisse werden überwacht, indem detaillierte Aufzeichnungen über die Anfragen erfasst werden, die an einen Amazon-S3-Bucket gestellt wurden. Jeder Zugriffsprotokolleintrag enthält Details zu einer einzelnen Zugriffsanfrage. Zu den Details gehören Auftraggeber, Bucket-Name, Anforderungszeit, Anforderungsaktion, Antwortstatus und Fehlercode, falls relevant.

Kontroll-ID	AWS Config	Empfehlungen
AttachmentC_7(h)	securityhub-enabled	AWS Security Hub hilft bei der Überwachung von unbefugte m Personal, Verbindungen, Geräten und Software. AWS Security Hub aggregiert, organisiert und priorisiert die Sicherheitswarnungen oder Ergebnisse mehrerer Dienste. AWS Einige dieser Dienste sind Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer und AWS Firewall Manager sowie AWS Partnerlösungen.
AttachmentC_7(h)	vpc-flow-logs-enabled	VPC-Flow-Protokolle erfassen detaillierte Informationsdatens ätze über den IP-Datenv erkehr, der zu und von Netzwerkschnittstellen in Ihrer Amazon Virtual Private Cloud (Amazon VPC) fließt. Standardmäßig enthalten Flow-Protokolldatensätze Werte für die verschiedenen Komponenten des IP-Flows, einschließlich Quelle, Ziel und Protokoll.

Kontroll-ID	AWS Config	Empfehlungen
AttachmentC_7(h)	rds-logging-enabled	Um die Protokollierung und Überwachung in Ihrer Umgebung zu erleichtern, stellen Sie sicher, dass die Amazon Relational Database Service (Amazon RDS)-Protokollierung aktiviert ist. Mit der Amazon-RDS-Protokollierung können Sie Ereignisse wie Verbindungen, Verbindungsabbrüche, Abfragen oder abgefragte Tabellen erfassen.
AttachmentC_7(h)	opensearch-logs-to-cloudwatch	Stellen Sie sicher, dass für Amazon OpenSearch Service-Domains Fehlerprotokolle aktiviert und zur Aufbewahrung und Beantwortung an Amazon CloudWatch Logs gestreamt werden. OpenSearch Service-Fehlerprotokolle können bei Sicherheits- und Zugriffsprüfungen helfen und bei der Diagnose von Verfügbarkeitsproblemen helfen.

Kontroll-ID	AWS Config	Empfehlungen
AttachmentC_7(h)	wafv2-logging-enabled	Um die Protokollierung und Überwachung in Ihrer Umgebung zu erleichte rn, aktivieren Sie die AWS WAF (V2) -Protokollierung im regionalen und globalen Internet ACLs. AWS Die WAF-Protokollierung bietet detaillie rte Informationen über den Datenverkehr, der von Ihrer Web-ACL analysiert wird. In den Protokollen werden die Uhrzeit aufgezeichnet, zu der die AWS WAF die Anfrage von Ihrer AWS Ressource erhalten hat, Informationen über die Anfrage und eine Aktion für die Regel, der jede Anfrage entsprach.
AttachmentC_7(h)	elasticsearch-logs-to-cloud watch	Stellen Sie sicher, dass für Amazon OpenSearch Service-Domains Fehlerprotokolle aktiviert und zur Aufbewahr ung und Beantwortung an Amazon CloudWatch Logs gestreamt werden. Domain-Fehlerprotokolle sind bei Sicherheits- und Zugriffsp rüfungen sowie bei der Diagnose von Verfügbar keitsproblemen nützlich.

Kontroll-ID	AWS Config	Empfehlungen
AttachmentC_7(i)	iam-user-unused-credentials-überprüfen	AWS Identity and Access Management (IAM) kann Ihnen bei Zugriffsberechtigungen und Autorisierungen helfen, indem es nach IAM-Passwörtern und Zugriffsschlüsseln sucht, die für einen bestimmten Zeitraum nicht verwendet wurden. Wenn ungenutzte Anmeldeinformationen identifiziert werden, müssen Sie sie deaktivieren und/oder entfernen, da dies gegen das Prinzip der geringsten Berechtigung verstoßen könnte. Für diese Regel müssen Sie einen Wert für das maxCredentialUsage Alter festlegen (Standardkonfiguration: 90). Der tatsächliche Wert muss den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	AWS Config	Empfehlungen
AttachmentC_7(j)	iam-user-mfa-enabled	Aktivieren Sie diese Regel, um den Zugriff auf Ressourcen in der AWS -Cloud einzuschränken. Diese Regel stellt sicher, dass die Multi-Faktor-Authentifizierung (MFA) für alle Benutzer aktiviert ist. MFA bietet eine weitere Schutzebene zusätzlich zum Benutzernamen und Passwort. Reduzieren Sie Fälle von kompromittierten Konten, indem Sie MFA für Benutzer vorschreiben.
AttachmentC_7(j)	mfa-enabled-for-iam-Konsolenzugriff	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass MFA für alle AWS Identity and Access Management (IAM) -Benutzer aktiviert ist, die über ein Konsolenkennwort verfügen. MFA sorgt für eine weitere Schutzebene zusätzlich zu den Anmeldeinformationen. Indem Sie MFA für Benutzer vorschreiben, können Sie Fälle kompromittierter Konten reduzieren und verhindern, dass unbefugte Benutzer auf vertrauliche Daten zugreifen.

Kontroll-ID	AWS Config	Empfehlungen
AttachmentC_7(j)	root-account-hardware-mfa-aktiviert	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Hardware-MFA für den Root-Benutzer aktiviert ist. Der Stammbenutzer ist der AWS-Konto-Benutzer mit den meisten Berechtigungen. MFA sorgt für eine weitere Schutzebene zusätzlich zu den Anmeldeinformationen. Indem Sie MFA für den Root-Benutzer vorschreiben, können Sie die Anzahl AWS-Konten kompromittierter Benutzer reduzieren.
AttachmentC_7(j)	root-account-mfa-enabled	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass MFA für den Root-Benutzer aktiviert ist. Der Stammbenutzer ist der AWS-Konto-Benutzer mit den meisten Berechtigungen. MFA bietet eine weitere Schutzebene zusätzlich zum Benutzernamen und Passwort. Indem Sie MFA für den Root-Benutzer vorschreiben, können Sie die Anzahl AWS-Konten kompromittierter Benutzer reduzieren.

Kontroll-ID	AWS Config	Empfehlungen
AttachmentC_8	opensearch-logs-to-cloudwatch	Stellen Sie sicher, dass für Amazon OpenSearch Service-Domains Fehlerprotokolle aktiviert und zur Aufbewahrung und Beantwortung an Amazon CloudWatch Logs gestreamt werden. OpenSearch Service-Fehlerprotokolle können bei Sicherheits- und Zugriffsprüfungen helfen und bei der Diagnose von Verfügbarkeitsproblemen helfen.
AttachmentC_8	api-gw-execution-logging-aktiviert	Die API-Gateway-Protokollierung zeigt detaillierte Ansichten der Benutzer, die auf die API zugegriffen haben, und wie diese Benutzer auf die API zugegriffen haben. Diese Einblicke ermöglichen die Transparenz von Benutzeraktivitäten.
AttachmentC_8	cloud-trail-cloud-watch-logs-aktiviert	Verwenden Sie Amazon CloudWatch , um Protokollereignisaktivitäten zentral zu sammeln und zu verwalten . Die Aufnahme von AWS CloudTrail Daten liefert Einzelheiten zu den API-Aufrufaktivitäten in Ihrem AWS-Konto.

Kontroll-ID	AWS Config	Empfehlungen
AttachmentC_8	cloudtrail-enabled	AWS CloudTrail kann bei der Nichtabstreitbarkeit helfen, indem Aktionen und API-Aufrufe der AWS Managemen t Console aufgezeichnet werden. Sie können die Benutzer und die Benutzer AWS-Konten , die einen AWS Dienst aufgerufen haben, die Quell-IP-Adresse, über die die Aufrufe generiert wurden, und den Zeitpunkt der Anrufe identifizieren. Einzelheiten zu den erfassten Daten finden Sie in den AWS CloudTrail Datensatzinhalten.
AttachmentC_8	cloudtrail-s3-dataevents-en abled	Die Erfassung von Simple Storage Service (Amazon S3)-Datenereignissen unterstützt die Erkennung von ungewöhnl ichen Aktivitäten. Zu den Details gehören Informati onen zu dem AWS -Konto, das auf einen Amazon-S3-Bucket zugegriffen hat, die IP-Adresse und die Uhrzeit des Ereignisses.

Kontroll-ID	AWS Config	Empfehlungen
AttachmentC_8	elb-logging-enabled	Die Elastic-Load-Balancing-Aktivität ist ein zentraler Kommunikationspunkt innerhalb einer Umgebung. Stellen Sie sicher, dass die ELB-Protokollierung aktiviert ist. Die gesammelten Daten enthalten detaillierte Informati onen zu Anfragen, die an den ELB gesendet wurden. Jedes Protokoll enthält Informati onen wie die Zeit, zu der die Anforderung einging, die Client-IP-Adresse, Latenzen, Anforderungspfade und Serverantworten.

Kontroll-ID	AWS Config	Empfehlungen
AttachmentC_8	multi-region-cloudtrail-enabled	AWS CloudTrail zeichnet Aktionen und API-Aufrufe der AWS Management Console auf. Sie können feststellen, welche Benutzer und Konten angerufen wurden AWS, von welcher Quell-IP-Adresse aus die Anrufe getätigt wurden und wann die Anrufe erfolgten . CloudTrail übermittelt Protokolldateien aus allen AWS Regionen an Ihren S3-Bucket, wenn MULTI_REG ION_CLOUD_TRAIL_EN ABLED aktiviert ist. Außerdem wird beim AWS Start einer neuen Region derselbe Trail in der neuen Region erstellt. CloudTrail Dadurch erhalten Sie automatisch Protokoll dateien mit API-Aktivitäten für die neue Region.

Kontroll-ID	AWS Config	Empfehlungen
AttachmentC_8	s-3 bucket-logging-enabled	Die Amazon Simple Storage Service (Amazon S3)-Serve rzugriffsprotokollierung bietet eine Methode zur Überwachung des Netzwerks im Hinblick auf potenzielle Cybersicherheitsereignisse. Die Ereignisse werden überwacht, indem detaillie rte Aufzeichnungen über die Anfragen erfasst werden, die an einen Amazon-S3-Bucket gestellt wurden. Jeder Zugriffsprotokolleintrag enthält Details zu einer einzelnen Zugriffsanfrage. Zu den Details gehören Auftragge ber, Bucket-Name, Anforderu ngszeit, Anforderungsaktion, Antwortstatus und Fehlercode, falls relevant.

Kontroll-ID	AWS Config	Empfehlungen
AttachmentC_8	vpc-flow-logs-enabled	VPC-Flow-Protokolle erfassen detaillierte Informationsdatensätze über den IP-Datenverkehr, der zu und von Netzwerkschnittstellen in Ihrer Amazon Virtual Private Cloud (Amazon VPC) fließt. Standardmäßig enthalten Flow-Protokolldatensätze Werte für die verschiedenen Komponenten des IP-Flows, einschließlich Quelle, Ziel und Protokoll.
AttachmentC_8	rds-logging-enabled	Um die Protokollierung und Überwachung in Ihrer Umgebung zu erleichtern, stellen Sie sicher, dass die Amazon Relational Database Service (Amazon RDS)-Protokollierung aktiviert ist. Mit der Amazon-RDS-Protokollierung können Sie Ereignisse wie Verbindungen, Verbindungsabbrüche, Abfragen oder abgefragte Tabellen erfassen.

Kontroll-ID	AWS Config	Empfehlungen
AttachmentC_8	wafv2-logging-enabled	Um die Protokollierung und Überwachung in Ihrer Umgebung zu erleichte rn, aktivieren Sie die AWS WAF (V2) -Protokollierung im regionalen und globalen Web ACLs. AWS Die WAF-Protokollierung bietet detaillie rte Informationen über den Datenverkehr, der von Ihrer Web-ACL analysiert wird. In den Protokollen werden die Uhrzeit aufgezeichnet, zu der die AWS WAF die Anfrage von Ihrer AWS Ressource erhalten hat, Informationen über die Anfrage und eine Aktion für die Regel, der jede Anfrage entsprach.
AttachmentC_8	elasticsearch-logs-to-cloud watch	Stellen Sie sicher, dass für Amazon OpenSearch Service-Domains Fehlerprotokolle aktiviert und zur Aufbewahr ung und Beantwortung an Amazon CloudWatch Logs gestreamt werden. Domain-Fehlerprotokolle sind bei Sicherheits- und Zugriffsp rüfungen sowie bei der Diagnose von Verfügbar keitsproblemen nützlich.

Kontroll-ID	AWS Config	Empfehlungen
AttachmentD_1	codebuild-project-envvar-awscred-überprüfen	Stellen Sie sicher, dass die Anmeldeinformationen AWS_ACCESS_KEY_ID AWS_SECRET_ACCESS_KEY nicht in AWS Codebuild -Projektumgebungen vorhanden sind. Speichern Sie diese Variablen nicht als Klartext. Das Speichern dieser Variablen im Klartext führt zu unbeabsichtigter Offenlegung von Daten und unberechtigtem Zugriff.
AttachmentD_1	codebuild-project-source-repo-URL-Prüfung	Stellen Sie sicher, dass die URL des Quell-Repositorys GitHub oder des Bitbucket -Quell-Repositorys keine persönlichen Zugriffstoken oder Anmeldeinformationen in Codebuild-Projektumgebungen enthält. AWS Verwende OAuth anstelle von persönlichen Zugriffstoken oder Anmeldedaten die Autorisierung für den Zugriff auf GitHub Bitbucket-Repositorys.

Kontroll-ID	AWS Config	Empfehlungen
AttachmentE_4	kms-cmk-not-scheduled-zum Löschen	Um Daten im Ruhezusta nd zu schützen, sollten Sie sicherstellen, dass die für den Kunden erforderlichen Masterschlüssel (CMKs) nicht für das Löschen im AWS Key Management Service (AWS KMS) vorgesehen sind. Da Schlüssel manchmal gelöscht werden müssen, können Sie mit dieser Regel alle zu löschenden Schlüssel überprüfen, falls ein Schlüssel versehentlich zur Löschung vorgemerkt wurde.
AttachmentE_4	cmk-backing-key-rotation-ak tiviert	Aktivieren Sie die Schlüssel rotation, um sicherzustellen, dass Schlüssel rotiert werden, sobald sie das Ende ihrer Kryptoperiode erreicht haben.
AttachmentE_5(d)	cmk-backing-key-rotation-ak tiviert	Aktivieren Sie die Schlüssel rotation, um sicherzustellen, dass Schlüssel rotiert werden, sobald sie das Ende ihrer Kryptoperiode erreicht haben.
AttachmentE_1(a)(b)(d)	opensearch-encrypted-at-rest	Da sensible Daten vorhanden sein können und um Daten im Ruhezustand zu schützen, sollten Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon OpenSearch Service-Domains aktiviert ist.

Kontroll-ID	AWS Config	Empfehlungen
AttachmentE_1(a)(b)(d)	opensearch-node-to-node-Verschlüsselungsprüfung	Stellen Sie sicher, dass die node-to-node Verschlüsselung für Amazon OpenSearch Service aktiviert ist. Node-to-nodeVerschlüsselung ermöglicht die TLS 1.2-Verschlüsselung für die gesamte Kommunikation innerhalb der Amazon Virtual Private Cloud (Amazon VPC). Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.
AttachmentE_1(a)(b)(d)	acm-certificate-expiration-check	Stellen Sie sicher, dass die Netzwerkintegrität geschützt ist, indem Sie sicherstellen, dass X509-Zertifikate von AWS ACM ausgestellt werden. Diese Zertifikate müssen gültig und dürfen nicht abgelaufen sein. Für diese Regel ist ein Wert für erforderlich daysToExpiration (Wert für bewährte AWS Grundregeln für Sicherheit: 90). Der tatsächliche Wert muss den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	AWS Config	Empfehlungen
AttachmentE_1(a)(b)(d)	alb-http-to-https-Umleitung sprüfung	Um Daten während der Übertragung zu schützen, stellen Sie sicher, dass Ihr Application Load Balancer unverschlüsselte HTTP-Anfr agen automatisch an HTTPS umleitet. Da sensible Daten vorhanden sein können, sollten Sie die Verschlüs selung bei der Übertragung aktivieren, um diese Daten zu schützen.
AttachmentE_1(a)(b)(d)	api-gw-cache-enabled-und-ve rschlüsselt	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass die Verschlüsselung für den Cache Ihrer API-Gatew ay-Stufe aktiviert ist. Da für die API-Methode sensible Daten erfasst werden können, sollten Sie die Verschlüsselung von Daten im Ruhezustand aktivieren, um diese Daten zu schützen.
AttachmentE_1(a)(b)(d)	cloud-trail-encryption-enabled	Zum Schutz von eventuell vorhandenen sensiblen Daten sowie Daten im Ruhezusta nd müssen Sie sicherstellen, dass die Verschlüsselung für Ihre AWS CloudTrail aktiviert ist.

Kontroll-ID	AWS Config	Empfehlungen
AttachmentE_1(a)(b)(d)	cloudwatch-log-group-encrypted	Um sensible Daten im Speicher zu schützen, stellen Sie sicher, dass die Verschlüsselung für Ihre Amazon CloudWatch Log Groups aktiviert ist.
AttachmentE_1(a)(b)(d)	efs-encrypted-check	Aktivieren Sie die Verschlüsselung für Ihr Amazon Elastic File System (EFS), um eventuell vorhandene sensible Daten sowie Daten im Ruhezustand zu schützen.
AttachmentE_1(a)(b)(d)	elasticsearch-encrypted-at-rest	Da sensible Daten vorhanden sein können und um Daten im Ruhezustand zu schützen, sollten Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon OpenSearch Service (OpenSearch Service) -Domains aktiviert ist.

Kontroll-ID	AWS Config	Empfehlungen
AttachmentE_1(a)(b)(d)	elb-acm-certificate-required	Zum Schutz von eventuell vorhandenen sensiblen Daten sowie von Daten während der Übertragung muss die Verschlüsselung für Ihr Elastic Load Balancing aktiviert sein. Verwenden Sie AWS Certifica te Manager, um öffentlic he und private SSL/TLS-Z ertifikate mit AWS Diensten und internen Ressourcen zu verwalten, bereitzustellen und bereitzustellen.
AttachmentE_1(a)(b)(d)	encrypted-volumes	Aktivieren Sie die Verschlüs selung für Ihre Volumes von Amazon Elastic Block Store (Amazon EBS), um eventuell vorhandene sensible Daten sowie Daten im Ruhezustand zu schützen.

Kontroll-ID	AWS Config	Empfehlungen
AttachmentE_1(a)(b)(d)	kms-cmk-not-scheduled-zum Löschen	Um Daten im Ruhezustand zu schützen, sollten Sie sicherstellen, dass die für den Kunden erforderlichen Masterschlüssel (CMKs) nicht für das Löschen im AWS Key Management Service (AWS KMS) vorgesehen sind. Da Schlüssel manchmal gelöscht werden müssen, können Sie mit dieser Regel alle zu löschenden Schlüssel überprüfen, falls ein Schlüssel versehentlich zur Löschung vorgemerkt wurde.
AttachmentE_1(a)(b)(d)	rds-storage-encrypted	Zum Schutz von Daten im Ruhezustand müssen Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon Relational Database Service (Amazon RDS)-Instances aktiviert ist. Da sensible Daten in Amazon-RDS-Instances gespeichert werden können, sollten Sie die Verschlüsselung von Daten im Ruhezustand aktivieren, um diese Daten zu schützen.

Kontroll-ID	AWS Config	Empfehlungen
AttachmentE_1(a)(b)(d)	redshift-cluster-configuration-check	Um Daten im Ruhezustand zu schützen, muss die Verschlüsselung für Ihre Amazon-Redshift-Cluster aktiviert sein. Sie müssen auch sicherstellen, dass die erforderlichen Konfigurationen auf Amazon-Redshift-Clustern bereitgestellt werden. Die Prüfungsprotokollierung muss aktiviert sein, um Informationen zu Verbindungen und Benutzeraktivitäten in der Datenbank bereitzustellen. Diese Regel erfordert, dass ein Wert für clusterDbEncrypted (Config Default: TRUE) und LoggingEnabled (Config Default: TRUE) gesetzt ist. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.
AttachmentE_1(a)(b)(d)	redshift-require-tls-ssl	Stellen Sie sicher, dass Ihre Amazon-Redshift-Cluster eine TLS/SSL-Verschlüsselung erfordern, um eine Verbindung zu SQL-Clients herzustellen. Da sensible Daten vorhanden sein können, sollten Sie die Verschlüsselung bei der Übertragung aktivieren, um diese Daten zu schützen.

Kontroll-ID	AWS Config	Empfehlungen
AttachmentE_1(a)(b)(d)	s3-aktiviert bucket-server-side-encryption	Zum Schutz von Daten im Ruhezustand müssen Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon Simple Storage Service (Amazon S3)-Buckets aktiviert ist. Da sensible Daten in Amazon-S3-Buckets gespeichert werden können, sollten Sie die Verschlüsselung aktivieren, um diese Daten zu schützen.
AttachmentE_1(a)(b)(d)	s-3 bucket-ssl-requests-only	Um Daten während der Übertragung zu schützen, stellen Sie sicher, dass Ihre Amazon Simple Storage Service (Amazon S3)-Buckets Anfragen zur Verwendung von Secure Socket Layer (SSL)-Buckets erfordern. Da sensible Daten vorhanden sein können, sollten Sie die Verschlüsselung bei der Übertragung aktivieren, um diese Daten zu schützen.

Kontroll-ID	AWS Config	Empfehlungen
AttachmentE_1(a)(b)(d)	sagemaker-endpoint-configuration-kms-key-konfiguriert	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass die Verschlüsselung mit dem AWS Key Management Service (AWS KMS) für Ihren Endpunkt aktiviert ist. SageMaker Da sensible Daten auf dem SageMaker Endgerät gespeichert werden können, sollten Sie die Verschlüsselung im Ruhezustand aktivieren, um diese Daten zu schützen.
AttachmentE_1(a)(b)(d)	sagemaker-notebook-instance-kms-schlüsselkonfiguriert	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass die Verschlüsselung mit dem AWS Key Management Service (AWS KMS) für Ihr Notebook aktiviert ist. SageMaker Da vertrauliche Daten im SageMaker Notebook gespeichert werden können, sollten Sie die Verschlüsselung im Ruhezustand aktivieren, um diese Daten zu schützen.

Kontroll-ID	AWS Config	Empfehlungen
AttachmentE_1(a)(b)(d)	sns-encrypted-kms	Um Daten im Ruhezusta nd zu schützen, stellen Sie sicher, dass Ihre Amazon Simple Notification Service (Amazon SNS) -Themen mit dem AWS Key Management Service (AWS KMS) verschlüs selt werden müssen. Um eventuell vorhandene sensible Daten im Ruhezustand in veröffentlichten Nachricht en zu schützen, muss die Verschlüsselung von Daten im Ruhezustand aktiviert sein.
AttachmentE_1(a)(b)(d)	ec2- ebs-encryption-by-default	Zum Schutz von Daten im Ruhezustand müssen Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon Elastic Block Store (Amazon EBS)-Volumes aktiviert ist. Aktivieren Sie die Verschlüsselung von Daten im Ruhezustand, um eventuell in diesen Volumes vorhandene sensible Daten im Ruhezusta nd zu schützen.

Kontroll-ID	AWS Config	Empfehlungen
AttachmentE_1(a)(b)(d)	rds-snapshot-encrypted	Stellen Sie sicher, dass die Verschlüsselung für Ihre Amazon Relational Database Service (Amazon RDS)-Snapshots aktiviert ist. Da sensible Daten auch im Ruhezustand vorhanden sein können, sollten Sie die Verschlüsselung von Daten im Ruhezustand aktivieren, um diese Daten zu schützen.
AttachmentE_1(a)(b)(d)	elasticsearch-node-to-node-Verschlüsselungsprüfung	Stellen Sie sicher, dass die node-to-node Verschlüsselung für Amazon OpenSearch Service aktiviert ist. Node-to-nodeVerschlüsselung ermöglicht die TLS 1.2-Versc hlüsselung für die gesamte Kommunikation innerhalb der Amazon Virtual Private Cloud (Amazon VPC). Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.
AttachmentE_1(a)(b)(d)	elb-tls-https-listeners-nur	Stellen Sie sicher, dass Ihre Elastic Load Balancer (ELBs) mit SSL- oder HTTPS-Lis tenern konfiguriert sind. Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	AWS Config	Empfehlungen
AttachmentE_1(a)(b)(d)	redshift-cluster-kms-enabled	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass die Verschlüsselung mit AWS Key Management Service (AWS KMS) für Ihren Amazon Redshift Redshift-Cluster aktiviert ist. Um eventuell vorhandene sensible Daten im Ruhezustand in Redshift-Clustern zu schützen, muss die Verschlüsselung von Daten im Ruhezustand aktiviert sein.
AttachmentE_1(a)(b)(d)	api-gw-ssl-enabled	Stellen Sie sicher, dass die REST-API-Stufen von Amazon API Gateway mit SSL-Zerti fikaten konfiguriert sind, damit Backend-Systeme überprüfe n können, ob Anforderungen von API Gateway stammen.

Vorlage

Die Vorlage ist verfügbar unter GitHub: Operational Best Practices for APRA CPG 234.

Bewährte Methoden für die Ausführung des Asset-Managements

Dieses Konformitätspaket enthält AWS Config Regeln, die auf dem darin enthaltenen AWS Asset Management basieren. Eine Liste aller verwalteten Regeln, die von unterstützt werden AWS Config, finden Sie unter Liste der AWS Config verwalteten Regeln.

Die Namen und Beschreibungen der erforderlichen Parameter finden Sie im `Parameters` Abschnitt der folgenden Vorlage.

Die Vorlage ist verfügbar unter GitHub: Operational Best Practices for Asset Management.

Bewährte Methoden für die Ausführung von AWS Backup

Dieses Konformitätspaket enthält AWS Config Regeln, die auf AWS Backup internen AWS Regeln basieren. Eine Liste aller verwalteten Regeln, die von unterstützt werden AWS Config, finden Sie unter Liste der AWS Config verwalteten Regeln.

Die Namen und Beschreibungen der erforderlichen Parameter finden Sie im `Parameters` Abschnitt der folgenden Vorlage.

Die Vorlage ist verfügbar unter GitHub: Operational Best Practices für AWS Backup.

Operative Best Practices für AWS Identitäts- und Zugriffsmanagement

Die Vorlage ist verfügbar unter GitHub: Operational Best Practices for AWS Identity and Access Management.

Operative Best Practices für die AWS Zuverlässigkeit eines gut konzipierten Frameworks

Konformitätspakete bieten ein allgemeines Compliance-Framework, das es Ihnen ermöglicht, mithilfe verwalteter oder benutzerdefinierter Regeln und Abhilfemaßnahmen Kontrollen zur Sicherheits-, Betriebs- oder Kostenoptimierung durchzuführen. AWS Config AWS Config Conformance Packs dienen als Beispielvorlagen nicht dazu, die vollständige Einhaltung eines bestimmten Governance- oder Compliance-Standards sicherzustellen. Sie sind dafür verantwortlich, selbst zu beurteilen, ob Ihre Nutzung der Services den geltenden gesetzlichen und behördlichen Anforderungen entspricht.

Im Folgenden finden Sie ein Beispiel für eine Zuordnung zwischen der Reliability Pillar des Well-Architected Framework von Amazon Web Services und den AWS verwalteten Konfigurationsregeln. Jede Config-Regel gilt für eine bestimmte AWS Ressource und bezieht sich auf eines oder mehrere Entwurfsprinzipien der Säule. Eine Well-Architected-Framework-Kategorie kann mit mehreren Konfigurationsregeln verknüpft werden. In der folgenden Tabelle finden Sie weitere Informationen und Anleitungen zu diesen Zuordnungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
REL-1	Wie werden Servicekontingente und -einschränkungen	dynamodb-throughput-limit-check	Aktivieren Sie diese Regel, um sicherzustellen, dass

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	verwaltet? Für cloudbasierte Workload-Architekturen gibt es Servicekontingente (die auch als Servicebeschränkungen bezeichnet werden). Mit diesen Kontingenten soll verhindert werden, dass versehentlich mehr Ressourcen bereitgestellt werden, als Sie benötigen, und es sollen die Anforderungsraten bei API-Vorgängen begrenzt werden, um Services vor Missbrauch zu schützen. Es gibt auch Einschränkungen für Ressourcen, z. B. im Bezug auf die Rate, mit der Bits über ein Glasfaserkabel übertragen werden können, oder die Menge an Speicherplatz auf einer physischen Festplatte.		die bereitgestellte Durchsatzkapazität in Ihren Amazon-DynamoDB-Tabellen überprüft wird. Dies ist der Umfang der Lese- und Schreibaktivitäten, der von den jeweiligen Tabellen unterstützt werden kann. DynamoDB verwendet diese Informationen für das Reservieren ausreichender Systemressourcen, um Ihren Durchsatzanforderungen gerecht zu werden. Diese Regel generiert eine Warnung, wenn sich der Durchsatz dem Höchstlimit für ein Kundenkonto nähert. Mit dieser Regel können Sie optional die Parameter RCUThreshold Kontoprozentsatz (Konfigurationsstandard: 80) und WCUThreshold Kontoprozentsatz

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			(Konfigurationsstandard: 80) festlegen. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
REL-1	Wie werden Servicekontingente und -einschränkungen verwaltet? Für cloudbasierte Workload-Architekturen gibt es Servicekontingente (die auch als Servicebeschränkungen bezeichnet werden). Mit diesen Kontingenten soll verhindert werden, dass versehentlich mehr Ressourcen bereitgestellt werden, als Sie benötigen, und es sollen die Anforderungsraten bei API-Vorgängen begrenzt werden, um Services vor Missbrauch zu schützen. Es gibt auch Einschränkungen für Ressourcen, z. B. im Bezug auf die Rate, mit der Bits über ein Glasfaserkabel übertragen werden können, oder die Menge an Speicherplatz auf	lambda-concurrency-check	Diese Regel stellt sicher, dass die Höchst- und Untergrenzen für die Gleichzeitigkeit einer Lambda-Funktion festgelegt werden. Dies kann Sie beim Baselining für die Anzahl der Anforderungen unterstützen, die Ihre Funktion zu einem bestimmten Zeitpunkt verarbeitet.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	einer physischen Festplatte.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
REL-1	Wie werden Servicekontingente und -einschränkungen verwaltet? Für cloudbasierte Workload-Architekturen gibt es Servicekontingente (die auch als Servicebeschränkungen bezeichnet werden). Mit diesen Kontingenten soll verhindert werden, dass versehentlich mehr Ressourcen bereitgestellt werden, als Sie benötigen, und es sollen die Anforderungsraten bei API-Vorgängen begrenzt werden, um Services vor Missbrauch zu schützen. Es gibt auch Einschränkungen für Ressourcen, z. B. im Bezug auf die Rate, mit der Bits über ein Glasfaserkabel übertragen werden können, oder die Menge an Speicherplatz auf	ecs-task-definition-memory-hartes Limit	Durch die Begrenzung des maximalen Speichers, der Ihren Amazon Elastic Container Service (ECS)-Containern zur Verfügung steht, wird sichergestellt, dass Ihre Ressourcennutzung im Falle eines böswilligen Zugriffs auf Ihre Container nicht missbraucht werden kann.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	einer physischen Festplatte.		
REL-2	Wie wird die Netzwerktopologie geplant? Workloads existieren oft in mehreren Umgebungen. Dazu gehören mehrere Cloud-Umgebungen (sowohl öffentlich zugänglich als auch privat) und möglicher weise Ihre bestehend e Rechenzentrumsinfr astruktur. Die Pläne müssen Netzwerka spekte wie systemint erne und systemübe rgreifende Konnektiv ität, Verwaltung öffentlicher IP-Adress en, Verwaltung privater IP-Adress en und Auflösung von Domainnamen beinhalten.	vpc-vpn-2-tunnels-up	Redundante Site-to-Site VPN-Tunne l können implement iert werden, um die Anforderungen an die Ausfallsicherheit zu erfüllen. Es verwendet zwei Tunnel, um die Konnektivität sicherzustellen, falls eine der Site-to-Site VPN-Verbindungen nicht verfügbar ist. Um sich vor einem Verbindungsverlust zu schützen, können Sie für den Fall, dass Ihr Kunden-Gateway nicht verfügbar ist, eine zweite Site-to-S ite VPN-Verbindung zu Ihrer Amazon Virtual Private Cloud (Amazon VPC) und Ihrem Virtual Private Gateway einrichten, indem Sie ein zweites Kunden-Gateway verwenden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
REL-2	Wie wird die Netzwerktopologie geplant? Workloads existieren oft in mehreren Umgebungen. Dazu gehören mehrere Cloud-Umgebungen (sowohl öffentlich zugänglich als auch privat) und möglicher weise Ihre bestehend e Rechenzentrumsinfr astruktur. Die Pläne müssen Netzwerka spekte wie systemint erne und systemübe rgreifende Konnektiv ität, Verwaltung öffentlicher IP-Adress en, Verwaltung privater IP-Adress en und Auflösung von Domainnamen beinhalten.	redshift-enhanced-vpc-routing-aktiviert	Mit Enhanced-VPC-Routing wird erzwungen, dass der gesamte COPY- und UNLOAD-Da tenverkehr zwischen Ihrem Cluster und Datenrepositorys über Ihre Amazon VPC erfolgt. Anschließ end können Sie VPC-Features wie Sicherheitsgruppen und Netzwerkz ugriffskontrolllisten verwenden, um den Netzwerkverkehr zu schützen. Sie können auch VPC-Fluss protokolle verwenden , um den Netzwerkv erkehr zu überwache n.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
REL-2	Wie wird die Netzwerktopologie geplant? Workloads existieren oft in mehreren Umgebungen. Dazu gehören mehrere Cloud-Umgebungen (sowohl öffentlich zugänglich als auch privat) und möglicher weise Ihre bestehend e Rechenzentrumsinfr astruktur. Die Pläne müssen Netzwerka spekte wie systemint erne und systemübe rgreifende Konnektiv ität, Verwaltung öffentlicher IP-Adress en, Verwaltung privater IP-Adress en und Auflösung von Domainnamen beinhalten.	ec2- instances-in-vpc	Stellen Sie Amazon Elastic Compute Cloud (Amazon EC2) -Instances innerhalb einer Amazon Virtual Private Cloud (Amazon VPC) bereit, um eine sichere Kommunika tion zwischen einer Instance und anderen Services innerhalb der Amazon VPC zu ermöglichen, ohne dass ein Internet-Gateway, ein NAT-Gerät oder eine VPN-Verbindung erforderlich ist. Der gesamte Datenverk ehr bleibt sicher in der AWS Cloud. Domains, die sich innerhalb einer VPC befinden, verfügen aufgrund ihrer logischen Isolierun g im Vergleich zu Domains mit öffentlic hen Endpunkten über eine zusätzlic he Sicherheitsebene. Weisen Sie EC2

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			Amazon-Instances einer Amazon-VPC zu, um den Zugriff ordnungsgemäß zu verwalten.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
REL-5	Wie werden Interaktionen in einem verteilten System gestaltet, um Ausfälle zu minimieren oder ihnen standzuhalten? Verteilte Systeme sind auf Kommunikationsnetzwerke angewiesen, um Komponenten wie Server oder Services miteinander zu verbinden. Ihre Workload muss trotz Datenverlust oder Latenz in diesen Netzwerken zuverlässig funktionieren. Die Komponenten des verteilten Systems müssen so funktionieren, dass sie sich nicht negativ auf andere Komponenten oder die Workload auswirken. Diese bewährten Methoden verhindern Ausfälle und verbessern die mittlere Betriebsdauer zwischen Ausfällen (MTBF).	lambda-dlq-check	Aktivieren Sie diese Regel, um das entsprechende Personal über Amazon Simple Queue Service (Amazon SQS) oder Amazon Simple Notification Service (Amazon SNS) zu benachrichtigen, wenn eine Funktion ausgefallen ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
REL-6	Wie werden Ihre Workload-Ressourcen überwacht? Protokolle und Metriken sind leistungsstarke Tools, mit denen Sie sich einen Überblick über den Zustand Ihrer Workload verschaffen können. Sie können Ihre Workload so konfigurieren, dass Protokolle und Metriken überwacht und Benachrichtigungen gesendet werden, wenn Schwellenwerte überschritten werden oder wichtige Ereignisse auftreten. Durch die Überwachung kann Ihre Workload erkennen, wenn Leistungsschwellenwerte überschritten werden oder wenn Ausfälle auftreten, sodass sie als Reaktion darauf automatisch	autoscaling-group-elb-healthcheck-erforderlich	Die Elastic Load Balancer (ELB) - Zustandsprüfungen für Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling Scaling-Gruppen unterstützen die Aufrechterhaltung einer angemessenen Kapazität und Verfügbarkeit. Der Load Balancer sendet regelmäßig Pings, versucht Verbindungen herzustellen oder sendet Anfragen, um den Zustand der EC2 Amazon-Instances in einer Gruppe mit auto-scaling zu testen. Wenn eine Instance nicht zurückmeldet, wird der Traffic an eine neue EC2 Amazon-Instance gesendet.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	wiederhergestellt werden kann.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
REL-6	Wie werden Ihre Workload-Ressourcen überwacht? Protokolle und Metriken sind leistungsstarke Tools, mit denen Sie sich einen Überblick über den Zustand Ihrer Workload verschaffen können. Sie können Ihre Workload so konfigurieren, dass Protokolle und Metriken überwacht und Benachrichtigungen gesendet werden, wenn Schwellenwerte überschritten werden oder wichtige Ereignisse auftreten. Durch die Überwachung kann Ihre Workload erkennen, wenn Leistungsschwellenwerte überschritten werden oder wenn Ausfälle auftreten, sodass sie als Reaktion darauf automatisch	api-gw-xray-enabled	AWS X-Ray sammelt Daten über Anfragen, die Ihre Anwendung bedient, und bietet Tools, mit denen Sie diese Daten anzeigen, filtern und Einblicke in sie gewinnen können, um Probleme und Optimierungsmöglichkeiten zu identifizieren. Stellen Sie sicher, dass X-Ray aktiviert ist, damit Sie detaillierte Informationen nicht nur über die Anfrage und Antwort, sondern auch über Aufrufe erhalten, die Ihre Anwendung an nachgelagerte AWS Ressourcen, Microservices, Datenbanken und HTTP-Web APIs tätigt.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	wiederhergestellt werden kann.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
REL-6	Wie werden Ihre Workload-Ressourcen überwacht? Protokolle und Metriken sind leistungsstarke Tools, mit denen Sie sich einen Überblick über den Zustand Ihrer Workload verschaffen können. Sie können Ihre Workload so konfigurieren, dass Protokolle und Metriken überwacht und Benachrichtigungen gesendet werden, wenn Schwellenwerte überschritten werden oder wichtige Ereignisse auftreten. Durch die Überwachung kann Ihre Workload erkennen, wenn Leistungsschwellenwerte überschritten werden oder wenn Ausfälle auftreten, sodass sie als Reaktion darauf automatisch	api-gw-execution-logging-aktiviert	Die API-Gateway-Protokollierung zeigt detaillierte Ansichten der Benutzer, die auf die API zugegriffen haben, und wie diese Benutzer auf die API zugegriffen haben. Diese Einblicke ermöglichen die Transparenz von Benutzeraktivitäten.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	wiederhergestellt werden kann.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
REL-6	Wie werden Ihre Workload-Ressourcen überwacht? Protokolle und Metriken sind leistungsstarke Tools, mit denen Sie sich einen Überblick über den Zustand Ihrer Workload verschaffen können. Sie können Ihre Workload so konfigurieren, dass Protokolle und Metriken überwacht und Benachrichtigungen gesendet werden, wenn Schwellenwerte überschritten werden oder wichtige Ereignisse auftreten. Durch die Überwachung kann Ihre Workload erkennen, wenn Leistungsschwellenwerte überschritten werden oder wenn Ausfälle auftreten, sodass sie als Reaktion darauf automatisch	beanstalk-enhanced-health-reporting-aktiviert	AWS Die verbesserte Zustandsberichterstattung von Elastic Beanstalk ermöglicht eine schnellere Reaktion auf Veränderungen im Zustand der zugrunde liegenden Infrastruktur. Diese Änderungen könnten zu einer mangelnden Verfügbarkeit der Anwendung führen. Die erweiterten Zustandsberichte von Elastic Beanstalk bieten eine Statusbeschreibung, um den Schweregrad der identifizierten Probleme einzuschätzen und mögliche Ursachen zu identifizieren, die untersucht werden müssen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	wiederhergestellt werden kann.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
REL-6	Wie werden Ihre Workload-Ressourcen überwacht? Protokolle und Metriken sind leistungsstarke Tools, mit denen Sie sich einen Überblick über den Zustand Ihrer Workload verschaffen können. Sie können Ihre Workload so konfigurieren, dass Protokolle und Metriken überwacht und Benachrichtigungen gesendet werden, wenn Schwellenwerte überschritten werden oder wichtige Ereignisse auftreten. Durch die Überwachung kann Ihre Workload erkennen, wenn Leistungsschwellenwerte überschritten werden oder wenn Ausfälle auftreten, sodass sie als Reaktion darauf automatisch	cloudwatch-alarm-action-check	Amazon CloudWatch alarmiert, wenn eine Metrik den Schwellenwert für eine bestimmte Anzahl von Bewertungszeiträumen überschreitet. Der Alarm führt eine oder mehrere Aktionen durch, die vom Wert der Metrik oder des Ausdrucks im Vergleich zu einem Schwellenwert in einer Reihe von Zeiträumen abhängt. Diese Regel erfordert einen Wert für alarmActionRequired (Config Default: True), insufficientDataAction Required (Config Default: True), okActionRequired (Config Default: False). Der tatsächliche Wert muss die Alarmaktionen für Ihre Umgebung widerspiegeln.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	wiederhergestellt werden kann.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
REL-6	Wie werden Ihre Workload-Ressourcen überwacht? Protokolle und Metriken sind leistungsstarke Tools, mit denen Sie sich einen Überblick über den Zustand Ihrer Workload verschaffen können. Sie können Ihre Workload so konfigurieren, dass Protokolle und Metriken überwacht und Benachrichtigungen gesendet werden, wenn Schwellenwerte überschritten werden oder wichtige Ereignisse auftreten. Durch die Überwachung kann Ihre Workload erkennen, wenn Leistungsschwellenwerte überschritten werden oder wenn Ausfälle auftreten, sodass sie als Reaktion darauf automatisch	cloud-trail-cloud-watch-logs-aktiviert	Verwenden Sie Amazon CloudWatch , um Protokollereignisaktivitäten zentral zu sammeln und zu verwalten. Die Aufnahme von AWS CloudTrail Daten liefert Einzelheiten zu den API-Aufrufaktivitäten in Ihrem AWS-Konto.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	wiederhergestellt werden kann.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
REL-6	Wie werden Ihre Workload-Ressourcen überwacht? Protokolle und Metriken sind leistungsstarke Tools, mit denen Sie sich einen Überblick über den Zustand Ihrer Workload verschaffen können. Sie können Ihre Workload so konfigurieren, dass Protokolle und Metriken überwacht und Benachrichtigungen gesendet werden, wenn Schwellenwerte überschritten werden oder wichtige Ereignisse auftreten. Durch die Überwachung kann Ihre Workload erkennen, wenn Leistungsschwellenwerte überschritten werden oder wenn Ausfälle auftreten, sodass sie als Reaktion darauf automatisch	cloudtrail-enabled	AWS CloudTrail kann bei der Nichtabstreitbarkeit helfen, indem Aktionen und API-Aufrufe der AWS Management Console aufgezeichnet werden. Sie können die Benutzer und die Benutzer AWS-Konten , die einen AWS Dienst aufgerufen haben, die Quell-IP-Adresse, über die die Aufrufe generiert wurden, und den Zeitpunkt der Anrufe identifizieren. Einzelheiten zu den erfassten Daten finden Sie in den AWS CloudTrail Datensatzinhalten.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	wiederhergestellt werden kann.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
REL-6	Wie werden Ihre Workload-Ressourcen überwacht? Protokolle und Metriken sind leistungsstarke Tools, mit denen Sie sich einen Überblick über den Zustand Ihrer Workload verschaffen können. Sie können Ihre Workload so konfigurieren, dass Protokolle und Metriken überwacht und Benachrichtigungen gesendet werden, wenn Schwellenwerte überschritten werden oder wichtige Ereignisse auftreten. Durch die Überwachung kann Ihre Workload erkennen, wenn Leistungsschwellenwerte überschritten werden oder wenn Ausfälle auftreten, sodass sie als Reaktion darauf automatisch	cloudtrail-s3-dataevents-enabled	Die Erfassung von Simple Storage Service (Amazon S3)-Datenereignissen unterstützt die Erkennung von ungewöhnlichen Aktivitäten. Zu den Details gehören AWS-Konto Informationen über den Zugriff auf einen Amazon S3 S3-Bucket, die IP-Adresse und die Uhrzeit des Ereignisses.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	wiederhergestellt werden kann.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
REL-6	Wie werden Ihre Workload-Ressourcen überwacht? Protokolle und Metriken sind leistungsstarke Tools, mit denen Sie sich einen Überblick über den Zustand Ihrer Workload verschaffen können. Sie können Ihre Workload so konfigurieren, dass Protokolle und Metriken überwacht und Benachrichtigungen gesendet werden, wenn Schwellenwerte überschritten werden oder wichtige Ereignisse auftreten. Durch die Überwachung kann Ihre Workload erkennen, wenn Leistungsschwellenwerte überschritten werden oder wenn Ausfälle auftreten, sodass sie als Reaktion darauf automatisch	elasticsearch-logs-to-cloudwatch	Stellen Sie sicher, dass für Amazon OpenSearch Service-Domains Fehlerprotokolle aktiviert und zur Aufbewahrung und Beantwortung an Amazon CloudWatch Logs gestreamt werden. Domain-Fehlerprotokolle sind bei Sicherheits- und Zugriffsprüfungen sowie bei der Diagnose von Verfügbarkeitsproblemen nützlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	wiederhergestellt werden kann.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
REL-6	Wie werden Ihre Workload-Ressourcen überwacht? Protokolle und Metriken sind leistungsstarke Tools, mit denen Sie sich einen Überblick über den Zustand Ihrer Workload verschaffen können. Sie können Ihre Workload so konfigurieren, dass Protokolle und Metriken überwacht und Benachrichtigungen gesendet werden, wenn Schwellenwerte überschritten werden oder wichtige Ereignisse auftreten. Durch die Überwachung kann Ihre Workload erkennen, wenn Leistungsschwellenwerte überschritten werden oder wenn Ausfälle auftreten, sodass sie als Reaktion darauf automatisch	opensearch-logs-to-cloudwatch	Stellen Sie sicher, dass für Amazon OpenSearch Service-Domains Fehlerprotokolle aktiviert und zur Aufbewahrung und Beantwortung an Amazon CloudWatch Logs gestreamt werden. OpenSearch Service-Fehlerprotokolle können bei Sicherheits- und Zugriffsprüfungen helfen und bei der Diagnose von Verfügbarkeitsproblemen helfen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	wiederhergestellt werden kann.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
REL-6	Wie werden Ihre Workload-Ressourcen überwacht? Protokolle und Metriken sind leistungsstarke Tools, mit denen Sie sich einen Überblick über den Zustand Ihrer Workload verschaffen können. Sie können Ihre Workload so konfigurieren, dass Protokolle und Metriken überwacht und Benachrichtigungen gesendet werden, wenn Schwellenwerte überschritten werden oder wichtige Ereignisse auftreten. Durch die Überwachung kann Ihre Workload erkennen, wenn Leistungsschwellenwerte überschritten werden oder wenn Ausfälle auftreten, sodass sie als Reaktion darauf automatisch	ecs-container-insights-enabled	Die Überwachung ist ein wichtiger Bestandteil der Aufrechterhaltung der Zuverlässigkeit, Verfügbarkeit und Leistung von Amazon Elastic Container Service (ECS) und Ihrer AWS Lösungen. Container Insights bietet auch Diagnoseinformationen, wie z. B.Fehler beim Container-Neustart, damit Sie Probleme schnell aufdecken und beheben können.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	wiederhergestellt werden kann.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
REL-6	Wie werden Ihre Workload-Ressourcen überwacht? Protokolle und Metriken sind leistungsstarke Tools, mit denen Sie sich einen Überblick über den Zustand Ihrer Workload verschaffen können. Sie können Ihre Workload so konfigurieren, dass Protokolle und Metriken überwacht und Benachrichtigungen gesendet werden, wenn Schwellenwerte überschritten werden oder wichtige Ereignisse auftreten. Durch die Überwachung kann Ihre Workload erkennen, wenn Leistungsschwellenwerte überschritten werden oder wenn Ausfälle auftreten, sodass sie als Reaktion darauf automatisch	elb-logging-enabled	Die Elastic-Load-Balancing-Aktivität ist ein zentraler Kommunikationspunkt innerhalb einer Umgebung. Stellen Sie sicher, dass die ELB-Protokollierung aktiviert ist. Die gesammelten Daten enthalten detaillierte Informationen zu Anfragen, die an den ELB gesendet wurden. Jedes Protokoll enthält Informationen wie die Zeit, zu der die Anforderung einging, die Client-IP-Adresse, Latenzen, Anforderungspfade und Serverantworten.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	wiederhergestellt werden kann.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
REL-6	Wie werden Ihre Workload-Ressourcen überwacht? Protokolle und Metriken sind leistungsstarke Tools, mit denen Sie sich einen Überblick über den Zustand Ihrer Workload verschaffen können. Sie können Ihre Workload so konfigurieren, dass Protokolle und Metriken überwacht und Benachrichtigungen gesendet werden, wenn Schwellenwerte überschritten werden oder wichtige Ereignisse auftreten. Durch die Überwachung kann Ihre Workload erkennen, wenn Leistungsschwellenwerte überschritten werden oder wenn Ausfälle auftreten, sodass sie als Reaktion darauf automatisch	multi-region-cloudtrail-enabled	AWS CloudTrail zeichnet Aktionen und API-Aufrufe der AWS Management Console auf. Sie können feststellen, welche Benutzer und Konten angerufen wurden AWS, von welcher Quell-IP-Adresse aus die Anrufe getätigt wurden und wann die Anrufe erfolgten. CloudTrail übermittelt Protokolldateien aus allen AWS Regionen an Ihren S3-Bucket, wenn MULTI_REGION_CLOUD_TRAIL_ENABLED aktiviert ist. Außerdem wird beim AWS Start einer neuen Region derselbe Trail in der neuen Region erstellt. CloudTrail Dadurch erhalten Sie automatisch Protokolldateien mit API-Aktivitäten für die neue Region.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	wiederhergestellt werden kann.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
REL-6	Wie werden Ihre Workload-Ressourcen überwacht? Protokolle und Metriken sind leistungsstarke Tools, mit denen Sie sich einen Überblick über den Zustand Ihrer Workload verschaffen können. Sie können Ihre Workload so konfigurieren, dass Protokolle und Metriken überwacht und Benachrichtigungen gesendet werden, wenn Schwellenwerte überschritten werden oder wichtige Ereignisse auftreten. Durch die Überwachung kann Ihre Workload erkennen, wenn Leistungsschwellenwerte überschritten werden oder wenn Ausfälle auftreten, sodass sie als Reaktion darauf automatisch	rds-logging-enabled	Um die Protokollierung und Überwachung in Ihrer Umgebung zu erleichtern, stellen Sie sicher, dass die Amazon Relational Database Service (Amazon RDS)-Protokollierung aktiviert ist. Mit der Amazon-RDS-Protokollierung können Sie Ereignisse wie Verbindungen, Verbindungsabbrüche, Abfragen oder abgefragte Tabellen erfassen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	wiederhergestellt werden kann.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
REL-6	Wie werden Ihre Workload-Ressourcen überwacht? Protokolle und Metriken sind leistungsstarke Tools, mit denen Sie sich einen Überblick über den Zustand Ihrer Workload verschaffen können. Sie können Ihre Workload so konfigurieren, dass Protokolle und Metriken überwacht und Benachrichtigungen gesendet werden, wenn Schwellenwerte überschritten werden oder wichtige Ereignisse auftreten. Durch die Überwachung kann Ihre Workload erkennen, wenn Leistungsschwellenwerte überschritten werden oder wenn Ausfälle auftreten, sodass sie als Reaktion darauf automatisch	ec-2 instance-detailed-monitoring-enabled	Aktivieren Sie diese Regel, um die Amazon Elastic Compute Cloud (Amazon EC2) - Instance-Überwachung auf der EC2 Amazon-Konsole zu verbessern, in der Monitoring-Diagramme mit einem Zeitraum von 1 Minute für die Instance angezeigt werden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	wiederhergestellt werden kann.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
REL-6	Wie werden Ihre Workload-Ressourcen überwacht? Protokolle und Metriken sind leistungsstarke Tools, mit denen Sie sich einen Überblick über den Zustand Ihrer Workload verschaffen können. Sie können Ihre Workload so konfigurieren, dass Protokolle und Metriken überwacht und Benachrichtigungen gesendet werden, wenn Schwellenwerte überschritten werden oder wichtige Ereignisse auftreten. Durch die Überwachung kann Ihre Workload erkennen, wenn Leistungsschwellenwerte überschritten werden oder wenn Ausfälle auftreten, sodass sie als Reaktion darauf automatisch	guardduty-enabled-centralized	Amazon GuardDuty kann mithilfe von Threat Intelligence Feeds helfen, potenzielle Cybersicherheitsereignisse zu überwachen und zu erkennen. Dazu gehören Listen mit bösartigen IPs und maschinellen Lernmethoden zur Identifizierung unerwarteter, nicht autorisierter und bösartiger Aktivitäten in Ihrer AWS Cloud-Umgebung.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	wiederhergestellt werden kann.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
REL-6	Wie werden Ihre Workload-Ressourcen überwacht? Protokolle und Metriken sind leistungsstarke Tools, mit denen Sie sich einen Überblick über den Zustand Ihrer Workload verschaffen können. Sie können Ihre Workload so konfigurieren, dass Protokolle und Metriken überwacht und Benachrichtigungen gesendet werden, wenn Schwellenwerte überschritten werden oder wichtige Ereignisse auftreten. Durch die Überwachung kann Ihre Workload erkennen, wenn Leistungsschwellenwerte überschritten werden oder wenn Ausfälle auftreten, sodass sie als Reaktion darauf automatisch	lambda-dlq-check	Aktivieren Sie diese Regel, um das entsprechende Personal über Amazon Simple Queue Service (Amazon SQS) oder Amazon Simple Notification Service (Amazon SNS) zu benachrichtigen, wenn eine Funktion ausgefallen ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	wiederhergestellt werden kann.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
REL-6	Wie werden Ihre Workload-Ressourcen überwacht? Protokolle und Metriken sind leistungsstarke Tools, mit denen Sie sich einen Überblick über den Zustand Ihrer Workload verschaffen können. Sie können Ihre Workload so konfigurieren, dass Protokolle und Metriken überwacht und Benachrichtigungen gesendet werden, wenn Schwellenwerte überschritten werden oder wichtige Ereignisse auftreten. Durch die Überwachung kann Ihre Workload erkennen, wenn Leistungsschwellenwerte überschritten werden oder wenn Ausfälle auftreten, sodass sie als Reaktion darauf automatisch	rds-enhanced-monitoring-enabled	Aktivieren Sie Amazon Relational Database Service (Amazon RDS), um die Verfügbarkeit von Amazon RDS zu überwachen. Dies bietet einen detaillierten Einblick in den Zustand Ihrer Amazon-RDS-Datenbank-Instances. Wenn der Amazon-RDS-Speicher mehr als ein zugrundeliegendes physisches Gerät verwendet, erfasst Enhanced Monitoring die Daten für jedes Gerät. Wenn die Amazon-RDS-Datenbank-Instance in einer Multi-AZ-Bereitstellung ausgeführt wird, werden außerdem die Daten für jedes Gerät auf dem sekundären Host sowie die Metriken des sekundären Hosts erfasst.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	wiederhergestellt werden kann.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
REL-6	Wie werden Ihre Workload-Ressourcen überwacht? Protokolle und Metriken sind leistungsstarke Tools, mit denen Sie sich einen Überblick über den Zustand Ihrer Workload verschaffen können. Sie können Ihre Workload so konfigurieren, dass Protokolle und Metriken überwacht und Benachrichtigungen gesendet werden, wenn Schwellenwerte überschritten werden oder wichtige Ereignisse auftreten. Durch die Überwachung kann Ihre Workload erkennen, wenn Leistungsschwellenwerte überschritten werden oder wenn Ausfälle auftreten, sodass sie als Reaktion darauf automatisch	redshift-enhanced-vpc-routing-aktiviert	Mit Enhanced-VPC-Routing wird erzwungen, dass der gesamte COPY- und UNLOAD-Datenverkehr zwischen Ihrem Cluster und Datenrepositorys über Ihre Amazon VPC erfolgt. Anschließend können Sie VPC-Features wie Sicherheitsgruppen und Netzwerkzugriffskontrolllisten verwenden, um den Netzwerkverkehr zu schützen. Sie können auch VPC-Flussprotokolle verwenden, um den Netzwerkverkehr zu überwachen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	wiederhergestellt werden kann.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
REL-6	Wie werden Ihre Workload-Ressourcen überwacht? Protokolle und Metriken sind leistungsstarke Tools, mit denen Sie sich einen Überblick über den Zustand Ihrer Workload verschaffen können. Sie können Ihre Workload so konfigurieren, dass Protokolle und Metriken überwacht und Benachrichtigungen gesendet werden, wenn Schwellenwerte überschritten werden oder wichtige Ereignisse auftreten. Durch die Überwachung kann Ihre Workload erkennen, wenn Leistungsschwellenwerte überschritten werden oder wenn Ausfälle auftreten, sodass sie als Reaktion darauf automatisch	s3- bucket-logging-enabled	Die Amazon Simple Storage Service (Amazon S3)-Serverzugriffsprotokollierung bietet eine Methode zur Überwachung des Netzwerks im Hinblick auf potenzielle Cybersicherheitsereignisse. Die Ereignisse werden überwacht, indem detaillierte Aufzeichnungen über die Anfragen erfasst werden, die an einen Amazon-S3-Bucket gestellt wurden. Jeder Zugriffsprotokolleintrag enthält Details zu einer einzelnen Zugriffsanfrage. Zu den Details gehören Auftraggeber, Bucket-Name, Anforderungszeit, Anforderungsaktion, Antwortstatus und Fehlercode, falls relevant.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	wiederhergestellt werden kann.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
REL-6	Wie werden Ihre Workload-Ressourcen überwacht? Protokolle und Metriken sind leistungsstarke Tools, mit denen Sie sich einen Überblick über den Zustand Ihrer Workload verschaffen können. Sie können Ihre Workload so konfigurieren, dass Protokolle und Metriken überwacht und Benachrichtigungen gesendet werden, wenn Schwellenwerte überschritten werden oder wichtige Ereignisse auftreten. Durch die Überwachung kann Ihre Workload erkennen, wenn Leistungsschwellenwerte überschritten werden oder wenn Ausfälle auftreten, sodass sie als Reaktion darauf automatisch	securityhub-enabled	AWS Security Hub hilft bei der Überwachung von unbefugtem Personal, Verbindungen, Geräten und Software. AWS Security Hub aggregiert, organisiert und priorisiert die Sicherheitswarnungen oder Ergebnisse mehrerer Dienste. AWS Einige dieser Dienste sind Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer und AWS Firewall Manager sowie AWS Partnerlösungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	wiederhergestellt werden kann.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
REL-6	Wie werden Ihre Workload-Ressourcen überwacht? Protokolle und Metriken sind leistungsstarke Tools, mit denen Sie sich einen Überblick über den Zustand Ihrer Workload verschaffen können. Sie können Ihre Workload so konfigurieren, dass Protokolle und Metriken überwacht und Benachrichtigungen gesendet werden, wenn Schwellenwerte überschritten werden oder wichtige Ereignisse auftreten. Durch die Überwachung kann Ihre Workload erkennen, wenn Leistungsschwellenwerte überschritten werden oder wenn Ausfälle auftreten, sodass sie als Reaktion darauf automatisch	vpc-flow-logs-enabled	VPC-Flow-Protokolle erfassen detaillierte Informationsdatensätze über den IP-Datenverkehr, der zu und von Netzwerkschnittstellen in Ihrer Amazon Virtual Private Cloud (Amazon VPC) fließt. Standardmäßig enthalten Flow-Protokolldatensätze Werte für die verschiedenen Komponenten des IP-Flows, einschließlich Quelle, Ziel und Protokoll.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	wiederhergestellt werden kann.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
REL-6	Wie werden Ihre Workload-Ressourcen überwacht? Protokolle und Metriken sind leistungsstarke Tools, mit denen Sie sich einen Überblick über den Zustand Ihrer Workload verschaffen können. Sie können Ihre Workload so konfigurieren, dass Protokolle und Metriken überwacht und Benachrichtigungen gesendet werden, wenn Schwellenwerte überschritten werden oder wichtige Ereignisse auftreten. Durch die Überwachung kann Ihre Workload erkennen, wenn Leistungsschwellenwerte überschritten werden oder wenn Ausfälle auftreten, sodass sie als Reaktion darauf automatisch	wafv2-logging-enabled	Um Ihnen bei der Protokollierung und Überwachung in Ihrer Umgebung zu helfen, aktivieren Sie die AWS WAF (V2) -Protokollierung im regionalen und globalen Web. ACLs AWS Die WAF-Protokollierung bietet detaillierte Informationen über den Datenverkehr, der von Ihrer Web-ACL analysiert wird. In den Protokollen werden die Uhrzeit aufgezeichnet, zu der die AWS WAF die Anfrage von Ihrer AWS Ressource erhalten hat, Informationen über die Anfrage und eine Aktion für die Regel, der jede Anfrage entsprach.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	wiederhergestellt werden kann.		
REL-7	Wie wird die Workload so gestaltet, dass sie sich an Veränderungen der Nachfrage anpasst? Eine skalierbare Workload bietet Elastizität, sodass Ressourcen automatisch hinzugefügt oder entfernt werden können, damit sie dem aktuellen Bedarf zu einem bestimmten Zeitpunkt genau entsprechen.	dynamodb-autoscaling-enabled	Amazon DynamoDB Auto Scaling verwendet den AWS Application Auto Scaling-Service, um die bereitgestellte Durchsatzkapazität so anzupassen, dass sie automatisch auf tatsächliche Verkehrsmuster reagiert. Auf diese Weise kann eine Tabelle oder ein globaler sekundärer Index die bereitgestellte Lese-/Schreibkapazität erhöhen, um plötzliche Erhöhungen des Datenverkehrs ohne Drosselung zu bewältigen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
REL-7	Wie wird die Workload so gestaltet, dass sie sich an Veränderungen der Nachfrage anpasst? Eine skalierbare Workload bietet Elastizität, sodass Ressourcen automatisch hinzugefügt oder entfernt werden können, damit sie dem aktuellen Bedarf zu einem bestimmten Zeitpunkt genau entsprechen.	autoscaling-group-elb-healthcheck-erforderlich	Die Elastic Load Balancer (ELB) - Zustandsprüfungen für Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling Scaling-Gruppen unterstützen die Aufrechterhaltung einer angemessenen Kapazität und Verfügbarkeit. Der Load Balancer sendet regelmäßig Pings, versucht Verbindungen herzustellen oder sendet Anfragen, um den Zustand der EC2 Amazon-Instances in einer Gruppe mit auto-scaling zu testen. Wenn eine Instance nicht zurückmeldet, wird der Traffic an eine neue EC2 Amazon-Instance gesendet.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
REL-7	Wie wird die Workload so gestaltet, dass sie sich an Veränderungen der Nachfrage anpasst? Eine skalierbare Workload bietet Elastizität, sodass Ressourcen automatisch hinzugefügt oder entfernt werden können, damit sie dem aktuellen Bedarf zu einem bestimmten Zeitpunkt genau entsprechen.	dynamodb-autoscaling-enabled	Amazon DynamoDB Auto Scaling verwendet den AWS Application Auto Scaling-Service, um die bereitgestellte Durchsatzkapazität so anzupassen, dass sie automatisch auf tatsächliche Verkehrsmuster reagiert. Auf diese Weise kann eine Tabelle oder ein globaler sekundärer Index die bereitgestellte Lese-/Schreibkapazität erhöhen, um plötzliche Erhöhungen des Datenverkehrs ohne Drosselung zu bewältigen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
REL-8	Wie werden Veränderungen implementiert? Kontrollierte Änderungen sind erforderlich, um neue Funktionen bereitzustellen und sicherzustellen, dass die Workloads und die Betriebsumgebung mit bekannter Software ausgeführt werden und diese auf vorhersehbare Weise gepatcht oder ersetzt werden kann. Wenn solche Änderunge n nicht kontrolliert sind, ist es schwierig , die Auswirkungen der Änderungen vorherzusagen oder Probleme zu lösen, die sich aus ihnen ergeben.	redshift-cluster-m aintenancesettings-check	Diese Regel stellt sicher, dass Amazon-Redshift-Cluster die bevorzugten Einstellungen für Ihre Organisation haben. Insbesondere sorgt sie dafür, dass Cluster bevorzugt e Wartungsfenster und automatisierte Aufbewahrungsfristen für Snapshots für die Datenbank haben. Für diese Regel müssen Sie die festlegen. allowVersionUpgrad e Der Standardwert ist „true“. Außerdem können Sie optional den Zeitraum preferredMaintenan ceWindow (der Standardwert ist sa: 16:00 -sa: 16:30) und den automated SnapshotRetention Zeitraum (der Standardwert ist 1) festlegen. Die tatsächlichen Werte müssen den Richtlini

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			en Ihrer Organisation entsprechen.
REL-8	Wie werden Veränderungen implementiert? Kontrollierte Änderungen sind erforderlich, um neue Funktionen bereitzustellen und sicherzustellen, dass die Workloads und die Betriebsumgebung mit bekannter Software ausgeführt werden und diese auf vorhersehbare Weise gepatcht oder ersetzt werden kann. Wenn solche Änderungen nicht kontrolliert sind, ist es schwierig, die Auswirkungen der Änderungen vorherzusagen oder Probleme zu lösen, die sich aus ihnen ergeben.	rds-automatic-minor-version-Upgrade aktiviert	Aktivieren Sie automatische Unterversions-Upgrades auf Ihren Amazon-Relational-Database-Service (RDS)-Instances, um sicherzustellen, dass die aktuellen Updates für Unterversionen des Relational Database Management System (RDBMS) installiert sind, die Sicherheitspatches und Bugfixes enthalten können.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
REL-8	Wie werden Veränderungen implementiert? Kontrollierte Änderungen sind erforderlich, um neue Funktionen bereitzustellen und sicherzustellen, dass die Workloads und die Betriebsumgebung mit bekannter Software ausgeführt werden und diese auf vorhersehbare Weise gepatcht oder ersetzt werden kann. Wenn solche Änderunge n nicht kontrolliert sind, ist es schwierig , die Auswirkungen der Änderungen vorherzusagen oder Probleme zu lösen, die sich aus ihnen ergeben.	ec2- prüfen managedinstance-pa tch-compliance-status	Aktivieren Sie diese Regel, um bei der Identifizierung und Dokumentation von Sicherheitslücken in Amazon Elastic Compute Cloud (Amazon EC2) zu helfen. Die Regel prüft, ob die EC2 Amazon-Instance die Patch-Konformität im AWS Systems Manager gemäß den Richtlinien und Verfahren Ihrer Organisation einhält.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
REL-8	Wie werden Veränderungen implementiert? Kontrollierte Änderungen sind erforderlich, um neue Funktionen bereitzustellen und sicherzustellen, dass die Workloads und die Betriebsumgebung mit bekannter Software ausgeführt werden und diese auf vorhersehbare Weise gepatcht oder ersetzt werden kann. Wenn solche Änderungen nicht kontrolliert sind, ist es schwierig, die Auswirkungen der Änderungen vorherzusagen oder Probleme zu lösen, die sich aus ihnen ergeben.	ec2-check managedinstance-association-compliance-status	Verwenden Sie AWS Systems Manager Associations, um bei der Inventarisierung von Softwareplattformen und Anwendungen innerhalb eines Unternehmens zu helfen. AWS Systems Manager weist Ihren verwalteten Instanzen einen Konfigurationsstatus zu und ermöglicht es Ihnen, Basiswerte für Betriebssystem-Patch-Levels, Softwareinstallationen, Anwendungskonfigurationen und andere Details zu Ihrer Umgebung festzulegen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
REL-9	Wie werden Daten gesichert? Sichern Sie Daten, Anwendungen und Konfigurationen, um Ihre Anforderungen an Recovery Time Objectives (RTO) und Recovery Point Objectives (RPO) zu erfüllen.	aurora-resources-protected-by-Backup-Plan	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon Aurora Aurora-Ressourcen Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
REL-9	Wie werden Daten gesichert? Sichern Sie Daten, Anwendungen und Konfigurationen, um Ihre Anforderungen an Recovery Time Objectives (RTO) und Recovery Point Objectives (RPO) zu erfüllen.	backup-plan-min-frequency-and-min-retention-check	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihr AWS Backup-Plan auf eine Mindestfrequenz und Aufbewahrung festgelegt ist. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen. Mit dieser Regel können Sie die Parameter requiredFrequencyValue (Config default: 1), requiredRetentionDays (Config default: 35) und requiredFrequencyUnit

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			(Config default: days) festlegen. Der tatsächliche Wert muss den Anforderungen Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
REL-9	Wie werden Daten gesichert? Sichern Sie Daten, Anwendungen und Konfigurationen, um Ihre Anforderungen an Recovery Time Objectives (RTO) und Recovery Point Objectives (RPO) zu erfüllen.	backup-recovery-point-minimum-Aufbewahrungsprüfung	Um bei Datensicherungsprozessen zu helfen, stellen Sie sicher, dass für Ihre AWS Backup-Wiederherstellungspunkte eine Mindestaufbewahrungsdauer festgelegt ist. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen. Mit dieser Regel können Sie den Parameter requiredRetentionDays (Config Default: 35) festlegen. Der tatsächliche Wert muss den Anforderu

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			ngen Ihrer Organisation entsprechen.
REL-9	Wie werden Daten gesichert? Sichern Sie Daten, Anwendungen und Konfigurationen, um Ihre Anforderungen an Recovery Time Objectives (RTO) und Recovery Point Objectives (RPO) zu erfüllen.	backup-recovery-point-encrypted	Stellen Sie sicher, dass die Verschlüsselung für Ihre AWS Backup-Wiederherstellungspunkte aktiviert ist. Da sensible Daten auch im Ruhezustand vorhanden sein können, sollten Sie die Verschlüsselung im Ruhezustand aktivieren, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
REL-9	Wie werden Daten gesichert? Sichern Sie Daten, Anwendungen und Konfigurationen, um Ihre Anforderungen an Recovery Time Objectives (RTO) und Recovery Point Objectives (RPO) zu erfüllen.	db-instance-backup-enabled	Die Sicherungsfunktion von Amazon RDS erstellt Sicherungen Ihrer Datenbanken und Transaktionsprotokolle. Amazon RDS erstellt einen Snapshot für das Speichervolume Ihrer DB-Instance, sodass die gesamte DB-Instance gesichert wird. Sie können im System spezifische Aufbewahrungsfristen festlegen, um Ihre Ausfallsicherheitsanforderungen zu erfüllen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
REL-9	Wie werden Daten gesichert? Sichern Sie Daten, Anwendungen und Konfigurationen, um Ihre Anforderungen an Recovery Time Objectives (RTO) und Recovery Point Objectives (RPO) zu erfüllen.	dynamodb-in-backup-plan	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon DynamoDB-Tabellen Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
REL-9	Wie werden Daten gesichert? Sichern Sie Daten, Anwendungen und Konfigurationen, um Ihre Anforderungen an Recovery Time Objectives (RTO) und Recovery Point Objectives (RPO) zu erfüllen.	dynamodb-pitr-enabled	Aktivieren Sie diese Regel, um zu überprüfen, ob die Informationen gesichert wurden. Es verwaltet auch die Backups, indem es sicherstellt, dass die point-in-time Wiederherstellung in Amazon DynamoDB aktiviert ist. Bei der Wiederherstellung werden fortlaufende Backups Ihrer Tabelle für die letzten 35 Tage gespeichert.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
REL-9	Wie werden Daten gesichert? Sichern Sie Daten, Anwendungen und Konfigurationen, um Ihre Anforderungen an Recovery Time Objectives (RTO) und Recovery Point Objectives (RPO) zu erfüllen.	dynamodb-table-encrypted-kms	Stellen Sie sicher, dass die Verschlüsselung für Ihre Amazon-DynamoDB-Tabellen aktiviert ist. Um eventuell vorhandene sensible Daten im Ruhezustand in diesen Tabellen zu schützen, müssen Sie die Verschlüsselung von Daten im Ruhezustand aktivieren. Standardmäßig werden DynamoDB-Tabellen mit einem AWS eigenen Kundenhauptschlüssel (CMK) verschlüsselt.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
REL-9	Wie werden Daten gesichert? Sichern Sie Daten, Anwendungen und Konfigurationen, um Ihre Anforderungen an Recovery Time Objectives (RTO) und Recovery Point Objectives (RPO) zu erfüllen.	ebs-in-backup-plan	Stellen Sie zur Unterstützung der Datensicherungspro zesse sicher, dass Ihre Amazon Elastic Block Store (Amazon EBS) -Volumes Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwaltet er Backup-Service mit einer richtlini enbasierten Backup-Lösung. Diese Lösung vereinfac ht Ihr Sicherung smanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforde rungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
REL-9	Wie werden Daten gesichert? Sichern Sie Daten, Anwendungen und Konfigurationen, um Ihre Anforderungen an Recovery Time Objectives (RTO) und Recovery Point Objectives (RPO) zu erfüllen.	ec-2 ebs-encryption-by-default	Zum Schutz von Daten im Ruhezustand müssen Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon Elastic Block Store (Amazon EBS)-Volumes aktiviert ist. Um eventuell vorhandene sensible Daten im Ruhezustand zu schützen, müssen Sie die Verschlüsselung von Daten im Ruhezustand aktivieren.
REL-9	Wie werden Daten gesichert? Sichern Sie Daten, Anwendungen und Konfigurationen, um Ihre Anforderungen an Recovery Time Objectives (RTO) und Recovery Point Objectives (RPO) zu erfüllen.	encrypted-volumes	Um eventuell vorhandene sensible Daten sowie Daten im Ruhezustand zu schützen, muss die Verschlüsselung für Ihre Amazon Elastic Block Store (Amazon EBS)-Volumes aktiviert sein.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
REL-9	Wie werden Daten gesichert? Sichern Sie Daten, Anwendungen und Konfigurationen, um Ihre Anforderungen an Recovery Time Objectives (RTO) und Recovery Point Objectives (RPO) zu erfüllen.	ec2-plan resources-protected-by-backup	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon Elastic Compute Cloud (Amazon EC2) -Ressourcen Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
REL-9	Wie werden Daten gesichert? Sichern Sie Daten, Anwendungen und Konfigurationen, um Ihre Anforderungen an Recovery Time Objectives (RTO) und Recovery Point Objectives (RPO) zu erfüllen.	efs-in-backup-plan	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon Elastic File System (Amazon EFS) -Dateisysteme Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
REL-9	Wie werden Daten gesichert? Sichern Sie Daten, Anwendungen und Konfigurationen, um Ihre Anforderungen an Recovery Time Objectives (RTO) und Recovery Point Objectives (RPO) zu erfüllen.	efs-encrypted-check	Aktivieren Sie die Verschlüsselung für Ihr Amazon Elastic File System (EFS), um eventuell vorhandene sensible Daten sowie Daten im Ruhezustand zu schützen.
REL-9	Wie werden Daten gesichert? Sichern Sie Daten, Anwendungen und Konfigurationen, um Ihre Anforderungen an Recovery Time Objectives (RTO) und Recovery Point Objectives (RPO) zu erfüllen.	elasticache-redis-cluster-automatic-Backup-Check	Wenn automatische Backups aktiviert sind, ElastiCache erstellt Amazon täglich ein Backup des Clusters. Die Sicherung kann für eine von Ihrer Organisation festgelegte Anzahl von Tagen aufbewahrt werden. Automatische Backups schützen vor Datenverlust. Bei einem Ausfall können Sie einen neuen Cluster erstellen, der Ihre Daten aus der aktuellen Sicherung wiederherstellt.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
REL-9	Wie werden Daten gesichert? Sichern Sie Daten, Anwendungen und Konfigurationen, um Ihre Anforderungen an Recovery Time Objectives (RTO) und Recovery Point Objectives (RPO) zu erfüllen.	elb-deletion-protection-enabled	Diese Regel sorgt dafür, dass der Löschschutz für Elastic Load Balancing aktiviert ist. Verwenden Sie diese Funktion, um zu verhindern, dass Ihr Load Balancer versehentlich oder böswillig gelöscht wird, was zum Verlust der Verfügbarkeit Ihrer Anwendungen führen kann.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
REL-9	Wie werden Daten gesichert? Sichern Sie Daten, Anwendungen und Konfigurationen, um Ihre Anforderungen an Recovery Time Objectives (RTO) und Recovery Point Objectives (RPO) zu erfüllen.	fsx-resources-protected-by-Backup-Plan	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre FSx Amazon-Dateisysteme Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
REL-9	Wie werden Daten gesichert? Sichern Sie Daten, Anwendungen und Konfigurationen, um Ihre Anforderungen an Recovery Time Objectives (RTO) und Recovery Point Objectives (RPO) zu erfüllen.	rds-in-backup-plan	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon Relational Database Service (Amazon RDS) -Instances Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
REL-9	Wie werden Daten gesichert? Sichern Sie Daten, Anwendungen und Konfigurationen, um Ihre Anforderungen an Recovery Time Objectives (RTO) und Recovery Point Objectives (RPO) zu erfüllen.	rds-storage-encrypted	Zum Schutz von Daten im Ruhezustand müssen Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon Relational Database Service (Amazon RDS)-Instances aktiviert ist. Um eventuell vorhandene sensible Daten im Ruhezustand in Amazon-RDS-Instances zu schützen, muss die Verschlüsselung von Daten im Ruhezustand aktiviert sein.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
REL-9	Wie werden Daten gesichert? Sichern Sie Daten, Anwendungen und Konfigurationen, um Ihre Anforderungen an Recovery Time Objectives (RTO) und Recovery Point Objectives (RPO) zu erfüllen.	rds-snapshot-encrypted	Stellen Sie sicher, dass die Verschlüsselung für Ihre Amazon Relational Database Service (Amazon RDS)-Snapshots aktiviert ist. Um eventuell vorhandene sensible Daten im Ruhezustand zu schützen, muss die Verschlüsselung von Daten im Ruhezustand aktiviert sein.
REL-9	Wie werden Daten gesichert? Sichern Sie Daten, Anwendungen und Konfigurationen, um Ihre Anforderungen an Recovery Time Objectives (RTO) und Recovery Point Objectives (RPO) zu erfüllen.	rds-instance-deletion-protection-aktiviert	Stellen Sie sicher, dass Amazon Relational Database Service (Amazon RDS)-Instances den Löschschutz aktiviert haben. Verwenden Sie den Löschschutz, um zu verhindern, dass Ihre Amazon-RDS-Instances versehentlich oder böswillig gelöscht werden, was zum Verlust der Verfügbarkeit Ihrer Anwendungen führen kann.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
REL-9	Wie werden Daten gesichert? Sichern Sie Daten, Anwendungen und Konfigurationen, um Ihre Anforderungen an Recovery Time Objectives (RTO) und Recovery Point Objectives (RPO) zu erfüllen.	s3- bucket-default-lock-enabled	Stellen Sie sicher, dass für Ihren Amazon Simple Storage Service (Amazon S3)-Bucket standardmäßig eine Sperre aktiviert ist. Zum Schutz eventuell vorhanden er sensibler Daten in S3-Buckets müssen Sie Objektsperren für Daten im Ruhezustand erzwingen.
REL-9	Wie werden Daten gesichert? Sichern Sie Daten, Anwendungen und Konfigurationen, um Ihre Anforderungen an Recovery Time Objectives (RTO) und Recovery Point Objectives (RPO) zu erfüllen.	s-3 bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) unterstützt die Aufrechterhaltung einer angemessenen Kapazität und Verfügbarkeit. CRR ermöglicht das automatische, asynchrone Kopieren von Objekten in Amazon-S3-Buckets, um die Datenverfügbarkeit sicherzustellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
REL-9	Wie werden Daten gesichert? Sichern Sie Daten, Anwendungen und Konfigurationen, um Ihre Anforderungen an Recovery Time Objectives (RTO) und Recovery Point Objectives (RPO) zu erfüllen.	s3- bucket-server-side -encryption -aktiviert	Zum Schutz von Daten im Ruhezustand müssen Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon Simple Storage Service (Amazon S3)-Buckets aktiviert ist. Um eventuell vorhandene sensible Daten im Ruhezustand in Amazon-S3-Buckets zu schützen, muss die Verschlüsselung aktiviert sein.
REL-9	Wie werden Daten gesichert? Sichern Sie Daten, Anwendungen und Konfigurationen, um Ihre Anforderungen an Recovery Time Objectives (RTO) und Recovery Point Objectives (RPO) zu erfüllen.	s-3 default-encryption -kms	Stellen Sie sicher, dass die Verschlüsselung für Ihre Amazon Simple Storage Service (Amazon S3)-Buckets aktiviert ist. Um eventuell vorhandene sensible Daten im Ruhezustand in einem Amazon-S3-Bucket zu schützen, muss die Verschlüsselung aktiviert sein.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
REL-9	Wie werden Daten gesichert? Sichern Sie Daten, Anwendungen und Konfigurationen, um Ihre Anforderungen an Recovery Time Objectives (RTO) und Recovery Point Objectives (RPO) zu erfüllen.	ebs-optimized-instance	Eine optimierte Instance im Amazon Elastic Block Store (Amazon EBS) bietet zusätzliche, dedizierte Kapazität für Amazon-EBS-I/O-Vorgänge. Diese Optimierung garantiert eine optimale Leistung für Ihr EBS-Volume, indem die Konflikte zwischen Amazon Amazon-EBS-I/O und anderem Datenverkehr von Ihrer Instance minimiert werden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
REL-9	Wie werden Daten gesichert? Sichern Sie Daten, Anwendungen und Konfigurationen, um Ihre Anforderungen an Recovery Time Objectives (RTO) und Recovery Point Objectives (RPO) zu erfüllen.	redshift-backup-enabled	Stellen Sie zur Unterstützung der Datensicherungsprozesse sicher, dass Ihre Amazon-Redshift-Cluster über automatisierte Snapshots verfügen. Wenn automatisierte Snapshots für einen Cluster aktiviert sind, erstellt Redshift in regelmäßigen Abständen Snapshots dieses Clusters. Standardmäßig erstellt Redshift alle acht Stunden oder alle 5 GB einen Snapshot für jeden Knoten mit Datenänderungen oder je nachdem, was zuerst eintritt.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
REL-9	Wie werden Daten gesichert? Sichern Sie Daten, Anwendungen und Konfigurationen, um Ihre Anforderungen an Recovery Time Objectives (RTO) und Recovery Point Objectives (RPO) zu erfüllen.	redshift-cluster-kms-enabled	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass die Verschlüs selung mit AWS Key Management Service (AWS KMS) für Ihren Amazon Redshift Redshift-Cluster aktiviert ist. Um eventuell vorhanden e sensible Daten im Ruhezustand in Redshift-Clustern zu schützen, muss die Verschlüsselung von Daten im Ruhezusta nd aktiviert sein.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
REL-9	Wie werden Daten gesichert? Sichern Sie Daten, Anwendungen und Konfigurationen, um Ihre Anforderungen an Recovery Time Objectives (RTO) und Recovery Point Objectives (RPO) zu erfüllen.	s-3 bucket-versioning-enabled	Die Versionsv erwaltung von Amazon Simple Storage Service (Amazon S3)-Bucke ts hilft dabei, mehrere Varianten eines Objekts im selben Amazon-S3-Bucket zu speichern. Verwenden Sie die Versionsv erwaltung, um sämtliche Versionen aller Objekte in Ihrem Amazon-S3-Bucket zu speichern , abzurufen oder wiederherzustellen . Mit der Versionsv erwaltung können Sie Versionen sowohl nach unbeabsic htigten Benutzera ktionen als auch nach Anwendungsfehlern problemlos wiederher stellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
REL-10	Wie wird die Fehleriso lierung zum Schützen der Workload verwendet? Fehleriso lierte Grenzen beschränken die Auswirkungen eines Fehlers innerhalb einer Workload auf eine begrenzte Anzahl von Komponent en. Komponenten außerhalb der Grenze sind von dem Ausfall nicht betroffen. Durch die Verwendung mehrerer fehleriso lierter Grenzen können Sie die Auswirkungen auf Ihre Workload einschrän ken.	elb-cross-zone-load-Balancing aktiviert	Aktivieren Sie zonenübergreifende s Load Balancing für Ihre Elastic Load Balancer (ELBs), um eine angemesse ne Kapazität und Verfügbarkeit aufrechtzuerhalten. Zonenübergreifende s Load Balancing reduziert die Notwendigkeit, die gleiche Anzahl von Instances in jeder aktivierten Availability Zone aufrechtzuerhalten. Es verbessert auch die Fähigkeit Ihrer Anwendung, den Verlust einer oder mehrerer Instances zu bewältigen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
REL-10	Wie wird die Fehleriso lierung zum Schützen der Workload verwendet? Fehleriso lierte Grenzen beschränken die Auswirkungen eines Fehlers innerhalb einer Workload auf eine begrenzte Anzahl von Komponent en. Komponenten außerhalb der Grenze sind von dem Ausfall nicht betroffen. Durch die Verwendung mehrerer fehleriso lierter Grenzen können Sie die Auswirkungen auf Ihre Workload einschrän ken.	clb-multiple-az	Elastic Load Balancing (ELB) verteilt Ihren eingehenden Traffic automatisch auf mehrere Ziele wie EC2 Instances, Container und IP-Adressen in einer Availability Zone. Um eine hohe Verfügbar keit zu gewährlei sten, stellen Sie sicher, dass Ihr ELB Instances aus mehreren Availability Zones registriert hat.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
REL-10	Wie wird die Fehleriso lierung zum Schützen der Workload verwendet? Fehleriso lierte Grenzen beschränken die Auswirkungen eines Fehlers innerhalb einer Workload auf eine begrenzte Anzahl von Komponent en. Komponenten außerhalb der Grenze sind von dem Ausfall nicht betroffen. Durch die Verwendung mehrerer fehleriso lierter Grenzen können Sie die Auswirkungen auf Ihre Workload einschrän ken.	elbv2-multiple-az	Elastic Load Balancing (ELB) verteilt Ihren eingehenden Traffic automatisch auf mehrere Ziele wie EC2 Instances, Container und IP-Adressen in einer Availability Zone. Um eine hohe Verfügbar keit zu gewährlei sten, stellen Sie sicher, dass Ihr ELB Instances aus mehreren Availability Zones registriert hat.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
REL-10	Wie wird die Fehleriso lierung zum Schützen der Workload verwendet? Fehleriso lierte Grenzen beschränken die Auswirkungen eines Fehlers innerhalb einer Workload auf eine begrenzte Anzahl von Komponent en. Komponenten außerhalb der Grenze sind von dem Ausfall nicht betroffen. Durch die Verwendung mehrerer fehleriso lierter Grenzen können Sie die Auswirkungen auf Ihre Workload einschrän ken.	lambda-vpc-multi-az-überprüfen	Wenn Ihre AWS Lambda-Funktion so konfiguriert ist, dass sie eine Verbindun g zu einer Virtual Private Cloud (VPC) in Ihrem Konto herstellt, stellen Sie die AWS Lambda-Fu nktion in mindesten s zwei verschied enen Availability Zones bereit, um sicherzustellen, dass Ihre Funktion für die Verarbeit ung von Ereigniss en im Falle einer Dienstunterbrechung in einer einzigen Zone verfügbar ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
REL-10	Wie wird die Fehleriso lierung zum Schützen der Workload verwendet? Fehleriso lierte Grenzen beschränken die Auswirkungen eines Fehlers innerhalb einer Workload auf eine begrenzte Anzahl von Komponent en. Komponenten außerhalb der Grenze sind von dem Ausfall nicht betroffen. Durch die Verwendung mehrerer fehleriso lierter Grenzen können Sie die Auswirkungen auf Ihre Workload einschrän ken.	opensearch-data-no de-fault-Toleranz	Amazon OpenSearc h Service (OpenSear ch Service) benötigt mindestens drei Datenknoten für hohe Verfügbarkeit und Fehlertoleranz. Durch die Bereitstellung einer OpenSearc h Service-Domain mit mindestens drei Datenknoten wird der Cluster-Betrieb gewährleistet, falls ein Knoten ausfällt.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
REL-10	Wie wird die Fehleriso lierung zum Schützen der Workload verwendet? Fehleriso lierte Grenzen beschränken die Auswirkungen eines Fehlers innerhalb einer Workload auf eine begrenzte Anzahl von Komponent en. Komponenten außerhalb der Grenze sind von dem Ausfall nicht betroffen. Durch die Verwendung mehrerer fehleriso lierter Grenzen können Sie die Auswirkungen auf Ihre Workload einschrän ken.	rds-multi-az-support	Die Multi-AZ-Unterstüt zung in Amazon Relational Database Service (Amazon RDS) bietet eine verbesserte Verfügbar keit und Beständig keit von Datenbank -Instances. Wenn Sie eine Multi-AZ-Datenbank-Instance bereitste llen, erstellt Amazon RDS automatisch eine primäre Datenbank-Instance und replizier t die Daten synchron auf eine Standby-Instance in einer anderen Availability Zone. Jede Availabil ity Zone läuft auf einer eigenen, physisch getrennte n, unabhängigen Infrastruktur und ist auf eine hohe Verfügbarkeit ausgelegt. Im Falle eines Infrastru kturausfalls führt Amazon RDS einen automatis

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			chen Failover zum Standby-Modus durch, sodass Sie den Datenbankbetrieb wieder aufnehmen können, sobald der Failover abgeschlo ssen ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
REL-10	Wie wird die Fehleriso lierung zum Schützen der Workload verwendet? Fehleriso lierte Grenzen beschränken die Auswirkungen eines Fehlers innerhalb einer Workload auf eine begrenzte Anzahl von Komponent en. Komponenten außerhalb der Grenze sind von dem Ausfall nicht betroffen. Durch die Verwendung mehrerer fehleriso lierter Grenzen können Sie die Auswirkungen auf Ihre Workload einschrän ken.	rds-cluster-multi-az-aktiviert	Die Multi-AZ-Unterstüt zung in Amazon Relational Database Service (Amazon RDS) bietet eine verbesserte Verfügbar keit und Beständig keit von Datenbank -Instances. Wenn Sie eine Multi-AZ-Datenbank-Instance bereitste llen, erstellt Amazon RDS automatisch eine primäre Datenbank-Instance und replizier t die Daten synchron auf eine Standby-Instance in einer anderen Availability Zone. Jede Availabil ity Zone läuft auf einer eigenen, physisch getrennte n, unabhängigen Infrastruktur und ist auf eine hohe Verfügbarkeit ausgelegt. Im Falle eines Infrastru kturausfalls führt Amazon RDS einen automatis

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			chen Failover zum Standby-Modus durch, sodass Sie den Datenbankbetrieb wieder aufnehmen können, sobald der Failover abgeschlo ssen ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
REL-10	Wie wird die Fehleriso lierung zum Schützen der Workload verwendet? Fehleriso lierte Grenzen beschränken die Auswirkungen eines Fehlers innerhalb einer Workload auf eine begrenzte Anzahl von Komponent en. Komponenten außerhalb der Grenze sind von dem Ausfall nicht betroffen. Durch die Verwendung mehrerer fehleriso lierter Grenzen können Sie die Auswirkungen auf Ihre Workload einschrän ken.	vpc-vpn-2-tunnels-up	Redundante Site-to-Site VPN-Tunne l können implement iert werden, um die Anforderungen an die Ausfallsicherheit zu erfüllen. Es verwendet zwei Tunnel, um die Konnektivität sicherzustellen, falls eine der Site-to-Site VPN-Verbindungen nicht verfügbar ist. Um sich vor einem Verbindungsverlust zu schützen, können Sie für den Fall, dass Ihr Kunden-Gateway nicht verfügbar ist, eine zweite Site-to-S ite VPN-Verbindung zu Ihrer Amazon Virtual Private Cloud (Amazon VPC) und Ihrem Virtual Private Gateway einrichten, indem Sie ein zweites Kunden-Gateway verwenden.

Vorlage

Die Vorlage ist verfügbar unter GitHub: Operational Best Practices for AWS Well-Architected Reliability Pillar.

Bewährte betriebliche Verfahren für die AWS Sicherheitssäule eines Well-Architected Frameworks

Konformitätspakete bieten ein allgemeines Compliance-Framework, das es Ihnen ermöglicht, mithilfe verwalteter oder benutzerdefinierter Regeln und Abhilfemaßnahmen Kontrollen zur Sicherheits-, Betriebs- oder Kostenoptimierung durchzuführen. AWS Config AWS Config Conformance Packs dienen als Beispielvorlagen nicht dazu, die vollständige Einhaltung eines bestimmten Governance- oder Compliance-Standards sicherzustellen. Sie sind dafür verantwortlich, selbst zu beurteilen, ob Ihre Nutzung der Services den geltenden gesetzlichen und behördlichen Anforderungen entspricht.

Im Folgenden finden Sie ein Beispiel für eine Zuordnung zwischen der Well-Architected Framework-Sicherheitspillar von Amazon Web Services und den AWS verwalteten Konfigurationsregeln. Jede Config-Regel gilt für eine bestimmte AWS Ressource und bezieht sich auf eines oder mehrere Entwurfsprinzipien der Säule. Eine Well-Architected-Framework-Kategorie kann mit mehreren Konfigurationsregeln verknüpft werden. In der folgenden Tabelle finden Sie weitere Informationen und Anleitungen zu diesen Zuordnungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SEC-1	Wie wird Ihre Workload sicher verwaltet? Um Ihre Workload sicher zu betreiben, müssen Sie in allen Sicherheitsbereichen übergreifende bewährte Methoden anwenden. Wenden Sie die Anforderungen und Prozesse, die Sie im	account-part-of-organizations	Durch die zentrale Verwaltung AWS-Konten innerhalb von AWS Organizations wird sichergestellt, dass die Konten den Vorschriften entsprechen. Eine fehlende zentrale Kontoverwaltung kann zu inkonsistenten Kontokonf

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	Bereich Operational Excellence auf Organisations- und Workload-Ebene definiert haben, auf alle Bereiche an. Wenn Sie über Branchenempfehlungen AWS und Bedrohungsinformationen auf dem Laufenden bleiben, können Sie Ihr Bedrohungsmodell und Ihre Kontrollziele weiterentwickeln. Durch die Automatisierung von Sicherheitsprozessen, Tests und Validierungen können Sie Ihre Sicherheitsabläufe skalieren.		igurationen führen, wodurch Ressourcen und sensible Daten offengelegt werden können.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SEC-1	Wie wird Ihre Workload sicher verwaltet? Um Ihre Workload sicher zu betreiben, müssen Sie in allen Sicherheitsbereichen übergreifende bewährte Methoden anwenden. Wenden Sie die Anforderungen und Prozesse, die Sie im Bereich Operational Excellence auf Organisations- und Workload-Ebene definiert haben, auf alle Bereiche an. Wenn Sie über Branchenempfehlungen AWS und Bedrohungsinformationen auf dem Laufenden bleiben, können Sie Ihr Bedrohungsmodell und Ihre Kontrollziele weiterentwickeln. Durch die Automatisierung von Sicherheitsprozessen, Tests und Validierungen können Sie Ihre	mfa-enabled-for-iam-Konsolenzugriff	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass MFA für alle AWS Identity and Access Management (IAM) -Benutzer aktiviert ist, die über ein Konsolenkennwort verfügen. MFA sorgt für eine weitere Schutzebene zusätzlich zu den Anmeldeinformationen. Indem Sie MFA für Benutzer vorschreiben, können Sie Fälle kompromittierter Konten reduzieren und verhindern, dass unbefugte Benutzer auf vertrauliche Daten zugreifen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	Sicherheitsabläufe skalieren.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SEC-1	Wie wird Ihre Workload sicher verwaltet? Um Ihre Workload sicher zu betreiben, müssen Sie in allen Sicherheitsbereichen übergreifende bewährte Methoden anwenden. Wenden Sie die Anforderungen und Prozesse, die Sie im Bereich Operational Excellence auf Organisations- und Workload-Ebene definiert haben, auf alle Bereiche an. Wenn Sie über Branchenempfehlungen AWS und Bedrohungsinformationen auf dem Laufenden bleiben, können Sie Ihr Bedrohungsmodell und Ihre Kontrollziele weiterentwickeln. Durch die Automatisierung von Sicherheitsprozessen, Tests und Validierungen können Sie Ihre	iam-user-mfa-enabled	Aktivieren Sie diese Regel, um den Zugriff auf Ressourcen in der AWS Cloud einzuschränken. Diese Regel sorgt dafür, dass die Multi-Faktor-Authentifizierung (MFA) für alle Benutzer aktiviert ist. MFA sorgt für eine weitere Schutzebene zusätzlich zu den Anmeldeinformationen. Reduzieren Sie Fälle von kompromittierten Konten, indem Sie MFA für Benutzer vorschreiben.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	Sicherheitsabläufe skalieren.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SEC-1	Wie wird Ihre Workload sicher verwaltet? Um Ihre Workload sicher zu betreiben, müssen Sie in allen Sicherheitsbereichen übergreifende bewährte Methoden anwenden. Wenden Sie die Anforderungen und Prozesse, die Sie im Bereich Operational Excellence auf Organisations- und Workload-Ebene definiert haben, auf alle Bereiche an. Wenn Sie über Branchenempfehlungen AWS und Bedrohungsinformationen auf dem Laufenden bleiben, können Sie Ihr Bedrohungsmodell und Ihre Kontrollziele weiterentwickeln. Durch die Automatisierung von Sicherheitsprozessen, Tests und Validierungen können Sie Ihre	iam-root-access-key-überprüfen	Der Zugriff auf Systeme und Ressourcen kann gesteuert werden, indem überprüft wird, ob der Root-Benutzer keine Zugriffsschlüssel mit seiner AWS Identity and Access Management (IAM) -Rolle verknüpft hat. Stellen Sie sicher, dass die Root-Zugriffsschlüssel gelöscht werden. Erstellen und verwenden Sie stattdessen rollenbasierte Funktionen, AWS-Konten um das Prinzip der geringsten Funktionalität zu berücksichtigen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	Sicherheitsabläufe skalieren.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SEC-1	Wie wird Ihre Workload sicher verwaltet? Um Ihre Workload sicher zu betreiben, müssen Sie in allen Sicherheitsbereichen übergreifende bewährte Methoden anwenden. Wenden Sie die Anforderungen und Prozesse, die Sie im Bereich Operational Excellence auf Organisations- und Workload-Ebene definiert haben, auf alle Bereiche an. Wenn Sie über Branchenempfehlungen AWS und Bedrohungsinformationen auf dem Laufenden bleiben, können Sie Ihr Bedrohungsmodell und Ihre Kontrollziele weiterentwickeln. Durch die Automatisierung von Sicherheitsprozessen, Tests und Validierungen können Sie Ihre	root-account-hardware-mfa-aktiviert	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Hardware-MFA für den Root-Benutzer aktiviert ist. Der Stammbenutzer ist der AWS-Konto-Benutzer mit den meisten Berechtigungen. MFA sorgt für eine weitere Schutzebene zusätzlich zu den Anmeldeinformationen. Indem Sie MFA für den Root-Benutzer vorschreiben, können Sie die Anzahl AWS-Konten kompromittierter Benutzer reduzieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	Sicherheitsabläufe skalieren.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SEC-1	Wie wird Ihre Workload sicher verwaltet? Um Ihre Workload sicher zu betreiben, müssen Sie in allen Sicherheitsbereichen übergreifende bewährte Methoden anwenden. Wenden Sie die Anforderungen und Prozesse, die Sie im Bereich Operational Excellence auf Organisations- und Workload-Ebene definiert haben, auf alle Bereiche an. Wenn Sie über Branchenempfehlungen AWS und Bedrohungsinformationen auf dem Laufenden bleiben, können Sie Ihr Bedrohungsmodell und Ihre Kontrollziele weiterentwickeln. Durch die Automatisierung von Sicherheitsprozessen, Tests und Validierungen können Sie Ihre	root-account-mfa-enabled	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass MFA für den Root-Benutzer aktiviert ist. Der Stammbenutzer ist der AWS-Konto-Benutzer mit den meisten Berechtigungen. MFA sorgt für eine weitere Schutzebene zusätzlich zu den Anmeldeinformationen. Indem Sie MFA für den Root-Benutzer vorschreiben, können Sie die Anzahl AWS-Konten kompromittierter Benutzer reduzieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	Sicherheitsabläufe skalieren.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SEC-1	Wie wird Ihre Workload sicher verwaltet? Um Ihre Workload sicher zu betreiben, müssen Sie in allen Sicherheitsbereichen übergreifende bewährte Methoden anwenden. Wenden Sie die Anforderungen und Prozesse, die Sie im Bereich Operational Excellence auf Organisations- und Workload-Ebene definiert haben, auf alle Bereiche an. Wenn Sie über Branchenempfehlungen AWS und Bedrohungsinformationen auf dem Laufenden bleiben, können Sie Ihr Bedrohungsmodell und Ihre Kontrollziele weiterentwickeln. Durch die Automatisierung von Sicherheitsprozessen, Tests und Validierungen können Sie Ihre	ec2-manager instance-managed-by-systems	Eine Bestandsaufnahme der Softwareplattformen und Anwendungen innerhalb des Unternehmens ist möglich, indem Amazon Elastic Compute Cloud (Amazon EC2) - Instances mit AWS Systems Manager verwaltet werden. Verwenden Sie AWS Systems Manager, um detaillierte Systemkonfigurationen, Betriebssystem-Patch-Levels, Namen und Typ der Dienste, Softwareinstallationen, Anwendungsname, Herausgeber und Version sowie andere Details zu Ihrer Umgebung bereitzustellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	Sicherheitsabläufe skalieren.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SEC-1	Wie wird Ihre Workload sicher verwaltet? Um Ihre Workload sicher zu betreiben, müssen Sie in allen Sicherheitsbereichen übergreifende bewährte Methoden anwenden. Wenden Sie die Anforderungen und Prozesse, die Sie im Bereich Operational Excellence auf Organisations- und Workload-Ebene definiert haben, auf alle Bereiche an. Wenn Sie über Branchenempfehlungen AWS und Bedrohungsinformationen auf dem Laufenden bleiben, können Sie Ihr Bedrohungsmodell und Ihre Kontrollziele weiterentwickeln. Durch die Automatisierung von Sicherheitsprozessen, Tests und Validierungen können Sie Ihre	ec2-check managedinstance-association-compliance-status	Verwenden Sie AWS Systems Manager Associations, um bei der Inventarisierung von Softwareplattformen und Anwendungen innerhalb eines Unternehmens zu helfen. AWS Systems Manager weist Ihren verwalteten Instanzen einen Konfigurationsstatus zu und ermöglicht es Ihnen, Basiswerte für Betriebssystem-Patch-Levels, Softwareinstallationen, Anwendungskonfigurationen und andere Details zu Ihrer Umgebung festzulegen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	Sicherheitsabläufe skalieren.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SEC-1	Wie wird Ihre Workload sicher verwaltet? Um Ihre Workload sicher zu betreiben, müssen Sie in allen Sicherheitsbereichen übergreifende bewährte Methoden anwenden. Wenden Sie die Anforderungen und Prozesse, die Sie im Bereich Operational Excellence auf Organisations- und Workload-Ebene definiert haben, auf alle Bereiche an. Wenn Sie über Branchenempfehlungen AWS und Bedrohungsinformationen auf dem Laufenden bleiben, können Sie Ihr Bedrohungsmodell und Ihre Kontrollziele weiterentwickeln. Durch die Automatisierung von Sicherheitsprozessen, Tests und Validierungen können Sie Ihre	ec2-check managedinstance-patch-compliance-status	Aktivieren Sie diese Regel, um bei der Identifizierung und Dokumentation von Sicherheitslücken in Amazon Elastic Compute Cloud (Amazon EC2) zu helfen. Die Regel prüft, ob die EC2 Amazon-Instance die Patch-Konformität im AWS Systems Manager gemäß den Richtlinien und Verfahren Ihrer Organisation einhält.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	Sicherheitsabläufe skalieren.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SEC-1	Wie wird Ihre Workload sicher verwaltet? Um Ihre Workload sicher zu betreiben, müssen Sie in allen Sicherheitsbereichen übergreifende bewährte Methoden anwenden. Wenden Sie die Anforderungen und Prozesse, die Sie im Bereich Operational Excellence auf Organisations- und Workload-Ebene definiert haben, auf alle Bereiche an. Wenn Sie über Branchenempfehlungen AWS und Bedrohungsinformationen auf dem Laufenden bleiben, können Sie Ihr Bedrohungsmodell und Ihre Kontrollziele weiterentwickeln. Durch die Automatisierung von Sicherheitsprozessen, Tests und Validierungen können Sie Ihre	codebuild-project-envvar-awscred-überprüfen	Stellen Sie sicher, dass die Anmeldeinformationen AWS_ACCESS_KEY_ID AWS_SECRET_ACCESS_KEY nicht in AWS Codebuild-Projektumgebungen vorhanden sind. Speichern Sie diese Variablen nicht als Klartext. Das Speichern dieser Variablen als Klartext bewirkt eine unbeabsichtigte Offenlegung von Daten sowie unberechtigte Zugriffe.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	Sicherheitsabläufe skalieren.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SEC-2	Wie werden Identitäten für Personen und Computer verwaltet? Es gibt zwei Arten von Identitäten, die Sie verwalten müssen, wenn Sie sichere AWS Workloads betreiben möchten. Wenn Sie wissen, welche Art von Identität Sie verwalten und mit Zugriffsberechtigungen ausstatten müssen, können Sie sicherstellen, dass die richtigen Identitäten unter den richtigen Bedingungen Zugriff auf die richtigen Ressourcen haben. Menschliche Identitäten: Ihre Administratoren, Entwickler, Betreiber und Endbenutzer benötigen eine Identität, um auf Ihre AWS Umgebungen und Anwendungen zugreifen zu können. Dies sind Mitglieder Ihrer Organisat	iam-password-policy	Die Identitäten und Anmeldeinformationen werden auf der Grundlage einer organisatorischen IAM-Passwortrichtlinie ausgestellt, verwaltet und verifiziert. Sie erfüllen oder übertreffen die Anforderungen, die von NIST SP 800-63 und dem Standard „Best Practices“ von AWS Foundational Security für die Passwortstärke festgelegt sind. Mit dieser Regel können Sie optional RequireUppercaseCharacters (Wert für AWS grundlegende Sicherheitsbewährte Methoden: wahr), RequireLowercaseCharacters (Wert für bewährte Methoden für AWS grundlegende Sicherheit: wahr), RequireSymbols (Wert für bewährte Methoden für AWS grundlege

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	ion oder externe Benutzer, mit denen Sie zusammenarbeiten und die über einen Webbrowser, eine Client-Anwendung oder interaktive Befehlszeilentools mit Ihren AWS Ressourcen interagieren. Maschinenidentitäten: Ihre Dienstanwendungen, Betriebstools und Workloads benötigen eine Identität, um Anfragen an AWS Dienste zu stellen — beispielsweise um Daten zu lesen. Zu diesen Identitäten gehören Maschinen, die in Ihrer AWS Umgebung ausgeführt werden, wie EC2 Amazon-Instances oder AWS Lambda-Funktionen. Sie können auch Maschinenidentitäten für externe Parteien verwalten, die Zugriff benötigen. Darüber hinaus benötigen Sie		nde Sicherheit: wahr), RequireNumbers (Wert für bewährte Methoden für AWS grundlegende Sicherheit: wahr), MinimumPasswordLength (Wert für bewährte Methoden für AWS grundlegende Sicherheit: 14), PasswordReusePrevention (Wert für bewährte Methoden für AWS grundlegende Sicherheit: 24) und MaxPasswordAge (Wert für bewährte Methoden für AWS grundlegende Sicherheit: 90) für Ihr IAM festlegen. Kennwortrichtlinie. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	möglicherweise auch Maschinen außerhalb AWS , die Zugriff auf Ihre AWS Umgebung benötigen.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SEC-2	Wie werden Identitäten für Personen und Computer verwaltet? Es gibt zwei Arten von Identitäten, die Sie verwalten müssen, wenn Sie sichere AWS Workloads betreiben möchten. Wenn Sie wissen, welche Art von Identität Sie verwalten und mit Zugriffsberechtigungen ausstatten müssen, können Sie sicherstellen, dass die richtigen Identitäten unter den richtigen Bedingungen Zugriff auf die richtigen Ressourcen haben. Menschliche Identitäten: Ihre Administratoren, Entwickler, Betreiber und Endbenutzer benötigen eine Identität, um auf Ihre AWS Umgebungen und Anwendungen zugreifen zu können. Dies sind Mitglieder Ihrer Organisat	root-account-hardware-mfa-aktiviert	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Hardware-MFA für den Root-Benutzer aktiviert ist. Der Stammbenutzer ist der AWS-Konto-Benutzer mit den meisten Berechtigungen. MFA sorgt für eine weitere Schutzebene zusätzlich zu den Anmeldeinformationen. Indem Sie MFA für den Root-Benutzer vorschreiben, können Sie die Anzahl AWS-Konten kompromittierter Benutzer reduzieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	ion oder externe Benutzer, mit denen Sie zusammena rbeiten und die über einen Webbrowse r, eine Client-An wendung oder interaktive Befehlsze ilentools mit Ihren AWS Ressource n interagieren. Maschinenidentität en: Ihre Dienstanw endungen, Betriebst ools und Workloads benötigen eine Identität, um Anfragen an AWS Dienste zu stellen — beispiels weise um Daten zu lesen. Zu diesen Identitäten gehören Maschinen, die in Ihrer AWS Umgebung ausgeführt werden, wie EC2 Amazon-In stances oder AWS Lambda-Funktionen. Sie können auch Maschinenidentitäten für externe Parteien verwalten, die Zugriff benötigen. Darüber hinaus benötigen Sie		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	möglicherweise auch Maschinen außerhalb AWS , die Zugriff auf Ihre AWS Umgebung benötigen.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SEC-2	Wie werden Identitäten für Personen und Computer verwaltet? Es gibt zwei Arten von Identitäten, die Sie verwalten müssen, wenn Sie sichere Workloads betreiben möchten. AWS Wenn Sie wissen, welche Art von Identität Sie verwalten und mit Zugriffsberechtigungen ausstatten müssen, können Sie sicherstellen, dass die richtigen Identitäten unter den richtigen Bedingungen Zugriff auf die richtigen Ressourcen haben. Menschliche Identitäten: Ihre Administratoren, Entwickler, Betreiber und Endbenutzer benötigen eine Identität, um auf Ihre AWS Umgebungen und Anwendungen zugreifen zu können. Dies sind Mitglieder Ihrer Organisat	root-account-mfa-enabled	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass MFA für den Root-Benutzer aktiviert ist. Der Stammbenutzer ist der AWS-Konto-Benutzer mit den meisten Berechtigungen. MFA sorgt für eine weitere Schutzebene zusätzlich zu den Anmeldeinformationen. Indem Sie MFA für den Root-Benutzer vorschreiben, können Sie die Anzahl AWS-Konten kompromittierter Benutzer reduzieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	ion oder externe Benutzer, mit denen Sie zusammena rbeiten und die über einen Webbrowse r, eine Client-An wendung oder interaktive Befehlsze ilentools mit Ihren AWS Ressource n interagieren. Maschinenidentität en: Ihre Dienstanw endungen, Betriebst ools und Workloads benötigen eine Identität, um Anfragen an AWS Dienste zu stellen — beispiels weise um Daten zu lesen. Zu diesen Identitäten gehören Maschinen, die in Ihrer AWS Umgebung ausgeführt werden, wie EC2 Amazon-In stances oder AWS Lambda-Funktionen. Sie können auch Maschinenidentitäten für externe Parteien verwalten, die Zugriff benötigen. Darüber hinaus benötigen Sie		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	möglicherweise auch Maschinen außerhalb AWS , die Zugriff auf Ihre AWS Umgebung benötigen.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SEC-2	Wie werden Identitäten für Personen und Computer verwaltet? Es gibt zwei Arten von Identitäten, die Sie verwalten müssen, wenn Sie sichere Workloads betreiben möchten. AWS Wenn Sie wissen, welche Art von Identität Sie verwalten und mit Zugriffsberechtigungen ausstatten müssen, können Sie sicherstellen, dass die richtigen Identitäten unter den richtigen Bedingungen Zugriff auf die richtigen Ressourcen haben. Menschliche Identitäten: Ihre Administratoren, Entwickler, Betreiber und Endbenutzer benötigen eine Identität, um auf Ihre AWS Umgebungen und Anwendungen zugreifen zu können. Dies sind Mitglieder Ihrer Organisat	iam-user-mfa-enabled	Aktivieren Sie diese Regel, um den Zugriff auf Ressourcen in der AWS Cloud einzuschränken. Diese Regel sorgt dafür, dass die Multi-Faktor-Authentifizierung (MFA) für alle Benutzer aktiviert ist. MFA sorgt für eine weitere Schutzebene zusätzlich zu den Anmeldeinformationen. Reduzieren Sie Fälle von kompromittierten Konten, indem Sie MFA für Benutzer vorschreiben.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	ion oder externe Benutzer, mit denen Sie zusammena rbeiten und die über einen Webbrowse r, eine Client-An wendung oder interaktive Befehlsze ilentools mit Ihren AWS Ressource n interagieren. Maschinenidentität en: Ihre Dienstanw endungen, Betriebst ools und Workloads benötigen eine Identität, um Anfragen an AWS Dienste zu stellen — beispiels weise um Daten zu lesen. Zu diesen Identitäten gehören Maschinen, die in Ihrer AWS Umgebung ausgeführt werden, wie EC2 Amazon-In stances oder AWS Lambda-Funktionen. Sie können auch Maschinenidentitäten für externe Parteien verwalten, die Zugriff benötigen. Darüber hinaus benötigen Sie		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	möglicherweise auch Maschinen außerhalb AWS , die Zugriff auf Ihre AWS Umgebung benötigen.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SEC-2	Wie werden Identitäten für Personen und Computer verwaltet? Es gibt zwei Arten von Identitäten, die Sie verwalten müssen, wenn Sie sichere AWS Workloads betreiben möchten. Wenn Sie wissen, welche Art von Identität Sie verwalten und mit Zugriffsberechtigungen ausstatten müssen, können Sie sicherstellen, dass die richtigen Identitäten unter den richtigen Bedingungen Zugriff auf die richtigen Ressourcen haben. Menschliche Identitäten: Ihre Administratoren, Entwickler, Betreiber und Endbenutzer benötigen eine Identität, um auf Ihre AWS Umgebungen und Anwendungen zugreifen zu können. Dies sind Mitglieder Ihrer Organisat	mfa-enabled-for-iam-Konsolenzugriff	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass MFA für alle AWS Identity and Access Management (IAM) -Benutzer aktiviert ist, die über ein Konsolenkennwort verfügen. MFA sorgt für eine weitere Schutzebene zusätzlich zu den Anmeldeinformationen. Indem Sie MFA für Benutzer vorschreiben, können Sie Fälle kompromittierter Konten reduzieren und verhindern, dass unbefugte Benutzer auf vertrauliche Daten zugreifen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	ion oder externe Benutzer, mit denen Sie zusammena rbeiten und die über einen Webbrowse r, eine Client-An wendung oder interaktive Befehlsze ilentools mit Ihren AWS Ressource n interagieren. Maschinenidentität en: Ihre Dienstanw endungen, Betriebst ools und Workloads benötigen eine Identität, um Anfragen an AWS Dienste zu stellen — beispiels weise um Daten zu lesen. Zu diesen Identitäten gehören Maschinen, die in Ihrer AWS Umgebung ausgeführt werden, wie EC2 Amazon-In stances oder AWS Lambda-Funktionen. Sie können auch Maschinenidentitäten für externe Parteien verwalten, die Zugriff benötigen. Darüber hinaus benötigen Sie		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	möglicherweise auch Maschinen außerhalb AWS , die Zugriff auf Ihre AWS Umgebung benötigen.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SEC-2	Wie werden Identitäten für Personen und Computer verwaltet? Es gibt zwei Arten von Identitäten, die Sie verwalten müssen, wenn Sie sichere Workloads betreiben möchten. AWS Wenn Sie wissen, welche Art von Identität Sie verwalten und mit Zugriffsberechtigungen ausstatten müssen, können Sie sicherstellen, dass die richtigen Identitäten unter den richtigen Bedingungen Zugriff auf die richtigen Ressourcen haben. Menschliche Identitäten: Ihre Administratoren, Entwickler, Betreiber und Endbenutzer benötigen eine Identität, um auf Ihre AWS Umgebungen und Anwendungen zugreifen zu können. Dies sind Mitglieder Ihrer Organisat	ecs-task-definition-user-for-host-mode-check	Wenn für eine Aufgabendefinition erhöhte Berechtigungen gelten, liegt das daran, dass der Kunde diesen Konfigurationen ausdrücklich zugestimmt hat. Diese Kontrolle prüft, ob eine unerwartete Berechtigungseskalation vorliegt, wenn für eine Aufgabendefinition das Host-Netzwerk aktiviert ist, der Kunde aber keine erhöhten Berechtigungen aktiviert hat.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	ion oder externe Benutzer, mit denen Sie zusammena rbeiten und die über einen Webbrowse r, eine Client-An wendung oder interaktive Befehlsze ilentools mit Ihren AWS Ressource n interagieren. Maschinenidentität en: Ihre Dienstanw endungen, Betriebst ools und Workloads benötigen eine Identität, um Anfragen an AWS Dienste zu stellen — beispiels weise um Daten zu lesen. Zu diesen Identitäten gehören Maschinen, die in Ihrer AWS Umgebung ausgeführt werden, wie EC2 Amazon-In stances oder AWS Lambda-Funktionen. Sie können auch Maschinenidentitäten für externe Parteien verwalten, die Zugriff benötigen. Darüber hinaus benötigen Sie		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	möglicherweise auch Maschinen außerhalb AWS , die Zugriff auf Ihre AWS Umgebung benötigen.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SEC-2	Wie werden Identitäten für Personen und Computer verwaltet? Es gibt zwei Arten von Identitäten, die Sie verwalten müssen, wenn Sie sichere AWS Workloads betreiben möchten. Wenn Sie wissen, welche Art von Identität Sie verwalten und mit Zugriffsberechtigungen ausstatten müssen, können Sie sicherstellen, dass die richtigen Identitäten unter den richtigen Bedingungen Zugriff auf die richtigen Ressourcen haben. Menschliche Identitäten: Ihre Administratoren, Entwickler, Betreiber und Endbenutzer benötigen eine Identität, um auf Ihre AWS Umgebungen und Anwendungen zugreifen zu können. Dies sind Mitglieder Ihrer Organisat	iam-group-has-users-überprüfen	AWS Identity and Access Management (IAM) kann Ihnen helfen, die Prinzipien der geringsten Rechte und der Aufgabentrennung mit Zugriffsberechtigungen und Autorisierungen zu integrieren, indem sichergestellt wird, dass IAM-Gruppen mindestens einen Benutzer haben. Die Einteilung von Benutzern in Gruppen auf der Grundlage der ihnen zugewiesenen Berechtigungen oder ihrer Funktion ist eine Möglichkeit, das Prinzip der geringsten Berechtigung zu implementieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	ion oder externe Benutzer, mit denen Sie zusammena rbeiten und die über einen Webbrowse r, eine Client-An wendung oder interaktive Befehlsze ilentools mit Ihren AWS Ressource n interagieren. Maschinenidentität en: Ihre Dienstanw endungen, Betriebst ools und Workloads benötigen eine Identität, um Anfragen an AWS Dienste zu stellen — beispiels weise um Daten zu lesen. Zu diesen Identitäten gehören Maschinen, die in Ihrer AWS Umgebung ausgeführt werden, wie EC2 Amazon-In stances oder AWS Lambda-Funktionen. Sie können auch Maschinenidentitäten für externe Parteien verwalten, die Zugriff benötigen. Darüber hinaus benötigen Sie		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	möglicherweise auch Maschinen außerhalb AWS , die Zugriff auf Ihre AWS Umgebung benötigen.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SEC-2	Wie werden Identitäten für Personen und Computer verwaltet? Es gibt zwei Arten von Identitäten, die Sie verwalten müssen, wenn Sie sichere Workloads betreiben möchten. AWS Wenn Sie wissen, welche Art von Identität Sie verwalten und mit Zugriffsberechtigungen ausstatten müssen, können Sie sicherstellen, dass die richtigen Identitäten unter den richtigen Bedingungen Zugriff auf die richtigen Ressourcen haben. Menschliche Identitäten: Ihre Administratoren, Entwickler, Betreiber und Endbenutzer benötigen eine Identität, um auf Ihre AWS Umgebungen und Anwendungen zugreifen zu können. Dies sind Mitglieder Ihrer Organisat	iam-no-inline-policy-überprüfen	Stellen Sie sicher, dass ein Benutzer, eine IAM-Rolle oder eine IAM-Gruppe (AWS Identity and Access Management) nicht über eine Inline-Richtlinie zur Zugriffskontrolle auf Systeme und Ressourcen verfügt. AWS empfiehlt, verwaltete Richtlinien anstelle von Inline-Richtlinien zu verwenden. Verwaltete Richtlinien ermöglichen Wiederverwendbarkeit, Versionsverwaltung, Rollback und Delegierung der Berechtigungsverwaltung.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	ion oder externe Benutzer, mit denen Sie zusammena rbeiten und die über einen Webbrowse r, eine Client-An wendung oder interaktive Befehlsze ilentools mit Ihren AWS Ressource n interagieren. Maschinenidentität en: Ihre Dienstanw endungen, Betriebst ools und Workloads benötigen eine Identität, um Anfragen an AWS Dienste zu stellen — beispiels weise um Daten zu lesen. Zu diesen Identitäten gehören Maschinen, die in Ihrer AWS Umgebung ausgeführt werden, wie EC2 Amazon-In stances oder AWS Lambda-Funktionen. Sie können auch Maschinenidentitäten für externe Parteien verwalten, die Zugriff benötigen. Darüber hinaus benötigen Sie		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	möglicherweise auch Maschinen außerhalb AWS , die Zugriff auf Ihre AWS Umgebung benötigen.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SEC-2	Wie werden Identitäten für Personen und Computer verwaltet? Es gibt zwei Arten von Identitäten, die Sie verwalten müssen, wenn Sie sichere AWS Workloads betreiben möchten. Wenn Sie wissen, welche Art von Identität Sie verwalten und mit Zugriffsberechtigungen ausstatten müssen, können Sie sicherstellen, dass die richtigen Identitäten unter den richtigen Bedingungen Zugriff auf die richtigen Ressourcen haben. Menschliche Identitäten: Ihre Administratoren, Entwickler, Betreiber und Endbenutzer benötigen eine Identität, um auf Ihre AWS Umgebungen und Anwendungen zugreifen zu können. Dies sind Mitglieder Ihrer Organisat	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) kann Ihnen dabei helfen, die Prinzipien der geringsten Rechte und der Aufgabentrennung in Zugriffsberechtigungen und Autorisierungen zu integrieren und so zu verhindern, dass Richtlinien „Effect“: „Allow“ mit „Action“: „*“ anstelle von „Resource“: „*“ enthalten. Wenn Benutzern mehr Rechte eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und der Aufgabentrennung verstoßen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	ion oder externe Benutzer, mit denen Sie zusammena rbeiten und die über einen Webbrowse r, eine Client-An wendung oder interaktive Befehlsze ilentools mit Ihren AWS Ressource n interagieren. Maschinenidentität en: Ihre Dienstanw endungen, Betriebst ools und Workloads benötigen eine Identität, um Anfragen an AWS Dienste zu stellen — beispiels weise um Daten zu lesen. Zu diesen Identitäten gehören Maschinen, die in Ihrer AWS Umgebung ausgeführt werden, wie EC2 Amazon-In stances oder AWS Lambda-Funktionen. Sie können auch Maschinenidentitäten für externe Parteien verwalten, die Zugriff benötigen. Darüber hinaus benötigen Sie		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	möglicherweise auch Maschinen außerhalb AWS , die Zugriff auf Ihre AWS Umgebung benötigen.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SEC-2	Wie werden Identitäten für Personen und Computer verwaltet? Es gibt zwei Arten von Identitäten, die Sie verwalten müssen, wenn es um betriebssichere Workloads geht. AWS Wenn Sie wissen, welche Art von Identität Sie verwalten und mit Zugriffsberechtigungen ausstatten müssen, können Sie sicherstellen, dass die richtigen Identitäten unter den richtigen Bedingungen Zugriff auf die richtigen Ressourcen haben. Menschliche Identitäten: Ihre Administratoren, Entwickler, Betreiber und Endbenutzer benötigen eine Identität, um auf Ihre AWS Umgebungen und Anwendungen zugreifen zu können. Dies sind Mitglieder Ihrer Organisat	iam-policy-no-statements-with-full-access	Stellen Sie sicher, dass IAM-Aktionen nur auf die benötigten Aktionen beschränkt sind. Wenn Benutzern mehr Berechtigungen eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und Aufgabentrennung verstoßen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	ion oder externe Benutzer, mit denen Sie zusammena rbeiten und die über einen Webbrowse r, eine Client-An wendung oder interaktive Befehlsze ilentools mit Ihren AWS Ressource n interagieren. Maschinenidentität en: Ihre Dienstanw endungen, Betriebst ools und Workloads benötigen eine Identität, um Anfragen an AWS Dienste zu stellen — beispiels weise um Daten zu lesen. Zu diesen Identitäten gehören Maschinen, die in Ihrer AWS Umgebung ausgeführt werden, wie EC2 Amazon-In stances oder AWS Lambda-Funktionen. Sie können auch Maschinenidentitäten für externe Parteien verwalten, die Zugriff benötigen. Darüber hinaus benötigen Sie		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	möglicherweise auch Maschinen außerhalb AWS , die Zugriff auf Ihre AWS Umgebung benötigen.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SEC-2	Wie werden Identitäten für Personen und Computer verwaltet? Es gibt zwei Arten von Identitäten, die Sie verwalten müssen, wenn Sie sichere AWS Workloads betreiben möchten. Wenn Sie wissen, welche Art von Identität Sie verwalten und mit Zugriffsberechtigungen ausstatten müssen, können Sie sicherstellen, dass die richtigen Identitäten unter den richtigen Bedingungen Zugriff auf die richtigen Ressourcen haben. Menschliche Identitäten: Ihre Administratoren, Entwickler, Betreiber und Endbenutzer benötigen eine Identität, um auf Ihre AWS Umgebungen und Anwendungen zugreifen zu können. Dies sind Mitglieder Ihrer Organisat	iam-user-group-membership-überprüfen	AWS Identity and Access Management (IAM) kann Ihnen helfen, Zugriffsberechtigungen und Autorisierungen einzuschränken, indem sichergestellt wird, dass Benutzer Mitglieder mindestens einer Gruppe sind. Wenn Benutzern mehr Berechtigungen eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und Aufgabentrennung verstoßen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	ion oder externe Benutzer, mit denen Sie zusammena rbeiten und die über einen Webbrowse r, eine Client-An wendung oder interaktive Befehlsze ilentools mit Ihren AWS Ressource n interagieren. Maschinenidentität en: Ihre Dienstanw endungen, Betriebst ools und Workloads benötigen eine Identität, um Anfragen an AWS Dienste zu stellen — beispiels weise um Daten zu lesen. Zu diesen Identitäten gehören Maschinen, die in Ihrer AWS Umgebung ausgeführt werden, wie EC2 Amazon-In stances oder AWS Lambda-Funktionen. Sie können auch Maschinenidentitäten für externe Parteien verwalten, die Zugriff benötigen. Darüber hinaus benötigen Sie		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	möglicherweise auch Maschinen außerhalb AWS , die Zugriff auf Ihre AWS Umgebung benötigen.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SEC-2	Wie werden Identitäten für Personen und Computer verwaltet? Es gibt zwei Arten von Identitäten, die Sie verwalten müssen, wenn Sie sichere Workloads betreiben möchten. AWS Wenn Sie wissen, welche Art von Identität Sie verwalten und mit Zugriffsberechtigungen ausstatten müssen, können Sie sicherstellen, dass die richtigen Identitäten unter den richtigen Bedingungen Zugriff auf die richtigen Ressourcen haben. Menschliche Identitäten: Ihre Administratoren, Entwickler, Betreiber und Endbenutzer benötigen eine Identität, um auf Ihre AWS Umgebungen und Anwendungen zugreifen zu können. Dies sind Mitglieder Ihrer Organisat	iam-user-unused-credentials-überprüfen	AWS Identity and Access Management (IAM) kann Ihnen bei Zugriffsberechtigungen und Autorisierungen helfen, indem es nach IAM-Passwörtern und Zugriffsschlüsseln sucht, die für einen bestimmten Zeitraum nicht verwendet wurden. Wenn ungenutzte Anmeldeinformationen identifiziert werden, müssen Sie sie deaktivieren und/oder entfernen, da dies gegen das Prinzip der geringsten Berechtigung verstoßen könnte. Für diese Regel müssen Sie einen Wert für das maxCredentialUsage Alter festlegen (Standardkonfiguration: 90). Der tatsächliche Wert muss den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	ion oder externe Benutzer, mit denen Sie zusammena rbeiten und die über einen Webbrowse r, eine Client-An wendung oder interaktive Befehlsze ilentools mit Ihren AWS Ressource n interagieren. Maschinenidentität en: Ihre Dienstanw endungen, Betriebst ools und Workloads benötigen eine Identität, um Anfragen an AWS Dienste zu stellen — beispiels weise um Daten zu lesen. Zu diesen Identitäten gehören Maschinen, die in Ihrer AWS Umgebung ausgeführt werden, wie EC2 Amazon-In stances oder AWS Lambda-Funktionen. Sie können auch Maschinenidentitäten für externe Parteien verwalten, die Zugriff benötigen. Darüber hinaus benötigen Sie		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	möglicherweise auch Maschinen außerhalb AWS , die Zugriff auf Ihre AWS Umgebung benötigen.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SEC-2	Wie werden Identitäten für Personen und Computer verwaltet? Es gibt zwei Arten von Identitäten, die Sie verwalten müssen, wenn Sie sichere AWS Workloads betreiben möchten. Wenn Sie wissen, welche Art von Identität Sie verwalten und mit Zugriffsberechtigungen ausstatten müssen, können Sie sicherstellen, dass die richtigen Identitäten unter den richtigen Bedingungen Zugriff auf die richtigen Ressourcen haben. Menschliche Identitäten: Ihre Administratoren, Entwickler, Betreiber und Endbenutzer benötigen eine Identität, um auf Ihre AWS Umgebungen und Anwendungen zugreifen zu können. Dies sind Mitglieder Ihrer Organisat	secretsmanager-rotation-enabled-check	Diese Regel stellt sicher, dass bei AWS Secrets Manager Manager-Geheimnissen die Rotation aktiviert ist. Die regelmäßige Rotation von Secrets kann den Zeitraum verkürzen, in dem ein Secret aktiv ist, und möglicherweise die Auswirkungen auf das Unternehmen verringern, falls das Secret kompromittiert wird.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	ion oder externe Benutzer, mit denen Sie zusammena rbeiten und die über einen Webbrowse r, eine Client-An wendung oder interaktive Befehlsze ilentools mit Ihren AWS Ressource n interagieren. Maschinenidentität en: Ihre Dienstanw endungen, Betriebst ools und Workloads benötigen eine Identität, um Anfragen an AWS Dienste zu stellen — beispiels weise um Daten zu lesen. Zu diesen Identitäten gehören Maschinen, die in Ihrer AWS Umgebung ausgeführt werden, wie EC2 Amazon-In stances oder AWS Lambda-Funktionen. Sie können auch Maschinenidentitäten für externe Parteien verwalten, die Zugriff benötigen. Darüber hinaus benötigen Sie		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	möglicherweise auch Maschinen außerhalb AWS , die Zugriff auf Ihre AWS Umgebung benötigen.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SEC-2	Wie werden Identitäten für Personen und Computer verwaltet? Es gibt zwei Arten von Identitäten, die Sie verwalten müssen, wenn Sie sichere AWS Workloads betreiben möchten. Wenn Sie wissen, welche Art von Identität Sie verwalten und mit Zugriffsberechtigungen ausstatten müssen, können Sie sicherstellen, dass die richtigen Identitäten unter den richtigen Bedingungen Zugriff auf die richtigen Ressourcen haben. Menschliche Identitäten: Ihre Administratoren, Entwickler, Betreiber und Endbenutzer benötigen eine Identität, um auf Ihre AWS Umgebungen und Anwendungen zugreifen zu können. Dies sind Mitglieder Ihrer Organisat	secretsmanager-scheduled-rotation-success-überprüfen	Diese Regel stellt sicher, dass AWS Secrets Manager Manager-Geheimnisse gemäß dem Rotationsplan erfolgreich rotiert wurden. Die regelmäßige Rotation von Secrets kann den Zeitraum verkürzen, in dem ein Secret aktiv ist, und möglicherweise die Auswirkungen auf das Unternehmen verringern, falls es kompromittiert wird.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	ion oder externe Benutzer, mit denen Sie zusammena rbeiten und die über einen Webbrowse r, eine Client-An wendung oder interaktive Befehlsze ilentools mit Ihren AWS Ressource n interagieren. Maschinenidentität en: Ihre Dienstanw endungen, Betriebst ools und Workloads benötigen eine Identität, um Anfragen an AWS Dienste zu stellen — beispiels weise um Daten zu lesen. Zu diesen Identitäten gehören Maschinen, die in Ihrer AWS Umgebung ausgeführt werden, wie EC2 Amazon-In stances oder AWS Lambda-Funktionen. Sie können auch Maschinenidentitäten für externe Parteien verwalten, die Zugriff benötigen. Darüber hinaus benötigen Sie		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	möglicherweise auch Maschinen außerhalb AWS , die Zugriff auf Ihre AWS Umgebung benötigen.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SEC-2	Wie werden Identitäten für Personen und Computer verwaltet? Es gibt zwei Arten von Identitäten, die Sie verwalten müssen, wenn Sie sichere AWS Workloads betreiben möchten. Wenn Sie wissen, welche Art von Identität Sie verwalten und mit Zugriffsberechtigungen ausstatten müssen, können Sie sicherstellen, dass die richtigen Identitäten unter den richtigen Bedingungen Zugriff auf die richtigen Ressourcen haben. Menschliche Identitäten: Ihre Administratoren, Entwickler, Betreiber und Endbenutzer benötigen eine Identität, um auf Ihre AWS Umgebungen und Anwendungen zugreifen zu können. Dies sind Mitglieder Ihrer Organisat	secretsmanager-secret-periodic-rotation	Diese Regel stellt sicher, dass bei AWS Secrets Manager Manager-Geheimnissen die regelmäßige Rotation aktiviert ist. Die regelmäßige Rotation von Secrets kann den Zeitraum verkürzen, in dem ein Secret aktiv ist, und möglicherweise die Auswirkungen auf das Unternehmen verringern, falls das Secret kompromittiert wird. Der Standardwert lautet 90 Tage.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	ion oder externe Benutzer, mit denen Sie zusammena rbeiten und die über einen Webbrowse r, eine Client-An wendung oder interaktive Befehlsze ilentools mit Ihren AWS Ressource n interagieren. Maschinenidentität en: Ihre Dienstanw endungen, Betriebst ools und Workloads benötigen eine Identität, um Anfragen an AWS Dienste zu stellen — beispiels weise um Daten zu lesen. Zu diesen Identitäten gehören Maschinen, die in Ihrer AWS Umgebung ausgeführt werden, wie EC2 Amazon-In stances oder AWS Lambda-Funktionen. Sie können auch Maschinenidentitäten für externe Parteien verwalten, die Zugriff benötigen. Darüber hinaus benötigen Sie		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	möglicherweise auch Maschinen außerhalb AWS , die Zugriff auf Ihre AWS Umgebung benötigen.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SEC-2	Wie werden Identitäten für Personen und Computer verwaltet? Es gibt zwei Arten von Identitäten, die Sie verwalten müssen, wenn Sie sichere AWS Workloads betreiben möchten. Wenn Sie wissen, welche Art von Identität Sie verwalten und mit Zugriffsberechtigungen ausstatten müssen, können Sie sicherstellen, dass die richtigen Identitäten unter den richtigen Bedingungen Zugriff auf die richtigen Ressourcen haben. Menschliche Identitäten: Ihre Administratoren, Entwickler, Betreiber und Endbenutzer benötigen eine Identität, um auf Ihre AWS Umgebungen und Anwendungen zugreifen zu können. Dies sind Mitglieder Ihrer Organisat	secretsmanager-secret-unused	Wenn in AWS Secrets Manager unbenutzte Anmeldeinformationen vorhanden sind, sollten Sie die Anmeldeinformationen deaktivieren und/oder entfernen, da dies gegen das Prinzip der geringsten Rechte verstoßen kann. Mit dieser Regel können Sie einen Wert auf unusedForDays (Config Default: 90) setzen. Der tatsächliche Wert muss den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	ion oder externe Benutzer, mit denen Sie zusammena rbeiten und die über einen Webbrowse r, eine Client-An wendung oder interaktive Befehlsze ilentools mit Ihren AWS Ressource n interagieren. Maschinenidentität en: Ihre Dienstanw endungen, Betriebst ools und Workloads benötigen eine Identität, um Anfragen an AWS Dienste zu stellen — beispiels weise um Daten zu lesen. Zu diesen Identitäten gehören Maschinen, die in Ihrer AWS Umgebung ausgeführt werden, wie EC2 Amazon-In stances oder AWS Lambda-Funktionen. Sie können auch Maschinenidentitäten für externe Parteien verwalten, die Zugriff benötigen. Darüber hinaus benötigen Sie		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	möglicherweise auch Maschinen außerhalb AWS , die Zugriff auf Ihre AWS Umgebung benötigen.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SEC-2	Wie werden Identitäten für Personen und Computer verwaltet? Es gibt zwei Arten von Identitäten, die Sie verwalten müssen, wenn Sie sichere AWS Workloads betreiben möchten. Wenn Sie wissen, welche Art von Identität Sie verwalten und mit Zugriffsberechtigungen ausstatten müssen, können Sie sicherstellen, dass die richtigen Identitäten unter den richtigen Bedingungen Zugriff auf die richtigen Ressourcen haben. Menschliche Identitäten: Ihre Administratoren, Entwickler, Betreiber und Endbenutzer benötigen eine Identität, um auf Ihre AWS Umgebungen und Anwendungen zugreifen zu können. Dies sind Mitglieder Ihrer Organisat	secretsmanager-using-cmk	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass die Verschlüsselung mit dem AWS Key Management Service (AWS KMS) für AWS Secrets Manager aktiviert ist. Aktivieren Sie die Verschlüsselung von Daten im Ruhezustand, um eventuell vorhandene sensible Daten im Ruhezustand im Secrets Manager zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	ion oder externe Benutzer, mit denen Sie zusammena rbeiten und die über einen Webbrowse r, eine Client-An wendung oder interaktive Befehlsze ilentools mit Ihren AWS Ressource n interagieren. Maschinenidentität en: Ihre Dienstanw endungen, Betriebst ools und Workloads benötigen eine Identität, um Anfragen an AWS Dienste zu stellen — beispiels weise um Daten zu lesen. Zu diesen Identitäten gehören Maschinen, die in Ihrer AWS Umgebung ausgeführt werden, wie EC2 Amazon-In stances oder AWS Lambda-Funktionen. Sie können auch Maschinenidentitäten für externe Parteien verwalten, die Zugriff benötigen. Darüber hinaus benötigen Sie		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	möglicherweise auch Maschinen außerhalb AWS , die Zugriff auf Ihre AWS Umgebung benötigen.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SEC-2	Wie werden Identitäten für Personen und Computer verwaltet? Es gibt zwei Arten von Identitäten, die Sie verwalten müssen, wenn Sie sichere AWS Workloads betreiben möchten. Wenn Sie wissen, welche Art von Identität Sie verwalten und mit Zugriffsberechtigungen ausstatten müssen, können Sie sicherstellen, dass die richtigen Identitäten unter den richtigen Bedingungen Zugriff auf die richtigen Ressourcen haben. Menschliche Identitäten: Ihre Administratoren, Entwickler, Betreiber und Endbenutzer benötigen eine Identität, um auf Ihre AWS Umgebungen und Anwendungen zugreifen zu können. Dies sind Mitglieder Ihrer Organisat	access-keys-rotated	Die Anmeldeinformationen für autorisierte Geräte, Benutzer und Prozesse werden geprüft, indem sichergestellt wird, dass die IAM-Zugriffsschlüssel entsprechend den Vorgaben der Unternehmensrichtlinie rotiert werden. Das regelmäßige Ändern der Zugriffsschlüssel ist eine bewährte Sicherheitsmethode. Es verkürzt den Zeitraum, in dem ein Zugriffsschlüssel aktiv ist, und reduziert die Auswirkungen auf das Unternehmen, wenn die Schlüssel kompromittiert werden. Diese Regel erfordert einen Wert für die Zugriffsschlüssel-Rotation (Standardkonfiguration: 90). Der tatsächliche Wert muss den Richtlini

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	ion oder externe Benutzer, mit denen Sie zusammena rbeiten und die über einen Webbrowse r, eine Client-An wendung oder interaktive Befehlsze ilentools mit Ihren AWS Ressource n interagieren. Maschinenidentität en: Ihre Dienstanw endungen, Betriebst ools und Workloads benötigen eine Identität, um Anfragen an AWS Dienste zu stellen — beispiels weise um Daten zu lesen. Zu diesen Identitäten gehören Maschinen, die in Ihrer AWS Umgebung ausgeführt werden, wie EC2 Amazon-In stances oder AWS Lambda-Funktionen. Sie können auch Maschinenidentitäten für externe Parteien verwalten, die Zugriff benötigen. Darüber hinaus benötigen Sie		en Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	möglicherweise auch Maschinen außerhalb AWS , die Zugriff auf Ihre AWS Umgebung benötigen.		
SEC-3	Wie werden Berechtigungen für Personen und Computer verwaltet? Auf jede Komponente oder Ressource Ihrer Workload müssen Administratoren, Endbenutzer oder andere Komponenten zugreifen können. Definieren Sie klar, wer oder was Zugriff auf die einzelnen Komponenten haben soll, und wählen Sie den geeigneten Identitätstyp und die Methode für die Authentifizierung und Autorisierung aus.	ec2-imdsv2-check	Stellen Sie sicher, dass die Methode Instance Metadata Service Version 2 (IMDSv2) aktiviert ist, um den Zugriff auf und die Kontrolle der Amazon Elastic Compute Cloud (Amazon EC2) - Instance-Metadaten zu schützen. Die IMDSv2 Methode verwendet sitzungsbasierte Kontrollen. Mit können Kontrollen implementiert werden IMDSv2, um Änderungen an Instanzmetadaten einzuschränken.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SEC-3	Wie werden Berechtigungen für Personen und Computer verwaltet? Auf jede Komponente oder Ressource Ihrer Workload müssen Administratoren, Endbenutzer oder andere Komponenten zugreifen können. Definieren Sie klar, wer oder was Zugriff auf die einzelnen Komponenten haben soll, und wählen Sie den geeigneten Identitätstyp und die Methode für die Authentifizierung und Autorisierung aus.	ec-2 instance-profile-attached	EC2 Instanzprofile übergeben eine IAM-Rolle an eine EC2 Instance. Das Anhängen eines Instance-Profils an Ihre Instances kann bei der Implementierung von geringsten Berechtigungen und der Berechtigungsverwaltung helfen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SEC-3	Wie werden Berechtigungen für Personen und Computer verwaltet? Auf jede Komponente oder Ressource Ihrer Workload müssen Administratoren, Endbenutzer oder andere Komponenten zugreifen können. Definieren Sie klar, wer oder was Zugriff auf die einzelnen Komponenten haben soll, und wählen Sie den geeigneten Identitätstyp und die Methode für die Authentifizierung und Autorisierung aus.	ecs-task-definition-user-for-host-mode-check	Wenn für eine Aufgabendefinition erhöhte Berechtigungen gelten, liegt das daran, dass der Kunde diesen Konfigurationen ausdrücklich zugestimmt hat. Diese Kontrolle prüft, ob eine unerwartete Berechtigungseskalation vorliegt, wenn für eine Aufgabendefinition das Host-Netzwerk aktiviert ist, der Kunde aber keine erhöhten Berechtigungen aktiviert hat.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SEC-3	Wie werden Berechtigungen für Personen und Computer verwaltet? Auf jede Komponente oder Ressource Ihrer Workload müssen Administratoren, Endbenutzer oder andere Komponenten zugreifen können. Definieren Sie klar, wer oder was Zugriff auf die einzelnen Komponenten haben soll, und wählen Sie den geeigneten Identitätstyp und die Methode für die Authentifizierung und Autorisierung aus.	ecs-task-definition-nonroot-Benutzer	Um Sie bei der Implementierung des Prinzips der geringsten Berechtigung zu unterstützen, stellen Sie sicher, dass ein Nicht-Root-Benutzer für den Zugriff auf Ihre Amazon Elastic Container Service (Amazon ECS)-Aufgabendefinitionen vorgesehen ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SEC-3	Wie werden Berechtigungen für Personen und Computer verwaltet? Auf jede Komponente oder Ressource Ihrer Workload müssen Administratoren, Endbenutzer oder andere Komponenten zugreifen können. Definieren Sie klar, wer oder was Zugriff auf die einzelnen Komponenten haben soll, und wählen Sie den geeigneten Identitätstyp und die Methode für die Authentifizierung und Autorisierung aus.	ecs-containers-nonprivileged	Um die Implementierung des Prinzips der geringsten Berechtigung zu unterstützen, dürfen in Amazon Elastic Container Service (Amazon ECS)-Aufgabendefinitionen keine erhöhten Berechtigungen aktiviert sein. Wenn dieser Parameter den Wert „true“ aufweist, erhält der Container erhöhte Berechtigungen auf der Host-Container-Instance (ähnlich wie der Root-Benutzer).

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SEC-3	Wie werden Berechtigungen für Personen und Computer verwaltet? Auf jede Komponente oder Ressource Ihrer Workload müssen Administratoren, Endbenutzer oder andere Komponenten zugreifen können. Definieren Sie klar, wer oder was Zugriff auf die einzelnen Komponenten haben soll, und wählen Sie den geeigneten Identitätstyp und die Methode für die Authentifizierung und Autorisierung aus.	ecs-containers-readonly-access	Die Aktivierung des schreibgeschützten Zugriffs auf Amazon Elastic Container Service (ECS)-Container kann dazu beitragen, das Prinzip der geringsten Berechtigung einzuhalten. Diese Option kann Angriffsvektoren reduzieren, da das Dateisystem der Container-Instance nur geändert werden kann, wenn es über ausdrückliche Lese- und Schreibberechtigungen verfügt.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SEC-3	Wie werden Berechtigungen für Personen und Computer verwaltet? Auf jede Komponente oder Ressource Ihrer Workload müssen Administratoren, Endbenutzer oder andere Komponenten zugreifen können. Definieren Sie klar, wer oder was Zugriff auf die einzelnen Komponenten haben soll, und wählen Sie den geeigneten Identitätstyp und die Methode für die Authentifizierung und Autorisierung aus.	efs-access-point-enforce-Benutzeridentität	Um die Implementierung des Prinzips der geringsten Rechte zu unterstützen, stellen Sie sicher, dass die Benutzerdurchsetzung für Ihr Amazon Elastic File System (Amazon EFS) aktiviert ist. Wenn diese Option aktiviert ist, ersetzt Amazon EFS den Benutzer und die Gruppe IDs des NFS-Clients durch die Identität, die auf dem Access Point für alle Dateisystemoperationen konfiguriert ist, und gewährt nur Zugriff auf diese erzwungene Benutzeridentität.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SEC-3	Wie werden Berechtigungen für Personen und Computer verwaltet? Auf jede Komponente oder Ressource Ihrer Workload müssen Administratoren, Endbenutzer oder andere Komponenten zugreifen können. Definieren Sie klar, wer oder was Zugriff auf die einzelnen Komponenten haben soll, und wählen Sie den geeigneten Identitätstyp und die Methode für die Authentifizierung und Autorisierung aus.	emr-kerberos-enabled	Die Zugriffsberechtigungen und -autorisierungen können verwaltet und nach den Prinzipien der geringsten Berechtigung und Aufgabentrennung integriert werden, indem Kerberos für Amazon-EMR-Cluster aktiviert wird. In Kerberos werden Services und Benutzer, die sich authentifizieren müssen, als Prinzipale bezeichnet. Prinzipale befinden sich in einem Kerberos-Bereich. Innerhalb dieses Bereichs wird ein Kerberos-Server als Key Distribution Center (KDC) bezeichnet. Über diesen Server können sich Prinzipale authentifizieren. Die Authentifizierung im KDC erfolgt durch die Ausstellung von Authentif

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			izierungstickets. Das KDC unterhält eine Datenbank der Prinzipale in seinem Bereich mit ihren Passwörtern und anderen administrativen Informationen zu jedem Prinzipal.
SEC-3	Wie werden Berechtigungen für Personen und Computer verwaltet? Auf jede Komponente oder Ressource Ihrer Workload müssen Administratoren, Endbenutzer oder andere Komponenten zugreifen können. Definieren Sie klar, wer oder was Zugriff auf die einzelnen Komponenten haben soll, und wählen Sie den geeigneten Identitätstyp und die Methode für die Authentifizierung und Autorisierung aus.	iam-group-has-users-überprüfen	AWS Identity and Access Management (IAM) kann Ihnen helfen, die Prinzipien der geringsten Rechte und der Aufgabentrennung mit Zugriffsberechtigungen und Autorisierungen zu integrieren, indem sichergestellt wird, dass IAM-Gruppen mindestens einen Benutzer haben. Die Einteilung von Benutzern in Gruppen auf der Grundlage der ihnen zugewiesenen Berechtigungen oder ihrer Funktion ist eine Möglichkeit, das Prinzip der geringsten Berechtigung zu implementieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SEC-3	Wie werden Berechtigungen für Personen und Computer verwaltet? Auf jede Komponente oder Ressource Ihrer Workload müssen Administratoren, Endbenutzer oder andere Komponenten zugreifen können. Definieren Sie klar, wer oder was Zugriff auf die einzelnen Komponenten haben soll, und wählen Sie den geeigneten Identitätstyp und die Methode für die Authentifizierung und Autorisierung aus.	iam-no-inline-policy-überprüfen	Stellen Sie sicher, dass ein Benutzer, eine IAM-Rolle oder eine IAM-Gruppe (AWS Identity and Access Management) nicht über eine Inline-Richtlinie zur Zugriffskontrolle auf Systeme und Ressourcen verfügt. AWS empfiehlt, verwaltete Richtlinien anstelle von Inline-Richtlinien zu verwenden. Verwaltete Richtlinien ermöglichen Wiederverwendbarkeit, Versionsverwaltung, Rollback und Delegierung der Berechtigungsverwaltung.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SEC-3	Wie werden Berechtigungen für Personen und Computer verwaltet? Auf jede Komponente oder Ressource Ihrer Workload müssen Administratoren, Endbenutzer oder andere Komponenten zugreifen können. Definieren Sie klar, wer oder was Zugriff auf die einzelnen Komponenten haben soll, und wählen Sie den geeigneten Identitätstyp und die Methode für die Authentifizierung und Autorisierung aus.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) kann Ihnen dabei helfen, die Prinzipien der geringsten Rechte und der Aufgabentrennung in Zugriffsberechtigungen und Autorisierungen zu integrieren und so zu verhindern, dass Richtlinien „Effect“: „Allow“ mit „Action“: „*“ anstelle von „Resource“: „*“ enthalten. Wenn Benutzern mehr Rechte eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und der Aufgabentrennung verstoßen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SEC-3	Wie werden Berechtigungen für Personen und Computer verwaltet? Auf jede Komponente oder Ressource Ihrer Workload müssen Administratoren, Endbenutzer oder andere Komponenten zugreifen können. Definieren Sie klar, wer oder was Zugriff auf die einzelnen Komponenten haben soll, und wählen Sie den geeigneten Identitätstyp und die Methode für die Authentifizierung und Autorisierung aus.	iam-policy-no-statements-with-full-access	Stellen Sie sicher, dass IAM-Aktionen nur auf die benötigten Aktionen beschränkt sind. Wenn Benutzern mehr Berechtigungen eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und Aufgabentrennung verstoßen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SEC-3	Wie werden Berechtigungen für Personen und Computer verwaltet? Auf jede Komponente oder Ressource Ihrer Workload müssen Administratoren, Endbenutzer oder andere Komponenten zugreifen können. Definieren Sie klar, wer oder was Zugriff auf die einzelnen Komponenten haben soll, und wählen Sie den geeigneten Identitätstyp und die Methode für die Authentifizierung und Autorisierung aus.	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) kann Ihnen dabei helfen, die Prinzipien der geringsten Rechte und der Aufgabentrennung in Zugriffsberechtigungen und Autorisierungen zu integrieren und so zu verhindern, dass Richtlinien blockierte Aktionen für alle AWS Schlüssel des Key Management Service enthalten. Wenn Benutzer mehr Rechte haben, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und Aufgabentrennung verstoßen. Mit dieser Regel können Sie den Parameter festlegen. blockedActionsPatterns (Wert „AWS Bewährte grundlegende

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			Sicherheitsmethoden“: kms: Entschlüsseln, kms:ReEncryptFrom). Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.
SEC-3	Wie werden Berechtigungen für Personen und Computer verwaltet? Auf jede Komponente oder Ressource Ihrer Workload müssen Administratoren, Endbenutzer oder andere Komponenten zugreifen können. Definieren Sie klar, wer oder was Zugriff auf die einzelnen Komponenten haben soll, und wählen Sie den geeigneten Identitätstyp und die Methode für die Authentifizierung und Autorisierung aus.	iam-group-has-users-überprüfen	AWS Identity and Access Management (IAM) kann Ihnen helfen, die Prinzipien der geringsten Rechte und der Aufgabentrennung mit Zugriffsberechtigungen und Autorisierungen zu integrieren, indem sichergestellt wird, dass IAM-Gruppen mindestens einen Benutzer haben. Die Einteilung von Benutzern in Gruppen auf der Grundlage der ihnen zugewiesenen Berechtigungen oder ihrer Funktion ist eine Möglichkeit, das Prinzip der geringsten Berechtigung zu implementieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SEC-3	Wie werden Berechtigungen für Personen und Computer verwaltet? Auf jede Komponente oder Ressource Ihrer Workload müssen Administratoren, Endbenutzer oder andere Komponenten zugreifen können. Definieren Sie klar, wer oder was Zugriff auf die einzelnen Komponenten haben soll, und wählen Sie den geeigneten Identitätstyp und die Methode für die Authentifizierung und Autorisierung aus.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) kann Ihnen dabei helfen, die Prinzipien der geringsten Rechte und der Aufgabentrennung in Zugriffsberechtigungen und Autorisierungen zu integrieren und so zu verhindern, dass Richtlinien „Effect“: „Allow“ mit „Action“: „*“ anstelle von „Resource“: „*“ enthalten. Wenn Benutzern mehr Rechte eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und der Aufgabentrennung verstoßen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SEC-3	Wie werden Berechtigungen für Personen und Computer verwaltet? Auf jede Komponente oder Ressource Ihrer Workload müssen Administratoren, Endbenutzer oder andere Komponenten zugreifen können. Definieren Sie klar, wer oder was Zugriff auf die einzelnen Komponenten haben soll, und wählen Sie den geeigneten Identitätstyp und die Methode für die Authentifizierung und Autorisierung aus.	iam-root-access-key-überprüfen	Der Zugriff auf Systeme und Ressourcen kann gesteuert werden, indem überprüft wird, ob der Root-Benutzer keine Zugriffsschlüssel mit seiner AWS Identity and Access Management (IAM) -Rolle verknüpft hat. Stellen Sie sicher, dass die Root-Zugriffsschlüssel gelöscht werden. Erstellen und verwenden Sie stattdessen rollenbasierte Funktionen, AWS-Konten um das Prinzip der geringsten Funktionalität zu berücksichtigen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SEC-3	Wie werden Berechtigungen für Personen und Computer verwaltet? Auf jede Komponente oder Ressource Ihrer Workload müssen Administratoren, Endbenutzer oder andere Komponenten zugreifen können. Definieren Sie klar, wer oder was Zugriff auf die einzelnen Komponenten haben soll, und wählen Sie den geeigneten Identitätstyp und die Methode für die Authentifizierung und Autorisierung aus.	iam-user-group-membership-überprüfen	AWS Identity and Access Management (IAM) kann Ihnen helfen, Zugriffsberechtigungen und Autorisierungen einzuschränken, indem sichergestellt wird, dass Benutzer Mitglieder mindestens einer Gruppe sind. Wenn Benutzern mehr Berechtigungen eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und Aufgabentrennung verstoßen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SEC-3	Wie werden Berechtigungen für Personen und Computer verwaltet? Auf jede Komponente oder Ressource Ihrer Workload müssen Administratoren, Endbenutzer oder andere Komponenten zugreifen können. Definieren Sie klar, wer oder was Zugriff auf die einzelnen Komponenten haben soll, und wählen Sie den geeigneten Identitätstyp und die Methode für die Authentifizierung und Autorisierung aus.	iam-user-unused-credentials-überprüfen	AWS Identity and Access Management (IAM) kann Ihnen bei Zugriffsberechtigungen und Autorisierungen helfen, indem es nach IAM-Passwörtern und Zugriffsschlüsseln sucht, die für einen bestimmten Zeitraum nicht verwendet wurden. Wenn ungenutzte Anmeldeinformationen identifiziert werden, müssen Sie sie deaktivieren und/oder entfernen, da dies gegen das Prinzip der geringsten Berechtigung verstoßen könnte. Für diese Regel müssen Sie einen Wert für das maxCredentialUsage Alter festlegen (Standardkonfiguration: 90). Der tatsächliche Wert muss den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SEC-3	Wie werden Berechtigungen für Personen und Computer verwaltet? Richten Sie gemeinsame Kontrollen ein, die den Zugriff auf alle Identitäten in Ihrer Organisation einschränken. Sie können beispielsweise den Zugriff auf bestimmte AWS Regionen einschränken oder verhindern, dass Ihre Operatoren gemeinsame Ressourcen löschen, z. B. eine IAM-Rolle, die für Ihr zentrales Sicherheitsteam verwendet wird	account-part-of-organizations	Durch die zentrale Verwaltung AWS-Konten innerhalb von AWS Organizations wird sichergestellt, dass die Konten den Vorschriften entsprechen. Eine fehlende zentrale Kontoverwaltung kann zu inkonsistenten Kontokonfigurationen führen, wodurch Ressourcen und sensible Daten offengelegt werden können.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SEC-3	Wie werden Berechtigungen für Personen und Computer verwaltet? Überwachen Sie kontinuierlich die Ergebnisse, die den öffentlichen und kontoübergreifenden Zugriff zeigen. Beschränken Sie den öffentlichen und den kontoübergreifenden Zugriff nur auf Ressourcen, für die diese Art von Zugriff erforderlich ist.	dms-replication-not-public	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass auf DMS-Replikationsinstanzen nicht öffentlich zugegriffen werden kann. DMS-Replikations-Instances können vertrauliche Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.
SEC-3	Wie werden Berechtigungen für Personen und Computer verwaltet? Überwachen Sie kontinuierlich die Ergebnisse, die den öffentlichen und kontoübergreifenden Zugriff zeigen. Beschränken Sie den öffentlichen und den kontoübergreifenden Zugriff nur auf Ressourcen, für die diese Art von Zugriff erforderlich ist.	ebs-snapshot-public-restorable-überprüfen	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass EBS-Snapshots nicht öffentlich wiederherstellbar sind. EBS-Volume-Snapshots können vertrauliche Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SEC-3	Wie werden Berechtigungen für Personen und Computer verwaltet? Überwachen Sie kontinuierlich die Ergebnisse, die den öffentlichen und kontoübergreifenden Zugriff zeigen. Beschränken Sie den öffentlichen und den kontoübergreifenden Zugriff nur auf Ressourcen, für die diese Art von Zugriff erforderlich ist.	ec-2 instance-no-public-ip	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon Elastic Compute Cloud (Amazon EC2) - Instances nicht öffentlich zugänglich sind. EC2 Amazon-Instances können vertrauliche Informationen enthalten, und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SEC-3	Wie werden Berechtigungen für Personen und Computer verwaltet? Überwachen Sie kontinuierlich die Ergebnisse, die den öffentlichen und kontoübergreifenden Zugriff zeigen. Beschränken Sie den öffentlichen und den kontoübergreifenden Zugriff nur auf Ressourcen, für die diese Art von Zugriff erforderlich ist.	elasticsearch-in-vpc-only	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass sich Amazon OpenSearch OpenSearch Service (Service) - Domains innerhalb einer Amazon Virtual Private Cloud (Amazon VPC) befinden. Eine OpenSearch Service-Domain innerhalb einer Amazon VPC ermöglicht die sichere Kommunikation zwischen OpenSearch Service und anderen Services innerhalb der Amazon VPC, ohne dass ein Internet-Gateway, ein NAT-Gerät oder eine VPN-Verbindung erforderlich ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SEC-3	Wie werden Berechtigungen für Personen und Computer verwaltet? Überwachen Sie kontinuierlich die Ergebnisse, die den öffentlichen und kontoübergreifenden Zugriff zeigen. Beschränken Sie den öffentlichen und den kontoübergreifenden Zugriff nur auf Ressourcen, für die diese Art von Zugriff erforderlich ist.	opensearch-in-vpc-only	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass sich Amazon OpenSearch Service-Domains innerhalb einer Amazon Virtual Private Cloud (Amazon VPC) befinden. Eine Amazon OpenSearch Service-Domain innerhalb einer Amazon VPC ermöglicht die sichere Kommunikation zwischen Amazon OpenSearch Service und anderen Services innerhalb der Amazon VPC, ohne dass ein Internet-Gateway, ein NAT-Gerät oder eine VPN-Verbindung erforderlich ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SEC-3	Wie werden Berechtigungen für Personen und Computer verwaltet? Überwachen Sie kontinuierlich die Ergebnisse, die den öffentlichen und kontoübergreifenden Zugriff zeigen. Beschränken Sie den öffentlichen und den kontoübergreifenden Zugriff nur auf Ressourcen, für die diese Art von Zugriff erforderlich ist.	emr-master-no-public-ip	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon EMR-Cluster-Masterknoten nicht öffentlich zugänglich sind. Amazon-EMR-Cluster-Hauptknoten können vertrauliche Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SEC-3	Wie werden Berechtigungen für Personen und Computer verwaltet? Überwachen Sie kontinuierlich die Ergebnisse, die den öffentlichen und kontoübergreifenden Zugriff zeigen. Beschränken Sie den öffentlichen und den kontoübergreifenden Zugriff nur auf Ressourcen, für die diese Art von Zugriff erforderlich ist.	ec-2 instances-in-vpc	Stellen Sie Amazon Elastic Compute Cloud (Amazon EC2) -Instances innerhalb einer Amazon Virtual Private Cloud (Amazon VPC) bereit, um eine sichere Kommunikation zwischen einer Instance und anderen Services innerhalb der Amazon VPC zu ermöglichen, ohne dass ein Internet-Gateway, ein NAT-Gerät oder eine VPN-Verbindung erforderlich ist. Der gesamte Datenverkehr bleibt sicher in der AWS Cloud. Domains, die sich innerhalb einer VPC befinden, verfügen aufgrund ihrer logischen Isolierung im Vergleich zu Domains mit öffentlichen Endpunkten über eine zusätzliche Sicherheitsebene. Weisen Sie EC2

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			Amazon-Instances einer Amazon-VPC zu, um den Zugriff ordnungsgemäß zu verwalten.
SEC-3	Wie werden Berechtigungen für Personen und Computer verwaltet? Überwachen Sie kontinuierlich die Ergebnisse, die den öffentlichen und kontoübergreifenden Zugriff zeigen. Beschränken Sie den öffentlichen und den kontoübergreifenden Zugriff nur auf Ressourcen, für die diese Art von Zugriff erforderlich ist.	lambda-function-public-access-verboten	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass AWS Lambda-Funktionen nicht öffentlich zugänglich sind. Der öffentliche Zugriff kann möglicherweise die Verfügbarkeit von Ressourcen beeinträchtigen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SEC-3	Wie werden Berechtigungen für Personen und Computer verwaltet? Überwachen Sie kontinuierlich die Ergebnisse, die den öffentlichen und kontoübergreifenden Zugriff zeigen. Beschränken Sie den öffentlichen und den kontoübergreifenden Zugriff nur auf Ressourcen, für die diese Art von Zugriff erforderlich ist.	lambda-inside-vpc	Stellen Sie AWS Lambda-Funktionen in einer Amazon Virtual Private Cloud (Amazon VPC) bereit, um eine sichere Kommunikation zwischen einer Funktion und anderen Diensten innerhalb der Amazon VPC zu gewährleisten. Bei dieser Konfiguration sind kein Internet-Gateway, kein NAT-Gerät und keine VPN-Verbindung erforderlich. Der gesamte Datenverkehr bleibt sicher in der Cloud. AWS Domains, die sich innerhalb einer VPC befinden, verfügen aufgrund ihrer logischen Isolierung im Vergleich zu Domains mit öffentlichen Endpunkten über eine zusätzliche Sicherheitsebene. Um den Zugriff ordnungsgemäß zu verwalten,

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			sollten AWS Lambda-Funktionen einer VPC zugewiesen werden.
SEC-3	Wie werden Berechtigungen für Personen und Computer verwaltet? Überwachen Sie kontinuierlich die Ergebnisse, die den öffentlichen und kontoübergreifenden Zugriff zeigen. Beschränken Sie den öffentlichen und den kontoübergreifenden Zugriff nur auf Ressourcen, für die diese Art von Zugriff erforderlich ist.	rds-instance-public-access-überprüfen	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Relational Database Service (Amazon RDS) -Instances nicht öffentlich sind. Amazon-RDS-Datenbank-Instances können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SEC-3	Wie werden Berechtigungen für Personen und Computer verwaltet? Überwachen Sie kontinuierlich die Ergebnisse, die den öffentlichen und kontoübergreifenden Zugriff zeigen. Beschränken Sie den öffentlichen und den kontoübergreifenden Zugriff nur auf Ressourcen, für die diese Art von Zugriff erforderlich ist.	rds-snapshots-public-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Relational Database Service (Amazon RDS) -Instances nicht öffentlich sind. Amazon-RDS-Datenbank-Instances können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SEC-3	Wie werden Berechtigungen für Personen und Computer verwaltet? Überwachen Sie kontinuierlich die Ergebnisse, die den öffentlichen und kontoübergreifenden Zugriff zeigen. Beschränken Sie den öffentlichen und den kontoübergreifenden Zugriff nur auf Ressourcen, für die diese Art von Zugriff erforderlich ist.	redshift-cluster-public-access-überprüfen	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Redshift Redshift-Cluster nicht öffentlich sind. Amazon-Redshift-Cluster können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SEC-3	Wie werden Berechtigungen für Personen und Computer verwaltet? Überwachen Sie kontinuierlich die Ergebnisse, die den öffentlichen und kontoübergreifenden Zugriff zeigen. Beschränken Sie den öffentlichen und den kontoübergreifenden Zugriff nur auf Ressourcen, für die diese Art von Zugriff erforderlich ist.	s3- -Block-periodisch account-level-public-access	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Simple Storage Service (Amazon S3) -Buckets nicht öffentlich zugänglich sind. Diese Regel trägt dazu bei, sensible Daten vor unbefugten Remote-Benutzern zu schützen, indem sie den öffentlichen Zugriff verhindert. Mit dieser Regel können Sie optional die Parameter ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) und restrictPublicBuckets Parameter (Config Default: True) festlegen. Die tatsächlichen Werte müssen den Richtlini

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			en Ihrer Organisation entsprechen.
SEC-3	Wie werden Berechtigungen für Personen und Computer verwaltet? Überwachen Sie kontinuierlich die Ergebnisse, die den öffentlichen und kontoübergreifenden Zugriff zeigen. Beschränken Sie den öffentlichen und den kontoübergreifenden Zugriff nur auf Ressourcen, für die diese Art von Zugriff erforderlich ist.	s3 bucket-level-public-access - verboten	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Simple Storage Service (Amazon S3) -Buckets nicht öffentlich zugänglich sind. Diese Regel trägt dazu bei, sensible Daten vor unbefugten Remote-Benutzern zu schützen, indem sie den öffentlichen Zugriff auf Bucket-Ebene verhindert.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SEC-3	Wie werden Berechtigungen für Personen und Computer verwaltet? Überwachen Sie kontinuierlich die Ergebnisse, die den öffentlichen und kontoübergreifenden Zugriff zeigen. Beschränken Sie den öffentlichen und den kontoübergreifenden Zugriff nur auf Ressourcen, für die diese Art von Zugriff erforderlich ist.	s-3 bucket-public-read-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie nur autorisierten Benutzern, Prozessen und Geräten Zugriff auf Amazon Simple Storage Service (Amazon S3) - Buckets gewähren. Die Verwaltung des Zugriffs sollte mit der Klassifizierung der Daten übereinstimmen.
SEC-3	Wie werden Berechtigungen für Personen und Computer verwaltet? Überwachen Sie kontinuierlich die Ergebnisse, die den öffentlichen und kontoübergreifenden Zugriff zeigen. Beschränken Sie den öffentlichen und den kontoübergreifenden Zugriff nur auf Ressourcen, für die diese Art von Zugriff erforderlich ist.	s3- bucket-public-write-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie nur autorisierten Benutzern, Prozessen und Geräten Zugriff auf Amazon Simple Storage Service (Amazon S3) - Buckets gewähren. Die Verwaltung des Zugriffs sollte mit der Klassifizierung der Daten übereinstimmen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SEC-3	Wie werden Berechtigungen für Personen und Computer verwaltet? Überwachen Sie kontinuierlich die Ergebnisse, die den öffentlichen und kontoübergreifenden Zugriff zeigen. Beschränken Sie den öffentlichen und den kontoübergreifenden Zugriff nur auf Ressourcen, für die diese Art von Zugriff erforderlich ist.	sagemaker-notebook-no-direct-Internetzugang	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass SageMaker Amazon-Notebooks keinen direkten Internetzugang zulassen. Indem Sie direkten Internetzugang blockieren, vermeiden Sie, dass unbefugte Benutzer auf sensible Daten zugreifen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SEC-3	Wie werden Berechtigungen für Personen und Computer verwaltet? Überwachen Sie kontinuierlich die Ergebnisse, die den öffentlichen und kontoübergreifenden Zugriff zeigen. Beschränken Sie den öffentlichen und den kontoübergreifenden Zugriff nur auf Ressourcen, für die diese Art von Zugriff erforderlich ist.	secretsmanager-secret-unused	Wenn in AWS Secrets Manager unbenutzte Anmeldeinformationen vorhanden sind, sollten Sie die Anmeldeinformationen deaktivieren und/oder entfernen, da dies gegen das Prinzip der geringsten Rechte verstoßen kann. Mit dieser Regel können Sie einen Wert auf unusedForDays (Config Default: 90) setzen. Der tatsächliche Wert muss den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SEC-3	Wie werden Berechtigungen für Personen und Computer verwaltet? Überwachen Sie kontinuierlich die Ergebnisse, die den öffentlichen und kontoübergreifenden Zugriff zeigen. Beschränken Sie den öffentlichen und den kontoübergreifenden Zugriff nur auf Ressourcen, für die diese Art von Zugriff erforderlich ist.	ssm-document-not-public	Stellen Sie sicher, dass AWS Systems Manager (SSM) - Dokumente nicht öffentlich sind, da dies einen unbeabsichtigten Zugriff auf Ihre SSM-Dokumente ermöglichen kann. Ein öffentliches SSM-Dokument kann Informationen über Ihr Konto, Ihre Ressourcen und internen Prozesse preisgeben.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SEC-3	Wie werden Berechtigungen für Personen und Computer verwaltet? Überwachen Sie kontinuierlich die Ergebnisse, die den öffentlichen und kontoübergreifenden Zugriff zeigen. Beschränken Sie den öffentlichen und den kontoübergreifenden Zugriff nur auf Ressourcen, für die diese Art von Zugriff erforderlich ist.	subnet-auto-assign-public-ip-deaktiviert	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon Virtual Private Cloud (VPC) -Subnetzen nicht automatisch eine öffentliche IP-Adresse zugewiesen wird. Amazon Elastic Compute Cloud (EC2) -Instances, die in Subnetzen gestartet werden, in denen dieses Attribut aktiviert ist, haben ihrer primären Netzwerkschnittstelle eine öffentliche IP-Adresse zugewiesen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SEC-3	Wie werden Berechtigungen für Personen und Computer verwaltet? Überwachen Sie kontinuierlich die Ergebnisse, die den öffentlichen und kontoübergreifenden Zugriff zeigen. Beschränken Sie den öffentlichen und den kontoübergreifenden Zugriff nur auf Ressourcen, für die diese Art von Zugriff erforderlich ist.	autoscaling-launch-config-public-ip-deaktiviert	Wenn Sie Ihre Netzwerkschnittstellen mit einer öffentlichen IP-Adresse konfigurieren, sind die diesen Netzwerkschnittstellen zugehörigen Ressourcen über das Internet erreichbar. EC2 Ressourcen sollten nicht öffentlich zugänglich sein, da dies einen unbeabsichtigten Zugriff auf Ihre Anwendungen oder Server ermöglichen kann.
SEC-4	Wie werden Sicherheitsereignisse erkannt und untersucht? Erfassen und analysieren Sie Ereignisse anhand von Protokollen und Metriken, um mehr Transparenz zu erhalten. Reagieren Sie auf Sicherheitsereignisse und potenzielle Bedrohungen, um Ihre Workload zu schützen.	api-gw-execution-logging-aktiviert	Die API-Gateway-Protokollierung zeigt detaillierte Ansichten der Benutzer, die auf die API zugegriffen haben, und wie diese Benutzer auf die API zugegriffen haben. Diese Einblicke ermöglichen die Transparenz von Benutzeraktivitäten.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SEC-4	Wie werden Sicherheitsereignisse erkannt und untersucht? Erfassen und analysieren Sie Ereignisse anhand von Protokollen und Metriken, um mehr Transparenz zu erhalten. Reagieren Sie auf Sicherheitsereignisse und potenzielle Bedrohungen, um Ihre Workload zu schützen.	opensearch-audit-logging-enabled	Stellen Sie sicher, dass die Audit-Protokollierung für Ihre Amazon OpenSearch Service-Domains aktiviert ist. Mit der Audit-Protokollierung können Sie Benutzeraktivitäten auf Ihren OpenSearch Domains verfolgen, einschließlich erfolgreicher und fehlgeschlagener Authentifizierungen OpenSearch, Anfragen an, Indexänderungen und eingehende Suchanfragen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SEC-4	Wie werden Sicherheitsereignisse erkannt und untersucht? Erfassen und analysieren Sie Ereignisse anhand von Protokollen und Metriken, um mehr Transparenz zu erhalten. Reagieren Sie auf Sicherheitsereignisse und potenzielle Bedrohungen, um Ihre Workload zu schützen.	cloud-trail-cloud-watch-Logs aktiviert	Verwenden Sie Amazon CloudWatch , um Protokollereignisaktivitäten zentral zu sammeln und zu verwalten. Die Aufnahme von AWS CloudTrail Daten liefert Einzelheiten zu den API-Aufrufaktivitäten in Ihrem AWS-Konto.
SEC-4	Wie werden Sicherheitsereignisse erkannt und untersucht? Erfassen und analysieren Sie Ereignisse anhand von Protokollen und Metriken, um mehr Transparenz zu erhalten. Reagieren Sie auf Sicherheitsereignisse und potenzielle Bedrohungen, um Ihre Workload zu schützen.	cloudtrail-s3-dataevents-enabled	Die Erfassung von Simple Storage Service (Amazon S3)-Datenereignissen unterstützt die Erkennung von ungewöhnlichen Aktivitäten. Zu den Details gehören AWS-Konto Informationen, die auf ein Objekt in einem Amazon S3 S3-Bucket zugegriffen haben, die IP-Adresse und die Uhrzeit des Ereignisses.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SEC-4	Wie werden Sicherheitsereignisse erkannt und untersucht? Erfassen und analysieren Sie Ereignisse anhand von Protokollen und Metriken, um mehr Transparenz zu erhalten. Reagieren Sie auf Sicherheitsereignisse und potenzielle Bedrohungen, um Ihre Workload zu schützen.	cw-loggroup-retention-period-überprüfen	Stellen Sie sicher, dass die Ereignisprotokolldaten für Ihre Protokollgruppen über eine Mindestdauer aufbewahrt werden, um die Fehlerbehebung und forensische Untersuchungen zu unterstützen. Fehlende frühere Ereignisprotokolldaten erschweren die Rekonstruierung und Identifizierung potenziell schädlicher Ereignisse.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SEC-4	Wie werden Sicherheitsereignisse erkannt und untersucht? Erfassen und analysieren Sie Ereignisse anhand von Protokollen und Metriken, um mehr Transparenz zu erhalten. Reagieren Sie auf Sicherheitsereignisse und potenzielle Bedrohungen, um Ihre Workload zu schützen.	elasticsearch-logs-to-cloudwatch	Stellen Sie sicher, dass für Amazon OpenSearch Service-Domains Fehlerprotokolle aktiviert und zur Aufbewahrung und Beantwortung an Amazon CloudWatch Logs gestreamt werden. Domain-Fehlerprotokolle sind bei Sicherheits- und Zugriffsprüfungen sowie bei der Diagnose von Verfügbarkeitsproblemen nützlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SEC-4	Wie werden Sicherheitsereignisse erkannt und untersucht? Erfassen und analysieren Sie Ereignisse anhand von Protokollen und Metriken, um mehr Transparenz zu erhalten. Reagieren Sie auf Sicherheitsereignisse und potenzielle Bedrohungen, um Ihre Workload zu schützen.	opensearch-logs-to-cloudwatch	Stellen Sie sicher, dass für Amazon OpenSearch Service-Domains Fehlerprotokolle aktiviert und zur Aufbewahrung und Beantwortung an Amazon CloudWatch Logs gestreamt werden. OpenSearch Service-Fehlerprotokolle können bei Sicherheits- und Zugriffsprüfungen helfen und bei der Diagnose von Verfügbarkeitsproblemen helfen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SEC-4	Wie werden Sicherheitsereignisse erkannt und untersucht? Erfassen und analysieren Sie Ereignisse anhand von Protokollen und Metriken, um mehr Transparenz zu erhalten. Reagieren Sie auf Sicherheitsereignisse und potenzielle Bedrohungen, um Ihre Workload zu schützen.	elb-logging-enabled	Die Elastic-Load-Balancing-Aktivität ist ein zentraler Kommunikationspunkt innerhalb einer Umgebung. Stellen Sie sicher, dass die ELB-Protokollierung aktiviert ist. Die gesammelten Daten enthalten detaillierte Informationen zu Anfragen, die an den ELB gesendet wurden. Jedes Protokoll enthält Informationen wie die Zeit, zu der die Anforderung einging, die Client-IP-Adresse, Latenzen, Anforderungspfade und Serverantworten.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SEC-4	Wie werden Sicherheitsereignisse erkannt und untersucht? Erfassen und analysieren Sie Ereignisse anhand von Protokollen und Metriken, um mehr Transparenz zu erhalten. Reagieren Sie auf Sicherheitsereignisse und potenzielle Bedrohungen, um Ihre Workload zu schützen.	multi-region-cloudtrail-enabled	AWS CloudTrail zeichnet Aktionen und API-Aufrufe der AWS Management Console auf. Sie können feststellen, welche Benutzer und Konten angerufen wurden AWS, von welcher Quell-IP-Adresse aus die Anrufe getätigt wurden und wann die Anrufe erfolgten. CloudTrail übermittelt Protokolldateien aus allen AWS Regionen an Ihren S3-Bucket, wenn MULTI_REGION_CLOUD_TRAIL_ENABLED aktiviert ist. Außerdem wird beim AWS Start einer neuen Region derselbe Trail in der neuen Region erstellt. CloudTrail Dadurch erhalten Sie automatisch Protokolldateien mit API-Aktivitäten für die neue Region.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SEC-4	Wie werden Sicherheitsereignisse erkannt und untersucht? Erfassen und analysieren Sie Ereignisse anhand von Protokollen und Metriken, um mehr Transparenz zu erhalten. Reagieren Sie auf Sicherheitsereignisse und potenzielle Bedrohungen, um Ihre Workload zu schützen.	rds-logging-enabled	Um die Protokollierung und Überwachung in Ihrer Umgebung zu erleichtern, stellen Sie sicher, dass die Amazon Relational Database Service (Amazon RDS)-Protokollierung aktiviert ist. Mit der Amazon-RDS-Protokollierung können Sie Ereignisse wie Verbindungen, Verbindungsabbrüche, Abfragen oder abgefragte Tabellen erfassen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SEC-4	Wie werden Sicherheitsereignisse erkannt und untersucht? Erfassen und analysieren Sie Ereignisse anhand von Protokollen und Metriken, um mehr Transparenz zu erhalten. Reagieren Sie auf Sicherheitsereignisse und potenzielle Bedrohungen, um Ihre Workload zu schützen.	s-3 bucket-logging-enabled	Die Amazon Simple Storage Service (Amazon S3)-Serverzugriffsprotokollierung bietet eine Methode zur Überwachung des Netzwerks im Hinblick auf potenzielle Cybersicherheitsereignisse. Die Ereignisse werden überwacht, indem detaillierte Aufzeichnungen über die Anfragen erfasst werden, die an einen Amazon-S3-Bucket gestellt wurden. Jeder Zugriffsprotokolleintrag enthält Details zu einer einzelnen Zugriffsanfrage. Zu den Details gehören Auftraggeber, Bucket-Name, Anforderungszeit, Anforderungsaktion, Antwortstatus und Fehlercode, falls relevant.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SEC-4	Wie werden Sicherheitsereignisse erkannt und untersucht? Erfassen und analysieren Sie Ereignisse anhand von Protokollen und Metriken, um mehr Transparenz zu erhalten. Reagieren Sie auf Sicherheitsereignisse und potenzielle Bedrohungen, um Ihre Workload zu schützen.	vpc-flow-logs-enabled	VPC-Flow-Protokolle erfassen detaillierte Informationsdatensätze über den IP-Datenverkehr, der zu und von Netzwerkschnittstellen in Ihrer Amazon Virtual Private Cloud (Amazon VPC) fließt. Standardmäßig enthalten Flow-Protokolldatensätze Werte für die verschiedenen Komponenten des IP-Flows, einschließlich Quelle, Ziel und Protokoll.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SEC-4	Wie werden Sicherheitsereignisse erkannt und untersucht? Erfassen und analysieren Sie Ereignisse anhand von Protokollen und Metriken, um mehr Transparenz zu erhalten. Reagieren Sie auf Sicherheitsereignisse und potenzielle Bedrohungen, um Ihre Workload zu schützen.	wafv2-logging-enabled	Um die Protokollierung und Überwachung in Ihrer Umgebung zu erleichtern, aktivieren Sie die AWS WAF (V2) -Protokollierung im regionalen und globalen Web ACLs. AWS Die WAF-Protokollierung bietet detaillierte Informationen über den Datenverkehr, der von Ihrer Web-ACL analysiert wird. In den Protokollen werden die Uhrzeit aufgezeichnet, zu der die AWS WAF die Anfrage von Ihrer AWS Ressource erhalten hat, Informationen über die Anfrage und eine Aktion für die Regel, der jede Anfrage entsprach.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SEC-4	Wie werden Sicherheitsereignisse erkannt und untersucht? Erfassen und analysieren Sie Ereignisse anhand von Protokollen und Metriken, um mehr Transparenz zu erhalten. Reagieren Sie auf Sicherheitsereignisse und potenzielle Bedrohungen, um Ihre Workload zu schützen.	cloudtrail-security-trail-enabled	Diese Regel trägt dazu bei, die Verwendung der AWS empfohlenen bewährten Sicherheitsmethoden für sicherzustellen AWS CloudTrail, indem geprüft wird, ob mehrere Einstellungen aktiviert sind. Dazu gehören die Verwendung von Protokollverschlüsselung, Protokollvalidierung und Aktivierung AWS CloudTrail in mehreren Regionen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SEC-4	Wie werden Sicherheitsereignisse erkannt und untersucht? Erfassen und analysieren Sie Ereignisse anhand von Protokollen und Metriken, um mehr Transparenz zu erhalten. Reagieren Sie auf Sicherheitsereignisse und potenzielle Bedrohungen, um Ihre Workload zu schützen.	redshift-cluster-configuration-check	Um Daten im Ruhezustand zu schützen, muss die Verschlüsselung für Ihre Amazon-Redshift-Cluster aktiviert sein. Sie müssen auch sicherstellen, dass die erforderlichen Konfigurationen auf Amazon-Redshift-Clustern bereitgestellt werden. Die Prüfungsprotokollierung muss aktiviert sein, um Informationen zu Verbindungen und Benutzeraktivitäten in der Datenbank bereitzustellen. Diese Regel erfordert, dass ein Wert für clusterDbEncrypted (Config Default: TRUE) und LoggingEnabled (Config Default: TRUE) gesetzt ist. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SEC-4	Wie werden Sicherheitsereignisse erkannt und untersucht? Erfassen und analysieren Sie Ereignisse anhand von Protokollen und Metriken, um mehr Transparenz zu erhalten. Reagieren Sie auf Sicherheitsereignisse und potenzielle Bedrohungen, um Ihre Workload zu schützen.	guardduty-enabled-centralized	Amazon GuardDuty kann mithilfe von Threat Intelligence Feeds helfen, potenzielle Cybersicherheitsereignisse zu überwachen und zu erkennen. Dazu gehören Listen mit bösartigen IPs und maschinellen Lernmethoden zur Identifizierung unerwarteter, nicht autorisierter und bösartiger Aktivitäten in Ihrer AWS Cloud-Umgebung.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SEC-4	Wie werden Sicherheitsereignisse erkannt und untersucht? Erfassen und analysieren Sie Ereignisse anhand von Protokollen und Metriken, um mehr Transparenz zu erhalten. Reagieren Sie auf Sicherheitsereignisse und potenzielle Bedrohungen, um Ihre Workload zu schützen.	securityhub-enabled	AWS Security Hub hilft bei der Überwachung von unbefugtem Personal, Verbindungen, Geräten und Software. AWS Security Hub aggregiert, organisiert und priorisiert die Sicherheitswarnungen oder Ergebnisse mehrerer Dienste. AWS Einige dieser Dienste sind Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer und AWS Firewall Manager sowie AWS Partnerlösungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SEC-4	Wie werden Sicherheitsereignisse erkannt und untersucht? Erfassen und analysieren Sie Ereignisse anhand von Protokollen und Metriken, um mehr Transparenz zu erhalten. Reagieren Sie auf Sicherheitsereignisse und potenzielle Bedrohungen, um Ihre Workload zu schützen.	cloudwatch-alarm-action-check	Amazon CloudWatch alarmiert, wenn eine Metrik den Schwellenwert für eine bestimmte Anzahl von Bewertungszeiträumen überschreitet. Der Alarm führt eine oder mehrere Aktionen durch, die vom Wert der Metrik oder des Ausdrucks im Vergleich zu einem Schwellenwert in einer Reihe von Zeiträumen abhängt. Diese Regel erfordert einen Wert für alarmActionRequired (Config Default: True), insufficientDataAction Required (Config Default: True), okActionRequired (Config Default: False). Der tatsächliche Wert muss die Alarmaktionen für Ihre Umgebung widerspiegeln.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SEC-5	Wie werden Ihre Netzwerkressourcen geschützt? Jede Workload, die über irgendeine Form von Netzwerkkonnektivität verfügt, ob über das Internet oder ein privates Netzwerk, benötigt mehrere Schutzebenen, um vor externen und internen netzwerkbasierten Bedrohungen geschützt zu sein.	elasticsearch-in-vpc-only	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass sich Amazon OpenSearch OpenSearch Service (Service) - Domains innerhalb einer Amazon Virtual Private Cloud (Amazon VPC) befinden. Eine OpenSearch Service-Domain innerhalb einer Amazon VPC ermöglicht die sichere Kommunikation zwischen OpenSearch Service und anderen Services innerhalb der Amazon VPC, ohne dass ein Internet-Gateway, ein NAT-Gerät oder eine VPN-Verbindung erforderlich ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SEC-5	Wie werden Ihre Netzwerkressourcen geschützt? Jede Workload, die über irgendeine Form von Netzwerkkonnektivität verfügt, ob über das Internet oder ein privates Netzwerk, benötigt mehrere Schutzebenen, um vor externen und internen netzwerkbasierten Bedrohungen geschützt zu sein.	opensearch-in-vpc-only	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass sich Amazon OpenSearch Service-Domains innerhalb einer Amazon Virtual Private Cloud (Amazon VPC) befinden. Eine Amazon OpenSearch Service-Domain innerhalb einer Amazon VPC ermöglicht die sichere Kommunikation zwischen Amazon OpenSearch Service und anderen Services innerhalb der Amazon VPC, ohne dass ein Internet-Gateway, ein NAT-Gerät oder eine VPN-Verbindung erforderlich ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SEC-5	Wie werden Ihre Netzwerkressourcen geschützt? Jede Workload, die über irgendeine Form von Netzwerkkonnektivität verfügt, ob über das Internet oder ein privates Netzwerk, benötigt mehrere Schutzebenen, um vor externen und internen netzwerkbasierten Bedrohungen geschützt zu sein.	ec2- instances-in-vpc	Stellen Sie Amazon Elastic Compute Cloud (Amazon EC2) -Instances innerhalb einer Amazon Virtual Private Cloud (Amazon VPC) bereit, um eine sichere Kommunikation zwischen einer Instance und anderen Services innerhalb der Amazon VPC zu ermöglichen, ohne dass ein Internet-Gateway, ein NAT-Gerät oder eine VPN-Verbindung erforderlich ist. Der gesamte Datenverkehr bleibt sicher in der AWS Cloud. Domains, die sich innerhalb einer VPC befinden, verfügen aufgrund ihrer logischen Isolierung im Vergleich zu Domains mit öffentlichen Endpunkten über eine zusätzliche Sicherheitsebene. Weisen Sie EC2

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			Amazon-Instances einer Amazon-VPC zu, um den Zugriff ordnungsgemäß zu verwalten.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SEC-5	Wie werden Ihre Netzwerkressourcen geschützt? Jede Workload, die über irgendeine Form von Netzwerkkonnektivität verfügt, ob über das Internet oder ein privates Netzwerk, benötigt mehrere Schutzebenen, um vor externen und internen netzwerkbasierten Bedrohungen geschützt zu sein.	lambda-inside-vpc	Stellen Sie AWS Lambda-Funktionen in einer Amazon Virtual Private Cloud (Amazon VPC) bereit, um eine sichere Kommunikation zwischen einer Funktion und anderen Diensten innerhalb der Amazon VPC zu gewährleisten. Bei dieser Konfiguration sind kein Internet-Gateway, kein NAT-Gerät und keine VPN-Verbindung erforderlich. Der gesamte Datenverkehr bleibt sicher in der Cloud. AWS Domains, die sich innerhalb einer VPC befinden, verfügen aufgrund ihrer logischen Isolierung im Vergleich zu Domains mit öffentlichen Endpunkten über eine zusätzliche Sicherheitsebene. Um den Zugriff ordnungsgemäß zu verwalten,

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			sollten AWS Lambda-Funktionen einer VPC zugewiesen werden.
SEC-5	Wie werden Ihre Netzwerkressourcen geschützt? Jede Workload, die über irgendeine Form von Netzwerkkonnektivität verfügt, ob über das Internet oder ein privates Netzwerk, benötigt mehrere Schutzebenen, um vor externen und internen netzwerkbasierten Bedrohungen geschützt zu sein.	redshift-enhanced-vpc-routing-aktiviert	Mit Enhanced-VPC-Routing wird erzwungen, dass der gesamte COPY- und UNLOAD-Datenverkehr zwischen Ihrem Cluster und Datenrepositorys über Ihre Amazon VPC erfolgt. Anschließend können Sie VPC-Features wie Sicherheitsgruppen und Netzwerkzugriffskontrolllisten verwenden, um den Netzwerkverkehr zu schützen. Sie können auch VPC-Flussprotokolle verwenden, um den Netzwerkverkehr zu überwachen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SEC-5	Wie werden Ihre Netzwerkressourcen geschützt? Jede Workload, die über irgendeine Form von Netzwerkkonnektivität verfügt, ob über das Internet oder ein privates Netzwerk, benötigt mehrere Schutzebenen, um vor externen und internen netzwerkbasierten Bedrohungen geschützt zu sein.	alb-waf-enabled	Stellen Sie sicher, dass AWS WAF auf Elastic Load Balancers (ELB) aktiviert ist, um Webanwendungen zu schützen. Eine WAF trägt zum Schutz Ihrer Webanwendungen oder APIs vor gängigen Web-Exploits bei. Diese Web-Exploits können sich auf die Verfügbarkeit auswirken, die Sicherheit gefährden oder übermäßige Ressourcen in Ihrer Umgebung verbrauchen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SEC-5	Wie werden Ihre Netzwerkressourcen geschützt? Jede Workload, die über irgendeine Form von Netzwerkkonnektivität verfügt, ob über das Internet oder ein privates Netzwerk, benötigt mehrere Schutzebenen, um vor externen und internen netzwerkbasierten Bedrohungen geschützt zu sein.	api-gw-associated-with-WAF	AWS Mit WAF können Sie eine Reihe von Regeln (als Web Access Control List (Web ACL) bezeichnet) konfigurieren, die Webanfragen auf der Grundlage von anpassbaren Websicherheitsregeln und -bedingungen, die Sie definieren, zulassen, blockieren oder zählen. Stellen Sie sicher, dass Ihre Amazon-API-Gateway-Stufe mit einer WAF-Web-ACL verknüpft ist, um sie vor böswilligen Angriffen zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SEC-5	Wie werden Ihre Netzwerkressourcen geschützt? Jede Workload, die über irgendeine Form von Netzwerkkonnektivität verfügt, ob über das Internet oder ein privates Netzwerk, benötigt mehrere Schutzebenen, um vor externen und internen netzwerkbasierten Bedrohungen geschützt zu sein.	dms-replication-not-public	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass auf DMS-Replikationsinstanzen nicht öffentlich zugegriffen werden kann. DMS-Replikations-Instances können vertrauliche Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.
SEC-5	Wie werden Ihre Netzwerkressourcen geschützt? Jede Workload, die über irgendeine Form von Netzwerkkonnektivität verfügt, ob über das Internet oder ein privates Netzwerk, benötigt mehrere Schutzebenen, um vor externen und internen netzwerkbasierten Bedrohungen geschützt zu sein.	ebs-snapshot-public-restorable-überprüfen	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass EBS-Snapshots nicht öffentlich wiederherstellbar sind. EBS-Volume-Snapshots können vertrauliche Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SEC-5	Wie werden Ihre Netzwerkressourcen geschützt? Jede Workload, die über irgendeine Form von Netzwerkkonnektivität verfügt, ob über das Internet oder ein privates Netzwerk, benötigt mehrere Schutzebenen, um vor externen und internen netzwerkbasierten Bedrohungen geschützt zu sein.	ec-2 instance-multiple-eni-check	Diese Regel prüft, ob Ihre Amazon Elastic Compute Cloud (Amazon EC2) -Instances mehrere haben ENIs. Wenn mehrere vorhanden sind, ENIs kann dies zu doppelt vernetzten Instanzen führen, d. h. zu Instanzen mit mehreren Subnetzen. Dies kann die Komplexität der Netzwerksicherheit erhöhen und unbeabsichtigte Netzwerkpfade und Zugriffe zur Folge haben.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SEC-5	Wie werden Ihre Netzwerkressourcen geschützt? Jede Workload, die über irgendeine Form von Netzwerkkonnektivität verfügt, ob über das Internet oder ein privates Netzwerk, benötigt mehrere Schutzebenen, um vor externen und internen netzwerkbasierten Bedrohungen geschützt zu sein.	ec-2 instance-no-public-ip	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon Elastic Compute Cloud (Amazon EC2) - Instances nicht öffentlich zugänglich sind. EC2 Amazon-Instances können vertrauliche Informationen enthalten, und für solche Konten ist eine Zugriffskontrolle erforderlich.
SEC-5	Wie werden Ihre Netzwerkressourcen geschützt? Jede Workload, die über irgendeine Form von Netzwerkkonnektivität verfügt, ob über das Internet oder ein privates Netzwerk, benötigt mehrere Schutzebenen, um vor externen und internen netzwerkbasierten Bedrohungen geschützt zu sein.	emr-master-no-public-ip	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon EMR-Cluster-Masterknoten nicht öffentlich zugänglich sind. Amazon-EMR-Cluster-Hauptknoten können vertrauliche Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SEC-5	Wie werden Ihre Netzwerkressourcen geschützt? Jede Workload, die über irgendeine Form von Netzwerkkonnektivität verfügt, ob über das Internet oder ein privates Netzwerk, benötigt mehrere Schutzebenen, um vor externen und internen netzwerkbasierten Bedrohungen geschützt zu sein.	lambda-function-public-access-verboten	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass AWS Lambda-Funktionen nicht öffentlich zugänglich sind. Der öffentliche Zugriff kann möglicherweise die Verfügbarkeit von Ressourcen beeinträchtigen.
SEC-5	Wie werden Ihre Netzwerkressourcen geschützt? Jede Workload, die über irgendeine Form von Netzwerkkonnektivität verfügt, ob über das Internet oder ein privates Netzwerk, benötigt mehrere Schutzebenen, um vor externen und internen netzwerkbasierten Bedrohungen geschützt zu sein.	no-unrestricted-route-to-igw	Stellen Sie sicher, dass EC2 Amazon-Routentabellen keine uneingeschränkten Routen zu einem Internet-Gateway enthalten. Durch das Entfernen oder Beschränken des Internetzugangs für Workloads innerhalb von Amazon VPCs können unbeabsichtigte Zugriffe in Ihrer Umgebung reduziert werden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SEC-5	Wie werden Ihre Netzwerkressourcen geschützt? Jede Workload, die über irgendeine Form von Netzwerkkonnektivität verfügt, ob über das Internet oder ein privates Netzwerk, benötigt mehrere Schutzebenen, um vor externen und internen netzwerkbasierten Bedrohungen geschützt zu sein.	rds-instance-public-access-überprüfen	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Relational Database Service (Amazon RDS) -Instances nicht öffentlich sind. Amazon-RDS-Datenbank-Instances können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SEC-5	Wie werden Ihre Netzwerkressourcen geschützt? Jede Workload, die über irgendeine Form von Netzwerkkonnektivität verfügt, ob über das Internet oder ein privates Netzwerk, benötigt mehrere Schutzebenen, um vor externen und internen netzwerkbasierten Bedrohungen geschützt zu sein.	rds-snapshots-public-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Relational Database Service (Amazon RDS) -Instances nicht öffentlich sind. Amazon-RDS-Datenbank-Instances können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SEC-5	Wie werden Ihre Netzwerkressourcen geschützt? Jede Workload, die über irgendeine Form von Netzwerkkonnektivität verfügt, ob über das Internet oder ein privates Netzwerk, benötigt mehrere Schutzebenen, um vor externen und internen netzwerkbasierten Bedrohungen geschützt zu sein.	redshift-cluster-public-access-überprüfen	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Redshift Redshift-Cluster nicht öffentlich sind. Amazon-Redshift-Cluster können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SEC-5	Wie werden Ihre Netzwerkressourcen geschützt? Jede Workload, die über irgendeine Form von Netzwerkkonnektivität verfügt, ob über das Internet oder ein privates Netzwerk, benötigt mehrere Schutzebenen, um vor externen und internen netzwerkbasierten Bedrohungen geschützt zu sein.	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) Security Groups können bei der Verwaltung des Netzwerkzugriffs helfen, indem sie eine statusbehaftete Filterung von eingehendem und ausgehendem Netzwerkverkehr zu Ressourcen bereitstellen. AWS Indem Sie eingehenden (oder ausgehenden) Datenverkehr von 0.0.0.0/0 zu Port 22 bei Ihren Ressourcen nicht zulassen, können Sie den Fernzugriff einschränken.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SEC-5	Wie werden Ihre Netzwerkressourcen geschützt? Jede Workload, die über irgendeine Form von Netzwerkkonnektivität verfügt, ob über das Internet oder ein privates Netzwerk, benötigt mehrere Schutzebenen, um vor externen und internen netzwerkbasierten Bedrohungen geschützt zu sein.	s3-Blöcke, periodisch account-level-public-access	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Simple Storage Service (Amazon S3) -Buckets nicht öffentlich zugänglich sind. Diese Regel trägt dazu bei, sensible Daten vor unbefugten Remote-Benutzern zu schützen, indem sie den öffentlichen Zugriff verhindert. Mit dieser Regel können Sie optional die Parameter ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) und restrictPublicBuckets Parameter (Config Default: True) festlegen. Die tatsächlichen Werte müssen den Richtlini

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			en Ihrer Organisation entsprechen.
SEC-5	Wie werden Ihre Netzwerkressourcen geschützt? Jede Workload, die über irgendeine Form von Netzwerkkonnektivität verfügt, ob über das Internet oder ein privates Netzwerk, benötigt mehrere Schutzebenen, um vor externen und internen netzwerkbasierten Bedrohungen geschützt zu sein.	s3 bucket-level-public-access - verboten	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Simple Storage Service (Amazon S3) -Buckets nicht öffentlich zugänglich sind. Diese Regel trägt dazu bei, sensible Daten vor unbefugten Remote-Benutzern zu schützen, indem sie den öffentlichen Zugriff auf Bucket-Ebene verhindert.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SEC-5	Wie werden Ihre Netzwerkressourcen geschützt? Jede Workload, die über irgendeine Form von Netzwerkkonnektivität verfügt, ob über das Internet oder ein privates Netzwerk, benötigt mehrere Schutzebenen, um vor externen und internen netzwerkbasierten Bedrohungen geschützt zu sein.	s-3 bucket-public-read-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie nur autorisierten Benutzern, Prozessen und Geräten Zugriff auf Amazon Simple Storage Service (Amazon S3) - Buckets gewähren. Die Verwaltung des Zugriffs sollte mit der Klassifizierung der Daten übereinstimmen.
SEC-5	Wie werden Ihre Netzwerkressourcen geschützt? Jede Workload, die über irgendeine Form von Netzwerkkonnektivität verfügt, ob über das Internet oder ein privates Netzwerk, benötigt mehrere Schutzebenen, um vor externen und internen netzwerkbasierten Bedrohungen geschützt zu sein.	s3- bucket-public-write-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie nur autorisierten Benutzern, Prozessen und Geräten Zugriff auf Amazon Simple Storage Service (Amazon S3) - Buckets gewähren. Die Verwaltung des Zugriffs sollte mit der Klassifizierung der Daten übereinstimmen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SEC-5	Wie werden Ihre Netzwerkressourcen geschützt? Jede Workload, die über irgendeine Form von Netzwerkkonnektivität verfügt, ob über das Internet oder ein privates Netzwerk, benötigt mehrere Schutzebenen, um vor externen und internen netzwerkbasierten Bedrohungen geschützt zu sein.	sagemaker-notebook-no-direct-Internetzugang	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass SageMaker Amazon-Notebooks keinen direkten Internetzugang zulassen. Indem Sie direkten Internetzugang blockieren, vermeiden Sie, dass unbefugte Benutzer auf sensible Daten zugreifen.
SEC-5	Wie werden Ihre Netzwerkressourcen geschützt? Jede Workload, die über irgendeine Form von Netzwerkkonnektivität verfügt, ob über das Internet oder ein privates Netzwerk, benötigt mehrere Schutzebenen, um vor externen und internen netzwerkbasierten Bedrohungen geschützt zu sein.	ssm-document-not-public	Stellen Sie sicher, dass AWS Systems Manager (SSM) - Dokumente nicht öffentlich sind, da dies einen unbeabsichtigten Zugriff auf Ihre SSM-Dokumente ermöglichen kann. Ein öffentliches SSM-Dokument kann Informationen über Ihr Konto, Ihre Ressourcen und internen Prozesse preisgeben.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SEC-5	Wie werden Ihre Netzwerkressourcen geschützt? Jede Workload, die über irgendeine Form von Netzwerkkonnektivität verfügt, ob über das Internet oder ein privates Netzwerk, benötigt mehrere Schutzebenen, um vor externen und internen netzwerkbasierten Bedrohungen geschützt zu sein.	subnet-auto-assign-public-ip-deaktiviert	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon Virtual Private Cloud (VPC) -Subnetzen nicht automatisch eine öffentliche IP-Adresse zugewiesen wird. Amazon Elastic Compute Cloud (EC2) -Instances, die in Subnetzen gestartet werden, in denen dieses Attribut aktiviert ist, haben ihrer primären Netzwerkschnittstelle eine öffentliche IP-Adresse zugewiesen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SEC-5	Wie werden Ihre Netzwerkressourcen geschützt? Jede Workload, die über irgendeine Form von Netzwerkkonnektivität verfügt, ob über das Internet oder ein privates Netzwerk, benötigt mehrere Schutzebenen, um vor externen und internen netzwerkbasierten Bedrohungen geschützt zu sein.	vpc-default-security-group-geschlossen	Sicherheitsgruppen von Amazon Elastic Compute Cloud (Amazon EC2) können bei der Verwaltung des Netzwerkzugriffs helfen, indem sie eine statusbehaftete Filterung des ein- und ausgehenden Netzwerkverkehrs zu Ressourcen bereitstellen. AWS Die Beschränkung des gesamten Datenverkehrs auf die Standardsicherheitsgruppe hilft dabei, den Fernzugriff auf Ihre Ressourcen einzuschränken. AWS

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SEC-5	Wie werden Ihre Netzwerkressourcen geschützt? Jede Workload, die über irgendeine Form von Netzwerkkonnektivität verfügt, ob über das Internet oder ein privates Netzwerk, benötigt mehrere Schutzebenen, um vor externen und internen netzwerkbasierten Bedrohungen geschützt zu sein.	autoscaling-launch-config-public-ip-deaktiviert	Wenn Sie Ihre Netzwerkschnittstellen mit einer öffentlichen IP-Adresse konfigurieren, sind die diesen Netzwerkschnittstellen zugehörigen Ressourcen über das Internet erreichbar. EC2 Ressourcen sollten nicht öffentlich zugänglich sein, da dies einen unbeabsichtigten Zugriff auf Ihre Anwendungen oder Server ermöglichen kann.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SEC-5	Wie werden Ihre Netzwerkressourcen geschützt? Jede Workload, die über irgendeine Form von Netzwerkkonnektivität verfügt, ob über das Internet oder ein privates Netzwerk, benötigt mehrere Schutzebenen, um vor externen und internen netzwerkbasierten Bedrohungen geschützt zu sein.	restricted-common-ports	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass gemeinsame Ports für Amazon Elastic Compute Cloud (Amazon EC2) -Sicherheitsgruppen eingeschränkt sind. Wenn der Zugriff auf Ports nicht auf vertrauenswürdige Quellen beschränkt wird, kann dies zu Angriffen auf die Verfügbarkeit, Integrität und Vertraulichkeit von Systemen führen. Mit dieser Regel können Sie optional die Parameter blockedPort1–blockedPort5 festlegen (Standardkonfigurationen: 20, 21, 3389, 3306, 4333). Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SEC-5	Wie werden Ihre Netzwerkressourcen geschützt? Jede Workload, die über irgendeine Form von Netzwerkkonnektivität verfügt, ob über das Internet oder ein privates Netzwerk, benötigt mehrere Schutzebenen, um vor externen und internen netzwerkbasierten Bedrohungen geschützt zu sein.	vpc-sg-open-only-to-authorized-ports	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass gemeinsame Ports für Amazon Elastic Compute Cloud (Amazon EC2) -Sicherheitsgruppen eingeschränkt sind. Wenn der Zugriff auf Ports nicht auf vertrauenswürdige Quellen beschränkt wird, kann dies zu Angriffen auf die Verfügbarkeit, Integrität und Vertraulichkeit von Systemen führen. Durch die Beschränkung des Zugriffs auf Ressourcen innerhalb einer Sicherheitsgruppe aus dem Internet (0.0.0.0/0) kann der Fernzugriff auf interne Systeme gesteuert werden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SEC-5	Wie werden Ihre Rechenressourcen geschützt? Die Rechenressourcen in Ihrer Workload erfordern mehrere Verteidigungsebenen, um sie vor externen und internen Bedrohungen zu schützen. Zu den Rechenressourcen gehören EC2 Instanzen, Container, AWS Lambda-Funktionen, Datenbankdienste, IoT-Geräte und mehr.	waf-regional-rule-not-leer	Stellen Sie sicher, dass Ihre AWS WAF eine Regel hat, die nicht leer ist. Eine Regel ohne Bedingungen kann zu unbeabsichtigtem Verhalten führen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SEC-5	Wie werden Ihre Rechenressourcen geschützt? Die Rechenressourcen in Ihrer Workload erfordern mehrere Verteidigungsebenen, um sie vor externen und internen Bedrohungen zu schützen. Zu den Rechenressourcen gehören EC2 Instanzen, Container, AWS Lambda-Funktionen, Datenbankdienste, IoT-Geräte und mehr.	waf-regional-rulegroup-not-leer	Stellen Sie sicher, dass Ihre AWS WAF eine Regelgruppe hat, die nicht leer ist. Eine leere Regelgruppe kann zu unbeabsichtigtem Verhalten führen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SEC-5	Wie werden Ihre Rechenressourcen geschützt? Die Rechenressourcen in Ihrer Workload erfordern mehrere Verteidigungsebene n, um sie vor externen und internen Bedrohungen zu schützen. Zu den Rechenressourcen gehören EC2 Instanzen, Container , AWS Lambda-Fu nktionen, Datenbank dienste, IoT-Geräte und mehr.	waf-regional-webacl-not-leer	Eine an eine AWS WAF angehängt e Web-ACL kann eine Sammlung von Regeln und Regelgruppen zur Überprüfung und Steuerung von Webanfragen enthalten. Wenn eine Web-ACL leer ist, wird der Webdatenverkehr weitergeleitet, ohne von der WAF erkannt oder bearbeitet zu werden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SEC-5	Wie werden Ihre Rechenressourcen geschützt? Die Rechenressourcen in Ihrer Workload erfordern mehrere Verteidigungsebenen, um sie vor externen und internen Bedrohungen zu schützen. Zu den Rechenressourcen gehören EC2 Instanzen, Container, AWS Lambda-Funktionen, Datenbankdienste, IoT-Geräte und mehr.	vpc-network-acl-unused-überprüfen	Diese Regel stellt sicher, dass Amazon Virtual Private Cloud (VPC)-Netzwerkzugriffskontrolllisten verwendet werden. Die Überwachung ungenutzter Netzwerkzugriffskontrolllisten kann zu einer genauen Inventarisierung und Verwaltung Ihrer Umgebung beitragen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SEC-5	Wie werden Ihre Netzwerkressourcen geschützt? Jede Workload, die über irgendeine Form von Netzwerkkonnektivität verfügt, ob über das Internet oder ein privates Netzwerk, benötigt mehrere Schutzebenen, um vor externen und internen netzwerkbasierten Bedrohungen geschützt zu sein.	guardduty-enabled-centralized	Amazon GuardDuty kann mithilfe von Threat Intelligence Feeds helfen, potenzielle Cybersicherheitsereignisse zu überwachen und zu erkennen. Dazu gehören Listen mit bösartigen IPs und maschinellen Lernmethoden zur Identifizierung unerwarteter, nicht autorisierter und bösartiger Aktivitäten in Ihrer AWS Cloud-Umgebung.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SEC-5	Wie werden Ihre Netzwerkressourcen geschützt? Jede Workload, die über irgendeine Form von Netzwerkkonnektivität verfügt, ob über das Internet oder ein privates Netzwerk, benötigt mehrere Schutzebenen, um vor externen und internen netzwerkbasierten Bedrohungen geschützt zu sein.	vpc-flow-logs-enabled	VPC-Flow-Protokolle erfassen detaillierte Informationsdatensätze über den IP-Datenverkehr, der zu und von Netzwerkschnittstellen in Ihrer Amazon Virtual Private Cloud (Amazon VPC) fließt. Standardmäßig enthalten Flow-Protokolldatensätze Werte für die verschiedenen Komponenten des IP-Flows, einschließlich Quelle, Ziel und Protokoll.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SEC-6	Wie werden Ihre Rechenressourcen geschützt? Die Rechenressourcen in Ihrer Workload erfordern mehrere Verteidigungsebenen, um sie vor externen und internen Bedrohungen zu schützen. Zu den Rechenressourcen gehören EC2 Instanzen, Container, AWS Lambda-Funktionen, Datenbankdienste, IoT-Geräte und mehr.	rds-automatic-minor-version-Upgrade-fähig	Aktivieren Sie automatische Unterversions-Upgrades auf Ihren Amazon Relational Database Service (RDS)-Instances, um sicherzustellen, dass die aktuellen Updates für Unterversionen des Relational Database Management System (RDBMS) installiert sind, die Sicherheitspatches und Fehlerkorrekturen enthalten können.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SEC-6	Wie werden Ihre Rechenressourcen geschützt? Die Rechenressourcen in Ihrer Workload erfordern mehrere Verteidigungsebenen, um sie vor externen und internen Bedrohungen zu schützen. Zu den Rechenressourcen gehören EC2 Instanzen, Container, AWS Lambda-Funktionen, Datenbankdienste, IoT-Geräte und mehr.	cloud-trail-log-file-Validierung aktiviert	Verwenden Sie die AWS CloudTrail Protokolldateivalidierung, um die Integrität von Protokollen zu überprüfen. CloudTrail Mithilfe der Protokolldateivalidierung kann festgestellt werden, ob eine Protokolldatei geändert oder gelöscht wurde oder ob sie nach der Übermittlung CloudTrail unverändert geblieben ist. Dieses Feature wurde mit dem Branchenstandard entsprechenden Algorithmen entwickelt: SHA-256 für die Hashfunktion und SHA-256 mit RSA für digitale Signaturen. Aus diesem Grund ist es rechnerisch unmöglich, CloudTrail Protokolldateien unbemerkt zu ändern, zu löschen oder zu fälschen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SEC-6	Wie werden Ihre Rechenressourcen geschützt? Die Rechenressourcen in Ihrer Workload erfordern mehrere Verteidigungsebenen, um sie vor externen und internen Bedrohungen zu schützen. Zu den Rechenressourcen gehören EC2 Instanzen, Container, AWS Lambda-Funktionen, Datenbankdienste, IoT-Geräte und mehr.	cloudtrail-security-trail-enabled	Diese Regel trägt dazu bei, die Verwendung der AWS empfohlenen bewährten Sicherheitsmethoden für sicherzustellen AWS CloudTrail, indem geprüft wird, ob mehrere Einstellungen aktiviert sind. Dazu gehören die Verwendung von Protokollverschlüsselung, Protokollvalidierung und Aktivierung AWS CloudTrail in mehreren Regionen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SEC-6	Wie werden Ihre Rechenressourcen geschützt? Die Rechenressourcen in Ihrer Workload erfordern mehrere Verteidigungsebenen, um sie vor externen und internen Bedrohungen zu schützen. Zu den Rechenressourcen gehören EC2 Instanzen, Container, AWS Lambda-Funktionen, Datenbankdienste, IoT-Geräte und mehr.	elastic-beanstalk-managed-updates-aktiviert	Durch die Aktivierung verwalteter Plattformupdates für eine Amazon-Elastic-Beanstalk-Umgebung wird sichergestellt, dass die aktuellen verfügbaren Plattform-Fixes, -Updates und -Features für die Umgebung installiert sind. Eine bewährte Methode zur Sicherung von Systemen besteht darin, stets die aktuellen Patches zu installieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SEC-6	Wie werden Ihre Rechenressourcen geschützt? Die Rechenressourcen in Ihrer Workload erfordern mehrere Verteidigungsebenen, um sie vor externen und internen Bedrohungen zu schützen. Zu den Rechenressourcen gehören EC2 Instanzen, Container, AWS Lambda-Funktionen, Datenbankdienste, IoT-Geräte und mehr.	lambda-inside-vpc	Stellen Sie AWS Lambda-Funktionen in einer Amazon Virtual Private Cloud (Amazon VPC) bereit, um eine sichere Kommunikation zwischen einer Funktion und anderen Diensten innerhalb der Amazon VPC zu gewährleisten. Bei dieser Konfiguration sind kein Internet-Gateway, kein NAT-Gerät und keine VPN-Verbindung erforderlich. Der gesamte Datenverkehr bleibt sicher in der Cloud. AWS Domains, die sich innerhalb einer VPC befinden, verfügen aufgrund ihrer logischen Isolierung im Vergleich zu Domains mit öffentlichen Endpunkten über eine zusätzliche Sicherheitsebene. Um den Zugriff ordnungsgemäß zu verwalten,

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			sollten AWS Lambda-Funktionen einer VPC zugewiesen werden.
SEC-6	Wie werden Ihre Rechenressourcen geschützt? Die Rechenressourcen in Ihrer Workload erfordern mehrere Verteidigungsebenen, um sie vor externen und internen Bedrohungen zu schützen. Zu den Rechenressourcen gehören EC2 Instanzen, Container, AWS Lambda-Funktionen, Datenbankdienste, IoT-Geräte und mehr.	ecr-private-image-scanning-aktiviert	Der Amazon Elastic Container Repository (ECR)-Image-Scan unterstützt die Identifizierung von Software-Schwachstellen in Ihren Container-Images. Durch die Aktivierung von Image-Scans in ECR-Repositorys werden die Integrität und Sicherheit der gespeicherten Images mit einer zusätzlichen Überprüfungsebene verbessert.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SEC-6	Wie werden Ihre Rechenressourcen geschützt? Die Rechenressourcen in Ihrer Workload erfordern mehrere Verteidigungsebenen, um sie vor externen und internen Bedrohungen zu schützen. Zu den Rechenressourcen gehören EC2 Instanzen, Container, AWS Lambda-Funktionen, Datenbankdienste, IoT-Geräte und mehr.	ecs-container-insights-enabled	Die Überwachung ist ein wichtiger Bestandteil der Aufrechterhaltung der Zuverlässigkeit, Verfügbarkeit und Leistung von Amazon Elastic Container Service (ECS) und Ihrer AWS Lösungen. Container Insights bietet auch Diagnoseinformationen, wie z. B.Fehler beim Container-Neustart, damit Sie Probleme schnell aufdecken und beheben können.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SEC-6	Wie werden Ihre Rechenressourcen geschützt? Die Rechenressourcen in Ihrer Workload erfordern mehrere Verteidigungsebenen, um sie vor externen und internen Bedrohungen zu schützen. Zu den Rechenressourcen gehören EC2 Instanzen, Container, AWS Lambda-Funktionen, Datenbankdienste, IoT-Geräte und mehr.	ecs-fargate-latest-platform-Version	Sicherheitsupdates und Patches werden automatisch für Ihre AWS Fargate-Aufgaben bereitgestellt. Wenn ein Sicherheitsproblem gefunden wird, das eine AWS Fargate-Plattformversion betrifft, AWS wird die Plattformversion gepatcht. Um Sie bei der Patchverwaltung Ihrer Amazon Elastic Container Service (ECS) - Aufgaben zu unterstützen, auf denen AWS Fargate ausgeführt wird, aktualisieren Sie Ihre eigenständigen Service-Aufgaben, sodass sie die neueste Plattformversion verwenden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SEC-6	Wie werden Ihre Rechenressourcen geschützt? Die Rechenressourcen in Ihrer Workload erfordern mehrere Verteidigungsebenen, um sie vor externen und internen Bedrohungen zu schützen. Zu den Rechenressourcen gehören EC2 Instanzen, Container, AWS Lambda-Funktionen, Datenbankdienste, IoT-Geräte und mehr.	redshift-cluster-maintenancesettings-check	Diese Regel stellt sicher, dass Amazon-Redshift-Cluster die bevorzugten Einstellungen für Ihre Organisation haben. Insbesondere sorgt sie dafür, dass Cluster bevorzugte Wartungsfenster und automatisierte Aufbewahrungsfristen für Snapshots für die Datenbank haben. Für diese Regel müssen Sie die allowVersionUpgrade festlegen. Der Standardwert ist „true“. Außerdem können Sie optional den Zeitraum preferredMaintenanceWindow (der Standardwert ist sa: 16:00 -sa: 16:30) und den automated SnapshotRetention Zeitraum (der Standardwert ist 1) festlegen. Die tatsächlichen Werte müssen den Richtlini

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			en Ihrer Organisation entsprechen.
SEC-6	Wie werden Ihre Rechenressourcen geschützt? Die Rechenressourcen in Ihrer Workload erfordern mehrere Verteidigungsebenen, um sie vor externen und internen Bedrohungen zu schützen. Zu den Rechenressourcen gehören EC2 Instanzen, Container, AWS Lambda-Funktionen, Datenbankdienste, IoT-Geräte und mehr.	ec2-imdsv2-check	Stellen Sie sicher, dass die Methode Instance Metadata Service Version 2 (IMDSv2) aktiviert ist, um den Zugriff auf und die Kontrolle der Amazon Elastic Compute Cloud (Amazon EC2) - Instance-Metadaten zu schützen. Die IMDSv2 Methode verwendet sitzungsbasierte Kontrollen. Mit können Kontrollen implementiert werden IMDSv2, um Änderungen an Instanzmetadaten einzuschränken.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SEC-6	Wie werden Ihre Rechenressourcen geschützt? Die Rechenressourcen in Ihrer Workload erfordern mehrere Verteidigungsebenen, um sie vor externen und internen Bedrohungen zu schützen. Zu den Rechenressourcen gehören EC2 Instanzen, Container, AWS Lambda-Funktionen, Datenbankdienste, IoT-Geräte und mehr.	ec2- instance-multiple-eni-check	Diese Regel prüft, ob Ihre Amazon Elastic Compute Cloud (Amazon EC2) -Instances mehrere haben ENIs. Wenn mehrere vorhanden sind, ENIs kann dies zu doppelt vernetzten Instanzen führen, d. h. zu Instanzen mit mehreren Subnetzen. Dies kann die Komplexität der Netzwerksicherheit erhöhen und unbeabsichtigte Netzwerkpfade und Zugriffe zur Folge haben.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SEC-6	Wie werden Ihre Rechenressourcen geschützt? Die Rechenressourcen in Ihrer Workload erfordern mehrere Verteidigungsebenen, um sie vor externen und internen Bedrohungen zu schützen. Zu den Rechenressourcen gehören EC2 Instanzen, Container, AWS Lambda-Funktionen, Datenbankdienste, IoT-Geräte und mehr.	ec2- instance-no-public-ip	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon Elastic Compute Cloud (Amazon EC2) - Instances nicht öffentlich zugänglich sind. EC2 Amazon-Instances können vertrauliche Informationen enthalten, und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SEC-6	Wie werden Ihre Rechenressourcen geschützt? Die Rechenressourcen in Ihrer Workload erfordern mehrere Verteidigungsebenen, um sie vor externen und internen Bedrohungen zu schützen. Zu den Rechenressourcen gehören EC2 Instanzen, Container, AWS Lambda-Funktionen, Datenbankdienste, IoT-Geräte und mehr.	ec2- instance-profile-attached	EC2 Instanzprofile übergeben eine IAM-Rolle an eine EC2 Instance. Das Anhängen eines Instance-Profils an Ihre Instances kann bei der Implementierung von geringsten Berechtigungen und der Berechtigungsverwaltung helfen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SEC-6	Wie werden Ihre Rechenressourcen geschützt? Die Rechenressourcen in Ihrer Workload erfordern mehrere Verteidigungsebenen, um sie vor externen und internen Bedrohungen zu schützen. Zu den Rechenressourcen gehören EC2 Instanzen, Container, AWS Lambda-Funktionen, Datenbankdienste, IoT-Geräte und mehr.	ec2-manager instance-managed-by-systems	Eine Bestandsaufnahme der Softwareplattformen und Anwendungen innerhalb des Unternehmens ist möglich, indem Amazon Elastic Compute Cloud (Amazon EC2) - Instances mit AWS Systems Manager verwaltet werden. Verwenden Sie AWS Systems Manager, um detaillierte Systemkonfigurationen, Betriebssystem-Patch-Levels, Namen und Typ der Dienste, Softwareinstallationen, Anwendungsname, Herausgeber und Version sowie andere Details zu Ihrer Umgebung bereitzustellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SEC-6	Wie werden Ihre Rechenressourcen geschützt? Die Rechenressourcen in Ihrer Workload erfordern mehrere Verteidigungsebenen, um sie vor externen und internen Bedrohungen zu schützen. Zu den Rechenressourcen gehören EC2 Instanzen, Container, AWS Lambda-Funktionen, Datenbankdienste, IoT-Geräte und mehr.	ec2- -eni-periodisch security-group-attached-to	Diese Regel stellt sicher, dass die Sicherheitsgruppen an eine Amazon Elastic Compute Cloud (Amazon EC2) -Instance oder an eine ENI angehängt sind. Diese Regel hilft bei der Überwachung ungenutzter Sicherheitsgruppen im Bestand und bei der Verwaltung Ihrer Umgebung.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SEC-6	Wie werden Ihre Rechenressourcen geschützt? Die Rechenressourcen in Ihrer Workload erfordern mehrere Verteidigungsebenen, um sie vor externen und internen Bedrohungen zu schützen. Zu den Rechenressourcen gehören EC2 Instanzen, Container, AWS Lambda-Funktionen, Datenbankdienste, IoT-Geräte und mehr.	ec2-stopped-instance	Aktivieren Sie diese Regel, um bei der Basiskonfiguration von Amazon Elastic Compute Cloud (Amazon EC2) - Instances zu helfen, indem Sie überprüfen, ob EC2 Amazon-Instances gemäß den Standards Ihrer Organisation für mehr als die zulässige Anzahl von Tagen gestoppt wurden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SEC-6	Wie werden Ihre Rechenressourcen geschützt? Die Rechenressourcen in Ihrer Workload erfordern mehrere Verteidigungsebenen, um sie vor externen und internen Bedrohungen zu schützen. Zu den Rechenressourcen gehören EC2 Instanzen, Container, AWS Lambda-Funktionen, Datenbankdienste, IoT-Geräte und mehr.	ec2- volume-inuse-check	Diese Regel stellt sicher, dass Amazon Elastic Block Store-Volumes, die an Amazon Elastic Compute Cloud (Amazon EC2) - Instances angehängt sind, zum Löschen markiert werden, wenn eine Instance beendet wird. Wenn ein Amazon-EBS-Volume nicht gelöscht wird, wenn die Instance, an die es angehängt ist, beendet wird, kann dies gegen das Konzept der geringsten Funktionalität verstoßen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SEC-6	Wie werden Ihre Rechenressourcen geschützt? Die Rechenressourcen in Ihrer Workload erfordern mehrere Verteidigungsebenen, um sie vor externen und internen Bedrohungen zu schützen. Zu den Rechenressourcen gehören EC2 Instanzen, Container, AWS Lambda-Funktionen, Datenbankdienste, IoT-Geräte und mehr.	ec2-check managedinstance-association-compliance-status	Verwenden Sie AWS Systems Manager Associations, um bei der Inventarisierung von Softwareplattformen und Anwendungen innerhalb eines Unternehmens zu helfen. AWS Systems Manager weist Ihren verwalteten Instanzen einen Konfigurationsstatus zu und ermöglicht es Ihnen, Basiswerte für Betriebssystem-Patch-Levels, Softwareinstallationen, Anwendungskonfigurationen und andere Details zu Ihrer Umgebung festzulegen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SEC-6	Wie werden Ihre Rechenressourcen geschützt? Die Rechenressourcen in Ihrer Workload erfordern mehrere Verteidigungsebenen, um sie vor externen und internen Bedrohungen zu schützen. Zu den Rechenressourcen gehören EC2 Instanzen, Container, AWS Lambda-Funktionen, Datenbankdienste, IoT-Geräte und mehr.	ec2-check managedinstance-patch-compliance-status	Aktivieren Sie diese Regel, um bei der Identifizierung und Dokumentation von Sicherheitslücken in Amazon Elastic Compute Cloud (Amazon EC2) zu helfen. Die Regel prüft, ob die EC2 Amazon-Instance die Patch-Konformität im AWS Systems Manager gemäß den Richtlinien und Verfahren Ihrer Organisation einhält.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SEC-8	Wie werden Ihre Daten im Ruhezustand geschützt? Schützen Sie Ihre Daten im Ruhezustand, indem Sie mehrere Kontrollen implementieren und so das Risiko eines unbefugten Zugriffs oder einer falschen Handhabung verringern.	api-gw-cache-enabled-und verschlüsselt	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass die Verschlüsselung für den Cache Ihrer API-Gateway-Stufe aktiviert ist. Zum Schutz von für die API-Methode erfassten sensiblen Daten müssen Sie die Verschlüsselung von Daten im Ruhezustand aktivieren.
SEC-8	Wie werden Ihre Daten im Ruhezustand geschützt? Schützen Sie Ihre Daten im Ruhezustand, indem Sie mehrere Kontrollen implementieren und so das Risiko eines unbefugten Zugriffs oder einer falschen Handhabung verringern.	backup-recovery-point-encrypted	Stellen Sie sicher, dass die Verschlüsselung für Ihre AWS Backup-Wiederherstellungspunkte aktiviert ist. Da sensible Daten auch im Ruhezustand vorhanden sein können, sollten Sie die Verschlüsselung im Ruhezustand aktivieren, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SEC-8	Wie werden Ihre Daten im Ruhezustand geschützt? Schützen Sie Ihre Daten im Ruhezustand, indem Sie mehrere Kontrollen implementieren und so das Risiko eines unbefugten Zugriffs oder einer falschen Handhabung verringern.	codebuild-project-artifact-encryption	Um sensible Daten im Ruhezustand zu schützen, stellen Sie sicher, dass die Verschlüsselung für Ihre AWS CodeBuild Artefakte aktiviert ist.
SEC-8	Wie werden Ihre Daten im Ruhezustand geschützt? Schützen Sie Ihre Daten im Ruhezustand, indem Sie mehrere Kontrollen implementieren und so das Risiko eines unbefugten Zugriffs oder einer falschen Handhabung verringern.	codebuild-project-s3-Log-verschlüsselt	Um sensible Daten im Speicher zu schützen, stellen Sie sicher, dass die Verschlüsselung für Ihre in Amazon S3 gespeicherten AWS CodeBuild Protokolle aktiviert ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SEC-8	Wie werden Ihre Daten im Ruhezustand geschützt? Schützen Sie Ihre Daten im Ruhezustand, indem Sie mehrere Kontrollen implementieren und so das Risiko eines unbefugten Zugriffs oder einer falschen Handhabung verringern.	kms-cmk-not-scheduled-zum Löschen	Um Daten im Ruhezustand zu schützen, sollten Sie sicherstellen, dass die für den Kunden erforderlichen Masterschlüssel (CMKs) nicht im AWS Key Management Service (AWS KMS) gelöscht werden. Da Schlüssel manchmal gelöscht werden müssen, können Sie mit dieser Regel alle zu löschenden Schlüssel überprüfen, falls ein Schlüssel versehentlich zur Löschung vorgemerkt wurde.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SEC-8	Wie werden Ihre Daten im Ruhezustand geschützt? Schützen Sie Ihre Daten im Ruhezustand, indem Sie mehrere Kontrollen implementieren und so das Risiko eines unbefugten Zugriffs oder einer falschen Handhabung verringern.	cloud-trail-encryption-enabled	Da sensible Daten vorhanden sein können und um Daten im Speicher zu schützen, sollten Sie sicherstellen, dass die Verschlüsselung für Ihre AWS CloudTrail Trails aktiviert ist.
SEC-8	Wie werden Ihre Daten im Ruhezustand geschützt? Schützen Sie Ihre Daten im Ruhezustand, indem Sie mehrere Kontrollen implementieren und so das Risiko eines unbefugten Zugriffs oder einer falschen Handhabung verringern.	cloudwatch-log-group-encrypted	Um sensible Daten im Speicher zu schützen, stellen Sie sicher, dass die Verschlüsselung für Ihre Amazon CloudWatch Log Groups aktiviert ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SEC-8	Wie werden Ihre Daten im Ruhezustand geschützt? Schützen Sie Ihre Daten im Ruhezustand, indem Sie mehrere Kontrollen implementieren und so das Risiko eines unbefugten Zugriffs oder einer falschen Handhabung verringern.	dynamodb-table-encrypted-kms	Stellen Sie sicher, dass die Verschlüsselung für Ihre Amazon-DynamoDB-Tabellen aktiviert ist. Um eventuell vorhandene sensible Daten im Ruhezustand in diesen Tabellen zu schützen, müssen Sie die Verschlüsselung von Daten im Ruhezustand aktivieren. Standardmäßig werden DynamoDB-Tabellen mit einem AWS eigenen Kundenhauptschlüssel (CMK) verschlüsselt.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SEC-8	Wie werden Ihre Daten im Ruhezustand geschützt? Schützen Sie Ihre Daten im Ruhezustand, indem Sie mehrere Kontrollen implementieren und so das Risiko eines unbefugten Zugriffs oder einer falschen Handhabung verringern.	ec2- ebs-encryption-by-default	Zum Schutz von Daten im Ruhezustand müssen Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon Elastic Block Store (Amazon EBS)-Volumes aktiviert ist. Um eventuell vorhandene sensible Daten im Ruhezustand zu schützen, müssen Sie die Verschlüsselung von Daten im Ruhezustand aktivieren.
SEC-8	Wie werden Ihre Daten im Ruhezustand geschützt? Schützen Sie Ihre Daten im Ruhezustand, indem Sie mehrere Kontrollen implementieren und so das Risiko eines unbefugten Zugriffs oder einer falschen Handhabung verringern.	efs-encrypted-check	Aktivieren Sie die Verschlüsselung für Ihr Amazon Elastic File System (EFS), um eventuell vorhandene sensible Daten sowie Daten im Ruhezustand zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SEC-8	Wie werden Ihre Daten im Ruhezustand geschützt? Schützen Sie Ihre Daten im Ruhezustand, indem Sie mehrere Kontrollen implementieren und so das Risiko eines unbefugten Zugriffs oder einer falschen Handhabung verringern.	elasticsearch-encrypted-at-rest	Da sensible Daten vorhanden sein können und um Daten im Ruhezustand zu schützen, sollten Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon OpenSearch Service (OpenSearch Service) -Domains aktiviert ist.
SEC-8	Wie werden Ihre Daten im Ruhezustand geschützt? Schützen Sie Ihre Daten im Ruhezustand, indem Sie mehrere Kontrollen implementieren und so das Risiko eines unbefugten Zugriffs oder einer falschen Handhabung verringern.	opensearch-encrypted-at-rest	Da sensible Daten vorhanden sein können und um Daten im Ruhezustand zu schützen, sollten Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon OpenSearch Service-Domains aktiviert ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SEC-8	Wie werden Ihre Daten im Ruhezustand geschützt? Schützen Sie Ihre Daten im Ruhezustand, indem Sie mehrere Kontrollen implementieren und so das Risiko eines unbefugten Zugriffs oder einer falschen Handhabung verringern.	encrypted-volumes	Um eventuell vorhandene sensible Daten sowie Daten im Ruhezustand zu schützen, muss die Verschlüsselung für Ihre Amazon Elastic Block Store (Amazon EBS)-Volumes aktiviert sein.
SEC-8	Wie werden Ihre Daten im Ruhezustand geschützt? Schützen Sie Ihre Daten im Ruhezustand, indem Sie mehrere Kontrollen implementieren und so das Risiko eines unbefugten Zugriffs oder einer falschen Handhabung verringern.	rds-snapshot-encrypted	Stellen Sie sicher, dass die Verschlüsselung für Ihre Amazon Relational Database Service (Amazon RDS)-Snapshots aktiviert ist. Um eventuell vorhandene sensible Daten im Ruhezustand zu schützen, muss die Verschlüsselung von Daten im Ruhezustand aktiviert sein.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SEC-8	Wie werden Ihre Daten im Ruhezustand geschützt? Schützen Sie Ihre Daten im Ruhezustand, indem Sie mehrere Kontrollen implementieren und so das Risiko eines unbefugten Zugriffs oder einer falschen Handhabung verringern.	rds-storage-encrypted	Zum Schutz von Daten im Ruhezustand müssen Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon Relational Database Service (Amazon RDS)-Instances aktiviert ist. Um eventuell vorhandene sensible Daten im Ruhezustand in Amazon-RDS-Instances zu schützen, muss die Verschlüsselung von Daten im Ruhezustand aktiviert sein.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SEC-8	Wie werden Ihre Daten im Ruhezustand geschützt? Schützen Sie Ihre Daten im Ruhezustand, indem Sie mehrere Kontrollen implementieren und so das Risiko eines unbefugten Zugriffs oder einer falschen Handhabung verringern.	redshift-cluster-configuration-check	Um Daten im Ruhezustand zu schützen, muss die Verschlüsselung für Ihre Amazon-Redshift-Cluster aktiviert sein. Sie müssen auch sicherstellen, dass die erforderlichen Konfigurationen auf Amazon-Redshift-Clustern bereitgestellt werden. Die Prüfungsprotokollierung muss aktiviert sein, um Informationen zu Verbindungen und Benutzeraktivitäten in der Datenbank bereitzustellen. Diese Regel erfordert, dass ein Wert für clusterDbEncrypted (Config Default: TRUE) und LoggingEnabled (Config Default: TRUE) gesetzt ist. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SEC-8	Wie werden Ihre Daten im Ruhezustand geschützt? Schützen Sie Ihre Daten im Ruhezustand, indem Sie mehrere Kontrollen implementieren und so das Risiko eines unbefugten Zugriffs oder einer falschen Handhabung verringern.	redshift-cluster-kms-enabled	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass die Verschlüsselung mit AWS Key Management Service (AWS KMS) für Ihren Amazon Redshift Redshift-Cluster aktiviert ist. Um eventuell vorhandene sensible Daten im Ruhezustand in Redshift-Clustern zu schützen, muss die Verschlüsselung von Daten im Ruhezustand aktiviert sein.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SEC-8	Wie werden Ihre Daten im Ruhezustand geschützt? Schützen Sie Ihre Daten im Ruhezustand, indem Sie mehrere Kontrollen implementieren und so das Risiko eines unbefugten Zugriffs oder einer falschen Handhabung verringern.	s3- aktiviert bucket-server-side-encryption	Zum Schutz von Daten im Ruhezustand müssen Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon Simple Storage Service (Amazon S3)-Buckets aktiviert ist. Um eventuell vorhandene sensible Daten im Ruhezustand in Amazon-S3-Buckets zu schützen, muss die Verschlüsselung aktiviert sein.
SEC-8	Wie werden Ihre Daten im Ruhezustand geschützt? Schützen Sie Ihre Daten im Ruhezustand, indem Sie mehrere Kontrollen implementieren und so das Risiko eines unbefugten Zugriffs oder einer falschen Handhabung verringern.	s-3 default-encryption-kms	Stellen Sie sicher, dass die Verschlüsselung für Ihre Amazon Simple Storage Service (Amazon S3)-Buckets aktiviert ist. Um eventuell vorhandene sensible Daten im Ruhezustand in einem Amazon-S3-Bucket zu schützen, muss die Verschlüsselung aktiviert sein.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SEC-8	Wie werden Ihre Daten im Ruhezustand geschützt? Schützen Sie Ihre Daten im Ruhezustand, indem Sie mehrere Kontrollen implementieren und so das Risiko eines unbefugten Zugriffs oder einer falschen Handhabung verringern.	sagemaker-endpoint-configuration-kms-key-konfiguriert	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass die Verschlüsselung mit dem AWS Key Management Service (AWS KMS) für Ihren Endpunkt aktiviert ist. SageMaker Da sensible Daten auf dem SageMaker Endgerät gespeichert werden können, sollten Sie die Verschlüsselung im Ruhezustand aktivieren, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SEC-8	Wie werden Ihre Daten im Ruhezustand geschützt? Schützen Sie Ihre Daten im Ruhezustand, indem Sie mehrere Kontrollen implementieren und so das Risiko eines unbefugten Zugriffs oder einer falschen Handhabung verringern.	sagemaker-notebook-instance-kms-schlüsselkonfiguriert	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass die Verschlüsselung mit dem AWS Key Management Service (AWS KMS) für Ihr Notebook aktiviert ist. SageMaker Da vertrauliche Daten im SageMaker Notebook gespeichert werden können, sollten Sie die Verschlüsselung im Ruhezustand aktivieren, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SEC-8	Wie werden Ihre Daten im Ruhezustand geschützt? Schützen Sie Ihre Daten im Ruhezustand, indem Sie mehrere Kontrollen implementieren und so das Risiko eines unbefugten Zugriffs oder einer falschen Handhabung verringern.	secretsmanager-using-cmk	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass die Verschlüsselung mit dem AWS Key Management Service (AWS KMS) für AWS Secrets Manager aktiviert ist. Aktivieren Sie die Verschlüsselung von Daten im Ruhezustand, um eventuell vorhandene sensible Daten im Ruhezustand im Secrets Manager zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SEC-8	Wie werden Ihre Daten im Ruhezustand geschützt? Schützen Sie Ihre Daten im Ruhezustand, indem Sie mehrere Kontrollen implementieren und so das Risiko eines unbefugten Zugriffs oder einer falschen Handhabung verringern.	sns-encrypted-kms	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass Ihre Amazon Simple Notification Service (Amazon SNS) -Themen mit dem AWS Key Management Service (AWS KMS) verschlüsselt werden müssen. Um eventuell vorhandene sensible Daten im Ruhezustand in veröffentlichten Nachrichten zu schützen, muss die Verschlüsselung von Daten im Ruhezustand aktiviert sein.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SEC-8	Wie werden Ihre Daten im Ruhezustand geschützt? Schützen Sie Ihre Daten im Ruhezustand, indem Sie mehrere Kontrollen implementieren und so das Risiko eines unbefugten Zugriffs oder einer falschen Handhabung verringern.	s3- bucket-versioning-enabled	Die Versionsverwaltung von Amazon Simple Storage Service (Amazon S3)-Buckets hilft dabei, mehrere Varianten eines Objekts im selben Amazon-S3-Bucket zu speichern. Verwenden Sie die Versionsverwaltung, um sämtliche Versionen aller Objekte in Ihrem Amazon-S3-Bucket zu speichern, abzurufen oder wiederherzustellen. Mit der Versionsverwaltung können Sie Versionen sowohl nach unbeabsichtigten Benutzeraktionen als auch nach Anwendungsfehlern problemlos wiederherstellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SEC-8	Wie werden Ihre Daten im Ruhezustand geschützt? Schützen Sie Ihre Daten im Ruhezustand, indem Sie mehrere Kontrollen implementieren und so das Risiko eines unbefugten Zugriffs oder einer falschen Handhabung verringern.	account-part-of-organizations	Durch die zentrale Verwaltung AWS-Konten innerhalb von AWS Organizations wird sichergestellt, dass die Konten den Vorschriften entsprechen. Eine fehlende zentrale Kontoverwaltung kann zu inkonsistenten Kontokonfigurationen führen, wodurch Ressourcen und sensible Daten offengelegt werden können.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SEC-8	Wie werden Ihre Daten im Ruhezustand geschützt? Schützen Sie Ihre Daten im Ruhezustand, indem Sie mehrere Kontrollen implementieren und so das Risiko eines unbefugten Zugriffs oder einer falschen Handhabung verringern.	S3- Blöcke account-level-public-access — periodisch	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Simple Storage Service (Amazon S3) -Buckets nicht öffentlich zugänglich sind. Diese Regel trägt dazu bei, sensible Daten vor unbefugten Remote-Benutzern zu schützen, indem sie den öffentlichen Zugriff verhindert. Mit dieser Regel können Sie optional die Parameter ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) und restrictPublicBuckets Parameter (Config Default: True) festlegen. Die tatsächlichen Werte müssen den Richtlini

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			en Ihrer Organisation entsprechen.
SEC-8	Wie werden Ihre Daten im Ruhezustand geschützt? Schützen Sie Ihre Daten im Ruhezustand, indem Sie mehrere Kontrollen implementieren und so das Risiko eines unbefugten Zugriffs oder einer falschen Handhabung verringern.	s3 bucket-level-public-access - verboten	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Simple Storage Service (Amazon S3) -Buckets nicht öffentlich zugänglich sind. Diese Regel trägt dazu bei, sensible Daten vor unbefugten Remote-Benutzern zu schützen, indem sie den öffentlichen Zugriff auf Bucket-Ebene verhindert.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SEC-8	Wie werden Ihre Daten im Ruhezustand geschützt? Schützen Sie Ihre Daten im Ruhezustand, indem Sie mehrere Kontrollen implementieren und so das Risiko eines unbefugten Zugriffs oder einer falschen Handhabung verringern.	s-3 bucket-public-read-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie nur autorisierten Benutzern, Prozessen und Geräten Zugriff auf Amazon Simple Storage Service (Amazon S3) - Buckets gewähren. Die Verwaltung des Zugriffs sollte mit der Klassifizierung der Daten übereinstimmen.
SEC-8	Wie werden Ihre Daten im Ruhezustand geschützt? Schützen Sie Ihre Daten im Ruhezustand, indem Sie mehrere Kontrollen implementieren und so das Risiko eines unbefugten Zugriffs oder einer falschen Handhabung verringern.	s3- bucket-public-write-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie nur autorisierten Benutzern, Prozessen und Geräten Zugriff auf Amazon Simple Storage Service (Amazon S3) - Buckets gewähren. Die Zugriffsverwaltung muss der Klassifizierung der Daten entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SEC-9	Wie werden Ihre Daten während der Übertragung geschützt? Schützen Sie Ihre Daten während der Übertragung, indem Sie mehrere Kontrollen implementieren und so das Risiko eines unbefugten Zugriffs oder eines Datenverlusts verringern.	acm-certificate-expiration-check	Stellen Sie sicher, dass die Netzwerkintegrität geschützt ist, indem Sie sicherstellen, dass X509-Zertifikate von AWS ACM ausgestellt werden. Diese Zertifikate müssen gültig und dürfen nicht abgelaufen sein. Für diese Regel ist ein Wert für erforderlich daysToExpiration (Wert für bewährte AWS Grundregeln für Sicherheit: 90). Der tatsächliche Wert muss den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SEC-9	Wie werden Ihre Daten während der Übertragung geschützt? Schützen Sie Ihre Daten während der Übertragung, indem Sie mehrere Kontrollen implementieren und so das Risiko eines unbefugten Zugriffs oder eines Datenverlusts verringern.	elbv-2 acm-certificate-required	Zum Schutz von eventuell vorhandenen sensiblen Daten sowie von Daten während der Übertragung muss die Verschlüsselung für Ihr Elastic Load Balancing aktiviert sein. Verwenden Sie AWS Certificate Manager, um öffentliche und private SSL/TLS-Zertifikate mit AWS Diensten und internen Ressourcen zu verwalten, bereitzustellen und bereitzustellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SEC-9	Wie werden Ihre Daten während der Übertragung geschützt? Schützen Sie Ihre Daten während der Übertragung, indem Sie mehrere Kontrollen implementieren und so das Risiko eines unbefugten Zugriffs oder eines Datenverlusts verringern.	elb-acm-certificate-required	Zum Schutz von eventuell vorhandenen sensiblen Daten sowie von Daten während der Übertragung muss die Verschlüsselung für Ihr Elastic Load Balancing aktiviert sein. Verwenden Sie AWS Certificate Manager, um öffentliche und private SSL/TLS-Zertifikate mit AWS Diensten und internen Ressourcen zu verwalten, bereitzustellen und bereitzustellen.
SEC-9	Wie werden Ihre Daten während der Übertragung geschützt? Schützen Sie Ihre Daten während der Übertragung, indem Sie mehrere Kontrollen implementieren und so das Risiko eines unbefugten Zugriffs oder eines Datenverlusts verringern.	alb-http-drop-invalid-Header-fähig	Stellen Sie sicher, dass Ihre Elastic Load Balancers (ELB) so konfiguriert sind, dass sie HTTP-Header löschen. Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SEC-9	Wie werden Ihre Daten während der Übertragung geschützt? Schützen Sie Ihre Daten während der Übertragung, indem Sie mehrere Kontrollen implementieren und so das Risiko eines unbefugten Zugriffs oder eines Datenverlusts verringern.	alb-http-to-https-Umleitungsprüfung	Um Daten während der Übertragung zu schützen, stellen Sie sicher, dass Ihr Application Load Balancer unverschlüsselte HTTP-Anfragen automatisch an HTTPS umleitet. Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.
SEC-9	Wie werden Ihre Daten während der Übertragung geschützt? Schützen Sie Ihre Daten während der Übertragung, indem Sie mehrere Kontrollen implementieren und so das Risiko eines unbefugten Zugriffs oder eines Datenverlusts verringern.	api-gw-ssl-enabled	Stellen Sie sicher, dass die REST-API-Stufen von Amazon API Gateway mit SSL-Zertifikaten konfiguriert sind, damit Backend-Systeme überprüfen können, ob Anforderungen von API Gateway stammen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SEC-9	Wie werden Ihre Daten während der Übertragung geschützt? Schützen Sie Ihre Daten während der Übertragung, indem Sie mehrere Kontrollen implementieren und so das Risiko eines unbefugten Zugriffs oder eines Datenverlusts verringern.	elasticsearch-node-to-node-Verschlüsselungsprüfung	Stellen Sie sicher, dass die node-to-node Verschlüsselung für Amazon OpenSearch Service aktiviert ist. Node-to-nodeVerschlüsselung ermöglicht die TLS 1.2-Verschlüsselung für die gesamte Kommunikation innerhalb der Amazon Virtual Private Cloud (Amazon VPC). Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SEC-9	Wie werden Ihre Daten während der Übertragung geschützt? Schützen Sie Ihre Daten während der Übertragung, indem Sie mehrere Kontrollen implementieren und so das Risiko eines unbefugten Zugriffs oder eines Datenverlusts verringern.	opensearch-node-to-node-Verschlüsselungsprüfung	Stellen Sie sicher, dass die node-to-node Verschlüsselung für Amazon OpenSearch Service aktiviert ist. Node-to-nodeVerschlüsselung ermöglicht die TLS 1.2-Verschlüsselung für die gesamte Kommunikation innerhalb der Amazon Virtual Private Cloud (Amazon VPC). Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SEC-9	Wie werden Ihre Daten während der Übertragung geschützt? Schützen Sie Ihre Daten während der Übertragung, indem Sie mehrere Kontrollen implementieren und so das Risiko eines unbefugten Zugriffs oder eines Datenverlusts verringern.	opensearch-https-required	Da sensible Daten existieren können und um Daten während der Übertragung zu schützen, sollten Sie sicherstellen, dass HTTPS für Verbindungen zu Ihren Amazon OpenSearch Service-Domains aktiviert ist.
SEC-9	Wie werden Ihre Daten während der Übertragung geschützt? Schützen Sie Ihre Daten während der Übertragung, indem Sie mehrere Kontrollen implementieren und so das Risiko eines unbefugten Zugriffs oder eines Datenverlusts verringern.	redshift-require-tls-ssl	Stellen Sie sicher, dass Ihre Amazon-Redshift-Cluster eine TLS/SSL-Verschlüsselung erfordern, um eine Verbindung zu SQL-Clients herzustellen. Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SEC-9	Wie werden Ihre Daten während der Übertragung geschützt? Schützen Sie Ihre Daten während der Übertragung, indem Sie mehrere Kontrollen implementieren und so das Risiko eines unbefugten Zugriffs oder eines Datenverlusts verringern.	s3- bucket-ssl-requests-only	Um Daten während der Übertragung zu schützen, stellen Sie sicher, dass Ihre Amazon Simple Storage Service (Amazon S3)-Buckets Anfragen zur Verwendung von Secure Socket Layer (SSL)-Buckets erfordern. Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.
SEC-9	Wie werden Ihre Daten während der Übertragung geschützt? Schützen Sie Ihre Daten während der Übertragung, indem Sie mehrere Kontrollen implementieren und so das Risiko eines unbefugten Zugriffs oder eines Datenverlusts verringern.	elb-tls-https-listeners-nur	Stellen Sie sicher, dass Ihre Elastic Load Balancer (ELBs) mit SSL- oder HTTPS-Listenern konfiguriert sind. Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SEC-9	Wie werden Ihre Daten während der Übertragung geschützt? Schützen Sie Ihre Daten während der Übertragung, indem Sie mehrere Kontrollen implementieren und so das Risiko eines unbefugten Zugriffs oder eines Datenverlusts verringern.	vpc-flow-logs-enabled	VPC-Flow-Protokolle erfassen detaillierte Informationsdatensätze über den IP-Datenverkehr, der zu und von Netzwerkschnittstellen in Ihrer Amazon Virtual Private Cloud (Amazon VPC) fließt. Standardmäßig enthalten Flow-Protokolldatensätze Werte für die verschiedenen Komponenten des IP-Flows, einschließlich Quelle, Ziel und Protokoll.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SEC-9	Wie werden Ihre Daten während der Übertragung geschützt? Schützen Sie Ihre Daten während der Übertragung, indem Sie mehrere Kontrollen implementieren und so das Risiko eines unbefugten Zugriffs oder eines Datenverlusts verringern.	guardduty-enabled-centralized	Amazon GuardDuty kann mithilfe von Threat Intelligence Feeds helfen, potenzielle Cybersicherheitsereignisse zu überwachen und zu erkennen. Dazu gehören Listen mit bösartigen IPs und maschinellen Lernmethoden zur Identifizierung unerwarteter, nicht autorisierter und bösartiger Aktivitäten in Ihrer AWS Cloud-Umgebung.

Vorlage

Die Vorlage ist verfügbar unter GitHub: Operational Best Practices for AWS Well-Architected Security Pillar.

Bewährte Methoden für die Ausführung von BCP und DR

Dieses Konformitätspaket enthält AWS Config Regeln, die auf BCP und DR basieren. AWS Eine Liste aller verwalteten Regeln, die von unterstützt werden AWS Config, finden Sie unter Liste der AWS Config verwalteten Regeln.

Die Namen und Beschreibungen der erforderlichen Parameter finden Sie im `Parameters` Abschnitt der folgenden Vorlage.

Die Vorlage ist verfügbar unter GitHub: Operationelle Best Practices für BCP und DR.

Bewährte Betriebspraktiken für BNM T RMi

Konformitätspakete bieten ein allgemeines Compliance-Framework, das es Ihnen ermöglicht, mithilfe verwalteter oder benutzerdefinierter AWS Config Regeln und Abhilfemaßnahmen Kontrollen zur Sicherheits-, Betriebs- oder Kostenoptimierung durchzuführen. AWS Config Conformance Packs dienen als Beispielvorlagen nicht dazu, die vollständige Einhaltung eines bestimmten Governance- oder Compliance-Standards sicherzustellen. Sie sind dafür verantwortlich, selbst zu beurteilen, ob Ihre Nutzung der Services den geltenden gesetzlichen und behördlichen Anforderungen entspricht.

Im Folgenden finden Sie ein Beispiel für eine Zuordnung zwischen den Regeln Risk Management in Technology (RMiT) und AWS Managed Config der Bank Negara Malaysia (BNM). Jede Config-Regel gilt für eine bestimmte AWS Ressource und bezieht sich auf eine oder mehrere BNM RMi T-Steuerelemente. Ein BNM RMi T-Steuerelement kann mit mehreren Config-Regeln verknüpft werden. In der folgenden Tabelle finden Sie weitere Informationen und Anleitungen zu diesen Zuordnungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.18	Ein Finanzinstitut muss die gebotene Sorgfalt walten lassen und die kryptogra fischen Kontrollen im Zusammenhang mit der verwendet en Technologie bewerten, um die Vertraulichkeit, Integrität, Authentif izierung, Autorisie rung und Nichtabst reitbarkeit von Informationen zu schützen. Generiert ein Finanzinstitut keine eigenen	alb-http-to-https-Weiterleitungsprüfung	Um Daten während der Übertragung zu schützen, stellen Sie sicher, dass Ihr Application Load Balancer unverschl üsselte HTTP-Anfr agen automatisch an HTTPS umleitet. Da sensible Daten vorhanden sein können, sollten Sie die Verschlüsselung bei der Übertragung aktivieren, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	Verschlüsselungsschlüssel, ergreift es geeignete Maßnahmen, um sicherzustellen, dass robuste Kontrollen und Verfahren für die Verwaltung der Verschlüsselungsschlüssel vorhanden sind. Wird dabei auf Bewertungen Dritter zurückgegriffen, so prüft das Finanzinstitut, ob ein solches Vertrauen mit der Risikobereitschaft und Risikobereitschaft des Finanzinstituts vereinbar ist. Ein Finanzinstitut muss außerdem die Systemressourcen, die zur Unterstützung der kryptografischen Kontrollen erforderlich sind, und das Risiko einer verringerten Sichtbarkeit verschlüsselter Daten im Netzwerkverkehr gebührend berücksichtigen.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.18	Ein Finanzinstitut muss die gebotene Sorgfalt walten lassen und die kryptogra fischen Kontrollen im Zusammenhang mit der verwendet en Technologie bewerten, um die Vertraulichkeit, Integrität, Authentif izierung, Autorisie rung und Nichtabst reitbarkeit von Informationen zu schützen. Generiert ein Finanzinstitut keine eigenen Verschlüsselungssc hlüssel, ergreift es geeignete Maßnahmen, um sicherzustellen, dass robuste Kontrollen und Verfahren für die Verwaltung der Verschlüsselungssc hlüssel vorhanden sind. Wird dabei auf Bewertungen Dritter zurückgegriffen, so prüft das Finanzins titut, ob ein solches	api-gw-cache-enabl ed-und verschlüsselt	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass die Verschlüsselung für den Cache Ihrer API-Gateway-Stufe aktiviert ist. Da für die API-Methode sensible Daten erfasst werden können, sollten Sie die Verschlüs selung von Daten im Ruhezustand aktiviere n, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	Vertrauen mit der Risikobereitschaft und Risikobereitschaft des Finanzins tituts vereinbar ist. Ein Finanzinstitut muss außerdem die Systemressourcen, die zur Unterstüt zung der kryptogra fischen Kontrolle n erforderlich sind, und das Risiko einer verringerten Sichtbark eit verschlüsselter Daten im Netzwerkv erkehr gebührend berücksichtigen.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.18	Ein Finanzinstitut muss die gebotene Sorgfalt walten lassen und die kryptogra fischen Kontrollen im Zusammenhang mit der verwendet en Technologie bewerten, um die Vertraulichkeit, Integrität, Authentif izierung, Autorisie rung und Nichtabst reitbarkeit von Informationen zu schützen. Generiert ein Finanzinstitut keine eigenen Verschlüsselungssc hlüssel, ergreift es geeignete Maßnahmen, um sicherzustellen, dass robuste Kontrollen und Verfahren für die Verwaltung der Verschlüsselungssc hlüssel vorhanden sind. Wird dabei auf Bewertungen Dritter zurückgegriffen, so prüft das Finanzins titut, ob ein solches	api-gw-ssl-enabled	Stellen Sie sicher, dass die REST-API-Stufen von Amazon API Gateway mit SSL-Zertifikaten konfiguri ert sind, damit Backend-Systeme überprüfen können, ob Anforderungen von API Gateway stammen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	Vertrauen mit der Risikobereitschaft und Risikobereitschaft des Finanzins tituts vereinbar ist. Ein Finanzinstitut muss außerdem die Systemressourcen, die zur Unterstüt zung der kryptogra fischen Kontrolle n erforderlich sind, und das Risiko einer verringerten Sichtbark eit verschlüsselter Daten im Netzwerkv erkehr gebührend berücksichtigen.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.18	Ein Finanzinstitut muss die gebotene Sorgfalt walten lassen und die kryptogra fischen Kontrollen im Zusammenhang mit der verwendet en Technologie bewerten, um die Vertraulichkeit, Integrität, Authentif izierung, Autorisie rung und Nichtabst reitbarkeit von Informationen zu schützen. Generiert ein Finanzinstitut keine eigenen Verschlüsselungssc hlüssel, ergreift es geeignete Maßnahmen, um sicherzustellen, dass robuste Kontrollen und Verfahren für die Verwaltung der Verschlüsselungssc hlüssel vorhanden sind. Wird dabei auf Bewertungen Dritter zurückgegriffen, so prüft das Finanzins titut, ob ein solches	backup-recovery-po int-encrypted	Stellen Sie sicher, dass die Verschlüs selung für Ihre AWS Backup-Wiederherst ellungspunkte aktiviert ist. Da sensible Daten auch im Ruhezusta nd vorhanden sein können, sollten Sie die Verschlüsselung im Ruhezustand aktivieren, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	Vertrauen mit der Risikobereitschaft und Risikobereitschaft des Finanzins tituts vereinbar ist. Ein Finanzinstitut muss außerdem die Systemressourcen, die zur Unterstüt zung der kryptogra fischen Kontrolle n erforderlich sind, und das Risiko einer verringerten Sichtbark eit verschlüsselter Daten im Netzwerkv erkehr gebührend berücksichtigen.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.18	Ein Finanzinstitut muss die gebotene Sorgfalt walten lassen und die kryptogra fischen Kontrollen im Zusammenhang mit der verwendet en Technologie bewerten, um die Vertraulichkeit, Integrität, Authentif izierung, Autorisie rung und Nichtabst reitbarkeit von Informationen zu schützen. Generiert ein Finanzinstitut keine eigenen Verschlüsselungssc hlüssel, ergreift es geeignete Maßnahmen, um sicherzustellen, dass robuste Kontrollen und Verfahren für die Verwaltung der Verschlüsselungssc hlüssel vorhanden sind. Wird dabei auf Bewertungen Dritter zurückgegriffen, so prüft das Finanzins titut, ob ein solches	cloudtrail-security-trail-enabled	Diese Regel trägt dazu bei, die Verwendung der AWS empfohlenen bewährten Sicherhei tsmethoden für sicherzustellen AWS CloudTrai l, indem geprüft wird, ob mehrere Einstellungen aktiviert sind. Dazu gehören die Verwendun g von Protokoll verschlüsselung, Protokollvalidieru ng und Aktivierung AWS CloudTrail in mehreren Regionen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	Vertrauen mit der Risikobereitschaft und Risikobereitschaft des Finanzins tituts vereinbar ist. Ein Finanzinstitut muss außerdem die Systemressourcen, die zur Unterstüt zung der kryptogra fischen Kontrolle n erforderlich sind, und das Risiko einer verringerten Sichtbark eit verschlüsselter Daten im Netzwerkv erkehr gebührend berücksichtigen.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.18	Ein Finanzinstitut muss die gebotene Sorgfalt walten lassen und die kryptogra fischen Kontrollen im Zusammenhang mit der verwendet en Technologie bewerten, um die Vertraulichkeit, Integrität, Authentif izierung, Autorisie rung und Nichtabst reitbarkeit von Informationen zu schützen. Generiert ein Finanzinstitut keine eigenen Verschlüsselungssc hlüssel, ergreift es geeignete Maßnahmen, um sicherzustellen, dass robuste Kontrollen und Verfahren für die Verwaltung der Verschlüsselungssc hlüssel vorhanden sind. Wird dabei auf Bewertungen Dritter zurückgegriffen, so prüft das Finanzins titut, ob ein solches	cloudwatch-log-group-encrypted	Um sensible Daten im Speicher zu schützen, stellen Sie sicher, dass die Verschlüs selung für Ihre Amazon CloudWatch Log Groups aktiviert ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	Vertrauen mit der Risikobereitschaft und Risikobereitschaft des Finanzins tituts vereinbar ist. Ein Finanzinstitut muss außerdem die Systemressourcen, die zur Unterstüt zung der kryptogra fischen Kontrolle n erforderlich sind, und das Risiko einer verringerten Sichtbark eit verschlüsselter Daten im Netzwerkv erkehr gebührend berücksichtigen.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.18	Ein Finanzinstitut muss die gebotene Sorgfalt walten lassen und die kryptogra fischen Kontrollen im Zusammenhang mit der verwendet en Technologie bewerten, um die Vertraulichkeit, Integrität, Authentif izierung, Autorisie rung und Nichtabst reitbarkeit von Informationen zu schützen. Generiert ein Finanzinstitut keine eigenen Verschlüsselungssc hlüssel, ergreift es geeignete Maßnahmen, um sicherzustellen, dass robuste Kontrollen und Verfahren für die Verwaltung der Verschlüsselungssc hlüssel vorhanden sind. Wird dabei auf Bewertungen Dritter zurückgegriffen, so prüft das Finanzins titut, ob ein solches	cmk-backing-key-ro tation-aktiviert	Aktivieren Sie die Schlüsselrotation, um sicherzustellen, dass Schlüssel rotiert werden, nachdem sie das Ende ihrer Krypto-Periode erreicht haben.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	Vertrauen mit der Risikobereitschaft und Risikobereitschaft des Finanzins tituts vereinbar ist. Ein Finanzinstitut muss außerdem die Systemressourcen, die zur Unterstüt zung der kryptogra fischen Kontrolle n erforderlich sind, und das Risiko einer verringerten Sichtbark eit verschlüsselter Daten im Netzwerkv erkehr gebührend berücksichtigen.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.18	Ein Finanzinstitut muss die gebotene Sorgfalt walten lassen und die kryptogra fischen Kontrollen im Zusammenhang mit der verwendet en Technologie bewerten, um die Vertraulichkeit, Integrität, Authentif izierung, Autorisie rung und Nichtabst reitbarkeit von Informationen zu schützen. Generiert ein Finanzinstitut keine eigenen Verschlüsselungssc hlüssel, ergreift es geeignete Maßnahmen, um sicherzustellen, dass robuste Kontrollen und Verfahren für die Verwaltung der Verschlüsselungssc hlüssel vorhanden sind. Wird dabei auf Bewertungen Dritter zurückgegriffen, so prüft das Finanzins titut, ob ein solches	dynamodb-table-enc rypted-kms	Stellen Sie sicher, dass die Verschlüs selung für Ihre Amazon-DynamoDB-Tabellen aktiviert ist. Um eventuell vorhandene sensible Daten im Ruhezusta nd in diesen Tabellen zu schützen, müssen Sie die Verschlüs selung von Daten im Ruhezustand aktiviere n. Standardmäßig werden DynamoDB-Tabellen mit einem AWS eigenen Kundenhauptschlüss el (CMK) verschlüs selt.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	Vertrauen mit der Risikobereitschaft und Risikobereitschaft des Finanzins tituts vereinbar ist. Ein Finanzinstitut muss außerdem die Systemressourcen, die zur Unterstüt zung der kryptogra fischen Kontrolle n erforderlich sind, und das Risiko einer verringerten Sichtbark eit verschlüsselter Daten im Netzwerkv erkehr gebührend berücksichtigen.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.18	Ein Finanzinstitut muss die gebotene Sorgfalt walten lassen und die kryptogra fischen Kontrollen im Zusammenhang mit der verwendet en Technologie bewerten, um die Vertraulichkeit, Integrität, Authentif izierung, Autorisie rung und Nichtabst reitbarkeit von Informationen zu schützen. Generiert ein Finanzinstitut keine eigenen Verschlüsselungssc hlüssel, ergreift es geeignete Maßnahmen, um sicherzustellen, dass robuste Kontrollen und Verfahren für die Verwaltung der Verschlüsselungssc hlüssel vorhanden sind. Wird dabei auf Bewertungen Dritter zurückgegriffen, so prüft das Finanzins titut, ob ein solches	ec2- ebs-encryption-by-default	Zum Schutz von Daten im Ruhezusta nd müssen Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon Elastic Block Store (Amazon EBS)-Volu mes aktiviert ist. Aktivieren Sie die Verschlüsselung von Daten im Ruhezusta nd, um eventuell in diesen Volumes vorhandene sensible Daten im Ruhezusta nd zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	Vertrauen mit der Risikobereitschaft und Risikobereitschaft des Finanzins tituts vereinbar ist. Ein Finanzinstitut muss außerdem die Systemressourcen, die zur Unterstüt zung der kryptogra fischen Kontrolle n erforderlich sind, und das Risiko einer verringerten Sichtbark eit verschlüsselter Daten im Netzwerkv erkehr gebührend berücksichtigen.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10,18	Ein Finanzinstitut muss die gebotene Sorgfalt walten lassen und die kryptogra fischen Kontrollen im Zusammenhang mit der verwendet en Technologie bewerten, um die Vertraulichkeit, Integrität, Authentif izierung, Autorisie rung und Nichtabst reitbarkeit von Informationen zu schützen. Generiert ein Finanzinstitut keine eigenen Verschlüsselungssc hlüssel, ergreift es geeignete Maßnahmen, um sicherzustellen, dass robuste Kontrollen und Verfahren für die Verwaltung der Verschlüsselungssc hlüssel vorhanden sind. Wird dabei auf Bewertungen Dritter zurückgegriffen, so prüft das Finanzins titut, ob ein solches	efs-encrypted-check	Aktivieren Sie die Verschlüsselung für Ihr Amazon Elastic File System (EFS), um eventuell vorhandene sensible Daten sowie Daten im Ruhezustand zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	Vertrauen mit der Risikobereitschaft und Risikobereitschaft des Finanzins tituts vereinbar ist. Ein Finanzinstitut muss außerdem die Systemressourcen, die zur Unterstüt zung der kryptogra fischen Kontrolle n erforderlich sind, und das Risiko einer verringerten Sichtbark eit verschlüsselter Daten im Netzwerkv erkehr gebührend berücksichtigen.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.18	Ein Finanzinstitut muss die gebotene Sorgfalt walten lassen und die kryptogra fischen Kontrollen im Zusammenhang mit der verwendet en Technologie bewerten, um die Vertraulichkeit, Integrität, Authentif izierung, Autorisie rung und Nichtabst reitbarkeit von Informationen zu schützen. Generiert ein Finanzinstitut keine eigenen Verschlüsselungssc hlüssel, ergreift es geeignete Maßnahmen, um sicherzustellen, dass robuste Kontrollen und Verfahren für die Verwaltung der Verschlüsselungssc hlüssel vorhanden sind. Wird dabei auf Bewertungen Dritter zurückgegriffen, so prüft das Finanzins titut, ob ein solches	elbv-2 acm-certificate-required	Zum Schutz von eventuell vorhanden en sensiblen Daten sowie von Daten während der Übertragung muss die Verschlüsselung für Ihr Elastic Load Balancing aktiviert sein. Verwenden Sie AWS Certificate Manager, um öffentlic he und private SSL/ TLS-Zertifikate mit AWS Diensten und internen Ressource n zu verwalten, bereitzustellen und bereitzustellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	Vertrauen mit der Risikobereitschaft und Risikobereitschaft des Finanzins tituts vereinbar ist. Ein Finanzinstitut muss außerdem die Systemressourcen, die zur Unterstüt zung der kryptogra fischen Kontrolle n erforderlich sind, und das Risiko einer verringerten Sichtbark eit verschlüsselter Daten im Netzwerkv erkehr gebührend berücksichtigen.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.18	Ein Finanzinstitut muss die gebotene Sorgfalt walten lassen und die kryptogra fischen Kontrollen im Zusammenhang mit der verwendet en Technologie bewerten, um die Vertraulichkeit, Integrität, Authentif izierung, Autorisie rung und Nichtabst reitbarkeit von Informationen zu schützen. Generiert ein Finanzinstitut keine eigenen Verschlüsselungssc hlüssel, ergreift es geeignete Maßnahmen, um sicherzustellen, dass robuste Kontrollen und Verfahren für die Verwaltung der Verschlüsselungssc hlüssel vorhanden sind. Wird dabei auf Bewertungen Dritter zurückgegriffen, so prüft das Finanzins titut, ob ein solches	encrypted-volumes	Aktivieren Sie die Verschlüsselung für Ihre Volumes von Amazon Elastic Block Store (Amazon EBS), um eventuell vorhandene sensible Daten sowie Daten im Ruhezustand zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	Vertrauen mit der Risikobereitschaft und Risikobereitschaft des Finanzins tituts vereinbar ist. Ein Finanzinstitut muss außerdem die Systemressourcen, die zur Unterstüt zung der kryptogra fischen Kontrolle n erforderlich sind, und das Risiko einer verringerten Sichtbark eit verschlüsselter Daten im Netzwerkv erkehr gebührend berücksichtigen.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.18	Ein Finanzinstitut muss die gebotene Sorgfalt walten lassen und die kryptogra fischen Kontrollen im Zusammenhang mit der verwendet en Technologie bewerten, um die Vertraulichkeit, Integrität, Authentif izierung, Autorisie rung und Nichtabst reitbarkeit von Informationen zu schützen. Generiert ein Finanzinstitut keine eigenen Verschlüsselungssc hlüssel, ergreift es geeignete Maßnahmen, um sicherzustellen, dass robuste Kontrollen und Verfahren für die Verwaltung der Verschlüsselungssc hlüssel vorhanden sind. Wird dabei auf Bewertungen Dritter zurückgegriffen, so prüft das Finanzins titut, ob ein solches	kms-cmk-not-schedu led-zum Löschen	Um Daten im Ruhezustand zu schützen, sollten Sie sicherstellen, dass die für den Kunden erforderl ichen Masterschlüssel (CMKs) nicht für das Löschen im AWS Key Management Service (AWS KMS) vorgesehen sind. Da Schlüssel manchmal gelöscht werden müssen, können Sie mit dieser Regel alle zu löschenden Schlüssel überprüfe n, falls ein Schlüssel versehentlich zur Löschung vorgemerkt wurde.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	Vertrauen mit der Risikobereitschaft und Risikobereitschaft des Finanzins tituts vereinbar ist. Ein Finanzinstitut muss außerdem die Systemressourcen, die zur Unterstüt zung der kryptogra fischen Kontrolle n erforderlich sind, und das Risiko einer verringerten Sichtbark eit verschlüsselter Daten im Netzwerkv erkehr gebührend berücksichtigen.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.18	Ein Finanzinstitut muss die gebotene Sorgfalt walten lassen und die kryptogra fischen Kontrollen im Zusammenhang mit der verwendet en Technologie bewerten, um die Vertraulichkeit, Integrität, Authentif izierung, Autorisie rung und Nichtabst reitbarkeit von Informationen zu schützen. Generiert ein Finanzinstitut keine eigenen Verschlüsselungssc hlüssel, ergreift es geeignete Maßnahmen, um sicherzustellen, dass robuste Kontrollen und Verfahren für die Verwaltung der Verschlüsselungssc hlüssel vorhanden sind. Wird dabei auf Bewertungen Dritter zurückgegriffen, so prüft das Finanzins titut, ob ein solches	opensearch-encrypt ed-at-rest	Da sensible Daten vorhanden sein können und um Daten im Ruhezustand zu schützen, sollten Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon OpenSearch Service-Domains aktiviert ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	Vertrauen mit der Risikobereitschaft und Risikobereitschaft des Finanzins tituts vereinbar ist. Ein Finanzinstitut muss außerdem die Systemressourcen, die zur Unterstüt zung der kryptogra fischen Kontrolle n erforderlich sind, und das Risiko einer verringerten Sichtbark eit verschlüsselter Daten im Netzwerkv erkehr gebührend berücksichtigen.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.18	Ein Finanzinstitut muss die gebotene Sorgfalt walten lassen und die kryptogra fischen Kontrollen im Zusammenhang mit der verwendet en Technologie bewerten, um die Vertraulichkeit, Integrität, Authentif izierung, Autorisie rung und Nichtabst reitbarkeit von Informationen zu schützen. Generiert ein Finanzinstitut keine eigenen Verschlüsselungssc hlüssel, ergreift es geeignete Maßnahmen, um sicherzustellen, dass robuste Kontrollen und Verfahren für die Verwaltung der Verschlüsselungssc hlüssel vorhanden sind. Wird dabei auf Bewertungen Dritter zurückgegriffen, so prüft das Finanzins titut, ob ein solches	opensearch-https-r equired	Da sensible Daten existieren können und um Daten während der Übertragung zu schützen, sollten Sie sicherstellen, dass HTTPS für Verbindun gen zu Ihren Amazon OpenSearch Service-Domains aktiviert ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	Vertrauen mit der Risikobereitschaft und Risikobereitschaft des Finanzins tituts vereinbar ist. Ein Finanzinstitut muss außerdem die Systemressourcen, die zur Unterstüt zung der kryptogra fischen Kontrolle n erforderlich sind, und das Risiko einer verringerten Sichtbark eit verschlüsselter Daten im Netzwerkv erkehr gebührend berücksichtigen.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.18	Ein Finanzinstitut muss die gebotene Sorgfalt walten lassen und die kryptogra fischen Kontrollen im Zusammenhang mit der verwendet en Technologie bewerten, um die Vertraulichkeit, Integrität, Authentif izierung, Autorisie rung und Nichtabst reitbarkeit von Informationen zu schützen. Generiert ein Finanzinstitut keine eigenen Verschlüsselungssc hlüssel, ergreift es geeignete Maßnahmen, um sicherzustellen, dass robuste Kontrollen und Verfahren für die Verwaltung der Verschlüsselungssc hlüssel vorhanden sind. Wird dabei auf Bewertungen Dritter zurückgegriffen, so prüft das Finanzins titut, ob ein solches	opensearch-node-to-node-Verschlüssel ungsprüfung	Stellen Sie sicher, dass die node-to-node Verschlüs selung für Amazon OpenSearch Service aktiviert ist. Node-to-nodeVerschlüsselung ermöglicht die TLS 1.2-Verschlüsselun g für die gesamte Kommunikation innerhalb der Amazon Virtual Private Cloud (Amazon VPC). Um eventuell vorhanden e sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	Vertrauen mit der Risikobereitschaft und Risikobereitschaft des Finanzins tituts vereinbar ist. Ein Finanzinstitut muss außerdem die Systemressourcen, die zur Unterstüt zung der kryptogra fischen Kontrolle n erforderlich sind, und das Risiko einer verringerten Sichtbark eit verschlüsselter Daten im Netzwerkv erkehr gebührend berücksichtigen.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.18	Ein Finanzinstitut muss die gebotene Sorgfalt walten lassen und die kryptogra fischen Kontrollen im Zusammenhang mit der verwendet en Technologie bewerten, um die Vertraulichkeit, Integrität, Authentif izierung, Autorisie rung und Nichtabst reitbarkeit von Informationen zu schützen. Generiert ein Finanzinstitut keine eigenen Verschlüsselungssc hlüssel, ergreift es geeignete Maßnahmen, um sicherzustellen, dass robuste Kontrollen und Verfahren für die Verwaltung der Verschlüsselungssc hlüssel vorhanden sind. Wird dabei auf Bewertungen Dritter zurückgegriffen, so prüft das Finanzins titut, ob ein solches	rds-snapshot-encry pted	Stellen Sie sicher, dass die Verschlüs selung für Ihre Amazon Relationa l Database Service (Amazon RDS)-Snap shots aktiviert ist. Da sensible Daten auch im Ruhezusta nd vorhanden sein können, sollten Sie die Verschlüs selung von Daten im Ruhezustand aktiviere n, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	Vertrauen mit der Risikobereitschaft und Risikobereitschaft des Finanzins tituts vereinbar ist. Ein Finanzinstitut muss außerdem die Systemressourcen, die zur Unterstüt zung der kryptogra fischen Kontrolle n erforderlich sind, und das Risiko einer verringerten Sichtbark eit verschlüsselter Daten im Netzwerkv erkehr gebührend berücksichtigen.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.18	Ein Finanzinstitut muss die gebotene Sorgfalt walten lassen und die kryptogra fischen Kontrollen im Zusammenhang mit der verwendet en Technologie bewerten, um die Vertraulichkeit, Integrität, Authentif izierung, Autorisie rung und Nichtabst reitbarkeit von Informationen zu schützen. Generiert ein Finanzinstitut keine eigenen Verschlüsselungssc hlüssel, ergreift es geeignete Maßnahmen, um sicherzustellen, dass robuste Kontrollen und Verfahren für die Verwaltung der Verschlüsselungssc hlüssel vorhanden sind. Wird dabei auf Bewertungen Dritter zurückgegriffen, so prüft das Finanzins titut, ob ein solches	rds-storage-encrypted	Zum Schutz von Daten im Ruhezusta nd müssen Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon Relational Database Service (Amazon RDS)-Instances aktiviert ist. Da sensible Daten in Amazon-RDS-Instances gespeiche rt werden können, sollten Sie die Verschlüsselung von Daten im Ruhezusta nd aktivieren, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	Vertrauen mit der Risikobereitschaft und Risikobereitschaft des Finanzins tituts vereinbar ist. Ein Finanzinstitut muss außerdem die Systemressourcen, die zur Unterstüt zung der kryptogra fischen Kontrolle n erforderlich sind, und das Risiko einer verringerten Sichtbark eit verschlüsselter Daten im Netzwerkv erkehr gebührend berücksichtigen.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.18	Ein Finanzinstitut muss die gebotene Sorgfalt walten lassen und die kryptogra fischen Kontrollen im Zusammenhang mit der verwendet en Technologie bewerten, um die Vertraulichkeit, Integrität, Authentif izierung, Autorisie rung und Nichtabst reitbarkeit von Informationen zu schützen. Generiert ein Finanzinstitut keine eigenen Verschlüsselungssc hlüssel, ergreift es geeignete Maßnahmen, um sicherzustellen, dass robuste Kontrollen und Verfahren für die Verwaltung der Verschlüsselungssc hlüssel vorhanden sind. Wird dabei auf Bewertungen Dritter zurückgegriffen, so prüft das Finanzins titut, ob ein solches	redshift-cluster-c onfiguration-check	Um Daten im Ruhezustand zu schützen, muss die Verschlüsselung für Ihre Amazon-Re dshift-Cluster aktiviert sein. Sie müssen auch sicherstellen, dass die erforderl ichen Konfigurationen auf Amazon-Redshift-Clustern bereitges tellt werden. Die Prüfungsprotokolli erung muss aktiviert sein, um Informati onen zu Verbindun gen und Benutzera ktivitäten in der Datenbank bereitzus tellen. Diese Regel erfordert, dass ein Wert für clusterDb Encrypted (Config Default: TRUE) und LoggingEnabled (Config Default: TRUE) gesetzt ist. Die tatsächlichen Werte müssen den Richtlini en Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	Vertrauen mit der Risikobereitschaft und Risikobereitschaft des Finanzins tituts vereinbar ist. Ein Finanzinstitut muss außerdem die Systemressourcen, die zur Unterstüt zung der kryptogra fischen Kontrolle n erforderlich sind, und das Risiko einer verringerten Sichtbark eit verschlüsselter Daten im Netzwerkv erkehr gebührend berücksichtigen.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.18	Ein Finanzinstitut muss die gebotene Sorgfalt walten lassen und die kryptogra fischen Kontrollen im Zusammenhang mit der verwendet en Technologie bewerten, um die Vertraulichkeit, Integrität, Authentif izierung, Autorisie rung und Nichtabst reitbarkeit von Informationen zu schützen. Generiert ein Finanzinstitut keine eigenen Verschlüsselungssc hlüssel, ergreift es geeignete Maßnahmen, um sicherzustellen, dass robuste Kontrollen und Verfahren für die Verwaltung der Verschlüsselungssc hlüssel vorhanden sind. Wird dabei auf Bewertungen Dritter zurückgegriffen, so prüft das Finanzins titut, ob ein solches	redshift-cluster-kms-enabled	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass die Verschlüs selung mit AWS Key Management Service (AWS KMS) für Ihren Amazon Redshift Redshift-Cluster aktiviert ist. Um eventuell vorhanden e sensible Daten im Ruhezustand in Redshift-Clustern zu schützen, muss die Verschlüsselung von Daten im Ruhezusta nd aktiviert sein.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	Vertrauen mit der Risikobereitschaft und Risikobereitschaft des Finanzins tituts vereinbar ist. Ein Finanzinstitut muss außerdem die Systemressourcen, die zur Unterstüt zung der kryptogra fischen Kontrolle n erforderlich sind, und das Risiko einer verringerten Sichtbark eit verschlüsselter Daten im Netzwerkv erkehr gebührend berücksichtigen.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.18	Ein Finanzinstitut muss die gebotene Sorgfalt walten lassen und die kryptogra fischen Kontrollen im Zusammenhang mit der verwendet en Technologie bewerten, um die Vertraulichkeit, Integrität, Authentif izierung, Autorisie rung und Nichtabst reitbarkeit von Informationen zu schützen. Generiert ein Finanzinstitut keine eigenen Verschlüsselungssc hlüssel, ergreift es geeignete Maßnahmen, um sicherzustellen, dass robuste Kontrollen und Verfahren für die Verwaltung der Verschlüsselungssc hlüssel vorhanden sind. Wird dabei auf Bewertungen Dritter zurückgegriffen, so prüft das Finanzins titut, ob ein solches	redshift-require-tls-ssl	Stellen Sie sicher, dass Ihre Amazon-Redshift-Cluster eine TLS/SSL-Verschlüss elung erfordern, um eine Verbindung zu SQL-Clients herzustel len. Da sensible Daten vorhanden sein können, sollten Sie die Verschlüsselung bei der Übertragung aktivieren, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	Vertrauen mit der Risikobereitschaft und Risikobereitschaft des Finanzins tituts vereinbar ist. Ein Finanzinstitut muss außerdem die Systemressourcen, die zur Unterstüt zung der kryptogra fischen Kontrolle n erforderlich sind, und das Risiko einer verringerten Sichtbark eit verschlüsselter Daten im Netzwerkv erkehr gebührend berücksichtigen.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.18	Ein Finanzinstitut muss die gebotene Sorgfalt walten lassen und die kryptogra fischen Kontrollen im Zusammenhang mit der verwendet en Technologie bewerten, um die Vertraulichkeit, Integrität, Authentif izierung, Autorisie rung und Nichtabst reitbarkeit von Informationen zu schützen. Generiert ein Finanzinstitut keine eigenen Verschlüsselungssc hlüssel, ergreift es geeignete Maßnahmen, um sicherzustellen, dass robuste Kontrollen und Verfahren für die Verwaltung der Verschlüsselungssc hlüssel vorhanden sind. Wird dabei auf Bewertungen Dritter zurückgegriffen, so prüft das Finanzins titut, ob ein solches	s3-aktiviert bucket-se rver-side-encryption	Zum Schutz von Daten im Ruhezusta nd müssen Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon Simple Storage Service (Amazon S3)-Bucke ts aktiviert ist. Da sensible Daten in Amazon-S3-Buckets gespeichert werden können, sollten Sie die Verschlüsselung aktivieren, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	Vertrauen mit der Risikobereitschaft und Risikobereitschaft des Finanzins tituts vereinbar ist. Ein Finanzinstitut muss außerdem die Systemressourcen, die zur Unterstüt zung der kryptogra fischen Kontrolle n erforderlich sind, und das Risiko einer verringerten Sichtbark eit verschlüsselter Daten im Netzwerkv erkehr gebührend berücksichtigen.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.18	Ein Finanzinstitut muss die gebotene Sorgfalt walten lassen und die kryptogra fischen Kontrollen im Zusammenhang mit der verwendet en Technologie bewerten, um die Vertraulichkeit, Integrität, Authentif izierung, Autorisie rung und Nichtabst reitbarkeit von Informationen zu schützen. Generiert ein Finanzinstitut keine eigenen Verschlüsselungssc hlüssel, ergreift es geeignete Maßnahmen, um sicherzustellen, dass robuste Kontrollen und Verfahren für die Verwaltung der Verschlüsselungssc hlüssel vorhanden sind. Wird dabei auf Bewertungen Dritter zurückgegriffen, so prüft das Finanzins titut, ob ein solches	s3- bucket-ssl-request s-only	Um Daten während der Übertragung zu schützen, stellen Sie sicher, dass Ihre Amazon Simple Storage Service (Amazon S3)-Bucke ts Anfragen zur Verwendung von Secure Socket Layer (SSL)-Buckets erfordern. Da sensible Daten vorhanden sein können, sollten Sie die Verschlüsselung bei der Übertragung aktivieren, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	Vertrauen mit der Risikobereitschaft und Risikobereitschaft des Finanzins tituts vereinbar ist. Ein Finanzinstitut muss außerdem die Systemressourcen, die zur Unterstüt zung der kryptogra fischen Kontrolle n erforderlich sind, und das Risiko einer verringerten Sichtbark eit verschlüsselter Daten im Netzwerkv erkehr gebührend berücksichtigen.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10,18	Ein Finanzinstitut muss die gebotene Sorgfalt walten lassen und die kryptogra fischen Kontrollen im Zusammenhang mit der verwendet en Technologie bewerten, um die Vertraulichkeit, Integrität, Authentif izierung, Autorisie rung und Nichtabst reitbarkeit von Informationen zu schützen. Generiert ein Finanzinstitut keine eigenen Verschlüsselungssc hlüssel, ergreift es geeignete Maßnahmen, um sicherzustellen, dass robuste Kontrollen und Verfahren für die Verwaltung der Verschlüsselungssc hlüssel vorhanden sind. Wird dabei auf Bewertungen Dritter zurückgegriffen, so prüft das Finanzins titut, ob ein solches	s3- default-encryption -kms	Stellen Sie sicher, dass die Verschlüs selung für Ihre Amazon Simple Storage Service (Amazon S3)-Bucke ts aktiviert ist. Da sensible Daten in einem Amazon-S3 -Bucket gespeiche rt werden können, sollten Sie die Verschlüsselung im Ruhezustand aktiviere n, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	Vertrauen mit der Risikobereitschaft und Risikobereitschaft des Finanzins tituts vereinbar ist. Ein Finanzinstitut muss außerdem die Systemressourcen, die zur Unterstüt zung der kryptogra fischen Kontrolle n erforderlich sind, und das Risiko einer verringerten Sichtbark eit verschlüsselter Daten im Netzwerkv erkehr gebührend berücksichtigen.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10,18	Ein Finanzinstitut muss die gebotene Sorgfalt walten lassen und die kryptogra fischen Kontrollen im Zusammenhang mit der verwendet en Technologie bewerten, um die Vertraulichkeit, Integrität, Authentif izierung, Autorisie rung und Nichtabst reitbarkeit von Informationen zu schützen. Generiert ein Finanzinstitut keine eigenen Verschlüsselungssc hlüssel, ergreift es geeignete Maßnahmen, um sicherzustellen, dass robuste Kontrollen und Verfahren für die Verwaltung der Verschlüsselungssc hlüssel vorhanden sind. Wird dabei auf Bewertungen Dritter zurückgegriffen, so prüft das Finanzins titut, ob ein solches	sagemaker-endpoint -configuration-kms- tastenkonfiguriert	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass die Verschlüsselung mit dem AWS Key Management Service (AWS KMS) für Ihren Endpunkt aktiviert ist. SageMaker Da sensible Daten auf dem SageMaker Endgerät gespeiche rt werden können, sollten Sie die Verschlüsselung im Ruhezustand aktiviere n, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	Vertrauen mit der Risikobereitschaft und Risikobereitschaft des Finanzins tituts vereinbar ist. Ein Finanzinstitut muss außerdem die Systemressourcen, die zur Unterstüt zung der kryptogra fischen Kontrolle n erforderlich sind, und das Risiko einer verringerten Sichtbark eit verschlüsselter Daten im Netzwerkv erkehr gebührend berücksichtigen.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.18	Ein Finanzinstitut muss die gebotene Sorgfalt walten lassen und die kryptogra fischen Kontrollen im Zusammenhang mit der verwendet en Technologie bewerten, um die Vertraulichkeit, Integrität, Authentif izierung, Autorisie rung und Nichtabst reitbarkeit von Informationen zu schützen. Generiert ein Finanzinstitut keine eigenen Verschlüsselungssc hlüssel, ergreift es geeignete Maßnahmen, um sicherzustellen, dass robuste Kontrollen und Verfahren für die Verwaltung der Verschlüsselungssc hlüssel vorhanden sind. Wird dabei auf Bewertungen Dritter zurückgegriffen, so prüft das Finanzins titut, ob ein solches	sagemaker-notebook -instance-kms-tast enkonfiguriert	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass die Verschlüsselung mit dem AWS Key Management Service (AWS KMS) für Ihr Notebook aktiviert ist. SageMaker Da vertrauliche Daten im SageMaker Notebook gespeichert werden können, sollten Sie die Verschlüsselung im Ruhezustand aktivieren, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	Vertrauen mit der Risikobereitschaft und Risikobereitschaft des Finanzins tituts vereinbar ist. Ein Finanzinstitut muss außerdem die Systemressourcen, die zur Unterstüt zung der kryptogra fischen Kontrolle n erforderlich sind, und das Risiko einer verringerten Sichtbark eit verschlüsselter Daten im Netzwerkv erkehr gebührend berücksichtigen.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.18	Ein Finanzinstitut muss die gebotene Sorgfalt walten lassen und die kryptogra fischen Kontrollen im Zusammenhang mit der verwendet en Technologie bewerten, um die Vertraulichkeit, Integrität, Authentif izierung, Autorisie rung und Nichtabst reitbarkeit von Informationen zu schützen. Generiert ein Finanzinstitut keine eigenen Verschlüsselungssc hlüssel, ergreift es geeignete Maßnahmen, um sicherzustellen, dass robuste Kontrollen und Verfahren für die Verwaltung der Verschlüsselungssc hlüssel vorhanden sind. Wird dabei auf Bewertungen Dritter zurückgegriffen, so prüft das Finanzins titut, ob ein solches	secretsmanager-usi ng-cmk	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass die Verschlüsselung mit dem AWS Key Management Service (AWS KMS) für AWS Secrets Manager aktiviert ist. Aktiviere n Sie die Verschlüs selung von Daten im Ruhezustand, um eventuell vorhanden e sensible Daten im Ruhezustand im Secrets Manager zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	Vertrauen mit der Risikobereitschaft und Risikobereitschaft des Finanzins tituts vereinbar ist. Ein Finanzinstitut muss außerdem die Systemressourcen, die zur Unterstüt zung der kryptogra fischen Kontrolle n erforderlich sind, und das Risiko einer verringerten Sichtbark eit verschlüsselter Daten im Netzwerkv erkehr gebührend berücksichtigen.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.18	Ein Finanzinstitut muss die gebotene Sorgfalt walten lassen und die kryptogra fischen Kontrollen im Zusammenhang mit der verwendet en Technologie bewerten, um die Vertraulichkeit, Integrität, Authentif izierung, Autorisie rung und Nichtabst reitbarkeit von Informationen zu schützen. Generiert ein Finanzinstitut keine eigenen Verschlüsselungssc hlüssel, ergreift es geeignete Maßnahmen, um sicherzustellen, dass robuste Kontrollen und Verfahren für die Verwaltung der Verschlüsselungssc hlüssel vorhanden sind. Wird dabei auf Bewertungen Dritter zurückgegriffen, so prüft das Finanzins titut, ob ein solches	sns-encrypted-kms	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass Ihre Amazon Simple Notification Service (Amazon SNS) -Themen mit dem AWS Key Management Service (AWS KMS) verschlüsselt werden müssen. Um eventuell vorhandene sensible Daten im Ruhezusta nd in veröffentlichten Nachrichten zu schützen, muss die Verschlüsselung von Daten im Ruhezusta nd aktiviert sein.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	Vertrauen mit der Risikobereitschaft und Risikobereitschaft des Finanzins tituts vereinbar ist. Ein Finanzinstitut muss außerdem die Systemressourcen, die zur Unterstüt zung der kryptogra fischen Kontrolle n erforderlich sind, und das Risiko einer verringerten Sichtbark eit verschlüsselter Daten im Netzwerkv erkehr gebührend berücksichtigen.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.20	Ein Finanzinstitut speichert öffentlic he kryptografische Schlüssel in einem Zertifikat, das von einer Zertifizi erungsstelle je nach Risikostufe ausgestel lt wurde. Solche Kundenzertifikate werden von anerkannt en Zertifizierungsste llen ausgestellt. Das Finanzinstitut muss sicherstellen, dass die Implementierung von Authentifizierungs - und Signaturp rotokollen, die solche Zertifikate verwenden , einem strengen Schutz unterlieg t. Dadurch wird gewährleistet, dass die Verwendung privater kryptogra fischer Schlüssel, die den Benutzerzertifikat en entsprechen, rechtsverbindlich und unwiderlegbar ist. Die erstmalige Ausstellu ng und die anschließ	acm-certificate-ex piration-check	Stellen Sie sicher, dass die Netzwerki ntegrität geschützt ist, indem Sie sicherste llen, dass X509-Zertifikate von AWS ACM ausgestel lt werden. Diese Zertifikate müssen gültig und dürfen nicht abgelaufen sein. Für diese Regel ist ein Wert für erforderlich daysToExpiration (Wert für bewährte AWS Grundregeln für Sicherheit: 90). Der tatsächliche Wert muss den Richtlini en Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	ende Verlängerung solcher Zertifika te müssen den bewährten Verfahren der Branche und den geltenden gesetzlic hen/regulatorische n Spezifikationen entsprechen.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10,20	Ein Finanzinstitut speichert öffentlic he kryptografische Schlüssel in einem Zertifikat, das von einer Zertifizi erungsstelle je nach Risikostufe ausgestel lt wurde. Solche Kundenzertifikate werden von anerkannt en Zertifizierungsste llen ausgestellt. Das Finanzinstitut muss sicherstellen, dass die Implementierung von Authentifizierungs - und Signaturp rotokollen, die solche Zertifikate verwenden , einem strengen Schutz unterlieg t. Dadurch wird gewährleistet, dass die Verwendung privater kryptogra fischer Schlüssel, die den Benutzerzertifikat en entsprechen, rechtsverbindlich und unwiderlegbar ist. Die erstmalige Ausstellu ng und die anschließ	Elb v 2 acm-certi ficate-required	Zum Schutz von eventuell vorhanden en sensiblen Daten sowie von Daten während der Übertragung muss die Verschlüsselung für Ihr Elastic Load Balancing aktiviert sein. Verwenden Sie AWS Certificate Manager, um öffentlic he und private SSL/ TLS-Zertifikate mit AWS Diensten und internen Ressource n zu verwalten, bereitzustellen und bereitzustellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	ende Verlängerung solcher Zertifika te müssen den bewährten Verfahren der Branche und den geltenden gesetzlic hen/regulatorische n Spezifikationen entsprechen.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.27	Ein Finanzinstitut muss Mechanismen zur Überwachung in Echtzeit einrichten, um die Kapazitätsauslastung und Leistung der wichtigsten Prozesse und Services nachzuverfolgen. Diese Überwachungsmechanismen müssen in der Lage sein, Administratoren rechtzeitig und mit konkreten Maßnahmen zu benachrichtigen.	autoscaling-group-elb-healthcheck-erforderlich	Die Elastic Load Balancer (ELB) - Zustandsprüfungen für Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling Scaling-Gruppen unterstützen die Aufrechterhaltung einer angemessenen Kapazität und Verfügbarkeit. Der Load Balancer sendet regelmäßig Pings, versucht Verbindungen herzustellen oder sendet Anfragen, um den Zustand der EC2 Amazon-Instances in einer Gruppe mit auto-scaling zu testen. Wenn eine Instance nicht zurückmeldet, wird der Traffic an eine neue EC2 Amazon-Instance gesendet.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.27	Ein Finanzinstitut muss Mechanismen zur Überwachung in Echtzeit einrichten, um die Kapazitätsauslastung und Leistung der wichtigsten Prozesse und Services nachzuverfolgen. Diese Überwachungsmechanismen müssen in der Lage sein, Administratoren rechtzeitig und mit konkreten Maßnahmen zu benachrichtigen.	beanstalk-enhanced-health-reporting-aktiviert	AWS Die verbesserte Zustandsberichterstattung von Elastic Beanstalk ermöglicht eine schnellere Reaktion auf Veränderungen im Zustand der zugrunde liegenden Infrastruktur. Diese Änderungen könnten zu einer mangelnden Verfügbarkeit der Anwendung führen. Die erweiterten Zustandsberichte von Elastic Beanstalk bieten eine Statusbeschreibung, um den Schweregrad der identifizierten Probleme einzuschätzen und mögliche Ursachen zu identifizieren, die untersucht werden müssen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.27	Ein Finanzinstitut muss Mechanismen zur Überwachung in Echtzeit einrichten, um die Kapazitätsauslastung und Leistung der wichtigsten Prozesse und Services nachzuverfolgen. Diese Überwachungsmechanismen müssen in der Lage sein, Administratoren rechtzeitig und mit konkreten Maßnahmen zu benachrichtigen.	cloudwatch-alarm-action-check	Amazon CloudWatch alarmiert, wenn eine Metrik den Schwellenwert für eine bestimmte Anzahl von Bewertungszeiträumen überschreitet. Der Alarm führt eine oder mehrere Aktionen durch, die vom Wert der Metrik oder des Ausdrucks im Vergleich zu einem Schwellenwert in einer Reihe von Zeiträumen abhängt. Diese Regel erfordert einen Wert für alarmActionRequired (Config Default: True), insufficientDataAction Required (Config Default: True), okActionRequired (Config Default: False). Der tatsächliche Wert muss die Alarmaktionen für Ihre Umgebung widerspiegeln.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.27	Ein Finanzinstitut muss Mechanismen zur Überwachung in Echtzeit einrichten, um die Kapazitätsauslastung und Leistung der wichtigsten Prozesse und Services nachzuverfolgen. Diese Überwachungsmechanismen müssen in der Lage sein, Administratoren rechtzeitig und mit konkreten Maßnahmen zu benachrichtigen.	cloud-trail-cloud-watch-logs-aktiviert	Verwenden Sie Amazon CloudWatch , um Protokoll ereignisaktivitäten zentral zu sammeln und zu verwalten. Die Aufnahme von AWS CloudTrail Daten liefert Einzelheiten zu den API-Aufrufaktivitäten in Ihrem AWS-Konto.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.27	Ein Finanzinstitut muss Mechanismen zur Überwachung in Echtzeit einrichten, um die Kapazitätsauslastung und Leistung der wichtigsten Prozesse und Services nachzuverfolgen. Diese Überwachungsmechanismen müssen in der Lage sein, Administratoren rechtzeitig und mit konkreten Maßnahmen zu benachrichtigen.	dynamodb-throughput-limit-check	Aktivieren Sie diese Regel, um sicherzustellen, dass die bereitgestellte Durchsatzkapazität in Ihren Amazon-DynamoDB-Tabellen überprüft wird. Dies ist der Umfang der Lese- und Schreibaktivitäten, der von den jeweiligen Tabellen unterstützt werden kann. DynamoDB verwendet diese Informationen für das Reservieren ausreichender Systemressourcen, um Ihren Durchsatzanforderungen gerecht zu werden. Diese Regel generiert eine Warnung, wenn sich der Durchsatz dem Höchstlimit für ein Kundenkonto nähert. Mit dieser Regel können Sie optional die Parameter RCUThreshold Kontoprozentsatz

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			(Konfigurationsstandard: 80) und WCUThreshold Kontoprozentsatz (Konfigurationsstandard: 80) festlegen. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.
10.27	Ein Finanzinstitut muss Mechanismen zur Überwachung in Echtzeit einrichten, um die Kapazitätsauslastung und Leistung der wichtigsten Prozesse und Services nachzuverfolgen. Diese Überwachungsmechanismen müssen in der Lage sein, Administratoren rechtzeitig und mit konkreten Maßnahmen zu benachrichtigen.	ec-2 instance-detailed-monitoring-enabled	Aktivieren Sie diese Regel, um die Amazon Elastic Compute Cloud (Amazon EC2) - Instance-Überwachung auf der EC2 Amazon-Konsole zu verbessern, in der Monitoring-Diagramme mit einem Zeitraum von 1 Minute für die Instance angezeigt werden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.27	Ein Finanzinstitut muss Mechanismen zur Überwachung in Echtzeit einrichten, um die Kapazitätsauslastung und Leistung der wichtigsten Prozesse und Services nachzuverfolgen. Diese Überwachungsmechanismen müssen in der Lage sein, Administratoren rechtzeitig und mit konkreten Maßnahmen zu benachrichtigen.	lambda-concurrency-check	Diese Regel stellt sicher, dass die Höchst- und Untergrenzen für die Gleichzeitigkeit einer Lambda-Funktion festgelegt werden. Dies kann Sie beim Baselining für die Anzahl der Anforderungen unterstützen, die Ihre Funktion zu einem bestimmten Zeitpunkt verarbeitet.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10,27	Ein Finanzinstitut muss Mechanismen zur Überwachung in Echtzeit einrichten, um die Kapazitätsauslastung und Leistung der wichtigsten Prozesse und Services nachzuverfolgen. Diese Überwachungsmechanismen müssen in der Lage sein, Administratoren rechtzeitig und mit konkreten Maßnahmen zu benachrichtigen.	opensearch-logs-to-cloudwatch	Stellen Sie sicher, dass für Amazon OpenSearch Service-Domains Fehlerprotokolle aktiviert und zur Aufbewahrung und Beantwortung an Amazon CloudWatch Logs gestreamt werden. OpenSearch Service-Fehlerprotokolle können bei Sicherheits- und Zugriffsprüfungen helfen und bei der Diagnose von Verfügbarkeitsproblemen helfen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.27	Ein Finanzinstitut muss Mechanismen zur Überwachung in Echtzeit einrichten, um die Kapazitätsauslastung und Leistung der wichtigsten Prozesse und Services nachzuverfolgen. Diese Überwachungsmechanismen müssen in der Lage sein, Administratoren rechtzeitig und mit konkreten Maßnahmen zu benachrichtigen.	rds-enhanced-monitoring-enabled	Aktivieren Sie Amazon Relational Database Service (Amazon RDS), um die Verfügbarkeit von Amazon RDS zu überwachen. Dies bietet einen detaillierten Einblick in den Zustand Ihrer Amazon-RDS-Datenbank-Instances. Wenn der Amazon-RDS-Speicher mehr als ein zugrunde liegendes physisches Gerät verwendet, erfasst Enhanced Monitoring die Daten für jedes Gerät. Wenn die Datenbank-Instance von Amazon RDS in einer Multi-AZ-Bereitstellung ausgeführt wird, werden außerdem die Daten für jedes Gerät auf dem sekundären Host sowie die Metriken des sekundären Hosts erfasst.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10,34	Ein Finanzinstitut muss sicherstellen, dass die Netzwerkd ienste für seine kritischen Systeme zuverlässig sind und keinen SPOF enthalten, um die kritischen Systeme vor potenziellen Netzwerkfehlern und Cyberbedrohungen zu schützen.	elb-deletion-prote ction-enabled	Diese Regel sorgt dafür, dass der Löschschutz für Elastic Load Balancing aktiviert ist. Verwenden Sie diese Funktion, um zu verhindern, dass Ihr Load Balancer versehentlich oder böswillig gelöscht wird, was zum Verlust der Verfügbarkeit Ihrer Anwendungen führen kann.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10,34	Ein Finanzinstitut muss sicherstellen, dass die Netzwerkd ienste für seine kritischen Systeme zuverlässig sind und keinen SPOF enthalten, um die kritischen Systeme vor potenziellen Netzwerkfehlern und Cyberbedrohungen zu schützen.	vpc-vpn-2-tunnels-up	Redundante Site-to-Site VPN-Tunne l können implement iert werden, um die Anforderungen an die Ausfallsicherheit zu erfüllen. Es verwendet zwei Tunnel, um die Konnektivität sicherzustellen, falls eine der Site-to-Site VPN-Verbindungen nicht verfügbar ist. Um sich vor einem Verbindungsverlust zu schützen, können Sie für den Fall, dass Ihr Kunden-Gateway nicht verfügbar ist, eine zweite Site-to-S ite VPN-Verbindung zu Ihrer Amazon Virtual Private Cloud (Amazon VPC) und Ihrem Virtual Private Gateway einrichten, indem Sie ein zweites Kunden-Gateway verwenden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.35	Ein Finanzinstitut muss Verfahren zur Überwachung der Netzwerkbandbreite in Echtzeit und entsprechende Messwerte für die Resilienz von Netzwerkdiensten einrichten, um jegliche Übernutzung der Bandbreite und Systemunterbrechungen aufgrund von Bandbreitenengpässen und Netzwerkfehlern zu kennzeichnen. Dazu gehört auch die Analyse des Datenverkehrs zur Erkennung von Trends und Anomalien.	api-gw-xray-enabled	AWS X-Ray sammelt Daten über Anfragen, die Ihre Anwendung bedient, und bietet Tools, mit denen Sie diese Daten anzeigen, filtern und Einblicke in sie gewinnen können, um Probleme und Optimierungsmöglichkeiten zu identifizieren. Stellen Sie sicher, dass X-Ray aktiviert ist, damit Sie detaillierte Informationen nicht nur über die Anfrage und Antwort, sondern auch über Aufrufe erhalten, die Ihre Anwendung an nachgelagerte AWS Ressourcen, Microservices, Datenbanken und HTTP-Web APIs tätigt.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.35	Ein Finanzinstitut muss Verfahren zur Überwachung der Netzwerkbandbreite in Echtzeit und entsprechende Messwerte für die Resilienz von Netzwerkdiensten einrichten, um jegliche Übernutzung der Bandbreite und Systemunterbrechungen aufgrund von Bandbreitenengpässen und Netzwerkfehlern zu kennzeichnen. Dazu gehört auch die Analyse des Datenverkehrs zur Erkennung von Trends und Anomalien.	cloudwatch-alarm-action-check	Amazon CloudWatch alarmiert, wenn eine Metrik den Schwellenwert für eine bestimmte Anzahl von Bewertungszeiträumen überschreitet. Der Alarm führt eine oder mehrere Aktionen durch, die vom Wert der Metrik oder des Ausdrucks im Vergleich zu einem Schwellenwert in einer Reihe von Zeiträumen abhängt. Diese Regel erfordert einen Wert für alarmActionRequired (Config Default: True), insufficientDataAction Required (Config Default: True), okActionRequired (Config Default: False). Der tatsächliche Wert muss die Alarmaktionen für Ihre Umgebung widerspiegeln.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.35	Ein Finanzinstitut muss Verfahren zur Überwachung der Netzwerkbandbreite in Echtzeit und entsprechende Messwerte für die Resilienz von Netzwerkdiensten einrichten, um jegliche Übernutzung der Bandbreite und Systemunterbrechungen aufgrund von Bandbreitenengpässen und Netzwerkfehlern zu kennzeichnen. Dazu gehört auch die Analyse des Datenverkehrs zur Erkennung von Trends und Anomalien.	elb-logging-enabled	Die Elastic-Load-Balancing-Aktivität ist ein zentraler Kommunikationspunkt innerhalb einer Umgebung. Stellen Sie sicher, dass die ELB-Protokollierung aktiviert ist. Die gesammelten Daten enthalten detaillierte Informationen zu Anfragen, die an den ELB gesendet wurden. Jedes Protokoll enthält Informationen wie die Zeit, zu der die Anforderung einging, die Client-IP-Adresse, Latenzen, Anforderungspfade und Serverantworten.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10,35	Ein Finanzinstitut muss Verfahren zur Überwachung der Netzwerkbandbreite in Echtzeit und entsprechende Messwerte für die Resilienz von Netzwerkdiensten einrichten, um jegliche Übernutzung der Bandbreite und Systemunterbrechungen aufgrund von Bandbreitenengpässen und Netzwerkfehlern zu kennzeichnen. Dazu gehört auch die Analyse des Datenverkehrs zur Erkennung von Trends und Anomalien.	vpc-flow-logs-enabled	VPC-Flow-Protokolle erfassen detaillierte Informationsdatensätze über den IP-Datenverkehr, der zu und von Netzwerkschnittstellen in Ihrer Amazon Virtual Private Cloud (Amazon VPC) fließt. Standardmäßig enthalten Flow-Protokolldatensätze Werte für die verschiedenen Komponenten des IP-Flows, einschließlich Quelle, Ziel und Protokoll.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10,36	Ein Finanzinstitut muss sicherstellen, dass Netzwerkdienste zur Unterstützung kritischer Systeme so konzipiert und implementiert werden, dass die Vertrauli chkeit, Integrität und Verfügbarkeit der Daten gewährleistet ist.	alb-http-to-https-Umleitungsprüfung	Um Daten während der Übertragung zu schützen, stellen Sie sicher, dass Ihr Application Load Balancer unverschl üsselte HTTP-Anfr agen automatisch an HTTPS umleitet. Da sensible Daten vorhanden sein können, sollten Sie die Verschlüsselung bei der Übertragung aktivieren, um diese Daten zu schützen.
10.36	Ein Finanzinstitut muss sicherstellen, dass Netzwerkdienste zur Unterstützung kritischer Systeme so konzipiert und implementiert werden, dass die Vertrauli chkeit, Integrität und Verfügbarkeit der Daten gewährleistet ist.	api-gw-ssl-enabled	Stellen Sie sicher, dass die REST-API-Stufen von Amazon API Gateway mit SSL-Zertifikaten konfiguri ert sind, damit Backend-Systeme überprüfen können, ob Anforderungen von API Gateway stammen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10,36	Ein Finanzinstitut muss sicherstellen, dass Netzwerkdienste zur Unterstützung kritischer Systeme so konzipiert und implementiert werden, dass die Vertrauli chkeit, Integrität und Verfügbarkeit der Daten gewährleistet ist.	Elb v 2 acm-certi ficate-required	Zum Schutz von eventuell vorhanden en sensiblen Daten sowie von Daten während der Übertragung muss die Verschlüsselung für Ihr Elastic Load Balancing aktiviert sein. Verwenden Sie AWS Certificate Manager, um öffentlic he und private SSL/ TLS-Zertifikate mit AWS Diensten und internen Ressource n zu verwalten, bereitzustellen und bereitzustellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.36	Ein Finanzinstitut muss sicherstellen, dass Netzwerkdienste zur Unterstützung kritischer Systeme so konzipiert und implementiert werden, dass die Vertrauli chkeit, Integrität und Verfügbarkeit der Daten gewährleistet ist.	elb-deletion-prote ction-enabled	Diese Regel sorgt dafür, dass der Löschschutz für Elastic Load Balancing aktiviert ist. Verwenden Sie diese Funktion, um zu verhindern, dass Ihr Load Balancer versehentlich oder böswillig gelöscht wird, was zum Verlust der Verfügbarkeit Ihrer Anwendungen führen kann.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10,36	Ein Finanzinstitut muss sicherstellen, dass Netzwerkdienste zur Unterstützung kritischer Systeme so konzipiert und implementiert werden, dass die Vertrauli chkeit, Integrität und Verfügbarkeit der Daten gewährleistet ist.	nlb-cross-zone-load-Balancing aktiviert	Aktivieren Sie den zonenübergreifende n Lastenausgleich für Ihre Network Load Balancer (NLBs), um eine angemesse ne Kapazität und Verfügbarkeit aufrechtzuerhalten. Zonenübergreifende s Load Balancing reduziert die Notwendigkeit, die gleiche Anzahl von Instances in jeder aktivierten Availability Zone aufrechtzuerhalten . Dadurch wird auch die Fähigkeit Ihrer Anwendung verbessert, den Verlust einer oder mehrerer Instances zu bewältigen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.38	Ein Finanzinstitut muss sicherstellen, dass ausreichende und relevante Netzwerkgeräteprotokolle für Untersuchungen und forensische Zwecke mindestens drei Jahre lang aufbewahrt werden.	cw-loggroup-retention-period-überprüfen	Stellen Sie sicher, dass die Ereignisprotokolldaten für Ihre Protokollgruppen über eine Mindestdauer aufbewahrt werden, um die Fehlerbehebung und forensische Untersuchungen zu unterstützen. Fehlende frühere Ereignisprotokolldaten erschweren die Rekonstruierung und Identifizierung potenziell schädlicher Ereignisse.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10,51	Ein Finanzinstitut muss bei der Nutzung von Cloud-Services angemessene Sicherheitsvorkehrungen für Kunden- und Gegenpartieiinformationen sowie für firmeneigene Daten ergreifen, um sich vor unbefugter Offenlegung und unbefugtem Zugriff zu schützen. Dies beinhaltet die Beibehaltung des Eigentums, der Kontrolle und der Verwaltung aller Daten, die sich auf Kunden- und Gegenparteiinformationen, firmeneigene Daten und in der Cloud gehostete Services beziehen, einschließlich der Verwaltung der entsprechenden kryptografischen Schlüssel.	access-keys-rotated	Die Anmeldeinformationen für autorisierte Geräte, Benutzer und Prozesse werden geprüft, indem sichergestellt wird, dass die IAM-Zugriffsschlüssel gemäß den Vorgaben der Unternehmensrichtlinie rotiert werden. Das regelmäßige Ändern der Zugriffsschlüssel ist eine bewährte Sicherheitsmethode. Es verkürzt den Zeitraum, in dem ein Zugriffsschlüssel aktiv ist, und reduziert die Auswirkungen auf das Unternehmen, wenn die Schlüssel kompromittiert werden. Diese Regel erfordert einen Wert für die Zugriffsschlüssel-Rotation (Standardkonfiguration: 90). Der tatsächliche Wert muss den Richtlini

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			en Ihrer Organisation entsprechen.
10.51	Ein Finanzinstitut muss bei der Nutzung von Cloud-Services angemessene Sicherheitsvorkehrungen für Kunden- und Gegenpartei informationen sowie für firmeneigene Daten ergreifen, um sich vor unbefugter Offenlegung und unbefugtem Zugriff zu schützen. Dies beinhaltet die Beibehaltung des Eigentums, der Kontrolle und der Verwaltung aller Daten, die sich auf Kunden- und Gegenparteiinformationen, firmeneigene Daten und in der Cloud gehostete Services beziehen, einschließlich der Verwaltung der entsprechenden kryptografischen Schlüssel.	account-part-of-organizations	Durch die zentrale Verwaltung AWS-Konten innerhalb von AWS Organizations wird sichergestellt, dass die Konten den Vorschriften entsprechen. Eine fehlende zentrale Kontoverwaltung kann zu inkonsistenten Kontokonfigurationen führen, wodurch Ressourcen und sensible Daten offengelegt werden können.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.51	Ein Finanzinstitut muss bei der Nutzung von Cloud-Services angemessene Sicherheitsvorkehrungen für Kunden- und Gegenpartieinformationen sowie für firmeneigene Daten ergreifen, um sich vor unbefugter Offenlegung und unbefugtem Zugriff zu schützen. Dies beinhaltet die Beibehaltung des Eigentums, der Kontrolle und der Verwaltung aller Daten, die sich auf Kunden- und Gegenparteiinformationen, firmeneigene Daten und in der Cloud gehostete Services beziehen, einschließlich der Verwaltung der entsprechenden kryptografischen Schlüssel.	alb-http-to-https-Umleitungsprüfung	Um Daten während der Übertragung zu schützen, stellen Sie sicher, dass Ihr Application Load Balancer unverschlüsselte HTTP-Anfragen automatisch an HTTPS umleitet. Da sensible Daten vorhanden sein können, sollten Sie die Verschlüsselung bei der Übertragung aktivieren, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.51	Ein Finanzinstitut muss bei der Nutzung von Cloud-Services angemessene Sicherheitsvorkehrungen für Kunden- und Gegenpartieinformationen sowie für firmeneigene Daten ergreifen, um sich vor unbefugter Offenlegung und unbefugtem Zugriff zu schützen. Dies beinhaltet die Beibehaltung des Eigentums, der Kontrolle und der Verwaltung aller Daten, die sich auf Kunden- und Gegenparteiinformationen, firmeneigene Daten und in der Cloud gehostete Services beziehen, einschließlich der Verwaltung der entsprechenden kryptografischen Schlüssel.	api-gw-cache-enabled-und-verschlüsselt	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass die Verschlüsselung für den Cache Ihrer API-Gateway-Stufe aktiviert ist. Da für die API-Methode sensible Daten erfasst werden können, sollten Sie die Verschlüsselung von Daten im Ruhezustand aktivieren, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.51	Ein Finanzinstitut muss bei der Nutzung von Cloud-Ser vices angemessene Sicherheitsvorkehr ungen für Kunden- und Gegenpart eiinformationen sowie für firmeneigene Daten ergreifen, um sich vor unbefugte r Offenlegung und unbefugtem Zugriff zu schützen. Dies beinhaltet die Beibehaltung des Eigentums, der Kontrolle und der Verwaltung aller Daten, die sich auf Kunden- und Gegenparteiinforma tionen, firmeneig ene Daten und in der Cloud gehostete Services beziehen, einschließlich der Verwaltung der entsprechenden kryptografischen Schlüssel.	api-gw-ssl-enabled	Stellen Sie sicher, dass die REST-API-Stufen von Amazon API Gateway mit SSL-Zertifikaten konfiguri ert sind, damit Backend-Systeme überprüfen können, ob Anforderungen von API Gateway stammen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10,51	Ein Finanzinstitut muss bei der Nutzung von Cloud-Services angemessene Sicherheitsvorkehrungen für Kunden- und Gegenpartei informationen sowie für firmeneigene Daten ergreifen, um sich vor unbefugter Offenlegung und unbefugtem Zugriff zu schützen. Dies beinhaltet die Beibehaltung des Eigentums, der Kontrolle und der Verwaltung aller Daten, die sich auf Kunden- und Gegenparteiinformationen, firmeneigene Daten und in der Cloud gehostete Services beziehen, einschließlich der Verwaltung der entsprechenden kryptografischen Schlüssel.	autoscaling-launch-config-public-ip-deaktiviert	Wenn Sie Ihre Netzwerkschnittstellen mit einer öffentlichen IP-Adresse konfigurieren, sind die diesen Netzwerkschnittstellen zugehörigen Ressourcen über das Internet erreichbar. EC2 Ressourcen sollten nicht öffentlich zugänglich sein, da dies einen unbeabsichtigten Zugriff auf Ihre Anwendungen oder Server ermöglichen kann.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.51	Ein Finanzinstitut muss bei der Nutzung von Cloud-Services angemessene Sicherheitsvorkehrungen für Kunden- und Gegenpartieinformationen sowie für firmeneigene Daten ergreifen, um sich vor unbefugter Offenlegung und unbefugtem Zugriff zu schützen. Dies beinhaltet die Beibehaltung des Eigentums, der Kontrolle und der Verwaltung aller Daten, die sich auf Kunden- und Gegenparteiinformationen, firmeneigene Daten und in der Cloud gehostete Services beziehen, einschließlich der Verwaltung der entsprechenden kryptografischen Schlüssel.	backup-recovery-point-encrypted	Stellen Sie sicher, dass die Verschlüsselung für Ihre AWS Backup-Wiederherstellungspunkte aktiviert ist. Da sensible Daten auch im Ruhezustand vorhanden sein können, sollten Sie die Verschlüsselung im Ruhezustand aktivieren, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.51	Ein Finanzinstitut muss bei der Nutzung von Cloud-Services angemessene Sicherheitsvorkehrungen für Kunden- und Gegenpartieinformationen sowie für firmeneigene Daten ergreifen, um sich vor unbefugter Offenlegung und unbefugtem Zugriff zu schützen. Dies beinhaltet die Beibehaltung des Eigentums, der Kontrolle und der Verwaltung aller Daten, die sich auf Kunden- und Gegenparteiinformationen, firmeneigene Daten und in der Cloud gehostete Services beziehen, einschließlich der Verwaltung der entsprechenden kryptografischen Schlüssel.	cloudtrail-security-trail-enabled	Diese Regel trägt dazu bei, die Verwendung der AWS empfohlenen bewährten Sicherheitsmethoden für sicherzustellen AWS CloudTrail, indem geprüft wird, ob mehrere Einstellungen aktiviert sind. Dazu gehören die Verwendung von Protokollverschlüsselung, Protokollvalidierung und Aktivierung AWS CloudTrail in mehreren Regionen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.51	Ein Finanzinstitut muss bei der Nutzung von Cloud-Ser vices angemessene Sicherheitsvorkehr ungen für Kunden- und Gegenpart eiinformationen sowie für firmeneigene Daten ergreifen, um sich vor unbefugte r Offenlegung und unbefugtem Zugriff zu schützen. Dies beinhaltet die Beibehaltung des Eigentums, der Kontrolle und der Verwaltung aller Daten, die sich auf Kunden- und Gegenparteiinforma tionen, firmeneig ene Daten und in der Cloud gehostete Services beziehen, einschließlich der Verwaltung der entsprechenden kryptografischen Schlüssel.	cloudwatch-log-group-encrypted	Um sensible Daten im Speicher zu schützen, stellen Sie sicher, dass die Verschlüs selung für Ihre Amazon CloudWatch Log Groups aktiviert ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.51	Ein Finanzinstitut muss bei der Nutzung von Cloud-Services angemessene Sicherheitsvorkehrungen für Kunden- und Gegenpartieinformationen sowie für firmeneigene Daten ergreifen, um sich vor unbefugter Offenlegung und unbefugtem Zugriff zu schützen. Dies beinhaltet die Beibehaltung des Eigentums, der Kontrolle und der Verwaltung aller Daten, die sich auf Kunden- und Gegenparteiinformationen, firmeneigene Daten und in der Cloud gehostete Services beziehen, einschließlich der Verwaltung der entsprechenden kryptografischen Schlüssel.	cmk-backing-key-rotation-aktiviert	Aktivieren Sie die Schlüsselrotation, um sicherzustellen, dass Schlüssel rotiert werden, nachdem sie das Ende ihrer Krypto-Periode erreicht haben.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.51	Ein Finanzinstitut muss bei der Nutzung von Cloud-Services angemessene Sicherheitsvorkehrungen für Kunden- und Gegenpartei informationen sowie für firmeneigene Daten ergreifen, um sich vor unbefugter Offenlegung und unbefugtem Zugriff zu schützen. Dies beinhaltet die Beibehaltung des Eigentums, der Kontrolle und der Verwaltung aller Daten, die sich auf Kunden- und Gegenparteiinformationen, firmeneigene Daten und in der Cloud gehostete Services beziehen, einschließlich der Verwaltung der entsprechenden kryptografischen Schlüssel.	dms-replication-not-public	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass auf DMS-Replikationsinstanzen nicht öffentlich zugegriffen werden kann. DMS-Replikations-Instances können vertrauliche Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.5.1	Ein Finanzinstitut muss bei der Nutzung von Cloud-Services angemessene Sicherheitsvorkehrungen für Kunden- und Gegenpartieiinformationen sowie für firmeneigene Daten ergreifen, um sich vor unbefugter Offenlegung und unbefugtem Zugriff zu schützen. Dies beinhaltet die Beibehaltung des Eigentums, der Kontrolle und der Verwaltung aller Daten, die sich auf Kunden- und Gegenparteiinformationen, firmeneigene Daten und in der Cloud gehostete Services beziehen, einschließlich der Verwaltung der entsprechenden kryptografischen Schlüssel.	dynamodb-table-encrypted-kms	Stellen Sie sicher, dass die Verschlüsselung für Ihre Amazon-DynamoDB-Tabellen aktiviert ist. Um eventuell vorhandene sensible Daten im Ruhezustand in diesen Tabellen zu schützen, müssen Sie die Verschlüsselung von Daten im Ruhezustand aktivieren. Standardmäßig werden DynamoDB-Tabellen mit einem AWS eigenen Kundenhauptschlüssel (CMK) verschlüsselt.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.51	Ein Finanzinstitut muss bei der Nutzung von Cloud-Ser vices angemessene Sicherheitsvorkehr ungen für Kunden- und Gegenpart eiinformationen sowie für firmeneigene Daten ergreifen, um sich vor unbefugte r Offenlegung und unbefugtem Zugriff zu schützen. Dies beinhaltet die Beibehaltung des Eigentums, der Kontrolle und der Verwaltung aller Daten, die sich auf Kunden- und Gegenparteiinforma tionen, firmeneig ene Daten und in der Cloud gehostete Services beziehen, einschließlich der Verwaltung der entsprechenden kryptografischen Schlüssel.	ebs-snapshot-public-restorable-überprüfen	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass EBS-Snapshots nicht öffentlich wiederher stellbar sind. EBS-Volume-Snapsho ts können vertrauli che Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.51	Ein Finanzinstitut muss bei der Nutzung von Cloud-Services angemessene Sicherheitsvorkehrungen für Kunden- und Gegenpartieinformationen sowie für firmeneigene Daten ergreifen, um sich vor unbefugter Offenlegung und unbefugtem Zugriff zu schützen. Dies beinhaltet die Beibehaltung des Eigentums, der Kontrolle und der Verwaltung aller Daten, die sich auf Kunden- und Gegenparteiinformationen, firmeneigene Daten und in der Cloud gehostete Services beziehen, einschließlich der Verwaltung der entsprechenden kryptografischen Schlüssel.	ec-2 ebs-encryption-by-default	Zum Schutz von Daten im Ruhezustand müssen Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon Elastic Block Store (Amazon EBS)-Volumes aktiviert ist. Aktivieren Sie die Verschlüsselung von Daten im Ruhezustand, um eventuell in diesen Volumes vorhandene sensible Daten im Ruhezustand zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10,51	Ein Finanzinstitut muss bei der Nutzung von Cloud-Ser vices angemessene Sicherheitsvorkehr ungen für Kunden- und Gegenpart eiinformationen sowie für firmeneigene Daten ergreifen, um sich vor unbefugte r Offenlegung und unbefugtem Zugriff zu schützen. Dies beinhaltet die Beibehaltung des Eigentums, der Kontrolle und der Verwaltung aller Daten, die sich auf Kunden- und Gegenparteiinforma tionen, firmeneig ene Daten und in der Cloud gehostete Services beziehen, einschließlich der Verwaltung der entsprechenden kryptografischen Schlüssel.	ec-2 instance-no-public-ip	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon Elastic Compute Cloud (Amazon EC2) - Instances nicht öffentlich zugänglich sind. EC2 Amazon-Instances können vertrauliche Informati onen enthalten, und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.51	Ein Finanzinstitut muss bei der Nutzung von Cloud-Ser vices angemessene Sicherheitsvorkehr ungen für Kunden- und Gegenpart eiinformationen sowie für firmeneigene Daten ergreifen, um sich vor unbefugte r Offenlegung und unbefugtem Zugriff zu schützen. Dies beinhaltet die Beibehaltung des Eigentums, der Kontrolle und der Verwaltung aller Daten, die sich auf Kunden- und Gegenparteiinforma tionen, firmeneig ene Daten und in der Cloud gehostete Services beziehen, einschließlich der Verwaltung der entsprechenden kryptografischen Schlüssel.	efs-encrypted-check	Aktivieren Sie die Verschlüsselung für Ihr Amazon Elastic File System (EFS), um eventuell vorhandene sensible Daten sowie Daten im Ruhezustand zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10,51	Ein Finanzinstitut muss bei der Nutzung von Cloud-Services angemessene Sicherheitsvorkehrungen für Kunden- und Gegenpartieinformationen sowie für firmeneigene Daten ergreifen, um sich vor unbefugter Offenlegung und unbefugtem Zugriff zu schützen. Dies beinhaltet die Beibehaltung des Eigentums, der Kontrolle und der Verwaltung aller Daten, die sich auf Kunden- und Gegenparteiinformationen, firmeneigene Daten und in der Cloud gehostete Services beziehen, einschließlich der Verwaltung der entsprechenden kryptografischen Schlüssel.	Elb v 2 acm-certificate-required	Zum Schutz von eventuell vorhandenen sensiblen Daten sowie von Daten während der Übertragung muss die Verschlüsselung für Ihr Elastic Load Balancing aktiviert sein. Verwenden Sie AWS Certificate Manager, um öffentliche und private SSL/TLS-Zertifikate mit AWS Diensten und internen Ressourcen zu verwalten, bereitzustellen und bereitzustellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.51	Ein Finanzinstitut muss bei der Nutzung von Cloud-Services angemessene Sicherheitsvorkehrungen für Kunden- und Gegenpartieinformationen sowie für firmeneigene Daten ergreifen, um sich vor unbefugter Offenlegung und unbefugtem Zugriff zu schützen. Dies beinhaltet die Beibehaltung des Eigentums, der Kontrolle und der Verwaltung aller Daten, die sich auf Kunden- und Gegenparteiinformationen, firmeneigene Daten und in der Cloud gehostete Services beziehen, einschließlich der Verwaltung der entsprechenden kryptografischen Schlüssel.	emr-kerberos-enabled	Die Zugriffsberechtigungen und -autorisierungen können verwaltet und nach den Prinzipien der geringsten Berechtigung und Aufgabentrennung integriert werden, indem Kerberos für Amazon-EMR-Cluster aktiviert wird. In Kerberos werden Services und Benutzer, die sich authentifizieren müssen, als Prinzipale bezeichnet. Prinzipale befinden sich in einem Kerberos-Bereich. Innerhalb dieses Bereichs wird ein Kerberos-Server als Key Distribution Center (KDC) bezeichnet. Über diesen Server können sich Prinzipale authentifizieren. Die Authentifizierung im KDC erfolgt durch die Ausstellung von Authentif

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			izierungstickets. Das KDC unterhält eine Datenbank der Prinzipale in seinem Bereich mit ihren Passwörtern und anderen administr ativen Informationen zu jedem Prinzipal.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10,51	Ein Finanzinstitut muss bei der Nutzung von Cloud-Ser vices angemessene Sicherheitsvorkehr ungen für Kunden- und Gegenpart eiinformationen sowie für firmeneigene Daten ergreifen, um sich vor unbefugte r Offenlegung und unbefugtem Zugriff zu schützen. Dies beinhaltet die Beibehaltung des Eigentums, der Kontrolle und der Verwaltung aller Daten, die sich auf Kunden- und Gegenparteiinforma tionen, firmeneig ene Daten und in der Cloud gehostete Services beziehen, einschließlich der Verwaltung der entsprechenden kryptografischen Schlüssel.	emr-master-no-public-ip	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon EMR-Clust er-Masterknoten nicht öffentlich zugänglic h sind. Amazon-EM R-Cluster-Hauptkno ten können vertrauli che Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.51	Ein Finanzinstitut muss bei der Nutzung von Cloud-Ser vices angemessene Sicherheitsvorkehr ungen für Kunden- und Gegenpart eiinformationen sowie für firmeneigene Daten ergreifen, um sich vor unbefugte r Offenlegung und unbefugtem Zugriff zu schützen. Dies beinhaltet die Beibehaltung des Eigentums, der Kontrolle und der Verwaltung aller Daten, die sich auf Kunden- und Gegenparteiinforma tionen, firmeneig ene Daten und in der Cloud gehostete Services beziehen, einschließlich der Verwaltung der entsprechenden kryptografischen Schlüssel.	encrypted-volumes	Aktivieren Sie die Verschlüsselung für Ihre Volumes von Amazon Elastic Block Store (Amazon EBS), um eventuell vorhandene sensible Daten sowie Daten im Ruhezustand zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10,51	Ein Finanzinstitut muss bei der Nutzung von Cloud-Services angemessene Sicherheitsvorkehrungen für Kunden- und Gegenpartieinformationen sowie für firmeneigene Daten ergreifen, um sich vor unbefugter Offenlegung und unbefugtem Zugriff zu schützen. Dies beinhaltet die Beibehaltung des Eigentums, der Kontrolle und der Verwaltung aller Daten, die sich auf Kunden- und Gegenparteiinformationen, firmeneigene Daten und in der Cloud gehostete Services beziehen, einschließlich der Verwaltung der entsprechenden kryptografischen Schlüssel.	iam-customer-policy-blocked-kms-Aktionen	AWS Identity and Access Management (IAM) kann Ihnen helfen, die Prinzipien der geringsten Rechte und der Aufgabentrennung in Zugriffsberechtigungen und Autorisierungen zu integrieren und so zu verhindern, dass Richtlinien blockierte Aktionen für alle AWS Schlüssel des Key Management Service enthalten. Wenn Benutzer mehr Rechte haben, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und Aufgabentrennung verstoßen. Mit dieser Regel können Sie den Parameter festlegen. blockedActionsPatterns (Wert „AWS Bewährte grundlegende Sicherheitsmethoden“: kms:

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			Decrypt, kms:ReEncryptFrom). Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10,51	Ein Finanzinstitut muss bei der Nutzung von Cloud-Ser vices angemessene Sicherheitsvorkehr ungen für Kunden- und Gegenpart eiinformationen sowie für firmeneigene Daten ergreifen, um sich vor unbefugte r Offenlegung und unbefugtem Zugriff zu schützen. Dies beinhaltet die Beibehaltung des Eigentums, der Kontrolle und der Verwaltung aller Daten, die sich auf Kunden- und Gegenparteiinforma tionen, firmeneig ene Daten und in der Cloud gehostete Services beziehen, einschließlich der Verwaltung der entsprechenden kryptografischen Schlüssel.	iam-no-inline-policy-überprüfen	Stellen Sie sicher, dass ein Benutzer, eine IAM-Rolle oder eine IAM-Gruppe (AWS Identity and Access Management) nicht über eine Inline-Richtlinie zur Zugriffsk ontrolle auf Systeme und Ressource n verfügt. AWS empfiehlt, verwaltet e Richtlinien anstelle von Inline-Richtlinien zu verwenden. Verwaltete Richtlini en ermöglichen Wiederverwendbarke it, Versionsverwaltung , Rollback und Delegierung der Berechtigungsverwa ltung.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.51	Ein Finanzinstitut muss bei der Nutzung von Cloud-Services angemessene Sicherheitsvorkehrungen für Kunden- und Gegenpartieiinformationen sowie für firmeneigene Daten ergreifen, um sich vor unbefugter Offenlegung und unbefugtem Zugriff zu schützen. Dies beinhaltet die Beibehaltung des Eigentums, der Kontrolle und der Verwaltung aller Daten, die sich auf Kunden- und Gegenparteiinformationen, firmeneigene Daten und in der Cloud gehostete Services beziehen, einschließlich der Verwaltung der entsprechenden kryptografischen Schlüssel.	iam-password-policy	Die Identitäten und Anmeldeinformationen werden auf der Grundlage einer organisatorischen IAM-Passwortrichtlinie ausgestellt, verwaltet und verifiziert. Sie erfüllen oder übertreffen die Anforderungen von NIST SP 800-63 und dem Standard „Best Practices“ von AWS Foundational Security für die Passwortstärke. Mit dieser Regel können Sie optional RequireUppercaseCharacters (Wert für AWS grundlegende Sicherheitsbewährte Methoden: wahr), RequireLowercaseCharacters (Wert für bewährte Methoden für AWS grundlegende Sicherheit: wahr), RequireSymbols (Wert für bewährte Methoden für AWS grundlegende Sicherheit:

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			wahr), RequireNumbers (Wert für bewährte Methoden für AWS grundlegende Sicherheit: wahr), MinimumPasswordLength (Wert für bewährte Methoden für AWS grundlegende Sicherheit: 14), PasswordReusePrevention (Wert für bewährte Methoden für AWS grundlegende Sicherheit: 24) und MaxPasswordAge (Wert für bewährte Methoden für AWS grundlegende Sicherheit: 90) für Ihr IAM festlegen Kennwortrichtlinie. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.51	Ein Finanzinstitut muss bei der Nutzung von Cloud-Services angemessene Sicherheitsvorkehrungen für Kunden- und Gegenpartieinformationen sowie für firmeneigene Daten ergreifen, um sich vor unbefugter Offenlegung und unbefugtem Zugriff zu schützen. Dies beinhaltet die Beibehaltung des Eigentums, der Kontrolle und der Verwaltung aller Daten, die sich auf Kunden- und Gegenparteiinformationen, firmeneigene Daten und in der Cloud gehostete Services beziehen, einschließlich der Verwaltung der entsprechenden kryptografischen Schlüssel.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) kann Ihnen dabei helfen, die Prinzipien der geringsten Rechte und der Aufgabentrennung in Zugriffsberechtigungen und Autorisierungen zu integrieren und so zu verhindern, dass Richtlinien „Effect“: „Allow“ mit „Action“: „*“ anstelle von „Resource“: „*“ enthalten. Wenn Benutzern mehr Rechte eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und der Aufgabentrennung verstoßen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10,51	Ein Finanzinstitut muss bei der Nutzung von Cloud-Services angemessene Sicherheitsvorkehrungen für Kunden- und Gegenpartieinformationen sowie für firmeneigene Daten ergreifen, um sich vor unbefugter Offenlegung und unbefugtem Zugriff zu schützen. Dies beinhaltet die Beibehaltung des Eigentums, der Kontrolle und der Verwaltung aller Daten, die sich auf Kunden- und Gegenparteiinformationen, firmeneigene Daten und in der Cloud gehostete Services beziehen, einschließlich der Verwaltung der entsprechenden kryptografischen Schlüssel.	iam-root-access-key-überprüfen	Der Zugriff auf Systeme und Ressourcen kann gesteuert werden, indem überprüft wird, ob der Root-Benutzer keine Zugriffsschlüssel mit seiner AWS Identity and Access Management (IAM) -Rolle verknüpft hat. Stellen Sie sicher, dass die Root-Zugriffsschlüssel gelöscht werden. Erstellen und verwenden Sie stattdessen rollenbasierte Funktionen, AWS-Konten um das Prinzip der geringsten Funktionalität zu berücksichtigen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.51	Ein Finanzinstitut muss bei der Nutzung von Cloud-Services angemessene Sicherheitsvorkehrungen für Kunden- und Gegenpartei informationen sowie für firmeneigene Daten ergreifen, um sich vor unbefugter Offenlegung und unbefugtem Zugriff zu schützen. Dies beinhaltet die Beibehaltung des Eigentums, der Kontrolle und der Verwaltung aller Daten, die sich auf Kunden- und Gegenparteiinformationen, firmeneigene Daten und in der Cloud gehostete Services beziehen, einschließlich der Verwaltung der entsprechenden kryptografischen Schlüssel.	iam-user-group-membership-überprüfen	AWS Identity and Access Management (IAM) kann Ihnen helfen, Zugriffsberechtigungen und Autorisierungen einzuschränken, indem sichergestellt wird, dass IAM-Benutzer Mitglieder mindestens einer Gruppe sind. Wenn Benutzern mehr Berechtigungen eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und Aufgabentrennung verstoßen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.51	Ein Finanzinstitut muss bei der Nutzung von Cloud-Ser vices angemessene Sicherheitsvorkehr ungen für Kunden- und Gegenpart eiinformationen sowie für firmeneigene Daten ergreifen, um sich vor unbefugte r Offenlegung und unbefugtem Zugriff zu schützen. Dies beinhaltet die Beibehaltung des Eigentums, der Kontrolle und der Verwaltung aller Daten, die sich auf Kunden- und Gegenparteiinforma tionen, firmeneig ene Daten und in der Cloud gehostete Services beziehen, einschließlich der Verwaltung der entsprechenden kryptografischen Schlüssel.	iam-user-mfa-enabled	Aktivieren Sie diese Regel, um den Zugriff auf Ressourcen in der AWS Cloud einzuschr änken. Diese Regel stellt sicher, dass die Multi-Faktor-Authe ntifizierung (MFA) für alle IAM-Benut zer aktiviert ist. MFA bietet eine weitere Schutzebene zusätzlic h zum Benutzern amen und Passwort. Reduzieren Sie Fälle von kompromittierten Konten, indem Sie MFA für IAM-Benutzer vorschreiben.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.51	Ein Finanzinstitut muss bei der Nutzung von Cloud-Services angemessene Sicherheitsvorkehrungen für Kunden- und Gegenpartei informationen sowie für firmeneigene Daten ergreifen, um sich vor unbefugter Offenlegung und unbefugtem Zugriff zu schützen. Dies beinhaltet die Beibehaltung des Eigentums, der Kontrolle und der Verwaltung aller Daten, die sich auf Kunden- und Gegenparteiinformationen, firmeneigene Daten und in der Cloud gehostete Services beziehen, einschließlich der Verwaltung der entsprechenden kryptografischen Schlüssel.	iam-user-no-policies-überprüfen	Diese Regel stellt sicher, dass AWS Identity and Access Management (IAM)-Richtlinien nur Gruppen oder Rollen zugewiesen werden, um den Zugriff auf Systeme und Ressourcen zu kontrollieren. Die Zuweisung von Berechtigungen auf Gruppen- oder Rollenebene trägt dazu bei, die Wahrscheinlichkeit zu verringern, dass eine Identität übermäßige Berechtigungen erhält oder beibehält.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.51	Ein Finanzinstitut muss bei der Nutzung von Cloud-Services angemessene Sicherheitsvorkehrungen für Kunden- und Gegenpartei informationen sowie für firmeneigene Daten ergreifen, um sich vor unbefugter Offenlegung und unbefugtem Zugriff zu schützen. Dies beinhaltet die Beibehaltung des Eigentums, der Kontrolle und der Verwaltung aller Daten, die sich auf Kunden- und Gegenparteiinformationen, firmeneigene Daten und in der Cloud gehostete Services beziehen, einschließlich der Verwaltung der entsprechenden kryptografischen Schlüssel.	iam-user-unused-credentials-überprüfen	AWS Identity and Access Management (IAM) kann Ihnen bei Zugriffsberechtigungen und Autorisierungen helfen, indem es nach IAM-Passwörtern und Zugriffsschlüsseln sucht, die für einen bestimmten Zeitraum nicht verwendet wurden. Wenn ungenutzte Anmeldeinformationen identifiziert werden, müssen Sie sie deaktivieren und/oder entfernen, da dies gegen das Prinzip der geringsten Berechtigung verstoßen könnte. Für diese Regel müssen Sie einen Wert für das maxCredentialUsage Alter festlegen (Standardkonfiguration: 90). Der tatsächliche Wert muss den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.51	Ein Finanzinstitut muss bei der Nutzung von Cloud-Services angemessene Sicherheitsvorkehrungen für Kunden- und Gegenpartieinformationen sowie für firmeneigene Daten ergreifen, um sich vor unbefugter Offenlegung und unbefugtem Zugriff zu schützen. Dies beinhaltet die Beibehaltung des Eigentums, der Kontrolle und der Verwaltung aller Daten, die sich auf Kunden- und Gegenparteiinformationen, firmeneigene Daten und in der Cloud gehostete Services beziehen, einschließlich der Verwaltung der entsprechenden kryptografischen Schlüssel.	internet-gateway-authorized-vpc-nur	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Internet-Gateways nur mit autorisierter Amazon Virtual Private Cloud (Amazon VPC) verbunden sind. Internet-Gateways ermöglichen den bidirektionalen Internetzugang zur und von der Amazon VPC, was möglicher weise zu einem unbefugten Zugriff auf Amazon-VPC-Ressourcen führen kann.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.51	Ein Finanzinstitut muss bei der Nutzung von Cloud-Services angemessene Sicherheitsvorkehrungen für Kunden- und Gegenpartieinformationen sowie für firmeneigene Daten ergreifen, um sich vor unbefugter Offenlegung und unbefugtem Zugriff zu schützen. Dies beinhaltet die Beibehaltung des Eigentums, der Kontrolle und der Verwaltung aller Daten, die sich auf Kunden- und Gegenparteiinformationen, firmeneigene Daten und in der Cloud gehostete Services beziehen, einschließlich der Verwaltung der entsprechenden kryptografischen Schlüssel.	kms-cmk-not-scheduled-zum Löschen	Um Daten im Ruhezustand zu schützen, sollten Sie sicherstellen, dass die für den Kunden erforderlichen Masterschlüssel (CMKs) nicht für das Löschen im AWS Key Management Service (AWS KMS) vorgesehen sind. Da Schlüssel manchmal gelöscht werden müssen, können Sie mit dieser Regel alle zu löschenden Schlüssel überprüfen, falls ein Schlüssel versehentlich zur Löschung vorgemerkt wurde.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.51	Ein Finanzinstitut muss bei der Nutzung von Cloud-Services angemessene Sicherheitsvorkehrungen für Kunden- und Gegenpartieinformationen sowie für firmeneigene Daten ergreifen, um sich vor unbefugter Offenlegung und unbefugtem Zugriff zu schützen. Dies beinhaltet die Beibehaltung des Eigentums, der Kontrolle und der Verwaltung aller Daten, die sich auf Kunden- und Gegenparteiinformationen, firmeneigene Daten und in der Cloud gehostete Services beziehen, einschließlich der Verwaltung der entsprechenden kryptografischen Schlüssel.	lambda-function-public-access-verboten	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass AWS Lambda-Funktionen nicht öffentlich zugänglich sind. Der öffentliche Zugriff kann möglicherweise die Verfügbarkeit von Ressourcen beeinträchtigen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.51	Ein Finanzinstitut muss bei der Nutzung von Cloud-Ser vices angemessene Sicherheitsvorkehr ungen für Kunden- und Gegenpart eiinformationen sowie für firmeneigene Daten ergreifen, um sich vor unbefugte r Offenlegung und unbefugtem Zugriff zu schützen. Dies beinhaltet die Beibehaltung des Eigentums, der Kontrolle und der Verwaltung aller Daten, die sich auf Kunden- und Gegenparteiinforma tionen, firmeneig ene Daten und in der Cloud gehostete Services beziehen, einschließlich der Verwaltung der entsprechenden kryptografischen Schlüssel.	lambda-inside-vpc	Stellen Sie AWS Lambda-Funktionen in einer Amazon Virtual Private Cloud (Amazon VPC) bereit, um eine sichere Kommunika tion zwischen einer Funktion und anderen Diensten innerhalb der Amazon VPC zu gewährleisten. Bei dieser Konfiguration sind kein Internet-Gateway, kein NAT-Gerät und keine VPN-Verbindung erforderlich. Der gesamte Datenverk ehr bleibt sicher in der Cloud. AWS Domains, die sich innerhalb einer VPC befinden, verfügen aufgrund ihrer logischen Isolierun g im Vergleich zu Domains mit öffentlic hen Endpunkten über eine zusätzliche Sicherheitsebene. Um den Zugriff ordnungsg emäß zu verwalten,

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			sollten AWS Lambda-Funktionen einer VPC zugewiesen werden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.51	Ein Finanzinstitut muss bei der Nutzung von Cloud-Ser vices angemessene Sicherheitsvorkehr ungen für Kunden- und Gegenpart eiinformationen sowie für firmeneigene Daten ergreifen, um sich vor unbefugte r Offenlegung und unbefugtem Zugriff zu schützen. Dies beinhaltet die Beibehaltung des Eigentums, der Kontrolle und der Verwaltung aller Daten, die sich auf Kunden- und Gegenparteiinforma tionen, firmeneig ene Daten und in der Cloud gehostete Services beziehen, einschließlich der Verwaltung der entsprechenden kryptografischen Schlüssel.	no-unrestricted-route-to-igw	Stellen Sie sicher, dass EC2 Amazon-Routentabellen keine uneingeschränkten Routen zu einem Internet-Gateway enthalten. Durch das Entfernen oder Beschränken des Internetzugangs für Workloads innerhalb von Amazon VPCs können unbeabsic htigte Zugriffe in Ihrer Umgebung reduziert werden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.51	Ein Finanzinstitut muss bei der Nutzung von Cloud-Services angemessene Sicherheitsvorkehrungen für Kunden- und Gegenpartieinformationen sowie für firmeneigene Daten ergreifen, um sich vor unbefugter Offenlegung und unbefugtem Zugriff zu schützen. Dies beinhaltet die Beibehaltung des Eigentums, der Kontrolle und der Verwaltung aller Daten, die sich auf Kunden- und Gegenparteiinformationen, firmeneigene Daten und in der Cloud gehostete Services beziehen, einschließlich der Verwaltung der entsprechenden kryptografischen Schlüssel.	opensearch-encrypted-at-rest	Da sensible Daten vorhanden sein können und um Daten im Ruhezustand zu schützen, sollten Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon OpenSearch Service-Domains aktiviert ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.51	Ein Finanzinstitut muss bei der Nutzung von Cloud-Services angemessene Sicherheitsvorkehrungen für Kunden- und Gegenpartei informationen sowie für firmeneigene Daten ergreifen, um sich vor unbefugter Offenlegung und unbefugtem Zugriff zu schützen. Dies beinhaltet die Beibehaltung des Eigentums, der Kontrolle und der Verwaltung aller Daten, die sich auf Kunden- und Gegenparteiinformationen, firmeneigene Daten und in der Cloud gehostete Services beziehen, einschließlich der Verwaltung der entsprechenden kryptografischen Schlüssel.	opensearch-https-required	Da sensible Daten existieren können und um Daten während der Übertragung zu schützen, sollten Sie sicherstellen, dass HTTPS für Verbindungen zu Ihren Amazon OpenSearch Service-Domains aktiviert ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.51	Ein Finanzinstitut muss bei der Nutzung von Cloud-Services angemessene Sicherheitsvorkehrungen für Kunden- und Gegenpartieiinformationen sowie für firmeneigene Daten ergreifen, um sich vor unbefugter Offenlegung und unbefugtem Zugriff zu schützen. Dies beinhaltet die Beibehaltung des Eigentums, der Kontrolle und der Verwaltung aller Daten, die sich auf Kunden- und Gegenparteiinformationen, firmeneigene Daten und in der Cloud gehostete Services beziehen, einschließlich der Verwaltung der entsprechenden kryptografischen Schlüssel.	opensearch-in-vpc-only	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass sich Amazon OpenSearch Service-Domains innerhalb einer Amazon Virtual Private Cloud (Amazon VPC) befinden. Eine Amazon OpenSearch Service-Domain innerhalb einer Amazon VPC ermöglicht die sichere Kommunikation zwischen Amazon OpenSearch Service und anderen Services innerhalb der Amazon VPC, ohne dass ein Internet-Gateway, ein NAT-Gerät oder eine VPN-Verbindung erforderlich ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.51	Ein Finanzinstitut muss bei der Nutzung von Cloud-Services angemessene Sicherheitsvorkehrungen für Kunden- und Gegenpartieinformationen sowie für firmeneigene Daten ergreifen, um sich vor unbefugter Offenlegung und unbefugtem Zugriff zu schützen. Dies beinhaltet die Beibehaltung des Eigentums, der Kontrolle und der Verwaltung aller Daten, die sich auf Kunden- und Gegenparteiinformationen, firmeneigene Daten und in der Cloud gehostete Services beziehen, einschließlich der Verwaltung der entsprechenden kryptografischen Schlüssel.	opensearch-node-to-node-Verschlüsselungsprüfung	Stellen Sie sicher, dass die node-to-node Verschlüsselung für Amazon OpenSearch Service aktiviert ist. Node-to-nodeVerschlüsselung ermöglicht die TLS 1.2-Verschlüsselung für die gesamte Kommunikation innerhalb der Amazon Virtual Private Cloud (Amazon VPC). Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.51	Ein Finanzinstitut muss bei der Nutzung von Cloud-Services angemessene Sicherheitsvorkehrungen für Kunden- und Gegenpartieinformationen sowie für firmeneigene Daten ergreifen, um sich vor unbefugter Offenlegung und unbefugtem Zugriff zu schützen. Dies beinhaltet die Beibehaltung des Eigentums, der Kontrolle und der Verwaltung aller Daten, die sich auf Kunden- und Gegenparteiinformationen, firmeneigene Daten und in der Cloud gehostete Services beziehen, einschließlich der Verwaltung der entsprechenden kryptografischen Schlüssel.	rds-instance-public-access-überprüfen	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Relational Database Service (Amazon RDS) -Instances nicht öffentlich sind. Amazon-RDS-Datenbank-Instances können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.51	Ein Finanzinstitut muss bei der Nutzung von Cloud-Services angemessene Sicherheitsvorkehrungen für Kunden- und Gegenpartieiinformationen sowie für firmeneigene Daten ergreifen, um sich vor unbefugter Offenlegung und unbefugtem Zugriff zu schützen. Dies beinhaltet die Beibehaltung des Eigentums, der Kontrolle und der Verwaltung aller Daten, die sich auf Kunden- und Gegenparteiinformationen, firmeneigene Daten und in der Cloud gehostete Services beziehen, einschließlich der Verwaltung der entsprechenden kryptografischen Schlüssel.	rds-snapshots-public-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Relational Database Service (Amazon RDS) -Instances nicht öffentlich sind. Amazon-RDS-Datenbank-Instances können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.51	Ein Finanzinstitut muss bei der Nutzung von Cloud-Services angemessene Sicherheitsvorkehrungen für Kunden- und Gegenpartieiinformationen sowie für firmeneigene Daten ergreifen, um sich vor unbefugter Offenlegung und unbefugtem Zugriff zu schützen. Dies beinhaltet die Beibehaltung des Eigentums, der Kontrolle und der Verwaltung aller Daten, die sich auf Kunden- und Gegenparteiinformationen, firmeneigene Daten und in der Cloud gehostete Services beziehen, einschließlich der Verwaltung der entsprechenden kryptografischen Schlüssel.	rds-snapshot-encrypted	Stellen Sie sicher, dass die Verschlüsselung für Ihre Amazon Relational Database Service (Amazon RDS)-Snapshots aktiviert ist. Da sensible Daten auch im Ruhezustand vorhanden sein können, sollten Sie die Verschlüsselung von Daten im Ruhezustand aktivieren, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10,51	Ein Finanzinstitut muss bei der Nutzung von Cloud-Services angemessene Sicherheitsvorkehrungen für Kunden- und Gegenpartieinformationen sowie für firmeneigene Daten ergreifen, um sich vor unbefugter Offenlegung und unbefugtem Zugriff zu schützen. Dies beinhaltet die Beibehaltung des Eigentums, der Kontrolle und der Verwaltung aller Daten, die sich auf Kunden- und Gegenparteiinformationen, firmeneigene Daten und in der Cloud gehostete Services beziehen, einschließlich der Verwaltung der entsprechenden kryptografischen Schlüssel.	rds-storage-encrypted	Zum Schutz von Daten im Ruhezustand müssen Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon Relational Database Service (Amazon RDS)-Instances aktiviert ist. Da sensible Daten in Amazon-RDS-Instances gespeichert werden können, sollten Sie die Verschlüsselung von Daten im Ruhezustand aktivieren, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10,51	Ein Finanzinstitut muss bei der Nutzung von Cloud-Services angemessene Sicherheitsvorkehrungen für Kunden- und Gegenpartei informationen sowie für firmeneigene Daten ergreifen, um sich vor unbefugter Offenlegung und unbefugtem Zugriff zu schützen. Dies beinhaltet die Beibehaltung des Eigentums, der Kontrolle und der Verwaltung aller Daten, die sich auf Kunden- und Gegenparteiinformationen, firmeneigene Daten und in der Cloud gehostete Services beziehen, einschließlich der Verwaltung der entsprechenden kryptografischen Schlüssel.	redshift-cluster-configuration-check	Um Daten im Ruhezustand zu schützen, muss die Verschlüsselung für Ihre Amazon-Redshift-Cluster aktiviert sein. Sie müssen auch sicherstellen, dass die erforderlichen Konfigurationen auf Amazon-Redshift-Clustern bereitgestellt werden. Die Prüfungsprotokollierung muss aktiviert sein, um Informationen zu Verbindungen und Benutzeraktivitäten in der Datenbank bereitzustellen. Diese Regel erfordert, dass ein Wert für clusterDbEncrypted (Config Default: TRUE) und LoggingEnabled (Config Default: TRUE) gesetzt ist. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.51	Ein Finanzinstitut muss bei der Nutzung von Cloud-Ser vices angemessene Sicherheitsvorkehr ungen für Kunden- und Gegenpart eiinformationen sowie für firmeneigene Daten ergreifen, um sich vor unbefugte r Offenlegung und unbefugtem Zugriff zu schützen. Dies beinhaltet die Beibehaltung des Eigentums, der Kontrolle und der Verwaltung aller Daten, die sich auf Kunden- und Gegenparteiinforma tionen, firmeneig ene Daten und in der Cloud gehostete Services beziehen, einschließlich der Verwaltung der entsprechenden kryptografischen Schlüssel.	redshift-cluster-kms-enabled	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass die Verschlüs selung mit AWS Key Management Service (AWS KMS) für Ihren Amazon Redshift Redshift-Cluster aktiviert ist. Um eventuell vorhanden e sensible Daten im Ruhezustand in Redshift-Clustern zu schützen, muss die Verschlüsselung von Daten im Ruhezusta nd aktiviert sein.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.51	Ein Finanzinstitut muss bei der Nutzung von Cloud-Services angemessene Sicherheitsvorkehrungen für Kunden- und Gegenpartei informationen sowie für firmeneigene Daten ergreifen, um sich vor unbefugter Offenlegung und unbefugtem Zugriff zu schützen. Dies beinhaltet die Beibehaltung des Eigentums, der Kontrolle und der Verwaltung aller Daten, die sich auf Kunden- und Gegenparteiinformationen, firmeneigene Daten und in der Cloud gehostete Services beziehen, einschließlich der Verwaltung der entsprechenden kryptografischen Schlüssel.	redshift-cluster-public-access-überprüfen	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Redshift Redshift-Cluster nicht öffentlich sind. Amazon-Redshift-Cluster können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.51	Ein Finanzinstitut muss bei der Nutzung von Cloud-Services angemessene Sicherheitsvorkehrungen für Kunden- und Gegenpartieinformationen sowie für firmeneigene Daten ergreifen, um sich vor unbefugter Offenlegung und unbefugtem Zugriff zu schützen. Dies beinhaltet die Beibehaltung des Eigentums, der Kontrolle und der Verwaltung aller Daten, die sich auf Kunden- und Gegenparteiinformationen, firmeneigene Daten und in der Cloud gehostete Services beziehen, einschließlich der Verwaltung der entsprechenden kryptografischen Schlüssel.	redshift-enhanced-vpc-routing-aktiviert	Mit Enhanced-VPC-Routing wird erzwungen, dass der gesamte COPY- und UNLOAD-Datenverkehr zwischen Ihrem Cluster und Datenrepositorys über Ihre Amazon VPC erfolgt. Anschließend können Sie VPC-Features wie Sicherheitsgruppen und Netzwerkzugriffskontrolllisten verwenden, um den Netzwerkverkehr zu schützen. Sie können auch VPC-Flow-Protokolle verwenden, um den Netzwerkverkehr zu überwachen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10,51	Ein Finanzinstitut muss bei der Nutzung von Cloud-Ser vices angemessene Sicherheitsvorkehr ungen für Kunden- und Gegenpart eiinformationen sowie für firmeneigene Daten ergreifen, um sich vor unbefugte r Offenlegung und unbefugtem Zugriff zu schützen. Dies beinhaltet die Beibehaltung des Eigentums, der Kontrolle und der Verwaltung aller Daten, die sich auf Kunden- und Gegenparteiinforma tionen, firmeneig ene Daten und in der Cloud gehostete Services beziehen, einschließlich der Verwaltung der entsprechenden kryptografischen Schlüssel.	redshift-require-tls-ssl	Stellen Sie sicher, dass Ihre Amazon-Redshift-Cluster eine TLS/SSL-Verschlüss elung erfordern, um eine Verbindung zu SQL-Clients herzustel len. Da sensible Daten vorhanden sein können, sollten Sie die Verschlüsselung bei der Übertragung aktivieren, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10,51	Ein Finanzinstitut muss bei der Nutzung von Cloud-Services angemessene Sicherheitsvorkehrungen für Kunden- und Gegenpartieinformationen sowie für firmeneigene Daten ergreifen, um sich vor unbefugter Offenlegung und unbefugtem Zugriff zu schützen. Dies beinhaltet die Beibehaltung des Eigentums, der Kontrolle und der Verwaltung aller Daten, die sich auf Kunden- und Gegenparteiinformationen, firmeneigene Daten und in der Cloud gehostete Services beziehen, einschließlich der Verwaltung der entsprechenden kryptografischen Schlüssel.	root-account-hardware-mfa-aktiviert	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Hardware-MFA für den Root-Benutzer aktiviert ist. Der Stammbenutzer ist der AWS-Konto-Benutzer mit den meisten Berechtigungen. MFA bietet eine weitere Schutzebene zusätzlich zum Benutzernamen und Passwort. Indem Sie MFA für den Root-Benutzer vorschreiben, können Sie die Anzahl AWS-Konten kompromittierter Benutzer reduzieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.51	Ein Finanzinstitut muss bei der Nutzung von Cloud-Services angemessene Sicherheitsvorkehrungen für Kunden- und Gegenpartei informationen sowie für firmeneigene Daten ergreifen, um sich vor unbefugter Offenlegung und unbefugtem Zugriff zu schützen. Dies beinhaltet die Beibehaltung des Eigentums, der Kontrolle und der Verwaltung aller Daten, die sich auf Kunden- und Gegenparteiinformationen, firmeneigene Daten und in der Cloud gehostete Services beziehen, einschließlich der Verwaltung der entsprechenden kryptografischen Schlüssel.	root-account-mfa-enabled	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass MFA für den Root-Benutzer aktiviert ist. Der Stammbenutzer ist der AWS-Konto-Benutzer mit den meisten Berechtigungen. MFA bietet eine weitere Schutzebene zusätzlich zum Benutzernamen und Passwort. Indem Sie MFA für den Root-Benutzer vorschreiben, können Sie die Anzahl AWS-Konten kompromittierter Benutzer reduzieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.51	Ein Finanzinstitut muss bei der Nutzung von Cloud-Services angemessene Sicherheitsvorkehrungen für Kunden- und Gegenpartieiinformationen sowie für firmeneigene Daten ergreifen, um sich vor unbefugter Offenlegung und unbefugtem Zugriff zu schützen. Dies beinhaltet die Beibehaltung des Eigentums, der Kontrolle und der Verwaltung aller Daten, die sich auf Kunden- und Gegenparteiinformationen, firmeneigene Daten und in der Cloud gehostete Services beziehen, einschließlich der Verwaltung der entsprechenden kryptografischen Schlüssel.	s3-Blöcke-periodisch account-level-public-access	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Simple Storage Service (Amazon S3) -Buckets nicht öffentlich zugänglich sind. Diese Regel trägt dazu bei, sensible Daten vor unbefugten Remote-Benutzern zu schützen, indem sie den öffentlichen Zugriff verhindert. Mit dieser Regel können Sie optional die Parameter ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) und restrictPublicBuckets Parameter (Config Default: True) festlegen. Die tatsächlichen Werte müssen den Richtlini

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			en Ihrer Organisation entsprechen.
10.51	Ein Finanzinstitut muss bei der Nutzung von Cloud-Services angemessene Sicherheitsvorkehrungen für Kunden- und Gegenpartei informationen sowie für firmeneigene Daten ergreifen, um sich vor unbefugter Offenlegung und unbefugtem Zugriff zu schützen. Dies beinhaltet die Beibehaltung des Eigentums, der Kontrolle und der Verwaltung aller Daten, die sich auf Kunden- und Gegenparteiinformationen, firmeneigene Daten und in der Cloud gehostete Services beziehen, einschließlich der Verwaltung der entsprechenden kryptografischen Schlüssel.	s-3 bucket-public-read-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie nur autorisierten Benutzern, Prozessen und Geräten Zugriff auf Amazon Simple Storage Service (Amazon S3) - Buckets gewähren. Die Verwaltung des Zugriffs sollte mit der Klassifizierung der Daten übereinstimmen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.51	Ein Finanzinstitut muss bei der Nutzung von Cloud-Services angemessene Sicherheitsvorkehrungen für Kunden- und Gegenpartieiinformationen sowie für firmeneigene Daten ergreifen, um sich vor unbefugter Offenlegung und unbefugtem Zugriff zu schützen. Dies beinhaltet die Beibehaltung des Eigentums, der Kontrolle und der Verwaltung aller Daten, die sich auf Kunden- und Gegenparteiinformationen, firmeneigene Daten und in der Cloud gehostete Services beziehen, einschließlich der Verwaltung der entsprechenden kryptografischen Schlüssel.	s-3 bucket-public-write-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie nur autorisierten Benutzern, Prozessen und Geräten Zugriff auf Amazon Simple Storage Service (Amazon S3) - Buckets gewähren. Die Verwaltung des Zugriffs sollte mit der Klassifizierung der Daten übereinstimmen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.51	Ein Finanzinstitut muss bei der Nutzung von Cloud-Services angemessene Sicherheitsvorkehrungen für Kunden- und Gegenpartei informationen sowie für firmeneigene Daten ergreifen, um sich vor unbefugter Offenlegung und unbefugtem Zugriff zu schützen. Dies beinhaltet die Beibehaltung des Eigentums, der Kontrolle und der Verwaltung aller Daten, die sich auf Kunden- und Gegenparteiinformationen, firmeneigene Daten und in der Cloud gehostete Services beziehen, einschließlich der Verwaltung der entsprechenden kryptografischen Schlüssel.	s3-fähig bucket-server-side-encryption	Zum Schutz von Daten im Ruhezustand müssen Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon Simple Storage Service (Amazon S3)-Buckets aktiviert ist. Da sensible Daten in Amazon-S3-Buckets gespeichert werden können, sollten Sie die Verschlüsselung aktivieren, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.51	Ein Finanzinstitut muss bei der Nutzung von Cloud-Services angemessene Sicherheitsvorkehrungen für Kunden- und Gegenpartieinformationen sowie für firmeneigene Daten ergreifen, um sich vor unbefugter Offenlegung und unbefugtem Zugriff zu schützen. Dies beinhaltet die Beibehaltung des Eigentums, der Kontrolle und der Verwaltung aller Daten, die sich auf Kunden- und Gegenparteiinformationen, firmeneigene Daten und in der Cloud gehostete Services beziehen, einschließlich der Verwaltung der entsprechenden kryptografischen Schlüssel.	s-3 bucket-ssl-requests-only	Um Daten während der Übertragung zu schützen, stellen Sie sicher, dass Ihre Amazon Simple Storage Service (Amazon S3)-Buckets Anfragen zur Verwendung von Secure Socket Layer (SSL)-Buckets erfordern. Da sensible Daten vorhanden sein können, sollten Sie die Verschlüsselung bei der Übertragung aktivieren, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10,51	Ein Finanzinstitut muss bei der Nutzung von Cloud-Services angemessene Sicherheitsvorkehrungen für Kunden- und Gegenpartieinformationen sowie für firmeneigene Daten ergreifen, um sich vor unbefugter Offenlegung und unbefugtem Zugriff zu schützen. Dies beinhaltet die Beibehaltung des Eigentums, der Kontrolle und der Verwaltung aller Daten, die sich auf Kunden- und Gegenparteiinformationen, firmeneigene Daten und in der Cloud gehostete Services beziehen, einschließlich der Verwaltung der entsprechenden kryptografischen Schlüssel.	s-3 default-encryption-kms	Stellen Sie sicher, dass die Verschlüsselung für Ihre Amazon Simple Storage Service (Amazon S3)-Buckets aktiviert ist. Da sensible Daten in einem Amazon-S3-Bucket gespeichert werden können, sollten Sie die Verschlüsselung im Ruhezustand aktivieren, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10,51	Ein Finanzinstitut muss bei der Nutzung von Cloud-Services angemessene Sicherheitsvorkehrungen für Kunden- und Gegenpartieinformationen sowie für firmeneigene Daten ergreifen, um sich vor unbefugter Offenlegung und unbefugtem Zugriff zu schützen. Dies beinhaltet die Beibehaltung des Eigentums, der Kontrolle und der Verwaltung aller Daten, die sich auf Kunden- und Gegenparteiinformationen, firmeneigene Daten und in der Cloud gehostete Services beziehen, einschließlich der Verwaltung der entsprechenden kryptografischen Schlüssel.	sagemaker-endpoint-configuration-kms-schlüsselkonfiguriert	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass die Verschlüsselung mit dem AWS Key Management Service (AWS KMS) für Ihren Endpunkt aktiviert ist. SageMaker Da sensible Daten auf dem SageMaker Endgerät gespeichert werden können, sollten Sie die Verschlüsselung im Ruhezustand aktivieren, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.51	Ein Finanzinstitut muss bei der Nutzung von Cloud-Services angemessene Sicherheitsvorkehrungen für Kunden- und Gegenpartieinformationen sowie für firmeneigene Daten ergreifen, um sich vor unbefugter Offenlegung und unbefugtem Zugriff zu schützen. Dies beinhaltet die Beibehaltung des Eigentums, der Kontrolle und der Verwaltung aller Daten, die sich auf Kunden- und Gegenparteiinformationen, firmeneigene Daten und in der Cloud gehostete Services beziehen, einschließlich der Verwaltung der entsprechenden kryptografischen Schlüssel.	sagemaker-notebook-instance-kms-schlüsselkonfiguriert	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass die Verschlüsselung mit dem AWS Key Management Service (AWS KMS) für Ihr Notebook aktiviert ist. SageMaker Da vertrauliche Daten im SageMaker Notebook gespeichert werden können, sollten Sie die Verschlüsselung im Ruhezustand aktivieren, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.51	Ein Finanzinstitut muss bei der Nutzung von Cloud-Services angemessene Sicherheitsvorkehrungen für Kunden- und Gegenpartei informationen sowie für firmeneigene Daten ergreifen, um sich vor unbefugter Offenlegung und unbefugtem Zugriff zu schützen. Dies beinhaltet die Beibehaltung des Eigentums, der Kontrolle und der Verwaltung aller Daten, die sich auf Kunden- und Gegenparteiinformationen, firmeneigene Daten und in der Cloud gehostete Services beziehen, einschließlich der Verwaltung der entsprechenden kryptografischen Schlüssel.	sagemaker-notebook-no-direct-Internetzugang	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass SageMaker Amazon-Notebooks keinen direkten Internetzugang zulassen. Indem Sie direkten Internetzugang blockieren, vermeiden Sie, dass unbefugte Benutzer auf sensible Daten zugreifen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.51	Ein Finanzinstitut muss bei der Nutzung von Cloud-Services angemessene Sicherheitsvorkehrungen für Kunden- und Gegenpartieiinformationen sowie für firmeneigene Daten ergreifen, um sich vor unbefugter Offenlegung und unbefugtem Zugriff zu schützen. Dies beinhaltet die Beibehaltung des Eigentums, der Kontrolle und der Verwaltung aller Daten, die sich auf Kunden- und Gegenparteiinformationen, firmeneigene Daten und in der Cloud gehostete Services beziehen, einschließlich der Verwaltung der entsprechenden kryptografischen Schlüssel.	sns-encrypted-kms	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass Ihre Amazon Simple Notification Service (Amazon SNS) -Themen mit dem AWS Key Management Service (AWS KMS) verschlüsselt werden müssen. Um eventuell vorhandene sensible Daten im Ruhezustand in veröffentlichten Nachrichten zu schützen, muss die Verschlüsselung von Daten im Ruhezustand aktiviert sein.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.51	Ein Finanzinstitut muss bei der Nutzung von Cloud-Services angemessene Sicherheitsvorkehrungen für Kunden- und Gegenpartieinformationen sowie für firmeneigene Daten ergreifen, um sich vor unbefugter Offenlegung und unbefugtem Zugriff zu schützen. Dies beinhaltet die Beibehaltung des Eigentums, der Kontrolle und der Verwaltung aller Daten, die sich auf Kunden- und Gegenparteiinformationen, firmeneigene Daten und in der Cloud gehostete Services beziehen, einschließlich der Verwaltung der entsprechenden kryptografischen Schlüssel.	ssm-document-not-public	Stellen Sie sicher, dass AWS Systems Manager (SSM) - Dokumente nicht öffentlich sind, da dies einen unbeabsichtigten Zugriff auf Ihre SSM-Dokumente ermöglichen kann. Ein öffentliches SSM-Dokument kann Informationen über Ihr Konto, Ihre Ressourcen und internen Prozesse preisgeben.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.51	Ein Finanzinstitut muss bei der Nutzung von Cloud-Ser vices angemessene Sicherheitsvorkehr ungen für Kunden- und Gegenpart eiinformationen sowie für firmeneigene Daten ergreifen, um sich vor unbefugte r Offenlegung und unbefugtem Zugriff zu schützen. Dies beinhaltet die Beibehaltung des Eigentums, der Kontrolle und der Verwaltung aller Daten, die sich auf Kunden- und Gegenparteiinforma tionen, firmeneig ene Daten und in der Cloud gehostete Services beziehen, einschließlich der Verwaltung der entsprechenden kryptografischen Schlüssel.	subnet-auto-assign-public-ip-deaktiviert	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon Virtual Private Cloud (VPC) -Subnetzen nicht automatisch eine öffentliche IP-Adress e zugewiesen wird. Amazon Elastic Compute Cloud (EC2) -Instances, die in Subnetzen gestartet werden, in denen dieses Attribut aktiviert ist, haben ihrer primären Netzwerkschnittste lle eine öffentliche IP-Adresse zugewiesen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.52	Ein Finanzinstitut muss angemessene Zugangskontrollen für die Identifizierung, Authentifizierung und Autorisierung von Benutzern (interne und externe Nutzer wie Drittanbieter) einführen. Dabei muss es sowohl um logische als auch um physische Zugriffskontrollen für Technologien gehen, die dem Risiko eines unbefugten Zugriffs auf seine Technologiesysteme angemessen sind.	access-keys-rotated	Die Anmeldeinformationen für autorisierte Geräte, Benutzer und Prozesse werden geprüft, indem sichergestellt wird, dass die IAM-Zugriffsschlüssel entsprechend den Vorgaben der Unternehmensrichtlinie rotiert werden. Das regelmäßige Ändern der Zugriffsschlüssel ist eine bewährte Sicherheitsmethode. Es verkürzt den Zeitraum, in dem ein Zugriffsschlüssel aktiv ist, und reduziert die Auswirkungen auf das Unternehmen, wenn die Schlüssel kompromittiert werden. Diese Regel erfordert einen Wert für die Zugriffsschlüssel-Rotation (Standard konfiguration: 90). Der tatsächliche Wert muss den Richtlini

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			en Ihrer Organisation entsprechen.
10.52	Ein Finanzinstitut muss angemessene Zugangskontrollen für die Identifizierung, Authentifizierung und Autorisierung von Benutzern (interne und externe Nutzer wie Drittanbieter) einführen. Dabei muss es sowohl um logische als auch um physische Zugriffskontrollen für Technologien gehen, die dem Risiko eines unbefugten Zugriffs auf seine Technologiesysteme angemessen sind.	account-part-of-organizations	Durch die zentrale Verwaltung AWS-Konten innerhalb von AWS Organizations wird sichergestellt, dass die Konten den Vorschriften entsprechen. Eine fehlende zentrale Kontoverwaltung kann zu inkonsistenten Kontokonfigurationen führen, wodurch Ressourcen und sensible Daten offengelegt werden können.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.52	Ein Finanzinstitut muss angemessene Zugangskontrollen für die Identifizierung, Authentifizierung und Autorisierung von Benutzern (interne und externe Nutzer wie Drittanbieter) einführen. Dabei muss es sowohl um logische als auch um physische Zugriffskontrollen für Technologien gehen, die dem Risiko eines unbefugten Zugriffs auf seine Technologiesysteme angemessen sind.	ec-2 instance-profile-attached	EC2 Instanzprofile übergeben eine IAM-Rolle an eine EC2 Instance. Das Anhängen eines Instance-Profils an Ihre Instances kann bei der Implementierung von geringsten Berechtigungen und der Berechtigungsverwaltung helfen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.52	Ein Finanzinstitut muss angemessene Zugangskontrollen für die Identifizierung, Authentifizierung und Autorisierung von Benutzern (interne und externe Nutzer wie Drittanbieter) einführen. Dabei muss es sowohl um logische als auch um physische Zugriffskontrollen für Technologien gehen, die dem Risiko eines unbefugten Zugriffs auf seine Technologiesysteme angemessen sind.	emr-kerberos-enabled	Die Zugriffsberechtigungen und -autorisierungen können verwaltet und nach den Prinzipien der geringsten Berechtigung und Aufgabentrennung integriert werden, indem Kerberos für Amazon-EMR-Cluster aktiviert wird. In Kerberos werden Services und Benutzer, die sich authentifizieren müssen, als Prinzipale bezeichnet. Prinzipale befinden sich in einem Kerberos-Bereich. Innerhalb dieses Bereichs wird ein Kerberos-Server als Key Distribution Center (KDC) bezeichnet. Über diesen Server können sich Prinzipale authentifizieren. Die Authentifizierung im KDC erfolgt durch die Ausstellung von Authentif

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			izierungstickets. Das KDC unterhält eine Datenbank der Prinzipale in seinem Bereich mit ihren Passwörtern und anderen administr ativen Informationen zu jedem Prinzipal.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.52	Ein Finanzinstitut muss angemessene Zugangskontrollen für die Identifizierung, Authentifizierung und Autorisierung von Benutzern (interne und externe Nutzer wie Drittanbieter) einführen. Dabei muss es sowohl um logische als auch um physische Zugriffskontrollen für Technologien gehen, die dem Risiko eines unbefugten Zugriffs auf seine Technologiesysteme angemessen sind.	iam-customer-policy-blocked-KMS-Aktionen	AWS Identity and Access Management (IAM) kann Ihnen helfen, die Prinzipien der geringsten Rechte und der Aufgabentrennung in Zugriffsberechtigungen und Autorisierungen zu integrieren und so zu verhindern, dass Richtlinien blockierte Aktionen für alle AWS Schlüssel des Key Management Service enthalten. Wenn Benutzer mehr Rechte haben, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und Aufgabentrennung verstoßen. Mit dieser Regel können Sie den Parameter festlegen. blockedActionsPatterns (Wert „AWS Bewährte grundlegende Sicherheitsmethoden“: kms:

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			Decrypt, kms:ReEncryptFrom). Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.
10,52	Ein Finanzinstitut muss angemessene Zugangskontrollen für die Identifizierung, Authentifizierung und Autorisierung von Benutzern (interne und externe Nutzer wie Drittanbieter) einführen. Dabei muss es sowohl um logische als auch um physische Zugriffskontrollen für Technologien gehen, die dem Risiko eines unbefugten Zugriffs auf seine Technologiesysteme angemessen sind.	iam-no-inline-policy-überprüfen	Stellen Sie sicher, dass ein Benutzer, eine IAM-Rolle oder eine IAM-Gruppe (AWS Identity and Access Management) nicht über eine Inline-Richtlinie zur Zugriffskontrolle auf Systeme und Ressourcen verfügt. AWS empfiehlt, verwaltete Richtlinien anstelle von Inline-Richtlinien zu verwenden. Verwaltete Richtlinien ermöglichen Wiederverwendbarkeit, Versionsverwaltung, Rollback und Delegierung der Berechtigungsverwaltung.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.52	Ein Finanzinstitut muss angemessene Zugangskontrollen für die Identifizierung, Authentifizierung und Autorisierung von Benutzern (interne und externe Nutzer wie Drittanbieter) einführen. Dabei muss es sowohl um logische als auch um physische Zugriffskontrollen für Technologien gehen, die dem Risiko eines unbefugten Zugriffs auf seine Technologiesysteme angemessen sind.	iam-password-policy	Die Identitäten und Anmeldeinformationen werden auf der Grundlage einer organisatorischen IAM-Passwortrichtlinie ausgestellt, verwaltet und verifiziert. Sie erfüllen oder übertreffen die Anforderungen des NIST SP 800-63 und des AWS Foundational Security Best Practices-Standards für Passwortstärke. Mit dieser Regel können Sie optional RequireUppercaseCharacters (Wert für AWS grundlegende Sicherheitsbewährte Methoden: wahr), RequireLowercaseCharacters (Wert für bewährte Methoden für AWS grundlegende Sicherheit: wahr), RequireSymbols (Wert für bewährte Methoden für AWS grundlegende Sicherheit:

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			wahr), RequireNumbers (Wert für bewährte Methoden für AWS grundlegende Sicherheit: wahr), MinimumPasswordLength (Wert für bewährte Methoden für AWS grundlegende Sicherheit: 14), PasswordReusePrevention (Wert für bewährte Methoden für AWS grundlegende Sicherheit: 24) und MaxPasswordAge (Wert für bewährte Methoden für AWS grundlegende Sicherheit: 90) für Ihr IAM festlegen Kennwortrichtlinie. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.52	Ein Finanzinstitut muss angemessene Zugangskontrollen für die Identifizierung, Authentifizierung und Autorisierung von Benutzern (interne und externe Nutzer wie Drittanbieter) einführen. Dabei muss es sowohl um logische als auch um physische Zugriffskontrollen für Technologien gehen, die dem Risiko eines unbefugten Zugriffs auf seine Technologiesysteme angemessen sind.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) kann Ihnen dabei helfen, die Prinzipien der geringsten Rechte und der Aufgabentrennung in Zugriffsberechtigungen und Autorisierungen zu integrieren und so zu verhindern, dass Richtlinien „Effect“: „Allow“ mit „Action“: „*“ anstelle von „Resource“: „*“ enthalten. Wenn Benutzern mehr Rechte eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und der Aufgabentrennung verstoßen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10,52	Ein Finanzinstitut muss angemessene Zugangskontrollen für die Identifizierung, Authentifizierung und Autorisierung von Benutzern (interne und externe Nutzer wie Drittanbieter) einführen. Dabei muss es sowohl um logische als auch um physische Zugriffskontrollen für Technologien gehen, die dem Risiko eines unbefugten Zugriffs auf seine Technolog iesysteme angemesse n sind.	iam-root-access-key-überprüfen	Der Zugriff auf Systeme und Ressourcen kann gesteuert werden, indem überprüft wird, ob der Root-Benu tzer keine Zugriffss chlüssel mit seiner AWS Identity and Access Management (IAM) -Rolle verknüpft hat. Stellen Sie sicher, dass die Root-Zugr iffsschlüssel gelöscht werden. Erstellen und verwenden Sie stattdessen rollenbas ierte Funktionen, AWS-Konten um das Prinzip der geringste n Funktionalität zu berücksichtigen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.52	Ein Finanzinstitut muss angemessene Zugangskontrollen für die Identifizierung, Authentifizierung und Autorisierung von Benutzern (interne und externe Nutzer wie Drittanbieter) einführen. Dabei muss es sowohl um logische als auch um physische Zugriffskontrollen für Technologien gehen, die dem Risiko eines unbefugten Zugriffs auf seine Technologiesysteme angemessen sind.	iam-user-group-membership-überprüfen	AWS Identity and Access Management (IAM) kann Ihnen helfen, Zugriffsberechtigungen und Autorisierungen einzuschränken, indem sichergestellt wird, dass IAM-Benutzer Mitglieder mindestens einer Gruppe sind. Wenn Benutzern mehr Berechtigungen eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und Aufgabentrennung verstoßen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.52	Ein Finanzinstitut muss angemessene Zugangskontrollen für die Identifizierung, Authentifizierung und Autorisierung von Benutzern (interne und externe Nutzer wie Drittanbieter) einführen. Dabei muss es sowohl um logische als auch um physische Zugriffskontrollen für Technologien gehen, die dem Risiko eines unbefugten Zugriffs auf seine Technologiesysteme angemessen sind.	iam-user-mfa-enabled	Aktivieren Sie diese Regel, um den Zugriff auf Ressourcen in der AWS Cloud einzuschränken. Diese Regel stellt sicher, dass die Multi-Faktor-Authentifizierung (MFA) für alle IAM-Benutzer aktiviert ist. MFA bietet eine weitere Schutzebene zusätzlich zum Benutzernamen und Passwort. Reduzieren Sie Fälle von kompromittierten Konten, indem Sie MFA für IAM-Benutzer vorschreiben.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.52	Ein Finanzinstitut muss angemessene Zugangskontrollen für die Identifizierung, Authentifizierung und Autorisierung von Benutzern (interne und externe Nutzer wie Drittanbieter) einführen. Dabei muss es sowohl um logische als auch um physische Zugriffskontrollen für Technologien gehen, die dem Risiko eines unbefugten Zugriffs auf seine Technolog iesysteme angemesse n sind.	iam-user-no-policies-überprüfen	Diese Regel stellt sicher, dass AWS Identity and Access Management (IAM) -Richtlinien nur Gruppen oder Rollen zugewiese n werden, um den Zugriff auf Systeme und Ressourcen zu kontrollieren. Die Zuweisung von Berechtig ungen auf Gruppen- oder Rollenebene trägt dazu bei, die Wahrscheinlichkeit zu verringern, dass eine Identität übermäßige Berechtigungen erhält oder beibehält.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.52	Ein Finanzinstitut muss angemessene Zugangskontrollen für die Identifizierung, Authentifizierung und Autorisierung von Benutzern (interne und externe Nutzer wie Drittanbieter) einführen. Dabei muss es sowohl um logische als auch um physische Zugriffskontrollen für Technologien gehen, die dem Risiko eines unbefugten Zugriffs auf seine Technologiesysteme angemessen sind.	iam-user-unused-credentials-überprüfen	AWS Identity and Access Management (IAM) kann Ihnen bei Zugriffsberechtigungen und Autorisierungen helfen, indem es nach IAM-Passwörtern und Zugriffsschlüsseln sucht, die für einen bestimmten Zeitraum nicht verwendet wurden. Wenn ungenutzte Anmeldeinformationen identifiziert werden, müssen Sie sie deaktivieren und/oder entfernen, da dies gegen das Prinzip der geringsten Berechtigung verstoßen könnte. Für diese Regel müssen Sie einen Wert für das maxCredentialUsage Alter festlegen (Standardkonfiguration: 90). Der tatsächliche Wert muss den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.52	Ein Finanzinstitut muss angemessene Zugangskontrollen für die Identifizierung, Authentifizierung und Autorisierung von Benutzern (interne und externe Nutzer wie Drittanbieter) einführen. Dabei muss es sowohl um logische als auch um physische Zugriffskontrollen für Technologien gehen, die dem Risiko eines unbefugten Zugriffs auf seine Technologiesysteme angemessen sind.	root-account-hardware-mfa-aktiviert	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Hardware-MFA für den Root-Benutzer aktiviert ist. Der Stammbenutzer ist der AWS-Konto-Benutzer mit den meisten Berechtigungen. MFA bietet eine weitere Schutzebene zusätzlich zum Benutzernamen und Passwort. Indem Sie MFA für den Root-Benutzer vorschreiben, können Sie die Anzahl AWS-Konten kompromittierter Benutzer reduzieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.52	Ein Finanzinstitut muss angemessene Zugangskontrollen für die Identifizierung, Authentifizierung und Autorisierung von Benutzern (interne und externe Nutzer wie Drittanbieter) einführen. Dabei muss es sowohl um logische als auch um physische Zugriffskontrollen für Technologien gehen, die dem Risiko eines unbefugten Zugriffs auf seine Technologiesysteme angemessen sind.	root-account-mfa-enabled	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass MFA für den Root-Benutzer aktiviert ist. Der Stammbenutzer ist der AWS-Konto-Benutzer mit den meisten Berechtigungen. MFA bietet eine weitere Schutzebene zusätzlich zum Benutzernamen und Passwort. Indem Sie MFA für den Root-Benutzer vorschreiben, können Sie die Anzahl AWS-Konten kompromittierter Benutzer reduzieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.53(b)(h)(i)	Bei der Einhaltung von Ziffer 10.52 sollte ein Finanzinstitut in seiner Zugriffskontrollpolitik die folgenden Grundsätze berücksichtigen: (b) Zugriffsrechte mit den geringsten Rechten oder auf einer need-to-have „Basis, bei der legitimen Benutzer nur die Mindestberechtigungen gewährt werden, um ihre Aufgaben wahrzunehmen; (h) die gemeinsame Nutzung von Benutzer-IDs und Passwörtern durch mehrere Benutzer einschränken und kontrollieren; und (i) die Verwendung generischer Benennungskonventionen für Benutzer-IDs zugunsten einer persönlicheren Identifizierung kontrollieren IDs.	iam-root-access-key-check	Der Zugriff auf Systeme und Ressourcen kann gesteuert werden, indem überprüft wird, ob der Root-Benutzer keine Zugriffsschlüssel mit seiner AWS Identity and Access Management (IAM) -Rolle verknüpft hat. Stellen Sie sicher, dass die Root-Zugriffsschlüssel gelöscht werden. Erstellen und verwenden Sie stattdessen rollenbasierte Funktionen, AWS-Konten um das Prinzip der geringsten Funktionalität zu berücksichtigen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.53(b)	Unter Beachtung von Ziffer 10.52 sollte ein Finanzins titut bei seiner Zugriffskontrolle die folgenden Grundsätz e berücksichtigen: (b) Zugangsrechte mit den geringsten Rechten oder auf der Basis von „“, wobei legitimen Benutzern nur die erforderlichen Mindestberechtigun gen zur Ausübung ihrer Aufgaben gewährt werden; need-to-have	ec-2 instance-profile-a ttached	EC2 Instanzprofile übergeben eine IAM-Rolle an eine EC2 Instance. Das Anhängen eines Instance-Profils an Ihre Instances kann bei der Implement ierung von geringste n Berechtigungen und der Berechtig ungsverwaltung helfen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.53(b)	Unter Beachtung von Ziffer 10.52 sollte ein Finanzinstitut bei seiner Zugriffskontrolle die folgenden Grundsätze berücksichtigen: (b) Zugriffsrechte mit den geringsten Rechten oder auf einer „need-to-have“ -Basis, bei der legitimen Benutzer nur die zur Ausübung ihrer Aufgaben erforderlichen Mindestberechtigungen gewährt werden;	emr-kerberos-enabled	Die Zugriffsberechtigungen und -autorisierungen können verwaltet und nach den Prinzipien der geringsten Berechtigung und Aufgabentrennung integriert werden, indem Kerberos für Amazon-EMR-Cluster aktiviert wird. In Kerberos werden Services und Benutzer, die sich authentifizieren müssen, als Prinzipale bezeichnet. Prinzipale befinden sich in einem Kerberos-Bereich. Innerhalb dieses Bereichs wird ein Kerberos-Server als Key Distribution Center (KDC) bezeichnet. Über diesen Server können sich Prinzipale authentifizieren. Die Authentifizierung im KDC erfolgt durch die Ausstellung von Authentif

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			izierungstickets. Das KDC unterhält eine Datenbank der Prinzipale in seinem Bereich mit ihren Passwörtern und anderen administr ativen Informationen zu jedem Prinzipal.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.53(b)	Bei der Einhaltung von Ziffer 10.52 sollte ein Finanzinstitut in seiner Zugriffskontrollpolitik die folgenden Grundsätze berücksichtigen: (b) Zugangsrechte mit den geringsten Rechten verwenden oder auf einer „need-to-have“ -Basis, bei der legitimen Benutzern nur die Mindestberechtigungen gewährt werden, die zur Ausübung ihrer Aufgaben ausreichen;	iam-customer-policy-blocked-KMS-Aktionen	AWS Identity and Access Management (IAM) kann Ihnen helfen, die Prinzipien der geringsten Rechte und der Aufgabentrennung in Zugriffsberechtigungen und Autorisierungen zu integrieren und so zu verhindern, dass Richtlinien blockierte Aktionen für alle AWS Schlüssel des Key Management Service enthalten. Wenn Benutzer mehr Rechte haben, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und Aufgabentrennung verstoßen. Mit dieser Regel können Sie den Parameter festlegen. blockedActionsPatterns (Wert „AWS Bewährte grundlegende Sicherheitsmethoden“: kms:

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			Decrypt, kms:ReEncryptFrom). Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.
10.53(b)	Unter Beachtung von Ziffer 10.52 sollte ein Finanzinstitut bei seiner Zugriffskontrolle die folgenden Grundsätze berücksichtigen: (b) Zugriffsrechte mit den geringsten Rechten oder auf einer „Basisneed-to-have“, bei der legitimen Benutzer nur die Mindestberechtigungen zur Ausübung ihrer Aufgaben gewährt werden;	iam-no-inline-policy-überprüfen	Stellen Sie sicher, dass ein Benutzer, eine IAM-Rolle oder eine IAM-Gruppe (AWS Identity and Access Management) nicht über eine Inline-Richtlinie zur Zugriffskontrolle auf Systeme und Ressourcen verfügt. AWS empfiehlt, verwaltete Richtlinien anstelle von Inline-Richtlinien zu verwenden. Verwaltete Richtlinien ermöglichen Wiederverwendbarkeit, Versionsverwaltung, Rollback und Delegierung der Berechtigungsverwaltung.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.53(b)	Unter Beachtung von Ziffer 10.52 sollte ein Finanzinstitut bei seinen Zugriffskontrollen die folgenden Grundsätze berücksichtigen: (b) Zugangsrechte mit den geringsten Rechten oder auf einer „need-to-have“-Basis verwenden, bei der legitimen Benutzer nur die geringsten Rechte erhalten, die zur Ausübung ihrer Aufgaben ausreichen;	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) kann Ihnen dabei helfen, die Prinzipien der geringsten Rechte und der Aufgabentrennung in Zugriffsberechtigungen und Autorisierungen zu integrieren und so zu verhindern, dass Richtlinien „Effect“: „Allow“ mit „Action“: „*“ anstelle von „Resource“: „*“ enthalten. Wenn Benutzern mehr Rechte eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und der Aufgabentrennung verstoßen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.53(b)	Bei der Einhaltung von Ziffer 10.52 sollte ein Finanzinstitut in seiner Zugriffskontrollpolitik die folgenden Grundsätze berücksichtigen: (b) Zugangsrechte mit den geringsten Rechten verwenden oder auf einer „need-to-have“ -Basis, bei der legitimen Benutzern nur die Mindestberechtigungen gewährt werden, die zur Ausübung ihrer Aufgaben ausreichen;	iam-user-group-membership-überprüfen	AWS Identity and Access Management (IAM) kann Ihnen helfen, Zugriffsberechtigungen und Autorisierungen einzuschränken, indem sichergestellt wird, dass IAM-Benutzer Mitglieder mindestens einer Gruppe sind. Wenn Benutzern mehr Berechtigungen eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und Aufgabentrennung verstoßen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.53(b)	Unter Beachtung von Paragraph 10.52 sollte ein Finanzins titut bei seiner Zugriffskontrolle die folgenden Grundsätz e berücksichtigen: (b) Zugriffsrechte mit den geringste n Rechten oder auf einer „Basisneed-to-have“ verwenden , bei der legitimen Benutzern nur die Mindestberechtigun gen gewährt werden, die zur Wahrnehmu ng ihrer Aufgaben ausreichen;	iam-user-no-policies-überprüfen	Diese Regel stellt sicher, dass AWS Identity and Access Management (IAM) -Richtlinien nur Gruppen oder Rollen zugewiese n werden, um den Zugriff auf Systeme und Ressourcen zu kontrollieren. Die Zuweisung von Berechtig ungen auf Gruppen- oder Rollenebene trägt dazu bei, die Wahrscheinlichkeit zu verringern, dass eine Identität übermäßige Berechtigungen erhält oder beibehält.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.53(c)(f)	Unter Beachtung von Ziffer 10.52 sollte ein Finanzins titut bei seiner Zugriffskontrollri chtlinie die folgenden Grundsätze berücksic htigen: (c) zeitlich begrenzte Zugriffsr echte anwenden, die den Zugriff auf einen bestimmten Zeitraum beschränk en, einschließlich der Zugriffsrechte, die Serviceanbietern gewährt werden; (f) Einführung einer stärkeren Authentif izierung für kritische Aktivitäten, auch für den Fernzugriff	iam-password-policy	Die Identitäten und Anmeldeinformation en werden auf der Grundlage einer organisatorischen IAM-Passwortrichtlinie ausgestellt, verwaltet und verifiziert. Sie erfüllen oder übertreff en die Anforderungen von NIST SP 800-63 und dem Standard „Best Practices“ von AWS Foundational Security in Bezug auf die Passwortstärke. Mit dieser Regel können Sie optional RequireUppercaseCh aracters (Wert für AWS grundlegende Sicherheitsbewährt e Methoden: wahr), RequireLowercaseCh aracters (Wert für bewährte Methoden für AWS grundlege nde Sicherheit: wahr), RequireSy mbols (Wert für bewährte Methoden für AWS grundlege nde Sicherheit:

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			wahr), RequireNumbers (Wert für bewährte Methoden für AWS grundlegende Sicherheit: wahr), MinimumPasswordLength (Wert für bewährte Methoden für AWS grundlegende Sicherheit: 14), PasswordReusePrevention (Wert für bewährte Methoden für AWS grundlegende Sicherheit: 24) und MaxPasswordAge (Wert für bewährte Methoden für AWS grundlegende Sicherheit: 90) für Ihr IAM festlegen Kennwortrichtlinie. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.53(f)(h)	Unter Beachtung von Ziffer 10.52 sollte ein Finanzinstitut bei seiner Zugriffsk ontrollrichtlinie die folgenden Grundsätz e berücksichtigen: (f) Einführung einer stärkeren Authentif izierung für kritische Aktivitäten, einschlie ßlich des Fernzugri ffs; (h) die gemeinsam e Nutzung von Benutzer-IDs und Passwörtern durch mehrere Benutzer einschränken und kontrollieren	iam-user-mfa-enabled	Aktivieren Sie diese Regel, um den Zugriff auf Ressourcen in der AWS Cloud einzuschr änken. Diese Regel stellt sicher, dass die Multi-Faktor-Authe ntifizierung (MFA) für alle IAM-Benut zer aktiviert ist. MFA bietet eine weitere Schutzebene zusätzlic h zum Benutzern amen und Passwort. Reduzieren Sie Fälle von kompromittierten Konten, indem Sie MFA für IAM-Benutzer vorschreiben.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.53(f)(h)	Unter Beachtung von Ziffer 10.54 sollte ein Finanzinstitut bei seiner Zugriffskontrollrichtlinie die folgenden Grundsätze berücksichtigen: (f) Einführung einer stärkeren Authentifizierung für kritische Aktivitäten, einschließlich des Fernzugriffs; (h) die gemeinsame Nutzung von Benutzer-IDs und Passwörtern durch mehrere Benutzer einschränken und kontrollieren	root-account-hardware-mfa-aktiviert	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Hardware-MFA für den Root-Benutzer aktiviert ist. Der Stammbenutzer ist der AWS-Konto-Benutzer mit den meisten Berechtigungen. MFA bietet eine weitere Schutzebene zusätzlich zum Benutzernamen und Passwort. Indem Sie MFA für den Root-Benutzer vorschreiben, können Sie die Anzahl AWS-Konten kompromittierter Benutzer reduzieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.53(f)(h)	Unter Beachtung von Ziffer 10.54 sollte ein Finanzinstitut bei seiner Zugriffsk ontrollrichtlinie die folgenden Grundsätz e berücksichtigen: (f) Einführung einer stärkeren Authentif izierung für kritische Aktivitäten, einschlie ßlich des Fernzugri ffs; (h) die gemeinsam e Nutzung von Benutzer-IDs und Passwörtern durch mehrere Benutzer einschränken und kontrollieren	root-account-mfa-e nabled	Verwalten Sie den Zugriff auf Ressource n in der AWS Cloud, indem Sie sicherste llen, dass MFA für den Root-Benu tzer aktiviert ist. Der Stammbenu tzer ist der AWS-Konto-Benutzer mit den meisten Berechtigungen. MFA bietet eine weitere Schutzebene zusätzlic h zum Benutzern amen und Passwort. Indem Sie MFA für den Root-Benutzer vorschreiben, können Sie die Anzahl AWS-Konten kompromit tierter Benutzer reduzieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.54	Ein Finanzins titut muss robuste Authentifizierungs prozesse einsetzen , um die Echtheit der verwendeten Identität en sicherzustellen. Authentifizierungs mechanismen müssen der Wichtigke it der Funktionen angemessen sein und mindestens einen oder mehrere dieser drei grundlegenden Authentifizierungs faktoren berücksic htigen, nämlich etwas, das der Benutzer weiß (zum Beispiel Passwort, PIN), etwas, das der Benutzer besitzt (zum Beispiel Smartcard , Sicherheitsgerät) und etwas, das der Benutzer ist (zum Beispiel biometrische Merkmale, wie ein Fingerabdruck oder ein Netzhautmuster).	iam-user-mfa-enabled	Aktivieren Sie diese Regel, um den Zugriff auf Ressourcen in der Cloud einzuschr änken. AWS Diese Regel stellt sicher, dass die Multi-Fak tor-Authentifizierung (MFA) für alle IAM-Benutzer aktiviert ist. MFA bietet eine weitere Schutzebe ne zusätzlich zum Benutzernamen und Passwort. Reduziere n Sie Fälle von kompromittierten Konten, indem Sie MFA für IAM-Benutzer vorschreiben.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.54	Ein Finanzinstitut muss robuste Authentifizierungsprozesse einsetzen, um die Echtheit der verwendeten Identitäten sicherzustellen. Authentifizierungsmechanismen müssen der Wichtigkeit der Funktionen angemessen sein und mindestens einen oder mehrere dieser drei grundlegenden Authentifizierungsfaktoren berücksichtigen, nämlich etwas, das der Benutzer weiß (z. B. Passwort, PIN), etwas, das der Benutzer besitzt (z. B. Smartcard, Sicherheitsgerät) und etwas, das der Benutzer ist (z. B. biometrische Merkmale wie Fingerabdruck oder Netzhautmuster).	root-account-hardware-mfa-aktiviert	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Hardware-MFA für den Root-Benutzer aktiviert ist. Der Stammbenutzer ist der AWS-Konto-Benutzer mit den meisten Berechtigungen. MFA bietet eine weitere Schutzebene zusätzlich zum Benutzernamen und Passwort. Indem Sie MFA für den Root-Benutzer vorschreiben, können Sie die Anzahl AWS-Konten kompromittierter Benutzer reduzieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.54	Ein Finanzins titut muss robuste Authentifizierungs prozesse einsetzen , um die Echtheit der verwendeten Identität en sicherzustellen. Authentifizierungs mechanismen müssen der Wichtigke it der Funktionen angemessen sein und mindestens einen oder mehrere dieser drei grundlegenden Authentifizierungs faktoren berücksic htigen, nämlich etwas, das der Benutzer weiß (zum Beispiel Passwort, PIN), etwas, das der Benutzer besitzt (zum Beispiel Smartcard , Sicherheitsgerät) und etwas, das der Benutzer ist (zum Beispiel biometrische Merkmale, wie ein Fingerabdruck oder ein Netzhautmuster).	root-account-mfa-e nabled	Verwalten Sie den Zugriff auf Ressource n in der AWS Cloud, indem Sie sicherste llen, dass MFA für den Root-Benu tzer aktiviert ist. Der Stammbenu tzer ist der AWS-Konto-Benutzer mit den meisten Berechtigungen. MFA bietet eine weitere Schutzebene zusätzlic h zum Benutzern amen und Passwort. Indem Sie MFA für den Root-Benutzer vorschreiben, können Sie die Anzahl AWS-Konten kompromit tierter Benutzer reduzieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.55	Ein Finanzins titut muss seine Passwortpraktiken regelmäßig überprüfe n und anpassen, um die Widerstan dsfähigkeit gegen sich entwickelnde Angriffe zu erhöhen. Dazu gehört auch die effektive und sichere Generierung von Passwörtern. Es müssen angemesse ne Kontrollen vorhanden sein, um die Stärke der erstellten Passwörter zu überprüfen.	iam-password-policy	Die Identitäten und Anmeldeinformation en werden auf der Grundlage einer organisatorischen IAM-Passwortrichtlinie ausgestellt, verwaltet und verifiziert. Sie erfüllen oder übertreff en die Anforderungen von NIST SP 800-63 und dem Standard „Best Practices“ von AWS Foundatio nal Security für die Passwortstärke. Mit dieser Regel können Sie optional RequireUppercaseCh aracters (Wert für AWS grundlegende Sicherheitsbewährt e Methoden: wahr), RequireLowercaseCh aracters (Wert für bewährte Methoden für AWS grundlege nde Sicherheit: wahr), RequireSy mbols (Wert für bewährte Methoden für AWS grundlege nde Sicherheit:

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			wahr), RequireNumbers (Wert für bewährte Methoden für AWS grundlegende Sicherheit: wahr), MinimumPasswordLength (Wert für bewährte Methoden für AWS grundlegende Sicherheit: 14), PasswordReusePrevention (Wert für bewährte Methoden für AWS grundlegende Sicherheit: 24) und MaxPasswordAge (Wert für bewährte Methoden für AWS grundlegende Sicherheit: 90) für Ihr IAM festlegen Kennwortrichtlinie. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.56	Authentifizierungs methoden, die von mehr als einem Faktor abhängen, sind in der Regel schwieriger zu kompromittieren als ein Einzelfak torsystem. Vor diesem Hintergrund werden Finanzinstitute ermutigt, die Multi-Faktor-Authentifizier ung (MFA) ordnungsg emäß zu konzipier en und umzusetze n (insbesondere in Systemen mit hohem Risiko oder „Single Sign-On“) , die zuverlässiger ist und eine stärkere Betrugsabschreckung bietet.	iam-user-mfa-enabled	Aktivieren Sie diese Regel, um den Zugriff auf Ressourcen in der AWS Cloud einzuschr änken. Diese Regel stellt sicher, dass die Multi-Faktor-Authe ntifizierung (MFA) für alle IAM-Benut zer aktiviert ist. MFA bietet eine weitere Schutzebene zusätzlic h zum Benutzern amen und Passwort. Reduzieren Sie Fälle von kompromittierten Konten, indem Sie MFA für IAM-Benutzer vorschreiben.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.56	Authentifizierungs methoden, die von mehr als einem Faktor abhängen, sind in der Regel schwieriger zu kompromittieren als ein Einzelfak torsystem. Vor diesem Hintergrund werden Finanzinstitute ermutigt, die Multi-Faktor-Authentifizier ung (MFA) ordnungsg emäß zu konzipier en und umzusetze n (insbesondere in Systemen mit hohem Risiko oder „Single Sign-On“) , die zuverlässiger ist und eine stärkere Betrugsabschreckung bietet.	root-account-hardw are-mfa-aktiviert	Verwalten Sie den Zugriff auf Ressource n in der AWS Cloud, indem Sie sicherste llen, dass Hardware-MFA für den Root-Benutzer aktiviert ist. Der Stammbenu tzer ist der AWS-Konto-Benutzer mit den meisten Berechtigungen. MFA bietet eine weitere Schutzebene zusätzlic h zum Benutzern amen und Passwort. Indem Sie MFA für den Root-Benutzer vorschreiben, können Sie die Anzahl AWS-Konten kompromit tierter Benutzer reduzieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.56	Authentifizierungs methoden, die von mehr als einem Faktor abhängen, sind in der Regel schwieriger zu kompromittieren als ein Einzelfak torsystem. Vor diesem Hintergrund werden Finanzinstitute ermutigt, die Multi-Faktor-Authentifizier ung (MFA) ordnungsg emäß zu konzipier en und umzusetze n (insbesondere in Systemen mit hohem Risiko oder „Single Sign-On“) , die zuverlässiger ist und eine stärkere Betrugsabschreckung bietet.	root-account-mfa-e nabled	Verwalten Sie den Zugriff auf Ressource n in der AWS Cloud, indem Sie sicherste llen, dass MFA für den Root-Benu tzer aktiviert ist. Der Stammbenu tzer ist der AWS-Konto-Benutzer mit den meisten Berechtigungen. MFA bietet eine weitere Schutzebene zusätzlic h zum Benutzern amen und Passwort. Indem Sie MFA für den Root-Benutzer vorschreiben, können Sie die Anzahl AWS-Konten kompromit tierter Benutzer reduzieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.59	Ein Finanzinstitut muss sicherstellen, dass (a) die Zugriffskontrollen zu unternehmensweiten Systemen wirksam verwaltet und überwacht werden und (b) Benutzeraktivitäten in kritischen Systemen für Prüfungen und Untersuchungen protokolliert werden. Aktivitätsprotokolle müssen mindestens drei Jahre lang aufbewahrt sowie regelmäßig und rechtzeitig überprüft werden.	access-keys-rotated	Die Anmeldeinformationen für autorisierte Geräte, Benutzer und Prozesse werden geprüft, indem sichergestellt wird, dass die IAM-Zugriffsschlüssel entsprechend den Vorgaben der Unternehmensrichtlinie rotiert werden. Das regelmäßige Ändern der Zugriffsschlüssel ist eine bewährte Sicherheitsmethode. Es verkürzt den Zeitraum, in dem ein Zugriffsschlüssel aktiv ist, und reduziert die Auswirkungen auf das Unternehmen, wenn die Schlüssel kompromittiert werden. Diese Regel erfordert einen Wert für die Zugriffsschlüssel-Rotation (Standardkonfiguration: 90). Der tatsächliche Wert muss den Richtlini

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			en Ihrer Organisation entsprechen.
10.59	Ein Finanzinstitut muss sicherstellen, dass (a) die Zugriffskontrollen zu unternehmensweiten Systemen wirksam verwaltet und überwacht werden und (b) Benutzeraktivitäten in kritischen Systemen für Prüfungen und Untersuchungen protokolliert werden. Aktivitätsprotokolle müssen mindestens drei Jahre lang aufbewahrt sowie regelmäßig und rechtzeitig überprüft werden.	account-part-of-organizations	Durch die zentrale Verwaltung AWS-Konten innerhalb von AWS Organizations wird sichergestellt, dass die Konten den Vorschriften entsprechen. Eine fehlende zentrale Kontoverwaltung kann zu inkonsistenten Kontokonfigurationen führen, wodurch Ressourcen und sensible Daten offengelegt werden können.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.59	Ein Finanzinstitut muss sicherstellen, dass (a) die Zugriffskontrollen zu unternehmensweiten Systemen wirksam verwaltet und überwacht werden und (b) Benutzeraktivitäten in kritischen Systemen für Prüfungen und Untersuchungen protokolliert werden. Aktivitätsprotokolle müssen mindestens drei Jahre lang aufbewahrt sowie regelmäßig und rechtzeitig überprüft werden.	api-gw-execution-logging-aktiviert	Die API-Gateway-Protokollierung zeigt detaillierte Ansichten der Benutzer, die auf die API zugegriffen haben, und wie diese Benutzer auf die API zugegriffen haben. Diese Einblicke ermöglichen die Transparenz von Benutzeraktivitäten.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10,59	Ein Finanzinstitut muss sicherstellen, dass (a) die Zugriffskontrollen zu unternehmensweiten Systemen wirksam verwaltet und überwacht werden und (b) Benutzeraktivitäten in kritischen Systemen für Prüfungen und Untersuchungen protokolliert werden. Aktivitätsprotokolle müssen mindestens drei Jahre lang aufbewahrt sowie regelmäßig und rechtzeitig überprüft werden.	cloudtrail-s3-dataevents-enabled	Die Erfassung von Simple Storage Service (Amazon S3)-Datenereignissen unterstützt die Erkennung von ungewöhnlichen Aktivitäten. Zu den Details gehören AWS-Konto Informationen über den Zugriff auf einen Amazon S3 S3-Bucket, die IP-Adresse und die Uhrzeit des Ereignisses.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.59	Ein Finanzinstitut muss sicherstellen, dass (a) die Zugriffskontrollen zu unternehmensweiten Systemen wirksam verwaltet und überwacht werden und (b) Benutzeraktivitäten in kritischen Systemen für Prüfungen und Untersuchungen protokolliert werden. Aktivitätsprotokolle müssen mindestens drei Jahre lang aufbewahrt sowie regelmäßig und rechtzeitig überprüft werden.	cloudtrail-security-trail-enabled	Diese Regel trägt dazu bei, die Verwendung der AWS empfohlenen bewährten Sicherheitsmethoden für sicherzustellen AWS CloudTrail, indem geprüft wird, ob mehrere Einstellungen aktiviert sind. Dazu gehören die Verwendung von Protokollverschlüsselung, Protokollvalidierung und Aktivierung AWS CloudTrail in mehreren Regionen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.59	Ein Finanzinstitut muss sicherstellen, dass (a) die Zugriffskontrollen zu unternehmensweiten Systemen wirksam verwaltet und überwacht werden und (b) Benutzeraktivitäten in kritischen Systemen für Prüfungen und Untersuchungen protokolliert werden. Aktivitätsprotokolle müssen mindestens drei Jahre lang aufbewahrt sowie regelmäßig und rechtzeitig überprüft werden.	cloud-trail-cloud-watch-logs-aktiviert	Verwenden Sie Amazon CloudWatch , um Protokollereignisaktivitäten zentral zu sammeln und zu verwalten. Die Aufnahme von AWS CloudTrail Daten liefert Einzelheiten zu den API-Aufrufaktivitäten in Ihrem AWS-Konto.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.59	Ein Finanzinstitut muss sicherstellen, dass (a) die Zugriffskontrollen zu unternehmensweiten Systemen wirksam verwaltet und überwacht werden und (b) Benutzeraktivitäten in kritischen Systemen für Prüfungen und Untersuchungen protokolliert werden. Aktivitätsprotokolle müssen mindestens drei Jahre lang aufbewahrt sowie regelmäßig und rechtzeitig überprüft werden.	cw-loggroup-retention-period-überprüfen	Stellen Sie sicher, dass die Ereignisprotokolldaten für Ihre Protokollgruppen über eine Mindestdauer aufbewahrt werden, um die Fehlerbehebung und forensische Untersuchungen zu unterstützen. Fehlende frühere Ereignisprotokolldaten erschweren die Rekonstruierung und Identifizierung potenziell schädlicher Ereignisse.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10,59	Ein Finanzinstitut muss sicherstellen, dass (a) die Zugriffskontrollen zu unternehmensweiten Systemen wirksam verwaltet und überwacht werden und (b) Benutzeraktivitäten in kritischen Systemen für Prüfungen und Untersuchungen protokolliert werden. Aktivitätsprotokolle müssen mindestens drei Jahre lang aufbewahrt sowie regelmäßig und rechtzeitig überprüft werden.	ec-2 instance-profile-attached	EC2 Instanzprofile übergeben eine IAM-Rolle an eine EC2 Instance. Das Anhängen eines Instance-Profils an Ihre Instances kann bei der Implementierung von geringsten Berechtigungen und der Berechtigungsverwaltung helfen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.59	Ein Finanzinstitut muss sicherstellen, dass (a) die Zugriffskontrollen zu unternehmensweiten Systemen wirksam verwaltet und überwacht werden und (b) Benutzeraktivitäten in kritischen Systemen für Prüfungen und Untersuchungen protokolliert werden. Aktivitätsprotokolle müssen mindestens drei Jahre lang aufbewahrt sowie regelmäßig und rechtzeitig überprüft werden.	elb-logging-enabled	Die Elastic-Load-Balancing-Aktivität ist ein zentraler Kommunikationspunkt innerhalb einer Umgebung. Stellen Sie sicher, dass die ELB-Protokollierung aktiviert ist. Die gesammelten Daten enthalten detaillierte Informationen zu Anfragen, die an den ELB gesendet wurden. Jedes Protokoll enthält Informationen wie die Zeit, zu der die Anforderung einging, die Client-IP-Adresse, Latenzen, Anforderungspfade und Serverantworten.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10,59	Ein Finanzinstitut muss sicherstellen, dass (a) die Zugriffskontrollen zu unternehmensweiten Systemen wirksam verwaltet und überwacht werden und (b) Benutzeraktivitäten in kritischen Systemen für Prüfungen und Untersuchungen protokolliert werden. Aktivitätsprotokolle müssen mindestens drei Jahre lang aufbewahrt sowie regelmäßig und rechtzeitig überprüft werden.	iam-customer-policy-blocked-kms-Aktionen	AWS Identity and Access Management (IAM) kann Ihnen helfen, die Prinzipien der geringsten Rechte und der Aufgabentrennung in Zugriffsberechtigungen und Autorisierungen zu integrieren und so zu verhindern, dass Richtlinien blockierte Aktionen für alle AWS Schlüssel des Key Management Service enthalten. Wenn Benutzer mehr Rechte haben, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und Aufgabentrennung verstoßen. Mit dieser Regel können Sie den Parameter festlegen. blockedActionsPatterns (Wert „AWS Bewährte grundlegende Sicherheitsmethoden“: kms:

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			Decrypt, kms:ReEncryptFrom). Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10,59	Ein Finanzinstitut muss sicherstellen, dass (a) die Zugriffskontrollen zu unternehmensweiten Systemen wirksam verwaltet und überwacht werden und (b) Benutzeraktivitäten in kritischen Systemen für Prüfungen und Untersuchungen protokolliert werden. Aktivitätsprotokolle müssen mindestens drei Jahre lang aufbewahrt sowie regelmäßig und rechtzeitig überprüft werden.	iam-password-policy	Die Identitäten und Anmeldeinformationen werden auf der Grundlage einer organisatorischen IAM-Passwortrichtlinie ausgestellt, verwaltet und verifiziert. Sie erfüllen oder übertreffen die Anforderungen von NIST SP 800-63 und dem Standard „Best Practices“ von AWS Foundational Security für die Passwortstärke. Mit dieser Regel können Sie optional RequireUppercaseCharacters (Wert für AWS grundlegende Sicherheitsbewährte Methoden: wahr), RequireLowercaseCharacters (Wert für bewährte Methoden für AWS grundlegende Sicherheit: wahr), RequireSymbols (Wert für bewährte Methoden für AWS grundlegende Sicherheit:

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			wahr), RequireNumbers (Wert für bewährte Methoden für AWS grundlegende Sicherheit: wahr), MinimumPasswordLength (Wert für bewährte Methoden für AWS grundlegende Sicherheit: 14), PasswordReusePrevention (Wert für bewährte Methoden für AWS grundlegende Sicherheit: 24) und MaxPasswordAge (Wert für bewährte Methoden für AWS grundlegende Sicherheit: 90) für Ihr IAM festlegen Kennwortrichtlinie. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.59	Ein Finanzinstitut muss sicherstellen, dass (a) die Zugriffskontrollen zu unternehmensweiten Systemen wirksam verwaltet und überwacht werden und (b) Benutzeraktivitäten in kritischen Systemen für Prüfungen und Untersuchungen protokolliert werden. Aktivitätsprotokolle müssen mindestens drei Jahre lang aufbewahrt sowie regelmäßig und rechtzeitig überprüft werden.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) kann Ihnen dabei helfen, die Prinzipien der geringsten Rechte und der Aufgabentrennung in Zugriffsberechtigungen und Autorisierungen zu integrieren und so zu verhindern, dass Richtlinien „Effect“: „Allow“ mit „Action“: „*“ anstelle von „Resource“: „*“ enthalten. Wenn Benutzern mehr Rechte eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und der Aufgabentrennung verstoßen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10,59	Ein Finanzinstitut muss sicherstellen, dass (a) die Zugriffskontrollen zu unternehmensweiten Systemen wirksam verwaltet und überwacht werden und (b) Benutzeraktivitäten in kritischen Systemen für Prüfungen und Untersuchungen protokolliert werden. Aktivitätsprotokolle müssen mindestens drei Jahre lang aufbewahrt sowie regelmäßig und rechtzeitig überprüft werden.	iam-root-access-key-überprüfen	Der Zugriff auf Systeme und Ressourcen kann gesteuert werden, indem überprüft wird, ob der Root-Benutzer keine Zugriffsschlüssel mit seiner AWS Identity and Access Management (IAM) -Rolle verknüpft hat. Stellen Sie sicher, dass die Root-Zugriffsschlüssel gelöscht werden. Erstellen und verwenden Sie stattdessen rollenbasierte Funktionen, AWS-Konten um das Prinzip der geringsten Funktionalität zu berücksichtigen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.59	Ein Finanzinstitut muss sicherstellen, dass (a) die Zugriffskontrollen zu unternehmensweiten Systemen wirksam verwaltet und überwacht werden und (b) Benutzeraktivitäten in kritischen Systemen für Prüfungen und Untersuchungen protokolliert werden. Aktivitätsprotokolle müssen mindestens drei Jahre lang aufbewahrt sowie regelmäßig und rechtzeitig überprüft werden.	iam-user-group-membership-überprüfen	AWS Identity and Access Management (IAM) kann Ihnen helfen, Zugriffsberechtigungen und Autorisierungen einzuschränken, indem sichergestellt wird, dass IAM-Benutzer Mitglieder mindestens einer Gruppe sind. Wenn Benutzern mehr Berechtigungen eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und Aufgabentrennung verstoßen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.59	Ein Finanzinstitut muss sicherstellen, dass (a) die Zugriffskontrollen zu unternehmensweiten Systemen wirksam verwaltet und überwacht werden und (b) Benutzeraktivitäten in kritischen Systemen für Prüfungen und Untersuchungen protokolliert werden. Aktivitätsprotokolle müssen mindestens drei Jahre lang aufbewahrt sowie regelmäßig und rechtzeitig überprüft werden.	iam-user-no-policies-überprüfen	Diese Regel stellt sicher, dass AWS Identity and Access Management (IAM)-Richtlinien nur Gruppen oder Rollen zugewiesen werden, um den Zugriff auf Systeme und Ressourcen zu kontrollieren. Die Zuweisung von Berechtigungen auf Gruppen- oder Rollenebene trägt dazu bei, die Wahrscheinlichkeit zu verringern, dass eine Identität übermäßige Berechtigungen erhält oder beibehält.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.59	Ein Finanzinstitut muss sicherstellen, dass (a) die Zugriffskontrollen zu unternehmensweiten Systemen wirksam verwaltet und überwacht werden und (b) Benutzeraktivitäten in kritischen Systemen für Prüfungen und Untersuchungen protokolliert werden. Aktivitätsprotokolle müssen mindestens drei Jahre lang aufbewahrt sowie regelmäßig und rechtzeitig überprüft werden.	opensearch-logs-to-cloudwatch	Stellen Sie sicher, dass für Amazon OpenSearch Service-Domains Fehlerprotokolle aktiviert und zur Aufbewahrung und Beantwortung an Amazon CloudWatch Logs gestreamt werden. OpenSearch Service-Fehlerprotokolle können bei Sicherheits- und Zugriffsprüfungen helfen und bei der Diagnose von Verfügbarkeitsproblemen helfen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.59	Ein Finanzinstitut muss sicherstellen, dass (a) die Zugriffskontrollen zu unternehmensweiten Systemen wirksam verwaltet und überwacht werden und (b) Benutzeraktivitäten in kritischen Systemen für Prüfungen und Untersuchungen protokolliert werden. Aktivitätsprotokolle müssen mindestens drei Jahre lang aufbewahrt sowie regelmäßig und rechtzeitig überprüft werden.	rds-logging-enabled	Um die Protokollierung und Überwachung in Ihrer Umgebung zu erleichtern, stellen Sie sicher, dass die Amazon Relational Database Service (Amazon RDS)-Protokollierung aktiviert ist. Mit der Amazon-RDS-Protokollierung können Sie Ereignisse wie Verbindungen, Verbindungsabbrüche, Abfragen oder abgefragte Tabellen erfassen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10,59	Ein Finanzinstitut muss sicherstellen, dass (a) die Zugriffskontrollen zu unternehmensweiten Systemen wirksam verwaltet und überwacht werden und (b) Benutzeraktivitäten in kritischen Systemen für Prüfungen und Untersuchungen protokolliert werden. Aktivitätsprotokolle müssen mindestens drei Jahre lang aufbewahrt sowie regelmäßig und rechtzeitig überprüft werden.	redshift-cluster-configuration-check	Um Daten im Ruhezustand zu schützen, muss die Verschlüsselung für Ihre Amazon-Redshift-Cluster aktiviert sein. Sie müssen auch sicherstellen, dass die erforderlichen Konfigurationen auf Amazon-Redshift-Clustern bereitgestellt werden. Die Prüfungsprotokollierung muss aktiviert sein, um Informationen zu Verbindungen und Benutzeraktivitäten in der Datenbank bereitzustellen. Diese Regel erfordert, dass ein Wert für clusterDbEncrypted (Config Default: TRUE) und LoggingEnabled (Config Default: TRUE) gesetzt ist. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.59	Ein Finanzinstitut muss sicherstellen, dass (a) die Zugriffskontrollen zu unternehmensweiten Systemen wirksam verwaltet und überwacht werden und (b) Benutzeraktivitäten in kritischen Systemen für Prüfungen und Untersuchungen protokolliert werden. Aktivitätsprotokolle müssen mindestens drei Jahre lang aufbewahrt sowie regelmäßig und rechtzeitig überprüft werden.	s-3 bucket-logging-enabled	Die Amazon Simple Storage Service (Amazon S3)-Serverzugriffsprotokollierung bietet eine Methode zur Überwachung des Netzwerks im Hinblick auf potenzielle Cybersicherheitsereignisse. Die Ereignisse werden überwacht, indem detaillierte Aufzeichnungen über die Anfragen erfasst werden, die an einen Amazon-S3-Bucket gestellt wurden. Jeder Zugriffsprotokolleintrag enthält Details zu einer einzelnen Zugriffsanfrage. Zu den Details gehören Auftraggeber, Bucket-Name, Anforderungszeit, Anforderungsaktion, Antwortstatus und Fehlercode, falls relevant.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10,59	Ein Finanzinstitut muss sicherstellen, dass (a) die Zugriffskontrollen zu unternehmensweiten Systemen wirksam verwaltet und überwacht werden und (b) Benutzeraktivitäten in kritischen Systemen für Prüfungen und Untersuchungen protokolliert werden. Aktivitätsprotokolle müssen mindestens drei Jahre lang aufbewahrt sowie regelmäßig und rechtzeitig überprüft werden.	wafv2-logging-enabled	Um die Protokollierung und Überwachung in Ihrer Umgebung zu erleichtern, aktivieren Sie die AWS WAF (V2) -Protokollierung im regionalen und globalen Web. ACLs AWS Die WAF-Protokollierung bietet detaillierte Informationen über den Datenverkehr, der von Ihrer Web-ACL analysiert wird. In den Protokollen werden die Uhrzeit aufgezeichnet, zu der die AWS WAF die Anfrage von Ihrer AWS Ressource erhalten hat, Informationen über die Anfrage und eine Aktion für die Regel, der jede Anfrage entsprach.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10,60	Damit große Finanzinstitute die in Absatz 10.59 genannten Anforderungen erfüllen, müssen sie (a) ein Identity Access Management System einrichten, um den Benutzerzugriff auf unternehmensweite Systeme effektiv zu verwalten und zu überwachen, und (b) automatisierte Prüfungstools einsetzen, um etwaige Anomalien zu melden.	cloud-trail-cloud-watch-logs-aktiviert	Verwenden Sie Amazon CloudWatch , um Protokoll ereignisaktivitäten zentral zu sammeln und zu verwalten. Die Aufnahme von AWS CloudTrail Daten liefert Einzelheiten zu den API-Aufrufaktivitäten in Ihrem AWS-Konto.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.60	Damit große Finanzinstitute die in Absatz 10.61 genannten Anforderungen erfüllen, müssen sie (a) ein Identity Access Management System einrichten, um den Benutzerzugriff auf unternehmensweite Systeme effektiv zu verwalten und zu überwachen, und (b) automatisierte Prüfungstools einsetzen, um etwaige Anomalien zu melden.	guardduty-enabled-centralized	Amazon GuardDuty kann mithilfe von Threat Intelligence Feeds helfen, potenzielle Cybersicherheitsereignisse zu überwachen und zu erkennen. Dazu gehören Listen mit bösartigen IPs und maschinellen Lernmethoden zur Identifizierung unerwarteter, nicht autorisierter und bösartiger Aktivitäten in Ihrer AWS Cloud-Umgebung.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10,60	Damit große Finanzinstitute die in Absatz 10.61 genannten Anforderungen erfüllen, müssen sie (a) ein Identity Access Management System einrichten, um den Benutzerzugriff auf unternehmensweite Systeme effektiv zu verwalten und zu überwachen, und (b) automatisierte Prüfungstools einsetzen, um etwaige Anomalien zu melden.	securityhub-enabled	AWS Security Hub hilft bei der Überwachung von unbefugtem Personal, Verbindungen, Geräten und Software. AWS Security Hub aggregiert, organisiert und priorisiert die Sicherheitswarnungen oder Ergebnisse mehrerer Dienste. AWS Einige dieser Dienste sind Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer und AWS Firewall Manager sowie AWS Partnerlösungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.61	Ein Finanzinstitut muss sicherstellen, dass kritische Systeme nicht auf veralteten Systemen mit bekannten Sicherheitslücken oder end-of-life (EOL-) Technologiesystemen laufen. In diesem Zusammenhang muss ein Finanzinstitut den identifizierten Funktionen klare Zuständigkeiten zuweisen: (a) um die neuesten Patch-Versionen kontinuierlich zu überwachen und rechtzeitig zu implementieren und (b) um kritische Technologiesysteme zu identifizieren, die sich EOL nähern, um weitere Abhilfemaßnahmen ergreifen zu können.	ec2-manager instance-managed-by-systems	Eine Bestandsaufnahme der Softwareplattformen und Anwendungen innerhalb des Unternehmens ist möglich, indem Amazon Elastic Compute Cloud (Amazon EC2) - Instances mit AWS Systems Manager verwaltet werden. Verwenden Sie AWS Systems Manager, um detaillierte Systemkonfigurationen, Betriebssystem-Patch-Levels, Namen und Typ der Dienste, Softwareinstallationen, Anwendungsname, Herausgeber und Version sowie andere Details zu Ihrer Umgebung bereitzustellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.61	Ein Finanzinstitut muss sicherstellen, dass kritische Systeme nicht auf veralteten Systemen mit bekannten Sicherheitslücken oder end-of-life (EOL-) Technologiesystemen laufen. In diesem Zusammenhang muss ein Finanzinstitut den identifizierten Funktionen klare Zuständigkeiten zuweisen: (a) um die neuesten Patch-Versionen kontinuierlich zu überwachen und rechtzeitig zu implementieren und (b) um kritische Technologiesysteme zu identifizieren, die sich EOL nähern, um weitere Abhilfemaßnahmen ergreifen zu können.	ec2-check managedinstance-association-compliance-status	Verwenden Sie AWS Systems Manager Associations, um bei der Inventarisierung von Softwareplattformen und Anwendungen innerhalb eines Unternehmens zu helfen. AWS Systems Manager weist Ihren verwalteten Instanzen einen Konfigurationsstatus zu und ermöglicht es Ihnen, Basiswerte für Betriebssystem-Patch-Levels, Softwareinstallationen, Anwendungskonfigurationen und andere Details zu Ihrer Umgebung festzulegen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.61	Ein Finanzinstitut muss sicherstellen, dass kritische Systeme nicht auf veralteten Systemen mit bekannten Sicherheitslücken oder end-of-life (EOL-) Technologiesystemen laufen. In diesem Zusammenhang muss ein Finanzinstitut den identifizierten Funktionen klare Zuständigkeiten zuweisen: (a) um die neuesten Patch-Versionen kontinuierlich zu überwachen und rechtzeitig zu implementieren und (b) um kritische Technologiesysteme zu identifizieren, die sich EOL nähern, um weitere Abhilfemaßnahmen ergreifen zu können.	ec2-check managedinstance-patch-compliance-status	Aktivieren Sie diese Regel, um bei der Identifizierung und Dokumentation von Sicherheitslücken in Amazon Elastic Compute Cloud (Amazon EC2) zu helfen. Die Regel prüft, ob die EC2 Amazon-Instance die Patch-Konformität im AWS Systems Manager gemäß den Richtlinien und Verfahren Ihrer Organisation einhält.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.61	Ein Finanzinstitut muss sicherstellen, dass kritische Systeme nicht auf veralteten Systemen mit bekannten Sicherheitslücken oder end-of-life (EOL-) Technologiesystemen laufen. In diesem Zusammenhang muss ein Finanzinstitut den identifizierten Funktionen klare Zuständigkeiten zuweisen: (a) um die neuesten Patch-Versionen kontinuierlich zu überwachen und rechtzeitig zu implementieren und (b) um kritische Technologiesysteme zu identifizieren, die sich EOL nähern, um weitere Abhilfemaßnahmen ergreifen zu können.	elastic-beanstalk-managed-updates-aktiviert	Durch die Aktivierung verwalteter Plattformupdates für eine Amazon-Elastic-Beanstalk-Umgebung wird sichergestellt, dass die aktuellen verfügbaren Plattform-Fixes, -Updates und -Features für die Umgebung installiert sind. Eine bewährte Methode zur Sicherung von Systemen besteht darin, stets die aktuellen Patches zu installieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10,61	Ein Finanzinstitut muss sicherstellen, dass kritische Systeme nicht auf veralteten Systemen mit bekannten Sicherheitslücken oder end-of-life (EOL-) Technologiesystemen laufen. In diesem Zusammenhang muss ein Finanzinstitut den identifizierten Funktionen klare Zuständigkeiten zuweisen: (a) um die neuesten Patch-Versionen kontinuierlich zu überwachen und rechtzeitig zu implementieren und (b) um kritische Technologiesysteme zu identifizieren, die sich EOL nähern, um weitere Abhilfemaßnahmen ergreifen zu können.	redshift-cluster-maintenancesettings-check	Diese Regel stellt sicher, dass Amazon-Redshift-Cluster die bevorzugten Einstellungen für Ihre Organisation haben. Insbesondere sorgt sie dafür, dass Cluster bevorzugte Wartungsfenster und automatisierte Aufbewahrungsfristen für Snapshots für die Datenbank haben. Für diese Regel müssen Sie die allowVersionUpgrade festlegen. Der Standardwert ist „true“. Außerdem können Sie optional den Zeitraum preferredMaintenanceWindow (der Standardwert ist sa: 16:00 -sa: 16:30) und den automated SnapshotRetention Zeitraum (der Standardwert ist 1) festlegen. Die tatsächlichen Werte müssen den Richtlini

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			en Ihrer Organisation entsprechen.
10.64(a)	Ein Finanzinstitut muss bei der Bereitstellung digitaler Dienste robuste technische Sicherheitskontrollen einführen, die Folgendes gewährleisten: (a) Vertraulichkeit und Integrität von Kunden- sowie Gegenparteiinformationen und Transaktionen	alb-http-to-https-Umleitungsprüfung	Um Daten während der Übertragung zu schützen, stellen Sie sicher, dass Ihr Application Load Balancer unverschlüsselte HTTP-Anfragen automatisch an HTTPS umleitet. Da sensible Daten vorhanden sein können, sollten Sie die Verschlüsselung bei der Übertragung aktivieren, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.64(a)	Ein Finanzinstitut muss bei der Bereitstellung digitaler Dienste robuste technische Sicherheitskontrollen einführen, die Folgendes gewährleisten: (a) Vertraulichkeit und Integrität von Kunden- sowie Gegenparteiinformationen und Transaktionen	api-gw-cache-enabled-und-verschlüsselt	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass die Verschlüsselung für den Cache Ihrer API-Gateway-Stufe aktiviert ist. Da für die API-Methode sensible Daten erfasst werden können, sollten Sie die Verschlüsselung von Daten im Ruhezustand aktivieren, um diese Daten zu schützen.
10.64(a)	Ein Finanzinstitut muss bei der Bereitstellung digitaler Dienste robuste technische Sicherheitskontrollen einführen, die Folgendes gewährleisten: (a) Vertraulichkeit und Integrität von Kunden- sowie Gegenparteiinformationen und Transaktionen	api-gw-ssl-enabled	Stellen Sie sicher, dass die REST-API-Stufen von Amazon API Gateway mit SSL-Zertifikaten konfiguriert sind, damit Backend-Systeme überprüfen können, ob Anforderungen von API Gateway stammen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.64(a)	Ein Finanzinstitut muss bei der Bereitstellung digitaler Dienste robuste technische Sicherheitskontrollen einführen, die Folgendes gewährleisten: (a) Vertraulichkeit und Integrität von Kunden- sowie Gegenparteiinformationen und Transaktionen	backup-recovery-point-encrypted	Stellen Sie sicher, dass die Verschlüsselung für Ihre AWS Backup-Wiederherstellungspunkte aktiviert ist. Da sensible Daten auch im Ruhezustand vorhanden sein können, sollten Sie die Verschlüsselung im Ruhezustand aktivieren, um diese Daten zu schützen.
10.64(a)	Ein Finanzinstitut muss bei der Bereitstellung digitaler Dienste robuste technische Sicherheitskontrollen einführen, die Folgendes gewährleisten: (a) Vertraulichkeit und Integrität von Kunden- sowie Gegenparteiinformationen und Transaktionen	cloudtrail-security-trail-enabled	Diese Regel trägt dazu bei, die Verwendung der AWS empfohlenen bewährten Sicherheitsmethoden für sicherzustellen AWS CloudTrail, indem überprüft wird, ob mehrere Einstellungen aktiviert sind. Dazu gehören die Verwendung von Protokollverschlüsselung, Protokollvalidierung und Aktivierung AWS CloudTrail in mehreren Regionen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.64(a)	Ein Finanzinstitut muss bei der Bereitstellung digitaler Dienste robuste technische Sicherheitskontrollen einführen, die Folgendes gewährleisten: (a) Vertraulichkeit und Integrität von Kunden- sowie Gegenparteiinformationen und Transaktionen	cloudwatch-log-group-encrypted	Um sensible Daten im Speicher zu schützen, stellen Sie sicher, dass die Verschlüsselung für Ihre Amazon CloudWatch Log Groups aktiviert ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.64(a)	Ein Finanzinstitut muss bei der Bereitstellung digitaler Dienste robuste technische Sicherheitskontrollen einführen, die Folgendes gewährleisten: (a) Vertraulichkeit und Integrität von Kunden- sowie Gegenparteiinformationen und Transaktionen	dynamodb-table-encrypted-kms	Stellen Sie sicher, dass die Verschlüsselung für Ihre Amazon-DynamoDB-Tabellen aktiviert ist. Um eventuell vorhandene sensible Daten im Ruhezustand in diesen Tabellen zu schützen, müssen Sie die Verschlüsselung von Daten im Ruhezustand aktivieren. Standardmäßig werden DynamoDB-Tabellen mit einem AWS eigenen Kundenhauptschlüssel (CMK) verschlüsselt.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.64(a)	Ein Finanzinstitut muss bei der Bereitstellung digitaler Dienste robuste technische Sicherheitskontrollen einführen, die Folgendes gewährleisten: (a) Vertraulichkeit und Integrität von Kunden- sowie Gegenparteiinformationen und Transaktionen	ec2- ebs-encryption-by-default	Zum Schutz von Daten im Ruhezustand müssen Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon Elastic Block Store (Amazon EBS)-Volumes aktiviert ist. Aktivieren Sie die Verschlüsselung von Daten im Ruhezustand, um eventuell in diesen Volumes vorhandene sensible Daten im Ruhezustand zu schützen.
10.64(a)	Ein Finanzinstitut muss bei der Bereitstellung digitaler Dienste robuste technische Sicherheitskontrollen einführen, die Folgendes gewährleisten: (a) Vertraulichkeit und Integrität von Kunden- sowie Gegenparteiinformationen und Transaktionen	efs-encrypted-check	Aktivieren Sie die Verschlüsselung für Ihr Amazon Elastic File System (EFS), um eventuell vorhandene sensible Daten sowie Daten im Ruhezustand zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.64(a)	Ein Finanzinstitut muss bei der Bereitstellung digitaler Dienste robuste technische Sicherheitskontrollen einführen, die Folgendes gewährleisten: (a) Vertraulichkeit und Integrität von Kunden- sowie Gegenparteiinformationen und Transaktionen	elv 2- acm-certificate-required	Zum Schutz von eventuell vorhandenen sensiblen Daten sowie von Daten während der Übertragung muss die Verschlüsselung für Ihr Elastic Load Balancing aktiviert sein. Verwenden Sie AWS Certificate Manager, um öffentliche und private SSL/TLS-Zertifikate mit AWS Diensten und internen Ressourcen zu verwalten, bereitzustellen und bereitzustellen.
10.64(a)	Ein Finanzinstitut muss bei der Bereitstellung digitaler Dienste robuste technische Sicherheitskontrollen einführen, die Folgendes gewährleisten: (a) Vertraulichkeit und Integrität von Kunden- sowie Gegenparteiinformationen und Transaktionen	encrypted-volumes	Aktivieren Sie die Verschlüsselung für Ihre Volumes von Amazon Elastic Block Store (Amazon EBS), um eventuell vorhandene sensible Daten sowie Daten im Ruhezustand zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.64(a)	Ein Finanzinstitut muss bei der Bereitstellung digitaler Dienste robuste technische Sicherheitskontrollen einführen, die Folgendes gewährleisten: (a) Vertraulichkeit und Integrität von Kunden- sowie Gegenparteiinformationen und Transaktionen	opensearch-encrypted-at-rest	Da sensible Daten vorhanden sein können und um Daten im Ruhezustand zu schützen, sollten Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon OpenSearch Service-Domains aktiviert ist.
10.64(a)	Ein Finanzinstitut muss bei der Bereitstellung digitaler Dienste robuste technische Sicherheitskontrollen einführen, die Folgendes gewährleisten: (a) Vertraulichkeit und Integrität von Kunden- sowie Gegenparteiinformationen und Transaktionen	opensearch-https-required	Da sensible Daten existieren können und um Daten während der Übertragung zu schützen, sollten Sie sicherstellen, dass HTTPS für Verbindungen zu Ihren Amazon OpenSearch Service-Domains aktiviert ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.64(a)	Ein Finanzinstitut muss bei der Bereitstellung digitaler Dienste robuste technische Sicherheitskontrollen einführen, die Folgendes gewährleisten: (a) Vertraulichkeit und Integrität von Kunden- sowie Gegenparteiinformationen und Transaktionen	opensearch-node-to-node-Verschlüsselungsprüfung	Stellen Sie sicher, dass die node-to-node Verschlüsselung für Amazon OpenSearch Service aktiviert ist. Node-to-nodeVerschlüsselung ermöglicht die TLS 1.2-Verschlüsselung für die gesamte Kommunikation innerhalb der Amazon Virtual Private Cloud (Amazon VPC). Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.64(a)	Ein Finanzinstitut muss bei der Bereitstellung digitaler Dienste robuste technische Sicherheitskontrollen einführen, die Folgendes gewährleisten: (a) Vertraulichkeit und Integrität von Kunden- sowie Gegenparteiinformationen und Transaktionen	rds-snapshot-encrypted	Stellen Sie sicher, dass die Verschlüsselung für Ihre Amazon Relational Database Service (Amazon RDS)-Snapshots aktiviert ist. Da sensible Daten auch im Ruhezustand vorhanden sein können, sollten Sie die Verschlüsselung von Daten im Ruhezustand aktivieren, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.64(a)	Ein Finanzinstitut muss bei der Bereitstellung digitaler Dienste robuste technische Sicherheitskontrollen einführen, die Folgendes gewährleisten: (a) Vertraulichkeit und Integrität von Kunden- sowie Gegenparteiinformationen und Transaktionen	rds-storage-encrypted	Zum Schutz von Daten im Ruhezustand müssen Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon Relational Database Service (Amazon RDS)-Instances aktiviert ist. Da sensible Daten in Amazon-RDS-Instances gespeichert werden können, sollten Sie die Verschlüsselung von Daten im Ruhezustand aktivieren, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.64(a)	Ein Finanzinstitut muss bei der Bereitstellung digitaler Dienste robuste technische Sicherheitskontrollen einführen, die Folgendes gewährleisten: (a) Vertraulichkeit und Integrität von Kunden- sowie Gegenparteiinformationen und Transaktionen	redshift-cluster-configuration-check	Um Daten im Ruhezustand zu schützen, muss die Verschlüsselung für Ihre Amazon-Redshift-Cluster aktiviert sein. Sie müssen auch sicherstellen, dass die erforderlichen Konfigurationen auf Amazon-Redshift-Clustern bereitgestellt werden. Die Prüfungsprotokollierung muss aktiviert sein, um Informationen zu Verbindungen und Benutzeraktivitäten in der Datenbank bereitzustellen. Diese Regel erfordert, dass ein Wert für clusterDbEncrypted (Config Default: TRUE) und LoggingEnabled (Config Default: TRUE) gesetzt ist. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.64(a)	Ein Finanzinstitut muss bei der Bereitstellung digitaler Dienste robuste technische Sicherheitskontrollen einführen, die Folgendes gewährleisten: (a) Vertraulichkeit und Integrität von Kunden- sowie Gegenparteiinformationen und Transaktionen	redshift-cluster-kms-enabled	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass die Verschlüsselung mit AWS Key Management Service (AWS KMS) für Ihren Amazon Redshift Redshift-Cluster aktiviert ist. Um eventuell vorhandene sensible Daten im Ruhezustand in Redshift-Clustern zu schützen, muss die Verschlüsselung von Daten im Ruhezustand aktiviert sein.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.64(a)	Ein Finanzinstitut muss bei der Bereitstellung digitaler Dienste robuste technische Sicherheitskontrollen einführen, die Folgendes gewährleisten: (a) Vertraulichkeit und Integrität von Kunden- sowie Gegenparteiinformationen und Transaktionen	redshift-require-tls-ssl	Stellen Sie sicher, dass Ihre Amazon-Redshift-Cluster eine TLS/SSL-Verschlüsselung erfordern, um eine Verbindung zu SQL-Clients herzustellen. Da sensible Daten vorhanden sein können, sollten Sie die Verschlüsselung bei der Übertragung aktivieren, um diese Daten zu schützen.
10.64(a)	Ein Finanzinstitut muss bei der Bereitstellung digitaler Dienste robuste technische Sicherheitskontrollen einführen, die Folgendes gewährleisten: (a) Vertraulichkeit und Integrität von Kunden- sowie Gegenparteiinformationen und Transaktionen	s3- aktiviert bucket-server-side-encryption	Zum Schutz von Daten im Ruhezustand müssen Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon Simple Storage Service (Amazon S3)-Buckets aktiviert ist. Da sensible Daten in Amazon-S3-Buckets gespeichert werden können, sollten Sie die Verschlüsselung aktivieren, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.64(a)	Ein Finanzinstitut muss bei der Bereitstellung digitaler Dienste robuste technische Sicherheitskontrollen einführen, die Folgendes gewährleisten: (a) Vertraulichkeit und Integrität von Kunden- sowie Gegenparteiinformationen und Transaktionen	s-3 bucket-ssl-requests-only	Um Daten während der Übertragung zu schützen, stellen Sie sicher, dass Ihre Amazon Simple Storage Service (Amazon S3)-Buckets Anfragen zur Verwendung von Secure Socket Layer (SSL)-Buckets erfordern. Da sensible Daten vorhanden sein können, sollten Sie die Verschlüsselung bei der Übertragung aktivieren, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.64(a)	Ein Finanzinstitut muss bei der Bereitstellung digitaler Dienste robuste technische Sicherheitskontrollen einführen, die Folgendes gewährleisten: (a) Vertraulichkeit und Integrität von Kunden- sowie Gegenparteiinformationen und Transaktionen	sagemaker-endpoint-configuration-kms-key-konfiguriert	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass die Verschlüsselung mit dem AWS Key Management Service (AWS KMS) für Ihren Endpunkt aktiviert ist. SageMaker Da sensible Daten auf dem SageMaker Endgerät gespeichert werden können, sollten Sie die Verschlüsselung im Ruhezustand aktivieren, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.64(a)	Ein Finanzinstitut muss bei der Bereitstellung digitaler Dienste robuste technische Sicherheitskontrollen einführen, die Folgendes gewährleisten: (a) Vertraulichkeit und Integrität von Kunden- sowie Gegenparteiinformationen und Transaktionen	sagemaker-notebook-instance-kms-schlüsselkonfiguriert	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass die Verschlüsselung mit dem AWS Key Management Service (AWS KMS) für Ihr Notebook aktiviert ist. SageMaker Da vertrauliche Daten im SageMaker Notebook gespeichert werden können, sollten Sie die Verschlüsselung im Ruhezustand aktivieren, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.64(a)	Ein Finanzinstitut muss bei der Bereitstellung digitaler Dienste robuste technische Sicherheitskontrollen einführen, die Folgendes gewährleisten: (a) Vertraulichkeit und Integrität von Kunden- sowie Gegenparteiinformationen und Transaktionen	secretsmanager-using-cmk	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass die Verschlüsselung mit dem AWS Key Management Service (AWS KMS) für AWS Secrets Manager aktiviert ist. Aktivieren Sie die Verschlüsselung von Daten im Ruhezustand, um eventuell vorhandene sensible Daten im Ruhezustand im Secrets Manager zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.64(a)	Ein Finanzinstitut muss bei der Bereitstellung digitaler Dienste robuste technische Sicherheitskontrollen einführen, die Folgendes gewährleisten: (a) Vertraulichkeit und Integrität von Kunden- sowie Gegenparteiinformationen und Transaktionen	sns-encrypted-kms	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass Ihre Amazon Simple Notification Service (Amazon SNS) -Themen mit dem AWS Key Management Service (AWS KMS) verschlüsselt werden müssen. Um eventuell vorhandene sensible Daten im Ruhezustand in veröffentlichten Nachrichten zu schützen, muss die Verschlüsselung von Daten im Ruhezustand aktiviert sein.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.64(b)	Ein Finanzinstitut muss bei der Bereitstellung digitaler Dienste robuste technische Sicherheitskontrollen implementieren, die Folgendes sicherstellen: (b) Zuverlässigkeit der über Kanäle und Geräte bereitgestellten Dienste bei minimaler Unterbrechung der Dienste	dynamodb-autoscaling-enabled	Amazon DynamoDB Auto Scaling verwendet den AWS Application Auto Scaling-Service, um die bereitgestellte Durchsatzkapazität so anzupassen, dass sie automatisch auf tatsächliche Verkehrsmuster reagiert. Auf diese Weise kann eine Tabelle oder ein globaler sekundärer Index die bereitgestellte Lese-/Schreibkapazität erhöhen, um plötzliche Erhöhungen des Datenverkehrs ohne Drosselung zu bewältigen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.64(b)	Ein Finanzinstitut muss bei der Bereitstellung digitaler Dienste robuste technische Sicherheitskontrollen implementieren, die Folgendes gewährleisten: (b) Zuverlässigkeit der über Kanäle und Geräte bereitgestellten Dienste bei minimaler Unterbrechung der Dienste	ec2-stopped-instance	Aktivieren Sie diese Regel, um bei der Basiskonfiguration von Amazon Elastic Compute Cloud (Amazon EC2) - Instances zu helfen, indem Sie überprüfen, ob EC2 Amazon-Instances gemäß den Standards Ihrer Organisation für mehr als die zulässige Anzahl von Tagen gestoppt wurden.
10.64(b)	Ein Finanzinstitut muss bei der Bereitstellung digitaler Dienste robuste technische Sicherheitskontrollen implementieren, die Folgendes gewährleisten: (b) Zuverlässigkeit der über Kanäle und Geräte bereitgestellten Dienste bei minimaler Unterbrechung der Dienste	elb-deletion-protection-enabled	Diese Regel sorgt dafür, dass der Löschschutz für Elastic Load Balancing aktiviert ist. Verwenden Sie diese Funktion, um zu verhindern, dass Ihr Load Balancer versehentlich oder böswillig gelöscht wird, was zum Verlust der Verfügbarkeit Ihrer Anwendungen führen kann.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.64(b)	Ein Finanzinstitut muss bei der Bereitstellung digitaler Dienste robuste technische Sicherheitskontrollen einführen, die Folgendes gewährleisten: (b) Zuverlässigkeit der über Kanäle und Geräte bereitgestellten Dienste bei minimaler Unterbrechung der Dienste	nlb-cross-zone-load-Balancing aktiviert	Aktivieren Sie den zonenübergreifenden Lastausgleich für Ihre NetworkLoad Balancer (NLBs), um eine angemessene Kapazität und Verfügbarkeit aufrechtzuerhalten. Zonenübergreifendes Load Balancing reduziert die Notwendigkeit, die gleiche Anzahl von Instances in jeder aktivierten Availability Zone aufrechtzuerhalten. Dadurch wird auch die Fähigkeit Ihrer Anwendung verbessert, den Verlust einer oder mehrerer Instances zu bewältigen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.64(b)	Ein Finanzinstitut muss bei der Bereitstellung digitaler Dienste robuste technische Sicherheitskontrollen einführen, die Folgendes gewährleisten: (b) Zuverlässigkeit der über Kanäle und Geräte bereitgestellten Dienste bei minimaler Unterbrechung der Dienste	rds-instance-deletion-protection-aktiviert	Stellen Sie sicher, dass Amazon Relational Database Service (Amazon RDS)-Instances den Löschschutz aktiviert haben. Verwenden Sie den Löschschutz, um zu verhindern, dass Ihre Amazon-RDS-Instances versehentlich oder böswillig gelöscht werden, was zum Verlust der Verfügbarkeit Ihrer Anwendungen führen kann.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.64(b)	Ein Finanzinstitut muss bei der Bereitstellung digitaler Dienste robuste technische Sicherheitskontrollen einführen, die Folgendes gewährleisten: (b) Zuverlässigkeit der über Kanäle und Geräte bereitgestellten Dienste bei minimaler Unterbrechung der Dienste	rds-multi-az-support	Die Multi-AZ-Unterstützung in Amazon Relational Database Service (Amazon RDS) bietet eine verbesserte Verfügbarkeit und Beständigkeit von Datenbank-Instances. Wenn Sie eine Multi-AZ-Datenbank-Instance bereitstellen, erstellt Amazon RDS automatisch eine primäre Datenbank-Instance und repliziert die Daten synchron auf eine Standby-Instance in einer anderen Availability Zone. Jede Availability Zone läuft auf einer eigenen, physisch getrennten, unabhängigen Infrastruktur und ist auf eine hohe Verfügbarkeit ausgelegt. Im Falle eines Infrastrukturausfalls führt Amazon RDS einen automatis

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			chen Failover zum Standby-Modus durch, sodass Sie den Datenbankbetrieb wieder aufnehmen können, sobald der Failover abgeschlo ssen ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.64(b)	Ein Finanzinstitut muss bei der Bereitstellung digitaler Dienste robuste technische Sicherheitskontrollen einführen, die Folgendes gewährleisten: (b) Zuverlässigkeit der über Kanäle und Geräte bereitgestellten Dienste bei minimaler Unterbrechung der Dienste	rds-cluster-multi-az-aktiviert	Die Multi-AZ-Unterstützung in Amazon Relational Database Service (Amazon RDS) bietet eine verbesserte Verfügbarkeit und Beständigkeit von Datenbank-Instances. Wenn Sie eine Multi-AZ-Datenbank-Instance bereitstellen, erstellt Amazon RDS automatisch eine primäre Datenbank-Instance und repliziert die Daten synchron auf eine Standby-Instance in einer anderen Availability Zone. Jede Availability Zone läuft auf einer eigenen, physisch getrennten, unabhängigen Infrastruktur und ist auf eine hohe Verfügbarkeit ausgelegt. Im Falle eines Infrastrukturausfalls führt Amazon RDS einen automatis

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			chen Failover zum Standby-Modus durch, sodass Sie den Datenbankbetrieb wieder aufnehmen können, sobald der Failover abgeschlo ssen ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.64(b)	Ein Finanzinstitut muss bei der Bereitstellung digitaler Dienste robuste technische Sicherheitskontrollen einführen, die Folgendes gewährleisten: (b) Zuverlässigkeit der über Kanäle und Geräte bereitgestellten Dienste bei minimaler Unterbrechung der Dienste	vpc-vpn-2-tunnels-up	Redundante Site-to-Site VPN-Tunnel können implementiert werden, um die Anforderungen an die Ausfallsicherheit zu erfüllen. Es verwendet zwei Tunnel, um die Konnektivität sicherzustellen, falls eine der Site-to-Site VPN-Verbindungen nicht verfügbar ist. Um sich vor einem Verbindungsverlust zu schützen, können Sie für den Fall, dass Ihr Kunden-Gateway nicht verfügbar ist, eine zweite Site-to-Site VPN-Verbindung zu Ihrer Amazon Virtual Private Cloud (Amazon VPC) und Ihrem Virtual Private Gateway einrichten, indem Sie ein zweites Kunden-Gateway verwenden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.64(d)	Ein Finanzinstitut muss bei der Bereitstellung digitaler Dienste robuste technische Sicherheitskontrollen einführen, die Folgendes sicherstellen: (d) Vorhandensein eines ausreichenden Audit Trail und die Überwachung anomaler Transaktionen	api-gw-execution-logging-aktiviert	Die API-Gateway-Protokollierung zeigt detaillierte Ansichten der Benutzer, die auf die API zugegriffen haben, und wie diese Benutzer auf die API zugegriffen haben. Diese Einblicke ermöglichen die Transparenz von Benutzeraktivitäten.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.64(d)	Ein Finanzinstitut muss bei der Bereitstellung digitaler Dienste robuste technische Sicherheitskontrollen einführen, die Folgendes sicherstellen: (d) Vorhandensein eines ausreichenden Audit Trail und die Überwachung anomaler Transaktionen	autoscaling-group-elb-healthcheck-erforderlich	Die Elastic Load Balancer (ELB) - Zustandsprüfungen für Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling Scaling-Gruppen unterstützen die Aufrechterhaltung einer angemessenen Kapazität und Verfügbarkeit. Der Load Balancer sendet regelmäßig Pings, versucht Verbindungen herzustellen oder sendet Anfragen, um den Zustand der EC2 Amazon-Instances in einer Gruppe mit auto-scaling zu testen. Wenn eine Instance nicht zurückmeldet, wird der Traffic an eine neue EC2 Amazon-Instance gesendet.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.64(d)	Ein Finanzinstitut muss bei der Bereitstellung digitaler Dienste robuste technische Sicherheitskontrollen einführen, die Folgendes sicherstellen: (d) Vorhandensein eines ausreichenden Audit Trail und die Überwachung anomaler Transaktionen	cloudtrail-s3-dataevents-enabled	Die Erfassung von Simple Storage Service (Amazon S3)-Datenereignissen unterstützt die Erkennung von ungewöhnlichen Aktivitäten. Zu den Details gehören AWS-Konto Informationen über den Zugriff auf einen Amazon S3 S3-Bucket, die IP-Adresse und die Uhrzeit des Ereignisses.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.64(d)	Ein Finanzinstitut muss bei der Bereitstellung digitaler Dienste robuste technische Sicherheitskontrollen einführen, die Folgendes sicherstellen: (d) Vorhandensein eines ausreichenden Audit Trail und die Überwachung anomaler Transaktionen	cloudtrail-security-trail-enabled	Diese Regel trägt dazu bei, die Verwendung der AWS empfohlenen bewährten Sicherheitsmethoden für sicherzustellen AWS CloudTrail, indem geprüft wird, ob mehrere Einstellungen aktiviert sind. Dazu gehören die Verwendung von Protokollverschlüsselung, Protokollvalidierung und Aktivierung AWS CloudTrail in mehreren Regionen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.64(d)	Ein Finanzinstitut muss bei der Bereitstellung digitaler Dienste robuste technische Sicherheitskontrollen einführen, die Folgendes sicherstellen: (d) Vorhandensein eines ausreichenden Audit Trail und die Überwachung anomaler Transaktionen	cloudwatch-alarm-action-check	Amazon CloudWatch alarmiert, wenn eine Metrik den Schwellenwert für eine bestimmte Anzahl von Bewertungszeiträumen überschreitet. Der Alarm führt eine oder mehrere Aktionen durch, die vom Wert der Metrik oder des Ausdrucks im Vergleich zu einem Schwellenwert in einer Reihe von Zeiträumen abhängt. Diese Regel erfordert einen Wert für alarmActionRequired (Config Default: True), insufficientDataAction Required (Config Default: True), okActionRequired (Config Default: False). Der tatsächliche Wert muss die Alarmaktionen für Ihre Umgebung widerspiegeln.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.64(d)	Ein Finanzinstitut muss bei der Bereitstellung digitaler Dienste robuste technische Sicherheitskontrollen einführen, die Folgendes sicherstellen: (d) Vorhandensein eines ausreichenden Audit Trail und die Überwachung anomaler Transaktionen	cloud-trail-cloud-watch-logs-aktiviert	Verwenden Sie Amazon CloudWatch , um Protokollereignisaktivitäten zentral zu sammeln und zu verwalten. Die Aufnahme von AWS CloudTrail Daten liefert Einzelheiten zu den API-Aufrufaktivitäten in Ihrem AWS-Konto.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.64(d)	Ein Finanzinstitut muss bei der Bereitstellung digitaler Dienste robuste technische Sicherheitskontrollen einführen, die Folgendes sicherstellen: (d) Vorhandensein eines ausreichenden Audit Trail und die Überwachung anomaler Transaktionen	dynamodb-throughput-limit-check	Aktivieren Sie diese Regel, um sicherzustellen, dass die bereitgestellte Durchsatzkapazität in Ihren Amazon-DynamoDB-Tabellen überprüft wird. Dies ist der Umfang der Lese- und Schreibaktivitäten, der von den jeweiligen Tabellen unterstützt werden kann. DynamoDB verwendet diese Informationen für das Reservieren ausreichender Systemressourcen, um Ihren Durchsatzanforderungen gerecht zu werden. Diese Regel generiert eine Warnung, wenn sich der Durchsatz dem Höchstlimit für ein Kundenkonto nähert. Mit dieser Regel können Sie optional die Parameter RCUThreshold Kontoprozentsatz

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			(Konfigurationsstandard: 80) und WCUThreshold Kontoprozentsatz (Konfigurationsstandard: 80) festlegen. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.
10.64(d)	Ein Finanzinstitut muss bei der Bereitstellung digitaler Dienste robuste technische Sicherheitskontrollen einführen, die Folgendes sicherstellen: (d) Vorhandensein eines ausreichenden Audit Trail und die Überwachung anomaler Transaktionen	ec2- instance-detailed-monitoring-enabled	Aktivieren Sie diese Regel, um die Amazon Elastic Compute Cloud (Amazon EC2) - Instance-Überwachung auf der EC2 Amazon-Konsole zu verbessern, in der Monitoring-Diagramme mit einem Zeitraum von 1 Minute für die Instance angezeigt werden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.64(d)	Ein Finanzinstitut muss bei der Bereitstellung digitaler Dienste robuste technische Sicherheitskontrollen einführen, die Folgendes sicherstellen: (d) Vorhandensein eines ausreichenden Audit Trail und die Überwachung anomaler Transaktionen	elb-logging-enabled	Die Elastic-Load-Balancing-Aktivität ist ein zentraler Kommunikationspunkt innerhalb einer Umgebung. Stellen Sie sicher, dass die ELB-Protokollierung aktiviert ist. Die gesammelten Daten enthalten detaillierte Informationen zu Anfragen, die an den ELB gesendet wurden. Jedes Protokoll enthält Informationen wie die Zeit, zu der die Anforderung einging, die Client-IP-Adresse, Latenzen, Anforderungspfade und Serverantworten.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.64(d)	Ein Finanzinstitut muss bei der Bereitstellung digitaler Dienste robuste technische Sicherheitskontrollen einführen, die Folgendes sicherstellen: (d) Vorhandensein eines ausreichenden Audit Trail und die Überwachung anomaler Transaktionen	guardduty-enabled-centralized	Amazon GuardDuty kann mithilfe von Threat Intelligence Feeds helfen, potenzielle Cybersicherheitsereignisse zu überwachen und zu erkennen. Dazu gehören Listen mit bösartigen IPs und maschinellen Lernmethoden zur Identifizierung unerwarteter, nicht autorisierter und bösartiger Aktivitäten in Ihrer AWS Cloud-Umgebung.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.64(d)	Ein Finanzinstitut muss bei der Bereitstellung digitaler Dienste robuste technische Sicherheitskontrollen einführen, die Folgendes sicherstellen: (d) Vorhandensein eines ausreichenden Audit Trail und die Überwachung anomaler Transaktionen	opensearch-logs-to-cloudwatch	Stellen Sie sicher, dass für Amazon OpenSearch Service-Domains Fehlerprotokolle aktiviert und zur Aufbewahrung und Beantwortung an Amazon CloudWatch Logs gestreamt werden. OpenSearch Service-Fehlerprotokolle können bei Sicherheits- und Zugriffsprüfungen helfen und bei der Diagnose von Verfügbarkeitsproblemen helfen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.64(d)	Ein Finanzinstitut muss bei der Bereitstellung digitaler Dienste robuste technische Sicherheitskontrollen einführen, die Folgendes sicherstellen: (d) Vorhandensein eines ausreichenden Audit Trail und die Überwachung anomaler Transaktionen	rds-enhanced-monitoring-enabled	Aktivieren Sie Amazon Relational Database Service (Amazon RDS), um die Verfügbarkeit von Amazon RDS zu überwachen. Dies bietet einen detaillierten Einblick in den Zustand Ihrer Amazon-RDS-Datenbank-Instances. Wenn der Amazon-RDS-Speicher mehr als ein zugrundeliegendes physisches Gerät verwendet, erfasst Enhanced Monitoring die Daten für jedes Gerät. Wenn die Datenbank-Instance von Amazon RDS in einer Multi-AZ-Bereitstellung ausgeführt wird, werden außerdem die Daten für jedes Gerät auf dem sekundären Host sowie die Metriken des sekundären Hosts erfasst.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.64(d)	Ein Finanzinstitut muss bei der Bereitstellung digitaler Dienste robuste technische Sicherheitskontrollen einführen, die Folgendes sicherstellen: (d) Vorhandensein eines ausreichenden Audit Trail und die Überwachung anomaler Transaktionen	rds-logging-enabled	Um die Protokollierung und Überwachung in Ihrer Umgebung zu erleichtern, stellen Sie sicher, dass die Amazon Relational Database Service (Amazon RDS)-Protokollierung aktiviert ist. Mit der Amazon-RDS-Protokollierung können Sie Ereignisse wie Verbindungen, Verbindungsabbrüche, Abfragen oder abgefragte Tabellen erfassen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.64(d)	Ein Finanzinstitut muss bei der Bereitstellung digitaler Dienste robuste technische Sicherheitskontrollen einführen, die Folgendes sicherstellen: (d) Vorhandensein eines ausreichenden Audit Trail und die Überwachung anomaler Transaktionen	redshift-cluster-configuration-check	Um Daten im Ruhezustand zu schützen, muss die Verschlüsselung für Ihre Amazon-Redshift-Cluster aktiviert sein. Sie müssen auch sicherstellen, dass die erforderlichen Konfigurationen auf Amazon-Redshift-Clustern bereitgestellt werden. Die Prüfungsprotokollierung muss aktiviert sein, um Informationen zu Verbindungen und Benutzeraktivitäten in der Datenbank bereitzustellen. Diese Regel erfordert, dass ein Wert für clusterDbEncrypted (Config Default: TRUE) und LoggingEnabled (Config Default: TRUE) gesetzt ist. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.64(d)	Ein Finanzinstitut muss bei der Bereitstellung digitaler Dienste robuste technische Sicherheitskontrollen einführen, die Folgendes sicherstellen: (d) Vorhandensein eines ausreichenden Audit Trail und die Überwachung anomaler Transaktionen	s3- bucket-logging-enabled	Die Amazon Simple Storage Service (Amazon S3)-Serverzugriffsprotokollierung bietet eine Methode zur Überwachung des Netzwerks im Hinblick auf potenzielle Cybersicherheitsereignisse. Die Ereignisse werden überwacht, indem detaillierte Aufzeichnungen über die Anfragen erfasst werden, die an einen Amazon-S3-Bucket gestellt wurden. Jeder Zugriffsprotokolleintrag enthält Details zu einer einzelnen Zugriffsanfrage. Zu den Details gehören Auftraggeber, Bucket-Name, Anforderungszeit, Anforderungsaktion, Antwortstatus und Fehlercode, falls relevant.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.64(d)	Ein Finanzinstitut muss bei der Bereitstellung digitaler Dienste robuste technische Sicherheitskontrollen einführen, die Folgendes sicherstellen: (d) Vorhandensein eines ausreichenden Audit Trail und die Überwachung anomaler Transaktionen	securityhub-enabled	AWS Security Hub hilft bei der Überwachung von unbefugtem Personal, Verbindungen, Geräten und Software. AWS Security Hub aggregiert, organisiert und priorisiert die Sicherheitswarnungen oder Ergebnisse mehrerer Dienste. AWS Einige dieser Dienste sind Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer und AWS Firewall Manager sowie AWS Partnerlösungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.64(d)	Ein Finanzinstitut muss bei der Bereitstellung digitaler Dienste robuste technische Sicherheitskontrollen einführen, die Folgendes sicherstellen: (d) Vorhandensein eines ausreichenden Audit Trail und die Überwachung anomaler Transaktionen	vpc-flow-logs-enabled	VPC-Flow-Protokolle erfassen detaillierte Informationsdatensätze über den IP-Datenverkehr, der zu und von Netzwerkschnittstellen in Ihrer Amazon Virtual Private Cloud (Amazon VPC) fließt. Standardmäßig enthalten Flow-Protokolldatensätze Werte für die verschiedenen Komponenten des IP-Flows, einschließlich Quelle, Ziel und Protokoll.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.64(d)	Ein Finanzinstitut muss bei der Bereitstellung digitaler Dienste robuste technische Sicherheitskontrollen einführen, die Folgendes sicherstellen: (d) Vorhandensein eines ausreichenden Audit Trail und die Überwachung anomaler Transaktionen	wafv2-logging-enabled	Um Ihnen bei der Protokollierung und Überwachung in Ihrer Umgebung zu helfen, aktivieren Sie die AWS WAF (V2) -Protokollierung im regionalen und globalen Web. ACLs AWS Die WAF-Protokollierung bietet detaillierte Informationen über den Datenverkehr, der von Ihrer Web-ACL analysiert wird. In den Protokollen werden die Uhrzeit aufgezeichnet, zu der die AWS WAF die Anfrage von Ihrer AWS Ressource erhalten hat, Informationen über die Anfrage und eine Aktion für die Regel, der jede Anfrage entsprach.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.64(e)	Ein Finanzinstitut muss bei der Bereitstellung digitaler Dienste robuste technische Sicherheitskontrollen einführen, die Folgendes gewährleisten: (e) Fähigkeit, den Wiederherstellungspunkt vor einem Vorfall oder einer Betriebsunterbrechung zu identifizieren und zu diesem zurückzukehren	aurora-resources-protected-by-Backup-Plan	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon Aurora Aurora-Ressourcen Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.64(e)	Ein Finanzinstitut muss bei der Bereitstellung digitaler Dienste robuste technische Sicherheitskontrollen einführen, die Folgendes gewährleisten: (e) Fähigkeit, den Wiederherstellungspunkt vor einem Vorfall oder einer Betriebsunterbrechung zu identifizieren und zu diesem zurückzukehren	db-instance-backup-enabled	Die Sicherungsfunktion von Amazon RDS erstellt Sicherungen Ihrer Datenbanken und Transaktionsprotokolle. Amazon RDS erstellt einen Snapshot für das Speichervolume Ihrer DB-Instance, sodass die gesamte DB-Instance gesichert wird. Sie können im System spezifische Aufbewahrungsfristen festlegen, um Ihre Ausfallsicherheitsanforderungen zu erfüllen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.64(e)	Ein Finanzinstitut muss bei der Bereitstellung digitaler Dienste robuste technische Sicherheitskontrollen einführen, die Folgendes gewährleisten: (e) Fähigkeit, den Wiederherstellungspunkt vor einem Vorfall oder einer Betriebsunterbrechung zu identifizieren und zu diesem zurückzukehren	dynamodb-pitr-enabled	Aktivieren Sie diese Regel, um zu überprüfen, ob die Informationen gesichert wurden. Es verwaltet auch die Backups, indem es sicherstellt, dass die point-in-time Wiederherstellung in Amazon DynamoDB aktiviert ist. Bei der Wiederherstellung werden fortlaufende Backups Ihrer Tabelle für die letzten 35 Tage gespeichert.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.64(e)	Ein Finanzinstitut muss bei der Bereitstellung digitaler Dienste robuste technische Sicherheitskontrollen einführen, die Folgendes gewährleisten: (e) Fähigkeit, den Wiederherstellungspunkt vor einem Vorfall oder einer Betriebsunterbrechung zu identifizieren und zu diesem zurückzukehren	dynamodb-resources-protected-by-Backup-Plan	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon DynamoDB DynamoDB-Ressourcen Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.64(e)	Ein Finanzinstitut muss bei der Bereitstellung digitaler Dienste robuste technische Sicherheitskontrollen einführen, die Folgendes gewährleisten: (e) Fähigkeit, den Wiederherstellungspunkt vor einem Vorfall oder einer Betriebsunterbrechung zu identifizieren und zu diesem zurückzukehren	ebs-optimized-instance	Eine optimierte Instance im Amazon Elastic Block Store (Amazon EBS) bietet zusätzliche, dedizierte Kapazität für Amazon-EBS-I/O-Vorgänge. Diese Optimierung bietet die beste Leistung für Ihr EBS-Volume, indem Konflikte zwischen Amazon-EBS-I/O und anderem Datenverkehr von Ihrer Instance minimiert werden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.64(e)	Ein Finanzinstitut muss bei der Bereitstellung digitaler Dienste robuste technische Sicherheitskontrollen einführen, die Folgendes gewährleisten: (e) Fähigkeit, den Wiederherstellungspunkt vor einem Vorfall oder einer Betriebsunterbrechung zu identifizieren und zu diesem zurückzukehren	ebs-resources-protected-by-Backup-Plan	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon Elastic Block Store (Amazon EBS) -Ressourcen Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.64(e)	Ein Finanzinstitut muss bei der Bereitstellung digitaler Dienste robuste technische Sicherheitskontrollen einführen, die Folgendes gewährleisten: (e) Fähigkeit, den Wiederherstellungspunkt vor einem Vorfall oder einer Betriebsunterbrechung zu identifizieren und zu diesem zurückzukehren	ec2--Plan resources-protected-by-backup	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon Elastic Compute Cloud (Amazon EC2) -Ressourcen Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.64(e)	Ein Finanzinstitut muss bei der Bereitstellung digitaler Dienste robuste technische Sicherheitskontrollen einführen, die Folgendes gewährleisten: (e) Fähigkeit, den Wiederherstellungspunkt vor einem Vorfall oder einer Betriebsunterbrechung zu identifizieren und zu diesem zurückzukehren	efs-resources-protected-by-Backup-Plan	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon Elastic File System (Amazon EFS) -Dateisysteme Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.64(e)	Ein Finanzinstitut muss bei der Bereitstellung digitaler Dienste robuste technische Sicherheitskontrollen einführen, die Folgendes gewährleisten: (e) Fähigkeit, den Wiederherstellungspunkt vor einem Vorfall oder einer Betriebsunterbrechung zu identifizieren und zu diesem zurückzukehren	elasticache-redis-cluster-automatic-Backup-Check	Wenn automatische Backups aktiviert sind, ElastiCache erstellt Amazon täglich ein Backup des Clusters. Die Sicherung kann für eine von Ihrer Organisation festgelegte Anzahl von Tagen aufbewahrt werden. Automatische Backups schützen vor Datenverlust. Bei einem Ausfall können Sie einen neuen Cluster erstellen, der Ihre Daten aus dem aktuellen Backup wiederherstellt.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.64(e)	Ein Finanzinstitut muss bei der Bereitstellung digitaler Dienste robuste technische Sicherheitskontrollen einführen, die Folgendes gewährleisten: (e) Fähigkeit, den Wiederherstellungspunkt vor einem Vorfall oder einer Betriebsunterbrechung zu identifizieren und zu diesem zurückzukehren	rds-resources-protected-by-Backup-Plan	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon Relational Database Service (Amazon RDS) -Ressourcen Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.64(e)	Ein Finanzinstitut muss bei der Bereitstellung digitaler Dienste robuste technische Sicherheitskontrollen einführen, die Folgendes gewährleisten: (e) Fähigkeit, den Wiederherstellungspunkt vor einem Vorfall oder einer Betriebsunterbrechung zu identifizieren und zu diesem zurückzukehren	redshift-backup-enabled	Stellen Sie zur Unterstützung der Datensicherungsprozesse sicher, dass Ihre Amazon-Redshift-Cluster über automatisierte Snapshots verfügen. Wenn automatisierte Snapshots für einen Cluster aktiviert sind, erstellt Redshift in regelmäßigen Abständen Snapshots dieses Clusters. Standardmäßig erstellt Redshift alle acht Stunden oder alle 5 GB einen Snapshot für jeden Knoten mit Datenänderungen oder je nachdem, was zuerst eintritt.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.64(e)	Ein Finanzinstitut muss bei der Bereitstellung digitaler Dienste robuste technische Sicherheitskontrollen einführen, die Folgendes gewährleisten: (e) Fähigkeit, den Wiederherstellungspunkt vor einem Vorfall oder einer Betriebsunterbrechung zu identifizieren und zu diesem zurückzukehren	s3- bucket-versioning-enabled	Die Versionsverwaltung von Amazon Simple Storage Service (Amazon S3)-Buckets hilft dabei, mehrere Varianten eines Objekts im selben Amazon-S3-Bucket zu speichern. Verwenden Sie die Versionsverwaltung, um sämtliche Versionen aller Objekte in Ihrem Amazon-S3-Bucket zu speichern, abzurufen oder wiederherzustellen. Mit der Versionsverwaltung können Sie Versionen sowohl nach unbeabsichtigten Benutzeraktionen als auch nach Anwendungsfehlern problemlos wiederherstellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.64(e)	Ein Finanzinstitut muss bei der Bereitstellung digitaler Dienste robuste technische Sicherheitskontrollen einführen, die Folgendes gewährleisten: (e) Fähigkeit, den Wiederherstellungspunkt vor einem Vorfall oder einer Betriebsunterbrechung zu identifizieren und zu diesem zurückzukehren	resources-protected-by-backups3-plan	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon Simple Storage Service (S3) -Buckets Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
11.7	Ein Finanzinstitut muss effektive Tools einsetzen, um die kontinuierliche und proaktive Überwachung und rechtzeitige Erkennung anomaler Aktivitäten in seiner Technologieinfrastruktur zu unterstützen. Der Umfang der Überwachung muss sich auf alle kritischen Systeme einschließlich der unterstützenden Infrastruktur erstrecken.	guardduty-enabled-centralized	Amazon GuardDuty kann mithilfe von Threat Intelligence Feeds helfen, potenzielle Cybersicherheitsereignisse zu überwachen und zu erkennen. Dazu gehören Listen mit bösartigen IPs und maschinellen Lernmethoden zur Identifizierung unerwarteter, nicht autorisierter und bösartiger Aktivitäten in Ihrer AWS Cloud-Umgebung.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
11.7	Ein Finanzinstitut muss effektive Tools einsetzen, um die kontinuierliche und proaktive Überwachung und rechtzeitige Erkennung anomaler Aktivitäten in seiner Technologieinfrastruktur zu unterstützen. Der Umfang der Überwachung muss sich auf alle kritischen Systeme einschließlich der unterstützenden Infrastruktur erstrecken.	securityhub-enabled	AWS Security Hub hilft bei der Überwachung von unbefugtem Personal, Verbindungen, Geräten und Software. AWS Security Hub aggregiert, organisiert und priorisiert die Sicherheitswarnungen oder Ergebnisse mehrerer Dienste. AWS Einige dieser Dienste sind Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer und AWS Firewall Manager sowie AWS Partnerlösungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
11.8	Ein Finanzinstitut muss sicherstellen, dass seine Cybersich erheitsaktivitäten kontinuierlich jede potenzielle Beeinträc htigung seiner Sicherheitskontrollen oder eine Schwächun g seiner Sicherhei tslage verhindern und aufdecken. Für große Finanzinstitute gehört die Durchführung einer vierteljährlichen Schwachstellenbewe rtung externer und interner Netzwerkk omponenten dazu, die alle kritischen Systeme unterstützen.	guardduty-enabled-centralized	Amazon GuardDuty kann mithilfe von Threat Intellige nce Feeds helfen, potenzielle Cybersich erheitsereignisse zu überwachen und zu erkennen. Dazu gehören Listen mit bösartigen IPs und maschinel len Lernmethoden zur Identifizierung unerwarteter, nicht autorisierter und bösartiger Aktivitäten in Ihrer AWS Cloud-Umgebung.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
11.8	Ein Finanzinstitut muss sicherstellen, dass seine Cybersicherheitsaktivitäten kontinuierlich jede potenzielle Beeinträchtigung seiner Sicherheitskontrollen oder eine Schwächung seiner Sicherheitslage verhindern und aufdecken. Für große Finanzinstitute gehört die Durchführung einer vierteljährlichen Schwachstellenbewertung externer und interner Netzwerkkomponenten dazu, die alle kritischen Systeme unterstützen.	securityhub-enabled	AWS Security Hub hilft bei der Überwachung von unbefugtem Personal, Verbindungen, Geräten und Software. AWS Security Hub aggregiert, organisiert und priorisiert die Sicherheitswarnungen oder Ergebnisse mehrerer Dienste. AWS Einige dieser Dienste sind Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer und AWS Firewall Manager sowie AWS Partnerlösungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
11.18(c)(f)	Das SOC muss in der Lage sein, die folgenden Funktione n zu erfüllen: (c) Schwachstellenmana gement; (f) Bereitste llung eines Lagebilds zur Erkennung von Gegnern und Bedrohungen, einschließlich der Analyse von Bedrohungsinformat ionen und -vorgängen sowie der Überwachu ng von Indicators of Compromise (IOC, Kompromittierungsi ndikatoren). Dazu gehören fortschri ttliche Verhalten sanalysen zur Erkennung signatur- und dateiloser Malware und zur Identifizierung von Anomalien, die Sicherheitsbedrohu ngen darstellen können, auch an Endpunkten und auf Netzwerkebenen.	guardduty-enabled-centralized	Amazon GuardDuty kann mithilfe von Threat Intellige nce Feeds helfen, potenzielle Cybersich erheitsereignisse zu überwachen und zu erkennen. Dazu gehören Listen mit bösartigen IPs und maschinel len Lernmethoden zur Identifizierung unerwarteter, nicht autorisierter und bösartiger Aktivitäten in Ihrer AWS Cloud-Umgebung.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
11.18(c)(f)	Das SOC muss in der Lage sein, die folgenden Funktionen zu erfüllen: (c) Schwachstellenmanagement; (f) Bereitstellung eines Lagebilds zur Erkennung von Gegnern und Bedrohungen, einschließlich der Analyse von Bedrohungsinformationen und -vorgängen sowie der Überwachung von Indicators of Compromise (IOC, Kompromittierungsindikatoren). Dazu gehören fortschrittliche Verhaltensanalysen zur Erkennung signatur- und dateiloser Malware und zur Identifizierung von Anomalien, die Sicherheitsbedrohungen darstellen können, auch an Endpunkten und auf Netzwerkebenen.	guardduty-non-archived-findings	Amazon GuardDuty hilft Ihnen dabei, die Auswirkungen eines Vorfalls zu verstehen, indem es die Ergebnisse nach Schweregrad klassifiziert: niedrig, mittel und hoch. Diese Klassifizierungen können Sie zur Festlegung von entsprechenden Strategien und Prioritäten zur Behebung solcher Vorfälle verwenden. Mit dieser Regel können Sie optional daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7) und daysHighSev (Config Default: 1) für nicht archivierte Ergebnisse festlegen, wie es die Richtlinien Ihrer Organisation erfordern.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
11.18(c)(f)	Das SOC muss in der Lage sein, die folgenden Funktione n zu erfüllen: (c) Schwachstellenmana gement; (f) Bereitste llung eines Lagebilds zur Erkennung von Gegnern und Bedrohungen, einschließlich der Analyse von Bedrohungsinformat ionen und -vorgängen sowie der Überwachu ng von Indicators of Compromise (IOC, Kompromittierungsi ndikatoren). Dazu gehören fortschri ttliche Verhalten sanalysen zur Erkennung signatur- und dateiloser Malware und zur Identifizierung von Anomalien, die Sicherheitsbedrohu ngen darstellen können, auch an Endpunkten und auf Netzwerkebenen.	securityhub-enabled	AWS Security Hub hilft bei der Überwachung von unbefugtem Personal, Verbindun gen, Geräten und Software. AWS Security Hub aggregiert, organisie rt und priorisie rt die Sicherhei tswarnungen oder Ergebnisse mehrerer Dienste. AWS Einige dieser Dienste sind Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer und AWS Firewall Manager sowie AWS Partnerlösungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
Anhang 5.1	Führen Sie regelmäßig eine Überprüfung der Konfigurations- und Regeleinstellungen für alle Sicherheitsgeräte durch. Verwenden Sie automatisierte Tools, um Änderungen an den Konfigurations- und Regeleinstellungen zu überprüfen und zu überwachen.	guardduty-enabled-centralized	Amazon GuardDuty kann mithilfe von Threat Intelligence Feeds helfen, potenzielle Cybersicherheitsereignisse zu überwachen und zu erkennen. Dazu gehören Listen mit bösartigen IPs und maschinellen Lernmethoden zur Identifizierung unerwarteter, nicht autorisierter und bösartiger Aktivitäten in Ihrer AWS Cloud-Umgebung.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
Anhang 5.1	Führen Sie regelmäßig eine Überprüfung der Konfigurations- und Regeleinstellungen für alle Sicherheitsgeräte durch. Verwenden Sie automatisierte Tools, um Änderungen an den Konfigurations- und Regeleinstellungen zu überprüfen und zu überwachen.	securityhub-enabled	AWS Security Hub hilft bei der Überwachung von unbefugtem Personal, Verbindungen, Geräten und Software. AWS Security Hub aggregiert, organisiert und priorisiert die Sicherheitswarnungen oder Ergebnisse mehrerer Dienste. AWS Einige dieser Dienste sind Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer und AWS Firewall Manager sowie AWS Partnerlösungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
Anhang 5.5(b)	Stellen Sie sicher, dass die Sicherheitskontrollen für server-to-server externe Netzwerkverbindungen Folgendes umfassen: (b) Verwendung sicherer Tunnel wie Transport Layer Security (TLS) und Virtual Private Network (VPN) IPSec	alb-http-to-https-Umleitungsprüfung	Um Daten während der Übertragung zu schützen, stellen Sie sicher, dass Ihr Application Load Balancer unverschlüsselte HTTP-Anfragen automatisch an HTTPS umleitet. Da sensible Daten vorhanden sein können, sollten Sie die Verschlüsselung bei der Übertragung aktivieren, um diese Daten zu schützen.
Anhang 5.5(b)	Stellen Sie sicher, dass die Sicherheitskontrollen für server-to-server externe Netzwerkverbindungen Folgendes umfassen: (b) Verwendung sicherer Tunnel wie Transport Layer Security (TLS) und Virtual Private Network (VPN) IPSec	api-gw-ssl-enabled	Stellen Sie sicher, dass die REST-API-Stufen von Amazon API Gateway mit SSL-Zertifikaten konfiguriert sind, damit Backend-Systeme überprüfen können, ob Anforderungen von API Gateway stammen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
Anhang 5.5(b)	Stellen Sie sicher, dass die Sicherheitskontrollen für server-to-server externe Netzwerkverbindungen Folgendes umfassen: (b) Verwendung sicherer Tunnel wie Transport Layer Security (TLS) und Virtual Private Network (VPN) IPSec	opensearch-https-required	Da sensible Daten existieren können und um Daten während der Übertragung zu schützen, sollten Sie sicherstellen, dass HTTPS für Verbindungen zu Ihren Amazon OpenSearch Service-Domains aktiviert ist.
Anhang 5.5(b)	Stellen Sie sicher, dass die Sicherheitskontrollen für server-to-server externe Netzwerkverbindungen Folgendes umfassen: (b) Verwendung sicherer Tunnel wie Transport Layer Security (TLS) und Virtual Private Network (VPN) IPSec	opensearch-node-to-node-Verschlüsselungsprüfung	Stellen Sie sicher, dass die node-to-node Verschlüsselung für Amazon OpenSearch Service aktiviert ist. Node-to-nodeVerschlüsselung ermöglicht die TLS 1.2-Verschlüsselung für die gesamte Kommunikation innerhalb der Amazon Virtual Private Cloud (Amazon VPC). Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
Anhang 5.5(b)	Stellen Sie sicher, dass die Sicherheitskontrollen für server-to-server externe Netzwerkverbindungen Folgendes umfassen: (b) Verwendung sicherer Tunnel wie Transport Layer Security (TLS) und Virtual Private Network (VPN) IPSec	redshift-require-tls-ssl	Stellen Sie sicher, dass Ihre Amazon-Redshift-Cluster eine TLS/SSL-Verschlüsselung erfordern, um eine Verbindung zu SQL-Clients herzustellen. Da sensible Daten vorhanden sein können, sollten Sie die Verschlüsselung bei der Übertragung aktivieren, um diese Daten zu schützen.
Anhang 5.5(b)	Stellen Sie sicher, dass die Sicherheitskontrollen für server-to-server externe Netzwerkverbindungen Folgendes umfassen: (b) Verwendung sicherer Tunnel wie Transport Layer Security (TLS) und Virtual Private Network (VPN) IPSec	s3- bucket-ssl-requests-only	Um Daten während der Übertragung zu schützen, stellen Sie sicher, dass Ihre Amazon Simple Storage Service (Amazon S3)-Buckets Anfragen zur Verwendung von Secure Socket Layer (SSL)-Buckets erfordern. Da sensible Daten vorhanden sein können, sollten Sie die Verschlüsselung bei der Übertragung aktivieren, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
Anhang 5.5(c)	Stellen Sie sicher, dass die Sicherheitskontrollen für server-to-server externe Netzwerkverbindungen Folgendes umfassen: (c) Bereitstellung von Staging-Servern mit adäquaten Perimeterabwehr- und Schutzmaßnahmen wie Firewall, IPS und Virenschutz.	guardduty-enabled-centralized	Amazon GuardDuty kann mithilfe von Threat Intelligence Feeds helfen, potenzielle Cybersicherheitsereignisse zu überwachen und zu erkennen. Dazu gehören Listen mit bösartigen IPs und maschinellen Lernmethoden zur Identifizierung unerwarteter, nicht autorisierter und bösartiger Aktivitäten in Ihrer AWS Cloud-Umgebung.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
Anhang 5.5(c)	Stellen Sie sicher, dass die Sicherheitskontrollen für server-to-server externe Netzwerkverbindungen Folgendes umfassen: (c) Bereitstellung von Staging-Servern mit angemessenem Perimeterschutz und Schutz wie Firewall, IPS und Virenschutz.	vpc-default-security-group-geschlossen	Sicherheitsgruppen von Amazon Elastic Compute Cloud (Amazon EC2) können bei der Verwaltung des Netzwerkzugriffs helfen, indem sie eine statusbehaftete Filterung des ein- und ausgehenden Netzwerkverkehrs zu Ressourcen bereitstellen. AWS Die Beschränkung des gesamten Datenverkehrs auf die Standardsicherheitsgruppe hilft dabei, den Fernzugriff auf Ihre Ressourcen einzuschränken. AWS

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
Anhang 5.5(c)	Stellen Sie sicher, dass die Sicherheitskontrollen für server-to-server externe Netzwerkverbindungen Folgendes umfassen: (c) Bereitstellung von Staging-Servern mit angemessenem Perimeterschutz und Schutz wie Firewall, IPS und Virenschutz.	vpc-sg-open-only-to-authorized-ports	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass gemeinsame Ports für Amazon Elastic Compute Cloud (Amazon EC2) -Sicherheitsgruppen eingeschränkt sind. Wenn der Zugriff auf Ports nicht auf vertrauenswürdige Quellen beschränkt wird, kann dies zu Angriffen auf die Verfügbarkeit, Integrität und Vertraulichkeit von Systemen führen. Durch die Beschränkung des Zugriffs auf Ressourcen innerhalb einer Sicherheitsgruppe aus dem Internet (0.0.0.0/0) kann der Fernzugriff auf interne Systeme gesteuert werden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
Anhang 5.6	Stellen Sie sicher, dass die Sicherheitskontrollen für den Fernzugriff auf Server Folgendes umfassen: (a) den Zugriff nur auf gehärtete und gesperrte Endpunktgeräte beschränken; (b) sichere Tunnel wie TLS und VPN verwenden IPSec; (c) Gateway-Server mit adäquaten Perimeterabwehr und Schutz wie Firewall, IPS und Virenschutz einsetzen; und (d) relevante Ports sofort nach Ablauf des Fernzugriffs schließen.	alb-http-to-https-Umleitungsprüfung	Um Daten während der Übertragung zu schützen, stellen Sie sicher, dass Ihr Application Load Balancer unverschlüsselte HTTP-Anfragen automatisch an HTTPS umleitet. Da sensible Daten vorhanden sein können, sollten Sie die Verschlüsselung bei der Übertragung aktivieren, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
Anhang 5.6	Stellen Sie sicher, dass die Sicherheitskontrollen für den Fernzugriff auf den Server Folgendes umfassen: (a) Beschränken Sie den Zugriff nur auf gehärtete und gesperrte Endgeräte; (b) verwenden Sie sichere Tunnel wie TLS und VPN IPSec; (c) stellen Sie einen Gateway-Server mit adäquaten Perimeterabwehrmaßnahmen und Schutzmaßnahmen wie Firewall, IPS und Virenschutz bereit; und (d) schließen Sie die entsprechenden Ports sofort nach Ablauf des Fernzugriffs.	api-gw-ssl-enabled	Stellen Sie sicher, dass die REST-API-Stufen von Amazon API Gateway mit SSL-Zertifikaten konfiguriert sind, damit Backend-Systeme überprüfen können, ob Anforderungen von API Gateway stammen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
Anhang 5.6	Stellen Sie sicher, dass die Sicherheitskontrollen für den Fernzugriff auf Server Folgendes umfassen: (a) Beschränken Sie den Zugriff nur auf gehärtete und gesperrte Endpunktgeräte; (b) verwenden Sie sichere Tunnel wie TLS und VPN IPSec; (c) stellen Sie einen Gateway-Server mit angemessenen Perimeter abwehrmaßnahmen und Schutzmaßnahmen wie Firewall, IPS und Virenschutz bereit; und (d) schließen Sie die entsprechenden Ports sofort nach Ablauf des Fernzugriffs.	opensearch-https-required	Da sensible Daten existieren können und um Daten während der Übertragung zu schützen, sollten Sie sicherstellen, dass HTTPS für Verbindungen zu Ihren Amazon OpenSearch Service-Domains aktiviert ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
Anhang 5.6	Stellen Sie sicher, dass die Sicherheitskontrollen für den Fernzugriff auf Server Folgendes umfassen: (a) den Zugriff nur auf gehärtete und gesperrte Endpunktgeräte beschränken; (b) sichere Tunnel wie TLS und VPN verwenden IPSec; (c) Gateway-Server mit adäquaten Perimeterabwehr und Schutz wie Firewall, IPS und Virenschutz einsetzen; und (d) relevante Ports sofort nach Ablauf des Fernzugriffs schließen.	redshift-require-tls-ssl	Stellen Sie sicher, dass Ihre Amazon-Redshift-Cluster eine TLS/SSL-Verschlüsselung erfordern, um eine Verbindung zu SQL-Clients herzustellen. Da sensible Daten vorhanden sein können, sollten Sie die Verschlüsselung bei der Übertragung aktivieren, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
Anhang 5.6	Stellen Sie sicher, dass die Sicherheitskontrollen für den Fernzugriff auf Server Folgendes umfassen: (a) Beschränken Sie den Zugriff nur auf gehärtete und gesperrte Endpunktgeräte; (b) verwenden Sie sichere Tunnel wie TLS und VPN IPSec; (c) stellen Sie einen Gateway-Server mit angemessenen Perimeter abwehrmaßnahmen und Schutzmaßnahmen wie Firewall, IPS und Virenschutz bereit; und (d) schließen Sie die entsprechenden Ports sofort nach Ablauf des Fernzugriffs.	vpc-default-security-group-geschlossen	Sicherheitsgruppen von Amazon Elastic Compute Cloud (Amazon EC2) können bei der Verwaltung des Netzwerkzugriffs helfen, indem sie eine statusbehaftete Filterung des ein- und ausgehenden Netzwerkverkehrs zu Ressourcen bereitstellen. AWS Die Beschränkung des gesamten Datenverkehrs auf die Standardsicherheitsgruppe hilft dabei, den Fernzugriff auf Ihre Ressourcen einzuschränken. AWS

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
Anhang 5.6	Stellen Sie sicher, dass die Sicherheitskontrollen für den Fernzugriff auf Server Folgendes umfassen: (a) den Zugriff nur auf gehärtete und gesperrte Endpunktgeräte beschränken; (b) sichere Tunnel wie TLS und VPN verwenden IPSec; (c) Gateway-Server mit adäquaten Perimeterabwehr und Schutz wie Firewall, IPS und Virenschutz einsetzen; und (d) relevante Ports sofort nach Ablauf des Fernzugriffs schließen.	vpc-sg-open-only-to-authorized-ports	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass gemeinsame Ports für Amazon Elastic Compute Cloud (Amazon EC2) -Sicherheitsgruppen eingeschränkt sind. Wenn der Zugriff auf Ports nicht auf vertrauenswürdige Quellen beschränkt wird, kann dies zu Angriffen auf die Verfügbarkeit, Integrität und Vertraulichkeit von Systemen führen. Durch die Beschränkung des Zugriffs auf Ressourcen innerhalb einer Sicherheitsgruppe aus dem Internet (0.0.0.0/0) kann der Fernzugriff auf interne Systeme gesteuert werden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
Anhang 10 Teil B – 1 (a)	Ein Finanzinstitut muss eine robuste Cloud-Architektur entwerfen und sicherstellen, dass diese Gestaltung den einschlägigen internationalen Standards für die beabsichtigte Anwendung entspricht.	account-part-of-organizations	Durch die zentrale Verwaltung AWS-Konten innerhalb von AWS Organizations wird sichergestellt, dass die Konten den Vorschriften entsprechen. Eine fehlende zentrale Kontoverwaltung kann zu inkonsistenten Kontokonfigurationen führen, wodurch Ressourcen und sensible Daten offengelegt werden können.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
Anhang 10 Teil B – 1 (b)	Finanzinstitute werden ermutigt, Zero-Trust-Prinzip ien einzuführen, um eine cyberresi stente Architekt ur zu schaffen, indem sie von einer „Sicherheitsverlet zung“ ausgehen, Mikrosegmentierung defense-in-depth durchsetzen, Zugriffsr echte mit deny-by-default „geringsten Rechten“ durchsetzen und gegebenenfalls gründliche Inspektio nen und kontinuie rliche Validierungen durchführen.	alb-waf-enabled	Stellen Sie sicher, dass AWS WAF auf Elastic Load Balancers (ELB) aktiviert ist, um Webanwendungen zu schützen. Eine WAF trägt zum Schutz Ihrer Webanwend ungen oder APIs vor gängigen Web-Explo its bei. Diese Web-Exploits können sich auf die Verfügbar keit auswirken, die Sicherheit gefährden oder übermäßige Ressourcen in Ihrer Umgebung verbrauch en.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
Anhang 10 Teil B – 1 (b)	Finanzinstitute werden ermutigt, Zero-Trust-Prinzipien anzuwenden, um eine cyberresistente Architektur zu schaffen, indem sie von einer „Sicherheitsverletzung“ ausgehen, Mikrosegmentierung und Zugriffsrechte mit deny-by-default „geringsten Rechten“ defense-in-depth durchsetzen und gegebenenfalls gründliche Inspektionen und kontinuierliche Validierungen durchführen.	subnet-auto-assign-public-ip ist deaktiviert	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon Virtual Private Cloud (VPC) -Subnetzen nicht automatisch eine öffentliche IP-Adresse zugewiesen wird. Amazon Elastic Compute Cloud (EC2) -Instances, die in Subnetzen gestartet werden, in denen dieses Attribut aktiviert ist, haben ihrer primären Netzwerkschnittstelle eine öffentliche IP-Adresse zugewiesen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
Anhang 10 Teil B – 1 (b)	Finanzinstitute werden ermutigt, Zero-Trust-Prinzip ien anzuwenden, um eine cyberresi stente Architekt ur zu schaffen, indem sie von einer „Sicherheitsverlet zung“ ausgehen, Mikrosegmentierung und Zugriffsrechte mit deny-by-default „geringsten Rechten“ kombinieren und gegebenenfalls gründliche Inspektio nen und kontinuie rliche Validierungen durchführen. defense-in-depth	vpc-default-security-group-geschlossen	Sicherheitsgruppen von Amazon Elastic Compute Cloud (Amazon EC2) können bei der Verwaltung des Netzwerkzugriffs helfen, indem sie eine statusbehaftete Filterung des ein- und ausgehenden Netzwerkverkehrs zu Ressourcen bereitstellen. AWS Die Beschränk ung des gesamten Datenverkehrs auf die Standardsicherheit sgruppe hilft dabei, den Fernzugriff auf Ihre Ressourcen einzuschränken. AWS

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
Anhang 10 Teil B – 1 (b)	Finanzinstitute werden ermutigt, Zero-Trust-Prinzipien anzuwenden, um eine cyberresistente Architektur zu schaffen, indem sie von einer „Sicherheitsverletzung“ ausgehen, Mikrosegmentierung und Zugriffsrechte mit den geringsten Rechten defense-in-depth durchsetzen und gegebenenfalls gründliche Inspektionen und kontinuierliche Validierungen durchführen. deny-by-default	vpc-sg-open-only-to-authorized-ports	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass gemeinsame Ports für Amazon Elastic Compute Cloud (Amazon EC2) -Sicherheitsgruppen eingeschränkt sind. Wenn der Zugriff auf Ports nicht auf vertrauenswürdige Quellen beschränkt wird, kann dies zu Angriffen auf die Verfügbarkeit, Integrität und Vertraulichkeit von Systemen führen. Durch die Beschränkung des Zugriffs auf Ressourcen innerhalb einer Sicherheitsgruppe aus dem Internet (0.0.0.0/0) kann der Fernzugriff auf interne Systeme gesteuert werden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
Anhang 10 Teil B – 1 (c)	Ein Finanzins titut sollte bei der Bewältigung der Komplexität der Cloud-Netzwerkumge bung den neuesten Netzwerkarchitektu ransatz und geeignete Netzwerkdesignkonz epte und -lösungen für die Verwaltun g und Überwachu ng der granularen Netzwerksicherheit und die zentrale Netzwerkbereitstel lung verwenden.	guardduty-enabled-centralized	Amazon GuardDuty kann mithilfe von Threat Intellige nce Feeds helfen, potenzielle Cybersich erheitsereignisse zu überwachen und zu erkennen. Dazu gehören Listen mit bösartigen IPs und maschinel len Lernmethoden zur Identifizierung unerwarteter, nicht autorisierter und bösartiger Aktivitäten in Ihrer AWS Cloud-Umgebung.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
Anhang 10 Teil B – 1 (c)	Ein Finanzinstitut sollte bei der Bewältigung der Komplexität der Cloud-Netzwerkumgebung den neuesten Netzwerkarchitektuansatz und geeignete Netzwerkdesignkonzepte und -lösungen für die Verwaltung und Überwachung der granularen Netzwerksicherheit und die zentrale Netzwerkbereitstellung verwenden.	vpc-flow-logs-enabled	VPC-Flow-Protokolle erfassen detaillierte Informationsdatensätze über den IP-Datenverkehr, der zu und von Netzwerkschnittstellen in Ihrer Amazon Virtual Private Cloud (Amazon VPC) fließt. Standardmäßig enthalten Flow-Protokolldatensätze Werte für die verschiedenen Komponenten des IP-Flows, einschließlich Quelle, Ziel und Protokoll.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
Anhang 10 Teil B – 1 (d)	Ein Finanzinstitut sollte sichere und verschlüsselte Kommunikationskanäle für die Migration physischer Server, Anwendungen oder Daten auf die Cloud-Plattformen einrichten und nutzen.	dms-replication-not-public	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass auf DMS-Replikationsinstanzen nicht öffentlich zugegriffen werden kann. DMS-Replikations-Instances können vertrauliche Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
Anhang 10 Teil B – 1 (d)	Ein Finanzinstitut sollte sichere und verschlüsselte Kommunikationskanäle für die Migration physischer Server, Anwendungen oder Daten auf die Cloud-Plattformen einrichten und nutzen.	s-3 bucket-ssl-requests-only	Um Daten während der Übertragung zu schützen, stellen Sie sicher, dass Ihre Amazon Simple Storage Service (Amazon S3)-Buckets Anfragen zur Verwendung von Secure Socket Layer (SSL)-Buckets erfordern. Da sensible Daten vorhanden sein können, sollten Sie die Verschlüsselung bei der Übertragung aktivieren, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
Anhang 10 Teil B – 1 (f) i)	Durch die zunehmende Nutzung von Anwendung sprogrammierschnittstellen (API) durch Finanzinstitute zur Vernetzung mit externen Anwendungsdienstleistern könnte die Effizienz der Bereitstellung neuer Dienste erhöht werden. Dies kann jedoch die Angriffsfläche für Cyberangriffe vergrößern und jedes Missmanagement kann die Auswirkungen eines Vorfalls im Bereich der Informationssicherheit verstärken. Ein Finanzinstitut sollte sicherstellen, dass es strengen Verwaltungs- und Kontrollmechanismen unterliegt, die Folgendes beinhalten: i) es APIs sollte so konzipiert sein, dass die Dienste widerstandsfähig APIs sind, um das Risiko	api-gwv2- authorization-type-configured	Stellen Sie sicher, dass für die API-Route von Amazon API Gateway v2 ein Autorisierungstyp festgelegt ist, um unbefugten Zugriff auf die zugrunde liegenden Backend-Ressourcen zu verhindern.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	einzelner Ausfallst ellen zu vermeiden, und sicher konfiguriert und mit angemesse nen Zugangsko ntrollen ausgestattet sein;		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
Anhang 10 Teil B – 1 (f) ii)	Durch die zunehmende Nutzung von Anwendungsprogrammierschnittstellen (API) durch Finanzinstitute zur Vernetzung mit externen Anwendungsdienstleistern könnte die Effizienz der Bereitstellung neuer Dienste erhöht werden. Dies kann jedoch die Angriffsfläche für Cyberangriffe vergrößern und jedes Missmanagement kann die Auswirkungen eines Vorfalls im Bereich der Informationssicherheit verstärken. Ein Finanzinstitut sollte sicherstellen, dass APIs es strengen Verwaltungs- und Kontrollmechanismen unterliegt, die Folgendes beinhalten: ii) sie APIs sollten mit angemessenen Maßnahmen zur Reaktion auf	api-gw-associated-with-WAF	AWS Mit WAF können Sie eine Reihe von Regeln (als Web Access Control List (Web ACL) bezeichnet) konfigurieren, die Webanfragen auf der Grundlage von anpassbaren Websicherheitsregeln und -bedingungen, die Sie definieren, zulassen, blockieren oder zählen. Stellen Sie sicher, dass Ihre Amazon-API-Gateway-Stufe mit einer WAF-Web-ACL verknüpft ist, um sie vor böswilligen Angriffen zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	Zwischenfälle verfolgt und vor Cyberangr iffen überwacht und rechtzeitig außer Betrieb genommen werden, wenn sie nicht mehr genutzt werden.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
Anhang 10 Teil B – 1 (f) ii)	Durch die zunehmende Nutzung von Anwendungsprogrammierschnittstellen (API) durch Finanzinstitute zur Vernetzung mit externen Anwendungsdienstleistern könnte die Effizienz der Bereitstellung neuer Dienste erhöht werden. Dies kann jedoch die Angriffsfläche für Cyberangriffe vergrößern und jedes Missmanagement kann die Auswirkungen eines Vorfalls im Bereich der Informationssicherheit verstärken. Ein Finanzinstitut sollte sicherstellen, dass APIs es strengen Verwaltungs- und Kontrollmechanismen unterliegt, die Folgendes beinhalten: ii) sie APIs sollten mit angemessenen Maßnahmen zur Reaktion auf	api-gw-execution-logging-aktiviert	Die API-Gateway-Protokollierung zeigt detaillierte Ansichten der Benutzer, die auf die API zugegriffen haben, und wie diese Benutzer auf die API zugegriffen haben. Diese Einblicke ermöglichen die Transparenz von Benutzeraktivitäten.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	Cyberangriffe verfolgt und überwacht werden und rechtzeitig außer Betrieb genommen werden, wenn sie nicht mehr genutzt werden.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
Anhang 10 Teil B – 2 (b) ii)	Ein Finanzinstitut sollte kontinuierlich erweiterte Cloud-Funktionen nutzen, um die Sicherhei t der Cloud-Ser vices zu verbesser n, und Finanzins titute werden unter anderem aufgeford ert: ii) unverände rliche Infrastru kturpraktiken für die Bereitstellung von Services anzuwende n, um das Ausfallri siko zu verringern, indem sie eine neue Umgebung mit der neuesten stabilen Version der Software schaffen. Die laufende Überwachung der Cloud-Umg ebung sollte auch die automatische Erkennung von Änderungen an der unverände rlichen Infrastruktur umfassen, um die Compliance-Prüfung zu verbessern und	cloudformation-stack-notification-check	Um unbeabsichtigte Änderungen an den zugrunde liegenden AWS Ressourcen zu erkennen, stellen Sie sicher, dass Ihr CloudFormation Stack so konfiguriert ist, dass er Ereignisb enachrichtigungen an ein Amazon SNS SNS-Thema sendet.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	sich entwickelnde Cyberangriffe zu bekämpfen.		
Anhang 10 Teil B – 3 (b) vi)	Ein Finanzinstitut sollte sicherstellen, dass virtuelle Maschinen- und Container-Images ordnungsgemäß konfiguriert, gehärtet und überwacht werden. Dies beinhaltet Folgendes: vi) Gespeicherte Images werden einer Sicherheitsüberwachung unterzogen, um unbefugten Zugriff und Änderungen zu verhindern.	cloudtrail-security-trail-enabled	Diese Regel trägt dazu bei, die Verwendung der AWS empfohlenen bewährten Sicherheitsmethoden für sicherzustellen AWS CloudTrail, indem geprüft wird, ob mehrere Einstellungen aktiviert sind. Dazu gehören die Verwendung von Protokollverschlüsselung, Protokollvalidierung und Aktivierung AWS CloudTrail in mehreren Regionen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
Anhang 10 Teil B – 5 (a) i)	Im Rahmen effektiver Wiederherstellungskapazitäten sollten Finanzinstitute sicherstellen, dass die bestehenden Sicherungs- und Wiederherstellungsverfahren auf Cloud-Services ausgedehnt werden, was Folgendes beinhaltet: i) Definition und Formalisierung der Sicherungs- und Wiederherstellungsstrategie in der Planungsphase der Cloud-Einführung;	aurora-resources-protected-by-Backup-Plan	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon Aurora Aurora-Ressourcen Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
Anhang 10 Teil B – 5 (a) i)	Im Rahmen effektiver Wiederherstellungskapazitäten sollten Finanzinstitute sicherstellen, dass die bestehenden Sicherungs- und Wiederherstellungsverfahren auf Cloud-Services ausgedehnt werden, was Folgendes beinhaltet: i) Definition und Formalisierung der Sicherungs- und Wiederherstellungsstrategie in der Planungsphase der Cloud-Einführung;	dynamodb-resources-protected-by-Backup-Plan	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon DynamoDB DynamoDB-Ressourcen Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
Anhang 10 Teil B – 5 (a) i)	Im Rahmen effektiver Wiederherstellungskapazitäten sollten Finanzinstitute sicherstellen, dass die bestehenden Sicherungs- und Wiederherstellungsverfahren auf Cloud-Services ausgedehnt werden, was Folgendes beinhaltet: i) Definition und Formalisierung der Sicherungs- und Wiederherstellungsstrategie in der Planungsphase der Cloud-Einführung;	ebs-resources-protected-by-Backup-Plan	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon Elastic Block Store (Amazon EBS) -Ressourcen Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
Anhang 10 Teil B – 5 (a) i)	Im Rahmen effektiver Wiederherstellungskapazitäten sollten Finanzinstitute sicherstellen, dass die bestehenden Sicherungs- und Wiederherstellungsverfahren auf Cloud-Services ausgedehnt werden, was Folgendes beinhaltet: i) Definition und Formalisierung der Sicherungs- und Wiederherstellungsstrategie in der Planungsphase der Cloud-Einführung;	efs-resources-protected-by-Backup-Plan	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon Elastic File System (Amazon EFS) -Dateisysteme Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
Anhang 10 Teil B – 5 (a) i)	Im Rahmen effektiver Wiederherstellungskapazitäten sollten Finanzinstitute sicherstellen, dass die bestehenden Sicherungs- und Wiederherstellungsverfahren auf Cloud-Services ausgedehnt werden, was Folgendes beinhaltet: i) Definition und Formalisierung der Sicherungs- und Wiederherstellungsstrategie in der Planungsphase der Cloud-Einführung;	rds-resources-protected-by-Backup-Plan	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon Relational Database Service (Amazon RDS) -Ressourcen Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
Anhang 10 Teil B – 5 (a) i)	Im Rahmen effektiver Wiederherstellungskapazitäten sollten Finanzinstitute sicherstellen, dass die bestehenden Sicherungs- und Wiederherstellungsverfahren auf Cloud-Services ausgedehnt werden, was Folgendes beinhaltet: i) Definition und Formalisierung der Sicherungs- und Wiederherstellungsstrategie in der Planungsphase der Cloud-Einführung;	s3-Plan resources-protected-by-backup	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon Simple Storage Service (S3) -Buckets Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
Anhang 10 Teil B – 5 (b)	Ein Finanzinstitut sollte sicherstellen, dass die Sicherungs- und Wiederherstellungsverfahren regelmäßig getestet werden, um die Wiederherstellungsfähigkeit zu überprüfen. Die Häufigkeit der Backup-Verfahren sollte der Kritikalität und dem Recovery Point Objective (RPO) des Systems angemessen sein. Bei erfolglosen Backups sollte das Finanzinstitut umgehend Abhilfemaßnahmen ergreifen.	backup-plan-min-frequency-and-min-retention-check	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihr AWS Backup-Plan auf eine Mindestfrequenz und Aufbewahrung festgelegt ist. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen. Mit dieser Regel können Sie die Parameter requiredFrequencyValue (Config default: 1), requiredRetentionDays (Config default: 35) und requiredFrequencyUnit

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			(Config default: days) festlegen. Der tatsächliche Wert muss den Anforderungen Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
Anhang 10 Teil B – 5 (c) i)	Ein Finanzinstitut sollte eine ausreichende Sicherung und Wiederherstellung der virtuellen Maschine und des Containers sicherstellen, einschließlich der Backup-Konfigurationseinstellungen (für IaaS und PaaS, sofern relevant), was Folgendes beinhaltet: i) die Fähigkeit zur Wiederherstellung einer virtuellen Maschine und eines Containers gemäß den Vorgaben der Geschäftswiederherstellungsziele sicherstellen; point-in-time	backup-plan-min-frequency-and-min-retention-check	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihr AWS Backup-Plan auf eine Mindestfrequenz und Aufbewahrung festgelegt ist. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen. Mit dieser Regel können Sie die Parameter requiredFrequencyValue (Config default: 1), requiredRetentionDays (Config default: 35) und requiredFrequencyUnit

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			(Config default: days) festlegen. Der tatsächliche Wert muss den Anforderungen Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
Anhang 10 Teil B – 5 (d) i)	Ein Finanzinstitut sollte die Resilienz anforderungen der Cloud-Ser vices bewerten und geeignete Maßnahmen festlegen , die der Kritikali tät des Systems angemessen sind, um die Verfügbar keit der Services in extrem ungünstigen Szenarien sicherzus tellen. Finanzins titute sollten einen risikobasierten Ansatz in Betracht ziehen sowie nach und nach geeignete Kontrollm aßnahmen ergreifen , um die Verfügbar keit der Services sicherzustellen und das Konzentrationsrisi ko zu mindern. Zu den praktikablen Optionen gehören: i) Nutzung der Hochverfü gbarkeits- und Redundanzfunktione n von Cloud-Ser vices, um sicherzus	autoscaling-multiple-az	Zur Gewährleistung einer hohen Verfügbar keit stellen Sie sicher, dass Ihre Auto-Scaling-Gruppe so konfiguriert ist, dass sie sich über mehrere Availability Zones erstreckt.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	tellen, dass Produktionsrechenzentren über redundante Kapazitäten in verschiedenen Availability Zones verfügen;		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
Anhang 10 Teil B – 5 (d) i)	Ein Finanzinstitut sollte die Resilienz anforderungen der Cloud-Ser vices bewerten und geeignete Maßnahmen festlegen , die der Kritikali tät des Systems angemessen sind, um die Verfügbar keit der Services in extrem ungünstigen Szenarien sicherzus tellen. Finanzins titute sollten einen risikobasierten Ansatz in Betracht ziehen sowie nach und nach geeignete Kontrollm aßnahmen ergreifen , um die Verfügbar keit der Services sicherzustellen und das Konzentrationsrisi ko zu mindern. Zu den praktikablen Optionen gehören: i) Nutzung der Hochverfü gbarkeits- und Redundanzfunktione n von Cloud-Ser vices, um sicherzus	elbv2-multiple-az	Elastic Load Balancing (ELB) verteilt Ihren eingehenden Traffic automatisch auf mehrere Ziele wie EC2 Instances, Container und IP-Adressen in einer Availability Zone. Zur Gewährlei stung einer hohen Verfügbarkeit stellen Sie sicher, dass Ihr ELB Instances aus mehreren Availability Zones registriert hat.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	tellen, dass Produktionsrechenzentren über redundante Kapazitäten in verschiedenen Availability Zones verfügen;		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
Anhang 10 Teil B – 5 (d) i)	Ein Finanzinstitut sollte die Resilienz anforderungen der Cloud-Ser vices bewerten und geeignete Maßnahmen festlegen , die der Kritikali tät des Systems angemessen sind, um die Verfügbar keit der Services in extrem ungünstigen Szenarien sicherzus tellen. Finanzins titute sollten einen risikobasierten Ansatz in Betracht ziehen sowie nach und nach geeignete Kontrollm aßnahmen ergreifen , um die Verfügbar keit der Services sicherzustellen und das Konzentrationsrisi ko zu mindern. Zu den praktikablen Optionen gehören: i) Nutzung der Hochverfü gbarkeits- und Redundanzfunktione n von Cloud-Ser vices, um sicherzus	lambda-vpc-multi-az-überprüfen	Wenn Ihre AWS Lambda-Funktion so konfiguriert ist, dass sie eine Verbindun g zu einer Virtual Private Cloud (VPC) in Ihrem Konto herstellt, stellen Sie die AWS Lambda-Fu nktion in mindesten s zwei verschied enen Availability Zones bereit, um sicherzustellen, dass Ihre Funktion für die Verarbeit ung von Ereigniss en im Falle einer Dienstunterbrechung in einer einzigen Zone verfügbar ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	tellen, dass Produktionsrechenzentren über redundante Kapazitäten in verschiedenen Availability Zones verfügen;		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
Anhang 10 Teil B – 5 (d) i)	Ein Finanzinstitut sollte die Resilienz anforderungen der Cloud-Ser vices bewerten und geeignete Maßnahmen festlegen , die der Kritikali tät des Systems angemessen sind, um die Verfügbar keit der Services in extrem ungünstigen Szenarien sicherzus tellen. Finanzins titute sollten einen risikobasierten Ansatz in Betracht ziehen sowie nach und nach geeignete Kontrollm aßnahmen ergreifen , um die Verfügbar keit der Services sicherzustellen und das Konzentrationsrisi ko zu mindern. Zu den praktikablen Optionen gehören: i) Nutzung der Hochverfü gbarkeits- und Redundanzfunktione n von Cloud-Ser vices, um sicherzus	nlb-cross-zone-load-Balancing aktiviert	Aktivieren Sie den zonenübergreifende n Lastausgleich für Ihre NetworkLoad Balancer (NLBs), um eine angemesse ne Kapazität und Verfügbarkeit aufrechtzuerhalten. Zonenübergreifende s Load Balancing reduziert die Notwendigkeit, die gleiche Anzahl von Instances in jeder aktivierten Availability Zone aufrechtzuerhalten . Dadurch wird auch die Fähigkeit Ihrer Anwendung verbessert, den Verlust einer oder mehrerer Instances zu bewältigen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	tellen, dass Produktionsrechenzentren über redundante Kapazitäten in verschiedenen Availability Zones verfügen;		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
Anhang 10 Teil B – 5 (d) i)	Ein Finanzinstitut sollte die Resilienz anforderungen der Cloud-Ser vices bewerten und geeignete Maßnahmen festlegen , die der Kritikali tät des Systems angemessen sind, um die Verfügbar keit der Services in extrem ungünstigen Szenarien sicherzus tellen. Finanzins titute sollten einen risikobasierten Ansatz in Betracht ziehen sowie nach und nach geeignete Kontrollm aßnahmen ergreifen , um die Verfügbar keit der Services sicherzustellen und das Konzentrationsrisi ko zu mindern. Zu den praktikablen Optionen gehören: i) Nutzung der Hochverfü gbarkeits- und Redundanzfunktione n von Cloud-Ser vices, um sicherzus	rds-cluster-multi-az-aktiviert	Für Cluster von Amazon Relationa l Database Service (Amazon RDS) sollte die Multi-AZ-Replikati on aktiviert sein, um die Verfügbarkeit der gespeicherten Daten zu gewährleisten. Availability Zones werden auf einer physisch getrennte n, unabhängi gen Infrastruktur ausgeführt und sind auf höchste Zuverläss igkeit ausgelegt . Im Falle eines Infrastrukturausfa lls führt Amazon RDS einen automatis chen Failover zum Standby-Modus durch, sodass Sie den Datenbankbetrieb wieder aufnehmen können, sobald der Failover abgeschlo ssen ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	tellen, dass Produktionsrechenzentren über redundante Kapazitäten in verschiedenen Availability Zones verfügen;		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
Anhang 10 Teil B – 5 (d) i)	Ein Finanzinstitut sollte die Resilienz anforderungen der Cloud-Ser vices bewerten und geeignete Maßnahmen festlegen , die der Kritikali tät des Systems angemessen sind, um die Verfügbar keit der Services in extrem ungünstigen Szenarien sicherzus tellen. Finanzins titute sollten einen risikobasierten Ansatz in Betracht ziehen sowie nach und nach geeignete Kontrollm aßnahmen ergreifen , um die Verfügbar keit der Services sicherzustellen und das Konzentrationsrisi ko zu mindern. Zu den praktikablen Optionen gehören: i) Nutzung der Hochverfü gbarkeits- und Redundanzfunktione n von Cloud-Ser vices, um sicherzus	rds-multi-az-support	Die Multi-AZ-Unterstüt zung in Amazon Relational Database Service (Amazon RDS) bietet eine verbesserte Verfügbar keit und Beständig keit von Datenbank -Instances. Wenn Sie eine Multi-AZ-Datenbank-Instance bereitste llen, erstellt Amazon RDS automatisch eine primäre Datenbank-Instance und replizier t die Daten synchron auf eine Standby-Instance in einer anderen Availability Zone. Jede Availabil ity Zone läuft auf einer eigenen, physisch getrennte n, unabhängigen Infrastruktur und ist auf eine hohe Verfügbarkeit ausgelegt. Im Falle eines Infrastru kturausfalls führt Amazon RDS einen automatis

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	tellen, dass Produktionsrechenzentren über redundante Kapazitäten in verschiedenen Availability Zones verfügen;		chen Failover zum Standby-Modus durch, sodass Sie den Datenbankbetrieb wieder aufnehmen können, sobald der Failover abgeschlossen ist.
Anhang 10 Teil B – 8 (a)	Ein Finanzinstitut sollte angemessene und relevante Verschlüsselungstechniken einsetzen, um die Vertraulichkeit und Integrität der in der Cloud gespeicherten sensiblen Daten zu schützen.	api-gw-cache-enabled-und-verschlüsselt	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass die Verschlüsselung für den Cache Ihrer API-Gateway-Stufe aktiviert ist. Da für die API-Methode sensible Daten erfasst werden können, sollten Sie die Verschlüsselung von Daten im Ruhezustand aktivieren, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
Anhang 10 Teil B – 8 (a)	Ein Finanzinstitut sollte angemessene und relevante Verschlüsselungstechniken einsetzen, um die Vertraulichkeit und Integrität der in der Cloud gespeicherten sensiblen Daten zu schützen.	backup-recovery-point-encrypted	Stellen Sie sicher, dass die Verschlüsselung für Ihre AWS Backup-Wiederherstellungspunkte aktiviert ist. Da sensible Daten auch im Ruhezustand vorhanden sein können, sollten Sie die Verschlüsselung im Ruhezustand aktivieren, um diese Daten zu schützen.
Anhang 10 Teil B – 8 (a)	Ein Finanzinstitut sollte angemessene und relevante Verschlüsselungstechniken einsetzen, um die Vertraulichkeit und Integrität der in der Cloud gespeicherten sensiblen Daten zu schützen.	cloudtrail-security-trail-enabled	Diese Regel trägt dazu bei, die Verwendung der AWS empfohlenen bewährten Sicherheitsmethoden für sicherzustellen AWS CloudTrail, indem überprüft wird, ob mehrere Einstellungen aktiviert sind. Dazu gehören die Verwendung von Protokollverschlüsselung, Protokollvalidierung und Aktivierung AWS CloudTrail in mehreren Regionen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
Anhang 10 Teil B – 8 (a)	Ein Finanzinstitut sollte angemessene und relevante Verschlüsselungstechniken einsetzen, um die Vertraulichkeit und Integrität der in der Cloud gespeicherten sensiblen Daten zu schützen.	cloudwatch-log-group-encrypted	Um sensible Daten im Speicher zu schützen, stellen Sie sicher, dass die Verschlüsselung für Ihre Amazon CloudWatch Log Groups aktiviert ist.
Anhang 10 Teil B – 8 (a)	Ein Finanzinstitut sollte angemessene und relevante Verschlüsselungstechniken einsetzen, um die Vertraulichkeit und Integrität der in der Cloud gespeicherten sensiblen Daten zu schützen.	dynamodb-table-encrypted-kms	Stellen Sie sicher, dass die Verschlüsselung für Ihre Amazon-DynamoDB-Tabellen aktiviert ist. Um eventuell vorhandene sensible Daten im Ruhezustand in diesen Tabellen zu schützen, müssen Sie die Verschlüsselung von Daten im Ruhezustand aktivieren. Standardmäßig werden DynamoDB-Tabellen mit einem AWS eigenen Kundenhauptschlüssel (CMK) verschlüselt.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
Anhang 10 Teil B – 8 (a)	Ein Finanzinstitut sollte angemessene und relevante Verschlüsselungstechniken einsetzen, um die Vertraulichkeit und Integrität der in der Cloud gespeicherten sensiblen Daten zu schützen.	ec2- ebs-encryption-by-default	Zum Schutz von Daten im Ruhezustand müssen Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon Elastic Block Store (Amazon EBS)-Volumes aktiviert ist. Aktivieren Sie die Verschlüsselung von Daten im Ruhezustand, um eventuell in diesen Volumes vorhandene sensible Daten im Ruhezustand zu schützen.
Anhang 10 Teil B – 8 (a)	Ein Finanzinstitut sollte angemessene und relevante Verschlüsselungstechniken einsetzen, um die Vertraulichkeit und Integrität der in der Cloud gespeicherten sensiblen Daten zu schützen.	efs-encrypted-check	Aktivieren Sie die Verschlüsselung für Ihr Amazon Elastic File System (EFS), um eventuell vorhandene sensible Daten sowie Daten im Ruhezustand zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
Anhang 10 Teil B – 8 (a)	Ein Finanzinstitut sollte angemessene und relevante Verschlüsselungstechniken einsetzen, um die Vertraulichkeit und Integrität der in der Cloud gespeicherten sensiblen Daten zu schützen.	eks-secrets-encrypted	Damit Daten im Ruhezustand geschützt werden, stellen Sie sicher, dass Ihre Amazon Elastic Kubernetes Service (EKS)-Cluster so konfiguriert sind, dass Kubernetes-Secrets verschlüsselt sind. Aktivieren Sie die Verschlüsselung von Daten im Ruhezustand, um eventuell in diesen Volumes vorhandene sensible Daten im Ruhezustand zu schützen.
Anhang 10 Teil B – 8 (a)	Ein Finanzinstitut sollte angemessene und relevante Verschlüsselungstechniken einsetzen, um die Vertraulichkeit und Integrität der in der Cloud gespeicherten sensiblen Daten zu schützen.	encrypted-volumes	Aktivieren Sie die Verschlüsselung für Ihre Volumes von Amazon Elastic Block Store (Amazon EBS), um eventuell vorhandene sensible Daten sowie Daten im Ruhezustand zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
Anhang 10 Teil B – 8 (a)	Ein Finanzinstitut sollte angemessene und relevante Verschlüsselungstechniken einsetzen, um die Vertraulichkeit und Integrität der in der Cloud gespeicherten sensiblen Daten zu schützen.	opensearch-encrypted-at-rest	Da sensible Daten vorhanden sein können und um Daten im Ruhezustand zu schützen, sollten Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon OpenSearch Service-Domains aktiviert ist.
Anhang 10 Teil B – 8 (a)	Ein Finanzinstitut sollte angemessene und relevante Verschlüsselungstechniken einsetzen, um die Vertraulichkeit und Integrität der in der Cloud gespeicherten sensiblen Daten zu schützen.	rds-snapshot-encrypted	Stellen Sie sicher, dass die Verschlüsselung für Ihre Amazon Relational Database Service (Amazon RDS)-Snapshots aktiviert ist. Da sensible Daten auch im Ruhezustand vorhanden sein können, sollten Sie die Verschlüsselung von Daten im Ruhezustand aktivieren, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
Anhang 10 Teil B – 8 (a)	Ein Finanzinstitut sollte angemessene und relevante Verschlüsselungstechniken einsetzen, um die Vertraulichkeit und Integrität der in der Cloud gespeicherten sensiblen Daten zu schützen.	redshift-cluster-kms-enabled	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass die Verschlüsselung mit AWS Key Management Service (AWS KMS) für Ihren Amazon Redshift Redshift-Cluster aktiviert ist. Um eventuell vorhandene sensible Daten im Ruhezustand in Redshift-Clustern zu schützen, muss die Verschlüsselung von Daten im Ruhezustand aktiviert sein.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
Anhang 10 Teil B – 8 (a)	Ein Finanzinstitut sollte angemessene und relevante Verschlüsselungstechniken einsetzen, um die Vertraulichkeit und Integrität der in der Cloud gespeicherten sensiblen Daten zu schützen.	s-3 default-encryption-kms	Stellen Sie sicher, dass die Verschlüsselung für Ihre Amazon Simple Storage Service (Amazon S3)-Buckets aktiviert ist. Da sensible Daten in einem Amazon-S3-Bucket gespeichert werden können, sollten Sie die Verschlüsselung im Ruhezustand aktivieren, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
Anhang 10 Teil B – 8 (a)	Ein Finanzinstitut sollte angemessene und relevante Verschlüsselungstechniken einsetzen, um die Vertraulichkeit und Integrität der in der Cloud gespeicherten sensiblen Daten zu schützen.	secretsmanager-using-cmk	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass die Verschlüsselung mit dem AWS Key Management Service (AWS KMS) für AWS Secrets Manager aktiviert ist. Aktivieren Sie die Verschlüsselung von Daten im Ruhezustand, um eventuell vorhandene sensible Daten im Ruhezustand im Secrets Manager zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
Anhang 10 Teil B – 8 (a)	Ein Finanzinstitut sollte angemessene und relevante Verschlüsselungstechniken einsetzen, um die Vertraulichkeit und Integrität der in der Cloud gespeicherten sensiblen Daten zu schützen.	sns-encrypted-kms	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass Ihre Amazon Simple Notification Service (Amazon SNS) -Themen mit dem AWS Key Management Service (AWS KMS) verschlüsselt werden müssen. Um eventuell vorhandene sensible Daten im Ruhezustand in veröffentlichten Nachrichten zu schützen, muss die Verschlüsselung von Daten im Ruhezustand aktiviert sein.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
Anhang 10 Teil B – 8 (d)	Mit der zunehmenden Nutzung der Cloud ist die Verwaltung vieler Verschlüsselungsschlüssel, die zum Schutz von Daten verwendet werden, immer komplexer geworden und kann Finanzinstitute vor neue Herausforderungen stellen. Ein Finanzinstitut sollte bei der Schlüsselverwaltung einen umfassenden und zentralisierten Ansatz verfolgen, einschließlich der Verwendung eines zentralen Schlüsselverwaltungssystems, das die Generierung, Speicherung und Verteilung von Schlüsseln auf sichere und skalierbare Weise handhaben kann.	cmk-backing-key-rotation-aktiviert	Aktivieren Sie die Schlüsselrotation, um sicherzustellen, dass Schlüssel rotiert werden, nachdem sie das Ende ihrer Krypto-Periode erreicht haben.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
Anhang 10 Teil B – 8 (d)	Mit der zunehmenden Nutzung der Cloud ist die Verwaltung vieler Verschlüsselungsschlüssel, die zum Schutz von Daten verwendet werden, immer komplexer geworden und kann Finanzinstitute vor neue Herausforderungen stellen. Ein Finanzinstitut sollte bei der Schlüsselverwaltung einen umfassenden und zentralisierten Ansatz verfolgen, einschließlich der Verwendung eines zentralen Schlüsselverwaltungssystems, das die Generierung, Speicherung und Verteilung von Schlüsseln auf sichere und skalierbare Weise handhaben kann.	kms-cmk-not-scheduled-zum Löschen	Um Daten im Ruhezustand zu schützen, sollten Sie sicherstellen, dass die für den Kunden erforderlichen Masterschlüssel (CMKs) nicht für das Löschen im AWS Key Management Service (AWS KMS) vorgesehen sind. Da Schlüssel manchmal gelöscht werden müssen, können Sie mit dieser Regel alle zu löschenden Schlüssel überprüfen, falls ein Schlüssel versehentlich zur Löschung vorgemerkt wurde.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
Anhang 10 Teil B – 9 (a) ii)	Die Managemen tebene ist ein wesentlicher Sicherheitsuntersc hied zwischen herkömmlicher Infrastruktur und Cloud-Computing, bei dem der Fernzugri ff standardmäßig unterstützt wird. Diese Zugriffsebene könnte anfällig für Cyberangr iffe sein und dadurch die Integrität der gesamten Cloud-Ber eitstellung gefährden. Vor diesem Hintergru nd sollten Finanzins titute sicherstellen, dass strenge Kontrolle n für den Zugriff auf die Verwaltungsebene angewendet werden, die Folgendes beinhalten können: ii) Einführung von „Least-Privilegien“ und starker Multi-Fak tor-Authentifizierung (MFA), z. B. sichere Passwörter, Soft-Tokens, privilegierte	iam-password-policy	Die Identitäten und Anmeldeinformation en werden auf der Grundlage einer organisatorischen IAM-Passwortrichtlinie ausgestellt, verwaltet und verifiziert. Sie erfüllen oder übertreff en die Anforderungen von NIST SP 800-63 und dem Standard „Best Practices für die Sicherheit von Passwörtern“ von AWS Fundational Security. Mit dieser Regel können Sie optional RequireUp percaseCharacters (Wert für AWS grundlegende Sicherheitsbewährt e Methoden: wahr), RequireLowercaseCh aracters (Wert für bewährte Methoden für AWS grundlege nde Sicherheit: wahr), RequireSy mbols (Wert für bewährte Methoden für AWS grundlege

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	Zugangsverwaltungstool und Maker-Checker-Funktionen;		nde Sicherheit: wahr), RequireNumbers (Wert für bewährte Methoden für AWS grundlegende Sicherheit: wahr), MinimumPasswordLength (Wert für bewährte Methoden für AWS grundlegende Sicherheit: 14), PasswordReusePrevention (Wert für bewährte Methoden für AWS grundlegende Sicherheit: 24) und MaxPasswordAge (Wert für bewährte Methoden für AWS grundlegende Sicherheit: 90) für Ihr IAM festlegen Kennwortrichtlinie. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
Anhang 10 Teil B – 9 (a) ii)	Die Managemen tebene ist ein wesentlicher Sicherheitsuntersc hied zwischen herkömmlicher Infrastruktur und Cloud-Computing, bei dem der Fernzugri ff standardmäßig unterstützt wird. Diese Zugriffsebene könnte anfällig für Cyberangr iffe sein und dadurch die Integrität der gesamten Cloud-Ber eitstellung gefährden. Vor diesem Hintergru nd sollten Finanzins titute sicherstellen, dass strenge Kontrolle n für den Zugriff auf die Verwaltungsebene angewendet werden, die Folgendes beinhalten können: ii) Einführung von „Least-Privilegien“ und starker Multi-Fak tor-Authentifizierung (MFA), z. B. sichere Passwörter, Soft-Tokens, privilegierte	iam-user-mfa-enabled	Aktivieren Sie diese Regel, um den Zugriff auf Ressourcen in der Cloud einzuschr änken. AWS Diese Regel stellt sicher, dass die Multi-Fak tor-Authentifizierung (MFA) für alle IAM-Benutzer aktiviert ist. MFA bietet eine weitere Schutzebe ne zusätzlich zum Benutzernamen und Passwort. Reduziere n Sie Fälle von kompromittierten Konten, indem Sie MFA für IAM-Benutzer vorschreiben.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	Zugangsverwaltungstool und Maker-Checker-Funktionen;		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
Anhang 10 Teil B – 9 (a) ii)	Die Managemen tebene ist ein wesentlicher Sicherheitsuntersc hied zwischen herkömmlicher Infrastruktur und Cloud-Computing, bei dem der Fernzugri ff standardmäßig unterstützt wird. Diese Zugriffsebene könnte anfällig für Cyberangr iffe sein und dadurch die Integrität der gesamten Cloud-Ber eitstellung gefährden. Vor diesem Hintergru nd sollten Finanzins titute sicherstellen, dass strenge Kontrolle n für den Zugriff auf die Verwaltungsebene angewendet werden, die Folgendes beinhalten können: ii) Einführung von „Least-Privilegien“ und starker Multi-Fak tor-Authentifizierung (MFA), z. B. sichere Passwörter, Soft-Tokens, privilegierte	root-account-hardw are-mfa-aktiviert	Verwalten Sie den Zugriff auf Ressource n in der AWS Cloud, indem Sie sicherste llen, dass Hardware-MFA für den Root-Benutzer aktiviert ist. Der Stammbenu tzer ist der AWS-Konto-Benutzer mit den meisten Berechtigungen. MFA bietet eine weitere Schutzebene zusätzlic h zum Benutzern amen und Passwort. Indem Sie MFA für den Root-Benutzer vorschreiben, können Sie die Anzahl AWS-Konten kompromit tierter Benutzer reduzieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	Zugangsverwaltungstool und Maker-Checker-Funktionen;		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
Anhang 10 Teil B – 9 (a) ii)	Die Managemen tebene ist ein wesentlicher Sicherheitsuntersc hied zwischen herkömmlicher Infrastruktur und Cloud-Computing, bei dem der Fernzugri ff standardmäßig unterstützt wird. Diese Zugriffsebene könnte anfällig für Cyberangr iffe sein und dadurch die Integrität der gesamten Cloud-Ber eitstellung gefährden. Vor diesem Hintergru nd sollten Finanzins titute sicherstellen, dass strenge Kontrolle n für den Zugriff auf die Verwaltungsebene angewendet werden, die Folgendes beinhalten können: ii) Einführung von „Least-Privilegien“ und starker Multi-Fak tor-Authentifizierung (MFA), z. B. sichere Passwörter, Soft-Tokens, privilegierte	root-account-mfa-e nabled	Verwalten Sie den Zugriff auf Ressource n in der AWS Cloud, indem Sie sicherste llen, dass MFA für den Root-Benu tzer aktiviert ist. Der Stammbenu tzer ist der AWS-Konto-Benutzer mit den meisten Berechtigungen. MFA bietet eine weitere Schutzebene zusätzlic h zum Benutzern amen und Passwort. Indem Sie MFA für den Root-Benutzer vorschreiben, können Sie die Anzahl AWS-Konten kompromit tierter Benutzer reduzieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	Zugangsverwaltungstool und Maker-Checker-Funktionen;		
Anhang 10 Teil B – 9 (a) iii)	Die Managementebene ist ein wesentlicher Sicherheitsunterschied zwischen herkömmlicher Infrastruktur und Cloud-Computing, bei dem der Fernzugriff standardmäßig unterstützt wird. Diese Zugriffsebene könnte anfällig für Cyberangriffe sein und dadurch die Integrität der gesamten Cloud-Bereitstellung gefährden. Vor diesem Hintergrund sollten Finanzinstitute den Einsatz strenger Kontrollen für den Zugang zur Managementebene sicherstellen, die Folgendes beinhalten können: iii) eine detaillierte Zuteilung von Rechten für privilegierte Benutzer;	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) kann Ihnen dabei helfen, die Prinzipien der geringsten Rechte und der Aufgabentrennung in Zugriffsberechtigungen und Autorisierungen zu integrieren und so zu verhindern, dass Richtlinien „Effect“: „Allow“ mit „Action“: „*“ anstelle von „Resource“: „*“ enthalten. Wenn Benutzern mehr Rechte eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und der Aufgabentrennung verstoßen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
Anhang 10 Teil B – 9 (a) iii)	Die Managemen tebene ist ein wesentlicher Sicherheitsuntersc hied zwischen herkömmlicher Infrastruktur und Cloud-Computing, bei dem der Fernzugri ff standardmäßig unterstützt wird. Diese Zugriffsebene könnte anfällig für Cyberangr iffe sein und dadurch die Integrität der gesamten Cloud-Ber eitstellung gefährden. Vor diesem Hintergru nd sollten Finanzins titute den Einsatz strenger Kontrollen für den Zugang zur Managementebene sicherstellen, die Folgendes beinhalte n können: iii) eine detaillierte Zuteilung von Rechten für privilegierte Benutzer;	iam-user-no-policies-überprüfen	Diese Regel stellt sicher, dass AWS Identity and Access Management (IAM) -Richtlinien nur Gruppen oder Rollen zugewiese n werden, um den Zugriff auf Systeme und Ressourcen zu kontrollieren. Die Zuweisung von Berechtig ungen auf Gruppen- oder Rollenebene trägt dazu bei, die Wahrscheinlichkeit zu verringern, dass eine Identität übermäßige Berechtigungen erhält oder beibehält.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
Anhang 10 Teil B – 9 (a) iv)	Die Managemen tebene ist ein wesentlicher Sicherheitsuntersc hied zwischen herkömmlicher Infrastruktur und Cloud-Computing, bei dem der Fernzugri ff standardmäßig unterstützt wird. Diese Zugriffsebene könnte anfällig für Cyberangr iffe sein und dadurch die Integrität der gesamten Cloud-Ber eitstellung gefährden. Vor diesem Hintergru nd sollten Finanzins titute den Einsatz strenger Kontrolle n für den Zugang zur Managemen tebene sicherste llen, die Folgendes beinhalten können: iv) eine kontinuie rliche Überwachung der von privilegierten Benutzern ausgeübte n Aktivitäten;	cloudtrail-security-trail-enabled	Diese Regel trägt dazu bei, die Verwendung der AWS empfohlenen bewährten Sicherhei tsmethoden für sicherzustellen AWS CloudTrai l, indem geprüft wird, ob mehrere Einstellungen aktiviert sind. Dazu gehören die Verwendun g von Protokoll verschlüsselung, Protokollvalidieru ng und Aktivierung AWS CloudTrail in mehreren Regionen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
Anhang 10 Teil B – 9 (a) iv)	Die Managemen tebene ist ein wesentlicher Sicherheitsuntersc hied zwischen herkömmlicher Infrastruktur und Cloud-Computing, bei dem der Fernzugri ff standardmäßig unterstützt wird. Diese Zugriffsebene könnte anfällig für Cyberangr iffe sein und dadurch die Integrität der gesamten Cloud-Ber eitstellung gefährden. Vor diesem Hintergru nd sollten Finanzins titute den Einsatz strenger Kontrolle n für den Zugang zur Managemen tebene sicherste llen, die Folgendes beinhalten können: iv) eine kontinuie rliche Überwachung der von privilegierten Benutzern ausgeübte n Aktivitäten;	cloud-trail-cloud-watch-logs-aktiviert	Verwenden Sie Amazon CloudWatc h , um Protokoll ereignisaktivitäten zentral zu sammeln und zu verwalten. Die Aufnahme von AWS CloudTrail Daten liefert Einzelheiten zu den API-Aufrufaktivitä ten in Ihrem AWS-Konto.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
Anhang 10 Teil B – 12 (a)	Ein Finanzinstitut sollte die in Cloud-Services gehostete n Daten gemäß den Bestimmungen des Abschnitts „Verhinde rung von Datenverl ust“ (Paragraphen 11.14 bis 11.16) dieses Grundsatz dokuments schützen, was auch die Erweiterung der Endpunktkapazität einschließt, wenn das Finanzinstitut seinen Mitarbeitern erlaubt, ihre eigenen Geräte für den Zugriff auf sensible Daten zu verwenden.	guardduty-enabled-centralized	Amazon GuardDuty kann mithilfe von Threat Intellige nce Feeds helfen, potenzielle Cybersich erheitsereignisse zu überwachen und zu erkennen. Dazu gehören Listen mit bösartigen IPs und maschinel len Lernmethoden zur Identifizierung unerwarteter, nicht autorisierter und bösartiger Aktivitäten in Ihrer AWS Cloud-Umgebung.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
Anhang 10 Teil B – 12 (a)	Ein Finanzinstitut sollte die in Cloud-Services gehostete n Daten gemäß den Bestimmungen des Abschnitts „Verhinde rung von Datenverl ust“ (Paragraphen 11.14 bis 11.16) dieses Grundsatz dokuments schützen, was auch die Erweiterung der Endpunktkapazität einschließt, wenn das Finanzinstitut seinen Mitarbeitern erlaubt, ihre eigenen Geräte für den Zugriff auf sensible Daten zu verwenden.	macie-status-check	Amazon Macie ist ein Datensicherheitsse rvice, der Machine Learning (ML) und Musterabgleich verwendet, um Ihre sensiblen Daten in Buckets von Amazon Simple Storage Service (Amazon S3) zu erkennen und zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
Anhang 10 Teil B – 14 (c) i)	Ein Finanzins titut sollte bei der Entwicklung seines CIRP die folgenden zusätzlic hen Maßnahmen in Betracht ziehen: i) Verbesserung seiner Fähigkeit, Sicherheitsverletz ungen aufzudeck en, um ein effektive s Vorfallmanagement zu erreichen, einschlie ßlich der Fähigkeit, Datenlecks im Dark Web aufzudecken;	guardduty-enabled-centralized	Amazon GuardDuty kann mithilfe von Threat Intellige nce Feeds helfen, potenzielle Cybersich erheitsereignisse zu überwachen und zu erkennen. Dazu gehören Listen mit bösartigen IPs und maschinel len Lernmethoden zur Identifizierung unerwarteter, nicht autorisierter und bösartiger Aktivitäten in Ihrer AWS Cloud-Umgebung.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
Anhang 10 Teil B – 14 (c) i)	Ein Finanzinstitut sollte bei der Entwicklung seines CIRP die folgenden zusätzlichen Maßnahmen in Betracht ziehen: i) Verbesserung seiner Fähigkeit, Sicherheitsverletzungen aufzudecken, um ein effektives Vorfallmanagement zu erreichen, einschließlich der Fähigkeit, Datenlecks im Dark Web aufzudecken;	guardduty-non-archived-findings	Amazon GuardDuty hilft Ihnen dabei, die Auswirkungen eines Vorfalls zu verstehen, indem es die Ergebnisse nach Schweregrad klassifiziert: niedrig, mittel und hoch. Diese Klassifizierungen können Sie zur Festlegung von entsprechenden Strategien und Prioritäten zur Behebung solcher Vorfälle verwenden. Mit dieser Regel können Sie optional daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7) und daysHighSev (Config Default: 1) für nicht archivierte Ergebnisse festlegen, wie es die Richtlinien Ihrer Organisation erfordern.

Vorlage

Die Vorlage ist verfügbar unter GitHub: Operational Best Practices for BNM T. RMi

Bewährte Methoden für das Canadian Centre for Cyber Security (CCCS)-Medium-Cloud-Kontrollprofil

Konformitätspakete bieten ein allgemeines Compliance-Framework, das es Ihnen ermöglicht, mithilfe verwalteter oder benutzerdefinierter AWS Config Regeln und Abhilfemaßnahmen Kontrollen zur Sicherheits-, Betriebs- oder Kostenoptimierung durchzuführen. AWS Config Conformance Packs dienen als Beispielvorlagen nicht dazu, die vollständige Einhaltung eines bestimmten Governance- oder Compliance-Standards sicherzustellen. Sie sind dafür verantwortlich, selbst zu beurteilen, ob Ihre Nutzung der Services den geltenden gesetzlichen und behördlichen Anforderungen entspricht.

Im Folgenden finden Sie ein Beispiel für eine Zuordnung zwischen dem Medium Cloud Control Profile des Canadian Centre for Cyber Security (CCCS) und AWS verwalteten Konfigurationsregeln. Jede Config-Regel gilt für eine bestimmte AWS Ressource und bezieht sich auf eine oder mehrere CCCS Medium Cloud Control Profile-Kontrollen. Eine CCCS-Medium-Cloud-Kontrollprofilsteuerung kann mit mehreren Konfigurationsregeln verknüpft werden. In der folgenden Tabelle finden Sie weitere Informationen und Anleitungen zu diesen Zuordnungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AC-2(1)	AC-2(1) Kontoverwaltung | Automatisierte Systemkontenverwaltung	cloudtrail-enabled	AWS CloudTrail kann bei der Nichtabstreitbarkeit helfen, indem Aktionen und API-Aufrufe der AWS Management Console aufgezeichnet werden. Sie können die Benutzer und die Benutzer AWS-Konten , die einen AWS Dienst aufgerufen haben, die Quell-IP-Adresse, über die die Aufrufe generiert wurden, und den Zeitpunkt

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
			der Anrufe identifizieren. Einzelheiten zu den erfassten Daten finden Sie in den AWS CloudTrail Datensatzinhalten.
CCCS-fPBMM-AC-2(1)	AC-2(1) Kontoverwaltung | Automatisierte Systemkontenverwaltung	ec2-imdsv2-check	Stellen Sie sicher, dass die Methode Instance Metadata Service Version 2 (IMDSv2) aktiviert ist, um den Zugriff auf und die Kontrolle der Amazon Elastic Compute Cloud (Amazon EC2) - Instance-Metadaten zu schützen. Die IMDSv2 Methode verwendet sitzungsbasierte Kontrollen. Mit können Kontrollen implementiert werden IMDSv2, um Änderungen an Instanzmetadaten einzuschränken.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AC-2(1)	AC-2(1) Kontoverwaltung | Automatisierte Systemkontenverwaltung	ecs-task-definition-user-for-host-mode-check	Wenn für eine Aufgabendefinition erhöhte Berechtigungen gelten, liegt das daran, dass der Kunde diesen Konfigurationen ausdrücklich zugestimmt hat. Diese Kontrolle prüft, ob eine unerwartete Berechtigungseskalation vorliegt, wenn für eine Aufgabendefinition das Host-Netzwerk aktiviert ist, die Kunden aber keine erhöhten Berechtigungen aktiviert haben.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AC-2(1)	AC-2(1) Kontoverwaltung | Automatisierte Systemkontenverwaltung	emr-kerberos-enabled	Die Zugriffsberechtigungen und -autorisierungen können verwaltet und nach den Prinzipien der geringsten Berechtigung und Aufgabentrennung integriert werden, indem Kerberos für Amazon-EMR-Cluster aktiviert wird. In Kerberos werden Services und Benutzer, die sich authentifizieren müssen, als Prinzipale bezeichnet. Prinzipale befinden sich in einem Kerberos-Bereich. Innerhalb dieses Bereichs wird ein Kerberos-Server als Key Distribution Center (KDC) bezeichnet. Über diesen Server können sich Prinzipale authentifizieren. Die Authentifizierung im KDC erfolgt durch die Ausstellung von Authentif

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
			izierungstickets. Das KDC unterhält eine Datenbank der Prinzipale in seinem Bereich mit ihren Passwörtern und anderen administr ativen Informationen zu jedem Prinzipal.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AC-2(1)	AC-2(1) Kontoverwaltung | Automatisierte Systemkontenverwaltung	iam-customer-policy-blocked-kms-Aktionen	AWS Identity and Access Management (IAM) kann Ihnen helfen, die Prinzipien der geringsten Rechte und der Aufgabentrennung in Zugriffsberechtigungen und Autorisierungen zu integrieren und so zu verhindern, dass Richtlinien blockierte Aktionen für alle AWS Schlüssel des Key Management Service enthalten. Wenn Benutzer mehr Rechte haben, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und Aufgabentrennung verstoßen. Mit dieser Regel können Sie den Parameter festlegen. blockedActionsPatterns (Wert „AWS Bewährte grundlegende Sicherheitsmethode

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
			n“: kms: Entschlüs seln, kms:ReEnc ryptFrom). Die tatsächlichen Werte müssen den Richtlini en Ihrer Organisation entsprechen.
CCCS-fPBMM-AC-2(1)	AC-2(1) Kontoverw altung | Automatisierte Systemkontenverwal tung	iam-group-has-users-überprüfen	AWS Identity and Access Managemen t (IAM) kann Ihnen helfen, die Prinzipien der geringsten Rechte und der Aufgabent rennung mit Zugriffsb erechtigungen und Autorisierungen zu integrieren, indem sichergestellt wird, dass IAM-Gruppen mindestens einen Benutzer haben. Die Einteilung von Benutzern in Gruppen auf der Grundlage der ihnen zugewiese nen Berechtigungen oder ihrer Funktion ist eine Möglichkeit, das Prinzip der geringste n Berechtigung zu implementieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AC-2(1)	AC-2(1) Kontoverwaltung | Automatisierte Systemkontenverwaltung	iam-inline-policy-blocked-kms-Aktionen	Stellen Sie sicher, dass ein Benutzer, eine IAM-Rolle oder eine IAM-Gruppe (AWS Identity and Access Management) nicht über eine Inline-Richtlinie verfügt, die blockierte Aktionen für alle AWS Schlüssel des Key Management Service zulässt. AWS empfiehlt, verwaltete Richtlinien anstelle von Inline-Richtlinien zu verwenden. Verwaltete Richtlinien ermöglichen Wiederverwendbarkeit, Versionsverwaltung, Rollback und Delegierung der Berechtigungsverwaltung. Mit dieser Regel können Sie den blockedActionsPatterns Parameter festlegen. (Wert „AWS Bewährte grundlegende Sicherheitsmethoden“: kms: Entschlüsseln, kms:ReEnc

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
			ryptFrom). Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.
CCCS-fPBMM-AC-2(1)	AC-2(1) Kontoverwaltung | Automatisierte Systemkontenverwaltung	iam-no-inline-policy-überprüfen	Stellen Sie sicher, dass ein Benutzer, eine IAM-Rolle oder eine IAM-Gruppe (AWS Identity and Access Management) nicht über eine Inline-Richtlinie zur Zugriffskontrolle auf Systeme und Ressourcen verfügt. AWS empfiehlt, verwaltete Richtlinien anstelle von Inline-Richtlinien zu verwenden. Verwaltete Richtlinien ermöglichen Wiederverwendbarkeit, Versionsverwaltung, Rollback und Delegierung der Berechtigungsverwaltung.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AC-2(1)	AC-2(1) Kontoverwaltung | Automatisierte Systemkontenverwaltung	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) kann Ihnen dabei helfen, die Prinzipien der geringsten Rechte und der Aufgabentrennung in Zugriffsberechtigungen und Autorisierungen zu integrieren und so zu verhindern, dass Richtlinien „Effect“: „Allow“ mit „Action“: „*“ anstelle von „Resource“: „*“ enthalten. Wenn Benutzern mehr Rechte eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und der Aufgabentrennung verstoßen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AC-2(1)	AC-2(1) Kontoverwaltung | Automatisierte Systemkontenverwaltung	iam-policy-no-statements-with-full-access	Stellen Sie sicher, dass IAM-Aktionen nur auf die benötigten Aktionen beschränkt sind. Wenn Benutzern mehr Rechte eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und der Aufgabentrennung verstoßen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AC-2(1)	AC-2(1) Kontoverwaltung | Automatisierte Systemkontenverwaltung	iam-root-access-key-überprüfen	Der Zugriff auf Systeme und Ressourcen kann gesteuert werden, indem überprüft wird, ob der Root-Benutzer keine Zugriffsschlüssel mit seiner AWS Identity and Access Management (IAM) -Rolle verknüpft hat. Stellen Sie sicher, dass die Root-Zugriffsschlüssel gelöscht werden. Erstellen und verwenden Sie stattdessen rollenbasierte Funktionen, AWS-Konten um das Prinzip der geringsten Funktionalität zu berücksichtigen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AC-2(1)	AC-2(1) Kontoverwaltung | Automatisierte Systemkontenverwaltung	iam-user-group-membership-überprüfen	AWS Identity and Access Management (IAM) kann Ihnen helfen, Zugriffsberechtigungen und Autorisierungen einzuschränken, indem sichergestellt wird, dass Benutzer Mitglieder mindestens einer Gruppe sind. Wenn Benutzern mehr Berechtigungen eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und Aufgabentrennung verstoßen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AC-2(1)	AC-2(1) Kontoverwaltung | Automatisierte Systemkontenverwaltung	iam-user-no-policies-überprüfen	Diese Regel stellt sicher, dass AWS Identity and Access Management (IAM) -Richtlinien nur Gruppen oder Rollen zugewiesen werden, um den Zugriff auf Systeme und Ressourcen zu kontrollieren. Die Zuweisung von Berechtigungen auf Gruppen- oder Rollenebene trägt dazu bei, die Wahrscheinlichkeit zu verringern, dass eine Identität übermäßige Berechtigungen erhält oder beibehält.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AC-2(1)	AC-2(1) Kontoverwaltung | Automatisierte Systemkontenverwaltung	iam-user-unused-credentials-überprüfen	AWS Identity and Access Management (IAM) kann Ihnen bei Zugriffsberechtigungen und Autorisierungen helfen, indem es nach IAM-Passwörtern und Zugriffsschlüsseln sucht, die für einen bestimmten Zeitraum nicht verwendet wurden. Wenn ungenutzte Anmeldeinformationen identifiziert werden, müssen Sie sie deaktivieren und/oder entfernen, da dies gegen das Prinzip der geringsten Berechtigung verstoßen könnte. Für diese Regel müssen Sie einen Wert für das maxCredentialUsage Alter festlegen (Standardkonfiguration: 90). Der tatsächliche Wert muss den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AC-2(1)	AC-2(1) Kontoverwaltung | Automatisierte Systemkontenverwaltung	multi-region-cloudtrail-enabled	AWS CloudTrail zeichnet Aktionen und API-Aufrufe der AWS Management Console auf. Sie können feststellen, welche Benutzer und Konten angerufen wurden AWS, von welcher Quell-IP-Adresse aus die Anrufe getätigt wurden und wann die Anrufe erfolgten. CloudTrail übermittelt Protokolldateien aus allen AWS Regionen an Ihren S3-Bucket , wenn MULTI_REGION_CLOUD_TRAIL_ENABLED aktiviert ist. Außerdem wird beim AWS Start einer neuen Region derselbe Trail in der neuen Region erstellt. CloudTrail Dadurch erhalten Sie automatisch Protokolldateien mit API-Aktivitäten für die neue Region.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AC-2(3)	AC-2(3) Kontoverwaltung | Inaktive Konten deaktivieren	iam-password-policy	Die Identitäten und Anmeldeinformationen werden auf der Grundlage einer organisatorischen IAM-Passwortrichtlinie ausgestellt, verwaltet und verifiziert. Sie erfüllen oder übertreffen die Anforderungen von NIST SP 800-63 und dem Standard „Best Practices“ von AWS Foundational Security in Bezug auf die Passwortstärke. Mit dieser Regel können Sie optional RequireUppercaseCharacters (Wert für AWS grundlegende Sicherheitsbewährte Methoden: wahr), RequireLowercaseCharacters (Wert für bewährte Methoden für AWS grundlegende Sicherheit: wahr), RequireSymbols (Wert für bewährte Methoden für AWS grundlegende Sicherheit:

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
			wahr), RequireNumbers (Wert für bewährte Methoden für AWS grundlegende Sicherheit: wahr), MinimumPasswordLength (Wert für bewährte Methoden für AWS grundlegende Sicherheit: 14), PasswordReusePrevention (Wert für bewährte Methoden für AWS grundlegende Sicherheit: 24) und MaxPasswordAge (Wert für bewährte Methoden für AWS grundlegende Sicherheit: 90) für Ihr IAM festlegen Kennwortrichtlinie. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AC-2(3)	AC-2(3) Kontoverwaltung | Inaktive Konten deaktivieren	iam-user-unused-credentials-überprüfen	AWS Identity and Access Management (IAM) kann Ihnen bei Zugriffsberechtigungen und Autorisierungen helfen, indem es nach IAM-Passwörtern und Zugriffsschlüsseln sucht, die für einen bestimmten Zeitraum nicht verwendet wurden. Wenn ungenutzte Anmeldeinformationen identifiziert werden, müssen Sie sie deaktivieren und/oder entfernen, da dies gegen das Prinzip der geringsten Berechtigung verstoßen könnte. Für diese Regel müssen Sie einen Wert für das maxCredentialUsage Alter festlegen (Standardkonfiguration: 90). Der tatsächliche Wert muss den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AC-2(4)	AC-2(4) Kontoverwaltung | Automatisierte Prüfungsaktionen	cloudtrail-s3-dataevents-enabled	Die Erfassung von Simple Storage Service (Amazon S3)-Datenereignissen unterstützt die Erkennung von ungewöhnlichen Aktivitäten. Zu den Details gehören Informationen zu dem AWS -Konto, das auf einen Amazon-S3-Bucket zugegriffen hat, die IP-Adresse und die Uhrzeit des Ereignisses.
CCCS-fPBMM-AC-2(4)	AC-2(4) Kontoverwaltung | Automatisierte Prüfungsaktionen	cloud-trail-cloud-watch-logs-aktiviert	Verwenden Sie Amazon CloudWatch , um Protokoll ereignisaktivitäten zentral zu sammeln und zu verwalten. Die Aufnahme von AWS CloudTrail Daten liefert Einzelheiten zu den API-Aufrufaktivitäten in Ihrem AWS-Konto.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AC-2(4)	AC-2(4) Kontoverwaltung | Automatisierte Prüfungsaktionen	cloudtrail-enabled	AWS CloudTrail kann bei der Nichtabstreitbarkeit helfen, indem Aktionen und API-Aufrufe der AWS Management Console aufgezeichnet werden. Sie können die Benutzer und die Benutzer AWS-Konten , die einen AWS Dienst aufgerufen haben, die Quell-IP-Adresse, über die die Aufrufe generiert wurden, und den Zeitpunkt der Anrufe identifizieren. Einzelheiten zu den erfassten Daten finden Sie in den AWS CloudTrail Datensatzinhalten.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AC-2(4)	AC-2(4) Kontoverwaltung | Automatisierte Prüfungsaktionen	multi-region-cloudtrail-enabled	AWS CloudTrail zeichnet Aktionen und API-Aufrufe der AWS Management Console auf. Sie können feststellen, welche Benutzer und Konten angerufen wurden AWS, von welcher Quell-IP-Adresse aus die Anrufe getätigt wurden und wann die Anrufe erfolgten. CloudTrail übermittelt Protokolldateien aus allen AWS Regionen an Ihren S3-Bucket , wenn MULTI_REGION_CLOUD_TRAIL_ENABLED aktiviert ist. Außerdem wird beim AWS Start einer neuen Region derselbe Trail in der neuen Region erstellt. CloudTrail Dadurch erhalten Sie automatisch Protokolldateien mit API-Aktivitäten für die neue Region.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AC-2(4)	AC-2(4) Kontoverwaltung | Automatisierte Prüfungsaktionen	rds-logging-enabled	Um die Protokollierung und Überwachung in Ihrer Umgebung zu erleichtern, stellen Sie sicher, dass die Amazon Relational Database Service (Amazon RDS)-Protokollierung aktiviert ist. Mit der Amazon-RDS-Protokollierung können Sie Ereignisse wie Verbindungen, Verbindungsabbrüche, Abfragen oder abgefragte Tabellen erfassen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AC-2(4)	AC-2(4) Kontoverwaltung | Automatisierte Prüfungsaktionen	redshift-cluster-configuration-check	Um Daten im Ruhezustand zu schützen, muss die Verschlüsselung für Ihre Amazon-Redshift-Cluster aktiviert sein. Sie müssen auch sicherstellen, dass die erforderlichen Konfigurationen auf Amazon-Redshift-Clustern bereitgestellt werden. Die Prüfungsprotokollierung muss aktiviert sein, um Informationen zu Verbindungen und Benutzeraktivitäten in der Datenbank bereitzustellen. Diese Regel erfordert, dass ein Wert für clusterDbEncrypted (Config Default: TRUE) und LoggingEnabled (Config Default: TRUE) gesetzt ist. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AC-2(4)	AC-2(4) Kontoverwaltung | Automatisierte Prüfungsaktionen	s3- bucket-logging-enabled	Die Amazon Simple Storage Service (Amazon S3)-Serverzugriffsprotokollierung bietet eine Methode zur Überwachung des Netzwerks im Hinblick auf potenzielle Cybersicherheitsereignisse. Die Ereignisse werden überwacht, indem detaillierte Aufzeichnungen über die Anfragen erfasst werden, die an einen Amazon-S3-Bucket gestellt wurden. Jeder Zugriffsprotokolleintrag enthält Details zu einer einzelnen Zugriffsanfrage. Zu den Details gehören Auftraggeber, Bucket-Name, Anforderungszeit, Anforderungsaktion, Antwortstatus und Fehlercode, falls relevant.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AC-2.A	AC-2.A Kontoverwaltung	cloudtrail-enabled	AWS CloudTrail kann durch die Aufzeichnung von Aktionen und API-Aufrufen in der AWS Management Console bei der Nichtabstreitbarkeit helfen. Sie können die Benutzer und die Benutzer AWS-Konten , die einen AWS Dienst aufgerufen haben, die Quell-IP-Adresse, über die die Aufrufe generiert wurden, und den Zeitpunkt der Anrufe identifizieren. Einzelheiten zu den erfassten Daten finden Sie in den AWS CloudTrail Datensatzinhalten.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AC-2.A	AC-2.A Kontoverwaltung	ec2-imdsv2-check	Stellen Sie sicher, dass die Methode Instance Metadata Service Version 2 (IMDSv2) aktiviert ist, um den Zugriff auf und die Kontrolle der Amazon Elastic Compute Cloud (Amazon EC2) - Instance-Metadaten zu schützen. Die IMDSv2 Methode verwendet sitzungsbasierte Kontrollen. Mit können Kontrollen implementiert werden IMDSv2, um Änderungen an Instanzmetadaten einzuschränken.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AC-2.A	AC-2.A Kontoverwaltung	ecs-task-definition-user-for-host-mode-check	Wenn für eine Aufgabendefinition erhöhte Berechtigungen gelten, liegt das daran, dass der Kunde diesen Konfigurationen ausdrücklich zugestimmt hat. Diese Kontrolle prüft, ob eine unerwartete Berechtigungseskalation vorliegt, wenn für eine Aufgabendefinition das Host-Netzwerk aktiviert ist, die Kunden aber keine erhöhten Berechtigungen aktiviert haben.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AC-2.A	AC-2.A Kontoverwaltung	emr-kerberos-enabled	Die Zugriffsberechtigungen und -autorisierungen können verwaltet und nach den Prinzipien der geringsten Berechtigung und Aufgabentrennung integriert werden, indem Kerberos für Amazon-EMR-Cluster aktiviert wird. In Kerberos werden Services und Benutzer, die sich authentifizieren müssen, als Prinzipale bezeichnet. Prinzipale befinden sich in einem Kerberos-Bereich. Innerhalb dieses Bereichs wird ein Kerberos-Server als Key Distribution Center (KDC) bezeichnet. Über diesen Server können sich Prinzipale authentifizieren. Die Authentifizierung im KDC erfolgt durch die Ausstellung von Authentif

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
			izierungstickets. Das KDC unterhält eine Datenbank der Prinzipale in seinem Bereich mit ihren Passwörtern und anderen administr ativen Informationen zu jedem Prinzipal.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AC-2.A	AC-2.A Kontoverwaltung	iam-customer-policy-blocked-kms-Aktionen	AWS Identity and Access Management (IAM) kann Ihnen helfen, die Prinzipien der geringsten Rechte und der Aufgabentrennung in Zugriffsberechtigungen und Autorisierungen zu integrieren und so zu verhindern, dass Richtlinien blockierte Aktionen für alle AWS Schlüssel des Key Management Service enthalten. Wenn Benutzer mehr Rechte haben, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und Aufgabentrennung verstoßen. Mit dieser Regel können Sie den Parameter festlegen. blockedActionsPatterns (Wert „AWS Bewährte grundlegende Sicherheitsmethode

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
			n“: kms: Entschlüs seln, kms:ReEnc ryptFrom). Die tatsächlichen Werte müssen den Richtlini en Ihrer Organisation entsprechen.
CCCS-fPBMM-AC-2.A	AC-2.A Kontoverw altung	iam-group-has-users-überprüfen	AWS Identity and Access Managemen t (IAM) kann Ihnen helfen, die Prinzipien der geringsten Rechte und der Aufgabent rennung mit Zugriffsb erechtigungen und Autorisierungen zu integrieren, indem sichergestellt wird, dass IAM-Gruppen mindestens einen Benutzer haben. Die Einteilung von Benutzern in Gruppen auf der Grundlage der ihnen zugewiese nen Berechtigungen oder ihrer Funktion ist eine Möglichkeit, das Prinzip der geringste n Berechtigung zu implementieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AC-2.A	AC-2.A Kontoverwaltung	iam-inline-policy-blocked-kms-Aktionen	Stellen Sie sicher, dass ein Benutzer, eine IAM-Rolle oder eine IAM-Gruppe (AWS Identity and Access Management) nicht über eine Inline-Richtlinie verfügt, die blockierte Aktionen für alle AWS Schlüssel des Key Management Service zulässt. AWS empfiehlt, verwaltete Richtlinien anstelle von Inline-Richtlinien zu verwenden. Verwaltete Richtlinien ermöglichen Wiederverwendbarkeit, Versionsverwaltung, Rollback und Delegierung der Berechtigungsverwaltung. Mit dieser Regel können Sie den blockedActionsPatterns Parameter festlegen. (Wert „AWS Bewährte grundlegende Sicherheitsmethoden“: kms: Entschlüsseln, kms:ReEnc

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
			ryptFrom). Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.
CCCS-fPBMM-AC-2.A	AC-2.A Kontoverwaltung	iam-no-inline-policy-überprüfen	Stellen Sie sicher, dass ein Benutzer, eine IAM-Rolle oder eine IAM-Gruppe (AWS Identity and Access Management) nicht über eine Inline-Richtlinie zur Zugriffskontrolle auf Systeme und Ressourcen verfügt. AWS empfiehlt, verwaltete Richtlinien anstelle von Inline-Richtlinien zu verwenden. Verwaltete Richtlinien ermöglichen Wiederverwendbarkeit, Versionsverwaltung, Rollback und Delegierung der Berechtigungsverwaltung.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AC-2.A	AC-2.A Kontoverwaltung	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) kann Ihnen dabei helfen, die Prinzipien der geringsten Rechte und der Aufgabentrennung in Zugriffsberechtigungen und Autorisierungen zu integrieren und so zu verhindern, dass Richtlinien „Effect“: „Allow“ mit „Action“: „*“ anstelle von „Resource“: „*“ enthalten. Wenn Benutzern mehr Rechte eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und der Aufgabentrennung verstoßen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AC-2.A	AC-2.A Kontoverwaltung	iam-policy-no-statements-with-full-access	Stellen Sie sicher, dass IAM-Aktionen nur auf die benötigten Aktionen beschränkt sind. Wenn Benutzern mehr Rechte eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und der Aufgabentrennung verstoßen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AC-2.A	AC-2.A Kontoverwaltung	iam-root-access-key-überprüfen	Der Zugriff auf Systeme und Ressourcen kann gesteuert werden, indem überprüft wird, ob der Root-Benutzer keine Zugriffsschlüssel mit seiner AWS Identity and Access Management (IAM) -Rolle verknüpft hat. Stellen Sie sicher, dass die Root-Zugriffsschlüssel gelöscht werden. Erstellen und verwenden Sie stattdessen rollenbasierte Funktionen, AWS-Konten um das Prinzip der geringsten Funktionalität zu berücksichtigen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AC-2.A	AC-2.A Kontoverwaltung	iam-user-group-membership-überprüfen	AWS Identity and Access Management (IAM) kann Ihnen helfen, Zugriffsberechtigungen und Autorisierungen einzuschränken, indem sichergestellt wird, dass Benutzer Mitglieder mindestens einer Gruppe sind. Wenn Benutzern mehr Berechtigungen eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und Aufgabentrennung verstoßen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AC-2.A	AC-2.A Kontoverwaltung	iam-user-no-policies-überprüfen	Diese Regel stellt sicher, dass AWS Identity and Access Management (IAM) -Richtlinien nur Gruppen oder Rollen zugewiesen werden, um den Zugriff auf Systeme und Ressourcen zu kontrollieren. Die Zuweisung von Berechtigungen auf Gruppen- oder Rollenebene trägt dazu bei, die Wahrscheinlichkeit zu verringern, dass eine Identität übermäßige Berechtigungen erhält oder beibehält.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AC-2.A	AC-2.A Kontoverwaltung	iam-user-unused-credentials-überprüfen	AWS Identity and Access Management (IAM) kann Ihnen bei Zugriffsberechtigungen und Autorisierungen helfen, indem es nach IAM-Passwörtern und Zugriffsschlüsseln sucht, die für einen bestimmten Zeitraum nicht verwendet wurden. Wenn ungenutzte Anmeldeinformationen identifiziert werden, müssen Sie sie deaktivieren und/oder entfernen, da dies gegen das Prinzip der geringsten Berechtigung verstoßen könnte. Für diese Regel müssen Sie einen Wert für das maxCredentialUsage Alter festlegen (Standardkonfiguration: 90). Der tatsächliche Wert muss den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AC-2.A	AC-2.A Kontoverwaltung	multi-region-cloudtrail-enabled	AWS CloudTrail zeichnet Aktionen und API-Aufrufe der AWS Management Console auf. Sie können feststellen, welche Benutzer und Konten angerufen wurden AWS, von welcher Quell-IP-Adresse aus die Anrufe getätigt wurden und wann die Anrufe erfolgten. CloudTrail übermittelt Protokolldateien aus allen AWS Regionen an Ihren S3-Bucket , wenn MULTI_REGION_CLOUD_TRAIL_ENABLED aktiviert ist. Außerdem wird beim AWS Start einer neuen Region derselbe Trail in der neuen Region erstellt. CloudTrail Dadurch erhalten Sie automatisch Protokolldateien mit API-Aktivitäten für die neue Region.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AC-2.B	AC-2.B Kontoverwaltung	cloudtrail-enabled	AWS CloudTrail kann durch die Aufzeichnung von Aktionen und API-Aufrufen in der AWS Management Console bei der Nichtabstreitbarkeit helfen. Sie können die Benutzer und die Benutzer AWS-Konten , die einen AWS Dienst aufgerufen haben, die Quell-IP-Adresse, über die die Aufrufe generiert wurden, und den Zeitpunkt der Anrufe identifizieren. Einzelheiten zu den erfassten Daten finden Sie in den AWS CloudTrail Datensatzinhalten.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AC-2.B	AC-2.B Kontoverwaltung	ec2-imdsv2-check	Stellen Sie sicher, dass die Methode Instance Metadata Service Version 2 (IMDSv2) aktiviert ist, um den Zugriff auf und die Kontrolle der Amazon Elastic Compute Cloud (Amazon EC2) - Instance-Metadaten zu schützen. Die IMDSv2 Methode verwendet sitzungsbasierte Kontrollen. Mit können Kontrollen implementiert werden IMDSv2, um Änderungen an Instanzmetadaten einzuschränken.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AC-2.B	AC-2.B Kontoverwaltung	ecs-task-definition-user-for-host-mode-check	Wenn für eine Aufgabendefinition erhöhte Berechtigungen gelten, liegt das daran, dass der Kunde diesen Konfigurationen ausdrücklich zugestimmt hat. Diese Kontrolle prüft, ob eine unerwartete Berechtigungseskalation vorliegt, wenn für eine Aufgabendefinition das Host-Netzwerk aktiviert ist, die Kunden aber keine erhöhten Berechtigungen aktiviert haben.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AC-2.B	AC-2.B Kontoverwaltung	emr-kerberos-enabled	Die Zugriffsberechtigungen und -autorisierungen können verwaltet und nach den Prinzipien der geringsten Berechtigung und Aufgabentrennung integriert werden, indem Kerberos für Amazon-EMR-Cluster aktiviert wird. In Kerberos werden Services und Benutzer, die sich authentifizieren müssen, als Prinzipale bezeichnet. Prinzipale befinden sich in einem Kerberos-Bereich. Innerhalb dieses Bereichs wird ein Kerberos-Server als Key Distribution Center (KDC) bezeichnet. Über diesen Server können sich Prinzipale authentifizieren. Die Authentifizierung im KDC erfolgt durch die Ausstellung von Authentif

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
			izierungstickets. Das KDC unterhält eine Datenbank der Prinzipale in seinem Bereich mit ihren Passwörtern und anderen administr ativen Informationen zu jedem Prinzipal.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AC-2.B	AC-2.B Kontoverwaltung	iam-customer-policy-blocked-kms-Aktionen	AWS Identity and Access Management (IAM) kann Ihnen helfen, die Prinzipien der geringsten Rechte und der Aufgabentrennung in Zugriffsberechtigungen und Autorisierungen zu integrieren und so zu verhindern, dass Richtlinien blockierte Aktionen für alle AWS Schlüssel des Key Management Service enthalten. Wenn Benutzer mehr Rechte haben, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und Aufgabentrennung verstoßen. Mit dieser Regel können Sie den Parameter festlegen. blockedActionsPatterns (Wert „AWS Bewährte grundlegende Sicherheitsmethode

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
			n“: kms: Entschlüs seln, kms:ReEnc ryptFrom). Die tatsächlichen Werte müssen den Richtlini en Ihrer Organisation entsprechen.
CCCS-fPBMM-AC-2.B	AC-2.B Kontoverw altung	iam-group-has-users-überprüfen	AWS Identity and Access Managemen t (IAM) kann Ihnen helfen, die Prinzipien der geringsten Rechte und der Aufgabent rennung mit Zugriffsb erechtigungen und Autorisierungen zu integrieren, indem sichergestellt wird, dass IAM-Gruppen mindestens einen Benutzer haben. Die Einteilung von Benutzern in Gruppen auf der Grundlage der ihnen zugewiese nen Berechtigungen oder ihrer Funktion ist eine Möglichkeit, das Prinzip der geringste n Berechtigung zu implementieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AC-2.B	AC-2.B Kontoverwaltung	iam-inline-policy-blocked-kms-Aktionen	Stellen Sie sicher, dass ein Benutzer, eine IAM-Rolle oder eine IAM-Gruppe (AWS Identity and Access Management) nicht über eine Inline-Richtlinie verfügt, die blockierte Aktionen für alle AWS Schlüssel des Key Management Service zulässt. AWS empfiehlt, verwaltete Richtlinien anstelle von Inline-Richtlinien zu verwenden. Verwaltete Richtlinien ermöglichen Wiederverwendbarkeit, Versionsverwaltung, Rollback und Delegierung der Berechtigungsverwaltung. Mit dieser Regel können Sie den blockedActionsPatterns Parameter festlegen. (Wert „AWS Bewährte grundlegende Sicherheitsmethoden“: kms: Entschlüsseln, kms:ReEnc

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
			ryptFrom). Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.
CCCS-fPBMM-AC-2.B	AC-2.B Kontoverwaltung	iam-no-inline-policy-überprüfen	Stellen Sie sicher, dass ein Benutzer, eine IAM-Rolle oder eine IAM-Gruppe (AWS Identity and Access Management) nicht über eine Inline-Richtlinie zur Zugriffskontrolle auf Systeme und Ressourcen verfügt. AWS empfiehlt, verwaltete Richtlinien anstelle von Inline-Richtlinien zu verwenden. Verwaltete Richtlinien ermöglichen Wiederverwendbarkeit, Versionsverwaltung, Rollback und Delegierung der Berechtigungsverwaltung.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AC-2.B	AC-2.B Kontoverwaltung	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) kann Ihnen dabei helfen, die Prinzipien der geringsten Rechte und der Aufgabentrennung in Zugriffsberechtigungen und Autorisierungen zu integrieren und so zu verhindern, dass Richtlinien „Effect“: „Allow“ mit „Action“: „*“ anstelle von „Resource“: „*“ enthalten. Wenn Benutzern mehr Rechte eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und der Aufgabentrennung verstoßen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AC-2.B	AC-2.B Kontoverwaltung	iam-policy-no-statements-with-full-access	Stellen Sie sicher, dass IAM-Aktionen nur auf die benötigten Aktionen beschränkt sind. Wenn Benutzern mehr Rechte eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und der Aufgabentrennung verstoßen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AC-2.B	AC-2.B Kontoverwaltung	iam-root-access-key-überprüfen	Der Zugriff auf Systeme und Ressourcen kann gesteuert werden, indem überprüft wird, ob der Root-Benutzer keine Zugriffsschlüssel mit seiner AWS Identity and Access Management (IAM) -Rolle verknüpft hat. Stellen Sie sicher, dass die Root-Zugriffsschlüssel gelöscht werden. Erstellen und verwenden Sie stattdessen rollenbasierte Funktionen, AWS-Konten um das Prinzip der geringsten Funktionalität zu berücksichtigen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AC-2.B	AC-2.B Kontoverwaltung	iam-user-group-membership-überprüfen	AWS Identity and Access Management (IAM) kann Ihnen helfen, Zugriffsberechtigungen und Autorisierungen einzuschränken, indem sichergestellt wird, dass Benutzer Mitglieder mindestens einer Gruppe sind. Wenn Benutzern mehr Berechtigungen eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und Aufgabentrennung verstoßen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AC-2.B	AC-2.B Kontoverwaltung	iam-user-no-policies-überprüfen	Diese Regel stellt sicher, dass AWS Identity and Access Management (IAM) -Richtlinien nur Gruppen oder Rollen zugewiesen werden, um den Zugriff auf Systeme und Ressourcen zu kontrollieren. Die Zuweisung von Berechtigungen auf Gruppen- oder Rollenebene trägt dazu bei, die Wahrscheinlichkeit zu verringern, dass eine Identität übermäßige Berechtigungen erhält oder beibehält.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AC-2.B	AC-2.B Kontoverwaltung	iam-user-unused-credentials-überprüfen	AWS Identity and Access Management (IAM) kann Ihnen bei Zugriffsberechtigungen und Autorisierungen helfen, indem es nach IAM-Passwörtern und Zugriffsschlüsseln sucht, die für einen bestimmten Zeitraum nicht verwendet wurden. Wenn ungenutzte Anmeldeinformationen identifiziert werden, müssen Sie sie deaktivieren und/oder entfernen, da dies gegen das Prinzip der geringsten Berechtigung verstoßen könnte. Für diese Regel müssen Sie einen Wert für das maxCredentialUsage Alter festlegen (Standardkonfiguration: 90). Der tatsächliche Wert muss den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AC-2.B	AC-2.B Kontoverwaltung	multi-region-cloudtrail-enabled	AWS CloudTrail zeichnet Aktionen und API-Aufrufe der AWS Management Console auf. Sie können feststellen, welche Benutzer und Konten angerufen wurden AWS, von welcher Quell-IP-Adresse aus die Anrufe getätigt wurden und wann die Anrufe erfolgten. CloudTrail übermittelt Protokolldateien aus allen AWS Regionen an Ihren S3-Bucket , wenn MULTI_REGION_CLOUD_TRAIL_ENABLED aktiviert ist. Außerdem wird beim AWS Start einer neuen Region derselbe Trail in der neuen Region erstellt. CloudTrail Dadurch erhalten Sie automatisch Protokolldateien mit API-Aktivitäten für die neue Region.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AC-2.C	AC-2.C Kontoverwaltung	cloudtrail-enabled	AWS CloudTrail kann durch die Aufzeichnung von Aktionen und API-Aufrufen in der AWS Management Console bei der Nichtabstreitbarkeit helfen. Sie können die Benutzer und die Benutzer AWS-Konten , die einen AWS Dienst aufgerufen haben, die Quell-IP-Adresse, über die die Aufrufe generiert wurden, und den Zeitpunkt der Anrufe identifizieren. Einzelheiten zu den erfassten Daten finden Sie in den AWS CloudTrail Datensatzinhalten.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AC-2.C	AC-2.C Kontoverwaltung	ec2-imdsv2-check	Stellen Sie sicher, dass die Methode Instance Metadata Service Version 2 (IMDSv2) aktiviert ist, um den Zugriff auf und die Kontrolle der Amazon Elastic Compute Cloud (Amazon EC2) - Instance-Metadaten zu schützen. Die IMDSv2 Methode verwendet sitzungsbasierte Kontrollen. Mit können Kontrollen implementiert werden IMDSv2, um Änderungen an Instanzmetadaten einzuschränken.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AC-2.C	AC-2.C Kontoverwaltung	ecs-task-definition-user-for-host-mode-check	Wenn für eine Aufgabendefinition erhöhte Berechtigungen gelten, liegt das daran, dass der Kunde diesen Konfigurationen ausdrücklich zugestimmt hat. Diese Kontrolle prüft, ob eine unerwartete Berechtigungseskalation vorliegt, wenn für eine Aufgabendefinition das Host-Netzwerk aktiviert ist, die Kunden aber keine erhöhten Berechtigungen aktiviert haben.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AC-2.C	AC-2.C Kontoverwaltung	emr-kerberos-enabled	Die Zugriffsberechtigungen und -autorisierungen können verwaltet und nach den Prinzipien der geringsten Berechtigung und Aufgabentrennung integriert werden, indem Kerberos für Amazon-EMR-Cluster aktiviert wird. In Kerberos werden Services und Benutzer, die sich authentifizieren müssen, als Prinzipale bezeichnet. Prinzipale befinden sich in einem Kerberos-Bereich. Innerhalb dieses Bereichs wird ein Kerberos-Server als Key Distribution Center (KDC) bezeichnet. Über diesen Server können sich Prinzipale authentifizieren. Die Authentifizierung im KDC erfolgt durch die Ausstellung von Authentif

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
			izierungstickets. Das KDC unterhält eine Datenbank der Prinzipale in seinem Bereich mit ihren Passwörtern und anderen administr ativen Informationen zu jedem Prinzipal.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AC-2.C	AC-2.C Kontoverwaltung	iam-customer-policy-blocked-kms-Aktionen	AWS Identity and Access Management (IAM) kann Ihnen helfen, die Prinzipien der geringsten Rechte und der Aufgabentrennung in Zugriffsberechtigungen und Autorisierungen zu integrieren und so zu verhindern, dass Richtlinien blockierte Aktionen für alle AWS Schlüssel des Key Management Service enthalten. Wenn Benutzer mehr Rechte haben, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und Aufgabentrennung verstoßen. Mit dieser Regel können Sie den Parameter festlegen. blockedActionsPatterns (Wert „AWS Bewährte grundlegende Sicherheitsmethode

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
			n“: kms: Entschlüs seln, kms:ReEnc ryptFrom). Die tatsächlichen Werte müssen den Richtlini en Ihrer Organisation entsprechen.
CCCS-fPBMM-AC-2.C	AC-2.C Kontoverw altung	iam-group-has-users-überprüfen	AWS Identity and Access Managemen t (IAM) kann Ihnen helfen, die Prinzipien der geringsten Rechte und der Aufgabent rennung mit Zugriffsb erechtigungen und Autorisierungen zu integrieren, indem sichergestellt wird, dass IAM-Gruppen mindestens einen Benutzer haben. Die Einteilung von Benutzern in Gruppen auf der Grundlage der ihnen zugewiese nen Berechtigungen oder ihrer Funktion ist eine Möglichkeit, das Prinzip der geringste n Berechtigung zu implementieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AC-2.C	AC-2.C Kontoverwaltung	iam-inline-policy-blocked-kms-Aktionen	Stellen Sie sicher, dass ein Benutzer, eine IAM-Rolle oder eine IAM-Gruppe (AWS Identity and Access Management) nicht über eine Inline-Richtlinie verfügt, die blockierte Aktionen für alle AWS Schlüssel des Key Management Service zulässt. AWS empfiehlt, verwaltete Richtlinien anstelle von Inline-Richtlinien zu verwenden. Verwaltete Richtlinien ermöglichen Wiederverwendbarkeit, Versionsverwaltung, Rollback und Delegierung der Berechtigungsverwaltung. Mit dieser Regel können Sie den blockedActionsPatterns Parameter festlegen. (Wert „AWS Bewährte grundlegende Sicherheitsmethoden“: kms: Entschlüsseln, kms:ReEnc

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
			ryptFrom). Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.
CCCS-fPBMM-AC-2.C	AC-2.C Kontoverwaltung	iam-no-inline-policy-überprüfen	Stellen Sie sicher, dass ein Benutzer, eine IAM-Rolle oder eine IAM-Gruppe (AWS Identity and Access Management) nicht über eine Inline-Richtlinie zur Zugriffskontrolle auf Systeme und Ressourcen verfügt. AWS empfiehlt, verwaltete Richtlinien anstelle von Inline-Richtlinien zu verwenden. Verwaltete Richtlinien ermöglichen Wiederverwendbarkeit, Versionsverwaltung, Rollback und Delegierung der Berechtigungsverwaltung.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AC-2.C	AC-2.C Kontoverwaltung	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) kann Ihnen dabei helfen, die Prinzipien der geringsten Rechte und der Aufgabentrennung in Zugriffsberechtigungen und Autorisierungen zu integrieren und so zu verhindern, dass Richtlinien „Effect“: „Allow“ mit „Action“: „*“ anstelle von „Resource“: „*“ enthalten. Wenn Benutzern mehr Rechte eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und der Aufgabentrennung verstoßen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AC-2.C	AC-2.C Kontoverwaltung	iam-policy-no-statements-with-full-access	Stellen Sie sicher, dass IAM-Aktionen nur auf die benötigten Aktionen beschränkt sind. Wenn Benutzern mehr Rechte eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und der Aufgabentrennung verstoßen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AC-2.C	AC-2.C Kontoverwaltung	iam-root-access-key-überprüfen	Der Zugriff auf Systeme und Ressourcen kann gesteuert werden, indem überprüft wird, ob der Root-Benutzer keine Zugriffsschlüssel mit seiner AWS Identity and Access Management (IAM) -Rolle verknüpft hat. Stellen Sie sicher, dass die Root-Zugriffsschlüssel gelöscht werden. Erstellen und verwenden Sie stattdessen rollenbasierte Funktionen, AWS-Konten um das Prinzip der geringsten Funktionalität zu berücksichtigen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AC-2.C	AC-2.C Kontoverwaltung	iam-user-group-membership-überprüfen	AWS Identity and Access Management (IAM) kann Ihnen helfen, Zugriffsberechtigungen und Autorisierungen einzuschränken, indem sichergestellt wird, dass Benutzer Mitglieder mindestens einer Gruppe sind. Wenn Benutzern mehr Berechtigungen eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und Aufgabentrennung verstoßen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AC-2.C	AC-2.C Kontoverwaltung	iam-user-no-policies-überprüfen	Diese Regel stellt sicher, dass AWS Identity and Access Management (IAM) -Richtlinien nur Gruppen oder Rollen zugewiesen werden, um den Zugriff auf Systeme und Ressourcen zu kontrollieren. Die Zuweisung von Berechtigungen auf Gruppen- oder Rollenebene trägt dazu bei, die Wahrscheinlichkeit zu verringern, dass eine Identität übermäßige Berechtigungen erhält oder beibehält.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AC-2.C	AC-2.C Kontoverwaltung	iam-user-unused-credentials-überprüfen	AWS Identity and Access Management (IAM) kann Ihnen bei Zugriffsberechtigungen und Autorisierungen helfen, indem es nach IAM-Passwörtern und Zugriffsschlüsseln sucht, die für einen bestimmten Zeitraum nicht verwendet wurden. Wenn ungenutzte Anmeldeinformationen identifiziert werden, müssen Sie sie deaktivieren und/oder entfernen, da dies gegen das Prinzip der geringsten Berechtigung verstoßen könnte. Für diese Regel müssen Sie einen Wert für das maxCredentialUsage Alter festlegen (Standardkonfiguration: 90). Der tatsächliche Wert muss den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AC-2.C	AC-2.C Kontoverwaltung	multi-region-cloudtrail-enabled	AWS CloudTrail zeichnet Aktionen und API-Aufrufe der AWS Management Console auf. Sie können feststellen, welche Benutzer und Konten angerufen wurden AWS, von welcher Quell-IP-Adresse aus die Anrufe getätigt wurden und wann die Anrufe erfolgten. CloudTrail übermittelt Protokolldateien aus allen AWS Regionen an Ihren S3-Bucket , wenn MULTI_REGION_CLOUD_TRAIL_ENABLED aktiviert ist. Außerdem wird beim AWS Start einer neuen Region derselbe Trail in der neuen Region erstellt. CloudTrail Dadurch erhalten Sie automatisch Protokolldateien mit API-Aktivitäten für die neue Region.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AC-2.D	AC-2.D Kontoverwaltung	cloudtrail-enabled	AWS CloudTrail kann durch die Aufzeichnung von Aktionen und API-Aufrufen in der AWS Management Console bei der Nichtabstreitbarkeit helfen. Sie können die Benutzer und die Benutzer AWS-Konten , die einen AWS Dienst aufgerufen haben, die Quell-IP-Adresse, über die die Aufrufe generiert wurden, und den Zeitpunkt der Anrufe identifizieren. Einzelheiten zu den erfassten Daten finden Sie in den AWS CloudTrail Datensatzinhalten.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AC-2.D	AC-2.D Kontoverwaltung	ec2-imdsv2-check	Stellen Sie sicher, dass die Methode Instance Metadata Service Version 2 (IMDSv2) aktiviert ist, um den Zugriff auf und die Kontrolle der Amazon Elastic Compute Cloud (Amazon EC2) - Instance-Metadaten zu schützen. Die IMDSv2 Methode verwendet sitzungsbasierte Kontrollen. Mit können Kontrollen implementiert werden IMDSv2, um Änderungen an Instanzmetadaten einzuschränken.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AC-2.D	AC-2.D Kontoverwaltung	ecs-task-definition-user-for-host-mode-check	Wenn für eine Aufgabendefinition erhöhte Berechtigungen gelten, liegt das daran, dass der Kunde diesen Konfigurationen ausdrücklich zugestimmt hat. Diese Kontrolle prüft, ob eine unerwartete Berechtigungseskalation vorliegt, wenn für eine Aufgabendefinition das Host-Netzwerk aktiviert ist, die Kunden aber keine erhöhten Berechtigungen aktiviert haben.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AC-2.D	AC-2.D Kontoverwaltung	emr-kerberos-enabled	Die Zugriffsberechtigungen und -autorisierungen können verwaltet und nach den Prinzipien der geringsten Berechtigung und Aufgabentrennung integriert werden, indem Kerberos für Amazon-EMR-Cluster aktiviert wird. In Kerberos werden Services und Benutzer, die sich authentifizieren müssen, als Prinzipale bezeichnet. Prinzipale befinden sich in einem Kerberos-Bereich. Innerhalb dieses Bereichs wird ein Kerberos-Server als Key Distribution Center (KDC) bezeichnet. Über diesen Server können sich Prinzipale authentifizieren. Die Authentifizierung im KDC erfolgt durch die Ausstellung von Authentif

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
			izierungstickets. Das KDC unterhält eine Datenbank der Prinzipale in seinem Bereich mit ihren Passwörtern und anderen administr ativen Informationen zu jedem Prinzipal.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AC-2.D	AC-2.D Kontoverwaltung	iam-customer-policy-blocked-kms-Aktionen	AWS Identity and Access Management (IAM) kann Ihnen helfen, die Prinzipien der geringsten Rechte und der Aufgabentrennung in Zugriffsberechtigungen und Autorisierungen zu integrieren und so zu verhindern, dass Richtlinien blockierte Aktionen für alle AWS Schlüssel des Key Management Service enthalten. Wenn Benutzer mehr Rechte haben, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und Aufgabentrennung verstoßen. Mit dieser Regel können Sie den Parameter festlegen. blockedActionsPatterns (Wert „AWS Bewährte grundlegende Sicherheitsmethode

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
			n“: kms: Entschlüs seln, kms:ReEnc ryptFrom). Die tatsächlichen Werte müssen den Richtlini en Ihrer Organisation entsprechen.
CCCS-fPBMM-AC-2.D	AC-2.D Kontoverw altung	iam-group-has-users-überprüfen	AWS Identity and Access Managemen t (IAM) kann Ihnen helfen, die Prinzipien der geringsten Rechte und der Aufgabent rennung mit Zugriffsb erechtigungen und Autorisierungen zu integrieren, indem sichergestellt wird, dass IAM-Gruppen mindestens einen Benutzer haben. Die Einteilung von Benutzern in Gruppen auf der Grundlage der ihnen zugewiese nen Berechtigungen oder ihrer Funktion ist eine Möglichkeit, das Prinzip der geringste n Berechtigung zu implementieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AC-2.D	AC-2.D Kontoverwaltung	iam-inline-policy-blocked-kms-Aktionen	Stellen Sie sicher, dass ein Benutzer, eine IAM-Rolle oder eine IAM-Gruppe (AWS Identity and Access Management) nicht über eine Inline-Richtlinie verfügt, die blockierte Aktionen für alle AWS Schlüssel des Key Management Service zulässt. AWS empfiehlt, verwaltete Richtlinien anstelle von Inline-Richtlinien zu verwenden. Verwaltete Richtlinien ermöglichen Wiederverwendbarkeit, Versionsverwaltung, Rollback und Delegierung der Berechtigungsverwaltung. Mit dieser Regel können Sie den blockedActionsPatterns Parameter festlegen. (Wert „AWS Bewährte grundlegende Sicherheitsmethoden“: kms: Entschlüsseln, kms:ReEnc

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
			ryptFrom). Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.
CCCS-fPBMM-AC-2.D	AC-2.D Kontoverwaltung	iam-no-inline-policy-überprüfen	Stellen Sie sicher, dass ein Benutzer, eine IAM-Rolle oder eine IAM-Gruppe (AWS Identity and Access Management) nicht über eine Inline-Richtlinie zur Zugriffskontrolle auf Systeme und Ressourcen verfügt. AWS empfiehlt, verwaltete Richtlinien anstelle von Inline-Richtlinien zu verwenden. Verwaltete Richtlinien ermöglichen Wiederverwendbarkeit, Versionsverwaltung, Rollback und Delegierung der Berechtigungsverwaltung.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AC-2.D	AC-2.D Kontoverwaltung	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) kann Ihnen dabei helfen, die Prinzipien der geringsten Rechte und der Aufgabentrennung in Zugriffsberechtigungen und Autorisierungen zu integrieren und so zu verhindern, dass Richtlinien „Effect“: „Allow“ mit „Action“: „*“ anstelle von „Resource“: „*“ enthalten. Wenn Benutzern mehr Rechte eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und der Aufgabentrennung verstoßen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AC-2.D	AC-2.D Kontoverwaltung	iam-policy-no-statements-with-full-access	Stellen Sie sicher, dass IAM-Aktionen nur auf die benötigten Aktionen beschränkt sind. Wenn Benutzern mehr Rechte eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und der Aufgabentrennung verstoßen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AC-2.D	AC-2.D Kontoverwaltung	iam-root-access-key-überprüfen	Der Zugriff auf Systeme und Ressourcen kann gesteuert werden, indem überprüft wird, ob der Root-Benutzer keine Zugriffsschlüssel mit seiner AWS Identity and Access Management (IAM) -Rolle verknüpft hat. Stellen Sie sicher, dass die Root-Zugriffsschlüssel gelöscht werden. Erstellen und verwenden Sie stattdessen rollenbasierte Funktionen, AWS-Konten um das Prinzip der geringsten Funktionalität zu berücksichtigen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AC-2.D	AC-2.D Kontoverwaltung	iam-user-group-membership-überprüfen	AWS Identity and Access Management (IAM) kann Ihnen helfen, Zugriffsberechtigungen und Autorisierungen einzuschränken, indem sichergestellt wird, dass Benutzer Mitglieder mindestens einer Gruppe sind. Wenn Benutzern mehr Berechtigungen eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und Aufgabentrennung verstoßen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AC-2.D	AC-2.D Kontoverwaltung	iam-user-no-policies-überprüfen	Diese Regel stellt sicher, dass AWS Identity and Access Management (IAM) -Richtlinien nur Gruppen oder Rollen zugewiesen werden, um den Zugriff auf Systeme und Ressourcen zu kontrollieren. Die Zuweisung von Berechtigungen auf Gruppen- oder Rollenebene trägt dazu bei, die Wahrscheinlichkeit zu verringern, dass eine Identität übermäßige Berechtigungen erhält oder beibehält.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AC-2.D	AC-2.D Kontoverwaltung	iam-user-unused-credentials-überprüfen	AWS Identity and Access Management (IAM) kann Ihnen bei Zugriffsberechtigungen und Autorisierungen helfen, indem es nach IAM-Passwörtern und Zugriffsschlüsseln sucht, die für einen bestimmten Zeitraum nicht verwendet wurden. Wenn ungenutzte Anmeldeinformationen identifiziert werden, müssen Sie sie deaktivieren und/oder entfernen, da dies gegen das Prinzip der geringsten Berechtigung verstoßen könnte. Für diese Regel müssen Sie einen Wert für das maxCredentialUsage Alter festlegen (Standardkonfiguration: 90). Der tatsächliche Wert muss den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AC-2.D	AC-2.D Kontoverwaltung	multi-region-cloudtrail-enabled	AWS CloudTrail zeichnet Aktionen und API-Aufrufe der AWS Management Console auf. Sie können feststellen, welche Benutzer und Konten angerufen wurden AWS, von welcher Quell-IP-Adresse aus die Anrufe getätigt wurden und wann die Anrufe erfolgten. CloudTrail übermittelt Protokolldateien aus allen AWS Regionen an Ihren S3-Bucket , wenn MULTI_REGION_CLOUD_TRAIL_ENABLED aktiviert ist. Außerdem wird beim AWS Start einer neuen Region derselbe Trail in der neuen Region erstellt. CloudTrail Dadurch erhalten Sie automatisch Protokolldateien mit API-Aktivitäten für die neue Region.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AC-2.E	AC-2.E Kontoverwaltung	cloudtrail-enabled	AWS CloudTrail kann durch die Aufzeichnung von Aktionen und API-Aufrufen in der AWS Management Console bei der Nichtabstreitbarkeit helfen. Sie können die Benutzer und die Benutzer AWS-Konten , die einen AWS Dienst aufgerufen haben, die Quell-IP-Adresse, über die die Aufrufe generiert wurden, und den Zeitpunkt der Anrufe identifizieren. Einzelheiten zu den erfassten Daten finden Sie in den AWS CloudTrail Datensatzinhalten.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AC-2.E	AC-2.E Kontoverwaltung	ec2-imdsv2-check	Stellen Sie sicher, dass die Methode Instance Metadata Service Version 2 (IMDSv2) aktiviert ist, um den Zugriff auf und die Kontrolle der Amazon Elastic Compute Cloud (Amazon EC2) - Instance-Metadaten zu schützen. Die IMDSv2 Methode verwendet sitzungsbasierte Kontrollen. Mit können Kontrollen implementiert werden IMDSv2, um Änderungen an Instanzmetadaten einzuschränken.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AC-2.E	AC-2.E Kontoverwaltung	ecs-task-definition-user-for-host-mode-check	Wenn für eine Aufgabendefinition erhöhte Berechtigungen gelten, liegt das daran, dass der Kunde diesen Konfigurationen ausdrücklich zugestimmt hat. Diese Kontrolle prüft, ob eine unerwartete Berechtigungseskalation vorliegt, wenn für eine Aufgabendefinition das Host-Netzwerk aktiviert ist, die Kunden aber keine erhöhten Berechtigungen aktiviert haben.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AC-2.E	AC-2.E Kontoverwaltung	emr-kerberos-enabled	Die Zugriffsberechtigungen und -autorisierungen können verwaltet und nach den Prinzipien der geringsten Berechtigung und Aufgabentrennung integriert werden, indem Kerberos für Amazon-EMR-Cluster aktiviert wird. In Kerberos werden Services und Benutzer, die sich authentifizieren müssen, als Prinzipale bezeichnet. Prinzipale befinden sich in einem Kerberos-Bereich. Innerhalb dieses Bereichs wird ein Kerberos-Server als Key Distribution Center (KDC) bezeichnet. Über diesen Server können sich Prinzipale authentifizieren. Die Authentifizierung im KDC erfolgt durch die Ausstellung von Authentif

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
			izierungstickets. Das KDC unterhält eine Datenbank der Prinzipale in seinem Bereich mit ihren Passwörtern und anderen administr ativen Informationen zu jedem Prinzipal.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AC-2.E	AC-2.E Kontoverwaltung	iam-customer-policy-blocked-kms-Aktionen	AWS Identity and Access Management (IAM) kann Ihnen helfen, die Prinzipien der geringsten Rechte und der Aufgabentrennung in Zugriffsberechtigungen und Autorisierungen zu integrieren und so zu verhindern, dass Richtlinien blockierte Aktionen für alle AWS Schlüssel des Key Management Service enthalten. Wenn Benutzer mehr Rechte haben, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und Aufgabentrennung verstoßen. Mit dieser Regel können Sie den Parameter festlegen. blockedActionsPatterns (Wert „AWS Bewährte grundlegende Sicherheitsmethode

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
			n“: kms: Entschlüs seln, kms:ReEnc ryptFrom). Die tatsächlichen Werte müssen den Richtlini en Ihrer Organisation entsprechen.
CCCS-fPBMM-AC-2.E	AC-2.E Kontoverw altung	iam-group-has-users-überprüfen	AWS Identity and Access Managemen t (IAM) kann Ihnen helfen, die Prinzipien der geringsten Rechte und der Aufgabent rennung mit Zugriffsb erechtigungen und Autorisierungen zu integrieren, indem sichergestellt wird, dass IAM-Gruppen mindestens einen Benutzer haben. Die Einteilung von Benutzern in Gruppen auf der Grundlage der ihnen zugewiese nen Berechtigungen oder ihrer Funktion ist eine Möglichkeit, das Prinzip der geringste n Berechtigung zu implementieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AC-2.E	AC-2.E Kontoverwaltung	iam-inline-policy-blocked-kms-Aktionen	Stellen Sie sicher, dass ein Benutzer, eine IAM-Rolle oder eine IAM-Gruppe (AWS Identity and Access Management) nicht über eine Inline-Richtlinie verfügt, die blockierte Aktionen für alle AWS Schlüssel des Key Management Service zulässt. AWS empfiehlt, verwaltete Richtlinien anstelle von Inline-Richtlinien zu verwenden. Verwaltete Richtlinien ermöglichen Wiederverwendbarkeit, Versionsverwaltung, Rollback und Delegierung der Berechtigungsverwaltung. Mit dieser Regel können Sie den blockedActionsPatterns Parameter festlegen. (Wert „AWS Bewährte grundlegende Sicherheitsmethoden“: kms: Entschlüsseln, kms:ReEnc

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
			ryptFrom). Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.
CCCS-fPBMM-AC-2.E	AC-2.E Kontoverwaltung	iam-no-inline-policy-überprüfen	Stellen Sie sicher, dass ein Benutzer, eine IAM-Rolle oder eine IAM-Gruppe (AWS Identity and Access Management) nicht über eine Inline-Richtlinie zur Zugriffskontrolle auf Systeme und Ressourcen verfügt. AWS empfiehlt, verwaltete Richtlinien anstelle von Inline-Richtlinien zu verwenden. Verwaltete Richtlinien ermöglichen Wiederverwendbarkeit, Versionsverwaltung, Rollback und Delegierung der Berechtigungsverwaltung.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AC-2.E	AC-2.E Kontoverwaltung	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) kann Ihnen dabei helfen, die Prinzipien der geringsten Rechte und der Aufgabentrennung in Zugriffsberechtigungen und Autorisierungen zu integrieren und so zu verhindern, dass Richtlinien „Effect“: „Allow“ mit „Action“: „*“ anstelle von „Resource“: „*“ enthalten. Wenn Benutzern mehr Rechte eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und der Aufgabentrennung verstoßen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AC-2.E	AC-2.E Kontoverwaltung	iam-policy-no-statements-with-full-access	Stellen Sie sicher, dass IAM-Aktionen nur auf die benötigten Aktionen beschränkt sind. Wenn Benutzern mehr Rechte eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und der Aufgabentrennung verstoßen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AC-2.E	AC-2.E Kontoverwaltung	iam-root-access-key-überprüfen	Der Zugriff auf Systeme und Ressourcen kann gesteuert werden, indem überprüft wird, ob der Root-Benutzer keine Zugriffsschlüssel mit seiner AWS Identity and Access Management (IAM) -Rolle verknüpft hat. Stellen Sie sicher, dass die Root-Zugriffsschlüssel gelöscht werden. Erstellen und verwenden Sie stattdessen rollenbasierte Funktionen, AWS-Konten um das Prinzip der geringsten Funktionalität zu berücksichtigen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AC-2.E	AC-2.E Kontoverwaltung	iam-user-group-membership-überprüfen	AWS Identity and Access Management (IAM) kann Ihnen helfen, Zugriffsberechtigungen und Autorisierungen einzuschränken, indem sichergestellt wird, dass Benutzer Mitglieder mindestens einer Gruppe sind. Wenn Benutzern mehr Berechtigungen eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und Aufgabentrennung verstoßen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AC-2.E	AC-2.E Kontoverwaltung	iam-user-no-policies-überprüfen	Diese Regel stellt sicher, dass AWS Identity and Access Management (IAM) -Richtlinien nur Gruppen oder Rollen zugewiesen werden, um den Zugriff auf Systeme und Ressourcen zu kontrollieren. Die Zuweisung von Berechtigungen auf Gruppen- oder Rollenebene trägt dazu bei, die Wahrscheinlichkeit zu verringern, dass eine Identität übermäßige Berechtigungen erhält oder beibehält.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AC-2.E	AC-2.E Kontoverwaltung	iam-user-unused-credentials-überprüfen	AWS Identity and Access Management (IAM) kann Ihnen bei Zugriffsberechtigungen und Autorisierungen helfen, indem es nach IAM-Passwörtern und Zugriffsschlüsseln sucht, die für einen bestimmten Zeitraum nicht verwendet wurden. Wenn ungenutzte Anmeldeinformationen identifiziert werden, müssen Sie sie deaktivieren und/oder entfernen, da dies gegen das Prinzip der geringsten Berechtigung verstoßen könnte. Für diese Regel müssen Sie einen Wert für das maxCredentialUsage Alter festlegen (Standardkonfiguration: 90). Der tatsächliche Wert muss den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AC-2.E	AC-2.E Kontoverwaltung	multi-region-cloudtrail-enabled	AWS CloudTrail zeichnet Aktionen und API-Aufrufe der AWS Management Console auf. Sie können feststellen, welche Benutzer und Konten angerufen wurden AWS, von welcher Quell-IP-Adresse aus die Anrufe getätigt wurden und wann die Anrufe erfolgten. CloudTrail übermittelt Protokolldateien aus allen AWS Regionen an Ihren S3-Bucket , wenn MULTI_REGION_CLOUD_TRAIL_ENABLED aktiviert ist. Außerdem wird beim AWS Start einer neuen Region derselbe Trail in der neuen Region erstellt. CloudTrail Dadurch erhalten Sie automatisch Protokolldateien mit API-Aktivitäten für die neue Region.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AC-2.F	AC-2.F Kontoverwaltung	cloudtrail-enabled	AWS CloudTrail kann durch die Aufzeichnung von Aktionen und API-Aufrufen in der AWS Management Console bei der Nichtabstreitbarkeit helfen. Sie können die Benutzer und die Benutzer AWS-Konten , die einen AWS Dienst aufgerufen haben, die Quell-IP-Adresse, über die die Aufrufe generiert wurden, und den Zeitpunkt der Anrufe identifizieren. Einzelheiten zu den erfassten Daten finden Sie in den AWS CloudTrail Datensatzinhalten.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AC-2.F	AC-2.F Kontoverwaltung	ec2-imdsv2-check	Stellen Sie sicher, dass die Methode Instance Metadata Service Version 2 (IMDSv2) aktiviert ist, um den Zugriff auf und die Kontrolle der Amazon Elastic Compute Cloud (Amazon EC2) - Instance-Metadaten zu schützen. Die IMDSv2 Methode verwendet sitzungsbasierte Kontrollen. Mit können Kontrollen implementiert werden IMDSv2, um Änderungen an Instanzmetadaten einzuschränken.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AC-2.F	AC-2.F Kontoverwaltung	ecs-task-definition-user-for-host-mode-check	Wenn für eine Aufgabendefinition erhöhte Berechtigungen gelten, liegt das daran, dass der Kunde diesen Konfigurationen ausdrücklich zugestimmt hat. Diese Kontrolle prüft, ob eine unerwartete Berechtigungseskalation vorliegt, wenn für eine Aufgabendefinition das Host-Netzwerk aktiviert ist, die Kunden aber keine erhöhten Berechtigungen aktiviert haben.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AC-2.F	AC-2.F Kontoverwaltung	emr-kerberos-enabled	Die Zugriffsberechtigungen und -autorisierungen können verwaltet und nach den Prinzipien der geringsten Berechtigung und Aufgabentrennung integriert werden, indem Kerberos für Amazon-EMR-Cluster aktiviert wird. In Kerberos werden Services und Benutzer, die sich authentifizieren müssen, als Prinzipale bezeichnet. Prinzipale befinden sich in einem Kerberos-Bereich. Innerhalb dieses Bereichs wird ein Kerberos-Server als Key Distribution Center (KDC) bezeichnet. Über diesen Server können sich Prinzipale authentifizieren. Die Authentifizierung im KDC erfolgt durch die Ausstellung von Authentif

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
			izierungstickets. Das KDC unterhält eine Datenbank der Prinzipale in seinem Bereich mit ihren Passwörtern und anderen administr ativen Informationen zu jedem Prinzipal.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AC-2.F	AC-2.F Kontoverwaltung	iam-customer-policy-blocked-kms-Aktionen	AWS Identity and Access Management (IAM) kann Ihnen helfen, die Prinzipien der geringsten Rechte und der Aufgabentrennung in Zugriffsberechtigungen und Autorisierungen zu integrieren und so zu verhindern, dass Richtlinien blockierte Aktionen für alle AWS Schlüssel des Key Management Service enthalten. Wenn Benutzer mehr Rechte haben, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und Aufgabentrennung verstoßen. Mit dieser Regel können Sie den Parameter festlegen. blockedActionsPatterns (Wert „AWS Bewährte grundlegende Sicherheitsmethode

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
			n“: kms: Entschlüs seln, kms:ReEnc ryptFrom). Die tatsächlichen Werte müssen den Richtlini en Ihrer Organisation entsprechen.
CCCS-fPBMM-AC-2.F	AC-2.F Kontoverw altung	iam-group-has-users-überprüfen	AWS Identity and Access Managemen t (IAM) kann Ihnen helfen, die Prinzipien der geringsten Rechte und der Aufgabent rennung mit Zugriffsb erechtigungen und Autorisierungen zu integrieren, indem sichergestellt wird, dass IAM-Gruppen mindestens einen Benutzer haben. Die Einteilung von Benutzern in Gruppen auf der Grundlage der ihnen zugewiese nen Berechtigungen oder ihrer Funktion ist eine Möglichkeit, das Prinzip der geringste n Berechtigung zu implementieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AC-2.F	AC-2.F Kontoverwaltung	iam-inline-policy-blocked-kms-Aktionen	Stellen Sie sicher, dass ein Benutzer, eine IAM-Rolle oder eine IAM-Gruppe (AWS Identity and Access Management) nicht über eine Inline-Richtlinie verfügt, die blockierte Aktionen für alle AWS Schlüssel des Key Management Service zulässt. AWS empfiehlt, verwaltete Richtlinien anstelle von Inline-Richtlinien zu verwenden. Verwaltete Richtlinien ermöglichen Wiederverwendbarkeit, Versionsverwaltung, Rollback und Delegierung der Berechtigungsverwaltung. Mit dieser Regel können Sie den blockedActionsPatterns Parameter festlegen. (Wert „AWS Bewährte grundlegende Sicherheitsmethoden“: kms: Entschlüsseln, kms:ReEnc

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
			ryptFrom). Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.
CCCS-fPBMM-AC-2.F	AC-2.F Kontoverwaltung	iam-no-inline-policy-überprüfen	Stellen Sie sicher, dass ein Benutzer, eine IAM-Rolle oder eine IAM-Gruppe (AWS Identity and Access Management) nicht über eine Inline-Richtlinie zur Zugriffskontrolle auf Systeme und Ressourcen verfügt. AWS empfiehlt, verwaltete Richtlinien anstelle von Inline-Richtlinien zu verwenden. Verwaltete Richtlinien ermöglichen Wiederverwendbarkeit, Versionsverwaltung, Rollback und Delegierung der Berechtigungsverwaltung.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AC-2.F	AC-2.F Kontoverwaltung	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) kann Ihnen dabei helfen, die Prinzipien der geringsten Rechte und der Aufgabentrennung in Zugriffsberechtigungen und Autorisierungen zu integrieren und so zu verhindern, dass Richtlinien „Effect“: „Allow“ mit „Action“: „*“ anstelle von „Resource“: „*“ enthalten. Wenn Benutzern mehr Rechte eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und der Aufgabentrennung verstoßen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AC-2.F	AC-2.F Kontoverwaltung	iam-policy-no-statements-with-full-access	Stellen Sie sicher, dass IAM-Aktionen nur auf die benötigten Aktionen beschränkt sind. Wenn Benutzern mehr Rechte eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und der Aufgabentrennung verstoßen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AC-2.F	AC-2.F Kontoverwaltung	iam-root-access-key-überprüfen	Der Zugriff auf Systeme und Ressourcen kann gesteuert werden, indem überprüft wird, ob der Root-Benutzer keine Zugriffsschlüssel mit seiner AWS Identity and Access Management (IAM) -Rolle verknüpft hat. Stellen Sie sicher, dass die Root-Zugriffsschlüssel gelöscht werden. Erstellen und verwenden Sie stattdessen rollenbasierte Funktionen, AWS-Konten um das Prinzip der geringsten Funktionalität zu berücksichtigen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AC-2.F	AC-2.F Kontoverwaltung	iam-user-group-membership-überprüfen	AWS Identity and Access Management (IAM) kann Ihnen helfen, Zugriffsberechtigungen und Autorisierungen einzuschränken, indem sichergestellt wird, dass Benutzer Mitglieder mindestens einer Gruppe sind. Wenn Benutzern mehr Berechtigungen eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und Aufgabentrennung verstoßen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AC-2.F	AC-2.F Kontoverwaltung	iam-user-no-policies-überprüfen	Diese Regel stellt sicher, dass AWS Identity and Access Management (IAM) -Richtlinien nur Gruppen oder Rollen zugewiesen werden, um den Zugriff auf Systeme und Ressourcen zu kontrollieren. Die Zuweisung von Berechtigungen auf Gruppen- oder Rollenebene trägt dazu bei, die Wahrscheinlichkeit zu verringern, dass eine Identität übermäßige Berechtigungen erhält oder beibehält.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AC-2.F	AC-2.F Kontoverwaltung	iam-user-unused-credentials-überprüfen	AWS Identity and Access Management (IAM) kann Ihnen bei Zugriffsberechtigungen und Autorisierungen helfen, indem es nach IAM-Passwörtern und Zugriffsschlüsseln sucht, die für einen bestimmten Zeitraum nicht verwendet wurden. Wenn ungenutzte Anmeldeinformationen identifiziert werden, müssen Sie sie deaktivieren und/oder entfernen, da dies gegen das Prinzip der geringsten Berechtigung verstoßen könnte. Für diese Regel müssen Sie einen Wert für das maxCredentialUsage Alter festlegen (Standardkonfiguration: 90). Der tatsächliche Wert muss den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AC-2.F	AC-2.F Kontoverwaltung	multi-region-cloudtrail-enabled	AWS CloudTrail zeichnet Aktionen und API-Aufrufe der AWS Management Console auf. Sie können feststellen, welche Benutzer und Konten angerufen wurden AWS, von welcher Quell-IP-Adresse aus die Anrufe getätigt wurden und wann die Anrufe erfolgten. CloudTrail übermittelt Protokolldateien aus allen AWS Regionen an Ihren S3-Bucket , wenn MULTI_REGION_CLOUD_TRAIL_ENABLED aktiviert ist. Außerdem wird beim AWS Start einer neuen Region derselbe Trail in der neuen Region erstellt. CloudTrail Dadurch erhalten Sie automatisch Protokolldateien mit API-Aktivitäten für die neue Region.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AC-2.G	AC-2.G Kontoverwaltung	cloudtrail-enabled	AWS CloudTrail kann durch die Aufzeichnung von Aktionen und API-Aufrufen in der AWS Management Console bei der Nichtabstreitbarkeit helfen. Sie können die Benutzer und die Benutzer AWS-Konten , die einen AWS Dienst aufgerufen haben, die Quell-IP-Adresse, über die die Aufrufe generiert wurden, und den Zeitpunkt der Anrufe identifizieren. Einzelheiten zu den erfassten Daten finden Sie in den AWS CloudTrail Datensatzinhalten.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AC-2.G	AC-2.G Kontoverwaltung	ec2-imdsv2-check	Stellen Sie sicher, dass die Methode Instance Metadata Service Version 2 (IMDSv2) aktiviert ist, um den Zugriff auf und die Kontrolle der Amazon Elastic Compute Cloud (Amazon EC2) - Instance-Metadaten zu schützen. Die IMDSv2 Methode verwendet sitzungsbasierte Kontrollen. Mit können Kontrollen implementiert werden IMDSv2, um Änderungen an Instanzmetadaten einzuschränken.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AC-2.G	AC-2.G Kontoverwaltung	ecs-task-definition-user-for-host-mode-check	Wenn für eine Aufgabendefinition erhöhte Berechtigungen gelten, liegt das daran, dass der Kunde diesen Konfigurationen ausdrücklich zugestimmt hat. Diese Kontrolle prüft, ob eine unerwartete Berechtigungseskalation vorliegt, wenn für eine Aufgabendefinition das Host-Netzwerk aktiviert ist, die Kunden aber keine erhöhten Berechtigungen aktiviert haben.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AC-2.G	AC-2.G Kontoverwaltung	emr-kerberos-enabled	Die Zugriffsberechtigungen und -autorisierungen können verwaltet und nach den Prinzipien der geringsten Berechtigung und Aufgabentrennung integriert werden, indem Kerberos für Amazon-EMR-Cluster aktiviert wird. In Kerberos werden Services und Benutzer, die sich authentifizieren müssen, als Prinzipale bezeichnet. Prinzipale befinden sich in einem Kerberos-Bereich. Innerhalb dieses Bereichs wird ein Kerberos-Server als Key Distribution Center (KDC) bezeichnet. Über diesen Server können sich Prinzipale authentifizieren. Die Authentifizierung im KDC erfolgt durch die Ausstellung von Authentif

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
			izierungstickets. Das KDC unterhält eine Datenbank der Prinzipale in seinem Bereich mit ihren Passwörtern und anderen administr ativen Informationen zu jedem Prinzipal.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AC-2.G	AC-2.G Kontoverwaltung	iam-customer-policy-blocked-kms-Aktionen	AWS Identity and Access Management (IAM) kann Ihnen helfen, die Prinzipien der geringsten Rechte und der Aufgabentrennung in Zugriffsberechtigungen und Autorisierungen zu integrieren und so zu verhindern, dass Richtlinien blockierte Aktionen für alle AWS Schlüssel des Key Management Service enthalten. Wenn Benutzer mehr Rechte haben, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und Aufgabentrennung verstoßen. Mit dieser Regel können Sie den Parameter festlegen. blockedActionsPatterns (Wert „AWS Bewährte grundlegende Sicherheitsmethode

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
			n“: kms: Entschlüs seln, kms:ReEnc ryptFrom). Die tatsächlichen Werte müssen den Richtlini en Ihrer Organisation entsprechen.
CCCS-fPBMM-AC-2.G	AC-2.G Kontoverw altung	iam-group-has-users-überprüfen	AWS Identity and Access Managemen t (IAM) kann Ihnen helfen, die Prinzipien der geringsten Rechte und der Aufgabent rennung mit Zugriffsb erechtigungen und Autorisierungen zu integrieren, indem sichergestellt wird, dass IAM-Gruppen mindestens einen Benutzer haben. Die Einteilung von Benutzern in Gruppen auf der Grundlage der ihnen zugewiese nen Berechtigungen oder ihrer Funktion ist eine Möglichkeit, das Prinzip der geringste n Berechtigung zu implementieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AC-2.G	AC-2.G Kontoverwaltung	iam-inline-policy-blocked-kms-Aktionen	Stellen Sie sicher, dass ein Benutzer, eine IAM-Rolle oder eine IAM-Gruppe (AWS Identity and Access Management) nicht über eine Inline-Richtlinie verfügt, die blockierte Aktionen für alle AWS Schlüssel des Key Management Service zulässt. AWS empfiehlt, verwaltete Richtlinien anstelle von Inline-Richtlinien zu verwenden. Verwaltete Richtlinien ermöglichen Wiederverwendbarkeit, Versionsverwaltung, Rollback und Delegierung der Berechtigungsverwaltung. Mit dieser Regel können Sie den blockedActionsPatterns Parameter festlegen. (Wert „AWS Bewährte grundlegende Sicherheitsmethoden“: kms: Entschlüsseln, kms:ReEnc

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
			ryptFrom). Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.
CCCS-fPBMM-AC-2.G	AC-2.G Kontoverwaltung	iam-no-inline-policy-überprüfen	Stellen Sie sicher, dass ein Benutzer, eine IAM-Rolle oder eine IAM-Gruppe (AWS Identity and Access Management) nicht über eine Inline-Richtlinie zur Zugriffskontrolle auf Systeme und Ressourcen verfügt. AWS empfiehlt, verwaltete Richtlinien anstelle von Inline-Richtlinien zu verwenden. Verwaltete Richtlinien ermöglichen Wiederverwendbarkeit, Versionsverwaltung, Rollback und Delegierung der Berechtigungsverwaltung.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AC-2.G	AC-2.G Kontoverwaltung	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) kann Ihnen dabei helfen, die Prinzipien der geringsten Rechte und der Aufgabentrennung in Zugriffsberechtigungen und Autorisierungen zu integrieren und so zu verhindern, dass Richtlinien „Effect“: „Allow“ mit „Action“: „*“ anstelle von „Resource“: „*“ enthalten. Wenn Benutzern mehr Rechte eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und der Aufgabentrennung verstoßen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AC-2.G	AC-2.G Kontoverwaltung	iam-policy-no-statements-with-full-access	Stellen Sie sicher, dass IAM-Aktionen nur auf die benötigten Aktionen beschränkt sind. Wenn Benutzern mehr Rechte eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und der Aufgabentrennung verstoßen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AC-2.G	AC-2.G Kontoverwaltung	iam-root-access-key-überprüfen	Der Zugriff auf Systeme und Ressourcen kann gesteuert werden, indem überprüft wird, ob der Root-Benutzer keine Zugriffsschlüssel mit seiner AWS Identity and Access Management (IAM) -Rolle verknüpft hat. Stellen Sie sicher, dass die Root-Zugriffsschlüssel gelöscht werden. Erstellen und verwenden Sie stattdessen rollenbasierte Funktionen, AWS-Konten um das Prinzip der geringsten Funktionalität zu berücksichtigen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AC-2.G	AC-2.G Kontoverwaltung	iam-user-group-membership-überprüfen	AWS Identity and Access Management (IAM) kann Ihnen helfen, Zugriffsberechtigungen und Autorisierungen einzuschränken, indem sichergestellt wird, dass Benutzer Mitglieder mindestens einer Gruppe sind. Wenn Benutzern mehr Berechtigungen eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und Aufgabentrennung verstoßen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AC-2.G	AC-2.G Kontoverwaltung	iam-user-no-policies-überprüfen	Diese Regel stellt sicher, dass AWS Identity and Access Management (IAM) -Richtlinien nur Gruppen oder Rollen zugewiesen werden, um den Zugriff auf Systeme und Ressourcen zu kontrollieren. Die Zuweisung von Berechtigungen auf Gruppen- oder Rollenebene trägt dazu bei, die Wahrscheinlichkeit zu verringern, dass eine Identität übermäßige Berechtigungen erhält oder beibehält.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AC-2.G	AC-2.G Kontoverwaltung	iam-user-unused-credentials-überprüfen	AWS Identity and Access Management (IAM) kann Ihnen bei Zugriffsberechtigungen und Autorisierungen helfen, indem es nach IAM-Passwörtern und Zugriffsschlüsseln sucht, die für einen bestimmten Zeitraum nicht verwendet wurden. Wenn ungenutzte Anmeldeinformationen identifiziert werden, müssen Sie sie deaktivieren und/oder entfernen, da dies gegen das Prinzip der geringsten Berechtigung verstoßen könnte. Für diese Regel müssen Sie einen Wert für das maxCredentialUsage Alter festlegen (Standardkonfiguration: 90). Der tatsächliche Wert muss den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AC-2.G	AC-2.G Kontoverwaltung	multi-region-cloudtrail-enabled	AWS CloudTrail zeichnet Aktionen und API-Aufrufe der AWS Management Console auf. Sie können feststellen, welche Benutzer und Konten angerufen wurden AWS, von welcher Quell-IP-Adresse aus die Anrufe getätigt wurden und wann die Anrufe erfolgten. CloudTrail übermittelt Protokolldateien aus allen AWS Regionen an Ihren S3-Bucket , wenn MULTI_REGION_CLOUD_TRAIL_ENABLED aktiviert ist. Außerdem wird beim AWS Start einer neuen Region derselbe Trail in der neuen Region erstellt. CloudTrail Dadurch erhalten Sie automatisch Protokolldateien mit API-Aktivitäten für die neue Region.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AC-2.H	AC-2.H Kontoverwaltung	cloudtrail-enabled	AWS CloudTrail kann durch die Aufzeichnung von Aktionen und API-Aufrufen in der AWS Management Console bei der Nichtabstreitbarkeit helfen. Sie können die Benutzer und die Benutzer AWS-Konten , die einen AWS Dienst aufgerufen haben, die Quell-IP-Adresse, über die die Aufrufe generiert wurden, und den Zeitpunkt der Anrufe identifizieren. Einzelheiten zu den erfassten Daten finden Sie in den AWS CloudTrail Datensatzinhalten.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AC-2.H	AC-2.H Kontoverwaltung	ec2-imdsv2-check	Stellen Sie sicher, dass die Methode Instance Metadata Service Version 2 (IMDSv2) aktiviert ist, um den Zugriff auf und die Kontrolle der Amazon Elastic Compute Cloud (Amazon EC2) - Instance-Metadaten zu schützen. Die IMDSv2 Methode verwendet sitzungsbasierte Kontrollen. Mit können Kontrollen implementiert werden IMDSv2, um Änderungen an Instanzmetadaten einzuschränken.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AC-2.H	AC-2.H Kontoverwaltung	ecs-task-definition-user-for-host-mode-check	Wenn für eine Aufgabendefinition erhöhte Berechtigungen gelten, liegt das daran, dass der Kunde diesen Konfigurationen ausdrücklich zugestimmt hat. Diese Kontrolle prüft, ob eine unerwartete Berechtigungseskalation vorliegt, wenn für eine Aufgabendefinition das Host-Netzwerk aktiviert ist, die Kunden aber keine erhöhten Berechtigungen aktiviert haben.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AC-2.H	AC-2.H Kontoverwaltung	emr-kerberos-enabled	Die Zugriffsberechtigungen und -autorisierungen können verwaltet und nach den Prinzipien der geringsten Berechtigung und Aufgabentrennung integriert werden, indem Kerberos für Amazon-EMR-Cluster aktiviert wird. In Kerberos werden Services und Benutzer, die sich authentifizieren müssen, als Prinzipale bezeichnet. Prinzipale befinden sich in einem Kerberos-Bereich. Innerhalb dieses Bereichs wird ein Kerberos-Server als Key Distribution Center (KDC) bezeichnet. Über diesen Server können sich Prinzipale authentifizieren. Die Authentifizierung im KDC erfolgt durch die Ausstellung von Authentif

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
			izierungstickets. Das KDC unterhält eine Datenbank der Prinzipale in seinem Bereich mit ihren Passwörtern und anderen administr ativen Informationen zu jedem Prinzipal.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AC-2.H	AC-2.H Kontoverwaltung	iam-customer-policy-blocked-kms-Aktionen	AWS Identity and Access Management (IAM) kann Ihnen helfen, die Prinzipien der geringsten Rechte und der Aufgabentrennung in Zugriffsberechtigungen und Autorisierungen zu integrieren und so zu verhindern, dass Richtlinien blockierte Aktionen für alle AWS Schlüssel des Key Management Service enthalten. Wenn Benutzer mehr Rechte haben, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und Aufgabentrennung verstoßen. Mit dieser Regel können Sie den Parameter festlegen. blockedActionsPatterns (Wert „AWS Bewährte grundlegende Sicherheitsmethode

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
			n“: kms: Entschlüs seln, kms:ReEnc ryptFrom). Die tatsächlichen Werte müssen den Richtlini en Ihrer Organisation entsprechen.
CCCS-fPBMM-AC-2.H	AC-2.H Kontoverw altung	iam-group-has-users-überprüfen	AWS Identity and Access Managemen t (IAM) kann Ihnen helfen, die Prinzipien der geringsten Rechte und der Aufgabent rennung mit Zugriffsb erechtigungen und Autorisierungen zu integrieren, indem sichergestellt wird, dass IAM-Gruppen mindestens einen Benutzer haben. Die Einteilung von Benutzern in Gruppen auf der Grundlage der ihnen zugewiese nen Berechtigungen oder ihrer Funktion ist eine Möglichkeit, das Prinzip der geringste n Berechtigung zu implementieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AC-2.H	AC-2.H Kontoverwaltung	iam-inline-policy-blocked-kms-Aktionen	Stellen Sie sicher, dass ein Benutzer, eine IAM-Rolle oder eine IAM-Gruppe (AWS Identity and Access Management) nicht über eine Inline-Richtlinie verfügt, die blockierte Aktionen für alle AWS Schlüssel des Key Management Service zulässt. AWS empfiehlt, verwaltete Richtlinien anstelle von Inline-Richtlinien zu verwenden. Verwaltete Richtlinien ermöglichen Wiederverwendbarkeit, Versionsverwaltung, Rollback und Delegierung der Berechtigungsverwaltung. Mit dieser Regel können Sie den blockedActionsPatterns Parameter festlegen. (Wert „AWS Bewährte grundlegende Sicherheitsmethoden“: kms: Entschlüsseln, kms:ReEnc

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
			ryptFrom). Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.
CCCS-fPBMM-AC-2.H	AC-2.H Kontoverwaltung	iam-no-inline-policy-überprüfen	Stellen Sie sicher, dass ein Benutzer, eine IAM-Rolle oder eine IAM-Gruppe (AWS Identity and Access Management) nicht über eine Inline-Richtlinie zur Zugriffskontrolle auf Systeme und Ressourcen verfügt. AWS empfiehlt, verwaltete Richtlinien anstelle von Inline-Richtlinien zu verwenden. Verwaltete Richtlinien ermöglichen Wiederverwendbarkeit, Versionsverwaltung, Rollback und Delegierung der Berechtigungsverwaltung.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AC-2.H	AC-2.H Kontoverwaltung	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) kann Ihnen dabei helfen, die Prinzipien der geringsten Rechte und der Aufgabentrennung in Zugriffsberechtigungen und Autorisierungen zu integrieren und so zu verhindern, dass Richtlinien „Effect“: „Allow“ mit „Action“: „*“ anstelle von „Resource“: „*“ enthalten. Wenn Benutzern mehr Rechte eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und der Aufgabentrennung verstoßen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AC-2.H	AC-2.H Kontoverwaltung	iam-policy-no-statements-with-full-access	Stellen Sie sicher, dass IAM-Aktionen nur auf die benötigten Aktionen beschränkt sind. Wenn Benutzern mehr Rechte eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und der Aufgabentrennung verstoßen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AC-2.H	AC-2.H Kontoverwaltung	iam-root-access-key-überprüfen	Der Zugriff auf Systeme und Ressourcen kann gesteuert werden, indem überprüft wird, ob der Root-Benutzer keine Zugriffsschlüssel mit seiner AWS Identity and Access Management (IAM) -Rolle verknüpft hat. Stellen Sie sicher, dass die Root-Zugriffsschlüssel gelöscht werden. Erstellen und verwenden Sie stattdessen rollenbasierte Funktionen, AWS-Konten um das Prinzip der geringsten Funktionalität zu berücksichtigen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AC-2.H	AC-2.H Kontoverwaltung	iam-user-group-membership-überprüfen	AWS Identity and Access Management (IAM) kann Ihnen helfen, Zugriffsberechtigungen und Autorisierungen einzuschränken, indem sichergestellt wird, dass Benutzer Mitglieder mindestens einer Gruppe sind. Wenn Benutzern mehr Berechtigungen eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und Aufgabentrennung verstoßen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AC-2.H	AC-2.H Kontoverwaltung	iam-user-no-policies-überprüfen	Diese Regel stellt sicher, dass AWS Identity and Access Management (IAM) -Richtlinien nur Gruppen oder Rollen zugewiesen werden, um den Zugriff auf Systeme und Ressourcen zu kontrollieren. Die Zuweisung von Berechtigungen auf Gruppen- oder Rollenebene trägt dazu bei, die Wahrscheinlichkeit zu verringern, dass eine Identität übermäßige Berechtigungen erhält oder beibehält.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AC-2.H	AC-2.H Kontoverwaltung	iam-user-unused-credentials-überprüfen	AWS Identity and Access Management (IAM) kann Ihnen bei Zugriffsberechtigungen und Autorisierungen helfen, indem es nach IAM-Passwörtern und Zugriffsschlüsseln sucht, die für einen bestimmten Zeitraum nicht verwendet wurden. Wenn ungenutzte Anmeldeinformationen identifiziert werden, müssen Sie sie deaktivieren und/oder entfernen, da dies gegen das Prinzip der geringsten Berechtigung verstoßen könnte. Für diese Regel müssen Sie einen Wert für das maxCredentialUsage Alter festlegen (Standardkonfiguration: 90). Der tatsächliche Wert muss den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AC-2.H	AC-2.H Kontoverwaltung	multi-region-cloudtrail-enabled	AWS CloudTrail zeichnet Aktionen und API-Aufrufe der AWS Management Console auf. Sie können feststellen, welche Benutzer und Konten angerufen wurden AWS, von welcher Quell-IP-Adresse aus die Anrufe getätigt wurden und wann die Anrufe erfolgten. CloudTrail übermittelt Protokolldateien aus allen AWS Regionen an Ihren S3-Bucket , wenn MULTI_REGION_CLOUD_TRAIL_ENABLED aktiviert ist. Außerdem wird beim AWS Start einer neuen Region derselbe Trail in der neuen Region erstellt. CloudTrail Dadurch erhalten Sie automatisch Protokolldateien mit API-Aktivitäten für die neue Region.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AC-2.I	AC-2.I Kontoverwaltung	cloudtrail-enabled	AWS CloudTrail kann durch die Aufzeichnung von Aktionen und API-Aufrufen in der AWS Management Console bei der Nichtabstreitbarkeit helfen. Sie können die Benutzer und die Benutzer AWS-Konten , die einen AWS Dienst aufgerufen haben, die Quell-IP-Adresse, über die die Aufrufe generiert wurden, und den Zeitpunkt der Anrufe identifizieren. Einzelheiten zu den erfassten Daten finden Sie in den AWS CloudTrail Datensatzinhalten.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AC-2.I	AC-2.I Kontoverwaltung	ec2-imdsv2-check	Stellen Sie sicher, dass die Methode Instance Metadata Service Version 2 (IMDSv2) aktiviert ist, um den Zugriff auf und die Kontrolle der Amazon Elastic Compute Cloud (Amazon EC2) - Instance-Metadaten zu schützen. Die IMDSv2 Methode verwendet sitzungsbasierte Kontrollen. Mit können Kontrollen implementiert werden IMDSv2, um Änderungen an Instanzmetadaten einzuschränken.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AC-2.I	AC-2.I Kontoverwaltung	ecs-task-definition-user-for-host-mode-check	Wenn für eine Aufgabendefinition erhöhte Berechtigungen gelten, liegt das daran, dass der Kunde diesen Konfigurationen ausdrücklich zugestimmt hat. Diese Kontrolle prüft, ob eine unerwartete Berechtigungseskalation vorliegt, wenn für eine Aufgabendefinition das Host-Netzwerk aktiviert ist, die Kunden aber keine erhöhten Berechtigungen aktiviert haben.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AC-2.I	AC-2.I Kontoverwaltung	emr-kerberos-enabled	Die Zugriffsberechtigungen und -autorisierungen können verwaltet und nach den Prinzipien der geringsten Berechtigung und Aufgabentrennung integriert werden, indem Kerberos für Amazon-EMR-Cluster aktiviert wird. In Kerberos werden Services und Benutzer, die sich authentifizieren müssen, als Prinzipale bezeichnet. Prinzipale befinden sich in einem Kerberos-Bereich. Innerhalb dieses Bereichs wird ein Kerberos-Server als Key Distribution Center (KDC) bezeichnet. Über diesen Server können sich Prinzipale authentifizieren. Die Authentifizierung im KDC erfolgt durch die Ausstellung von Authentif

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
			izierungstickets. Das KDC unterhält eine Datenbank der Prinzipale in seinem Bereich mit ihren Passwörtern und anderen administr ativen Informationen zu jedem Prinzipal.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AC-2.I	AC-2.I Kontoverwaltung	iam-customer-policy-blocked-kms-Aktionen	AWS Identity and Access Management (IAM) kann Ihnen helfen, die Prinzipien der geringsten Rechte und der Aufgabentrennung in Zugriffsberechtigungen und Autorisierungen zu integrieren und so zu verhindern, dass Richtlinien blockierte Aktionen für alle AWS Schlüssel des Key Management Service enthalten. Wenn Benutzer mehr Rechte haben, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und Aufgabentrennung verstoßen. Mit dieser Regel können Sie den Parameter festlegen. blockedActionsPatterns (Wert „AWS Bewährte grundlegende Sicherheitsmethode

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
			n“: kms: Entschlüs seln, kms:ReEnc ryptFrom). Die tatsächlichen Werte müssen den Richtlini en Ihrer Organisation entsprechen.
CCCS-fPBMM-AC-2.I	AC-2.I Kontoverw altung	iam-group-has-users-überprüfen	AWS Identity and Access Managemen t (IAM) kann Ihnen helfen, die Prinzipien der geringsten Rechte und der Aufgabent rennung mit Zugriffsb erechtigungen und Autorisierungen zu integrieren, indem sichergestellt wird, dass IAM-Gruppen mindestens einen Benutzer haben. Die Einteilung von Benutzern in Gruppen auf der Grundlage der ihnen zugewiese nen Berechtigungen oder ihrer Funktion ist eine Möglichkeit, das Prinzip der geringste n Berechtigung zu implementieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AC-2.I	AC-2.I Kontoverwaltung	iam-inline-policy-blocked-kms-Aktionen	Stellen Sie sicher, dass ein Benutzer, eine IAM-Rolle oder eine IAM-Gruppe (AWS Identity and Access Management) nicht über eine Inline-Richtlinie verfügt, die blockierte Aktionen für alle AWS Schlüssel des Key Management Service zulässt. AWS empfiehlt, verwaltete Richtlinien anstelle von Inline-Richtlinien zu verwenden. Verwaltete Richtlinien ermöglichen Wiederverwendbarkeit, Versionsverwaltung, Rollback und Delegierung der Berechtigungsverwaltung. Mit dieser Regel können Sie den blockedActionsPatterns Parameter festlegen. (Wert „AWS Bewährte grundlegende Sicherheitsmethoden“: kms: Entschlüsseln, kms:ReEnc

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
			ryptFrom). Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.
CCCS-fPBMM-AC-2.I	AC-2.I Kontoverwaltung	iam-no-inline-policy-überprüfen	Stellen Sie sicher, dass ein Benutzer, eine IAM-Rolle oder eine IAM-Gruppe (AWS Identity and Access Management) nicht über eine Inline-Richtlinie zur Zugriffskontrolle auf Systeme und Ressourcen verfügt. AWS empfiehlt, verwaltete Richtlinien anstelle von Inline-Richtlinien zu verwenden. Verwaltete Richtlinien ermöglichen Wiederverwendbarkeit, Versionsverwaltung, Rollback und Delegierung der Berechtigungsverwaltung.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AC-2.I	AC-2.I Kontoverwaltung	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) kann Ihnen dabei helfen, die Prinzipien der geringsten Rechte und der Aufgabentrennung in Zugriffsberechtigungen und Autorisierungen zu integrieren und so zu verhindern, dass Richtlinien „Effect“: „Allow“ mit „Action“: „*“ anstelle von „Resource“: „*“ enthalten. Wenn Benutzern mehr Rechte eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und der Aufgabentrennung verstoßen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AC-2.I	AC-2.I Kontoverwaltung	iam-policy-no-statements-with-full-access	Stellen Sie sicher, dass IAM-Aktionen nur auf die benötigten Aktionen beschränkt sind. Wenn Benutzern mehr Rechte eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und der Aufgabentrennung verstoßen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AC-2.I	AC-2.I Kontoverwaltung	iam-root-access-key-überprüfen	Der Zugriff auf Systeme und Ressourcen kann gesteuert werden, indem überprüft wird, ob der Root-Benutzer keine Zugriffsschlüssel mit seiner AWS Identity and Access Management (IAM) -Rolle verknüpft hat. Stellen Sie sicher, dass die Root-Zugriffsschlüssel gelöscht werden. Erstellen und verwenden Sie stattdessen rollenbasierte Funktionen, AWS-Konten um das Prinzip der geringsten Funktionalität zu berücksichtigen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AC-2.I	AC-2.I Kontoverwaltung	iam-user-group-membership-überprüfen	AWS Identity and Access Management (IAM) kann Ihnen helfen, Zugriffsberechtigungen und Autorisierungen einzuschränken, indem sichergestellt wird, dass Benutzer Mitglieder mindestens einer Gruppe sind. Wenn Benutzern mehr Berechtigungen eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und Aufgabentrennung verstoßen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AC-2.I	AC-2.I Kontoverwaltung	iam-user-no-policies-überprüfen	Diese Regel stellt sicher, dass AWS Identity and Access Management (IAM) -Richtlinien nur Gruppen oder Rollen zugewiesen werden, um den Zugriff auf Systeme und Ressourcen zu kontrollieren. Die Zuweisung von Berechtigungen auf Gruppen- oder Rollenebene trägt dazu bei, die Wahrscheinlichkeit zu verringern, dass eine Identität übermäßige Berechtigungen erhält oder beibehält.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AC-2.I	AC-2.I Kontoverwaltung	iam-user-unused-credentials-überprüfen	AWS Identity and Access Management (IAM) kann Ihnen bei Zugriffsberechtigungen und Autorisierungen helfen, indem es nach IAM-Passwörtern und Zugriffsschlüsseln sucht, die für einen bestimmten Zeitraum nicht verwendet wurden. Wenn ungenutzte Anmeldeinformationen identifiziert werden, müssen Sie sie deaktivieren und/oder entfernen, da dies gegen das Prinzip der geringsten Berechtigung verstoßen könnte. Für diese Regel müssen Sie einen Wert für das maxCredentialUsage Alter festlegen (Standardkonfiguration: 90). Der tatsächliche Wert muss den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AC-2.I	AC-2.I Kontoverwaltung	multi-region-cloudtrail-enabled	AWS CloudTrail zeichnet Aktionen und API-Aufrufe der AWS Management Console auf. Sie können feststellen, welche Benutzer und Konten angerufen wurden AWS, von welcher Quell-IP-Adresse aus die Anrufe getätigt wurden und wann die Anrufe erfolgten. CloudTrail übermittelt Protokolldateien aus allen AWS Regionen an Ihren S3-Bucket , wenn MULTI_REGION_CLOUD_TRAIL_ENABLED aktiviert ist. Außerdem wird beim AWS Start einer neuen Region derselbe Trail in der neuen Region erstellt. CloudTrail Dadurch erhalten Sie automatisch Protokolldateien mit API-Aktivitäten für die neue Region.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AC-2.J	AC-2.J Kontoverwaltung	cloudtrail-enabled	AWS CloudTrail kann durch die Aufzeichnung von Aktionen und API-Aufrufen in der AWS Management Console bei der Nichtabstreitbarkeit helfen. Sie können die Benutzer und die Benutzer AWS-Konten , die einen AWS Dienst aufgerufen haben, die Quell-IP-Adresse, über die die Aufrufe generiert wurden, und den Zeitpunkt der Anrufe identifizieren. Einzelheiten zu den erfassten Daten finden Sie in den AWS CloudTrail Datensatzinhalten.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AC-2.J	AC-2.J Kontoverwaltung	ec2-imdsv2-check	Stellen Sie sicher, dass die Methode Instance Metadata Service Version 2 (IMDSv2) aktiviert ist, um den Zugriff auf und die Kontrolle der Amazon Elastic Compute Cloud (Amazon EC2) - Instance-Metadaten zu schützen. Die IMDSv2 Methode verwendet sitzungsbasierte Kontrollen. Mit können Kontrollen implementiert werden IMDSv2, um Änderungen an Instanzmetadaten einzuschränken.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AC-2.J	AC-2.J Kontoverwaltung	ecs-task-definition-user-for-host-mode-check	Wenn für eine Aufgabendefinition erhöhte Berechtigungen gelten, liegt das daran, dass der Kunde diesen Konfigurationen ausdrücklich zugestimmt hat. Diese Kontrolle prüft, ob eine unerwartete Berechtigungseskalation vorliegt, wenn für eine Aufgabendefinition das Host-Netzwerk aktiviert ist, die Kunden aber keine erhöhten Berechtigungen aktiviert haben.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AC-2.J	AC-2.J Kontoverwaltung	emr-kerberos-enabled	Die Zugriffsberechtigungen und -autorisierungen können verwaltet und nach den Prinzipien der geringsten Berechtigung und Aufgabentrennung integriert werden, indem Kerberos für Amazon-EMR-Cluster aktiviert wird. In Kerberos werden Services und Benutzer, die sich authentifizieren müssen, als Prinzipale bezeichnet. Prinzipale befinden sich in einem Kerberos-Bereich. Innerhalb dieses Bereichs wird ein Kerberos-Server als Key Distribution Center (KDC) bezeichnet. Über diesen Server können sich Prinzipale authentifizieren. Die Authentifizierung im KDC erfolgt durch die Ausstellung von Authentif

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
			izierungstickets. Das KDC unterhält eine Datenbank der Prinzipale in seinem Bereich mit ihren Passwörtern und anderen administr ativen Informationen zu jedem Prinzipal.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AC-2.J	AC-2.J Kontoverwaltung	iam-customer-policy-blocked-kms-Aktionen	AWS Identity and Access Management (IAM) kann Ihnen helfen, die Prinzipien der geringsten Rechte und der Aufgabentrennung in Zugriffsberechtigungen und Autorisierungen zu integrieren und so zu verhindern, dass Richtlinien blockierte Aktionen für alle AWS Schlüssel des Key Management Service enthalten. Wenn Benutzer mehr Rechte haben, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und Aufgabentrennung verstoßen. Mit dieser Regel können Sie den Parameter festlegen. blockedActionsPatterns (Wert „AWS Bewährte grundlegende Sicherheitsmethode

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
			n“: kms: Entschlüs seln, kms:ReEnc ryptFrom). Die tatsächlichen Werte müssen den Richtlini en Ihrer Organisation entsprechen.
CCCS-fPBMM-AC-2.J	AC-2.J Kontoverw altung	iam-group-has-users-überprüfen	AWS Identity and Access Managemen t (IAM) kann Ihnen helfen, die Prinzipien der geringsten Rechte und der Aufgabent rennung mit Zugriffsb erechtigungen und Autorisierungen zu integrieren, indem sichergestellt wird, dass IAM-Gruppen mindestens einen Benutzer haben. Die Einteilung von Benutzern in Gruppen auf der Grundlage der ihnen zugewiese nen Berechtigungen oder ihrer Funktion ist eine Möglichkeit, das Prinzip der geringste n Berechtigung zu implementieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AC-2.J	AC-2.J Kontoverwaltung	iam-inline-policy-blocked-kms-Aktionen	Stellen Sie sicher, dass ein Benutzer, eine IAM-Rolle oder eine IAM-Gruppe (AWS Identity and Access Management) nicht über eine Inline-Richtlinie verfügt, die blockierte Aktionen für alle AWS Schlüssel des Key Management Service zulässt. AWS empfiehlt, verwaltete Richtlinien anstelle von Inline-Richtlinien zu verwenden. Verwaltete Richtlinien ermöglichen Wiederverwendbarkeit, Versionsverwaltung, Rollback und Delegierung der Berechtigungsverwaltung. Mit dieser Regel können Sie den blockedActionsPatterns Parameter festlegen. (Wert „AWS Bewährte grundlegende Sicherheitsmethoden“: kms: Entschlüsseln, kms:ReEnc

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
			ryptFrom). Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.
CCCS-fPBMM-AC-2.J	AC-2.J Kontoverwaltung	iam-no-inline-policy-überprüfen	Stellen Sie sicher, dass ein Benutzer, eine IAM-Rolle oder eine IAM-Gruppe (AWS Identity and Access Management) nicht über eine Inline-Richtlinie zur Zugriffskontrolle auf Systeme und Ressourcen verfügt. AWS empfiehlt, verwaltete Richtlinien anstelle von Inline-Richtlinien zu verwenden. Verwaltete Richtlinien ermöglichen Wiederverwendbarkeit, Versionsverwaltung, Rollback und Delegierung der Berechtigungsverwaltung.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AC-2.J	AC-2.J Kontoverwaltung	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) kann Ihnen dabei helfen, die Prinzipien der geringsten Rechte und der Aufgabentrennung in Zugriffsberechtigungen und Autorisierungen zu integrieren und so zu verhindern, dass Richtlinien „Effect“: „Allow“ mit „Action“: „*“ anstelle von „Resource“: „*“ enthalten. Wenn Benutzern mehr Rechte eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und der Aufgabentrennung verstoßen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AC-2.J	AC-2.J Kontoverwaltung	iam-policy-no-statements-with-full-access	Stellen Sie sicher, dass IAM-Aktionen nur auf die benötigten Aktionen beschränkt sind. Wenn Benutzern mehr Rechte eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und der Aufgabentrennung verstoßen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AC-2.J	AC-2.J Kontoverwaltung	iam-root-access-key-überprüfen	Der Zugriff auf Systeme und Ressourcen kann gesteuert werden, indem überprüft wird, ob der Root-Benutzer keine Zugriffsschlüssel mit seiner AWS Identity and Access Management (IAM) -Rolle verknüpft hat. Stellen Sie sicher, dass die Root-Zugriffsschlüssel gelöscht werden. Erstellen und verwenden Sie stattdessen rollenbasierte Funktionen, AWS-Konten um das Prinzip der geringsten Funktionalität zu berücksichtigen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AC-2.J	AC-2.J Kontoverwaltung	iam-user-group-membership-überprüfen	AWS Identity and Access Management (IAM) kann Ihnen helfen, Zugriffsberechtigungen und Autorisierungen einzuschränken, indem sichergestellt wird, dass Benutzer Mitglieder mindestens einer Gruppe sind. Wenn Benutzern mehr Berechtigungen eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und Aufgabentrennung verstoßen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AC-2.J	AC-2.J Kontoverwaltung	iam-user-no-policies-überprüfen	Diese Regel stellt sicher, dass AWS Identity and Access Management (IAM) -Richtlinien nur Gruppen oder Rollen zugewiesen werden, um den Zugriff auf Systeme und Ressourcen zu kontrollieren. Die Zuweisung von Berechtigungen auf Gruppen- oder Rollenebene trägt dazu bei, die Wahrscheinlichkeit zu verringern, dass eine Identität übermäßige Berechtigungen erhält oder beibehält.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AC-2.J	AC-2.J Kontoverwaltung	iam-user-unused-credentials-überprüfen	AWS Identity and Access Management (IAM) kann Ihnen bei Zugriffsberechtigungen und Autorisierungen helfen, indem es nach IAM-Passwörtern und Zugriffsschlüsseln sucht, die für einen bestimmten Zeitraum nicht verwendet wurden. Wenn ungenutzte Anmeldeinformationen identifiziert werden, müssen Sie sie deaktivieren und/oder entfernen, da dies gegen das Prinzip der geringsten Berechtigung verstoßen könnte. Für diese Regel müssen Sie einen Wert für das maxCredentialUsage Alter festlegen (Standardkonfiguration: 90). Der tatsächliche Wert muss den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AC-2.J	AC-2.J Kontoverwaltung	multi-region-cloudtrail-enabled	AWS CloudTrail zeichnet Aktionen und API-Aufrufe der AWS Management Console auf. Sie können feststellen, welche Benutzer und Konten angerufen wurden AWS, von welcher Quell-IP-Adresse aus die Anrufe getätigt wurden und wann die Anrufe erfolgten. CloudTrail übermittelt Protokolldateien aus allen AWS Regionen an Ihren S3-Bucket , wenn MULTI_REGION_CLOUD_TRAIL_ENABLED aktiviert ist. Außerdem wird beim AWS Start einer neuen Region derselbe Trail in der neuen Region erstellt. CloudTrail Dadurch erhalten Sie automatisch Protokolldateien mit API-Aktivitäten für die neue Region.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AC-2.K	AC-2.K Kontoverwaltung	cloudtrail-enabled	AWS CloudTrail kann durch die Aufzeichnung von Aktionen und API-Aufrufen in der AWS Management Console bei der Nichtabstreitbarkeit helfen. Sie können die Benutzer und die Benutzer AWS-Konten , die einen AWS Dienst aufgerufen haben, die Quell-IP-Adresse, über die die Aufrufe generiert wurden, und den Zeitpunkt der Anrufe identifizieren. Einzelheiten zu den erfassten Daten finden Sie unter Inhalt des AWS CloudTrail Datensatzes.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AC-2.K	AC-2.K Kontoverwaltung	ec2-imdsv2-check	Stellen Sie sicher, dass die Methode Instance Metadata Service Version 2 (IMDSv2) aktiviert ist, um den Zugriff auf und die Kontrolle der Amazon Elastic Compute Cloud (Amazon EC2) - Instance-Metadaten zu schützen. Die IMDSv2 Methode verwendet sitzungsbasierte Kontrollen. Mit können Kontrollen implementiert werden IMDSv2, um Änderungen an Instanzmetadaten einzuschränken.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AC-2.K	AC-2.K Kontoverwaltung	ecs-task-definition-user-for-host-mode-check	Wenn für eine Aufgabendefinition erhöhte Berechtigungen gelten, liegt das daran, dass der Kunde diesen Konfigurationen ausdrücklich zugestimmt hat. Diese Kontrolle prüft, ob eine unerwartete Berechtigungseskalation vorliegt, wenn für eine Aufgabendefinition das Host-Netzwerk aktiviert ist, die Kunden aber keine erhöhten Berechtigungen aktiviert haben.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AC-2.K	AC-2.K Kontoverwaltung	emr-kerberos-enabled	Die Zugriffsberechtigungen und -autorisierungen können verwaltet und nach den Prinzipien der geringsten Berechtigung und Aufgabentrennung integriert werden, indem Kerberos für Amazon-EMR-Cluster aktiviert wird. In Kerberos werden Services und Benutzer, die sich authentifizieren müssen, als Prinzipale bezeichnet. Prinzipale befinden sich in einem Kerberos-Bereich. Innerhalb dieses Bereichs wird ein Kerberos-Server als Key Distribution Center (KDC) bezeichnet. Über diesen Server können sich Prinzipale authentifizieren. Die Authentifizierung im KDC erfolgt durch die Ausstellung von Authentif

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
			izierungstickets. Das KDC unterhält eine Datenbank der Prinzipale in seinem Bereich mit ihren Passwörtern und anderen administr ativen Informationen zu jedem Prinzipal.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AC-2.K	AC-2.K Kontoverwaltung	iam-customer-policy-blocked-kms-Aktionen	AWS Identity and Access Management (IAM) kann Ihnen helfen, die Prinzipien der geringsten Rechte und der Aufgabentrennung in Zugriffsberechtigungen und Autorisierungen zu integrieren und so zu verhindern, dass Richtlinien blockierte Aktionen für alle AWS Schlüssel des Key Management Service enthalten. Wenn Benutzer mehr Rechte haben, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und Aufgabentrennung verstoßen. Mit dieser Regel können Sie den Parameter festlegen. blockedActionsPatterns (Wert „AWS Bewährte grundlegende Sicherheitsmethode

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
			n“: kms: Entschlüs seln, kms:ReEnc ryptFrom). Die tatsächlichen Werte müssen den Richtlini en Ihrer Organisation entsprechen.
CCCS-fPBMM-AC-2.K	AC-2.K Kontoverw altung	iam-group-has-users-überprüfen	AWS Identity and Access Managemen t (IAM) kann Ihnen helfen, die Prinzipien der geringsten Rechte und der Aufgabent rennung mit Zugriffsb erechtigungen und Autorisierungen zu integrieren, indem sichergestellt wird, dass IAM-Gruppen mindestens einen Benutzer haben. Die Einteilung von Benutzern in Gruppen auf der Grundlage der ihnen zugewiese nen Berechtigungen oder ihrer Funktion ist eine Möglichkeit, das Prinzip der geringste n Berechtigung zu implementieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AC-2.K	AC-2.K Kontoverwaltung	iam-inline-policy-blocked-kms-Aktionen	Stellen Sie sicher, dass ein Benutzer, eine IAM-Rolle oder eine IAM-Gruppe (AWS Identity and Access Management) nicht über eine Inline-Richtlinie verfügt, die blockierte Aktionen für alle AWS Schlüssel des Key Management Service zulässt. AWS empfiehlt, verwaltete Richtlinien anstelle von Inline-Richtlinien zu verwenden. Verwaltete Richtlinien ermöglichen Wiederverwendbarkeit, Versionsverwaltung, Rollback und Delegierung der Berechtigungsverwaltung. Mit dieser Regel können Sie den blockedActionsPatterns Parameter festlegen. (Wert „AWS Bewährte grundlegende Sicherheitsmethoden“: kms: Entschlüsseln, kms:ReEnc

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
			ryptFrom). Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.
CCCS-fPBMM-AC-2.K	AC-2.K Kontoverwaltung	iam-no-inline-policy-überprüfen	Stellen Sie sicher, dass ein Benutzer, eine IAM-Rolle oder eine IAM-Gruppe (AWS Identity and Access Management) nicht über eine Inline-Richtlinie zur Zugriffskontrolle auf Systeme und Ressourcen verfügt. AWS empfiehlt, verwaltete Richtlinien anstelle von Inline-Richtlinien zu verwenden. Verwaltete Richtlinien ermöglichen Wiederverwendbarkeit, Versionsverwaltung, Rollback und Delegierung der Berechtigungsverwaltung.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AC-2.K	AC-2.K Kontoverwaltung	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) kann Ihnen dabei helfen, die Prinzipien der geringsten Rechte und der Aufgabentrennung in Zugriffsberechtigungen und Autorisierungen zu integrieren und so zu verhindern, dass Richtlinien „Effect“: „Allow“ mit „Action“: „*“ anstelle von „Resource“: „*“ enthalten. Wenn Benutzern mehr Rechte eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und der Aufgabentrennung verstoßen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AC-2.K	AC-2.K Kontoverwaltung	iam-policy-no-statements-with-full-access	Stellen Sie sicher, dass IAM-Aktionen nur auf die benötigten Aktionen beschränkt sind. Wenn Benutzern mehr Rechte eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und der Aufgabentrennung verstoßen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AC-2.K	AC-2.K Kontoverwaltung	iam-root-access-key-überprüfen	Der Zugriff auf Systeme und Ressourcen kann gesteuert werden, indem überprüft wird, ob der Root-Benutzer keine Zugriffsschlüssel mit seiner AWS Identity and Access Management (IAM) -Rolle verknüpft hat. Stellen Sie sicher, dass die Root-Zugriffsschlüssel gelöscht werden. Erstellen und verwenden Sie stattdessen rollenbasierte Funktionen, AWS-Konten um das Prinzip der geringsten Funktionalität zu berücksichtigen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AC-2.K	AC-2.K Kontoverwaltung	iam-user-group-membership-überprüfen	AWS Identity and Access Management (IAM) kann Ihnen helfen, Zugriffsberechtigungen und Autorisierungen einzuschränken, indem sichergestellt wird, dass Benutzer Mitglieder mindestens einer Gruppe sind. Wenn Benutzern mehr Berechtigungen eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und Aufgabentrennung verstoßen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AC-2.K	AC-2.K Kontoverwaltung	iam-user-no-policies-überprüfen	Diese Regel stellt sicher, dass AWS Identity and Access Management (IAM) -Richtlinien nur Gruppen oder Rollen zugewiesen werden, um den Zugriff auf Systeme und Ressourcen zu kontrollieren. Die Zuweisung von Berechtigungen auf Gruppen- oder Rollenebene trägt dazu bei, die Wahrscheinlichkeit zu verringern, dass eine Identität übermäßige Berechtigungen erhält oder beibehält.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AC-2.K	AC-2.K Kontoverwaltung	iam-user-unused-credentials-überprüfen	AWS Identity and Access Management (IAM) kann Ihnen bei Zugriffsberechtigungen und Autorisierungen helfen, indem es nach IAM-Passwörtern und Zugriffsschlüsseln sucht, die für einen bestimmten Zeitraum nicht verwendet wurden. Wenn ungenutzte Anmeldeinformationen identifiziert werden, müssen Sie sie deaktivieren und/oder entfernen, da dies gegen das Prinzip der geringsten Berechtigung verstoßen könnte. Für diese Regel müssen Sie einen Wert für das maxCredentialUsage Alter festlegen (Standardkonfiguration: 90). Der tatsächliche Wert muss den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AC-2.K	AC-2.K Kontoverwaltung	multi-region-cloudtrail-enabled	AWS CloudTrail zeichnet Aktionen und API-Aufrufe der AWS Management Console auf. Sie können feststellen, welche Benutzer und Konten angerufen wurden AWS, von welcher Quell-IP-Adresse aus die Anrufe getätigt wurden und wann die Anrufe erfolgten. CloudTrail übermittelt Protokolldateien aus allen AWS Regionen an Ihren S3-Bucket , wenn MULTI_REGION_CLOUD_TRAIL_ENABLED aktiviert ist. Außerdem wird beim AWS Start einer neuen Region derselbe Trail in der neuen Region erstellt. CloudTrail Dadurch erhalten Sie automatisch Protokolldateien mit API-Aktivitäten für die neue Region.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AC-3.A	AC-3.A Durchsetzung des Zugriffs	dms-replication-not-public	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass auf DMS-Replikationsinstanzen nicht öffentlich zugegriffen werden kann. DMS-Replikations-Instances können vertrauliche Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.
CCCS-fPBMM-AC-3.A	AC-3.A Durchsetzung des Zugriffs	ebs-snapshot-public-restorable-überprüfen	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass EBS-Snapshots nicht öffentlich wiederherstellbar sind. EBS-Volume-Snapshots können vertrauliche Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AC-3.A	AC-3.A Durchsetzung des Zugriffs	ec2-imdsv2-check	Stellen Sie sicher, dass die Methode Instance Metadata Service Version 2 (IMDSv2) aktiviert ist, um den Zugriff auf und die Kontrolle der Amazon Elastic Compute Cloud (Amazon EC2) - Instance-Metadaten zu schützen. Die IMDSv2 Methode verwendet sitzungsbasierte Kontrollen. Mit können Kontrollen implementiert werden IMDSv2, um Änderungen an Instanzmetadaten einzuschränken.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AC-3.A	AC-3.A Durchsetzung des Zugriffs	ec-2 instance-no-public-ip	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon Elastic Compute Cloud (Amazon EC2) - Instances nicht öffentlich zugänglic h sind. EC2Amazon -Instances können vertrauliche Informati onen enthalten, und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AC-3.A	AC-3.A Durchsetzung des Zugriffs	ecs-task-definition-user-for-host-mode-check	Wenn für eine Aufgabendefinition erhöhte Berechtigungen gelten, liegt das daran, dass der Kunde diesen Konfigurationen ausdrücklich zugestimmt hat. Diese Kontrolle prüft, ob eine unerwartete Berechtigungseskalation vorliegt, wenn für eine Aufgabendefinition das Host-Netzwerk aktiviert ist, die Kunden aber keine erhöhten Berechtigungen aktiviert haben.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AC-3.A	AC-3.A Durchsetzung des Zugriffs	elasticsearch-in-vpc-only	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass sich Amazon OpenSearch OpenSearch Service (Service) - Domains innerhalb einer Amazon Virtual Private Cloud (Amazon VPC) befinden. Eine OpenSearch Service-Domain innerhalb einer Amazon VPC ermöglicht die sichere Kommunikation zwischen OpenSearch Service und anderen Services innerhalb der Amazon VPC, ohne dass ein Internet-Gateway, ein NAT-Gerät oder eine VPN-Verbindung erforderlich ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AC-3.A	AC-3.A Durchsetzung des Zugriffs	emr-kerberos-enabled	Die Zugriffsberechtigungen und -autorisierungen können verwaltet und nach den Prinzipien der geringsten Berechtigung und Aufgabentrennung integriert werden, indem Kerberos für Amazon-EMR-Cluster aktiviert wird. In Kerberos werden Services und Benutzer, die sich authentifizieren müssen, als Prinzipale bezeichnet. Prinzipale befinden sich in einem Kerberos-Bereich. Innerhalb dieses Bereichs wird ein Kerberos-Server als Key Distribution Center (KDC) bezeichnet. Über diesen Server können sich Prinzipale authentifizieren. Die Authentifizierung im KDC erfolgt durch die Ausstellung von Authentif

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
			izierungstickets. Das KDC unterhält eine Datenbank der Prinzipale in seinem Bereich mit ihren Passwörtern und anderen administrativen Informationen zu jedem Prinzipal.
CCCS-fPBMM-AC-3.A	AC-3.A Durchsetzung des Zugriffs	emr-master-no-public-ip	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon EMR-Cluster-Masterknoten nicht öffentlich zugänglich sind. Amazon-EMR-Cluster-Hauptknoten können vertrauliche Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AC-3.A	AC-3.A Durchsetzung des Zugriffs	iam-customer-policy-blocked-kms-Aktionen	AWS Identity and Access Management (IAM) kann Ihnen helfen, die Prinzipien der geringsten Rechte und der Aufgabentrennung in Zugriffsberechtigungen und Autorisierungen zu integrieren und so zu verhindern, dass Richtlinien blockierte Aktionen für alle AWS Schlüssel des Key Management Service enthalten. Wenn Benutzer mehr Rechte haben, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und Aufgabentrennung verstoßen. Mit dieser Regel können Sie den Parameter festlegen. blockedActionsPatterns (Wert „AWS Bewährte grundlegende Sicherheitsmethode

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
			n“: kms: Entschlüs seln, kms:ReEnc ryptFrom). Die tatsächlichen Werte müssen den Richtlini en Ihrer Organisation entsprechen.
CCCS-fPBMM-AC-3.A	AC-3.A Durchsetzung des Zugriffs	iam-group-has-users-überprüfen	AWS Identity and Access Managemen t (IAM) kann Ihnen helfen, die Prinzipien der geringsten Rechte und der Aufgabent rennung mit Zugriffsb erechtigungen und Autorisierungen zu integrieren, indem sichergestellt wird, dass IAM-Gruppen mindestens einen Benutzer haben. Die Einteilung von Benutzern in Gruppen auf der Grundlage der ihnen zugewiese nen Berechtigungen oder ihrer Funktion ist eine Möglichkeit, das Prinzip der geringste n Berechtigung zu implementieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AC-3.A	AC-3.A Durchsetzung des Zugriffs	iam-inline-policy-blocked-kms-Aktionen	Stellen Sie sicher, dass ein Benutzer, eine IAM-Rolle oder eine IAM-Gruppe (AWS Identity and Access Management) nicht über eine Inline-Richtlinie verfügt, die blockierte Aktionen für alle AWS Schlüssel des Key Management Service zulässt. AWS empfiehlt, verwaltete Richtlinien anstelle von Inline-Richtlinien zu verwenden. Verwaltete Richtlinien ermöglichen Wiederverwendbarkeit, Versionsverwaltung, Rollback und Delegierung der Berechtigungsverwaltung. Mit dieser Regel können Sie den blockedActionsPatterns Parameter festlegen. (Wert „AWS Bewährte grundlegende Sicherheitsmethoden“: kms: Entschlüsseln, kms:ReEnc

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
			ryptFrom). Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.
CCCS-fPBMM-AC-3.A	AC-3.A Durchsetzung des Zugriffs	iam-no-inline-policy-überprüfen	Stellen Sie sicher, dass ein Benutzer, eine IAM-Rolle oder eine IAM-Gruppe (AWS Identity and Access Management) nicht über eine Inline-Richtlinie zur Zugriffskontrolle auf Systeme und Ressourcen verfügt. AWS empfiehlt, verwaltete Richtlinien anstelle von Inline-Richtlinien zu verwenden. Verwaltete Richtlinien ermöglichen Wiederverwendbarkeit, Versionsverwaltung, Rollback und Delegierung der Berechtigungsverwaltung.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AC-3.A	AC-3.A Durchsetzung des Zugriffs	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) kann Ihnen dabei helfen, die Prinzipien der geringsten Rechte und der Aufgabentrennung in Zugriffsberechtigungen und Autorisierungen zu integrieren und so zu verhindern, dass Richtlinien „Effect“: „Allow“ mit „Action“: „*“ anstelle von „Resource“: „*“ enthalten. Wenn Benutzern mehr Rechte eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und der Aufgabentrennung verstoßen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AC-3.A	AC-3.A Durchsetzung des Zugriffs	iam-user-group-membership-überprüfen	AWS Identity and Access Management (IAM) kann Ihnen helfen, Zugriffsberechtigungen und Autorisierungen einzuschränken, indem sichergestellt wird, dass Benutzer Mitglieder mindestens einer Gruppe sind. Wenn Benutzern mehr Berechtigungen eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und Aufgabentrennung verstoßen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AC-3.A	AC-3.A Durchsetzung des Zugriffs	iam-user-mfa-enabled	Aktivieren Sie diese Regel, um den Zugriff auf Ressourcen in der AWS -Cloud einzuschränken. Diese Regel stellt sicher, dass die Multi-Faktor-Authentifizierung (MFA) für alle Benutzer aktiviert ist. MFA bietet eine weitere Schutzebene zusätzlich zum Benutzernamen und Passwort. Reduzieren Sie Fälle von kompromittierten Konten, indem Sie MFA für Benutzer vorschreiben.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AC-3.A	AC-3.A Durchsetzung des Zugriffs	iam-user-no-policies-überprüfen	Diese Regel stellt sicher, dass AWS Identity and Access Management (IAM) -Richtlinien nur Gruppen oder Rollen zugewiese n werden, um den Zugriff auf Systeme und Ressourcen zu kontrollieren. Die Zuweisung von Berechtig ungen auf Gruppen- oder Rollenebene trägt dazu bei, die Wahrscheinlichkeit zu verringern, dass eine Identität übermäßige Berechtigungen erhält oder beibehält.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AC-3.A	AC-3.A Durchsetzung des Zugriffs	iam-user-unused-credentials-überprüfen	AWS Identity and Access Management (IAM) kann Ihnen bei Zugriffsberechtigungen und Autorisierungen helfen, indem es nach IAM-Passwörtern und Zugriffsschlüsseln sucht, die für einen bestimmten Zeitraum nicht verwendet wurden. Wenn ungenutzte Anmeldeinformationen identifiziert werden, müssen Sie sie deaktivieren und/oder entfernen, da dies gegen das Prinzip der geringsten Berechtigung verstoßen könnte. Für diese Regel müssen Sie einen Wert für das maxCredentialUsage Alter festlegen (Standardkonfiguration: 90). Der tatsächliche Wert muss den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AC-3.A	AC-3.A Durchsetzung des Zugriffs	internet-gateway-authorized-vpc-nur	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Internet-Gateways nur mit autorisierter Amazon Virtual Private Cloud (Amazon VPC) verbunden sind. Internet-Gateways ermöglichen den bidirektionalen Internetzugang zur und von der Amazon VPC, was möglicher weise zu einem unbefugten Zugriff auf Amazon-VPC-Ressourcen führen kann.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AC-3.A	AC-3.A Durchsetzung des Zugriffs	lambda-function-public-access-verboten	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass AWS Lambda-Funktionen nicht öffentlich zugänglich sind. Der öffentliche Zugriff kann möglicherweise die Verfügbarkeit von Ressourcen beeinträchtigen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AC-3.A	AC-3.A Durchsetzung des Zugriffs	lambda-inside-vpc	Stellen Sie AWS Lambda-Funktionen in einer Amazon Virtual Private Cloud (Amazon VPC) bereit, um eine sichere Kommunikation zwischen einer Funktion und anderen Diensten innerhalb der Amazon VPC zu gewährleisten. Bei dieser Konfiguration sind kein Internet-Gateway, kein NAT-Gerät und keine VPN-Verbindung erforderlich. Der gesamte Datenverkehr bleibt sicher in der Cloud. AWS Domains, die sich innerhalb einer VPC befinden, verfügen aufgrund ihrer logischen Isolierung im Vergleich zu Domains mit öffentlichen Endpunkten über eine zusätzliche Sicherheitsebene. Um den Zugriff ordnungsgemäß zu verwalten,

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
			sollten AWS Lambda-Funktionen einer VPC zugewiesen werden.
CCCS-fPBMM-AC-3.A	AC-3.A Durchsetzung des Zugriffs	mfa-enabled-for-iam-Konsolenzugriff	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass MFA für alle AWS Identity and Access Management (IAM) -Benutzer aktiviert ist, die über ein Konsolenkennwort verfügen. MFA sorgt für eine weitere Schutzebene zusätzlich zu den Anmeldeinformationen. Indem Sie MFA für Benutzer vorschreiben, können Sie Fälle kompromittierter Konten reduzieren und verhindern, dass unbefugte Benutzer auf vertrauliche Daten zugreifen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AC-3.A	AC-3.A Durchsetzung des Zugriffs	opensearch-in-vpc-only	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass sich Amazon OpenSearch Service-Domains innerhalb einer Amazon Virtual Private Cloud (Amazon VPC) befinden. Eine Amazon OpenSearch Service-Domain innerhalb einer Amazon VPC ermöglicht die sichere Kommunikation zwischen Amazon OpenSearch Service und anderen Services innerhalb der Amazon VPC, ohne dass ein Internet-Gateway, ein NAT-Gerät oder eine VPN-Verbindung erforderlich ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AC-3.A	AC-3.A Durchsetzung des Zugriffs	rds-instance-public-access-überprüfen	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Relational Database Service (Amazon RDS) -Instances nicht öffentlich sind. Amazon-RDS-Datenbank-Instances können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AC-3.A	AC-3.A Durchsetzung des Zugriffs	rds-snapshots-public-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Relational Database Service (Amazon RDS) -Instances nicht öffentlich sind. Amazon-RDS-Datenbank-Instances können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AC-3.A	AC-3.A Durchsetzung des Zugriffs	redshift-cluster-public-access-überprüfen	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Redshift Redshift-Cluster nicht öffentlich sind. Amazon-Redshift-Cluster können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AC-3.A	AC-3.A Durchsetzung des Zugriffs	root-account-mfa-enabled	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass MFA für den Root-Benutzer aktiviert ist. Der Stammbenutzer ist der AWS-Konto-Benutzer mit den meisten Berechtigungen. MFA bietet eine weitere Schutzebene zusätzlich zum Benutzernamen und Passwort. Indem Sie MFA für den Root-Benutzer vorschreiben, können Sie die Anzahl AWS-Konten kompromittierter Benutzer reduzieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AC-3.A	AC-3.A Durchsetzung des Zugriffs	s3- -blöcke-periodisch account-level-public-access	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Simple Storage Service (Amazon S3) -Buckets nicht öffentlich zugänglich sind. Diese Regel trägt dazu bei, sensible Daten vor unbefugten Remote-Benutzern zu schützen, indem sie den öffentlichen Zugriff verhindert. Mit dieser Regel können Sie optional die Parameter ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) und restrictPublicBuckets Parameter (Config Default: True) festlegen. Die tatsächlichen Werte müssen den Richtlini

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
			en Ihrer Organisation entsprechen.
CCCS-fPBMM-AC-3.A	AC-3.A Durchsetzung des Zugriffs	s3 bucket-level-public-access - verboten	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Simple Storage Service (Amazon S3) -Buckets nicht öffentlich zugänglich sind. Diese Regel trägt dazu bei, sensible Daten vor unbefugten Remote-Benutzern zu schützen, indem sie den öffentlichen Zugriff auf Bucket-Ebene verhindert.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AC-3.A	AC-3.A Durchsetzung des Zugriffs	s-3 bucket-public-read-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie nur autorisierten Benutzern, Prozessen und Geräten Zugriff auf Amazon Simple Storage Service (Amazon S3) - Buckets gewähren. Die Verwaltung des Zugriffs sollte mit der Klassifizierung der Daten übereinst immen.
CCCS-fPBMM-AC-3.A	AC-3.A Durchsetzung des Zugriffs	s3- bucket-public-write-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie nur autorisierten Benutzern, Prozessen und Geräten Zugriff auf Amazon Simple Storage Service (Amazon S3) - Buckets gewähren. Die Verwaltung des Zugriffs sollte mit der Klassifizierung der Daten übereinst immen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AC-3.A	AC-3.A Durchsetzung des Zugriffs	sagemaker-notebook-no-direct-Internetzugang	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass SageMaker Amazon-Notebooks keinen direkten Internetzugang zulassen. Indem Sie direkten Internetzugang blockieren, vermeiden Sie, dass unbefugte Benutzer auf sensible Daten zugreifen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AC-3.A	AC-3.A Durchsetzung des Zugriffs	subnet-auto-assign-public-ip-deaktiviert	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon Virtual Private Cloud (VPC) -Subnetzen nicht automatisch eine öffentliche IP-Adresse zugewiesen wird. Amazon Elastic Compute Cloud (EC2) -Instances, die in Subnetzen gestartet werden, in denen dieses Attribut aktiviert ist, haben ihrer primären Netzwerkschnittstelle eine öffentliche IP-Adresse zugewiesen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AC-4(21)	AC-4(21) Durchsetzung des Informationsflusses | Physische oder logische Trennung der Informationsflüsse	alb-http-to-https-Umleitungsprüfung	Um Daten während der Übertragung zu schützen, stellen Sie sicher, dass Ihr Application Load Balancer unverschlüsselte HTTP-Anfragen automatisch an HTTPS umleitet. Da sensible Daten vorhanden sein können, sollten Sie die Verschlüsselung bei der Übertragung aktivieren, um diese Daten zu schützen.
CCCS-fPBMM-AC-4(21)	AC-4(21) Durchsetzung des Informationsflusses | Physische oder logische Trennung der Informationsflüsse	api-gw-ssl-enabled	Stellen Sie sicher, dass die REST-API-Stufen von Amazon API Gateway mit SSL-Zertifikaten konfiguriert sind, damit Backend-Systeme überprüfen können, ob Anforderungen von API Gateway stammen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AC-4(21)	AC-4(21) Durchsetzung des Informationsflusses | Physische oder logische Trennung der Informationsflüsse	elasticsearch-node-to-node-Verschlüsselungsprüfung	Stellen Sie sicher, dass die node-to-node Verschlüsselung für Amazon OpenSearch Service aktiviert ist. Node-to-nodeVerschlüsselung ermöglicht die TLS 1.2-Verschlüsselung für die gesamte Kommunikation innerhalb der Amazon Virtual Private Cloud (Amazon VPC). Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AC-4(21)	AC-4(21) Durchsetzung des Informationsflusses | Physische oder logische Trennung der Informationsflüsse	elb-acm-certificate-required	Zum Schutz von eventuell vorhandenen sensiblen Daten sowie von Daten während der Übertragung muss die Verschlüsselung für Ihr Elastic Load Balancing aktiviert sein. Verwenden Sie AWS Certificate Manager, um öffentliche und private SSL/TLS-Zertifikate mit AWS Diensten und internen Ressourcen zu verwalten, bereitzustellen und bereitzustellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AC-4(21)	AC-4(21) Durchsetzung des Informationsflusses | Physische oder logische Trennung der Informationsflüsse	elb-predefined-security-policy-ssl-check	Stellen Sie sicher, dass Ihre SSL-Listener von Classic Elastic Load Balancing eine vordefinierte Sicherheitsrichtlinie verwenden, um Daten während der Übertragung zu schützen. Elastic Load Balancing bietet vordefinierte Aushandlungskonfigurationen, die für die SSL-Aushandlung verwendet werden, wenn eine Verbindung zwischen einem Client und Ihrem Load Balancer hergestellt wurde. Die SSL-Aushandlungskonfigurationen sind mit einer breiten Palette von Clients kompatibel und verwenden hochfeste kryptografische Algorithmen. Diese Regel verlangt, dass Sie eine vordefinierte Sicherheitsrichtlinie für Ihre SSL-Liste

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
			ner festlegen. Die Standard-Sicherheitsrichtlinie lautet: Policy-TLS-1-2-2017-0. ELBSecurity Der tatsächliche Wert muss den Richtlinien Ihrer Organisation entsprechen.
CCCS-fPBMM-AC-4(21)	AC-4(21) Durchsetzung des Informationsflusses | Physische oder logische Trennung der Informationsflüsse	elb-tls-https-listeners-nur	Stellen Sie sicher, dass Ihre Elastic Load Balancer (ELBs) mit SSL- oder HTTPS-Listenern konfiguriert sind. Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AC-4(21)	AC-4(21) Durchsetzung des Informationsflusses | Physische oder logische Trennung der Informationsflüsse	opensearch-node-to-node-Verschlüsselungsprüfung	Stellen Sie sicher, dass die node-to-node Verschlüsselung für Amazon OpenSearch Service aktiviert ist. Node-to-nodeVerschlüsselung ermöglicht die TLS 1.2-Verschlüsselung für die gesamte Kommunikation innerhalb der Amazon Virtual Private Cloud (Amazon VPC). Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AC-4(21)	AC-4(21) Durchsetzung des Informationsflusses | Physische oder logische Trennung der Informationsflüsse	redshift-require-tls-ssl	Stellen Sie sicher, dass Ihre Amazon-Redshift-Cluster eine TLS/SSL-Verschlüsselung erfordern, um eine Verbindung zu SQL-Clients herzustellen. Da sensible Daten vorhanden sein können, sollten Sie die Verschlüsselung bei der Übertragung aktivieren, um diese Daten zu schützen.
CCCS-fPBMM-AC-4(21)	AC-4(21) Durchsetzung des Informationsflusses | Physische oder logische Trennung der Informationsflüsse	s-3 bucket-ssl-requests-only	Um Daten während der Übertragung zu schützen, stellen Sie sicher, dass Ihre Amazon Simple Storage Service (Amazon S3)-Buckets Anfragen zur Verwendung von Secure Socket Layer (SSL)-Buckets erfordern. Da sensible Daten vorhanden sein können, sollten Sie die Verschlüsselung bei der Übertragung aktivieren, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AC-4.A	AC-4.A Durchsetzung des Informationsflusses	alb-http-to-https-Umleitungsprüfung	Um Daten während der Übertragung zu schützen, stellen Sie sicher, dass Ihr Application Load Balancer unverschlüsselte HTTP-Anfragen automatisch an HTTPS umleitet. Da sensible Daten vorhanden sein können, sollten Sie die Verschlüsselung bei der Übertragung aktivieren, um diese Daten zu schützen.
CCCS-fPBMM-AC-4.A	AC-4.A Durchsetzung des Informationsflusses	api-gw-ssl-enabled	Stellen Sie sicher, dass die REST-API-Stufen von Amazon API Gateway mit SSL-Zertifikaten konfiguriert sind, damit Backend-Systeme überprüfen können, ob Anforderungen von API Gateway stammen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AC-4.A	AC-4.A Durchsetzung des Informationsflusses	dms-replication-not-public	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass auf DMS-Replikationsinstanzen nicht öffentlich zugegriffen werden kann. DMS-Replikations-Instances können vertrauliche Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.
CCCS-fPBMM-AC-4.A	AC-4.A Durchsetzung des Informationsflusses	ebs-snapshot-public-restorable-überprüfen	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass EBS-Snapshots nicht öffentlich wiederherstellbar sind. EBS-Volume-Snapshots können vertrauliche Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AC-4.A	AC-4.A Durchsetzung des Informationsflusses	ec-2 instance-no-public-ip	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon Elastic Compute Cloud (Amazon EC2) - Instances nicht öffentlich zugänglich sind. EC2Amazon -Instances können vertrauliche Informationen enthalten, und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AC-4.A	AC-4.A Durchsetzung des Informationsflusses	elasticsearch-in-vpc-only	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass sich Amazon OpenSearch OpenSearch Service (Service) - Domains innerhalb einer Amazon Virtual Private Cloud (Amazon VPC) befinden. Eine OpenSearch Service-Domain innerhalb einer Amazon VPC ermöglicht die sichere Kommunikation zwischen OpenSearch Service und anderen Services innerhalb der Amazon VPC, ohne dass ein Internet-Gateway, ein NAT-Gerät oder eine VPN-Verbindung erforderlich ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AC-4.A	AC-4.A Durchsetzung des Informationsflusses	elasticsearch-node-to-node-Verschlüsselungsprüfung	Stellen Sie sicher, dass die node-to-node Verschlüsselung für Amazon OpenSearch Service aktiviert ist. Node-to-nodeVerschlüsselung ermöglicht die TLS 1.2-Verschlüsselung für die gesamte Kommunikation innerhalb der Amazon Virtual Private Cloud (Amazon VPC). Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AC-4.A	AC-4.A Durchsetzung des Informationsflusses	elb-acm-certificate-required	Zum Schutz von eventuell vorhandenen sensiblen Daten sowie von Daten während der Übertragung muss die Verschlüsselung für Ihr Elastic Load Balancing aktiviert sein. Verwenden Sie AWS Certificate Manager, um öffentliche und private SSL/TLS-Zertifikate mit AWS Diensten und internen Ressourcen zu verwalten, bereitzustellen und bereitzustellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AC-4.A	AC-4.A Durchsetzung des Informationsflusses	elb-predefined-security-policy-ssl-check	Stellen Sie sicher, dass Ihre SSL-Listener von Classic Elastic Load Balancing eine vordefinierte Sicherheitsrichtlinie verwenden, um Daten während der Übertragung zu schützen. Elastic Load Balancing bietet vordefinierte Aushandlungskonfigurationen, die für die SSL-Aushandlung verwendet werden, wenn eine Verbindung zwischen einem Client und Ihrem Load Balancer hergestellt wurde. Die SSL-Aushandlungskonfigurationen sind mit einer breiten Palette von Clients kompatibel und verwenden hochfeste kryptografische Algorithmen. Diese Regel verlangt, dass Sie eine vordefinierte Sicherheitsrichtlinie für Ihre SSL-Liste

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
			ner festlegen. Die Standard-Sicherheitsrichtlinie lautet: Policy-TLS-1-2-2017-0. ELBSecurity Der tatsächliche Wert muss den Richtlinien Ihrer Organisation entsprechen.
CCCS-fPBMM-AC-4.A	AC-4.A Durchsetzung des Informationsflusses	elb-tls-https-listeners-nur	Stellen Sie sicher, dass Ihre Elastic Load Balancer (ELBs) mit SSL- oder HTTPS-Listenern konfiguriert sind. Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AC-4.A	AC-4.A Durchsetzung des Informationsflusses	emr-master-no-public-ip	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon EMR-Cluster-Masterknoten nicht öffentlich zugänglich sind. Amazon-EMR-Cluster-Hauptknoten können vertrauliche Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AC-4.A	AC-4.A Durchsetzung des Informationsflusses	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) Security Groups können bei der Verwaltung des Netzwerkzugriffs helfen, indem sie eine statusbehaftete Filterung des ein- und ausgehenden Netzwerkverkehrs zu Ressourcen bereitstellen. AWS Wenn Sie eingehenden (oder entfernten) Datenverkehr von 0.0.0.0/0 bis Port 22 auf Ihren Ressourcen nicht zulassen, können Sie den Remote-Zugriff einschränken.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AC-4.A	AC-4.A Durchsetzung des Informationsflusses	ec-2 instances-in-vpc	Stellen Sie Amazon Elastic Compute Cloud (Amazon EC2)-Instances innerhalb einer Amazon Virtual Private Cloud (Amazon VPC) bereit, um eine sichere Kommunikation zwischen einer Instance und anderen Services innerhalb der Amazon VPC zu ermöglichen, ohne dass ein Internet-Gateway, ein NAT-Gerät oder eine VPN-Verbindung erforderlich ist. Der gesamte Datenverkehr bleibt sicher in der AWS Cloud. Domains, die sich innerhalb einer VPC befinden, verfügen aufgrund ihrer logischen Isolierung im Vergleich zu Domains mit öffentlichen Endpunkten über eine zusätzliche Sicherheitsebene. Weisen Sie EC2

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
			Amazon-Instances einer Amazon VPC zu, um den Zugriff ordnungsgemäß zu verwalten.
CCCS-fPBMM-AC-4.A	AC-4.A Durchsetzung des Informationsflusses	internet-gateway-authorized-vpc-nur	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Internet-Gateways nur mit autorisierter Amazon Virtual Private Cloud (Amazon VPC) verbunden sind. Internet-Gateways ermöglichen den bidirektionalen Internetzugang zur und von der Amazon VPC, was möglicherweise zu einem unbefugten Zugriff auf Amazon-VPC-Ressourcen führen kann.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AC-4.A	AC-4.A Durchsetzung des Informationsflusses	lambda-function-public-access-verboten	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass AWS Lambda-Funktionen nicht öffentlich zugänglich sind. Der öffentliche Zugriff kann möglicherweise die Verfügbarkeit von Ressourcen beeinträchtigen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AC-4.A	AC-4.A Durchsetzung des Informationsflusses	lambda-inside-vpc	Stellen Sie AWS Lambda-Funktionen in einer Amazon Virtual Private Cloud (Amazon VPC) bereit, um eine sichere Kommunikation zwischen einer Funktion und anderen Diensten innerhalb der Amazon VPC zu gewährleisten. Bei dieser Konfiguration sind kein Internet-Gateway, kein NAT-Gerät und keine VPN-Verbindung erforderlich. Der gesamte Datenverkehr bleibt sicher in der Cloud. AWS Domains, die sich innerhalb einer VPC befinden, verfügen aufgrund ihrer logischen Isolierung im Vergleich zu Domains mit öffentlichen Endpunkten über eine zusätzliche Sicherheitsebene. Um den Zugriff ordnungsgemäß zu verwalten,

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
			sollten AWS Lambda-Funktionen einer VPC zugewiesen werden.
CCCS-fPBMM-AC-4.A	AC-4.A Durchsetzung des Informationsflusses	opensearch-node-to-node-Verschlüsselungsprüfung	Stellen Sie sicher, dass die node-to-node Verschlüsselung für Amazon OpenSearch Service aktiviert ist. Node-to-nodeVerschlüsselung ermöglicht die TLS 1.2-Verschlüsselung für die gesamte Kommunikation innerhalb der Amazon Virtual Private Cloud (Amazon VPC). Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AC-4.A	AC-4.A Durchsetzung des Informationsflusses	rds-instance-public-access-überprüfen	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Relational Database Service (Amazon RDS) -Instances nicht öffentlich sind. Amazon-RDS-Datenbank-Instances können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AC-4.A	AC-4.A Durchsetzung des Informationsflusses	rds-snapshots-public-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Relational Database Service (Amazon RDS) -Instances nicht öffentlich sind. Amazon-RDS-Datenbank-Instances können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AC-4.A	AC-4.A Durchsetzung des Informationsflusses	redshift-cluster-public-access-überprüfen	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Redshift Redshift-Cluster nicht öffentlich sind. Amazon-Redshift-Cluster können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.
CCCS-fPBMM-AC-4.A	AC-4.A Durchsetzung des Informationsflusses	redshift-require-tls-ssl	Stellen Sie sicher, dass Ihre Amazon-Redshift-Cluster eine TLS/SSL-Verschlüsselung erfordern, um eine Verbindung zu SQL-Clients herzustellen. Da sensible Daten vorhanden sein können, sollten Sie die Verschlüsselung bei der Übertragung aktivieren, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AC-4.A	AC-4.A Durchsetzung des Informationsflusses	restricted-common-ports	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass gemeinsame Ports für Amazon Elastic Compute Cloud (Amazon EC2) -Sicherheitsgruppen eingeschränkt sind. Wenn der Zugriff auf Ports nicht auf vertrauenswürdige Quellen beschränkt wird, kann dies zu Angriffen auf die Verfügbarkeit, Integrität und Vertraulichkeit von Systemen führen. Mit dieser Regel können Sie optional die Parameter blockedPort1–blockedPort5 festlegen (Standardkonfigurationen: 20, 21, 3389, 3306, 4333). Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AC-4.A	AC-4.A Durchsetzung des Informationsflusses	s3- account-level-public-access -blöcke-periodisch	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Simple Storage Service (Amazon S3) -Buckets nicht öffentlich zugänglich sind. Diese Regel trägt dazu bei, sensible Daten vor unbefugten Remote-Benutzern zu schützen, indem sie den öffentlichen Zugriff verhindert. Mit dieser Regel können Sie optional die Parameter ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) und restrictPublicBuckets Parameter (Config Default: True) festlegen. Die tatsächlichen Werte müssen den Richtlini

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
			en Ihrer Organisation entsprechen.
CCCS-fPBMM-AC-4.A	AC-4.A Durchsetzung des Informationsflusses	s3 bucket-level-public-access - verboten	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Simple Storage Service (Amazon S3) -Buckets nicht öffentlich zugänglich sind. Diese Regel trägt dazu bei, sensible Daten vor unbefugten Remote-Benutzern zu schützen, indem sie den öffentlichen Zugriff auf Bucket-Ebene verhindert.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AC-4.A	AC-4.A Durchsetzung des Informationsflusses	s-3 bucket-public-read-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie nur autorisierten Benutzern, Prozessen und Geräten Zugriff auf Amazon Simple Storage Service (Amazon S3) - Buckets gewähren. Die Verwaltung des Zugriffs sollte mit der Klassifizierung der Daten übereinstimmen.
CCCS-fPBMM-AC-4.A	AC-4.A Durchsetzung des Informationsflusses	s3- bucket-public-write-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie nur autorisierten Benutzern, Prozessen und Geräten Zugriff auf Amazon Simple Storage Service (Amazon S3) - Buckets gewähren. Die Verwaltung des Zugriffs sollte mit der Klassifizierung der Daten übereinstimmen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AC-4.A	AC-4.A Durchsetzung des Informationsflusses	s3- bucket-ssl-requests-only	Um Daten während der Übertragung zu schützen, stellen Sie sicher, dass Ihre Amazon Simple Storage Service (Amazon S3)-Buckets Anfragen zur Verwendung von Secure Socket Layer (SSL)-Buckets erfordern. Da sensible Daten vorhanden sein können, sollten Sie die Verschlüsselung bei der Übertragung aktivieren, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AC-4.A	AC-4.A Durchsetzung des Informationsflusses	sagemaker-notebook-no-direct-Internetzugang	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass SageMaker Amazon-Notebooks keinen direkten Internetzugang zulassen. Indem Sie direkten Internetzugang blockieren, vermeiden Sie, dass unbefugte Benutzer auf sensible Daten zugreifen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AC-4.A	AC-4.A Durchsetzung des Informationsflusses	subnet-auto-assign-public-ip-deaktiviert	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon Virtual Private Cloud (VPC) -Subnetzen nicht automatisch eine öffentliche IP-Adresse zugewiesen wird. Amazon Elastic Compute Cloud (EC2) -Instances, die in Subnetzen gestartet werden, in denen dieses Attribut aktiviert ist, haben ihrer primären Netzwerkschnittstelle eine öffentliche IP-Adresse zugewiesen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AC-4.A	AC-4.A Durchsetzung des Informationsflusses	vpc-default-security-group-geschlossen	Sicherheitsgruppen von Amazon Elastic Compute Cloud (Amazon EC2) können bei der Verwaltung des Netzwerkzugriffs helfen, indem sie eine statusbehaftete Filterung des ein- und ausgehenden Netzwerkverkehrs zu Ressourcen bereitstellen. AWS Die Beschränkung des gesamten Datenverkehrs auf die Standardsicherheitsgruppe hilft dabei, den Fernzugriff auf Ihre Ressourcen einzuschränken. AWS

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AC-4.A	AC-4.A Durchsetzung des Informationsflusses	vpc-sg-open-only-to-authorized-ports	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass gemeinsame Ports für Amazon Elastic Compute Cloud (Amazon EC2) -Sicherheitsgruppen eingeschränkt sind. Wenn der Zugriff auf Ports nicht auf vertrauenswürdige Quellen beschränkt wird, kann dies zu Angriffen auf die Verfügbarkeit, Integrität und Vertraulichkeit von Systemen führen. Durch die Beschränkung des Zugriffs auf Ressourcen innerhalb einer Sicherheitsgruppe aus dem Internet (0.0.0.0/0) kann der Fernzugriff auf interne Systeme gesteuert werden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AC-5.A	AC-5.A Aufgabentrennung	ecs-task-definition-user-for-host-mode-check	Wenn für eine Aufgabendefinition erhöhte Berechtigungen gelten, liegt das daran, dass der Kunde diesen Konfigurationen ausdrücklich zugestimmt hat. Diese Kontrolle prüft, ob eine unerwartete Berechtigungseskalation vorliegt, wenn für eine Aufgabendefinition das Host-Netzwerk aktiviert ist, die Kunden aber keine erhöhten Berechtigungen aktiviert haben.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AC-5.A	AC-5.A Aufgabentrennung	emr-kerberos-enabled	Die Zugriffsberechtigungen und -autorisierungen können verwaltet und nach den Prinzipien der geringsten Berechtigung und Aufgabentrennung integriert werden, indem Kerberos für Amazon-EMR-Cluster aktiviert wird. In Kerberos werden Services und Benutzer, die sich authentifizieren müssen, als Prinzipale bezeichnet. Prinzipale befinden sich in einem Kerberos-Bereich. Innerhalb dieses Bereichs wird ein Kerberos-Server als Key Distribution Center (KDC) bezeichnet. Über diesen Server können sich Prinzipale authentifizieren. Die Authentifizierung im KDC erfolgt durch die Ausstellung von Authentif

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
			izierungstickets. Das KDC unterhält eine Datenbank der Prinzipale in seinem Bereich mit ihren Passwörtern und anderen administr ativen Informationen zu jedem Prinzipal.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AC-5.A	AC-5.A Aufgabentrennung	iam-customer-policy-blocked-kms-Aktionen	AWS Identity and Access Management (IAM) kann Ihnen helfen, die Prinzipien der geringsten Rechte und der Aufgabentrennung in Zugriffsberechtigungen und Autorisierungen zu integrieren und so zu verhindern, dass Richtlinien blockierte Aktionen für alle AWS Schlüssel des Key Management Service enthalten. Wenn Benutzer mehr Rechte haben, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und Aufgabentrennung verstoßen. Mit dieser Regel können Sie den Parameter festlegen. blockedActionsPatterns (Wert „AWS Bewährte grundlegende Sicherheitsmethode

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
			n“: kms: Entschlüs seln, kms:ReEnc ryptFrom). Die tatsächlichen Werte müssen den Richtlini en Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AC-5.A	AC-5.A Aufgabent rennung	iam-inline-policy-blocked-kms-Aktionen	Stellen Sie sicher, dass ein Benutzer, eine IAM-Rolle oder eine IAM-Gruppe (AWS Identity and Access Management) nicht über eine Inline-Richtlinie verfügt, die blockierte Aktionen für alle AWS Schlüssel des Key Management Service zulässt. AWS empfiehlt, verwaltet e Richtlinien anstelle von Inline-Richtlinien zu verwenden. Verwaltete Richtlini en ermöglichen Wiederverwendbarke it, Versionsverwaltung , Rollback und Delegierung der Berechtigungsverwa ltung. Mit dieser Regel können Sie den blockedActionsPatt erns Parameter festlegen. (Wert „AWS Bewährte grundlege nde Sicherhei tsmethoden“: kms: Decrypt, kms:ReEnc ryptFrom). Die

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
			tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.
CCCS-fPBMM-AC-5.A	AC-5.A Aufgabentrennung	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) kann Ihnen dabei helfen, die Prinzipien der geringsten Rechte und der Aufgabentrennung in Zugriffsberechtigungen und Autorisierungen zu integrieren und so zu verhindern, dass Richtlinien „Effect“: „Allow“ mit „Action“: „*“ anstelle von „Resource“: „*“ enthalten. Wenn Benutzern mehr Rechte eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und der Aufgabentrennung verstoßen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AC-6(1)	AC-6(1) Geringste Berechtigung | Autorisieren des Zugriffs auf Sicherheitsfunktionen	ecs-task-definition-user-for-host-mode-check	Wenn für eine Aufgabendefinition erhöhte Berechtigungen gelten, liegt das daran, dass der Kunde diesen Konfigurationen ausdrücklich zugestimmt hat. Diese Kontrolle prüft, ob eine unerwartete Berechtigungseskalation vorliegt, wenn für eine Aufgabendefinition das Host-Netzwerk aktiviert ist, die Kunden aber keine erhöhten Berechtigungen aktiviert haben.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AC-6(1)	AC-6(1) Geringste Berechtigung | Autorisieren des Zugriffs auf Sicherheitsfunktionen	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) kann Ihnen dabei helfen, die Prinzipien der geringsten Rechte und der Aufgabentrennung in Zugriffsberechtigungen und Autorisierungen zu integrieren und so zu verhindern, dass Richtlinien „Effect“: „Allow“ mit „Action“: „*“ anstelle von „Resource“: „*“ enthalten. Wenn Benutzern mehr Rechte eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und der Aufgabentrennung verstoßen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AC-6(1)	AC-6(1) Geringste Berechtigung | Autorisieren des Zugriffs auf Sicherheitsfunktionen	iam-user-mfa-enabled	Aktivieren Sie diese Regel, um den Zugriff auf Ressourcen in der AWS -Cloud einzuschränken. Diese Regel stellt sicher, dass die Multi-Faktor-Authentifizierung (MFA) für alle Benutzer aktiviert ist. MFA bietet eine weitere Schutzebene zusätzlich zum Benutzernamen und Passwort. Reduzieren Sie Fälle von kompromittierten Konten, indem Sie MFA für Benutzer vorschreiben.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AC-6(1)	AC-6(1) Geringste Berechtigung | Autorisieren des Zugriffs auf Sicherheitsfunktionen	mfa-enabled-for-iam-Konsolenzugriff	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass MFA für alle AWS Identity and Access Management (IAM) -Benutzer aktiviert ist, die über ein Konsolenkennwort verfügen. MFA sorgt für eine weitere Schutzebene zusätzlich zu den Anmeldeinformationen. Indem Sie MFA für Benutzer vorschreiben, können Sie Fälle kompromittierter Konten reduzieren und verhindern, dass unbefugte Benutzer auf vertrauliche Daten zugreifen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AC-6(1)	AC-6(1) Geringste Berechtigung | Autorisieren des Zugriffs auf Sicherheitsfunktionen	root-account-mfa-enabled	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass MFA für den Root-Benutzer aktiviert ist. Der Stammbenutzer ist der AWS-Konto-Benutzer mit den meisten Berechtigungen. MFA bietet eine weitere Schutzebene zusätzlich zum Benutzernamen und Passwort. Indem Sie MFA für den Root-Benutzer vorschreiben, können Sie die Anzahl AWS-Konten kompromittierter Benutzer reduzieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AC-6(2)	AC-6(2) Geringste Berechtigung | Nicht privilegierter Zugriff auf nicht sicherheitsrelevante Funktionen	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) kann Ihnen dabei helfen, die Prinzipien der geringsten Rechte und der Aufgabentrennung in Zugriffsberechtigungen und Autorisierungen zu integrieren und so zu verhindern, dass Richtlinien „Effect“: „Allow“ mit „Action“: „*“ anstelle von „Resource“: „*“ enthalten. Wenn Benutzern mehr Rechte eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und der Aufgabentrennung verstoßen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AC-6(2)	AC-6(2) Geringste Berechtigung | Nicht privilegierter Zugriff auf nicht sicherheitsrelevante Funktionen	iam-root-access-key-überprüfen	Der Zugriff auf Systeme und Ressourcen kann gesteuert werden, indem überprüft wird, ob der Root-Benutzer keine Zugriffsschlüssel mit seiner AWS Identity and Access Management (IAM) -Rolle verknüpft hat. Stellen Sie sicher, dass die Root-Zugriffsschlüssel gelöscht werden. Erstellen und verwenden Sie stattdessen rollenbasierte Funktionen, AWS-Konten um das Prinzip der geringsten Funktionalität zu berücksichtigen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AC-6(2)	AC-6(2) Geringste Berechtigung | Nicht privilegierter Zugriff auf nicht sicherheitsrelevante Funktionen	iam-user-mfa-enabled	Aktivieren Sie diese Regel, um den Zugriff auf Ressourcen in der AWS -Cloud einzuschränken. Diese Regel stellt sicher, dass die Multi-Faktor-Authentifizierung (MFA) für alle Benutzer aktiviert ist. MFA bietet eine weitere Schutzebene zusätzlich zum Benutzernamen und Passwort. Reduzieren Sie Fälle von kompromittierten Konten, indem Sie MFA für Benutzer vorschreiben.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AC-6(2)	AC-6(2) Geringste Berechtigung | Nicht privilegierter Zugriff auf nicht sicherheitsrelevante Funktionen	mfa-enabled-for-iam-Konsolenzugriff	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass MFA für alle AWS Identity and Access Management (IAM) -Benutzer aktiviert ist, die über ein Konsolenkennwort verfügen. MFA sorgt für eine weitere Schutzebene zusätzlich zu den Anmeldeinformationen. Indem Sie MFA für Benutzer vorschreiben, können Sie Fälle kompromittierter Konten reduzieren und verhindern, dass unbefugte Benutzer auf vertrauliche Daten zugreifen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AC-6(2)	AC-6(2) Geringste Berechtigung | Nicht privilegierter Zugriff auf nicht sicherheitsrelevante Funktionen	root-account-mfa-enabled	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass MFA für den Root-Benutzer aktiviert ist. Der Stammbenutzer ist der AWS-Konto-Benutzer mit den meisten Berechtigungen. MFA bietet eine weitere Schutzebene zusätzlich zum Benutzernamen und Passwort. Indem Sie MFA für den Root-Benutzer vorschreiben, können Sie die Anzahl AWS-Konten kompromittierter Benutzer reduzieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AC-6(5)	AC-6(5) Geringste Berechtigung | Privilegierte Konten	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) kann Ihnen dabei helfen, die Prinzipien der geringsten Rechte und der Aufgabentrennung in Zugriffsberechtigungen und Autorisierungen zu integrieren und so zu verhindern, dass Richtlinien „Effect“: „Allow“ mit „Action“: „*“ anstelle von „Resource“: „*“ enthalten. Wenn Benutzern mehr Rechte eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und der Aufgabentrennung verstoßen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AC-6(5)	AC-6(5) Geringste Berechtigung | Privilegierte Konten	iam-user-mfa-enabled	Aktivieren Sie diese Regel, um den Zugriff auf Ressourcen in der AWS -Cloud einzuschränken. Diese Regel stellt sicher, dass die Multi-Faktor-Authentifizierung (MFA) für alle Benutzer aktiviert ist. MFA bietet eine weitere Schutzebene zusätzlich zum Benutzernamen und Passwort. Reduzieren Sie Fälle von kompromittierten Konten, indem Sie MFA für Benutzer vorschreiben.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AC-6(5)	AC-6(5) Geringste Berechtigung | Privilegierte Konten	mfa-enabled-for-iam-Konsolenzugriff	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass MFA für alle AWS Identity and Access Management (IAM) -Benutzer aktiviert ist, die über ein Konsolenkennwort verfügen. MFA sorgt für eine weitere Schutzebene zusätzlich zu den Anmeldeinformationen. Indem Sie MFA für Benutzer vorschreiben, können Sie Fälle kompromittierter Konten reduzieren und verhindern, dass unbefugte Benutzer auf vertrauliche Daten zugreifen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AC-6(5)	AC-6(5) Geringste Berechtigung | Privilegierte Konten	root-account-mfa-enabled	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass MFA für den Root-Benutzer aktiviert ist. Der Stammbenutzer ist der AWS-Konto-Benutzer mit den meisten Berechtigungen. MFA bietet eine weitere Schutzebene zusätzlich zum Benutzernamen und Passwort. Indem Sie MFA für den Root-Benutzer vorschreiben, können Sie die Anzahl AWS-Konten kompromittierter Benutzer reduzieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AC-6(9)	AC-6(9) Geringste Berechtigung | Prüfung der Nutzung privilegierter Funktionen	cloudtrail-s3-data events-enabled	Die Erfassung von Simple Storage Service (Amazon S3)-Datenereignissen unterstützt die Erkennung von ungewöhnlichen Aktivitäten. Zu den Details gehören Informationen zu dem AWS -Konto, das auf einen Amazon-S3-Bucket zugegriffen hat, die IP-Adresse und die Uhrzeit des Ereignisses.
CCCS-fPBMM-AC-6(9)	AC-6(9) Geringste Berechtigung | Prüfung der Nutzung privilegierter Funktionen	cloud-trail-cloud-watch-logs-aktiviert	Verwenden Sie Amazon CloudWatch , um Protokoll ereignisaktivitäten zentral zu sammeln und zu verwalten. Die Aufnahme von AWS CloudTrail Daten liefert Einzelheiten zu den API-Aufrufaktivitäten in Ihrem AWS-Konto.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AC-6(9)	AC-6(9) Geringste Berechtigung | Prüfung der Nutzung privilegierter Funktionen	cloudtrail-enabled	AWS CloudTrail kann bei der Nichtabstreitbarkeit helfen, indem Aktionen und API-Aufrufe der AWS Management Console aufgezeichnet werden. Sie können die Benutzer und die Benutzer AWS-Konten , die einen AWS Dienst aufgerufen haben, die Quell-IP-Adresse, über die die Aufrufe generiert wurden, und den Zeitpunkt der Anrufe identifizieren. Einzelheiten zu den erfassten Daten finden Sie unter Inhalt des AWS CloudTrail Datensatzes.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AC-6(9)	AC-6(9) Geringste Berechtigung | Prüfung der Nutzung privilegierter Funktionen	multi-region-cloudtrail-enabled	AWS CloudTrail zeichnet Aktionen und API-Aufrufe der AWS Management Console auf. Sie können feststellen, welche Benutzer und Konten angerufen wurden AWS, von welcher Quell-IP-Adresse aus die Anrufe getätigt wurden und wann die Anrufe erfolgten. CloudTrail übermittelt Protokolldateien aus allen AWS Regionen an Ihren S3-Bucket , wenn MULTI_REGION_CLOUD_TRAIL_ENABLED aktiviert ist. Außerdem wird beim AWS Start einer neuen Region derselbe Trail in der neuen Region erstellt. CloudTrail Dadurch erhalten Sie automatisch Protokolldateien mit API-Aktivitäten für die neue Region.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AC-6(9)	AC-6(9) Geringste Berechtigung | Prüfung der Nutzung privilegierter Funktionen	rds-logging-enabled	Um die Protokollierung und Überwachung in Ihrer Umgebung zu erleichtern, stellen Sie sicher, dass die Amazon Relational Database Service (Amazon RDS)-Protokollierung aktiviert ist. Mit der Amazon-RDS-Protokollierung können Sie Ereignisse wie Verbindungen, Verbindungsabbrüche, Abfragen oder abgefragte Tabellen erfassen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AC-6(9)	AC-6(9) Geringste Berechtigung | Prüfung der Nutzung privilegierter Funktionen	redshift-cluster-configuration-check	Um Daten im Ruhezustand zu schützen, muss die Verschlüsselung für Ihre Amazon-Redshift-Cluster aktiviert sein. Sie müssen auch sicherstellen, dass die erforderlichen Konfigurationen auf Amazon-Redshift-Clustern bereitgestellt werden. Die Prüfungsprotokollierung muss aktiviert sein, um Informationen zu Verbindungen und Benutzeraktivitäten in der Datenbank bereitzustellen. Diese Regel erfordert, dass ein Wert für clusterDbEncrypted (Config Default: TRUE) und LoggingEnabled (Config Default: TRUE) gesetzt ist. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AC-6(9)	AC-6(9) Geringste Berechtigung | Prüfung der Nutzung privilegierter Funktionen	s3- bucket-logging-enabled	Die Amazon Simple Storage Service (Amazon S3)-Serverzugriffs protokollierung bietet eine Methode zur Überwachu ng des Netzwerks im Hinblick auf potenzielle Cybersich erheitsereignisse. Die Ereignisse werden überwacht, indem detaillierte Aufzeichn ungen über die Anfragen erfasst werden, die an einen Amazon-S3-Bucket gestellt wurden. Jeder Zugriffsprotokolle intrag enthält Details zu einer einzelnen Zugriffsanfrage. Zu den Details gehören Auftraggeber, Bucket-Name, Anforderu ngszeit, Anforderu ngsaktion, Antwortst atus und Fehlercode, falls relevant.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AC-6(10)	AC-6(10) Geringste Berechtigung | Verhinderung der Ausführung privilegierter Funktionen durch nicht privilegierte Benutzer	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) kann Ihnen dabei helfen, die Prinzipien der geringsten Rechte und der Aufgabentrennung in Zugriffsberechtigungen und Autorisierungen zu integrieren und so zu verhindern, dass Richtlinien „Effect“: „Allow“ mit „Action“: „*“ anstelle von „Resource“: „*“ enthalten. Wenn Benutzern mehr Rechte eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und der Aufgabentrennung verstoßen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AC-6(10)	AC-6(10) Geringste Berechtigung | Verhinderung der Ausführung privilegierter Funktionen durch nicht privilegierte Benutzer	iam-root-access-key-überprüfen	Der Zugriff auf Systeme und Ressourcen kann gesteuert werden, indem überprüft wird, ob der Root-Benutzer keine Zugriffsschlüssel mit seiner AWS Identity and Access Management (IAM) -Rolle verknüpft hat. Stellen Sie sicher, dass die Root-Zugriffsschlüssel gelöscht werden. Erstellen und verwenden Sie stattdessen rollenbasierte Funktionen, AWS-Konten um das Prinzip der geringsten Funktionalität zu berücksichtigen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AC-6(10)	AC-6(10) Geringste Berechtigung | Verhinderung der Ausführung privilegierter Funktionen durch nicht privilegierte Benutzer	iam-user-mfa-enabled	Aktivieren Sie diese Regel, um den Zugriff auf Ressourcen in der AWS -Cloud einzuschränken. Diese Regel stellt sicher, dass die Multi-Faktor-Authentifizierung (MFA) für alle Benutzer aktiviert ist. MFA bietet eine weitere Schutzebene zusätzlich zum Benutzernamen und Passwort. Reduzieren Sie Fälle von kompromittierten Konten, indem Sie MFA für Benutzer vorschreiben.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AC-6(10)	AC-6(10) Geringste Berechtigung | Verhinderung der Ausführung privilegierter Funktionen durch nicht privilegierte Benutzer	mfa-enabled-for-iam-Konsolenzugriff	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass MFA für alle AWS Identity and Access Management (IAM) -Benutzer aktiviert ist, die über ein Konsolenkennwort verfügen. MFA sorgt für eine weitere Schutzebene zusätzlich zu den Anmeldeinformationen. Indem Sie MFA für Benutzer vorschreiben, können Sie Fälle kompromittierter Konten reduzieren und verhindern, dass unbefugte Benutzer auf vertrauliche Daten zugreifen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AC-6(10)	AC-6(10) Geringste Berechtigung | Verhinderung der Ausführung privilegierter Funktionen durch nicht privilegierte Benutzer	root-account-mfa-enabled	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass MFA für den Root-Benutzer aktiviert ist. Der Stammbenutzer ist der AWS-Konto-Benutzer mit den meisten Berechtigungen. MFA bietet eine weitere Schutzebene zusätzlich zum Benutzernamen und Passwort. Indem Sie MFA für den Root-Benutzer vorschreiben, können Sie die Anzahl AWS-Konten kompromittierter Benutzer reduzieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AC-6.A	AC-6.A Geringste Berechtigung	dms-replication-not-public	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass auf DMS-Replikationsinstanzen nicht öffentlich zugegriffen werden kann. DMS-Replikations-Instances können vertrauliche Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.
CCCS-fPBMM-AC-6.A	AC-6.A Geringste Berechtigung	ebs-snapshot-public-restorable-überprüfen	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass EBS-Snapshots nicht öffentlich wiederherstellbar sind. EBS-Volume-Snapshots können vertrauliche Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AC-6.A	AC-6.A Geringste Berechtigung	ec2-imdsv2-check	Stellen Sie sicher, dass die Methode Instance Metadata Service Version 2 (IMDSv2) aktiviert ist, um den Zugriff auf und die Kontrolle der Amazon Elastic Compute Cloud (Amazon EC2) - Instance-Metadaten zu schützen. Die IMDSv2 Methode verwendet sitzungsbasierte Kontrollen. Mit können Kontrollen implementiert werden IMDSv2, um Änderungen an Instanzmetadaten einzuschränken.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AC-6.A	AC-6.A Geringste Berechtigung	ec-2 instance-no-public-ip	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon Elastic Compute Cloud (Amazon EC2) - Instances nicht öffentlich zugänglic h sind. EC2Amazon -Instances können vertrauliche Informati onen enthalten, und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AC-6.A	AC-6.A Geringste Berechtigung	ecs-task-definition-user-for-host-mode-check	Wenn für eine Aufgabendefinition erhöhte Berechtigungen gelten, liegt das daran, dass der Kunde diesen Konfigurationen ausdrücklich zugestimmt hat. Diese Kontrolle prüft, ob eine unerwartete Berechtigungseskalation vorliegt, wenn für eine Aufgabendefinition das Host-Netzwerk aktiviert ist, die Kunden aber keine erhöhten Berechtigungen aktiviert haben.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AC-6.A	AC-6.A Geringste Berechtigung	elasticsearch-in-vpc-only	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass sich Amazon OpenSearch OpenSearch Service (Service) - Domains innerhalb einer Amazon Virtual Private Cloud (Amazon VPC) befinden. Eine OpenSearch Service-Domain innerhalb einer Amazon VPC ermöglicht die sichere Kommunikation zwischen OpenSearch Service und anderen Services innerhalb der Amazon VPC, ohne dass ein Internet-Gateway, ein NAT-Gerät oder eine VPN-Verbindung erforderlich ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AC-6.A	AC-6.A Geringste Berechtigung	emr-kerberos-enabled	Die Zugriffsberechtigungen und -autorisierungen können verwaltet und nach den Prinzipien der geringsten Berechtigung und Aufgabentrennung integriert werden, indem Kerberos für Amazon-EMR-Cluster aktiviert wird. In Kerberos werden Services und Benutzer, die sich authentifizieren müssen, als Prinzipale bezeichnet. Prinzipale befinden sich in einem Kerberos-Bereich. Innerhalb dieses Bereichs wird ein Kerberos-Server als Key Distribution Center (KDC) bezeichnet. Über diesen Server können sich Prinzipale authentifizieren. Die Authentifizierung im KDC erfolgt durch die Ausstellung von Authentif

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
			izierungstickets. Das KDC unterhält eine Datenbank der Prinzipale in seinem Bereich mit ihren Passwörtern und anderen administrativen Informationen zu jedem Prinzipal.
CCCS-fPBMM-AC-6.A	AC-6.A Geringste Berechtigung	emr-master-no-public-ip	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon EMR-Cluster-Masterknoten nicht öffentlich zugänglich sind. Amazon-EMR-Cluster-Hauptknoten können vertrauliche Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AC-6.A	AC-6.A Geringste Berechtigung	iam-customer-policy-blocked-kms-Aktionen	AWS Identity and Access Management (IAM) kann Ihnen helfen, die Prinzipien der geringsten Rechte und der Aufgabentrennung in Zugriffsberechtigungen und Autorisierungen zu integrieren und so zu verhindern, dass Richtlinien blockierte Aktionen für alle AWS Schlüssel des Key Management Service enthalten. Wenn Benutzer mehr Rechte haben, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und Aufgabentrennung verstoßen. Mit dieser Regel können Sie den Parameter festlegen. blockedActionsPatterns (Wert „AWS Bewährte grundlegende Sicherheitsmethode

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
			n“: kms: Entschlüs seln, kms:ReEnc ryptFrom). Die tatsächlichen Werte müssen den Richtlini en Ihrer Organisation entsprechen.
CCCS-fPBMM-AC-6.A	AC-6.A Geringste Berechtigung	iam-group-has-users-überprüfen	AWS Identity and Access Managemen t (IAM) kann Ihnen helfen, die Prinzipien der geringsten Rechte und der Aufgabent rennung mit Zugriffsb erechtigungen und Autorisierungen zu integrieren, indem sichergestellt wird, dass IAM-Gruppen mindestens einen Benutzer haben. Die Einteilung von Benutzern in Gruppen auf der Grundlage der ihnen zugewiese nen Berechtigungen oder ihrer Funktion ist eine Möglichkeit, das Prinzip der geringste n Berechtigung zu implementieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AC-6.A	AC-6.A Geringste Berechtigung	iam-inline-policy-blocked-kms-Aktionen	Stellen Sie sicher, dass ein Benutzer, eine IAM-Rolle oder eine IAM-Gruppe (AWS Identity and Access Management) nicht über eine Inline-Richtlinie verfügt, die blockierte Aktionen für alle AWS Schlüssel des Key Management Service zulässt. AWS empfiehlt, verwaltete Richtlinien anstelle von Inline-Richtlinien zu verwenden. Verwaltete Richtlinien ermöglichen Wiederverwendbarkeit, Versionsverwaltung, Rollback und Delegierung der Berechtigungsverwaltung. Mit dieser Regel können Sie den blockedActionsPatterns Parameter festlegen. (Wert „AWS Bewährte grundlegende Sicherheitsmethoden“: kms:Decrypt, kms:ReEncryptFrom). Die

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
			tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.
CCCS-fPBMM-AC-6.A	AC-6.A Geringste Berechtigung	iam-no-inline-policy-überprüfen	Stellen Sie sicher, dass ein Benutzer, eine IAM-Rolle oder eine IAM-Gruppe (AWS Identity and Access Management) nicht über eine Inline-Richtlinie zur Zugriffskontrolle auf Systeme und Ressourcen verfügt. AWS empfiehlt, verwaltete Richtlinien anstelle von Inline-Richtlinien zu verwenden. Verwaltete Richtlinien ermöglichen Wiederverwendbarkeit, Versionsverwaltung, Rollback und Delegierung der Berechtigungsverwaltung.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AC-6.A	AC-6.A Geringste Berechtigung	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) kann Ihnen dabei helfen, die Prinzipien der geringsten Rechte und der Aufgabentrennung in Zugriffsberechtigungen und Autorisierungen zu integrieren und so zu verhindern, dass Richtlinien „Effect“: „Allow“ mit „Action“: „*“ anstelle von „Resource“: „*“ enthalten. Wenn Benutzern mehr Rechte eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und der Aufgabentrennung verstoßen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AC-6.A	AC-6.A Geringste Berechtigung	iam-root-access-key-überprüfen	Der Zugriff auf Systeme und Ressourcen kann gesteuert werden, indem überprüft wird, ob der Root-Benutzer keine Zugriffsschlüssel mit seiner AWS Identity and Access Management (IAM) -Rolle verknüpft hat. Stellen Sie sicher, dass die Root-Zugriffsschlüssel gelöscht werden. Erstellen und verwenden Sie stattdessen rollenbasierte Funktionen, AWS-Konten um das Prinzip der geringsten Funktionalität zu berücksichtigen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AC-6.A	AC-6.A Geringste Berechtigung	iam-user-group-membership-überprüfen	AWS Identity and Access Management (IAM) kann Ihnen helfen, Zugriffsberechtigungen und Autorisierungen einzuschränken, indem sichergestellt wird, dass Benutzer Mitglieder mindestens einer Gruppe sind. Wenn Benutzern mehr Berechtigungen eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und Aufgabentrennung verstoßen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AC-6.A	AC-6.A Geringste Berechtigung	iam-user-no-policies-überprüfen	Diese Regel stellt sicher, dass AWS Identity and Access Management (IAM) -Richtlinien nur Gruppen oder Rollen zugewiesen werden, um den Zugriff auf Systeme und Ressourcen zu kontrollieren. Die Zuweisung von Berechtigungen auf Gruppen- oder Rollenebene trägt dazu bei, die Wahrscheinlichkeit zu verringern, dass eine Identität übermäßige Berechtigungen erhält oder beibehält.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AC-6.A	AC-6.A Geringste Berechtigung	iam-user-unused-credentials-überprüfen	AWS Identity and Access Management (IAM) kann Ihnen bei Zugriffsberechtigungen und Autorisierungen helfen, indem es nach IAM-Passwörtern und Zugriffsschlüsseln sucht, die für einen bestimmten Zeitraum nicht verwendet wurden. Wenn ungenutzte Anmeldeinformationen identifiziert werden, müssen Sie sie deaktivieren und/oder entfernen, da dies gegen das Prinzip der geringsten Berechtigung verstoßen könnte. Für diese Regel müssen Sie einen Wert für das maxCredentialUsage Alter festlegen (Standardkonfiguration: 90). Der tatsächliche Wert muss den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AC-6.A	AC-6.A Geringste Berechtigung	ec2- instances-in-vpc	Stellen Sie Amazon Elastic Compute Cloud (Amazon EC2) -Instances innerhalb einer Amazon Virtual Private Cloud (Amazon VPC) bereit, um eine sichere Kommunika tion zwischen einer Instance und anderen Services innerhalb der Amazon VPC zu ermöglichen, ohne dass ein Internet-Gateway, ein NAT-Gerät oder eine VPN-Verbindung erforderlich ist. Der gesamte Datenverk ehr bleibt sicher in der AWS Cloud. Domains, die sich innerhalb einer VPC befinden, verfügen aufgrund ihrer logischen Isolierun g im Vergleich zu Domains mit öffentlic hen Endpunkten über eine zusätzlic he Sicherheitsebene. Weisen Sie EC2

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
			Amazon-Instances einer Amazon VPC zu, um den Zugriff ordnungsgemäß zu verwalten.
CCCS-fPBMM-AC-6.A	AC-6.A Geringste Berechtigung	internet-gateway-authorized-vpc-nur	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Internet-Gateways nur mit autorisierter Amazon Virtual Private Cloud (Amazon VPC) verbunden sind. Internet-Gateways ermöglichen den bidirektionalen Internetzugang zur und von der Amazon VPC, was möglicher weise zu einem unbefugten Zugriff auf Amazon-VPC-Ressourcen führen kann.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AC-6.A	AC-6.A Geringste Berechtigung	lambda-function-public-access-verboten	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass AWS Lambda-Funktionen nicht öffentlich zugänglich sind. Der öffentliche Zugriff kann möglicherweise die Verfügbarkeit von Ressourcen beeinträchtigen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AC-6.A	AC-6.A Geringste Berechtigung	lambda-inside-vpc	Stellen Sie AWS Lambda-Funktionen in einer Amazon Virtual Private Cloud (Amazon VPC) bereit, um eine sichere Kommunikation zwischen einer Funktion und anderen Diensten innerhalb der Amazon VPC zu gewährleisten. Bei dieser Konfiguration sind kein Internet-Gateway, kein NAT-Gerät und keine VPN-Verbindung erforderlich. Der gesamte Datenverkehr bleibt sicher in der Cloud. AWS Domains, die sich innerhalb einer VPC befinden, verfügen aufgrund ihrer logischen Isolierung im Vergleich zu Domains mit öffentlichen Endpunkten über eine zusätzliche Sicherheitsebene. Um den Zugriff ordnungsgemäß zu verwalten,

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
			sollten AWS Lambda-Funktionen einer VPC zugewiesen werden.
CCCS-fPBMM-AC-6.A	AC-6.A Geringste Berechtigung	opensearch-in-vpc-only	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass sich Amazon OpenSearch Service-Domains innerhalb einer Amazon Virtual Private Cloud (Amazon VPC) befinden. Eine Amazon OpenSearch Service-Domain innerhalb einer Amazon VPC ermöglicht die sichere Kommunikation zwischen Amazon OpenSearch Service und anderen Services innerhalb der Amazon VPC, ohne dass ein Internet-Gateway, ein NAT-Gerät oder eine VPN-Verbindung erforderlich ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AC-6.A	AC-6.A Geringste Berechtigung	rds-instance-public-access-überprüfen	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Relational Database Service (Amazon RDS) -Instances nicht öffentlich sind. Amazon-RDS-Datenbank-Instances können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AC-6.A	AC-6.A Geringste Berechtigung	rds-snapshots-public-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Relational Database Service (Amazon RDS) -Instances nicht öffentlich sind. Amazon-RDS-Datenbank-Instances können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AC-6.A	AC-6.A Geringste Berechtigung	redshift-cluster-public-access-überprüfen	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Redshift Redshift-Cluster nicht öffentlich sind. Amazon-Redshift-Cluster können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AC-6.A	AC-6.A Geringste Berechtigung	s3- -Block-periodisch account-level-public-access	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Simple Storage Service (Amazon S3) -Buckets nicht öffentlich zugänglich sind. Diese Regel trägt dazu bei, sensible Daten vor unbefugten Remote-Benutzern zu schützen, indem sie den öffentlichen Zugriff verhindert. Mit dieser Regel können Sie optional die Parameter ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) und restrictPublicBuckets Parameter (Config Default: True) festlegen. Die tatsächlichen Werte müssen den Richtlini

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
			en Ihrer Organisation entsprechen.
CCCS-fPBMM-AC-6.A	AC-6.A Geringste Berechtigung	s3 bucket-level-public-access - verboten	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Simple Storage Service (Amazon S3) -Buckets nicht öffentlich zugänglich sind. Diese Regel trägt dazu bei, sensible Daten vor unbefugten Remote-Benutzern zu schützen, indem sie den öffentlichen Zugriff auf Bucket-Ebene verhindert.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AC-6.A	AC-6.A Geringste Berechtigung	s-3 bucket-public-read-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie nur autorisierten Benutzern, Prozessen und Geräten Zugriff auf Amazon Simple Storage Service (Amazon S3) - Buckets gewähren. Die Verwaltung des Zugriffs sollte mit der Klassifizierung der Daten übereinst immen.
CCCS-fPBMM-AC-6.A	AC-6.A Geringste Berechtigung	s3- bucket-public-write-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie nur autorisierten Benutzern, Prozessen und Geräten Zugriff auf Amazon Simple Storage Service (Amazon S3) - Buckets gewähren. Die Verwaltung des Zugriffs sollte mit der Klassifizierung der Daten übereinst immen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AC-6.A	AC-6.A Geringste Berechtigung	sagemaker-notebook-no-direct-Internetzugang	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass SageMaker Amazon-Notebooks keinen direkten Internetzugang zulassen. Indem Sie direkten Internetzugang blockieren, vermeiden Sie, dass unbefugte Benutzer auf sensible Daten zugreifen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AC-6.A	AC-6.A Geringste Berechtigung	subnet-auto-assign-public-ip-deaktiviert	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon Virtual Private Cloud (VPC) -Subnetzen nicht automatisch eine öffentliche IP-Adresse zugewiesen wird. Amazon Elastic Compute Cloud (EC2) -Instances, die in Subnetzen gestartet werden, in denen dieses Attribut aktiviert ist, haben ihrer primären Netzwerkschnittstelle eine öffentliche IP-Adresse zugewiesen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AC-17(1)	AC-17(1) Fernzugriff | Automatisierte Überwachung/Steuerung	alb-waf-enabled	Stellen Sie sicher, dass AWS WAF auf Elastic Load Balancers (ELB) aktiviert ist, um Webanwendungen zu schützen. Eine WAF trägt zum Schutz Ihrer Webanwendungen oder APIs vor gängigen Web-Exploits bei. Diese Web-Exploits können sich auf die Verfügbarkeit auswirken, die Sicherheit gefährden oder übermäßige Ressourcen in Ihrer Umgebung verbrauchen.
CCCS-fPBMM-AC-17(1)	AC-17(1) Fernzugriff | Automatisierte Überwachung/Steuerung	api-gw-execution-logging-aktiviert	Die API-Gateway-Protokollierung zeigt detaillierte Ansichten der Benutzer, die auf die API zugegriffen haben, und wie diese Benutzer auf die API zugegriffen haben. Diese Einblicke ermöglichen die Transparenz von Benutzeraktivitäten.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AC-17(1)	AC-17(1) Fernzugriff | Automatisierte Überwachung/Steuerung	cloud-trail-cloud-watch-logs-aktiviert	Verwenden Sie Amazon CloudWatch , um Protokoll ereignisaktivitäten zentral zu sammeln und zu verwalten. Die Aufnahme von AWS CloudTrail Daten liefert Einzelheiten zu den API-Aufrufaktivitäten in Ihrem AWS-Konto.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AC-17(1)	AC-17(1) Fernzugriff | Automatisierte Überwachung/Steuerung	cloudtrail-enabled	AWS CloudTrail kann bei der Nichtabstreitbarkeit helfen, indem Aktionen und API-Aufrufe der AWS Management Console aufgezeichnet werden. Sie können die Benutzer und die Benutzer AWS-Konten , die einen AWS Dienst aufgerufen haben, die Quell-IP-Adresse, über die die Aufrufe generiert wurden, und den Zeitpunkt der Anrufe identifizieren. Einzelheiten zu den erfassten Daten finden Sie unter Inhalt des AWS CloudTrail Datensatzes.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AC-17(1)	AC-17(1) Fernzugriff | Automatisierte Überwachung/Steuerung	dms-replication-not-public	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass auf DMS-Replikationsinstanzen nicht öffentlich zugegriffen werden kann. DMS-Replikations-Instances können vertrauliche Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.
CCCS-fPBMM-AC-17(1)	AC-17(1) Fernzugriff | Automatisierte Überwachung/Steuerung	ebs-snapshot-public-restorable-überprüfen	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass EBS-Snapshots nicht öffentlich wiederherstellbar sind. EBS-Volume-Snapshots können vertrauliche Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AC-17(1)	AC-17(1) Fernzugriff | Automatisierte Überwachung/Steuerung	ec-2 instance-no-public-ip	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon Elastic Compute Cloud (Amazon EC2) - Instances nicht öffentlich zugänglich sind. EC2Amazon -Instances können vertrauliche Informationen enthalten, und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AC-17(1)	AC-17(1) Fernzugriff | Automatisierte Überwachung/Steuerung	elasticsearch-in-vpc-only	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass sich Amazon OpenSearch OpenSearch Service (Service) - Domains innerhalb einer Amazon Virtual Private Cloud (Amazon VPC) befinden. Eine OpenSearch Service-Domain innerhalb einer Amazon VPC ermöglicht die sichere Kommunikation zwischen OpenSearch Service und anderen Services innerhalb der Amazon VPC, ohne dass ein Internet-Gateway, ein NAT-Gerät oder eine VPN-Verbindung erforderlich ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AC-17(1)	AC-17(1) Fernzugriff | Automatisierte Überwachung/Steuerung	elb-logging-enabled	Die Elastic-Load-Balancing-Aktivität ist ein zentraler Kommunikationspunkt innerhalb einer Umgebung. Stellen Sie sicher, dass die ELB-Protokollierung aktiviert ist. Die gesammelten Daten enthalten detaillierte Informationen zu Anfragen, die an den ELB gesendet wurden. Jedes Protokoll enthält Informationen wie die Zeit, zu der die Anforderung einging, die Client-IP-Adresse, Latenzen, Anforderungspfade und Serverantworten.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AC-17(1)	AC-17(1) Fernzugriff | Automatisierte Überwachung/Steuerung	emr-master-no-public-ip	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon EMR-Cluster-Masterknoten nicht öffentlich zugänglich sind. Amazon-EMR-Cluster-Hauptknoten können vertrauliche Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AC-17(1)	AC-17(1) Fernzugriff | Automatisierte Überwachung/Steuerung	guardduty-enabled-centralized	Amazon GuardDuty kann mithilfe von Threat Intelligence Feeds helfen, potenzielle Cybersicherheitsereignisse zu überwachen und zu erkennen. Dazu gehören Listen mit bösartigen IPs und maschinellen Lernmethoden zur Identifizierung unerwarteter, nicht autorisierter und bösartiger Aktivitäten in Ihrer AWS Cloud-Umgebung.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AC-17(1)	AC-17(1) Fernzugriff | Automatisierte Überwachung/Steuerung	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) Security Groups können bei der Verwaltung des Netzwerkzugriffs helfen, indem sie eine statusbehaftete Filterung des ein- und ausgehenden Netzwerkverkehrs zu Ressourcen bereitstellen. AWS Wenn Sie eingehenden (oder entfernten) Datenverkehr von 0.0.0.0/0 bis Port 22 auf Ihren Ressourcen nicht zulassen, können Sie den Remote-Zugriff einschränken.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AC-17(1)	AC-17(1) Fernzugriff | Automatisierte Überwachung/Steuerung	ec-2 instances-in-vpc	Stellen Sie Amazon Elastic Compute Cloud (Amazon EC2) -Instances innerhalb einer Amazon Virtual Private Cloud (Amazon VPC) bereit, um eine sichere Kommunikation zwischen einer Instance und anderen Services innerhalb der Amazon VPC zu ermöglichen, ohne dass ein Internet-Gateway, ein NAT-Gerät oder eine VPN-Verbindung erforderlich ist. Der gesamte Datenverkehr bleibt sicher in der AWS Cloud. Domains, die sich innerhalb einer VPC befinden, verfügen aufgrund ihrer logischen Isolierung im Vergleich zu Domains mit öffentlichen Endpunkten über eine zusätzliche Sicherheitsebene. Weisen Sie EC2

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
			Amazon-Instances einer Amazon VPC zu, um den Zugriff ordnungsgemäß zu verwalten.
CCCS-fPBMM-AC-17(1)	AC-17(1) Fernzugriff | Automatisierte Überwachung/Steuerung	internet-gateway-authorized-vpc-nur	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Internet-Gateways nur mit autorisierter Amazon Virtual Private Cloud (Amazon VPC) verbunden sind. Internet-Gateways ermöglichen den bidirektionalen Internetzugang zur und von der Amazon VPC, was möglicherweise zu einem unbefugten Zugriff auf Amazon-VPC-Ressourcen führen kann.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AC-17(1)	AC-17(1) Fernzugriff | Automatisierte Überwachung/Steuerung	lambda-function-public-access-verboten	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass AWS Lambda-Funktionen nicht öffentlich zugänglich sind. Der öffentliche Zugriff kann möglicherweise die Verfügbarkeit von Ressourcen beeinträchtigen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AC-17(1)	AC-17(1) Fernzugriff | Automatisierte Überwachung/Steuerung	lambda-inside-vpc	Stellen Sie AWS Lambda-Funktionen in einer Amazon Virtual Private Cloud (Amazon VPC) bereit, um eine sichere Kommunikation zwischen einer Funktion und anderen Diensten innerhalb der Amazon VPC zu gewährleisten. Bei dieser Konfiguration sind kein Internet-Gateway, kein NAT-Gerät und keine VPN-Verbindung erforderlich. Der gesamte Datenverkehr bleibt sicher in der Cloud. AWS Domains, die sich innerhalb einer VPC befinden, verfügen aufgrund ihrer logischen Isolierung im Vergleich zu Domains mit öffentlichen Endpunkten über eine zusätzliche Sicherheitsebene. Um den Zugriff ordnungsgemäß zu verwalten,

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
			sollten AWS Lambda-Funktionen einer VPC zugewiesen werden.
CCCS-fPBMM-AC-17(1)	AC-17(1) Fernzugriff | Automatisierte Überwachung/Steuerung	opensearch-in-vpc-only	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass sich Amazon OpenSearch Service-Domains innerhalb einer Amazon Virtual Private Cloud (Amazon VPC) befinden. Eine Amazon OpenSearch Service-Domain innerhalb einer Amazon VPC ermöglicht die sichere Kommunikation zwischen Amazon OpenSearch Service und anderen Services innerhalb der Amazon VPC, ohne dass ein Internet-Gateway, ein NAT-Gerät oder eine VPN-Verbindung erforderlich ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AC-17(1)	AC-17(1) Fernzugriff | Automatisierte Überwachung/Steuerung	rds-instance-public-access-überprüfen	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Relational Database Service (Amazon RDS) -Instances nicht öffentlich sind. Amazon-RDS-Datenbank-Instances können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AC-17(1)	AC-17(1) Fernzugriff | Automatisierte Überwachung/Steuerung	rds-snapshots-public-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Relational Database Service (Amazon RDS) -Instances nicht öffentlich sind. Amazon-RDS-Datenbank-Instances können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AC-17(1)	AC-17(1) Fernzugriff | Automatisierte Überwachung/Steuerung	redshift-cluster-public-access-überprüfen	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Redshift Redshift-Cluster nicht öffentlich sind. Amazon-Redshift-Cluster können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AC-17(1)	AC-17(1) Fernzugriff | Automatisierte Überwachung/Steuerung	restricted-common-ports	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass gemeinsame Ports für Amazon Elastic Compute Cloud (Amazon EC2) -Sicherheitsgruppen eingeschränkt sind. Wenn der Zugriff auf Ports nicht auf vertrauenswürdige Quellen beschränkt wird, kann dies zu Angriffen auf die Verfügbarkeit, Integrität und Vertraulichkeit von Systemen führen. Mit dieser Regel können Sie optional die Parameter blockedPort1–blockedPort5 festlegen (Standardkonfigurationen: 20, 21, 3389, 3306, 4333). Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AC-17(1)	AC-17(1) Fernzugriff | Automatisierte Überwachung/Steuerung	s3- account-level-public-access -blöcke-periodisch	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Simple Storage Service (Amazon S3) -Buckets nicht öffentlich zugänglich sind. Diese Regel trägt dazu bei, sensible Daten vor unbefugten Remote-Benutzern zu schützen, indem sie den öffentlichen Zugriff verhindert. Mit dieser Regel können Sie optional die Parameter ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) und restrictPublicBuckets Parameter (Config Default: True) festlegen. Die tatsächlichen Werte müssen den Richtlini

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
			en Ihrer Organisation entsprechen.
CCCS-fPBMM-AC-17(1)	AC-17(1) Fernzugriff | Automatisierte Überwachung/Steuerung	s3 bucket-level-public-access - verboten	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Simple Storage Service (Amazon S3) -Buckets nicht öffentlich zugänglich sind. Diese Regel trägt dazu bei, sensible Daten vor unbefugten Remote-Benutzern zu schützen, indem sie den öffentlichen Zugriff auf Bucket-Ebene verhindert.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AC-17(1)	AC-17(1) Fernzugriff | Automatisierte Überwachung/Steuerung	s-3 bucket-public-read-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie nur autorisierten Benutzern, Prozessen und Geräten Zugriff auf Amazon Simple Storage Service (Amazon S3) - Buckets gewähren. Die Verwaltung des Zugriffs sollte mit der Klassifizierung der Daten übereinstimmen.
CCCS-fPBMM-AC-17(1)	AC-17(1) Fernzugriff | Automatisierte Überwachung/Steuerung	s3- bucket-public-write-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie nur autorisierten Benutzern, Prozessen und Geräten Zugriff auf Amazon Simple Storage Service (Amazon S3) - Buckets gewähren. Die Verwaltung des Zugriffs sollte mit der Klassifizierung der Daten übereinstimmen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AC-17(1)	AC-17(1) Fernzugriff | Automatisierte Überwachung/Steuerung	sagemaker-notebook-no-direct-Internetzugang	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass SageMaker Amazon-Notebooks keinen direkten Internetzugang zulassen. Indem Sie direkten Internetzugang blockieren, vermeiden Sie, dass unbefugte Benutzer auf sensible Daten zugreifen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AC-17(1)	AC-17(1) Fernzugriff | Automatisierte Überwachung/Steuerung	subnet-auto-assign-public-ip-deaktiviert	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon Virtual Private Cloud (VPC) -Subnetzen nicht automatisch eine öffentliche IP-Adresse zugewiesen wird. Amazon Elastic Compute Cloud (EC2) -Instances, die in Subnetzen gestartet werden, in denen dieses Attribut aktiviert ist, haben ihrer primären Netzwerkschnittstelle eine öffentliche IP-Adresse zugewiesen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AC-17(1)	AC-17(1) Fernzugriff | Automatisierte Überwachung/Steuerung	vpc-default-security-group-geschlossen	Sicherheitsgruppen von Amazon Elastic Compute Cloud (Amazon EC2) können bei der Verwaltung des Netzwerkzugriffs helfen, indem sie eine statusbehaftete Filterung des ein- und ausgehenden Netzwerkverkehrs zu Ressourcen bereitstellen. AWS Die Beschränkung des gesamten Datenverkehrs auf die Standardsicherheitsgruppe hilft dabei, den Fernzugriff auf Ihre Ressourcen einzuschränken. AWS

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AC-17(1)	AC-17(1) Fernzugriff | Automatisierte Überwachung/Steuerung	vpc-flow-logs-enabled	VPC-Flow-Protokolle erfassen detaillierte Informationsdatensätze über den IP-Datenverkehr, der zu und von Netzwerkschnittstellen in Ihrer Amazon Virtual Private Cloud (Amazon VPC) fließt. Standardmäßig enthalten Flow-Protokolldatensätze Werte für die verschiedenen Komponenten des IP-Flows, einschließlich Quelle, Ziel und Protokoll.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AC-17(1)	AC-17(1) Fernzugriff | Automatisierte Überwachung/Steuerung	vpc-sg-open-only-to-authorized-ports	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass gemeinsame Ports für Amazon Elastic Compute Cloud (Amazon EC2) -Sicherheitsgruppen eingeschränkt sind. Wenn der Zugriff auf Ports nicht auf vertrauenswürdige Quellen beschränkt wird, kann dies zu Angriffen auf die Verfügbarkeit, Integrität und Vertraulichkeit von Systemen führen. Durch die Beschränkung des Zugriffs auf Ressourcen innerhalb einer Sicherheitsgruppe aus dem Internet (0.0.0.0/0) kann der Fernzugriff auf interne Systeme gesteuert werden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AC-17(1)	AC-17(1) Fernzugriff | Automatisierte Überwachung/Steuerung	wafv2-logging-enabled	Um die Protokollierung und Überwachung in Ihrer Umgebung zu erleichtern, aktivieren Sie die AWS WAF (V2) -Protokollierung im regionalen und globalen Web ACLs. AWS Die WAF-Protokollierung bietet detaillierte Informationen über den Datenverkehr, der von Ihrer Web-ACL analysiert wird. In den Protokollen werden die Uhrzeit aufgezeichnet, zu der die AWS WAF die Anfrage von Ihrer AWS Ressource erhalten hat, Informationen zu der Anfrage und eine Aktion für die Regel, der jede Anfrage entsprach.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AC-17(2)	AC-17(2) Fernzugriff | Schutz von Vertraulichkeit/Integrität durch Verschlüsselung	alb-http-to-https-Umleitungsprüfung	Um Daten während der Übertragung zu schützen, stellen Sie sicher, dass Ihr Application Load Balancer unverschlüsselte HTTP-Anfragen automatisch an HTTPS umleitet. Da sensible Daten vorhanden sein können, sollten Sie die Verschlüsselung bei der Übertragung aktivieren, um diese Daten zu schützen.
CCCS-fPBMM-AC-17(2)	AC-17(2) Fernzugriff | Schutz von Vertraulichkeit/Integrität durch Verschlüsselung	api-gw-ssl-enabled	Stellen Sie sicher, dass die REST-API-Stufen von Amazon API Gateway mit SSL-Zertifikaten konfiguriert sind, damit Backend-Systeme überprüfen können, ob Anforderungen von API Gateway stammen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AC-17(2)	AC-17(2) Fernzugriff | Schutz von Vertraulichkeit/Integrität durch Verschlüsselung	elb-acm-certificate-required	Zum Schutz von eventuell vorhandenen sensiblen Daten sowie von Daten während der Übertragung muss die Verschlüsselung für Ihr Elastic Load Balancing aktiviert sein. Verwenden Sie AWS Certificate Manager, um öffentliche und private SSL/TLS-Zertifikate mit AWS Diensten und internen Ressourcen zu verwalten, bereitzustellen und bereitzustellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AC-17(2)	AC-17(2) Fernzugriff | Schutz von Vertraulichkeit/Integrität durch Verschlüsselung	elb-predefined-security-policy-ssl-check	Stellen Sie sicher, dass Ihre SSL-Listener von Classic Elastic Load Balancing eine vordefinierte Sicherheitsrichtlinie verwenden, um Daten während der Übertragung zu schützen. Elastic Load Balancing bietet vordefinierte Aushandlungskonfigurationen, die für die SSL-Aushandlung verwendet werden, wenn eine Verbindung zwischen einem Client und Ihrem Load Balancer hergestellt wurde. Die SSL-Aushandlungskonfigurationen sind mit einer breiten Palette von Clients kompatibel und verwenden hochfeste kryptografische Algorithmen. Diese Regel verlangt, dass Sie eine vordefinierte Sicherheitsrichtlinie für Ihre SSL-Liste

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
			ner festlegen. Die Standard-Sicherheitsrichtlinie lautet: Policy-TLS-1-2-2017-0. ELBSecurity Der tatsächliche Wert muss den Richtlinien Ihrer Organisation entsprechen.
CCCS-fPBMM-AC-17(2)	AC-17(2) Fernzugriff | Schutz von Vertraulichkeit/Integrität durch Verschlüsselung	elb-tls-https-listeners-nur	Stellen Sie sicher, dass Ihre Elastic Load Balancer (ELBs) mit SSL- oder HTTPS-Listenern konfiguriert sind. Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AC-17(2)	AC-17(2) Fernzugriff | Schutz von Vertraulichkeit/Integrität durch Verschlüsselung	s-3 bucket-ssl-requests-only	Um Daten während der Übertragung zu schützen, stellen Sie sicher, dass Ihre Amazon Simple Storage Service (Amazon S3)-Buckets Anfragen zur Verwendung von Secure Socket Layer (SSL)-Buckets erfordern. Da sensible Daten vorhanden sein können, sollten Sie die Verschlüsselung bei der Übertragung aktivieren, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AC-17(3)	AC-17(3) Fernzugriff | Verwaltete Zugriffskontrollpunkte	internet-gateway-authorized-vpc-nur	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Internet-Gateways nur mit autorisierter Amazon Virtual Private Cloud (Amazon VPC) verbunden sind. Internet-Gateways ermöglichen den bidirektionalen Internetzugang zur und von der Amazon VPC, was möglicherweise zu einem unbefugten Zugriff auf Amazon-VPC-Ressourcen führen kann.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AC-17(4)	AC-17(4) Fernzugriff | Privilegierter Befehl/Zugriff	iam-user-mfa-enabled	Aktivieren Sie diese Regel, um den Zugriff auf Ressourcen in der AWS -Cloud einzuschränken. Diese Regel stellt sicher, dass die Multi-Faktor-Authentifizierung (MFA) für alle Benutzer aktiviert ist. MFA bietet eine weitere Schutzebene zusätzlich zum Benutzernamen und Passwort. Reduzieren Sie Fälle von kompromittierten Konten, indem Sie MFA für Benutzer vorschreiben.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AC-17(4)	AC-17(4) Fernzugriff | Privilegierter Befehl/Zugriff	mfa-enabled-for-iam-Konsolenzugriff	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass MFA für alle AWS Identity and Access Management (IAM) -Benutzer aktiviert ist, die über ein Konsolenkennwort verfügen. MFA sorgt für eine weitere Schutzebene zusätzlich zu den Anmeldeinformationen. Indem Sie MFA für Benutzer vorschreiben, können Sie Fälle kompromittierter Konten reduzieren und verhindern, dass unbefugte Benutzer auf vertrauliche Daten zugreifen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AC-17(4)	AC-17(4) Fernzugriff | Privilegierter Befehl/Zugriff	root-account-mfa-enabled	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass MFA für den Root-Benutzer aktiviert ist. Der Stammbenutzer ist der AWS-Konto-Benutzer mit den meisten Berechtigungen. MFA bietet eine weitere Schutzebene zusätzlich zum Benutzernamen und Passwort. Indem Sie MFA für den Root-Benutzer vorschreiben, können Sie die Anzahl AWS-Konten kompromittierter Benutzer reduzieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AC-17.A	AC-17.A Fernzugriff	dms-replication-not-public	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass auf DMS-Replikationsinstanzen nicht öffentlich zugegriffen werden kann. DMS-Replikations-Instances können vertrauliche Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.
CCCS-fPBMM-AC-17.A	AC-17.A Fernzugriff	ebs-snapshot-public-restorable-überprüfen	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass EBS-Snapshots nicht öffentlich wiederherstellbar sind. EBS-Volume-Snapshots können vertrauliche Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AC-17.A	AC-17.A Fernzugriff	ec-2 instance-no-public-ip	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon Elastic Compute Cloud (Amazon EC2) - Instances nicht öffentlich zugänglic h sind. EC2Amazon -Instances können vertrauliche Informati onen enthalten, und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AC-17.A	AC-17.A Fernzugriff	elasticsearch-in-vpc-only	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass sich Amazon OpenSearch OpenSearch Service (Service) - Domains innerhalb einer Amazon Virtual Private Cloud (Amazon VPC) befinden. Eine OpenSearch Service-Domain innerhalb einer Amazon VPC ermöglicht die sichere Kommunikation zwischen OpenSearch Service und anderen Services innerhalb der Amazon VPC, ohne dass ein Internet-Gateway, ein NAT-Gerät oder eine VPN-Verbindung erforderlich ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AC-17.A	AC-17.A Fernzugriff	emr-master-no-public-ip	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon EMR-Cluster-Masterknoten nicht öffentlich zugänglich sind. Amazon-EMR-Cluster-Hauptknoten können vertrauliche Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AC-17.A	AC-17.A Fernzugriff	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) Security Groups können bei der Verwaltung des Netzwerkzugriffs helfen, indem sie eine statusbehaftete Filterung des ein- und ausgehenden Netzwerkverkehrs zu Ressourcen bereitstellen. AWS Wenn Sie eingehenden (oder entfernten) Datenverkehr von 0.0.0.0/0 bis Port 22 auf Ihren Ressourcen nicht zulassen, können Sie den Remote-Zugriff einschränken.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AC-17.A	AC-17.A Fernzugriff	ec-2 instances-in-vpc	Stellen Sie Amazon Elastic Compute Cloud (Amazon EC2) -Instances innerhalb einer Amazon Virtual Private Cloud (Amazon VPC) bereit, um eine sichere Kommunikation zwischen einer Instance und anderen Services innerhalb der Amazon VPC zu ermöglichen, ohne dass ein Internet-Gateway, ein NAT-Gerät oder eine VPN-Verbindung erforderlich ist. Der gesamte Datenverkehr bleibt sicher in der AWS Cloud. Domains, die sich innerhalb einer VPC befinden, verfügen aufgrund ihrer logischen Isolierung im Vergleich zu Domains mit öffentlichen Endpunkten über eine zusätzliche Sicherheitsebene. Weisen Sie EC2

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
			Amazon-Instances einer Amazon VPC zu, um den Zugriff ordnungsgemäß zu verwalten.
CCCS-fPBMM-AC-17.A	AC-17.A Fernzugriff	internet-gateway-authorized-vpc-nur	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Internet-Gateways nur mit autorisierter Amazon Virtual Private Cloud (Amazon VPC) verbunden sind. Internet-Gateways ermöglichen den bidirektionalen Internetzugang zur und von der Amazon VPC, was möglicher weise zu einem unbefugten Zugriff auf Amazon-VPC-Ressourcen führen kann.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AC-17.A	AC-17.A Fernzugriff	lambda-function-public-access-verboten	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass AWS Lambda-Funktionen nicht öffentlich zugänglich sind. Der öffentliche Zugriff kann möglicherweise die Verfügbarkeit von Ressourcen beeinträchtigen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AC-17.A	AC-17.A Fernzugriff	lambda-inside-vpc	Stellen Sie AWS Lambda-Funktionen in einer Amazon Virtual Private Cloud (Amazon VPC) bereit, um eine sichere Kommunika tion zwischen einer Funktion und anderen Diensten innerhalb der Amazon VPC zu gewährleisten. Bei dieser Konfiguration sind kein Internet-Gateway, kein NAT-Gerät und keine VPN-Verbindung erforderlich. Der gesamte Datenverk ehr bleibt sicher in der Cloud. AWS Domains, die sich innerhalb einer VPC befinden, verfügen aufgrund ihrer logischen Isolierun g im Vergleich zu Domains mit öffentlic hen Endpunkten über eine zusätzliche Sicherheitsebene. Um den Zugriff ordnungsg emäß zu verwalten,

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
			sollten AWS Lambda-Funktionen einer VPC zugewiesen werden.
CCCS-fPBMM-AC-17.A	AC-17.A Fernzugriff	opensearch-in-vpc-only	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass sich Amazon OpenSearch Service-Domains innerhalb einer Amazon Virtual Private Cloud (Amazon VPC) befinden. Eine Amazon OpenSearch Service-Domain innerhalb einer Amazon VPC ermöglicht die sichere Kommunikation zwischen Amazon OpenSearch Service und anderen Services innerhalb der Amazon VPC, ohne dass ein Internet-Gateway, ein NAT-Gerät oder eine VPN-Verbindung erforderlich ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AC-17.A	AC-17.A Fernzugriff	rds-instance-public-access-überprüfen	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Relational Database Service (Amazon RDS) -Instances nicht öffentlich sind. Amazon-RDS-Datenbank-Instances können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AC-17.A	AC-17.A Fernzugriff	rds-snapshots-public-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Relational Database Service (Amazon RDS) -Instances nicht öffentlich sind. Amazon-RDS-Datenbank-Instances können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AC-17.A	AC-17.A Fernzugriff	redshift-cluster-public-access-überprüfen	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Redshift Redshift-Cluster nicht öffentlich sind. Amazon-Redshift-Cluster können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AC-17.A	AC-17.A Fernzugriff	restricted-common-ports	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass gemeinsame Ports für Amazon Elastic Compute Cloud (Amazon EC2) -Sicherheitsgruppen eingeschränkt sind. Wenn der Zugriff auf Ports nicht auf vertrauenswürdige Quellen beschränkt wird, kann dies zu Angriffen auf die Verfügbarkeit, Integrität und Vertraulichkeit von Systemen führen. Mit dieser Regel können Sie optional die Parameter blockedPort1–blockedPort5 festlegen (Standardkonfigurationen: 20, 21, 3389, 3306, 4333). Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AC-17.A	AC-17.A Fernzugriff	s3- account-level-public-access -blöcke-periodisch	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Simple Storage Service (Amazon S3) -Buckets nicht öffentlich zugänglich sind. Diese Regel trägt dazu bei, sensible Daten vor unbefugten Remote-Benutzern zu schützen, indem sie den öffentlichen Zugriff verhindert. Mit dieser Regel können Sie optional die Parameter ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) und restrictPublicBuckets Parameter (Config Default: True) festlegen. Die tatsächlichen Werte müssen den Richtlini

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
			en Ihrer Organisation entsprechen.
CCCS-fPBMM-AC-17.A	AC-17.A Fernzugriff	s3 bucket-level-public-access - verboten	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Simple Storage Service (Amazon S3) -Buckets nicht öffentlich zugänglich sind. Diese Regel trägt dazu bei, sensible Daten vor unbefugten Remote-Benutzern zu schützen, indem sie den öffentlichen Zugriff auf Bucket-Ebene verhindert.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AC-17.A	AC-17.A Fernzugriff	s-3 bucket-public-read-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie nur autorisierten Benutzern, Prozessen und Geräten Zugriff auf Amazon Simple Storage Service (Amazon S3) - Buckets gewähren. Die Verwaltung des Zugriffs sollte mit der Klassifizierung der Daten übereinst immen.
CCCS-fPBMM-AC-17.A	AC-17.A Fernzugriff	s3- bucket-public-write-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie nur autorisierten Benutzern, Prozessen und Geräten Zugriff auf Amazon Simple Storage Service (Amazon S3) - Buckets gewähren. Die Verwaltung des Zugriffs sollte mit der Klassifizierung der Daten übereinst immen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AC-17.A	AC-17.A Fernzugriff	sagemaker-notebook-no-direct-Internetzugang	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass SageMaker Amazon-Notebooks keinen direkten Internetzugang zulassen. Indem Sie direkten Internetzugang blockieren, vermeiden Sie, dass unbefugte Benutzer auf sensible Daten zugreifen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AC-17.A	AC-17.A Fernzugriff	subnet-auto-assign-public-ip-deaktiviert	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon Virtual Private Cloud (VPC) -Subnetzen nicht automatisch eine öffentliche IP-Adresse zugewiesen wird. Amazon Elastic Compute Cloud (EC2) -Instances, die in Subnetzen gestartet werden, in denen dieses Attribut aktiviert ist, haben ihrer primären Netzwerkschnittstelle eine öffentliche IP-Adresse zugewiesen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AC-17.A	AC-17.A Fernzugriff	vpc-default-security-group-geschlossen	Sicherheitsgruppen von Amazon Elastic Compute Cloud (Amazon EC2) können bei der Verwaltung des Netzwerkzugriffs helfen, indem sie eine statusbehaftete Filterung des ein- und ausgehenden Netzwerkverkehrs zu Ressourcen bereitstellen. AWS Die Beschränk ung des gesamten Datenverkehrs auf die Standardsicherheit sgruppe hilft dabei, den Fernzugriff auf Ihre Ressourcen einzuschränken. AWS

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AC-17.A	AC-17.A Fernzugriff	vpc-sg-open-only-to-authorized-ports	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass gemeinsame Ports für Amazon Elastic Compute Cloud (Amazon EC2) -Sicherheitsgruppen eingeschränkt sind. Wenn der Zugriff auf Ports nicht auf vertrauenswürdige Quellen beschränkt wird, kann dies zu Angriffen auf die Verfügbarkeit, Integrität und Vertraulichkeit von Systemen führen. Durch die Beschränkung des Zugriffs auf Ressourcen innerhalb einer Sicherheitsgruppe aus dem Internet (0.0.0.0/0) kann der Fernzugriff auf interne Systeme gesteuert werden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AC-17.AA	AC-17.AA Fernzugriff	dms-replication-not-public	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass auf DMS-Replikationsinstanzen nicht öffentlich zugegriffen werden kann. DMS-Replikations-Instances können vertrauliche Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.
CCCS-fPBMM-AC-17.AA	AC-17.AA Fernzugriff	ebs-snapshot-public-restorable-überprüfen	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass EBS-Snapshots nicht öffentlich wiederherstellbar sind. EBS-Volume-Snapshots können vertrauliche Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AC-17.AA	AC-17.AA Fernzugriff	ec-2 instance-no-public-ip	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon Elastic Compute Cloud (Amazon EC2) - Instances nicht öffentlich zugänglic h sind. EC2Amazon -Instances können vertrauliche Informati onen enthalten, und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AC-17.AA	AC-17.AA Fernzugriff	elasticsearch-in-vpc-only	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass sich Amazon OpenSearch OpenSearch Service (Service) - Domains innerhalb einer Amazon Virtual Private Cloud (Amazon VPC) befinden. Eine OpenSearch Service-Domain innerhalb einer Amazon VPC ermöglicht die sichere Kommunikation zwischen OpenSearch Service und anderen Services innerhalb der Amazon VPC, ohne dass ein Internet-Gateway, ein NAT-Gerät oder eine VPN-Verbindung erforderlich ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AC-17.AA	AC-17.AA Fernzugriff	emr-master-no-public-ip	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon EMR-Cluster-Masterknoten nicht öffentlich zugänglich sind. Amazon-EMR-Cluster-Hauptknoten können vertrauliche Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AC-17.AA	AC-17.AA Fernzugriff	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) Security Groups können bei der Verwaltung des Netzwerkzugriffs helfen, indem sie eine statusbehaftete Filterung des ein- und ausgehenden Netzwerkverkehrs zu Ressourcen bereitstellen. AWS Wenn Sie eingehenden (oder entfernten) Datenverkehr von 0.0.0.0/0 bis Port 22 auf Ihren Ressourcen nicht zulassen, können Sie den Remote-Zugriff einschränken.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AC-17.AA	AC-17.AA Fernzugriff	ec-2 instances-in-vpc	Stellen Sie Amazon Elastic Compute Cloud (Amazon EC2) -Instances innerhalb einer Amazon Virtual Private Cloud (Amazon VPC) bereit, um eine sichere Kommunika tion zwischen einer Instance und anderen Services innerhalb der Amazon VPC zu ermöglichen, ohne dass ein Internet-Gateway, ein NAT-Gerät oder eine VPN-Verbindung erforderlich ist. Der gesamte Datenverk ehr bleibt sicher in der AWS Cloud. Domains, die sich innerhalb einer VPC befinden, verfügen aufgrund ihrer logischen Isolierun g im Vergleich zu Domains mit öffentlic hen Endpunkten über eine zusätzlic he Sicherheitsebene. Weisen Sie EC2

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
			Amazon-Instances einer Amazon VPC zu, um den Zugriff ordnungsgemäß zu verwalten.
CCCS-fPBMM-AC-17.AA	AC-17.AA Fernzugriff	internet-gateway-authorized-vpc-nur	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Internet-Gateways nur mit autorisierter Amazon Virtual Private Cloud (Amazon VPC) verbunden sind. Internet-Gateways ermöglichen den bidirektionalen Internetzugang zur und von der Amazon VPC, was möglicher weise zu einem unbefugten Zugriff auf Amazon-VPC-Ressourcen führen kann.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AC-17.AA	AC-17.AA Fernzugriff	lambda-function-public-access-verboten	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass AWS Lambda-Funktionen nicht öffentlich zugänglich sind. Der öffentliche Zugriff kann möglicherweise die Verfügbarkeit von Ressourcen beeinträchtigen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AC-17.AA	AC-17.AA Fernzugriff	lambda-inside-vpc	Stellen Sie AWS Lambda-Funktionen in einer Amazon Virtual Private Cloud (Amazon VPC) bereit, um eine sichere Kommunika tion zwischen einer Funktion und anderen Diensten innerhalb der Amazon VPC zu gewährleisten. Bei dieser Konfiguration sind kein Internet-Gateway, kein NAT-Gerät und keine VPN-Verbindung erforderlich. Der gesamte Datenverk ehr bleibt sicher in der Cloud. AWS Domains, die sich innerhalb einer VPC befinden, verfügen aufgrund ihrer logischen Isolierun g im Vergleich zu Domains mit öffentlic hen Endpunkten über eine zusätzliche Sicherheitsebene. Um den Zugriff ordnungsg emäß zu verwalten,

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
			sollten AWS Lambda-Funktionen einer VPC zugewiesen werden.
CCCS-fPBMM-AC-17.AA	AC-17.AA Fernzugriff	opensearch-in-vpc-only	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass sich Amazon OpenSearch Service-Domains innerhalb einer Amazon Virtual Private Cloud (Amazon VPC) befinden. Eine Amazon OpenSearch Service-Domain innerhalb einer Amazon VPC ermöglicht die sichere Kommunikation zwischen Amazon OpenSearch Service und anderen Services innerhalb der Amazon VPC, ohne dass ein Internet-Gateway, ein NAT-Gerät oder eine VPN-Verbindung erforderlich ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AC-17.AA	AC-17.AA Fernzugriff	rds-instance-public-access-überprüfen	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Relational Database Service (Amazon RDS) -Instances nicht öffentlich sind. Amazon-RDS-Datenbank-Instances können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AC-17.AA	AC-17.AA Fernzugriff	rds-snapshots-public-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Relational Database Service (Amazon RDS) -Instances nicht öffentlich sind. Amazon-RDS-Datenbank-Instances können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AC-17.AA	AC-17.AA Fernzugriff	redshift-cluster-public-access-überprüfen	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Redshift Redshift-Cluster nicht öffentlich sind. Amazon-Redshift-Cluster können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AC-17.AA	AC-17.AA Fernzugriff	restricted-common-ports	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass gemeinsame Ports für Amazon Elastic Compute Cloud (Amazon EC2) -Sicherheitsgruppen eingeschränkt sind. Wenn der Zugriff auf Ports nicht auf vertrauenswürdige Quellen beschränkt wird, kann dies zu Angriffen auf die Verfügbarkeit, Integrität und Vertraulichkeit von Systemen führen. Mit dieser Regel können Sie optional die Parameter blockedPort1–blockedPort5 festlegen (Standardkonfigurationen: 20, 21, 3389, 3306, 4333). Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AC-17.AA	AC-17.AA Fernzugriff	s3- account-level-public-access -blöcke-periodisch	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Simple Storage Service (Amazon S3) -Buckets nicht öffentlich zugänglich sind. Diese Regel trägt dazu bei, sensible Daten vor unbefugten Remote-Benutzern zu schützen, indem sie den öffentlichen Zugriff verhindert. Mit dieser Regel können Sie optional die Parameter ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) und restrictPublicBuckets Parameter (Config Default: True) festlegen. Die tatsächlichen Werte müssen den Richtlini

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
			en Ihrer Organisation entsprechen.
CCCS-fPBMM-AC-17.AA	AC-17.AA Fernzugriff	s3 bucket-level-public-access - verboten	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Simple Storage Service (Amazon S3) -Buckets nicht öffentlich zugänglich sind. Diese Regel trägt dazu bei, sensible Daten vor unbefugten Remote-Benutzern zu schützen, indem sie den öffentlichen Zugriff auf Bucket-Ebene verhindert.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AC-17.AA	AC-17.AA Fernzugriff	s-3 bucket-public-read-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie nur autorisierten Benutzern, Prozessen und Geräten Zugriff auf Amazon Simple Storage Service (Amazon S3) - Buckets gewähren. Die Verwaltung des Zugriffs sollte mit der Klassifizierung der Daten übereinst immen.
CCCS-fPBMM-AC-17.AA	AC-17.AA Fernzugriff	s3- bucket-public-write-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie nur autorisierten Benutzern, Prozessen und Geräten Zugriff auf Amazon Simple Storage Service (Amazon S3) - Buckets gewähren. Die Verwaltung des Zugriffs sollte mit der Klassifizierung der Daten übereinst immen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AC-17.AA	AC-17.AA Fernzugriff	sagemaker-notebook-no-direct-Internetzugang	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass SageMaker Amazon-Notebooks keinen direkten Internetzugang zulassen. Indem Sie direkten Internetzugang blockieren, vermeiden Sie, dass unbefugte Benutzer auf sensible Daten zugreifen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AC-17.AA	AC-17.AA Fernzugriff	subnet-auto-assign-public-ip-deaktiviert	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon Virtual Private Cloud (VPC) -Subnetzen nicht automatisch eine öffentliche IP-Adresse zugewiesen wird. Amazon Elastic Compute Cloud (EC2) -Instances, die in Subnetzen gestartet werden, in denen dieses Attribut aktiviert ist, haben ihrer primären Netzwerkschnittstelle eine öffentliche IP-Adresse zugewiesen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AC-17.AA	AC-17.AA Fernzugriff	vpc-default-security-group-geschlossen	Sicherheitsgruppen von Amazon Elastic Compute Cloud (Amazon EC2) können bei der Verwaltung des Netzwerkzugriffs helfen, indem sie eine statusbehaftete Filterung des ein- und ausgehenden Netzwerkverkehrs zu Ressourcen bereitstellen. AWS Die Beschränk ung des gesamten Datenverkehrs auf die Standardsicherheit sgruppe hilft dabei, den Fernzugriff auf Ihre Ressourcen einzuschränken. AWS

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AC-17.AA	AC-17.AA Fernzugriff	vpc-sg-open-only-to-authorized-ports	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass gemeinsame Ports für Amazon Elastic Compute Cloud (Amazon EC2) -Sicherheitsgruppen eingeschränkt sind. Wenn der Zugriff auf Ports nicht auf vertrauenswürdige Quellen beschränkt wird, kann dies zu Angriffen auf die Verfügbarkeit, Integrität und Vertraulichkeit von Systemen führen. Durch die Beschränkung des Zugriffs auf Ressourcen innerhalb einer Sicherheitsgruppe aus dem Internet (0.0.0.0/0) kann der Fernzugriff auf interne Systeme gesteuert werden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AC-17.B	AC-17.B Fernzugriff	dms-replication-not-public	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass auf DMS-Replikationsin stanzen nicht öffentlic h zugegriffen werden kann. DMS-Repli kations-Instances können vertrauli che Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.
CCCS-fPBMM-AC-17.B	AC-17.B Fernzugriff	ebs-snapshot-public-restorable-überprüfen	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass EBS-Snapshots nicht öffentlich wiederher stellbar sind. EBS-Volume-Snapsho ts können vertrauli che Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AC-17.B	AC-17.B Fernzugriff	ec-2 instance-no-public-ip	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon Elastic Compute Cloud (Amazon EC2) - Instances nicht öffentlich zugänglic h sind. EC2Amazon -Instances können vertrauliche Informati onen enthalten, und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AC-17.B	AC-17.B Fernzugriff	elasticsearch-in-vpc-only	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass sich Amazon OpenSearch OpenSearch Service (Service) - Domains innerhalb einer Amazon Virtual Private Cloud (Amazon VPC) befinden. Eine OpenSearch Service-Domain innerhalb einer Amazon VPC ermöglicht die sichere Kommunikation zwischen OpenSearch Service und anderen Services innerhalb der Amazon VPC, ohne dass ein Internet-Gateway, ein NAT-Gerät oder eine VPN-Verbindung erforderlich ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AC-17.B	AC-17.B Fernzugriff	emr-master-no-public-ip	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon EMR-Cluster-Masterknoten nicht öffentlich zugänglich sind. Amazon-EMR-Cluster-Hauptknoten können vertrauliche Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AC-17.B	AC-17.B Fernzugriff	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) Security Groups können bei der Verwaltung des Netzwerkzugriffs helfen, indem sie eine statusbehaftete Filterung des ein- und ausgehenden Netzwerkverkehrs zu Ressourcen bereitstellen. AWS Wenn Sie eingehenden (oder entfernten) Datenverkehr von 0.0.0.0/0 bis Port 22 auf Ihren Ressourcen nicht zulassen, können Sie den Remote-Zugriff einschränken.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AC-17.B	AC-17.B Fernzugriff	ec-2 instances-in-vpc	Stellen Sie Amazon Elastic Compute Cloud (Amazon EC2) -Instances innerhalb einer Amazon Virtual Private Cloud (Amazon VPC) bereit, um eine sichere Kommunikation zwischen einer Instance und anderen Services innerhalb der Amazon VPC zu ermöglichen, ohne dass ein Internet-Gateway, ein NAT-Gerät oder eine VPN-Verbindung erforderlich ist. Der gesamte Datenverkehr bleibt sicher in der AWS Cloud. Domains, die sich innerhalb einer VPC befinden, verfügen aufgrund ihrer logischen Isolierung im Vergleich zu Domains mit öffentlichen Endpunkten über eine zusätzliche Sicherheitsebene. Weisen Sie EC2

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
			Amazon-Instances einer Amazon VPC zu, um den Zugriff ordnungsgemäß zu verwalten.
CCCS-fPBMM-AC-17.B	AC-17.B Fernzugriff	internet-gateway-authorized-vpc-nur	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Internet-Gateways nur mit autorisierter Amazon Virtual Private Cloud (Amazon VPC) verbunden sind. Internet-Gateways ermöglichen den bidirektionalen Internetzugang zur und von der Amazon VPC, was möglicher weise zu einem unbefugten Zugriff auf Amazon-VPC-Ressourcen führen kann.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AC-17.B	AC-17.B Fernzugriff	lambda-function-public-access-verboten	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass AWS Lambda-Funktionen nicht öffentlich zugänglich sind. Der öffentliche Zugriff kann möglicherweise die Verfügbarkeit von Ressourcen beeinträchtigen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AC-17.B	AC-17.B Fernzugriff	lambda-inside-vpc	Stellen Sie AWS Lambda-Funktionen in einer Amazon Virtual Private Cloud (Amazon VPC) bereit, um eine sichere Kommunika tion zwischen einer Funktion und anderen Diensten innerhalb der Amazon VPC zu gewährleisten. Bei dieser Konfiguration sind kein Internet-Gateway, kein NAT-Gerät und keine VPN-Verbindung erforderlich. Der gesamte Datenverk ehr bleibt sicher in der Cloud. AWS Domains, die sich innerhalb einer VPC befinden, verfügen aufgrund ihrer logischen Isolierun g im Vergleich zu Domains mit öffentlic hen Endpunkten über eine zusätzliche Sicherheitsebene. Um den Zugriff ordnungsg emäß zu verwalten,

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
			sollten AWS Lambda-Funktionen einer VPC zugewiesen werden.
CCCS-fPBMM-AC-17.B	AC-17.B Fernzugriff	opensearch-in-vpc-only	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass sich Amazon OpenSearch Service-Domains innerhalb einer Amazon Virtual Private Cloud (Amazon VPC) befinden. Eine Amazon OpenSearch Service-Domain innerhalb einer Amazon VPC ermöglicht die sichere Kommunikation zwischen Amazon OpenSearch Service und anderen Services innerhalb der Amazon VPC, ohne dass ein Internet-Gateway, ein NAT-Gerät oder eine VPN-Verbindung erforderlich ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AC-17.B	AC-17.B Fernzugriff	rds-instance-public-access-überprüfen	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Relational Database Service (Amazon RDS) -Instances nicht öffentlich sind. Amazon-RDS-Datenbank-Instances können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AC-17.B	AC-17.B Fernzugriff	rds-snapshots-public-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Relational Database Service (Amazon RDS) -Instances nicht öffentlich sind. Amazon-RDS-Datenbank-Instances können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AC-17.B	AC-17.B Fernzugriff	redshift-cluster-public-access-überprüfen	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Redshift Redshift-Cluster nicht öffentlich sind. Amazon-Redshift-Cluster können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AC-17.B	AC-17.B Fernzugriff	restricted-common-ports	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass gemeinsame Ports für Amazon Elastic Compute Cloud (Amazon EC2) -Sicherheitsgruppen eingeschränkt sind. Wenn der Zugriff auf Ports nicht auf vertrauenswürdige Quellen beschränkt wird, kann dies zu Angriffen auf die Verfügbarkeit, Integrität und Vertraulichkeit von Systemen führen. Mit dieser Regel können Sie optional die Parameter blockedPort1–blockedPort5 festlegen (Standardkonfigurationen: 20, 21, 3389, 3306, 4333). Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AC-17.B	AC-17.B Fernzugriff	s3- account-level-public-access -blöcke-periodisch	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Simple Storage Service (Amazon S3) -Buckets nicht öffentlich zugänglich sind. Diese Regel trägt dazu bei, sensible Daten vor unbefugten Remote-Benutzern zu schützen, indem sie den öffentlichen Zugriff verhindert. Mit dieser Regel können Sie optional die Parameter ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) und restrictPublicBuckets Parameter (Config Default: True) festlegen. Die tatsächlichen Werte müssen den Richtlini

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
			en Ihrer Organisation entsprechen.
CCCS-fPBMM-AC-17.B	AC-17.B Fernzugriff	s3 bucket-level-public-access - verboten	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Simple Storage Service (Amazon S3) -Buckets nicht öffentlich zugänglich sind. Diese Regel trägt dazu bei, sensible Daten vor unbefugten Remote-Benutzern zu schützen, indem sie den öffentlichen Zugriff auf Bucket-Ebene verhindert.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AC-17.B	AC-17.B Fernzugriff	s-3 bucket-public-read-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie nur autorisierten Benutzern, Prozessen und Geräten Zugriff auf Amazon Simple Storage Service (Amazon S3) - Buckets gewähren. Die Verwaltung des Zugriffs sollte mit der Klassifizierung der Daten übereinst immen.
CCCS-fPBMM-AC-17.B	AC-17.B Fernzugriff	s3- bucket-public-write-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie nur autorisierten Benutzern, Prozessen und Geräten Zugriff auf Amazon Simple Storage Service (Amazon S3) - Buckets gewähren. Die Verwaltung des Zugriffs sollte mit der Klassifizierung der Daten übereinst immen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AC-17.B	AC-17.B Fernzugriff	sagemaker-notebook-no-direct-Internetzugang	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass SageMaker Amazon-Notebooks keinen direkten Internetzugang zulassen. Indem Sie direkten Internetzugang blockieren, vermeiden Sie, dass unbefugte Benutzer auf sensible Daten zugreifen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AC-17.B	AC-17.B Fernzugriff	subnet-auto-assign-public-ip-deaktiviert	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon Virtual Private Cloud (VPC) -Subnetzen nicht automatisch eine öffentliche IP-Adresse zugewiesen wird. Amazon Elastic Compute Cloud (EC2) -Instances, die in Subnetzen gestartet werden, in denen dieses Attribut aktiviert ist, haben ihrer primären Netzwerkschnittstelle eine öffentliche IP-Adresse zugewiesen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AC-17.B	AC-17.B Fernzugriff	vpc-default-security-group-geschlossen	Sicherheitsgruppen von Amazon Elastic Compute Cloud (Amazon EC2) können bei der Verwaltung des Netzwerkzugriffs helfen, indem sie eine statusbehaftete Filterung des ein- und ausgehenden Netzwerkverkehrs zu Ressourcen bereitstellen. AWS Die Beschränk ung des gesamten Datenverkehrs auf die Standardsicherheit sgruppe hilft dabei, den Fernzugriff auf Ihre Ressourcen einzuschränken. AWS

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AC-17.B	AC-17.B Fernzugriff	vpc-sg-open-only-to-authorized-ports	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass gemeinsame Ports für Amazon Elastic Compute Cloud (Amazon EC2) -Sicherheitsgruppen eingeschränkt sind. Wenn der Zugriff auf Ports nicht auf vertrauenswürdige Quellen beschränkt wird, kann dies zu Angriffen auf die Verfügbarkeit, Integrität und Vertraulichkeit von Systemen führen. Durch die Beschränkung des Zugriffs auf Ressourcen innerhalb einer Sicherheitsgruppe aus dem Internet (0.0.0.0/0) kann der Fernzugriff auf interne Systeme gesteuert werden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AU-2.A	AU-2.A Prüfereignisse	api-gw-execution-logging-aktiviert	Die API-Gateway-Protokollierung zeigt detaillierte Ansichten der Benutzer, die auf die API zugegriffen haben, und wie diese Benutzer auf die API zugegriffen haben. Diese Einblicke ermöglichen die Transparenz von Benutzeraktivitäten.
CCCS-fPBMM-AU-2.A	AU-2.A Prüfereignisse	cloudtrail-s3-dataevents-enabled	Die Erfassung von Simple Storage Service (Amazon S3)-Datenereignissen unterstützt die Erkennung von ungewöhnlichen Aktivitäten. Zu den Details gehören Informationen zu dem AWS -Konto, das auf einen Amazon-S3-Bucket zugegriffen hat, die IP-Adresse und die Uhrzeit des Ereignisses.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AU-2.A	AU-2.A Prüfereignisse	cloud-trail-cloud-watch-logs-aktiviert	Verwenden Sie Amazon CloudWatch , um Protokoll ereignisaktivitäten zentral zu sammeln und zu verwalten. Die Aufnahme von AWS CloudTrail Daten liefert Einzelheiten zu den API-Aufrufaktivitäten in Ihrem AWS-Konto.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AU-2.A	AU-2.A Prüfereignisse	cloudtrail-enabled	AWS CloudTrail kann bei der Nichtabstreitbarkeit helfen, indem Aktionen und API-Aufrufe der AWS Management Console aufgezeichnet werden. Sie können die Benutzer und die Benutzer AWS-Konten , die einen AWS Dienst aufgerufen haben, die Quell-IP-Adresse, über die die Aufrufe generiert wurden, und den Zeitpunkt der Anrufe identifizieren. Einzelheiten zu den erfassten Daten finden Sie unter Inhalt des AWS CloudTrail Datensatzes.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AU-2.A	AU-2.A Prüfereignisse	elb-logging-enabled	Die Elastic-Load-Balancing-Aktivität ist ein zentraler Kommunikationspunkt innerhalb einer Umgebung. Stellen Sie sicher, dass die ELB-Protokollierung aktiviert ist. Die gesammelten Daten enthalten detaillierte Informationen zu Anfragen, die an den ELB gesendet wurden. Jedes Protokoll enthält Informationen wie die Zeit, zu der die Anforderung einging, die Client-IP-Adresse, Latenzen, Anforderungspfade und Serverantworten.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AU-2.A	AU-2.A Prüfereignisse	multi-region-cloudtrail-enabled	AWS CloudTrail zeichnet Aktionen und API-Aufrufe der AWS Management Console auf. Sie können feststellen, welche Benutzer und Konten angerufen wurden AWS, von welcher Quell-IP-Adresse aus die Anrufe getätigt wurden und wann die Anrufe erfolgten. CloudTrail übermittelt Protokolldateien aus allen AWS Regionen an Ihren S3-Bucket , wenn MULTI_REGION_CLOUD_TRAIL_ENABLED aktiviert ist. Außerdem wird beim AWS Start einer neuen Region derselbe Trail in der neuen Region erstellt. CloudTrail Dadurch erhalten Sie automatisch Protokolldateien mit API-Aktivitäten für die neue Region.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AU-2.A	AU-2.A Prüfereignisse	rds-logging-enabled	Um die Protokollierung und Überwachung in Ihrer Umgebung zu erleichtern, stellen Sie sicher, dass die Amazon Relational Database Service (Amazon RDS)-Protokollierung aktiviert ist. Mit der Amazon-RDS-Protokollierung können Sie Ereignisse wie Verbindungen, Verbindungsabbrüche, Abfragen oder abgefragte Tabellen erfassen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AU-2.A	AU-2.A Prüfereignisse	redshift-cluster-configuration-check	Um Daten im Ruhezustand zu schützen, muss die Verschlüsselung für Ihre Amazon-Redshift-Cluster aktiviert sein. Sie müssen auch sicherstellen, dass die erforderlichen Konfigurationen auf Amazon-Redshift-Clustern bereitgestellt werden. Die Prüfungsprotokollierung muss aktiviert sein, um Informationen zu Verbindungen und Benutzeraktivitäten in der Datenbank bereitzustellen. Diese Regel erfordert, dass ein Wert für clusterDbEncrypted (Config Default: TRUE) und LoggingEnabled (Config Default: TRUE) gesetzt ist. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AU-2.A	AU-2.A Prüfereignisse	s3- bucket-logging-enabled	Die Amazon Simple Storage Service (Amazon S3)-Serverzugriffs protokollierung bietet eine Methode zur Überwachu ng des Netzwerks im Hinblick auf potenzielle Cybersich erheitsereignisse. Die Ereignisse werden überwacht, indem detaillierte Aufzeichn ungen über die Anfragen erfasst werden, die an einen Amazon-S3-Bucket gestellt wurden. Jeder Zugriffsprotokolle intrag enthält Details zu einer einzelnen Zugriffsanfrage. Zu den Details gehören Auftraggeber, Bucket-Name, Anforderu ngszeit, Anforderu ngsaktion, Antwortst atus und Fehlercode, falls relevant.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AU-2.A	AU-2.A Prüfereignisse	vpc-flow-logs-enabled	VPC-Flow-Protokolle erfassen detaillierte Informationsdatensätze über den IP-Datenverkehr, der zu und von Netzwerkschnittstellen in Ihrer Amazon Virtual Private Cloud (Amazon VPC) fließt. Standardmäßig enthalten Flow-Protokolldatensätze Werte für die verschiedenen Komponenten des IP-Flows, einschließlich Quelle, Ziel und Protokoll.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AU-2.A	AU-2.A Prüfereignisse	wafv2-logging-enabled	Um die Protokollierung und Überwachung in Ihrer Umgebung zu erleichtern, aktivieren Sie die AWS WAF (V2) -Protokollierung im regionalen und globalen Web ACLs. AWS Die WAF-Protokollierung bietet detaillierte Informationen über den Datenverkehr, der von Ihrer Web-ACL analysiert wird. In den Protokollen werden die Uhrzeit aufgezeichnet, zu der die AWS WAF die Anfrage von Ihrer AWS Ressource erhalten hat, Informationen zu der Anfrage und eine Aktion für die Regel, der jede Anfrage entsprach.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AU-2.B	AU-2.B Prüfereignisse	api-gw-execution-logging-aktiviert	Die API-Gateway-Protokollierung zeigt detaillierte Ansichten der Benutzer, die auf die API zugegriffen haben, und wie diese Benutzer auf die API zugegriffen haben. Diese Einblicke ermöglichen die Transparenz von Benutzeraktivitäten.
CCCS-fPBMM-AU-2.B	AU-2.B Prüfereignisse	cloudtrail-s3-dataevents-enabled	Die Erfassung von Simple Storage Service (Amazon S3)-Datenereignissen unterstützt die Erkennung von ungewöhnlichen Aktivitäten. Zu den Details gehören Informationen zu dem AWS -Konto, das auf einen Amazon-S3-Bucket zugegriffen hat, die IP-Adresse und die Uhrzeit des Ereignisses.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AU-2.B	AU-2.B Prüfereignisse	cloud-trail-cloud-watch-logs-aktiviert	Verwenden Sie Amazon CloudWatch , um Protokoll ereignisaktivitäten zentral zu sammeln und zu verwalten. Die Aufnahme von AWS CloudTrail Daten liefert Einzelheiten zu den API-Aufrufaktivitäten in Ihrem AWS-Konto.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AU-2.B	AU-2.B Prüfereignisse	cloudtrail-enabled	AWS CloudTrail kann bei der Nichtabstreitbarkeit helfen, indem Aktionen und API-Aufrufe der AWS Management Console aufgezeichnet werden. Sie können die Benutzer und die Benutzer AWS-Konten , die einen AWS Dienst aufgerufen haben, die Quell-IP-Adresse, über die die Aufrufe generiert wurden, und den Zeitpunkt der Anrufe identifizieren. Einzelheiten zu den erfassten Daten finden Sie unter Inhalt des AWS CloudTrail Datensatzes.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AU-2.B	AU-2.B Prüfereignisse	elb-logging-enabled	Die Elastic-Load-Balancing-Aktivität ist ein zentraler Kommunikationspunkt innerhalb einer Umgebung. Stellen Sie sicher, dass die ELB-Protokollierung aktiviert ist. Die gesammelten Daten enthalten detaillierte Informationen zu Anfragen, die an den ELB gesendet wurden. Jedes Protokoll enthält Informationen wie die Zeit, zu der die Anforderung einging, die Client-IP-Adresse, Latenzen, Anforderungspfade und Serverantworten.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AU-2.B	AU-2.B Prüfereignisse	multi-region-cloudtrail-enabled	AWS CloudTrail zeichnet Aktionen und API-Aufrufe der AWS Management Console auf. Sie können feststellen, welche Benutzer und Konten angerufen wurden AWS, von welcher Quell-IP-Adresse aus die Anrufe getätigt wurden und wann die Anrufe erfolgten. CloudTrail übermittelt Protokolldateien aus allen AWS Regionen an Ihren S3-Bucket , wenn MULTI_REGION_CLOUD_TRAIL_ENABLED aktiviert ist. Außerdem wird beim AWS Start einer neuen Region derselbe Trail in der neuen Region erstellt. CloudTrail Dadurch erhalten Sie automatisch Protokolldateien mit API-Aktivitäten für die neue Region.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AU-2.B	AU-2.B Prüfereignisse	rds-logging-enabled	Um die Protokollierung und Überwachung in Ihrer Umgebung zu erleichtern, stellen Sie sicher, dass die Amazon Relational Database Service (Amazon RDS)-Protokollierung aktiviert ist. Mit der Amazon-RDS-Protokollierung können Sie Ereignisse wie Verbindungen, Verbindungsabbrüche, Abfragen oder abgefragte Tabellen erfassen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AU-2.B	AU-2.B Prüfereignisse	redshift-cluster-configuration-check	Um Daten im Ruhezustand zu schützen, muss die Verschlüsselung für Ihre Amazon-Redshift-Cluster aktiviert sein. Sie müssen auch sicherstellen, dass die erforderlichen Konfigurationen auf Amazon-Redshift-Clustern bereitgestellt werden. Die Prüfungsprotokollierung muss aktiviert sein, um Informationen zu Verbindungen und Benutzeraktivitäten in der Datenbank bereitzustellen. Diese Regel erfordert, dass ein Wert für clusterDbEncrypted (Config Default: TRUE) und LoggingEnabled (Config Default: TRUE) gesetzt ist. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AU-2.B	AU-2.B Prüfereignisse	s3- bucket-logging-enabled	Die Amazon Simple Storage Service (Amazon S3)-Serverzugriffs protokollierung bietet eine Methode zur Überwachu ng des Netzwerks im Hinblick auf potenzielle Cybersich erheitsereignisse. Die Ereignisse werden überwacht, indem detaillierte Aufzeichn ungen über die Anfragen erfasst werden, die an einen Amazon-S3-Bucket gestellt wurden. Jeder Zugriffsprotokolle intrag enthält Details zu einer einzelnen Zugriffsanfrage. Zu den Details gehören Auftraggeber, Bucket-Name, Anforderu ngszeit, Anforderu ngsaktion, Antwortst atus und Fehlercode, falls relevant.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AU-2.B	AU-2.B Prüfereignisse	vpc-flow-logs-enabled	VPC-Flow-Protokolle erfassen detaillierte Informationsdatensätze über den IP-Datenverkehr, der zu und von Netzwerkschnittstellen in Ihrer Amazon Virtual Private Cloud (Amazon VPC) fließt. Standardmäßig enthalten Flow-Protokolldatensätze Werte für die verschiedenen Komponenten des IP-Flows, einschließlich Quelle, Ziel und Protokoll.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AU-2.B	AU-2.B Prüfereignisse	wafv2-logging-enabled	Um die Protokollierung und Überwachung in Ihrer Umgebung zu erleichtern, aktivieren Sie die AWS WAF (V2) -Protokollierung im regionalen und globalen Web ACLs. AWS Die WAF-Protokollierung bietet detaillierte Informationen über den Datenverkehr, der von Ihrer Web-ACL analysiert wird. In den Protokollen werden die Uhrzeit aufgezeichnet, zu der die AWS WAF die Anfrage von Ihrer AWS Ressource erhalten hat, Informationen zu der Anfrage und eine Aktion für die Regel, der jede Anfrage entsprach.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AU-2.C	AU-2.C Prüfereignisse	api-gw-execution-logging-aktiviert	Die API-Gateway-Protokollierung zeigt detaillierte Ansichten der Benutzer, die auf die API zugegriffen haben, und wie diese Benutzer auf die API zugegriffen haben. Diese Einblicke ermöglichen die Transparenz von Benutzeraktivitäten.
CCCS-fPBMM-AU-2.C	AU-2.C Prüfereignisse	cloudtrail-s3-dataevents-enabled	Die Erfassung von Simple Storage Service (Amazon S3)-Datenereignissen unterstützt die Erkennung von ungewöhnlichen Aktivitäten. Zu den Details gehören Informationen zu dem AWS -Konto, das auf einen Amazon-S3-Bucket zugegriffen hat, die IP-Adresse und die Uhrzeit des Ereignisses.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AU-2.C	AU-2.C Prüfereignisse	cloud-trail-cloud-watch-logs-aktiviert	Verwenden Sie Amazon CloudWatch , um Protokoll ereignisaktivitäten zentral zu sammeln und zu verwalten. Die Aufnahme von AWS CloudTrail Daten liefert Einzelheiten zu den API-Aufrufaktivitäten in Ihrem AWS-Konto.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AU-2.C	AU-2.C Prüfereignisse	cloudtrail-enabled	AWS CloudTrail kann bei der Nichtabstreitbarkeit helfen, indem Aktionen und API-Aufrufe der AWS Management Console aufgezeichnet werden. Sie können die Benutzer und die Benutzer AWS-Konten , die einen AWS Dienst aufgerufen haben, die Quell-IP-Adresse, über die die Aufrufe generiert wurden, und den Zeitpunkt der Anrufe identifizieren. Einzelheiten zu den erfassten Daten finden Sie unter Inhalt des AWS CloudTrail Datensatzes.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AU-2.C	AU-2.C Prüfereignisse	elb-logging-enabled	Die Elastic-Load-Balancing-Aktivität ist ein zentraler Kommunikationspunkt innerhalb einer Umgebung. Stellen Sie sicher, dass die ELB-Protokollierung aktiviert ist. Die gesammelten Daten enthalten detaillierte Informationen zu Anfragen, die an den ELB gesendet wurden. Jedes Protokoll enthält Informationen wie die Zeit, zu der die Anforderung einging, die Client-IP-Adresse, Latenzen, Anforderungspfade und Serverantworten.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AU-2.C	AU-2.C Prüfereignisse	multi-region-cloudtrail-enabled	AWS CloudTrail zeichnet Aktionen und API-Aufrufe der AWS Management Console auf. Sie können feststellen, welche Benutzer und Konten angerufen wurden AWS, von welcher Quell-IP-Adresse aus die Anrufe getätigt wurden und wann die Anrufe erfolgten. CloudTrail übermittelt Protokolldateien aus allen AWS Regionen an Ihren S3-Bucket , wenn MULTI_REGION_CLOUD_TRAIL_ENABLED aktiviert ist. Außerdem wird beim AWS Start einer neuen Region derselbe Trail in der neuen Region erstellt. CloudTrail Dadurch erhalten Sie automatisch Protokolldateien mit API-Aktivitäten für die neue Region.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AU-2.C	AU-2.C Prüfereignisse	rds-logging-enabled	Um die Protokollierung und Überwachung in Ihrer Umgebung zu erleichtern, stellen Sie sicher, dass die Amazon Relational Database Service (Amazon RDS)-Protokollierung aktiviert ist. Mit der Amazon-RDS-Protokollierung können Sie Ereignisse wie Verbindungen, Verbindungsabbrüche, Abfragen oder abgefragte Tabellen erfassen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AU-2.C	AU-2.C Prüfereignisse	redshift-cluster-configuration-check	Um Daten im Ruhezustand zu schützen, muss die Verschlüsselung für Ihre Amazon-Redshift-Cluster aktiviert sein. Sie müssen auch sicherstellen, dass die erforderlichen Konfigurationen auf Amazon-Redshift-Clustern bereitgestellt werden. Die Prüfungsprotokollierung muss aktiviert sein, um Informationen zu Verbindungen und Benutzeraktivitäten in der Datenbank bereitzustellen. Diese Regel erfordert, dass ein Wert für clusterDbEncrypted (Config Default: TRUE) und LoggingEnabled (Config Default: TRUE) gesetzt ist. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AU-2.C	AU-2.C Prüfereignisse	s3- bucket-logging-enabled	Die Amazon Simple Storage Service (Amazon S3)-Serverzugriffs protokollierung bietet eine Methode zur Überwachu ng des Netzwerks im Hinblick auf potenzielle Cybersich erheitsereignisse. Die Ereignisse werden überwacht, indem detaillierte Aufzeichn ungen über die Anfragen erfasst werden, die an einen Amazon-S3-Bucket gestellt wurden. Jeder Zugriffsprotokolle intrag enthält Details zu einer einzelnen Zugriffsanfrage. Zu den Details gehören Auftraggeber, Bucket-Name, Anforderu ngszeit, Anforderu ngsaktion, Antwortst atus und Fehlercode, falls relevant.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AU-2.C	AU-2.C Prüfereignisse	vpc-flow-logs-enabled	VPC-Flow-Protokolle erfassen detaillierte Informationsdatensätze über den IP-Datenverkehr, der zu und von Netzwerkschnittstellen in Ihrer Amazon Virtual Private Cloud (Amazon VPC) fließt. Standardmäßig enthalten Flow-Protokolldatensätze Werte für die verschiedenen Komponenten des IP-Flows, einschließlich Quelle, Ziel und Protokoll.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AU-2.C	AU-2.C Prüfereignisse	wafv2-logging-enabled	Um die Protokollierung und Überwachung in Ihrer Umgebung zu erleichtern, aktivieren Sie die AWS WAF (V2) -Protokollierung im regionalen und globalen Web ACLs. AWS Die WAF-Protokollierung bietet detaillierte Informationen über den Datenverkehr, der von Ihrer Web-ACL analysiert wird. In den Protokollen werden die Uhrzeit aufgezeichnet, zu der die AWS WAF die Anfrage von Ihrer AWS Ressource erhalten hat, Informationen zu der Anfrage und eine Aktion für die Regel, der jede Anfrage entsprach.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AU-2.D	AU-2.D Prüfereignisse	api-gw-execution-logging-aktiviert	Die API-Gateway-Protokollierung zeigt detaillierte Ansichten der Benutzer, die auf die API zugegriffen haben, und wie diese Benutzer auf die API zugegriffen haben. Diese Einblicke ermöglichen die Transparenz von Benutzeraktivitäten.
CCCS-fPBMM-AU-2.D	AU-2.D Prüfereignisse	cloudtrail-s3-dataevents-enabled	Die Erfassung von Simple Storage Service (Amazon S3)-Datenereignissen unterstützt die Erkennung von ungewöhnlichen Aktivitäten. Zu den Details gehören Informationen zu dem AWS -Konto, das auf einen Amazon-S3-Bucket zugegriffen hat, die IP-Adresse und die Uhrzeit des Ereignisses.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AU-2.D	AU-2.D Prüfereignisse	cloud-trail-cloud-watch-logs-aktiviert	Verwenden Sie Amazon CloudWatch , um Protokoll ereignisaktivitäten zentral zu sammeln und zu verwalten. Die Aufnahme von AWS CloudTrail Daten liefert Einzelheiten zu den API-Aufrufaktivitäten in Ihrem AWS-Konto.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AU-2.D	AU-2.D Prüfereignisse	cloudtrail-enabled	AWS CloudTrail kann bei der Nichtabstreitbarkeit helfen, indem Aktionen und API-Aufrufe der AWS Management Console aufgezeichnet werden. Sie können die Benutzer und die Benutzer AWS-Konten , die einen AWS Dienst aufgerufen haben, die Quell-IP-Adresse, über die die Aufrufe generiert wurden, und den Zeitpunkt der Anrufe identifizieren. Einzelheiten zu den erfassten Daten finden Sie unter Inhalt des AWS CloudTrail Datensatzes.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AU-2.D	AU-2.D Prüfereignisse	elb-logging-enabled	Die Elastic-Load-Balancing-Aktivität ist ein zentraler Kommunikationspunkt innerhalb einer Umgebung. Stellen Sie sicher, dass die ELB-Protokollierung aktiviert ist. Die gesammelten Daten enthalten detaillierte Informationen zu Anfragen, die an den ELB gesendet wurden. Jedes Protokoll enthält Informationen wie die Zeit, zu der die Anforderung einging, die Client-IP-Adresse, Latenzen, Anforderungspfade und Serverantworten.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AU-2.D	AU-2.D Prüfereignisse	multi-region-cloudtrail-enabled	AWS CloudTrail zeichnet Aktionen und API-Aufrufe der AWS Management Console auf. Sie können feststellen, welche Benutzer und Konten angerufen wurden AWS, von welcher Quell-IP-Adresse aus die Anrufe getätigt wurden und wann die Anrufe erfolgten. CloudTrail übermittelt Protokolldateien aus allen AWS Regionen an Ihren S3-Bucket , wenn MULTI_REGION_CLOUD_TRAIL_ENABLED aktiviert ist. Außerdem wird beim AWS Start einer neuen Region derselbe Trail in der neuen Region erstellt. CloudTrail Dadurch erhalten Sie automatisch Protokolldateien mit API-Aktivitäten für die neue Region.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AU-2.D	AU-2.D Prüfereignisse	rds-logging-enabled	Um die Protokollierung und Überwachung in Ihrer Umgebung zu erleichtern, stellen Sie sicher, dass die Amazon Relational Database Service (Amazon RDS)-Protokollierung aktiviert ist. Mit der Amazon-RDS-Protokollierung können Sie Ereignisse wie Verbindungen, Verbindungsabbrüche, Abfragen oder abgefragte Tabellen erfassen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AU-2.D	AU-2.D Prüfereignisse	redshift-cluster-configuration-check	Um Daten im Ruhezustand zu schützen, muss die Verschlüsselung für Ihre Amazon-Redshift-Cluster aktiviert sein. Sie müssen auch sicherstellen, dass die erforderlichen Konfigurationen auf Amazon-Redshift-Clustern bereitgestellt werden. Die Prüfungsprotokollierung muss aktiviert sein, um Informationen zu Verbindungen und Benutzeraktivitäten in der Datenbank bereitzustellen. Diese Regel erfordert, dass ein Wert für clusterDbEncrypted (Config Default: TRUE) und LoggingEnabled (Config Default: TRUE) gesetzt ist. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AU-2.D	AU-2.D Prüfereignisse	s3- bucket-logging-enabled	Die Amazon Simple Storage Service (Amazon S3)-Serverzugriffs protokollierung bietet eine Methode zur Überwachu ng des Netzwerks im Hinblick auf potenzielle Cybersich erheitsereignisse. Die Ereignisse werden überwacht, indem detaillierte Aufzeichn ungen über die Anfragen erfasst werden, die an einen Amazon-S3-Bucket gestellt wurden. Jeder Zugriffsprotokolle intrag enthält Details zu einer einzelnen Zugriffsanfrage. Zu den Details gehören Auftraggeber, Bucket-Name, Anforderu ngszeit, Anforderu ngsaktion, Antwortst atus und Fehlercode, falls relevant.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AU-2.D	AU-2.D Prüfereignisse	vpc-flow-logs-enabled	VPC-Flow-Protokolle erfassen detaillierte Informationsdatensätze über den IP-Datenverkehr, der zu und von Netzwerkschnittstellen in Ihrer Amazon Virtual Private Cloud (Amazon VPC) fließt. Standardmäßig enthalten Flow-Protokolldatensätze Werte für die verschiedenen Komponenten des IP-Flows, einschließlich Quelle, Ziel und Protokoll.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AU-2.D	AU-2.D Prüfereignisse	wafv2-logging-enabled	Um die Protokollierung und Überwachung in Ihrer Umgebung zu erleichtern, aktivieren Sie die AWS WAF (V2) -Protokollierung im regionalen und globalen Web ACLs. AWS Die WAF-Protokollierung bietet detaillierte Informationen über den Datenverkehr, der von Ihrer Web-ACL analysiert wird. In den Protokollen werden die Uhrzeit aufgezeichnet, zu der die AWS WAF die Anfrage von Ihrer AWS Ressource erhalten hat, Informationen zu der Anfrage und eine Aktion für die Regel, der jede Anfrage entsprach.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AU-3(1)	AU-3(1) Inhalt der Prüfungsaufzeichnungen | Zusätzliche Prüfungsinformationen	api-gw-execution-logging-aktiviert	Die API-Gateway-Protokollierung zeigt detaillierte Ansichten der Benutzer, die auf die API zugegriffen haben, und wie diese Benutzer auf die API zugegriffen haben. Diese Einblicke ermöglichen die Transparenz von Benutzeraktivitäten.
CCCS-fPBMM-AU-3(1)	AU-3(1) Inhalt der Prüfungsaufzeichnungen | Zusätzliche Prüfungsinformationen	cloudtrail-s3-dataevents-enabled	Die Erfassung von Simple Storage Service (Amazon S3)-Datenereignissen unterstützt die Erkennung von ungewöhnlichen Aktivitäten. Zu den Details gehören Informationen zu dem AWS -Konto, das auf einen Amazon-S3-Bucket zugegriffen hat, die IP-Adresse und die Uhrzeit des Ereignisses.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AU-3(1)	AU-3(1) Inhalt der Prüfungsaufzeichnungen | Zusätzliche Prüfungsinformationen	cloud-trail-cloud-watch-logs-aktiviert	Verwenden Sie Amazon CloudWatch , um Protokoll ereignisaktivitäten zentral zu sammeln und zu verwalten. Die Aufnahme von AWS CloudTrail Daten liefert Einzelheiten zu den API-Aufrufaktivitäten in Ihrem AWS-Konto.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AU-3(1)	AU-3(1) Inhalt der Prüfungsaufzeichnungen | Zusätzliche Prüfungsinformationen	cloudtrail-enabled	AWS CloudTrail kann bei der Nichtabstreitbarkeit helfen, indem Aktionen und API-Aufrufe der AWS Management Console aufgezeichnet werden. Sie können die Benutzer und die Benutzer AWS-Konten , die einen AWS Dienst aufgerufen haben, die Quell-IP-Adresse, über die die Aufrufe generiert wurden, und den Zeitpunkt der Anrufe identifizieren. Einzelheiten zu den erfassten Daten finden Sie unter Inhalt des AWS CloudTrail Datensatzes.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AU-3(1)	AU-3(1) Inhalt der Prüfungsaufzeichnungen | Zusätzliche Prüfungsinformationen	elb-logging-enabled	Die Elastic-Load-Balancing-Aktivität ist ein zentraler Kommunikationspunkt innerhalb einer Umgebung. Stellen Sie sicher, dass die ELB-Protokollierung aktiviert ist. Die gesammelten Daten enthalten detaillierte Informationen zu Anfragen, die an den ELB gesendet wurden. Jedes Protokoll enthält Informationen wie die Zeit, zu der die Anforderung einging, die Client-IP-Adresse, Latenzen, Anforderungspfade und Serverantworten.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AU-3(1)	AU-3(1) Inhalt der Prüfungsaufzeichnungen | Zusätzliche Prüfungsinformationen	rds-logging-enabled	Um die Protokollierung und Überwachung in Ihrer Umgebung zu erleichtern, stellen Sie sicher, dass die Amazon Relational Database Service (Amazon RDS)-Protokollierung aktiviert ist. Mit der Amazon-RDS-Protokollierung können Sie Ereignisse wie Verbindungen, Verbindungsabbrüche, Abfragen oder abgefragte Tabellen erfassen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AU-3(1)	AU-3(1) Inhalt der Prüfungsaufzeichnungen | Zusätzliche Prüfungsinformationen	redshift-cluster-configuration-check	Um Daten im Ruhezustand zu schützen, muss die Verschlüsselung für Ihre Amazon-Redshift-Cluster aktiviert sein. Sie müssen auch sicherstellen, dass die erforderlichen Konfigurationen auf Amazon-Redshift-Clustern bereitgestellt werden. Die Prüfungsprotokollierung muss aktiviert sein, um Informationen zu Verbindungen und Benutzeraktivitäten in der Datenbank bereitzustellen. Diese Regel erfordert, dass ein Wert für clusterDbEncrypted (Config Default: TRUE) und LoggingEnabled (Config Default: TRUE) gesetzt ist. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AU-3(1)	AU-3(1) Inhalt der Prüfungsaufzeichnungen | Zusätzliche Prüfungsinformationen	s3- bucket-logging-enabled	Die Amazon Simple Storage Service (Amazon S3)-Serverzugriffsprotokollierung bietet eine Methode zur Überwachung des Netzwerks im Hinblick auf potenzielle Cybersicherheitsereignisse. Die Ereignisse werden überwacht, indem detaillierte Aufzeichnungen über die Anfragen erfasst werden, die an einen Amazon-S3-Bucket gestellt wurden. Jeder Zugriffsprotokolleintrag enthält Details zu einer einzelnen Zugriffsanfrage. Zu den Details gehören Auftraggeber, Bucket-Name, Anforderungszeit, Anforderungsaktion, Antwortstatus und Fehlercode, falls relevant.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AU-3.A	AU-3.A Inhalt von Prüfungsunterlagen	api-gw-execution-logging-aktiviert	Die API-Gateway-Protokollierung zeigt detaillierte Ansichten der Benutzer, die auf die API zugegriffen haben, und wie diese Benutzer auf die API zugegriffen haben. Diese Einblicke ermöglichen die Transparenz von Benutzeraktivitäten.
CCCS-fPBMM-AU-3.A	AU-3.A Inhalt von Prüfungsunterlagen	cloudtrail-s3-dataevents-enabled	Die Erfassung von Simple Storage Service (Amazon S3)-Datenereignissen unterstützt die Erkennung von ungewöhnlichen Aktivitäten. Zu den Details gehören Informationen zu dem AWS -Konto, das auf einen Amazon-S3-Bucket zugegriffen hat, die IP-Adresse und die Uhrzeit des Ereignisses.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AU-3.A	AU-3.A Inhalt von Prüfungsunterlagen	cloud-trail-cloud-watch-logs-aktiviert	Verwenden Sie Amazon CloudWatch , um Protokoll ereignisaktivitäten zentral zu sammeln und zu verwalten. Die Aufnahme von AWS CloudTrail Daten liefert Einzelheiten zu den API-Aufrufaktivitäten in Ihrem AWS-Konto.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AU-3.A	AU-3.A Inhalt von Prüfungsunterlagen	cloudtrail-enabled	AWS CloudTrail kann bei der Nichtabstreitbarkeit helfen, indem Aktionen und API-Aufrufe der AWS Management Console aufgezeichnet werden. Sie können die Benutzer und die Benutzer AWS-Konten , die einen AWS Dienst aufgerufen haben, die Quell-IP-Adresse, über die die Aufrufe generiert wurden, und den Zeitpunkt der Anrufe identifizieren. Einzelheiten zu den erfassten Daten finden Sie unter Inhalt des AWS CloudTrail Datensatzes.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AU-3.A	AU-3.A Inhalt von Prüfungsunterlagen	elasticsearch-logs-to-cloudwatch	Stellen Sie sicher, dass für Amazon OpenSearch Service-Domains Fehlerprotokolle aktiviert und zur Aufbewahrung und Beantwortung an Amazon CloudWatch Logs gestreamt werden. Domain-Fehlerprotokolle sind bei Sicherheits- und Zugriffsprüfungen sowie bei der Diagnose von Verfügbarkeitsproblemen nützlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AU-3.A	AU-3.A Inhalt von Prüfungsunterlagen	elb-logging-enabled	Die Elastic-Load-Balancing-Aktivität ist ein zentraler Kommunikationspunkt innerhalb einer Umgebung. Stellen Sie sicher, dass die ELB-Protokollierung aktiviert ist. Die gesammelten Daten enthalten detaillierte Informationen zu Anfragen, die an den ELB gesendet wurden. Jedes Protokoll enthält Informationen wie die Zeit, zu der die Anforderung einging, die Client-IP-Adresse, Latenzen, Anforderungspfade und Serverantworten.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AU-3.A	AU-3.A Inhalt von Prüfungsunterlagen	multi-region-cloudtrail-enabled	AWS CloudTrail zeichnet Aktionen und API-Aufrufe der AWS Management Console auf. Sie können feststellen, welche Benutzer und Konten angerufen wurden AWS, von welcher Quell-IP-Adresse aus die Anrufe getätigt wurden und wann die Anrufe erfolgten. CloudTrail übermittelt Protokolldateien aus allen AWS Regionen an Ihren S3-Bucket , wenn MULTI_REGION_CLOUD_TRAIL_ENABLED aktiviert ist. Außerdem wird beim AWS Start einer neuen Region derselbe Trail in der neuen Region erstellt. CloudTrail Dadurch erhalten Sie automatisch Protokolldateien mit API-Aktivitäten für die neue Region.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AU-3.A	AU-3.A Inhalt von Prüfungsunterlagen	opensearch-logs-to-cloudwatch	Stellen Sie sicher, dass für Amazon OpenSearch Service-Domains Fehlerprotokolle aktiviert und zur Aufbewahrung und Beantwortung an Amazon CloudWatch Logs gestreamt werden. OpenSearch Service-Fehlerprotokolle können bei Sicherheits- und Zugriffsprüfungen helfen und bei der Diagnose von Verfügbarkeitsproblemen helfen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AU-3.A	AU-3.A Inhalt von Prüfungsunterlagen	rds-logging-enabled	Um die Protokollierung und Überwachung in Ihrer Umgebung zu erleichtern, stellen Sie sicher, dass die Amazon Relational Database Service (Amazon RDS)-Protokollierung aktiviert ist. Mit der Amazon-RDS-Protokollierung können Sie Ereignisse wie Verbindungen, Verbindungsabbrüche, Abfragen oder abgefragte Tabellen erfassen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AU-3.A	AU-3.A Inhalt von Prüfungsunterlagen	redshift-cluster-configuration-check	Um Daten im Ruhezustand zu schützen, muss die Verschlüsselung für Ihre Amazon-Redshift-Cluster aktiviert sein. Sie müssen auch sicherstellen, dass die erforderlichen Konfigurationen auf Amazon-Redshift-Clustern bereitgestellt werden. Die Prüfungsprotokollierung muss aktiviert sein, um Informationen zu Verbindungen und Benutzeraktivitäten in der Datenbank bereitzustellen. Diese Regel erfordert, dass ein Wert für clusterDbEncrypted (Config Default: TRUE) und LoggingEnabled (Config Default: TRUE) gesetzt ist. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AU-3.A	AU-3.A Inhalt von Prüfungsunterlagen	s3- bucket-logging-enabled	Die Amazon Simple Storage Service (Amazon S3)-Serverzugriffs protokollierung bietet eine Methode zur Überwachu ng des Netzwerks im Hinblick auf potenzielle Cybersich erheitsereignisse. Die Ereignisse werden überwacht, indem detaillierte Aufzeichn ungen über die Anfragen erfasst werden, die an einen Amazon-S3-Bucket gestellt wurden. Jeder Zugriffsprotokolle intrag enthält Details zu einer einzelnen Zugriffsanfrage. Zu den Details gehören Auftraggeber, Bucket-Name, Anforderu ngszeit, Anforderu ngsaktion, Antwortst atus und Fehlercode, falls relevant.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AU-3.A	AU-3.A Inhalt von Prüfungsunterlagen	vpc-flow-logs-enabled	VPC-Flow-Protokolle erfassen detaillierte Informationsdatensätze über den IP-Datenverkehr, der zu und von Netzwerkschnittstellen in Ihrer Amazon Virtual Private Cloud (Amazon VPC) fließt. Standardmäßig enthalten Flow-Protokolldatensätze Werte für die verschiedenen Komponenten des IP-Flows, einschließlich Quelle, Ziel und Protokoll.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AU-3.A	AU-3.A Inhalt von Prüfungsunterlagen	wafv2-logging-enabled	Um die Protokollierung und Überwachung in Ihrer Umgebung zu erleichtern, aktivieren Sie die AWS WAF (V2) -Protokollierung im regionalen und globalen Web ACLs. AWS Die WAF-Protokollierung bietet detaillierte Informationen über den Datenverkehr, der von Ihrer Web-ACL analysiert wird. In den Protokollen werden die Uhrzeit aufgezeichnet, zu der die AWS WAF die Anfrage von Ihrer AWS Ressource erhalten hat, Informationen zu der Anfrage und eine Aktion für die Regel, der jede Anfrage entsprach.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AU-5.A	AU-5.A Reaktion auf Fehler bei der Prüfungsverarbeitung	cloudwatch-alarm-action-check	Amazon CloudWatch alarmiert, wenn eine Metrik den Schwellenwert für eine bestimmte Anzahl von Bewertungszeiträumen überschreitet. Der Alarm führt eine oder mehrere Aktionen durch, die vom Wert der Metrik oder des Ausdrucks im Vergleich zu einem Schwellenwert in einer Reihe von Zeiträumen abhängt. Diese Regel erfordert einen Wert für alarmActionRequired (Config Default: True), insufficientDataAction Required (Config Default: True), okActionRequired (Config Default: False). Der tatsächliche Wert muss die Alarmaktionen für Ihre Umgebung widerspiegeln.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AU-5.B	AU-5.B Reaktion auf Fehler bei der Prüfungsverarbeitung	cloudwatch-alarm-action-check	Amazon CloudWatch alarmiert, wenn eine Metrik den Schwellenwert für eine bestimmte Anzahl von Bewertungszeiträumen überschreitet. Der Alarm führt eine oder mehrere Aktionen durch, die vom Wert der Metrik oder des Ausdrucks im Vergleich zu einem Schwellenwert in einer Reihe von Zeiträumen abhängt. Diese Regel erfordert einen Wert für alarmActionRequired (Config Default: True), insufficientDataAction Required (Config Default: True), okActionRequired (Config Default: False). Der tatsächliche Wert muss die Alarmaktionen für Ihre Umgebung widerspiegeln.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AU-6(1)	AU-6(1) Prüfung, Analyse und Berichterstattung | Prozessintegration	cloudwatch-alarm-action-check	Amazon CloudWatch alarmiert, wenn eine Metrik den Schwellenwert für eine bestimmte Anzahl von Bewertungszeiträumen überschreitet. Der Alarm führt eine oder mehrere Aktionen durch, die vom Wert der Metrik oder des Ausdrucks im Vergleich zu einem Schwellenwert in einer Reihe von Zeiträumen abhängt. Diese Regel erfordert einen Wert für alarmActionRequired (Config Default: True), insufficientDataAction Required (Config Default: True), okActionRequired (Config Default: False). Der tatsächliche Wert muss die Alarmaktionen für Ihre Umgebung widerspiegeln.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AU-6(1)	AU-6(1) Prüfung, Analyse und Berichterstattung | Prozessintegration	cloud-trail-cloud-watch-logs-aktiviert	Verwenden Sie Amazon CloudWatch , um Protokollereignisaktivitäten zentral zu sammeln und zu verwalten. Die Aufnahme von AWS CloudTrail Daten liefert Einzelheiten zu den API-Aufrufaktivitäten in Ihrem AWS-Konto.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AU-6(1)	AU-6(1) Prüfung, Analyse und Berichterstattung | Prozessintegration	cloudtrail-enabled	AWS CloudTrail kann bei der Nichtabstreitbarkeit helfen, indem Aktionen und API-Aufrufe der AWS Management Console aufgezeichnet werden. Sie können die Benutzer und die Benutzer AWS-Konten , die einen AWS Dienst aufgerufen haben, die Quell-IP-Adresse, über die die Aufrufe generiert wurden, und den Zeitpunkt der Anrufe identifizieren. Einzelheiten zu den erfassten Daten finden Sie unter Inhalt des AWS CloudTrail Datensatzes.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AU-6(1)	AU-6(1) Prüfung, Analyse und Berichterstattung | Prozessintegration	guardduty-enabled-centralized	Amazon GuardDuty kann mithilfe von Threat Intelligence Feeds helfen, potenzielle Cybersicherheitsereignisse zu überwachen und zu erkennen. Dazu gehören Listen mit bösartigen IPs und maschinellen Lernmethoden zur Identifizierung unerwarteter, nicht autorisierter und bösartiger Aktivitäten in Ihrer AWS Cloud-Umgebung.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AU-6(1)	AU-6(1) Prüfung, Analyse und Berichterstattung | Prozessintegration	multi-region-cloudtrail-enabled	AWS CloudTrail zeichnet Aktionen und API-Aufrufe der AWS Management Console auf. Sie können feststellen, welche Benutzer und Konten angerufen wurden AWS, von welcher Quell-IP-Adresse aus die Anrufe getätigt wurden und wann die Anrufe erfolgten. CloudTrail übermittelt Protokolldateien aus allen AWS Regionen an Ihren S3-Bucket , wenn MULTI_REGION_CLOUD_TRAIL_ENABLED aktiviert ist. Außerdem wird beim AWS Start einer neuen Region derselbe Trail in der neuen Region erstellt. CloudTrail Dadurch erhalten Sie automatisch Protokolldateien mit API-Aktivitäten für die neue Region.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AU-6(1)	AU-6(1) Prüfung, Analyse und Berichterstattung | Prozessintegration	securityhub-enabled	AWS Security Hub hilft bei der Überwachung von unbefugtem Personal, Verbindungen, Geräten und Software. AWS Security Hub aggregiert, organisiert und priorisiert die Sicherheitswarnungen oder Ergebnisse mehrerer Dienste. AWS Einige dieser Dienste sind Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer und AWS Firewall Manager sowie AWS Partnerlösungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AU-6(3)	AU-6(3) Prüfung, Analyse und Berichterstattung | Korrelation der Prüfungs-Repositorys	api-gw-execution-logging-aktiviert	Die API-Gateway-Protokollierung zeigt detaillierte Ansichten der Benutzer, die auf die API zugegriffen haben, und wie diese Benutzer auf die API zugegriffen haben. Diese Einblicke ermöglichen die Transparenz von Benutzeraktivitäten.
CCCS-fPBMM-AU-6(3)	AU-6(3) Prüfung, Analyse und Berichterstattung | Korrelation der Prüfungs-Repositorys	cloudtrail-s3-dataevents-enabled	Die Erfassung von Simple Storage Service (Amazon S3)-Datenereignissen unterstützt die Erkennung von ungewöhnlichen Aktivitäten. Zu den Details gehören Informationen zu dem AWS -Konto, das auf einen Amazon-S3-Bucket zugegriffen hat, die IP-Adresse und die Uhrzeit des Ereignisses.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AU-6(3)	AU-6(3) Prüfung, Analyse und Berichterstattung | Korrelation der Prüfungs-Repositorys	cloud-trail-cloud-watch-logs-aktiviert	Verwenden Sie Amazon CloudWatch , um Protokoll ereignisaktivitäten zentral zu sammeln und zu verwalten. Die Aufnahme von AWS CloudTrail Daten liefert Einzelheiten zu den API-Aufrufaktivitäten in Ihrem AWS-Konto.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AU-6(3)	AU-6(3) Prüfung, Analyse und Berichterstattung | Korrelation der Prüfungs-Repositorys	cloudtrail-enabled	AWS CloudTrail kann bei der Nichtabstreitbarkeit helfen, indem Aktionen und API-Aufrufe der AWS Management Console aufgezeichnet werden. Sie können die Benutzer und die Benutzer AWS-Konten , die einen AWS Dienst aufgerufen haben, die Quell-IP-Adresse, über die die Aufrufe generiert wurden, und den Zeitpunkt der Anrufe identifizieren. Einzelheiten zu den erfassten Daten finden Sie unter Inhalt des AWS CloudTrail Datensatzes.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AU-6(3)	AU-6(3) Prüfung, Analyse und Berichterstattung | Korrelation der Prüfungs-Repositorys	cloud-trail-log-file-Validierung aktiviert	Verwenden Sie die AWS CloudTrail Protokolldateivalidierung, um die Integrität von Protokollen zu überprüfen. CloudTrail Mithilfe der Protokolldateivalidierung kann festgestellt werden, ob eine Protokolldatei geändert oder gelöscht wurde oder ob sie nach der Übermittlung CloudTrail unverändert geblieben ist. Dieses Feature wurde mit dem Branchenstandard entsprechenden Algorithmen entwickelt: SHA-256 für die Hashfunktion und SHA-256 mit RSA für digitale Signaturen. Aus diesem Grund ist es rechnerisch unmöglich, CloudTrail Protokolldateien unbemerkt zu ändern, zu löschen oder zu fälschen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AU-6(3)	AU-6(3) Prüfung, Analyse und Berichterstattung | Korrelation der Prüfungs-Repositorys	cw-loggroup-retention-period-überprüfen	Stellen Sie sicher, dass die Ereignisprotokolldaten für Ihre Protokollgruppen über eine Mindestdauer aufbewahrt werden, um die Fehlerbehebung und forensische Untersuchungen zu unterstützen. Fehlende frühere Ereignisprotokolldaten erschweren die Rekonstruierung und Identifizierung potenziell schädlicher Ereignisse.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AU-6(3)	AU-6(3) Prüfung, Analyse und Berichterstattung | Korrelation der Prüfungs-Repositorys	elasticsearch-logs-to-cloudwatch	Stellen Sie sicher, dass für Amazon OpenSearch Service-Domains Fehlerprotokolle aktiviert und zur Aufbewahrung und Beantwortung an Amazon CloudWatch Logs gestreamt werden. Domain-Fehlerprotokolle sind bei Sicherheits- und Zugriffsprüfungen sowie bei der Diagnose von Verfügbarkeitsproblemen nützlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AU-6(3)	AU-6(3) Prüfung, Analyse und Berichterstattung | Korrelation der Prüfungs-Repositorys	elb-logging-enabled	Die Elastic-Load-Balancing-Aktivität ist ein zentraler Kommunikationspunkt innerhalb einer Umgebung. Stellen Sie sicher, dass die ELB-Protokollierung aktiviert ist. Die gesammelten Daten enthalten detaillierte Informationen zu Anfragen, die an den ELB gesendet wurden. Jedes Protokoll enthält Informationen wie die Zeit, zu der die Anforderung einging, die Client-IP-Adresse, Latenzen, Anforderungspfade und Serverantworten.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AU-6(3)	AU-6(3) Prüfung, Analyse und Berichterstattung | Korrelation der Prüfungs-Repositorys	multi-region-cloudtrail-enabled	AWS CloudTrail zeichnet Aktionen und API-Aufrufe der AWS Management Console auf. Sie können feststellen, welche Benutzer und Konten angerufen wurden AWS, von welcher Quell-IP-Adresse aus die Anrufe getätigt wurden und wann die Anrufe erfolgten. CloudTrail übermittelt Protokolldateien aus allen AWS Regionen an Ihren S3-Bucket, wenn MULTI_REGION_CLOUD_TRAIL_ENABLED aktiviert ist. Außerdem wird beim AWS Start einer neuen Region derselbe Trail in der neuen Region erstellt. CloudTrail Dadurch erhalten Sie automatisch Protokolldateien mit API-Aktivitäten für die neue Region.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AU-6(3)	AU-6(3) Prüfung, Analyse und Berichterstattung | Korrelation der Prüfungs-Repositorys	opensearch-logs-to-cloudwatch	Stellen Sie sicher, dass für Amazon OpenSearch Service-Domains Fehlerprotokolle aktiviert und zur Aufbewahrung und Beantwortung an Amazon CloudWatch Logs gestreamt werden. OpenSearch Service-Fehlerprotokolle können bei Sicherheits- und Zugriffsprüfungen helfen und bei der Diagnose von Verfügbarkeitsproblemen helfen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AU-6(3)	AU-6(3) Prüfung, Analyse und Berichterstattung | Korrelation der Prüfungs-Repositorys	rds-logging-enabled	Um die Protokollierung und Überwachung in Ihrer Umgebung zu erleichtern, stellen Sie sicher, dass die Amazon Relational Database Service (Amazon RDS)-Protokollierung aktiviert ist. Mit der Amazon-RDS-Protokollierung können Sie Ereignisse wie Verbindungen, Verbindungsabbrüche, Abfragen oder abgefragte Tabellen erfassen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AU-6(3)	AU-6(3) Prüfung, Analyse und Berichterstattung | Korrelation der Prüfungs-Repositorys	redshift-cluster-configuration-check	Um Daten im Ruhezustand zu schützen, muss die Verschlüsselung für Ihre Amazon-Redshift-Cluster aktiviert sein. Sie müssen auch sicherstellen, dass die erforderlichen Konfigurationen auf Amazon-Redshift-Clustern bereitgestellt werden. Die Prüfungsprotokollierung muss aktiviert sein, um Informationen zu Verbindungen und Benutzeraktivitäten in der Datenbank bereitzustellen. Diese Regel erfordert, dass ein Wert für clusterDbEncrypted (Config Default: TRUE) und LoggingEnabled (Config Default: TRUE) gesetzt ist. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AU-6(3)	AU-6(3) Prüfung, Analyse und Berichterstattung | Korrelation der Prüfungs-Repositorys	s3- bucket-logging-enabled	Die Amazon Simple Storage Service (Amazon S3)-Serverzugriffsprotokollierung bietet eine Methode zur Überwachung des Netzwerks im Hinblick auf potenzielle Cybersicherheitsereignisse. Die Ereignisse werden überwacht, indem detaillierte Aufzeichnungen über die Anfragen erfasst werden, die an einen Amazon-S3-Bucket gestellt wurden. Jeder Zugriffsprotokolleintrag enthält Details zu einer einzelnen Zugriffsanfrage. Zu den Details gehören Auftraggeber, Bucket-Name, Anforderungszeit, Anforderungsaktion, Antwortstatus und Fehlercode, falls relevant.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AU-6(3)	AU-6(3) Prüfung, Analyse und Berichterstattung | Korrelation der Prüfungs-Repositorys	vpc-flow-logs-enabled	VPC-Flow-Protokolle erfassen detaillierte Informationsdatensätze über den IP-Datenverkehr, der zu und von Netzwerkschnittstellen in Ihrer Amazon Virtual Private Cloud (Amazon VPC) fließt. Standardmäßig enthalten Flow-Protokolldatensätze Werte für die verschiedenen Komponenten des IP-Flows, einschließlich Quelle, Ziel und Protokoll.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AU-6(3)	AU-6(3) Prüfung, Analyse und Berichterstattung | Korrelation der Prüfungs-Repositorys	wafv2-logging-enabled	Um die Protokollierung und Überwachung in Ihrer Umgebung zu erleichtern, aktivieren Sie die AWS WAF (V2) -Protokollierung im regionalen und globalen Web ACLs. AWS Die WAF-Protokollierung bietet detaillierte Informationen über den Datenverkehr, der von Ihrer Web-ACL analysiert wird. In den Protokollen werden die Uhrzeit aufgezeichnet, zu der die AWS WAF die Anfrage von Ihrer AWS Ressource erhalten hat, Informationen zu der Anfrage und eine Aktion für die Regel, der jede Anfrage entsprach.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AU-7(1)	AU-7(1) Reduzierung von Prüfungen und Berichtserstellung | Automatische Verarbeitung	cloud-trail-cloud-watch-logs-aktiviert	Verwenden Sie Amazon CloudWatch , um Protokoll ereignisaktivitäten zentral zu sammeln und zu verwalten. Die Aufnahme von AWS CloudTrail Daten liefert Einzelheiten zu den API-Aufrufaktivitäten in Ihrem AWS-Konto.
CCCS-fPBMM-AU-8.B	AU-8.B Zeitstempel	api-gw-execution-logging-aktiviert	Die API-Gateway-Protokollierung zeigt detaillierte Ansichten der Benutzer, die auf die API zugegriffen haben, und wie diese Benutzer auf die API zugegriffen haben. Diese Einblicke ermöglichen die Transparenz von Benutzeraktivitäten.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AU-8.B	AU-8.B Zeitstempel	cloudtrail-s3-data events-enabled	Die Erfassung von Simple Storage Service (Amazon S3)-Datenereignissen unterstützt die Erkennung von ungewöhnlichen Aktivitäten. Zu den Details gehören Informationen zu dem AWS -Konto, das auf einen Amazon-S3-Bucket zugegriffen hat, die IP-Adresse und die Uhrzeit des Ereignisses.
CCCS-fPBMM-AU-8.B	AU-8.B Zeitstempel	cloud-trail-cloud-watch-logs-aktiviert	Verwenden Sie Amazon CloudWatch , um Protokoll ereignisaktivitäten zentral zu sammeln und zu verwalten. Die Aufnahme von AWS CloudTrail Daten liefert Einzelheiten zu den API-Aufrufaktivitäten in Ihrem AWS-Konto.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AU-8.B	AU-8.B Zeitstempel	cloudtrail-enabled	AWS CloudTrail kann bei der Nichtabstreitbarkeit helfen, indem Aktionen und API-Aufrufe der AWS Management Console aufgezeichnet werden. Sie können die Benutzer und die Benutzer AWS-Konten , die einen AWS Dienst aufgerufen haben, die Quell-IP-Adresse, über die die Aufrufe generiert wurden, und den Zeitpunkt der Anrufe identifizieren. Einzelheiten zu den erfassten Daten finden Sie unter Inhalt des AWS CloudTrail Datensatzes.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AU-8.B	AU-8.B Zeitstempel	elasticsearch-logs-to-cloudwatch	Stellen Sie sicher, dass für Amazon OpenSearch Service-Domains Fehlerprotokolle aktiviert und zur Aufbewahrung und Beantwortung an Amazon CloudWatch Logs gestreamt werden. Domain-Fehlerprotokolle sind bei Sicherheits- und Zugriffsprüfungen sowie bei der Diagnose von Verfügbarkeitsproblemen nützlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AU-8.B	AU-8.B Zeitstempel	elb-logging-enabled	Die Elastic-Load-Balancing-Aktivität ist ein zentraler Kommunikationspunkt innerhalb einer Umgebung. Stellen Sie sicher, dass die ELB-Protokollierung aktiviert ist. Die gesammelten Daten enthalten detaillierte Informationen zu Anfragen, die an den ELB gesendet wurden. Jedes Protokoll enthält Informationen wie die Zeit, zu der die Anforderung einging, die Client-IP-Adresse, Latenzen, Anforderungspfade und Serverantworten.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AU-8.B	AU-8.B Zeitstempel	multi-region-cloudtrail-enabled	AWS CloudTrail zeichnet Aktionen und API-Aufrufe der AWS Management Console auf. Sie können feststellen, welche Benutzer und Konten angerufen wurden AWS, von welcher Quell-IP-Adresse aus die Anrufe getätigt wurden und wann die Anrufe erfolgten. CloudTrail übermittelt Protokolldateien aus allen AWS Regionen an Ihren S3-Bucket , wenn MULTI_REGION_CLOUD_TRAIL_ENABLED aktiviert ist. Außerdem wird beim AWS Start einer neuen Region derselbe Trail in der neuen Region erstellt. CloudTrail Dadurch erhalten Sie automatisch Protokolldateien mit API-Aktivitäten für die neue Region.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AU-8.B	AU-8.B Zeitstempel	opensearch-logs-to-cloudwatch	Stellen Sie sicher, dass für Amazon OpenSearch Service-Domains Fehlerprotokolle aktiviert und zur Aufbewahrung und Beantwortung an Amazon CloudWatch Logs gestreamt werden. OpenSearch Service-Fehlerprotokolle können bei Sicherheits- und Zugriffsprüfungen helfen und bei der Diagnose von Verfügbarkeitsproblemen helfen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AU-8.B	AU-8.B Zeitstempel	rds-logging-enabled	Um die Protokollierung und Überwachung in Ihrer Umgebung zu erleichtern, stellen Sie sicher, dass die Amazon Relational Database Service (Amazon RDS)-Protokollierung aktiviert ist. Mit der Amazon-RDS-Protokollierung können Sie Ereignisse wie Verbindungen, Verbindungsabbrüche, Abfragen oder abgefragte Tabellen erfassen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AU-8.B	AU-8.B Zeitstempel	redshift-cluster-configuration-check	Um Daten im Ruhezustand zu schützen, muss die Verschlüsselung für Ihre Amazon-Redshift-Cluster aktiviert sein. Sie müssen auch sicherstellen, dass die erforderlichen Konfigurationen auf Amazon-Redshift-Clustern bereitgestellt werden. Die Prüfungsprotokollierung muss aktiviert sein, um Informationen zu Verbindungen und Benutzeraktivitäten in der Datenbank bereitzustellen. Diese Regel erfordert, dass ein Wert für clusterDbEncrypted (Config Default: TRUE) und LoggingEnabled (Config Default: TRUE) gesetzt ist. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AU-8.B	AU-8.B Zeitstempel	s3- bucket-logging-enabled	Die Amazon Simple Storage Service (Amazon S3)-Serverzugriffs protokollierung bietet eine Methode zur Überwachu ng des Netzwerks im Hinblick auf potenzielle Cybersich erheitsereignisse. Die Ereignisse werden überwacht, indem detaillierte Aufzeichn ungen über die Anfragen erfasst werden, die an einen Amazon-S3-Bucket gestellt wurden. Jeder Zugriffsprotokolle intrag enthält Details zu einer einzelnen Zugriffsanfrage. Zu den Details gehören Auftraggeber, Bucket-Name, Anforderu ngszeit, Anforderu ngsaktion, Antwortst atus und Fehlercode, falls relevant.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AU-8.B	AU-8.B Zeitstempel	vpc-flow-logs-enabled	VPC-Flow-Protokolle erfassen detaillierte Informationsdatensätze über den IP-Datenverkehr, der zu und von Netzwerkschnittstellen in Ihrer Amazon Virtual Private Cloud (Amazon VPC) fließt. Standardmäßig enthalten Flow-Protokolldatensätze Werte für die verschiedenen Komponenten des IP-Flows, einschließlich Quelle, Ziel und Protokoll.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AU-8.B	AU-8.B Zeitstempel	wafv2-logging-enabled	Um die Protokollierung und Überwachung in Ihrer Umgebung zu erleichtern, aktivieren Sie die AWS WAF (V2) -Protokollierung im regionalen und globalen Web ACLs. AWS Die WAF-Protokollierung bietet detaillierte Informationen über den Datenverkehr, der von Ihrer Web-ACL analysiert wird. In den Protokollen werden die Uhrzeit aufgezeichnet, zu der die AWS WAF die Anfrage von Ihrer AWS Ressource erhalten hat, Informationen zu der Anfrage und eine Aktion für die Regel, der jede Anfrage entsprach.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AU-9(2)	AU-9(2) Schutz von Prüfungsinformationen | Prüfungs-Backup auf separaten physischen Systemen/Komponenten	backup-plan-min-frequency-and-min-retention-check	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihr AWS Backup-Plan auf eine Mindestfrequenz und Aufbewahrung festgelegt ist. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen. Mit dieser Regel können Sie die Parameter requiredFrequencyValue (Config default: 1), requiredRetentionDays (Config default: 35) und requiredFrequencyUnit

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
			(Config default: days) festlegen. Der tatsächliche Wert muss den Anforderungen Ihrer Organisation entsprechen.
CCCS-fPBMM-AU-9(2)	AU-9(2) Schutz von Prüfungsinformationen | Prüfungs-Backup auf separaten physischen Systemen/Komponenten	s3- bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) unterstützt die Aufrechterhaltung einer angemessenen Kapazität und Verfügbarkeit. CRR ermöglicht das automatische, asynchrone Kopieren von Objekten in Amazon-S3-Buckets, um die Datenverfügbarkeit sicherzustellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AU-9(2)	AU-9(2) Schutz von Prüfungsinformationen | Prüfungs-Backup auf separaten physischen Systemen/Komponenten	s-3 bucket-versioning-enabled	Die Versionsverwaltung von Amazon Simple Storage Service (Amazon S3)-Buckets hilft dabei, mehrere Varianten eines Objekts im selben Amazon-S3-Bucket zu speichern. Verwenden Sie die Versionsverwaltung, um sämtliche Versionen aller Objekte in Ihrem Amazon-S3-Bucket zu speichern, abzurufen oder wiederherzustellen. Mit der Versionsverwaltung können Sie Versionen sowohl nach unbeabsichtigten Benutzeraktionen als auch nach Anwendungsfehlern problemlos wiederherstellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AU-9.A	AU-9.A Schutz von Prüfungsinformationen	cloud-trail-encryption-enabled	Zum Schutz von eventuell vorhandenen sensiblen Daten sowie Daten im Ruhezustand müssen Sie sicherstellen, dass die Verschlüsselung für Ihre AWS CloudTrail aktiviert ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AU-9.A	AU-9.A Schutz von Prüfungsinformationen	cloud-trail-log-file-Validierung aktiviert	Verwenden Sie die AWS CloudTrail Protokolldateivalidierung, um die Integrität von Protokollen zu überprüfen. CloudTrail Mithilfe der Protokolldateivalidierung kann festgestellt werden, ob eine Protokolldatei geändert oder gelöscht wurde oder ob sie nach der Übermittlung CloudTrail unverändert geblieben ist. Dieses Feature wurde mit dem Branchenstandard entsprechenden Algorithmen entwickelt: SHA-256 für die Hashfunktion und SHA-256 mit RSA für digitale Signaturen. Aus diesem Grund ist es rechnerisch unmöglich, CloudTrail Protokolldateien unbemerkt zu ändern, zu löschen oder zu fälschen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AU-9.A	AU-9.A Schutz von Prüfungsinformationen	s3- aktiviert bucket-server-side-encryption	Zum Schutz von Daten im Ruhezustand müssen Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon Simple Storage Service (Amazon S3)-Buckets aktiviert ist. Da sensible Daten in Amazon-S3-Buckets gespeichert werden können, sollten Sie die Verschlüsselung aktivieren, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AU-11.A	AU-11.A Aufbewahrung von Prüfungsaufzeichnungen	cw-loggroup-retention-period-überprüfen	Stellen Sie sicher, dass die Ereignisprotokolldaten für Ihre Protokollgruppen über eine Mindestdauer aufbewahrt werden, um die Fehlerbehebung und forensische Untersuchungen zu unterstützen. Fehlende frühere Ereignisprotokolldaten erschweren die Rekonstruierung und Identifizierung potenziell schädlicher Ereignisse.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AU-11.B	AU-11.B Aufbewahrung von Prüfungsaufzeichnungen	cw-loggroup-retention-period-überprüfen	Stellen Sie sicher, dass die Ereignisprotokolldaten für Ihre Protokollgruppen über eine Mindestdauer aufbewahrt werden, um die Fehlerbehebung und forensische Untersuchungen zu unterstützen. Fehlende frühere Ereignisprotokolldaten erschweren die Rekonstruierung und Identifizierung potenziell schädlicher Ereignisse.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AU-11.C	AU-11.C Aufbewahrung von Prüfungsaufzeichnungen	cw-loggroup-retention-period-überprüfen	Stellen Sie sicher, dass die Ereignisprotokolldaten für Ihre Protokollgruppen über eine Mindestdauer aufbewahrt werden, um die Fehlerbehebung und forensische Untersuchungen zu unterstützen. Fehlende frühere Ereignisprotokolldaten erschweren die Rekonstruierung und Identifizierung potenziell schädlicher Ereignisse.
CCCS-fPBMM-AU-12.A	AU-12.A Generierung von Prüfungen	api-gw-execution-logging-aktiviert	Die API-Gateway-Protokollierung zeigt detaillierte Ansichten der Benutzer, die auf die API zugegriffen haben, und wie diese Benutzer auf die API zugegriffen haben. Diese Einblicke ermöglichen die Transparenz von Benutzeraktivitäten.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AU-12.A	AU-12.A Generierung von Prüfungen	cloudtrail-s3-data events-enabled	Die Erfassung von Simple Storage Service (Amazon S3)-Datenereignissen unterstützt die Erkennung von ungewöhnlichen Aktivitäten. Zu den Details gehören Informationen zu dem AWS -Konto, das auf einen Amazon-S3-Bucket zugegriffen hat, die IP-Adresse und die Uhrzeit des Ereignisses.
CCCS-fPBMM-AU-12.A	AU-12.A Generierung von Prüfungen	cloud-trail-cloud-watch-logs-aktiviert	Verwenden Sie Amazon CloudWatch , um Protokoll ereignisaktivitäten zentral zu sammeln und zu verwalten. Die Aufnahme von AWS CloudTrail Daten liefert Einzelheiten zu den API-Aufrufaktivitäten in Ihrem AWS-Konto.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AU-12.A	AU-12.A Generierung von Prüfungen	cloudtrail-enabled	AWS CloudTrail kann bei der Nichtabstreitbarkeit helfen, indem Aktionen und API-Aufrufe der AWS Management Console aufgezeichnet werden. Sie können die Benutzer und die Benutzer AWS-Konten , die einen AWS Dienst aufgerufen haben, die Quell-IP-Adresse, über die die Aufrufe generiert wurden, und den Zeitpunkt der Anrufe identifizieren. Einzelheiten zu den erfassten Daten finden Sie unter Inhalt des AWS CloudTrail Datensatzes.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AU-12.A	AU-12.A Generierung von Prüfungen	elasticsearch-logs-to-cloudwatch	Stellen Sie sicher, dass für Amazon OpenSearch Service-Domains Fehlerprotokolle aktiviert und zur Aufbewahrung und Beantwortung an Amazon CloudWatch Logs gestreamt werden. Domain-Fehlerprotokolle sind bei Sicherheits- und Zugriffsprüfungen sowie bei der Diagnose von Verfügbarkeitsproblemen nützlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AU-12.A	AU-12.A Generierung von Prüfungen	elb-logging-enabled	Die Elastic-Load-Balancing-Aktivität ist ein zentraler Kommunikationspunkt innerhalb einer Umgebung. Stellen Sie sicher, dass die ELB-Protokollierung aktiviert ist. Die gesammelten Daten enthalten detaillierte Informationen zu Anfragen, die an den ELB gesendet wurden. Jedes Protokoll enthält Informationen wie die Zeit, zu der die Anforderung einging, die Client-IP-Adresse, Latenzen, Anforderungspfade und Serverantworten.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AU-12.A	AU-12.A Generierung von Prüfungen	multi-region-cloudtrail-enabled	AWS CloudTrail zeichnet Aktionen und API-Aufrufe der AWS Management Console auf. Sie können feststellen, welche Benutzer und Konten angerufen wurden AWS, von welcher Quell-IP-Adresse aus die Anrufe getätigt wurden und wann die Anrufe erfolgten. CloudTrail übermittelt Protokolldateien aus allen AWS Regionen an Ihren S3-Bucket , wenn MULTI_REGION_CLOUD_TRAIL_ENABLED aktiviert ist. Außerdem wird beim AWS Start einer neuen Region derselbe Trail in der neuen Region erstellt. CloudTrail Dadurch erhalten Sie automatisch Protokolldateien mit API-Aktivitäten für die neue Region.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AU-12.A	AU-12.A Generierung von Prüfungen	opensearch-logs-to-cloudwatch	Stellen Sie sicher, dass für Amazon OpenSearch Service-Domains Fehlerprotokolle aktiviert und zur Aufbewahrung und Beantwortung an Amazon CloudWatch Logs gestreamt werden. OpenSearch Service-Fehlerprotokolle können bei Sicherheits- und Zugriffsprüfungen helfen und bei der Diagnose von Verfügbarkeitsproblemen helfen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AU-12.A	AU-12.A Generierung von Prüfungen	rds-logging-enabled	Um die Protokollierung und Überwachung in Ihrer Umgebung zu erleichtern, stellen Sie sicher, dass die Amazon Relational Database Service (Amazon RDS)-Protokollierung aktiviert ist. Mit der Amazon-RDS-Protokollierung können Sie Ereignisse wie Verbindungen, Verbindungsabbrüche, Abfragen oder abgefragte Tabellen erfassen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AU-12.A	AU-12.A Generierung von Prüfungen	redshift-cluster-configuration-check	Um Daten im Ruhezustand zu schützen, muss die Verschlüsselung für Ihre Amazon-Redshift-Cluster aktiviert sein. Sie müssen auch sicherstellen, dass die erforderlichen Konfigurationen auf Amazon-Redshift-Clustern bereitgestellt werden. Die Prüfungsprotokollierung muss aktiviert sein, um Informationen zu Verbindungen und Benutzeraktivitäten in der Datenbank bereitzustellen. Diese Regel erfordert, dass ein Wert für clusterDbEncrypted (Config Default: TRUE) und LoggingEnabled (Config Default: TRUE) gesetzt ist. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AU-12.A	AU-12.A Generierung von Prüfungen	s3- bucket-logging-enabled	Die Amazon Simple Storage Service (Amazon S3)-Serverzugriffs protokollierung bietet eine Methode zur Überwachu ng des Netzwerks im Hinblick auf potenzielle Cybersich erheitsereignisse. Die Ereignisse werden überwacht, indem detaillierte Aufzeichn ungen über die Anfragen erfasst werden, die an einen Amazon-S3-Bucket gestellt wurden. Jeder Zugriffsprotokolle intrag enthält Details zu einer einzelnen Zugriffsanfrage. Zu den Details gehören Auftraggeber, Bucket-Name, Anforderu ngszeit, Anforderu ngsaktion, Antwortst atus und Fehlercode, falls relevant.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AU-12.A	AU-12.A Generierung von Prüfungen	vpc-flow-logs-enabled	VPC-Flow-Protokolle erfassen detaillierte Informationsdatensätze über den IP-Datenverkehr, der zu und von Netzwerkschnittstellen in Ihrer Amazon Virtual Private Cloud (Amazon VPC) fließt. Standardmäßig enthalten Flow-Protokolldatensätze Werte für die verschiedenen Komponenten des IP-Flows, einschließlich Quelle, Ziel und Protokoll.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AU-12.A	AU-12.A Generierung von Prüfungen	wafv2-logging-enabled	Um die Protokollierung und Überwachung in Ihrer Umgebung zu erleichtern, aktivieren Sie die AWS WAF (V2) -Protokollierung im regionalen und globalen Web ACLs. AWS Die WAF-Protokollierung bietet detaillierte Informationen über den Datenverkehr, der von Ihrer Web-ACL analysiert wird. In den Protokollen werden die Uhrzeit aufgezeichnet, zu der die AWS WAF die Anfrage von Ihrer AWS Ressource erhalten hat, Informationen zu der Anfrage und eine Aktion für die Regel, der jede Anfrage entsprach.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AU-12.C	AU-12.C Generierung von Prüfungen	api-gw-execution-logging-aktiviert	Die API-Gateway-Protokollierung zeigt detaillierte Ansichten der Benutzer, die auf die API zugegriffen haben, und wie diese Benutzer auf die API zugegriffen haben. Diese Einblicke ermöglichen die Transparenz von Benutzeraktivitäten.
CCCS-fPBMM-AU-12.C	AU-12.C Generierung von Prüfungen	cloudtrail-s3-dataevents-enabled	Die Erfassung von Simple Storage Service (Amazon S3)-Datenereignissen unterstützt die Erkennung von ungewöhnlichen Aktivitäten. Zu den Details gehören Informationen zu dem AWS -Konto, das auf einen Amazon-S3-Bucket zugegriffen hat, die IP-Adresse und die Uhrzeit des Ereignisses.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AU-12.C	AU-12.C Generierung von Prüfungen	cloud-trail-cloud-watch-logs-aktiviert	Verwenden Sie Amazon CloudWatch , um Protokoll ereignisaktivitäten zentral zu sammeln und zu verwalten. Die Aufnahme von AWS CloudTrail Daten liefert Einzelheiten zu den API-Aufrufaktivitäten in Ihrem AWS-Konto.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AU-12.C	AU-12.C Generierung von Prüfungen	cloudtrail-enabled	AWS CloudTrail kann bei der Nichtabstreitbarkeit helfen, indem Aktionen und API-Aufrufe der AWS Management Console aufgezeichnet werden. Sie können die Benutzer und die Benutzer AWS-Konten , die einen AWS Dienst aufgerufen haben, die Quell-IP-Adresse, über die die Aufrufe generiert wurden, und den Zeitpunkt der Anrufe identifizieren. Einzelheiten zu den erfassten Daten finden Sie unter Inhalt des AWS CloudTrail Datensatzes.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AU-12.C	AU-12.C Generierung von Prüfungen	elb-logging-enabled	Die Elastic-Load-Balancing-Aktivität ist ein zentraler Kommunikationspunkt innerhalb einer Umgebung. Stellen Sie sicher, dass die ELB-Protokollierung aktiviert ist. Die gesammelten Daten enthalten detaillierte Informationen zu Anfragen, die an den ELB gesendet wurden. Jedes Protokoll enthält Informationen wie die Zeit, zu der die Anforderung einging, die Client-IP-Adresse, Latenzen, Anforderungspfade und Serverantworten.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AU-12.C	AU-12.C Generierung von Prüfungen	multi-region-cloudtrail-enabled	AWS CloudTrail zeichnet Aktionen und API-Aufrufe der AWS Management Console auf. Sie können feststellen, welche Benutzer und Konten angerufen wurden AWS, von welcher Quell-IP-Adresse aus die Anrufe getätigt wurden und wann die Anrufe erfolgten. CloudTrail übermittelt Protokolldateien aus allen AWS Regionen an Ihren S3-Bucket , wenn MULTI_REGION_CLOUD_TRAIL_ENABLED aktiviert ist. Außerdem wird beim AWS Start einer neuen Region derselbe Trail in der neuen Region erstellt. CloudTrail Dadurch erhalten Sie automatisch Protokolldateien mit API-Aktivitäten für die neue Region.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AU-12.C	AU-12.C Generierung von Prüfungen	rds-logging-enabled	Um die Protokollierung und Überwachung in Ihrer Umgebung zu erleichtern, stellen Sie sicher, dass die Amazon Relational Database Service (Amazon RDS)-Protokollierung aktiviert ist. Mit der Amazon-RDS-Protokollierung können Sie Ereignisse wie Verbindungen, Verbindungsabbrüche, Abfragen oder abgefragte Tabellen erfassen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AU-12.C	AU-12.C Generierung von Prüfungen	redshift-cluster-configuration-check	Um Daten im Ruhezustand zu schützen, muss die Verschlüsselung für Ihre Amazon-Redshift-Cluster aktiviert sein. Sie müssen auch sicherstellen, dass die erforderlichen Konfigurationen auf Amazon-Redshift-Clustern bereitgestellt werden. Die Prüfungsprotokollierung muss aktiviert sein, um Informationen zu Verbindungen und Benutzeraktivitäten in der Datenbank bereitzustellen. Diese Regel erfordert, dass ein Wert für clusterDbEncrypted (Config Default: TRUE) und LoggingEnabled (Config Default: TRUE) gesetzt ist. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AU-12.C	AU-12.C Generierung von Prüfungen	s3- bucket-logging-enabled	Die Amazon Simple Storage Service (Amazon S3)-Serverzugriffs protokollierung bietet eine Methode zur Überwachu ng des Netzwerks im Hinblick auf potenzielle Cybersich erheitsereignisse. Die Ereignisse werden überwacht, indem detaillierte Aufzeichn ungen über die Anfragen erfasst werden, die an einen Amazon-S3-Bucket gestellt wurden. Jeder Zugriffsprotokolle intrag enthält Details zu einer einzelnen Zugriffsanfrage. Zu den Details gehören Auftraggeber, Bucket-Name, Anforderu ngszeit, Anforderu ngsaktion, Antwortst atus und Fehlercode, falls relevant.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AU-12.C	AU-12.C Generierung von Prüfungen	vpc-flow-logs-enabled	VPC-Flow-Protokolle erfassen detaillierte Informationsdatensätze über den IP-Datenverkehr, der zu und von Netzwerkschnittstellen in Ihrer Amazon Virtual Private Cloud (Amazon VPC) fließt. Standardmäßig enthalten Flow-Protokolldatensätze Werte für die verschiedenen Komponenten des IP-Flows, einschließlich Quelle, Ziel und Protokoll.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-AU-12.C	AU-12.C Generierung von Prüfungen	wafv2-logging-enabled	Um die Protokollierung und Überwachung in Ihrer Umgebung zu erleichtern, aktivieren Sie die AWS WAF (V2) -Protokollierung im regionalen und globalen Web ACLs. AWS Die WAF-Protokollierung bietet detaillierte Informationen über den Datenverkehr, der von Ihrer Web-ACL analysiert wird. In den Protokollen werden die Uhrzeit aufgezeichnet, zu der die AWS WAF die Anfrage von Ihrer AWS Ressource erhalten hat, Informationen zu der Anfrage und eine Aktion für die Regel, der jede Anfrage entsprach.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CA-3(5)	CA-3(5) Systemverbindungen | Einschränkungen bei externen Netzwerkverbindungen	dms-replication-not-public	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass auf DMS-Replikationsinstanzen nicht öffentlich zugegriffen werden kann. DMS-Replikations-Instances können vertrauliche Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.
CCCS-fPBMM-CA-3(5)	CA-3(5) Systemverbindungen | Einschränkungen bei externen Netzwerkverbindungen	ebs-snapshot-public-restorable-überprüfen	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass EBS-Snapshots nicht öffentlich wiederherstellbar sind. EBS-Volume-Snapshots können vertrauliche Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CA-3(5)	CA-3(5) Systemverbindungen | Einschränkungen bei externen Netzwerkverbindungen	ec-2 instance-no-public-ip	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon Elastic Compute Cloud (Amazon EC2) - Instances nicht öffentlich zugänglich sind. EC2Amazon -Instances können vertrauliche Informationen enthalten, und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CA-3(5)	CA-3(5) Systemverbindungen | Einschränkungen bei externen Netzwerkverbindungen	eip-attached	Diese Regel stellt sicher, dass Elastic, die einer Amazon Virtual Private Cloud (Amazon VPC) IPs zugewiesen sind, an Amazon Elastic Compute Cloud (Amazon EC2) - Instances oder verwendete Elastic Network Interfaces angehängt sind. Diese Regel hilft bei der Überwachung ungenutzter Inhalte EIPs in Ihrer Umgebung.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CA-3(5)	CA-3(5) Systemverbindungen | Einschränkungen bei externen Netzwerkverbindungen	elasticsearch-in-vpc-only	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass sich Amazon OpenSearch OpenSearch Service (Service) - Domains innerhalb einer Amazon Virtual Private Cloud (Amazon VPC) befinden. Eine OpenSearch Service-Domain innerhalb einer Amazon VPC ermöglicht die sichere Kommunikation zwischen OpenSearch Service und anderen Services innerhalb der Amazon VPC, ohne dass ein Internet-Gateway, ein NAT-Gerät oder eine VPN-Verbindung erforderlich ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CA-3(5)	CA-3(5) Systemverbindungen | Einschränkungen bei externen Netzwerkverbindungen	emr-master-no-public-ip	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon EMR-Cluster-Masterknoten nicht öffentlich zugänglich sind. Amazon-EMR-Cluster-Hauptknoten können vertrauliche Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CA-3(5)	CA-3(5) Systemverbindungen | Einschränkungen bei externen Netzwerkverbindungen	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) Security Groups können bei der Verwaltung des Netzwerkzugriffs helfen, indem sie eine statusbehaftete Filterung des ein- und ausgehenden Netzwerkverkehrs zu Ressourcen bereitstellen. AWS Wenn Sie eingehenden (oder entfernten) Datenverkehr von 0.0.0.0/0 bis Port 22 auf Ihren Ressourcen nicht zulassen, können Sie den Remote-Zugriff einschränken.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CA-3(5)	CA-3(5) Systemverbindungen | Einschränkungen bei externen Netzwerkverbindungen	ec-2 instances-in-vpc	Stellen Sie Amazon Elastic Compute Cloud (Amazon EC2) -Instances innerhalb einer Amazon Virtual Private Cloud (Amazon VPC) bereit, um eine sichere Kommunikation zwischen einer Instance und anderen Services innerhalb der Amazon VPC zu ermöglichen, ohne dass ein Internet-Gateway, ein NAT-Gerät oder eine VPN-Verbindung erforderlich ist. Der gesamte Datenverkehr bleibt sicher in der AWS Cloud. Domains, die sich innerhalb einer VPC befinden, verfügen aufgrund ihrer logischen Isolierung im Vergleich zu Domains mit öffentlichen Endpunkten über eine zusätzliche Sicherheitsebene. Weisen Sie EC2

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
			Amazon-Instances einer Amazon VPC zu, um den Zugriff ordnungsgemäß zu verwalten.
CCCS-fPBMM-CA-3(5)	CA-3(5) Systemverbindungen | Einschränkungen bei externen Netzwerkverbindungen	internet-gateway-authorized-vpc-nur	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Internet-Gateways nur mit autorisierter Amazon Virtual Private Cloud (Amazon VPC) verbunden sind. Internet-Gateways ermöglichen den bidirektionalen Internetzugang zur und von der Amazon VPC, was möglicherweise zu einem unbefugten Zugriff auf Amazon-VPC-Ressourcen führen kann.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CA-3(5)	CA-3(5) Systemverbindungen | Einschränkungen bei externen Netzwerkverbindungen	lambda-function-public-access-verboten	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass AWS Lambda-Funktionen nicht öffentlich zugänglich sind. Der öffentliche Zugriff kann möglicherweise die Verfügbarkeit von Ressourcen beeinträchtigen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CA-3(5)	CA-3(5) Systemverbindungen | Einschränkungen bei externen Netzwerkverbindungen	lambda-inside-vpc	Stellen Sie AWS Lambda-Funktionen in einer Amazon Virtual Private Cloud (Amazon VPC) bereit, um eine sichere Kommunikation zwischen einer Funktion und anderen Diensten innerhalb der Amazon VPC zu gewährleisten. Bei dieser Konfiguration sind kein Internet-Gateway, kein NAT-Gerät und keine VPN-Verbindung erforderlich. Der gesamte Datenverkehr bleibt sicher in der Cloud. AWS Domains, die sich innerhalb einer VPC befinden, verfügen aufgrund ihrer logischen Isolierung im Vergleich zu Domains mit öffentlichen Endpunkten über eine zusätzliche Sicherheitsebene. Um den Zugriff ordnungsgemäß zu verwalten,

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
			sollten AWS Lambda-Funktionen einer VPC zugewiesen werden.
CCCS-fPBMM-CA-3(5)	CA-3(5) Systemverbindungen | Einschränkungen bei externen Netzwerkverbindungen	opensearch-in-vpc-only	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass sich Amazon OpenSearch Service-Domains innerhalb einer Amazon Virtual Private Cloud (Amazon VPC) befinden. Eine Amazon OpenSearch Service-Domain innerhalb einer Amazon VPC ermöglicht die sichere Kommunikation zwischen Amazon OpenSearch Service und anderen Services innerhalb der Amazon VPC, ohne dass ein Internet-Gateway, ein NAT-Gerät oder eine VPN-Verbindung erforderlich ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CA-3(5)	CA-3(5) Systemverbindungen | Einschränkungen bei externen Netzwerkverbindungen	rds-instance-public-access-überprüfen	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Relational Database Service (Amazon RDS) -Instances nicht öffentlich sind. Amazon-RDS-Datenbank-Instances können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CA-3(5)	CA-3(5) Systemverbindungen | Einschränkungen bei externen Netzwerkverbindungen	rds-snapshots-public-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Relational Database Service (Amazon RDS) -Instances nicht öffentlich sind. Amazon-RDS-Datenbank-Instances können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CA-3(5)	CA-3(5) Systemverbindungen | Einschränkungen bei externen Netzwerkverbindungen	redshift-cluster-public-access-überprüfen	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Redshift Redshift-Cluster nicht öffentlich sind. Amazon-Redshift-Cluster können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CA-3(5)	CA-3(5) Systemverbindungen | Einschränkungen bei externen Netzwerkverbindungen	restricted-common-ports	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass gemeinsame Ports für Amazon Elastic Compute Cloud (Amazon EC2) -Sicherheitsgruppen eingeschränkt sind. Wenn der Zugriff auf Ports nicht auf vertrauenswürdige Quellen beschränkt wird, kann dies zu Angriffen auf die Verfügbarkeit, Integrität und Vertraulichkeit von Systemen führen. Mit dieser Regel können Sie optional die Parameter blockedPort1–blockedPort5 festlegen (Standardkonfigurationen: 20, 21, 3389, 3306, 4333). Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CA-3(5)	CA-3(5) Systemverbindungen | Einschränkungen bei externen Netzwerkverbindungen	s3- account-level-public-access -blöcke-periodisch	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Simple Storage Service (Amazon S3) -Buckets nicht öffentlich zugänglich sind. Diese Regel trägt dazu bei, sensible Daten vor unbefugten Remote-Benutzern zu schützen, indem sie den öffentlichen Zugriff verhindert. Mit dieser Regel können Sie optional die Parameter ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) und restrictPublicBuckets Parameter (Config Default: True) festlegen. Die tatsächlichen Werte müssen den Richtlini

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
			en Ihrer Organisation entsprechen.
CCCS-fPBMM-CA-3(5)	CA-3(5) Systemverbindungen | Einschränkungen bei externen Netzwerkverbindungen	s3 bucket-level-public-access - verboten	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Simple Storage Service (Amazon S3) -Buckets nicht öffentlich zugänglich sind. Diese Regel trägt dazu bei, sensible Daten vor unbefugten Remote-Benutzern zu schützen, indem sie den öffentlichen Zugriff auf Bucket-Ebene verhindert.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CA-3(5)	CA-3(5) Systemverbindungen | Einschränkungen bei externen Netzwerkverbindungen	s-3 bucket-public-read-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie nur autorisierten Benutzern, Prozessen und Geräten Zugriff auf Amazon Simple Storage Service (Amazon S3) - Buckets gewähren. Die Verwaltung des Zugriffs sollte mit der Klassifizierung der Daten übereinstimmen.
CCCS-fPBMM-CA-3(5)	CA-3(5) Systemverbindungen | Einschränkungen bei externen Netzwerkverbindungen	s3- bucket-public-write-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie nur autorisierten Benutzern, Prozessen und Geräten Zugriff auf Amazon Simple Storage Service (Amazon S3) - Buckets gewähren. Die Verwaltung des Zugriffs sollte mit der Klassifizierung der Daten übereinstimmen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CA-3(5)	CA-3(5) Systemverbindungen | Einschränkungen bei externen Netzwerkverbindungen	sagemaker-notebook-no-direct-Internetzugang	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass SageMaker Amazon-Notebooks keinen direkten Internetzugang zulassen. Indem Sie direkten Internetzugang blockieren, vermeiden Sie, dass unbefugte Benutzer auf sensible Daten zugreifen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CA-3(5)	CA-3(5) Systemverbindungen | Einschränkungen bei externen Netzwerkverbindungen	subnet-auto-assign-public-ip-deaktiviert	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon Virtual Private Cloud (VPC) -Subnetzen nicht automatisch eine öffentliche IP-Adresse zugewiesen wird. Amazon Elastic Compute Cloud (EC2) -Instances, die in Subnetzen gestartet werden, in denen dieses Attribut aktiviert ist, haben ihrer primären Netzwerkschnittstelle eine öffentliche IP-Adresse zugewiesen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CA-3(5)	CA-3(5) Systemverbindungen | Einschränkungen bei externen Netzwerkverbindungen	vpc-default-security-group-geschlossen	Sicherheitsgruppen von Amazon Elastic Compute Cloud (Amazon EC2) können bei der Verwaltung des Netzwerkzugriffs helfen, indem sie eine statusbehaftete Filterung des ein- und ausgehenden Netzwerkverkehrs zu Ressourcen bereitstellen. AWS Die Beschränkung des gesamten Datenverkehrs auf die Standardsicherheitsgruppe hilft dabei, den Fernzugriff auf Ihre Ressourcen einzuschränken. AWS

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CA-3(5)	CA-3(5) Systemverbindungen | Einschränkungen bei externen Netzwerkverbindungen	vpc-sg-open-only-to-authorized-ports	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass gemeinsame Ports für Amazon Elastic Compute Cloud (Amazon EC2) -Sicherheitsgruppen eingeschränkt sind. Wenn der Zugriff auf Ports nicht auf vertrauenswürdige Quellen beschränkt wird, kann dies zu Angriffen auf die Verfügbarkeit, Integrität und Vertraulichkeit von Systemen führen. Durch die Beschränkung des Zugriffs auf Ressourcen innerhalb einer Sicherheitsgruppe aus dem Internet (0.0.0.0/0) kann der Fernzugriff auf interne Systeme gesteuert werden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CA-7.A	CA-7.A Fortlaufende Überwachung	api-gw-execution-logging-aktiviert	Die API-Gateway-Protokollierung zeigt detaillierte Ansichten der Benutzer, die auf die API zugegriffen haben, und wie diese Benutzer auf die API zugegriffen haben. Diese Einblicke ermöglichen die Transparenz von Benutzeraktivitäten.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CA-7.A	CA-7.A Fortlaufende Überwachung	api-gw-xray-enabled	AWS X-Ray sammelt Daten über Anfragen, die Ihre Anwendung bedient, und bietet Tools, mit denen Sie diese Daten anzeigen, filtern und Einblicke in sie gewinnen können, um Probleme und Optimierungsmöglichkeiten zu identifizieren. Stellen Sie sicher, dass X-Ray aktiviert ist, damit Sie detaillierte Informationen nicht nur über die Anfrage und Antwort, sondern auch über Aufrufe erhalten, die Ihre Anwendung an nachgelagerte AWS Ressourcen, Microservices, Datenbanken und HTTP-Web APIs tätigt.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CA-7.A	CA-7.A Fortlaufende Überwachung	autoscaling-group-elb-healthcheck-erforderlich	Die Elastic Load Balancer (ELB) - Zustandsprüfungen für Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling Scaling-Gruppen unterstützen die Aufrechterhaltung einer angemessenen Kapazität und Verfügbarkeit. Der Load Balancer sendet regelmäßig Pings, versucht Verbindungen herzustellen oder sendet Anfragen, um den Zustand der EC2 Amazon-Instances in einer Gruppe mit auto-scaling zu testen. Wenn eine Instance nicht zurückmeldet, wird der Traffic an eine neue EC2 Amazon-Instance gesendet.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CA-7.A	CA-7.A Fortlaufende Überwachung	beanstalk-enhanced-health-reporting-aktiviert	AWS Die verbesserte Zustandsberichterstattung von Elastic Beanstalk ermöglicht eine schnellere Reaktion auf Veränderungen im Zustand der zugrunde liegenden Infrastruktur. Diese Änderungen könnten zu einer mangelnden Verfügbarkeit der Anwendung führen. Die erweiterten Zustandsberichte von Elastic Beanstalk bieten eine Statusbeschreibung, um den Schweregrad der identifizierten Probleme einzuschätzen und mögliche Ursachen zu identifizieren, die untersucht werden müssen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CA-7.A	CA-7.A Fortlaufende Überwachung	cloudtrail-s3-dataevents-enabled	Die Erfassung von Simple Storage Service (Amazon S3)-Datenereignissen unterstützt die Erkennung von ungewöhnlichen Aktivitäten. Zu den Details gehören Informationen zu dem AWS -Konto, das auf einen Amazon-S3-Bucket zugegriffen hat, die IP-Adresse und die Uhrzeit des Ereignisses.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CA-7.A	CA-7.A Fortlaufende Überwachung	cloudwatch-alarm-action-check	Amazon CloudWatch alarmiert, wenn eine Metrik den Schwellenwert für eine bestimmte Anzahl von Bewertungszeiträumen überschreitet. Der Alarm führt eine oder mehrere Aktionen durch, die vom Wert der Metrik oder des Ausdrucks im Vergleich zu einem Schwellenwert in einer Reihe von Zeiträumen abhängt. Diese Regel erfordert einen Wert für alarmActionRequired (Config Default: True), insufficientDataAction Required (Config Default: True), okActionRequired (Config Default: False). Der tatsächliche Wert muss die Alarmaktionen für Ihre Umgebung widerspiegeln.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CA-7.A	CA-7.A Fortlaufende Überwachung	cloud-trail-cloud-watch-logs-aktiviert	Verwenden Sie Amazon CloudWatch , um Protokoll ereignisaktivitäten zentral zu sammeln und zu verwalten. Die Aufnahme von AWS CloudTrail Daten liefert Einzelheiten zu den API-Aufrufaktivitäten in Ihrem AWS-Konto.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CA-7.A	CA-7.A Fortlaufende Überwachung	cloudtrail-enabled	AWS CloudTrail kann bei der Nichtabstreitbarkeit helfen, indem Aktionen und API-Aufrufe der AWS Management Console aufgezeichnet werden. Sie können die Benutzer und die Benutzer AWS-Konten , die einen AWS Dienst aufgerufen haben, die Quell-IP-Adresse, über die die Aufrufe generiert wurden, und den Zeitpunkt der Anrufe identifizieren. Einzelheiten zu den erfassten Daten finden Sie unter Inhalt des AWS CloudTrail Datensatzes.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CA-7.A	CA-7.A Fortlaufende Überwachung	cw-loggroup-retention-period-überprüfen	Stellen Sie sicher, dass die Ereignisprotokolldaten für Ihre Protokollgruppen über eine Mindestdauer aufbewahrt werden, um die Fehlerbehebung und forensische Untersuchungen zu unterstützen. Fehlende frühere Ereignisprotokolldaten erschweren die Rekonstruierung und Identifizierung potenziell schädlicher Ereignisse.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CA-7.A	CA-7.A Fortlaufende Überwachung	dynamodb-throughput-limit-check	Aktivieren Sie diese Regel, um sicherzustellen, dass die bereitgestellte Durchsatzkapazität in Ihren Amazon-DynamoDB-Tabellen überprüft wird. Dies ist der Umfang der Lese- und Schreibaktivitäten, der von den jeweiligen Tabellen unterstützt werden kann. DynamoDB verwendet diese Informationen für das Reservieren ausreichender Systemressourcen, um Ihren Durchsatz anforderungen gerecht zu werden. Diese Regel generiert eine Warnung, wenn sich der Durchsatz dem Höchstlimit für ein Kundenkonto nähert. Mit dieser Regel können Sie optional die Parameter RCUThreshold Kontoprozentsatz

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
			(Konfigurationsstandard: 80) und WCUThreshold Kontoprozentsatz (Konfigurationsstandard: 80) festlegen. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.
CCCS-fPBMM-CA-7.A	CA-7.A Fortlaufende Überwachung	ec2-imdsv2-check	Stellen Sie sicher, dass die Methode Instance Metadata Service Version 2 (IMDSv2) aktiviert ist, um den Zugriff auf und die Kontrolle der Amazon Elastic Compute Cloud (Amazon EC2) - Instance-Metadaten zu schützen. Die IMDSv2 Methode verwendet sitzungsbasierte Kontrollen. Mit können Kontrollen implementiert werden IMDSv2, um Änderungen an Instanzmetadaten einzuschränken.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CA-7.A	CA-7.A Fortlaufende Überwachung	ec-2 instance-detailed-monitoring-enabled	Aktivieren Sie diese Regel, um die Amazon Elastic Compute Cloud (Amazon EC2) - Instance-Überwachung auf der EC2 Amazon-Konsole zu verbessern, in der Monitoring-Diagramme mit einem Zeitraum von 1 Minute für die Instance angezeigt werden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CA-7.A	CA-7.A Fortlaufende Überwachung	ecs-task-definition-user-for-host-mode-check	Wenn für eine Aufgabendefinition erhöhte Berechtigungen gelten, liegt das daran, dass der Kunde diesen Konfigurationen ausdrücklich zugestimmt hat. Diese Kontrolle prüft, ob eine unerwartete Berechtigungseskalation vorliegt, wenn für eine Aufgabendefinition das Host-Netzwerk aktiviert ist, die Kunden aber keine erhöhten Berechtigungen aktiviert haben.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CA-7.A	CA-7.A Fortlaufende Überwachung	elb-logging-enabled	Die Elastic-Load-Balancing-Aktivität ist ein zentraler Kommunikationspunkt innerhalb einer Umgebung. Stellen Sie sicher, dass die ELB-Protokollierung aktiviert ist. Die gesammelten Daten enthalten detaillierte Informationen zu Anfragen, die an den ELB gesendet wurden. Jedes Protokoll enthält Informationen wie die Zeit, zu der die Anforderung einging, die Client-IP-Adresse, Latenzen, Anforderungspfade und Serverantworten.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CA-7.A	CA-7.A Fortlaufende Überwachung	guardduty-enabled-centralized	Amazon GuardDuty kann mithilfe von Threat Intellige nce Feeds helfen, potenzielle Cybersich erheitsereignisse zu überwachen und zu erkennen. Dazu gehören Listen mit bösartigen IPs und maschinel len Lernmethoden zur Identifizierung unerwarteter, nicht autorisierter und bösartiger Aktivitäten in Ihrer AWS Cloud-Umgebung.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CA-7.A	CA-7.A Fortlaufende Überwachung	guardduty-non-archived-findings	Amazon GuardDuty hilft Ihnen dabei, die Auswirkungen eines Vorfalls zu verstehen, indem es die Ergebnisse nach Schweregrad klassifiziert: niedrig, mittel und hoch. Diese Klassifizierungen können Sie zur Festlegung von entsprechenden Strategien und Prioritäten zur Behebung solcher Vorfälle verwenden. Mit dieser Regel können Sie optional daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7) und daysHighSev (Config Default: 1) für nicht archivierte Ergebnisse festlegen, wie es die Richtlinien Ihrer Organisation erfordern.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CA-7.A	CA-7.A Fortlaufende Überwachung	lambda-dlq-check	Aktivieren Sie diese Regel, um das entsprechende Personal über Amazon Simple Queue Service (Amazon SQS) oder Amazon Simple Notification Service (Amazon SNS) zu benachrichtigen, wenn eine Funktion ausgefallen ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CA-7.A	CA-7.A Fortlaufende Überwachung	multi-region-cloudtrail-enabled	AWS CloudTrail zeichnet Aktionen und API-Aufrufe der AWS Management Console auf. Sie können feststellen, welche Benutzer und Konten angerufen wurden AWS, von welcher Quell-IP-Adresse aus die Anrufe getätigt wurden und wann die Anrufe erfolgten. CloudTrail übermittelt Protokolldateien aus allen AWS Regionen an Ihren S3-Bucket , wenn MULTI_REGION_CLOUD_TRAIL_ENABLED aktiviert ist. Außerdem wird beim AWS Start einer neuen Region derselbe Trail in der neuen Region erstellt. CloudTrail Dadurch erhalten Sie automatisch Protokolldateien mit API-Aktivitäten für die neue Region.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CA-7.A	CA-7.A Fortlaufende Überwachung	rds-enhanced-monitoring-enabled	Aktivieren Sie Amazon Relational Database Service (Amazon RDS), um die Verfügbarkeit von Amazon RDS zu überwachen. Dies bietet einen detaillierten Einblick in den Zustand Ihrer Amazon-RDS-Datenbank-Instances. Wenn der Amazon-RDS-Speicher mehr als ein zugrunde liegendes physisches Gerät verwendet, erfasst Enhanced Monitoring die Daten für jedes Gerät. Wenn die Datenbank-Instance von Amazon RDS in einer Multi-AZ-Bereitstellung ausgeführt wird, werden außerdem die Daten für jedes Gerät auf dem sekundären Host sowie die Metriken des sekundären Hosts erfasst.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CA-7.A	CA-7.A Fortlaufende Überwachung	rds-logging-enabled	Um die Protokollierung und Überwachung in Ihrer Umgebung zu erleichtern, stellen Sie sicher, dass die Amazon Relational Database Service (Amazon RDS)-Protokollierung aktiviert ist. Mit der Amazon-RDS-Protokollierung können Sie Ereignisse wie Verbindungen, Verbindungsabbrüche, Abfragen oder abgefragte Tabellen erfassen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CA-7.A	CA-7.A Fortlaufende Überwachung	redshift-cluster-configuration-check	Um Daten im Ruhezustand zu schützen, muss die Verschlüsselung für Ihre Amazon-Redshift-Cluster aktiviert sein. Sie müssen auch sicherstellen, dass die erforderlichen Konfigurationen auf Amazon-Redshift-Clustern bereitgestellt werden. Die Prüfungsprotokollierung muss aktiviert sein, um Informationen zu Verbindungen und Benutzeraktivitäten in der Datenbank bereitzustellen. Diese Regel erfordert, dass ein Wert für clusterDbEncrypted (Config Default: TRUE) und LoggingEnabled (Config Default: TRUE) gesetzt ist. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CA-7.A	CA-7.A Fortlaufende Überwachung	s3- bucket-logging-enabled	Die Amazon Simple Storage Service (Amazon S3)-Serverzugriffs protokollierung bietet eine Methode zur Überwachu ng des Netzwerks im Hinblick auf potenzielle Cybersich erheitsereignisse. Die Ereignisse werden überwacht, indem detaillierte Aufzeichn ungen über die Anfragen erfasst werden, die an einen Amazon-S3-Bucket gestellt wurden. Jeder Zugriffsprotokolle intrag enthält Details zu einer einzelnen Zugriffsanfrage. Zu den Details gehören Auftraggeber, Bucket-Name, Anforderu ngszeit, Anforderu ngsaktion, Antwortst atus und Fehlercode, falls relevant.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CA-7.A	CA-7.A Fortlaufende Überwachung	securityhub-enabled	AWS Security Hub hilft bei der Überwachung von unbefugtem Personal, Verbindungen, Geräten und Software. AWS Security Hub aggregiert, organisiert und priorisiert die Sicherheitswarnungen oder Ergebnisse mehrerer Dienste. AWS Einige dieser Dienste sind Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer und AWS Firewall Manager sowie AWS Partnerlösungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CA-7.A	CA-7.A Fortlaufende Überwachung	vpc-flow-logs-enabled	VPC-Flow-Protokolle erfassen detaillierte Informationsdatensätze über den IP-Datenverkehr, der zu und von Netzwerkschnittstellen in Ihrer Amazon Virtual Private Cloud (Amazon VPC) fließt. Standardmäßig enthalten Flow-Protokolldatensätze Werte für die verschiedenen Komponenten des IP-Flows, einschließlich Quelle, Ziel und Protokoll.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CA-7.A	CA-7.A Fortlaufende Überwachung	wafv2-logging-enabled	Um Ihnen bei der Protokollierung und Überwachung in Ihrer Umgebung zu helfen, aktivieren Sie die AWS WAF (V2) -Protokollierung im regionalen und globalen Web. ACLs AWS Die WAF-Protokollierung bietet detaillierte Informationen über den Datenverkehr, der von Ihrer Web-ACL analysiert wird. In den Protokollen werden die Uhrzeit aufgezeichnet, zu der die AWS WAF die Anfrage von Ihrer AWS Ressource erhalten hat, Informationen zu der Anfrage und eine Aktion für die Regel, der jede Anfrage entsprach.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CA-7.B	CA-7.B Fortlaufende Überwachung	api-gw-execution-logging-aktiviert	Die API-Gateway-Protokollierung zeigt detaillierte Ansichten der Benutzer, die auf die API zugegriffen haben, und wie diese Benutzer auf die API zugegriffen haben. Diese Einblicke ermöglichen die Transparenz von Benutzeraktivitäten.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CA-7.B	CA-7.B Fortlaufende Überwachung	api-gw-xray-enabled	AWS X-Ray sammelt Daten über Anfragen, die Ihre Anwendung bedient, und bietet Tools, mit denen Sie diese Daten anzeigen, filtern und Einblicke in sie gewinnen können, um Probleme und Optimierungsmöglichkeiten zu identifizieren. Stellen Sie sicher, dass X-Ray aktiviert ist, damit Sie detaillierte Informationen nicht nur über die Anfrage und Antwort, sondern auch über Aufrufe erhalten, die Ihre Anwendung an nachgelagerte AWS Ressourcen, Microservices, Datenbanken und HTTP-Web APIs tätigt.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CA-7.B	CA-7.B Fortlaufende Überwachung	autoscaling-group-elb-healthcheck-erforderlich	Die Elastic Load Balancer (ELB) - Zustandsprüfungen für Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling Scaling-Gruppen unterstützen die Aufrechterhaltung einer angemessenen Kapazität und Verfügbarkeit. Der Load Balancer sendet regelmäßig Pings, versucht Verbindungen herzustellen oder sendet Anfragen, um den Zustand der EC2 Amazon-Instances in einer Gruppe mit auto-scaling zu testen. Wenn eine Instance nicht zurückmeldet, wird der Traffic an eine neue EC2 Amazon-Instance gesendet.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CA-7.B	CA-7.B Fortlaufende Überwachung	beanstalk-enhanced-health-reporting-aktiviert	AWS Die verbesserte Zustandsberichterstattung von Elastic Beanstalk ermöglicht eine schnellere Reaktion auf Veränderungen im Zustand der zugrunde liegenden Infrastruktur. Diese Änderungen könnten zu einer mangelnden Verfügbarkeit der Anwendung führen. Die erweiterten Zustandsberichte von Elastic Beanstalk bieten eine Statusbeschreibung, um den Schweregrad der identifizierten Probleme einzuschätzen und mögliche Ursachen zu identifizieren, die untersucht werden müssen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CA-7.B	CA-7.B Fortlaufende Überwachung	cloudtrail-s3-data events-enabled	Die Erfassung von Simple Storage Service (Amazon S3)-Datenereignissen unterstützt die Erkennung von ungewöhnlichen Aktivitäten. Zu den Details gehören Informationen zu dem AWS -Konto, das auf einen Amazon-S3-Bucket zugegriffen hat, die IP-Adresse und die Uhrzeit des Ereignisses.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CA-7.B	CA-7.B Fortlaufende Überwachung	cloudwatch-alarm-action-check	Amazon CloudWatch alarmiert, wenn eine Metrik den Schwellenwert für eine bestimmte Anzahl von Bewertungszeiträumen überschreitet. Der Alarm führt eine oder mehrere Aktionen durch, die vom Wert der Metrik oder des Ausdrucks im Vergleich zu einem Schwellenwert in einer Reihe von Zeiträumen abhängt. Diese Regel erfordert einen Wert für alarmActionRequired (Config Default: True), insufficientDataAction Required (Config Default: True), okActionRequired (Config Default: False). Der tatsächliche Wert muss die Alarmaktionen für Ihre Umgebung widerspiegeln.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CA-7.B	CA-7.B Fortlaufende Überwachung	cloud-trail-cloud-watch-logs-aktiviert	Verwenden Sie Amazon CloudWatch , um Protokoll ereignisaktivitäten zentral zu sammeln und zu verwalten. Die Aufnahme von AWS CloudTrail Daten liefert Einzelheiten zu den API-Aufrufaktivitäten in Ihrem AWS-Konto.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CA-7.B	CA-7.B Fortlaufende Überwachung	cloudtrail-enabled	AWS CloudTrail kann bei der Nichtabstreitbarkeit helfen, indem Aktionen und API-Aufrufe der AWS Management Console aufgezeichnet werden. Sie können die Benutzer und die Benutzer AWS-Konten , die einen AWS Dienst aufgerufen haben, die Quell-IP-Adresse, über die die Aufrufe generiert wurden, und den Zeitpunkt der Anrufe identifizieren. Einzelheiten zu den erfassten Daten finden Sie unter Inhalt des AWS CloudTrail Datensatzes.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CA-7.B	CA-7.B Fortlaufende Überwachung	cw-loggroup-retention-period-überprüfen	Stellen Sie sicher, dass die Ereignisprotokolldaten für Ihre Protokollgruppen über eine Mindestdauer aufbewahrt werden, um die Fehlerbehebung und forensische Untersuchungen zu unterstützen. Fehlende frühere Ereignisprotokolldaten erschweren die Rekonstruierung und Identifizierung potenziell schädlicher Ereignisse.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CA-7.B	CA-7.B Fortlaufende Überwachung	dynamodb-throughput-limit-check	Aktivieren Sie diese Regel, um sicherzustellen, dass die bereitgestellte Durchsatzkapazität in Ihren Amazon-DynamoDB-Tabellen überprüft wird. Dies ist der Umfang der Lese- und Schreibaktivitäten, der von den jeweiligen Tabellen unterstützt werden kann. DynamoDB verwendet diese Informationen für das Reservieren ausreichender Systemressourcen, um Ihren Durchsatz anforderungen gerecht zu werden. Diese Regel generiert eine Warnung, wenn sich der Durchsatz dem Höchstlimit für ein Kundenkonto nähert. Mit dieser Regel können Sie optional die Parameter RCUThreshold Kontoprozentsatz

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
			(Konfigurationsstandard: 80) und WCUThreshold Kontoprozentsatz (Konfigurationsstandard: 80) festlegen. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.
CCCS-fPBMM-CA-7.B	CA-7.B Fortlaufende Überwachung	ec2- instance-detailed-monitoring-enabled	Aktivieren Sie diese Regel, um die Amazon Elastic Compute Cloud (Amazon EC2) - Instance-Überwachung auf der EC2 Amazon-Konsole zu verbessern, in der Monitoring-Diagramme mit einem Zeitraum von 1 Minute für die Instance angezeigt werden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CA-7.B	CA-7.B Fortlaufende Überwachung	ec2-manager instance-managed-by-systems	Eine Bestandsaufnahme der Softwareplattformen und Anwendungen innerhalb des Unternehmens ist möglich, indem Amazon Elastic Compute Cloud (Amazon EC2) - Instances mit AWS Systems Manager verwaltet werden. Verwenden Sie AWS Systems Manager, um detaillierte Systemkonfigurationen, Betriebssystem-Patch-Levels, Namen und Typ der Dienste, Softwareinstallationen, Anwendungsname, Herausgeber und Version sowie andere Details zu Ihrer Umgebung bereitzustellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CA-7.B	CA-7.B Fortlaufende Überwachung	ec2-check managedinstance-association-compliance-status	Verwenden Sie AWS Systems Manager Associations, um bei der Inventarisierung von Softwareplattformen und Anwendungen innerhalb eines Unternehmens zu helfen. AWS Systems Manager weist Ihren verwalteten Instances einen Konfigurationsstatus zu und ermöglicht es Ihnen, Basiswerte für Betriebssystem-Patch-Levels, Softwareinstallationen, Anwendungskonfigurationen und andere Details zu Ihrer Umgebung festzulegen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CA-7.B	CA-7.B Fortlaufende Überwachung	ec2-prüfen managedinstance-patch-compliance-status	Aktivieren Sie diese Regel, um bei der Identifizierung und Dokumentation von Sicherheitslücken in Amazon Elastic Compute Cloud (Amazon EC2) zu helfen. Die Regel prüft, ob die EC2 Amazon-Instance die Patch-Konformität im AWS Systems Manager gemäß den Richtlinien und Verfahren Ihrer Organisation einhält.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CA-7.B	CA-7.B Fortlaufende Überwachung	eip-attached	Diese Regel stellt sicher, dass Elastic, die einer Amazon Virtual Private Cloud (Amazon VPC) IPs zugewiesen sind, an Amazon Elastic Compute Cloud (Amazon EC2) - Instances oder verwendete Elastic Network Interface s angehängt sind. Diese Regel hilft bei der Überwachu ng ungenutzter Inhalte EIPs in Ihrer Umgebung.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CA-7.B	CA-7.B Fortlaufende Überwachung	elb-logging-enabled	Die Elastic-Load-Balancing-Aktivität ist ein zentraler Kommunikationspunkt innerhalb einer Umgebung. Stellen Sie sicher, dass die ELB-Protokollierung aktiviert ist. Die gesammelten Daten enthalten detaillierte Informationen zu Anfragen, die an den ELB gesendet wurden. Jedes Protokoll enthält Informationen wie die Zeit, zu der die Anforderung einging, die Client-IP-Adresse, Latenzen, Anforderungspfade und Serverantworten.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CA-7.B	CA-7.B Fortlaufende Überwachung	guardduty-enabled-centralized	Amazon GuardDuty kann mithilfe von Threat Intellige nce Feeds helfen, potenzielle Cybersich erheitsereignisse zu überwachen und zu erkennen. Dazu gehören Listen mit bösartigen IPs und maschinel len Lernmethoden zur Identifizierung unerwarteter, nicht autorisierter und bösartiger Aktivitäten in Ihrer AWS Cloud-Umgebung.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CA-7.B	CA-7.B Fortlaufende Überwachung	guardduty-non-archived-findings	Amazon GuardDuty hilft Ihnen dabei, die Auswirkungen eines Vorfalls zu verstehen, indem es die Ergebnisse nach Schweregrad klassifiziert: niedrig, mittel und hoch. Diese Klassifizierungen können Sie zur Festlegung von entsprechenden Strategien und Prioritäten zur Behebung solcher Vorfälle verwenden. Mit dieser Regel können Sie optional daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7) und daysHighSev (Config Default: 1) für nicht archivierte Ergebnisse festlegen, wie es die Richtlinien Ihrer Organisation erfordern.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CA-7.B	CA-7.B Fortlaufende Überwachung	lambda-dlq-check	Aktivieren Sie diese Regel, um das entsprechende Personal über Amazon Simple Queue Service (Amazon SQS) oder Amazon Simple Notification Service (Amazon SNS) zu benachrichtigen, wenn eine Funktion ausgefallen ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CA-7.B	CA-7.B Fortlaufende Überwachung	multi-region-cloudtrail-enabled	AWS CloudTrail zeichnet Aktionen und API-Aufrufe der AWS Management Console auf. Sie können feststellen, welche Benutzer und Konten angerufen wurden AWS, von welcher Quell-IP-Adresse aus die Anrufe getätigt wurden und wann die Anrufe erfolgten. CloudTrail übermittelt Protokolldateien aus allen AWS Regionen an Ihren S3-Bucket , wenn MULTI_REGION_CLOUD_TRAIL_ENABLED aktiviert ist. Außerdem wird beim AWS Start einer neuen Region derselbe Trail in der neuen Region erstellt. CloudTrail Dadurch erhalten Sie automatisch Protokolldateien mit API-Aktivitäten für die neue Region.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CA-7.B	CA-7.B Fortlaufende Überwachung	rds-enhanced-monitoring-enabled	Aktivieren Sie Amazon Relational Database Service (Amazon RDS), um die Verfügbarkeit von Amazon RDS zu überwachen. Dies bietet einen detaillierten Einblick in den Zustand Ihrer Amazon-RDS-Datenbank-Instances. Wenn der Amazon-RDS-Speicher mehr als ein zugrunde liegendes physisches Gerät verwendet, erfasst Enhanced Monitoring die Daten für jedes Gerät. Wenn die Datenbank-Instance von Amazon RDS in einer Multi-AZ-Bereitstellung ausgeführt wird, werden außerdem die Daten für jedes Gerät auf dem sekundären Host sowie die Metriken des sekundären Hosts erfasst.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CA-7.B	CA-7.B Fortlaufende Überwachung	rds-logging-enabled	Um die Protokollierung und Überwachung in Ihrer Umgebung zu erleichtern, stellen Sie sicher, dass die Amazon Relational Database Service (Amazon RDS)-Protokollierung aktiviert ist. Mit der Amazon-RDS-Protokollierung können Sie Ereignisse wie Verbindungen, Verbindungsabbrüche, Abfragen oder abgefragte Tabellen erfassen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CA-7.B	CA-7.B Fortlaufende Überwachung	redshift-cluster-configuration-check	Um Daten im Ruhezustand zu schützen, muss die Verschlüsselung für Ihre Amazon-Redshift-Cluster aktiviert sein. Sie müssen auch sicherstellen, dass die erforderlichen Konfigurationen auf Amazon-Redshift-Clustern bereitgestellt werden. Die Prüfungsprotokollierung muss aktiviert sein, um Informationen zu Verbindungen und Benutzeraktivitäten in der Datenbank bereitzustellen. Diese Regel erfordert, dass ein Wert für clusterDbEncrypted (Config Default: TRUE) und LoggingEnabled (Config Default: TRUE) gesetzt ist. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CA-7.B	CA-7.B Fortlaufende Überwachung	s3- bucket-logging-enabled	Die Amazon Simple Storage Service (Amazon S3)-Serverzugriffs protokollierung bietet eine Methode zur Überwachu ng des Netzwerks im Hinblick auf potenzielle Cybersich erheitsereignisse. Die Ereignisse werden überwacht, indem detaillierte Aufzeichn ungen über die Anfragen erfasst werden, die an einen Amazon-S3-Bucket gestellt wurden. Jeder Zugriffsprotokolle intrag enthält Details zu einer einzelnen Zugriffsanfrage. Zu den Details gehören Auftraggeber, Bucket-Name, Anforderu ngszeit, Anforderu ngsaktion, Antwortst atus und Fehlercode, falls relevant.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CA-7.B	CA-7.B Fortlaufende Überwachung	securityhub-enabled	AWS Security Hub hilft bei der Überwachung von unbefugtem Personal, Verbindungen, Geräten und Software. AWS Security Hub aggregiert, organisiert und priorisiert die Sicherheitswarnungen oder Ergebnisse mehrerer Dienste. AWS Einige dieser Dienste sind Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer und AWS Firewall Manager sowie AWS Partnerlösungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CA-7.B	CA-7.B Fortlaufende Überwachung	vpc-flow-logs-enabled	VPC-Flow-Protokolle erfassen detaillierte Informationsdatensätze über den IP-Datenverkehr, der zu und von Netzwerkschnittstellen in Ihrer Amazon Virtual Private Cloud (Amazon VPC) fließt. Standardmäßig enthalten Flow-Protokolldatensätze Werte für die verschiedenen Komponenten des IP-Flows, einschließlich Quelle, Ziel und Protokoll.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CA-7.B	CA-7.B Fortlaufende Überwachung	wafv2-logging-enabled	Um Ihnen bei der Protokollierung und Überwachung in Ihrer Umgebung zu helfen, aktivieren Sie die AWS WAF (V2) -Protokollierung im regionalen und globalen Web. ACLs AWS Die WAF-Protokollierung bietet detaillierte Informationen über den Datenverkehr, der von Ihrer Web-ACL analysiert wird. In den Protokollen werden die Uhrzeit aufgezeichnet, zu der die AWS WAF die Anfrage von Ihrer AWS Ressource erhalten hat, Informationen zu der Anfrage und eine Aktion für die Regel, der jede Anfrage entsprach.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CA-7.C	CA-7.C Fortlaufende Überwachung	api-gw-execution-logging-aktiviert	Die API-Gateway-Protokollierung zeigt detaillierte Ansichten der Benutzer, die auf die API zugegriffen haben, und wie diese Benutzer auf die API zugegriffen haben. Diese Einblicke ermöglichen die Transparenz von Benutzeraktivitäten.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CA-7.C	CA-7.C Fortlaufende Überwachung	api-gw-xray-enabled	AWS X-Ray sammelt Daten über Anfragen, die Ihre Anwendung bedient, und bietet Tools, mit denen Sie diese Daten anzeigen, filtern und Einblicke in sie gewinnen können, um Probleme und Optimierungsmöglichkeiten zu identifizieren. Stellen Sie sicher, dass X-Ray aktiviert ist, damit Sie detaillierte Informationen nicht nur über die Anfrage und Antwort, sondern auch über Aufrufe erhalten, die Ihre Anwendung an nachgelagerte AWS Ressourcen, Microservices, Datenbanken und HTTP-Web APIs tätigt.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CA-7.C	CA-7.C Fortlaufende Überwachung	autoscaling-group-elb-healthcheck-erforderlich	Die Elastic Load Balancer (ELB) - Zustandsprüfungen für Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling Scaling-Gruppen unterstützen die Aufrechterhaltung einer angemessenen Kapazität und Verfügbarkeit. Der Load Balancer sendet regelmäßig Pings, versucht Verbindungen herzustellen oder sendet Anfragen, um den Zustand der EC2 Amazon-Instances in einer Gruppe mit auto-scaling zu testen. Wenn eine Instance nicht zurückmeldet, wird der Traffic an eine neue EC2 Amazon-Instance gesendet.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CA-7.C	CA-7.C Fortlaufende Überwachung	beanstalk-enhanced-health-reporting-aktiviert	AWS Die verbesserte Zustandsberichterstattung von Elastic Beanstalk ermöglicht eine schnellere Reaktion auf Veränderungen im Zustand der zugrunde liegenden Infrastruktur. Diese Änderungen könnten zu einer mangelnden Verfügbarkeit der Anwendung führen. Die erweiterten Zustandsberichte von Elastic Beanstalk bieten eine Statusbeschreibung, um den Schweregrad der identifizierten Probleme einzuschätzen und mögliche Ursachen zu identifizieren, die untersucht werden müssen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CA-7.C	CA-7.C Fortlaufende Überwachung	cloudtrail-s3-dataevents-enabled	Die Erfassung von Simple Storage Service (Amazon S3)-Datenereignissen unterstützt die Erkennung von ungewöhnlichen Aktivitäten. Zu den Details gehören Informationen zu dem AWS -Konto, das auf einen Amazon-S3-Bucket zugegriffen hat, die IP-Adresse und die Uhrzeit des Ereignisses.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CA-7.C	CA-7.C Fortlaufende Überwachung	cloudwatch-alarm-action-check	Amazon CloudWatch alarmiert, wenn eine Metrik den Schwellenwert für eine bestimmte Anzahl von Bewertungszeiträumen überschreitet. Der Alarm führt eine oder mehrere Aktionen durch, die vom Wert der Metrik oder des Ausdrucks im Vergleich zu einem Schwellenwert in einer Reihe von Zeiträumen abhängt. Diese Regel erfordert einen Wert für alarmActionRequired (Config Default: True), insufficientDataAction Required (Config Default: True), okActionRequired (Config Default: False). Der tatsächliche Wert muss die Alarmaktionen für Ihre Umgebung widerspiegeln.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CA-7.C	CA-7.C Fortlaufende Überwachung	cloud-trail-cloud-watch-logs-aktiviert	Verwenden Sie Amazon CloudWatch , um Protokoll ereignisaktivitäten zentral zu sammeln und zu verwalten. Die Aufnahme von AWS CloudTrail Daten liefert Einzelheiten zu den API-Aufrufaktivitäten in Ihrem AWS-Konto.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CA-7.C	CA-7.C Fortlaufende Überwachung	cloudtrail-enabled	AWS CloudTrail kann bei der Nichtabstreitbarkeit helfen, indem Aktionen und API-Aufrufe der AWS Management Console aufgezeichnet werden. Sie können die Benutzer und die Benutzer AWS-Konten , die einen AWS Dienst aufgerufen haben, die Quell-IP-Adresse, über die die Aufrufe generiert wurden, und den Zeitpunkt der Anrufe identifizieren. Einzelheiten zu den erfassten Daten finden Sie unter Inhalt des AWS CloudTrail Datensatzes.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CA-7.C	CA-7.C Fortlaufende Überwachung	cw-loggroup-retention-period-überprüfen	Stellen Sie sicher, dass die Ereignisprotokolldaten für Ihre Protokollgruppen über eine Mindestdauer aufbewahrt werden, um die Fehlerbehebung und forensische Untersuchungen zu unterstützen. Fehlende frühere Ereignisprotokolldaten erschweren die Rekonstruierung und Identifizierung potenziell schädlicher Ereignisse.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CA-7.C	CA-7.C Fortlaufende Überwachung	dynamodb-throughput-limit-check	Aktivieren Sie diese Regel, um sicherzustellen, dass die bereitgestellte Durchsatzkapazität in Ihren Amazon-DynamoDB-Tabellen überprüft wird. Dies ist der Umfang der Lese- und Schreibaktivitäten, der von den jeweiligen Tabellen unterstützt werden kann. DynamoDB verwendet diese Informationen für das Reservieren ausreichender Systemressourcen, um Ihren Durchsatz anforderungen gerecht zu werden. Diese Regel generiert eine Warnung, wenn sich der Durchsatz dem Höchstlimit für ein Kundenkonto nähert. Mit dieser Regel können Sie optional die Parameter RCUThreshold Kontoprozentsatz

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
			(Konfigurationsstandard: 80) und WCUThreshold Kontoprozentsatz (Konfigurationsstandard: 80) festlegen. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.
CCCS-fPBMM-CA-7.C	CA-7.C Fortlaufende Überwachung	ec2- instance-detailed-monitoring-enabled	Aktivieren Sie diese Regel, um die Amazon Elastic Compute Cloud (Amazon EC2) - Instance-Überwachung auf der EC2 Amazon-Konsole zu verbessern, in der Monitoring-Diagramme mit einem Zeitraum von 1 Minute für die Instance angezeigt werden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CA-7.C	CA-7.C Fortlaufende Überwachung	ec2-manager instance-managed-by-systems	Eine Bestandsaufnahme der Softwareplattformen und Anwendungen innerhalb des Unternehmens ist möglich, indem Amazon Elastic Compute Cloud (Amazon EC2) - Instances mit AWS Systems Manager verwaltet werden. Verwenden Sie AWS Systems Manager, um detaillierte Systemkonfigurationen, Betriebssystem-Patch-Levels, Namen und Typ der Dienste, Softwareinstallationen, Anwendungsname, Herausgeber und Version sowie andere Details zu Ihrer Umgebung bereitzustellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CA-7.C	CA-7.C Fortlaufende Überwachung	ec2-check managedinstance-association-compliance-status	Verwenden Sie AWS Systems Manager Associations, um bei der Inventarisierung von Softwareplattformen und Anwendungen innerhalb eines Unternehmens zu helfen. AWS Systems Manager weist Ihren verwalteten Instances einen Konfigurationsstatus zu und ermöglicht es Ihnen, Basiswerte für Betriebssystem-Patch-Levels, Softwareinstallationen, Anwendungskonfigurationen und andere Details zu Ihrer Umgebung festzulegen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CA-7.C	CA-7.C Fortlaufende Überwachung	ec2-prüfen managedinstance-patch-compliance-status	Aktivieren Sie diese Regel, um bei der Identifizierung und Dokumentation von Sicherheitslücken in Amazon Elastic Compute Cloud (Amazon EC2) zu helfen. Die Regel prüft, ob die EC2 Amazon-Instance die Patch-Konformität im AWS Systems Manager gemäß den Richtlinien und Verfahren Ihrer Organisation einhält.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CA-7.C	CA-7.C Fortlaufende Überwachung	eip-attached	Diese Regel stellt sicher, dass Elastic, die einer Amazon Virtual Private Cloud (Amazon VPC) IPs zugewiesen sind, an Amazon Elastic Compute Cloud (Amazon EC2) - Instances oder verwendete Elastic Network Interface s angehängt sind. Diese Regel hilft bei der Überwachu ng ungenutzter Inhalte EIPs in Ihrer Umgebung.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CA-7.C	CA-7.C Fortlaufende Überwachung	elb-logging-enabled	Die Elastic-Load-Balancing-Aktivität ist ein zentraler Kommunikationspunkt innerhalb einer Umgebung. Stellen Sie sicher, dass die ELB-Protokollierung aktiviert ist. Die gesammelten Daten enthalten detaillierte Informationen zu Anfragen, die an den ELB gesendet wurden. Jedes Protokoll enthält Informationen wie die Zeit, zu der die Anforderung einging, die Client-IP-Adresse, Latenzen, Anforderungspfade und Serverantworten.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CA-7.C	CA-7.C Fortlaufende Überwachung	guardduty-enabled-centralized	Amazon GuardDuty kann mithilfe von Threat Intellige nce Feeds helfen, potenzielle Cybersich erheitsereignisse zu überwachen und zu erkennen. Dazu gehören Listen mit bösartigen IPs und maschinel len Lernmethoden zur Identifizierung unerwarteter, nicht autorisierter und bösartiger Aktivitäten in Ihrer AWS Cloud-Umgebung.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CA-7.C	CA-7.C Fortlaufende Überwachung	guardduty-non-archived-findings	Amazon GuardDuty hilft Ihnen dabei, die Auswirkungen eines Vorfalls zu verstehen, indem es die Ergebnisse nach Schweregrad klassifiziert: niedrig, mittel und hoch. Diese Klassifizierungen können Sie zur Festlegung von entsprechenden Strategien und Prioritäten zur Behebung solcher Vorfälle verwenden. Mit dieser Regel können Sie optional daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7) und daysHighSev (Config Default: 1) für nicht archivierte Ergebnisse festlegen, wie es die Richtlinien Ihrer Organisation erfordern.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CA-7.C	CA-7.C Fortlaufende Überwachung	lambda-dlq-check	Aktivieren Sie diese Regel, um das entsprechende Personal über Amazon Simple Queue Service (Amazon SQS) oder Amazon Simple Notification Service (Amazon SNS) zu benachrichtigen, wenn eine Funktion ausgefallen ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CA-7.C	CA-7.C Fortlaufende Überwachung	multi-region-cloudtrail-enabled	AWS CloudTrail zeichnet Aktionen und API-Aufrufe der AWS Management Console auf. Sie können feststellen, welche Benutzer und Konten angerufen wurden AWS, von welcher Quell-IP-Adresse aus die Anrufe getätigt wurden und wann die Anrufe erfolgten. CloudTrail übermittelt Protokolldateien aus allen AWS Regionen an Ihren S3-Bucket , wenn MULTI_REGION_CLOUD_TRAIL_ENABLED aktiviert ist. Außerdem wird beim AWS Start einer neuen Region derselbe Trail in der neuen Region erstellt. CloudTrail Dadurch erhalten Sie automatisch Protokolldateien mit API-Aktivitäten für die neue Region.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CA-7.C	CA-7.C Fortlaufende Überwachung	rds-enhanced-monitoring-enabled	Aktivieren Sie Amazon Relational Database Service (Amazon RDS), um die Verfügbarkeit von Amazon RDS zu überwachen. Dies bietet einen detaillierten Einblick in den Zustand Ihrer Amazon-RDS-Datenbank-Instances. Wenn der Amazon-RDS-Speicher mehr als ein zugrunde liegendes physisches Gerät verwendet, erfasst Enhanced Monitoring die Daten für jedes Gerät. Wenn die Datenbank-Instance von Amazon RDS in einer Multi-AZ-Bereitstellung ausgeführt wird, werden außerdem die Daten für jedes Gerät auf dem sekundären Host sowie die Metriken des sekundären Hosts erfasst.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CA-7.C	CA-7.C Fortlaufende Überwachung	rds-logging-enabled	Um die Protokollierung und Überwachung in Ihrer Umgebung zu erleichtern, stellen Sie sicher, dass die Amazon Relational Database Service (Amazon RDS)-Protokollierung aktiviert ist. Mit der Amazon-RDS-Protokollierung können Sie Ereignisse wie Verbindungen, Verbindungsabbrüche, Abfragen oder abgefragte Tabellen erfassen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CA-7.C	CA-7.C Fortlaufende Überwachung	redshift-cluster-configuration-check	Um Daten im Ruhezustand zu schützen, muss die Verschlüsselung für Ihre Amazon-Redshift-Cluster aktiviert sein. Sie müssen auch sicherstellen, dass die erforderlichen Konfigurationen auf Amazon-Redshift-Clustern bereitgestellt werden. Die Prüfungsprotokollierung muss aktiviert sein, um Informationen zu Verbindungen und Benutzeraktivitäten in der Datenbank bereitzustellen. Diese Regel erfordert, dass ein Wert für clusterDbEncrypted (Config Default: TRUE) und LoggingEnabled (Config Default: TRUE) gesetzt ist. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CA-7.C	CA-7.C Fortlaufende Überwachung	s3- bucket-logging-enabled	Die Amazon Simple Storage Service (Amazon S3)-Serverzugriffs protokollierung bietet eine Methode zur Überwachu ng des Netzwerks im Hinblick auf potenzielle Cybersich erheitsereignisse. Die Ereignisse werden überwacht, indem detaillierte Aufzeichn ungen über die Anfragen erfasst werden, die an einen Amazon-S3-Bucket gestellt wurden. Jeder Zugriffsprotokolle intrag enthält Details zu einer einzelnen Zugriffsanfrage. Zu den Details gehören Auftraggeber, Bucket-Name, Anforderu ngszeit, Anforderu ngsaktion, Antwortst atus und Fehlercode, falls relevant.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CA-7.C	CA-7.C Fortlaufende Überwachung	securityhub-enabled	AWS Security Hub hilft bei der Überwachung von unbefugtem Personal, Verbindungen, Geräten und Software. AWS Security Hub aggregiert, organisiert und priorisiert die Sicherheitswarnungen oder Ergebnisse mehrerer Dienste. AWS Einige dieser Dienste sind Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer und AWS Firewall Manager sowie AWS Partnerlösungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CA-7.C	CA-7.C Fortlaufende Überwachung	vpc-flow-logs-enabled	VPC-Flow-Protokolle erfassen detaillierte Informationsdatensätze über den IP-Datenverkehr, der zu und von Netzwerkschnittstellen in Ihrer Amazon Virtual Private Cloud (Amazon VPC) fließt. Standardmäßig enthalten Flow-Protokolldatensätze Werte für die verschiedenen Komponenten des IP-Flows, einschließlich Quelle, Ziel und Protokoll.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CA-7.C	CA-7.C Fortlaufende Überwachung	wafv2-logging-enabled	Um Ihnen bei der Protokollierung und Überwachung in Ihrer Umgebung zu helfen, aktivieren Sie die AWS WAF (V2) -Protokollierung im regionalen und globalen Web. ACLs AWS Die WAF-Protokollierung bietet detaillierte Informationen über den Datenverkehr, der von Ihrer Web-ACL analysiert wird. In den Protokollen werden die Uhrzeit aufgezeichnet, zu der die AWS WAF die Anfrage von Ihrer AWS Ressource erhalten hat, Informationen zu der Anfrage und eine Aktion für die Regel, der jede Anfrage entsprach.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CA-7.D	CA-7.D Fortlaufende Überwachung	api-gw-execution-logging-aktiviert	Die API-Gateway-Protokollierung zeigt detaillierte Ansichten der Benutzer, die auf die API zugegriffen haben, und wie diese Benutzer auf die API zugegriffen haben. Diese Einblicke ermöglichen die Transparenz von Benutzeraktivitäten.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CA-7.D	CA-7.D Fortlaufende Überwachung	api-gw-xray-enabled	AWS X-Ray sammelt Daten über Anfragen, die Ihre Anwendung bedient, und bietet Tools, mit denen Sie diese Daten anzeigen, filtern und Einblicke in sie gewinnen können, um Probleme und Optimierungsmöglichkeiten zu identifizieren. Stellen Sie sicher, dass X-Ray aktiviert ist, damit Sie detaillierte Informationen nicht nur über die Anfrage und Antwort, sondern auch über Aufrufe erhalten, die Ihre Anwendung an nachgelagerte AWS Ressourcen, Microservices, Datenbanken und HTTP-Web APIs tätigt.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CA-7.D	CA-7.D Fortlaufende Überwachung	autoscaling-group-elb-healthcheck-erforderlich	Die Elastic Load Balancer (ELB) - Zustandsprüfungen für Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling Scaling-Gruppen unterstützen die Aufrechterhaltung einer angemessenen Kapazität und Verfügbarkeit. Der Load Balancer sendet regelmäßig Pings, versucht Verbindungen herzustellen oder sendet Anfragen, um den Zustand der EC2 Amazon-Instances in einer Gruppe mit auto-scaling zu testen. Wenn eine Instance nicht zurückmeldet, wird der Traffic an eine neue EC2 Amazon-Instance gesendet.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CA-7.D	CA-7.D Fortlaufende Überwachung	beanstalk-enhanced-health-reporting-aktiviert	AWS Die verbesserte Zustandsberichterstattung von Elastic Beanstalk ermöglicht eine schnellere Reaktion auf Veränderungen im Zustand der zugrunde liegenden Infrastruktur. Diese Änderungen könnten zu einer mangelnden Verfügbarkeit der Anwendung führen. Die erweiterten Zustandsberichte von Elastic Beanstalk bieten eine Statusbeschreibung, um den Schweregrad der identifizierten Probleme einzuschätzen und mögliche Ursachen zu identifizieren, die untersucht werden müssen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CA-7.D	CA-7.D Fortlaufende Überwachung	cloudtrail-s3-data events-enabled	Die Erfassung von Simple Storage Service (Amazon S3)-Datenereignissen unterstützt die Erkennung von ungewöhnlichen Aktivitäten. Zu den Details gehören Informationen zu dem AWS -Konto, das auf einen Amazon-S3-Bucket zugegriffen hat, die IP-Adresse und die Uhrzeit des Ereignisses.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CA-7.D	CA-7.D Fortlaufende Überwachung	cloudwatch-alarm-action-check	Amazon CloudWatch alarmiert, wenn eine Metrik den Schwellenwert für eine bestimmte Anzahl von Bewertungszeiträumen überschreitet. Der Alarm führt eine oder mehrere Aktionen durch, die vom Wert der Metrik oder des Ausdrucks im Vergleich zu einem Schwellenwert in einer Reihe von Zeiträumen abhängt. Diese Regel erfordert einen Wert für alarmActionRequired (Config Default: True), insufficientDataAction Required (Config Default: True), okActionRequired (Config Default: False). Der tatsächliche Wert muss die Alarmaktionen für Ihre Umgebung widerspiegeln.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CA-7.D	CA-7.D Fortlaufende Überwachung	cloud-trail-cloud-watch-logs-aktiviert	Verwenden Sie Amazon CloudWatch , um Protokoll ereignisaktivitäten zentral zu sammeln und zu verwalten. Die Aufnahme von AWS CloudTrail Daten liefert Einzelheiten zu den API-Aufrufaktivitäten in Ihrem AWS-Konto.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CA-7.D	CA-7.D Fortlaufende Überwachung	cloudtrail-enabled	AWS CloudTrail kann bei der Nichtabstreitbarkeit helfen, indem Aktionen und API-Aufrufe der AWS Management Console aufgezeichnet werden. Sie können die Benutzer und die Benutzer AWS-Konten , die einen AWS Dienst aufgerufen haben, die Quell-IP-Adresse, über die die Aufrufe generiert wurden, und den Zeitpunkt der Anrufe identifizieren. Einzelheiten zu den erfassten Daten finden Sie unter Inhalt des AWS CloudTrail Datensatzes.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CA-7.D	CA-7.D Fortlaufende Überwachung	cw-loggroup-retention-period-überprüfen	Stellen Sie sicher, dass die Ereignisprotokolldaten für Ihre Protokollgruppen über eine Mindestdauer aufbewahrt werden, um die Fehlerbehebung und forensische Untersuchungen zu unterstützen. Fehlende frühere Ereignisprotokolldaten erschweren die Rekonstruierung und Identifizierung potenziell schädlicher Ereignisse.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CA-7.D	CA-7.D Fortlaufende Überwachung	dynamodb-throughput-limit-check	Aktivieren Sie diese Regel, um sicherzustellen, dass die bereitgestellte Durchsatzkapazität in Ihren Amazon-DynamoDB-Tabellen überprüft wird. Dies ist der Umfang der Lese- und Schreibaktivitäten, der von den jeweiligen Tabellen unterstützt werden kann. DynamoDB verwendet diese Informationen für das Reservieren ausreichender Systemressourcen, um Ihren Durchsatz anforderungen gerecht zu werden. Diese Regel generiert eine Warnung, wenn sich der Durchsatz dem Höchstlimit für ein Kundenkonto nähert. Mit dieser Regel können Sie optional die Parameter RCUThreshold Kontoprozentsatz

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
			(Konfigurationsstandard: 80) und WCUThreshold Kontoprozentsatz (Konfigurationsstandard: 80) festlegen. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.
CCCS-fPBMM-CA-7.D	CA-7.D Fortlaufende Überwachung	ec2- instance-detailed-monitoring-enabled	Aktivieren Sie diese Regel, um die Amazon Elastic Compute Cloud (Amazon EC2) - Instance-Überwachung auf der EC2 Amazon-Konsole zu verbessern, in der Monitoring-Diagramme mit einem Zeitraum von 1 Minute für die Instance angezeigt werden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CA-7.D	CA-7.D Fortlaufende Überwachung	ec2-manager instance-managed-by-systems	Eine Bestandsaufnahme der Softwareplattformen und Anwendungen innerhalb des Unternehmens ist möglich, indem Amazon Elastic Compute Cloud (Amazon EC2) - Instances mit AWS Systems Manager verwaltet werden. Verwenden Sie AWS Systems Manager, um detaillierte Systemkonfigurationen, Betriebssystem-Patch-Levels, Namen und Typ der Dienste, Softwareinstallationen, Anwendungsname, Herausgeber und Version sowie andere Details zu Ihrer Umgebung bereitzustellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CA-7.D	CA-7.D Fortlaufende Überwachung	ec2-check managedinstance-association-compliance-status	Verwenden Sie AWS Systems Manager Associations, um bei der Inventarisierung von Softwareplattformen und Anwendungen innerhalb eines Unternehmens zu helfen. AWS Systems Manager weist Ihren verwalteten Instances einen Konfigurationsstatus zu und ermöglicht es Ihnen, Basiswerte für Betriebssystem-Patch-Levels, Softwareinstallationen, Anwendungskonfigurationen und andere Details zu Ihrer Umgebung festzulegen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CA-7.D	CA-7.D Fortlaufende Überwachung	ec2-prüfen managedinstance-patch-compliance-status	Aktivieren Sie diese Regel, um bei der Identifizierung und Dokumentation von Sicherheitslücken in Amazon Elastic Compute Cloud (Amazon EC2) zu helfen. Die Regel prüft, ob die EC2 Amazon-Instance die Patch-Konformität im AWS Systems Manager gemäß den Richtlinien und Verfahren Ihrer Organisation einhält.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CA-7.D	CA-7.D Fortlaufende Überwachung	eip-attached	Diese Regel stellt sicher, dass Elastic, die einer Amazon Virtual Private Cloud (Amazon VPC) IPs zugewiesen sind, an Amazon Elastic Compute Cloud (Amazon EC2) - Instances oder verwendete Elastic Network Interface s angehängt sind. Diese Regel hilft bei der Überwachu ng ungenutzter Inhalte EIPs in Ihrer Umgebung.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CA-7.D	CA-7.D Fortlaufende Überwachung	elb-logging-enabled	Die Elastic-Load-Balancing-Aktivität ist ein zentraler Kommunikationspunkt innerhalb einer Umgebung. Stellen Sie sicher, dass die ELB-Protokollierung aktiviert ist. Die gesammelten Daten enthalten detaillierte Informationen zu Anfragen, die an den ELB gesendet wurden. Jedes Protokoll enthält Informationen wie die Zeit, zu der die Anforderung einging, die Client-IP-Adresse, Latenzen, Anforderungspfade und Serverantworten.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CA-7.D	CA-7.D Fortlaufende Überwachung	guardduty-enabled-centralized	Amazon GuardDuty kann mithilfe von Threat Intellige nce Feeds helfen, potenzielle Cybersich erheitsereignisse zu überwachen und zu erkennen. Dazu gehören Listen mit bösartigen IPs und maschinel len Lernmethoden zur Identifizierung unerwarteter, nicht autorisierter und bösartiger Aktivitäten in Ihrer AWS Cloud-Umgebung.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CA-7.D	CA-7.D Fortlaufende Überwachung	guardduty-non-archived-findings	Amazon GuardDuty hilft Ihnen dabei, die Auswirkungen eines Vorfalls zu verstehen, indem es die Ergebnisse nach Schweregrad klassifiziert: niedrig, mittel und hoch. Diese Klassifizierungen können Sie zur Festlegung von entsprechenden Strategien und Prioritäten zur Behebung solcher Vorfälle verwenden. Mit dieser Regel können Sie optional daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7) und daysHighSev (Config Default: 1) für nicht archivierte Ergebnisse festlegen, wie es die Richtlinien Ihrer Organisation erfordern.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CA-7.D	CA-7.D Fortlaufende Überwachung	lambda-dlq-check	Aktivieren Sie diese Regel, um das entsprechende Personal über Amazon Simple Queue Service (Amazon SQS) oder Amazon Simple Notification Service (Amazon SNS) zu benachrichtigen, wenn eine Funktion ausgefallen ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CA-7.D	CA-7.D Fortlaufende Überwachung	multi-region-cloudtrail-enabled	AWS CloudTrail zeichnet Aktionen und API-Aufrufe der AWS Management Console auf. Sie können feststellen, welche Benutzer und Konten angerufen wurden AWS, von welcher Quell-IP-Adresse aus die Anrufe getätigt wurden und wann die Anrufe erfolgten. CloudTrail übermittelt Protokolldateien aus allen AWS Regionen an Ihren S3-Bucket , wenn MULTI_REGION_CLOUD_TRAIL_ENABLED aktiviert ist. Außerdem wird beim AWS Start einer neuen Region derselbe Trail in der neuen Region erstellt. CloudTrail Dadurch erhalten Sie automatisch Protokolldateien mit API-Aktivitäten für die neue Region.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CA-7.D	CA-7.D Fortlaufende Überwachung	rds-enhanced-monitoring-enabled	Aktivieren Sie Amazon Relational Database Service (Amazon RDS), um die Verfügbarkeit von Amazon RDS zu überwachen. Dies bietet einen detaillierten Einblick in den Zustand Ihrer Amazon-RDS-Datenbank-Instances. Wenn der Amazon-RDS-Speicher mehr als ein zugrunde liegendes physisches Gerät verwendet, erfasst Enhanced Monitoring die Daten für jedes Gerät. Wenn die Datenbank-Instance von Amazon RDS in einer Multi-AZ-Bereitstellung ausgeführt wird, werden außerdem die Daten für jedes Gerät auf dem sekundären Host sowie die Metriken des sekundären Hosts erfasst.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CA-7.D	CA-7.D Fortlaufende Überwachung	rds-logging-enabled	Um die Protokollierung und Überwachung in Ihrer Umgebung zu erleichtern, stellen Sie sicher, dass die Amazon Relational Database Service (Amazon RDS)-Protokollierung aktiviert ist. Mit der Amazon-RDS-Protokollierung können Sie Ereignisse wie Verbindungen, Verbindungsabbrüche, Abfragen oder abgefragte Tabellen erfassen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CA-7.D	CA-7.D Fortlaufende Überwachung	redshift-cluster-configuration-check	Um Daten im Ruhezustand zu schützen, muss die Verschlüsselung für Ihre Amazon-Redshift-Cluster aktiviert sein. Sie müssen auch sicherstellen, dass die erforderlichen Konfigurationen auf Amazon-Redshift-Clustern bereitgestellt werden. Die Prüfungsprotokollierung muss aktiviert sein, um Informationen zu Verbindungen und Benutzeraktivitäten in der Datenbank bereitzustellen. Diese Regel erfordert, dass ein Wert für clusterDbEncrypted (Config Default: TRUE) und LoggingEnabled (Config Default: TRUE) gesetzt ist. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CA-7.D	CA-7.D Fortlaufende Überwachung	s3- bucket-logging-enabled	Die Amazon Simple Storage Service (Amazon S3)-Serverzugriffs protokollierung bietet eine Methode zur Überwachu ng des Netzwerks im Hinblick auf potenzielle Cybersich erheitsereignisse. Die Ereignisse werden überwacht, indem detaillierte Aufzeichn ungen über die Anfragen erfasst werden, die an einen Amazon-S3-Bucket gestellt wurden. Jeder Zugriffsprotokolle intrag enthält Details zu einer einzelnen Zugriffsanfrage. Zu den Details gehören Auftraggeber, Bucket-Name, Anforderu ngszeit, Anforderu ngsaktion, Antwortst atus und Fehlercode, falls relevant.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CA-7.D	CA-7.D Fortlaufende Überwachung	securityhub-enabled	AWS Security Hub hilft bei der Überwachung von unbefugtem Personal, Verbindungen, Geräten und Software. AWS Security Hub aggregiert, organisiert und priorisiert die Sicherheitswarnungen oder Ergebnisse mehrerer Dienste. AWS Einige dieser Dienste sind Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer und AWS Firewall Manager sowie AWS Partnerlösungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CA-7.D	CA-7.D Fortlaufende Überwachung	vpc-flow-logs-enabled	VPC-Flow-Protokolle erfassen detaillierte Informationsdatensätze über den IP-Datenverkehr, der zu und von Netzwerkschnittstellen in Ihrer Amazon Virtual Private Cloud (Amazon VPC) fließt. Standardmäßig enthalten Flow-Protokolldatensätze Werte für die verschiedenen Komponenten des IP-Flows, einschließlich Quelle, Ziel und Protokoll.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CA-7.D	CA-7.D Fortlaufende Überwachung	wafv2-logging-enabled	Um Ihnen bei der Protokollierung und Überwachung in Ihrer Umgebung zu helfen, aktivieren Sie die AWS WAF (V2) -Protokollierung im regionalen und globalen Web. ACLs AWS Die WAF-Protokollierung bietet detaillierte Informationen über den Datenverkehr, der von Ihrer Web-ACL analysiert wird. In den Protokollen werden die Uhrzeit aufgezeichnet, zu der die AWS WAF die Anfrage von Ihrer AWS Ressource erhalten hat, Informationen zu der Anfrage und eine Aktion für die Regel, der jede Anfrage entsprach.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CA-7.E	CA-7.E Fortlaufende Überwachung	api-gw-execution-logging-aktiviert	Die API-Gateway-Protokollierung zeigt detaillierte Ansichten der Benutzer, die auf die API zugegriffen haben, und wie diese Benutzer auf die API zugegriffen haben. Diese Einblicke ermöglichen die Transparenz von Benutzeraktivitäten.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CA-7.E	CA-7.E Fortlaufende Überwachung	api-gw-xray-enabled	AWS X-Ray sammelt Daten über Anfragen, die Ihre Anwendung bedient, und bietet Tools, mit denen Sie diese Daten anzeigen, filtern und Einblicke in sie gewinnen können, um Probleme und Optimierungsmöglichkeiten zu identifizieren. Stellen Sie sicher, dass X-Ray aktiviert ist, damit Sie detaillierte Informationen nicht nur über die Anfrage und Antwort, sondern auch über Aufrufe erhalten, die Ihre Anwendung an nachgelagerte AWS Ressourcen, Microservices, Datenbanken und HTTP-Web APIs tätigt.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CA-7.E	CA-7.E Fortlaufende Überwachung	autoscaling-group-elb-healthcheck-erforderlich	Die Elastic Load Balancer (ELB) - Zustandsprüfungen für Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling Scaling-Gruppen unterstützen die Aufrechterhaltung einer angemessenen Kapazität und Verfügbarkeit. Der Load Balancer sendet regelmäßig Pings, versucht Verbindungen herzustellen oder sendet Anfragen, um den Zustand der EC2 Amazon-Instances in einer Gruppe mit auto-scaling zu testen. Wenn eine Instance nicht zurückmeldet, wird der Traffic an eine neue EC2 Amazon-Instance gesendet.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CA-7.E	CA-7.E Fortlaufende Überwachung	beanstalk-enhanced-health-reporting-aktiviert	AWS Die verbesserte Zustandsberichterstattung von Elastic Beanstalk ermöglicht eine schnellere Reaktion auf Veränderungen im Zustand der zugrunde liegenden Infrastruktur. Diese Änderungen könnten zu einer mangelnden Verfügbarkeit der Anwendung führen. Die erweiterten Zustandsberichte von Elastic Beanstalk bieten eine Statusbeschreibung, um den Schweregrad der identifizierten Probleme einzuschätzen und mögliche Ursachen zu identifizieren, die untersucht werden müssen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CA-7.E	CA-7.E Fortlaufende Überwachung	cloudtrail-s3-dataevents-enabled	Die Erfassung von Simple Storage Service (Amazon S3)-Datenereignissen unterstützt die Erkennung von ungewöhnlichen Aktivitäten. Zu den Details gehören Informationen zu dem AWS -Konto, das auf einen Amazon-S3-Bucket zugegriffen hat, die IP-Adresse und die Uhrzeit des Ereignisses.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CA-7.E	CA-7.E Fortlaufende Überwachung	cloudwatch-alarm-action-check	Amazon CloudWatch alarmiert, wenn eine Metrik den Schwellenwert für eine bestimmte Anzahl von Bewertungszeiträumen überschreitet. Der Alarm führt eine oder mehrere Aktionen durch, die vom Wert der Metrik oder des Ausdrucks im Vergleich zu einem Schwellenwert in einer Reihe von Zeiträumen abhängt. Diese Regel erfordert einen Wert für alarmActionRequired (Config Default: True), insufficientDataAction Required (Config Default: True), okActionRequired (Config Default: False). Der tatsächliche Wert muss die Alarmaktionen für Ihre Umgebung widerspiegeln.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CA-7.E	CA-7.E Fortlaufende Überwachung	cloud-trail-cloud-watch-logs-aktiviert	Verwenden Sie Amazon CloudWatch , um Protokoll ereignisaktivitäten zentral zu sammeln und zu verwalten. Die Aufnahme von AWS CloudTrail Daten liefert Einzelheiten zu den API-Aufrufaktivitäten in Ihrem AWS-Konto.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CA-7.E	CA-7.E Fortlaufende Überwachung	cloudtrail-enabled	AWS CloudTrail kann bei der Nichtabstreitbarkeit helfen, indem Aktionen und API-Aufrufe der AWS Management Console aufgezeichnet werden. Sie können die Benutzer und die Benutzer AWS-Konten , die einen AWS Dienst aufgerufen haben, die Quell-IP-Adresse, über die die Aufrufe generiert wurden, und den Zeitpunkt der Anrufe identifizieren. Einzelheiten zu den erfassten Daten finden Sie unter Inhalt des AWS CloudTrail Datensatzes.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CA-7.E	CA-7.E Fortlaufende Überwachung	cw-loggroup-retention-period-überprüfen	Stellen Sie sicher, dass die Ereignisprotokolldaten für Ihre Protokollgruppen über eine Mindestdauer aufbewahrt werden, um die Fehlerbehebung und forensische Untersuchungen zu unterstützen. Fehlende frühere Ereignisprotokolldaten erschweren die Rekonstruierung und Identifizierung potenziell schädlicher Ereignisse.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CA-7.E	CA-7.E Fortlaufende Überwachung	dynamodb-throughput-limit-check	Aktivieren Sie diese Regel, um sicherzustellen, dass die bereitgestellte Durchsatzkapazität in Ihren Amazon-DynamoDB-Tabellen überprüft wird. Dies ist der Umfang der Lese- und Schreibaktivitäten, der von den jeweiligen Tabellen unterstützt werden kann. DynamoDB verwendet diese Informationen für das Reservieren ausreichender Systemressourcen, um Ihren Durchsatz anforderungen gerecht zu werden. Diese Regel generiert eine Warnung, wenn sich der Durchsatz dem Höchstlimit für ein Kundenkonto nähert. Mit dieser Regel können Sie optional die Parameter RCUThreshold Kontoprozentsatz

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
			(Konfigurationsstandard: 80) und WCUThreshold Kontoprozentsatz (Konfigurationsstandard: 80) festlegen. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.
CCCS-fPBMM-CA-7.E	CA-7.E Fortlaufende Überwachung	ec2- instance-detailed-monitoring-enabled	Aktivieren Sie diese Regel, um die Amazon Elastic Compute Cloud (Amazon EC2) - Instance-Überwachung auf der EC2 Amazon-Konsole zu verbessern, in der Monitoring-Diagramme mit einem Zeitraum von 1 Minute für die Instance angezeigt werden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CA-7.E	CA-7.E Fortlaufende Überwachung	ec2-manager instance-managed-by-systems	Eine Bestandsaufnahme der Softwareplattformen und Anwendungen innerhalb des Unternehmens ist möglich, indem Amazon Elastic Compute Cloud (Amazon EC2) - Instances mit AWS Systems Manager verwaltet werden. Verwenden Sie AWS Systems Manager, um detaillierte Systemkonfigurationen, Betriebssystem-Patch-Levels, Namen und Typ der Dienste, Softwareinstallationen, Anwendungsname, Herausgeber und Version sowie andere Details zu Ihrer Umgebung bereitzustellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CA-7.E	CA-7.E Fortlaufende Überwachung	ec2-check managedinstance-association-compliance-status	Verwenden Sie AWS Systems Manager Associations, um bei der Inventarisierung von Softwareplattformen und Anwendungen innerhalb eines Unternehmens zu helfen. AWS Systems Manager weist Ihren verwalteten Instances einen Konfigurationsstatus zu und ermöglicht es Ihnen, Basiswerte für Betriebssystem-Patch-Levels, Softwareinstallationen, Anwendungskonfigurationen und andere Details zu Ihrer Umgebung festzulegen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CA-7.E	CA-7.E Fortlaufende Überwachung	ec2-prüfen managedinstance-patch-compliance-status	Aktivieren Sie diese Regel, um bei der Identifizierung und Dokumentation von Sicherheitslücken in Amazon Elastic Compute Cloud (Amazon EC2) zu helfen. Die Regel prüft, ob die EC2 Amazon-Instance die Patch-Konformität im AWS Systems Manager gemäß den Richtlinien und Verfahren Ihrer Organisation einhält.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CA-7.E	CA-7.E Fortlaufende Überwachung	eip-attached	Diese Regel stellt sicher, dass Elastic, die einer Amazon Virtual Private Cloud (Amazon VPC) IPs zugewiesen sind, an Amazon Elastic Compute Cloud (Amazon EC2) - Instances oder verwendete Elastic Network Interface s angehängt sind. Diese Regel hilft bei der Überwachu ng ungenutzter Inhalte EIPs in Ihrer Umgebung.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CA-7.E	CA-7.E Fortlaufende Überwachung	elb-logging-enabled	Die Elastic-Load-Balancing-Aktivität ist ein zentraler Kommunikationspunkt innerhalb einer Umgebung. Stellen Sie sicher, dass die ELB-Protokollierung aktiviert ist. Die gesammelten Daten enthalten detaillierte Informationen zu Anfragen, die an den ELB gesendet wurden. Jedes Protokoll enthält Informationen wie die Zeit, zu der die Anforderung einging, die Client-IP-Adresse, Latenzen, Anforderungspfade und Serverantworten.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CA-7.E	CA-7.E Fortlaufende Überwachung	guardduty-enabled-centralized	Amazon GuardDuty kann mithilfe von Threat Intellige nce Feeds helfen, potenzielle Cybersich erheitsereignisse zu überwachen und zu erkennen. Dazu gehören Listen mit bösartigen IPs und maschinel len Lernmethoden zur Identifizierung unerwarteter, nicht autorisierter und bösartiger Aktivitäten in Ihrer AWS Cloud-Umgebung.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CA-7.E	CA-7.E Fortlaufende Überwachung	guardduty-non-archived-findings	Amazon GuardDuty hilft Ihnen dabei, die Auswirkungen eines Vorfalls zu verstehen, indem es die Ergebnisse nach Schweregrad klassifiziert: niedrig, mittel und hoch. Diese Klassifizierungen können Sie zur Festlegung von entsprechenden Strategien und Prioritäten zur Behebung solcher Vorfälle verwenden. Mit dieser Regel können Sie optional daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7) und daysHighSev (Config Default: 1) für nicht archivierte Ergebnisse festlegen, wie es die Richtlinien Ihrer Organisation erfordern.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CA-7.E	CA-7.E Fortlaufende Überwachung	lambda-dlq-check	Aktivieren Sie diese Regel, um das entsprechende Personal über Amazon Simple Queue Service (Amazon SQS) oder Amazon Simple Notification Service (Amazon SNS) zu benachrichtigen, wenn eine Funktion ausgefallen ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CA-7.E	CA-7.E Fortlaufende Überwachung	multi-region-cloudtrail-enabled	AWS CloudTrail zeichnet Aktionen und API-Aufrufe der AWS Management Console auf. Sie können feststellen, welche Benutzer und Konten angerufen wurden AWS, von welcher Quell-IP-Adresse aus die Anrufe getätigt wurden und wann die Anrufe erfolgten. CloudTrail übermittelt Protokolldateien aus allen AWS Regionen an Ihren S3-Bucket , wenn MULTI_REGION_CLOUD_TRAIL_ENABLED aktiviert ist. Außerdem wird beim AWS Start einer neuen Region derselbe Trail in der neuen Region erstellt. CloudTrail Dadurch erhalten Sie automatisch Protokolldateien mit API-Aktivitäten für die neue Region.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CA-7.E	CA-7.E Fortlaufende Überwachung	rds-enhanced-monitoring-enabled	Aktivieren Sie Amazon Relational Database Service (Amazon RDS), um die Verfügbarkeit von Amazon RDS zu überwachen. Dies bietet einen detaillierten Einblick in den Zustand Ihrer Amazon-RDS-Datenbank-Instances. Wenn der Amazon-RDS-Speicher mehr als ein zugrunde liegendes physisches Gerät verwendet, erfasst Enhanced Monitoring die Daten für jedes Gerät. Wenn die Datenbank-Instance von Amazon RDS in einer Multi-AZ-Bereitstellung ausgeführt wird, werden außerdem die Daten für jedes Gerät auf dem sekundären Host sowie die Metriken des sekundären Hosts erfasst.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CA-7.E	CA-7.E Fortlaufende Überwachung	rds-logging-enabled	Um die Protokollierung und Überwachung in Ihrer Umgebung zu erleichtern, stellen Sie sicher, dass die Amazon Relational Database Service (Amazon RDS)-Protokollierung aktiviert ist. Mit der Amazon-RDS-Protokollierung können Sie Ereignisse wie Verbindungen, Verbindungsabbrüche, Abfragen oder abgefragte Tabellen erfassen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CA-7.E	CA-7.E Fortlaufende Überwachung	redshift-cluster-configuration-check	Um Daten im Ruhezustand zu schützen, muss die Verschlüsselung für Ihre Amazon-Redshift-Cluster aktiviert sein. Sie müssen auch sicherstellen, dass die erforderlichen Konfigurationen auf Amazon-Redshift-Clustern bereitgestellt werden. Die Prüfungsprotokollierung muss aktiviert sein, um Informationen zu Verbindungen und Benutzeraktivitäten in der Datenbank bereitzustellen. Diese Regel erfordert, dass ein Wert für clusterDbEncrypted (Config Default: TRUE) und LoggingEnabled (Config Default: TRUE) gesetzt ist. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CA-7.E	CA-7.E Fortlaufende Überwachung	s3- bucket-logging-enabled	Die Amazon Simple Storage Service (Amazon S3)-Serverzugriffs protokollierung bietet eine Methode zur Überwachu ng des Netzwerks im Hinblick auf potenzielle Cybersich erheitsereignisse. Die Ereignisse werden überwacht, indem detaillierte Aufzeichn ungen über die Anfragen erfasst werden, die an einen Amazon-S3-Bucket gestellt wurden. Jeder Zugriffsprotokolle intrag enthält Details zu einer einzelnen Zugriffsanfrage. Zu den Details gehören Auftraggeber, Bucket-Name, Anforderu ngszeit, Anforderu ngsaktion, Antwortst atus und Fehlercode, falls relevant.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CA-7.E	CA-7.E Fortlaufende Überwachung	securityhub-enabled	AWS Security Hub hilft bei der Überwachung von unbefugtem Personal, Verbindungen, Geräten und Software. AWS Security Hub aggregiert, organisiert und priorisiert die Sicherheitswarnungen oder Ergebnisse mehrerer Dienste. AWS Einige dieser Dienste sind Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer und AWS Firewall Manager sowie AWS Partnerlösungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CA-7.E	CA-7.E Fortlaufende Überwachung	vpc-flow-logs-enabled	VPC-Flow-Protokolle erfassen detaillierte Informationsdatensätze über den IP-Datenverkehr, der zu und von Netzwerkschnittstellen in Ihrer Amazon Virtual Private Cloud (Amazon VPC) fließt. Standardmäßig enthalten Flow-Protokolldatensätze Werte für die verschiedenen Komponenten des IP-Flows, einschließlich Quelle, Ziel und Protokoll.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CA-7.E	CA-7.E Fortlaufende Überwachung	wafv2-logging-enabled	Um Ihnen bei der Protokollierung und Überwachung in Ihrer Umgebung zu helfen, aktivieren Sie die AWS WAF (V2) -Protokollierung im regionalen und globalen Web. ACLs AWS Die WAF-Protokollierung bietet detaillierte Informationen über den Datenverkehr, der von Ihrer Web-ACL analysiert wird. In den Protokollen werden die Uhrzeit aufgezeichnet, zu der die AWS WAF die Anfrage von Ihrer AWS Ressource erhalten hat, Informationen zu der Anfrage und eine Aktion für die Regel, der jede Anfrage entsprach.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CA-7.F	CA-7.F Fortlaufende Überwachung	api-gw-execution-logging-aktiviert	Die API-Gateway-Protokollierung zeigt detaillierte Ansichten der Benutzer, die auf die API zugegriffen haben, und wie diese Benutzer auf die API zugegriffen haben. Diese Einblicke ermöglichen die Transparenz von Benutzeraktivitäten.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CA-7.F	CA-7.F Fortlaufende Überwachung	api-gw-xray-enabled	AWS X-Ray sammelt Daten über Anfragen, die Ihre Anwendung bedient, und bietet Tools, mit denen Sie diese Daten anzeigen, filtern und Einblicke in sie gewinnen können, um Probleme und Optimierungsmöglichkeiten zu identifizieren. Stellen Sie sicher, dass X-Ray aktiviert ist, damit Sie detaillierte Informationen nicht nur über die Anfrage und Antwort, sondern auch über Aufrufe erhalten, die Ihre Anwendung an nachgelagerte AWS Ressourcen, Microservices, Datenbanken und HTTP-Web APIs tätigt.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CA-7.F	CA-7.F Fortlaufende Überwachung	autoscaling-group-elb-healthcheck-erforderlich	Die Elastic Load Balancer (ELB) - Zustandsprüfungen für Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling Scaling-Gruppen unterstützen die Aufrechterhaltung einer angemessenen Kapazität und Verfügbarkeit. Der Load Balancer sendet regelmäßig Pings, versucht Verbindungen herzustellen oder sendet Anfragen, um den Zustand der EC2 Amazon-Instances in einer Gruppe mit auto-scaling zu testen. Wenn eine Instance nicht zurückmeldet, wird der Traffic an eine neue EC2 Amazon-Instance gesendet.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CA-7.F	CA-7.F Fortlaufende Überwachung	beanstalk-enhanced-health-reporting-aktiviert	AWS Die verbesserte Zustandsberichterstattung von Elastic Beanstalk ermöglicht eine schnellere Reaktion auf Veränderungen im Zustand der zugrunde liegenden Infrastruktur. Diese Änderungen könnten zu einer mangelnden Verfügbarkeit der Anwendung führen. Die erweiterten Zustandsberichte von Elastic Beanstalk bieten eine Statusbeschreibung, um den Schweregrad der identifizierten Probleme einzuschätzen und mögliche Ursachen zu identifizieren, die untersucht werden müssen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CA-7.F	CA-7.F Fortlaufende Überwachung	cloudtrail-s3-data events-enabled	Die Erfassung von Simple Storage Service (Amazon S3)-Datenereignissen unterstützt die Erkennung von ungewöhnlichen Aktivitäten. Zu den Details gehören Informationen zu dem AWS -Konto, das auf einen Amazon-S3-Bucket zugegriffen hat, die IP-Adresse und die Uhrzeit des Ereignisses.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CA-7.F	CA-7.F Fortlaufende Überwachung	cloudwatch-alarm-action-check	Amazon CloudWatch alarmiert, wenn eine Metrik den Schwellenwert für eine bestimmte Anzahl von Bewertungszeiträumen überschreitet. Der Alarm führt eine oder mehrere Aktionen durch, die vom Wert der Metrik oder des Ausdrucks im Vergleich zu einem Schwellenwert in einer Reihe von Zeiträumen abhängt. Diese Regel erfordert einen Wert für alarmActionRequired (Config Default: True), insufficientDataAction Required (Config Default: True), okActionRequired (Config Default: False). Der tatsächliche Wert muss die Alarmaktionen für Ihre Umgebung widerspiegeln.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CA-7.F	CA-7.F Fortlaufende Überwachung	cloud-trail-cloud-watch-logs-aktiviert	Verwenden Sie Amazon CloudWatch , um Protokoll ereignisaktivitäten zentral zu sammeln und zu verwalten. Die Aufnahme von AWS CloudTrail Daten liefert Einzelheiten zu den API-Aufrufaktivitäten in Ihrem AWS-Konto.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CA-7.F	CA-7.F Fortlaufende Überwachung	cloudtrail-enabled	AWS CloudTrail kann bei der Nichtabstreitbarkeit helfen, indem Aktionen und API-Aufrufe der AWS Management Console aufgezeichnet werden. Sie können die Benutzer und die Benutzer AWS-Konten , die einen AWS Dienst aufgerufen haben, die Quell-IP-Adresse, über die die Aufrufe generiert wurden, und den Zeitpunkt der Anrufe identifizieren. Einzelheiten zu den erfassten Daten finden Sie unter Inhalt des AWS CloudTrail Datensatzes.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CA-7.F	CA-7.F Fortlaufende Überwachung	cw-loggroup-retention-period-überprüfen	Stellen Sie sicher, dass die Ereignisprotokolldaten für Ihre Protokollgruppen über eine Mindestdauer aufbewahrt werden, um die Fehlerbehebung und forensische Untersuchungen zu unterstützen. Fehlende frühere Ereignisprotokolldaten erschweren die Rekonstruierung und Identifizierung potenziell schädlicher Ereignisse.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CA-7.F	CA-7.F Fortlaufende Überwachung	dynamodb-throughput-limit-check	Aktivieren Sie diese Regel, um sicherzustellen, dass die bereitgestellte Durchsatzkapazität in Ihren Amazon-DynamoDB-Tabellen überprüft wird. Dies ist der Umfang der Lese- und Schreibaktivitäten, der von den jeweiligen Tabellen unterstützt werden kann. DynamoDB verwendet diese Informationen für das Reservieren ausreichender Systemressourcen, um Ihren Durchsatz anforderungen gerecht zu werden. Diese Regel generiert eine Warnung, wenn sich der Durchsatz dem Höchstlimit für ein Kundenkonto nähert. Mit dieser Regel können Sie optional die Parameter RCUThreshold Kontoprozentsatz

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
			(Konfigurationsstandard: 80) und WCUThreshold Kontoprozentsatz (Konfigurationsstandard: 80) festlegen. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.
CCCS-fPBMM-CA-7.F	CA-7.F Fortlaufende Überwachung	ec2- instance-detailed-monitoring-enabled	Aktivieren Sie diese Regel, um die Amazon Elastic Compute Cloud (Amazon EC2) - Instance-Überwachung auf der EC2 Amazon-Konsole zu verbessern, in der Monitoring-Diagramme mit einem Zeitraum von 1 Minute für die Instance angezeigt werden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CA-7.F	CA-7.F Fortlaufende Überwachung	ec2-manager instance-managed-by-systems	Eine Bestandsaufnahme der Softwareplattformen und Anwendungen innerhalb des Unternehmens ist möglich, indem Amazon Elastic Compute Cloud (Amazon EC2) - Instances mit AWS Systems Manager verwaltet werden. Verwenden Sie AWS Systems Manager, um detaillierte Systemkonfigurationen, Betriebssystem-Patch-Levels, Namen und Typ der Dienste, Softwareinstallationen, Anwendungsname, Herausgeber und Version sowie andere Details zu Ihrer Umgebung bereitzustellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CA-7.F	CA-7.F Fortlaufende Überwachung	ec2-check managedinstance-association-compliance-status	Verwenden Sie AWS Systems Manager Associations, um bei der Inventarisierung von Softwareplattformen und Anwendungen innerhalb eines Unternehmens zu helfen. AWS Systems Manager weist Ihren verwalteten Instances einen Konfigurationsstatus zu und ermöglicht es Ihnen, Basiswerte für Betriebssystem-Patch-Levels, Softwareinstallationen, Anwendungskonfigurationen und andere Details zu Ihrer Umgebung festzulegen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CA-7.F	CA-7.F Fortlaufende Überwachung	ec2-prüfen managedinstance-patch-compliance-status	Aktivieren Sie diese Regel, um bei der Identifizierung und Dokumentation von Sicherheitslücken in Amazon Elastic Compute Cloud (Amazon EC2) zu helfen. Die Regel prüft, ob die EC2 Amazon-Instance die Patch-Konformität im AWS Systems Manager gemäß den Richtlinien und Verfahren Ihrer Organisation einhält.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CA-7.F	CA-7.F Fortlaufende Überwachung	eip-attached	Diese Regel stellt sicher, dass Elastic, die einer Amazon Virtual Private Cloud (Amazon VPC) IPs zugewiesen sind, an Amazon Elastic Compute Cloud (Amazon EC2) - Instances oder verwendete Elastic Network Interface s angehängt sind. Diese Regel hilft bei der Überwachu ng ungenutzter Inhalte EIPs in Ihrer Umgebung.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CA-7.F	CA-7.F Fortlaufende Überwachung	elb-logging-enabled	Die Elastic-Load-Balancing-Aktivität ist ein zentraler Kommunikationspunkt innerhalb einer Umgebung. Stellen Sie sicher, dass die ELB-Protokollierung aktiviert ist. Die gesammelten Daten enthalten detaillierte Informationen zu Anfragen, die an den ELB gesendet wurden. Jedes Protokoll enthält Informationen wie die Zeit, zu der die Anforderung einging, die Client-IP-Adresse, Latenzen, Anforderungspfade und Serverantworten.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CA-7.F	CA-7.F Fortlaufende Überwachung	guardduty-enabled-centralized	Amazon GuardDuty kann mithilfe von Threat Intellige nce Feeds helfen, potenzielle Cybersich erheitsereignisse zu überwachen und zu erkennen. Dazu gehören Listen mit bösartigen IPs und maschinel len Lernmethoden zur Identifizierung unerwarteter, nicht autorisierter und bösartiger Aktivitäten in Ihrer AWS Cloud-Umgebung.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CA-7.F	CA-7.F Fortlaufende Überwachung	guardduty-non-archived-findings	Amazon GuardDuty hilft Ihnen dabei, die Auswirkungen eines Vorfalls zu verstehen, indem es die Ergebnisse nach Schweregrad klassifiziert: niedrig, mittel und hoch. Diese Klassifizierungen können Sie zur Festlegung von entsprechenden Strategien und Prioritäten zur Behebung solcher Vorfälle verwenden. Mit dieser Regel können Sie optional daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7) und daysHighSev (Config Default: 1) für nicht archivierte Ergebnisse festlegen, wie es die Richtlinien Ihrer Organisation erfordern.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CA-7.F	CA-7.F Fortlaufende Überwachung	lambda-dlq-check	Aktivieren Sie diese Regel, um das entsprechende Personal über Amazon Simple Queue Service (Amazon SQS) oder Amazon Simple Notification Service (Amazon SNS) zu benachrichtigen, wenn eine Funktion ausgefallen ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CA-7.F	CA-7.F Fortlaufende Überwachung	multi-region-cloudtrail-enabled	AWS CloudTrail zeichnet Aktionen und API-Aufrufe der AWS Management Console auf. Sie können feststellen, welche Benutzer und Konten angerufen wurden AWS, von welcher Quell-IP-Adresse aus die Anrufe getätigt wurden und wann die Anrufe erfolgten. CloudTrail übermittelt Protokolldateien aus allen AWS Regionen an Ihren S3-Bucket , wenn MULTI_REG ION_CLOUD _TRAIL_ENABLED aktiviert ist. Außerdem wird beim AWS Start einer neuen Region derselbe Trail in der neuen Region erstellt. CloudTrail Dadurch erhalten Sie automatis ch Protokolldateien mit API-Aktivitäten für die neue Region.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CA-7.F	CA-7.F Fortlaufende Überwachung	rds-enhanced-monitoring-enabled	Aktivieren Sie Amazon Relational Database Service (Amazon RDS), um die Verfügbarkeit von Amazon RDS zu überwachen. Dies bietet einen detaillierten Einblick in den Zustand Ihrer Amazon-RDS-Datenbank-Instances. Wenn der Amazon-RDS-Speicher mehr als ein zugrunde liegendes physisches Gerät verwendet, erfasst Enhanced Monitoring die Daten für jedes Gerät. Wenn die Datenbank-Instance von Amazon RDS in einer Multi-AZ-Bereitstellung ausgeführt wird, werden außerdem die Daten für jedes Gerät auf dem sekundären Host sowie die Metriken des sekundären Hosts erfasst.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CA-7.F	CA-7.F Fortlaufende Überwachung	rds-logging-enabled	Um die Protokollierung und Überwachung in Ihrer Umgebung zu erleichtern, stellen Sie sicher, dass die Amazon Relational Database Service (Amazon RDS)-Protokollierung aktiviert ist. Mit der Amazon-RDS-Protokollierung können Sie Ereignisse wie Verbindungen, Verbindungsabbrüche, Abfragen oder abgefragte Tabellen erfassen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CA-7.F	CA-7.F Fortlaufende Überwachung	redshift-cluster-configuration-check	Um Daten im Ruhezustand zu schützen, muss die Verschlüsselung für Ihre Amazon-Redshift-Cluster aktiviert sein. Sie müssen auch sicherstellen, dass die erforderlichen Konfigurationen auf Amazon-Redshift-Clustern bereitgestellt werden. Die Prüfungsprotokollierung muss aktiviert sein, um Informationen zu Verbindungen und Benutzeraktivitäten in der Datenbank bereitzustellen. Diese Regel erfordert, dass ein Wert für clusterDbEncrypted (Config Default: TRUE) und LoggingEnabled (Config Default: TRUE) gesetzt ist. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CA-7.F	CA-7.F Fortlaufende Überwachung	s3- bucket-logging-enabled	Die Amazon Simple Storage Service (Amazon S3)-Serverzugriffs protokollierung bietet eine Methode zur Überwachu ng des Netzwerks im Hinblick auf potenzielle Cybersich erheitsereignisse. Die Ereignisse werden überwacht, indem detaillierte Aufzeichn ungen über die Anfragen erfasst werden, die an einen Amazon-S3-Bucket gestellt wurden. Jeder Zugriffsprotokolle intrag enthält Details zu einer einzelnen Zugriffsanfrage. Zu den Details gehören Auftraggeber, Bucket-Name, Anforderu ngszeit, Anforderu ngsaktion, Antwortst atus und Fehlercode, falls relevant.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CA-7.F	CA-7.F Fortlaufende Überwachung	securityhub-enabled	AWS Security Hub hilft bei der Überwachung von unbefugtem Personal, Verbindungen, Geräten und Software. AWS Security Hub aggregiert, organisiert und priorisiert die Sicherheitswarnungen oder Ergebnisse mehrerer Dienste. AWS Einige dieser Dienste sind Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer und AWS Firewall Manager sowie AWS Partnerlösungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CA-7.F	CA-7.F Fortlaufende Überwachung	vpc-flow-logs-enabled	VPC-Flow-Protokolle erfassen detaillierte Informationsdatensätze über den IP-Datenverkehr, der zu und von Netzwerkschnittstellen in Ihrer Amazon Virtual Private Cloud (Amazon VPC) fließt. Standardmäßig enthalten Flow-Protokolldatensätze Werte für die verschiedenen Komponenten des IP-Flows, einschließlich Quelle, Ziel und Protokoll.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CA-7.F	CA-7.F Fortlaufende Überwachung	wafv2-logging-enabled	Um Ihnen bei der Protokollierung und Überwachung in Ihrer Umgebung zu helfen, aktivieren Sie die AWS WAF (V2) -Protokollierung im regionalen und globalen Web. ACLs AWS Die WAF-Protokollierung bietet detaillierte Informationen über den Datenverkehr, der von Ihrer Web-ACL analysiert wird. In den Protokollen werden die Uhrzeit aufgezeichnet, zu der die AWS WAF die Anfrage von Ihrer AWS Ressource erhalten hat, Informationen zu der Anfrage und eine Aktion für die Regel, der jede Anfrage entsprach.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CA-7.G	CA-7.G Fortlaufende Überwachung	api-gw-execution-logging-aktiviert	Die API-Gateway-Protokollierung zeigt detaillierte Ansichten der Benutzer, die auf die API zugegriffen haben, und wie diese Benutzer auf die API zugegriffen haben. Diese Einblicke ermöglichen die Transparenz von Benutzeraktivitäten.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CA-7.G	CA-7.G Fortlaufende Überwachung	api-gw-xray-enabled	AWS X-Ray sammelt Daten über Anfragen, die Ihre Anwendung bedient, und bietet Tools, mit denen Sie diese Daten anzeigen, filtern und Einblicke in sie gewinnen können, um Probleme und Optimierungsmöglichkeiten zu identifizieren. Stellen Sie sicher, dass X-Ray aktiviert ist, damit Sie detaillierte Informationen nicht nur über die Anfrage und Antwort, sondern auch über Aufrufe erhalten, die Ihre Anwendung an nachgelagerte AWS Ressourcen, Microservices, Datenbanken und HTTP-Web APIs tätigt.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CA-7.G	CA-7.G Fortlaufende Überwachung	autoscaling-group-elb-healthcheck-erforderlich	Die Elastic Load Balancer (ELB) - Zustandsprüfungen für Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling Scaling-Gruppen unterstützen die Aufrechterhaltung einer angemessenen Kapazität und Verfügbarkeit. Der Load Balancer sendet regelmäßig Pings, versucht Verbindungen herzustellen oder sendet Anfragen, um den Zustand der EC2 Amazon-Instances in einer Gruppe mit auto-scaling zu testen. Wenn eine Instance nicht zurückmeldet, wird der Traffic an eine neue EC2 Amazon-Instance gesendet.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CA-7.G	CA-7.G Fortlaufende Überwachung	beanstalk-enhanced-health-reporting-aktiviert	AWS Die verbesserte Zustandsberichterstattung von Elastic Beanstalk ermöglicht eine schnellere Reaktion auf Veränderungen im Zustand der zugrunde liegenden Infrastruktur. Diese Änderungen könnten zu einer mangelnden Verfügbarkeit der Anwendung führen. Die erweiterten Zustandsberichte von Elastic Beanstalk bieten eine Statusbeschreibung, um den Schweregrad der identifizierten Probleme einzuschätzen und mögliche Ursachen zu identifizieren, die untersucht werden müssen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CA-7.G	CA-7.G Fortlaufende Überwachung	cloudtrail-s3-dataevents-enabled	Die Erfassung von Simple Storage Service (Amazon S3)-Datenereignissen unterstützt die Erkennung von ungewöhnlichen Aktivitäten. Zu den Details gehören Informationen zu dem AWS -Konto, das auf einen Amazon-S3-Bucket zugegriffen hat, die IP-Adresse und die Uhrzeit des Ereignisses.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CA-7.G	CA-7.G Fortlaufende Überwachung	cloudwatch-alarm-action-check	Amazon CloudWatch alarmiert, wenn eine Metrik den Schwellenwert für eine bestimmte Anzahl von Bewertungszeiträumen überschreitet. Der Alarm führt eine oder mehrere Aktionen durch, die vom Wert der Metrik oder des Ausdrucks im Vergleich zu einem Schwellenwert in einer Reihe von Zeiträumen abhängt. Diese Regel erfordert einen Wert für alarmActionRequired (Config Default: True), insufficientDataAction Required (Config Default: True), okActionRequired (Config Default: False). Der tatsächliche Wert muss die Alarmaktionen für Ihre Umgebung widerspiegeln.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CA-7.G	CA-7.G Fortlaufende Überwachung	cloud-trail-cloud-watch-logs-aktiviert	Verwenden Sie Amazon CloudWatch , um Protokoll ereignisaktivitäten zentral zu sammeln und zu verwalten. Die Aufnahme von AWS CloudTrail Daten liefert Einzelheiten zu den API-Aufrufaktivitäten in Ihrem AWS-Konto.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CA-7.G	CA-7.G Fortlaufende Überwachung	cloudtrail-enabled	AWS CloudTrail kann bei der Nichtabstreitbarkeit helfen, indem Aktionen und API-Aufrufe der AWS Management Console aufgezeichnet werden. Sie können die Benutzer und die Benutzer AWS-Konten , die einen AWS Dienst aufgerufen haben, die Quell-IP-Adresse, über die die Aufrufe generiert wurden, und den Zeitpunkt der Anrufe identifizieren. Einzelheiten zu den erfassten Daten finden Sie unter Inhalt des AWS CloudTrail Datensatzes.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CA-7.G	CA-7.G Fortlaufende Überwachung	cw-loggroup-retention-period-überprüfen	Stellen Sie sicher, dass die Ereignisprotokolldaten für Ihre Protokollgruppen über eine Mindestdauer aufbewahrt werden, um die Fehlerbehebung und forensische Untersuchungen zu unterstützen. Fehlende frühere Ereignisprotokolldaten erschweren die Rekonstruierung und Identifizierung potenziell schädlicher Ereignisse.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CA-7.G	CA-7.G Fortlaufende Überwachung	dynamodb-throughput-limit-check	Aktivieren Sie diese Regel, um sicherzustellen, dass die bereitgestellte Durchsatzkapazität in Ihren Amazon-DynamoDB-Tabellen überprüft wird. Dies ist der Umfang der Lese- und Schreibaktivitäten, der von den jeweiligen Tabellen unterstützt werden kann. DynamoDB verwendet diese Informationen für das Reservieren ausreichender Systemressourcen, um Ihren Durchsatz anforderungen gerecht zu werden. Diese Regel generiert eine Warnung, wenn sich der Durchsatz dem Höchstlimit für ein Kundenkonto nähert. Mit dieser Regel können Sie optional die Parameter RCUThreshold Kontoprozentsatz

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
			(Konfigurationsstandard: 80) und WCUThreshold Kontoprozentsatz (Konfigurationsstandard: 80) festlegen. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.
CCCS-fPBMM-CA-7.G	CA-7.G Fortlaufende Überwachung	ec2- instance-detailed-monitoring-enabled	Aktivieren Sie diese Regel, um die Amazon Elastic Compute Cloud (Amazon EC2) - Instance-Überwachung auf der EC2 Amazon-Konsole zu verbessern, in der Monitoring-Diagramme mit einem Zeitraum von 1 Minute für die Instance angezeigt werden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CA-7.G	CA-7.G Fortlaufende Überwachung	ec2-manager instance-managed-by-systems	Eine Bestandsaufnahme der Softwareplattformen und Anwendungen innerhalb des Unternehmens ist möglich, indem Amazon Elastic Compute Cloud (Amazon EC2) - Instances mit AWS Systems Manager verwaltet werden. Verwenden Sie AWS Systems Manager, um detaillierte Systemkonfigurationen, Betriebssystem-Patch-Levels, Namen und Typ der Dienste, Softwareinstallationen, Anwendungsname, Herausgeber und Version sowie andere Details zu Ihrer Umgebung bereitzustellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CA-7.G	CA-7.G Fortlaufende Überwachung	ec2-check managedinstance-association-compliance-status	Verwenden Sie AWS Systems Manager Associations, um bei der Inventarisierung von Softwareplattformen und Anwendungen innerhalb eines Unternehmens zu helfen. AWS Systems Manager weist Ihren verwalteten Instances einen Konfigurationsstatus zu und ermöglicht es Ihnen, Basiswerte für Betriebssystem-Patch-Levels, Softwareinstallationen, Anwendungskonfigurationen und andere Details zu Ihrer Umgebung festzulegen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CA-7.G	CA-7.G Fortlaufende Überwachung	ec2-prüfen managedinstance-patch-compliance-status	Aktivieren Sie diese Regel, um bei der Identifizierung und Dokumentation von Sicherheitslücken in Amazon Elastic Compute Cloud (Amazon EC2) zu helfen. Die Regel prüft, ob die EC2 Amazon-Instance die Patch-Konformität im AWS Systems Manager gemäß den Richtlinien und Verfahren Ihrer Organisation einhält.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CA-7.G	CA-7.G Fortlaufende Überwachung	eip-attached	Diese Regel stellt sicher, dass Elastic, die einer Amazon Virtual Private Cloud (Amazon VPC) IPs zugewiesen sind, an Amazon Elastic Compute Cloud (Amazon EC2) - Instances oder verwendete Elastic Network Interface s angehängt sind. Diese Regel hilft bei der Überwachu ng ungenutzter Inhalte EIPs in Ihrer Umgebung.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CA-7.G	CA-7.G Fortlaufende Überwachung	elb-logging-enabled	Die Elastic-Load-Balancing-Aktivität ist ein zentraler Kommunikationspunkt innerhalb einer Umgebung. Stellen Sie sicher, dass die ELB-Protokollierung aktiviert ist. Die gesammelten Daten enthalten detaillierte Informationen zu Anfragen, die an den ELB gesendet wurden. Jedes Protokoll enthält Informationen wie die Zeit, zu der die Anforderung einging, die Client-IP-Adresse, Latenzen, Anforderungspfade und Serverantworten.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CA-7.G	CA-7.G Fortlaufende Überwachung	guardduty-enabled-centralized	Amazon GuardDuty kann mithilfe von Threat Intellige nce Feeds helfen, potenzielle Cybersich erheitsereignisse zu überwachen und zu erkennen. Dazu gehören Listen mit bösartigen IPs und maschinel len Lernmethoden zur Identifizierung unerwarteter, nicht autorisierter und bösartiger Aktivitäten in Ihrer AWS Cloud-Umgebung.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CA-7.G	CA-7.G Fortlaufende Überwachung	guardduty-non-archived-findings	Amazon GuardDuty hilft Ihnen dabei, die Auswirkungen eines Vorfalls zu verstehen, indem es die Ergebnisse nach Schweregrad klassifiziert: niedrig, mittel und hoch. Diese Klassifizierungen können Sie zur Festlegung von entsprechenden Strategien und Prioritäten zur Behebung solcher Vorfälle verwenden. Mit dieser Regel können Sie optional daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7) und daysHighSev (Config Default: 1) für nicht archivierte Ergebnisse festlegen, wie es die Richtlinien Ihrer Organisation erfordern.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CA-7.G	CA-7.G Fortlaufende Überwachung	lambda-dlq-check	Aktivieren Sie diese Regel, um das entsprechende Personal über Amazon Simple Queue Service (Amazon SQS) oder Amazon Simple Notification Service (Amazon SNS) zu benachrichtigen, wenn eine Funktion ausgefallen ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CA-7.G	CA-7.G Fortlaufende Überwachung	multi-region-cloudtrail-enabled	AWS CloudTrail zeichnet Aktionen und API-Aufrufe der AWS Management Console auf. Sie können feststellen, welche Benutzer und Konten angerufen wurden AWS, von welcher Quell-IP-Adresse aus die Anrufe getätigt wurden und wann die Anrufe erfolgten. CloudTrail übermittelt Protokolldateien aus allen AWS Regionen an Ihren S3-Bucket , wenn MULTI_REGION_CLOUD_TRAIL_ENABLED aktiviert ist. Außerdem wird beim AWS Start einer neuen Region derselbe Trail in der neuen Region erstellt. CloudTrail Dadurch erhalten Sie automatisch Protokolldateien mit API-Aktivitäten für die neue Region.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CA-7.G	CA-7.G Fortlaufende Überwachung	rds-enhanced-monitoring-enabled	Aktivieren Sie Amazon Relational Database Service (Amazon RDS), um die Verfügbarkeit von Amazon RDS zu überwachen. Dies bietet einen detaillierten Einblick in den Zustand Ihrer Amazon-RDS-Datenbank-Instances. Wenn der Amazon-RDS-Speicher mehr als ein zugrunde liegendes physisches Gerät verwendet, erfasst Enhanced Monitoring die Daten für jedes Gerät. Wenn die Datenbank-Instance von Amazon RDS in einer Multi-AZ-Bereitstellung ausgeführt wird, werden außerdem die Daten für jedes Gerät auf dem sekundären Host sowie die Metriken des sekundären Hosts erfasst.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CA-7.G	CA-7.G Fortlaufende Überwachung	rds-logging-enabled	Um die Protokollierung und Überwachung in Ihrer Umgebung zu erleichtern, stellen Sie sicher, dass die Amazon Relational Database Service (Amazon RDS)-Protokollierung aktiviert ist. Mit der Amazon-RDS-Protokollierung können Sie Ereignisse wie Verbindungen, Verbindungsabbrüche, Abfragen oder abgefragte Tabellen erfassen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CA-7.G	CA-7.G Fortlaufende Überwachung	redshift-cluster-configuration-check	Um Daten im Ruhezustand zu schützen, muss die Verschlüsselung für Ihre Amazon-Redshift-Cluster aktiviert sein. Sie müssen auch sicherstellen, dass die erforderlichen Konfigurationen auf Amazon-Redshift-Clustern bereitgestellt werden. Die Prüfungsprotokollierung muss aktiviert sein, um Informationen zu Verbindungen und Benutzeraktivitäten in der Datenbank bereitzustellen. Diese Regel erfordert, dass ein Wert für clusterDbEncrypted (Config Default: TRUE) und LoggingEnabled (Config Default: TRUE) gesetzt ist. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CA-7.G	CA-7.G Fortlaufende Überwachung	s3- bucket-logging-enabled	Die Amazon Simple Storage Service (Amazon S3)-Serverzugriffs protokollierung bietet eine Methode zur Überwachu ng des Netzwerks im Hinblick auf potenzielle Cybersich erheitsereignisse. Die Ereignisse werden überwacht, indem detaillierte Aufzeichn ungen über die Anfragen erfasst werden, die an einen Amazon-S3-Bucket gestellt wurden. Jeder Zugriffsprotokolle intrag enthält Details zu einer einzelnen Zugriffsanfrage. Zu den Details gehören Auftraggeber, Bucket-Name, Anforderu ngszeit, Anforderu ngsaktion, Antwortst atus und Fehlercode, falls relevant.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CA-7.G	CA-7.G Fortlaufende Überwachung	securityhub-enabled	AWS Security Hub hilft bei der Überwachung von unbefugtem Personal, Verbindungen, Geräten und Software. AWS Security Hub aggregiert, organisiert und priorisiert die Sicherheitswarnungen oder Ergebnisse mehrerer Dienste. AWS Einige dieser Dienste sind Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer und AWS Firewall Manager sowie AWS Partnerlösungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CA-7.G	CA-7.G Fortlaufende Überwachung	vpc-flow-logs-enabled	VPC-Flow-Protokolle erfassen detaillierte Informationsdatensätze über den IP-Datenverkehr, der zu und von Netzwerkschnittstellen in Ihrer Amazon Virtual Private Cloud (Amazon VPC) fließt. Standardmäßig enthalten Flow-Protokolldatensätze Werte für die verschiedenen Komponenten des IP-Flows, einschließlich Quelle, Ziel und Protokoll.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CA-7.G	CA-7.G Fortlaufende Überwachung	wafv2-logging-enabled	Um Ihnen bei der Protokollierung und Überwachung in Ihrer Umgebung zu helfen, aktivieren Sie die AWS WAF (V2) -Protokollierung im regionalen und globalen Web. ACLs AWS Die WAF-Protokollierung bietet detaillierte Informationen über den Datenverkehr, der von Ihrer Web-ACL analysiert wird. In den Protokollen werden die Uhrzeit aufgezeichnet, zu der die AWS WAF die Anfrage von Ihrer AWS Ressource erhalten hat, Informationen zu der Anfrage und eine Aktion für die Regel, der jede Anfrage entsprach.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CA-9.A	CA-9.A Interne Systemverbindungen	alb-http-to-https-Umleitungsprüfung	Um Daten während der Übertragung zu schützen, stellen Sie sicher, dass Ihr Application Load Balancer unverschlüsselte HTTP-Anfragen automatisch an HTTPS umleitet. Da sensible Daten vorhanden sein können, sollten Sie die Verschlüsselung bei der Übertragung aktivieren, um diese Daten zu schützen.
CCCS-fPBMM-CA-9.A	CA-9.A Interne Systemverbindungen	api-gw-ssl-enabled	Stellen Sie sicher, dass die REST-API-Stufen von Amazon API Gateway mit SSL-Zertifikaten konfiguriert sind, damit Backend-Systeme überprüfen können, ob Anforderungen von API Gateway stammen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CA-9.A	CA-9.A Interne Systemverbindungen	dms-replication-not-public	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass auf DMS-Replikationsinstanzen nicht öffentlich zugegriffen werden kann. DMS-Replikations-Instances können vertrauliche Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.
CCCS-fPBMM-CA-9.A	CA-9.A Interne Systemverbindungen	ebs-snapshot-public-restorable-überprüfen	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass EBS-Snapshots nicht öffentlich wiederherstellbar sind. EBS-Volume-Snapshots können vertrauliche Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CA-9.A	CA-9.A Interne Systemverbindungen	ec-2 instance-no-public-ip	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon Elastic Compute Cloud (Amazon EC2) - Instances nicht öffentlich zugänglic h sind. EC2Amazon -Instances können vertrauliche Informati onen enthalten, und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CA-9.A	CA-9.A Interne Systemverbindungen	elasticsearch-in-vpc-only	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass sich Amazon OpenSearch OpenSearch Service (Service) - Domains innerhalb einer Amazon Virtual Private Cloud (Amazon VPC) befinden. Eine OpenSearch Service-Domain innerhalb einer Amazon VPC ermöglicht die sichere Kommunikation zwischen OpenSearch Service und anderen Services innerhalb der Amazon VPC, ohne dass ein Internet-Gateway, ein NAT-Gerät oder eine VPN-Verbindung erforderlich ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CA-9.A	CA-9.A Interne Systemverbindungen	elasticsearch-node-to-node-Verschlüsselungsprüfung	Stellen Sie sicher, dass die node-to-node Verschlüsselung für Amazon OpenSearch Service aktiviert ist. Node-to-nodeVerschlüsselung ermöglicht die TLS 1.2-Verschlüsselung für die gesamte Kommunikation innerhalb der Amazon Virtual Private Cloud (Amazon VPC). Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CA-9.A	CA-9.A Interne Systemverbindungen	elb-acm-certificate-required	Zum Schutz von eventuell vorhanden en sensiblen Daten sowie von Daten während der Übertragung muss die Verschlüsselung für Ihr Elastic Load Balancing aktiviert sein. Verwenden Sie AWS Certificate Manager, um öffentlic he und private SSL/ TLS-Zertifikate mit AWS Diensten und internen Ressource n zu verwalten, bereitzustellen und bereitzustellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CA-9.A	CA-9.A Interne Systemverbindungen	elb-predefined-security-policy-ssl-check	Stellen Sie sicher, dass Ihre SSL-Listener von Classic Elastic Load Balancing eine vordefinierte Sicherheitsrichtlinie verwenden, um Daten während der Übertragung zu schützen. Elastic Load Balancing bietet vordefinierte Aushandlungskonfigurationen, die für die SSL-Aushandlung verwendet werden, wenn eine Verbindung zwischen einem Client und Ihrem Load Balancer hergestellt wurde. Die SSL-Aushandlungskonfigurationen sind mit einer breiten Palette von Clients kompatibel und verwenden hochfeste kryptografische Algorithmen. Diese Regel verlangt, dass Sie eine vordefinierte Sicherheitsrichtlinie für Ihre SSL-Liste

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
			ner festlegen. Die Standard-Sicherheitsrichtlinie lautet: Policy-TLS-1-2-2017-0. ELBSecurity Der tatsächliche Wert muss den Richtlinien Ihrer Organisation entsprechen.
CCCS-fPBMM-CA-9.A	CA-9.A Interne Systemverbindungen	elb-tls-https-listeners-nur	Stellen Sie sicher, dass Ihre Elastic Load Balancer (ELBs) mit SSL- oder HTTPS-Listenern konfiguriert sind. Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CA-9.A	CA-9.A Interne Systemverbindungen	emr-master-no-public-ip	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon EMR-Cluster-Masterknoten nicht öffentlich zugänglich sind. Amazon-EMR-Cluster-Hauptknoten können vertrauliche Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CA-9.A	CA-9.A Interne Systemverbindungen	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) Security Groups können bei der Verwaltung des Netzwerkzugriffs helfen, indem sie eine statusbehaftete Filterung des ein- und ausgehenden Netzwerkverkehrs zu Ressourcen bereitstellen. AWS Wenn Sie eingehenden (oder entfernten) Datenverkehr von 0.0.0.0/0 bis Port 22 auf Ihren Ressourcen nicht zulassen, können Sie den Remote-Zugriff einschränken.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CA-9.A	CA-9.A Interne Systemverbindungen	ec-2 instances-in-vpc	Stellen Sie Amazon Elastic Compute Cloud (Amazon EC2) -Instances innerhalb einer Amazon Virtual Private Cloud (Amazon VPC) bereit, um eine sichere Kommunika tion zwischen einer Instance und anderen Services innerhalb der Amazon VPC zu ermöglichen, ohne dass ein Internet-Gateway, ein NAT-Gerät oder eine VPN-Verbindung erforderlich ist. Der gesamte Datenverk ehr bleibt sicher in der AWS Cloud. Domains, die sich innerhalb einer VPC befinden, verfügen aufgrund ihrer logischen Isolierun g im Vergleich zu Domains mit öffentlic hen Endpunkten über eine zusätzlic he Sicherheitsebene. Weisen Sie EC2

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
			Amazon-Instances einer Amazon VPC zu, um den Zugriff ordnungsgemäß zu verwalten.
CCCS-fPBMM-CA-9.A	CA-9.A Interne Systemverbindungen	internet-gateway-authorized-vpc-nur	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Internet-Gateways nur mit autorisierter Amazon Virtual Private Cloud (Amazon VPC) verbunden sind. Internet-Gateways ermöglichen den bidirektionalen Internetzugang zur und von der Amazon VPC, was möglicher weise zu einem unbefugten Zugriff auf Amazon-VPC-Ressourcen führen kann.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CA-9.A	CA-9.A Interne Systemverbindungen	lambda-function-public-access-verboten	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass AWS Lambda-Funktionen nicht öffentlich zugänglich sind. Der öffentliche Zugriff kann möglicherweise die Verfügbarkeit von Ressourcen beeinträchtigen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CA-9.A	CA-9.A Interne Systemverbindungen	lambda-inside-vpc	Stellen Sie AWS Lambda-Funktionen in einer Amazon Virtual Private Cloud (Amazon VPC) bereit, um eine sichere Kommunikation zwischen einer Funktion und anderen Diensten innerhalb der Amazon VPC zu gewährleisten. Bei dieser Konfiguration sind kein Internet-Gateway, kein NAT-Gerät und keine VPN-Verbindung erforderlich. Der gesamte Datenverkehr bleibt sicher in der Cloud. AWS Domains, die sich innerhalb einer VPC befinden, verfügen aufgrund ihrer logischen Isolierung im Vergleich zu Domains mit öffentlichen Endpunkten über eine zusätzliche Sicherheitsebene. Um den Zugriff ordnungsgemäß zu verwalten,

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
			sollten AWS Lambda-Funktionen einer VPC zugewiesen werden.
CCCS-fPBMM-CA-9.A	CA-9.A Interne Systemverbindungen	opensearch-node-to-node-Verschlüsselungsprüfung	Stellen Sie sicher, dass die node-to-node Verschlüsselung für Amazon OpenSearch Service aktiviert ist. Node-to-nodeVerschlüsselung ermöglicht die TLS 1.2-Verschlüsselung für die gesamte Kommunikation innerhalb der Amazon Virtual Private Cloud (Amazon VPC). Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CA-9.A	CA-9.A Interne Systemverbindungen	rds-instance-public-access-überprüfen	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Relational Database Service (Amazon RDS) -Instances nicht öffentlich sind. Amazon-RDS-Datenbank-Instances können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CA-9.A	CA-9.A Interne Systemverbindungen	rds-snapshots-public-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Relational Database Service (Amazon RDS) -Instances nicht öffentlich sind. Amazon-RDS-Datenbank-Instances können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CA-9.A	CA-9.A Interne Systemverbindungen	redshift-cluster-public-access-überprüfen	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Redshift Redshift-Cluster nicht öffentlich sind. Amazon-Redshift-Cluster können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.
CCCS-fPBMM-CA-9.A	CA-9.A Interne Systemverbindungen	redshift-require-tls-ssl	Stellen Sie sicher, dass Ihre Amazon-Redshift-Cluster eine TLS/SSL-Verschlüsselung erfordern, um eine Verbindung zu SQL-Clients herzustellen. Da sensible Daten vorhanden sein können, sollten Sie die Verschlüsselung bei der Übertragung aktivieren, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CA-9.A	CA-9.A Interne Systemverbindungen	restricted-common-ports	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass gemeinsame Ports für Amazon Elastic Compute Cloud (Amazon EC2) -Sicherheitsgruppen eingeschränkt sind. Wenn der Zugriff auf Ports nicht auf vertrauenswürdige Quellen beschränkt wird, kann dies zu Angriffen auf die Verfügbarkeit, Integrität und Vertraulichkeit von Systemen führen. Mit dieser Regel können Sie optional die Parameter blockedPort1–blockedPort5 festlegen (Standardkonfigurationen: 20, 21, 3389, 3306, 4333). Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CA-9.A	CA-9.A Interne Systemverbindungen	s3- account-level-public-access -blöcke-periodisch	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Simple Storage Service (Amazon S3) -Buckets nicht öffentlich zugänglich sind. Diese Regel trägt dazu bei, sensible Daten vor unbefugten Remote-Benutzern zu schützen, indem sie den öffentlichen Zugriff verhindert. Mit dieser Regel können Sie optional die Parameter ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) und restrictPublicBuckets Parameter (Config Default: True) festlegen. Die tatsächlichen Werte müssen den Richtlini

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
			en Ihrer Organisation entsprechen.
CCCS-fPBMM-CA-9.A	CA-9.A Interne Systemverbindungen	s3 bucket-level-public-access - verboten	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Simple Storage Service (Amazon S3) -Buckets nicht öffentlich zugänglich sind. Diese Regel trägt dazu bei, sensible Daten vor unbefugten Remote-Benutzern zu schützen, indem sie den öffentlichen Zugriff auf Bucket-Ebene verhindert.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CA-9.A	CA-9.A Interne Systemverbindungen	s-3 bucket-public-read-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie nur autorisierten Benutzern, Prozessen und Geräten Zugriff auf Amazon Simple Storage Service (Amazon S3) - Buckets gewähren. Die Verwaltung des Zugriffs sollte mit der Klassifizierung der Daten übereinst immen.
CCCS-fPBMM-CA-9.A	CA-9.A Interne Systemverbindungen	s3- bucket-public-write-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie nur autorisierten Benutzern, Prozessen und Geräten Zugriff auf Amazon Simple Storage Service (Amazon S3) - Buckets gewähren. Die Verwaltung des Zugriffs sollte mit der Klassifizierung der Daten übereinst immen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CA-9.A	CA-9.A Interne Systemverbindungen	s3- bucket-ssl-requests-only	Um Daten während der Übertragung zu schützen, stellen Sie sicher, dass Ihre Amazon Simple Storage Service (Amazon S3)-Buckets Anfragen zur Verwendung von Secure Socket Layer (SSL)-Buckets erfordern. Da sensible Daten vorhanden sein können, sollten Sie die Verschlüsselung bei der Übertragung aktivieren, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CA-9.A	CA-9.A Interne Systemverbindungen	sagemaker-notebook-no-direct-Internetzugang	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass SageMaker Amazon-Notebooks keinen direkten Internetzugang zulassen. Indem Sie direkten Internetzugang blockieren, vermeiden Sie, dass unbefugte Benutzer auf sensible Daten zugreifen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CA-9.A	CA-9.A Interne Systemverbindungen	subnet-auto-assign-public-ip-deaktiviert	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon Virtual Private Cloud (VPC) -Subnetzen nicht automatisch eine öffentliche IP-Adresse zugewiesen wird. Amazon Elastic Compute Cloud (EC2) -Instances, die in Subnetzen gestartet werden, in denen dieses Attribut aktiviert ist, haben ihrer primären Netzwerkschnittstelle eine öffentliche IP-Adresse zugewiesen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CA-9.A	CA-9.A Interne Systemverbindungen	vpc-default-security-group-geschlossen	Sicherheitsgruppen von Amazon Elastic Compute Cloud (Amazon EC2) können bei der Verwaltung des Netzwerkzugriffs helfen, indem sie eine statusbehaftete Filterung des ein- und ausgehenden Netzwerkverkehrs zu Ressourcen bereitstellen. AWS Die Beschränk ung des gesamten Datenverkehrs auf die Standardsicherheit sgruppe hilft dabei, den Fernzugriff auf Ihre Ressourcen einzuschränken. AWS

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CA-9.A	CA-9.A Interne Systemverbindungen	vpc-sg-open-only-to-authorized-ports	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass gemeinsame Ports für Amazon Elastic Compute Cloud (Amazon EC2) -Sicherheitsgruppen eingeschränkt sind. Wenn der Zugriff auf Ports nicht auf vertrauenswürdige Quellen beschränkt wird, kann dies zu Angriffen auf die Verfügbarkeit, Integrität und Vertraulichkeit von Systemen führen. Durch die Beschränkung des Zugriffs auf Ressourcen innerhalb einer Sicherheitsgruppe aus dem Internet (0.0.0.0/0) kann der Fernzugriff auf interne Systeme gesteuert werden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CM-2.A	CM-2.A Basiskonfiguration	ec2-manager instance-managed-by-systems	Eine Bestandsaufnahme der Softwareplattformen und Anwendungen innerhalb des Unternehmens ist möglich, indem Amazon Elastic Compute Cloud (Amazon EC2) - Instances mit AWS Systems Manager verwaltet werden. Verwenden Sie AWS Systems Manager, um detaillierte Systemkonfigurationen, Betriebssystem-Patch-Levels, Namen und Typ der Dienste, Softwareinstallationen, Anwendungsname, Herausgeber und Version sowie andere Details zu Ihrer Umgebung bereitzustellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CM-2.A	CM-2.A Basiskonfiguration	ec2-check managedinstance-association-compliance-status	Verwenden Sie AWS Systems Manager Associations, um bei der Inventarisierung von Softwareplattformen und Anwendungen innerhalb eines Unternehmens zu helfen. AWS Systems Manager weist Ihren verwalteten Instances einen Konfigurationsstatus zu und ermöglicht es Ihnen, Basiswerte für Betriebssystem-Patch-Levels, Softwareinstallationen, Anwendungskonfigurationen und andere Details zu Ihrer Umgebung festzulegen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CM-2.A	CM-2.A Basiskonfiguration	ec2-stopped-instance	Aktivieren Sie diese Regel, um bei der Basiskonfiguration von Amazon Elastic Compute Cloud (Amazon EC2) - Instances zu helfen, indem Sie überprüfen, ob EC2 Amazon-Instances gemäß den Standards Ihrer Organisation für mehr als die zulässige Anzahl von Tagen gestoppt wurden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CM-2.A	CM-2.A Basiskonfiguration	ec2- volume-inuse-check	Diese Regel stellt sicher, dass Amazon Elastic Block Store-Volumes, die an Amazon Elastic Compute Cloud (Amazon EC2) - Instances angehängt sind, zum Löschen markiert werden, wenn eine Instance beendet wird. Wenn ein Amazon-EBS-Volume nicht gelöscht wird, wenn die Instance, an die es angehängt ist, beendet wird, kann dies gegen das Konzept der geringsten Funktionalität verstoßen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CM-2.A	CM-2.A Basiskonfiguration	elb-deletion-protection-enabled	Diese Regel sorgt dafür, dass der Löschschutz für Elastic Load Balancing aktiviert ist. Verwenden Sie diese Funktion, um zu verhindern, dass Ihr Load Balancer versehentlich oder böswillig gelöscht wird, was zum Verlust der Verfügbarkeit Ihrer Anwendungen führen kann.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CM-2.A	CM-2.A Basiskonfiguration	redshift-cluster-maintenancesettings-check	Diese Regel stellt sicher, dass Amazon-Redshift-Cluster die bevorzugten Einstellungen für Ihre Organisation haben. Insbesondere sorgt sie dafür, dass Cluster bevorzugte Wartungsfenster und automatisierte Aufbewahrungsfristen für Snapshots für die Datenbank haben. Für diese Regel müssen Sie die festlegen allowVersionUpgrade. Der Standardwert ist „true“. Außerdem können Sie optional den Zeitraum preferredMaintenanceWindow (der Standardwert ist sa: 16:00 -sa: 16:30) und den automated SnapshotRetention Zeitraum (der Standardwert ist 1) festlegen. Die tatsächlichen Werte müssen den Richtlini

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
			en Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CM-2.A	CM-2.A Basiskonfiguration	restricted-common-ports	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass gemeinsame Ports für Amazon Elastic Compute Cloud (Amazon EC2) -Sicherheitsgruppen eingeschränkt sind. Wenn der Zugriff auf Ports nicht auf vertrauenswürdige Quellen beschränkt wird, kann dies zu Angriffen auf die Verfügbarkeit, Integrität und Vertraulichkeit von Systemen führen. Mit dieser Regel können Sie optional die Parameter blockedPort1–blockedPort5 festlegen (Standardkonfigurationen: 20, 21, 3389, 3306, 4333). Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CM-3.A	CM-3.A Kontrolle von Konfigurationsänderungen	cloudtrail-enabled	AWS CloudTrail kann durch die Aufzeichnung von Aktionen und API-Aufrufen in der AWS Management Console bei der Nichtabstreitbarkeit helfen. Sie können die Benutzer und die Benutzer AWS-Konten , die einen AWS Dienst aufgerufen haben, die Quell-IP-Adresse, über die die Aufrufe generiert wurden, und den Zeitpunkt der Anrufe identifizieren. Einzelheiten zu den erfassten Daten finden Sie unter Inhalt des AWS CloudTrail Datensatzes.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CM-3.A	CM-3.A Kontrolle von Konfigurationsände rungen	multi-region-cloudtrail-enabled	AWS CloudTrail zeichnet Aktionen und API-Aufrufe der AWS Management Console auf. Sie können feststellen, welche Benutzer und Konten angerufen wurden AWS, von welcher Quell-IP-Adresse aus die Anrufe getätigt wurden und wann die Anrufe erfolgten. CloudTrail übermittelt Protokolldateien aus allen AWS Regionen an Ihren S3-Bucket , wenn MULTI_REG ION_CLOUD _TRAIL_ENABLED aktiviert ist. Außerdem wird beim AWS Start einer neuen Region derselbe Trail in der neuen Region erstellt. CloudTrail Dadurch erhalten Sie automatis ch Protokolldateien mit API-Aktivitäten für die neue Region.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CM-3.B	CM-3.B Kontrolle von Konfigurationsänderungen	cloudtrail-enabled	AWS CloudTrail kann durch die Aufzeichnung von Aktionen und API-Aufrufen in der AWS Management Console bei der Nichtabstreitbarkeit helfen. Sie können die Benutzer und die Benutzer AWS-Konten , die einen AWS Dienst aufgerufen haben, die Quell-IP-Adresse, über die die Aufrufe generiert wurden, und den Zeitpunkt der Anrufe identifizieren. Einzelheiten zu den erfassten Daten finden Sie unter Inhalt des AWS CloudTrail Datensatzes.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CM-3.B	CM-3.B Kontrolle von Konfigurationsände rungen	multi-region-cloudtrail-enabled	AWS CloudTrail zeichnet Aktionen und API-Aufrufe der AWS Management Console auf. Sie können feststellen, welche Benutzer und Konten angerufen wurden AWS, von welcher Quell-IP-Adresse aus die Anrufe getätigt wurden und wann die Anrufe erfolgten. CloudTrail übermittelt Protokolldateien aus allen AWS Regionen an Ihren S3-Bucket , wenn MULTI_REG ION_CLOUD _TRAIL_ENABLED aktiviert ist. Außerdem wird beim AWS Start einer neuen Region derselbe Trail in der neuen Region erstellt. CloudTrail Dadurch erhalten Sie automatis ch Protokolldateien mit API-Aktivitäten für die neue Region.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CM-3.C	CM-3.C Kontrolle von Konfigurationsänderungen	cloudtrail-enabled	AWS CloudTrail kann durch die Aufzeichnung von Aktionen und API-Aufrufen in der AWS Management Console bei der Nichtabstreitbarkeit helfen. Sie können die Benutzer und die Benutzer AWS-Konten , die einen AWS Dienst aufgerufen haben, die Quell-IP-Adresse, über die die Aufrufe generiert wurden, und den Zeitpunkt der Anrufe identifizieren. Einzelheiten zu den erfassten Daten finden Sie unter Inhalt des AWS CloudTrail Datensatzes.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CM-3.C	CM-3.C Kontrolle von Konfigurationsände rungen	multi-region-cloudtrail-enabled	AWS CloudTrail zeichnet Aktionen und API-Aufrufe der AWS Management Console auf. Sie können feststellen, welche Benutzer und Konten angerufen wurden AWS, von welcher Quell-IP-Adresse aus die Anrufe getätigt wurden und wann die Anrufe erfolgten. CloudTrail übermittelt Protokolldateien aus allen AWS Regionen an Ihren S3-Bucket , wenn MULTI_REG ION_CLOUD _TRAIL_ENABLED aktiviert ist. Außerdem wird beim AWS Start einer neuen Region derselbe Trail in der neuen Region erstellt. CloudTrail Dadurch erhalten Sie automatis ch Protokolldateien mit API-Aktivitäten für die neue Region.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CM-3.D	CM-3.D Kontrolle von Konfigurationsänderungen	cloudtrail-enabled	AWS CloudTrail kann durch die Aufzeichnung von Aktionen und API-Aufrufen in der AWS Management Console bei der Nichtabstreitbarkeit helfen. Sie können die Benutzer und die Benutzer AWS-Konten , die einen AWS Dienst aufgerufen haben, die Quell-IP-Adresse, über die die Aufrufe generiert wurden, und den Zeitpunkt der Anrufe identifizieren. Einzelheiten zu den erfassten Daten finden Sie unter Inhalt des AWS CloudTrail Datensatzes.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CM-3.D	CM-3.D Kontrolle von Konfigurationsände rungen	multi-region-cloudtrail-enabled	AWS CloudTrail zeichnet Aktionen und API-Aufrufe der AWS Management Console auf. Sie können feststellen, welche Benutzer und Konten angerufen wurden AWS, von welcher Quell-IP-Adresse aus die Anrufe getätigt wurden und wann die Anrufe erfolgten. CloudTrail übermittelt Protokolldateien aus allen AWS Regionen an Ihren S3-Bucket , wenn MULTI_REG ION_CLOUD _TRAIL_ENABLED aktiviert ist. Außerdem wird beim AWS Start einer neuen Region derselbe Trail in der neuen Region erstellt. CloudTrail Dadurch erhalten Sie automatis ch Protokolldateien mit API-Aktivitäten für die neue Region.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CM-3.E	CM-3.E Kontrolle von Konfigurationsänderungen	cloudtrail-enabled	AWS CloudTrail kann durch die Aufzeichnung von Aktionen und API-Aufrufen in der AWS Management Console bei der Nichtabstreitbarkeit helfen. Sie können die Benutzer und die Benutzer AWS-Konten , die einen AWS Dienst aufgerufen haben, die Quell-IP-Adresse, über die die Aufrufe generiert wurden, und den Zeitpunkt der Anrufe identifizieren. Einzelheiten zu den erfassten Daten finden Sie unter Inhalt des AWS CloudTrail Datensatzes.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CM-3.E	CM-3.E Kontrolle von Konfigurationsände rungen	multi-region-cloudtrail-enabled	AWS CloudTrail zeichnet Aktionen und API-Aufrufe der AWS Management Console auf. Sie können feststellen, welche Benutzer und Konten angerufen wurden AWS, von welcher Quell-IP-Adresse aus die Anrufe getätigt wurden und wann die Anrufe erfolgten. CloudTrail übermittelt Protokolldateien aus allen AWS Regionen an Ihren S3-Bucket , wenn MULTI_REG ION_CLOUD _TRAIL_ENABLED aktiviert ist. Außerdem wird beim AWS Start einer neuen Region derselbe Trail in der neuen Region erstellt. CloudTrail Dadurch erhalten Sie automatis ch Protokolldateien mit API-Aktivitäten für die neue Region.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CM-3.F	CM-3F Kontrolle von Konfigurationsänderungen	cloudtrail-enabled	AWS CloudTrail kann durch die Aufzeichnung von Aktionen und API-Aufrufen in der AWS Management Console bei der Nichtabstreitbarkeit helfen. Sie können die Benutzer und die Benutzer AWS-Konten , die einen AWS Dienst aufgerufen haben, die Quell-IP-Adresse, über die die Aufrufe generiert wurden, und den Zeitpunkt der Anrufe identifizieren. Einzelheiten zu den erfassten Daten finden Sie unter Inhalt des AWS CloudTrail Datensatzes.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CM-3.F	CM-3F Kontrolle von Konfigurationsände rungen	multi-region-cloudtrail-enabled	AWS CloudTrail zeichnet Aktionen und API-Aufrufe der AWS Management Console auf. Sie können feststellen, welche Benutzer und Konten angerufen wurden AWS, von welcher Quell-IP-Adresse aus die Anrufe getätigt wurden und wann die Anrufe erfolgten. CloudTrail übermittelt Protokolldateien aus allen AWS Regionen an Ihren S3-Bucket , wenn MULTI_REG ION_CLOUD _TRAIL_ENABLED aktiviert ist. Außerdem wird beim AWS Start einer neuen Region derselbe Trail in der neuen Region erstellt. CloudTrail Dadurch erhalten Sie automatis ch Protokolldateien mit API-Aktivitäten für die neue Region.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CM-3.G	CM-3.G Kontrolle von Konfigurationsänderungen	cloudtrail-enabled	AWS CloudTrail kann durch die Aufzeichnung von Aktionen und API-Aufrufen in der AWS Management Console bei der Nichtabstreitbarkeit helfen. Sie können die Benutzer und die Benutzer AWS-Konten , die einen AWS Dienst aufgerufen haben, die Quell-IP-Adresse, über die die Aufrufe generiert wurden, und den Zeitpunkt der Anrufe identifizieren. Einzelheiten zu den erfassten Daten finden Sie unter Inhalt des AWS CloudTrail Datensatzes.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CM-3.G	CM-3.G Kontrolle von Konfigurationsände rungen	multi-region-cloudtrail-enabled	AWS CloudTrail zeichnet Aktionen und API-Aufrufe der AWS Management Console auf. Sie können feststellen, welche Benutzer und Konten angerufen wurden AWS, von welcher Quell-IP-Adresse aus die Anrufe getätigt wurden und wann die Anrufe erfolgten. CloudTrail übermittelt Protokolldateien aus allen AWS Regionen an Ihren S3-Bucket , wenn MULTI_REG ION_CLOUD _TRAIL_ENABLED aktiviert ist. Außerdem wird beim AWS Start einer neuen Region derselbe Trail in der neuen Region erstellt. CloudTrail Dadurch erhalten Sie automatis ch Protokolldateien mit API-Aktivitäten für die neue Region.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CM-5(1)	CM-5(1) Zugriffsbeschränkungen aufgrund von Änderungen | Automatisierte Durchsetzung des Zugriffs/der Prüfung	access-keys-rotated	Die Anmeldeinformationen für autorisierte Geräte, Benutzer und Prozesse werden geprüft, indem sichergestellt wird, dass die IAM-Zugriffsschlüssel entsprechend den Vorgaben der Unternehmensrichtlinie rotiert werden. Das regelmäßige Ändern der Zugriffsschlüssel ist eine bewährte Sicherheitsmethode. Es verkürzt den Zeitraum, in dem ein Zugriffsschlüssel aktiv ist, und reduziert die Auswirkungen auf das Unternehmen, wenn die Schlüssel kompromittiert werden. Diese Regel erfordert einen Wert für die Zugriffsschlüssel-Rotation (Standardkonfiguration: 90). Der tatsächliche Wert muss den Richtlini

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
			en Ihrer Organisation entsprechen.
CCCS-fPBMM-CM-5(1)	CM-5(1) Zugriffsbeschränkungen aufgrund von Änderungen | Automatisierte Durchsetzung des Zugriffs/der Prüfung	api-gw-execution-logging-aktiviert	Die API-Gateway-Protokollierung zeigt detaillierte Ansichten der Benutzer, die auf die API zugegriffen haben, und wie diese Benutzer auf die API zugegriffen haben. Diese Einblicke ermöglichen die Transparenz von Benutzeraktivitäten.
CCCS-fPBMM-CM-5(1)	CM-5(1) Zugriffsbeschränkungen aufgrund von Änderungen | Automatisierte Durchsetzung des Zugriffs/der Prüfung	cloudtrail-s3-dataevents-enabled	Die Erfassung von Simple Storage Service (Amazon S3)-Datenereignissen unterstützt die Erkennung von ungewöhnlichen Aktivitäten. Zu den Details gehören Informationen zu dem AWS -Konto, das auf einen Amazon-S3-Bucket zugegriffen hat, die IP-Adresse und die Uhrzeit des Ereignisses.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CM-5(1)	CM-5(1) Zugriffsbeschränkungen aufgrund von Änderungen | Automatisierte Durchsetzung des Zugriffs/der Prüfung	cloud-trail-cloud-watch-logs-aktiviert	Verwenden Sie Amazon CloudWatch , um Protokoll ereignisaktivitäten zentral zu sammeln und zu verwalten. Die Aufnahme von AWS CloudTrail Daten liefert Einzelheiten zu den API-Aufrufaktivitäten in Ihrem AWS-Konto.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CM-5(1)	CM-5(1) Zugriffsbeschränkungen aufgrund von Änderungen | Automatisierte Durchsetzung des Zugriffs/der Prüfung	cloudtrail-enabled	AWS CloudTrail kann bei der Nichtabstreitbarkeit helfen, indem Aktionen und API-Aufrufe der AWS Management Console aufgezeichnet werden. Sie können die Benutzer und die Benutzer AWS-Konten , die einen AWS Dienst aufgerufen haben, die Quell-IP-Adresse, über die die Aufrufe generiert wurden, und den Zeitpunkt der Anrufe identifizieren. Einzelheiten zu den erfassten Daten finden Sie unter Inhalt des AWS CloudTrail Datensatzes.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CM-5(1)	CM-5(1) Zugriffsbeschränkungen aufgrund von Änderungen | Automatisierte Durchsetzung des Zugriffs/der Prüfung	cloud-trail-log-file-Validierung aktiviert	Verwenden Sie die AWS CloudTrail Protokolldateivalidierung, um die Integrität von Protokollen zu überprüfen. CloudTrail Mithilfe der Protokolldateivalidierung kann festgestellt werden, ob eine Protokolldatei geändert oder gelöscht wurde oder ob sie nach der Übermittlung CloudTrail unverändert geblieben ist. Dieses Feature wurde mit dem Branchenstandard entsprechenden Algorithmen entwickelt: SHA-256 für die Hashfunktion und SHA-256 mit RSA für digitale Signaturen. Aus diesem Grund ist es rechnerisch unmöglich, CloudTrail Protokolldateien unbemerkt zu ändern, zu löschen oder zu fälschen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CM-5(1)	CM-5(1) Zugriffsbeschränkungen aufgrund von Änderungen | Automatisierte Durchsetzung des Zugriffs/der Prüfung	cw-loggroup-retention-period-überprüfen	Stellen Sie sicher, dass die Ereignisprotokolldaten für Ihre Protokollgruppen über eine Mindestdauer aufbewahrt werden, um die Fehlerbehebung und forensische Untersuchungen zu unterstützen. Fehlende frühere Ereignisprotokolldaten erschweren die Rekonstruierung und Identifizierung potenziell schädlicher Ereignisse.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CM-5(1)	CM-5(1) Zugriffsbeschränkungen aufgrund von Änderungen | Automatisierte Durchsetzung des Zugriffs/der Prüfung	ec2-imdsv2-check	Stellen Sie sicher, dass die Methode Instance Metadata Service Version 2 (IMDSv2) aktiviert ist, um den Zugriff auf und die Kontrolle der Amazon Elastic Compute Cloud (Amazon EC2) - Instance-Metadaten zu schützen. Die IMDSv2 Methode verwendet sitzungsbasierte Kontrollen. Mit können Kontrollen implementiert werden IMDSv2, um Änderungen an Instanzmetadaten einzuschränken.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CM-5(1)	CM-5(1) Zugriffsbeschränkungen aufgrund von Änderungen | Automatisierte Durchsetzung des Zugriffs/der Prüfung	ecs-task-definition-user-for-host-mode-check	Wenn für eine Aufgabendefinition erhöhte Berechtigungen gelten, liegt das daran, dass der Kunde diesen Konfigurationen ausdrücklich zugestimmt hat. Diese Kontrolle prüft, ob eine unerwartete Berechtigungseskalation vorliegt, wenn für eine Aufgabendefinition das Host-Netzwerk aktiviert ist, die Kunden aber keine erhöhten Berechtigungen aktiviert haben.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CM-5(1)	CM-5(1) Zugriffsbeschränkungen aufgrund von Änderungen | Automatisierte Durchsetzung des Zugriffs/der Prüfung	elb-logging-enabled	Die Elastic-Load-Balancing-Aktivität ist ein zentraler Kommunikationspunkt innerhalb einer Umgebung. Stellen Sie sicher, dass die ELB-Protokollierung aktiviert ist. Die gesammelten Daten enthalten detaillierte Informationen zu Anfragen, die an den ELB gesendet wurden. Jedes Protokoll enthält Informationen wie die Zeit, zu der die Anforderung einging, die Client-IP-Adresse, Latenzen, Anforderungspfade und Serverantworten.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CM-5(1)	CM-5(1) Zugriffsbeschränkungen aufgrund von Änderungen | Automatisierte Durchsetzung des Zugriffs/der Prüfung	emr-kerberos-enabled	Die Zugriffsberechtigungen und -autorisierungen können verwaltet und nach den Prinzipien der geringsten Berechtigung und Aufgabentrennung integriert werden, indem Kerberos für Amazon-EMR-Cluster aktiviert wird. In Kerberos werden Services und Benutzer, die sich authentifizieren müssen, als Prinzipale bezeichnet. Prinzipale befinden sich in einem Kerberos-Bereich. Innerhalb dieses Bereichs wird ein Kerberos-Server als Key Distribution Center (KDC) bezeichnet. Über diesen Server können sich Prinzipale authentifizieren. Die Authentifizierung im KDC erfolgt durch die Ausstellung von Authentif

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
			izierungstickets. Das KDC unterhält eine Datenbank der Prinzipale in seinem Bereich mit ihren Passwörtern und anderen administr ativen Informationen zu jedem Prinzipal.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CM-5(1)	CM-5(1) Zugriffsbeschränkungen aufgrund von Änderungen | Automatisierte Durchsetzung des Zugriffs/der Prüfung	iam-customer-policy-blocked-kms-Aktionen	AWS Identity and Access Management (IAM) kann Ihnen helfen, die Prinzipien der geringsten Rechte und der Aufgabentrennung in Zugriffsberechtigungen und Autorisierungen zu integrieren und so zu verhindern, dass Richtlinien blockierte Aktionen für alle AWS Schlüssel des Key Management Service enthalten. Wenn Benutzer mehr Rechte haben, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und Aufgabentrennung verstoßen. Mit dieser Regel können Sie den Parameter festlegen. blockedActionsPatterns (Wert „AWS Bewährte grundlegende Sicherheitsmethode

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
			n“: kms: Entschlüs seln, kms:ReEnc ryptFrom). Die tatsächlichen Werte müssen den Richtlini en Ihrer Organisation entsprechen.
CCCS-fPBMM-CM-5(1)	CM-5(1) Zugriffsb eschränkungen aufgrund von Änderungen | Automatisierte Durchsetzung des Zugriffs/der Prüfung	iam-group-has-users-überprüfen	AWS Identity and Access Managemen t (IAM) kann Ihnen helfen, die Prinzipien der geringsten Rechte und der Aufgabent rennung mit Zugriffsb erechtigungen und Autorisierungen zu integrieren, indem sichergestellt wird, dass IAM-Gruppen mindestens einen Benutzer haben. Die Einteilung von Benutzern in Gruppen auf der Grundlage der ihnen zugewiese nen Berechtigungen oder ihrer Funktion ist eine Möglichkeit, das Prinzip der geringste n Berechtigung zu implementieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CM-5(1)	CM-5(1) Zugriffsbeschränkungen aufgrund von Änderungen | Automatisierte Durchsetzung des Zugriffs/der Prüfung	iam-inline-policy-blocked-kms-Aktionen	Stellen Sie sicher, dass ein Benutzer, eine IAM-Rolle oder eine IAM-Gruppe (AWS Identity and Access Management) nicht über eine Inline-Richtlinie verfügt, die blockierte Aktionen für alle AWS Schlüssel des Key Management Service zulässt. AWS empfiehlt, verwaltete Richtlinien anstelle von Inline-Richtlinien zu verwenden. Verwaltete Richtlinien ermöglichen Wiederverwendbarkeit, Versionsverwaltung, Rollback und Delegierung der Berechtigungsverwaltung. Mit dieser Regel können Sie den blockedActionsPatterns Parameter festlegen. (Wert „AWS Bewährte grundlegende Sicherheitsmethoden“: kms:Decrypt, kms:ReEncryptFrom). Die

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
			tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.
CCCS-fPBMM-CM-5(1)	CM-5(1) Zugriffsbeschränkungen aufgrund von Änderungen | Automatisierte Durchsetzung des Zugriffs/der Prüfung	iam-no-inline-policy-überprüfen	Stellen Sie sicher, dass ein Benutzer, eine IAM-Rolle oder eine IAM-Gruppe (AWS Identity and Access Management) nicht über eine Inline-Richtlinie zur Zugriffskontrolle auf Systeme und Ressourcen verfügt. AWS empfiehlt, verwaltete Richtlinien anstelle von Inline-Richtlinien zu verwenden. Verwaltete Richtlinien ermöglichen Wiederverwendbarkeit, Versionsverwaltung, Rollback und Delegierung der Berechtigungsverwaltung.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CM-5(1)	CM-5(1) Zugriffsbeschränkungen aufgrund von Änderungen | Automatisierte Durchsetzung des Zugriffs/der Prüfung	iam-password-policy	Die Identitäten und Anmeldeinformationen werden auf der Grundlage einer organisatorischen IAM-Passwortrichtlinie ausgestellt, verwaltet und verifiziert. Sie erfüllen oder übertreffen die Anforderungen von NIST SP 800-63 und dem Standard „Best Practices“ von AWS Foundational Security für die Passwortstärke. Mit dieser Regel können Sie optional RequireUppercaseCharacters (Wert für AWS grundlegende Sicherheitsbewährte Methoden: wahr), RequireLowercaseCharacters (Wert für bewährte Methoden für AWS grundlegende Sicherheit: wahr), RequireSymbols (Wert für bewährte Methoden für AWS grundlegende Sicherheit:

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
			wahr), RequireNumbers (Wert für bewährte Methoden für AWS grundlegende Sicherheit: wahr), MinimumPasswordLength (Wert für bewährte Methoden für AWS grundlegende Sicherheit: 14), PasswordReusePrevention (Wert für bewährte Methoden für AWS grundlegende Sicherheit: 24) und MaxPasswordAge (Wert für bewährte Methoden für AWS grundlegende Sicherheit: 90) für Ihr IAM festlegen Kennwortrichtlinie. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CM-5(1)	CM-5(1) Zugriffsbeschränkungen aufgrund von Änderungen | Automatisierte Durchsetzung des Zugriffs/der Prüfung	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) kann Ihnen dabei helfen, die Prinzipien der geringsten Rechte und der Aufgabentrennung in Zugriffsberechtigungen und Autorisierungen zu integrieren und so zu verhindern, dass Richtlinien „Effect“: „Allow“ mit „Action“: „*“ anstelle von „Resource“: „*“ enthalten. Wenn Benutzern mehr Rechte eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und der Aufgabentrennung verstoßen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CM-5(1)	CM-5(1) Zugriffsbeschränkungen aufgrund von Änderungen | Automatisierte Durchsetzung des Zugriffs/der Prüfung	iam-root-access-key-überprüfen	Der Zugriff auf Systeme und Ressourcen kann gesteuert werden, indem überprüft wird, ob der Root-Benutzer keine Zugriffsschlüssel mit seiner AWS Identity and Access Management (IAM) -Rolle verknüpft hat. Stellen Sie sicher, dass die Root-Zugriffsschlüssel gelöscht werden. Erstellen und verwenden Sie stattdessen rollenbasierte Funktionen, AWS-Konten um das Prinzip der geringsten Funktionalität zu berücksichtigen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CM-5(1)	CM-5(1) Zugriffsbeschränkungen aufgrund von Änderungen | Automatisierte Durchsetzung des Zugriffs/der Prüfung	iam-user-group-membership-überprüfen	AWS Identity and Access Management (IAM) kann Ihnen helfen, Zugriffsberechtigungen und Autorisierungen einzuschränken, indem sichergestellt wird, dass Benutzer Mitglieder mindestens einer Gruppe sind. Wenn Benutzern mehr Berechtigungen eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und Aufgabentrennung verstoßen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CM-5(1)	CM-5(1) Zugriffsbeschränkungen aufgrund von Änderungen | Automatisierte Durchsetzung des Zugriffs/der Prüfung	iam-user-mfa-enabled	Aktivieren Sie diese Regel, um den Zugriff auf Ressourcen in der AWS -Cloud einzuschränken. Diese Regel stellt sicher, dass die Multi-Faktor-Authentifizierung (MFA) für alle Benutzer aktiviert ist. MFA bietet eine weitere Schutzebene zusätzlich zum Benutzernamen und Passwort. Reduzieren Sie Fälle von kompromittierten Konten, indem Sie MFA für Benutzer vorschreiben.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CM-5(1)	CM-5(1) Zugriffsbeschränkungen aufgrund von Änderungen | Automatisierte Durchsetzung des Zugriffs/der Prüfung	iam-user-no-policies-überprüfen	Diese Regel stellt sicher, dass AWS Identity and Access Management (IAM) -Richtlinien nur Gruppen oder Rollen zugewiesen werden, um den Zugriff auf Systeme und Ressourcen zu kontrollieren. Die Zuweisung von Berechtigungen auf Gruppen- oder Rollenebene trägt dazu bei, die Wahrscheinlichkeit zu verringern, dass eine Identität übermäßige Berechtigungen erhält oder beibehält.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CM-5(1)	CM-5(1) Zugriffsbeschränkungen aufgrund von Änderungen | Automatisierte Durchsetzung des Zugriffs/der Prüfung	iam-user-unused-credentials-überprüfen	AWS Identity and Access Management (IAM) kann Ihnen bei Zugriffsberechtigungen und Autorisierungen helfen, indem es nach IAM-Passwörtern und Zugriffsschlüsseln sucht, die für einen bestimmten Zeitraum nicht verwendet wurden. Wenn ungenutzte Anmeldeinformationen identifiziert werden, müssen Sie sie deaktivieren und/oder entfernen, da dies gegen das Prinzip der geringsten Berechtigung verstoßen könnte. Für diese Regel müssen Sie einen Wert für das maxCredentialUsage Alter festlegen (Standardkonfiguration: 90). Der tatsächliche Wert muss den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CM-5(1)	CM-5(1) Zugriffsbeschränkungen aufgrund von Änderungen | Automatisierte Durchsetzung des Zugriffs/der Prüfung	mfa-enabled-for-iam-Konsolenzugriff	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass MFA für alle AWS Identity and Access Management (IAM) -Benutzer aktiviert ist, die über ein Konsolenkennwort verfügen. MFA sorgt für eine weitere Schutzebene zusätzlich zu den Anmeldeinformationen. Indem Sie MFA für Benutzer vorschreiben, können Sie Fälle kompromittierter Konten reduzieren und verhindern, dass unbefugte Benutzer auf vertrauliche Daten zugreifen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CM-5(1)	CM-5(1) Zugriffsbeschränkungen aufgrund von Änderungen | Automatisierte Durchsetzung des Zugriffs/der Prüfung	multi-region-cloudtrail-enabled	AWS CloudTrail zeichnet Aktionen und API-Aufrufe der AWS Management Console auf. Sie können feststellen, welche Benutzer und Konten angerufen wurden AWS, von welcher Quell-IP-Adresse aus die Anrufe getätigt wurden und wann die Anrufe erfolgten. CloudTrail übermittelt Protokolldateien aus allen AWS Regionen an Ihren S3-Bucket , wenn MULTI_REGION_CLOUD_TRAIL_ENABLED aktiviert ist. Außerdem wird beim AWS Start einer neuen Region derselbe Trail in der neuen Region erstellt. CloudTrail Dadurch erhalten Sie automatisch Protokolldateien mit API-Aktivitäten für die neue Region.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CM-5(1)	CM-5(1) Zugriffsbeschränkungen aufgrund von Änderungen | Automatisierte Durchsetzung des Zugriffs/der Prüfung	rds-logging-enabled	Um die Protokollierung und Überwachung in Ihrer Umgebung zu erleichtern, stellen Sie sicher, dass die Amazon Relational Database Service (Amazon RDS)-Protokollierung aktiviert ist. Mit der Amazon-RDS-Protokollierung können Sie Ereignisse wie Verbindungen, Verbindungsabbrüche, Abfragen oder abgefragte Tabellen erfassen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CM-5(1)	CM-5(1) Zugriffsbeschränkungen aufgrund von Änderungen | Automatisierte Durchsetzung des Zugriffs/der Prüfung	redshift-cluster-configuration-check	Um Daten im Ruhezustand zu schützen, muss die Verschlüsselung für Ihre Amazon-Redshift-Cluster aktiviert sein. Sie müssen auch sicherstellen, dass die erforderlichen Konfigurationen auf Amazon-Redshift-Clustern bereitgestellt werden. Die Prüfungsprotokollierung muss aktiviert sein, um Informationen zu Verbindungen und Benutzeraktivitäten in der Datenbank bereitzustellen. Diese Regel erfordert, dass ein Wert für clusterDbEncrypted (Config Default: TRUE) und LoggingEnabled (Config Default: TRUE) gesetzt ist. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CM-5(1)	CM-5(1) Zugriffsbeschränkungen aufgrund von Änderungen | Automatisierte Durchsetzung des Zugriffs/der Prüfung	root-account-mfa-enabled	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass MFA für den Root-Benutzer aktiviert ist. Der Stammbenutzer ist der AWS-Konto-Benutzer mit den meisten Berechtigungen. MFA bietet eine weitere Schutzebene zusätzlich zum Benutzernamen und Passwort. Indem Sie MFA für den Root-Benutzer vorschreiben, können Sie die Anzahl AWS-Konten kompromittierter Benutzer reduzieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CM-5(1)	CM-5(1) Zugriffsbeschränkungen aufgrund von Änderungen | Automatisierte Durchsetzung des Zugriffs/der Prüfung	s-3 bucket-logging-enabled	Die Amazon Simple Storage Service (Amazon S3)-Serverzugriffsprotokollierung bietet eine Methode zur Überwachung des Netzwerks im Hinblick auf potenzielle Cybersicherheitsereignisse. Die Ereignisse werden überwacht, indem detaillierte Aufzeichnungen über die Anfragen erfasst werden, die an einen Amazon-S3-Bucket gestellt wurden. Jeder Zugriffsprotokolleintrag enthält Details zu einer einzelnen Zugriffsanfrage. Zu den Details gehören Auftraggeber, Bucket-Name, Anforderungszeit, Anforderungsaktion, Antwortstatus und Fehlercode, falls relevant.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CM-5(1)	CM-5(1) Zugriffsbeschränkungen aufgrund von Änderungen | Automatisierte Durchsetzung des Zugriffs/der Prüfung	secretsmanager-rotation-enabled-check	Diese Regel stellt sicher, dass bei AWS Secrets Manager Manager-Geheimnissen die Rotation aktiviert ist. Die regelmäßige Rotation von Secrets kann den Zeitraum verkürzen, in dem ein Secret aktiv ist, und möglicher weise die Auswirkungen auf das Geschäft verringern, falls das Secret kompromittiert wird.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CM-5(1)	CM-5(1) Zugriffsbeschränkungen aufgrund von Änderungen | Automatisierte Durchsetzung des Zugriffs/der Prüfung	secretsmanager-scheduled-rotation-success-überprüfen	Diese Regel stellt sicher, dass AWS Secrets Manager Manager-Geheimnisse gemäß dem Rotationsplan erfolgreich rotiert wurden. Die regelmäßige Rotation von Secrets kann den Zeitraum verkürzen, in dem ein Secret aktiv ist, und möglicherweise die Auswirkungen auf das Unternehmen verringern, falls es kompromittiert wird.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CM-5(1)	CM-5(1) Zugriffsbeschränkungen aufgrund von Änderungen | Automatisierte Durchsetzung des Zugriffs/der Prüfung	vpc-flow-logs-enabled	VPC-Flow-Protokolle erfassen detaillierte Informationsdatensätze über den IP-Datenverkehr, der zu und von Netzwerkschnittstellen in Ihrer Amazon Virtual Private Cloud (Amazon VPC) fließt. Standardmäßig enthalten Flow-Protokolldatensätze Werte für die verschiedenen Komponenten des IP-Flows, einschließlich Quelle, Ziel und Protokoll.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CM-5(1)	CM-5(1) Zugriffsbeschränkungen aufgrund von Änderungen | Automatisierte Durchsetzung des Zugriffs/der Prüfung	wafv2-logging-enabled	Um die Protokollierung und Überwachung in Ihrer Umgebung zu erleichtern, aktivieren Sie die AWS WAF (V2) -Protokollierung im regionalen und globalen Web ACLs. AWS Die WAF-Protokollierung bietet detaillierte Informationen über den Datenverkehr, der von Ihrer Web-ACL analysiert wird. In den Protokollen werden die Uhrzeit aufgezeichnet, zu der die AWS WAF die Anfrage von Ihrer AWS Ressource erhalten hat, Informationen zu der Anfrage und eine Aktion für die Regel, der jede Anfrage entsprach.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CM-5(5)	CM-5(5) Zugriffsbeschränkungen aufgrund von Änderungen | Einschränkung der Produktions- und Betriebsrechte	backup-recovery-point-manual-Löschen-deaktiviert	Stellen Sie sicher, dass Ihren AWS Backup-Wiederherstellungspunkten eine ressourcenbasierte Richtlinie zugeordnet ist, die das Löschen von Wiederherstellungspunkten verhindert. Die Verwendung einer ressourcenbasierten Richtlinie zur Verhinderung des Löschens von Wiederherstellungspunkten kann dazu beitragen, ein versehentliches oder absichtliches Löschen zu unterbinden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CM-5(5)	CM-5(5) Zugriffsbeschränkungen aufgrund von Änderungen | Einschränkung der Produktions- und Betriebsrechte	ec2-imdsv2-check	Stellen Sie sicher, dass die Methode Instance Metadata Service Version 2 (IMDSv2) aktiviert ist, um den Zugriff auf und die Kontrolle der Amazon Elastic Compute Cloud (Amazon EC2) - Instance-Metadaten zu schützen. Die IMDSv2 Methode verwendet sitzungsbasierte Kontrollen. Mit können Kontrollen implementiert werden IMDSv2, um Änderungen an Instanzmetadaten einzuschränken.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CM-5(5)	CM-5(5) Zugriffsbeschränkungen aufgrund von Änderungen | Einschränkung der Produktions- und Betriebsrechte	ecs-task-definition-user-for-host-mode-check	Wenn für eine Aufgabendefinition erhöhte Berechtigungen gelten, liegt das daran, dass der Kunde diesen Konfigurationen ausdrücklich zugestimmt hat. Diese Kontrolle prüft, ob eine unerwartete Berechtigungseskalation vorliegt, wenn für eine Aufgabendefinition das Host-Netzwerk aktiviert ist, die Kunden aber keine erhöhten Berechtigungen aktiviert haben.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CM-5(5)	CM-5(5) Zugriffsbeschränkungen aufgrund von Änderungen | Einschränkung der Produktions- und Betriebsrechte	emr-kerberos-enabled	Die Zugriffsberechtigungen und -autorisierungen können verwaltet und nach den Prinzipien der geringsten Berechtigung und Aufgabentrennung integriert werden, indem Kerberos für Amazon-EMR-Cluster aktiviert wird. In Kerberos werden Services und Benutzer, die sich authentifizieren müssen, als Prinzipale bezeichnet. Prinzipale befinden sich in einem Kerberos-Bereich. Innerhalb dieses Bereichs wird ein Kerberos-Server als Key Distribution Center (KDC) bezeichnet. Über diesen Server können sich Prinzipale authentifizieren. Die Authentifizierung im KDC erfolgt durch die Ausstellung von Authentif

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
			izierungstickets. Das KDC unterhält eine Datenbank der Prinzipale in seinem Bereich mit ihren Passwörtern und anderen administr ativen Informationen zu jedem Prinzipal.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CM-5(5)	CM-5(5) Zugriffsbeschränkungen aufgrund von Änderungen | Einschränkung der Produktions- und Betriebsrechte	iam-customer-policy-blocked-kms-Aktionen	AWS Identity and Access Management (IAM) kann Ihnen helfen, die Prinzipien der geringsten Rechte und der Aufgabentrennung in Zugriffsberechtigungen und Autorisierungen zu integrieren und so zu verhindern, dass Richtlinien blockierte Aktionen für alle AWS Schlüssel des Key Management Service enthalten. Wenn Benutzer mehr Rechte haben, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und Aufgabentrennung verstoßen. Mit dieser Regel können Sie den Parameter festlegen. blockedActionsPatterns (Wert „AWS Bewährte grundlegende Sicherheitsmethode

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
			n“: kms: Entschlüs seln, kms:ReEnc ryptFrom). Die tatsächlichen Werte müssen den Richtlini en Ihrer Organisation entsprechen.
CCCS-fPBMM-CM-5(5)	CM-5(5) Zugriffsb eschränkungen aufgrund von Änderungen | Einschränkung der Produktions- und Betriebsrechte	iam-group-has-users-überprüfen	AWS Identity and Access Managemen t (IAM) kann Ihnen helfen, die Prinzipien der geringsten Rechte und der Aufgabent rennung mit Zugriffsb erechtigungen und Autorisierungen zu integrieren, indem sichergestellt wird, dass IAM-Gruppen mindestens einen Benutzer haben. Die Einteilung von Benutzern in Gruppen auf der Grundlage der ihnen zugewiese nen Berechtigungen oder ihrer Funktion ist eine Möglichkeit, das Prinzip der geringste n Berechtigung zu implementieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CM-5(5)	CM-5(5) Zugriffsbeschränkungen aufgrund von Änderungen | Einschränkung der Produktions- und Betriebsrechte	iam-inline-policy-blocked-kms-Aktionen	Stellen Sie sicher, dass ein Benutzer, eine IAM-Rolle oder eine IAM-Gruppe (AWS Identity and Access Management) nicht über eine Inline-Richtlinie verfügt, die blockierte Aktionen für alle AWS Schlüssel des Key Management Service zulässt. AWS empfiehlt, verwaltete Richtlinien anstelle von Inline-Richtlinien zu verwenden. Verwaltete Richtlinien ermöglichen Wiederverwendbarkeit, Versionsverwaltung, Rollback und Delegierung der Berechtigungsverwaltung. Mit dieser Regel können Sie den blockedActionsPatterns Parameter festlegen. (Wert „AWS Bewährte grundlegende Sicherheitsmethoden“: kms:Decrypt, kms:ReEncryptFrom). Die

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
			tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.
CCCS-fPBMM-CM-5(5)	CM-5(5) Zugriffsbeschränkungen aufgrund von Änderungen | Einschränkung der Produktions- und Betriebsrechte	iam-no-inline-policy-überprüfen	Stellen Sie sicher, dass ein Benutzer, eine IAM-Rolle oder eine IAM-Gruppe (AWS Identity and Access Management) nicht über eine Inline-Richtlinie zur Zugriffskontrolle auf Systeme und Ressourcen verfügt. AWS empfiehlt, verwaltete Richtlinien anstelle von Inline-Richtlinien zu verwenden. Verwaltete Richtlinien ermöglichen Wiederverwendbarkeit, Versionsverwaltung, Rollback und Delegierung der Berechtigungsverwaltung.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CM-5(5)	CM-5(5) Zugriffsbeschränkungen aufgrund von Änderungen | Einschränkung der Produktions- und Betriebsrechte	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) kann Ihnen dabei helfen, die Prinzipien der geringsten Rechte und der Aufgabentrennung in Zugriffsberechtigungen und Autorisierungen zu integrieren und so zu verhindern, dass Richtlinien „Effect“: „Allow“ mit „Action“: „*“ anstelle von „Resource“: „*“ enthalten. Wenn Benutzern mehr Rechte eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und der Aufgabentrennung verstoßen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CM-5(5)	CM-5(5) Zugriffsbeschränkungen aufgrund von Änderungen | Einschränkung der Produktions- und Betriebsrechte	iam-root-access-key-überprüfen	Der Zugriff auf Systeme und Ressourcen kann gesteuert werden, indem überprüft wird, ob der Root-Benutzer keine Zugriffsschlüssel mit seiner AWS Identity and Access Management (IAM) -Rolle verknüpft hat. Stellen Sie sicher, dass die Root-Zugriffsschlüssel gelöscht werden. Erstellen und verwenden Sie stattdessen rollenbasierte Funktionen, AWS-Konten um das Prinzip der geringsten Funktionalität zu berücksichtigen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CM-5(5)	CM-5(5) Zugriffsbeschränkungen aufgrund von Änderungen | Einschränkung der Produktions- und Betriebsrechte	iam-user-group-membership-überprüfen	AWS Identity and Access Management (IAM) kann Ihnen helfen, Zugriffsberechtigungen und Autorisierungen einzuschränken, indem sichergestellt wird, dass Benutzer Mitglieder mindestens einer Gruppe sind. Wenn Benutzern mehr Berechtigungen eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und Aufgabentrennung verstoßen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CM-5(5)	CM-5(5) Zugriffsbeschränkungen aufgrund von Änderungen | Einschränkung der Produktions- und Betriebsrechte	iam-user-no-policies-überprüfen	Diese Regel stellt sicher, dass AWS Identity and Access Management (IAM) -Richtlinien nur Gruppen oder Rollen zugewiesen werden, um den Zugriff auf Systeme und Ressourcen zu kontrollieren. Die Zuweisung von Berechtigungen auf Gruppen- oder Rollenebene trägt dazu bei, die Wahrscheinlichkeit zu verringern, dass eine Identität übermäßige Berechtigungen erhält oder beibehält.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CM-5(5)	CM-5(5) Zugriffsbeschränkungen aufgrund von Änderungen | Einschränkung der Produktions- und Betriebsrechte	iam-user-unused-credentials-überprüfen	AWS Identity and Access Management (IAM) kann Ihnen bei Zugriffsberechtigungen und Autorisierungen helfen, indem es nach IAM-Passwörtern und Zugriffsschlüsseln sucht, die für einen bestimmten Zeitraum nicht verwendet wurden. Wenn ungenutzte Anmeldeinformationen identifiziert werden, müssen Sie sie deaktivieren und/oder entfernen, da dies gegen das Prinzip der geringsten Berechtigung verstoßen könnte. Für diese Regel müssen Sie einen Wert für das maxCredentialUsage Alter festlegen (Standardkonfiguration: 90). Der tatsächliche Wert muss den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CM-5.A	CM-5.A Zugriffsbeschränkungen aufgrund von Änderungen	backup-recovery-point-manual-löschen-deaktiviert	Stellen Sie sicher, dass Ihren AWS Backup-Wiederherstellungspunkten eine ressourcenbasierte Richtlinie zugeordnet ist, die das Löschen von Wiederherstellungspunkten verhindert. Die Verwendung einer ressourcenbasierten Richtlinie zur Verhinderung des Löschens von Wiederherstellungspunkten kann dazu beitragen, ein versehentliches oder absichtliches Löschen zu unterbinden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CM-5.A	CM-5.A Zugriffsbeschränkungen aufgrund von Änderungen	ec2-imdsv2-check	Stellen Sie sicher, dass die Methode Instance Metadata Service Version 2 (IMDSv2) aktiviert ist, um den Zugriff auf und die Kontrolle der Amazon Elastic Compute Cloud (Amazon EC2) - Instance-Metadaten zu schützen. Die IMDSv2 Methode verwendet sitzungsbasierte Kontrollen. Mit können Kontrollen implementiert werden IMDSv2, um Änderungen an Instanzmetadaten einzuschränken.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CM-5.A	CM-5.A Zugriffsbeschränkungen aufgrund von Änderungen	ecs-task-definition-user-for-host-mode-check	Wenn für eine Aufgabendefinition erhöhte Berechtigungen gelten, liegt das daran, dass der Kunde diesen Konfigurationen ausdrücklich zugestimmt hat. Diese Kontrolle prüft, ob eine unerwartete Berechtigungseskalation vorliegt, wenn für eine Aufgabendefinition das Host-Netzwerk aktiviert ist, die Kunden aber keine erhöhten Berechtigungen aktiviert haben.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CM-5.A	CM-5.A Zugriffsbeschränkungen aufgrund von Änderungen	emr-kerberos-enabled	Die Zugriffsberechtigungen und -autorisierungen können verwaltet und nach den Prinzipien der geringsten Berechtigung und Aufgabentrennung integriert werden, indem Kerberos für Amazon-EMR-Cluster aktiviert wird. In Kerberos werden Services und Benutzer, die sich authentifizieren müssen, als Prinzipale bezeichnet. Prinzipale befinden sich in einem Kerberos-Bereich. Innerhalb dieses Bereichs wird ein Kerberos-Server als Key Distribution Center (KDC) bezeichnet. Über diesen Server können sich Prinzipale authentifizieren. Die Authentifizierung im KDC erfolgt durch die Ausstellung von Authentif

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
			izierungstickets. Das KDC unterhält eine Datenbank der Prinzipale in seinem Bereich mit ihren Passwörtern und anderen administr ativen Informationen zu jedem Prinzipal.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CM-5.A	CM-5.A Zugriffsbeschränkungen aufgrund von Änderungen	iam-customer-policy-blocked-kms-Aktionen	AWS Identity and Access Management (IAM) kann Ihnen helfen, die Prinzipien der geringsten Rechte und der Aufgabentrennung in Zugriffsberechtigungen und Autorisierungen zu integrieren und so zu verhindern, dass Richtlinien blockierte Aktionen für alle AWS Schlüssel des Key Management Service enthalten. Wenn Benutzer mehr Rechte haben, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und Aufgabentrennung verstoßen. Mit dieser Regel können Sie den Parameter festlegen. blockedActionsPatterns (Wert „AWS Bewährte grundlegende Sicherheitsmethode

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
			n“: kms: Entschlüs seln, kms:ReEnc ryptFrom). Die tatsächlichen Werte müssen den Richtlini en Ihrer Organisation entsprechen.
CCCS-fPBMM-CM-5.A	CM-5.A Zugriffsb eschränkungen aufgrund von Änderungen	iam-group-has-users-überprüfen	AWS Identity and Access Managemen t (IAM) kann Ihnen helfen, die Prinzipien der geringsten Rechte und der Aufgabent rennung mit Zugriffsb erechtigungen und Autorisierungen zu integrieren, indem sichergestellt wird, dass IAM-Gruppen mindestens einen Benutzer haben. Die Einteilung von Benutzern in Gruppen auf der Grundlage der ihnen zugewiese nen Berechtigungen oder ihrer Funktion ist eine Möglichkeit, das Prinzip der geringste n Berechtigung zu implementieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CM-5.A	CM-5.A Zugriffsbeschränkungen aufgrund von Änderungen	iam-inline-policy-blocked-kms-Aktionen	Stellen Sie sicher, dass ein Benutzer, eine IAM-Rolle oder eine IAM-Gruppe (AWS Identity and Access Management) nicht über eine Inline-Richtlinie verfügt, die blockierte Aktionen für alle AWS Schlüssel des Key Management Service zulässt. AWS empfiehlt, verwaltete Richtlinien anstelle von Inline-Richtlinien zu verwenden. Verwaltete Richtlinien ermöglichen Wiederverwendbarkeit, Versionsverwaltung, Rollback und Delegierung der Berechtigungsverwaltung. Mit dieser Regel können Sie den blockedActionsPatterns Parameter festlegen. (Wert „AWS Bewährte grundlegende Sicherheitsmethoden“: kms:Decrypt, kms:ReEncryptFrom). Die

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
			tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.
CCCS-fPBMM-CM-5.A	CM-5.A Zugriffsbeschränkungen aufgrund von Änderungen	iam-no-inline-policy-überprüfen	Stellen Sie sicher, dass ein Benutzer, eine IAM-Rolle oder eine IAM-Gruppe (AWS Identity and Access Management) nicht über eine Inline-Richtlinie zur Zugriffskontrolle auf Systeme und Ressourcen verfügt. AWS empfiehlt, verwaltete Richtlinien anstelle von Inline-Richtlinien zu verwenden. Verwaltete Richtlinien ermöglichen Wiederverwendbarkeit, Versionsverwaltung, Rollback und Delegierung der Berechtigungsverwaltung.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CM-5.A	CM-5.A Zugriffsbeschränkungen aufgrund von Änderungen	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) kann Ihnen dabei helfen, die Prinzipien der geringsten Rechte und der Aufgabentrennung in Zugriffsberechtigungen und Autorisierungen zu integrieren und so zu verhindern, dass Richtlinien „Effect“: „Allow“ mit „Action“: „*“ anstelle von „Resource“: „*“ enthalten. Wenn Benutzern mehr Rechte eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und der Aufgabentrennung verstoßen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CM-5.A	CM-5.A Zugriffsbeschränkungen aufgrund von Änderungen	iam-root-access-key-überprüfen	Der Zugriff auf Systeme und Ressourcen kann gesteuert werden, indem überprüft wird, ob der Root-Benutzer keine Zugriffsschlüssel mit seiner AWS Identity and Access Management (IAM) -Rolle verknüpft hat. Stellen Sie sicher, dass die Root-Zugriffsschlüssel gelöscht werden. Erstellen und verwenden Sie stattdessen rollenbasierte Funktionen, AWS-Konten um das Prinzip der geringsten Funktionalität zu berücksichtigen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CM-5.A	CM-5.A Zugriffsbeschränkungen aufgrund von Änderungen	iam-user-group-membership-überprüfen	AWS Identity and Access Management (IAM) kann Ihnen helfen, Zugriffsberechtigungen und Autorisierungen einzuschränken, indem sichergestellt wird, dass Benutzer Mitglieder mindestens einer Gruppe sind. Wenn Benutzern mehr Berechtigungen eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und Aufgabentrennung verstoßen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CM-5.A	CM-5.A Zugriffsbeschränkungen aufgrund von Änderungen	iam-user-no-policies-überprüfen	Diese Regel stellt sicher, dass AWS Identity and Access Management (IAM) -Richtlinien nur Gruppen oder Rollen zugewiesen werden, um den Zugriff auf Systeme und Ressourcen zu kontrollieren. Die Zuweisung von Berechtigungen auf Gruppen- oder Rollenebene trägt dazu bei, die Wahrscheinlichkeit zu verringern, dass eine Identität übermäßige Berechtigungen erhält oder beibehält.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CM-5.A	CM-5.A Zugriffsbeschränkungen aufgrund von Änderungen	iam-user-unused-credentials-überprüfen	AWS Identity and Access Management (IAM) kann Ihnen bei Zugriffsberechtigungen und Autorisierungen helfen, indem es nach IAM-Passwörtern und Zugriffsschlüsseln sucht, die für einen bestimmten Zeitraum nicht verwendet wurden. Wenn ungenutzte Anmeldeinformationen identifiziert werden, müssen Sie sie deaktivieren und/oder entfernen, da dies gegen das Prinzip der geringsten Berechtigung verstoßen könnte. Für diese Regel müssen Sie einen Wert für das maxCredentialUsage Alter festlegen (Standardkonfiguration: 90). Der tatsächliche Wert muss den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CM-6(1)	CM-6(1) Konfigurationseinstellungen | Automatisierte zentrale Verwaltung/Anwendung/Überprüfung	ec2-manager instance-managed-by-systems	Eine Bestandsaufnahme der Softwareplattformen und Anwendungen innerhalb des Unternehmens ist möglich, indem Amazon Elastic Compute Cloud (Amazon EC2) - Instances mit AWS Systems Manager verwaltet werden. Verwenden Sie AWS Systems Manager, um detaillierte Systemkonfigurationen, Betriebssystem-Patch-Levels, Namen und Typ der Dienste, Softwareinstallationen, Anwendungsname, Herausgeber und Version sowie andere Details zu Ihrer Umgebung bereitzustellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CM-6(1)	CM-6(1) Konfigurationseinstellungen | Automatisierte zentrale Verwaltung/Anwendung/Überprüfung	ec2-check managedinstance-association-compliance-status	Verwenden Sie AWS Systems Manager Associations, um bei der Inventarisierung von Softwareplattformen und Anwendungen innerhalb eines Unternehmens zu helfen. AWS Systems Manager weist Ihren verwalteten Instances einen Konfigurationsstatus zu und ermöglicht es Ihnen, Basiswerte für Betriebssystem-Patch-Levels, Softwareinstallationen, Anwendungskonfigurationen und andere Details zu Ihrer Umgebung festzulegen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CM-6(1)	CM-6(1) Konfigurationseinstellungen | Automatisierte zentrale Verwaltung/Anwendung/Überprüfung	ec2-prüfen managedinstance-patch-compliance-status	Aktivieren Sie diese Regel, um bei der Identifizierung und Dokumentation von Sicherheitslücken in Amazon Elastic Compute Cloud (Amazon EC2) zu helfen. Die Regel prüft, ob die EC2 Amazon-Instance die Patch-Konformität im AWS Systems Manager gemäß den Richtlinien und Verfahren Ihrer Organisation einhält.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CM-6.A	CM-6.A Konfigurationseinstellungen	access-keys-rotated	Die Anmeldeinformationen für autorisierte Geräte, Benutzer und Prozesse werden geprüft, indem sichergestellt wird, dass die IAM-Zugriffsschlüssel gemäß den Vorgaben der Unternehmensrichtlinie rotiert werden. Das regelmäßige Ändern der Zugriffsschlüssel ist eine bewährte Sicherheitsmethode. Es verkürzt den Zeitraum, in dem ein Zugriffsschlüssel aktiv ist, und reduziert die Auswirkungen auf das Unternehmen, wenn die Schlüssel kompromittiert werden. Diese Regel erfordert einen Wert für die Zugriffsschlüssel-Rotation (Standard konfiguration: 90). Der tatsächliche Wert muss den Richtlini

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
			en Ihrer Organisation entsprechen.
CCCS-fPBMM-CM-6.A	CM-6.A Konfigurationseinstellungen	autoscaling-group-elb-healthcheck-erforderlich	Die Elastic Load Balancer (ELB) - Zustandsprüfungen für Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling Scaling-Gruppen unterstützen die Aufrechterhaltung einer angemessenen Kapazität und Verfügbarkeit. Der Load Balancer sendet regelmäßig Pings, versucht Verbindungen herzustellen oder sendet Anfragen, um den Zustand der EC2 Amazon-Instances in einer Gruppe mit auto-scaling zu testen. Wenn eine Instance nicht zurückmeldet, wird der Traffic an eine neue EC2 Amazon-Instance gesendet.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CM-6.A	CM-6.A Konfigurationseinstellungen	cloudtrail-s3-dataevents-enabled	Die Erfassung von Simple Storage Service (Amazon S3)-Datenereignissen unterstützt die Erkennung von ungewöhnlichen Aktivitäten. Zu den Details gehören Informationen zu dem AWS -Konto, das auf einen Amazon-S3-Bucket zugegriffen hat, die IP-Adresse und die Uhrzeit des Ereignisses.
CCCS-fPBMM-CM-6.A	CM-6.A Konfigurationseinstellungen	cloud-trail-cloud-watch-logs-aktiviert	Verwenden Sie Amazon CloudWatch , um Protokoll ereignisaktivitäten zentral zu sammeln und zu verwalten. Die Aufnahme von AWS CloudTrail Daten liefert Einzelheiten zu den API-Aufrufaktivitäten in Ihrem AWS-Konto.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CM-6.A	CM-6.A Konfigurationseinstellungen	cloud-trail-encryption-enabled	Zum Schutz von eventuell vorhandenen sensiblen Daten sowie Daten im Ruhezustand müssen Sie sicherstellen, dass die Verschlüsselung für Ihre AWS CloudTrail aktiviert ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CM-6.A	CM-6.A Konfigurationseinstellungen	cloud-trail-log-file-Validierung aktiviert	Verwenden Sie die AWS CloudTrail Protokolldateivalidierung, um die Integrität von Protokollen zu überprüfen. CloudTrail Mithilfe der Protokolldateivalidierung kann festgestellt werden, ob eine Protokolldatei geändert oder gelöscht wurde oder ob sie nach der Übermittlung CloudTrail unverändert geblieben ist. Dieses Feature wurde mit dem Branchenstandard entsprechenden Algorithmen entwickelt: SHA-256 für die Hashfunktion und SHA-256 mit RSA für digitale Signaturen. Aus diesem Grund ist es rechnerisch unmöglich, CloudTrail Protokolldateien unbemerkt zu ändern, zu löschen oder zu fälschen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CM-6.A	CM-6.A Konfigurationseinstellungen	cmk-backing-key-rotation-aktiviert	Aktivieren Sie die Schlüsselrotation, um sicherzustellen, dass Schlüssel rotiert werden, sobald sie das Ende ihrer Kryptoperiode erreicht haben.
CCCS-fPBMM-CM-6.A	CM-6.A Konfigurationseinstellungen	ec2- ebs-encryption-by-default	Zum Schutz von Daten im Ruhezustand müssen Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon Elastic Block Store (Amazon EBS)-Volumes aktiviert ist. Aktivieren Sie die Verschlüsselung von Daten im Ruhezustand, um eventuell in diesen Volumes vorhandene sensible Daten im Ruhezustand zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CM-6.A	CM-6.A Konfigurationseinstellungen	encrypted-volumes	Aktivieren Sie die Verschlüsselung für Ihre Volumes von Amazon Elastic Block Store (Amazon EBS), um eventuell vorhandene sensible Daten sowie Daten im Ruhezustand zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CM-6.A	CM-6.A Konfigurationseinstellungen	iam-no-inline-policy-überprüfen	Stellen Sie sicher, dass ein Benutzer, eine IAM-Rolle oder eine IAM-Gruppe (AWS Identity and Access Management) nicht über eine Inline-Richtlinie zur Zugriffskontrolle auf Systeme und Ressourcen verfügt. AWS empfiehlt, verwaltete Richtlinien anstelle von Inline-Richtlinien zu verwenden. Verwaltete Richtlinien ermöglichen Wiederverwendbarkeit, Versionsverwaltung, Rollback und Delegierung der Berechtigungsverwaltung.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CM-6.A	CM-6.A Konfigurationseinstellungen	iam-password-policy	Die Identitäten und Anmeldeinformationen werden auf der Grundlage einer organisatorischen IAM-Passwortrichtlinie ausgestellt, verwaltet und verifiziert. Sie erfüllen oder übertreffen die Anforderungen von NIST SP 800-63 und dem Standard „Best Practices“ von AWS Foundational Security für die Passwortstärke. Mit dieser Regel können Sie optional RequireUppercaseCharacters (Wert für AWS grundlegende Sicherheitsbewährte Methoden: wahr), RequireLowercaseCharacters (Wert für bewährte Methoden für AWS grundlegende Sicherheit: wahr), RequireSymbols (Wert für bewährte Methoden für AWS grundlegende Sicherheit:

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
			wahr), RequireNumbers (Wert für bewährte Methoden für AWS grundlegende Sicherheit: wahr), MinimumPasswordLength (Wert für bewährte Methoden für AWS grundlegende Sicherheit: 14), PasswordReusePrevention (Wert für bewährte Methoden für AWS grundlegende Sicherheit: 24) und MaxPasswordAge (Wert für bewährte Methoden für AWS grundlegende Sicherheit: 90) für Ihr IAM festlegen Kennwortrichtlinie. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CM-6.A	CM-6.A Konfigurationseinstellungen	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) kann Ihnen dabei helfen, die Prinzipien der geringsten Rechte und der Aufgabentrennung in Zugriffsberechtigungen und Autorisierungen zu integrieren und so zu verhindern, dass Richtlinien „Effect“: „Allow“ mit „Action“: „*“ anstelle von „Resource“: „*“ enthalten. Wenn Benutzern mehr Rechte eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und der Aufgabentrennung verstoßen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CM-6.A	CM-6.A Konfigurationseinstellungen	iam-root-access-key-überprüfen	Der Zugriff auf Systeme und Ressourcen kann gesteuert werden, indem überprüft wird, ob der Root-Benutzer keine Zugriffsschlüssel mit seiner AWS Identity and Access Management (IAM) -Rolle verknüpft hat. Stellen Sie sicher, dass die Root-Zugriffsschlüssel gelöscht werden. Erstellen und verwenden Sie stattdessen rollenbasierte Funktionen, AWS-Konten um das Prinzip der geringsten Funktionalität zu berücksichtigen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CM-6.A	CM-6.A Konfigurationseinstellungen	iam-user-group-membership-überprüfen	AWS Identity and Access Management (IAM) kann Ihnen helfen, Zugriffsberechtigungen und Autorisierungen einzuschränken, indem sichergestellt wird, dass Benutzer Mitglieder mindestens einer Gruppe sind. Wenn Benutzern mehr Berechtigungen eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und Aufgabentrennung verstoßen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CM-6.A	CM-6.A Konfigurationseinstellungen	iam-user-no-policies-überprüfen	Diese Regel stellt sicher, dass AWS Identity and Access Management (IAM) -Richtlinien nur Gruppen oder Rollen zugewiesen werden, um den Zugriff auf Systeme und Ressourcen zu kontrollieren. Die Zuweisung von Berechtigungen auf Gruppen- oder Rollenebene trägt dazu bei, die Wahrscheinlichkeit zu verringern, dass eine Identität übermäßige Berechtigungen erhält oder beibehält.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CM-6.A	CM-6.A Konfigurationseinstellungen	iam-user-unused-credentials-überprüfen	AWS Identity and Access Management (IAM) kann Ihnen bei Zugriffsberechtigungen und Autorisierungen helfen, indem es nach IAM-Passwörtern und Zugriffsschlüsseln sucht, die für einen bestimmten Zeitraum nicht verwendet wurden. Wenn ungenutzte Anmeldeinformationen identifiziert werden, müssen Sie sie deaktivieren und/oder entfernen, da dies gegen das Prinzip der geringsten Berechtigung verstoßen könnte. Für diese Regel müssen Sie einen Wert für das maxCredentialUsage Alter festlegen (Standardkonfiguration: 90). Der tatsächliche Wert muss den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CM-6.A	CM-6.A Konfigurationseinstellungen	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) Security Groups können bei der Verwaltung des Netzwerkzugriffs helfen, indem sie eine statusbehaftete Filterung des ein- und ausgehenden Netzwerkverkehrs zu Ressourcen bereitstellen. AWS Wenn Sie eingehenden (oder entfernten) Datenverkehr von 0.0.0.0/0 bis Port 22 auf Ihren Ressourcen nicht zulassen, können Sie den Remote-Zugriff einschränken.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CM-6.A	CM-6.A Konfigurationseinstellungen	mfa-enabled-for-iam-Konsolenzugriff	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass MFA für alle AWS Identity and Access Management (IAM) -Benutzer aktiviert ist, die über ein Konsolenkennwort verfügen. MFA sorgt für eine weitere Schutzebene zusätzlich zu den Anmeldeinformationen. Indem Sie MFA für Benutzer vorschreiben, können Sie Fälle kompromittierter Konten reduzieren und verhindern, dass unbefugte Benutzer auf vertrauliche Daten zugreifen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CM-6.A	CM-6.A Konfigurationseinstellungen	multi-region-cloudtrail-enabled	AWS CloudTrail zeichnet Aktionen und API-Aufrufe der AWS Management Console auf. Sie können feststellen, welche Benutzer und Konten angerufen wurden AWS, von welcher Quell-IP-Adresse aus die Anrufe getätigt wurden und wann die Anrufe erfolgten. CloudTrail übermittelt Protokolldateien aus allen AWS Regionen an Ihren S3-Bucket , wenn MULTI_REGION_CLOUD_TRAIL_ENABLED aktiviert ist. Außerdem wird beim AWS Start einer neuen Region derselbe Trail in der neuen Region erstellt. CloudTrail Dadurch erhalten Sie automatisch Protokolldateien mit API-Aktivitäten für die neue Region.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CM-6.A	CM-6.A Konfigurationseinstellungen	restricted-common-ports	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass gemeinsame Ports für Amazon Elastic Compute Cloud (Amazon EC2) -Sicherheitsgruppen eingeschränkt sind. Wenn der Zugriff auf Ports nicht auf vertrauenswürdige Quellen beschränkt wird, kann dies zu Angriffen auf die Verfügbarkeit, Integrität und Vertraulichkeit von Systemen führen. Mit dieser Regel können Sie optional die Parameter blockedPort1–blockedPort5 festlegen (Standardkonfigurationen: 20, 21, 3389, 3306, 4333). Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CM-6.A	CM-6.A Konfigurationseinstellungen	root-account-mfa-enabled	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass MFA für den Root-Benutzer aktiviert ist. Der Stammbenutzer ist der AWS-Konto-Benutzer mit den meisten Berechtigungen. MFA bietet eine weitere Schutzebene zusätzlich zum Benutzernamen und Passwort. Indem Sie MFA für den Root-Benutzer vorschreiben, können Sie die Anzahl AWS-Konten kompromittierter Benutzer reduzieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CM-6.A	CM-6.A Konfigurationseinstellungen	s3- -blöcke-periodisch account-level-public-access	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Simple Storage Service (Amazon S3) -Buckets nicht öffentlich zugänglich sind. Diese Regel trägt dazu bei, sensible Daten vor unbefugten Remote-Benutzern zu schützen, indem sie den öffentlichen Zugriff verhindert. Mit dieser Regel können Sie optional die Parameter ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) und restrictPublicBuckets Parameter (Config Default: True) festlegen. Die tatsächlichen Werte müssen den Richtlini

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
			en Ihrer Organisation entsprechen.
CCCS-fPBMM-CM-6.A	CM-6.A Konfigurationseinstellungen	s3- bucket-logging-enabled	Die Amazon Simple Storage Service (Amazon S3)-Serverzugriffsprotokollierung bietet eine Methode zur Überwachung des Netzwerks im Hinblick auf potenzielle Cybersicherheitsereignisse. Die Ereignisse werden überwacht, indem detaillierte Aufzeichnungen über die Anfragen erfasst werden, die an einen Amazon-S3-Bucket gestellt wurden. Jeder Zugriffsprotokolleintrag enthält Details zu einer einzelnen Zugriffsanfrage. Zu den Details gehören Auftraggeber, Bucket-Name, Anforderungszeit, Anforderungsaktion, Antwortstatus und Fehlercode, falls relevant.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CM-6.A	CM-6.A Konfigurationseinstellungen	s-3 bucket-public-read-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie nur autorisierten Benutzern, Prozessen und Geräten Zugriff auf Amazon Simple Storage Service (Amazon S3) - Buckets gewähren. Die Verwaltung des Zugriffs sollte mit der Klassifizierung der Daten übereinstimmen.
CCCS-fPBMM-CM-6.A	CM-6.A Konfigurationseinstellungen	s3- bucket-public-write-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie nur autorisierten Benutzern, Prozessen und Geräten Zugriff auf Amazon Simple Storage Service (Amazon S3) - Buckets gewähren. Die Verwaltung des Zugriffs sollte mit der Klassifizierung der Daten übereinstimmen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CM-6.A	CM-6.A Konfigurationseinstellungen	s3- bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) unterstützt die Aufrechterhaltung einer angemessenen Kapazität und Verfügbarkeit. CRR ermöglicht das automatische, asynchrone Kopieren von Objekten in Amazon-S3-Buckets, um die Datenverfügbarkeit sicherzustellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CM-6.A	CM-6.A Konfigurationseinstellungen	s3- bucket-server-side-encryption -aktiviert	Zum Schutz von Daten im Ruhezustand müssen Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon Simple Storage Service (Amazon S3)-Buckets aktiviert ist. Da sensible Daten in Amazon-S3-Buckets gespeichert werden können, sollten Sie die Verschlüsselung aktivieren, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CM-6.A	CM-6.A Konfigurationseinstellungen	s-3 bucket-ssl-requests-only	Um Daten während der Übertragung zu schützen, stellen Sie sicher, dass Ihre Amazon Simple Storage Service (Amazon S3)-Buckets Anfragen zur Verwendung von Secure Socket Layer (SSL)-Buckets erfordern. Da sensible Daten vorhanden sein können, sollten Sie die Verschlüsselung bei der Übertragung aktivieren, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CM-6.A	CM-6.A Konfigurationseinstellungen	vpc-default-security-group-geschlossen	Sicherheitsgruppen von Amazon Elastic Compute Cloud (Amazon EC2) können bei der Verwaltung des Netzwerkzugriffs helfen, indem sie eine statusbehaftete Filterung des ein- und ausgehenden Netzwerkverkehrs zu Ressourcen bereitstellen. AWS Die Beschränkung des gesamten Datenverkehrs auf die Standardsicherheitsgruppe hilft dabei, den Fernzugriff auf Ihre Ressourcen einzuschränken. AWS

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CM-6.A	CM-6.A Konfigurationseinstellungen	vpc-flow-logs-enabled	VPC-Flow-Protokolle erfassen detaillierte Informationsdatensätze über den IP-Datenverkehr, der zu und von Netzwerkschnittstellen in Ihrer Amazon Virtual Private Cloud (Amazon VPC) fließt. Standardmäßig enthalten Flow-Protokolldatensätze Werte für die verschiedenen Komponenten des IP-Flows, einschließlich Quelle, Ziel und Protokoll.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CM-6.B	CM-6.B Konfigurationseinstellungen	access-keys-rotated	Die Anmeldeinformationen für autorisierte Geräte, Benutzer und Prozesse werden geprüft, indem sichergestellt wird, dass die IAM-Zugriffsschlüssel gemäß den Vorgaben der Unternehmensrichtlinie rotiert werden. Das regelmäßige Ändern der Zugriffsschlüssel ist eine bewährte Sicherheitsmethode. Es verkürzt den Zeitraum, in dem ein Zugriffsschlüssel aktiv ist, und reduziert die Auswirkungen auf das Unternehmen, wenn die Schlüssel kompromittiert werden. Diese Regel erfordert einen Wert für die Zugriffsschlüssel-Rotation (Standard konfiguration: 90). Der tatsächliche Wert muss den Richtlini

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
			en Ihrer Organisation entsprechen.
CCCS-fPBMM-CM-6.B	CM-6.B Konfigurationseinstellungen	autoscaling-group-elb-healthcheck-erforderlich	Die Elastic Load Balancer (ELB) - Zustandsprüfungen für Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling Scaling-Gruppen unterstützen die Aufrechterhaltung einer angemessenen Kapazität und Verfügbarkeit. Der Load Balancer sendet regelmäßig Pings, versucht Verbindungen herzustellen oder sendet Anfragen, um den Zustand der EC2 Amazon-Instances in einer Gruppe mit auto-scaling zu testen. Wenn eine Instance nicht zurückmeldet, wird der Traffic an eine neue EC2 Amazon-Instance gesendet.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CM-6.B	CM-6.B Konfigurationseinstellungen	cloudtrail-s3-dataevents-enabled	Die Erfassung von Simple Storage Service (Amazon S3)-Datenereignissen unterstützt die Erkennung von ungewöhnlichen Aktivitäten. Zu den Details gehören Informationen zu dem AWS -Konto, das auf einen Amazon-S3-Bucket zugegriffen hat, die IP-Adresse und die Uhrzeit des Ereignisses.
CCCS-fPBMM-CM-6.B	CM-6.B Konfigurationseinstellungen	cloud-trail-cloud-watch-logs-aktiviert	Verwenden Sie Amazon CloudWatch , um Protokoll ereignisaktivitäten zentral zu sammeln und zu verwalten. Die Aufnahme von AWS CloudTrail Daten liefert Einzelheiten zu den API-Aufrufaktivitäten in Ihrem AWS-Konto.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CM-6.B	CM-6.B Konfigurationseinstellungen	cloud-trail-encryption-enabled	Zum Schutz von eventuell vorhandenen sensiblen Daten sowie Daten im Ruhezustand müssen Sie sicherstellen, dass die Verschlüsselung für Ihre AWS CloudTrail aktiviert ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CM-6.B	CM-6.B Konfigurationseinstellungen	cloud-trail-log-file-Validierung aktiviert	Verwenden Sie die AWS CloudTrail Protokolldateivalidierung, um die Integrität von Protokollen zu überprüfen. CloudTrail Mithilfe der Protokolldateivalidierung kann festgestellt werden, ob eine Protokolldatei geändert oder gelöscht wurde oder ob sie nach der Übermittlung CloudTrail unverändert geblieben ist. Dieses Feature wurde mit dem Branchenstandard entsprechenden Algorithmen entwickelt: SHA-256 für die Hashfunktion und SHA-256 mit RSA für digitale Signaturen. Aus diesem Grund ist es rechnerisch unmöglich, CloudTrail Protokolldateien unbemerkt zu ändern, zu löschen oder zu fälschen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CM-6.B	CM-6.B Konfigurationseinstellungen	cmk-backing-key-rotation-aktiviert	Aktivieren Sie die Schlüsselrotation, um sicherzustellen, dass Schlüssel rotiert werden, sobald sie das Ende ihrer Kryptoperiode erreicht haben.
CCCS-fPBMM-CM-6.B	CM-6.B Konfigurationseinstellungen	ec2- ebs-encryption-by-default	Zum Schutz von Daten im Ruhezustand müssen Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon Elastic Block Store (Amazon EBS)-Volumes aktiviert ist. Aktivieren Sie die Verschlüsselung von Daten im Ruhezustand, um eventuell in diesen Volumes vorhandene sensible Daten im Ruhezustand zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CM-6.B	CM-6.B Konfigurationseinstellungen	encrypted-volumes	Aktivieren Sie die Verschlüsselung für Ihre Volumes von Amazon Elastic Block Store (Amazon EBS), um eventuell vorhandene sensible Daten sowie Daten im Ruhezustand zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CM-6.B	CM-6.B Konfigurationseinstellungen	iam-no-inline-policy-überprüfen	Stellen Sie sicher, dass ein Benutzer, eine IAM-Rolle oder eine IAM-Gruppe (AWS Identity and Access Management) nicht über eine Inline-Richtlinie zur Zugriffskontrolle auf Systeme und Ressourcen verfügt. AWS empfiehlt, verwaltete Richtlinien anstelle von Inline-Richtlinien zu verwenden. Verwaltete Richtlinien ermöglichen Wiederverwendbarkeit, Versionsverwaltung, Rollback und Delegierung der Berechtigungsverwaltung.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CM-6.B	CM-6.B Konfigurationseinstellungen	iam-password-policy	Die Identitäten und Anmeldeinformationen werden auf der Grundlage einer organisatorischen IAM-Passwortrichtlinie ausgestellt, verwaltet und verifiziert. Sie erfüllen oder übertreffen die Anforderungen von NIST SP 800-63 und dem Standard „Best Practices“ von AWS Foundational Security für die Passwortstärke. Mit dieser Regel können Sie optional RequireUppercaseCharacters (Wert für AWS grundlegende Sicherheitsbewährte Methoden: wahr), RequireLowercaseCharacters (Wert für bewährte Methoden für AWS grundlegende Sicherheit: wahr), RequireSymbols (Wert für bewährte Methoden für AWS grundlegende Sicherheit:

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
			wahr), RequireNumbers (Wert für bewährte Methoden für AWS grundlegende Sicherheit: wahr), MinimumPasswordLength (Wert für bewährte Methoden für AWS grundlegende Sicherheit: 14), PasswordReusePrevention (Wert für bewährte Methoden für AWS grundlegende Sicherheit: 24) und MaxPasswordAge (Wert für bewährte Methoden für AWS grundlegende Sicherheit: 90) für Ihr IAM festlegen Kennwortrichtlinie. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CM-6.B	CM-6.B Konfigurationseinstellungen	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) kann Ihnen dabei helfen, die Prinzipien der geringsten Rechte und der Aufgabentrennung in Zugriffsberechtigungen und Autorisierungen zu integrieren und so zu verhindern, dass Richtlinien „Effect“: „Allow“ mit „Action“: „*“ anstelle von „Resource“: „*“ enthalten. Wenn Benutzern mehr Rechte eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und der Aufgabentrennung verstoßen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CM-6.B	CM-6.B Konfigurationseinstellungen	iam-root-access-key-überprüfen	Der Zugriff auf Systeme und Ressourcen kann gesteuert werden, indem überprüft wird, ob der Root-Benutzer keine Zugriffsschlüssel mit seiner AWS Identity and Access Management (IAM) -Rolle verknüpft hat. Stellen Sie sicher, dass die Root-Zugriffsschlüssel gelöscht werden. Erstellen und verwenden Sie stattdessen rollenbasierte Funktionen, AWS-Konten um das Prinzip der geringsten Funktionalität zu berücksichtigen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CM-6.B	CM-6.B Konfigurationseinstellungen	iam-user-group-membership-überprüfen	AWS Identity and Access Management (IAM) kann Ihnen helfen, Zugriffsberechtigungen und Autorisierungen einzuschränken, indem sichergestellt wird, dass Benutzer Mitglieder mindestens einer Gruppe sind. Wenn Benutzern mehr Berechtigungen eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und Aufgabentrennung verstoßen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CM-6.B	CM-6.B Konfigurationseinstellungen	iam-user-no-policies-überprüfen	Diese Regel stellt sicher, dass AWS Identity and Access Management (IAM) -Richtlinien nur Gruppen oder Rollen zugewiesen werden, um den Zugriff auf Systeme und Ressourcen zu kontrollieren. Die Zuweisung von Berechtigungen auf Gruppen- oder Rollenebene trägt dazu bei, die Wahrscheinlichkeit zu verringern, dass eine Identität übermäßige Berechtigungen erhält oder beibehält.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CM-6.B	CM-6.B Konfigurationseinstellungen	iam-user-unused-credentials-überprüfen	AWS Identity and Access Management (IAM) kann Ihnen bei Zugriffsberechtigungen und Autorisierungen helfen, indem es nach IAM-Passwörtern und Zugriffsschlüsseln sucht, die für einen bestimmten Zeitraum nicht verwendet wurden. Wenn ungenutzte Anmeldeinformationen identifiziert werden, müssen Sie sie deaktivieren und/oder entfernen, da dies gegen das Prinzip der geringsten Berechtigung verstoßen könnte. Für diese Regel müssen Sie einen Wert für das maxCredentialUsage Alter festlegen (Standardkonfiguration: 90). Der tatsächliche Wert muss den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CM-6.B	CM-6.B Konfigurationseinstellungen	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) Security Groups können bei der Verwaltung des Netzwerkzugriffs helfen, indem sie eine statusbehaftete Filterung des ein- und ausgehenden Netzwerkverkehrs zu Ressourcen bereitstellen. AWS Wenn Sie eingehenden (oder entfernten) Datenverkehr von 0.0.0.0/0 bis Port 22 auf Ihren Ressourcen nicht zulassen, können Sie den Remote-Zugriff einschränken.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CM-6.B	CM-6.B Konfigurationseinstellungen	mfa-enabled-for-iam-Konsolenzugriff	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass MFA für alle AWS Identity and Access Management (IAM) -Benutzer aktiviert ist, die über ein Konsolenkennwort verfügen. MFA sorgt für eine weitere Schutzebene zusätzlich zu den Anmeldeinformationen. Indem Sie MFA für Benutzer vorschreiben, können Sie Fälle kompromittierter Konten reduzieren und verhindern, dass unbefugte Benutzer auf vertrauliche Daten zugreifen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CM-6.B	CM-6.B Konfigurationseinstellungen	multi-region-cloudtrail-enabled	AWS CloudTrail zeichnet Aktionen und API-Aufrufe der AWS Management Console auf. Sie können feststellen, welche Benutzer und Konten angerufen wurden AWS, von welcher Quell-IP-Adresse aus die Anrufe getätigt wurden und wann die Anrufe erfolgten. CloudTrail übermittelt Protokolldateien aus allen AWS Regionen an Ihren S3-Bucket , wenn MULTI_REGION_CLOUD_TRAIL_ENABLED aktiviert ist. Außerdem wird beim AWS Start einer neuen Region derselbe Trail in der neuen Region erstellt. CloudTrail Dadurch erhalten Sie automatisch Protokolldateien mit API-Aktivitäten für die neue Region.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CM-6.B	CM-6.B Konfigurationseinstellungen	restricted-common-ports	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass gemeinsame Ports für Amazon Elastic Compute Cloud (Amazon EC2) -Sicherheitsgruppen eingeschränkt sind. Wenn der Zugriff auf Ports nicht auf vertrauenswürdige Quellen beschränkt wird, kann dies zu Angriffen auf die Verfügbarkeit, Integrität und Vertraulichkeit von Systemen führen. Mit dieser Regel können Sie optional die Parameter blockedPort1–blockedPort5 festlegen (Standardkonfigurationen: 20, 21, 3389, 3306, 4333). Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CM-6.B	CM-6.B Konfigurationseinstellungen	root-account-mfa-enabled	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass MFA für den Root-Benutzer aktiviert ist. Der Stammbenutzer ist der AWS-Konto-Benutzer mit den meisten Berechtigungen. MFA bietet eine weitere Schutzebene zusätzlich zum Benutzernamen und Passwort. Indem Sie MFA für den Root-Benutzer vorschreiben, können Sie die Anzahl AWS-Konten kompromittierter Benutzer reduzieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CM-6.B	CM-6.B Konfigurationseinstellungen	s3- -blöcke-periodisch account-level-public-access	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Simple Storage Service (Amazon S3) -Buckets nicht öffentlich zugänglich sind. Diese Regel trägt dazu bei, sensible Daten vor unbefugten Remote-Benutzern zu schützen, indem sie den öffentlichen Zugriff verhindert. Mit dieser Regel können Sie optional die Parameter ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) und restrictPublicBuckets Parameter (Config Default: True) festlegen. Die tatsächlichen Werte müssen den Richtlini

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
			en Ihrer Organisation entsprechen.
CCCS-fPBMM-CM-6.B	CM-6.B Konfigurationseinstellungen	s3- bucket-logging-enabled	Die Amazon Simple Storage Service (Amazon S3)-Serverzugriffsprotokollierung bietet eine Methode zur Überwachung des Netzwerks im Hinblick auf potenzielle Cybersicherheitsereignisse. Die Ereignisse werden überwacht, indem detaillierte Aufzeichnungen über die Anfragen erfasst werden, die an einen Amazon-S3-Bucket gestellt wurden. Jeder Zugriffsprotokolleintrag enthält Details zu einer einzelnen Zugriffsanfrage. Zu den Details gehören Auftraggeber, Bucket-Name, Anforderungszeit, Anforderungsaktion, Antwortstatus und Fehlercode, falls relevant.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CM-6.B	CM-6.B Konfigurationseinstellungen	s-3 bucket-public-read-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie nur autorisierten Benutzern, Prozessen und Geräten Zugriff auf Amazon Simple Storage Service (Amazon S3) - Buckets gewähren. Die Verwaltung des Zugriffs sollte mit der Klassifizierung der Daten übereinstimmen.
CCCS-fPBMM-CM-6.B	CM-6.B Konfigurationseinstellungen	s3- bucket-public-write-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie nur autorisierten Benutzern, Prozessen und Geräten Zugriff auf Amazon Simple Storage Service (Amazon S3) - Buckets gewähren. Die Verwaltung des Zugriffs sollte mit der Klassifizierung der Daten übereinstimmen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CM-6.B	CM-6.B Konfigurationseinstellungen	s3- bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) unterstützt die Aufrechterhaltung einer angemessenen Kapazität und Verfügbarkeit. CRR ermöglicht das automatische, asynchrone Kopieren von Objekten in Amazon-S3-Buckets, um die Datenverfügbarkeit sicherzustellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CM-6.B	CM-6.B Konfigurationseinstellungen	s3- bucket-server-side-encryption -aktiviert	Zum Schutz von Daten im Ruhezustand müssen Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon Simple Storage Service (Amazon S3)-Buckets aktiviert ist. Da sensible Daten in Amazon-S3-Buckets gespeichert werden können, sollten Sie die Verschlüsselung aktivieren, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CM-6.B	CM-6.B Konfigurationseinstellungen	s-3 bucket-ssl-requests-only	Um Daten während der Übertragung zu schützen, stellen Sie sicher, dass Ihre Amazon Simple Storage Service (Amazon S3)-Buckets Anfragen zur Verwendung von Secure Socket Layer (SSL)-Buckets erfordern. Da sensible Daten vorhanden sein können, sollten Sie die Verschlüsselung bei der Übertragung aktivieren, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CM-6.B	CM-6.B Konfigurationseinstellungen	vpc-default-security-group-geschlossen	Sicherheitsgruppen von Amazon Elastic Compute Cloud (Amazon EC2) können bei der Verwaltung des Netzwerkzugriffs helfen, indem sie eine statusbehaftete Filterung des ein- und ausgehenden Netzwerkverkehrs zu Ressourcen bereitstellen. AWS Die Beschränkung des gesamten Datenverkehrs auf die Standardsicherheitsgruppe hilft dabei, den Fernzugriff auf Ihre Ressourcen einzuschränken. AWS

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CM-6.B	CM-6.B Konfigurationseinstellungen	vpc-flow-logs-enabled	VPC-Flow-Protokolle erfassen detaillierte Informationsdatensätze über den IP-Datenverkehr, der zu und von Netzwerkschnittstellen in Ihrer Amazon Virtual Private Cloud (Amazon VPC) fließt. Standardmäßig enthalten Flow-Protokolldatensätze Werte für die verschiedenen Komponenten des IP-Flows, einschließlich Quelle, Ziel und Protokoll.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CM-6.C	CM-6.C Konfigurationseinstellungen	access-keys-rotated	Die Anmeldeinformationen für autorisierte Geräte, Benutzer und Prozesse werden geprüft, indem sichergestellt wird, dass die IAM-Zugriffsschlüssel gemäß den Vorgaben der Unternehmensrichtlinie rotiert werden. Das regelmäßige Ändern der Zugriffsschlüssel ist eine bewährte Sicherheitsmethode. Es verkürzt den Zeitraum, in dem ein Zugriffsschlüssel aktiv ist, und reduziert die Auswirkungen auf das Unternehmen, wenn die Schlüssel kompromittiert werden. Diese Regel erfordert einen Wert für die Zugriffsschlüssel-Rotation (Standard konfiguration: 90). Der tatsächliche Wert muss den Richtlini

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
			en Ihrer Organisation entsprechen.
CCCS-fPBMM-CM-6.C	CM-6.C Konfigurationseinstellungen	autoscaling-group-elb-healthcheck-erforderlich	Die Elastic Load Balancer (ELB) - Zustandsprüfungen für Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling Scaling-Gruppen unterstützen die Aufrechterhaltung einer angemessenen Kapazität und Verfügbarkeit. Der Load Balancer sendet regelmäßig Pings, versucht Verbindungen herzustellen oder sendet Anfragen, um den Zustand der EC2 Amazon-Instances in einer Gruppe mit auto-scaling zu testen. Wenn eine Instance nicht zurückmeldet, wird der Traffic an eine neue EC2 Amazon-Instance gesendet.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CM-6.C	CM-6.C Konfigurationseinstellungen	cloudtrail-s3-dataevents-enabled	Die Erfassung von Simple Storage Service (Amazon S3)-Datenereignissen unterstützt die Erkennung von ungewöhnlichen Aktivitäten. Zu den Details gehören Informationen zu dem AWS -Konto, das auf einen Amazon-S3-Bucket zugegriffen hat, die IP-Adresse und die Uhrzeit des Ereignisses.
CCCS-fPBMM-CM-6.C	CM-6.C Konfigurationseinstellungen	cloud-trail-cloud-watch-logs-aktiviert	Verwenden Sie Amazon CloudWatch , um Protokoll ereignisaktivitäten zentral zu sammeln und zu verwalten. Die Aufnahme von AWS CloudTrail Daten liefert Einzelheiten zu den API-Aufrufaktivitäten in Ihrem AWS-Konto.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CM-6.C	CM-6.C Konfigurationseinstellungen	cloud-trail-encryption-enabled	Zum Schutz von eventuell vorhandenen sensiblen Daten sowie Daten im Ruhezustand müssen Sie sicherstellen, dass die Verschlüsselung für Ihre AWS CloudTrail aktiviert ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CM-6.C	CM-6.C Konfigurationseinstellungen	cloud-trail-log-file-Validierung aktiviert	Verwenden Sie die AWS CloudTrail Protokolldateivalidierung, um die Integrität von Protokollen zu überprüfen. CloudTrail Mithilfe der Protokolldateivalidierung kann festgestellt werden, ob eine Protokolldatei geändert oder gelöscht wurde oder ob sie nach der Übermittlung CloudTrail unverändert geblieben ist. Dieses Feature wurde mit dem Branchenstandard entsprechenden Algorithmen entwickelt: SHA-256 für die Hashfunktion und SHA-256 mit RSA für digitale Signaturen. Aus diesem Grund ist es rechnerisch unmöglich, CloudTrail Protokolldateien unbemerkt zu ändern, zu löschen oder zu fälschen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CM-6.C	CM-6.C Konfigurationseinstellungen	cmk-backing-key-rotation-aktiviert	Aktivieren Sie die Schlüsselrotation, um sicherzustellen, dass Schlüssel rotiert werden, sobald sie das Ende ihrer Kryptoperiode erreicht haben.
CCCS-fPBMM-CM-6.C	CM-6.C Konfigurationseinstellungen	ec2- ebs-encryption-by-default	Zum Schutz von Daten im Ruhezustand müssen Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon Elastic Block Store (Amazon EBS)-Volumes aktiviert ist. Aktivieren Sie die Verschlüsselung von Daten im Ruhezustand, um eventuell in diesen Volumes vorhandene sensible Daten im Ruhezustand zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CM-6.C	CM-6.C Konfigurationseinstellungen	encrypted-volumes	Aktivieren Sie die Verschlüsselung für Ihre Volumes von Amazon Elastic Block Store (Amazon EBS), um eventuell vorhandene sensible Daten sowie Daten im Ruhezustand zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CM-6.C	CM-6.C Konfigurationseinstellungen	iam-no-inline-policy-überprüfen	Stellen Sie sicher, dass ein Benutzer, eine IAM-Rolle oder eine IAM-Gruppe (AWS Identity and Access Management) nicht über eine Inline-Richtlinie zur Zugriffskontrolle auf Systeme und Ressourcen verfügt. AWS empfiehlt, verwaltete Richtlinien anstelle von Inline-Richtlinien zu verwenden. Verwaltete Richtlinien ermöglichen Wiederverwendbarkeit, Versionsverwaltung, Rollback und Delegierung der Berechtigungsverwaltung.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CM-6.C	CM-6.C Konfigurationseinstellungen	iam-password-policy	Die Identitäten und Anmeldeinformationen werden auf der Grundlage einer organisatorischen IAM-Passwortrichtlinie ausgestellt, verwaltet und verifiziert. Sie erfüllen oder übertreffen die Anforderungen von NIST SP 800-63 und dem Standard „Best Practices“ von AWS Foundational Security für die Passwortstärke. Mit dieser Regel können Sie optional RequireUppercaseCharacters (Wert für AWS grundlegende Sicherheitsbewährte Verfahren: wahr), RequireLowercaseCharacters (Wert für bewährte Methoden für AWS grundlegende Sicherheit: wahr), RequireSymbols (Wert für bewährte Methoden für AWS grundlegende Sicherheit:

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
			wahr), RequireNumbers (Wert für bewährte Methoden für AWS grundlegende Sicherheit: wahr), MinimumPasswordLength (Wert für bewährte Methoden für AWS grundlegende Sicherheit: 14), PasswordReusePrevention (Wert für bewährte Methoden für AWS grundlegende Sicherheit: 24) und MaxPasswordAge (Wert für bewährte Methoden für AWS grundlegende Sicherheit: 90) für Ihr IAM festlegen Kennwortrichtlinie. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CM-6.C	CM-6.C Konfigurationseinstellungen	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) kann Ihnen dabei helfen, die Prinzipien der geringsten Rechte und der Aufgabentrennung in Zugriffsberechtigungen und Autorisierungen zu integrieren und so zu verhindern, dass Richtlinien „Effect“: „Allow“ mit „Action“: „*“ anstelle von „Resource“: „*“ enthalten. Wenn Benutzern mehr Rechte eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und der Aufgabentrennung verstoßen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CM-6.C	CM-6.C Konfigurationseinstellungen	iam-root-access-key-überprüfen	Der Zugriff auf Systeme und Ressourcen kann gesteuert werden, indem überprüft wird, ob der Root-Benutzer keine Zugriffsschlüssel mit seiner AWS Identity and Access Management (IAM) -Rolle verknüpft hat. Stellen Sie sicher, dass die Root-Zugriffsschlüssel gelöscht werden. Erstellen und verwenden Sie stattdessen rollenbasierte Funktionen, AWS-Konten um das Prinzip der geringsten Funktionalität zu berücksichtigen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CM-6.C	CM-6.C Konfigurationseinstellungen	iam-user-group-membership-überprüfen	AWS Identity and Access Management (IAM) kann Ihnen helfen, Zugriffsberechtigungen und Autorisierungen einzuschränken, indem sichergestellt wird, dass Benutzer Mitglieder mindestens einer Gruppe sind. Wenn Benutzern mehr Berechtigungen eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und Aufgabentrennung verstoßen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CM-6.C	CM-6.C Konfigurationseinstellungen	iam-user-no-policies-überprüfen	Diese Regel stellt sicher, dass AWS Identity and Access Management (IAM) -Richtlinien nur Gruppen oder Rollen zugewiesen werden, um den Zugriff auf Systeme und Ressourcen zu kontrollieren. Die Zuweisung von Berechtigungen auf Gruppen- oder Rollenebene trägt dazu bei, die Wahrscheinlichkeit zu verringern, dass eine Identität übermäßige Berechtigungen erhält oder beibehält.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CM-6.C	CM-6.C Konfigurationseinstellungen	iam-user-unused-credentials-überprüfen	AWS Identity and Access Management (IAM) kann Ihnen bei Zugriffsberechtigungen und Autorisierungen helfen, indem es nach IAM-Passwörtern und Zugriffsschlüsseln sucht, die für einen bestimmten Zeitraum nicht verwendet wurden. Wenn ungenutzte Anmeldeinformationen identifiziert werden, müssen Sie sie deaktivieren und/oder entfernen, da dies gegen das Prinzip der geringsten Berechtigung verstoßen könnte. Für diese Regel müssen Sie einen Wert für das maxCredentialUsage Alter festlegen (Standardkonfiguration: 90). Der tatsächliche Wert muss den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CM-6.C	CM-6.C Konfigurationseinstellungen	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) Security Groups können bei der Verwaltung des Netzwerkzugriffs helfen, indem sie eine statusbehaftete Filterung des ein- und ausgehenden Netzwerkverkehrs zu Ressourcen bereitstellen. AWS Wenn Sie eingehenden (oder entfernten) Datenverkehr von 0.0.0.0/0 bis Port 22 auf Ihren Ressourcen nicht zulassen, können Sie den Remote-Zugriff einschränken.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CM-6.C	CM-6.C Konfigurationseinstellungen	mfa-enabled-for-iam-Konsolenzugriff	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass MFA für alle AWS Identity and Access Management (IAM) -Benutzer aktiviert ist, die über ein Konsolenkennwort verfügen. MFA sorgt für eine weitere Schutzebene zusätzlich zu den Anmeldeinformationen. Indem Sie MFA für Benutzer vorschreiben, können Sie Fälle kompromittierter Konten reduzieren und verhindern, dass unbefugte Benutzer auf vertrauliche Daten zugreifen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CM-6.C	CM-6.C Konfigurationseinstellungen	multi-region-cloudtrail-enabled	AWS CloudTrail zeichnet Aktionen und API-Aufrufe der AWS Management Console auf. Sie können feststellen, welche Benutzer und Konten angerufen wurden AWS, von welcher Quell-IP-Adresse aus die Anrufe getätigt wurden und wann die Anrufe erfolgten. CloudTrail übermittelt Protokolldateien aus allen AWS Regionen an Ihren S3-Bucket , wenn MULTI_REGION_CLOUD_TRAIL_ENABLED aktiviert ist. Außerdem wird beim AWS Start einer neuen Region derselbe Trail in der neuen Region erstellt. CloudTrail Dadurch erhalten Sie automatisch Protokolldateien mit API-Aktivitäten für die neue Region.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CM-6.C	CM-6.C Konfigurationseinstellungen	restricted-common-ports	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass gemeinsame Ports für Amazon Elastic Compute Cloud (Amazon EC2) -Sicherheitsgruppen eingeschränkt sind. Wenn der Zugriff auf Ports nicht auf vertrauenswürdige Quellen beschränkt wird, kann dies zu Angriffen auf die Verfügbarkeit, Integrität und Vertraulichkeit von Systemen führen. Mit dieser Regel können Sie optional die Parameter blockedPort1–blockedPort5 festlegen (Standardkonfigurationen: 20, 21, 3389, 3306, 4333). Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CM-6.C	CM-6.C Konfigurationseinstellungen	root-account-mfa-enabled	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass MFA für den Root-Benutzer aktiviert ist. Der Stammbenutzer ist der AWS-Konto-Benutzer mit den meisten Berechtigungen. MFA bietet eine weitere Schutzebene zusätzlich zum Benutzernamen und Passwort. Indem Sie MFA für den Root-Benutzer vorschreiben, können Sie die Anzahl AWS-Konten kompromittierter Benutzer reduzieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CM-6.C	CM-6.C Konfigurationseinstellungen	s3- -blöcke-periodisch account-level-public-access	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Simple Storage Service (Amazon S3) -Buckets nicht öffentlich zugänglich sind. Diese Regel trägt dazu bei, sensible Daten vor unbefugten Remote-Benutzern zu schützen, indem sie den öffentlichen Zugriff verhindert. Mit dieser Regel können Sie optional die Parameter ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) und restrictPublicBuckets Parameter (Config Default: True) festlegen. Die tatsächlichen Werte müssen den Richtlini

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
			en Ihrer Organisation entsprechen.
CCCS-fPBMM-CM-6.C	CM-6.C Konfigurationseinstellungen	s3- bucket-logging-enabled	Die Amazon Simple Storage Service (Amazon S3)-Serverzugriffsprotokollierung bietet eine Methode zur Überwachung des Netzwerks im Hinblick auf potenzielle Cybersicherheitsereignisse. Die Ereignisse werden überwacht, indem detaillierte Aufzeichnungen über die Anfragen erfasst werden, die an einen Amazon-S3-Bucket gestellt wurden. Jeder Zugriffsprotokolleintrag enthält Details zu einer einzelnen Zugriffsanfrage. Zu den Details gehören Auftraggeber, Bucket-Name, Anforderungszeit, Anforderungsaktion, Antwortstatus und Fehlercode, falls relevant.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CM-6.C	CM-6.C Konfigurationseinstellungen	s-3 bucket-public-read-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie nur autorisierten Benutzern, Prozessen und Geräten Zugriff auf Amazon Simple Storage Service (Amazon S3) - Buckets gewähren. Die Verwaltung des Zugriffs sollte mit der Klassifizierung der Daten übereinstimmen.
CCCS-fPBMM-CM-6.C	CM-6.C Konfigurationseinstellungen	s3- bucket-public-write-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie nur autorisierten Benutzern, Prozessen und Geräten Zugriff auf Amazon Simple Storage Service (Amazon S3) - Buckets gewähren. Die Verwaltung des Zugriffs sollte mit der Klassifizierung der Daten übereinstimmen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CM-6.C	CM-6.C Konfigurationseinstellungen	s3- bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) unterstützt die Aufrechterhaltung einer angemessenen Kapazität und Verfügbarkeit. CRR ermöglicht das automatische, asynchrone Kopieren von Objekten in Amazon-S3-Buckets, um die Datenverfügbarkeit sicherzustellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CM-6.C	CM-6.C Konfigurationseinstellungen	s3- bucket-server-side-encryption -aktiviert	Zum Schutz von Daten im Ruhezustand müssen Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon Simple Storage Service (Amazon S3)-Buckets aktiviert ist. Da sensible Daten in Amazon-S3-Buckets gespeichert werden können, sollten Sie die Verschlüsselung aktivieren, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CM-6.C	CM-6.C Konfigurationseinstellungen	s-3 bucket-ssl-requests-only	Um Daten während der Übertragung zu schützen, stellen Sie sicher, dass Ihre Amazon Simple Storage Service (Amazon S3)-Buckets Anfragen zur Verwendung von Secure Socket Layer (SSL)-Buckets erfordern. Da sensible Daten vorhanden sein können, sollten Sie die Verschlüsselung bei der Übertragung aktivieren, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CM-6.C	CM-6.C Konfigurationseinstellungen	vpc-default-security-group-geschlossen	Sicherheitsgruppen von Amazon Elastic Compute Cloud (Amazon EC2) können bei der Verwaltung des Netzwerkzugriffs helfen, indem sie eine statusbehaftete Filterung des ein- und ausgehenden Netzwerkverkehrs zu Ressourcen bereitstellen. AWS Die Beschränkung des gesamten Datenverkehrs auf die Standardsicherheitsgruppe hilft dabei, den Fernzugriff auf Ihre Ressourcen einzuschränken. AWS

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CM-6.C	CM-6.C Konfigurationseinstellungen	vpc-flow-logs-enabled	VPC-Flow-Protokolle erfassen detaillierte Informationsdatensätze über den IP-Datenverkehr, der zu und von Netzwerkschnittstellen in Ihrer Amazon Virtual Private Cloud (Amazon VPC) fließt. Standardmäßig enthalten Flow-Protokolldatensätze Werte für die verschiedenen Komponenten des IP-Flows, einschließlich Quelle, Ziel und Protokoll.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CM-6.D	CM-6.D Konfigurationseinstellungen	access-keys-rotated	Die Anmeldeinformationen für autorisierte Geräte, Benutzer und Prozesse werden geprüft, indem sichergestellt wird, dass die IAM-Zugriffsschlüssel gemäß den Vorgaben der Unternehmensrichtlinie rotiert werden. Das regelmäßige Ändern der Zugriffsschlüssel ist eine bewährte Sicherheitsmethode. Es verkürzt den Zeitraum, in dem ein Zugriffsschlüssel aktiv ist, und reduziert die Auswirkungen auf das Unternehmen, wenn die Schlüssel kompromittiert werden. Diese Regel erfordert einen Wert für die Zugriffsschlüssel-Rotation (Standard konfiguration: 90). Der tatsächliche Wert muss den Richtlini

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
			en Ihrer Organisation entsprechen.
CCCS-fPBMM-CM-6.D	CM-6.D Konfigurationseinstellungen	autoscaling-group-elb-healthcheck-erforderlich	Die Elastic Load Balancer (ELB) - Zustandsprüfungen für Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling Scaling-Gruppen unterstützen die Aufrechterhaltung einer angemessenen Kapazität und Verfügbarkeit. Der Load Balancer sendet regelmäßig Pings, versucht Verbindungen herzustellen oder sendet Anfragen, um den Zustand der EC2 Amazon-Instances in einer Gruppe mit auto-scaling zu testen. Wenn eine Instance nicht zurückmeldet, wird der Traffic an eine neue EC2 Amazon-Instance gesendet.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CM-6.D	CM-6.D Konfigurationseinstellungen	cloudtrail-s3-dataevents-enabled	Die Erfassung von Simple Storage Service (Amazon S3)-Datenereignissen unterstützt die Erkennung von ungewöhnlichen Aktivitäten. Zu den Details gehören Informationen zu dem AWS -Konto, das auf einen Amazon-S3-Bucket zugegriffen hat, die IP-Adresse und die Uhrzeit des Ereignisses.
CCCS-fPBMM-CM-6.D	CM-6.D Konfigurationseinstellungen	cloud-trail-cloud-watch-logs-aktiviert	Verwenden Sie Amazon CloudWatch , um Protokoll ereignisaktivitäten zentral zu sammeln und zu verwalten. Die Aufnahme von AWS CloudTrail Daten liefert Einzelheiten zu den API-Aufrufaktivitäten in Ihrem AWS-Konto.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CM-6.D	CM-6.D Konfigurationseinstellungen	cloud-trail-encryption-enabled	Zum Schutz von eventuell vorhandenen sensiblen Daten sowie Daten im Ruhezustand müssen Sie sicherstellen, dass die Verschlüsselung für Ihre AWS CloudTrail aktiviert ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CM-6.D	CM-6.D Konfigurationseinstellungen	cloud-trail-log-file-Validierung aktiviert	Verwenden Sie die AWS CloudTrail Protokolldateivalidierung, um die Integrität von Protokollen zu überprüfen. CloudTrail Mithilfe der Protokolldateivalidierung kann festgestellt werden, ob eine Protokolldatei geändert oder gelöscht wurde oder ob sie nach der Übermittlung CloudTrail unverändert geblieben ist. Dieses Feature wurde mit dem Branchenstandard entsprechenden Algorithmen entwickelt: SHA-256 für die Hashfunktion und SHA-256 mit RSA für digitale Signaturen. Aus diesem Grund ist es rechnerisch unmöglich, CloudTrail Protokolldateien unbemerkt zu ändern, zu löschen oder zu fälschen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CM-6.D	CM-6.D Konfigurationseinstellungen	cmk-backing-key-rotation-aktiviert	Aktivieren Sie die Schlüsselrotation, um sicherzustellen, dass Schlüssel rotiert werden, sobald sie das Ende ihrer Kryptoperiode erreicht haben.
CCCS-fPBMM-CM-6.D	CM-6.D Konfigurationseinstellungen	ec2- ebs-encryption-by-default	Zum Schutz von Daten im Ruhezustand müssen Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon Elastic Block Store (Amazon EBS)-Volumes aktiviert ist. Aktivieren Sie die Verschlüsselung von Daten im Ruhezustand, um eventuell in diesen Volumes vorhandene sensible Daten im Ruhezustand zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CM-6.D	CM-6.D Konfigurationseinstellungen	encrypted-volumes	Aktivieren Sie die Verschlüsselung für Ihre Volumes von Amazon Elastic Block Store (Amazon EBS), um eventuell vorhandene sensible Daten sowie Daten im Ruhezustand zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CM-6.D	CM-6.D Konfigurationseinstellungen	iam-no-inline-policy-überprüfen	Stellen Sie sicher, dass ein Benutzer, eine IAM-Rolle oder eine IAM-Gruppe (AWS Identity and Access Management) nicht über eine Inline-Richtlinie zur Zugriffskontrolle auf Systeme und Ressourcen verfügt. AWS empfiehlt, verwaltete Richtlinien anstelle von Inline-Richtlinien zu verwenden. Verwaltete Richtlinien ermöglichen Wiederverwendbarkeit, Versionsverwaltung, Rollback und Delegierung der Berechtigungsverwaltung.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CM-6.D	CM-6.D Konfigurationseinstellungen	iam-password-policy	Die Identitäten und Anmeldeinformationen werden auf der Grundlage einer organisatorischen IAM-Passwortrichtlinie ausgestellt, verwaltet und verifiziert. Sie erfüllen oder übertreffen die Anforderungen von NIST SP 800-63 und dem Standard „Best Practices“ von AWS Foundational Security für die Passwortstärke. Mit dieser Regel können Sie optional RequireUppercaseCharacters (Wert für AWS grundlegende Sicherheitsbewährte Verfahren: wahr), RequireLowercaseCharacters (Wert für bewährte Methoden für AWS grundlegende Sicherheit: wahr), RequireSymbols (Wert für bewährte Methoden für AWS grundlegende Sicherheit:

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
			wahr), RequireNumbers (Wert für bewährte Methoden für AWS grundlegende Sicherheit: wahr), MinimumPasswordLength (Wert für bewährte Methoden für AWS grundlegende Sicherheit: 14), PasswordReusePrevention (Wert für bewährte Methoden für AWS grundlegende Sicherheit: 24) und MaxPasswordAge (Wert für bewährte Methoden für AWS grundlegende Sicherheit: 90) für Ihr IAM festlegen Kennwortrichtlinie. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CM-6.D	CM-6.D Konfigurationseinstellungen	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) kann Ihnen dabei helfen, die Prinzipien der geringsten Rechte und der Aufgabentrennung in Zugriffsberechtigungen und Autorisierungen zu integrieren und so zu verhindern, dass Richtlinien „Effect“: „Allow“ mit „Action“: „*“ anstelle von „Resource“: „*“ enthalten. Wenn Benutzern mehr Rechte eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und der Aufgabentrennung verstoßen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CM-6.D	CM-6.D Konfigurationseinstellungen	iam-root-access-key-überprüfen	Der Zugriff auf Systeme und Ressourcen kann gesteuert werden, indem überprüft wird, ob der Root-Benutzer keine Zugriffsschlüssel mit seiner AWS Identity and Access Management (IAM) -Rolle verknüpft hat. Stellen Sie sicher, dass die Root-Zugriffsschlüssel gelöscht werden. Erstellen und verwenden Sie stattdessen rollenbasierte Funktionen, AWS-Konten um das Prinzip der geringsten Funktionalität zu berücksichtigen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CM-6.D	CM-6.D Konfigurationseinstellungen	iam-user-group-membership-überprüfen	AWS Identity and Access Management (IAM) kann Ihnen helfen, Zugriffsberechtigungen und Autorisierungen einzuschränken, indem sichergestellt wird, dass Benutzer Mitglieder mindestens einer Gruppe sind. Wenn Benutzern mehr Berechtigungen eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und Aufgabentrennung verstoßen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CM-6.D	CM-6.D Konfigurationseinstellungen	iam-user-no-policies-überprüfen	Diese Regel stellt sicher, dass AWS Identity and Access Management (IAM) -Richtlinien nur Gruppen oder Rollen zugewiesen werden, um den Zugriff auf Systeme und Ressourcen zu kontrollieren. Die Zuweisung von Berechtigungen auf Gruppen- oder Rollenebene trägt dazu bei, die Wahrscheinlichkeit zu verringern, dass eine Identität übermäßige Berechtigungen erhält oder beibehält.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CM-6.D	CM-6.D Konfigurationseinstellungen	iam-user-unused-credentials-überprüfen	AWS Identity and Access Management (IAM) kann Ihnen bei Zugriffsberechtigungen und Autorisierungen helfen, indem es nach IAM-Passwörtern und Zugriffsschlüsseln sucht, die für einen bestimmten Zeitraum nicht verwendet wurden. Wenn ungenutzte Anmeldeinformationen identifiziert werden, müssen Sie sie deaktivieren und/oder entfernen, da dies gegen das Prinzip der geringsten Berechtigung verstoßen könnte. Für diese Regel müssen Sie einen Wert für das maxCredentialUsage Alter festlegen (Standardkonfiguration: 90). Der tatsächliche Wert muss den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CM-6.D	CM-6.D Konfigurationseinstellungen	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) Security Groups können bei der Verwaltung des Netzwerkzugriffs helfen, indem sie eine statusbehaftete Filterung des ein- und ausgehenden Netzwerkverkehrs zu Ressourcen bereitstellen. AWS Wenn Sie eingehenden (oder entfernten) Datenverkehr von 0.0.0.0/0 bis Port 22 auf Ihren Ressourcen nicht zulassen, können Sie den Remote-Zugriff einschränken.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CM-6.D	CM-6.D Konfigurationseinstellungen	mfa-enabled-for-iam-Konsolenzugriff	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass MFA für alle AWS Identity and Access Management (IAM) -Benutzer aktiviert ist, die über ein Konsolenkennwort verfügen. MFA sorgt für eine weitere Schutzebene zusätzlich zu den Anmeldeinformationen. Indem Sie MFA für Benutzer vorschreiben, können Sie Fälle kompromittierter Konten reduzieren und verhindern, dass unbefugte Benutzer auf vertrauliche Daten zugreifen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CM-6.D	CM-6.D Konfigurationseinstellungen	multi-region-cloudtrail-enabled	AWS CloudTrail zeichnet Aktionen und API-Aufrufe der AWS Management Console auf. Sie können feststellen, welche Benutzer und Konten angerufen wurden AWS, von welcher Quell-IP-Adresse aus die Anrufe getätigt wurden und wann die Anrufe erfolgten. CloudTrail übermittelt Protokolldateien aus allen AWS Regionen an Ihren S3-Bucket , wenn MULTI_REGION_CLOUD_TRAIL_ENABLED aktiviert ist. Außerdem wird beim AWS Start einer neuen Region derselbe Trail in der neuen Region erstellt. CloudTrail Dadurch erhalten Sie automatisch Protokolldateien mit API-Aktivitäten für die neue Region.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CM-6.D	CM-6.D Konfigurationseinstellungen	restricted-common-ports	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass gemeinsame Ports für Amazon Elastic Compute Cloud (Amazon EC2) -Sicherheitsgruppen eingeschränkt sind. Wenn der Zugriff auf Ports nicht auf vertrauenswürdige Quellen beschränkt wird, kann dies zu Angriffen auf die Verfügbarkeit, Integrität und Vertraulichkeit von Systemen führen. Mit dieser Regel können Sie optional die Parameter blockedPort1–blockedPort5 festlegen (Standardkonfigurationen: 20, 21, 3389, 3306, 4333). Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CM-6.D	CM-6.D Konfigurationseinstellungen	root-account-mfa-enabled	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass MFA für den Root-Benutzer aktiviert ist. Der Stammbenutzer ist der AWS-Konto-Benutzer mit den meisten Berechtigungen. MFA bietet eine weitere Schutzebene zusätzlich zum Benutzernamen und Passwort. Indem Sie MFA für den Root-Benutzer vorschreiben, können Sie die Anzahl AWS-Konten kompromittierter Benutzer reduzieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CM-6.D	CM-6.D Konfigurationseinstellungen	s3- -blöcke-periodisch account-level-public-access	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Simple Storage Service (Amazon S3) -Buckets nicht öffentlich zugänglich sind. Diese Regel trägt dazu bei, sensible Daten vor unbefugten Remote-Benutzern zu schützen, indem sie den öffentlichen Zugriff verhindert. Mit dieser Regel können Sie optional die Parameter ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) und restrictPublicBuckets Parameter (Config Default: True) festlegen. Die tatsächlichen Werte müssen den Richtlini

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
			en Ihrer Organisation entsprechen.
CCCS-fPBMM-CM-6.D	CM-6.D Konfigurationseinstellungen	s3- bucket-logging-enabled	Die Amazon Simple Storage Service (Amazon S3)-Serverzugriffsprotokollierung bietet eine Methode zur Überwachung des Netzwerks im Hinblick auf potenzielle Cybersicherheitsereignisse. Die Ereignisse werden überwacht, indem detaillierte Aufzeichnungen über die Anfragen erfasst werden, die an einen Amazon-S3-Bucket gestellt wurden. Jeder Zugriffsprotokolleintrag enthält Details zu einer einzelnen Zugriffsanfrage. Zu den Details gehören Auftraggeber, Bucket-Name, Anforderungszeit, Anforderungsaktion, Antwortstatus und Fehlercode, falls relevant.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CM-6.D	CM-6.D Konfigurationseinstellungen	s-3 bucket-public-read-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie nur autorisierten Benutzern, Prozessen und Geräten Zugriff auf Amazon Simple Storage Service (Amazon S3) - Buckets gewähren. Die Verwaltung des Zugriffs sollte mit der Klassifizierung der Daten übereinstimmen.
CCCS-fPBMM-CM-6.D	CM-6.D Konfigurationseinstellungen	s3- bucket-public-write-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie nur autorisierten Benutzern, Prozessen und Geräten Zugriff auf Amazon Simple Storage Service (Amazon S3) - Buckets gewähren. Die Verwaltung des Zugriffs sollte mit der Klassifizierung der Daten übereinstimmen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CM-6.D	CM-6.D Konfigurationseinstellungen	s3- bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) unterstützt die Aufrechterhaltung einer angemessenen Kapazität und Verfügbarkeit. CRR ermöglicht das automatische, asynchrone Kopieren von Objekten in Amazon-S3-Buckets, um die Datenverfügbarkeit sicherzustellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CM-6.D	CM-6.D Konfigurationseinstellungen	s3- bucket-server-side-encryption -aktiviert	Zum Schutz von Daten im Ruhezustand müssen Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon Simple Storage Service (Amazon S3)-Buckets aktiviert ist. Da sensible Daten in Amazon-S3-Buckets gespeichert werden können, sollten Sie die Verschlüsselung aktivieren, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CM-6.D	CM-6.D Konfigurationseinstellungen	s-3 bucket-ssl-requests-only	Um Daten während der Übertragung zu schützen, stellen Sie sicher, dass Ihre Amazon Simple Storage Service (Amazon S3)-Buckets Anfragen zur Verwendung von Secure Socket Layer (SSL)-Buckets erfordern. Da sensible Daten vorhanden sein können, sollten Sie die Verschlüsselung bei der Übertragung aktivieren, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CM-6.D	CM-6.D Konfigurationseinstellungen	vpc-default-security-group-geschlossen	Sicherheitsgruppen von Amazon Elastic Compute Cloud (Amazon EC2) können bei der Verwaltung des Netzwerkzugriffs helfen, indem sie eine statusbehaftete Filterung des ein- und ausgehenden Netzwerkverkehrs zu Ressourcen bereitstellen. AWS Die Beschränkung des gesamten Datenverkehrs auf die Standardsicherheitsgruppe hilft dabei, den Fernzugriff auf Ihre Ressourcen einzuschränken. AWS

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CM-6.D	CM-6.D Konfigurationseinstellungen	vpc-flow-logs-enabled	VPC-Flow-Protokolle erfassen detaillierte Informationsdatensätze über den IP-Datenverkehr, der zu und von Netzwerkschnittstellen in Ihrer Amazon Virtual Private Cloud (Amazon VPC) fließt. Standardmäßig enthalten Flow-Protokolldatensätze Werte für die verschiedenen Komponenten des IP-Flows, einschließlich Quelle, Ziel und Protokoll.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CM-7.A	CM-7.A Geringste Funktionalität	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) Security Groups können bei der Verwaltung des Netzwerkzugriffs helfen, indem sie eine statusbehaftete Filterung des ein- und ausgehenden Netzwerkverkehrs zu Ressourcen bereitstellen. AWS Wenn Sie eingehenden (oder entfernten) Datenverkehr von 0.0.0.0/0 bis Port 22 auf Ihren Ressourcen nicht zulassen, können Sie den Remote-Zugriff einschränken.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CM-7.A	CM-7.A Geringste Funktionalität	restricted-common-ports	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass gemeinsame Ports für Amazon Elastic Compute Cloud (Amazon EC2) -Sicherheitsgruppen eingeschränkt sind. Wenn der Zugriff auf Ports nicht auf vertrauenswürdige Quellen beschränkt wird, kann dies zu Angriffen auf die Verfügbarkeit, Integrität und Vertraulichkeit von Systemen führen. Mit dieser Regel können Sie optional die Parameter blockedPort1–blockedPort5 festlegen (Standardkonfigurationen: 20, 21, 3389, 3306, 4333). Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CM-7.B	CM-7.B Geringste Funktionalität	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) Security Groups können bei der Verwaltung des Netzwerkzugriffs helfen, indem sie eine statusbehaftete Filterung des ein- und ausgehenden Netzwerkverkehrs zu Ressourcen bereitstellen. AWS Wenn Sie eingehenden (oder entfernten) Datenverkehr von 0.0.0.0/0 bis Port 22 auf Ihren Ressourcen nicht zulassen, können Sie den Remote-Zugriff einschränken.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CM-7.B	CM-7.B Geringste Funktionalität	restricted-common-ports	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass gemeinsame Ports für Amazon Elastic Compute Cloud (Amazon EC2) -Sicherheitsgruppen eingeschränkt sind. Wenn der Zugriff auf Ports nicht auf vertrauenswürdige Quellen beschränkt wird, kann dies zu Angriffen auf die Verfügbarkeit, Integrität und Vertraulichkeit von Systemen führen. Mit dieser Regel können Sie optional die Parameter blockedPort1–blockedPort5 festlegen (Standardkonfigurationen: 20, 21, 3389, 3306, 4333). Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CM-8(1)	CM-8(1) Inventar der Komponenten des Informationssystems | Updates während der Installation/Deinstallation	ec2-manager instance-managed-by-systems	Eine Bestandsaufnahme der Softwareplattformen und Anwendungen innerhalb des Unternehmens ist möglich, indem Amazon Elastic Compute Cloud (Amazon EC2) - Instances mit AWS Systems Manager verwaltet werden. Verwenden Sie AWS Systems Manager, um detaillierte Systemkonfigurationen, Betriebssystem-Patch-Levels, Namen und Typ der Dienste, Softwareinstallationen, Anwendungsname, Herausgeber und Version sowie andere Details zu Ihrer Umgebung bereitzustellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CM-8(1)	CM-8(1) Inventar der Komponenten des Informationssystems | Updates während der Installation/Deinstallation	ec2-check managedinstance-association-compliance-status	Verwenden Sie AWS Systems Manager Associations, um bei der Inventarisierung von Softwareplattformen und Anwendungen innerhalb eines Unternehmens zu helfen. AWS Systems Manager weist Ihren verwalteten Instances einen Konfigurationsstatus zu und ermöglicht es Ihnen, Basiswerte für Betriebssystem-Patch-Levels, Softwareinstallationen, Anwendungskonfigurationen und andere Details zu Ihrer Umgebung festzulegen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CM-8(2)	CM-8(1) Inventar der Komponenten des Informationssystems | Automatisierte Wartung	ec2-manager instance-managed-by-systems	Eine Bestandsaufnahme der Softwareplattformen und Anwendungen innerhalb des Unternehmens ist möglich, indem Amazon Elastic Compute Cloud (Amazon EC2) - Instances mit AWS Systems Manager verwaltet werden. Verwenden Sie AWS Systems Manager, um detaillierte Systemkonfigurationen, Betriebssystem-Patch-Levels, Namen und Typ der Dienste, Softwareinstallationen, Anwendungsname, Herausgeber und Version sowie andere Details zu Ihrer Umgebung bereitzustellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CM-8(2)	CM-8(1) Inventar der Komponenten des Informationssystems | Automatisierte Wartung	ec2-check managedinstance-association-compliance-status	Verwenden Sie AWS Systems Manager Associations, um bei der Inventarisierung von Softwareplattformen und Anwendungen innerhalb eines Unternehmens zu helfen. AWS Systems Manager weist Ihren verwalteten Instances einen Konfigurationsstatus zu und ermöglicht es Ihnen, Basiswerte für Betriebssystem-Patch-Levels, Softwareinstallationen, Anwendungskonfigurationen und andere Details zu Ihrer Umgebung festzulegen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CM-8(3)	CM-8(3) Inventar der Komponenten des Informationssystems | Automatisierte Erkennung nicht autorisierter Komponenten	ec2-manager instance-managed-by-systems	Eine Bestandsaufnahme der Softwareplattformen und Anwendungen innerhalb des Unternehmens ist möglich, indem Amazon Elastic Compute Cloud (Amazon EC2) - Instances mit AWS Systems Manager verwaltet werden. Verwenden Sie AWS Systems Manager, um detaillierte Systemkonfigurationen, Betriebssystem-Patch-Levels, Namen und Typ der Dienste, Softwareinstallationen, Anwendungsname, Herausgeber und Version sowie andere Details zu Ihrer Umgebung bereitzustellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CM-8(3)	CM-8(3) Inventar der Komponenten des Informationssystems | Automatisierte Erkennung nicht autorisierter Komponenten	ec2-check managedinstance-association-compliance-status	Verwenden Sie AWS Systems Manager Associations, um bei der Inventarisierung von Softwareplattformen und Anwendungen innerhalb eines Unternehmens zu helfen. AWS Systems Manager weist Ihren verwalteten Instances einen Konfigurationsstatus zu und ermöglicht es Ihnen, Basiswerte für Betriebssystem-Patch-Levels, Softwareinstallationen, Anwendungskonfigurationen und andere Details zu Ihrer Umgebung festzulegen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CM-8(3)	CM-8(3) Inventar der Komponenten des Informationssystems | Automatisierte Erkennung nicht autorisierter Komponenten	ec2-prüfen managedinstance-patch-compliance-status	Aktivieren Sie diese Regel, um bei der Identifizierung und Dokumentation von Sicherheitslücken in Amazon Elastic Compute Cloud (Amazon EC2) zu helfen. Die Regel prüft, ob die EC2 Amazon-Instance die Patch-Konformität im AWS Systems Manager gemäß den Richtlinien und Verfahren Ihrer Organisation einhält.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CM-8(3)	CM-8(3) Inventar der Komponenten des Informationssystems | Automatisierte Erkennung nicht autorisierter Komponenten	guardduty-enabled-centralized	Amazon GuardDuty kann mithilfe von Threat Intelligence Feeds helfen, potenzielle Cybersicherheitsereignisse zu überwachen und zu erkennen. Dazu gehören Listen mit bösartigen IPs und maschinellen Lernmethoden zur Identifizierung unerwarteter, nicht autorisierter und bösartiger Aktivitäten in Ihrer AWS Cloud-Umgebung.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CM-8.A	CM-8.A Inventar der Komponenten des Informationssystems	ec2-manager instance-managed-by-systems	Eine Bestandsaufnahme der Softwareplattformen und Anwendungen innerhalb des Unternehmens ist möglich, indem Amazon Elastic Compute Cloud (Amazon EC2) - Instances mit AWS Systems Manager verwaltet werden. Verwenden Sie AWS Systems Manager, um detaillierte Systemkonfigurationen, Betriebssystem-Patch-Levels, Namen und Typ der Dienste, Softwareinstallationen, Anwendungsname, Herausgeber und Version sowie andere Details zu Ihrer Umgebung bereitzustellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CM-8.A	CM-8.A Inventar der Komponenten des Informationssystems	ec2-check managedinstance-association-compliance-status	Verwenden Sie AWS Systems Manager Associations, um bei der Inventarisierung von Softwareplattformen und Anwendungen innerhalb eines Unternehmens zu helfen. AWS Systems Manager weist Ihren verwalteten Instances einen Konfigurationsstatus zu und ermöglicht es Ihnen, Basiswerte für Betriebssystem-Patch-Levels, Softwareinstallationen, Anwendungskonfigurationen und andere Details zu Ihrer Umgebung festzulegen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CM-8.B	CM-8.B Inventar der Komponenten des Informationssystems	ec2-manager instance-managed-by-systems	Eine Bestandsaufnahme der Softwareplattformen und Anwendungen innerhalb des Unternehmens ist möglich, indem Amazon Elastic Compute Cloud (Amazon EC2) - Instances mit AWS Systems Manager verwaltet werden. Verwenden Sie AWS Systems Manager, um detaillierte Systemkonfigurationen, Betriebssystem-Patch-Levels, Namen und Typ der Dienste, Softwareinstallationen, Anwendungsname, Herausgeber und Version sowie andere Details zu Ihrer Umgebung bereitzustellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CM-8.B	CM-8.B Inventar der Komponenten des Informationssystems	ec2-check managedinstance-association-compliance-status	Verwenden Sie AWS Systems Manager Associations, um bei der Inventarisierung von Softwareplattformen und Anwendungen innerhalb eines Unternehmens zu helfen. AWS Systems Manager weist Ihren verwalteten Instances einen Konfigurationsstatus zu und ermöglicht es Ihnen, Basiswerte für Betriebssystem-Patch-Levels, Softwareinstallationen, Anwendungskonfigurationen und andere Details zu Ihrer Umgebung festzulegen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CM-8.C	CM-8.C Inventar der Komponenten des Informationssystems	ec2-manager instance-managed-by-systems	Eine Bestandsaufnahme der Softwareplattformen und Anwendungen innerhalb des Unternehmens ist möglich, indem Amazon Elastic Compute Cloud (Amazon EC2) - Instances mit AWS Systems Manager verwaltet werden. Verwenden Sie AWS Systems Manager, um detaillierte Systemkonfigurationen, Betriebssystem-Patch-Levels, Namen und Typ der Dienste, Softwareinstallationen, Anwendungsname, Herausgeber und Version sowie andere Details zu Ihrer Umgebung bereitzustellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CM-8.C	CM-8.C Inventar der Komponenten des Informationssystems	ec2-check managedinstance-association-compliance-status	Verwenden Sie AWS Systems Manager Associations, um bei der Inventarisierung von Softwareplattformen und Anwendungen innerhalb eines Unternehmens zu helfen. AWS Systems Manager weist Ihren verwalteten Instances einen Konfigurationsstatus zu und ermöglicht es Ihnen, Basiswerte für Betriebssystem-Patch-Levels, Softwareinstallationen, Anwendungskonfigurationen und andere Details zu Ihrer Umgebung festzulegen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CM-8.D	CM-8.D Inventar der Komponenten des Informationssystems	ec2-manager instance-managed-by-systems	Eine Bestandsaufnahme der Softwareplattformen und Anwendungen innerhalb des Unternehmens ist möglich, indem Amazon Elastic Compute Cloud (Amazon EC2) - Instances mit AWS Systems Manager verwaltet werden. Verwenden Sie AWS Systems Manager, um detaillierte Systemkonfigurationen, Betriebssystem-Patch-Levels, Namen und Typ der Dienste, Softwareinstallationen, Anwendungsname, Herausgeber und Version sowie andere Details zu Ihrer Umgebung bereitzustellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CM-8.D	CM-8.D Inventar der Komponenten des Informationssystems	ec2-check managedinstance-association-compliance-status	Verwenden Sie AWS Systems Manager Associations, um bei der Inventarisierung von Softwareplattformen und Anwendungen innerhalb eines Unternehmens zu helfen. AWS Systems Manager weist Ihren verwalteten Instances einen Konfigurationsstatus zu und ermöglicht es Ihnen, Basiswerte für Betriebssystem-Patch-Levels, Softwareinstallationen, Anwendungskonfigurationen und andere Details zu Ihrer Umgebung festzulegen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CM-8.E	CM-8.E Inventar der Komponenten des Informationssystems	ec2-manager instance-managed-by-systems	Eine Bestandsaufnahme der Softwareplattformen und Anwendungen innerhalb des Unternehmens ist möglich, indem Amazon Elastic Compute Cloud (Amazon EC2) - Instances mit AWS Systems Manager verwaltet werden. Verwenden Sie AWS Systems Manager, um detaillierte Systemkonfigurationen, Betriebssystem-Patch-Levels, Namen und Typ der Dienste, Softwareinstallationen, Anwendungsname, Herausgeber und Version sowie andere Details zu Ihrer Umgebung bereitzustellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CM-8.E	CM-8.E Inventar der Komponenten des Informationssystems	ec2-check managedinstance-association-compliance-status	Verwenden Sie AWS Systems Manager Associations, um bei der Inventarisierung von Softwareplattformen und Anwendungen innerhalb eines Unternehmens zu helfen. AWS Systems Manager weist Ihren verwalteten Instances einen Konfigurationsstatus zu und ermöglicht es Ihnen, Basiswerte für Betriebssystem-Patch-Levels, Softwareinstallationen, Anwendungskonfigurationen und andere Details zu Ihrer Umgebung festzulegen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CP-2(5)	CP-2(5) Notfallplan | Fortsetzung wichtiger Aufgaben/Geschäftsfunktionen	aurora-resources-protected-by-Backup-Plan	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon Aurora Aurora-Ressourcen Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CP-2(5)	CP-2(5) Notfallplan | Fortsetzung wichtiger Aufgaben/Geschäftsfunktionen	backup-plan-min-frequency-and-min-retention-check	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihr AWS Backup-Plan auf eine Mindestfrequenz und Aufbewahrung festgelegt ist. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen. Mit dieser Regel können Sie die Parameter requiredFrequencyValue (Config default: 1), requiredRetentionDays (Config default: 35) und requiredFrequencyUnit

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
			(Config default: days) festlegen. Der tatsächliche Wert muss den Anforderungen Ihrer Organisation entsprechen.
CCCS-fPBMM-CP-2(5)	CP-2(5) Notfallplan | Fortsetzung wichtiger Aufgaben/Geschäftsfunktionen	backup-recovery-point-encrypted	Stellen Sie sicher, dass die Verschlüsselung für Ihre AWS Backup-Wiederherstellungspunkte aktiviert ist. Da sensible Daten auch im Ruhezustand vorhanden sein können, sollten Sie die Verschlüsselung im Ruhezustand aktivieren, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CP-2(5)	CP-2(5) Notfallplan | Fortsetzung wichtiger Aufgaben/Geschäftsfunktionen	backup-recovery-point-manual-Löschen-deaktiviert	Stellen Sie sicher, dass Ihren AWS Backup-Wiederherstellungspunkten eine ressourcenbasierte Richtlinie zugeordnet ist, die das Löschen von Wiederherstellungspunkten verhindert. Die Verwendung einer ressourcenbasierten Richtlinie zur Verhinderung des Löschens von Wiederherstellungspunkten kann dazu beitragen, ein versehentliches oder absichtliches Löschen zu unterbinden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CP-2(5)	CP-2(5) Notfallplan | Fortsetzung wichtiger Aufgaben/Geschäftsfunktionen	backup-recovery-point-minimum-Aufbewahrungsprüfung	Um bei Datensicherungsprozessen zu helfen, stellen Sie sicher, dass für Ihre AWS Backup-Wiederherstellungspunkte eine Mindestaufbewahrungsdauer festgelegt ist. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen. Mit dieser Regel können Sie den Parameter requiredRetentionDays (Standardkonfiguration: 35) festlegen. Der tatsächliche Wert muss den Anforderu

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
			ngen Ihrer Organisation entsprechen.
CCCS-fPBMM-CP-2(5)	CP-2(5) Notfallplan | Fortsetzung wichtiger Aufgaben/Geschäftsfunktionen	db-instance-backup-enabled	Die Sicherungsfunktion von Amazon RDS erstellt Sicherungen Ihrer Datenbanken und Transaktionsprotokolle. Amazon RDS erstellt einen Snapshot für das Speichervolume Ihrer DB-Instance, sodass die gesamte DB-Instance gesichert wird. Sie können im System spezifische Aufbewahrungsfristen festlegen, um Ihre Ausfallsicherheitsanforderungen zu erfüllen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CP-2(5)	CP-2(5) Notfallplan | Fortsetzung wichtiger Aufgaben/Geschäfts funktionen	dynamodb-autoscaling-enabled	Amazon DynamoDB Auto Scaling verwendet den AWS Application Auto Scaling-Service, um die bereitgestellte Durchsatzkapazität so anzupassen, dass sie automatisch auf tatsächliche Verkehrsmuster reagiert. Auf diese Weise kann eine Tabelle oder ein globaler sekundärer Index die bereitgestellte Lese-/Schreibkapazität erhöhen, um plötzliche Erhöhungen des Datenverkehrs ohne Drosselung zu bewältigen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CP-2(5)	CP-2(5) Notfallplan | Fortsetzung wichtiger Aufgaben/Geschäfts funktionen	dynamodb-pitr-enabled	Aktivieren Sie diese Regel, um zu überprüfen, ob die Informationen gesichert wurden. Es verwaltet auch die Backups, indem es sicherstellt, dass die point-in-time Wiederherstellung in Amazon DynamoDB aktiviert ist. Bei der Wiederherstellung werden fortlaufende Backups Ihrer Tabelle für die letzten 35 Tage gespeichert.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CP-2(5)	CP-2(5) Notfallplan | Fortsetzung wichtiger Aufgaben/Geschäfts funktionen	dynamodb-resources-protected-by-Backup-Plan	Um Sie bei Datensich erungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon DynamoDB DynamoDB-Ressourcen Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwaltet er Backup-Service mit einer richtlini enbasierten Backup-Lösung. Diese Lösung vereinfac ht Ihr Sicherung smanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforde rungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CP-2(5)	CP-2(5) Notfallplan | Fortsetzung wichtiger Aufgaben/Geschäfts funktionen	ebs-optimized-instance	Eine optimierte Instance im Amazon Elastic Block Store (Amazon EBS) bietet zusätzliche, dedizierte Kapazität für Amazon-EBS-I/O-Vorgänge. Diese Optimierung bietet die beste Leistung für Ihr EBS-Volume, indem Konflikte zwischen Amazon-EBS-I/O und anderem Datenverkehr von Ihrer Instance minimiert werden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CP-2(5)	CP-2(5) Notfallplan | Fortsetzung wichtiger Aufgaben/Geschäftsfunktionen	ebs-resources-protected-by-Backup-Plan	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon Elastic Block Store (Amazon EBS) -Ressourcen Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihre Backup-Verwaltung und ermöglicht es Ihnen, Ihre geschäftlichen und behördlichen Anforderungen bezüglich Backups zu erfüllen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CP-2(5)	CP-2(5) Notfallplan | Fortsetzung wichtiger Aufgaben/Geschäfts funktionen	ec2--Plan resources-protected-by-backup	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon Elastic Compute Cloud (Amazon EC2) -Ressourcen Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CP-2(5)	CP-2(5) Notfallplan | Fortsetzung wichtiger Aufgaben/Geschäftsfunktionen	efs-resources-protected-by-Backup-Plan	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon Elastic File System (Amazon EFS) -Dateisysteme Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CP-2(5)	CP-2(5) Notfallplan | Fortsetzung wichtiger Aufgaben/Geschäfts funktionen	elasticache-redis-cluster-automatic-Backup-Check	Wenn automatische Backups aktiviert sind, ElastiCache erstellt Amazon täglich ein Backup des Clusters. Die Sicherung kann für eine von Ihrer Organisation festgelegte Anzahl von Tagen aufbewahrt werden. Automatische Backups schützen vor Datenverlust. Bei einem Ausfall können Sie einen neuen Cluster erstellen, der Ihre Daten aus dem aktuellen Backup wiederherstellt.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CP-2(5)	CP-2(5) Notfallplan | Fortsetzung wichtiger Aufgaben/Geschäfts funktionen	elb-cross-zone-load-Balancing aktiviert	Aktivieren Sie zonenübergreifende s Load Balancing für Ihre Elastic Load Balancer (ELBs), um eine angemesse ne Kapazität und Verfügbarkeit aufrechtzuerhalten. Zonenübergreifende s Load Balancing reduziert die Notwendigkeit, die gleiche Anzahl von Instances in jeder aktivierten Availability Zone aufrechtzuerhalten . Dadurch wird auch die Fähigkeit Ihrer Anwendung verbessert, den Verlust einer oder mehrerer Instances zu bewältigen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CP-2(5)	CP-2(5) Notfallplan | Fortsetzung wichtiger Aufgaben/Geschäfts funktionen	elb-deletion-protection-enabled	Diese Regel sorgt dafür, dass der Löschschutz für Elastic Load Balancing aktiviert ist. Verwenden Sie diese Funktion, um zu verhindern, dass Ihr Load Balancer versehentlich oder böswillig gelöscht wird, was zum Verlust der Verfügbarkeit Ihrer Anwendungen führen kann.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CP-2(5)	CP-2(5) Notfallplan | Fortsetzung wichtiger Aufgaben/Geschäftsfunktionen	fsx-resources-protected-by-Backup-Plan	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre FSx Amazon-Dateisysteme Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CP-2(5)	CP-2(5) Notfallplan | Fortsetzung wichtiger Aufgaben/Geschäfts funktionen	rds-cluster-deletion-protection-aktiviert	Stellen Sie sicher, dass Amazon Relational Database Service (Amazon RDS)-Instances den Löschschutz aktiviert haben. Verwenden Sie den Löschschu tz, um zu verhindern, dass Ihre Amazon-RD S-Instances versehent lich oder böswillig gelöscht werden, was zum Verlust der Verfügbarkeit Ihrer Anwendungen führen kann.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CP-2(5)	CP-2(5) Notfallplan | Fortsetzung wichtiger Aufgaben/Geschäfts funktionen	rds-cluster-multi-az-aktiviert	Für Cluster von Amazon Relationa l Database Service (Amazon RDS) sollte die Multi-AZ-Replikati on aktiviert sein, um die Verfügbarkeit der gespeicherten Daten zu gewährleisten. Availability Zones werden auf einer physisch getrennte n, unabhängi gen Infrastruktur ausgeführt und sind auf höchste Zuverläss igkeit ausgelegt . Im Falle eines Infrastrukturausfa lls führt Amazon RDS einen automatis chen Failover zum Standby-Modus durch, sodass Sie den Datenbankbetrieb wieder aufnehmen können, sobald der Failover abgeschlo ssen ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CP-2(5)	CP-2(5) Notfallplan | Fortsetzung wichtiger Aufgaben/Geschäfts funktionen	rds-instance-deletion-protection-aktiviert	Stellen Sie sicher, dass Amazon Relational Database Service (Amazon RDS)-Instances den Löschschutz aktiviert haben. Verwenden Sie den Löschschu tz, um zu verhindern, dass Ihre Amazon-RD S-Instances versehent lich oder böswillig gelöscht werden, was zum Verlust der Verfügbarkeit Ihrer Anwendungen führen kann.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CP-2(5)	CP-2(5) Notfallplan | Fortsetzung wichtiger Aufgaben/Geschäfts funktionen	rds-multi-az-support	Die Multi-AZ-Unterstützung in Amazon Relational Database Service (Amazon RDS) bietet eine verbesserte Verfügbarkeit und Beständigkeit von Datenbank-Instances. Wenn Sie eine Multi-AZ-Datenbank-Instance bereitstellen, erstellt Amazon RDS automatisch eine primäre Datenbank-Instance und repliziert die Daten synchron auf eine Standby-Instance in einer anderen Availability Zone. Jede Availability Zone läuft auf einer eigenen, physisch getrennten, unabhängigen Infrastruktur und ist auf eine hohe Verfügbarkeit ausgelegt. Im Falle eines Infrastrukturausfalls führt Amazon RDS einen automatis

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
			chen Failover zum Standby-Modus durch, sodass Sie den Datenbankbetrieb wieder aufnehmen können, sobald der Failover abgeschlo ssen ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CP-2(5)	CP-2(5) Notfallplan | Fortsetzung wichtiger Aufgaben/Geschäftsfunktionen	rds-resources-protected-by-Backup-Plan	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon Relational Database Service (Amazon RDS) -Ressourcen Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CP-2(5)	CP-2(5) Notfallplan | Fortsetzung wichtiger Aufgaben/Geschäftsfunktionen	redshift-backup-enabled	Stellen Sie zur Unterstützung der Datensicherungsprozesse sicher, dass Ihre Amazon-Redshift-Cluster über automatisierte Snapshots verfügen. Wenn automatisierte Snapshots für einen Cluster aktiviert sind, erstellt Redshift in regelmäßigen Abständen Snapshots dieses Clusters. Standardmäßig erstellt Redshift alle acht Stunden oder alle 5 GB einen Snapshot für jeden Knoten mit Datenänderungen oder je nachdem, was zuerst eintritt.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CP-2(5)	CP-2(5) Notfallplan | Fortsetzung wichtiger Aufgaben/Geschäfts funktionen	s3- bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) unterstützt die Aufrechterhaltung einer angemesse nen Kapazität und Verfügbarkeit. CRR ermöglicht das automatische, asynchrone Kopieren von Objekten in Amazon-S3-Buckets, um die Datenverf ügbarkeit sicherzus tellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CP-2(5)	CP-2(5) Notfallplan | Fortsetzung wichtiger Aufgaben/Geschäfts funktionen	s-3 bucket-versioning-enabled	Die Versionsv erwaltung von Amazon Simple Storage Service (Amazon S3)-Bucke ts hilft dabei, mehrere Varianten eines Objekts im selben Amazon-S3-Bucket zu speichern. Verwenden Sie die Versionsv erwaltung, um sämtliche Versionen aller Objekte in Ihrem Amazon-S3-Bucket zu speichern , abzurufen oder wiederherzustellen . Mit der Versionsv erwaltung können Sie Versionen sowohl nach unbeabsic htigten Benutzera ktionen als auch nach Anwendungsfehlern problemlos wiederher stellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CP-2(5)	CP-2(5) Notfallplan | Fortsetzung wichtiger Aufgaben/Geschäfts funktionen	vpc-vpn-2-tunnels-up	Redundante Site-to-Site VPN-Tunnel können implementiert werden, um die Anforderungen an die Ausfallsicherheit zu erfüllen. Es verwendet zwei Tunnel, um die Konnektivität sicherzustellen, falls eine der Site-to-Site VPN-Verbindungen nicht verfügbar ist. Um sich vor einem Verbindungsverlust zu schützen, können Sie für den Fall, dass Ihr Kunden-Gateway nicht verfügbar ist, eine zweite Site-to-Site VPN-Verbindung zu Ihrer Amazon Virtual Private Cloud (Amazon VPC) und Ihrem Virtual Private Gateway einrichten, indem Sie ein zweites Kunden-Gateway verwenden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CP-2(6)	CP-2(6) Notfallplan | Alternativer Verarbeitungs-/Speicherort	dynamodb-autoscaling-enabled	Amazon DynamoDB Auto Scaling verwendet den AWS Application Auto Scaling-Service, um die bereitgestellte Durchsatzkapazität so anzupassen, dass sie automatisch auf tatsächliche Verkehrsmuster reagiert. Auf diese Weise kann eine Tabelle oder ein globaler sekundärer Index die bereitgestellte Lese-/Schreibkapazität erhöhen, um plötzliche Erhöhungen des Datenverkehrs ohne Drosselung zu bewältigen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CP-2(6)	CP-2(6) Notfallplan | Alternativer Verarbeitungs-/Speicherort	elb-cross-zone-load-Balancing aktiviert	Aktivieren Sie zonenübergreifendes Load Balancing für Ihre Elastic Load Balancer (ELBs), um eine angemessene Kapazität und Verfügbarkeit aufrechtzuerhalten. Zonenübergreifendes Load Balancing reduziert die Notwendigkeit, die gleiche Anzahl von Instances in jeder aktivierten Availability Zone aufrechtzuerhalten. Dadurch wird auch die Fähigkeit Ihrer Anwendung verbessert, den Verlust einer oder mehrerer Instances zu bewältigen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CP-2(6)	CP-2(6) Notfallplan | Alternativer Verarbeitungs-/Speicherort	multi-region-cloudtrail-enabled	AWS CloudTrail zeichnet Aktionen und API-Aufrufe der AWS Management Console auf. Sie können feststellen, welche Benutzer und Konten angerufen wurden AWS, von welcher Quell-IP-Adresse aus die Anrufe getätigt wurden und wann die Anrufe erfolgten. CloudTrail übermittelt Protokolldateien aus allen AWS Regionen an Ihren S3-Bucket , wenn MULTI_REGION_CLOUD_TRAIL_ENABLED aktiviert ist. Außerdem wird beim AWS Start einer neuen Region derselbe Trail in der neuen Region erstellt. CloudTrail Dadurch erhalten Sie automatisch Protokolldateien mit API-Aktivitäten für die neue Region.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CP-2(6)	CP-2(6) Notfallplan | Alternativer Verarbeitungs-/Speicherort	rds-cluster-multi-az-aktiviert	Für Cluster von Amazon Relational Database Service (Amazon RDS) sollte die Multi-AZ-Replikation aktiviert sein, um die Verfügbarkeit der gespeicherten Daten zu gewährleisten. Availability Zones werden auf einer physisch getrennten, unabhängigen Infrastruktur ausgeführt und sind auf höchste Zuverlässigkeit ausgelegt. Im Falle eines Infrastrukturausfalls führt Amazon RDS einen automatischen Failover zum Standby-Modus durch, sodass Sie den Datenbankbetrieb wieder aufnehmen können, sobald der Failover abgeschlossen ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CP-2(6)	CP-2(6) Notfallplan | Alternativer Verarbeitungs-/Speicherort	rds-multi-az-support	Die Multi-AZ-Unterstützung in Amazon Relational Database Service (Amazon RDS) bietet eine verbesserte Verfügbarkeit und Beständigkeit von Datenbank-Instances. Wenn Sie eine Multi-AZ-Datenbank-Instance bereitstellen, erstellt Amazon RDS automatisch eine primäre Datenbank-Instance und repliziert die Daten synchron auf eine Standby-Instance in einer anderen Availability Zone. Jede Availability Zone läuft auf einer eigenen, physisch getrennten, unabhängigen Infrastruktur und ist auf eine hohe Verfügbarkeit ausgelegt. Im Falle eines Infrastrukturausfalls führt Amazon RDS einen automatis

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
			chen Failover zum Standby-Modus durch, sodass Sie den Datenbankbetrieb wieder aufnehmen können, sobald der Failover abgeschlo ssen ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CP-2(6)	CP-2(6) Notfallplan | Alternativer Verarbeitungs-/Speicherort	vpc-vpn-2-tunnels-up	Redundante Site-to-Site VPN-Tunnel können implementiert werden, um die Anforderungen an die Ausfallsicherheit zu erfüllen. Es verwendet zwei Tunnel, um die Konnektivität sicherzustellen, falls eine der Site-to-Site VPN-Verbindungen nicht verfügbar ist. Um sich vor einem Verbindungsverlust zu schützen, können Sie für den Fall, dass Ihr Kunden-Gateway nicht verfügbar ist, eine zweite Site-to-Site VPN-Verbindung zu Ihrer Amazon Virtual Private Cloud (Amazon VPC) und Ihrem Virtual Private Gateway einrichten, indem Sie ein zweites Kunden-Gateway verwenden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CP-2.A	CP-2.A Notfallplan	dynamodb-autoscaling-enabled	Amazon DynamoDB Auto Scaling verwendet den AWS Application Auto Scaling-Service, um die bereitgestellte Durchsatzkapazität so anzupassen, dass sie automatisch auf tatsächliche Verkehrsmuster reagiert. Auf diese Weise kann eine Tabelle oder ein globaler sekundärer Index die bereitgestellte Lese-/Schreibkapazität erhöhen, um plötzliche Erhöhungen des Datenverkehrs ohne Drosselung zu bewältigen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CP-2.A	CP-2.A Notfallplan	elb-cross-zone-load-Balancing aktiviert	Aktivieren Sie zonenübergreifendes Load Balancing für Ihre Elastic Load Balancer (ELBs), um eine angemessene Kapazität und Verfügbarkeit aufrechtzuerhalten. Zonenübergreifendes Load Balancing reduziert die Notwendigkeit, die gleiche Anzahl von Instances in jeder aktivierten Availability Zone aufrechtzuerhalten. Dadurch wird auch die Fähigkeit Ihrer Anwendung verbessert, den Verlust einer oder mehrerer Instances zu bewältigen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CP-2.A	CP-2.A Notfallplan	elb-deletion-protection-enabled	Diese Regel sorgt dafür, dass der Löschschutz für Elastic Load Balancing aktiviert ist. Verwenden Sie diese Funktion, um zu verhindern, dass Ihr Load Balancer versehentlich oder böswillig gelöscht wird, was zum Verlust der Verfügbarkeit Ihrer Anwendungen führen kann.
CCCS-fPBMM-CP-2.A	CP-2.A Notfallplan	rds-cluster-deletion-protection-aktiviert	Stellen Sie sicher, dass Amazon Relational Database Service (Amazon RDS)-Instances den Löschschutz aktiviert haben. Verwenden Sie den Löschschutz, um zu verhindern, dass Ihre Amazon-RDS-Instances versehentlich oder böswillig gelöscht werden, was zum Verlust der Verfügbarkeit Ihrer Anwendungen führen kann.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CP-2.A	CP-2.A Notfallplan	rds-cluster-multi-az-aktiviert	Für Cluster von Amazon Relational Database Service (Amazon RDS) sollte die Multi-AZ-Replikation aktiviert sein, um die Verfügbarkeit der gespeicherten Daten zu gewährleisten. Availability Zones werden auf einer physisch getrennten, unabhängigen Infrastruktur ausgeführt und sind auf höchste Zuverlässigkeit ausgelegt. Im Falle eines Infrastrukturausfalls führt Amazon RDS einen automatischen Failover zum Standby-Modus durch, sodass Sie den Datenbankbetrieb wieder aufnehmen können, sobald der Failover abgeschlossen ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CP-2.A	CP-2.A Notfallplan	rds-instance-deletion-protection-aktiviert	Stellen Sie sicher, dass Amazon Relational Database Service (Amazon RDS)-Instances den Löschschutz aktiviert haben. Verwenden Sie den Löschschutz, um zu verhindern, dass Ihre Amazon-RDS-Instances versehentlich oder böswillig gelöscht werden, was zum Verlust der Verfügbarkeit Ihrer Anwendungen führen kann.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CP-2.A	CP-2.A Notfallplan	rds-multi-az-support	Die Multi-AZ-Unterstützung in Amazon Relational Database Service (Amazon RDS) bietet eine verbesserte Verfügbarkeit und Beständigkeit von Datenbank-Instances. Wenn Sie eine Multi-AZ-Datenbank-Instance bereitstellen, erstellt Amazon RDS automatisch eine primäre Datenbank-Instance und repliziert die Daten synchron auf eine Standby-Instance in einer anderen Availability Zone. Jede Availability Zone läuft auf einer eigenen, physisch getrennten, unabhängigen Infrastruktur und ist auf eine hohe Verfügbarkeit ausgelegt. Im Falle eines Infrastrukturausfalls führt Amazon RDS einen automatis

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
			chen Failover zum Standby-Modus durch, sodass Sie den Datenbankbetrieb wieder aufnehmen können, sobald der Failover abgeschlo ssen ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CP-2.A	CP-2.A Notfallplan	vpc-vpn-2-tunnels-up	Redundante Site-to-Site VPN-Tunnel können implementiert werden, um die Anforderungen an die Ausfallsicherheit zu erfüllen. Es verwendet zwei Tunnel, um die Konnektivität sicherzustellen, falls eine der Site-to-Site VPN-Verbindungen nicht verfügbar ist. Um sich vor einem Verbindungsverlust zu schützen, können Sie für den Fall, dass Ihr Kunden-Gateway nicht verfügbar ist, eine zweite Site-to-Site VPN-Verbindung zu Ihrer Amazon Virtual Private Cloud (Amazon VPC) und Ihrem Virtual Private Gateway einrichten, indem Sie ein zweites Kunden-Gateway verwenden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CP-2.B	CP-2.B Notfallplan	dynamodb-autoscaling-enabled	Amazon DynamoDB Auto Scaling verwendet den AWS Application Auto Scaling-Service, um die bereitgestellte Durchsatzkapazität so anzupassen, dass sie automatisch auf tatsächliche Verkehrsmuster reagiert. Auf diese Weise kann eine Tabelle oder ein globaler sekundärer Index die bereitgestellte Lese-/Schreibkapazität erhöhen, um plötzliche Erhöhungen des Datenverkehrs ohne Drosselung zu bewältigen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CP-2.B	CP-2.B Notfallplan	elb-cross-zone-load-Balancing aktiviert	Aktivieren Sie zonenübergreifendes Load Balancing für Ihre Elastic Load Balancer (ELBs), um eine angemessene Kapazität und Verfügbarkeit aufrechtzuerhalten. Zonenübergreifendes Load Balancing reduziert die Notwendigkeit, die gleiche Anzahl von Instances in jeder aktivierten Availability Zone aufrechtzuerhalten. Dadurch wird auch die Fähigkeit Ihrer Anwendung verbessert, den Verlust einer oder mehrerer Instances zu bewältigen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CP-2.B	CP-2.B Notfallplan	elb-deletion-protection-enabled	Diese Regel sorgt dafür, dass der Löschschutz für Elastic Load Balancing aktiviert ist. Verwenden Sie diese Funktion, um zu verhindern, dass Ihr Load Balancer versehentlich oder böswillig gelöscht wird, was zum Verlust der Verfügbarkeit Ihrer Anwendungen führen kann.
CCCS-fPBMM-CP-2.B	CP-2.B Notfallplan	rds-cluster-deletion-protection-aktiviert	Stellen Sie sicher, dass Amazon Relational Database Service (Amazon RDS)-Instances den Löschschutz aktiviert haben. Verwenden Sie den Löschschutz, um zu verhindern, dass Ihre Amazon-RDS-Instances versehentlich oder böswillig gelöscht werden, was zum Verlust der Verfügbarkeit Ihrer Anwendungen führen kann.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CP-2.B	CP-2.B Notfallplan	rds-cluster-multi-az-aktiviert	Für Cluster von Amazon Relational Database Service (Amazon RDS) sollte die Multi-AZ-Replikation aktiviert sein, um die Verfügbarkeit der gespeicherten Daten zu gewährleisten. Availability Zones werden auf einer physisch getrennten, unabhängigen Infrastruktur ausgeführt und sind auf höchste Zuverlässigkeit ausgelegt. Im Falle eines Infrastrukturausfalls führt Amazon RDS einen automatischen Failover zum Standby-Modus durch, sodass Sie den Datenbankbetrieb wieder aufnehmen können, sobald der Failover abgeschlossen ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CP-2.B	CP-2.B Notfallplan	rds-instance-deletion-protection-aktiviert	Stellen Sie sicher, dass Amazon Relational Database Service (Amazon RDS)-Instances den Löschschutz aktiviert haben. Verwenden Sie den Löschschutz, um zu verhindern, dass Ihre Amazon-RDS-Instances versehentlich oder böswillig gelöscht werden, was zum Verlust der Verfügbarkeit Ihrer Anwendungen führen kann.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CP-2.B	CP-2.B Notfallplan	rds-multi-az-support	Die Multi-AZ-Unterstützung in Amazon Relational Database Service (Amazon RDS) bietet eine verbesserte Verfügbarkeit und Beständigkeit von Datenbank-Instances. Wenn Sie eine Multi-AZ-Datenbank-Instance bereitstellen, erstellt Amazon RDS automatisch eine primäre Datenbank-Instance und repliziert die Daten synchron auf eine Standby-Instance in einer anderen Availability Zone. Jede Availability Zone läuft auf einer eigenen, physisch getrennten, unabhängigen Infrastruktur und ist auf eine hohe Verfügbarkeit ausgelegt. Im Falle eines Infrastrukturausfalls führt Amazon RDS einen automatis

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
			chen Failover zum Standby-Modus durch, sodass Sie den Datenbankbetrieb wieder aufnehmen können, sobald der Failover abgeschlo ssen ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CP-2.B	CP-2.B Notfallplan	vpc-vpn-2-tunnels-up	Redundante Site-to-Site VPN-Tunnel können implementiert werden, um die Anforderungen an die Ausfallsicherheit zu erfüllen. Es verwendet zwei Tunnel, um die Konnektivität sicherzustellen, falls eine der Site-to-Site VPN-Verbindungen nicht verfügbar ist. Um sich vor einem Verbindungsverlust zu schützen, können Sie für den Fall, dass Ihr Kunden-Gateway nicht verfügbar ist, eine zweite Site-to-Site VPN-Verbindung zu Ihrer Amazon Virtual Private Cloud (Amazon VPC) und Ihrem Virtual Private Gateway einrichten, indem Sie ein zweites Kunden-Gateway verwenden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CP-2.C	CP-2.C Notfallplan	dynamodb-autoscaling-enabled	Amazon DynamoDB Auto Scaling verwendet den AWS Application Auto Scaling-Service, um die bereitgestellte Durchsatzkapazität so anzupassen, dass sie automatisch auf tatsächliche Verkehrsmuster reagiert. Auf diese Weise kann eine Tabelle oder ein globaler sekundärer Index die bereitgestellte Lese-/Schreibkapazität erhöhen, um plötzliche Erhöhungen des Datenverkehrs ohne Drosselung zu bewältigen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CP-2.C	CP-2.C Notfallplan	elb-cross-zone-load-Balancing aktiviert	Aktivieren Sie zonenübergreifendes Load Balancing für Ihre Elastic Load Balancer (ELBs), um eine angemessene Kapazität und Verfügbarkeit aufrechtzuerhalten. Zonenübergreifendes Load Balancing reduziert die Notwendigkeit, die gleiche Anzahl von Instances in jeder aktivierten Availability Zone aufrechtzuerhalten. Dadurch wird auch die Fähigkeit Ihrer Anwendung verbessert, den Verlust einer oder mehrerer Instances zu bewältigen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CP-2.C	CP-2.C Notfallplan	elb-deletion-protection-enabled	Diese Regel sorgt dafür, dass der Löschschutz für Elastic Load Balancing aktiviert ist. Verwenden Sie diese Funktion, um zu verhindern, dass Ihr Load Balancer versehentlich oder böswillig gelöscht wird, was zum Verlust der Verfügbarkeit Ihrer Anwendungen führen kann.
CCCS-fPBMM-CP-2.C	CP-2.C Notfallplan	rds-cluster-deletion-protection-aktiviert	Stellen Sie sicher, dass Amazon Relational Database Service (Amazon RDS)-Instances den Löschschutz aktiviert haben. Verwenden Sie den Löschschutz, um zu verhindern, dass Ihre Amazon-RDS-Instances versehentlich oder böswillig gelöscht werden, was zum Verlust der Verfügbarkeit Ihrer Anwendungen führen kann.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CP-2.C	CP-2.C Notfallplan	rds-cluster-multi-az-aktiviert	Für Cluster von Amazon Relational Database Service (Amazon RDS) sollte die Multi-AZ-Replikation aktiviert sein, um die Verfügbarkeit der gespeicherten Daten zu gewährleisten. Availability Zones werden auf einer physisch getrennten, unabhängigen Infrastruktur ausgeführt und sind auf höchste Zuverlässigkeit ausgelegt. Im Falle eines Infrastrukturausfalls führt Amazon RDS einen automatischen Failover zum Standby-Modus durch, sodass Sie den Datenbankbetrieb wieder aufnehmen können, sobald der Failover abgeschlossen ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CP-2.C	CP-2.C Notfallplan	rds-instance-deletion-protection-aktiviert	Stellen Sie sicher, dass Amazon Relational Database Service (Amazon RDS)-Instances den Löschschutz aktiviert haben. Verwenden Sie den Löschschutz, um zu verhindern, dass Ihre Amazon-RDS-Instances versehentlich oder böswillig gelöscht werden, was zum Verlust der Verfügbarkeit Ihrer Anwendungen führen kann.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CP-2.C	CP-2.C Notfallplan	rds-multi-az-support	Die Multi-AZ-Unterstützung in Amazon Relational Database Service (Amazon RDS) bietet eine verbesserte Verfügbarkeit und Beständigkeit von Datenbank-Instances. Wenn Sie eine Multi-AZ-Datenbank-Instance bereitstellen, erstellt Amazon RDS automatisch eine primäre Datenbank-Instance und repliziert die Daten synchron auf eine Standby-Instance in einer anderen Availability Zone. Jede Availability Zone läuft auf einer eigenen, physisch getrennten, unabhängigen Infrastruktur und ist auf eine hohe Verfügbarkeit ausgelegt. Im Falle eines Infrastrukturausfalls führt Amazon RDS einen automatis

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
			chen Failover zum Standby-Modus durch, sodass Sie den Datenbankbetrieb wieder aufnehmen können, sobald der Failover abgeschlo ssen ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CP-2.C	CP-2.C Notfallplan	vpc-vpn-2-tunnels-up	Redundante Site-to-Site VPN-Tunnel können implementiert werden, um die Anforderungen an die Ausfallsicherheit zu erfüllen. Es verwendet zwei Tunnel, um die Konnektivität sicherzustellen, falls eine der Site-to-Site VPN-Verbindungen nicht verfügbar ist. Um sich vor einem Verbindungsverlust zu schützen, können Sie für den Fall, dass Ihr Kunden-Gateway nicht verfügbar ist, eine zweite Site-to-Site VPN-Verbindung zu Ihrer Amazon Virtual Private Cloud (Amazon VPC) und Ihrem Virtual Private Gateway einrichten, indem Sie ein zweites Kunden-Gateway verwenden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CP-2.D	CP-2.D Notfallplan	dynamodb-autoscaling-enabled	Amazon DynamoDB Auto Scaling verwendet den AWS Application Auto Scaling-Service, um die bereitgestellte Durchsatzkapazität so anzupassen, dass sie automatisch auf tatsächliche Verkehrsmuster reagiert. Auf diese Weise kann eine Tabelle oder ein globaler sekundärer Index die bereitgestellte Lese-/Schreibkapazität erhöhen, um plötzliche Erhöhungen des Datenverkehrs ohne Drosselung zu bewältigen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CP-2.D	CP-2.D Notfallplan	elb-cross-zone-load-Balancing aktiviert	Aktivieren Sie zonenübergreifendes Load Balancing für Ihre Elastic Load Balancer (ELBs), um eine angemessene Kapazität und Verfügbarkeit aufrechtzuerhalten. Zonenübergreifendes Load Balancing reduziert die Notwendigkeit, die gleiche Anzahl von Instances in jeder aktivierten Availability Zone aufrechtzuerhalten. Dadurch wird auch die Fähigkeit Ihrer Anwendung verbessert, den Verlust einer oder mehrerer Instances zu bewältigen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CP-2.D	CP-2.D Notfallplan	elb-deletion-protection-enabled	Diese Regel sorgt dafür, dass der Löschschutz für Elastic Load Balancing aktiviert ist. Verwenden Sie diese Funktion, um zu verhindern, dass Ihr Load Balancer versehentlich oder böswillig gelöscht wird, was zum Verlust der Verfügbarkeit Ihrer Anwendungen führen kann.
CCCS-fPBMM-CP-2.D	CP-2.D Notfallplan	rds-cluster-deletion-protection-aktiviert	Stellen Sie sicher, dass Amazon Relational Database Service (Amazon RDS)-Instances den Löschschutz aktiviert haben. Verwenden Sie den Löschschutz, um zu verhindern, dass Ihre Amazon-RDS-Instances versehentlich oder böswillig gelöscht werden, was zum Verlust der Verfügbarkeit Ihrer Anwendungen führen kann.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CP-2.D	CP-2.D Notfallplan	rds-cluster-multi-az-aktiviert	Für Cluster von Amazon Relational Database Service (Amazon RDS) sollte die Multi-AZ-Replikation aktiviert sein, um die Verfügbarkeit der gespeicherten Daten zu gewährleisten. Availability Zones werden auf einer physisch getrennten, unabhängigen Infrastruktur ausgeführt und sind auf höchste Zuverlässigkeit ausgelegt. Im Falle eines Infrastrukturausfalls führt Amazon RDS einen automatischen Failover zum Standby-Modus durch, sodass Sie den Datenbankbetrieb wieder aufnehmen können, sobald der Failover abgeschlossen ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CP-2.D	CP-2.D Notfallplan	rds-instance-deletion-protection-aktiviert	Stellen Sie sicher, dass Amazon Relational Database Service (Amazon RDS)-Instances den Löschschutz aktiviert haben. Verwenden Sie den Löschschutz, um zu verhindern, dass Ihre Amazon-RDS-Instances versehentlich oder böswillig gelöscht werden, was zum Verlust der Verfügbarkeit Ihrer Anwendungen führen kann.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CP-2.D	CP-2.D Notfallplan	rds-multi-az-support	Die Multi-AZ-Unterstützung in Amazon Relational Database Service (Amazon RDS) bietet eine verbesserte Verfügbarkeit und Beständigkeit von Datenbank-Instances. Wenn Sie eine Multi-AZ-Datenbank-Instance bereitstellen, erstellt Amazon RDS automatisch eine primäre Datenbank-Instance und repliziert die Daten synchron auf eine Standby-Instance in einer anderen Availability Zone. Jede Availability Zone läuft auf einer eigenen, physisch getrennten, unabhängigen Infrastruktur und ist auf eine hohe Verfügbarkeit ausgelegt. Im Falle eines Infrastrukturausfalls führt Amazon RDS einen automatis

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
			chen Failover zum Standby-Modus durch, sodass Sie den Datenbankbetrieb wieder aufnehmen können, sobald der Failover abgeschlo ssen ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CP-2.D	CP-2.D Notfallplan	vpc-vpn-2-tunnels-up	Redundante Site-to-Site VPN-Tunnel können implementiert werden, um die Anforderungen an die Ausfallsicherheit zu erfüllen. Es verwendet zwei Tunnel, um die Konnektivität sicherzustellen, falls eine der Site-to-Site VPN-Verbindungen nicht verfügbar ist. Um sich vor einem Verbindungsverlust zu schützen, können Sie für den Fall, dass Ihr Kunden-Gateway nicht verfügbar ist, eine zweite Site-to-Site VPN-Verbindung zu Ihrer Amazon Virtual Private Cloud (Amazon VPC) und Ihrem Virtual Private Gateway einrichten, indem Sie ein zweites Kunden-Gateway verwenden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CP-2.E	CP-2.E Notfallplan	dynamodb-autoscaling-enabled	Amazon DynamoDB Auto Scaling verwendet den AWS Application Auto Scaling-Service, um die bereitgestellte Durchsatzkapazität so anzupassen, dass sie automatisch auf tatsächliche Verkehrsmuster reagiert. Auf diese Weise kann eine Tabelle oder ein globaler sekundärer Index die bereitgestellte Lese-/Schreibkapazität erhöhen, um plötzliche Erhöhungen des Datenverkehrs ohne Drosselung zu bewältigen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CP-2.E	CP-2.E Notfallplan	elb-cross-zone-load-Balancing aktiviert	Aktivieren Sie zonenübergreifendes Load Balancing für Ihre Elastic Load Balancer (ELBs), um eine angemessene Kapazität und Verfügbarkeit aufrechtzuerhalten. Zonenübergreifendes Load Balancing reduziert die Notwendigkeit, die gleiche Anzahl von Instances in jeder aktivierten Availability Zone aufrechtzuerhalten. Dadurch wird auch die Fähigkeit Ihrer Anwendung verbessert, den Verlust einer oder mehrerer Instances zu bewältigen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CP-2.E	CP-2.E Notfallplan	elb-deletion-protection-enabled	Diese Regel sorgt dafür, dass der Löschschutz für Elastic Load Balancing aktiviert ist. Verwenden Sie diese Funktion, um zu verhindern, dass Ihr Load Balancer versehentlich oder böswillig gelöscht wird, was zum Verlust der Verfügbarkeit Ihrer Anwendungen führen kann.
CCCS-fPBMM-CP-2.E	CP-2.E Notfallplan	rds-cluster-deletion-protection-aktiviert	Stellen Sie sicher, dass Amazon Relational Database Service (Amazon RDS)-Instances den Löschschutz aktiviert haben. Verwenden Sie den Löschschutz, um zu verhindern, dass Ihre Amazon-RDS-Instances versehentlich oder böswillig gelöscht werden, was zum Verlust der Verfügbarkeit Ihrer Anwendungen führen kann.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CP-2.E	CP-2.E Notfallplan	rds-cluster-multi-az-aktiviert	Für Cluster von Amazon Relational Database Service (Amazon RDS) sollte die Multi-AZ-Replikation aktiviert sein, um die Verfügbarkeit der gespeicherten Daten zu gewährleisten. Availability Zones werden auf einer physisch getrennten, unabhängigen Infrastruktur ausgeführt und sind auf höchste Zuverlässigkeit ausgelegt. Im Falle eines Infrastrukturausfalls führt Amazon RDS einen automatischen Failover zum Standby-Modus durch, sodass Sie den Datenbankbetrieb wieder aufnehmen können, sobald der Failover abgeschlossen ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CP-2.E	CP-2.E Notfallplan	rds-instance-deletion-protection-aktiviert	Stellen Sie sicher, dass Amazon Relational Database Service (Amazon RDS)-Instances den Löschschutz aktiviert haben. Verwenden Sie den Löschschutz, um zu verhindern, dass Ihre Amazon-RDS-Instances versehentlich oder böswillig gelöscht werden, was zum Verlust der Verfügbarkeit Ihrer Anwendungen führen kann.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CP-2.E	CP-2.E Notfallplan	rds-multi-az-support	Die Multi-AZ-Unterstützung in Amazon Relational Database Service (Amazon RDS) bietet eine verbesserte Verfügbarkeit und Beständigkeit von Datenbank-Instances. Wenn Sie eine Multi-AZ-Datenbank-Instance bereitstellen, erstellt Amazon RDS automatisch eine primäre Datenbank-Instance und repliziert die Daten synchron auf eine Standby-Instance in einer anderen Availability Zone. Jede Availability Zone läuft auf einer eigenen, physisch getrennten, unabhängigen Infrastruktur und ist auf eine hohe Verfügbarkeit ausgelegt. Im Falle eines Infrastrukturausfalls führt Amazon RDS einen automatis

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
			chen Failover zum Standby-Modus durch, sodass Sie den Datenbankbetrieb wieder aufnehmen können, sobald der Failover abgeschlo ssen ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CP-2.E	CP-2.E Notfallplan	vpc-vpn-2-tunnels-up	Redundante Site-to-Site VPN-Tunnel können implementiert werden, um die Anforderungen an die Ausfallsicherheit zu erfüllen. Es verwendet zwei Tunnel, um die Konnektivität sicherzustellen, falls eine der Site-to-Site VPN-Verbindungen nicht verfügbar ist. Um sich vor einem Verbindungsverlust zu schützen, können Sie für den Fall, dass Ihr Kunden-Gateway nicht verfügbar ist, eine zweite Site-to-Site VPN-Verbindung zu Ihrer Amazon Virtual Private Cloud (Amazon VPC) und Ihrem Virtual Private Gateway einrichten, indem Sie ein zweites Kunden-Gateway verwenden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CP-2.F	CP-2.F Notfallplan	dynamodb-autoscaling-enabled	Amazon DynamoDB Auto Scaling verwendet den AWS Application Auto Scaling-Service, um die bereitgestellte Durchsatzkapazität so anzupassen, dass sie automatisch auf tatsächliche Verkehrsmuster reagiert. Auf diese Weise kann eine Tabelle oder ein globaler sekundärer Index die bereitgestellte Lese-/Schreibkapazität erhöhen, um plötzliche Erhöhungen des Datenverkehrs ohne Drosselung zu bewältigen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CP-2.F	CP-2.F Notfallplan	elb-cross-zone-load-Balancing aktiviert	Aktivieren Sie zonenübergreifendes Load Balancing für Ihre Elastic Load Balancer (ELBs), um eine angemessene Kapazität und Verfügbarkeit aufrechtzuerhalten. Zonenübergreifendes Load Balancing reduziert die Notwendigkeit, die gleiche Anzahl von Instances in jeder aktivierten Availability Zone aufrechtzuerhalten. Dadurch wird auch die Fähigkeit Ihrer Anwendung verbessert, den Verlust einer oder mehrerer Instances zu bewältigen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CP-2.F	CP-2.F Notfallplan	elb-deletion-protection-enabled	Diese Regel sorgt dafür, dass der Löschschutz für Elastic Load Balancing aktiviert ist. Verwenden Sie diese Funktion, um zu verhindern, dass Ihr Load Balancer versehentlich oder böswillig gelöscht wird, was zum Verlust der Verfügbarkeit Ihrer Anwendungen führen kann.
CCCS-fPBMM-CP-2.F	CP-2.F Notfallplan	rds-cluster-deletion-protection-aktiviert	Stellen Sie sicher, dass Amazon Relational Database Service (Amazon RDS)-Instances den Löschschutz aktiviert haben. Verwenden Sie den Löschschutz, um zu verhindern, dass Ihre Amazon-RDS-Instances versehentlich oder böswillig gelöscht werden, was zum Verlust der Verfügbarkeit Ihrer Anwendungen führen kann.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CP-2.F	CP-2.F Notfallplan	rds-cluster-multi-az-aktiviert	Für Cluster von Amazon Relational Database Service (Amazon RDS) sollte die Multi-AZ-Replikation aktiviert sein, um die Verfügbarkeit der gespeicherten Daten zu gewährleisten. Availability Zones werden auf einer physisch getrennten, unabhängigen Infrastruktur ausgeführt und sind auf höchste Zuverlässigkeit ausgelegt. Im Falle eines Infrastrukturausfalls führt Amazon RDS einen automatischen Failover zum Standby-Modus durch, sodass Sie den Datenbankbetrieb wieder aufnehmen können, sobald der Failover abgeschlossen ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CP-2.F	CP-2.F Notfallplan	rds-instance-deletion-protection-aktiviert	Stellen Sie sicher, dass Amazon Relational Database Service (Amazon RDS)-Instances den Löschschutz aktiviert haben. Verwenden Sie den Löschschutz, um zu verhindern, dass Ihre Amazon-RDS-Instances versehentlich oder böswillig gelöscht werden, was zum Verlust der Verfügbarkeit Ihrer Anwendungen führen kann.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CP-2.F	CP-2.F Notfallplan	rds-multi-az-support	Die Multi-AZ-Unterstützung in Amazon Relational Database Service (Amazon RDS) bietet eine verbesserte Verfügbarkeit und Beständigkeit von Datenbank-Instances. Wenn Sie eine Multi-AZ-Datenbank-Instance bereitstellen, erstellt Amazon RDS automatisch eine primäre Datenbank-Instance und repliziert die Daten synchron auf eine Standby-Instance in einer anderen Availability Zone. Jede Availability Zone läuft auf einer eigenen, physisch getrennten, unabhängigen Infrastruktur und ist auf eine hohe Verfügbarkeit ausgelegt. Im Falle eines Infrastrukturausfalls führt Amazon RDS einen automatis

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
			chen Failover zum Standby-Modus durch, sodass Sie den Datenbankbetrieb wieder aufnehmen können, sobald der Failover abgeschlo ssen ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CP-2.F	CP-2.F Notfallplan	vpc-vpn-2-tunnels-up	Redundante Site-to-Site VPN-Tunnel können implementiert werden, um die Anforderungen an die Ausfallsicherheit zu erfüllen. Es verwendet zwei Tunnel, um die Konnektivität sicherzustellen, falls eine der Site-to-Site VPN-Verbindungen nicht verfügbar ist. Um sich vor einem Verbindungsverlust zu schützen, können Sie für den Fall, dass Ihr Kunden-Gateway nicht verfügbar ist, eine zweite Site-to-Site VPN-Verbindung zu Ihrer Amazon Virtual Private Cloud (Amazon VPC) und Ihrem Virtual Private Gateway einrichten, indem Sie ein zweites Kunden-Gateway verwenden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CP-2.G	CP-2.G Notfallplan	dynamodb-autoscaling-enabled	Amazon DynamoDB Auto Scaling verwendet den AWS Application Auto Scaling-Service, um die bereitgestellte Durchsatzkapazität so anzupassen, dass sie automatisch auf tatsächliche Verkehrsmuster reagiert. Auf diese Weise kann eine Tabelle oder ein globaler sekundärer Index die bereitgestellte Lese-/Schreibkapazität erhöhen, um plötzliche Erhöhungen des Datenverkehrs ohne Drosselung zu bewältigen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CP-2.G	CP-2.G Notfallplan	elb-cross-zone-load-Balancing aktiviert	Aktivieren Sie zonenübergreifendes Load Balancing für Ihre Elastic Load Balancer (ELBs), um eine angemessene Kapazität und Verfügbarkeit aufrechtzuerhalten. Zonenübergreifendes Load Balancing reduziert die Notwendigkeit, die gleiche Anzahl von Instances in jeder aktivierten Availability Zone aufrechtzuerhalten. Dadurch wird auch die Fähigkeit Ihrer Anwendung verbessert, den Verlust einer oder mehrerer Instances zu bewältigen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CP-2.G	CP-2.G Notfallplan	elb-deletion-protection-enabled	Diese Regel sorgt dafür, dass der Löschschutz für Elastic Load Balancing aktiviert ist. Verwenden Sie diese Funktion, um zu verhindern, dass Ihr Load Balancer versehentlich oder böswillig gelöscht wird, was zum Verlust der Verfügbarkeit Ihrer Anwendungen führen kann.
CCCS-fPBMM-CP-2.G	CP-2.G Notfallplan	rds-cluster-deletion-protection-aktiviert	Stellen Sie sicher, dass Amazon Relational Database Service (Amazon RDS)-Instances den Löschschutz aktiviert haben. Verwenden Sie den Löschschutz, um zu verhindern, dass Ihre Amazon-RDS-Instances versehentlich oder böswillig gelöscht werden, was zum Verlust der Verfügbarkeit Ihrer Anwendungen führen kann.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CP-2.G	CP-2.G Notfallplan	rds-cluster-multi-az-aktiviert	Für Cluster von Amazon Relational Database Service (Amazon RDS) sollte die Multi-AZ-Replikation aktiviert sein, um die Verfügbarkeit der gespeicherten Daten zu gewährleisten. Availability Zones werden auf einer physisch getrennten, unabhängigen Infrastruktur ausgeführt und sind auf höchste Zuverlässigkeit ausgelegt. Im Falle eines Infrastrukturausfalls führt Amazon RDS einen automatischen Failover zum Standby-Modus durch, sodass Sie den Datenbankbetrieb wieder aufnehmen können, sobald der Failover abgeschlossen ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CP-2.G	CP-2.G Notfallplan	rds-instance-deletion-protection-aktiviert	Stellen Sie sicher, dass Amazon Relational Database Service (Amazon RDS)-Instances den Löschschutz aktiviert haben. Verwenden Sie den Löschschutz, um zu verhindern, dass Ihre Amazon-RDS-Instances versehentlich oder böswillig gelöscht werden, was zum Verlust der Verfügbarkeit Ihrer Anwendungen führen kann.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CP-2.G	CP-2.G Notfallplan	rds-multi-az-support	Die Multi-AZ-Unterstützung in Amazon Relational Database Service (Amazon RDS) bietet eine verbesserte Verfügbarkeit und Beständigkeit von Datenbank-Instances. Wenn Sie eine Multi-AZ-Datenbank-Instance bereitstellen, erstellt Amazon RDS automatisch eine primäre Datenbank-Instance und repliziert die Daten synchron auf eine Standby-Instance in einer anderen Availability Zone. Jede Availability Zone läuft auf einer eigenen, physisch getrennten, unabhängigen Infrastruktur und ist auf eine hohe Verfügbarkeit ausgelegt. Im Falle eines Infrastrukturausfalls führt Amazon RDS einen automatis

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
			chen Failover zum Standby-Modus durch, sodass Sie den Datenbankbetrieb wieder aufnehmen können, sobald der Failover abgeschlo ssen ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CP-2.G	CP-2.G Notfallplan	vpc-vpn-2-tunnels-up	Redundante Site-to-Site VPN-Tunnel können implementiert werden, um die Anforderungen an die Ausfallsicherheit zu erfüllen. Es verwendet zwei Tunnel, um die Konnektivität sicherzustellen, falls eine der Site-to-Site VPN-Verbindungen nicht verfügbar ist. Um sich vor einem Verbindungsverlust zu schützen, können Sie für den Fall, dass Ihr Kunden-Gateway nicht verfügbar ist, eine zweite Site-to-Site VPN-Verbindung zu Ihrer Amazon Virtual Private Cloud (Amazon VPC) und Ihrem Virtual Private Gateway einrichten, indem Sie ein zweites Kunden-Gateway verwenden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CP-6(1)	CP-6(1) Alternativer Speicherort | Trennung vom primären Standort	aurora-resources-protected-by-Backup-Plan	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon Aurora Aurora-Ressourcen Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CP-6(1)	CP-6(1) Alternativer Speicherort | Trennung vom primären Standort	backup-plan-min-frequency-and-min-retention-check	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihr AWS Backup-Plan auf eine Mindestfrequenz und Aufbewahrung festgelegt ist. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen. Mit dieser Regel können Sie die Parameter requiredFrequencyValue (Config default: 1), requiredRetentionDays (Config default: 35) und requiredFrequencyUnit

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
			(Config default: days) festlegen. Der tatsächliche Wert muss den Anforderungen Ihrer Organisation entsprechen.
CCCS-fPBMM-CP-6(1)	CP-6(1) Alternativer Speicherort | Trennung vom primären Standort	backup-recovery-point-encrypted	Stellen Sie sicher, dass die Verschlüsselung für Ihre AWS Backup-Wiederherstellungspunkte aktiviert ist. Da sensible Daten auch im Ruhezustand vorhanden sein können, sollten Sie die Verschlüsselung im Ruhezustand aktivieren, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CP-6(1)	CP-6(1) Alternativer Speicherort | Trennung vom primären Standort	backup-recovery-point-manual-Löschen-deaktiviert	Stellen Sie sicher, dass Ihren AWS Backup-Wiederherstellungspunkten eine ressourcenbasierte Richtlinie zugeordnet ist, die das Löschen von Wiederherstellungspunkten verhindert. Die Verwendung einer ressourcenbasierten Richtlinie zur Verhinderung des Löschens von Wiederherstellungspunkten kann dazu beitragen, ein versehentliches oder absichtliches Löschen zu unterbinden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CP-6(1)	CP-6(1) Alternativer Speicherort | Trennung vom primären Standort	backup-recovery-point-minimum-Aufbewahrungsprüfung	Um bei Datensicherungsprozessen zu helfen, stellen Sie sicher, dass für Ihre AWS Backup-Wiederherstellungspunkte eine Mindestaufbewahrungsdauer festgelegt ist. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen. Mit dieser Regel können Sie den Parameter requiredRetentionDays (Standardkonfiguration: 35) festlegen. Der tatsächliche Wert muss den Anforderu

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
			ngen Ihrer Organisation entsprechen.
CCCS-fPBMM-CP-6(1)	CP-6(1) Alternativer Speicherort | Trennung vom primären Standort	db-instance-backup-enabled	Die Sicherungsfunktion von Amazon RDS erstellt Sicherungen Ihrer Datenbanken und Transaktionsprotokolle. Amazon RDS erstellt einen Snapshot für das Speichervolume Ihrer DB-Instance, sodass die gesamte DB-Instance gesichert wird. Sie können im System spezifische Aufbewahrungsfristen festlegen, um Ihre Ausfallsicherheitsanforderungen zu erfüllen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CP-6(1)	CP-6(1) Alternativer Speicherort | Trennung vom primären Standort	dynamodb-resources-protected-by-Backup-Plan	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon DynamoDB DynamoDB-Ressourcen Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CP-6(1)	CP-6(1) Alternativer Speicherort | Trennung vom primären Standort	ebs-resources-protected-by-Backup-Plan	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon Elastic Block Store (Amazon EBS) -Ressourcen Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihre Backup-Verwaltung und ermöglicht es Ihnen, Ihre geschäftlichen und behördlichen Anforderungen bezüglich Backups zu erfüllen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CP-6(1)	CP-6(1) Alternativer Speicherort | Trennung vom primären Standort	ec2--Plan resources-protected-by-backup	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon Elastic Compute Cloud (Amazon EC2) -Ressourcen Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CP-6(1)	CP-6(1) Alternativer Speicherort | Trennung vom primären Standort	efs-resources-protected-by-Backup-Plan	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon Elastic File System (Amazon EFS) -Dateisysteme Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CP-6(1)	CP-6(1) Alternativer Speicherort | Trennung vom primären Standort	elasticache-redis-cluster-automatic-Backup-Check	Wenn automatische Backups aktiviert sind, ElastiCache erstellt Amazon täglich ein Backup des Clusters. Die Sicherung kann für eine von Ihrer Organisation festgelegte Anzahl von Tagen aufbewahrt werden. Automatische Backups schützen vor Datenverlust. Bei einem Ausfall können Sie einen neuen Cluster erstellen, der Ihre Daten aus dem aktuellen Backup wiederherstellt.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CP-6(1)	CP-6(1) Alternativer Speicherort | Trennung vom primären Standort	fsx-resources-protected-by-Backup-Plan	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre FSx Amazon-Dateisysteme Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CP-6(1)	CP-6(1) Alternativer Speicherort | Trennung vom primären Standort	multi-region-cloudtrail-enabled	AWS CloudTrail zeichnet Aktionen und API-Aufrufe der AWS Management Console auf. Sie können feststellen, welche Benutzer und Konten angerufen wurden AWS, von welcher Quell-IP-Adresse aus die Anrufe getätigt wurden und wann die Anrufe erfolgten. CloudTrail übermittelt Protokolldateien aus allen AWS Regionen an Ihren S3-Bucket, wenn MULTI_REGION_CLOUD_TRAIL_ENABLED aktiviert ist. Außerdem wird beim AWS Start einer neuen Region derselbe Trail in der neuen Region erstellt. CloudTrail Dadurch erhalten Sie automatisch Protokolldateien mit API-Aktivitäten für die neue Region.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CP-6(1)	CP-6(1) Alternativer Speicherort | Trennung vom primären Standort	rds-resources-protected-by-Backup-Plan	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon Relational Database Service (Amazon RDS) -Ressourcen Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CP-6(1)	CP-6(1) Alternativer Speicherort | Trennung vom primären Standort	redshift-backup-enabled	Stellen Sie zur Unterstützung der Datensicherungsprozesse sicher, dass Ihre Amazon-Redshift-Cluster über automatisierte Snapshots verfügen. Wenn automatisierte Snapshots für einen Cluster aktiviert sind, erstellt Redshift in regelmäßigen Abständen Snapshots dieses Clusters. Standardmäßig erstellt Redshift alle acht Stunden oder alle 5 GB einen Snapshot für jeden Knoten mit Datenänderungen oder je nachdem, was zuerst eintritt.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CP-6(1)	CP-6(1) Alternativer Speicherort | Trennung vom primären Standort	s3- bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) unterstützt die Aufrechterhaltung einer angemessenen Kapazität und Verfügbarkeit. CRR ermöglicht das automatische, asynchrone Kopieren von Objekten in Amazon-S3-Buckets, um die Datenverfügbarkeit sicherzustellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CP-6(1)	CP-6(1) Alternativer Speicherort | Trennung vom primären Standort	s-3 bucket-versioning-enabled	Die Versionsverwaltung von Amazon Simple Storage Service (Amazon S3)-Buckets hilft dabei, mehrere Varianten eines Objekts im selben Amazon-S3-Bucket zu speichern. Verwenden Sie die Versionsverwaltung, um sämtliche Versionen aller Objekte in Ihrem Amazon-S3-Bucket zu speichern, abzurufen oder wiederherzustellen. Mit der Versionsverwaltung können Sie Versionen sowohl nach unbeabsichtigten Benutzeraktionen als auch nach Anwendungsfehlern problemlos wiederherstellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CP-6(2)	CP-6(2) Alternativer Speicherort | Recovery Times/Recovery Point Objectives	aurora-resources-protected-by-Ersatzplan	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon Aurora Aurora-Ressourcen Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CP-6(2)	CP-6(2) Alternativer Speicherort | Recovery Times/Recovery Point Objectives	backup-plan-min-frequency-and-min-retention-check	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihr AWS Backup-Plan auf eine Mindestfrequenz und Aufbewahrung festgelegt ist. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen. Mit dieser Regel können Sie die Parameter requiredFrequencyValue (Config default: 1), requiredRetentionDays (Config default: 35) und requiredFrequencyUnit

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
			(Config default: days) festlegen. Der tatsächliche Wert muss den Anforderungen Ihrer Organisation entsprechen.
CCCS-fPBMM-CP-6(2)	CP-6(2) Alternativer Speicherort | Recovery Times/Recovery Point Objectives	backup-recovery-point-encrypted	Stellen Sie sicher, dass die Verschlüsselung für Ihre AWS Backup-Wiederherstellungspunkte aktiviert ist. Da sensible Daten auch im Ruhezustand vorhanden sein können, sollten Sie die Verschlüsselung im Ruhezustand aktivieren, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CP-6(2)	CP-6(2) Alternativer Speicherort | Recovery Times/Recovery Point Objectives	backup-recovery-point-manual-Löschen-deaktiviert	Stellen Sie sicher, dass Ihren AWS Backup-Wiederherstellungspunkten eine ressourcenbasierte Richtlinie zugeordnet ist, die das Löschen von Wiederherstellungspunkten verhindert. Die Verwendung einer ressourcenbasierten Richtlinie zur Verhinderung des Löschens von Wiederherstellungspunkten kann dazu beitragen, ein versehentliches oder absichtliches Löschen zu unterbinden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CP-6(2)	CP-6(2) Alternativer Speicherort | Recovery Times/Recovery Point Objectives	backup-recovery-point-minimum-Aufbewahrungsprüfung	Um bei Datensicherungsprozessen zu helfen, stellen Sie sicher, dass für Ihre AWS Backup-Wiederherstellungspunkte eine Mindestaufbewahrungsdauer festgelegt ist. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen. Mit dieser Regel können Sie den Parameter requiredRetentionDays (Standardkonfiguration: 35) festlegen. Der tatsächliche Wert muss den Anforderu

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
			ngen Ihrer Organisation entsprechen.
CCCS-fPBMM-CP-6(2)	CP-6(2) Alternativer Speicherort | Recovery Times/Recovery Point Objectives	db-instance-backup-enabled	Die Sicherungsfunktion von Amazon RDS erstellt Sicherungen Ihrer Datenbanken und Transaktionsprotokolle. Amazon RDS erstellt einen Snapshot für das Speichervolume Ihrer DB-Instance, sodass die gesamte DB-Instance gesichert wird. Sie können im System spezifische Aufbewahrungsfristen festlegen, um Ihre Ausfallsicherheitsanforderungen zu erfüllen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CP-6(2)	CP-6(2) Alternativer Speicherort | Recovery Times/Recovery Point Objectives	dynamodb-resources-protected-by-Backup-Plan	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon DynamoDB DynamoDB-Ressourcen Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CP-6(2)	CP-6(2) Alternativer Speicherort | Recovery Times/Recovery Point Objectives	ebs-resources-protected-by-Backup-Plan	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon Elastic Block Store (Amazon EBS) -Ressourcen Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihre Backup-Verwaltung und ermöglicht es Ihnen, Ihre geschäftlichen und behördlichen Anforderungen bezüglich Backups zu erfüllen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CP-6(2)	CP-6(2) Alternativer Speicherort | Recovery Times/Recovery Point Objectives	ec2--Plan resources-protected-by-backup	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon Elastic Compute Cloud (Amazon EC2) -Ressourcen Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CP-6(2)	CP-6(2) Alternativer Speicherort | Recovery Times/Recovery Point Objectives	efs-resources-protected-by-Backup-Plan	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon Elastic File System (Amazon EFS) -Dateisysteme Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CP-6(2)	CP-6(2) Alternativer Speicherort | Recovery Times/Recovery Point Objectives	elasticache-redis-cluster-automatic-Backup-Check	Wenn automatische Backups aktiviert sind, ElastiCache erstellt Amazon täglich ein Backup des Clusters. Die Sicherung kann für eine von Ihrer Organisation festgelegte Anzahl von Tagen aufbewahrt werden. Automatische Backups schützen vor Datenverlust. Bei einem Ausfall können Sie einen neuen Cluster erstellen, der Ihre Daten aus dem aktuellen Backup wiederherstellt.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CP-6(2)	CP-6(2) Alternativer Speicherort | Recovery Times/Recovery Point Objectives	fsx-resources-protected-by-Backup-Plan	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre FSx Amazon-Dateisysteme Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CP-6(2)	CP-6(2) Alternativer Speicherort | Recovery Times/Recovery Point Objectives	multi-region-cloudtrail-enabled	AWS CloudTrail zeichnet Aktionen und API-Aufrufe der AWS Management Console auf. Sie können feststellen, welche Benutzer und Konten angerufen wurden AWS, von welcher Quell-IP-Adresse aus die Anrufe getätigt wurden und wann die Anrufe erfolgten. CloudTrail übermittelt Protokolldateien aus allen AWS Regionen an Ihren S3-Bucket, wenn MULTI_REGION_CLOUD_TRAIL_ENABLED aktiviert ist. Außerdem wird beim AWS Start einer neuen Region derselbe Trail in der neuen Region erstellt. CloudTrail Dadurch erhalten Sie automatisch Protokolldateien mit API-Aktivitäten für die neue Region.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CP-6(2)	CP-6(2) Alternativer Speicherort | Recovery Times/Recovery Point Objectives	rds-resources-protected-by-Backup-Plan	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon Relational Database Service (Amazon RDS) -Ressourcen Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CP-6(2)	CP-6(2) Alternativer Speicherort | Recovery Times/Recovery Point Objectives	redshift-backup-enabled	Stellen Sie zur Unterstützung der Datensicherungsprozesse sicher, dass Ihre Amazon-Redshift-Cluster über automatisierte Snapshots verfügen. Wenn automatisierte Snapshots für einen Cluster aktiviert sind, erstellt Redshift in regelmäßigen Abständen Snapshots dieses Clusters. Standardmäßig erstellt Redshift alle acht Stunden oder alle 5 GB einen Snapshot für jeden Knoten mit Datenänderungen oder je nachdem, was zuerst eintritt.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CP-6(2)	CP-6(2) Alternativer Speicherort | Recovery Times/Recovery Point Objectives	s3- bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) unterstützt die Aufrechterhaltung einer angemessenen Kapazität und Verfügbarkeit. CRR ermöglicht das automatische, asynchrone Kopieren von Objekten in Amazon-S3-Buckets, um die Datenverfügbarkeit sicherzustellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CP-6(2)	CP-6(2) Alternativer Speicherort | Recovery Times/Recovery Point Objectives	s-3 bucket-versioning-enabled	Die Versionsverwaltung von Amazon Simple Storage Service (Amazon S3)-Buckets hilft dabei, mehrere Varianten eines Objekts im selben Amazon-S3-Bucket zu speichern. Verwenden Sie die Versionsverwaltung, um sämtliche Versionen aller Objekte in Ihrem Amazon-S3-Bucket zu speichern, abzurufen oder wiederherzustellen. Mit der Versionsverwaltung können Sie Versionen sowohl nach unbeabsichtigten Benutzeraktionen als auch nach Anwendungsfehlern problemlos wiederherstellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CP-6.A	CP-6.A Alternativer Speicherort	aurora-resources-protected-by-Ersatzplan	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon Aurora Aurora-Ressourcen Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CP-6.A	CP-6.A Alternativer Speicherort	backup-plan-min-frequency-and-min-retention-check	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihr AWS Backup-Plan auf eine Mindestfrequenz und Aufbewahrung festgelegt ist. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen. Mit dieser Regel können Sie die Parameter requiredFrequencyValue (Config default: 1), requiredRetentionDays (Config default: 35) und requiredFrequencyUnit

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
			(Config default: days) festlegen. Der tatsächliche Wert muss den Anforderungen Ihrer Organisation entsprechen.
CCCS-fPBMM-CP-6.A	CP-6.A Alternativer Speicherort	backup-recovery-point-encrypted	Stellen Sie sicher, dass die Verschlüsselung für Ihre AWS Backup-Wiederherstellungspunkte aktiviert ist. Da sensible Daten auch im Ruhezustand vorhanden sein können, sollten Sie die Verschlüsselung im Ruhezustand aktivieren, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CP-6.A	CP-6.A Alternativer Speicherort	backup-recovery-point-manual-Löschen-deaktiviert	Stellen Sie sicher, dass Ihren AWS Backup-Wiederherstellungspunkten eine ressourcenbasierte Richtlinie zugeordnet ist, die das Löschen von Wiederherstellungspunkten verhindert. Die Verwendung einer ressourcenbasierten Richtlinie zur Verhinderung des Löschens von Wiederherstellungspunkten kann dazu beitragen, ein versehentliches oder absichtliches Löschen zu unterbinden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CP-6.A	CP-6.A Alternativer Speicherort	backup-recovery-point-minimum-Aufbewahrungsprüfung	Um bei Datensicherungsprozessen zu helfen, stellen Sie sicher, dass für Ihre AWS Backup-Wiederherstellungspunkte eine Mindestaufbewahrungsdauer festgelegt ist. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen. Mit dieser Regel können Sie den Parameter requiredRetentionDays (Standardkonfiguration: 35) festlegen. Der tatsächliche Wert muss den Anforderu

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
			ngen Ihrer Organisation entsprechen.
CCCS-fPBMM-CP-6.A	CP-6.A Alternativer Speicherort	db-instance-backup-enabled	Die Sicherungsfunktion von Amazon RDS erstellt Sicherungen Ihrer Datenbanken und Transaktionsprotokolle. Amazon RDS erstellt einen Snapshot für das Speichervolume Ihrer DB-Instance, sodass die gesamte DB-Instance gesichert wird. Sie können im System spezifische Aufbewahrungsfristen festlegen, um Ihre Ausfallsicherheitsanforderungen zu erfüllen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CP-6.A	CP-6.A Alternativer Speicherort	dynamodb-resources-protected-by-Backup-Plan	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon DynamoDB DynamoDB-Ressourcen Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CP-6.A	CP-6.A Alternativer Speicherort	ebs-resources-protected-by-Backup-Plan	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon Elastic Block Store (Amazon EBS) -Ressourcen Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihre Backup-Verwaltung und ermöglicht es Ihnen, Ihre geschäftlichen und behördlichen Anforderungen bezüglich Backups zu erfüllen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CP-6.A	CP-6.A Alternativer Speicherort	ec2--Plan resources-protected-by-backup	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon Elastic Compute Cloud (Amazon EC2) -Ressourcen Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CP-6.A	CP-6.A Alternativer Speicherort	efs-resources-protected-by-Backup-Plan	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon Elastic File System (Amazon EFS) -Dateisysteme Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CP-6.A	CP-6.A Alternativer Speicherort	elasticache-redis-cluster-automatic-Backup-Check	Wenn automatische Backups aktiviert sind, ElastiCache erstellt Amazon täglich ein Backup des Clusters. Die Sicherung kann für eine von Ihrer Organisation festgelegte Anzahl von Tagen aufbewahrt werden. Automatische Backups schützen vor Datenverlust. Bei einem Ausfall können Sie einen neuen Cluster erstellen, der Ihre Daten aus dem aktuellen Backup wiederherstellt.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CP-6.A	CP-6.A Alternativer Speicherort	fsx-resources-protected-by-Backup-Plan	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre FSx Amazon-Dateisysteme Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CP-6.A	CP-6.A Alternativer Speicherort	multi-region-cloudtrail-enabled	AWS CloudTrail zeichnet Aktionen und API-Aufrufe der AWS Management Console auf. Sie können feststellen, welche Benutzer und Konten angerufen wurden AWS, von welcher Quell-IP-Adresse aus die Anrufe getätigt wurden und wann die Anrufe erfolgten. CloudTrail übermittelt Protokolldateien aus allen AWS Regionen an Ihren S3-Bucket , wenn MULTI_REGION_CLOUD_TRAIL_ENABLED aktiviert ist. Außerdem wird beim AWS Start einer neuen Region derselbe Trail in der neuen Region erstellt. CloudTrail Dadurch erhalten Sie automatisch Protokolldateien mit API-Aktivitäten für die neue Region.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CP-6.A	CP-6.A Alternativer Speicherort	rds-resources-protected-by-Backup-Plan	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon Relational Database Service (Amazon RDS) -Ressourcen Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CP-6.A	CP-6.A Alternativer Speicherort	redshift-backup-enabled	Stellen Sie zur Unterstützung der Datensicherungsprozesse sicher, dass Ihre Amazon-Redshift-Cluster über automatisierte Snapshots verfügen. Wenn automatisierte Snapshots für einen Cluster aktiviert sind, erstellt Redshift in regelmäßigen Abständen Snapshots dieses Clusters. Standardmäßig erstellt Redshift alle acht Stunden oder alle 5 GB einen Snapshot für jeden Knoten mit Datenänderungen oder je nachdem, was zuerst eintritt.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CP-6.A	CP-6.A Alternativer Speicherort	s3- bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) unterstützt die Aufrechterhaltung einer angemesse nen Kapazität und Verfügbarkeit. CRR ermöglicht das automatische, asynchrone Kopieren von Objekten in Amazon-S3-Buckets, um die Datenverf ügbarkeit sicherzus tellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CP-6.A	CP-6.A Alternativer Speicherort	s-3 bucket-versioning-enabled	Die Versionsv erwaltung von Amazon Simple Storage Service (Amazon S3)-Bucke ts hilft dabei, mehrere Varianten eines Objekts im selben Amazon-S3-Bucket zu speichern. Verwenden Sie die Versionsv erwaltung, um sämtliche Versionen aller Objekte in Ihrem Amazon-S3-Bucket zu speichern , abzurufen oder wiederherzustellen . Mit der Versionsv erwaltung können Sie Versionen sowohl nach unbeabsic htigten Benutzera ktionen als auch nach Anwendungsfehlern problemlos wiederher stellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CP-6.B	CP-6.B Alternativer Speicherort	aurora-resources-protected-by-Ersatzplan	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon Aurora Aurora-Ressourcen Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CP-6.B	CP-6.B Alternativer Speicherort	backup-plan-min-frequency-and-min-retention-check	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihr AWS Backup-Plan auf eine Mindestfrequenz und Aufbewahrung festgelegt ist. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen. Mit dieser Regel können Sie die Parameter requiredFrequencyValue (Config default: 1), requiredRetentionDays (Config default: 35) und requiredFrequencyUnit

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
			(Config default: days) festlegen. Der tatsächliche Wert muss den Anforderungen Ihrer Organisation entsprechen.
CCCS-fPBMM-CP-6.B	CP-6.B Alternativer Speicherort	backup-recovery-point-encrypted	Stellen Sie sicher, dass die Verschlüsselung für Ihre AWS Backup-Wiederherstellungspunkte aktiviert ist. Da sensible Daten auch im Ruhezustand vorhanden sein können, sollten Sie die Verschlüsselung im Ruhezustand aktivieren, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CP-6.B	CP-6.B Alternativer Speicherort	backup-recovery-point-manual-Löschen-deaktiviert	Stellen Sie sicher, dass Ihren AWS Backup-Wiederherstellungspunkten eine ressourcenbasierte Richtlinie zugeordnet ist, die das Löschen von Wiederherstellungspunkten verhindert. Die Verwendung einer ressourcenbasierten Richtlinie zur Verhinderung des Löschens von Wiederherstellungspunkten kann dazu beitragen, ein versehentliches oder absichtliches Löschen zu unterbinden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CP-6.B	CP-6.B Alternativer Speicherort	backup-recovery-point-minimum-Aufbewahrungsprüfung	Um bei Datensicherungsprozessen zu helfen, stellen Sie sicher, dass für Ihre AWS Backup-Wiederherstellungspunkte eine Mindestaufbewahrungsdauer festgelegt ist. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen. Mit dieser Regel können Sie den Parameter requiredRetentionDays (Standardkonfiguration: 35) festlegen. Der tatsächliche Wert muss den Anforderu

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
			ngen Ihrer Organisation entsprechen.
CCCS-fPBMM-CP-6.B	CP-6.B Alternativer Speicherort	db-instance-backup-enabled	Die Sicherungsfunktion von Amazon RDS erstellt Sicherungen Ihrer Datenbanken und Transaktionsprotokolle. Amazon RDS erstellt einen Snapshot für das Speichervolume Ihrer DB-Instance, sodass die gesamte DB-Instance gesichert wird. Sie können im System spezifische Aufbewahrungsfristen festlegen, um Ihre Ausfallsicherheitsanforderungen zu erfüllen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CP-6.B	CP-6.B Alternativer Speicherort	dynamodb-resources-protected-by-Backup-Plan	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon DynamoDB DynamoDB-Ressourcen Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CP-6.B	CP-6.B Alternativer Speicherort	ebs-resources-protected-by-Backup-Plan	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon Elastic Block Store (Amazon EBS) -Ressourcen Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihre Backup-Verwaltung und ermöglicht es Ihnen, Ihre geschäftlichen und behördlichen Anforderungen bezüglich Backups zu erfüllen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CP-6.B	CP-6.B Alternativer Speicherort	ec2--Plan resources-protected-by-backup	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon Elastic Compute Cloud (Amazon EC2) -Ressourcen Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CP-6.B	CP-6.B Alternativer Speicherort	efs-resources-protected-by-Backup-Plan	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon Elastic File System (Amazon EFS) -Dateisysteme Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CP-6.B	CP-6.B Alternativer Speicherort	elasticache-redis-cluster-automatic-Backup-Check	Wenn automatische Backups aktiviert sind, ElastiCache erstellt Amazon täglich ein Backup des Clusters. Die Sicherung kann für eine von Ihrer Organisation festgelegte Anzahl von Tagen aufbewahrt werden. Automatische Backups schützen vor Datenverlust. Bei einem Ausfall können Sie einen neuen Cluster erstellen, der Ihre Daten aus dem aktuellen Backup wiederherstellt.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CP-6.B	CP-6.B Alternativer Speicherort	fsx-resources-protected-by-Backup-Plan	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre FSx Amazon-Dateisysteme Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CP-6.B	CP-6.B Alternativer Speicherort	multi-region-cloudtrail-enabled	AWS CloudTrail zeichnet Aktionen und API-Aufrufe der AWS Management Console auf. Sie können feststellen, welche Benutzer und Konten angerufen wurden AWS, von welcher Quell-IP-Adresse aus die Anrufe getätigt wurden und wann die Anrufe erfolgten. CloudTrail übermittelt Protokolldateien aus allen AWS Regionen an Ihren S3-Bucket , wenn MULTI_REGION_CLOUD_TRAIL_ENABLED aktiviert ist. Außerdem wird beim AWS Start einer neuen Region derselbe Trail in der neuen Region erstellt. CloudTrail Dadurch erhalten Sie automatisch Protokolldateien mit API-Aktivitäten für die neue Region.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CP-6.B	CP-6.B Alternativer Speicherort	rds-resources-protected-by-Backup-Plan	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon Relational Database Service (Amazon RDS) -Ressourcen Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CP-6.B	CP-6.B Alternativer Speicherort	redshift-backup-enabled	Stellen Sie zur Unterstützung der Datensicherungsprozesse sicher, dass Ihre Amazon-Redshift-Cluster über automatisierte Snapshots verfügen. Wenn automatisierte Snapshots für einen Cluster aktiviert sind, erstellt Redshift in regelmäßigen Abständen Snapshots dieses Clusters. Standardmäßig erstellt Redshift alle acht Stunden oder alle 5 GB einen Snapshot für jeden Knoten mit Datenänderungen oder je nachdem, was zuerst eintritt.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CP-6.B	CP-6.B Alternativer Speicherort	s3- bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) unterstützt die Aufrechterhaltung einer angemessenen Kapazität und Verfügbarkeit. CRR ermöglicht das automatische, asynchrone Kopieren von Objekten in Amazon-S3-Buckets, um die Datenverfügbarkeit sicherzustellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CP-6.B	CP-6.B Alternativer Speicherort	s-3 bucket-versioning-enabled	Die Versionsv erwaltung von Amazon Simple Storage Service (Amazon S3)-Bucke ts hilft dabei, mehrere Varianten eines Objekts im selben Amazon-S3-Bucket zu speichern. Verwenden Sie die Versionsv erwaltung, um sämtliche Versionen aller Objekte in Ihrem Amazon-S3-Bucket zu speichern , abzurufen oder wiederherzustellen . Mit der Versionsv erwaltung können Sie Versionen sowohl nach unbeabsic htigten Benutzera ktionen als auch nach Anwendungsfehlern problemlos wiederher stellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CP-9(3)	CP-9(3) Informationssystem-Backup | Separater Speicher für kritische Informationen	aurora-resources-protected-by-Ersatzplan	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon Aurora Aurora-Ressourcen Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CP-9(3)	CP-9(3) Informationssystem-Backup | Separater Speicher für kritische Informationen	backup-plan-min-frequency-and-min-retention-check	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihr AWS Backup-Plan auf eine Mindestfrequenz und Aufbewahrung festgelegt ist. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen. Mit dieser Regel können Sie die Parameter requiredFrequencyValue (Config default: 1), requiredRetentionDays (Config default: 35) und requiredFrequencyUnit

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
			(Config default: days) festlegen. Der tatsächliche Wert muss den Anforderungen Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CP-9(3)	CP-9(3) Informationssystem-Backup | Separater Speicher für kritische Informationen	backup-recovery-point-minimum-Aufbewahrungsprüfung	Um bei Datensicherungsprozessen zu helfen, stellen Sie sicher, dass für Ihre AWS Backup-Wiederherstellungspunkte eine Mindestaufbewahrungsdauer festgelegt ist. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen. Mit dieser Regel können Sie den Parameter requiredRetentionDays (Standardkonfiguration: 35) festlegen. Der tatsächliche Wert muss den Anforderu

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
			ngen Ihrer Organisation entsprechen.
CCCS-fPBMM-CP-9(3)	CP-9(3) Informationssystem-Backup | Separater Speicher für kritische Informationen	db-instance-backup-enabled	Die Sicherungsfunktion von Amazon RDS erstellt Sicherungen Ihrer Datenbanken und Transaktionsprotokolle. Amazon RDS erstellt einen Snapshot für das Speichervolume Ihrer DB-Instance, sodass die gesamte DB-Instance gesichert wird. Sie können im System spezifische Aufbewahrungsfristen festlegen, um Ihre Ausfallsicherheitsanforderungen zu erfüllen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CP-9(3)	CP-9(3) Informationssystem-Backup | Separater Speicher für kritische Informationen	dynamodb-pitr-enabled	Aktivieren Sie diese Regel, um zu überprüfen, ob die Informationen gesichert wurden. Es verwaltet auch die Backups, indem es sicherstellt, dass die point-in-time Wiederherstellung in Amazon DynamoDB aktiviert ist. Bei der Wiederherstellung werden fortlaufende Backups Ihrer Tabelle für die letzten 35 Tage gespeichert.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CP-9(3)	CP-9(3) Informationssystem-Backup | Separater Speicher für kritische Informationen	dynamodb-resources-protected-by-Backup-Plan	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon DynamoDB DynamoDB-Ressourcen Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CP-9(3)	CP-9(3) Informationssystem-Backup | Separater Speicher für kritische Informationen	ebs-optimized-instance	Eine optimierte Instance im Amazon Elastic Block Store (Amazon EBS) bietet zusätzliche, dedizierte Kapazität für Amazon-EBS-I/O-Vorgänge. Diese Optimierung bietet die beste Leistung für Ihr EBS-Volume, indem Konflikte zwischen Amazon-EBS-I/O und anderem Datenverkehr von Ihrer Instance minimiert werden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CP-9(3)	CP-9(3) Informationssystem-Backup | Separater Speicher für kritische Informationen	ebs-resources-protected-by-Backup-Plan	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon Elastic Block Store (Amazon EBS) -Ressourcen Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihre Backup-Verwaltung und ermöglicht es Ihnen, Ihre geschäftlichen und behördlichen Anforderungen bezüglich Backups zu erfüllen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CP-9(3)	CP-9(3) Informationssystem-Backup | Separater Speicher für kritische Informationen	ec2--Plan resources-protected-by-backup	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon Elastic Compute Cloud (Amazon EC2) -Ressourcen Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CP-9(3)	CP-9(3) Informationssystem-Backup | Separater Speicher für kritische Informationen	efs-resources-protected-by-Backup-Plan	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon Elastic File System (Amazon EFS) -Dateisysteme Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CP-9(3)	CP-9(3) Informationssystem-Backup | Separater Speicher für kritische Informationen	elasticache-redis-cluster-automatic-Backup-Check	Wenn automatische Backups aktiviert sind, ElastiCache erstellt Amazon täglich ein Backup des Clusters. Die Sicherung kann für eine von Ihrer Organisation festgelegte Anzahl von Tagen aufbewahrt werden. Automatische Backups schützen vor Datenverlust. Bei einem Ausfall können Sie einen neuen Cluster erstellen, der Ihre Daten aus dem aktuellen Backup wiederherstellt.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CP-9(3)	CP-9(3) Informationssystem-Backup | Separater Speicher für kritische Informationen	fsx-resources-protected-by-Backup-Plan	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre FSx Amazon-Dateisysteme Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CP-9(3)	CP-9(3) Informationssystem-Backup | Separater Speicher für kritische Informationen	rds-resources-protected-by-Backup-Plan	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon Relational Database Service (Amazon RDS) -Ressourcen Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CP-9(3)	CP-9(3) Informationssystem-Backup | Separater Speicher für kritische Informationen	redshift-backup-enabled	Stellen Sie zur Unterstützung der Datensicherungsprozesse sicher, dass Ihre Amazon-Redshift-Cluster über automatisierte Snapshots verfügen. Wenn automatisierte Snapshots für einen Cluster aktiviert sind, erstellt Redshift in regelmäßigen Abständen Snapshots dieses Clusters. Standardmäßig erstellt Redshift alle acht Stunden oder alle 5 GB einen Snapshot für jeden Knoten mit Datenänderungen oder je nachdem, was zuerst eintritt.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CP-9(3)	CP-9(3) Informationssystem-Backup | Separater Speicher für kritische Informationen	s3- bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) unterstützt die Aufrechterhaltung einer angemessenen Kapazität und Verfügbarkeit. CRR ermöglicht das automatische, asynchrone Kopieren von Objekten in Amazon-S3-Buckets, um die Datenverfügbarkeit sicherzustellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CP-9(3)	CP-9(3) Informationssystem-Backup | Separater Speicher für kritische Informationen	s-3 bucket-versioning-enabled	Die Versionsverwaltung von Amazon Simple Storage Service (Amazon S3)-Buckets hilft dabei, mehrere Varianten eines Objekts im selben Amazon-S3-Bucket zu speichern. Verwenden Sie die Versionsverwaltung, um sämtliche Versionen aller Objekte in Ihrem Amazon-S3-Bucket zu speichern, abzurufen oder wiederherzustellen. Mit der Versionsverwaltung können Sie Versionen sowohl nach unbeabsichtigten Benutzeraktionen als auch nach Anwendungsfehlern problemlos wiederherstellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CP-9(7)	CP-9(7) Informationssystem-Backup | Doppelte Autorisierung	backup-recovery-point-manual-Löschen-deaktiviert	Stellen Sie sicher, dass Ihren AWS Backup-Wiederherstellungspunkten eine ressourcenbasierte Richtlinie zugeordnet ist, die das Löschen von Wiederherstellungspunkten verhindert. Die Verwendung einer ressourcenbasierten Richtlinie zur Verhinderung des Löschens von Wiederherstellungspunkten kann dazu beitragen, ein versehentliches oder absichtliches Löschen zu unterbinden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CP-9(7)	CP-9(7) Informationssystem-Backup | Doppelte Autorisierung	s-3 bucket-versioning-enabled	Die Versionsverwaltung von Amazon Simple Storage Service (Amazon S3)-Buckets hilft dabei, mehrere Varianten eines Objekts im selben Amazon-S3-Bucket zu speichern. Verwenden Sie die Versionsverwaltung, um sämtliche Versionen aller Objekte in Ihrem Amazon-S3-Bucket zu speichern, abzurufen oder wiederherzustellen. Mit der Versionsverwaltung können Sie Versionen sowohl nach unbeabsichtigten Benutzeraktionen als auch nach Anwendungsfehlern problemlos wiederherstellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CP-9.A	CP-9.A Informationssystem-Backup	aurora-resources-protected-by-Ersatzplan	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon Aurora Aurora-Ressourcen Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CP-9.A	CP-9.A Informationssystem-Backup	backup-plan-min-frequency-and-min-retention-check	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihr AWS Backup-Plan auf eine Mindestfrequenz und Aufbewahrung festgelegt ist. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen. Mit dieser Regel können Sie die Parameter requiredFrequencyValue (Config default: 1), requiredRetentionDays (Config default: 35) und requiredFrequencyUnit

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
			(Config default: days) festlegen. Der tatsächliche Wert muss den Anforderungen Ihrer Organisation entsprechen.
CCCS-fPBMM-CP-9.A	CP-9.A Informationssystem-Backup	backup-recovery-point-encrypted	Stellen Sie sicher, dass die Verschlüsselung für Ihre AWS Backup-Wiederherstellungspunkte aktiviert ist. Da sensible Daten auch im Ruhezustand vorhanden sein können, sollten Sie die Verschlüsselung im Ruhezustand aktivieren, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CP-9.A	CP-9.A Informationssystem-Backup	backup-recovery-point-manual-Löschen-deaktiviert	Stellen Sie sicher, dass Ihren AWS Backup-Wiederherstellungspunkten eine ressourcenbasierte Richtlinie zugeordnet ist, die das Löschen von Wiederherstellungspunkten verhindert. Die Verwendung einer ressourcenbasierten Richtlinie zur Verhinderung des Löschens von Wiederherstellungspunkten kann dazu beitragen, ein versehentliches oder absichtliches Löschen zu unterbinden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CP-9.A	CP-9.A Informationssystem-Backup	backup-recovery-point-minimum-Aufbewahrungsprüfung	Um bei Datensicherungsprozessen zu helfen, stellen Sie sicher, dass für Ihre AWS Backup-Wiederherstellungspunkte eine Mindestaufbewahrungsdauer festgelegt ist. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen. Mit dieser Regel können Sie den Parameter requiredRetentionDays (Standardkonfiguration: 35) festlegen. Der tatsächliche Wert muss den Anforderu

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
			ngen Ihrer Organisation entsprechen.
CCCS-fPBMM-CP-9.A	CP-9.A Informationssystem-Backup	db-instance-backup-enabled	Die Sicherungsfunktion von Amazon RDS erstellt Sicherungen Ihrer Datenbanken und Transaktionsprotokolle. Amazon RDS erstellt einen Snapshot für das Speichervolume Ihrer DB-Instance, sodass die gesamte DB-Instance gesichert wird. Sie können im System spezifische Aufbewahrungsfristen festlegen, um Ihre Ausfallsicherheitsanforderungen zu erfüllen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CP-9.A	CP-9.A Informationssystem-Backup	dynamodb-pitr-enabled	Aktivieren Sie diese Regel, um zu überprüfen, ob die Informationen gesichert wurden. Es verwaltet auch die Backups, indem es sicherstellt, dass die point-in-time Wiederherstellung in Amazon DynamoDB aktiviert ist. Bei der Wiederherstellung werden fortlaufende Backups Ihrer Tabelle für die letzten 35 Tage gespeichert.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CP-9.A	CP-9.A Informationssystem-Backup	dynamodb-resources-protected-by-Backup-Plan	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon DynamoDB DynamoDB-Ressourcen Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CP-9.A	CP-9.A Informationssystem-Backup	ebs-optimized-instance	Eine optimierte Instance im Amazon Elastic Block Store (Amazon EBS) bietet zusätzliche, dedizierte Kapazität für Amazon-EBS-I/O-Vorgänge. Diese Optimierung bietet die beste Leistung für Ihr EBS-Volume, indem Konflikte zwischen Amazon-EBS-I/O und anderem Datenverkehr von Ihrer Instance minimiert werden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CP-9.A	CP-9.A Informationssystem-Backup	ebs-resources-protected-by-Backup-Plan	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon Elastic Block Store (Amazon EBS) -Ressourcen Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihre Backup-Verwaltung und ermöglicht es Ihnen, Ihre geschäftlichen und behördlichen Anforderungen bezüglich Backups zu erfüllen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CP-9.A	CP-9.A Informationssystem-Backup	ebs-snapshot-public-restorable-überprüfen	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass EBS-Snapshots nicht öffentlich wiederherstellbar sind. EBS-Volume-Snapshots können vertrauliche Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CP-9.A	CP-9.A Informationssystem-Backup	ec2--Plan resources-protected-by-backup	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon Elastic Compute Cloud (Amazon EC2) -Ressourcen Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CP-9.A	CP-9.A Informationssystem-Backup	efs-resources-protected-by-Backup-Plan	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon Elastic File System (Amazon EFS) -Dateisysteme Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CP-9.A	CP-9.A Informationssystem-Backup	elasticache-redis-cluster-automatic-Backup-Check	Wenn automatische Backups aktiviert sind, ElastiCache erstellt Amazon täglich ein Backup des Clusters. Die Sicherung kann für eine von Ihrer Organisation festgelegte Anzahl von Tagen aufbewahrt werden. Automatische Backups schützen vor Datenverlust. Bei einem Ausfall können Sie einen neuen Cluster erstellen, der Ihre Daten aus dem aktuellen Backup wiederherstellt.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CP-9.A	CP-9.A Informationssystem-Backup	fsx-resources-protected-by-Backup-Plan	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre FSx Amazon-Dateisysteme Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CP-9.A	CP-9.A Informationssystem-Backup	rds-resources-protected-by-Backup-Plan	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon Relational Database Service (Amazon RDS) -Ressourcen Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CP-9.A	CP-9.A Informationssystem-Backup	rds-snapshots-public-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Relational Database Service (Amazon RDS) -Instances nicht öffentlich sind. Amazon-RDS-Datenbank-Instances können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CP-9.A	CP-9.A Informationssystem-Backup	rds-snapshot-encrypted	Stellen Sie sicher, dass die Verschlüsselung für Ihre Amazon Relational Database Service (Amazon RDS)-Snapshots aktiviert ist. Da sensible Daten auch im Ruhezustand vorhanden sein können, sollten Sie die Verschlüsselung von Daten im Ruhezustand aktivieren, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CP-9.A	CP-9.A Informationssystem-Backup	redshift-backup-enabled	Stellen Sie zur Unterstützung der Datensicherungsprozesse sicher, dass Ihre Amazon-Redshift-Cluster über automatisierte Snapshots verfügen. Wenn automatisierte Snapshots für einen Cluster aktiviert sind, erstellt Redshift in regelmäßigen Abständen Snapshots dieses Clusters. Standardmäßig erstellt Redshift alle acht Stunden oder alle 5 GB einen Snapshot für jeden Knoten mit Datenänderungen oder je nachdem, was zuerst eintritt.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CP-9.A	CP-9.A Informationssystem-Backup	redshift-cluster-maintenancesettings-check	Diese Regel stellt sicher, dass Amazon-Redshift-Cluster die bevorzugten Einstellungen für Ihre Organisation haben. Insbesondere sorgt sie dafür, dass Cluster bevorzugte Wartungsfenster und automatisierte Aufbewahrungsfristen für Snapshots für die Datenbank haben. Für diese Regel müssen Sie die festlegen. allowVersionUpgrade Der Standardwert ist „true“. Außerdem können Sie optional den Zeitraum preferredMaintenanceWindow (der Standardwert ist sa: 16:00 -sa: 16:30) und den automated SnapshotRetention Zeitraum (der Standardwert ist 1) festlegen. Die tatsächlichen Werte müssen den Richtlini

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
			en Ihrer Organisation entsprechen.
CCCS-fPBMM-CP-9.A	CP-9.A Informationssystem-Backup	s3- bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) unterstützt die Aufrechterhaltung einer angemessenen Kapazität und Verfügbarkeit. CRR ermöglicht das automatische, asynchrone Kopieren von Objekten in Amazon-S3-Buckets, um die Datenverfügbarkeit sicherzustellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CP-9.A	CP-9.A Informationssystem-Backup	s-3 bucket-versioning-enabled	Die Versionsverwaltung von Amazon Simple Storage Service (Amazon S3)-Buckets hilft dabei, mehrere Varianten eines Objekts im selben Amazon-S3-Bucket zu speichern. Verwenden Sie die Versionsverwaltung, um sämtliche Versionen aller Objekte in Ihrem Amazon-S3-Bucket zu speichern, abzurufen oder wiederherzustellen. Mit der Versionsverwaltung können Sie Versionen sowohl nach unbeabsichtigten Benutzeraktionen als auch nach Anwendungsfehlern problemlos wiederherstellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CP-9.AA	CP-9.AA Informationssystem-Backup	aurora-resources-protected-by-Ersatzplan	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon Aurora Aurora-Ressourcen Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CP-9.AA	CP-9.AA Informationssystem-Backup	backup-plan-min-frequency-and-min-retention-check	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihr AWS Backup-Plan auf eine Mindestfrequenz und Aufbewahrung festgelegt ist. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen. Mit dieser Regel können Sie die Parameter requiredFrequencyValue (Config default: 1), requiredRetentionDays (Config default: 35) und requiredFrequencyUnit

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
			(Config default: days) festlegen. Der tatsächliche Wert muss den Anforderungen Ihrer Organisation entsprechen.
CCCS-fPBMM-CP-9.AA	CP-9.AA Informationssystem-Backup	backup-recovery-point-encrypted	Stellen Sie sicher, dass die Verschlüsselung für Ihre AWS Backup-Wiederherstellungspunkte aktiviert ist. Da sensible Daten auch im Ruhezustand vorhanden sein können, sollten Sie die Verschlüsselung im Ruhezustand aktivieren, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CP-9.AA	CP-9.AA Informationssystem-Backup	backup-recovery-point-manual-Löschen-deaktiviert	Stellen Sie sicher, dass Ihren AWS Backup-Wiederherstellungspunkten eine ressourcenbasierte Richtlinie zugeordnet ist, die das Löschen von Wiederherstellungspunkten verhindert. Die Verwendung einer ressourcenbasierten Richtlinie zur Verhinderung des Löschens von Wiederherstellungspunkten kann dazu beitragen, ein versehentliches oder absichtliches Löschen zu unterbinden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CP-9.AA	CP-9.AA Informationssystem-Backup	backup-recovery-point-minimum-Aufbewahrungsprüfung	Um bei Datensicherungsprozessen zu helfen, stellen Sie sicher, dass für Ihre AWS Backup-Wiederherstellungspunkte eine Mindestaufbewahrungsdauer festgelegt ist. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen. Mit dieser Regel können Sie den Parameter requiredRetentionDays (Standardkonfiguration: 35) festlegen. Der tatsächliche Wert muss den Anforderu

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
			ngen Ihrer Organisation entsprechen.
CCCS-fPBMM-CP-9.AA	CP-9.AA Informationssystem-Backup	db-instance-backup-enabled	Die Sicherungsfunktion von Amazon RDS erstellt Sicherungen Ihrer Datenbanken und Transaktionsprotokolle. Amazon RDS erstellt einen Snapshot für das Speichervolume Ihrer DB-Instance, sodass die gesamte DB-Instance gesichert wird. Sie können im System spezifische Aufbewahrungsfristen festlegen, um Ihre Ausfallsicherheitsanforderungen zu erfüllen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CP-9.AA	CP-9.AA Informationssystem-Backup	dynamodb-pitr-enabled	Aktivieren Sie diese Regel, um zu überprüfen, ob die Informationen gesichert wurden. Es verwaltet auch die Backups, indem es sicherstellt, dass die point-in-time Wiederherstellung in Amazon DynamoDB aktiviert ist. Bei der Wiederherstellung werden fortlaufende Backups Ihrer Tabelle für die letzten 35 Tage gespeichert.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CP-9.AA	CP-9.AA Informationssystem-Backup	dynamodb-resources-protected-by-Backup-Plan	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon DynamoDB DynamoDB-Ressourcen Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CP-9.AA	CP-9.AA Informationssystem-Backup	ebs-optimized-instance	Eine optimierte Instance im Amazon Elastic Block Store (Amazon EBS) bietet zusätzliche, dedizierte Kapazität für Amazon-EBS-I/O-Vorgänge. Diese Optimierung bietet die beste Leistung für Ihr EBS-Volume, indem Konflikte zwischen Amazon-EBS-I/O und anderem Datenverkehr von Ihrer Instance minimiert werden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CP-9.AA	CP-9.AA Informationssystem-Backup	ebs-resources-protected-by-Backup-Plan	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon Elastic Block Store (Amazon EBS) -Ressourcen Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihre Backup-Verwaltung und ermöglicht es Ihnen, Ihre geschäftlichen und behördlichen Anforderungen bezüglich Backups zu erfüllen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CP-9.AA	CP-9.AA Informationssystem-Backup	ebs-snapshot-public-restorable-überprüfen	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass EBS-Snapshots nicht öffentlich wiederherstellbar sind. EBS-Volume-Snapshots können vertrauliche Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CP-9.AA	CP-9.AA Informationssystem-Backup	ec2--Plan resources-protected-by-backup	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon Elastic Compute Cloud (Amazon EC2) -Ressourcen Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CP-9.AA	CP-9.AA Informationssystem-Backup	efs-resources-protected-by-Backup-Plan	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon Elastic File System (Amazon EFS) -Dateisysteme Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CP-9.AA	CP-9.AA Informationssystem-Backup	elasticache-redis-cluster-automatic-Backup-Check	Wenn automatische Backups aktiviert sind, ElastiCache erstellt Amazon täglich ein Backup des Clusters. Die Sicherung kann für eine von Ihrer Organisation festgelegte Anzahl von Tagen aufbewahrt werden. Automatische Backups schützen vor Datenverlust. Bei einem Ausfall können Sie einen neuen Cluster erstellen, der Ihre Daten aus dem aktuellen Backup wiederherstellt.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CP-9.AA	CP-9.AA Informationssystem-Backup	fsx-resources-protected-by-Backup-Plan	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre FSx Amazon-Dateisysteme Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CP-9.AA	CP-9.AA Informationssystem-Backup	rds-resources-protected-by-Backup-Plan	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon Relational Database Service (Amazon RDS) -Ressourcen Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CP-9.AA	CP-9.AA Informationssystem-Backup	rds-snapshots-public-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Relational Database Service (Amazon RDS) -Instances nicht öffentlich sind. Amazon-RDS-Datenbank-Instances können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CP-9.AA	CP-9.AA Informationssystem-Backup	rds-snapshot-encrypted	Stellen Sie sicher, dass die Verschlüsselung für Ihre Amazon Relational Database Service (Amazon RDS)-Snapshots aktiviert ist. Da sensible Daten auch im Ruhezustand vorhanden sein können, sollten Sie die Verschlüsselung von Daten im Ruhezustand aktivieren, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CP-9.AA	CP-9.AA Informationssystem-Backup	redshift-backup-enabled	Stellen Sie zur Unterstützung der Datensicherungsprozesse sicher, dass Ihre Amazon-Redshift-Cluster über automatisierte Snapshots verfügen. Wenn automatisierte Snapshots für einen Cluster aktiviert sind, erstellt Redshift in regelmäßigen Abständen Snapshots dieses Clusters. Standardmäßig erstellt Redshift alle acht Stunden oder alle 5 GB einen Snapshot für jeden Knoten mit Datenänderungen oder je nachdem, was zuerst eintritt.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CP-9.AA	CP-9.AA Informationssystem-Backup	redshift-cluster-maintenancesettings-check	Diese Regel stellt sicher, dass Amazon-Redshift-Cluster die bevorzugten Einstellungen für Ihre Organisation haben. Insbesondere sorgt sie dafür, dass Cluster bevorzugte Wartungsfenster und automatisierte Aufbewahrungsfristen für Snapshots für die Datenbank haben. Für diese Regel müssen Sie die festlegen. allowVersionUpgrade Der Standardwert ist „true“. Außerdem können Sie optional den Zeitraum preferredMaintenanceWindow (der Standardwert ist sa: 16:00 -sa: 16:30) und den automated SnapshotRetention Zeitraum (der Standardwert ist 1) festlegen. Die tatsächlichen Werte müssen den Richtlini

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
			en Ihrer Organisation entsprechen.
CCCS-fPBMM-CP-9.AA	CP-9.AA Informationssystem-Backup	s3- bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) unterstützt die Aufrechterhaltung einer angemessenen Kapazität und Verfügbarkeit. CRR ermöglicht das automatische, asynchrone Kopieren von Objekten in Amazon-S3-Buckets, um die Datenverfügbarkeit sicherzustellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CP-9.AA	CP-9.AA Informationssystem-Backup	s-3 bucket-versioning-enabled	Die Versionsverwaltung von Amazon Simple Storage Service (Amazon S3)-Buckets hilft dabei, mehrere Varianten eines Objekts im selben Amazon-S3-Bucket zu speichern. Verwenden Sie die Versionsverwaltung, um sämtliche Versionen aller Objekte in Ihrem Amazon-S3-Bucket zu speichern, abzurufen oder wiederherzustellen. Mit der Versionsverwaltung können Sie Versionen sowohl nach unbeabsichtigten Benutzeraktionen als auch nach Anwendungsfehlern problemlos wiederherstellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CP-9.B	CP-9.B Informationssystem-Backup	aurora-resources-protected-by-Ersatzplan	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon Aurora Aurora-Ressourcen Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CP-9.B	CP-9.B Informationssystem-Backup	backup-plan-min-frequency-and-min-retention-check	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihr AWS Backup-Plan auf eine Mindestfrequenz und Aufbewahrung festgelegt ist. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen. Mit dieser Regel können Sie die Parameter requiredFrequencyValue (Config default: 1), requiredRetentionDays (Config default: 35) und requiredFrequencyUnit

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
			(Config default: days) festlegen. Der tatsächliche Wert muss den Anforderungen Ihrer Organisation entsprechen.
CCCS-fPBMM-CP-9.B	CP-9.B Informationssystem-Backup	backup-recovery-point-encrypted	Stellen Sie sicher, dass die Verschlüsselung für Ihre AWS Backup-Wiederherstellungspunkte aktiviert ist. Da sensible Daten auch im Ruhezustand vorhanden sein können, sollten Sie die Verschlüsselung im Ruhezustand aktivieren, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CP-9.B	CP-9.B Informationssystem-Backup	backup-recovery-point-manual-Löschen-deaktiviert	Stellen Sie sicher, dass Ihren AWS Backup-Wiederherstellungspunkten eine ressourcenbasierte Richtlinie zugeordnet ist, die das Löschen von Wiederherstellungspunkten verhindert. Die Verwendung einer ressourcenbasierten Richtlinie zur Verhinderung des Löschens von Wiederherstellungspunkten kann dazu beitragen, ein versehentliches oder absichtliches Löschen zu unterbinden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CP-9.B	CP-9.B Informationssystem-Backup	backup-recovery-point-minimum-Aufbewahrungsprüfung	Um bei Datensicherungsprozessen zu helfen, stellen Sie sicher, dass für Ihre AWS Backup-Wiederherstellungspunkte eine Mindestaufbewahrungsdauer festgelegt ist. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen. Mit dieser Regel können Sie den Parameter requiredRetentionDays (Standardkonfiguration: 35) festlegen. Der tatsächliche Wert muss den Anforderu

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
			ngen Ihrer Organisation entsprechen.
CCCS-fPBMM-CP-9.B	CP-9.B Informationssystem-Backup	db-instance-backup-enabled	Die Sicherungsfunktion von Amazon RDS erstellt Sicherungen Ihrer Datenbanken und Transaktionsprotokolle. Amazon RDS erstellt einen Snapshot für das Speichervolume Ihrer DB-Instance, sodass die gesamte DB-Instance gesichert wird. Sie können im System spezifische Aufbewahrungsfristen festlegen, um Ihre Ausfallsicherheitsanforderungen zu erfüllen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CP-9.B	CP-9.B Informationssystem-Backup	dynamodb-pitr-enabled	Aktivieren Sie diese Regel, um zu überprüfen, ob die Informationen gesichert wurden. Es verwaltet auch die Backups, indem es sicherstellt, dass die point-in-time Wiederherstellung in Amazon DynamoDB aktiviert ist. Bei der Wiederherstellung werden fortlaufende Backups Ihrer Tabelle für die letzten 35 Tage gespeichert.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CP-9.B	CP-9.B Informationssystem-Backup	dynamodb-resources-protected-by-Backup-Plan	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon DynamoDB DynamoDB-Ressourcen Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CP-9.B	CP-9.B Informationssystem-Backup	ebs-optimized-instance	Eine optimierte Instance im Amazon Elastic Block Store (Amazon EBS) bietet zusätzliche, dedizierte Kapazität für Amazon-EBS-I/O-Vorgänge. Diese Optimierung bietet die beste Leistung für Ihr EBS-Volume, indem Konflikte zwischen Amazon-EBS-I/O und anderem Datenverkehr von Ihrer Instance minimiert werden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CP-9.B	CP-9.B Informationssystem-Backup	ebs-resources-protected-by-Backup-Plan	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon Elastic Block Store (Amazon EBS) -Ressourcen Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihre Backup-Verwaltung und ermöglicht es Ihnen, Ihre geschäftlichen und behördlichen Anforderungen bezüglich Backups zu erfüllen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CP-9.B	CP-9.B Informationssystem-Backup	ebs-snapshot-public-restorable-überprüfen	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass EBS-Snapshots nicht öffentlich wiederherstellbar sind. EBS-Volume-Snapshots können vertrauliche Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CP-9.B	CP-9.B Informationssystem-Backup	ec2--Plan resources-protected-by-backup	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon Elastic Compute Cloud (Amazon EC2) -Ressourcen Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CP-9.B	CP-9.B Informationssystem-Backup	efs-resources-protected-by-Backup-Plan	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon Elastic File System (Amazon EFS) -Dateisysteme Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CP-9.B	CP-9.B Informationssystem-Backup	elasticache-redis-cluster-automatic-Backup-Check	Wenn automatische Backups aktiviert sind, ElastiCache erstellt Amazon täglich ein Backup des Clusters. Die Sicherung kann für eine von Ihrer Organisation festgelegte Anzahl von Tagen aufbewahrt werden. Automatische Backups schützen vor Datenverlust. Bei einem Ausfall können Sie einen neuen Cluster erstellen, der Ihre Daten aus dem aktuellen Backup wiederherstellt.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CP-9.B	CP-9.B Informationssystem-Backup	fsx-resources-protected-by-Backup-Plan	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre FSx Amazon-Dateisysteme Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CP-9.B	CP-9.B Informationssystem-Backup	rds-resources-protected-by-Backup-Plan	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon Relational Database Service (Amazon RDS) -Ressourcen Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CP-9.B	CP-9.B Informationssystem-Backup	rds-snapshots-public-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Relational Database Service (Amazon RDS) -Instances nicht öffentlich sind. Amazon-RDS-Datenbank-Instances können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CP-9.B	CP-9.B Informationssystem-Backup	rds-snapshot-encrypted	Stellen Sie sicher, dass die Verschlüsselung für Ihre Amazon Relational Database Service (Amazon RDS)-Snapshots aktiviert ist. Da sensible Daten auch im Ruhezustand vorhanden sein können, sollten Sie die Verschlüsselung von Daten im Ruhezustand aktivieren, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CP-9.B	CP-9.B Informationssystem-Backup	redshift-backup-enabled	Stellen Sie zur Unterstützung der Datensicherungsprozesse sicher, dass Ihre Amazon-Redshift-Cluster über automatisierte Snapshots verfügen. Wenn automatisierte Snapshots für einen Cluster aktiviert sind, erstellt Redshift in regelmäßigen Abständen Snapshots dieses Clusters. Standardmäßig erstellt Redshift alle acht Stunden oder alle 5 GB einen Snapshot für jeden Knoten mit Datenänderungen oder je nachdem, was zuerst eintritt.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CP-9.B	CP-9.B Informationssystem-Backup	redshift-cluster-maintenancesettings-check	Diese Regel stellt sicher, dass Amazon-Redshift-Cluster die bevorzugten Einstellungen für Ihre Organisation haben. Insbesondere sorgt sie dafür, dass Cluster bevorzugte Wartungsfenster und automatisierte Aufbewahrungsfristen für Snapshots für die Datenbank haben. Für diese Regel müssen Sie die festlegen. allowVersionUpgrade Der Standardwert ist „true“. Außerdem können Sie optional den Zeitraum preferredMaintenanceWindow (der Standardwert ist sa: 16:00 -sa: 16:30) und den automated SnapshotRetention Zeitraum (der Standardwert ist 1) festlegen. Die tatsächlichen Werte müssen den Richtlini

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
			en Ihrer Organisation entsprechen.
CCCS-fPBMM-CP-9.B	CP-9.B Informationssystem-Backup	s3- bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) unterstützt die Aufrechterhaltung einer angemessenen Kapazität und Verfügbarkeit. CRR ermöglicht das automatische, asynchrone Kopieren von Objekten in Amazon-S3-Buckets, um die Datenverfügbarkeit sicherzustellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CP-9.B	CP-9.B Informationssystem-Backup	s-3 bucket-versioning-enabled	Die Versionsverwaltung von Amazon Simple Storage Service (Amazon S3)-Buckets hilft dabei, mehrere Varianten eines Objekts im selben Amazon-S3-Bucket zu speichern. Verwenden Sie die Versionsverwaltung, um sämtliche Versionen aller Objekte in Ihrem Amazon-S3-Bucket zu speichern, abzurufen oder wiederherzustellen. Mit der Versionsverwaltung können Sie Versionen sowohl nach unbeabsichtigten Benutzeraktionen als auch nach Anwendungsfehlern problemlos wiederherstellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CP-9.C	CP-9.C Informationssystem-Backup	aurora-resources-protected-by-Ersatzplan	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon Aurora Aurora-Ressourcen Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CP-9.C	CP-9.C Informationssystem-Backup	backup-plan-min-frequency-and-min-retention-check	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihr AWS Backup-Plan auf eine Mindestfrequenz und Aufbewahrung festgelegt ist. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen. Mit dieser Regel können Sie die Parameter requiredFrequencyValue (Config default: 1), requiredRetentionDays (Config default: 35) und requiredFrequencyUnit

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
			(Config default: days) festlegen. Der tatsächliche Wert muss den Anforderungen Ihrer Organisation entsprechen.
CCCS-fPBMM-CP-9.C	CP-9.C Informationssystem-Backup	backup-recovery-point-encrypted	Stellen Sie sicher, dass die Verschlüsselung für Ihre AWS Backup-Wiederherstellungspunkte aktiviert ist. Da sensible Daten auch im Ruhezustand vorhanden sein können, sollten Sie die Verschlüsselung im Ruhezustand aktivieren, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CP-9.C	CP-9.C Informationssystem-Backup	backup-recovery-point-manual-Löschen-deaktiviert	Stellen Sie sicher, dass Ihren AWS Backup-Wiederherstellungspunkten eine ressourcenbasierte Richtlinie zugeordnet ist, die das Löschen von Wiederherstellungspunkten verhindert. Die Verwendung einer ressourcenbasierten Richtlinie zur Verhinderung des Löschens von Wiederherstellungspunkten kann dazu beitragen, ein versehentliches oder absichtliches Löschen zu unterbinden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CP-9.C	CP-9.C Informationssystem-Backup	backup-recovery-point-minimum-Aufbewahrungsprüfung	Um bei Datensicherungsprozessen zu helfen, stellen Sie sicher, dass für Ihre AWS Backup-Wiederherstellungspunkte eine Mindestaufbewahrungsdauer festgelegt ist. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen. Mit dieser Regel können Sie den Parameter requiredRetentionDays (Standardkonfiguration: 35) festlegen. Der tatsächliche Wert muss den Anforderu

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
			ngen Ihrer Organisation entsprechen.
CCCS-fPBMM-CP-9.C	CP-9.C Informationssystem-Backup	db-instance-backup-enabled	Die Sicherungsfunktion von Amazon RDS erstellt Sicherungen Ihrer Datenbanken und Transaktionsprotokolle. Amazon RDS erstellt einen Snapshot für das Speichervolume Ihrer DB-Instance, sodass die gesamte DB-Instance gesichert wird. Sie können im System spezifische Aufbewahrungsfristen festlegen, um Ihre Ausfallsicherheitsanforderungen zu erfüllen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CP-9.C	CP-9.C Informationssystem-Backup	dynamodb-pitr-enabled	Aktivieren Sie diese Regel, um zu überprüfen, ob die Informationen gesichert wurden. Es verwaltet auch die Backups, indem es sicherstellt, dass die point-in-time Wiederherstellung in Amazon DynamoDB aktiviert ist. Bei der Wiederherstellung werden fortlaufende Backups Ihrer Tabelle für die letzten 35 Tage gespeichert.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CP-9.C	CP-9.C Informationssystem-Backup	dynamodb-resources-protected-by-Backup-Plan	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon DynamoDB DynamoDB-Ressourcen Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CP-9.C	CP-9.C Informationssystem-Backup	ebs-optimized-instance	Eine optimierte Instance im Amazon Elastic Block Store (Amazon EBS) bietet zusätzliche, dedizierte Kapazität für Amazon-EBS-I/O-Vorgänge. Diese Optimierung bietet die beste Leistung für Ihr EBS-Volume, indem Konflikte zwischen Amazon-EBS-I/O und anderem Datenverkehr von Ihrer Instance minimiert werden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CP-9.C	CP-9.C Informationssystem-Backup	ebs-resources-protected-by-Backup-Plan	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon Elastic Block Store (Amazon EBS) -Ressourcen Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihre Backup-Verwaltung und ermöglicht es Ihnen, Ihre geschäftlichen und behördlichen Anforderungen bezüglich Backups zu erfüllen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CP-9.C	CP-9.C Informationssystem-Backup	ebs-snapshot-public-restorable-überprüfen	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass EBS-Snapshots nicht öffentlich wiederherstellbar sind. EBS-Volume-Snapshots können vertrauliche Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CP-9.C	CP-9.C Informationssystem-Backup	ec2--Plan resources-protected-by-backup	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon Elastic Compute Cloud (Amazon EC2) -Ressourcen Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CP-9.C	CP-9.C Informationssystem-Backup	efs-resources-protected-by-Backup-Plan	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon Elastic File System (Amazon EFS) -Dateisysteme Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CP-9.C	CP-9.C Informationssystem-Backup	elasticache-redis-cluster-automatic-Backup-Check	Wenn automatische Backups aktiviert sind, ElastiCache erstellt Amazon täglich ein Backup des Clusters. Die Sicherung kann für eine von Ihrer Organisation festgelegte Anzahl von Tagen aufbewahrt werden. Automatische Backups schützen vor Datenverlust. Bei einem Ausfall können Sie einen neuen Cluster erstellen, der Ihre Daten aus dem aktuellen Backup wiederherstellt.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CP-9.C	CP-9.C Informationssystem-Backup	fsx-resources-protected-by-Backup-Plan	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre FSx Amazon-Dateisysteme Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CP-9.C	CP-9.C Informationssystem-Backup	rds-resources-protected-by-Backup-Plan	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon Relational Database Service (Amazon RDS) -Ressourcen Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CP-9.C	CP-9.C Informationssystem-Backup	rds-snapshots-public-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Relational Database Service (Amazon RDS) -Instances nicht öffentlich sind. Amazon-RDS-Datenbank-Instances können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CP-9.C	CP-9.C Informationssystem-Backup	rds-snapshot-encrypted	Stellen Sie sicher, dass die Verschlüsselung für Ihre Amazon Relational Database Service (Amazon RDS)-Snapshots aktiviert ist. Da sensible Daten auch im Ruhezustand vorhanden sein können, sollten Sie die Verschlüsselung von Daten im Ruhezustand aktivieren, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CP-9.C	CP-9.C Informationssystem-Backup	redshift-backup-enabled	Stellen Sie zur Unterstützung der Datensicherungsprozesse sicher, dass Ihre Amazon-Redshift-Cluster über automatisierte Snapshots verfügen. Wenn automatisierte Snapshots für einen Cluster aktiviert sind, erstellt Redshift in regelmäßigen Abständen Snapshots dieses Clusters. Standardmäßig erstellt Redshift alle acht Stunden oder alle 5 GB einen Snapshot für jeden Knoten mit Datenänderungen oder je nachdem, was zuerst eintritt.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CP-9.C	CP-9.C Informationssystem-Backup	redshift-cluster-maintenancesettings-check	Diese Regel stellt sicher, dass Amazon-Redshift-Cluster die bevorzugten Einstellungen für Ihre Organisation haben. Insbesondere sorgt sie dafür, dass Cluster bevorzugte Wartungsfenster und automatisierte Aufbewahrungsfristen für Snapshots für die Datenbank haben. Für diese Regel müssen Sie die festlegen. allowVersionUpgrade Der Standardwert ist „true“. Außerdem können Sie optional den Zeitraum preferredMaintenanceWindow (der Standardwert ist sa: 16:00 -sa: 16:30) und den automated SnapshotRetention Zeitraum (der Standardwert ist 1) festlegen. Die tatsächlichen Werte müssen den Richtlini

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
			en Ihrer Organisation entsprechen.
CCCS-fPBMM-CP-9.C	CP-9.C Informationssystem-Backup	s3- bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) unterstützt die Aufrechterhaltung einer angemessenen Kapazität und Verfügbarkeit. CRR ermöglicht das automatische, asynchrone Kopieren von Objekten in Amazon-S3-Buckets, um die Datenverfügbarkeit sicherzustellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CP-9.C	CP-9.C Informationssystem-Backup	s-3 bucket-versioning-enabled	Die Versionsverwaltung von Amazon Simple Storage Service (Amazon S3)-Buckets hilft dabei, mehrere Varianten eines Objekts im selben Amazon-S3-Bucket zu speichern. Verwenden Sie die Versionsverwaltung, um sämtliche Versionen aller Objekte in Ihrem Amazon-S3-Bucket zu speichern, abzurufen oder wiederherzustellen. Mit der Versionsverwaltung können Sie Versionen sowohl nach unbeabsichtigten Benutzeraktionen als auch nach Anwendungsfehlern problemlos wiederherstellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CP-9.D	CP-9.D Informationssystem-Backup	aurora-resources-protected-by-Ersatzplan	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon Aurora Aurora-Ressourcen Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CP-9.D	CP-9.D Informationssystem-Backup	backup-plan-min-frequency-and-min-retention-check	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihr AWS Backup-Plan auf eine Mindestfrequenz und Aufbewahrung festgelegt ist. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen. Mit dieser Regel können Sie die Parameter requiredFrequencyValue (Config default: 1), requiredRetentionDays (Config default: 35) und requiredFrequencyUnit

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
			(Config default: days) festlegen. Der tatsächliche Wert muss den Anforderungen Ihrer Organisation entsprechen.
CCCS-fPBMM-CP-9.D	CP-9.D Informationssystem-Backup	backup-recovery-point-encrypted	Stellen Sie sicher, dass die Verschlüsselung für Ihre AWS Backup-Wiederherstellungspunkte aktiviert ist. Da sensible Daten auch im Ruhezustand vorhanden sein können, sollten Sie die Verschlüsselung im Ruhezustand aktivieren, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CP-9.D	CP-9.D Informationssystem-Backup	backup-recovery-point-manual-Löschen-deaktiviert	Stellen Sie sicher, dass Ihren AWS Backup-Wiederherstellungspunkten eine ressourcenbasierte Richtlinie zugeordnet ist, die das Löschen von Wiederherstellungspunkten verhindert. Die Verwendung einer ressourcenbasierten Richtlinie zur Verhinderung des Löschens von Wiederherstellungspunkten kann dazu beitragen, ein versehentliches oder absichtliches Löschen zu unterbinden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CP-9.D	CP-9.D Informationssystem-Backup	backup-recovery-point-minimum-Aufbewahrungsprüfung	Um bei Datensicherungsprozessen zu helfen, stellen Sie sicher, dass für Ihre AWS Backup-Wiederherstellungspunkte eine Mindestaufbewahrungsdauer festgelegt ist. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen. Mit dieser Regel können Sie den Parameter requiredRetentionDays (Standardkonfiguration: 35) festlegen. Der tatsächliche Wert muss den Anforderu

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
			ngen Ihrer Organisation entsprechen.
CCCS-fPBMM-CP-9.D	CP-9.D Informationssystem-Backup	db-instance-backup-enabled	Die Sicherungsfunktion von Amazon RDS erstellt Sicherungen Ihrer Datenbanken und Transaktionsprotokolle. Amazon RDS erstellt einen Snapshot für das Speichervolume Ihrer DB-Instance, sodass die gesamte DB-Instance gesichert wird. Sie können im System spezifische Aufbewahrungsfristen festlegen, um Ihre Ausfallsicherheitsanforderungen zu erfüllen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CP-9.D	CP-9.D Informationssystem-Backup	dynamodb-pitr-enabled	Aktivieren Sie diese Regel, um zu überprüfen, ob die Informationen gesichert wurden. Es verwaltet auch die Backups, indem es sicherstellt, dass die point-in-time Wiederherstellung in Amazon DynamoDB aktiviert ist. Bei der Wiederherstellung werden fortlaufende Backups Ihrer Tabelle für die letzten 35 Tage gespeichert.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CP-9.D	CP-9.D Informationssystem-Backup	dynamodb-resources-protected-by-Backup-Plan	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon DynamoDB DynamoDB-Ressourcen Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CP-9.D	CP-9.D Informationssystem-Backup	ebs-optimized-instance	Eine optimierte Instance im Amazon Elastic Block Store (Amazon EBS) bietet zusätzliche, dedizierte Kapazität für Amazon-EBS-I/O-Vorgänge. Diese Optimierung bietet die beste Leistung für Ihr EBS-Volume, indem Konflikte zwischen Amazon-EBS-I/O und anderem Datenverkehr von Ihrer Instance minimiert werden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CP-9.D	CP-9.D Informationssystem-Backup	ebs-resources-protected-by-Backup-Plan	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon Elastic Block Store (Amazon EBS) -Ressourcen Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihre Backup-Verwaltung und ermöglicht es Ihnen, Ihre geschäftlichen und behördlichen Anforderungen bezüglich Backups zu erfüllen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CP-9.D	CP-9.D Informationssystem-Backup	ebs-snapshot-public-restorable-überprüfen	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass EBS-Snapshots nicht öffentlich wiederherstellbar sind. EBS-Volume-Snapshots können vertrauliche Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CP-9.D	CP-9.D Informationssystem-Backup	ec2--Plan resources-protected-by-backup	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon Elastic Compute Cloud (Amazon EC2) -Ressourcen Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CP-9.D	CP-9.D Informationssystem-Backup	efs-resources-protected-by-Backup-Plan	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon Elastic File System (Amazon EFS) -Dateisysteme Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CP-9.D	CP-9.D Informationssystem-Backup	elasticache-redis-cluster-automatic-Backup-Check	Wenn automatische Backups aktiviert sind, ElastiCache erstellt Amazon täglich ein Backup des Clusters. Die Sicherung kann für eine von Ihrer Organisation festgelegte Anzahl von Tagen aufbewahrt werden. Automatische Backups schützen vor Datenverlust. Bei einem Ausfall können Sie einen neuen Cluster erstellen, der Ihre Daten aus dem aktuellen Backup wiederherstellt.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CP-9.D	CP-9.D Informationssystem-Backup	fsx-resources-protected-by-Backup-Plan	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre FSx Amazon-Dateisysteme Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CP-9.D	CP-9.D Informationssystem-Backup	rds-resources-protected-by-Backup-Plan	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon Relational Database Service (Amazon RDS) -Ressourcen Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CP-9.D	CP-9.D Informationssystem-Backup	rds-snapshots-public-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Relational Database Service (Amazon RDS) -Instances nicht öffentlich sind. Amazon-RDS-Datenbank-Instances können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CP-9.D	CP-9.D Informationssystem-Backup	rds-snapshot-encrypted	Stellen Sie sicher, dass die Verschlüsselung für Ihre Amazon Relational Database Service (Amazon RDS)-Snapshots aktiviert ist. Da sensible Daten auch im Ruhezustand vorhanden sein können, sollten Sie die Verschlüsselung von Daten im Ruhezustand aktivieren, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CP-9.D	CP-9.D Informationssystem-Backup	redshift-backup-enabled	Stellen Sie zur Unterstützung der Datensicherungsprozesse sicher, dass Ihre Amazon-Redshift-Cluster über automatisierte Snapshots verfügen. Wenn automatisierte Snapshots für einen Cluster aktiviert sind, erstellt Redshift in regelmäßigen Abständen Snapshots dieses Clusters. Standardmäßig erstellt Redshift alle acht Stunden oder alle 5 GB einen Snapshot für jeden Knoten mit Datenänderungen oder je nachdem, was zuerst eintritt.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CP-9.D	CP-9.D Informationssystem-Backup	redshift-cluster-maintenancesettings-check	Diese Regel stellt sicher, dass Amazon-Redshift-Cluster die bevorzugten Einstellungen für Ihre Organisation haben. Insbesondere sorgt sie dafür, dass Cluster bevorzugte Wartungsfenster und automatisierte Aufbewahrungsfristen für Snapshots für die Datenbank haben. Für diese Regel müssen Sie die festlegen. allowVersionUpgrade Der Standardwert ist „true“. Außerdem können Sie optional den Zeitraum preferredMaintenanceWindow (der Standardwert ist sa: 16:00 -sa: 16:30) und den automated SnapshotRetention Zeitraum (der Standardwert ist 1) festlegen. Die tatsächlichen Werte müssen den Richtlini

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
			en Ihrer Organisation entsprechen.
CCCS-fPBMM-CP-9.D	CP-9.D Informationssystem-Backup	s3- bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) unterstützt die Aufrechterhaltung einer angemessenen Kapazität und Verfügbarkeit. CRR ermöglicht das automatische, asynchrone Kopieren von Objekten in Amazon-S3-Buckets, um die Datenverfügbarkeit sicherzustellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CP-9.D	CP-9.D Informationssystem-Backup	s-3 bucket-versioning-enabled	Die Versionsverwaltung von Amazon Simple Storage Service (Amazon S3)-Buckets hilft dabei, mehrere Varianten eines Objekts im selben Amazon-S3-Bucket zu speichern. Verwenden Sie die Versionsverwaltung, um sämtliche Versionen aller Objekte in Ihrem Amazon-S3-Bucket zu speichern, abzurufen oder wiederherzustellen. Mit der Versionsverwaltung können Sie Versionen sowohl nach unbeabsichtigten Benutzeraktionen als auch nach Anwendungsfehlern problemlos wiederherstellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CP-10.A	CP-10.A Wiederherstellung und Rekonstitution des Informationssystems	db-instance-backup-enabled	Die Sicherungsfunktion von Amazon RDS erstellt Sicherungen Ihrer Datenbanken und Transaktionsprotokolle. Amazon RDS erstellt einen Snapshot für das Speichervolume Ihrer DB-Instance, sodass die gesamte DB-Instance gesichert wird. Sie können im System spezifische Aufbewahrungsfristen festlegen, um Ihre Ausfallsicherheitsanforderungen zu erfüllen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CP-10.A	CP-10.A Wiederherstellung und Rekonstitution des Informationssystems	dynamodb-autoscaling-enabled	Amazon DynamoDB Auto Scaling verwendet den AWS Application Auto Scaling-Service, um die bereitgestellte Durchsatzkapazität so anzupassen, dass sie automatisch auf tatsächliche Verkehrsmuster reagiert. Auf diese Weise kann eine Tabelle oder ein globaler sekundärer Index die bereitgestellte Lese-/Schreibkapazität erhöhen, um plötzliche Erhöhungen des Datenverkehrs ohne Drosselung zu bewältigen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CP-10.A	CP-10.A Wiederherstellung und Rekonstitution des Informationssystems	dynamodb-pitr-enabled	Aktivieren Sie diese Regel, um zu überprüfen, ob die Informationen gesichert wurden. Es verwaltet auch die Backups, indem es sicherstellt, dass die point-in-time Wiederherstellung in Amazon DynamoDB aktiviert ist. Bei der Wiederherstellung werden fortlaufende Backups Ihrer Tabelle für die letzten 35 Tage gespeichert.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CP-10.A	CP-10.A Wiederherstellung und Rekonstitution des Informationssystems	ebs-optimized-instance	Eine optimierte Instance im Amazon Elastic Block Store (Amazon EBS) bietet zusätzliche, dedizierte Kapazität für Amazon-EBS-I/O-Vorgänge. Diese Optimierung bietet die beste Leistung für Ihr EBS-Volume, indem Konflikte zwischen Amazon-EBS-I/O und anderem Datenverkehr von Ihrer Instance minimiert werden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CP-10.A	CP-10.A Wiederherstellung und Rekonstitution des Informationssystems	elasticache-redis-cluster-automatic-Backup-Prüfung	Wenn automatische Backups aktiviert sind, ElastiCache erstellt Amazon täglich ein Backup des Clusters. Die Sicherung kann für eine von Ihrer Organisation festgelegte Anzahl von Tagen aufbewahrt werden. Automatische Backups schützen vor Datenverlust. Bei einem Ausfall können Sie einen neuen Cluster erstellen, der Ihre Daten aus dem aktuellen Backup wiederherstellt.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CP-10.A	CP-10.A Wiederherstellung und Rekonstitution des Informationssystems	elb-cross-zone-load-Balancing aktiviert	Aktivieren Sie zonenübergreifendes Load Balancing für Ihre Elastic Load Balancer (ELBs), um eine angemessene Kapazität und Verfügbarkeit aufrechtzuerhalten. Zonenübergreifendes Load Balancing reduziert die Notwendigkeit, die gleiche Anzahl von Instances in jeder aktivierten Availability Zone aufrechtzuerhalten. Dadurch wird auch die Fähigkeit Ihrer Anwendung verbessert, den Verlust einer oder mehrerer Instances zu bewältigen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CP-10.A	CP-10.A Wiederherstellung und Rekonstitution des Informationssystems	rds-cluster-multi-az-aktiviert	Für Cluster von Amazon Relational Database Service (Amazon RDS) sollte die Multi-AZ-Replikation aktiviert sein, um die Verfügbarkeit der gespeicherten Daten zu gewährleisten. Availability Zones werden auf einer physisch getrennten, unabhängigen Infrastruktur ausgeführt und sind auf höchste Zuverlässigkeit ausgelegt. Im Falle eines Infrastrukturausfalls führt Amazon RDS einen automatischen Failover zum Standby-Modus durch, sodass Sie den Datenbankbetrieb wieder aufnehmen können, sobald der Failover abgeschlossen ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CP-10.A	CP-10.A Wiederherstellung und Rekonstitution des Informationssystems	rds-multi-az-support	Die Multi-AZ-Unterstützung in Amazon Relational Database Service (Amazon RDS) bietet eine verbesserte Verfügbarkeit und Beständigkeit von Datenbank-Instances. Wenn Sie eine Multi-AZ-Datenbank-Instance bereitstellen, erstellt Amazon RDS automatisch eine primäre Datenbank-Instance und repliziert die Daten synchron auf eine Standby-Instance in einer anderen Availability Zone. Jede Availability Zone läuft auf einer eigenen, physisch getrennten, unabhängigen Infrastruktur und ist auf eine hohe Verfügbarkeit ausgelegt. Im Falle eines Infrastrukturausfalls führt Amazon RDS einen automatis

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
			chen Failover zum Standby-Modus durch, sodass Sie den Datenbankbetrieb wieder aufnehmen können, sobald der Failover abgeschlo ssen ist.
CCCS-fPBMM-CP-10.A	CP-10.A Wiederher stellung und Rekonstit ution des Informati onssystems	redshift-backup-en abled	Stellen Sie zur Unterstützung der Datensicherungspro zesse sicher, dass Ihre Amazon-Re dshift-Cluster über automatisierte Snapshots verfügen. Wenn automatis ierte Snapshots für einen Cluster aktiviert sind, erstellt Redshift in regelmäßi gen Abständen Snapshots dieses Clusters. Standardm äßig erstellt Redshift alle acht Stunden oder alle 5 GB einen Snapshot für jeden Knoten mit Datenände rungen oder je nachdem, was zuerst eintritt.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CP-10.A	CP-10.A Wiederherstellung und Rekonstitution des Informationssystems	s3- bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) unterstützt die Aufrechterhaltung einer angemessenen Kapazität und Verfügbarkeit. CRR ermöglicht das automatische, asynchrone Kopieren von Objekten in Amazon-S3-Buckets, um die Datenverfügbarkeit sicherzustellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CP-10.A	CP-10.A Wiederherstellung und Rekonstitution des Informationssystems	s-3 bucket-versioning-enabled	Die Versionsverwaltung von Amazon Simple Storage Service (Amazon S3)-Buckets hilft dabei, mehrere Varianten eines Objekts im selben Amazon-S3-Bucket zu speichern. Verwenden Sie die Versionsverwaltung, um sämtliche Versionen aller Objekte in Ihrem Amazon-S3-Bucket zu speichern, abzurufen oder wiederherzustellen. Mit der Versionsverwaltung können Sie Versionen sowohl nach unbeabsichtigten Benutzeraktionen als auch nach Anwendungsfehlern problemlos wiederherstellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-CP-10.A	CP-10.A Wiederherstellung und Rekonstitution des Informationssystems	vpc-vpn-2-tunnels-up	Redundante Site-to-Site VPN-Tunnel können implementiert werden, um die Anforderungen an die Ausfallsicherheit zu erfüllen. Es verwendet zwei Tunnel, um die Konnektivität sicherzustellen, falls eine der Site-to-Site VPN-Verbindungen nicht verfügbar ist. Um sich vor einem Verbindungsverlust zu schützen, können Sie für den Fall, dass Ihr Kunden-Gateway nicht verfügbar ist, eine zweite Site-to-Site VPN-Verbindung zu Ihrer Amazon Virtual Private Cloud (Amazon VPC) und Ihrem Virtual Private Gateway einrichten, indem Sie ein zweites Kunden-Gateway verwenden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-IA-2(1)	IA-2(1) Identifiz ierung und Authentif izierung (Benutzer im Unternehmen) | Netzwerkzugriff auf privilegierte Konten	iam-user-mfa-enabled	Aktivieren Sie diese Regel, um den Zugriff auf Ressourcen in der AWS -Cloud einzuschränken. Diese Regel stellt sicher, dass die Multi-Faktor-Authe ntifizierung (MFA) für alle Benutzer aktiviert ist. MFA bietet eine weitere Schutzebene zusätzlic h zum Benutzern amen und Passwort. Reduzieren Sie Fälle von kompromittierten Konten, indem Sie MFA für Benutzer vorschreiben.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-IA-2(1)	IA-2(1) Identifizierung und Authentifizierung (Benutzer im Unternehmen) | Netzwerkzugriff auf privilegierte Konten	mfa-enabled-for-iam-Konsolenzugriff	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass MFA für alle AWS Identity and Access Management (IAM) -Benutzer aktiviert ist, die über ein Konsolenkennwort verfügen. MFA sorgt für eine weitere Schutzebene zusätzlich zu den Anmeldeinformationen. Indem Sie MFA für Benutzer vorschreiben, können Sie Fälle kompromittierter Konten reduzieren und verhindern, dass unbefugte Benutzer auf vertrauliche Daten zugreifen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-IA-2(1)	IA-2(1) Identifizierung und Authentifizierung (Benutzer im Unternehmen) | Netzwerkzugriff auf privilegierte Konten	root-account-mfa-enabled	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass MFA für den Root-Benutzer aktiviert ist. Der Stammbenutzer ist der AWS-Konto-Benutzer mit den meisten Berechtigungen. MFA bietet eine weitere Schutzebene zusätzlich zum Benutzernamen und Passwort. Indem Sie MFA für den Root-Benutzer vorschreiben, können Sie die Anzahl AWS-Konten kompromittierter Benutzer reduzieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-IA-2(3)	IA-2(3) Identifiz ierung und Authentif izierung (Benutzer im Unternehmen) | Lokaler Zugriff auf privilegierte Konten	iam-user-mfa-enabled	Aktivieren Sie diese Regel, um den Zugriff auf Ressourcen in der AWS -Cloud einzuschränken. Diese Regel stellt sicher, dass die Multi-Faktor-Authe ntifizierung (MFA) für alle Benutzer aktiviert ist. MFA bietet eine weitere Schutzebene zusätzlic h zum Benutzern amen und Passwort. Reduzieren Sie Fälle von kompromittierten Konten, indem Sie MFA für Benutzer vorschreiben.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-IA-2(3)	IA-2(3) Identifizierung und Authentifizierung (Benutzer im Unternehmen) | Lokaler Zugriff auf privilegierte Konten	mfa-enabled-for-iam-Konsolenzugriff	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass MFA für alle AWS Identity and Access Management (IAM) -Benutzer aktiviert ist, die über ein Konsolenkennwort verfügen. MFA sorgt für eine weitere Schutzebene zusätzlich zu den Anmeldeinformationen. Indem Sie MFA für Benutzer vorschreiben, können Sie Fälle kompromittierter Konten reduzieren und verhindern, dass unbefugte Benutzer auf vertrauliche Daten zugreifen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-IA-2(3)	IA-2(3) Identifizierung und Authentifizierung (Benutzer im Unternehmen) | Lokaler Zugriff auf privilegierte Konten	root-account-mfa-enabled	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass MFA für den Root-Benutzer aktiviert ist. Der Stammbenutzer ist der AWS-Konto-Benutzer mit den meisten Berechtigungen. MFA bietet eine weitere Schutzebene zusätzlich zum Benutzernamen und Passwort. Indem Sie MFA für den Root-Benutzer vorschreiben, können Sie die Anzahl AWS-Konten kompromittierter Benutzer reduzieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-IA-2(8)	IA-2(8) Identifiz ierung und Authentif izierung (Benutzer im Unternehmen) | Netzwerkzugriff auf privilegierte Konten – wiedergaberesistent	iam-user-mfa-enabled	Aktivieren Sie diese Regel, um den Zugriff auf Ressourcen in der AWS -Cloud einzuschränken. Diese Regel stellt sicher, dass die Multi-Faktor-Authe ntifizierung (MFA) für alle Benutzer aktiviert ist. MFA bietet eine weitere Schutzebene zusätzlic h zum Benutzern amen und Passwort. Reduzieren Sie Fälle von kompromittierten Konten, indem Sie MFA für Benutzer vorschreiben.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-IA-2(8)	IA-2(8) Identifizierung und Authentifizierung (Benutzer im Unternehmen) | Netzwerkzugriff auf privilegierte Konten – wiedergaberesistent	mfa-enabled-for-iam-Konsolenzugriff	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass MFA für alle AWS Identity and Access Management (IAM) -Benutzer aktiviert ist, die über ein Konsolenkennwort verfügen. MFA sorgt für eine weitere Schutzebene zusätzlich zu den Anmeldeinformationen. Indem Sie MFA für Benutzer vorschreiben, können Sie Fälle kompromittierter Konten reduzieren und verhindern, dass unbefugte Benutzer auf vertrauliche Daten zugreifen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-IA-2(8)	IA-2(8) Identifizierung und Authentifizierung (Benutzer im Unternehmen) | Netzwerkzugriff auf privilegierte Konten – wiedergaberesistent	root-account-mfa-enabled	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass MFA für den Root-Benutzer aktiviert ist. Der Stammbenutzer ist der AWS-Konto-Benutzer mit den meisten Berechtigungen. MFA bietet eine weitere Schutzebene zusätzlich zum Benutzernamen und Passwort. Indem Sie MFA für den Root-Benutzer vorschreiben, können Sie die Anzahl AWS-Konten kompromittierter Benutzer reduzieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-IA-2(11)	IA-2(11) Identifizierung und Authentifizierung (Benutzer im Unternehmen) | Zugriff auf Konten – separates Gerät	iam-user-mfa-enabled	Aktivieren Sie diese Regel, um den Zugriff auf Ressourcen in der AWS -Cloud einzuschränken. Diese Regel stellt sicher, dass die Multi-Faktor-Authentifizierung (MFA) für alle Benutzer aktiviert ist. MFA bietet eine weitere Schutzebene zusätzlich zum Benutzernamen und Passwort. Reduzieren Sie Fälle von kompromittierten Konten, indem Sie MFA für Benutzer vorschreiben.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-IA-2(11)	IA-2(11) Identifizierung und Authentifizierung (Benutzer im Unternehmen) | Zugriff auf Konten – separates Gerät	mfa-enabled-for-iam-Konsolenzugriff	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass MFA für alle AWS Identity and Access Management (IAM) -Benutzer aktiviert ist, die über ein Konsolenkennwort verfügen. MFA sorgt für eine weitere Schutzebene zusätzlich zu den Anmeldeinformationen. Indem Sie MFA für Benutzer vorschreiben, können Sie Fälle kompromittierter Konten reduzieren und verhindern, dass unbefugte Benutzer auf vertrauliche Daten zugreifen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-IA-2(11)	IA-2(11) Identifizierung und Authentifizierung (Benutzer im Unternehmen) | Zugriff auf Konten – separates Gerät	root-account-mfa-enabled	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass MFA für den Root-Benutzer aktiviert ist. Der Stammbenutzer ist der AWS-Konto-Benutzer mit den meisten Berechtigungen. MFA bietet eine weitere Schutzebene zusätzlich zum Benutzernamen und Passwort. Indem Sie MFA für den Root-Benutzer vorschreiben, können Sie die Anzahl AWS-Konten kompromittierter Benutzer reduzieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-IA-2.A	IA-2.A Identifizierung und Authentifizierung (Benutzer im Unternehmen)	iam-password-policy	Die Identitäten und Anmeldeinformationen werden auf der Grundlage einer organisatorischen IAM-Passwortrichtlinie ausgestellt, verwaltet und verifiziert. Sie erfüllen oder übertreffen die Anforderungen von NIST SP 800-63 und dem Standard „Best Practices“ von AWS Foundational Security für die Passwortstärke. Mit dieser Regel können Sie optional RequireUppercaseCharacters (Wert für AWS grundlegende Sicherheitsbewährte Verfahren: wahr), RequireLowercaseCharacters (Wert für bewährte Methoden für AWS grundlegende Sicherheit: wahr), RequireSymbols (Wert für bewährte Methoden für AWS grundlegende Sicherheit:

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
			wahr), RequireNumbers (Wert für bewährte Methoden für AWS grundlegende Sicherheit: wahr), MinimumPasswordLength (Wert für bewährte Methoden für AWS grundlegende Sicherheit: 14), PasswordReusePrevention (Wert für bewährte Methoden für AWS grundlegende Sicherheit: 24) und MaxPasswordAge (Wert für bewährte Methoden für AWS grundlegende Sicherheit: 90) für Ihr IAM festlegen Kennwortrichtlinie. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-IA-2.A	IA-2.A Identifizierung und Authentifizierung (Benutzer im Unternehmen)	iam-user-mfa-enabled	Aktivieren Sie diese Regel, um den Zugriff auf Ressourcen in der AWS -Cloud einzuschränken. Diese Regel stellt sicher, dass die Multi-Faktor-Authentifizierung (MFA) für alle Benutzer aktiviert ist. MFA bietet eine weitere Schutzebene zusätzlich zum Benutzernamen und Passwort. Reduzieren Sie Fälle von kompromittierten Konten, indem Sie MFA für Benutzer vorschreiben.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-IA-2.A	IA-2.A Identifizierung und Authentifizierung (Benutzer im Unternehmen)	mfa-enabled-for-iam-Konsolenzugriff	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass MFA für alle AWS Identity and Access Management (IAM) -Benutzer aktiviert ist, die über ein Konsolenkennwort verfügen. MFA sorgt für eine weitere Schutzebene zusätzlich zu den Anmeldeinformationen. Indem Sie MFA für Benutzer vorschreiben, können Sie Fälle kompromittierter Konten reduzieren und verhindern, dass unbefugte Benutzer auf vertrauliche Daten zugreifen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-IA-2.A	IA-2.A Identifizierung und Authentifizierung (Benutzer im Unternehmen)	root-account-mfa-enabled	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass MFA für den Root-Benutzer aktiviert ist. Der Stammbenutzer ist der AWS-Konto-Benutzer mit den meisten Berechtigungen. MFA bietet eine weitere Schutzebene zusätzlich zum Benutzernamen und Passwort. Indem Sie MFA für den Root-Benutzer vorschreiben, können Sie die Anzahl AWS-Konten kompromittierter Benutzer reduzieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-IA-4(4)	IA-4(4) Verwaltung von Identifikatoren | Identifizieren des Benutzerstatus	iam-root-access-key-überprüfen	Der Zugriff auf Systeme und Ressourcen kann gesteuert werden, indem überprüft wird, ob der Root-Benutzer keine Zugriffsschlüssel mit seiner AWS Identity and Access Management (IAM) -Rolle verknüpft hat. Stellen Sie sicher, dass die Root-Zugriffsschlüssel gelöscht werden. Erstellen und verwenden Sie stattdessen rollenbasierte Funktionen, AWS-Konten um das Prinzip der geringsten Funktionalität zu berücksichtigen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-IA-4.A	IA-4.A Verwaltung von Identifikatoren	access-keys-rotated	Die Anmeldein formationen für autorisierte Geräte, Benutzer und Prozesse werden geprüft, indem sichergestellt wird, dass die IAM-Zugri ffsschlüssel entsprech end den Vorgaben der Unternehmensrichtl inie rotiert werden. Das regelmäßi ge Ändern der Zugriffsschlüssel ist eine bewährte Sicherheitsmethode . Es verkürzt den Zeitraum, in dem ein Zugriffsschlüssel aktiv ist, und reduziert die Auswirkungen auf das Unternehmen, wenn die Schlüssel kompromittiert werden. Diese Regel erfordert einen Wert für die Zugriffsschlüssel-Rotation (Standard konfiguration: 90). Der tatsächliche Wert muss den Richtlini

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
			en Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-IA-4.A	IA-4.A Verwaltung von Identifikatoren	iam-password-policy	Die Identitäten und Anmeldeinformationen werden auf der Grundlage einer organisatorischen IAM-Passwortrichtlinie ausgestellt, verwaltet und verifiziert. Sie erfüllen oder übertreffen die Anforderungen von NIST SP 800-63 und dem Standard „Best Practices“ von AWS Foundational Security in Bezug auf die Passwortstärke. Mit dieser Regel können Sie optional RequireUppercaseCharacters (Wert für AWS grundlegende Sicherheitsbewährte Verfahren: wahr), RequireLowercaseCharacters (Wert für bewährte Methoden für AWS grundlegende Sicherheit: wahr), RequireSymbols (Wert für bewährte Methoden für AWS grundlegende Sicherheit:

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
			wahr), RequireNumbers (Wert für bewährte Methoden für AWS grundlegende Sicherheit: wahr), MinimumPasswordLength (Wert für bewährte Methoden für AWS grundlegende Sicherheit: 14), PasswordReusePrevention (Wert für bewährte Methoden für AWS grundlegende Sicherheit: 24) und MaxPasswordAge (Wert für bewährte Methoden für AWS grundlegende Sicherheit: 90) für Ihr IAM festlegen Kennwortrichtlinie. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-IA-4.A	IA-4.A Verwaltung von Identifikatoren	iam-root-access-key-überprüfen	Der Zugriff auf Systeme und Ressourcen kann gesteuert werden, indem überprüft wird, ob der Root-Benutzer keine Zugriffsschlüssel mit seiner AWS Identity and Access Management (IAM) -Rolle verknüpft hat. Stellen Sie sicher, dass die Root-Zugriffsschlüssel gelöscht werden. Erstellen und verwenden Sie stattdessen rollenbasierte Funktionen, AWS-Konten um das Prinzip der geringsten Funktionalität zu berücksichtigen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-IA-4.B	IA-4.B Verwaltung von Identifikatoren	access-keys-rotated	Die Anmeldein formationen für autorisierte Geräte, Benutzer und Prozesse werden geprüft, indem sichergestellt wird, dass die IAM-Zugri ffsschlüssel entsprech end den Vorgaben der Unternehmensrichtl inie rotiert werden. Das regelmäßi ge Ändern der Zugriffsschlüssel ist eine bewährte Sicherheitsmethode . Es verkürzt den Zeitraum, in dem ein Zugriffsschlüssel aktiv ist, und reduziert die Auswirkungen auf das Unternehmen, wenn die Schlüssel kompromittiert werden. Diese Regel erfordert einen Wert für die Zugriffsschlüssel-Rotation (Standard konfiguration: 90). Der tatsächliche Wert muss den Richtlini

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
			en Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-IA-4.B	IA-4.B Verwaltung von Identifikatoren	iam-password-policy	Die Identitäten und Anmeldeinformationen werden auf der Grundlage einer organisatorischen IAM-Passwortrichtlinie ausgestellt, verwaltet und verifiziert. Sie erfüllen oder übertreffen die Anforderungen von NIST SP 800-63 und dem Standard „Best Practices“ von AWS Foundational Security in Bezug auf die Passwortstärke. Mit dieser Regel können Sie optional RequireUppercaseCharacters (Wert für AWS grundlegende Sicherheitsbewährte Verfahren: wahr), RequireLowercaseCharacters (Wert für bewährte Methoden für AWS grundlegende Sicherheit: wahr), RequireSymbols (Wert für bewährte Methoden für AWS grundlegende Sicherheit:

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
			wahr), RequireNumbers (Wert für bewährte Methoden für AWS grundlegende Sicherheit: wahr), MinimumPasswordLength (Wert für bewährte Methoden für AWS grundlegende Sicherheit: 14), PasswordReusePrevention (Wert für bewährte Methoden für AWS grundlegende Sicherheit: 24) und MaxPasswordAge (Wert für bewährte Methoden für AWS grundlegende Sicherheit: 90) für Ihr IAM festlegen Kennwortrichtlinie. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-IA-4.B	IA-4.B Verwaltung von Identifikatoren	iam-root-access-key-überprüfen	Der Zugriff auf Systeme und Ressourcen kann gesteuert werden, indem überprüft wird, ob der Root-Benutzer keine Zugriffsschlüssel mit seiner AWS Identity and Access Management (IAM) -Rolle verknüpft hat. Stellen Sie sicher, dass die Root-Zugriffsschlüssel gelöscht werden. Erstellen und verwenden Sie stattdessen rollenbasierte Funktionen, AWS-Konten um das Prinzip der geringsten Funktionalität zu berücksichtigen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-IA-4.C	IA-4.C Verwaltung von Identifikatoren	access-keys-rotated	Die Anmeldein formationen für autorisierte Geräte, Benutzer und Prozesse werden geprüft, indem sichergestellt wird, dass die IAM-Zugri ffsschlüssel entsprech end den Vorgaben der Unternehmensrichtl inie rotiert werden. Das regelmäßi ge Ändern der Zugriffsschlüssel ist eine bewährte Sicherheitsmethode . Es verkürzt den Zeitraum, in dem ein Zugriffsschlüssel aktiv ist, und reduziert die Auswirkungen auf das Unternehmen, wenn die Schlüssel kompromittiert werden. Diese Regel erfordert einen Wert für die Zugriffsschlüssel-Rotation (Standard konfiguration: 90). Der tatsächliche Wert muss den Richtlini

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
			en Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-IA-4.C	IA-4.C Verwaltung von Identifikatoren	iam-password-policy	Die Identitäten und Anmeldeinformationen werden auf der Grundlage einer organisatorischen IAM-Passwortrichtlinie ausgestellt, verwaltet und verifiziert. Sie erfüllen oder übertreffen die Anforderungen von NIST SP 800-63 und dem Standard „Best Practices“ von AWS Foundational Security in Bezug auf die Passwortstärke. Mit dieser Regel können Sie optional RequireUppercaseCharacters (Wert für AWS grundlegende Sicherheitsbewährte Verfahren: wahr), RequireLowercaseCharacters (Wert für bewährte Methoden für AWS grundlegende Sicherheit: wahr), RequireSymbols (Wert für bewährte Methoden für AWS grundlegende Sicherheit:

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
			wahr), RequireNumbers (Wert für bewährte Methoden für AWS grundlegende Sicherheit: wahr), MinimumPasswordLength (Wert für bewährte Methoden für AWS grundlegende Sicherheit: 14), PasswordReusePrevention (Wert für bewährte Methoden für AWS grundlegende Sicherheit: 24) und MaxPasswordAge (Wert für bewährte Methoden für AWS grundlegende Sicherheit: 90) für Ihr IAM festlegen Kennwortrichtlinie. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-IA-4.C	IA-4.C Verwaltung von Identifikatoren	iam-root-access-key-überprüfen	Der Zugriff auf Systeme und Ressourcen kann gesteuert werden, indem überprüft wird, ob der Root-Benutzer keine Zugriffsschlüssel mit seiner AWS Identity and Access Management (IAM) -Rolle verknüpft hat. Stellen Sie sicher, dass die Root-Zugriffsschlüssel gelöscht werden. Erstellen und verwenden Sie stattdessen rollenbasierte Funktionen, AWS-Konten um das Prinzip der geringsten Funktionalität zu berücksichtigen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-IA-4.D	IA-4.D Verwaltung von Identifikatoren	access-keys-rotated	Die Anmeldein formationen für autorisierte Geräte, Benutzer und Prozesse werden geprüft, indem sichergestellt wird, dass die IAM-Zugri ffsschlüssel entsprech end den Vorgaben der Unternehmensrichtl inie rotiert werden. Das regelmäßi ge Ändern der Zugriffsschlüssel ist eine bewährte Sicherheitsmethode . Es verkürzt den Zeitraum, in dem ein Zugriffsschlüssel aktiv ist, und reduziert die Auswirkungen auf das Unternehmen, wenn die Schlüssel kompromittiert werden. Diese Regel erfordert einen Wert für die Zugriffsschlüssel-Rotation (Standard konfiguration: 90). Der tatsächliche Wert muss den Richtlini

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
			en Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-IA-4.D	IA-4.D Verwaltung von Identifikatoren	iam-password-policy	Die Identitäten und Anmeldeinformationen werden auf der Grundlage einer organisatorischen IAM-Passwortrichtlinie ausgestellt, verwaltet und verifiziert. Sie erfüllen oder übertreffen die Anforderungen von NIST SP 800-63 und dem Standard „Best Practices“ von AWS Foundational Security in Bezug auf die Passwortstärke. Mit dieser Regel können Sie optional RequireUppercaseCharacters (Wert für AWS grundlegende Sicherheitsbewährte Verfahren: wahr), RequireLowercaseCharacters (Wert für bewährte Methoden für AWS grundlegende Sicherheit: wahr), RequireSymbols (Wert für bewährte Methoden für AWS grundlegende Sicherheit:

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
			wahr), RequireNumbers (Wert für bewährte Methoden für AWS grundlegende Sicherheit: wahr), MinimumPasswordLength (Wert für bewährte Methoden für AWS grundlegende Sicherheit: 14), PasswordReusePrevention (Wert für bewährte Methoden für AWS grundlegende Sicherheit: 24) und MaxPasswordAge (Wert für bewährte Methoden für AWS grundlegende Sicherheit: 90) für Ihr IAM festlegen Kennwortrichtlinie. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-IA-4.D	IA-4.D Verwaltung von Identifikatoren	iam-root-access-key-überprüfen	Der Zugriff auf Systeme und Ressourcen kann gesteuert werden, indem überprüft wird, ob der Root-Benutzer keine Zugriffsschlüssel mit seiner AWS Identity and Access Management (IAM) -Rolle verknüpft hat. Stellen Sie sicher, dass die Root-Zugriffsschlüssel gelöscht werden. Erstellen und verwenden Sie stattdessen rollenbasierte Funktionen, AWS-Konten um das Prinzip der geringsten Funktionalität zu berücksichtigen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-IA-4.E	IA-4.E Verwaltung von Identifikatoren	access-keys-rotated	Die Anmeldein formationen für autorisierte Geräte, Benutzer und Prozesse werden geprüft, indem sichergestellt wird, dass die IAM-Zugri ffsschlüssel entsprech end den Vorgaben der Unternehmensrichtl inie rotiert werden. Das regelmäßi ge Ändern der Zugriffsschlüssel ist eine bewährte Sicherheitsmethode . Es verkürzt den Zeitraum, in dem ein Zugriffsschlüssel aktiv ist, und reduziert die Auswirkungen auf das Unternehmen, wenn die Schlüssel kompromittiert werden. Diese Regel erfordert einen Wert für die Zugriffsschlüssel-Rotation (Standard konfiguration: 90). Der tatsächliche Wert muss den Richtlini

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
			en Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-IA-4.E	IA-4.E Verwaltung von Identifikatoren	iam-password-policy	Die Identitäten und Anmeldeinformationen werden auf der Grundlage einer organisatorischen IAM-Passwortrichtlinie ausgestellt, verwaltet und verifiziert. Sie erfüllen oder übertreffen die Anforderungen von NIST SP 800-63 und dem Standard „Best Practices“ von AWS Foundational Security in Bezug auf die Passwortstärke. Mit dieser Regel können Sie optional RequireUppercaseCharacters (Wert für AWS grundlegende Sicherheitsbewährte Verfahren: wahr), RequireLowercaseCharacters (Wert für bewährte Methoden für AWS grundlegende Sicherheit: wahr), RequireSymbols (Wert für bewährte Methoden für AWS grundlegende Sicherheit:

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
			wahr), RequireNumbers (Wert für bewährte Methoden für AWS grundlegende Sicherheit: wahr), MinimumPasswordLength (Wert für bewährte Methoden für AWS grundlegende Sicherheit: 14), PasswordReusePrevention (Wert für bewährte Methoden für AWS grundlegende Sicherheit: 24) und MaxPasswordAge (Wert für bewährte Methoden für AWS grundlegende Sicherheit: 90) für Ihr IAM festlegen Kennwortrichtlinie. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-IA-4.E	IA-4.E Verwaltung von Identifikatoren	iam-root-access-key-überprüfen	Der Zugriff auf Systeme und Ressourcen kann gesteuert werden, indem überprüft wird, ob der Root-Benutzer keine Zugriffsschlüssel mit seiner AWS Identity and Access Management (IAM) -Rolle verknüpft hat. Stellen Sie sicher, dass die Root-Zugriffsschlüssel gelöscht werden. Erstellen und verwenden Sie stattdessen rollenbasierte Funktionen, AWS-Konten um das Prinzip der geringsten Funktionalität zu berücksichtigen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-IA-5(1)	IA-5(1) Verwaltung von Authentifikatoren | Passwortbasierte Authentifizierung	iam-password-policy	Die Identitäten und Anmeldeinformationen werden auf der Grundlage einer organisatorischen IAM-Passwortrichtlinie ausgestellt, verwaltet und verifiziert. Sie erfüllen oder übertreffen die Anforderungen, die von NIST SP 800-63 und dem Standard „Best Practices“ von AWS Foundational Security in Bezug auf die Passwortstärke festgelegt wurden. Mit dieser Regel können Sie optional RequireUppercaseCharacters (Wert für AWS grundlegende Sicherheitsbewährte Verfahren: wahr), RequireLowercaseCharacters (Wert für bewährte Methoden für AWS grundlegende Sicherheit: wahr), RequireSymbols (Wert für bewährte Methoden

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
			für AWS grundlegende Sicherheit: wahr), RequireNumbers (Wert für bewährte Methoden für AWS grundlegende Sicherheit: wahr), MinimumPasswordLength (Wert für bewährte Methoden für AWS grundlegende Sicherheit: 14), PasswordReusePrevention (Wert für bewährte Methoden für AWS grundlegende Sicherheit: 24) und MaxPasswordAge (Wert für bewährte Methoden für AWS grundlegende Sicherheit: 90) für Ihr IAM festlegen Kennwortrichtlinie. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-IA-5(2)	IA-5(2) Verwaltung von Authentifikatoren | PKI-basierte Authentifizierung	elb-v-2 acm-certificate-required	Zum Schutz von eventuell vorhanden en sensiblen Daten sowie von Daten während der Übertragung muss die Verschlüsselung für Ihr Elastic Load Balancing aktiviert sein. Verwenden Sie AWS Certificate Manager, um öffentlic he und private SSL/ TLS-Zertifikate mit AWS Diensten und internen Ressource n zu verwalten, bereitzustellen und bereitzustellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-IA-5(2)	IA-5(2) Verwaltung von Authentifikatoren | PKI-basierte Authentifizierung	elb-acm-certificate-required	Zum Schutz von eventuell vorhanden en sensiblen Daten sowie von Daten während der Übertragung muss die Verschlüsselung für Ihr Elastic Load Balancing aktiviert sein. Verwenden Sie AWS Certificate Manager, um öffentlic he und private SSL/ TLS-Zertifikate mit AWS Diensten und internen Ressource n zu verwalten, bereitzustellen und bereitzustellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-IA-5(4)	IA-5(4) Verwaltung von Authentifikatoren | Automatisierter Support für die Bestimmung der Passwortstärke	iam-password-policy	Die Identitäten und Anmeldeinformationen werden auf der Grundlage einer organisatorischen IAM-Passwortrichtlinie ausgestellt, verwaltet und verifiziert. Sie erfüllen oder übertreffen die Anforderungen von NIST SP 800-63 und dem Standard „Best Practices“ von AWS Foundational Security für die Passwortstärke. Mit dieser Regel können Sie optional RequireUppercaseCharacters (Wert für AWS grundlegende Sicherheitsbewährte Verfahren: wahr), RequireLowercaseCharacters (Wert für bewährte Methoden für AWS grundlegende Sicherheit: wahr), RequireSymbols (Wert für bewährte Methoden für AWS grundlegende Sicherheit:

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
			wahr), RequireNumbers (Wert für bewährte Methoden für AWS grundlegende Sicherheit: wahr), MinimumPasswordLength (Wert für bewährte Methoden für AWS grundlegende Sicherheit: 14), PasswordReusePrevention (Wert für bewährte Methoden für AWS grundlegende Sicherheit: 24) und MaxPasswordAge (Wert für bewährte Methoden für AWS grundlegende Sicherheit: 90) für Ihr IAM festlegen Kennwortrichtlinie. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-IA-5(8)	IA-5(8) Verwaltung von Authentifikatoren | Mehrere Informati onssystemkonten	iam-root-access-key-überprüfen	Der Zugriff auf Systeme und Ressourcen kann gesteuert werden, indem überprüft wird, ob der Root-Benu tzer keine Zugriffss chlüssel mit seiner AWS Identity and Access Management (IAM) -Rolle verknüpft hat. Stellen Sie sicher, dass die Root-Zugr iffsschlüssel gelöscht werden. Erstellen und verwenden Sie stattdessen rollenbas ierte Funktionen, AWS-Konten um das Prinzip der geringste n Funktionalität zu berücksichtigen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-IA-5(8)	IA-5(8) Verwaltung von Authentifikatoren | Mehrere Informati onssystemkonten	iam-user-mfa-enabled	Aktivieren Sie diese Regel, um den Zugriff auf Ressourcen in der AWS -Cloud einzuschränken. Diese Regel stellt sicher, dass die Multi-Faktor-Authe ntifizierung (MFA) für alle Benutzer aktiviert ist. MFA bietet eine weitere Schutzebene zusätzlic h zum Benutzern amen und Passwort. Reduzieren Sie Fälle von kompromittierten Konten, indem Sie MFA für Benutzer vorschreiben.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-IA-5(8)	IA-5(8) Verwaltung von Authentifikatoren | Mehrere Informationssystemkonten	mfa-enabled-for-iam-Konsolenzugriff	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass MFA für alle AWS Identity and Access Management (IAM) -Benutzer aktiviert ist, die über ein Konsolenkennwort verfügen. MFA sorgt für eine weitere Schutzebene zusätzlich zu den Anmeldeinformationen. Indem Sie MFA für Benutzer vorschreiben, können Sie Fälle kompromittierter Konten reduzieren und verhindern, dass unbefugte Benutzer auf vertrauliche Daten zugreifen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-IA-5.A	IA-5.A Verwaltung von Authentifikatoren	iam-password-policy	Die Identitäten und Anmeldeinformationen werden auf der Grundlage einer organisatorischen IAM-Passwortrichtlinie ausgestellt, verwaltet und verifiziert. Sie erfüllen oder übertreffen die Anforderungen von NIST SP 800-63 und dem Standard „Best Practices“ von AWS Foundational Security für die Passwortstärke. Mit dieser Regel können Sie optional RequireUppercaseCharacters (Wert für AWS grundlegende Sicherheitsbewährte Verfahren: wahr), RequireLowercaseCharacters (Wert für bewährte Methoden für AWS grundlegende Sicherheit: wahr), RequireSymbols (Wert für bewährte Methoden für AWS grundlegende Sicherheit:

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
			wahr), RequireNumbers (Wert für bewährte Methoden für AWS grundlegende Sicherheit: wahr), MinimumPasswordLength (Wert für bewährte Methoden für AWS grundlegende Sicherheit: 14), PasswordReusePrevention (Wert für bewährte Methoden für AWS grundlegende Sicherheit: 24) und MaxPasswordAge (Wert für bewährte Methoden für AWS grundlegende Sicherheit: 90) für Ihr IAM festlegen Kennwortrichtlinie. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-IA-5.A	IA-5.A Verwaltung von Authentifikatoren	iam-user-mfa-enabled	Aktivieren Sie diese Regel, um den Zugriff auf Ressourcen in der AWS -Cloud einzuschränken. Diese Regel stellt sicher, dass die Multi-Faktor-Authentifizierung (MFA) für alle Benutzer aktiviert ist. MFA bietet eine weitere Schutzebene zusätzlich zum Benutzernamen und Passwort. Reduzieren Sie Fälle von kompromittierten Konten, indem Sie MFA für Benutzer vorschreiben.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-IA-5.A	IA-5.A Verwaltung von Authentifikatoren	mfa-enabled-for-iam-Konsolenzugriff	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass MFA für alle AWS Identity and Access Management (IAM) -Benutzer aktiviert ist, die über ein Konsolenkennwort verfügen. MFA sorgt für eine weitere Schutzebene zusätzlich zu den Anmeldeinformationen. Indem Sie MFA für Benutzer vorschreiben, können Sie Fälle kompromittierter Konten reduzieren und verhindern, dass unbefugte Benutzer auf vertrauliche Daten zugreifen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-IA-5.A	IA-5.A Verwaltung von Authentifikatoren	root-account-mfa-enabled	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass MFA für den Root-Benutzer aktiviert ist. Der Stammbenutzer ist der AWS-Konto-Benutzer mit den meisten Berechtigungen. MFA bietet eine weitere Schutzebene zusätzlich zum Benutzernamen und Passwort. Indem Sie MFA für den Root-Benutzer vorschreiben, können Sie die Anzahl AWS-Konten kompromittierter Benutzer reduzieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-IA-5.B	IA-5.B Verwaltung von Authentifikatoren	iam-password-policy	Die Identitäten und Anmeldeinformationen werden auf der Grundlage einer organisatorischen IAM-Passwortrichtlinie ausgestellt, verwaltet und verifiziert. Sie erfüllen oder übertreffen die Anforderungen von NIST SP 800-63 und dem Standard „Best Practices“ von AWS Foundational Security für die Passwortstärke. Mit dieser Regel können Sie optional RequireUppercaseCharacters (Wert für AWS grundlegende Sicherheitsbewährte Verfahren: wahr), RequireLowercaseCharacters (Wert für bewährte Methoden für AWS grundlegende Sicherheit: wahr), RequireSymbols (Wert für bewährte Methoden für AWS grundlegende Sicherheit:

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
			wahr), RequireNumbers (Wert für bewährte Methoden für AWS grundlegende Sicherheit: wahr), MinimumPasswordLength (Wert für bewährte Methoden für AWS grundlegende Sicherheit: 14), PasswordReusePrevention (Wert für bewährte Methoden für AWS grundlegende Sicherheit: 24) und MaxPasswordAge (Wert für bewährte Methoden für AWS grundlegende Sicherheit: 90) für Ihr IAM festlegen Kennwortrichtlinie. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-IA-5.B	IA-5.B Verwaltung von Authentifikatoren	iam-user-mfa-enabled	Aktivieren Sie diese Regel, um den Zugriff auf Ressourcen in der AWS -Cloud einzuschränken. Diese Regel stellt sicher, dass die Multi-Faktor-Authentifizierung (MFA) für alle Benutzer aktiviert ist. MFA bietet eine weitere Schutzebene zusätzlich zum Benutzernamen und Passwort. Reduzieren Sie Fälle von kompromittierten Konten, indem Sie MFA für Benutzer vorschreiben.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-IA-5.B	IA-5.B Verwaltung von Authentifikatoren	mfa-enabled-for-iam-Konsolenzugriff	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass MFA für alle AWS Identity and Access Management (IAM) -Benutzer aktiviert ist, die über ein Konsolenkennwort verfügen. MFA sorgt für eine weitere Schutzebene zusätzlich zu den Anmeldeinformationen. Indem Sie MFA für Benutzer vorschreiben, können Sie Fälle kompromittierter Konten reduzieren und verhindern, dass unbefugte Benutzer auf vertrauliche Daten zugreifen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-IA-5.B	IA-5.B Verwaltung von Authentifikatoren	root-account-mfa-enabled	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass MFA für den Root-Benutzer aktiviert ist. Der Stammbenutzer ist der AWS-Konto-Benutzer mit den meisten Berechtigungen. MFA bietet eine weitere Schutzebene zusätzlich zum Benutzernamen und Passwort. Indem Sie MFA für den Root-Benutzer vorschreiben, können Sie die Anzahl AWS-Konten kompromittierter Benutzer reduzieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-IA-5.C	IA-5.C Verwaltung von Authentifikatoren	iam-password-policy	Die Identitäten und Anmeldeinformationen werden auf der Grundlage einer organisatorischen IAM-Passwortrichtlinie ausgestellt, verwaltet und verifiziert. Sie erfüllen oder übertreffen die Anforderungen von NIST SP 800-63 und dem Standard „Best Practices“ von AWS Foundational Security für die Passwortstärke. Mit dieser Regel können Sie optional RequireUppercaseCharacters (Wert für AWS grundlegende Sicherheitsbewährte Verfahren: wahr), RequireLowercaseCharacters (Wert für bewährte Methoden für AWS grundlegende Sicherheit: wahr), RequireSymbols (Wert für bewährte Methoden für AWS grundlegende Sicherheit:

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
			wahr), RequireNumbers (Wert für bewährte Methoden für AWS grundlegende Sicherheit: wahr), MinimumPasswordLength (Wert für bewährte Methoden für AWS grundlegende Sicherheit: 14), PasswordReusePrevention (Wert für bewährte Methoden für AWS grundlegende Sicherheit: 24) und MaxPasswordAge (Wert für bewährte Methoden für AWS grundlegende Sicherheit: 90) für Ihr IAM festlegen Kennwortrichtlinie. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-IA-5.C	IA-5.C Verwaltung von Authentifikatoren	iam-user-mfa-enabled	Aktivieren Sie diese Regel, um den Zugriff auf Ressourcen in der AWS -Cloud einzuschränken. Diese Regel stellt sicher, dass die Multi-Faktor-Authentifizierung (MFA) für alle Benutzer aktiviert ist. MFA bietet eine weitere Schutzebene zusätzlich zum Benutzernamen und Passwort. Reduzieren Sie Fälle von kompromittierten Konten, indem Sie MFA für Benutzer vorschreiben.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-IA-5.C	IA-5.C Verwaltung von Authentifikatoren	mfa-enabled-for-iam-Konsolenzugriff	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass MFA für alle AWS Identity and Access Management (IAM) -Benutzer aktiviert ist, die über ein Konsolenkennwort verfügen. MFA sorgt für eine weitere Schutzebene zusätzlich zu den Anmeldeinformationen. Indem Sie MFA für Benutzer vorschreiben, können Sie Fälle kompromittierter Konten reduzieren und verhindern, dass unbefugte Benutzer auf vertrauliche Daten zugreifen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-IA-5.C	IA-5.C Verwaltung von Authentifikatoren	root-account-mfa-enabled	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass MFA für den Root-Benutzer aktiviert ist. Der Stammbenutzer ist der AWS-Konto-Benutzer mit den meisten Berechtigungen. MFA bietet eine weitere Schutzebene zusätzlich zum Benutzernamen und Passwort. Indem Sie MFA für den Root-Benutzer vorschreiben, können Sie die Anzahl AWS-Konten kompromittierter Benutzer reduzieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-IA-5.D	IA-5.D Verwaltung von Authentifikatoren	iam-password-policy	Die Identitäten und Anmeldeinformationen werden auf der Grundlage einer organisatorischen IAM-Passwortrichtlinie ausgestellt, verwaltet und verifiziert. Sie erfüllen oder übertreffen die Anforderungen von NIST SP 800-63 und dem Standard „Best Practices“ von AWS Foundational Security für die Passwortstärke. Mit dieser Regel können Sie optional RequireUppercaseCharacters (Wert für AWS grundlegende Sicherheitsbewährte Verfahren: wahr), RequireLowercaseCharacters (Wert für bewährte Methoden für AWS grundlegende Sicherheit: wahr), RequireSymbols (Wert für bewährte Methoden für AWS grundlegende Sicherheit:

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
			wahr), RequireNumbers (Wert für bewährte Methoden für AWS grundlegende Sicherheit: wahr), MinimumPasswordLength (Wert für bewährte Methoden für AWS grundlegende Sicherheit: 14), PasswordReusePrevention (Wert für bewährte Methoden für AWS grundlegende Sicherheit: 24) und MaxPasswordAge (Wert für bewährte Methoden für AWS grundlegende Sicherheit: 90) für Ihr IAM festlegen Kennwortrichtlinie. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-IA-5.D	IA-5.D Verwaltung von Authentifikatoren	iam-user-mfa-enabled	Aktivieren Sie diese Regel, um den Zugriff auf Ressourcen in der AWS -Cloud einzuschränken. Diese Regel stellt sicher, dass die Multi-Faktor-Authentifizierung (MFA) für alle Benutzer aktiviert ist. MFA bietet eine weitere Schutzebene zusätzlich zum Benutzernamen und Passwort. Reduzieren Sie Fälle von kompromittierten Konten, indem Sie MFA für Benutzer vorschreiben.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-IA-5.D	IA-5.D Verwaltung von Authentifikatoren	mfa-enabled-for-iam-Konsolenzugriff	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass MFA für alle AWS Identity and Access Management (IAM) -Benutzer aktiviert ist, die über ein Konsolenkennwort verfügen. MFA sorgt für eine weitere Schutzebene zusätzlich zu den Anmeldeinformationen. Indem Sie MFA für Benutzer vorschreiben, können Sie Fälle kompromittierter Konten reduzieren und verhindern, dass unbefugte Benutzer auf vertrauliche Daten zugreifen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-IA-5.D	IA-5.D Verwaltung von Authentifikatoren	root-account-mfa-enabled	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass MFA für den Root-Benutzer aktiviert ist. Der Stammbenutzer ist der AWS-Konto-Benutzer mit den meisten Berechtigungen. MFA bietet eine weitere Schutzebene zusätzlich zum Benutzernamen und Passwort. Indem Sie MFA für den Root-Benutzer vorschreiben, können Sie die Anzahl AWS-Konten kompromittierter Benutzer reduzieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-IA-5.E	IA-5.E Verwaltung von Authentifikatoren	iam-password-policy	Die Identitäten und Anmeldeinformationen werden auf der Grundlage einer organisatorischen IAM-Passwortrichtlinie ausgestellt, verwaltet und verifiziert. Sie erfüllen oder übertreffen die Anforderungen von NIST SP 800-63 und dem Standard „Best Practices“ von AWS Foundational Security für die Passwortstärke. Mit dieser Regel können Sie optional RequireUppercaseCharacters (Wert für AWS grundlegende Sicherheitsbewährte Verfahren: wahr), RequireLowercaseCharacters (Wert für bewährte Methoden für AWS grundlegende Sicherheit: wahr), RequireSymbols (Wert für bewährte Methoden für AWS grundlegende Sicherheit:

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
			wahr), RequireNumbers (Wert für bewährte Methoden für AWS grundlegende Sicherheit: wahr), MinimumPasswordLength (Wert für bewährte Methoden für AWS grundlegende Sicherheit: 14), PasswordReusePrevention (Wert für bewährte Methoden für AWS grundlegende Sicherheit: 24) und MaxPasswordAge (Wert für bewährte Methoden für AWS grundlegende Sicherheit: 90) für Ihr IAM festlegen Kennwortrichtlinie. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-IA-5.E	IA-5.E Verwaltung von Authentifikatoren	iam-user-mfa-enabled	Aktivieren Sie diese Regel, um den Zugriff auf Ressourcen in der AWS -Cloud einzuschränken. Diese Regel stellt sicher, dass die Multi-Faktor-Authentifizierung (MFA) für alle Benutzer aktiviert ist. MFA bietet eine weitere Schutzebene zusätzlich zum Benutzernamen und Passwort. Reduzieren Sie Fälle von kompromittierten Konten, indem Sie MFA für Benutzer vorschreiben.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-IA-5.E	IA-5.E Verwaltung von Authentifikatoren	mfa-enabled-for-iam-Konsolenzugriff	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass MFA für alle AWS Identity and Access Management (IAM) -Benutzer aktiviert ist, die über ein Konsolenkennwort verfügen. MFA sorgt für eine weitere Schutzebene zusätzlich zu den Anmeldeinformationen. Indem Sie MFA für Benutzer vorschreiben, können Sie Fälle kompromittierter Konten reduzieren und verhindern, dass unbefugte Benutzer auf vertrauliche Daten zugreifen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-IA-5.E	IA-5.E Verwaltung von Authentifikatoren	root-account-mfa-enabled	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass MFA für den Root-Benutzer aktiviert ist. Der Stammbenutzer ist der AWS-Konto-Benutzer mit den meisten Berechtigungen. MFA bietet eine weitere Schutzebene zusätzlich zum Benutzernamen und Passwort. Indem Sie MFA für den Root-Benutzer vorschreiben, können Sie die Anzahl AWS-Konten kompromittierter Benutzer reduzieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-IA-5.F	IA-5.F Verwaltung von Authentifikatoren	iam-password-policy	Die Identitäten und Anmeldeinformationen werden auf der Grundlage einer organisatorischen IAM-Passwortrichtlinie ausgestellt, verwaltet und verifiziert. Sie erfüllen oder übertreffen die Anforderungen von NIST SP 800-63 und dem Standard „Best Practices“ von AWS Foundational Security für die Passwortstärke. Mit dieser Regel können Sie optional RequireUppercaseCharacters (Wert für AWS grundlegende Sicherheitsbewährte Verfahren: wahr), RequireLowercaseCharacters (Wert für bewährte Methoden für AWS grundlegende Sicherheit: wahr), RequireSymbols (Wert für bewährte Methoden für AWS grundlegende Sicherheit:

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
			wahr), RequireNumbers (Wert für bewährte Methoden für AWS grundlegende Sicherheit: wahr), MinimumPasswordLength (Wert für bewährte Methoden für AWS grundlegende Sicherheit: 14), PasswordReusePrevention (Wert für bewährte Methoden für AWS grundlegende Sicherheit: 24) und MaxPasswordAge (Wert für bewährte Methoden für AWS grundlegende Sicherheit: 90) für Ihr IAM festlegen Kennwortrichtlinie. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-IA-5.F	IA-5.F Verwaltung von Authentifikatoren	iam-user-mfa-enabled	Aktivieren Sie diese Regel, um den Zugriff auf Ressourcen in der AWS -Cloud einzuschränken. Diese Regel stellt sicher, dass die Multi-Faktor-Authentifizierung (MFA) für alle Benutzer aktiviert ist. MFA bietet eine weitere Schutzebene zusätzlich zum Benutzernamen und Passwort. Reduzieren Sie Fälle von kompromittierten Konten, indem Sie MFA für Benutzer vorschreiben.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-IA-5.F	IA-5.F Verwaltung von Authentifikatoren	mfa-enabled-for-iam-Konsolenzugriff	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass MFA für alle AWS Identity and Access Management (IAM) -Benutzer aktiviert ist, die über ein Konsolenkennwort verfügen. MFA sorgt für eine weitere Schutzebene zusätzlich zu den Anmeldeinformationen. Indem Sie MFA für Benutzer vorschreiben, können Sie Fälle kompromittierter Konten reduzieren und verhindern, dass unbefugte Benutzer auf vertrauliche Daten zugreifen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-IA-5.F	IA-5.F Verwaltung von Authentifikatoren	root-account-mfa-enabled	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass MFA für den Root-Benutzer aktiviert ist. Der Stammbenutzer ist der AWS-Konto-Benutzer mit den meisten Berechtigungen. MFA bietet eine weitere Schutzebene zusätzlich zum Benutzernamen und Passwort. Indem Sie MFA für den Root-Benutzer vorschreiben, können Sie die Anzahl AWS-Konten kompromittierter Benutzer reduzieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-IA-5.G	IA-5.G Verwaltung von Authentifikatoren	iam-password-policy	Die Identitäten und Anmeldeinformationen werden auf der Grundlage einer organisatorischen IAM-Passwortrichtlinie ausgestellt, verwaltet und verifiziert. Sie erfüllen oder übertreffen die Anforderungen von NIST SP 800-63 und dem Standard „Best Practices“ von AWS Foundational Security für die Passwortstärke. Mit dieser Regel können Sie optional RequireUppercaseCharacters (Wert für AWS grundlegende Sicherheitsbewährte Verfahren: wahr), RequireLowercaseCharacters (Wert für bewährte Methoden für AWS grundlegende Sicherheit: wahr), RequireSymbols (Wert für bewährte Methoden für AWS grundlegende Sicherheit:

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
			wahr), RequireNumbers (Wert für bewährte Methoden für AWS grundlegende Sicherheit: wahr), MinimumPasswordLength (Wert für bewährte Methoden für AWS grundlegende Sicherheit: 14), PasswordReusePrevention (Wert für bewährte Methoden für AWS grundlegende Sicherheit: 24) und MaxPasswordAge (Wert für bewährte Methoden für AWS grundlegende Sicherheit: 90) für Ihr IAM festlegen Kennwortrichtlinie. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-IA-5.G	IA-5.G Verwaltung von Authentifikatoren	iam-user-mfa-enabled	Aktivieren Sie diese Regel, um den Zugriff auf Ressourcen in der AWS -Cloud einzuschränken. Diese Regel stellt sicher, dass die Multi-Faktor-Authentifizierung (MFA) für alle Benutzer aktiviert ist. MFA bietet eine weitere Schutzebene zusätzlich zum Benutzernamen und Passwort. Reduzieren Sie Fälle von kompromittierten Konten, indem Sie MFA für Benutzer vorschreiben.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-IA-5.G	IA-5.G Verwaltung von Authentifikatoren	mfa-enabled-for-iam-Konsolenzugriff	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass MFA für alle AWS Identity and Access Management (IAM) -Benutzer aktiviert ist, die über ein Konsolenkennwort verfügen. MFA sorgt für eine weitere Schutzebene zusätzlich zu den Anmeldeinformationen. Indem Sie MFA für Benutzer vorschreiben, können Sie Fälle kompromittierter Konten reduzieren und verhindern, dass unbefugte Benutzer auf vertrauliche Daten zugreifen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-IA-5.G	IA-5.G Verwaltung von Authentifikatoren	root-account-mfa-enabled	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass MFA für den Root-Benutzer aktiviert ist. Der Stammbenutzer ist der AWS-Konto-Benutzer mit den meisten Berechtigungen. MFA bietet eine weitere Schutzebene zusätzlich zum Benutzernamen und Passwort. Indem Sie MFA für den Root-Benutzer vorschreiben, können Sie die Anzahl AWS-Konten kompromittierter Benutzer reduzieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-IA-5.H	IA-5.H Verwaltung von Authentifikatoren	iam-password-policy	Die Identitäten und Anmeldeinformationen werden auf der Grundlage einer organisatorischen IAM-Passwortrichtlinie ausgestellt, verwaltet und verifiziert. Sie erfüllen oder übertreffen die Anforderungen von NIST SP 800-63 und dem Standard „Best Practices“ von AWS Foundational Security für die Passwortstärke. Mit dieser Regel können Sie optional RequireUppercaseCharacters (Wert für AWS grundlegende Sicherheitsbewährte Verfahren: wahr), RequireLowercaseCharacters (Wert für bewährte Methoden für AWS grundlegende Sicherheit: wahr), RequireSymbols (Wert für bewährte Methoden für AWS grundlegende Sicherheit:

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
			wahr), RequireNumbers (Wert für bewährte Methoden für AWS grundlegende Sicherheit: wahr), MinimumPasswordLength (Wert für bewährte Methoden für AWS grundlegende Sicherheit: 14), PasswordReusePrevention (Wert für bewährte Methoden für AWS grundlegende Sicherheit: 24) und MaxPasswordAge (Wert für bewährte Methoden für AWS grundlegende Sicherheit: 90) für Ihr IAM festlegen Kennwortrichtlinie. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-IA-5.H	IA-5.H Verwaltung von Authentifikatoren	iam-user-mfa-enabled	Aktivieren Sie diese Regel, um den Zugriff auf Ressourcen in der AWS -Cloud einzuschränken. Diese Regel stellt sicher, dass die Multi-Faktor-Authentifizierung (MFA) für alle Benutzer aktiviert ist. MFA bietet eine weitere Schutzebene zusätzlich zum Benutzernamen und Passwort. Reduzieren Sie Fälle von kompromittierten Konten, indem Sie MFA für Benutzer vorschreiben.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-IA-5.H	IA-5.H Verwaltung von Authentifikatoren	mfa-enabled-for-iam-Konsolenzugriff	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass MFA für alle AWS Identity and Access Management (IAM) -Benutzer aktiviert ist, die über ein Konsolenkennwort verfügen. MFA sorgt für eine weitere Schutzebene zusätzlich zu den Anmeldeinformationen. Indem Sie MFA für Benutzer vorschreiben, können Sie Fälle kompromittierter Konten reduzieren und verhindern, dass unbefugte Benutzer auf vertrauliche Daten zugreifen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-IA-5.H	IA-5.H Verwaltung von Authentifikatoren	root-account-mfa-enabled	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass MFA für den Root-Benutzer aktiviert ist. Der Stammbenutzer ist der AWS-Konto-Benutzer mit den meisten Berechtigungen. MFA bietet eine weitere Schutzebene zusätzlich zum Benutzernamen und Passwort. Indem Sie MFA für den Root-Benutzer vorschreiben, können Sie die Anzahl AWS-Konten kompromittierter Benutzer reduzieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-IA-5.I	IA-5.I Verwaltung von Authentifikatoren	iam-password-policy	Die Identitäten und Anmeldeinformationen werden auf der Grundlage einer organisatorischen IAM-Passwortrichtlinie ausgestellt, verwaltet und verifiziert. Sie erfüllen oder übertreffen die Anforderungen von NIST SP 800-63 und dem Standard „Best Practices“ von AWS Foundational Security für die Passwortstärke. Mit dieser Regel können Sie optional RequireUppercaseCharacters (Wert für AWS grundlegende Sicherheitsbewährte Verfahren: wahr), RequireLowercaseCharacters (Wert für bewährte Methoden für AWS grundlegende Sicherheit: wahr), RequireSymbols (Wert für bewährte Methoden für AWS grundlegende Sicherheit:

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
			wahr), RequireNumbers (Wert für bewährte Methoden für AWS grundlegende Sicherheit: wahr), MinimumPasswordLength (Wert für bewährte Methoden für AWS grundlegende Sicherheit: 14), PasswordReusePrevention (Wert für bewährte Methoden für AWS grundlegende Sicherheit: 24) und MaxPasswordAge (Wert für bewährte Methoden für AWS grundlegende Sicherheit: 90) für Ihr IAM festlegen Kennwortrichtlinie. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-IA-5.I	IA-5.I Verwaltung von Authentifikatoren	iam-user-mfa-enabled	Aktivieren Sie diese Regel, um den Zugriff auf Ressourcen in der AWS -Cloud einzuschränken. Diese Regel stellt sicher, dass die Multi-Faktor-Authentifizierung (MFA) für alle Benutzer aktiviert ist. MFA bietet eine weitere Schutzebene zusätzlich zum Benutzernamen und Passwort. Reduzieren Sie Fälle von kompromittierten Konten, indem Sie MFA für Benutzer vorschreiben.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-IA-5.I	IA-5.I Verwaltung von Authentifikatoren	mfa-enabled-for-iam-Konsolenzugriff	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass MFA für alle AWS Identity and Access Management (IAM) -Benutzer aktiviert ist, die über ein Konsolenkennwort verfügen. MFA sorgt für eine weitere Schutzebene zusätzlich zu den Anmeldeinformationen. Indem Sie MFA für Benutzer vorschreiben, können Sie Fälle kompromittierter Konten reduzieren und verhindern, dass unbefugte Benutzer auf vertrauliche Daten zugreifen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-IA-5.I	IA-5.I Verwaltung von Authentifikatoren	root-account-mfa-enabled	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass MFA für den Root-Benutzer aktiviert ist. Der Stammbenutzer ist der AWS-Konto-Benutzer mit den meisten Berechtigungen. MFA bietet eine weitere Schutzebene zusätzlich zum Benutzernamen und Passwort. Indem Sie MFA für den Root-Benutzer vorschreiben, können Sie die Anzahl AWS-Konten kompromittierter Benutzer reduzieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-IA-5.J	IA-5.J Verwaltung von Authentifikatoren	iam-password-policy	Die Identitäten und Anmeldeinformationen werden auf der Grundlage einer organisatorischen IAM-Passwortrichtlinie ausgestellt, verwaltet und verifiziert. Sie erfüllen oder übertreffen die Anforderungen von NIST SP 800-63 und dem Standard „Best Practices“ von AWS Foundational Security für die Passwortstärke. Mit dieser Regel können Sie optional RequireUppercaseCharacters (Wert für AWS grundlegende Sicherheitsbewährte Verfahren: wahr), RequireLowercaseCharacters (Wert für bewährte Methoden für AWS grundlegende Sicherheit: wahr), RequireSymbols (Wert für bewährte Methoden für AWS grundlegende Sicherheit:

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
			wahr), RequireNumbers (Wert für bewährte Methoden für AWS grundlegende Sicherheit: wahr), MinimumPasswordLength (Wert für bewährte Methoden für AWS grundlegende Sicherheit: 14), PasswordReusePrevention (Wert für bewährte Methoden für AWS grundlegende Sicherheit: 24) und MaxPasswordAge (Wert für bewährte Methoden für AWS grundlegende Sicherheit: 90) für Ihr IAM festlegen Kennwortrichtlinie. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-IA-5.J	IA-5.J Verwaltung von Authentifikatoren	iam-user-mfa-enabled	Aktivieren Sie diese Regel, um den Zugriff auf Ressourcen in der AWS -Cloud einzuschränken. Diese Regel stellt sicher, dass die Multi-Faktor-Authentifizierung (MFA) für alle Benutzer aktiviert ist. MFA bietet eine weitere Schutzebene zusätzlich zum Benutzernamen und Passwort. Reduzieren Sie Fälle von kompromittierten Konten, indem Sie MFA für Benutzer vorschreiben.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-IA-5.J	IA-5.J Verwaltung von Authentifikatoren	mfa-enabled-for-iam-Konsolenzugriff	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass MFA für alle AWS Identity and Access Management (IAM) -Benutzer aktiviert ist, die über ein Konsolenkennwort verfügen. MFA sorgt für eine weitere Schutzebene zusätzlich zu den Anmeldeinformationen. Indem Sie MFA für Benutzer vorschreiben, können Sie Fälle kompromittierter Konten reduzieren und verhindern, dass unbefugte Benutzer auf vertrauliche Daten zugreifen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-IA-5.J	IA-5.J Verwaltung von Authentifikatoren	root-account-mfa-enabled	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass MFA für den Root-Benutzer aktiviert ist. Der Stammbenutzer ist der AWS-Konto-Benutzer mit den meisten Berechtigungen. MFA bietet eine weitere Schutzebene zusätzlich zum Benutzernamen und Passwort. Indem Sie MFA für den Root-Benutzer vorschreiben, können Sie die Anzahl AWS-Konten kompromittierter Benutzer reduzieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-IR-6(1)	IR-6(1) Meldung von Vorfällen | Automatisierte Berichterstattung	guardduty-enabled-centralized	Amazon GuardDuty kann mithilfe von Threat Intelligence Feeds helfen, potenzielle Cybersicherheitsereignisse zu überwachen und zu erkennen. Dazu gehören Listen mit bösartigen IPs und maschinellen Lernmethoden zur Identifizierung unerwarteter, nicht autorisierter und bösartiger Aktivitäten in Ihrer AWS Cloud-Umgebung.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-MA-3.A	MA-3.A Wartungswerkzeuge	ec2-manager instance-managed-by-systems	Eine Bestandsaufnahme der Softwareplattformen und Anwendungen innerhalb des Unternehmens ist möglich, indem Amazon Elastic Compute Cloud (Amazon EC2) - Instances mit AWS Systems Manager verwaltet werden. Verwenden Sie AWS Systems Manager, um detaillierte Systemkonfigurationen, Betriebssystem-Patch-Levels, Namen und Typ der Dienste, Softwareinstallationen, Anwendungsname, Herausgeber und Version sowie andere Details zu Ihrer Umgebung bereitzustellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-MA-3.A	MA-3.A Wartungswerkzeuge	ec2-check managedinstance-patch-compliance-status	Aktivieren Sie diese Regel, um bei der Identifizierung und Dokumentation von Sicherheitslücken in Amazon Elastic Compute Cloud (Amazon EC2) zu helfen. Die Regel prüft, ob die EC2 Amazon-Instance die Patch-Konformität im AWS Systems Manager gemäß den Richtlinien und Verfahren Ihrer Organisation einhält.
CCCS-fPBMM-MA-4(1)	MA-4(1) Nicht lokale Wartung | Prüfung und Überprüfung	api-gw-execution-logging-aktiviert	Die API-Gateway-Protokollierung zeigt detaillierte Ansichten der Benutzer, die auf die API zugegriffen haben, und wie diese Benutzer auf die API zugegriffen haben. Diese Einblicke ermöglichen die Transparenz von Benutzeraktivitäten.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-MA-4(1)	MA-4(1) Nicht lokale Wartung | Prüfung und Überprüfung	cloudtrail-s3-data events-enabled	Die Erfassung von Simple Storage Service (Amazon S3)-Datenereignissen unterstützt die Erkennung von ungewöhnlichen Aktivitäten. Zu den Details gehören Informationen zu dem AWS -Konto, das auf einen Amazon-S3-Bucket zugegriffen hat, die IP-Adresse und die Uhrzeit des Ereignisses.
CCCS-fPBMM-MA-4(1)	MA-4(1) Nicht lokale Wartung | Prüfung und Überprüfung	cloud-trail-cloud-watch-logs-aktiviert	Verwenden Sie Amazon CloudWatch , um Protokoll ereignisaktivitäten zentral zu sammeln und zu verwalten. Die Aufnahme von AWS CloudTrail Daten liefert Einzelheiten zu den API-Aufrufaktivitäten in Ihrem AWS-Konto.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-MA-4(1)	MA-4(1) Nicht lokale Wartung | Prüfung und Überprüfung	cloudtrail-enabled	AWS CloudTrail kann bei der Nichtabstreitbarkeit helfen, indem Aktionen und API-Aufrufe der AWS Management Console aufgezeichnet werden. Sie können die Benutzer und die Benutzer AWS-Konten , die einen AWS Dienst aufgerufen haben, die Quell-IP-Adresse, über die die Aufrufe generiert wurden, und den Zeitpunkt der Anrufe identifizieren. Einzelheiten zu den erfassten Daten finden Sie unter Inhalt des AWS CloudTrail Datensatzes.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-MA-4(1)	MA-4(1) Nicht lokale Wartung | Prüfung und Überprüfung	elb-logging-enabled	Die Elastic-Load-Balancing-Aktivität ist ein zentraler Kommunikationspunkt innerhalb einer Umgebung. Stellen Sie sicher, dass die ELB-Protokollierung aktiviert ist. Die gesammelten Daten enthalten detaillierte Informationen zu Anfragen, die an den ELB gesendet wurden. Jedes Protokoll enthält Informationen wie die Zeit, zu der die Anforderung einging, die Client-IP-Adresse, Latenzen, Anforderungspfade und Serverantworten.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-MA-4(1)	MA-4(1) Nicht lokale Wartung | Prüfung und Überprüfung	multi-region-cloudtrail-enabled	AWS CloudTrail zeichnet Aktionen und API-Aufrufe der AWS Management Console auf. Sie können feststellen, welche Benutzer und Konten angerufen wurden AWS, von welcher Quell-IP-Adresse aus die Anrufe getätigt wurden und wann die Anrufe erfolgten. CloudTrail übermittelt Protokolldateien aus allen AWS Regionen an Ihren S3-Bucket , wenn MULTI_REGION_CLOUD_TRAIL_ENABLED aktiviert ist. Außerdem wird beim AWS Start einer neuen Region derselbe Trail in der neuen Region erstellt. CloudTrail Dadurch erhalten Sie automatisch Protokolldateien mit API-Aktivitäten für die neue Region.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-MA-4(1)	MA-4(1) Nicht lokale Wartung | Prüfung und Überprüfung	rds-logging-enabled	Um die Protokollierung und Überwachung in Ihrer Umgebung zu erleichtern, stellen Sie sicher, dass die Amazon Relational Database Service (Amazon RDS)-Protokollierung aktiviert ist. Mit der Amazon-RDS-Protokollierung können Sie Ereignisse wie Verbindungen, Verbindungsabbrüche, Abfragen oder abgefragte Tabellen erfassen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-MA-4(1)	MA-4(1) Nicht lokale Wartung | Prüfung und Überprüfung	redshift-cluster-configuration-check	Um Daten im Ruhezustand zu schützen, muss die Verschlüsselung für Ihre Amazon-Redshift-Cluster aktiviert sein. Sie müssen auch sicherstellen, dass die erforderlichen Konfigurationen auf Amazon-Redshift-Clustern bereitgestellt werden. Die Prüfungsprotokollierung muss aktiviert sein, um Informationen zu Verbindungen und Benutzeraktivitäten in der Datenbank bereitzustellen. Diese Regel erfordert, dass ein Wert für clusterDbEncrypted (Config Default: TRUE) und LoggingEnabled (Config Default: TRUE) gesetzt ist. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-MA-4(1)	MA-4(1) Nicht lokale Wartung | Prüfung und Überprüfung	s3- bucket-logging-enabled	Die Amazon Simple Storage Service (Amazon S3)-Serverzugriffs protokollierung bietet eine Methode zur Überwachu ng des Netzwerks im Hinblick auf potenzielle Cybersich erheitsereignisse. Die Ereignisse werden überwacht, indem detaillierte Aufzeichn ungen über die Anfragen erfasst werden, die an einen Amazon-S3-Bucket gestellt wurden. Jeder Zugriffsprotokolle intrag enthält Details zu einer einzelnen Zugriffsanfrage. Zu den Details gehören Auftraggeber, Bucket-Name, Anforderu ngszeit, Anforderu ngsaktion, Antwortst atus und Fehlercode, falls relevant.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-MA-4(1)	MA-4(1) Nicht lokale Wartung | Prüfung und Überprüfung	vpc-flow-logs-enabled	VPC-Flow-Protokolle erfassen detaillierte Informationsdatensätze über den IP-Datenverkehr, der zu und von Netzwerkschnittstellen in Ihrer Amazon Virtual Private Cloud (Amazon VPC) fließt. Standardmäßig enthalten Flow-Protokolldatensätze Werte für die verschiedenen Komponenten des IP-Flows, einschließlich Quelle, Ziel und Protokoll.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-MA-4(1)	MA-4(1) Nicht lokale Wartung | Prüfung und Überprüfung	wafv2-logging-enabled	Um die Protokollierung und Überwachung in Ihrer Umgebung zu erleichtern, aktivieren Sie die AWS WAF (V2) -Protokollierung im regionalen und globalen Web ACLs. AWS Die WAF-Protokollierung bietet detaillierte Informationen über den Datenverkehr, der von Ihrer Web-ACL analysiert wird. In den Protokollen werden die Uhrzeit aufgezeichnet, zu der die AWS WAF die Anfrage von Ihrer AWS Ressource erhalten hat, Informationen zu der Anfrage und eine Aktion für die Regel, der jede Anfrage entsprach.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-MP-2.A	MP-2.A Medienzugriff	dms-replication-not-public	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass auf DMS-Replikationsinstanzen nicht öffentlich zugegriffen werden kann. DMS-Replikations-Instances können vertrauliche Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.
CCCS-fPBMM-MP-2.A	MP-2.A Medienzugriff	ebs-snapshot-public-restorable-überprüfen	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass EBS-Snapshots nicht öffentlich wiederherstellbar sind. EBS-Volume-Snapshots können vertrauliche Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-MP-2.A	MP-2.A Medienzugriff	ec2-imdsv2-check	Stellen Sie sicher, dass die Methode Instance Metadata Service Version 2 (IMDSv2) aktiviert ist, um den Zugriff auf und die Kontrolle der Amazon Elastic Compute Cloud (Amazon EC2) - Instance-Metadaten zu schützen. Die IMDSv2 Methode verwendet sitzungsbasierte Kontrollen. Mit können Kontrollen implementiert werden IMDSv2, um Änderungen an Instanzmetadaten einzuschränken.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-MP-2.A	MP-2.A Medienzugriff	ec-2 instance-no-public-ip	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon Elastic Compute Cloud (Amazon EC2) - Instances nicht öffentlich zugänglic h sind. EC2Amazon -Instances können vertrauliche Informati onen enthalten, und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-MP-2.A	MP-2.A Medienzugriff	ecs-task-definition-user-for-host-mode-check	Wenn für eine Aufgabendefinition erhöhte Berechtigungen gelten, liegt das daran, dass der Kunde diesen Konfigurationen ausdrücklich zugestimmt hat. Diese Kontrolle prüft, ob eine unerwartete Berechtigungseskalation vorliegt, wenn für eine Aufgabendefinition das Host-Netzwerk aktiviert ist, die Kunden aber keine erhöhten Berechtigungen aktiviert haben.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-MP-2.A	MP-2.A Medienzugriff	elasticsearch-in-vpc-only	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass sich Amazon OpenSearch OpenSearch Service (Service) - Domains innerhalb einer Amazon Virtual Private Cloud (Amazon VPC) befinden. Eine OpenSearch Service-Domain innerhalb einer Amazon VPC ermöglicht die sichere Kommunikation zwischen OpenSearch Service und anderen Services innerhalb der Amazon VPC, ohne dass ein Internet-Gateway, ein NAT-Gerät oder eine VPN-Verbindung erforderlich ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-MP-2.A	MP-2.A Medienzugriff	emr-kerberos-enabled	Die Zugriffsberechtigungen und -autorisierungen können verwaltet und nach den Prinzipien der geringsten Berechtigung und Aufgabentrennung integriert werden, indem Kerberos für Amazon-EMR-Cluster aktiviert wird. In Kerberos werden Services und Benutzer, die sich authentifizieren müssen, als Prinzipale bezeichnet. Prinzipale befinden sich in einem Kerberos-Bereich. Innerhalb dieses Bereichs wird ein Kerberos-Server als Key Distribution Center (KDC) bezeichnet. Über diesen Server können sich Prinzipale authentifizieren. Die Authentifizierung im KDC erfolgt durch die Ausstellung von Authentif

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
			izierungstickets. Das KDC unterhält eine Datenbank der Prinzipale in seinem Bereich mit ihren Passwörtern und anderen administrativen Informationen zu jedem Prinzipal.
CCCS-fPBMM-MP-2.A	MP-2.A Medienzugriff	emr-master-no-public-ip	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon EMR-Cluster-Masterknoten nicht öffentlich zugänglich sind. Amazon-EMR-Cluster-Hauptknoten können vertrauliche Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-MP-2.A	MP-2.A Medienzugriff	iam-customer-policy-blocked-kms-Aktionen	AWS Identity and Access Management (IAM) kann Ihnen helfen, die Prinzipien der geringsten Rechte und der Aufgabentrennung in Zugriffsberechtigungen und Autorisierungen zu integrieren und so zu verhindern, dass Richtlinien blockierte Aktionen für alle AWS Schlüssel des Key Management Service enthalten. Wenn Benutzer mehr Rechte haben, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und Aufgabentrennung verstoßen. Mit dieser Regel können Sie den Parameter festlegen. blockedActionsPatterns (Wert „AWS Bewährte grundlegende Sicherheitsmethode

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
			n“: kms: Entschlüs seln, kms:ReEnc ryptFrom). Die tatsächlichen Werte müssen den Richtlini en Ihrer Organisation entsprechen.
CCCS-fPBMM-MP-2.A	MP-2.A Medienzugriff	iam-group-has-users-überprüfen	AWS Identity and Access Managemen t (IAM) kann Ihnen helfen, die Prinzipien der geringsten Rechte und der Aufgabent rennung mit Zugriffsb erechtigungen und Autorisierungen zu integrieren, indem sichergestellt wird, dass IAM-Gruppen mindestens einen Benutzer haben. Die Einteilung von Benutzern in Gruppen auf der Grundlage der ihnen zugewiese nen Berechtigungen oder ihrer Funktion ist eine Möglichkeit, das Prinzip der geringste n Berechtigung zu implementieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-MP-2.A	MP-2.A Medienzugriff	iam-inline-policy-blocked-kms-Aktionen	Stellen Sie sicher, dass ein Benutzer, eine IAM-Rolle oder eine IAM-Gruppe (AWS Identity and Access Management) nicht über eine Inline-Richtlinie verfügt, die blockierte Aktionen für alle AWS Schlüssel des Key Management Service zulässt. AWS empfiehlt, verwaltete Richtlinien anstelle von Inline-Richtlinien zu verwenden. Verwaltete Richtlinien ermöglichen Wiederverwendbarkeit, Versionsverwaltung, Rollback und Delegierung der Berechtigungsverwaltung. Mit dieser Regel können Sie den blockedActionsPatterns Parameter festlegen. (Wert „AWS Bewährte grundlegende Sicherheitsmethoden“: kms:Decrypt, kms:ReEncryptFrom). Die

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
			tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.
CCCS-fPBMM-MP-2.A	MP-2.A Medienzugriff	iam-no-inline-policy-überprüfen	Stellen Sie sicher, dass ein Benutzer, eine IAM-Rolle oder eine IAM-Gruppe (AWS Identity and Access Management) nicht über eine Inline-Richtlinie zur Zugriffskontrolle auf Systeme und Ressourcen verfügt. AWS empfiehlt, verwaltete Richtlinien anstelle von Inline-Richtlinien zu verwenden. Verwaltete Richtlinien ermöglichen Wiederverwendbarkeit, Versionsverwaltung, Rollback und Delegierung der Berechtigungsverwaltung.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-MP-2.A	MP-2.A Medienzugriff	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) kann Ihnen dabei helfen, die Prinzipien der geringsten Rechte und der Aufgabentrennung in Zugriffsberechtigungen und Autorisierungen zu integrieren und so zu verhindern, dass Richtlinien „Effect“: „Allow“ mit „Action“: „*“ anstelle von „Resource“: „*“ enthalten. Wenn Benutzern mehr Rechte eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und der Aufgabentrennung verstoßen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-MP-2.A	MP-2.A Medienzugriff	iam-root-access-key-überprüfen	Der Zugriff auf Systeme und Ressourcen kann gesteuert werden, indem überprüft wird, ob der Root-Benutzer keine Zugriffsschlüssel mit seiner AWS Identity and Access Management (IAM) -Rolle verknüpft hat. Stellen Sie sicher, dass die Root-Zugriffsschlüssel gelöscht werden. Erstellen und verwenden Sie stattdessen rollenbasierte Funktionen, AWS-Konten um das Prinzip der geringsten Funktionalität zu berücksichtigen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-MP-2.A	MP-2.A Medienzugriff	iam-user-group-membership-überprüfen	AWS Identity and Access Management (IAM) kann Ihnen helfen, Zugriffsberechtigungen und Autorisierungen einzuschränken, indem sichergestellt wird, dass Benutzer Mitglieder mindestens einer Gruppe sind. Wenn Benutzern mehr Berechtigungen eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und Aufgabentrennung verstoßen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-MP-2.A	MP-2.A Medienzugriff	iam-user-no-policies-überprüfen	Diese Regel stellt sicher, dass AWS Identity and Access Management (IAM) -Richtlinien nur Gruppen oder Rollen zugewiesen werden, um den Zugriff auf Systeme und Ressourcen zu kontrollieren. Die Zuweisung von Berechtigungen auf Gruppen- oder Rollenebene trägt dazu bei, die Wahrscheinlichkeit zu verringern, dass eine Identität übermäßige Berechtigungen erhält oder beibehält.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-MP-2.A	MP-2.A Medienzugriff	iam-user-unused-credentials-überprüfen	AWS Identity and Access Management (IAM) kann Ihnen bei Zugriffsberechtigungen und Autorisierungen helfen, indem es nach IAM-Passwörtern und Zugriffsschlüsseln sucht, die für einen bestimmten Zeitraum nicht verwendet wurden. Wenn ungenutzte Anmeldeinformationen identifiziert werden, müssen Sie sie deaktivieren und/oder entfernen, da dies gegen das Prinzip der geringsten Berechtigung verstoßen könnte. Für diese Regel müssen Sie einen Wert für das maxCredentialUsage Alter festlegen (Standardkonfiguration: 90). Der tatsächliche Wert muss den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-MP-2.A	MP-2.A Medienzugriff	ec2- instances-in-vpc	Stellen Sie Amazon Elastic Compute Cloud (Amazon EC2) -Instances innerhalb einer Amazon Virtual Private Cloud (Amazon VPC) bereit, um eine sichere Kommunikation zwischen einer Instance und anderen Services innerhalb der Amazon VPC zu ermöglichen, ohne dass ein Internet-Gateway, ein NAT-Gerät oder eine VPN-Verbindung erforderlich ist. Der gesamte Datenverkehr bleibt sicher in der AWS Cloud. Domains, die sich innerhalb einer VPC befinden, verfügen aufgrund ihrer logischen Isolierung im Vergleich zu Domains mit öffentlichen Endpunkten über eine zusätzliche Sicherheitsebene. Weisen Sie EC2

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
			Amazon-Instances einer Amazon VPC zu, um den Zugriff ordnungsgemäß zu verwalten.
CCCS-fPBMM-MP-2.A	MP-2.A Medienzugriff	internet-gateway-authorized-vpc-nur	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Internet-Gateways nur mit autorisierter Amazon Virtual Private Cloud (Amazon VPC) verbunden sind. Internet-Gateways ermöglichen den bidirektionalen Internetzugang zur und von der Amazon VPC, was möglicher weise zu einem unbefugten Zugriff auf Amazon-VPC-Ressourcen führen kann.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-MP-2.A	MP-2.A Medienzugriff	lambda-function-public-access-verboten	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass AWS Lambda-Funktionen nicht öffentlich zugänglich sind. Der öffentliche Zugriff kann möglicherweise die Verfügbarkeit von Ressourcen beeinträchtigen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-MP-2.A	MP-2.A Medienzugriff	lambda-inside-vpc	Stellen Sie AWS Lambda-Funktionen in einer Amazon Virtual Private Cloud (Amazon VPC) bereit, um eine sichere Kommunikation zwischen einer Funktion und anderen Diensten innerhalb der Amazon VPC zu gewährleisten. Bei dieser Konfiguration sind kein Internet-Gateway, kein NAT-Gerät und keine VPN-Verbindung erforderlich. Der gesamte Datenverkehr bleibt sicher in der Cloud. AWS Domains, die sich innerhalb einer VPC befinden, verfügen aufgrund ihrer logischen Isolierung im Vergleich zu Domains mit öffentlichen Endpunkten über eine zusätzliche Sicherheitsebene. Um den Zugriff ordnungsgemäß zu verwalten,

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
			sollten AWS Lambda-Funktionen einer VPC zugewiesen werden.
CCCS-fPBMM-MP-2.A	MP-2.A Medienzugriff	opensearch-in-vpc-only	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass sich Amazon OpenSearch Service-Domains innerhalb einer Amazon Virtual Private Cloud (Amazon VPC) befinden. Eine Amazon OpenSearch Service-Domain innerhalb einer Amazon VPC ermöglicht die sichere Kommunikation zwischen Amazon OpenSearch Service und anderen Services innerhalb der Amazon VPC, ohne dass ein Internet-Gateway, ein NAT-Gerät oder eine VPN-Verbindung erforderlich ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-MP-2.A	MP-2.A Medienzugriff	rds-instance-public-access-überprüfen	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Relational Database Service (Amazon RDS) -Instances nicht öffentlich sind. Amazon-RDS-Datenbank-Instances können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-MP-2.A	MP-2.A Medienzugriff	rds-snapshots-public-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Relational Database Service (Amazon RDS) -Instances nicht öffentlich sind. Amazon-RDS-Datenbank-Instances können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-MP-2.A	MP-2.A Medienzugriff	redshift-cluster-public-access-überprüfen	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Redshift Redshift-Cluster nicht öffentlich sind. Amazon-Redshift-Cluster können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-MP-2.A	MP-2.A Medienzugriff	s3- -Block-periodisch account-level-public-access	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Simple Storage Service (Amazon S3) -Buckets nicht öffentlich zugänglich sind. Diese Regel trägt dazu bei, sensible Daten vor unbefugten Remote-Benutzern zu schützen, indem sie den öffentlichen Zugriff verhindert. Mit dieser Regel können Sie optional die Parameter ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) und restrictPublicBuckets Parameter (Config Default: True) festlegen. Die tatsächlichen Werte müssen den Richtlini

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
			en Ihrer Organisation entsprechen.
CCCS-fPBMM-MP-2.A	MP-2.A Medienzugriff	s3 bucket-level-public-access - verboten	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Simple Storage Service (Amazon S3) -Buckets nicht öffentlich zugänglich sind. Diese Regel trägt dazu bei, sensible Daten vor unbefugten Remote-Benutzern zu schützen, indem sie den öffentlichen Zugriff auf Bucket-Ebene verhindert.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-MP-2.A	MP-2.A Medienzugriff	s-3 bucket-public-read-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie nur autorisierten Benutzern, Prozessen und Geräten Zugriff auf Amazon Simple Storage Service (Amazon S3) - Buckets gewähren. Die Verwaltung des Zugriffs sollte mit der Klassifizierung der Daten übereinst immen.
CCCS-fPBMM-MP-2.A	MP-2.A Medienzugriff	s3- bucket-public-write-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie nur autorisierten Benutzern, Prozessen und Geräten Zugriff auf Amazon Simple Storage Service (Amazon S3) - Buckets gewähren. Die Verwaltung des Zugriffs sollte mit der Klassifizierung der Daten übereinst immen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-MP-2.A	MP-2.A Medienzugriff	sagemaker-notebook-no-direct-Internetzugang	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass SageMaker Amazon-Notebooks keinen direkten Internetzugang zulassen. Indem Sie direkten Internetzugang blockieren, vermeiden Sie, dass unbefugte Benutzer auf sensible Daten zugreifen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-MP-2.A	MP-2.A Medienzugriff	subnet-auto-assign-public-ip-deaktiviert	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon Virtual Private Cloud (VPC) -Subnetzen nicht automatisch eine öffentliche IP-Adresse zugewiesen wird. Amazon Elastic Compute Cloud (EC2) -Instances, die in Subnetzen gestartet werden, in denen dieses Attribut aktiviert ist, haben ihrer primären Netzwerkschnittstelle eine öffentliche IP-Adresse zugewiesen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-RA-5.A	RA-5.A Schwachst ellenscans	guardduty-enabled-centralized	Amazon GuardDuty kann mithilfe von Threat Intellige nce Feeds helfen, potenzielle Cybersich erheitsereignisse zu überwachen und zu erkennen. Dazu gehören Listen mit bösartigen IPs und maschinel len Lernmethoden zur Identifizierung unerwarteter, nicht autorisierter und bösartiger Aktivitäten in Ihrer AWS Cloud-Umgebung.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-RA-5.B	RA-5.B Schwachst ellenscans	guardduty-enabled-centralized	Amazon GuardDuty kann mithilfe von Threat Intellige nce Feeds helfen, potenzielle Cybersich erheitsereignisse zu überwachen und zu erkennen. Dazu gehören Listen mit bösartigen IPs und maschinel len Lernmethoden zur Identifizierung unerwarteter, nicht autorisierter und bösartiger Aktivitäten in Ihrer AWS Cloud-Umgebung.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-RA-5.C	RA-5.C Schwachstellenscans	guardduty-enabled-centralized	Amazon GuardDuty kann mithilfe von Threat Intelligence Feeds helfen, potenzielle Cybersicherheitsereignisse zu überwachen und zu erkennen. Dazu gehören Listen mit bösartigen IPs und maschinellen Lernmethoden zur Identifizierung unerwarteter, nicht autorisierter und bösartiger Aktivitäten in Ihrer AWS Cloud-Umgebung.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-RA-5.D	RA-5.D Schwachst ellenscans	guardduty-enabled-centralized	Amazon GuardDuty kann mithilfe von Threat Intellige nce Feeds helfen, potenzielle Cybersich erheitsereignisse zu überwachen und zu erkennen. Dazu gehören Listen mit bösartigen IPs und maschinel len Lernmethoden zur Identifizierung unerwarteter, nicht autorisierter und bösartiger Aktivitäten in Ihrer AWS Cloud-Umgebung.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-RA-5.E	RA-5.E Schwachst ellenscans	guardduty-enabled-centralized	Amazon GuardDuty kann mithilfe von Threat Intellige nce Feeds helfen, potenzielle Cybersich erheitsereignisse zu überwachen und zu erkennen. Dazu gehören Listen mit bösartigen IPs und maschinel len Lernmethoden zur Identifizierung unerwarteter, nicht autorisierter und bösartiger Aktivitäten in Ihrer AWS Cloud-Umgebung.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-SA-10(1)	SA-10(1) Konfigurationsmanagement für Entwickler | Überprüfung der Software-/Firmware-Integrität	cloud-trail-log-file-Validierung aktiviert	Verwenden Sie die AWS CloudTrail Protokolldateivalidierung, um die Integrität von Protokollen zu überprüfen. CloudTrail Mithilfe der Protokolldateivalidierung kann festgestellt werden, ob eine Protokolldatei geändert oder gelöscht wurde oder ob sie nach der Übermittlung CloudTrail unverändert geblieben ist. Dieses Feature wurde mit dem Branchenstandard entsprechenden Algorithmen entwickelt: SHA-256 für die Hashfunktion und SHA-256 mit RSA für digitale Signaturen. Aus diesem Grund ist es rechnerisch unmöglich, CloudTrail Protokolldateien unbemerkt zu ändern, zu löschen oder zu fälschen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-SC-5.A	SC-5.A Denial-of-Service-Schutz	alb-waf-enabled	Stellen Sie sicher, dass AWS WAF auf Elastic Load Balancers (ELB) aktiviert ist, um Webanwendungen zu schützen. Eine WAF trägt zum Schutz Ihrer Webanwend ungen oder APIs vor gängigen Web-Explo its bei. Diese Web-Exploits können sich auf die Verfügbar keit auswirken, die Sicherheit gefährden oder übermäßige Ressourcen in Ihrer Umgebung verbrauch en.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-SC-5.A	SC-5.A Denial-of-Service-Schutz	guardduty-enabled-centralized	Amazon GuardDuty kann mithilfe von Threat Intellige nce Feeds helfen, potenzielle Cybersich erheitsereignisse zu überwachen und zu erkennen. Dazu gehören Listen mit bösartigen IPs und maschinel len Lernmethoden zur Identifizierung unerwarteter, nicht autorisierter und bösartiger Aktivitäten in Ihrer AWS Cloud-Umgebung.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-SC-6.A	SC-6.A Ressource nverfügbarkeit	autoscaling-group-elb-healthcheck-erforderlich	Die Elastic Load Balancer (ELB) - Zustandsprüfungen für Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling Scaling-Gruppen unterstützen die Aufrechterhaltung einer angemessenen Kapazität und Verfügbarkeit. Der Load Balancer sendet regelmäßig Pings, versucht Verbindungen herzustellen oder sendet Anfragen, um den Zustand der EC2 Amazon-Instances in einer Gruppe mit auto-scaling zu testen. Wenn eine Instance nicht zurückmeldet, wird der Traffic an eine neue EC2 Amazon-Instance gesendet.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-SC-6.A	SC-6.A Ressource nverfügbarkeit	beanstalk-enhanced-health-reporting-aktiviert	AWS Die verbesserte Zustandsberichterstattung von Elastic Beanstalk ermöglicht eine schnellere Reaktion auf Veränderungen im Zustand der zugrunde liegenden Infrastruktur. Diese Änderungen könnten zu einer mangelnden Verfügbarkeit der Anwendung führen. Die erweiterten Zustandsberichte von Elastic Beanstalk bieten eine Statusbeschreibung, um den Schweregrad der identifizierten Probleme einzuschätzen und mögliche Ursachen zu identifizieren, die untersucht werden müssen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-SC-6.A	SC-6.A Ressource nverfügbarkeit	dynamodb-autoscaling-enabled	Amazon DynamoDB Auto Scaling verwendet den AWS Application Auto Scaling-Service, um die bereitgestellte Durchsatzkapazität so anzupassen, dass sie automatisch auf tatsächliche Verkehrsmuster reagiert. Auf diese Weise kann eine Tabelle oder ein globaler sekundärer Index die bereitgestellte Lese-/Schreibkapazität erhöhen, um plötzliche Erhöhungen des Datenverkehrs ohne Drosselung zu bewältigen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-SC-6.A	SC-6.A Ressource nverfügbarkeit	dynamodb-throughput-limit-check	Aktivieren Sie diese Regel, um sicherzustellen, dass die bereitgestellte Durchsatzkapazität in Ihren Amazon-DynamoDB-Tabellen überprüft wird. Dies ist der Umfang der Lese- und Schreibaktivitäten, der von den jeweiligen Tabellen unterstützt werden kann. DynamoDB verwendet diese Informationen für das Reservieren ausreichender Systemressourcen, um Ihren Durchsatz anforderungen gerecht zu werden. Diese Regel generiert eine Warnung, wenn sich der Durchsatz dem Höchstlimit für ein Kundenkonto nähert. Mit dieser Regel können Sie optional die Parameter RCUThreshold Kontoprozentsatz

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
			(Konfigurationsstandard: 80) und WCUThreshold Kontoprozentsatz (Konfigurationsstandard: 80) festlegen. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-SC-6.A	SC-6.A Ressource nverfügbarkeit	elb-cross-zone-load-Balancing aktiviert	Aktivieren Sie zonenübergreifende s Load Balancing für Ihre Elastic Load Balancer (ELBs), um eine angemesse ne Kapazität und Verfügbarkeit aufrechtzuerhalten. Zonenübergreifende s Load Balancing reduziert die Notwendigkeit, die gleiche Anzahl von Instances in jeder aktivierten Availability Zone aufrechtzuerhalten . Dadurch wird auch die Fähigkeit Ihrer Anwendung verbessert, den Verlust einer oder mehrerer Instances zu bewältigen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-SC-6.A	SC-6.A Ressource nverfügbarkeit	rds-cluster-multi-az-aktiviert	Für Cluster von Amazon Relationa l Database Service (Amazon RDS) sollte die Multi-AZ-Replikati on aktiviert sein, um die Verfügbarkeit der gespeicherten Daten zu gewährleisten. Availability Zones werden auf einer physisch getrennte n, unabhängi gen Infrastruktur ausgeführt und sind auf höchste Zuverläss igkeit ausgelegt . Im Falle eines Infrastrukturausfa lls führt Amazon RDS einen automatis chen Failover zum Standby-Modus durch, sodass Sie den Datenbankbetrieb wieder aufnehmen können, sobald der Failover abgeschlo ssen ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-SC-6.A	SC-6.A Ressource nverfügbarkeit	rds-multi-az-support	Die Multi-AZ-Unterstützung in Amazon Relational Database Service (Amazon RDS) bietet eine verbesserte Verfügbarkeit und Beständigkeit von Datenbank-Instances. Wenn Sie eine Multi-AZ-Datenbank-Instance bereitstellen, erstellt Amazon RDS automatisch eine primäre Datenbank-Instance und repliziert die Daten synchron auf eine Standby-Instance in einer anderen Availability Zone. Jede Availability Zone läuft auf einer eigenen, physisch getrennten, unabhängigen Infrastruktur und ist auf eine hohe Verfügbarkeit ausgelegt. Im Falle eines Infrastrukturausfalls führt Amazon RDS einen automatis

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
			chen Failover zum Standby-Modus durch, sodass Sie den Datenbankbetrieb wieder aufnehmen können, sobald der Failover abgeschlo ssen ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-SC-6.A	SC-6.A Ressource nverfügbarkeit	vpc-vpn-2-tunnels-up	Redundante Site-to-Site VPN-Tunnel können implementiert werden, um die Anforderungen an die Ausfallsicherheit zu erfüllen. Es verwendet zwei Tunnel, um die Konnektivität sicherzustellen, falls eine der Site-to-Site VPN-Verbindungen nicht verfügbar ist. Um sich vor einem Verbindungsverlust zu schützen, können Sie für den Fall, dass Ihr Kunden-Gateway nicht verfügbar ist, eine zweite Site-to-Site VPN-Verbindung zu Ihrer Amazon Virtual Private Cloud (Amazon VPC) und Ihrem Virtual Private Gateway einrichten, indem Sie ein zweites Kunden-Gateway verwenden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-SC-7(3)	SC-7(3) Grenzschutz | Zugangspunkte	dms-replication-not-public	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass auf DMS-Replikationsin stanzen nicht öffentlic h zugegriffen werden kann. DMS-Repli kations-Instances können vertrauli che Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.
CCCS-fPBMM-SC-7(3)	SC-7(3) Grenzschutz | Zugangspunkte	ebs-snapshot-public-restorable-überprüfen	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass EBS-Snapshots nicht öffentlich wiederher stellbar sind. EBS-Volume-Snapsho ts können vertrauli che Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-SC-7(3)	SC-7(3) Grenzschutz | Zugangspunkte	ec-2 instance-no-public-ip	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon Elastic Compute Cloud (Amazon EC2) - Instances nicht öffentlich zugänglic h sind. EC2Amazon -Instances können vertrauliche Informati onen enthalten, und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-SC-7(3)	SC-7(3) Grenzschutz | Zugangspunkte	elasticsearch-in-vpc-only	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass sich Amazon OpenSearch OpenSearch Service (Service) - Domains innerhalb einer Amazon Virtual Private Cloud (Amazon VPC) befinden. Eine OpenSearch Service-Domain innerhalb einer Amazon VPC ermöglicht die sichere Kommunikation zwischen OpenSearch Service und anderen Services innerhalb der Amazon VPC, ohne dass ein Internet-Gateway, ein NAT-Gerät oder eine VPN-Verbindung erforderlich ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-SC-7(3)	SC-7(3) Grenzschutz | Zugangspunkte	emr-master-no-public-ip	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon EMR-Cluster-Masterknoten nicht öffentlich zugänglich sind. Amazon-EMR-Cluster-Hauptknoten können vertrauliche Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-SC-7(3)	SC-7(3) Grenzschutz | Zugangspunkte	ec-2 instances-in-vpc	Stellen Sie Amazon Elastic Compute Cloud (Amazon EC2) -Instances innerhalb einer Amazon Virtual Private Cloud (Amazon VPC) bereit, um eine sichere Kommunika tion zwischen einer Instance und anderen Services innerhalb der Amazon VPC zu ermöglichen, ohne dass ein Internet-Gateway, ein NAT-Gerät oder eine VPN-Verbindung erforderlich ist. Der gesamte Datenverk ehr bleibt sicher in der AWS Cloud. Domains, die sich innerhalb einer VPC befinden, verfügen aufgrund ihrer logischen Isolierun g im Vergleich zu Domains mit öffentlic hen Endpunkten über eine zusätzlic he Sicherheitsebene. Weisen Sie EC2

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
			Amazon-Instances einer Amazon VPC zu, um den Zugriff ordnungsgemäß zu verwalten.
CCCS-fPBMM-SC-7(3)	SC-7(3) Grenzschutz | Zugangspunkte	internet-gateway-authorized-vpc-nur	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Internet-Gateways nur mit autorisierter Amazon Virtual Private Cloud (Amazon VPC) verbunden sind. Internet-Gateways ermöglichen den bidirektionalen Internetzugang zur und von der Amazon VPC, was möglicher weise zu einem unbefugten Zugriff auf Amazon-VPC-Ressourcen führen kann.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-SC-7(3)	SC-7(3) Grenzschutz | Zugangspunkte	lambda-function-public-access-verboten	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass AWS Lambda-Funktionen nicht öffentlich zugänglich sind. Der öffentliche Zugriff kann möglicherweise die Verfügbarkeit von Ressourcen beeinträchtigen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-SC-7(3)	SC-7(3) Grenzschutz | Zugangspunkte	lambda-inside-vpc	Stellen Sie AWS Lambda-Funktionen in einer Amazon Virtual Private Cloud (Amazon VPC) bereit, um eine sichere Kommunika tion zwischen einer Funktion und anderen Diensten innerhalb der Amazon VPC zu gewährleisten. Bei dieser Konfiguration sind kein Internet-Gateway, kein NAT-Gerät und keine VPN-Verbindung erforderlich. Der gesamte Datenverk ehr bleibt sicher in der Cloud. AWS Domains, die sich innerhalb einer VPC befinden, verfügen aufgrund ihrer logischen Isolierun g im Vergleich zu Domains mit öffentlic hen Endpunkten über eine zusätzliche Sicherheitsebene. Um den Zugriff ordnungsg emäß zu verwalten,

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
			sollten AWS Lambda-Funktionen einer VPC zugewiesen werden.
CCCS-fPBMM-SC-7(3)	SC-7(3) Grenzschutz | Zugangspunkte	opensearch-in-vpc-only	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass sich Amazon OpenSearch Service-Domains innerhalb einer Amazon Virtual Private Cloud (Amazon VPC) befinden. Eine Amazon OpenSearch Service-Domain innerhalb einer Amazon VPC ermöglicht die sichere Kommunikation zwischen Amazon OpenSearch Service und anderen Services innerhalb der Amazon VPC, ohne dass ein Internet-Gateway, ein NAT-Gerät oder eine VPN-Verbindung erforderlich ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-SC-7(3)	SC-7(3) Grenzschutz | Zugangspunkte	rds-instance-public-access-überprüfen	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Relational Database Service (Amazon RDS) -Instances nicht öffentlich sind. Amazon-RDS-Datenbank-Instances können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-SC-7(3)	SC-7(3) Grenzschutz | Zugangspunkte	rds-snapshots-public-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Relational Database Service (Amazon RDS) -Instances nicht öffentlich sind. Amazon-RDS-Datenbank-Instances können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-SC-7(3)	SC-7(3) Grenzschutz | Zugangspunkte	redshift-cluster-public-access-überprüfen	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Redshift Redshift-Cluster nicht öffentlich sind. Amazon-Redshift-Cluster können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-SC-7(3)	SC-7(3) Grenzschutz | Zugangspunkte	s3- -Block-periodisch account-level-public-access	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Simple Storage Service (Amazon S3) -Buckets nicht öffentlich zugänglich sind. Diese Regel trägt dazu bei, sensible Daten vor unbefugten Remote-Benutzern zu schützen, indem sie den öffentlichen Zugriff verhindert. Mit dieser Regel können Sie optional die Parameter ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) und restrictPublicBuckets Parameter (Config Default: True) festlegen. Die tatsächlichen Werte müssen den Richtlini

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
			en Ihrer Organisation entsprechen.
CCCS-fPBMM-SC-7(3)	SC-7(3) Grenzschutz | Zugangspunkte	s3 bucket-level-public-access - verboten	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Simple Storage Service (Amazon S3) -Buckets nicht öffentlich zugänglich sind. Diese Regel trägt dazu bei, sensible Daten vor unbefugten Remote-Benutzern zu schützen, indem sie den öffentlichen Zugriff auf Bucket-Ebene verhindert.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-SC-7(3)	SC-7(3) Grenzschutz | Zugangspunkte	s-3 bucket-public-read-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie nur autorisierten Benutzern, Prozessen und Geräten Zugriff auf Amazon Simple Storage Service (Amazon S3) - Buckets gewähren. Die Verwaltung des Zugriffs sollte mit der Klassifizierung der Daten übereinst immen.
CCCS-fPBMM-SC-7(3)	SC-7(3) Grenzschutz | Zugangspunkte	s3- bucket-public-write-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie nur autorisierten Benutzern, Prozessen und Geräten Zugriff auf Amazon Simple Storage Service (Amazon S3) - Buckets gewähren. Die Verwaltung des Zugriffs sollte mit der Klassifizierung der Daten übereinst immen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-SC-7(3)	SC-7(3) Grenzschutz | Zugangspunkte	sagemaker-notebook-no-direct-Internetzugang	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass SageMaker Amazon-Notebooks keinen direkten Internetzugang zulassen. Indem Sie direkten Internetzugang blockieren, vermeiden Sie, dass unbefugte Benutzer auf sensible Daten zugreifen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-SC-7(3)	SC-7(3) Grenzschutz | Zugangspunkte	subnet-auto-assign-public-ip-deaktiviert	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon Virtual Private Cloud (VPC) -Subnetzen nicht automatisch eine öffentliche IP-Adresse zugewiesen wird. Amazon Elastic Compute Cloud (EC2) -Instances, die in Subnetzen gestartet werden, in denen dieses Attribut aktiviert ist, haben ihrer primären Netzwerkschnittstelle eine öffentliche IP-Adresse zugewiesen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-SC-7(4)	SC-7(4) Grenzschutz | Externe Telekommunikationsservices	alb-http-to-https-Umleitungsprüfung	Um Daten während der Übertragung zu schützen, stellen Sie sicher, dass Ihr Application Load Balancer unverschlüsselte HTTP-Anfragen automatisch an HTTPS umleitet. Da sensible Daten vorhanden sein können, sollten Sie die Verschlüsselung bei der Übertragung aktivieren, um diese Daten zu schützen.
CCCS-fPBMM-SC-7(4)	SC-7(4) Grenzschutz | Externe Telekommunikationsservices	api-gw-ssl-enabled	Stellen Sie sicher, dass die REST-API-Stufen von Amazon API Gateway mit SSL-Zertifikaten konfiguriert sind, damit Backend-Systeme überprüfen können, ob Anforderungen von API Gateway stammen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-SC-7(4)	SC-7(4) Grenzschutz | Externe Telekommunikationsservices	dms-replication-not-public	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass auf DMS-Replikationsinstanzen nicht öffentlich zugegriffen werden kann. DMS-Replikations-Instances können vertrauliche Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.
CCCS-fPBMM-SC-7(4)	SC-7(4) Grenzschutz | Externe Telekommunikationsservices	ebs-snapshot-public-restorable-überprüfen	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass EBS-Snapshots nicht öffentlich wiederherstellbar sind. EBS-Volume-Snapshots können vertrauliche Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-SC-7(4)	SC-7(4) Grenzschutz | Externe Telekommunikationsservices	ec-2 instance-no-public-ip	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon Elastic Compute Cloud (Amazon EC2) - Instances nicht öffentlich zugänglich sind. EC2Amazon -Instances können vertrauliche Informationen enthalten, und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-SC-7(4)	SC-7(4) Grenzschutz | Externe Telekommunikationsservices	elasticsearch-in-vpc-only	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass sich Amazon OpenSearch OpenSearch Service (Service) - Domains innerhalb einer Amazon Virtual Private Cloud (Amazon VPC) befinden. Eine OpenSearch Service-Domain innerhalb einer Amazon VPC ermöglicht die sichere Kommunikation zwischen OpenSearch Service und anderen Services innerhalb der Amazon VPC, ohne dass ein Internet-Gateway, ein NAT-Gerät oder eine VPN-Verbindung erforderlich ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-SC-7(4)	SC-7(4) Grenzschutz | Externe Telekommunikationsservices	elasticsearch-node-to-node-Verschlüsselungsprüfung	Stellen Sie sicher, dass die node-to-node Verschlüsselung für Amazon OpenSearch Service aktiviert ist. Node-to-nodeVerschlüsselung ermöglicht die TLS 1.2-Verschlüsselung für die gesamte Kommunikation innerhalb der Amazon Virtual Private Cloud (Amazon VPC). Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-SC-7(4)	SC-7(4) Grenzschutz | Externe Telekommunikationsservices	elb-acm-certificate-required	Zum Schutz von eventuell vorhanden en sensiblen Daten sowie von Daten während der Übertragung muss die Verschlüsselung für Ihr Elastic Load Balancing aktiviert sein. Verwenden Sie AWS Certificate Manager, um öffentlic he und private SSL/ TLS-Zertifikate mit AWS Diensten und internen Ressource n zu verwalten, bereitzustellen und bereitzustellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-SC-7(4)	SC-7(4) Grenzschutz | Externe Telekommunikationsservices	elb-predefined-security-policy-ssl-check	Stellen Sie sicher, dass Ihre SSL-Listener von Classic Elastic Load Balancing eine vordefinierte Sicherheitsrichtlinie verwenden, um Daten während der Übertragung zu schützen. Elastic Load Balancing bietet vordefinierte Aushandlungskonfigurationen, die für die SSL-Aushandlung verwendet werden, wenn eine Verbindung zwischen einem Client und Ihrem Load Balancer hergestellt wurde. Die SSL-Aushandlungskonfigurationen sind mit einer breiten Palette von Clients kompatibel und verwenden hochfeste kryptografische Algorithmen. Diese Regel verlangt, dass Sie eine vordefinierte Sicherheitsrichtlinie für Ihre SSL-Liste

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
			ner festlegen. Die Standard-Sicherheitsrichtlinie lautet: Policy-TLS-1-2-2017-0. ELBSecurity Der tatsächliche Wert muss den Richtlinien Ihrer Organisation entsprechen.
CCCS-fPBMM-SC-7(4)	SC-7(4) Grenzschutz | Externe Telekommunikationsservices	elb-tls-https-listeners-nur	Stellen Sie sicher, dass Ihre Elastic Load Balancer (ELBs) mit SSL- oder HTTPS-Listenern konfiguriert sind. Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-SC-7(4)	SC-7(4) Grenzschutz | Externe Telekommunikationsservices	emr-master-no-public-ip	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon EMR-Cluster-Masterknoten nicht öffentlich zugänglich sind. Amazon-EMR-Cluster-Hauptknoten können vertrauliche Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-SC-7(4)	SC-7(4) Grenzschutz | Externe Telekommunikationsservices	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) Security Groups können bei der Verwaltung des Netzwerkzugriffs helfen, indem sie eine statusbehaftete Filterung des ein- und ausgehenden Netzwerkverkehrs zu Ressourcen bereitstellen. AWS Wenn Sie eingehenden (oder entfernten) Datenverkehr von 0.0.0.0/0 bis Port 22 auf Ihren Ressourcen nicht zulassen, können Sie den Remote-Zugriff einschränken.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-SC-7(4)	SC-7(4) Grenzschutz | Externe Telekommunikationsservices	ec-2 instances-in-vpc	Stellen Sie Amazon Elastic Compute Cloud (Amazon EC2) -Instances innerhalb einer Amazon Virtual Private Cloud (Amazon VPC) bereit, um eine sichere Kommunikation zwischen einer Instance und anderen Services innerhalb der Amazon VPC zu ermöglichen, ohne dass ein Internet-Gateway, ein NAT-Gerät oder eine VPN-Verbindung erforderlich ist. Der gesamte Datenverkehr bleibt sicher in der AWS Cloud. Domains, die sich innerhalb einer VPC befinden, verfügen aufgrund ihrer logischen Isolierung im Vergleich zu Domains mit öffentlichen Endpunkten über eine zusätzliche Sicherheitsebene. Weisen Sie EC2

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
			Amazon-Instances einer Amazon VPC zu, um den Zugriff ordnungsgemäß zu verwalten.
CCCS-fPBMM-SC-7(4)	SC-7(4) Grenzschutz | Externe Telekommunikationsservices	internet-gateway-authorized-vpc-nur	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Internet-Gateways nur mit autorisierter Amazon Virtual Private Cloud (Amazon VPC) verbunden sind. Internet-Gateways ermöglichen den bidirektionalen Internetzugang zur und von der Amazon VPC, was möglicherweise zu einem unbefugten Zugriff auf Amazon-VPC-Ressourcen führen kann.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-SC-7(4)	SC-7(4) Grenzschutz | Externe Telekommunikationsservices	lambda-function-public-access-verboten	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass AWS Lambda-Funktionen nicht öffentlich zugänglich sind. Der öffentliche Zugriff kann möglicherweise die Verfügbarkeit von Ressourcen beeinträchtigen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-SC-7(4)	SC-7(4) Grenzschutz | Externe Telekommunikationsservices	lambda-inside-vpc	Stellen Sie AWS Lambda-Funktionen in einer Amazon Virtual Private Cloud (Amazon VPC) bereit, um eine sichere Kommunikation zwischen einer Funktion und anderen Diensten innerhalb der Amazon VPC zu gewährleisten. Bei dieser Konfiguration sind kein Internet-Gateway, kein NAT-Gerät und keine VPN-Verbindung erforderlich. Der gesamte Datenverkehr bleibt sicher in der Cloud. AWS Domains, die sich innerhalb einer VPC befinden, verfügen aufgrund ihrer logischen Isolierung im Vergleich zu Domains mit öffentlichen Endpunkten über eine zusätzliche Sicherheitsebene. Um den Zugriff ordnungsgemäß zu verwalten,

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
			sollten AWS Lambda-Funktionen einer VPC zugewiesen werden.
CCCS-fPBMM-SC-7(4)	SC-7(4) Grenzschutz | Externe Telekommunikationsservices	opensearch-in-vpc-only	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass sich Amazon OpenSearch Service-Domains innerhalb einer Amazon Virtual Private Cloud (Amazon VPC) befinden. Eine Amazon OpenSearch Service-Domain innerhalb einer Amazon VPC ermöglicht die sichere Kommunikation zwischen Amazon OpenSearch Service und anderen Services innerhalb der Amazon VPC, ohne dass ein Internet-Gateway, ein NAT-Gerät oder eine VPN-Verbindung erforderlich ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-SC-7(4)	SC-7(4) Grenzschutz | Externe Telekommunikationsservices	rds-instance-public-access-überprüfen	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Relational Database Service (Amazon RDS) -Instances nicht öffentlich sind. Amazon-RDS-Datenbank-Instances können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-SC-7(4)	SC-7(4) Grenzschutz | Externe Telekommunikationsservices	rds-snapshots-public-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Relational Database Service (Amazon RDS) -Instances nicht öffentlich sind. Amazon-RDS-Datenbank-Instances können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-SC-7(4)	SC-7(4) Grenzschutz | Externe Telekommunikationsservices	redshift-cluster-public-access-überprüfen	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Redshift Redshift-Cluster nicht öffentlich sind. Amazon-Redshift-Cluster können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.
CCCS-fPBMM-SC-7(4)	SC-7(4) Grenzschutz | Externe Telekommunikationsservices	redshift-require-tls-ssl	Stellen Sie sicher, dass Ihre Amazon-Redshift-Cluster eine TLS/SSL-Verschlüsselung erfordern, um eine Verbindung zu SQL-Clients herzustellen. Da sensible Daten vorhanden sein können, sollten Sie die Verschlüsselung bei der Übertragung aktivieren, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-SC-7(4)	SC-7(4) Grenzschutz | Externe Telekommunikationsservices	restricted-common-ports	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass gemeinsame Ports für Amazon Elastic Compute Cloud (Amazon EC2) -Sicherheitsgruppen eingeschränkt sind. Wenn der Zugriff auf Ports nicht auf vertrauenswürdige Quellen beschränkt wird, kann dies zu Angriffen auf die Verfügbarkeit, Integrität und Vertraulichkeit von Systemen führen. Mit dieser Regel können Sie optional die Parameter blockedPort1–blockedPort5 festlegen (Standardkonfigurationen: 20, 21, 3389, 3306, 4333). Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-SC-7(4)	SC-7(4) Grenzschutz | Externe Telekommunikationsservices	s3- account-level-public-access -blöcke-periodisch	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Simple Storage Service (Amazon S3) -Buckets nicht öffentlich zugänglich sind. Diese Regel trägt dazu bei, sensible Daten vor unbefugten Remote-Benutzern zu schützen, indem sie den öffentlichen Zugriff verhindert. Mit dieser Regel können Sie optional die Parameter ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) und restrictPublicBuckets Parameter (Config Default: True) festlegen. Die tatsächlichen Werte müssen den Richtlini

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
			en Ihrer Organisation entsprechen.
CCCS-fPBMM-SC-7(4)	SC-7(4) Grenzschutz | Externe Telekommunikationsservices	s3 bucket-level-public-access - verboten	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Simple Storage Service (Amazon S3) -Buckets nicht öffentlich zugänglich sind. Diese Regel trägt dazu bei, sensible Daten vor unbefugten Remote-Benutzern zu schützen, indem sie den öffentlichen Zugriff auf Bucket-Ebene verhindert.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-SC-7(4)	SC-7(4) Grenzschutz | Externe Telekommunikationsservices	s-3 bucket-public-read-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie nur autorisierten Benutzern, Prozessen und Geräten Zugriff auf Amazon Simple Storage Service (Amazon S3) - Buckets gewähren. Die Verwaltung des Zugriffs sollte mit der Klassifizierung der Daten übereinstimmen.
CCCS-fPBMM-SC-7(4)	SC-7(4) Grenzschutz | Externe Telekommunikationsservices	s3- bucket-public-write-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie nur autorisierten Benutzern, Prozessen und Geräten Zugriff auf Amazon Simple Storage Service (Amazon S3) - Buckets gewähren. Die Verwaltung des Zugriffs sollte mit der Klassifizierung der Daten übereinstimmen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-SC-7(4)	SC-7(4) Grenzschutz | Externe Telekommunikationsservices	s3- bucket-ssl-requests-only	Um Daten während der Übertragung zu schützen, stellen Sie sicher, dass Ihre Amazon Simple Storage Service (Amazon S3)-Buckets Anfragen zur Verwendung von Secure Socket Layer (SSL)-Buckets erfordern. Da sensible Daten vorhanden sein können, sollten Sie die Verschlüsselung bei der Übertragung aktivieren, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-SC-7(4)	SC-7(4) Grenzschutz | Externe Telekommunikationsservices	sagemaker-notebook-no-direct-Internetzugang	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass SageMaker Amazon-Notebooks keinen direkten Internetzugang zulassen. Indem Sie direkten Internetzugang blockieren, vermeiden Sie, dass unbefugte Benutzer auf sensible Daten zugreifen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-SC-7(4)	SC-7(4) Grenzschutz | Externe Telekommunikationsservices	subnet-auto-assign-public-ip-deaktiviert	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon Virtual Private Cloud (VPC) -Subnetzen nicht automatisch eine öffentliche IP-Adresse zugewiesen wird. Amazon Elastic Compute Cloud (EC2) -Instances, die in Subnetzen gestartet werden, in denen dieses Attribut aktiviert ist, haben ihrer primären Netzwerkschnittstelle eine öffentliche IP-Adresse zugewiesen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-SC-7(4)	SC-7(4) Grenzschutz | Externe Telekommunikationsservices	vpc-default-security-group-geschlossen	Sicherheitsgruppen von Amazon Elastic Compute Cloud (Amazon EC2) können bei der Verwaltung des Netzwerkzugriffs helfen, indem sie eine statusbehaftete Filterung des ein- und ausgehenden Netzwerkverkehrs zu Ressourcen bereitstellen. AWS Die Beschränkung des gesamten Datenverkehrs auf die Standardsicherheitsgruppe hilft dabei, den Fernzugriff auf Ihre Ressourcen einzuschränken. AWS

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-SC-7(4)	SC-7(4) Grenzschutz | Externe Telekommunikationsservices	vpc-sg-open-only-to-authorized-ports	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass gemeinsame Ports für Amazon Elastic Compute Cloud (Amazon EC2) -Sicherheitsgruppen eingeschränkt sind. Wenn der Zugriff auf Ports nicht auf vertrauenswürdige Quellen beschränkt wird, kann dies zu Angriffen auf die Verfügbarkeit, Integrität und Vertraulichkeit von Systemen führen. Durch die Beschränkung des Zugriffs auf Ressourcen innerhalb einer Sicherheitsgruppe aus dem Internet (0.0.0.0/0) kann der Fernzugriff auf interne Systeme gesteuert werden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-SC-7(5)	SC-7(5) Grenzschutz | Standardmäßige Zugriffsverweigerung/Ausnahmsweise Genehmigung	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) Security Groups können bei der Verwaltung des Netzwerkzugriffs helfen, indem sie eine statusbehaftete Filterung des ein- und ausgehenden Netzwerkverkehrs zu Ressourcen bereitstellen. AWS Wenn Sie eingehenden (oder entfernten) Datenverkehr von 0.0.0.0/0 bis Port 22 auf Ihren Ressourcen nicht zulassen, können Sie den Remote-Zugriff einschränken.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-SC-7(5)	SC-7(5) Grenzschutz | Standardmäßige Zugriffsverweigerung/Ausnahmsweise Genehmigung	restricted-common-ports	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass gemeinsame Ports für Amazon Elastic Compute Cloud (Amazon EC2) -Sicherheitsgruppen eingeschränkt sind. Wenn der Zugriff auf Ports nicht auf vertrauenswürdige Quellen beschränkt wird, kann dies zu Angriffen auf die Verfügbarkeit, Integrität und Vertraulichkeit von Systemen führen. Mit dieser Regel können Sie optional die Parameter blockedPort1–blockedPort5 festlegen (Standardkonfigurationen: 20, 21, 3389, 3306, 4333). Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-SC-7(5)	SC-7(5) Grenzschutz | Standardmäßige Zugriffsverweigerung/Ausnahmsweise Genehmigung	vpc-default-security-group-geschlossen	Sicherheitsgruppen von Amazon Elastic Compute Cloud (Amazon EC2) können bei der Verwaltung des Netzwerkzugriffs helfen, indem sie eine statusbehaftete Filterung des ein- und ausgehenden Netzwerkverkehrs zu Ressourcen bereitstellen. AWS Die Beschränkung des gesamten Datenverkehrs auf die Standardsicherheitsgruppe hilft dabei, den Fernzugriff auf Ihre Ressourcen einzuschränken. AWS

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-SC-7(5)	SC-7(5) Grenzschutz | Standardmäßige Zugriffsverweigerung/Ausnahmsweise Genehmigung	vpc-sg-open-only-to-authorized-ports	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass gemeinsame Ports für Amazon Elastic Compute Cloud (Amazon EC2) -Sicherheitsgruppen eingeschränkt sind. Wenn der Zugriff auf Ports nicht auf vertrauenswürdige Quellen beschränkt wird, kann dies zu Angriffen auf die Verfügbarkeit, Integrität und Vertraulichkeit von Systemen führen. Durch die Beschränkung des Zugriffs auf Ressourcen innerhalb einer Sicherheitsgruppe aus dem Internet (0.0.0.0/0) kann der Fernzugriff auf interne Systeme gesteuert werden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-SC-7(7)	SC-7(7) Grenzschutz | Verhindern von Split-Tunneling für Remote-Geräte	dms-replication-not-public	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass auf DMS-Replikationsinstanzen nicht öffentlich zugegriffen werden kann. DMS-Replikations-Instances können vertrauliche Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.
CCCS-fPBMM-SC-7(7)	SC-7(7) Grenzschutz | Verhindern von Split-Tunneling für Remote-Geräte	ebs-snapshot-public-restorable-überprüfen	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass EBS-Snapshots nicht öffentlich wiederherstellbar sind. EBS-Volume-Snapshots können vertrauliche Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-SC-7(7)	SC-7(7) Grenzschutz | Verhindern von Split-Tunneling für Remote-Geräte	ec-2 instance-no-public-ip	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon Elastic Compute Cloud (Amazon EC2) - Instances nicht öffentlich zugänglich sind. EC2Amazon -Instances können vertrauliche Informationen enthalten, und für solche Konten ist eine Zugriffskontrolle erforderlich.
CCCS-fPBMM-SC-7(7)	SC-7(7) Grenzschutz | Verhindern von Split-Tunneling für Remote-Geräte	emr-master-no-public-ip	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon EMR-Cluster-Masterknoten nicht öffentlich zugänglich sind. Amazon-EMR-Cluster-Hauptknoten können vertrauliche Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-SC-7(7)	SC-7(7) Grenzschutz | Verhindern von Split-Tunneling für Remote-Geräte	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) Security Groups können bei der Verwaltung des Netzwerkzugriffs helfen, indem sie eine statusbehaftete Filterung des ein- und ausgehenden Netzwerkverkehrs zu Ressourcen bereitstellen. AWS Wenn Sie eingehenden (oder entfernten) Datenverkehr von 0.0.0.0/0 bis Port 22 auf Ihren Ressourcen nicht zulassen, können Sie den Remote-Zugriff einschränken.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-SC-7(7)	SC-7(7) Grenzschutz | Verhindern von Split-Tunneling für Remote-Geräte	internet-gateway-authorized-vpc-nur	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Internet-Gateways nur mit autorisierter Amazon Virtual Private Cloud (Amazon VPC) verbunden sind. Internet-Gateways ermöglichen den bidirektionalen Internetzugang zur und von der Amazon VPC, was möglicherweise zu einem unbefugten Zugriff auf Amazon-VPC-Ressourcen führen kann.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-SC-7(7)	SC-7(7) Grenzschutz | Verhindern von Split-Tunneling für Remote-Geräte	lambda-function-public-access-verboten	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass AWS Lambda-Funktionen nicht öffentlich zugänglich sind. Der öffentliche Zugriff kann möglicherweise die Verfügbarkeit von Ressourcen beeinträchtigen.
CCCS-fPBMM-SC-7(7)	SC-7(7) Grenzschutz | Verhindern von Split-Tunneling für Remote-Geräte	rds-instance-public-access-überprüfen	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Relational Database Service (Amazon RDS) -Instances nicht öffentlich sind. Amazon-RDS-Datenbank-Instances können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-SC-7(7)	SC-7(7) Grenzschutz | Verhindern von Split-Tunneling für Remote-Geräte	rds-snapshots-public-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Relational Database Service (Amazon RDS) -Instances nicht öffentlich sind. Amazon-RDS-Datenbank-Instances können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-SC-7(7)	SC-7(7) Grenzschutz | Verhindern von Split-Tunneling für Remote-Geräte	redshift-cluster-public-access-überprüfen	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Redshift Redshift-Cluster nicht öffentlich sind. Amazon-Redshift-Cluster können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-SC-7(7)	SC-7(7) Grenzschutz | Verhindern von Split-Tunneling für Remote-Geräte	restricted-common-ports	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass gemeinsame Ports für Amazon Elastic Compute Cloud (Amazon EC2) -Sicherheitsgruppen eingeschränkt sind. Wenn der Zugriff auf Ports nicht auf vertrauenswürdige Quellen beschränkt wird, kann dies zu Angriffen auf die Verfügbarkeit, Integrität und Vertraulichkeit von Systemen führen. Mit dieser Regel können Sie optional die Parameter blockedPort1–blockedPort5 festlegen (Standardkonfigurationen: 20, 21, 3389, 3306, 4333). Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-SC-7(7)	SC-7(7) Grenzschutz | Verhindern von Split-Tunneling für Remote-Geräte	s3- account-level-public-access -blöcke-periodisch	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Simple Storage Service (Amazon S3) -Buckets nicht öffentlich zugänglich sind. Diese Regel trägt dazu bei, sensible Daten vor unbefugten Remote-Benutzern zu schützen, indem sie den öffentlichen Zugriff verhindert. Mit dieser Regel können Sie optional die Parameter ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) und restrictPublicBuckets Parameter (Config Default: True) festlegen. Die tatsächlichen Werte müssen den Richtlini

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
			en Ihrer Organisation entsprechen.
CCCS-fPBMM-SC-7(7)	SC-7(7) Grenzschutz | Verhindern von Split-Tunneling für Remote-Geräte	s3 bucket-level-public-access - verboten	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Simple Storage Service (Amazon S3) -Buckets nicht öffentlich zugänglich sind. Diese Regel trägt dazu bei, sensible Daten vor unbefugten Remote-Benutzern zu schützen, indem sie den öffentlichen Zugriff auf Bucket-Ebene verhindert.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-SC-7(7)	SC-7(7) Grenzschutz | Verhindern von Split-Tunneling für Remote-Geräte	s-3 bucket-public-read-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie nur autorisierten Benutzern, Prozessen und Geräten Zugriff auf Amazon Simple Storage Service (Amazon S3) - Buckets gewähren. Die Verwaltung des Zugriffs sollte mit der Klassifizierung der Daten übereinst immen.
CCCS-fPBMM-SC-7(7)	SC-7(7) Grenzschutz | Verhindern von Split-Tunneling für Remote-Geräte	s3- bucket-public-write-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie nur autorisierten Benutzern, Prozessen und Geräten Zugriff auf Amazon Simple Storage Service (Amazon S3) - Buckets gewähren. Die Verwaltung des Zugriffs sollte mit der Klassifizierung der Daten übereinst immen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-SC-7(7)	SC-7(7) Grenzschutz | Verhindern von Split-Tunneling für Remote-Geräte	sagemaker-notebook-no-direct-Internetzugang	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass SageMaker Amazon-Notebooks keinen direkten Internetzugang zulassen. Indem Sie direkten Internetzugang blockieren, vermeiden Sie, dass unbefugte Benutzer auf sensible Daten zugreifen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-SC-7(7)	SC-7(7) Grenzschutz | Verhindern von Split-Tunneling für Remote-Geräte	subnet-auto-assign-public-ip-deaktiviert	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon Virtual Private Cloud (VPC) -Subnetzen nicht automatisch eine öffentliche IP-Adresse zugewiesen wird. Amazon Elastic Compute Cloud (EC2) -Instances, die in Subnetzen gestartet werden, in denen dieses Attribut aktiviert ist, haben ihrer primären Netzwerkschnittstelle eine öffentliche IP-Adresse zugewiesen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-SC-7(7)	SC-7(7) Grenzschutz | Verhindern von Split-Tunneling für Remote-Geräte	vpc-default-security-group-geschlossen	Sicherheitsgruppen von Amazon Elastic Compute Cloud (Amazon EC2) können bei der Verwaltung des Netzwerkzugriffs helfen, indem sie eine statusbehaftete Filterung des ein- und ausgehenden Netzwerkverkehrs zu Ressourcen bereitstellen. AWS Die Beschränk ung des gesamten Datenverkehrs auf die Standardsicherheit sgruppe hilft dabei, den Fernzugriff auf Ihre Ressourcen einzuschränken. AWS

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-SC-7.A	SC-7.A Grenzschutz	dms-replication-not-public	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass auf DMS-Replikationsin stanzen nicht öffentlic h zugegriffen werden kann. DMS-Repli kations-Instances können vertrauli che Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.
CCCS-fPBMM-SC-7.A	SC-7.A Grenzschutz	ebs-snapshot-public-restorable-überprüfen	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass EBS-Snapshots nicht öffentlich wiederher stellbar sind. EBS-Volume-Snapsho ts können vertrauli che Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-SC-7.A	SC-7.A Grenzschutz	ec-2 instance-no-public-ip	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon Elastic Compute Cloud (Amazon EC2) - Instances nicht öffentlich zugänglic h sind. EC2Amazon -Instances können vertrauliche Informati onen enthalten, und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-SC-7.A	SC-7.A Grenzschutz	elasticsearch-in-vpc-only	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass sich Amazon OpenSearch OpenSearch Service (Service) - Domains innerhalb einer Amazon Virtual Private Cloud (Amazon VPC) befinden. Eine OpenSearch Service-Domain innerhalb einer Amazon VPC ermöglicht die sichere Kommunikation zwischen OpenSearch Service und anderen Services innerhalb der Amazon VPC, ohne dass ein Internet-Gateway, ein NAT-Gerät oder eine VPN-Verbindung erforderlich ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-SC-7.A	SC-7.A Grenzschutz	emr-master-no-public-ip	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon EMR-Cluster-Masterknoten nicht öffentlich zugänglich sind. Amazon-EMR-Cluster-Hauptknoten können vertrauliche Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-SC-7.A	SC-7.A Grenzschutz	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) Security Groups können bei der Verwaltung des Netzwerkzugriffs helfen, indem sie eine statusbehaftete Filterung des ein- und ausgehenden Netzwerkverkehrs zu Ressourcen bereitstellen. AWS Wenn Sie eingehenden (oder entfernten) Datenverkehr von 0.0.0.0/0 bis Port 22 auf Ihren Ressourcen nicht zulassen, können Sie den Remote-Zugriff einschränken.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-SC-7.A	SC-7.A Grenzschutz	ec2- instances-in-vpc	Stellen Sie Amazon Elastic Compute Cloud (Amazon EC2) -Instances innerhalb einer Amazon Virtual Private Cloud (Amazon VPC) bereit, um eine sichere Kommunika tion zwischen einer Instance und anderen Services innerhalb der Amazon VPC zu ermöglichen, ohne dass ein Internet-Gateway, ein NAT-Gerät oder eine VPN-Verbindung erforderlich ist. Der gesamte Datenverk ehr bleibt sicher in der AWS Cloud. Domains, die sich innerhalb einer VPC befinden, verfügen aufgrund ihrer logischen Isolierun g im Vergleich zu Domains mit öffentlic hen Endpunkten über eine zusätzlic he Sicherheitsebene. Weisen Sie EC2

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
			Amazon-Instances einer Amazon VPC zu, um den Zugriff ordnungsgemäß zu verwalten.
CCCS-fPBMM-SC-7.A	SC-7.A Grenzschutz	internet-gateway-authorized-vpc-nur	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Internet-Gateways nur mit autorisierter Amazon Virtual Private Cloud (Amazon VPC) verbunden sind. Internet-Gateways ermöglichen den bidirektionalen Internetzugang zur und von der Amazon VPC, was möglicher weise zu einem unbefugten Zugriff auf Amazon-VPC-Ressourcen führen kann.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-SC-7.A	SC-7.A Grenzschutz	lambda-function-public-access-verboten	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass AWS Lambda-Funktionen nicht öffentlich zugänglich sind. Der öffentliche Zugriff kann möglicherweise die Verfügbarkeit von Ressourcen beeinträchtigen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-SC-7.A	SC-7.A Grenzschutz	lambda-inside-vpc	Stellen Sie AWS Lambda-Funktionen in einer Amazon Virtual Private Cloud (Amazon VPC) bereit, um eine sichere Kommunika tion zwischen einer Funktion und anderen Diensten innerhalb der Amazon VPC zu gewährleisten. Bei dieser Konfiguration sind kein Internet-Gateway, kein NAT-Gerät und keine VPN-Verbindung erforderlich. Der gesamte Datenverk ehr bleibt sicher in der Cloud. AWS Domains, die sich innerhalb einer VPC befinden, verfügen aufgrund ihrer logischen Isolierun g im Vergleich zu Domains mit öffentlic hen Endpunkten über eine zusätzliche Sicherheitsebene. Um den Zugriff ordnungsg emäß zu verwalten,

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
			sollten AWS Lambda-Funktionen einer VPC zugewiesen werden.
CCCS-fPBMM-SC-7.A	SC-7.A Grenzschutz	opensearch-in-vpc-only	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass sich Amazon OpenSearch Service-Domains innerhalb einer Amazon Virtual Private Cloud (Amazon VPC) befinden. Eine Amazon OpenSearch Service-Domain innerhalb einer Amazon VPC ermöglicht die sichere Kommunikation zwischen Amazon OpenSearch Service und anderen Services innerhalb der Amazon VPC, ohne dass ein Internet-Gateway, ein NAT-Gerät oder eine VPN-Verbindung erforderlich ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-SC-7.A	SC-7.A Grenzschutz	rds-instance-public-access-überprüfen	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Relational Database Service (Amazon RDS) -Instances nicht öffentlich sind. Amazon-RDS-Datenbank-Instances können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-SC-7.A	SC-7.A Grenzschutz	rds-snapshots-public-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Relational Database Service (Amazon RDS) -Instances nicht öffentlich sind. Amazon-RDS-Datenbank-Instances können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-SC-7.A	SC-7.A Grenzschutz	redshift-cluster-public-access-überprüfen	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Redshift Redshift-Cluster nicht öffentlich sind. Amazon-Redshift-Cluster können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-SC-7.A	SC-7.A Grenzschutz	restricted-common-ports	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass gemeinsame Ports für Amazon Elastic Compute Cloud (Amazon EC2) -Sicherheitsgruppen eingeschränkt sind. Wenn der Zugriff auf Ports nicht auf vertrauenswürdige Quellen beschränkt wird, kann dies zu Angriffen auf die Verfügbarkeit, Integrität und Vertraulichkeit von Systemen führen. Mit dieser Regel können Sie optional die Parameter blockedPort1–blockedPort5 festlegen (Standardkonfigurationen: 20, 21, 3389, 3306, 4333). Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-SC-7.A	SC-7.A Grenzschutz	s3- account-level-public-access -blöcke-periodisch	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Simple Storage Service (Amazon S3) -Buckets nicht öffentlich zugänglich sind. Diese Regel trägt dazu bei, sensible Daten vor unbefugten Remote-Benutzern zu schützen, indem sie den öffentlichen Zugriff verhindert. Mit dieser Regel können Sie optional die Parameter ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) und restrictPublicBuckets Parameter (Config Default: True) festlegen. Die tatsächlichen Werte müssen den Richtlini

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
			en Ihrer Organisation entsprechen.
CCCS-fPBMM-SC-7.A	SC-7.A Grenzschutz	s3 bucket-level-public-access - verboten	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Simple Storage Service (Amazon S3) -Buckets nicht öffentlich zugänglich sind. Diese Regel trägt dazu bei, sensible Daten vor unbefugten Remote-Benutzern zu schützen, indem sie den öffentlichen Zugriff auf Bucket-Ebene verhindert.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-SC-7.A	SC-7.A Grenzschutz	s-3 bucket-public-read-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie nur autorisierten Benutzern, Prozessen und Geräten Zugriff auf Amazon Simple Storage Service (Amazon S3) - Buckets gewähren. Die Verwaltung des Zugriffs sollte mit der Klassifizierung der Daten übereinst immen.
CCCS-fPBMM-SC-7.A	SC-7.A Grenzschutz	s3- bucket-public-write-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie nur autorisierten Benutzern, Prozessen und Geräten Zugriff auf Amazon Simple Storage Service (Amazon S3) - Buckets gewähren. Die Verwaltung des Zugriffs sollte mit der Klassifizierung der Daten übereinst immen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-SC-7.A	SC-7.A Grenzschutz	sagemaker-notebook-no-direct-Internetzugang	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass SageMaker Amazon-Notebooks keinen direkten Internetzugang zulassen. Indem Sie direkten Internetzugang blockieren, vermeiden Sie, dass unbefugte Benutzer auf sensible Daten zugreifen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-SC-7.A	SC-7.A Grenzschutz	subnet-auto-assign-public-ip-deaktiviert	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon Virtual Private Cloud (VPC) -Subnetzen nicht automatisch eine öffentliche IP-Adresse zugewiesen wird. Amazon Elastic Compute Cloud (EC2) -Instances, die in Subnetzen gestartet werden, in denen dieses Attribut aktiviert ist, haben ihrer primären Netzwerkschnittstelle eine öffentliche IP-Adresse zugewiesen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-SC-7.A	SC-7.A Grenzschutz	vpc-default-security-group-geschlossen	Sicherheitsgruppen von Amazon Elastic Compute Cloud (Amazon EC2) können bei der Verwaltung des Netzwerkzugriffs helfen, indem sie eine statusbehaftete Filterung des ein- und ausgehenden Netzwerkverkehrs zu Ressourcen bereitstellen. AWS Die Beschränk ung des gesamten Datenverkehrs auf die Standardsicherheit sgruppe hilft dabei, den Fernzugriff auf Ihre Ressourcen einzuschränken. AWS

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-SC-7.A	SC-7.A Grenzschutz	vpc-sg-open-only-to-authorized-ports	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass gemeinsame Ports für Amazon Elastic Compute Cloud (Amazon EC2) -Sicherheitsgruppen eingeschränkt sind. Wenn der Zugriff auf Ports nicht auf vertrauenswürdige Quellen beschränkt wird, kann dies zu Angriffen auf die Verfügbarkeit, Integrität und Vertraulichkeit von Systemen führen. Durch die Beschränkung des Zugriffs auf Ressourcen innerhalb einer Sicherheitsgruppe aus dem Internet (0.0.0.0/0) kann der Fernzugriff auf interne Systeme gesteuert werden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-SC-7.B	SC-7.B Grenzschutz	dms-replication-not-public	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass auf DMS-Replikationsin stanzen nicht öffentlic h zugegriffen werden kann. DMS-Repli kations-Instances können vertrauli che Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.
CCCS-fPBMM-SC-7.B	SC-7.B Grenzschutz	ebs-snapshot-public-restorable-überprüfen	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass EBS-Snapshots nicht öffentlich wiederher stellbar sind. EBS-Volume-Snapsho ts können vertrauli che Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-SC-7.B	SC-7.B Grenzschutz	ec-2 instance-no-public-ip	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon Elastic Compute Cloud (Amazon EC2) - Instances nicht öffentlich zugänglic h sind. EC2Amazon -Instances können vertrauliche Informati onen enthalten, und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-SC-7.B	SC-7.B Grenzschutz	elasticsearch-in-vpc-only	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass sich Amazon OpenSearch OpenSearch Service (Service) - Domains innerhalb einer Amazon Virtual Private Cloud (Amazon VPC) befinden. Eine OpenSearch Service-Domain innerhalb einer Amazon VPC ermöglicht die sichere Kommunikation zwischen OpenSearch Service und anderen Services innerhalb der Amazon VPC, ohne dass ein Internet-Gateway, ein NAT-Gerät oder eine VPN-Verbindung erforderlich ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-SC-7.B	SC-7.B Grenzschutz	emr-master-no-public-ip	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon EMR-Cluster-Masterknoten nicht öffentlich zugänglich sind. Amazon-EMR-Cluster-Hauptknoten können vertrauliche Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-SC-7.B	SC-7.B Grenzschutz	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) Security Groups können bei der Verwaltung des Netzwerkzugriffs helfen, indem sie eine statusbehaftete Filterung des ein- und ausgehenden Netzwerkverkehrs zu Ressourcen bereitstellen. AWS Wenn Sie eingehenden (oder entfernten) Datenverkehr von 0.0.0.0/0 bis Port 22 auf Ihren Ressourcen nicht zulassen, können Sie den Remote-Zugriff einschränken.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-SC-7.B	SC-7.B Grenzschutz	ec2- instances-in-vpc	Stellen Sie Amazon Elastic Compute Cloud (Amazon EC2) -Instances innerhalb einer Amazon Virtual Private Cloud (Amazon VPC) bereit, um eine sichere Kommunika tion zwischen einer Instance und anderen Services innerhalb der Amazon VPC zu ermöglichen, ohne dass ein Internet-Gateway, ein NAT-Gerät oder eine VPN-Verbindung erforderlich ist. Der gesamte Datenverk ehr bleibt sicher in der AWS Cloud. Domains, die sich innerhalb einer VPC befinden, verfügen aufgrund ihrer logischen Isolierun g im Vergleich zu Domains mit öffentlic hen Endpunkten über eine zusätzlic he Sicherheitsebene. Weisen Sie EC2

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
			Amazon-Instances einer Amazon VPC zu, um den Zugriff ordnungsgemäß zu verwalten.
CCCS-fPBMM-SC-7.B	SC-7.B Grenzschutz	internet-gateway-authorized-vpc-nur	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Internet-Gateways nur mit autorisierter Amazon Virtual Private Cloud (Amazon VPC) verbunden sind. Internet-Gateways ermöglichen den bidirektionalen Internetzugang zur und von der Amazon VPC, was möglicher weise zu einem unbefugten Zugriff auf Amazon-VPC-Ressourcen führen kann.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-SC-7.B	SC-7.B Grenzschutz	lambda-function-public-access-verboten	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass AWS Lambda-Funktionen nicht öffentlich zugänglich sind. Der öffentliche Zugriff kann möglicherweise die Verfügbarkeit von Ressourcen beeinträchtigen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-SC-7.B	SC-7.B Grenzschutz	lambda-inside-vpc	Stellen Sie AWS Lambda-Funktionen in einer Amazon Virtual Private Cloud (Amazon VPC) bereit, um eine sichere Kommunika tion zwischen einer Funktion und anderen Diensten innerhalb der Amazon VPC zu gewährleisten. Bei dieser Konfiguration sind kein Internet-Gateway, kein NAT-Gerät und keine VPN-Verbindung erforderlich. Der gesamte Datenverk ehr bleibt sicher in der Cloud. AWS Domains, die sich innerhalb einer VPC befinden, verfügen aufgrund ihrer logischen Isolierun g im Vergleich zu Domains mit öffentlic hen Endpunkten über eine zusätzliche Sicherheitsebene. Um den Zugriff ordnungsg emäß zu verwalten,

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
			sollten AWS Lambda-Funktionen einer VPC zugewiesen werden.
CCCS-fPBMM-SC-7.B	SC-7.B Grenzschutz	opensearch-in-vpc-only	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass sich Amazon OpenSearch Service-Domains innerhalb einer Amazon Virtual Private Cloud (Amazon VPC) befinden. Eine Amazon OpenSearch Service-Domain innerhalb einer Amazon VPC ermöglicht die sichere Kommunikation zwischen Amazon OpenSearch Service und anderen Services innerhalb der Amazon VPC, ohne dass ein Internet-Gateway, ein NAT-Gerät oder eine VPN-Verbindung erforderlich ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-SC-7.B	SC-7.B Grenzschutz	rds-instance-public-access-überprüfen	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Relational Database Service (Amazon RDS) -Instances nicht öffentlich sind. Amazon-RDS-Datenbank-Instances können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-SC-7.B	SC-7.B Grenzschutz	rds-snapshots-public-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Relational Database Service (Amazon RDS) -Instances nicht öffentlich sind. Amazon-RDS-Datenbank-Instances können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-SC-7.B	SC-7.B Grenzschutz	redshift-cluster-public-access-überprüfen	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Redshift Redshift-Cluster nicht öffentlich sind. Amazon-Redshift-Cluster können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-SC-7.B	SC-7.B Grenzschutz	restricted-common-ports	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass gemeinsame Ports für Amazon Elastic Compute Cloud (Amazon EC2) -Sicherheitsgruppen eingeschränkt sind. Wenn der Zugriff auf Ports nicht auf vertrauenswürdige Quellen beschränkt wird, kann dies zu Angriffen auf die Verfügbarkeit, Integrität und Vertraulichkeit von Systemen führen. Mit dieser Regel können Sie optional die Parameter blockedPort1–blockedPort5 festlegen (Standardkonfigurationen: 20, 21, 3389, 3306, 4333). Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-SC-7.B	SC-7.B Grenzschutz	s3- account-level-public-access -blöcke-periodisch	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Simple Storage Service (Amazon S3) -Buckets nicht öffentlich zugänglich sind. Diese Regel trägt dazu bei, sensible Daten vor unbefugten Remote-Benutzern zu schützen, indem sie den öffentlichen Zugriff verhindert. Mit dieser Regel können Sie optional die Parameter ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) und restrictPublicBuckets Parameter (Config Default: True) festlegen. Die tatsächlichen Werte müssen den Richtlini

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
			en Ihrer Organisation entsprechen.
CCCS-fPBMM-SC-7.B	SC-7.B Grenzschutz	s3 bucket-level-public-access - verboten	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Simple Storage Service (Amazon S3) -Buckets nicht öffentlich zugänglich sind. Diese Regel trägt dazu bei, sensible Daten vor unbefugten Remote-Benutzern zu schützen, indem sie den öffentlichen Zugriff auf Bucket-Ebene verhindert.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-SC-7.B	SC-7.B Grenzschutz	s-3 bucket-public-read-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie nur autorisierten Benutzern, Prozessen und Geräten Zugriff auf Amazon Simple Storage Service (Amazon S3) - Buckets gewähren. Die Verwaltung des Zugriffs sollte mit der Klassifizierung der Daten übereinst immen.
CCCS-fPBMM-SC-7.B	SC-7.B Grenzschutz	s3- bucket-public-write-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie nur autorisierten Benutzern, Prozessen und Geräten Zugriff auf Amazon Simple Storage Service (Amazon S3) - Buckets gewähren. Die Verwaltung des Zugriffs sollte mit der Klassifizierung der Daten übereinst immen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-SC-7.B	SC-7.B Grenzschutz	sagemaker-notebook-no-direct-Internetzugang	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass SageMaker Amazon-Notebooks keinen direkten Internetzugang zulassen. Indem Sie direkten Internetzugang blockieren, vermeiden Sie, dass unbefugte Benutzer auf sensible Daten zugreifen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-SC-7.B	SC-7.B Grenzschutz	subnet-auto-assign-public-ip-deaktiviert	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon Virtual Private Cloud (VPC) -Subnetzen nicht automatisch eine öffentliche IP-Adresse zugewiesen wird. Amazon Elastic Compute Cloud (EC2) -Instances, die in Subnetzen gestartet werden, in denen dieses Attribut aktiviert ist, haben ihrer primären Netzwerkschnittstelle eine öffentliche IP-Adresse zugewiesen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-SC-7.B	SC-7.B Grenzschutz	vpc-default-security-group-geschlossen	Sicherheitsgruppen von Amazon Elastic Compute Cloud (Amazon EC2) können bei der Verwaltung des Netzwerkzugriffs helfen, indem sie eine statusbehaftete Filterung des ein- und ausgehenden Netzwerkverkehrs zu Ressourcen bereitstellen. AWS Die Beschränk ung des gesamten Datenverkehrs auf die Standardsicherheit sgruppe hilft dabei, den Fernzugriff auf Ihre Ressourcen einzuschränken. AWS

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-SC-7.B	SC-7.B Grenzschutz	vpc-sg-open-only-to-authorized-ports	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass gemeinsame Ports für Amazon Elastic Compute Cloud (Amazon EC2) -Sicherheitsgruppen eingeschränkt sind. Wenn der Zugriff auf Ports nicht auf vertrauenswürdige Quellen beschränkt wird, kann dies zu Angriffen auf die Verfügbarkeit, Integrität und Vertraulichkeit von Systemen führen. Durch die Beschränkung des Zugriffs auf Ressourcen innerhalb einer Sicherheitsgruppe aus dem Internet (0.0.0.0/0) kann der Fernzugriff auf interne Systeme gesteuert werden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-SC-7.C	SC-7.C Grenzschutz	dms-replication-not-public	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass auf DMS-Replikationsin stanzen nicht öffentlic h zugegriffen werden kann. DMS-Repli kations-Instances können vertrauli che Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.
CCCS-fPBMM-SC-7.C	SC-7.C Grenzschutz	ebs-snapshot-public-restorable-überprüfen	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass EBS-Snapshots nicht öffentlich wiederher stellbar sind. EBS-Volume-Snapsho ts können vertrauli che Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-SC-7.C	SC-7.C Grenzschutz	ec-2 instance-no-public-ip	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon Elastic Compute Cloud (Amazon EC2) - Instances nicht öffentlich zugänglic h sind. EC2Amazon -Instances können vertrauliche Informati onen enthalten, und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-SC-7.C	SC-7.C Grenzschutz	elasticsearch-in-vpc-only	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass sich Amazon OpenSearch OpenSearch Service (Service) - Domains innerhalb einer Amazon Virtual Private Cloud (Amazon VPC) befinden. Eine OpenSearch Service-Domain innerhalb einer Amazon VPC ermöglicht die sichere Kommunikation zwischen OpenSearch Service und anderen Services innerhalb der Amazon VPC, ohne dass ein Internet-Gateway, ein NAT-Gerät oder eine VPN-Verbindung erforderlich ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-SC-7.C	SC-7.C Grenzschutz	emr-master-no-public-ip	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon EMR-Cluster-Masterknoten nicht öffentlich zugänglich sind. Amazon-EMR-Cluster-Hauptknoten können vertrauliche Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-SC-7.C	SC-7.C Grenzschutz	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) Security Groups können bei der Verwaltung des Netzwerkzugriffs helfen, indem sie eine statusbehaftete Filterung des ein- und ausgehenden Netzwerkverkehrs zu Ressourcen bereitstellen. AWS Wenn Sie eingehenden (oder entfernten) Datenverkehr von 0.0.0.0/0 bis Port 22 auf Ihren Ressourcen nicht zulassen, können Sie den Remote-Zugriff einschränken.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-SC-7.C	SC-7.C Grenzschutz	ec2- instances-in-vpc	Stellen Sie Amazon Elastic Compute Cloud (Amazon EC2) -Instances innerhalb einer Amazon Virtual Private Cloud (Amazon VPC) bereit, um eine sichere Kommunika tion zwischen einer Instance und anderen Services innerhalb der Amazon VPC zu ermöglichen, ohne dass ein Internet-Gateway, ein NAT-Gerät oder eine VPN-Verbindung erforderlich ist. Der gesamte Datenverk ehr bleibt sicher in der AWS Cloud. Domains, die sich innerhalb einer VPC befinden, verfügen aufgrund ihrer logischen Isolierun g im Vergleich zu Domains mit öffentlic hen Endpunkten über eine zusätzlic he Sicherheitsebene. Weisen Sie EC2

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
			Amazon-Instances einer Amazon VPC zu, um den Zugriff ordnungsgemäß zu verwalten.
CCCS-fPBMM-SC-7.C	SC-7.C Grenzschutz	internet-gateway-authorized-vpc-nur	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Internet-Gateways nur mit autorisierter Amazon Virtual Private Cloud (Amazon VPC) verbunden sind. Internet-Gateways ermöglichen den bidirektionalen Internetzugang zur und von der Amazon VPC, was möglicher weise zu einem unbefugten Zugriff auf Amazon-VPC-Ressourcen führen kann.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-SC-7.C	SC-7.C Grenzschutz	lambda-function-public-access-verboten	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass AWS Lambda-Funktionen nicht öffentlich zugänglich sind. Der öffentliche Zugriff kann möglicherweise die Verfügbarkeit von Ressourcen beeinträchtigen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-SC-7.C	SC-7.C Grenzschutz	lambda-inside-vpc	Stellen Sie AWS Lambda-Funktionen in einer Amazon Virtual Private Cloud (Amazon VPC) bereit, um eine sichere Kommunika tion zwischen einer Funktion und anderen Diensten innerhalb der Amazon VPC zu gewährleisten. Bei dieser Konfiguration sind kein Internet-Gateway, kein NAT-Gerät und keine VPN-Verbindung erforderlich. Der gesamte Datenverk ehr bleibt sicher in der Cloud. AWS Domains, die sich innerhalb einer VPC befinden, verfügen aufgrund ihrer logischen Isolierun g im Vergleich zu Domains mit öffentlic hen Endpunkten über eine zusätzliche Sicherheitsebene. Um den Zugriff ordnungsg emäß zu verwalten,

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
			sollten AWS Lambda-Funktionen einer VPC zugewiesen werden.
CCCS-fPBMM-SC-7.C	SC-7.C Grenzschutz	opensearch-in-vpc-only	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass sich Amazon OpenSearch Service-Domains innerhalb einer Amazon Virtual Private Cloud (Amazon VPC) befinden. Eine Amazon OpenSearch Service-Domain innerhalb einer Amazon VPC ermöglicht die sichere Kommunikation zwischen Amazon OpenSearch Service und anderen Services innerhalb der Amazon VPC, ohne dass ein Internet-Gateway, ein NAT-Gerät oder eine VPN-Verbindung erforderlich ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-SC-7.C	SC-7.C Grenzschutz	rds-instance-public-access-überprüfen	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Relational Database Service (Amazon RDS) -Instances nicht öffentlich sind. Amazon-RDS-Datenbank-Instances können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-SC-7.C	SC-7.C Grenzschutz	rds-snapshots-public-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Relational Database Service (Amazon RDS) -Instances nicht öffentlich sind. Amazon-RDS-Datenbank-Instances können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-SC-7.C	SC-7.C Grenzschutz	redshift-cluster-public-access-überprüfen	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Redshift Redshift-Cluster nicht öffentlich sind. Amazon-Redshift-Cluster können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-SC-7.C	SC-7.C Grenzschutz	restricted-common-ports	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass gemeinsame Ports für Amazon Elastic Compute Cloud (Amazon EC2) -Sicherheitsgruppen eingeschränkt sind. Wenn der Zugriff auf Ports nicht auf vertrauenswürdige Quellen beschränkt wird, kann dies zu Angriffen auf die Verfügbarkeit, Integrität und Vertraulichkeit von Systemen führen. Mit dieser Regel können Sie optional die Parameter blockedPort1–blockedPort5 festlegen (Standardkonfigurationen: 20, 21, 3389, 3306, 4333). Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-SC-7.C	SC-7.C Grenzschutz	s3- account-level-public-access -blöcke-periodisch	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Simple Storage Service (Amazon S3) -Buckets nicht öffentlich zugänglich sind. Diese Regel trägt dazu bei, sensible Daten vor unbefugten Remote-Benutzern zu schützen, indem sie den öffentlichen Zugriff verhindert. Mit dieser Regel können Sie optional die Parameter ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) und restrictPublicBuckets Parameter (Config Default: True) festlegen. Die tatsächlichen Werte müssen den Richtlini

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
			en Ihrer Organisation entsprechen.
CCCS-fPBMM-SC-7.C	SC-7.C Grenzschutz	s3 bucket-level-public-access - verboten	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Simple Storage Service (Amazon S3) -Buckets nicht öffentlich zugänglich sind. Diese Regel trägt dazu bei, sensible Daten vor unbefugten Remote-Benutzern zu schützen, indem sie den öffentlichen Zugriff auf Bucket-Ebene verhindert.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-SC-7.C	SC-7.C Grenzschutz	s-3 bucket-public-read-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie nur autorisierten Benutzern, Prozessen und Geräten Zugriff auf Amazon Simple Storage Service (Amazon S3) - Buckets gewähren. Die Verwaltung des Zugriffs sollte mit der Klassifizierung der Daten übereinst immen.
CCCS-fPBMM-SC-7.C	SC-7.C Grenzschutz	s3- bucket-public-write-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie nur autorisierten Benutzern, Prozessen und Geräten Zugriff auf Amazon Simple Storage Service (Amazon S3) - Buckets gewähren. Die Verwaltung des Zugriffs sollte mit der Klassifizierung der Daten übereinst immen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-SC-7.C	SC-7.C Grenzschutz	sagemaker-notebook-no-direct-Internetzugang	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass SageMaker Amazon-Notebooks keinen direkten Internetzugang zulassen. Indem Sie direkten Internetzugang blockieren, vermeiden Sie, dass unbefugte Benutzer auf sensible Daten zugreifen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-SC-7.C	SC-7.C Grenzschutz	subnet-auto-assign-public-ip-deaktiviert	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon Virtual Private Cloud (VPC) -Subnetzen nicht automatisch eine öffentliche IP-Adresse zugewiesen wird. Amazon Elastic Compute Cloud (EC2) -Instances, die in Subnetzen gestartet werden, in denen dieses Attribut aktiviert ist, haben ihrer primären Netzwerkschnittstelle eine öffentliche IP-Adresse zugewiesen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-SC-7.C	SC-7.C Grenzschutz	vpc-default-security-group-geschlossen	Sicherheitsgruppen von Amazon Elastic Compute Cloud (Amazon EC2) können bei der Verwaltung des Netzwerkzugriffs helfen, indem sie eine statusbehaftete Filterung des ein- und ausgehenden Netzwerkverkehrs zu Ressourcen bereitstellen. AWS Die Beschränk ung des gesamten Datenverkehrs auf die Standardsicherheit sgruppe hilft dabei, den Fernzugriff auf Ihre Ressourcen einzuschränken. AWS

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-SC-7.C	SC-7.C Grenzschutz	vpc-sg-open-only-to-authorized-ports	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass gemeinsame Ports für Amazon Elastic Compute Cloud (Amazon EC2) -Sicherheitsgruppen eingeschränkt sind. Wenn der Zugriff auf Ports nicht auf vertrauenswürdige Quellen beschränkt wird, kann dies zu Angriffen auf die Verfügbarkeit, Integrität und Vertraulichkeit von Systemen führen. Durch die Beschränkung des Zugriffs auf Ressourcen innerhalb einer Sicherheitsgruppe aus dem Internet (0.0.0.0/0) kann der Fernzugriff auf interne Systeme gesteuert werden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-SC-8(1)	SC-8 (1) Vertrauli chkeit und Integrität von Übertragungen | Kryptografischer oder alternativer physische r Schutz	alb-http-to-https-Umleitungsprüfung	Um Daten während der Übertragung zu schützen, stellen Sie sicher, dass Ihr Application Load Balancer unverschl üsselte HTTP-Anfr agen automatisch an HTTPS umleitet. Da sensible Daten vorhanden sein können, sollten Sie die Verschlüsselung bei der Übertragung aktivieren, um diese Daten zu schützen.
CCCS-fPBMM-SC-8(1)	SC-8 (1) Vertrauli chkeit und Integrität von Übertragungen | Kryptografischer oder alternativer physische r Schutz	api-gw-ssl-enabled	Stellen Sie sicher, dass die REST-API-Stufen von Amazon API Gateway mit SSL-Zertifikaten konfiguri ert sind, damit Backend-Systeme überprüfen können, ob Anforderungen von API Gateway stammen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-SC-8(1)	SC-8 (1) Vertraulichkeit und Integrität von Übertragungen | Kryptografischer oder alternativer physischer Schutz	elasticsearch-node-to-node-Verschlüsselungsprüfung	Stellen Sie sicher, dass die node-to-node Verschlüsselung für Amazon OpenSearch Service aktiviert ist. Node-to-nodeVerschlüsselung ermöglicht die TLS 1.2-Verschlüsselung für die gesamte Kommunikation innerhalb der Amazon Virtual Private Cloud (Amazon VPC). Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-SC-8(1)	SC-8 (1) Vertraulichkeit und Integrität von Übertragungen | Kryptografischer oder alternativer physischer Schutz	elb-acm-certificate-required	Zum Schutz von eventuell vorhandenen sensiblen Daten sowie von Daten während der Übertragung muss die Verschlüsselung für Ihr Elastic Load Balancing aktiviert sein. Verwenden Sie AWS Certificate Manager, um öffentliche und private SSL/TLS-Zertifikate mit AWS Diensten und internen Ressourcen zu verwalten, bereitzustellen und bereitzustellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-SC-8(1)	SC-8 (1) Vertraulichkeit und Integrität von Übertragungen | Kryptografischer oder alternativer physischer Schutz	elb-predefined-security-policy-ssl-check	Stellen Sie sicher, dass Ihre SSL-Listener von Classic Elastic Load Balancing eine vordefinierte Sicherheitsrichtlinie verwenden, um Daten während der Übertragung zu schützen. Elastic Load Balancing bietet vordefinierte Aushandlungskonfigurationen, die für die SSL-Aushandlung verwendet werden, wenn eine Verbindung zwischen einem Client und Ihrem Load Balancer hergestellt wurde. Die SSL-Aushandlungskonfigurationen sind mit einer breiten Palette von Clients kompatibel und verwenden hochfeste kryptografische Algorithmen. Diese Regel verlangt, dass Sie eine vordefinierte Sicherheitsrichtlinie für Ihre SSL-Liste

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
			ner festlegen. Die Standard-Sicherheitsrichtlinie lautet: Policy-TLS-1-2-2017-0. ELBSecurity Der tatsächliche Wert muss den Richtlinien Ihrer Organisation entsprechen.
CCCS-fPBMM-SC-8(1)	SC-8 (1) Vertraulichkeit und Integrität von Übertragungen | Kryptografischer oder alternativer physischer Schutz	elb-tls-https-listeners-nur	Stellen Sie sicher, dass Ihre Elastic Load Balancer (ELBs) mit SSL- oder HTTPS-Listenern konfiguriert sind. Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-SC-8(1)	SC-8 (1) Vertraulichkeit und Integrität von Übertragungen | Kryptografischer oder alternativer physischer Schutz	opensearch-node-to-node-Verschlüsselungsprüfung	Stellen Sie sicher, dass die node-to-node Verschlüsselung für Amazon OpenSearch Service aktiviert ist. Node-to-nodeVerschlüsselung ermöglicht die TLS 1.2-Verschlüsselung für die gesamte Kommunikation innerhalb der Amazon Virtual Private Cloud (Amazon VPC). Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-SC-8(1)	SC-8 (1) Vertrauli chkeit und Integrität von Übertragungen | Kryptografischer oder alternativer physische r Schutz	redshift-require-tls-ssl	Stellen Sie sicher, dass Ihre Amazon-Redshift-Cluster eine TLS/SSL-Verschlüss elung erfordern, um eine Verbindung zu SQL-Clients herzustel len. Da sensible Daten vorhanden sein können, sollten Sie die Verschlüsselung bei der Übertragung aktivieren, um diese Daten zu schützen.
CCCS-fPBMM-SC-8(1)	SC-8 (1) Vertrauli chkeit und Integrität von Übertragungen | Kryptografischer oder alternativer physische r Schutz	s-3 bucket-ssl-request s-only	Um Daten während der Übertragung zu schützen, stellen Sie sicher, dass Ihre Amazon Simple Storage Service (Amazon S3)-Bucke ts Anfragen zur Verwendung von Secure Socket Layer (SSL)-Buckets erfordern. Da sensible Daten vorhanden sein können, sollten Sie die Verschlüsselung bei der Übertragung aktivieren, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-SC-8.A	SC-8.A Vertraulichkeit und Integrität von Übertragungen	alb-http-to-https-Umleitungsprüfung	Um Daten während der Übertragung zu schützen, stellen Sie sicher, dass Ihr Application Load Balancer unverschlüsselte HTTP-Anfragen automatisch an HTTPS umleitet. Da sensible Daten vorhanden sein können, sollten Sie die Verschlüsselung bei der Übertragung aktivieren, um diese Daten zu schützen.
CCCS-fPBMM-SC-8.A	SC-8.A Vertraulichkeit und Integrität von Übertragungen	api-gw-ssl-enabled	Stellen Sie sicher, dass die REST-API-Stufen von Amazon API Gateway mit SSL-Zertifikaten konfiguriert sind, damit Backend-Systeme überprüfen können, ob Anforderungen von API Gateway stammen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-SC-8.A	SC-8.A Vertraulichkeit und Integrität von Übertragungen	elasticsearch-node-to-node-Verschlüsselungsprüfung	Stellen Sie sicher, dass die node-to-node Verschlüsselung für Amazon OpenSearch Service aktiviert ist. Node-to-nodeVerschlüsselung ermöglicht die TLS 1.2-Verschlüsselung für die gesamte Kommunikation innerhalb der Amazon Virtual Private Cloud (Amazon VPC). Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-SC-8.A	SC-8.A Vertraulichkeit und Integrität von Übertragungen	elb-acm-certificate-required	Zum Schutz von eventuell vorhanden en sensiblen Daten sowie von Daten während der Übertragung muss die Verschlüsselung für Ihr Elastic Load Balancing aktiviert sein. Verwenden Sie AWS Certificate Manager, um öffentlic he und private SSL/ TLS-Zertifikate mit AWS Diensten und internen Ressource n zu verwalten, bereitzustellen und bereitzustellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-SC-8.A	SC-8.A Vertraulichkeit und Integrität von Übertragungen	elb-predefined-security-policy-ssl-check	Stellen Sie sicher, dass Ihre SSL-Listener von Classic Elastic Load Balancing eine vordefinierte Sicherheitsrichtlinie verwenden, um Daten während der Übertragung zu schützen. Elastic Load Balancing bietet vordefinierte Aushandlungskonfigurationen, die für die SSL-Aushandlung verwendet werden, wenn eine Verbindung zwischen einem Client und Ihrem Load Balancer hergestellt wurde. Die SSL-Aushandlungskonfigurationen sind mit einer breiten Palette von Clients kompatibel und verwenden hochfeste kryptografische Algorithmen. Diese Regel verlangt, dass Sie eine vordefinierte Sicherheitsrichtlinie für Ihre SSL-Liste

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
			ner festlegen. Die Standard-Sicherheitsrichtlinie lautet: Policy-TLS-1-2-2017-0. ELBSecurity Der tatsächliche Wert muss den Richtlinien Ihrer Organisation entsprechen.
CCCS-fPBMM-SC-8.A	SC-8.A Vertraulichkeit und Integrität von Übertragungen	elb-tls-https-listeners-nur	Stellen Sie sicher, dass Ihre Elastic Load Balancer (ELBs) mit SSL- oder HTTPS-Listenern konfiguriert sind. Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-SC-8.A	SC-8.A Vertraulichkeit und Integrität von Übertragungen	opensearch-node-to-node-Verschlüsselungsprüfung	Stellen Sie sicher, dass die node-to-node Verschlüsselung für Amazon OpenSearch Service aktiviert ist. Node-to-nodeVerschlüsselung ermöglicht die TLS 1.2-Verschlüsselung für die gesamte Kommunikation innerhalb der Amazon Virtual Private Cloud (Amazon VPC). Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-SC-8.A	SC-8.A Vertraulichkeit und Integrität von Übertragungen	redshift-require-tls-ssl	Stellen Sie sicher, dass Ihre Amazon-Redshift-Cluster eine TLS/SSL-Verschlüsselung erfordern, um eine Verbindung zu SQL-Clients herzustellen. Da sensible Daten vorhanden sein können, sollten Sie die Verschlüsselung bei der Übertragung aktivieren, um diese Daten zu schützen.
CCCS-fPBMM-SC-8.A	SC-8.A Vertraulichkeit und Integrität von Übertragungen	s-3 bucket-ssl-requests-only	Um Daten während der Übertragung zu schützen, stellen Sie sicher, dass Ihre Amazon Simple Storage Service (Amazon S3)-Buckets Anfragen zur Verwendung von Secure Socket Layer (SSL)-Buckets erfordern. Da sensible Daten vorhanden sein können, sollten Sie die Verschlüsselung bei der Übertragung aktivieren, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-SC-12(1)	SC-12(1) Einrichtung und Verwaltung kryptografischer Schlüssel | Verfügbarkeit	kms-cmk-not-scheduled-zum Löschen	Um Daten im Ruhezustand zu schützen, sollten Sie sicherstellen, dass die für den Kunden erforderlichen Masterschlüssel (CMKs) nicht für das Löschen im AWS Key Management Service (AWS KMS) vorgesehen sind. Da Schlüssel manchmal gelöscht werden müssen, können Sie mit dieser Regel alle zu löschenden Schlüssel überprüfen, falls ein Schlüssel versehentlich zur Löschung vorgemerkt wurde.
CCCS-fPBMM-SC-12(2)	SC-12(2) Einrichtung und Verwaltung kryptografischer Schlüssel | Symmetrische Schlüssel	cmk-backing-key-rotation-aktiviert	Aktivieren Sie die Schlüsselrotation, um sicherzustellen, dass Schlüssel rotiert werden, sobald sie das Ende ihrer Kryptoperiode erreicht haben.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-SC-12(2)	SC-12(2) Einrichtung und Verwaltung kryptografischer Schlüssel | Symmetrische Schlüssel	kms-cmk-not-scheduled-zum Löschen	Um Daten im Ruhezustand zu schützen, sollten Sie sicherstellen, dass die für den Kunden erforderlichen Masterschlüssel (CMKs) nicht für das Löschen im AWS Key Management Service (AWS KMS) vorgesehen sind. Da Schlüssel manchmal gelöscht werden müssen, können Sie mit dieser Regel alle zu löschenden Schlüssel überprüfen, falls ein Schlüssel versehentlich zur Löschung vorgemerkt wurde.
CCCS-fPBMM-SC-12.A	SC-12.A Einrichtung und Verwaltung kryptografischer Schlüssel	cmk-backing-key-rotation-aktiviert	Aktivieren Sie die Schlüsselrotation, um sicherzustellen, dass Schlüssel rotiert werden, sobald sie das Ende ihrer Kryptoperiode erreicht haben.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-SC-12.A	SC-12.A Einrichtung und Verwaltung kryptografischer Schlüssel	kms-cmk-not-scheduled-zum Löschen	Um Daten im Ruhezustand zu schützen, sollten Sie sicherstellen, dass die für den Kunden erforderlichen Masterschlüssel (CMKs) nicht für das Löschen im AWS Key Management Service (AWS KMS) vorgesehen sind. Da Schlüssel manchmal gelöscht werden müssen, können Sie mit dieser Regel alle zu löschenden Schlüssel überprüfen, falls ein Schlüssel versehentlich zur Löschung vorgemerkt wurde.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-SC-13.A	SC-13.A Kryptografischer Schutz	alb-http-to-https-Umleitungsprüfung	Um Daten während der Übertragung zu schützen, stellen Sie sicher, dass Ihr Application Load Balancer unverschlüsselte HTTP-Anfragen automatisch an HTTPS umleitet. Da sensible Daten vorhanden sein können, sollten Sie die Verschlüsselung bei der Übertragung aktivieren, um diese Daten zu schützen.
CCCS-fPBMM-SC-13.A	SC-13.A Kryptografischer Schutz	api-gw-ssl-enabled	Stellen Sie sicher, dass die REST-API-Stufen von Amazon API Gateway mit SSL-Zertifikaten konfiguriert sind, damit Backend-Systeme überprüfen können, ob Anforderungen von API Gateway stammen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-SC-13.A	SC-13.A Kryptografischer Schutz	cloud-trail-encryption-enabled	Zum Schutz von eventuell vorhandenen sensiblen Daten sowie Daten im Ruhezustand müssen Sie sicherstellen, dass die Verschlüsselung für Ihre AWS CloudTrail aktiviert ist.
CCCS-fPBMM-SC-13.A	SC-13.A Kryptografischer Schutz	ec2- ebs-encryption-by-default	Zum Schutz von Daten im Ruhezustand müssen Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon Elastic Block Store (Amazon EBS)-Volumes aktiviert ist. Aktivieren Sie die Verschlüsselung von Daten im Ruhezustand, um eventuell in diesen Volumes vorhandene sensible Daten im Ruhezustand zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-SC-13.A	SC-13.A Kryptografischer Schutz	efs-encrypted-check	Aktivieren Sie die Verschlüsselung für Ihr Amazon Elastic File System (EFS), um eventuell vorhandene sensible Daten sowie Daten im Ruhezustand zu schützen.
CCCS-fPBMM-SC-13.A	SC-13.A Kryptografischer Schutz	elasticsearch-encrypted-at-rest	Da sensible Daten vorhanden sein können und um Daten im Ruhezustand zu schützen, sollten Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon OpenSearch Service (OpenSearch Service) -Domains aktiviert ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-SC-13.A	SC-13.A Kryptografischer Schutz	elasticsearch-node-to-node-Verschlüsselungsprüfung	Stellen Sie sicher, dass die node-to-node Verschlüsselung für Amazon OpenSearch Service aktiviert ist. Node-to-nodeVerschlüsselung ermöglicht die TLS 1.2-Verschlüsselung für die gesamte Kommunikation innerhalb der Amazon Virtual Private Cloud (Amazon VPC). Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-SC-13.A	SC-13.A Kryptografischer Schutz	elb-acm-certificate-required	Zum Schutz von eventuell vorhandenen sensiblen Daten sowie von Daten während der Übertragung muss die Verschlüsselung für Ihr Elastic Load Balancing aktiviert sein. Verwenden Sie AWS Certificate Manager, um öffentliche und private SSL/TLS-Zertifikate mit AWS Diensten und internen Ressourcen zu verwalten, bereitzustellen und bereitzustellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-SC-13.A	SC-13.A Kryptografischer Schutz	elb-predefined-security-policy-ssl-check	Stellen Sie sicher, dass Ihre SSL-Listener von Classic Elastic Load Balancing eine vordefinierte Sicherheitsrichtlinie verwenden, um Daten während der Übertragung zu schützen. Elastic Load Balancing bietet vordefinierte Aushandlungskonfigurationen, die für die SSL-Aushandlung verwendet werden, wenn eine Verbindung zwischen einem Client und Ihrem Load Balancer hergestellt wurde. Die SSL-Aushandlungskonfigurationen sind mit einer breiten Palette von Clients kompatibel und verwenden hochfeste kryptografische Algorithmen. Diese Regel verlangt, dass Sie eine vordefinierte Sicherheitsrichtlinie für Ihre SSL-Liste

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
			ner festlegen. Die Standard-Sicherheitsrichtlinie lautet: Policy-TLS-1-2-2017-0. ELBSecurity Der tatsächliche Wert muss den Richtlinien Ihrer Organisation entsprechen.
CCCS-fPBMM-SC-13.A	SC-13.A Kryptografischer Schutz	elb-tls-https-listeners-nur	Stellen Sie sicher, dass Ihre Elastic Load Balancer (ELBs) mit SSL- oder HTTPS-Listenern konfiguriert sind. Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.
CCCS-fPBMM-SC-13.A	SC-13.A Kryptografischer Schutz	encrypted-volumes	Aktivieren Sie die Verschlüsselung für Ihre Volumes von Amazon Elastic Block Store (Amazon EBS), um eventuell vorhandene sensible Daten sowie Daten im Ruhezustand zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-SC-13.A	SC-13.A Kryptografischer Schutz	opensearch-encrypted-at-rest	Da sensible Daten vorhanden sein können und um Daten im Ruhezustand zu schützen, sollten Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon OpenSearch Service-Domains aktiviert ist.
CCCS-fPBMM-SC-13.A	SC-13.A Kryptografischer Schutz	opensearch-node-to-node-Verschlüsselungsprüfung	Stellen Sie sicher, dass die node-to-node Verschlüsselung für Amazon OpenSearch Service aktiviert ist. Node-to-nodeVerschlüsselung ermöglicht die TLS 1.2-Verschlüsselung für die gesamte Kommunikation innerhalb der Amazon Virtual Private Cloud (Amazon VPC). Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-SC-13.A	SC-13.A Kryptografischer Schutz	rds-snapshot-encrypted	Stellen Sie sicher, dass die Verschlüsselung für Ihre Amazon Relational Database Service (Amazon RDS)-Snapshots aktiviert ist. Da sensible Daten auch im Ruhezustand vorhanden sein können, sollten Sie die Verschlüsselung von Daten im Ruhezustand aktivieren, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-SC-13.A	SC-13.A Kryptografischer Schutz	rds-storage-encrypted	Zum Schutz von Daten im Ruhezustand müssen Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon Relational Database Service (Amazon RDS)-Instances aktiviert ist. Da sensible Daten in Amazon-RDS-Instances gespeichert werden können, sollten Sie die Verschlüsselung von Daten im Ruhezustand aktivieren, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-SC-13.A	SC-13.A Kryptografischer Schutz	redshift-cluster-configuration-check	Um Daten im Ruhezustand zu schützen, muss die Verschlüsselung für Ihre Amazon-Redshift-Cluster aktiviert sein. Sie müssen auch sicherstellen, dass die erforderlichen Konfigurationen auf Amazon-Redshift-Clustern bereitgestellt werden. Die Prüfungsprotokollierung muss aktiviert sein, um Informationen zu Verbindungen und Benutzeraktivitäten in der Datenbank bereitzustellen. Diese Regel erfordert, dass ein Wert für clusterDbEncrypted (Config Default: TRUE) und LoggingEnabled (Config Default: TRUE) gesetzt ist. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-SC-13.A	SC-13.A Kryptografischer Schutz	redshift-cluster-kms-enabled	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass die Verschlüsselung mit AWS Key Management Service (AWS KMS) für Ihren Amazon Redshift Redshift-Cluster aktiviert ist. Um eventuell vorhandene sensible Daten im Ruhezustand in Redshift-Clustern zu schützen, muss die Verschlüsselung von Daten im Ruhezustand aktiviert sein.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-SC-13.A	SC-13.A Kryptografischer Schutz	redshift-require-tls-ssl	Stellen Sie sicher, dass Ihre Amazon-Redshift-Cluster eine TLS/SSL-Verschlüsselung erfordern, um eine Verbindung zu SQL-Clients herzustellen. Da sensible Daten vorhanden sein können, sollten Sie die Verschlüsselung bei der Übertragung aktivieren, um diese Daten zu schützen.
CCCS-fPBMM-SC-13.A	SC-13.A Kryptografischer Schutz	s3- aktiviert bucket-server-side-encryption	Zum Schutz von Daten im Ruhezustand müssen Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon Simple Storage Service (Amazon S3)-Buckets aktiviert ist. Da sensible Daten in Amazon-S3-Buckets gespeichert werden können, sollten Sie die Verschlüsselung aktivieren, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-SC-13.A	SC-13.A Kryptografischer Schutz	s-3 bucket-ssl-requests-only	Um Daten während der Übertragung zu schützen, stellen Sie sicher, dass Ihre Amazon Simple Storage Service (Amazon S3)-Buckets Anfragen zur Verwendung von Secure Socket Layer (SSL)-Buckets erfordern. Da sensible Daten vorhanden sein können, sollten Sie die Verschlüsselung bei der Übertragung aktivieren, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-SC-13.A	SC-13.A Kryptografischer Schutz	sagemaker-endpoint-configuration-kms-key-konfiguriert	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass die Verschlüsselung mit dem AWS Key Management Service (AWS KMS) für Ihren Endpunkt aktiviert ist. SageMaker Da sensible Daten auf dem SageMaker Endgerät gespeichert werden können, sollten Sie die Verschlüsselung im Ruhezustand aktivieren, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-SC-13.A	SC-13.A Kryptografischer Schutz	sagemaker-notebook-instance-kms-schlüsselkonfiguriert	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass die Verschlüsselung mit dem AWS Key Management Service (AWS KMS) für Ihr Notebook aktiviert ist. SageMaker Da vertrauliche Daten im SageMaker Notebook gespeichert werden können, sollten Sie die Verschlüsselung im Ruhezustand aktivieren, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-SC-13.A	SC-13.A Kryptografischer Schutz	secretsmanager-using-cmk	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass die Verschlüsselung mit dem AWS Key Management Service (AWS KMS) für AWS Secrets Manager aktiviert ist. Aktivieren Sie die Verschlüsselung von Daten im Ruhezustand, um eventuell vorhandene sensible Daten im Ruhezustand im Secrets Manager zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-SC-13.A	SC-13.A Kryptografischer Schutz	sns-encrypted-kms	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass Ihre Amazon Simple Notification Service (Amazon SNS) -Themen mit dem AWS Key Management Service (AWS KMS) verschlüsselt werden müssen. Um eventuell vorhandene sensible Daten im Ruhezustand in veröffentlichten Nachrichten zu schützen, muss die Verschlüsselung von Daten im Ruhezustand aktiviert sein.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-SC-22.A	SC-22.A Architektur und Bereitstellung für den Service zur Namens-/Adressauflösung	elb-deletion-protection-enabled	Diese Regel sorgt dafür, dass der Löschschutz für Elastic Load Balancing aktiviert ist. Verwenden Sie diese Funktion, um zu verhindern, dass Ihr Load Balancer versehentlich oder böswillig gelöscht wird, was zum Verlust der Verfügbarkeit Ihrer Anwendungen führen kann.
CCCS-fPBMM-SC-23.A	SC-23.A Sitzungsauthentizität	alb-http-to-https-Umleitungsprüfung	Um Daten während der Übertragung zu schützen, stellen Sie sicher, dass Ihr Application Load Balancer unverschlüsselte HTTP-Anfragen automatisch an HTTPS umleitet. Da sensible Daten vorhanden sein können, sollten Sie die Verschlüsselung bei der Übertragung aktivieren, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-SC-23.A	SC-23.A Sitzungsauthentizität	api-gw-ssl-enabled	Stellen Sie sicher, dass die REST-API-Stufen von Amazon API Gateway mit SSL-Zertifikaten konfiguriert sind, damit Backend-Systeme überprüfen können, ob Anforderungen von API Gateway stammen.
CCCS-fPBMM-SC-23.A	SC-23.A Sitzungsauthentizität	elasticsearch-node-to-node-Verschlüsselungsprüfung	Stellen Sie sicher, dass die node-to-node Verschlüsselung für Amazon OpenSearch Service aktiviert ist. Node-to-nodeVerschlüsselung ermöglicht die TLS 1.2-Verschlüsselung für die gesamte Kommunikation innerhalb der Amazon Virtual Private Cloud (Amazon VPC). Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-SC-23.A	SC-23.A Sitzungsauthentizität	elb-acm-certificate-required	Zum Schutz von eventuell vorhanden en sensiblen Daten sowie von Daten während der Übertragung muss die Verschlüsselung für Ihr Elastic Load Balancing aktiviert sein. Verwenden Sie AWS Certificate Manager, um öffentlic he und private SSL/TLS-Zertifikate mit AWS Diensten und internen Ressource n zu verwalten, bereitzustellen und bereitzustellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-SC-23.A	SC-23.A Sitzungsauthentizität	elb-predefined-security-policy-ssl-check	Stellen Sie sicher, dass Ihre SSL-Listener von Classic Elastic Load Balancing eine vordefinierte Sicherheitsrichtlinie verwenden, um Daten während der Übertragung zu schützen. Elastic Load Balancing bietet vordefinierte Aushandlungskonfigurationen, die für die SSL-Aushandlung verwendet werden, wenn eine Verbindung zwischen einem Client und Ihrem Load Balancer hergestellt wurde. Die SSL-Aushandlungskonfigurationen sind mit einer breiten Palette von Clients kompatibel und verwenden hochfeste kryptografische Algorithmen. Diese Regel verlangt, dass Sie eine vordefinierte Sicherheitsrichtlinie für Ihre SSL-Liste

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
			ner festlegen. Die Standard-Sicherheitsrichtlinie lautet: Policy-TLS-1-2-2017-0. ELBSecurity Der tatsächliche Wert muss den Richtlinien Ihrer Organisation entsprechen.
CCCS-fPBMM-SC-23.A	SC-23.A Sitzungsauthentizität	elb-tls-https-listeners-nur	Stellen Sie sicher, dass Ihre Elastic Load Balancer (ELBs) mit SSL- oder HTTPS-Listenern konfiguriert sind. Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-SC-23.A	SC-23.A Sitzungsauthentizität	opensearch-node-to-node-Verschlüsselungsprüfung	Stellen Sie sicher, dass die node-to-node Verschlüsselung für Amazon OpenSearch Service aktiviert ist. Node-to-nodeVerschlüsselung ermöglicht die TLS 1.2-Verschlüsselung für die gesamte Kommunikation innerhalb der Amazon Virtual Private Cloud (Amazon VPC). Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-SC-23.A	SC-23.A Sitzungsauthentizität	redshift-require-tls-ssl	Stellen Sie sicher, dass Ihre Amazon-Redshift-Cluster eine TLS/SSL-Verschlüsselung erfordern, um eine Verbindung zu SQL-Clients herzustellen. Da sensible Daten vorhanden sein können, sollten Sie die Verschlüsselung bei der Übertragung aktivieren, um diese Daten zu schützen.
CCCS-fPBMM-SC-23.A	SC-23.A Sitzungsauthentizität	s-3 bucket-ssl-requests-only	Um Daten während der Übertragung zu schützen, stellen Sie sicher, dass Ihre Amazon Simple Storage Service (Amazon S3)-Buckets Anfragen zur Verwendung von Secure Socket Layer (SSL)-Buckets erfordern. Da sensible Daten vorhanden sein können, sollten Sie die Verschlüsselung bei der Übertragung aktivieren, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-SC-28(1)	SC-28(1) Schutz von Informationen im Ruhezustand | Kryptografischer Schutz	cloud-trail-encryption-enabled	Zum Schutz von eventuell vorhanden en sensiblen Daten sowie Daten im Ruhezustand müssen Sie sicherstellen, dass die Verschlüs selung für Ihre AWS CloudTrail aktiviert ist.
CCCS-fPBMM-SC-28(1)	SC-28(1) Schutz von Informationen im Ruhezustand | Kryptografischer Schutz	ec2- ebs-encryption-by-default	Zum Schutz von Daten im Ruhezusta nd müssen Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon Elastic Block Store (Amazon EBS)-Volu mes aktiviert ist. Aktivieren Sie die Verschlüsselung von Daten im Ruhezusta nd, um eventuell in diesen Volumes vorhandene sensible Daten im Ruhezusta nd zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-SC-28(1)	SC-28(1) Schutz von Informationen im Ruhezustand | Kryptografischer Schutz	efs-encrypted-check	Aktivieren Sie die Verschlüsselung für Ihr Amazon Elastic File System (EFS), um eventuell vorhandene sensible Daten sowie Daten im Ruhezustand zu schützen.
CCCS-fPBMM-SC-28(1)	SC-28(1) Schutz von Informationen im Ruhezustand | Kryptografischer Schutz	elasticsearch-encrypted-at-rest	Da sensible Daten vorhanden sein können und um Daten im Ruhezustand zu schützen, sollten Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon OpenSearch Service (OpenSearch Service) -Domains aktiviert ist.
CCCS-fPBMM-SC-28(1)	SC-28(1) Schutz von Informationen im Ruhezustand | Kryptografischer Schutz	encrypted-volumes	Aktivieren Sie die Verschlüsselung für Ihre Volumes von Amazon Elastic Block Store (Amazon EBS), um eventuell vorhandene sensible Daten sowie Daten im Ruhezustand zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-SC-28(1)	SC-28(1) Schutz von Informationen im Ruhezustand | Kryptografischer Schutz	opensearch-encrypted-at-rest	Da sensible Daten vorhanden sein können und um Daten im Ruhezustand zu schützen, sollten Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon OpenSearch Service-Domains aktiviert ist.
CCCS-fPBMM-SC-28(1)	SC-28(1) Schutz von Informationen im Ruhezustand | Kryptografischer Schutz	rds-snapshot-encrypted	Stellen Sie sicher, dass die Verschlüsselung für Ihre Amazon Relational Database Service (Amazon RDS)-Snapshots aktiviert ist. Da sensible Daten auch im Ruhezustand vorhanden sein können, sollten Sie die Verschlüsselung von Daten im Ruhezustand aktivieren, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-SC-28(1)	SC-28(1) Schutz von Informationen im Ruhezustand | Kryptografischer Schutz	rds-storage-encrypted	Zum Schutz von Daten im Ruhezustand müssen Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon Relational Database Service (Amazon RDS)-Instances aktiviert ist. Da sensible Daten in Amazon-RDS-Instances gespeichert werden können, sollten Sie die Verschlüsselung von Daten im Ruhezustand aktivieren, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-SC-28(1)	SC-28(1) Schutz von Informationen im Ruhezustand | Kryptografischer Schutz	redshift-cluster-configuration-check	Um Daten im Ruhezustand zu schützen, muss die Verschlüsselung für Ihre Amazon-Redshift-Cluster aktiviert sein. Sie müssen auch sicherstellen, dass die erforderlichen Konfigurationen auf Amazon-Redshift-Clustern bereitgestellt werden. Die Prüfungsprotokollierung muss aktiviert sein, um Informationen zu Verbindungen und Benutzeraktivitäten in der Datenbank bereitzustellen. Diese Regel erfordert, dass ein Wert für clusterDbEncrypted (Config Default: TRUE) und LoggingEnabled (Config Default: TRUE) gesetzt ist. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-SC-28(1)	SC-28(1) Schutz von Informationen im Ruhezustand | Kryptografischer Schutz	redshift-cluster-kms-enabled	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass die Verschlüs selung mit AWS Key Management Service (AWS KMS) für Ihren Amazon Redshift Redshift-Cluster aktiviert ist. Um eventuell vorhanden e sensible Daten im Ruhezustand in Redshift-Clustern zu schützen, muss die Verschlüsselung von Daten im Ruhezusta nd aktiviert sein.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-SC-28(1)	SC-28(1) Schutz von Informationen im Ruhezustand | Kryptografischer Schutz	s3- aktiviert bucket-server-side-encryption	Zum Schutz von Daten im Ruhezustand müssen Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon Simple Storage Service (Amazon S3)-Buckets aktiviert ist. Da sensible Daten in Amazon-S3-Buckets gespeichert werden können, sollten Sie die Verschlüsselung aktivieren, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-SC-28(1)	SC-28(1) Schutz von Informationen im Ruhezustand | Kryptografischer Schutz	sagemaker-endpoint-configuration-kms-key-konfiguriert	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass die Verschlüsselung mit dem AWS Key Management Service (AWS KMS) für Ihren Endpunkt aktiviert ist. SageMaker Da sensible Daten auf dem SageMaker Endgerät gespeiche rt werden können, sollten Sie die Verschlüsselung im Ruhezustand aktiviere n, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-SC-28(1)	SC-28(1) Schutz von Informationen im Ruhezustand | Kryptografischer Schutz	sagemaker-notebook-instance-kms-schlüsselkonfiguriert	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass die Verschlüsselung mit dem AWS Key Management Service (AWS KMS) für Ihr Notebook aktiviert ist. SageMaker Da vertrauliche Daten im SageMaker Notebook gespeichert werden können, sollten Sie die Verschlüsselung im Ruhezustand aktivieren, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-SC-28(1)	SC-28(1) Schutz von Informationen im Ruhezustand | Kryptografischer Schutz	secretsmanager-using-cmk	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass die Verschlüsselung mit dem AWS Key Management Service (AWS KMS) für AWS Secrets Manager aktiviert ist. Aktivieren Sie die Verschlüsselung von Daten im Ruhezustand, um eventuell vorhandene sensible Daten im Ruhezustand im Secrets Manager zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-SC-28(1)	SC-28(1) Schutz von Informationen im Ruhezustand | Kryptografischer Schutz	sns-encrypted-kms	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass Ihre Amazon Simple Notification Service (Amazon SNS) -Themen mit dem AWS Key Management Service (AWS KMS) verschlüsselt werden müssen. Um eventuell vorhandene sensible Daten im Ruhezustand in veröffentlichten Nachrichten zu schützen, muss die Verschlüsselung von Daten im Ruhezustand aktiviert sein.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-SC-28.A	SC-28.A Schutz von Informationen im Ruhezustand	backup-recovery-point-encrypted	Stellen Sie sicher, dass die Verschlüsselung für Ihre AWS Backup-Wiederherstellungspunkte aktiviert ist. Da sensible Daten auch im Ruhezustand vorhanden sein können, sollten Sie die Verschlüsselung im Ruhezustand aktivieren, um diese Daten zu schützen.
CCCS-fPBMM-SC-28.A	SC-28.A Schutz von Informationen im Ruhezustand	cloud-trail-encryption-enabled	Zum Schutz von eventuell vorhandenen sensiblen Daten sowie Daten im Ruhezustand müssen Sie sicherstellen, dass die Verschlüsselung für Ihre AWS CloudTrail aktiviert ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-SC-28.A	SC-28.A Schutz von Informationen im Ruhezustand	ec2- ebs-encryption-by-default	Zum Schutz von Daten im Ruhezustand müssen Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon Elastic Block Store (Amazon EBS)-Volumes aktiviert ist. Aktivieren Sie die Verschlüsselung von Daten im Ruhezustand, um eventuell in diesen Volumes vorhandene sensible Daten im Ruhezustand zu schützen.
CCCS-fPBMM-SC-28.A	SC-28.A Schutz von Informationen im Ruhezustand	efs-encrypted-check	Aktivieren Sie die Verschlüsselung für Ihr Amazon Elastic File System (EFS), um eventuell vorhandene sensible Daten sowie Daten im Ruhezustand zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-SC-28.A	SC-28.A Schutz von Informationen im Ruhezustand	elasticsearch-encrypted-at-rest	Da sensible Daten vorhanden sein können und um Daten im Ruhezustand zu schützen, sollten Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon OpenSearch Service (OpenSearch Service) -Domains aktiviert ist.
CCCS-fPBMM-SC-28.A	SC-28.A Schutz von Informationen im Ruhezustand	elasticsearch-node-to-node-Verschlüsselungsprüfung	Stellen Sie sicher, dass die node-to-node Verschlüsselung für Amazon OpenSearch Service aktiviert ist. Node-to-nodeVerschlüsselung ermöglicht die TLS 1.2-Verschlüsselung für die gesamte Kommunikation innerhalb der Amazon Virtual Private Cloud (Amazon VPC). Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-SC-28.A	SC-28.A Schutz von Informationen im Ruhezustand	elb-acm-certificate-required	Zum Schutz von eventuell vorhanden en sensiblen Daten sowie von Daten während der Übertragung muss die Verschlüsselung für Ihr Elastic Load Balancing aktiviert sein. Verwenden Sie AWS Certificate Manager, um öffentlic he und private SSL/ TLS-Zertifikate mit AWS Diensten und internen Ressource n zu verwalten, bereitzustellen und bereitzustellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-SC-28.A	SC-28.A Schutz von Informationen im Ruhezustand	elb-predefined-security-policy-ssl-check	Stellen Sie sicher, dass Ihre SSL-Listener von Classic Elastic Load Balancing eine vordefinierte Sicherheitsrichtlinie verwenden, um Daten während der Übertragung zu schützen. Elastic Load Balancing bietet vordefinierte Aushandlungskonfigurationen, die für die SSL-Aushandlung verwendet werden, wenn eine Verbindung zwischen einem Client und Ihrem Load Balancer hergestellt wurde. Die SSL-Aushandlungskonfigurationen sind mit einer breiten Palette von Clients kompatibel und verwenden hochfeste kryptografische Algorithmen. Diese Regel verlangt, dass Sie eine vordefinierte Sicherheitsrichtlinie für Ihre SSL-Liste

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
			ner festlegen. Die Standard-Sicherheitsrichtlinie lautet: Policy-TLS-1-2-2017-0. ELBSecurity Der tatsächliche Wert muss den Richtlinien Ihrer Organisation entsprechen.
CCCS-fPBMM-SC-28.A	SC-28.A Schutz von Informationen im Ruhezustand	elb-tls-https-listeners-nur	Stellen Sie sicher, dass Ihre Elastic Load Balancer (ELBs) mit SSL- oder HTTPS-Listenern konfiguriert sind. Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.
CCCS-fPBMM-SC-28.A	SC-28.A Schutz von Informationen im Ruhezustand	encrypted-volumes	Aktivieren Sie die Verschlüsselung für Ihre Volumes von Amazon Elastic Block Store (Amazon EBS), um eventuell vorhandene sensible Daten sowie Daten im Ruhezustand zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-SC-28.A	SC-28.A Schutz von Informationen im Ruhezustand	opensearch-encrypted-at-rest	Da sensible Daten vorhanden sein können und um Daten im Ruhezustand zu schützen, sollten Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon OpenSearch Service-Domains aktiviert ist.
CCCS-fPBMM-SC-28.A	SC-28.A Schutz von Informationen im Ruhezustand	opensearch-node-to-node-Verschlüsselungsprüfung	Stellen Sie sicher, dass die node-to-node Verschlüsselung für Amazon OpenSearch Service aktiviert ist. Node-to-nodeVerschlüsselung ermöglicht die TLS 1.2-Verschlüsselung für die gesamte Kommunikation innerhalb der Amazon Virtual Private Cloud (Amazon VPC). Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-SC-28.A	SC-28.A Schutz von Informationen im Ruhezustand	rds-snapshot-encrypted	Stellen Sie sicher, dass die Verschlüsselung für Ihre Amazon Relational Database Service (Amazon RDS)-Snapshots aktiviert ist. Da sensible Daten auch im Ruhezustand vorhanden sein können, sollten Sie die Verschlüsselung von Daten im Ruhezustand aktivieren, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-SC-28.A	SC-28.A Schutz von Informationen im Ruhezustand	rds-storage-encrypted	Zum Schutz von Daten im Ruhezustand müssen Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon Relational Database Service (Amazon RDS)-Instances aktiviert ist. Da sensible Daten in Amazon-RDS-Instances gespeichert werden können, sollten Sie die Verschlüsselung von Daten im Ruhezustand aktivieren, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-SC-28.A	SC-28.A Schutz von Informationen im Ruhezustand	redshift-cluster-configuration-check	Um Daten im Ruhezustand zu schützen, muss die Verschlüsselung für Ihre Amazon-Redshift-Cluster aktiviert sein. Sie müssen auch sicherstellen, dass die erforderlichen Konfigurationen auf Amazon-Redshift-Clustern bereitgestellt werden. Die Prüfungsprotokollierung muss aktiviert sein, um Informationen zu Verbindungen und Benutzeraktivitäten in der Datenbank bereitzustellen. Diese Regel erfordert, dass ein Wert für clusterDbEncrypted (Config Default: TRUE) und LoggingEnabled (Config Default: TRUE) gesetzt ist. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-SC-28.A	SC-28.A Schutz von Informationen im Ruhezustand	redshift-cluster-kms-enabled	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass die Verschlüs selung mit AWS Key Management Service (AWS KMS) für Ihren Amazon Redshift Redshift-Cluster aktiviert ist. Da sensible Daten in Redshift-Clustern gespeichert werden können, sollten Sie die Verschlüs selung von Daten im Ruhezustand aktiviere n, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-SC-28.A	SC-28.A Schutz von Informationen im Ruhezustand	redshift-require-tls-ssl	Stellen Sie sicher, dass Ihre Amazon-Redshift-Cluster eine TLS/SSL-Verschlüsselung erfordern, um eine Verbindung zu SQL-Clients herzustellen. Da sensible Daten vorhanden sein können, sollten Sie die Verschlüsselung bei der Übertragung aktivieren, um diese Daten zu schützen.
CCCS-fPBMM-SC-28.A	SC-28.A Schutz von Informationen im Ruhezustand	s3- aktiviert bucket-server-side-encryption	Zum Schutz von Daten im Ruhezustand müssen Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon Simple Storage Service (Amazon S3)-Buckets aktiviert ist. Da sensible Daten in Amazon-S3-Buckets gespeichert werden können, sollten Sie die Verschlüsselung aktivieren, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-SC-28.A	SC-28.A Schutz von Informationen im Ruhezustand	s-3 bucket-ssl-requests-only	Um Daten während der Übertragung zu schützen, stellen Sie sicher, dass Ihre Amazon Simple Storage Service (Amazon S3)-Buckets Anfragen zur Verwendung von Secure Socket Layer (SSL)-Buckets erfordern. Da sensible Daten vorhanden sein können, sollten Sie die Verschlüsselung bei der Übertragung aktivieren, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-SC-28.A	SC-28.A Schutz von Informationen im Ruhezustand	sagemaker-endpoint-configuration-kms-key-konfiguriert	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass die Verschlüsselung mit dem AWS Key Management Service (AWS KMS) für Ihren Endpunkt aktiviert ist. SageMaker Da sensible Daten auf dem SageMaker Endgerät gespeiche rt werden können, sollten Sie die Verschlüsselung im Ruhezustand aktiviere n, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-SC-28.A	SC-28.A Schutz von Informationen im Ruhezustand	sagemaker-notebook-instance-kms-schlüsselkonfiguriert	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass die Verschlüsselung mit dem AWS Key Management Service (AWS KMS) für Ihr Notebook aktiviert ist. SageMaker Da vertrauliche Daten im SageMaker Notebook gespeichert werden können, sollten Sie die Verschlüsselung im Ruhezustand aktivieren, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-SC-28.A	SC-28.A Schutz von Informationen im Ruhezustand	secretsmanager-using-cmk	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass die Verschlüsselung mit dem AWS Key Management Service (AWS KMS) für AWS Secrets Manager aktiviert ist. Aktivieren Sie die Verschlüsselung von Daten im Ruhezustand, um eventuell vorhandene sensible Daten im Ruhezustand im Secrets Manager zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-SC-28.A	SC-28.A Schutz von Informationen im Ruhezustand	sns-encrypted-kms	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass Ihre Amazon Simple Notification Service (Amazon SNS) -Themen mit dem AWS Key Management Service (AWS KMS) verschlüsselt werden müssen. Um eventuell vorhandene sensible Daten im Ruhezustand in veröffentlichten Nachrichten zu schützen, muss die Verschlüsselung von Daten im Ruhezustand aktiviert sein.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-SI-2(2)	SI-2(2) Fehlerkorrektur | Status der automatisierten Fehlerkorrektur	autoscaling-group-elb-healthcheck-erforderlich	Die Elastic Load Balancer (ELB) - Zustandsprüfungen für Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling Scaling-Gruppen unterstützen die Aufrechterhaltung einer angemessenen Kapazität und Verfügbarkeit. Der Load Balancer sendet regelmäßig Pings, versucht Verbindungen herzustellen oder sendet Anfragen, um den Zustand der EC2 Amazon-Instances in einer Gruppe mit auto-scaling zu testen. Wenn eine Instance nicht zurückmeldet, wird der Traffic an eine neue EC2 Amazon-Instance gesendet.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-SI-2(2)	SI-2(2) Fehlerkorrektur | Status der automatisierten Fehlerkorrektur	beanstalk-enhanced-health-reporting-aktiviert	AWS Die verbesserte Zustandsberichterstattung von Elastic Beanstalk ermöglicht eine schnellere Reaktion auf Veränderungen im Zustand der zugrunde liegenden Infrastruktur. Diese Änderungen könnten zu einer mangelnden Verfügbarkeit der Anwendung führen. Die erweiterten Zustandsberichte von Elastic Beanstalk bieten eine Statusbeschreibung, um den Schweregrad der identifizierten Probleme einzuschätzen und mögliche Ursachen zu identifizieren, die untersucht werden müssen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-SI-2(2)	SI-2(2) Fehlerkorrektur | Status der automatisierten Fehlerkorrektur	cloudwatch-alarm-action-check	Amazon CloudWatch alarmiert, wenn eine Metrik den Schwellenwert für eine bestimmte Anzahl von Bewertungszeiträumen überschreitet. Der Alarm führt eine oder mehrere Aktionen durch, die vom Wert der Metrik oder des Ausdrucks im Vergleich zu einem Schwellenwert in einer Reihe von Zeiträumen abhängt. Diese Regel erfordert einen Wert für alarmActionRequired (Config Default: True), insufficientDataAction Required (Config Default: True), okActionRequired (Config Default: False). Der tatsächliche Wert muss die Alarmaktionen für Ihre Umgebung widerspiegeln.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-SI-2(2)	SI-2(2) Fehlerkorrektur | Status der automatisierten Fehlerkorrektur	dynamodb-throughput-limit-check	Aktivieren Sie diese Regel, um sicherzustellen, dass die bereitgestellte Durchsatzkapazität in Ihren Amazon-DynamoDB-Tabellen überprüft wird. Dies ist der Umfang der Lese- und Schreibaktivitäten, der von den jeweiligen Tabellen unterstützt werden kann. DynamoDB verwendet diese Informationen für das Reservieren ausreichender Systemressourcen, um Ihren Durchsatz anforderungen gerecht zu werden. Diese Regel generiert eine Warnung, wenn sich der Durchsatz dem Höchstlimit für ein Kundenkonto nähert. Mit dieser Regel können Sie optional die Parameter RCUThreshold Kontoprozentsatz

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
			(Konfigurationsstandard: 80) und WCUThreshold Kontoprozentsatz (Konfigurationsstandard: 80) festlegen. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.
CCCS-fPBMM-SI-2(2)	SI-2(2) Fehlerkorrektur | Status der automatisierten Fehlerkorrektur	ec2- instance-detailed-monitoring-enabled	Aktivieren Sie diese Regel, um die Amazon Elastic Compute Cloud (Amazon EC2) - Instance-Überwachung auf der EC2 Amazon-Konsole zu verbessern, in der Monitoring-Diagramme mit einem Zeitraum von 1 Minute für die Instance angezeigt werden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-SI-2(2)	SI-2(2) Fehlerkorrektur | Status der automatisierten Fehlerkorrektur	ec2-manager instance-managed-by-systems	Eine Bestandsaufnahme der Softwareplattformen und Anwendungen innerhalb des Unternehmens ist möglich, indem Amazon Elastic Compute Cloud (Amazon EC2) - Instances mit AWS Systems Manager verwaltet werden. Verwenden Sie AWS Systems Manager, um detaillierte Systemkonfigurationen, Betriebssystem-Patch-Levels, Namen und Typ der Dienste, Softwareinstallationen, Anwendungsname, Herausgeber und Version sowie andere Details zu Ihrer Umgebung bereitzustellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-SI-2(2)	SI-2(2) Fehlerkorrektur | Status der automatisierten Fehlerkorrektur	ec2-check managedinstance-association-compliance-status	Verwenden Sie AWS Systems Manager Associations, um bei der Inventarisierung von Softwareplattformen und Anwendungen innerhalb eines Unternehmens zu helfen. AWS Systems Manager weist Ihren verwalteten Instances einen Konfigurationsstatus zu und ermöglicht es Ihnen, Basiswerte für Betriebssystem-Patch-Levels, Softwareinstallationen, Anwendungskonfigurationen und andere Details zu Ihrer Umgebung festzulegen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-SI-2(2)	SI-2(2) Fehlerkorrektur | Status der automatisierten Fehlerkorrektur	ec2-prüfen managedinstance-patch-compliance-status	Aktivieren Sie diese Regel, um bei der Identifizierung und Dokumentation von Sicherheitslücken in Amazon Elastic Compute Cloud (Amazon EC2) zu helfen. Die Regel prüft, ob die EC2 Amazon-Instance die Patch-Konformität im AWS Systems Manager gemäß den Richtlinien und Verfahren Ihrer Organisation einhält.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-SI-2(2)	SI-2(2) Fehlerkorrektur | Status der automatisierten Fehlerkorrektur	elastic-beanstalk-managed-updates-aktiviert	Durch die Aktivierung verwalteter Plattform updates für eine Amazon-Elastic-Beanstalk-Umgebung wird sichergestellt, dass die aktuellen verfügbaren Plattform -Fixes, -Updates und -Features für die Umgebung installiert sind. Eine bewährte Methode zur Sicherung von Systemen besteht darin, stets die aktuellen Patches zu installieren.
CCCS-fPBMM-SI-2(2)	SI-2(2) Fehlerkorrektur | Status der automatisierten Fehlerkorrektur	lambda-dlq-check	Aktivieren Sie diese Regel, um das entsprechende Personal über Amazon Simple Queue Service (Amazon SQS) oder Amazon Simple Notification Service (Amazon SNS) zu benachrichtigen, wenn eine Funktion ausgefallen ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-SI-2(2)	SI-2(2) Fehlerkorrektur | Status der automatisierten Fehlerkorrektur	rds-enhanced-monitoring-enabled	Aktivieren Sie Amazon Relational Database Service (Amazon RDS), um die Verfügbarkeit von Amazon RDS zu überwachen. Dies bietet einen detaillierten Einblick in den Zustand Ihrer Amazon-RDS-Datenbank-Instances. Wenn der Amazon-RDS-Speicher mehr als ein zugrunde liegendes physisches Gerät verwendet, erfasst Enhanced Monitoring die Daten für jedes Gerät. Wenn die Datenbank-Instance von Amazon RDS in einer Multi-AZ-Bereitstellung ausgeführt wird, werden außerdem die Daten für jedes Gerät auf dem sekundären Host sowie die Metriken des sekundären Hosts erfasst.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-SI-2(2)	SI-2(2) Fehlerkorrektur | Status der automatisierten Fehlerkorrektur	redshift-cluster-maintenancesettings-check	Diese Regel stellt sicher, dass Amazon-Redshift-Cluster die bevorzugten Einstellungen für Ihre Organisation haben. Insbesondere sorgt sie dafür, dass Cluster bevorzugte Wartungsfenster und automatisierte Aufbewahrungsfristen für Snapshots für die Datenbank haben. Für diese Regel müssen Sie die allowVersionUpgrade festlegen. Der Standardwert ist „true“. Außerdem können Sie optional den Zeitraum preferredMaintenanceWindow (der Standardwert ist sa: 16:00 -sa: 16:30) und den automated SnapshotRetention Zeitraum (der Standardwert ist 1) festlegen. Die tatsächlichen Werte müssen den Richtlini

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
			en Ihrer Organisation entsprechen.
CCCS-fPBMM-SI-2(3)	SI-2(3) Fehlerkorrektur | Dauer der Fehlerkorrektur/ Benchmarks für Korrekturmaßnahmen	guardduty-non-archived-findings	Amazon GuardDuty hilft Ihnen dabei, die Auswirkungen eines Vorfalls zu verstehen, indem es die Ergebnisse nach Schweregrad klassifiziert: niedrig, mittel und hoch. Diese Klassifizierungen können Sie zur Festlegung von entsprechenden Strategien und Prioritäten zur Behebung solcher Vorfälle verwenden. Mit dieser Regel können Sie optional daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7) und daysHighSev (Config Default: 1) für nicht archivierte Ergebnisse festlegen, wie es die Richtlinien Ihrer Organisation erfordern.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-SI-2.A	SI-2.A Behebung von Fehlern	autoscaling-group-elb-healthcheck-erforderlich	Die Elastic Load Balancer (ELB) - Zustandsprüfungen für Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling Scaling-Gruppen unterstützen die Aufrechterhaltung einer angemessenen Kapazität und Verfügbarkeit. Der Load Balancer sendet regelmäßig Pings, versucht Verbindungen herzustellen oder sendet Anfragen, um den Zustand der EC2 Amazon-Instances in einer Gruppe mit auto-scaling zu testen. Wenn eine Instance nicht zurückmeldet, wird der Traffic an eine neue EC2 Amazon-Instance gesendet.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-SI-2.A	SI-2.A Behebung von Fehlern	beanstalk-enhanced-health-reporting-aktiviert	AWS Die verbesserte Zustandsberichterstattung von Elastic Beanstalk ermöglicht eine schnellere Reaktion auf Veränderungen im Zustand der zugrunde liegenden Infrastruktur. Diese Änderungen könnten zu einer mangelnden Verfügbarkeit der Anwendung führen. Die erweiterten Zustandsberichte von Elastic Beanstalk bieten eine Statusbeschreibung, um den Schweregrad der identifizierten Probleme einzuschätzen und mögliche Ursachen zu identifizieren, die untersucht werden müssen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-SI-2.A	SI-2.A Behebung von Fehlern	cloudwatch-alarm-action-check	Amazon CloudWatch alarmiert, wenn eine Metrik den Schwellenwert für eine bestimmte Anzahl von Bewertungszeiträumen überschreitet. Der Alarm führt eine oder mehrere Aktionen durch, die vom Wert der Metrik oder des Ausdrucks im Vergleich zu einem Schwellenwert in einer Reihe von Zeiträumen abhängt. Diese Regel erfordert einen Wert für alarmActionRequired (Config Default: True), insufficientDataAction Required (Config Default: True), okActionRequired (Config Default: False). Der tatsächliche Wert muss die Alarmaktionen für Ihre Umgebung widerspiegeln.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-SI-2.A	SI-2.A Behebung von Fehlern	dynamodb-throughput-limit-check	Aktivieren Sie diese Regel, um sicherzustellen, dass die bereitgestellte Durchsatzkapazität in Ihren Amazon-DynamoDB-Tabellen überprüft wird. Dies ist der Umfang der Lese- und Schreibaktivitäten, der von den jeweiligen Tabellen unterstützt werden kann. DynamoDB verwendet diese Informationen für das Reservieren ausreichender Systemressourcen, um Ihren Durchsatz anforderungen gerecht zu werden. Diese Regel generiert eine Warnung, wenn sich der Durchsatz dem Höchstlimit für ein Kundenkonto nähert. Mit dieser Regel können Sie optional die Parameter RCUThreshold Kontoprozentsatz

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
			(Konfigurationsstandard: 80) und WCUThreshold Kontoprozentsatz (Konfigurationsstandard: 80) festlegen. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.
CCCS-fPBMM-SI-2.A	SI-2.A Behebung von Fehlern	ec2- instance-detailed-monitoring-enabled	Aktivieren Sie diese Regel, um die Amazon Elastic Compute Cloud (Amazon EC2) - Instance-Überwachung auf der EC2 Amazon-Konsole zu verbessern, in der Monitoring-Diagramme mit einem Zeitraum von 1 Minute für die Instance angezeigt werden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-SI-2.A	SI-2.A Behebung von Fehlern	ec2-manager instance-managed-by-systems	Eine Bestandsaufnahme der Softwareplattformen und Anwendungen innerhalb des Unternehmens ist möglich, indem Amazon Elastic Compute Cloud (Amazon EC2) - Instances mit AWS Systems Manager verwaltet werden. Verwenden Sie AWS Systems Manager, um detaillierte Systemkonfigurationen, Betriebssystem-Patch-Levels, Namen und Typ der Dienste, Softwareinstallationen, Anwendungsname, Herausgeber und Version sowie andere Details zu Ihrer Umgebung bereitzustellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-SI-2.A	SI-2.A Behebung von Fehlern	ec2-check managedinstance-association-compliance-status	Verwenden Sie AWS Systems Manager Associations, um bei der Inventarisierung von Softwareplattformen und Anwendungen innerhalb eines Unternehmens zu helfen. AWS Systems Manager weist Ihren verwalteten Instances einen Konfigurationsstatus zu und ermöglicht es Ihnen, Basiswerte für Betriebssystem-Patch-Levels, Softwareinstallationen, Anwendungskonfigurationen und andere Details zu Ihrer Umgebung festzulegen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-SI-2.A	SI-2.A Behebung von Fehlern	ec2-prüfen managedinstance-patch-compliance-status	Aktivieren Sie diese Regel, um bei der Identifizierung und Dokumentation von Sicherheitslücken in Amazon Elastic Compute Cloud (Amazon EC2) zu helfen. Die Regel prüft, ob die EC2 Amazon-Instance die Patch-Konformität im AWS Systems Manager gemäß den Richtlinien und Verfahren Ihrer Organisation einhält.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-SI-2.A	SI-2.A Behebung von Fehlern	elastic-beanstalk-managed-updates-aktiviert	Durch die Aktivierung verwalteter Plattform updates für eine Amazon-Elastic-Beanstalk-Umgebung wird sichergestellt, dass die aktuellen verfügbaren Plattform -Fixes, -Updates und -Features für die Umgebung installiert sind. Eine bewährte Methode zur Sicherung von Systemen besteht darin, stets die aktuellen Patches zu installieren.
CCCS-fPBMM-SI-2.A	SI-2.A Behebung von Fehlern	lambda-dlq-check	Aktivieren Sie diese Regel, um das entsprechende Personal über Amazon Simple Queue Service (Amazon SQS) oder Amazon Simple Notification Service (Amazon SNS) zu benachrichtigen, wenn eine Funktion ausgefallen ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-SI-2.A	SI-2.A Behebung von Fehlern	rds-enhanced-monitoring-enabled	Aktivieren Sie Amazon Relational Database Service (Amazon RDS), um die Verfügbarkeit von Amazon RDS zu überwachen. Dies bietet einen detaillierten Einblick in den Zustand Ihrer Amazon-RDS-Datenbank-Instances. Wenn der Amazon-RDS-Speicher mehr als ein zugrunde liegendes physisches Gerät verwendet, erfasst Enhanced Monitoring die Daten für jedes Gerät. Wenn die Datenbank-Instance von Amazon RDS in einer Multi-AZ-Bereitstellung ausgeführt wird, werden außerdem die Daten für jedes Gerät auf dem sekundären Host sowie die Metriken des sekundären Hosts erfasst.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-SI-2.A	SI-2.A Behebung von Fehlern	redshift-cluster-maintenancesettings-check	Diese Regel stellt sicher, dass Amazon-Redshift-Cluster die bevorzugten Einstellungen für Ihre Organisation haben. Insbesondere sorgt sie dafür, dass Cluster bevorzugte Wartungsfenster und automatisierte Aufbewahrungsfristen für Snapshots für die Datenbank haben. Für diese Regel müssen Sie die allowVersionUpgrade festlegen. Der Standardwert ist „true“. Außerdem können Sie optional den Zeitraum preferredMaintenanceWindow (der Standardwert ist sa: 16:00 -sa: 16:30) und den automated SnapshotRetention Zeitraum (der Standardwert ist 1) festlegen. Die tatsächlichen Werte müssen den Richtlini

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
			en Ihrer Organisation entsprechen.
CCCS-fPBMM-SI-2.B	SI-2.B Behebung von Fehlern	autoscaling-group-elb-healthcheck-erforderlich	Die Elastic Load Balancer (ELB) - Zustandsprüfungen für Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling Scaling-Gruppen unterstützen die Aufrechterhaltung einer angemessenen Kapazität und Verfügbarkeit. Der Load Balancer sendet regelmäßig Pings, versucht Verbindungen herzustellen oder sendet Anfragen, um den Zustand der EC2 Amazon-Instances in einer Gruppe mit auto-scaling zu testen. Wenn eine Instance nicht zurückmeldet, wird der Traffic an eine neue EC2 Amazon-Instance gesendet.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-SI-2.B	SI-2.B Behebung von Fehlern	beanstalk-enhanced-health-reporting-aktiviert	AWS Die verbesserte Zustandsberichterstattung von Elastic Beanstalk ermöglicht eine schnellere Reaktion auf Veränderungen im Zustand der zugrunde liegenden Infrastruktur. Diese Änderungen könnten zu einer mangelnden Verfügbarkeit der Anwendung führen. Die erweiterten Zustandsberichte von Elastic Beanstalk bieten eine Statusbeschreibung, um den Schweregrad der identifizierten Probleme einzuschätzen und mögliche Ursachen zu identifizieren, die untersucht werden müssen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-SI-2.B	SI-2.B Behebung von Fehlern	cloudwatch-alarm-action-check	Amazon CloudWatch alarmiert, wenn eine Metrik den Schwellenwert für eine bestimmte Anzahl von Bewertungszeiträumen überschreitet. Der Alarm führt eine oder mehrere Aktionen durch, die vom Wert der Metrik oder des Ausdrucks im Vergleich zu einem Schwellenwert in einer Reihe von Zeiträumen abhängt. Diese Regel erfordert einen Wert für alarmActionRequired (Config Default: True), insufficientDataAction Required (Config Default: True), okActionRequired (Config Default: False). Der tatsächliche Wert muss die Alarmaktionen für Ihre Umgebung widerspiegeln.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-SI-2.B	SI-2.B Behebung von Fehlern	dynamodb-throughput-limit-check	Aktivieren Sie diese Regel, um sicherzustellen, dass die bereitgestellte Durchsatzkapazität in Ihren Amazon-DynamoDB-Tabellen überprüft wird. Dies ist der Umfang der Lese- und Schreibaktivitäten, der von den jeweiligen Tabellen unterstützt werden kann. DynamoDB verwendet diese Informationen für das Reservieren ausreichender Systemressourcen, um Ihren Durchsatz anforderungen gerecht zu werden. Diese Regel generiert eine Warnung, wenn sich der Durchsatz dem Höchstlimit für ein Kundenkonto nähert. Mit dieser Regel können Sie optional die Parameter RCUThreshold Kontoprozentsatz

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
			(Konfigurationsstandard: 80) und WCUThreshold Kontoprozentsatz (Konfigurationsstandard: 80) festlegen. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.
CCCS-fPBMM-SI-2.B	SI-2.B Behebung von Fehlern	ec2- instance-detailed-monitoring-enabled	Aktivieren Sie diese Regel, um die Amazon Elastic Compute Cloud (Amazon EC2) - Instance-Überwachung auf der EC2 Amazon-Konsole zu verbessern, in der Monitoring-Diagramme mit einem Zeitraum von 1 Minute für die Instance angezeigt werden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-SI-2.B	SI-2.B Behebung von Fehlern	ec2-manager instance-managed-by-systems	Eine Bestandsaufnahme der Softwareplattformen und Anwendungen innerhalb des Unternehmens ist möglich, indem Amazon Elastic Compute Cloud (Amazon EC2) - Instances mit AWS Systems Manager verwaltet werden. Verwenden Sie AWS Systems Manager, um detaillierte Systemkonfigurationen, Betriebssystem-Patch-Levels, Namen und Typ der Dienste, Softwareinstallationen, Anwendungsname, Herausgeber und Version sowie andere Details zu Ihrer Umgebung bereitzustellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-SI-2.B	SI-2.B Behebung von Fehlern	ec2-check managedinstance-association-compliance-status	Verwenden Sie AWS Systems Manager Associations, um bei der Inventarisierung von Softwareplattformen und Anwendungen innerhalb eines Unternehmens zu helfen. AWS Systems Manager weist Ihren verwalteten Instances einen Konfigurationsstatus zu und ermöglicht es Ihnen, Basiswerte für Betriebssystem-Patch-Levels, Softwareinstallationen, Anwendungskonfigurationen und andere Details zu Ihrer Umgebung festzulegen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-SI-2.B	SI-2.B Behebung von Fehlern	ec2-prüfen managedinstance-patch-compliance-status	Aktivieren Sie diese Regel, um bei der Identifizierung und Dokumentation von Sicherheitslücken in Amazon Elastic Compute Cloud (Amazon EC2) zu helfen. Die Regel prüft, ob die EC2 Amazon-Instance die Patch-Konformität im AWS Systems Manager gemäß den Richtlinien und Verfahren Ihrer Organisation einhält.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-SI-2.B	SI-2.B Behebung von Fehlern	elastic-beanstalk-managed-updates-aktiviert	Durch die Aktivierung verwalteter Plattform updates für eine Amazon-Elastic-Beanstalk-Umgebung wird sichergestellt, dass die aktuellen verfügbaren Plattform -Fixes, -Updates und -Features für die Umgebung installiert sind. Eine bewährte Methode zur Sicherung von Systemen besteht darin, stets die aktuellen Patches zu installieren.
CCCS-fPBMM-SI-2.B	SI-2.B Behebung von Fehlern	lambda-dlq-check	Aktivieren Sie diese Regel, um das entsprechende Personal über Amazon Simple Queue Service (Amazon SQS) oder Amazon Simple Notification Service (Amazon SNS) zu benachrichtigen, wenn eine Funktion ausgefallen ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-SI-2.B	SI-2.B Behebung von Fehlern	rds-enhanced-monitoring-enabled	Aktivieren Sie Amazon Relational Database Service (Amazon RDS), um die Verfügbarkeit von Amazon RDS zu überwachen. Dies bietet einen detaillierten Einblick in den Zustand Ihrer Amazon-RDS-Datenbank-Instances. Wenn der Amazon-RDS-Speicher mehr als ein zugrunde liegendes physisches Gerät verwendet, erfasst Enhanced Monitoring die Daten für jedes Gerät. Wenn die Datenbank-Instance von Amazon RDS in einer Multi-AZ-Bereitstellung ausgeführt wird, werden außerdem die Daten für jedes Gerät auf dem sekundären Host sowie die Metriken des sekundären Hosts erfasst.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-SI-2.B	SI-2.B Behebung von Fehlern	redshift-cluster-maintenancesettings-check	Diese Regel stellt sicher, dass Amazon-Redshift-Cluster die bevorzugten Einstellungen für Ihre Organisation haben. Insbesondere sorgt sie dafür, dass Cluster bevorzugte Wartungsfenster und automatisierte Aufbewahrungsfristen für Snapshots für die Datenbank haben. Für diese Regel müssen Sie die allowVersionUpgrade festlegen. Der Standardwert ist „true“. Außerdem können Sie optional den Zeitraum preferredMaintenanceWindow (der Standardwert ist sa: 16:00 -sa: 16:30) und den automated SnapshotRetention Zeitraum (der Standardwert ist 1) festlegen. Die tatsächlichen Werte müssen den Richtlini

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
			en Ihrer Organisation entsprechen.
CCCS-fPBMM-SI-2.C	SI-2.C Behebung von Fehlern	autoscaling-group-elb-healthcheck-erforderlich	Die Elastic Load Balancer (ELB) - Zustandsprüfungen für Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling Scaling-Gruppen unterstützen die Aufrechterhaltung einer angemessenen Kapazität und Verfügbarkeit. Der Load Balancer sendet regelmäßig Pings, versucht Verbindungen herzustellen oder sendet Anfragen, um den Zustand der EC2 Amazon-Instances in einer Gruppe mit auto-scaling zu testen. Wenn eine Instance nicht zurückmeldet, wird der Traffic an eine neue EC2 Amazon-Instance gesendet.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-SI-2.C	SI-2.C Behebung von Fehlern	beanstalk-enhanced-health-reporting-aktiviert	AWS Die verbesserte Zustandsberichterstattung von Elastic Beanstalk ermöglicht eine schnellere Reaktion auf Veränderungen im Zustand der zugrunde liegenden Infrastruktur. Diese Änderungen könnten zu einer mangelnden Verfügbarkeit der Anwendung führen. Die erweiterten Zustandsberichte von Elastic Beanstalk bieten eine Statusbeschreibung, um den Schweregrad der identifizierten Probleme einzuschätzen und mögliche Ursachen zu identifizieren, die untersucht werden müssen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-SI-2.C	SI-2.C Behebung von Fehlern	cloudwatch-alarm-action-check	Amazon CloudWatch alarmiert, wenn eine Metrik den Schwellenwert für eine bestimmte Anzahl von Bewertungszeiträumen überschreitet. Der Alarm führt eine oder mehrere Aktionen durch, die vom Wert der Metrik oder des Ausdrucks im Vergleich zu einem Schwellenwert in einer Reihe von Zeiträumen abhängt. Diese Regel erfordert einen Wert für alarmActionRequired (Config Default: True), insufficientDataAction Required (Config Default: True), okActionRequired (Config Default: False). Der tatsächliche Wert muss die Alarmaktionen für Ihre Umgebung widerspiegeln.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-SI-2.C	SI-2.C Behebung von Fehlern	dynamodb-throughput-limit-check	Aktivieren Sie diese Regel, um sicherzustellen, dass die bereitgestellte Durchsatzkapazität in Ihren Amazon-DynamoDB-Tabellen überprüft wird. Dies ist der Umfang der Lese- und Schreibaktivitäten, der von den jeweiligen Tabellen unterstützt werden kann. DynamoDB verwendet diese Informationen für das Reservieren ausreichender Systemressourcen, um Ihren Durchsatz anforderungen gerecht zu werden. Diese Regel generiert eine Warnung, wenn sich der Durchsatz dem Höchstlimit für ein Kundenkonto nähert. Mit dieser Regel können Sie optional die Parameter RCUThreshold Kontoprozentsatz

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
			(Konfigurationsstandard: 80) und WCUThreshold Kontoprozentsatz (Konfigurationsstandard: 80) festlegen. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.
CCCS-fPBMM-SI-2.C	SI-2.C Behebung von Fehlern	ec2- instance-detailed-monitoring-enabled	Aktivieren Sie diese Regel, um die Amazon Elastic Compute Cloud (Amazon EC2) - Instance-Überwachung auf der EC2 Amazon-Konsole zu verbessern, in der Monitoring-Diagramme mit einem Zeitraum von 1 Minute für die Instance angezeigt werden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-SI-2.C	SI-2.C Behebung von Fehlern	ec2-manager instance-managed-by-systems	Eine Bestandsaufnahme der Softwareplattformen und Anwendungen innerhalb des Unternehmens ist möglich, indem Amazon Elastic Compute Cloud (Amazon EC2) - Instances mit AWS Systems Manager verwaltet werden. Verwenden Sie AWS Systems Manager, um detaillierte Systemkonfigurationen, Betriebssystem-Patch-Levels, Namen und Typ der Dienste, Softwareinstallationen, Anwendungsname, Herausgeber und Version sowie andere Details zu Ihrer Umgebung bereitzustellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-SI-2.C	SI-2.C Behebung von Fehlern	ec2-check managedinstance-association-compliance-status	Verwenden Sie AWS Systems Manager Associations, um bei der Inventarisierung von Softwareplattformen und Anwendungen innerhalb eines Unternehmens zu helfen. AWS Systems Manager weist Ihren verwalteten Instances einen Konfigurationsstatus zu und ermöglicht es Ihnen, Basiswerte für Betriebssystem-Patch-Levels, Softwareinstallationen, Anwendungskonfigurationen und andere Details zu Ihrer Umgebung festzulegen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-SI-2.C	SI-2.C Behebung von Fehlern	ec2-prüfen managedinstance-patch-compliance-status	Aktivieren Sie diese Regel, um bei der Identifizierung und Dokumentation von Sicherheitslücken in Amazon Elastic Compute Cloud (Amazon EC2) zu helfen. Die Regel prüft, ob die EC2 Amazon-Instance die Patch-Konformität im AWS Systems Manager gemäß den Richtlinien und Verfahren Ihrer Organisation einhält.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-SI-2.C	SI-2.C Behebung von Fehlern	elastic-beanstalk-managed-updates-aktiviert	Durch die Aktivierung verwalteter Plattform updates für eine Amazon-Elastic-Beanstalk-Umgebung wird sichergestellt, dass die aktuellen verfügbaren Plattform -Fixes, -Updates und -Features für die Umgebung installiert sind. Eine bewährte Methode zur Sicherung von Systemen besteht darin, stets die aktuellen Patches zu installieren.
CCCS-fPBMM-SI-2.C	SI-2.C Behebung von Fehlern	lambda-dlq-check	Aktivieren Sie diese Regel, um das entsprechende Personal über Amazon Simple Queue Service (Amazon SQS) oder Amazon Simple Notification Service (Amazon SNS) zu benachrichtigen, wenn eine Funktion ausgefallen ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-SI-2.C	SI-2.C Behebung von Fehlern	rds-enhanced-monitoring-enabled	Aktivieren Sie Amazon Relational Database Service (Amazon RDS), um die Verfügbarkeit von Amazon RDS zu überwachen. Dies bietet einen detaillierten Einblick in den Zustand Ihrer Amazon-RDS-Datenbank-Instances. Wenn der Amazon-RDS-Speicher mehr als ein zugrunde liegendes physisches Gerät verwendet, erfasst Enhanced Monitoring die Daten für jedes Gerät. Wenn die Datenbank-Instance von Amazon RDS in einer Multi-AZ-Bereitstellung ausgeführt wird, werden außerdem die Daten für jedes Gerät auf dem sekundären Host sowie die Metriken des sekundären Hosts erfasst.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-SI-2.C	SI-2.C Behebung von Fehlern	redshift-cluster-maintenancesettings-check	Diese Regel stellt sicher, dass Amazon-Redshift-Cluster die bevorzugten Einstellungen für Ihre Organisation haben. Insbesondere sorgt sie dafür, dass Cluster bevorzugte Wartungsfenster und automatisierte Aufbewahrungsfristen für Snapshots für die Datenbank haben. Für diese Regel müssen Sie die allowVersionUpgrade festlegen. Der Standardwert ist „true“. Außerdem können Sie optional den Zeitraum preferredMaintenanceWindow (der Standardwert ist sa: 16:00 -sa: 16:30) und den automated SnapshotRetention Zeitraum (der Standardwert ist 1) festlegen. Die tatsächlichen Werte müssen den Richtlini

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
			en Ihrer Organisation entsprechen.
CCCS-fPBMM-SI-2.D	SI-2.D Behebung von Fehlern	autoscaling-group-elb-healthcheck-erforderlich	Die Elastic Load Balancer (ELB) - Zustandsprüfungen für Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling Scaling-Gruppen unterstützen die Aufrechterhaltung einer angemessenen Kapazität und Verfügbarkeit. Der Load Balancer sendet regelmäßig Pings, versucht Verbindungen herzustellen oder sendet Anfragen, um den Zustand der EC2 Amazon-Instances in einer Gruppe mit auto-scaling zu testen. Wenn eine Instance nicht zurückmeldet, wird der Traffic an eine neue EC2 Amazon-Instance gesendet.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-SI-2.D	SI-2.D Behebung von Fehlern	beanstalk-enhanced-health-reporting-aktiviert	AWS Die verbesserte Zustandsberichterstattung von Elastic Beanstalk ermöglicht eine schnellere Reaktion auf Veränderungen im Zustand der zugrunde liegenden Infrastruktur. Diese Änderungen könnten zu einer mangelnden Verfügbarkeit der Anwendung führen. Die erweiterten Zustandsberichte von Elastic Beanstalk bieten eine Statusbeschreibung, um den Schweregrad der identifizierten Probleme einzuschätzen und mögliche Ursachen zu identifizieren, die untersucht werden müssen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-SI-2.D	SI-2.D Behebung von Fehlern	cloudwatch-alarm-action-check	Amazon CloudWatch alarmiert, wenn eine Metrik den Schwellenwert für eine bestimmte Anzahl von Bewertungszeiträumen überschreitet. Der Alarm führt eine oder mehrere Aktionen durch, die vom Wert der Metrik oder des Ausdrucks im Vergleich zu einem Schwellenwert in einer Reihe von Zeiträumen abhängt. Diese Regel erfordert einen Wert für alarmActionRequired (Config Default: True), insufficientDataAction Required (Config Default: True), okActionRequired (Config Default: False). Der tatsächliche Wert muss die Alarmaktionen für Ihre Umgebung widerspiegeln.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-SI-2.D	SI-2.D Behebung von Fehlern	dynamodb-throughput-limit-check	Aktivieren Sie diese Regel, um sicherzustellen, dass die bereitgestellte Durchsatzkapazität in Ihren Amazon-DynamoDB-Tabellen überprüft wird. Dies ist der Umfang der Lese- und Schreibaktivitäten, der von den jeweiligen Tabellen unterstützt werden kann. DynamoDB verwendet diese Informationen für das Reservieren ausreichender Systemressourcen, um Ihren Durchsatz anforderungen gerecht zu werden. Diese Regel generiert eine Warnung, wenn sich der Durchsatz dem Höchstlimit für ein Kundenkonto nähert. Mit dieser Regel können Sie optional die Parameter RCUThreshold Kontoprozentsatz

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
			(Konfigurationsstandard: 80) und WCUThreshold Kontoprozentsatz (Konfigurationsstandard: 80) festlegen. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.
CCCS-fPBMM-SI-2.D	SI-2.D Behebung von Fehlern	ec2- instance-detailed-monitoring-enabled	Aktivieren Sie diese Regel, um die Amazon Elastic Compute Cloud (Amazon EC2) - Instance-Überwachung auf der EC2 Amazon-Konsole zu verbessern, in der Monitoring-Diagramme mit einem Zeitraum von 1 Minute für die Instance angezeigt werden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-SI-2.D	SI-2.D Behebung von Fehlern	ec2-manager instance-managed-by-systems	Eine Bestandsaufnahme der Softwareplattformen und Anwendungen innerhalb des Unternehmens ist möglich, indem Amazon Elastic Compute Cloud (Amazon EC2) - Instances mit AWS Systems Manager verwaltet werden. Verwenden Sie AWS Systems Manager, um detaillierte Systemkonfigurationen, Betriebssystem-Patch-Levels, Namen und Typ der Dienste, Softwareinstallationen, Anwendungsname, Herausgeber und Version sowie andere Details zu Ihrer Umgebung bereitzustellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-SI-2.D	SI-2.D Behebung von Fehlern	ec2-check managedinstance-association-compliance-status	Verwenden Sie AWS Systems Manager Associations, um bei der Inventarisierung von Softwareplattformen und Anwendungen innerhalb eines Unternehmens zu helfen. AWS Systems Manager weist Ihren verwalteten Instances einen Konfigurationsstatus zu und ermöglicht es Ihnen, Basiswerte für Betriebssystem-Patch-Levels, Softwareinstallationen, Anwendungskonfigurationen und andere Details zu Ihrer Umgebung festzulegen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-SI-2.D	SI-2.D Behebung von Fehlern	ec2-prüfen managedinstance-patch-compliance-status	Aktivieren Sie diese Regel, um bei der Identifizierung und Dokumentation von Sicherheitslücken in Amazon Elastic Compute Cloud (Amazon EC2) zu helfen. Die Regel prüft, ob die EC2 Amazon-Instance die Patch-Konformität im AWS Systems Manager gemäß den Richtlinien und Verfahren Ihrer Organisation einhält.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-SI-2.D	SI-2.D Behebung von Fehlern	elastic-beanstalk-managed-updates-aktiviert	Durch die Aktivierung verwalteter Plattform updates für eine Amazon-Elastic-Beanstalk-Umgebung wird sichergestellt, dass die aktuellen verfügbaren Plattform -Fixes, -Updates und -Features für die Umgebung installiert sind. Eine bewährte Methode zur Sicherung von Systemen besteht darin, stets die aktuellen Patches zu installieren.
CCCS-fPBMM-SI-2.D	SI-2.D Behebung von Fehlern	lambda-dlq-check	Aktivieren Sie diese Regel, um das entsprechende Personal über Amazon Simple Queue Service (Amazon SQS) oder Amazon Simple Notification Service (Amazon SNS) zu benachrichtigen, wenn eine Funktion ausgefallen ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-SI-2.D	SI-2.D Behebung von Fehlern	rds-enhanced-monitoring-enabled	Aktivieren Sie Amazon Relational Database Service (Amazon RDS), um die Verfügbarkeit von Amazon RDS zu überwachen. Dies bietet einen detaillierten Einblick in den Zustand Ihrer Amazon-RDS-Datenbank-Instances. Wenn der Amazon-RDS-Speicher mehr als ein zugrunde liegendes physisches Gerät verwendet, erfasst Enhanced Monitoring die Daten für jedes Gerät. Wenn die Datenbank-Instance von Amazon RDS in einer Multi-AZ-Bereitstellung ausgeführt wird, werden außerdem die Daten für jedes Gerät auf dem sekundären Host sowie die Metriken des sekundären Hosts erfasst.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-SI-2.D	SI-2.D Behebung von Fehlern	redshift-cluster-maintenancesettings-check	Diese Regel stellt sicher, dass Amazon-Redshift-Cluster die bevorzugten Einstellungen für Ihre Organisation haben. Insbesondere sorgt sie dafür, dass Cluster bevorzugte Wartungsfenster und automatisierte Aufbewahrungsfristen für Snapshots für die Datenbank haben. Für diese Regel müssen Sie die allowVersionUpgrade festlegen. Der Standardwert ist „true“. Außerdem können Sie optional den Zeitraum preferredMaintenanceWindow (der Standardwert ist sa: 16:00 -sa: 16:30) und den automated SnapshotRetention Zeitraum (der Standardwert ist 1) festlegen. Die tatsächlichen Werte müssen den Richtlini

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
			en Ihrer Organisation entsprechen.
CCCS-fPBMM-SI-3(1)	SI-3(1) Schutz vor bösartigem Code | Zentrale Verwaltung	guardduty-enabled-centralized	Amazon GuardDuty kann mithilfe von Threat Intellige nce Feeds helfen, potenzielle Cybersich erheitsereignisse zu überwachen und zu erkennen. Dazu gehören Listen mit bösartigen IPs und maschinel len Lernmethoden zur Identifizierung unerwarteter, nicht autorisierter und bösartiger Aktivitäten in Ihrer AWS Cloud-Umgebung.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-SI-3(7)	SI-3(7) Schutz vor bösartigem Code | Erkennung ohne Signatur	guardduty-enabled-centralized	Amazon GuardDuty kann mithilfe von Threat Intellige nce Feeds helfen, potenzielle Cybersich erheitsereignisse zu überwachen und zu erkennen. Dazu gehören Listen mit bösartigen IPs und maschinel len Lernmethoden zur Identifizierung unerwarteter, nicht autorisierter und bösartiger Aktivitäten in Ihrer AWS Cloud-Umgebung.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-SI-3.A	SI-3.A Schutz vor bösartigem Code	alb-waf-enabled	Stellen Sie sicher, dass AWS WAF auf Elastic Load Balancers (ELB) aktiviert ist, um Webanwendungen zu schützen. Eine WAF trägt zum Schutz Ihrer Webanwend ungen oder APIs vor gängigen Web-Explo its bei. Diese Web-Exploits können sich auf die Verfügbar keit auswirken, die Sicherheit gefährden oder übermäßige Ressourcen in Ihrer Umgebung verbrauch en.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-SI-3.A	SI-3.A Schutz vor bösartigem Code	ec2-manager instance-managed-by-systems	Eine Bestandsaufnahme der Softwareplattformen und Anwendungen innerhalb des Unternehmens ist möglich, indem Amazon Elastic Compute Cloud (Amazon EC2) - Instances mit AWS Systems Manager verwaltet werden. Verwenden Sie AWS Systems Manager, um detaillierte Systemkonfigurationen, Betriebssystem-Patch-Levels, Namen und Typ der Dienste, Softwareinstallationen, Anwendungsname, Herausgeber und Version sowie andere Details zu Ihrer Umgebung bereitzustellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-SI-3.A	SI-3.A Schutz vor bösartigem Code	ec2-check managedinstance-association-compliance-status	Verwenden Sie AWS Systems Manager Associations, um bei der Inventarisierung von Softwareplattformen und Anwendungen innerhalb eines Unternehmens zu helfen. AWS Systems Manager weist Ihren verwalteten Instances einen Konfigurationsstatus zu und ermöglicht es Ihnen, Basiswerte für Betriebssystem-Patch-Levels, Softwareinstallationen, Anwendungskonfigurationen und andere Details zu Ihrer Umgebung festzulegen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-SI-3.A	SI-3.A Schutz vor bösartigem Code	ec2-prüfen managedinstance-patch-compliance-status	Aktivieren Sie diese Regel, um bei der Identifizierung und Dokumentation von Sicherheitslücken in Amazon Elastic Compute Cloud (Amazon EC2) zu helfen. Die Regel prüft, ob die EC2 Amazon-Instance die Patch-Konformität im AWS Systems Manager gemäß den Richtlinien und Verfahren Ihrer Organisation einhält.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-SI-3.A	SI-3.A Schutz vor bösartigem Code	guardduty-enabled-centralized	Amazon GuardDuty kann mithilfe von Threat Intellige nce Feeds helfen, potenzielle Cybersich erheitsereignisse zu überwachen und zu erkennen. Dazu gehören Listen mit bösartigen IPs und maschinel len Lernmethoden zur Identifizierung unerwarteter, nicht autorisierter und bösartiger Aktivitäten in Ihrer AWS Cloud-Umgebung.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-SI-3.B	SI-3.B Schutz vor bösartigem Code	ec2-manager instance-managed-by-systems	Eine Bestandsaufnahme der Softwareplattformen und Anwendungen innerhalb des Unternehmens ist möglich, indem Amazon Elastic Compute Cloud (Amazon EC2) - Instances mit AWS Systems Manager verwaltet werden. Verwenden Sie AWS Systems Manager, um detaillierte Systemkonfigurationen, Betriebssystem-Patch-Levels, Namen und Typ der Dienste, Softwareinstallationen, Anwendungsname, Herausgeber und Version sowie andere Details zu Ihrer Umgebung bereitzustellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-SI-3.B	SI-3.B Schutz vor bösartigem Code	ec2-check managedinstance-association-compliance-status	Verwenden Sie AWS Systems Manager Associations, um bei der Inventarisierung von Softwareplattformen und Anwendungen innerhalb eines Unternehmens zu helfen. AWS Systems Manager weist Ihren verwalteten Instances einen Konfigurationsstatus zu und ermöglicht es Ihnen, Basiswerte für Betriebssystem-Patch-Levels, Softwareinstallationen, Anwendungskonfigurationen und andere Details zu Ihrer Umgebung festzulegen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-SI-3.B	SI-3.B Schutz vor bösartigem Code	ec2-prüfen managedinstance-patch-compliance-status	Aktivieren Sie diese Regel, um bei der Identifizierung und Dokumentation von Sicherheitslücken in Amazon Elastic Compute Cloud (Amazon EC2) zu helfen. Die Regel prüft, ob die EC2 Amazon-Instance die Patch-Konformität im AWS Systems Manager gemäß den Richtlinien und Verfahren Ihrer Organisation einhält.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-SI-3.B	SI-3.B Schutz vor bösartigem Code	guardduty-enabled-centralized	Amazon GuardDuty kann mithilfe von Threat Intellige nce Feeds helfen, potenzielle Cybersich erheitsereignisse zu überwachen und zu erkennen. Dazu gehören Listen mit bösartigen IPs und maschinel len Lernmethoden zur Identifizierung unerwarteter, nicht autorisierter und bösartiger Aktivitäten in Ihrer AWS Cloud-Umgebung.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-SI-3.C	SI-3.C Schutz vor bösartigem Code	ec2-manager instance-managed-by-systems	Eine Bestandsaufnahme der Softwareplattformen und Anwendungen innerhalb des Unternehmens ist möglich, indem Amazon Elastic Compute Cloud (Amazon EC2) - Instances mit AWS Systems Manager verwaltet werden. Verwenden Sie AWS Systems Manager, um detaillierte Systemkonfigurationen, Betriebssystem-Patch-Levels, Namen und Typ der Dienste, Softwareinstallationen, Anwendungsname, Herausgeber und Version sowie andere Details zu Ihrer Umgebung bereitzustellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-SI-3.C	SI-3.C Schutz vor bösartigem Code	ec2-check managedinstance-association-compliance-status	Verwenden Sie AWS Systems Manager Associations, um bei der Inventarisierung von Softwareplattformen und Anwendungen innerhalb eines Unternehmens zu helfen. AWS Systems Manager weist Ihren verwalteten Instances einen Konfigurationsstatus zu und ermöglicht es Ihnen, Basiswerte für Betriebssystem-Patch-Levels, Softwareinstallationen, Anwendungskonfigurationen und andere Details zu Ihrer Umgebung festzulegen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-SI-3.C	SI-3.C Schutz vor bösartigem Code	ec2-prüfen managedinstance-patch-compliance-status	Aktivieren Sie diese Regel, um bei der Identifizierung und Dokumentation von Sicherheitslücken in Amazon Elastic Compute Cloud (Amazon EC2) zu helfen. Die Regel prüft, ob die EC2 Amazon-Instance die Patch-Konformität im AWS Systems Manager gemäß den Richtlinien und Verfahren Ihrer Organisation einhält.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-SI-3.C	SI-3.C Schutz vor bösartigem Code	guardduty-enabled-centralized	Amazon GuardDuty kann mithilfe von Threat Intellige nce Feeds helfen, potenzielle Cybersich erheitsereignisse zu überwachen und zu erkennen. Dazu gehören Listen mit bösartigen IPs und maschinel len Lernmethoden zur Identifizierung unerwarteter, nicht autorisierter und bösartiger Aktivitäten in Ihrer AWS Cloud-Umgebung.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-SI-3.D	SI-3.D Schutz vor bösartigem Code	ec2-manager instance-managed-by-systems	Eine Bestandsaufnahme der Softwareplattformen und Anwendungen innerhalb des Unternehmens ist möglich, indem Amazon Elastic Compute Cloud (Amazon EC2) - Instances mit AWS Systems Manager verwaltet werden. Verwenden Sie AWS Systems Manager, um detaillierte Systemkonfigurationen, Betriebssystem-Patch-Levels, Namen und Typ der Dienste, Softwareinstallationen, Anwendungsname, Herausgeber und Version sowie andere Details zu Ihrer Umgebung bereitzustellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-SI-3.D	SI-3.D Schutz vor bösartigem Code	ec2-check managedinstance-association-compliance-status	Verwenden Sie AWS Systems Manager Associations, um bei der Inventarisierung von Softwareplattformen und Anwendungen innerhalb eines Unternehmens zu helfen. AWS Systems Manager weist Ihren verwalteten Instances einen Konfigurationsstatus zu und ermöglicht es Ihnen, Basiswerte für Betriebssystem-Patch-Levels, Softwareinstallationen, Anwendungskonfigurationen und andere Details zu Ihrer Umgebung festzulegen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-SI-3.D	SI-3.D Schutz vor bösartigem Code	ec2-prüfen managedinstance-patch-compliance-status	Aktivieren Sie diese Regel, um bei der Identifizierung und Dokumentation von Sicherheitslücken in Amazon Elastic Compute Cloud (Amazon EC2) zu helfen. Die Regel prüft, ob die EC2 Amazon-Instance die Patch-Konformität im AWS Systems Manager gemäß den Richtlinien und Verfahren Ihrer Organisation einhält.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-SI-3.D	SI-3.D Schutz vor bösartigem Code	guardduty-enabled-centralized	Amazon GuardDuty kann mithilfe von Threat Intellige nce Feeds helfen, potenzielle Cybersich erheitsereignisse zu überwachen und zu erkennen. Dazu gehören Listen mit bösartigen IPs und maschinel len Lernmethoden zur Identifizierung unerwarteter, nicht autorisierter und bösartiger Aktivitäten in Ihrer AWS Cloud-Umgebung.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-SI-4(1)	SI-4(1) Überwachung des Informationssystems | Systemweites Angriffsmeldesystem	guardduty-enabled-centralized	Amazon GuardDuty kann mithilfe von Threat Intelligence Feeds helfen, potenzielle Cybersicherheitsereignisse zu überwachen und zu erkennen. Dazu gehören Listen mit bösartigen IPs und maschinellen Lernmethoden zur Identifizierung unerwarteter, nicht autorisierter und bösartiger Aktivitäten in Ihrer AWS Cloud-Umgebung.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-SI-4(1)	SI-4(1) Überwachung des Informationssystems | Systemweites Angriffsmeldesystem	securityhub-enabled	AWS Security Hub hilft bei der Überwachung von unbefugtem Personal, Verbindungen, Geräten und Software. AWS Security Hub aggregiert, organisiert und priorisiert die Sicherheitswarnungen oder Ergebnisse mehrerer Dienste. AWS Einige dieser Dienste sind Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer und AWS Firewall Manager sowie AWS Partnerlösungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-SI-4(2)	SI-4(2) Überwachung des Informationssystems | Automatisierte Tools für Echtzeitanalysen	guardduty-enabled-centralized	Amazon GuardDuty kann mithilfe von Threat Intelligence Feeds helfen, potenzielle Cybersicherheitsereignisse zu überwachen und zu erkennen. Dazu gehören Listen mit bösartigen IPs und maschinellen Lernmethoden zur Identifizierung unerwarteter, nicht autorisierter und bösartiger Aktivitäten in Ihrer AWS Cloud-Umgebung.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-SI-4(2)	SI-4(2) Überwachung des Informationssystems | Automatisierte Tools für Echtzeitanalysen	securityhub-enabled	AWS Security Hub hilft bei der Überwachung von unbefugtem Personal, Verbindungen, Geräten und Software. AWS Security Hub aggregiert, organisiert und priorisiert die Sicherheitswarnungen oder Ergebnisse mehrerer Dienste. AWS Einige dieser Dienste sind Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer und AWS Firewall Manager sowie AWS Partnerlösungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-SI-4(4)	SI-4(4) Überwachung des Informationssystems | Eingehender und ausgehender Kommunikationsverkehr	guardduty-enabled-centralized	Amazon GuardDuty kann mithilfe von Threat Intelligence Feeds helfen, potenzielle Cybersicherheitsereignisse zu überwachen und zu erkennen. Dazu gehören Listen mit bösartigen IPs und maschinellen Lernmethoden zur Identifizierung unerwarteter, nicht autorisierter und bösartiger Aktivitäten in Ihrer AWS Cloud-Umgebung.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-SI-4(4)	SI-4(4) Überwachung des Informationssystems | Eingehender und ausgehender Kommunikationsverkehr	vpc-flow-logs-enabled	VPC-Flow-Protokolle erfassen detaillierte Informationsdatensätze über den IP-Datenverkehr, der zu und von Netzwerkschnittstellen in Ihrer Amazon Virtual Private Cloud (Amazon VPC) fließt. Standardmäßig enthalten Flow-Protokolldatensätze Werte für die verschiedenen Komponenten des IP-Flows, einschließlich Quelle, Ziel und Protokoll.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-SI-4(5)	SI-4(5) Überwachung des Informationssystems | Vom System generierte Warnmeldungen	cloudwatch-alarm-action-check	Amazon CloudWatch alarmiert, wenn eine Metrik den Schwellenwert für eine bestimmte Anzahl von Bewertungszeiträumen überschreitet. Der Alarm führt eine oder mehrere Aktionen durch, die vom Wert der Metrik oder des Ausdrucks im Vergleich zu einem Schwellenwert in einer Reihe von Zeiträumen abhängt. Diese Regel erfordert einen Wert für alarmActionRequired (Config Default: True), insufficientDataAction Required (Config Default: True), okActionRequired (Config Default: False). Der tatsächliche Wert muss die Alarmaktionen für Ihre Umgebung widerspiegeln.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-SI-4(11)	SI-4(11) Überwachung des Informationssystems | Analyse von Anomalien des Kommunikationsverkehrs	guardduty-enabled-centralized	Amazon GuardDuty kann mithilfe von Threat Intelligence Feeds helfen, potenzielle Cybersicherheitsereignisse zu überwachen und zu erkennen. Dazu gehören Listen mit bösartigen IPs und maschinellen Lernmethoden zur Identifizierung unerwarteter, nicht autorisierter und bösartiger Aktivitäten in Ihrer AWS Cloud-Umgebung.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-SI-4(11)	SI-4(11) Überwachung des Informationssystems | Analyse von Anomalien des Kommunikationsverkehrs	securityhub-enabled	AWS Security Hub hilft bei der Überwachung von unbefugtem Personal, Verbindungen, Geräten und Software. AWS Security Hub aggregiert, organisiert und priorisiert die Sicherheitswarnungen oder Ergebnisse mehrerer Dienste. AWS Einige dieser Dienste sind Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer und AWS Firewall Manager sowie AWS Partnerlösungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-SI-4(16)	SI-4(16) Überwachung des Informationssystems | Korrelieren von Überwachungsinformationen	guardduty-enabled-centralized	Amazon GuardDuty kann mithilfe von Threat Intelligence Feeds helfen, potenzielle Cybersicherheitsereignisse zu überwachen und zu erkennen. Dazu gehören Listen mit bösartigen IPs und maschinellen Lernmethoden zur Identifizierung unerwarteter, nicht autorisierter und bösartiger Aktivitäten in Ihrer AWS Cloud-Umgebung.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-SI-4(16)	SI-4(16) Überwachung des Informationssystems | Korrelieren von Überwachungsinformationen	securityhub-enabled	AWS Security Hub hilft bei der Überwachung von unbefugtem Personal, Verbindungen, Geräten und Software. AWS Security Hub aggregiert, organisiert und priorisiert die Sicherheitswarnungen oder Ergebnisse mehrerer Dienste. AWS Einige dieser Dienste sind Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer und AWS Firewall Manager sowie AWS Partnerlösungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-SI-4(20)	SI-4(20) Überwachung des Informationssystems | Privilegierter Benutzer	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) kann Ihnen dabei helfen, die Prinzipien der geringsten Rechte und der Aufgabentrennung in Zugriffsberechtigungen und Autorisierungen zu integrieren und so zu verhindern, dass Richtlinien „Effect“: „Allow“ mit „Action“: „*“ anstelle von „Resource“: „*“ enthalten. Wenn Benutzern mehr Rechte eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und der Aufgabentrennung verstoßen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-SI-4(23)	SI-4(23) Überwachung des Informationssystems | Host-basierte Geräte	cloudtrail-enabled	AWS CloudTrail kann durch die Aufzeichnung AWS von Aktionen und API-Aufrufen der Management Console bei der Nichtabstreitbarkeit helfen. Sie können die Benutzer und die Benutzer AWS-Konten , die einen AWS Dienst aufgerufen haben, die Quell-IP-Adresse, über die die Aufrufe generiert wurden, und den Zeitpunkt der Anrufe identifizieren. Einzelheiten zu den erfassten Daten finden Sie unter Inhalt des AWS CloudTrail Datensatzes.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-SI-4(23)	SI-4(23) Überwachung des Informationssystems | Host-basierte Geräte	multi-region-cloudtrail-enabled	AWS CloudTrail zeichnet Aktionen und API-Aufrufe der AWS Management Console auf. Sie können feststellen, welche Benutzer und Konten angerufen wurden AWS, von welcher Quell-IP-Adresse aus die Anrufe getätigt wurden und wann die Anrufe erfolgten. CloudTrail übermittelt Protokolldateien aus allen AWS Regionen an Ihren S3-Bucket, wenn MULTI_REGION_CLOUD_TRAIL_ENABLED aktiviert ist. Außerdem wird beim AWS Start einer neuen Region derselbe Trail in der neuen Region erstellt. CloudTrail Dadurch erhalten Sie automatisch Protokolldateien mit API-Aktivitäten für die neue Region.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-SI-4.A	SI-4.A Überwachung des Informationssystems	cloudwatch-alarm-action-check	Amazon CloudWatch alarmiert, wenn eine Metrik den Schwellenwert für eine bestimmte Anzahl von Bewertungszeiträumen überschreitet. Der Alarm führt eine oder mehrere Aktionen durch, die vom Wert der Metrik oder des Ausdrucks im Vergleich zu einem Schwellenwert in einer Reihe von Zeiträumen abhängt. Diese Regel erfordert einen Wert für alarmActionRequired (Config Default: True), insufficientDataAction Required (Config Default: True), okActionRequired (Config Default: False). Der tatsächliche Wert muss die Alarmaktionen für Ihre Umgebung widerspiegeln.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-SI-4.A	SI-4.A Überwachung des Informationssystems	cloud-trail-log-file-validierung aktiviert	Verwenden Sie die AWS CloudTrail Protokolldateivalidierung, um die Integrität von Protokollen zu überprüfen. CloudTrail Mithilfe der Protokolldateivalidierung kann festgestellt werden, ob eine Protokolldatei geändert oder gelöscht wurde oder ob sie nach der Übermittlung CloudTrail unverändert geblieben ist. Dieses Feature wurde mit dem Branchenstandard entsprechenden Algorithmen entwickelt: SHA-256 für die Hashfunktion und SHA-256 mit RSA für digitale Signaturen. Aus diesem Grund ist es rechnerisch unmöglich, CloudTrail Protokolldateien unbemerkt zu ändern, zu löschen oder zu fälschen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-SI-4.A	SI-4.A Überwachung des Informationssystems	guardduty-enabled-centralized	Amazon GuardDuty kann mithilfe von Threat Intelligence Feeds helfen, potenzielle Cybersicherheitsereignisse zu überwachen und zu erkennen. Dazu gehören Listen mit bösartigen IPs und maschinellen Lernmethoden zur Identifizierung unerwarteter, nicht autorisierter und bösartiger Aktivitäten in Ihrer AWS Cloud-Umgebung.
CCCS-fPBMM-SI-4.A	SI-4.A Überwachung des Informationssystems	lambda-dlq-check	Aktivieren Sie diese Regel, um das entsprechende Personal über Amazon Simple Queue Service (Amazon SQS) oder Amazon Simple Notification Service (Amazon SNS) zu benachrichtigen, wenn eine Funktion ausgefallen ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-SI-4.A	SI-4.A Überwachung des Informationssystems	securityhub-enabled	AWS Security Hub hilft bei der Überwachung von unbefugtem Personal, Verbindungen, Geräten und Software. AWS Security Hub aggregiert, organisiert und priorisiert die Sicherheitswarnungen oder Ergebnisse mehrerer Dienste. AWS Einige dieser Dienste sind Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer und AWS Firewall Manager sowie AWS Partnerlösungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-SI-4.B	SI-4.B Überwachung des Informationssystems	cloudwatch-alarm-action-check	Amazon CloudWatch alarmiert, wenn eine Metrik den Schwellenwert für eine bestimmte Anzahl von Bewertungszeiträumen überschreitet. Der Alarm führt eine oder mehrere Aktionen durch, die vom Wert der Metrik oder des Ausdrucks im Vergleich zu einem Schwellenwert in einer Reihe von Zeiträumen abhängt. Diese Regel erfordert einen Wert für alarmActionRequired (Config Default: True), insufficientDataAction Required (Config Default: True), okActionRequired (Config Default: False). Der tatsächliche Wert muss die Alarmaktionen für Ihre Umgebung widerspiegeln.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-SI-4.B	SI-4.B Überwachung des Informationssystems	cloud-trail-log-file-validierung aktiviert	Verwenden Sie die AWS CloudTrail Protokolldateivalidierung, um die Integrität von Protokollen zu überprüfen. CloudTrail Mithilfe der Protokolldateivalidierung kann festgestellt werden, ob eine Protokolldatei geändert oder gelöscht wurde oder ob sie nach der Übermittlung CloudTrail unverändert geblieben ist. Dieses Feature wurde mit dem Branchenstandard entsprechenden Algorithmen entwickelt: SHA-256 für die Hashfunktion und SHA-256 mit RSA für digitale Signaturen. Aus diesem Grund ist es rechnerisch unmöglich, CloudTrail Protokolldateien unbemerkt zu ändern, zu löschen oder zu fälschen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-SI-4.B	SI-4.B Überwachung des Informationssystems	guardduty-enabled-centralized	Amazon GuardDuty kann mithilfe von Threat Intelligence Feeds helfen, potenzielle Cybersicherheitsereignisse zu überwachen und zu erkennen. Dazu gehören Listen mit bösartigen IPs und maschinellen Lernmethoden zur Identifizierung unerwarteter, nicht autorisierter und bösartiger Aktivitäten in Ihrer AWS Cloud-Umgebung.
CCCS-fPBMM-SI-4.B	SI-4.B Überwachung des Informationssystems	lambda-dlq-check	Aktivieren Sie diese Regel, um das entsprechende Personal über Amazon Simple Queue Service (Amazon SQS) oder Amazon Simple Notification Service (Amazon SNS) zu benachrichtigen, wenn eine Funktion ausgefallen ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-SI-4.B	SI-4.B Überwachung des Informationssystems	securityhub-enabled	AWS Security Hub hilft bei der Überwachung von unbefugtem Personal, Verbindungen, Geräten und Software. AWS Security Hub aggregiert, organisiert und priorisiert die Sicherheitswarnungen oder Ergebnisse mehrerer Dienste. AWS Einige dieser Dienste sind Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer und AWS Firewall Manager sowie AWS Partnerlösungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-SI-4.C	SI-4.C Überwachung des Informationssystems	cloudwatch-alarm-action-check	Amazon CloudWatch alarmiert, wenn eine Metrik den Schwellenwert für eine bestimmte Anzahl von Bewertungszeiträumen überschreitet. Der Alarm führt eine oder mehrere Aktionen durch, die vom Wert der Metrik oder des Ausdrucks im Vergleich zu einem Schwellenwert in einer Reihe von Zeiträumen abhängt. Diese Regel erfordert einen Wert für alarmActionRequired (Config Default: True), insufficientDataAction Required (Config Default: True), okActionRequired (Config Default: False). Der tatsächliche Wert muss die Alarmaktionen für Ihre Umgebung widerspiegeln.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-SI-4.C	SI-4.C Überwachung des Informationssystems	cloud-trail-log-file-validierung aktiviert	Verwenden Sie die AWS CloudTrail Protokolldateivalidierung, um die Integrität von Protokollen zu überprüfen. CloudTrail Mithilfe der Protokolldateivalidierung kann festgestellt werden, ob eine Protokolldatei geändert oder gelöscht wurde oder ob sie nach der Übermittlung CloudTrail unverändert geblieben ist. Dieses Feature wurde mit dem Branchenstandard entsprechenden Algorithmen entwickelt: SHA-256 für die Hashfunktion und SHA-256 mit RSA für digitale Signaturen. Aus diesem Grund ist es rechnerisch unmöglich, CloudTrail Protokolldateien unbemerkt zu ändern, zu löschen oder zu fälschen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-SI-4.C	SI-4.C Überwachung des Informationssystems	guardduty-enabled-centralized	Amazon GuardDuty kann mithilfe von Threat Intelligence Feeds helfen, potenzielle Cybersicherheitsereignisse zu überwachen und zu erkennen. Dazu gehören Listen mit bösartigen IPs und maschinellen Lernmethoden zur Identifizierung unerwarteter, nicht autorisierter und bösartiger Aktivitäten in Ihrer AWS Cloud-Umgebung.
CCCS-fPBMM-SI-4.C	SI-4.C Überwachung des Informationssystems	lambda-dlq-check	Aktivieren Sie diese Regel, um das entsprechende Personal über Amazon Simple Queue Service (Amazon SQS) oder Amazon Simple Notification Service (Amazon SNS) zu benachrichtigen, wenn eine Funktion ausgefallen ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-SI-4.C	SI-4.C Überwachung des Informationssystems	securityhub-enabled	AWS Security Hub hilft bei der Überwachung von unbefugtem Personal, Verbindungen, Geräten und Software. AWS Security Hub aggregiert, organisiert und priorisiert die Sicherheitswarnungen oder Ergebnisse mehrerer Dienste. AWS Einige dieser Dienste sind Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer und AWS Firewall Manager sowie AWS Partnerlösungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-SI-4.D	SI-4.D Überwachung des Informationssystems	cloudwatch-alarm-action-check	Amazon CloudWatch alarmiert, wenn eine Metrik den Schwellenwert für eine bestimmte Anzahl von Bewertungszeiträumen überschreitet. Der Alarm führt eine oder mehrere Aktionen durch, die vom Wert der Metrik oder des Ausdrucks im Vergleich zu einem Schwellenwert in einer Reihe von Zeiträumen abhängt. Diese Regel erfordert einen Wert für alarmActionRequired (Config Default: True), insufficientDataAction Required (Config Default: True), okActionRequired (Config Default: False). Der tatsächliche Wert muss die Alarmaktionen für Ihre Umgebung widerspiegeln.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-SI-4.D	SI-4.D Überwachung des Informationssystems	cloud-trail-log-file-validierung aktiviert	Verwenden Sie die AWS CloudTrail Protokolldateivalidierung, um die Integrität von Protokollen zu überprüfen. CloudTrail Mithilfe der Protokolldateivalidierung kann festgestellt werden, ob eine Protokolldatei geändert oder gelöscht wurde oder ob sie nach der Übermittlung CloudTrail unverändert geblieben ist. Dieses Feature wurde mit dem Branchenstandard entsprechenden Algorithmen entwickelt: SHA-256 für die Hashfunktion und SHA-256 mit RSA für digitale Signaturen. Aus diesem Grund ist es rechnerisch unmöglich, CloudTrail Protokolldateien unbemerkt zu ändern, zu löschen oder zu fälschen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-SI-4.D	SI-4.D Überwachung des Informationssystems	guardduty-enabled-centralized	Amazon GuardDuty kann mithilfe von Threat Intelligence Feeds helfen, potenzielle Cybersicherheitsereignisse zu überwachen und zu erkennen. Dazu gehören Listen mit bösartigen IPs und maschinellen Lernmethoden zur Identifizierung unerwarteter, nicht autorisierter und bösartiger Aktivitäten in Ihrer AWS Cloud-Umgebung.
CCCS-fPBMM-SI-4.D	SI-4.D Überwachung des Informationssystems	lambda-dlq-check	Aktivieren Sie diese Regel, um das entsprechende Personal über Amazon Simple Queue Service (Amazon SQS) oder Amazon Simple Notification Service (Amazon SNS) zu benachrichtigen, wenn eine Funktion ausgefallen ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-SI-4.D	SI-4.D Überwachung des Informationssystems	securityhub-enabled	AWS Security Hub hilft bei der Überwachung von unbefugtem Personal, Verbindungen, Geräten und Software. AWS Security Hub aggregiert, organisiert und priorisiert die Sicherheitswarnungen oder Ergebnisse mehrerer Dienste. AWS Einige dieser Dienste sind Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer und AWS Firewall Manager sowie AWS Partnerlösungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-SI-4.E	SI-4.E Überwachung des Informationssystems	cloudwatch-alarm-action-check	Amazon CloudWatch alarmiert, wenn eine Metrik den Schwellenwert für eine bestimmte Anzahl von Bewertungszeiträumen überschreitet. Der Alarm führt eine oder mehrere Aktionen durch, die vom Wert der Metrik oder des Ausdrucks im Vergleich zu einem Schwellenwert in einer Reihe von Zeiträumen abhängt. Diese Regel erfordert einen Wert für alarmActionRequired (Config Default: True), insufficientDataAction Required (Config Default: True), okActionRequired (Config Default: False). Der tatsächliche Wert muss die Alarmaktionen für Ihre Umgebung widerspiegeln.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-SI-4.E	SI-4.E Überwachung des Informationssystems	cloud-trail-log-file-validierung aktiviert	Verwenden Sie die AWS CloudTrail Protokolldateivalidierung, um die Integrität von Protokollen zu überprüfen. CloudTrail Mithilfe der Protokolldateivalidierung kann festgestellt werden, ob eine Protokolldatei geändert oder gelöscht wurde oder ob sie nach der Übermittlung CloudTrail unverändert geblieben ist. Dieses Feature wurde mit dem Branchenstandard entsprechenden Algorithmen entwickelt: SHA-256 für die Hashfunktion und SHA-256 mit RSA für digitale Signaturen. Aus diesem Grund ist es rechnerisch unmöglich, CloudTrail Protokolldateien unbemerkt zu ändern, zu löschen oder zu fälschen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-SI-4.E	SI-4.E Überwachung des Informationssystems	guardduty-enabled-centralized	Amazon GuardDuty kann mithilfe von Threat Intelligence Feeds helfen, potenzielle Cybersicherheitsereignisse zu überwachen und zu erkennen. Dazu gehören Listen mit bösartigen IPs und maschinellen Lernmethoden zur Identifizierung unerwarteter, nicht autorisierter und bösartiger Aktivitäten in Ihrer AWS Cloud-Umgebung.
CCCS-fPBMM-SI-4.E	SI-4.E Überwachung des Informationssystems	lambda-dlq-check	Aktivieren Sie diese Regel, um das entsprechende Personal über Amazon Simple Queue Service (Amazon SQS) oder Amazon Simple Notification Service (Amazon SNS) zu benachrichtigen, wenn eine Funktion ausgefallen ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-SI-4.E	SI-4.E Überwachung des Informationssystems	securityhub-enabled	AWS Security Hub hilft bei der Überwachung von unbefugtem Personal, Verbindungen, Geräten und Software. AWS Security Hub aggregiert, organisiert und priorisiert die Sicherheitswarnungen oder Ergebnisse mehrerer Dienste. AWS Einige dieser Dienste sind Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer und AWS Firewall Manager sowie AWS Partnerlösungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-SI-4.F	SI-4.F Überwachung des Informationssystems	cloudwatch-alarm-action-check	Amazon CloudWatch alarmiert, wenn eine Metrik den Schwellenwert für eine bestimmte Anzahl von Bewertungszeiträumen überschreitet. Der Alarm führt eine oder mehrere Aktionen durch, die vom Wert der Metrik oder des Ausdrucks im Vergleich zu einem Schwellenwert in einer Reihe von Zeiträumen abhängt. Diese Regel erfordert einen Wert für alarmActionRequired (Config Default: True), insufficientDataAction Required (Config Default: True), okActionRequired (Config Default: False). Der tatsächliche Wert muss die Alarmaktionen für Ihre Umgebung widerspiegeln.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-SI-4.F	SI-4.F Überwachung des Informationssystems	cloud-trail-log-file-validierung aktiviert	Verwenden Sie die AWS CloudTrail Protokolldateivalidierung, um die Integrität von Protokollen zu überprüfen. CloudTrail Mithilfe der Protokolldateivalidierung kann festgestellt werden, ob eine Protokolldatei geändert oder gelöscht wurde oder ob sie nach der Übermittlung CloudTrail unverändert geblieben ist. Dieses Feature wurde mit dem Branchenstandard entsprechenden Algorithmen entwickelt: SHA-256 für die Hashfunktion und SHA-256 mit RSA für digitale Signaturen. Aus diesem Grund ist es rechnerisch unmöglich, CloudTrail Protokolldateien unbemerkt zu ändern, zu löschen oder zu fälschen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-SI-4.F	SI-4.F Überwachung des Informationssystems	guardduty-enabled-centralized	Amazon GuardDuty kann mithilfe von Threat Intelligence Feeds helfen, potenzielle Cybersicherheitsereignisse zu überwachen und zu erkennen. Dazu gehören Listen mit bösartigen IPs und maschinellen Lernmethoden zur Identifizierung unerwarteter, nicht autorisierter und bösartiger Aktivitäten in Ihrer AWS Cloud-Umgebung.
CCCS-fPBMM-SI-4.F	SI-4.F Überwachung des Informationssystems	lambda-dlq-check	Aktivieren Sie diese Regel, um das entsprechende Personal über Amazon Simple Queue Service (Amazon SQS) oder Amazon Simple Notification Service (Amazon SNS) zu benachrichtigen, wenn eine Funktion ausgefallen ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-SI-4.F	SI-4.F Überwachung des Informationssystems	securityhub-enabled	AWS Security Hub hilft bei der Überwachung von unbefugtem Personal, Verbindungen, Geräten und Software. AWS Security Hub aggregiert, organisiert und priorisiert die Sicherheitswarnungen oder Ergebnisse mehrerer Dienste. AWS Einige dieser Dienste sind Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer und AWS Firewall Manager sowie AWS Partnerlösungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-SI-4.G	SI-4.G Überwachung des Informationssystems	cloudwatch-alarm-action-check	Amazon CloudWatch alarmiert, wenn eine Metrik den Schwellenwert für eine bestimmte Anzahl von Bewertungszeiträumen überschreitet. Der Alarm führt eine oder mehrere Aktionen durch, die vom Wert der Metrik oder des Ausdrucks im Vergleich zu einem Schwellenwert in einer Reihe von Zeiträumen abhängt. Diese Regel erfordert einen Wert für alarmActionRequired (Config Default: True), insufficientDataAction Required (Config Default: True), okActionRequired (Config Default: False). Der tatsächliche Wert muss die Alarmaktionen für Ihre Umgebung widerspiegeln.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-SI-4.G	SI-4.G Überwachung des Informationssystems	cloud-trail-log-file-validierung aktiviert	Verwenden Sie die AWS CloudTrail Protokolldateivalidierung, um die Integrität von Protokollen zu überprüfen. CloudTrail Mithilfe der Protokolldateivalidierung kann festgestellt werden, ob eine Protokolldatei geändert oder gelöscht wurde oder ob sie nach der Übermittlung CloudTrail unverändert geblieben ist. Dieses Feature wurde mit dem Branchenstandard entsprechenden Algorithmen entwickelt: SHA-256 für die Hashfunktion und SHA-256 mit RSA für digitale Signaturen. Aus diesem Grund ist es rechnerisch unmöglich, CloudTrail Protokolldateien unbemerkt zu ändern, zu löschen oder zu fälschen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-SI-4.G	SI-4.G Überwachung des Informationssystems	guardduty-enabled-centralized	Amazon GuardDuty kann mithilfe von Threat Intelligence Feeds helfen, potenzielle Cybersicherheitsereignisse zu überwachen und zu erkennen. Dazu gehören Listen mit bösartigen IPs und maschinellen Lernmethoden zur Identifizierung unerwarteter, nicht autorisierter und bösartiger Aktivitäten in Ihrer AWS Cloud-Umgebung.
CCCS-fPBMM-SI-4.G	SI-4.G Überwachung des Informationssystems	lambda-dlq-check	Aktivieren Sie diese Regel, um das entsprechende Personal über Amazon Simple Queue Service (Amazon SQS) oder Amazon Simple Notification Service (Amazon SNS) zu benachrichtigen, wenn eine Funktion ausgefallen ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-SI-4.G	SI-4.G Überwachung des Informationssystems	securityhub-enabled	AWS Security Hub hilft bei der Überwachung von unbefugtem Personal, Verbindungen, Geräten und Software. AWS Security Hub aggregiert, organisiert und priorisiert die Sicherheitswarnungen oder Ergebnisse mehrerer Dienste. AWS Einige dieser Dienste sind Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer und AWS Firewall Manager sowie AWS Partnerlösungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-SI-5.A	SI-5.A Sicherheitswarnungen, Hinweise und Richtlinien	guardduty-enabled-centralized	Amazon GuardDuty kann mithilfe von Threat Intelligence Feeds helfen, potenzielle Cybersicherheitsereignisse zu überwachen und zu erkennen. Dazu gehören Listen mit bösartigen IPs und maschinellen Lernmethoden zur Identifizierung unerwarteter, nicht autorisierter und bösartiger Aktivitäten in Ihrer AWS Cloud-Umgebung.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-SI-5.B	SI-5.B Sicherheitswarnungen, Hinweise und Richtlinien	guardduty-enabled-centralized	Amazon GuardDuty kann mithilfe von Threat Intelligence Feeds helfen, potenzielle Cybersicherheitsereignisse zu überwachen und zu erkennen. Dazu gehören Listen mit bösartigen IPs und maschinellen Lernmethoden zur Identifizierung unerwarteter, nicht autorisierter und bösartiger Aktivitäten in Ihrer AWS Cloud-Umgebung.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-SI-5.C	SI-5.C Sicherheitswarnungen, Hinweise und Richtlinien	guardduty-enabled-centralized	Amazon GuardDuty kann mithilfe von Threat Intelligence Feeds helfen, potenzielle Cybersicherheitsereignisse zu überwachen und zu erkennen. Dazu gehören Listen mit bösartigen IPs und maschinellen Lernmethoden zur Identifizierung unerwarteter, nicht autorisierter und bösartiger Aktivitäten in Ihrer AWS Cloud-Umgebung.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-SI-5.D	SI-5.D Sicherheitswarnungen, Hinweise und Richtlinien	guardduty-enabled-centralized	Amazon GuardDuty kann mithilfe von Threat Intelligence Feeds helfen, potenzielle Cybersicherheitsereignisse zu überwachen und zu erkennen. Dazu gehören Listen mit bösartigen IPs und maschinellen Lernmethoden zur Identifizierung unerwarteter, nicht autorisierter und bösartiger Aktivitäten in Ihrer AWS Cloud-Umgebung.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-SI-7(1)	SI-7(1) Software-, Firmware- und Informationsintegrität | Integritätsprüfungen	cloud-trail-log-file-Validierung aktiviert	Verwenden Sie die AWS CloudTrail Protokolldateivalidierung, um die Integrität von Protokollen zu überprüfen. CloudTrail Mithilfe der Protokolldateivalidierung kann festgestellt werden, ob eine Protokolldatei geändert oder gelöscht wurde oder ob sie nach der Übermittlung CloudTrail unverändert geblieben ist. Dieses Feature wurde mit dem Branchenstandard entsprechenden Algorithmen entwickelt: SHA-256 für die Hashfunktion und SHA-256 mit RSA für digitale Signaturen. Aus diesem Grund ist es rechnerisch unmöglich, CloudTrail Protokolldateien unbemerkt zu ändern, zu löschen oder zu fälschen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-SI-7(7)	SI-7(7) Software-, Firmware- und Informationsintegrität | Integration von Erkennung und Reaktion	cloud-trail-log-file-Validierung aktiviert	Verwenden Sie die AWS CloudTrail Protokolldateivalidierung, um die Integrität von Protokollen zu überprüfen. CloudTrail Mithilfe der Protokolldateivalidierung kann festgestellt werden, ob eine Protokolldatei geändert oder gelöscht wurde oder ob sie nach der Übermittlung CloudTrail unverändert geblieben ist. Dieses Feature wurde mit dem Branchenstandard entsprechenden Algorithmen entwickelt: SHA-256 für die Hashfunktion und SHA-256 mit RSA für digitale Signaturen. Aus diesem Grund ist es rechnerisch unmöglich, CloudTrail Protokolldateien unbemerkt zu ändern, zu löschen oder zu fälschen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-SI-7.A	SI-7.A Software-, Firmware- und Informationsintegrität	cloud-trail-log-file-Validierung aktiviert	Verwenden Sie die AWS CloudTrail Protokolldateivalidierung, um die Integrität von Protokollen zu überprüfen. CloudTrail Mithilfe der Protokolldateivalidierung kann festgestellt werden, ob eine Protokolldatei geändert oder gelöscht wurde oder ob sie nach der Übermittlung CloudTrail unverändert geblieben ist. Dieses Feature wurde mit dem Branchenstandard entsprechenden Algorithmen entwickelt: SHA-256 für die Hashfunktion und SHA-256 mit RSA für digitale Signaturen. Aus diesem Grund ist es rechnerisch unmöglich, CloudTrail Protokolldateien unbemerkt zu ändern, zu löschen oder zu fälschen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Leitfaden
CCCS-fPBMM-SI-12.A	SI-12.A Umgang und Aufbewahrung von Informationen	cw-loggroup-retention-period-überprüfen	Stellen Sie sicher, dass die Ereignisprotokolldaten für Ihre Protokollgruppen über eine Mindestdauer aufbewahrt werden, um die Fehlerbehebung und forensische Untersuchungen zu unterstützen. Fehlende frühere Ereignisprotokolldaten erschweren die Rekonstruierung und Identifizierung potenziell schädlicher Ereignisse.

Vorlage

Die Vorlage ist verfügbar unter GitHub: Operational Best Practices for Canadian Centre for Cyber Security (CCCS) Medium Cloud Control Profile.

Best Practices für den Betrieb von CIS AWS Foundations Benchmark v1.4 Level 1

Konformitätspakete bieten ein allgemeines Compliance-Framework, das es Ihnen ermöglicht, mithilfe verwalteter oder benutzerdefinierter AWS Config Regeln und Abhilfemaßnahmen Kontrollen zur Sicherheits-, Betriebs- oder Kostenoptimierung durchzuführen. AWS Config Conformance Packs dienen als Beispielvorlagen nicht dazu, die vollständige Einhaltung eines bestimmten Governance- oder Compliance-Standards sicherzustellen. Sie sind dafür verantwortlich, selbst zu beurteilen, ob Ihre Nutzung der Services den geltenden gesetzlichen und behördlichen Anforderungen entspricht.

Im Folgenden finden Sie ein Beispiel für eine Zuordnung zwischen dem Center for Internet Security (CIS) Amazon Web Services Foundation v1.4 Level 1 und AWS verwalteten Konfigurationsregeln/ Prozessprüfungen AWS Config . Jede Config-Regel gilt für eine bestimmte AWS Ressource und bezieht sich auf eine oder mehrere CIS Amazon Web Services Foundation v1.4 Level 1-Steuerelemente. Eine CIS-Amazon-Web-Services-Foundation-v1.4-Level-1-Kontrolle kann mit mehreren Config-Regeln verknüpft werden. In der folgenden Tabelle finden Sie weitere Informationen und Anleitungen zu diesen Zuordnungen.

Weitere Informationen zu Prozessprüfungen finden Sie unter Prozessprüfungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
1.1	Verwalten der aktuellen Kontaktdaten	account-contact-details-configured (Prozessüberprüfung)	Stellen Sie sicher, dass die Kontakt-E-Mail-Adresse und Telefonnummer für AWS -Konten aktuell und mehr als einer Person in Ihrer Organisation zugeordnet sind. Stellen Sie sicher, dass im Bereich „Mein Konto“ der Konsole im Abschnitt „Kontaktinformationen“ die richtigen Informationen angegeben sind. Weitere Informationen zur Prüfung dieser Kontrolle finden Sie im Dokument CIS Amazon Web Services Foundations Benchmark Version 1.4.0, das unter

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			https://www.cisecurity verfügbar ist. org/benchmark/amazon_web_services/
1.2	Sicherstellen, dass Kontaktdaten für Sicherheitsfragen registriert sind	account-security-contact-configured (Prozessüberprüfung)	Stellen Sie sicher, dass die Kontakt-E-Mail-Adresse und die Telefonnummer des Sicherheitsteams Ihres Unternehmens aktuell sind. Stellen Sie sicher, dass im Bereich „Mein Konto“ der AWS Management-Konsole im Bereich Sicherheit die richtigen Informationen angegeben sind. Weitere Informationen zur Prüfung dieser Kontrolle finden Sie im Dokument CIS Amazon Web Services Foundations Benchmark Version 1.4.0, das unter https://www.cisecurity verfügbar ist. org/benchmark/amazon_web_services/

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
1.4	Sicherstellen, dass kein Root-Benutzerzugriffsschlüssel vorhanden ist	iam-root-access-key-überprüfen	Der Zugriff auf Systeme und Ressourcen kann gesteuert werden, indem überprüft wird, ob der Root-Benutzer keine Zugriffsschlüssel mit seiner AWS Identity and Access Management (IAM) -Rolle verknüpft hat. Stellen Sie sicher, dass die Root-Zugriffsschlüssel gelöscht werden. Erstellen und verwenden Sie stattdessen rollenbasierte Funktionen, AWS-Konten um das Prinzip der geringsten Funktionalität zu berücksichtigen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
1.5	Sicherstellen, dass MFA für den Root-Benutzer aktiviert ist	root-account-mfa-enabled	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass MFA für den Root-Benutzer aktiviert ist. Der Stammbenutzer ist der AWS-Konto-Benutzer mit den meisten Berechtigungen. MFA bietet eine weitere Schutzebene zusätzlich zum Benutzernamen und Passwort. Indem Sie MFA für den Root-Benutzer vorschreiben, können Sie die Anzahl AWS-Konten kompromittierter Benutzer reduzieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
1,7	Beseitigen der Verwendung des Root-Benutzers für administrative und tägliche Aufgaben	root-account-regular-use (Prozessüberprüfung)	Stellen Sie sicher, dass das Root-Konto nicht für alltägliche Aufgaben verwendet wird. Führen Sie in IAM einen Anmeldeinformationsbericht aus, um zu untersuchen, wann der Root-Benutzer zuletzt verwendet wurde. Weitere Informationen zur Prüfung dieser Kontrolle finden Sie im Dokument CIS Amazon Web Services Foundations Benchmark Version 1.4.0, das unter https://www.cisecurity verfügbar ist. org/benchmark/amazon_web_services/

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
1.8	Sicherstellen, dass die IAM-Passwortrichtlinie eine Mindestlänge von 14 Zeichen oder mehr erfordert	iam-password-policy	Die Identitäten und Anmeldeinformationen werden auf der Grundlage einer organisatorischen IAM-Passwortrichtlinie ausgestellt, verwaltet und verifiziert. Sie erfüllen oder übertreffen die Anforderungen von NIST SP 800-63 und dem Standard „Best Practices“ von AWS Foundational Security für die Passwortstärke. Mit dieser Regel können Sie optional RequireUppercaseCharacters (Wert für AWS grundlegende Sicherheitsbewährte Methoden: wahr), RequireLowercaseCharacters (Wert für bewährte Methoden für AWS grundlegende Sicherheit: wahr), RequireSymbols (Wert für bewährte Methoden für AWS grundlegende Sicherheit:

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			wahr), RequireNumbers (Wert für bewährte Methoden für AWS grundlegende Sicherheit: wahr), MinimumPasswordLength (Wert für bewährte Methoden für AWS grundlegende Sicherheit: 14), PasswordReusePrevention (Wert für bewährte Methoden für AWS grundlegende Sicherheit: 24) und MaxPasswordAge (Wert für bewährte Methoden für AWS grundlegende Sicherheit: 90) für Ihr IAM festlegen Kennwortrichtlinie. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
1.9	Sicherstellen, dass die IAM-Passw ortrichtlinie die Wiederverwendung von Passwörtern verhindert	iam-password-policy	Die Identitäten und Anmeldeinformation en werden auf der Grundlage einer organisatorischen IAM-Passwortrichtlinie ausgestellt, verwaltet und verifiziert. Sie erfüllen oder übertreff en die Anforderungen von NIST SP 800-63 und dem Standard „Best Practices“ von AWS Foundatio nal Security für die Passwortstärke. Mit dieser Regel können Sie optional RequireUppercaseCh aracters (Wert für AWS grundlegende Sicherheitsbewährt e Methoden: wahr), RequireLowercaseCh aracters (Wert für bewährte Methoden für AWS grundlege nde Sicherheit: wahr), RequireSy mbols (Wert für bewährte Methoden für AWS grundlege nde Sicherheit:

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			wahr), RequireNumbers (Wert für bewährte Methoden für AWS grundlegende Sicherheit: wahr), MinimumPasswordLength (Wert für bewährte Methoden für AWS grundlegende Sicherheit: 14), PasswordReusePrevention (Wert für bewährte Methoden für AWS grundlegende Sicherheit: 24) und MaxPasswordAge (Wert für bewährte Methoden für AWS grundlegende Sicherheit: 90) für Ihr IAM festlegen Kennwortrichtlinie. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
1.10	Sicherstellen, dass für alle Benutzer mit Konsolenpasswort die Multi-Faktor-Authentifizierung (MFA) aktiviert ist	mfa-enabled-for-iam-Konsolenzugriff	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass MFA für alle AWS Identity and Access Management (IAM) -Benutzer aktiviert ist, die über ein Konsolenkennwort verfügen. MFA sorgt für eine weitere Schutzebene zusätzlich zu den Anmeldeinformationen. Indem Sie MFA für Benutzer vorschreiben, können Sie Fälle kompromittierter Konten reduzieren und verhindern, dass unbefugte Benutzer auf vertrauliche Daten zugreifen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
1.11	Kein Einrichten von Zugangssc hlüsseln bei der Ersteinrichtung für alle Benutzer mit Konsolenpasswort	iam-user-console-and- api-access-at-creation (Prozessü berprüfung)	Stellen Sie sicher, dass bei der Ersteinrichtung für alle Benutzer mit Konsolenpasswort keine Zugangssc hlüssel eingerichtet werden. Vergleichen Sie für alle Benutzer mit Konsolenzugriff die Erstellungszeit des Benutzers mit dem Erstellungsdatum des Zugriffsschlüssels . Weitere Informati onen zur Prüfung dieser Kontrolle finden Sie im Dokument CIS Amazon Web Services Foundations Benchmark Version 1.4.0, das unter https://www.cisecu rity verfügbar ist. org/ benchmark/amaz on_web_services/

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
1.12	Sicherstellen, dass Anmeldeinformationen, die 45 Tage oder länger nicht verwendet wurden, deaktiviert werden	iam-user-unused-credentials-überprüfen	AWS Identity and Access Management (IAM) kann Ihnen bei Zugriffsberechtigungen und Autorisierungen helfen, indem es nach IAM-Passwörtern und Zugriffsschlüsseln sucht, die für einen bestimmten Zeitraum nicht verwendet wurden. Wenn ungenutzte Anmeldeinformationen identifiziert werden, müssen Sie sie deaktivieren und/oder entfernen, da dies gegen das Prinzip der geringsten Berechtigung verstoßen könnte. Für diese Regel müssen Sie einen Wert für das maxCredentialUsageAlter festlegen (CIS-Standardwert: 45). Der tatsächliche Wert muss den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
1.13	Sicherstellen, dass für jeden Benutzer nur ein aktiver Zugriffss chlüssel verfügbar ist	iam-user-single-ac cess-Taste (Prozessp rüfung)	Stellen Sie sicher, dass für jeden einzelnen Benutzer nur ein aktiver Zugriffsschlüssel verfügbar ist. Stellen Sie für alle Benutzer sicher, dass auf der Registerkarte Sicherheitsanmelde informationen für jeden Benutzer in IAM nur ein aktiver Schlüssel verwendet wird. Weitere Informati onen zur Prüfung dieser Kontrolle finden Sie im Dokument CIS Amazon Web Services Foundations Benchmark Version 1.4.0, das unter https://www.cisecu rity verfügbar ist. org/ benchmark/amaz on_web_services/

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
1.14	Sicherstellen, dass die Zugriffsschlüssel spätestens alle 90 Tage rotiert werden	access-keys-rotated	Die Anmeldein formationen für autorisierte Geräte, Benutzer und Prozesse werden geprüft, indem sichergestellt wird, dass die IAM-Zugri ffsschlüssel gemäß den Vorgaben der Unternehmensrichtl inie rotiert werden. Das regelmäßi ge Ändern der Zugriffsschlüssel ist eine bewährte Sicherheitsmethode . Es verkürzt den Zeitraum, in dem ein Zugriffsschlüssel aktiv ist, und reduziert die Auswirkungen auf das Unternehmen, wenn die Schlüssel kompromittiert werden. Diese Regel erfordert einen Wert für die Zugriffsschlüssel-Rotation (Standard konfiguration: 90). Der tatsächliche Wert muss den Richtlini

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			en Ihrer Organisation entsprechen.
1.15	Sicherstellen, dass Benutzer Berechtigungen nur über Gruppen erhalten	iam-user-no-policies-überprüfen	Diese Regel stellt sicher, dass AWS Identity and Access Management (IAM) -Richtlinien nur Gruppen oder Rollen zugewiesen werden, um den Zugriff auf Systeme und Ressourcen zu kontrollieren. Die Zuweisung von Berechtigungen auf Gruppen- oder Rollenebene trägt dazu bei, die Wahrscheinlichkeit zu verringern, dass eine Identität übermäßige Berechtigungen erhält oder beibehält.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
1.15	Sicherstellen, dass Benutzer Berechtigungen nur über Gruppen erhalten	iam-no-inline-policy-überprüfen	Stellen Sie sicher, dass ein Benutzer, eine IAM-Rolle oder eine IAM-Gruppe (AWS Identity and Access Management) nicht über eine Inline-Richtlinie zur Zugriffskontrolle auf Systeme und Ressourcen verfügt. AWS empfiehlt, verwaltete Richtlinien anstelle von Inline-Richtlinien zu verwenden. Verwaltete Richtlinien ermöglichen Wiederverwendbarkeit, Versionsverwaltung, Rollback und Delegierung der Berechtigungsverwaltung.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
1.15	Sicherstellen, dass Benutzer Berechtigungen nur über Gruppen erhalten	iam-user-group-membership-überprüfen	AWS Identity and Access Management (IAM) kann Ihnen helfen, Zugriffsberechtigungen und Autorisierungen einzuschränken, indem sichergestellt wird, dass Benutzer Mitglieder mindestens einer Gruppe sind. Wenn Benutzern mehr Berechtigungen eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und Aufgabentrennung verstoßen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
1.16	Sicherstellen, dass keine IAM-Richtlinien angehängt werden, die vollständige Administratorrechte (*:*) zulassen	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) kann Ihnen dabei helfen, die Prinzipien der geringsten Rechte und der Aufgabentrennung in Zugriffsberechtigungen und Autorisierungen zu integrieren und so zu verhindern, dass Richtlinien „Effect“: „Allow“ mit „Action“: „*“ anstelle von „Resource“: „*“ enthalten. Wenn Benutzern mehr Rechte eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und der Aufgabentrennung verstoßen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
1,17	Stellen Sie sicher, dass eine Support-Rolle eingerichtet wurde, um Vorfälle mit AWS Support zu verwalten	iam-policy-in-use	AWS Identity and Access Managemen t (IAM) kann Sie bei der Verwaltung von Zugriffsberechtigu ngen und Autorisie rungen unterstützen, indem sichergestellt wird, dass IAM-Richt linien den entsprech enden Benutzern, Rollen oder Gruppen zugewiesen werden. Die Einschränkung dieser Richtlinien beinhaltet auch die Prinzipien der geringsten Berechtigung und der Aufgabent rennung. Diese Regel erfordert, dass Sie das policyARN auf arn:aws:iam: AWSSupport :aws:poli cy/ Access setzen, um das Incident Management mit Support zu ermöglich en. AWS

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
1.19	Sicherstellen, dass alle abgelaufenen SSL/TLS-Zertifikate, die in AWS IAM gespeichert sind, entfernt werden	iam-expired-certificates (Prozessüberprüfung)	Stellen Sie sicher, dass alle abgelaufenen SSL/TLS-Zertifikate, die in IAM gespeichert sind, entfernt werden. Führen Sie in der Befehlszeile mit der installierten AWS CLI den Befehl „AWS iam list-server-certificates“ aus und ermitteln Sie, ob abgelaufene Serverzertifikate vorhanden sind. Weitere Informationen zur Prüfung dieser Kontrolle finden Sie im Dokument CIS Amazon Web Services Foundations Benchmark Version 1.4.0, das unter https://www.cisecurity verfügbar ist. org/benchmark/amazon_web_services/

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
1,20	Stellen Sie sicher, dass AWS IAM Access Analyzer aktiviert ist	iam-access-analyzer-enabled (Prozessüberprüfung)	Stellen Sie sicher, dass IAM Access Analyzer aktiviert ist. Wählen Sie im IAM-Bereich der Konsole „Zugriffs-Analyzer“ aus und stellen Sie sicher, dass der STATUS auf „Aktiv“ gesetzt ist. Weitere Informationen zur Prüfung dieser Kontrolle finden Sie im Dokument CIS Amazon Web Services Foundations Benchmark Version 1.4.0, das unter https://www.cisecurity verfügbar ist. org/benchmark/amazon_web_services/

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
2.1.3	Sicherstellen, dass die MFA-Lösch funktion für S3-Bucket s aktiviert ist	s-3 bucket-versioning-enabled	Mit der Versionsv erwaltung von Amazon-Simple-Storage-Servi ce (Amazon-S3)-Buckets können Sie mehrere Varianten eines Objekts im selben Amazon-S3 -Bucket speichern. Das Hinzufügen der Multi-Faktor-Authe ntifizierung (MFA)-Lös chfunktion zu einem S3-Bucket erfordert einen zusätzlichen Authentifizierungs faktor, um den Versionsstatus Ihres Buckets zu ändern oder eine Objektver sion zu löschen. Die MFA-Löschfunktion kann eine zusätzlic he Sicherheitsebene für den Fall hinzufüge n, dass Sicherhei tsanmeldeinformati onen kompromit tiert oder unbefugte Zugriffe gewährt werden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
2.1.5	Sicherstellen, dass S3-Buckets mit „Öffentlichen Zugriff blockieren (Bucket-Einstellungen)“ konfiguriert sind	s3- account-level-public-access -blöcke-periodisch	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Simple Storage Service (Amazon S3) -Buckets nicht öffentlich zugänglich sind. Diese Regel trägt dazu bei, sensible Daten vor unbefugten Remote-Benutzern zu schützen, indem sie den öffentlichen Zugriff verhindert. Mit dieser Regel können Sie optional die Parameter ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) und restrictPublicBuckets Parameter (Config Default: True) festlegen. Die tatsächlichen Werte müssen den Richtlini

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			en Ihrer Organisation entsprechen.
2.1.5	Sicherstellen, dass S3-Buckets mit „Öffentlichen Zugriff blockieren (Bucket-Einstellungen)“ konfiguriert sind	s3 bucket-level-public-access - verboten	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Simple Storage Service (Amazon S3) -Buckets nicht öffentlich zugänglich sind. Diese Regel trägt dazu bei, sensible Daten vor unbefugten Remote-Benutzern zu schützen, indem sie den öffentlichen Zugriff auf Bucket-Ebene verhindert.
2.2.1	Sicherstellen, dass die EBS-Volume-Verschlüsselung aktiviert ist	encrypted-volumes	Aktivieren Sie die Verschlüsselung für Ihre Amazon-Elastic-Block-Store (Amazon-EBS)-Volumes, um eventuell vorhandene sensible Daten sowie Daten im Ruhezustand zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
2.2.1	Sicherstellen, dass die EBS-Volume-Verschlüsselung aktiviert ist	ec2- ebs-encryption-by-default	Zum Schutz von Daten im Ruhezustand müssen Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon Elastic Block Store (Amazon EBS)-Volumes aktiviert ist. Da sensible Daten auch im Ruhezustand vorhanden sein können, sollten Sie die Verschlüsselung im Ruhezustand aktivieren, um diese Daten zu schützen.
2.3.1	Sicherstellen, dass die Verschlüsselung für RDS-Instances aktiviert ist	rds-snapshot-encrypted	Stellen Sie sicher, dass die Verschlüsselung für Ihre Amazon Relational Database Service (Amazon RDS)-Snapshots aktiviert ist. Da sensible Daten auch im Ruhezustand vorhanden sein können, sollten Sie die Verschlüsselung im Ruhezustand aktivieren, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
2.3.1	Sicherstellen, dass die Verschlüsselung für RDS-Instances aktiviert ist	rds-storage-encrypted	Zum Schutz von Daten im Ruhezustand müssen Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon Relational Database Service (Amazon RDS)-Instances aktiviert ist. Um eventuell vorhandene sensible Daten im Ruhezustand in Amazon-RDS-Instances zu schützen, muss die Verschlüsselung von Daten im Ruhezustand aktiviert sein.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.1	Stellen Sie sicher CloudTrail , dass es in allen Regionen aktiviert ist	multi-region-cloudtrail-enabled	AWS CloudTrail zeichnet Aktionen und API-Aufrufe der AWS Management Console auf. Sie können feststellen, welche Benutzer und Konten angerufen wurden AWS, von welcher Quell-IP-Adresse aus die Anrufe getätigt wurden und wann die Anrufe erfolgten. CloudTrail übermittelt Protokolldateien aus allen AWS Regionen an Ihren S3-Bucket , wenn MULTI_REGION_CLOUD_TRAIL_ENABLED aktiviert ist. Außerdem wird beim AWS Start einer neuen Region derselbe Trail in der neuen Region erstellt. CloudTrail Dadurch erhalten Sie automatisch Protokolldateien mit API-Aktivitäten für die neue Region.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.3	Stellen Sie sicher, dass der zum Speichern von CloudTrail Protokoll en verwendete S3-Bucket nicht öffentlich zugänglich ist	s-3 bucket-public-read -prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie nur autorisierten Benutzern, Prozessen und Geräten Zugriff auf Amazon Simple Storage Service (Amazon S3) - Buckets gewähren. Die Verwaltung des Zugriffs sollte mit der Klassifizierung der Daten übereinst immen.
3.3	Stellen Sie sicher, dass der zum Speichern von CloudTrail Protokoll en verwendete S3-Bucket nicht öffentlich zugänglich ist	s-3 bucket-public-writ e-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie nur autorisierten Benutzern, Prozessen und Geräten Zugriff auf Amazon Simple Storage Service (Amazon S3) - Buckets gewähren. Die Verwaltung des Zugriffs sollte mit der Klassifizierung der Daten übereinst immen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.3	Stellen Sie sicher, dass der zum Speichern von CloudTrail Protokollen verwendete S3-Bucket nicht öffentlich zugänglich ist	s3 bucket-level-public-access - verboten	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Simple Storage Service (Amazon S3) -Buckets nicht öffentlich zugänglich sind. Diese Regel trägt dazu bei, sensible Daten vor unbefugten Remote-Benutzern zu schützen, indem sie den öffentlichen Zugriff auf Bucket-Ebene verhindert.
3.4	Stellen Sie sicher, dass die CloudTrail Pfade in Logs integriert CloudWatch sind	cloud-trail-cloud-watch-Logs aktiviert	Verwenden Sie Amazon CloudWatch , um Protokollereignisaktivitäten zentral zu sammeln und zu verwalten. Die Aufnahme von AWS CloudTrail Daten liefert Einzelheiten zu den API-Aufrufaktivitäten in Ihrem AWS-Konto.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.6	Stellen Sie sicher, dass die Protokoll ierung des S3-Bucket -Zugriffs auf dem CloudTrail S3-Bucket aktiviert ist	s-3 bucket-logging-enabled	Die Amazon Simple Storage Service (Amazon S3)-Serverzugriffs protokollierung bietet eine Methode zur Überwachu ng des Netzwerks im Hinblick auf potenzielle Cybersich erheitsereignisse. Die Ereignisse werden überwacht, indem detaillierte Aufzeichn ungen über die Anfragen erfasst werden, die an einen Amazon-S3-Bucket gestellt wurden. Jeder Zugriffsprotokolle intrag enthält Details zu einer einzelnen Zugriffsanfrage. Zu den Details gehören Anforderer, Bucket-Name, Anforderu ngszeit, Anforderu ngsaktion, Antwortst atus und Fehlercode, falls relevant.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
4.1	Sicherstellen, dass ein Protokollmetrikfilter und ein Alarm für nicht autorisierte API-Aufrufe vorhanden sind	alarm-unauthorized-api-calls (Prozessüberprüfung)	Stellen Sie sicher, dass ein Protokollmetrikfilter und ein Alarm für nicht autorisierte API-Aufrufe vorhanden sind. Weitere Informationen zur Prüfung dieser Kontrolle finden Sie im Dokument CIS Amazon Web Services Foundations Benchmark Version 1.4.0, das unter https://www.cisecurity verfügbar ist. org/benchmark/amazon_web_services/

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
4.2	Sicherstellen, dass ein Protokollmetrikfilter und ein Alarm für die Anmeldung in der Managementkonsole ohne MFA vorhanden sind	alarm-sign-in-without-mfa (Prozessüberprüfung)	Stellen Sie sicher, dass ein Protokollmetrikfilter und ein Alarm für die Anmeldung bei der AWS Management Console ohne Multi-Faktor-Authentifizierung (MFA) vorhanden sind. Weitere Informationen zur Prüfung dieser Kontrolle finden Sie im Dokument CIS Amazon Web Services Foundations Benchmark Version 1.4.0, das unter https://www.cisecurity verfügbar ist. org/benchmark/amazon_web_services/

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
4.3	Sicherstellen, dass ein Protokollmetrikfilter und ein Alarm für die Verwendung des Root-Kontos vorhanden sind	alarm-root-account-use (Prozessüberprüfung)	Stellen Sie sicher, dass ein Protokollmetrikfilter und ein Alarm für die Verwendung des Root-Kontos vorhanden sind. Weitere Informationen zur Prüfung dieser Kontrolle finden Sie im Dokument CIS Amazon Web Services Foundations Benchmark Version 1.4.0, das unter https://www.cisecurity verfügbar ist. org/benchmark/amazon_web_services/

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
4.4	Sicherstellen, dass ein Protokollmetrikfilter und ein Alarm für Änderungen an der IAM-Richtlinie vorhanden sind	alarm-iam-policy-change (Prozessüberprüfung)	Stellen Sie sicher, dass ein Protokollmetrikfilter und ein Alarm für Änderungen an der IAM-Richtlinie vorhanden sind. Weitere Informationen zur Prüfung dieser Kontrolle finden Sie im Dokument CIS Amazon Web Services Foundations Benchmark Version 1.4.0, das unter https://www.cisecurity verfügbar ist. org/benchmark/amazon_web_services/

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
4.5	Stellen Sie sicher, dass ein Log-Metrikfilter und ein Alarm für CloudTrail Konfigurationsänderungen vorhanden sind	alarm-cloudtrail-config-change (Prozessüberprüfung)	Stellen Sie sicher, dass ein Log-Metrikfilter und ein Alarm für AWS Cloud Trail Konfigurationsänderungen vorhanden sind. Weitere Informationen zur Prüfung dieser Kontrolle finden Sie im Dokument CIS Amazon Web Services Foundations Benchmark Version 1.4.0, das unter https://www.cisecurity verfügbar ist. org/benchmark/amazon_web_services/

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
4.8	Sicherstellen, dass ein Protokollmetrikfilter und ein Alarm für Änderungen an der S3-Bucket-Richtlinie vorhanden sind	alarm-s3- bucket-policy-change (Prozessüberprüfung)	Stellen Sie sicher, dass ein Protokollmetrikfilter und ein Alarm für Änderungen an der S3-Bucket-Richtlinie vorhanden sind. Weitere Informationen zur Prüfung dieser Kontrolle finden Sie im Dokument CIS Amazon Web Services Foundations Benchmark Version 1.4.0, das unter https://www.cisecurity verfügbar ist. org/benchmark/amazon_web_services/

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
4.12	Sicherstellen, dass ein Protokollmetrikfilter und ein Alarm für Änderungen an Network-Gateways vorhanden sind	alarm-vpc-network-gateway-ändern (Prozessprüfung)	Stellen Sie sicher, dass ein Protokoll metrikfilter und ein Alarm für Änderungen an Network-Gateways vorhanden sind. Weitere Informationen zur Prüfung dieser Kontrolle finden Sie im Dokument CIS Amazon Web Services Foundations Benchmark Version 1.4.0, das unter https://www.cisecurity verfügbar ist. org/benchmark/amazon_web_services/

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
4.13	Sicherstellen, dass ein Protokollmetrikfilter und ein Alarm für Änderungen an der Routing-Tabelle vorhanden sind	alarm-vpc-route-table-ändern (Prozessprüfung)	Stellen Sie sicher, dass ein Protokollmetrikfilter und ein Alarm für Änderungen an der Routing-Tabelle vorhanden sind. Weitere Informationen zur Prüfung dieser Kontrolle finden Sie im Dokument CIS Amazon Web Services Foundations Benchmark Version 1.4.0, das unter https://www.cisecurity verfügbar ist. org/benchmark/amazon_web_services/

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
4,14	Sicherstellen, dass ein Protokollmetrikfilter und ein Alarm für VPC-Änderungen vorhanden sind	alarm-vpc-change (Prozessüberprüfung)	Stellen Sie sicher, dass ein Protokoll metrikfilter und ein Alarm für Änderungen an der Amazon Virtual Private Cloud (VPC) vorhanden sind. Weitere Informationen zur Prüfung dieser Kontrolle finden Sie im Dokument CIS Amazon Web Services Foundations Benchmark Version 1.4.0, das unter https://www.cisecurity verfügbar ist. org/benchmark/amazon_web_services/

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
4,15	Sicherstellen, dass ein Protokollmetrikfilter und ein Alarm für Änderungen an AWS Organizations vorhanden sind	alarm-organizations-change (Prozessüberprüfung)	Stellen Sie sicher, dass ein Protokollmetrikfilter und ein Alarm für Änderungen an AWS Organizations vorhanden sind. Weitere Informationen zur Prüfung dieser Kontrolle finden Sie im Dokument CIS Amazon Web Services Foundations Benchmark Version 1.4.0, das unter https://www.cisecurity verfügbar ist. org/benchmark/amazon_web_services/

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
5.1	Stellen Sie sicher, dass das Netzwerk keinen Zugriff von 0.0.0.0/0 zu den Verwaltungsports des Remoteservers ACLs zulässt	nacl-no-unrestricted-ssh-rdp	Stellen Sie sicher, dass kein Netzwerk öffentlichen ACLs Zugriff auf die Verwaltungsports des Remoteser vers zulässt. Stellen Sie sicher, dass im VPC-Bereich der Konsole ein Netzwerk ACLs mit der Quelle '0.0.0.0/ 0' vorhanden ist, die Ports oder Portberei che zulassen, einschließlich Remote-Server-Admi n-Ports. Weitere Informationen zur Prüfung dieser Kontrolle finden Sie im Dokument CIS Amazon Web Services Foundations Benchmark Version 1.4.0, das unter https://www.cisecu rity verfügbar ist. org/ benchmark/amaz on_web_services/

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
5.2	Sicherstellen, dass keine Sicherhei tsgruppen den Zugang von 0.0.0.0/0 zu Remoteserver-Verwaltungsports zulassen	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) Security Groups können bei der Verwaltung des Netzwerkzugriffs helfen, indem sie eine statusbeh aftete Filterung von eingehendem und ausgehendem Netzwerkverkehr zu Ressourcen bereitste llen. AWS Wenn Sie eingehenden (oder entfernten) Datenverk ehr von 0.0.0.0/0 bis Port 22 auf Ihren Ressourcen nicht zulassen, können Sie den Remote-Zugriff einschränken.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
5.2	Sicherstellen, dass keine Sicherheitsgruppen den Zugang von 0.0.0.0/0 zu Remoteserver-Verwaltungsports zulassen	restricted-common-ports	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass gemeinsame Ports für Amazon Elastic Compute Cloud (Amazon EC2) -Sicherheitsgruppen eingeschränkt sind. Wenn der Zugriff auf Ports nicht auf vertrauenswürdige Quellen beschränkt wird, kann dies zu Angriffen auf die Verfügbarkeit, Integrität und Vertraulichkeit von Systemen führen. Mit dieser Regel können Sie optional die Parameter BlockedPort1–BlockedPort5 festlegen (CIS-Standardwert: 3389). Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Vorlage

Die Vorlage ist verfügbar unter GitHub: Operational Best Practices for CIS AWS Foundations Benchmark v1.4 Level 1.

Best Practices für den Betrieb von CIS AWS Foundations Benchmark v1.4 Level 2

Konformitätspakete bieten ein allgemeines Compliance-Framework, das es Ihnen ermöglicht, mithilfe verwalteter oder benutzerdefinierter AWS Config Regeln und Abhilfemaßnahmen Kontrollen zur Sicherheits-, Betriebs- oder Kostenoptimierung durchzuführen. AWS Config Conformance Packs dienen als Beispielvorlagen nicht dazu, die vollständige Einhaltung eines bestimmten Governance- oder Compliance-Standards sicherzustellen. Sie sind dafür verantwortlich, selbst zu beurteilen, ob Ihre Nutzung der Services den geltenden gesetzlichen und behördlichen Anforderungen entspricht.

Im Folgenden finden Sie ein Beispiel für eine Zuordnung zwischen dem Center for Internet Security (CIS) Amazon Web Services Foundation v1.4 Level 2 und AWS verwalteten Konfigurationsregeln/Prozessprüfungen AWS Config . Jede Config-Regel gilt für eine bestimmte AWS Ressource und bezieht sich auf eine oder mehrere CIS Amazon Web Services Foundation v1.4 Level 2-Steuerelemente. Eine CIS-Amazon-Web-Services-Foundation-v1.4-Level-2-Kontrolle kann mit mehreren Config-Regeln verknüpft werden. In der folgenden Tabelle finden Sie weitere Informationen und Anleitungen zu diesen Zuordnungen.

Weitere Informationen zu Prozessprüfungen finden Sie unter Prozessprüfungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
1.1	Verwalten der aktuellen Kontaktdaten	account-contact-details-configured (Prozessüberprüfung)	Stellen Sie sicher, dass die Kontakt-E-Mail-Adresse und Telefonnummer für AWS -Konten aktuell und mehr als einer Person in Ihrer Organisation zugeordnet sind. Stellen Sie sicher,

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			dass im Bereich „Mein Konto“ der Konsole im Abschnitt „Kontaktinformationen“ die richtigen Informationen angegeben sind. Weitere Informationen zur Prüfung dieser Kontrolle finden Sie im Dokument CIS Amazon Web Services Foundations Benchmark Version 1.4.0, das unter https://www.cisecurity verfügbar ist. org/benchmark/amazon_web_services/

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
1.2	Sicherstellen, dass Kontaktdaten für Sicherheitsfragen registriert sind	account-security-contact-configured (Prozessüberprüfung)	Stellen Sie sicher, dass die Kontakt-E-Mail-Adresse und die Telefonnummer des Sicherheitsteams Ihres Unternehmens aktuell sind. Stellen Sie sicher, dass im Bereich „Mein Konto“ der AWS Management-Konsole im Bereich Sicherheit die richtigen Informationen angegeben sind. Weitere Informationen zur Prüfung dieser Kontrolle finden Sie im Dokument CIS Amazon Web Services Foundations Benchmark Version 1.4.0, das unter https://www.cisecurity verfügbar ist. org/benchmark/amazon_web_services/

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
1.4	Sicherstellen, dass kein Root-Benutzerzugriffsschlüssel vorhanden ist	iam-root-access-key-überprüfen	Der Zugriff auf Systeme und Ressourcen kann gesteuert werden, indem überprüft wird, ob der Root-Benutzer keine Zugriffsschlüssel mit seiner AWS Identity and Access Management (IAM) -Rolle verknüpft hat. Stellen Sie sicher, dass die Root-Zugriffsschlüssel gelöscht werden. Erstellen und verwenden Sie stattdessen rollenbasierte Funktionen, AWS-Konten um das Prinzip der geringsten Funktionalität zu berücksichtigen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
1.5	Sicherstellen, dass MFA für den Root-Benutzer aktiviert ist	root-account-mfa-enabled	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass MFA für den Root-Benutzer aktiviert ist. Der Stammbenutzer ist der AWS-Konto-Benutzer mit den meisten Berechtigungen. MFA bietet eine weitere Schutzebene zusätzlich zum Benutzernamen und Passwort. Indem Sie MFA für den Root-Benutzer vorschreiben, können Sie die Anzahl AWS-Konten kompromittierter Benutzer reduzieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
1,6	Sicherstellen, dass MFA für den Root-Benutzer aktiviert ist	root-account-hardware-mfa-aktiviert	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Hardware-MFA für den Root-Benutzer aktiviert ist. Der Stammbenutzer ist der AWS-Konto-Benutzer mit den meisten Berechtigungen. MFA sorgt für eine weitere Schutzebene zusätzlich zu den Anmeldeinformationen. Indem Sie MFA für den Root-Benutzer vorschreiben, können Sie die Anzahl AWS-Konten kompromittierter Benutzer reduzieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
1,7	Beseitigen der Verwendung des Root-Benutzers für administrative und tägliche Aufgaben	root-account-regular-use (Prozessüberprüfung)	Stellen Sie sicher, dass das Root-Konto nicht für alltägliche Aufgaben verwendet wird. Führen Sie in IAM einen Anmeldeinformationsbericht aus, um zu untersuchen, wann der Root-Benutzer zuletzt verwendet wurde. Weitere Informationen zur Prüfung dieser Kontrolle finden Sie im Dokument CIS Amazon Web Services Foundations Benchmark Version 1.4.0, das unter https://www.cisecurity verfügbar ist. org/benchmark/amazon_web_services/

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
1.8	Sicherstellen, dass die IAM-Passwortrichtlinie eine Mindestlänge von 14 Zeichen oder mehr erfordert	iam-password-policy	Die Identitäten und Anmeldeinformationen werden auf der Grundlage einer organisatorischen IAM-Passwortrichtlinie ausgestellt, verwaltet und verifiziert. Sie erfüllen oder übertreffen die Anforderungen von NIST SP 800-63 und dem Standard „Best Practices“ von AWS Foundational Security für die Passwortstärke. Mit dieser Regel können Sie optional RequireUppercaseCharacters (Wert für AWS grundlegende Sicherheitsbewährte Methoden: wahr), RequireLowercaseCharacters (Wert für bewährte Methoden für AWS grundlegende Sicherheit: wahr), RequireSymbols (Wert für bewährte Methoden für AWS grundlegende Sicherheit:

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			wahr), RequireNumbers (Wert für bewährte Methoden für AWS grundlegende Sicherheit: wahr), MinimumPasswordLength (Wert für bewährte Methoden für AWS grundlegende Sicherheit: 14), PasswordReusePrevention (Wert für bewährte Methoden für AWS grundlegende Sicherheit: 24) und MaxPasswordAge (Wert für bewährte Methoden für AWS grundlegende Sicherheit: 90) für Ihr IAM festlegen. Kennwortrichtlinie. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
1.9	Sicherstellen, dass die IAM-Passw ortrichtlinie die Wiederverwendung von Passwörtern verhindert	iam-password-policy	Die Identitäten und Anmeldeinformation en werden auf der Grundlage einer organisatorischen IAM-Passwortrichtlinie ausgestellt, verwaltet und verifiziert. Sie erfüllen oder übertreff en die Anforderungen von NIST SP 800-63 und dem Standard „Best Practices“ von AWS Foundatio nal Security für die Passwortstärke. Mit dieser Regel können Sie optional RequireUppercaseCh aracters (Wert für AWS grundlegende Sicherheitsbewährt e Methoden: wahr), RequireLowercaseCh aracters (Wert für bewährte Methoden für AWS grundlege nde Sicherheit: wahr), RequireSy mbols (Wert für bewährte Methoden für AWS grundlege nde Sicherheit:

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			wahr), RequireNumbers (Wert für bewährte Methoden für AWS grundlegende Sicherheit: wahr), MinimumPasswordLength (Wert für bewährte Methoden für AWS grundlegende Sicherheit: 14), PasswordReusePrevention (Wert für bewährte Methoden für AWS grundlegende Sicherheit: 24) und MaxPasswordAge (Wert für bewährte Methoden für AWS grundlegende Sicherheit: 90) für Ihr IAM festlegen. Kennwortrichtlinie. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
1.10	Sicherstellen, dass für alle Benutzer mit Konsolenpasswort die Multi-Faktor-Authentifizierung (MFA) aktiviert ist	mfa-enabled-for-iam-Konsolenzugriff	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass MFA für alle AWS Identity and Access Management (IAM) -Benutzer aktiviert ist, die über ein Konsolenkennwort verfügen. MFA sorgt für eine weitere Schutzebene zusätzlich zu den Anmeldeinformationen. Indem Sie MFA für Benutzer vorschreiben, können Sie Fälle kompromittierter Konten reduzieren und verhindern, dass unbefugte Benutzer auf vertrauliche Daten zugreifen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
1.11	Kein Einrichten von Zugangssc hlüsseln bei der Ersteinrichtung für alle Benutzer mit Konsolenpasswort	iam-user-console-and- api-access-at-creation (Prozessü berprüfung)	Stellen Sie sicher, dass bei der Ersteinrichtung für alle Benutzer mit Konsolenpasswort keine Zugangssc hlüssel eingerichtet werden. Vergleichen Sie für alle Benutzer mit Konsolenzugriff die Erstellungszeit des Benutzers mit dem Erstellungsdatum des Zugriffsschlüssels . Weitere Informati onen zur Prüfung dieser Kontrolle finden Sie im Dokument CIS Amazon Web Services Foundations Benchmark Version 1.4.0, das unter https://www.cisecu rity verfügbar ist. org/ benchmark/amaz on_web_services/

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
1.12	Sicherstellen, dass Anmeldeinformationen, die 45 Tage oder länger nicht verwendet wurden, deaktiviert werden	iam-user-unused-credentials-überprüfen	AWS Identity and Access Management (IAM) kann Ihnen bei Zugriffsberechtigungen und Autorisierungen helfen, indem es nach IAM-Passwörtern und Zugriffsschlüsseln sucht, die für einen bestimmten Zeitraum nicht verwendet wurden. Wenn ungenutzte Anmeldeinformationen identifiziert werden, müssen Sie sie deaktivieren und/oder entfernen, da dies gegen das Prinzip der geringsten Berechtigung verstoßen könnte. Für diese Regel müssen Sie einen Wert für das maxCredentialUsageAlter festlegen (CIS-Standardwert: 45). Der tatsächliche Wert muss den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
1.13	Sicherstellen, dass für jeden Benutzer nur ein aktiver Zugriffss chlüssel verfügbar ist	iam-user-single-ac cess-Taste (Prozessp rüfung)	Stellen Sie sicher, dass für jeden einzelnen Benutzer nur ein aktiver Zugriffsschlüssel verfügbar ist. Stellen Sie für alle Benutzer sicher, dass auf der Registerkarte Sicherheitsanmelde informationen für jeden Benutzer in IAM nur ein aktiver Schlüssel verwendet wird. Weitere Informati onen zur Prüfung dieser Kontrolle finden Sie im Dokument CIS Amazon Web Services Foundations Benchmark Version 1.4.0, das unter https://www.cisecu rity verfügbar ist. org/ benchmark/amaz on_web_services/

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
1.14	Sicherstellen, dass die Zugriffsschlüssel spätestens alle 90 Tage rotiert werden	access-keys-rotated	Die Anmeldein formationen für autorisierte Geräte, Benutzer und Prozesse werden geprüft, indem sichergestellt wird, dass die IAM-Zugri ffsschlüssel gemäß den Vorgaben der Unternehmensrichtl inie rotiert werden. Das regelmäßi ge Ändern der Zugriffsschlüssel ist eine bewährte Sicherheitsmethode . Es verkürzt den Zeitraum, in dem ein Zugriffsschlüssel aktiv ist, und reduziert die Auswirkungen auf das Unternehmen, wenn die Schlüssel kompromittiert werden. Diese Regel erfordert einen Wert für die Zugriffsschlüssel-Rotation (Standard konfiguration: 90). Der tatsächliche Wert muss den Richtlini

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			en Ihrer Organisation entsprechen.
1.15	Sicherstellen, dass Benutzer Berechtigungen nur über Gruppen erhalten	iam-user-no-policies-überprüfen	Diese Regel stellt sicher, dass AWS Identity and Access Management (IAM) -Richtlinien nur Gruppen oder Rollen zugewiesen werden, um den Zugriff auf Systeme und Ressourcen zu kontrollieren. Die Zuweisung von Berechtigungen auf Gruppen- oder Rollenebene trägt dazu bei, die Wahrscheinlichkeit zu verringern, dass eine Identität übermäßige Berechtigungen erhält oder beibehält.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
1.15	Sicherstellen, dass Benutzer Berechtigungen nur über Gruppen erhalten	iam-no-inline-policy-überprüfen	Stellen Sie sicher, dass ein Benutzer, eine IAM-Rolle oder eine IAM-Gruppe (AWS Identity and Access Management) nicht über eine Inline-Richtlinie zur Zugriffskontrolle auf Systeme und Ressourcen verfügt. AWS empfiehlt, verwaltete Richtlinien anstelle von Inline-Richtlinien zu verwenden. Verwaltete Richtlinien ermöglichen Wiederverwendbarkeit, Versionsverwaltung, Rollback und Delegierung der Berechtigungsverwaltung.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
1.15	Sicherstellen, dass Benutzer Berechtigungen nur über Gruppen erhalten	iam-user-group-membership-überprüfen	AWS Identity and Access Management (IAM) kann Ihnen helfen, Zugriffsberechtigungen und Autorisierungen einzuschränken, indem sichergestellt wird, dass Benutzer Mitglieder mindestens einer Gruppe sind. Wenn Benutzern mehr Berechtigungen eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und Aufgabentrennung verstoßen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
1.16	Sicherstellen, dass keine IAM-Richtlinien angehängt werden, die vollständige Administratorrechte (*:*) zulassen	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) kann Ihnen dabei helfen, die Prinzipien der geringsten Rechte und der Aufgabentrennung in Zugriffsberechtigungen und Autorisierungen zu integrieren und zu verhindern, dass Richtlinien „Effect“: „Allow“ mit „Action“: „*“ anstelle von „Resource“: „*“ enthalten. Wenn Benutzern mehr Rechte eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und der Aufgabentrennung verstoßen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
1,17	Stellen Sie sicher, dass eine Support-Rolle eingerichtet wurde, um Vorfälle mit AWS Support zu verwalten	iam-policy-in-use	AWS Identity and Access Managemen t (IAM) kann Sie bei der Verwaltung von Zugriffsberechtigu ngen und Autorisie rungen unterstützen, indem sichergestellt wird, dass IAM-Richt linien den entsprech enden Benutzern, Rollen oder Gruppen zugewiesen werden. Die Einschränkung dieser Richtlinien beinhaltet auch die Prinzipien der geringsten Berechtigung und der Aufgabent rennung. Diese Regel erfordert, dass Sie das policyARN auf arn:aws:iam: AWSSupport :aws:poli cy/ Access setzen, um das Vorfallma nagement mit Support zu ermöglichen. AWS

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
1.18	Stellen Sie sicher, dass IAM-Instanzrollen für den AWS Ressourcenzugriff von Instanzen aus verwendet werden	ec2- instance-profile-attached	EC2 Instanzprofile übergeben eine IAM-Rolle an eine Instanz EC2 . Das Anhängen eines Instance-Profils an Ihre Instances kann bei der Implementierung von geringsten Berechtigungen und der Berechtigungsverwaltung helfen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
1.19	Sicherstellen, dass alle abgelaufenen SSL/TLS-Zertifikate, die in AWS IAM gespeichert sind, entfernt werden	iam-expired-certificates (Prozessüberprüfung)	Stellen Sie sicher, dass alle abgelaufenen SSL/TLS-Zertifikate, die in IAM gespeichert sind, entfernt werden. Führen Sie in der Befehlszeile mit der installierten AWS CLI den Befehl „AWS iam list-server-certificates“ aus und ermitteln Sie, ob abgelaufene Serverzertifikate vorhanden sind. Weitere Informationen zur Prüfung dieser Kontrolle finden Sie im Dokument CIS Amazon Web Services Foundations Benchmark Version 1.4.0, das unter https://www.cisecurity verfügbar ist. org/benchmark/amazon_web_services/

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
1,20	Stellen Sie sicher, dass AWS IAM Access Analyzer aktiviert ist	iam-access-analyzer-enabled (Prozessüberprüfung)	Stellen Sie sicher, dass IAM Access Analyzer aktiviert ist. Wählen Sie im IAM-Bereich der Konsole „Zugriffs-Analyzer“ aus und stellen Sie sicher, dass der STATUS auf „Aktiv“ gesetzt ist. Weitere Informationen zur Prüfung dieser Kontrolle finden Sie im Dokument CIS Amazon Web Services Foundations Benchmark Version 1.4.0, das unter https://www.cisecurity verfügbar ist. org/benchmark/amazon_web_services/

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
1,21	Stellen Sie sicher, dass Benutzer zentral über den Identitätsverbund oder AWS Organizations für Umgebungen mit mehreren Konten verwaltet werden	account-part-of-organizations	Durch die zentrale Verwaltung AWS-Konten innerhalb von AWS Organizations wird sichergestellt, dass die Konten den Vorschriften entsprechen. Eine fehlende zentrale Kontoverwaltung kann zu inkonsistenten Kontokonfigurationen führen, wodurch Ressourcen und sensible Daten offengelegt werden können.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
2.1.1	Stellen Sie sicher, dass alle S3-Buckets verwendet werden encryption-at-rest	s3-aktiviert bucket-server-side-encryption	Zum Schutz von Daten im Ruhezustand müssen Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon Simple Storage Service (Amazon S3)-Buckets aktiviert ist. Um eventuell vorhandene sensible Daten im Ruhezustand in Amazon-S3-Buckets zu schützen, muss die Verschlüsselung aktiviert sein.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
2.1.2	Sicherstellen, dass die S3-Bucket-Richtlinie so eingestellt ist, dass HTTP-Anfragen abgelehnt werden	s-3 bucket-ssl-requests-only	Um Daten während der Übertragung zu schützen, stellen Sie sicher, dass Ihre Amazon Simple Storage Service (Amazon S3)-Buckets Anfragen zur Verwendung von Secure Socket Layer (SSL)-Buckets erfordern. Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
2.1.3	Sicherstellen, dass die MFA-Lösch funktion für S3-Bucket s aktiviert ist	s-3 bucket-versioning-enabled	Mit der Versionsv erwaltung von Amazon-Simple-Storage-Servi ce (Amazon-S3)-Buckets können Sie mehrere Varianten eines Objekts im selben Amazon-S3 -Bucket speichern. Das Hinzufügen der Multi-Faktor-Authe ntifizierung (MFA)-Lös chfunktion zu einem S3-Bucket erfordert einen zusätzlichen Authentifizierungs faktor, um den Versionsstatus Ihres Buckets zu ändern oder eine Objektver sion zu löschen. Die MFA-Löschfunktion kann eine zusätzlic he Sicherheitsebene für den Fall hinzufüge n, dass Sicherhei tsanmeldeinformati onen kompromit tiert oder unbefugte Zugriffe gewährt werden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
2.1.5	Sicherstellen, dass S3-Buckets mit „Öffentlichen Zugriff blockieren (Bucket-Einstellungen)“ konfiguriert sind	s3- account-level-public-access -blöcke-periodisch	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Simple Storage Service (Amazon S3) -Buckets nicht öffentlich zugänglich sind. Diese Regel trägt dazu bei, sensible Daten vor unbefugten Remote-Benutzern zu schützen, indem sie den öffentlichen Zugriff verhindert. Mit dieser Regel können Sie optional die Parameter ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) und restrictPublicBuckets Parameter (Config Default: True) festlegen. Die tatsächlichen Werte müssen den Richtlini

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			en Ihrer Organisation entsprechen.
2.1.5	Sicherstellen, dass S3-Buckets mit „Öffentlichen Zugriff blockieren (Bucket-Einstellungen)“ konfiguriert sind	s3 bucket-level-public-access - verboten	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Simple Storage Service (Amazon S3) -Buckets nicht öffentlich zugänglich sind. Diese Regel trägt dazu bei, sensible Daten vor unbefugten Remote-Benutzern zu schützen, indem sie den öffentlichen Zugriff auf Bucket-Ebene verhindert.
2.2.1	Sicherstellen, dass die EBS-Volume-Verschlüsselung aktiviert ist	encrypted-volumes	Aktivieren Sie die Verschlüsselung für Ihre Amazon-Elastic-Block-Store (Amazon-EBS)-Volumes, um eventuell vorhandene sensible Daten sowie Daten im Ruhezustand zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
2.2.1	Sicherstellen, dass die EBS-Volume-Verschlüsselung aktiviert ist	ec2- ebs-encryption-by-default	Zum Schutz von Daten im Ruhezustand müssen Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon Elastic Block Store (Amazon EBS)-Volumes aktiviert ist. Da sensible Daten auch im Ruhezustand vorhanden sein können, sollten Sie die Verschlüsselung im Ruhezustand aktivieren, um diese Daten zu schützen.
2.3.1	Sicherstellen, dass die Verschlüsselung für RDS-Instances aktiviert ist	rds-snapshot-encrypted	Stellen Sie sicher, dass die Verschlüsselung für Ihre Amazon Relational Database Service (Amazon RDS)-Snapshots aktiviert ist. Da sensible Daten auch im Ruhezustand vorhanden sein können, sollten Sie die Verschlüsselung im Ruhezustand aktivieren, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
2.3.1	Sicherstellen, dass die Verschlüsselung für RDS-Instances aktiviert ist	rds-storage-encrypted	Zum Schutz von Daten im Ruhezustand müssen Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon Relational Database Service (Amazon RDS)-Instances aktiviert ist. Um eventuell vorhandene sensible Daten im Ruhezustand in Amazon-RDS-Instances zu schützen, muss die Verschlüsselung von Daten im Ruhezustand aktiviert sein.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.1	Stellen Sie sicher CloudTrail , dass es in allen Regionen aktiviert ist	multi-region-cloudtrail-enabled	AWS CloudTrail zeichnet Aktionen und API-Aufrufe der AWS Management Console auf. Sie können feststellen, welche Benutzer und Konten angerufen wurden AWS, von welcher Quell-IP-Adresse aus die Anrufe getätigt wurden und wann die Anrufe erfolgten. CloudTrail übermittelt Protokolldateien aus allen AWS Regionen an Ihren S3-Bucket , wenn MULTI_REGION_CLOUD_TRAIL_ENABLED aktiviert ist. Außerdem wird beim AWS Start einer neuen Region derselbe Trail in der neuen Region erstellt. CloudTrail Dadurch erhalten Sie automatisch Protokolldateien mit API-Aktivitäten für die neue Region.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.2	Stellen CloudTrai l Sie sicher, dass die Überprüfung der Protokolldatei aktiviert ist	cloud-trail-log-file-Validierung aktiviert	Verwenden Sie die AWS CloudTrail Protokolldateivali dierung, um die Integrität von Protokoll en zu überprüfen. CloudTrail Mithilfe der Protokolldateivali dierung kann festgestellt werden, ob eine Protokoll datei geändert oder gelöscht wurde oder ob sie nach der Übermittlung CloudTrail unverände rt geblieben ist. Dieses Feature wurde mit dem Branchens tandard entsprech enden Algorithmen entwickelt: SHA-256 für die Hashfunktion und SHA-256 mit RSA für digitale Signature n. Aus diesem Grund ist es rechnerisch unmöglich, CloudTrai l Protokolldateien unbemerkt zu ändern, zu löschen oder zu fälschen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.3	Stellen Sie sicher, dass der zum Speichern von CloudTrail Protokoll en verwendete S3-Bucket nicht öffentlich zugänglich ist	s-3 bucket-public-read -prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie nur autorisierten Benutzern, Prozessen und Geräten Zugriff auf Amazon Simple Storage Service (Amazon S3) - Buckets gewähren. Die Verwaltung des Zugriffs sollte mit der Klassifizierung der Daten übereinst immen.
3.3	Stellen Sie sicher, dass der zum Speichern von CloudTrail Protokoll en verwendete S3-Bucket nicht öffentlich zugänglich ist	s-3 bucket-public-writ e-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie nur autorisierten Benutzern, Prozessen und Geräten Zugriff auf Amazon Simple Storage Service (Amazon S3) - Buckets gewähren. Die Verwaltung des Zugriffs sollte mit der Klassifizierung der Daten übereinst immen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.3	Stellen Sie sicher, dass der zum Speichern von CloudTrail Protokoll en verwendete S3-Bucket nicht öffentlich zugänglich ist	s3 bucket-level-public-access - verboten	Verwalten Sie den Zugriff auf Ressource n in der AWS Cloud, indem Sie sicherste llen, dass Amazon Simple Storage Service (Amazon S3) -Buckets nicht öffentlich zugänglic h sind. Diese Regel trägt dazu bei, sensible Daten vor unbefugten Remote-Benutzern zu schützen, indem sie den öffentlichen Zugriff auf Bucket-Eb ene verhindert.
3.4	Stellen Sie sicher, dass die CloudTrai l Pfade in Logs integriert CloudWatch sind	cloud-trail-cloud-watch-Logs aktiviert	Verwenden Sie Amazon CloudWatc h , um Protokoll ereignisaktivitäten zentral zu sammeln und zu verwalten. Die Aufnahme von AWS CloudTrail Daten liefert Einzelheiten zu den API-Aufrufaktivitä ten in Ihrem AWS-Konto.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.5	Stellen Sie sicher, dass AWS Config in allen Regionen aktiviert ist	config-enabled-all-regions (Prozessüberprüfung)	Stellen Sie sicher, dass AWS Config in allen AWS Regionen aktiviert ist. Stellen Sie im AWS Config-Bereich der Konsole für jede aktivierte Region sicher, dass der AWS Config-Recorder korrekt konfiguriert ist. Stellen Sie sicher, dass die Aufzeichnung globaler AWS -Ressourcen in mindestens einer Region aktiviert ist. Weitere Informationen zur Prüfung dieser Kontrolle finden Sie im Dokument CIS Amazon Web Services Foundations Benchmark Version 1.4.0, das unter https://www.cisecurity verfügbar ist. org/benchmark/amazon_web_services/

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.6	Stellen Sie sicher, dass die Protokoll ierung des S3-Bucket -Zugriffs auf dem S3-Bucket aktiviert ist CloudTrail	s-3 bucket-logging-enabled	Die Amazon Simple Storage Service (Amazon S3)-Serverzugriffs protokollierung bietet eine Methode zur Überwachu ng des Netzwerks im Hinblick auf potenzielle Cybersich erheitsereignisse. Die Ereignisse werden überwacht, indem detaillierte Aufzeichn ungen über die Anfragen erfasst werden, die an einen Amazon-S3-Bucket gestellt wurden. Jeder Zugriffsprotokolle intrag enthält Details zu einer einzelnen Zugriffsanfrage. Zu den Details gehören Anforderer, Bucket-Name, Anforderu ngszeit, Anforderu ngsaktion, Antwortst atus und Fehlercode, falls relevant.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.7	Stellen Sie sicher, dass CloudTrai l Protokolle im Ruhezustand mit KMS verschlüsselt sind CMKs	cloud-trail-encryption-enabled	Zum Schutz von eventuell vorhanden en sensiblen Daten sowie Daten im Ruhezustand müssen Sie sicherstellen, dass die Verschlüs selung für Ihre AWS CloudTrail aktiviert ist.
3.8	Stellen Sie sicher, dass die Rotation für vom Kunden erstellte CMKs Benutzer aktiviert ist	cmk-backing-key-ro tation-aktiviert	Aktivieren Sie die Schlüsselrotation, um sicherzustellen, dass Schlüssel rotiert werden, sobald sie das Ende ihrer Kryptoperiode erreicht haben.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.9	Stellen Sie sicher, dass die VPC-Flow-Protokollierung in allen aktiviert ist VPCs	vpc-flow-logs-enabled	VPC-Flow-Protokolle erfassen detaillierte Informationsdatensätze über den IP-Datenverkehr, der zu und von Netzwerkschnittstellen in Ihrer Amazon Virtual Private Cloud (Amazon VPC) fließt. Standardmäßig enthalten Flow-Protokolldatensätze Werte für die verschiedenen Komponenten des IP-Flows, einschließlich Quelle, Ziel und Protokoll.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.10	Sicherstellen, dass die Protokollierung auf Objektebene für Schreibereignisse für den S3-Bucket aktiviert ist	cloudtrail-s3-data events-enabled	Die Erfassung von Simple Storage Service (Amazon S3)-Datenereigniss en unterstützt die Erkennung von ungewöhnlichen Aktivitäten. Zu den Details gehören Informationen zu dem AWS -Konto, das auf einen Amazon-S3-Bucket zugegriffen hat, die IP-Adresse und die Uhrzeit des Ereignisses.
3,11	Sicherstellen, dass die Protokollierung auf Objektebene für Schreibereignisse für den S3-Bucket aktiviert ist	cloudtrail-s3-data events-enabled	Die Erfassung von Simple Storage Service (Amazon S3)-Datenereigniss en unterstützt die Erkennung von ungewöhnlichen Aktivitäten. Zu den Details gehören Informationen zu dem AWS -Konto, das auf einen Amazon-S3-Bucket zugegriffen hat, die IP-Adresse und die Uhrzeit des Ereignisses.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
4.1	Sicherstellen, dass ein Protokollmetrikfilter und ein Alarm für nicht autorisierte API-Aufrufe vorhanden sind	alarm-unauthorized-api-calls (Prozessüberprüfung)	Stellen Sie sicher, dass ein Protokollmetrikfilter und ein Alarm für nicht autorisierte API-Aufrufe vorhanden sind. Weitere Informationen zur Prüfung dieser Kontrolle finden Sie im Dokument CIS Amazon Web Services Foundations Benchmark Version 1.4.0, das unter https://www.cisecurity verfügbar ist. org/benchmark/amazon_web_services/

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
4.2	Sicherstellen, dass ein Protokollmetrikfilter und ein Alarm für die Anmeldung in der Managementkonsole ohne MFA vorhanden sind	alarm-sign-in-without-mfa (Prozessüberprüfung)	Stellen Sie sicher, dass ein Protokollmetrikfilter und ein Alarm für die Anmeldung bei der AWS Management Console ohne Multi-Faktor-Authentifizierung (MFA) vorhanden sind. Weitere Informationen zur Prüfung dieser Kontrolle finden Sie im Dokument CIS Amazon Web Services Foundations Benchmark Version 1.4.0, das unter https://www.cisecurity verfügbar ist. org/benchmark/amazon_web_services/

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
4.3	Sicherstellen, dass ein Protokollmetrikfilter und ein Alarm für die Verwendung des Root-Kontos vorhanden sind	alarm-root-account-use (Prozessüberprüfung)	Stellen Sie sicher, dass ein Protokollmetrikfilter und ein Alarm für die Verwendung des Root-Kontos vorhanden sind. Weitere Informationen zur Prüfung dieser Kontrolle finden Sie im Dokument CIS Amazon Web Services Foundations Benchmark Version 1.4.0, das unter https://www.cisecurity verfügbar ist. org/benchmark/amazon_web_services/

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
4.4	Sicherstellen, dass ein Protokollmetrikfilter und ein Alarm für Änderungen an der IAM-Richtlinie vorhanden sind	alarm-iam-policy-change (Prozessüberprüfung)	Stellen Sie sicher, dass ein Protokollmetrikfilter und ein Alarm für Änderungen an der IAM-Richtlinie vorhanden sind. Weitere Informationen zur Prüfung dieser Kontrolle finden Sie im Dokument CIS Amazon Web Services Foundations Benchmark Version 1.4.0, das unter https://www.cisecurity verfügbar ist. org/benchmark/amazon_web_services/

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
4.5	Stellen Sie sicher, dass ein Log-Metrikfilter und ein Alarm für CloudTrail Konfigurationsänderungen vorhanden sind	alarm-cloudtrail-config-change (Prozessüberprüfung)	Stellen Sie sicher, dass ein Log-Metrikfilter und ein Alarm für AWS Cloud Trail Konfigurationsänderungen vorhanden sind. Weitere Informationen zur Prüfung dieser Kontrolle finden Sie im Dokument CIS Amazon Web Services Foundations Benchmark Version 1.4.0, das unter https://www.cisecurity verfügbar ist. org/benchmark/amazon_web_services/

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
4.6	Sicherstellen, dass ein Protokollmetrikfilter und ein Alarm für Authentifizierungsfehler in der AWS Management Console vorhanden sind	alarm-console-auth-failures (Prozessüberprüfung)	Stellen Sie sicher, dass ein Protokollmetrikfilter und ein Alarm für Authentifizierungsfehler in der AWS Management Console vorhanden sind. Weitere Informationen zur Prüfung dieser Kontrolle finden Sie im Dokument CIS Amazon Web Services Foundations Benchmark Version 1.4.0, das unter https://www.cisecurity verfügbar ist. org/benchmark/amazon_web_services/

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
4.7	Stellen Sie sicher, dass ein Log-Metrikfilter und ein Alarm vorhanden sind, um vom Kunden erstellte Dateien zu deaktivieren oder zu löschen CMKs	alarm-kms-disable-or-delete-cmk (Prozessprüfung)	Stellen Sie sicher, dass ein Log-Metrikfilter und ein Alarm zur Deaktivierung oder zum geplanten Löschen von vom Kunden erstellten Daten vorhanden sind. CMKs Weitere Informationen zur Prüfung dieser Kontrolle finden Sie im Dokument CIS Amazon Web Services Foundations Benchmark Version 1.4.0, das unter https://www.cisecurity verfügbar ist. org/benchmark/amazon_web_services/

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
4.8	Sicherstellen, dass ein Protokollmetrikfilter und ein Alarm für Änderungen an der S3-Bucket-Richtlinie vorhanden sind	alarm-s3- bucket-policy-change (Prozessüberprüfung)	Stellen Sie sicher, dass ein Protokollmetrikfilter und ein Alarm für Änderungen an der S3-Bucket-Richtlinie vorhanden sind. Weitere Informationen zur Prüfung dieser Kontrolle finden Sie im Dokument CIS Amazon Web Services Foundations Benchmark Version 1.4.0, das unter https://www.cisecurity verfügbar ist. org/benchmark/amazon_web_services/

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
4,9 bis 4,9	Stellen Sie sicher, dass ein Log-Metrikfilter und ein Alarm für AWS Konfigurationsänderungen vorhanden sind	alarm-aws-config-change (Prozessüberprüfung)	Stellen Sie sicher, dass ein Protokoll metrikfilter und ein Alarm für AWS -Config-Konfigurationsänderungen vorhanden sind. Weitere Informationen zur Prüfung dieser Kontrolle finden Sie im Dokument CIS Amazon Web Services Foundations Benchmark Version 1.4.0, das unter https://www.cisecurity verfügbar ist. org/benchmark/amazon_web_services/

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
4,10	Sicherstellen, dass ein Protokollmetrikfilter und ein Alarm für Änderungen an der Sicherheitsgruppe vorhanden sind	alarm-vpc-secrity-group-ändern (Prozessprüfung)	Stellen Sie sicher, dass ein Protokoll metrikfilter und ein Alarm für Änderungen an der Sicherheitsgruppe vorhanden sind. Weitere Informationen zur Prüfung dieser Kontrolle finden Sie im Dokument CIS Amazon Web Services Foundations Benchmark Version 1.4.0, das unter https://www.cisecurity verfügbar ist. org/benchmark/amazon_web_services/

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
4.11	Sicherstellen, dass ein Protokollmetrikfilter und ein Alarm für Änderungen an den Network Access Control Lists (NACL) vorhanden sind	alarm-vpc-nacl-change (Prozessüberprüfung)	Stellen Sie sicher, dass ein Protokollmetrikfilter und ein Alarm für Änderungen an den Network Access Control Lists (NACL) vorhanden sind. Weitere Informationen zur Prüfung dieser Kontrolle finden Sie im Dokument CIS Amazon Web Services Foundations Benchmark Version 1.4.0, das unter https://www.cisecurity verfügbar ist. org/benchmark/amazon_web_services/

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
4.12	Sicherstellen, dass ein Protokollmetrikfilter und ein Alarm für Änderungen an Network-Gateways vorhanden sind	alarm-vpc-network-gateway-ändern (Prozessprüfung)	Stellen Sie sicher, dass ein Protokoll metrikfilter und ein Alarm für Änderungen an Network-Gateways vorhanden sind. Weitere Informationen zur Prüfung dieser Kontrolle finden Sie im Dokument CIS Amazon Web Services Foundations Benchmark Version 1.4.0, das unter https://www.cisecurity verfügbar ist. org/benchmark/amazon_web_services/

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
4.13	Sicherstellen, dass ein Protokollmetrikfilter und ein Alarm für Änderungen an der Routing-Tabelle vorhanden sind	alarm-vpc-route-table-ändern (Prozessprüfung)	Stellen Sie sicher, dass ein Protokollmetrikfilter und ein Alarm für Änderungen an der Routing-Tabelle vorhanden sind. Weitere Informationen zur Prüfung dieser Kontrolle finden Sie im Dokument CIS Amazon Web Services Foundations Benchmark Version 1.4.0, das unter https://www.cisecurity verfügbar ist. org/benchmark/amazon_web_services/

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
4,14	Sicherstellen, dass ein Protokollmetrikfilter und ein Alarm für VPC-Änderungen vorhanden sind	alarm-vpc-change (Prozessüberprüfung)	Stellen Sie sicher, dass ein Protokoll metrikfilter und ein Alarm für Änderungen an der Amazon Virtual Private Cloud (VPC) vorhanden sind. Weitere Informationen zur Prüfung dieser Kontrolle finden Sie im Dokument CIS Amazon Web Services Foundations Benchmark Version 1.4.0, das unter https://www.cisecurity verfügbar ist. org/benchmark/amazon_web_services/

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
4,15	Sicherstellen, dass ein Protokollmetrikfilter und ein Alarm für Änderungen an AWS Organizations vorhanden sind	alarm-organizations-change (Prozessüberprüfung)	Stellen Sie sicher, dass ein Protokollmetrikfilter und ein Alarm für Änderungen an AWS Organizations vorhanden sind. Weitere Informationen zur Prüfung dieser Kontrolle finden Sie im Dokument CIS Amazon Web Services Foundations Benchmark Version 1.4.0, das unter https://www.cisecurity verfügbar ist. org/benchmark/amazon_web_services/

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
5.1	Stellen Sie sicher, dass das Netzwerk keinen Zugriff von 0.0.0.0/0 zu den Verwaltungsports des Remoteservers ACLs zulässt	nacl-no-unrestricted-ssh-rdp	Stellen Sie sicher, dass kein Netzwerk öffentlichen ACLs Zugriff auf die Verwaltungsports des Remoteser vers zulässt. Stellen Sie sicher, dass es im VPC-Berei ch der Konsole ein Netzwerk ACLs mit der Quelle '0.0.0.0/ 0' gibt, die Ports oder Portbereiche zulassen, einschlie ßlich Remote-Se rver-Admin-Ports. Weitere Informati onen zur Prüfung dieser Kontrolle finden Sie im Dokument CIS Amazon Web Services Foundations Benchmark Version 1.4.0, das unter https://www.cisecu rity verfügbar ist. org/ benchmark/amaz on_web_services/

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
5.2	Sicherstellen, dass keine Sicherhei tsgruppen den Zugang von 0.0.0.0/0 zu Remoteserver-Verwaltungsports zulassen	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) Security Groups können bei der Verwaltung des Netzwerkzugriffs helfen, indem sie eine statusbeh aftete Filterung von eingehendem und ausgehendem Netzwerkverkehr zu Ressourcen bereitste llen. AWS Wenn Sie eingehenden (oder entfernten) Datenverk ehr von 0.0.0.0/0 bis Port 22 auf Ihren Ressourcen nicht zulassen, können Sie den Remote-Zugriff einschränken.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
5.2	Sicherstellen, dass keine Sicherheitsgruppen den Zugang von 0.0.0.0/0 zu Remoteserver-Verwaltungsports zulassen	restricted-common-ports	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass gemeinsame Ports für Amazon Elastic Compute Cloud (Amazon EC2) -Sicherheitsgruppen eingeschränkt sind. Wenn der Zugriff auf Ports nicht auf vertrauenswürdige Quellen beschränkt wird, kann dies zu Angriffen auf die Verfügbarkeit, Integrität und Vertraulichkeit von Systemen führen. Mit dieser Regel können Sie optional die Parameter BlockedPort1–BlockedPort5 festlegen (CIS-Standardwert: 3389). Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
5.3	Sicherstellen, dass die Standards icherheitsgruppe jeder VPC den gesamten Datenverk ehr einschränkt	vpc-default-security-group-geschlossen	Sicherheitsgruppen von Amazon Elastic Compute Cloud (Amazon EC2) können bei der Verwaltung des Netzwerkzugriffs helfen, indem sie eine statusbehaftete Filterung des ein- und ausgehenden Netzwerkverkehrs zu Ressourcen bereitstellen. AWS Die Beschränk ung des gesamten Datenverkehrs auf die Standardsicherheit sgruppe hilft dabei, den Fernzugriff auf Ihre Ressourcen einzuschränken. AWS

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
5.4	Sicherstellen, dass Routing-Tabellen für VPC-Peering den „geringsten Zugriff“ haben	vpc-peering-least-access (Prozessprüfung)	Stellen Sie sicher, dass Routing-Tabellen für Amazon-VPC-Peering den „geringsten Zugriff“ haben. Überprüfen Sie im VPC-Bereich der Konsole die Einträge in der Routing-Tabelle, um sicherzustellen, dass die geringste Anzahl von Subnetzen oder Hosts, die zur Erfüllung des Peering-Zwecks erforderlich sind, routingfähig ist. Weitere Informationen zur Prüfung dieser Kontrolle finden Sie im Dokument CIS Amazon Web Services Foundations Benchmark Version 1.4.0, das unter https://www.cisecurity verfügbar ist. org/benchmark/amazon_web_services/

Vorlage

Die Vorlage ist verfügbar unter GitHub: Operational Best Practices for CIS AWS Foundations Benchmark v1.4 Level 2.

Bewährte Betriebspraktiken für kritische Sicherheitskontrollen der GUS v8 IG1

Konformitätspakete bieten ein allgemeines Compliance-Framework, das es Ihnen ermöglicht, mithilfe verwalteter oder benutzerdefinierter AWS Config Regeln und Abhilfemaßnahmen Kontrollen zur Sicherheits-, Betriebs- oder Kostenoptimierung durchzuführen. AWS Config Conformance Packs dienen als Beispielvorlagen nicht dazu, die vollständige Einhaltung eines bestimmten Governance- oder Compliance-Standards sicherzustellen. Sie sind dafür verantwortlich, selbst zu beurteilen, ob Ihre Nutzung der Services den geltenden gesetzlichen und behördlichen Anforderungen entspricht.

Im Folgenden finden Sie ein Beispiel für eine Zuordnung zwischen den Critical Security Controls v8 des Center for Internet Security (CIS) IG1 und den AWS verwalteten Konfigurationsregeln. Jede AWS Config bezieht sich auf eine bestimmte AWS Ressource und bezieht sich auf eine oder mehrere CIS Critical Security Controls IG1 v8-Steuerelemente. Ein CIS Critical Security Controls IG1 v8-Steuerelement kann sich auf mehrere AWS Config Regeln beziehen. In der folgenden Tabelle finden Sie weitere Informationen und Anleitungen zu diesen Zuordnungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
1.1	Einrichtung und Pflege eines detaillierten Inventars der Unternehmensressourcen	eip-attached	Diese Regel stellt sicher, dass Elastic, die einer Amazon Virtual Private Cloud (Amazon VPC) IPs zugewiesen sind, an Amazon Elastic Compute Cloud (Amazon EC2) - Instances oder verwendete Elastic Network Interface

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			s angehängt sind. Diese Regel hilft bei der Überwachung ungenutzter Inhalte EIPs in Ihrer Umgebung.
1.1	Einrichtung und Pflege eines detaillierten Inventars der Unternehmensressourcen	ec2-stopped-instance	Aktivieren Sie diese Regel, um bei der Basiskonfiguration von Amazon Elastic Compute Cloud (Amazon EC2) - Instances zu helfen, indem Sie überprüfen, ob EC2 Amazon-Instances gemäß den Standards Ihrer Organisation für mehr als die zulässige Anzahl von Tagen gestoppt wurden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
1.1	Einrichtung und Pflege eines detaillierten Inventars der Unternehmensressourcen	vpc-network-acl-unused-überprüfen	Diese Regel stellt sicher, dass Amazon Virtual Private Cloud (VPC)-Netzwerkzugriffskontrolllisten verwendet werden. Die Überwachung ungenutzter Netzwerkzugriffskontrolllisten kann zu einer genauen Inventarisierung und Verwaltung Ihrer Umgebung beitragen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
1.1	Einrichtung und Pflege eines detaillierten Inventars der Unternehmensressourcen	ec2- -Manager instance-managed-by-systems	Eine Bestandsaufnahme der Softwareplattformen und Anwendungen innerhalb des Unternehmens ist möglich, indem Amazon Elastic Compute Cloud (Amazon EC2) - Instances mit AWS Systems Manager verwaltet werden. Verwenden Sie AWS Systems Manager, um detaillierte Systemkonfigurationen, Betriebssystem-Patch-Levels, Namen und Typ der Dienste, Softwareinstallationen, Anwendungsname, Herausgeber und Version sowie andere Details zu Ihrer Umgebung bereitzustellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
1.1	Einrichtung und Pflege eines detaillierten Inventars der Unternehmensressourcen	ec2-check managedinstance-association-compliance-status	Verwenden Sie AWS Systems Manager Associations, um bei der Inventarisierung von Softwareplattformen und Anwendungen innerhalb eines Unternehmens zu helfen. AWS Systems Manager weist Ihren verwalteten Instances einen Konfigurationsstatus zu und ermöglicht es Ihnen, Basiswerte für Betriebssystem-Patch-Levels, Softwareinstallationen, Anwendungskonfigurationen und andere Details zu Ihrer Umgebung festzulegen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
1.1	Einrichtung und Pflege eines detaillierten Inventars der Unternehmensressourcen	ec2-eni security-group-attached-to	Diese Regel stellt sicher, dass die Sicherheitsgruppen an eine Amazon Elastic Compute Cloud (Amazon EC2) -Instance oder an eine ENI angehängt sind. Diese Regel unterstützt die Überwachung ungenutzter Sicherheitsgruppen im Bestand und die Verwaltung Ihrer Umgebung.
2.2	Sicherstellen, dass autorisierte Software derzeit unterstützt wird	elastic-beanstalk-managed-updates-aktiviert	Durch die Aktivierung verwalteter Plattformupdates für eine Amazon-Elastic-Beanstalk-Umgebung wird sichergestellt, dass die aktuellen verfügbaren Plattform-Fixes, -Updates und -Features für die Umgebung installiert sind. Eine bewährte Methode zur Sicherung von Systemen besteht darin, stets die aktuellen Patches zu installieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
2.2	Sicherstellen, dass autorisierte Software derzeit unterstützt wird	ec2- prüfen managedinstance-patch-compliance-status	Aktivieren Sie diese Regel, um bei der Identifizierung und Dokumentation von Sicherheitslücken in Amazon Elastic Compute Cloud (Amazon EC2) zu helfen. Die Regel prüft, ob die EC2 Amazon-Instance die Patch-Konformität im AWS Systems Manager gemäß den Richtlinien und Verfahren Ihrer Organisation einhält.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
2.2	Sicherstellen, dass autorisierte Software derzeit unterstützt wird	ecs-fargate-latest-platform-Version	Sicherheitsupdates und Patches werden automatisch für Ihre AWS Fargate-Aufgaben bereitgestellt. Wenn ein Sicherheitsproblem gefunden wird, das eine AWS Fargate-Plattformversion betrifft, AWS wird die Plattformversion gepatcht. Um Sie bei der Patchverwaltung Ihrer Amazon Elastic Container Service (ECS) - Aufgaben zu unterstützen, auf denen AWS Fargate ausgeführt wird, aktualisieren Sie Ihre eigenständigen Service-Aufgaben, sodass sie die neueste Plattformversion verwenden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.3	Datenzugriffskontrolllisten konfigurieren	ec2-imdsv2-check	Stellen Sie sicher, dass die Methode Instance Metadata Service Version 2 (IMDSv2) aktiviert ist, um den Zugriff auf und die Kontrolle der Amazon Elastic Compute Cloud (Amazon EC2) - Instance-Metadaten zu schützen. Die IMDSv2 Methode verwendet sitzungsbasierte Kontrollen. Mit können Kontrollen implementiert werden IMDSv2, um Änderungen an Instanzmetadaten einzuschränken.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.3	Datenzugriffskontrolllisten konfigurieren	ec2- instance-profile-attached	EC2 Instanzprofile übergeben eine IAM-Rolle an eine Instanz EC2 . Das Anhängen eines Instance-Profils an Ihre Instances kann bei der Implementierung von geringsten Berechtigungen und der Berechtigungsverwaltung helfen.
3.3	Datenzugriffskontrolllisten konfigurieren	dms-replication-not-public	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass auf DMS-Replikationsinstanzen nicht öffentlich zugegriffen werden kann. DMS-Replikations-Instances können vertrauliche Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.3	Datenzugriffskontrolllisten konfigurieren	ebs-snapshot-public-restorable-überprüfen	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass EBS-Snapshots nicht öffentlich wiederherstellbar sind. EBS-Volume-Snapshots können vertrauliche Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.3	Datenzugriffskontrolllisten konfigurieren	emr-kerberos-enabled	Die Zugriffsberechtigungen und -autorisierungen können verwaltet und nach den Prinzipien der geringsten Berechtigung und Aufgabentrennung integriert werden, indem Kerberos für Amazon-EMR-Cluster aktiviert wird. In Kerberos werden Services und Benutzer, die sich authentifizieren müssen, als Prinzipale bezeichnet. Prinzipale befinden sich in einem Kerberos-Bereich. Innerhalb dieses Bereichs wird ein Kerberos-Server als Key Distribution Center (KDC) bezeichnet. Über diesen Server können sich Prinzipale authentifizieren. Die Authentifizierung im KDC erfolgt durch die Ausstellung von Authentif

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			izierungstickets. Das KDC unterhält eine Datenbank der Prinzipale in seinem Bereich mit ihren Passwörtern und anderen administr ativen Informationen zu jedem Prinzipal.
3.3	Datenzugriffskontr olllisten konfigurieren	iam-group-has-users-überprüfen	AWS Identity and Access Managemen t (IAM) kann Ihnen helfen, die Prinzipien der geringsten Rechte und der Aufgabent rennung mit Zugriffsb erechtigungen und Autorisierungen zu integrieren, indem sichergestellt wird, dass IAM-Gruppen mindestens einen Benutzer haben. Die Einteilung von Benutzern in Gruppen auf der Grundlage der ihnen zugewiese nen Berechtigungen oder ihrer Funktion ist eine Möglichkeit, das Prinzip der geringste n Berechtigung zu implementieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.3	Datenzugriffskontrolllisten konfigurieren	iam-no-inline-policy-überprüfen	Stellen Sie sicher, dass ein Benutzer, eine IAM-Rolle oder eine IAM-Gruppe (AWS Identity and Access Management) nicht über eine Inline-Richtlinie zur Zugriffskontrolle auf Systeme und Ressourcen verfügt. AWS empfiehlt, verwaltete Richtlinien anstelle von Inline-Richtlinien zu verwenden. Verwaltete Richtlinien ermöglichen Wiederverwendbarkeit, Versionsverwaltung, Rollback und Delegierung der Berechtigungsverwaltung.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.3	Datenzugriffskontrolllisten konfigurieren	ec2- instance-no-public-ip	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon Elastic Compute Cloud (Amazon EC2) - Instances nicht öffentlich zugänglich sind. EC2Amazon -Instances können vertrauliche Informationen enthalten, und für solche Konten ist eine Zugriffskontrolle erforderlich.
3.3	Datenzugriffskontrolllisten konfigurieren	iam-policy-no-statements-with-full-access	Stellen Sie sicher, dass IAM-Aktionen nur auf die benötigten Aktionen beschränkt sind. Wenn Benutzern mehr Rechte eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und der Aufgabentrennung verstoßen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.3	Datenzugriffskontrolllisten konfigurieren	elasticsearch-in-vpc-only	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass sich Amazon OpenSearch OpenSearch Service (Service) - Domains innerhalb einer Amazon Virtual Private Cloud (Amazon VPC) befinden. Eine OpenSearch Service-Domain innerhalb einer Amazon VPC ermöglicht die sichere Kommunikation zwischen OpenSearch Service und anderen Services innerhalb der Amazon VPC, ohne dass ein Internet-Gateway, ein NAT-Gerät oder eine VPN-Verbindung erforderlich ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.3	Datenzugriffskontrolllisten konfigurieren	iam-user-group-membership-überprüfen	AWS Identity and Access Management (IAM) kann Ihnen helfen, Zugriffsberechtigungen und Autorisierungen einzuschränken, indem sichergestellt wird, dass Benutzer Mitglieder mindestens einer Gruppe sind. Wenn Benutzern mehr Berechtigungen eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und Aufgabentrennung verstoßen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.3	Datenzugriffskontrolllisten konfigurieren	ec2- instances-in-vpc	Stellen Sie Amazon Elastic Compute Cloud (Amazon EC2) -Instances innerhalb einer Amazon Virtual Private Cloud (Amazon VPC) bereit, um eine sichere Kommunikation zwischen einer Instance und anderen Services innerhalb der Amazon VPC zu ermöglichen, ohne dass ein Internet-Gateway, ein NAT-Gerät oder eine VPN-Verbindung erforderlich ist. Der gesamte Datenverkehr bleibt sicher in der AWS Cloud. Domains, die sich innerhalb einer VPC befinden, verfügen aufgrund ihrer logischen Isolierung im Vergleich zu Domains mit öffentlichen Endpunkten über eine zusätzliche Sicherheitsebene. Weisen Sie EC2

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			Amazon-Instances einer Amazon VPC zu, um den Zugriff ordnungsgemäß zu verwalten.
3.3	Datenzugriffskontrolllisten konfigurieren	emr-master-no-public-ip	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon EMR-Cluster-Masterknoten nicht öffentlich zugänglich sind. Amazon-EMR-Cluster-Hauptknoten können vertrauliche Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.3	Datenzugriffskontrolllisten konfigurieren	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) kann Ihnen dabei helfen, die Prinzipien der geringsten Rechte und der Aufgabentrennung in Zugriffsberechtigungen und Autorisierungen zu integrieren und so zu verhindern, dass Richtlinien „Effect“: „Allow“ mit „Action“: „*“ anstelle von „Resource“: „*“ enthalten. Wenn Benutzern mehr Rechte eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und der Aufgabentrennung verstoßen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.3	Datenzugriffskontrolllisten konfigurieren	iam-user-no-policies-überprüfen	Diese Regel stellt sicher, dass AWS Identity and Access Management (IAM) -Richtlinien nur Gruppen oder Rollen zugewiesen werden, um den Zugriff auf Systeme und Ressourcen zu kontrollieren. Die Zuweisung von Berechtigungen auf Gruppen- oder Rollenebene trägt dazu bei, die Wahrscheinlichkeit zu verringern, dass eine Identität übermäßige Berechtigungen erhält oder beibehält.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.3	Datenzugriffskontrolllisten konfigurieren	iam-root-access-key-überprüfen	Der Zugriff auf Systeme und Ressourcen kann gesteuert werden, indem überprüft wird, ob der Root-Benutzer keine Zugriffsschlüssel mit seiner AWS Identity and Access Management (IAM) -Rolle verknüpft hat. Stellen Sie sicher, dass die Root-Zugriffsschlüssel gelöscht werden. Erstellen und verwenden Sie stattdessen rollenbasierte Funktionen, AWS-Konten um das Prinzip der geringsten Funktionalität zu berücksichtigen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.3	Datenzugriffskontrolllisten konfigurieren	iam-user-unused-credentials-überprüfen	AWS Identity and Access Management (IAM) kann Ihnen bei Zugriffsberechtigungen und Autorisierungen helfen, indem es nach IAM-Passwörtern und Zugriffsschlüsseln sucht, die für einen bestimmten Zeitraum nicht verwendet wurden. Wenn ungenutzte Anmeldeinformationen identifiziert werden, müssen Sie sie deaktivieren und/oder entfernen, da dies gegen das Prinzip der geringsten Berechtigung verstoßen könnte. Für diese Regel müssen Sie einen Wert für das maxCredentialUsage Alter festlegen (Standardkonfiguration: 90). Der tatsächliche Wert muss den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.3	Datenzugriffskontrolllisten konfigurieren	iam-customer-policy-blocked-kms-Aktionen	AWS Identity and Access Management (IAM) kann Ihnen helfen, die Prinzipien der geringsten Rechte und der Aufgabentrennung in Zugriffsberechtigungen und Autorisierungen zu integrieren und so zu verhindern, dass Richtlinien blockierte Aktionen für alle AWS Schlüssel des Key Management Service enthalten. Wenn Benutzer mehr Rechte haben, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und Aufgabentrennung verstoßen. Mit dieser Regel können Sie den Parameter festlegen. blockedActionsPatterns (Wert „AWS Bewährte grundlegende Sicherheitsmethode

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			n“: kms: Entschlüs seln, kms:ReEnc ryptFrom). Die tatsächlichen Werte müssen den Richtlini en Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.3	Datenzugriffskontrolllisten konfigurieren	iam-inline-policy-blocked-kms-Aktionen	Stellen Sie sicher, dass ein Benutzer, eine IAM-Rolle oder eine IAM-Gruppe (AWS Identity and Access Management) nicht über eine Inline-Richtlinie verfügt, die blockierte Aktionen für alle AWS Schlüssel des Key Management Service zulässt. AWS empfiehlt, verwaltete Richtlinien anstelle von Inline-Richtlinien zu verwenden. Verwaltete Richtlinien ermöglichen Wiederverwendbarkeit, Versionsverwaltung, Rollback und Delegierung der Berechtigungsverwaltung. Mit dieser Regel können Sie den blockedActionsPatterns Parameter festlegen. (Wert „AWS Bewährte grundlegende Sicherheitsmethoden“: kms: Entschlüsseln, kms:ReEnc

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			ryptFrom). Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.
3.3	Datenzugriffskontrolllisten konfigurieren	lambda-function-public-access-verboten	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass AWS Lambda-Funktionen nicht öffentlich zugänglich sind. Der öffentliche Zugriff kann möglicherweise die Verfügbarkeit von Ressourcen beeinträchtigen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.3	Datenzugriffskontrolllisten konfigurieren	lambda-inside-vpc	Stellen Sie AWS Lambda-Funktionen in einer Amazon Virtual Private Cloud (Amazon VPC) bereit, um eine sichere Kommunikation zwischen einer Funktion und anderen Diensten innerhalb der Amazon VPC zu gewährleisten. Bei dieser Konfiguration sind kein Internet-Gateway, kein NAT-Gerät und keine VPN-Verbindung erforderlich. Der gesamte Datenverkehr bleibt sicher in der Cloud. AWS Domains, die sich innerhalb einer VPC befinden, verfügen aufgrund ihrer logischen Isolierung im Vergleich zu Domains mit öffentlichen Endpunkten über eine zusätzliche Sicherheitsebene. Um den Zugriff ordnungsgemäß zu verwalten,

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			sollten AWS Lambda-Funktionen einer VPC zugewiesen werden.
3.3	Datenzugriffskontrolllisten konfigurieren	rds-snapshots-public-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Relational Database Service (Amazon RDS) -Instances nicht öffentlich sind. Amazon-RDS-Datenbank-Instances können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.3	Datenzugriffskontrolllisten konfigurieren	rds-instance-public-access-überprüfen	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Relational Database Service (Amazon RDS) -Instances nicht öffentlich sind. Amazon-RDS-Datenbank-Instances können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.3	Datenzugriffskontrolllisten konfigurieren	redshift-cluster-public-access-überprüfen	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Redshift Redshift-Cluster nicht öffentlich sind. Amazon-Redshift-Cluster können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.3	Datenzugriffskontrolllisten konfigurieren	s3 bucket-level-public-access - verboten	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Simple Storage Service (Amazon S3) -Buckets nicht öffentlich zugänglich sind. Diese Regel trägt dazu bei, sensible Daten vor unbefugten Remote-Benutzern zu schützen, indem sie den öffentlichen Zugriff auf Bucket-Ebene verhindert.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.3	Datenzugriffskontrolllisten konfigurieren	account-level-public-accesss3-Blöcke-periodisch	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Simple Storage Service (Amazon S3) -Buckets nicht öffentlich zugänglich sind. Diese Regel trägt dazu bei, sensible Daten vor unbefugten Remote-Benutzern zu schützen, indem sie den öffentlichen Zugriff verhindert. Mit dieser Regel können Sie optional die Parameter ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) und restrictPublicBuckets Parameter (Config Default: True) festlegen. Die tatsächlichen Werte müssen den Richtlini

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			en Ihrer Organisation entsprechen.
3.3	Datenzugriffskontrolllisten konfigurieren	s-3 bucket-public-read-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie nur autorisierten Benutzern, Prozessen und Geräten Zugriff auf Amazon Simple Storage Service (Amazon S3) - Buckets gewähren. Die Verwaltung des Zugriffs sollte mit der Klassifizierung der Daten übereinstimmen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.3	Datenzugriffskontrolllisten konfigurieren	s-3 bucket-public-write-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie nur autorisierten Benutzern, Prozessen und Geräten Zugriff auf Amazon Simple Storage Service (Amazon S3) - Buckets gewähren. Die Verwaltung des Zugriffs sollte mit der Klassifizierung der Daten übereinstimmen.
3.3	Datenzugriffskontrolllisten konfigurieren	sagemaker-notebook-no-direct-Internetzugang	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass SageMaker Amazon-Notebooks keinen direkten Internetzugang zulassen. Indem Sie direkten Internetzugang blockieren, vermeiden Sie, dass unbefugte Benutzer auf sensible Daten zugreifen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.3	Datenzugriffskontrolllisten konfigurieren	subnet-auto-assign-public-ip-deaktiviert	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon Virtual Private Cloud (VPC) -Subnetzen nicht automatisch eine öffentliche IP-Adresse zugewiesen wird. Amazon Elastic Compute Cloud (EC2) -Instances, die in Subnetzen gestartet werden, in denen dieses Attribut aktiviert ist, haben ihrer primären Netzwerkschnittstelle eine öffentliche IP-Adresse zugewiesen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.3	Datenzugriffskontrolllisten konfigurieren	ssm-document-not-public	Stellen Sie sicher, dass AWS Systems Manager (SSM) - Dokumente nicht öffentlich sind, da dies einen unbeabsichtigten Zugriff auf Ihre SSM-Dokumente ermöglichen kann. Ein öffentliches SSM-Dokument kann Informationen über Ihr Konto, Ihre Ressourcen und internen Prozesse preisgeben.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.3	Datenzugriffskontr olllisten konfigurieren	ecs-task-definition-user-for-host-mode-check	Wenn für eine Aufgabendefinition erhöhte Berechtig ungen gelten, liegt das daran, dass der Kunde diesen Konfigura tionen ausdrücklich zugestimmt hat. Diese Kontrolle prüft, ob eine unerwartete Berechtigungseskal ation vorliegt, wenn für eine Aufgabend efinition das Host-Netzwerk aktiviert ist, die Kunden aber keine erhöhten Berechtigungen aktiviert haben.
3.3	Datenzugriffskontr olllisten konfigurieren	ecs-task-definition-nonroot-benutzer	Sie bestimmen einen Nicht-Root-Benutzer für den Zugriff auf Ihre Aufgabendefinitionen des Amazon Elastic Container Service (Amazon ECS), um die Implementierung des Prinzips der geringsten Berechtig ung zu unterstützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.3	Datenzugriffskontrolllisten konfigurieren	autoscaling-launch-config-public-ip-deaktiviert	Wenn Sie Ihre Netzwerkschnittstellen mit einer öffentlichen IP-Adresse konfigurieren, sind die diesen Netzwerkschnittstellen zugehörigen Ressourcen über das Internet erreichbar. EC2 Ressourcen sollten nicht öffentlich zugänglich sein, da dies einen unbeabsichtigten Zugriff auf Ihre Anwendungen oder Server ermöglichen kann.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.3	Datenzugriffskontrolllisten konfigurieren	opensearch-in-vpc-only	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass sich Amazon OpenSearch Service-Domains innerhalb einer Amazon Virtual Private Cloud (Amazon VPC) befinden. Eine Amazon OpenSearch Service-Domain innerhalb einer Amazon VPC ermöglicht die sichere Kommunikation zwischen Amazon OpenSearch Service und anderen Services innerhalb der Amazon VPC, ohne dass ein Internet-Gateway, ein NAT-Gerät oder eine VPN-Verbindung erforderlich ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.3	Datenzugriffskontrolllisten konfigurieren	efs-access-point-enforce-root-Verzeichnis	Die Durchsetzung eines Stammverzeichnisses für einen Amazon-Elastic-File-System (Amazon-EFS)-Zugangspunkt trägt dazu bei, den Datenzugriff einzuschränken, indem sichergestellt wird, dass Benutzer des Zugangspunkts nur auf Dateien des angegebenen Unterverzeichnisses zugreifen können.
3.4	Datenaufbewahrung erzwingen	s3- version-lifecycle-policy-check	Mit Amazon-S3-Lebenszyklusregeln können Sie Aktionen definieren, die Amazon S3 während der Lebensdauer eines Objekts ausführen soll (z. B. die Überführung von Objekten in eine andere Speicherklasse, ihre Archivierung oder Löschung nach einem bestimmten Zeitraum).

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.4	Datenaufbewahrung erzwingen	cw-loggroup-retention-period-überprüfen	Stellen Sie sicher, dass die Ereignisprotokolldaten für Ihre Protokollgruppen über eine Mindestdauer aufbewahrt werden, um die Fehlerbehebung und forensische Untersuchungen zu unterstützen. Fehlende frühere Ereignisprotokolldaten erschweren die Rekonstruierung und Identifizierung potenziell schädlicher Ereignisse.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
4.1	Einrichtung und Pflege eines sicheren Konfigurationsprozesses	account-part-of-organizations	Durch die zentrale Verwaltung AWS-Konten innerhalb von AWS Organizations wird sichergestellt, dass die Konten den Vorschriften entsprechen. Eine fehlende zentrale Kontoverwaltung kann zu inkonsistenten Kontokonfigurationen führen, wodurch Ressourcen und sensible Daten offengelegt werden können.
4.1	Einrichtung und Pflege eines sicheren Konfigurationsprozesses	ec2-stopped-instance	Aktivieren Sie diese Regel, um bei der Basiskonfiguration von Amazon Elastic Compute Cloud (Amazon EC2) - Instances zu helfen, indem Sie überprüfen, ob EC2 Amazon-Instances gemäß den Standards Ihrer Organisation für mehr als die zulässige Anzahl von Tagen gestoppt wurden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
4.1	Einrichtung und Pflege eines sicheren Konfigurationsprozesses	ec2- volume-inuse-check	Diese Regel stellt sicher, dass Amazon Elastic Block Store-Volumes, die an Amazon Elastic Compute Cloud (Amazon EC2) - Instances angehängt sind, zum Löschen markiert werden, wenn eine Instance beendet wird. Wenn ein Amazon-EBS-Volume nicht gelöscht wird, wenn die Instance, an die es angehängt ist, beendet wird, kann dies gegen das Konzept der geringsten Funktionalität verstoßen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
4.1	Einrichtung und Pflege eines sicheren Konfigurationsprozesses	redshift-cluster-maintenancesettings-check	Diese Regel stellt sicher, dass Amazon-Redshift-Cluster die bevorzugten Einstellungen für Ihre Organisation haben. Insbesondere sorgt sie dafür, dass Cluster bevorzugte Wartungsfenster und automatisierte Aufbewahrungsfristen für Snapshots für die Datenbank haben. Für diese Regel müssen Sie die festlegen allowVersionUpgrade. Der Standardwert ist „true“. Außerdem können Sie optional den Zeitraum preferredMaintenanceWindow (der Standardwert ist sa: 16:00 -sa: 16:30) und den automated SnapshotRetention Zeitraum (der Standardwert ist 1) festlegen. Die tatsächlichen Werte müssen den Richtlini

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			en Ihrer Organisation entsprechen.
4.1	Einrichtung und Pflege eines sicheren Konfigurationsprozesses	ec2-manager instance-managed-by-systems	Eine Bestandsaufnahme der Softwareplattformen und Anwendungen innerhalb des Unternehmens ist möglich, indem Amazon Elastic Compute Cloud (Amazon EC2) - Instances mit AWS Systems Manager verwaltet werden. Verwenden Sie AWS Systems Manager, um detaillierte Systemkonfigurationen, Betriebssystem-Patch-Levels, Namen und Typ der Dienste, Softwareinstallationen, Anwendungsname, Herausgeber und Version sowie andere Details zu Ihrer Umgebung bereitzustellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
4.1	Einrichtung und Pflege eines sicheren Konfigurationsprozesses	ec2-check managedinstance-association-compliance-status	Verwenden Sie AWS Systems Manager Associations, um bei der Inventarisierung von Softwareplattformen und Anwendungen innerhalb eines Unternehmens zu helfen. AWS Systems Manager weist Ihren verwalteten Instances einen Konfigurationsstatus zu und ermöglicht es Ihnen, Basiswerte für Betriebssystem-Patch-Levels, Softwareinstallationen, Anwendungskonfigurationen und andere Details zu Ihrer Umgebung festzulegen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
4.1	Einrichtung und Pflege eines sicheren Konfigurationsprozesses	efs-access-point-enforce-root-Verzeichnis	Die Durchsetzung eines Stammverzeichnisses für einen Amazon-Elastic-File-System (Amazon-EFS)-Zugangspunkt trägt dazu bei, den Datenzugriff einzuschränken, indem sichergestellt wird, dass Benutzer des Zugangspunkts nur auf Dateien des angegebenen Unterverzeichnisses zugreifen können.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
4.1	Einrichtung und Pflege eines sicheren Konfigurationsprozesses	secretsmanager-rotation-enabled-check	Diese Regel stellt sicher, dass bei AWS Secrets Manager Manager-Geheimnissen die Rotation aktiviert ist. Die regelmäßige Rotation von Secrets kann den Zeitraum verkürzen, in dem ein Secret aktiv ist, und möglicherweise die Auswirkungen auf das Unternehmen verringern, falls das Secret kompromittiert wird.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
4.1	Einrichtung und Pflege eines sicheren Konfigurationsprozesses	access-keys-rotated	Die Anmeldeinformationen für autorisierte Geräte, Benutzer und Prozesse werden geprüft, indem sichergestellt wird, dass die IAM-Zugriffsschlüssel gemäß den Vorgaben der Unternehmensrichtlinie rotiert werden. Das regelmäßige Ändern der Zugriffsschlüssel ist eine bewährte Sicherheitsmethode. Es verkürzt den Zeitraum, in dem ein Zugriffsschlüssel aktiv ist, und reduziert die Auswirkungen auf das Unternehmen, wenn die Schlüssel kompromittiert werden. Diese Regel erfordert einen Wert für die Zugriffsschlüssel-Rotation (Standardkonfiguration: 90). Der tatsächliche Wert muss den Richtlini

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			en Ihrer Organisation entsprechen.
4.6	Sichere Verwaltung von Unternehmensressourcen und -software	alb-http-to-https-Umleitungsprüfung	Um Daten während der Übertragung zu schützen, stellen Sie sicher, dass Ihr Application Load Balancer unverschlüsselte HTTP-Anfragen automatisch an HTTPS umleitet. Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.
4.6	Sichere Verwaltung von Unternehmensressourcen und -software	elb-tls-https-listeners-nur	Stellen Sie sicher, dass Ihre Elastic Load Balancer (ELBs) mit SSL- oder HTTPS-Listenern konfiguriert sind. Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
4.6	Sichere Verwaltung von Unternehmensressourcen und -software	api-gw-ssl-enabled	Stellen Sie sicher, dass die REST-API-Stufen von Amazon API Gateway mit SSL-Zertifikaten konfiguriert sind, damit Backend-Systeme überprüfen können, ob Anforderungen von API Gateway stammen.
4,6	Sichere Verwaltung von Unternehmensressourcen und -software	redshift-require-tls-ssl	Stellen Sie sicher, dass Ihre Amazon-Redshift-Cluster eine TLS/SSL-Verschlüsselung erfordern, um eine Verbindung zu SQL-Clients herzustellen. Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
4,6	Sichere Verwaltung von Unternehmensressourcen und -software	s-3 bucket-ssl-requests-only	Um Daten während der Übertragung zu schützen, stellen Sie sicher, dass Ihre Amazon Simple Storage Service (Amazon S3)-Buckets Anfragen zur Verwendung von Secure Socket Layer (SSL)-Buckets erfordern. Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.
4,6	Sichere Verwaltung von Unternehmensressourcen und -software	opensearch-https-required	Da sensible Daten existieren können und um Daten während der Übertragung zu schützen, sollten Sie sicherstellen, dass HTTPS für Verbindungen zu Ihren Amazon OpenSearch Service-Domains aktiviert ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
4.7	Standardkonten für Unternehmensressourcen und -software verwalten	iam-root-access-key-überprüfen	Der Zugriff auf Systeme und Ressourcen kann gesteuert werden, indem überprüft wird, ob der Root-Benutzer keine Zugriffsschlüssel mit seiner AWS Identity and Access Management (IAM) -Rolle verknüpft hat. Stellen Sie sicher, dass die Root-Zugriffsschlüssel gelöscht werden. Erstellen und verwenden Sie stattdessen rollenbasierte Funktionen, AWS-Konten um das Prinzip der geringsten Funktionalität zu berücksichtigen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
5.1	Erstellen und Verwalten eines Konteninventars	account-part-of-organizations	Durch die zentrale Verwaltung AWS-Konten innerhalb von AWS Organizations wird sichergestellt, dass die Konten den Vorschriften entsprechen. Eine fehlende zentrale Kontoverwaltung kann zu inkonsistenten Kontokonfigurationen führen, wodurch Ressourcen und sensible Daten offengelegt werden können.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
5.2	Verwendung eindeutiger Passwörter	iam-password-policy	Die Identitäten und Anmeldeinformationen werden auf der Grundlage einer organisatorischen IAM-Passwortrichtlinie ausgestellt, verwaltet und verifiziert. Sie erfüllen oder übertreffen die Anforderungen des NIST SP 800-63 und des AWS Foundational Security Best Practices-Standards für die Passwortstärke. Mit dieser Regel können Sie optional RequireUppercaseCharacters (Wert für AWS grundlegende Sicherheitsbewährte Methoden: wahr), RequireLowercaseCharacters (Wert für bewährte Methoden für AWS grundlegende Sicherheit: wahr), RequireSymbols (Wert für bewährte Methoden für AWS grundlegende Sicherheit:

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			wahr), RequireNumbers (Wert für bewährte Methoden für AWS grundlegende Sicherheit: wahr), MinimumPasswordLength (Wert für bewährte Methoden für AWS grundlegende Sicherheit: 14), PasswordReusePrevention (Wert für bewährte Methoden für AWS grundlegende Sicherheit: 24) und MaxPasswordAge (Wert für bewährte Methoden für AWS grundlegende Sicherheit: 90) für Ihr IAM festlegen Kennwortrichtlinie. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
5.2	Verwendung eindeutiger Passwörter	iam-user-mfa-enabled	Aktivieren Sie diese Regel, um den Zugriff auf Ressourcen in der AWS -Cloud einzuschränken. Diese Regel stellt sicher, dass die Multi-Faktor-Authentifizierung (MFA) für alle Benutzer aktiviert ist. MFA bietet eine weitere Schutzebene zusätzlich zum Benutzernamen und Passwort. Reduzieren Sie Fälle von kompromittierten Konten, indem Sie MFA für Benutzer vorschreiben.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
5.2	Verwendung eindeutiger Passwörter	mfa-enabled-for-iam-Konsolenzugriff	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass MFA für alle AWS Identity and Access Management (IAM) -Benutzer aktiviert ist, die über ein Konsolenkennwort verfügen. MFA sorgt für eine weitere Schutzebene zusätzlich zu den Anmeldeinformationen. Indem Sie MFA für Benutzer vorschreiben, können Sie Fälle kompromittierter Konten reduzieren und verhindern, dass unbefugte Benutzer auf vertrauliche Daten zugreifen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
5.2	Verwendung eindeutiger Passwörter	root-account-mfa-enabled	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass MFA für den Root-Benutzer aktiviert ist. Der Stammbenutzer ist der AWS-Konto-Benutzer mit den meisten Berechtigungen. MFA bietet eine weitere Schutzebene zusätzlich zum Benutzernamen und Passwort. Indem Sie MFA für den Root-Benutzer vorschreiben, können Sie die Anzahl AWS-Konten kompromittierter Benutzer reduzieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
5.3	Deaktivierung inaktiver Konten	iam-user-unused-credentials-überprüfen	AWS Identity and Access Management (IAM) kann Ihnen bei Zugriffsberechtigungen und Autorisierungen helfen, indem es nach IAM-Passwörtern und Zugriffsschlüsseln sucht, die für einen bestimmten Zeitraum nicht verwendet wurden. Wenn ungenutzte Anmeldeinformationen identifiziert werden, müssen Sie sie deaktivieren und/oder entfernen, da dies gegen das Prinzip der geringsten Berechtigung verstoßen könnte. Für diese Regel müssen Sie einen Wert für das maxCredentialUsage Alter festlegen (Standardkonfiguration: 90). Der tatsächliche Wert muss den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
5.4	Beschränkung der Administratorrechte auf spezielle Administratorkonten	iam-root-access-key-überprüfen	Der Zugriff auf Systeme und Ressourcen kann gesteuert werden, indem überprüft wird, ob der Root-Benutzer keine Zugriffsschlüssel mit seiner AWS Identity and Access Management (IAM) -Rolle verknüpft hat. Stellen Sie sicher, dass die Root-Zugriffsschlüssel gelöscht werden. Erstellen und verwenden Sie stattdessen rollenbasierte Funktionen, AWS-Konten um das Prinzip der geringsten Funktionalität zu berücksichtigen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
5.4	Beschränkung der Administratorrechte auf spezielle Administratorkonten	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) kann Ihnen dabei helfen, die Prinzipien der geringsten Rechte und der Aufgabentrennung in Zugriffsberechtigungen und Autorisierungen zu integrieren und so zu verhindern, dass Richtlinien „Effect“: „Allow“ mit „Action“: „*“ anstelle von „Resource“: „*“ enthalten. Wenn Benutzern mehr Rechte eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und der Aufgabentrennung verstoßen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
6.4	Erzwingen von MFA für Remote-Netzwerkzugriff	iam-user-mfa-enabled	Aktivieren Sie diese Regel, um den Zugriff auf Ressourcen in der AWS -Cloud einzuschränken. Diese Regel stellt sicher, dass die Multi-Faktor-Authentifizierung (MFA) für alle Benutzer aktiviert ist. MFA bietet eine weitere Schutzebene zusätzlich zum Benutzernamen und Passwort. Reduzieren Sie Fälle von kompromittierten Konten, indem Sie MFA für Benutzer vorschreiben.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
6.4	Erzwingen von MFA für Remote-Netzwerkzugriff	mfa-enabled-for-iam-Konsolenzugriff	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass MFA für alle AWS Identity and Access Management (IAM) -Benutzer aktiviert ist, die über ein Konsolenkennwort verfügen. MFA sorgt für eine weitere Schutzebene zusätzlich zu den Anmeldeinformationen. Indem Sie MFA für Benutzer vorschreiben, können Sie Fälle kompromittierter Konten reduzieren und verhindern, dass unbefugte Benutzer auf vertrauliche Daten zugreifen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
6.4	Erzwingen von MFA für Remote-Netzwerkzugriff	root-account-mfa-enabled	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass MFA für den Root-Benutzer aktiviert ist. Der Stammbenutzer ist der AWS-Konto-Benutzer mit den meisten Berechtigungen. MFA bietet eine weitere Schutzebene zusätzlich zum Benutzernamen und Passwort. Indem Sie MFA für den Root-Benutzer vorschreiben, können Sie die Anzahl AWS-Konten kompromittierter Benutzer reduzieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
6,5	Erzwingen von MFA für Administratorzugriff	root-account-hardware-mfa-aktiviert	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Hardware-MFA für den Root-Benutzer aktiviert ist. Der Stammbenutzer ist der AWS-Konto-Benutzer mit den meisten Berechtigungen. MFA sorgt für eine weitere Schutzebene zusätzlich zu den Anmeldeinformationen. Indem Sie MFA für den Root-Benutzer vorschreiben, können Sie die Anzahl AWS-Konten kompromittierter Benutzer reduzieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
7.1	Einrichtung und Pflege eines Prozesses für das Schwachstellenmanagement	guardduty-enabled-centralized	Amazon GuardDuty kann mithilfe von Threat Intelligence Feeds helfen, potenzielle Cybersicherheitsereignisse zu überwachen und zu erkennen. Dazu gehören Listen mit bösartigen IPs und maschinellen Lernmethoden zur Identifizierung unerwarteter, nicht autorisierter und bösartiger Aktivitäten in Ihrer AWS Cloud-Umgebung.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
7.1	Einrichtung und Pflege eines Prozesses für das Schwachstellenmanagement	securityhub-enabled	AWS Security Hub hilft bei der Überwachung von unbefugtem Personal, Verbindungen, Geräten und Software. AWS Security Hub aggregiert, organisiert und priorisiert die Sicherheitswarnungen oder Ergebnisse mehrerer Dienste. AWS Einige dieser Dienste sind Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer und AWS Firewall Manager sowie AWS Partnerlösungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
7.1	Einrichtung und Pflege eines Prozesses für das Schwachstellenmanagement	ec2-prüfen managedinstance-patch-compliance-status	Aktivieren Sie diese Regel, um bei der Identifizierung und Dokumentation von Sicherheitslücken in Amazon Elastic Compute Cloud (Amazon EC2) zu helfen. Die Regel prüft, ob die EC2 Amazon-Instance die Patch-Konformität im AWS Systems Manager gemäß den Richtlinien und Verfahren Ihrer Organisation einhält.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
7.3	Durchführen eines automatisierten Betriebssystem-Patch-Managements	ec2-check managedinstance-patch-compliance-status	Aktivieren Sie diese Regel, um bei der Identifizierung und Dokumentation von Sicherheitslücken in Amazon Elastic Compute Cloud (Amazon EC2) zu helfen. Die Regel prüft, ob die EC2 Amazon-Instance die Patch-Konformität im AWS Systems Manager gemäß den Richtlinien und Verfahren Ihrer Organisation einhält.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
7.3	Durchführen eines automatisierten Betriebssystem-Patch-Managements	elastic-beanstalk-managed-updates-aktiviert	Durch die Aktivierung verwalteter Plattform updates für eine Amazon-Elastic-Beanstalk-Umgebung wird sichergestellt, dass die aktuellen verfügbaren Plattform -Fixes, -Updates und -Features für die Umgebung installiert sind. Eine bewährte Methode zur Sicherung von Systemen besteht darin, stets die aktuellen Patches zu installieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
7.3	Durchführen eines automatisierten Betriebssystem-Patch-Managements	redshift-cluster-maintenancesettings-check	Diese Regel stellt sicher, dass Amazon-Redshift-Cluster die bevorzugten Einstellungen für Ihre Organisation haben. Insbesondere sorgt sie dafür, dass Cluster bevorzugte Wartungsfenster und automatisierte Aufbewahrungsfristen für Snapshots für die Datenbank haben. Für diese Regel müssen Sie die allowVersionUpgrade festlegen. Der Standardwert ist „true“. Außerdem können Sie optional den Zeitraum preferredMaintenanceWindow (der Standardwert ist sa: 16:00 -sa: 16:30) und den automated SnapshotRetention Zeitraum (der Standardwert ist 1) festlegen. Die tatsächlichen Werte müssen den Richtlini

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			en Ihrer Organisation entsprechen.
7.4	Durchführen eines automatisierten Anwendungspatch-Managements	ec2- -check managedinstance-patch-compliance-status	Aktivieren Sie diese Regel, um bei der Identifizierung und Dokumentation von Sicherheitslücken in Amazon Elastic Compute Cloud (Amazon EC2) zu helfen. Die Regel prüft, ob die EC2 Amazon-Instance die Patch-Konformität im AWS Systems Manager gemäß den Richtlinien und Verfahren Ihrer Organisation einhält.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
7.4	Durchführen eines automatisierten Anwendungspatch-Managements	elastic-beanstalk-managed-updates-aktiviert	Durch die Aktivierung verwalteter Plattform updates für eine Amazon-Elastic-Beanstalk-Umgebung wird sichergestellt, dass die aktuellen verfügbaren Plattform -Fixes, -Updates und -Features für die Umgebung installiert sind. Eine bewährte Methode zur Sicherung von Systemen besteht darin, stets die aktuellen Patches zu installieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
7.4	Durchführen eines automatisierten Anwendungspatch-Managements	redshift-cluster-maintenancesettings-check	Diese Regel stellt sicher, dass Amazon-Redshift-Cluster die bevorzugten Einstellungen für Ihre Organisation haben. Insbesondere sorgt sie dafür, dass Cluster bevorzugte Wartungsfenster und automatisierte Aufbewahrungsfristen für Snapshots für die Datenbank haben. Für diese Regel müssen Sie die allowVersionUpgrade festlegen. Der Standardwert ist „true“. Außerdem können Sie optional den Zeitraum preferredMaintenanceWindow (der Standardwert ist sa: 16:00 -sa: 16:30) und den automated SnapshotRetention Zeitraum (der Standardwert ist 1) festlegen. Die tatsächlichen Werte müssen den Richtlini

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			en Ihrer Organisation entsprechen.
8.1	Einrichtung und Pflege eines Prozesses zur Verwaltung von Prüfprotokollen	audit-log-policy-exists (Prozessprüfung)	Richten Sie eine Richtlinie zur Verwaltung von Prüfprotokollen ein, in der die Protokoll ierungsanforderung en Ihres Unternehm ens definiert sind, und pflegen Sie diese Richtlinie. Dies beinhaltet, ist aber nicht beschränkt auf die Überprüfung und Aufbewahrung von Prüfprotokollen.
8.2	Erfassung von Prüfprotokollen	api-gw-execution-l ogging-aktiviert	Die API-Gateway-Protokollierung zeigt detaillierte Ansichten der Benutzer, die auf die API zugegriff en haben, und wie diese Benutzer auf die API zugegriff en haben. Diese Einblicke ermöglichen die Transparenz von Benutzeraktivitäten.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
8.2	Erfassung von Prüfprotokollen	multi-region-cloudtrail-enabled	AWS CloudTrail zeichnet Aktionen und API-Aufrufe der AWS Management Console auf. Sie können feststellen, welche Benutzer und Konten angerufen wurden AWS, von welcher Quell-IP-Adresse aus die Anrufe getätigt wurden und wann die Anrufe erfolgten. CloudTrail übermittelt Protokolldateien aus allen AWS Regionen an Ihren S3-Bucket , wenn MULTI_REG ION_CLOUD _TRAIL_ENABLED aktiviert ist. Außerdem wird beim AWS Start einer neuen Region derselbe Trail in der neuen Region erstellt. CloudTrail Dadurch erhalten Sie automatis ch Protokolldateien mit API-Aktivitäten für die neue Region.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
8.2	Erfassung von Prüfprotokollen	cloudtrail-s3-data events-enabled	Die Erfassung von Simple Storage Service (Amazon S3)-Datenereignissen unterstützt die Erkennung von ungewöhnlichen Aktivitäten. Zu den Details gehören Informationen zu dem AWS -Konto, das auf einen Amazon-S3-Bucket zugegriffen hat, die IP-Adresse und die Uhrzeit des Ereignisses.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
8.2	Erfassung von Prüfprotokollen	cloudtrail-enabled	AWS CloudTrai l kann durch die Aufzeichnung von Aktionen und API-Aufrufen in der AWS Management Console bei der Nichtabst reitbarkeit helfen. Sie können die Benutzer und die Benutzer AWS-Konten , die einen AWS Dienst aufgerufen haben, die Quell-IP-Adresse, über die die Aufrufe generiert wurden, und den Zeitpunkt der Anrufe identifiz ieren. Einzelheiten zu den erfassten Daten finden Sie in den AWS CloudTrail Datensatzinhalten.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
8.2	Erfassung von Prüfprotokollen	cloud-trail-cloud-watch-logs-aktiviert	Verwenden Sie Amazon CloudWatch , um Protokoll ereignisaktivitäten zentral zu sammeln und zu verwalten. Die Aufnahme von AWS CloudTrail Daten liefert Einzelheiten zu den API-Aufrufaktivitäten in Ihrem AWS-Konto.
8.2	Erfassung von Prüfprotokollen	elasticsearch-logs-to-cloudwatch	Stellen Sie sicher, dass für Amazon OpenSearch Service-Domains Fehlerprotokolle aktiviert und zur Aufbewahrung und Beantwortung an Amazon CloudWatch Logs gestreamt werden. Domain-Fehlerprotokolle sind bei Sicherheits- und Zugriffsprüfungen sowie bei der Diagnose von Verfügbarkeitsproblemen nützlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
8.2	Erfassung von Prüfprotokollen	vpc-flow-logs-enabled	VPC-Flow-Protokolle erfassen detaillierte Informationsdatensätze über den IP-Datenverkehr, der zu und von Netzwerkschnittstellen in Ihrer Amazon Virtual Private Cloud (Amazon VPC) fließt. Standardmäßig enthalten Flow-Protokolldatensätze Werte für die verschiedenen Komponenten des IP-Flows, einschließlich Quelle, Ziel und Protokoll.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
8.2	Erfassung von Prüfprotokollen	elb-logging-enabled	Die Elastic-Load-Balancing-Aktivität ist ein zentraler Kommunikationspunkt innerhalb einer Umgebung. Stellen Sie sicher, dass die ELB-Protokollierung aktiviert ist. Die gesammelten Daten enthalten detaillierte Informationen zu Anfragen, die an den ELB gesendet wurden. Jedes Protokoll enthält Informationen wie die Zeit, zu der die Anforderung einging, die Client-IP-Adresse, Latenzen, Anforderungspfade und Serverantworten.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
8.2	Erfassung von Prüfprotokollen	rds-logging-enabled	Um die Protokollierung und Überwachung in Ihrer Umgebung zu erleichtern, stellen Sie sicher, dass die Amazon Relational Database Service (Amazon RDS)-Protokollierung aktiviert ist. Mit der Amazon-RDS-Protokollierung können Sie Ereignisse wie Verbindungen, Verbindungsabbrüche, Abfragen oder abgefragte Tabellen erfassen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
8.2	Erfassung von Prüfprotokollen	s-3 bucket-logging-enabled	Die Amazon Simple Storage Service (Amazon S3)-Serverzugriffs protokollierung bietet eine Methode zur Überwachu ng des Netzwerks im Hinblick auf potenzielle Cybersich erheitsereignisse. Die Ereignisse werden überwacht, indem detaillierte Aufzeichn ungen über die Anfragen erfasst werden, die an einen Amazon-S3-Bucket gestellt wurden. Jeder Zugriffsprotokolle intrag enthält Details zu einer einzelnen Zugriffsanfrage. Zu den Details gehören Anforderer, Bucket-Name, Anforderu ngszeit, Anforderu ngsaktion, Antwortst atus und Fehlercode, falls relevant.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
8,2	Erfassung von Prüfprotokollen	redshift-cluster-configuration-check	Um Daten im Ruhezustand zu schützen, muss die Verschlüsselung für Ihre Amazon-Redshift-Cluster aktiviert sein. Sie müssen auch sicherstellen, dass die erforderlichen Konfigurationen auf Amazon-Redshift-Clustern bereitgestellt werden. Die Prüfungsprotokollierung muss aktiviert sein, um Informationen zu Verbindungen und Benutzeraktivitäten in der Datenbank bereitzustellen. Diese Regel erfordert, dass ein Wert für clusterDbEncrypted (Config Default: TRUE) und LoggingEnabled (Config Default: TRUE) gesetzt ist. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
8.2	Erfassung von Prüfprotokollen	wafv2-logging-enabled	Um die Protokollierung und Überwachung in Ihrer Umgebung zu erleichtern, aktivieren Sie die AWS WAF (V2) -Protokollierung im regionalen und globalen Web ACLs. AWS Die WAF-Protokollierung bietet detaillierte Informationen über den Datenverkehr, der von Ihrer Web-ACL analysiert wird. In den Protokollen werden die Uhrzeit aufgezeichnet, zu der die AWS WAF die Anfrage von Ihrer AWS Ressource erhalten hat, Informationen über die Anfrage und eine Aktion für die Regel, der jede Anfrage entsprach.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
8.2	Erfassung von Prüfprotokollen	codebuild-project-logging-enabled	Stellen Sie sicher, dass die AWS CodeBuild Projektprotokollierung aktiviert ist, damit Ihre Build-Ausgabeprotokolle entweder an Amazon CloudWatch oder Amazon Simple Storage Service (Amazon S3) gesendet werden. Build-Ausgabeprotokolle enthalten detaillierte Informationen zu Ihrem Build-Projekt.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
8.3	Gewährleisten einer angemessene Speicherung der Prüfprotokolle	s-3 version-lifecycle-policy-check	Mit Amazon-S3-Lebenszyklusregeln können Sie Aktionen definieren, die Amazon S3 während der Lebensdauer eines Objekts ausführen soll (z. B. die Überführung von Objekten in eine andere Speicherklasse, ihre Archivierung oder Löschung nach einem bestimmten Zeitraum).

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.1	Bereitstellung und Wartung von Anti-Malware-Software	guardduty-enabled-centralized	Amazon GuardDuty kann mithilfe von Threat Intellige nce Feeds helfen, potenzielle Cybersich erheitsereignisse zu überwachen und zu erkennen. Dazu gehören Listen mit bösartigen IPs und maschinel len Lernmethoden zur Identifizierung unerwarteter, nicht autorisierter und bösartiger Aktivitäten in Ihrer AWS Cloud-Umgebung.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.2	Konfigurierung automatischer Anti-Malware-Signatur-Updates	guardduty-enabled-centralized	Amazon GuardDuty kann mithilfe von Threat Intellige nce Feeds helfen, potenzielle Cybersich erheitsereignisse zu überwachen und zu erkennen. Dazu gehören Listen mit bösartigen IPs und maschinel len Lernmethoden zur Identifizierung unerwarteter, nicht autorisierter und bösartiger Aktivitäten in Ihrer AWS Cloud-Umgebung.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
11.2	Durchführen automatisierter Backups	dynamodb-in-backup-plan	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon DynamoDB-Tabellen Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
11.2	Durchführen automatisierter Backups	ebs-in-backup-plan	Stellen Sie zur Unterstützung der Datensicherungspro zesse sicher, dass Ihre Amazon Elastic Block Store (Amazon EBS) -Volumes Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwaltet er Backup-Service mit einer richtlini enbasierten Backup-Lösung. Diese Lösung vereinfacht Ihre Backup-Verwaltung und ermöglicht es Ihnen, Ihre geschäftl ichen und behördlic hen Anforderungen bezüglich Backups zu erfüllen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
11.2	Durchführen automatisierter Backups	ebs-optimized-instance	Eine optimierte Instance im Amazon Elastic Block Store (Amazon EBS) bietet zusätzliche, dedizierte Kapazität für Amazon-EBS-I/O-Vorgänge. Diese Optimierung bietet die beste Leistung für Ihr EBS-Volume, indem Konflikte zwischen Amazon-EBS-I/O und anderem Datenverkehr von Ihrer Instance minimiert werden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
11.2	Durchführen automatisierter Backups	dynamodb-pitr-enabled	Aktivieren Sie diese Regel, um zu überprüfen, ob die Informationen gesichert wurden. Es verwaltet auch die Backups, indem es sicherstellt, dass die point-in-time Wiederherstellung in Amazon DynamoDB aktiviert ist. Bei der Wiederherstellung werden fortlaufende Backups Ihrer Tabelle für die letzten 35 Tage gespeichert.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
11.2	Durchführen automatisierter Backups	elasticache-redis-cluster-automatic-Backup-Prüfung	Wenn automatische Backups aktiviert sind, ElastiCache erstellt Amazon täglich ein Backup des Clusters. Die Sicherung kann für eine von Ihrer Organisation festgelegte Anzahl von Tagen aufbewahrt werden. Automatische Backups schützen vor Datenverlust. Bei einem Ausfall können Sie einen neuen Cluster erstellen, der Ihre Daten aus dem aktuellen Backup wiederherstellt.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
11.2	Durchführen automatisierter Backups	efs-in-backup-plan	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon Elastic File System (Amazon EFS) -Dateisysteme Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
11.2	Durchführen automatisierter Backups	db-instance-backup-enabled	Die Sicherungsfunktion von Amazon RDS erstellt Sicherungen Ihrer Datenbanken und Transaktionsprotokolle. Amazon RDS erstellt einen Snapshot für das Speichervolume Ihrer DB-Instance, sodass die gesamte DB-Instance gesichert wird. Sie können im System spezifische Aufbewahrungsfristen festlegen, um Ihre Ausfallsicherheitsanforderungen zu erfüllen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
11.2	Durchführen automatisierter Backups	redshift-backup-enabled	Stellen Sie zur Unterstützung der Datensicherungsprozesse sicher, dass Ihre Amazon-Redshift-Cluster über automatisierte Snapshots verfügen. Wenn automatisierte Snapshots für einen Cluster aktiviert sind, erstellt Redshift in regelmäßigen Abständen Snapshots dieses Clusters. Standardmäßig erstellt Redshift alle acht Stunden oder alle 5 GB einen Snapshot für jeden Knoten mit Datenänderungen oder je nachdem, was zuerst eintritt.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
11.2	Durchführen automatisierter Backups	s3- bucket-versioning-enabled	Die Versionsv erwaltung von Amazon Simple Storage Service (Amazon S3)-Bucke ts hilft dabei, mehrere Varianten eines Objekts im selben Amazon-S3-Bucket zu speichern. Verwenden Sie die Versionsv erwaltung, um sämtliche Versionen aller Objekte in Ihrem Amazon-S3-Bucket zu speichern , abzurufen oder wiederherzustellen . Mit der Versionsv erwaltung können Sie Versionen sowohl nach unbeabsic htigten Benutzera ktionen als auch nach Anwendungsfehlern problemlos wiederher stellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
11.2	Durchführen automatisierter Backups	redshift-cluster-maintenancesettings-check	Diese Regel stellt sicher, dass Amazon-Redshift-Cluster die bevorzugten Einstellungen für Ihre Organisation haben. Insbesondere sorgt sie dafür, dass Cluster bevorzugte Wartungsfenster und automatisierte Aufbewahrungsfristen für Snapshots für die Datenbank haben. Für diese Regel müssen Sie die festlegen allowVersionUpgrade. Der Standardwert ist „true“. Außerdem können Sie optional den Zeitraum preferredMaintenanceWindow (der Standardwert ist sa: 16:00 -sa: 16:30) und den automated SnapshotRetention Zeitraum (der Standardwert ist 1) festlegen. Die tatsächlichen Werte müssen den Richtlini

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			en Ihrer Organisation entsprechen.
11.2	Durchführen automatisierter Backups	s3- bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) unterstützt die Aufrechterhaltung einer angemesse nen Kapazität und Verfügbarkeit. CRR ermöglicht das automatische, asynchrone Kopieren von Objekten in Amazon-S3-Buckets, um die Datenverf ügbarkeit sicherzus tellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
11.2	Durchführen automatisierter Backups	s-3 version-lifecycle-policy-check	Mit Amazon-S3-Lebenszyklusregeln können Sie Aktionen definieren, die Amazon S3 während der Lebensdau er eines Objekts ausführen soll (z. B. die Überführu ng von Objekten in eine andere Speicherklasse, ihre Archivierung oder Löschung nach einem bestimmten Zeitraum) .
11,3	Schutz von Wiederher stellungsdaten	backup-recovery-po int-encrypted	Stellen Sie sicher, dass die Verschlüs selung für Ihre AWS Backup-Wiederherst ellungspunkte aktiviert ist. Da sensible Daten auch im Ruhezusta nd vorhanden sein können, sollten Sie die Verschlüsselung im Ruhezustand aktivieren, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
11.3	Schutz von Wiederherstellungsdaten	encrypted-volumes	Aktivieren Sie die Verschlüsselung für Ihre Amazon-Elastic-Block-Store (Amazon-EBS)-Volumes, um eventuell vorhandene sensible Daten sowie Daten im Ruhezustand zu schützen.
11,3	Schutz von Wiederherstellungsdaten	ec-2 ebs-encryption-by-default	Zum Schutz von Daten im Ruhezustand müssen Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon Elastic Block Store (Amazon EBS)-Volumes aktiviert ist. Da sensible Daten auch im Ruhezustand vorhanden sein können, sollten Sie die Verschlüsselung im Ruhezustand aktivieren, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
11,3	Schutz von Wiederherstellungsdaten	rds-storage-encrypted	Zum Schutz von Daten im Ruhezustand müssen Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon Relational Database Service (Amazon RDS)-Instances aktiviert ist. Um eventuell vorhandene sensible Daten im Ruhezustand in Amazon-RDS-Instances zu schützen, muss die Verschlüsselung von Daten im Ruhezustand aktiviert sein.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
11.4	Einrichtung und Verwaltung einer isolierten Instance für Wiederherstellungs daten	dynamodb-in-backup-plan	Um Sie bei Datensich erungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon DynamoDB-Tabellen Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwaltet er Backup-Service mit einer richtlini enbasierten Backup-Lösung. Diese Lösung vereinfacht Ihre Backup-Verwaltung und ermöglicht es Ihnen, Ihre geschäftl ichen und behördlic hen Anforderungen bezüglich Backups zu erfüllen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
11.4	Einrichtung und Verwaltung einer isolierten Instance für Wiederherstellungs daten	ebs-in-backup-plan	Stellen Sie zur Unterstützung der Datensicherungspro zesse sicher, dass Ihre Amazon Elastic Block Store (Amazon EBS) -Volumes Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwaltet er Backup-Service mit einer richtlini enbasierten Backup-Lösung. Diese Lösung vereinfacht Ihre Backup-Verwaltung und ermöglicht es Ihnen, Ihre geschäftl ichen und behördlic hen Anforderungen bezüglich Backups zu erfüllen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
11.4	Einrichtung und Verwaltung einer isolierten Instance für Wiederherstellungs daten	ebs-optimized-instance	Eine optimierte Instance im Amazon Elastic Block Store (Amazon EBS) bietet zusätzliche, dedizierte Kapazität für Amazon-EBS-I/O-Vorgänge. Diese Optimierung bietet die beste Leistung für Ihr EBS-Volume, indem Konflikte zwischen Amazon-EBS-I/O und anderem Datenverkehr von Ihrer Instance minimiert werden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
11.4	Einrichtung und Verwaltung einer isolierten Instance für Wiederherstellungs daten	dynamodb-pitr-enabled	Aktivieren Sie diese Regel, um zu überprüfen, ob die Informationen gesichert wurden. Es verwaltet auch die Backups, indem es sicherstellt, dass die point-in-time Wiederherstellung in Amazon DynamoDB aktiviert ist. Bei der Wiederherstellung werden fortlaufende Backups Ihrer Tabelle für die letzten 35 Tage gespeichert.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
11.4	Einrichtung und Verwaltung einer isolierten Instance für Wiederherstellungs daten	elasticache-redis-cluster-automatic-Backup-Prüfung	Wenn automatische Backups aktiviert sind, ElastiCache erstellt Amazon täglich ein Backup des Clusters. Die Sicherung kann für eine von Ihrer Organisation festgelegte Anzahl von Tagen aufbewahrt werden. Automatische Backups schützen vor Datenverlust. Bei einem Ausfall können Sie einen neuen Cluster erstellen, der Ihre Daten aus dem aktuellen Backup wiederherstellt.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
11.4	Einrichtung und Verwaltung einer isolierten Instance für Wiederherstellungs daten	efs-in-backup-plan	Um Sie bei Datensich erungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon Elastic File System (Amazon EFS) -Dateisysteme Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwaltet er Backup-Service mit einer richtlini enbasierten Backup-Lösung. Diese Lösung vereinfacht Ihre Backup-Verwaltung und ermöglicht es Ihnen, Ihre geschäftl ichen und behördlic hen Anforderungen bezüglich Backups zu erfüllen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
11.4	Einrichtung und Verwaltung einer isolierten Instance für Wiederherstellungs daten	db-instance-backup-enabled	Die Sicherung sfunktion von Amazon RDS erstellt Sicherung en Ihrer Datenbank en und Transakti onsprotokolle. Amazon RDS erstellt einen Snapshot für das Speichervolume Ihrer DB-Instance, sodass die gesamte DB-Instance gesichert wird. Sie können im System spezifische Aufbewahrungsfrist en festlegen, um Ihre Ausfallsicherheits anforderungen zu erfüllen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
11.4	Einrichtung und Verwaltung einer isolierten Instance für Wiederherstellungs daten	redshift-backup-enabled	Stellen Sie zur Unterstützung der Datensicherungspro zesse sicher, dass Ihre Amazon-Re dshift-Cluster über automatisierte Snapshots verfügen. Wenn automatis ierte Snapshots für einen Cluster aktiviert sind, erstellt Redshift in regelmäßi gen Abständen Snapshots dieses Clusters. Standardm äßig erstellt Redshift alle acht Stunden oder alle 5 GB einen Snapshot für jeden Knoten mit Datenände rungen oder je nachdem, was zuerst eintritt.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
11.4	Einrichtung und Verwaltung einer isolierten Instance für Wiederherstellungs daten	s3- bucket-versioning-enabled	Die Versionsv erwaltung von Amazon Simple Storage Service (Amazon S3)-Bucke ts hilft dabei, mehrere Varianten eines Objekts im selben Amazon-S3-Bucket zu speichern. Verwenden Sie die Versionsv erwaltung, um sämtliche Versionen aller Objekte in Ihrem Amazon-S3-Bucket zu speichern , abzurufen oder wiederherzustellen . Mit der Versionsv erwaltung können Sie Versionen sowohl nach unbeabsic htigten Benutzera ktionen als auch nach Anwendungsfehlern problemlos wiederher stellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
11.4	Einrichtung und Verwaltung einer isolierten Instance für Wiederherstellungs daten	redshift-cluster-maintenancesettings-check	Diese Regel stellt sicher, dass Amazon-Redshift-Cluster die bevorzugten Einstellungen für Ihre Organisation haben. Insbesondere sorgt sie dafür, dass Cluster bevorzugte Wartungsfenster und automatisierte Aufbewahrungsfristen für Snapshots für die Datenbank haben. Für diese Regel müssen Sie die festlegen allowVersionUpgrade. Der Standardwert ist „true“. Außerdem können Sie optional den Zeitraum preferredMaintenanceWindow (der Standardwert ist sa: 16:00 -sa: 16:30) und den automated SnapshotRetention Zeitraum (der Standardwert ist 1) festlegen. Die tatsächlichen Werte müssen den Richtlini

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			en Ihrer Organisation entsprechen.
11.4	Einrichtung und Verwaltung einer isolierten Instance für Wiederherstellungs daten	s3- bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) unterstützt die Aufrechterhaltung einer angemesse nen Kapazität und Verfügbarkeit. CRR ermöglicht das automatische, asynchrone Kopieren von Objekten in Amazon-S3-Buckets, um die Datenverf ügbarkeit sicherzus tellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
11.4	Einrichtung und Verwaltung einer isolierten Instance für Wiederherstellungs daten	s-3 version-lifecycle-policy-check	Mit Amazon-S3-Lebenszyklusregeln können Sie Aktionen definieren, die Amazon S3 während der Lebensdau er eines Objekts ausführen soll (z. B. die Überführu ng von Objekten in eine andere Speicherklasse, ihre Archivierung oder Löschung nach einem bestimmten Zeitraum) .

Vorlage

Die Vorlage ist verfügbar unter GitHub: Operational Best Practices for CIS Critical Security Controls v8 IG1.

Bewährte Betriebspraktiken für kritische Sicherheitskontrollen der GUS v8 IG2

Konformitätspakete bieten ein allgemeines Compliance-Framework, das es Ihnen ermöglicht, mithilfe verwalteter oder benutzerdefinierter AWS Config Regeln und Abhilfemaßnahmen Kontrollen zur Sicherheits-, Betriebs- oder Kostenoptimierung durchzuführen. AWS Config Conformance Packs dienen als Beispielvorlagen nicht dazu, die vollständige Einhaltung eines bestimmten Governance- oder Compliance-Standards sicherzustellen. Sie sind dafür verantwortlich, selbst zu beurteilen, ob Ihre Nutzung der Services den geltenden gesetzlichen und behördlichen Anforderungen entspricht.

Im Folgenden finden Sie ein Beispiel für eine Zuordnung zwischen den Critical Security Controls v8 des Center for Internet Security (CIS) IG2 und den AWS verwalteten Konfigurationsregeln. Jede

AWS Config bezieht sich auf eine bestimmte AWS Ressource und bezieht sich auf eine oder mehrere CIS Critical Security Controls IG2 v8-Steuerelemente. Ein CIS Critical Security Controls IG2 v8-Steuerelement kann sich auf mehrere AWS Config Regeln beziehen. In der folgenden Tabelle finden Sie weitere Informationen und Anleitungen zu diesen Zuordnungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
1.1	Einrichtung und Pflege eines detaillierten Inventars der Unternehmensressourcen	eip-attached	Diese Regel stellt sicher, dass Elastic, die einer Amazon Virtual Private Cloud (Amazon VPC) IPs zugewiesen sind, an Amazon Elastic Compute Cloud (Amazon EC2) - Instances oder verwendete Elastic Network Interfaces angehängt sind. Diese Regel hilft bei der Überwachung ungenutzter Inhalte EIPs in Ihrer Umgebung.
1.1	Einrichtung und Pflege eines detaillierten Inventars der Unternehmensressourcen	ec2-stopped-instance	Aktivieren Sie diese Regel, um bei der Basiskonfiguration von Amazon Elastic Compute Cloud (Amazon EC2) - Instances zu helfen, indem Sie überprüfen, ob EC2 Amazon-Instances gemäß

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			den Standards Ihrer Organisation für mehr als die zulässige Anzahl von Tagen gestoppt wurden.
1.1	Einrichtung und Pflege eines detaillierten Inventars der Unternehmensressourcen	vpc-network-acl-unused-überprüfen	Diese Regel stellt sicher, dass Amazon Virtual Private Cloud (VPC)-Netzwerkzugriffskontrolllisten verwendet werden. Die Überwachung ungenutzter Netzwerkzugriffskontrolllisten kann zu einer genauen Inventarisierung und Verwaltung Ihrer Umgebung beitragen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
1.1	Einrichtung und Pflege eines detaillierten Inventars der Unternehmensressourcen	ec2- -Manager instance-managed-by-systems	Eine Bestandsaufnahme der Softwareplattformen und Anwendungen innerhalb des Unternehmens ist möglich, indem Amazon Elastic Compute Cloud (Amazon EC2) - Instances mit AWS Systems Manager verwaltet werden. Verwenden Sie AWS Systems Manager, um detaillierte Systemkonfigurationen, Betriebssystem-Patch-Levels, Namen und Typ der Dienste, Softwareinstallationen, Anwendungsname, Herausgeber und Version sowie andere Details zu Ihrer Umgebung bereitzustellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
1.1	Einrichtung und Pflege eines detaillierten Inventars der Unternehmensressourcen	ec2-check managedinstance-association-compliance-status	Verwenden Sie AWS Systems Manager Associations, um bei der Inventarisierung von Softwareplattformen und Anwendungen innerhalb eines Unternehmens zu helfen. AWS Systems Manager weist Ihren verwalteten Instances einen Konfigurationsstatus zu und ermöglicht es Ihnen, Basiswerte für Betriebssystem-Patch-Levels, Softwareinstallationen, Anwendungskonfigurationen und andere Details zu Ihrer Umgebung festzulegen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
1.1	Einrichtung und Pflege eines detaillierten Inventars der Unternehmensressourcen	ec2-eni security-group-attached-to	Diese Regel stellt sicher, dass die Sicherheitsgruppen an eine Amazon Elastic Compute Cloud (Amazon EC2) -Instance oder an eine ENI angehängt sind. Diese Regel unterstützt die Überwachung ungenutzter Sicherheitsgruppen im Bestand und die Verwaltung Ihrer Umgebung.
2.2	Sicherstellen, dass autorisierte Software derzeit unterstützt wird	elastic-beanstalk-managed-updates-aktiviert	Durch die Aktivierung verwalteter Plattformupdates für eine Amazon-Elastic-Beanstalk-Umgebung wird sichergestellt, dass die aktuellen verfügbaren Plattform-Fixes, -Updates und -Features für die Umgebung installiert sind. Eine bewährte Methode zur Sicherung von Systemen besteht darin, stets die aktuellen Patches zu installieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
2.2	Sicherstellen, dass autorisierte Software derzeit unterstützt wird	ec2- prüfen managedinstance-patch-compliance-status	Aktivieren Sie diese Regel, um bei der Identifizierung und Dokumentation von Sicherheitslücken in Amazon Elastic Compute Cloud (Amazon EC2) zu helfen. Die Regel prüft, ob die EC2 Amazon-Instance die Patch-Konformität im AWS Systems Manager gemäß den Richtlinien und Verfahren Ihrer Organisation einhält.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
2.2	Sicherstellen, dass autorisierte Software derzeit unterstützt wird	ecs-fargate-latest-platform-Version	Sicherheitsupdates und Patches werden automatisch für Ihre AWS Fargate-Aufgaben bereitgestellt. Wenn ein Sicherheitsproblem gefunden wird, das eine AWS Fargate-Plattformversion betrifft, AWS wird die Plattformversion gepatcht. Um Sie bei der Patchverwaltung Ihrer Amazon Elastic Container Service (ECS) - Aufgaben zu unterstützen, auf denen AWS Fargate ausgeführt wird, aktualisieren Sie Ihre eigenständigen Service-Aufgaben, sodass sie die neueste Plattformversion verwenden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
2.4	Tools zur automatisierten Softwareinventur nutzen	ec2-manager instance-managed-by-systems	Eine Bestandsaufnahme der Softwareplattformen und Anwendungen innerhalb des Unternehmens ist möglich, indem Amazon Elastic Compute Cloud (Amazon EC2) - Instances mit AWS Systems Manager verwaltet werden. Verwenden Sie AWS Systems Manager, um detaillierte Systemkonfigurationen, Betriebssystem-Patch-Levels, Namen und Typ der Dienste, Softwareinstallationen, Anwendungsname, Herausgeber und Version sowie andere Details zu Ihrer Umgebung bereitzustellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
2.4	Tools zur automatisierten Softwareinventur nutzen	ec2-check managedinstance-association-compliance-status	Verwenden Sie AWS Systems Manager Associations, um bei der Inventarisierung von Softwareplattformen und Anwendungen innerhalb eines Unternehmens zu helfen. AWS Systems Manager weist Ihren verwalteten Instances einen Konfigurationsstatus zu und ermöglicht es Ihnen, Basiswerte für Betriebssystem-Patch-Levels, Softwareinstallationen, Anwendungskonfigurationen und andere Details zu Ihrer Umgebung festzulegen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.3	Datenzugriffskontrolllisten konfigurieren	ec2-imdsv2-check	Stellen Sie sicher, dass die Methode Instance Metadata Service Version 2 (IMDSv2) aktiviert ist, um den Zugriff auf und die Kontrolle der Amazon Elastic Compute Cloud (Amazon EC2) - Instance-Metadaten zu schützen. Die IMDSv2 Methode verwendet sitzungsbasierte Kontrollen. Mit können Kontrollen implementiert werden IMDSv2, um Änderungen an Instanzmetadaten einzuschränken.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.3	Datenzugriffskontrolllisten konfigurieren	ec2- instance-profile-attached	EC2 Instanzprofile übergeben eine IAM-Rolle an eine Instanz EC2 . Das Anhängen eines Instance-Profils an Ihre Instances kann bei der Implementierung von geringsten Berechtigungen und der Berechtigungsverwaltung helfen.
3.3	Datenzugriffskontrolllisten konfigurieren	dms-replication-not-public	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass auf DMS-Replikationsinstanzen nicht öffentlich zugegriffen werden kann. DMS-Replikations-Instances können vertrauliche Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.3	Datenzugriffskontrolllisten konfigurieren	ebs-snapshot-public-restorable-überprüfen	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass EBS-Snapshots nicht öffentlich wiederherstellbar sind. EBS-Volume-Snapshots können vertrauliche Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.3	Datenzugriffskontrolllisten konfigurieren	emr-kerberos-enabled	Die Zugriffsberechtigungen und -autorisierungen können verwaltet und nach den Prinzipien der geringsten Berechtigung und Aufgabentrennung integriert werden, indem Kerberos für Amazon-EMR-Cluster aktiviert wird. In Kerberos werden Services und Benutzer, die sich authentifizieren müssen, als Prinzipale bezeichnet. Prinzipale befinden sich in einem Kerberos-Bereich. Innerhalb dieses Bereichs wird ein Kerberos-Server als Key Distribution Center (KDC) bezeichnet. Über diesen Server können sich Prinzipale authentifizieren. Die Authentifizierung im KDC erfolgt durch die Ausstellung von Authentif

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			izierungstickets. Das KDC unterhält eine Datenbank der Prinzipale in seinem Bereich mit ihren Passwörtern und anderen administr ativen Informationen zu jedem Prinzipal.
3.3	Datenzugriffskontr olllisten konfigurieren	iam-group-has-users-überprüfen	AWS Identity and Access Managemen t (IAM) kann Ihnen helfen, die Prinzipien der geringsten Rechte und der Aufgabent rennung mit Zugriffsb erechtigungen und Autorisierungen zu integrieren, indem sichergestellt wird, dass IAM-Gruppen mindestens einen Benutzer haben. Die Einteilung von Benutzern in Gruppen auf der Grundlage der ihnen zugewiese nen Berechtigungen oder ihrer Funktion ist eine Möglichkeit, das Prinzip der geringste n Berechtigung zu implementieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.3	Datenzugriffskontrolllisten konfigurieren	iam-no-inline-policy-überprüfen	Stellen Sie sicher, dass ein Benutzer, eine IAM-Rolle oder eine IAM-Gruppe (AWS Identity and Access Management) nicht über eine Inline-Richtlinie zur Zugriffskontrolle auf Systeme und Ressourcen verfügt. AWS empfiehlt, verwaltete Richtlinien anstelle von Inline-Richtlinien zu verwenden. Verwaltete Richtlinien ermöglichen Wiederverwendbarkeit, Versionsverwaltung, Rollback und Delegierung der Berechtigungsverwaltung.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.3	Datenzugriffskontrolllisten konfigurieren	ec2- instance-no-public-ip	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon Elastic Compute Cloud (Amazon EC2) - Instances nicht öffentlich zugänglich sind. EC2Amazon -Instances können vertrauliche Informationen enthalten, und für solche Konten ist eine Zugriffskontrolle erforderlich.
3.3	Datenzugriffskontrolllisten konfigurieren	iam-policy-no-statements-with-full-access	Stellen Sie sicher, dass IAM-Aktionen nur auf die benötigten Aktionen beschränkt sind. Wenn Benutzern mehr Rechte eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und der Aufgabentrennung verstoßen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.3	Datenzugriffskontrolllisten konfigurieren	elasticsearch-in-vpc-only	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass sich Amazon OpenSearch OpenSearch Service (Service) - Domains innerhalb einer Amazon Virtual Private Cloud (Amazon VPC) befinden. Eine OpenSearch Service-Domain innerhalb einer Amazon VPC ermöglicht die sichere Kommunikation zwischen OpenSearch Service und anderen Services innerhalb der Amazon VPC, ohne dass ein Internet-Gateway, ein NAT-Gerät oder eine VPN-Verbindung erforderlich ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.3	Datenzugriffskontrolllisten konfigurieren	iam-user-group-membership-überprüfen	AWS Identity and Access Management (IAM) kann Ihnen helfen, Zugriffsberechtigungen und Autorisierungen einzuschränken, indem sichergestellt wird, dass Benutzer Mitglieder mindestens einer Gruppe sind. Wenn Benutzern mehr Berechtigungen eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und Aufgabentrennung verstoßen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.3	Datenzugriffskontrolllisten konfigurieren	ec2- instances-in-vpc	Stellen Sie Amazon Elastic Compute Cloud (Amazon EC2) -Instances innerhalb einer Amazon Virtual Private Cloud (Amazon VPC) bereit, um eine sichere Kommunikation zwischen einer Instance und anderen Services innerhalb der Amazon VPC zu ermöglichen, ohne dass ein Internet-Gateway, ein NAT-Gerät oder eine VPN-Verbindung erforderlich ist. Der gesamte Datenverkehr bleibt sicher in der AWS Cloud. Domains, die sich innerhalb einer VPC befinden, verfügen aufgrund ihrer logischen Isolierung im Vergleich zu Domains mit öffentlichen Endpunkten über eine zusätzliche Sicherheitsebene. Weisen Sie EC2

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			Amazon-Instances einer Amazon-VPC zu, um den Zugriff ordnungsgemäß zu verwalten.
3.3	Datenzugriffskontrolllisten konfigurieren	emr-master-no-public-ip	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon EMR-Cluster-Masterknoten nicht öffentlich zugänglich sind. Amazon-EMR-Cluster-Hauptknoten können vertrauliche Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.3	Datenzugriffskontrolllisten konfigurieren	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) kann Ihnen dabei helfen, die Prinzipien der geringsten Rechte und der Aufgabentrennung in Zugriffsberechtigungen und Autorisierungen zu integrieren und zu verhindern, dass Richtlinien „Effect“: „Allow“ mit „Action“: „*“ anstelle von „Resource“: „*“ enthalten. Wenn Benutzern mehr Rechte eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und der Aufgabentrennung verstoßen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.3	Datenzugriffskontrolllisten konfigurieren	iam-user-no-policies-überprüfen	Diese Regel stellt sicher, dass AWS Identity and Access Management (IAM) -Richtlinien nur Gruppen oder Rollen zugewiesen werden, um den Zugriff auf Systeme und Ressourcen zu kontrollieren. Die Zuweisung von Berechtigungen auf Gruppen- oder Rollenebene trägt dazu bei, die Wahrscheinlichkeit zu verringern, dass eine Identität übermäßige Berechtigungen erhält oder beibehält.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.3	Datenzugriffskontrolllisten konfigurieren	iam-root-access-key-überprüfen	Der Zugriff auf Systeme und Ressourcen kann gesteuert werden, indem überprüft wird, ob der Root-Benutzer keine Zugriffsschlüssel mit seiner AWS Identity and Access Management (IAM) -Rolle verknüpft hat. Stellen Sie sicher, dass die Root-Zugriffsschlüssel gelöscht werden. Erstellen und verwenden Sie stattdessen rollenbasierte Funktionen, AWS-Konten um das Prinzip der geringsten Funktionalität zu berücksichtigen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.3	Datenzugriffskontrolllisten konfigurieren	iam-user-unused-credentials-überprüfen	AWS Identity and Access Management (IAM) kann Ihnen bei Zugriffsberechtigungen und Autorisierungen helfen, indem es nach IAM-Passwörtern und Zugriffsschlüsseln sucht, die für einen bestimmten Zeitraum nicht verwendet wurden. Wenn ungenutzte Anmeldeinformationen identifiziert werden, müssen Sie sie deaktivieren und/oder entfernen, da dies gegen das Prinzip der geringsten Berechtigung verstoßen könnte. Für diese Regel müssen Sie einen Wert für das maxCredentialUsage Alter festlegen (Standardkonfiguration: 90). Der tatsächliche Wert muss den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.3	Datenzugriffskontrolllisten konfigurieren	iam-customer-policy-blocked-kms-Aktionen	AWS Identity and Access Management (IAM) kann Ihnen helfen, die Prinzipien der geringsten Rechte und der Aufgabentrennung in Zugriffsberechtigungen und Autorisierungen zu integrieren und so zu verhindern, dass Richtlinien blockierte Aktionen für alle AWS Schlüssel des Key Management Service enthalten. Wenn Benutzer mehr Rechte haben, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und Aufgabentrennung verstoßen. Mit dieser Regel können Sie den Parameter festlegen. blockedActionsPatterns (Wert „AWS Bewährte grundlegende Sicherheitsmethode

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			n“: kms: Entschlüs seln, kms:ReEnc ryptFrom). Die tatsächlichen Werte müssen den Richtlini en Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.3	Datenzugriffskontrolllisten konfigurieren	iam-inline-policy-blocked-kms-Aktionen	Stellen Sie sicher, dass ein Benutzer, eine IAM-Rolle oder eine IAM-Gruppe (AWS Identity and Access Management) nicht über eine Inline-Richtlinie verfügt, die blockierte Aktionen für alle AWS Schlüssel des Key Management Service zulässt. AWS empfiehlt, verwaltete Richtlinien anstelle von Inline-Richtlinien zu verwenden. Verwaltete Richtlinien ermöglichen Wiederverwendbarkeit, Versionsverwaltung, Rollback und Delegierung der Berechtigungsverwaltung. Mit dieser Regel können Sie den blockedActionsPatterns Parameter festlegen. (Wert „AWS Bewährte grundlegende Sicherheitsmethoden“: kms: Entschlüsseln, kms:ReEnc

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			ryptFrom). Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.
3.3	Datenzugriffskontrolllisten konfigurieren	lambda-function-public-access-verboten	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass AWS Lambda-Funktionen nicht öffentlich zugänglich sind. Der öffentliche Zugriff kann möglicherweise die Verfügbarkeit von Ressourcen beeinträchtigen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.3	Datenzugriffskontrolllisten konfigurieren	lambda-inside-vpc	Stellen Sie AWS Lambda-Funktionen in einer Amazon Virtual Private Cloud (Amazon VPC) bereit, um eine sichere Kommunikation zwischen einer Funktion und anderen Diensten innerhalb der Amazon VPC zu gewährleisten. Bei dieser Konfiguration sind kein Internet-Gateway, kein NAT-Gerät und keine VPN-Verbindung erforderlich. Der gesamte Datenverkehr bleibt sicher in der Cloud. AWS Domains, die sich innerhalb einer VPC befinden, verfügen aufgrund ihrer logischen Isolierung im Vergleich zu Domains mit öffentlichen Endpunkten über eine zusätzliche Sicherheitsebene. Um den Zugriff ordnungsgemäß zu verwalten,

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			sollten AWS Lambda-Funktionen einer VPC zugewiesen werden.
3.3	Datenzugriffskontrolllisten konfigurieren	rds-snapshots-public-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Relational Database Service (Amazon RDS) -Instances nicht öffentlich sind. Amazon-RDS-Datenbank-Instances können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.3	Datenzugriffskontrolllisten konfigurieren	rds-instance-public-access-überprüfen	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Relational Database Service (Amazon RDS) -Instances nicht öffentlich sind. Amazon-RDS-Datenbank-Instances können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.3	Datenzugriffskontrolllisten konfigurieren	redshift-cluster-public-access-überprüfen	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Redshift Redshift-Cluster nicht öffentlich sind. Amazon-Redshift-Cluster können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.3	Datenzugriffskontrolllisten konfigurieren	s3 bucket-level-public-access - verboten	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Simple Storage Service (Amazon S3) -Buckets nicht öffentlich zugänglich sind. Diese Regel trägt dazu bei, sensible Daten vor unbefugten Remote-Benutzern zu schützen, indem sie den öffentlichen Zugriff auf Bucket-Ebene verhindert.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.3	Datenzugriffskontrolllisten konfigurieren	account-level-public-accesss3-Blöcke-periodisch	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Simple Storage Service (Amazon S3) -Buckets nicht öffentlich zugänglich sind. Diese Regel trägt dazu bei, sensible Daten vor unbefugten Remote-Benutzern zu schützen, indem sie den öffentlichen Zugriff verhindert. Mit dieser Regel können Sie optional die Parameter ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) und restrictPublicBuckets Parameter (Config Default: True) festlegen. Die tatsächlichen Werte müssen den Richtlini

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			en Ihrer Organisation entsprechen.
3.3	Datenzugriffskontrolllisten konfigurieren	s-3 bucket-public-read-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie nur autorisierten Benutzern, Prozessen und Geräten Zugriff auf Amazon Simple Storage Service (Amazon S3) - Buckets gewähren. Die Verwaltung des Zugriffs sollte mit der Klassifizierung der Daten übereinstimmen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.3	Datenzugriffskontrolllisten konfigurieren	s-3 bucket-public-write-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie nur autorisierten Benutzern, Prozessen und Geräten Zugriff auf Amazon Simple Storage Service (Amazon S3) - Buckets gewähren. Die Verwaltung des Zugriffs sollte mit der Klassifizierung der Daten übereinstimmen.
3.3	Datenzugriffskontrolllisten konfigurieren	sagemaker-notebook-no-direct-Internetzugang	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass SageMaker Amazon-Notebooks keinen direkten Internetzugang zulassen. Indem Sie direkten Internetzugang blockieren, vermeiden Sie, dass unbefugte Benutzer auf sensible Daten zugreifen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.3	Datenzugriffskontrolllisten konfigurieren	subnet-auto-assign-public-ip-deaktiviert	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon Virtual Private Cloud (VPC) -Subnetzen nicht automatisch eine öffentliche IP-Adresse zugewiesen wird. Amazon Elastic Compute Cloud (EC2) -Instances, die in Subnetzen gestartet werden, in denen dieses Attribut aktiviert ist, haben ihrer primären Netzwerkschnittstelle eine öffentliche IP-Adresse zugewiesen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.3	Datenzugriffskontrolllisten konfigurieren	ssm-document-not-public	Stellen Sie sicher, dass AWS Systems Manager (SSM) - Dokumente nicht öffentlich sind, da dies einen unbeabsichtigten Zugriff auf Ihre SSM-Dokumente ermöglichen kann. Ein öffentliches SSM-Dokument kann Informationen über Ihr Konto, Ihre Ressourcen und internen Prozesse preisgeben.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.3	Datenzugriffskontr olllisten konfigurieren	ecs-task-definition-user-for-host-mode-check	Wenn für eine Aufgabendefinition erhöhte Berechtig ungen gelten, liegt das daran, dass der Kunde diesen Konfigura tionen ausdrücklich zugestimmt hat. Diese Kontrolle prüft, ob eine unerwartete Berechtigungseskal ation vorliegt, wenn für eine Aufgabend efinition das Host-Netzwerk aktiviert ist, die Kunden aber keine erhöhten Berechtigungen aktiviert haben.
3.3	Datenzugriffskontr olllisten konfigurieren	ecs-task-definition-nonroot-benutzer	Sie bestimmen einen Nicht-Root-Benutzer für den Zugriff auf Ihre Aufgabendefinitionen des Amazon Elastic Container Service (Amazon ECS), um die Implementierung des Prinzips der geringsten Berechtig ung zu unterstützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.3	Datenzugriffskontrolllisten konfigurieren	autoscaling-launch-config-public-ip-deaktiviert	Wenn Sie Ihre Netzwerkschnittstellen mit einer öffentlichen IP-Adresse konfigurieren, sind die diesen Netzwerkschnittstellen zugehörigen Ressourcen über das Internet erreichbar. EC2 Ressourcen sollten nicht öffentlich zugänglich sein, da dies einen unbeabsichtigten Zugriff auf Ihre Anwendungen oder Server ermöglichen kann.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.3	Datenzugriffskontrolllisten konfigurieren	opensearch-in-vpc-only	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass sich Amazon OpenSearch Service-Domains innerhalb einer Amazon Virtual Private Cloud (Amazon VPC) befinden. Eine Amazon OpenSearch Service-Domain innerhalb einer Amazon VPC ermöglicht die sichere Kommunikation zwischen Amazon OpenSearch Service und anderen Services innerhalb der Amazon VPC, ohne dass ein Internet-Gateway, ein NAT-Gerät oder eine VPN-Verbindung erforderlich ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.3	Datenzugriffskontrolllisten konfigurieren	efs-access-point-enforce-root-Verzeichnis	Die Durchsetzung eines Stammverzeichnisses für einen Amazon-Elastic-File-System (Amazon-EFS)-Zugangspunkt trägt dazu bei, den Datenzugriff einzuschränken, indem sichergestellt wird, dass Benutzer des Zugangspunkts nur auf Dateien des angegebenen Unterverzeichnisses zugreifen können.
3.4	Datenaufbewahrung erzwingen	s3- version-lifecycle-policy-check	Mit Amazon-S3-Lebenszyklusregeln können Sie Aktionen definieren, die Amazon S3 während der Lebensdauer eines Objekts ausführen soll (z. B. die Überführung von Objekten in eine andere Speicherklasse, ihre Archivierung oder Löschung nach einem bestimmten Zeitraum).

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.4	Datenaufbewahrung erzwingen	cw-loggroup-retention-period-überprüfen	Stellen Sie sicher, dass die Ereignisprotokolldaten für Ihre Protokollgruppen über eine Mindestdauer aufbewahrt werden, um die Fehlerbehebung und forensische Untersuchungen zu unterstützen. Fehlende frühere Ereignisprotokolldaten erschweren die Rekonstruierung und Identifizierung potenziell schädlicher Ereignisse.
3.10	Verschlüsselung von sensiblen Daten während der Übertragung	api-gw-ssl-enabled	Stellen Sie sicher, dass die REST-API-Stufen von Amazon API Gateway mit SSL-Zertifikaten konfiguriert sind, damit Backend-Systeme überprüfen können, ob Anforderungen von API Gateway stammen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3,10	Verschlüsselung von sensiblen Daten während der Übertragung	alb-http-to-https-Umleitungsprüfung	Um Daten während der Übertragung zu schützen, stellen Sie sicher, dass Ihr Application Load Balancer unverschlüsselte HTTP-Anfragen automatisch an HTTPS umleitet. Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.10	Verschlüsselung von sensiblen Daten während der Übertragung	elb-acm-certificate-required	Zum Schutz von eventuell vorhanden en sensiblen Daten sowie von Daten während der Übertragung muss die Verschlüsselung für Ihr Elastic Load Balancing aktiviert sein. Verwenden Sie AWS Certificate Manager, um öffentlic he und private SSL/ TLS-Zertifikate mit AWS Diensten und internen Ressource n zu verwalten, bereitzustellen und bereitzustellen.
3.10	Verschlüsselung von sensiblen Daten während der Übertragung	elb-tls-https-listeners-nur	Stellen Sie sicher, dass Ihre Elastic Load Balancer (ELBs) mit SSL- oder HTTPS-Listenern konfiguriert sind. Um eventuell vorhanden e sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.10	Verschlüsselung von sensiblen Daten während der Übertragung	s-3 bucket-ssl-requests-only	Um Daten während der Übertragung zu schützen, stellen Sie sicher, dass Ihre Amazon Simple Storage Service (Amazon S3)-Buckets Anfragen zur Verwendung von Secure Socket Layer (SSL)-Buckets erfordern. Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.
3,10	Verschlüsselung von sensiblen Daten während der Übertragung	redshift-require-tls-ssl	Stellen Sie sicher, dass Ihre Amazon-Redshift-Cluster eine TLS/SSL-Verschlüsselung erfordern, um eine Verbindung zu SQL-Clients herzustellen. Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3,10	Verschlüsselung von sensiblen Daten während der Übertragung	Elb v 2 acm-certificate-required	Zum Schutz von eventuell vorhanden en sensiblen Daten sowie von Daten während der Übertragung muss die Verschlüsselung für Ihr Elastic Load Balancing aktiviert sein. Verwenden Sie AWS Certificate Manager, um öffentlic he und private SSL/ TLS-Zertifikate mit AWS Diensten und internen Ressource n zu verwalten, bereitzustellen und bereitzustellen.
3.10	Verschlüsselung von sensiblen Daten während der Übertragung	opensearch-https-required	Da sensible Daten existieren können und um Daten während der Übertragung zu schützen, sollten Sie sicherstellen, dass HTTPS für Verbindun gen zu Ihren Amazon OpenSearch Service-Domains aktiviert ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.10	Verschlüsselung von sensiblen Daten während der Übertragung	elasticsearch-node-to-node-Verschlüsselungsprüfung	Stellen Sie sicher, dass die node-to-node Verschlüsselung für Amazon OpenSearch Service aktiviert ist. Node-to-nodeVerschlüsselung ermöglicht die TLS 1.2-Verschlüsselung für die gesamte Kommunikation innerhalb der Amazon Virtual Private Cloud (Amazon VPC). Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.10	Verschlüsselung von sensiblen Daten während der Übertragung	opensearch-node-to-node-Verschlüsselungsprüfung	Stellen Sie sicher, dass die node-to-node Verschlüsselung für Amazon OpenSearch Service aktiviert ist. Node-to-nodeVerschlüsselung ermöglicht die TLS 1.2-Verschlüsselung für die gesamte Kommunikation innerhalb der Amazon Virtual Private Cloud (Amazon VPC). Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.
3.11	Verschlüsselung von sensiblen Daten im Ruhezustand	cloud-trail-encryption-enabled	Zum Schutz von eventuell vorhandenen sensiblen Daten sowie Daten im Ruhezustand müssen Sie sicherstellen, dass die Verschlüsselung für Ihre AWS CloudTrail aktiviert ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3,11	Verschlüsselung von sensiblen Daten im Ruhezustand	encrypted-volumes	Aktivieren Sie die Verschlüsselung für Ihre Amazon-Elastic-Block-Store (Amazon-EBS)-Volumes, um eventuell vorhandene sensible Daten sowie Daten im Ruhezustand zu schützen.
3,11	Verschlüsselung von sensiblen Daten im Ruhezustand	ec-2 ebs-encryption-by-default	Zum Schutz von Daten im Ruhezustand müssen Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon Elastic Block Store (Amazon EBS)-Volumes aktiviert ist. Da sensible Daten auch im Ruhezustand vorhanden sein können, sollten Sie die Verschlüsselung im Ruhezustand aktivieren, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.11	Verschlüsselung von sensiblen Daten im Ruhezustand	efs-encrypted-check	Aktivieren Sie die Verschlüsselung für Ihr Amazon Elastic File System (EFS), um eventuell vorhandene sensible Daten sowie Daten im Ruhezustand zu schützen.
3,11	Verschlüsselung von sensiblen Daten im Ruhezustand	backup-recovery-point-encrypted	Stellen Sie sicher, dass die Verschlüsselung für Ihre AWS Backup-Wiederherstellungspunkte aktiviert ist. Da sensible Daten auch im Ruhezustand vorhanden sein können, sollten Sie die Verschlüsselung im Ruhezustand aktivieren, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.11	Verschlüsselung von sensiblen Daten im Ruhezustand	elasticsearch-encrypted-at-rest	Da sensible Daten vorhanden sein können und um Daten im Ruhezustand zu schützen, sollten Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon OpenSearch Service (OpenSearch Service) -Domains aktiviert ist.
3.11	Verschlüsselung von sensiblen Daten im Ruhezustand	redshift-cluster-kms-enabled	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass die Verschlüs selung mit AWS Key Management Service (AWS KMS) für Ihren Amazon Redshift Redshift-Cluster aktiviert ist. Um eventuell vorhanden e sensible Daten im Ruhezustand in Redshift-Clustern zu schützen, muss die Verschlüsselung von Daten im Ruhezusta nd aktiviert sein.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.11	Verschlüsselung von sensiblen Daten im Ruhezustand	rds-storage-encrypted	Zum Schutz von Daten im Ruhezustand müssen Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon Relational Database Service (Amazon RDS)-Instances aktiviert ist. Um eventuell vorhandene sensible Daten im Ruhezustand in Amazon-RDS-Instances zu schützen, muss die Verschlüsselung von Daten im Ruhezustand aktiviert sein.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3,11	Verschlüsselung von sensiblen Daten im Ruhezustand	rds-snapshot-encrypted	Stellen Sie sicher, dass die Verschlüsselung für Ihre Amazon Relational Database Service (Amazon RDS)-Snapshots aktiviert ist. Da sensible Daten auch im Ruhezustand vorhanden sein können, sollten Sie die Verschlüsselung im Ruhezustand aktivieren, um diese Daten zu schützen.
3,11	Verschlüsselung von sensiblen Daten im Ruhezustand	s-3 default-encryption-kms	Stellen Sie sicher, dass die Verschlüsselung für Ihre Amazon Simple Storage Service (Amazon S3)-Buckets aktiviert ist. Um eventuell vorhandene sensible Daten im Ruhezustand in einem Amazon-S3-Bucket zu schützen, muss die Verschlüsselung aktiviert sein.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3,11	Verschlüsselung von sensiblen Daten im Ruhezustand	redshift-cluster-configuration-check	Um Daten im Ruhezustand zu schützen, muss die Verschlüsselung für Ihre Amazon-Redshift-Cluster aktiviert sein. Sie müssen auch sicherstellen, dass die erforderlichen Konfigurationen auf Amazon-Redshift-Clustern bereitgestellt werden. Die Prüfungsprotokollierung muss aktiviert sein, um Informationen zu Verbindungen und Benutzeraktivitäten in der Datenbank bereitzustellen. Diese Regel erfordert, dass ein Wert für clusterDbEncrypted (Config Default: TRUE) und LoggingEnabled (Config Default: TRUE) gesetzt ist. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.11	Verschlüsselung von sensiblen Daten im Ruhezustand	sagemaker-endpoint-configuration-kms-schlüsselkonfiguriert	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass die Verschlüsselung mit dem AWS Key Management Service (AWS KMS) für Ihren Endpunkt aktiviert ist. SageMaker Da sensible Daten auf dem SageMaker Endgerät gespeiche rt werden können, sollten Sie die Verschlüsselung im Ruhezustand aktiviere n, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.11	Verschlüsselung von sensiblen Daten im Ruhezustand	sagemaker-notebook-instance-kms-schlüsselkonfiguriert	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass die Verschlüsselung mit dem AWS Key Management Service (AWS KMS) für Ihr Notebook aktiviert ist. SageMaker Da vertrauliche Daten im SageMaker Notebook gespeichert werden können, sollten Sie die Verschlüsselung im Ruhezustand aktivieren, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.11	Verschlüsselung von sensiblen Daten im Ruhezustand	secretsmanager-using-cmk	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass die Verschlüsselung mit dem AWS Key Management Service (AWS KMS) für AWS Secrets Manager aktiviert ist. Aktivieren Sie die Verschlüsselung von Daten im Ruhezustand, um eventuell vorhandene sensible Daten im Ruhezustand im Secrets Manager zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.11	Verschlüsselung von sensiblen Daten im Ruhezustand	s3-fähig bucket-server-side-encryption	Zum Schutz von Daten im Ruhezustand müssen Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon Simple Storage Service (Amazon S3)-Buckets aktiviert ist. Um eventuell vorhandene sensible Daten im Ruhezustand in Amazon-S3-Buckets zu schützen, muss die Verschlüsselung aktiviert sein.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.11	Verschlüsselung von sensiblen Daten im Ruhezustand	sns-encrypted-kms	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass Ihre Amazon Simple Notification Service (Amazon SNS) -Themen mit dem AWS Key Management Service (AWS KMS) verschlüsselt werden müssen. Um eventuell vorhandene sensible Daten im Ruhezustand in veröffentlichten Nachrichten zu schützen, muss die Verschlüsselung von Daten im Ruhezustand aktiviert sein.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.11	Verschlüsselung von sensiblen Daten im Ruhezustand	dynamodb-table-encrypted-kms	Stellen Sie sicher, dass die Verschlüsselung für Ihre Amazon-DynamoDB-Tabellen aktiviert ist. Um eventuell vorhandene sensible Daten im Ruhezustand in diesen Tabellen zu schützen, müssen Sie die Verschlüsselung von Daten im Ruhezustand aktivieren. Standardmäßig werden DynamoDB-Tabellen mit einem AWS eigenen Kundenhauptschlüssel (CMK) verschlüselt.
3.11	Verschlüsselung von sensiblen Daten im Ruhezustand	opensearch-encrypted-at-rest	Da sensible Daten vorhanden sein können und um Daten im Ruhezustand zu schützen, sollten Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon OpenSearch Service-Domains aktiviert ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
4.1	Einrichtung und Pflege eines sicheren Konfigurationsprozesses	account-part-of-organizations	Durch die zentrale Verwaltung AWS-Konten innerhalb von AWS Organizations wird sichergestellt, dass die Konten den Vorschriften entsprechen. Eine fehlende zentrale Kontoverwaltung kann zu inkonsistenten Kontokonfigurationen führen, wodurch Ressourcen und sensible Daten offengelegt werden können.
4.1	Einrichtung und Pflege eines sicheren Konfigurationsprozesses	ec2-stopped-instance	Aktivieren Sie diese Regel, um bei der Basiskonfiguration von Amazon Elastic Compute Cloud (Amazon EC2) - Instances zu helfen, indem Sie überprüfen, ob EC2 Amazon-Instances gemäß den Standards Ihrer Organisation für mehr als die zulässige Anzahl von Tagen gestoppt wurden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
4.1	Einrichtung und Pflege eines sicheren Konfigurationsprozesses	ec2- volume-inuse-check	Diese Regel stellt sicher, dass Amazon Elastic Block Store-Volumes, die an Amazon Elastic Compute Cloud (Amazon EC2) - Instances angehängt sind, zum Löschen markiert werden, wenn eine Instance beendet wird. Wenn ein Amazon-EBS-Volume nicht gelöscht wird, wenn die Instance, an die es angehängt ist, beendet wird, kann dies gegen das Konzept der geringsten Funktionalität verstoßen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
4.1	Einrichtung und Pflege eines sicheren Konfigurationsprozesses	redshift-cluster-maintenancesettings-check	Diese Regel stellt sicher, dass Amazon-Redshift-Cluster die bevorzugten Einstellungen für Ihre Organisation haben. Insbesondere sorgt sie dafür, dass Cluster bevorzugte Wartungsfenster und automatisierte Aufbewahrungsfristen für Snapshots für die Datenbank haben. Für diese Regel müssen Sie die festlegen allowVersionUpgrade. Der Standardwert ist „true“. Außerdem können Sie optional den Zeitraum preferredMaintenanceWindow (der Standardwert ist sa: 16:00 -sa: 16:30) und den automated SnapshotRetention Zeitraum (der Standardwert ist 1) festlegen. Die tatsächlichen Werte müssen den Richtlini

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			en Ihrer Organisation entsprechen.
4.1	Einrichtung und Pflege eines sicheren Konfigurationsprozesses	ec2-manager instance-managed-by-systems	Eine Bestandsaufnahme der Softwareplattformen und Anwendungen innerhalb des Unternehmens ist möglich, indem Amazon Elastic Compute Cloud (Amazon EC2) - Instances mit AWS Systems Manager verwaltet werden. Verwenden Sie AWS Systems Manager, um detaillierte Systemkonfigurationen, Betriebssystem-Patch-Levels, Namen und Typ der Dienste, Softwareinstallationen, Anwendungsname, Herausgeber und Version sowie andere Details zu Ihrer Umgebung bereitzustellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
4.1	Einrichtung und Pflege eines sicheren Konfigurationsprozesses	ec2-check managedinstance-association-compliance-status	Verwenden Sie AWS Systems Manager Associations, um bei der Inventarisierung von Softwareplattformen und Anwendungen innerhalb eines Unternehmens zu helfen. AWS Systems Manager weist Ihren verwalteten Instances einen Konfigurationsstatus zu und ermöglicht es Ihnen, Basiswerte für Betriebssystem-Patch-Levels, Softwareinstallationen, Anwendungskonfigurationen und andere Details zu Ihrer Umgebung festzulegen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
4.1	Einrichtung und Pflege eines sicheren Konfigurationsprozesses	efs-access-point-enforce-root-Verzeichnis	Die Durchsetzung eines Stammverzeichnisses für einen Amazon-Elastic-File-System (Amazon-EFS)-Zugangspunkt trägt dazu bei, den Datenzugriff einzuschränken, indem sichergestellt wird, dass Benutzer des Zugangspunkts nur auf Dateien des angegebenen Unterverzeichnisses zugreifen können.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
4.1	Einrichtung und Pflege eines sicheren Konfigurationsprozesses	secretsmanager-rotation-enabled-check	Diese Regel stellt sicher, dass bei AWS Secrets Manager Manager-Geheimnissen die Rotation aktiviert ist. Die regelmäßige Rotation von Secrets kann den Zeitraum verkürzen, in dem ein Secret aktiv ist, und möglicherweise die Auswirkungen auf das Unternehmen verringern, falls das Secret kompromittiert wird.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
4.1	Einrichtung und Pflege eines sicheren Konfigurationsprozesses	access-keys-rotated	Die Anmeldeinformationen für autorisierte Geräte, Benutzer und Prozesse werden geprüft, indem sichergestellt wird, dass die IAM-Zugriffsschlüssel gemäß den Vorgaben der Unternehmensrichtlinie rotiert werden. Das regelmäßige Ändern der Zugriffsschlüssel ist eine bewährte Sicherheitsmethode. Es verkürzt den Zeitraum, in dem ein Zugriffsschlüssel aktiv ist, und reduziert die Auswirkungen auf das Unternehmen, wenn die Schlüssel kompromittiert werden. Diese Regel erfordert einen Wert für die Zugriffsschlüssel-Rotation (Standardkonfiguration: 90). Der tatsächliche Wert muss den Richtlini

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			en Ihrer Organisation entsprechen.
4.6	Sichere Verwaltung von Unternehmensressourcen und -software	alb-http-to-https-Umleitungsprüfung	Um Daten während der Übertragung zu schützen, stellen Sie sicher, dass Ihr Application Load Balancer unverschlüsselte HTTP-Anfragen automatisch an HTTPS umleitet. Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.
4.6	Sichere Verwaltung von Unternehmensressourcen und -software	elb-tls-https-listeners-nur	Stellen Sie sicher, dass Ihre Elastic Load Balancer (ELBs) mit SSL- oder HTTPS-Listenern konfiguriert sind. Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
4.6	Sichere Verwaltung von Unternehmensressourcen und -software	api-gw-ssl-enabled	Stellen Sie sicher, dass die REST-API-Stufen von Amazon API Gateway mit SSL-Zertifikaten konfiguriert sind, damit Backend-Systeme überprüfen können, ob Anforderungen von API Gateway stammen.
4,6	Sichere Verwaltung von Unternehmensressourcen und -software	redshift-require-tls-ssl	Stellen Sie sicher, dass Ihre Amazon-Redshift-Cluster eine TLS/SSL-Verschlüsselung erfordern, um eine Verbindung zu SQL-Clients herzustellen. Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
4,6	Sichere Verwaltung von Unternehmensressourcen und -software	s-3 bucket-ssl-requests-only	Um Daten während der Übertragung zu schützen, stellen Sie sicher, dass Ihre Amazon Simple Storage Service (Amazon S3)-Buckets Anfragen zur Verwendung von Secure Socket Layer (SSL)-Buckets erfordern. Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.
4,6	Sichere Verwaltung von Unternehmensressourcen und -software	opensearch-https-required	Da sensible Daten existieren können und um Daten während der Übertragung zu schützen, sollten Sie sicherstellen, dass HTTPS für Verbindungen zu Ihren Amazon OpenSearch Service-Domains aktiviert ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
4.7	Standardkonten für Unternehmensressourcen und -software verwalten	iam-root-access-key-überprüfen	Der Zugriff auf Systeme und Ressourcen kann gesteuert werden, indem überprüft wird, ob der Root-Benutzer keine Zugriffsschlüssel mit seiner AWS Identity and Access Management (IAM) -Rolle verknüpft hat. Stellen Sie sicher, dass die Root-Zugriffsschlüssel gelöscht werden. Erstellen und verwenden Sie stattdessen rollenbasierte Funktionen, AWS-Konten um das Prinzip der geringsten Funktionalität zu berücksichtigen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
5.1	Erstellen und Verwalten eines Konteninventars	account-part-of-organizations	Durch die zentrale Verwaltung AWS-Konten innerhalb von AWS Organizations wird sichergestellt, dass die Konten den Vorschriften entsprechen. Eine fehlende zentrale Kontoverwaltung kann zu inkonsistenten Kontokonfigurationen führen, wodurch Ressourcen und sensible Daten offengelegt werden können.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
5.2	Verwendung eindeutiger Passwörter	iam-password-policy	Die Identitäten und Anmeldeinformationen werden auf der Grundlage einer organisatorischen IAM-Passwortrichtlinie ausgestellt, verwaltet und verifiziert. Sie erfüllen oder übertreffen die Anforderungen des NIST SP 800-63 und des AWS Foundational Security Best Practices-Standards für Passwortstärke. Mit dieser Regel können Sie optional RequireUppercaseCharacters (Wert für AWS grundlegende Sicherheitsbewährte Methoden: wahr), RequireLowercaseCharacters (Wert für bewährte Methoden für AWS grundlegende Sicherheit: wahr), RequireSymbols (Wert für bewährte Methoden für AWS grundlegende Sicherheit:

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			wahr), RequireNumbers (Wert für bewährte Methoden für AWS grundlegende Sicherheit: wahr), MinimumPasswordLength (Wert für bewährte Methoden für AWS grundlegende Sicherheit: 14), PasswordReusePrevention (Wert für bewährte Methoden für AWS grundlegende Sicherheit: 24) und MaxPasswordAge (Wert für bewährte Methoden für AWS grundlegende Sicherheit: 90) für Ihr IAM festlegen Kennwortrichtlinie. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
5.2	Verwendung eindeutiger Passwörter	iam-user-mfa-enabled	Aktivieren Sie diese Regel, um den Zugriff auf Ressourcen in der AWS -Cloud einzuschränken. Diese Regel stellt sicher, dass die Multi-Faktor-Authentifizierung (MFA) für alle Benutzer aktiviert ist. MFA bietet eine weitere Schutzebene zusätzlich zum Benutzernamen und Passwort. Reduzieren Sie Fälle von kompromittierten Konten, indem Sie MFA für Benutzer vorschreiben.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
5.2	Verwendung eindeutiger Passwörter	mfa-enabled-for-iam-Konsolenzugriff	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass MFA für alle AWS Identity and Access Management (IAM) -Benutzer aktiviert ist, die über ein Konsolenkennwort verfügen. MFA sorgt für eine weitere Schutzebene zusätzlich zu den Anmeldeinformationen. Indem Sie MFA für Benutzer vorschreiben, können Sie Fälle kompromittierter Konten reduzieren und verhindern, dass unbefugte Benutzer auf vertrauliche Daten zugreifen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
5.2	Verwendung eindeutiger Passwörter	root-account-mfa-enabled	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass MFA für den Root-Benutzer aktiviert ist. Der Stammbenutzer ist der AWS-Konto-Benutzer mit den meisten Berechtigungen. MFA bietet eine weitere Schutzebene zusätzlich zum Benutzernamen und Passwort. Indem Sie MFA für den Root-Benutzer vorschreiben, können Sie die Anzahl AWS-Konten kompromittierter Benutzer reduzieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
5.3	Deaktivierung inaktiver Konten	iam-user-unused-credentials-überprüfen	AWS Identity and Access Management (IAM) kann Ihnen bei Zugriffsberechtigungen und Autorisierungen helfen, indem es nach IAM-Passwörtern und Zugriffsschlüsseln sucht, die für einen bestimmten Zeitraum nicht verwendet wurden. Wenn ungenutzte Anmeldeinformationen identifiziert werden, müssen Sie sie deaktivieren und/oder entfernen, da dies gegen das Prinzip der geringsten Berechtigung verstoßen könnte. Für diese Regel müssen Sie einen Wert für das maxCredentialUsage Alter festlegen (Standardkonfiguration: 90). Der tatsächliche Wert muss den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
5.4	Beschränkung der Administratorrechte auf spezielle Administratorkonten	iam-root-access-key-überprüfen	Der Zugriff auf Systeme und Ressourcen kann gesteuert werden, indem überprüft wird, ob der Root-Benutzer keine Zugriffsschlüssel mit seiner AWS Identity and Access Management (IAM) -Rolle verknüpft hat. Stellen Sie sicher, dass die Root-Zugriffsschlüssel gelöscht werden. Erstellen und verwenden Sie stattdessen rollenbasierte Funktionen, AWS-Konten um das Prinzip der geringsten Funktionalität zu berücksichtigen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
5.4	Beschränkung der Administratorrechte auf spezielle Administratorkonten	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) kann Ihnen dabei helfen, die Prinzipien der geringsten Rechte und der Aufgabentrennung in Zugriffsberechtigungen und Autorisierungen zu integrieren und zu verhindern, dass Richtlinien „Effect“: „Allow“ mit „Action“: „*“ anstelle von „Resource“: „*“ enthalten. Wenn Benutzern mehr Rechte eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und der Aufgabentrennung verstoßen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
5.6	Zentralisierung der Kontoverwaltung	account-part-of-organizations	Durch die zentrale Verwaltung AWS-Konten innerhalb von AWS Organizations wird sichergestellt, dass die Konten den Vorschriften entsprechen. Eine fehlende zentrale Kontoverwaltung kann zu inkonsistenten Kontokonfigurationen führen, wodurch Ressourcen und sensible Daten offengelegt werden können.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
6.4	Erzwingen von MFA für Remote-Netzwerkzugriff	iam-user-mfa-enabled	Aktivieren Sie diese Regel, um den Zugriff auf Ressourcen in der AWS -Cloud einzuschränken. Diese Regel stellt sicher, dass die Multi-Faktor-Authentifizierung (MFA) für alle Benutzer aktiviert ist. MFA bietet eine weitere Schutzebene zusätzlich zum Benutzernamen und Passwort. Reduzieren Sie Fälle von kompromittierten Konten, indem Sie MFA für Benutzer vorschreiben.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
6.4	Erzwingen von MFA für Remote-Netzwerkzugriff	mfa-enabled-for-iam-Konsolenzugriff	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass MFA für alle AWS Identity and Access Management (IAM) -Benutzer aktiviert ist, die über ein Konsolenkennwort verfügen. MFA sorgt für eine weitere Schutzebene zusätzlich zu den Anmeldeinformationen. Indem Sie MFA für Benutzer vorschreiben, können Sie Fälle kompromittierter Konten reduzieren und verhindern, dass unbefugte Benutzer auf vertrauliche Daten zugreifen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
6.4	Erzwingen von MFA für Remote-Netzwerkzugriff	root-account-mfa-enabled	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass MFA für den Root-Benutzer aktiviert ist. Der Stammbenutzer ist der AWS-Konto-Benutzer mit den meisten Berechtigungen. MFA bietet eine weitere Schutzebene zusätzlich zum Benutzernamen und Passwort. Indem Sie MFA für den Root-Benutzer vorschreiben, können Sie die Anzahl AWS-Konten kompromittierter Benutzer reduzieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
6,5	Erzwingen von MFA für Administratorzugriff	root-account-hardware-mfa-aktiviert	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Hardware-MFA für den Root-Benutzer aktiviert ist. Der Stammbenutzer ist der AWS-Konto-Benutzer mit den meisten Berechtigungen. MFA sorgt für eine weitere Schutzebene zusätzlich zu den Anmeldeinformationen. Indem Sie MFA für den Root-Benutzer vorschreiben, können Sie die Anzahl AWS-Konten kompromittierter Benutzer reduzieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
6.7	Zentralisierung der Zugriffskontrolle	account-part-of-organizations	Durch die zentrale Verwaltung AWS-Konten innerhalb von AWS Organizations wird sichergestellt, dass die Konten den Vorschriften entsprechen. Eine fehlende zentrale Kontoverwaltung kann zu inkonsistenten Kontokonfigurationen führen, wodurch Ressourcen und sensible Daten offengelegt werden können.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
7.1	Einrichtung und Pflege eines Prozesses für das Schwachstellenmanagement	guardduty-enabled-centralized	Amazon GuardDuty kann mithilfe von Threat Intelligence Feeds helfen, potenzielle Cybersicherheitsereignisse zu überwachen und zu erkennen. Dazu gehören Listen mit bösartigen IPs und maschinellen Lernmethoden zur Identifizierung unerwarteter, nicht autorisierter und bösartiger Aktivitäten in Ihrer AWS Cloud-Umgebung.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
7.1	Einrichtung und Pflege eines Prozesses für das Schwachstellenmanagement	securityhub-enabled	AWS Security Hub hilft bei der Überwachung von unbefugtem Personal, Verbindungen, Geräten und Software. AWS Security Hub aggregiert, organisiert und priorisiert die Sicherheitswarnungen oder Ergebnisse mehrerer Dienste. AWS Einige dieser Dienste sind Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer und AWS Firewall Manager sowie AWS Partnerlösungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
7.1	Einrichtung und Pflege eines Prozesses für das Schwachstellenmanagement	ec2-prüfen managedinstance-patch-compliance-status	Aktivieren Sie diese Regel, um bei der Identifizierung und Dokumentation von Sicherheitslücken in Amazon Elastic Compute Cloud (Amazon EC2) zu helfen. Die Regel prüft, ob die EC2 Amazon-Instance die Patch-Konformität im AWS Systems Manager gemäß den Richtlinien und Verfahren Ihrer Organisation einhält.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
7.3	Durchführen eines automatisierten Betriebssystem-Patch-Managements	ec2-check managedinstance-patch-compliance-status	Aktivieren Sie diese Regel, um bei der Identifizierung und Dokumentation von Sicherheitslücken in Amazon Elastic Compute Cloud (Amazon EC2) zu helfen. Die Regel prüft, ob die EC2 Amazon-Instance die Patch-Konformität im AWS Systems Manager gemäß den Richtlinien und Verfahren Ihrer Organisation einhält.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
7.3	Durchführen eines automatisierten Betriebssystem-Patch-Managements	elastic-beanstalk-managed-updates-aktiviert	Durch die Aktivierung verwalteter Plattform updates für eine Amazon-Elastic-Beanstalk-Umgebung wird sichergestellt, dass die aktuellen verfügbaren Plattform -Fixes, -Updates und -Features für die Umgebung installiert sind. Eine bewährte Methode zur Sicherung von Systemen besteht darin, stets die aktuellen Patches zu installieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
7.3	Durchführen eines automatisierten Betriebssystem-Patch-Managements	redshift-cluster-maintenancesettings-check	Diese Regel stellt sicher, dass Amazon-Redshift-Cluster die bevorzugten Einstellungen für Ihre Organisation haben. Insbesondere sorgt sie dafür, dass Cluster bevorzugte Wartungsfenster und automatisierte Aufbewahrungsfristen für Snapshots für die Datenbank haben. Für diese Regel müssen Sie die allowVersionUpgrade festlegen. Der Standardwert ist „true“. Außerdem können Sie optional den Zeitraum preferredMaintenanceWindow (der Standardwert ist sa: 16:00 -sa: 16:30) und den automated SnapshotRetention Zeitraum (der Standardwert ist 1) festlegen. Die tatsächlichen Werte müssen den Richtlini

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			en Ihrer Organisation entsprechen.
7.4	Durchführen eines automatisierten Anwendungspatch-Managements	ec2- -check managedinstance-patch-compliance-status	Aktivieren Sie diese Regel, um bei der Identifizierung und Dokumentation von Sicherheitslücken in Amazon Elastic Compute Cloud (Amazon EC2) zu helfen. Die Regel prüft, ob die EC2 Amazon-Instance die Patch-Konformität im AWS Systems Manager gemäß den Richtlinien und Verfahren Ihrer Organisation einhält.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
7.4	Durchführen eines automatisierten Anwendungspatch-Managements	elastic-beanstalk-managed-updates-aktiviert	Durch die Aktivierung verwalteter Plattform updates für eine Amazon-Elastic-Beanstalk-Umgebung wird sichergestellt, dass die aktuellen verfügbaren Plattform -Fixes, -Updates und -Features für die Umgebung installiert sind. Eine bewährte Methode zur Sicherung von Systemen besteht darin, stets die aktuellen Patches zu installieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
7.4	Durchführen eines automatisierten Anwendungspatch-Managements	redshift-cluster-maintenancesettings-check	Diese Regel stellt sicher, dass Amazon-Redshift-Cluster die bevorzugten Einstellungen für Ihre Organisation haben. Insbesondere sorgt sie dafür, dass Cluster bevorzugte Wartungsfenster und automatisierte Aufbewahrungsfristen für Snapshots für die Datenbank haben. Für diese Regel müssen Sie die allowVersionUpgrade festlegen. Der Standardwert ist „true“. Außerdem können Sie optional den Zeitraum preferredMaintenanceWindow (der Standardwert ist sa: 16:00 -sa: 16:30) und den automated SnapshotRetention Zeitraum (der Standardwert ist 1) festlegen. Die tatsächlichen Werte müssen den Richtlini

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			en Ihrer Organisation entsprechen.
7,5	Durchführen eines automatisierten Schwachstellenscans interner Unternehmensressourcen	ecr-private-image-scanning-aktiviert	Der Amazon Elastic Container Repository (ECR)-Image-Scan unterstützt die Identifizierung von Software-Schwachstellen in Ihren Container-Images. Durch die Aktivierung von Image-Scans in ECR-Repositorys werden die Integrität und Sicherheit der gespeicherten Images mit einer zusätzlichen Überprüfungsebene verbessert.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
8.1	Einrichtung und Pflege eines Prozesses zur Verwaltung von Prüfprotokollen	audit-log-policy-exists (Prozessprüfung)	Richten Sie eine Richtlinie zur Verwaltung von Prüfprotokollen ein, in der die Protokoll ierungsanforderung en Ihres Unternehm ens definiert sind, und pflegen Sie diese Richtlinie. Dies beinhaltet, ist aber nicht beschränkt auf die Überprüfung und Aufbewahrung von Prüfprotokollen.
8.2	Erfassung von Prüfprotokollen	api-gw-execution-l ogging-aktiviert	Die API-Gateway-Protokollierung zeigt detaillierte Ansichten der Benutzer, die auf die API zugegriff en haben, und wie diese Benutzer auf die API zugegriff en haben. Diese Einblicke ermöglichen die Transparenz von Benutzeraktivitäten.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
8.2	Erfassung von Prüfprotokollen	multi-region-cloudtrail-enabled	AWS CloudTrail zeichnet Aktionen und API-Aufrufe der AWS Management Console auf. Sie können feststellen, welche Benutzer und Konten angerufen wurden AWS, von welcher Quell-IP-Adresse aus die Anrufe getätigt wurden und wann die Anrufe erfolgten. CloudTrail übermittelt Protokolldateien aus allen AWS Regionen an Ihren S3-Bucket , wenn MULTI_REG ION_CLOUD _TRAIL_ENABLED aktiviert ist. Außerdem wird beim AWS Start einer neuen Region derselbe Trail in der neuen Region erstellt. CloudTrail Dadurch erhalten Sie automatis ch Protokolldateien mit API-Aktivitäten für die neue Region.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
8.2	Erfassung von Prüfprotokollen	cloudtrail-s3-data events-enabled	Die Erfassung von Simple Storage Service (Amazon S3)-Datenereignissen unterstützt die Erkennung von ungewöhnlichen Aktivitäten. Zu den Details gehören Informationen zu dem AWS -Konto, das auf einen Amazon-S3-Bucket zugegriffen hat, die IP-Adresse und die Uhrzeit des Ereignisses.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
8.2	Erfassung von Prüfprotokollen	cloudtrail-enabled	AWS CloudTrai l kann durch die Aufzeichnung von Aktionen und API-Aufrufen in der AWS Management Console bei der Nichtabst reitbarkeit helfen. Sie können die Benutzer und die Benutzer AWS-Konten , die einen AWS Dienst aufgerufen haben, die Quell-IP-Adresse, über die die Aufrufe generiert wurden, und den Zeitpunkt der Anrufe identifiz ieren. Einzelheiten zu den erfassten Daten finden Sie in den AWS CloudTrail Datensatzinhalten.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
8.2	Erfassung von Prüfprotokollen	cloud-trail-cloud-watch-logs-aktiviert	Verwenden Sie Amazon CloudWatch , um Protokoll ereignisaktivitäten zentral zu sammeln und zu verwalten. Die Aufnahme von AWS CloudTrail Daten liefert Einzelheiten zu den API-Aufrufaktivitäten in Ihrem AWS-Konto.
8.2	Erfassung von Prüfprotokollen	elasticsearch-logs-to-cloudwatch	Stellen Sie sicher, dass für Amazon OpenSearch Service-Domains Fehlerprotokolle aktiviert und zur Aufbewahrung und Beantwortung an Amazon CloudWatch Logs gestreamt werden. Domain-Fehlerprotokolle sind bei Sicherheits- und Zugriffsprüfungen sowie bei der Diagnose von Verfügbarkeitsproblemen nützlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
8.2	Erfassung von Prüfprotokollen	vpc-flow-logs-enabled	VPC-Flow-Protokolle erfassen detaillierte Informationsdatensätze über den IP-Datenverkehr, der zu und von Netzwerkschnittstellen in Ihrer Amazon Virtual Private Cloud (Amazon VPC) fließt. Standardmäßig enthalten Flow-Protokolldatensätze Werte für die verschiedenen Komponenten des IP-Flows, einschließlich Quelle, Ziel und Protokoll.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
8.2	Erfassung von Prüfprotokollen	elb-logging-enabled	Die Elastic-Load-Balancing-Aktivität ist ein zentraler Kommunikationspunkt innerhalb einer Umgebung. Stellen Sie sicher, dass die ELB-Protokollierung aktiviert ist. Die gesammelten Daten enthalten detaillierte Informationen zu Anfragen, die an den ELB gesendet wurden. Jedes Protokoll enthält Informationen wie die Zeit, zu der die Anforderung einging, die Client-IP-Adresse, Latenzen, Anforderungspfade und Serverantworten.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
8.2	Erfassung von Prüfprotokollen	rds-logging-enabled	Um die Protokollierung und Überwachung in Ihrer Umgebung zu erleichtern, stellen Sie sicher, dass die Amazon Relational Database Service (Amazon RDS)-Protokollierung aktiviert ist. Mit der Amazon-RDS-Protokollierung können Sie Ereignisse wie Verbindungen, Verbindungsabbrüche, Abfragen oder abgefragte Tabellen erfassen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
8.2	Erfassung von Prüfprotokollen	s-3 bucket-logging-enabled	Die Amazon Simple Storage Service (Amazon S3)-Serverzugriffs protokollierung bietet eine Methode zur Überwachu ng des Netzwerks im Hinblick auf potenzielle Cybersich erheitsereignisse. Die Ereignisse werden überwacht, indem detaillierte Aufzeichn ungen über die Anfragen erfasst werden, die an einen Amazon-S3-Bucket gestellt wurden. Jeder Zugriffsprotokolle intrag enthält Details zu einer einzelnen Zugriffsanfrage. Zu den Details gehören Anforderer, Bucket-Name, Anforderu ngszeit, Anforderu ngsaktion, Antwortst atus und Fehlercode, falls relevant.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
8,2	Erfassung von Prüfprotokollen	redshift-cluster-configuration-check	Um Daten im Ruhezustand zu schützen, muss die Verschlüsselung für Ihre Amazon-Redshift-Cluster aktiviert sein. Sie müssen auch sicherstellen, dass die erforderlichen Konfigurationen auf Amazon-Redshift-Clustern bereitgestellt werden. Die Prüfungsprotokollierung muss aktiviert sein, um Informationen zu Verbindungen und Benutzeraktivitäten in der Datenbank bereitzustellen. Diese Regel erfordert, dass ein Wert für clusterDbEncrypted (Config Default: TRUE) und LoggingEnabled (Config Default: TRUE) gesetzt ist. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
8.2	Erfassung von Prüfprotokollen	wafv2-logging-enabled	Um die Protokollierung und Überwachung in Ihrer Umgebung zu erleichtern, aktivieren Sie die AWS WAF (V2) -Protokollierung im regionalen und globalen Web ACLs. AWS Die WAF-Protokollierung bietet detaillierte Informationen über den Datenverkehr, der von Ihrer Web-ACL analysiert wird. In den Protokollen werden die Uhrzeit aufgezeichnet, zu der die AWS WAF die Anfrage von Ihrer AWS Ressource erhalten hat, Informationen über die Anfrage und eine Aktion für die Regel, der jede Anfrage entsprach.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
8.2	Erfassung von Prüfprotokollen	codebuild-project-logging-enabled	Stellen Sie sicher, dass die AWS CodeBuild Projektprotokollierung aktiviert ist, damit Ihre Build-Ausgabeprotokolle entweder an Amazon CloudWatch oder Amazon Simple Storage Service (Amazon S3) gesendet werden. Build-Ausgabeprotokolle enthalten detaillierte Informationen zu Ihrem Build-Projekt.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
8.3	Gewährleisten einer angemessene Speicherung der Prüfprotokolle	s-3 version-lifecycle-policy-check	Mit Amazon-S3-Lebenszyklusregeln können Sie Aktionen definieren, die Amazon S3 während der Lebensdauer eines Objekts ausführen soll (z. B. die Überführung von Objekten in eine andere Speicherklasse, ihre Archivierung oder Löschung nach einem bestimmten Zeitraum).
8,5	Erfassung detaillierter Prüfprotokolle	api-gw-execution-logging-aktiviert	Die API-Gateway-Protokollierung zeigt detaillierte Ansichten der Benutzer, die auf die API zugegriffen haben, und wie diese Benutzer auf die API zugegriffen haben. Diese Einblicke ermöglichen die Transparenz von Benutzeraktivitäten.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
8.5	Erfassung detaillierter Prüfprotokolle	multi-region-cloudtrail-enabled	AWS CloudTrail zeichnet Aktionen und API-Aufrufe der AWS Management Console auf. Sie können feststellen, welche Benutzer und Konten angerufen wurden AWS, von welcher Quell-IP-Adresse aus die Anrufe getätigt wurden und wann die Anrufe erfolgten. CloudTrail übermittelt Protokolldateien aus allen AWS Regionen an Ihren S3-Bucket , wenn MULTI_REG ION_CLOUD _TRAIL_ENABLED aktiviert ist. Außerdem wird beim AWS Start einer neuen Region derselbe Trail in der neuen Region erstellt. CloudTrail Dadurch erhalten Sie automatis ch Protokolldateien mit API-Aktivitäten für die neue Region.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
8.5	Erfassung detaillierter Prüfprotokolle	cloudtrail-s3-data events-enabled	Die Erfassung von Simple Storage Service (Amazon S3)-Datenereignissen unterstützt die Erkennung von ungewöhnlichen Aktivitäten. Zu den Details gehören Informationen zu dem AWS -Konto, das auf einen Amazon-S3-Bucket zugegriffen hat, die IP-Adresse und die Uhrzeit des Ereignisses.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
8,5	Erfassung detaillierter Prüfprotokolle	cloudtrail-enabled	AWS CloudTrail kann bei der Nichtabstreitbarkeit helfen, indem Aktionen und API-Aufrufe der AWS Management Console aufgezeichnet werden. Sie können die Benutzer und die Benutzer AWS-Konten , die einen AWS Dienst aufgerufen haben, die Quell-IP-Adresse, über die die Aufrufe generiert wurden, und den Zeitpunkt der Anrufe identifizieren. Einzelheiten zu den erfassten Daten finden Sie in den AWS CloudTrail Datensatzinhalten.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
8.5	Erfassung detaillierter Prüfprotokolle	cloud-trail-cloud-watch-logs-aktiviert	Verwenden Sie Amazon CloudWatch , um Protokoll ereignisaktivitäten zentral zu sammeln und zu verwalten. Die Aufnahme von AWS CloudTrail Daten liefert Einzelheiten zu den API-Aufrufaktivitäten in Ihrem AWS-Konto.
8.5	Erfassung detaillierter Prüfprotokolle	elasticsearch-logs-to-cloudwatch	Stellen Sie sicher, dass für Amazon OpenSearch Service-Domains Fehlerprotokolle aktiviert und zur Aufbewahrung und Beantwortung an Amazon CloudWatch Logs gestreamt werden. Domain-Fehlerprotokolle sind bei Sicherheits- und Zugriffsprüfungen sowie bei der Diagnose von Verfügbarkeitsproblemen nützlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
8.5	Erfassung detaillierter Prüfprotokolle	vpc-flow-logs-enabled	VPC-Flow-Protokolle erfassen detaillierte Informationsdatensätze über den IP-Datenverkehr, der zu und von Netzwerkschnittstellen in Ihrer Amazon Virtual Private Cloud (Amazon VPC) fließt. Standardmäßig enthalten Flow-Protokolldatensätze Werte für die verschiedenen Komponenten des IP-Flows, einschließlich Quelle, Ziel und Protokoll.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
8,5	Erfassung detaillierter Prüfprotokolle	elb-logging-enabled	Die Elastic-Load-Balancing-Aktivität ist ein zentraler Kommunikationspunkt innerhalb einer Umgebung. Stellen Sie sicher, dass die ELB-Protokollierung aktiviert ist. Die gesammelten Daten enthalten detaillierte Informationen zu Anfragen, die an den ELB gesendet wurden. Jedes Protokoll enthält Informationen wie die Zeit, zu der die Anforderung einging, die Client-IP-Adresse, Latenzen, Anforderungspfade und Serverantworten.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
8,5	Erfassung detaillierter Prüfprotokolle	rds-logging-enabled	Um die Protokollierung und Überwachung in Ihrer Umgebung zu erleichtern, stellen Sie sicher, dass die Amazon Relational Database Service (Amazon RDS)-Protokollierung aktiviert ist. Mit der Amazon-RDS-Protokollierung können Sie Ereignisse wie Verbindungen, Verbindungsabbrüche, Abfragen oder abgefragte Tabellen erfassen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
8,5	Erfassung detaillierter Prüfprotokolle	s-3 bucket-logging-enabled	Die Amazon Simple Storage Service (Amazon S3)-Serverzugriffs protokollierung bietet eine Methode zur Überwachu ng des Netzwerks im Hinblick auf potenzielle Cybersich erheitsereignisse. Die Ereignisse werden überwacht, indem detaillierte Aufzeichn ungen über die Anfragen erfasst werden, die an einen Amazon-S3-Bucket gestellt wurden. Jeder Zugriffsprotokolle intrag enthält Details zu einer einzelnen Zugriffsanfrage. Zu den Details gehören Anforderer, Bucket-Name, Anforderu ngszeit, Anforderu ngsaktion, Antwortst atus und Fehlercode, falls relevant.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
8,5	Erfassung detaillierter Prüfprotokolle	redshift-cluster-configuration-check	Um Daten im Ruhezustand zu schützen, muss die Verschlüsselung für Ihre Amazon-Redshift-Cluster aktiviert sein. Sie müssen auch sicherstellen, dass die erforderlichen Konfigurationen auf Amazon-Redshift-Clustern bereitgestellt werden. Die Prüfungsprotokollierung muss aktiviert sein, um Informationen zu Verbindungen und Benutzeraktivitäten in der Datenbank bereitzustellen. Diese Regel erfordert, dass ein Wert für clusterDbEncrypted (Config Default: TRUE) und LoggingEnabled (Config Default: TRUE) gesetzt ist. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
8.5	Erfassung detaillierter Prüfprotokolle	wafv2-logging-enabled	Um die Protokollierung und Überwachung in Ihrer Umgebung zu erleichtern, aktivieren Sie die AWS WAF (V2) -Protokollierung im regionalen und globalen Web ACLs. AWS Die WAF-Protokollierung bietet detaillierte Informationen über den Datenverkehr, der von Ihrer Web-ACL analysiert wird. In den Protokollen werden die Uhrzeit aufgezeichnet, zu der die AWS WAF die Anfrage von Ihrer AWS Ressource erhalten hat, Informationen über die Anfrage und eine Aktion für die Regel, der jede Anfrage entsprach.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
8.5	Erfassung detaillierter Prüfprotokolle	guardduty-enabled-centralized	Amazon GuardDuty kann mithilfe von Threat Intellige nce Feeds helfen, potenzielle Cybersich erheitsereignisse zu überwachen und zu erkennen. Dazu gehören Listen mit bösartigen IPs und maschinel len Lernmethoden zur Identifizierung unerwarteter, nicht autorisierter und bösartiger Aktivitäten in Ihrer AWS Cloud-Umgebung.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
8.5	Erfassung detaillierter Prüfprotokolle	codebuild-project-logging-enabled	Stellen Sie sicher, dass die AWS CodeBuild Projektprotokollierung aktiviert ist, damit Ihre Build-Ausgabeprotokolle entweder an Amazon CloudWatch oder Amazon Simple Storage Service (Amazon S3) gesendet werden. Build-Ausgabeprotokolle enthalten detaillierte Informationen zu Ihrem Build-Projekt.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
8.7	Erfassung von Prüfprotokollen für URL-Anforderungen	elb-logging-enabled	Die Elastic-Load-Balancing-Aktivität ist ein zentraler Kommunikationspunkt innerhalb einer Umgebung. Stellen Sie sicher, dass die ELB-Protokollierung aktiviert ist. Die gesammelten Daten enthalten detaillierte Informationen zu Anfragen, die an den ELB gesendet wurden. Jedes Protokoll enthält Informationen wie die Zeit, zu der die Anforderung einging, die Client-IP-Adresse, Latenzen, Anforderungspfade und Serverantworten.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
8,9	Zentralisierung von Prüfprotokollen	cloud-trail-cloud-watch-logs-aktiviert	Verwenden Sie Amazon CloudWatch , um Protokoll ereignisaktivitäten zentral zu sammeln und zu verwalten. Die Aufnahme von AWS CloudTrail Daten liefert Einzelheiten zu den API-Aufrufaktivitäten in Ihrem AWS-Konto.
8.10	Aufbewahrung von Prüfprotokollen	s-3 version-lifecycle-policy-check	Mit Amazon-S3-Lebenszyklusregeln können Sie Aktionen definieren, die Amazon S3 während der Lebensdauer eines Objekts ausführen soll (z. B. die Überführung von Objekten in eine andere Speicherklasse, ihre Archivierung oder Löschung nach einem bestimmten Zeitraum).

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
8,10	Aufbewahrung von Prüfprotokollen	cw-loggroup-retention-period-überprüfen	Stellen Sie sicher, dass die Ereignisprotokolldaten für Ihre Protokollgruppen über eine Mindestdauer aufbewahrt werden, um die Fehlerbehebung und forensische Untersuchungen zu unterstützen. Fehlende frühere Ereignisprotokolldaten erschweren die Rekonstruierung und Identifizierung potenziell schädlicher Ereignisse.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.1	Bereitstellung und Wartung von Anti-Malware-Software	guardduty-enabled-centralized	Amazon GuardDuty kann mithilfe von Threat Intellige nce Feeds helfen, potenzielle Cybersich erheitsereignisse zu überwachen und zu erkennen. Dazu gehören Listen mit bösartigen IPs und maschinel len Lernmethoden zur Identifizierung unerwarteter, nicht autorisierter und bösartiger Aktivitäten in Ihrer AWS Cloud-Umgebung.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.2	Konfigurierung automatischer Anti-Malware-Signatur-Updates	guardduty-enabled-centralized	Amazon GuardDuty kann mithilfe von Threat Intellige nce Feeds helfen, potenzielle Cybersich erheitsereignisse zu überwachen und zu erkennen. Dazu gehören Listen mit bösartigen IPs und maschinel len Lernmethoden zur Identifizierung unerwarteter, nicht autorisierter und bösartiger Aktivitäten in Ihrer AWS Cloud-Umgebung.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.4	Konfigurierung automatischer Anti-Malware-Scans von Wechselmedien	guardduty-enabled-centralized	Amazon GuardDuty kann mithilfe von Threat Intellige nce Feeds helfen, potenzielle Cybersich erheitsereignisse zu überwachen und zu erkennen. Dazu gehören Listen mit bösartigen IPs und maschinel len Lernmethoden zur Identifizierung unerwarteter, nicht autorisierter und bösartiger Aktivitäten in Ihrer AWS Cloud-Umgebung.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.6	Zentrale Verwaltun g von Anti-Malware-Software	guardduty-enabled-centralized	Amazon GuardDuty kann mithilfe von Threat Intellige nce Feeds helfen, potenzielle Cybersich erheitsereignisse zu überwachen und zu erkennen. Dazu gehören Listen mit bösartigen IPs und maschinel len Lernmethoden zur Identifizierung unerwarteter, nicht autorisierter und bösartiger Aktivitäten in Ihrer AWS Cloud-Umgebung.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.7	Verwendung von verhaltensbasierter Anti-Malware-Software	guardduty-enabled-centralized	Amazon GuardDuty kann mithilfe von Threat Intelligence Feeds helfen, potenzielle Cybersicherheitsereignisse zu überwachen und zu erkennen. Dazu gehören Listen mit bösartigen IPs und maschinellen Lernmethoden zur Identifizierung unerwarteter, nicht autorisierter und bösartiger Aktivitäten in Ihrer AWS Cloud-Umgebung.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
11.2	Durchführen automatisierter Backups	dynamodb-in-backup-plan	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon DynamoDB-Tabellen Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
11.2	Durchführen automatisierter Backups	ebs-in-backup-plan	Stellen Sie zur Unterstützung der Datensicherungspro zesse sicher, dass Ihre Amazon Elastic Block Store (Amazon EBS) -Volumes Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwaltet er Backup-Service mit einer richtlini enbasierten Backup-Lösung. Diese Lösung vereinfacht Ihre Backup-Verwaltung und ermöglicht es Ihnen, Ihre geschäftl ichen und behördlic hen Anforderungen bezüglich Backups zu erfüllen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
11.2	Durchführen automatisierter Backups	ebs-optimized-instance	Eine optimierte Instance im Amazon Elastic Block Store (Amazon EBS) bietet zusätzliche, dedizierte Kapazität für Amazon-EBS-I/O-Vorgänge. Diese Optimierung bietet die beste Leistung für Ihr EBS-Volume, indem Konflikte zwischen Amazon-EBS-I/O und anderem Datenverkehr von Ihrer Instance minimiert werden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
11.2	Durchführen automatisierter Backups	dynamodb-pitr-enabled	Aktivieren Sie diese Regel, um zu überprüfen, ob die Informationen gesichert wurden. Es verwaltet auch die Backups, indem es sicherstellt, dass die point-in-time Wiederherstellung in Amazon DynamoDB aktiviert ist. Bei der Wiederherstellung werden fortlaufende Backups Ihrer Tabelle für die letzten 35 Tage gespeichert.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
11.2	Durchführen automatisierter Backups	elasticache-redis-cluster-automatic-Backup-Prüfung	Wenn automatische Backups aktiviert sind, ElastiCache erstellt Amazon täglich ein Backup des Clusters. Die Sicherung kann für eine von Ihrer Organisation festgelegte Anzahl von Tagen aufbewahrt werden. Automatische Backups schützen vor Datenverlust. Bei einem Ausfall können Sie einen neuen Cluster erstellen, der Ihre Daten aus dem aktuellen Backup wiederherstellt.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
11.2	Durchführen automatisierter Backups	efs-in-backup-plan	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon Elastic File System (Amazon EFS) -Dateisysteme Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
11.2	Durchführen automatisierter Backups	db-instance-backup-enabled	Die Sicherungsfunktion von Amazon RDS erstellt Sicherungen Ihrer Datenbanken und Transaktionsprotokolle. Amazon RDS erstellt einen Snapshot für das Speichervolume Ihrer DB-Instance, sodass die gesamte DB-Instance gesichert wird. Sie können im System spezifische Aufbewahrungsfristen festlegen, um Ihre Ausfallsicherheitsanforderungen zu erfüllen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
11.2	Durchführen automatisierter Backups	redshift-backup-enabled	Stellen Sie zur Unterstützung der Datensicherungsprozesse sicher, dass Ihre Amazon-Redshift-Cluster über automatisierte Snapshots verfügen. Wenn automatisierte Snapshots für einen Cluster aktiviert sind, erstellt Redshift in regelmäßigen Abständen Snapshots dieses Clusters. Standardmäßig erstellt Redshift alle acht Stunden oder alle 5 GB einen Snapshot für jeden Knoten mit Datenänderungen oder je nachdem, was zuerst eintritt.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
11.2	Durchführen automatisierter Backups	s3- bucket-versioning-enabled	Die Versionsv erwaltung von Amazon Simple Storage Service (Amazon S3)-Bucke ts hilft dabei, mehrere Varianten eines Objekts im selben Amazon-S3-Bucket zu speichern. Verwenden Sie die Versionsv erwaltung, um sämtliche Versionen aller Objekte in Ihrem Amazon-S3-Bucket zu speichern , abzurufen oder wiederherzustellen . Mit der Versionsv erwaltung können Sie Versionen sowohl nach unbeabsic htigten Benutzera ktionen als auch nach Anwendungsfehlern problemlos wiederher stellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
11.2	Durchführen automatisierter Backups	redshift-cluster-maintenancesettings-check	Diese Regel stellt sicher, dass Amazon-Redshift-Cluster die bevorzugten Einstellungen für Ihre Organisation haben. Insbesondere sorgt sie dafür, dass Cluster bevorzugte Wartungsfenster und automatisierte Aufbewahrungsfristen für Snapshots für die Datenbank haben. Für diese Regel müssen Sie die festlegen allowVersionUpgrade. Der Standardwert ist „true“. Außerdem können Sie optional den Zeitraum preferredMaintenanceWindow (der Standardwert ist sa: 16:00 -sa: 16:30) und den automated SnapshotRetention Zeitraum (der Standardwert ist 1) festlegen. Die tatsächlichen Werte müssen den Richtlini

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			en Ihrer Organisation entsprechen.
11.2	Durchführen automatisierter Backups	s3- bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) unterstützt die Aufrechterhaltung einer angemesse nen Kapazität und Verfügbarkeit. CRR ermöglicht das automatische, asynchrone Kopieren von Objekten in Amazon-S3-Buckets, um die Datenverf ügbarkeit sicherzus tellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
11.2	Durchführen automatisierter Backups	s-3 version-lifecycle-policy-check	Mit Amazon-S3-Lebenszyklusregeln können Sie Aktionen definieren, die Amazon S3 während der Lebensdau er eines Objekts ausführen soll (z. B. die Überführu ng von Objekten in eine andere Speicherklasse, ihre Archivierung oder Löschung nach einem bestimmten Zeitraum) .
11,3	Schutz von Wiederher stellungsdaten	backup-recovery-point-encrypted	Stellen Sie sicher, dass die Verschlüs selung für Ihre AWS Backup-Wiederherst ellungspunkte aktiviert ist. Da sensible Daten auch im Ruhezusta nd vorhanden sein können, sollten Sie die Verschlüsselung im Ruhezustand aktivieren, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
11.3	Schutz von Wiederherstellungsdaten	encrypted-volumes	Aktivieren Sie die Verschlüsselung für Ihre Amazon-Elastic-Block-Store (Amazon-EBS)-Volumes, um eventuell vorhandene sensible Daten sowie Daten im Ruhezustand zu schützen.
11,3	Schutz von Wiederherstellungsdaten	ec-2 ebs-encryption-by-default	Zum Schutz von Daten im Ruhezustand müssen Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon Elastic Block Store (Amazon EBS)-Volumes aktiviert ist. Da sensible Daten auch im Ruhezustand vorhanden sein können, sollten Sie die Verschlüsselung im Ruhezustand aktivieren, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
11,3	Schutz von Wiederherstellungsdaten	rds-storage-encrypted	Zum Schutz von Daten im Ruhezustand müssen Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon Relational Database Service (Amazon RDS)-Instances aktiviert ist. Um eventuell vorhandene sensible Daten im Ruhezustand in Amazon-RDS-Instances zu schützen, muss die Verschlüsselung von Daten im Ruhezustand aktiviert sein.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
11.4	Einrichtung und Verwaltung einer isolierten Instance für Wiederherstellungs daten	dynamodb-in-backup-plan	Um Sie bei Datensich erungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon DynamoDB-Tabellen Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwaltet er Backup-Service mit einer richtlini enbasierten Backup-Lösung. Diese Lösung vereinfacht Ihre Backup-Verwaltung und ermöglicht es Ihnen, Ihre geschäftl ichen und behördlic hen Anforderungen bezüglich Backups zu erfüllen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
11.4	Einrichtung und Verwaltung einer isolierten Instance für Wiederherstellungs daten	ebs-in-backup-plan	Stellen Sie zur Unterstützung der Datensicherungspro zesse sicher, dass Ihre Amazon Elastic Block Store (Amazon EBS) -Volumes Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwaltet er Backup-Service mit einer richtlini enbasierten Backup-Lösung. Diese Lösung vereinfacht Ihre Backup-Verwaltung und ermöglicht es Ihnen, Ihre geschäftl ichen und behördlic hen Anforderungen bezüglich Backups zu erfüllen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
11.4	Einrichtung und Verwaltung einer isolierten Instance für Wiederherstellungs daten	ebs-optimized-instance	Eine optimierte Instance im Amazon Elastic Block Store (Amazon EBS) bietet zusätzliche, dedizierte Kapazität für Amazon-EBS-I/O-Vorgänge. Diese Optimierung bietet die beste Leistung für Ihr EBS-Volume, indem Konflikte zwischen Amazon-EBS-I/O und anderem Datenverkehr von Ihrer Instance minimiert werden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
11.4	Einrichtung und Verwaltung einer isolierten Instance für Wiederherstellungs daten	dynamodb-pitr-enabled	Aktivieren Sie diese Regel, um zu überprüfen, ob die Informationen gesichert wurden. Es verwaltet auch die Backups, indem es sicherstellt, dass die point-in-time Wiederherstellung in Amazon DynamoDB aktiviert ist. Bei der Wiederherstellung werden fortlaufende Backups Ihrer Tabelle für die letzten 35 Tage gespeichert.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
11.4	Einrichtung und Verwaltung einer isolierten Instance für Wiederherstellungs daten	elasticache-redis-cluster-automatic-Backup-Prüfung	Wenn automatische Backups aktiviert sind, ElastiCache erstellt Amazon täglich ein Backup des Clusters. Die Sicherung kann für eine von Ihrer Organisation festgelegte Anzahl von Tagen aufbewahrt werden. Automatische Backups schützen vor Datenverlust. Bei einem Ausfall können Sie einen neuen Cluster erstellen, der Ihre Daten aus dem aktuellen Backup wiederherstellt.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
11.4	Einrichtung und Verwaltung einer isolierten Instance für Wiederherstellungs daten	efs-in-backup-plan	Um Sie bei Datensich erungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon Elastic File System (Amazon EFS) -Dateisysteme Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwaltet er Backup-Service mit einer richtlini enbasierten Backup-Lösung. Diese Lösung vereinfacht Ihre Backup-Verwaltung und ermöglicht es Ihnen, Ihre geschäftl ichen und behördlic hen Anforderungen bezüglich Backups zu erfüllen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
11.4	Einrichtung und Verwaltung einer isolierten Instance für Wiederherstellungs daten	db-instance-backup-enabled	Die Sicherung sfunktion von Amazon RDS erstellt Sicherung en Ihrer Datenbank en und Transakti onsprotokolle. Amazon RDS erstellt einen Snapshot für das Speichervolume Ihrer DB-Instance, sodass die gesamte DB-Instance gesichert wird. Sie können im System spezifische Aufbewahrungsfrist en festlegen, um Ihre Ausfallsicherheits anforderungen zu erfüllen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
11.4	Einrichtung und Verwaltung einer isolierten Instance für Wiederherstellungs daten	redshift-backup-enabled	Stellen Sie zur Unterstützung der Datensicherungspro zesse sicher, dass Ihre Amazon-Re dshift-Cluster über automatisierte Snapshots verfügen. Wenn automatis ierte Snapshots für einen Cluster aktiviert sind, erstellt Redshift in regelmäßi gen Abständen Snapshots dieses Clusters. Standardm äßig erstellt Redshift alle acht Stunden oder alle 5 GB einen Snapshot für jeden Knoten mit Datenände rungen oder je nachdem, was zuerst eintritt.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
11.4	Einrichtung und Verwaltung einer isolierten Instance für Wiederherstellungs daten	s3- bucket-versioning-enabled	Die Versionsv erwaltung von Amazon Simple Storage Service (Amazon S3)-Bucke ts hilft dabei, mehrere Varianten eines Objekts im selben Amazon-S3-Bucket zu speichern. Verwenden Sie die Versionsv erwaltung, um sämtliche Versionen aller Objekte in Ihrem Amazon-S3-Bucket zu speichern , abzurufen oder wiederherzustellen . Mit der Versionsv erwaltung können Sie Versionen sowohl nach unbeabsic htigten Benutzera ktionen als auch nach Anwendungsfehlern problemlos wiederher stellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
11.4	Einrichtung und Verwaltung einer isolierten Instance für Wiederherstellungs daten	redshift-cluster-maintenancesettings-check	Diese Regel stellt sicher, dass Amazon-Redshift-Cluster die bevorzugten Einstellungen für Ihre Organisation haben. Insbesondere sorgt sie dafür, dass Cluster bevorzugte Wartungsfenster und automatisierte Aufbewahrungsfristen für Snapshots für die Datenbank haben. Für diese Regel müssen Sie die festlegen allowVersionUpgrade. Der Standardwert ist „true“. Außerdem können Sie optional den Zeitraum preferredMaintenanceWindow (der Standardwert ist sa: 16:00 -sa: 16:30) und den automated SnapshotRetention Zeitraum (der Standardwert ist 1) festlegen. Die tatsächlichen Werte müssen den Richtlini

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			en Ihrer Organisation entsprechen.
11.4	Einrichtung und Verwaltung einer isolierten Instance für Wiederherstellungs daten	s3- bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) unterstützt die Aufrechterhaltung einer angemesse nen Kapazität und Verfügbarkeit. CRR ermöglicht das automatische, asynchrone Kopieren von Objekten in Amazon-S3-Buckets, um die Datenverf ügbarkeit sicherzus tellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
11.4	Einrichtung und Verwaltung einer isolierten Instance für Wiederherstellungs daten	s-3 version-lifecycle-policy-check	Mit Amazon-S3-Lebenszyklusregeln können Sie Aktionen definieren, die Amazon S3 während der Lebensdau er eines Objekts ausführen soll (z. B. die Überführu ng von Objekten in eine andere Speicherklasse, ihre Archivierung oder Löschung nach einem bestimmten Zeitraum) .

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
12.2	Einrichtung und Pflege einer sicheren Netzwerkarchitektur	acm-certificate-expiration-check	Stellen Sie sicher, dass die Netzwerkintegrität geschützt ist, indem Sie sicherstellen, dass X509-Zertifikate von AWS ACM ausgestellt werden. Diese Zertifikate müssen gültig und dürfen nicht abgelaufen sein. Für diese Regel ist ein Wert für erforderlich daysToExpiration (Wert für bewährte AWS Grundregeln für Sicherheit: 90). Der tatsächliche Wert muss den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
12.2	Einrichtung und Pflege einer sicheren Netzwerkarchitektur	dms-replication-not-public	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass auf DMS-Replikationsin stanzen nicht öffentlic h zugegriffen werden kann. DMS-Repli kations-Instances können vertrauli che Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.
12.2	Einrichtung und Pflege einer sicheren Netzwerkarchitektur	ebs-snapshot-public-restorable-überprüfen	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass EBS-Snapshots nicht öffentlich wiederher stellbar sind. EBS-Volume-Snapsho ts können vertrauli che Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
12.2	Einrichtung und Pflege einer sicheren Netzwerkarchitektur	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) Security Groups können bei der Verwaltung des Netzwerkzugriffs helfen, indem sie eine statusbeh aftete Filterung von eingehendem und ausgehendem Netzwerkverkehr zu Ressourcen bereitste llen. AWS Wenn Sie eingehenden (oder entfernten) Datenverk ehr von 0.0.0.0/0 bis Port 22 auf Ihren Ressourcen nicht zulassen, können Sie den Remote-Zugriff einschränken.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
12.2	Einrichtung und Pflege einer sicheren Netzwerkarchitektur	vpc-default-security-group-geschlossen	Sicherheitsgruppen von Amazon Elastic Compute Cloud (Amazon EC2) können bei der Verwaltung des Netzwerkzugriffs helfen, indem sie eine statusbehaftete Filterung des ein- und ausgehenden Netzwerkverkehrs zu Ressourcen bereitstellen. AWS Die Beschränk ung des gesamten Datenverkehrs auf die Standardsicherheit sgruppe hilft dabei, den Fernzugriff auf Ihre Ressourcen einzuschränken. AWS

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
12.2	Einrichtung und Pflege einer sicheren Netzwerkarchitektur	ec2- instance-no-public-ip	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon Elastic Compute Cloud (Amazon EC2) - Instances nicht öffentlich zugänglic h sind. EC2Amazon -Instances können vertrauliche Informati onen enthalten, und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
12.2	Einrichtung und Pflege einer sicheren Netzwerkarchitektur	elasticsearch-in-vpc-only	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass sich Amazon OpenSearch OpenSearch Service (Service) - Domains innerhalb einer Amazon Virtual Private Cloud (Amazon VPC) befinden. Eine OpenSearch Service-Domain innerhalb einer Amazon VPC ermöglicht die sichere Kommunikation zwischen OpenSearch Service und anderen Services innerhalb der Amazon VPC, ohne dass ein Internet-Gateway, ein NAT-Gerät oder eine VPN-Verbindung erforderlich ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
12.2	Einrichtung und Pflege einer sicheren Netzwerkarchitektur	ec2- instances-in-vpc	Stellen Sie Amazon Elastic Compute Cloud (Amazon EC2) -Instances innerhalb einer Amazon Virtual Private Cloud (Amazon VPC) bereit, um eine sichere Kommunika tion zwischen einer Instance und anderen Services innerhalb der Amazon VPC zu ermöglichen, ohne dass ein Internet-Gateway, ein NAT-Gerät oder eine VPN-Verbindung erforderlich ist. Der gesamte Datenverk ehr bleibt sicher in der AWS Cloud. Domains, die sich innerhalb einer VPC befinden, verfügen aufgrund ihrer logischen Isolierun g im Vergleich zu Domains mit öffentlic hen Endpunkten über eine zusätzlic he Sicherheitsebene. Weisen Sie EC2

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			Amazon-Instances einer Amazon-VPC zu, um den Zugriff ordnungsgemäß zu verwalten.
12.2	Einrichtung und Pflege einer sicheren Netzwerkarchitektur	emr-master-no-public-ip	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon EMR-Cluster-Masterknoten nicht öffentlich zugänglich sind. Amazon-EMR-Cluster-Hauptknoten können vertrauliche Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
12.2	Einrichtung und Pflege einer sicheren Netzwerkarchitektur	no-unrestricted-route-to-igw	Stellen Sie sicher, dass EC2 Amazon-Routentabellen keine uneingeschränkten Routen zu einem Internet-Gateway enthalten. Durch das Entfernen oder Beschränken des Internetzugangs für Workloads innerhalb von Amazon VPCs können unbeabsichtigte Zugriffe in Ihrer Umgebung reduziert werden.
12.2	Einrichtung und Pflege einer sicheren Netzwerkarchitektur	lambda-function-public-access-verboten	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass AWS Lambda-Funktionen nicht öffentlich zugänglich sind. Der öffentliche Zugriff kann möglicherweise die Verfügbarkeit von Ressourcen beeinträchtigen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
12.2	Einrichtung und Pflege einer sicheren Netzwerkarchitektur	lambda-inside-vpc	Stellen Sie AWS Lambda-Funktionen in einer Amazon Virtual Private Cloud (Amazon VPC) bereit, um eine sichere Kommunika tion zwischen einer Funktion und anderen Diensten innerhalb der Amazon VPC zu gewährleisten. Bei dieser Konfiguration sind kein Internet-Gateway, kein NAT-Gerät und keine VPN-Verbindung erforderlich. Der gesamte Datenverk ehr bleibt sicher in der Cloud. AWS Domains, die sich innerhalb einer VPC befinden, verfügen aufgrund ihrer logischen Isolierun g im Vergleich zu Domains mit öffentlic hen Endpunkten über eine zusätzliche Sicherheitsebene. Um den Zugriff ordnungsg emäß zu verwalten,

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			sollten AWS Lambda-Funktionen einer VPC zugewiesen werden.
12.2	Einrichtung und Pflege einer sicheren Netzwerkarchitektur	rds-snapshots-public-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Relational Database Service (Amazon RDS) -Instances nicht öffentlich sind. Amazon-RDS-Datenbank-Instances können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
12.2	Einrichtung und Pflege einer sicheren Netzwerkarchitektur	rds-instance-public-access-überprüfen	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Relational Database Service (Amazon RDS) -Instances nicht öffentlich sind. Amazon-RDS-Datenbank-Instances können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
12.2	Einrichtung und Pflege einer sicheren Netzwerkarchitektur	restricted-common-ports	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass gemeinsame Ports für Amazon Elastic Compute Cloud (Amazon EC2) -Sicherheitsgruppen eingeschränkt sind. Wenn der Zugriff auf Ports nicht auf vertrauenswürdige Quellen beschränkt wird, kann dies zu Angriffen auf die Verfügbarkeit, Integrität und Vertraulichkeit von Systemen führen. Mit dieser Regel können Sie optional die Parameter blockedPort1–blockedPort5 festlegen (Standardkonfigurationen: 20, 21, 3389, 3306, 4333). Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
12.2	Einrichtung und Pflege einer sicheren Netzwerkarchitektur	redshift-cluster-public-access-überprüfen	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Redshift Redshift-Cluster nicht öffentlich sind. Amazon-Redshift-Cluster können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
12.2	Einrichtung und Pflege einer sicheren Netzwerkarchitektur	s3- -Block-periodisch account-level-public-access	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Simple Storage Service (Amazon S3) -Buckets nicht öffentlich zugänglich sind. Diese Regel trägt dazu bei, sensible Daten vor unbefugten Remote-Benutzern zu schützen, indem sie den öffentlichen Zugriff verhindert. Mit dieser Regel können Sie optional die Parameter ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) und restrictPublicBuckets Parameter (Config Default: True) festlegen. Die tatsächlichen Werte müssen den Richtlini

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			en Ihrer Organisation entsprechen.
12.2	Einrichtung und Pflege einer sicheren Netzwerkarchitektur	s3- bucket-public-read -prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie nur autorisierten Benutzern, Prozessen und Geräten Zugriff auf Amazon Simple Storage Service (Amazon S3) - Buckets gewähren. Die Verwaltung des Zugriffs sollte mit der Klassifizierung der Daten übereinst immen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
12.2	Einrichtung und Pflege einer sicheren Netzwerkarchitektur	s3- bucket-public-write-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie nur autorisierten Benutzern, Prozessen und Geräten Zugriff auf Amazon Simple Storage Service (Amazon S3) - Buckets gewähren. Die Verwaltung des Zugriffs sollte mit der Klassifizierung der Daten übereinstimmen.
12.2	Einrichtung und Pflege einer sicheren Netzwerkarchitektur	sagemaker-notebook-no-direct-Internetzugang	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass SageMaker Amazon-Notebooks keinen direkten Internetzugang zulassen. Indem Sie direkten Internetzugang blockieren, vermeiden Sie, dass unbefugte Benutzer auf sensible Daten zugreifen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
12.2	Einrichtung und Pflege einer sicheren Netzwerkarchitektur	subnet-auto-assign-public-ip-deaktiviert	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon Virtual Private Cloud (VPC) -Subnetzen nicht automatisch eine öffentliche IP-Adresse zugewiesen wird. Amazon Elastic Compute Cloud (EC2) -Instances, die in Subnetzen gestartet werden, in denen dieses Attribut aktiviert ist, haben ihrer primären Netzwerkschnittstelle eine öffentliche IP-Adresse zugewiesen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
12.2	Einrichtung und Pflege einer sicheren Netzwerkarchitektur	vpc-sg-open-only-to-authorized-ports	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass gemeinsame Ports für Amazon Elastic Compute Cloud (Amazon EC2) -Sicherheitsgruppen eingeschränkt sind. Wenn der Zugriff auf Ports nicht auf vertrauenswürdige Quellen beschränkt wird, kann dies zu Angriffen auf die Verfügbarkeit, Integrität und Vertraulichkeit von Systemen führen. Durch die Beschränkung des Zugriffs auf Ressourcen innerhalb einer Sicherheitsgruppe aus dem Internet (0.0.0.0/0) kann der Remote-Zugriff auf interne Systeme gesteuert werden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
12.2	Einrichtung und Pflege einer sicheren Netzwerkarchitektur	ssm-document-not-public	Stellen Sie sicher, dass AWS Systems Manager (SSM) - Dokumente nicht öffentlich sind, da dies einen unbeabsichtigten Zugriff auf Ihre SSM-Dokumente ermöglichen kann. Ein öffentliches SSM-Dokument kann Informationen über Ihr Konto, Ihre Ressourcen und internen Prozesse preisgeben.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
12.2	Einrichtung und Pflege einer sicheren Netzwerkarchitektur	autoscaling-launch-config-public-ip-deaktiviert	Wenn Sie Ihre Netzwerkschnittstellen mit einer öffentlichen IP-Adresse konfigurieren, sind die diesen Netzwerkschnittstellen zugehörigen Ressourcen über das Internet erreichbar. EC2 Ressourcen sollten nicht öffentlich zugänglich sein, da dies einen unbeabsichtigten Zugriff auf Ihre Anwendungen oder Server ermöglichen kann.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
12.2	Einrichtung und Pflege einer sicheren Netzwerkarchitektur	redshift-enhanced-vpc-routing-aktiviert	Mit Enhanced-VPC-Routing wird erzwungen, dass der gesamte COPY- und UNLOAD-Datenverkehr zwischen Ihrem Cluster und Datenrepositorys über Ihre Amazon VPC erfolgt. Anschließend können Sie VPC-Features wie Sicherheitsgruppen und Netzwerkzugriffskontrolllisten verwenden, um den Netzwerkverkehr zu schützen. Sie können auch VPC-Flow-Protokolle verwenden, um den Netzwerkverkehr zu überwachen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
12.2	Einrichtung und Pflege einer sicheren Netzwerkarchitektur	dynamodb-autoscaling-enabled	Amazon DynamoDB Auto Scaling verwendet den AWS Application Auto Scaling-Service, um die bereitgestellte Durchsatzkapazität so anzupassen, dass sie automatisch auf tatsächliche Verkehrsmuster reagiert. Auf diese Weise kann eine Tabelle oder ein globaler sekundärer Index die bereitgestellte Lese-/Schreibkapazität erhöhen, um plötzliche Erhöhungen des Datenverkehrs ohne Drosselung zu bewältigen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
12.2	Einrichtung und Pflege einer sicheren Netzwerkarchitektur	elb-cross-zone-load-Balancing aktiviert	Aktivieren Sie zonenübergreifendes Load Balancing für Ihre Elastic Load Balancer (ELBs), um eine angemessene Kapazität und Verfügbarkeit aufrechtzuerhalten. Zonenübergreifendes Load Balancing reduziert die Notwendigkeit, die gleiche Anzahl von Instances in jeder aktivierten Availability Zone aufrechtzuerhalten. Es verbessert auch die Fähigkeit Ihrer Anwendung, den Verlust einer oder mehrerer Instances zu bewältigen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
12.2	Einrichtung und Pflege einer sicheren Netzwerkarchitektur	elb-deletion-protection-enabled	Diese Regel sorgt dafür, dass der Löschschutz für Elastic Load Balancing aktiviert ist. Verwenden Sie diese Funktion, um zu verhindern, dass Ihr Load Balancer versehentlich oder böswillig gelöscht wird, was zum Verlust der Verfügbarkeit Ihrer Anwendungen führen kann.
12.2	Einrichtung und Pflege einer sicheren Netzwerkarchitektur	rds-instance-deletion-protection-aktiviert	Stellen Sie sicher, dass Amazon Relational Database Service (Amazon RDS)-Instances den Löschschutz aktiviert haben. Verwenden Sie den Löschschutz, um zu verhindern, dass Ihre Amazon-RDS-Instances versehentlich oder böswillig gelöscht werden, was zum Verlust der Verfügbarkeit Ihrer Anwendungen führen kann.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
12.2	Einrichtung und Pflege einer sicheren Netzwerkarchitektur	rds-multi-az-support	Die Multi-AZ-Unterstützung in Amazon Relational Database Service (Amazon RDS) bietet eine verbesserte Verfügbarkeit und Beständigkeit von Datenbank-Instances. Wenn Sie eine Multi-AZ-Datenbank-Instance bereitstellen, erstellt Amazon RDS automatisch eine primäre Datenbank-Instance und repliziert die Daten synchron auf eine Standby-Instance in einer anderen Availability Zone. Jede Availability Zone läuft auf einer eigenen, physisch getrennten, unabhängigen Infrastruktur und ist auf eine hohe Verfügbarkeit ausgelegt. Im Falle eines Infrastrukturausfalls führt Amazon RDS einen automatis

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			chen Failover zum Standby-Modus durch, sodass Sie den Datenbankbetrieb wieder aufnehmen können, sobald der Failover abgeschlo ssen ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
12.2	Einrichtung und Pflege einer sicheren Netzwerkarchitektur	rds-cluster-multi-az-aktiviert	Die Multi-AZ-Unterstützung in Amazon Relational Database Service (Amazon RDS) bietet eine verbesserte Verfügbarkeit und Beständigkeit von Datenbank-Instances. Wenn Sie eine Multi-AZ-Datenbank-Instance bereitstellen, erstellt Amazon RDS automatisch eine primäre Datenbank-Instance und repliziert die Daten synchron auf eine Standby-Instance in einer anderen Availability Zone. Jede Availability Zone läuft auf einer eigenen, physisch getrennten, unabhängigen Infrastruktur und ist auf eine hohe Verfügbarkeit ausgelegt. Im Falle eines Infrastrukturausfalls führt Amazon RDS einen automatis

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			chen Failover zum Standby-Modus durch, sodass Sie den Datenbankbetrieb wieder aufnehmen können, sobald der Failover abgeschlo ssen ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
12.2	Einrichtung und Pflege einer sicheren Netzwerkarchitektur	vpc-vpn-2-tunnels-up	Redundante Site-to-Site VPN-Tunnel können implementiert werden, um die Anforderungen an die Ausfallsicherheit zu erfüllen. Es verwendet zwei Tunnel, um die Konnektivität sicherzustellen, falls eine der Site-to-Site VPN-Verbindungen nicht verfügbar ist. Um sich vor einem Verbindungsverlust zu schützen, können Sie für den Fall, dass Ihr Kunden-Gateway nicht verfügbar ist, eine zweite Site-to-Site VPN-Verbindung zu Ihrer Amazon Virtual Private Cloud (Amazon VPC) und Ihrem Virtual Private Gateway einrichten, indem Sie ein zweites Kunden-Gateway verwenden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
12.2	Einrichtung und Pflege einer sicheren Netzwerkarchitektur	opensearch-in-vpc-only	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass sich Amazon OpenSearch Service-Domains innerhalb einer Amazon Virtual Private Cloud (Amazon VPC) befinden. Eine Amazon OpenSearch Service-Domain innerhalb einer Amazon VPC ermöglicht die sichere Kommunikation zwischen Amazon OpenSearch Service und anderen Services innerhalb der Amazon VPC, ohne dass ein Internet-Gateway, ein NAT-Gerät oder eine VPN-Verbindung erforderlich ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
12.2	Einrichtung und Pflege einer sicheren Netzwerkarchitektur	elbv2-multiple-az	Elastic Load Balancing (ELB) verteilt Ihren eingehenden Traffic automatisch auf mehrere Ziele wie EC2 Instances, Container und IP-Adressen in einer Availability Zone. Zur Gewährlei stung einer hohen Verfügbarkeit stellen Sie sicher, dass Ihr ELB Instances aus mehreren Availability Zones registriert hat.
12.3	Netzwerkinfrastruktur sicher verwalten	api-gw-ssl-enabled	Stellen Sie sicher, dass die REST-API-Stufen von Amazon API Gateway mit SSL-Zertifikaten konfiguri ert sind, damit Backend-Systeme überprüfen können, ob Anforderungen von API Gateway stammen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
12.3	Netzwerkinfrastruktur sicher verwalten	alb-http-to-https-Umleitungsprüfung	Um Daten während der Übertragung zu schützen, stellen Sie sicher, dass Ihr Application Load Balancer unverschlüsselte HTTP-Anfragen automatisch an HTTPS umleitet. Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
12.3	Netzwerkinfrastruktur sicher verwalten	elb-acm-certificate-required	Zum Schutz von eventuell vorhanden en sensiblen Daten sowie von Daten während der Übertragung muss die Verschlüsselung für Ihr Elastic Load Balancing aktiviert sein. Verwenden Sie AWS Certificate Manager, um öffentlic he und private SSL/ TLS-Zertifikate mit AWS Diensten und internen Ressource n zu verwalten, bereitzustellen und bereitzustellen.
12.3	Netzwerkinfrastruktur sicher verwalten	elb-tls-https-listeners-nur	Stellen Sie sicher, dass Ihre Elastic Load Balancer (ELBs) mit SSL- oder HTTPS-Listenern konfiguriert sind. Um eventuell vorhanden e sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
12.3	Netzwerkinfrastruktur sicher verwalten	s-3 bucket-ssl-requests-only	Um Daten während der Übertragung zu schützen, stellen Sie sicher, dass Ihre Amazon Simple Storage Service (Amazon S3)-Buckets Anfragen zur Verwendung von Secure Socket Layer (SSL)-Buckets erfordern. Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.
12.3	Netzwerkinfrastruktur sicher verwalten	redshift-require-tls-ssl	Stellen Sie sicher, dass Ihre Amazon-Redshift-Cluster eine TLS/SSL-Verschlüsselung erfordern, um eine Verbindung zu SQL-Clients herzustellen. Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
12.3	Netzwerkinfrastruktur sicher verwalten	Elb v 2- acm-certificate-required	Zum Schutz von eventuell vorhanden en sensiblen Daten sowie von Daten während der Übertragung muss die Verschlüsselung für Ihr Elastic Load Balancing aktiviert sein. Verwenden Sie AWS Certificate Manager, um öffentlic he und private SSL/ TLS-Zertifikate mit AWS Diensten und internen Ressource n zu verwalten, bereitzustellen und bereitzustellen.
12.3	Netzwerkinfrastruktur sicher verwalten	opensearch-https-required	Da sensible Daten existieren können und um Daten während der Übertragung zu schützen, sollten Sie sicherstellen, dass HTTPS für Verbindun gen zu Ihren Amazon OpenSearch Service-Domains aktiviert ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
12.6	Verwendung von sicheren Netzwerkmanagement- und Kommunikationsprotokollen	api-gw-ssl-enabled	Stellen Sie sicher, dass die REST-API-Stufen von Amazon API Gateway mit SSL-Zertifikaten konfiguriert sind, damit Backend-Systeme überprüfen können, ob Anforderungen von API Gateway stammen.
12.6	Verwendung von sicheren Netzwerkmanagement- und Kommunikationsprotokollen	alb-http-to-https-Umleitungsprüfung	Um Daten während der Übertragung zu schützen, stellen Sie sicher, dass Ihr Application Load Balancer unverschlüsselte HTTP-Anfragen automatisch an HTTPS umleitet. Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
12.6	Verwendung von sicheren Netzwerkmanagement- und Kommunikationsprotokollen	elb-acm-certificate-required	Zum Schutz von eventuell vorhanden en sensiblen Daten sowie von Daten während der Übertragung muss die Verschlüsselung für Ihr Elastic Load Balancing aktiviert sein. Verwenden Sie AWS Certificate Manager, um öffentlic he und private SSL/ TLS-Zertifikate mit AWS Diensten und internen Ressource n zu verwalten, bereitzustellen und bereitzustellen.
12.6	Verwendung von sicheren Netzwerkmanagement- und Kommunikationsprotokollen	elb-tls-https-listeners-nur	Stellen Sie sicher, dass Ihre Elastic Load Balancer (ELBs) mit SSL- oder HTTPS-Listenern konfiguriert sind. Um eventuell vorhanden e sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
12.6	Verwendung von sicheren Netzwerkmanagement- und Kommunikationsprotokollen	s-3 bucket-ssl-requests-only	Um Daten während der Übertragung zu schützen, stellen Sie sicher, dass Ihre Amazon Simple Storage Service (Amazon S3)-Buckets Anfragen zur Verwendung von Secure Socket Layer (SSL)-Buckets erfordern. Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.
12.6	Verwendung von sicheren Netzwerkmanagement- und Kommunikationsprotokollen	redshift-require-tls-ssl	Stellen Sie sicher, dass Ihre Amazon-Redshift-Cluster eine TLS/SSL-Verschlüsselung erfordern, um eine Verbindung zu SQL-Clients herzustellen. Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
12.6	Verwendung von sicheren Netzwerkmanagement- und Kommunikationsprotokollen	Elb v 2- acm-certificate-required	Zum Schutz von eventuell vorhandenen sensiblen Daten sowie von Daten während der Übertragung muss die Verschlüsselung für Ihr Elastic Load Balancing aktiviert sein. Verwenden Sie AWS Certificate Manager, um öffentliche und private SSL/TLS-Zertifikate mit AWS Diensten und internen Ressourcen zu verwalten, bereitzustellen und bereitzustellen.
12.6	Verwendung von sicheren Netzwerkmanagement- und Kommunikationsprotokollen	opensearch-https-required	Da sensible Daten existieren können und um Daten während der Übertragung zu schützen, sollten Sie sicherstellen, dass HTTPS für Verbindungen zu Ihren Amazon OpenSearch Service-Domains aktiviert ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
13.1	Zentralisieren der Warnung vor Sicherheitsereignissen	guardduty-enabled-centralized	Amazon GuardDuty kann mithilfe von Threat Intelligence Feeds helfen, potenzielle Cybersicherheitsereignisse zu überwachen und zu erkennen. Dazu gehören Listen mit bösartigen IPs und maschinellen Lernmethoden zur Identifizierung unerwarteter, nicht autorisierter und bösartiger Aktivitäten in Ihrer AWS Cloud-Umgebung.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
13.1	Zentralisieren der Warnung vor Sicherheitsereignissen	securityhub-enabled	AWS Security Hub hilft bei der Überwachung von unbefugtem Personal, Verbindungen, Geräten und Software. AWS Security Hub aggregiert, organisiert und priorisiert die Sicherheitswarnungen oder Ergebnisse mehrerer Dienste. AWS Einige dieser Dienste sind Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer und AWS Firewall Manager sowie AWS Partnerlösungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
13.3	Bereitstellen einer Lösung zur Erkennung von Netzwerkeindringlingen	guardduty-enabled-centralized	Amazon GuardDuty kann mithilfe von Threat Intelligence Feeds helfen, potenzielle Cybersicherheitsereignisse zu überwachen und zu erkennen. Dazu gehören Listen mit bösartigen IPs und maschinellen Lernmethoden zur Identifizierung unerwarteter, nicht autorisierter und bösartiger Aktivitäten in Ihrer AWS Cloud-Umgebung.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
13.6	Sammeln von Protokollen zum Netzwerkdatenverkehr	vpc-flow-logs-enabled	VPC-Flow-Protokolle erfassen detaillierte Informationsdatensätze über den IP-Datenverkehr, der zu und von Netzwerkschnittstellen in Ihrer Amazon Virtual Private Cloud (Amazon VPC) fließt. Standardmäßig enthalten Flow-Protokolldatensätze Werte für die verschiedenen Komponenten des IP-Flows, einschließlich Quelle, Ziel und Protokoll.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
13,6	Sammeln von Protokollen zum Netzwerkdatenverkehr	wafv2-logging-enabled	Um die Protokollierung und Überwachung in Ihrer Umgebung zu erleichtern, aktivieren Sie die AWS WAF (V2) -Protokollierung im regionalen und globalen Web. ACLs AWS Die WAF-Protokollierung bietet detaillierte Informationen über den Datenverkehr, der von Ihrer Web-ACL analysiert wird. In den Protokollen werden die Uhrzeit aufgezeichnet, zu der die AWS WAF die Anfrage von Ihrer AWS Ressource erhalten hat, Informationen über die Anfrage und eine Aktion für die Regel, der jede Anfrage entsprach.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
16.1	Einrichtung und Aufrechterhaltung eines sicheren Anwendungsentwicklungsprozesses	codebuild-project-envvar-awscred-überprüfen	Stellen Sie sicher, dass die Anmeldeinformationen AWS_ACCESS_KEY_ID AWS_SECRET_ACCESS_KEY nicht in AWS Codebuild-Projektumgebungen vorhanden sind. Speichern Sie diese Variablen nicht als Klartext. Das Speichern dieser Variablen als Klartext bewirkt eine unbeabsichtigte Offenlegung von Daten sowie unberechtigte Zugriffe.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
16.1	Einrichtung und Aufrechterhaltung eines sicheren Anwendungsentwicklungsprozesses	codebuild-project-source-repo-URL-Prüfung	Stellen Sie sicher, dass die URL des Quell-Repositorys GitHub oder des Bitbucket-Quell-Repositorys keine persönlichen Zugriffstoken oder Anmeldeinformationen in Codebuild-Projektumgebungen enthält. AWS Verwende OAuth anstelle von persönlichen Zugriffstoken oder Anmeldedaten die Autorisierung für den Zugriff auf GitHub Bitbucket-Repositorys.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
16.1	Einrichtung und Aufrechterhaltung eines sicheren Anwendungsentwicklungsprozesses	codebuild-project-environment-privileged-überprüfen	Um Sie bei der Implementierung des Prinzips der geringsten Rechte zu unterstützen, stellen Sie sicher, dass in Ihrer CodeBuild Amazon-Projektumgebung der privilegierte Modus nicht aktiviert ist. Diese Einstellung sollte deaktiviert werden, um einen unbeabsichtigten Zugriff auf Docker APIs sowie auf die dem Container zugrunde liegende Hardware zu verhindern.
16.1	Einrichtung und Aufrechterhaltung eines sicheren Anwendungsentwicklungsprozesses	codebuild-project-artifact-encryption	Um sensible Daten im Speicher zu schützen, stellen Sie sicher, dass die Verschlüsselung für Ihre AWS CodeBuild Artefakte aktiviert ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
16.1	Einrichtung und Aufrechterhaltung eines sicheren Anwendungsentwicklungsprozesses	codebuild-project-logging-enabled	Stellen Sie sicher, dass die AWS CodeBuild Projektprotokollierung aktiviert ist, damit Ihre Build-Ausgabeprotokolle entweder an Amazon CloudWatch oder Amazon Simple Storage Service (Amazon S3) gesendet werden. Build-Ausgabeprotokolle enthalten detaillierte Informationen zu Ihrem Build-Projekt.

Vorlage

Die Vorlage ist verfügbar unter GitHub: Operational Best Practices for CIS Critical Security Controls v8 IG2.

Bewährte Betriebspraktiken für kritische Sicherheitskontrollen der GUS v8 IG3

Konformitätspakete bieten ein allgemeines Compliance-Framework, das es Ihnen ermöglicht, mithilfe verwalteter oder benutzerdefinierter AWS Config Regeln und Abhilfemaßnahmen Kontrollen zur Sicherheits-, Betriebs- oder Kostenoptimierung durchzuführen. AWS Config Conformance Packs dienen als Beispielvorlagen nicht dazu, die vollständige Einhaltung eines bestimmten Governance- oder Compliance-Standards sicherzustellen. Sie sind dafür verantwortlich, selbst zu beurteilen, ob Ihre Nutzung der Services den geltenden gesetzlichen und behördlichen Anforderungen entspricht.

Im Folgenden finden Sie ein Beispiel für eine Zuordnung zwischen den Critical Security Controls v8 des Center for Internet Security (CIS) IG3 und den AWS verwalteten Konfigurationsregeln. Jede AWS Config bezieht sich auf eine bestimmte AWS Ressource und bezieht sich auf eine oder mehrere CIS Critical Security Controls IG3 v8-Steuerelemente. Ein CIS Critical Security Controls IG3 v8-Steuerelement kann sich auf mehrere AWS Config Regeln beziehen. In der folgenden Tabelle finden Sie weitere Informationen und Anleitungen zu diesen Zuordnungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
1.1	Einrichtung und Pflege eines detaillierten Inventars der Unternehmensressourcen	eip-attached	Diese Regel stellt sicher, dass Elastic, die einer Amazon Virtual Private Cloud (Amazon VPC) IPs zugewiesen sind, an Amazon Elastic Compute Cloud (Amazon EC2) - Instances oder verwendete Elastic Network Interfaces angehängt sind. Diese Regel hilft bei der Überwachung ungenutzter Inhalte EIPs in Ihrer Umgebung.
1.1	Einrichtung und Pflege eines detaillierten Inventars der Unternehmensressourcen	ec2-stopped-instance	Aktivieren Sie diese Regel, um bei der Basiskonfiguration von Amazon Elastic Compute Cloud (Amazon EC2) - Instances zu helfen, indem Sie überprüfe

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			n, ob EC2 Amazon-Instances gemäß den Standards Ihrer Organisation für mehr als die zulässige Anzahl von Tagen gestoppt wurden.
1.1	Einrichtung und Pflege eines detaillierten Inventars der Unternehmensressourcen	vpc-network-acl-unused-überprüfen	Diese Regel stellt sicher, dass Amazon Virtual Private Cloud (VPC)-Netzwerkzugriffskontrolllisten verwendet werden. Die Überwachung ungenutzter Netzwerkzugriffskontrolllisten kann zu einer genauen Inventarisierung und Verwaltung Ihrer Umgebung beitragen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
1.1	Einrichtung und Pflege eines detaillierten Inventars der Unternehmensressourcen	ec2- -Manager instance-managed-by-systems	Eine Bestandsaufnahme der Softwareplattformen und Anwendungen innerhalb des Unternehmens ist möglich, indem Amazon Elastic Compute Cloud (Amazon EC2) - Instances mit AWS Systems Manager verwaltet werden. Verwenden Sie AWS Systems Manager, um detaillierte Systemkonfigurationen, Betriebssystem-Patch-Levels, Namen und Typ der Dienste, Softwareinstallationen, Anwendungsname, Herausgeber und Version sowie andere Details zu Ihrer Umgebung bereitzustellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
1.1	Einrichtung und Pflege eines detaillierten Inventars der Unternehmensressourcen	ec2-check managedinstance-association-compliance-status	Verwenden Sie AWS Systems Manager Associations, um bei der Inventarisierung von Softwareplattformen und Anwendungen innerhalb eines Unternehmens zu helfen. AWS Systems Manager weist Ihren verwalteten Instances einen Konfigurationsstatus zu und ermöglicht es Ihnen, Basiswerte für Betriebssystem-Patch-Levels, Softwareinstallationen, Anwendungskonfigurationen und andere Details zu Ihrer Umgebung festzulegen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
1.1	Einrichtung und Pflege eines detaillierten Inventars der Unternehmensressourcen	ec2-eni security-group-attached-to	Diese Regel stellt sicher, dass die Sicherheitsgruppen an eine Amazon Elastic Compute Cloud (Amazon EC2) -Instance oder an eine ENI angehängt sind. Diese Regel unterstützt die Überwachung ungenutzter Sicherheitsgruppen im Bestand und die Verwaltung Ihrer Umgebung.
2.2	Sicherstellen, dass autorisierte Software derzeit unterstützt wird	elastic-beanstalk-managed-updates-aktiviert	Durch die Aktivierung verwalteter Plattformupdates für eine Amazon-Elastic-Beanstalk-Umgebung wird sichergestellt, dass die aktuellen verfügbaren Plattform-Fixes, -Updates und -Features für die Umgebung installiert sind. Eine bewährte Methode zur Sicherung von Systemen besteht darin, stets die aktuellen Patches zu installieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
2.2	Sicherstellen, dass autorisierte Software derzeit unterstützt wird	ec2- prüfen managedinstance-patch-compliance-status	Aktivieren Sie diese Regel, um bei der Identifizierung und Dokumentation von Sicherheitslücken in Amazon Elastic Compute Cloud (Amazon EC2) zu helfen. Die Regel prüft, ob die EC2 Amazon-Instance die Patch-Konformität im AWS Systems Manager gemäß den Richtlinien und Verfahren Ihrer Organisation einhält.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
2.2	Sicherstellen, dass autorisierte Software derzeit unterstützt wird	ecs-fargate-latest-platform-Version	Sicherheitsupdates und Patches werden automatisch für Ihre AWS Fargate-Aufgaben bereitgestellt. Wenn ein Sicherheitsproblem gefunden wird, das eine AWS Fargate-Plattformversion betrifft, AWS wird die Plattformversion gepatcht. Um Sie bei der Patchverwaltung Ihrer Amazon Elastic Container Service (ECS) - Aufgaben zu unterstützen, auf denen AWS Fargate ausgeführt wird, aktualisieren Sie Ihre eigenständigen Service-Aufgaben, sodass sie die neueste Plattformversion verwenden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
2.4	Tools zur automatisierten Softwareinventur nutzen	ec2-manager instance-managed-by-systems	Eine Bestandsaufnahme der Softwareplattformen und Anwendungen innerhalb des Unternehmens ist möglich, indem Amazon Elastic Compute Cloud (Amazon EC2) - Instances mit AWS Systems Manager verwaltet werden. Verwenden Sie AWS Systems Manager, um detaillierte Systemkonfigurationen, Betriebssystem-Patch-Levels, Namen und Typ der Dienste, Softwareinstallationen, Anwendungsname, Herausgeber und Version sowie andere Details zu Ihrer Umgebung bereitzustellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
2.4	Tools zur automatisierten Softwareinventur nutzen	ec2-check managedinstance-association-compliance-status	Verwenden Sie AWS Systems Manager Associations, um bei der Inventarisierung von Softwareplattformen und Anwendungen innerhalb eines Unternehmens zu helfen. AWS Systems Manager weist Ihren verwalteten Instances einen Konfigurationsstatus zu und ermöglicht es Ihnen, Basiswerte für Betriebssystem-Patch-Levels, Softwareinstallationen, Anwendungskonfigurationen und andere Details zu Ihrer Umgebung festzulegen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.3	Datenzugriffskontrolllisten konfigurieren	ec2-imdsv2-check	Stellen Sie sicher, dass die Methode Instance Metadata Service Version 2 (IMDSv2) aktiviert ist, um den Zugriff auf und die Kontrolle der Amazon Elastic Compute Cloud (Amazon EC2) - Instance-Metadaten zu schützen. Die IMDSv2 Methode verwendet sitzungsbasierte Kontrollen. Mit können Kontrollen implementiert werden IMDSv2, um Änderungen an Instanzmetadaten einzuschränken.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.3	Datenzugriffskontrolllisten konfigurieren	ec2- instance-profile-attached	EC2 Instanzprofile übergeben eine IAM-Rolle an eine EC2 Instance. Das Anhängen eines Instance-Profils an Ihre Instances kann bei der Implementierung von geringsten Berechtigungen und der Berechtigungsverwaltung helfen.
3.3	Datenzugriffskontrolllisten konfigurieren	dms-replication-not-public	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass auf DMS-Replikationsinstanzen nicht öffentlich zugegriffen werden kann. DMS-Replikations-Instances können vertrauliche Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.3	Datenzugriffskontrolllisten konfigurieren	ebs-snapshot-public-restorable-überprüfen	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass EBS-Snapshots nicht öffentlich wiederherstellbar sind. EBS-Volume-Snapshots können vertrauliche Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.3	Datenzugriffskontrolllisten konfigurieren	emr-kerberos-enabled	Die Zugriffsberechtigungen und -autorisierungen können verwaltet und nach den Prinzipien der geringsten Berechtigung und Aufgabentrennung integriert werden, indem Kerberos für Amazon-EMR-Cluster aktiviert wird. In Kerberos werden Services und Benutzer, die sich authentifizieren müssen, als Prinzipale bezeichnet. Prinzipale befinden sich in einem Kerberos-Bereich. Innerhalb dieses Bereichs wird ein Kerberos-Server als Key Distribution Center (KDC) bezeichnet. Über diesen Server können sich Prinzipale authentifizieren. Die Authentifizierung im KDC erfolgt durch die Ausstellung von Authentif

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			izierungstickets. Das KDC unterhält eine Datenbank der Prinzipale in seinem Bereich mit ihren Passwörtern und anderen administr ativen Informationen zu jedem Prinzipal.
3.3	Datenzugriffskontr olllisten konfigurieren	iam-group-has-users-überprüfen	AWS Identity and Access Managemen t (IAM) kann Ihnen helfen, die Prinzipien der geringsten Rechte und der Aufgabent rennung mit Zugriffsb erechtigungen und Autorisierungen zu integrieren, indem sichergestellt wird, dass IAM-Gruppen mindestens einen Benutzer haben. Die Einteilung von Benutzern in Gruppen auf der Grundlage der ihnen zugewiese nen Berechtigungen oder ihrer Funktion ist eine Möglichkeit, das Prinzip der geringste n Berechtigung zu implementieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.3	Datenzugriffskontrolllisten konfigurieren	iam-no-inline-policy-überprüfen	Stellen Sie sicher, dass ein Benutzer, eine IAM-Rolle oder eine IAM-Gruppe (AWS Identity and Access Management) nicht über eine Inline-Richtlinie zur Zugriffskontrolle auf Systeme und Ressourcen verfügt. AWS empfiehlt, verwaltete Richtlinien anstelle von Inline-Richtlinien zu verwenden. Verwaltete Richtlinien ermöglichen Wiederverwendbarkeit, Versionsverwaltung, Rollback und Delegierung der Berechtigungsverwaltung.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.3	Datenzugriffskontrolllisten konfigurieren	ec2- instance-no-public-ip	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon Elastic Compute Cloud (Amazon EC2) - Instances nicht öffentlich zugänglich sind. EC2Amazon -Instances können vertrauliche Informationen enthalten, und für solche Konten ist eine Zugriffskontrolle erforderlich.
3.3	Datenzugriffskontrolllisten konfigurieren	iam-policy-no-statements-with-full-access	Stellen Sie sicher, dass IAM-Aktionen nur auf die benötigten Aktionen beschränkt sind. Wenn Benutzern mehr Rechte eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und der Aufgabentrennung verstoßen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.3	Datenzugriffskontrolllisten konfigurieren	elasticsearch-in-vpc-only	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass sich Amazon OpenSearch OpenSearch Service (Service) - Domains innerhalb einer Amazon Virtual Private Cloud (Amazon VPC) befinden. Eine OpenSearch Service-Domain innerhalb einer Amazon VPC ermöglicht die sichere Kommunikation zwischen OpenSearch Service und anderen Services innerhalb der Amazon VPC, ohne dass ein Internet-Gateway, ein NAT-Gerät oder eine VPN-Verbindung erforderlich ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.3	Datenzugriffskontrolllisten konfigurieren	iam-user-group-membership-überprüfen	AWS Identity and Access Management (IAM) kann Ihnen helfen, Zugriffsberechtigungen und Autorisierungen einzuschränken, indem sichergestellt wird, dass Benutzer Mitglieder mindestens einer Gruppe sind. Wenn Benutzern mehr Berechtigungen eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und Aufgabentrennung verstoßen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.3	Datenzugriffskontrolllisten konfigurieren	ec2- instances-in-vpc	Stellen Sie Amazon Elastic Compute Cloud (Amazon EC2) -Instances innerhalb einer Amazon Virtual Private Cloud (Amazon VPC) bereit, um eine sichere Kommunikation zwischen einer Instance und anderen Services innerhalb der Amazon VPC zu ermöglichen, ohne dass ein Internet-Gateway, ein NAT-Gerät oder eine VPN-Verbindung erforderlich ist. Der gesamte Datenverkehr bleibt sicher in der AWS Cloud. Domains, die sich innerhalb einer VPC befinden, verfügen aufgrund ihrer logischen Isolierung im Vergleich zu Domains mit öffentlichen Endpunkten über eine zusätzliche Sicherheitsebene. Weisen Sie EC2

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			Amazon-Instances einer Amazon-VPC zu, um den Zugriff ordnungsgemäß zu verwalten.
3.3	Datenzugriffskontrolllisten konfigurieren	emr-master-no-public-ip	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon EMR-Cluster-Masterknoten nicht öffentlich zugänglich sind. Amazon-EMR-Cluster-Hauptknoten können vertrauliche Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.3	Datenzugriffskontrolllisten konfigurieren	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) kann Ihnen dabei helfen, die Prinzipien der geringsten Rechte und der Aufgabentrennung in Zugriffsberechtigungen und Autorisierungen zu integrieren und so zu verhindern, dass Richtlinien „Effect“: „Allow“ mit „Action“: „*“ anstelle von „Resource“: „*“ enthalten. Wenn Benutzern mehr Rechte eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und der Aufgabentrennung verstoßen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.3	Datenzugriffskontrolllisten konfigurieren	iam-user-no-policies-überprüfen	Diese Regel stellt sicher, dass AWS Identity and Access Management (IAM) -Richtlinien nur Gruppen oder Rollen zugewiesen werden, um den Zugriff auf Systeme und Ressourcen zu kontrollieren. Die Zuweisung von Berechtigungen auf Gruppen- oder Rollenebene trägt dazu bei, die Wahrscheinlichkeit zu verringern, dass eine Identität übermäßige Berechtigungen erhält oder beibehält.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.3	Datenzugriffskontrolllisten konfigurieren	iam-root-access-key-überprüfen	Der Zugriff auf Systeme und Ressourcen kann gesteuert werden, indem überprüft wird, ob der Root-Benutzer keine Zugriffsschlüssel mit seiner AWS Identity and Access Management (IAM) -Rolle verknüpft hat. Stellen Sie sicher, dass die Root-Zugriffsschlüssel gelöscht werden. Erstellen und verwenden Sie stattdessen rollenbasierte Funktionen, AWS-Konten um das Prinzip der geringsten Funktionalität zu berücksichtigen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.3	Datenzugriffskontrolllisten konfigurieren	iam-user-unused-credentials-überprüfen	AWS Identity and Access Management (IAM) kann Ihnen bei Zugriffsberechtigungen und Autorisierungen helfen, indem es nach IAM-Passwörtern und Zugriffsschlüsseln sucht, die für einen bestimmten Zeitraum nicht verwendet wurden. Wenn ungenutzte Anmeldeinformationen identifiziert werden, müssen Sie sie deaktivieren und/oder entfernen, da dies gegen das Prinzip der geringsten Berechtigung verstoßen könnte. Für diese Regel müssen Sie einen Wert für das maxCredentialUsage Alter festlegen (Standardkonfiguration: 90). Der tatsächliche Wert muss den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.3	Datenzugriffskontrolllisten konfigurieren	iam-customer-policy-blocked-kms-Aktionen	AWS Identity and Access Management (IAM) kann Ihnen helfen, die Prinzipien der geringsten Rechte und der Aufgabentrennung in Zugriffsberechtigungen und Autorisierungen zu integrieren und so zu verhindern, dass Richtlinien blockierte Aktionen für alle AWS Schlüssel des Key Management Service enthalten. Wenn Benutzer mehr Rechte haben, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und Aufgabentrennung verstoßen. Mit dieser Regel können Sie den Parameter festlegen. blockedActionsPatterns (Wert „AWS Bewährte grundlegende Sicherheitsmethode

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			n“: kms: Entschlüs seln, kms:ReEnc ryptFrom). Die tatsächlichen Werte müssen den Richtlini en Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.3	Datenzugriffskontrolllisten konfigurieren	iam-inline-policy-blocked-kms-Aktionen	Stellen Sie sicher, dass ein Benutzer, eine IAM-Rolle oder eine IAM-Gruppe (AWS Identity and Access Management) nicht über eine Inline-Richtlinie verfügt, die blockierte Aktionen für alle AWS Schlüssel des Key Management Service zulässt. AWS empfiehlt, verwaltete Richtlinien anstelle von Inline-Richtlinien zu verwenden. Verwaltete Richtlinien ermöglichen Wiederverwendbarkeit, Versionsverwaltung, Rollback und Delegierung der Berechtigungsverwaltung. Mit dieser Regel können Sie den blockedActionsPatterns Parameter festlegen. (Wert „AWS Bewährte grundlegende Sicherheitsmethoden“: kms: Entschlüsseln, kms:ReEnc

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			ryptFrom). Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.
3.3	Datenzugriffskontrolllisten konfigurieren	lambda-function-public-access-verboten	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass AWS Lambda-Funktionen nicht öffentlich zugänglich sind. Der öffentliche Zugriff kann möglicherweise die Verfügbarkeit von Ressourcen beeinträchtigen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.3	Datenzugriffskontrolllisten konfigurieren	lambda-inside-vpc	Stellen Sie AWS Lambda-Funktionen in einer Amazon Virtual Private Cloud (Amazon VPC) bereit, um eine sichere Kommunikation zwischen einer Funktion und anderen Diensten innerhalb der Amazon VPC zu gewährleisten. Bei dieser Konfiguration sind kein Internet-Gateway, kein NAT-Gerät und keine VPN-Verbindung erforderlich. Der gesamte Datenverkehr bleibt sicher in der Cloud. AWS Domains, die sich innerhalb einer VPC befinden, verfügen aufgrund ihrer logischen Isolierung im Vergleich zu Domains mit öffentlichen Endpunkten über eine zusätzliche Sicherheitsebene. Um den Zugriff ordnungsgemäß zu verwalten,

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			sollten AWS Lambda-Funktionen einer VPC zugewiesen werden.
3.3	Datenzugriffskontrolllisten konfigurieren	rds-snapshots-public-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Relational Database Service (Amazon RDS) -Instances nicht öffentlich sind. Amazon-RDS-Datenbank-Instances können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.3	Datenzugriffskontrolllisten konfigurieren	rds-instance-public-access-überprüfen	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Relational Database Service (Amazon RDS) -Instances nicht öffentlich sind. Amazon-RDS-Datenbank-Instances können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.3	Datenzugriffskontrolllisten konfigurieren	redshift-cluster-public-access-überprüfen	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Redshift Redshift-Cluster nicht öffentlich sind. Amazon-Redshift-Cluster können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.3	Datenzugriffskontrolllisten konfigurieren	account-level-public-accesss3-Blöcke-periodisch	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Simple Storage Service (Amazon S3) -Buckets nicht öffentlich zugänglich sind. Diese Regel trägt dazu bei, sensible Daten vor unbefugten Remote-Benutzern zu schützen, indem sie den öffentlichen Zugriff verhindert. Mit dieser Regel können Sie optional die Parameter ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) und restrictPublicBuckets Parameter (Config Default: True) festlegen. Die tatsächlichen Werte müssen den Richtlini

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			en Ihrer Organisation entsprechen.
3.3	Datenzugriffskontrolllisten konfigurieren	s-3 bucket-public-read-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie nur autorisierten Benutzern, Prozessen und Geräten Zugriff auf Amazon Simple Storage Service (Amazon S3) - Buckets gewähren. Die Verwaltung des Zugriffs sollte mit der Klassifizierung der Daten übereinstimmen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.3	Datenzugriffskontrolllisten konfigurieren	s-3 bucket-public-write-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie nur autorisierten Benutzern, Prozessen und Geräten Zugriff auf Amazon Simple Storage Service (Amazon S3) - Buckets gewähren. Die Verwaltung des Zugriffs sollte mit der Klassifizierung der Daten übereinstimmen.
3.3	Datenzugriffskontrolllisten konfigurieren	sagemaker-notebook-no-direct-Internetzugang	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass SageMaker Amazon-Notebooks keinen direkten Internetzugang zulassen. Indem Sie direkten Internetzugang blockieren, vermeiden Sie, dass unbefugte Benutzer auf sensible Daten zugreifen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.3	Datenzugriffskontrolllisten konfigurieren	subnet-auto-assign-public-ip-deaktiviert	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon Virtual Private Cloud (VPC) -Subnetzen nicht automatisch eine öffentliche IP-Adresse zugewiesen wird. Amazon Elastic Compute Cloud (EC2) -Instances, die in Subnetzen gestartet werden, in denen dieses Attribut aktiviert ist, haben ihrer primären Netzwerkschnittstelle eine öffentliche IP-Adresse zugewiesen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.3	Datenzugriffskontrolllisten konfigurieren	ssm-document-not-public	Stellen Sie sicher, dass AWS Systems Manager (SSM) - Dokumente nicht öffentlich sind, da dies einen unbeabsichtigten Zugriff auf Ihre SSM-Dokumente ermöglichen kann. Ein öffentliches SSM-Dokument kann Informationen über Ihr Konto, Ihre Ressourcen und internen Prozesse preisgeben.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.3	Datenzugriffskontrolllisten konfigurieren	ecs-task-definition-user-for-host-mode-check	Wenn für eine Aufgabendefinition erhöhte Berechtigungen gelten, liegt das daran, dass der Kunde diesen Konfigurationen ausdrücklich zugestimmt hat. Diese Kontrolle prüft, ob eine unerwartete Berechtigungseskalation vorliegt, wenn für eine Aufgabendefinition das Host-Netzwerk aktiviert ist, die Kunden aber keine erhöhten Berechtigungen aktiviert haben.
3.3	Datenzugriffskontrolllisten konfigurieren	ecs-task-definition-nonroot-benutzer	Sie bestimmen einen Nicht-Root-Benutzer für den Zugriff auf Ihre Aufgabendefinitionen des Amazon Elastic Container Service (Amazon ECS), um die Implementierung des Prinzips der geringsten Berechtigung zu unterstützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.3	Datenzugriffskontrolllisten konfigurieren	autoscaling-launch-config-public-ip-deaktiviert	Wenn Sie Ihre Netzwerkschnittstellen mit einer öffentlichen IP-Adresse konfigurieren, sind die diesen Netzwerkschnittstellen zugehörigen Ressourcen über das Internet erreichbar. EC2 Ressourcen sollten nicht öffentlich zugänglich sein, da dies einen unbeabsichtigten Zugriff auf Ihre Anwendungen oder Server ermöglichen kann.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.3	Datenzugriffskontrolllisten konfigurieren	opensearch-in-vpc-only	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass sich Amazon OpenSearch Service-Domains innerhalb einer Amazon Virtual Private Cloud (Amazon VPC) befinden. Eine Amazon OpenSearch Service-Domain innerhalb einer Amazon VPC ermöglicht die sichere Kommunikation zwischen Amazon OpenSearch Service und anderen Services innerhalb der Amazon VPC, ohne dass ein Internet-Gateway, ein NAT-Gerät oder eine VPN-Verbindung erforderlich ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.3	Datenzugriffskontrolllisten konfigurieren	efs-access-point-enforce-Stammverzeichnis	Die Durchsetzung eines Stammverzeichnisses für einen Amazon-Elastic-File-System (Amazon-EFS)-Zugangspunkt trägt dazu bei, den Datenzugriff einzuschränken, indem sichergestellt wird, dass Benutzer des Zugangspunkts nur auf Dateien des angegebenen Unterverzeichnisses zugreifen können.
3.4	Datenaufbewahrung erzwingen	s3- version-lifecycle-policy-check	Mit Amazon-S3-Lebenszyklusregeln können Sie Aktionen definieren, die Amazon S3 während der Lebensdauer eines Objekts ausführen soll (z. B. die Überführung von Objekten in eine andere Speicherklasse, ihre Archivierung oder Löschung nach einem bestimmten Zeitraum).

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.4	Datenaufbewahrung erzwingen	cw-loggroup-retention-period-überprüfen	Stellen Sie sicher, dass die Ereignisprotokolldaten für Ihre Protokollgruppen über eine Mindestdauer aufbewahrt werden, um die Fehlerbehebung und forensische Untersuchungen zu unterstützen. Fehlende frühere Ereignisprotokolldaten erschweren die Rekonstruierung und Identifizierung potenziell schädlicher Ereignisse.
3.10	Verschlüsselung von sensiblen Daten während der Übertragung	api-gw-ssl-enabled	Stellen Sie sicher, dass die REST-API-Stufen von Amazon API Gateway mit SSL-Zertifikaten konfiguriert sind, damit Backend-Systeme überprüfen können, ob Anforderungen von API Gateway stammen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3,10	Verschlüsselung von sensiblen Daten während der Übertragung	alb-http-to-https-Umleitungsprüfung	Um Daten während der Übertragung zu schützen, stellen Sie sicher, dass Ihr Application Load Balancer unverschlüsselte HTTP-Anfragen automatisch an HTTPS umleitet. Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.10	Verschlüsselung von sensiblen Daten während der Übertragung	elb-acm-certificate-required	Zum Schutz von eventuell vorhanden en sensiblen Daten sowie von Daten während der Übertragung muss die Verschlüsselung für Ihr Elastic Load Balancing aktiviert sein. Verwenden Sie AWS Certificate Manager, um öffentlic he und private SSL/ TLS-Zertifikate mit AWS Diensten und internen Ressource n zu verwalten, bereitzustellen und bereitzustellen.
3.10	Verschlüsselung von sensiblen Daten während der Übertragung	elb-tls-https-listeners-nur	Stellen Sie sicher, dass Ihre Elastic Load Balancer (ELBs) mit SSL- oder HTTPS-Listenern konfiguriert sind. Um eventuell vorhanden e sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.10	Verschlüsselung von sensiblen Daten während der Übertragung	s-3 bucket-ssl-requests-only	Um Daten während der Übertragung zu schützen, stellen Sie sicher, dass Ihre Amazon Simple Storage Service (Amazon S3)-Buckets Anfragen zur Verwendung von Secure Socket Layer (SSL)-Buckets erfordern. Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.
3,10	Verschlüsselung von sensiblen Daten während der Übertragung	redshift-require-tls-ssl	Stellen Sie sicher, dass Ihre Amazon-Redshift-Cluster eine TLS/SSL-Verschlüsselung erfordern, um eine Verbindung zu SQL-Clients herzustellen. Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3,10	Verschlüsselung von sensiblen Daten während der Übertragung	Elb v 2 acm-certificate-required	Zum Schutz von eventuell vorhanden en sensiblen Daten sowie von Daten während der Übertragung muss die Verschlüsselung für Ihr Elastic Load Balancing aktiviert sein. Verwenden Sie AWS Certificate Manager, um öffentlic he und private SSL/ TLS-Zertifikate mit AWS Diensten und internen Ressource n zu verwalten, bereitzustellen und bereitzustellen.
3.10	Verschlüsselung von sensiblen Daten während der Übertragung	opensearch-https-required	Da sensible Daten existieren können und um Daten während der Übertragung zu schützen, sollten Sie sicherstellen, dass HTTPS für Verbindun gen zu Ihren Amazon OpenSearch Service-Domains aktiviert ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.10	Verschlüsselung von sensiblen Daten während der Übertragung	elasticsearch-node-to-node-Verschlüsselungsprüfung	Stellen Sie sicher, dass die node-to-node Verschlüsselung für Amazon OpenSearch Service aktiviert ist. Node-to-nodeVerschlüsselung ermöglicht die TLS 1.2-Verschlüsselung für die gesamte Kommunikation innerhalb der Amazon Virtual Private Cloud (Amazon VPC). Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.10	Verschlüsselung von sensiblen Daten während der Übertragung	opensearch-node-to-node-Verschlüsselungsprüfung	Stellen Sie sicher, dass die node-to-node Verschlüsselung für Amazon OpenSearch Service aktiviert ist. Node-to-nodeVerschlüsselung ermöglicht die TLS 1.2-Verschlüsselung für die gesamte Kommunikation innerhalb der Amazon Virtual Private Cloud (Amazon VPC). Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.
3.11	Verschlüsselung von sensiblen Daten im Ruhezustand	cloud-trail-encryption-enabled	Zum Schutz von eventuell vorhandenen sensiblen Daten sowie Daten im Ruhezustand müssen Sie sicherstellen, dass die Verschlüsselung für Ihre AWS CloudTrail aktiviert ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3,11	Verschlüsselung von sensiblen Daten im Ruhezustand	encrypted-volumes	Aktivieren Sie die Verschlüsselung für Ihre Amazon-Elastic-Block-Store (Amazon-EBS)-Volumes, um eventuell vorhandene sensible Daten sowie Daten im Ruhezustand zu schützen.
3,11	Verschlüsselung von sensiblen Daten im Ruhezustand	ec-2 ebs-encryption-by-default	Zum Schutz von Daten im Ruhezustand müssen Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon Elastic Block Store (Amazon EBS)-Volumes aktiviert ist. Da sensible Daten auch im Ruhezustand vorhanden sein können, sollten Sie die Verschlüsselung im Ruhezustand aktivieren, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.11	Verschlüsselung von sensiblen Daten im Ruhezustand	efs-encrypted-check	Aktivieren Sie die Verschlüsselung für Ihr Amazon Elastic File System (EFS), um eventuell vorhandene sensible Daten sowie Daten im Ruhezustand zu schützen.
3,11	Verschlüsselung von sensiblen Daten im Ruhezustand	backup-recovery-point-encrypted	Stellen Sie sicher, dass die Verschlüsselung für Ihre AWS Backup-Wiederherstellungspunkte aktiviert ist. Da sensible Daten auch im Ruhezustand vorhanden sein können, sollten Sie die Verschlüsselung im Ruhezustand aktivieren, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.11	Verschlüsselung von sensiblen Daten im Ruhezustand	elasticsearch-encrypted-at-rest	Da sensible Daten vorhanden sein können und um Daten im Ruhezustand zu schützen, sollten Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon OpenSearch Service (OpenSearch Service) -Domains aktiviert ist.
3.11	Verschlüsselung von sensiblen Daten im Ruhezustand	redshift-cluster-kms-enabled	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass die Verschlüs selung mit AWS Key Management Service (AWS KMS) für Ihren Amazon Redshift Redshift-Cluster aktiviert ist. Um eventuell vorhanden e sensible Daten im Ruhezustand in Redshift-Clustern zu schützen, muss die Verschlüsselung von Daten im Ruhezusta nd aktiviert sein.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.11	Verschlüsselung von sensiblen Daten im Ruhezustand	rds-storage-encrypted	Zum Schutz von Daten im Ruhezustand müssen Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon Relational Database Service (Amazon RDS)-Instances aktiviert ist. Um eventuell vorhandene sensible Daten im Ruhezustand in Amazon-RDS-Instances zu schützen, muss die Verschlüsselung von Daten im Ruhezustand aktiviert sein.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3,11	Verschlüsselung von sensiblen Daten im Ruhezustand	rds-snapshot-encrypted	Stellen Sie sicher, dass die Verschlüsselung für Ihre Amazon Relational Database Service (Amazon RDS)-Snapshots aktiviert ist. Da sensible Daten auch im Ruhezustand vorhanden sein können, sollten Sie die Verschlüsselung im Ruhezustand aktivieren, um diese Daten zu schützen.
3,11	Verschlüsselung von sensiblen Daten im Ruhezustand	s-3 default-encryption-kms	Stellen Sie sicher, dass die Verschlüsselung für Ihre Amazon Simple Storage Service (Amazon S3)-Buckets aktiviert ist. Um eventuell vorhandene sensible Daten im Ruhezustand in einem Amazon-S3-Bucket zu schützen, muss die Verschlüsselung aktiviert sein.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3,11	Verschlüsselung von sensiblen Daten im Ruhezustand	redshift-cluster-configuration-check	Um Daten im Ruhezustand zu schützen, muss die Verschlüsselung für Ihre Amazon-Redshift-Cluster aktiviert sein. Sie müssen auch sicherstellen, dass die erforderlichen Konfigurationen auf Amazon-Redshift-Clustern bereitgestellt werden. Die Prüfungsprotokollierung muss aktiviert sein, um Informationen zu Verbindungen und Benutzeraktivitäten in der Datenbank bereitzustellen. Diese Regel erfordert, dass ein Wert für clusterDbEncrypted (Config Default: TRUE) und LoggingEnabled (Config Default: TRUE) gesetzt ist. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.11	Verschlüsselung von sensiblen Daten im Ruhezustand	sagemaker-endpoint-configuration-kms-schlüsselkonfiguriert	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass die Verschlüsselung mit dem AWS Key Management Service (AWS KMS) für Ihren Endpunkt aktiviert ist. SageMaker Da sensible Daten auf dem SageMaker Endgerät gespeiche rt werden können, sollten Sie die Verschlüsselung im Ruhezustand aktiviere n, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.11	Verschlüsselung von sensiblen Daten im Ruhezustand	sagemaker-notebook-instance-kms-schlüsselkonfiguriert	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass die Verschlüsselung mit dem AWS Key Management Service (AWS KMS) für Ihr Notebook aktiviert ist. SageMaker Da vertrauliche Daten im SageMaker Notebook gespeichert werden können, sollten Sie die Verschlüsselung im Ruhezustand aktivieren, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.11	Verschlüsselung von sensiblen Daten im Ruhezustand	secretsmanager-using-cmk	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass die Verschlüsselung mit dem AWS Key Management Service (AWS KMS) für AWS Secrets Manager aktiviert ist. Aktivieren Sie die Verschlüsselung von Daten im Ruhezustand, um eventuell vorhandene sensible Daten im Ruhezustand im Secrets Manager zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.11	Verschlüsselung von sensiblen Daten im Ruhezustand	s3-fähig bucket-server-side-encryption	Zum Schutz von Daten im Ruhezustand müssen Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon Simple Storage Service (Amazon S3)-Buckets aktiviert ist. Um eventuell vorhandene sensible Daten im Ruhezustand in Amazon-S3-Buckets zu schützen, muss die Verschlüsselung aktiviert sein.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.11	Verschlüsselung von sensiblen Daten im Ruhezustand	sns-encrypted-kms	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass Ihre Amazon Simple Notification Service (Amazon SNS) -Themen mit dem AWS Key Management Service (AWS KMS) verschlüsselt werden müssen. Um eventuell vorhandene sensible Daten im Ruhezustand in veröffentlichten Nachrichten zu schützen, muss die Verschlüsselung von Daten im Ruhezustand aktiviert sein.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.11	Verschlüsselung von sensiblen Daten im Ruhezustand	dynamodb-table-encrypted-kms	Stellen Sie sicher, dass die Verschlüsselung für Ihre Amazon-DynamoDB-Tabellen aktiviert ist. Um eventuell vorhandene sensible Daten im Ruhezustand in diesen Tabellen zu schützen, müssen Sie die Verschlüsselung von Daten im Ruhezustand aktivieren. Standardmäßig werden DynamoDB-Tabellen mit einem AWS eigenen Kundenhauptschlüssel (CMK) verschlüselt.
3.11	Verschlüsselung von sensiblen Daten im Ruhezustand	opensearch-encrypted-at-rest	Da sensible Daten vorhanden sein können und um Daten im Ruhezustand zu schützen, sollten Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon OpenSearch Service-Domains aktiviert ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.14	Protokollieren der Zugriffe auf sensible Daten	api-gw-execution-logging-aktiviert	Die API-Gateway-Protokollierung zeigt detaillierte Ansichten der Benutzer, die auf die API zugegriffen haben, und wie diese Benutzer auf die API zugegriffen haben. Diese Einblicke ermöglichen die Transparenz von Benutzeraktivitäten.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.14	Protokollieren der Zugriffe auf sensible Daten	multi-region-cloudtrail-enabled	AWS CloudTrail zeichnet Aktionen und API-Aufrufe der AWS Management Console auf. Sie können feststellen, welche Benutzer und Konten angerufen wurden AWS, von welcher Quell-IP-Adresse aus die Anrufe getätigt wurden und wann die Anrufe erfolgten. CloudTrail übermittelt Protokolldateien aus allen AWS Regionen an Ihren S3-Bucket , wenn MULTI_REG ION_CLOUD _TRAIL_ENABLED aktiviert ist. Außerdem wird beim AWS Start einer neuen Region derselbe Trail in der neuen Region erstellt. CloudTrail Dadurch erhalten Sie automatis ch Protokolldateien mit API-Aktivitäten für die neue Region.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.14	Protokollieren der Zugriffe auf sensible Daten	cloudtrail-s3-data events-enabled	Die Erfassung von Simple Storage Service (Amazon S3)-Datenereignissen unterstützt die Erkennung von ungewöhnlichen Aktivitäten. Zu den Details gehören Informationen zu dem AWS -Konto, das auf einen Amazon-S3-Bucket zugegriffen hat, die IP-Adresse und die Uhrzeit des Ereignisses.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3,14	Protokollieren der Zugriffe auf sensible Daten	cloudtrail-enabled	AWS CloudTrai l kann durch die Aufzeichnung von Aktionen und API-Aufrufen in der AWS Management Console bei der Nichtabst reitbarkeit helfen. Sie können die Benutzer und die Benutzer AWS-Konten , die einen AWS Dienst aufgerufen haben, die Quell-IP-Adresse, über die die Aufrufe generiert wurden, und den Zeitpunkt der Anrufe identifiz ieren. Einzelheiten zu den erfassten Daten finden Sie unter Inhalt des AWS CloudTrail Datensatzes.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.14	Protokollieren der Zugriffe auf sensible Daten	cloud-trail-cloud-watch-logs-aktiviert	Verwenden Sie Amazon CloudWatch , um Protokoll ereignisaktivitäten zentral zu sammeln und zu verwalten. Die Aufnahme von AWS CloudTrail Daten liefert Einzelheiten zu den API-Aufrufaktivitäten in Ihrem AWS-Konto.
3.14	Protokollieren der Zugriffe auf sensible Daten	elasticsearch-logs-to-cloudwatch	Stellen Sie sicher, dass für Amazon OpenSearch Service-Domains Fehlerprotokolle aktiviert und zur Aufbewahrung und Beantwortung an Amazon CloudWatch Logs gestreamt werden. Domain-Fehlerprotokolle sind bei Sicherheits- und Zugriffsprüfungen sowie bei der Diagnose von Verfügbarkeitsproblemen nützlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.14	Protokollieren der Zugriffe auf sensible Daten	vpc-flow-logs-enabled	VPC-Flow-Protokolle erfassen detaillierte Informationsdatensätze über den IP-Datenverkehr, der zu und von Netzwerkschnittstellen in Ihrer Amazon Virtual Private Cloud (Amazon VPC) fließt. Standardmäßig enthalten Flow-Protokolldatensätze Werte für die verschiedenen Komponenten des IP-Flows, einschließlich Quelle, Ziel und Protokoll.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3,14	Protokollieren der Zugriffe auf sensible Daten	elb-logging-enabled	Die Elastic-Load-Balancing-Aktivität ist ein zentraler Kommunikationspunkt innerhalb einer Umgebung. Stellen Sie sicher, dass die ELB-Protokollierung aktiviert ist. Die gesammelten Daten enthalten detaillierte Informationen zu Anfragen, die an den ELB gesendet wurden. Jedes Protokoll enthält Informationen wie die Zeit, zu der die Anforderung einging, die Client-IP-Adresse, Latenzen, Anforderungspfade und Serverantworten.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3,14	Protokollieren der Zugriffe auf sensible Daten	rds-logging-enabled	Um die Protokollierung und Überwachung in Ihrer Umgebung zu erleichtern, stellen Sie sicher, dass die Amazon Relational Database Service (Amazon RDS)-Protokollierung aktiviert ist. Mit der Amazon-RDS-Protokollierung können Sie Ereignisse wie Verbindungen, Verbindungsabbrüche, Abfragen oder abgefragte Tabellen erfassen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3,14	Protokollieren der Zugriffe auf sensible Daten	s-3 bucket-logging-enabled	Die Amazon Simple Storage Service (Amazon S3)-Serverzugriffs protokollierung bietet eine Methode zur Überwachu ng des Netzwerks im Hinblick auf potenzielle Cybersich erheitsereignisse. Die Ereignisse werden überwacht, indem detaillierte Aufzeichn ungen über die Anfragen erfasst werden, die an einen Amazon-S3-Bucket gestellt wurden. Jeder Zugriffsprotokolle intrag enthält Details zu einer einzelnen Zugriffsanfrage. Zu den Details gehören Anforderer, Bucket-Name, Anforderu ngszeit, Anforderu ngsaktion, Antwortst atus und Fehlercode, falls relevant.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3,14	Protokollieren der Zugriffe auf sensible Daten	redshift-cluster-configuration-check	Um Daten im Ruhezustand zu schützen, muss die Verschlüsselung für Ihre Amazon-Redshift-Cluster aktiviert sein. Sie müssen auch sicherstellen, dass die erforderlichen Konfigurationen auf Amazon-Redshift-Clustern bereitgestellt werden. Die Prüfungsprotokollierung muss aktiviert sein, um Informationen zu Verbindungen und Benutzeraktivitäten in der Datenbank bereitzustellen. Diese Regel erfordert, dass ein Wert für clusterDbEncrypted (Config Default: TRUE) und LoggingEnabled (Config Default: TRUE) gesetzt ist. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.14	Protokollieren der Zugriffe auf sensible Daten	wafv2-logging-enabled	Um die Protokollierung und Überwachung in Ihrer Umgebung zu erleichtern, aktivieren Sie die AWS WAF (V2) -Protokollierung im regionalen und globalen Web. ACLs AWS Die WAF-Protokollierung bietet detaillierte Informationen über den Datenverkehr, der von Ihrer Web-ACL analysiert wird. In den Protokollen werden die Uhrzeit aufgezeichnet, zu der die AWS WAF die Anfrage von Ihrer AWS Ressource erhalten hat, Informationen über die Anfrage und eine Aktion für die Regel, der jede Anfrage entsprach.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.14	Protokollieren der Zugriffe auf sensible Daten	guardduty-enabled-centralized	Amazon GuardDuty kann mithilfe von Threat Intellige nce Feeds helfen, potenzielle Cybersich erheitsereignisse zu überwachen und zu erkennen. Dazu gehören Listen mit bösartigen IPs und maschinel len Lernmethoden zur Identifizierung unerwarteter, nicht autorisierter und bösartiger Aktivitäten in Ihrer AWS Cloud-Umgebung.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.14	Protokollieren der Zugriffe auf sensible Daten	codebuild-project-logging-enabled	Stellen Sie sicher, dass die AWS CodeBuild Projektprotokollierung aktiviert ist, damit Ihre Build-Ausgabeprotokolle entweder an Amazon CloudWatch oder Amazon Simple Storage Service (Amazon S3) gesendet werden. Build-Ausgabeprotokolle enthalten detaillierte Informationen zu Ihrem Build-Projekt.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
4.1	Einrichtung und Pflege eines sicheren Konfigurationsprozesses	account-part-of-organizations	Durch die zentrale Verwaltung AWS-Konten innerhalb von AWS Organizations wird sichergestellt, dass die Konten den Vorschriften entsprechen. Eine fehlende zentrale Kontoverwaltung kann zu inkonsistenten Kontokonfigurationen führen, wodurch Ressourcen und sensible Daten offengelegt werden können.
4.1	Einrichtung und Pflege eines sicheren Konfigurationsprozesses	ec2-stopped-instance	Aktivieren Sie diese Regel, um bei der Basiskonfiguration von Amazon Elastic Compute Cloud (Amazon EC2) - Instances zu helfen, indem Sie überprüfen, ob EC2 Amazon-Instances gemäß den Standards Ihrer Organisation für mehr als die zulässige Anzahl von Tagen gestoppt wurden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
4.1	Einrichtung und Pflege eines sicheren Konfigurationsprozesses	ec2- volume-inuse-check	Diese Regel stellt sicher, dass Amazon Elastic Block Store-Volumes, die an Amazon Elastic Compute Cloud (Amazon EC2) - Instances angehängt sind, zum Löschen markiert werden, wenn eine Instance beendet wird. Wenn ein Amazon-EBS-Volume nicht gelöscht wird, wenn die Instance, an die es angehängt ist, beendet wird, kann dies gegen das Konzept der geringsten Funktionalität verstoßen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
4.1	Einrichtung und Pflege eines sicheren Konfigurationsprozesses	redshift-cluster-maintenancesettings-check	Diese Regel stellt sicher, dass Amazon-Redshift-Cluster die bevorzugten Einstellungen für Ihre Organisation haben. Insbesondere sorgt sie dafür, dass Cluster bevorzugte Wartungsfenster und automatisierte Aufbewahrungsfristen für Snapshots für die Datenbank haben. Für diese Regel müssen Sie die festlegen allowVersionUpgrade. Der Standardwert ist „true“. Außerdem können Sie optional den Zeitraum preferredMaintenanceWindow (der Standardwert ist sa: 16:00 -sa: 16:30) und den automated SnapshotRetention Zeitraum (der Standardwert ist 1) festlegen. Die tatsächlichen Werte müssen den Richtlini

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			en Ihrer Organisation entsprechen.
4.1	Einrichtung und Pflege eines sicheren Konfigurationsprozesses	ec2- -Manager instance-managed-by-systems	Eine Bestandsaufnahme der Softwareplattformen und Anwendungen innerhalb des Unternehmens ist möglich, indem Amazon Elastic Compute Cloud (Amazon EC2) - Instances mit AWS Systems Manager verwaltet werden. Verwenden Sie AWS Systems Manager, um detaillierte Systemkonfigurationen, Betriebssystem-Patch-Levels, Namen und Typ der Dienste, Softwareinstallationen, Anwendungsname, Herausgeber und Version sowie andere Details zu Ihrer Umgebung bereitzustellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
4.1	Einrichtung und Pflege eines sicheren Konfigurationsprozesses	ec2-check managedinstance-association-compliance-status	Verwenden Sie AWS Systems Manager Associations, um bei der Inventarisierung von Softwareplattformen und Anwendungen innerhalb eines Unternehmens zu helfen. AWS Systems Manager weist Ihren verwalteten Instances einen Konfigurationsstatus zu und ermöglicht es Ihnen, Basiswerte für Betriebssystem-Patch-Levels, Softwareinstallationen, Anwendungskonfigurationen und andere Details zu Ihrer Umgebung festzulegen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
4.1	Einrichtung und Pflege eines sicheren Konfigurationsprozesses	efs-access-point-enforce-root-Verzeichnis	Die Durchsetzung eines Stammverzeichnisses für einen Amazon-Elastic-File-System (Amazon-EFS)-Zugangspunkt trägt dazu bei, den Datenzugriff einzuschränken, indem sichergestellt wird, dass Benutzer des Zugangspunkts nur auf Dateien des angegebenen Unterverzeichnisses zugreifen können.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
4.1	Einrichtung und Pflege eines sicheren Konfigurationsprozesses	secretsmanager-rotation-enabled-check	Diese Regel stellt sicher, dass bei AWS Secrets Manager Manager-Geheimnissen die Rotation aktiviert ist. Die regelmäßige Rotation von Secrets kann den Zeitraum verkürzen, in dem ein Secret aktiv ist, und möglicherweise die Auswirkungen auf das Unternehmen verringern, falls das Secret kompromittiert wird.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
4.1	Einrichtung und Pflege eines sicheren Konfigurationsprozesses	access-keys-rotated	Die Anmeldeinformationen für autorisierte Geräte, Benutzer und Prozesse werden geprüft, indem sichergestellt wird, dass die IAM-Zugriffsschlüssel gemäß den Vorgaben der Unternehmensrichtlinie rotiert werden. Das regelmäßige Ändern der Zugriffsschlüssel ist eine bewährte Sicherheitsmethode. Es verkürzt den Zeitraum, in dem ein Zugriffsschlüssel aktiv ist, und reduziert die Auswirkungen auf das Unternehmen, wenn die Schlüssel kompromittiert werden. Diese Regel erfordert einen Wert für die Zugriffsschlüssel-Rotation (Standardkonfiguration: 90). Der tatsächliche Wert muss den Richtlini

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			en Ihrer Organisation entsprechen.
4.6	Sichere Verwaltung von Unternehmensressourcen und -software	alb-http-to-https-Umleitungsprüfung	Um Daten während der Übertragung zu schützen, stellen Sie sicher, dass Ihr Application Load Balancer unverschlüsselte HTTP-Anfragen automatisch an HTTPS umleitet. Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.
4.6	Sichere Verwaltung von Unternehmensressourcen und -software	elb-tls-https-listeners-nur	Stellen Sie sicher, dass Ihre Elastic Load Balancer (ELBs) mit SSL- oder HTTPS-Listenern konfiguriert sind. Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
4.6	Sichere Verwaltung von Unternehmensressourcen und -software	api-gw-ssl-enabled	Stellen Sie sicher, dass die REST-API-Stufen von Amazon API Gateway mit SSL-Zertifikaten konfiguriert sind, damit Backend-Systeme überprüfen können, ob Anforderungen von API Gateway stammen.
4,6	Sichere Verwaltung von Unternehmensressourcen und -software	redshift-require-tls-ssl	Stellen Sie sicher, dass Ihre Amazon-Redshift-Cluster eine TLS/SSL-Verschlüsselung erfordern, um eine Verbindung zu SQL-Clients herzustellen. Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
4,6	Sichere Verwaltung von Unternehmensressourcen und -software	s-3 bucket-ssl-requests-only	Um Daten während der Übertragung zu schützen, stellen Sie sicher, dass Ihre Amazon Simple Storage Service (Amazon S3)-Buckets Anfragen zur Verwendung von Secure Socket Layer (SSL)-Buckets erfordern. Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.
4,6	Sichere Verwaltung von Unternehmensressourcen und -software	opensearch-https-required	Da sensible Daten existieren können und um Daten während der Übertragung zu schützen, sollten Sie sicherstellen, dass HTTPS für Verbindungen zu Ihren Amazon OpenSearch Service-Domains aktiviert ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
4.7	Standardkonten für Unternehmensressourcen und -software verwalten	iam-root-access-key-überprüfen	Der Zugriff auf Systeme und Ressourcen kann gesteuert werden, indem überprüft wird, ob der Root-Benutzer keine Zugriffsschlüssel mit seiner AWS Identity and Access Management (IAM) -Rolle verknüpft hat. Stellen Sie sicher, dass die Root-Zugriffsschlüssel gelöscht werden. Erstellen und verwenden Sie stattdessen rollenbasierte Funktionen, AWS-Konten um das Prinzip der geringsten Funktionalität zu berücksichtigen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
5.1	Erstellen und Verwalten eines Konteninventars	account-part-of-organizations	Durch die zentrale Verwaltung AWS-Konten innerhalb von AWS Organizations wird sichergestellt, dass die Konten den Vorschriften entsprechen. Eine fehlende zentrale Kontoverwaltung kann zu inkonsistenten Kontokonfigurationen führen, wodurch Ressourcen und sensible Daten offengelegt werden können.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
5.2	Verwendung eindeutiger Passwörter	iam-password-policy	Die Identitäten und Anmeldeinformationen werden auf der Grundlage einer organisatorischen IAM-Passwortrichtlinie ausgestellt, verwaltet und verifiziert. Sie erfüllen oder übertreffen die Anforderungen des NIST SP 800-63 und des AWS Foundational Security Best Practices-Standards für Passwortstärke. Mit dieser Regel können Sie optional RequireUppercaseCharacters (Wert für AWS grundlegende Sicherheitsbewährte Methoden: wahr), RequireLowercaseCharacters (Wert für bewährte Methoden für AWS grundlegende Sicherheit: wahr), RequireSymbols (Wert für bewährte Methoden für AWS grundlegende Sicherheit:

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			wahr), RequireNumbers (Wert für bewährte Methoden für AWS grundlegende Sicherheit: wahr), MinimumPasswordLength (Wert für bewährte Methoden für AWS grundlegende Sicherheit: 14), PasswordReusePrevention (Wert für bewährte Methoden für AWS grundlegende Sicherheit: 24) und MaxPasswordAge (Wert für bewährte Methoden für AWS grundlegende Sicherheit: 90) für Ihr IAM festlegen Kennwortrichtlinie. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
5.2	Verwendung eindeutiger Passwörter	iam-user-mfa-enabled	Aktivieren Sie diese Regel, um den Zugriff auf Ressourcen in der AWS -Cloud einzuschränken. Diese Regel stellt sicher, dass die Multi-Faktor-Authentifizierung (MFA) für alle Benutzer aktiviert ist. MFA bietet eine weitere Schutzebene zusätzlich zum Benutzernamen und Passwort. Reduzieren Sie Fälle von kompromittierten Konten, indem Sie MFA für Benutzer vorschreiben.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
5.2	Verwendung eindeutiger Passwörter	mfa-enabled-for-iam-Konsolenzugriff	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass MFA für alle AWS Identity and Access Management (IAM) -Benutzer aktiviert ist, die über ein Konsolenkennwort verfügen. MFA sorgt für eine weitere Schutzebene zusätzlich zu den Anmeldeinformationen. Indem Sie MFA für Benutzer vorschreiben, können Sie Fälle kompromittierter Konten reduzieren und verhindern, dass unbefugte Benutzer auf vertrauliche Daten zugreifen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
5.2	Verwendung eindeutiger Passwörter	root-account-mfa-enabled	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass MFA für den Root-Benutzer aktiviert ist. Der Stammbenutzer ist der AWS-Konto-Benutzer mit den meisten Berechtigungen. MFA bietet eine weitere Schutzebene zusätzlich zum Benutzernamen und Passwort. Indem Sie MFA für den Root-Benutzer vorschreiben, können Sie die Anzahl AWS-Konten kompromittierter Benutzer reduzieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
5.3	Deaktivierung inaktiver Konten	iam-user-unused-credentials-überprüfen	AWS Identity and Access Management (IAM) kann Ihnen bei Zugriffsberechtigungen und Autorisierungen helfen, indem es nach IAM-Passwörtern und Zugriffsschlüsseln sucht, die für einen bestimmten Zeitraum nicht verwendet wurden. Wenn ungenutzte Anmeldeinformationen identifiziert werden, müssen Sie sie deaktivieren und/oder entfernen, da dies gegen das Prinzip der geringsten Berechtigung verstoßen könnte. Für diese Regel müssen Sie einen Wert für das maxCredentialUsage Alter festlegen (Standardkonfiguration: 90). Der tatsächliche Wert muss den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
5.4	Beschränkung der Administratorrechte auf spezielle Administratorkonten	iam-root-access-key-überprüfen	Der Zugriff auf Systeme und Ressourcen kann gesteuert werden, indem überprüft wird, ob der Root-Benutzer keine Zugriffsschlüssel mit seiner AWS Identity and Access Management (IAM) -Rolle verknüpft hat. Stellen Sie sicher, dass die Root-Zugriffsschlüssel gelöscht werden. Erstellen und verwenden Sie stattdessen rollenbasierte Funktionen, AWS-Konten um das Prinzip der geringsten Funktionalität zu berücksichtigen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
5.4	Beschränkung der Administratorrechte auf spezielle Administratorkonten	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) kann Ihnen dabei helfen, die Prinzipien der geringsten Rechte und der Aufgabentrennung in Zugriffsberechtigungen und Autorisierungen zu integrieren und so zu verhindern, dass Richtlinien „Effect“: „Allow“ mit „Action“: „*“ anstelle von „Resource“: „*“ enthalten. Wenn Benutzern mehr Rechte eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und der Aufgabentrennung verstoßen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
5.6	Zentralisierung der Kontoverwaltung	account-part-of-organizations	Durch die zentrale Verwaltung AWS-Konten innerhalb von AWS Organizations wird sichergestellt, dass die Konten den Vorschriften entsprechen. Eine fehlende zentrale Kontoverwaltung kann zu inkonsistenten Kontokonfigurationen führen, wodurch Ressourcen und sensible Daten offengelegt werden können.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
6.4	Erzwingen von MFA für Remote-Netzwerkzugriff	iam-user-mfa-enabled	Aktivieren Sie diese Regel, um den Zugriff auf Ressourcen in der AWS -Cloud einzuschränken. Diese Regel stellt sicher, dass die Multi-Faktor-Authentifizierung (MFA) für alle Benutzer aktiviert ist. MFA bietet eine weitere Schutzebene zusätzlich zum Benutzernamen und Passwort. Reduzieren Sie Fälle von kompromittierten Konten, indem Sie MFA für Benutzer vorschreiben.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
6.4	Erzwingen von MFA für Remote-Netzwerkzugriff	mfa-enabled-for-iam-Konsolenzugriff	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass MFA für alle AWS Identity and Access Management (IAM) -Benutzer aktiviert ist, die über ein Konsolenkennwort verfügen. MFA sorgt für eine weitere Schutzebene zusätzlich zu den Anmeldeinformationen. Indem Sie MFA für Benutzer vorschreiben, können Sie Fälle kompromittierter Konten reduzieren und verhindern, dass unbefugte Benutzer auf vertrauliche Daten zugreifen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
6.4	Erzwingen von MFA für Remote-Netzwerkzugriff	root-account-mfa-enabled	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass MFA für den Root-Benutzer aktiviert ist. Der Stammbenutzer ist der AWS-Konto-Benutzer mit den meisten Berechtigungen. MFA bietet eine weitere Schutzebene zusätzlich zum Benutzernamen und Passwort. Indem Sie MFA für den Root-Benutzer vorschreiben, können Sie die Anzahl AWS-Konten kompromittierter Benutzer reduzieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
6,5	Erzwingen von MFA für Administratorzugriff	root-account-hardware-mfa-aktiviert	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Hardware-MFA für den Root-Benutzer aktiviert ist. Der Stammbenutzer ist der AWS-Konto-Benutzer mit den meisten Berechtigungen. MFA sorgt für eine weitere Schutzebene zusätzlich zu den Anmeldeinformationen. Indem Sie MFA für den Root-Benutzer vorschreiben, können Sie die Anzahl AWS-Konten kompromittierter Benutzer reduzieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
6.7	Zentralisierung der Zugriffskontrolle	account-part-of-organizations	Durch die zentrale Verwaltung AWS-Konten innerhalb von AWS Organizations wird sichergestellt, dass die Konten den Vorschriften entsprechen. Eine fehlende zentrale Kontoverwaltung kann zu inkonsistenten Kontokonfigurationen führen, wodurch Ressourcen und sensible Daten offengelegt werden können.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
7.1	Einrichtung und Pflege eines Prozesses für das Schwachstellenmanagement	guardduty-enabled-centralized	Amazon GuardDuty kann mithilfe von Threat Intelligence Feeds helfen, potenzielle Cybersicherheitsereignisse zu überwachen und zu erkennen. Dazu gehören Listen mit bösartigen IPs und maschinellen Lernmethoden zur Identifizierung unerwarteter, nicht autorisierter und bösartiger Aktivitäten in Ihrer AWS Cloud-Umgebung.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
7.1	Einrichtung und Pflege eines Prozesses für das Schwachstellenmanagement	securityhub-enabled	AWS Security Hub hilft bei der Überwachung von unbefugtem Personal, Verbindungen, Geräten und Software. AWS Security Hub aggregiert, organisiert und priorisiert die Sicherheitswarnungen oder Ergebnisse mehrerer Dienste. AWS Einige dieser Dienste sind Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer und AWS Firewall Manager sowie AWS Partnerlösungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
7.1	Einrichtung und Pflege eines Prozesses für das Schwachstellenmanagement	ec2-prüfen managedinstance-patch-compliance-status	Aktivieren Sie diese Regel, um bei der Identifizierung und Dokumentation von Sicherheitslücken in Amazon Elastic Compute Cloud (Amazon EC2) zu helfen. Die Regel prüft, ob die EC2 Amazon-Instance die Patch-Konformität im AWS Systems Manager gemäß den Richtlinien und Verfahren Ihrer Organisation einhält.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
7.3	Durchführen eines automatisierten Betriebssystem-Patch-Managements	ec2-check managedinstance-patch-compliance-status	Aktivieren Sie diese Regel, um bei der Identifizierung und Dokumentation von Sicherheitslücken in Amazon Elastic Compute Cloud (Amazon EC2) zu helfen. Die Regel prüft, ob die EC2 Amazon-Instance die Patch-Konformität im AWS Systems Manager gemäß den Richtlinien und Verfahren Ihrer Organisation einhält.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
7.3	Durchführen eines automatisierten Betriebssystem-Patch-Managements	elastic-beanstalk-managed-updates-aktiviert	Durch die Aktivierung verwalteter Plattform updates für eine Amazon-Elastic-Beanstalk-Umgebung wird sichergestellt, dass die aktuellen verfügbaren Plattform -Fixes, -Updates und -Features für die Umgebung installiert sind. Eine bewährte Methode zur Sicherung von Systemen besteht darin, stets die aktuellen Patches zu installieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
7.3	Durchführen eines automatisierten Betriebssystem-Patch-Managements	redshift-cluster-maintenancesettings-check	Diese Regel stellt sicher, dass Amazon-Redshift-Cluster die bevorzugten Einstellungen für Ihre Organisation haben. Insbesondere sorgt sie dafür, dass Cluster bevorzugte Wartungsfenster und automatisierte Aufbewahrungsfristen für Snapshots für die Datenbank haben. Für diese Regel müssen Sie die allowVersionUpgrade festlegen. Der Standardwert ist „true“. Außerdem können Sie optional den Zeitraum preferredMaintenanceWindow (der Standardwert ist sa: 16:00 -sa: 16:30) und den automated SnapshotRetention Zeitraum (der Standardwert ist 1) festlegen. Die tatsächlichen Werte müssen den Richtlini

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			en Ihrer Organisation entsprechen.
7.4	Durchführen eines automatisierten Anwendungspatch-Managements	ec2- -check managedinstance-patch-compliance-status	Aktivieren Sie diese Regel, um bei der Identifizierung und Dokumentation von Sicherheitslücken in Amazon Elastic Compute Cloud (Amazon EC2) zu helfen. Die Regel prüft, ob die EC2 Amazon-Instance die Patch-Konformität im AWS Systems Manager gemäß den Richtlinien und Verfahren Ihrer Organisation einhält.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
7.4	Durchführen eines automatisierten Anwendungspatch-Managements	elastic-beanstalk-managed-updates-aktiviert	Durch die Aktivierung verwalteter Plattform updates für eine Amazon-Elastic-Beanstalk-Umgebung wird sichergestellt, dass die aktuellen verfügbaren Plattform -Fixes, -Updates und -Features für die Umgebung installiert sind. Eine bewährte Methode zur Sicherung von Systemen besteht darin, stets die aktuellen Patches zu installieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
7.4	Durchführen eines automatisierten Anwendungspatch-Managements	redshift-cluster-maintenancesettings-check	Diese Regel stellt sicher, dass Amazon-Redshift-Cluster die bevorzugten Einstellungen für Ihre Organisation haben. Insbesondere sorgt sie dafür, dass Cluster bevorzugte Wartungsfenster und automatisierte Aufbewahrungsfristen für Snapshots für die Datenbank haben. Für diese Regel müssen Sie die allowVersionUpgrade festlegen. Der Standardwert ist „true“. Außerdem können Sie optional den Zeitraum preferredMaintenanceWindow (der Standardwert ist sa: 16:00 -sa: 16:30) und den automated SnapshotRetention Zeitraum (der Standardwert ist 1) festlegen. Die tatsächlichen Werte müssen den Richtlini

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			en Ihrer Organisation entsprechen.
7,5	Durchführen eines automatisierten Schwachstellenscans interner Unternehmensressourcen	ecr-private-image-scanning-aktiviert	Der Amazon Elastic Container Repository (ECR)-Image-Scan unterstützt die Identifizierung von Software-Schwachstellen in Ihren Container-Images. Durch die Aktivierung von Image-Scans in ECR-Repositorys werden die Integrität und Sicherheit der gespeicherten Images mit einer zusätzlichen Überprüfungsebene verbessert.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
8.1	Einrichtung und Pflege eines Prozesses zur Verwaltung von Prüfprotokollen	audit-log-policy-exists (Prozessprüfung)	Richten Sie eine Richtlinie zur Verwaltung von Prüfprotokollen ein, in der die Protokoll ierungsanforderung en Ihres Unternehm ens definiert sind, und pflegen Sie diese Richtlinie. Dies beinhaltet, ist aber nicht beschränkt auf die Überprüfung und Aufbewahrung von Prüfprotokollen.
8.2	Erfassung von Prüfprotokollen	api-gw-execution-l ogging-aktiviert	Die API-Gateway-Protokollierung zeigt detaillierte Ansichten der Benutzer, die auf die API zugegriff en haben, und wie diese Benutzer auf die API zugegriff en haben. Diese Einblicke ermöglichen die Transparenz von Benutzeraktivitäten.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
8.2	Erfassung von Prüfprotokollen	multi-region-cloudtrail-enabled	AWS CloudTrail zeichnet Aktionen und API-Aufrufe der AWS Management Console auf. Sie können feststellen, welche Benutzer und Konten angerufen wurden AWS, von welcher Quell-IP-Adresse aus die Anrufe getätigt wurden und wann die Anrufe erfolgten. CloudTrail übermittelt Protokolldateien aus allen AWS Regionen an Ihren S3-Bucket , wenn MULTI_REG ION_CLOUD _TRAIL_ENABLED aktiviert ist. Außerdem wird beim AWS Start einer neuen Region derselbe Trail in der neuen Region erstellt. CloudTrail Dadurch erhalten Sie automatis ch Protokolldateien mit API-Aktivitäten für die neue Region.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
8.2	Erfassung von Prüfprotokollen	cloudtrail-s3-data events-enabled	Die Erfassung von Simple Storage Service (Amazon S3)-Datenereignissen unterstützt die Erkennung von ungewöhnlichen Aktivitäten. Zu den Details gehören Informationen zu dem AWS -Konto, das auf einen Amazon-S3-Bucket zugegriffen hat, die IP-Adresse und die Uhrzeit des Ereignisses.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
8.2	Erfassung von Prüfprotokollen	cloudtrail-enabled	AWS CloudTrail kann bei der Nichtabstreitbarkeit helfen, indem Aktionen und API-Aufrufe der AWS Management Console aufgezeichnet werden. Sie können die Benutzer und die Benutzer AWS-Konten , die einen AWS Dienst aufgerufen haben, die Quell-IP-Adresse, über die die Aufrufe generiert wurden, und den Zeitpunkt der Anrufe identifizieren. Einzelheiten zu den erfassten Daten finden Sie unter Inhalt des AWS CloudTrail Datensatzes.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
8.2	Erfassung von Prüfprotokollen	cloud-trail-cloud-watch-logs-aktiviert	Verwenden Sie Amazon CloudWatch , um Protokoll ereignisaktivitäten zentral zu sammeln und zu verwalten. Die Aufnahme von AWS CloudTrail Daten liefert Einzelheiten zu den API-Aufrufaktivitäten in Ihrem AWS-Konto.
8.2	Erfassung von Prüfprotokollen	elasticsearch-logs-to-cloudwatch	Stellen Sie sicher, dass für Amazon OpenSearch Service-Domains Fehlerprotokolle aktiviert und zur Aufbewahrung und Beantwortung an Amazon CloudWatch Logs gestreamt werden. Domain-Fehlerprotokolle sind bei Sicherheits- und Zugriffsprüfungen sowie bei der Diagnose von Verfügbarkeitsproblemen nützlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
8.2	Erfassung von Prüfprotokollen	vpc-flow-logs-enabled	VPC-Flow-Protokolle erfassen detaillierte Informationsdatensätze über den IP-Datenverkehr, der zu und von Netzwerkschnittstellen in Ihrer Amazon Virtual Private Cloud (Amazon VPC) fließt. Standardmäßig enthalten Flow-Protokolldatensätze Werte für die verschiedenen Komponenten des IP-Flows, einschließlich Quelle, Ziel und Protokoll.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
8.2	Erfassung von Prüfprotokollen	elb-logging-enabled	Die Elastic-Load-Balancing-Aktivität ist ein zentraler Kommunikationspunkt innerhalb einer Umgebung. Stellen Sie sicher, dass die ELB-Protokollierung aktiviert ist. Die gesammelten Daten enthalten detaillierte Informationen zu Anfragen, die an den ELB gesendet wurden. Jedes Protokoll enthält Informationen wie die Zeit, zu der die Anforderung einging, die Client-IP-Adresse, Latenzen, Anforderungspfade und Serverantworten.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
8.2	Erfassung von Prüfprotokollen	rds-logging-enabled	Um die Protokollierung und Überwachung in Ihrer Umgebung zu erleichtern, stellen Sie sicher, dass die Amazon Relational Database Service (Amazon RDS)-Protokollierung aktiviert ist. Mit der Amazon-RDS-Protokollierung können Sie Ereignisse wie Verbindungen, Verbindungsabbrüche, Abfragen oder abgefragte Tabellen erfassen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
8.2	Erfassung von Prüfprotokollen	s-3 bucket-logging-enabled	Die Amazon Simple Storage Service (Amazon S3)-Serverzugriffs protokollierung bietet eine Methode zur Überwachu ng des Netzwerks im Hinblick auf potenzielle Cybersich erheitsereignisse. Die Ereignisse werden überwacht, indem detaillierte Aufzeichn ungen über die Anfragen erfasst werden, die an einen Amazon-S3-Bucket gestellt wurden. Jeder Zugriffsprotokolle intrag enthält Details zu einer einzelnen Zugriffsanfrage. Zu den Details gehören Anforderer, Bucket-Name, Anforderu ngszeit, Anforderu ngsaktion, Antwortst atus und Fehlercode, falls relevant.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
8,2	Erfassung von Prüfprotokollen	redshift-cluster-configuration-check	Um Daten im Ruhezustand zu schützen, muss die Verschlüsselung für Ihre Amazon-Redshift-Cluster aktiviert sein. Sie müssen auch sicherstellen, dass die erforderlichen Konfigurationen auf Amazon-Redshift-Clustern bereitgestellt werden. Die Prüfungsprotokollierung muss aktiviert sein, um Informationen zu Verbindungen und Benutzeraktivitäten in der Datenbank bereitzustellen. Diese Regel erfordert, dass ein Wert für clusterDbEncrypted (Config Default: TRUE) und LoggingEnabled (Config Default: TRUE) gesetzt ist. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
8.2	Erfassung von Prüfprotokollen	wafv2-logging-enabled	Um die Protokollierung und Überwachung in Ihrer Umgebung zu erleichtern, aktivieren Sie die AWS WAF (V2) -Protokollierung im regionalen und globalen Web ACLs. AWS Die WAF-Protokollierung bietet detaillierte Informationen über den Datenverkehr, der von Ihrer Web-ACL analysiert wird. In den Protokollen werden die Uhrzeit aufgezeichnet, zu der die AWS WAF die Anfrage von Ihrer AWS Ressource erhalten hat, Informationen über die Anfrage und eine Aktion für die Regel, der jede Anfrage entsprach.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
8.2	Erfassung von Prüfprotokollen	codebuild-project-logging-enabled	Stellen Sie sicher, dass die AWS CodeBuild Projektprotokollierung aktiviert ist, damit Ihre Build-Ausgabeprotokolle entweder an Amazon CloudWatch oder Amazon Simple Storage Service (Amazon S3) gesendet werden. Build-Ausgabeprotokolle enthalten detaillierte Informationen zu Ihrem Build-Projekt.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
8.3	Gewährleisten einer angemessene Speicherung der Prüfprotokolle	s-3 version-lifecycle-policy-check	Mit Amazon-S3-Lebenszyklusregeln können Sie Aktionen definieren, die Amazon S3 während der Lebensdauer eines Objekts ausführen soll (z. B. die Überführung von Objekten in eine andere Speicherklasse, ihre Archivierung oder Löschung nach einem bestimmten Zeitraum).
8,5	Erfassung detaillierter Prüfprotokolle	api-gw-execution-logging-aktiviert	Die API-Gateway-Protokollierung zeigt detaillierte Ansichten der Benutzer, die auf die API zugegriffen haben, und wie diese Benutzer auf die API zugegriffen haben. Diese Einblicke ermöglichen die Transparenz von Benutzeraktivitäten.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
8.5	Erfassung detaillierter Prüfprotokolle	multi-region-cloudtrail-enabled	AWS CloudTrail zeichnet Aktionen und API-Aufrufe der AWS Management Console auf. Sie können feststellen, welche Benutzer und Konten angerufen wurden AWS, von welcher Quell-IP-Adresse aus die Anrufe getätigt wurden und wann die Anrufe erfolgten. CloudTrail übermittelt Protokolldateien aus allen AWS Regionen an Ihren S3-Bucket , wenn MULTI_REG ION_CLOUD _TRAIL_ENABLED aktiviert ist. Außerdem wird beim AWS Start einer neuen Region derselbe Trail in der neuen Region erstellt. CloudTrail Dadurch erhalten Sie automatis ch Protokolldateien mit API-Aktivitäten für die neue Region.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
8.5	Erfassung detaillierter Prüfprotokolle	cloudtrail-s3-data events-enabled	Die Erfassung von Simple Storage Service (Amazon S3)-Datenereignissen unterstützt die Erkennung von ungewöhnlichen Aktivitäten. Zu den Details gehören Informationen zu dem AWS -Konto, das auf einen Amazon-S3-Bucket zugegriffen hat, die IP-Adresse und die Uhrzeit des Ereignisses.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
8,5	Erfassung detaillierter Prüfprotokolle	cloudtrail-enabled	AWS CloudTrail kann bei der Nichtabst reitbarkeit helfen, indem Aktionen und API-Aufrufe der AWS Management Console aufgezeic hnet werden. Sie können die Benutzer und die Benutzer AWS-Konten , die einen AWS Dienst aufgerufen haben, die Quell-IP-Adresse, über die die Aufrufe generiert wurden, und den Zeitpunkt der Anrufe identifiz ieren. Einzelheiten zu den erfassten Daten finden Sie unter Inhalt des AWS CloudTrail Datensatzes.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
8.5	Erfassung detaillierter Prüfprotokolle	cloud-trail-cloud-watch-logs-aktiviert	Verwenden Sie Amazon CloudWatch , um Protokoll ereignisaktivitäten zentral zu sammeln und zu verwalten. Die Aufnahme von AWS CloudTrail Daten liefert Einzelheiten zu den API-Aufrufaktivitäten in Ihrem AWS-Konto.
8.5	Erfassung detaillierter Prüfprotokolle	elasticsearch-logs-to-cloudwatch	Stellen Sie sicher, dass für Amazon OpenSearch Service-Domains Fehlerprotokolle aktiviert und zur Aufbewahrung und Beantwortung an Amazon CloudWatch Logs gestreamt werden. Domain-Fehlerprotokolle sind bei Sicherheits- und Zugriffsprüfungen sowie bei der Diagnose von Verfügbarkeitsproblemen nützlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
8.5	Erfassung detaillierter Prüfprotokolle	vpc-flow-logs-enabled	VPC-Flow-Protokolle erfassen detaillierte Informationsdatensätze über den IP-Datenverkehr, der zu und von Netzwerkschnittstellen in Ihrer Amazon Virtual Private Cloud (Amazon VPC) fließt. Standardmäßig enthalten Flow-Protokolldatensätze Werte für die verschiedenen Komponenten des IP-Flows, einschließlich Quelle, Ziel und Protokoll.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
8,5	Erfassung detaillierter Prüfprotokolle	elb-logging-enabled	Die Elastic-Load-Balancing-Aktivität ist ein zentraler Kommunikationspunkt innerhalb einer Umgebung. Stellen Sie sicher, dass die ELB-Protokollierung aktiviert ist. Die gesammelten Daten enthalten detaillierte Informationen zu Anfragen, die an den ELB gesendet wurden. Jedes Protokoll enthält Informationen wie die Zeit, zu der die Anforderung einging, die Client-IP-Adresse, Latenzen, Anforderungspfade und Serverantworten.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
8,5	Erfassung detaillierter Prüfprotokolle	rds-logging-enabled	Um die Protokollierung und Überwachung in Ihrer Umgebung zu erleichtern, stellen Sie sicher, dass die Amazon Relational Database Service (Amazon RDS)-Protokollierung aktiviert ist. Mit der Amazon-RDS-Protokollierung können Sie Ereignisse wie Verbindungen, Verbindungsabbrüche, Abfragen oder abgefragte Tabellen erfassen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
8,5	Erfassung detaillierter Prüfprotokolle	s-3 bucket-logging-enabled	Die Amazon Simple Storage Service (Amazon S3)-Serverzugriffs protokollierung bietet eine Methode zur Überwachu ng des Netzwerks im Hinblick auf potenzielle Cybersich erheitsereignisse. Die Ereignisse werden überwacht, indem detaillierte Aufzeichn ungen über die Anfragen erfasst werden, die an einen Amazon-S3-Bucket gestellt wurden. Jeder Zugriffsprotokolle intrag enthält Details zu einer einzelnen Zugriffsanfrage. Zu den Details gehören Anforderer, Bucket-Name, Anforderu ngszeit, Anforderu ngsaktion, Antwortst atus und Fehlercode, falls relevant.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
8,5	Erfassung detaillierter Prüfprotokolle	redshift-cluster-configuration-check	Um Daten im Ruhezustand zu schützen, muss die Verschlüsselung für Ihre Amazon-Redshift-Cluster aktiviert sein. Sie müssen auch sicherstellen, dass die erforderlichen Konfigurationen auf Amazon-Redshift-Clustern bereitgestellt werden. Die Prüfungsprotokollierung muss aktiviert sein, um Informationen zu Verbindungen und Benutzeraktivitäten in der Datenbank bereitzustellen. Diese Regel erfordert, dass ein Wert für clusterDbEncrypted (Config Default: TRUE) und LoggingEnabled (Config Default: TRUE) gesetzt ist. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
8.5	Erfassung detaillierter Prüfprotokolle	wafv2-logging-enabled	Um die Protokollierung und Überwachung in Ihrer Umgebung zu erleichtern, aktivieren Sie die AWS WAF (V2) -Protokollierung im regionalen und globalen Web ACLs. AWS Die WAF-Protokollierung bietet detaillierte Informationen über den Datenverkehr, der von Ihrer Web-ACL analysiert wird. In den Protokollen werden die Uhrzeit aufgezeichnet, zu der die AWS WAF die Anfrage von Ihrer AWS Ressource erhalten hat, Informationen über die Anfrage und eine Aktion für die Regel, der jede Anfrage entsprach.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
8.5	Erfassung detaillierter Prüfprotokolle	guardduty-enabled-centralized	Amazon GuardDuty kann mithilfe von Threat Intellige nce Feeds helfen, potenzielle Cybersich erheitsereignisse zu überwachen und zu erkennen. Dazu gehören Listen mit bösartigen IPs und maschinel len Lernmethoden zur Identifizierung unerwarteter, nicht autorisierter und bösartiger Aktivitäten in Ihrer AWS Cloud-Umgebung.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
8.5	Erfassung detaillierter Prüfprotokolle	codebuild-project-logging-enabled	Stellen Sie sicher, dass die AWS CodeBuild Projektprotokollierung aktiviert ist, damit Ihre Build-Ausgabeprotokolle entweder an Amazon CloudWatch oder Amazon Simple Storage Service (Amazon S3) gesendet werden. Build-Ausgabeprotokolle enthalten detaillierte Informationen zu Ihrem Build-Projekt.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
8.7	Erfassung von Prüfprotokollen für URL-Anforderungen	elb-logging-enabled	Die Elastic-Load-Balancing-Aktivität ist ein zentraler Kommunikationspunkt innerhalb einer Umgebung. Stellen Sie sicher, dass die ELB-Protokollierung aktiviert ist. Die gesammelten Daten enthalten detaillierte Informationen zu Anfragen, die an den ELB gesendet wurden. Jedes Protokoll enthält Informationen wie die Zeit, zu der die Anforderung einging, die Client-IP-Adresse, Latenzen, Anforderungspfade und Serverantworten.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
8,9	Zentralisierung von Prüfprotokollen	cloud-trail-cloud-watch-logs-aktiviert	Verwenden Sie Amazon CloudWatch , um Protokoll ereignisaktivitäten zentral zu sammeln und zu verwalten. Die Aufnahme von AWS CloudTrail Daten liefert Einzelheiten zu den API-Aufrufaktivitäten in Ihrem AWS-Konto.
8.10	Aufbewahrung von Prüfprotokollen	s-3 version-lifecycle-policy-check	Mit Amazon-S3-Lebenszyklusregeln können Sie Aktionen definieren, die Amazon S3 während der Lebensdauer eines Objekts ausführen soll (z. B. die Überführung von Objekten in eine andere Speicherklasse, ihre Archivierung oder Löschung nach einem bestimmten Zeitraum).

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
8,10	Aufbewahrung von Prüfprotokollen	cw-loggroup-retention-period-überprüfen	Stellen Sie sicher, dass die Ereignisprotokolldaten für Ihre Protokollgruppen über eine Mindestdauer aufbewahrt werden, um die Fehlerbehebung und forensische Untersuchungen zu unterstützen. Fehlende frühere Ereignisprotokolldaten erschweren die Rekonstruierung und Identifizierung potenziell schädlicher Ereignisse.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.1	Bereitstellung und Wartung von Anti-Malware-Software	guardduty-enabled-centralized	Amazon GuardDuty kann mithilfe von Threat Intellige nce Feeds helfen, potenzielle Cybersich erheitsereignisse zu überwachen und zu erkennen. Dazu gehören Listen mit bösartigen IPs und maschinel len Lernmethoden zur Identifizierung unerwarteter, nicht autorisierter und bösartiger Aktivitäten in Ihrer AWS Cloud-Umgebung.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.2	Konfigurierung automatischer Anti-Malware-Signatur-Updates	guardduty-enabled-centralized	Amazon GuardDuty kann mithilfe von Threat Intellige nce Feeds helfen, potenzielle Cybersich erheitsereignisse zu überwachen und zu erkennen. Dazu gehören Listen mit bösartigen IPs und maschinel len Lernmethoden zur Identifizierung unerwarteter, nicht autorisierter und bösartiger Aktivitäten in Ihrer AWS Cloud-Umgebung.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.4	Konfigurierung automatischer Anti-Malware-Scans von Wechselmedien	guardduty-enabled-centralized	Amazon GuardDuty kann mithilfe von Threat Intellige nce Feeds helfen, potenzielle Cybersich erheitsereignisse zu überwachen und zu erkennen. Dazu gehören Listen mit bösartigen IPs und maschinel len Lernmethoden zur Identifizierung unerwarteter, nicht autorisierter und bösartiger Aktivitäten in Ihrer AWS Cloud-Umgebung.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.6	Zentrale Verwaltun g von Anti-Malware-Software	guardduty-enabled-centralized	Amazon GuardDuty kann mithilfe von Threat Intellige nce Feeds helfen, potenzielle Cybersich erheitsereignisse zu überwachen und zu erkennen. Dazu gehören Listen mit bösartigen IPs und maschinel len Lernmethoden zur Identifizierung unerwarteter, nicht autorisierter und bösartiger Aktivitäten in Ihrer AWS Cloud-Umgebung.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.7	Verwendung von verhaltensbasierter Anti-Malware-Software	guardduty-enabled-centralized	Amazon GuardDuty kann mithilfe von Threat Intelligence Feeds helfen, potenzielle Cybersicherheitsereignisse zu überwachen und zu erkennen. Dazu gehören Listen mit bösartigen IPs und maschinellen Lernmethoden zur Identifizierung unerwarteter, nicht autorisierter und bösartiger Aktivitäten in Ihrer AWS Cloud-Umgebung.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
11.2	Durchführen automatisierter Backups	dynamodb-in-backup-plan	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon DynamoDB-Tabellen Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
11.2	Durchführen automatisierter Backups	ebs-in-backup-plan	Stellen Sie zur Unterstützung der Datensicherungspro zesse sicher, dass Ihre Amazon Elastic Block Store (Amazon EBS) -Volumes Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwaltet er Backup-Service mit einer richtlini enbasierten Backup-Lösung. Diese Lösung vereinfacht Ihre Backup-Verwaltung und ermöglicht es Ihnen, Ihre geschäftl ichen und behördlic hen Anforderungen bezüglich Backups zu erfüllen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
11.2	Durchführen automatisierter Backups	ebs-optimized-instance	Eine optimierte Instance im Amazon Elastic Block Store (Amazon EBS) bietet zusätzliche, dedizierte Kapazität für Amazon-EBS-I/O-Vorgänge. Diese Optimierung bietet die beste Leistung für Ihr EBS-Volume, indem Konflikte zwischen Amazon-EBS-I/O und anderem Datenverkehr von Ihrer Instance minimiert werden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
11.2	Durchführen automatisierter Backups	dynamodb-pitr-enabled	Aktivieren Sie diese Regel, um zu überprüfen, ob die Informationen gesichert wurden. Es verwaltet auch die Backups, indem es sicherstellt, dass die point-in-time Wiederherstellung in Amazon DynamoDB aktiviert ist. Bei der Wiederherstellung werden fortlaufende Backups Ihrer Tabelle für die letzten 35 Tage gespeichert.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
11.2	Durchführen automatisierter Backups	elasticache-redis-cluster-automatic-Backup-Prüfung	Wenn automatische Backups aktiviert sind, ElastiCache erstellt Amazon täglich ein Backup des Clusters. Die Sicherung kann für eine von Ihrer Organisation festgelegte Anzahl von Tagen aufbewahrt werden. Automatische Backups schützen vor Datenverlust. Bei einem Ausfall können Sie einen neuen Cluster erstellen, der Ihre Daten aus dem aktuellen Backup wiederherstellt.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
11.2	Durchführen automatisierter Backups	efs-in-backup-plan	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon Elastic File System (Amazon EFS) -Dateisysteme Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
11.2	Durchführen automatisierter Backups	db-instance-backup-enabled	Die Sicherungsfunktion von Amazon RDS erstellt Sicherungen Ihrer Datenbanken und Transaktionsprotokolle. Amazon RDS erstellt einen Snapshot für das Speichervolume Ihrer DB-Instance, sodass die gesamte DB-Instance gesichert wird. Sie können im System spezifische Aufbewahrungsfristen festlegen, um Ihre Ausfallsicherheitsanforderungen zu erfüllen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
11.2	Durchführen automatisierter Backups	redshift-backup-enabled	Stellen Sie zur Unterstützung der Datensicherungsprozesse sicher, dass Ihre Amazon-Redshift-Cluster über automatisierte Snapshots verfügen. Wenn automatisierte Snapshots für einen Cluster aktiviert sind, erstellt Redshift in regelmäßigen Abständen Snapshots dieses Clusters. Standardmäßig erstellt Redshift alle acht Stunden oder alle 5 GB einen Snapshot für jeden Knoten mit Datenänderungen oder je nachdem, was zuerst eintritt.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
11.2	Durchführen automatisierter Backups	s3- bucket-versioning-enabled	Die Versionsv erwaltung von Amazon Simple Storage Service (Amazon S3)-Bucke ts hilft dabei, mehrere Varianten eines Objekts im selben Amazon-S3-Bucket zu speichern. Verwenden Sie die Versionsv erwaltung, um sämtliche Versionen aller Objekte in Ihrem Amazon-S3-Bucket zu speichern , abzurufen oder wiederherzustellen . Mit der Versionsv erwaltung können Sie Versionen sowohl nach unbeabsic htigten Benutzera ktionen als auch nach Anwendungsfehlern problemlos wiederher stellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
11.2	Durchführen automatisierter Backups	redshift-cluster-maintenancesettings-check	Diese Regel stellt sicher, dass Amazon-Redshift-Cluster die bevorzugten Einstellungen für Ihre Organisation haben. Insbesondere sorgt sie dafür, dass Cluster bevorzugte Wartungsfenster und automatisierte Aufbewahrungsfristen für Snapshots für die Datenbank haben. Für diese Regel müssen Sie die festlegen allowVersionUpgrade. Der Standardwert ist „true“. Außerdem können Sie optional den Zeitraum preferredMaintenanceWindow (der Standardwert ist sa: 16:00 -sa: 16:30) und den automated SnapshotRetention Zeitraum (der Standardwert ist 1) festlegen. Die tatsächlichen Werte müssen den Richtlini

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			en Ihrer Organisation entsprechen.
11.2	Durchführen automatisierter Backups	s3- bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) unterstützt die Aufrechterhaltung einer angemesse nen Kapazität und Verfügbarkeit. CRR ermöglicht das automatische, asynchrone Kopieren von Objekten in Amazon-S3-Buckets, um die Datenverf ügbarkeit sicherzus tellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
11.2	Durchführen automatisierter Backups	s-3 version-lifecycle-policy-check	Mit Amazon-S3-Lebenszyklusregeln können Sie Aktionen definieren, die Amazon S3 während der Lebensdau er eines Objekts ausführen soll (z. B. die Überführu ng von Objekten in eine andere Speicherklasse, ihre Archivierung oder Löschung nach einem bestimmten Zeitraum) .
11,3	Schutz von Wiederher stellungsdaten	backup-recovery-point-encrypted	Stellen Sie sicher, dass die Verschlüs selung für Ihre AWS Backup-Wiederherst ellungspunkte aktiviert ist. Da sensible Daten auch im Ruhezusta nd vorhanden sein können, sollten Sie die Verschlüsselung im Ruhezustand aktivieren, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
11.3	Schutz von Wiederherstellungsdaten	encrypted-volumes	Aktivieren Sie die Verschlüsselung für Ihre Amazon-Elastic-Block-Store (Amazon-EBS)-Volumes, um eventuell vorhandene sensible Daten sowie Daten im Ruhezustand zu schützen.
11,3	Schutz von Wiederherstellungsdaten	ec-2 ebs-encryption-by-default	Zum Schutz von Daten im Ruhezustand müssen Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon Elastic Block Store (Amazon EBS)-Volumes aktiviert ist. Da sensible Daten auch im Ruhezustand vorhanden sein können, sollten Sie die Verschlüsselung im Ruhezustand aktivieren, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
11,3	Schutz von Wiederherstellungsdaten	rds-storage-encrypted	Zum Schutz von Daten im Ruhezustand müssen Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon Relational Database Service (Amazon RDS)-Instances aktiviert ist. Um eventuell vorhandene sensible Daten im Ruhezustand in Amazon-RDS-Instances zu schützen, muss die Verschlüsselung von Daten im Ruhezustand aktiviert sein.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
11.4	Einrichtung und Verwaltung einer isolierten Instance für Wiederherstellungs daten	dynamodb-in-backup-plan	Um Sie bei Datensich erungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon DynamoDB-Tabellen Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwaltet er Backup-Service mit einer richtlini enbasierten Backup-Lösung. Diese Lösung vereinfacht Ihre Backup-Verwaltung und ermöglicht es Ihnen, Ihre geschäftl ichen und behördlic hen Anforderungen bezüglich Backups zu erfüllen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
11.4	Einrichtung und Verwaltung einer isolierten Instance für Wiederherstellungs daten	ebs-in-backup-plan	Stellen Sie zur Unterstützung der Datensicherungspro zesse sicher, dass Ihre Amazon Elastic Block Store (Amazon EBS) -Volumes Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwaltet er Backup-Service mit einer richtlini enbasierten Backup-Lösung. Diese Lösung vereinfacht Ihre Backup-Verwaltung und ermöglicht es Ihnen, Ihre geschäftl ichen und behördlic hen Anforderungen bezüglich Backups zu erfüllen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
11.4	Einrichtung und Verwaltung einer isolierten Instance für Wiederherstellungs daten	ebs-optimized-instance	Eine optimierte Instance im Amazon Elastic Block Store (Amazon EBS) bietet zusätzliche, dedizierte Kapazität für Amazon-EBS-I/O-Vorgänge. Diese Optimierung bietet die beste Leistung für Ihr EBS-Volume, indem Konflikte zwischen Amazon-EBS-I/O und anderem Datenverk ehr von Ihrer Instance minimiert werden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
11.4	Einrichtung und Verwaltung einer isolierten Instance für Wiederherstellungs daten	dynamodb-pitr-enabled	Aktivieren Sie diese Regel, um zu überprüfen, ob die Informationen gesichert wurden. Es verwaltet auch die Backups, indem es sicherstellt, dass die point-in-time Wiederherstellung in Amazon DynamoDB aktiviert ist. Bei der Wiederherstellung werden fortlaufende Backups Ihrer Tabelle für die letzten 35 Tage gespeichert.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
11.4	Einrichtung und Verwaltung einer isolierten Instance für Wiederherstellungs daten	elasticache-redis-cluster-automatic-Backup-Prüfung	Wenn automatische Backups aktiviert sind, ElastiCache erstellt Amazon täglich ein Backup des Clusters. Die Sicherung kann für eine von Ihrer Organisation festgelegte Anzahl von Tagen aufbewahrt werden. Automatische Backups schützen vor Datenverlust. Bei einem Ausfall können Sie einen neuen Cluster erstellen, der Ihre Daten aus dem aktuellen Backup wiederherstellt.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
11.4	Einrichtung und Verwaltung einer isolierten Instance für Wiederherstellungs daten	efs-in-backup-plan	Um Sie bei Datensich erungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon Elastic File System (Amazon EFS) -Dateisysteme Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwaltet er Backup-Service mit einer richtlini enbasierten Backup-Lösung. Diese Lösung vereinfacht Ihre Backup-Verwaltung und ermöglicht es Ihnen, Ihre geschäftl ichen und behördlic hen Anforderungen bezüglich Backups zu erfüllen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
11.4	Einrichtung und Verwaltung einer isolierten Instance für Wiederherstellungs daten	db-instance-backup-enabled	Die Sicherung sfunktion von Amazon RDS erstellt Sicherung en Ihrer Datenbank en und Transakti onsprotokolle. Amazon RDS erstellt einen Snapshot für das Speichervolume Ihrer DB-Instance, sodass die gesamte DB-Instance gesichert wird. Sie können im System spezifische Aufbewahrungsfrist en festlegen, um Ihre Ausfallsicherheits anforderungen zu erfüllen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
11.4	Einrichtung und Verwaltung einer isolierten Instance für Wiederherstellungs daten	redshift-backup-enabled	Stellen Sie zur Unterstützung der Datensicherungspro zesse sicher, dass Ihre Amazon-Re dshift-Cluster über automatisierte Snapshots verfügen. Wenn automatis ierte Snapshots für einen Cluster aktiviert sind, erstellt Redshift in regelmäßi gen Abständen Snapshots dieses Clusters. Standardm äßig erstellt Redshift alle acht Stunden oder alle 5 GB einen Snapshot für jeden Knoten mit Datenände rungen oder je nachdem, was zuerst eintritt.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
11.4	Einrichtung und Verwaltung einer isolierten Instance für Wiederherstellungs daten	s3- bucket-versioning-enabled	Die Versionsv erwaltung von Amazon Simple Storage Service (Amazon S3)-Bucke ts hilft dabei, mehrere Varianten eines Objekts im selben Amazon-S3-Bucket zu speichern. Verwenden Sie die Versionsv erwaltung, um sämtliche Versionen aller Objekte in Ihrem Amazon-S3-Bucket zu speichern , abzurufen oder wiederherzustellen . Mit der Versionsv erwaltung können Sie Versionen sowohl nach unbeabsic htigten Benutzera ktionen als auch nach Anwendungsfehlern problemlos wiederher stellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
11.4	Einrichtung und Verwaltung einer isolierten Instance für Wiederherstellungs daten	redshift-cluster-maintenancesettings-check	Diese Regel stellt sicher, dass Amazon-Redshift-Cluster die bevorzugten Einstellungen für Ihre Organisation haben. Insbesondere sorgt sie dafür, dass Cluster bevorzugte Wartungsfenster und automatisierte Aufbewahrungsfristen für Snapshots für die Datenbank haben. Für diese Regel müssen Sie die festlegen allowVersionUpgrade. Der Standardwert ist „true“. Außerdem können Sie optional den Zeitraum preferredMaintenanceWindow (der Standardwert ist sa: 16:00 -sa: 16:30) und den automated SnapshotRetention Zeitraum (der Standardwert ist 1) festlegen. Die tatsächlichen Werte müssen den Richtlini

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			en Ihrer Organisation entsprechen.
11.4	Einrichtung und Verwaltung einer isolierten Instance für Wiederherstellungs daten	s3- bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) unterstützt die Aufrechterhaltung einer angemesse nen Kapazität und Verfügbarkeit. CRR ermöglicht das automatische, asynchrone Kopieren von Objekten in Amazon-S3-Buckets, um die Datenverf ügbarkeit sicherzus tellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
11.4	Einrichtung und Verwaltung einer isolierten Instance für Wiederherstellungs daten	s-3 version-lifecycle-policy-check	Mit Amazon-S3-Lebenszyklusregeln können Sie Aktionen definieren, die Amazon S3 während der Lebensdau er eines Objekts ausführen soll (z. B. die Überführu ng von Objekten in eine andere Speicherklasse, ihre Archivierung oder Löschung nach einem bestimmten Zeitraum) .

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
12.2	Einrichtung und Pflege einer sicheren Netzwerkarchitektur	acm-certificate-expiration-check	Stellen Sie sicher, dass die Netzwerkintegrität geschützt ist, indem Sie sicherstellen, dass X509-Zertifikate von AWS ACM ausgestellt werden. Diese Zertifikate müssen gültig und dürfen nicht abgelaufen sein. Für diese Regel ist ein Wert für erforderlich daysToExpiration (Wert für bewährte AWS Grundregeln für Sicherheit: 90). Der tatsächliche Wert muss den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
12.2	Einrichtung und Pflege einer sicheren Netzwerkarchitektur	dms-replication-not-public	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass auf DMS-Replikationsin stanzen nicht öffentlic h zugegriffen werden kann. DMS-Repli kations-Instances können vertrauli che Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.
12.2	Einrichtung und Pflege einer sicheren Netzwerkarchitektur	ebs-snapshot-public-restorable-überprüfen	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass EBS-Snapshots nicht öffentlich wiederher stellbar sind. EBS-Volume-Snapsho ts können vertrauli che Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
12.2	Einrichtung und Pflege einer sicheren Netzwerkarchitektur	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) Security Groups können bei der Verwaltung des Netzwerkzugriffs helfen, indem sie eine statusbeh aftete Filterung von eingehendem und ausgehendem Netzwerkverkehr zu Ressourcen bereitste llen. AWS Wenn Sie eingehenden (oder entfernten) Datenverk ehr von 0.0.0.0/0 bis Port 22 auf Ihren Ressourcen nicht zulassen, können Sie den Remote-Zugriff einschränken.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
12.2	Einrichtung und Pflege einer sicheren Netzwerkarchitektur	vpc-default-security-group-geschlossen	Sicherheitsgruppen von Amazon Elastic Compute Cloud (Amazon EC2) können bei der Verwaltung des Netzwerkzugriffs helfen, indem sie eine statusbehaftete Filterung des ein- und ausgehenden Netzwerkverkehrs zu Ressourcen bereitstellen. AWS Die Beschränk ung des gesamten Datenverkehrs auf die Standardsicherheit sgruppe hilft dabei, den Fernzugriff auf Ihre Ressourcen einzuschränken. AWS

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
12.2	Einrichtung und Pflege einer sicheren Netzwerkarchitektur	ec2- instance-no-public-ip	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon Elastic Compute Cloud (Amazon EC2) - Instances nicht öffentlich zugänglic h sind. EC2Amazon -Instances können vertrauliche Informati onen enthalten, und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
12.2	Einrichtung und Pflege einer sicheren Netzwerkarchitektur	elasticsearch-in-vpc-only	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass sich Amazon OpenSearch OpenSearch Service (Service) - Domains innerhalb einer Amazon Virtual Private Cloud (Amazon VPC) befinden. Eine OpenSearch Service-Domain innerhalb einer Amazon VPC ermöglicht die sichere Kommunikation zwischen OpenSearch Service und anderen Services innerhalb der Amazon VPC, ohne dass ein Internet-Gateway, ein NAT-Gerät oder eine VPN-Verbindung erforderlich ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
12.2	Einrichtung und Pflege einer sicheren Netzwerkarchitektur	ec2- instances-in-vpc	Stellen Sie Amazon Elastic Compute Cloud (Amazon EC2) -Instances innerhalb einer Amazon Virtual Private Cloud (Amazon VPC) bereit, um eine sichere Kommunika tion zwischen einer Instance und anderen Services innerhalb der Amazon VPC zu ermöglichen, ohne dass ein Internet-Gateway, ein NAT-Gerät oder eine VPN-Verbindung erforderlich ist. Der gesamte Datenverk ehr bleibt sicher in der AWS Cloud. Domains, die sich innerhalb einer VPC befinden, verfügen aufgrund ihrer logischen Isolierun g im Vergleich zu Domains mit öffentlic hen Endpunkten über eine zusätzlic he Sicherheitsebene. Weisen Sie EC2

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			Amazon-Instances einer Amazon-VPC zu, um den Zugriff ordnungsgemäß zu verwalten.
12.2	Einrichtung und Pflege einer sicheren Netzwerkarchitektur	emr-master-no-public-ip	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon EMR-Cluster-Masterknoten nicht öffentlich zugänglich sind. Amazon-EMR-Cluster-Hauptknoten können vertrauliche Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
12.2	Einrichtung und Pflege einer sicheren Netzwerkarchitektur	no-unrestricted-route-to-igw	Stellen Sie sicher, dass EC2 Amazon-Routentabellen keine uneingeschränkten Routen zu einem Internet-Gateway enthalten. Durch das Entfernen oder Beschränken des Internetzugangs für Workloads innerhalb von Amazon VPCs können unbeabsichtigte Zugriffe in Ihrer Umgebung reduziert werden.
12.2	Einrichtung und Pflege einer sicheren Netzwerkarchitektur	lambda-function-public-access-verboten	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass AWS Lambda-Funktionen nicht öffentlich zugänglich sind. Der öffentliche Zugriff kann möglicherweise die Verfügbarkeit von Ressourcen beeinträchtigen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
12.2	Einrichtung und Pflege einer sicheren Netzwerkarchitektur	lambda-inside-vpc	Stellen Sie AWS Lambda-Funktionen in einer Amazon Virtual Private Cloud (Amazon VPC) bereit, um eine sichere Kommunika tion zwischen einer Funktion und anderen Diensten innerhalb der Amazon VPC zu gewährleisten. Bei dieser Konfiguration sind kein Internet-Gateway, kein NAT-Gerät und keine VPN-Verbindung erforderlich. Der gesamte Datenverk ehr bleibt sicher in der Cloud. AWS Domains, die sich innerhalb einer VPC befinden, verfügen aufgrund ihrer logischen Isolierun g im Vergleich zu Domains mit öffentlic hen Endpunkten über eine zusätzliche Sicherheitsebene. Um den Zugriff ordnungsg emäß zu verwalten,

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			sollten AWS Lambda-Funktionen einer VPC zugewiesen werden.
12.2	Einrichtung und Pflege einer sicheren Netzwerkarchitektur	rds-snapshots-public-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Relational Database Service (Amazon RDS) -Instances nicht öffentlich sind. Amazon-RDS-Datenbank-Instances können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
12.2	Einrichtung und Pflege einer sicheren Netzwerkarchitektur	rds-instance-public-access-überprüfen	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Relational Database Service (Amazon RDS) -Instances nicht öffentlich sind. Amazon-RDS-Datenbank-Instances können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
12.2	Einrichtung und Pflege einer sicheren Netzwerkarchitektur	restricted-common-ports	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass gemeinsame Ports für Amazon Elastic Compute Cloud (Amazon EC2) -Sicherheitsgruppen eingeschränkt sind. Wenn der Zugriff auf Ports nicht auf vertrauenswürdige Quellen beschränkt wird, kann dies zu Angriffen auf die Verfügbarkeit, Integrität und Vertraulichkeit von Systemen führen. Mit dieser Regel können Sie optional die Parameter blockedPort1–blockedPort5 festlegen (Standardkonfigurationen: 20, 21, 3389, 3306, 4333). Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
12.2	Einrichtung und Pflege einer sicheren Netzwerkarchitektur	redshift-cluster-public-access-überprüfen	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Redshift Redshift-Cluster nicht öffentlich sind. Amazon-Redshift-Cluster können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
12.2	Einrichtung und Pflege einer sicheren Netzwerkarchitektur	s3- -Block-periodisch account-level-public-access	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Simple Storage Service (Amazon S3) -Buckets nicht öffentlich zugänglich sind. Diese Regel trägt dazu bei, sensible Daten vor unbefugten Remote-Benutzern zu schützen, indem sie den öffentlichen Zugriff verhindert. Mit dieser Regel können Sie optional die Parameter ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) und restrictPublicBuckets Parameter (Config Default: True) festlegen. Die tatsächlichen Werte müssen den Richtlini

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			en Ihrer Organisation entsprechen.
12.2	Einrichtung und Pflege einer sicheren Netzwerkarchitektur	s3- bucket-public-read -prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie nur autorisierten Benutzern, Prozessen und Geräten Zugriff auf Amazon Simple Storage Service (Amazon S3) - Buckets gewähren. Die Verwaltung des Zugriffs sollte mit der Klassifizierung der Daten übereinst immen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
12.2	Einrichtung und Pflege einer sicheren Netzwerkarchitektur	s3- bucket-public-write-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie nur autorisierten Benutzern, Prozessen und Geräten Zugriff auf Amazon Simple Storage Service (Amazon S3) - Buckets gewähren. Die Verwaltung des Zugriffs sollte mit der Klassifizierung der Daten übereinstimmen.
12.2	Einrichtung und Pflege einer sicheren Netzwerkarchitektur	sagemaker-notebook-no-direct-Internetzugang	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass SageMaker Amazon-Notebooks keinen direkten Internetzugang zulassen. Indem Sie direkten Internetzugang blockieren, vermeiden Sie, dass unbefugte Benutzer auf sensible Daten zugreifen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
12.2	Einrichtung und Pflege einer sicheren Netzwerkarchitektur	subnet-auto-assign-public-ip-deaktiviert	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon Virtual Private Cloud (VPC) -Subnetzen nicht automatisch eine öffentliche IP-Adresse zugewiesen wird. Amazon Elastic Compute Cloud (EC2) -Instances, die in Subnetzen gestartet werden, in denen dieses Attribut aktiviert ist, haben ihrer primären Netzwerkschnittstelle eine öffentliche IP-Adresse zugewiesen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
12.2	Einrichtung und Pflege einer sicheren Netzwerkarchitektur	vpc-sg-open-only-to-authorized-ports	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass gemeinsame Ports für Amazon Elastic Compute Cloud (Amazon EC2) -Sicherheitsgruppen eingeschränkt sind. Wenn der Zugriff auf Ports nicht auf vertrauenswürdige Quellen beschränkt wird, kann dies zu Angriffen auf die Verfügbarkeit, Integrität und Vertraulichkeit von Systemen führen. Durch die Beschränkung des Zugriffs auf Ressourcen innerhalb einer Sicherheitsgruppe aus dem Internet (0.0.0.0/0) kann der Remote-Zugriff auf interne Systeme gesteuert werden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
12.2	Einrichtung und Pflege einer sicheren Netzwerkarchitektur	ssm-document-not-public	Stellen Sie sicher, dass AWS Systems Manager (SSM) - Dokumente nicht öffentlich sind, da dies einen unbeabsichtigten Zugriff auf Ihre SSM-Dokumente ermöglichen kann. Ein öffentliches SSM-Dokument kann Informationen über Ihr Konto, Ihre Ressourcen und internen Prozesse preisgeben.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
12.2	Einrichtung und Pflege einer sicheren Netzwerkarchitektur	autoscaling-launch-config-public-ip-deaktiviert	Wenn Sie Ihre Netzwerkschnittstellen mit einer öffentlichen IP-Adresse konfigurieren, sind die diesen Netzwerkschnittstellen zugehörigen Ressourcen über das Internet erreichbar. EC2 Ressourcen sollten nicht öffentlich zugänglich sein, da dies einen unbeabsichtigten Zugriff auf Ihre Anwendungen oder Server ermöglichen kann.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
12.2	Einrichtung und Pflege einer sicheren Netzwerkarchitektur	redshift-enhanced-vpc-routing-aktiviert	Mit Enhanced-VPC-Routing wird erzwungen, dass der gesamte COPY- und UNLOAD-Datenverkehr zwischen Ihrem Cluster und Datenrepositorys über Ihre Amazon VPC erfolgt. Anschließend können Sie VPC-Features wie Sicherheitsgruppen und Netzwerkzugriffskontrolllisten verwenden, um den Netzwerkverkehr zu schützen. Sie können auch VPC-Flow-Protokolle verwenden, um den Netzwerkverkehr zu überwachen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
12.2	Einrichtung und Pflege einer sicheren Netzwerkarchitektur	dynamodb-autoscaling-enabled	Amazon DynamoDB Auto Scaling verwendet den AWS Application Auto Scaling-Service, um die bereitgestellte Durchsatzkapazität so anzupassen, dass sie automatisch auf tatsächliche Verkehrsmuster reagiert. Auf diese Weise kann eine Tabelle oder ein globaler sekundärer Index die bereitgestellte Lese-/Schreibkapazität erhöhen, um plötzliche Erhöhungen des Datenverkehrs ohne Drosselung zu bewältigen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
12.2	Einrichtung und Pflege einer sicheren Netzwerkarchitektur	elb-cross-zone-load-Balancing aktiviert	Aktivieren Sie zonenübergreifendes Load Balancing für Ihre Elastic Load Balancer (ELBs), um eine angemessene Kapazität und Verfügbarkeit aufrechtzuerhalten. Zonenübergreifendes Load Balancing reduziert die Notwendigkeit, die gleiche Anzahl von Instances in jeder aktivierten Availability Zone aufrechtzuerhalten. Es verbessert auch die Fähigkeit Ihrer Anwendung, den Verlust einer oder mehrerer Instances zu bewältigen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
12.2	Einrichtung und Pflege einer sicheren Netzwerkarchitektur	elb-deletion-protection-enabled	Diese Regel sorgt dafür, dass der Löschschutz für Elastic Load Balancing aktiviert ist. Verwenden Sie diese Funktion, um zu verhindern, dass Ihr Load Balancer versehentlich oder böswillig gelöscht wird, was zum Verlust der Verfügbarkeit Ihrer Anwendungen führen kann.
12.2	Einrichtung und Pflege einer sicheren Netzwerkarchitektur	rds-instance-deletion-protection-aktiviert	Stellen Sie sicher, dass Amazon Relational Database Service (Amazon RDS)-Instances den Löschschutz aktiviert haben. Verwenden Sie den Löschschutz, um zu verhindern, dass Ihre Amazon-RDS-Instances versehentlich oder böswillig gelöscht werden, was zum Verlust der Verfügbarkeit Ihrer Anwendungen führen kann.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
12.2	Einrichtung und Pflege einer sicheren Netzwerkarchitektur	rds-multi-az-support	Die Multi-AZ-Unterstützung in Amazon Relational Database Service (Amazon RDS) bietet eine verbesserte Verfügbarkeit und Beständigkeit von Datenbank-Instances. Wenn Sie eine Multi-AZ-Datenbank-Instance bereitstellen, erstellt Amazon RDS automatisch eine primäre Datenbank-Instance und repliziert die Daten synchron auf eine Standby-Instance in einer anderen Availability Zone. Jede Availability Zone läuft auf einer eigenen, physisch getrennten, unabhängigen Infrastruktur und ist auf eine hohe Verfügbarkeit ausgelegt. Im Falle eines Infrastrukturausfalls führt Amazon RDS einen automatis

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			chen Failover zum Standby-Modus durch, sodass Sie den Datenbankbetrieb wieder aufnehmen können, sobald der Failover abgeschlo ssen ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
12.2	Einrichtung und Pflege einer sicheren Netzwerkarchitektur	rds-cluster-multi-az-aktiviert	Die Multi-AZ-Unterstützung in Amazon Relational Database Service (Amazon RDS) bietet eine verbesserte Verfügbarkeit und Beständigkeit von Datenbank-Instances. Wenn Sie eine Multi-AZ-Datenbank-Instance bereitstellen, erstellt Amazon RDS automatisch eine primäre Datenbank-Instance und repliziert die Daten synchron auf eine Standby-Instance in einer anderen Availability Zone. Jede Availability Zone läuft auf einer eigenen, physisch getrennten, unabhängigen Infrastruktur und ist auf eine hohe Verfügbarkeit ausgelegt. Im Falle eines Infrastrukturausfalls führt Amazon RDS einen automatis

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			chen Failover zum Standby-Modus durch, sodass Sie den Datenbankbetrieb wieder aufnehmen können, sobald der Failover abgeschlo ssen ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
12.2	Einrichtung und Pflege einer sicheren Netzwerkarchitektur	vpc-vpn-2-tunnels-up	Redundante Site-to-Site VPN-Tunnel können implementiert werden, um die Anforderungen an die Ausfallsicherheit zu erfüllen. Es verwendet zwei Tunnel, um die Konnektivität sicherzustellen, falls eine der Site-to-Site VPN-Verbindungen nicht verfügbar ist. Um sich vor einem Verbindungsverlust zu schützen, können Sie für den Fall, dass Ihr Kunden-Gateway nicht verfügbar ist, eine zweite Site-to-Site VPN-Verbindung zu Ihrer Amazon Virtual Private Cloud (Amazon VPC) und Ihrem Virtual Private Gateway einrichten, indem Sie ein zweites Kunden-Gateway verwenden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
12.2	Einrichtung und Pflege einer sicheren Netzwerkarchitektur	opensearch-in-vpc-only	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass sich Amazon OpenSearch Service-Domains innerhalb einer Amazon Virtual Private Cloud (Amazon VPC) befinden. Eine Amazon OpenSearch Service-Domain innerhalb einer Amazon VPC ermöglicht die sichere Kommunikation zwischen Amazon OpenSearch Service und anderen Services innerhalb der Amazon VPC, ohne dass ein Internet-Gateway, ein NAT-Gerät oder eine VPN-Verbindung erforderlich ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
12.2	Einrichtung und Pflege einer sicheren Netzwerkarchitektur	elbv2-multiple-az	Elastic Load Balancing (ELB) verteilt Ihren eingehenden Traffic automatisch auf mehrere Ziele wie EC2 Instances, Container und IP-Adressen in einer Availability Zone. Zur Gewährlei stung einer hohen Verfügbarkeit stellen Sie sicher, dass Ihr ELB Instances aus mehreren Availability Zones registriert hat.
12.3	Netzwerkinfrastruktur sicher verwalten	api-gw-ssl-enabled	Stellen Sie sicher, dass die REST-API-Stufen von Amazon API Gateway mit SSL-Zertifikaten konfiguri ert sind, damit Backend-Systeme überprüfen können, ob Anforderungen von API Gateway stammen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
12.3	Netzwerkinfrastruktur sicher verwalten	alb-http-to-https-Umleitungsprüfung	Um Daten während der Übertragung zu schützen, stellen Sie sicher, dass Ihr Application Load Balancer unverschlüsselte HTTP-Anfragen automatisch an HTTPS umleitet. Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
12.3	Netzwerkinfrastruktur sicher verwalten	elb-acm-certificate-required	Zum Schutz von eventuell vorhanden en sensiblen Daten sowie von Daten während der Übertragung muss die Verschlüsselung für Ihr Elastic Load Balancing aktiviert sein. Verwenden Sie AWS Certificate Manager, um öffentlic he und private SSL/ TLS-Zertifikate mit AWS Diensten und internen Ressource n zu verwalten, bereitzustellen und bereitzustellen.
12.3	Netzwerkinfrastruktur sicher verwalten	elb-tls-https-listeners-nur	Stellen Sie sicher, dass Ihre Elastic Load Balancer (ELBs) mit SSL- oder HTTPS-Listenern konfiguriert sind. Um eventuell vorhanden e sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
12.3	Netzwerkinfrastruktur sicher verwalten	s-3 bucket-ssl-requests-only	Um Daten während der Übertragung zu schützen, stellen Sie sicher, dass Ihre Amazon Simple Storage Service (Amazon S3)-Buckets Anfragen zur Verwendung von Secure Socket Layer (SSL)-Buckets erfordern. Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.
12.3	Netzwerkinfrastruktur sicher verwalten	redshift-require-tls-ssl	Stellen Sie sicher, dass Ihre Amazon-Redshift-Cluster eine TLS/SSL-Verschlüsselung erfordern, um eine Verbindung zu SQL-Clients herzustellen. Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
12.3	Netzwerkinfrastruktur sicher verwalten	Elb v 2- acm-certificate-required	Zum Schutz von eventuell vorhanden en sensiblen Daten sowie von Daten während der Übertragung muss die Verschlüsselung für Ihr Elastic Load Balancing aktiviert sein. Verwenden Sie AWS Certificate Manager, um öffentlic he und private SSL/ TLS-Zertifikate mit AWS Diensten und internen Ressource n zu verwalten, bereitzustellen und bereitzustellen.
12.3	Netzwerkinfrastruktur sicher verwalten	opensearch-https-required	Da sensible Daten existieren können und um Daten während der Übertragung zu schützen, sollten Sie sicherstellen, dass HTTPS für Verbindun gen zu Ihren Amazon OpenSearch Service-Domains aktiviert ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
12.6	Verwendung von sicheren Netzwerkmanagement- und Kommunikationsprotokollen	api-gw-ssl-enabled	Stellen Sie sicher, dass die REST-API-Stufen von Amazon API Gateway mit SSL-Zertifikaten konfiguriert sind, damit Backend-Systeme überprüfen können, ob Anforderungen von API Gateway stammen.
12.6	Verwendung von sicheren Netzwerkmanagement- und Kommunikationsprotokollen	alb-http-to-https-Umleitungsprüfung	Um Daten während der Übertragung zu schützen, stellen Sie sicher, dass Ihr Application Load Balancer unverschlüsselte HTTP-Anfragen automatisch an HTTPS umleitet. Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
12.6	Verwendung von sicheren Netzwerkmanagement- und Kommunikationsprotokollen	elb-acm-certificate-required	Zum Schutz von eventuell vorhanden en sensiblen Daten sowie von Daten während der Übertragung muss die Verschlüsselung für Ihr Elastic Load Balancing aktiviert sein. Verwenden Sie AWS Certificate Manager, um öffentlic he und private SSL/TLS-Zertifikate mit AWS Diensten und internen Ressource n zu verwalten, bereitzustellen und bereitzustellen.
12.6	Verwendung von sicheren Netzwerkmanagement- und Kommunikationsprotokollen	elb-tls-https-listeners-nur	Stellen Sie sicher, dass Ihre Elastic Load Balancer (ELBs) mit SSL- oder HTTPS-Listenern konfiguriert sind. Um eventuell vorhanden e sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
12.6	Verwendung von sicheren Netzwerkmanagement- und Kommunikationsprotokollen	s-3 bucket-ssl-requests-only	Um Daten während der Übertragung zu schützen, stellen Sie sicher, dass Ihre Amazon Simple Storage Service (Amazon S3)-Buckets Anfragen zur Verwendung von Secure Socket Layer (SSL)-Buckets erfordern. Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.
12.6	Verwendung von sicheren Netzwerkmanagement- und Kommunikationsprotokollen	redshift-require-tls-ssl	Stellen Sie sicher, dass Ihre Amazon-Redshift-Cluster eine TLS/SSL-Verschlüsselung erfordern, um eine Verbindung zu SQL-Clients herzustellen. Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
12.6	Verwendung von sicheren Netzwerkmanagement- und Kommunikationsprotokollen	Elb v 2- acm-certificate-required	Zum Schutz von eventuell vorhandenen sensiblen Daten sowie von Daten während der Übertragung muss die Verschlüsselung für Ihr Elastic Load Balancing aktiviert sein. Verwenden Sie AWS Certificate Manager, um öffentliche und private SSL/TLS-Zertifikate mit AWS Diensten und internen Ressourcen zu verwalten, bereitzustellen und bereitzustellen.
12.6	Verwendung von sicheren Netzwerkmanagement- und Kommunikationsprotokollen	opensearch-https-required	Da sensible Daten existieren können und um Daten während der Übertragung zu schützen, sollten Sie sicherstellen, dass HTTPS für Verbindungen zu Ihren Amazon OpenSearch Service-Domains aktiviert ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
13.1	Zentralisieren der Warnung vor Sicherheitsereignissen	guardduty-enabled-centralized	Amazon GuardDuty kann mithilfe von Threat Intelligence Feeds helfen, potenzielle Cybersicherheitsereignisse zu überwachen und zu erkennen. Dazu gehören Listen mit bösartigen IPs und maschinellen Lernmethoden zur Identifizierung unerwarteter, nicht autorisierter und bösartiger Aktivitäten in Ihrer AWS Cloud-Umgebung.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
13.1	Zentralisieren der Warnung vor Sicherheitsereignissen	securityhub-enabled	AWS Security Hub hilft bei der Überwachung von unbefugtem Personal, Verbindungen, Geräten und Software. AWS Security Hub aggregiert, organisiert und priorisiert die Sicherheitswarnungen oder Ergebnisse mehrerer Dienste. AWS Einige dieser Dienste sind Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer und AWS Firewall Manager sowie AWS Partnerlösungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
13.3	Bereitstellen einer Lösung zur Erkennung von Netzwerkeindringlingen	guardduty-enabled-centralized	Amazon GuardDuty kann mithilfe von Threat Intelligence Feeds helfen, potenzielle Cybersicherheitsereignisse zu überwachen und zu erkennen. Dazu gehören Listen mit bösartigen IPs und maschinellen Lernmethoden zur Identifizierung unerwarteter, nicht autorisierter und bösartiger Aktivitäten in Ihrer AWS Cloud-Umgebung.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
13.6	Sammeln von Protokollen zum Netzwerkdatenverkehr	vpc-flow-logs-enabled	VPC-Flow-Protokolle erfassen detaillierte Informationsdatensätze über den IP-Datenverkehr, der zu und von Netzwerkschnittstellen in Ihrer Amazon Virtual Private Cloud (Amazon VPC) fließt. Standardmäßig enthalten Flow-Protokolldatensätze Werte für die verschiedenen Komponenten des IP-Flows, einschließlich Quelle, Ziel und Protokoll.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
13,6	Sammeln von Protokollen zum Netzwerkdatenverkehr	wafv2-logging-enabled	Um die Protokollierung und Überwachung in Ihrer Umgebung zu erleichtern, aktivieren Sie die AWS WAF (V2) -Protokollierung im regionalen und globalen Web. ACLs AWS Die WAF-Protokollierung bietet detaillierte Informationen über den Datenverkehr, der von Ihrer Web-ACL analysiert wird. In den Protokollen werden die Uhrzeit aufgezeichnet, zu der die AWS WAF die Anfrage von Ihrer AWS Ressource erhalten hat, Informationen über die Anfrage und eine Aktion für die Regel, der jede Anfrage entsprach.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
13.10	Durchführen der Filterung auf Anwendungsebene	api-gw-associated-with-WAF	AWS Mit WAF können Sie eine Reihe von Regeln (als Web Access Control List (Web ACL) bezeichnet) konfigurieren, die Webanfragen auf der Grundlage von anpassbaren Websicherheitsregeln und -bedingungen, die Sie definieren, zulassen, blockieren oder zählen. Stellen Sie sicher, dass Ihre Amazon-API-Gateway-Stufe mit einer WAF-Web-ACL verknüpft ist, um sie vor böswilligen Angriffen zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
16.1	Einrichtung und Aufrechterhaltung eines sicheren Anwendungsentwicklungsprozesses	codebuild-project-envvar-awscred-überprüfen	Stellen Sie sicher, dass die Anmeldeinformationen AWS_ACCESS_KEY_ID AWS_SECRET_ACCESS_KEY nicht in AWS Codebuild-Projektumgebungen vorhanden sind. Speichern Sie diese Variablen nicht als Klartext. Das Speichern dieser Variablen als Klartext bewirkt eine unbeabsichtigte Offenlegung von Daten sowie unberechtigte Zugriffe.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
16.1	Einrichtung und Aufrechterhaltung eines sicheren Anwendungsentwicklungsprozesses	codebuild-project-source-repo-URL-Prüfung	Stellen Sie sicher, dass die URL des Quell-Repositorys GitHub oder des Bitbucket-Quell-Repositorys keine persönlichen Zugriffstoken oder Anmeldeinformationen in Codebuild-Projektumgebungen enthält. AWS Verwende OAuth anstelle von persönlichen Zugriffstoken oder Anmeldedaten die Autorisierung für den Zugriff auf GitHub Bitbucket-Repositorys.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
16.1	Einrichtung und Aufrechterhaltung eines sicheren Anwendungsentwicklungsprozesses	codebuild-project-environment-privileged-überprüfen	Um die Implementierung des Prinzips der geringsten Rechte zu unterstützen, stellen Sie sicher, dass in Ihrer CodeBuild Amazon-Projektumgebung der privilegierte Modus nicht aktiviert ist. Diese Einstellung sollte deaktiviert werden, um einen unbeabsichtigten Zugriff auf Docker APIs sowie auf die dem Container zugrundeliegende Hardware zu verhindern.
16.1	Einrichtung und Aufrechterhaltung eines sicheren Anwendungsentwicklungsprozesses	codebuild-project-artifact-encryption	Um sensible Daten im Speicher zu schützen, stellen Sie sicher, dass die Verschlüsselung für Ihre AWS CodeBuild Artefakte aktiviert ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
16.1	Einrichtung und Aufrechterhaltung eines sicheren Anwendungsentwicklungsprozesses	codebuild-project-logging-enabled	Stellen Sie sicher, dass die AWS CodeBuild Projektprotokollierung aktiviert ist, damit Ihre Build-Ausgabeprotokolle entweder an Amazon CloudWatch oder Amazon Simple Storage Service (Amazon S3) gesendet werden. Build-Ausgabeprotokolle enthalten detaillierte Informationen zu Ihrem Build-Projekt.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
16.12	Implementieren von Sicherheitsprüfungen auf Codeebene	codebuild-project-envvar-awscred-überprüfen	Stellen Sie sicher, dass die Anmeldeinformationen AWS_ACCESS_KEY_ID AWS_SECRET_ACCESS_KEY nicht in AWS Codebuild-Projektumgebungen vorhanden sind. Speichern Sie diese Variablen nicht als Klartext. Das Speichern dieser Variablen als Klartext bewirkt eine unbeabsichtigte Offenlegung von Daten sowie unberechtigte Zugriffe.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
16.12	Implementieren von Sicherheitsprüfungen auf Codeebene	codebuild-project-source-repo-URL-Prüfung	Stellen Sie sicher, dass die URL des Quell-Repositorys GitHub oder des Bitbucket-Quell-Repositorys keine persönlichen Zugriffstoken oder Anmeldeinformationen in Codebuild-Projektumgebungen enthält. AWS Verwende OAuth anstelle von persönlichen Zugriffstoken oder Anmeldedaten die Autorisierung für den Zugriff auf GitHub Bitbucket-Repositorys.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
16.12	Implementieren von Sicherheitsprüfungen auf Codeebene	codebuild-project-environment-privileged-überprüfen	Um die Implementierung des Prinzips der geringsten Rechte zu unterstützen, stellen Sie sicher, dass in Ihrer CodeBuild Amazon-Projektumgebung der privilegierte Modus nicht aktiviert ist. Diese Einstellung sollte deaktiviert werden, um einen unbeabsichtigten Zugriff auf Docker APIs sowie auf die dem Container zugrunde liegende Hardware zu verhindern.
16.12	Implementieren von Sicherheitsprüfungen auf Codeebene	codebuild-project-artifact-encryption	Um sensible Daten im Speicher zu schützen, stellen Sie sicher, dass die Verschlüsselung für Ihre AWS CodeBuild Artefakte aktiviert ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
16.12	Implementieren von Sicherheitsprüfungen auf Codeebene	codebuild-project-logging-enabled	Stellen Sie sicher, dass die AWS CodeBuild Projektprotokollierung aktiviert ist, damit Ihre Build-Ausgabeprotokolle entweder an Amazon CloudWatch oder Amazon Simple Storage Service (Amazon S3) gesendet werden. Build-Ausgabeprotokolle enthalten detaillierte Informationen zu Ihrem Build-Projekt.

Vorlage

Die Vorlage ist verfügbar unter GitHub: Operational Best Practices for CIS Critical Security Controls v8 IG3.

Bewährte Methoden für die Ausführung von CIS Top 20

Konformitätspakete bieten ein allgemeines Compliance-Framework, das es Ihnen ermöglicht, mithilfe verwalteter oder benutzerdefinierter AWS Config Regeln und Abhilfemaßnahmen Kontrollen zur Sicherheits-, Betriebs- oder Kostenoptimierung durchzuführen. AWS Config Conformance Packs dienen als Beispielvorlagen nicht dazu, die vollständige Einhaltung eines bestimmten Governance- oder Compliance-Standards sicherzustellen. Sie sind dafür verantwortlich, selbst zu beurteilen, ob Ihre Nutzung der Services den geltenden gesetzlichen und behördlichen Anforderungen entspricht.

Im Folgenden finden Sie ein Beispiel für eine Zuordnung zwischen den 20 wichtigsten Sicherheitskontrollen des Center for Internet Security (CIS) und den AWS verwalteten

Konfigurationsregeln. Jede Config-Regel gilt für eine bestimmte AWS Ressource und bezieht sich auf eine oder mehrere CIS Top 20-Kontrollen. Eine CIS-Top-20-Kontrolle kann mehreren Config-Regeln zugeordnet werden. In der folgenden Tabelle finden Sie weitere Informationen und Anleitungen zu diesen Zuordnungen.

Dieses Konformitätspaket wurde von AWS Security Assurance Services LLC (AWS SAS) validiert. Dabei handelt es sich um ein Team von qualifizierten Sicherheitsbewertern (QSAs) für die Zahlungskartenbranche (), HITRUST-zertifizierten Common Security Framework Practitionern (CCSFPs) und Compliance-Experten, die für die Beratung und Bewertung verschiedener Branchen-Frameworks zertifiziert sind. AWS Die Experten von SAS haben dieses Conformance Pack entwickelt, um es einem Kunden zu ermöglichen, sich auf eine Untergruppe der Top 20 der GUS-Staaten einzustellen.

Kontroll-ID	AWS Config Regel	Empfehlungen
CIS.2	ec2-check managedinstance-association-compliance-status	Verwenden Sie AWS Systems Manager Associations, um bei der Inventarisierung von Softwareplattformen und Anwendungen innerhalb eines Unternehmens zu helfen. AWS Systems Manager weist Ihren verwalteten Instances einen Konfigurationsstatus zu und ermöglicht es Ihnen, Basiswerte für Betriebss ystem-Patch-Levels, Softwarei nstallationen, Anwendung skonfigurationen und andere Details zu Ihrer Umgebung festzulegen.
CIS.2	ec2-prüfen managedinstance-patch-compliance-status	Aktivieren Sie diese Regel, um bei der Identifizierung und Dokumentation von Sicherhei tslücken in Amazon Elastic Compute Cloud (Amazon

Kontroll-ID	AWS Config Regel	Empfehlungen
		EC2) zu helfen. Die Regel prüft, ob die EC2 Amazon-Instance die Patch-Konformität im AWS Systems Manager gemäß den Richtlinien und Verfahren Ihrer Organisation einhält.
CIS.2	ec2- -eni security-group-attached-to	Diese Regel stellt sicher, dass die Sicherheitsgruppen an eine Amazon Elastic Compute Cloud (Amazon EC2) - Instance oder an eine ENI angehängt sind. Diese Regel unterstützt die Überwachung ungenutzter Sicherheitsgruppen im Bestand und die Verwaltung Ihrer Umgebung.
CIS.2	ec2-stopped-instance	Aktivieren Sie diese Regel, um bei der Basiskonfiguration von Amazon Elastic Compute Cloud (Amazon EC2) - Instances zu helfen, indem Sie überprüfen, ob EC2 Amazon-Instances gemäß den Standards Ihrer Organisation für mehr als die zulässige Anzahl von Tagen gestoppt wurden.

Kontroll-ID	AWS Config Regel	Empfehlungen
CIS.2	ec2- volume-inuse-check	Diese Regel stellt sicher, dass Amazon Elastic Block Store-Volumes, die an Amazon Elastic Compute Cloud (Amazon EC2) -Instances angehängt sind, zum Löschen markiert werden, wenn eine Instance beendet wird. Wenn ein Amazon-EBS-Volume beim Löschen der Instance, an die es angehängt ist, beendet wird, kann dies gegen das Konzept der geringsten Funktionalität verstoßen.
CIS.2	eip-attached	Diese Regel stellt sicher, dass Elastic, die einer Amazon Virtual Private Cloud (Amazon VPC) IPs zugewiesen sind, an Amazon Elastic Compute Cloud (Amazon EC2) -Instances oder verwendete Elastic Network Interfaces angehängt sind. Diese Regel hilft bei der Überwachung ungenutzter Inhalte EIPs in Ihrer Umgebung.

Kontroll-ID	AWS Config Regel	Empfehlungen
CIS.3	guardduty-enabled-centralized	Amazon GuardDuty kann mithilfe von Threat Intelligence Feeds helfen, potenzielle Cybersicherheitsereignisse zu überwachen und zu erkennen. Dazu gehören Listen mit bösartigen IPs und maschinellen Lernmethoden zur Identifizierung unerwarteter, nicht autorisierter und bösartiger Aktivitäten in Ihrer AWS Cloud-Umgebung.
CIS.3	guardduty-non-archived-findings	Amazon GuardDuty hilft Ihnen dabei, die Auswirkungen eines Vorfalls zu verstehen, indem es die Ergebnisse nach Schweregrad klassifiziert: niedrig, mittel und hoch. Diese Klassifizierungen können Sie zur Festlegung von entsprechenden Strategien und Prioritäten zur Behebung solcher Vorfälle verwenden. Mit dieser Regel können Sie optional daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7) und daysHighSev (Config Default: 1) für nicht archivierte Ergebnisse festlegen, wie es die Richtlinien Ihrer Organisation erfordern.

Kontroll-ID	AWS Config Regel	Empfehlungen
CIS.3	securityhub-enabled	AWS Security Hub hilft bei der Überwachung von unbefugte m Personal, Verbindungen, Geräten und Software. AWS Security Hub aggregiert, organisiert und priorisiert die Sicherheitswarnungen oder Ergebnisse mehrerer Dienste. AWS Einige dieser Dienste sind Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer und AWS Firewall Manager sowie AWS Partnerlösungen.
CIS.4	guardduty-enabled-centralized	Amazon GuardDuty kann mithilfe von Threat Intellige nce Feeds helfen, potenzielle Cybersicherheitsereignisse zu überwachen und zu erkennen. Dazu gehören Listen mit bösartigen IPs und maschinel len Lernmethoden zur Identifiz ierung unerwarteter, nicht autorisierter und bösartige r Aktivitäten in Ihrer AWS Cloud-Umgebung.

Kontroll-ID	AWS Config Regel	Empfehlungen
CIS.4	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) kann Ihnen dabei helfen, die Prinzipien der geringsten Rechte und der Aufgabent rennung in Zugriffsberechtigu ngen und Autorisierungen zu integrieren und so zu verhindern, dass Richtlinien „Effect“: „Allow“ mit „Action“: „*“ anstelle von „Resource“: „*“ enthalten. Wenn Benutzern mehr Rechte eingeräumt werden, als für die Ausführun g einer Aufgabe erforderl ich sind, kann dies gegen das Prinzip der geringste n Berechtigung und der Aufgabentrennung verstoßen.

Kontroll-ID	AWS Config Regel	Empfehlungen
CIS.4	iam-root-access-key-überprüfen	Der Zugriff auf Systeme und Ressourcen kann gesteuert werden, indem überprüft wird, ob der Root-Benutzer keine Zugriffsschlüssel mit seiner AWS Identity and Access Management (IAM) -Rolle verknüpft hat. Stellen Sie sicher, dass die Root-Zugriffsschlüssel gelöscht werden. Erstellen und verwenden Sie stattdessen rollenbasierte Funktionen, AWS-Konten um das Prinzip der geringsten Funktionalität zu berücksichtigen.
CIS.4	root-account-hardware-mfa-aktiviert	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Hardware-MFA für den Root-Benutzer aktiviert ist. Der Stammbenutzer ist der AWS-Konto-Benutzer mit den meisten Berechtigungen. MFA sorgt für eine weitere Schutzebene zusätzlich zu den Anmeldeinformationen. Indem Sie MFA für den Root-Benutzer vorschreiben, können Sie die Anzahl AWS-Konten kompromittierter Benutzer reduzieren.

Kontroll-ID	AWS Config Regel	Empfehlungen
CIS.4	root-account-mfa-enabled	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass MFA für den Root-Benutzer aktiviert ist. Der Stammbenutzer ist der AWS-Konto-Benutzer mit den meisten Berechtigungen. MFA bietet eine weitere Schutzebene zusätzlich zum Benutzernamen und Passwort. Indem Sie MFA für den Root-Benutzer vorschreiben, können Sie die Anzahl AWS-Konten kompromittierter Benutzer reduzieren.
CIS.4	securityhub-enabled	AWS Security Hub hilft bei der Überwachung von unbefugtem Personal, Verbindungen, Geräten und Software. AWS Security Hub aggregiert, organisiert und priorisiert die Sicherheitswarnungen oder Ergebnisse mehrerer Dienste. AWS Einige dieser Dienste sind Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer und AWS Firewall Manager sowie AWS Partnerlösungen.

Kontroll-ID	AWS Config Regel	Empfehlungen
CIS.5	ec2-manager instance-managed-by-systems	Eine Bestandsaufnahme der Softwareplattformen und Anwendungen innerhalb des Unternehmens ist möglich, indem Amazon Elastic Compute Cloud (Amazon EC2) -Instances mit AWS Systems Manager verwaltet werden. Verwenden Sie AWS Systems Manager, um detaillierte Systemkonfigurationen, Betriebssystem-Patch-Levels, Namen und Typ der Dienste, Softwareinstallationen, Anwendungsname, Herausgeber und Version sowie andere Details zu Ihrer Umgebung bereitzustellen.

Kontroll-ID	AWS Config Regel	Empfehlungen
CIS.5	ec2-check managedinstance-association-compliance-status	Verwenden Sie AWS Systems Manager Associations, um bei der Inventarisierung von Softwareplattformen und Anwendungen innerhalb eines Unternehmens zu helfen. AWS Systems Manager weist Ihren verwalteten Instances einen Konfigurationsstatus zu und ermöglicht es Ihnen, Basiswerte für Betriebss ystem-Patch-Levels, Softwarei nstallationen, Anwendung skonfigurationen und andere Details zu Ihrer Umgebung festzulegen.
CIS.5	ec2-prüfen managedinstance-patch-compliance-status	Aktivieren Sie diese Regel, um bei der Identifizierung und Dokumentation von Sicherhei tslücken in Amazon Elastic Compute Cloud (Amazon EC2) zu helfen. Die Regel prüft, ob die EC2 Amazon-In stance die Patch-Konformität im AWS Systems Manager gemäß den Richtlinien und Verfahren Ihrer Organisation einhält.

Kontroll-ID	AWS Config Regel	Empfehlungen
CIS.5	redshift-cluster-configuration-check	Um Daten im Ruhezustand zu schützen, muss die Verschlüsselung für Ihre Amazon-Redshift-Cluster aktiviert sein. Sie müssen auch sicherstellen, dass die erforderlichen Konfigurationen auf Amazon-Redshift-Clustern bereitgestellt werden. Die Prüfungsprotokollierung muss aktiviert sein, um Informationen zu Verbindungen und Benutzeraktivitäten in der Datenbank bereitzustellen. Diese Regel erfordert, dass ein Wert für clusterDbEncrypted (Config Default: TRUE) und LoggingEnabled (Config Default: TRUE) gesetzt ist. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	AWS Config Regel	Empfehlungen
CIS.5	redshift-cluster-maintenancesettings-check	Diese Regel stellt sicher, dass Amazon-Redshift-Cluster die bevorzugten Einstellungen für Ihre Organisation haben. Insbesondere sorgt sie dafür, dass Cluster bevorzugte Wartungsfenster und automatisierte Aufbewahrungsfristen für Snapshots für die Datenbank haben. Für diese Regel müssen Sie den festlegen. allowVersionUpgrade Der Standardwert ist „true“. Außerdem können Sie optional den Zeitraum preferredMaintenanceWindow (der Standardwert ist sa: 16:00 -sa: 16:30) und den automatedSnapshotRetention Zeitraum (der Standardwert ist 1) festlegen. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.
CIS.6	api-gw-execution-logging-aktiviert	Die API-Gateway-Protokollierung zeigt detaillierte Ansichten der Benutzer, die auf die API zugegriffen haben, und wie diese Benutzer auf die API zugegriffen haben. Diese Einblicke ermöglichen die Transparenz von Benutzeraktivitäten.

Kontroll-ID	AWS Config Regel	Empfehlungen
CIS.6	cloud-trail-cloud-watch-logs-aktiviert	Verwenden Sie Amazon CloudWatch , um Protokoll ereignisaktivitäten zentral zu sammeln und zu verwalten . Die Aufnahme von AWS CloudTrail Daten liefert Einzelheiten zu den API-Aufru faktivitäten in Ihrem AWS-Konto.
CIS.6	cloudtrail-enabled	AWS CloudTrail kann bei der Nichtabstreitbarkeit helfen, indem Aktionen und API-Aufrufe der AWS Manag ement Console aufgezeic hnet werden. Sie können die Benutzer und die Benutzer AWS-Konten , die einen AWS Dienst aufgerufen haben, die Quell-IP-Adresse, über die die Aufrufe generiert wurden, und den Zeitpunkt der Anrufe identifizieren. Einzelheiten zu den erfassten Daten finden Sie in den AWS CloudTrail Datensatzinhalten.

Kontroll-ID	AWS Config Regel	Empfehlungen
CIS.6	cloud-trail-log-file-Validierung aktiviert	Verwenden Sie die AWS CloudTrail Protokolldateivalidierung, um die Integrität von Protokollen zu überprüfen. CloudTrail Mithilfe der Protokolldateivalidierung kann festgestellt werden, ob eine Protokolldatei geändert oder gelöscht wurde oder ob sie nach der Übermittlung CloudTrail unverändert geblieben ist. Dieses Feature wurde mit dem Branchenstandard entsprechenden Algorithmen entwickelt: SHA-256 für die Hashfunktion und SHA-256 mit RSA für digitale Signaturen. Aus diesem Grund ist es rechnerisch unmöglich, CloudTrail Protokolldateien unbemerkt zu ändern, zu löschen oder zu fälschen.

Kontroll-ID	AWS Config Regel	Empfehlungen
CIS.6	cloudtrail-s3-dataevents-enabled	Die Erfassung von Datenereignissen des Simple Storage Service (Amazon S3) hilft bei der Erkennung von ungewöhnlichen Aktivitäten. Zu den Details gehören Informationen zu dem AWS-Konto -Konto, das auf einen Amazon S3-Bucket zugegriffen hat, die IP-Adresse und die Uhrzeit des Ereignisses.
CIS.6	cloudwatch-alarm-action-check	Amazon CloudWatch alarmiert, wenn eine Metrik den Schwellenwert für eine bestimmte Anzahl von Bewertungszeiträumen überschreitet. Der Alarm führt eine oder mehrere Aktionen durch, die vom Wert der Metrik oder des Ausdrucks im Vergleich zu einem Schwellenwert in einer Reihe von Zeiträumen abhängt. Diese Regel erfordert einen Wert für alarmActionRequired (Config Default: True), insufficientDataActionRequired (Config Default: True), okActionRequired (Config Default: False). Der tatsächliche Wert muss die Alarmaktionen für Ihre Umgebung widerspiegeln.

Kontroll-ID	AWS Config Regel	Empfehlungen
CIS.6	elb-logging-enabled	Die Elastic-Load-Balancing-Aktivität ist ein zentraler Kommunikationspunkt innerhalb einer Umgebung. Stellen Sie sicher, dass die ELB-Protokollierung aktiviert ist. Die gesammelten Daten enthalten detaillierte Informati onen zu Anfragen, die an den ELB gesendet wurden. Jedes Protokoll enthält Informati onen wie die Zeit, zu der die Anforderung einging, die Client-IP-Adresse, Latenzen, Anforderungspfade und Serverantworten.
CIS.6	guardduty-enabled-centralized	Amazon GuardDuty kann mithilfe von Threat Intellige nce Feeds helfen, potenzielle Cybersicherheitsereignisse zu überwachen und zu erkennen. Dazu gehören Listen mit bösartigen IPs und maschinel len Lernmethoden zur Identifiz ierung unerwarteter, nicht autorisierter und bösartige r Aktivitäten in Ihrer AWS Cloud-Umgebung.

Kontroll-ID	AWS Config Regel	Empfehlungen
CIS.6	guardduty-non-archived-findings	Amazon GuardDuty hilft Ihnen dabei, die Auswirkungen eines Vorfalls zu verstehen, indem es die Ergebnisse nach Schweregrad klassifiziert: niedrig, mittel und hoch. Diese Klassifizierungen können Sie zur Festlegung von entsprechenden Strategien und Prioritäten zur Behebung solcher Vorfälle verwenden. Mit dieser Regel können Sie optional daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7) und daysHighSev (Config Default: 1) für nicht archivierte Ergebnisse festlegen, wie es die Richtlinien Ihrer Organisation erfordern.

Kontroll-ID	AWS Config Regel	Empfehlungen
CIS.6	multi-region-cloudtrail-enabled	AWS CloudTrail zeichnet Aktionen und API-Aufrufe der AWS Management Console auf. Sie können feststellen, welche Benutzer und Konten angerufen wurden AWS, von welcher Quell-IP-Adresse aus die Anrufe getätigt wurden und wann die Anrufe erfolgten . CloudTrail übermittelt Protokolldateien von allen an Ihren S3-Bucket AWS-Regionen , wenn MULTI_REGION_CLOUD_TRAIL_ENABLED aktiviert ist. Außerdem wird beim AWS Start einer neuen Region derselbe Trail in der neuen Region erstellt. CloudTrail Dadurch erhalten Sie automatisch Protokoll dateien mit API-Aktivitäten für die neue Region.

Kontroll-ID	AWS Config Regel	Empfehlungen
CIS.6	redshift-cluster-configuration-check	Um Daten im Ruhezustand zu schützen, muss die Verschlüsselung für Ihre Amazon-Redshift-Cluster aktiviert sein. Sie müssen auch sicherstellen, dass die erforderlichen Konfigurationen auf Amazon-Redshift-Clustern bereitgestellt werden. Die Prüfungsprotokollierung muss aktiviert sein, um Informationen zu Verbindungen und Benutzeraktivitäten in der Datenbank bereitzustellen. Diese Regel erfordert, dass ein Wert für clusterDbEncrypted (Config Default: TRUE) und LoggingEnabled (Config Default: TRUE) gesetzt ist. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	AWS Config Regel	Empfehlungen
CIS.6	s3- bucket-logging-enabled	Die Amazon Simple Storage Service (Amazon S3)-Serve rzugriffsprotokollierung bietet eine Methode zur Überwachung des Netzwerks im Hinblick auf potenzielle Cybersicherheitsereignisse. Die Ereignisse werden überwacht, indem detaillie rte Aufzeichnungen über die Anfragen erfasst werden, die an einen Amazon-S3-Bucket gestellt wurden. Jeder Zugriffsprotokolleintrag enthält Details zu einer einzelnen Zugriffsanfrage. Zu den Details gehören Anfordere r, Bucket-Name, Anforderu ngszeit, Anforderungsaktion, Antwortstatus und Fehlercode, falls relevant.

Kontroll-ID	AWS Config Regel	Empfehlungen
CIS.6	securityhub-enabled	AWS Security Hub hilft bei der Überwachung von unbefugte m Personal, Verbindungen, Geräten und Software. AWS Security Hub aggregiert, organisiert und priorisiert die Sicherheitswarnungen oder Ergebnisse mehrerer Dienste. AWS Einige dieser Dienste sind Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer und AWS Firewall Manager sowie AWS Partnerlösungen.
CIS.6	vpc-flow-logs-enabled	VPC-Flow-Protokolle erfassen detaillierte Informationsdatens ätze über den IP-Datenv erkehr, der zu und von Netzwerkschnittstellen in Ihrer Amazon Virtual Private Cloud (Amazon VPC) fließt. Standardmäßig enthalten Flow-Protokolldatensätze Werte für die verschiedenen Komponenten des IP-Flows, einschließlich Quelle, Ziel und Protokoll.

Kontroll-ID	AWS Config Regel	Empfehlungen
CIS.8	guardduty-enabled-centralized	Amazon GuardDuty kann mithilfe von Threat Intelligence Feeds helfen, potenzielle Cybersicherheitsereignisse zu überwachen und zu erkennen. Dazu gehören Listen mit bösartigen IPs und maschinellen Lernmethoden zur Identifizierung unerwarteter, nicht autorisierter und bösartiger Aktivitäten in Ihrer AWS Cloud-Umgebung.
CIS.9	dms-replication-not-public	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass auf DMS-Replikationsinstanzen nicht öffentlich zugegriffen werden kann. DMS-Replikations-Instances können vertrauliche Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.
CIS.9	ebs-snapshot-public-restorable-überprüfen	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass EBS-Snapshots nicht öffentlich wiederherstellbar sind. EBS-Volume-Snapshots können vertrauliche Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	AWS Config Regel	Empfehlungen
CIS.9	ec-2 instance-no-public-ip	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon Elastic Compute Cloud (Amazon EC2) -Instances nicht öffentlich zugänglich sind. EC2Amazon-Instances können vertrauliche Informati onen enthalten, und für solche Konten ist eine Zugriffsk ontrolle erforderlich.
CIS.9	elasticsearch-in-vpc-only	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass sich Amazon OpenSearch OpenSearch Service (Service) -Domains innerhalb einer Amazon Virtual Private Cloud (Amazon VPC) befinden. Eine OpenSearch Service-D omain innerhalb einer Amazon VPC ermöglicht die sichere Kommunikation zwischen OpenSearch Service und anderen Services innerhalb der Amazon VPC, ohne dass ein Internet-Gateway, ein NAT-Gerät oder eine VPN-Verbindung erforderlich ist.

Kontroll-ID	AWS Config Regel	Empfehlungen
CIS.9	emr-master-no-public-ip	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon EMR-Cluster-Masterknoten nicht öffentlich zugänglich sind. Amazon-EMR-Cluster-Hauptknoten können vertrauliche Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.
CIS.9	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) Security Groups können bei der Verwaltung des Netzwerkzugriffs helfen, indem sie eine statusbehaftete Filterung von eingehendem und ausgehendem Netzwerkverkehr zu Ressourcen bereitstellen. AWS Wenn Sie eingehenden (oder entfernten) Datenverkehr von 0.0.0.0/0 bis Port 22 auf Ihren Ressourcen nicht zulassen, können Sie den Remote-Zugriff einschränken.

Kontroll-ID	AWS Config Regel	Empfehlungen
CIS.9	ec2- instances-in-vpc	Stellen Sie Amazon Elastic Compute Cloud (Amazon EC2) -Instances innerhalb einer Amazon Virtual Private Cloud (Amazon VPC) bereit, um eine sichere Kommunika tion zwischen einer Instance und anderen Services innerhalb der Amazon VPC zu ermöglichen, ohne dass ein Internet-Gateway, ein NAT-Gerät oder eine VPN-Verbindung erforderlich ist. Der gesamte Datenverkehr bleibt sicher in der AWS Cloud. Domänen, die sich innerhalb einer Amazon VPC befinden, verfügen aufgrund ihrer logischen Isolierung im Vergleich zu Domänen, die öffentliche Endpunkte nutzen, über eine zusätzlic he Sicherheitsebene. Weisen Sie EC2 Amazon-Instances einer Amazon-VPC zu, um den Zugriff ordnungsgemäß zu verwalten.

Kontroll-ID	AWS Config Regel	Empfehlungen
CIS.9	internet-gateway-authorized-vpc-nur	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Internet-Gateways nur mit autorisierter Amazon Virtual Private Cloud (Amazon VPC) verbunden sind. Internet-Gateways ermöglichen den bidirekti onalen Internetzugang zur und von der Amazon VPC, was möglicherweise zu einem unbefugten Zugriff auf Amazon-VPC-Ressourcen führen kann.
CIS.9	lambda-function-public-acce ss-verboten	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherste llen, dass AWS Lambda-Funktionen nicht öffentlich zugänglich sind. Der öffentlic he Zugriff kann möglicher weise die Verfügbarkeit von Ressourcen beeinträchtigen.

Kontroll-ID	AWS Config Regel	Empfehlungen
CIS.9	lambda-inside-vpc	Stellen Sie AWS Lambda-Funktionen in einer Amazon Virtual Private Cloud (Amazon VPC) bereit, um eine sichere Kommunikation zwischen einer Funktion und anderen Diensten innerhalb der Amazon VPC zu gewährleisten. Bei dieser Konfiguration sind kein Internet-Gateway, kein NAT-Gerät und keine VPN-Verbindung erforderlich. Der gesamte Datenverkehr bleibt sicher in der Cloud. AWS Domains, die sich innerhalb einer VPC befinden, verfügen aufgrund ihrer logischen Isolierung im Vergleich zu Domains mit öffentlichen Endpunkten über eine zusätzliche Sicherheitsebene. Um den Zugriff ordnungsgemäß zu verwalten, sollten AWS Lambda-Funktionen einer VPC zugewiesen werden.

Kontroll-ID	AWS Config Regel	Empfehlungen
CIS.9	rds-instance-public-access-überprüfen	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Relational Database Service (Amazon RDS) -Instances nicht öffentlich sind. Amazon-RDS-Datenbank-Instances können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.
CIS.9	rds-snapshots-public-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Relational Database Service (Amazon RDS) -Instances nicht öffentlich sind. Amazon-RDS-Datenbank-Instances können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	AWS Config Regel	Empfehlungen
CIS.9	redshift-cluster-public-access-überprüfen	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Redshift Redshift-Cluster nicht öffentlich sind. Amazon-Redshift-Cluster können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.
CIS.9	restricted-common-ports	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass gemeinsame Ports für Amazon Elastic Compute Cloud (Amazon EC2) - Sicherheitsgruppen eingeschränkt sind. Wenn der Zugriff auf Ports nicht auf vertrauenswürdige Quellen beschränkt wird, kann dies zu Angriffen auf die Verfügbarkeit, Integrität und Vertraulichkeit von Systemen führen. Mit dieser Regel können Sie optional die Parameter blockedPort1–blockedPort5 festlegen (Standardkonfigurationen: 20, 21, 3389, 3306, 4333). Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	AWS Config Regel	Empfehlungen
CIS.9	account-level-public-accesss3-Blöcke	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Simple Storage Service (Amazon S3) -Buckets nicht öffentlich zugänglich sind. Diese Regel trägt dazu bei, sensible Daten vor unbefugten Remote-Benutzern zu schützen, indem sie den öffentlichen Zugriff verhindert. Mit dieser Regel können Sie optional die Parameter ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) und restrictPublicBuckets Parameter (Config Default: True) festlegen. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	AWS Config Regel	Empfehlungen
CIS.9	s3- bucket-public-read-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie nur autorisierten Benutzern, Prozessen und Geräten Zugriff auf Amazon Simple Storage Service (Amazon S3) -Buckets gewähren. Die Verwaltung des Zugriffs sollte mit der Klassifizierung der Daten übereinstimmen.
CIS.9	s3- bucket-public-write-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie nur autorisierten Benutzern, Prozessen und Geräten Zugriff auf Amazon Simple Storage Service (Amazon S3) -Buckets gewähren. Die Verwaltung des Zugriffs sollte mit der Klassifizierung der Daten übereinstimmen.
CIS.9	sagemaker-notebook-no-direct-Internetzugang	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass SageMaker Amazon-Notebooks keinen direkten Internetzugang zulassen. Indem Sie direkten Internetzugang blockieren, vermeiden Sie, dass unbefugte Benutzer auf sensible Daten zugreifen.

Kontroll-ID	AWS Config Regel	Empfehlungen
CIS.9	vpc-default-security-group-geschlossen	Sicherheitsgruppen von Amazon Elastic Compute Cloud (Amazon EC2) können bei der Verwaltung des Netzwerkzugriffs helfen, indem sie eine statusbeh aftete Filterung des ein- und ausgehenden Netzwerkv erkehrs zu Ressourcen bereitstellen. AWS Die Beschränkung des gesamten Datenverkehrs auf die Standardsicherheitsgruppe hilft dabei, den Fernzugriff auf Ihre Ressourcen einzuschr änken. AWS

Kontroll-ID	AWS Config Regel	Empfehlungen
CIS.9	vpc-sg-open-only-to-authorized-ports	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass gemeinsame Ports für Amazon Elastic Compute Cloud (Amazon EC2) - Sicherheitsgruppen eingeschränkt sind. Wenn der Zugriff auf Ports nicht auf vertrauenswürdige Quellen beschränkt wird, kann dies zu Angriffen auf die Verfügbarkeit, Integrität und Vertraulichkeit von Systemen führen. Durch die Beschränkung des Zugriffs auf Ressourcen innerhalb einer Sicherheitsgruppe aus dem Internet (0.0.0.0/0) kann der Remote-Zugriff auf interne Systeme gesteuert werden.

Kontroll-ID	AWS Config Regel	Empfehlungen
CIS.10	db-instance-backup-enabled	Die Sicherungsfunktion von Amazon RDS erstellt Sicherungen Ihrer Datenbanken und Transaktionsprotokolle. Amazon RDS erstellt einen Snapshot für das Speichervolume Ihrer DB-Instance, sodass die gesamte DB-Instance gesichert wird. Sie können im System spezifische Aufbewahrungsfristen festlegen, um Ihre Ausfallsicherheitsanforderungen zu erfüllen.
CIS.10	dynamodb-pitr-enabled	Aktivieren Sie diese Regel, um zu überprüfen, ob die Informationen gesichert wurden. Es verwaltet auch die Backups, indem es sicherstellt, dass die point-in-time Wiederherstellung in Amazon DynamoDB aktiviert ist. Bei der Wiederherstellung werden fortlaufende Backups Ihrer Tabelle für die letzten 35 Tage gespeichert.

Kontroll-ID	AWS Config Regel	Empfehlungen
CIS.10	elasticache-redis-cluster-automatic-Backup-Prüfung	Wenn automatische Backups aktiviert sind, ElastiCache erstellt Amazon täglich ein Backup des Clusters. Die Sicherung kann für eine von Ihrer Organisation festgelegte Anzahl von Tagen aufbewahrt werden. Automatische Backups schützen vor Datenverlust. Bei einem Ausfall können Sie einen neuen Cluster erstellen, der Ihre Daten aus dem aktuellen Backup wiederherstellt.
CIS.10	s-3 bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) unterstützt die Aufrechterhaltung einer angemessenen Kapazität und Verfügbarkeit. CRR ermöglicht das automatische, asynchrone Kopieren von Objekten in Amazon-S3-Buckets, um die Datenverfügbarkeit sicherzustellen.

Kontroll-ID	AWS Config Regel	Empfehlungen
CIS.10	s-3 bucket-versioning-enabled	Die Versionsverwaltung von Amazon Simple Storage Service (Amazon S3)-Buckets hilft dabei, mehrere Varianten eines Objekts im selben Amazon-S3-Bucket zu speichern. Verwenden Sie die Versionsverwaltung, um sämtliche Versionen aller Objekte in Ihrem Amazon-S3-Bucket zu speichern, abzurufen oder wiederher zustellen. Mit der Versionsv erwaltung können Sie Versionen sowohl nach unbeabsichtigten Benutzera ktionen als auch nach Anwendungsfehlern problemlo s wiederherstellen.
CIS.11	ec2-eni security-group-att ached-to	Diese Regel stellt sicher, dass die Sicherheitsgruppen an eine Amazon Elastic Compute Cloud (Amazon EC2) - Instance oder an eine ENI angehängt sind. Diese Regel unterstützt die Überwachu ng ungenutzter Sicherhei tsgruppen im Bestand und die Verwaltung Ihrer Umgebung.

Kontroll-ID	AWS Config Regel	Empfehlungen
CIS.11	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) Security Groups können bei der Verwaltung des Netzwerkz ugriffs helfen, indem sie eine statusbehaftete Filterung von eingehendem und ausgehend em Netzwerkverkehr zu Ressourcen bereitstellen. AWS Wenn Sie eingehenden (oder entfernten) Datenverk ehr von 0.0.0.0/0 bis Port 22 auf Ihren Ressourcen nicht zulassen, können Sie den Remote-Zugriff einschränken.

Kontroll-ID	AWS Config Regel	Empfehlungen
CIS.11	restricted-common-ports	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass gemeinsame Ports für Amazon Elastic Compute Cloud (Amazon EC2) - Sicherheitsgruppen eingeschränkt sind. Wenn der Zugriff auf Ports nicht auf vertrauenswürdige Quellen beschränkt wird, kann dies zu Angriffen auf die Verfügbarkeit, Integrität und Vertraulichkeit von Systemen führen. Mit dieser Regel können Sie optional die Parameter blockedPort1–blockedPort5 festlegen (Standardkonfigurationen: 20, 21, 3389, 3306, 4333). Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	AWS Config Regel	Empfehlungen
CIS.11	vpc-default-security-group-geschlossen	Sicherheitsgruppen von Amazon Elastic Compute Cloud (Amazon EC2) können bei der Verwaltung des Netzwerkzugriffs helfen, indem sie eine statusbeh aftete Filterung des ein- und ausgehenden Netzwerkv erkehrs zu Ressourcen bereitstellen. AWS Die Beschränkung des gesamten Datenverkehrs auf die Standardsicherheitsgruppe hilft dabei, den Fernzugriff auf Ihre Ressourcen einzuschr änken. AWS

Kontroll-ID	AWS Config Regel	Empfehlungen
CIS.11	vpc-sg-open-only-to-authorized-ports	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass gemeinsame Ports für Amazon Elastic Compute Cloud (Amazon EC2) - Sicherheitsgruppen eingeschränkt sind. Wenn der Zugriff auf Ports nicht auf vertrauenswürdige Quellen beschränkt wird, kann dies zu Angriffen auf die Verfügbarkeit, Integrität und Vertraulichkeit von Systemen führen. Durch die Beschränkung des Zugriffs auf Ressourcen innerhalb einer Sicherheitsgruppe aus dem Internet (0.0.0.0/0) kann der Remote-Zugriff auf interne Systeme gesteuert werden.
CIS.12	dms-replication-not-public	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass auf DMS-Replikationsinstanzen nicht öffentlich zugegriffen werden kann. DMS-Replikations-Instances können vertrauliche Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	AWS Config Regel	Empfehlungen
CIS.12	ebs-snapshot-public-restorable-überprüfen	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass EBS-Snapshots nicht öffentlich wiederherstellbar sind. EBS-Volume-Snapshots können vertrauliche Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.
CIS.12	ec-2 instance-no-public-ip	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon Elastic Compute Cloud (Amazon EC2) -Instances nicht öffentlich zugänglich sind. EC2Amazon-Instances können vertrauliche Informationen enthalten, und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	AWS Config Regel	Empfehlungen
CIS.12	elasticsearch-in-vpc-only	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass sich Amazon OpenSearch OpenSearch Service (Service) -Domains innerhalb einer Amazon Virtual Private Cloud (Amazon VPC) befinden. Eine OpenSearch Service-Domain innerhalb einer Amazon VPC ermöglicht die sichere Kommunikation zwischen OpenSearch Service und anderen Services innerhalb der Amazon VPC, ohne dass ein Internet-Gateway, ein NAT-Gerät oder eine VPN-Verbindung erforderlich ist.
CIS.12	emr-master-no-public-ip	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon EMR-Cluster-Masterknoten nicht öffentlich zugänglich sind. Amazon-EMR-Cluster-Hauptknoten können vertrauliche Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	AWS Config Regel	Empfehlungen
CIS.12	guardduty-enabled-centralized	Amazon GuardDuty kann mithilfe von Threat Intellige nce Feeds helfen, potenzielle Cybersicherheitsereignisse zu überwachen und zu erkennen. Dazu gehören Listen mit bösartigen IPs und maschinel len Lernmethoden zur Identifiz ierung unerwarteter, nicht autorisierter und bösartige r Aktivitäten in Ihrer AWS Cloud-Umgebung.
CIS.12	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) Security Groups können bei der Verwaltung des Netzwerkz ugriffs helfen, indem sie eine statusbehaftete Filterung von eingehendem und ausgehend em Netzwerkverkehr zu Ressourcen bereitstellen. AWS Wenn Sie eingehenden (oder entfernten) Datenverk ehr von 0.0.0.0/0 bis Port 22 auf Ihren Ressourcen nicht zulassen, können Sie den Remote-Zugriff einschränken.

Kontroll-ID	AWS Config Regel	Empfehlungen
CIS.12	ec2- instances-in-vpc	Stellen Sie Amazon Elastic Compute Cloud (Amazon EC2) -Instances innerhalb einer Amazon Virtual Private Cloud (Amazon VPC) bereit, um eine sichere Kommunika tion zwischen einer Instance und anderen Services innerhalb der Amazon VPC zu ermöglichen, ohne dass ein Internet-Gateway, ein NAT-Gerät oder eine VPN-Verbindung erforderlich ist. Der gesamte Datenverkehr bleibt sicher in der AWS Cloud. Domänen, die sich innerhalb einer Amazon VPC befinden, verfügen aufgrund ihrer logischen Isolierung im Vergleich zu Domänen, die öffentliche Endpunkte nutzen, über eine zusätzlic he Sicherheitsebene. Weisen Sie EC2 Amazon-Instances einer Amazon-VPC zu, um den Zugriff ordnungsgemäß zu verwalten.

Kontroll-ID	AWS Config Regel	Empfehlungen
CIS.12	internet-gateway-authorized-vpc-nur	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Internet-Gateways nur mit autorisierter Amazon Virtual Private Cloud (Amazon VPC) verbunden sind. Internet-Gateways ermöglichen den bidirekti onalen Internetzugang zur und von der Amazon VPC, was möglicherweise zu einem unbefugten Zugriff auf Amazon-VPC-Ressourcen führen kann.
CIS.12	lambda-function-public-acce ss-verboten	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherste llen, dass AWS Lambda-Funktionen nicht öffentlich zugänglich sind. Der öffentlic he Zugriff kann möglicher weise die Verfügbarkeit von Ressourcen beeinträchtigen.

Kontroll-ID	AWS Config Regel	Empfehlungen
CIS.12	lambda-inside-vpc	Stellen Sie AWS Lambda-Funktionen in einer Amazon Virtual Private Cloud (Amazon VPC) bereit, um eine sichere Kommunikation zwischen einer Funktion und anderen Diensten innerhalb der Amazon VPC zu gewährleisten. Bei dieser Konfiguration sind kein Internet-Gateway, kein NAT-Gerät und keine VPN-Verbindung erforderlich. Der gesamte Datenverkehr bleibt sicher in der Cloud. AWS Domains, die sich innerhalb einer VPC befinden, verfügen aufgrund ihrer logischen Isolierung im Vergleich zu Domains mit öffentlichen Endpunkten über eine zusätzliche Sicherheitsebene. Um den Zugriff ordnungsgemäß zu verwalten, sollten AWS Lambda-Funktionen einer VPC zugewiesen werden.

Kontroll-ID	AWS Config Regel	Empfehlungen
CIS.12	rds-instance-public-access-überprüfen	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Relational Database Service (Amazon RDS) -Instances nicht öffentlich sind. Amazon-RDS-Datenbank-Instances können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.
CIS.12	rds-snapshots-public-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Relational Database Service (Amazon RDS) -Instances nicht öffentlich sind. Amazon-RDS-Datenbank-Instances können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	AWS Config Regel	Empfehlungen
CIS.12	redshift-cluster-public-access-überprüfen	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Redshift Redshift-Cluster nicht öffentlich sind. Amazon-Redshift-Cluster können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.
CIS.12	restricted-common-ports	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass gemeinsame Ports für Amazon Elastic Compute Cloud (Amazon EC2) - Sicherheitsgruppen eingeschränkt sind. Wenn der Zugriff auf Ports nicht auf vertrauenswürdige Quellen beschränkt wird, kann dies zu Angriffen auf die Verfügbarkeit, Integrität und Vertraulichkeit von Systemen führen. Mit dieser Regel können Sie optional die Parameter blockedPort1–blockedPort5 festlegen (Standardkonfigurationen: 20, 21, 3389, 3306, 4333). Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	AWS Config Regel	Empfehlungen
CIS.12	account-level-public-accesss3-Blöcke	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Simple Storage Service (Amazon S3) -Buckets nicht öffentlich zugänglich sind. Diese Regel trägt dazu bei, sensible Daten vor unbefugten Remote-Benutzern zu schützen, indem sie den öffentlichen Zugriff verhindert. Mit dieser Regel können Sie optional die Parameter ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) und restrictPublicBuckets Parameter (Config Default: True) festlegen. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	AWS Config Regel	Empfehlungen
CIS.12	s3- bucket-public-read-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie nur autorisierten Benutzern, Prozessen und Geräten Zugriff auf Amazon Simple Storage Service (Amazon S3) -Buckets gewähren. Die Verwaltung des Zugriffs sollte mit der Klassifizierung der Daten übereinstimmen.
CIS.12	s3- bucket-public-write-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie nur autorisierten Benutzern, Prozessen und Geräten Zugriff auf Amazon Simple Storage Service (Amazon S3) -Buckets gewähren. Die Verwaltung des Zugriffs sollte mit der Klassifizierung der Daten übereinstimmen.
CIS.12	sagemaker-notebook-no-direct-Internetzugang	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass SageMaker Amazon-Notebooks keinen direkten Internetzugang zulassen. Indem Sie direkten Internetzugang blockieren, vermeiden Sie, dass unbefugte Benutzer auf sensible Daten zugreifen.

Kontroll-ID	AWS Config Regel	Empfehlungen
CIS.12	securityhub-enabled	AWS Security Hub hilft bei der Überwachung von unbefugte m Personal, Verbindungen, Geräten und Software. AWS Security Hub aggregiert, organisiert und priorisiert die Sicherheitswarnungen oder Ergebnisse mehrerer Dienste. AWS Einige dieser Dienste sind Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer und AWS Firewall Manager sowie AWS Partnerlösungen.
CIS.12	vpc-default-security-group-geschlossen	Sicherheitsgruppen von Amazon Elastic Compute Cloud (Amazon EC2) können bei der Verwaltung des Netzwerkzugriffs helfen, indem sie eine statusbeh aftete Filterung des ein- und ausgehenden Netzwerkv erkehrs zu Ressourcen bereitstellen. AWS Die Beschränkung des gesamten Datenverkehrs auf die Standardsicherheitsgruppe hilft dabei, den Fernzugriff auf Ihre Ressourcen einzuschr änken. AWS

Kontroll-ID	AWS Config Regel	Empfehlungen
CIS.12	vpc-sg-open-only-to-authorized-ports	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass gemeinsame Ports für Amazon Elastic Compute Cloud (Amazon EC2) - Sicherheitsgruppen eingeschränkt sind. Wenn der Zugriff auf Ports nicht auf vertrauenswürdige Quellen beschränkt wird, kann dies zu Angriffen auf die Verfügbarkeit, Integrität und Vertraulichkeit von Systemen führen. Durch die Beschränkung des Zugriffs auf Ressourcen innerhalb einer Sicherheitsgruppe aus dem Internet (0.0.0.0/0) kann der Remote-Zugriff auf interne Systeme gesteuert werden.

Kontroll-ID	AWS Config Regel	Empfehlungen
CIS.13	acm-certificate-expiration-check	Stellen Sie sicher, dass die Netzwerkintegrität geschützt ist, indem Sie sicherstellen, dass X509-Zertifikate von AWS ACM ausgestellt werden. Diese Zertifikate müssen gültig und dürfen nicht abgelaufe n sein. Für diese Regel ist ein Wert für erforderlich daysToExpiration (Wert für bewährte AWS Grundrege ln für Sicherheit: 90). Der tatsächliche Wert muss den Richtlinien Ihrer Organisation entsprechen.
CIS.13	alb-http-to-https-Umleitung sprüfung	Um Daten während der Übertragung zu schützen, stellen Sie sicher, dass Ihr Application Load Balancer unverschlüsselte HTTP-Anfragen automatisch an HTTPS umleitet. Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	AWS Config Regel	Empfehlungen
CIS.13	api-gw-cache-enabled-und-verschlüsselt	Aktivieren Sie die Verschlüsselung für den Cache Ihrer API-Gateway-Stufe, um Daten im Ruhezustand zu schützen. Da für die API-Methode sensible Daten erfasst werden können, sollten Sie die Verschlüsselung von Daten im Ruhezustand aktivieren, um diese Daten zu schützen.
CIS.13	cloud-trail-encryption-enabled	Da sensible Daten vorhanden sein können und um Daten im Ruhezustand zu schützen, sollten Sie sicherstellen, dass die Verschlüsselung für Ihre AWS CloudTrail Trails aktiviert ist.
CIS.13	cloudwatch-log-group-encrypted	Um sensible Daten im Speicher zu schützen, stellen Sie sicher, dass die Verschlüsselung für Ihre Amazon CloudWatch Log Groups aktiviert ist.

Kontroll-ID	AWS Config Regel	Empfehlungen
CIS.13	ec2- ebs-encryption-by-default	Zum Schutz von Daten im Ruhezustand müssen Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon Elastic Block Store (Amazon EBS)-Volumes aktiviert ist. Da sensible Daten auch im Ruhezusta nd vorhanden sein können, sollten Sie die Verschlüs selung im Ruhezustand aktivieren, um diese Daten zu schützen.
CIS.13	efs-encrypted-check	Aktivieren Sie die Verschlüs selung für Ihr Amazon Elastic File System (EFS), um eventuell vorhandene sensible Daten sowie Daten im Ruhezustand zu schützen.
CIS.13	elasticsearch-encrypted-at-rest	Da sensible Daten vorhanden sein können und um Daten im Ruhezustand zu schützen, sollten Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon OpenSearch Service (OpenSearch Service) -Domains aktiviert ist.

Kontroll-ID	AWS Config Regel	Empfehlungen
CIS.13	elb-acm-certificate-required	Zum Schutz von eventuell vorhandenen sensiblen Daten sowie von Daten während der Übertragung muss die Verschlüsselung für Ihr Elastic Load Balancing aktiviert sein. Verwenden Sie AWS Certifica te Manager, um öffentlic he und private SSL/TLS-Z ertifikate mit AWS Diensten und internen Ressourcen zu verwalten, bereitzustellen und bereitzustellen.
CIS.13	encrypted-volumes	Aktivieren Sie die Verschlüs selung für Ihre Amazon-El astic-Block-Store (Amazon-EBS)-Volumes, um eventuell vorhandene sensible Daten sowie Daten im Ruhezustand zu schützen.
CIS.13	guardduty-enabled-centralized	Amazon GuardDuty kann mithilfe von Threat Intellige nce Feeds helfen, potenzielle Cybersicherheitsereignisse zu überwachen und zu erkennen. Dazu gehören Listen mit bösartigen IPs und maschinel len Lernmethoden zur Identifiz ierung unerwarteter, nicht autorisierter und bösartige r Aktivitäten in Ihrer AWS Cloud-Umgebung.

Kontroll-ID	AWS Config Regel	Empfehlungen
CIS.13	kms-cmk-not-scheduled-zum Löschen	Um Daten im Ruhezustand zu schützen, sollten Sie sicherstellen, dass die für den Kunden erforderlichen Masterschlüssel (CMKs) nicht für das Löschen im AWS Key Management Service (AWS KMS) vorgesehen sind. Da Schlüssel manchmal gelöscht werden müssen, können Sie mit dieser Regel alle zu löschenden Schlüssel überprüfen, falls ein Schlüssel versehentlich zur Löschung vorgemerkt wurde.
CIS.13	rds-snapshot-encrypted	Stellen Sie sicher, dass die Verschlüsselung für Ihre Amazon Relational Database Service (Amazon RDS)-Snapshots aktiviert ist. Da sensible Daten auch im Ruhezustand vorhanden sein können, sollten Sie die Verschlüsselung im Ruhezustand aktivieren, um diese Daten zu schützen.

Kontroll-ID	AWS Config Regel	Empfehlungen
CIS.13	rds-storage-encrypted	Zum Schutz von Daten im Ruhezustand müssen Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon Relational Database Service (Amazon RDS)-Instances aktiviert ist. Um eventuell vorhandene sensible Daten im Ruhezustand in Amazon-RDS-Instanc es zu schützen, muss die Verschlüsselung von Daten im Ruhezustand aktiviert sein.

Kontroll-ID	AWS Config Regel	Empfehlungen
CIS.13	redshift-cluster-configuration-check	Um Daten im Ruhezustand zu schützen, muss die Verschlüsselung für Ihre Amazon-Redshift-Cluster aktiviert sein. Sie müssen auch sicherstellen, dass die erforderlichen Konfigurationen auf Amazon-Redshift-Clustern bereitgestellt werden. Die Prüfungsprotokollierung muss aktiviert sein, um Informationen zu Verbindungen und Benutzeraktivitäten in der Datenbank bereitzustellen. Diese Regel erfordert, dass ein Wert für clusterDbEncrypted (Config Default: TRUE) und LoggingEnabled (Config Default: TRUE) gesetzt ist. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.
CIS.13	redshift-require-tls-ssl	Stellen Sie sicher, dass Ihre Amazon-Redshift-Cluster eine TLS/SSL-Verschlüsselung erfordern, um eine Verbindung zu SQL-Clients herzustellen. Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	AWS Config Regel	Empfehlungen
CIS.13	s3- bucket-default-lock-enabled	Stellen Sie sicher, dass für Ihren Amazon Simple Storage Service (Amazon S3)-Bucket standardmäßig eine Sperre aktiviert ist. Zum Schutz eventuell vorhandener sensibler Daten in S3-Bucket s müssen Sie Objektsperren für Daten im Ruhezustand erzwingen.
CIS.13	s3- bucket-server-side-encryption -aktiviert	Zum Schutz von Daten im Ruhezustand müssen Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon Simple Storage Service (Amazon S3)-Bucke ts aktiviert ist. Um eventuell vorhandene sensible Daten im Ruhezustand in Amazon-S3 -Buckets zu schützen, muss die Verschlüsselung aktiviert sein.

Kontroll-ID	AWS Config Regel	Empfehlungen
CIS.13	s-3 bucket-ssl-requests-only	Um Daten während der Übertragung zu schützen, stellen Sie sicher, dass Ihre Amazon Simple Storage Service (Amazon S3)-Bucke ts Anfragen zur Verwendun g von Secure Socket Layer (SSL)-Buckets erfordern. Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.
CIS.13	sagemaker-endpoint-configur ation-kms-key-konfiguriert	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass die Verschlüsselung mit dem AWS Key Managemen t Service (AWS KMS) für Ihren Endpunkt aktiviert ist. SageMaker Da sensible Daten auf dem SageMaker Endgerät gespeichert werden können, sollten Sie die Verschlüs selung im Ruhezustand aktivieren, um diese Daten zu schützen.

Kontroll-ID	AWS Config Regel	Empfehlungen
CIS.13	sagemaker-notebook-instance-kms-schlüsselkonfiguriert	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass die Verschlüsselung mit dem AWS Key Management Service (AWS KMS) für Ihr Notebook aktiviert ist. SageMaker Da vertrauliche Daten im SageMaker Notebook gespeichert werden können, sollten Sie die Verschlüsselung im Ruhezustand aktivieren, um diese Daten zu schützen.
CIS.13	sns-encrypted-kms	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass Ihre Amazon Simple Notification Service (Amazon SNS) -Themen mit dem AWS Key Management Service (AWS KMS) verschlüsselt werden müssen. Um eventuell vorhandene sensible Daten im Ruhezustand in veröffentlichten Nachrichten zu schützen, muss die Verschlüsselung von Daten im Ruhezustand aktiviert sein.

Kontroll-ID	AWS Config Regel	Empfehlungen
CIS.14	acm-certificate-expiration-check	Stellen Sie sicher, dass die Netzwerkintegrität geschützt ist, indem Sie sicherstellen, dass X509-Zertifikate von AWS ACM ausgestellt werden. Diese Zertifikate müssen gültig und dürfen nicht abgelaufe n sein. Für diese Regel ist ein Wert für erforderlich daysToExpiration (Wert für bewährte AWS Grundrege ln für Sicherheit: 90). Der tatsächliche Wert muss den Richtlinien Ihrer Organisation entsprechen.
CIS.14	alb-http-to-https-Umleitung sprüfung	Um Daten während der Übertragung zu schützen, stellen Sie sicher, dass Ihr Application Load Balancer unverschlüsselte HTTP-Anfragen automatisch an HTTPS umleitet. Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	AWS Config Regel	Empfehlungen
CIS.14	api-gw-cache-enabled-und-verschlüsselt	Aktivieren Sie die Verschlüsselung für den Cache Ihrer API-Gateway-Stufe, um Daten im Ruhezustand zu schützen. Da für die API-Methode sensible Daten erfasst werden können, sollten Sie die Verschlüsselung von Daten im Ruhezustand aktivieren, um diese Daten zu schützen.
CIS.14	cloud-trail-encryption-enabled	Da sensible Daten vorhanden sein können und um Daten im Ruhezustand zu schützen, sollten Sie sicherstellen, dass die Verschlüsselung für Ihre AWS CloudTrail Trails aktiviert ist.
CIS.14	cloudwatch-log-group-encrypted	Um sensible Daten im Speicher zu schützen, stellen Sie sicher, dass die Verschlüsselung für Ihre Amazon CloudWatch Log Groups aktiviert ist.

Kontroll-ID	AWS Config Regel	Empfehlungen
CIS.14	dms-replication-not-public	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass auf DMS-Replikationsinstanzen nicht öffentlich zugegriffen werden kann. DMS-Replikations-Instances können vertrauliche Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.
CIS.14	ebs-snapshot-public-restorable-überprüfen	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass EBS-Snapshots nicht öffentlich wiederherstellbar sind. EBS-Volume-Snapshots können vertrauliche Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.
CIS.14	ec-2 ebs-encryption-by-default	Zum Schutz von Daten im Ruhezustand müssen Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon Elastic Block Store (Amazon EBS)-Volumes aktiviert ist. Da sensible Daten auch im Ruhezustand vorhanden sein können, sollten Sie die Verschlüsselung im Ruhezustand aktivieren, um diese Daten zu schützen.

Kontroll-ID	AWS Config Regel	Empfehlungen
CIS.14	ec2- instance-no-public-ip	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon Elastic Compute Cloud (Amazon EC2) -Instances nicht öffentlich zugänglich sind. EC2Amazon-Instances können vertrauliche Informati onen enthalten, und für solche Konten ist eine Zugriffsk ontrolle erforderlich.
CIS.14	efs-encrypted-check	Aktivieren Sie die Verschlüs selung für Ihr Amazon Elastic File System (EFS), um eventuell vorhandene sensible Daten sowie Daten im Ruhezustand zu schützen.
CIS.14	elasticsearch-encrypted-at-rest	Da sensible Daten vorhanden sein können und um Daten im Ruhezustand zu schützen, sollten Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon OpenSearch Service (OpenSearch Service) -Domains aktiviert ist.

Kontroll-ID	AWS Config Regel	Empfehlungen
CIS.14	elb-acm-certificate-required	Zum Schutz von eventuell vorhandenen sensiblen Daten sowie von Daten während der Übertragung muss die Verschlüsselung für Ihr Elastic Load Balancing aktiviert sein. Verwenden Sie AWS Certifica te Manager, um öffentlic he und private SSL/TLS-Z ertifikate mit AWS Diensten und internen Ressourcen zu verwalten, bereitzustellen und bereitzustellen.

Kontroll-ID	AWS Config Regel	Empfehlungen
CIS.14	emr-kerberos-enabled	Die Zugriffsberechtigungen und -autorisierungen können verwaltet und nach den Prinzipien der geringsten Berechtigung und Aufgabent rennung integriert werden, indem Kerberos für Amazon-EMR-Cluster aktiviert wird. In Kerberos werden Services und Benutzer, die sich authentifizieren müssen, als Prinzipale bezeichnet. Prinzipale befinden sich in einem Kerberos-Bereich. Innerhalb dieses Bereichs wird ein Kerberos-Server als Key Distribution Center (KDC) bezeichnet. Über diesen Server können sich Prinzipale authentifizieren. Die Authentifizierung im KDC erfolgt durch die Ausstellu ng von Authentifizierungs tickets. Das KDC unterhält eine Datenbank der Prinzipal e in seinem Bereich mit ihren Passwörtern und anderen administrativen Informationen zu jedem Prinzipal.

Kontroll-ID	AWS Config Regel	Empfehlungen
CIS.14	encrypted-volumes	Aktivieren Sie die Verschlüs selung für Ihre Amazon-El astic-Block-Store (Amazon-EBS)-Volumes, um eventuell vorhandene sensible Daten sowie Daten im Ruhezustand zu schützen.
CIS.14	kms-cmk-not-scheduled-zum Löschen	Um Daten im Ruhezusta nd zu schützen, sollten Sie sicherstellen, dass die für den Kunden erforderlichen Masterschlüssel (CMKs) nicht für das Löschen im AWS Key Management Service (AWS KMS) vorgesehen sind. Da Schlüssel manchmal gelöscht werden müssen, können Sie mit dieser Regel alle zu löschenden Schlüssel überprüfen, falls ein Schlüssel versehentlich zur Löschung vorgemerkt wurde.

Kontroll-ID	AWS Config Regel	Empfehlungen
CIS.14	rds-instance-public-access-überprüfen	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Relational Database Service (Amazon RDS) -Instances nicht öffentlich sind. Amazon-RDS-Datenbank-Instances können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.
CIS.14	rds-snapshot-encrypted	Stellen Sie sicher, dass die Verschlüsselung für Ihre Amazon Relational Database Service (Amazon RDS)-Snapshots aktiviert ist. Da sensible Daten auch im Ruhezustand vorhanden sein können, sollten Sie die Verschlüsselung im Ruhezustand aktivieren, um diese Daten zu schützen.

Kontroll-ID	AWS Config Regel	Empfehlungen
CIS.14	rds-snapshots-public-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Relational Database Service (Amazon RDS) -Instances nicht öffentlich sind. Amazon-RDS-Datenbank-Instances können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.
CIS.14	rds-storage-encrypted	Zum Schutz von Daten im Ruhezustand müssen Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon Relational Database Service (Amazon RDS)-Instances aktiviert ist. Um eventuell vorhandene sensible Daten im Ruhezustand in Amazon-RDS-Instances zu schützen, muss die Verschlüsselung von Daten im Ruhezustand aktiviert sein.

Kontroll-ID	AWS Config Regel	Empfehlungen
CIS.14	redshift-cluster-public-access-überprüfen	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Redshift Redshift-Cluster nicht öffentlich sind. Amazon-Redshift-Cluster können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.
CIS.14	redshift-require-tls-ssl	Stellen Sie sicher, dass Ihre Amazon-Redshift-Cluster eine TLS/SSL-Verschlüsselung erfordern, um eine Verbindung zu SQL-Clients herzustellen. Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	AWS Config Regel	Empfehlungen
CIS.14	s3-Blöcke account-level-public-access	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Simple Storage Service (Amazon S3) -Buckets nicht öffentlich zugänglich sind. Diese Regel trägt dazu bei, sensible Daten vor unbefugten Remote-Benutzern zu schützen, indem sie den öffentlichen Zugriff verhindert. Mit dieser Regel können Sie optional die Parameter ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) und restrictPublicBuckets Parameter (Config Default: True) festlegen. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	AWS Config Regel	Empfehlungen
CIS.14	s3- bucket-default-lock-enabled	Stellen Sie sicher, dass für Ihren Amazon Simple Storage Service (Amazon S3)-Bucket standardmäßig eine Sperre aktiviert ist. Zum Schutz eventuell vorhandener sensibler Daten in S3-Bucket s müssen Sie Objektsperren für Daten im Ruhezustand erzwingen.
CIS.14	s-3 bucket-policy-grantee-check	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie s3_bucket_policy_grantee_check aktivieren. Diese Regel prüft, ob der vom Amazon S3 S3-Bucket gewährte Zugriff durch die von Ihnen bereitgestellten AWS Principals, Verbundbe nutzer, Service Principals, IP-Adressen oder Amazon Virtual Private Cloud (Amazon VPC) IDs eingeschränkt ist.
CIS.14	s-3 bucket-public-read-prohibit ed	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie nur autorisie rten Benutzern, Prozessen und Geräten Zugriff auf Amazon Simple Storage Service (Amazon S3) -Buckets gewähren. Die Verwaltung des Zugriffs sollte mit der Klassifiz ierung der Daten übereinst immen.

Kontroll-ID	AWS Config Regel	Empfehlungen
CIS.14	s3- bucket-public-write-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie nur autorisierten Benutzern, Prozessen und Geräten Zugriff auf Amazon Simple Storage Service (Amazon S3) -Buckets gewähren. Die Verwaltung des Zugriffs sollte mit der Klassifizierung der Daten übereinstimmen.
CIS.14	s3-fähig bucket-server-side-encryption	Zum Schutz von Daten im Ruhezustand müssen Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon Simple Storage Service (Amazon S3)-Buckets aktiviert ist. Um eventuell vorhandene sensible Daten im Ruhezustand in Amazon-S3 -Buckets zu schützen, muss die Verschlüsselung aktiviert sein.

Kontroll-ID	AWS Config Regel	Empfehlungen
CIS.14	s-3 bucket-ssl-requests-only	Um Daten während der Übertragung zu schützen, stellen Sie sicher, dass Ihre Amazon Simple Storage Service (Amazon S3)-Bucke ts Anfragen zur Verwendun g von Secure Socket Layer (SSL)-Buckets erfordern. Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.
CIS.14	sagemaker-endpoint-configur ation-kms-key-konfiguriert	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass die Verschlüsselung mit dem AWS Key Managemen t Service (AWS KMS) für Ihren Endpunkt aktiviert ist. SageMaker Da sensible Daten auf dem SageMaker Endgerät gespeichert werden können, sollten Sie die Verschlüs selung im Ruhezustand aktivieren, um diese Daten zu schützen.

Kontroll-ID	AWS Config Regel	Empfehlungen
CIS.14	sagemaker-notebook-instance-kms-schlüsselkonfiguriert	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass die Verschlüsselung mit dem AWS Key Management Service (AWS KMS) für Ihr Notebook aktiviert ist. SageMaker Da vertrauliche Daten im SageMaker Notebook gespeichert werden können, sollten Sie die Verschlüsselung im Ruhezustand aktivieren, um diese Daten zu schützen.
CIS.14	sns-encrypted-kms	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass Ihre Amazon Simple Notification Service (Amazon SNS) -Themen mit dem AWS Key Management Service (AWS KMS) verschlüsselt werden müssen. Um eventuell vorhandene sensible Daten im Ruhezustand in veröffentlichten Nachrichten zu schützen, muss die Verschlüsselung von Daten im Ruhezustand aktiviert sein.

Kontroll-ID	AWS Config Regel	Empfehlungen
CIS.16	access-keys-rotated	Die Anmeldeinformationen für autorisierte Geräte, Benutzer und Prozesse werden geprüft, indem sichergestellt wird, dass die IAM-Zugriffsschlüssel gemäß den Vorgaben der Unternehmensrichtlinie rotiert werden. Das regelmäßige Ändern der Zugriffsschlüssel ist eine bewährte Sicherheitsmethode. Es verkürzt den Zeitraum, in dem ein Zugriffsschlüssel aktiv ist, und reduziert die Auswirkungen auf das Unternehmen, wenn die Schlüssel kompromittiert werden. Diese Regel erfordert einen Wert für die Zugriffsschlüssel-Rotation (Standardkonfiguration: 90). Der tatsächliche Wert muss den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	AWS Config Regel	Empfehlungen
CIS.16	cloudtrail-enabled	AWS CloudTrail kann durch die Aufzeichnung von Aktionen und API-Aufrufen in der AWS Management Console helfen, die Ablehnung zu verhindern. Sie können die Benutzer und die Benutzer AWS-Konten , die einen AWS Dienst aufgerufen haben, die Quell-IP-Adresse, über die die Aufrufe generiert wurden, und den Zeitpunkt der Anrufe identifizieren. Einzelheiten zu den erfassten Daten finden Sie in den AWS CloudTrail Datensatzinhalten.

Kontroll-ID	AWS Config Regel	Empfehlungen
CIS.16	cloudwatch-alarm-action-check	Amazon CloudWatch alarmiert, wenn eine Metrik den Schwellenwert für eine bestimmte Anzahl von Bewertungszeiträumen überschreitet. Der Alarm führt eine oder mehrere Aktionen durch, die vom Wert der Metrik oder des Ausdrucks im Vergleich zu einem Schwellenwert in einer Reihe von Zeiträumen abhängt. Diese Regel erfordert einen Wert für alarmActionRequired (Config Default: True), insufficientDataActionRequired (Config Default: True), okActionRequired (Config Default: False). Der tatsächliche Wert muss die Alarmaktionen für Ihre Umgebung widerspiegeln.

Kontroll-ID	AWS Config Regel	Empfehlungen
CIS.16	emr-kerberos-enabled	Die Zugriffsberechtigungen und -autorisierungen können verwaltet und nach den Prinzipien der geringsten Berechtigung und Aufgabent rennung integriert werden, indem Kerberos für Amazon-EMR-Cluster aktiviert wird. In Kerberos werden Services und Benutzer, die sich authentifizieren müssen, als Prinzipale bezeichnet. Prinzipale befinden sich in einem Kerberos-Bereich. Innerhalb dieses Bereichs wird ein Kerberos-Server als Key Distribution Center (KDC) bezeichnet. Über diesen Server können sich Prinzipale authentifizieren. Die Authentifizierung im KDC erfolgt durch die Ausstellu ng von Authentifizierungs tickets. Das KDC unterhält eine Datenbank der Prinzipal e in seinem Bereich mit ihren Passwörtern und anderen administrativen Informationen zu jedem Prinzipal.

Kontroll-ID	AWS Config Regel	Empfehlungen
CIS.16	guardduty-enabled-centralized	Amazon GuardDuty kann mithilfe von Threat Intelligence Feeds helfen, potenzielle Cybersicherheitsereignisse zu überwachen und zu erkennen. Dazu gehören Listen mit bösartigen IPs und maschinellen Lernmethoden zur Identifizierung unerwarteter, nicht autorisierter und bösartiger Aktivitäten in Ihrer AWS Cloud-Umgebung.
CIS.16	guardduty-non-archived-findings	Amazon GuardDuty hilft Ihnen dabei, die Auswirkungen eines Vorfalls zu verstehen, indem es die Ergebnisse nach Schweregrad klassifiziert: niedrig, mittel und hoch. Diese Klassifizierungen können Sie zur Festlegung von entsprechenden Strategien und Prioritäten zur Behebung solcher Vorfälle verwenden. Mit dieser Regel können Sie optional daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7) und daysHighSev (Config Default: 1) für nicht archivierte Ergebnisse festlegen, wie es die Richtlinien Ihrer Organisation erfordern.

Kontroll-ID	AWS Config Regel	Empfehlungen
CIS.16	iam-password-policy	Die Identitäten und Anmeldein formationen werden auf der Grundlage einer organisat orischen IAM-Passwortrichtl inie ausgestellt, verwaltet und verifiziert. Sie erfüllen oder übertreffen die Anforderungen von NIST SP 800-63 und dem Benchmark der Centers for Internet Security (CIS) AWS Foundations in Bezug auf die Passwortstärke. Mit dieser Regel können Sie optional RequireUppercaseCharacters (Wert für AWS grundlege nde Sicherheitsbewährte Methoden: wahr), RequireLo wercaseCharacters (Wert für bewährte Methoden für AWS grundlegende Sicherhei t: wahr), RequireSymbols (Wert für bewährte Methoden für AWS grundlegende Sicherheit: wahr), RequireNu mbers (Wert für bewährte Methoden für AWS grund legende Sicherheit: wahr), MinimumPasswordLength (Wert für bewährte Methoden für AWS grundlegende Sicherheit: 14), PasswordR eusePrevention (Wert für bewährte Methoden für AWS grundlegende Sicherheit:

Kontroll-ID	AWS Config Regel	Empfehlungen
		24) und MaxPasswordAge (Wert für bewährte Methoden für AWS grundlegende Sicherheit: 90) für Ihr IAM festlegen Kennwortrichtlinie . Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.
CIS.16	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) kann Ihnen dabei helfen, die Prinzipien der geringsten Rechte und der Aufgabent rennung in Zugriffsberechtigu ngen und Autorisierungen zu integrieren und zu verhinder n, dass Richtlinien „Effect“: „Allow“ mit „Action“: „*“ anstelle von „Resource“: „*“ enthalten. Wenn Benutzern mehr Rechte eingeräumt werden, als für die Ausführun g einer Aufgabe erforderl ich sind, kann dies gegen das Prinzip der geringste n Berechtigung und der Aufgabentrennung verstoßen.

Kontroll-ID	AWS Config Regel	Empfehlungen
CIS.16	iam-root-access-key-überprüfen	Der Zugriff auf Systeme und Ressourcen kann gesteuert werden, indem überprüft wird, ob der Root-Benutzer keine Zugriffsschlüssel mit seiner AWS Identity and Access Management (IAM) -Rolle verknüpft hat. Stellen Sie sicher, dass die Root-Zugriffsschlüssel gelöscht werden. Erstellen und verwenden Sie stattdessen rollenbasierte Funktionen, AWS-Konten um das Prinzip der geringsten Funktionalität zu berücksichtigen.
CIS.16	iam-user-group-membership-überprüfen	AWS Identity and Access Management (IAM) kann Ihnen helfen, Zugriffsberechtigungen und Autorisierungen einzuschränken, indem sichergestellt wird, dass Benutzer Mitglieder mindestens einer Gruppe sind. Wenn Benutzern mehr Berechtigungen eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und Aufgabentrennung verstoßen.

Kontroll-ID	AWS Config Regel	Empfehlungen
CIS.16	iam-user-mfa-enabled	Aktivieren Sie diese Regel, um den Zugriff auf Ressourcen in der AWS -Cloud einzuschränken. Diese Regel stellt sicher, dass die Multi-Faktor-Authentifizierung (MFA) für alle Benutzer aktiviert ist. MFA bietet eine weitere Schutzebene zusätzlich zum Benutzernamen und Passwort. Reduzieren Sie Fälle von kompromittierten Konten, indem Sie MFA für Benutzer vorschreiben.
CIS.16	iam-user-no-policies-überprüfen	Diese Regel stellt sicher, dass AWS Identity and Access Management (IAM) -Richtlinien nur Gruppen oder Rollen zugewiesen werden, um den Zugriff auf Systeme und Ressourcen zu kontrollieren. Die Zuweisung von Berechtigungen auf Gruppen- oder Rollenebene trägt dazu bei, die Wahrscheinlichkeit zu verringern, dass eine Identität übermäßige Berechtigungen erhält oder beibehält.

Kontroll-ID	AWS Config Regel	Empfehlungen
CIS.16	iam-user-unused-credentials-überprüfen	AWS Identity and Access Management (IAM) kann Ihnen bei Zugriffsberechtigungen und Autorisierungen helfen, indem es nach IAM-Passwörtern und Zugriffsschlüsseln sucht, die für einen bestimmten Zeitraum nicht verwendet wurden. Wenn ungenutzte Anmeldeinformationen identifiziert werden, müssen Sie sie deaktivieren und/oder entfernen, da dies gegen das Prinzip der geringsten Berechtigung verstoßen könnte. Für diese Regel müssen Sie einen Wert für das maxCredentialUsage Alter festlegen (Standardkonfiguration: 90). Der tatsächliche Wert muss den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	AWS Config Regel	Empfehlungen
CIS.16	mfa-enabled-for-iam-Konsolenzugriff	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass MFA für alle AWS Identity and Access Management (IAM) -Benutzer aktiviert ist, die über ein Konsolenkennwort verfügen. MFA sorgt für eine weitere Schutzebene zusätzlich zu den Anmeldeinformationen. Indem Sie MFA für Benutzer vorschreiben, können Sie Fälle kompromittierter Konten reduzieren und verhindern, dass unbefugte Benutzer auf vertrauliche Daten zugreifen.
CIS.16	root-account-hardware-mfa-aktiviert	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Hardware-MFA für den Root-Benutzer aktiviert ist. Der Stammbenutzer ist der AWS-Konto-Benutzer mit den meisten Berechtigungen. MFA sorgt für eine weitere Schutzebene zusätzlich zu den Anmeldeinformationen. Indem Sie MFA für den Root-Benutzer vorschreiben, können Sie die Anzahl AWS-Konten kompromittierter Benutzer reduzieren.

Kontroll-ID	AWS Config Regel	Empfehlungen
CIS.16	root-account-mfa-enabled	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass MFA für den Root-Benutzer aktiviert ist. Der Stammbenutzer ist der AWS-Konto-Benutzer mit den meisten Berechtigungen. MFA bietet eine weitere Schutzebene zusätzlich zum Benutzernamen und Passwort. Indem Sie MFA für den Root-Benutzer vorschreiben, können Sie die Anzahl AWS-Konten kompromittierter Benutzer reduzieren.
CIS.16	secretsmanager-rotation-enabled-check	Diese Regel stellt sicher, dass bei AWS Secrets Manager Manager-Geheimnissen die Rotation aktiviert ist. Die regelmäßige Rotation von Secrets kann den Zeitraum verkürzen, in dem ein Secret aktiv ist, und möglicherweise die Auswirkungen auf das Unternehmen verringern, falls das Secret kompromittiert wird.

Kontroll-ID	AWS Config Regel	Empfehlungen
CIS.16	secretsmanager-scheduled-rotation-success-überprüfen	Diese Regel stellt sicher, dass AWS Secrets Manager Manager-Geheimnisse gemäß dem Rotationsplan erfolgreich rotiert wurden. Die regelmäßige Rotation von Secrets kann den Zeitraum verkürzen, in dem ein Secret aktiv ist, und möglicherweise die Auswirkungen auf das Unternehmen verringern, falls es kompromittiert wird.
CIS.16	securityhub-enabled	AWS Security Hub hilft bei der Überwachung von unbefugtem Personal, Verbindungen, Geräten und Software. AWS Security Hub aggregiert, organisiert und priorisiert die Sicherheitswarnungen oder Ergebnisse mehrerer Dienste. AWS Einige dieser Dienste sind Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer und AWS Firewall Manager sowie AWS Partnerlösungen.

Kontroll-ID	AWS Config Regel	Empfehlungen
CIS.18	codebuild-project-envvar-awscred-überprüfen	Stellen Sie sicher, dass die Anmeldeinformationen AWS_ACCESS_KEY_ID AWS_SECRET_ACCESS_KEY nicht in AWS Codebuild -Projektumgebungen vorhanden sind. Speichern Sie diese Variablen nicht als Klartext. Das Speichern dieser Variablen als Klartext bewirkt eine unbeabsichtigte Offenlegung von Daten sowie unberechtigte Zugriffe.
CIS.18	codebuild-project-source-repo-URL-Prüfung	Stellen Sie sicher, dass die URL des Quell-Repositorys GitHub oder des Bitbucket -Quell-Repositorys keine persönlichen Zugriffstoken oder Anmeldeinformationen in Codebuild-Projektumgebungen enthält. AWS Verwende OAuth anstelle von persönlichen Zugriffstoken oder Anmeldedaten die Autorisierung für den Zugriff auf GitHub Bitbucket-Repositorys.

Kontroll-ID	AWS Config Regel	Empfehlungen
CIS.19	guardduty-enabled-centralized	Amazon GuardDuty kann mithilfe von Threat Intelligence Feeds helfen, potenzielle Cybersicherheitsereignisse zu überwachen und zu erkennen. Dazu gehören Listen mit bösartigen IPs und maschinellen Lernmethoden zur Identifizierung unerwarteter, nicht autorisierter und bösartiger Aktivitäten in Ihrer AWS Cloud-Umgebung.
CIS.19	guardduty-non-archived-findings	Amazon GuardDuty hilft Ihnen dabei, die Auswirkungen eines Vorfalls zu verstehen, indem es die Ergebnisse nach Schweregrad klassifiziert: niedrig, mittel und hoch. Diese Klassifizierungen können Sie zur Festlegung von entsprechenden Strategien und Prioritäten zur Behebung solcher Vorfälle verwenden. Mit dieser Regel können Sie optional daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7) und daysHighSev (Config Default: 1) für nicht archivierte Ergebnisse festlegen, wie es die Richtlinien Ihrer Organisation erfordern.

Kontroll-ID	AWS Config Regel	Empfehlungen
CIS.19	securityhub-enabled	AWS Security Hub hilft bei der Überwachung von unbefugte m Personal, Verbindungen, Geräten und Software. AWS Security Hub aggregiert, organisiert und priorisiert die Sicherheitswarnungen oder Ergebnisse mehrerer Dienste. AWS Einige dieser Dienste sind Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer und AWS Firewall Manager sowie AWS Partnerlösungen.

Kontroll-ID	AWS Config Regel	Empfehlungen
CIS.2	ec2-manager instance-managed-by-systems	Eine Bestandsaufnahme der Softwareplattformen und Anwendungen innerhalb des Unternehmens ist möglich, indem Amazon Elastic Compute Cloud (Amazon EC2) -Instances mit AWS Systems Manager verwaltet werden. Verwenden Sie AWS Systems Manager, um detaillierte Systemkonfigurationen, Betriebssystem-Patch-Levels, Namen und Typ der Dienste, Softwareinstallationen, Anwendungsname, Herausgeber und Version sowie andere Details zu Ihrer Umgebung bereitzustellen.

Vorlage

Die Vorlage ist verfügbar unter GitHub: Operational Best Practices for CIS Top 20.

Bewährte Methoden für die Ausführung von CISA Cyber Essentials

Konformitätspakete bieten ein allgemeines Compliance-Framework, das es Ihnen ermöglicht, mithilfe verwalteter oder benutzerdefinierter AWS Config Regeln und Abhilfemaßnahmen Kontrollen zur Sicherheits-, Betriebs- oder Kostenoptimierung durchzuführen. AWS Config Conformance Packs dienen als Beispielvorlagen nicht dazu, die vollständige Einhaltung eines bestimmten Governance- oder Compliance-Standards sicherzustellen. Sie sind dafür verantwortlich, selbst zu beurteilen, ob Ihre Nutzung der Services den geltenden gesetzlichen und behördlichen Anforderungen entspricht.

Im Folgenden finden Sie ein Beispiel für eine Zuordnung zwischen den Cyber Essentials (CE) der Cybersecurity & Infrastructure Security Agency (CISA) und AWS verwalteten Konfigurationsregeln. Jede AWS Config Regel gilt für eine bestimmte AWS Ressource und bezieht sich auf eine oder

mehrere CISA CE-Kontrollen. Eine CISA CE-Steuerung kann sich auf mehrere AWS Config Regeln beziehen. In der folgenden Tabelle finden Sie weitere Informationen und Anleitungen zu diesen Zuordnungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
Ihre Mitarbeiter-1	Entwickeln Sie eine Kultur des Bewusstseins, um die Mitarbeiter zu ermutigen, online gute Entscheidungen zu treffen.	security-awareness-program-exists(Prozessüberprüfung)	Etablieren und pflegen Sie ein Programm zur Förderung des Sicherheitsbewusstseins in Ihrer Organisation. Programme zur Förderung des Sicherheitsbewusstseins der Mitarbeiter vermitteln ihnen, wie sie ihre Organisation vor diversen Sicherheitsverletzungen oder Sicherheitsvorfällen schützen können.
Ihre Mitarbeiter-2	Erfahren Sie mehr über Risiken wie Phishing und die Kompromittierung von Geschäfts-E-Mails. XXXXX.	security-awareness-program-exists(Prozessüberprüfung)	Etablieren und pflegen Sie ein Programm zur Förderung des Sicherheitsbewusstseins in Ihrer Organisation. Programme zur Förderung des Sicherheitsbewusstseins der Mitarbeiter vermitteln ihnen, wie

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			sie ihre Organisation vor diversen Sicherheitsverletzungen oder Sicherheitsvorfällen schützen können.
Ihre Mitarbeiter-3	Seien Sie stets über aktuelle Ereignisse im Zusammenhang mit der Cybersicherheit informiert und nutzen Sie gewonnene Erkenntnisse und gemeldete Ereignisse, um im aktuellen Bedrohungsumfeld wachsam und bei Cybersicherheitstrends agil zu bleiben.	security-awareness-program-exists(Prozessüberprüfung)	Etablieren und pflegen Sie ein Programm zur Förderung des Sicherheitsbewusstseins in Ihrer Organisation. Programme zur Förderung des Sicherheitsbewusstseins der Mitarbeiter vermitteln ihnen, wie sie ihre Organisation vor diversen Sicherheitsverletzungen oder Sicherheitsvorfällen schützen können.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
Ihre Mitarbeiter-4	Nutzen Sie grundlegende Cybersicherheitsschulungen, um sich besser mit Konzepten, Terminologie und Aktivitäten im Zusammenhang mit der Implementierung von Best Practices im Bereich Cybersicherheit vertraut zu machen.	security-awareness-program-exists(Prozessüberprüfung)	Etablieren und pflegen Sie ein Programm zur Förderung des Sicherheitsbewusstseins in Ihrer Organisation. Programme zur Förderung des Sicherheitsbewusstseins der Mitarbeiter vermitteln ihnen, wie sie ihre Organisation vor diversen Sicherheitsverletzungen oder Sicherheitsvorfällen schützen können.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
Ihre Mitarbeiter-5	Identifizieren Sie verfügbare Schulungsressourcen von Berufsverbänden, akademischen Einrichtungen, dem privaten Sektor und staatlichen Quellen.	security-awareness-program-exists(Prozessüberprüfung)	Etablieren und pflegen Sie ein Programm zur Förderung des Sicherheitsbewusstseins in Ihrer Organisation. Programme zur Förderung des Sicherheitsbewusstseins der Mitarbeiter vermitteln ihnen, wie sie ihre Organisation vor diversen Sicherheitsverletzungen oder Sicherheitsvorfällen schützen können.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
Ihre Systeme-1	Erfahren Sie, was sich in Ihrem Netzwerk befindet. Führen Sie eine Bestandsaufnahme der Hardware- und Software-Ressourcen durch, um zu wissen, was im Einsatz ist und wie hoch das Risiko eines Angriffs ist.	eip-attached	Diese Regel stellt sicher, dass Elastic, die einer Amazon Virtual Private Cloud (Amazon VPC) IPs zugewiesen sind, an Amazon Elastic Compute Cloud (Amazon EC2) - Instances oder verwendete Elastic Network Interface s angehängt sind. Diese Regel hilft bei der Überwachu ng ungenutzter Inhalte EIPs in Ihrer Umgebung.
Ihre Systeme-1	Erfahren Sie, was sich in Ihrem Netzwerk befindet. Führen Sie eine Bestandsaufnahme der Hardware- und Software-Ressourcen durch, um zu wissen, was im Einsatz ist und wie hoch das Risiko eines Angriffs ist.	vpc-network-acl-un used-überprüfen	Diese Regel stellt sicher, dass Amazon Virtual Private Cloud (VPC)-Netzwerkzugr iffskontrolllisten verwendet werden. Die Überwachu ng ungenutzter Netzwerkzugriffsko ntrolllisten kann zu einer genauen Inventarisierung und Verwaltung Ihrer Umgebung beitragen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
Ihre Systeme-1	Erfahren Sie, was sich in Ihrem Netzwerk befindet. Führen Sie eine Bestandsaufnahme der Hardware- und Software-Ressourcen durch, um zu wissen, was im Einsatz ist und wie hoch das Risiko eines Angriffs ist.	ec2- -Manager instance-managed-by-systems	Eine Bestandsaufnahme der Softwareplattformen und Anwendungen innerhalb des Unternehmens ist möglich, indem Amazon Elastic Compute Cloud (Amazon EC2) - Instances mit AWS Systems Manager verwaltet werden. Verwenden Sie AWS Systems Manager, um detaillierte Systemkonfigurationen, Betriebssystem-Patch-Levels, Namen und Typ der Dienste, Softwareinstallationen, Anwendungsname, Herausgeber und Version sowie andere Details zu Ihrer Umgebung bereitzustellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
Ihre Systeme-1	Erfahren Sie, was sich in Ihrem Netzwerk befindet. Führen Sie eine Bestandsaufnahme der Hardware- und Software-Ressourcen durch, um zu wissen, was im Einsatz ist und wie hoch das Risiko eines Angriffs ist.	ec2-check managedinstance-association-compliance-status	Verwenden Sie AWS Systems Manager Associations, um bei der Inventarisierung von Softwareplattformen und Anwendungen innerhalb eines Unternehmens zu helfen. AWS Systems Manager weist Ihren verwalteten Instanzen einen Konfigurationsstatus zu und ermöglicht es Ihnen, Basiswerte für Betriebssystem-Patch-Levels, Softwareinstallationen, Anwendungskonfigurationen und andere Details zu Ihrer Umgebung festzulegen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
Ihre Systeme-1	Erfahren Sie, was sich in Ihrem Netzwerk befindet. Führen Sie eine Bestandsaufnahme der Hardware- und Software-Ressourcen durch, um zu wissen, was im Einsatz ist und wie hoch das Risiko eines Angriffs ist.	ec2-check managedinstance-patch-compliance-status	Aktivieren Sie diese Regel, um bei der Identifizierung und Dokumentation von Sicherheitslücken in Amazon Elastic Compute Cloud (Amazon EC2) zu helfen. Die Regel prüft, ob die EC2 Amazon-Instance die Patch-Konformität im AWS Systems Manager gemäß den Richtlinien und Verfahren Ihrer Organisation einhält.
Ihre Systeme-1	Erfahren Sie, was sich in Ihrem Netzwerk befindet. Führen Sie eine Bestandsaufnahme der Hardware- und Software-Ressourcen durch, um zu wissen, was im Einsatz ist und wie hoch das Risiko eines Angriffs ist.	ec2-stopped-instance	Aktivieren Sie diese Regel, um bei der Basiskonfiguration von Amazon Elastic Compute Cloud (Amazon EC2) - Instances zu helfen, indem Sie überprüfen, ob EC2 Amazon-Instances gemäß den Standards Ihrer Organisation für mehr als die zulässige Anzahl von Tagen gestoppt wurden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
Ihre Systeme-1	Erfahren Sie, was sich in Ihrem Netzwerk befindet. Führen Sie eine Bestandsaufnahme der Hardware- und Software-Ressourcen durch, um zu wissen, was im Einsatz ist und wie hoch das Risiko eines Angriffs ist.	ec2- volume-inuse-check	Diese Regel stellt sicher, dass Amazon Elastic Block Store-Volumes, die an Amazon Elastic Compute Cloud (Amazon EC2) - Instances angehängt sind, zum Löschen markiert werden, wenn eine Instance beendet wird. Wenn ein Amazon-EB S-Volume nicht gelöscht wird, wenn die Instance, an die es angehängt ist, beendet wird, kann dies gegen das Konzept der geringsten Funktiona lität verstoßen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
Ihre Systeme-2	Nutzen Sie automatische Updates für alle Betriebssysteme und Software von Drittanbietern.	ec2-check managedinstance-patch-compliance-status	Aktivieren Sie diese Regel, um bei der Identifizierung und Dokumentation von Sicherheitslücken in Amazon Elastic Compute Cloud (Amazon EC2) zu helfen. Die Regel prüft, ob die EC2 Amazon-Instance die Patch-Konformität im AWS Systems Manager gemäß den Richtlinien und Verfahren Ihrer Organisation einhält.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
Ihre Systeme-2	Nutzen Sie automatische Updates für alle Betriebssysteme und Software von Drittanbietern.	elastic-beanstalk-managed-updates-aktiviert	Durch die Aktivierung verwalteter Plattformupdates für eine Amazon-Elastic-Beanstalk-Umgebung wird sichergestellt, dass die aktuellen verfügbaren Plattform-Fixes, -Updates und -Features für die Umgebung installiert sind. Eine bewährte Methode zur Sicherung von Systemen besteht darin, stets die aktuellen Patches zu installieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
Ihre Systeme-2	Nutzen Sie automatische Updates für alle Betriebssysteme und Software von Drittanbietern.	redshift-cluster-maintenancesettings-check	Diese Regel stellt sicher, dass Amazon-Redshift-Cluster die bevorzugten Einstellungen für Ihre Organisation haben. Insbesondere sorgt sie dafür, dass Cluster bevorzugte Wartungsfenster und automatisierte Aufbewahrungsfristen für Snapshots für die Datenbank haben. Für diese Regel müssen Sie die allowVersionUpgrade festlegen. Der Standardwert ist „true“. Außerdem können Sie optional den Zeitraum preferredMaintenanceWindow (der Standardwert ist sa: 16:00 -sa: 16:30) und den automated SnapshotRetention Zeitraum (der Standardwert ist 1) festlegen. Die tatsächlichen Werte müssen den Richtlini

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			en Ihrer Organisation entsprechen.
Ihre Systeme-2	Nutzen Sie automatische Updates für alle Betriebssysteme und Software von Drittanbietern.	rds-automatic-minor-version-Upgrade aktiviert	Aktivieren Sie automatische Unterversions-Upgrades auf Ihren Amazon-Relational-Database-Service (RDS)-Instances, um sicherzustellen, dass die aktuellen Updates für Unterversionen des Relational Database Management System (RDBMS) installiert sind, die Sicherheitspatches und Bugfixes enthalten können.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
Ihre Systeme-3	Implementieren Sie Sicherheitskonfigurationen für alle Hardware- und Softwareressourcen.	access-keys-rotated	Die Anmeldeinformationen für autorisierte Geräte, Benutzer und Prozesse werden geprüft, indem sichergestellt wird, dass die IAM-Zugriffsschlüssel entsprechend den Vorgaben der Unternehmensrichtlinie rotiert werden. Das regelmäßige Ändern der Zugriffsschlüssel ist eine bewährte Sicherheitsmethode. Es verkürzt den Zeitraum, in dem ein Zugriffsschlüssel aktiv ist, und reduziert die Auswirkungen auf das Unternehmen, wenn die Schlüssel kompromittiert werden. Diese Regel erfordert einen Wert für die Zugriffsschlüssel-Rotation (Standardkonfiguration: 90). Der tatsächliche Wert muss den Richtlini

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			en Ihrer Organisation entsprechen.
Ihre Systeme-3	Implementieren Sie Sicherheitskonfigurationen für alle Hardware- und Softwareressourcen.	alb-http-to-https-Umleitungsprüfung	Um Daten während der Übertragung zu schützen, stellen Sie sicher, dass Ihr Application Load Balancer unverschlüsselte HTTP-Anfragen automatisch an HTTPS umleitet. Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
Ihre Systeme-3	Implementieren Sie Sicherheitskonfigurationen für alle Hardware- und Softwareressourcen.	alb-waf-enabled	Stellen Sie sicher, dass AWS WAF auf Elastic Load Balancers (ELB) aktiviert ist, um Webanwendungen zu schützen. Eine WAF trägt zum Schutz Ihrer Webanwendungen oder APIs vor gängigen Web-Exploits bei. Diese Web-Exploits können sich auf die Verfügbarkeit auswirken, die Sicherheit gefährden oder übermäßige Ressourcen in Ihrer Umgebung verbrauchen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
Ihre Systeme-3	Implementieren Sie Sicherheitskonfigurationen für alle Hardware- und Softwareressourcen.	api-gw-associated-with-WAF	AWS Mit WAF können Sie eine Reihe von Regeln (als Web Access Control List (Web ACL) bezeichnet) konfigurieren, die Webanfragen auf der Grundlage von anpassbaren Websicherheitsregeln und -bedingungen, die Sie definieren, zulassen, blockieren oder zählen. Stellen Sie sicher, dass Ihre Amazon-API-Gateway-Stufe mit einer WAF-Web-ACL verknüpft ist, um sie vor böswilligen Angriffen zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
Ihre Systeme-3	Implementieren Sie Sicherheitskonfigurationen für alle Hardware- und Softwareressourcen.	cloud-trail-log-file-Validierung aktiviert	Verwenden Sie die AWS CloudTrail Protokolldateivalidierung, um die Integrität von Protokollen zu überprüfen. CloudTrail Mithilfe der Protokolldateivalidierung kann festgestellt werden, ob eine Protokolldatei geändert oder gelöscht wurde oder ob sie nach der Übermittlung CloudTrail unverändert geblieben ist. Dieses Feature wurde mit dem Branchenstandard entsprechenden Algorithmen entwickelt: SHA-256 für die Hashfunktion und SHA-256 mit RSA für digitale Signaturen. Aus diesem Grund ist es rechnerisch unmöglich, CloudTrail Protokolldateien unbemerkt zu ändern, zu löschen oder zu fälschen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
Ihre Systeme-3	Implementieren Sie Sicherheitskonfigurationen für alle Hardware- und Softwareressourcen.	codebuild-project-envvar-awscred-überprüfen	Stellen Sie sicher, dass die Anmeldeinformationen AWS_ACCESS_KEY_ID AWS_SECRET_ACCESS_KEY nicht in AWS Codebuild-Projektumgebungen vorhanden sind. Speichern Sie diese Variablen nicht als Klartext. Das Speichern dieser Variablen als Klartext bewirkt eine unbeabsichtigte Offenlegung von Daten sowie unberechtigte Zugriffe.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
Ihre Systeme-3	Implementieren Sie Sicherheitskonfigurationen für alle Hardware- und Softwareressourcen.	codebuild-project-source-repo-URL-Prüfung	Stellen Sie sicher, dass die URL des Quell-Repositorys GitHub oder des Bitbucket-Quell-Repositorys keine persönlichen Zugriffstoken oder Anmeldeinformationen in Codebuild-Projektumgebungen enthält. AWS Verwende OAuth anstelle von persönlichen Zugriffstoken oder Anmeldedaten die Autorisierung für den Zugriff auf GitHub Bitbucket-Repositorys.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
Ihre Systeme-3	Implementieren Sie Sicherheitskonfigurationen für alle Hardware- und Softwareressourcen.	elasticsearch-logs-to-cloudwatch	Stellen Sie sicher, dass für Amazon OpenSearch Service-Domains Fehlerprotokolle aktiviert und zur Aufbewahrung und Beantwortung an Amazon CloudWatch Logs gestreamt werden. Domain-Fehlerprotokolle sind bei Sicherheits- und Zugriffsprüfungen sowie bei der Diagnose von Verfügbarkeitsproblemen nützlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
Ihre Systeme-3	Implementieren Sie Sicherheitskonfigurationen für alle Hardware- und Softwareressourcen.	opensearch-logs-to-cloudwatch	Stellen Sie sicher, dass für Amazon OpenSearch Service-Domains Fehlerprotokolle aktiviert und zur Aufbewahrung und Beantwortung an Amazon CloudWatch Logs gestreamt werden. OpenSearch Service-Fehlerprotokolle können bei Sicherheits- und Zugriffsprüfungen helfen und bei der Diagnose von Verfügbarkeitsproblemen helfen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
Ihre Systeme-3	Implementieren Sie Sicherheitskonfigurationen für alle Hardware- und Softwareressourcen.	elbv-2 acm-certificate-required	Zum Schutz von eventuell vorhandenen sensiblen Daten sowie von Daten während der Übertragung muss die Verschlüsselung für Ihr Elastic Load Balancing aktiviert sein. Verwenden Sie AWS Certificate Manager, um öffentliche und private SSL/TLS-Zertifikate mit AWS Diensten und internen Ressourcen zu verwalten, bereitzustellen und bereitzustellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
Ihre Systeme-3	Implementieren Sie Sicherheitskonfigurationen für alle Hardware- und Softwareressourcen.	iam-policy-no-statements-with-full-access	Stellen Sie sicher, dass IAM-Aktionen nur auf die benötigten Aktionen beschränkt sind. Wenn Benutzern mehr Rechte eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und der Aufgabentrennung verstoßen.
Ihre Systeme-3	Implementieren Sie Sicherheitskonfigurationen für alle Hardware- und Softwareressourcen.	no-unrestricted-route-to-igw	Stellen Sie sicher, dass EC2 Amazon-Routentabellen keine uneingeschränkten Routen zu einem Internet-Gateway enthalten. Durch das Entfernen oder Beschränken des Internetzugangs für Workloads innerhalb von Amazon VPCs können unbeabsichtigte Zugriffe in Ihrer Umgebung reduziert werden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
Ihre Systeme-3	Implementieren Sie Sicherheitskonfigurationen für alle Hardware- und Softwareressourcen.	s3- -blöcke-periodisch account-level-public-access	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Simple Storage Service (Amazon S3) -Buckets nicht öffentlich zugänglich sind. Diese Regel trägt dazu bei, sensible Daten vor unbefugten Remote-Benutzern zu schützen, indem sie den öffentlichen Zugriff verhindert. Mit dieser Regel können Sie optional die Parameter ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) und restrictPublicBuckets Parameter (Config Default: True) festlegen. Die tatsächlichen Werte müssen den Richtlini

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			en Ihrer Organisation entsprechen.
Ihre Systeme-3	Implementieren Sie Sicherheitskonfigurationen für alle Hardware- und Softwareressourcen.	ssm-document-not-public	Stellen Sie sicher, dass AWS Systems Manager (SSM) - Dokumente nicht öffentlich sind, da dies einen unbeabsichtigten Zugriff auf Ihre SSM-Dokumente ermöglichen kann. Ein öffentliches SSM-Dokument kann Informationen über Ihr Konto, Ihre Ressourcen und internen Prozesse preisgeben.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
Ihre Systeme-3	Implementieren Sie Sicherheitskonfigurationen für alle Hardware- und Softwareressourcen.	api-gw-cache-enabled-und verschlüsselt	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass die Verschlüsselung für den Cache Ihrer API-Gateway-Stufe aktiviert ist. Da für die API-Methode sensible Daten erfasst werden können, sollten Sie die Verschlüsselung von Daten im Ruhezustand aktivieren, um diese Daten zu schützen.
Ihre Systeme-3	Implementieren Sie Sicherheitskonfigurationen für alle Hardware- und Softwareressourcen.	api-gw-execution-logging-aktiviert	Die API-Gateway-Protokollierung zeigt detaillierte Ansichten der Benutzer, die auf die API zugegriffen haben, und wie diese Benutzer auf die API zugegriffen haben. Diese Einblicke ermöglichen die Transparenz von Benutzeraktivitäten.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
Ihre Systeme-3	Implementieren Sie Sicherheitskonfigurationen für alle Hardware- und Softwareressourcen.	api-gw-ssl-enabled	Stellen Sie sicher, dass die REST-API-Stufen von Amazon API Gateway mit SSL-Zertifikaten konfiguriert sind, damit Backend-Systeme überprüfen können, ob Anforderungen von API Gateway stammen.
Ihre Systeme-3	Implementieren Sie Sicherheitskonfigurationen für alle Hardware- und Softwareressourcen.	cloudtrail-s3-dataevents-enabled	Die Erfassung von Simple Storage Service (Amazon S3)-Datenereignissen unterstützt die Erkennung von ungewöhnlichen Aktivitäten. Zu den Details gehören AWS-Konto Informationen über den Zugriff auf einen Amazon S3 S3-Bucket, die IP-Adresse und die Uhrzeit des Ereignisses.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
Ihre Systeme-3	Implementieren Sie Sicherheitskonfigurationen für alle Hardware- und Softwareressourcen.	cloudtrail-security-trail-enabled	Diese Regel trägt dazu bei, die Verwendung der AWS empfohlenen bewährten Sicherheitsmethoden für sicherzustellen AWS CloudTrail, indem geprüft wird, ob mehrere Einstellungen aktiviert sind. Dazu gehören die Verwendung von Protokollverschlüsselung, Protokollvalidierung und Aktivierung AWS CloudTrail in mehreren Regionen.
Ihre Systeme-3	Implementieren Sie Sicherheitskonfigurationen für alle Hardware- und Softwareressourcen.	cloudwatch-log-group-encrypted	Um sensible Daten im Speicher zu schützen, stellen Sie sicher, dass die Verschlüsselung für Ihre Amazon CloudWatch Log Groups aktiviert ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
Ihre Systeme-3	Implementieren Sie Sicherheitskonfigurationen für alle Hardware- und Softwareressourcen.	cmk-backing-key-rotation-aktiviert	Aktivieren Sie die Schlüsselrotation, um sicherzustellen, dass Schlüssel rotiert werden, nachdem sie das Ende ihrer Krypto-Periode erreicht haben.
Ihre Systeme-3	Implementieren Sie Sicherheitskonfigurationen für alle Hardware- und Softwareressourcen.	db-instance-backup-enabled	Die Sicherungsfunktion von Amazon RDS erstellt Sicherungen Ihrer Datenbanken und Transaktionsprotokolle. Amazon RDS erstellt einen Snapshot für das Speichervolume Ihrer DB-Instance, sodass die gesamte DB-Instance gesichert wird. Sie können im System spezifische Aufbewahrungsfristen festlegen, um Ihre Ausfallsicherheitsanforderungen zu erfüllen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
Ihre Systeme-3	Implementieren Sie Sicherheitskonfigurationen für alle Hardware- und Softwareressourcen.	dms-replication-not-public	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass auf DMS-Replikationsinstanzen nicht öffentlich zugegriffen werden kann. DMS-Replikations-Instances können vertrauliche Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
Ihre Systeme-3	Implementieren Sie Sicherheitskonfigurationen für alle Hardware- und Softwareressourcen.	dynamodb-autoscaling-enabled	Amazon DynamoDB Auto Scaling verwendet den AWS Application Auto Scaling-Service, um die bereitgestellte Durchsatzkapazität so anzupassen, dass sie automatisch auf tatsächliche Verkehrsmuster reagiert. Auf diese Weise kann eine Tabelle oder ein globaler sekundärer Index die bereitgestellte Lese-/Schreibkapazität erhöhen, um plötzliche Erhöhungen des Datenverkehrs ohne Drosselung zu bewältigen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
Ihre Systeme-3	Implementieren Sie Sicherheitskonfigurationen für alle Hardware- und Softwareressourcen.	dynamodb-in-backup-plan	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon DynamoDB-Tabellen Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
Ihre Systeme-3	Implementieren Sie Sicherheitskonfigurationen für alle Hardware- und Softwareressourcen.	dynamodb-pitr-enabled	Aktivieren Sie diese Regel, um zu überprüfen, ob die Informationen gesichert wurden. Es verwaltet auch die Backups, indem es sicherstellt, dass die point-in-time Wiederherstellung in Amazon DynamoDB aktiviert ist. Bei der Wiederherstellung werden fortlaufende Backups Ihrer Tabelle für die letzten 35 Tage gespeichert.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
Ihre Systeme-3	Implementieren Sie Sicherheitskonfigurationen für alle Hardware- und Softwareressourcen.	dynamodb-table-encrypted-kms	Stellen Sie sicher, dass die Verschlüsselung für Ihre Amazon-DynamoDB-Tabellen aktiviert ist. Um eventuell vorhandene sensible Daten im Ruhezustand in diesen Tabellen zu schützen, müssen Sie die Verschlüsselung von Daten im Ruhezustand aktivieren. Standardmäßig werden DynamoDB-Tabellen mit einem AWS eigenen Kundenhauptschlüssel (CMK) verschlüselt.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
Ihre Systeme-3	Implementieren Sie Sicherheitskonfigurationen für alle Hardware- und Softwareressourcen.	ebs-in-backup-plan	Stellen Sie zur Unterstützung der Datensicherungsprozesse sicher, dass Ihre Amazon Elastic Block Store (Amazon EBS) -Volumes Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
Ihre Systeme-3	Implementieren Sie Sicherheitskonfigurationen für alle Hardware- und Softwareressourcen.	ebs-optimized-instance	Eine optimierte Instance im Amazon Elastic Block Store (Amazon EBS) bietet zusätzliche, dedizierte Kapazität für Amazon-EBS-I/O-Vorgänge. Diese Optimierung bietet die beste Leistung für Ihr EBS-Volume, indem Konflikte zwischen Amazon-EBS-I/O und anderem Datenverkehr von Ihrer Instance minimiert werden.
Ihre Systeme-3	Implementieren Sie Sicherheitskonfigurationen für alle Hardware- und Softwareressourcen.	ebs-snapshot-public-restorable-überprüfen	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass EBS-Snapshots nicht öffentlich wiederherstellbar sind. EBS-Volume-Snapshots können vertrauliche Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
Ihre Systeme-3	Implementieren Sie Sicherheitskonfigurationen für alle Hardware- und Softwareressourcen.	ec-2 ebs-encryption-by-default	Zum Schutz von Daten im Ruhezustand müssen Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon Elastic Block Store (Amazon EBS)-Volumes aktiviert ist. Da sensible Daten auch im Ruhezustand vorhanden sein können, sollten Sie die Verschlüsselung im Ruhezustand aktivieren, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
Ihre Systeme-3	Implementieren Sie Sicherheitskonfigurationen für alle Hardware- und Softwareressourcen.	ec2- instance-no-public-ip	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon Elastic Compute Cloud (Amazon EC2) - Instances nicht öffentlich zugänglich sind. EC2 Amazon-Instances können vertrauliche Informationen enthalten, und für solche Konten ist eine Zugriffskontrolle erforderlich.
Ihre Systeme-3	Implementieren Sie Sicherheitskonfigurationen für alle Hardware- und Softwareressourcen.	efs-encrypted-check	Aktivieren Sie die Verschlüsselung für Ihr Amazon Elastic File System (EFS), um eventuell vorhandene sensible Daten sowie Daten im Ruhezustand zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
Ihre Systeme-3	Implementieren Sie Sicherheitskonfigurationen für alle Hardware- und Softwareressourcen.	efs-in-backup-plan	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon Elastic File System (Amazon EFS) -Dateisysteme Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
Ihre Systeme-3	Implementieren Sie Sicherheitskonfigurationen für alle Hardware- und Softwareressourcen.	elasticsearch-encrypted-at-rest	Da sensible Daten vorhanden sein können und um Daten im Ruhezustand zu schützen, sollten Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon OpenSearch Service (OpenSearch Service) -Domains aktiviert ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
Ihre Systeme-3	Implementieren Sie Sicherheitskonfigurationen für alle Hardware- und Softwareressourcen.	elasticsearch-in-vpc-only	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass sich Amazon OpenSearch OpenSearch Service (Service) - Domains innerhalb einer Amazon Virtual Private Cloud (Amazon VPC) befinden. Eine OpenSearch Service-Domain innerhalb einer Amazon VPC ermöglicht die sichere Kommunikation zwischen OpenSearch Service und anderen Services innerhalb der Amazon VPC, ohne dass ein Internet-Gateway, ein NAT-Gerät oder eine VPN-Verbindung erforderlich ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
Ihre Systeme-3	Implementieren Sie Sicherheitskonfigurationen für alle Hardware- und Softwareressourcen.	opensearch-node-to-node-Verschlüsselungsprüfung	Stellen Sie sicher, dass die node-to-node Verschlüsselung für Amazon OpenSearch Service aktiviert ist. Node-to-nodeVerschlüsselung ermöglicht die TLS 1.2-Verschlüsselung für die gesamte Kommunikation innerhalb der Amazon Virtual Private Cloud (Amazon VPC). Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
Ihre Systeme-3	Implementieren Sie Sicherheitskonfigurationen für alle Hardware- und Softwareressourcen.	elb-acm-certificate-required	Zum Schutz von eventuell vorhanden en sensiblen Daten sowie von Daten während der Übertragung muss die Verschlüsselung für Ihr Elastic Load Balancing aktiviert sein. Verwenden Sie AWS Certificate Manager, um öffentlic he und private SSL/ TLS-Zertifikate mit AWS Diensten und internen Ressource n zu verwalten, bereitzustellen und bereitzustellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
Ihre Systeme-3	Implementieren Sie Sicherheitskonfigurationen für alle Hardware- und Softwareressourcen.	opensearch-data-node-fault-Toleranz	Amazon OpenSearch Service (OpenSearch Service) benötigt mindestens drei Datenknoten für hohe Verfügbarkeit und Fehlertoleranz. Durch die Bereitstellung einer OpenSearch Service-Domain mit mindestens drei Datenknoten wird der Cluster-Betrieb gewährleistet, falls ein Knoten ausfällt.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
Ihre Systeme-3	Implementieren Sie Sicherheitskonfigurationen für alle Hardware- und Softwareressourcen.	elbv2- acm-certificate-required	Zum Schutz von eventuell vorhanden en sensiblen Daten sowie von Daten während der Übertragung muss die Verschlüsselung für Ihr Elastic Load Balancing aktiviert sein. Verwenden Sie AWS Certificate Manager, um öffentlic he und private SSL/ TLS-Zertifikate mit AWS Diensten und internen Ressource n zu verwalten, bereitzustellen und bereitzustellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
Ihre Systeme-3	Implementieren Sie Sicherheitskonfigurationen für alle Hardware- und Softwareressourcen.	elb-cross-zone-load-Balancing aktiviert	Aktivieren Sie zonenübergreifendes Load Balancing für Ihre Elastic Load Balancer (ELBs), um eine angemessene Kapazität und Verfügbarkeit aufrechtzuerhalten. Zonenübergreifendes Load Balancing reduziert die Notwendigkeit, die gleiche Anzahl von Instances in jeder aktivierten Availability Zone aufrechtzuerhalten. Es verbessert auch die Fähigkeit Ihrer Anwendung, den Verlust einer oder mehrerer Instances zu bewältigen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
Ihre Systeme-3	Implementieren Sie Sicherheitskonfigurationen für alle Hardware- und Softwareressourcen.	elb-deletion-protection-enabled	Diese Regel sorgt dafür, dass der Löschschutz für Elastic Load Balancing aktiviert ist. Verwenden Sie diese Funktion, um zu verhindern, dass Ihr Load Balancer versehentlich oder böswillig gelöscht wird, was zum Verlust der Verfügbarkeit Ihrer Anwendungen führen kann.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
Ihre Systeme-3	Implementieren Sie Sicherheitskonfigurationen für alle Hardware- und Softwareressourcen.	elb-logging-enabled	Die Elastic-Load-Balancing-Aktivität ist ein zentraler Kommunikationspunkt innerhalb einer Umgebung. Stellen Sie sicher, dass die ELB-Protokollierung aktiviert ist. Die gesammelten Daten enthalten detaillierte Informationen zu Anfragen, die an den ELB gesendet wurden. Jedes Protokoll enthält Informationen wie die Zeit, zu der die Anforderung einging, die Client-IP-Adresse, Latenzen, Anforderungspfade und Serverantworten.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
Ihre Systeme-3	Implementieren Sie Sicherheitskonfigurationen für alle Hardware- und Softwareressourcen.	elb-tls-https-listeners-nur	Stellen Sie sicher, dass Ihre Elastic Load Balancer (ELBs) mit SSL- oder HTTPS-Listenern konfiguriert sind. Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.
Ihre Systeme-3	Implementieren Sie Sicherheitskonfigurationen für alle Hardware- und Softwareressourcen.	emr-master-no-public-ip	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon EMR-Cluster-Masterknoten nicht öffentlich zugänglich sind. Amazon-EMR-Cluster-Hauptknoten können vertrauliche Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
Ihre Systeme-3	Implementieren Sie Sicherheitskonfigurationen für alle Hardware- und Softwareressourcen.	encrypted-volumes	Aktivieren Sie die Verschlüsselung für Ihre Amazon-Elastic-Block-Store (Amazon-EBS)-Volumes, um eventuell vorhandene sensible Daten sowie Daten im Ruhezustand zu schützen.
Ihre Systeme-3	Implementieren Sie Sicherheitskonfigurationen für alle Hardware- und Softwareressourcen.	guardduty-enabled-centralized	Amazon GuardDuty kann mithilfe von Threat Intelligence Feeds helfen, potenzielle Cybersicherheitsereignisse zu überwachen und zu erkennen. Dazu gehören Listen mit bösartigen IPs und maschinellen Lernmethoden zur Identifizierung unerwarteter, nicht autorisierter und bösartiger Aktivitäten in Ihrer AWS Cloud-Umgebung.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
Ihre Systeme-3	Implementieren Sie Sicherheitskonfigurationen für alle Hardware- und Softwareressourcen.	iam-inline-policy-blocked-kms-Aktionen	Stellen Sie sicher, dass ein Benutzer, eine IAM-Rolle oder eine IAM-Gruppe (AWS Identity and Access Management) nicht über eine Inline-Richtlinie verfügt, die blockierte Aktionen für alle AWS Schlüssel des Key Management Service zulässt. AWS empfiehlt, verwaltete Richtlinien anstelle von Inline-Richtlinien zu verwenden. Verwaltete Richtlinien ermöglichen Wiederverwendbarkeit, Versionsverwaltung, Rollback und Delegierung der Berechtigungsverwaltung. Mit dieser Regel können Sie den blockedActionsPatterns Parameter festlegen. (Wert „AWS Bewährte grundlegende Sicherheitsmethoden“: kms:Decrypt, kms:ReEncryptFrom). Die

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.
Ihre Systeme-3	Implementieren Sie Sicherheitskonfigurationen für alle Hardware- und Softwareressourcen.	iam-no-inline-policy-überprüfen	Stellen Sie sicher, dass ein Benutzer, eine IAM-Rolle oder eine IAM-Gruppe (AWS Identity and Access Management) nicht über eine Inline-Richtlinie zur Zugriffskontrolle auf Systeme und Ressourcen verfügt. AWS empfiehlt, verwaltete Richtlinien anstelle von Inline-Richtlinien zu verwenden. Verwaltete Richtlinien ermöglichen Wiederverwendbarkeit, Versionsverwaltung, Rollback und Delegierung der Berechtigungsverwaltung.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
Ihre Systeme-3	Implementieren Sie Sicherheitskonfigurationen für alle Hardware- und Softwareressourcen.	iam-password-policy	Die Identitäten und Anmeldeinformationen werden auf der Grundlage einer organisatorischen IAM-Passwortrichtlinie ausgestellt, verwaltet und verifiziert. Sie erfüllen oder übertreffen die Anforderungen von NIST SP 800-63 und dem Standard „Best Practices“ von AWS Foundational Security für die Passwortstärke. Mit dieser Regel können Sie optional RequireUppercaseCharacters (Wert für AWS grundlegende Sicherheitsbewährte Methoden: wahr), RequireLowercaseCharacters (Wert für bewährte Methoden für AWS grundlegende Sicherheit: wahr), RequireSymbols (Wert für bewährte Methoden für AWS grundlegende Sicherheit:

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			wahr), RequireNumbers (Wert für bewährte Methoden für AWS grundlegende Sicherheit: wahr), MinimumPasswordLength (Wert für bewährte Methoden für AWS grundlegende Sicherheit: 14), PasswordReusePrevention (Wert für bewährte Methoden für AWS grundlegende Sicherheit: 24) und MaxPasswordAge (Wert für bewährte Methoden für AWS grundlegende Sicherheit: 90) für Ihr IAM festlegen Kennwortrichtlinie. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
Ihre Systeme-3	Implementieren Sie Sicherheitskonfigurationen für alle Hardware- und Softwareressourcen.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) kann Ihnen dabei helfen, die Prinzipien der geringsten Rechte und der Aufgabentrennung in Zugriffsberechtigungen und Autorisierungen zu integrieren und so zu verhindern, dass Richtlinien „Effect“: „Allow“ mit „Action“: „*“ anstelle von „Resource“: „*“ enthalten. Wenn Benutzern mehr Rechte eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und der Aufgabentrennung verstoßen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
Ihre Systeme-3	Implementieren Sie Sicherheitskonfigurationen für alle Hardware- und Softwareressourcen.	iam-root-access-key-überprüfen	Der Zugriff auf Systeme und Ressourcen kann gesteuert werden, indem überprüft wird, ob der Root-Benutzer keine Zugriffsschlüssel mit seiner AWS Identity and Access Management (IAM) -Rolle verknüpft hat. Stellen Sie sicher, dass die Root-Zugriffsschlüssel gelöscht werden. Erstellen und verwenden Sie stattdessen rollenbasierte Funktionen, AWS-Konten um das Prinzip der geringsten Funktionalität zu berücksichtigen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
Ihre Systeme-3	Implementieren Sie Sicherheitskonfigurationen für alle Hardware- und Softwareressourcen.	iam-user-mfa-enabled	Aktivieren Sie diese Regel, um den Zugriff auf Ressourcen in der AWS Cloud einzuschränken. Diese Regel sorgt dafür, dass die Multi-Faktor-Authentifizierung (MFA) für alle Benutzer aktiviert ist. MFA sorgt für eine weitere Schutzebene zusätzlich zu den Anmeldeinformationen. Reduzieren Sie Fälle von kompromittierten Konten, indem Sie MFA für Benutzer vorschreiben.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
Ihre Systeme-3	Implementieren Sie Sicherheitskonfigurationen für alle Hardware- und Softwareressourcen.	iam-user-no-policies-überprüfen	Diese Regel stellt sicher, dass AWS Identity and Access Management (IAM) -Richtlinien nur Gruppen oder Rollen zugewiesen werden, um den Zugriff auf Systeme und Ressourcen zu kontrollieren. Die Zuweisung von Berechtigungen auf Gruppen- oder Rollenebene trägt dazu bei, die Wahrscheinlichkeit zu verringern, dass eine Identität übermäßige Berechtigungen erhält oder beibehält.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
Ihre Systeme-3	Implementieren Sie Sicherheitskonfigurationen für alle Hardware- und Softwareressourcen.	iam-user-unused-credentials-überprüfen	AWS Identity and Access Management (IAM) kann Ihnen bei Zugriffsberechtigungen und Autorisierungen helfen, indem es nach IAM-Passwörtern und Zugriffsschlüsseln sucht, die für einen bestimmten Zeitraum nicht verwendet wurden. Wenn ungenutzte Anmeldeinformationen identifiziert werden, müssen Sie sie deaktivieren und/oder entfernen, da dies gegen das Prinzip der geringsten Berechtigung verstoßen könnte. Für diese Regel müssen Sie einen Wert für das maxCredentialUsage Alter festlegen (Standardkonfiguration: 90). Der tatsächliche Wert muss den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
Ihre Systeme-3	Implementieren Sie Sicherheitskonfigurationen für alle Hardware- und Softwareressourcen.	ec2- instances-in-vpc	Stellen Sie Amazon Elastic Compute Cloud (Amazon EC2) -Instances innerhalb einer Amazon Virtual Private Cloud (Amazon VPC) bereit, um eine sichere Kommunikation zwischen einer Instance und anderen Services innerhalb der Amazon VPC zu ermöglichen, ohne dass ein Internet-Gateway, ein NAT-Gerät oder eine VPN-Verbindung erforderlich ist. Der gesamte Datenverkehr bleibt sicher in der AWS Cloud. Domains, die sich innerhalb einer VPC befinden, verfügen aufgrund ihrer logischen Isolierung im Vergleich zu Domains mit öffentlichen Endpunkten über eine zusätzliche Sicherheitsebene. Weisen Sie EC2

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			Amazon-Instances einer Amazon-VPC zu, um den Zugriff ordnungsgemäß zu verwalten.
Ihre Systeme-3	Implementieren Sie Sicherheitskonfigurationen für alle Hardware- und Softwareressourcen.	kms-cmk-not-scheduled-zum Löschen	Um Daten im Ruhezustand zu schützen, sollten Sie sicherstellen, dass die für den Kunden erforderlichen Masterschlüssel (CMKs) nicht für das Löschen im AWS Key Management Service (AWS KMS) vorgesehen sind. Da Schlüssel manchmal gelöscht werden müssen, können Sie mit dieser Regel alle zu löschenden Schlüssel überprüfen, falls ein Schlüssel versehentlich zur Löschung vorgemerkt wurde.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
Ihre Systeme-3	Implementieren Sie Sicherheitskonfigurationen für alle Hardware- und Softwareressourcen.	lambda-function-public-access-verboten	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass AWS Lambda-Funktionen nicht öffentlich zugänglich sind. Der öffentliche Zugriff kann möglicherweise die Verfügbarkeit von Ressourcen beeinträchtigen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
Ihre Systeme-3	Implementieren Sie Sicherheitskonfigurationen für alle Hardware- und Softwareressourcen.	lambda-inside-vpc	Stellen Sie AWS Lambda-Funktionen in einer Amazon Virtual Private Cloud (Amazon VPC) bereit, um eine sichere Kommunikation zwischen einer Funktion und anderen Diensten innerhalb der Amazon VPC zu gewährleisten. Bei dieser Konfiguration sind kein Internet-Gateway, kein NAT-Gerät und keine VPN-Verbindung erforderlich. Der gesamte Datenverkehr bleibt sicher in der Cloud. AWS Domains, die sich innerhalb einer VPC befinden, verfügen aufgrund ihrer logischen Isolierung im Vergleich zu Domains mit öffentlichen Endpunkten über eine zusätzliche Sicherheitsebene. Um den Zugriff ordnungsgemäß zu verwalten,

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			sollten AWS Lambda-Funktionen einer VPC zugewiesen werden.
Ihre Systeme-3	Implementieren Sie Sicherheitskonfigurationen für alle Hardware- und Softwareressourcen.	mfa-enabled-for-iam-Konsolenzugriff	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass MFA für alle AWS Identity and Access Management (IAM) -Benutzer aktiviert ist, die über ein Konsolenkennwort verfügen. MFA sorgt für eine weitere Schutzebene zusätzlich zu den Anmeldeinformationen. Indem Sie MFA für Benutzer vorschreiben, können Sie Fälle kompromittierter Konten reduzieren und verhindern, dass unbefugte Benutzer auf vertrauliche Daten zugreifen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
Ihre Systeme-3	Implementieren Sie Sicherheitskonfigurationen für alle Hardware- und Softwareressourcen.	multi-region-cloudtrail-enabled	AWS CloudTrail zeichnet Aktionen und API-Aufrufe der AWS Management Console auf. Sie können feststellen, welche Benutzer und Konten angerufen wurden AWS, von welcher Quell-IP-Adresse aus die Anrufe getätigt wurden und wann die Anrufe erfolgten. CloudTrail übermittelt Protokolldateien aus allen AWS Regionen an Ihren S3-Bucket , wenn MULTI_REGION_CLOUD_TRAIL_ENABLED aktiviert ist. Außerdem wird beim AWS Start einer neuen Region derselbe Trail in der neuen Region erstellt. CloudTrail Dadurch erhalten Sie automatisch Protokolldateien mit API-Aktivitäten für die neue Region.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
Ihre Systeme-3	Implementieren Sie Sicherheitskonfigurationen für alle Hardware- und Softwareressourcen.	rds-enhanced-monitoring-enabled	Aktivieren Sie Amazon Relational Database Service (Amazon RDS), um die Verfügbarkeit von Amazon RDS zu überwachen. Dies bietet einen detaillierten Einblick in den Zustand Ihrer Amazon-RDS-Datenbank-Instances. Wenn der Amazon-RDS-Speicher mehr als ein zugrunde liegendes physisches Gerät verwendet, erfasst Enhanced Monitoring die Daten für jedes Gerät. Wenn die Amazon-RDS-Datenbank-Instance in einer Multi-AZ-Bereitstellung ausgeführt wird, werden außerdem die Daten für jedes Gerät auf dem sekundären Host sowie die Metriken des sekundären Hosts erfasst.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
Ihre Systeme-3	Implementieren Sie Sicherheitskonfigurationen für alle Hardware- und Softwareressourcen.	rds-in-backup-plan	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon Relational Database Service (Amazon RDS) -Instances Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
Ihre Systeme-3	Implementieren Sie Sicherheitskonfigurationen für alle Hardware- und Softwareressourcen.	rds-instance-deletion-protection-aktiviert	Stellen Sie sicher, dass Amazon Relational Database Service (Amazon RDS)-Instances den Löschschutz aktiviert haben. Verwenden Sie den Löschschutz, um zu verhindern, dass Ihre Amazon-RDS-Instances versehentlich oder böswillig gelöscht werden, was zum Verlust der Verfügbarkeit Ihrer Anwendungen führen kann.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
Ihre Systeme-3	Implementieren Sie Sicherheitskonfigurationen für alle Hardware- und Softwareressourcen.	rds-instance-public-access-überprüfen	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Relational Database Service (Amazon RDS) -Instances nicht öffentlich sind. Amazon-RDS-Datenbank-Instances können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
Ihre Systeme-3	Implementieren Sie Sicherheitskonfigurationen für alle Hardware- und Softwareressourcen.	rds-logging-enabled	Um die Protokollierung und Überwachung in Ihrer Umgebung zu erleichtern, stellen Sie sicher, dass die Amazon Relational Database Service (Amazon RDS)-Protokollierung aktiviert ist. Mit der Amazon-RDS-Protokollierung können Sie Ereignisse wie Verbindungen, Verbindungsabbrüche, Abfragen oder abgefragte Tabellen erfassen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
Ihre Systeme-3	Implementieren Sie Sicherheitskonfigurationen für alle Hardware- und Softwareressourcen.	rds-multi-az-support	Die Multi-AZ-Unterstützung in Amazon Relational Database Service (Amazon RDS) bietet eine verbesserte Verfügbarkeit und Beständigkeit von Datenbank-Instances. Wenn Sie eine Multi-AZ-Datenbank-Instance bereitstellen, erstellt Amazon RDS automatisch eine primäre Datenbank-Instance und repliziert die Daten synchron auf eine Standby-Instance in einer anderen Availability Zone. Jede Availability Zone läuft auf einer eigenen, physisch getrennten, unabhängigen Infrastruktur und ist auf eine hohe Verfügbarkeit ausgelegt. Im Falle eines Infrastrukturausfalls führt Amazon RDS einen automatis

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			chen Failover zum Standby-Modus durch, sodass Sie den Datenbankbetrieb wieder aufnehmen können, sobald der Failover abgeschlo ssen ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
Ihre Systeme-3	Implementieren Sie Sicherheitskonfigurationen für alle Hardware- und Softwareressourcen.	rds-cluster-multi-az-aktiviert	Die Multi-AZ-Unterstützung in Amazon Relational Database Service (Amazon RDS) bietet eine verbesserte Verfügbarkeit und Beständigkeit von Datenbank-Instances. Wenn Sie eine Multi-AZ-Datenbank-Instance bereitstellen, erstellt Amazon RDS automatisch eine primäre Datenbank-Instance und repliziert die Daten synchron auf eine Standby-Instance in einer anderen Availability Zone. Jede Availability Zone läuft auf einer eigenen, physisch getrennten, unabhängigen Infrastruktur und ist auf eine hohe Verfügbarkeit ausgelegt. Im Falle eines Infrastrukturausfalls führt Amazon RDS einen automatis

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			chen Failover zum Standby-Modus durch, sodass Sie den Datenbankbetrieb wieder aufnehmen können, sobald der Failover abgeschlo ssen ist.
Ihre Systeme-3	Implementieren Sie Sicherheitskonfigu rationen für alle Hardware- und Softwareressourcen.	rds-snapshot-encry pted	Stellen Sie sicher, dass die Verschlüs selung für Ihre Amazon Relationa l Database Service (Amazon RDS)-Snap shots aktiviert ist. Da sensible Daten auch im Ruhezusta nd vorhanden sein können, sollten Sie die Verschlüsselung im Ruhezustand aktivieren, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
Ihre Systeme-3	Implementieren Sie Sicherheitskonfigurationen für alle Hardware- und Softwareressourcen.	rds-snapshots-public-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Relational Database Service (Amazon RDS) -Instances nicht öffentlich sind. Amazon-RDS-Datenbank-Instances können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
Ihre Systeme-3	Implementieren Sie Sicherheitskonfigurationen für alle Hardware- und Softwareressourcen.	rds-storage-encrypted	Zum Schutz von Daten im Ruhezustand müssen Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon Relational Database Service (Amazon RDS)-Instances aktiviert ist. Um eventuell vorhandene sensible Daten im Ruhezustand in Amazon-RDS-Instances zu schützen, muss die Verschlüsselung von Daten im Ruhezustand aktiviert sein.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
Ihre Systeme-3	Implementieren Sie Sicherheitskonfigurationen für alle Hardware- und Softwareressourcen.	redshift-backup-enabled	Stellen Sie zur Unterstützung der Datensicherungsprozesse sicher, dass Ihre Amazon-Redshift-Cluster über automatisierte Snapshots verfügen. Wenn automatisierte Snapshots für einen Cluster aktiviert sind, erstellt Redshift in regelmäßigen Abständen Snapshots dieses Clusters. Standardmäßig erstellt Redshift alle acht Stunden oder alle 5 GB einen Snapshot für jeden Knoten mit Datenänderungen oder je nachdem, was zuerst eintritt.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
Ihre Systeme-3	Implementieren Sie Sicherheitskonfigurationen für alle Hardware- und Softwareressourcen.	redshift-cluster-configuration-check	Um Daten im Ruhezustand zu schützen, muss die Verschlüsselung für Ihre Amazon-Redshift-Cluster aktiviert sein. Sie müssen auch sicherstellen, dass die erforderlichen Konfigurationen auf Amazon-Redshift-Clustern bereitgestellt werden. Die Prüfungsprotokollierung muss aktiviert sein, um Informationen zu Verbindungen und Benutzeraktivitäten in der Datenbank bereitzustellen. Diese Regel erfordert, dass ein Wert für clusterDbEncrypted (Config Default: TRUE) und LoggingEnabled (Config Default: TRUE) gesetzt ist. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
Ihre Systeme-3	Implementieren Sie Sicherheitskonfigurationen für alle Hardware- und Softwareressourcen.	redshift-cluster-kms-enabled	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass die Verschlüsselung mit AWS Key Management Service (AWS KMS) für Ihren Amazon Redshift Redshift-Cluster aktiviert ist. Um eventuell vorhandene sensible Daten im Ruhezustand in Redshift-Clustern zu schützen, muss die Verschlüsselung von Daten im Ruhezustand aktiviert sein.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
Ihre Systeme-3	Implementieren Sie Sicherheitskonfigurationen für alle Hardware- und Softwareressourcen.	redshift-cluster-public-access-überprüfen	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Redshift Redshift-Cluster nicht öffentlich sind. Amazon-Redshift-Cluster können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.
Ihre Systeme-3	Implementieren Sie Sicherheitskonfigurationen für alle Hardware- und Softwareressourcen.	redshift-require-tls-ssl	Stellen Sie sicher, dass Ihre Amazon-Redshift-Cluster eine TLS/SSL-Verschlüsselung erfordern, um eine Verbindung zu SQL-Clients herzustellen. Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
Ihre Systeme-3	Implementieren Sie Sicherheitskonfigurationen für alle Hardware- und Softwareressourcen.	restricted-common-ports	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass gemeinsame Ports für Amazon Elastic Compute Cloud (Amazon EC2) -Sicherheitsgruppen eingeschränkt sind. Wenn der Zugriff auf Ports nicht auf vertrauenswürdige Quellen beschränkt wird, kann dies zu Angriffen auf die Verfügbarkeit, Integrität und Vertraulichkeit von Systemen führen. Mit dieser Regel können Sie optional die Parameter blockedPort1–blockedPort5 festlegen (Standardkonfigurationen: 20, 21, 3389, 3306, 4333). Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
Ihre Systeme-3	Implementieren Sie Sicherheitskonfigurationen für alle Hardware- und Softwareressourcen.	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) Security Groups können bei der Verwaltung des Netzwerkzugriffs helfen, indem sie eine statusbehaftete Filterung von eingehendem und ausgehendem Netzwerkverkehr zu Ressourcen bereitstellen. AWS Wenn Sie eingehenden (oder entfernten) Datenverkehr von 0.0.0.0/0 bis Port 22 auf Ihren Ressourcen nicht zulassen, können Sie den Remote-Zugriff einschränken.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
Ihre Systeme-3	Implementieren Sie Sicherheitskonfigurationen für alle Hardware- und Softwareressourcen.	root-account-hardware-mfa-aktiviert	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Hardware-MFA für den Root-Benutzer aktiviert ist. Der Stammbenutzer ist der AWS-Konto-Benutzer mit den meisten Berechtigungen. MFA sorgt für eine weitere Schutzebene zusätzlich zu den Anmeldeinformationen. Indem Sie MFA für den Root-Benutzer vorschreiben, können Sie die Anzahl AWS-Konten kompromittierter Benutzer reduzieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
Ihre Systeme-3	Implementieren Sie Sicherheitskonfigurationen für alle Hardware- und Softwareressourcen.	root-account-mfa-enabled	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass MFA für den Root-Benutzer aktiviert ist. Der Stammbenutzer ist der AWS-Konto-Benutzer mit den meisten Berechtigungen. MFA sorgt für eine weitere Schutzebene zusätzlich zu den Anmeldeinformationen. Indem Sie MFA für den Root-Benutzer vorschreiben, können Sie die Anzahl AWS-Konten kompromittierter Benutzer reduzieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
Ihre Systeme-3	Implementieren Sie Sicherheitskonfigurationen für alle Hardware- und Softwareressourcen.	s-3 bucket-logging-enabled	Die Amazon Simple Storage Service (Amazon S3)-Serverzugriffsprotokollierung bietet eine Methode zur Überwachung des Netzwerks im Hinblick auf potenzielle Cybersicherheitsereignisse. Die Ereignisse werden überwacht, indem detaillierte Aufzeichnungen über die Anfragen erfasst werden, die an einen Amazon-S3-Bucket gestellt wurden. Jeder Zugriffsprotokolleintrag enthält Details zu einer einzelnen Zugriffsanfrage. Zu den Details gehören Anforderer, Bucket-Name, Anforderungszeit, Anforderungsaktion, Antwortstatus und Fehlercode, falls relevant.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
Ihre Systeme-3	Implementieren Sie Sicherheitskonfigurationen für alle Hardware- und Softwareressourcen.	s-3 bucket-public-read-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie nur autorisierten Benutzern, Prozessen und Geräten Zugriff auf Amazon Simple Storage Service (Amazon S3) - Buckets gewähren. Die Verwaltung des Zugriffs sollte mit der Klassifizierung der Daten übereinstimmen.
Ihre Systeme-3	Implementieren Sie Sicherheitskonfigurationen für alle Hardware- und Softwareressourcen.	s3- bucket-public-write-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie nur autorisierten Benutzern, Prozessen und Geräten Zugriff auf Amazon Simple Storage Service (Amazon S3) - Buckets gewähren. Die Verwaltung des Zugriffs sollte mit der Klassifizierung der Daten übereinstimmen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
Ihre Systeme-3	Implementieren Sie Sicherheitskonfigurationen für alle Hardware- und Softwareressourcen.	s3- bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) unterstützt die Aufrechterhaltung einer angemessenen Kapazität und Verfügbarkeit. CRR ermöglicht das automatische, asynchrone Kopieren von Objekten in Amazon-S3-Buckets, um die Datenverfügbarkeit sicherzustellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
Ihre Systeme-3	Implementieren Sie Sicherheitskonfigurationen für alle Hardware- und Softwareressourcen.	s3- bucket-server-side -encryption -aktiviert	Zum Schutz von Daten im Ruhezustand müssen Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon Simple Storage Service (Amazon S3)-Buckets aktiviert ist. Um eventuell vorhandene sensible Daten im Ruhezustand in Amazon-S3-Buckets zu schützen, muss die Verschlüsselung aktiviert sein.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
Ihre Systeme-3	Implementieren Sie Sicherheitskonfigurationen für alle Hardware- und Softwareressourcen.	s-3 bucket-ssl-requests-only	Um Daten während der Übertragung zu schützen, stellen Sie sicher, dass Ihre Amazon Simple Storage Service (Amazon S3)-Buckets Anfragen zur Verwendung von Secure Socket Layer (SSL)-Buckets erfordern. Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
Ihre Systeme-3	Implementieren Sie Sicherheitskonfigurationen für alle Hardware- und Softwareressourcen.	s-3 bucket-versioning-enabled	Die Versionsverwaltung von Amazon Simple Storage Service (Amazon S3)-Buckets hilft dabei, mehrere Varianten eines Objekts im selben Amazon-S3-Bucket zu speichern. Verwenden Sie die Versionsverwaltung, um sämtliche Versionen aller Objekte in Ihrem Amazon-S3-Bucket zu speichern, abzurufen oder wiederherzustellen. Mit der Versionsverwaltung können Sie Versionen sowohl nach unbeabsichtigten Benutzeraktionen als auch nach Anwendungsfehlern problemlos wiederherstellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
Ihre Systeme-3	Implementieren Sie Sicherheitskonfigurationen für alle Hardware- und Softwareressourcen.	s-3 default-encryption-kms	Stellen Sie sicher, dass die Verschlüsselung für Ihre Amazon Simple Storage Service (Amazon S3)-Buckets aktiviert ist. Um eventuell vorhandene sensible Daten im Ruhezustand in einem Amazon-S3-Bucket zu schützen, muss die Verschlüsselung aktiviert sein.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
Ihre Systeme-3	Implementieren Sie Sicherheitskonfigurationen für alle Hardware- und Softwareressourcen.	sagemaker-endpoint-configuration-kms-key-konfiguriert	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass die Verschlüsselung mit dem AWS Key Management Service (AWS KMS) für Ihren Endpunkt aktiviert ist. SageMaker Da sensible Daten auf dem SageMaker Endgerät gespeichert werden können, sollten Sie die Verschlüsselung im Ruhezustand aktivieren, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
Ihre Systeme-3	Implementieren Sie Sicherheitskonfigurationen für alle Hardware- und Softwareressourcen.	sagemaker-notebook-instance-kms-schlüsselkonfiguriert	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass die Verschlüsselung mit dem AWS Key Management Service (AWS KMS) für Ihr Notebook aktiviert ist. SageMaker Da vertrauliche Daten im SageMaker Notebook gespeichert werden können, sollten Sie die Verschlüsselung im Ruhezustand aktivieren, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
Ihre Systeme-3	Implementieren Sie Sicherheitskonfigurationen für alle Hardware- und Softwareressourcen.	sagemaker-notebook-no-direct-Internetzugang	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass SageMaker Amazon-Notebooks keinen direkten Internetzugang zulassen. Indem Sie direkten Internetzugang blockieren, vermeiden Sie, dass unbefugte Benutzer auf sensible Daten zugreifen.
Ihre Systeme-3	Implementieren Sie Sicherheitskonfigurationen für alle Hardware- und Softwareressourcen.	secretsmanager-rotation-enabled-check	Diese Regel stellt sicher, dass bei AWS Secrets Manager Manager-Geheimnissen die Rotation aktiviert ist. Die regelmäßige Rotation von Secrets kann den Zeitraum verkürzen, in dem ein Secret aktiv ist, und möglicherweise die Auswirkungen auf das Unternehmen verringern, falls das Secret kompromittiert wird.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
Ihre Systeme-3	Implementieren Sie Sicherheitskonfigurationen für alle Hardware- und Softwareressourcen.	secretsmanager-secret-periodic-rotation	Diese Regel stellt sicher, dass bei AWS Secrets Manager Manager-Geheimnissen die regelmäßige Rotation aktiviert ist. Die regelmäßige Rotation von Secrets kann den Zeitraum verkürzen, in dem ein Secret aktiv ist, und möglicherweise die Auswirkungen auf das Unternehmen verringern, falls das Secret kompromittiert wird. Der Standardwert lautet 90 Tage.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
Ihre Systeme-3	Implementieren Sie Sicherheitskonfigurationen für alle Hardware- und Softwareressourcen.	secretsmanager-secret-unused	Wenn in AWS Secrets Manager unbenutzte Anmeldeinformationen vorhanden sind, sollten Sie die Anmeldeinformationen deaktivieren und/oder entfernen, da dies gegen das Prinzip der geringsten Rechte verstoßen kann. Mit dieser Regel können Sie einen Wert auf unusedForDays (Config Default: 90) setzen. Der tatsächliche Wert muss den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
Ihre Systeme-3	Implementieren Sie Sicherheitskonfigurationen für alle Hardware- und Softwareressourcen.	securityhub-enabled	AWS Security Hub hilft bei der Überwachung von unbefugtem Personal, Verbindungen, Geräten und Software. AWS Security Hub aggregiert, organisiert und priorisiert die Sicherheitswarnungen oder Ergebnisse mehrerer Dienste. AWS Einige dieser Dienste sind Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer und AWS Firewall Manager sowie AWS Partnerlösungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
Ihre Systeme-3	Implementieren Sie Sicherheitskonfigurationen für alle Hardware- und Softwareressourcen.	sns-encrypted-kms	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass Ihre Amazon Simple Notification Service (Amazon SNS) -Themen mit dem AWS Key Management Service (AWS KMS) verschlüsselt werden müssen. Um eventuell vorhandene sensible Daten im Ruhezustand in veröffentlichten Nachrichten zu schützen, muss die Verschlüsselung von Daten im Ruhezustand aktiviert sein.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
Ihre Systeme-3	Implementieren Sie Sicherheitskonfigurationen für alle Hardware- und Softwareressourcen.	subnet-auto-assign-public-ip-deaktiviert	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon Virtual Private Cloud (VPC) -Subnetzen nicht automatisch eine öffentliche IP-Adresse zugewiesen wird. Amazon Elastic Compute Cloud (EC2) -Instances, die in Subnetzen gestartet werden, in denen dieses Attribut aktiviert ist, haben ihrer primären Netzwerkschnittstelle eine öffentliche IP-Adresse zugewiesen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
Ihre Systeme-3	Implementieren Sie Sicherheitskonfigurationen für alle Hardware- und Softwareressourcen.	vpc-default-security-group-geschlossen	Sicherheitsgruppen von Amazon Elastic Compute Cloud (Amazon EC2) können bei der Verwaltung des Netzwerkzugriffs helfen, indem sie eine statusbehaftete Filterung des ein- und ausgehenden Netzwerkverkehrs zu Ressourcen bereitstellen. AWS Die Beschränkung des gesamten Datenverkehrs auf die Standardsicherheitsgruppe hilft dabei, den Fernzugriff auf Ihre Ressourcen einzuschränken. AWS

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
Ihre Systeme-3	Implementieren Sie Sicherheitskonfigurationen für alle Hardware- und Softwareressourcen.	vpc-sg-open-only-to-authorized-ports	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass gemeinsame Ports für Amazon Elastic Compute Cloud (Amazon EC2) -Sicherheitsgruppen eingeschränkt sind. Wenn der Zugriff auf Ports nicht auf vertrauenswürdige Quellen beschränkt wird, kann dies zu Angriffen auf die Verfügbarkeit, Integrität und Vertraulichkeit von Systemen führen. Durch die Beschränkung des Zugriffs auf Ressourcen innerhalb einer Sicherheitsgruppe aus dem Internet (0.0.0.0/0) kann der Remote-Zugriff auf interne Systeme gesteuert werden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
Ihre Systeme-3	Implementieren Sie Sicherheitskonfigurationen für alle Hardware- und Softwareressourcen.	wafv2-logging-enabled	Um die Protokollierung und Überwachung in Ihrer Umgebung zu erleichtern, aktivieren Sie die AWS WAF (V2) -Protokollierung im regionalen und globalen Web ACLs. AWS Die WAF-Protokollierung bietet detaillierte Informationen über den Datenverkehr, der von Ihrer Web-ACL analysiert wird. In den Protokollen werden die Uhrzeit aufgezeichnet, zu der die AWS WAF die Anfrage von Ihrer AWS Ressource erhalten hat, Informationen über die Anfrage und eine Aktion für die Regel, der jede Anfrage entsprach.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
Ihre Systeme-3	Implementieren Sie Sicherheitskonfigurationen für alle Hardware- und Softwareressourcen.	ecs-task-definition-user-for-host-mode-check	Wenn für eine Aufgabendefinition erhöhte Berechtigungen gelten, liegt das daran, dass der Kunde diesen Konfigurationen ausdrücklich zugestimmt hat. Diese Kontrolle prüft, ob eine unerwartete Berechtigungseskalation vorliegt, wenn für eine Aufgabendefinition das Host-Netzwerk aktiviert ist, die Kunden aber keine erhöhten Berechtigungen aktiviert haben.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
Ihre Systeme-3	Implementieren Sie Sicherheitskonfigurationen für alle Hardware- und Softwareressourcen.	autoscaling-launch-config-public-ip-deaktiviert	Wenn Sie Ihre Netzwerkschnittstellen mit einer öffentlichen IP-Adresse konfigurieren, sind die diesen Netzwerkschnittstellen zugehörigen Ressourcen über das Internet erreichbar. EC2 Ressourcen sollten nicht öffentlich zugänglich sein, da dies einen unbeabsichtigten Zugriff auf Ihre Anwendungen oder Server ermöglichen kann.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
Ihre Systeme-3	Implementieren Sie Sicherheitskonfigurationen für alle Hardware- und Softwareressourcen.	aurora-resources-protected-by-Backup-Plan	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon Aurora Aurora-Ressourcen Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
Ihre Systeme-3	Implementieren Sie Sicherheitskonfigurationen für alle Hardware- und Softwareressourcen.	backup-recovery-point-encrypted	Stellen Sie sicher, dass die Verschlüsselung für Ihre AWS Backup-Wiederherstellungspunkte aktiviert ist. Da sensible Daten auch im Ruhezustand vorhanden sein können, sollten Sie die Verschlüsselung im Ruhezustand aktivieren, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
Ihre Systeme-3	Implementieren Sie Sicherheitskonfigurationen für alle Hardware- und Softwareressourcen.	backup-recovery-point-manual-Löschen-deaktiviert	Stellen Sie sicher, dass Ihren AWS Backup-Wiederherstellungspunkten eine ressourcenbasierte Richtlinie zugeordnet ist, die das Löschen von Wiederherstellungspunkten verhindert. Die Verwendung einer ressourcenbasierten Richtlinie zur Verhinderung des Löschens von Wiederherstellungspunkten kann dazu beitragen, ein versehentliches oder absichtliches Löschen zu unterbinden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
Ihre Systeme-3	Implementieren Sie Sicherheitskonfigurationen für alle Hardware- und Softwareressourcen.	dynamodb-resources-protected-by-Backup-Plan	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon DynamoDB DynamoDB-Ressourcen Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
Ihre Systeme-3	Implementieren Sie Sicherheitskonfigurationen für alle Hardware- und Softwareressourcen.	ec2--Plan resources-protected-by-backup	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon Elastic Compute Cloud (Amazon EC2) -Ressourcen Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
Ihre Systeme-3	Implementieren Sie Sicherheitskonfigurationen für alle Hardware- und Softwareressourcen.	fsx-resources-protected-by-Backup-Plan	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre FSx Amazon-Dateisysteme Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
Ihre Systeme-4	Entfernen Sie nicht unterstützte oder nicht autorisierte Hardware und Software von den Systemen.	securityhub-enabled	AWS Security Hub hilft bei der Überwachung von unbefugtem Personal, Verbindungen, Geräten und Software. AWS Security Hub aggregiert, organisiert und priorisiert die Sicherheitswarnungen oder Ergebnisse mehrerer Dienste. AWS Einige dieser Dienste sind Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer und AWS Firewall Manager sowie AWS Partnerlösungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
Ihre Umgebungen-1	Erfahren Sie, wer sich in Ihrem Netzwerk befindet. Führen Sie eine Bestandsaufnahme der Netzwerkv erbindungen durch (Benutzer, Anbieter, Geschäftspartner usw.).	eip-attached	Diese Regel stellt sicher, dass Elastic, die einer Amazon Virtual Private Cloud (Amazon VPC) IPs zugewiesen sind, an Amazon Elastic Compute Cloud (Amazon EC2) - Instances oder verwendete Elastic Network Interface s angehängt sind. Diese Regel hilft bei der Überwachu ng ungenutzter Inhalte EIPs in Ihrer Umgebung.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
Ihre Umgebungen-1	Erfahren Sie, wer sich in Ihrem Netzwerk befindet. Führen Sie eine Bestandsaufnahme der Netzwerkv erbindungen durch (Benutzer, Anbieter, Geschäftspartner usw.).	vpc-flow-logs-enabled	VPC-Flow-Protokoll e erfassen detaillierte Informationsdatens ätze über den IP-Datenverkehr, der zu und von Netzwerkschnittste llen in Ihrer Amazon Virtual Private Cloud (Amazon VPC) fließt. Standardmäßig enthalten Flow-Prot okolldatensätze Werte für die verschiedenen Komponenten des IP-Flows, einschlie ßlich Quelle, Ziel und Protokoll.
Ihre Umgebungen-1	Erfahren Sie, wer sich in Ihrem Netzwerk befindet. Führen Sie eine Bestandsaufnahme der Netzwerkv erbindungen durch (Benutzer, Anbieter, Geschäftspartner usw.).	vpc-network-acl-un used-überprüfen	Diese Regel stellt sicher, dass Amazon Virtual Private Cloud (VPC)-Netzwerkzugr iffskontrolllisten verwendet werden. Die Überwachu ng ungenutzter Netzwerkzugriffsko ntrolllisten kann zu einer genauen Inventarisierung und Verwaltung Ihrer Umgebung beitragen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
Ihre Umgebungen-2	Nutzen Sie die Multi-Faktor-Authentifizierung für alle Benutzer, angefangen bei privilegierten Benutzern sowie Benutzern mit Administratorrechten und Remote-Zugriff.	iam-user-mfa-enabled	Aktivieren Sie diese Regel, um den Zugriff auf Ressourcen in der AWS Cloud einzuschränken. Diese Regel sorgt dafür, dass die Multi-Faktor-Authentifizierung (MFA) für alle Benutzer aktiviert ist. MFA sorgt für eine weitere Schutzebene zusätzlich zu den Anmeldeinformationen. Reduzieren Sie Fälle von kompromittierten Konten, indem Sie MFA für Benutzer vorschreiben.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
Ihre Umgebungen-2	Nutzen Sie die Multi-Faktor-Authentifizierung für alle Benutzer, angefangen bei privilegierten Benutzern sowie Benutzern mit Administratorrechten und Remote-Zugriff.	mfa-enabled-for-iam-Konsolenzugriff	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass MFA für alle AWS Identity and Access Management (IAM) -Benutzer aktiviert ist, die über ein Konsolenkennwort verfügen. MFA sorgt für eine weitere Schutzebene zusätzlich zu den Anmeldeinformationen. Indem Sie MFA für Benutzer vorschreiben, können Sie Fälle kompromittierter Konten reduzieren und verhindern, dass unbefugte Benutzer auf vertrauliche Daten zugreifen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
Ihre Umgebungen-2	Nutzen Sie die Multi-Faktor-Authentifizierung für alle Benutzer, angefangen bei privilegierten Benutzern sowie Benutzern mit Administratorrechten und Remote-Zugriff.	root-account-hardware-mfa-aktiviert	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Hardware-MFA für den Root-Benutzer aktiviert ist. Der Stammbenutzer ist der AWS-Konto-Benutzer mit den meisten Berechtigungen. MFA sorgt für eine weitere Schutzebene zusätzlich zu den Anmeldeinformationen. Indem Sie MFA für den Root-Benutzer vorschreiben, können Sie die Anzahl AWS-Konten kompromittierter Benutzer reduzieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
Ihre Umgebungen-2	Nutzen Sie die Multi-Faktor-Authentifizierung für alle Benutzer, angefangen bei privilegierten Benutzern sowie Benutzern mit Administratorrechten und Remote-Zugriff.	root-account-mfa-enabled	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass MFA für den Root-Benutzer aktiviert ist. Der Stammbenutzer ist der AWS-Konto-Benutzer mit den meisten Berechtigungen. MFA sorgt für eine weitere Schutzebene zusätzlich zu den Anmeldeinformationen. Indem Sie MFA für den Root-Benutzer vorschreiben, können Sie die Anzahl AWS-Konten kompromittierter Benutzer reduzieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
Ihre Umgebungen-3	Gewähren Sie Zugriffs- und Administratorberechtigungen auf der Grundlage der need-to-know geringsten Rechte.	iam-no-inline-policy-überprüfen	Stellen Sie sicher, dass ein Benutzer, eine IAM-Rolle oder eine IAM-Gruppe (AWS Identity and Access Management) nicht über eine Inline-Richtlinie zur Zugriffskontrolle auf Systeme und Ressourcen verfügt. AWS empfiehlt, verwaltete Richtlinien anstelle von Inline-Richtlinien zu verwenden. Verwaltete Richtlinien ermöglichen Wiederverwendbarkeit, Versionsverwaltung, Rollback und Delegierung der Berechtigungsverwaltung.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
Ihre Umgebungen-3	Gewähren Sie Zugriffs- und Administratorberechtigungen auf der Grundlage der need-to-know geringsten Rechte.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) kann Ihnen dabei helfen, die Prinzipien der geringsten Rechte und der Aufgabentrennung in Zugriffsberechtigungen und Autorisierungen zu integrieren und so zu verhindern, dass Richtlinien „Effect“: „Allow“ mit „Action“: „*“ anstelle von „Resource“: „*“ enthalten. Wenn Benutzern mehr Rechte eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und der Aufgabentrennung verstoßen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
Ihre Umgebungen-3	Gewähren Sie Zugriffs- und Administratorberechtigungen auf der Grundlage der geringsten need-to-know Rechte.	iam-policy-no-statements-with-full-access	Stellen Sie sicher, dass IAM-Aktionen nur auf die benötigten Aktionen beschränkt sind. Wenn Benutzern mehr Rechte eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und der Aufgabentrennung verstoßen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
Ihre Umgebungen-3	Gewähren Sie Zugriffs- und Administratorberechtigungen auf der Grundlage der need-to-know geringsten Rechte.	iam-root-access-key-überprüfen	Der Zugriff auf Systeme und Ressourcen kann gesteuert werden, indem überprüft wird, ob der Root-Benutzer keine Zugriffsschlüssel mit seiner AWS Identity and Access Management (IAM) -Rolle verknüpft hat. Stellen Sie sicher, dass die Root-Zugriffsschlüssel gelöscht werden. Erstellen und verwenden Sie stattdessen rollenbasierte Funktionen, AWS-Konten um das Prinzip der geringsten Funktionalität zu berücksichtigen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
Ihre Umgebungen-3	Gewähren Sie Zugriffs- und Administratorberechtigungen auf der Grundlage der need-to-know geringsten Rechte.	s-3 bucket-policy-grantee-check	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie s3_bucket_policy_grantee_check aktivieren. Diese Regel prüft, ob der vom Amazon S3 S3-Bucket gewährte Zugriff durch die von Ihnen bereitgestellten AWS Principals, Verbundbenutzer, Service Principals, IP-Adressen oder Amazon Virtual Private Cloud (Amazon VPC) IDs eingeschränkt ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
Ihre Umgebungen-3	Gewähren Sie Zugriffs- und Administratorberechtigungen auf need-to-know der Grundlage der geringsten Rechte.	secretsmanager-secret-unused	Wenn in AWS Secrets Manager unbenutzte Anmeldeinformationen vorhanden sind, sollten Sie die Anmeldeinformationen deaktivieren und/oder entfernen, da dies gegen das Prinzip der geringsten Rechte verstoßen kann. Mit dieser Regel können Sie einen Wert auf unusedForDays (Config Default: 90) setzen. Der tatsächliche Wert muss den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
Ihre Umgebungen-3	Gewähren Sie Zugriffs- und Administratorberechtigungen auf der Grundlage der need-to-know geringsten Rechte.	opensearch-access-control-enabled	Stellen Sie sicher, dass eine detaillierte Zugriffskontrolle für Ihre Amazon OpenSearch Service-Domains aktiviert ist. Eine differenzierte Zugriffskontrolle bietet erweiterte Autorisierungsmechanismen, um den Zugriff auf Amazon Service-Domains mit den geringsten Rechten zu erreichen. OpenSearch Es ermöglicht eine rollenbasierte Zugriffskontrolle auf die Domain sowie Sicherheit auf Index-, Dokument- und Feldebene, Unterstützung für OpenSearch Service-Dashboards, Mehrmandantenfähigkeit und HTTP-Basisauthentifizierung für Service und Kibana. OpenSearch

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
Ihre Umgebungen-4	Nutzen Sie eindeutige Passwörter für alle Benutzer.	iam-password-policy	Die Identitäten und Anmeldeinformationen werden auf der Grundlage einer organisatorischen IAM-Passwortrichtlinie ausgestellt, verwaltet und verifiziert. Sie erfüllen oder übertreffen die Anforderungen von NIST SP 800-63 und dem Standard „Best Practices“ von Foundational Security für die Passwortstärke. AWS Mit dieser Regel können Sie optional RequireUppercaseCharacters (Wert für AWS grundlegende Sicherheitsbewährte Methoden: wahr), RequireLowercaseCharacters (Wert für bewährte Methoden für AWS grundlegende Sicherheit: wahr), RequireSymbols (Wert für bewährte Methoden für AWS grundlegende Sicherheit:

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			wahr), RequireNumbers (Wert für bewährte Methoden für AWS grundlegende Sicherheit: wahr), MinimumPasswordLength (Wert für bewährte Methoden für AWS grundlegende Sicherheit: 14), PasswordReusePrevention (Wert für bewährte Methoden für AWS grundlegende Sicherheit: 24) und MaxPasswordAge (Wert für bewährte Methoden für AWS grundlegende Sicherheit: 90) für Ihr IAM festlegen Kennwortrichtlinie. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
Ihre Daten-1	Erfahren Sie, wie Ihre Daten geschützt werden.	kms-cmk-not-scheduled-zum Löschen	Um Daten im Ruhezustand zu schützen, sollten Sie sicherstellen, dass die für den Kunden erforderlichen Masterschlüssel (CMKs) nicht für das Löschen im AWS Key Management Service (AWS KMS) vorgesehen sind. Da Schlüssel manchmal gelöscht werden müssen, können Sie mit dieser Regel alle zu löschenden Schlüssel überprüfen, falls ein Schlüssel versehentlich zur Löschung vorgemerkt wurde.
Ihre Daten-1	Erfahren Sie, wie Ihre Daten geschützt werden.	opensearch-encrypted-at-rest	Da sensible Daten vorhanden sein können und um Daten im Ruhezustand zu schützen, sollten Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon OpenSearch Service-Domains aktiviert ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
Ihre Daten-1	Erfahren Sie, wie Ihre Daten geschützt werden.	opensearch-https-required	Da sensible Daten existieren können und um Daten während der Übertragung zu schützen, sollten Sie sicherstellen, dass HTTPS für Verbindungen zu Ihren Amazon OpenSearch Service-Domains aktiviert ist.
Ihre Daten-1	Erfahren Sie, wie Ihre Daten geschützt werden.	alb-http-to-https-Umleitungsprüfung	Um Daten während der Übertragung zu schützen, stellen Sie sicher, dass Ihr Application Load Balancer unverschlüsselte HTTP-Anfragen automatisch an HTTPS umleitet. Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
Ihre Daten-1	Erfahren Sie, wie Ihre Daten geschützt werden.	api-gw-cache-enabled-und-verschlüsselt	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass die Verschlüsselung für den Cache Ihrer API-Gateway-Stufe aktiviert ist. Da für die API-Methode sensible Daten erfasst werden können, sollten Sie die Verschlüsselung von Daten im Ruhezustand aktivieren, um diese Daten zu schützen.
Ihre Daten-1	Erfahren Sie, wie Ihre Daten geschützt werden.	cloudwatch-log-group-encrypted	Um sensible Daten im Speicher zu schützen, stellen Sie sicher, dass die Verschlüsselung für Ihre Amazon CloudWatch Log Groups aktiviert ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
Ihre Daten-1	Erfahren Sie, wie Ihre Daten geschützt werden.	dynamodb-table-encrypted-kms	Stellen Sie sicher, dass die Verschlüsselung für Ihre Amazon-DynamoDB-Tabellen aktiviert ist. Um eventuell vorhandene sensible Daten im Ruhezustand in diesen Tabellen zu schützen, müssen Sie die Verschlüsselung von Daten im Ruhezustand aktivieren. Standardmäßig werden DynamoDB-Tabellen mit einem AWS eigenen Kundenhauptschlüssel (CMK) verschlüselt.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
Ihre Daten-1	Erfahren Sie, wie Ihre Daten geschützt werden.	ec2- ebs-encryption-by-default	Zum Schutz von Daten im Ruhezustand müssen Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon Elastic Block Store (Amazon EBS)-Volumes aktiviert ist. Da sensible Daten auch im Ruhezustand vorhanden sein können, sollten Sie die Verschlüsselung im Ruhezustand aktivieren, um diese Daten zu schützen.
Ihre Daten-1	Erfahren Sie, wie Ihre Daten geschützt werden.	efs-encrypted-check	Aktivieren Sie die Verschlüsselung für Ihr Amazon Elastic File System (EFS), um eventuell vorhandene sensible Daten sowie Daten im Ruhezustand zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
Ihre Daten-1	Erfahren Sie, wie Ihre Daten geschützt werden.	elasticsearch-encrypted-at-rest	Da sensible Daten vorhanden sein können und um Daten im Ruhezustand zu schützen, sollten Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon OpenSearch Service (OpenSearch Service) -Domains aktiviert ist.
Ihre Daten-1	Erfahren Sie, wie Ihre Daten geschützt werden.	encrypted-volumes	Aktivieren Sie die Verschlüsselung für Ihre Amazon-Elastic-Block-Store (Amazon-EBS)-Volumes, um eventuell vorhandene sensible Daten sowie Daten im Ruhezustand zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
Ihre Daten-1	Erfahren Sie, wie Ihre Daten geschützt werden.	elb-acm-certificate-required	Zum Schutz von eventuell vorhanden en sensiblen Daten sowie von Daten während der Übertragung muss die Verschlüsselung für Ihr Elastic Load Balancing aktiviert sein. Verwenden Sie AWS Certificate Manager, um öffentlic he und private SSL/ TLS-Zertifikate mit AWS Diensten und internen Ressource n zu verwalten, bereitzustellen und bereitzustellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
Ihre Daten-1	Erfahren Sie, wie Ihre Daten geschützt werden.	elbv2- acm-certificate-required	Zum Schutz von eventuell vorhanden en sensiblen Daten sowie von Daten während der Übertragung muss die Verschlüsselung für Ihr Elastic Load Balancing aktiviert sein. Verwenden Sie AWS Certificate Manager, um öffentlic he und private SSL/ TLS-Zertifikate mit AWS Diensten und internen Ressource n zu verwalten, bereitzustellen und bereitzustellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
Ihre Daten-1	Erfahren Sie, wie Ihre Daten geschützt werden.	rds-snapshot-encrypted	Stellen Sie sicher, dass die Verschlüsselung für Ihre Amazon Relational Database Service (Amazon RDS)-Snapshots aktiviert ist. Da sensible Daten auch im Ruhezustand vorhanden sein können, sollten Sie die Verschlüsselung im Ruhezustand aktivieren, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
Ihre Daten-1	Erfahren Sie, wie Ihre Daten geschützt werden.	rds-storage-encrypted	Zum Schutz von Daten im Ruhezustand müssen Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon Relational Database Service (Amazon RDS)-Instances aktiviert ist. Um eventuell vorhandene sensible Daten im Ruhezustand in Amazon-RDS-Instances zu schützen, muss die Verschlüsselung von Daten im Ruhezustand aktiviert sein.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
Ihre Daten-1	Erfahren Sie, wie Ihre Daten geschützt werden.	redshift-cluster-configuration-check	Um Daten im Ruhezustand zu schützen, muss die Verschlüsselung für Ihre Amazon-Redshift-Cluster aktiviert sein. Sie müssen auch sicherstellen, dass die erforderlichen Konfigurationen auf Amazon-Redshift-Clustern bereitgestellt werden. Die Prüfungsprotokollierung muss aktiviert sein, um Informationen zu Verbindungen und Benutzeraktivitäten in der Datenbank bereitzustellen. Diese Regel erfordert, dass ein Wert für clusterDbEncrypted (Config Default: TRUE) und LoggingEnabled (Config Default: TRUE) gesetzt ist. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
Ihre Daten-1	Erfahren Sie, wie Ihre Daten geschützt werden.	redshift-cluster-kms-enabled	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass die Verschlüs selung mit AWS Key Management Service (AWS KMS) für Ihren Amazon Redshift Redshift-Cluster aktiviert ist. Um eventuell vorhanden e sensible Daten im Ruhezustand in Redshift-Clustern zu schützen, muss die Verschlüsselung von Daten im Ruhezusta nd aktiviert sein.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
Ihre Daten-1	Erfahren Sie, wie Ihre Daten geschützt werden.	s3- aktiviert bucket-server-side-encryption	Zum Schutz von Daten im Ruhezustand müssen Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon Simple Storage Service (Amazon S3)-Buckets aktiviert ist. Um eventuell vorhandene sensible Daten im Ruhezustand in Amazon-S3-Buckets zu schützen, muss die Verschlüsselung aktiviert sein.
Ihre Daten-1	Erfahren Sie, wie Ihre Daten geschützt werden.	s-3 default-encryption-kms	Stellen Sie sicher, dass die Verschlüsselung für Ihre Amazon Simple Storage Service (Amazon S3)-Buckets aktiviert ist. Um eventuell vorhandene sensible Daten im Ruhezustand in einem Amazon-S3-Bucket zu schützen, muss die Verschlüsselung aktiviert sein.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
Ihre Daten-1	Erfahren Sie, wie Ihre Daten geschützt werden.	s-3 bucket-ssl-requests-only	Um Daten während der Übertragung zu schützen, stellen Sie sicher, dass Ihre Amazon Simple Storage Service (Amazon S3)-Buckets Anfragen zur Verwendung von Secure Socket Layer (SSL)-Buckets erfordern. Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
Ihre Daten-1	Erfahren Sie, wie Ihre Daten geschützt werden.	sagemaker-endpoint-configuration-kms-key-konfiguriert	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass die Verschlüsselung mit dem AWS Key Management Service (AWS KMS) für Ihren Endpunkt aktiviert ist. SageMaker Da sensible Daten auf dem SageMaker Endgerät gespeiche rt werden können, sollten Sie die Verschlüsselung im Ruhezustand aktiviere n, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
Ihre Daten-1	Erfahren Sie, wie Ihre Daten geschützt werden.	sagemaker-notebook-instance-kms-schlüsselkonfiguriert	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass die Verschlüsselung mit dem AWS Key Management Service (AWS KMS) für Ihr Notebook aktiviert ist. SageMaker Da vertrauliche Daten im SageMaker Notebook gespeichert werden können, sollten Sie die Verschlüsselung im Ruhezustand aktivieren, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
Ihre Daten-1	Erfahren Sie, wie Ihre Daten geschützt werden.	sns-encrypted-kms	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass Ihre Amazon Simple Notification Service (Amazon SNS) -Themen mit dem AWS Key Management Service (AWS KMS) verschlüsselt werden müssen. Um eventuell vorhandene sensible Daten im Ruhezustand in veröffentlichten Nachrichten zu schützen, muss die Verschlüsselung von Daten im Ruhezustand aktiviert sein.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
Ihre Daten-1	Erfahren Sie, wie Ihre Daten geschützt werden.	backup-recovery-point-encrypted	Stellen Sie sicher, dass die Verschlüsselung für Ihre AWS Backup-Wiederherstellungspunkte aktiviert ist. Da sensible Daten auch im Ruhezustand vorhanden sein können, sollten Sie die Verschlüsselung im Ruhezustand aktivieren, um diese Daten zu schützen.
Ihre Daten-2	Erfahren Sie, was in Ihrem Netzwerk passiert. Verwalten Sie Netzwerk- und Perimeterkomponenten, Host- und Gerätekomponenten sowie Aktivitäten während der Übertragung data-at-rest und des Benutzerverhaltens.	opensearch-audit-logging-enabled	Stellen Sie sicher, dass die Audit-Protokollierung für Ihre Amazon OpenSearch Service-Domains aktiviert ist. Mit der Audit-Protokollierung können Sie Benutzeraktivitäten auf Ihren OpenSearch Domains verfolgen, einschließlich erfolgreicher und fehlgeschlagener Authentifizierungen OpenSearch, Anfragen an, Indexänderungen und eingehende Suchanfragen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
Ihre Daten-2	Erfahren Sie, was in Ihrem Netzwerk passiert. Verwalten Sie Netzwerk- und Perimeterkomponenten, Host- und Gerätekomponenten sowie Aktivitäten während der Übertragung data-at-rest und des Benutzerverhaltens.	api-gw-cache-enabled-und verschlüsselt	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass die Verschlüsselung für den Cache Ihrer API-Gateway-Stufe aktiviert ist. Da für die API-Methode sensible Daten erfasst werden können, sollten Sie die Verschlüsselung von Daten im Ruhezustand aktivieren, um diese Daten zu schützen.
Ihre Daten-2	Erfahren Sie, was in Ihrem Netzwerk passiert. Verwalten Sie Netzwerk- und Perimeterkomponenten, Host- und Gerätekomponenten sowie Aktivitäten während der Übertragung data-at-rest und des Benutzerverhaltens.	opensearch-encrypted-at-rest	Da sensible Daten vorhanden sein können und um Daten im Ruhezustand zu schützen, sollten Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon OpenSearch Service-Domains aktiviert ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
Ihre Daten-2	Erfahren Sie, was in Ihrem Netzwerk passiert. Verwalten Sie Netzwerk- und Perimeterkomponenten, Host- und Gerätekomponenten sowie Aktivitäten während der Übertragung data-at-rest und des Benutzerverhaltens.	opensearch-https-required	Da sensible Daten existieren können und um Daten während der Übertragung zu schützen, sollten Sie sicherstellen, dass HTTPS für Verbindungen zu Ihren Amazon OpenSearch Service-Domains aktiviert ist.
Ihre Daten-2	Erfahren Sie, was in Ihrem Netzwerk passiert. Verwalten Sie Netzwerk- und Perimeterkomponenten, Host- und Gerätekomponenten sowie Aktivitäten während der Übertragung data-at-rest und des Benutzerverhaltens.	api-gw-execution-logging-aktiviert	Die API-Gateway-Protokollierung zeigt detaillierte Ansichten der Benutzer, die auf die API zugegriffen haben, und wie diese Benutzer auf die API zugegriffen haben. Diese Einblicke ermöglichen die Transparenz von Benutzeraktivitäten.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
Ihre Daten-2	Erfahren Sie, was in Ihrem Netzwerk passiert. Verwalten Sie Netzwerk- und Perimeterkomponenten, Host- und Gerätekomponenten sowie Aktivitäten während der Übertragung data-at-rest und des Benutzerverhaltens.	opensearch-logs-to-cloudwatch	Stellen Sie sicher, dass für Amazon OpenSearch Service-Domains Fehlerprotokolle aktiviert und zur Aufbewahrung und Beantwortung an Amazon CloudWatch Logs gestreamt werden. OpenSearch Service-Fehlerprotokolle können bei Sicherheits- und Zugriffsprüfungen helfen und bei der Diagnose von Verfügbarkeitsproblemen helfen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
Ihre Daten-2	Erfahren Sie, was in Ihrem Netzwerk passiert. Verwalten Sie Netzwerk- und Perimeterkomponenten, Host- und Gerätekomponenten sowie Aktivitäten während der Übertragung data-at-rest und des Benutzerverhaltens.	opensearch-node-to-node-Verschlüsselungsprüfung	Stellen Sie sicher, dass die node-to-node Verschlüsselung für Amazon OpenSearch Service aktiviert ist. Node-to-nodeVerschlüsselung ermöglicht die TLS 1.2-Verschlüsselung für die gesamte Kommunikation innerhalb der Amazon Virtual Private Cloud (Amazon VPC). Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
Ihre Daten-2	Erfahren Sie, was in Ihrem Netzwerk passiert. Verwalten Sie Netzwerk- und Perimeter komponenten, Host- und Gerätekom ponenten sowie Aktivitäten während der Übertragung data-at-rest und Benutzerv erhalten.	acm-certificate-ex piration-check	Stellen Sie sicher, dass die Netzwerki ntegrität geschützt ist, indem Sie sicherste llen, dass X509-Zertifikate von ACM ausgestellt werden. AWS Diese Zertifika te müssen gültig und dürfen nicht abgelaufen sein. Für diese Regel ist ein Wert für erforderlich daysToExpiration (Wert für bewährte AWS Grundregeln für Sicherheit: 90). Der tatsächliche Wert muss den Richtlini en Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
Ihre Daten-2	Erfahren Sie, was in Ihrem Netzwerk passiert. Verwalten Sie Netzwerk- und Perimeterkomponenten, Host- und Gerätekomponenten sowie Aktivitäten während der Übertragung data-at-rest und des Benutzerverhaltens.	alb-http-to-https-Umleitungsprüfung	Um Daten während der Übertragung zu schützen, stellen Sie sicher, dass Ihr Application Load Balancer unverschlüsselte HTTP-Anfragen automatisch an HTTPS umleitet. Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
Ihre Daten-2	Erfahren Sie, was in Ihrem Netzwerk passiert. Verwalten Sie Netzwerk- und Perimeterkomponenten, Host- und Gerätekomponenten sowie Aktivitäten während der Übertragung und des data-at-rest Benutzerverhaltens.	elbv2- acm-certificate-required	Zum Schutz von eventuell vorhandenen sensiblen Daten sowie von Daten während der Übertragung muss die Verschlüsselung für Ihr Elastic Load Balancing aktiviert sein. Verwenden Sie AWS Certificate Manager, um öffentliche und private SSL/TLS-Zertifikate mit AWS Diensten und internen Ressourcen zu verwalten, bereitzustellen und bereitzustellen.
Ihre Daten-2	Erfahren Sie, was in Ihrem Netzwerk passiert. Verwalten Sie Netzwerk- und Perimeterkomponenten, Host- und Gerätekomponenten sowie Aktivitäten während der Übertragung data-at-rest und des Benutzerverhaltens.	api-gw-execution-logging-aktiviert	Die API-Gateway-Protokollierung zeigt detaillierte Ansichten der Benutzer, die auf die API zugegriffen haben, und wie diese Benutzer auf die API zugegriffen haben. Diese Einblicke ermöglichen die Transparenz von Benutzeraktivitäten.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
Ihre Daten-2	Erfahren Sie, was in Ihrem Netzwerk passiert. Verwalten Sie Netzwerk- und Perimeterkomponenten, Host- und Gerätekomponenten sowie Aktivitäten während der Übertragung data-at-rest und des Benutzerverhaltens.	codebuild-project-source-repo-URL-Prüfung	Stellen Sie sicher, dass die URL des Quell-Repositorys GitHub oder des Bitbucket-Quell-Repositorys keine persönlichen Zugriffstoken oder Anmeldeinformationen in Codebuild-Projektumgebungen enthält. AWS Verwende OAuth anstelle von persönlichen Zugriffstoken oder Anmeldedaten die Autorisierung für den Zugriff auf GitHub Bitbucket-Repositorys.
Ihre Daten-2	Erfahre, was in deinem Netzwerk passiert. Verwalte Netzwerk- und Perimeterkomponenten, Host- und Gerätekomponenten sowie Aktivitäten während der Übertragung data-at-rest und des Benutzerverhaltens.	cloud-trail-cloud-watch-Logs aktiviert	Verwenden Sie Amazon CloudWatch , um Protokollereignisaktivitäten zentral zu sammeln und zu verwalten. Die Aufnahme von AWS CloudTrail Daten liefert Einzelheiten zu den API-Aufrufaktivitäten in Ihrem AWS-Konto.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
Ihre Daten-2	Erfahren Sie, was in Ihrem Netzwerk passiert. Verwalten Sie Netzwerk- und Perimeterkomponenten, Host- und Gerätekomponenten sowie Aktivitäten während der Übertragung data-at-rest und des Benutzerverhaltens.	cloudtrail-s3-dataevents-enabled	Die Erfassung von Simple Storage Service (Amazon S3)-Datenereignissen unterstützt die Erkennung von ungewöhnlichen Aktivitäten. Zu den Details gehören AWS-Konto Informationen über den Zugriff auf einen Amazon S3 S3-Bucket, die IP-Adresse und die Uhrzeit des Ereignisses.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
Ihre Daten-2	Erfahren Sie, was in Ihrem Netzwerk passiert. Verwalten Sie Netzwerk- und Perimeterkomponenten, Host- und Gerätekomponenten sowie Aktivitäten während der Übertragung data-at-rest und des Benutzerverhaltens.	elb-logging-enabled	Die Elastic-Load-Balancing-Aktivität ist ein zentraler Kommunikationspunkt innerhalb einer Umgebung. Stellen Sie sicher, dass die ELB-Protokollierung aktiviert ist. Die gesammelten Daten enthalten detaillierte Informationen zu Anfragen, die an den ELB gesendet wurden. Jedes Protokoll enthält Informationen wie die Zeit, zu der die Anforderung einging, die Client-IP-Adresse, Latenzen, Anforderungspfade und Serverantworten.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
Ihre Daten-2	Erfahren Sie, was in Ihrem Netzwerk passiert. Verwalten Sie Netzwerk- und Perimeterkomponenten, Host- und Gerätekomponenten sowie Aktivitäten während der Übertragung data-at-rest und des Benutzerverhaltens.	multi-region-cloudtrail-enabled	AWS CloudTrail zeichnet Aktionen und API-Aufrufe der AWS Management Console auf. Sie können feststellen, welche Benutzer und Konten angerufen wurden AWS, von welcher Quell-IP-Adresse aus die Anrufe getätigt wurden und wann die Anrufe erfolgten. CloudTrail übermittelt Protokolldateien aus allen AWS Regionen an Ihren S3-Bucket, wenn MULTI_REGION_CLOUD_TRAIL_ENABLED aktiviert ist. Außerdem wird beim AWS Start einer neuen Region derselbe Trail in der neuen Region erstellt. CloudTrail Dadurch erhalten Sie automatisch Protokolldateien mit API-Aktivitäten für die neue Region.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
Ihre Daten-2	Erfahren Sie, was in Ihrem Netzwerk passiert. Verwalten Sie Netzwerk- und Perimeterkomponenten, Host- und Gerätekomponenten sowie Aktivitäten während der Übertragung data-at-rest und des Benutzerverhaltens.	rds-logging-enabled	Um die Protokollierung und Überwachung in Ihrer Umgebung zu erleichtern, stellen Sie sicher, dass die Amazon Relational Database Service (Amazon RDS)-Protokollierung aktiviert ist. Mit der Amazon-RDS-Protokollierung können Sie Ereignisse wie Verbindungen, Verbindungsabbrüche, Abfragen oder abgefragte Tabellen erfassen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
Ihre Daten-2	Erfahren Sie, was in Ihrem Netzwerk passiert. Verwalten Sie Netzwerk- und Perimeterkomponenten, Host- und Gerätekomponenten sowie Aktivitäten während der Übertragung data-at-rest und des Benutzerverhaltens.	s-3 bucket-logging-enabled	Die Amazon Simple Storage Service (Amazon S3)-Serverzugriffsprotokollierung bietet eine Methode zur Überwachung des Netzwerks im Hinblick auf potenzielle Cybersicherheitsereignisse. Die Ereignisse werden überwacht, indem detaillierte Aufzeichnungen über die Anfragen erfasst werden, die an einen Amazon-S3-Bucket gestellt wurden. Jeder Zugriffsprotokolleintrag enthält Details zu einer einzelnen Zugriffsanfrage. Zu den Details gehören Anforderer, Bucket-Name, Anforderungszeit, Anforderungsaktion, Antwortstatus und Fehlercode, falls relevant.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
Ihre Daten-2	Erfahren Sie, was in Ihrem Netzwerk passiert. Verwalten Sie Netzwerk- und Perimeterkomponenten, Host- und Gerätekomponenten sowie Aktivitäten während der Übertragung data-at-rest und des Benutzerverhaltens.	vpc-flow-logs-enabled	VPC-Flow-Protokolle erfassen detaillierte Informationsdatensätze über den IP-Datenverkehr, der zu und von Netzwerkschnittstellen in Ihrer Amazon Virtual Private Cloud (Amazon VPC) fließt. Standardmäßig enthalten Flow-Protokolldatensätze Werte für die verschiedenen Komponenten des IP-Flows, einschließlich Quelle, Ziel und Protokoll.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
Ihre Daten-2	Erfahren Sie, was in Ihrem Netzwerk passiert. Verwalten Sie Netzwerk- und Perimeterkomponenten, Host- und Gerätekomponenten sowie Aktivitäten während der Übertragung data-at-rest und des Benutzerverhaltens.	wafv2-logging-enabled	Um Sie bei der Protokollierung und Überwachung in Ihrer Umgebung zu unterstützen, aktivieren Sie die AWS WAF (V2) -Protokollierung im regionalen und globalen Internet. ACLs AWS Die WAF-Protokollierung bietet detaillierte Informationen über den Datenverkehr, der von Ihrer Web-ACL analysiert wird. In den Protokollen werden die Uhrzeit aufgezeichnet, zu der die AWS WAF die Anfrage von Ihrer AWS Ressource erhalten hat, Informationen über die Anfrage und eine Aktion für die Regel, der jede Anfrage entsprach.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
Ihre Daten-2	Erfahren Sie, was in Ihrem Netzwerk passiert. Verwalten Sie Netzwerk- und Perimeterkomponenten, Host- und Gerätekomponenten sowie Aktivitäten während der Übertragung data-at-rest und des Benutzerverhaltens.	elasticsearch-logs-to-cloudwatch	Stellen Sie sicher, dass für Amazon OpenSearch Service-Domains Fehlerprotokolle aktiviert und zur Aufbewahrung und Beantwortung an Amazon CloudWatch Logs gestreamt werden. Domain-Fehlerprotokolle sind bei Sicherheits- und Zugriffsprüfungen sowie bei der Diagnose von Verfügbarkeitsproblemen nützlich.
Ihre Daten-2	Erfahren Sie, was in Ihrem Netzwerk passiert. Verwalten Sie Netzwerk- und Perimeterkomponenten, Host- und Gerätekomponenten sowie Aktivitäten während der Übertragung data-at-rest und des Benutzerverhaltens.	cloudwatch-log-group-encrypted	Um sensible Daten im Speicher zu schützen, stellen Sie sicher, dass die Verschlüsselung für Ihre Amazon CloudWatch Log Groups aktiviert ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
Ihre Daten-2	Erfahren Sie, was in Ihrem Netzwerk passiert. Verwalten Sie Netzwerk- und Perimeterkomponenten, Host- und Gerätekomponenten sowie Aktivitäten während der Übertragung data-at-rest und des Benutzerverhaltens.	dynamodb-table-encrypted-kms	Stellen Sie sicher, dass die Verschlüsselung für Ihre Amazon-DynamoDB-Tabellen aktiviert ist. Um eventuell vorhandene sensible Daten im Ruhezustand in diesen Tabellen zu schützen, müssen Sie die Verschlüsselung von Daten im Ruhezustand aktivieren. Standardmäßig werden DynamoDB-Tabellen mit einem AWS eigenen Kundenhauptschlüssel (CMK) verschlüsselt.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
Ihre Daten-2	Erfahren Sie, was in Ihrem Netzwerk passiert. Verwalten Sie Netzwerk- und Perimeter komponenten, Host- und Gerätekom ponenten sowie Aktivitäten während der Übertragung data-at-rest und Benutzerv erhalten.	ec2- ebs-encryption-by-default	Zum Schutz von Daten im Ruhezusta nd müssen Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon Elastic Block Store (Amazon EBS)-Volu mes aktiviert ist. Da sensible Daten auch im Ruhezusta nd vorhanden sein können, sollten Sie die Verschlüsselung im Ruhezustand aktivieren, um diese Daten zu schützen.
Ihre Daten-2	Erfahren Sie, was in Ihrem Netzwerk passiert. Verwalten Sie Netzwerk- und Perimeterkomponent en, Host- und Gerätekomponenten sowie Aktivität en während der Übertragung data-at-r est und des Benutzerv erhaltens.	efs-encrypted-check	Aktivieren Sie die Verschlüsselung für Ihr Amazon Elastic File System (EFS), um eventuell vorhandene sensible Daten sowie Daten im Ruhezustand zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
Ihre Daten-2	Erfahren Sie, was in Ihrem Netzwerk passiert. Verwalten Sie Netzwerk- und Perimeterkomponenten, Host- und Gerätekomponenten sowie Aktivitäten während der Übertragung data-at-rest und des Benutzerverhaltens.	elasticsearch-encrypted-at-rest	Da sensible Daten vorhanden sein können und um Daten im Ruhezustand zu schützen, sollten Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon OpenSearch Service (OpenSearch Service)-Domains aktiviert ist.
Ihre Daten-2	Erfahren Sie, was in Ihrem Netzwerk passiert. Verwalten Sie Netzwerk- und Perimeterkomponenten, Host- und Gerätekomponenten sowie Aktivitäten während der Übertragung data-at-rest und des Benutzerverhaltens.	encrypted-volumes	Aktivieren Sie die Verschlüsselung für Ihre Amazon-Elastic-Block-Store (Amazon-EBS)-Volumes, um eventuell vorhandene sensible Daten sowie Daten im Ruhezustand zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
Ihre Daten-2	Erfahren Sie, was in Ihrem Netzwerk passiert. Verwalten Sie Netzwerk- und Perimeterkomponenten, Host- und Gerätekomponenten sowie Aktivitäten während der Übertragung data-at-rest und des Benutzerverhaltens.	rds-snapshot-encrypted	Stellen Sie sicher, dass die Verschlüsselung für Ihre Amazon Relational Database Service (Amazon RDS)-Snapshots aktiviert ist. Da sensible Daten auch im Ruhezustand vorhanden sein können, sollten Sie die Verschlüsselung im Ruhezustand aktivieren, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
Ihre Daten-2	Erfahren Sie, was in Ihrem Netzwerk passiert. Verwalten Sie Netzwerk- und Perimeterkomponenten, Host- und Gerätekomponenten sowie Aktivitäten während der Übertragung data-at-rest und des Benutzerverhaltens.	rds-storage-encrypted	Zum Schutz von Daten im Ruhezustand müssen Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon Relational Database Service (Amazon RDS)-Instances aktiviert ist. Um eventuell vorhandene sensible Daten im Ruhezustand in Amazon-RDS-Instances zu schützen, muss die Verschlüsselung von Daten im Ruhezustand aktiviert sein.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
Ihre Daten-2	Erfahren Sie, was in Ihrem Netzwerk passiert. Verwalten Sie Netzwerk- und Perimeterkomponenten, Host- und Gerätekomponenten sowie Aktivitäten während der Übertragung data-at-rest und des Benutzerverhaltens.	redshift-cluster-configuration-check	Um Daten im Ruhezustand zu schützen, muss die Verschlüsselung für Ihre Amazon-Redshift-Cluster aktiviert sein. Sie müssen auch sicherstellen, dass die erforderlichen Konfigurationen auf Amazon-Redshift-Clustern bereitgestellt werden. Die Prüfungsprotokollierung muss aktiviert sein, um Informationen zu Verbindungen und Benutzeraktivitäten in der Datenbank bereitzustellen. Diese Regel erfordert, dass ein Wert für clusterDbEncrypted (Config Default: TRUE) und LoggingEnabled (Config Default: TRUE) gesetzt ist. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
Ihre Daten-2	Erfahren Sie, was in Ihrem Netzwerk passiert. Verwalten Sie Netzwerk- und Perimeterkomponenten, Host- und Gerätekomponenten sowie Aktivitäten während der Übertragung data-at-rest und des Benutzerverhaltens.	redshift-cluster-kms-enabled	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass die Verschlüsselung mit AWS Key Management Service (AWS KMS) für Ihren Amazon Redshift Redshift-Cluster aktiviert ist. Um eventuell vorhandene sensible Daten im Ruhezustand in Redshift-Clustern zu schützen, muss die Verschlüsselung von Daten im Ruhezustand aktiviert sein.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
Ihre Daten-2	Erfahren Sie, was in Ihrem Netzwerk passiert. Verwalten Sie Netzwerk- und Perimeterkomponenten, Host- und Gerätekomponenten sowie Aktivitäten während der Übertragung data-at-rest und des Benutzerverhaltens.	s3-fähig bucket-server-side-encryption	Zum Schutz von Daten im Ruhezustand müssen Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon Simple Storage Service (Amazon S3)-Buckets aktiviert ist. Um eventuell vorhandene sensible Daten im Ruhezustand in Amazon-S3-Buckets zu schützen, muss die Verschlüsselung aktiviert sein.
Ihre Daten-2	Erfahren Sie, was in Ihrem Netzwerk passiert. Verwalten Sie Netzwerk- und Perimeterkomponenten, Host- und Gerätekomponenten sowie Aktivitäten während der Übertragung data-at-rest und des Benutzerverhaltens.	s-3 default-encryption-kms	Stellen Sie sicher, dass die Verschlüsselung für Ihre Amazon Simple Storage Service (Amazon S3)-Buckets aktiviert ist. Um eventuell vorhandene sensible Daten im Ruhezustand in einem Amazon-S3-Bucket zu schützen, muss die Verschlüsselung aktiviert sein.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
Ihre Daten-2	Erfahren Sie, was in Ihrem Netzwerk passiert. Verwalten Sie Netzwerk- und Perimeterkomponenten, Host- und Gerätekomponenten sowie Aktivitäten während der Übertragung data-at-rest und des Benutzerverhaltens.	sagemaker-endpoint-configuration-kms-schlüsselkonfiguriert	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass die Verschlüsselung mit dem AWS Key Management Service (AWS KMS) für Ihren Endpunkt aktiviert ist. SageMaker Da sensible Daten auf dem SageMaker Endgerät gespeichert werden können, sollten Sie die Verschlüsselung im Ruhezustand aktivieren, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
Ihre Daten-2	Erfahren Sie, was in Ihrem Netzwerk passiert. Verwalten Sie Netzwerk- und Perimeterkomponenten, Host- und Gerätekomponenten data-at-rest sowie Aktivitäten während der Übertragung und Benutzerverhalten.	sagemaker-notebook-instance-kms-schlüsselkonfiguriert	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass die Verschlüsselung mit dem AWS Key Management Service (AWS KMS) für Ihr Notebook aktiviert ist. SageMaker Da vertrauliche Daten im SageMaker Notebook gespeichert werden können, sollten Sie die Verschlüsselung im Ruhezustand aktivieren, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
Ihre Daten-2	Erfahren Sie, was in Ihrem Netzwerk passiert. Verwalten Sie Netzwerk- und Perimeterkomponenten, Host- und Gerätekomponenten data-at-rest sowie Aktivitäten während der Übertragung und Benutzerverhalten.	sns-encrypted-kms	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass Ihre Amazon Simple Notification Service (Amazon SNS) -Themen mit dem AWS Key Management Service (AWS KMS) verschlüsselt werden müssen. Um eventuell vorhandene sensible Daten im Ruhezustand in veröffentlichten Nachrichten zu schützen, muss die Verschlüsselung von Daten im Ruhezustand aktiviert sein.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
Ihre Daten-2	Erfahren Sie, was in Ihrem Netzwerk passiert. Verwalten Sie Netzwerk- und Perimeter komponenten, Host- und Gerätekom ponenten sowie Aktivitäten während der Übertragung data-at-rest und Benutzerv erhalten.	backup-recovery-po int-encrypted	Stellen Sie sicher, dass die Verschlüs selung für Ihre AWS Backup-Wiederherst ellungspunkte aktiviert ist. Da sensible Daten auch im Ruhezusta nd vorhanden sein können, sollten Sie die Verschlüsselung im Ruhezustand aktivieren, um diese Daten zu schützen.
Ihre Daten-2	Erfahren Sie, was in Ihrem Netzwerk passiert. Verwalten Sie Netzwerk- und Perimeterkomponent en, Host- und Gerätekomponenten sowie Aktivität en während der Übertragung data-at-r est und des Benutzerv erhaltens.	api-gw-ssl-enabled	Stellen Sie sicher, dass die REST-API-Stufen von Amazon API Gateway mit SSL-Zertifikaten konfiguri ert sind, damit Backend-Systeme überprüfen können, ob Anforderungen von API Gateway stammen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
Ihre Daten-2	Erfahren Sie, was in Ihrem Netzwerk passiert. Verwalten Sie Netzwerk- und Perimeterkomponenten, Host- und Gerätekomponenten sowie Aktivitäten während der Übertragung data-at-rest und des Benutzerverhaltens.	elasticsearch-node-to-node-Verschlüsselungsprüfung	Stellen Sie sicher, dass die node-to-node Verschlüsselung für Amazon OpenSearch Service aktiviert ist. Node-to-nodeVerschlüsselung ermöglicht die TLS 1.2-Verschlüsselung für die gesamte Kommunikation innerhalb der Amazon Virtual Private Cloud (Amazon VPC). Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
Ihre Daten-2	Erfahren Sie, was in Ihrem Netzwerk passiert. Verwalten Sie Netzwerk- und Perimeter komponenten, Host- und Gerätekom ponenten sowie Aktivitäten während der Übertragung data-at-rest und Benutzerv erhalten.	elb-acm-certificate-required	Zum Schutz von eventuell vorhanden en sensiblen Daten sowie von Daten während der Übertragung muss die Verschlüsselung für Ihr Elastic Load Balancing aktiviert sein. Verwenden Sie AWS Certificate Manager, um öffentlic he und private SSL/ TLS-Zertifikate mit AWS Diensten und internen Ressource n zu verwalten, bereitzustellen und bereitzustellen.
Ihre Daten-2	Erfahren Sie, was in Ihrem Netzwerk passiert. Verwalten Sie Netzwerk- und Perimeterkomponent en, Host- und Gerätekomponenten sowie Aktivität en während der Übertragung data-at-r est und des Benutzerv erhaltens.	elb-tls-https-listeners-nur	Stellen Sie sicher, dass Ihre Elastic Load Balancer (ELBs) mit SSL- oder HTTPS-Listenern konfiguriert sind. Um eventuell vorhanden e sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
Ihre Daten-2	Erfahren Sie, was in Ihrem Netzwerk passiert. Verwalten Sie Netzwerk- und Perimeterkomponenten, Host- und Gerätekomponenten sowie Aktivitäten während der Übertragung data-at-rest und des Benutzerverhaltens.	redshift-require-tls-ssl	Stellen Sie sicher, dass Ihre Amazon-Redshift-Cluster eine TLS/SSL-Verschlüsselung erfordern, um eine Verbindung zu SQL-Clients herzustellen. Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.
Ihre Daten-2	Erfahren Sie, was in Ihrem Netzwerk passiert. Verwalten Sie Netzwerk- und Perimeterkomponenten, Host- und Gerätekomponenten sowie Aktivitäten während der Übertragung data-at-rest und des Benutzerverhaltens.	s-3 bucket-ssl-requests-only	Um Daten während der Übertragung zu schützen, stellen Sie sicher, dass Ihre Amazon Simple Storage Service (Amazon S3)-Buckets Anfragen zur Verwendung von Secure Socket Layer (SSL)-Buckets erfordern. Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
Ihre Daten-2	Erfahren Sie, was in Ihrem Netzwerk passiert. Verwalten Sie Netzwerk- und Perimeterkomponenten, Host- und Gerätekomponenten sowie Aktivitäten während der Übertragung data-at-rest und des Benutzerverhaltens.	alb-waf-enabled	Stellen Sie sicher, dass AWS WAF auf Elastic Load Balancers (ELB) aktiviert ist, um Webanwendungen zu schützen. Eine WAF trägt zum Schutz Ihrer Webanwendungen oder APIs vor gängigen Web-Exploits bei. Diese Web-Exploits können sich auf die Verfügbarkeit auswirken, die Sicherheit gefährden oder übermäßige Ressourcen in Ihrer Umgebung verbrauchen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
Ihre Daten-2	Erfahren Sie, was in Ihrem Netzwerk passiert. Verwalten Sie Netzwerk- und Perimeterkomponenten, Host- und Gerätekomponenten sowie Aktivitäten während der Übertragung data-at-rest und des Benutzerverhaltens.	dms-replication-not-public	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass auf DMS-Replikationsinstanzen nicht öffentlich zugegriffen werden kann. DMS-Replikations-Instances können vertrauliche Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.
Ihre Daten-2	Erfahren Sie, was in Ihrem Netzwerk passiert. Verwalten Sie Netzwerk- und Perimeterkomponenten, Host- und Gerätekomponenten sowie Aktivitäten während der Übertragung data-at-rest und des Benutzerverhaltens.	ebs-snapshot-public-restorable-überprüfen	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass EBS-Snapshots nicht öffentlich wiederherstellbar sind. EBS-Volume-Snapshots können vertrauliche Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
Ihre Daten-2	Erfahren Sie, was in Ihrem Netzwerk passiert. Verwalten Sie Netzwerk- und Perimeterkomponenten, Host- und Gerätekomponenten sowie Aktivitäten während der Übertragung data-at-rest und des Benutzerverhaltens.	ec2- instance-no-public-ip	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon Elastic Compute Cloud (Amazon EC2) - Instances nicht öffentlich zugänglich sind. EC2 Amazon-Instances können vertrauliche Informationen enthalten, und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
Ihre Daten-2	Erfahren Sie, was in Ihrem Netzwerk passiert. Verwalten Sie Netzwerk- und Perimeterkomponenten, Host- und Gerätekomponenten sowie Aktivitäten während der Übertragung data-at-rest und des Benutzerverhaltens.	elasticsearch-in-vpc-only	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass sich Amazon OpenSearch OpenSearch Service (Service) - Domains innerhalb einer Amazon Virtual Private Cloud (Amazon VPC) befinden. Eine OpenSearch Service-Domain innerhalb einer Amazon VPC ermöglicht die sichere Kommunikation zwischen OpenSearch Service und anderen Services innerhalb der Amazon VPC, ohne dass ein Internet-Gateway, ein NAT-Gerät oder eine VPN-Verbindung erforderlich ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
Ihre Daten-2	Erfahren Sie, was in Ihrem Netzwerk passiert. Verwalten Sie Netzwerk- und Perimeterkomponenten, Host- und Gerätekomponenten sowie Aktivitäten während der Übertragung data-at-rest und des Benutzerverhaltens.	emr-master-no-public-ip	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon EMR-Cluster-Masterknoten nicht öffentlich zugänglich sind. Amazon-EMR-Cluster-Hauptknoten können vertrauliche Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
Ihre Daten-2	Erfahren Sie, was in Ihrem Netzwerk passiert. Verwalten Sie Netzwerk- und Perimeterkomponenten, Host- und Gerätekomponenten sowie Aktivitäten während der Übertragung data-at-rest und des Benutzerverhaltens.	ec2- instances-in-vpc	Stellen Sie Amazon Elastic Compute Cloud (Amazon EC2) -Instances innerhalb einer Amazon Virtual Private Cloud (Amazon VPC) bereit, um eine sichere Kommunikation zwischen einer Instance und anderen Services innerhalb der Amazon VPC zu ermöglichen, ohne dass ein Internet-Gateway, ein NAT-Gerät oder eine VPN-Verbindung erforderlich ist. Der gesamte Datenverkehr bleibt sicher in der AWS Cloud. Domains, die sich innerhalb einer VPC befinden, verfügen aufgrund ihrer logischen Isolierung im Vergleich zu Domains mit öffentlichen Endpunkten über eine zusätzliche Sicherheitsebene. Weisen Sie EC2

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			Amazon-Instances einer Amazon-VPC zu, um den Zugriff ordnungsgemäß zu verwalten.
Ihre Daten-2	Erfahren Sie, was in Ihrem Netzwerk passiert. Verwalten Sie Netzwerk- und Perimeter komponenten, Host- und Gerätekom ponenten sowie Aktivitäten während der Übertragung data-at-rest und Benutzerv erhalten.	lambda-function-pu blic-access-verboten	Verwalten Sie den Zugriff auf Ressource n in der AWS Cloud, indem Sie sicherste llen, dass AWS Lambda-Funktionen nicht öffentlich zugänglich sind. Der öffentliche Zugriff kann möglicherweise die Verfügbarkeit von Ressourcen beeinträc htigen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
Ihre Daten-2	Erfahren Sie, was in Ihrem Netzwerk passiert. Verwalten Sie Netzwerk- und Perimeterkomponenten, Host- und Gerätekomponenten sowie Aktivitäten während der Übertragung data-at-rest und des Benutzerverhaltens.	lambda-inside-vpc	Stellen Sie AWS Lambda-Funktionen in einer Amazon Virtual Private Cloud (Amazon VPC) bereit, um eine sichere Kommunikation zwischen einer Funktion und anderen Diensten innerhalb der Amazon VPC zu gewährleisten. Bei dieser Konfiguration sind kein Internet-Gateway, kein NAT-Gerät und keine VPN-Verbindung erforderlich. Der gesamte Datenverkehr bleibt sicher in der Cloud. AWS Domains, die sich innerhalb einer VPC befinden, verfügen aufgrund ihrer logischen Isolierung im Vergleich zu Domains mit öffentlichen Endpunkten über eine zusätzliche Sicherheitsebene. Um den Zugriff ordnungsgemäß zu verwalten,

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			sollten AWS Lambda-Funktionen einer VPC zugewiesen werden.
Ihre Daten-2	Erfahren Sie, was in Ihrem Netzwerk passiert. Verwalten Sie Netzwerk- und Perimeterkomponenten, Host- und Gerätekomponenten sowie Aktivitäten während der Übertragung data-at-rest und des Benutzerverhaltens.	rds-instance-public-access-überprüfen	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Relational Database Service (Amazon RDS) -Instances nicht öffentlich sind. Amazon-RDS-Datenbank-Instances können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
Ihre Daten-2	Erfahren Sie, was in Ihrem Netzwerk passiert. Verwalten Sie Netzwerk- und Perimeterkomponenten, Host- und Gerätekomponenten sowie Aktivitäten während der Übertragung data-at-rest und des Benutzerverhaltens.	rds-snapshots-public-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Relational Database Service (Amazon RDS) -Instances nicht öffentlich sind. Amazon-RDS-Datenbank-Instances können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
Ihre Daten-2	Erfahren Sie, was in Ihrem Netzwerk passiert. Verwalten Sie Netzwerk- und Perimeterkomponenten, Host- und Gerätekomponenten sowie Aktivitäten während der Übertragung data-at-rest und des Benutzerverhaltens.	redshift-cluster-public-access-überprüfen	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Redshift Redshift-Cluster nicht öffentlich sind. Amazon-Redshift-Cluster können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
Ihre Daten-2	Erfahren Sie, was in Ihrem Netzwerk passiert. Verwalten Sie Netzwerk- und Perimeterkomponenten, Host- und Gerätekomponenten sowie Aktivitäten während der Übertragung data-at-rest und des Benutzerverhaltens.	restricted-common-ports	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass gemeinsame Ports für Amazon Elastic Compute Cloud (Amazon EC2) -Sicherheitsgruppen eingeschränkt sind. Wenn der Zugriff auf Ports nicht auf vertrauenswürdige Quellen beschränkt wird, kann dies zu Angriffen auf die Verfügbarkeit, Integrität und Vertraulichkeit von Systemen führen. Mit dieser Regel können Sie optional die Parameter blockedPort1–blockedPort5 festlegen (Standardkonfigurationen: 20, 21, 3389, 3306, 4333). Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
Ihre Daten-2	Erfahren Sie, was in Ihrem Netzwerk passiert. Verwalten Sie Netzwerk- und Perimeterkomponenten, Host- und Gerätekomponenten sowie Aktivitäten während der Übertragung data-at-rest und des Benutzerverhaltens.	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) Security Groups können bei der Verwaltung des Netzwerkzugriffs helfen, indem sie eine statusbehaftete Filterung von eingehendem und ausgehendem Netzwerkverkehr zu Ressourcen bereitstellen. AWS Wenn Sie eingehenden (oder entfernten) Datenverkehr von 0.0.0.0/0 bis Port 22 auf Ihren Ressourcen nicht zulassen, können Sie den Remote-Zugriff einschränken.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
Ihre Daten-2	Erfahren Sie, was in Ihrem Netzwerk passiert. Verwalten Sie Netzwerk- und Perimeterkomponenten, Host- und Gerätekomponenten sowie Aktivitäten während der Übertragung data-at-rest und des Benutzerverhaltens.	iam-no-inline-policy-überprüfen	Stellen Sie sicher, dass ein Benutzer, eine IAM-Rolle oder eine IAM-Gruppe (AWS Identity and Access Management) nicht über eine Inline-Richtlinie zur Zugriffskontrolle auf Systeme und Ressourcen verfügt. AWS empfiehlt, verwaltete Richtlinien anstelle von Inline-Richtlinien zu verwenden. Verwaltete Richtlinien ermöglichen Wiederverwendbarkeit, Versionsverwaltung, Rollback und Delegierung der Berechtigungsverwaltung.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
Ihre Daten-2	Erfahren Sie, was in Ihrem Netzwerk passiert. Verwalten Sie Netzwerk- und Perimeterkomponenten, Host- und Gerätekomponenten sowie Aktivitäten während der Übertragung data-at-rest und des Benutzerverhaltens.	s3- -Block-periodisch account-level-public-access	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Simple Storage Service (Amazon S3) -Buckets nicht öffentlich zugänglich sind. Diese Regel trägt dazu bei, sensible Daten vor unbefugten Remote-Benutzern zu schützen, indem sie den öffentlichen Zugriff verhindert. Mit dieser Regel können Sie optional die Parameter ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) und restrictPublicBuckets Parameter (Config Default: True) festlegen. Die tatsächlichen Werte müssen den Richtlini

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			en Ihrer Organisation entsprechen.
Ihre Daten-2	Erfahren Sie, was in Ihrem Netzwerk passiert. Verwalten Sie Netzwerk- und Perimeterkomponenten, Host- und Gerätekomponenten data-at-rest sowie Aktivitäten während der Übertragung und Benutzerverhalten.	s-3 bucket-public-read-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie nur autorisierten Benutzern, Prozessen und Geräten Zugriff auf Amazon Simple Storage Service (Amazon S3) - Buckets gewähren. Die Verwaltung des Zugriffs sollte mit der Klassifizierung der Daten übereinstimmen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
Ihre Daten-2	Erfahren Sie, was in Ihrem Netzwerk passiert. Verwalten Sie Netzwerk- und Perimeterkomponenten, Host- und Gerätekomponenten sowie Aktivitäten während der Übertragung data-at-rest und des Benutzerverhaltens.	s-3 bucket-public-write-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie nur autorisierten Benutzern, Prozessen und Geräten Zugriff auf Amazon Simple Storage Service (Amazon S3) - Buckets gewähren. Die Verwaltung des Zugriffs sollte mit der Klassifizierung der Daten übereinstimmen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
Ihre Daten-2	Erfahren Sie, was in Ihrem Netzwerk passiert. Verwalten Sie Netzwerk- und Perimeterkomponenten, Host- und Gerätekomponenten sowie Aktivitäten während der Übertragung data-at-rest und des Benutzerverhaltens.	s-3 bucket-policy-grantee-check	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie s3_bucket_policy_grantee_check aktivieren. Diese Regel prüft, ob der vom Amazon S3 S3-Bucket gewährte Zugriff durch die von Ihnen bereitgestellten AWS Principals, Verbundbenutzer, Service Principals, IP-Adressen oder Amazon Virtual Private Cloud (Amazon VPC) IDs eingeschränkt ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
Ihre Daten-2	Erfahren Sie, was in Ihrem Netzwerk passiert. Verwalten Sie Netzwerk- und Perimeterkomponenten, Host- und Gerätekomponenten sowie Aktivitäten während der Übertragung und des data-at-rest Benutzerverhaltens.	sagemaker-notebook-no-direct-Internetzugang	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass SageMaker Amazon-Notebooks keinen direkten Internetzugang zulassen. Indem Sie direkten Internetzugang blockieren, vermeiden Sie, dass unbefugte Benutzer auf sensible Daten zugreifen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
Ihre Daten-2	Erfahren Sie, was in Ihrem Netzwerk passiert. Verwalten Sie Netzwerk- und Perimeterkomponenten, Host- und Gerätekomponenten sowie Aktivitäten während der Übertragung data-at-rest und des Benutzerverhaltens.	subnet-auto-assign-public-ip-deaktiviert	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon Virtual Private Cloud (VPC) -Subnetzen nicht automatisch eine öffentliche IP-Adresse zugewiesen wird. Amazon Elastic Compute Cloud (EC2) -Instances, die in Subnetzen gestartet werden, in denen dieses Attribut aktiviert ist, haben ihrer primären Netzwerkschnittstelle eine öffentliche IP-Adresse zugewiesen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
Ihre Daten-2	Erfahren Sie, was in Ihrem Netzwerk passiert. Verwalten Sie Netzwerk- und Perimeterkomponenten, Host- und Gerätekomponenten sowie Aktivitäten während der Übertragung data-at-rest und des Benutzerverhaltens.	vpc-default-security-group-geschlossen	Sicherheitsgruppen von Amazon Elastic Compute Cloud (Amazon EC2) können bei der Verwaltung des Netzwerkzugriffs helfen, indem sie eine statusbehaftete Filterung des ein- und ausgehenden Netzwerkverkehrs zu Ressourcen bereitstellen. AWS Die Beschränkung des gesamten Datenverkehrs auf die Standardsicherheitsgruppe hilft dabei, den Fernzugriff auf Ihre Ressourcen einzuschränken. AWS

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
Ihre Daten-2	Erfahren Sie, was in Ihrem Netzwerk passiert. Verwalten Sie Netzwerk- und Perimeterkomponenten, Host- und Gerätekomponenten sowie Aktivitäten während der Übertragung data-at-rest und des Benutzerverhaltens.	vpc-sg-open-only-to-authorized-ports	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass gemeinsame Ports für Amazon Elastic Compute Cloud (Amazon EC2) -Sicherheitsgruppen eingeschränkt sind. Wenn der Zugriff auf Ports nicht auf vertrauenswürdige Quellen beschränkt wird, kann dies zu Angriffen auf die Verfügbarkeit, Integrität und Vertraulichkeit von Systemen führen. Durch die Beschränkung des Zugriffs auf Ressourcen innerhalb einer Sicherheitsgruppe aus dem Internet (0.0.0.0/0) kann der Remote-Zugriff auf interne Systeme gesteuert werden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
Ihre Daten-2	Erfahren Sie, was in Ihrem Netzwerk passiert. Verwalten Sie Netzwerk- und Perimeterkomponenten, Host- und Gerätekomponenten sowie Aktivitäten während der Übertragung data-at-rest und des Benutzerverhaltens.	autoscaling-launch-config-public-ip-deaktiviert	Wenn Sie Ihre Netzwerkschnittstellen mit einer öffentlichen IP-Adresse konfigurieren, sind die diesen Netzwerkschnittstellen zugehörigen Ressourcen über das Internet erreichbar. EC2 Ressourcen sollten nicht öffentlich zugänglich sein, da dies einen unbeabsichtigten Zugriff auf Ihre Anwendungen oder Server ermöglichen kann.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
Ihre Daten-3	Schutz des Domain Name System.	alb-waf-enabled	Stellen Sie sicher, dass AWS WAF auf Elastic Load Balancers (ELB) aktiviert ist, um Webanwendungen zu schützen. Eine WAF trägt zum Schutz Ihrer Webanwend ungen oder APIs vor gängigen Web-Explo its bei. Diese Web-Exploits können sich auf die Verfügbar keit auswirken, die Sicherheit gefährden oder übermäßige Ressourcen in Ihrer Umgebung verbrauch en.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
Ihre Daten-4	Richten Sie regelmäßige automatisierte Backups und Redundanzen wichtiger Systeme ein.	db-instance-backup-enabled	Die Sicherungsfunktion von Amazon RDS erstellt Sicherungen Ihrer Datenbanken und Transaktionsprotokolle. Amazon RDS erstellt einen Snapshot für das Speichervolume Ihrer DB-Instance, sodass die gesamte DB-Instance gesichert wird. Sie können im System spezifische Aufbewahrungsfristen festlegen, um Ihre Ausfallsicherheitsanforderungen zu erfüllen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
Ihre Daten-4	Richten Sie regelmäßige automatisierte Backups und Redundanzen wichtiger Systeme ein.	elb-deletion-protection-enabled	Diese Regel sorgt dafür, dass der Löschschutz für Elastic Load Balancing aktiviert ist. Verwenden Sie diese Funktion, um zu verhindern, dass Ihr Load Balancer versehentlich oder böswillig gelöscht wird, was zum Verlust der Verfügbarkeit Ihrer Anwendungen führen kann.
Ihre Daten-4	Richten Sie regelmäßige automatisierte Backups und Redundanzen wichtiger Systeme ein.	rds-instance-deletion-protection-aktiviert	Stellen Sie sicher, dass Amazon Relational Database Service (Amazon RDS)-Instances den Löschschutz aktiviert haben. Verwenden Sie den Löschschutz, um zu verhindern, dass Ihre Amazon-RDS-Instances versehentlich oder böswillig gelöscht werden, was zum Verlust der Verfügbarkeit Ihrer Anwendungen führen kann.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
Ihre Daten-4	Richten Sie regelmäßige automatisierte Backups und Redundanzen wichtiger Systeme ein.	dynamodb-in-backup-plan	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon DynamoDB-Tabellen Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
Ihre Daten-4	Richten Sie regelmäßige automatisierte Backups und Redundanzen wichtiger Systeme ein.	dynamodb-pitr-enabled	Aktivieren Sie diese Regel, um zu überprüfen, ob die Informationen gesichert wurden. Es verwaltet auch die Backups, indem es sicherstellt, dass die point-in-time Wiederherstellung in Amazon DynamoDB aktiviert ist. Bei der Wiederherstellung werden fortlaufende Backups Ihrer Tabelle für die letzten 35 Tage gespeichert.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
Ihre Daten-4	Richten Sie regelmäßige automatisierte Backups und Redundanzen wichtiger Systeme ein.	ebs-in-backup-plan	Stellen Sie zur Unterstützung der Datensicherungsprozesse sicher, dass Ihre Amazon Elastic Block Store (Amazon EBS) -Volumes Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
Ihre Daten-4	Richten Sie regelmäßige automatisierte Backups und Redundanzen wichtiger Systeme ein.	ebs-optimized-instance	Eine optimierte Instance im Amazon Elastic Block Store (Amazon EBS) bietet zusätzliche, dedizierte Kapazität für Amazon-EBS-I/O-Vorgänge. Diese Optimierung bietet die beste Leistung für Ihr EBS-Volume, indem Konflikte zwischen Amazon-EBS-I/O und anderem Datenverkehr von Ihrer Instance minimiert werden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
Ihre Daten-4	Richten Sie regelmäßige automatisierte Backups und Redundanzen wichtiger Systeme ein.	efs-in-backup-plan	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon Elastic File System (Amazon EFS) -Dateisysteme Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
Ihre Daten-4	Richten Sie regelmäßige automatisierte Backups und Redundanzen wichtiger Systeme ein.	elasticache-redis-cluster-automatic-Backup-Check	Wenn automatische Backups aktiviert sind, ElastiCache erstellt Amazon täglich ein Backup des Clusters. Die Sicherung kann für eine von Ihrer Organisation festgelegte Anzahl von Tagen aufbewahrt werden. Automatische Backups schützen vor Datenverlust. Bei einem Ausfall können Sie einen neuen Cluster erstellen, der Ihre Daten aus dem aktuellen Backup wiederherstellt.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
Ihre Daten-4	Richten Sie regelmäßige automatisierte Backups und Redundanzen wichtiger Systeme ein.	rds-in-backup-plan	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon Relational Database Service (Amazon RDS) -Instances Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
Ihre Daten-4	Richten Sie regelmäßige automatisierte Backups und Redundanzen wichtiger Systeme ein.	redshift-backup-enabled	Stellen Sie zur Unterstützung der Datensicherungsprozesse sicher, dass Ihre Amazon-Redshift-Cluster über automatisierte Snapshots verfügen. Wenn automatisierte Snapshots für einen Cluster aktiviert sind, erstellt Redshift in regelmäßigen Abständen Snapshots dieses Clusters. Standardmäßig erstellt Redshift alle acht Stunden oder alle 5 GB einen Snapshot für jeden Knoten mit Datenänderungen oder je nachdem, was zuerst eintritt.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
Ihre Daten-4	Richten Sie regelmäßige automatisierte Backups und Redundanzen wichtiger Systeme ein.	s3- bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) unterstützt die Aufrechterhaltung einer angemessenen Kapazität und Verfügbarkeit. CRR ermöglicht das automatische, asynchrone Kopieren von Objekten in Amazon-S3-Buckets, um die Datenverfügbarkeit sicherzustellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
Ihre Daten-4	Richten Sie regelmäßige automatisierte Backups und Redundanzen wichtiger Systeme ein.	s-3 bucket-versioning-enabled	Die Versionsverwaltung von Amazon Simple Storage Service (Amazon S3)-Buckets hilft dabei, mehrere Varianten eines Objekts im selben Amazon-S3-Bucket zu speichern. Verwenden Sie die Versionsverwaltung, um sämtliche Versionen aller Objekte in Ihrem Amazon-S3-Bucket zu speichern, abzurufen oder wiederherzustellen. Mit der Versionsverwaltung können Sie Versionen sowohl nach unbeabsichtigten Benutzeraktionen als auch nach Anwendungsfehlern problemlos wiederherstellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
Ihre Daten-4	Richten Sie regelmäßige automatisierte Backups und Redundanzen wichtiger Systeme ein.	aurora-resources-protected-by-Backup-Plan	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon Aurora Aurora-Ressourcen Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
Ihre Daten-4	Richten Sie regelmäßige automatisierte Backups und Redundanzen wichtiger Systeme ein.	backup-plan-min-frequency-and-min-retention-check	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihr AWS Backup-Plan auf eine Mindestfrequenz und Aufbewahrung festgelegt ist. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen. Mit dieser Regel können Sie die Parameter requiredFrequencyValue (Config default: 1), requiredRetentionDays (Config default: 35) und requiredFrequencyUnit

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			(Config default: days) festlegen. Der tatsächliche Wert muss den Anforderungen Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
Ihre Daten-4	Richten Sie regelmäßige automatisierte Backups und Redundanzen wichtiger Systeme ein.	backup-recovery-point-minimum-Aufbewahrungsprüfung	Um bei Datensicherungsprozessen zu helfen, stellen Sie sicher, dass für Ihre AWS Backup-Wiederherstellungspunkte eine Mindestaufbewahrungsdauer festgelegt ist. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen. Mit dieser Regel können Sie den Parameter requiredRetentionDays (Config Default: 35) festlegen. Der tatsächliche Wert muss den Anforderu

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			ngen Ihrer Organisation entsprechen.
Ihre Daten-4	Richten Sie regelmäßige automatisierte Backups und Redundanzen wichtiger Systeme ein.	ec2--Plan resources-protected-by-backup	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon Elastic Compute Cloud (Amazon EC2) -Ressourcen Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
Ihre Daten-4	Richten Sie regelmäßige automatisierte Backups und Redundanzen wichtiger Systeme ein.	fsx-resources-protected-by-Backup-Plan	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre FSx Amazon-Dateisysteme Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
Ihre Daten-5	Nutzen Sie Schutzmaßnahmen für Backups, einschließlich physischer Sicherheit, Verschlüsselung und Offline-Kopien.	backup-recovery-point-encrypted	Stellen Sie sicher, dass die Verschlüsselung für Ihre AWS Backup-Wiederherstellungspunkte aktiviert ist. Da sensible Daten auch im Ruhezustand vorhanden sein können, sollten Sie die Verschlüsselung im Ruhezustand aktivieren, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
Ihre Daten-5	Nutzen Sie Schutzmaßnahmen für Backups, einschließlich physischer Sicherheit, Verschlüsselung und Offline-Kopien.	backup-recovery-point-manual-Löschen-deaktiviert	Stellen Sie sicher, dass Ihren AWS Backup-Wiederherstellungspunkten eine ressourcenbasierte Richtlinie zugeordnet ist, die das Löschen von Wiederherstellungspunkten verhindert. Die Verwendung einer ressourcenbasierten Richtlinie zur Verhinderung des Löschens von Wiederherstellungspunkten kann dazu beitragen, ein versehentliches oder absichtliches Löschen zu unterbinden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
Ihre Reaktion auf Krisen-2	Leiten Sie die Entwicklung einer internen Berichter stattungsstruktur zur Erkennung, Mitteilung und Eindämmung von Angriffen.	guardduty-enabled-centralized	Amazon GuardDuty kann mithilfe von Threat Intellige nce Feeds helfen, potenzielle Cybersich erheitsereignisse zu überwachen und zu erkennen. Dazu gehören Listen mit bösartigen IPs und maschinel len Lernmethoden zur Identifizierung unerwarteter, nicht autorisierter und bösartiger Aktivitäten in Ihrer AWS Cloud-Umgebung.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
Ihre Reaktion auf Krisen-2	Leiten Sie die Entwicklung einer internen Berichter stattungsstruktur zur Erkennung, Mitteilung und Eindämmung von Angriffen.	securityhub-enabled	AWS Security Hub hilft bei der Überwachung von unbefugtem Personal, Verbindun gen, Geräten und Software. AWS Security Hub aggregiert, organisie rt und priorisie rt die Sicherhei tswarnungen oder Ergebnisse mehrerer Dienste. AWS Einige dieser Dienste sind Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer und AWS Firewall Manager sowie AWS Partnerlösungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
Starten: Was Sie zuerst tun sollten-1	Verwenden Sie eine Backup-Lösung, die automatisch und kontinuierlich kritische Daten und Systemkon figurationen sichert.	db-instance-backup-enabled	Die Sicherung sfunktion von Amazon RDS erstellt Sicherung en Ihrer Datenbank en und Transakti onsprotokolle. Amazon RDS erstellt einen Snapshot für das Speichervolume Ihrer DB-Instance, sodass die gesamte DB-Instance gesichert wird. Sie können im System spezifische Aufbewahrungsfrist en festlegen, um Ihre Ausfallsicherheits anforderungen zu erfüllen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
Starten: Was Sie zuerst tun sollten-1	Verwenden Sie eine Backup-Lösung, die automatisch und kontinuierlich kritische Daten und Systemkon figurationen sichert.	dynamodb-in-backup-plan	Um Sie bei Datensich erungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon DynamoDB-Tabellen Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwaltet er Backup-Service mit einer richtlini enbasierten Backup-Lösung. Diese Lösung vereinfac ht Ihr Sicherung smanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforde rungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
Starten: Was Sie zuerst tun sollten-1	Verwenden Sie eine Backup-Lösung, die automatisch und kontinuierlich kritische Daten und Systemkonfigurationen sichert.	dynamodb-pitr-enabled	Aktivieren Sie diese Regel, um zu überprüfen, ob die Informationen gesichert wurden. Es verwaltet auch die Backups, indem es sicherstellt, dass die point-in-time Wiederherstellung in Amazon DynamoDB aktiviert ist. Bei der Wiederherstellung werden fortlaufende Backups Ihrer Tabelle für die letzten 35 Tage gespeichert.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
Starten: Was Sie zuerst tun sollten-1	Verwenden Sie eine Backup-Lösung, die automatisch und kontinuierlich kritische Daten und Systemkon figurationen sichert.	ebs-in-backup-plan	Stellen Sie zur Unterstützung der Datensicherungspro zesse sicher, dass Ihre Amazon Elastic Block Store (Amazon EBS) -Volumes Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwaltet er Backup-Service mit einer richtlini enbasierten Backup-Lösung. Diese Lösung vereinfac ht Ihr Sicherung smanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforde rungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
Starten: Was Sie zuerst tun sollten-1	Verwenden Sie eine Backup-Lösung, die automatisch und kontinuierlich kritische Daten und Systemkonfigurationen sichert.	ebs-optimized-instance	Eine optimierte Instance im Amazon Elastic Block Store (Amazon EBS) bietet zusätzliche, dedizierte Kapazität für Amazon-EBS-I/O-Vorgänge. Diese Optimierung bietet die beste Leistung für Ihr EBS-Volume, indem Konflikte zwischen Amazon-EBS-I/O und anderem Datenverkehr von Ihrer Instance minimiert werden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
Starten: Was Sie zuerst tun sollten-1	Verwenden Sie eine Backup-Lösung, die automatisch und kontinuierlich kritische Daten und Systemkon figurationen sichert.	efs-in-backup-plan	Um Sie bei Datensich erungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon Elastic File System (Amazon EFS) -Dateisysteme Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwaltet er Backup-Service mit einer richtlini enbasierten Backup-Lösung. Diese Lösung vereinfac ht Ihr Sicherung smanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforde rungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
Starten: Was Sie zuerst tun sollten-1	Verwenden Sie eine Backup-Lösung, die automatisch und kontinuierlich kritische Daten und Systemkon figurationen sichert.	elasticache-redis-cluster-automatic-Backup-Check	Wenn automatische Backups aktiviert sind, ElastiCache erstellt Amazon täglich ein Backup des Clusters. Die Sicherung kann für eine von Ihrer Organisation festgelegte Anzahl von Tagen aufbewahrt werden. Automatische Backups schützen vor Datenverlust. Bei einem Ausfall können Sie einen neuen Cluster erstellen, der Ihre Daten aus dem aktuellen Backup wiederherstellt.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
Starten: Was Sie zuerst tun sollten-1	Verwenden Sie eine Backup-Lösung, die automatisch und kontinuierlich kritische Daten und Systemkon figurationen sichert.	rds-in-backup-plan	Um Sie bei Datensich erungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon Relational Database Service (Amazon RDS) -Instance s Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwaltet er Backup-Service mit einer richtlini enbasierten Backup-Lösung. Diese Lösung vereinfac ht Ihr Sicherung smanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforde rungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
Starten: Was Sie zuerst tun sollten-1	Verwenden Sie eine Backup-Lösung, die automatisch und kontinuierlich kritische Daten und Systemkonfigurationen sichert.	redshift-backup-enabled	Stellen Sie zur Unterstützung der Datensicherungsprozesse sicher, dass Ihre Amazon-Redshift-Cluster über automatisierte Snapshots verfügen. Wenn automatisierte Snapshots für einen Cluster aktiviert sind, erstellt Redshift in regelmäßigen Abständen Snapshots dieses Clusters. Standardmäßig erstellt Redshift alle acht Stunden oder alle 5 GB einen Snapshot für jeden Knoten mit Datenänderungen oder je nachdem, was zuerst eintritt.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
Starten: Was Sie zuerst tun sollten-1	Verwenden Sie eine Backup-Lösung, die automatisch und kontinuierlich kritische Daten und Systemkon figurationen sichert.	s3- bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) unterstützt die Aufrechterhaltung einer angemesse nen Kapazität und Verfügbarkeit. CRR ermöglicht das automatische, asynchrone Kopieren von Objekten in Amazon-S3-Buckets, um die Datenverf ügbarkeit sicherzus tellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
Starten: Was Sie zuerst tun sollten-1	Verwenden Sie eine Backup-Lösung, die automatisch und kontinuierlich kritische Daten und Systemkonfigurationen sichert.	s-3 bucket-versioning-enabled	Die Versionsverwaltung von Amazon Simple Storage Service (Amazon S3)-Buckets hilft dabei, mehrere Varianten eines Objekts im selben Amazon-S3-Bucket zu speichern. Verwenden Sie die Versionsverwaltung, um sämtliche Versionen aller Objekte in Ihrem Amazon-S3-Bucket zu speichern, abzurufen oder wiederherzustellen. Mit der Versionsverwaltung können Sie Versionen sowohl nach unbeabsichtigten Benutzeraktionen als auch nach Anwendungsfehlern problemlos wiederherstellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
Starten: Was Sie zuerst tun sollten-1	Verwenden Sie eine Backup-Lösung, die automatisch und kontinuierlich kritische Daten und Systemkonfigurationen sichert.	aurora-resources-protected-by-Backup-Plan	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon Aurora Aurora-Ressourcen Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
Starten: Was Sie zuerst tun sollten-1	Verwenden Sie eine Backup-Lösung, die automatisch und kontinuierlich kritische Daten und Systemkonfigurationen sichert.	backup-plan-min-frequency-and-min-retention-check	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihr AWS Backup-Plan auf eine Mindestfrequenz und Aufbewahrung festgelegt ist. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen. Mit dieser Regel können Sie die Parameter requiredFrequencyValue (Config default: 1), requiredRetentionDays (Config default: 35) und requiredFrequencyUnit

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			(Config default: days) festlegen. Der tatsächliche Wert muss den Anforderungen Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
Starten: Was Sie zuerst tun sollten-1	Verwenden Sie eine Backup-Lösung, die automatisch und kontinuierlich kritische Daten und Systemkonfigurationen sichert.	backup-recovery-point-minimum-Aufbewahrungsprüfung	Um bei Datensicherungsprozessen zu helfen, stellen Sie sicher, dass für Ihre AWS Backup-Wiederherstellungspunkte eine Mindestaufbewahrungsdauer festgelegt ist. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen. Mit dieser Regel können Sie den Parameter requiredRetentionDays (Config Default: 35) festlegen. Der tatsächliche Wert muss den Anforderu

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			ngen Ihrer Organisat ion entsprechen.
Starten: Was Sie zuerst tun sollten-1	Verwenden Sie eine Backup-Lösung, die automatisch und kontinuierlich kritische Daten und Systemkon figurationen sichert.	dynamodb-resources-protected-by-Backup-Plan	Um Sie bei Datensich erungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon DynamoDB DynamoDB-Ressourcen Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwaltet er Backup-Service mit einer richtlini enbasierten Backup-Lösung. Diese Lösung vereinfac ht Ihr Sicherung smanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforde rungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
Starten: Was Sie zuerst tun sollten-1	Verwenden Sie eine Backup-Lösung, die automatisch und kontinuierlich kritische Daten und Systemkon figurationen sichert.	ec2--Plan resources-protected-by-backup	Um Sie bei Datensich erungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon Elastic Compute Cloud (Amazon EC2) -Ressourc en Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwaltet er Backup-Service mit einer richtlini enbasierten Backup-Lösung. Diese Lösung vereinfac ht Ihr Sicherung smanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforde rungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
Starten: Was Sie zuerst tun sollten-1	Verwenden Sie eine Backup-Lösung, die automatisch und kontinuierlich kritische Daten und Systemkonfigurationen sichert.	fsx-resources-protected-by-Backup-Plan	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre FSx Amazon-Dateisysteme Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
Starten: Was Sie zuerst tun sollten-2	Verlangen Sie, wann immer möglich, eine Multi-Faktor-Authentifizierung (MFA) für den Zugriff auf Ihre Systeme. MFA sollte von allen Benutzern verlangt werden, aber beginnen Sie bei privilegierten Benutzern sowie Benutzern mit Administratorrechten und Remote-Zugriff.	iam-user-mfa-enabled	Aktivieren Sie diese Regel, um den Zugriff auf Ressourcen in der AWS Cloud einzuschränken. Diese Regel sorgt dafür, dass die Multi-Faktor-Authentifizierung (MFA) für alle Benutzer aktiviert ist. MFA sorgt für eine weitere Schutzebene zusätzlich zu den Anmeldeinformationen. Reduzieren Sie Fälle von kompromittierten Konten, indem Sie MFA für Benutzer vorschreiben.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
Starten: Was Sie zuerst tun sollten-2	Verlangen Sie, wann immer möglich, eine Multi-Faktor-Authentifizierung (MFA) für den Zugriff auf Ihre Systeme. MFA sollte von allen Benutzern verlangt werden, aber beginnen Sie bei privilegierten Benutzern sowie Benutzern mit Administratorrechten und Remote-Zugriff.	mfa-enabled-for-iam-Konsolenzugriff	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass MFA für alle AWS Identity and Access Management (IAM) -Benutzer aktiviert ist, die über ein Konsolenkennwort verfügen. MFA sorgt für eine weitere Schutzebene zusätzlich zu den Anmeldeinformationen. Indem Sie MFA für Benutzer vorschreiben, können Sie Fälle kompromittierter Konten reduzieren und verhindern, dass unbefugte Benutzer auf vertrauliche Daten zugreifen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
Starten: Was Sie zuerst tun sollten-2	Verlangen Sie, wann immer möglich, eine Multi-Faktor-Authentifizierung (MFA) für den Zugriff auf Ihre Systeme. MFA sollte von allen Benutzern verlangt werden, aber beginnen Sie bei privilegierten Benutzern sowie Benutzern mit Administratorrechten und Remote-Zugriff.	root-account-hardware-mfa-aktiviert	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Hardware-MFA für den Root-Benutzer aktiviert ist. Der Stammbenutzer ist der AWS-Konto-Benutzer mit den meisten Berechtigungen. MFA sorgt für eine weitere Schutzebene zusätzlich zu den Anmeldeinformationen. Indem Sie MFA für den Root-Benutzer vorschreiben, können Sie die Anzahl AWS-Konten kompromittierter Benutzer reduzieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
Starten: Was Sie zuerst tun sollten-2	Verlangen Sie, wann immer möglich, eine Multi-Faktor-Authentifizierung (MFA) für den Zugriff auf Ihre Systeme. MFA sollte von allen Benutzern verlangt werden, aber beginnen Sie bei privilegierten Benutzern sowie Benutzern mit Administratorrechten und Remote-Zugriff.	root-account-mfa-enabled	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass MFA für den Root-Benutzer aktiviert ist. Der Stammbenutzer ist der AWS-Konto-Benutzer mit den meisten Berechtigungen. MFA sorgt für eine weitere Schutzebene zusätzlich zu den Anmeldeinformationen. Indem Sie MFA für den Root-Benutzer vorschreiben, können Sie die Anzahl AWS-Konten kompromittierter Benutzer reduzieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
Starten: Was Sie zuerst tun sollten-3	Aktivieren Sie automatische Updates, wann immer dies möglich ist. Ersetzen Sie nicht unterstützte Betriebssysteme, Anwendungen und Hardware. Testen und implementieren Sie Patches schnell.	ec2-check managedinstance-patch-compliance-status	Aktivieren Sie diese Regel, um bei der Identifizierung und Dokumentation von Sicherheitslücken in Amazon Elastic Compute Cloud (Amazon EC2) zu helfen. Die Regel prüft, ob die EC2 Amazon-Instance die Patch-Konformität im AWS Systems Manager gemäß den Richtlinien und Verfahren Ihrer Organisation einhält.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
Starten: Was Sie zuerst tun sollten-3	Aktivieren Sie automatische Updates, wann immer dies möglich ist. Ersetzen Sie nicht unterstützte Betriebssysteme, Anwendungen und Hardware. Testen und implementieren Sie Patches schnell.	rds-automatic-minor-version-Upgrade aktiviert	Aktivieren Sie automatische Unterversions-Upgrades auf Ihren Amazon-Relational-Database-Service (RDS)-Instances, um sicherzustellen, dass die aktuellen Updates für Unterversionen des Relational Database Management System (RDBMS) installiert sind, die Sicherheitspatches und Bugfixes enthalten können.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
Starten: Was Sie zuerst tun sollten-3	Aktivieren Sie automatische Updates, wann immer dies möglich ist. Ersetzen Sie nicht unterstützte Betriebssysteme, Anwendungen und Hardware. Testen und implementieren Sie Patches schnell.	elastic-beanstalk-managed-updates-aktiviert	Durch die Aktivierung verwalteter Plattform updates für eine Amazon-Elastic-Beanstalk-Umgebung wird sichergestellt, dass die aktuellen verfügbaren Plattform-Fixes, -Updates und -Features für die Umgebung installiert sind. Eine bewährte Methode zur Sicherung von Systemen besteht darin, stets die aktuellen Patches zu installieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
Starten: Was Sie zuerst tun sollten-3	Aktivieren Sie automatische Updates, wann immer dies möglich ist. Ersetzen Sie nicht unterstützte Betriebssysteme, Anwendungen und Hardware. Testen und implementieren Sie Patches schnell.	redshift-cluster-maintenancesettings-check	Diese Regel stellt sicher, dass Amazon-Redshift-Cluster die bevorzugten Einstellungen für Ihre Organisation haben. Insbesondere sorgt sie dafür, dass Cluster bevorzugte Wartungsfenster und automatisierte Aufbewahrungsfristen für Snapshots für die Datenbank haben. Für diese Regel müssen Sie die allowVersionUpgrade festlegen. Der Standardwert ist „true“. Außerdem können Sie optional den Zeitraum preferredMaintenanceWindow (der Standardwert ist sa: 16:00 -sa: 16:30) und den automated SnapshotRetention Zeitraum (der Standardwert ist 1) festlegen. Die tatsächlichen Werte müssen den Richtlini

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			en Ihrer Organisation entsprechen.

Vorlage

Die Vorlage ist verfügbar unter GitHub: Operational Best Practices for CISA Cyber Essentials.

Bewährte Methoden für die Ausführung von Criminal Justice Information Services (CJIS)

Konformitätspakete bieten ein allgemeines Compliance-Framework, das es Ihnen ermöglicht, mithilfe verwalteter oder benutzerdefinierter AWS Config Regeln und Abhilfemaßnahmen Kontrollen zur Sicherheits-, Betriebs- oder Kostenoptimierung durchzuführen. AWS Config Conformance Packs dienen als Beispielvorlagen nicht dazu, die vollständige Einhaltung eines bestimmten Governance- oder Compliance-Standards sicherzustellen. Sie sind dafür verantwortlich, selbst zu beurteilen, ob Ihre Nutzung der Services den geltenden gesetzlichen und behördlichen Anforderungen entspricht.

Im Folgenden finden Sie ein Beispiel für eine Zuordnung zwischen den Compliance-Anforderungen der Criminal Justice Information Services (CJIS) und den AWS verwalteten Konfigurationsregeln. Jede Config-Regel gilt für eine bestimmte AWS Ressource und bezieht sich auf ein oder mehrere CJIS-Steuerelemente. Eine CJIS-Kontrolle kann mehreren Config-Regeln zugeordnet werden. In der folgenden Tabelle finden Sie weitere Informationen und Anleitungen zu diesen Zuordnungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
5.2	Schulung zum Sicherheitsbewusstsein	security-awareness-program-exists (Prozessüberprüfung)	Etablieren und pflegen Sie ein Programm zur Förderung des Sicherheitsbewusstseins in Ihrer Organisation. Programme zur

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			Förderung des Sicherheitsbewusstseins der Mitarbeiter vermitteln ihnen, wie sie ihre Organisation vor diversen Sicherheitsverletzungen oder Sicherheitsvorfällen schützen können.
5.3	Vorfallreaktion	response-plan-exists-maintained (Prozessüberprüfung)	Stellen Sie sicher, dass Vorfallreaktionspläne erstellt, verwaltet und an das verantwortliche Personal verteilt werden. Aktualisierte und formal dokumentierte Reaktionspläne können dazu beitragen, dass das zuständige Personal die Rollen, Verantwortlichkeiten und Prozesse versteht, die bei einem Vorfall einzuhalten sind.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
5.3	Vorfallreaktion	response-plan-tested (Prozessüberprüfung)	Stellen Sie sicher, dass die Vorfallre aktions- und Wiederherstellungs pläne getestet wurden. Dies kann Ihnen helfen zu verstehen, ob Ihr Plan bei einem Vorfall wirksam ist und ob etwaige Lücken behoben oder Aktualisierungen vorgenommen werden müssen.
5.4	Prüfung und Rechenschaftspflicht	audit-log-policy-exists (Prozessprüfung)	Richten Sie eine Richtlinie zur Verwaltung von Prüfprotokollen ein, in der die Protokoll ierungsanforderung en Ihres Unternehm ens definiert sind, und pflegen Sie diese Richtlinie. Dies beinhaltet, ist aber nicht beschränkt auf die Überprüfung und Aufbewahrung von Prüfprotokollen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
5.4.1	Überprüfbare Ereignisse und Inhalte (Informationssysteme)	api-gw-execution-logging-aktiviert	Die API-Gateway-Protokollierung zeigt detaillierte Ansichten der Benutzer, die auf die API zugegriffen haben, und wie diese Benutzer auf die API zugegriffen haben. Diese Einblicke ermöglichen die Transparenz von Benutzeraktivitäten.
5.4.1	Überprüfbare Ereignisse und Inhalte (Informationssysteme)	cloudwatch-log-group-encrypted	Um sensible Daten im Speicher zu schützen, stellen Sie sicher, dass die Verschlüsselung für Ihre Amazon CloudWatch Log Groups aktiviert ist.
5.4.1	Überprüfbare Ereignisse und Inhalte (Informationssysteme)	cloud-trail-cloud-watch-logs-aktiviert	Verwenden Sie Amazon CloudWatch , um Protokollereignisaktivitäten zentral zu sammeln und zu verwalten. Die Aufnahme von AWS CloudTrail Daten liefert Einzelheiten zu den API-Aufrufaktivitäten in Ihrem AWS-Konto.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
5.4.1	Überprüfbare Ereignisse und Inhalte (Informationssysteme)	cloud-trail-log-file-Validierung aktiviert	Verwenden Sie die AWS CloudTrail Protokolldateivalidierung, um die Integrität von Protokollen zu überprüfen. CloudTrail Mithilfe der Protokolldateivalidierung kann festgestellt werden, ob eine Protokolldatei geändert oder gelöscht wurde oder ob sie nach der Übermittlung CloudTrail unverändert geblieben ist. Dieses Feature wurde mit dem Branchenstandard entsprechenden Algorithmen entwickelt: SHA-256 für die Hashfunktion und SHA-256 mit RSA für digitale Signaturen. Aus diesem Grund ist es rechnerisch unmöglich, CloudTrail Protokolldateien unbemerkt zu ändern, zu löschen oder zu fälschen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
5.4.1	Überprüfbare Ereignisse und Inhalte (Informationssysteme)	codebuild-project-logging-enabled	Stellen Sie sicher, dass die AWS CodeBuild Projektprotokollierung aktiviert ist, damit Ihre Build-Ausgabeprotokolle entweder an Amazon CloudWatch oder Amazon Simple Storage Service (Amazon S3) gesendet werden. Build-Ausgabeprotokolle enthalten detaillierte Informationen zu Ihrem Build-Projekt.
5.4.1	Überprüfbare Ereignisse und Inhalte (Informationssysteme)	codebuild-project-s3-Log-verschlüsselt	Um sensible Daten im Speicher zu schützen, stellen Sie sicher, dass die Verschlüsselung für Ihre in Amazon S3 gespeicherten AWS CodeBuild Protokolle aktiviert ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
5.4.1	Überprüfbare Ereignisse und Inhalte (Informationssysteme)	cw-loggroup-retention-period-überprüfen	Stellen Sie sicher, dass die Ereignisprotokolldaten für Ihre Protokollgruppen über eine Mindestdauer aufbewahrt werden, um die Fehlerbehebung und forensische Untersuchungen zu unterstützen. Fehlende frühere Ereignisprotokolldaten erschweren die Rekonstruierung und Identifizierung potenziell schädlicher Ereignisse.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
5.4.1	Überprüfbare Ereignisse und Inhalte (Informationssysteme)	elasticsearch-logs-to-cloudwatch	Stellen Sie sicher, dass für Amazon OpenSearch Service-Domains Fehlerprotokolle aktiviert und zur Aufbewahrung und Beantwortung an Amazon CloudWatch Logs gestreamt werden. Domain-Fehlerprotokolle sind bei Sicherheits- und Zugriffsprüfungen sowie bei der Diagnose von Verfügbarkeitsproblemen nützlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
5.4.1	Überprüfbare Ereignisse und Inhalte (Informationssysteme)	elb-logging-enabled	Die Elastic-Load-Balancing-Aktivität ist ein zentraler Kommunikationspunkt innerhalb einer Umgebung. Stellen Sie sicher, dass die ELB-Protokollierung aktiviert ist. Die gesammelten Daten enthalten detaillierte Informationen zu Anfragen, die an den ELB gesendet wurden. Jedes Protokoll enthält Informationen wie die Zeit, zu der die Anforderung einging, die Client-IP-Adresse, Latenzen, Anforderungspfade und Serverantworten.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
5.4.1	Überprüfbare Ereignisse und Inhalte (Informationssysteme)	multi-region-cloudtrail-enabled	AWS CloudTrail zeichnet Aktionen und API-Aufrufe der AWS Management Console auf. Sie können feststellen, welche Benutzer und Konten angerufen wurden AWS, von welcher Quell-IP-Adresse aus die Anrufe getätigt wurden und wann die Anrufe erfolgten. CloudTrail übermittelt Protokolldateien aus allen AWS Regionen an Ihren S3-Bucket , wenn MULTI_REG ION_CLOUD _TRAIL_ENABLED aktiviert ist. Außerdem wird beim AWS Start einer neuen Region derselbe Trail in der neuen Region erstellt. CloudTrail Dadurch erhalten Sie automatis ch Protokolldateien mit API-Aktivitäten für die neue Region.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
5.4.1	Überprüfbare Ereignisse und Inhalte (Informationssysteme)	rds-logging-enabled	Um die Protokollierung und Überwachung in Ihrer Umgebung zu erleichtern, stellen Sie sicher, dass die Amazon Relational Database Service (Amazon RDS)-Protokollierung aktiviert ist. Mit der Amazon-RDS-Protokollierung können Sie Ereignisse wie Verbindungen, Verbindungsabbrüche, Abfragen oder abgefragte Tabellen erfassen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
5.4.1	Überprüfbare Ereignisse und Inhalte (Informationssysteme)	s-3 bucket-logging-enabled	Die Amazon Simple Storage Service (Amazon S3)-Serverzugriffs protokollierung bietet eine Methode zur Überwachu ng des Netzwerks im Hinblick auf potenzielle Cybersich erheitsereignisse. Die Ereignisse werden überwacht, indem detaillierte Aufzeichn ungen über die Anfragen erfasst werden, die an einen Amazon-S3-Bucket gestellt wurden. Jeder Zugriffsprotokolle intrag enthält Details zu einer einzelnen Zugriffsanfrage. Zu den Details gehören Anforderer, Bucket-Name, Anforderu ngszeit, Anforderu ngsaktion, Antwortst atus und Fehlercode, falls relevant.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
5.4.1	Überprüfbare Ereignisse und Inhalte (Informationssysteme)	vpc-flow-logs-enabled	VPC-Flow-Protokolle erfassen detaillierte Informationsdatensätze über den IP-Datenverkehr, der zu und von Netzwerkschnittstellen in Ihrer Amazon Virtual Private Cloud (Amazon VPC) fließt. Standardmäßig enthalten Flow-Protokolldatensätze Werte für die verschiedenen Komponenten des IP-Flows, einschließlich Quelle, Ziel und Protokoll.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
5.4.1	Überprüfbare Ereignisse und Inhalte (Informationssysteme)	wafv2-logging-enabled	Um die Protokollierung und Überwachung in Ihrer Umgebung zu erleichtern, aktivieren Sie die AWS WAF (V2) -Protokollierung im regionalen und globalen Web. ACLs AWS Die WAF-Protokollierung bietet detaillierte Informationen über den Datenverkehr, der von Ihrer Web-ACL analysiert wird. In den Protokollen werden die Uhrzeit aufgezeichnet, zu der die AWS WAF die Anfrage von Ihrer AWS Ressource erhalten hat, Informationen über die Anfrage und eine Aktion für die Regel, der jede Anfrage entsprach.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
5.4.1	Überprüfbare Ereignisse und Inhalte (Informationssysteme)	opensearch-audit-logging-enabled	Stellen Sie sicher, dass die Audit-Protokollierung für Ihre Amazon OpenSearch Service-Domains aktiviert ist. Mit der Audit-Protokollierung können Sie Benutzeraktivitäten auf Ihren OpenSearch Domains verfolgen, einschließlich erfolgreicher und fehlgeschlagener Authentifizierungen OpenSearch, Anfragen an, Indexänderungen und eingehende Suchanfragen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
5.4.1	Überprüfbare Ereignisse und Inhalte (Informationssysteme)	opensearch-logs-to-cloudwatch	Stellen Sie sicher, dass für Amazon OpenSearch Service-Domains Fehlerprotokolle aktiviert und zur Aufbewahrung und Beantwortung an Amazon CloudWatch Logs gestreamt werden. OpenSearch Service-Fehlerprotokolle können bei Sicherheits- und Zugriffsprüfungen helfen und bei der Diagnose von Verfügbarkeitsproblemen helfen.
5.4.1	Überprüfbare Ereignisse und Inhalte (Informationssysteme)	redshift-audit-logging-enabled	Um Informationen über Verbindungen und Benutzeraktivitäten in Ihrem Amazon-Redshift-Cluster zu erfassen, stellen Sie sicher, dass die Prüfprotokollierung aktiviert ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
5.4.5	Schutz von Prüfungsinformationen	cloudwatch-log-group-encrypted	Um sensible Daten im Speicher zu schützen, stellen Sie sicher, dass die Verschlüsselung für Ihre Amazon CloudWatch Log Groups aktiviert ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
5.4.5	Schutz von Prüfungsinformationen	cloud-trail-log-file-Validierung aktiviert	Verwenden Sie die AWS CloudTrail Protokolldateivalidierung, um die Integrität von Protokollen zu überprüfen. CloudTrail Mithilfe der Protokolldateivalidierung kann festgestellt werden, ob eine Protokolldatei geändert oder gelöscht wurde oder ob sie nach der Übermittlung CloudTrail unverändert geblieben ist. Dieses Feature wurde mit dem Branchenstandard entsprechenden Algorithmen entwickelt: SHA-256 für die Hashfunktion und SHA-256 mit RSA für digitale Signaturen. Aus diesem Grund ist es rechnerisch unmöglich, CloudTrail Protokolldateien unbemerkt zu ändern, zu löschen oder zu fälschen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
5.4.5	Schutz von Prüfungsinformationen	codebuild-project-s3-Log-verschlüsselt	Um sensible Daten im Speicher zu schützen, stellen Sie sicher, dass die Verschlüsselung für Ihre in Amazon S3 gespeicherten AWS CodeBuild Protokolle aktiviert ist.
5.4.6	Aufbewahrung von Prüfungsaufzeichnungen	cw-loggroup-retention-period-überprüfen	Stellen Sie sicher, dass die Ereignisprotokolldaten für Ihre Protokollgruppen über eine Mindestdauer aufbewahrt werden, um die Fehlerbehebung und forensische Untersuchungen zu unterstützen. Fehlende frühere Ereignisprotokolldaten erschweren die Rekonstruierung und Identifizierung potenziell schädlicher Ereignisse.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
5.4.6	Aufbewahrung von Prüfungsaufzeichnungen	s-3 bucket-default-lock-enabled	Stellen Sie sicher, dass für Ihren Amazon Simple Storage Service (Amazon S3)-Bucket standardmäßig eine Sperre aktiviert ist. Zum Schutz eventuell vorhandener sensibler Daten in S3-Buckets müssen Sie Objektsperren für Daten im Ruhezustand erzwingen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
5.5.2	Durchsetzung des Zugriffs	access-keys-rotated	Die Anmeldein formationen für autorisierte Geräte, Benutzer und Prozesse werden geprüft, indem sichergestellt wird, dass die IAM-Zugri ffsschlüssel entsprech end den Vorgaben der Unternehmensrichtl inie rotiert werden. Das regelmäßi ge Ändern der Zugriffsschlüssel ist eine bewährte Sicherheitsmethode . Es verkürzt den Zeitraum, in dem ein Zugriffsschlüssel aktiv ist, und reduziert die Auswirkungen auf das Unternehmen, wenn die Schlüssel kompromittiert werden. Diese Regel erfordert einen Wert für die Zugriffsschlüssel-Rotation (Standard konfiguration: 90). Der tatsächliche Wert muss den Richtlini

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			en Ihrer Organisation entsprechen.
5.5.2	Durchsetzung des Zugriffs	account-part-of-organizations	Durch die zentrale Verwaltung AWS-Konten innerhalb von AWS Organizations wird sichergestellt, dass die Konten den Vorschriften entsprechen. Eine fehlende zentrale Kontoverwaltung kann zu inkonsistenten Kontokonfigurationen führen, wodurch Ressourcen und sensible Daten offengelegt werden können.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
5.5.2	Durchsetzung des Zugriffs	iam-inline-policy-blocked-kms-Aktionen	Stellen Sie sicher, dass ein Benutzer, eine IAM-Rolle oder eine IAM-Gruppe (AWS Identity and Access Management) nicht über eine Inline-Richtlinie verfügt, die blockierte Aktionen für alle AWS Schlüssel des Key Management Service zulässt. AWS empfiehlt, verwaltete Richtlinien anstelle von Inline-Richtlinien zu verwenden. Verwaltete Richtlinien ermöglichen Wiederverwendbarkeit, Versionsverwaltung, Rollback und Delegierung der Berechtigungsverwaltung. Mit dieser Regel können Sie den blockedActionsPatterns Parameter festlegen. (Wert „AWS Bewährte grundlegende Sicherheitsmethoden“: kms:Decrypt, kms:ReEncryptFrom). Die

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.
5.5.2	Durchsetzung des Zugriffs	iam-no-inline-policy-überprüfen	Stellen Sie sicher, dass ein Benutzer, eine IAM-Rolle oder eine IAM-Gruppe (AWS Identity and Access Management) nicht über eine Inline-Richtlinie zur Zugriffskontrolle auf Systeme und Ressourcen verfügt. AWS empfiehlt, verwaltete Richtlinien anstelle von Inline-Richtlinien zu verwenden. Verwaltete Richtlinien ermöglichen Wiederverwendbarkeit, Versionsverwaltung, Rollback und Delegierung der Berechtigungsverwaltung.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
5.5.2	Durchsetzung des Zugriffs	iam-password-policy	Die Identitäten und Anmeldeinformationen werden auf der Grundlage einer organisatorischen IAM-Passwortrichtlinie ausgestellt, verwaltet und verifiziert. Sie erfüllen oder übertreffen die Anforderungen von NIST SP 800-63 und dem Standard „Best Practices“ von AWS Foundational Security für die Passwortstärke. Mit dieser Regel können Sie optional RequireUppercaseCharacters (CJIS-Wert: falsch), RequireLowercaseCharacters (CJIS-Wert: falsch), RequireSymbols (CJIS-Wert: falsch), RequireNumbers (CJIS-Wert: falsch), MinimumPasswordLength (CJIS-Wert: 8), PasswordReusePrevention (CJIS-Wert: 10) und MaxPasswo

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			rdAge (CJIS-Wert: 90) für Ihre IAM-Passwortrichtlinie festlegen. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.
5.5.2	Durchsetzung des Zugriffs	iam-policy-no-statements-with-full-access	Stellen Sie sicher, dass IAM-Aktionen nur auf die benötigten Aktionen beschränkt sind. Wenn Benutzern mehr Rechte eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und der Aufgabentrennung verstoßen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
5.5.2	Durchsetzung des Zugriffs	iam-root-access-key-überprüfen	Der Zugriff auf Systeme und Ressourcen kann gesteuert werden, indem überprüft wird, ob der Root-Benutzer keine Zugriffsschlüssel mit seiner AWS Identity and Access Management (IAM) -Rolle verknüpft hat. Stellen Sie sicher, dass die Root-Zugriffsschlüssel gelöscht werden. Erstellen und verwenden Sie stattdessen rollenbasierte Funktionen, AWS-Konten um das Prinzip der geringsten Funktionalität zu berücksichtigen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
5.5.2	Durchsetzung des Zugriffs	iam-user-group-membership-überprüfen	AWS Identity and Access Management (IAM) kann Ihnen helfen, Zugriffsberechtigungen und Autorisierungen einzuschränken, indem sichergestellt wird, dass Benutzer Mitglieder mindestens einer Gruppe sind. Wenn Benutzern mehr Berechtigungen eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und Aufgabentrennung verstoßen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
5.5.2	Durchsetzung des Zugriffs	iam-user-mfa-enabled	Aktivieren Sie diese Regel, um den Zugriff auf Ressourcen in der AWS Cloud einzuschränken. Diese Regel sorgt dafür, dass die Multi-Faktor-Authentifizierung (MFA) für alle Benutzer aktiviert ist. MFA sorgt für eine weitere Schutzebene zusätzlich zu den Anmeldeinformationen. Reduzieren Sie Fälle von kompromittierten Konten, indem Sie MFA für Benutzer vorschreiben.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
5.5.2	Durchsetzung des Zugriffs	iam-user-no-policies-überprüfen	Diese Regel stellt sicher, dass AWS Identity and Access Management (IAM) -Richtlinien nur Gruppen oder Rollen zugewiese n werden, um den Zugriff auf Systeme und Ressourcen zu kontrollieren. Die Zuweisung von Berechtig ungen auf Gruppen- oder Rollenebene trägt dazu bei, die Wahrscheinlichkeit zu verringern, dass eine Identität übermäßige Berechtigungen erhält oder beibehält.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
5.5.2	Durchsetzung des Zugriffs	iam-user-unused-credentials-überprüfen	AWS Identity and Access Management (IAM) kann Ihnen bei Zugriffsberechtigungen und Autorisierungen helfen, indem es nach IAM-Passwörtern und Zugriffsschlüsseln sucht, die für einen bestimmten Zeitraum nicht verwendet wurden. Wenn ungenutzte Anmeldeinformationen identifiziert werden, müssen Sie sie deaktivieren und/oder entfernen, da dies gegen das Prinzip der geringsten Berechtigung verstoßen könnte. Für diese Regel müssen Sie einen Wert für das maxCredentialUsage Alter festlegen (Standardkonfiguration: 90). Der tatsächliche Wert muss den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
5.5.2	Durchsetzung des Zugriffs	mfa-enabled-for-iam-Konsolenzugriff	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass MFA für alle AWS Identity and Access Management (IAM) -Benutzer aktiviert ist, die über ein Konsolenkennwort verfügen. MFA sorgt für eine weitere Schutzebene zusätzlich zu den Anmeldeinformationen. Indem Sie MFA für Benutzer vorschreiben, können Sie Fälle kompromittierter Konten reduzieren und verhindern, dass unbefugte Benutzer auf vertrauliche Daten zugreifen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
5.5.2	Durchsetzung des Zugriffs	rds-instance-iam-authentication-aktiviert	Stellen Sie sicher, dass eine AWS Identity and Access Management (IAM) -Authentifizierung auf Amazon Relational Database Service (Amazon RDS) -Instances aktiviert ist, um den Zugriff auf Systeme und Ressourcen zu kontrollieren. Dadurch wird die Verschlüsselung von ausgehendem und eingehendem Netzwerkverkehr von und zur Datenbank anhand von Secure Sockets Layer (SSL) durchgesetzt. Da die Authentifizierung extern verwaltet wird, ist es nicht erforderlich, Benutzeranmeldeinformationen in der Datenbank zu speichern.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
5.5.2	Durchsetzung des Zugriffs	s-3 bucket-acl-prohibited	Diese Regel prüft, ob Access Control Lists (ACLs) für die Zugriffskontrolle auf Amazon S3 S3-Buckets verwendet werden. ACLs sind veraltete Zugriffskontrollmechanismen für Amazon S3 S3-Buckets, die älter sind als AWS Identity and Access Management (IAM). Stattdessen empfiehlt es sich ACLs, IAM-Richtlinien oder S3-Bucket-Richtlinien zu verwenden, um den Zugriff auf Ihre S3-Buckets einfacher zu verwalten.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
5.5.2.1	Geringste Berechtigung	codebuild-project-environment-privileged-überprüfen	Um Sie bei der Implementierung des Prinzips der geringsten Rechte zu unterstützen, stellen Sie sicher, dass in Ihrer CodeBuild Amazon-Projektumgebung der privilegierte Modus nicht aktiviert ist. Diese Einstellung sollte deaktiviert werden, um einen unbeabsichtigten Zugriff auf Docker APIs sowie die dem Container zugrunde liegende Hardware zu verhindern.™
5.5.2.1	Geringste Berechtigung	ec-2 instance-profile-attached	EC2 Instanzprofile übergeben eine IAM-Rolle an eine Instanz EC2 . Das Anhängen eines Instance-Profils an Ihre Instances kann bei der Implementierung von geringsten Berechtigungen und der Berechtigungsverwaltung helfen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
5.5.2.1	Geringste Berechtigung	emr-kerberos-enabled	Die Zugriffsberechtigungen und -autorisierungen können verwaltet und nach den Prinzipien der geringsten Berechtigung und Aufgabentrennung integriert werden, indem Kerberos für Amazon-EMR-Cluster aktiviert wird. In Kerberos werden Services und Benutzer, die sich authentifizieren müssen, als Prinzipale bezeichnet. Prinzipale befinden sich in einem Kerberos-Bereich. Innerhalb dieses Bereichs wird ein Kerberos-Server als Key Distribution Center (KDC) bezeichnet. Über diesen Server können sich Prinzipale authentifizieren. Die Authentifizierung im KDC erfolgt durch die Ausstellung von Authentif

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			izierungstickets. Das KDC unterhält eine Datenbank der Prinzipale in seinem Bereich mit ihren Passwörtern und anderen administr ativen Informationen zu jedem Prinzipal.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
5.5.2.1	Geringste Berechtigung	iam-customer-policy-blocked-kms-Aktionen	AWS Identity and Access Management (IAM) kann Ihnen helfen, die Prinzipien der geringsten Rechte und der Aufgabentrennung in Zugriffsberechtigungen und Autorisierungen zu integrieren und so zu verhindern, dass Richtlinien blockierte Aktionen für alle AWS Schlüssel des Key Management Service enthalten. Wenn Benutzer mehr Rechte haben, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und Aufgabentrennung verstoßen. Mit dieser Regel können Sie den Parameter festlegen. blockedActionsPatterns (Wert „AWS Bewährte grundlegende Sicherheitsmethoden“: kms:

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			Decrypt, kms:ReEncryptFrom). Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.
5.5.2.1	Geringste Berechtigung	iam-group-has-users-überprüfen	AWS Identity and Access Management (IAM) kann Ihnen helfen, die Prinzipien der geringsten Rechte und der Aufgabentrennung mit Zugriffsberechtigungen und Autorisierungen zu integrieren, indem sichergestellt wird, dass IAM-Gruppen mindestens einen Benutzer haben. Die Einteilung von Benutzern in Gruppen auf der Grundlage der ihnen zugewiesenen Berechtigungen oder ihrer Funktion ist eine Möglichkeit, das Prinzip der geringsten Berechtigung zu implementieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
5.5.2.1	Geringste Berechtigung	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) kann Ihnen dabei helfen, die Prinzipien der geringsten Rechte und der Aufgabentrennung in Zugriffsberechtigungen und Autorisierungen zu integrieren und so zu verhindern, dass Richtlinien „Effect“: „Allow“ mit „Action“: „*“ anstelle von „Resource“: „*“ enthalten. Wenn Benutzern mehr Rechte eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und der Aufgabentrennung verstoßen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
5.5.2.1	Geringste Berechtigung	iam-policy-no-statements-with-full-access	Stellen Sie sicher, dass IAM-Aktionen nur auf die benötigten Aktionen beschränkt sind. Wenn Benutzern mehr Rechte eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und der Aufgabentrennung verstoßen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
5.5.2.1	Geringste Berechtigung	iam-user-group-membership-überprüfen	AWS Identity and Access Management (IAM) kann Ihnen helfen, Zugriffsberechtigungen und Autorisierungen einzuschränken, indem sichergestellt wird, dass Benutzer Mitglieder mindestens einer Gruppe sind. Wenn Benutzern mehr Berechtigungen eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und Aufgabentrennung verstoßen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
5.5.2.1	Geringste Berechtigung	iam-user-unused-credentials-überprüfen	AWS Identity and Access Management (IAM) kann Ihnen bei Zugriffsberechtigungen und Autorisierungen helfen, indem es nach IAM-Passwörtern und Zugriffsschlüsseln sucht, die für einen bestimmten Zeitraum nicht verwendet wurden. Wenn ungenutzte Anmeldeinformationen identifiziert werden, müssen Sie sie deaktivieren und/oder entfernen, da dies gegen das Prinzip der geringsten Berechtigung verstoßen könnte. Für diese Regel müssen Sie einen Wert für das maxCredentialUsage Alter festlegen (Standardkonfiguration: 90). Der tatsächliche Wert muss den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
5.5.2.1	Geringste Berechtigung	ecs-containers-nonprivileged	Um die Implementierung des Prinzips der geringsten Berechtigung zu unterstützen, dürfen in Amazon Elastic Container Service (Amazon ECS)-Aufgabendefinitionen keine erhöhten Berechtigungen aktiviert sein. Wenn dieser Parameter den Wert „true“ aufweist, erhält der Container erhöhte Berechtigungen auf der Host-Container-Instance (ähnlich wie der Root-Benutzer).

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
5.5.2.1	Geringste Berechtigung	ecs-containers-readonly-access	Die Aktivierung des schreibgeschützten Zugriffs auf Amazon-Elastic-Container-Service (ECS)-Container kann dazu beitragen, das Prinzip der geringsten Berechtigung einzuhalten. Diese Option kann Angriffsvektoren reduzieren, da das Dateisystem der Container-Instance nur geändert werden kann, wenn es über ausdrückliche Lese- und Schreibberechtigungen verfügt.
5.5.2.1	Geringste Berechtigung	ecs-task-definition-nonroot-Benutzer	Sie bestimmen einen Nicht-Root-Benutzer für den Zugriff auf Ihre Aufgabendefinitionen des Amazon Elastic Container Service (Amazon ECS), um die Implementierung des Prinzips der geringsten Berechtigung zu unterstützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
5.5.2.1	Geringste Berechtigung	efs-access-point-enforce-Benutzeridentität	Um die Implementierung des Prinzips der geringsten Rechte zu unterstützen, stellen Sie sicher, dass die Benutzerdurchsetzung für Ihr Amazon Elastic File System (Amazon EFS) aktiviert ist. Wenn diese Option aktiviert ist, ersetzt Amazon EFS den Benutzer und die Gruppe IDs des NFS-Clients durch die Identität, die auf dem Access Point für alle Dateisystemoperationen konfiguriert ist, und gewährt nur Zugriff auf diese erzwungene Benutzeridentität.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
5.5.2.1	Geringste Berechtigung	secretsmanager-secret-unused	Wenn in AWS Secrets Manager unbenutzte Anmeldeinformationen vorhanden sind, sollten Sie die Anmeldeinformationen deaktivieren und/oder entfernen, da dies gegen das Prinzip der geringsten Rechte verstoßen kann. Mit dieser Regel können Sie einen Wert auf unusedForDays (Config Default: 90) setzen. Der tatsächliche Wert muss den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
5.5.6	Remote-Zugriff	vpc-sg-open-only-to-authorized-ports	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass gemeinsame Ports für Amazon Elastic Compute Cloud (Amazon EC2) -Sicherheitsgruppen eingeschränkt sind. Wenn der Zugriff auf Ports nicht auf vertrauenswürdige Quellen beschränkt wird, kann dies zu Angriffen auf die Verfügbarkeit, Integrität und Vertraulichkeit von Systemen führen. Durch die Beschränkung des Zugriffs auf Ressourcen innerhalb einer Sicherheitsgruppe aus dem Internet (0.0.0.0/0) kann der Remote-Zugriff auf interne Systeme gesteuert werden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
5.5.6	Remote-Zugriff	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) Security Groups können bei der Verwaltung des Netzwerkzugriffs helfen, indem sie eine statusbehaftete Filterung des ein- und ausgehenden Netzwerkverkehrs zu Ressourcen bereitstellen. AWS Wenn Sie eingehenden (oder entfernten) Datenverkehr von 0.0.0.0/0 bis Port 22 auf Ihren Ressourcen nicht zulassen, können Sie den Remote-Zugriff einschränken.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
5.6.2.1.1	Passwort	iam-password-policy	Die Identitäten und Anmeldeinformationen werden auf der Grundlage einer organisatorischen IAM-Passwortrichtlinie ausgestellt, verwaltet und verifiziert. Sie erfüllen oder übertreffen die Anforderungen des NIST SP 800-63 und des AWS Foundational Security Best Practices-Standards für Passwortstärke. Mit dieser Regel können Sie optional RequireUppercaseCharacters (CJIS-Wert: falsch), RequireLowercaseCharacters (CJIS-Wert: falsch), RequireSymbols (CJIS-Wert: falsch), RequireNumbers (CJIS-Wert: falsch), MinimumPasswordLength (CJIS-Wert: 8), PasswordReusePrevention (CJIS-Wert: 10) und MaxPasswo

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			rdAge (CJIS-Wert: 90) für Ihre IAM-Passwortrichtlinie festlegen. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
5.6.2.2	Erweiterte Authentif izierung	emr-kerberos-enabled	Die Zugriffsberechtigu ngen und -autorisi erungen können verwaltet und nach den Prinzipien der geringsten Berechtig ung und Aufgabent rennung integrier t werden, indem Kerberos für Amazon-EMR-Cluster aktiviert wird. In Kerberos werden Services und Benutzer, die sich authentif izieren müssen, als Prinzipale bezeichnet. Prinzipal e befinden sich in einem Kerberos-Bereich. Innerhalb dieses Bereichs wird ein Kerberos-Server als Key Distribution Center (KDC) bezeichnet. Über diesen Server können sich Prinzipal e authentifizieren. Die Authentifizierung im KDC erfolgt durch die Ausstellu ng von Authentif

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			izierungstickets. Das KDC unterhält eine Datenbank der Prinzipale in seinem Bereich mit ihren Passwörtern und anderen administr ativen Informationen zu jedem Prinzipal.
5.6.2.2	Erweiterte Authentif izierung	iam-user-mfa-enabled	Aktivieren Sie diese Regel, um den Zugriff auf Ressourcen in der AWS Cloud einzuschr änken. Diese Regel sorgt dafür, dass die Multi-Faktor-Authe ntifizierung (MFA) für alle Benutzer aktiviert ist. MFA sorgt für eine weitere Schutzebe ne zusätzlich zu den Anmeldeinformation en. Reduzieren Sie Fälle von kompromit tierten Konten, indem Sie MFA für Benutzer vorschreiben.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
5.6.2.2	Erweiterte Authentifizierung	mfa-enabled-for-iam-Konsolenzugriff	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass MFA für alle AWS Identity and Access Management (IAM) -Benutzer aktiviert ist, die über ein Konsolenkennwort verfügen. MFA sorgt für eine weitere Schutzebene zusätzlich zu den Anmeldeinformationen. Indem Sie MFA für Benutzer vorschreiben, können Sie Fälle kompromittierter Konten reduzieren und verhindern, dass unbefugte Benutzer auf vertrauliche Daten zugreifen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
5.6.2.2	Erweiterte Authentifizierung	root-account-hardware-mfa-aktiviert	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Hardware-MFA für den Root-Benutzer aktiviert ist. Der Stammbenutzer ist der AWS-Konto-Benutzer mit den meisten Berechtigungen. MFA sorgt für eine weitere Schutzebene zusätzlich zu den Anmeldeinformationen. Indem Sie MFA für den Root-Benutzer vorschreiben, können Sie die Anzahl AWS-Konten kompromittierter Benutzer reduzieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
5.6.2.2	Erweiterte Authentifizierung	root-account-mfa-enabled	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass MFA für den Root-Benutzer aktiviert ist. Der Stammbenutzer ist der AWS-Konto-Benutzer mit den meisten Berechtigungen. MFA sorgt für eine weitere Schutzebene zusätzlich zu den Anmeldeinformationen. Indem Sie MFA für den Root-Benutzer vorschreiben, können Sie die Anzahl AWS-Konten kompromittierter Benutzer reduzieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
5.6.3.1	Verwaltung von Identifikatoren	iam-user-unused-credentials-überprüfen	AWS Identity and Access Management (IAM) kann Ihnen bei Zugriffsberechtigungen und Autorisierungen helfen, indem es nach IAM-Passwörtern und Zugriffsschlüsseln sucht, die für einen bestimmten Zeitraum nicht verwendet wurden. Wenn ungenutzte Anmeldeinformationen identifiziert werden, müssen Sie sie deaktivieren und/oder entfernen, da dies gegen das Prinzip der geringsten Berechtigung verstoßen könnte. Für diese Regel müssen Sie einen Wert für das maxCredentialUsage Alter festlegen (Standardkonfiguration: 90). Der tatsächliche Wert muss den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
5.7.1.1	Geringste Funktionalität	autoscaling-launch-config-public-ip-deaktiviert	Wenn Sie Ihre Netzwerkschnittstellen mit einer öffentlichen IP-Adresse konfigurieren, sind die diesen Netzwerkschnittstellen zugehörigen Ressourcen über das Internet erreichbar. EC2 Ressourcen sollten nicht öffentlich zugänglich sein, da dies einen unbeabsichtigten Zugriff auf Ihre Anwendungen oder Server ermöglichen kann.
5.7.1.1	Geringste Funktionalität	dms-replication-not-public	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass auf DMS-Replikationsinstanzen nicht öffentlich zugegriffen werden kann. DMS-Replikations-Instances können vertrauliche Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
5.7.1.1	Geringste Funktionalität	ebs-snapshot-public-restorable-überprüfen	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass EBS-Snapshots nicht öffentlich wiederherstellbar sind. EBS-Volume-Snapshots können vertrauliche Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.
5.7.1.1	Geringste Funktionalität	ec-2 instance-no-public-ip	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon Elastic Compute Cloud (Amazon EC2) - Instances nicht öffentlich zugänglich sind. EC2 Amazon-Instances können vertrauliche Informationen enthalten, und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
5.7.1.1	Geringste Funktionalität	elasticsearch-in-vpc-only	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass sich Amazon OpenSearch OpenSearch Service (Service) - Domains innerhalb einer Amazon Virtual Private Cloud (Amazon VPC) befinden. Eine OpenSearch Service-Domain innerhalb einer Amazon VPC ermöglicht die sichere Kommunikation zwischen OpenSearch Service und anderen Services innerhalb der Amazon VPC, ohne dass ein Internet-Gateway, ein NAT-Gerät oder eine VPN-Verbindung erforderlich ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
5.7.1.1	Geringste Funktionalität	emr-master-no-public-ip	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon EMR-Cluster-Masterknoten nicht öffentlich zugänglich sind. Amazon-EMR-Cluster-Hauptknoten können vertrauliche Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
5.7.1.1	Geringste Funktionalität	iam-root-access-key-überprüfen	Der Zugriff auf Systeme und Ressourcen kann gesteuert werden, indem überprüft wird, ob der Root-Benutzer keine Zugriffsschlüssel mit seiner AWS Identity and Access Management (IAM) -Rolle verknüpft hat. Stellen Sie sicher, dass die Root-Zugriffsschlüssel gelöscht werden. Erstellen und verwenden Sie stattdessen rollenbasierte Funktionen, AWS-Konten um das Prinzip der geringsten Funktionalität zu berücksichtigen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
5.7.1.1	Geringste Funktionalität	iam-user-group-membership-überprüfen	AWS Identity and Access Management (IAM) kann Ihnen helfen, Zugriffsberechtigungen und Autorisierungen einzuschränken, indem sichergestellt wird, dass Benutzer Mitglieder mindestens einer Gruppe sind. Wenn Benutzern mehr Berechtigungen eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und Aufgabentrennung verstoßen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
5.7.1.1	Geringste Funktionalität	iam-user-unused-credentials-überprüfen	AWS Identity and Access Management (IAM) kann Ihnen bei Zugriffsberechtigungen und Autorisierungen helfen, indem es nach IAM-Passwörtern und Zugriffsschlüsseln sucht, die für einen bestimmten Zeitraum nicht verwendet wurden. Wenn ungenutzte Anmeldeinformationen identifiziert werden, müssen Sie sie deaktivieren und/oder entfernen, da dies gegen das Prinzip der geringsten Berechtigung verstoßen könnte. Für diese Regel müssen Sie einen Wert für das maxCredentialUsage Alter festlegen (Standardkonfiguration: 90). Der tatsächliche Wert muss den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
5.7.1.1	Geringste Funktionalität	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) Security Groups können bei der Verwaltung des Netzwerkzugriffs helfen, indem sie eine statusbehaftete Filterung des ein- und ausgehenden Netzwerkverkehrs zu Ressourcen bereitstellen. AWS Wenn Sie eingehenden (oder entfernten) Datenverkehr von 0.0.0.0/0 bis Port 22 auf Ihren Ressourcen nicht zulassen, können Sie den Remote-Zugriff einschränken.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
5.7.1.1	Geringste Funktionalität	ec-2 instances-in-vpc	Stellen Sie Amazon Elastic Compute Cloud (Amazon EC2) -Instances innerhalb einer Amazon Virtual Private Cloud (Amazon VPC) bereit, um eine sichere Kommunikation zwischen einer Instance und anderen Services innerhalb der Amazon VPC zu ermöglichen, ohne dass ein Internet-Gateway, ein NAT-Gerät oder eine VPN-Verbindung erforderlich ist. Der gesamte Datenverkehr bleibt sicher in der AWS Cloud. Domains, die sich innerhalb einer VPC befinden, verfügen aufgrund ihrer logischen Isolierung im Vergleich zu Domains mit öffentlichen Endpunkten über eine zusätzliche Sicherheitsebene. Weisen Sie EC2

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			Amazon-Instances einer Amazon-VPC zu, um den Zugriff ordnungsgemäß zu verwalten.
5.7.1.1	Geringste Funktionalität	lambda-function-public-access-verboten	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass AWS Lambda-Funktionen nicht öffentlich zugänglich sind. Der öffentliche Zugriff kann möglicherweise die Verfügbarkeit von Ressourcen beeinträchtigen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
5.7.1.1	Geringste Funktionalität	lambda-inside-vpc	Stellen Sie AWS Lambda-Funktionen in einer Amazon Virtual Private Cloud (Amazon VPC) bereit, um eine sichere Kommunikation zwischen einer Funktion und anderen Diensten innerhalb der Amazon VPC zu gewährleisten. Bei dieser Konfiguration sind kein Internet-Gateway, kein NAT-Gerät und keine VPN-Verbindung erforderlich. Der gesamte Datenverkehr bleibt sicher in der Cloud. AWS Domains, die sich innerhalb einer VPC befinden, verfügen aufgrund ihrer logischen Isolierung im Vergleich zu Domains mit öffentlichen Endpunkten über eine zusätzliche Sicherheitsebene. Um den Zugriff ordnungsgemäß zu verwalten,

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			sollten AWS Lambda-Funktionen einer VPC zugewiesen werden.
5.7.1.1	Geringste Funktionalität	no-unrestricted-route-to-igw	Stellen Sie sicher, dass EC2 Amazon-Routentabellen keine uneingeschränkten Routen zu einem Internet-Gateway enthalten. Durch das Entfernen oder Beschränken des Internetzugangs für Workloads innerhalb von Amazon VPCs können unbeabsichtigte Zugriffe in Ihrer Umgebung reduziert werden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
5.7.1.1	Geringste Funktionalität	rds-instance-public-access-überprüfen	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Relational Database Service (Amazon RDS) -Instances nicht öffentlich sind. Amazon-RDS-Datenbank-Instances können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
5.7.1.1	Geringste Funktionalität	rds-snapshots-public-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Relational Database Service (Amazon RDS) -Instances nicht öffentlich sind. Amazon-RDS-Datenbank-Instances können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
5.7.1.1	Geringste Funktionalität	redshift-cluster-public-access-überprüfen	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Redshift Redshift-Cluster nicht öffentlich sind. Amazon-Redshift-Cluster können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
5.7.1.1	Geringste Funktionalität	s3-Blöcke-periodisch account-level-public-access	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Simple Storage Service (Amazon S3) -Buckets nicht öffentlich zugänglich sind. Diese Regel trägt dazu bei, sensible Daten vor unbefugten Remote-Benutzern zu schützen, indem sie den öffentlichen Zugriff verhindert. Mit dieser Regel können Sie optional die Parameter ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) und restrictPublicBuckets Parameter (Config Default: True) festlegen. Die tatsächlichen Werte müssen den Richtlini

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			en Ihrer Organisation entsprechen.
5.7.1.1	Geringste Funktionalität	s-3 bucket-public-read-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie nur autorisierten Benutzern, Prozessen und Geräten Zugriff auf Amazon Simple Storage Service (Amazon S3) - Buckets gewähren. Die Verwaltung des Zugriffs sollte mit der Klassifizierung der Daten übereinstimmen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
5.7.1.1	Geringste Funktionalität	s-3 bucket-public-write-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie nur autorisierten Benutzern, Prozessen und Geräten Zugriff auf Amazon Simple Storage Service (Amazon S3) - Buckets gewähren. Die Verwaltung des Zugriffs sollte mit der Klassifizierung der Daten übereinstimmen.
5.7.1.1	Geringste Funktionalität	sagemaker-notebook-no-direct-Internetzugang	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass SageMaker Amazon-Notebooks keinen direkten Internetzugang zulassen. Indem Sie direkten Internetzugang blockieren, vermeiden Sie, dass unbefugte Benutzer auf sensible Daten zugreifen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
5.7.1.1	Geringste Funktionalität	vpc-default-security-group-geschlossen	Sicherheitsgruppen von Amazon Elastic Compute Cloud (Amazon EC2) können bei der Verwaltung des Netzwerkzugriffs helfen, indem sie eine statusbehaftete Filterung des ein- und ausgehenden Netzwerkverkehrs zu Ressourcen bereitstellen. AWS Die Beschränkung des gesamten Datenverkehrs auf die Standardsicherheitsgruppe hilft dabei, den Fernzugriff auf Ihre Ressourcen einzuschränken. AWS

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
5.7.1.1	Geringste Funktionalität	vpc-sg-open-only-to-authorized-ports	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass gemeinsame Ports für Amazon Elastic Compute Cloud (Amazon EC2) -Sicherheitsgruppen eingeschränkt sind. Wenn der Zugriff auf Ports nicht auf vertrauenswürdige Quellen beschränkt wird, kann dies zu Angriffen auf die Verfügbarkeit, Integrität und Vertraulichkeit von Systemen führen. Durch die Beschränkung des Zugriffs auf Ressourcen innerhalb einer Sicherheitsgruppe aus dem Internet (0.0.0.0/0) kann der Remote-Zugriff auf interne Systeme gesteuert werden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
5.7.1.1	Geringste Funktionalität	ec2-prüfen managedinstance-association-compliance-status	Verwenden Sie AWS Systems Manager Associations, um bei der Inventarisierung von Softwareplattformen und Anwendungen innerhalb eines Unternehmens zu helfen. AWS Systems Manager weist Ihren verwalteten Instanzen einen Konfigurationsstatus zu und ermöglicht es Ihnen, Basiswerte für Betriebssystem-Patch-Levels, Softwareinstallationen, Anwendungskonfigurationen und andere Details zu Ihrer Umgebung festzulegen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
5.7.1.1	Geringste Funktionalität	opensearch-in-vpc-only	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass sich Amazon OpenSearch Service-Domains innerhalb einer Amazon Virtual Private Cloud (Amazon VPC) befinden. Eine Amazon OpenSearch Service-Domain innerhalb einer Amazon VPC ermöglicht die sichere Kommunikation zwischen Amazon OpenSearch Service und anderen Services innerhalb der Amazon VPC, ohne dass ein Internet-Gateway, ein NAT-Gerät oder eine VPN-Verbindung erforderlich ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
5.7.1.1	Geringste Funktionalität	restricted-common-ports	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass gemeinsame Ports für Amazon Elastic Compute Cloud (Amazon EC2) -Sicherheitsgruppen eingeschränkt sind. Wenn der Zugriff auf Ports nicht auf vertrauenswürdige Quellen beschränkt wird, kann dies zu Angriffen auf die Verfügbarkeit, Integrität und Vertraulichkeit von Systemen führen. Mit dieser Regel können Sie optional die Parameter blockedPort1–blockedPort5 festlegen (Standardkonfigurationen: 20, 21, 3389, 3306, 4333). Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
5.7.1.1	Geringste Funktionalität	s3- verboten bucket-level-public-access	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Simple Storage Service (Amazon S3) -Buckets nicht öffentlich zugänglich sind. Diese Regel trägt dazu bei, sensible Daten vor unbefugten Remote-Benutzern zu schützen, indem sie den öffentlichen Zugriff auf Bucket-Ebene verhindert.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
5.7.1.1	Geringste Funktionalität	subnet-auto-assign-public-ip-deaktiviert	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon Virtual Private Cloud (VPC) -Subnetzen nicht automatisch eine öffentliche IP-Adresse zugewiesen wird. Amazon Elastic Compute Cloud (EC2) -Instances, die in Subnetzen gestartet werden, in denen dieses Attribut aktiviert ist, haben ihrer primären Netzwerkschnittstelle eine öffentliche IP-Adresse zugewiesen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
5.10	System- und Kommunikationsschutz und Informationsintegrität	alb-http-drop-invalid-Header-fähig	Stellen Sie sicher, dass Ihre Elastic Load Balancers (ELB) so konfiguriert sind, dass sie HTTP-Header löschen. Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.
5.10	System- und Kommunikationsschutz und Informationsintegrität	alb-http-to-https-Umleitungsprüfung	Um Daten während der Übertragung zu schützen, stellen Sie sicher, dass Ihr Application Load Balancer unverschlüsselte HTTP-Anfragen automatisch an HTTPS umleitet. Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
5.10	System- und Kommunikationsschutz und Informationsintegrität	api-gw-associated-with-WAF	AWS Mit WAF können Sie eine Reihe von Regeln (als Web Access Control List (Web ACL) bezeichnet) konfigurieren, die Webanfragen auf der Grundlage von anpassbaren Websicherheitsregeln und -bedingungen, die Sie definieren, zulassen, blockieren oder zählen. Stellen Sie sicher, dass Ihre Amazon-API-Gateway-Stufe mit einer WAF-Web-ACL verknüpft ist, um sie vor böswilligen Angriffen zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
5.10	System- und Kommunikationsschutz und Informationsintegrität	elasticsearch-node-to-node-Verschlüsselungsprüfung	Stellen Sie sicher, dass die node-to-node Verschlüsselung für Amazon OpenSearch Service aktiviert ist. Node-to-nodeVerschlüsselung ermöglicht die TLS 1.2-Verschlüsselung für die gesamte Kommunikation innerhalb der Amazon Virtual Private Cloud (Amazon VPC). Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.
5.10	System- und Kommunikationsschutz und Informationsintegrität	elb-tls-https-listeners-nur	Stellen Sie sicher, dass Ihre Elastic Load Balancer (ELBs) mit SSL- oder HTTPS-Listenern konfiguriert sind. Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
5.10	System- und Kommunikationsschutz und Informationsintegrität	redshift-require-tls-ssl	Stellen Sie sicher, dass Ihre Amazon-Redshift-Cluster eine TLS/SSL-Verschlüsselung erfordern, um eine Verbindung zu SQL-Clients herzustellen. Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
5,10	System- und Kommunikationsschutz und Informationsintegrität	s3-Blöcke-periodisch account-level-public-access	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Simple Storage Service (Amazon S3) -Buckets nicht öffentlich zugänglich sind. Diese Regel trägt dazu bei, sensible Daten vor unbefugten Remote-Benutzern zu schützen, indem sie den öffentlichen Zugriff verhindert. Mit dieser Regel können Sie optional die Parameter ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) und restrictPublicBuckets Parameter (Config Default: True) festlegen. Die tatsächlichen Werte müssen den Richtlini

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			en Ihrer Organisation entsprechen.
5.10	System- und Kommunikationsschutz und Informationsintegrität	s-3 bucket-ssl-requests-only	Um Daten während der Übertragung zu schützen, stellen Sie sicher, dass Ihre Amazon Simple Storage Service (Amazon S3)-Buckets Anfragen zur Verwendung von Secure Socket Layer (SSL)-Buckets erfordern. Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
5,10	System- und Kommunikationsschutz und Informationsintegrität	wafv2-logging-enabled	Um die Protokollierung und Überwachung in Ihrer Umgebung zu erleichtern, aktivieren Sie die AWS WAF (V2) -Protokollierung im regionalen und globalen Web. ACLs AWS Die WAF-Protokollierung bietet detaillierte Informationen über den Datenverkehr, der von Ihrer Web-ACL analysiert wird. In den Protokollen werden die Uhrzeit aufgezeichnet, zu der die AWS WAF die Anfrage von Ihrer AWS Ressource erhalten hat, Informationen über die Anfrage und eine Aktion für die Regel, der jede Anfrage entsprach.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
5.10	System- und Kommunikationsschutz und Informationsintegrität	opensearch-node-to-node-Verschlüsselungsprüfung	Stellen Sie sicher, dass die node-to-node Verschlüsselung für Amazon OpenSearch Service aktiviert ist. Node-to-nodeVerschlüsselung ermöglicht die TLS 1.2-Verschlüsselung für die gesamte Kommunikation innerhalb der Amazon Virtual Private Cloud (Amazon VPC). Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
5.10	System- und Kommunikationsschutz und Informationsintegrität	s-3 bucket-acl-prohibited	Diese Regel prüft, ob Access Control Lists (ACLs) für die Zugriffskontrolle auf Amazon S3 S3-Buckets verwendet werden. ACLs sind veraltete Zugriffskontrollmechanismen für Amazon S3 S3-Buckets, die älter sind als AWS Identity and Access Management (IAM). Stattdessen empfiehlt es sich ACLs, IAM-Richtlinien oder S3-Bucket-Richtlinien zu verwenden, um den Zugriff auf Ihre S3-Buckets einfacher zu verwalten.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
5.10	System- und Kommunikationsschutz und Informationsintegrität	vpc-network-acl-unused-überprüfen	Diese Regel stellt sicher, dass Amazon Virtual Private Cloud (VPC)-Netzwerkzugriffskontrolllisten verwendet werden. Die Überwachung ungenutzter Netzwerkzugriffskontrolllisten kann zu einer genauen Inventarisierung und Verwaltung Ihrer Umgebung beitragen.
5.10	System- und Kommunikationsschutz und Informationsintegrität	waf-regional-webacl-not-leer	Eine an eine AWS WAF angehängte Web-ACL kann eine Sammlung von Regeln und Regelgruppen zur Überprüfung und Steuerung von Webanfragen enthalten. Wenn eine Web-ACL leer ist, wird der Webdatenverkehr weitergeleitet, ohne von der WAF erkannt oder bearbeitet zu werden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
5.10.1	Durchsetzung des Informationsflusses	alb-http-drop-invalid-Header-fähig	Stellen Sie sicher, dass Ihre Elastic Load Balancers (ELB) so konfiguriert sind, dass sie HTTP-Header löschen. Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.
5.10.1	Durchsetzung des Informationsflusses	alb-http-to-https-Umleitungsprüfung	Um Daten während der Übertragung zu schützen, stellen Sie sicher, dass Ihr Application Load Balancer unverschlüsselte HTTP-Anfragen automatisch an HTTPS umleitet. Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
5.10.1	Durchsetzung des Informationsflusses	elasticsearch-node-to-node-Verschlüsselungsprüfung	Stellen Sie sicher, dass die node-to-node Verschlüsselung für Amazon OpenSearch Service aktiviert ist. Node-to-nodeVerschlüsselung ermöglicht die TLS 1.2-Verschlüsselung für die gesamte Kommunikation innerhalb der Amazon Virtual Private Cloud (Amazon VPC). Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.
5.10.1	Durchsetzung des Informationsflusses	elb-tls-https-listeners-nur	Stellen Sie sicher, dass Ihre Elastic Load Balancer (ELBs) mit SSL- oder HTTPS-Listenern konfiguriert sind. Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
5.10.1	Durchsetzung des Informationsflusses	ec-2 instances-in-vpc	Stellen Sie Amazon Elastic Compute Cloud (Amazon EC2) -Instances innerhalb einer Amazon Virtual Private Cloud (Amazon VPC) bereit, um eine sichere Kommunika tion zwischen einer Instance und anderen Services innerhalb der Amazon VPC zu ermöglichen, ohne dass ein Internet-Gateway, ein NAT-Gerät oder eine VPN-Verbindung erforderlich ist. Der gesamte Datenverk ehr bleibt sicher in der AWS Cloud. Domains, die sich innerhalb einer VPC befinden, verfügen aufgrund ihrer logischen Isolierun g im Vergleich zu Domains mit öffentlic hen Endpunkten über eine zusätzlic he Sicherheitsebene. Weisen Sie EC2

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			Amazon-Instances einer Amazon-VPC zu, um den Zugriff ordnungsgemäß zu verwalten.
5.10.1	Durchsetzung des Informationsflusses	redshift-require-tls-ssl	Stellen Sie sicher, dass Ihre Amazon-Redshift-Cluster eine TLS/SSL-Verschlüsselung erfordern, um eine Verbindung zu SQL-Clients herzustellen. Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
5.10.1	Durchsetzung des Informationsflusses	s3-Blöcke-periodisch account-level-public-access	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Simple Storage Service (Amazon S3) -Buckets nicht öffentlich zugänglich sind. Diese Regel trägt dazu bei, sensible Daten vor unbefugten Remote-Benutzern zu schützen, indem sie den öffentlichen Zugriff verhindert. Mit dieser Regel können Sie optional die Parameter ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) und restrictPublicBuckets Parameter (Config Default: True) festlegen. Die tatsächlichen Werte müssen den Richtlini

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			en Ihrer Organisation entsprechen.
5.10.1	Durchsetzung des Informationsflusses	s-3 bucket-ssl-requests-only	Um Daten während der Übertragung zu schützen, stellen Sie sicher, dass Ihre Amazon Simple Storage Service (Amazon S3)-Buckets Anfragen zur Verwendung von Secure Socket Layer (SSL)-Buckets erfordern. Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
5.10.1	Durchsetzung des Informationsflusses	acm-certificate-expiration-check	Stellen Sie sicher, dass die Netzwerkintegrität geschützt ist, indem Sie sicherstellen, dass X509-Zertifikate von AWS ACM ausgestellt werden. Diese Zertifikate müssen gültig und dürfen nicht abgelaufen sein. Für diese Regel ist ein Wert für erforderlich daysToExpiration (Wert für bewährte AWS Grundregeln für Sicherheit: 90). Der tatsächliche Wert muss den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
5.10.1	Durchsetzung des Informationsflusses	dms-replication-not-public	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass auf DMS-Replikationsin stanzen nicht öffentlic h zugegriffen werden kann. DMS-Repli kations-Instances können vertrauli che Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.
5.10.1	Durchsetzung des Informationsflusses	ebs-snapshot-public-restorable-überprüfen	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass EBS-Snapshots nicht öffentlich wiederher stellbar sind. EBS-Volume-Snapsho ts können vertrauli che Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
5.10.1	Durchsetzung des Informationsflusses	ec-2 instance-no-public-ip	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon Elastic Compute Cloud (Amazon EC2) - Instances nicht öffentlich zugänglich sind. EC2 Amazon-Instances können vertrauliche Informationen enthalten, und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
5.10.1	Durchsetzung des Informationsflusses	elasticsearch-in-vpc-only	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass sich Amazon OpenSearch OpenSearch Service (Service) - Domains innerhalb einer Amazon Virtual Private Cloud (Amazon VPC) befinden. Eine OpenSearch Service-Domain innerhalb einer Amazon VPC ermöglicht die sichere Kommunikation zwischen OpenSearch Service und anderen Services innerhalb der Amazon VPC, ohne dass ein Internet-Gateway, ein NAT-Gerät oder eine VPN-Verbindung erforderlich ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
5.10.1	Durchsetzung des Informationsflusses	emr-master-no-public-ip	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon EMR-Cluster-Masterknoten nicht öffentlich zugänglich sind. Amazon-EMR-Cluster-Hauptknoten können vertrauliche Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
5.10.1	Durchsetzung des Informationsflusses	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) Security Groups können bei der Verwaltung des Netzwerkzugriffs helfen, indem sie eine statusbehaftete Filterung des ein- und ausgehenden Netzwerkverkehrs zu Ressourcen bereitstellen. AWS Wenn Sie eingehenden (oder entfernten) Datenverkehr von 0.0.0.0/0 bis Port 22 auf Ihren Ressourcen nicht zulassen, können Sie den Remote-Zugriff einschränken.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
5.10.1	Durchsetzung des Informationsflusses	lambda-function-public-access-verboten	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass AWS Lambda-Funktionen nicht öffentlich zugänglich sind. Der öffentliche Zugriff kann möglicherweise die Verfügbarkeit von Ressourcen beeinträchtigen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
5.10.1	Durchsetzung des Informationsflusses	lambda-inside-vpc	Stellen Sie AWS Lambda-Funktionen in einer Amazon Virtual Private Cloud (Amazon VPC) bereit, um eine sichere Kommunika tion zwischen einer Funktion und anderen Diensten innerhalb der Amazon VPC zu gewährleisten. Bei dieser Konfiguration sind kein Internet-Gateway, kein NAT-Gerät und keine VPN-Verbindung erforderlich. Der gesamte Datenverk ehr bleibt sicher in der Cloud. AWS Domains, die sich innerhalb einer VPC befinden, verfügen aufgrund ihrer logischen Isolierun g im Vergleich zu Domains mit öffentlic hen Endpunkten über eine zusätzliche Sicherheitsebene. Um den Zugriff ordnungsg emäß zu verwalten,

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			sollten AWS Lambda-Funktionen einer VPC zugewiesen werden.
5.10.1	Durchsetzung des Informationsflusses	opensearch-in-vpc-only	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass sich Amazon OpenSearch Service-Domains innerhalb einer Amazon Virtual Private Cloud (Amazon VPC) befinden. Eine Amazon OpenSearch Service-Domain innerhalb einer Amazon VPC ermöglicht die sichere Kommunikation zwischen Amazon OpenSearch Service und anderen Services innerhalb der Amazon VPC, ohne dass ein Internet-Gateway, ein NAT-Gerät oder eine VPN-Verbindung erforderlich ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
5.10.1	Durchsetzung des Informationsflusses	opensearch-node-to-node-Verschlüsselungsprüfung	Stellen Sie sicher, dass die node-to-node Verschlüsselung für Amazon OpenSearch Service aktiviert ist. Node-to-nodeVerschlüsselung ermöglicht die TLS 1.2-Verschlüsselung für die gesamte Kommunikation innerhalb der Amazon Virtual Private Cloud (Amazon VPC). Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
5.10.1	Durchsetzung des Informationsflusses	rds-instance-public-access-überprüfen	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Relational Database Service (Amazon RDS) -Instances nicht öffentlich sind. Amazon-RDS-Datenbank-Instances können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
5.10.1	Durchsetzung des Informationsflusses	rds-snapshots-public-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Relational Database Service (Amazon RDS) -Instances nicht öffentlich sind. Amazon-RDS-Datenbank-Instances können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
5.10.1	Durchsetzung des Informationsflusses	redshift-cluster-public-access-überprüfen	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Redshift Redshift-Cluster nicht öffentlich sind. Amazon-Redshift-Cluster können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
5.10.1	Durchsetzung des Informationsflusses	restricted-common-ports	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass gemeinsame Ports für Amazon Elastic Compute Cloud (Amazon EC2) -Sicherheitsgruppen eingeschränkt sind. Wenn der Zugriff auf Ports nicht auf vertrauenswürdige Quellen beschränkt wird, kann dies zu Angriffen auf die Verfügbarkeit, Integrität und Vertraulichkeit von Systemen führen. Mit dieser Regel können Sie optional die Parameter blockedPort1–blockedPort5 festlegen (Standardkonfigurationen: 20, 21, 3389, 3306, 4333). Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
5.10.1	Durchsetzung des Informationsflusses	s-3 bucket-public-read-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie nur autorisierten Benutzern, Prozessen und Geräten Zugriff auf Amazon Simple Storage Service (Amazon S3) - Buckets gewähren. Die Verwaltung des Zugriffs sollte mit der Klassifizierung der Daten übereinst immen.
5.10.1	Durchsetzung des Informationsflusses	s-3 bucket-public-write-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie nur autorisierten Benutzern, Prozessen und Geräten Zugriff auf Amazon Simple Storage Service (Amazon S3) - Buckets gewähren. Die Verwaltung des Zugriffs sollte mit der Klassifizierung der Daten übereinst immen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
5.10.1	Durchsetzung des Informationsflusses	sagemaker-notebook-no-direct-Internetzugang	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass SageMaker Amazon-Notebooks keinen direkten Internetzugang zulassen. Indem Sie direkten Internetzugang blockieren, vermeiden Sie, dass unbefugte Benutzer auf sensible Daten zugreifen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
5.10.1	Durchsetzung des Informationsflusses	vpc-default-security-group-geschlossen	Sicherheitsgruppen von Amazon Elastic Compute Cloud (Amazon EC2) können bei der Verwaltung des Netzwerkzugriffs helfen, indem sie eine statusbehaftete Filterung des ein- und ausgehenden Netzwerkverkehrs zu Ressourcen bereitstellen. AWS Die Beschränk ung des gesamten Datenverkehrs auf die Standardsicherheit sgruppe hilft dabei, den Fernzugriff auf Ihre Ressourcen einzuschränken. AWS

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
5.10.1	Durchsetzung des Informationsflusses	vpc-sg-open-only-to-authorized-ports	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass gemeinsame Ports für Amazon Elastic Compute Cloud (Amazon EC2) -Sicherheitsgruppen eingeschränkt sind. Wenn der Zugriff auf Ports nicht auf vertrauenswürdige Quellen beschränkt wird, kann dies zu Angriffen auf die Verfügbarkeit, Integrität und Vertraulichkeit von Systemen führen. Durch die Beschränkung des Zugriffs auf Ressourcen innerhalb einer Sicherheitsgruppe aus dem Internet (0.0.0.0/0) kann der Remote-Zugriff auf interne Systeme gesteuert werden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
5.10.1.1	Grenzschutz	alb-http-to-https-Umleitungsprüfung	Um Daten während der Übertragung zu schützen, stellen Sie sicher, dass Ihr Application Load Balancer unverschlüsselte HTTP-Anfragen automatisch an HTTPS umleitet. Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
5.10.1.1	Grenzschutz	alb-waf-enabled	Stellen Sie sicher, dass AWS WAF auf Elastic Load Balancers (ELB) aktiviert ist, um Webanwendungen zu schützen. Eine WAF trägt zum Schutz Ihrer Webanwend ungen oder APIs vor gängigen Web-Explo its bei. Diese Web-Exploits können sich auf die Verfügbar keit auswirken, die Sicherheit gefährden oder übermäßige Ressourcen in Ihrer Umgebung verbrauch en.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
5.10.1.1	Grenzschutz	api-gw-associated-with-WAF	AWS Mit WAF können Sie eine Reihe von Regeln (als Web Access Control List (Web ACL) bezeichnet) konfigurieren, die Webanfragen auf der Grundlage von anpassbaren Websicherheitsregeln und -bedingungen, die Sie definieren, zulassen, blockieren oder zählen. Stellen Sie sicher, dass Ihre Amazon-API-Gateway-Stufe mit einer WAF-Web-ACL verknüpft ist, um sie vor böswilligen Angriffen zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
5.10.1.1	Grenzschutz	elb-tls-https-listeners-nur	Stellen Sie sicher, dass Ihre Elastic Load Balancer (ELBs) mit SSL- oder HTTPS-Listenern konfiguriert sind. Um eventuell vorhanden e sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.
5.10.1.1	Grenzschutz	guardduty-enabled-centralized	Amazon GuardDuty kann mithilfe von Threat Intellige nce Feeds helfen, potenzielle Cybersich erheitsereignisse zu überwachen und zu erkennen. Dazu gehören Listen mit bösartigen IPs und maschinel len Lernmethoden zur Identifizierung unerwarteter, nicht autorisierter und bösartiger Aktivitäten in Ihrer AWS Cloud-Umgebung.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
5.10.1.1	Grenzschutz	guardduty-non-archived-findings	Amazon GuardDuty hilft Ihnen dabei, die Auswirkungen eines Vorfalls zu verstehen, indem es die Ergebnisse nach Schweregrad klassifiziert: niedrig, mittel und hoch. Diese Klassifizierungen können Sie zur Festlegung von entsprechenden Strategien und Prioritäten zur Behebung solcher Vorfälle verwenden. Mit dieser Regel können Sie optional daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7) und daysHighSev (Config Default: 1) für nicht archivierte Ergebnisse festlegen, wie es die Richtlinien Ihrer Organisation erfordern.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
5.10.1.1	Grenzschutz	wafv2-logging-enabled	Um die Protokollierung und Überwachung in Ihrer Umgebung zu erleichtern, aktivieren Sie die AWS WAF (V2) -Protokollierung im regionalen und globalen Web. ACLs AWS Die WAF-Protokollierung bietet detaillierte Informationen über den Datenverkehr, der von Ihrer Web-ACL analysiert wird. In den Protokollen werden die Uhrzeit aufgezeichnet, zu der die AWS WAF die Anfrage von Ihrer AWS Ressource erhalten hat, Informationen über die Anfrage und eine Aktion für die Regel, der jede Anfrage entsprach.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
5.10.1.1	Grenzschutz	opensearch-https-required	Da sensible Daten existieren können und um Daten während der Übertragung zu schützen, sollten Sie sicherstellen, dass HTTPS für Verbindungen zu Ihren Amazon OpenSearch Service-Domains aktiviert ist.
5.10.1.1	Grenzschutz	waf-regional-rule-not-leer	Stellen Sie sicher, dass Ihre AWS WAF eine Regel hat, die nicht leer ist. Eine Regel ohne Bedingungen kann zu unbeabsichtigtem Verhalten führen.
5.10.1.1	Grenzschutz	waf-regional-rulegroup-not-leer	Stellen Sie sicher, dass Ihre AWS WAF eine Regelgruppe hat, die nicht leer ist. Eine leere Regelgruppe kann zu unbeabsichtigtem Verhalten führen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
5.10.1.1	Grenzschutz	waf-regional-webacl-not-leer	Eine an eine AWS WAF angehängte Web-ACL kann eine Sammlung von Regeln und Regelgruppen zur Überprüfung und Steuerung von Webanfragen enthalten. Wenn eine Web-ACL leer ist, wird der Webdatenverkehr weitergeleitet, ohne von der WAF erkannt oder bearbeitet zu werden.
5.10.1.2	Verschlüsselung	alb-http-drop-invalid-Header-fähig	Stellen Sie sicher, dass Ihre Elastic Load Balancers (ELB) so konfiguriert sind, dass sie HTTP-Header löschen. Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
5.10.1.2	Verschlüsselung	alb-http-to-https-Umleitungsprüfung	Um Daten während der Übertragung zu schützen, stellen Sie sicher, dass Ihr Application Load Balancer unverschlüsselte HTTP-Anfragen automatisch an HTTPS umleitet. Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.
5.10.1.2	Verschlüsselung	api-gw-cache-enabled-und-verschlüsselt	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass die Verschlüsselung für den Cache Ihrer API-Gateway-Stufe aktiviert ist. Da für die API-Methode sensible Daten erfasst werden können, sollten Sie die Verschlüsselung von Daten im Ruhezustand aktivieren, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
5.10.1.2	Verschlüsselung	cloudtrail-security-trail-enabled	Diese Regel trägt dazu bei, die Verwendung der AWS empfohlenen bewährten Sicherheitsmethoden für sicherzustellen AWS CloudTrail, indem geprüft wird, ob mehrere Einstellungen aktiviert sind. Dazu gehören die Verwendung von Protokollverschlüsselung, Protokollvalidierung und Aktivierung AWS CloudTrail in mehreren Regionen.
5.10.1.2	Verschlüsselung	cloudwatch-log-group-encrypted	Um sensible Daten im Speicher zu schützen, stellen Sie sicher, dass die Verschlüsselung für Ihre Amazon CloudWatch Log Groups aktiviert ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
5.10.1.2	Verschlüsselung	cloud-trail-encryption-enabled	Da sensible Daten vorhanden sein können und um Daten im Ruhezustand zu schützen, sollten Sie sicherstellen, dass die Verschlüsselung für Ihre AWS CloudTrail Trails aktiviert ist.
5.10.1.2	Verschlüsselung	codebuild-project-artifact-encryption	Stellen Sie zum Schutz vertraulicher Daten im Ruhezustand sicher, dass die Verschlüsselung für Ihre AWS CodeBuild Artefakte aktiviert ist.
5.10.1.2	Verschlüsselung	codebuild-project-s3-Log-verschlüsselt	Um sensible Daten im Speicher zu schützen, stellen Sie sicher, dass die Verschlüsselung für Ihre in Amazon S3 gespeicherten AWS CodeBuild Protokolle aktiviert ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
5.10.1.2	Verschlüsselung	dynamodb-table-encrypted-kms	Stellen Sie sicher, dass die Verschlüsselung für Ihre Amazon-DynamoDB-Tabellen aktiviert ist. Um eventuell vorhandene sensible Daten im Ruhezustand in diesen Tabellen zu schützen, müssen Sie die Verschlüsselung von Daten im Ruhezustand aktivieren. Standardmäßig werden DynamoDB-Tabellen mit einem AWS eigenen Kundenhauptschlüssel (CMK) verschlüselt.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
5.10.1.2	Verschlüsselung	ec-2 ebs-encryption-by-default	Zum Schutz von Daten im Ruhezustand müssen Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon Elastic Block Store (Amazon EBS)-Volumes aktiviert ist. Da sensible Daten auch im Ruhezustand vorhanden sein können, sollten Sie die Verschlüsselung im Ruhezustand aktivieren, um diese Daten zu schützen.
5.10.1.2	Verschlüsselung	efs-encrypted-check	Aktivieren Sie die Verschlüsselung für Ihr Amazon Elastic File System (EFS), um eventuell vorhandene sensible Daten sowie Daten im Ruhezustand zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
5.10.1.2	Verschlüsselung	elasticsearch-encrypted-at-rest	Da sensible Daten vorhanden sein können und um Daten im Ruhezustand zu schützen, sollten Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon OpenSearch Service (OpenSearch Service) -Domains aktiviert ist.
5.10.1.2	Verschlüsselung	elasticsearch-node-to-node-Verschlüsselungsprüfung	Stellen Sie sicher, dass die node-to-node Verschlüsselung für Amazon OpenSearch Service aktiviert ist. Node-to-nodeVerschlüsselung ermöglicht die TLS 1.2-Verschlüsselung für die gesamte Kommunikation innerhalb der Amazon Virtual Private Cloud (Amazon VPC). Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
5.10.1.2	Verschlüsselung	elv 2- acm-certificate-required	Zum Schutz von eventuell vorhanden en sensiblen Daten sowie von Daten während der Übertragung muss die Verschlüsselung für Ihr Elastic Load Balancing aktiviert sein. Verwenden Sie AWS Certificate Manager, um öffentlic he und private SSL/ TLS-Zertifikate mit AWS Diensten und internen Ressource n zu verwalten, bereitzustellen und bereitzustellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
5.10.1.2	Verschlüsselung	elb-acm-certificate-required	Zum Schutz von eventuell vorhanden en sensiblen Daten sowie von Daten während der Übertragung muss die Verschlüsselung für Ihr Elastic Load Balancing aktiviert sein. Verwenden Sie AWS Certificate Manager, um öffentlic he und private SSL/ TLS-Zertifikate mit AWS Diensten und internen Ressource n zu verwalten, bereitzustellen und bereitzustellen.
5.10.1.2	Verschlüsselung	elb-tls-https-listeners-nur	Stellen Sie sicher, dass Ihre Elastic Load Balancer (ELBs) mit SSL- oder HTTPS-Listenern konfiguriert sind. Um eventuell vorhanden e sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
5.10.1.2	Verschlüsselung	encrypted-volumes	Aktivieren Sie die Verschlüsselung für Ihre Amazon-Elastic-Block-Store (Amazon-EBS)-Volumes, um eventuell vorhandene sensible Daten sowie Daten im Ruhezustand zu schützen.
5.10.1.2	Verschlüsselung	kinesis-stream-encrypted	Aktivieren Sie die Verschlüsselung für Ihre Amazon-Kinesis-Streams, um eventuell vorhandene sensible Daten sowie Daten im Ruhezustand zu schützen.
5.10.1.2	Verschlüsselung	rds-snapshot-encrypted	Stellen Sie sicher, dass die Verschlüsselung für Ihre Amazon Relational Database Service (Amazon RDS)-Snapshots aktiviert ist. Da sensible Daten auch im Ruhezustand vorhanden sein können, sollten Sie die Verschlüsselung im Ruhezustand aktivieren, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
5.10.1.2	Verschlüsselung	rds-storage-encrypted	Zum Schutz von Daten im Ruhezustand müssen Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon Relational Database Service (Amazon RDS)-Instances aktiviert ist. Um eventuell vorhandene sensible Daten im Ruhezustand in Amazon-RDS-Instances zu schützen, muss die Verschlüsselung von Daten im Ruhezustand aktiviert sein.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
5.10.1.2	Verschlüsselung	redshift-cluster-configuration-check	Um Daten im Ruhezustand zu schützen, muss die Verschlüsselung für Ihre Amazon-Redshift-Cluster aktiviert sein. Sie müssen auch sicherstellen, dass die erforderlichen Konfigurationen auf Amazon-Redshift-Clustern bereitgestellt werden. Die Prüfungsprotokollierung muss aktiviert sein, um Informationen zu Verbindungen und Benutzeraktivitäten in der Datenbank bereitzustellen. Diese Regel erfordert, dass ein Wert für clusterDbEncrypted (Config Default: TRUE) und LoggingEnabled (Config Default: TRUE) gesetzt ist. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
5.10.1.2	Verschlüsselung	redshift-require-tls-ssl	Stellen Sie sicher, dass Ihre Amazon-Redshift-Cluster eine TLS/SSL-Verschlüsselung erfordern, um eine Verbindung zu SQL-Clients herzustellen. Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.
5.10.1.2	Verschlüsselung	s3-fähig bucket-server-side-encryption	Zum Schutz von Daten im Ruhezustand müssen Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon Simple Storage Service (Amazon S3)-Buckets aktiviert ist. Um eventuell vorhandene sensible Daten im Ruhezustand in Amazon-S3-Buckets zu schützen, muss die Verschlüsselung aktiviert sein.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
5.10.1.2	Verschlüsselung	s-3 bucket-ssl-requests-only	Um Daten während der Übertragung zu schützen, stellen Sie sicher, dass Ihre Amazon Simple Storage Service (Amazon S3)-Buckets Anfragen zur Verwendung von Secure Socket Layer (SSL)-Buckets erfordern. Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.
5.10.1.2	Verschlüsselung	s-3 default-encryption-kms	Stellen Sie sicher, dass die Verschlüsselung für Ihre Amazon Simple Storage Service (Amazon S3)-Buckets aktiviert ist. Um eventuell vorhandene sensible Daten im Ruhezustand in einem Amazon-S3-Bucket zu schützen, muss die Verschlüsselung aktiviert sein.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
5.10.1.2	Verschlüsselung	sagemaker-endpoint-configuration-kms-key-konfiguriert	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass die Verschlüsselung mit dem AWS Key Management Service (AWS KMS) für Ihren Endpunkt aktiviert ist. SageMaker Da sensible Daten auf dem SageMaker Endgerät gespeiche rt werden können, sollten Sie die Verschlüsselung im Ruhezustand aktiviere n, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
5.10.1.2	Verschlüsselung	sagemaker-notebook-instance-kms-key-konfiguriert	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass die Verschlüsselung mit dem AWS Key Management Service (AWS KMS) für Ihr Notebook aktiviert ist. SageMaker Da vertrauliche Daten im SageMaker Notebook gespeichert werden können, sollten Sie die Verschlüsselung im Ruhezustand aktivieren, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
5.10.1.2	Verschlüsselung	sns-encrypted-kms	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass Ihre Amazon Simple Notification Service (Amazon SNS) -Themen mit dem AWS Key Management Service (AWS KMS) verschlüsselt werden müssen. Um eventuell vorhandene sensible Daten im Ruhezustand in veröffentlichten Nachrichten zu schützen, muss die Verschlüsselung von Daten im Ruhezustand aktiviert sein.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
5.10.1.2	Verschlüsselung	backup-recovery-point-encrypted	Stellen Sie sicher, dass die Verschlüsselung für Ihre AWS Backup-Wiederherstellungspunkte aktiviert ist. Da sensible Daten auch im Ruhezustand vorhanden sein können, sollten Sie die Verschlüsselung im Ruhezustand aktivieren, um diese Daten zu schützen.
5.10.1.2	Verschlüsselung	opensearch-encrypted-at-rest	Da sensible Daten vorhanden sein können und um Daten im Ruhezustand zu schützen, sollten Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon OpenSearch Service-Domains aktiviert ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
5.10.1.2	Verschlüsselung	opensearch-node-to-node-Verschlüsselungsprüfung	Stellen Sie sicher, dass die node-to-node Verschlüsselung für Amazon OpenSearch Service aktiviert ist. Node-to-nodeVerschlüsselung ermöglicht die TLS 1.2-Verschlüsselung für die gesamte Kommunikation innerhalb der Amazon Virtual Private Cloud (Amazon VPC). Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
5.10.1.2	Verschlüsselung	redshift-cluster-kms-enabled	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass die Verschlüs selung mit AWS Key Management Service (AWS KMS) für Ihren Amazon Redshift Redshift-Cluster aktiviert ist. Um eventuell vorhanden e sensible Daten im Ruhezustand in Redshift-Clustern zu schützen, muss die Verschlüsselung von Daten im Ruhezusta nd aktiviert sein.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
5.10.1.2	Verschlüsselung	secretsmanager-using-cmk	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass die Verschlüsselung mit dem AWS Key Management Service (AWS KMS) für AWS Secrets Manager aktiviert ist. Aktivieren Sie die Verschlüsselung von Daten im Ruhezustand, um eventuell vorhandene sensible Daten im Ruhezustand im Secrets Manager zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
5.10.1.3	Tools und Techniken zur Erkennung von Eindringlingen	guardduty-enabled-centralized	Amazon GuardDuty kann mithilfe von Threat Intellige nce Feeds helfen, potenzielle Cybersich erheitsereignisse zu überwachen und zu erkennen. Dazu gehören Listen mit bösartigen IPs und maschinel len Lernmethoden zur Identifizierung unerwarteter, nicht autorisierter und bösartiger Aktivitäten in Ihrer AWS Cloud-Umgebung.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
5.10.1.3	Tools und Techniken zur Erkennung von Eindringlingen	guardduty-non-archived-findings	Amazon GuardDuty hilft Ihnen dabei, die Auswirkungen eines Vorfalls zu verstehen, indem es die Ergebnisse nach Schweregrad klassifiziert: niedrig, mittel und hoch. Diese Klassifizierungen können Sie zur Festlegung von entsprechenden Strategien und Prioritäten zur Behebung solcher Vorfälle verwenden. Mit dieser Regel können Sie optional daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7) und daysHighSev (Config Default: 1) für nicht archivierte Ergebnisse festlegen, wie es die Richtlinien Ihrer Organisation erfordern.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
5.10.1.3	Tools und Techniken zur Erkennung von Eindringlingen	securityhub-enabled	AWS Security Hub hilft bei der Überwachung von unbefugtem Personal, Verbindungen, Geräten und Software. AWS Security Hub aggregiert, organisiert und priorisiert die Sicherheitswarnungen oder Ergebnisse mehrerer Dienste. AWS Einige dieser Dienste sind Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer und AWS Firewall Manager sowie AWS Partnerlösungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
5.10.4.1	Patch-Management	ec2-manager instance-managed-by-systems	Eine Bestandsaufnahme der Softwareplattformen und Anwendungen innerhalb des Unternehmens ist möglich, indem Amazon Elastic Compute Cloud (Amazon EC2) - Instances mit AWS Systems Manager verwaltet werden. Verwenden Sie AWS Systems Manager, um detaillierte Systemkonfigurationen, Betriebssystem-Patch-Levels, Namen und Typ der Dienste, Softwareinstallationen, Anwendungsname, Herausgeber und Version sowie andere Details zu Ihrer Umgebung bereitzustellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
5.10.4.1	Patch-Management	ec2-prüfen managedinstance-association-compliance-status	Verwenden Sie AWS Systems Manager Associations, um bei der Inventarisierung von Softwareplattformen und Anwendungen innerhalb eines Unternehmens zu helfen. AWS Systems Manager weist Ihren verwalteten Instanzen einen Konfigurationsstatus zu und ermöglicht es Ihnen, Basiswerte für Betriebssystem-Patch-Levels, Softwareinstallationen, Anwendungskonfigurationen und andere Details zu Ihrer Umgebung festzulegen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
5.10.4.1	Patch-Management	ec2-prüfen managedinstance-patch-compliance-status	Aktivieren Sie diese Regel, um bei der Identifizierung und Dokumentation von Sicherheitslücken in Amazon Elastic Compute Cloud (Amazon EC2) zu helfen. Die Regel prüft, ob die EC2 Amazon-Instance die Patch-Konformität im AWS Systems Manager gemäß den Richtlinien und Verfahren Ihrer Organisation einhält.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
5.10.4.1	Patch-Management	ecs-fargate-latest-platform-Ausführung	Sicherheitsupdates und Patches werden automatisch für Ihre AWS Fargate-Aufgaben bereitgestellt. Wenn ein Sicherheitsproblem gefunden wird, das eine AWS Fargate-Plattformversion betrifft, AWS wird die Plattformversion gepatcht. Um Sie bei der Patchverwaltung Ihrer Amazon Elastic Container Service (ECS) - Aufgaben zu unterstützen, auf denen AWS Fargate ausgeführt wird, aktualisieren Sie Ihre eigenständigen Service-Aufgaben, sodass sie die neueste Plattformversion verwenden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
5.10.4.1	Patch-Management	elastic-beanstalk-managed-updates-aktiviert	Durch die Aktivierung verwalteter Plattform updates für eine Amazon-Elastic-Beanstalk-Umgebung wird sichergestellt, dass die aktuellen verfügbaren Plattform -Fixes, -Updates und -Features für die Umgebung installiert sind. Eine bewährte Methode zur Sicherung von Systemen besteht darin, stets die aktuellen Patches zu installieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
5.10.4.4	Sicherheitswarnungen und -hinweise	guardduty-enabled-centralized	Amazon GuardDuty kann mithilfe von Threat Intellige nce Feeds helfen, potenzielle Cybersich erheitsereignisse zu überwachen und zu erkennen. Dazu gehören Listen mit bösartigen IPs und maschinel len Lernmethoden zur Identifizierung unerwarteter, nicht autorisierter und bösartiger Aktivitäten in Ihrer AWS Cloud-Umgebung.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
5.10.4.4	Sicherheitswarnungen und -hinweise	guardduty-non-archived-findings	Amazon GuardDuty hilft Ihnen dabei, die Auswirkungen eines Vorfalls zu verstehen, indem es die Ergebnisse nach Schweregrad klassifiziert: niedrig, mittel und hoch. Diese Klassifizierungen können Sie zur Festlegung von entsprechenden Strategien und Prioritäten zur Behebung solcher Vorfälle verwenden. Mit dieser Regel können Sie optional daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7) und daysHighSev (Config Default: 1) für nicht archivierte Ergebnisse festlegen, wie es die Richtlinien Ihrer Organisation erfordern.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
5.10.4.4	Sicherheitswarnungen und -hinweise	securityhub-enabled	AWS Security Hub hilft bei der Überwachung von unbefugtem Personal, Verbindungen, Geräten und Software. AWS Security Hub aggregiert, organisiert und priorisiert die Sicherheitswarnungen oder Ergebnisse mehrerer Dienste. AWS Einige dieser Dienste sind Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer und AWS Firewall Manager sowie AWS Partnerlösungen.

Vorlage

Die Vorlage ist verfügbar unter GitHub: Operational Best Practices for CJIS.

Bewährte Methoden für die Ausführung von CMMC 2.0 Level 1

Konformitätspakete bieten ein allgemeines Compliance-Framework, das es Ihnen ermöglicht, mithilfe verwalteter oder benutzerdefinierter Regeln und Abhilfemaßnahmen Kontrollen zur Sicherheits-, Betriebs- oder Kostenoptimierung durchzuführen. AWS Config AWS Config Conformance Packs

dienen als Beispielvorlagen nicht dazu, die vollständige Einhaltung eines bestimmten Governance- oder Compliance-Standards sicherzustellen. Sie sind dafür verantwortlich, selbst zu beurteilen, ob Ihre Nutzung der Services den geltenden gesetzlichen und behördlichen Anforderungen entspricht.

Im Folgenden finden Sie ein Beispiel für eine Zuordnung zwischen der Cybersecurity Maturity Model Certification (CMMC) 2.0 Level 1 und den AWS verwalteten Konfigurationsregeln. Jede Config-Regel gilt für eine bestimmte AWS Ressource und bezieht sich auf ein oder mehrere CMMC 2.0 Level 1-Steuerelemente. Eine CMMC-2.0-Level-1-Kontrolle kann mehreren Config-Regeln zugeordnet werden. In der folgenden Tabelle finden Sie weitere Informationen und Anleitungen zu diesen Zuordnungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC.L1-3.1.1	Beschränken Sie den Zugriff auf Informationssystem e auf autorisierte Benutzer, Prozesse von autorisierten Benutzern oder Geräte (einschließlich anderer Informati onssysteme).	access-keys-rotated	Die Anmeldein formationen für autorisierte Geräte, Benutzer und Prozesse werden geprüft, indem sichergestellt wird, dass die IAM-Zugri ffsschlüssel gemäß den Vorgaben der Unternehmensrichtl inie rotiert werden. Das regelmäßi ge Ändern der Zugriffsschlüssel ist eine bewährte Sicherheitsmethode . Es verkürzt den Zeitraum, in dem ein Zugriffsschlüssel aktiv ist, und reduziert die Auswirkungen auf das Unternehmen,

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			wenn die Schlüssel kompromittiert werden. Diese Regel erfordert einen Wert für die Zugriffsschlüssel-Rotation (Standard konfiguration: 90). Der tatsächliche Wert muss den Richtlini en Ihrer Organisation entsprechen.
AC.L1-3.1.1	Beschränken Sie den Zugriff auf Informationssystem e auf autorisierte Benutzer, Prozesse von autorisierten Benutzern oder Geräte (einschließlich anderer Informati onssysteme).	dms-replication-not-public	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass auf DMS-Replikationsin stanzen nicht öffentlic h zugegriffen werden kann. DMS-Repli kations-Instances können vertrauli che Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC.L1-3.1.1	Beschränken Sie den Zugriff auf Informationssystem e auf autorisierte Benutzer, Prozesse von autorisierten Benutzern oder Geräte (einschließlich anderer Informati onssysteme).	ebs-snapshot-public-restorable-überprüfen	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass EBS-Snapshots nicht öffentlich wiederher stellbar sind. EBS-Volume-Snapsho ts können vertrauli che Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC.L1-3.1.1	Beschränken Sie den Zugriff auf Informationssystem e auf autorisierte Benutzer, Prozesse von autorisierten Benutzern oder Geräte (einschließlich anderer Informati onssysteme).	ec2-imdsv2-check	Stellen Sie sicher, dass die Methode Instance Metadata Service Version 2 (IMDSv2) aktiviert ist, um den Zugriff auf und die Kontrolle der Amazon Elastic Compute Cloud (Amazon EC2) - Instance-Metadate n zu schützen. Die IMDSv2 Methode verwendet sitzungsb asierte Kontrollen. Mit können Kontrolle n implementiert werden IMDSv2, um Änderungen an Instanzmetadaten einzuschränken.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC.L1-3.1.1	Beschränken Sie den Zugriff auf Informationssystem e auf autorisierte Benutzer, Prozesse von autorisierten Benutzern oder Geräte (einschließlich anderer Informati onssysteme).	ec-2 instance-no-public-ip	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon Elastic Compute Cloud (Amazon EC2) - Instances nicht öffentlich zugänglich sind. EC2 Amazon-Instances können vertrauliche Informati onen enthalten, und für solche Konten ist eine Zugriffskontrolle erforderlich.
AC.L1-3.1.1	Beschränken Sie den Zugriff auf Informationssystem e auf autorisierte Benutzer, Prozesse von autorisierten Benutzern oder Geräte (einschließlich anderer Informati onssysteme).	ec-2 instance-profile-a ttached	EC2 Instanzprofile übergeben eine IAM-Rolle an eine EC2 Instance. Das Anhängen eines Instance-Profils an Ihre Instances kann bei der Implement ierung von geringste n Berechtigungen und der Berechtig ungsverwaltung helfen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC.L1-3.1.1	Beschränken Sie den Zugriff auf Informationssystem e auf autorisierte Benutzer, Prozesse von autorisierten Benutzern oder Geräte (einschließlich anderer Informati onssysteme).	elasticsearch-in-vpc-only	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherste llen, dass sich Amazon OpenSearc h OpenSearch Service (Service) - Domains innerhalb einer Amazon Virtual Private Cloud (Amazon VPC) befinden. Eine OpenSearch Service-Domain innerhalb einer Amazon VPC ermöglicht die sichere Kommunikation zwischen OpenSearc h Service und anderen Services innerhalb der Amazon VPC, ohne dass ein Internet-Gateway, ein NAT-Gerät oder eine VPN-Verbindung erforderlich ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC.L1-3.1.1	Beschränken Sie den Zugriff auf Informationssystem e auf autorisierte Benutzer, Prozesse von autorisierten Benutzern oder Geräte (einschließlich anderer Informati onssysteme).	emr-kerberos-enabled	Die Zugriffsberechtigu ngen und -autorisi erungen können verwaltet und nach den Prinzipien der geringsten Berechtig ung und Aufgabent rennung integrier t werden, indem Kerberos für Amazon-EMR-Cluster aktiviert wird. In Kerberos werden Services und Benutzer, die sich authentif izieren müssen, als Prinzipale bezeichnet. Prinzipal e befinden sich in einem Kerberos-Bereich. Innerhalb dieses Bereichs wird ein Kerberos-Server als Key Distribution Center (KDC) bezeichnet. Über diesen Server können sich Prinzipal e authentifizieren. Die Authentifizierung im KDC erfolgt durch die Ausstellu ng von Authentif

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			izierungstickets. Das KDC unterhält eine Datenbank der Prinzipale in seinem Bereich mit ihren Passwörtern und anderen administrativen Informationen zu jedem Prinzipal.
AC.L1-3.1.1	Beschränken Sie den Zugriff auf Informationssysteme auf autorisierte Benutzer, Prozesse von autorisierten Benutzern oder Geräte (einschließlich anderer Informationssysteme).	emr-master-no-public-ip	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon EMR-Cluster-Masterknoten nicht öffentlich zugänglich sind. Amazon-EMR-Cluster-Hauptknoten können vertrauliche Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC.L1-3.1.1	Beschränken Sie den Zugriff auf Informationssystem e auf autorisierte Benutzer, Prozesse von autorisierten Benutzern oder Geräte (einschließlich anderer Informati onssysteme).	iam-customer-policy-blocked-kms-Aktionen	AWS Identity and Access Managemen t (IAM) kann Ihnen helfen, die Prinzipien der geringsten Rechte und der Aufgabent rennung in Zugriffsb erechtigungen und Autorisierungen zu integrieren und so zu verhindern, dass Richtlinien blockiert e Aktionen für alle AWS Schlüssel des Key Management Service enthalten. Wenn Benutzer mehr Rechte haben, als für die Ausführun g einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringste n Berechtigung und Aufgabentrennung verstoßen. Mit dieser Regel können Sie den Parameter festlegen. blockedAc tionsPatterns (Wert „AWS Bewährte grundlegende Sicherheitsmethode

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			n“: kms: Entschlüs seln, kms:ReEnc ryptFrom). Die tatsächlichen Werte müssen den Richtlini en Ihrer Organisation entsprechen.
AC.L1-3.1.1	Beschränken Sie den Zugriff auf Informationssystem e auf autorisierte Benutzer, Prozesse von autorisierten Benutzern oder Geräte (einschließlich anderer Informati onssysteme).	iam-group-has-users-überprüfen	AWS Identity and Access Managemen t (IAM) kann Ihnen helfen, die Prinzipien der geringsten Rechte und der Aufgabent rennung mit Zugriffsb erechtigungen und Autorisierungen zu integrieren, indem sichergestellt wird, dass IAM-Gruppen mindestens einen Benutzer haben. Die Einteilung von Benutzern in Gruppen auf der Grundlage der ihnen zugewiese nen Berechtigungen oder ihrer Funktion ist eine Möglichkeit, das Prinzip der geringste n Berechtigung zu implementieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC.L1-3.1.1	Beschränken Sie den Zugriff auf Informationssystem e auf autorisierte Benutzer, Prozesse von autorisierten Benutzern oder Geräte (einschließlich anderer Informati onssysteme).	iam-inline-policy-blocked-kms-Aktionen	Stellen Sie sicher, dass ein Benutzer, eine IAM-Rolle oder eine IAM-Gruppe (AWS Identity and Access Management) nicht über eine Inline-Richtlinie verfügt, die blockierte Aktionen für alle AWS Schlüssel des Key Management Service zulässt. AWS empfiehlt, verwaltet e Richtlinien anstelle von Inline-Richtlinien zu verwenden. Verwaltete Richtlini en ermöglichen Wiederverwendbarke it, Versionsverwaltung , Rollback und Delegierung der Berechtigungsverwa ltung. Mit dieser Regel können Sie den blockedActionsPatt erns Parameter festlegen. (Wert „AWS Bewährte grundlegende Sicherheitsmethode n“: kms: Entschlüs seln, kms:ReEnc

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			ryptFrom). Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.
AC.L1-3.1.1	Beschränken Sie den Zugriff auf Informationssysteme auf autorisierte Benutzer, Prozesse von autorisierten Benutzern oder Geräte (einschließlich anderer Informationssysteme).	iam-no-inline-policy-überprüfen	Stellen Sie sicher, dass ein Benutzer, eine IAM-Rolle oder eine IAM-Gruppe (AWS Identity and Access Management) nicht über eine Inline-Richtlinie zur Zugriffskontrolle auf Systeme und Ressourcen verfügt. AWS empfiehlt, verwaltete Richtlinien anstelle von Inline-Richtlinien zu verwenden. Verwaltete Richtlinien ermöglichen Wiederverwendbarkeit, Versionsverwaltung, Rollback und Delegierung der Berechtigungsverwaltung.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC.L1-3.1.1	Beschränken Sie den Zugriff auf Informationssystem e auf autorisierte Benutzer, Prozesse von autorisierten Benutzern oder Geräte (einschließlich anderer Informati onssysteme).	iam-policy-no-stat ements-with-admin-access	AWS Identity and Access Managemen t (IAM) kann Ihnen dabei helfen, die Prinzipien der geringsten Rechte und der Aufgabent rennung in Zugriffsb erechtigungen und Autorisierungen zu integrieren und so zu verhindern, dass Richtlinien „Effect“: „Allow“ mit „Action“: „*“ anstelle von „Resource“: „*“ enthalten. Wenn Benutzern mehr Rechte eingeräum t werden, als für die Ausführung einer Aufgabe erforderl ich sind, kann dies gegen das Prinzip der geringsten Berechtigung und der Aufgabentrennung verstoßen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC.L1-3.1.1	Beschränken Sie den Zugriff auf Informationssysteme auf autorisierte Benutzer, Prozesse von autorisierten Benutzern oder Geräte (einschließlich anderer Informationssysteme).	iam-policy-no-statements-with-full-access	Stellen Sie sicher, dass IAM-Aktionen nur auf die benötigten Aktionen beschränkt sind. Wenn Benutzern mehr Rechte eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und der Aufgabentrennung verstoßen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC.L1-3.1.1	Beschränken Sie den Zugriff auf Informationssystem e auf autorisierte Benutzer, Prozesse von autorisierten Benutzern oder Geräte (einschließlich anderer Informati onssysteme).	iam-root-access-key-überprüfen	Der Zugriff auf Systeme und Ressourcen kann gesteuert werden, indem überprüft wird, ob der Root-Benu tzer keine Zugriffss chlüssel mit seiner AWS Identity and Access Management (IAM) -Rolle verknüpft hat. Stellen Sie sicher, dass die Root-Zugr iffsschlüssel gelöscht werden. Erstellen und verwenden Sie stattdessen rollenbas ierte Funktionen, AWS-Konten um das Prinzip der geringste n Funktionalität zu berücksichtigen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC.L1-3.1.1	Beschränken Sie den Zugriff auf Informationssystem e auf autorisierte Benutzer, Prozesse von autorisierten Benutzern oder Geräte (einschließlich anderer Informati onssysteme).	iam-user-group-mem bership-überprüfen	AWS Identity and Access Managemen t (IAM) kann Ihnen helfen, Zugriffsb erechtigungen und Autorisierungen einzuschränken, indem sichergestellt wird, dass Benutzer Mitglieder mindesten s einer Gruppe sind. Wenn Benutzern mehr Berechtigungen eingeräumt werden, als für die Ausführun g einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringste n Berechtigung und Aufgabentrennung verstoßen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC.L1-3.1.1	Beschränken Sie den Zugriff auf Informationssystem e auf autorisierte Benutzer, Prozesse von autorisierten Benutzern oder Geräte (einschließlich anderer Informati onssysteme).	iam-user-mfa-enabled	Aktivieren Sie diese Regel, um den Zugriff auf Ressourcen in der AWS Cloud einzuschr änken. Diese Regel sorgt dafür, dass die Multi-Faktor-Authe ntifizierung (MFA) für alle Benutzer aktiviert ist. MFA sorgt für eine weitere Schutzebe ne zusätzlich zu den Anmeldeinformation en. Reduzieren Sie Fälle von kompromit tierten Konten, indem Sie MFA für Benutzer vorschreiben.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC.L1-3.1.1	Beschränken Sie den Zugriff auf Informationssystem e auf autorisierte Benutzer, Prozesse von autorisierten Benutzern oder Geräte (einschließlich anderer Informati onssysteme).	iam-user-no-policies-überprüfen	Diese Regel stellt sicher, dass AWS Identity and Access Management (IAM) -Richtlinien nur Gruppen oder Rollen zugewiese n werden, um den Zugriff auf Systeme und Ressourcen zu kontrollieren. Die Zuweisung von Berechtig ungen auf Gruppen- oder Rollenebene trägt dazu bei, die Wahrscheinlichkeit zu verringern, dass eine Identität übermäßige Berechtigungen erhält oder beibehält.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC.L1-3.1.1	Beschränken Sie den Zugriff auf Informationssysteme auf autorisierte Benutzer, Prozesse von autorisierten Benutzern oder Geräte (einschließlich anderer Informationssysteme).	iam-user-unused-credentials-überprüfen	AWS Identity and Access Management (IAM) kann Ihnen bei Zugriffsberechtigungen und Autorisierungen helfen, indem es nach IAM-Passwörtern und Zugriffsschlüsseln sucht, die für einen bestimmten Zeitraum nicht verwendet wurden. Wenn ungenutzte Anmeldeinformationen identifiziert werden, müssen Sie sie deaktivieren und/oder entfernen, da dies gegen das Prinzip der geringsten Berechtigung verstoßen könnte. Für diese Regel müssen Sie einen Wert für das maxCredentialUsage Alter festlegen (Standardkonfiguration: 90). Der tatsächliche Wert muss den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC.L1-3.1.1	Beschränken Sie den Zugriff auf Informationssystem e auf autorisierte Benutzer, Prozesse von autorisierten Benutzern oder Geräte (einschließlich anderer Informati onssysteme).	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) Security Groups können bei der Verwaltung des Netzwerkzugriffs helfen, indem sie eine statusbeh aftete Filterung von eingehendem und ausgehendem Netzwerkverkehr zu Ressourcen bereitste llen. AWS Wenn Sie eingehenden (oder entfernten) Datenverk ehr von 0.0.0.0/0 bis Port 22 auf Ihren Ressourcen nicht zulassen, können Sie den Remote-Zugriff einschränken.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC.L1-3.1.1	Beschränken Sie den Zugriff auf Informationssystem e auf autorisierte Benutzer, Prozesse von autorisierten Benutzern oder Geräte (einschließlich anderer Informati onssysteme).	ec-2 instances-in-vpc	Stellen Sie Amazon Elastic Compute Cloud (Amazon EC2) -Instances innerhalb einer Amazon Virtual Private Cloud (Amazon VPC) bereit, um eine sichere Kommunika tion zwischen einer Instance und anderen Services innerhalb der Amazon VPC zu ermöglichen, ohne dass ein Internet-Gateway, ein NAT-Gerät oder eine VPN-Verbindung erforderlich ist. Der gesamte Datenverk ehr bleibt sicher in der AWS Cloud. Domains, die sich innerhalb einer VPC befinden, verfügen aufgrund ihrer logischen Isolierun g im Vergleich zu Domains mit öffentlic hen Endpunkten über eine zusätzlic he Sicherheitsebene. Weisen Sie EC2

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			Amazon-Instances einer Amazon-VPC zu, um den Zugriff ordnungsgemäß zu verwalten.
AC.L1-3.1.1	Beschränken Sie den Zugriff auf Informationssysteme auf autorisierte Benutzer, Prozesse von autorisierten Benutzern oder Geräte (einschließlich anderer Informationssysteme).	internet-gateway-authorized-vpc-nur	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Internet-Gateways nur mit autorisierter Amazon Virtual Private Cloud (Amazon VPC) verbunden sind. Internet-Gateways ermöglichen den bidirektionalen Internetzugang zur und von der Amazon VPC, was möglicherweise zu einem unbefugten Zugriff auf Amazon-VPC-Ressourcen führen kann.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC.L1-3.1.1	Beschränken Sie den Zugriff auf Informationssysteme auf autorisierte Benutzer, Prozesse von autorisierten Benutzern oder Geräte (einschließlich anderer Informationssysteme).	lambda-function-public-access-verboten	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass AWS Lambda-Funktionen nicht öffentlich zugänglich sind. Der öffentliche Zugriff kann möglicherweise die Verfügbarkeit von Ressourcen beeinträchtigen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC.L1-3.1.1	Beschränken Sie den Zugriff auf Informationssystem e auf autorisierte Benutzer, Prozesse von autorisierten Benutzern oder Geräte (einschließlich anderer Informati onssysteme).	lambda-inside-vpc	Stellen Sie AWS Lambda-Funktionen in einer Amazon Virtual Private Cloud (Amazon VPC) bereit, um eine sichere Kommunika tion zwischen einer Funktion und anderen Diensten innerhalb der Amazon VPC zu gewährleisten. Bei dieser Konfiguration sind kein Internet-Gateway, kein NAT-Gerät und keine VPN-Verbindung erforderlich. Der gesamte Datenverk ehr bleibt sicher in der Cloud. AWS Domains, die sich innerhalb einer VPC befinden, verfügen aufgrund ihrer logischen Isolierun g im Vergleich zu Domains mit öffentlic hen Endpunkten über eine zusätzliche Sicherheitsebene. Um den Zugriff ordnungsg emäß zu verwalten,

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			sollten AWS Lambda-Funktionen einer VPC zugewiesen werden.
AC.L1-3.1.1	Beschränken Sie den Zugriff auf Informationssystem e auf autorisierte Benutzer, Prozesse von autorisierten Benutzern oder Geräte (einschließlich anderer Informati onssysteme).	mfa-enabled-for-iam-Konsolenzugriff	Verwalten Sie den Zugriff auf Ressource n in der AWS Cloud, indem Sie sicherste llen, dass MFA für alle AWS Identity and Access Managemen t (IAM) -Benutzer aktiviert ist, die über ein Konsolenk ennwort verfügen. MFA sorgt für eine weitere Schutzebe ne zusätzlich zu den Anmeldeinformation en. Indem Sie MFA für Benutzer vorschrei ben, können Sie Fälle kompromittierter Konten reduzieren und verhindern, dass unbefugte Benutzer auf vertrauliche Daten zugreifen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC.L1-3.1.1	Beschränken Sie den Zugriff auf Informationssystem e auf autorisierte Benutzer, Prozesse von autorisierten Benutzern oder Geräte (einschließlich anderer Informati onssysteme).	rds-instance-public-access-überprüfen	Verwalten Sie den Zugriff auf Ressource n in der AWS Cloud, indem Sie sicherste llen, dass Amazon Relational Database Service (Amazon RDS) -Instance s nicht öffentlic h sind. Amazon-RDS-Datenbank-Instances können vertrauliche Informati onen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC.L1-3.1.1	Beschränken Sie den Zugriff auf Informationssystem e auf autorisierte Benutzer, Prozesse von autorisierten Benutzern oder Geräte (einschließlich anderer Informati onssysteme).	rds-snapshots-public-prohibited	Verwalten Sie den Zugriff auf Ressource n in der AWS Cloud, indem Sie sicherste llen, dass Amazon Relational Database Service (Amazon RDS) -Instance s nicht öffentlic h sind. Amazon-RDS-Datenbank-Instances können vertrauliche Informati onen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC.L1-3.1.1	Beschränken Sie den Zugriff auf Informationssystem e auf autorisierte Benutzer, Prozesse von autorisierten Benutzern oder Geräte (einschließlich anderer Informati onssysteme).	redshift-cluster-public-access-überprüfen	Verwalten Sie den Zugriff auf Ressource n in der AWS Cloud, indem Sie sicherste llen, dass Amazon Redshift Redshift-Cluster nicht öffentlic h sind. Amazon-Re dshift-Cluster können vertrauliche Informati onen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC.L1-3.1.1	Beschränken Sie den Zugriff auf Informationssystem e auf autorisierte Benutzer, Prozesse von autorisierten Benutzern oder Geräte (einschließlich anderer Informati onssysteme).	restricted-common-ports	Verwalten Sie den Zugriff auf Ressource n in der AWS Cloud, indem Sie sicherste llen, dass gemeinsam e Ports für Amazon Elastic Compute Cloud (Amazon EC2) -Sicherhe itsgruppen eingeschr änkt sind. Wenn der Zugriff auf Ports nicht auf vertrauen swürdige Quellen beschränkt wird, kann dies zu Angriffen auf die Verfügbar keit, Integrität und Vertraulichkeit von Systemen führen. Mit dieser Regel können Sie optional die Parameter blockedPo rt1–blockedPort5 festlegen (Standard konfigurationen: 20, 21, 3389, 3306, 4333). Die tatsächli chen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC.L1-3.1.1	Beschränken Sie den Zugriff auf Informationssysteme auf autorisierte Benutzer, Prozesse von autorisierten Benutzern oder Geräte (einschließlich anderer Informationssysteme).	root-account-hardware-mfa-aktiviert	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Hardware-MFA für den Root-Benutzer aktiviert ist. Der Stammbenutzer ist der AWS-Konto-Benutzer mit den meisten Berechtigungen. MFA sorgt für eine weitere Schutzebene zusätzlich zu den Anmeldeinformationen. Indem Sie MFA für den Root-Benutzer vorschreiben, können Sie die Anzahl AWS-Konten kompromittierter Benutzer reduzieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC.L1-3.1.1	Beschränken Sie den Zugriff auf Informationssysteme auf autorisierte Benutzer, Prozesse von autorisierten Benutzern oder Geräte (einschließlich anderer Informationssysteme).	root-account-mfa-enabled	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass MFA für den Root-Benutzer aktiviert ist. Der Stammbenutzer ist der AWS-Konto-Benutzer mit den meisten Berechtigungen. MFA sorgt für eine weitere Schutzebene zusätzlich zu den Anmeldeinformationen. Indem Sie MFA für den Root-Benutzer vorschreiben, können Sie die Anzahl AWS-Konten kompromittierter Benutzer reduzieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC.L1-3.1.1	Beschränken Sie den Zugriff auf Informationssystem e auf autorisierte Benutzer, Prozesse von autorisierten Benutzern oder Geräte (einschließlich anderer Informati onssysteme).	s3- -blöcke-periodisch account-level-public-access	Verwalten Sie den Zugriff auf Ressource n in der AWS Cloud, indem Sie sicherste llen, dass Amazon Simple Storage Service (Amazon S3) -Buckets nicht öffentlich zugänglic h sind. Diese Regel trägt dazu bei, sensible Daten vor unbefugten Remote-Benutzern zu schützen, indem sie den öffentlichen Zugriff verhinder t. Mit dieser Regel können Sie optional die Parameter ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) und restrictPublicBuck ets Parameter (Config Default: True) festlegen. Die tatsächlichen Werte müssen den Richtlini

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			en Ihrer Organisation entsprechen.
AC.L1-3.1.1	Beschränken Sie den Zugriff auf Informationssystem e auf autorisierte Benutzer, Prozesse von autorisierten Benutzern oder Geräte (einschließlich anderer Informati onssysteme).	s3 bucket-level-public-access - verboten	Verwalten Sie den Zugriff auf Ressource n in der AWS Cloud, indem Sie sicherste llen, dass Amazon Simple Storage Service (Amazon S3) -Buckets nicht öffentlich zugänglic h sind. Diese Regel trägt dazu bei, sensible Daten vor unbefugten Remote-Benutzern zu schützen, indem sie den öffentlichen Zugriff auf Bucket-Eb ene verhindert.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC.L1-3.1.1	Beschränken Sie den Zugriff auf Informationssysteme auf autorisierte Benutzer, Prozesse von autorisierten Benutzern oder Geräte (einschließlich anderer Informationssysteme).	s-3 bucket-policy-grantee-check	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie s3_bucket_policy_grantee_check aktivieren. Diese Regel prüft, ob der vom Amazon S3 S3-Bucket gewährte Zugriff durch die von Ihnen bereitgestellten AWS Principals, Verbundbenutzer, Service Principals, IP-Adressen oder Amazon Virtual Private Cloud (Amazon VPC) IDs eingeschränkt ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC.L1-3.1.1	Beschränken Sie den Zugriff auf Informationssystem e auf autorisierte Benutzer, Prozesse von autorisierten Benutzern oder Geräte (einschließlich anderer Informati onssysteme).	s-3 bucket-public-read -prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie nur autorisierten Benutzern, Prozessen und Geräten Zugriff auf Amazon Simple Storage Service (Amazon S3) - Buckets gewähren. Die Verwaltung des Zugriffs sollte mit der Klassifizierung der Daten übereinst immen.
AC.L1-3.1.1	Beschränken Sie den Zugriff auf Informationssystem e auf autorisierte Benutzer, Prozesse von autorisierten Benutzern oder Geräte (einschließlich anderer Informati onssysteme).	s3- bucket-public-writ e-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie nur autorisierten Benutzern, Prozessen und Geräten Zugriff auf Amazon Simple Storage Service (Amazon S3) - Buckets gewähren. Die Verwaltung des Zugriffs sollte mit der Klassifizierung der Daten übereinst immen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC.L1-3.1.1	Beschränken Sie den Zugriff auf Informationssystem e auf autorisierte Benutzer, Prozesse von autorisierten Benutzern oder Geräte (einschließlich anderer Informati onssysteme).	sagemaker-notebook -no-direct-Interne tzugang	Verwalten Sie den Zugriff auf Ressource n in der AWS Cloud, indem Sie sicherste llen, dass SageMaker Amazon-Notebooks keinen direkten Internetzugang zulassen. Indem Sie direkten Internetz ugang blockieren, vermeiden Sie, dass unbefugte Benutzer auf sensible Daten zugreifen.
AC.L1-3.1.1	Beschränken Sie den Zugriff auf Informationssystem e auf autorisierte Benutzer, Prozesse von autorisierten Benutzern oder Geräte (einschließlich anderer Informati onssysteme).	secretsmanager-rot ation-enabled-check	Diese Regel stellt sicher, dass bei AWS Secrets Manager Manager-Geheimnissen die Rotation aktiviert ist. Die regelmäßige Rotation von Secrets kann den Zeitraum verkürzen, in dem ein Secret aktiv ist, und möglicherweise die Auswirkungen auf das Unternehmen verringern, falls das Secret kompromittiert wird.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC.L1-3.1.1	Beschränken Sie den Zugriff auf Informationssysteme auf autorisierte Benutzer, Prozesse von autorisierten Benutzern oder Geräte (einschließlich anderer Informationssysteme).	secretsmanager-scheduled-rotation-success-überprüfen	Diese Regel stellt sicher, dass AWS Secrets Manager Manager-Geheimnisse gemäß dem Rotationsplan erfolgreich rotiert wurden. Die regelmäßige Rotation von Secrets kann den Zeitraum verkürzen, in dem ein Secret aktiv ist, und möglicherweise die Auswirkungen auf das Unternehmen verringern, falls es kompromittiert wird.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC.L1-3.1.1	Beschränken Sie den Zugriff auf Informationssystem e auf autorisierte Benutzer, Prozesse von autorisierten Benutzern oder Geräte (einschließlich anderer Informati onssysteme).	ssm-document-not-p ublic	Stellen Sie sicher, dass AWS Systems Manager (SSM) - Dokumente nicht öffentlich sind, da dies einen unbeabsic htigten Zugriff auf Ihre SSM-Dokum ente ermöglichen kann. Ein öffentlic hes SSM-Dokum ent kann Informati onen über Ihr Konto, Ihre Ressourcen und internen Prozesse preisgeben.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC.L1-3.1.1	Beschränken Sie den Zugriff auf Informationssystem e auf autorisierte Benutzer, Prozesse von autorisierten Benutzern oder Geräte (einschließlich anderer Informati onssysteme).	vpc-default-security-group-geschlossen	Sicherheitsgruppen von Amazon Elastic Compute Cloud (Amazon EC2) können bei der Verwaltung des Netzwerkzugriffs helfen, indem sie eine statusbehaftete Filterung des ein- und ausgehenden Netzwerkverkehrs zu Ressourcen bereitstellen. AWS Die Beschränk ung des gesamten Datenverkehrs auf die Standardsicherheit sgruppe hilft dabei, den Fernzugriff auf Ihre Ressourcen einzuschränken. AWS

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC.L1-3.1.1	Beschränken Sie den Zugriff auf Informationssystem e auf autorisierte Benutzer, Prozesse von autorisierten Benutzern oder Geräte (einschließlich anderer Informati onssysteme).	vpc-sg-open-only-to-authorized-ports	Verwalten Sie den Zugriff auf Ressource n in der AWS Cloud, indem Sie sicherste llen, dass gemeinsam e Ports für Amazon Elastic Compute Cloud (Amazon EC2) -Sicherhe itsgruppen eingeschr ränkt sind. Wenn der Zugriff auf Ports nicht auf vertrauen swürdige Quellen beschränkt wird, kann dies zu Angriffen auf die Verfügbar keit, Integrität und Vertraulichkeit von Systemen führen. Durch die Beschränk ung des Zugriffs auf Ressourcen innerhalb einer Sicherhei tsgruppe aus dem Internet (0.0.0.0/0) kann der Remote-Zugriff auf interne Systeme gesteuert werden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC.L1-3.1.1	Beschränken Sie den Zugriff auf Informationssystem e auf autorisierte Benutzer, Prozesse von autorisierten Benutzern oder Geräte (einschließlich anderer Informati onssysteme).	opensearch-in-vpc-only	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass sich Amazon OpenSearch Service-Domains innerhalb einer Amazon Virtual Private Cloud (Amazon VPC) befinden. Eine Amazon OpenSearc h Service-Domain innerhalb einer Amazon VPC ermöglicht die sichere Kommunikation zwischen Amazon OpenSearch Service und anderen Services innerhalb der Amazon VPC, ohne dass ein Internet-Gateway, ein NAT-Gerät oder eine VPN-Verbindung erforderlich ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC.L1-3.1.2	Beschränken Sie den Zugriff auf das Informationssystem auf jene Transaktionen und Funktionen, die autorisierte Benutzer ausführen dürfen.	dms-replication-not-public	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass auf DMS-Replikationsinstanzen nicht öffentlich zugegriffen werden kann. DMS-Replikations-Instances können vertrauliche Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.
AC.L1-3.1.2	Beschränken Sie den Zugriff auf das Informationssystem auf jene Transaktionen und Funktionen, die autorisierte Benutzer ausführen dürfen.	ebs-snapshot-public-restorable-überprüfen	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass EBS-Snapshots nicht öffentlich wiederherstellbar sind. EBS-Volume-Snapshots können vertrauliche Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC.L1-3.1.2	Beschränken Sie den Zugriff auf das Informationssystem auf jene Transaktionen und Funktionen, die autorisierte Benutzer ausführen dürfen.	ec2-imdsv2-check	Stellen Sie sicher, dass die Methode Instance Metadata Service Version 2 (IMDSv2) aktiviert ist, um den Zugriff auf und die Kontrolle der Amazon Elastic Compute Cloud (Amazon EC2) - Instance-Metadaten zu schützen. Die IMDSv2 Methode verwendet sitzungsbasierte Kontrollen. Mit können Kontrollen implementiert werden IMDSv2, um Änderungen an Instanzmetadaten einzuschränken.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC.L1-3.1.2	Beschränken Sie den Zugriff auf das Informationssystem auf jene Transaktionen und Funktionen, die autorisierte Benutzer ausführen dürfen.	ec-2 instance-no-public-ip	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon Elastic Compute Cloud (Amazon EC2) - Instances nicht öffentlich zugänglich sind. EC2 Amazon-Instances können vertrauliche Informationen enthalten, und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC.L1-3.1.2	Beschränken Sie den Zugriff auf das Informationssystem auf jene Transaktionen und Funktionen, die autorisierte Benutzer ausführen dürfen.	elasticsearch-in-vpc-only	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass sich Amazon OpenSearch OpenSearch Service (Service) - Domains innerhalb einer Amazon Virtual Private Cloud (Amazon VPC) befinden. Eine OpenSearch Service-Domain innerhalb einer Amazon VPC ermöglicht die sichere Kommunikation zwischen OpenSearch Service und anderen Services innerhalb der Amazon VPC, ohne dass ein Internet-Gateway, ein NAT-Gerät oder eine VPN-Verbindung erforderlich ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC.L1-3.1.2	Beschränken Sie den Zugriff auf das Informationssystem auf jene Transaktionen und Funktionen, die autorisierte Benutzer ausführen dürfen.	emr-kerberos-enabled	Die Zugriffsberechtigungen und -autorisierungen können verwaltet und nach den Prinzipien der geringsten Berechtigung und Aufgabentrennung integriert werden, indem Kerberos für Amazon-EMR-Cluster aktiviert wird. In Kerberos werden Services und Benutzer, die sich authentifizieren müssen, als Prinzipale bezeichnet. Prinzipale befinden sich in einem Kerberos-Bereich. Innerhalb dieses Bereichs wird ein Kerberos-Server als Key Distribution Center (KDC) bezeichnet. Über diesen Server können sich Prinzipale authentifizieren. Die Authentifizierung im KDC erfolgt durch die Ausstellung von Authentif

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			izierungstickets. Das KDC unterhält eine Datenbank der Prinzipale in seinem Bereich mit ihren Passwörtern und anderen administrativen Informationen zu jedem Prinzipal.
AC.L1-3.1.2	Beschränken Sie den Zugriff auf das Informationssystem auf jene Transaktionen und Funktionen, die autorisierte Benutzer ausführen dürfen.	emr-master-no-public-ip	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon EMR-Cluster-Masterknoten nicht öffentlich zugänglich sind. Amazon-EMR-Cluster-Hauptknoten können vertrauliche Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC.L1-3.1.2	Beschränken Sie den Zugriff auf das Informationssystem auf jene Transaktionen und Funktionen, die autorisierte Benutzer ausführen dürfen.	iam-no-inline-policy-überprüfen	Stellen Sie sicher, dass ein Benutzer, eine IAM-Rolle oder eine IAM-Gruppe (AWS Identity and Access Management) nicht über eine Inline-Richtlinie zur Zugriffskontrolle auf Systeme und Ressourcen verfügt. AWS empfiehlt, verwaltete Richtlinien anstelle von Inline-Richtlinien zu verwenden. Verwaltete Richtlinien ermöglichen Wiederverwendbarkeit, Versionsverwaltung, Rollback und Delegierung der Berechtigungsverwaltung.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC.L1-3.1.2	Beschränken Sie den Zugriff auf das Informationssystem auf jene Transaktionen und Funktionen, die autorisierte Benutzer ausführen dürfen.	iam-password-policy	Die Identitäten und Anmeldeinformationen werden auf der Grundlage einer organisatorischen IAM-Passwortrichtlinie ausgestellt, verwaltet und verifiziert. Sie erfüllen oder übertreffen die Anforderungen von NIST SP 800-63 und dem Standard „Best Practices“ von AWS Foundational Security für die Passwortstärke. Mit dieser Regel können Sie optional RequireUppercaseCharacters (Wert für AWS grundlegende Sicherheitsbewährte Methoden: wahr), RequireLowercaseCharacters (Wert für bewährte Methoden für AWS grundlegende Sicherheit: wahr), RequireSymbols (Wert für bewährte Methoden für AWS grundlegende Sicherheit:

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			wahr), RequireNumbers (Wert für bewährte Methoden für AWS grundlegende Sicherheit: wahr), MinimumPasswordLength (Wert für bewährte Methoden für AWS grundlegende Sicherheit: 14), PasswordReusePrevention (Wert für bewährte Methoden für AWS grundlegende Sicherheit: 24) und MaxPasswordAge (Wert für bewährte Methoden für AWS grundlegende Sicherheit: 90) für Ihr IAM festlegen Kennwortrichtlinie. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC.L1-3.1.2	Beschränken Sie den Zugriff auf das Informationssystem auf jene Transaktionen und Funktionen, die autorisierte Benutzer ausführen dürfen.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) kann Ihnen dabei helfen, die Prinzipien der geringsten Rechte und der Aufgabentrennung in Zugriffsberechtigungen und Autorisierungen zu integrieren und so zu verhindern, dass Richtlinien „Effect“: „Allow“ mit „Action“: „*“ anstelle von „Resource“: „*“ enthalten. Wenn Benutzern mehr Rechte eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und der Aufgabentrennung verstoßen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC.L1-3.1.2	Beschränken Sie den Zugriff auf das Informationssystem auf jene Transaktionen und Funktionen, die autorisierte Benutzer ausführen dürfen.	iam-root-access-key-überprüfen	Der Zugriff auf Systeme und Ressourcen kann gesteuert werden, indem überprüft wird, ob der Root-Benutzer keine Zugriffsschlüssel mit seiner AWS Identity and Access Management (IAM) -Rolle verknüpft hat. Stellen Sie sicher, dass die Root-Zugriffsschlüssel gelöscht werden. Erstellen und verwenden Sie stattdessen rollenbasierte Funktionen, AWS-Konten um das Prinzip der geringsten Funktionalität zu berücksichtigen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC.L1-3.1.2	Beschränken Sie den Zugriff auf das Informationssystem auf jene Transaktionen und Funktionen, die autorisierte Benutzer ausführen dürfen.	iam-user-group-membership-überprüfen	AWS Identity and Access Management (IAM) kann Ihnen helfen, Zugriffsberechtigungen und Autorisierungen einzuschränken, indem sichergestellt wird, dass Benutzer Mitglieder mindestens einer Gruppe sind. Wenn Benutzern mehr Berechtigungen eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und Aufgabentrennung verstoßen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC.L1-3.1.2	Beschränken Sie den Zugriff auf das Informationssystem auf jene Transaktionen und Funktionen, die autorisierte Benutzer ausführen dürfen.	iam-user-mfa-enabled	Aktivieren Sie diese Regel, um den Zugriff auf Ressourcen in der AWS Cloud einzuschränken. Diese Regel sorgt dafür, dass die Multi-Faktor-Authentifizierung (MFA) für alle Benutzer aktiviert ist. MFA sorgt für eine weitere Schutzebene zusätzlich zu den Anmeldeinformationen. Reduzieren Sie Fälle von kompromittierten Konten, indem Sie MFA für Benutzer vorschreiben.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC.L1-3.1.2	Beschränken Sie den Zugriff auf das Informationssystem auf jene Transaktionen und Funktionen, die autorisierte Benutzer ausführen dürfen.	iam-user-no-policies-überprüfen	Diese Regel stellt sicher, dass AWS Identity and Access Management (IAM)-Richtlinien nur Gruppen oder Rollen zugewiesen werden, um den Zugriff auf Systeme und Ressourcen zu kontrollieren. Die Zuweisung von Berechtigungen auf Gruppen- oder Rollenebene trägt dazu bei, die Wahrscheinlichkeit zu verringern, dass eine Identität übermäßige Berechtigungen erhält oder beibehält.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC.L1-3.1.2	Beschränken Sie den Zugriff auf das Informationssystem auf jene Transaktionen und Funktionen, die autorisierte Benutzer ausführen dürfen.	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) Security Groups können bei der Verwaltung des Netzwerkzugriffs helfen, indem sie eine statusbehaftete Filterung von eingehendem und ausgehendem Netzwerkverkehr zu Ressourcen bereitstellen. AWS Wenn Sie eingehenden (oder entfernten) Datenverkehr von 0.0.0.0/0 bis Port 22 auf Ihren Ressourcen nicht zulassen, können Sie den Remote-Zugriff einschränken.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC.L1-3.1.2	Beschränken Sie den Zugriff auf das Informationssystem auf jene Transaktionen und Funktionen, die autorisierte Benutzer ausführen dürfen.	ec-2 instances-in-vpc	Stellen Sie Amazon Elastic Compute Cloud (Amazon EC2) -Instances innerhalb einer Amazon Virtual Private Cloud (Amazon VPC) bereit, um eine sichere Kommunikation zwischen einer Instance und anderen Services innerhalb der Amazon VPC zu ermöglichen, ohne dass ein Internet-Gateway, ein NAT-Gerät oder eine VPN-Verbindung erforderlich ist. Der gesamte Datenverkehr bleibt sicher in der AWS Cloud. Domains, die sich innerhalb einer VPC befinden, verfügen aufgrund ihrer logischen Isolierung im Vergleich zu Domains mit öffentlichen Endpunkten über eine zusätzliche Sicherheitsebene. Weisen Sie EC2

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			Amazon-Instances einer Amazon-VPC zu, um den Zugriff ordnungsgemäß zu verwalten.
AC.L1-3.1.2	Beschränken Sie den Zugriff auf das Informationssystem auf jene Transaktionen und Funktionen, die autorisierte Benutzer ausführen dürfen.	internet-gateway-authorized-vpc-nur	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Internet-Gateways nur mit autorisierter Amazon Virtual Private Cloud (Amazon VPC) verbunden sind. Internet-Gateways ermöglichen den bidirektionalen Internetzugang zur und von der Amazon VPC, was möglicherweise zu einem unbefugten Zugriff auf Amazon-VPC-Ressourcen führen kann.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC.L1-3.1.2	Beschränken Sie den Zugriff auf das Informationssystem auf jene Transaktionen und Funktionen, die autorisierte Benutzer ausführen dürfen.	lambda-function-public-access-verboten	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass AWS Lambda-Funktionen nicht öffentlich zugänglich sind. Der öffentliche Zugriff kann möglicherweise die Verfügbarkeit von Ressourcen beeinträchtigen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC.L1-3.1.2	Beschränken Sie den Zugriff auf das Informationssystem auf jene Transaktionen und Funktionen, die autorisierte Benutzer ausführen dürfen.	lambda-inside-vpc	Stellen Sie AWS Lambda-Funktionen in einer Amazon Virtual Private Cloud (Amazon VPC) bereit, um eine sichere Kommunikation zwischen einer Funktion und anderen Diensten innerhalb der Amazon VPC zu gewährleisten. Bei dieser Konfiguration sind kein Internet-Gateway, kein NAT-Gerät und keine VPN-Verbindung erforderlich. Der gesamte Datenverkehr bleibt sicher in der Cloud. AWS Domains, die sich innerhalb einer VPC befinden, verfügen aufgrund ihrer logischen Isolierung im Vergleich zu Domains mit öffentlichen Endpunkten über eine zusätzliche Sicherheitsebene. Um den Zugriff ordnungsgemäß zu verwalten,

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			sollten AWS Lambda-Funktionen einer VPC zugewiesen werden.
AC.L1-3.1.2	Beschränken Sie den Zugriff auf das Informationssystem auf jene Transaktionen und Funktionen, die autorisierte Benutzer ausführen dürfen.	mfa-enabled-for-iam-Konsolenzugriff	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass MFA für alle AWS Identity and Access Management (IAM) -Benutzer aktiviert ist, die über ein Konsolenkennwort verfügen. MFA sorgt für eine weitere Schutzebene zusätzlich zu den Anmeldeinformationen. Indem Sie MFA für Benutzer vorschreiben, können Sie Fälle kompromittierter Konten reduzieren und verhindern, dass unbefugte Benutzer auf vertrauliche Daten zugreifen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC.L1-3.1.2	Beschränken Sie den Zugriff auf das Informationssystem auf jene Transaktionen und Funktionen, die autorisierte Benutzer ausführen dürfen.	rds-instance-public-access-überprüfen	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Relational Database Service (Amazon RDS) -Instances nicht öffentlich sind. Amazon-RDS-Datenbank-Instances können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC.L1-3.1.2	Beschränken Sie den Zugriff auf das Informationssystem auf jene Transaktionen und Funktionen, die autorisierte Benutzer ausführen dürfen.	rds-snapshots-public-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Relational Database Service (Amazon RDS) -Instances nicht öffentlich sind. Amazon-RDS-Datenbank-Instances können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC.L1-3.1.2	Beschränken Sie den Zugriff auf das Informationssystem auf jene Transaktionen und Funktionen, die autorisierte Benutzer ausführen dürfen.	redshift-cluster-public-access-überprüfen	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Redshift Redshift-Cluster nicht öffentlich sind. Amazon-Redshift-Cluster können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC.L1-3.1.2	Beschränken Sie den Zugriff auf das Informationssystem auf jene Transaktionen und Funktionen, die autorisierte Benutzer ausführen dürfen.	restricted-common-ports	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass gemeinsame Ports für Amazon Elastic Compute Cloud (Amazon EC2) -Sicherheitsgruppen eingeschränkt sind. Wenn der Zugriff auf Ports nicht auf vertrauenswürdige Quellen beschränkt wird, kann dies zu Angriffen auf die Verfügbarkeit, Integrität und Vertraulichkeit von Systemen führen. Mit dieser Regel können Sie optional die Parameter blockedPort1–blockedPort5 festlegen (Standardkonfigurationen: 20, 21, 3389, 3306, 4333). Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC.L1-3.1.2	Beschränken Sie den Zugriff auf das Informationssystem auf jene Transaktionen und Funktionen, die autorisierte Benutzer ausführen dürfen.	root-account-hardware-mfa-aktiviert	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Hardware-MFA für den Root-Benutzer aktiviert ist. Der Stammbenutzer ist der AWS-Konto-Benutzer mit den meisten Berechtigungen. MFA sorgt für eine weitere Schutzebene zusätzlich zu den Anmeldeinformationen. Indem Sie MFA für den Root-Benutzer vorschreiben, können Sie die Anzahl AWS-Konten kompromittierter Benutzer reduzieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC.L1-3.1.2	Beschränken Sie den Zugriff auf das Informationssystem auf jene Transaktionen und Funktionen, die autorisierte Benutzer ausführen dürfen.	root-account-mfa-enabled	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass MFA für den Root-Benutzer aktiviert ist. Der Stammbenutzer ist der AWS-Konto-Benutzer mit den meisten Berechtigungen. MFA sorgt für eine weitere Schutzebene zusätzlich zu den Anmeldeinformationen. Indem Sie MFA für den Root-Benutzer vorschreiben, können Sie die Anzahl AWS-Konten kompromittierter Benutzer reduzieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC.L1-3.1.2	Beschränken Sie den Zugriff auf das Informationssystem auf jene Transaktionen und Funktionen, die autorisierte Benutzer ausführen dürfen.	s3- -blöcke-periodisch account-level-public-access	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Simple Storage Service (Amazon S3) -Buckets nicht öffentlich zugänglich sind. Diese Regel trägt dazu bei, sensible Daten vor unbefugten Remote-Benutzern zu schützen, indem sie den öffentlichen Zugriff verhindert. Mit dieser Regel können Sie optional die Parameter ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) und restrictPublicBuckets Parameter (Config Default: True) festlegen. Die tatsächlichen Werte müssen den Richtlini

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			en Ihrer Organisation entsprechen.
AC.L1-3.1.2	Beschränken Sie den Zugriff auf das Informationssystem auf jene Transaktionen und Funktionen, die autorisierte Benutzer ausführen dürfen.	s3 bucket-level-public-access - verboten	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Simple Storage Service (Amazon S3) -Buckets nicht öffentlich zugänglich sind. Diese Regel trägt dazu bei, sensible Daten vor unbefugten Remote-Benutzern zu schützen, indem sie den öffentlichen Zugriff auf Bucket-Ebene verhindert.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC.L1-3.1.2	Beschränken Sie den Zugriff auf das Informationssystem auf jene Transaktionen und Funktionen, die autorisierte Benutzer ausführen dürfen.	s-3 bucket-policy-grantee-check	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie s3_bucket_policy_grantee_check aktivieren. Diese Regel prüft, ob der vom Amazon S3 S3-Bucket gewährte Zugriff durch die von Ihnen bereitgestellten AWS Principals, Verbundbenutzer, Service Principals, IP-Adressen oder Amazon Virtual Private Cloud (Amazon VPC) IDs eingeschränkt ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC.L1-3.1.2	Beschränken Sie den Zugriff auf das Informationssystem auf jene Transaktionen und Funktionen, die autorisierte Benutzer ausführen dürfen.	s-3 bucket-public-read-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie nur autorisierten Benutzern, Prozessen und Geräten Zugriff auf Amazon Simple Storage Service (Amazon S3) - Buckets gewähren. Die Verwaltung des Zugriffs sollte mit der Klassifizierung der Daten übereinstimmen.
AC.L1-3.1.2	Beschränken Sie den Zugriff auf das Informationssystem auf jene Transaktionen und Funktionen, die autorisierte Benutzer ausführen dürfen.	s3- bucket-public-write-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie nur autorisierten Benutzern, Prozessen und Geräten Zugriff auf Amazon Simple Storage Service (Amazon S3) - Buckets gewähren. Die Verwaltung des Zugriffs sollte mit der Klassifizierung der Daten übereinstimmen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC.L1-3.1.2	Beschränken Sie den Zugriff auf das Informationssystem auf jene Transaktionen und Funktionen, die autorisierte Benutzer ausführen dürfen.	sagemaker-notebook-no-direct-Internetzugang	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass SageMaker Amazon-Notebooks keinen direkten Internetzugang zulassen. Indem Sie direkten Internetzugang blockieren, vermeiden Sie, dass unbefugte Benutzer auf sensible Daten zugreifen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC.L1-3.1.2	Beschränken Sie den Zugriff auf das Informationssystem auf jene Transakti onen und Funktione n, die autorisierte Benutzer ausführen dürfen.	vpc-default-security-group-geschlossen	Sicherheitsgruppen von Amazon Elastic Compute Cloud (Amazon EC2) können bei der Verwaltung des Netzwerkzugriffs helfen, indem sie eine statusbehaftete Filterung des ein- und ausgehenden Netzwerkverkehrs zu Ressourcen bereitstellen. AWS Die Beschränk ung des gesamten Datenverkehrs auf die Standardsicherheit sgruppe hilft dabei, den Fernzugriff auf Ihre Ressourcen einzuschränken. AWS

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC.L1-3.1.2	Beschränken Sie den Zugriff auf das Informationssystem auf jene Transaktionen und Funktionen, die autorisierte Benutzer ausführen dürfen.	vpc-sg-open-only-to-authorized-ports	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass gemeinsame Ports für Amazon Elastic Compute Cloud (Amazon EC2) -Sicherheitsgruppen eingeschränkt sind. Wenn der Zugriff auf Ports nicht auf vertrauenswürdige Quellen beschränkt wird, kann dies zu Angriffen auf die Verfügbarkeit, Integrität und Vertraulichkeit von Systemen führen. Durch die Beschränkung des Zugriffs auf Ressourcen innerhalb einer Sicherheitsgruppe aus dem Internet (0.0.0.0/0) kann der Remote-Zugriff auf interne Systeme gesteuert werden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC.L1-3.1.2	Beschränken Sie den Zugriff auf das Informationssystem auf jene Transaktionen und Funktionen, die autorisierte Benutzer ausführen dürfen.	opensearch-in-vpc-only	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass sich Amazon OpenSearch Service-Domains innerhalb einer Amazon Virtual Private Cloud (Amazon VPC) befinden. Eine Amazon OpenSearch Service-Domain innerhalb einer Amazon VPC ermöglicht die sichere Kommunikation zwischen Amazon OpenSearch Service und anderen Services innerhalb der Amazon VPC, ohne dass ein Internet-Gateway, ein NAT-Gerät oder eine VPN-Verbindung erforderlich ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC.L1-3.1.20	Überprüfen und kontrollieren/beschränken Sie die Verbindungen zu externen Informationssystemen und deren Nutzung.	alb-waf-enabled	Stellen Sie sicher, dass AWS WAF auf Elastic Load Balancers (ELB) aktiviert ist, um Webanwendungen zu schützen. Eine WAF trägt zum Schutz Ihrer Webanwendungen oder APIs vor gängigen Web-Exploits bei. Diese Web-Exploits können sich auf die Verfügbarkeit auswirken, die Sicherheit gefährden oder übermäßige Ressourcen in Ihrer Umgebung verbrauchen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC.L1-3.1.20	Überprüfen und kontrollieren/beschränken Sie die Verbindungen zu externen Informationssystemen und deren Nutzung.	autoscaling-launch-config-public-ip-deaktiviert	Wenn Sie Ihre Netzwerkschnittstellen mit einer öffentlichen IP-Adresse konfigurieren, sind die diesen Netzwerkschnittstellen zugehörigen Ressourcen über das Internet erreichbar. EC2 Ressourcen sollten nicht öffentlich zugänglich sein, da dies einen unbeabsichtigten Zugriff auf Ihre Anwendungen oder Server ermöglichen kann.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC.L1-3.1.20	Überprüfen und kontrollieren/beschränken Sie die Verbindungen zu externen Informationssystemen und deren Nutzung.	ec2- instance-no-public-ip	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon Elastic Compute Cloud (Amazon EC2) - Instances nicht öffentlich zugänglich sind. EC2 Amazon-Instances können vertrauliche Informationen enthalten, und für solche Konten ist eine Zugriffskontrolle erforderlich.
AC.L1-3.1.20	Überprüfen und kontrollieren/beschränken Sie die Verbindungen zu externen Informationssystemen und deren Nutzung.	emr-master-no-public-ip	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon EMR-Cluster-Masterknoten nicht öffentlich zugänglich sind. Amazon-EMR-Cluster-Hauptknoten können vertrauliche Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC.L1-3.1.20	Überprüfen und kontrollieren/beschränken Sie die Verbindungen zu externen Informationssystemen und deren Nutzung.	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) Security Groups können bei der Verwaltung des Netzwerkzugriffs helfen, indem sie eine statusbehaftete Filterung von eingehendem und ausgehendem Netzwerkverkehr zu Ressourcen bereitstellen. AWS Wenn Sie eingehenden (oder entfernten) Datenverkehr von 0.0.0.0/0 bis Port 22 auf Ihren Ressourcen nicht zulassen, können Sie den Remote-Zugriff einschränken.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC.L1-3.1.20	Überprüfen und kontrollieren/beschränken Sie die Verbindungen zu externen Informationssystemen und deren Nutzung.	internet-gateway-authorized-vpc-nur	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Internet-Gateways nur mit autorisierter Amazon Virtual Private Cloud (Amazon VPC) verbunden sind. Internet-Gateways ermöglichen den bidirektionalen Internetzugang zur und von der Amazon VPC, was möglicher weise zu einem unbefugten Zugriff auf Amazon-VPC-Ressourcen führen kann.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC.L1-3.1.20	Überprüfen und kontrollieren/beschränken Sie die Verbindungen zu externen Informationssystemen und deren Nutzung.	lambda-function-public-access-verboten	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass AWS Lambda-Funktionen nicht öffentlich zugänglich sind. Der öffentliche Zugriff kann möglicherweise die Verfügbarkeit von Ressourcen beeinträchtigen.
AC.L1-3.1.20	Überprüfen und kontrollieren/beschränken Sie die Verbindungen zu externen Informationssystemen und deren Nutzung.	no-unrestricted-route-to-igw	Stellen Sie sicher, dass EC2 Amazon-Routentabellen keine uneingeschränkten Routen zu einem Internet-Gateway enthalten. Durch das Entfernen oder Beschränken des Internetzugangs für Workloads innerhalb von Amazon VPCs können unbeabsichtigte Zugriffe in Ihrer Umgebung reduziert werden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC.L1-3.1.20	Überprüfen und kontrollieren/beschränken Sie die Verbindungen zu externen Informationssystemen und deren Nutzung.	rds-instance-public-access-überprüfen	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Relational Database Service (Amazon RDS) -Instances nicht öffentlich sind. Amazon-RDS-Datenbank-Instances können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC.L1-3.1.20	Überprüfen und kontrollieren/beschränken Sie die Verbindungen zu externen Informationssystemen und deren Nutzung.	redshift-cluster-public-access-überprüfen	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Redshift Redshift-Cluster nicht öffentlich sind. Amazon-Redshift-Cluster können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC.L1-3.1.20	Überprüfen und kontrollieren/beschränken Sie die Verbindungen zu externen Informationssystemen und deren Nutzung.	restricted-common-ports	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass gemeinsame Ports für Amazon Elastic Compute Cloud (Amazon EC2) -Sicherheitsgruppen eingeschränkt sind. Wenn der Zugriff auf Ports nicht auf vertrauenswürdige Quellen beschränkt wird, kann dies zu Angriffen auf die Verfügbarkeit, Integrität und Vertraulichkeit von Systemen führen. Mit dieser Regel können Sie optional die Parameter blockedPort1–blockedPort5 festlegen (Standardkonfigurationen: 20, 21, 3389, 3306, 4333). Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC.L1-3.1.20	Überprüfen und kontrollieren/beschränken Sie die Verbindungen zu externen Informationssystemen und deren Nutzung.	s3- account-level-public-access -blöcke-periodisch	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Simple Storage Service (Amazon S3) -Buckets nicht öffentlich zugänglich sind. Diese Regel trägt dazu bei, sensible Daten vor unbefugten Remote-Benutzern zu schützen, indem sie den öffentlichen Zugriff verhindert. Mit dieser Regel können Sie optional die Parameter ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) und restrictPublicBuckets Parameter (Config Default: True) festlegen. Die tatsächlichen Werte müssen den Richtlini

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			en Ihrer Organisation entsprechen.
AC.L1-3.1.20	Überprüfen und kontrollieren/beschränken Sie die Verbindungen zu externen Informationssystemen und deren Nutzung.	s3 bucket-level-public-access - verboten	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Simple Storage Service (Amazon S3) -Buckets nicht öffentlich zugänglich sind. Diese Regel trägt dazu bei, sensible Daten vor unbefugten Remote-Benutzern zu schützen, indem sie den öffentlichen Zugriff auf Bucket-Ebene verhindert.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC.L1-3.1.20	Überprüfen und kontrollieren/beschränken Sie die Verbindungen zu externen Informationssystemen und deren Nutzung.	s-3 bucket-public-read-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie nur autorisierten Benutzern, Prozessen und Geräten Zugriff auf Amazon Simple Storage Service (Amazon S3) - Buckets gewähren. Die Verwaltung des Zugriffs sollte mit der Klassifizierung der Daten übereinstimmen.
AC.L1-3.1.20	Überprüfen und kontrollieren/beschränken Sie die Verbindungen zu externen Informationssystemen und deren Nutzung.	s3- bucket-public-write-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie nur autorisierten Benutzern, Prozessen und Geräten Zugriff auf Amazon Simple Storage Service (Amazon S3) - Buckets gewähren. Die Verwaltung des Zugriffs sollte mit der Klassifizierung der Daten übereinstimmen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC.L1-3.1.20	Überprüfen und kontrollieren/beschränken Sie die Verbindungen zu externen Informationssystemen und deren Nutzung.	sagemaker-notebook-no-direct-Internetzugang	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass SageMaker Amazon-Notebooks keinen direkten Internetzugang zulassen. Indem Sie direkten Internetzugang blockieren, vermeiden Sie, dass unbefugte Benutzer auf sensible Daten zugreifen.
AC.L1-3.1.20	Überprüfen und kontrollieren/beschränken Sie die Verbindungen zu externen Informationssystemen und deren Nutzung.	ssm-document-not-public	Stellen Sie sicher, dass AWS Systems Manager (SSM) - Dokumente nicht öffentlich sind, da dies einen unbeabsichtigten Zugriff auf Ihre SSM-Dokumente ermöglichen kann. Ein öffentliches SSM-Dokument kann Informationen über Ihr Konto, Ihre Ressourcen und internen Prozesse preisgeben.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC.L1-3.1.20	Überprüfen und kontrollieren/beschränken Sie die Verbindungen zu externen Informationssystemen und deren Nutzung.	subnet-auto-assign-public-ip-deaktiviert	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon Virtual Private Cloud (VPC) -Subnetzen nicht automatisch eine öffentliche IP-Adresse zugewiesen wird. Amazon Elastic Compute Cloud (EC2) -Instances, die in Subnetzen gestartet werden, in denen dieses Attribut aktiviert ist, haben ihrer primären Netzwerkschnittstelle eine öffentliche IP-Adresse zugewiesen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC.L1-3.1.20	Überprüfen und kontrollieren/beschränken Sie die Verbindungen zu externen Informationssystemen und deren Nutzung.	vpc-default-security-group-geschlossen	Sicherheitsgruppen von Amazon Elastic Compute Cloud (Amazon EC2) können bei der Verwaltung des Netzwerkzugriffs helfen, indem sie eine statusbehaftete Filterung des ein- und ausgehenden Netzwerkverkehrs zu Ressourcen bereitstellen. AWS Die Beschränkung des gesamten Datenverkehrs auf die Standardsicherheitsgruppe hilft dabei, den Fernzugriff auf Ihre Ressourcen einzuschränken. AWS

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC.L1-3.1.20	Überprüfen und kontrollieren/beschränken Sie die Verbindungen zu externen Informationssystemen und deren Nutzung.	vpc-sg-open-only-to-authorized-ports	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass gemeinsame Ports für Amazon Elastic Compute Cloud (Amazon EC2) -Sicherheitsgruppen eingeschränkt sind. Wenn der Zugriff auf Ports nicht auf vertrauenswürdige Quellen beschränkt wird, kann dies zu Angriffen auf die Verfügbarkeit, Integrität und Vertraulichkeit von Systemen führen. Durch die Beschränkung des Zugriffs auf Ressourcen innerhalb einer Sicherheitsgruppe aus dem Internet (0.0.0.0/0) kann der Remote-Zugriff auf interne Systeme gesteuert werden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
IA.L1-3.5.1	Identifizieren Sie Benutzer von Informationssystemen, Prozesse von Benutzern oder Geräte.	api-gw-execution-logging-aktiviert	Die API-Gateway-Protokollierung zeigt detaillierte Ansichten der Benutzer, die auf die API zugegriffen haben, und wie diese Benutzer auf die API zugegriffen haben. Diese Einblicke ermöglichen die Transparenz von Benutzeraktivitäten.
IA.L1-3.5.1	Identifizieren Sie Benutzer von Informationssystemen, Prozesse von Benutzern oder Geräte.	cloudtrail-s3-dataevents-enabled	Die Erfassung von Simple Storage Service (Amazon S3)-Datenereignissen unterstützt die Erkennung von ungewöhnlichen Aktivitäten. Zu den Details gehören AWS-Konto Informationen über den Zugriff auf einen Amazon S3 S3-Bucket, die IP-Adresse und die Uhrzeit des Ereignisses.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
IA.L1-3.5.1	Identifizieren Sie Benutzer von Informationssystemen, Prozesse von Benutzern oder Geräte.	cloud-trail-cloud-watch-logs-aktiviert	Verwenden Sie Amazon CloudWatch , um Protokoll ereignisaktivitäten zentral zu sammeln und zu verwalten. Die Aufnahme von AWS CloudTrail Daten liefert Einzelheiten zu den API-Aufrufaktivitäten in Ihrem AWS-Konto.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
IA.L1-3.5.1	Identifizieren Sie Benutzer von Informationssystemen, Prozesse von Benutzern oder Geräte.	elb-logging-enabled	Die Elastic-Load-Balancing-Aktivität ist ein zentraler Kommunikationspunkt innerhalb einer Umgebung. Stellen Sie sicher, dass die ELB-Protokollierung aktiviert ist. Die gesammelten Daten enthalten detaillierte Informationen zu Anfragen, die an den ELB gesendet wurden. Jedes Protokoll enthält Informationen wie die Zeit, zu der die Anforderung einging, die Client-IP-Adresse, Latenzen, Anforderungspfade und Serverantworten.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
IA.L1-3.5.1	Identifizieren Sie Benutzer von Informationssystemen, Prozesse von Benutzern oder Geräte.	emr-kerberos-enabled	Die Zugriffsberechtigungen und -autorisierungen können verwaltet und nach den Prinzipien der geringsten Berechtigung und Aufgabentrennung integriert werden, indem Kerberos für Amazon-EMR-Cluster aktiviert wird. In Kerberos werden Services und Benutzer, die sich authentifizieren müssen, als Prinzipale bezeichnet. Prinzipale befinden sich in einem Kerberos-Bereich. Innerhalb dieses Bereichs wird ein Kerberos-Server als Key Distribution Center (KDC) bezeichnet. Über diesen Server können sich Prinzipale authentifizieren. Die Authentifizierung im KDC erfolgt durch die Ausstellung von Authentif

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			izierungstickets. Das KDC unterhält eine Datenbank der Prinzipale in seinem Bereich mit ihren Passwörtern und anderen administr ativen Informationen zu jedem Prinzipal.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
IA.L1-3.5.1	Identifizieren Sie Benutzer von Informationssystemen, Prozesse von Benutzern oder Geräte.	multi-region-cloudtrail-enabled	AWS CloudTrail zeichnet Aktionen und API-Aufrufe der AWS Management Console auf. Sie können feststellen, welche Benutzer und Konten angerufen wurden AWS, von welcher Quell-IP-Adresse aus die Anrufe getätigt wurden und wann die Anrufe erfolgten. CloudTrail übermittelt Protokolldateien aus allen AWS Regionen an Ihren S3-Bucket , wenn MULTI_REGION_CLOUD_TRAIL_ENABLED aktiviert ist. Außerdem wird beim AWS Start einer neuen Region derselbe Trail in der neuen Region erstellt. CloudTrail Dadurch erhalten Sie automatisch Protokolldateien mit API-Aktivitäten für die neue Region.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
IA.L1-3.5.1	Identifizieren Sie Benutzer von Informationssystemen, Prozesse von Benutzern oder Geräte.	rds-logging-enabled	Um die Protokollierung und Überwachung in Ihrer Umgebung zu erleichtern, stellen Sie sicher, dass die Amazon Relational Database Service (Amazon RDS)-Protokollierung aktiviert ist. Mit der Amazon-RDS-Protokollierung können Sie Ereignisse wie Verbindungen, Verbindungsabbrüche, Abfragen oder abgefragte Tabellen erfassen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
IA.L1-3.5.1	Identifizieren Sie Benutzer von Informationssystemen, Prozesse von Benutzern oder Geräte.	s-3 bucket-logging-enabled	Die Amazon Simple Storage Service (Amazon S3)-Serverzugriffsprotokollierung bietet eine Methode zur Überwachung des Netzwerks im Hinblick auf potenzielle Cybersicherheitsereignisse. Die Ereignisse werden überwacht, indem detaillierte Aufzeichnungen über die Anfragen erfasst werden, die an einen Amazon-S3-Bucket gestellt wurden. Jeder Zugriffsprotokolleintrag enthält Details zu einer einzelnen Zugriffsanfrage. Zu den Details gehören Anforderer, Bucket-Name, Anforderungszeit, Anforderungsaktion, Antwortstatus und Fehlercode, falls relevant.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
IA.L1-3.5.1	Identifizieren Sie Benutzer von Informationssystemen, Prozesse von Benutzern oder Geräte.	wafv2-logging-enabled	Um die Protokollierung und Überwachung in Ihrer Umgebung zu erleichtern, aktivieren Sie die AWS WAF (V2) -Protokollierung im regionalen und globalen Web ACLs. AWS Die WAF-Protokollierung bietet detaillierte Informationen über den Datenverkehr, der von Ihrer Web-ACL analysiert wird. In den Protokollen werden die Uhrzeit aufgezeichnet, zu der die AWS WAF die Anfrage von Ihrer AWS Ressource erhalten hat, Informationen über die Anfrage und eine Aktion für die Regel, der jede Anfrage entsprach.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
IA.L1-3.5.2	Authentifizieren (oder verifizieren) Sie die Identitäten dieser Benutzer, Prozesse oder Geräte als Voraussetzung für den Zugriff auf Informationssysteme der Organisation.	emr-kerberos-enabled	Die Zugriffsberechtigungen und -autorisierungen können verwaltet und nach den Prinzipien der geringsten Berechtigung und Aufgabentrennung integriert werden, indem Kerberos für Amazon-EMR-Cluster aktiviert wird. In Kerberos werden Services und Benutzer, die sich authentifizieren müssen, als Prinzipale bezeichnet. Prinzipale befinden sich in einem Kerberos-Bereich. Innerhalb dieses Bereichs wird ein Kerberos-Server als Key Distribution Center (KDC) bezeichnet. Über diesen Server können sich Prinzipale authentifizieren. Die Authentifizierung im KDC erfolgt durch die Ausstellung von Authentif

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			izierungstickets. Das KDC unterhält eine Datenbank der Prinzipale in seinem Bereich mit ihren Passwörtern und anderen administr ativen Informationen zu jedem Prinzipal.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
IA.L1-3.5.2	Authentifizieren (oder verifizieren) Sie die Identitäten dieser Benutzer, Prozesse oder Geräte als Voraussetzung für den Zugriff auf Informationssysteme der Organisation.	iam-password-policy	Die Identitäten und Anmeldeinformationen werden auf der Grundlage einer organisatorischen IAM-Passwortrichtlinie ausgestellt, verwaltet und verifiziert. Sie erfüllen oder übertreffen die Anforderungen von NIST SP 800-63 und dem Standard „Best Practices“ von AWS Foundational Security für die Passwortstärke. Mit dieser Regel können Sie optional RequireUppercaseCharacters (Wert für AWS grundlegende Sicherheitsbewährte Methoden: wahr), RequireLowercaseCharacters (Wert für bewährte Methoden für AWS grundlegende Sicherheit: wahr), RequireSymbols (Wert für bewährte Methoden für AWS grundlegende Sicherheit:

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			wahr), RequireNumbers (Wert für bewährte Methoden für AWS grundlegende Sicherheit: wahr), MinimumPasswordLength (Wert für bewährte Methoden für AWS grundlegende Sicherheit: 14), PasswordReusePrevention (Wert für bewährte Methoden für AWS grundlegende Sicherheit: 24) und MaxPasswordAge (Wert für bewährte Methoden für AWS grundlegende Sicherheit: 90) für Ihr IAM festlegen Kennwortrichtlinie. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
IA.L1-3.5.2	Authentifizieren (oder verifizieren) Sie die Identitäten dieser Benutzer, Prozesse oder Geräte als Voraussetzung für den Zugriff auf Informationssysteme der Organisation.	iam-user-mfa-enabled	Aktivieren Sie diese Regel, um den Zugriff auf Ressourcen in der AWS Cloud einzuschränken. Diese Regel sorgt dafür, dass die Multi-Faktor-Authentifizierung (MFA) für alle Benutzer aktiviert ist. MFA sorgt für eine weitere Schutzebene zusätzlich zu den Anmeldeinformationen. Reduzieren Sie Fälle von kompromittierten Konten, indem Sie MFA für Benutzer vorschreiben.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
IA.L1-3.5.2	Authentifizieren (oder verifizieren) Sie die Identitäten dieser Benutzer, Prozesse oder Geräte als Voraussetzung für den Zugriff auf Informationssysteme der Organisation.	mfa-enabled-for-iam-Konsolenzugriff	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass MFA für alle AWS Identity and Access Management (IAM) -Benutzer aktiviert ist, die über ein Konsolenkennwort verfügen. MFA sorgt für eine weitere Schutzebene zusätzlich zu den Anmeldeinformationen. Indem Sie MFA für Benutzer vorschreiben, können Sie Fälle kompromittierter Konten reduzieren und verhindern, dass unbefugte Benutzer auf vertrauliche Daten zugreifen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
IA.L1-3.5.2	Authentifizieren (oder verifizieren) Sie die Identitäten dieser Benutzer, Prozesse oder Geräte als Voraussetzung für den Zugriff auf Informationssysteme der Organisation.	root-account-hardware-mfa-aktiviert	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Hardware-MFA für den Root-Benutzer aktiviert ist. Der Stammbenutzer ist der AWS-Konto-Benutzer mit den meisten Berechtigungen. MFA sorgt für eine weitere Schutzebene zusätzlich zu den Anmeldeinformationen. Indem Sie MFA für den Root-Benutzer vorschreiben, können Sie die Anzahl AWS-Konten kompromittierter Benutzer reduzieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
IA.L1-3.5.2	Authentifizieren (oder verifizieren) Sie die Identitäten dieser Benutzer, Prozesse oder Geräte als Voraussetzung für den Zugriff auf Informationssysteme der Organisation.	root-account-mfa-enabled	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass MFA für den Root-Benutzer aktiviert ist. Der Stammbenutzer ist der AWS-Konto-Benutzer mit den meisten Berechtigungen. MFA sorgt für eine weitere Schutzebene zusätzlich zu den Anmeldeinformationen. Indem Sie MFA für den Root-Benutzer vorschreiben, können Sie die Anzahl AWS-Konten kompromittierter Benutzer reduzieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC.L1-3.13.1	Überwachen, kontrollieren und schützen Sie die Unternehmenskommunikation (d. h. Informationen, die von Informationssystemen der Organisation übertragen oder empfangen werden) an externen und wichtigen internen Grenzen der Informationssysteme.	alb-http-drop-invalid-Header-fähig	Stellen Sie sicher, dass Ihre Elastic Load Balancers (ELB) so konfiguriert sind, dass sie HTTP-Header löschen. Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.
SC.L1-3.13.1	Überwachen, kontrollieren und schützen Sie die Unternehmenskommunikation (d. h. Informationen, die von Informationssystemen der Organisation übertragen oder empfangen werden) an externen und wichtigen internen Grenzen der Informationssysteme.	alb-http-to-https-Umleitungsprüfung	Um Daten während der Übertragung zu schützen, stellen Sie sicher, dass Ihr Application Load Balancer unverschlüsselte HTTP-Anfragen automatisch an HTTPS umleitet. Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC.L1-3.13.1	Überwachen, kontrollieren und schützen Sie die Unternehmenskommunikation (d. h. Informationen, die von Informationssystemen der Organisation übertragen oder empfangen werden) an externen und wichtigen internen Grenzen der Informationssysteme.	alb-waf-enabled	Stellen Sie sicher, dass AWS WAF auf Elastic Load Balancers (ELB) aktiviert ist, um Webanwendungen zu schützen. Eine WAF trägt zum Schutz Ihrer Webanwendungen oder APIs vor gängigen Web-Exploits bei. Diese Web-Exploits können sich auf die Verfügbarkeit auswirken, die Sicherheit gefährden oder übermäßige Ressourcen in Ihrer Umgebung verbrauchen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC.L1-3.13.1	Überwachen, kontrollieren und schützen Sie die Unternehmenskommunikation (d. h. Informationen, die von Informationssystemen der Organisation übertragen oder empfangen werden) an externen und wichtigen internen Grenzen der Informationssysteme.	api-gw-associated-with-WAF	AWS Mit WAF können Sie eine Reihe von Regeln (als Web Access Control List (Web ACL) bezeichnet) konfigurieren, die Webanfragen auf der Grundlage von anpassbaren Websicherheitsregeln und -bedingungen, die Sie definieren, zulassen, blockieren oder zählen. Stellen Sie sicher, dass Ihre Amazon-API-Gateway-Stufe mit einer WAF-Web-ACL verknüpft ist, um sie vor böswilligen Angriffen zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC.L1-3.13.1	Überwachen, kontrollieren und schützen Sie die Unternehmenskommunikation (d. h. Informationen, die von Informationssystemen der Organisation übertragen oder empfangen werden) an externen und wichtigen internen Grenzen der Informationssysteme.	cloudwatch-alarm-action-check	Amazon CloudWatch alarmiert, wenn eine Metrik den Schwellenwert für eine bestimmte Anzahl von Bewertungszeiträumen überschreitet. Der Alarm führt eine oder mehrere Aktionen durch, die vom Wert der Metrik oder des Ausdrucks im Vergleich zu einem Schwellenwert in einer Reihe von Zeiträumen abhängt. Diese Regel erfordert einen Wert für alarmActionRequired (Config Default: True), insufficientDataAction Required (Config Default: True), okActionRequired (Config Default: False). Der tatsächliche Wert muss die Alarmaktionen für Ihre Umgebung widerspiegeln.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC.L1-3.13.1	Überwachen, kontrollieren und schützen Sie die Unternehmenskommunikation (d. h. Informationen, die von Informationssystemen der Organisation übertragen oder empfangen werden) an externen und wichtigen internen Grenzen der Informationssysteme.	dms-replication-not-public	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass auf DMS-Replikationsinstanzen nicht öffentlich zugegriffen werden kann. DMS-Replikations-Instances können vertrauliche Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.
SC.L1-3.13.1	Überwachen, kontrollieren und schützen Sie die Unternehmenskommunikation (d. h. Informationen, die von Informationssystemen der Organisation übertragen oder empfangen werden) an externen und wichtigen internen Grenzen der Informationssysteme.	ebs-snapshot-public-restorable-überprüfen	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass EBS-Snapshots nicht öffentlich wiederherstellbar sind. EBS-Volume-Snapshots können vertrauliche Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC.L1-3.13.1	Überwachen, kontrollieren und schützen Sie die Unternehmenskommunikation (d. h. Informationen, die von Informationssystemen der Organisation übertragen oder empfangen werden) an externen und wichtigen internen Grenzen der Informationssysteme.	elasticsearch-in-vpc-only	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass sich Amazon OpenSearch OpenSearch Service (Service) - Domains innerhalb einer Amazon Virtual Private Cloud (Amazon VPC) befinden. Eine OpenSearch Service-Domain innerhalb einer Amazon VPC ermöglicht die sichere Kommunikation zwischen OpenSearch Service und anderen Services innerhalb der Amazon VPC, ohne dass ein Internet-Gateway, ein NAT-Gerät oder eine VPN-Verbindung erforderlich ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC.L1-3.13.1	Überwachen, kontrollieren und schützen Sie die Unternehmenskommunikation (d. h. Informationen, die von Informationssystemen der Organisation übertragen oder empfangen werden) an externen und wichtigen internen Grenzen der Informationssysteme.	elasticsearch-node-to-node-Verschlüsselungsprüfung	Stellen Sie sicher, dass die node-to-node Verschlüsselung für Amazon OpenSearch Service aktiviert ist. Node-to-nodeVerschlüsselung ermöglicht die TLS 1.2-Verschlüsselung für die gesamte Kommunikation innerhalb der Amazon Virtual Private Cloud (Amazon VPC). Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC.L1-3.13.1	Überwachen, kontrollieren und schützen Sie die Unternehmenskommunikation (d. h. Informationen, die von Informationssystemen der Organisation übertragen oder empfangen werden) an externen und wichtigen internen Grenzen der Informationssysteme.	elb-acm-certificate-required	Zum Schutz von eventuell vorhandenen sensiblen Daten sowie von Daten während der Übertragung muss die Verschlüsselung für Ihr Elastic Load Balancing aktiviert sein. Verwenden Sie AWS Certificate Manager, um öffentliche und private SSL/TLS-Zertifikate mit AWS Diensten und internen Ressourcen zu verwalten, bereitzustellen und bereitzustellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC.L1-3.13.1	Überwachen, kontrollieren und schützen Sie die Unternehmenskommunikation (d. h. Informationen, die von Informationssystemen der Organisation übertragen oder empfangen werden) an externen und wichtigen internen Grenzen der Informationssysteme.	elb-tls-https-listeners-nur	Stellen Sie sicher, dass Ihre Elastic Load Balancer (ELBs) mit SSL- oder HTTPS-Listenern konfiguriert sind. Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.
SC.L1-3.13.1	Überwachen, kontrollieren und schützen Sie die Unternehmenskommunikation (d. h. Informationen, die von Informationssystemen der Organisation übertragen oder empfangen werden) an externen und wichtigen internen Grenzen der Informationssysteme.	guardduty-enabled-centralized	Amazon GuardDuty kann mithilfe von Threat Intelligence Feeds helfen, potenzielle Cybersicherheitsereignisse zu überwachen und zu erkennen. Dazu gehören Listen mit bösartigen IPs und maschinellen Lernmethoden zur Identifizierung unerwarteter, nicht autorisierter und bösartiger Aktivitäten in Ihrer AWS Cloud-Umgebung.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC.L1-3.13.1	Überwachen, kontrollieren und schützen Sie die Unternehmenskommunikation (d. h. Informationen, die von Informationssystemen der Organisation übertragen oder empfangen werden) an externen und wichtigen internen Grenzen der Informationssysteme.	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) Security Groups können bei der Verwaltung des Netzwerkzugriffs helfen, indem sie eine statusbehaftete Filterung von eingehendem und ausgehendem Netzwerkverkehr zu Ressourcen bereitstellen. AWS Wenn Sie eingehenden (oder entfernten) Datenverkehr von 0.0.0.0/0 bis Port 22 auf Ihren Ressourcen nicht zulassen, können Sie den Remote-Zugriff einschränken.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC.L1-3.13.1	Überwachen, kontrollieren und schützen Sie die Unternehmenskommunikation (d. h. Informationen, die von Informationssystemen der Organisation übertragen oder empfangen werden) an externen und wichtigen internen Grenzen der Informationssysteme.	ec-2 instances-in-vpc	Stellen Sie Amazon Elastic Compute Cloud (Amazon EC2) -Instances innerhalb einer Amazon Virtual Private Cloud (Amazon VPC) bereit, um eine sichere Kommunikation zwischen einer Instance und anderen Services innerhalb der Amazon VPC zu ermöglichen, ohne dass ein Internet-Gateway, ein NAT-Gerät oder eine VPN-Verbindung erforderlich ist. Der gesamte Datenverkehr bleibt sicher in der AWS Cloud. Domains, die sich innerhalb einer VPC befinden, verfügen aufgrund ihrer logischen Isolierung im Vergleich zu Domains mit öffentlichen Endpunkten über eine zusätzliche Sicherheitsebene. Weisen Sie EC2

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			Amazon-Instances einer Amazon-VPC zu, um den Zugriff ordnungsgemäß zu verwalten.
SC.L1-3.13.1	Überwachen, kontrollieren und schützen Sie die Unternehmenskommunikation (d. h. Informationen, die von Informationssystemen der Organisation übertragen oder empfangen werden) an externen und wichtigen internen Grenzen der Informationssysteme.	internet-gateway-authorized-vpc-nur	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Internet-Gateways nur mit autorisierter Amazon Virtual Private Cloud (Amazon VPC) verbunden sind. Internet-Gateways ermöglichen den bidirektionalen Internetzugang zur und von der Amazon VPC, was möglicherweise zu einem unbefugten Zugriff auf Amazon-VPC-Ressourcen führen kann.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC.L1-3.13.1	Überwachen, kontrollieren und schützen Sie die Unternehmenskommunikation (d. h. Informationen, die von Informationssystemen der Organisation übertragen oder empfangen werden) an externen und wichtigen internen Grenzen der Informationssysteme.	lambda-function-public-access-verboten	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass AWS Lambda-Funktionen nicht öffentlich zugänglich sind. Der öffentliche Zugriff kann möglicherweise die Verfügbarkeit von Ressourcen beeinträchtigen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC.L1-3.13.1	Überwachen, kontrollieren und schützen Sie die Unternehmenskommunikation (d. h. Informationen, die von Informationssystemen der Organisation übertragen oder empfangen werden) an externen und wichtigen internen Grenzen der Informationssysteme.	lambda-inside-vpc	Stellen Sie AWS Lambda-Funktionen in einer Amazon Virtual Private Cloud (Amazon VPC) bereit, um eine sichere Kommunikation zwischen einer Funktion und anderen Diensten innerhalb der Amazon VPC zu gewährleisten. Bei dieser Konfiguration sind kein Internet-Gateway, kein NAT-Gerät und keine VPN-Verbindung erforderlich. Der gesamte Datenverkehr bleibt sicher in der Cloud. AWS Domains, die sich innerhalb einer VPC befinden, verfügen aufgrund ihrer logischen Isolierung im Vergleich zu Domains mit öffentlichen Endpunkten über eine zusätzliche Sicherheitsebene. Um den Zugriff ordnungsgemäß zu verwalten,

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			sollten AWS Lambda-Funktionen einer VPC zugewiesen werden.
SC.L1-3.13.1	Überwachen, kontrollieren und schützen Sie die Unternehmenskommunikation (d. h. Informationen, die von Informationssystemen der Organisation übertragen oder empfangen werden) an externen und wichtigen internen Grenzen der Informationssysteme.	no-unrestricted-route-to-igw	Stellen Sie sicher, dass EC2 Amazon-Routentabellen keine uneingeschränkten Routen zu einem Internet-Gateway enthalten. Durch das Entfernen oder Beschränken des Internetzugangs für Workloads innerhalb von Amazon VPCs können unbeabsichtigte Zugriffe in Ihrer Umgebung reduziert werden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC.L1-3.13.1	Überwachen, kontrollieren und schützen Sie die Unternehmenskommunikation (d. h. Informationen, die von Informationssystemen der Organisation übertragen oder empfangen werden) an externen und wichtigen internen Grenzen der Informationssysteme.	rds-instance-public-access-überprüfen	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Relational Database Service (Amazon RDS) -Instances nicht öffentlich sind. Amazon-RDS-Datenbank-Instances können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC.L1-3.13.1	Überwachen, kontrollieren und schützen Sie die Unternehmenskommunikation (d. h. Informationen, die von Informationssystemen der Organisation übertragen oder empfangen werden) an externen und wichtigen internen Grenzen der Informationssysteme.	rds-snapshots-public-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Relational Database Service (Amazon RDS) -Instances nicht öffentlich sind. Amazon-RDS-Datenbank-Instances können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC.L1-3.13.1	Überwachen, kontrollieren und schützen Sie die Unternehmenskommunikation (d. h. Informationen, die von Informationssystemen der Organisation übertragen oder empfangen werden) an externen und wichtigen internen Grenzen der Informationssysteme.	redshift-cluster-public-access-überprüfen	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Redshift Redshift-Cluster nicht öffentlich sind. Amazon-Redshift-Cluster können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.
SC.L1-3.13.1	Überwachen, kontrollieren und schützen Sie die Unternehmenskommunikation (d. h. Informationen, die von Informationssystemen der Organisation übertragen oder empfangen werden) an externen und wichtigen internen Grenzen der Informationssysteme.	redshift-require-tls-ssl	Stellen Sie sicher, dass Ihre Amazon-Redshift-Cluster eine TLS/SSL-Verschlüsselung erfordern, um eine Verbindung zu SQL-Clients herzustellen. Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC.L1-3.13.1	Überwachen, kontrollieren und schützen Sie die Unternehmenskommunikation (d. h. Informationen, die von Informationssystemen der Organisation übertragen oder empfangen werden) an externen und wichtigen internen Grenzen der Informationssysteme.	restricted-common-ports	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass gemeinsame Ports für Amazon Elastic Compute Cloud (Amazon EC2) -Sicherheitsgruppen eingeschränkt sind. Wenn der Zugriff auf Ports nicht auf vertrauenswürdige Quellen beschränkt wird, kann dies zu Angriffen auf die Verfügbarkeit, Integrität und Vertraulichkeit von Systemen führen. Mit dieser Regel können Sie optional die Parameter blockedPort1–blockedPort5 festlegen (Standardkonfigurationen: 20, 21, 3389, 3306, 4333). Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC.L1-3.13.1	Überwachen, kontrollieren und schützen Sie die Unternehmenskommunikation (d. h. Informationen, die von Informationssystemen der Organisation übertragen oder empfangen werden) an externen und wichtigen internen Grenzen der Informationssysteme.	s3- account-level-public-access -blöcke-periodisch	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Simple Storage Service (Amazon S3) -Buckets nicht öffentlich zugänglich sind. Diese Regel trägt dazu bei, sensible Daten vor unbefugten Remote-Benutzern zu schützen, indem sie den öffentlichen Zugriff verhindert. Mit dieser Regel können Sie optional die Parameter ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) und restrictPublicBuckets Parameter (Config Default: True) festlegen. Die tatsächlichen Werte müssen den Richtlini

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			en Ihrer Organisation entsprechen.
SC.L1-3.13.1	Überwachen, kontrollieren und schützen Sie die Unternehmenskommunikation (d. h. Informationen, die von Informationssystemen der Organisation übertragen oder empfangen werden) an externen und wichtigen internen Grenzen der Informationssysteme.	s3 bucket-level-public-access - verboten	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Simple Storage Service (Amazon S3) -Buckets nicht öffentlich zugänglich sind. Diese Regel trägt dazu bei, sensible Daten vor unbefugten Remote-Benutzern zu schützen, indem sie den öffentlichen Zugriff auf Bucket-Ebene verhindert.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC.L1-3.13.1	Überwachen, kontrollieren und schützen Sie die Unternehmenskommunikation (d. h. Informationen, die von Informationssystemen der Organisation übertragen oder empfangen werden) an externen und wichtigen internen Grenzen der Informationssysteme.	s-3 bucket-public-read-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie nur autorisierten Benutzern, Prozessen und Geräten Zugriff auf Amazon Simple Storage Service (Amazon S3) - Buckets gewähren. Die Verwaltung des Zugriffs sollte mit der Klassifizierung der Daten übereinstimmen.
SC.L1-3.13.1	Überwachen, kontrollieren und schützen Sie die Unternehmenskommunikation (d. h. Informationen, die von Informationssystemen der Organisation übertragen oder empfangen werden) an externen und wichtigen internen Grenzen der Informationssysteme.	s3- bucket-public-write-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie nur autorisierten Benutzern, Prozessen und Geräten Zugriff auf Amazon Simple Storage Service (Amazon S3) - Buckets gewähren. Die Verwaltung des Zugriffs sollte mit der Klassifizierung der Daten übereinstimmen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC.L1-3.13.1	Überwachen, kontrollieren und schützen Sie die Unternehmenskommunikation (d. h. Informationen, die von Informationssystemen der Organisation übertragen oder empfangen werden) an externen und wichtigen internen Grenzen der Informationssysteme.	s3- bucket-ssl-requests-only	Um Daten während der Übertragung zu schützen, stellen Sie sicher, dass Ihre Amazon Simple Storage Service (Amazon S3)-Buckets Anfragen zur Verwendung von Secure Socket Layer (SSL)-Buckets erfordern. Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC.L1-3.13.1	Überwachen, kontrollieren und schützen Sie die Unternehmenskommunikation (d. h. Informationen, die von Informationssystemen der Organisation übertragen oder empfangen werden) an externen und wichtigen internen Grenzen der Informationssysteme.	sagemaker-notebook-no-direct-Internetzugang	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass SageMaker Amazon-Notebooks keinen direkten Internetzugang zulassen. Indem Sie direkten Internetzugang blockieren, vermeiden Sie, dass unbefugte Benutzer auf sensible Daten zugreifen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC.L1-3.13.1	Überwachen, kontrollieren und schützen Sie die Unternehmenskommunikation (d. h. Informationen, die von Informationssystemen der Organisation übertragen oder empfangen werden) an externen und wichtigen internen Grenzen der Informationssysteme.	securityhub-enabled	AWS Security Hub hilft bei der Überwachung von unbefugtem Personal, Verbindungen, Geräten und Software. AWS Security Hub aggregiert, organisiert und priorisiert die Sicherheitswarnungen oder Ergebnisse mehrerer Dienste. AWS Einige dieser Dienste sind Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer und AWS Firewall Manager sowie AWS Partnerlösungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC.L1-3.13.1	Überwachen, kontrollieren und schützen Sie die Unternehmenskommunikation (d. h. Informationen, die von Informationssystemen der Organisation übertragen oder empfangen werden) an externen und wichtigen internen Grenzen der Informationssysteme.	ssm-document-not-public	Stellen Sie sicher, dass AWS Systems Manager (SSM) - Dokumente nicht öffentlich sind, da dies einen unbeabsichtigten Zugriff auf Ihre SSM-Dokumente ermöglichen kann. Ein öffentliches SSM-Dokument kann Informationen über Ihr Konto, Ihre Ressourcen und internen Prozesse preisgeben.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC.L1-3.13.1	Überwachen, kontrollieren und schützen Sie die Unternehmenskommunikation (d. h. Informationen, die von Informationssystemen der Organisation übertragen oder empfangen werden) an externen und wichtigen internen Grenzen der Informationssysteme.	vpc-default-security-group-geschlossen	Sicherheitsgruppen von Amazon Elastic Compute Cloud (Amazon EC2) können bei der Verwaltung des Netzwerkzugriffs helfen, indem sie eine statusbehaftete Filterung des ein- und ausgehenden Netzwerkverkehrs zu Ressourcen bereitstellen. AWS Die Beschränkung des gesamten Datenverkehrs auf die Standardsicherheitsgruppe hilft dabei, den Fernzugriff auf Ihre Ressourcen einzuschränken. AWS

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC.L1-3.13.1	Überwachen, kontrollieren und schützen Sie die Unternehmenskommunikation (d. h. Informationen, die von Informationssystemen der Organisation übertragen oder empfangen werden) an externen und wichtigen internen Grenzen der Informationssysteme.	vpc-sg-open-only-to-authorized-ports	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass gemeinsame Ports für Amazon Elastic Compute Cloud (Amazon EC2) -Sicherheitsgruppen eingeschränkt sind. Wenn der Zugriff auf Ports nicht auf vertrauenswürdige Quellen beschränkt wird, kann dies zu Angriffen auf die Verfügbarkeit, Integrität und Vertraulichkeit von Systemen führen. Durch die Beschränkung des Zugriffs auf Ressourcen innerhalb einer Sicherheitsgruppe aus dem Internet (0.0.0.0/0) kann der Remote-Zugriff auf interne Systeme gesteuert werden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC.L1-3.13.1	Überwachen, kontrollieren und schützen Sie die Unternehmenskommunikation (d. h. Informationen, die von Informationssystemen der Organisation übertragen oder empfangen werden) an externen und wichtigen internen Grenzen der Informationssysteme.	opensearch-in-vpc-only	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass sich Amazon OpenSearch Service-Domains innerhalb einer Amazon Virtual Private Cloud (Amazon VPC) befinden. Eine Amazon OpenSearch Service-Domain innerhalb einer Amazon VPC ermöglicht die sichere Kommunikation zwischen Amazon OpenSearch Service und anderen Services innerhalb der Amazon VPC, ohne dass ein Internet-Gateway, ein NAT-Gerät oder eine VPN-Verbindung erforderlich ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC.L1-3.13.1	Überwachen, kontrollieren und schützen Sie die Unternehmenskommunikation (d. h. Informationen, die von Informationssystemen der Organisation übertragen oder empfangen werden) an externen und wichtigen internen Grenzen der Informationssysteme.	opensearch-node-to-node-Verschlüsselungsprüfung	Stellen Sie sicher, dass die node-to-node Verschlüsselung für Amazon OpenSearch Service aktiviert ist. Node-to-nodeVerschlüsselung ermöglicht die TLS 1.2-Verschlüsselung für die gesamte Kommunikation innerhalb der Amazon Virtual Private Cloud (Amazon VPC). Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SI.L1-3.14.1	Identifizieren, melden und korrigieren Sie Fehler in Informationen und Informationssystemen rechtzeitig.	cloudwatch-alarm-action-check	Amazon CloudWatch alarmiert, wenn eine Metrik den Schwellenwert für eine bestimmte Anzahl von Bewertungszeiträumen überschreitet. Der Alarm führt eine oder mehrere Aktionen durch, die vom Wert der Metrik oder des Ausdrucks im Vergleich zu einem Schwellenwert in einer Reihe von Zeiträumen abhängt. Diese Regel erfordert einen Wert für alarmActionRequired (Config Default: True), insufficientDataAction Required (Config Default: True), okActionRequired (Config Default: False). Der tatsächliche Wert muss die Alarmaktionen für Ihre Umgebung widerspiegeln.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SI.L1-3.14.1	Identifizieren, melden und korrigieren Sie Fehler in Informati onen und Informati onssystemen rechtzeit ig.	guardduty-enabled-centralized	Amazon GuardDuty kann mithilfe von Threat Intellige nce Feeds helfen, potenzielle Cybersich erheitsereignisse zu überwachen und zu erkennen. Dazu gehören Listen mit bösartigen IPs und maschinel len Lernmethoden zur Identifizierung unerwarteter, nicht autorisierter und bösartiger Aktivitäten in Ihrer AWS Cloud-Umgebung.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SI.L1-3.14.1	Identifizieren, melden und korrigieren Sie Fehler in Informati onen und Informati onssystemen rechtzeit ig.	securityhub-enabled	AWS Security Hub hilft bei der Überwachung von unbefugtem Personal, Verbindun gen, Geräten und Software. AWS Security Hub aggregiert, organisie rt und priorisie rt die Sicherhei tswarnungen oder Ergebnisse mehrerer Dienste. AWS Einige dieser Dienste sind Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer und AWS Firewall Manager sowie AWS Partnerlösungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SI.L1-3.14.2	Richten Sie Sicherheitsvorkehrungen zum Schutz vor schädlichem Code an geeigneten Stellen innerhalb der Informationssysteme der Organisation ein.	guardduty-enabled-centralized	Amazon GuardDuty kann mithilfe von Threat Intelligence Feeds helfen, potenzielle Cybersicherheitsereignisse zu überwachen und zu erkennen. Dazu gehören Listen mit bösartigen IPs und maschinellen Lernmethoden zur Identifizierung unerwarteter, nicht autorisierter und bösartiger Aktivitäten in Ihrer AWS Cloud-Umgebung.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SI.L1-3.14.5	Führen Sie während des Herunterladens, Öffnens und Ausführens von Dateien regelmäßige Scans des Informationssystems sowie Echtzeitscans von Dateien aus externen Quellen durch.	ecr-private-image-scanning-aktiviert	Der Amazon Elastic Container Repository (ECR)-Image-Scan unterstützt die Identifizierung von Software-Schwachstellen in Ihren Container-Images. Durch die Aktivierung von Image-Scans in ECR-Repositorys werden die Integrität und Sicherheit der gespeicherten Images mit einer zusätzlichen Überprüfungsebene verbessert.

Vorlage

Die Vorlage ist verfügbar unter GitHub: Operational Best Practices for CMMC 2.0 Level 1.

Bewährte Methoden für die Ausführung von CMMC 2.0 Level 2

Konformitätspakete bieten ein allgemeines Compliance-Framework, das es Ihnen ermöglicht, mithilfe verwalteter oder benutzerdefinierter Regeln und Abhilfemaßnahmen Kontrollen zur Sicherheits-, Betriebs- oder Kostenoptimierung durchzuführen. AWS Config AWS Config Conformance Packs dienen als Beispielvorlagen nicht dazu, die vollständige Einhaltung eines bestimmten Governance- oder Compliance-Standards sicherzustellen. Sie sind dafür verantwortlich, selbst zu beurteilen, ob Ihre Nutzung der Services den geltenden gesetzlichen und behördlichen Anforderungen entspricht.

Im Folgenden finden Sie ein Beispiel für eine Zuordnung zwischen der Cybersecurity Maturity Model Certification (CMMC) 2.0 Level 2 und den AWS verwalteten Konfigurationsregeln. Jede Config-Regel

gilt für eine bestimmte AWS Ressource und bezieht sich auf eine oder mehrere CMMC 2.0 Level 2-Steuerelemente. Eine CMMC-2.0-Level-2-Kontrolle kann mehreren Config-Regeln zugeordnet werden. In der folgenden Tabelle finden Sie weitere Informationen und Anleitungen zu diesen Zuordnungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC.L2-3.1.1	Beschränken Sie den Zugriff auf Informationssystem e auf autorisierte Benutzer, Prozesse von autorisierten Benutzern oder Geräte (einschließlich anderer Informati onssysteme).	access-keys-rotated	Die Anmeldein formationen für autorisierte Geräte, Benutzer und Prozesse werden geprüft, indem sichergestellt wird, dass die IAM-Zugri ffsschlüssel gemäß den Vorgaben der Unternehmensrichtl inie rotiert werden. Das regelmäßi ge Ändern der Zugriffsschlüssel ist eine bewährte Sicherheitsmethode . Es verkürzt den Zeitraum, in dem ein Zugriffsschlüssel aktiv ist, und reduziert die Auswirkungen auf das Unternehmen, wenn die Schlüssel kompromittiert werden. Diese Regel erfordert einen Wert für die Zugriffsschlüssel-

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			Rotation (Standard konfiguration: 90). Der tatsächliche Wert muss den Richtlini en Ihrer Organisation entsprechen.
AC.L2-3.1.1	Beschränken Sie den Zugriff auf Informationssystem e auf autorisierte Benutzer, Prozesse von autorisierten Benutzern oder Geräte (einschließlich anderer Informati onssysteme).	dms-replication-not-public	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass auf DMS-Replikationsin stanzen nicht öffentlic h zugegriffen werden kann. DMS-Repli kations-Instances können vertrauli che Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC.L2-3.1.1	Beschränken Sie den Zugriff auf Informationssystem e auf autorisierte Benutzer, Prozesse von autorisierten Benutzern oder Geräte (einschließlich anderer Informati onssysteme).	ebs-snapshot-public-restorable-überprüfen	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass EBS-Snapshots nicht öffentlich wiederher stellbar sind. EBS-Volume-Snapsho ts können vertrauli che Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC.L2-3.1.1	Beschränken Sie den Zugriff auf Informationssystem e auf autorisierte Benutzer, Prozesse von autorisierten Benutzern oder Geräte (einschließlich anderer Informati onssysteme).	ec2-imdsv2-check	Stellen Sie sicher, dass die Methode Instance Metadata Service Version 2 (IMDSv2) aktiviert ist, um den Zugriff auf und die Kontrolle der Amazon Elastic Compute Cloud (Amazon EC2) - Instance-Metadate n zu schützen. Die IMDSv2 Methode verwendet sitzungsb asierte Kontrollen. Mit können Kontrolle n implementiert werden IMDSv2, um Änderungen an Instanzmetadaten einzuschränken.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC.L2-3.1.1	Beschränken Sie den Zugriff auf Informationssystem e auf autorisierte Benutzer, Prozesse von autorisierten Benutzern oder Geräte (einschließlich anderer Informati onssysteme).	ec-2 instance-no-public-ip	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon Elastic Compute Cloud (Amazon EC2) - Instances nicht öffentlich zugänglich sind. EC2 Amazon-Instances können vertrauliche Informati onen enthalten, und für solche Konten ist eine Zugriffskontrolle erforderlich.
AC.L2-3.1.1	Beschränken Sie den Zugriff auf Informationssystem e auf autorisierte Benutzer, Prozesse von autorisierten Benutzern oder Geräte (einschließlich anderer Informati onssysteme).	ec-2 instance-profile-a ttached	EC2 Instanzprofile übergeben eine IAM-Rolle an eine EC2 Instance. Das Anhängen eines Instance-Profils an Ihre Instances kann bei der Implement ierung von geringste n Berechtigungen und der Berechtig ungsverwaltung helfen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC.L2-3.1.1	Beschränken Sie den Zugriff auf Informationssystem e auf autorisierte Benutzer, Prozesse von autorisierten Benutzern oder Geräte (einschließlich anderer Informati onssysteme).	elasticsearch-in-vpc-only	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherste llen, dass sich Amazon OpenSearc h OpenSearch Service (Service) - Domains innerhalb einer Amazon Virtual Private Cloud (Amazon VPC) befinden. Eine OpenSearch Service-Domain innerhalb einer Amazon VPC ermöglicht die sichere Kommunikation zwischen OpenSearc h Service und anderen Services innerhalb der Amazon VPC, ohne dass ein Internet-Gateway, ein NAT-Gerät oder eine VPN-Verbindung erforderlich ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC.L2-3.1.1	Beschränken Sie den Zugriff auf Informationssystem e auf autorisierte Benutzer, Prozesse von autorisierten Benutzern oder Geräte (einschließlich anderer Informati onssysteme).	emr-kerberos-enabled	Die Zugriffsberechtigu ngen und -autorisi erungen können verwaltet und nach den Prinzipien der geringsten Berechtig ung und Aufgabent rennung integrier t werden, indem Kerberos für Amazon-EMR-Cluster aktiviert wird. In Kerberos werden Services und Benutzer, die sich authentif izieren müssen, als Prinzipale bezeichnet. Prinzipal e befinden sich in einem Kerberos-Bereich. Innerhalb dieses Bereichs wird ein Kerberos-Server als Key Distribution Center (KDC) bezeichnet. Über diesen Server können sich Prinzipal e authentifizieren. Die Authentifizierung im KDC erfolgt durch die Ausstellu ng von Authentif

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			izierungstickets. Das KDC unterhält eine Datenbank der Prinzipale in seinem Bereich mit ihren Passwörtern und anderen administrativen Informationen zu jedem Prinzipal.
AC.L2-3.1.1	Beschränken Sie den Zugriff auf Informationssysteme auf autorisierte Benutzer, Prozesse von autorisierten Benutzern oder Geräte (einschließlich anderer Informationssysteme).	emr-master-no-public-ip	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon EMR-Cluster-Masterknoten nicht öffentlich zugänglich sind. Amazon-EMR-Cluster-Hauptknoten können vertrauliche Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC.L2-3.1.1	Beschränken Sie den Zugriff auf Informationssystem e auf autorisierte Benutzer, Prozesse von autorisierten Benutzern oder Geräte (einschließlich anderer Informati onssysteme).	iam-customer-policy-blocked-kms-Aktionen	AWS Identity and Access Managemen t (IAM) kann Ihnen helfen, die Prinzipien der geringsten Rechte und der Aufgabent rennung in Zugriffsb erechtigungen und Autorisierungen zu integrieren und so zu verhindern, dass Richtlinien blockiert e Aktionen für alle AWS Schlüssel des Key Management Service enthalten. Wenn Benutzer mehr Rechte haben, als für die Ausführung einer Aufgabe erforderl ich sind, kann dies gegen das Prinzip der geringsten Berechtig ung und Aufgabent rennung verstoßen . Mit dieser Regel können Sie den Parameter festlegen . blockedActionsPatt erns (Wert „AWS Bewährte grundlege nde Sicherhei tsmethoden“: kms:

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			Decrypt, kms:ReEncryptFrom). Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC.L2-3.1.1	Beschränken Sie den Zugriff auf Informationssystem e auf autorisierte Benutzer, Prozesse von autorisierten Benutzern oder Geräte (einschließlich anderer Informati onssysteme).	iam-inline-policy-blocked-kms-Aktionen	Stellen Sie sicher, dass ein Benutzer, eine IAM-Rolle oder eine IAM-Gruppe (AWS Identity and Access Management) nicht über eine Inline-Richtlinie verfügt, die blockierte Aktionen für alle AWS Schlüssel des Key Management Service zulässt. AWS empfiehlt, verwaltet e Richtlinien anstelle von Inline-Richtlinien zu verwenden. Verwaltete Richtlini en ermöglichen Wiederverwendbarke it, Versionsverwaltung , Rollback und Delegierung der Berechtigungsverwa ltung. Mit dieser Regel können Sie den blockedActionsPatt erns Parameter festlegen. (Wert „AWS Bewährte grundlege nde Sicherhei tsmethoden“: kms: Decrypt, kms:ReEnc ryptFrom). Die

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.
AC.L2-3.1.1	Beschränken Sie den Zugriff auf Informationssysteme auf autorisierte Benutzer, Prozesse von autorisierten Benutzern oder Geräte (einschließlich anderer Informationssysteme).	iam-no-inline-policy-überprüfen	Stellen Sie sicher, dass ein Benutzer, eine IAM-Rolle oder eine IAM-Gruppe (AWS Identity and Access Management) nicht über eine Inline-Richtlinie zur Zugriffskontrolle auf Systeme und Ressourcen verfügt. AWS empfiehlt, verwaltete Richtlinien anstelle von Inline-Richtlinien zu verwenden. Verwaltete Richtlinien ermöglichen Wiederverwendbarkeit, Versionsverwaltung, Rollback und Delegierung der Berechtigungsverwaltung.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC.L2-3.1.1	Beschränken Sie den Zugriff auf Informationssysteme auf autorisierte Benutzer, Prozesse von autorisierten Benutzern oder Geräte (einschließlich anderer Informationssysteme).	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) kann Ihnen dabei helfen, die Prinzipien der geringsten Rechte und der Aufgabentrennung in Zugriffsberechtigungen und Autorisierungen zu integrieren und so zu verhindern, dass Richtlinien „Effect“: „Allow“ mit „Action“: „*“ anstelle von „Resource“: „*“ enthalten. Wenn Benutzern mehr Rechte eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und der Aufgabentrennung verstoßen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC.L2-3.1.1	Beschränken Sie den Zugriff auf Informationssysteme auf autorisierte Benutzer, Prozesse von autorisierten Benutzern oder Geräte (einschließlich anderer Informationssysteme).	iam-policy-no-statements-with-full-access	Stellen Sie sicher, dass IAM-Aktionen nur auf die benötigten Aktionen beschränkt sind. Wenn Benutzern mehr Rechte eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und der Aufgabentrennung verstoßen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC.L2-3.1.1	Beschränken Sie den Zugriff auf Informationssystem e auf autorisierte Benutzer, Prozesse von autorisierten Benutzern oder Geräte (einschließlich anderer Informati onssysteme).	iam-root-access-key-überprüfen	Der Zugriff auf Systeme und Ressourcen kann gesteuert werden, indem überprüft wird, ob der Root-Benu tzer keine Zugriffss chlüssel mit seiner AWS Identity and Access Management (IAM) -Rolle verknüpft hat. Stellen Sie sicher, dass die Root-Zugr iffsschlüssel gelöscht werden. Erstellen und verwenden Sie stattdessen rollenbas ierte Funktionen, AWS-Konten um das Prinzip der geringste n Funktionalität zu berücksichtigen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC.L2-3.1.1	Beschränken Sie den Zugriff auf Informationssystem e auf autorisierte Benutzer, Prozesse von autorisierten Benutzern oder Geräte (einschließlich anderer Informati onssysteme).	iam-user-group-mem bership-überprüfen	AWS Identity and Access Managemen t (IAM) kann Ihnen helfen, Zugriffsb erechtigungen und Autorisierungen einzuschränken, indem sichergestellt wird, dass Benutzer Mitglieder mindesten s einer Gruppe sind. Wenn Benutzern mehr Berechtigungen eingeräumt werden, als für die Ausführun g einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringste n Berechtigung und Aufgabentrennung verstoßen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC.L2-3.1.1	Beschränken Sie den Zugriff auf Informationssystem e auf autorisierte Benutzer, Prozesse von autorisierten Benutzern oder Geräte (einschließlich anderer Informati onssysteme).	iam-user-mfa-enabled	Aktivieren Sie diese Regel, um den Zugriff auf Ressourcen in der Cloud einzuschr änken. AWS Diese Regel sorgt dafür, dass die Multi-Fak tor-Authentifizier ung (MFA) für alle Benutzer aktiviert ist. MFA sorgt für eine weitere Schutzebe ne zusätzlich zu den Anmeldeinformation en. Reduzieren Sie Fälle von kompromit tierten Konten, indem Sie MFA für Benutzer vorschreiben.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC.L2-3.1.1	Beschränken Sie den Zugriff auf Informationssystem e auf autorisierte Benutzer, Prozesse von autorisierten Benutzern oder Geräte (einschließlich anderer Informati onssysteme).	iam-user-no-policies-überprüfen	Diese Regel stellt sicher, dass AWS Identity and Access Management (IAM) -Richtlinien nur Gruppen oder Rollen zugewiese n werden, um den Zugriff auf Systeme und Ressourcen zu kontrollieren. Die Zuweisung von Berechtig ungen auf Gruppen- oder Rollenebene trägt dazu bei, die Wahrscheinlichkeit zu verringern, dass eine Identität übermäßige Berechtigungen erhält oder beibehält.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC.L2-3.1.1	Beschränken Sie den Zugriff auf Informationssystem e auf autorisierte Benutzer, Prozesse von autorisierten Benutzern oder Geräte (einschließlich anderer Informati onssysteme).	iam-user-unused-cr edentials-überprüfen	AWS Identity and Access Managemen t (IAM) kann Ihnen bei Zugriffsberechtigu ngen und Autorisie rungen helfen, indem es nach IAM-Passw örtern und Zugriffss chlüsseln sucht, die für einen bestimmte n Zeitraum nicht verwendet wurden. Wenn ungenutzte Anmeldeinformation en identifiziert werden, müssen Sie sie deaktivieren und/oder entfernen , da dies gegen das Prinzip der geringste n Berechtigung verstoßen könnte. Für diese Regel müssen Sie einen Wert für das maxCreden tialUsage Alter festlegen (Standard konfiguration: 90). Der tatsächliche Wert muss den Richtlini en Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC.L2-3.1.1	Beschränken Sie den Zugriff auf Informationssystem e auf autorisierte Benutzer, Prozesse von autorisierten Benutzern oder Geräte (einschließlich anderer Informati onssysteme).	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) Security Groups können bei der Verwaltung des Netzwerkzugriffs helfen, indem sie eine statusbeh aftete Filterung von eingehendem und ausgehendem Netzwerkverkehr zu Ressourcen bereitste llen. AWS Wenn Sie eingehenden (oder entfernten) Datenverk ehr von 0.0.0.0/0 bis Port 22 auf Ihren Ressourcen nicht zulassen, können Sie den Remote-Zugriff einschränken.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC.L2-3.1.1	Beschränken Sie den Zugriff auf Informationssystem e auf autorisierte Benutzer, Prozesse von autorisierten Benutzern oder Geräte (einschließlich anderer Informati onssysteme).	ec-2 instances-in-vpc	Stellen Sie Amazon Elastic Compute Cloud (Amazon EC2) -Instances innerhalb einer Amazon Virtual Private Cloud (Amazon VPC) bereit, um eine sichere Kommunika tion zwischen einer Instance und anderen Services innerhalb der Amazon VPC zu ermöglichen, ohne dass ein Internet-Gateway, ein NAT-Gerät oder eine VPN-Verbindung erforderlich ist. Der gesamte Datenverk ehr bleibt sicher in der AWS Cloud. Domains, die sich innerhalb einer VPC befinden, verfügen aufgrund ihrer logischen Isolierun g im Vergleich zu Domains mit öffentlic hen Endpunkten über eine zusätzlic he Sicherheitsebene. Weisen Sie EC2

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			Amazon-Instances einer Amazon-VPC zu, um den Zugriff ordnungsgemäß zu verwalten.
AC.L2-3.1.1	Beschränken Sie den Zugriff auf Informationssysteme auf autorisierte Benutzer, Prozesse von autorisierten Benutzern oder Geräte (einschließlich anderer Informationssysteme).	internet-gateway-authorized-vpc-nur	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Internet-Gateways nur mit autorisierter Amazon Virtual Private Cloud (Amazon VPC) verbunden sind. Internet-Gateways ermöglichen den bidirektionalen Internetzugang zur und von der Amazon VPC, was möglicherweise zu einem unbefugten Zugriff auf Amazon-VPC-Ressourcen führen kann.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC.L2-3.1.1	Beschränken Sie den Zugriff auf Informationssysteme auf autorisierte Benutzer, Prozesse von autorisierten Benutzern oder Geräte (einschließlich anderer Informationssysteme).	lambda-function-public-access-verboten	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass AWS Lambda-Funktionen nicht öffentlich zugänglich sind. Der öffentliche Zugriff kann möglicherweise die Verfügbarkeit von Ressourcen beeinträchtigen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC.L2-3.1.1	Beschränken Sie den Zugriff auf Informationssystem e auf autorisierte Benutzer, Prozesse von autorisierten Benutzern oder Geräte (einschließlich anderer Informati onssysteme).	lambda-inside-vpc	Stellen Sie AWS Lambda-Funktionen in einer Amazon Virtual Private Cloud (Amazon VPC) bereit, um eine sichere Kommunika tion zwischen einer Funktion und anderen Diensten innerhalb der Amazon VPC zu gewährleisten. Bei dieser Konfiguration sind kein Internet-Gateway, kein NAT-Gerät und keine VPN-Verbindung erforderlich. Der gesamte Datenverk ehr bleibt sicher in der Cloud. AWS Domains, die sich innerhalb einer VPC befinden, verfügen aufgrund ihrer logischen Isolierun g im Vergleich zu Domains mit öffentlic hen Endpunkten über eine zusätzliche Sicherheitsebene. Um den Zugriff ordnungsg emäß zu verwalten,

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			sollten AWS Lambda-Funktionen einer VPC zugewiesen werden.
AC.L2-3.1.1	Beschränken Sie den Zugriff auf Informationssysteme auf autorisierte Benutzer, Prozesse von autorisierten Benutzern oder Geräte (einschließlich anderer Informationssysteme).	mfa-enabled-for-iam-Konsolenzugriff	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass MFA für alle AWS Identity and Access Management (IAM) -Benutzer aktiviert ist, die über ein Konsolenkennwort verfügen. MFA sorgt für eine weitere Schutzebene zusätzlich zu den Anmeldeinformationen. Indem Sie MFA für Benutzer vorschreiben, können Sie Fälle kompromittierter Konten reduzieren und verhindern, dass unbefugte Benutzer auf vertrauliche Daten zugreifen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC.L2-3.1.1	Beschränken Sie den Zugriff auf Informationssystem e auf autorisierte Benutzer, Prozesse von autorisierten Benutzern oder Geräte (einschließlich anderer Informati onssysteme).	rds-instance-public-access-überprüfen	Verwalten Sie den Zugriff auf Ressource n in der AWS Cloud, indem Sie sicherste llen, dass Amazon Relational Database Service (Amazon RDS) -Instance s nicht öffentlic h sind. Amazon-RDS-Datenbank-Instances können vertrauliche Informati onen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC.L2-3.1.1	Beschränken Sie den Zugriff auf Informationssystem e auf autorisierte Benutzer, Prozesse von autorisierten Benutzern oder Geräte (einschließlich anderer Informati onssysteme).	rds-snapshots-public-prohibited	Verwalten Sie den Zugriff auf Ressource n in der AWS Cloud, indem Sie sicherste llen, dass Amazon Relational Database Service (Amazon RDS) -Instance s nicht öffentlic h sind. Amazon-RDS-Datenbank-Instances können vertrauliche Informati onen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC.L2-3.1.1	Beschränken Sie den Zugriff auf Informationssystem e auf autorisierte Benutzer, Prozesse von autorisierten Benutzern oder Geräte (einschließlich anderer Informati onssysteme).	redshift-cluster-public-access-überprüfen	Verwalten Sie den Zugriff auf Ressource n in der AWS Cloud, indem Sie sicherste llen, dass Amazon Redshift Redshift-Cluster nicht öffentlic h sind. Amazon-Re dshift-Cluster können vertrauliche Informati onen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC.L2-3.1.1	Beschränken Sie den Zugriff auf Informationssysteme auf autorisierte Benutzer, Prozesse von autorisierten Benutzern oder Geräte (einschließlich anderer Informationssysteme).	restricted-common-ports	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass gemeinsame Ports für Amazon Elastic Compute Cloud (Amazon EC2) -Sicherheitsgruppen eingeschränkt sind. Wenn der Zugriff auf Ports nicht auf vertrauenswürdige Quellen beschränkt wird, kann dies zu Angriffen auf die Verfügbarkeit, Integrität und Vertraulichkeit von Systemen führen. Mit dieser Regel können Sie optional die Parameter blockedPort1–blockedPort5 festlegen (Standardkonfigurationen: 20, 21, 3389, 3306, 4333). Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC.L2-3.1.1	Beschränken Sie den Zugriff auf Informationssysteme auf autorisierte Benutzer, Prozesse von autorisierten Benutzern oder Geräte (einschließlich anderer Informationssysteme).	root-account-hardware-mfa-aktiviert	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Hardware-MFA für den Root-Benutzer aktiviert ist. Der Stammbenutzer ist der AWS-Konto-Benutzer mit den meisten Berechtigungen. MFA sorgt für eine weitere Schutzebene zusätzlich zu den Anmeldeinformationen. Indem Sie MFA für den Root-Benutzer vorschreiben, können Sie die Anzahl AWS-Konten kompromittierter Benutzer reduzieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC.L2-3.1.1	Beschränken Sie den Zugriff auf Informationssystem e auf autorisierte Benutzer, Prozesse von autorisierten Benutzern oder Geräte (einschließlich anderer Informati onssysteme).	root-account-mfa-e nabled	Verwalten Sie den Zugriff auf Ressource n in der AWS Cloud, indem Sie sicherste llen, dass MFA für den Root-Benutzer aktiviert ist. Der Stammbenutzer ist der AWS-Konto-Benutzer mit den meisten Berechtig ungen. MFA sorgt für eine weitere Schutzebene zusätzlic h zu den Anmeldein formationen. Indem Sie MFA für den Root-Benutzer vorschrei ben, können Sie die Anzahl AWS-Konte n kompromittierter Benutzer reduzieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC.L2-3.1.1	Beschränken Sie den Zugriff auf Informationssystem e auf autorisierte Benutzer, Prozesse von autorisierten Benutzern oder Geräte (einschließlich anderer Informati onssysteme).	s3-Blöcke-periodisch account-level-public-access	Verwalten Sie den Zugriff auf Ressource n in der AWS Cloud, indem Sie sicherste llen, dass Amazon Simple Storage Service (Amazon S3) -Buckets nicht öffentlich zugänglic h sind. Diese Regel trägt dazu bei, sensible Daten vor unbefugten Remote-Benutzern zu schützen, indem sie den öffentlichen Zugriff verhinder t. Mit dieser Regel können Sie optional die Parameter ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) und restrictPublicBuck ets Parameter (Config Default: True) festlegen. Die tatsächlichen Werte müssen den Richtlini

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			en Ihrer Organisation entsprechen.
AC.L2-3.1.1	Beschränken Sie den Zugriff auf Informationssystem e auf autorisierte Benutzer, Prozesse von autorisierten Benutzern oder Geräte (einschließlich anderer Informati onssysteme).	s-3 bucket-policy-gran tee-check	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie s3_ bucket_policy_gran tee_check aktiviere n. Diese Regel prüft, ob der vom Amazon S3 S3-Bucket gewährte Zugriff durch die von Ihnen bereitgestellten AWS Principals, Verbundbe nutzer, Service Principals, IP-Adress en oder Amazon Virtual Private Cloud (Amazon VPC) IDs eingeschränkt ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC.L2-3.1.1	Beschränken Sie den Zugriff auf Informationssysteme auf autorisierte Benutzer, Prozesse von autorisierten Benutzern oder Geräte (einschließlich anderer Informationssysteme).	s-3 bucket-public-read-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie nur autorisierten Benutzern, Prozessen und Geräten Zugriff auf Amazon Simple Storage Service (Amazon S3) - Buckets gewähren. Die Verwaltung des Zugriffs sollte mit der Klassifizierung der Daten übereinstimmen.
AC.L2-3.1.1	Beschränken Sie den Zugriff auf Informationssysteme auf autorisierte Benutzer, Prozesse von autorisierten Benutzern oder Geräte (einschließlich anderer Informationssysteme).	s-3 bucket-public-write-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie nur autorisierten Benutzern, Prozessen und Geräten Zugriff auf Amazon Simple Storage Service (Amazon S3) - Buckets gewähren. Die Verwaltung des Zugriffs sollte mit der Klassifizierung der Daten übereinstimmen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC.L2-3.1.1	Beschränken Sie den Zugriff auf Informationssystem e auf autorisierte Benutzer, Prozesse von autorisierten Benutzern oder Geräte (einschließlich anderer Informati onssysteme).	sagemaker-notebook -no-direct-Interne tzugang	Verwalten Sie den Zugriff auf Ressource n in der AWS Cloud, indem Sie sicherste llen, dass SageMaker Amazon-Notebooks keinen direkten Internetzugang zulassen. Indem Sie direkten Internetz ugang blockieren, vermeiden Sie, dass unbefugte Benutzer auf sensible Daten zugreifen.
AC.L2-3.1.1	Beschränken Sie den Zugriff auf Informationssystem e auf autorisierte Benutzer, Prozesse von autorisierten Benutzern oder Geräte (einschließlich anderer Informati onssysteme).	secretsmanager-rot ation-enabled-check	Diese Regel stellt sicher, dass bei AWS Secrets Manager Manager-Geheimnissen die Rotation aktiviert ist. Die regelmäßige Rotation von Secrets kann den Zeitraum verkürzen, in dem ein Secret aktiv ist, und möglicherweise die Auswirkungen auf das Unternehmen verringern, falls das Secret kompromittiert wird.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC.L2-3.1.1	Beschränken Sie den Zugriff auf Informationssysteme auf autorisierte Benutzer, Prozesse von autorisierten Benutzern oder Geräte (einschließlich anderer Informationssysteme).	secretsmanager-scheduled-rotation-success-überprüfen	Diese Regel stellt sicher, dass AWS Secrets Manager Manager-Geheimnisse gemäß dem Rotationsplan erfolgreich rotiert wurden. Die regelmäßige Rotation von Secrets kann den Zeitraum verkürzen, in dem ein Secret aktiv ist, und möglicherweise die Auswirkungen auf das Unternehmen verringern, falls es kompromittiert wird.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC.L2-3.1.1	Beschränken Sie den Zugriff auf Informationssystem e auf autorisierte Benutzer, Prozesse von autorisierten Benutzern oder Geräte (einschließlich anderer Informati onssysteme).	ssm-document-not-p ublic	Stellen Sie sicher, dass AWS Systems Manager (SSM) - Dokumente nicht öffentlich sind, da dies einen unbeabsic htigten Zugriff auf Ihre SSM-Dokum ente ermöglichen kann. Ein öffentlic hes SSM-Dokum ent kann Informati onen über Ihr Konto, Ihre Ressourcen und internen Prozesse preisgeben.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC.L2-3.1.1	Beschränken Sie den Zugriff auf Informationssystem e auf autorisierte Benutzer, Prozesse von autorisierten Benutzern oder Geräte (einschließlich anderer Informati onssysteme).	vpc-default-security-group-geschlossen	Sicherheitsgruppen von Amazon Elastic Compute Cloud (Amazon EC2) können bei der Verwaltung des Netzwerkzugriffs helfen, indem sie eine statusbehaftete Filterung des ein- und ausgehenden Netzwerkverkehrs zu Ressourcen bereitstellen. AWS Die Beschränk ung des gesamten Datenverkehrs auf die Standardsicherheit sgruppe hilft dabei, den Fernzugriff auf Ihre Ressourcen einzuschränken. AWS

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC.L2-3.1.1	Beschränken Sie den Zugriff auf Informationssystem e auf autorisierte Benutzer, Prozesse von autorisierten Benutzern oder Geräte (einschließlich anderer Informati onssysteme).	vpc-sg-open-only-to-authorized-ports	Verwalten Sie den Zugriff auf Ressource n in der AWS Cloud, indem Sie sicherste llen, dass gemeinsam e Ports für Amazon Elastic Compute Cloud (Amazon EC2) -Sicherhe itsgruppen eingeschr ränkt sind. Wenn der Zugriff auf Ports nicht auf vertrauen swürdige Quellen beschränkt wird, kann dies zu Angriffen auf die Verfügbar keit, Integrität und Vertraulichkeit von Systemen führen. Durch die Beschränk ung des Zugriffs auf Ressourcen innerhalb einer Sicherhei tsgruppe aus dem Internet (0.0.0.0/0) kann der Remote-Zugriff auf interne Systeme gesteuert werden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC.L2-3.1.1	Beschränken Sie den Zugriff auf Informationssystem e auf autorisierte Benutzer, Prozesse von autorisierten Benutzern oder Geräte (einschließlich anderer Informati onssysteme).	opensearch-in-vpc-only	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass sich Amazon OpenSearch Service-Domains innerhalb einer Amazon Virtual Private Cloud (Amazon VPC) befinden. Eine Amazon OpenSearc h Service-Domain innerhalb einer Amazon VPC ermöglicht die sichere Kommunikation zwischen Amazon OpenSearch Service und anderen Services innerhalb der Amazon VPC, ohne dass ein Internet-Gateway, ein NAT-Gerät oder eine VPN-Verbindung erforderlich ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC.L2-3.1.2	Beschränken Sie den Zugriff auf das Informationssystem auf jene Transaktionen und Funktionen, die autorisierte Benutzer ausführen dürfen.	dms-replication-not-public	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass auf DMS-Replikationsinstanzen nicht öffentlich zugegriffen werden kann. DMS-Replikations-Instances können vertrauliche Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.
AC.L2-3.1.2	Beschränken Sie den Zugriff auf das Informationssystem auf jene Transaktionen und Funktionen, die autorisierte Benutzer ausführen dürfen.	ebs-snapshot-public-restorable-überprüfen	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass EBS-Snapshots nicht öffentlich wiederherstellbar sind. EBS-Volume-Snapshots können vertrauliche Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC.L2-3.1.2	Beschränken Sie den Zugriff auf das Informationssystem auf jene Transaktionen und Funktionen, die autorisierte Benutzer ausführen dürfen.	ec2-imdsv2-check	Stellen Sie sicher, dass die Methode Instance Metadata Service Version 2 (IMDSv2) aktiviert ist, um den Zugriff auf und die Kontrolle der Amazon Elastic Compute Cloud (Amazon EC2) - Instance-Metadaten zu schützen. Die IMDSv2 Methode verwendet sitzungsbasierte Kontrollen. Mit können Kontrollen implementiert werden IMDSv2, um Änderungen an Instanzmetadaten einzuschränken.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC.L2-3.1.2	Beschränken Sie den Zugriff auf das Informationssystem auf jene Transaktionen und Funktionen, die autorisierte Benutzer ausführen dürfen.	ec-2 instance-no-public-ip	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon Elastic Compute Cloud (Amazon EC2) - Instances nicht öffentlich zugänglich sind. EC2 Amazon-Instances können vertrauliche Informationen enthalten, und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC.L2-3.1.2	Beschränken Sie den Zugriff auf das Informationssystem auf jene Transaktionen und Funktionen, die autorisierte Benutzer ausführen dürfen.	elasticsearch-in-vpc-only	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass sich Amazon OpenSearch OpenSearch Service (Service) - Domains innerhalb einer Amazon Virtual Private Cloud (Amazon VPC) befinden. Eine OpenSearch Service-Domain innerhalb einer Amazon VPC ermöglicht die sichere Kommunikation zwischen OpenSearch Service und anderen Services innerhalb der Amazon VPC, ohne dass ein Internet-Gateway, ein NAT-Gerät oder eine VPN-Verbindung erforderlich ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC.L2-3.1.2	Beschränken Sie den Zugriff auf das Informationssystem auf jene Transaktionen und Funktionen, die autorisierte Benutzer ausführen dürfen.	emr-kerberos-enabled	Die Zugriffsberechtigungen und -autorisierungen können verwaltet und nach den Prinzipien der geringsten Berechtigung und Aufgabentrennung integriert werden, indem Kerberos für Amazon-EMR-Cluster aktiviert wird. In Kerberos werden Services und Benutzer, die sich authentifizieren müssen, als Prinzipale bezeichnet. Prinzipale befinden sich in einem Kerberos-Bereich. Innerhalb dieses Bereichs wird ein Kerberos-Server als Key Distribution Center (KDC) bezeichnet. Über diesen Server können sich Prinzipale authentifizieren. Die Authentifizierung im KDC erfolgt durch die Ausstellung von Authentif

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			izierungstickets. Das KDC unterhält eine Datenbank der Prinzipale in seinem Bereich mit ihren Passwörtern und anderen administrativen Informationen zu jedem Prinzipal.
AC.L2-3.1.2	Beschränken Sie den Zugriff auf das Informationssystem auf jene Transaktionen und Funktionen, die autorisierte Benutzer ausführen dürfen.	emr-master-no-public-ip	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon EMR-Cluster-Masterknoten nicht öffentlich zugänglich sind. Amazon-EMR-Cluster-Hauptknoten können vertrauliche Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC.L2-3.1.2	Beschränken Sie den Zugriff auf das Informationssystem auf jene Transaktionen und Funktionen, die autorisierte Benutzer ausführen dürfen.	iam-no-inline-policy-überprüfen	Stellen Sie sicher, dass ein Benutzer, eine IAM-Rolle oder eine IAM-Gruppe (AWS Identity and Access Management) nicht über eine Inline-Richtlinie zur Zugriffskontrolle auf Systeme und Ressourcen verfügt. AWS empfiehlt, verwaltete Richtlinien anstelle von Inline-Richtlinien zu verwenden. Verwaltete Richtlinien ermöglichen Wiederverwendbarkeit, Versionsverwaltung, Rollback und Delegierung der Berechtigungsverwaltung.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC.L2-3.1.2	Beschränken Sie den Zugriff auf das Informationssystem auf jene Transaktionen und Funktionen, die autorisierte Benutzer ausführen dürfen.	iam-password-policy	Die Identitäten und Anmeldeinformationen werden auf der Grundlage einer organisatorischen IAM-Passwortrichtlinie ausgestellt, verwaltet und verifiziert. Sie erfüllen oder übertreffen die Anforderungen von NIST SP 800-63 und dem Standard „Best Practices“ von AWS Foundational Security für Passwortstärke. Mit dieser Regel können Sie optional RequireUppercaseCharacters (Wert für AWS grundlegende Sicherheitsbewährte Methoden: wahr), RequireLowercaseCharacters (Wert für bewährte Methoden für AWS grundlegende Sicherheit: wahr), RequireSymbols (Wert für bewährte Methoden für AWS grundlegende Sicherheit:

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			wahr), RequireNumbers (Wert für bewährte Methoden für AWS grundlegende Sicherheit: wahr), MinimumPasswordLength (Wert für bewährte Methoden für AWS grundlegende Sicherheit: 14), PasswordReusePrevention (Wert für bewährte Methoden für AWS grundlegende Sicherheit: 24) und MaxPasswordAge (Wert für bewährte Methoden für AWS grundlegende Sicherheit: 90) für Ihr IAM festlegen Kennwortrichtlinie. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC.L2-3.1.2	Beschränken Sie den Zugriff auf das Informationssystem auf jene Transaktionen und Funktionen, die autorisierte Benutzer ausführen dürfen.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) kann Ihnen dabei helfen, die Prinzipien der geringsten Rechte und der Aufgabentrennung in Zugriffsberechtigungen und Autorisierungen zu integrieren und so zu verhindern, dass Richtlinien „Effect“: „Allow“ mit „Action“: „*“ anstelle von „Resource“: „*“ enthalten. Wenn Benutzern mehr Rechte eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und der Aufgabentrennung verstoßen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC.L2-3.1.2	Beschränken Sie den Zugriff auf das Informationssystem auf jene Transaktionen und Funktionen, die autorisierte Benutzer ausführen dürfen.	iam-root-access-key-überprüfen	Der Zugriff auf Systeme und Ressourcen kann gesteuert werden, indem überprüft wird, ob der Root-Benutzer keine Zugriffsschlüssel mit seiner AWS Identity and Access Management (IAM) -Rolle verknüpft hat. Stellen Sie sicher, dass die Root-Zugriffsschlüssel gelöscht werden. Erstellen und verwenden Sie stattdessen rollenbasierte Funktionen, AWS-Konten um das Prinzip der geringsten Funktionalität zu berücksichtigen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC.L2-3.1.2	Beschränken Sie den Zugriff auf das Informationssystem auf jene Transaktionen und Funktionen, die autorisierte Benutzer ausführen dürfen.	iam-user-group-membership-überprüfen	AWS Identity and Access Management (IAM) kann Ihnen helfen, Zugriffsberechtigungen und Autorisierungen einzuschränken, indem sichergestellt wird, dass Benutzer Mitglieder mindestens einer Gruppe sind. Wenn Benutzern mehr Berechtigungen eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und Aufgabentrennung verstoßen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC.L2-3.1.2	Beschränken Sie den Zugriff auf das Informationssystem auf jene Transaktionen und Funktionen, die autorisierte Benutzer ausführen dürfen.	iam-user-mfa-enabled	Aktivieren Sie diese Regel, um den Zugriff auf Ressourcen in der Cloud einzuschränken. AWS Diese Regel sorgt dafür, dass die Multi-Faktor-Authentifizierung (MFA) für alle Benutzer aktiviert ist. MFA sorgt für eine weitere Schutzebene zusätzlich zu den Anmeldeinformationen. Reduzieren Sie Fälle von kompromittierten Konten, indem Sie MFA für Benutzer vorschreiben.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC.L2-3.1.2	Beschränken Sie den Zugriff auf das Informationssystem auf jene Transaktionen und Funktionen, die autorisierte Benutzer ausführen dürfen.	iam-user-no-policies-überprüfen	Diese Regel stellt sicher, dass AWS Identity and Access Management (IAM)-Richtlinien nur Gruppen oder Rollen zugewiesen werden, um den Zugriff auf Systeme und Ressourcen zu kontrollieren. Die Zuweisung von Berechtigungen auf Gruppen- oder Rollenebene trägt dazu bei, die Wahrscheinlichkeit zu verringern, dass eine Identität übermäßige Berechtigungen erhält oder beibehält.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC.L2-3.1.2	Beschränken Sie den Zugriff auf das Informationssystem auf jene Transaktionen und Funktionen, die autorisierte Benutzer ausführen dürfen.	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) Security Groups können bei der Verwaltung des Netzwerkzugriffs helfen, indem sie eine statusbehaftete Filterung von eingehendem und ausgehendem Netzwerkverkehr zu Ressourcen bereitstellen. AWS Wenn Sie eingehenden (oder entfernten) Datenverkehr von 0.0.0.0/0 bis Port 22 auf Ihren Ressourcen nicht zulassen, können Sie den Remote-Zugriff einschränken.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC.L2-3.1.2	Beschränken Sie den Zugriff auf das Informationssystem auf jene Transaktionen und Funktionen, die autorisierte Benutzer ausführen dürfen.	ec-2 instances-in-vpc	Stellen Sie Amazon Elastic Compute Cloud (Amazon EC2) -Instances innerhalb einer Amazon Virtual Private Cloud (Amazon VPC) bereit, um eine sichere Kommunikation zwischen einer Instance und anderen Services innerhalb der Amazon VPC zu ermöglichen, ohne dass ein Internet-Gateway, ein NAT-Gerät oder eine VPN-Verbindung erforderlich ist. Der gesamte Datenverkehr bleibt sicher in der AWS Cloud. Domains, die sich innerhalb einer VPC befinden, verfügen aufgrund ihrer logischen Isolierung im Vergleich zu Domains mit öffentlichen Endpunkten über eine zusätzliche Sicherheitsebene. Weisen Sie EC2

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			Amazon-Instances einer Amazon-VPC zu, um den Zugriff ordnungsgemäß zu verwalten.
AC.L2-3.1.2	Beschränken Sie den Zugriff auf das Informationssystem auf jene Transaktionen und Funktionen, die autorisierte Benutzer ausführen dürfen.	internet-gateway-authorized-vpc-nur	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Internet-Gateways nur mit autorisierter Amazon Virtual Private Cloud (Amazon VPC) verbunden sind. Internet-Gateways ermöglichen den bidirektionalen Internetzugang zur und von der Amazon VPC, was möglicher weise zu einem unbefugten Zugriff auf Amazon-VPC-Ressourcen führen kann.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC.L2-3.1.2	Beschränken Sie den Zugriff auf das Informationssystem auf jene Transaktionen und Funktionen, die autorisierte Benutzer ausführen dürfen.	lambda-function-public-access-verboten	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass AWS Lambda-Funktionen nicht öffentlich zugänglich sind. Der öffentliche Zugriff kann möglicherweise die Verfügbarkeit von Ressourcen beeinträchtigen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC.L2-3.1.2	Beschränken Sie den Zugriff auf das Informationssystem auf jene Transaktionen und Funktionen, die autorisierte Benutzer ausführen dürfen.	lambda-inside-vpc	Stellen Sie AWS Lambda-Funktionen in einer Amazon Virtual Private Cloud (Amazon VPC) bereit, um eine sichere Kommunikation zwischen einer Funktion und anderen Diensten innerhalb der Amazon VPC zu gewährleisten. Bei dieser Konfiguration sind kein Internet-Gateway, kein NAT-Gerät und keine VPN-Verbindung erforderlich. Der gesamte Datenverkehr bleibt sicher in der Cloud. AWS Domains, die sich innerhalb einer VPC befinden, verfügen aufgrund ihrer logischen Isolierung im Vergleich zu Domains mit öffentlichen Endpunkten über eine zusätzliche Sicherheitsebene. Um den Zugriff ordnungsgemäß zu verwalten,

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			sollten AWS Lambda-Funktionen einer VPC zugewiesen werden.
AC.L2-3.1.2	Beschränken Sie den Zugriff auf das Informationssystem auf jene Transaktionen und Funktionen, die autorisierte Benutzer ausführen dürfen.	mfa-enabled-for-iam-Konsolenzugriff	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass MFA für alle AWS Identity and Access Management (IAM) -Benutzer aktiviert ist, die über ein Konsolenkennwort verfügen. MFA sorgt für eine weitere Schutzebene zusätzlich zu den Anmeldeinformationen. Indem Sie MFA für Benutzer vorschreiben, können Sie Fälle kompromittierter Konten reduzieren und verhindern, dass unbefugte Benutzer auf vertrauliche Daten zugreifen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC.L2-3.1.2	Beschränken Sie den Zugriff auf das Informationssystem auf jene Transaktionen und Funktionen, die autorisierte Benutzer ausführen dürfen.	rds-instance-public-access-überprüfen	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Relational Database Service (Amazon RDS) -Instances nicht öffentlich sind. Amazon-RDS-Datenbank-Instances können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC.L2-3.1.2	Beschränken Sie den Zugriff auf das Informationssystem auf jene Transaktionen und Funktionen, die autorisierte Benutzer ausführen dürfen.	rds-snapshots-public-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Relational Database Service (Amazon RDS) -Instances nicht öffentlich sind. Amazon-RDS-Datenbank-Instances können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC.L2-3.1.2	Beschränken Sie den Zugriff auf das Informationssystem auf jene Transaktionen und Funktionen, die autorisierte Benutzer ausführen dürfen.	redshift-cluster-public-access-überprüfen	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Redshift Redshift-Cluster nicht öffentlich sind. Amazon-Redshift-Cluster können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC.L2-3.1.2	Beschränken Sie den Zugriff auf das Informationssystem auf jene Transaktionen und Funktionen, die autorisierte Benutzer ausführen dürfen.	restricted-common-ports	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass gemeinsame Ports für Amazon Elastic Compute Cloud (Amazon EC2) -Sicherheitsgruppen eingeschränkt sind. Wenn der Zugriff auf Ports nicht auf vertrauenswürdige Quellen beschränkt wird, kann dies zu Angriffen auf die Verfügbarkeit, Integrität und Vertraulichkeit von Systemen führen. Mit dieser Regel können Sie optional die Parameter blockedPort1–blockedPort5 festlegen (Standardkonfigurationen: 20, 21, 3389, 3306, 4333). Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC.L2-3.1.2	Beschränken Sie den Zugriff auf das Informationssystem auf jene Transaktionen und Funktionen, die autorisierte Benutzer ausführen dürfen.	root-account-hardware-mfa-aktiviert	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Hardware-MFA für den Root-Benutzer aktiviert ist. Der Stammbenutzer ist der AWS-Konto-Benutzer mit den meisten Berechtigungen. MFA sorgt für eine weitere Schutzebene zusätzlich zu den Anmeldeinformationen. Indem Sie MFA für den Root-Benutzer vorschreiben, können Sie die Anzahl AWS-Konten kompromittierter Benutzer reduzieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC.L2-3.1.2	Beschränken Sie den Zugriff auf das Informationssystem auf jene Transaktionen und Funktionen, die autorisierte Benutzer ausführen dürfen.	root-account-mfa-enabled	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass MFA für den Root-Benutzer aktiviert ist. Der Stammbenutzer ist der AWS-Konto-Benutzer mit den meisten Berechtigungen. MFA sorgt für eine weitere Schutzebene zusätzlich zu den Anmeldeinformationen. Indem Sie MFA für den Root-Benutzer vorschreiben, können Sie die Anzahl AWS-Konten kompromittierter Benutzer reduzieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC.L2-3.1.2	Beschränken Sie den Zugriff auf das Informationssystem auf jene Transaktionen und Funktionen, die autorisierte Benutzer ausführen dürfen.	s3-Blöcke-periodisch account-level-public-access	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Simple Storage Service (Amazon S3) -Buckets nicht öffentlich zugänglich sind. Diese Regel trägt dazu bei, sensible Daten vor unbefugten Remote-Benutzern zu schützen, indem sie den öffentlichen Zugriff verhindert. Mit dieser Regel können Sie optional die Parameter ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) und restrictPublicBuckets Parameter (Config Default: True) festlegen. Die tatsächlichen Werte müssen den Richtlini

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			en Ihrer Organisation entsprechen.
AC.L2-3.1.2	Beschränken Sie den Zugriff auf das Informationssystem auf jene Transaktionen und Funktionen, die autorisierte Benutzer ausführen dürfen.	s-3 bucket-policy-grantee-check	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie s3_bucket_policy_grantee_check aktivieren. Diese Regel prüft, ob der vom Amazon S3 S3-Bucket gewährte Zugriff durch die von Ihnen bereitgestellten AWS Principals, Verbundbenutzer, Service Principals, IP-Adressen oder Amazon Virtual Private Cloud (Amazon VPC) IDs eingeschränkt ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC.L2-3.1.2	Beschränken Sie den Zugriff auf das Informationssystem auf jene Transaktionen und Funktionen, die autorisierte Benutzer ausführen dürfen.	s-3 bucket-public-read-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie nur autorisierten Benutzern, Prozessen und Geräten Zugriff auf Amazon Simple Storage Service (Amazon S3) - Buckets gewähren. Die Verwaltung des Zugriffs sollte mit der Klassifizierung der Daten übereinstimmen.
AC.L2-3.1.2	Beschränken Sie den Zugriff auf das Informationssystem auf jene Transaktionen und Funktionen, die autorisierte Benutzer ausführen dürfen.	s-3 bucket-public-write-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie nur autorisierten Benutzern, Prozessen und Geräten Zugriff auf Amazon Simple Storage Service (Amazon S3) - Buckets gewähren. Die Verwaltung des Zugriffs sollte mit der Klassifizierung der Daten übereinstimmen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC.L2-3.1.2	Beschränken Sie den Zugriff auf das Informationssystem auf jene Transaktionen und Funktionen, die autorisierte Benutzer ausführen dürfen.	sagemaker-notebook-no-direct-Internetzugang	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass SageMaker Amazon-Notebooks keinen direkten Internetzugang zulassen. Indem Sie direkten Internetzugang blockieren, vermeiden Sie, dass unbefugte Benutzer auf sensible Daten zugreifen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC.L2-3.1.2	Beschränken Sie den Zugriff auf das Informationssystem auf jene Transaktionen und Funktionen, die autorisierte Benutzer ausführen dürfen.	vpc-default-security-group-geschlossen	Sicherheitsgruppen von Amazon Elastic Compute Cloud (Amazon EC2) können bei der Verwaltung des Netzwerkzugriffs helfen, indem sie eine statusbehaftete Filterung des ein- und ausgehenden Netzwerkverkehrs zu Ressourcen bereitstellen. AWS Die Beschränkung des gesamten Datenverkehrs auf die Standardsicherheitsgruppe hilft dabei, den Fernzugriff auf Ihre Ressourcen einzuschränken. AWS

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC.L2-3.1.2	Beschränken Sie den Zugriff auf das Informationssystem auf jene Transaktionen und Funktionen, die autorisierte Benutzer ausführen dürfen.	vpc-sg-open-only-to-authorized-ports	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass gemeinsame Ports für Amazon Elastic Compute Cloud (Amazon EC2) -Sicherheitsgruppen eingeschränkt sind. Wenn der Zugriff auf Ports nicht auf vertrauenswürdige Quellen beschränkt wird, kann dies zu Angriffen auf die Verfügbarkeit, Integrität und Vertraulichkeit von Systemen führen. Durch die Beschränkung des Zugriffs auf Ressourcen innerhalb einer Sicherheitsgruppe aus dem Internet (0.0.0.0/0) kann der Remote-Zugriff auf interne Systeme gesteuert werden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC.L2-3.1.2	Beschränken Sie den Zugriff auf das Informationssystem auf jene Transaktionen und Funktionen, die autorisierte Benutzer ausführen dürfen.	opensearch-in-vpc-only	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass sich Amazon OpenSearch Service-Domains innerhalb einer Amazon Virtual Private Cloud (Amazon VPC) befinden. Eine Amazon OpenSearch Service-Domain innerhalb einer Amazon VPC ermöglicht die sichere Kommunikation zwischen Amazon OpenSearch Service und anderen Services innerhalb der Amazon VPC, ohne dass ein Internet-Gateway, ein NAT-Gerät oder eine VPN-Verbindung erforderlich ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC.L2-3.1.20	Überprüfen und kontrollieren/beschränken Sie die Verbindungen zu externen Informationssystemen und deren Nutzung.	alb-waf-enabled	Stellen Sie sicher, dass AWS WAF auf Elastic Load Balancers (ELB) aktiviert ist, um Webanwendungen zu schützen. Eine WAF trägt zum Schutz Ihrer Webanwendungen oder APIs vor gängigen Web-Exploits bei. Diese Web-Exploits können sich auf die Verfügbarkeit auswirken, die Sicherheit gefährden oder übermäßige Ressourcen in Ihrer Umgebung verbrauchen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC.L2-3.1.20	Überprüfen und kontrollieren/beschränken Sie die Verbindungen zu externen Informationssystemen und deren Nutzung.	autoscaling-launch-config-public-ip-deaktiviert	Wenn Sie Ihre Netzwerkschnittstellen mit einer öffentlichen IP-Adresse konfigurieren, sind die diesen Netzwerkschnittstellen zugehörigen Ressourcen über das Internet erreichbar. EC2 Ressourcen sollten nicht öffentlich zugänglich sein, da dies einen unbeabsichtigten Zugriff auf Ihre Anwendungen oder Server ermöglichen kann.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC.L2-3.1.20	Überprüfen und kontrollieren/beschränken Sie die Verbindungen zu externen Informationssystemen und deren Nutzung.	ec2- instance-no-public-ip	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon Elastic Compute Cloud (Amazon EC2) - Instances nicht öffentlich zugänglich sind. EC2 Amazon-Instances können vertrauliche Informationen enthalten, und für solche Konten ist eine Zugriffskontrolle erforderlich.
AC.L2-3.1.20	Überprüfen und kontrollieren/beschränken Sie die Verbindungen zu externen Informationssystemen und deren Nutzung.	emr-master-no-public-ip	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon EMR-Cluster-Masterknoten nicht öffentlich zugänglich sind. Amazon-EMR-Cluster-Hauptknoten können vertrauliche Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC.L2-3.1.20	Überprüfen und kontrollieren/beschränken Sie die Verbindungen zu externen Informationssystemen und deren Nutzung.	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) Security Groups können bei der Verwaltung des Netzwerkzugriffs helfen, indem sie eine statusbehaftete Filterung von eingehendem und ausgehendem Netzwerkverkehr zu Ressourcen bereitstellen. AWS Wenn Sie eingehenden (oder entfernten) Datenverkehr von 0.0.0.0/0 bis Port 22 auf Ihren Ressourcen nicht zulassen, können Sie den Remote-Zugriff einschränken.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC.L2-3.1.20	Überprüfen und kontrollieren/beschränken Sie die Verbindungen zu externen Informationssystemen und deren Nutzung.	internet-gateway-authorized-vpc-nur	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Internet-Gateways nur mit autorisierter Amazon Virtual Private Cloud (Amazon VPC) verbunden sind. Internet-Gateways ermöglichen den bidirektionalen Internetzugang zur und von der Amazon VPC, was möglicher weise zu einem unbefugten Zugriff auf Amazon-VPC-Ressourcen führen kann.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC.L2-3.1.20	Überprüfen und kontrollieren/beschränken Sie die Verbindungen zu externen Informationssystemen und deren Nutzung.	lambda-function-public-access-verboten	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass AWS Lambda-Funktionen nicht öffentlich zugänglich sind. Der öffentliche Zugriff kann möglicherweise die Verfügbarkeit von Ressourcen beeinträchtigen.
AC.L2-3.1.20	Überprüfen und kontrollieren/beschränken Sie die Verbindungen zu externen Informationssystemen und deren Nutzung.	no-unrestricted-route-to-igw	Stellen Sie sicher, dass EC2 Amazon-Routentabellen keine uneingeschränkten Routen zu einem Internet-Gateway enthalten. Durch das Entfernen oder Beschränken des Internetzugangs für Workloads innerhalb von Amazon VPCs können unbeabsichtigte Zugriffe in Ihrer Umgebung reduziert werden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC.L2-3.1.20	Überprüfen und kontrollieren/beschränken Sie die Verbindungen zu externen Informationssystemen und deren Nutzung.	rds-instance-public-access-überprüfen	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Relational Database Service (Amazon RDS) -Instances nicht öffentlich sind. Amazon-RDS-Datenbank-Instances können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC.L2-3.1.20	Überprüfen und kontrollieren/beschränken Sie die Verbindungen zu externen Informationssystemen und deren Nutzung.	redshift-cluster-public-access-überprüfen	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Redshift Redshift-Cluster nicht öffentlich sind. Amazon-Redshift-Cluster können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC.L2-3.1.20	Überprüfen und kontrollieren/beschränken Sie die Verbindungen zu externen Informationssystemen und deren Nutzung.	restricted-common-ports	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass gemeinsame Ports für Amazon Elastic Compute Cloud (Amazon EC2) -Sicherheitsgruppen eingeschränkt sind. Wenn der Zugriff auf Ports nicht auf vertrauenswürdige Quellen beschränkt wird, kann dies zu Angriffen auf die Verfügbarkeit, Integrität und Vertraulichkeit von Systemen führen. Mit dieser Regel können Sie optional die Parameter blockedPort1–blockedPort5 festlegen (Standardkonfigurationen: 20, 21, 3389, 3306, 4333). Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC.L2-3.1.20	Überprüfen und kontrollieren/beschränken Sie die Verbindungen zu externen Informationssystemen und deren Nutzung.	s3-Blöcke-periodisch account-level-public-access	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Simple Storage Service (Amazon S3) -Buckets nicht öffentlich zugänglich sind. Diese Regel trägt dazu bei, sensible Daten vor unbefugten Remote-Benutzern zu schützen, indem sie den öffentlichen Zugriff verhindert. Mit dieser Regel können Sie optional die Parameter ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) und restrictPublicBuckets Parameter (Config Default: True) festlegen. Die tatsächlichen Werte müssen den Richtlini

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			en Ihrer Organisation entsprechen.
AC.L2-3.1.20	Überprüfen und kontrollieren/beschränken Sie die Verbindungen zu externen Informationssystemen und deren Nutzung.	s-3 bucket-public-read-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie nur autorisierten Benutzern, Prozessen und Geräten Zugriff auf Amazon Simple Storage Service (Amazon S3) - Buckets gewähren. Die Verwaltung des Zugriffs sollte mit der Klassifizierung der Daten übereinstimmen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC.L2-3.1.20	Überprüfen und kontrollieren/beschränken Sie die Verbindungen zu externen Informationssystemen und deren Nutzung.	s-3 bucket-public-write-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie nur autorisierten Benutzern, Prozessen und Geräten Zugriff auf Amazon Simple Storage Service (Amazon S3) - Buckets gewähren. Die Verwaltung des Zugriffs sollte mit der Klassifizierung der Daten übereinstimmen.
AC.L2-3.1.20	Überprüfen und kontrollieren/beschränken Sie die Verbindungen zu externen Informationssystemen und deren Nutzung.	sagemaker-notebook-no-direct-Internet-Zugang	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass SageMaker Amazon-Notebooks keinen direkten Internetzugang zulassen. Indem Sie direkten Internetzugang blockieren, vermeiden Sie, dass unbefugte Benutzer auf sensible Daten zugreifen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC.L2-3.1.20	Überprüfen und kontrollieren/beschränken Sie die Verbindungen zu externen Informationssystemen und deren Nutzung.	ssm-document-not-public	Stellen Sie sicher, dass AWS Systems Manager (SSM) - Dokumente nicht öffentlich sind, da dies einen unbeabsichtigten Zugriff auf Ihre SSM-Dokumente ermöglichen kann. Ein öffentliches SSM-Dokument kann Informationen über Ihr Konto, Ihre Ressourcen und internen Prozesse preisgeben.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC.L2-3.1.20	Überprüfen und kontrollieren/beschränken Sie die Verbindungen zu externen Informationssystemen und deren Nutzung.	subnet-auto-assign-public-ip-deaktiviert	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon Virtual Private Cloud (VPC) -Subnetzen nicht automatisch eine öffentliche IP-Adresse zugewiesen wird. Amazon Elastic Compute Cloud (EC2) -Instances, die in Subnetzen gestartet werden, in denen dieses Attribut aktiviert ist, haben ihrer primären Netzwerkschnittstelle eine öffentliche IP-Adresse zugewiesen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC.L2-3.1.20	Überprüfen und kontrollieren/beschränken Sie die Verbindungen zu externen Informationssystemen und deren Nutzung.	vpc-default-security-group-geschlossen	Sicherheitsgruppen von Amazon Elastic Compute Cloud (Amazon EC2) können bei der Verwaltung des Netzwerkzugriffs helfen, indem sie eine statusbehaftete Filterung des ein- und ausgehenden Netzwerkverkehrs zu Ressourcen bereitstellen. AWS Die Beschränkung des gesamten Datenverkehrs auf die Standardsicherheitsgruppe hilft dabei, den Fernzugriff auf Ihre Ressourcen einzuschränken. AWS

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC.L2-3.1.20	Überprüfen und kontrollieren/beschränken Sie die Verbindungen zu externen Informationssystemen und deren Nutzung.	vpc-sg-open-only-to-authorized-ports	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass gemeinsame Ports für Amazon Elastic Compute Cloud (Amazon EC2) -Sicherheitsgruppen eingeschränkt sind. Wenn der Zugriff auf Ports nicht auf vertrauenswürdige Quellen beschränkt wird, kann dies zu Angriffen auf die Verfügbarkeit, Integrität und Vertraulichkeit von Systemen führen. Durch die Beschränkung des Zugriffs auf Ressourcen innerhalb einer Sicherheitsgruppe aus dem Internet (0.0.0.0/0) kann der Remote-Zugriff auf interne Systeme gesteuert werden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC.L2-3.1.3	Steuern Sie den CUI-Fluss gemäß den genehmigten Autorisierungen.	alb-waf-enabled	Stellen Sie sicher, dass AWS WAF auf Elastic Load Balancers (ELB) aktiviert ist, um Webanwendungen zu schützen. Eine WAF trägt zum Schutz Ihrer Webanwendungen oder APIs vor gängigen Web-Exploits bei. Diese Web-Exploits können sich auf die Verfügbarkeit auswirken, die Sicherheit gefährden oder übermäßige Ressourcen in Ihrer Umgebung verbrauchen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC.L2-3.1.3	Steuern Sie den CUI-Fluss gemäß den genehmigten Autorisierungen.	api-gw-associated-with-WAF	AWS Mit WAF können Sie eine Reihe von Regeln (als Web Access Control List (Web ACL) bezeichnet) konfigurieren, die Webanfragen auf der Grundlage von anpassbaren Websicherheitsregeln und -bedingungen, die Sie definieren, zulassen, blockieren oder zählen. Stellen Sie sicher, dass Ihre Amazon-API-Gateway-Stufe mit einer WAF-Web-ACL verknüpft ist, um sie vor böswilligen Angriffen zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC.L2-3.1.3	Steuern Sie den CUI-Fluss gemäß den genehmigten Autorisierungen.	autoscaling-launch-config-public-ip-deaktiviert	Wenn Sie Ihre Netzwerkschnittstellen mit einer öffentlichen IP-Adresse konfigurieren, sind die diesen Netzwerkschnittstellen zugehörigen Ressourcen über das Internet erreichbar. EC2 Ressourcen sollten nicht öffentlich zugänglich sein, da dies einen unbeabsichtigten Zugriff auf Ihre Anwendungen oder Server ermöglichen kann.
AC.L2-3.1.3	Steuern Sie den CUI-Fluss gemäß den genehmigten Autorisierungen.	dms-replication-not-public	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass auf DMS-Replikationsinstanzen nicht öffentlich zugegriffen werden kann. DMS-Replikations-Instances können vertrauliche Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC.L2-3.1.3	Steuern Sie den CUI-Fluss gemäß den genehmigten Autorisierungen.	ebs-snapshot-public-restorable-überprüfen	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass EBS-Snapshots nicht öffentlich wiederherstellbar sind. EBS-Volume-Snapshots können vertrauliche Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.
AC.L2-3.1.3	Steuern Sie den CUI-Fluss gemäß den genehmigten Autorisierungen.	ec-2 instance-no-public-ip	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon Elastic Compute Cloud (Amazon EC2) - Instances nicht öffentlich zugänglich sind. EC2 Amazon-Instances können vertrauliche Informationen enthalten, und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC.L2-3.1.3	Steuern Sie den CUI-Fluss gemäß den genehmigten Autorisierungen.	elasticsearch-in-vpc-only	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass sich Amazon OpenSearch OpenSearch Service (Service) - Domains innerhalb einer Amazon Virtual Private Cloud (Amazon VPC) befinden. Eine OpenSearch Service-Domain innerhalb einer Amazon VPC ermöglicht die sichere Kommunikation zwischen OpenSearch Service und anderen Services innerhalb der Amazon VPC, ohne dass ein Internet-Gateway, ein NAT-Gerät oder eine VPN-Verbindung erforderlich ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC.L2-3.1.3	Steuern Sie den CUI-Fluss gemäß den genehmigten Autorisierungen.	emr-master-no-public-ip	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon EMR-Cluster-Masterknoten nicht öffentlich zugänglich sind. Amazon-EMR-Cluster-Hauptknoten können vertrauliche Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC.L2-3.1.3	Steuern Sie den CUI-Fluss gemäß den genehmigten Autorisierungen.	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) Security Groups können bei der Verwaltung des Netzwerkzugriffs helfen, indem sie eine statusbehaftete Filterung von eingehendem und ausgehendem Netzwerkverkehr zu Ressourcen bereitstellen. AWS Wenn Sie eingehenden (oder entfernten) Datenverkehr von 0.0.0.0/0 bis Port 22 auf Ihren Ressourcen nicht zulassen, können Sie den Remote-Zugriff einschränken.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC.L2-3.1.3	Steuern Sie den CUI-Fluss gemäß den genehmigten Autorisierungen.	ec-2 instances-in-vpc	Stellen Sie Amazon Elastic Compute Cloud (Amazon EC2) -Instances innerhalb einer Amazon Virtual Private Cloud (Amazon VPC) bereit, um eine sichere Kommunikation zwischen einer Instance und anderen Services innerhalb der Amazon VPC zu ermöglichen, ohne dass ein Internet-Gateway, ein NAT-Gerät oder eine VPN-Verbindung erforderlich ist. Der gesamte Datenverkehr bleibt sicher in der AWS Cloud. Domains, die sich innerhalb einer VPC befinden, verfügen aufgrund ihrer logischen Isolierung im Vergleich zu Domains mit öffentlichen Endpunkten über eine zusätzliche Sicherheitsebene. Weisen Sie EC2

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			Amazon-Instances einer Amazon-VPC zu, um den Zugriff ordnungsgemäß zu verwalten.
AC.L2-3.1.3	Steuern Sie den CUI-Fluss gemäß den genehmigten Autorisierungen.	internet-gateway-authorized-vpc-nur	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Internet-Gateways nur mit autorisierter Amazon Virtual Private Cloud (Amazon VPC) verbunden sind. Internet-Gateways ermöglichen den bidirektionalen Internetzugang zur und von der Amazon VPC, was möglicher weise zu einem unbefugten Zugriff auf Amazon-VPC-Ressourcen führen kann.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC.L2-3.1.3	Steuern Sie den CUI-Fluss gemäß den genehmigten Autorisierungen.	lambda-function-public-access-verboten	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass AWS Lambda-Funktionen nicht öffentlich zugänglich sind. Der öffentliche Zugriff kann möglicherweise die Verfügbarkeit von Ressourcen beeinträchtigen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC.L2-3.1.3	Steuern Sie den CUI-Fluss gemäß den genehmigten Autorisierungen.	lambda-inside-vpc	Stellen Sie AWS Lambda-Funktionen in einer Amazon Virtual Private Cloud (Amazon VPC) bereit, um eine sichere Kommunikation zwischen einer Funktion und anderen Diensten innerhalb der Amazon VPC zu gewährleisten. Bei dieser Konfiguration sind kein Internet-Gateway, kein NAT-Gerät und keine VPN-Verbindung erforderlich. Der gesamte Datenverkehr bleibt sicher in der Cloud. AWS Domains, die sich innerhalb einer VPC befinden, verfügen aufgrund ihrer logischen Isolierung im Vergleich zu Domains mit öffentlichen Endpunkten über eine zusätzliche Sicherheitsebene. Um den Zugriff ordnungsgemäß zu verwalten,

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			sollten AWS Lambda-Funktionen einer VPC zugewiesen werden.
AC.L2-3.1.3	Steuern Sie den CUI-Fluss gemäß den genehmigten Autorisierungen.	no-unrestricted-route-to-igw	Stellen Sie sicher, dass EC2 Amazon-Routentabellen keine uneingeschränkten Routen zu einem Internet-Gateway enthalten. Durch das Entfernen oder Beschränken des Internetzugangs für Workloads innerhalb von Amazon VPCs können unbeabsichtigte Zugriffe in Ihrer Umgebung reduziert werden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC.L2-3.1.3	Steuern Sie den CUI-Fluss gemäß den genehmigten Autorisierungen.	rds-instance-public-access-überprüfen	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Relational Database Service (Amazon RDS) -Instances nicht öffentlich sind. Amazon-RDS-Datenbank-Instances können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC.L2-3.1.3	Steuern Sie den CUI-Fluss gemäß den genehmigten Autorisierungen.	rds-snapshots-public-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Relational Database Service (Amazon RDS) -Instances nicht öffentlich sind. Amazon-RDS-Datenbank-Instances können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC.L2-3.1.3	Steuern Sie den CUI-Fluss gemäß den genehmigten Autorisierungen.	redshift-cluster-public-access-überprüfen	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Redshift Redshift-Cluster nicht öffentlich sind. Amazon-Redshift-Cluster können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC.L2-3.1.3	Steuern Sie den CUI-Fluss gemäß den genehmigten Autorisierungen.	restricted-common-ports	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass gemeinsame Ports für Amazon Elastic Compute Cloud (Amazon EC2) -Sicherheitsgruppen eingeschränkt sind. Wenn der Zugriff auf Ports nicht auf vertrauenswürdige Quellen beschränkt wird, kann dies zu Angriffen auf die Verfügbarkeit, Integrität und Vertraulichkeit von Systemen führen. Mit dieser Regel können Sie optional die Parameter blockedPort1–blockedPort5 festlegen (Standardkonfigurationen: 20, 21, 3389, 3306, 4333). Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC.L2-3.1.3	Steuern Sie den CUI-Fluss gemäß den genehmigten Autorisierungen.	s3- account-level-public-access -blöcke-periodisch	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Simple Storage Service (Amazon S3) -Buckets nicht öffentlich zugänglich sind. Diese Regel trägt dazu bei, sensible Daten vor unbefugten Remote-Benutzern zu schützen, indem sie den öffentlichen Zugriff verhindert. Mit dieser Regel können Sie optional die Parameter ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) und restrictPublicBuckets Parameter (Config Default: True) festlegen. Die tatsächlichen Werte müssen den Richtlini

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			en Ihrer Organisation entsprechen.
AC.L2-3.1.3	Steuern Sie den CUI-Fluss gemäß den genehmigten Autorisierungen.	s3- bucket-public-read-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie nur autorisierten Benutzern, Prozessen und Geräten Zugriff auf Amazon Simple Storage Service (Amazon S3) - Buckets gewähren. Die Verwaltung des Zugriffs sollte mit der Klassifizierung der Daten übereinstimmen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC.L2-3.1.3	Steuern Sie den CUI-Fluss gemäß den genehmigten Autorisierungen.	s3- bucket-public-write-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie nur autorisierten Benutzern, Prozessen und Geräten Zugriff auf Amazon Simple Storage Service (Amazon S3) - Buckets gewähren. Die Verwaltung des Zugriffs sollte mit der Klassifizierung der Daten übereinstimmen.
AC.L2-3.1.3	Steuern Sie den CUI-Fluss gemäß den genehmigten Autorisierungen.	sagemaker-notebook-no-direct-Internetzugang	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass SageMaker Amazon-Notebooks keinen direkten Internetzugang zulassen. Indem Sie direkten Internetzugang blockieren, vermeiden Sie, dass unbefugte Benutzer auf sensible Daten zugreifen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC.L2-3.1.3	Steuern Sie den CUI-Fluss gemäß den genehmigten Autorisierungen.	ssm-document-not-public	Stellen Sie sicher, dass AWS Systems Manager (SSM) - Dokumente nicht öffentlich sind, da dies einen unbeabsichtigten Zugriff auf Ihre SSM-Dokumente ermöglichen kann. Ein öffentliches SSM-Dokument kann Informationen über Ihr Konto, Ihre Ressourcen und internen Prozesse preisgeben.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC.L2-3.1.3	Steuern Sie den CUI-Fluss gemäß den genehmigten Autorisierungen.	subnet-auto-assign-public-ip-deaktiviert	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon Virtual Private Cloud (VPC) -Subnetzen nicht automatisch eine öffentliche IP-Adresse zugewiesen wird. Amazon Elastic Compute Cloud (EC2) -Instances, die in Subnetzen gestartet werden, in denen dieses Attribut aktiviert ist, haben ihrer primären Netzwerkschnittstelle eine öffentliche IP-Adresse zugewiesen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC.L2-3.1.3	Steuern Sie den CUI-Fluss gemäß den genehmigten Autorisierungen.	vpc-default-security-group-geschlossen	Sicherheitsgruppen von Amazon Elastic Compute Cloud (Amazon EC2) können bei der Verwaltung des Netzwerkzugriffs helfen, indem sie eine statusbehaftete Filterung des ein- und ausgehenden Netzwerkverkehrs zu Ressourcen bereitstellen. AWS Die Beschränkung des gesamten Datenverkehrs auf die Standardsicherheitsgruppe hilft dabei, den Fernzugriff auf Ihre Ressourcen einzuschränken. AWS

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC.L2-3.1.3	Steuern Sie den CUI-Fluss gemäß den genehmigten Autorisierungen.	vpc-sg-open-only-to-authorized-ports	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass gemeinsame Ports für Amazon Elastic Compute Cloud (Amazon EC2) -Sicherheitsgruppen eingeschränkt sind. Wenn der Zugriff auf Ports nicht auf vertrauenswürdige Quellen beschränkt wird, kann dies zu Angriffen auf die Verfügbarkeit, Integrität und Vertraulichkeit von Systemen führen. Durch die Beschränkung des Zugriffs auf Ressourcen innerhalb einer Sicherheitsgruppe aus dem Internet (0.0.0.0/0) kann der Remote-Zugriff auf interne Systeme gesteuert werden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC.L2-3.1.3	Steuern Sie den CUI-Fluss gemäß den genehmigten Autorisierungen.	opensearch-in-vpc-only	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass sich Amazon OpenSearch Service-Domains innerhalb einer Amazon Virtual Private Cloud (Amazon VPC) befinden. Eine Amazon OpenSearch Service-Domain innerhalb einer Amazon VPC ermöglicht die sichere Kommunikation zwischen Amazon OpenSearch Service und anderen Services innerhalb der Amazon VPC, ohne dass ein Internet-Gateway, ein NAT-Gerät oder eine VPN-Verbindung erforderlich ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC.L2-3.1.4	Teilen Sie Aufgaben auf mehrere Personen auf, um das Risiko böswilliger Aktivitäten durch fehlende Absprache zu verringern.	emr-kerberos-enabled	Die Zugriffsberechtigungen und -autorisierungen können verwaltet und nach den Prinzipien der geringsten Berechtigung und Aufgabentrennung integriert werden, indem Kerberos für Amazon-EMR-Cluster aktiviert wird. In Kerberos werden Services und Benutzer, die sich authentifizieren müssen, als Prinzipale bezeichnet. Prinzipale befinden sich in einem Kerberos-Bereich. Innerhalb dieses Bereichs wird ein Kerberos-Server als Key Distribution Center (KDC) bezeichnet. Über diesen Server können sich Prinzipale authentifizieren. Die Authentifizierung im KDC erfolgt durch die Ausstellung von Authentif

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			izierungstickets. Das KDC unterhält eine Datenbank der Prinzipale in seinem Bereich mit ihren Passwörtern und anderen administr ativen Informationen zu jedem Prinzipal.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC.L2-3.1.4	Teilen Sie Aufgaben auf mehrere Personen auf, um das Risiko böswilliger Aktivitäten durch fehlende Absprache zu verringern.	iam-customer-policy-blocked-kms-Aktionen	AWS Identity and Access Management (IAM) kann Ihnen helfen, die Prinzipien der geringsten Rechte und der Aufgabentrennung in Zugriffsberechtigungen und Autorisierungen zu integrieren und so zu verhindern, dass Richtlinien blockierte Aktionen für alle AWS Schlüssel des Key Management Service enthalten. Wenn Benutzer mehr Rechte haben, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und Aufgabentrennung verstoßen. Mit dieser Regel können Sie den Parameter festlegen. blockedActionsPatterns (Wert „AWS Bewährte grundlegende Sicherheitsmethoden“: kms:

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			Decrypt, kms:ReEncryptFrom). Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.
AC.L2-3.1.4	Teilen Sie Aufgaben auf mehrere Personen auf, um das Risiko böswilliger Aktivitäten durch fehlende Absprache zu verringern.	iam-group-has-users-überprüfen	AWS Identity and Access Management (IAM) kann Ihnen helfen, die Prinzipien der geringsten Rechte und der Aufgabentrennung mit Zugriffsberechtigungen und Autorisierungen zu integrieren, indem sichergestellt wird, dass IAM-Gruppen mindestens einen Benutzer haben. Die Einteilung von Benutzern in Gruppen auf der Grundlage der ihnen zugewiesenen Berechtigungen oder ihrer Funktion ist eine Möglichkeit, das Prinzip der geringsten Berechtigung zu implementieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC.L2-3.1.4	Teilen Sie Aufgaben auf mehrere Personen auf, um das Risiko böswilliger Aktivität en durch fehlende Absprache zu verringern.	iam-no-inline-policy-überprüfen	Stellen Sie sicher, dass ein Benutzer, eine IAM-Rolle oder eine IAM-Gruppe (AWS Identity and Access Management) nicht über eine Inline-Richtlinie zur Zugriffsk ontrolle auf Systeme und Ressource n verfügt. AWS empfiehlt, verwaltet e Richtlinien anstelle von Inline-Richtlinien zu verwenden. Verwaltete Richtlini en ermöglichen Wiederverwendbarke it, Versionsverwaltung , Rollback und Delegierung der Berechtigungsverwa ltung.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC.L2-3.1.4	Teilen Sie Aufgaben auf mehrere Personen auf, um das Risiko böswilliger Aktivitäten durch fehlende Absprache zu verringern.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) kann Ihnen dabei helfen, die Prinzipien der geringsten Rechte und der Aufgabentrennung in Zugriffsberechtigungen und Autorisierungen zu integrieren und so zu verhindern, dass Richtlinien „Effect“: „Allow“ mit „Action“: „*“ anstelle von „Resource“: „*“ enthalten. Wenn Benutzern mehr Rechte eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und der Aufgabentrennung verstoßen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC.L2-3.1.4	Teilen Sie Aufgaben auf mehrere Personen auf, um das Risiko böswilliger Aktivitäten durch fehlende Absprache zu verringern.	iam-policy-no-statements-with-full-access	Stellen Sie sicher, dass IAM-Aktionen nur auf die benötigten Aktionen beschränkt sind. Wenn Benutzern mehr Rechte eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und der Aufgabentrennung verstoßen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC.L2-3.1.4	Teilen Sie Aufgaben auf mehrere Personen auf, um das Risiko böswilliger Aktivität en durch fehlende Absprache zu verringern.	iam-root-access-key-überprüfen	Der Zugriff auf Systeme und Ressourcen kann gesteuert werden, indem überprüft wird, ob der Root-Benu tzer keine Zugriffss chlüssel mit seiner AWS Identity and Access Management (IAM) -Rolle verknüpft hat. Stellen Sie sicher, dass die Root-Zugr iffsschlüssel gelöscht werden. Erstellen und verwenden Sie stattdessen rollenbas ierte Funktionen, AWS-Konten um das Prinzip der geringste n Funktionalität zu berücksichtigen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC.L2-3.1.4	Teilen Sie Aufgaben auf mehrere Personen auf, um das Risiko böswilliger Aktivitäten durch fehlende Absprache zu verringern.	iam-user-group-membership-überprüfen	AWS Identity and Access Management (IAM) kann Ihnen helfen, Zugriffsberechtigungen und Autorisierungen einzuschränken, indem sichergestellt wird, dass Benutzer Mitglieder mindestens einer Gruppe sind. Wenn Benutzern mehr Berechtigungen eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und Aufgabentrennung verstoßen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC.L2-3.1.4	Teilen Sie Aufgaben auf mehrere Personen auf, um das Risiko böswilliger Aktivität en durch fehlende Absprache zu verringern.	iam-user-no-policies-überprüfen	Diese Regel stellt sicher, dass AWS Identity and Access Management (IAM) -Richtlinien nur Gruppen oder Rollen zugewiese n werden, um den Zugriff auf Systeme und Ressourcen zu kontrollieren. Die Zuweisung von Berechtig ungen auf Gruppen- oder Rollenebene trägt dazu bei, die Wahrscheinlichkeit zu verringern, dass eine Identität übermäßige Berechtigungen erhält oder beibehält.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC.L2-3.1.4	Teilen Sie Aufgaben auf mehrere Personen auf, um das Risiko böswilliger Aktivität en durch fehlende Absprache zu verringern.	s3- bucket-policy-gran tee-check	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie s3_ bucket_policy_gran tee_check aktiviere n. Diese Regel prüft, ob der vom Amazon S3 S3-Bucket gewährte Zugriff durch die von Ihnen bereitgestellten AWS Principals, Verbundbe nutzer, Service Principals, IP-Adress en oder Amazon Virtual Private Cloud (Amazon VPC) IDs eingeschränkt ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC.L2-3.1.5	Wenden Sie das Prinzip der geringsten Berechtigung an, auch für spezifische Sicherheitsfunktionen und privilegierte Konten.	dms-replication-not-public	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass auf DMS-Replikationsinstanzen nicht öffentlich zugegriffen werden kann. DMS-Replikations-Instances können vertrauliche Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.
AC.L2-3.1.5	Wenden Sie das Prinzip der geringsten Berechtigung an, auch für spezifische Sicherheitsfunktionen und privilegierte Konten.	ebs-snapshot-public-restorable-überprüfen	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass EBS-Snapshots nicht öffentlich wiederherstellbar sind. EBS-Volume-Snapshots können vertrauliche Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC.L2-3.1.5	Wenden Sie das Prinzip der geringsten Berechtigung an, auch für spezifische Sicherheitsfunktionen und privilegierte Konten.	ec2-imdsv2-check	Stellen Sie sicher, dass die Methode Instance Metadata Service Version 2 (IMDSv2) aktiviert ist, um den Zugriff auf und die Kontrolle der Amazon Elastic Compute Cloud (Amazon EC2) - Instance-Metadaten zu schützen. Die IMDSv2 Methode verwendet sitzungsbasierte Kontrollen. Mit können Kontrollen implementiert werden IMDSv2, um Änderungen an Instanzmetadaten einzuschränken.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC.L2-3.1.5	Wenden Sie das Prinzip der geringsten Berechtigung an, auch für spezifische Sicherheitsfunktionen und privilegierte Konten.	ec-2 instance-no-public-ip	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon Elastic Compute Cloud (Amazon EC2) - Instances nicht öffentlich zugänglich sind. EC2 Amazon-Instances können vertrauliche Informationen enthalten, und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC.L2-3.1.5	Wenden Sie das Prinzip der geringsten Berechtigung an, auch für spezifische Sicherheitsfunktionen und privilegierte Konten.	elasticsearch-in-vpc-only	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass sich Amazon OpenSearch OpenSearch Service (Service) - Domains innerhalb einer Amazon Virtual Private Cloud (Amazon VPC) befinden. Eine OpenSearch Service-Domain innerhalb einer Amazon VPC ermöglicht die sichere Kommunikation zwischen OpenSearch Service und anderen Services innerhalb der Amazon VPC, ohne dass ein Internet-Gateway, ein NAT-Gerät oder eine VPN-Verbindung erforderlich ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC.L2-3.1.5	Wenden Sie das Prinzip der geringsten Berechtigung an, auch für spezifische Sicherheitsfunktionen und privilegierte Konten.	emr-kerberos-enabled	Die Zugriffsberechtigungen und -autorisierungen können verwaltet und nach den Prinzipien der geringsten Berechtigung und Aufgabentrennung integriert werden, indem Kerberos für Amazon-EMR-Cluster aktiviert wird. In Kerberos werden Services und Benutzer, die sich authentifizieren müssen, als Prinzipale bezeichnet. Prinzipale befinden sich in einem Kerberos-Bereich. Innerhalb dieses Bereichs wird ein Kerberos-Server als Key Distribution Center (KDC) bezeichnet. Über diesen Server können sich Prinzipale authentifizieren. Die Authentifizierung im KDC erfolgt durch die Ausstellung von Authentif

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			izierungstickets. Das KDC unterhält eine Datenbank der Prinzipale in seinem Bereich mit ihren Passwörtern und anderen administrativen Informationen zu jedem Prinzipal.
AC.L2-3.1.5	Wenden Sie das Prinzip der geringsten Berechtigung an, auch für spezifische Sicherheitsfunktionen und privilegierte Konten.	emr-master-no-public-ip	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon EMR-Cluster-Masterknoten nicht öffentlich zugänglich sind. Amazon-EMR-Cluster-Hauptknoten können vertrauliche Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC.L2-3.1.5	Wenden Sie das Prinzip der geringsten Berechtigung an, auch für spezifische Sicherheitsfunktionen und privilegierte Konten.	iam-customer-policy-blocked-kms-Aktionen	AWS Identity and Access Management (IAM) kann Ihnen helfen, die Prinzipien der geringsten Rechte und der Aufgabentrennung in Zugriffsberechtigungen und Autorisierungen zu integrieren und so zu verhindern, dass Richtlinien blockierte Aktionen für alle AWS Schlüssel des Key Management Service enthalten. Wenn Benutzer mehr Rechte haben, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und Aufgabentrennung verstoßen. Mit dieser Regel können Sie den Parameter festlegen. blockedActionsPatterns (Wert „AWS Bewährte grundlegende Sicherheitsmethoden“: kms:

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			Decrypt, kms:ReEncryptFrom). Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.
AC.L2-3.1.5	Wenden Sie das Prinzip der geringsten Berechtigung an, auch für spezifische Sicherheitsfunktionen und privilegierte Konten.	iam-group-has-users-überprüfen	AWS Identity and Access Management (IAM) kann Ihnen helfen, die Prinzipien der geringsten Rechte und der Aufgabentrennung mit Zugriffsberechtigungen und Autorisierungen zu integrieren, indem sichergestellt wird, dass IAM-Gruppen mindestens einen Benutzer haben. Die Einteilung von Benutzern in Gruppen auf der Grundlage der ihnen zugewiesenen Berechtigungen oder ihrer Funktion ist eine Möglichkeit, das Prinzip der geringsten Berechtigung zu implementieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC.L2-3.1.5	Wenden Sie das Prinzip der geringsten Berechtigung an, auch für spezifische Sicherheitsfunktionen und privilegierte Konten.	iam-inline-policy-blocked-kms-Aktionen	Stellen Sie sicher, dass ein Benutzer, eine IAM-Rolle oder eine IAM-Gruppe (AWS Identity and Access Management) nicht über eine Inline-Richtlinie verfügt, die blockierte Aktionen für alle AWS Schlüssel des Key Management Service zulässt. AWS empfiehlt, verwaltete Richtlinien anstelle von Inline-Richtlinien zu verwenden. Verwaltete Richtlinien ermöglichen Wiederverwendbarkeit, Versionsverwaltung, Rollback und Delegierung der Berechtigungsverwaltung. Mit dieser Regel können Sie den blockedActionsPatterns Parameter festlegen. (Wert „AWS Bewährte grundlegende Sicherheitsmethoden“: kms:Decrypt, kms:ReEncryptFrom). Die

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.
AC.L2-3.1.5	Wenden Sie das Prinzip der geringsten Berechtigung an, auch für spezifische Sicherheitsfunktionen und privilegierte Konten.	iam-no-inline-policy-überprüfen	Stellen Sie sicher, dass ein Benutzer, eine IAM-Rolle oder eine IAM-Gruppe (AWS Identity and Access Management) nicht über eine Inline-Richtlinie zur Zugriffskontrolle auf Systeme und Ressourcen verfügt. AWS empfiehlt, verwaltete Richtlinien anstelle von Inline-Richtlinien zu verwenden. Verwaltete Richtlinien ermöglichen Wiederverwendbarkeit, Versionsverwaltung, Rollback und Delegierung der Berechtigungsverwaltung.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC.L2-3.1.5	Wenden Sie das Prinzip der geringsten Berechtigung an, auch für spezifische Sicherheitsfunktionen und privilegierte Konten.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) kann Ihnen dabei helfen, die Prinzipien der geringsten Rechte und der Aufgabentrennung in Zugriffsberechtigungen und Autorisierungen zu integrieren und so zu verhindern, dass Richtlinien „Effect“: „Allow“ mit „Action“: „*“ anstelle von „Resource“: „*“ enthalten. Wenn Benutzern mehr Rechte eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und der Aufgabentrennung verstoßen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC.L2-3.1.5	Wenden Sie das Prinzip der geringsten Berechtigung an, auch für spezifische Sicherheitsfunktionen und privilegierte Konten.	iam-policy-no-statements-with-full-access	Stellen Sie sicher, dass IAM-Aktionen nur auf die benötigten Aktionen beschränkt sind. Wenn Benutzern mehr Rechte eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und der Aufgabentrennung verstoßen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC.L2-3.1.5	Wenden Sie das Prinzip der geringsten Berechtigung an, auch für spezifische Sicherheitsfunktionen und privilegierte Konten.	iam-root-access-key-überprüfen	Der Zugriff auf Systeme und Ressourcen kann gesteuert werden, indem überprüft wird, ob der Root-Benutzer keine Zugriffsschlüssel mit seiner AWS Identity and Access Management (IAM) -Rolle verknüpft hat. Stellen Sie sicher, dass die Root-Zugriffsschlüssel gelöscht werden. Erstellen und verwenden Sie stattdessen rollenbasierte Funktionen, AWS-Konten um das Prinzip der geringsten Funktionalität zu berücksichtigen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC.L2-3.1.5	Wenden Sie das Prinzip der geringsten Berechtigung an, auch für spezifische Sicherheitsfunktionen und privilegierte Konten.	iam-user-group-membership-überprüfen	AWS Identity and Access Management (IAM) kann Ihnen helfen, Zugriffsberechtigungen und Autorisierungen einzuschränken, indem sichergestellt wird, dass Benutzer Mitglieder mindestens einer Gruppe sind. Wenn Benutzern mehr Berechtigungen eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und Aufgabentrennung verstoßen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC.L2-3.1.5	Wenden Sie das Prinzip der geringsten Berechtigung an, auch für spezifische Sicherheitsfunktionen und privilegierte Konten.	iam-user-no-policies-überprüfen	Diese Regel stellt sicher, dass AWS Identity and Access Management (IAM) -Richtlinien nur Gruppen oder Rollen zugewiesen werden, um den Zugriff auf Systeme und Ressourcen zu kontrollieren. Die Zuweisung von Berechtigungen auf Gruppen- oder Rollenebene trägt dazu bei, die Wahrscheinlichkeit zu verringern, dass eine Identität übermäßige Berechtigungen erhält oder beibehält.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC.L2-3.1.5	Wenden Sie das Prinzip der geringsten Berechtigung an, auch für spezifische Sicherheitsfunktionen und privilegierte Konten.	internet-gateway-authorized-vpc-nur	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Internet-Gateways nur mit autorisierter Amazon Virtual Private Cloud (Amazon VPC) verbunden sind. Internet-Gateways ermöglichen den bidirektionalen Internetzugang zur und von der Amazon VPC, was möglicherweise zu einem unbefugten Zugriff auf Amazon-VPC-Ressourcen führen kann.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC.L2-3.1.5	Wenden Sie das Prinzip der geringsten Berechtigung an, auch für spezifische Sicherheitsfunktionen und privilegierte Konten.	lambda-function-public-access-verboten	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass AWS Lambda-Funktionen nicht öffentlich zugänglich sind. Der öffentliche Zugriff kann möglicherweise die Verfügbarkeit von Ressourcen beeinträchtigen.
AC.L2-3.1.5	Wenden Sie das Prinzip der geringsten Berechtigung an, auch für spezifische Sicherheitsfunktionen und privilegierte Konten.	rds-instance-public-access-überprüfen	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Relational Database Service (Amazon RDS) -Instances nicht öffentlich sind. Amazon-RDS-Datenbank-Instances können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC.L2-3.1.5	Wenden Sie das Prinzip der geringsten Berechtigung an, auch für spezifische Sicherheitsfunktionen und privilegierte Konten.	rds-snapshots-public-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Relational Database Service (Amazon RDS) -Instances nicht öffentlich sind. Amazon-RDS-Datenbank-Instances können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC.L2-3.1.5	Wenden Sie das Prinzip der geringsten Berechtigung an, auch für spezifische Sicherheitsfunktionen und privilegierte Konten.	redshift-cluster-public-access-überprüfen	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Redshift Redshift-Cluster nicht öffentlich sind. Amazon-Redshift-Cluster können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC.L2-3.1.5	Wenden Sie das Prinzip der geringsten Berechtigung an, auch für spezifische Sicherheitsfunktionen und privilegierte Konten.	s3- -Block-periodisch account-level-public-access	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Simple Storage Service (Amazon S3) -Buckets nicht öffentlich zugänglich sind. Diese Regel trägt dazu bei, sensible Daten vor unbefugten Remote-Benutzern zu schützen, indem sie den öffentlichen Zugriff verhindert. Mit dieser Regel können Sie optional die Parameter ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) und restrictPublicBuckets Parameter (Config Default: True) festlegen. Die tatsächlichen Werte müssen den Richtlini

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			en Ihrer Organisation entsprechen.
AC.L2-3.1.5	Wenden Sie das Prinzip der geringsten Berechtigung an, auch für spezifische Sicherheitsfunktionen und privilegierte Konten.	s3- bucket-policy-grantee-check	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie s3_bucket_policy_grantee_check aktivieren. Diese Regel prüft, ob der vom Amazon S3 S3-Bucket gewährte Zugriff durch die von Ihnen bereitgestellten AWS Principals, Verbundbenutzer, Service Principals, IP-Adressen oder Amazon Virtual Private Cloud (Amazon VPC) IDs eingeschränkt ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC.L2-3.1.5	Wenden Sie das Prinzip der geringsten Berechtigung an, auch für spezifische Sicherheitsfunktionen und privilegierte Konten.	s-3 bucket-public-read-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie nur autorisierten Benutzern, Prozessen und Geräten Zugriff auf Amazon Simple Storage Service (Amazon S3) - Buckets gewähren. Die Verwaltung des Zugriffs sollte mit der Klassifizierung der Daten übereinstimmen.
AC.L2-3.1.5	Wenden Sie das Prinzip der geringsten Berechtigung an, auch für spezifische Sicherheitsfunktionen und privilegierte Konten.	s3- bucket-public-write-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie nur autorisierten Benutzern, Prozessen und Geräten Zugriff auf Amazon Simple Storage Service (Amazon S3) - Buckets gewähren. Die Verwaltung des Zugriffs sollte mit der Klassifizierung der Daten übereinstimmen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC.L2-3.1.5	Wenden Sie das Prinzip der geringsten Berechtigung an, auch für spezifische Sicherheitsfunktionen und privilegierte Konten.	sagemaker-notebook-no-direct-Internetzugang	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass SageMaker Amazon-Notebooks keinen direkten Internetzugang zulassen. Indem Sie direkten Internetzugang blockieren, vermeiden Sie, dass unbefugte Benutzer auf sensible Daten zugreifen.
AC.L2-3.1.5	Wenden Sie das Prinzip der geringsten Berechtigung an, auch für spezifische Sicherheitsfunktionen und privilegierte Konten.	ssm-document-not-public	Stellen Sie sicher, dass AWS Systems Manager (SSM) - Dokumente nicht öffentlich sind, da dies einen unbeabsichtigten Zugriff auf Ihre SSM-Dokumente ermöglichen kann. Ein öffentliches SSM-Dokument kann Informationen über Ihr Konto, Ihre Ressourcen und internen Prozesse preisgeben.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC.L2-3.1.5	Wenden Sie das Prinzip der geringsten Berechtigung an, auch für spezifische Sicherheitsfunktionen und privilegierte Konten.	opensearch-in-vpc-only	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass sich Amazon OpenSearch Service-Domains innerhalb einer Amazon Virtual Private Cloud (Amazon VPC) befinden. Eine Amazon OpenSearch Service-Domain innerhalb einer Amazon VPC ermöglicht die sichere Kommunikation zwischen Amazon OpenSearch Service und anderen Services innerhalb der Amazon VPC, ohne dass ein Internet-Gateway, ein NAT-Gerät oder eine VPN-Verbindung erforderlich ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC.L2-3.1.6	Verwenden Sie Konten oder Rollen ohne Berechtigungen, wenn Sie auf nicht sicherheitsrelevante Funktionen zugreifen.	emr-kerberos-enabled	Die Zugriffsberechtigungen und -autorisierungen können verwaltet und nach den Prinzipien der geringsten Berechtigung und Aufgabentrennung integriert werden, indem Kerberos für Amazon-EMR-Cluster aktiviert wird. In Kerberos werden Services und Benutzer, die sich authentifizieren müssen, als Prinzipale bezeichnet. Prinzipale befinden sich in einem Kerberos-Bereich. Innerhalb dieses Bereichs wird ein Kerberos-Server als Key Distribution Center (KDC) bezeichnet. Über diesen Server können sich Prinzipale authentifizieren. Die Authentifizierung im KDC erfolgt durch die Ausstellung von Authentif

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			izierungstickets. Das KDC unterhält eine Datenbank der Prinzipale in seinem Bereich mit ihren Passwörtern und anderen administr ativen Informationen zu jedem Prinzipal.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC.L2-3.1.6	Verwenden Sie Konten oder Rollen ohne Berechtigungen, wenn Sie auf nicht sicherheitsrelevante Funktionen zugreifen.	iam-customer-policy-blocked-kms-Aktionen	AWS Identity and Access Managemen t (IAM) kann Ihnen helfen, die Prinzipien der geringsten Rechte und der Aufgabent rennung in Zugriffsb erechtigungen und Autorisierungen zu integrieren und so zu verhindern, dass Richtlinien blockiert e Aktionen für alle AWS Schlüssel des Key Management Service enthalten. Wenn Benutzer mehr Rechte haben, als für die Ausführung einer Aufgabe erforderl ich sind, kann dies gegen das Prinzip der geringsten Berechtig ung und Aufgabent rennung verstoßen . Mit dieser Regel können Sie den Parameter festlegen . blockedActionsPatt erns (Wert „AWS Bewährte grundlege nde Sicherhei tsmethoden“: kms:

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			Decrypt, kms:ReEncryptFrom). Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.
AC.L2-3.1.6	Verwenden Sie Konten oder Rollen ohne Berechtigungen, wenn Sie auf nicht sicherheitsrelevante Funktionen zugreifen.	iam-group-has-users-überprüfen	AWS Identity and Access Management (IAM) kann Ihnen helfen, die Prinzipien der geringsten Rechte und der Aufgabentrennung mit Zugriffsberechtigungen und Autorisierungen zu integrieren, indem sichergestellt wird, dass IAM-Gruppen mindestens einen Benutzer haben. Die Einteilung von Benutzern in Gruppen auf der Grundlage der ihnen zugewiesenen Berechtigungen oder ihrer Funktion ist eine Möglichkeit, das Prinzip der geringsten Berechtigung zu implementieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC.L2-3.1.6	Verwenden Sie Konten oder Rollen ohne Berechtigungen, wenn Sie auf nicht sicherheitsrelevante Funktionen zugreifen.	iam-inline-policy-blocked-kms-Aktionen	Stellen Sie sicher, dass ein Benutzer, eine IAM-Rolle oder eine IAM-Gruppe (AWS Identity and Access Management) nicht über eine Inline-Richtlinie verfügt, die blockierte Aktionen für alle AWS Schlüssel des Key Management Service zulässt. AWS empfiehlt, verwaltete Richtlinien anstelle von Inline-Richtlinien zu verwenden. Verwaltete Richtlinien ermöglichen Wiederverwendbarkeit, Versionsverwaltung, Rollback und Delegierung der Berechtigungsverwaltung. Mit dieser Regel können Sie den blockedActionsPatterns Parameter festlegen. (Wert „AWS Bewährte grundlegende Sicherheitsmethoden“: kms:Decrypt, kms:ReEncryptFrom). Die

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.
AC.L2-3.1.6	Verwenden Sie Konten oder Rollen ohne Berechtigungen, wenn Sie auf nicht sicherheitsrelevante Funktionen zugreifen.	iam-no-inline-policy-überprüfen	Stellen Sie sicher, dass ein Benutzer, eine IAM-Rolle oder eine IAM-Gruppe (AWS Identity and Access Management) nicht über eine Inline-Richtlinie zur Zugriffskontrolle auf Systeme und Ressourcen verfügt. AWS empfiehlt, verwaltete Richtlinien anstelle von Inline-Richtlinien zu verwenden. Verwaltete Richtlinien ermöglichen Wiederverwendbarkeit, Versionsverwaltung, Rollback und Delegierung der Berechtigungsverwaltung.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC.L2-3.1.6	Verwenden Sie Konten oder Rollen ohne Berechtigungen, wenn Sie auf nicht sicherheitsrelevante Funktionen zugreifen.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) kann Ihnen dabei helfen, die Prinzipien der geringsten Rechte und der Aufgabentrennung in Zugriffsberechtigungen und Autorisierungen zu integrieren und so zu verhindern, dass Richtlinien „Effect“: „Allow“ mit „Action“: „*“ anstelle von „Resource“: „*“ enthalten. Wenn Benutzern mehr Rechte eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und der Aufgabentrennung verstoßen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC.L2-3.1.6	Verwenden Sie Konten oder Rollen ohne Berechtigungen, wenn Sie auf nicht sicherheitsrelevante Funktionen zugreifen.	iam-policy-no-statements-with-full-access	Stellen Sie sicher, dass IAM-Aktionen nur auf die benötigten Aktionen beschränkt sind. Wenn Benutzern mehr Rechte eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und der Aufgabentrennung verstoßen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC.L2-3.1.6	Verwenden Sie Konten oder Rollen ohne Berechtigungen, wenn Sie auf nicht sicherheitsrelevante Funktionen zugreifen.	iam-root-access-key-überprüfen	Der Zugriff auf Systeme und Ressourcen kann gesteuert werden, indem überprüft wird, ob der Root-Benutzer keine Zugriffsschlüssel mit seiner AWS Identity and Access Management (IAM) -Rolle verknüpft hat. Stellen Sie sicher, dass die Root-Zugriffsschlüssel gelöscht werden. Erstellen und verwenden Sie stattdessen rollenbasierte Funktionen, AWS-Konten um das Prinzip der geringsten Funktionalität zu berücksichtigen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC.L2-3.1.6	Verwenden Sie Konten oder Rollen ohne Berechtigungen, wenn Sie auf nicht sicherheitsrelevante Funktionen zugreifen.	iam-user-group-membership-überprüfen	AWS Identity and Access Management (IAM) kann Ihnen helfen, Zugriffsberechtigungen und Autorisierungen einzuschränken, indem sichergestellt wird, dass Benutzer Mitglieder mindestens einer Gruppe sind. Wenn Benutzern mehr Berechtigungen eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und Aufgabentrennung verstoßen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC.L2-3.1.6	Verwenden Sie Konten oder Rollen ohne Berechtigungen, wenn Sie auf nicht sicherheitsrelevante Funktionen zugreifen.	iam-user-no-policies-überprüfen	Diese Regel stellt sicher, dass AWS Identity and Access Management (IAM) -Richtlinien nur Gruppen oder Rollen zugewiese n werden, um den Zugriff auf Systeme und Ressourcen zu kontrollieren. Die Zuweisung von Berechtig ungen auf Gruppen- oder Rollenebene trägt dazu bei, die Wahrscheinlichkeit zu verringern, dass eine Identität übermäßige Berechtigungen erhält oder beibehält.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC.L2-3.1.7	Verhindern Sie, dass Benutzer ohne Berechtigungen Funktionen ausführen, für die Berechtigungen erforderlich sind, und erfassen Sie die Ausführung solcher Funktionen in Prüfprotokollen.	api-gw-execution-logging-aktiviert	Die API-Gateway-Protokollierung zeigt detaillierte Ansichten der Benutzer, die auf die API zugegriffen haben, und wie diese Benutzer auf die API zugegriffen haben. Diese Einblicke ermöglichen die Transparenz von Benutzeraktivitäten.
AC.L2-3.1.7	Verhindern Sie, dass Benutzer ohne Berechtigungen Funktionen ausführen, für die Berechtigungen erforderlich sind, und erfassen Sie die Ausführung solcher Funktionen in Prüfprotokollen.	cloudtrail-s3-dataevents-enabled	Die Erfassung von Simple Storage Service (Amazon S3)-Datenereignissen unterstützt die Erkennung von ungewöhnlichen Aktivitäten. Zu den Details gehören AWS-Konto Informationen über den Zugriff auf einen Amazon S3 S3-Bucket, die IP-Adresse und die Uhrzeit des Ereignisses.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC.L2-3.1.7	Verhindern Sie, dass Benutzer ohne Berechtigungen Funktionen ausführen , für die Berechtig ungen erforderlich sind, und erfassen Sie die Ausführung solcher Funktionen in Prüfprotokollen.	cloud-trail-cloud-watch-logs-aktiviert	Verwenden Sie Amazon CloudWatc h , um Protokoll ereignisaktivitäten zentral zu sammeln und zu verwalten. Die Aufnahme von AWS CloudTrail Daten liefert Einzelheiten zu den API-Aufrufaktivitä ten in Ihrem AWS-Konto.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC.L2-3.1.7	Verhindern Sie, dass Benutzer ohne Berechtigungen Funktionen ausführen , für die Berechtig ungen erforderlich sind, und erfassen Sie die Ausführung solcher Funktionen in Prüfprotokollen.	cloudtrail-enabled	AWS CloudTrail kann bei der Nichtabst reitbarkeit helfen, indem Aktionen und API-Aufrufe der AWS Management Console aufgezeic hnet werden. Sie können die Benutzer und die Benutzer AWS-Konten , die einen AWS Dienst aufgerufen haben, die Quell-IP-Adresse, über die die Aufrufe generiert wurden, und den Zeitpunkt der Anrufe identifiz ieren. Einzelheiten zu den erfassten Daten finden Sie in den AWS CloudTrail Datensatzinhalten.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC.L2-3.1.7	Verhindern Sie, dass Benutzer ohne Berechtigungen Funktionen ausführen, für die Berechtigungen erforderlich sind, und erfassen Sie die Ausführung solcher Funktionen in Prüfprotokollen.	elb-logging-enabled	Die Elastic-Load-Balancing-Aktivität ist ein zentraler Kommunikationspunkt innerhalb einer Umgebung. Stellen Sie sicher, dass die ELB-Protokollierung aktiviert ist. Die gesammelten Daten enthalten detaillierte Informationen zu Anfragen, die an den ELB gesendet wurden. Jedes Protokoll enthält Informationen wie die Zeit, zu der die Anforderung einging, die Client-IP-Adresse, Latenzen, Anforderungspfade und Serverantworten.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC.L2-3.1.7	Verhindern Sie, dass Benutzer ohne Berechtigungen Funktionen ausführen, für die Berechtigungen erforderlich sind, und erfassen Sie die Ausführung solcher Funktionen in Prüfprotokollen.	emr-kerberos-enabled	Die Zugriffsberechtigungen und -autorisierungen können verwaltet und nach den Prinzipien der geringsten Berechtigung und Aufgabentrennung integriert werden, indem Kerberos für Amazon-EMR-Cluster aktiviert wird. In Kerberos werden Services und Benutzer, die sich authentifizieren müssen, als Prinzipale bezeichnet. Prinzipale befinden sich in einem Kerberos-Bereich. Innerhalb dieses Bereichs wird ein Kerberos-Server als Key Distribution Center (KDC) bezeichnet. Über diesen Server können sich Prinzipale authentifizieren. Die Authentifizierung im KDC erfolgt durch die Ausstellung von Authentif

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			izierungstickets. Das KDC unterhält eine Datenbank der Prinzipale in seinem Bereich mit ihren Passwörtern und anderen administr ativen Informationen zu jedem Prinzipal.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC.L2-3.1.7	Verhindern Sie, dass Benutzer ohne Berechtigungen Funktionen ausführen, für die Berechtigungen erforderlich sind, und erfassen Sie die Ausführung solcher Funktionen in Prüfprotokollen.	iam-customer-policy-blocked-kms-Aktionen	AWS Identity and Access Management (IAM) kann Ihnen helfen, die Prinzipien der geringsten Rechte und der Aufgabentrennung in Zugriffsberechtigungen und Autorisierungen zu integrieren und so zu verhindern, dass Richtlinien blockierte Aktionen für alle AWS Schlüssel des Key Management Service enthalten. Wenn Benutzer mehr Rechte haben, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und Aufgabentrennung verstoßen. Mit dieser Regel können Sie den Parameter festlegen. blockedActionsPatterns (Wert „AWS Bewährte grundlegende Sicherheitsmethoden“: kms:

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			Decrypt, kms:ReEncryptFrom). Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.
AC.L2-3.1.7	Verhindern Sie, dass Benutzer ohne Berechtigungen Funktionen ausführen, für die Berechtigungen erforderlich sind, und erfassen Sie die Ausführung solcher Funktionen in Prüfprotokollen.	iam-group-has-users-überprüfen	AWS Identity and Access Management (IAM) kann Ihnen helfen, die Prinzipien der geringsten Rechte und der Aufgabentrennung mit Zugriffsberechtigungen und Autorisierungen zu integrieren, indem sichergestellt wird, dass IAM-Gruppen mindestens einen Benutzer haben. Die Einteilung von Benutzern in Gruppen auf der Grundlage der ihnen zugewiesenen Berechtigungen oder ihrer Funktion ist eine Möglichkeit, das Prinzip der geringsten Berechtigung zu implementieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC.L2-3.1.7	Verhindern Sie, dass Benutzer ohne Berechtigungen Funktionen ausführen , für die Berechtig ungen erforderlich sind, und erfassen Sie die Ausführung solcher Funktionen in Prüfprotokollen.	iam-inline-policy-blocked-kms-Aktionen	Stellen Sie sicher, dass ein Benutzer, eine IAM-Rolle oder eine IAM-Gruppe (AWS Identity and Access Management) nicht über eine Inline-Richtlinie verfügt, die blockierte Aktionen für alle AWS Schlüssel des Key Management Service zulässt. AWS empfiehlt, verwaltet e Richtlinien anstelle von Inline-Richtlinien zu verwenden. Verwaltete Richtlini en ermöglichen Wiederverwendbarke it, Versionsverwaltung , Rollback und Delegierung der Berechtigungsverwa ltung. Mit dieser Regel können Sie den blockedActionsPatt erns Parameter festlegen. (Wert „AWS Bewährte grundlege nde Sicherhei tsmethoden“: kms: Decrypt, kms:ReEnc ryptFrom). Die

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.
AC.L2-3.1.7	Verhindern Sie, dass Benutzer ohne Berechtigungen Funktionen ausführen, für die Berechtigungen erforderlich sind, und erfassen Sie die Ausführung solcher Funktionen in Prüfprotokollen.	iam-no-inline-policy-überprüfen	Stellen Sie sicher, dass ein Benutzer, eine IAM-Rolle oder eine IAM-Gruppe (AWS Identity and Access Management) nicht über eine Inline-Richtlinie zur Zugriffskontrolle auf Systeme und Ressourcen verfügt. AWS empfiehlt, verwaltete Richtlinien anstelle von Inline-Richtlinien zu verwenden. Verwaltete Richtlinien ermöglichen Wiederverwendbarkeit, Versionsverwaltung, Rollback und Delegierung der Berechtigungsverwaltung.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC.L2-3.1.7	Verhindern Sie, dass Benutzer ohne Berechtigungen Funktionen ausführen, für die Berechtigungen erforderlich sind, und erfassen Sie die Ausführung solcher Funktionen in Prüfprotokollen.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) kann Ihnen dabei helfen, die Prinzipien der geringsten Rechte und der Aufgabentrennung in Zugriffsberechtigungen und Autorisierungen zu integrieren und so zu verhindern, dass Richtlinien „Effect“: „Allow“ mit „Action“: „*“ anstelle von „Resource“: „*“ enthalten. Wenn Benutzern mehr Rechte eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und der Aufgabentrennung verstoßen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC.L2-3.1.7	Verhindern Sie, dass Benutzer ohne Berechtigungen Funktionen ausführen, für die Berechtigungen erforderlich sind, und erfassen Sie die Ausführung solcher Funktionen in Prüfprotokollen.	iam-policy-no-statements-with-full-access	Stellen Sie sicher, dass IAM-Aktionen nur auf die benötigten Aktionen beschränkt sind. Wenn Benutzern mehr Rechte eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und der Aufgabentrennung verstoßen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC.L2-3.1.7	Verhindern Sie, dass Benutzer ohne Berechtigungen Funktionen ausführen , für die Berechtig ungen erforderlich sind, und erfassen Sie die Ausführung solcher Funktionen in Prüfprotokollen.	iam-root-access-key-überprüfen	Der Zugriff auf Systeme und Ressourcen kann gesteuert werden, indem überprüft wird, ob der Root-Benu tzer keine Zugriffss chlüssel mit seiner AWS Identity and Access Management (IAM) -Rolle verknüpft hat. Stellen Sie sicher, dass die Root-Zugr iffsschlüssel gelöscht werden. Erstellen und verwenden Sie stattdessen rollenbas ierte Funktionen, AWS-Konten um das Prinzip der geringste n Funktionalität zu berücksichtigen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC.L2-3.1.7	Verhindern Sie, dass Benutzer ohne Berechtigungen Funktionen ausführen, für die Berechtigungen erforderlich sind, und erfassen Sie die Ausführung solcher Funktionen in Prüfprotokollen.	iam-user-group-membership-überprüfen	AWS Identity and Access Management (IAM) kann Ihnen helfen, Zugriffsberechtigungen und Autorisierungen einzuschränken, indem sichergestellt wird, dass Benutzer Mitglieder mindestens einer Gruppe sind. Wenn Benutzern mehr Berechtigungen eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und Aufgabentrennung verstoßen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC.L2-3.1.7	Verhindern Sie, dass Benutzer ohne Berechtigungen Funktionen ausführen , für die Berechtig ungen erforderlich sind, und erfassen Sie die Ausführung solcher Funktionen in Prüfprotokollen.	iam-user-no-policies-überprüfen	Diese Regel stellt sicher, dass AWS Identity and Access Management (IAM) -Richtlinien nur Gruppen oder Rollen zugewiese n werden, um den Zugriff auf Systeme und Ressourcen zu kontrollieren. Die Zuweisung von Berechtig ungen auf Gruppen- oder Rollenebene trägt dazu bei, die Wahrscheinlichkeit zu verringern, dass eine Identität übermäßige Berechtigungen erhält oder beibehält.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC.L2-3.1.7	Verhindern Sie, dass Benutzer ohne Berechtigungen Funktionen ausführen , für die Berechtig ungen erforderlich sind, und erfassen Sie die Ausführung solcher Funktionen in Prüfprotokollen.	multi-region-cloudtrail-enabled	AWS CloudTrail zeichnet Aktionen und API-Aufrufe der AWS Management Console auf. Sie können feststellen, welche Benutzer und Konten angerufen wurden AWS, von welcher Quell-IP-Adresse aus die Anrufe getätigt wurden und wann die Anrufe erfolgten. CloudTrail übermittelt Protokolldateien aus allen AWS Regionen an Ihren S3-Bucket , wenn MULTI_REG ION_CLOUD _TRAIL_ENABLED aktiviert ist. Außerdem wird beim AWS Start einer neuen Region derselbe Trail in der neuen Region erstellt. CloudTrail Dadurch erhalten Sie automatis ch Protokolldateien mit API-Aktivitäten für die neue Region.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC.L2-3.1.7	Verhindern Sie, dass Benutzer ohne Berechtigungen Funktionen ausführen, für die Berechtigungen erforderlich sind, und erfassen Sie die Ausführung solcher Funktionen in Prüfprotokollen.	rds-logging-enabled	Um die Protokollierung und Überwachung in Ihrer Umgebung zu erleichtern, stellen Sie sicher, dass die Amazon Relational Database Service (Amazon RDS)-Protokollierung aktiviert ist. Mit der Amazon-RDS-Protokollierung können Sie Ereignisse wie Verbindungen, Verbindungsabbrüche, Abfragen oder abgefragte Tabellen erfassen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC.L2-3.1.7	Verhindern Sie, dass Benutzer ohne Berechtigungen Funktionen ausführen , für die Berechtig ungen erforderlich sind, und erfassen Sie die Ausführung solcher Funktionen in Prüfprotokollen.	s-3 bucket-logging-enabled	Die Amazon Simple Storage Service (Amazon S3)-Serverzugriffs protokollierung bietet eine Methode zur Überwachu ng des Netzwerks im Hinblick auf potenzielle Cybersich erheitsereignisse. Die Ereignisse werden überwacht, indem detaillierte Aufzeichn ungen über die Anfragen erfasst werden, die an einen Amazon-S3-Bucket gestellt wurden. Jeder Zugriffsprotokolle intrag enthält Details zu einer einzelnen Zugriffsanfrage. Zu den Details gehören Anforderer, Bucket-Name, Anforderu ngszeit, Anforderu ngsaktion, Antwortst atus und Fehlercode, falls relevant.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC.L2-3.1.7	Verhindern Sie, dass Benutzer ohne Berechtigungen Funktionen ausführen, für die Berechtigungen erforderlich sind, und erfassen Sie die Ausführung solcher Funktionen in Prüfprotokollen.	s-3 bucket-policy-grantee-check	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie s3_bucket_policy_grantee_check aktivieren. Diese Regel prüft, ob der vom Amazon S3 S3-Bucket gewährte Zugriff durch die von Ihnen bereitgestellten AWS Principals, Verbundbenutzer, Service Principals, IP-Adressen oder Amazon Virtual Private Cloud (Amazon VPC) IDs eingeschränkt ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC.L2-3.1.12	Überwachen und steuern Sie Remote-Zugriffssitzungen.	cloudwatch-alarm-action-check	Amazon CloudWatch alarmiert, wenn eine Metrik den Schwellenwert für eine bestimmte Anzahl von Bewertungszeiträumen überschreitet. Der Alarm führt eine oder mehrere Aktionen durch, die vom Wert der Metrik oder des Ausdrucks im Vergleich zu einem Schwellenwert in einer Reihe von Zeiträumen abhängt. Diese Regel erfordert einen Wert für alarmActionRequired (Config Default: True), insufficientDataAction Required (Config Default: True), okActionRequired (Config Default: False). Der tatsächliche Wert muss die Alarmaktionen für Ihre Umgebung widerspiegeln.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC.L2-3.1.12	Überwachen und steuern Sie Remote-Zugriffssitzungen.	cloud-trail-cloud-watch-logs-aktiviert	Verwenden Sie Amazon CloudWatch , um Protokoll ereignisaktivitäten zentral zu sammeln und zu verwalten. Die Aufnahme von AWS CloudTrail Daten liefert Einzelheiten zu den API-Aufrufaktivitäten in Ihrem AWS-Konto.
AC.L2-3.1.12	Überwachen und steuern Sie Remote-Zugriffssitzungen.	guardduty-enabled-centralized	Amazon GuardDuty kann mithilfe von Threat Intelligence Feeds helfen, potenzielle Cybersicherheitsereignisse zu überwachen und zu erkennen. Dazu gehören Listen mit bösartigen IPs und maschinellen Lernmethoden zur Identifizierung unerwarteter, nicht autorisierter und bösartiger Aktivitäten in Ihrer AWS Cloud-Umgebung.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC.L2-3.1.12	Überwachen und steuern Sie Remote-Zugriffssitzungen.	securityhub-enabled	AWS Security Hub hilft bei der Überwachung von unbefugtem Personal, Verbindungen, Geräten und Software. AWS Security Hub aggregiert, organisiert und priorisiert die Sicherheitswarnungen oder Ergebnisse mehrerer Dienste. AWS Einige dieser Dienste sind Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer und AWS Firewall Manager sowie AWS Partnerlösungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC.L2-3.1.13	Setzen Sie kryptografische Mechanismen ein, um die Vertraulichkeit von Remote-Zugriffssitzungen zu schützen.	acm-certificate-expiration-check	Stellen Sie sicher, dass die Netzwerkintegrität geschützt ist, indem Sie sicherstellen, dass X509-Zertifikate von ACM ausgestellt werden. AWS Diese Zertifikate müssen gültig und dürfen nicht abgelaufen sein. Für diese Regel ist ein Wert für erforderlich daysToExpiration (Wert für bewährte AWS Grundregeln für Sicherheit: 90). Der tatsächliche Wert muss den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC.L2-3.1.13	Setzen Sie kryptografische Mechanismen ein, um die Vertraulichkeit von Remote-Zugriffssitzungen zu schützen.	alb-http-to-https-Umleitungsprüfung	Um Daten während der Übertragung zu schützen, stellen Sie sicher, dass Ihr Application Load Balancer unverschlüsselte HTTP-Anfragen automatisch an HTTPS umleitet. Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.
AC.L2-3.1.13	Setzen Sie kryptografische Mechanismen ein, um die Vertraulichkeit von Remote-Zugriffssitzungen zu schützen.	api-gw-ssl-enabled	Stellen Sie sicher, dass die REST-API-Stufen von Amazon API Gateway mit SSL-Zertifikaten konfiguriert sind, damit Backend-Systeme überprüfen können, ob Anforderungen von API Gateway stammen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC.L2-3.1.13	Setzen Sie kryptografische Mechanismen ein, um die Vertraulichkeit von Remote-Zugriffssitzungen zu schützen.	elasticsearch-node-to-node-Verschlüsselungsprüfung	Stellen Sie sicher, dass die node-to-node Verschlüsselung für Amazon OpenSearch Service aktiviert ist. Node-to-nodeVerschlüsselung ermöglicht die TLS 1.2-Verschlüsselung für die gesamte Kommunikation innerhalb der Amazon Virtual Private Cloud (Amazon VPC). Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC.L2-3.1.13	Setzen Sie kryptografische Mechanismen ein, um die Vertraulichkeit von Remote-Zugriffssitzungen zu schützen.	elbv-2 acm-certificate-required	Zum Schutz von eventuell vorhandenen sensiblen Daten sowie von Daten während der Übertragung muss die Verschlüsselung für Ihr Elastic Load Balancing aktiviert sein. Verwenden Sie AWS Certificate Manager, um öffentliche und private SSL/TLS-Zertifikate mit AWS Diensten und internen Ressourcen zu verwalten, bereitzustellen und bereitzustellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC.L2-3.1.13	Setzen Sie kryptografische Mechanismen ein, um die Vertraulichkeit von Remote-Zugriffssitzungen zu schützen.	elb-acm-certificate-required	Zum Schutz von eventuell vorhandenen sensiblen Daten sowie von Daten während der Übertragung muss die Verschlüsselung für Ihr Elastic Load Balancing aktiviert sein. Verwenden Sie AWS Certificate Manager, um öffentliche und private SSL/TLS-Zertifikate mit AWS Diensten und internen Ressourcen zu verwalten, bereitzustellen und bereitzustellen.
AC.L2-3.1.13	Setzen Sie kryptografische Mechanismen ein, um die Vertraulichkeit von Remote-Zugriffssitzungen zu schützen.	elb-tls-https-listeners-nur	Stellen Sie sicher, dass Ihre Elastic Load Balancer (ELBs) mit SSL- oder HTTPS-Listenern konfiguriert sind. Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC.L2-3.1.13	Setzen Sie kryptografische Mechanismen ein, um die Vertraulichkeit von Remote-Zugriffssitzungen zu schützen.	redshift-require-tls-ssl	Stellen Sie sicher, dass Ihre Amazon-Redshift-Cluster eine TLS/SSL-Verschlüsselung erfordern, um eine Verbindung zu SQL-Clients herzustellen. Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.
AC.L2-3.1.13	Setzen Sie kryptografische Mechanismen ein, um die Vertraulichkeit von Remote-Zugriffssitzungen zu schützen.	s-3 bucket-ssl-requests-only	Um Daten während der Übertragung zu schützen, stellen Sie sicher, dass Ihre Amazon Simple Storage Service (Amazon S3)-Buckets Anfragen zur Verwendung von Secure Socket Layer (SSL)-Buckets erfordern. Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC.L2-3.1.13	Setzen Sie kryptografische Mechanismen ein, um die Vertraulichkeit von Remote-Zugriffssitzungen zu schützen.	opensearch-node-to-node-Verschlüsselungsprüfung	Stellen Sie sicher, dass die node-to-node Verschlüsselung für Amazon OpenSearch Service aktiviert ist. Node-to-nodeVerschlüsselung ermöglicht die TLS 1.2-Verschlüsselung für die gesamte Kommunikation innerhalb der Amazon Virtual Private Cloud (Amazon VPC). Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AU.L2-3.3.1	Erstellen und speichern Sie Systemüberwachungsprotokolle und Aufzeichnungen, soweit dies für die Überwachung, Analyse, Untersuchung und Meldung rechtswidriger oder nicht autorisierter Systemaktivitäten erforderlich ist.	api-gw-execution-logging-aktiviert	Die API-Gateway-Protokollierung zeigt detaillierte Ansichten der Benutzer, die auf die API zugegriffen haben, und wie diese Benutzer auf die API zugegriffen haben. Diese Einblicke ermöglichen die Transparenz von Benutzeraktivitäten.
AU.L2-3.3.1	Erstellen und speichern Sie Systemüberwachungsprotokolle und Aufzeichnungen, soweit dies für die Überwachung, Analyse, Untersuchung und Meldung rechtswidriger oder nicht autorisierter Systemaktivitäten erforderlich ist.	cloudtrail-s3-dataevents-enabled	Die Erfassung von Simple Storage Service (Amazon S3)-Datenereignissen unterstützt die Erkennung von ungewöhnlichen Aktivitäten. Zu den Details gehören AWS-Konto Informationen über den Zugriff auf einen Amazon S3 S3-Bucket, die IP-Adresse und die Uhrzeit des Ereignisses.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AU.L2-3.3.1	Erstellen und speichern Sie Systemüberwachungs protokolle und Aufzeichnungen, soweit dies für die Überwachung, Analyse, Untersuch ung und Meldung rechtswidriger oder nicht autorisierter Systemaktivitäten erforderlich ist.	cloud-trail-cloud-watch-logs-aktiviert	Verwenden Sie Amazon CloudWatc h , um Protokoll ereignisaktivitäten zentral zu sammeln und zu verwalten. Die Aufnahme von AWS CloudTrail Daten liefert Einzelheiten zu den API-Aufrufaktivitä ten in Ihrem AWS-Konto.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AU.L2-3.3.1	Erstellen und speichern Sie Systemüberwachungs protokolle und Aufzeichnungen, soweit dies für die Überwachung, Analyse, Untersuch ung und Meldung rechtswidriger oder nicht autorisierter Systemaktivitäten erforderlich ist.	cloudtrail-enabled	AWS CloudTrail kann bei der Nichtabst reitbarkeit helfen, indem Aktionen und API-Aufrufe der AWS Management Console aufgezeic hnet werden. Sie können die Benutzer und die Benutzer AWS-Konten , die einen AWS Dienst aufgerufen haben, die Quell-IP-Adresse, über die die Aufrufe generiert wurden, und den Zeitpunkt der Anrufe identifiz ieren. Einzelheiten zu den erfassten Daten finden Sie in den AWS CloudTrail Datensatzinhalten.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AU.L2-3.3.1	Erstellen und speichern Sie Systemüberwachungsprotokolle und Aufzeichnungen, soweit dies für die Überwachung, Analyse, Untersuchung und Meldung rechtswidriger oder nicht autorisierter Systemaktivitäten erforderlich ist.	cw-loggroup-retention-period-überprüfen	Stellen Sie sicher, dass die Ereignisprotokolldaten für Ihre Protokollgruppen über eine Mindestdauer aufbewahrt werden, um die Fehlerbehebung und forensische Untersuchungen zu unterstützen. Fehlende frühere Ereignisprotokolldaten erschweren die Rekonstruierung und Identifizierung potenziell schädlicher Ereignisse.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AU.L2-3.3.1	Erstellen und speichern Sie Systemüberwachungsprotokolle und Aufzeichnungen, soweit dies für die Überwachung, Analyse, Untersuchung und Meldung rechtswidriger oder nicht autorisierter Systemaktivitäten erforderlich ist.	elb-logging-enabled	Die Elastic-Load-Balancing-Aktivität ist ein zentraler Kommunikationspunkt innerhalb einer Umgebung. Stellen Sie sicher, dass die ELB-Protokollierung aktiviert ist. Die gesammelten Daten enthalten detaillierte Informationen zu Anfragen, die an den ELB gesendet wurden. Jedes Protokoll enthält Informationen wie die Zeit, zu der die Anforderung einging, die Client-IP-Adresse, Latenzen, Anforderungspfade und Serverantworten.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AU.L2-3.3.1	Erstellen und speichern Sie Systemüberwachungs protokolle und Aufzeichnungen, soweit dies für die Überwachung, Analyse, Untersuch ung und Meldung rechtswidriger oder nicht autorisierter Systemaktivitäten erforderlich ist.	multi-region-cloudtrail-enabled	AWS CloudTrail zeichnet Aktionen und API-Aufrufe der AWS Management Console auf. Sie können feststellen, welche Benutzer und Konten angerufen wurden AWS, von welcher Quell-IP-Adresse aus die Anrufe getätigt wurden und wann die Anrufe erfolgten. CloudTrail übermittelt Protokolldateien aus allen AWS Regionen an Ihren S3-Bucket , wenn MULTI_REG ION_CLOUD _TRAIL_ENABLED aktiviert ist. Außerdem wird beim AWS Start einer neuen Region derselbe Trail in der neuen Region erstellt. CloudTrail Dadurch erhalten Sie automatis ch Protokolldateien mit API-Aktivitäten für die neue Region.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AU.L2-3.3.1	Erstellen und speichern Sie Systemüberwachungsprotokolle und Aufzeichnungen, soweit dies für die Überwachung, Analyse, Untersuchung und Meldung rechtswidriger oder nicht autorisierter Systemaktivitäten erforderlich ist.	rds-logging-enabled	Um die Protokollierung und Überwachung in Ihrer Umgebung zu erleichtern, stellen Sie sicher, dass die Amazon Relational Database Service (Amazon RDS)-Protokollierung aktiviert ist. Mit der Amazon-RDS-Protokollierung können Sie Ereignisse wie Verbindungen, Verbindungsabbrüche, Abfragen oder abgefragte Tabellen erfassen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AU.L2-3.3.1	Erstellen und speichern Sie Systemüberwachungs protokolle und Aufzeichnungen, soweit dies für die Überwachung, Analyse, Untersuch ung und Meldung rechtswidriger oder nicht autorisierter Systemaktivitäten erforderlich ist.	s-3 bucket-logging-enabled	Die Amazon Simple Storage Service (Amazon S3)-Serverzugriffs protokollierung bietet eine Methode zur Überwachu ng des Netzwerks im Hinblick auf potenzielle Cybersich erheitsereignisse. Die Ereignisse werden überwacht, indem detaillierte Aufzeichn ungen über die Anfragen erfasst werden, die an einen Amazon-S3-Bucket gestellt wurden. Jeder Zugriffsprotokolle intrag enthält Details zu einer einzelnen Zugriffsanfrage. Zu den Details gehören Anforderer, Bucket-Name, Anforderu ngszeit, Anforderu ngsaktion, Antwortst atus und Fehlercode, falls relevant.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AU.L2-3.3.1	Erstellen und speichern Sie Systemüberwachungsprotokolle und Aufzeichnungen, soweit dies für die Überwachung, Analyse, Untersuchung und Meldung rechtswidriger oder nicht autorisierter Systemaktivitäten erforderlich ist.	wafv2-logging-enabled	Um die Protokollierung und Überwachung in Ihrer Umgebung zu erleichtern, aktivieren Sie die AWS WAF (V2) -Protokollierung im regionalen und globalen Web ACLs. AWS Die WAF-Protokollierung bietet detaillierte Informationen über den Datenverkehr, der von Ihrer Web-ACL analysiert wird. In den Protokollen werden die Uhrzeit aufgezeichnet, zu der die AWS WAF die Anfrage von Ihrer AWS Ressource erhalten hat, Informationen über die Anfrage und eine Aktion für die Regel, der jede Anfrage entsprach.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AU.L2-3.3.2	Stellen Sie sicher, dass die Aktionen einzelner Systemben utzer eindeutig auf diese Benutzer zurückgeführt werden können, sodass sie für ihre Aktionen zur Rechenschaft gezogen werden können.	api-gw-execution-l ogging-aktiviert	Die API-Gateway-Protokollierung zeigt detaillierte Ansichten der Benutzer, die auf die API zugegriff en haben, und wie diese Benutzer auf die API zugegriff en haben. Diese Einblicke ermöglichen die Transparenz von Benutzeraktivitäten.
AU.L2-3.3.2	Stellen Sie sicher, dass die Aktionen einzelner Systemben utzer eindeutig auf diese Benutzer zurückgeführt werden können, sodass sie für ihre Aktionen zur Rechenschaft gezogen werden können.	cloudtrail-s3-data events-enabled	Die Erfassung von Simple Storage Service (Amazon S3)-Datenereigniss en unterstützt die Erkennung von ungewöhnlichen Aktivitäten. Zu den Details gehören AWS-Konto Informationen über den Zugriff auf einen Amazon S3 S3-Bucket, die IP-Adress e und die Uhrzeit des Ereignisses.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AU.L2-3.3.2	Stellen Sie sicher, dass die Aktionen einzelner Systemben utzer eindeutig auf diese Benutzer zurückgeführt werden können, sodass sie für ihre Aktionen zur Rechenschaft gezogen werden können.	cloud-trail-cloud-watch-logs-aktiviert	Verwenden Sie Amazon CloudWatc h , um Protokoll ereignisaktivitäten zentral zu sammeln und zu verwalten. Die Aufnahme von AWS CloudTrail Daten liefert Einzelheiten zu den API-Aufrufaktivitä ten in Ihrem AWS-Konto.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AU.L2-3.3.2	Stellen Sie sicher, dass die Aktionen einzelner Systemben utzer eindeutig auf diese Benutzer zurückgeführt werden können, sodass sie für ihre Aktionen zur Rechenschaft gezogen werden können.	cloudtrail-enabled	AWS CloudTrail kann bei der Nichtabst reitbarkeit helfen, indem Aktionen und API-Aufrufe der AWS Management Console aufgezeic hnet werden. Sie können die Benutzer und die Benutzer AWS-Konten , die einen AWS Dienst aufgerufen haben, die Quell-IP-Adresse, über die die Aufrufe generiert wurden, und den Zeitpunkt der Anrufe identifiz ieren. Einzelheiten zu den erfassten Daten finden Sie in den AWS CloudTrail Datensatzinhalten.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AU.L2-3.3.2	Stellen Sie sicher, dass die Aktionen einzelner Systemben utzer eindeutig auf diese Benutzer zurückgeführt werden können, sodass sie für ihre Aktionen zur Rechenschaft gezogen werden können.	elb-logging-enabled	Die Elastic-Load-Balancing-Aktivität ist ein zentraler Kommunikationspunk t innerhalb einer Umgebung. Stellen Sie sicher, dass die ELB-Protokollierun g aktiviert ist. Die gesammelten Daten enthalten detaillie rte Informationen zu Anfragen, die an den ELB gesendet wurden. Jedes Protokoll enthält Informationen wie die Zeit, zu der die Anforderung einging, die Client-IP -Adresse, Latenzen, Anforderungspfade und Serverantworten.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AU.L2-3.3.2	Stellen Sie sicher, dass die Aktionen einzelner Systemben utzer eindeutig auf diese Benutzer zurückgeführt werden können, sodass sie für ihre Aktionen zur Rechenschaft gezogen werden können.	multi-region-cloudtrail-enabled	AWS CloudTrail zeichnet Aktionen und API-Aufrufe der AWS Management Console auf. Sie können feststellen, welche Benutzer und Konten angerufen wurden AWS, von welcher Quell-IP-Adresse aus die Anrufe getätigt wurden und wann die Anrufe erfolgten. CloudTrail übermittelt Protokolldateien aus allen AWS Regionen an Ihren S3-Bucket , wenn MULTI_REG ION_CLOUD _TRAIL_ENABLED aktiviert ist. Außerdem wird beim AWS Start einer neuen Region derselbe Trail in der neuen Region erstellt. CloudTrail Dadurch erhalten Sie automatis ch Protokolldateien mit API-Aktivitäten für die neue Region.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AU.L2-3.3.2	Stellen Sie sicher, dass die Aktionen einzelner Systemben utzer eindeutig auf diese Benutzer zurückgeführt werden können, sodass sie für ihre Aktionen zur Rechenschaft gezogen werden können.	rds-logging-enabled	Um die Protokoll ierung und Überwachung in Ihrer Umgebung zu erleichtern, stellen Sie sicher, dass die Amazon Relationa l Database Service (Amazon RDS)-Prot okollierung aktiviert ist. Mit der Amazon-RDS-Protokollierung können Sie Ereigniss e wie Verbindungen, Verbindungsabbrüch e, Abfragen oder abgefragte Tabellen erfassen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AU.L2-3.3.2	Stellen Sie sicher, dass die Aktionen einzelner Systemben utzer eindeutig auf diese Benutzer zurückgeführt werden können, sodass sie für ihre Aktionen zur Rechenschaft gezogen werden können.	s-3 bucket-logging-enabled	Die Amazon Simple Storage Service (Amazon S3)-Serverzugriffs protokollierung bietet eine Methode zur Überwachu ng des Netzwerks im Hinblick auf potenzielle Cybersich erheitsereignisse. Die Ereignisse werden überwacht, indem detaillierte Aufzeichn ungen über die Anfragen erfasst werden, die an einen Amazon-S3-Bucket gestellt wurden. Jeder Zugriffsprotokolle intrag enthält Details zu einer einzelnen Zugriffsanfrage. Zu den Details gehören Anforderer, Bucket-Name, Anforderu ngszeit, Anforderu ngsaktion, Antwortst atus und Fehlercode, falls relevant.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AU.L2-3.3.2	Stellen Sie sicher, dass die Aktionen einzelner Systembenutzer eindeutig auf diese Benutzer zurückgeführt werden können, sodass sie für ihre Aktionen zur Rechenschaft gezogen werden können.	wafv2-logging-enabled	Um die Protokollierung und Überwachung in Ihrer Umgebung zu erleichtern, aktivieren Sie die AWS WAF (V2) -Protokollierung im regionalen und globalen Web ACLs. AWS Die WAF-Protokollierung bietet detaillierte Informationen über den Datenverkehr, der von Ihrer Web-ACL analysiert wird. In den Protokollen werden die Uhrzeit aufgezeichnet, zu der die AWS WAF die Anfrage von Ihrer AWS Ressource erhalten hat, Informationen über die Anfrage und eine Aktion für die Regel, der jede Anfrage entsprach.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AU.L2-3.3.4	Warnung im Falle eines Fehlers bei der Prüfprotokollierung.	cloudwatch-alarm-action-check	Amazon CloudWatch alarmiert, wenn eine Metrik den Schwellenwert für eine bestimmte Anzahl von Bewertungszeiträumen überschreitet. Der Alarm führt eine oder mehrere Aktionen durch, die vom Wert der Metrik oder des Ausdrucks im Vergleich zu einem Schwellenwert in einer Reihe von Zeiträumen abhängt. Diese Regel erfordert einen Wert für alarmActionRequired (Config Default: True), insufficientDataAction Required (Config Default: True), okActionRequired (Config Default: False). Der tatsächliche Wert muss die Alarmaktionen für Ihre Umgebung widerspiegeln.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AU.L2-3.3.4	Warnung im Falle eines Fehlers bei der Prüfprotokollierung.	cloud-trail-cloud-watch-logs-aktiviert	Verwenden Sie Amazon CloudWatch , um Protokoll ereignisaktivitäten zentral zu sammeln und zu verwalten. Die Aufnahme von AWS CloudTrail Daten liefert Einzelheiten zu den API-Aufrufaktivitäten in Ihrem AWS-Konto.
AU.L2-3.3.4	Warnung im Falle eines Fehlers bei der Prüfprotokollierung.	guardduty-enabled-centralized	Amazon GuardDuty kann mithilfe von Threat Intelligence Feeds helfen, potenzielle Cybersicherheitsereignisse zu überwachen und zu erkennen. Dazu gehören Listen mit bösartigen IPs und maschinellen Lernmethoden zur Identifizierung unerwarteter, nicht autorisierter und bösartiger Aktivitäten in Ihrer AWS Cloud-Umgebung.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AU.L2-3.3.4	Warnung im Falle eines Fehlers bei der Prüfprotokollierung.	securityhub-enabled	AWS Security Hub hilft bei der Überwachung von unbefugtem Personal, Verbindungen, Geräten und Software. AWS Security Hub aggregiert, organisiert und priorisiert die Sicherheitswarnungen oder Ergebnisse mehrerer Dienste. AWS Einige dieser Dienste sind Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer und AWS Firewall Manager sowie AWS Partnerlösungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AU.L2-3.3.5	Koordinieren Sie die Prüfungs-, Analyse- und Berichtsprozesse für die Untersuch ung von und die Reaktion auf Hinweise auf rechtswidrige, unbefugte, verdächti ge oder ungewöhnl iche Aktivitäten.	guardduty-enabled-centralized	Amazon GuardDuty kann mithilfe von Threat Intellige nce Feeds helfen, potenzielle Cybersich erheitsereignisse zu überwachen und zu erkennen. Dazu gehören Listen mit bösartigen IPs und maschinel len Lernmethoden zur Identifizierung unerwarteter, nicht autorisierter und bösartiger Aktivitäten in Ihrer AWS Cloud-Umgebung.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AU.L2-3.3.5	Koordinieren Sie die Prüfungs-, Analyse- und Berichtsprozesse für die Untersuch ung von und die Reaktion auf Hinweise auf rechtswidrige, unbefugte, verdächti ge oder ungewöhnl iche Aktivitäten.	securityhub-enabled	AWS Security Hub hilft bei der Überwachung von unbefugtem Personal, Verbindun gen, Geräten und Software. AWS Security Hub aggregiert, organisie rt und priorisie rt die Sicherhei tswarnungen oder Ergebnisse mehrerer Dienste. AWS Einige dieser Dienste sind Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer und AWS Firewall Manager sowie AWS Partnerlösungen.
AU.L2-3.3.8	Schützen Sie Prüfungsinformatio nen und Tools zur Prüfprotokollierun g vor unbefugtem Zugriff, Änderung und Löschung.	cloudwatch-log-group-encrypted	Um sensible Daten im Speicher zu schützen, stellen Sie sicher, dass die Verschlüs selung für Ihre Amazon CloudWatch Log Groups aktiviert ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AU.L2-3.3.8	Schützen Sie Prüfungsinformationen und Tools zur Prüfprotokollierung vor unbefugtem Zugriff, Änderung und Löschung.	cloud-trail-encryption-enabled	Da sensible Daten vorhanden sein können und um Daten im Speicher zu schützen, sollten Sie sicherstellen, dass die Verschlüsselung für Ihre AWS CloudTrail Trails aktiviert ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AU.L2-3.3.8	Schützen Sie Prüfungsinformationen und Tools zur Prüfprotokollierung vor unbefugtem Zugriff, Änderung und Löschung.	cloud-trail-log-file-Validierung aktiviert	Verwenden Sie die AWS CloudTrail Protokolldateivalidierung, um die Integrität von Protokollen zu überprüfen. CloudTrail Mithilfe der Protokolldateivalidierung kann festgestellt werden, ob eine Protokolldatei geändert oder gelöscht wurde oder ob sie nach der Übermittlung CloudTrail unverändert geblieben ist. Dieses Feature wurde mit dem Branchenstandard entsprechenden Algorithmen entwickelt: SHA-256 für die Hashfunktion und SHA-256 mit RSA für digitale Signaturen. Aus diesem Grund ist es rechnerisch unmöglich, CloudTrail Protokolldateien unbemerkt zu ändern, zu löschen oder zu fälschen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AU.L2-3.3.8	Schützen Sie Prüfungsinformationen und Tools zur Prüfprotokollierung vor unbefugtem Zugriff, Änderung und Löschung.	s3- -Blocke-periodisch account-level-public-access	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Simple Storage Service (Amazon S3) -Buckets nicht öffentlich zugänglich sind. Diese Regel trägt dazu bei, sensible Daten vor unbefugten Remote-Benutzern zu schützen, indem sie den öffentlichen Zugriff verhindert. Mit dieser Regel können Sie optional die Parameter ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) und restrictPublicBuckets Parameter (Config Default: True) festlegen. Die tatsächlichen Werte müssen den Richtlini

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			en Ihrer Organisation entsprechen.
AU.L2-3.3.8	Schützen Sie Prüfungsinformationen und Tools zur Prüfprotokollierung vor unbefugtem Zugriff, Änderung und Löschung.	s3- bucket-default-lock-enabled	Stellen Sie sicher, dass für Ihren Amazon Simple Storage Service (Amazon S3)-Bucket standardmäßig eine Sperre aktiviert ist. Zum Schutz eventuell vorhandener sensibler Daten in S3-Buckets müssen Sie Objektsperren für Daten im Ruhezustand erzwingen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AU.L2-3.3.8	Schützen Sie Prüfungsinformationen und Tools zur Prüfprotokollierung vor unbefugtem Zugriff, Änderung und Löschung.	s-3 bucket-policy-grantee-check	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie s3_bucket_policy_grantee_check aktivieren. Diese Regel prüft, ob der vom Amazon S3 S3-Bucket gewährte Zugriff durch die von Ihnen bereitgestellten AWS Principals, Verbundbenutzer, Service Principals, IP-Adressen oder Amazon Virtual Private Cloud (Amazon VPC) IDs eingeschränkt ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AU.L2-3.3.8	Schützen Sie Prüfungsinformationen und Tools zur Prüfprotokollierung vor unbefugtem Zugriff, Änderung und Löschung.	s-3 bucket-public-read-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie nur autorisierten Benutzern, Prozessen und Geräten Zugriff auf Amazon Simple Storage Service (Amazon S3) - Buckets gewähren. Die Verwaltung des Zugriffs sollte mit der Klassifizierung der Daten übereinstimmen.
AU.L2-3.3.8	Schützen Sie Prüfungsinformationen und Tools zur Prüfprotokollierung vor unbefugtem Zugriff, Änderung und Löschung.	s3- bucket-public-write-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie nur autorisierten Benutzern, Prozessen und Geräten Zugriff auf Amazon Simple Storage Service (Amazon S3) - Buckets gewähren. Die Verwaltung des Zugriffs sollte mit der Klassifizierung der Daten übereinstimmen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AU.L2-3.3.8	Schützen Sie Prüfungsinformationen und Tools zur Prüfprotokollierung vor unbefugtem Zugriff, Änderung und Löschung.	s3-fähig bucket-server-side-encryption	Zum Schutz von Daten im Ruhezustand müssen Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon Simple Storage Service (Amazon S3)-Buckets aktiviert ist. Um eventuell vorhandene sensible Daten im Ruhezustand in Amazon-S3-Buckets zu schützen, muss die Verschlüsselung aktiviert sein.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AU.L2-3.3.8	Schützen Sie Prüfungsinformationen und Tools zur Prüfprotokollierung vor unbefugtem Zugriff, Änderung und Löschung.	s-3 bucket-ssl-requests-only	Um Daten während der Übertragung zu schützen, stellen Sie sicher, dass Ihre Amazon Simple Storage Service (Amazon S3)-Buckets Anfragen zur Verwendung von Secure Socket Layer (SSL)-Buckets erfordern. Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AU.L2-3.3.8	Schützen Sie Prüfungsinformationen und Tools zur Prüfprotokollierung vor unbefugtem Zugriff, Änderung und Löschung.	s-3 bucket-versioning-enabled	Die Versionsverwaltung von Amazon Simple Storage Service (Amazon S3)-Buckets hilft dabei, mehrere Varianten eines Objekts im selben Amazon-S3-Bucket zu speichern. Verwenden Sie die Versionsverwaltung, um sämtliche Versionen aller Objekte in Ihrem Amazon-S3-Bucket zu speichern, abzurufen oder wiederherzustellen. Mit der Versionsverwaltung können Sie Versionen sowohl nach unbeabsichtigten Benutzeraktionen als auch nach Anwendungsfehlern problemlos wiederherstellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AU.L2-3.3.8	Schützen Sie Prüfungsinformationen und Tools zur Prüfprotokollierung vor unbefugtem Zugriff, Änderung und Löschung.	s-3 default-encryption-kms	Stellen Sie sicher, dass die Verschlüsselung für Ihre Amazon Simple Storage Service (Amazon S3)-Buckets aktiviert ist. Um eventuell vorhandene sensible Daten im Ruhezustand in einem Amazon-S3-Bucket zu schützen, muss die Verschlüsselung aktiviert sein.
CA.L2-3.12.2	Entwickeln und implementieren Sie Aktionsplänen zur Behebung von Mängeln und zur Verringerung oder Beseitigung von Schwachstellen in Organisationssystemen.	vuln-management-plan-exists (Prozessüberprüfung)	Stellen Sie sicher, dass ein Plan für das Schwachstellenmanagement entwickelt und implementiert wird, damit Sie über formell definierte Prozesse zur Behebung von Schwachstellen in Ihrer Umgebung verfügen. Dazu zählen Tools für das Schwachstellenmanagement, regelmäßige Umgebungsscans sowie entsprechende Rollen und Verantwortlichkeiten.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CA.L2-3.12.3	Überwachen Sie kontinuierlich die Sicherheitskontrollen, um ihre anhaltende Effektivität sicherzus tellen.	guardduty-enabled-centralized	Amazon GuardDuty kann mithilfe von Threat Intellige nce Feeds helfen, potenzielle Cybersich erheitsereignisse zu überwachen und zu erkennen. Dazu gehören Listen mit bösartigen IPs und maschinel len Lernmethoden zur Identifizierung unerwarteter, nicht autorisierter und bösartiger Aktivitäten in Ihrer AWS Cloud-Umgebung.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CA.L2-3.12.3	Überwachen Sie kontinuierlich die Sicherheitskontrollen, um ihre anhaltende Effektivität sicherzus tellen.	guardduty-enabled-centralized	Amazon GuardDuty kann mithilfe von Threat Intellige nce Feeds helfen, potenzielle Cybersich erheitsereignisse zu überwachen und zu erkennen. Dazu gehören Listen mit bösartigen IPs und maschinel len Lernmethoden zur Identifizierung unerwarteter, nicht autorisierter und bösartiger Aktivitäten in Ihrer AWS Cloud-Umgebung.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CA.L2-3.12.3	Überwachen Sie kontinuierlich die Sicherheitskontrollen, um ihre anhaltende Effektivität sicherzus tellen.	securityhub-enabled	AWS Security Hub hilft bei der Überwachung von unbefugtem Personal, Verbindun gen, Geräten und Software. AWS Security Hub aggregiert, organisie rt und priorisie rt die Sicherhei tswarnungen oder Ergebnisse mehrerer Dienste. AWS Einige dieser Dienste sind Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer und AWS Firewall Manager sowie AWS Partnerlösungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CM.L2-3.4.1	Etablieren und pflegen Sie Basiskonfigurationen und Inventare der Organisationssysteme (einschließlich Hardware, Software, Firmware und Dokumentation) während der jeweiligen Lebenszyklen der Systementwicklung.	ec2-prüfen managedinstance-association-compliance-status	Verwenden Sie AWS Systems Manager Associations, um bei der Inventarisierung von Softwareplattformen und Anwendungen innerhalb eines Unternehmens zu helfen. AWS Systems Manager weist Ihren verwalteten Instanzen einen Konfigurationsstatus zu und ermöglicht es Ihnen, Basiswerte für Betriebssystem-Patch-Levels, Softwareinstallationen, Anwendungskonfigurationen und andere Details zu Ihrer Umgebung festzulegen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CM.L2-3.4.1	Etablieren und pflegen Sie Basiskonfigurationen und Inventare der Organisationssysteme (einschließlich Hardware, Software, Firmware und Dokumentation) während der jeweiligen Lebenszyklen der Systementwicklung.	ec2-check managedinstance-patch-compliance-status	Aktivieren Sie diese Regel, um bei der Identifizierung und Dokumentation von Sicherheitslücken in Amazon Elastic Compute Cloud (Amazon EC2) zu helfen. Die Regel prüft, ob die EC2 Amazon-Instance die Patch-Konformität im AWS Systems Manager gemäß den Richtlinien und Verfahren Ihrer Organisation einhält.
CM.L2-3.4.1	Etablieren und pflegen Sie Basiskonfigurationen und Inventare der Organisationssysteme (einschließlich Hardware, Software, Firmware und Dokumentation) während der jeweiligen Lebenszyklen der Systementwicklung.	ec2-stopped-instance	Aktivieren Sie diese Regel, um bei der Basiskonfiguration von Amazon Elastic Compute Cloud (Amazon EC2) - Instances zu helfen, indem Sie überprüfen, ob EC2 Amazon-Instances gemäß den Standards Ihrer Organisation für mehr als die zulässige Anzahl von Tagen gestoppt wurden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CM.L2-3.4.1	Etablieren und pflegen Sie Basiskonfigurationen und Inventare der Organisationssysteme (einschließlich Hardware, Software, Firmware und Dokumentation) während der jeweiligen Lebenszyklen der Systementwicklung.	ec2- volume-inuse-check	Diese Regel stellt sicher, dass Amazon Elastic Block Store-Volumes, die an Amazon Elastic Compute Cloud (Amazon EC2) - Instances angehängt sind, zum Löschen markiert werden, wenn eine Instance beendet wird. Wenn ein Amazon-EBS-Volume nicht gelöscht wird, wenn die Instance, an die es angehängt ist, beendet wird, kann dies gegen das Konzept der geringsten Funktionalität verstoßen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CM.L2-3.4.1	Etablieren und pflegen Sie Basiskonfigurationen und Inventare der Organisationssysteme (einschließlich Hardware, Software, Firmware und Dokumentation) während der jeweiligen Lebenszyklen der Systementwicklung.	eip-attached	Diese Regel stellt sicher, dass Elastic, die einer Amazon Virtual Private Cloud (Amazon VPC) IPs zugewiesen sind, an Amazon Elastic Compute Cloud (Amazon EC2) - Instances oder verwendete Elastic Network Interfaces angehängt sind. Diese Regel hilft bei der Überwachung ungenutzter Inhalte EIPs in Ihrer Umgebung.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CM.L2-3.4.2	Etablieren und implementieren Sie Sicherheitskonfigurationseinstellungen für IT-Produkte, die in Systemen der Organisation eingesetzt werden.	account-part-of-organizations	Durch die zentrale Verwaltung AWS-Konten innerhalb von AWS Organizations wird sichergestellt, dass die Konten den Vorschriften entsprechen. Eine fehlende zentrale Kontoverwaltung kann zu inkonsistenten Kontokonfigurationen führen, wodurch Ressourcen und sensible Daten offengelegt werden können.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CM.L2-3.4.2	Etablieren und implementieren Sie Sicherheitskonfigurationseinstellungen für IT-Produkte, die in Systemen der Organisation eingesetzt werden.	cloudtrail-security-trail-enabled	Diese Regel trägt dazu bei, die Verwendung der AWS empfohlenen bewährten Sicherheitsmethoden für sicherzustellen AWS CloudTrail, indem geprüft wird, ob mehrere Einstellungen aktiviert sind. Dazu gehören die Verwendung von Protokollverschlüsselung, Protokollvalidierung und Aktivierung AWS CloudTrail in mehreren Regionen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CM.L2-3.4.2	Etablieren und implementieren Sie Sicherheitskonfigurationseinstellungen für IT-Produkte, die in Systemen der Organisation eingesetzt werden.	cloud-trail-log-file-Validierung aktiviert	Verwenden Sie die AWS CloudTrail Protokolldateivalidierung, um die Integrität von Protokollen zu überprüfen. CloudTrail Mithilfe der Protokolldateivalidierung kann festgestellt werden, ob eine Protokolldatei geändert oder gelöscht wurde oder ob sie nach der Übermittlung CloudTrail unverändert geblieben ist. Dieses Feature wurde mit dem Branchenstandard entsprechenden Algorithmen entwickelt: SHA-256 für die Hashfunktion und SHA-256 mit RSA für digitale Signaturen. Aus diesem Grund ist es rechnerisch unmöglich, CloudTrail Protokolldateien unbemerkt zu ändern, zu löschen oder zu fälschen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CM.L2-3.4.2	Etablieren und implementieren Sie Sicherheitskonfigurationseinstellungen für IT-Produkte, die in Systemen der Organisation eingesetzt werden.	ec2-managerinstance-managed-by-systems	Eine Bestandsaufnahme der Softwareplattformen und Anwendungen innerhalb des Unternehmens ist möglich, indem Amazon Elastic Compute Cloud (Amazon EC2) - Instances mit AWS Systems Manager verwaltet werden. Verwenden Sie AWS Systems Manager, um detaillierte Systemkonfigurationen, Betriebssystem-Patch-Levels, Namen und Typ der Dienste, Softwareinstallationen, Anwendungsname, Herausgeber und Version sowie andere Details zu Ihrer Umgebung bereitzustellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CM.L2-3.4.2	Etablieren und implementieren Sie Sicherheitskonfigurationseinstellungen für IT-Produkte, die in Systemen der Organisation eingesetzt werden.	ec2-check managedinstance-association-compliance-status	Verwenden Sie AWS Systems Manager Associations, um bei der Inventarisierung von Softwareplattformen und Anwendungen innerhalb eines Unternehmens zu helfen. AWS Systems Manager weist Ihren verwalteten Instanzen einen Konfigurationsstatus zu und ermöglicht es Ihnen, Basiswerte für Betriebssystem-Patch-Levels, Softwareinstallationen, Anwendungskonfigurationen und andere Details zu Ihrer Umgebung festzulegen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CM.L2-3.4.2	Etablieren und implementieren Sie Sicherheitskonfigurationseinstellungen für IT-Produkte, die in Systemen der Organisation eingesetzt werden.	ec2-check managedinstance-patch-compliance-status	Aktivieren Sie diese Regel, um bei der Identifizierung und Dokumentation von Sicherheitslücken in Amazon Elastic Compute Cloud (Amazon EC2) zu helfen. Die Regel prüft, ob die EC2 Amazon-Instance die Patch-Konformität im AWS Systems Manager gemäß den Richtlinien und Verfahren Ihrer Organisation einhält.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CM.L2-3.4.2	Etablieren und implementieren Sie Sicherheitskonfigurationseinstellungen für IT-Produkte, die in Systemen der Organisation eingesetzt werden.	elastic-beanstalk-managed-updates-aktiviert	Durch die Aktivierung verwalteter Plattform updates für eine Amazon-Elastic-Beanstalk-Umgebung wird sichergestellt, dass die aktuellen verfügbaren Plattform -Fixes, -Updates und -Features für die Umgebung installiert sind. Eine bewährte Methode zur Sicherung von Systemen besteht darin, stets die aktuellen Patches zu installieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CM.L2-3.4.2	Etablieren und implementieren Sie Sicherheitskonfigurationseinstellungen für IT-Produkte, die in Systemen der Organisation eingesetzt werden.	guardduty-enabled-centralized	Amazon GuardDuty kann mithilfe von Threat Intelligence Feeds helfen, potenzielle Cybersicherheitsereignisse zu überwachen und zu erkennen. Dazu gehören Listen mit bösartigen IPs und maschinellen Lernmethoden zur Identifizierung unerwarteter, nicht autorisierter und bösartiger Aktivitäten in Ihrer AWS Cloud-Umgebung.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CM.L2-3.4.2	Etablieren und implementieren Sie Sicherheitskonfigurationseinstellungen für IT-Produkte, die in Systemen der Organisation eingesetzt werden.	rds-automatic-minor-version-Upgrade-fähig	Aktivieren Sie automatische Unterversions-Upgrades auf Ihren Amazon-Relational-Database-Service (RDS)-Instances, um sicherzustellen, dass die aktuellen Updates für Unterversionen des Relational Database Management System (RDBMS) installiert sind, die Sicherheitspatches und Bugfixes enthalten können.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CM.L2-3.4.2	Etablieren und implementieren Sie Sicherheitskonfigurationseinstellungen für IT-Produkte, die in Systemen der Organisation eingesetzt werden.	redshift-cluster-maintenancesettings-check	Diese Regel stellt sicher, dass Amazon-Redshift-Cluster die bevorzugten Einstellungen für Ihre Organisation haben. Insbesondere sorgt sie dafür, dass Cluster bevorzugte Wartungsfenster und automatisierte Aufbewahrungsfristen für Snapshots für die Datenbank haben. Für diese Regel müssen Sie die festlegen. allowVersionUpgrade Der Standardwert ist „true“. Außerdem können Sie optional den Zeitraum preferredMaintenanceWindow (der Standardwert ist sa: 16:00 -sa: 16:30) und den automated SnapshotRetention Zeitraum (der Standardwert ist 1) festlegen. Die tatsächlichen Werte müssen den Richtlini

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			en Ihrer Organisation entsprechen.
CM.L2-3.4.2	Etablieren und implementieren Sie Sicherheitskonfigurationseinstellungen für IT-Produkte, die in Systemen der Organisation eingesetzt werden.	securityhub-enabled	AWS Security Hub hilft bei der Überwachung von unbefugtem Personal, Verbindungen, Geräten und Software. AWS Security Hub aggregiert, organisiert und priorisiert die Sicherheitswarnungen oder Ergebnisse mehrerer Dienste. AWS Einige dieser Dienste sind Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer und AWS Firewall Manager sowie AWS Partnerlösungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CM.L2-3.4.3	Sie können Änderungen an Organisationssysteme n verfolgen , überprüfen, genehmigen oder ablehnen und protokollieren.	api-gw-execution-logging-aktiviert	Die API-Gateway-Protokollierung zeigt detaillierte Ansichten der Benutzer, die auf die API zugegriffen haben, und wie diese Benutzer auf die API zugegriffen haben. Diese Einblicke ermöglichen die Transparenz von Benutzeraktivitäten.
CM.L2-3.4.3	Sie können Änderungen an Organisationssysteme n verfolgen , überprüfen, genehmigen oder ablehnen und protokollieren.	cloudtrail-s3-dataevents-enabled	Die Erfassung von Simple Storage Service (Amazon S3)-Datenereignissen unterstützt die Erkennung von ungewöhnlichen Aktivitäten. Zu den Details gehören AWS-Konto Informationen über den Zugriff auf einen Amazon S3 S3-Bucket, die IP-Adresse und die Uhrzeit des Ereignisses.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CM.L2-3.4.3	Sie können Änderungen an Organisationssystemen verfolgen , überprüfen, genehmigen oder ablehnen und protokollieren.	cloud-trail-cloud-watch-logs-aktiviert	Verwenden Sie Amazon CloudWatch , um Protokoll ereignisaktivitäten zentral zu sammeln und zu verwalten. Die Aufnahme von AWS CloudTrail Daten liefert Einzelheiten zu den API-Aufrufaktivitäten in Ihrem AWS-Konto.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CM.L2-3.4.3	Sie können Änderungen an Organisationssysteme n verfolgen , überprüfen, genehmigen oder ablehnen und protokollieren.	cloudtrail-enabled	AWS CloudTrail kann bei der Nichtabstreitbarkeit helfen, indem Aktionen und API-Aufrufe der AWS Management Console aufgezeichnet werden. Sie können die Benutzer und die Benutzer AWS-Konten , die einen AWS Dienst aufgerufen haben, die Quell-IP-Adresse, über die die Aufrufe generiert wurden, und den Zeitpunkt der Anrufe identifizieren. Einzelheiten zu den erfassten Daten finden Sie in den AWS CloudTrail Datensatzinhalten.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CM.L2-3.4.3	Sie können Änderungen an Organisationssysteme n verfolgen , überprüfen, genehmigen oder ablehnen und protokollieren.	ec2-manager instance-managed-by-systems	Eine Bestandsaufnahme der Softwareplattformen und Anwendungen innerhalb des Unternehmens ist möglich, indem Amazon Elastic Compute Cloud (Amazon EC2) - Instances mit AWS Systems Manager verwaltet werden. Verwenden Sie AWS Systems Manager, um detaillierte Systemkonfigurationen, Betriebssystem-Patch-Levels, Namen und Typ der Dienste, Softwareinstallationen, Anwendungsname, Herausgeber und Version sowie andere Details zu Ihrer Umgebung bereitzustellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CM.L2-3.4.3	Sie können Änderungen an Organisationssysteme n verfolgen , überprüfen, genehmigen oder ablehnen und protokollieren.	ec2-check managedinstance-association-compliance-status	Verwenden Sie AWS Systems Manager Associations, um bei der Inventarisierung von Softwareplattformen und Anwendungen innerhalb eines Unternehmens zu helfen. AWS Systems Manager weist Ihren verwalteten Instanzen einen Konfigurationsstatus zu und ermöglicht es Ihnen, Basiswerte für Betriebssystem-Patch-Levels , Softwareinstallationen, Anwendungskonfigurationen und andere Details zu Ihrer Umgebung festzulegen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CM.L2-3.4.3	Sie können Änderungen an Organisationssystemen verfolgen, überprüfen, genehmigen oder ablehnen und protokollieren.	ec2-check managedinstance-patch-compliance-status	Aktivieren Sie diese Regel, um bei der Identifizierung und Dokumentation von Sicherheitslücken in Amazon Elastic Compute Cloud (Amazon EC2) zu helfen. Die Regel prüft, ob die EC2 Amazon-Instance die Patch-Konformität im AWS Systems Manager gemäß den Richtlinien und Verfahren Ihrer Organisation einhält.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CM.L2-3.4.3	Sie können Änderungen an Organisationssysteme n verfolgen , überprüfen, genehmigen oder ablehnen und protokollieren.	elb-logging-enabled	Die Elastic-Load-Balancing-Aktivität ist ein zentraler Kommunikationspunkt innerhalb einer Umgebung. Stellen Sie sicher, dass die ELB-Protokollierung aktiviert ist. Die gesammelten Daten enthalten detaillierte Informationen zu Anfragen, die an den ELB gesendet wurden. Jedes Protokoll enthält Informationen wie die Zeit, zu der die Anforderung einging, die Client-IP-Adresse, Latenzen, Anforderungspfade und Serverantworten.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CM.L2-3.4.3	Sie können Änderungen an Organisationssysteme n verfolgen , überprüfen, genehmigen oder ablehnen und protokollieren.	multi-region-cloudtrail-enabled	AWS CloudTrail zeichnet Aktionen und API-Aufrufe der AWS Management Console auf. Sie können feststellen, welche Benutzer und Konten angerufen wurden AWS, von welcher Quell-IP-Adresse aus die Anrufe getätigt wurden und wann die Anrufe erfolgten. CloudTrail übermittelt Protokolldateien aus allen AWS Regionen an Ihren S3-Bucket , wenn MULTI_REGION_CLOUD_TRAIL_ENABLED aktiviert ist. Außerdem wird beim AWS Start einer neuen Region derselbe Trail in der neuen Region erstellt. CloudTrail Dadurch erhalten Sie automatisch Protokolldateien mit API-Aktivitäten für die neue Region.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CM.L2-3.4.3	Sie können Änderungen an Organisationssysteme n verfolgen , überprüfen, genehmigen oder ablehnen und protokollieren.	rds-logging-enabled	Um die Protokoll ierung und Überwachung in Ihrer Umgebung zu erleichtern, stellen Sie sicher, dass die Amazon Relationa l Database Service (Amazon RDS)-Prot okollierung aktiviert ist. Mit der Amazon-RDS-Protokollierung können Sie Ereigniss e wie Verbindungen, Verbindungsabbrüch e, Abfragen oder abgefragte Tabellen erfassen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CM.L2-3.4.3	Sie können Änderungen an Organisationssysteme n verfolgen , überprüfen, genehmigen oder ablehnen und protokollieren.	s-3 bucket-logging-enabled	Die Amazon Simple Storage Service (Amazon S3)-Serverzugriffs protokollierung bietet eine Methode zur Überwachu ng des Netzwerks im Hinblick auf potenzielle Cybersich erheitsereignisse. Die Ereignisse werden überwacht, indem detaillierte Aufzeichn ungen über die Anfragen erfasst werden, die an einen Amazon-S3-Bucket gestellt wurden. Jeder Zugriffsprotokolle intrag enthält Details zu einer einzelnen Zugriffsanfrage. Zu den Details gehören Anforderer, Bucket-Name, Anforderu ngszeit, Anforderu ngsaktion, Antwortst atus und Fehlercode, falls relevant.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CM.L2-3.4.3	Sie können Änderungen an Organisationssystemen verfolgen, überprüfen, genehmigen oder ablehnen und protokollieren.	wafv2-logging-enabled	Um die Protokollierung und Überwachung in Ihrer Umgebung zu erleichtern, aktivieren Sie die AWS WAF (V2) -Protokollierung im regionalen und globalen Web ACLs. AWS Die WAF-Protokollierung bietet detaillierte Informationen über den Datenverkehr, der von Ihrer Web-ACL analysiert wird. In den Protokollen werden die Uhrzeit aufgezeichnet, zu der die AWS WAF die Anfrage von Ihrer AWS Ressource erhalten hat, Informationen über die Anfrage und eine Aktion für die Regel, der jede Anfrage entsprach.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CM.L2-3.4.6	Wenden Sie das Prinzip der geringsten Funktionalität an, indem Sie Organisationssysteme so konfigurieren, dass sie nur unbedingt erforderliche Funktionen bereitstellen.	autoscaling-launch-config-public-ip-deaktiviert	Wenn Sie Ihre Netzwerkschnittstellen mit einer öffentlichen IP-Adresse konfigurieren, sind die diesen Netzwerkschnittstellen zugehörigen Ressourcen über das Internet erreichbar. EC2 Ressourcen sollten nicht öffentlich zugänglich sein, da dies einen unbeabsichtigten Zugriff auf Ihre Anwendungen oder Server ermöglichen kann.
CM.L2-3.4.6	Wenden Sie das Prinzip der geringsten Funktionalität an, indem Sie Organisationssysteme so konfigurieren, dass sie nur unbedingt erforderliche Funktionen bereitstellen.	dms-replication-not-public	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass auf DMS-Replikationsinstanzen nicht öffentlich zugegriffen werden kann. DMS-Replikations-Instances können vertrauliche Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CM.L2-3.4.6	Wenden Sie das Prinzip der geringsten Funktionalität an, indem Sie Organisationssysteme so konfigurieren, dass sie nur unbedingt erforderliche Funktionen bereitstellen.	ebs-snapshot-public-restorable-überprüfen	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass EBS-Snapshots nicht öffentlich wiederherstellbar sind. EBS-Volume-Snapshots können vertrauliche Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CM.L2-3.4.6	Wenden Sie das Prinzip der geringsten Funktionalität an, indem Sie Organisationssysteme so konfigurieren, dass sie nur unbedingt erforderliche Funktionen bereitstellen.	ec2-manager instance-managed-by-systems	Eine Bestandsaufnahme der Softwareplattformen und Anwendungen innerhalb des Unternehmens ist möglich, indem Amazon Elastic Compute Cloud (Amazon EC2) - Instances mit AWS Systems Manager verwaltet werden. Verwenden Sie AWS Systems Manager, um detaillierte Systemkonfigurationen, Betriebssystem-Patch-Levels, Namen und Typ der Dienste, Softwareinstallationen, Anwendungsname, Herausgeber und Version sowie andere Details zu Ihrer Umgebung bereitzustellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CM.L2-3.4.6	Wenden Sie das Prinzip der geringsten Funktionalität an, indem Sie Organisationssysteme so konfigurieren, dass sie nur unbedingt erforderliche Funktionen bereitstellen.	ec2- instance-no-public-ip	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon Elastic Compute Cloud (Amazon EC2) - Instances nicht öffentlich zugänglich sind. EC2 Amazon-Instances können vertrauliche Informationen enthalten, und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CM.L2-3.4.6	Wenden Sie das Prinzip der geringsten Funktionalität an, indem Sie Organisationssysteme so konfigurieren, dass sie nur unbedingt erforderliche Funktionen bereitstellen.	ec2-check managedinstance-association-compliance-status	Verwenden Sie AWS Systems Manager Associations, um bei der Inventarisierung von Softwareplattformen und Anwendungen innerhalb eines Unternehmens zu helfen. AWS Systems Manager weist Ihren verwalteten Instanzen einen Konfigurationsstatus zu und ermöglicht es Ihnen, Basiswerte für Betriebssystem-Patch-Levels, Softwareinstallationen, Anwendungskonfigurationen und andere Details zu Ihrer Umgebung festzulegen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CM.L2-3.4.6	Wenden Sie das Prinzip der geringsten Funktionalität an, indem Sie Organisationssysteme so konfigurieren, dass sie nur unbedingt erforderliche Funktionen bereitstellen.	ec-2 volume-inuse-check	Diese Regel stellt sicher, dass Amazon Elastic Block Store-Volumes, die an Amazon Elastic Compute Cloud (Amazon EC2) - Instances angehängt sind, zum Löschen markiert werden, wenn eine Instance beendet wird. Wenn ein Amazon-EBS-Volume nicht gelöscht wird, wenn die Instance, an die es angehängt ist, beendet wird, kann dies gegen das Konzept der geringsten Funktionalität verstoßen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CM.L2-3.4.6	Wenden Sie das Prinzip der geringsten Funktionalität an, indem Sie Organisationssysteme so konfigurieren, dass sie nur unbedingt erforderliche Funktionen bereitstellen.	elasticsearch-in-vpc-only	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass sich Amazon OpenSearch OpenSearch Service (Service) - Domains innerhalb einer Amazon Virtual Private Cloud (Amazon VPC) befinden. Eine OpenSearch Service-Domain innerhalb einer Amazon VPC ermöglicht die sichere Kommunikation zwischen OpenSearch Service und anderen Services innerhalb der Amazon VPC, ohne dass ein Internet-Gateway, ein NAT-Gerät oder eine VPN-Verbindung erforderlich ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CM.L2-3.4.6	Wenden Sie das Prinzip der geringsten Funktionalität an, indem Sie Organisationssysteme so konfigurieren, dass sie nur unbedingt erforderliche Funktionen bereitstellen.	emr-master-no-public-ip	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon EMR-Cluster-Masterknoten nicht öffentlich zugänglich sind. Amazon-EMR-Cluster-Hauptknoten können vertrauliche Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CM.L2-3.4.6	Wenden Sie das Prinzip der geringsten Funktionalität an, indem Sie Organisationssysteme so konfigurieren, dass sie nur unbedingt erforderliche Funktionen bereitstellen.	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) Security Groups können bei der Verwaltung des Netzwerkzugriffs helfen, indem sie eine statusbehaftete Filterung von eingehendem und ausgehendem Netzwerkverkehr zu Ressourcen bereitstellen. AWS Wenn Sie eingehenden (oder entfernten) Datenverkehr von 0.0.0.0/0 bis Port 22 auf Ihren Ressourcen nicht zulassen, können Sie den Remote-Zugriff einschränken.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CM.L2-3.4.6	Wenden Sie das Prinzip der geringsten Funktionalität an, indem Sie Organisationssysteme so konfigurieren, dass sie nur unbedingt erforderliche Funktionen bereitstellen.	internet-gateway-authorized-vpc-nur	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Internet-Gateways nur mit autorisierter Amazon Virtual Private Cloud (Amazon VPC) verbunden sind. Internet-Gateways ermöglichen den bidirektionalen Internetzugang zur und von der Amazon VPC, was möglicherweise zu einem unbefugten Zugriff auf Amazon-VPC-Ressourcen führen kann.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CM.L2-3.4.6	Wenden Sie das Prinzip der geringsten Funktionalität an, indem Sie Organisationssysteme so konfigurieren, dass sie nur unbedingt erforderliche Funktionen bereitstellen.	lambda-function-public-access-verboten	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass AWS Lambda-Funktionen nicht öffentlich zugänglich sind. Der öffentliche Zugriff kann möglicherweise die Verfügbarkeit von Ressourcen beeinträchtigen.
CM.L2-3.4.6	Wenden Sie das Prinzip der geringsten Funktionalität an, indem Sie Organisationssysteme so konfigurieren, dass sie nur unbedingt erforderliche Funktionen bereitstellen.	no-unrestricted-route-to-igw	Stellen Sie sicher, dass EC2 Amazon-Routentabellen keine uneingeschränkten Routen zu einem Internet-Gateway enthalten. Durch das Entfernen oder Beschränken des Internetzugangs für Workloads innerhalb von Amazon VPCs können unbeabsichtigte Zugriffe in Ihrer Umgebung reduziert werden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CM.L2-3.4.6	Wenden Sie das Prinzip der geringsten Funktionalität an, indem Sie Organisationssysteme so konfigurieren, dass sie nur unbedingt erforderliche Funktionen bereitstellen.	rds-instance-public-access-überprüfen	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Relational Database Service (Amazon RDS) -Instances nicht öffentlich sind. Amazon-RDS-Datenbank-Instances können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CM.L2-3.4.6	Wenden Sie das Prinzip der geringsten Funktionalität an, indem Sie Organisationssysteme so konfigurieren, dass sie nur unbedingt erforderliche Funktionen bereitstellen.	rds-snapshots-public-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Relational Database Service (Amazon RDS) -Instances nicht öffentlich sind. Amazon-RDS-Datenbank-Instances können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CM.L2-3.4.6	Wenden Sie das Prinzip der geringsten Funktionalität an, indem Sie Organisationssysteme so konfigurieren, dass sie nur unbedingt erforderliche Funktionen bereitstellen.	redshift-cluster-public-access-überprüfen	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Redshift Redshift-Cluster nicht öffentlich sind. Amazon-Redshift-Cluster können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CM.L2-3.4.6	Wenden Sie das Prinzip der geringsten Funktionalität an, indem Sie Organisationssysteme so konfigurieren, dass sie nur unbedingt erforderliche Funktionen bereitstellen.	restricted-common-ports	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass gemeinsame Ports für Amazon Elastic Compute Cloud (Amazon EC2) -Sicherheitsgruppen eingeschränkt sind. Wenn der Zugriff auf Ports nicht auf vertrauenswürdige Quellen beschränkt wird, kann dies zu Angriffen auf die Verfügbarkeit, Integrität und Vertraulichkeit von Systemen führen. Mit dieser Regel können Sie optional die Parameter blockedPort1–blockedPort5 festlegen (Standardkonfigurationen: 20, 21, 3389, 3306, 4333). Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CM.L2-3.4.6	Wenden Sie das Prinzip der geringsten Funktionalität an, indem Sie Organisationssysteme so konfigurieren, dass sie nur unbedingt erforderliche Funktionen bereitstellen.	s3- account-level-public-access -blöcke-periodisch	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Simple Storage Service (Amazon S3) -Buckets nicht öffentlich zugänglich sind. Diese Regel trägt dazu bei, sensible Daten vor unbefugten Remote-Benutzern zu schützen, indem sie den öffentlichen Zugriff verhindert. Mit dieser Regel können Sie optional die Parameter ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) und restrictPublicBuckets Parameter (Config Default: True) festlegen. Die tatsächlichen Werte müssen den Richtlini

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			en Ihrer Organisation entsprechen.
CM.L2-3.4.6	Wenden Sie das Prinzip der geringsten Funktionalität an, indem Sie Organisationssysteme so konfigurieren, dass sie nur unbedingt erforderliche Funktionen bereitstellen.	s3- bucket-public-read-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie nur autorisierten Benutzern, Prozessen und Geräten Zugriff auf Amazon Simple Storage Service (Amazon S3) - Buckets gewähren. Die Verwaltung des Zugriffs sollte mit der Klassifizierung der Daten übereinstimmen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CM.L2-3.4.6	Wenden Sie das Prinzip der geringsten Funktionalität an, indem Sie Organisationssysteme so konfigurieren, dass sie nur unbedingt erforderliche Funktionen bereitstellen.	s3- bucket-public-write-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie nur autorisierten Benutzern, Prozessen und Geräten Zugriff auf Amazon Simple Storage Service (Amazon S3) - Buckets gewähren. Die Verwaltung des Zugriffs sollte mit der Klassifizierung der Daten übereinstimmen.
CM.L2-3.4.6	Wenden Sie das Prinzip der geringsten Funktionalität an, indem Sie Organisationssysteme so konfigurieren, dass sie nur unbedingt erforderliche Funktionen bereitstellen.	sagemaker-notebook-no-direct-Internetzugang	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass SageMaker Amazon-Notebooks keinen direkten Internetzugang zulassen. Indem Sie direkten Internetzugang blockieren, vermeiden Sie, dass unbefugte Benutzer auf sensible Daten zugreifen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CM.L2-3.4.6	Wenden Sie das Prinzip der geringsten Funktionalität an, indem Sie Organisationssysteme so konfigurieren, dass sie nur unbedingt erforderliche Funktionen bereitstellen.	ssm-document-not-public	Stellen Sie sicher, dass AWS Systems Manager (SSM) - Dokumente nicht öffentlich sind, da dies einen unbeabsichtigten Zugriff auf Ihre SSM-Dokumente ermöglichen kann. Ein öffentliches SSM-Dokument kann Informationen über Ihr Konto, Ihre Ressourcen und internen Prozesse preisgeben.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CM.L2-3.4.6	Wenden Sie das Prinzip der geringsten Funktionalität an, indem Sie Organisationssysteme so konfigurieren, dass sie nur unbedingt erforderliche Funktionen bereitstellen.	subnet-auto-assign-public-ip-deaktiviert	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon Virtual Private Cloud (VPC) -Subnetzen nicht automatisch eine öffentliche IP-Adresse zugewiesen wird. Amazon Elastic Compute Cloud (EC2) -Instances, die in Subnetzen gestartet werden, in denen dieses Attribut aktiviert ist, haben ihrer primären Netzwerkschnittstelle eine öffentliche IP-Adresse zugewiesen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CM.L2-3.4.6	Wenden Sie das Prinzip der geringsten Funktionalität an, indem Sie Organisationssysteme so konfigurieren, dass sie nur unbedingt erforderliche Funktionen bereitstellen.	vpc-default-security-group-geschlossen	Sicherheitsgruppen von Amazon Elastic Compute Cloud (Amazon EC2) können bei der Verwaltung des Netzwerkzugriffs helfen, indem sie eine statusbehaftete Filterung des ein- und ausgehenden Netzwerkverkehrs zu Ressourcen bereitstellen. AWS Die Beschränkung des gesamten Datenverkehrs auf die Standardsicherheitsgruppe hilft dabei, den Fernzugriff auf Ihre Ressourcen einzuschränken. AWS

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CM.L2-3.4.6	Wenden Sie das Prinzip der geringsten Funktionalität an, indem Sie Organisationssysteme so konfigurieren, dass sie nur unbedingt erforderliche Funktionen bereitstellen.	vpc-sg-open-only-to-authorized-ports	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass gemeinsame Ports für Amazon Elastic Compute Cloud (Amazon EC2) -Sicherheitsgruppen eingeschränkt sind. Wenn der Zugriff auf Ports nicht auf vertrauenswürdige Quellen beschränkt wird, kann dies zu Angriffen auf die Verfügbarkeit, Integrität und Vertraulichkeit von Systemen führen. Durch die Beschränkung des Zugriffs auf Ressourcen innerhalb einer Sicherheitsgruppe aus dem Internet (0.0.0.0/0) kann der Remote-Zugriff auf interne Systeme gesteuert werden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CM.L2-3.4.6	Wenden Sie das Prinzip der geringsten Funktionalität an, indem Sie Organisationssysteme so konfigurieren, dass sie nur unbedingt erforderliche Funktionen bereitstellen.	opensearch-in-vpc-only	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass sich Amazon OpenSearch Service-Domains innerhalb einer Amazon Virtual Private Cloud (Amazon VPC) befinden. Eine Amazon OpenSearch Service-Domain innerhalb einer Amazon VPC ermöglicht die sichere Kommunikation zwischen Amazon OpenSearch Service und anderen Services innerhalb der Amazon VPC, ohne dass ein Internet-Gateway, ein NAT-Gerät oder eine VPN-Verbindung erforderlich ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CM.L2-3.4.7	Beschränken, deaktivieren oder verhindern Sie die Verwendung unnötiger Programme, Funktionen, Ports, Protokolle und Services.	autoscaling-launch-config-public-ip-deaktiviert	Wenn Sie Ihre Netzwerkschnittstellen mit einer öffentlichen IP-Adresse konfigurieren, sind die diesen Netzwerkschnittstellen zugehörigen Ressourcen über das Internet erreichbar. EC2 Ressourcen sollten nicht öffentlich zugänglich sein, da dies einen unbeabsichtigten Zugriff auf Ihre Anwendungen oder Server ermöglichen kann.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CM.L2-3.4.7	Beschränken, deaktivieren oder verhindern Sie die Verwendung unnötiger Programme , Funktionen, Ports, Protokolle und Services.	ec2- instance-no-public-ip	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon Elastic Compute Cloud (Amazon EC2) - Instances nicht öffentlich zugänglich sind. EC2 Amazon-Instances können vertrauliche Informati onen enthalten, und für solche Konten ist eine Zugriffskontrolle erforderlich.
CM.L2-3.4.7	Beschränken, deaktivieren oder verhindern Sie die Verwendung unnötiger Programme , Funktionen, Ports, Protokolle und Services.	emr-master-no-public-ip	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon EMR-Clust er-Masterknoten nicht öffentlich zugänglic h sind. Amazon-EM R-Cluster-Hauptkno ten können vertrauli che Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CM.L2-3.4.7	Beschränken, deaktivieren oder verhindern Sie die Verwendung unnötiger Programme , Funktionen, Ports, Protokolle und Services.	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) Security Groups können bei der Verwaltung des Netzwerkzugriffs helfen, indem sie eine statusbeh aftete Filterung von eingehendem und ausgehendem Netzwerkverkehr zu Ressourcen bereitste llen. AWS Wenn Sie eingehenden (oder entfernten) Datenverk ehr von 0.0.0.0/0 bis Port 22 auf Ihren Ressourcen nicht zulassen, können Sie den Remote-Zugriff einschränken.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CM.L2-3.4.7	Beschränken, deaktivieren oder verhindern Sie die Verwendung unnötiger Programme, Funktionen, Ports, Protokolle und Services.	internet-gateway-authorized-vpc-nur	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Internet-Gateways nur mit autorisierter Amazon Virtual Private Cloud (Amazon VPC) verbunden sind. Internet-Gateways ermöglichen den bidirektionalen Internetzugang zur und von der Amazon VPC, was möglicher weise zu einem unbefugten Zugriff auf Amazon-VPC-Ressourcen führen kann.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CM.L2-3.4.7	Beschränken, deaktivieren oder verhindern Sie die Verwendung unnötiger Programme, Funktionen, Ports, Protokolle und Services.	lambda-function-public-access-verboten	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass AWS Lambda-Funktionen nicht öffentlich zugänglich sind. Der öffentliche Zugriff kann möglicherweise die Verfügbarkeit von Ressourcen beeinträchtigen.
CM.L2-3.4.7	Beschränken, deaktivieren oder verhindern Sie die Verwendung unnötiger Programme, Funktionen, Ports, Protokolle und Services.	no-unrestricted-route-to-igw	Stellen Sie sicher, dass EC2 Amazon-Routentabellen keine uneingeschränkten Routen zu einem Internet-Gateway enthalten. Durch das Entfernen oder Beschränken des Internetzugangs für Workloads innerhalb von Amazon VPCs können unbeabsichtigte Zugriffe in Ihrer Umgebung reduziert werden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CM.L2-3.4.7	Beschränken, deaktivieren oder verhindern Sie die Verwendung unnötiger Programme, Funktionen, Ports, Protokolle und Services.	rds-instance-public-access-überprüfen	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Relational Database Service (Amazon RDS) -Instances nicht öffentlich sind. Amazon-RDS-Datenbank-Instances können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CM.L2-3.4.7	Beschränken, deaktivieren oder verhindern Sie die Verwendung unnötiger Programme, Funktionen, Ports, Protokolle und Services.	redshift-cluster-public-access-überprüfen	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Redshift Redshift-Cluster nicht öffentlich sind. Amazon-Redshift-Cluster können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CM.L2-3.4.7	Beschränken, deaktivieren oder verhindern Sie die Verwendung unnötiger Programme, Funktionen, Ports, Protokolle und Services.	restricted-common-ports	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass gemeinsame Ports für Amazon Elastic Compute Cloud (Amazon EC2) -Sicherheitsgruppen eingeschränkt sind. Wenn der Zugriff auf Ports nicht auf vertrauenswürdige Quellen beschränkt wird, kann dies zu Angriffen auf die Verfügbarkeit, Integrität und Vertraulichkeit von Systemen führen. Mit dieser Regel können Sie optional die Parameter blockedPort1–blockedPort5 festlegen (Standardkonfigurationen: 20, 21, 3389, 3306, 4333). Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CM.L2-3.4.7	Beschränken, deaktivieren oder verhindern Sie die Verwendung unnötiger Programme, Funktionen, Ports, Protokolle und Services.	s3- account-level-public-access -blöcke-periodisch	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Simple Storage Service (Amazon S3) -Buckets nicht öffentlich zugänglich sind. Diese Regel trägt dazu bei, sensible Daten vor unbefugten Remote-Benutzern zu schützen, indem sie den öffentlichen Zugriff verhindert. Mit dieser Regel können Sie optional die Parameter ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) und restrictPublicBuckets Parameter (Config Default: True) festlegen. Die tatsächlichen Werte müssen den Richtlini

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			en Ihrer Organisation entsprechen.
CM.L2-3.4.7	Beschränken, deaktivieren oder verhindern Sie die Verwendung unnötiger Programme , Funktionen, Ports, Protokolle und Services.	s3- bucket-public-read -prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie nur autorisierten Benutzern, Prozessen und Geräten Zugriff auf Amazon Simple Storage Service (Amazon S3) - Buckets gewähren. Die Verwaltung des Zugriffs sollte mit der Klassifizierung der Daten übereinst immen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CM.L2-3.4.7	Beschränken, deaktivieren oder verhindern Sie die Verwendung unnötiger Programme, Funktionen, Ports, Protokolle und Services.	s3- bucket-public-write-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie nur autorisierten Benutzern, Prozessen und Geräten Zugriff auf Amazon Simple Storage Service (Amazon S3) - Buckets gewähren. Die Verwaltung des Zugriffs sollte mit der Klassifizierung der Daten übereinstimmen.
CM.L2-3.4.7	Beschränken, deaktivieren oder verhindern Sie die Verwendung unnötiger Programme, Funktionen, Ports, Protokolle und Services.	sagemaker-notebook-no-direct-Internetzugang	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass SageMaker Amazon-Notebooks keinen direkten Internetzugang zulassen. Indem Sie direkten Internetzugang blockieren, vermeiden Sie, dass unbefugte Benutzer auf sensible Daten zugreifen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CM.L2-3.4.7	Beschränken, deaktivieren oder verhindern Sie die Verwendung unnötiger Programme, Funktionen, Ports, Protokolle und Services.	ssm-document-not-public	Stellen Sie sicher, dass AWS Systems Manager (SSM) - Dokumente nicht öffentlich sind, da dies einen unbeabsichtigten Zugriff auf Ihre SSM-Dokumente ermöglichen kann. Ein öffentliches SSM-Dokument kann Informationen über Ihr Konto, Ihre Ressourcen und internen Prozesse preisgeben.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CM.L2-3.4.7	Beschränken, deaktivieren oder verhindern Sie die Verwendung unnötiger Programme , Funktionen, Ports, Protokolle und Services.	subnet-auto-assign-public-ip-deaktiviert	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon Virtual Private Cloud (VPC) -Subnetzen nicht automatisch eine öffentliche IP-Adresse zugewiesen wird. Amazon Elastic Compute Cloud (EC2) -Instances, die in Subnetzen gestartet werden, in denen dieses Attribut aktiviert ist, haben ihrer primären Netzwerkschnittstelle eine öffentliche IP-Adresse zugewiesen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CM.L2-3.4.7	Beschränken, deaktivieren oder verhindern Sie die Verwendung unnötiger Programme , Funktionen, Ports, Protokolle und Services.	vpc-default-security-group-geschlossen	Sicherheitsgruppen von Amazon Elastic Compute Cloud (Amazon EC2) können bei der Verwaltung des Netzwerkzugriffs helfen, indem sie eine statusbehaftete Filterung des ein- und ausgehenden Netzwerkverkehrs zu Ressourcen bereitstellen. AWS Die Beschränk ung des gesamten Datenverkehrs auf die Standardsicherheit sgruppe hilft dabei, den Fernzugriff auf Ihre Ressourcen einzuschränken. AWS

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CM.L2-3.4.7	Beschränken, deaktivieren oder verhindern Sie die Verwendung unnötiger Programme, Funktionen, Ports, Protokolle und Services.	vpc-sg-open-only-to-authorized-ports	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass gemeinsame Ports für Amazon Elastic Compute Cloud (Amazon EC2) -Sicherheitsgruppen eingeschränkt sind. Wenn der Zugriff auf Ports nicht auf vertrauenswürdige Quellen beschränkt wird, kann dies zu Angriffen auf die Verfügbarkeit, Integrität und Vertraulichkeit von Systemen führen. Durch die Beschränkung des Zugriffs auf Ressourcen innerhalb einer Sicherheitsgruppe aus dem Internet (0.0.0.0/0) kann der Remote-Zugriff auf interne Systeme gesteuert werden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CM.L2-3.4.9	Kontrollieren und überwachen Sie von Benutzern installierte Software.	ec2-manager instance-managed-by-systems	Eine Bestandsaufnahme der Softwareplattformen und Anwendungen innerhalb des Unternehmens ist möglich, indem Amazon Elastic Compute Cloud (Amazon EC2) - Instances mit AWS Systems Manager verwaltet werden. Verwenden Sie AWS Systems Manager, um detaillierte Systemkonfigurationen, Betriebssystem-Patch-Levels, Namen und Typ der Dienste, Softwareinstallationen, Anwendungsname, Herausgeber und Version sowie andere Details zu Ihrer Umgebung bereitzustellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CM.L2-3.4.9	Kontrollieren und überwachen Sie von Benutzern installierte Software.	ec2-check managedinstance-association-compliance-status	Verwenden Sie AWS Systems Manager Associations, um bei der Inventarisierung von Softwareplattformen und Anwendungen innerhalb eines Unternehmens zu helfen. AWS Systems Manager weist Ihren verwalteten Instanzen einen Konfigurationsstatus zu und ermöglicht es Ihnen, Basiswerte für Betriebssystem-Patch-Levels, Softwareinstallationen, Anwendungskonfigurationen und andere Details zu Ihrer Umgebung festzulegen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CM.L2-3.4.9	Kontrollieren und überwachen Sie von Benutzern installierte Software.	ec2-check managedinstance-patch-compliance-status	Aktivieren Sie diese Regel, um bei der Identifizierung und Dokumentation von Sicherheitslücken in Amazon Elastic Compute Cloud (Amazon EC2) zu helfen. Die Regel prüft, ob die EC2 Amazon-Instance die Patch-Konformität im AWS Systems Manager gemäß den Richtlinien und Verfahren Ihrer Organisation einhält.
IA.L2-3.5.1	Identifizieren Sie Benutzer von Informationssystemen, Prozesse von Benutzern oder Geräte.	api-gw-execution-logging-aktiviert	Die API-Gateway-Protokollierung zeigt detaillierte Ansichten der Benutzer, die auf die API zugegriffen haben, und wie diese Benutzer auf die API zugegriffen haben. Diese Einblicke ermöglichen die Transparenz von Benutzeraktivitäten.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
IA.L2-3.5.1	Identifizieren Sie Benutzer von Informationssystemen, Prozesse von Benutzern oder Geräte.	cloudtrail-s3-dataevents-enabled	Die Erfassung von Simple Storage Service (Amazon S3)-Datenereignissen unterstützt die Erkennung von ungewöhnlichen Aktivitäten. Zu den Details gehören AWS-Konto Informationen über den Zugriff auf einen Amazon S3 S3-Bucket, die IP-Adresse und die Uhrzeit des Ereignisses.
IA.L2-3.5.1	Identifizieren Sie Benutzer von Informationssystemen, Prozesse von Benutzern oder Geräte.	cloud-trail-cloud-watch-logs-aktiviert	Verwenden Sie Amazon CloudWatch , um Protokoll ereignisaktivitäten zentral zu sammeln und zu verwalten. Die Aufnahme von AWS CloudTrail Daten liefert Einzelheiten zu den API-Aufrufaktivitäten in Ihrem AWS-Konto.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
IA.L2-3.5.1	Identifizieren Sie Benutzer von Informationssystemen, Prozesse von Benutzern oder Geräte.	elb-logging-enabled	Die Elastic-Load-Balancing-Aktivität ist ein zentraler Kommunikationspunkt innerhalb einer Umgebung. Stellen Sie sicher, dass die ELB-Protokollierung aktiviert ist. Die gesammelten Daten enthalten detaillierte Informationen zu Anfragen, die an den ELB gesendet wurden. Jedes Protokoll enthält Informationen wie die Zeit, zu der die Anforderung einging, die Client-IP-Adresse, Latenzen, Anforderungspfade und Serverantworten.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
IA.L2-3.5.1	Identifizieren Sie Benutzer von Informationssystemen, Prozesse von Benutzern oder Geräte.	emr-kerberos-enabled	Die Zugriffsberechtigungen und -autorisierungen können verwaltet und nach den Prinzipien der geringsten Berechtigung und Aufgabentrennung integriert werden, indem Kerberos für Amazon-EMR-Cluster aktiviert wird. In Kerberos werden Services und Benutzer, die sich authentifizieren müssen, als Prinzipale bezeichnet. Prinzipale befinden sich in einem Kerberos-Bereich. Innerhalb dieses Bereichs wird ein Kerberos-Server als Key Distribution Center (KDC) bezeichnet. Über diesen Server können sich Prinzipale authentifizieren. Die Authentifizierung im KDC erfolgt durch die Ausstellung von Authentif

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			izierungstickets. Das KDC unterhält eine Datenbank der Prinzipale in seinem Bereich mit ihren Passwörtern und anderen administr ativen Informationen zu jedem Prinzipal.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
IA.L2-3.5.1	Identifizieren Sie Benutzer von Informationssystemen, Prozesse von Benutzern oder Geräte.	multi-region-cloudtrail-enabled	AWS CloudTrail zeichnet Aktionen und API-Aufrufe der AWS Management Console auf. Sie können feststellen, welche Benutzer und Konten angerufen wurden AWS, von welcher Quell-IP-Adresse aus die Anrufe getätigt wurden und wann die Anrufe erfolgten. CloudTrail übermittelt Protokolldateien aus allen AWS Regionen an Ihren S3-Bucket , wenn MULTI_REGION_CLOUD_TRAIL_ENABLED aktiviert ist. Außerdem wird beim AWS Start einer neuen Region derselbe Trail in der neuen Region erstellt. CloudTrail Dadurch erhalten Sie automatisch Protokolldateien mit API-Aktivitäten für die neue Region.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
IA.L2-3.5.1	Identifizieren Sie Benutzer von Informationssystemen, Prozesse von Benutzern oder Geräte.	rds-logging-enabled	Um die Protokollierung und Überwachung in Ihrer Umgebung zu erleichtern, stellen Sie sicher, dass die Amazon Relational Database Service (Amazon RDS)-Protokollierung aktiviert ist. Mit der Amazon-RDS-Protokollierung können Sie Ereignisse wie Verbindungen, Verbindungsabbrüche, Abfragen oder abgefragte Tabellen erfassen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
IA.L2-3.5.1	Identifizieren Sie Benutzer von Informationssystemen, Prozesse von Benutzern oder Geräte.	s-3 bucket-logging-enabled	Die Amazon Simple Storage Service (Amazon S3)-Serverzugriffsprotokollierung bietet eine Methode zur Überwachung des Netzwerks im Hinblick auf potenzielle Cybersicherheitsereignisse. Die Ereignisse werden überwacht, indem detaillierte Aufzeichnungen über die Anfragen erfasst werden, die an einen Amazon-S3-Bucket gestellt wurden. Jeder Zugriffsprotokolleintrag enthält Details zu einer einzelnen Zugriffsanfrage. Zu den Details gehören Anforderer, Bucket-Name, Anforderungszeit, Anforderungsaktion, Antwortstatus und Fehlercode, falls relevant.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
IA.L2-3.5.1	Identifizieren Sie Benutzer von Informationssystemen, Prozesse von Benutzern oder Geräte.	wafv2-logging-enabled	Um die Protokollierung und Überwachung in Ihrer Umgebung zu erleichtern, aktivieren Sie die AWS WAF (V2) -Protokollierung im regionalen und globalen Web. ACLs AWS Die WAF-Protokollierung bietet detaillierte Informationen über den Datenverkehr, der von Ihrer Web-ACL analysiert wird. In den Protokollen werden die Uhrzeit aufgezeichnet, zu der die AWS WAF die Anfrage von Ihrer AWS Ressource erhalten hat, Informationen über die Anfrage und eine Aktion für die Regel, der jede Anfrage entsprach.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
IA.L2-3.5.2	Authentifizieren (oder verifizieren) Sie die Identitäten dieser Benutzer, Prozesse oder Geräte als Voraussetzung für den Zugriff auf Informationssysteme der Organisation.	emr-kerberos-enabled	Die Zugriffsberechtigungen und -autorisierungen können verwaltet und nach den Prinzipien der geringsten Berechtigung und Aufgabentrennung integriert werden, indem Kerberos für Amazon-EMR-Cluster aktiviert wird. In Kerberos werden Services und Benutzer, die sich authentifizieren müssen, als Prinzipale bezeichnet. Prinzipale befinden sich in einem Kerberos-Bereich. Innerhalb dieses Bereichs wird ein Kerberos-Server als Key Distribution Center (KDC) bezeichnet. Über diesen Server können sich Prinzipale authentifizieren. Die Authentifizierung im KDC erfolgt durch die Ausstellung von Authentif

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			izierungstickets. Das KDC unterhält eine Datenbank der Prinzipale in seinem Bereich mit ihren Passwörtern und anderen administr ativen Informationen zu jedem Prinzipal.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
IA.L2-3.5.2	Authentifizieren (oder verifizieren) Sie die Identitäten dieser Benutzer, Prozesse oder Geräte als Voraussetzung für den Zugriff auf Informationssysteme der Organisation.	iam-password-policy	Die Identitäten und Anmeldeinformationen werden auf der Grundlage einer organisatorischen IAM-Passwortrichtlinie ausgestellt, verwaltet und verifiziert. Sie erfüllen oder übertreffen die Anforderungen von NIST SP 800-63 und dem Standard „Best Practices“ von AWS Foundational Security für Passwortstärke. Mit dieser Regel können Sie optional RequireUppercaseCharacters (Wert für AWS grundlegende Sicherheitsbewährte Methoden: wahr), RequireLowercaseCharacters (Wert für bewährte Methoden für AWS grundlegende Sicherheit: wahr), RequireSymbols (Wert für bewährte Methoden für AWS grundlegende Sicherheit:

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			wahr), RequireNumbers (Wert für bewährte Methoden für AWS grundlegende Sicherheit: wahr), MinimumPasswordLength (Wert für bewährte Methoden für AWS grundlegende Sicherheit: 14), PasswordReusePrevention (Wert für bewährte Methoden für AWS grundlegende Sicherheit: 24) und MaxPasswordAge (Wert für bewährte Methoden für AWS grundlegende Sicherheit: 90) für Ihr IAM festlegen Kennwortrichtlinie. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
IA.L2-3.5.2	Authentifizieren (oder verifizieren) Sie die Identitäten dieser Benutzer, Prozesse oder Geräte als Voraussetzung für den Zugriff auf Informationssysteme der Organisation.	iam-user-mfa-enabled	Aktivieren Sie diese Regel, um den Zugriff auf Ressourcen in der Cloud einzuschr änken. AWS Diese Regel sorgt dafür, dass die Multi-Fak tor-Authentifizier ung (MFA) für alle Benutzer aktiviert ist. MFA sorgt für eine weitere Schutzebe ne zusätzlich zu den Anmeldeinformation en. Reduzieren Sie Fälle von kompromit tierten Konten, indem Sie MFA für Benutzer vorschreiben.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
IA.L2-3.5.2	Authentifizieren (oder verifizieren) Sie die Identitäten dieser Benutzer, Prozesse oder Geräte als Voraussetzung für den Zugriff auf Informationssysteme der Organisation.	mfa-enabled-for-iam-Konsolenzugriff	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass MFA für alle AWS Identity and Access Management (IAM) -Benutzer aktiviert ist, die über ein Konsolenkennwort verfügen. MFA sorgt für eine weitere Schutzebene zusätzlich zu den Anmeldeinformationen. Indem Sie MFA für Benutzer vorschreiben, können Sie Fälle kompromittierter Konten reduzieren und verhindern, dass unbefugte Benutzer auf vertrauliche Daten zugreifen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
IA.L2-3.5.2	Authentifizieren (oder verifizieren) Sie die Identitäten dieser Benutzer, Prozesse oder Geräte als Voraussetzung für den Zugriff auf Informationssysteme der Organisation.	root-account-hardware-mfa-aktiviert	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Hardware-MFA für den Root-Benutzer aktiviert ist. Der Stammbenutzer ist der AWS-Konto-Benutzer mit den meisten Berechtigungen. MFA sorgt für eine weitere Schutzebene zusätzlich zu den Anmeldeinformationen. Indem Sie MFA für den Root-Benutzer vorschreiben, können Sie die Anzahl AWS-Konten kompromittierter Benutzer reduzieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
IA.L2-3.5.2	Authentifizieren (oder verifizieren) Sie die Identitäten dieser Benutzer, Prozesse oder Geräte als Voraussetzung für den Zugriff auf Informationssysteme der Organisation.	root-account-mfa-enabled	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass MFA für den Root-Benutzer aktiviert ist. Der Stammbenutzer ist der AWS-Konto-Benutzer mit den meisten Berechtigungen. MFA sorgt für eine weitere Schutzebene zusätzlich zu den Anmeldeinformationen. Indem Sie MFA für den Root-Benutzer vorschreiben, können Sie die Anzahl AWS-Konten kompromittierter Benutzer reduzieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
IA.L2-3.5.3	Verwenden Sie die Multi-Faktor-Authentifizierung für den lokalen und Netzwerkzugriff auf privilegierte Konten und für den Netzwerkzugriff auf nicht privilegierte Konten.	iam-user-mfa-enabled	Aktivieren Sie diese Regel, um den Zugriff auf Ressourcen in der AWS Cloud einzuschränken. Diese Regel sorgt dafür, dass die Multi-Faktor-Authentifizierung (MFA) für alle Benutzer aktiviert ist. MFA sorgt für eine weitere Schutzebene zusätzlich zu den Anmeldeinformationen. Reduzieren Sie Fälle von kompromittierten Konten, indem Sie MFA für Benutzer vorschreiben.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
IA.L2-3.5.3	Verwenden Sie die Multi-Faktor-Authentifizierung für den lokalen und Netzwerkzugriff auf privilegierte Konten und für den Netzwerkzugriff auf nicht privilegierte Konten.	mfa-enabled-for-iam-Konsolenzugriff	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass MFA für alle AWS Identity and Access Management (IAM) -Benutzer aktiviert ist, die über ein Konsolenkennwort verfügen. MFA sorgt für eine weitere Schutzebene zusätzlich zu den Anmeldeinformationen. Indem Sie MFA für Benutzer vorschreiben, können Sie Fälle kompromittierter Konten reduzieren und verhindern, dass unbefugte Benutzer auf vertrauliche Daten zugreifen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
IA.L2-3.5.3	Verwenden Sie die Multi-Faktor-Authentifizierung für den lokalen und Netzwerkzugriff auf privilegierte Konten und für den Netzwerkzugriff auf nicht privilegierte Konten.	root-account-hardware-mfa-aktiviert	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Hardware-MFA für den Root-Benutzer aktiviert ist. Der Stammbenutzer ist der AWS-Konto-Benutzer mit den meisten Berechtigungen. MFA sorgt für eine weitere Schutzebene zusätzlich zu den Anmeldeinformationen. Indem Sie MFA für den Root-Benutzer vorschreiben, können Sie die Anzahl AWS-Konten kompromittierter Benutzer reduzieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
IA.L2-3.5.3	Verwenden Sie die Multi-Faktor-Authentifizierung für den lokalen und Netzwerkzugriff auf privilegierte Konten und für den Netzwerkzugriff auf nicht privilegierte Konten.	root-account-mfa-enabled	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass MFA für den Root-Benutzer aktiviert ist. Der Stammbenutzer ist der AWS-Konto-Benutzer mit den meisten Berechtigungen. MFA sorgt für eine weitere Schutzebene zusätzlich zu den Anmeldeinformationen. Indem Sie MFA für den Root-Benutzer vorschreiben, können Sie die Anzahl AWS-Konten kompromittierter Benutzer reduzieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
IA.L2-3.5.6	Deaktivieren Sie Identifikatoren nach einem bestimmten Zeitraum der Inaktivität.	iam-password-policy	Die Identitäten und Anmeldeinformationen werden auf der Grundlage einer organisatorischen IAM-Passwortrichtlinie ausgestellt, verwaltet und verifiziert. Sie erfüllen oder übertreffen die Anforderungen von NIST SP 800-63 und dem Standard „Best Practices“ von AWS Foundational Security für die Passwortstärke. Mit dieser Regel können Sie optional RequireUppercaseCharacters (Wert für AWS grundlegende Sicherheitsbewährte Methoden: wahr), RequireLowercaseCharacters (Wert für bewährte Methoden für AWS grundlegende Sicherheit: wahr), RequireSymbols (Wert für bewährte Methoden für AWS grundlegende Sicherheit:

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			wahr), RequireNumbers (Wert für bewährte Methoden für AWS grundlegende Sicherheit: wahr), MinimumPasswordLength (Wert für bewährte Methoden für AWS grundlegende Sicherheit: 14), PasswordReusePrevention (Wert für bewährte Methoden für AWS grundlegende Sicherheit: 24) und MaxPasswordAge (Wert für bewährte Methoden für AWS grundlegende Sicherheit: 90) für Ihr IAM festlegen Kennwortrichtlinie. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
IA.L2-3.5.6	Deaktivieren Sie Identifikatoren nach einem bestimmten Zeitraum der Inaktivität.	iam-user-unused-credentials-überprüfen	AWS Identity and Access Management (IAM) kann Ihnen bei Zugriffsberechtigungen und Autorisierungen helfen, indem es nach IAM-Passwörtern und Zugriffsschlüsseln sucht, die für einen bestimmten Zeitraum nicht verwendet wurden. Wenn ungenutzte Anmeldeinformationen identifiziert werden, müssen Sie sie deaktivieren und/oder entfernen, da dies gegen das Prinzip der geringsten Berechtigung verstoßen könnte. Für diese Regel müssen Sie einen Wert für das maxCredentialUsage Alter festlegen (Standardkonfiguration: 90). Der tatsächliche Wert muss den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
IA.L2-3.5.7	Erzwingen Sie bei der Erstellung neuer Passwörter eine Mindestkomplexität und eine Änderung der Zeichen.	iam-password-policy	Die Identitäten und Anmeldeinformationen werden auf der Grundlage einer organisatorischen IAM-Passwortrichtlinie ausgestellt, verwaltet und verifiziert. Sie erfüllen oder übertreffen die Anforderungen von NIST SP 800-63 und dem Standard „Best Practices“ von AWS Foundational Security für die Passwortstärke. Mit dieser Regel können Sie optional RequireUppercaseCharacters (Wert für AWS grundlegende Sicherheitsbewährte Methoden: wahr), RequireLowercaseCharacters (Wert für bewährte Methoden für AWS grundlegende Sicherheit: wahr), RequireSymbols (Wert für bewährte Methoden für AWS grundlegende Sicherheit:

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			wahr), RequireNumbers (Wert für bewährte Methoden für AWS grundlegende Sicherheit: wahr), MinimumPasswordLength (Wert für bewährte Methoden für AWS grundlegende Sicherheit: 14), PasswordReusePrevention (Wert für bewährte Methoden für AWS grundlegende Sicherheit: 24) und MaxPasswordAge (Wert für bewährte Methoden für AWS grundlegende Sicherheit: 90) für Ihr IAM festlegen Kennwortrichtlinie. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
IA.L2-3.5.8	Verbietet die Wiederverwendung von Passwörtern für eine bestimmte Anzahl neu generiert er Passwörter.	iam-password-policy	Die Identitäten und Anmeldeinformation en werden auf der Grundlage einer organisatorischen IAM-Passwortrichtlinie ausgestellt, verwaltet und verifiziert. Sie erfüllen oder übertreff en die Anforderu ngen des NIST SP 800-63 und des AWS Foundatio nal Security Best Practices-Standards für Passwortstärke. Mit dieser Regel können Sie optional RequireUppercaseCh aracters (Wert für AWS grundlegende Sicherheitsbewährt e Methoden: wahr), RequireLowercaseCh aracters (Wert für bewährte Methoden für AWS grundlege nde Sicherheit: wahr), RequireSy mbols (Wert für bewährte Methoden für AWS grundlege nde Sicherheit:

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			wahr), RequireNumbers (Wert für bewährte Methoden für AWS grundlegende Sicherheit: wahr), MinimumPasswordLength (Wert für bewährte Methoden für AWS grundlegende Sicherheit: 14), PasswordReusePrevention (Wert für bewährte Methoden für AWS grundlegende Sicherheit: 24) und MaxPasswordAge (Wert für bewährte Methoden für AWS grundlegende Sicherheit: 90) für Ihr IAM festlegen Kennwortrichtlinie. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
IA.L2-3.5.10	Speichern und übertragen Sie nur kryptografisch geschützte Passwörter.	alb-http-drop-invalid-Header-fähig	Stellen Sie sicher, dass Ihre Elastic Load Balancers (ELB) so konfiguriert sind, dass sie HTTP-Header löschen. Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.
IA.L2-3.5.10	Speichern und übertragen Sie nur kryptografisch geschützte Passwörter.	alb-http-to-https-Umleitungsprüfung	Um Daten während der Übertragung zu schützen, stellen Sie sicher, dass Ihr Application Load Balancer unverschlüsselte HTTP-Anfragen automatisch an HTTPS umleitet. Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
IA.L2-3.5.10	Speichern und übertragen Sie nur kryptografisch geschützte Passwörter.	api-gw-cache-enabled-und-verschlüsselt	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass die Verschlüsselung für den Cache Ihrer API-Gateway-Stufe aktiviert ist. Da für die API-Methode sensible Daten erfasst werden können, sollten Sie die Verschlüsselung von Daten im Ruhezustand aktivieren, um diese Daten zu schützen.
IA.L2-3.5.10	Speichern und übertragen Sie nur kryptografisch geschützte Passwörter.	api-gw-ssl-enabled	Stellen Sie sicher, dass die REST-API-Stufen von Amazon API Gateway mit SSL-Zertifikaten konfiguriert sind, damit Backend-Systeme überprüfen können, ob Anforderungen von API Gateway stammen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
IA.L2-3.5.10	Speichern und übertragen Sie nur kryptografisch geschützte Passwörter.	ec2- ebs-encryption-by-default	Zum Schutz von Daten im Ruhezustand müssen Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon Elastic Block Store (Amazon EBS)-Volumes aktiviert ist. Da sensible Daten auch im Ruhezustand vorhanden sein können, sollten Sie die Verschlüsselung im Ruhezustand aktivieren, um diese Daten zu schützen.
IA.L2-3.5.10	Speichern und übertragen Sie nur kryptografisch geschützte Passwörter.	efs-encrypted-check	Aktivieren Sie die Verschlüsselung für Ihr Amazon Elastic File System (EFS), um eventuell vorhandene sensible Daten sowie Daten im Ruhezustand zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
IA.L2-3.5.10	Speichern und übertragen Sie nur kryptografisch geschützte Passwörter.	elasticsearch-encrypted-at-rest	Da sensible Daten vorhanden sein können und um Daten im Ruhezustand zu schützen, sollten Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon OpenSearch Service (OpenSearch Service) -Domains aktiviert ist.
IA.L2-3.5.10	Speichern und übertragen Sie nur kryptografisch geschützte Passwörter.	elasticsearch-node-to-node-Verschlüsselungsprüfung	Stellen Sie sicher, dass die node-to-node Verschlüsselung für Amazon OpenSearch Service aktiviert ist. Node-to-nodeVerschlüsselung ermöglicht die TLS 1.2-Verschlüsselung für die gesamte Kommunikation innerhalb der Amazon Virtual Private Cloud (Amazon VPC). Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
IA.L2-3.5.10	Speichern und übertragen Sie nur kryptografisch geschützte Passwörter.	elbv-2 acm-certificate-required	Zum Schutz von eventuell vorhandenen sensiblen Daten sowie von Daten während der Übertragung muss die Verschlüsselung für Ihr Elastic Load Balancing aktiviert sein. Verwenden Sie AWS Certificate Manager, um öffentliche und private SSL/TLS-Zertifikate mit AWS Diensten und internen Ressourcen zu verwalten, bereitzustellen und bereitzustellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
IA.L2-3.5.10	Speichern und übertragen Sie nur kryptografisch geschützte Passwörter.	elb-acm-certificate-required	Zum Schutz von eventuell vorhandenen sensiblen Daten sowie von Daten während der Übertragung muss die Verschlüsselung für Ihr Elastic Load Balancing aktiviert sein. Verwenden Sie AWS Certificate Manager, um öffentliche und private SSL/TLS-Zertifikate mit AWS Diensten und internen Ressourcen zu verwalten, bereitzustellen und bereitzustellen.
IA.L2-3.5.10	Speichern und übertragen Sie nur kryptografisch geschützte Passwörter.	elb-tls-https-listeners-nur	Stellen Sie sicher, dass Ihre Elastic Load Balancer (ELBs) mit SSL- oder HTTPS-Listenern konfiguriert sind. Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
IA.L2-3.5.10	Speichern und übertragen Sie nur kryptografisch geschützte Passwörter.	encrypted-volumes	Aktivieren Sie die Verschlüsselung für Ihre Amazon-Elastic-Block-Store (Amazon-EBS)-Volumes, um eventuell vorhandene sensible Daten sowie Daten im Ruhezustand zu schützen.
IA.L2-3.5.10	Speichern und übertragen Sie nur kryptografisch geschützte Passwörter.	rds-snapshot-encrypted	Stellen Sie sicher, dass die Verschlüsselung für Ihre Amazon Relational Database Service (Amazon RDS)-Snapshots aktiviert ist. Da sensible Daten auch im Ruhezustand vorhanden sein können, sollten Sie die Verschlüsselung im Ruhezustand aktivieren, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
IA.L2-3.5.10	Speichern und übertragen Sie nur kryptografisch geschützte Passwörter.	rds-storage-encrypted	Zum Schutz von Daten im Ruhezustand müssen Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon Relational Database Service (Amazon RDS)-Instances aktiviert ist. Um eventuell vorhandene sensible Daten im Ruhezustand in Amazon-RDS-Instances zu schützen, muss die Verschlüsselung von Daten im Ruhezustand aktiviert sein.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
IA.L2-3.5.10	Speichern und übertragen Sie nur kryptografisch geschützte Passwörter.	redshift-cluster-kms-enabled	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass die Verschlüsselung mit AWS Key Management Service (AWS KMS) für Ihren Amazon Redshift Redshift-Cluster aktiviert ist. Um eventuell vorhandene sensible Daten im Ruhezustand in Redshift-Clustern zu schützen, muss die Verschlüsselung von Daten im Ruhezustand aktiviert sein.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
IA.L2-3.5.10	Speichern und übertragen Sie nur kryptografisch geschützte Passwörter.	redshift-require-tls-ssl	Stellen Sie sicher, dass Ihre Amazon-Redshift-Cluster eine TLS/SSL-Verschlüsselung erfordern, um eine Verbindung zu SQL-Clients herzustellen. Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.
IA.L2-3.5.10	Speichern und übertragen Sie nur kryptografisch geschützte Passwörter.	s3- aktiviert bucket-server-side-encryption	Zum Schutz von Daten im Ruhezustand müssen Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon Simple Storage Service (Amazon S3)-Buckets aktiviert ist. Um eventuell vorhandene sensible Daten im Ruhezustand in Amazon-S3-Buckets zu schützen, muss die Verschlüsselung aktiviert sein.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
IA.L2-3.5.10	Speichern und übertragen Sie nur kryptografisch geschützte Passwörter.	s-3 bucket-ssl-requests-only	Um Daten während der Übertragung zu schützen, stellen Sie sicher, dass Ihre Amazon Simple Storage Service (Amazon S3)-Buckets Anfragen zur Verwendung von Secure Socket Layer (SSL)-Buckets erfordern. Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.
IA.L2-3.5.10	Speichern und übertragen Sie nur kryptografisch geschützte Passwörter.	s-3 default-encryption-kms	Stellen Sie sicher, dass die Verschlüsselung für Ihre Amazon Simple Storage Service (Amazon S3)-Buckets aktiviert ist. Um eventuell vorhandene sensible Daten im Ruhezustand in einem Amazon-S3-Bucket zu schützen, muss die Verschlüsselung aktiviert sein.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
IA.L2-3.5.10	Speichern und übertragen Sie nur kryptografisch geschützte Passwörter.	sagemaker-endpoint-configuration-kms-key-konfiguriert	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass die Verschlüsselung mit dem AWS Key Management Service (AWS KMS) für Ihren Endpunkt aktiviert ist. SageMaker Da sensible Daten auf dem SageMaker Endgerät gespeichert werden können, sollten Sie die Verschlüsselung im Ruhezustand aktivieren, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
IA.L2-3.5.10	Speichern und übertragen Sie nur kryptografisch geschützte Passwörter.	sagemaker-notebook-instance-kms-schlüsselkonfiguriert	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass die Verschlüsselung mit dem AWS Key Management Service (AWS KMS) für Ihr Notebook aktiviert ist. SageMaker Da vertrauliche Daten im SageMaker Notebook gespeichert werden können, sollten Sie die Verschlüsselung im Ruhezustand aktivieren, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
IA.L2-3.5.10	Speichern und übertragen Sie nur kryptografisch geschützte Passwörter.	sns-encrypted-kms	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass Ihre Amazon Simple Notification Service (Amazon SNS) -Themen mit dem AWS Key Management Service (AWS KMS) verschlüsselt werden müssen. Um eventuell vorhandene sensible Daten im Ruhezustand in veröffentlichten Nachrichten zu schützen, muss die Verschlüsselung von Daten im Ruhezustand aktiviert sein.
IA.L2-3.5.10	Speichern und übertragen Sie nur kryptografisch geschützte Passwörter.	opensearch-encrypted-at-rest	Da sensible Daten vorhanden sein können und um Daten im Ruhezustand zu schützen, sollten Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon OpenSearch Service-Domains aktiviert ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
IA.L2-3.5.10	Speichern und übertragen Sie nur kryptografisch geschützte Passwörter.	opensearch-node-to-node-Verschlüsselungsprüfung	Stellen Sie sicher, dass die node-to-node Verschlüsselung für Amazon OpenSearch Service aktiviert ist. Node-to-nodeVerschlüsselung ermöglicht die TLS 1.2-Verschlüsselung für die gesamte Kommunikation innerhalb der Amazon Virtual Private Cloud (Amazon VPC). Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
IR.L2-3.6.1	Richten Sie eine Funktion zur Bearbeitung von Betriebsvorfällen für Organisationssysteme ein, die Maßnahmen zur Vorbereitung, Erkennung, Analyse, Eindämmung und Wiederherstellung sowie Benutzerr eaktionen umfasst.	guardduty-enabled-centralized	Amazon GuardDuty kann mithilfe von Threat Intellige nce Feeds helfen, potenzielle Cybersich erheitsereignisse zu überwachen und zu erkennen. Dazu gehören Listen mit bösartigen IPs und maschinel len Lernmethoden zur Identifizierung unerwarteter, nicht autorisierter und bösartiger Aktivitäten in Ihrer AWS Cloud-Umgebung.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
IR.L2-3.6.1	Richten Sie eine Funktion zur Bearbeitung von Betriebsvorfällen für Organisationssysteme ein, die Maßnahmen zur Vorbereitung, Erkennung, Analyse, Eindämmung und Wiederherstellung sowie Benutzerreaktionen umfasst.	guardduty-non-archived-findings	Amazon GuardDuty hilft Ihnen dabei, die Auswirkungen eines Vorfalls zu verstehen, indem es die Ergebnisse nach Schweregrad klassifiziert: niedrig, mittel und hoch. Diese Klassifizierungen können Sie zur Festlegung von entsprechenden Strategien und Prioritäten zur Behebung solcher Vorfälle verwenden. Mit dieser Regel können Sie optional daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7) und daysHighSev (Config Default: 1) für nicht archivierte Ergebnisse festlegen, wie es die Richtlinien Ihrer Organisation erfordern.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
IR.L2-3.6.1	Richten Sie eine Funktion zur Bearbeitung von Betriebsvorfällen für Organisationssysteme ein, die Maßnahmen zur Vorbereitung, Erkennung, Analyse, Eindämmung und Wiederherstellung sowie Benutzerr eaktionen umfasst.	lambda-dlq-check	Aktivieren Sie diese Regel, um das entsprechende Personal über Amazon Simple Queue Service (Amazon SQS) oder Amazon Simple Notification Service (Amazon SNS) zu benachrichtigen, wenn eine Funktion ausgefallen ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
IR.L2-3.6.1	Richten Sie eine Funktion zur Bearbeitung von Betriebsvorfällen für Organisationssysteme ein, die Maßnahmen zur Vorbereitung, Erkennung, Analyse, Eindämmung und Wiederherstellung sowie Benutzerr eaktionen umfasst.	securityhub-enabled	AWS Security Hub hilft bei der Überwachung von unbefugtem Personal, Verbindun gen, Geräten und Software. AWS Security Hub aggregiert, organisie rt und priorisie rt die Sicherhei tswarnungen oder Ergebnisse mehrerer Dienste. AWS Einige dieser Dienste sind Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer und AWS Firewall Manager sowie AWS Partnerlösungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
IR.L2-3.6.3	Testen Sie die Reaktionsfähigkeit der Organisation auf Vorfälle.	response-plan-tested (Prozessüberprüfung)	Stellen Sie sicher, dass die Vorfallre aktions- und Wiederherstellungs pläne getestet wurden. Dies kann Ihnen helfen zu verstehen, ob Ihr Plan bei einem Vorfall wirksam ist und ob etwaige Lücken behoben oder Aktualisierungen vorgenommen werden müssen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
MA.L2-3.7.5	Erfordert eine mehrstufige Authentifizierung, um nichtlokale Wartungssitzungen von externen Netzwerkverbindungen aus einzurichten und solche Verbindungen zu beenden, wenn die nichtlokale Wartung abgeschlossen ist.	iam-user-mfa-enabled	Aktivieren Sie diese Regel, um den Zugriff auf Ressourcen in der Cloud einzuschränken. AWS Diese Regel sorgt dafür, dass die Multi-Faktor-Authentifizierung (MFA) für alle Benutzer aktiviert ist. MFA sorgt für eine weitere Schutzebene zusätzlich zu den Anmeldeinformationen. Reduzieren Sie Fälle von kompromittierten Konten, indem Sie MFA für Benutzer vorschreiben.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
MA.L2-3.7.5	Erfordern Sie eine Multifaktor-Authentifizierung, um nichtlokale Wartungssitzungen von externen Netzwerkverbindungen aus einzurichten und solche Verbindungen zu beenden, wenn die nichtlokale Wartung abgeschlossen ist.	mfa-enabled-for-iam-Konsolenzugriff	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass MFA für alle AWS Identity and Access Management (IAM) -Benutzer aktiviert ist, die über ein Konsolenkennwort verfügen. MFA sorgt für eine weitere Schutzebene zusätzlich zu den Anmeldeinformationen. Indem Sie MFA für Benutzer vorschreiben, können Sie Fälle kompromittierter Konten reduzieren und verhindern, dass unbefugte Benutzer auf vertrauliche Daten zugreifen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
RA.L2-3.11.2	Suchen Sie regelmäßig nach Schwachstellen in den Systemen und Anwendungen der Organisation und bei der Identifizierung neuer Schwachstellen in diesen Systemen und Anwendungen.	ec2-check managedinstance-patch-compliance-status	Aktivieren Sie diese Regel, um bei der Identifizierung und Dokumentation von Sicherheitslücken in Amazon Elastic Compute Cloud (Amazon EC2) zu helfen. Die Regel prüft, ob die EC2 Amazon-Instance die Patch-Konformität im AWS Systems Manager gemäß den Richtlinien und Verfahren Ihrer Organisation einhält.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
RA.L2-3.11.2	Suchen Sie regelmäßig nach Schwachstellen in den Systemen und Anwendungen der Organisation und bei der Identifizierung neuer Schwachstellen in diesen Systemen und Anwendungen.	guardduty-enabled-centralized	Amazon GuardDuty kann mithilfe von Threat Intelligence Feeds helfen, potenzielle Cybersicherheitsereignisse zu überwachen und zu erkennen. Dazu gehören Listen mit bösartigen IPs und maschinellen Lernmethoden zur Identifizierung unerwarteter, nicht autorisierter und bösartiger Aktivitäten in Ihrer AWS Cloud-Umgebung.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
RA.L2-3.11.2	Suchen Sie regelmäßig nach Schwachstellen in den Systemen und Anwendungen der Organisation und bei der Identifizierung neuer Schwachstellen in diesen Systemen und Anwendungen.	guardduty-non-archived-findings	Amazon GuardDuty hilft Ihnen dabei, die Auswirkungen eines Vorfalls zu verstehen, indem es die Ergebnisse nach Schweregrad klassifiziert: niedrig, mittel und hoch. Diese Klassifizierungen können Sie zur Festlegung von entsprechenden Strategien und Prioritäten zur Behebung solcher Vorfälle verwenden. Mit dieser Regel können Sie optional daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7) und daysHighSev (Config Default: 1) für nicht archivierte Ergebnisse festlegen, wie es die Richtlinien Ihrer Organisation erfordern.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
RA.L2-3.11.2	Suchen Sie regelmäßig nach Schwachstellen in den Systemen und Anwendungen der Organisation und bei der Identifizierung neuer Schwachstellen in diesen Systemen und Anwendungen.	securityhub-enabled	AWS Security Hub hilft bei der Überwachung von unbefugtem Personal, Verbindungen, Geräten und Software. AWS Security Hub aggregiert, organisiert und priorisiert die Sicherheitswarnungen oder Ergebnisse mehrerer Dienste. AWS Einige dieser Dienste sind Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer und AWS Firewall Manager sowie AWS Partnerlösungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC.L2-3.13.1	Überwachen, kontrollieren und schützen Sie die Unternehmenskommunikation (d. h. Informationen, die von Informationssystemen der Organisation übertragen oder empfangen werden) an externen und wichtigen internen Grenzen der Informationssysteme.	alb-http-drop-invalid-Header-fähig	Stellen Sie sicher, dass Ihre Elastic Load Balancers (ELB) so konfiguriert sind, dass sie HTTP-Header löschen. Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.
SC.L2-3.13.1	Überwachen, kontrollieren und schützen Sie die Unternehmenskommunikation (d. h. Informationen, die von Informationssystemen der Organisation übertragen oder empfangen werden) an externen und wichtigen internen Grenzen der Informationssysteme.	alb-http-to-https-Umleitungsprüfung	Um Daten während der Übertragung zu schützen, stellen Sie sicher, dass Ihr Application Load Balancer unverschlüsselte HTTP-Anfragen automatisch an HTTPS umleitet. Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC.L2-3.13.1	Überwachen, kontrollieren und schützen Sie die Unternehmenskommunikation (d. h. Informationen, die von Informationssystemen der Organisation übertragen oder empfangen werden) an externen und wichtigen internen Grenzen der Informationssysteme.	alb-waf-enabled	Stellen Sie sicher, dass AWS WAF auf Elastic Load Balancers (ELB) aktiviert ist, um Webanwendungen zu schützen. Eine WAF trägt zum Schutz Ihrer Webanwendungen oder APIs vor gängigen Web-Exploits bei. Diese Web-Exploits können sich auf die Verfügbarkeit auswirken, die Sicherheit gefährden oder übermäßige Ressourcen in Ihrer Umgebung verbrauchen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC.L2-3.13.1	Überwachen, kontrollieren und schützen Sie die Unternehmenskommunikation (d. h. Informationen, die von Informationssystemen der Organisation übertragen oder empfangen werden) an externen und wichtigen internen Grenzen der Informationssysteme.	api-gw-associated-with-WAF	AWS Mit WAF können Sie eine Reihe von Regeln (als Web Access Control List (Web ACL) bezeichnet) konfigurieren, die Webanfragen auf der Grundlage von anpassbaren Websicherheitsregeln und -bedingungen, die Sie definieren, zulassen, blockieren oder zählen. Stellen Sie sicher, dass Ihre Amazon-API-Gateway-Stufe mit einer WAF-Web-ACL verknüpft ist, um sie vor böswilligen Angriffen zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC.L2-3.13.1	Überwachen, kontrollieren und schützen Sie die Unternehmenskommunikation (d. h. Informationen, die von Informationssystemen der Organisation übertragen oder empfangen werden) an externen und wichtigen internen Grenzen der Informationssysteme.	cloudwatch-alarm-action-check	Amazon CloudWatch alarmiert, wenn eine Metrik den Schwellenwert für eine bestimmte Anzahl von Bewertungszeiträumen überschreitet. Der Alarm führt eine oder mehrere Aktionen durch, die vom Wert der Metrik oder des Ausdrucks im Vergleich zu einem Schwellenwert in einer Reihe von Zeiträumen abhängt. Diese Regel erfordert einen Wert für alarmActionRequired (Config Default: True), insufficientDataAction Required (Config Default: True), okActionRequired (Config Default: False). Der tatsächliche Wert muss die Alarmaktionen für Ihre Umgebung widerspiegeln.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC.L2-3.13.1	Überwachen, kontrollieren und schützen Sie die Unternehmenskommunikation (d. h. Informationen, die von Informationssystemen der Organisation übertragen oder empfangen werden) an externen und wichtigen internen Grenzen der Informationssysteme.	dms-replication-not-public	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass auf DMS-Replikationsinstanzen nicht öffentlich zugegriffen werden kann. DMS-Replikations-Instances können vertrauliche Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.
SC.L2-3.13.1	Überwachen, kontrollieren und schützen Sie die Unternehmenskommunikation (d. h. Informationen, die von Informationssystemen der Organisation übertragen oder empfangen werden) an externen und wichtigen internen Grenzen der Informationssysteme.	ebs-snapshot-public-restorable-überprüfen	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass EBS-Snapshots nicht öffentlich wiederherstellbar sind. EBS-Volume-Snapshots können vertrauliche Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC.L2-3.13.1	Überwachen, kontrollieren und schützen Sie die Unternehmenskommunikation (d. h. Informationen, die von Informationssystemen der Organisation übertragen oder empfangen werden) an externen und wichtigen internen Grenzen der Informationssysteme.	elasticsearch-in-vpc-only	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass sich Amazon OpenSearch OpenSearch Service (Service) - Domains innerhalb einer Amazon Virtual Private Cloud (Amazon VPC) befinden. Eine OpenSearch Service-Domain innerhalb einer Amazon VPC ermöglicht die sichere Kommunikation zwischen OpenSearch Service und anderen Services innerhalb der Amazon VPC, ohne dass ein Internet-Gateway, ein NAT-Gerät oder eine VPN-Verbindung erforderlich ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC.L2-3.13.1	Überwachen, kontrollieren und schützen Sie die Unternehmenskommunikation (d. h. Informationen, die von Informationssystemen der Organisation übertragen oder empfangen werden) an externen und wichtigen internen Grenzen der Informationssysteme.	elasticsearch-node-to-node-Verschlüsselungsprüfung	Stellen Sie sicher, dass die node-to-node Verschlüsselung für Amazon OpenSearch Service aktiviert ist. Node-to-nodeVerschlüsselung ermöglicht die TLS 1.2-Verschlüsselung für die gesamte Kommunikation innerhalb der Amazon Virtual Private Cloud (Amazon VPC). Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC.L2-3.13.1	Überwachen, kontrollieren und schützen Sie die Unternehmenskommunikation (d. h. Informationen, die von Informationssystemen der Organisation übertragen oder empfangen werden) an externen und wichtigen internen Grenzen der Informationssysteme.	elb-acm-certificate-required	Zum Schutz von eventuell vorhanden en sensiblen Daten sowie von Daten während der Übertragung muss die Verschlüsselung für Ihr Elastic Load Balancing aktiviert sein. Verwenden Sie AWS Certificate Manager, um öffentliche und private SSL/TLS-Zertifikate mit AWS Diensten und internen Ressourcen zu verwalten, bereitzustellen und bereitzustellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC.L2-3.13.1	Überwachen, kontrollieren und schützen Sie die Unternehmenskommunikation (d. h. Informationen, die von Informationssystemen der Organisation übertragen oder empfangen werden) an externen und wichtigen internen Grenzen der Informationssysteme.	elb-tls-https-listeners-nur	Stellen Sie sicher, dass Ihre Elastic Load Balancer (ELBs) mit SSL- oder HTTPS-Listenern konfiguriert sind. Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.
SC.L2-3.13.1	Überwachen, kontrollieren und schützen Sie die Unternehmenskommunikation (d. h. Informationen, die von Informationssystemen der Organisation übertragen oder empfangen werden) an externen und wichtigen internen Grenzen der Informationssysteme.	guardduty-enabled-centralized	Amazon GuardDuty kann mithilfe von Threat Intelligence Feeds helfen, potenzielle Cybersicherheitsereignisse zu überwachen und zu erkennen. Dazu gehören Listen mit bösartigen IPs und maschinellen Lernmethoden zur Identifizierung unerwarteter, nicht autorisierter und bösartiger Aktivitäten in Ihrer AWS Cloud-Umgebung.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC.L2-3.13.1	Überwachen, kontrollieren und schützen Sie die Unternehmenskommunikation (d. h. Informationen, die von Informationssystemen der Organisation übertragen oder empfangen werden) an externen und wichtigen internen Grenzen der Informationssysteme.	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) Security Groups können bei der Verwaltung des Netzwerkzugriffs helfen, indem sie eine statusbehaftete Filterung von eingehendem und ausgehendem Netzwerkverkehr zu Ressourcen bereitstellen. AWS Wenn Sie eingehenden (oder entfernten) Datenverkehr von 0.0.0.0/0 bis Port 22 auf Ihren Ressourcen nicht zulassen, können Sie den Remote-Zugriff einschränken.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC.L2-3.13.1	Überwachen, kontrollieren und schützen Sie die Unternehmenskommunikation (d. h. Informationen, die von Informationssystemen der Organisation übertragen oder empfangen werden) an externen und wichtigen internen Grenzen der Informationssysteme.	ec-2 instances-in-vpc	Stellen Sie Amazon Elastic Compute Cloud (Amazon EC2) -Instances innerhalb einer Amazon Virtual Private Cloud (Amazon VPC) bereit, um eine sichere Kommunikation zwischen einer Instance und anderen Services innerhalb der Amazon VPC zu ermöglichen, ohne dass ein Internet-Gateway, ein NAT-Gerät oder eine VPN-Verbindung erforderlich ist. Der gesamte Datenverkehr bleibt sicher in der AWS Cloud. Domains, die sich innerhalb einer VPC befinden, verfügen aufgrund ihrer logischen Isolierung im Vergleich zu Domains mit öffentlichen Endpunkten über eine zusätzliche Sicherheitsebene. Weisen Sie EC2

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			Amazon-Instances einer Amazon-VPC zu, um den Zugriff ordnungsgemäß zu verwalten.
SC.L2-3.13.1	Überwachen, kontrollieren und schützen Sie die Unternehmenskommunikation (d. h. Informationen, die von Informationssystemen der Organisation übertragen oder empfangen werden) an externen und wichtigen internen Grenzen der Informationssysteme.	internet-gateway-authorized-vpc-nur	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Internet-Gateways nur mit autorisierter Amazon Virtual Private Cloud (Amazon VPC) verbunden sind. Internet-Gateways ermöglichen den bidirektionalen Internetzugang zur und von der Amazon VPC, was möglicherweise zu einem unbefugten Zugriff auf Amazon-VPC-Ressourcen führen kann.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC.L2-3.13.1	Überwachen, kontrollieren und schützen Sie die Unternehmenskommunikation (d. h. Informationen, die von Informationssystemen der Organisation übertragen oder empfangen werden) an externen und wichtigen internen Grenzen der Informationssysteme.	lambda-function-public-access-verboten	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass AWS Lambda-Funktionen nicht öffentlich zugänglich sind. Der öffentliche Zugriff kann möglicherweise die Verfügbarkeit von Ressourcen beeinträchtigen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC.L2-3.13.1	Überwachen, kontrollieren und schützen Sie die Unternehmenskommunikation (d. h. Informationen, die von Informationssystemen der Organisation übertragen oder empfangen werden) an externen und wichtigen internen Grenzen der Informationssysteme.	lambda-inside-vpc	Stellen Sie AWS Lambda-Funktionen in einer Amazon Virtual Private Cloud (Amazon VPC) bereit, um eine sichere Kommunikation zwischen einer Funktion und anderen Diensten innerhalb der Amazon VPC zu gewährleisten. Bei dieser Konfiguration sind kein Internet-Gateway, kein NAT-Gerät und keine VPN-Verbindung erforderlich. Der gesamte Datenverkehr bleibt sicher in der Cloud. AWS Domains, die sich innerhalb einer VPC befinden, verfügen aufgrund ihrer logischen Isolierung im Vergleich zu Domains mit öffentlichen Endpunkten über eine zusätzliche Sicherheitsebene. Um den Zugriff ordnungsgemäß zu verwalten,

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			sollten AWS Lambda-Funktionen einer VPC zugewiesen werden.
SC.L2-3.13.1	Überwachen, kontrollieren und schützen Sie die Unternehmenskommunikation (d. h. Informationen, die von Informationssystemen der Organisation übertragen oder empfangen werden) an externen und wichtigen internen Grenzen der Informationssysteme.	no-unrestricted-route-to-igw	Stellen Sie sicher, dass EC2 Amazon-Routentabellen keine uneingeschränkten Routen zu einem Internet-Gateway enthalten. Durch das Entfernen oder Beschränken des Internetzugangs für Workloads innerhalb von Amazon VPCs können unbeabsichtigte Zugriffe in Ihrer Umgebung reduziert werden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC.L2-3.13.1	Überwachen, kontrollieren und schützen Sie die Unternehmenskommunikation (d. h. Informationen, die von Informationssystemen der Organisation übertragen oder empfangen werden) an externen und wichtigen internen Grenzen der Informationssysteme.	rds-instance-public-access-überprüfen	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Relational Database Service (Amazon RDS) -Instances nicht öffentlich sind. Amazon-RDS-Datenbank-Instances können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC.L2-3.13.1	Überwachen, kontrollieren und schützen Sie die Unternehmenskommunikation (d. h. Informationen, die von Informationssystemen der Organisation übertragen oder empfangen werden) an externen und wichtigen internen Grenzen der Informationssysteme.	rds-snapshots-public-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Relational Database Service (Amazon RDS) -Instances nicht öffentlich sind. Amazon-RDS-Datenbank-Instances können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC.L2-3.13.1	Überwachen, kontrollieren und schützen Sie die Unternehmenskommunikation (d. h. Informationen, die von Informationssystemen der Organisation übertragen oder empfangen werden) an externen und wichtigen internen Grenzen der Informationssysteme.	redshift-cluster-public-access-überprüfen	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Redshift Redshift-Cluster nicht öffentlich sind. Amazon-Redshift-Cluster können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.
SC.L2-3.13.1	Überwachen, kontrollieren und schützen Sie die Unternehmenskommunikation (d. h. Informationen, die von Informationssystemen der Organisation übertragen oder empfangen werden) an externen und wichtigen internen Grenzen der Informationssysteme.	redshift-require-tls-ssl	Stellen Sie sicher, dass Ihre Amazon-Redshift-Cluster eine TLS/SSL-Verschlüsselung erfordern, um eine Verbindung zu SQL-Clients herzustellen. Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC.L2-3.13.1	Überwachen, kontrollieren und schützen Sie die Unternehmenskommunikation (d. h. Informationen, die von Informationssystemen der Organisation übertragen oder empfangen werden) an externen und wichtigen internen Grenzen der Informationssysteme.	restricted-common-ports	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass gemeinsame Ports für Amazon Elastic Compute Cloud (Amazon EC2) -Sicherheitsgruppen eingeschränkt sind. Wenn der Zugriff auf Ports nicht auf vertrauenswürdige Quellen beschränkt wird, kann dies zu Angriffen auf die Verfügbarkeit, Integrität und Vertraulichkeit von Systemen führen. Mit dieser Regel können Sie optional die Parameter blockedPort1–blockedPort5 festlegen (Standardkonfigurationen: 20, 21, 3389, 3306, 4333). Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC.L2-3.13.1	Überwachen, kontrollieren und schützen Sie die Unternehmenskommunikation (d. h. Informationen, die von Informationssystemen der Organisation übertragen oder empfangen werden) an externen und wichtigen internen Grenzen der Informationssysteme.	s3- -blöcke-periodisch account-level-public-access	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Simple Storage Service (Amazon S3) -Buckets nicht öffentlich zugänglich sind. Diese Regel trägt dazu bei, sensible Daten vor unbefugten Remote-Benutzern zu schützen, indem sie den öffentlichen Zugriff verhindert. Mit dieser Regel können Sie optional die Parameter ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) und restrictPublicBuckets Parameter (Config Default: True) festlegen. Die tatsächlichen Werte müssen den Richtlini

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			en Ihrer Organisation entsprechen.
SC.L2-3.13.1	Überwachen, kontrollieren und schützen Sie die Unternehmenskommunikation (d. h. Informationen, die von Informationssystemen der Organisation übertragen oder empfangen werden) an externen und wichtigen internen Grenzen der Informationssysteme.	s-3 bucket-public-read-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie nur autorisierten Benutzern, Prozessen und Geräten Zugriff auf Amazon Simple Storage Service (Amazon S3) - Buckets gewähren. Die Verwaltung des Zugriffs sollte mit der Klassifizierung der Daten übereinstimmen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC.L2-3.13.1	Überwachen, kontrollieren und schützen Sie die Unternehmenskommunikation (d. h. Informationen, die von Informationssystemen der Organisation übertragen oder empfangen werden) an externen und wichtigen internen Grenzen der Informationssysteme.	s-3 bucket-public-write-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie nur autorisierten Benutzern, Prozessen und Geräten Zugriff auf Amazon Simple Storage Service (Amazon S3) - Buckets gewähren. Die Verwaltung des Zugriffs sollte mit der Klassifizierung der Daten übereinstimmen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC.L2-3.13.1	Überwachen, kontrollieren und schützen Sie die Unternehmenskommunikation (d. h. Informationen, die von Informationssystemen der Organisation übertragen oder empfangen werden) an externen und wichtigen internen Grenzen der Informationssysteme.	s-3 bucket-ssl-requests-only	Um Daten während der Übertragung zu schützen, stellen Sie sicher, dass Ihre Amazon Simple Storage Service (Amazon S3)-Buckets Anfragen zur Verwendung von Secure Socket Layer (SSL)-Buckets erfordern. Da sensible Daten vorhanden sein können, sollten Sie die Verschlüsselung bei der Übertragung aktivieren, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC.L2-3.13.1	Überwachen, kontrollieren und schützen Sie die Unternehmenskommunikation (d. h. Informationen, die von Informationssystemen der Organisation übertragen oder empfangen werden) an externen und wichtigen internen Grenzen der Informationssysteme.	sagemaker-notebook-no-direct-Internetzugang	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass SageMaker Amazon-Notebooks keinen direkten Internetzugang zulassen. Indem Sie direkten Internetzugang blockieren, vermeiden Sie, dass unbefugte Benutzer auf sensible Daten zugreifen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC.L2-3.13.1	Überwachen, kontrollieren und schützen Sie die Unternehmenskommunikation (d. h. Informationen, die von Informationssystemen der Organisation übertragen oder empfangen werden) an externen und wichtigen internen Grenzen der Informationssysteme.	securityhub-enabled	AWS Security Hub hilft bei der Überwachung von unbefugtem Personal, Verbindungen, Geräten und Software. AWS Security Hub aggregiert, organisiert und priorisiert die Sicherheitswarnungen oder Ergebnisse mehrerer Dienste. AWS Einige dieser Dienste sind Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer und AWS Firewall Manager sowie AWS Partnerlösungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC.L2-3.13.1	Überwachen, kontrollieren und schützen Sie die Unternehmenskommunikation (d. h. Informationen, die von Informationssystemen der Organisation übertragen oder empfangen werden) an externen und wichtigen internen Grenzen der Informationssysteme.	ssm-document-not-public	Stellen Sie sicher, dass AWS Systems Manager (SSM) - Dokumente nicht öffentlich sind, da dies einen unbeabsichtigten Zugriff auf Ihre SSM-Dokumente ermöglichen kann. Ein öffentliches SSM-Dokument kann Informationen über Ihr Konto, Ihre Ressourcen und internen Prozesse preisgeben.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC.L2-3.13.1	Überwachen, kontrollieren und schützen Sie die Unternehmenskommunikation (d. h. Informationen, die von Informationssystemen der Organisation übertragen oder empfangen werden) an externen und wichtigen internen Grenzen der Informationssysteme.	vpc-default-security-group-geschlossen	Sicherheitsgruppen von Amazon Elastic Compute Cloud (Amazon EC2) können bei der Verwaltung des Netzwerkzugriffs helfen, indem sie eine statusbehaftete Filterung des ein- und ausgehenden Netzwerkverkehrs zu Ressourcen bereitstellen. AWS Die Beschränkung des gesamten Datenverkehrs auf die Standardsicherheitsgruppe hilft dabei, den Fernzugriff auf Ihre Ressourcen einzuschränken. AWS

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC.L2-3.13.1	Überwachen, kontrollieren und schützen Sie die Unternehmenskommunikation (d. h. Informationen, die von Informationssystemen der Organisation übertragen oder empfangen werden) an externen und wichtigen internen Grenzen der Informationssysteme.	vpc-sg-open-only-to-authorized-ports	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass gemeinsame Ports für Amazon Elastic Compute Cloud (Amazon EC2) -Sicherheitsgruppen eingeschränkt sind. Wenn der Zugriff auf Ports nicht auf vertrauenswürdige Quellen beschränkt wird, kann dies zu Angriffen auf die Verfügbarkeit, Integrität und Vertraulichkeit von Systemen führen. Durch die Beschränkung des Zugriffs auf Ressourcen innerhalb einer Sicherheitsgruppe aus dem Internet (0.0.0.0/0) kann der Remote-Zugriff auf interne Systeme gesteuert werden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC.L2-3.13.1	Überwachen, kontrollieren und schützen Sie die Unternehmenskommunikation (d. h. Informationen, die von Informationssystemen der Organisation übertragen oder empfangen werden) an externen und wichtigen internen Grenzen der Informationssysteme.	opensearch-in-vpc-only	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass sich Amazon OpenSearch Service-Domains innerhalb einer Amazon Virtual Private Cloud (Amazon VPC) befinden. Eine Amazon OpenSearch Service-Domain innerhalb einer Amazon VPC ermöglicht die sichere Kommunikation zwischen Amazon OpenSearch Service und anderen Services innerhalb der Amazon VPC, ohne dass ein Internet-Gateway, ein NAT-Gerät oder eine VPN-Verbindung erforderlich ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC.L2-3.13.1	Überwachen, kontrollieren und schützen Sie die Unternehmenskommunikation (d. h. Informationen, die von Informationssystemen der Organisation übertragen oder empfangen werden) an externen und wichtigen internen Grenzen der Informationssysteme.	opensearch-node-to-node-Verschlüsselungsprüfung	Stellen Sie sicher, dass die node-to-node Verschlüsselung für Amazon OpenSearch Service aktiviert ist. Node-to-nodeVerschlüsselung ermöglicht die TLS 1.2-Verschlüsselung für die gesamte Kommunikation innerhalb der Amazon Virtual Private Cloud (Amazon VPC). Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC.L2-3.13.2	Verwenden Sie Architekturdesigns, Softwareentwicklungstechniken und Prinzipien der Systemtechnik, die eine effektive Informationssicherheit innerhalb von Organisationssystemen fördern.	account-part-of-organizations	Durch die zentrale Verwaltung AWS-Konten innerhalb von AWS Organizations wird sichergestellt, dass die Konten den Vorschriften entsprechen. Eine fehlende zentrale Kontoverwaltung kann zu inkonsistenten Kontokonfigurationen führen, wodurch Ressourcen und sensible Daten offengelegt werden können.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC.L2-3.13.2	Verwenden Sie Architekturdesigns, Softwareentwicklungstechniken und Prinzipien der Systemtechnik, die eine effektive Informationssicherheit innerhalb von Organisationssystemen fördern.	alb-waf-enabled	Stellen Sie sicher, dass AWS WAF auf Elastic Load Balancers (ELB) aktiviert ist, um Webanwendungen zu schützen. Eine WAF trägt zum Schutz Ihrer Webanwendungen oder APIs vor gängigen Web-Exploits bei. Diese Web-Exploits können sich auf die Verfügbarkeit auswirken, die Sicherheit gefährden oder übermäßige Ressourcen in Ihrer Umgebung verbrauchen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC.L2-3.13.2	Verwenden Sie Architekturdesigns, Softwareentwicklungstechniken und Prinzipien der Systemtechnik, die eine effektive Informationssicherheit innerhalb von Organisationssystemen fördern.	api-gw-associated-with-WAF	AWS Mit WAF können Sie eine Reihe von Regeln (als Web Access Control List (Web ACL) bezeichnet) konfigurieren, die Webanfragen auf der Grundlage von anpassbaren Websicherheitsregeln und -bedingungen, die Sie definieren, zulassen, blockieren oder zählen. Stellen Sie sicher, dass Ihre Amazon-API-Gateway-Stufe mit einer WAF-Web-ACL verknüpft ist, um sie vor böswilligen Angriffen zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC.L2-3.13.2	Verwenden Sie Architekturdesigns, Softwareentwicklungstechniken und Prinzipien der Systemtechnik, die eine effektive Informationssicherheit innerhalb von Organisationssystemen fördern.	autoscaling-launch-config-public-ip-deaktiviert	Wenn Sie Ihre Netzwerkschnittstellen mit einer öffentlichen IP-Adresse konfigurieren, sind die diesen Netzwerkschnittstellen zugehörigen Ressourcen über das Internet erreichbar. EC2 Ressourcen sollten nicht öffentlich zugänglich sein, da dies einen unbeabsichtigten Zugriff auf Ihre Anwendungen oder Server ermöglichen kann.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC.L2-3.13.2	Verwenden Sie Architekturdesigns, Softwareentwicklungstechniken und Prinzipien der Systemtechnik, die eine effektive Informationssicherheit innerhalb von Organisationssystemen fördern.	backup-plan-min-frequency-and-min-retention-check	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihr AWS Backup-Plan auf eine Mindestfrequenz und Aufbewahrung festgelegt ist. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen. Mit dieser Regel können Sie die Parameter requiredFrequencyValue (Config default: 1), requiredRetentionDays (Config default: 35) und requiredFrequencyUnit

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			(Config default: days) festlegen. Der tatsächliche Wert muss den Anforderungen Ihrer Organisation entsprechen.
SC.L2-3.13.2	Verwenden Sie Architekturdesigns, Softwareentwicklungstechniken und Prinzipien der Systemtechnik, die eine effektive Informationssicherheit innerhalb von Organisationssystemen fördern.	cloudtrail-security-trail-enabled	Diese Regel trägt dazu bei, die Verwendung der AWS empfohlenen bewährten Sicherheitsmethoden für sicherzustellen AWS CloudTrail, indem geprüft wird, ob mehrere Einstellungen aktiviert sind. Dazu gehören die Verwendung von Protokollverschlüsselung, Protokollvalidierung und Aktivierung AWS CloudTrail in mehreren Regionen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC.L2-3.13.2	Verwenden Sie Architekturdesigns, Softwareentwicklungstechniken und Prinzipien der Systemtechnik, die eine effektive Informationssicherheit innerhalb von Organisationssystemen fördern.	codebuild-project-envvar-awscred-überprüfen	Stellen Sie sicher, dass die Anmeldeinformationen AWS_ACCESS_KEY_ID AWS_SECRET_ACCESS_KEY nicht in AWS Codebuild-Projektumgebungen vorhanden sind. Speichern Sie diese Variablen nicht als Klartext. Das Speichern dieser Variablen als Klartext bewirkt eine unbeabsichtigte Offenlegung von Daten sowie unberechtigte Zugriffe.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC.L2-3.13.2	Verwenden Sie Architekturdesigns, Softwareentwicklungstechniken und Prinzipien der Systemtechnik, die eine effektive Informationssicherheit innerhalb von Organisationssystemen fördern.	codebuild-project-source-repo-URL-Prüfung	Stellen Sie sicher, dass die URL des Quell-Repositorys GitHub oder des Bitbucket-Quell-Repositorys keine persönlichen Zugriffstoken oder Anmeldeinformationen in Codebuild-Projektumgebungen enthält. AWS Verwende OAuth anstelle von persönlichen Zugriffstoken oder Anmeldedaten die Autorisierung für den Zugriff auf GitHub Bitbucket-Repositorys.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC.L2-3.13.2	Verwenden Sie Architekturdesigns, Softwareentwicklungstechniken und Prinzipien der Systemtechnik, die eine effektive Informationssicherheit innerhalb von Organisationssystemen fördern.	db-instance-backup-enabled	Die Sicherungsfunktion von Amazon RDS erstellt Sicherungen Ihrer Datenbanken und Transaktionsprotokolle. Amazon RDS erstellt einen Snapshot für das Speichervolume Ihrer DB-Instance, sodass die gesamte DB-Instance gesichert wird. Sie können im System spezifische Aufbewahrungsfristen festlegen, um Ihre Ausfallsicherheitsanforderungen zu erfüllen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC.L2-3.13.2	Verwenden Sie Architekturdesigns, Softwareentwicklungstechniken und Prinzipien der Systemtechnik, die eine effektive Informationssicherheit innerhalb von Organisationssystemen fördern.	dms-replication-not-public	Verwalte den Zugriff auf die AWS Cloud, indem du sicherstellst, dass auf DMS-Replikationsinstanzen nicht öffentlich zugegriffen werden kann. DMS-Replikations-Instances können vertrauliche Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC.L2-3.13.2	Verwenden Sie Architekturdesigns, Softwareentwicklungstechniken und Prinzipien der Systemtechnik, die eine effektive Informationssicherheit innerhalb von Organisationssystemen fördern.	dynamodb-autoscaling-enabled	Amazon DynamoDB Auto Scaling verwendet den AWS Application Auto Scaling-Service, um die bereitgestellte Durchsatzkapazität so anzupassen, dass sie automatisch auf tatsächliche Verkehrsmuster reagiert. Auf diese Weise kann eine Tabelle oder ein globaler sekundärer Index die bereitgestellte Lese-/Schreibkapazität erhöhen, um plötzliche Erhöhungen des Datenverkehrs ohne Drosselung zu bewältigen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC.L2-3.13.2	Verwenden Sie Architekturdesigns, Softwareentwicklungstechniken und Prinzipien der Systemtechnik, die eine effektive Informationssicherheit innerhalb von Organisationssystemen fördern.	dynamodb-in-backup-plan	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon DynamoDB-Tabellen Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC.L2-3.13.2	Verwenden Sie Architekturdesigns, Softwareentwicklungstechniken und Prinzipien der Systemtechnik, die eine effektive Informationssicherheit innerhalb von Organisationssystemen fördern.	dynamodb-pitr-enabled	Aktivieren Sie diese Regel, um zu überprüfen, ob die Informationen gesichert wurden. Es verwaltet auch die Backups, indem es sicherstellt, dass die point-in-time Wiederherstellung in Amazon DynamoDB aktiviert ist. Bei der Wiederherstellung werden fortlaufende Backups Ihrer Tabelle für die letzten 35 Tage gespeichert.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC.L2-3.13.2	Verwenden Sie Architekturdesigns, Softwareentwicklungstechniken und Prinzipien der Systemtechnik, die eine effektive Informationssicherheit innerhalb von Organisationssystemen fördern.	ebs-in-backup-plan	Stellen Sie zur Unterstützung der Datensicherungsprozesse sicher, dass Ihre Amazon Elastic Block Store (Amazon EBS) -Volumes Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC.L2-3.13.2	Verwenden Sie Architekturdesigns, Softwareentwicklungstechniken und Prinzipien der Systemtechnik, die eine effektive Informationssicherheit innerhalb von Organisationssystemen fördern.	ebs-optimized-instance	Eine optimierte Instance im Amazon Elastic Block Store (Amazon EBS) bietet zusätzliche, dedizierte Kapazität für Amazon-EBS-I/O-Vorgänge. Diese Optimierung bietet die beste Leistung für Ihr EBS-Volume, indem Konflikte zwischen Amazon-EBS-I/O und anderem Datenverkehr von Ihrer Instance minimiert werden.
SC.L2-3.13.2	Verwenden Sie Architekturdesigns, Softwareentwicklungstechniken und Prinzipien der Systemtechnik, die eine effektive Informationssicherheit innerhalb von Organisationssystemen fördern.	ebs-snapshot-public-restorable-überprüfen	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass EBS-Snapshots nicht öffentlich wiederherstellbar sind. EBS-Volume-Snapshots können vertrauliche Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC.L2-3.13.2	Verwenden Sie Architekturdesigns, Softwareentwicklungstechniken und Prinzipien der Systemtechnik, die eine effektive Informationssicherheit innerhalb von Organisationssystemen fördern.	ec-2 instance-no-public-ip	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon Elastic Compute Cloud (Amazon EC2) - Instances nicht öffentlich zugänglich sind. EC2 Amazon-Instances können vertrauliche Informationen enthalten, und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC.L2-3.13.2	Verwenden Sie Architekturdesigns, Softwareentwicklungstechniken und Prinzipien der Systemtechnik, die eine effektive Informationssicherheit innerhalb von Organisationssystemen fördern.	efs-in-backup-plan	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon Elastic File System (Amazon EFS) -Dateisysteme Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC.L2-3.13.2	Verwenden Sie Architekturdesigns, Softwareentwicklungstechniken und Prinzipien der Systemtechnik, die eine effektive Informationssicherheit innerhalb von Organisationssystemen fördern.	elasticache-redis-cluster-automatic-Backup-Check	Wenn automatische Backups aktiviert sind, ElastiCache erstellt Amazon täglich ein Backup des Clusters. Die Sicherung kann für eine von Ihrer Organisation festgelegte Anzahl von Tagen aufbewahrt werden. Automatische Backups schützen vor Datenverlust. Bei einem Ausfall können Sie einen neuen Cluster erstellen, der Ihre Daten aus dem aktuellen Backup wiederherstellt.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC.L2-3.13.2	Verwenden Sie Architekturdesigns, Softwareentwicklungstechniken und Prinzipien der Systemtechnik, die eine effektive Informationssicherheit innerhalb von Organisationssystemen fördern.	elasticsearch-in-vpc-only	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass sich Amazon OpenSearch OpenSearch Service (Service) - Domains innerhalb einer Amazon Virtual Private Cloud (Amazon VPC) befinden. Eine OpenSearch Service-Domain innerhalb einer Amazon VPC ermöglicht die sichere Kommunikation zwischen OpenSearch Service und anderen Services innerhalb der Amazon VPC, ohne dass ein Internet-Gateway, ein NAT-Gerät oder eine VPN-Verbindung erforderlich ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC.L2-3.13.2	Verwenden Sie Architekturdesigns, Softwareentwicklungstechniken und Prinzipien der Systemtechnik, die eine effektive Informationssicherheit innerhalb von Organisationssystemen fördern.	elb-cross-zone-load-Balancing aktiviert	Aktivieren Sie zonenübergreifendes Load Balancing für Ihre Elastic Load Balancer (ELBs), um eine angemessene Kapazität und Verfügbarkeit aufrechtzuerhalten. Zonenübergreifendes Load Balancing reduziert die Notwendigkeit, die gleiche Anzahl von Instances in jeder aktivierten Availability Zone aufrechtzuerhalten. Es verbessert auch die Fähigkeit Ihrer Anwendung, den Verlust einer oder mehrerer Instances zu bewältigen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC.L2-3.13.2	Verwenden Sie Architekturdesigns, Softwareentwicklungstechniken und Prinzipien der Systemtechnik, die eine effektive Informationssicherheit innerhalb von Organisationssystemen fördern.	elb-deletion-protection-enabled	Diese Regel sorgt dafür, dass der Löschschutz für Elastic Load Balancing aktiviert ist. Verwenden Sie diese Funktion, um zu verhindern, dass Ihr Load Balancer versehentlich oder böswillig gelöscht wird, was zum Verlust der Verfügbarkeit Ihrer Anwendungen führen kann.
SC.L2-3.13.2	Verwenden Sie Architekturdesigns, Softwareentwicklungstechniken und Prinzipien der Systemtechnik, die eine effektive Informationssicherheit innerhalb von Organisationssystemen fördern.	emr-master-no-public-ip	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon EMR-Cluster-Masterknoten nicht öffentlich zugänglich sind. Amazon-EMR-Cluster-Hauptknoten können vertrauliche Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC.L2-3.13.2	Verwenden Sie Architekturdesigns, Softwareentwicklungstechniken und Prinzipien der Systemtechnik, die eine effektive Informationssicherheit innerhalb von Organisationssystemen fördern.	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) Security Groups können bei der Verwaltung des Netzwerkzugriffs helfen, indem sie eine statusbehaftete Filterung von eingehendem und ausgehendem Netzwerkverkehr zu Ressourcen bereitstellen. AWS Wenn Sie eingehenden (oder entfernten) Datenverkehr von 0.0.0.0/0 bis Port 22 auf Ihren Ressourcen nicht zulassen, können Sie den Remote-Zugriff einschränken.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC.L2-3.13.2	Verwenden Sie Architekturdesigns, Softwareentwicklungstechniken und Prinzipien der Systemtechnik, die eine effektive Informationssicherheit innerhalb von Organisationssystemen fördern.	ec-2 instances-in-vpc	Stellen Sie Amazon Elastic Compute Cloud (Amazon EC2) -Instances innerhalb einer Amazon Virtual Private Cloud (Amazon VPC) bereit, um eine sichere Kommunikation zwischen einer Instance und anderen Services innerhalb der Amazon VPC zu ermöglichen, ohne dass ein Internet-Gateway, ein NAT-Gerät oder eine VPN-Verbindung erforderlich ist. Der gesamte Datenverkehr bleibt sicher in der AWS Cloud. Domains, die sich innerhalb einer VPC befinden, verfügen aufgrund ihrer logischen Isolierung im Vergleich zu Domains mit öffentlichen Endpunkten über eine zusätzliche Sicherheitsebene. Weisen Sie EC2

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			Amazon-Instances einer Amazon-VPC zu, um den Zugriff ordnungsgemäß zu verwalten.
SC.L2-3.13.2	Verwenden Sie Architekturdesigns, Softwareentwicklungstechniken und Prinzipien der Systemtechnik, die eine effektive Informationssicherheit innerhalb von Organisationssystemen fördern.	internet-gateway-authorized-vpc-nur	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Internet-Gateways nur mit autorisierter Amazon Virtual Private Cloud (Amazon VPC) verbunden sind. Internet-Gateways ermöglichen den bidirektionalen Internetzugang zur und von der Amazon VPC, was möglicherweise zu einem unbefugten Zugriff auf Amazon-VPC-Ressourcen führen kann.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC.L2-3.13.2	Verwenden Sie Architekturdesigns, Softwareentwicklungstechniken und Prinzipien der Systemtechnik, die eine effektive Informationssicherheit innerhalb von Organisationssystemen fördern.	lambda-function-public-access-verboten	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass AWS Lambda-Funktionen nicht öffentlich zugänglich sind. Der öffentliche Zugriff kann möglicherweise die Verfügbarkeit von Ressourcen beeinträchtigen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC.L2-3.13.2	Verwenden Sie Architekturdesigns, Softwareentwicklungstechniken und Prinzipien der Systemtechnik, die eine effektive Informationssicherheit innerhalb von Organisationssystemen fördern.	lambda-inside-vpc	Stellen Sie AWS Lambda-Funktionen in einer Amazon Virtual Private Cloud (Amazon VPC) bereit, um eine sichere Kommunikation zwischen einer Funktion und anderen Diensten innerhalb der Amazon VPC zu gewährleisten. Bei dieser Konfiguration sind kein Internet-Gateway, kein NAT-Gerät und keine VPN-Verbindung erforderlich. Der gesamte Datenverkehr bleibt sicher in der Cloud. AWS Domains, die sich innerhalb einer VPC befinden, verfügen aufgrund ihrer logischen Isolierung im Vergleich zu Domains mit öffentlichen Endpunkten über eine zusätzliche Sicherheitsebene. Um den Zugriff ordnungsgemäß zu verwalten,

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			sollten AWS Lambda-Funktionen einer VPC zugewiesen werden.
SC.L2-3.13.2	Verwenden Sie Architekturdesigns, Softwareentwicklungstechniken und Prinzipien der Systemtechnik, die eine effektive Informationssicherheit innerhalb von Organisationssystemen fördern.	no-unrestricted-route-to-igw	Stellen Sie sicher, dass EC2 Amazon-Routentabellen keine uneingeschränkten Routen zu einem Internet-Gateway enthalten. Durch das Entfernen oder Beschränken des Internetzugangs für Workloads innerhalb von Amazon VPCs können unbeabsichtigte Zugriffe in Ihrer Umgebung reduziert werden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC.L2-3.13.2	Verwenden Sie Architekturdesigns, Softwareentwicklungstechniken und Prinzipien der Systemtechnik, die eine effektive Informationssicherheit innerhalb von Organisationssystemen fördern.	rds-instance-deletion-protection-aktiviert	Stellen Sie sicher, dass Amazon Relational Database Service (Amazon RDS)-Instances den Löschschutz aktiviert haben. Verwenden Sie den Löschschutz, um zu verhindern, dass Ihre Amazon-RDS-Instances versehentlich oder böswillig gelöscht werden, was zum Verlust der Verfügbarkeit Ihrer Anwendungen führen kann.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC.L2-3.13.2	Verwenden Sie Architekturdesigns, Softwareentwicklungstechniken und Prinzipien der Systemtechnik, die eine effektive Informationssicherheit innerhalb von Organisationssystemen fördern.	rds-instance-public-access-überprüfen	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Relational Database Service (Amazon RDS) -Instances nicht öffentlich sind. Amazon-RDS-Datenbank-Instances können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC.L2-3.13.2	Verwenden Sie Architekturdesigns, Softwareentwicklungstechniken und Prinzipien der Systemtechnik, die eine effektive Informationssicherheit innerhalb von Organisationssystemen fördern.	rds-in-backup-plan	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon Relational Database Service (Amazon RDS) -Instances Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC.L2-3.13.2	Verwenden Sie Architekturdesigns, Softwareentwicklungstechniken und Prinzipien der Systemtechnik, die eine effektive Informationssicherheit innerhalb von Organisationssystemen fördern.	rds-multi-az-support	Die Multi-AZ-Unterstützung in Amazon Relational Database Service (Amazon RDS) bietet eine verbesserte Verfügbarkeit und Beständigkeit von Datenbank-Instances. Wenn Sie eine Multi-AZ-Datenbank-Instance bereitstellen, erstellt Amazon RDS automatisch eine primäre Datenbank-Instance und repliziert die Daten synchron auf eine Standby-Instance in einer anderen Availability Zone. Jede Availability Zone läuft auf einer eigenen, physisch getrennten, unabhängigen Infrastruktur und ist auf eine hohe Verfügbarkeit ausgelegt. Im Falle eines Infrastrukturausfalls führt Amazon RDS einen automatis

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			chen Failover zum Standby-Modus durch, sodass Sie den Datenbankbetrieb wieder aufnehmen können, sobald der Failover abgeschlo ssen ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC.L2-3.13.2	Verwenden Sie Architekturdesigns, Softwareentwicklungstechniken und Prinzipien der Systemtechnik, die eine effektive Informationssicherheit innerhalb von Organisationssystemen fördern.	rds-cluster-multi-az-aktiviert	Die Multi-AZ-Unterstützung in Amazon Relational Database Service (Amazon RDS) bietet eine verbesserte Verfügbarkeit und Beständigkeit von Datenbank-Instances. Wenn Sie eine Multi-AZ-Datenbank-Instance bereitstellen, erstellt Amazon RDS automatisch eine primäre Datenbank-Instance und repliziert die Daten synchron auf eine Standby-Instance in einer anderen Availability Zone. Jede Availability Zone läuft auf einer eigenen, physisch getrennten, unabhängigen Infrastruktur und ist auf eine hohe Verfügbarkeit ausgelegt. Im Falle eines Infrastrukturausfalls führt Amazon RDS einen automatis

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			chen Failover zum Standby-Modus durch, sodass Sie den Datenbankbetrieb wieder aufnehmen können, sobald der Failover abgeschlo ssen ist.
SC.L2-3.13.2	Verwenden Sie Architekturdesigns, Softwareentwicklun gstechniken und Prinzipien der Systemtechnik, die eine effektive Informationssicher heit innerhalb von Organisationssyste men fördern.	rds-snapshots-public-prohibited	Verwalten Sie den Zugriff auf Ressource n in der AWS Cloud, indem Sie sicherste llen, dass Amazon Relational Database Service (Amazon RDS) -Instance s nicht öffentlic h sind. Amazon-RDS-Datenbank-Instances können vertrauliche Informati onen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC.L2-3.13.2	Verwenden Sie Architekturdesigns, Softwareentwicklungstechniken und Prinzipien der Systemtechnik, die eine effektive Informationssicherheit innerhalb von Organisationssystemen fördern.	redshift-backup-enabled	Stellen Sie zur Unterstützung der Datensicherungsprozesse sicher, dass Ihre Amazon-Redshift-Cluster über automatisierte Snapshots verfügen. Wenn automatisierte Snapshots für einen Cluster aktiviert sind, erstellt Redshift in regelmäßigen Abständen Snapshots dieses Clusters. Standardmäßig erstellt Redshift alle acht Stunden oder alle 5 GB einen Snapshot für jeden Knoten mit Datenänderungen oder je nachdem, was zuerst eintritt.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC.L2-3.13.2	Verwenden Sie Architekturdesigns, Softwareentwicklungstechniken und Prinzipien der Systemtechnik, die eine effektive Informationssicherheit innerhalb von Organisationssystemen fördern.	redshift-cluster-public-access-überprüfen	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Redshift Redshift-Cluster nicht öffentlich sind. Amazon-Redshift-Cluster können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC.L2-3.13.2	Verwenden Sie Architekturdesigns, Softwareentwicklungstechniken und Prinzipien der Systemtechnik, die eine effektive Informationssicherheit innerhalb von Organisationssystemen fördern.	restricted-common-ports	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass gemeinsame Ports für Amazon Elastic Compute Cloud (Amazon EC2) -Sicherheitsgruppen eingeschränkt sind. Wenn der Zugriff auf Ports nicht auf vertrauenswürdige Quellen beschränkt wird, kann dies zu Angriffen auf die Verfügbarkeit, Integrität und Vertraulichkeit von Systemen führen. Mit dieser Regel können Sie optional die Parameter blockedPort1–blockedPort5 festlegen (Standardkonfigurationen: 20, 21, 3389, 3306, 4333). Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC.L2-3.13.2	Verwenden Sie Architekturdesigns, Softwareentwicklungstechniken und Prinzipien der Systemtechnik, die eine effektive Informationssicherheit innerhalb von Organisationssystemen fördern.	s3- account-level-public-access -blöcke-periodisch	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Simple Storage Service (Amazon S3) -Buckets nicht öffentlich zugänglich sind. Diese Regel trägt dazu bei, sensible Daten vor unbefugten Remote-Benutzern zu schützen, indem sie den öffentlichen Zugriff verhindert. Mit dieser Regel können Sie optional die Parameter ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) und restrictPublicBuckets Parameter (Config Default: True) festlegen. Die tatsächlichen Werte müssen den Richtlini

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			en Ihrer Organisation entsprechen.
SC.L2-3.13.2	Verwenden Sie Architekturdesigns, Softwareentwicklungstechniken und Prinzipien der Systemtechnik, die eine effektive Informationssicherheit innerhalb von Organisationssystemen fördern.	s3- bucket-default-lock-enabled	Stellen Sie sicher, dass für Ihren Amazon Simple Storage Service (Amazon S3)-Bucket standardmäßig eine Sperre aktiviert ist. Zum Schutz eventuell vorhandener sensibler Daten in S3-Buckets müssen Sie Objektsperren für Daten im Ruhezustand erzwingen.
SC.L2-3.13.2	Verwenden Sie Architekturdesigns, Softwareentwicklungstechniken und Prinzipien der Systemtechnik, die eine effektive Informationssicherheit innerhalb von Organisationssystemen fördern.	s-3 bucket-public-read-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie nur autorisierten Benutzern, Prozessen und Geräten Zugriff auf Amazon Simple Storage Service (Amazon S3) - Buckets gewähren. Die Verwaltung des Zugriffs sollte mit der Klassifizierung der Daten übereinstimmen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC.L2-3.13.2	Verwenden Sie Architekturdesigns, Softwareentwicklungstechniken und Prinzipien der Systemtechnik, die eine effektive Informationssicherheit innerhalb von Organisationssystemen fördern.	s3- bucket-public-write-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie nur autorisierten Benutzern, Prozessen und Geräten Zugriff auf Amazon Simple Storage Service (Amazon S3) - Buckets gewähren. Die Verwaltung des Zugriffs sollte mit der Klassifizierung der Daten übereinstimmen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC.L2-3.13.2	Verwenden Sie Architekturdesigns, Softwareentwicklungstechniken und Prinzipien der Systemtechnik, die eine effektive Informationssicherheit innerhalb von Organisationssystemen fördern.	s3- bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) unterstützt die Aufrechterhaltung einer angemessenen Kapazität und Verfügbarkeit. CRR ermöglicht das automatische, asynchrone Kopieren von Objekten in Amazon-S3-Buckets, um die Datenverfügbarkeit sicherzustellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC.L2-3.13.2	Verwenden Sie Architekturdesigns, Softwareentwicklungstechniken und Prinzipien der Systemtechnik, die eine effektive Informationssicherheit innerhalb von Organisationssystemen fördern.	s-3 bucket-versioning-enabled	Die Versionsverwaltung von Amazon Simple Storage Service (Amazon S3)-Buckets hilft dabei, mehrere Varianten eines Objekts im selben Amazon-S3-Bucket zu speichern. Verwenden Sie die Versionsverwaltung, um sämtliche Versionen aller Objekte in Ihrem Amazon-S3-Bucket zu speichern, abzurufen oder wiederherzustellen. Mit der Versionsverwaltung können Sie Versionen sowohl nach unbeabsichtigten Benutzeraktionen als auch nach Anwendungsfehlern problemlos wiederherstellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC.L2-3.13.2	Verwenden Sie Architekturdesigns, Softwareentwicklungstechniken und Prinzipien der Systemtechnik, die eine effektive Informationssicherheit innerhalb von Organisationssystemen fördern.	sagemaker-notebook-no-direct-Internet-Zugang	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass SageMaker Amazon-Notebooks keinen direkten Internetzugang zulassen. Indem Sie direkten Internetzugang blockieren, vermeiden Sie, dass unbefugte Benutzer auf sensible Daten zugreifen.
SC.L2-3.13.2	Verwenden Sie Architekturdesigns, Softwareentwicklungstechniken und Prinzipien der Systemtechnik, die eine effektive Informationssicherheit innerhalb von Organisationssystemen fördern.	ssm-document-not-public	Stellen Sie sicher, dass AWS Systems Manager (SSM) - Dokumente nicht öffentlich sind, da dies einen unbeabsichtigten Zugriff auf Ihre SSM-Dokumente ermöglichen kann. Ein öffentliches SSM-Dokument kann Informationen über Ihr Konto, Ihre Ressourcen und internen Prozesse preisgeben.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC.L2-3.13.2	Verwenden Sie Architekturdesigns, Softwareentwicklungstechniken und Prinzipien der Systemtechnik, die eine effektive Informationssicherheit innerhalb von Organisationssystemen fördern.	subnet-auto-assign-public-ip-deaktiviert	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon Virtual Private Cloud (VPC) -Subnetzen nicht automatisch eine öffentliche IP-Adresse zugewiesen wird. Amazon Elastic Compute Cloud (EC2) -Instances, die in Subnetzen gestartet werden, in denen dieses Attribut aktiviert ist, haben ihrer primären Netzwerkschnittstelle eine öffentliche IP-Adresse zugewiesen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC.L2-3.13.2	Verwenden Sie Architekturdesigns, Softwareentwicklungstechniken und Prinzipien der Systemtechnik, die eine effektive Informationssicherheit innerhalb von Organisationssystemen fördern.	vpc-default-security-group-geschlossen	Sicherheitsgruppen von Amazon Elastic Compute Cloud (Amazon EC2) können bei der Verwaltung des Netzwerkzugriffs helfen, indem sie eine statusbehaftete Filterung des ein- und ausgehenden Netzwerkverkehrs zu Ressourcen bereitstellen. AWS Die Beschränkung des gesamten Datenverkehrs auf die Standardsicherheitsgruppe hilft dabei, den Fernzugriff auf Ihre Ressourcen einzuschränken. AWS

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC.L2-3.13.2	Verwenden Sie Architekturdesigns, Softwareentwicklungstechniken und Prinzipien der Systemtechnik, die eine effektive Informationssicherheit innerhalb von Organisationssystemen fördern.	vpc-sg-open-only-to-authorized-ports	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass gemeinsame Ports für Amazon Elastic Compute Cloud (Amazon EC2) -Sicherheitsgruppen eingeschränkt sind. Wenn der Zugriff auf Ports nicht auf vertrauenswürdige Quellen beschränkt wird, kann dies zu Angriffen auf die Verfügbarkeit, Integrität und Vertraulichkeit von Systemen führen. Durch die Beschränkung des Zugriffs auf Ressourcen innerhalb einer Sicherheitsgruppe aus dem Internet (0.0.0.0/0) kann der Remote-Zugriff auf interne Systeme gesteuert werden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC.L2-3.13.2	Verwenden Sie Architekturdesigns, Softwareentwicklungstechniken und Prinzipien der Systemtechnik, die eine effektive Informationssicherheit innerhalb von Organisationssystemen fördern.	vpc-vpn-2-tunnels-up	Redundante Site-to-Site VPN-Tunnel können implementiert werden, um die Anforderungen an die Ausfallsicherheit zu erfüllen. Es verwendet zwei Tunnel, um die Konnektivität sicherzustellen, falls eine der Site-to-Site VPN-Verbindungen nicht verfügbar ist. Um sich vor einem Verbindungsverlust zu schützen, können Sie für den Fall, dass Ihr Kunden-Gateway nicht verfügbar ist, eine zweite Site-to-Site VPN-Verbindung zu Ihrer Amazon Virtual Private Cloud (Amazon VPC) und Ihrem Virtual Private Gateway einrichten, indem Sie ein zweites Kunden-Gateway verwenden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC.L2-3.13.2	Verwenden Sie Architekturdesigns, Softwareentwicklungstechniken und Prinzipien der Systemtechnik, die eine effektive Informationssicherheit innerhalb von Organisationssystemen fördern.	opensearch-in-vpc-only	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass sich Amazon OpenSearch Service-Domains innerhalb einer Amazon Virtual Private Cloud (Amazon VPC) befinden. Eine Amazon OpenSearch Service-Domain innerhalb einer Amazon VPC ermöglicht die sichere Kommunikation zwischen Amazon OpenSearch Service und anderen Services innerhalb der Amazon VPC, ohne dass ein Internet-Gateway, ein NAT-Gerät oder eine VPN-Verbindung erforderlich ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC.L2-3.13.4	Verhindern Sie die unbefugte und unbeabsichtigte Übertragung von Informationen aus gemeinsam genutzten Systemressourcen.	dms-replication-not-public	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass auf DMS-Replikationsinstanzen nicht öffentlich zugegriffen werden kann. DMS-Replikations-Instances können vertrauliche Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.
SC.L2-3.13.4	Verhindern Sie die unbefugte und unbeabsichtigte Übertragung von Informationen aus gemeinsam genutzten Systemressourcen.	ebs-snapshot-public-restorable-überprüfen	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass EBS-Snapshots nicht öffentlich wiederherstellbar sind. EBS-Volume-Snapshots können vertrauliche Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC.L2-3.13.4	Verhindern Sie die unbefugte und unbeabsichtigte Übertragung von Informationen aus gemeinsam genutzten Systemressourcen.	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) Security Groups können bei der Verwaltung des Netzwerkzugriffs helfen, indem sie eine statusbeh aftete Filterung von eingehendem und ausgehendem Netzwerkverkehr zu Ressourcen bereitste llen. AWS Wenn Sie eingehenden (oder entfernten) Datenverk ehr von 0.0.0.0/0 bis Port 22 auf Ihren Ressourcen nicht zulassen, können Sie den Remote-Zugriff einschränken.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC.L2-3.13.4	Verhindern Sie die unbefugte und unbeabsichtigte Übertragung von Informationen aus gemeinsam genutzten Systemressourcen.	internet-gateway-authorized-vpc-nur	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Internet-Gateways nur mit autorisierter Amazon Virtual Private Cloud (Amazon VPC) verbunden sind. Internet-Gateways ermöglichen den bidirektionalen Internetzugang zur und von der Amazon VPC, was möglicherweise zu einem unbefugten Zugriff auf Amazon-VPC-Ressourcen führen kann.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC.L2-3.13.4	Verhindern Sie die unbefugte und unbeabsichtigte Übertragung von Informationen aus gemeinsam genutzten Systemressourcen.	lambda-function-public-access-verboten	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass AWS Lambda-Funktionen nicht öffentlich zugänglich sind. Der öffentliche Zugriff kann möglicherweise die Verfügbarkeit von Ressourcen beeinträchtigen.
SC.L2-3.13.4	Verhindern Sie die unbefugte und unbeabsichtigte Übertragung von Informationen aus gemeinsam genutzten Systemressourcen.	no-unrestricted-route-to-igw	Stellen Sie sicher, dass EC2 Amazon-Routentabellen keine uneingeschränkten Routen zu einem Internet-Gateway enthalten. Durch das Entfernen oder Beschränken des Internetzugangs für Workloads innerhalb von Amazon VPCs können unbeabsichtigte Zugriffe in Ihrer Umgebung reduziert werden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC.L2-3.13.4	Verhindern Sie die unbefugte und unbeabsichtigte Übertragung von Informationen aus gemeinsam genutzten Systemressourcen.	rds-instance-public-access-überprüfen	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Relational Database Service (Amazon RDS) -Instances nicht öffentlich sind. Amazon-RDS-Datenbank-Instances können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC.L2-3.13.4	Verhindern Sie die unbefugte und unbeabsichtigte Übertragung von Informationen aus gemeinsam genutzten Systemressourcen.	rds-snapshots-public-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Relational Database Service (Amazon RDS) -Instances nicht öffentlich sind. Amazon-RDS-Datenbank-Instances können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC.L2-3.13.4	Verhindern Sie die unbefugte und unbeabsichtigte Übertragung von Informationen aus gemeinsam genutzten Systemressourcen.	redshift-cluster-public-access-überprüfen	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Redshift Redshift-Cluster nicht öffentlich sind. Amazon-Redshift-Cluster können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC.L2-3.13.4	Verhindern Sie die unbefugte und unbeabsichtigte Übertragung von Informationen aus gemeinsam genutzten Systemressourcen.	restricted-common-ports	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass gemeinsame Ports für Amazon Elastic Compute Cloud (Amazon EC2) -Sicherheitsgruppen eingeschränkt sind. Wenn der Zugriff auf Ports nicht auf vertrauenswürdige Quellen beschränkt wird, kann dies zu Angriffen auf die Verfügbarkeit, Integrität und Vertraulichkeit von Systemen führen. Mit dieser Regel können Sie optional die Parameter blockedPort1–blockedPort5 festlegen (Standardkonfigurationen: 20, 21, 3389, 3306, 4333). Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC.L2-3.13.4	Verhindern Sie die unbefugte und unbeabsichtigte Übertragung von Informationen aus gemeinsam genutzten Systemressourcen.	s3- -Block-periodisch account-level-public-access	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Simple Storage Service (Amazon S3) -Buckets nicht öffentlich zugänglich sind. Diese Regel trägt dazu bei, sensible Daten vor unbefugten Remote-Benutzern zu schützen, indem sie den öffentlichen Zugriff verhindert. Mit dieser Regel können Sie optional die Parameter ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) und restrictPublicBuckets Parameter (Config Default: True) festlegen. Die tatsächlichen Werte müssen den Richtlini

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			en Ihrer Organisation entsprechen.
SC.L2-3.13.4	Verhindern Sie die unbefugte und unbeabsichtigte Übertragung von Informationen aus gemeinsam genutzten Systemressourcen.	s-3 bucket-public-read-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie nur autorisierten Benutzern, Prozessen und Geräten Zugriff auf Amazon Simple Storage Service (Amazon S3) - Buckets gewähren. Die Verwaltung des Zugriffs sollte mit der Klassifizierung der Daten übereinst immen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC.L2-3.13.4	Verhindern Sie die unbefugte und unbeabsichtigte Übertragung von Informationen aus gemeinsam genutzten Systemressourcen.	s-3 bucket-public-write-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie nur autorisierten Benutzern, Prozessen und Geräten Zugriff auf Amazon Simple Storage Service (Amazon S3) - Buckets gewähren. Die Verwaltung des Zugriffs sollte mit der Klassifizierung der Daten übereinstimmen.
SC.L2-3.13.4	Verhindern Sie die unbefugte und unbeabsichtigte Übertragung von Informationen aus gemeinsam genutzten Systemressourcen.	sagemaker-notebook-no-direct-Internetzugang	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass SageMaker Amazon-Notebooks keinen direkten Internetzugang zulassen. Indem Sie direkten Internetzugang blockieren, vermeiden Sie, dass unbefugte Benutzer auf sensible Daten zugreifen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC.L2-3.13.4	Verhindern Sie die unbefugte und unbeabsichtigte Übertragung von Informationen aus gemeinsam genutzten Systemressourcen.	ssm-document-not-public	Stellen Sie sicher, dass AWS Systems Manager (SSM) - Dokumente nicht öffentlich sind, da dies einen unbeabsichtigten Zugriff auf Ihre SSM-Dokumente ermöglichen kann. Ein öffentliches SSM-Dokument kann Informationen über Ihr Konto, Ihre Ressourcen und internen Prozesse preisgeben.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC.L2-3.13.4	Verhindern Sie die unbefugte und unbeabsichtigte Übertragung von Informationen aus gemeinsam genutzten Systemressourcen.	vpc-default-security-group-geschlossen	Sicherheitsgruppen von Amazon Elastic Compute Cloud (Amazon EC2) können bei der Verwaltung des Netzwerkzugriffs helfen, indem sie eine statusbehaftete Filterung des ein- und ausgehenden Netzwerkverkehrs zu Ressourcen bereitstellen. AWS Die Beschränk ung des gesamten Datenverkehrs auf die Standardsicherheit sgruppe hilft dabei, den Fernzugriff auf Ihre Ressourcen einzuschränken. AWS

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC.L2-3.13.4	Verhindern Sie die unbefugte und unbeabsichtigte Übertragung von Informationen aus gemeinsam genutzten Systemressourcen.	vpc-sg-open-only-to-authorized-ports	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass gemeinsame Ports für Amazon Elastic Compute Cloud (Amazon EC2) -Sicherheitsgruppen eingeschränkt sind. Wenn der Zugriff auf Ports nicht auf vertrauenswürdige Quellen beschränkt wird, kann dies zu Angriffen auf die Verfügbarkeit, Integrität und Vertraulichkeit von Systemen führen. Durch die Beschränkung des Zugriffs auf Ressourcen innerhalb einer Sicherheitsgruppe aus dem Internet (0.0.0.0/0) kann der Remote-Zugriff auf interne Systeme gesteuert werden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC.L2-3.13.8	Implementieren Sie kryptografische Mechanismen, um die unbefugte Offenlegung von CUI während der Übertragung zu verhindern, sofern dies nicht anderweitig durch alternative physische Schutzmaßnahmen vermieden wird.	acm-certificate-expiration-check	Stellen Sie sicher, dass die Netzwerkintegrität geschützt ist, indem Sie sicherstellen, dass X509-Zertifikate von AWS ACM ausgestellt werden. Diese Zertifikate müssen gültig und dürfen nicht abgelaufen sein. Für diese Regel ist ein Wert für erforderlich daysToExpiration (Wert für bewährte AWS Grundregeln für Sicherheit: 90). Der tatsächliche Wert muss den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC.L2-3.13.8	Implementieren Sie kryptografische Mechanismen, um die unbefugte Offenlegung von CUI während der Übertragung zu verhindern, sofern dies nicht anderweitig durch alternative physische Schutzmaßnahmen vermieden wird.	alb-http-drop-invalid-Header-aktiviert	Stellen Sie sicher, dass Ihre Elastic Load Balancers (ELB) so konfiguriert sind, dass sie HTTP-Header löschen. Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.
SC.L2-3.13.8	Implementieren Sie kryptografische Mechanismen, um die unbefugte Offenlegung von CUI während der Übertragung zu verhindern, sofern dies nicht anderweitig durch alternative physische Schutzmaßnahmen vermieden wird.	alb-http-to-https-Umleitungsprüfung	Um Daten während der Übertragung zu schützen, stellen Sie sicher, dass Ihr Application Load Balancer unverschlüsselte HTTP-Anfragen automatisch an HTTPS umleitet. Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC.L2-3.13.8	Implementieren Sie kryptografische Mechanismen, um die unbefugte Offenlegung von CUI während der Übertragung zu verhindern, sofern dies nicht anderweitig durch alternative physische Schutzmaßnahmen vermieden wird.	api-gw-ssl-enabled	Stellen Sie sicher, dass die REST-API-Stufen von Amazon API Gateway mit SSL-Zertifikaten konfiguriert sind, damit Backend-Systeme überprüfen können, ob Anforderungen von API Gateway stammen.
SC.L2-3.13.8	Implementieren Sie kryptografische Mechanismen, um die unbefugte Offenlegung von CUI während der Übertragung zu verhindern, sofern dies nicht anderweitig durch alternative physische Schutzmaßnahmen vermieden wird.	elasticsearch-node-to-node-Verschlüsselungsprüfung	Stellen Sie sicher, dass die node-to-node Verschlüsselung für Amazon OpenSearch Service aktiviert ist. Node-to-nodeVerschlüsselung ermöglicht die TLS 1.2-Verschlüsselung für die gesamte Kommunikation innerhalb der Amazon Virtual Private Cloud (Amazon VPC). Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC.L2-3.13.8	Implementieren Sie kryptografische Mechanismen, um die unbefugte Offenlegung von CUI während der Übertragung zu verhindern, sofern dies nicht anderweitig durch alternative physische Schutzmaßnahmen vermieden wird.	elbv-2 acm-certificate-required	Zum Schutz von eventuell vorhanden en sensiblen Daten sowie von Daten während der Übertragung muss die Verschlüsselung für Ihr Elastic Load Balancing aktiviert sein. Verwenden Sie AWS Certificate Manager, um öffentliche und private SSL/TLS-Zertifikate mit AWS Diensten und internen Ressourcen zu verwalten, bereitzustellen und bereitzustellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC.L2-3.13.8	Implementieren Sie kryptografische Mechanismen, um die unbefugte Offenlegung von CUI während der Übertragung zu verhindern, sofern dies nicht anderweitig durch alternative physische Schutzmaßnahmen vermieden wird.	elb-acm-certificate-required	Zum Schutz von eventuell vorhanden en sensiblen Daten sowie von Daten während der Übertragung muss die Verschlüsselung für Ihr Elastic Load Balancing aktiviert sein. Verwenden Sie AWS Certificate Manager, um öffentliche und private SSL/TLS-Zertifikate mit AWS Diensten und internen Ressourcen zu verwalten, bereitzustellen und bereitzustellen.
SC.L2-3.13.8	Implementieren Sie kryptografische Mechanismen, um die unbefugte Offenlegung von CUI während der Übertragung zu verhindern, sofern dies nicht anderweitig durch alternative physische Schutzmaßnahmen vermieden wird.	elb-tls-https-listeners-nur	Stellen Sie sicher, dass Ihre Elastic Load Balancer (ELBs) mit SSL- oder HTTPS-Listenern konfiguriert sind. Um eventuell vorhanden e sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC.L2-3.13.8	Implementieren Sie kryptografische Mechanismen, um die unbefugte Offenlegung von CUI während der Übertragung zu verhindern, sofern dies nicht anderweitig durch alternative physische Schutzmaßnahmen vermieden wird.	redshift-require-tls-ssl	Stellen Sie sicher, dass Ihre Amazon-Redshift-Cluster eine TLS/SSL-Verschlüsselung erfordern, um eine Verbindung zu SQL-Clients herzustellen. Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.
SC.L2-3.13.8	Implementieren Sie kryptografische Mechanismen, um die unbefugte Offenlegung von CUI während der Übertragung zu verhindern, sofern dies nicht anderweitig durch alternative physische Schutzmaßnahmen vermieden wird.	s-3 bucket-ssl-requests-only	Um Daten während der Übertragung zu schützen, stellen Sie sicher, dass Ihre Amazon Simple Storage Service (Amazon S3)-Buckets Anfragen zur Verwendung von Secure Socket Layer (SSL)-Buckets erfordern. Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC.L2-3.13.8	Implementieren Sie kryptografische Mechanismen, um die unbefugte Offenlegung von CUI während der Übertragung zu verhindern, sofern dies nicht anderweitig durch alternative physische Schutzmaßnahmen vermieden wird.	opensearch-node-to-node-Verschlüsselungsprüfung	Stellen Sie sicher, dass die node-to-node Verschlüsselung für Amazon OpenSearch Service aktiviert ist. Node-to-nodeVerschlüsselung ermöglicht die TLS 1.2-Verschlüsselung für die gesamte Kommunikation innerhalb der Amazon Virtual Private Cloud (Amazon VPC). Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.
SC.L2-3.13.10	Etablieren und verwalten Sie kryptografische Schlüssel für die in Organisationssystemen eingesetzte Kryptografie.	cmk-backing-key-rotation-aktiviert	Aktivieren Sie die Schlüsselrotation, um sicherzustellen, dass Schlüssel rotiert werden, nachdem sie das Ende ihrer Krypto-Periode erreicht haben.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC.L2-3.13.10	Etablieren und verwalten Sie kryptografische Schlüssel für die in Organisationssystemen eingesetzte Kryptografie.	kms-cmk-not-scheduled-zum Löschen	Um Daten im Ruhezustand zu schützen, sollten Sie sicherstellen, dass die für den Kunden erforderlichen Masterschlüssel (CMKs) nicht im AWS Key Management Service (AWS KMS) gelöscht werden. Da Schlüssel manchmal gelöscht werden müssen, können Sie mit dieser Regel alle zu löschenden Schlüssel überprüfen, falls ein Schlüssel versehentlich zur Löschung vorgemerkt wurde.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC.L2-3.13.15	Schützen Sie die Authentizität von Kommunikationssitzungen.	alb-http-to-https-Umleitungsprüfung	Um Daten während der Übertragung zu schützen, stellen Sie sicher, dass Ihr Application Load Balancer unverschlüsselte HTTP-Anfragen automatisch an HTTPS umleitet. Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.
SC.L2-3.13.15	Schützen Sie die Authentizität von Kommunikationssitzungen.	api-gw-ssl-enabled	Stellen Sie sicher, dass die REST-API-Stufen von Amazon API Gateway mit SSL-Zertifikaten konfiguriert sind, damit Backend-Systeme überprüfen können, ob Anforderungen von API Gateway stammen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC.L2-3.13.15	Schützen Sie die Authentizität von Kommunikationssitzungen.	elv 2- acm-certificate-required	Zum Schutz von eventuell vorhandenen sensiblen Daten sowie von Daten während der Übertragung muss die Verschlüsselung für Ihr Elastic Load Balancing aktiviert sein. Verwenden Sie AWS Certificate Manager, um öffentliche und private SSL/TLS-Zertifikate mit AWS Diensten und internen Ressourcen zu verwalten, bereitzustellen und bereitzustellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC.L2-3.13.15	Schützen Sie die Authentizität von Kommunikationssitzungen.	elb-acm-certificate-required	Zum Schutz von eventuell vorhandenen sensiblen Daten sowie von Daten während der Übertragung muss die Verschlüsselung für Ihr Elastic Load Balancing aktiviert sein. Verwenden Sie AWS Certificate Manager, um öffentliche und private SSL/TLS-Zertifikate mit AWS Diensten und internen Ressourcen zu verwalten, bereitzustellen und bereitzustellen.
SC.L2-3.13.15	Schützen Sie die Authentizität von Kommunikationssitzungen.	elb-tls-https-listeners-nur	Stellen Sie sicher, dass Ihre Elastic Load Balancer (ELBs) mit SSL- oder HTTPS-Listenern konfiguriert sind. Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC.L2-3.13.15	Schützen Sie die Authentizität von Kommunikationssitzungen.	redshift-require-tls-ssl	Stellen Sie sicher, dass Ihre Amazon-Redshift-Cluster eine TLS/SSL-Verschlüsselung erfordern, um eine Verbindung zu SQL-Clients herzustellen. Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.
SC.L2-3.13.16	Schützen Sie die Vertraulichkeit von CUI im Ruhezustand.	api-gw-cache-enabled-und verschlüsselt	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass die Verschlüsselung für den Cache Ihrer API-Gateway-Stufe aktiviert ist. Da für die API-Methode sensible Daten erfasst werden können, sollten Sie die Verschlüsselung von Daten im Ruhezustand aktivieren, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC.L2-3.13.16	Schützen Sie die Vertraulichkeit von CUI im Ruhezustand.	cloudwatch-log-group-encrypted	Um sensible Daten im Speicher zu schützen, stellen Sie sicher, dass die Verschlüs selung für Ihre Amazon CloudWatch Log Groups aktiviert ist.
SC.L2-3.13.16	Schützen Sie die Vertraulichkeit von CUI im Ruhezustand.	cloud-trail-encryption-enabled	Da sensible Daten vorhanden sein können und um Daten im Speicher zu schützen, sollten Sie sicherstellen, dass die Verschlüsselung für Ihre AWS CloudTrail Trails aktiviert ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC.L2-3.13.16	Schützen Sie die Vertraulichkeit von CUI im Ruhezustand.	ec-2 ebs-encryption-by-default	Zum Schutz von Daten im Ruhezustand müssen Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon Elastic Block Store (Amazon EBS)-Volumes aktiviert ist. Da sensible Daten auch im Ruhezustand vorhanden sein können, sollten Sie die Verschlüsselung im Ruhezustand aktivieren, um diese Daten zu schützen.
SC.L2-3.13.16	Schützen Sie die Vertraulichkeit von CUI im Ruhezustand.	efs-encrypted-check	Aktivieren Sie die Verschlüsselung für Ihr Amazon Elastic File System (EFS), um eventuell vorhandene sensible Daten sowie Daten im Ruhezustand zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC.L2-3.13.16	Schützen Sie die Vertraulichkeit von CUI im Ruhezustand.	elasticsearch-encrypted-at-rest	Da sensible Daten vorhanden sein können und um Daten im Ruhezustand zu schützen, sollten Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon OpenSearch Service (OpenSearch Service) -Domains aktiviert ist.
SC.L2-3.13.16	Schützen Sie die Vertraulichkeit von CUI im Ruhezustand.	encrypted-volumes	Aktivieren Sie die Verschlüsselung für Ihre Amazon-Elastic-Block-Store (Amazon-EBS)-Volumes, um eventuell vorhandene sensible Daten sowie Daten im Ruhezustand zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC.L2-3.13.16	Schützen Sie die Vertraulichkeit von CUI im Ruhezustand.	rds-snapshot-encrypted	Stellen Sie sicher, dass die Verschlüsselung für Ihre Amazon Relational Database Service (Amazon RDS)-Snapshots aktiviert ist. Da sensible Daten auch im Ruhezustand vorhanden sein können, sollten Sie die Verschlüsselung im Ruhezustand aktivieren, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC.L2-3.13.16	Schützen Sie die Vertraulichkeit von CUI im Ruhezustand.	rds-storage-encrypted	Zum Schutz von Daten im Ruhezustand müssen Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon Relational Database Service (Amazon RDS)-Instances aktiviert ist. Um eventuell vorhandene sensible Daten im Ruhezustand in Amazon-RDS-Instances zu schützen, muss die Verschlüsselung von Daten im Ruhezustand aktiviert sein.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC.L2-3.13.16	Schützen Sie die Vertraulichkeit von CUI im Ruhezustand.	redshift-cluster-kms-enabled	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass die Verschlüs selung mit AWS Key Management Service (AWS KMS) für Ihren Amazon Redshift Redshift-Cluster aktiviert ist. Um eventuell vorhanden e sensible Daten im Ruhezustand in Redshift-Clustern zu schützen, muss die Verschlüsselung von Daten im Ruhezusta nd aktiviert sein.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC.L2-3.13.16	Schützen Sie die Vertraulichkeit von CUI im Ruhezustand.	s3- aktiviert bucket-server-side-encryption	Zum Schutz von Daten im Ruhezustand müssen Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon Simple Storage Service (Amazon S3)-Buckets aktiviert ist. Um eventuell vorhandene sensible Daten im Ruhezustand in Amazon-S3-Buckets zu schützen, muss die Verschlüsselung aktiviert sein.
SC.L2-3.13.16	Schützen Sie die Vertraulichkeit von CUI im Ruhezustand.	s-3 default-encryption-kms	Stellen Sie sicher, dass die Verschlüsselung für Ihre Amazon Simple Storage Service (Amazon S3)-Buckets aktiviert ist. Um eventuell vorhandene sensible Daten im Ruhezustand in einem Amazon-S3-Bucket zu schützen, muss die Verschlüsselung aktiviert sein.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC.L2-3.13.16	Schützen Sie die Vertraulichkeit von CUI im Ruhezustand.	sagemaker-endpoint-configuration-kms-key-konfiguriert	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass die Verschlüsselung mit dem AWS Key Management Service (AWS KMS) für Ihren Endpunkt aktiviert ist. SageMaker Da sensible Daten auf dem SageMaker Endgerät gespeiche rt werden können, sollten Sie die Verschlüsselung im Ruhezustand aktiviere n, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC.L2-3.13.16	Schützen Sie die Vertraulichkeit von CUI im Ruhezustand.	sagemaker-notebook-instance-kms-schlüsselkonfiguriert	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass die Verschlüsselung mit dem AWS Key Management Service (AWS KMS) für Ihr Notebook aktiviert ist. SageMaker Da vertrauliche Daten im SageMaker Notebook gespeichert werden können, sollten Sie die Verschlüsselung im Ruhezustand aktivieren, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC.L2-3.13.16	Schützen Sie die Vertraulichkeit von CUI im Ruhezustand.	sns-encrypted-kms	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass Ihre Amazon Simple Notification Service (Amazon SNS) -Themen mit dem AWS Key Management Service (AWS KMS) verschlüsselt werden müssen. Um eventuell vorhandene sensible Daten im Ruhezustand in veröffentlichten Nachrichten zu schützen, muss die Verschlüsselung von Daten im Ruhezustand aktiviert sein.
SC.L2-3.13.16	Schützen Sie die Vertraulichkeit von CUI im Ruhezustand.	opensearch-encrypted-at-rest	Da sensible Daten vorhanden sein können und um Daten im Ruhezustand zu schützen, sollten Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon OpenSearch Service-Domains aktiviert ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SI.L2-3.14.1	Identifizieren, melden und korrigieren Sie Fehler in Informationen und Informationssystemen rechtzeitig.	cloudwatch-alarm-action-check	Amazon CloudWatch alarmiert, wenn eine Metrik den Schwellenwert für eine bestimmte Anzahl von Bewertungszeiträumen überschreitet. Der Alarm führt eine oder mehrere Aktionen durch, die vom Wert der Metrik oder des Ausdrucks im Vergleich zu einem Schwellenwert in einer Reihe von Zeiträumen abhängt. Diese Regel erfordert einen Wert für alarmActionRequired (Config Default: True), insufficientDataAction Required (Config Default: True), okActionRequired (Config Default: False). Der tatsächliche Wert muss die Alarmaktionen für Ihre Umgebung widerspiegeln.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SI.L2-3.14.1	Identifizieren, melden und korrigieren Sie Fehler in Informati onen und Informati onssystemen rechtzeit ig.	guardduty-enabled-centralized	Amazon GuardDuty kann mithilfe von Threat Intellige nce Feeds helfen, potenzielle Cybersich erheitsereignisse zu überwachen und zu erkennen. Dazu gehören Listen mit bösartigen IPs und maschinel len Lernmethoden zur Identifizierung unerwarteter, nicht autorisierter und bösartiger Aktivitäten in Ihrer AWS Cloud-Umgebung.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SI.L2-3.14.1	Identifizieren, melden und korrigieren Sie Fehler in Informati onen und Informati onssystemen rechtzeit ig.	securityhub-enabled	AWS Security Hub hilft bei der Überwachung von unbefugtem Personal, Verbindun gen, Geräten und Software. AWS Security Hub aggregiert, organisie rt und priorisie rt die Sicherhei tswarnungen oder Ergebnisse mehrerer Dienste. AWS Einige dieser Dienste sind Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer und AWS Firewall Manager sowie AWS Partnerlösungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SI.L2-3.14.2	Richten Sie Sicherheitsvorkehrungen zum Schutz vor schädlichem Code an geeigneten Stellen innerhalb der Informationssysteme der Organisation ein.	guardduty-enabled-centralized	Amazon GuardDuty kann mithilfe von Threat Intelligence Feeds helfen, potenzielle Cybersicherheitsereignisse zu überwachen und zu erkennen. Dazu gehören Listen mit bösartigen IPs und maschinellen Lernmethoden zur Identifizierung unerwarteter, nicht autorisierter und bösartiger Aktivitäten in Ihrer AWS Cloud-Umgebung.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SI.L2-3.14.5	Führen Sie während des Herunterladens, Öffnens und Ausführens von Dateien regelmäßige Scans des Informationssystems sowie Echtzeitscans von Dateien aus externen Quellen durch.	ecr-private-image-scanning-aktiviert	Der Amazon Elastic Container Repository (ECR)-Image-Scan unterstützt die Identifizierung von Software-Schwachstellen in Ihren Container-Images. Durch die Aktivierung von Image-Scans in ECR-Repositorys werden die Integrität und Sicherheit der gespeicherten Images mit einer zusätzlichen Überprüfungsebene verbessert.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SI.L2-3.14.3	Überwachen Sie die Warnmeldungen und Hinweise zur Systemsicherheit und ergreifen Sie entsprechende Maßnahmen.	alb-waf-enabled	Stellen Sie sicher, dass AWS WAF auf Elastic Load Balancers (ELB) aktiviert ist, um Webanwendungen zu schützen. Eine WAF trägt zum Schutz Ihrer Webanwend ungen oder APIs vor gängigen Web-Explo its bei. Diese Web-Exploits können sich auf die Verfügbar keit auswirken, die Sicherheit gefährden oder übermäßige Ressourcen in Ihrer Umgebung verbrauch en.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SI.L2-3.14.3	Überwachen Sie die Warnmeldungen und Hinweise zur Systemsicherheit und ergreifen Sie entsprechende Maßnahmen.	api-gw-associated-with-WAF	AWS Mit WAF können Sie eine Reihe von Regeln (als Web Access Control List (Web ACL) bezeichnet) konfigurieren, die Webanfragen auf der Grundlage von anpassbaren Websicherheitsregeln und -bedingungen, die Sie definieren, zulassen, blockieren oder zählen. Stellen Sie sicher, dass Ihre Amazon-API-Gateway-Stufe mit einer WAF-Web-ACL verknüpft ist, um sie vor böswilligen Angriffen zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SI.L2-3.14.3	Überwachen Sie die Warnmeldungen und Hinweise zur Systemsicherheit und ergreifen Sie entsprechende Maßnahmen.	cloudwatch-alarm-action-check	Amazon CloudWatch alarmiert, wenn eine Metrik den Schwellenwert für eine bestimmte Anzahl von Bewertungszeiträumen überschreitet. Der Alarm führt eine oder mehrere Aktionen durch, die vom Wert der Metrik oder des Ausdrucks im Vergleich zu einem Schwellenwert in einer Reihe von Zeiträumen abhängt. Diese Regel erfordert einen Wert für alarmActionRequired (Config Default: True), insufficientDataAction Required (Config Default: True), okActionRequired (Config Default: False). Der tatsächliche Wert muss die Alarmaktionen für Ihre Umgebung widerspiegeln.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SI.L2-3.14.3	Überwachen Sie die Warnmeldungen und Hinweise zur Systemsicherheit und ergreifen Sie entsprechende Maßnahmen.	cloud-trail-cloud-watch-logs-aktiviert	Verwenden Sie Amazon CloudWatch , um Protokoll ereignisaktivitäten zentral zu sammeln und zu verwalten. Die Aufnahme von AWS CloudTrail Daten liefert Einzelheiten zu den API-Aufrufaktivitäten in Ihrem AWS-Konto.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SI.L2-3.14.3	Überwachen Sie die Warnmeldungen und Hinweise zur Systemsicherheit und ergreifen Sie entsprechende Maßnahmen.	cloudtrail-enabled	AWS CloudTrail kann bei der Nichtabstreitbarkeit helfen, indem Aktionen und API-Aufrufe der AWS Management Console aufgezeichnet werden. Sie können die Benutzer und die Benutzer AWS-Konten , die einen AWS Dienst aufgerufen haben, die Quell-IP-Adresse, über die die Aufrufe generiert wurden, und den Zeitpunkt der Anrufe identifizieren. Einzelheiten zu den erfassten Daten finden Sie in den AWS CloudTrail Datensatzinhalten.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SI.L2-3.14.3	Überwachen Sie die Warnmeldungen und Hinweise zur Systemsicherheit und ergreifen Sie entsprechende Maßnahmen.	ec2-check managedinstance-association-compliance-status	Verwenden Sie AWS Systems Manager Associations, um bei der Inventarisierung von Softwareplattformen und Anwendungen innerhalb eines Unternehmens zu helfen. AWS Systems Manager weist Ihren verwalteten Instanzen einen Konfigurationsstatus zu und ermöglicht es Ihnen, Basiswerte für Betriebssystem-Patch-Levels, Softwareinstallationen, Anwendungskonfigurationen und andere Details zu Ihrer Umgebung festzulegen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SI.L2-3.14.3	Überwachen Sie die Warnmeldungen und Hinweise zur Systemsicherheit und ergreifen Sie entsprechende Maßnahmen.	guardduty-enabled-centralized	Amazon GuardDuty kann mithilfe von Threat Intellige nce Feeds helfen, potenzielle Cybersich erheitsereignisse zu überwachen und zu erkennen. Dazu gehören Listen mit bösartigen IPs und maschinel len Lernmethoden zur Identifizierung unerwarteter, nicht autorisierter und bösartiger Aktivitäten in Ihrer AWS Cloud-Umgebung.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SI.L2-3.14.3	Überwachen Sie die Warnmeldungen und Hinweise zur Systemsicherheit und ergreifen Sie entsprechende Maßnahmen.	multi-region-cloudtrail-enabled	AWS CloudTrail zeichnet Aktionen und API-Aufrufe der AWS Management Console auf. Sie können feststellen, welche Benutzer und Konten angerufen wurden AWS, von welcher Quell-IP-Adresse aus die Anrufe getätigt wurden und wann die Anrufe erfolgten. CloudTrail übermittelt Protokolldateien aus allen AWS Regionen an Ihren S3-Bucket , wenn MULTI_REG ION_CLOUD _TRAIL_ENABLED aktiviert ist. Außerdem wird beim AWS Start einer neuen Region derselbe Trail in der neuen Region erstellt. CloudTrail Dadurch erhalten Sie automatis ch Protokolldateien mit API-Aktivitäten für die neue Region.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SI.L2-3.14.3	Überwachen Sie die Warnmeldungen und Hinweise zur Systemsicherheit und ergreifen Sie entsprechende Maßnahmen.	securityhub-enabled	AWS Security Hub hilft bei der Überwachung von unbefugtem Personal, Verbindungen, Geräten und Software. AWS Security Hub aggregiert, organisiert und priorisiert die Sicherheitswarnungen oder Ergebnisse mehrerer Dienste. AWS Einige dieser Dienste sind Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer und AWS Firewall Manager sowie AWS Partnerlösungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SI.L2-3.14.6	Überwachen Sie die Organisationssysteme, einschließlich eingehenden und ausgehenden Kommunikationsverkehrs, um Angriffe und Hinweise für potenzielle Angriffe zu erkennen.	alb-waf-enabled	Stellen Sie sicher, dass AWS WAF auf Elastic Load Balancers (ELB) aktiviert ist, um Webanwendungen zu schützen. Eine WAF trägt zum Schutz Ihrer Webanwendungen oder APIs vor gängigen Web-Exploits bei. Diese Web-Exploits können sich auf die Verfügbarkeit auswirken, die Sicherheit gefährden oder übermäßige Ressourcen in Ihrer Umgebung verbrauchen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SI.L2-3.14.6	Überwachen Sie die Organisationssysteme, einschließlich eingehenden und ausgehenden Kommunikationsverkehrs, um Angriffe und Hinweise für potenzielle Angriffe zu erkennen.	api-gw-associated-with-WAF	AWS Mit WAF können Sie eine Reihe von Regeln (als Web Access Control List (Web ACL) bezeichnet) konfigurieren, die Webanfragen auf der Grundlage von anpassbaren Websicherheitsregeln und -bedingungen, die Sie definieren, zulassen, blockieren oder zählen. Stellen Sie sicher, dass Ihre Amazon-API-Gateway-Stufe mit einer WAF-Web-ACL verknüpft ist, um sie vor böswilligen Angriffen zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SI.L2-3.14.6	Überwachen Sie die Organisationssysteme, einschließlich eingehenden und ausgehenden Kommunikationsverkehrs, um Angriffe und Hinweise für potenzielle Angriffe zu erkennen.	cloud-trail-cloud-watch-Logs aktiviert	Verwenden Sie Amazon CloudWatch , um Protokoll ereignisaktivitäten zentral zu sammeln und zu verwalten. Die Aufnahme von AWS CloudTrail Daten liefert Einzelheiten zu den API-Aufrufaktivitäten in Ihrem AWS-Konto.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SI.L2-3.14.6	Überwachen Sie die Organisationssysteme, einschließlich eingehenden und ausgehenden Kommunikationsverkehrs, um Angriffe und Hinweise für potenzielle Angriffe zu erkennen.	cloudtrail-enabled	AWS CloudTrail kann bei der Nichtabstreitbarkeit helfen, indem Aktionen und API-Aufrufe der AWS Management Console aufgezeichnet werden. Sie können die Benutzer und die Benutzer AWS-Konten , die einen AWS Dienst aufgerufen haben, die Quell-IP-Adresse, über die die Aufrufe generiert wurden, und den Zeitpunkt der Anrufe identifizieren. Einzelheiten zu den erfassten Daten finden Sie in den AWS CloudTrail Datensatzinhalten.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SI.L2-3.14.6	Überwachen Sie die Organisationssysteme, einschließlich eingehenden und ausgehenden Kommunikationsverkehrs, um Angriffe und Hinweise für potenzielle Angriffe zu erkennen.	guardduty-enabled-centralized	Amazon GuardDuty kann mithilfe von Threat Intelligence Feeds helfen, potenzielle Cybersicherheitsereignisse zu überwachen und zu erkennen. Dazu gehören Listen mit bösartigen IPs und maschinellen Lernmethoden zur Identifizierung unerwarteter, nicht autorisierter und bösartiger Aktivitäten in Ihrer AWS Cloud-Umgebung.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SI.L2-3.14.6	Überwachen Sie die Organisationssysteme, einschließlich eingehenden und ausgehenden Kommunikationsverkehrs, um Angriffe und Hinweise für potenzielle Angriffe zu erkennen.	multi-region-cloudtrail-enabled	AWS CloudTrail zeichnet Aktionen und API-Aufrufe der AWS Management Console auf. Sie können feststellen, welche Benutzer und Konten angerufen wurden AWS, von welcher Quell-IP-Adresse aus die Anrufe getätigt wurden und wann die Anrufe erfolgten. CloudTrail übermittelt Protokolldateien aus allen AWS Regionen an Ihren S3-Bucket, wenn MULTI_REGION_CLOUD_TRAIL_ENABLED aktiviert ist. Außerdem wird beim AWS Start einer neuen Region derselbe Trail in der neuen Region erstellt. CloudTrail Dadurch erhalten Sie automatisch Protokolldateien mit API-Aktivitäten für die neue Region.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SI.L2-3.14.6	Überwachen Sie die Organisationssysteme, einschließlich eingehenden und ausgehenden Kommunikationsverkehrs, um Angriffe und Hinweise für potenzielle Angriffe zu erkennen.	securityhub-enabled	AWS Security Hub hilft bei der Überwachung von unbefugtem Personal, Verbindungen, Geräten und Software. AWS Security Hub aggregiert, organisiert und priorisiert die Sicherheitswarnungen oder Ergebnisse mehrerer Dienste. AWS Einige dieser Dienste sind Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer und AWS Firewall Manager sowie AWS Partnerlösungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SI.L2-3.14.6	Überwachen Sie die Organisationssysteme, einschließlich eingehenden und ausgehenden Kommunikationsverkehrs, um Angriffe und Hinweise für potenzielle Angriffe zu erkennen.	wafv2-logging-enabled	Um Ihnen bei der Protokollierung und Überwachung in Ihrer Umgebung zu helfen, aktivieren Sie die AWS WAF (V2) -Protokollierung im regionalen und globalen Web. ACLs AWS Die WAF-Protokollierung bietet detaillierte Informationen über den Datenverkehr, der von Ihrer Web-ACL analysiert wird. In den Protokollen werden die Uhrzeit aufgezeichnet, zu der die AWS WAF die Anfrage von Ihrer AWS Ressource erhalten hat, Informationen über die Anfrage und eine Aktion für die Regel, der jede Anfrage entsprach.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SI.L2-3.14.7	Identifizieren Sie die unbefugte Nutzung von Organisat ionssystemen.	api-gw-execution-l ogging-aktiviert	Die API-Gateway-Protokollierung zeigt detaillierte Ansichten der Benutzer, die auf die API zugegriff en haben, und wie diese Benutzer auf die API zugegriff en haben. Diese Einblicke ermöglichen die Transparenz von Benutzeraktivitäten.
SI.L2-3.14.7	Identifizieren Sie die unbefugte Nutzung von Organisat ionssystemen.	cloudtrail-s3-data events-enabled	Die Erfassung von Simple Storage Service (Amazon S3)-Datenereigniss en unterstützt die Erkennung von ungewöhnlichen Aktivitäten. Zu den Details gehören AWS-Konto Informationen über den Zugriff auf einen Amazon S3 S3-Bucket, die IP-Adress e und die Uhrzeit des Ereignisses.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SI.L2-3.14.7	Identifizieren Sie die unbefugte Nutzung von Organisat ionssystemen.	cloud-trail-cloud-watch-logs-aktiviert	Verwenden Sie Amazon CloudWatc h , um Protokoll ereignisaktivitäten zentral zu sammeln und zu verwalten. Die Aufnahme von AWS CloudTrail Daten liefert Einzelheiten zu den API-Aufrufaktivitä ten in Ihrem AWS-Konto.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SI.L2-3.14.7	Identifizieren Sie die unbefugte Nutzung von Organisat ionssystemen.	cloudtrail-enabled	AWS CloudTrail kann bei der Nichtabst reitbarkeit helfen, indem Aktionen und API-Aufrufe der AWS Management Console aufgezeic hnet werden. Sie können die Benutzer und die Benutzer AWS-Konten , die einen AWS Dienst aufgerufen haben, die Quell-IP-Adresse, über die die Aufrufe generiert wurden, und den Zeitpunkt der Anrufe identifiz ieren. Einzelheiten zu den erfassten Daten finden Sie in den AWS CloudTrail Datensatzinhalten.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SI.L2-3.14.7	Identifizieren Sie die unbefugte Nutzung von Organisationssystemen.	ec2-check managedinstance-association-compliance-status	Verwenden Sie AWS Systems Manager Associations, um bei der Inventarisierung von Softwareplattformen und Anwendungen innerhalb eines Unternehmens zu helfen. AWS Systems Manager weist Ihren verwalteten Instanzen einen Konfigurationsstatus zu und ermöglicht es Ihnen, Basiswerte für Betriebssystem-Patch-Levels, Softwareinstallationen, Anwendungskonfigurationen und andere Details zu Ihrer Umgebung festzulegen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SI.L2-3.14.7	Identifizieren Sie die unbefugte Nutzung von Organisat ionssystemen.	elb-logging-enabled	Die Elastic-Load-Balancing-Aktivität ist ein zentraler Kommunikationspunk t innerhalb einer Umgebung. Stellen Sie sicher, dass die ELB-Protokollierun g aktiviert ist. Die gesammelten Daten enthalten detaillie rte Informationen zu Anfragen, die an den ELB gesendet wurden. Jedes Protokoll enthält Informationen wie die Zeit, zu der die Anforderung einging, die Client-IP -Adresse, Latenzen, Anforderungspfade und Serverantworten.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SI.L2-3.14.7	Identifizieren Sie die unbefugte Nutzung von Organisat ionssystemen.	guardduty-enabled-centralized	Amazon GuardDuty kann mithilfe von Threat Intellige nce Feeds helfen, potenzielle Cybersich erheitsereignisse zu überwachen und zu erkennen. Dazu gehören Listen mit bösartigen IPs und maschinel len Lernmethoden zur Identifizierung unerwarteter, nicht autorisierter und bösartiger Aktivitäten in Ihrer AWS Cloud-Umgebung.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SI.L2-3.14.7	Identifizieren Sie die unbefugte Nutzung von Organisat ionssystemen.	multi-region-cloudtrail-enabled	AWS CloudTrail zeichnet Aktionen und API-Aufrufe der AWS Management Console auf. Sie können feststellen, welche Benutzer und Konten angerufen wurden AWS, von welcher Quell-IP-Adresse aus die Anrufe getätigt wurden und wann die Anrufe erfolgten. CloudTrail übermittelt Protokolldateien aus allen AWS Regionen an Ihren S3-Bucket , wenn MULTI_REG ION_CLOUD _TRAIL_ENABLED aktiviert ist. Außerdem wird beim AWS Start einer neuen Region derselbe Trail in der neuen Region erstellt. CloudTrail Dadurch erhalten Sie automatis ch Protokolldateien mit API-Aktivitäten für die neue Region.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SI.L2-3.14.7	Identifizieren Sie die unbefugte Nutzung von Organisat ionssystemen.	rds-logging-enabled	Um die Protokoll ierung und Überwachung in Ihrer Umgebung zu erleichtern, stellen Sie sicher, dass die Amazon Relationa l Database Service (Amazon RDS)-Prot okollierung aktiviert ist. Mit der Amazon-RDS-Protokollierung können Sie Ereigniss e wie Verbindungen, Verbindungsabbrüch e, Abfragen oder abgefragte Tabellen erfassen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SI.L2-3.14.7	Identifizieren Sie die unbefugte Nutzung von Organisat ionssystemen.	s-3 bucket-logging-enabled	Die Amazon Simple Storage Service (Amazon S3)-Serverzugriffs protokollierung bietet eine Methode zur Überwachu ng des Netzwerks im Hinblick auf potenzielle Cybersich erheitsereignisse. Die Ereignisse werden überwacht, indem detaillierte Aufzeichn ungen über die Anfragen erfasst werden, die an einen Amazon-S3-Bucket gestellt wurden. Jeder Zugriffsprotokolle intrag enthält Details zu einer einzelnen Zugriffsanfrage. Zu den Details gehören Anforderer, Bucket-Name, Anforderu ngszeit, Anforderu ngsaktion, Antwortst atus und Fehlercode, falls relevant.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SI.L2-3.14.7	Identifizieren Sie die unbefugte Nutzung von Organisat ionssystemen.	securityhub-enabled	AWS Security Hub hilft bei der Überwachung von unbefugtem Personal, Verbindun gen, Geräten und Software. AWS Security Hub aggregiert, organisie rt und priorisie rt die Sicherhei tswarnungen oder Ergebnisse mehrerer Dienste. AWS Einige dieser Dienste sind Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer und AWS Firewall Manager sowie AWS Partnerlösungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SI.L2-3.14.7	Identifizieren Sie die unbefugte Nutzung von Organisat ionssystemen.	wafv2-logging-enab led	Um Ihnen bei der Protokollierung und Überwachung in Ihrer Umgebung zu helfen, aktivieren Sie die AWS WAF (V2) -Protokollierung im regionalen und globalen Web. ACLs AWS Die WAF-Protokollierung bietet detaillierte Informationen über den Datenverkehr, der von Ihrer Web-ACL analysiert wird. In den Protokollen werden die Uhrzeit aufgezeic hnet, zu der die AWS WAF die Anfrage von Ihrer AWS Ressource erhalten hat, Informati onen über die Anfrage und eine Aktion für die Regel, der jede Anfrage entsprach.

Vorlage

Die Vorlage ist verfügbar unter GitHub: Operational Best Practices for CMMC 2.0 Level 2.

Bewährte Methoden für die Ausführung von Datenverarbeitungsservices

Dieses Conformance Pack enthält AWS Config Regeln, die auf Compute Services basieren. Weitere Informationen finden Sie unter Datenverarbeitung für jede Workload. Eine Liste aller verwalteten Regeln, die von unterstützt werden AWS Config, finden Sie unter Liste der AWS Config verwalteten Regeln.

Die Namen und Beschreibungen der erforderlichen Parameter finden Sie im `Parameters` Abschnitt der folgenden Vorlage.

Die Vorlage ist verfügbar unter GitHub: Operational Best Practices for Compute Services.

Bewährte Methoden für die Erreichung von Ausfallsicherheit

Eine Liste aller verwalteten Regeln, die von unterstützt werden AWS Config, finden Sie unter Liste der AWS Config verwalteten Regeln.

Die Namen und Beschreibungen der erforderlichen Parameter finden Sie im `Parameters` Abschnitt der folgenden Vorlage.

Die Vorlage ist verfügbar unter GitHub: Operational Best Practices for Data Resiliency.

Bewährte Methoden für die Ausführung von Datenbankservices

Dieses Conformance Pack enthält AWS Config Regeln, die auf Databases Services basieren. Weitere Informationen finden Sie unter Datenbanken auf AWS. Eine Liste aller verwalteten Regeln, die von unterstützt werden AWS Config, finden Sie unter Liste der AWS Config verwalteten Regeln.

Die Namen und Beschreibungen der erforderlichen Parameter finden Sie im `Parameters` Abschnitt der folgenden Vorlage.

Die Vorlage ist verfügbar unter GitHub: Operational Best Practices for Databases Services.

Bewährte Methoden für die Ausführung von Data Lakes und Analyseservices

Dieses Conformance Pack enthält AWS Config Regeln für Data Lakes und Analytics Services. Weitere Informationen finden Sie unter Data Lakes und Analytics auf AWS. Eine Liste aller verwalteten Regeln, die von unterstützt werden AWS Config, finden Sie unter Liste der AWS Config verwalteten Regeln.

Die Namen und Beschreibungen der erforderlichen Parameter finden Sie im `Parameters` Abschnitt der folgenden Vorlage.

Die Vorlage ist verfügbar unter GitHub: Operational Best Practices for Data Lakes and Analytics Services.

Bewährte Methoden für die Ausführung von DevOps

Dieses Konformitätspaket enthält AWS Config Regeln, die auf DevOps internen AWS Regeln basieren. Eine Liste aller verwalteten Regeln, die von unterstützt werden AWS Config, finden Sie unter Liste der AWS Config verwalteten Regeln.

Die Namen und Beschreibungen der erforderlichen Parameter finden Sie im `Parameters` Abschnitt der folgenden Vorlage.

Die Vorlage ist verfügbar unter GitHub: Operational Best Practices für DevOps.

Bewährte Methoden für die Ausführung von EC2

Dieses Konformitätspaket enthält AWS Config Regeln, die auf EC2 basieren. Eine Liste aller verwalteten Regeln, die von unterstützt werden AWS Config, finden Sie unter Liste der AWS Config verwalteten Regeln.

Die Namen und Beschreibungen der erforderlichen Parameter finden Sie im `Parameters` Abschnitt der folgenden Vorlage.

Die Vorlage ist verfügbar unter GitHub: Operational Best Practices für EC2.

Bewährte Methoden für die Verwendung von Verschlüsselung und Schlüsselverwaltung

Eine Liste aller verwalteten Regeln, die von unterstützt werden AWS Config, finden Sie unter Liste der AWS Config verwalteten Regeln.

Die Namen und Beschreibungen der erforderlichen Parameter finden Sie im `Parameters` Abschnitt der folgenden Vorlage.

Die Vorlage ist verfügbar unter GitHub: Operational Best Practices for Encryption and Key Management.

Leitfaden für bewährte Betriebspraktiken für die ENISA-Cybersicherheit für SMEs

Konformitätspakete bieten ein allgemeines Compliance-Framework, das es Ihnen ermöglicht, mithilfe verwalteter oder benutzerdefinierter AWS Config Regeln und Abhilfemaßnahmen Kontrollen zur Sicherheits-, Betriebs- oder Kostenoptimierung durchzuführen. AWS Config Conformance Packs dienen als Beispielvorlagen nicht dazu, die vollständige Einhaltung eines bestimmten Governance- oder Compliance-Standards sicherzustellen. Sie sind dafür verantwortlich, selbst zu beurteilen, ob Ihre Nutzung der Services den geltenden gesetzlichen und behördlichen Anforderungen entspricht.

Im Folgenden finden Sie ein Beispiel für eine Zuordnung zwischen dem Cybersicherheitsleitfaden der Agentur der Europäischen Union für Cybersicherheit (ENISA) SMEs und den AWS verwalteten Konfigurationsregeln. Jede Config-Regel gilt für eine bestimmte AWS Ressource und bezieht sich auf einen oder mehrere ENISA-Cybersicherheitsleitfäden für SMEs Kontrollen. Ein ENISA-Cybersicherheitsleitfaden zur SMEs Kontrolle kann sich auf mehrere Konfigurationsregeln beziehen. In der folgenden Tabelle finden Sie weitere Informationen und Anleitungen zu diesen Zuordnungen.

Diese Vorlage für ein Konformitätspaket enthält Zuordnungen zu Kontrollen, die aus dem ENISA-Cybersicherheitsleitfaden für übernommen wurden. SMEs Der ENISA-Leitfaden zur Cybersicherheit für SMEs ist unter Cybersicherheitsleitfaden für SMEs — 12 Schritte zur Absicherung Ihres Unternehmens verfügbar.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
1_ENTWICKELN EINER GUTEN CYBERSICHERHEITSKULTUR: VERÖFFENTLICHEN VON CYBERSICHERHEITSRICHTLINIEN	Die Cybersicherheit erfordert klare und konkrete Regeln	security-awareness-program-exists(Prozessüberprüfung)	Etablieren und pflegen Sie ein Programm zur Förderung des Sicherheitsbewusstseins in Ihrer Organisation. Programme zur Förderung des Sicherheitsbewusstseins der Mitarbeiter vermitteln ihnen, wie

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			sie ihre Organisation vor diversen Sicherheitsverletzungen oder Sicherheitsvorfällen schützen können.
1_ENTWICKELN EINER GUTEN CYBERSICHERHEITSKULTUR: DENKEN SIE AN DEN DATENSCHUTZ	Gemäß der Allgemeinen Datenschutzverordnung1 der EU müssen alle SMEs , die personenbezogene Daten von Bürgern der EU/des EWR verarbeiten oder speichern, sicherstellen, dass angemessene Sicherheitskontrollen zum Schutz dieser Daten vorhanden sind. Dazu gehört auch, dass Dritte, die im Namen des KMU arbeiten, über angemessene Sicherheitsmaßnahmen verfügen.	autoscaling-launch-config-public-ip-deaktiviert	Wenn Sie Ihre Netzwerkschnittstellen mit einer öffentlichen IP-Adresse konfigurieren, sind die diesen Netzwerkschnittstellen zugehörigen Ressourcen über das Internet erreichbar. EC2 Ressourcen sollten nicht öffentlich zugänglich sein, da dies einen unbeabsichtigten Zugriff auf Ihre Anwendungen oder Server ermöglichen kann.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
1_ENTWICKELN EINER GUTEN CYBERSICHERHEITSKULTUR: DENKEN SIE AN DEN DATENSCHUTZ	Gemäß der Allgemeinen Datenschutzverordnung1 der EU müssen alle SMEs , die personenbezogene Daten von Bürgern der EU/des EWR verarbeiten oder speichern, sicherstellen, dass angemessene Sicherheitskontrollen zum Schutz dieser Daten vorhanden sind. Dazu gehört auch, dass Dritte, die im Namen des KMU arbeiten, über angemessene Sicherheitsmaßnahmen verfügen.	dms-replication-not-public	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass auf DMS-Replikationsinstanzen nicht öffentlich zugegriffen werden kann. DMS-Replikations-Instances können vertrauliche Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
1_ENTWICKELN EINER GUTEN CYBERSICHERHEITSKULTUR: DENKEN SIE AN DEN DATENSCHUTZ	Gemäß der Allgemeinen Datenschutzverordnung1 der EU müssen alle SMEs , die personenbezogene Daten von Bürgern der EU/des EWR verarbeiten oder speichern, sicherstellen, dass angemessene Sicherheitskontrollen zum Schutz dieser Daten vorhanden sind. Dazu gehört auch, dass Dritte, die im Namen des KMU arbeiten, über angemessene Sicherheitsmaßnahmen verfügen.	ebs-snapshot-public-restorable-überprüfen	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass EBS-Snapshots nicht öffentlich wiederherstellbar sind. EBS-Volume-Snapshots können vertrauliche Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
1_ENTWICKELN EINER GUTEN CYBERSICHERHEITSKULTUR: DENKEN SIE AN DEN DATENSCHUTZ	Gemäß der Allgemeinen Datenschutzverordnung1 der EU müssen alle SMEs , die personenbezogene Daten von Bürgern der EU/des EWR verarbeiten oder speichern, sicherstellen, dass angemessene Sicherheitskontrollen zum Schutz dieser Daten vorhanden sind. Dazu gehört auch, dass Dritte, die im Namen des KMU arbeiten, über angemessene Sicherheitsmaßnahmen verfügen.	ec2- instance-no-public-ip	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon Elastic Compute Cloud (Amazon EC2) - Instances nicht öffentlich zugänglich sind. EC2 Amazon-Instances können vertrauliche Informationen enthalten, und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
1_ENTWICKELN EINER GUTEN CYBERSICHERHEITSKULTUR: DENKEN SIE AN DEN DATENSCHUTZ	Gemäß der Allgemeinen Datenschutzverordnung1 der EU müssen alle SMEs , die personenbezogene Daten von Bürgern der EU/des EWR verarbeiten oder speichern, sicherstellen, dass angemessene Sicherheitskontrollen zum Schutz dieser Daten vorhanden sind. Dazu gehört auch, dass Dritte, die im Namen des KMU arbeiten, über angemessene Sicherheitsmaßnahmen verfügen.	emr-master-no-public-ip	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon EMR-Cluster-Masterknoten nicht öffentlich zugänglich sind. Amazon-EMR-Cluster-Hauptknoten können vertrauliche Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
1_ENTWICKELN EINER GUTEN CYBERSICHERHEITSKULTUR: DENKEN SIE AN DEN DATENSCHUTZ	Gemäß der Allgemeinen Datenschutzverordnung1 der EU müssen alle SMEs , die personenbezogene Daten von Bürgern der EU/des EWR verarbeiten oder speichern, sicherstellen, dass angemessene Sicherheitskontrollen zum Schutz dieser Daten vorhanden sind. Dazu gehört auch, dass Dritte, die im Namen des KMU arbeiten, über angemessene Sicherheitsmaßnahmen verfügen.	lambda-function-public-access-verboten	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass AWS Lambda-Funktionen nicht öffentlich zugänglich sind. Der öffentliche Zugriff kann möglicherweise die Verfügbarkeit von Ressourcen beeinträchtigen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
1_ENTWICKELN EINER GUTEN CYBERSICHERHEITSKULTUR: DENKEN SIE AN DEN DATENSCHUTZ	Gemäß der Allgemeinen Datenschutzverordnung1 der EU müssen alle SMEs , die personenbezogene Daten von Bürgern der EU/des EWR verarbeiten oder speichern, sicherstellen, dass angemessene Sicherheitskontrollen zum Schutz dieser Daten vorhanden sind. Dazu gehört auch, dass Dritte, die im Namen des KMU arbeiten, über angemessene Sicherheitsmaßnahmen verfügen.	rds-instance-public-access-überprüfen	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Relational Database Service (Amazon RDS) -Instances nicht öffentlich sind. Amazon-RDS-Datenbank-Instances können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
1_ENTWICKELN EINER GUTEN CYBERSICHERHEITSKULTUR: DENKEN SIE AN DEN DATENSCHUTZ	Gemäß der Allgemeinen Datenschutzverordnung1 der EU müssen alle SMEs , die personenbezogene Daten von Bürgern der EU/des EWR verarbeiten oder speichern, sicherstellen, dass angemessene Sicherheitskontrollen zum Schutz dieser Daten vorhanden sind. Dazu gehört auch, dass Dritte, die im Namen des KMU arbeiten, über angemessene Sicherheitsmaßnahmen verfügen.	rds-snapshots-public-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Relational Database Service (Amazon RDS) -Instances nicht öffentlich sind. Amazon-RDS-Datenbank-Instances können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
1_ENTWICKELN EINER GUTEN CYBERSICHERHEITSKULTUR: DENKEN SIE AN DEN DATENSCHUTZ	Gemäß der Allgemeinen Datenschutzverordnung1 der EU müssen alle SMEs , die personenbezogene Daten von Bürgern der EU/des EWR verarbeiten oder speichern, sicherstellen, dass angemessene Sicherheitskontrollen zum Schutz dieser Daten vorhanden sind. Dazu gehört auch, dass Dritte, die im Namen des KMU arbeiten, über angemessene Sicherheitsmaßnahmen verfügen.	redshift-cluster-public-access-überprüfen	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Redshift Redshift-Cluster nicht öffentlich sind. Amazon-Redshift-Cluster können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
1_ENTWICKELN EINER GUTEN CYBERSICHERHEITSKULTUR: DENKEN SIE AN DEN DATENSCHUTZ	Gemäß der Allgemeinen Datenschutzverordnung1 der EU müssen alle SMEs , die personenbezogene Daten von Bürgern der EU/des EWR verarbeiten oder speichern, sicherstellen, dass angemessene Sicherheitskontrollen zum Schutz dieser Daten vorhanden sind. Dazu gehört auch, dass Dritte, die im Namen des KMU arbeiten, über angemessene Sicherheitsmaßnahmen verfügen.	s3- -blöcke-periodisch account-level-public-access	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Simple Storage Service (Amazon S3) -Buckets nicht öffentlich zugänglich sind. Diese Regel trägt dazu bei, sensible Daten vor unbefugten Remote-Benutzern zu schützen, indem sie den öffentlichen Zugriff verhindert. Mit dieser Regel können Sie optional die Parameter ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) und restrictPublicBuckets Parameter (Config Default: True) festlegen. Die tatsächlichen Werte müssen den Richtlini

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			en Ihrer Organisation entsprechen.
1_ENTWICKELN EINER GUTEN CYBERSICHERHEITSKULTUR: DENKEN SIE AN DEN DATENSCHUTZ	Gemäß der Allgemeinen Datenschutzverordnung1 der EU müssen alle SMEs , die personenbezogene Daten von Bürgern der EU/des EWR verarbeiten oder speichern, sicherstellen, dass angemessene Sicherheitskontrollen zum Schutz dieser Daten vorhanden sind. Dazu gehört auch, dass Dritte, die im Namen des KMU arbeiten, über angemessene Sicherheitsmaßnahmen verfügen.	s3- verboten bucket-level-public-access	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Simple Storage Service (Amazon S3) -Buckets nicht öffentlich zugänglich sind. Diese Regel trägt dazu bei, sensible Daten vor unbefugten Remote-Benutzern zu schützen, indem sie den öffentlichen Zugriff auf Bucket-Ebene verhindert.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
1_ENTWICKELN EINER GUTEN CYBERSICHERHEITSKULTUR: DENKEN SIE AN DEN DATENSCHUTZ	Gemäß der Allgemeinen Datenschutzverordnung1 der EU müssen alle SMEs , die personenbezogene Daten von Bürgern der EU/des EWR verarbeiten oder speichern, sicherstellen, dass angemessene Sicherheitskontrollen zum Schutz dieser Daten vorhanden sind. Dazu gehört auch, dass Dritte, die im Namen des KMU arbeiten, über angemessene Sicherheitsmaßnahmen verfügen.	s3- bucket-public-read-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie nur autorisierten Benutzern, Prozessen und Geräten Zugriff auf Amazon Simple Storage Service (Amazon S3) - Buckets gewähren. Die Verwaltung des Zugriffs sollte mit der Klassifizierung der Daten übereinstimmen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
1_ENTWICKELN EINER GUTEN CYBERSICHERHEITSKULTUR: DENKEN SIE AN DEN DATENSCHUTZ	Gemäß der Allgemeinen Datenschutzverordnung1 der EU müssen alle SMEs , die personenbezogene Daten von Bürgern der EU/des EWR verarbeiten oder speichern, sicherstellen, dass angemessene Sicherheitskontrollen zum Schutz dieser Daten vorhanden sind. Dazu gehört auch, dass Dritte, die im Namen des KMU arbeiten, über angemessene Sicherheitsmaßnahmen verfügen.	s3- bucket-public-write-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie nur autorisierten Benutzern, Prozessen und Geräten Zugriff auf Amazon Simple Storage Service (Amazon S3) - Buckets gewähren. Die Verwaltung des Zugriffs sollte mit der Klassifizierung der Daten übereinstimmen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
1_ENTWICKELN EINER GUTEN CYBERSICHERHEITSKULTUR: DENKEN SIE AN DEN DATENSCHUTZ	Gemäß der Allgemeinen Datenschutzverordnung1 der EU müssen alle SMEs , die personenbezogene Daten von Bürgern der EU/des EWR verarbeiten oder speichern, sicherstellen, dass angemessene Sicherheitskontrollen zum Schutz dieser Daten vorhanden sind. Dazu gehört auch, dass Dritte, die im Namen des KMU arbeiten, über angemessene Sicherheitsmaßnahmen verfügen.	s3- bucket-acl-prohibited	Diese Regel prüft, ob Access Control Lists (ACLs) für die Zugriffskontrolle auf Amazon S3 S3-Buckets verwendet werden. ACLs sind veraltete Zugriffskontrollmechanismen für Amazon S3 S3-Buckets, die älter sind als AWS Identity and Access Management (IAM). Stattdessen empfiehlt es sich ACLs, IAM-Richtlinien oder S3-Bucket-Richtlinien zu verwenden, um den Zugriff auf Ihre S3-Buckets einfacher zu verwalten.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
1_ENTWICKELN EINER GUTEN CYBERSICHERHEITSKULTUR: DENKEN SIE AN DEN DATENSCHUTZ	Gemäß der Allgemeinen Datenschutzverordnung1 der EU müssen alle SMEs , die personenbezogene Daten von Bürgern der EU/des EWR verarbeiten oder speichern, sicherstellen, dass angemessene Sicherheitskontrollen zum Schutz dieser Daten vorhanden sind. Dazu gehört auch, dass Dritte, die im Namen des KMU arbeiten, über angemessene Sicherheitsmaßnahmen verfügen.	ssm-document-not-public	Stellen Sie sicher, dass AWS Systems Manager (SSM) - Dokumente nicht öffentlich sind, da dies einen unbeabsichtigten Zugriff auf Ihre SSM-Dokumente ermöglichen kann. Ein öffentliches SSM-Dokument kann Informationen über Ihr Konto, Ihre Ressourcen und internen Prozesse preisgeben.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
1_ENTWICKELN EINER GUTEN CYBERSICHERHEITSKULTUR: DENKEN SIE AN DEN DATENSCHUTZ	Gemäß der Allgemeinen Datenschutzverordnung1 der EU müssen alle SMEs , die personenbezogene Daten von Bürgern der EU/des EWR verarbeiten oder speichern, sicherstellen, dass angemessene Sicherheitskontrollen zum Schutz dieser Daten vorhanden sind. Dazu gehört auch, dass Dritte, die im Namen des KMU arbeiten, über angemessene Sicherheitsmaßnahmen verfügen.	subnet-auto-assign-public-ip-deaktiviert	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon Virtual Private Cloud (VPC) -Subnetzen nicht automatisch eine öffentliche IP-Adresse zugewiesen wird. Amazon Elastic Compute Cloud (EC2) -Instances, die in Subnetzen gestartet werden, in denen dieses Attribut aktiviert ist, haben ihrer primären Netzwerkschnittstelle eine öffentliche IP-Adresse zugewiesen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
1_ENTWICKELN EINER GUTEN CYBERSICHERHEITSKULTUR: DENKEN SIE AN DEN DATENSCHUTZ	Gemäß der Allgemeinen Datenschutzverordnung1 der EU müssen alle SMEs , die personenbezogene Daten von Bürgern der EU/des EWR verarbeiten oder speichern, sicherstellen, dass angemessene Sicherheitskontrollen zum Schutz dieser Daten vorhanden sind. Dazu gehört auch, dass Dritte, die im Namen des KMU arbeiten, über angemessene Sicherheitsmaßnahmen verfügen.	alb-http-to-https-Weiterleitungsprüfung	Um Daten während der Übertragung zu schützen, stellen Sie sicher, dass Ihr Application Load Balancer unverschlüsselte HTTP-Anfragen automatisch an HTTPS umleitet. Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
1_ENTWICKELN EINER GUTEN CYBERSICHERHEITSKULTUR: DENKEN SIE AN DEN DATENSCHUTZ	Gemäß der Allgemeinen Datenschutzverordnung1 der EU müssen alle SMEs , die personenbezogene Daten von Bürgern der EU/des EWR verarbeiten oder speichern, sicherstellen, dass angemessene Sicherheitskontrollen zum Schutz dieser Daten vorhanden sind. Dazu gehört auch, dass Dritte, die im Namen des KMU arbeiten, über angemessene Sicherheitsmaßnahmen verfügen.	alb-http-drop-invalid-Header-fähig	Stellen Sie sicher, dass Ihre Elastic Load Balancers (ELB) so konfiguriert sind, dass sie HTTP-Header löschen. Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
1_ENTWICKELN EINER GUTEN CYBERSICHERHEITSKULTUR: DENKEN SIE AN DEN DATENSCHUTZ	Gemäß der Allgemeinen Datenschutzverordnung1 der EU müssen alle SMEs , die personenbezogene Daten von Bürgern der EU/des EWR verarbeiten oder speichern, sicherstellen, dass angemessene Sicherheitskontrollen zum Schutz dieser Daten vorhanden sind. Dazu gehört auch, dass Dritte, die im Namen des KMU arbeiten, über angemessene Sicherheitsmaßnahmen verfügen.	api-gw-cache-enabled-und verschlüsselt	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass die Verschlüsselung für den Cache Ihrer API-Gateway-Stufe aktiviert ist. Da für die API-Methode sensible Daten erfasst werden können, sollten Sie die Verschlüsselung von Daten im Ruhezustand aktivieren, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
1_ENTWICKELN EINER GUTEN CYBERSICHERHEITSKULTUR: DENKEN SIE AN DEN DATENSCHUTZ	Gemäß der Allgemeinen Datenschutzverordnung1 der EU müssen alle SMEs , die personenbezogene Daten von Bürgern der EU/des EWR verarbeiten oder speichern, sicherstellen, dass angemessene Sicherheitskontrollen zum Schutz dieser Daten vorhanden sind. Dazu gehört auch, dass Dritte, die im Namen des KMU arbeiten, über angemessene Sicherheitsmaßnahmen verfügen.	api-gw-ssl-enabled	Stellen Sie sicher, dass die REST-API-Stufen von Amazon API Gateway mit SSL-Zertifikaten konfiguriert sind, damit Backend-Systeme überprüfen können, ob Anforderungen von API Gateway stammen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
1_ENTWICKELN EINER GUTEN CYBERSICHERHEITSKULTUR: DENKEN SIE AN DEN DATENSCHUTZ	Gemäß der Allgemeinen Datenschutzverordnung1 der EU müssen alle SMEs , die personenbezogene Daten von Bürgern der EU/des EWR verarbeiten oder speichern, sicherstellen, dass angemessene Sicherheitskontrollen zum Schutz dieser Daten vorhanden sind. Dazu gehört auch, dass Dritte, die im Namen des KMU arbeiten, über angemessene Sicherheitsmaßnahmen verfügen.	backup-recovery-point-encrypted	Stellen Sie sicher, dass die Verschlüsselung für Ihre AWS Backup-Wiederherstellungspunkte aktiviert ist. Da sensible Daten auch im Ruhezustand vorhanden sein können, sollten Sie die Verschlüsselung im Ruhezustand aktivieren, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
1_ENTWICKELN EINER GUTEN CYBERSICHERHEITSKULTUR: DENKEN SIE AN DEN DATENSCHUTZ	Gemäß der Allgemeinen Datenschutzverordnung1 der EU müssen alle Personen SMEs , die personenbezogene Daten von Bürgern der EU/des EWR verarbeiten oder speichern, sicherstellen, dass angemessene Sicherheitskontrollen zum Schutz dieser Daten vorhanden sind. Dazu gehört auch, dass Dritte, die im Namen des KMU arbeiten, über angemessene Sicherheitsmaßnahmen verfügen.	backup-recovery-point-manual-Löschen-deaktiviert	Stellen Sie sicher, dass Ihren AWS Backup-Wiederherstellungspunkten eine ressourcenbasierte Richtlinie zugeordnet ist, die das Löschen von Wiederherstellungspunkten verhindert. Die Verwendung einer ressourcenbasierten Richtlinie zur Verhinderung des Löschens von Wiederherstellungspunkten kann dazu beitragen, ein versehentliches oder absichtliches Löschen zu unterbinden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
1_ENTWICKELN EINER GUTEN CYBERSICHERHEITSKULTUR: DENKEN SIE AN DEN DATENSCHUTZ	Gemäß der Allgemeinen Datenschutzverordnung1 der EU müssen alle Personen SMEs , die personenbezogene Daten von Bürgern der EU/des EWR verarbeiten oder speichern, sicherstellen, dass angemessene Sicherheitskontrollen zum Schutz dieser Daten vorhanden sind. Dazu gehört auch, dass Dritte, die im Namen des KMU arbeiten, über angemessene Sicherheitsmaßnahmen verfügen.	cloud-trail-encryption-enabled	Da sensible Daten vorhanden sein können und um Daten im Speicher zu schützen, sollten Sie sicherstellen, dass die Verschlüsselung Ihrer Daten aktiviert ist. AWS CloudTrail

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
1_ENTWICKELN EINER GUTEN CYBERSICHERHEITSKULTUR: DENKEN SIE AN DEN DATENSCHUTZ	Gemäß der Allgemeinen Datenschutzverordnung1 der EU müssen alle SMEs , die personenbezogene Daten von Bürgern der EU/des EWR verarbeiten oder speichern, sicherstellen, dass angemessene Sicherheitskontrollen zum Schutz dieser Daten vorhanden sind. Dazu gehört auch, dass Dritte, die im Namen des KMU arbeiten, über angemessene Sicherheitsmaßnahmen verfügen.	dynamodb-table-encrypted-kms	Stellen Sie sicher, dass die Verschlüsselung für Ihre Amazon-DynamoDB-Tabellen aktiviert ist. Um eventuell vorhandene sensible Daten im Ruhezustand in diesen Tabellen zu schützen, müssen Sie die Verschlüsselung von Daten im Ruhezustand aktivieren. Standardmäßig werden DynamoDB-Tabellen mit einem AWS eigenen Kundenhauptschlüssel (CMK) verschlüselt.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
1_ENTWICKELN EINER GUTEN CYBERSICHERHEITSKULTUR: DENKEN SIE AN DEN DATENSCHUTZ	Gemäß der Allgemeinen Datenschutzverordnung1 der EU müssen alle SMEs , die personenbezogene Daten von Bürgern der EU/des EWR verarbeiten oder speichern, sicherstellen, dass angemessene Sicherheitskontrollen zum Schutz dieser Daten vorhanden sind. Dazu gehört auch, dass Dritte, die im Namen des KMU arbeiten, über angemessene Sicherheitsmaßnahmen verfügen.	ec2- ebs-encryption-by-default	Zum Schutz von Daten im Ruhezustand müssen Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon Elastic Block Store (Amazon EBS)-Volumes aktiviert ist. Da sensible Daten auch im Ruhezustand vorhanden sein können, sollten Sie die Verschlüsselung im Ruhezustand aktivieren, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
1_ENTWICKELN EINER GUTEN CYBERSICHERHEITSKULTUR: DENKEN SIE AN DEN DATENSCHUTZ	Gemäß der Allgemeinen Datenschutzverordnung1 der EU müssen alle SMEs , die personenbezogene Daten von Bürgern der EU/des EWR verarbeiten oder speichern, sicherstellen, dass angemessene Sicherheitskontrollen zum Schutz dieser Daten vorhanden sind. Dazu gehört auch, dass Dritte, die im Namen des KMU arbeiten, über angemessene Sicherheitsmaßnahmen verfügen.	efs-encrypted-check	Aktivieren Sie die Verschlüsselung für Ihr Amazon Elastic File System (EFS), um eventuell vorhandene sensible Daten sowie Daten im Ruhezustand zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
1_ENTWICKELN EINER GUTEN CYBERSICHERHEITSKULTUR: DENKEN SIE AN DEN DATENSCHUTZ	Gemäß der Allgemeinen Datenschutzverordnung1 der EU müssen alle SMEs , die personenbezogene Daten von Bürgern der EU/des EWR verarbeiten oder speichern, sicherstellen, dass angemessene Sicherheitskontrollen zum Schutz dieser Daten vorhanden sind. Dazu gehört auch, dass Dritte, die im Namen des KMU arbeiten, über angemessene Sicherheitsmaßnahmen verfügen.	elasticsearch-encrypted-at-rest	Aktivieren Sie die Verschlüsselung für Ihre Domains im Amazon Elasticsearch Service (Amazon ES), um eventuell vorhandene sensible Daten sowie Daten im Ruhezustand zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
1_ENTWICKELN EINER GUTEN CYBERSICHERHEITSKULTUR: DENKEN SIE AN DEN DATENSCHUTZ	Gemäß der Allgemeinen Datenschutzverordnung1 der EU müssen alle SMEs , die personenbezogene Daten von Bürgern der EU/des EWR verarbeiten oder speichern, sicherstellen, dass angemessene Sicherheitskontrollen zum Schutz dieser Daten vorhanden sind. Dazu gehört auch, dass Dritte, die im Namen des KMU arbeiten, über angemessene Sicherheitsmaßnahmen verfügen.	efs-access-point-enforce-Stammverzeichnis	Die Durchsetzung eines Stammverzeichnisses für einen Amazon-Elastic-File-System (Amazon-EFS)-Zugangspunkt trägt dazu bei, den Datenzugriff einzuschränken, indem sichergestellt wird, dass Benutzer des Zugangspunkts nur auf Dateien des angegebenen Unterverzeichnisses zugreifen können.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
1_ENTWICKELN EINER GUTEN CYBERSICHERHEITSKULTUR: DENKEN SIE AN DEN DATENSCHUTZ	Gemäß der Allgemeinen Datenschutzverordnung1 der EU müssen alle SMEs , die personenbezogene Daten von Bürgern der EU/des EWR verarbeiten oder speichern, sicherstellen, dass angemessene Sicherheitskontrollen zum Schutz dieser Daten vorhanden sind. Dazu gehört auch, dass Dritte, die im Namen des KMU arbeiten, über angemessene Sicherheitsmaßnahmen verfügen.	efs-access-point-enforce-Benutzeridentität	Um die Implementierung des Prinzips der geringsten Rechte zu unterstützen, stellen Sie sicher, dass die Benutzerdurchsetzung für Ihr Amazon Elastic File System (Amazon EFS) aktiviert ist. Wenn diese Option aktiviert ist, ersetzt Amazon EFS den Benutzer und die Gruppe IDs des NFS-Clients durch die Identität, die auf dem Access Point für alle Dateisystemoperationen konfiguriert ist, und gewährt nur Zugriff auf diese erzwungene Benutzeridentität.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
1_ENTWICKELN EINER GUTEN CYBERSICHERHEITSKULTUR: DENKEN SIE AN DEN DATENSCHUTZ	Gemäß der Allgemeinen Datenschutzverordnung1 der EU müssen alle SMEs , die personenbezogene Daten von Bürgern der EU/des EWR verarbeiten oder speichern, sicherstellen, dass angemessene Sicherheitskontrollen zum Schutz dieser Daten vorhanden sind. Dazu gehört auch, dass Dritte, die im Namen des KMU arbeiten, über angemessene Sicherheitsmaßnahmen verfügen.	encrypted-volumes	Aktivieren Sie die Verschlüsselung für Ihre Amazon-Elastic-Block-Store (Amazon-EBS)-Volumes, um eventuell vorhandene sensible Daten sowie Daten im Ruhezustand zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
1_ENTWICKELN EINER GUTEN CYBERSICHERHEITSKULTUR: DENKEN SIE AN DEN DATENSCHUTZ	Gemäß der Allgemeinen Datenschutzverordnung1 der EU müssen alle SMEs , die personenbezogene Daten von Bürgern der EU/des EWR verarbeiten oder speichern, sicherstellen, dass angemessene Sicherheitskontrollen zum Schutz dieser Daten vorhanden sind. Dazu gehört auch, dass Dritte, die im Namen des KMU arbeiten, über angemessene Sicherheitsmaßnahmen verfügen.	cloud-trail-log-file-Validierung aktiviert	Verwenden Sie die AWS CloudTrail Protokolldateivalidierung, um die Integrität von Protokollen zu überprüfen. CloudTrail Mithilfe der Protokolldateivalidierung kann festgestellt werden, ob eine Protokolldatei geändert oder gelöscht wurde oder ob sie nach der Übermittlung CloudTrail unverändert geblieben ist. Dieses Feature wurde mit dem Branchenstandard entsprechenden Algorithmen entwickelt: SHA-256 für die Hashfunktion und SHA-256 mit RSA für digitale Signaturen. Aus diesem Grund ist es rechnerisch unmöglich, CloudTrail Protokolldateien unbemerkt zu ändern, zu löschen oder zu fälschen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
1_ENTWICKELN EINER GUTEN CYBERSICHERHEITSKULTUR: DENKEN SIE AN DEN DATENSCHUTZ	Gemäß der Allgemeinen Datenschutzverordnung1 der EU müssen alle SMEs , die personenbezogene Daten von Bürgern der EU/des EWR verarbeiten oder speichern, sicherstellen, dass angemessene Sicherheitskontrollen zum Schutz dieser Daten vorhanden sind. Dazu gehört auch, dass Dritte, die im Namen des KMU arbeiten, über angemessene Sicherheitsmaßnahmen verfügen.	cloudwatch-log-group-encrypted	Um sensible Daten im Speicher zu schützen, stellen Sie sicher, dass die Verschlüsselung für Ihre Amazon CloudWatch Log Groups aktiviert ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
1_ENTWICKELN EINER GUTEN CYBERSICHERHEITSKULTUR: DENKEN SIE AN DEN DATENSCHUTZ	Gemäß der Allgemeinen Datenschutzverordnung1 der EU müssen alle SMEs , die personenbezogene Daten von Bürgern der EU/des EWR verarbeiten oder speichern, sicherstellen, dass angemessene Sicherheitskontrollen zum Schutz dieser Daten vorhanden sind. Dazu gehört auch, dass Dritte, die im Namen des KMU arbeiten, über angemessene Sicherheitsmaßnahmen verfügen.	codebuild-project-artifact-encryption	Um sensible Daten im Speicher zu schützen, stellen Sie sicher, dass die Verschlüsselung für Ihre Artefakte aktiviert ist. AWS CodeBuild

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
1_ENTWICKELN EINER GUTEN CYBERSICHERHEITSKULTUR: DENKEN SIE AN DEN DATENSCHUTZ	Gemäß der Allgemeinen Datenschutzverordnung1 der EU müssen alle SMEs , die personenbezogene Daten von Bürgern der EU/des EWR verarbeiten oder speichern, sicherstellen, dass angemessene Sicherheitskontrollen zum Schutz dieser Daten vorhanden sind. Dazu gehört auch, dass Dritte, die im Namen des KMU arbeiten, über angemessene Sicherheitsmaßnahmen verfügen.	secretsmanager-using-cmk	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass die Verschlüsselung mit dem AWS Key Management Service (AWS KMS) für AWS Secrets Manager aktiviert ist. Aktivieren Sie die Verschlüsselung von Daten im Ruhezustand, um eventuell vorhandene sensible Daten im Ruhezustand im Secrets Manager zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
1_ENTWICKELN EINER GUTEN CYBERSICHERHEITSKULTUR: DENKEN SIE AN DEN DATENSCHUTZ	Gemäß der Allgemeinen Datenschutzverordnung1 der EU müssen alle SMEs , die personenbezogene Daten von Bürgern der EU/des EWR verarbeiten oder speichern, sicherstellen, dass angemessene Sicherheitskontrollen zum Schutz dieser Daten vorhanden sind. Dazu gehört auch, dass Dritte, die im Namen des KMU arbeiten, über angemessene Sicherheitsmaßnahmen verfügen.	codebuild-project-sVerschlüsselung mit 3 Protokollen	Um sensible Daten im Speicher zu schützen, stellen Sie sicher, dass die Verschlüsselung für Ihre in Amazon S3 gespeicherten AWS CodeBuild Protokolle aktiviert ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
1_ENTWICKELN EINER GUTEN CYBERSICHERHEITSKULTUR: DENKEN SIE AN DEN DATENSCHUTZ	Gemäß der Allgemeinen Datenschutzverordnung1 der EU müssen alle SMEs , die personenbezogene Daten von Bürgern der EU/des EWR verarbeiten oder speichern, sicherstellen, dass angemessene Sicherheitskontrollen zum Schutz dieser Daten vorhanden sind. Dazu gehört auch, dass Dritte, die im Namen des KMU arbeiten, über angemessene Sicherheitsmaßnahmen verfügen.	opensearch-encrypted-at-rest	Da sensible Daten vorhanden sein können und um Daten im Ruhezustand zu schützen, sollten Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon OpenSearch Service-Domains aktiviert ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
1_ENTWICKELN EINER GUTEN CYBERSICHERHEITSKULTUR: DENKEN SIE AN DEN DATENSCHUTZ	Gemäß der Allgemeinen Datenschutzverordnung1 der EU müssen alle SMEs , die personenbezogene Daten von Bürgern der EU/des EWR verarbeiten oder speichern, sicherstellen, dass angemessene Sicherheitskontrollen zum Schutz dieser Daten vorhanden sind. Dazu gehört auch, dass Dritte, die im Namen des KMU arbeiten, über angemessene Sicherheitsmaßnahmen verfügen.	elasticsearch-node-to-node-Verschlüsselungsprüfung	Stellen Sie sicher, dass die node-to-node Verschlüsselung für Amazon Elasticsearch Service aktiviert ist. Node-to-nodeVerschlüsselung ermöglicht die TLS 1.2-Verschlüsselung für die gesamte Kommunikation innerhalb der Amazon Virtual Private Cloud (Amazon VPC). Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
1_ENTWICKELN EINER GUTEN CYBERSICHERHEITSKULTUR: DENKEN SIE AN DEN DATENSCHUTZ	Gemäß der Allgemeinen Datenschutzverordnung1 der EU müssen alle SMEs , die personenbezogene Daten von Bürgern der EU/des EWR verarbeiten oder speichern, sicherstellen, dass angemessene Sicherheitskontrollen zum Schutz dieser Daten vorhanden sind. Dazu gehört auch, dass Dritte, die im Namen des KMU arbeiten, über angemessene Sicherheitsmaßnahmen verfügen.	opensearch-node-to-node-Verschlüsselungsprüfung	Stellen Sie sicher, dass die node-to-node Verschlüsselung für Amazon OpenSearch Service aktiviert ist. Node-to-nodeVerschlüsselung ermöglicht die TLS 1.2-Verschlüsselung für die gesamte Kommunikation innerhalb der Amazon Virtual Private Cloud (Amazon VPC). Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
1_ENTWICKELN EINER GUTEN CYBERSICHERHEITSKULTUR: DENKEN SIE AN DEN DATENSCHUTZ	Gemäß der Allgemeinen Datenschutzverordnung1 der EU müssen alle SMEs , die personenbezogene Daten von Bürgern der EU/des EWR verarbeiten oder speichern, sicherstellen, dass angemessene Sicherheitskontrollen zum Schutz dieser Daten vorhanden sind. Dazu gehört auch, dass Dritte, die im Namen des KMU arbeiten, über angemessene Sicherheitsmaßnahmen verfügen.	elb-tls-https-listeners-nur	Stellen Sie sicher, dass Ihre Elastic Load Balancer (ELBs) mit SSL- oder HTTPS-Listenern konfiguriert sind. Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
1_ENTWICKELN EINER GUTEN CYBERSICHERHEITSKULTUR: DENKEN SIE AN DEN DATENSCHUTZ	Gemäß der Allgemeinen Datenschutzverordnung1 der EU müssen alle SMEs , die personenbezogene Daten von Bürgern der EU/des EWR verarbeiten oder speichern, sicherstellen, dass angemessene Sicherheitskontrollen zum Schutz dieser Daten vorhanden sind. Dazu gehört auch, dass Dritte, die im Namen des KMU arbeiten, über angemessene Sicherheitsmaßnahmen verfügen.	elb-acm-certificate-required	Zum Schutz von eventuell vorhandenen sensiblen Daten sowie von Daten während der Übertragung muss die Verschlüsselung für Ihr Elastic Load Balancing aktiviert sein. Verwenden Sie AWS Certificate Manager, um öffentliche und private SSL/TLS-Zertifikate mit AWS Diensten und internen Ressourcen zu verwalten, bereitzustellen und bereitzustellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
1_ENTWICKELN EINER GUTEN CYBERSICHERHEITSKULTUR: DENKEN SIE AN DEN DATENSCHUTZ	Gemäß der Allgemeinen Datenschutzverordnung1 der EU müssen alle SMEs , die personenbezogene Daten von Bürgern der EU/des EWR verarbeiten oder speichern, sicherstellen, dass angemessene Sicherheitskontrollen zum Schutz dieser Daten vorhanden sind. Dazu gehört auch, dass Dritte, die im Namen des KMU arbeiten, über angemessene Sicherheitsmaßnahmen verfügen.	elbv2- acm-certificate-required	Zum Schutz von eventuell vorhandenen sensiblen Daten sowie von Daten während der Übertragung muss die Verschlüsselung für Ihr Elastic Load Balancing aktiviert sein. Verwenden Sie AWS Certificate Manager, um öffentliche und private SSL/TLS-Zertifikate mit AWS Diensten und internen Ressourcen zu verwalten, bereitzustellen und bereitzustellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
1_ENTWICKELN EINER GUTEN CYBERSICHERHEITSKULTUR: DENKEN SIE AN DEN DATENSCHUTZ	Gemäß der Allgemeinen Datenschutzverordnung1 der EU müssen alle SMEs , die personenbezogene Daten von Bürgern der EU/des EWR verarbeiten oder speichern, sicherstellen, dass angemessene Sicherheitskontrollen zum Schutz dieser Daten vorhanden sind. Dazu gehört auch, dass Dritte, die im Namen des KMU arbeiten, über angemessene Sicherheitsmaßnahmen verfügen.	encrypted-volumes	Aktivieren Sie die Verschlüsselung für Ihre Amazon-Elastic-Block-Store (Amazon-EBS)-Volumes, um eventuell vorhandene sensible Daten sowie Daten im Ruhezustand zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
1_ENTWICKELN EINER GUTEN CYBERSICHERHEITSKULTUR: DENKEN SIE AN DEN DATENSCHUTZ	Gemäß der Allgemeinen Datenschutzverordnung1 der EU müssen alle SMEs , die personenbezogene Daten von Bürgern der EU/des EWR verarbeiten oder speichern, sicherstellen, dass angemessene Sicherheitskontrollen zum Schutz dieser Daten vorhanden sind. Dazu gehört auch, dass Dritte, die im Namen des KMU arbeiten, über angemessene Sicherheitsmaßnahmen verfügen.	kinesis-stream-encrypted	Aktivieren Sie die Verschlüsselung für Ihre Amazon-Kinesis-Streams, um eventuell vorhandene sensible Daten sowie Daten im Ruhezustand zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
1_ENTWICKELN EINER GUTEN CYBERSICHERHEITSKULTUR: DENKEN SIE AN DEN DATENSCHUTZ	Gemäß der Allgemeinen Datenschutzverordnung1 der EU müssen alle SMEs , die personenbezogene Daten von Bürgern der EU/des EWR verarbeiten oder speichern, sicherstellen, dass angemessene Sicherheitskontrollen zum Schutz dieser Daten vorhanden sind. Dazu gehört auch, dass Dritte, die im Namen des KMU arbeiten, über angemessene Sicherheitsmaßnahmen verfügen.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) kann Ihnen dabei helfen, die Prinzipien der geringsten Rechte und der Aufgabentrennung in Zugriffsberechtigungen und Autorisierungen zu integrieren und so zu verhindern, dass Richtlinien „Effect“: „Allow“ mit „Action“: „*“ anstelle von „Resource“: „*“ enthalten. Wenn Benutzern mehr Rechte eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und der Aufgabentrennung verstoßen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
1_ENTWICKELN EINER GUTEN CYBERSICHERHEITSKULTUR: DENKEN SIE AN DEN DATENSCHUTZ	Gemäß der Allgemeinen Datenschutzverordnung1 der EU müssen alle SMEs , die personenbezogene Daten von Bürgern der EU/des EWR verarbeiten oder speichern, sicherstellen, dass angemessene Sicherheitskontrollen zum Schutz dieser Daten vorhanden sind. Dazu gehört auch, dass Dritte, die im Namen des KMU arbeiten, über angemessene Sicherheitsmaßnahmen verfügen.	iam-policy-no-statements-with-full-access	Stellen Sie sicher, dass IAM-Aktionen nur auf die benötigten Aktionen beschränkt sind. Wenn Benutzern mehr Rechte eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und der Aufgabentrennung verstoßen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
1_ENTWICKELN EINER GUTEN CYBERSICHERHEITSKULTUR: DENKEN SIE AN DEN DATENSCHUTZ	Gemäß der Allgemeinen Datenschutzverordnung1 der EU müssen alle SMEs , die personenbezogene Daten von Bürgern der EU/des EWR verarbeiten oder speichern, sicherstellen, dass angemessene Sicherheitskontrollen zum Schutz dieser Daten vorhanden sind. Dazu gehört auch, dass Dritte, die im Namen des KMU arbeiten, über angemessene Sicherheitsmaßnahmen verfügen.	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) Security Groups können bei der Verwaltung des Netzwerkzugriffs helfen, indem sie eine statusbehaftete Filterung von eingehendem und ausgehendem Netzwerkverkehr zu Ressourcen bereitstellen. AWS Wenn Sie eingehenden (oder entfernten) Datenverkehr von 0.0.0.0/0 bis Port 22 auf Ihren Ressourcen nicht zulassen, können Sie den Remote-Zugriff einschränken.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
1_ENTWICKELN EINER GUTEN CYBERSICHERHEITSKULTUR: DENKEN SIE AN DEN DATENSCHUTZ	Gemäß der Allgemeinen Datenschutzverordnung1 der EU müssen alle SMEs , die personenbezogene Daten von Bürgern der EU/des EWR verarbeiten oder speichern, sicherstellen, dass angemessene Sicherheitskontrollen zum Schutz dieser Daten vorhanden sind. Dazu gehört auch, dass Dritte, die im Namen des KMU arbeiten, über angemessene Sicherheitsmaßnahmen verfügen.	internet-gateway-authorized-vpc-nur	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Internet-Gateways nur mit autorisierter Amazon Virtual Private Cloud (Amazon VPC) verbunden sind. Internet-Gateways ermöglichen den bidirektionalen Internetzugang zur und von der Amazon VPC, was möglicher weise zu einem unbefugten Zugriff auf Amazon-VPC-Ressourcen führen kann.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
1_ENTWICKELN EINER GUTEN CYBERSICHERHEITSKULTUR: DENKEN SIE AN DEN DATENSCHUTZ	Gemäß der Allgemeinen Datenschutzverordnung1 der EU müssen alle SMEs , die personenbezogene Daten von Bürgern der EU/des EWR verarbeiten oder speichern, sicherstellen, dass angemessene Sicherheitskontrollen zum Schutz dieser Daten vorhanden sind. Dazu gehört auch, dass Dritte, die im Namen des KMU arbeiten, über angemessene Sicherheitsmaßnahmen verfügen.	no-unrestricted-route-to-igw	Stellen Sie sicher, dass EC2 Amazon-Routentabellen keine uneingeschränkten Routen zu einem Internet-Gateway enthalten. Durch das Entfernen oder Beschränken des Internetzugangs für Workloads innerhalb von Amazon VPCs können unbeabsichtigte Zugriffe in Ihrer Umgebung reduziert werden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
1_ENTWICKELN EINER GUTEN CYBERSICHERHEITSKULTUR: DENKEN SIE AN DEN DATENSCHUTZ	Gemäß der Allgemeinen Datenschutzverordnung1 der EU müssen alle SMEs , die personenbezogene Daten von Bürgern der EU/des EWR verarbeiten oder speichern, sicherstellen, dass angemessene Sicherheitskontrollen zum Schutz dieser Daten vorhanden sind. Dazu gehört auch, dass Dritte, die im Namen des KMU arbeiten, über angemessene Sicherheitsmaßnahmen verfügen.	rds-snapshot-encrypted	Stellen Sie sicher, dass die Verschlüsselung für Ihre Amazon Relational Database Service (Amazon RDS)-Snapshots aktiviert ist. Da sensible Daten auch im Ruhezustand vorhanden sein können, sollten Sie die Verschlüsselung im Ruhezustand aktivieren, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
1_ENTWICKELN EINER GUTEN CYBERSICHERHEITSKULTUR: DENKEN SIE AN DEN DATENSCHUTZ	Gemäß der Allgemeinen Datenschutzverordnung1 der EU müssen alle SMEs , die personenbezogene Daten von Bürgern der EU/des EWR verarbeiten oder speichern, sicherstellen, dass angemessene Sicherheitskontrollen zum Schutz dieser Daten vorhanden sind. Dazu gehört auch, dass Dritte, die im Namen des KMU arbeiten, über angemessene Sicherheitsmaßnahmen verfügen.	rds-storage-encrypted	Zum Schutz von Daten im Ruhezustand müssen Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon Relational Database Service (Amazon RDS)-Instances aktiviert ist. Um eventuell vorhandene sensible Daten im Ruhezustand in Amazon-RDS-Instances zu schützen, muss die Verschlüsselung von Daten im Ruhezustand aktiviert sein.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
1_ENTWICKELN EINER GUTEN CYBERSICHERHEITSKULTUR: DENKEN SIE AN DEN DATENSCHUTZ	Gemäß der Allgemeinen Datenschutzverordnung1 der EU müssen alle SMEs , die personenbezogene Daten von Bürgern der EU/des EWR verarbeiten oder speichern, sicherstellen, dass angemessene Sicherheitskontrollen zum Schutz dieser Daten vorhanden sind. Dazu gehört auch, dass Dritte, die im Namen des KMU arbeiten, über angemessene Sicherheitsmaßnahmen verfügen.	redshift-cluster-configuration-check	Um Daten im Ruhezustand zu schützen, muss die Verschlüsselung für Ihre Amazon-Redshift-Cluster aktiviert sein. Sie müssen auch sicherstellen, dass die erforderlichen Konfigurationen auf Amazon-Redshift-Clustern bereitgestellt werden. Die Prüfungsprotokollierung muss aktiviert sein, um Informationen zu Verbindungen und Benutzeraktivitäten in der Datenbank bereitzustellen. Diese Regel erfordert, dass ein Wert für clusterDbEncrypted (Config Default: TRUE) und LoggingEnabled (Config Default: TRUE) gesetzt ist. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
1_ENTWICKELN EINER GUTEN CYBERSICHERHEITSKULTUR: DENKEN SIE AN DEN DATENSCHUTZ	Gemäß der Allgemeinen Datenschutzverordnung1 der EU müssen alle SMEs , die personenbezogene Daten von Bürgern der EU/des EWR verarbeiten oder speichern, sicherstellen, dass angemessene Sicherheitskontrollen zum Schutz dieser Daten vorhanden sind. Dazu gehört auch, dass Dritte, die im Namen des KMU arbeiten, über angemessene Sicherheitsmaßnahmen verfügen.	redshift-require-tls-ssl	Stellen Sie sicher, dass Ihre Amazon-Redshift-Cluster eine TLS/SSL-Verschlüsselung erfordern, um eine Verbindung zu SQL-Clients herzustellen. Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
1_ENTWICKELN EINER GUTEN CYBERSICHERHEITSKULTUR: DENKEN SIE AN DEN DATENSCHUTZ	Gemäß der Allgemeinen Datenschutzverordnung1 der EU müssen alle SMEs , die personenbezogene Daten von Bürgern der EU/des EWR verarbeiten oder speichern, sicherstellen, dass angemessene Sicherheitskontrollen zum Schutz dieser Daten vorhanden sind. Dazu gehört auch, dass Dritte, die im Namen des KMU arbeiten, über angemessene Sicherheitsmaßnahmen verfügen.	redshift-cluster-kms-enabled	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass die Verschlüsselung mit AWS Key Management Service (AWS KMS) für Ihren Amazon Redshift Redshift-Cluster aktiviert ist. Um eventuell vorhandene sensible Daten im Ruhezustand in Redshift-Clustern zu schützen, muss die Verschlüsselung von Daten im Ruhezustand aktiviert sein.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
1_ENTWICKELN EINER GUTEN CYBERSICHERHEITSKULTUR: DENKEN SIE AN DEN DATENSCHUTZ	Gemäß der Allgemeinen Datenschutzverordnung1 der EU müssen alle SMEs , die personenbezogene Daten von Bürgern der EU/des EWR verarbeiten oder speichern, sicherstellen, dass angemessene Sicherheitskontrollen zum Schutz dieser Daten vorhanden sind. Dazu gehört auch, dass Dritte, die im Namen des KMU arbeiten, über angemessene Sicherheitsmaßnahmen verfügen.	s3- default-encryption-kms	Stellen Sie sicher, dass die Verschlüsselung für Ihre Amazon Simple Storage Service (Amazon S3)-Buckets aktiviert ist. Um eventuell vorhandene sensible Daten im Ruhezustand in einem Amazon-S3-Bucket zu schützen, muss die Verschlüsselung aktiviert sein.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
1_ENTWICKELN EINER GUTEN CYBERSICHERHEITSKULTUR: DENKEN SIE AN DEN DATENSCHUTZ	Gemäß der Allgemeinen Datenschutzverordnung1 der EU müssen alle SMEs , die personenbezogene Daten von Bürgern der EU/des EWR verarbeiten oder speichern, sicherstellen, dass angemessene Sicherheitskontrollen zum Schutz dieser Daten vorhanden sind. Dazu gehört auch, dass Dritte, die im Namen des KMU arbeiten, über angemessene Sicherheitsmaßnahmen verfügen.	s3-fähig bucket-server-side-encryption	Zum Schutz von Daten im Ruhezustand müssen Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon Simple Storage Service (Amazon S3)-Buckets aktiviert ist. Um eventuell vorhandene sensible Daten im Ruhezustand in Amazon-S3-Buckets zu schützen, muss die Verschlüsselung aktiviert sein.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
1_ENTWICKELN EINER GUTEN CYBERSICHERHEITSKULTUR: DENKEN SIE AN DEN DATENSCHUTZ	Gemäß der Allgemeinen Datenschutzverordnung1 der EU müssen alle SMEs , die personenbezogene Daten von Bürgern der EU/des EWR verarbeiten oder speichern, sicherstellen, dass angemessene Sicherheitskontrollen zum Schutz dieser Daten vorhanden sind. Dazu gehört auch, dass Dritte, die im Namen des KMU arbeiten, über angemessene Sicherheitsmaßnahmen verfügen.	s3- bucket-ssl-requests-only	Um Daten während der Übertragung zu schützen, stellen Sie sicher, dass Ihre Amazon Simple Storage Service (Amazon S3)-Buckets Anfragen zur Verwendung von Secure Socket Layer (SSL)-Buckets erfordern. Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
1_ENTWICKELN EINER GUTEN CYBERSICHERHEITSKULTUR: DENKEN SIE AN DEN DATENSCHUTZ	Gemäß der Allgemeinen Datenschutzverordnung1 der EU müssen alle SMEs , die personenbezogene Daten von Bürgern der EU/des EWR verarbeiten oder speichern, sicherstellen, dass angemessene Sicherheitskontrollen zum Schutz dieser Daten vorhanden sind. Dazu gehört auch, dass Dritte, die im Namen des KMU arbeiten, über angemessene Sicherheitsmaßnahmen verfügen.	sagemaker-endpoint-configuration-kms-schlüsselkonfiguriert	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass die Verschlüsselung mit dem AWS Key Management Service (AWS KMS) für Ihren Endpunkt aktiviert ist. SageMaker Da sensible Daten auf dem SageMaker Endgerät gespeichert werden können, sollten Sie die Verschlüsselung im Ruhezustand aktivieren, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
1_ENTWICKELN EINER GUTEN CYBERSICHERHEITSKULTUR: DENKEN SIE AN DEN DATENSCHUTZ	Gemäß der Allgemeinen Datenschutzverordnung1 der EU müssen alle SMEs , die personenbezogene Daten von Bürgern der EU/des EWR verarbeiten oder speichern, sicherstellen, dass angemessene Sicherheitskontrollen zum Schutz dieser Daten vorhanden sind. Dazu gehört auch, dass Dritte, die im Namen des KMU arbeiten, über angemessene Sicherheitsmaßnahmen verfügen.	sagemaker-notebook-instance-kms-schlüsselkonfiguriert	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass die Verschlüsselung mit dem AWS Key Management Service (AWS KMS) für Ihr Notebook aktiviert ist. SageMaker Da vertrauliche Daten im SageMaker Notebook gespeichert werden können, sollten Sie die Verschlüsselung im Ruhezustand aktivieren, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
1_ENTWICKELN EINER GUTEN CYBERSICHERHEITSKULTUR: DENKEN SIE AN DEN DATENSCHUTZ	Gemäß der Allgemeinen Datenschutzverordnung1 der EU müssen alle SMEs , die personenbezogene Daten von Bürgern der EU/des EWR verarbeiten oder speichern, sicherstellen, dass angemessene Sicherheitskontrollen zum Schutz dieser Daten vorhanden sind. Dazu gehört auch, dass Dritte, die im Namen des KMU arbeiten, über angemessene Sicherheitsmaßnahmen verfügen.	sagemaker-notebook-no-direct-Internetzugang	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass SageMaker Amazon-Notebooks keinen direkten Internetzugang zulassen. Indem Sie direkten Internetzugang blockieren, vermeiden Sie, dass unbefugte Benutzer auf sensible Daten zugreifen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
1_ENTWICKELN EINER GUTEN CYBERSICHERHEITSKULTUR: DENKEN SIE AN DEN DATENSCHUTZ	Gemäß der Allgemeinen Datenschutzverordnung1 der EU müssen alle SMEs , die personenbezogene Daten von Bürgern der EU/des EWR verarbeiten oder speichern, sicherstellen, dass angemessene Sicherheitskontrollen zum Schutz dieser Daten vorhanden sind. Dazu gehört auch, dass Dritte, die im Namen des KMU arbeiten, über angemessene Sicherheitsmaßnahmen verfügen.	sns-encrypted-kms	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass Ihre Amazon Simple Notification Service (Amazon SNS) -Themen mit dem AWS Key Management Service (AWS KMS) verschlüsselt werden müssen. Um eventuell vorhandene sensible Daten im Ruhezustand in veröffentlichten Nachrichten zu schützen, muss die Verschlüsselung von Daten im Ruhezustand aktiviert sein.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
1_ENTWICKELN EINER GUTEN CYBERSICHERHEITSKULTUR: DENKEN SIE AN DEN DATENSCHUTZ	Gemäß der Allgemeinen Datenschutzverordnung1 der EU müssen alle SMEs , die personenbezogene Daten von Bürgern der EU/des EWR verarbeiten oder speichern, sicherstellen, dass angemessene Sicherheitskontrollen zum Schutz dieser Daten vorhanden sind. Dazu gehört auch, dass Dritte, die im Namen des KMU arbeiten, über angemessene Sicherheitsmaßnahmen verfügen.	vpc-sg-open-only-to-authorized-ports	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass gemeinsame Ports für Amazon Elastic Compute Cloud (Amazon EC2) -Sicherheitsgruppen eingeschränkt sind. Wenn der Zugriff auf Ports nicht auf vertrauenswürdige Quellen beschränkt wird, kann dies zu Angriffen auf die Verfügbarkeit, Integrität und Vertraulichkeit von Systemen führen. Durch die Beschränkung des Zugriffs auf Ressourcen innerhalb einer Sicherheitsgruppe aus dem Internet (0.0.0.0/0) kann der Remote-Zugriff auf interne Systeme gesteuert werden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
2_ANGEMESSENE SCHULUNGEN ANBIETEN	Bieten Sie regelmäßige Schulungen zum Thema Cybersicherheit für alle Mitarbeiter an, damit sie die verschiedenen Cybersicherheitsbedrohungen erkennen und damit umgehen können. Diese Schulungen sollten auf KMU zugeschnitten sein und sich auf reale Situationen konzentrieren. Bieten Sie spezielle Cybersicherheitsschulungen für Mitarbeiter an, die für das Cybersicherheitsmanagement innerhalb des Unternehmens verantwortlich sind, damit sie die für ihre Arbeit erforderlichen Fähigkeiten und Kompetenzen besitzen.	security-awareness-program-exists(Prozessüberprüfung)	Etablieren und pflegen Sie ein Programm zur Förderung des Sicherheitsbewusstseins in Ihrer Organisation. Programme zur Förderung des Sicherheitsbewusstseins der Mitarbeiter vermitteln ihnen, wie sie ihre Organisation vor diversen Sicherheitsverletzungen oder Sicherheitsvorfällen schützen können.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
4_EINEN PLAN ZUR REAKTION AUF VORFÄLLE ENTWICKELN	Entwickeln Sie einen formellen Plan zur Reaktion auf Vorfälle, der klare und dokumentierte Richtlinien, Rollen und Zuständigkeiten enthält, damit auf alle Sicherheitsvorfälle rechtzeitig, professionell und angemessen reagiert wird. Suchen Sie nach Tools, die verdächtige Aktivitäten oder Sicherheitsverletzungen überwachen und Warnmeldungen ausgeben können, um umgehend auf Sicherheitsbedrohungen reagieren zu können.	response-plan-exists-maintained(Prozessüberprüfung)	Stellen Sie sicher, dass Vorfallreaktionspläne erstellt, verwaltet und an das verantwortliche Personal verteilt werden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
5_SICHERER ZUGRIFF AUF SYSTEME	Ermutigen Sie alle, eine Passphrase zu verwenden, d. h. eine Sammlung von mindestens drei zufälligen gebräuchlichen Wörtern, die zu einer Phrase kombiniert werden und eine sehr gute Kombination aus Einprägsamkeit und Sicherheit bieten. Wenn Sie sich für ein typisches Passwort entscheiden: - Erstellen Sie ein langes Passwort mit Klein- und Großbuchstaben und eventuell auch Zahlen und Sonderzeichen. - Vermeiden Sie offensichtliche Wörter wie „Passwort“, Buchstabenfolgen wie „abc“ oder Zahlenfolgen wie „123“. - Vermeiden Sie die Verwendung persönlicher Daten, die online zu finden sind. Außerdem	iam-password-policy	Die Identitäten und Anmeldeinformationen werden auf der Grundlage einer organisatorischen IAM-Passwortrichtlinie ausgestellt, verwaltet und verifiziert. Sie erfüllen oder übertreffen die Anforderungen von NIST SP 800-63 und dem Standard „Best Practices“ von AWS Foundational Security für die Passwortstärke. Mit dieser Regel können Sie optional RequireUppercaseCharacters (Wert für AWS grundlegende Sicherheitsbewährte Methoden: wahr), RequireLowercaseCharacters (Wert für bewährte Methoden für AWS grundlegende Sicherheit: wahr), RequireSymbols (Wert für bewährte Methoden für AWS grundlegende Sicherheit:

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	gilt, dass weder Passphrasen noch Passwörter nicht auch an anderer Stelle verwendet werden dürfen. - Geben Sie sie nicht an Kollegen weiter. - Aktivieren Sie die Multi-Faktor-Authentifizierung. - Verwenden Sie einen speziellen Passwort-Manager.		wahr), RequireNumbers (Wert für bewährte Methoden für AWS grundlegende Sicherheit: wahr), MinimumPasswordLength (Wert für bewährte Methoden für AWS grundlegende Sicherheit: 14), PasswordReusePrevention (Wert für bewährte Methoden für AWS grundlegende Sicherheit: 24) und MaxPasswordAge (Wert für bewährte Methoden für AWS grundlegende Sicherheit: 90) für Ihr IAM festlegen Kennwortrichtlinie. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
5_SICHERER ZUGRIFF AUF SYSTEME	Ermutigen Sie alle, eine Passphrase zu verwenden, d. h. eine Sammlung von mindestens drei zufälligen gebräuchlichen Wörtern, die zu einer Phrase kombiniert werden und eine sehr gute Kombination aus Einprägsamkeit und Sicherheit bieten. Wenn Sie sich für ein typisches Passwort entscheiden: - Erstellen Sie ein langes Passwort mit Klein- und Großbuchstaben und eventuell auch Zahlen und Sonderzeichen. - Vermeiden Sie offensichtliche Wörter wie „Passwort“, Buchstabenfolgen wie „abc“ oder Zahlenfolgen wie „123“. - Vermeiden Sie die Verwendung persönlicher Daten, die online zu finden sind. Außerdem	iam-user-mfa-enabled	Aktivieren Sie diese Regel, um den Zugriff auf Ressourcen in der AWS Cloud einzuschränken. Diese Regel sorgt dafür, dass die Multi-Faktor-Authentifizierung (MFA) für alle Benutzer aktiviert ist. MFA sorgt für eine weitere Schutzebene zusätzlich zu den Anmeldeinformationen. Reduzieren Sie Fälle von kompromittierten Konten, indem Sie MFA für Benutzer vorschreiben.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	gilt, dass weder Passphrasen noch Passwörter nicht auch an anderer Stelle verwendet werden dürfen. - Geben Sie sie nicht an Kollegen weiter. - Aktivieren Sie die Multi-Faktor-Authentifizierung. - Verwenden Sie einen speziellen Passwort-Manager.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
5_SICHERER ZUGRIFF AUF SYSTEME	Ermutigen Sie alle, eine Passphrase zu verwenden, d. h. eine Sammlung von mindestens drei zufälligen gebräuchlichen Wörtern, die zu einer Phrase kombiniert werden und eine sehr gute Kombination aus Einprägsamkeit und Sicherheit bieten. Wenn Sie sich für ein typisches Passwort entscheiden: - Erstellen Sie ein langes Passwort mit Klein- und Großbuchstaben und eventuell auch Zahlen und Sonderzeichen. - Vermeiden Sie offensichtliche Wörter wie „Passwort“, Buchstabenfolgen wie „abc“ oder Zahlenfolgen wie „123“. - Vermeiden Sie die Verwendung persönlicher Daten, die online zu finden sind. Außerdem	mfa-enabled-for-iam-Konsolenzugriff	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass MFA für alle AWS Identity and Access Management (IAM) -Benutzer aktiviert ist, die über ein Konsolenkennwort verfügen. MFA sorgt für eine weitere Schutzebene zusätzlich zu den Anmeldeinformationen. Indem Sie MFA für Benutzer vorschreiben, können Sie Fälle kompromittierter Konten reduzieren und verhindern, dass unbefugte Benutzer auf vertrauliche Daten zugreifen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	gilt, dass weder Passphrasen noch Passwörter nicht auch an anderer Stelle verwendet werden dürfen. - Geben Sie sie nicht an Kollegen weiter. - Aktivieren Sie die Multi-Faktor-Authentifizierung. - Verwenden Sie einen speziellen Passwort-Manager.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
5_SICHERER ZUGRIFF AUF SYSTEME	Ermutigen Sie alle, eine Passphrase zu verwenden, d. h. eine Sammlung von mindestens drei zufälligen gebräuchlichen Wörtern, die zu einer Phrase kombiniert werden und eine sehr gute Kombination aus Einprägsamkeit und Sicherheit bieten. Wenn Sie sich für ein typisches Passwort entscheiden: - Erstellen Sie ein langes Passwort mit Klein- und Großbuchstaben und eventuell auch Zahlen und Sonderzeichen. - Vermeiden Sie offensichtliche Wörter wie „Passwort“, Buchstabenfolgen wie „abc“ oder Zahlenfolgen wie „123“. - Vermeiden Sie die Verwendung persönlicher Daten, die online zu finden sind. Außerdem	root-account-hardware-mfa-aktiviert	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Hardware-MFA für den Root-Benutzer aktiviert ist. Der Stammbenutzer ist der AWS-Konto-Benutzer mit den meisten Berechtigungen. MFA sorgt für eine weitere Schutzebene zusätzlich zu den Anmeldeinformationen. Indem Sie MFA für den Root-Benutzer vorschreiben, können Sie die Anzahl AWS-Konten kompromittierter Benutzer reduzieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	gilt, dass weder Passphrasen noch Passwörter nicht auch an anderer Stelle verwendet werden dürfen. - Geben Sie sie nicht an Kollegen weiter. - Aktivieren Sie die Multi-Faktor-Authentifizierung. - Verwenden Sie einen speziellen Passwort-Manager.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
5_SICHERER ZUGRIFF AUF SYSTEME	Ermutigen Sie alle, eine Passphrase zu verwenden, d. h. eine Sammlung von mindestens drei zufälligen gebräuchlichen Wörtern, die zu einer Phrase kombiniert werden und eine sehr gute Kombination aus Einprägsamkeit und Sicherheit bieten. Wenn Sie sich für ein typisches Passwort entscheiden: - Erstellen Sie ein langes Passwort mit Klein- und Großbuchstaben und eventuell auch Zahlen und Sonderzeichen. - Vermeiden Sie offensichtliche Wörter wie „Passwort“, Buchstabenfolgen wie „abc“ oder Zahlenfolgen wie „123“. - Vermeiden Sie die Verwendung persönlicher Daten, die online zu finden sind. Außerdem	root-account-mfa-enabled	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass MFA für den Root-Benutzer aktiviert ist. Der Stammbenutzer ist der AWS-Konto-Benutzer mit den meisten Berechtigungen. MFA sorgt für eine weitere Schutzebene zusätzlich zu den Anmeldeinformationen. Indem Sie MFA für den Root-Benutzer vorschreiben, können Sie die Anzahl AWS-Konten kompromittierter Benutzer reduzieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	gilt, dass weder Passphrasen noch Passwörter nicht auch an anderer Stelle verwendet werden dürfen. - Geben Sie sie nicht an Kollegen weiter. - Aktivieren Sie die Multi-Faktor-Authentifizierung. - Verwenden Sie einen speziellen Passwort-Manager.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
6_GERÄTESICHERHEIT: SOFTWARE PATCHEN UND AKTUALISIEREN	Idealerweise verwenden Sie eine zentrale Plattform zur Verwaltung von Patches. Es wird dringend empfohlen für: - Regelmäßig die gesamte Software SMEs zu aktualisieren. - Aktivierung automatischer Updates, wann immer dies möglich ist. - Identifizierung von Software und Hardware, für die manuelle Updates erforderlich sind. - Berücksichtigung von Mobil- und IoT-Geräten.	ec2-check managedinstance-association-compliance-status	Verwenden Sie AWS Systems Manager Associations, um bei der Inventarisierung von Softwareplattformen und Anwendungen innerhalb eines Unternehmens zu helfen. AWS Systems Manager weist Ihren verwalteten Instanzen einen Konfigurationsstatus zu und ermöglicht es Ihnen, Basiswerte für Betriebssystem-Patch-Levels, Softwareinstallationen, Anwendungskonfigurationen und andere Details zu Ihrer Umgebung festzulegen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
6_GERÄTESICHERHEIT: SOFTWARE PATCHEN UND AKTUALISIEREN	Idealerweise verwenden Sie eine zentrale Plattform zur Verwaltung von Patches. Es wird dringend empfohlen für: - Regelmäßig die gesamte Software SMEs zu aktualisieren. - Aktivierung automatischer Updates, wann immer dies möglich ist. - Identifizierung von Software und Hardware, für die manuelle Updates erforderlich sind. - Berücksichtigung von Mobil- und IoT-Geräten.	ec2-check managedinstance-patch-compliance-status	Aktivieren Sie diese Regel, um bei der Identifizierung und Dokumentation von Sicherheitslücken in Amazon Elastic Compute Cloud (Amazon EC2) zu helfen. Die Regel prüft, ob die EC2 Amazon-Instance die Patch-Konformität im AWS Systems Manager gemäß den Richtlinien und Verfahren Ihrer Organisation einhält.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
6_GERÄTESICHERHEIT: SOFTWARE PATCHEN UND AKTUALISIEREN	Idealerweise verwenden Sie eine zentrale Plattform zur Verwaltung von Patches. Es wird dringend empfohlen: - Die gesamte Software des Unternehmens regelmäßig zu aktualisieren. SMEs - Aktivierung automatischer Updates, wann immer dies möglich ist. - Identifizierung von Software und Hardware, für die manuelle Updates erforderlich sind. - Berücksichtigung von Mobil- und IoT-Geräten.	ec2- -Manager instance-managed-by-systems	Eine Bestandsaufnahme der Softwareplattformen und Anwendungen innerhalb des Unternehmens ist möglich, indem Amazon Elastic Compute Cloud (Amazon EC2) - Instances mit AWS Systems Manager verwaltet werden. Verwenden Sie AWS Systems Manager, um detaillierte Systemkonfigurationen, Betriebssystem-Patch-Levels, Namen und Typ der Dienste, Softwareinstallationen, Anwendungsname, Herausgeber und Version sowie andere Details zu Ihrer Umgebung bereitzustellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
6_GERÄTESICHERHEIT: SOFTWARE PATCHEN UND AKTUALISIEREN	Idealerweise verwenden Sie eine zentrale Plattform zur Verwaltung von Patches. Es wird dringend empfohlen für SMEs : - Regelmäßig die gesamte Software zu aktualisieren. - Aktivierung automatischer Updates, wann immer dies möglich ist. - Identifizierung von Software und Hardware, für die manuelle Updates erforderlich sind. - Berücksichtigung von Mobil- und IoT-Geräten.	ecs-fargate-latest-platform-Version	Sicherheitsupdates und Patches werden automatisch für Ihre AWS Fargate-Aufgaben bereitgestellt. Wenn ein Sicherheitsproblem gefunden wird, das eine AWS Fargate-Plattformversion betrifft, AWS wird die Plattformversion gepatcht. Um Sie bei der Patchverwaltung Ihrer Amazon Elastic Container Service (ECS) - Aufgaben zu unterstützen, auf denen AWS Fargate ausgeführt wird, aktualisieren Sie Ihre eigenständigen Service-Aufgaben, sodass sie die neueste Plattformversion verwenden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
6_GERÄTESICHERHEIT: SOFTWARE PATCHEN UND AKTUALISIEREN	Idealerweise verwenden Sie eine zentrale Plattform zur Verwaltung von Patches. Es wird dringend empfohlen für SMEs : - Regelmäßig die gesamte Software zu aktualisieren. - Aktivierung automatischer Updates, wann immer dies möglich ist. - Identifizierung von Software und Hardware, für die manuelle Updates erforderlich sind. - Berücksichtigung von Mobil- und IoT-Geräten.	elastic-beanstalk-managed-updates-aktiviert	Durch die Aktivierung verwalteter Plattformupdates für eine Amazon-Elastic-Beanstalk-Umgebung wird sichergestellt, dass die aktuellen verfügbaren Plattform-Fixes, -Updates und -Features für die Umgebung installiert sind. Eine bewährte Methode zur Sicherung von Systemen besteht darin, stets die aktuellen Patches zu installieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
6_GERÄTESICHERHEIT: SOFTWARE PATCHEN UND AKTUALISIEREN	Idealerweise verwenden Sie eine zentrale Plattform zur Verwaltung von Patches. Es wird dringend empfohlen für SMEs : - Regelmäßig die gesamte Software zu aktualisieren. - Aktivierung automatischer Updates, wann immer dies möglich ist. - Identifizierung von Software und Hardware, für die manuelle Updates erforderlich sind. - Berücksichtigung von Mobil- und IoT-Geräten.	rds-automatic-minor-version-Upgrade-fähig	Aktivieren Sie automatische Unterversions-Upgrades auf Ihren Amazon-Relational-Database-Service (RDS)-Instances, um sicherzustellen, dass die aktuellen Updates für Unterversionen des Relational Database Management System (RDBMS) installiert sind, die Sicherheitspatches und Bugfixes enthalten können.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
6_GERÄTESICHERHEIT: SOFTWARE PATCHEN UND AKTUALISIEREN	Idealerweise verwenden Sie eine zentrale Plattform zur Verwaltung von Patches. Es wird dringend empfohlen für: - Regelmäßig die gesamte Software SMEs zu aktualisieren. - Aktivierung automatischer Updates, wann immer dies möglich ist. - Identifizierung von Software und Hardware, für die manuelle Updates erforderlich sind. - Berücksichtigung von Mobil- und IoT-Geräten.	redshift-cluster-maintenancesettings-check	Diese Regel stellt sicher, dass Amazon-Redshift-Cluster die bevorzugten Einstellungen für Ihre Organisation haben. Insbesondere sorgt sie dafür, dass Cluster bevorzugte Wartungsfenster und automatisierte Aufbewahrungsfristen für Snapshots für die Datenbank haben. Für diese Regel müssen Sie die festlegen allowVersionUpgrade. Der Standardwert ist „true“. Außerdem können Sie optional den Zeitraum preferredMaintenanceWindow (der Standardwert ist sa: 16:00 -sa: 16:30) und den automated SnapshotRetention Zeitraum (der Standardwert ist 1) festlegen. Die tatsächlichen Werte müssen den Richtlini

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			en Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
6_GERÄTESICHERHEIT: VERSCHLÜSSELUNG	Schützen Sie Daten, indem Sie sie verschlüsseln. SMEssollte sicherstellen, dass die auf Mobilgeräten wie Laptops, Smartphones und Tablets gespeicherten Daten verschlüsselt sind. Stellen Sie bei Daten, die über öffentliche Netzwerke wie Hotel- oder WiFi Flughafennetzwerke übertragen werden, sicher, dass die Daten verschlüsselt sind, indem Sie entweder ein virtuelles privates Netzwerk (VPN) verwenden oder über sichere Verbindungen mithilfe des SSL/TLS-Protokolls auf Websites zugreifen. Stellen Sie sicher, dass ihre eigenen Websites geeignete Verschlüsselungstechnologien verwenden, um Kundendaten während der	api-gw-cache-enabled-und verschlüsselt	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass die Verschlüsselung für den Cache Ihrer API-Gateway-Stufe aktiviert ist. Da für die API-Methode sensible Daten erfasst werden können, sollten Sie die Verschlüsselung von Daten im Ruhezustand aktivieren, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	Übertragung über das Internet zu schützen.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
6_GERÄTESICHERHEIT: VERSCHLÜSSELUNG	Schützen Sie Daten, indem Sie sie verschlüsseln. SMEssollte sicherstellen, dass die auf Mobilgeräten wie Laptops, Smartphones und Tablets gespeicherten Daten verschlüsselt sind. Stellen Sie bei Daten, die über öffentliche Netzwerke wie Hotel- oder WiFi Flughafennetzwerke übertragen werden, sicher, dass die Daten verschlüsselt sind, indem Sie entweder ein virtuelles privates Netzwerk (VPN) verwenden oder über sichere Verbindungen mithilfe des SSL/TLS-Protokolls auf Websites zugreifen. Stellen Sie sicher, dass ihre eigenen Websites geeignete Verschlüsselungstechnologien verwenden, um Kundendaten während der	backup-recovery-point-encrypted	Stellen Sie sicher, dass die Verschlüsselung für Ihre AWS Backup-Wiederherstellungspunkte aktiviert ist. Da sensible Daten auch im Ruhezustand vorhanden sein können, sollten Sie die Verschlüsselung im Ruhezustand aktivieren, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	Übertragung über das Internet zu schützen.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
6_GERÄTESICHERHEIT: VERSCHLÜSSELUNG	Schützen Sie Daten, indem Sie sie verschlüsseln. SMEssollte sicherstellen, dass die auf Mobilgeräten wie Laptops, Smartphones und Tablets gespeicherten Daten verschlüsselt sind. Stellen Sie bei Daten, die über öffentliche Netzwerke wie Hotel- oder WiFi Flughafennetzwerke übertragen werden, sicher, dass die Daten verschlüsselt sind, indem Sie entweder ein virtuelles privates Netzwerk (VPN) verwenden oder über sichere Verbindungen mithilfe des SSL/TLS-Protokolls auf Websites zugreifen. Stellen Sie sicher, dass ihre eigenen Websites geeignete Verschlüsselungstechnologien verwenden, um Kundendaten während der	cloud-trail-encryption-enabled	Da sensible Daten vorhanden sein können und um Daten im Ruhezustand zu schützen, sollten Sie sicherstellen, dass die Verschlüsselung für Ihre Pfade aktiviert ist. AWS CloudTrail

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	Übertragung über das Internet zu schützen.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
6_GERÄTESICHERHEIT: VERSCHLÜSSELUNG	Schützen Sie Daten, indem Sie sie verschlüsseln. SMEssollte sicherstellen, dass die auf Mobilgeräten wie Laptops, Smartphones und Tablets gespeicherten Daten verschlüsselt sind. Stellen Sie bei Daten, die über öffentliche Netzwerke wie Hotel- oder WiFi Flughafennetzwerke übertragen werden, sicher, dass die Daten verschlüsselt sind, indem Sie entweder ein virtuelles privates Netzwerk (VPN) verwenden oder über sichere Verbindungen mithilfe des SSL/TLS-Protokolls auf Websites zugreifen. Stellen Sie sicher, dass ihre eigenen Websites geeignete Verschlüsselungstechnologien verwenden, um Kundendaten während der	cloud-trail-log-file-Validierung aktiviert	Verwenden Sie die AWS CloudTrail Protokolldateivalidierung, um die Integrität von Protokollen zu überprüfen. CloudTrail Mithilfe der Protokolldateivalidierung kann festgestellt werden, ob eine Protokolldatei geändert oder gelöscht wurde oder ob sie nach der Übermittlung CloudTrail unverändert geblieben ist. Dieses Feature wurde mit dem Branchenstandard entsprechenden Algorithmen entwickelt: SHA-256 für die Hashfunktion und SHA-256 mit RSA für digitale Signaturen. Aus diesem Grund ist es rechnerisch unmöglich, CloudTrail Protokolldateien unbemerkt zu ändern, zu löschen oder zu fälschen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	Übertragung über das Internet zu schützen.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
6_GERÄTESICHERHEIT: VERSCHLÜSSELUNG	Schützen Sie Daten, indem Sie sie verschlüsseln. SMEssollte sicherstellen, dass die auf Mobilgeräten wie Laptops, Smartphones und Tablets gespeicherten Daten verschlüsselt sind. Stellen Sie bei Daten, die über öffentliche Netzwerke wie Hotel- oder WiFi Flughafennetzwerke übertragen werden, sicher, dass die Daten verschlüsselt sind, indem Sie entweder ein virtuelles privates Netzwerk (VPN) verwenden oder über sichere Verbindungen mithilfe des SSL/TLS-Protokolls auf Websites zugreifen. Stellen Sie sicher, dass ihre eigenen Websites geeignete Verschlüsselungstechnologien verwenden, um Kundendaten während der	cloudwatch-log-group-encrypted	Um sensible Daten im Speicher zu schützen, stellen Sie sicher, dass die Verschlüsselung für Ihre Amazon CloudWatch Log Groups aktiviert ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	Übertragung über das Internet zu schützen.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
6_GERÄTESICHERHEIT: VERSCHLÜSSELUNG	Schützen Sie Daten, indem Sie sie verschlüsseln. SMEssollte sicherstellen, dass die auf Mobilgeräten wie Laptops, Smartphones und Tablets gespeicherten Daten verschlüsselt sind. Stellen Sie bei Daten, die über öffentliche Netzwerke wie Hotel- oder WiFi Flughafennetzwerke übertragen werden, sicher, dass die Daten verschlüsselt sind, indem Sie entweder ein virtuelles privates Netzwerk (VPN) verwenden oder über sichere Verbindungen mithilfe des SSL/TLS-Protokolls auf Websites zugreifen. Stellen Sie sicher, dass ihre eigenen Websites geeignete Verschlüsselungstechnologien verwenden, um Kundendaten während der	codebuild-project-artifact-encryption	Um sensible Daten im Ruhezustand zu schützen, sollten Sie sicherstellen, dass die Verschlüsselung für Ihre Artefakte aktiviert ist. AWS CodeBuild

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	Übertragung über das Internet zu schützen.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
6_GERÄTESICHERHEIT: VERSCHLÜSSELUNG	Schützen Sie Daten, indem Sie sie verschlüsseln. SMEssollte sicherstellen, dass die auf Mobilgeräten wie Laptops, Smartphones und Tablets gespeicherten Daten verschlüsselt sind. Stellen Sie bei Daten, die über öffentliche Netzwerke wie Hotel- oder WiFi Flughafennetzwerke übertragen werden, sicher, dass die Daten verschlüsselt sind, indem Sie entweder ein virtuelles privates Netzwerk (VPN) verwenden oder über sichere Verbindungen mithilfe des SSL/TLS-Protokolls auf Websites zugreifen. Stellen Sie sicher, dass ihre eigenen Websites geeignete Verschlüsselungstechnologien verwenden, um Kundendaten während der	codebuild-project-sVerschlüsselung mit 3 Protokollen	Um sensible Daten im Speicher zu schützen, stellen Sie sicher, dass die Verschlüsselung für Ihre in Amazon S3 gespeicherten AWS CodeBuild Protokolle aktiviert ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	Übertragung über das Internet zu schützen.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
6_GERÄTESICHERHEIT: VERSCHLÜSSELUNG	Schützen Sie Daten, indem Sie sie verschlüsseln. SMEssollte sicherstellen, dass die auf Mobilgeräten wie Laptops, Smartphones und Tablets gespeicherten Daten verschlüsselt sind. Stellen Sie bei Daten, die über öffentliche Netzwerke wie Hotel- oder WiFi Flughafennetzwerke übertragen werden, sicher, dass die Daten verschlüsselt sind, indem Sie entweder ein virtuelles privates Netzwerk (VPN) verwenden oder über sichere Verbindungen mithilfe des SSL/TLS-Protokolls auf Websites zugreifen. Stellen Sie sicher, dass ihre eigenen Websites geeignete Verschlüsselungstechnologien verwenden, um Kundendaten während der	dynamodb-table-encrypted-kms	Stellen Sie sicher, dass die Verschlüsselung für Ihre Amazon-DynamoDB-Tabellen aktiviert ist. Um eventuell vorhandene sensible Daten im Ruhezustand in diesen Tabellen zu schützen, müssen Sie die Verschlüsselung von Daten im Ruhezustand aktivieren. Standardmäßig werden DynamoDB-Tabellen mit einem AWS eigenen Kundenhauptschlüssel (CMK) verschlüsselt.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	Übertragung über das Internet zu schützen.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
6_GERÄTESICHERHEIT: VERSCHLÜSSELUNG	Schützen Sie Daten, indem Sie sie verschlüsseln. SMEssollte sicherstellen, dass die auf Mobilgeräten wie Laptops, Smartphones und Tablets gespeicherten Daten verschlüsselt sind. Stellen Sie bei Daten, die über öffentliche Netzwerke wie Hotel- oder WiFi Flughafennetzwerke übertragen werden, sicher, dass die Daten verschlüsselt sind, indem Sie entweder ein virtuelles privates Netzwerk (VPN) verwenden oder über sichere Verbindungen mithilfe des SSL/TLS-Protokolls auf Websites zugreifen. Stellen Sie sicher, dass ihre eigenen Websites geeignete Verschlüsselungstechnologien verwenden, um Kundendaten während der	ec-2 ebs-encryption-by-default	Zum Schutz von Daten im Ruhezustand müssen Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon Elastic Block Store (Amazon EBS)-Volumes aktiviert ist. Da sensible Daten auch im Ruhezustand vorhanden sein können, sollten Sie die Verschlüsselung im Ruhezustand aktivieren, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	Übertragung über das Internet zu schützen.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
6_GERÄTESICHERHEIT: VERSCHLÜSSELUNG	Schützen Sie Daten, indem Sie sie verschlüsseln. SMEssollte sicherstellen, dass die auf Mobilgeräten wie Laptops, Smartphones und Tablets gespeicherten Daten verschlüsselt sind. Stellen Sie bei Daten, die über öffentliche Netzwerke wie Hotel- oder WiFi Flughafennetzwerke übertragen werden, sicher, dass die Daten verschlüsselt sind, indem Sie entweder ein virtuelles privates Netzwerk (VPN) verwenden oder über sichere Verbindungen mithilfe des SSL/TLS-Protokolls auf Websites zugreifen. Stellen Sie sicher, dass ihre eigenen Websites geeignete Verschlüsselungstechnologien verwenden, um Kundendaten während der	efs-encrypted-check	Aktivieren Sie die Verschlüsselung für Ihr Amazon Elastic File System (EFS), um eventuell vorhandene sensible Daten sowie Daten im Ruhezustand zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	Übertragung über das Internet zu schützen.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
6_GERÄTESICHERHEIT: VERSCHLÜSSELUNG	Schützen Sie Daten, indem Sie sie verschlüsseln. SMEssollte sicherstellen, dass die auf Mobilgeräten wie Laptops, Smartphones und Tablets gespeicherten Daten verschlüsselt sind. Stellen Sie bei Daten, die über öffentliche Netzwerke wie Hotel- oder WiFi Flughafennetzwerke übertragen werden, sicher, dass die Daten verschlüsselt sind, indem Sie entweder ein virtuelles privates Netzwerk (VPN) verwenden oder über sichere Verbindungen mithilfe des SSL/TLS-Protokolls auf Websites zugreifen. Stellen Sie sicher, dass ihre eigenen Websites geeignete Verschlüsselungstechnologien verwenden, um Kundendaten während der	elasticsearch-encrypted-at-rest	Aktivieren Sie die Verschlüsselung für Ihre Domains im Amazon Elasticsearch Service (Amazon ES), um eventuell vorhandene sensible Daten sowie Daten im Ruhezustand zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	Übertragung über das Internet zu schützen.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
6_GERÄTESICHERHEIT: VERSCHLÜSSELUNG	Schützen Sie Daten, indem Sie sie verschlüsseln. SMEssollte sicherstellen, dass die auf Mobilgeräten wie Laptops, Smartphones und Tablets gespeicherten Daten verschlüsselt sind. Stellen Sie bei Daten, die über öffentliche Netzwerke wie Hotel- oder WiFi Flughafennetzwerke übertragen werden, sicher, dass die Daten verschlüsselt sind, indem Sie entweder ein virtuelles privates Netzwerk (VPN) verwenden oder über sichere Verbindungen mithilfe des SSL/TLS-Protokolls auf Websites zugreifen. Stellen Sie sicher, dass ihre eigenen Websites geeignete Verschlüsselungstechnologien verwenden, um Kundendaten während der	elb-acm-certificate-required	Zum Schutz von eventuell vorhandenen sensiblen Daten sowie von Daten während der Übertragung muss die Verschlüsselung für Ihr Elastic Load Balancing aktiviert sein. Verwenden Sie AWS Certificate Manager, um öffentliche und private SSL/TLS-Zertifikate mit AWS Diensten und internen Ressourcen zu verwalten, bereitzustellen und bereitzustellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	Übertragung über das Internet zu schützen.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
6_GERÄTESICHERHEIT: VERSCHLÜSSELUNG	Schützen Sie Daten, indem Sie sie verschlüsseln. SMEssollte sicherstellen, dass die auf Mobilgeräten wie Laptops, Smartphones und Tablets gespeicherten Daten verschlüsselt sind. Stellen Sie bei Daten, die über öffentliche Netzwerke wie Hotel- oder WiFi Flughafennetzwerke übertragen werden, sicher, dass die Daten verschlüsselt sind, indem Sie entweder ein virtuelles privates Netzwerk (VPN) verwenden oder über sichere Verbindungen mithilfe des SSL/TLS-Protokolls auf Websites zugreifen. Stellen Sie sicher, dass ihre eigenen Websites geeignete Verschlüsselungstechnologien verwenden, um Kundendaten während der	elbv-2 acm-certificate-required	Zum Schutz von eventuell vorhandenen sensiblen Daten sowie von Daten während der Übertragung muss die Verschlüsselung für Ihr Elastic Load Balancing aktiviert sein. Verwenden Sie AWS Certificate Manager, um öffentliche und private SSL/TLS-Zertifikate mit AWS Diensten und internen Ressourcen zu verwalten, bereitzustellen und bereitzustellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	Übertragung über das Internet zu schützen.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
6_GERÄTESICHERHEIT: VERSCHLÜSSELUNG	Schützen Sie Daten, indem Sie sie verschlüsseln. SMEssollte sicherstellen, dass die auf Mobilgeräten wie Laptops, Smartphones und Tablets gespeicherten Daten verschlüsselt sind. Stellen Sie bei Daten, die über öffentliche Netzwerke wie Hotel- oder WiFi Flughafennetzwerke übertragen werden, sicher, dass die Daten verschlüsselt sind, indem Sie entweder ein virtuelles privates Netzwerk (VPN) verwenden oder über sichere Verbindungen mithilfe des SSL/TLS-Protokolls auf Websites zugreifen. Stellen Sie sicher, dass ihre eigenen Websites geeignete Verschlüsselungstechnologien verwenden, um Kundendaten während der	opensearch-encrypted-at-rest	Da sensible Daten vorhanden sein können und um Daten im Ruhezustand zu schützen, sollten Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon OpenSearch Service-Domains aktiviert ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	Übertragung über das Internet zu schützen.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
6_GERÄTESICHERHEIT: VERSCHLÜSSELUNG	Schützen Sie Daten, indem Sie sie verschlüsseln. SMEssollte sicherstellen, dass die auf Mobilgeräten wie Laptops, Smartphones und Tablets gespeicherten Daten verschlüsselt sind. Stellen Sie bei Daten, die über öffentliche Netzwerke wie Hotel- oder WiFi Flughafennetzwerke übertragen werden, sicher, dass die Daten verschlüsselt sind, indem Sie entweder ein virtuelles privates Netzwerk (VPN) verwenden oder über sichere Verbindungen mithilfe des SSL/TLS-Protokolls auf Websites zugreifen. Stellen Sie sicher, dass ihre eigenen Websites geeignete Verschlüsselungstechnologien verwenden, um Kundendaten während der	elasticsearch-node-to-node-Verschlüsselungsprüfung	Stellen Sie sicher, dass die node-to-node Verschlüsselung für Amazon Elasticsearch Service aktiviert ist. Node-to-nodeVerschlüsselung ermöglicht die TLS 1.2-Verschlüsselung für die gesamte Kommunikation innerhalb der Amazon Virtual Private Cloud (Amazon VPC). Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	Übertragung über das Internet zu schützen.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
6_GERÄTESICHERHEIT: VERSCHLÜSSELUNG	Schützen Sie Daten, indem Sie sie verschlüsseln. SMEssollte sicherstellen, dass die auf Mobilgeräten wie Laptops, Smartphones und Tablets gespeicherten Daten verschlüsselt sind. Stellen Sie bei Daten, die über öffentliche Netzwerke wie Hotel- oder WiFi Flughafennetzwerke übertragen werden, sicher, dass die Daten verschlüsselt sind, indem Sie entweder ein virtuelles privates Netzwerk (VPN) verwenden oder über sichere Verbindungen mithilfe des SSL/TLS-Protokolls auf Websites zugreifen. Stellen Sie sicher, dass ihre eigenen Websites geeignete Verschlüsselungstechnologien verwenden, um Kundendaten während der	opensearch-node-to-node-Verschlüsselungsprüfung	Stellen Sie sicher, dass die node-to-node Verschlüsselung für Amazon OpenSearch Service aktiviert ist. Node-to-nodeVerschlüsselung ermöglicht die TLS 1.2-Verschlüsselung für die gesamte Kommunikation innerhalb der Amazon Virtual Private Cloud (Amazon VPC). Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	Übertragung über das Internet zu schützen.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
6_GERÄTESICHERHEIT: VERSCHLÜSSELUNG	Schützen Sie Daten, indem Sie sie verschlüsseln. SMEssollte sicherstellen, dass die auf Mobilgeräten wie Laptops, Smartphones und Tablets gespeicherten Daten verschlüsselt sind. Stellen Sie bei Daten, die über öffentliche Netzwerke wie Hotel- oder WiFi Flughafennetzwerke übertragen werden, sicher, dass die Daten verschlüsselt sind, indem Sie entweder ein virtuelles privates Netzwerk (VPN) verwenden oder über sichere Verbindungen mithilfe des SSL/TLS-Protokolls auf Websites zugreifen. Stellen Sie sicher, dass ihre eigenen Websites geeignete Verschlüsselungstechnologien verwenden, um Kundendaten während der	opensearch-https-required	Da sensible Daten existieren können und um Daten während der Übertragung zu schützen, sollten Sie sicherstellen, dass HTTPS für Verbindungen zu Ihren Amazon OpenSearch Service-Domains aktiviert ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	Übertragung über das Internet zu schützen.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
6_GERÄTESICHERHEIT: VERSCHLÜSSELUNG	Schützen Sie Daten, indem Sie sie verschlüsseln. SMEssollte sicherstellen, dass die auf Mobilgeräten wie Laptops, Smartphones und Tablets gespeicherten Daten verschlüsselt sind. Stellen Sie bei Daten, die über öffentliche Netzwerke wie Hotel- oder WiFi Flughafennetzwerke übertragen werden, sicher, dass die Daten verschlüsselt sind, indem Sie entweder ein virtuelles privates Netzwerk (VPN) verwenden oder über sichere Verbindungen mithilfe des SSL/TLS-Protokolls auf Websites zugreifen. Stellen Sie sicher, dass ihre eigenen Websites geeignete Verschlüsselungstechnologien verwenden, um Kundendaten während der	secretsmanager-using-cmk	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass die Verschlüsselung mit dem AWS Key Management Service (AWS KMS) für AWS Secrets Manager aktiviert ist. Aktivieren Sie die Verschlüsselung von Daten im Ruhezustand, um eventuell vorhandene sensible Daten im Ruhezustand im Secrets Manager zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	Übertragung über das Internet zu schützen.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
6_GERÄTESICHERHEIT: VERSCHLÜSSELUNG	Schützen Sie Daten, indem Sie sie verschlüsseln. SMEssollte sicherstellen, dass die auf Mobilgeräten wie Laptops, Smartphones und Tablets gespeicherten Daten verschlüsselt sind. Stellen Sie bei Daten, die über öffentliche Netzwerke wie Hotel- oder WiFi Flughafennetzwerke übertragen werden, sicher, dass die Daten verschlüsselt sind, indem Sie entweder ein virtuelles privates Netzwerk (VPN) verwenden oder über sichere Verbindungen mithilfe des SSL/TLS-Protokolls auf Websites zugreifen. Stellen Sie sicher, dass ihre eigenen Websites geeignete Verschlüsselungstechnologien verwenden, um Kundendaten während der	encrypted-volumes	Aktivieren Sie die Verschlüsselung für Ihre Amazon-Elastic-Block-Store (Amazon-EBS)-Volumes, um eventuell vorhandene sensible Daten sowie Daten im Ruhezustand zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	Übertragung über das Internet zu schützen.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
6_GERÄTESICHERHEIT: VERSCHLÜSSELUNG	Schützen Sie Daten, indem Sie sie verschlüsseln. SMEssollte sicherstellen, dass die auf Mobilgeräten wie Laptops, Smartphones und Tablets gespeicherten Daten verschlüsselt sind. Stellen Sie bei Daten, die über öffentliche Netzwerke wie Hotel- oder WiFi Flughafennetzwerke übertragen werden, sicher, dass die Daten verschlüsselt sind, indem Sie entweder ein virtuelles privates Netzwerk (VPN) verwenden oder über sichere Verbindungen mithilfe des SSL/TLS-Protokolls auf Websites zugreifen. Stellen Sie sicher, dass ihre eigenen Websites geeignete Verschlüsselungstechnologien verwenden, um Kundendaten während der	kinesis-stream-encrypted	Aktivieren Sie die Verschlüsselung für Ihre Amazon-Kinesis-Streams, um eventuell vorhandene sensible Daten sowie Daten im Ruhezustand zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	Übertragung über das Internet zu schützen.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
6_GERÄTESICHERHEIT: VERSCHLÜSSELUNG	Schützen Sie Daten, indem Sie sie verschlüsseln. SMEssollte sicherstellen, dass die auf Mobilgeräten wie Laptops, Smartphones und Tablets gespeicherten Daten verschlüsselt sind. Stellen Sie bei Daten, die über öffentliche Netzwerke wie Hotel- oder WiFi Flughafennetzwerke übertragen werden, sicher, dass die Daten verschlüsselt sind, indem Sie entweder ein virtuelles privates Netzwerk (VPN) verwenden oder über sichere Verbindungen mithilfe des SSL/TLS-Protokolls auf Websites zugreifen. Stellen Sie sicher, dass ihre eigenen Websites geeignete Verschlüsselungstechnologien verwenden, um Kundendaten während der	rds-snapshot-encrypted	Stellen Sie sicher, dass die Verschlüsselung für Ihre Amazon Relational Database Service (Amazon RDS)-Snapshots aktiviert ist. Da sensible Daten auch im Ruhezustand vorhanden sein können, sollten Sie die Verschlüsselung im Ruhezustand aktivieren, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	Übertragung über das Internet zu schützen.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
6_GERÄTESICHERHEIT: VERSCHLÜSSELUNG	Schützen Sie Daten, indem Sie sie verschlüsseln. SMEssollte sicherstellen, dass die auf Mobilgeräten wie Laptops, Smartphones und Tablets gespeicherten Daten verschlüsselt sind. Stellen Sie bei Daten, die über öffentliche Netzwerke wie Hotel- oder WiFi Flughafennetzwerke übertragen werden, sicher, dass die Daten verschlüsselt sind, indem Sie entweder ein virtuelles privates Netzwerk (VPN) verwenden oder über sichere Verbindungen mithilfe des SSL/TLS-Protokolls auf Websites zugreifen. Stellen Sie sicher, dass ihre eigenen Websites geeignete Verschlüsselungstechnologien verwenden, um Kundendaten während der	rds-storage-encrypted	Zum Schutz von Daten im Ruhezustand müssen Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon Relational Database Service (Amazon RDS)-Instances aktiviert ist. Um eventuell vorhandene sensible Daten im Ruhezustand in Amazon-RDS-Instances zu schützen, muss die Verschlüsselung von Daten im Ruhezustand aktiviert sein.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	Übertragung über das Internet zu schützen.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
6_GERÄTESICHERHEIT: VERSCHLÜSSELUNG	Schützen Sie Daten, indem Sie sie verschlüsseln. SMEssollte sicherstellen, dass die auf Mobilgeräten wie Laptops, Smartphones und Tablets gespeicherten Daten verschlüsselt sind. Stellen Sie bei Daten, die über öffentliche Netzwerke wie Hotel- oder WiFi Flughafennetzwerke übertragen werden, sicher, dass die Daten verschlüsselt sind, indem Sie entweder ein virtuelles privates Netzwerk (VPN) verwenden oder über sichere Verbindungen mithilfe des SSL/TLS-Protokolls auf Websites zugreifen. Stellen Sie sicher, dass ihre eigenen Websites geeignete Verschlüsselungstechnologien verwenden, um Kundendaten während der	s3-fähig bucket-server-side-encryption	Zum Schutz von Daten im Ruhezustand müssen Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon Simple Storage Service (Amazon S3)-Buckets aktiviert ist. Um eventuell vorhandene sensible Daten im Ruhezustand in Amazon-S3-Buckets zu schützen, muss die Verschlüsselung aktiviert sein.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	Übertragung über das Internet zu schützen.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
6_GERÄTESICHERHEIT: VERSCHLÜSSELUNG	Schützen Sie Daten, indem Sie sie verschlüsseln. SMEssollte sicherstellen, dass die auf Mobilgeräten wie Laptops, Smartphones und Tablets gespeicherten Daten verschlüsselt sind. Stellen Sie bei Daten, die über öffentliche Netzwerke wie Hotel- oder WiFi Flughafennetzwerke übertragen werden, sicher, dass die Daten verschlüsselt sind, indem Sie entweder ein virtuelles privates Netzwerk (VPN) verwenden oder über sichere Verbindungen mithilfe des SSL/TLS-Protokolls auf Websites zugreifen. Stellen Sie sicher, dass ihre eigenen Websites geeignete Verschlüsselungstechnologien verwenden, um Kundendaten während der	sns-encrypted-kms	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass Ihre Amazon Simple Notification Service (Amazon SNS) -Themen mit dem AWS Key Management Service (AWS KMS) verschlüsselt werden müssen. Um eventuell vorhandene sensible Daten im Ruhezustand in veröffentlichten Nachrichten zu schützen, muss die Verschlüsselung von Daten im Ruhezustand aktiviert sein.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	Übertragung über das Internet zu schützen.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
6_GERÄTESICHERHEIT: VERSCHLÜSSELUNG	Schützen Sie Daten, indem Sie sie verschlüsseln. SMEssollte sicherstellen, dass die auf Mobilgeräten wie Laptops, Smartphones und Tablets gespeicherten Daten verschlüsselt sind. Stellen Sie bei Daten, die über öffentliche Netzwerke wie Hotel- oder WiFi Flughafennetzwerke übertragen werden, sicher, dass die Daten verschlüsselt sind, indem Sie entweder ein virtuelles privates Netzwerk (VPN) verwenden oder über sichere Verbindungen mithilfe des SSL/TLS-Protokolls auf Websites zugreifen. Stellen Sie sicher, dass ihre eigenen Websites geeignete Verschlüsselungstechnologien verwenden, um Kundendaten während der	redshift-cluster-kms-enabled	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass die Verschlüsselung mit AWS Key Management Service (AWS KMS) für Ihren Amazon Redshift Redshift-Cluster aktiviert ist. Um eventuell vorhandene sensible Daten im Ruhezustand in Redshift-Clustern zu schützen, muss die Verschlüsselung von Daten im Ruhezustand aktiviert sein.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	Übertragung über das Internet zu schützen.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
6_GERÄTESICHERHEIT: VERSCHLÜSSELUNG	Schützen Sie Daten, indem Sie sie verschlüsseln. SMEssollte sicherstellen, dass die auf Mobilgeräten wie Laptops, Smartphones und Tablets gespeicherten Daten verschlüsselt sind. Stellen Sie bei Daten, die über öffentliche Netzwerke wie Hotel- oder WiFi Flughafennetzwerke übertragen werden, sicher, dass die Daten verschlüsselt sind, indem Sie entweder ein virtuelles privates Netzwerk (VPN) verwenden oder über sichere Verbindungen mithilfe des SSL/TLS-Protokolls auf Websites zugreifen. Stellen Sie sicher, dass ihre eigenen Websites geeignete Verschlüsselungstechnologien verwenden, um Kundendaten während der	s3- default-encryption-kms	Stellen Sie sicher, dass die Verschlüsselung für Ihre Amazon Simple Storage Service (Amazon S3)-Buckets aktiviert ist. Um eventuell vorhandene sensible Daten im Ruhezustand in einem Amazon-S3-Bucket zu schützen, muss die Verschlüsselung aktiviert sein.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	Übertragung über das Internet zu schützen.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
6_GERÄTESICHERHEIT: VERSCHLÜSSELUNG	Schützen Sie Daten, indem Sie sie verschlüsseln. SMEssollte sicherstellen, dass die auf Mobilgeräten wie Laptops, Smartphones und Tablets gespeicherten Daten verschlüsselt sind. Stellen Sie bei Daten, die über öffentliche Netzwerke wie Hotel- oder WiFi Flughafennetzwerke übertragen werden, sicher, dass die Daten verschlüsselt sind, indem Sie entweder ein virtuelles privates Netzwerk (VPN) verwenden oder über sichere Verbindungen mithilfe des SSL/TLS-Protokolls auf Websites zugreifen. Stellen Sie sicher, dass ihre eigenen Websites geeignete Verschlüsselungstechnologien verwenden, um Kundendaten während der	sagemaker-endpoint-configuration-kms-schlüsselkonfiguriert	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass die Verschlüsselung mit dem AWS Key Management Service (AWS KMS) für Ihren Endpunkt aktiviert ist. SageMaker Dasensible Daten auf dem SageMaker Endgerät gespeichert werden können, sollten Sie die Verschlüsselung im Ruhezustand aktivieren, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	Übertragung über das Internet zu schützen.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
6_GERÄTESICHERHEIT: VERSCHLÜSSELUNG	Schützen Sie Daten, indem Sie sie verschlüsseln. SMEssollte sicherstellen, dass die auf Mobilgeräten wie Laptops, Smartphones und Tablets gespeicherten Daten verschlüsselt sind. Stellen Sie bei Daten, die über öffentliche Netzwerke wie Hotel- oder WiFi Flughafennetzwerke übertragen werden, sicher, dass die Daten verschlüsselt sind, indem Sie entweder ein virtuelles privates Netzwerk (VPN) verwenden oder über sichere Verbindungen mithilfe des SSL/TLS-Protokolls auf Websites zugreifen. Stellen Sie sicher, dass ihre eigenen Websites geeignete Verschlüsselungstechnologien verwenden, um Kundendaten während der	sagemaker-notebook-instance-kms-schlüsselkonfiguriert	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass die Verschlüsselung mit dem AWS Key Management Service (AWS KMS) für Ihr Notebook aktiviert ist. SageMaker Da vertrauliche Daten im SageMaker Notebook gespeichert werden können, sollten Sie die Verschlüsselung im Ruhezustand aktivieren, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	Übertragung über das Internet zu schützen.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
6_GERÄTESICHERHEIT: VERSCHLÜSSELUNG	Schützen Sie Daten, indem Sie sie verschlüsseln. SMEssollte sicherstellen, dass die auf Mobilgeräten wie Laptops, Smartphones und Tablets gespeicherten Daten verschlüsselt sind. Stellen Sie bei Daten, die über öffentliche Netzwerke wie Hotel- oder WiFi Flughafennetzwerke übertragen werden, sicher, dass die Daten verschlüsselt sind, indem Sie entweder ein virtuelles privates Netzwerk (VPN) verwenden oder über sichere Verbindungen mithilfe des SSL/TLS-Protokolls auf Websites zugreifen. Stellen Sie sicher, dass ihre eigenen Websites geeignete Verschlüsselungstechnologien verwenden, um Kundendaten während der	alb-http-to-https-Umleitungsprüfung	Um Daten während der Übertragung zu schützen, stellen Sie sicher, dass Ihr Application Load Balancer unverschlüsselte HTTP-Anfragen automatisch an HTTPS umleitet. Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	Übertragung über das Internet zu schützen.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
6_GERÄTESICHERHEIT: VERSCHLÜSSELUNG	Schützen Sie Daten, indem Sie sie verschlüsseln. SMEssollte sicherstellen, dass die auf Mobilgeräten wie Laptops, Smartphones und Tablets gespeicherten Daten verschlüsselt sind. Stellen Sie bei Daten, die über öffentliche Netzwerke wie Hotel- oder WiFi Flughafennetzwerke übertragen werden, sicher, dass die Daten verschlüsselt sind, indem Sie entweder ein virtuelles privates Netzwerk (VPN) verwenden oder über sichere Verbindungen mithilfe des SSL/TLS-Protokolls auf Websites zugreifen. Stellen Sie sicher, dass ihre eigenen Websites geeignete Verschlüsselungstechnologien verwenden, um Kundendaten während der	elb-tls-https-listeners-nur	Stellen Sie sicher, dass Ihre Elastic Load Balancer (ELBs) mit SSL- oder HTTPS-Listenern konfiguriert sind. Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	Übertragung über das Internet zu schützen.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
6_GERÄTESICHERHEIT: VERSCHLÜSSELUNG	Schützen Sie Daten, indem Sie sie verschlüsseln. SMEssollte sicherstellen, dass die auf Mobilgeräten wie Laptops, Smartphones und Tablets gespeicherten Daten verschlüsselt sind. Stellen Sie bei Daten, die über öffentliche Netzwerke wie Hotel- oder WiFi Flughafennetzwerke übertragen werden, sicher, dass die Daten verschlüsselt sind, indem Sie entweder ein virtuelles privates Netzwerk (VPN) verwenden oder über sichere Verbindungen mithilfe des SSL/TLS-Protokolls auf Websites zugreifen. Stellen Sie sicher, dass ihre eigenen Websites geeignete Verschlüsselungstechnologien verwenden, um Kundendaten während der	api-gw-ssl-enabled	Stellen Sie sicher, dass die REST-API-Stufen von Amazon API Gateway mit SSL-Zertifikaten konfiguriert sind, damit Backend-Systeme überprüfen können, ob Anforderungen von API Gateway stammen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	Übertragung über das Internet zu schützen.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
6_GERÄTESICHERHEIT: VERSCHLÜSSELUNG	Schützen Sie Daten, indem Sie sie verschlüsseln. SMEssollte sicherstellen, dass die auf Mobilgeräten wie Laptops, Smartphones und Tablets gespeicherten Daten verschlüsselt sind. Stellen Sie bei Daten, die über öffentliche Netzwerke wie Hotel- oder WiFi Flughafennetzwerke übertragen werden, sicher, dass die Daten verschlüsselt sind, indem Sie entweder ein virtuelles privates Netzwerk (VPN) verwenden oder über sichere Verbindungen mithilfe des SSL/TLS-Protokolls auf Websites zugreifen. Stellen Sie sicher, dass ihre eigenen Websites geeignete Verschlüsselungstechnologien verwenden, um Kundendaten während der	redshift-require-tls-ssl	Stellen Sie sicher, dass Ihre Amazon-Redshift-Cluster eine TLS/SSL-Verschlüsselung erfordern, um eine Verbindung zu SQL-Clients herzustellen. Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	Übertragung über das Internet zu schützen.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
6_GERÄTESICHERHEIT: VERSCHLÜSSELUNG	Schützen Sie Daten, indem Sie sie verschlüsseln. SMEssollte sicherstellen, dass die auf Mobilgeräten wie Laptops, Smartphones und Tablets gespeicherten Daten verschlüsselt sind. Stellen Sie bei Daten, die über öffentliche Netzwerke wie Hotel- oder WiFi Flughafennetzwerke übertragen werden, sicher, dass die Daten verschlüsselt sind, indem Sie entweder ein virtuelles privates Netzwerk (VPN) verwenden oder über sichere Verbindungen mithilfe des SSL/TLS-Protokolls auf Websites zugreifen. Stellen Sie sicher, dass ihre eigenen Websites geeignete Verschlüsselungstechnologien verwenden, um Kundendaten während der	s3- bucket-ssl-requests-only	Um Daten während der Übertragung zu schützen, stellen Sie sicher, dass Ihre Amazon Simple Storage Service (Amazon S3)-Buckets Anfragen zur Verwendung von Secure Socket Layer (SSL)-Buckets erfordern. Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	Übertragung über das Internet zu schützen.		
7_NETZWERKSCHUTZ: EINSATZ VON FIREWALLS	Firewalls verwalten den ein- und ausgehenden Datenverkehr in ein Netzwerk und sind ein wichtiges Instrument zum Schutz von SMEs Systemen. Firewalls sollten zum Schutz aller kritischen Systeme eingesetzt werden, insbesondere sollte eine Firewall gerichtet werden, um das Netzwerk von KMU vor Gefahren aus dem Internet zu schützen.	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) Security Groups können bei der Verwaltung des Netzwerkzugriffs helfen, indem sie eine statusbehaftete Filterung von eingehendem und ausgehendem Netzwerkverkehr zu Ressourcen bereitstellen. AWS Wenn Sie eingehenden (oder entfernten) Datenverkehr von 0.0.0.0/0 bis Port 22 auf Ihren Ressourcen nicht zulassen, können Sie den Remote-Zugriff einschränken.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
7_NETZWERKSCHUTZ: EINSATZ VON FIREWALLS	Firewalls verwalten den Datenverkehr, der in ein Netzwerk ein- und ausströmt, und sind ein wichtiges Instrument zum Schutz von Systemen. SMEs Firewalls sollten zum Schutz aller kritischen Systeme eingesetzt werden, insbesondere sollte eine Firewall gerichtet werden, um das Netzwerk von KMU vor Gefahren aus dem Internet zu schützen.	restricted-common-ports	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass gemeinsame Ports für Amazon Elastic Compute Cloud (Amazon EC2) -Sicherheitsgruppen eingeschränkt sind. Wenn der Zugriff auf Ports nicht auf vertrauenswürdige Quellen beschränkt wird, kann dies zu Angriffen auf die Verfügbarkeit, Integrität und Vertraulichkeit von Systemen führen. Mit dieser Regel können Sie optional die Parameter blockedPort1–blockedPort5 festlegen (Standardkonfigurationen: 20, 21, 3389, 3306, 4333). Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
7_NETZWERKSCHUTZ: EINSATZ VON FIREWALLS	Firewalls verwalten den Datenverkehr, der in ein Netzwerk ein- und ausströmt, und sind ein wichtiges Instrument zum Schutz von SMEs Systemen. Firewalls sollten zum Schutz aller kritischen Systeme eingesetzt werden, insbesondere sollte eine Firewall gerichtet werden, um das Netzwerk von KMU vor Gefahren aus dem Internet zu schützen.	vpc-default-security-group-geschlossen	Sicherheitsgruppen von Amazon Elastic Compute Cloud (Amazon EC2) können bei der Verwaltung des Netzwerkzugriffs helfen, indem sie eine statusbehaftete Filterung des ein- und ausgehenden Netzwerkverkehrs zu Ressourcen bereitstellen. AWS Die Beschränkung des gesamten Datenverkehrs auf die Standardsicherheitsgruppe hilft dabei, den Fernzugriff auf Ihre Ressourcen einzuschränken. AWS

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
7_NETZWERKSCHUTZ: EINSATZ VON FIREWALLS	Firewalls verwalten den ein- und ausgehenden Datenverkehr in ein Netzwerk und sind ein wichtiges Instrument zum Schutz von Systemen. SMEs Firewalls sollten zum Schutz aller kritischen Systeme eingesetzt werden, insbesondere sollte eine Firewall gerichtet werden, um das Netzwerk von KMU vor Gefahren aus dem Internet zu schützen.	vpc-sg-open-only-to-authorized-ports	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass gemeinsame Ports für Amazon Elastic Compute Cloud (Amazon EC2) -Sicherheitsgruppen eingeschränkt sind. Wenn der Zugriff auf Ports nicht auf vertrauenswürdige Quellen beschränkt wird, kann dies zu Angriffen auf die Verfügbarkeit, Integrität und Vertraulichkeit von Systemen führen. Durch die Beschränkung des Zugriffs auf Ressourcen innerhalb einer Sicherheitsgruppe aus dem Internet (0.0.0.0/0) kann der Remote-Zugriff auf interne Systeme gesteuert werden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
7_NETZWERKSCHUTZ: EINSATZ VON FIREWALLS	Firewalls verwalten den Datenverkehr, der in ein Netzwerk eingeht und es verlässt, und sind ein wichtiges Instrument zum Schutz von SMEs Systemen. Firewalls sollten zum Schutz aller kritischen Systeme eingesetzt werden, insbesondere sollte eine Firewall gerichtet werden, um das Netzwerk von KMU vor Gefahren aus dem Internet zu schützen.	alb-waf-enabled	Stellen Sie sicher, dass AWS WAF auf Elastic Load Balancers (ELB) aktiviert ist, um Webanwendungen zu schützen. Eine WAF trägt zum Schutz Ihrer Webanwendungen oder APIs vor gängigen Web-Exploits bei. Diese Web-Exploits können sich auf die Verfügbarkeit auswirken, die Sicherheit gefährden oder übermäßige Ressourcen in Ihrer Umgebung verbrauchen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
7_NETZWERKSCHUTZ: EINSATZ VON FIREWALLS	Firewalls verwalten den ein- und ausgehenden Datenverkehr in ein Netzwerk und sind ein wichtiges Instrument zum Schutz von Systemen. SMEs Firewalls sollten zum Schutz aller kritischen Systeme eingesetzt werden, insbesondere sollte eine Firewall gerichtet werden, um das Netzwerk von KMU vor Gefahren aus dem Internet zu schützen.	api-gw-associated-with-WAF	AWS Mit WAF können Sie eine Reihe von Regeln (als Web Access Control List (Web ACL) bezeichnet) konfigurieren, die Webanfragen auf der Grundlage von anpassbaren Websicherheitsregeln und -bedingungen, die Sie definieren, zulassen, blockieren oder zählen. Stellen Sie sicher, dass Ihre Amazon-API-Gateway-Stufe mit einer WAF-Web-ACL verknüpft ist, um sie vor böswilligen Angriffen zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
7_NETZWERKSCHUTZ: EINSATZ VON FIREWALLS	Firewalls verwalten den ein- und ausgehenden Datenverkehr in ein Netzwerk und sind ein wichtiges Instrument zum Schutz SMEs von Systemen. Firewalls sollten zum Schutz aller kritischen Systeme eingesetzt werden, insbesondere sollte eine Firewall gerichtet werden, um das Netzwerk von KMU vor Gefahren aus dem Internet zu schützen.	netfw-policy-rule-group-assoziiert	Eine AWS Netzwerk-Firewall-Richtlinie definiert, wie Ihre Firewall den Verkehr in einer Amazon VPC überwacht und verarbeitet. Sie konfigurieren statusfreie und statusbehaftete Regelgruppen, um Pakete und Datenverkehrsströme zu filtern, und Sie definieren den standardmäßigen Umgang mit Datenverkehr.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
7_NETZWERKSCHUTZ: EINSATZ VON FIREWALLS	Firewalls verwalten den Datenverkehr, der in ein Netzwerk eingeht und es verlässt, und sind ein wichtiges Instrument zum Schutz SMEs von Systemen. Firewalls sollten zum Schutz aller kritischen Systeme eingesetzt werden, insbesondere sollte eine Firewall gerichtet werden, um das Netzwerk von KMU vor Gefahren aus dem Internet zu schützen.	netfw-stateless-rule-group-nicht leer	Eine AWS Netzwerkfirewall-Regelgruppe enthält Regeln, die definieren, wie Ihre Firewall den Verkehr in Ihrer VPC verarbeitet. Wenn eine leere statuslose Regelgruppe in einer Firewall-Richtlinie vorhanden ist, verarbeitet sie keinen Datenverkehr.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
7_NETZWERKSCHUTZ: EINSATZ VON FIREWALLS	Firewalls verwalten den Datenverkehr, der in ein Netzwerk eingeht und es verlässt, und sind ein wichtiges Instrument zum Schutz SMEs von Systemen. Firewalls sollten zum Schutz aller kritischen Systeme eingesetzt werden, insbesondere sollte eine Firewall gerichtet werden, um das Netzwerk von KMU vor Gefahren aus dem Internet zu schützen.	waf-regional-rule-not-leer	Stellen Sie sicher, dass Ihre AWS WAF eine Regel hat, die nicht leer ist. Eine Regel ohne Bedingungen kann zu unbeabsichtigtem Verhalten führen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
7_NETZWERKSCHUTZ: EINSATZ VON FIREWALLS	Firewalls verwalten den Datenverkehr, der in ein Netzwerk ein- und ausströmt, und sind ein wichtiges Instrument zum Schutz SMEs von Systemen. Firewalls sollten zum Schutz aller kritischen Systeme eingesetzt werden, insbesondere sollte eine Firewall gerichtet werden, um das Netzwerk von KMU vor Gefahren aus dem Internet zu schützen.	waf-regional-rulegroup-not-leer	Stellen Sie sicher, dass Ihre AWS WAF eine Regelgruppe hat, die nicht leer ist. Eine leere Regelgruppe kann zu unbeabsichtigtem Verhalten führen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
7_NETZWERKSCHUTZ: EINSATZ VON FIREWALLS	Firewalls verwalten den Datenverkehr, der in ein Netzwerk ein- und ausströmt, und sind ein wichtiges Instrument zum Schutz SMEs von Systemen. Firewalls sollten zum Schutz aller kritischen Systeme eingesetzt werden, insbesondere sollte eine Firewall gerichtet werden, um das Netzwerk von KMU vor Gefahren aus dem Internet zu schützen.	waf-regional-webacl-not-leer	Eine an eine AWS WAF angehängte Web-ACL kann eine Sammlung von Regeln und Regelgruppen zur Überprüfung und Steuerung von Webanfragen enthalten. Wenn eine Web-ACL leer ist, wird der Webdatenverkehr weitergeleitet, ohne von der WAF erkannt oder bearbeitet zu werden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
7_NETZWERKSCHUTZ: RECHERCHE ÜBER REMOTE-ZUGRIFFSLÖSUNGEN	SMEs sollte alle Fernzugriffstools regelmäßig überprüfen, um sicherzustellen, dass sie sicher sind, insbesondere: - Stellen Sie sicher, dass die gesamte Fernzugriffssoftware gepatcht und auf dem neuesten Stand ist. - Den Remote-Zugriff von verdächtigen geografischen Standorten oder bestimmten IP-Adressen beschränken. - Den Remote-Zugriff von Mitarbeitern auf Systeme und Computer beschränken, die sie für ihre Arbeit benötigen. - Sichere Passwörter für den Remote-Zugriff erzwingen und nach Möglichkeit die Multi-Faktor-Authentifizierung aktivieren. - Sicherstellen, dass Überwachung und Warnmeldungen aktiviert sind, um vor	iam-password-policy	Die Identitäten und Anmeldeinformationen werden auf der Grundlage einer organisatorischen IAM-Passwortrichtlinie ausgestellt, verwaltet und verifiziert. Sie erfüllen oder übertreffen die Anforderungen von NIST SP 800-63 und dem Standard „Best Practices“ von AWS Foundational Security in Bezug auf die Passwortstärke. Mit dieser Regel können Sie optional RequireUppercaseCharacters (Wert für AWS grundlegende Sicherheitsbewährte Methoden: wahr), RequireLowercaseCharacters (Wert für bewährte Methoden für AWS grundlegende Sicherheit: wahr), RequireSymbols (Wert für bewährte Methoden für AWS grundlegende Sicherheit:

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	vermuteten Angriffen oder ungewöhnlichen verdächtigen Aktivitäten zu warnen.		wahr), RequireNumbers (Wert für bewährte Methoden für AWS grundlegende Sicherheit: wahr), MinimumPasswordLength (Wert für bewährte Methoden für AWS grundlegende Sicherheit: 14), PasswordReusePrevention (Wert für bewährte Methoden für AWS grundlegende Sicherheit: 24) und MaxPasswordAge (Wert für bewährte Methoden für AWS grundlegende Sicherheit: 90) für Ihr IAM festlegen Kennwortrichtlinie. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
7_NETZWERKSCHUTZ: RECHERCHE ÜBER REMOTE-ZUGRIFFSLÖSUNGEN	SMEs sollte alle Fernzugriffstools regelmäßig überprüfen, um sicherzustellen, dass sie sicher sind, insbesondere: - Stellen Sie sicher, dass die gesamte Fernzugriffssoftware gepatcht und auf dem neuesten Stand ist. - Den Remote-Zugriff von verdächtigen geografischen Standorten oder bestimmten IP-Adressen beschränken. - Den Remote-Zugriff von Mitarbeitern auf Systeme und Computer beschränken, die sie für ihre Arbeit benötigen. - Sichere Passwörter für den Remote-Zugriff erzwingen und nach Möglichkeit die Multi-Faktor-Authentifizierung aktivieren. - Sicherstellen, dass Überwachung und Warnmeldungen aktiviert sind, um vor	iam-user-mfa-enabled	Aktivieren Sie diese Regel, um den Zugriff auf Ressourcen in der AWS Cloud einzuschränken. Diese Regel sorgt dafür, dass die Multi-Faktor-Authentifizierung (MFA) für alle Benutzer aktiviert ist. MFA sorgt für eine weitere Schutzebene zusätzlich zu den Anmeldeinformationen. Reduzieren Sie Fälle von kompromittierten Konten, indem Sie MFA für Benutzer vorschreiben.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	vermuteten Angriffen oder ungewöhnlichen verdächtigen Aktivitäten zu warnen.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
7_NETZWERKSCHUTZ: RECHERCHE ÜBER REMOTE-ZUGRIFFSLÖSUNGEN	SMEs sollte alle Fernzugriffstools regelmäßig überprüfen, um sicherzustellen, dass sie sicher sind, insbesondere: - Stellen Sie sicher, dass die gesamte Fernzugriffssoftware gepatcht und auf dem neuesten Stand ist. - Den Remote-Zugriff von verdächtigen geografischen Standorten oder bestimmten IP-Adressen beschränken. - Den Remote-Zugriff von Mitarbeitern auf Systeme und Computer beschränken, die sie für ihre Arbeit benötigen. - Sichere Passwörter für den Remote-Zugriff erzwingen und nach Möglichkeit die Multi-Faktor-Authentifizierung aktivieren. - Sicherstellen, dass Überwachung und Warnmeldungen aktiviert sind, um vor	mfa-enabled-for-iam-Konsolenzugriff	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass MFA für alle AWS Identity and Access Management (IAM) -Benutzer aktiviert ist, die über ein Konsolenkennwort verfügen. MFA sorgt für eine weitere Schutzebene zusätzlich zu den Anmeldeinformationen. Indem Sie MFA für Benutzer vorschreiben, können Sie Fälle kompromittierter Konten reduzieren und verhindern, dass unbefugte Benutzer auf vertrauliche Daten zugreifen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	vermuteten Angriffen oder ungewöhnlichen verdächtigen Aktivitäten zu warnen.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
7_NETZWERKSCHUTZ: RECHERCHE ÜBER REMOTE-ZUGRIFFSLÖSUNGEN	SMEs sollte alle Fernzugriffstools regelmäßig überprüfen, um sicherzustellen, dass sie sicher sind, insbesondere: - Stellen Sie sicher, dass die gesamte Fernzugriffssoftware gepatcht und auf dem neuesten Stand ist. - Den Remote-Zugriff von verdächtigen geografischen Standorten oder bestimmten IP-Adressen beschränken. - Den Remote-Zugriff von Mitarbeitern auf Systeme und Computer beschränken, die sie für ihre Arbeit benötigen. - Sichere Passwörter für den Remote-Zugriff erzwingen und nach Möglichkeit die Multi-Faktor-Authentifizierung aktivieren. - Sicherstellen, dass Überwachung und Warnmeldungen aktiviert sind, um vor	root-account-hardware-mfa-aktiviert	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Hardware-MFA für den Root-Benutzer aktiviert ist. Der Stammbenutzer ist der AWS-Konto-Benutzer mit den meisten Berechtigungen. MFA sorgt für eine weitere Schutzebene zusätzlich zu den Anmeldeinformationen. Indem Sie MFA für den Root-Benutzer vorschreiben, können Sie die Anzahl AWS-Konten kompromittierter Benutzer reduzieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	vermuteten Angriffen oder ungewöhnlichen verdächtigen Aktivitäten zu warnen.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
7_NETZWERKSCHUTZ: RECHERCHE ÜBER REMOTE-ZUGRIFFSLÖSUNGEN	SMEs sollten alle Fernzugriffstools regelmäßig überprüfen, um sicherzustellen, dass sie sicher sind, insbesondere: - Stellen Sie sicher, dass die gesamte Fernzugriffssoftware gepatcht und auf dem neuesten Stand ist. - Den Remote-Zugriff von verdächtigen geografischen Standorten oder bestimmten IP-Adressen beschränken. - Den Remote-Zugriff von Mitarbeitern auf Systeme und Computer beschränken, die sie für ihre Arbeit benötigen. - Sichere Passwörter für den Remote-Zugriff erzwingen und nach Möglichkeit die Multi-Faktor-Authentifizierung aktivieren. - Sicherstellen, dass Überwachung und Warnmeldungen aktiviert sind, um vor	root-account-mfa-enabled	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass MFA für den Root-Benutzer aktiviert ist. Der Stammbenutzer ist der AWS-Konto-Benutzer mit den meisten Berechtigungen. MFA sorgt für eine weitere Schutzebene zusätzlich zu den Anmeldeinformationen. Indem Sie MFA für den Root-Benutzer vorschreiben, können Sie die Anzahl AWS-Konten kompromittierter Benutzer reduzieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	vermuteten Angriffen oder ungewöhnlichen verdächtigen Aktivitäten zu warnen.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
7_NETZWERKSCHUTZ: RECHERCHE ÜBER REMOTE-ZUGRIFFSLÖSUNGEN	SMEs sollten alle Fernzugriffstools regelmäßig überprüfen, um sicherzustellen, dass sie sicher sind, insbesondere: - Stellen Sie sicher, dass die gesamte Fernzugriffssoftware gepatcht und auf dem neuesten Stand ist. - Den Remote-Zugriff von verdächtigen geografischen Standorten oder bestimmten IP-Adressen beschränken. - Den Remote-Zugriff von Mitarbeitern auf Systeme und Computer beschränken, die sie für ihre Arbeit benötigen. - Sichere Passwörter für den Remote-Zugriff erzwingen und nach Möglichkeit die Multi-Faktor-Authentifizierung aktivieren. - Sicherstellen, dass Überwachung und Warnmeldungen aktiviert sind, um vor	api-gw-execution-logging-aktiviert	Die API-Gateway-Protokollierung zeigt detaillierte Ansichten der Benutzer, die auf die API zugegriffen haben, und wie diese Benutzer auf die API zugegriffen haben. Diese Einblicke ermöglichen die Transparenz von Benutzeraktivitäten.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	vermuteten Angriffen oder ungewöhnlichen verdächtigen Aktivitäten zu warnen.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
7_NETZWERKSCHUTZ: RECHERCHE ÜBER REMOTE-ZUGRIFFSLÖSUNGEN	SMEs sollte alle Fernzugriffstools regelmäßig überprüfen, um sicherzustellen, dass sie sicher sind, insbesondere: - Stellen Sie sicher, dass die gesamte Fernzugriffssoftware gepatcht und auf dem neuesten Stand ist. - Den Remote-Zugriff von verdächtigen geografischen Standorten oder bestimmten IP-Adressen beschränken. - Den Remote-Zugriff von Mitarbeitern auf Systeme und Computer beschränken, die sie für ihre Arbeit benötigen. - Sichere Passwörter für den Remote-Zugriff erzwingen und nach Möglichkeit die Multi-Faktor-Authentifizierung aktivieren. - Sicherstellen, dass Überwachung und Warnmeldungen aktiviert sind, um vor	cloud-trail-cloud-watch-Logs aktiviert	Verwenden Sie Amazon CloudWatch , um Protokoll ereignisaktivitäten zentral zu sammeln und zu verwalten. Die Aufnahme von AWS CloudTrail Daten liefert Einzelheiten zu den API-Aufrufaktivitäten in Ihrem AWS-Konto.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	vermuteten Angriffen oder ungewöhnlichen verdächtigen Aktivitäten zu warnen.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
7_NETZWERKSCHUTZ: RECHERCHE ÜBER REMOTE-ZUGRIFFSLÖSUNGEN	SMEs sollte alle Fernzugriffstools regelmäßig überprüfen, um sicherzustellen, dass sie sicher sind, insbesondere: - Stellen Sie sicher, dass die gesamte Fernzugriffssoftware gepatcht und auf dem neuesten Stand ist. - Den Remote-Zugriff von verdächtigen geografischen Standorten oder bestimmten IP-Adressen beschränken. - Den Remote-Zugriff von Mitarbeitern auf Systeme und Computer beschränken, die sie für ihre Arbeit benötigen. - Sichere Passwörter für den Remote-Zugriff erzwingen und nach Möglichkeit die Multi-Faktor-Authentifizierung aktivieren. - Sicherstellen, dass Überwachung und Warnmeldungen aktiviert sind, um vor	elasticsearch-logs-to-cloudwatch	Stellen Sie sicher, dass für Amazon Elasticsearch Service-Domains Fehlerprotokolle aktiviert und zur Aufbewahrung und Beantwortung an Amazon CloudWatch Logs gestreamt werden. Domain-Fehlerprotokolle sind bei Sicherheits- und Zugriffsprüfungen sowie bei der Diagnose von Verfügbarkeitsproblemen nützlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	vermuteten Angriffen oder ungewöhnlichen verdächtigen Aktivitäten zu warnen.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
7_NETZWERKSCHUTZ: RECHERCHE ÜBER REMOTE-ZUGRIFFSLÖSUNGEN	SMEs sollte alle Fernzugriffstools regelmäßig überprüfen, um sicherzustellen, dass sie sicher sind, insbesondere: - Stellen Sie sicher, dass die gesamte Fernzugriffssoftware gepatcht und auf dem neuesten Stand ist. - Den Remote-Zugriff von verdächtigen geografischen Standorten oder bestimmten IP-Adressen beschränken. - Den Remote-Zugriff von Mitarbeitern auf Systeme und Computer beschränken, die sie für ihre Arbeit benötigen. - Sichere Passwörter für den Remote-Zugriff erzwingen und nach Möglichkeit die Multi-Faktor-Authentifizierung aktivieren. - Sicherstellen, dass Überwachung und Warnmeldungen aktiviert sind, um vor	cloudtrail-enabled	AWS CloudTrail kann durch die Aufzeichnung von Aktionen und API-Aufrufen in der AWS Management Console helfen, die Ablehnung zu verhindern. Sie können die Benutzer und die Benutzer AWS-Konten , die einen AWS Dienst aufgerufen haben, die Quell-IP-Adresse, über die die Aufrufe generiert wurden, und den Zeitpunkt der Anrufe identifizieren. Einzelheiten zu den erfassten Daten finden Sie unter Inhalt des AWS CloudTrail Datensatzes.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	vermuteten Angriffen oder ungewöhnlichen verdächtigen Aktivitäten zu warnen.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
7_NETZWERKSCHUTZ: RECHERCHE ÜBER REMOTE-ZUGRIFFSLÖSUNGEN	SMEs sollte alle Fernzugriffstools regelmäßig überprüfen, um sicherzustellen, dass sie sicher sind, insbesondere: - Stellen Sie sicher, dass die gesamte Fernzugriffssoftware gepatcht und auf dem neuesten Stand ist. - Den Remote-Zugriff von verdächtigen geografischen Standorten oder bestimmten IP-Adressen beschränken. - Den Remote-Zugriff von Mitarbeitern auf Systeme und Computer beschränken, die sie für ihre Arbeit benötigen. - Sichere Passwörter für den Remote-Zugriff erzwingen und nach Möglichkeit die Multi-Faktor-Authentifizierung aktivieren. - Sicherstellen, dass Überwachung und Warnmeldungen aktiviert sind, um vor	opensearch-logs-to-cloudwatch	Stellen Sie sicher, dass für Amazon OpenSearch Service-Domains Fehlerprotokolle aktiviert und zur Aufbewahrung und Beantwortung an Amazon CloudWatch Logs gestreamt werden. OpenSearch Service-Fehlerprotokolle können bei Sicherheits- und Zugriffsprüfungen helfen und bei der Diagnose von Verfügbarkeitsproblemen helfen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	vermuteten Angriffen oder ungewöhnlichen verdächtigen Aktivitäten zu warnen.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
7_NETZWERKSCHUTZ: RECHERCHE ÜBER REMOTE-ZUGRIFFSLÖSUNGEN	SMEs sollte alle Fernzugriffstools regelmäßig überprüfen, um sicherzustellen, dass sie sicher sind, insbesondere: - Stellen Sie sicher, dass die gesamte Fernzugriffssoftware gepatcht und auf dem neuesten Stand ist. - Den Remote-Zugriff von verdächtigen geografischen Standorten oder bestimmten IP-Adressen beschränken. - Den Remote-Zugriff von Mitarbeitern auf Systeme und Computer beschränken, die sie für ihre Arbeit benötigen. - Sichere Passwörter für den Remote-Zugriff erzwingen und nach Möglichkeit die Multi-Faktor-Authentifizierung aktivieren. - Sicherstellen, dass Überwachung und Warnmeldungen aktiviert sind, um vor	elb-logging-enabled	Die Elastic-Load-Balancing-Aktivität ist ein zentraler Kommunikationspunkt innerhalb einer Umgebung. Stellen Sie sicher, dass die ELB-Protokollierung aktiviert ist. Die gesammelten Daten enthalten detaillierte Informationen zu Anfragen, die an den ELB gesendet wurden. Jedes Protokoll enthält Informationen wie die Zeit, zu der die Anforderung einging, die Client-IP-Adresse, Latenzen, Anforderungspfade und Serverantworten.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	vermuteten Angriffen oder ungewöhnlichen verdächtigen Aktivitäten zu warnen.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
7_NETZWERKSCHUTZ: RECHERCHE ÜBER REMOTE-ZUGRIFFSLÖSUNGEN	SMEs sollte alle Fernzugriffstools regelmäßig überprüfen, um sicherzustellen, dass sie sicher sind, insbesondere: - Stellen Sie sicher, dass die gesamte Fernzugriffssoftware gepatcht und auf dem neuesten Stand ist. - Den Remote-Zugriff von verdächtigen geografischen Standorten oder bestimmten IP-Adressen beschränken. - Den Remote-Zugriff von Mitarbeitern auf Systeme und Computer beschränken, die sie für ihre Arbeit benötigen. - Sichere Passwörter für den Remote-Zugriff erzwingen und nach Möglichkeit die Multi-Faktor-Authentifizierung aktivieren. - Sicherstellen, dass Überwachung und Warnmeldungen aktiviert sind, um vor	rds-logging-enabled	Um die Protokollierung und Überwachung in Ihrer Umgebung zu erleichtern, stellen Sie sicher, dass die Amazon Relational Database Service (Amazon RDS)-Protokollierung aktiviert ist. Mit der Amazon-RDS-Protokollierung können Sie Ereignisse wie Verbindungen, Verbindungsabbrüche, Abfragen oder abgefragte Tabellen erfassen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	vermuteten Angriffen oder ungewöhnlichen verdächtigen Aktivitäten zu warnen.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
7_NETZWERKSCHUTZ: RECHERCHE ÜBER REMOTE-ZUGRIFFSLÖSUNGEN	SMEs sollte alle Fernzugriffstools regelmäßig überprüfen, um sicherzustellen, dass sie sicher sind, insbesondere: - Stellen Sie sicher, dass die gesamte Fernzugriffssoftware gepatcht und auf dem neuesten Stand ist. - Den Remote-Zugriff von verdächtigen geografischen Standorten oder bestimmten IP-Adressen beschränken. - Den Remote-Zugriff von Mitarbeitern auf Systeme und Computer beschränken, die sie für ihre Arbeit benötigen. - Sichere Passwörter für den Remote-Zugriff erzwingen und nach Möglichkeit die Multi-Faktor-Authentifizierung aktivieren. - Sicherstellen, dass Überwachung und Warnmeldungen aktiviert sind, um vor	s-3 bucket-logging-enabled	Die Amazon Simple Storage Service (Amazon S3)-Serverzugriffsprotokollierung bietet eine Methode zur Überwachung des Netzwerks im Hinblick auf potenzielle Cybersicherheitsereignisse. Die Ereignisse werden überwacht, indem detaillierte Aufzeichnungen über die Anfragen erfasst werden, die an einen Amazon-S3-Bucket gestellt wurden. Jeder Zugriffsprotokolleintrag enthält Details zu einer einzelnen Zugriffsanfrage. Zu den Details gehören Anforderer, Bucket-Name, Anforderungszeit, Anforderungsaktion, Antwortstatus und Fehlercode, falls relevant.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	vermuteten Angriffen oder ungewöhnlichen verdächtigen Aktivitäten zu warnen.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
7_NETZWERKSCHUTZ: RECHERCHE ÜBER REMOTE-ZUGRIFFSLÖSUNGEN	SMEs sollte alle Fernzugriffstools regelmäßig überprüfen, um sicherzustellen, dass sie sicher sind, insbesondere: - Stellen Sie sicher, dass die gesamte Fernzugriffssoftware gepatcht und auf dem neuesten Stand ist. - Den Remote-Zugriff von verdächtigen geografischen Standorten oder bestimmten IP-Adressen beschränken. - Den Remote-Zugriff von Mitarbeitern auf Systeme und Computer beschränken, die sie für ihre Arbeit benötigen. - Sichere Passwörter für den Remote-Zugriff erzwingen und nach Möglichkeit die Multi-Faktor-Authentifizierung aktivieren. - Sicherstellen, dass Überwachung und Warnmeldungen aktiviert sind, um vor	securityhub-enabled	AWS Security Hub hilft bei der Überwachung von unbefugtem Personal, Verbindungen, Geräten und Software. AWS Security Hub aggregiert, organisiert und priorisiert die Sicherheitswarnungen oder Ergebnisse mehrerer Dienste. AWS Einige dieser Dienste sind Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer und AWS Firewall Manager sowie AWS Partnerlösungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	vermuteten Angriffen oder ungewöhnlichen verdächtigen Aktivitäten zu warnen.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
7_NETZWERKSCHUTZ: RECHERCHE ÜBER REMOTE-ZUGRIFFSLÖSUNGEN	SMEs sollte alle Fernzugriffstools regelmäßig überprüfen, um sicherzustellen, dass sie sicher sind, insbesondere: - Stellen Sie sicher, dass die gesamte Fernzugriffssoftware gepatcht und auf dem neuesten Stand ist. - Den Remote-Zugriff von verdächtigen geografischen Standorten oder bestimmten IP-Adressen beschränken. - Den Remote-Zugriff von Mitarbeitern auf Systeme und Computer beschränken, die sie für ihre Arbeit benötigen. - Sichere Passwörter für den Remote-Zugriff erzwingen und nach Möglichkeit die Multi-Faktor-Authentifizierung aktivieren. - Sicherstellen, dass Überwachung und Warnmeldungen aktiviert sind, um vor	vpc-flow-logs-enabled	VPC-Flow-Protokolle erfassen detaillierte Informationsdatensätze über den IP-Datenverkehr, der zu und von Netzwerkschnittstellen in Ihrer Amazon Virtual Private Cloud (Amazon VPC) fließt. Standardmäßig enthalten Flow-Protokolldatensätze Werte für die verschiedenen Komponenten des IP-Flows, einschließlich Quelle, Ziel und Protokoll.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	vermuteten Angriffen oder ungewöhnlichen verdächtigen Aktivitäten zu warnen.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
7_NETZWERKSCHUTZ: RECHERCHE ÜBER REMOTE-ZUGRIFFSLÖSUNGEN	SMEs sollte alle Fernzugriffstools regelmäßig überprüfen, um sicherzustellen, dass sie sicher sind, insbesondere: - Stellen Sie sicher, dass die gesamte Fernzugriffssoftware gepatcht und auf dem neuesten Stand ist. - Den Remote-Zugriff von verdächtigen geografischen Standorten oder bestimmten IP-Adressen beschränken. - Den Remote-Zugriff von Mitarbeitern auf Systeme und Computer beschränken, die sie für ihre Arbeit benötigen. - Sichere Passwörter für den Remote-Zugriff erzwingen und nach Möglichkeit die Multi-Faktor-Authentifizierung aktivieren. - Sicherstellen, dass Überwachung und Warnmeldungen aktiviert sind, um vor	wafv2-logging-enabled	Um die Protokollierung und Überwachung in Ihrer Umgebung zu erleichtern, aktivieren Sie die AWS WAF (V2) -Protokollierung im regionalen und globalen Internet. ACLs AWS Die WAF-Protokollierung bietet detaillierte Informationen über den Datenverkehr, der von Ihrer Web-ACL analysiert wird. In den Protokollen werden die Uhrzeit aufgezeichnet, zu der die AWS WAF die Anfrage von Ihrer AWS Ressource erhalten hat, Informationen über die Anfrage und eine Aktion für die Regel, der jede Anfrage entsprach.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	vermuteten Angriffen oder ungewöhnlichen verdächtigen Aktivitäten zu warnen.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
7_NETZWERKSCHUTZ: RECHERCHE ÜBER REMOTE-ZUGRIFFSLÖSUNGEN	SMEs sollte alle Fernzugriffstools regelmäßig überprüfen, um sicherzustellen, dass sie sicher sind, insbesondere: - Stellen Sie sicher, dass die gesamte Fernzugriffssoftware gepatcht und auf dem neuesten Stand ist. - Den Remote-Zugriff von verdächtigen geografischen Standorten oder bestimmten IP-Adressen beschränken. - Den Remote-Zugriff von Mitarbeitern auf Systeme und Computer beschränken, die sie für ihre Arbeit benötigen. - Sichere Passwörter für den Remote-Zugriff erzwingen und nach Möglichkeit die Multi-Faktor-Authentifizierung aktivieren. - Sicherstellen, dass Überwachung und Warnmeldungen aktiviert sind, um vor	cloudwatch-alarm-action-check	Amazon CloudWatch alarmiert, wenn eine Metrik den Schwellenwert für eine bestimmte Anzahl von Bewertungszeiträumen überschreitet. Der Alarm führt eine oder mehrere Aktionen durch, die vom Wert der Metrik oder des Ausdrucks im Vergleich zu einem Schwellenwert in einer Reihe von Zeiträumen abhängt. Diese Regel erfordert einen Wert für alarmActionRequired (Config Default: True), insufficientDataAction Required (Config Default: True), okActionRequired (Config Default: False). Der tatsächliche Wert muss die Alarmaktionen für Ihre Umgebung widerspiegeln.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	vermuteten Angriffen oder ungewöhnlichen verdächtigen Aktivitäten zu warnen.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
7_NETZWERKSCHUTZ: RECHERCHE ÜBER REMOTE-ZUGRIFFSLÖSUNGEN	SMEs sollte alle Fernzugriffstools regelmäßig überprüfen, um sicherzustellen, dass sie sicher sind, insbesondere: - Stellen Sie sicher, dass die gesamte Fernzugriffssoftware gepatcht und auf dem neuesten Stand ist. - Den Remote-Zugriff von verdächtigen geografischen Standorten oder bestimmten IP-Adressen beschränken. - Den Remote-Zugriff von Mitarbeitern auf Systeme und Computer beschränken, die sie für ihre Arbeit benötigen. - Sichere Passwörter für den Remote-Zugriff erzwingen und nach Möglichkeit die Multi-Faktor-Authentifizierung aktivieren. - Sicherstellen, dass Überwachung und Warnmeldungen aktiviert sind, um vor	redshift-cluster-configuration-check	Um Daten im Ruhezustand zu schützen, muss die Verschlüsselung für Ihre Amazon-Redshift-Cluster aktiviert sein. Sie müssen auch sicherstellen, dass die erforderlichen Konfigurationen auf Amazon-Redshift-Clustern bereitgestellt werden. Die Prüfungsprotokollierung muss aktiviert sein, um Informationen zu Verbindungen und Benutzeraktivitäten in der Datenbank bereitzustellen. Diese Regel erfordert, dass ein Wert für clusterDbEncrypted (Config Default: TRUE) und LoggingEnabled (Config Default: TRUE) gesetzt ist. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	vermuteten Angriffen oder ungewöhnlichen verdächtigen Aktivitäten zu warnen.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
7_NETZWERKSCHUTZ: RECHERCHE ÜBER REMOTE-ZUGRIFFSLÖSUNGEN	SMEs sollte alle Fernzugriffstools regelmäßig überprüfen, um sicherzustellen, dass sie sicher sind, insbesondere: - Stellen Sie sicher, dass die gesamte Fernzugriffssoftware gepatcht und auf dem neuesten Stand ist. - Den Remote-Zugriff von verdächtigen geografischen Standorten oder bestimmten IP-Adressen beschränken. - Den Remote-Zugriff von Mitarbeitern auf Systeme und Computer beschränken, die sie für ihre Arbeit benötigen. - Sichere Passwörter für den Remote-Zugriff erzwingen und nach Möglichkeit die Multi-Faktor-Authentifizierung aktivieren. - Sicherstellen, dass Überwachung und Warnmeldungen aktiviert sind, um vor	redshift-enhanced-vpc-routing-aktiviert	Mit Enhanced-VPC-Routing wird erzwungen, dass der gesamte COPY- und UNLOAD-Datenverkehr zwischen Ihrem Cluster und Datenrepositorys über Ihre Amazon VPC erfolgt. Anschließend können Sie VPC-Features wie Sicherheitsgruppen und Netzwerkzugriffskontrolllisten verwenden, um den Netzwerkverkehr zu schützen. Sie können auch VPC-Flow-Protokolle verwenden, um den Netzwerkverkehr zu überwachen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	vermuteten Angriffen oder ungewöhnlichen verdächtigen Aktivitäten zu warnen.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
9_SICHERE BACKUPS	Für die Wiederherstellung von Schlüsselbildungen sollten Backups aufbewahrt werden, da sie eine effektive Methode zur Wiederherstellung nach Katastrophen wie einem Ransomware-Angriff darstellen. Die folgenden Backup-Regeln sollten gelten: - Backups werden regelmäßig und wann immer möglich automatisiert durchgeführt, - Backups werden getrennt von der Produktionsumgebung des KMU aufbewahrt, - Backups sind verschlüsselt, insbesondere wenn sie zwischen Standorten übertragen werden sollen, - die Fähigkeit zur regelmäßigen Wiederherstellung von Daten aus den Backups wird	aurora-resources-protected-by-Backup-Plan	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon Aurora Aurora-Ressourcen Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	getestet. Idealerweise sollte eine vollständ ige Wiederherstellung regelmäßig von Anfang bis Ende getestet werden.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
9_SICHERE BACKUPS	Für die Wiederherstellung von Schlüsselbildungen sollten Backups aufbewahrt werden, da sie eine effektive Methode zur Wiederherstellung nach Katastrophen wie einem Ransomware-Angriff darstellen. Die folgenden Backup-Regeln sollten gelten: - Backups werden regelmäßig und wann immer möglich automatisiert durchgeführt, - Backups werden getrennt von der Produktionsumgebung des KMU aufbewahrt, - Backups sind verschlüsselt, insbesondere wenn sie zwischen Standorten übertragen werden sollen, - die Fähigkeit zur regelmäßigen Wiederherstellung von Daten aus den Backups wird	backup-plan-min-frequency-and-min-retention-check	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihr AWS Backup-Plan auf eine Mindestfrequenz und Aufbewahrung festgelegt ist. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen. Mit dieser Regel können Sie die Parameter requiredFrequencyValue (Config default: 1), requiredRetentionDays (Config default: 35) und requiredFrequencyUnit

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	getestet. Idealerweise sollte eine vollständ ige Wiederherstellung regelmäßig von Anfang bis Ende getestet werden.		(Config default: days) festlegen. Der tatsächliche Wert muss den Anforderu ngen Ihrer Organisat ion entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
9_SICHERE BACKUPS	Für die Wiederherstellung von Schlüsselbildungen sollten Backups aufbewahrt werden, da sie eine effektive Methode zur Wiederherstellung nach Katastrophen wie einem Ransomware-Angriff darstellen. Die folgenden Backup-Regeln sollten gelten: - Backups werden regelmäßig und wann immer möglich automatisiert durchgeführt, - Backups werden getrennt von der Produktionsumgebung des KMU aufbewahrt, - Backups sind verschlüsselt, insbesondere wenn sie zwischen Standorten übertragen werden sollen, - die Fähigkeit zur regelmäßigen Wiederherstellung von Daten aus den Backups wird	backup-recovery-point-encrypted	Stellen Sie sicher, dass die Verschlüsselung für Ihre AWS Backup-Wiederherstellungspunkte aktiviert ist. Da sensible Daten auch im Ruhezustand vorhanden sein können, sollten Sie die Verschlüsselung im Ruhezustand aktivieren, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	getestet. Idealerweise sollte eine vollständ ige Wiederherstellung regelmäßig von Anfang bis Ende getestet werden.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
9_SICHERE BACKUPS	Für die Wiederherstellung von Schlüsselbildungen sollten Backups aufbewahrt werden, da sie eine effektive Methode zur Wiederherstellung nach Katastrophen wie einem Ransomware-Angriff darstellen. Die folgenden Backup-Regeln sollten gelten: - Backups werden regelmäßig und wann immer möglich automatisiert durchgeführt, - Backups werden getrennt von der Produktionsumgebung des KMU aufbewahrt, - Backups sind verschlüsselt, insbesondere wenn sie zwischen Standorten übertragen werden sollen, - die Fähigkeit zur regelmäßigen Wiederherstellung von Daten aus den Backups wird	backup-recovery-point-manual-Löschen-deaktiviert	Stellen Sie sicher, dass Ihren AWS Backup-Wiederherstellungspunkten eine ressourcenbasierte Richtlinie zugeordnet ist, die das Löschen von Wiederherstellungspunkten verhindert. Die Verwendung einer ressourcenbasierten Richtlinie zur Verhinderung des Löschens von Wiederherstellungspunkten kann dazu beitragen, ein versehentliches oder absichtliches Löschen zu unterbinden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	getestet. Idealerweise sollte eine vollständ ige Wiederherstellung regelmäßig von Anfang bis Ende getestet werden.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
9_SICHERE BACKUPS	Für die Wiederherstellung von Schlüsselbildungen sollten Backups aufbewahrt werden, da sie eine effektive Methode zur Wiederherstellung nach Katastrophen wie einem Ransomware-Angriff darstellen. Die folgenden Backup-Regeln sollten gelten: - Backups werden regelmäßig und wann immer möglich automatisiert durchgeführt, - Backups werden getrennt von der Produktionsumgebung des KMU aufbewahrt, - Backups sind verschlüsselt, insbesondere wenn sie zwischen Standorten übertragen werden sollen, - die Fähigkeit zur regelmäßigen Wiederherstellung von Daten aus den Backups wird	backup-recovery-point-minimum-Aufbewahrungsprüfung	Um bei Datensicherungsprozessen zu helfen, stellen Sie sicher, dass für Ihre AWS Backup-Wiederherstellungspunkte eine Mindestaufbewahrungsdauer festgelegt ist. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen. Mit dieser Regel können Sie den Parameter requiredRetentionDays (Standardkonfiguration: 35) festlegen. Der tatsächliche Wert muss den Anforderu

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	getestet. Idealerweise sollte eine vollständ ige Wiederherstellung regelmäßig von Anfang bis Ende getestet werden.		ngen Ihrer Organisat ion entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
9_SICHERE BACKUPS	Für die Wiederherstellung von Schlüsselbildungen sollten Backups aufbewahrt werden, da sie eine effektive Methode zur Wiederherstellung nach Katastrophen wie einem Ransomware-Angriff darstellen. Die folgenden Backup-Regeln sollten gelten: - Backups werden regelmäßig und wann immer möglich automatisiert durchgeführt, - Backups werden getrennt von der Produktionsumgebung des KMU aufbewahrt, - Backups sind verschlüsselt, insbesondere wenn sie zwischen Standorten übertragen werden sollen, - die Fähigkeit zur regelmäßigen Wiederherstellung von Daten aus den Backups wird	db-instance-backup-enabled	Die Sicherungsfunktion von Amazon RDS erstellt Sicherungen Ihrer Datenbanken und Transaktionsprotokolle. Amazon RDS erstellt einen Snapshot für das Speichervolume Ihrer DB-Instance, sodass die gesamte DB-Instance gesichert wird. Sie können im System spezifische Aufbewahrungsfristen festlegen, um Ihre Ausfallsicherheitsanforderungen zu erfüllen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	getestet. Idealerweise sollte eine vollständ ige Wiederherstellung regelmäßig von Anfang bis Ende getestet werden.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
9_SICHERE BACKUPS	Für die Wiederherstellung von Schlüsselbildungen sollten Backups aufbewahrt werden, da sie eine effektive Methode zur Wiederherstellung nach Katastrophen wie einem Ransomware-Angriff darstellen. Die folgenden Backup-Regeln sollten gelten: - Backups werden regelmäßig und wann immer möglich automatisiert durchgeführt, - Backups werden getrennt von der Produktionsumgebung des KMU aufbewahrt, - Backups sind verschlüsselt, insbesondere wenn sie zwischen Standorten übertragen werden sollen, - die Fähigkeit zur regelmäßigen Wiederherstellung von Daten aus den Backups wird	dynamodb-in-backup-plan	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon DynamoDB-Tabellen Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	getestet. Idealerweise sollte eine vollständ ige Wiederherstellung regelmäßig von Anfang bis Ende getestet werden.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
9_SICHERE BACKUPS	Für die Wiederherstellung von Schlüsselbildungen sollten Backups aufbewahrt werden, da sie eine effektive Methode zur Wiederherstellung nach Katastrophen wie einem Ransomware-Angriff darstellen. Die folgenden Backup-Regeln sollten gelten: - Backups werden regelmäßig und wann immer möglich automatisiert durchgeführt, - Backups werden getrennt von der Produktionsumgebung des KMU aufbewahrt, - Backups sind verschlüsselt, insbesondere wenn sie zwischen Standorten übertragen werden sollen, - die Fähigkeit zur regelmäßigen Wiederherstellung von Daten aus den Backups wird	dynamodb-pitr-enabled	Aktivieren Sie diese Regel, um zu überprüfen, ob die Informationen gesichert wurden. Es verwaltet auch die Backups, indem es sicherstellt, dass die point-in-time Wiederherstellung in Amazon DynamoDB aktiviert ist. Bei der Wiederherstellung werden fortlaufende Backups Ihrer Tabelle für die letzten 35 Tage gespeichert.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	getestet. Idealerweise sollte eine vollständ ige Wiederherstellung regelmäßig von Anfang bis Ende getestet werden.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
9_SICHERE BACKUPS	Für die Wiederherstellung von Schlüsselbildungen sollten Backups aufbewahrt werden, da sie eine effektive Methode zur Wiederherstellung nach Katastrophen wie einem Ransomware-Angriff darstellen. Die folgenden Backup-Regeln sollten gelten: - Backups werden regelmäßig und wann immer möglich automatisiert durchgeführt, - Backups werden getrennt von der Produktionsumgebung des KMU aufbewahrt, - Backups sind verschlüsselt, insbesondere wenn sie zwischen Standorten übertragen werden sollen, - die Fähigkeit zur regelmäßigen Wiederherstellung von Daten aus den Backups wird	ebs-in-backup-plan	Stellen Sie zur Unterstützung der Datensicherungsprozesse sicher, dass Ihre Amazon Elastic Block Store (Amazon EBS) -Volumes Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	getestet. Idealerweise sollte eine vollständ ige Wiederherstellung regelmäßig von Anfang bis Ende getestet werden.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
9_SICHERE BACKUPS	Für die Wiederherstellung von Schlüsselbildungen sollten Backups aufbewahrt werden, da sie eine effektive Methode zur Wiederherstellung nach Katastrophen wie einem Ransomware-Angriff darstellen. Die folgenden Backup-Regeln sollten gelten: - Backups werden regelmäßig und wann immer möglich automatisiert durchgeführt, - Backups werden getrennt von der Produktionsumgebung des KMU aufbewahrt, - Backups sind verschlüsselt, insbesondere wenn sie zwischen Standorten übertragen werden sollen, - die Fähigkeit zur regelmäßigen Wiederherstellung von Daten aus den Backups wird	ec2--Plan resources-protected-by-backup	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon Elastic Compute Cloud (Amazon EC2) -Ressourcen Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	getestet. Idealerweise sollte eine vollständ ige Wiederherstellung regelmäßig von Anfang bis Ende getestet werden.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
9_SICHERE BACKUPS	Für die Wiederherstellung von Schlüsselbildungen sollten Backups aufbewahrt werden, da sie eine effektive Methode zur Wiederherstellung nach Katastrophen wie einem Ransomware-Angriff darstellen. Die folgenden Backup-Regeln sollten gelten: - Backups werden regelmäßig und wann immer möglich automatisiert durchgeführt, - Backups werden getrennt von der Produktionsumgebung des KMU aufbewahrt, - Backups sind verschlüsselt, insbesondere wenn sie zwischen Standorten übertragen werden sollen, - die Fähigkeit zur regelmäßigen Wiederherstellung von Daten aus den Backups wird	efs-in-backup-plan	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon Elastic File System (Amazon EFS) -Dateisysteme Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	getestet. Idealerweise sollte eine vollständ ige Wiederherstellung regelmäßig von Anfang bis Ende getestet werden.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
9_SICHERE BACKUPS	Für die Wiederherstellung von Schlüsselbildungen sollten Backups aufbewahrt werden, da sie eine effektive Methode zur Wiederherstellung nach Katastrophen wie einem Ransomware-Angriff darstellen. Die folgenden Backup-Regeln sollten gelten: - Backups werden regelmäßig und wann immer möglich automatisiert durchgeführt, - Backups werden getrennt von der Produktionsumgebung des KMU aufbewahrt, - Backups sind verschlüsselt, insbesondere wenn sie zwischen Standorten übertragen werden sollen, - die Fähigkeit zur regelmäßigen Wiederherstellung von Daten aus den Backups wird	elasticache-redis-cluster-automatic-Backup-Check	Wenn automatische Backups aktiviert sind, ElastiCache erstellt Amazon täglich ein Backup des Clusters. Die Sicherung kann für eine von Ihrer Organisation festgelegte Anzahl von Tagen aufbewahrt werden. Automatische Backups schützen vor Datenverlust. Bei einem Ausfall können Sie einen neuen Cluster erstellen, der Ihre Daten aus dem aktuellen Backup wiederherstellt.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	getestet. Idealerweise sollte eine vollständ ige Wiederherstellung regelmäßig von Anfang bis Ende getestet werden.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
9_SICHERE BACKUPS	Für die Wiederherstellung von Schlüsselbildungen sollten Backups aufbewahrt werden, da sie eine effektive Methode zur Wiederherstellung nach Katastrophen wie einem Ransomware-Angriff darstellen. Die folgenden Backup-Regeln sollten gelten: - Backups werden regelmäßig und wann immer möglich automatisiert durchgeführt, - Backups werden getrennt von der Produktionsumgebung des KMU aufbewahrt, - Backups sind verschlüsselt, insbesondere wenn sie zwischen Standorten übertragen werden sollen, - die Fähigkeit zur regelmäßigen Wiederherstellung von Daten aus den Backups wird	fsx-resources-protected-by-Backup-Plan	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre FSx Amazon-Dateisysteme Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	getestet. Idealerweise sollte eine vollständ ige Wiederherstellung regelmäßig von Anfang bis Ende getestet werden.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
9_SICHERE BACKUPS	Für die Wiederherstellung von Schlüsselbildungen sollten Backups aufbewahrt werden, da sie eine effektive Methode zur Wiederherstellung nach Katastrophen wie einem Ransomware-Angriff darstellen. Die folgenden Backup-Regeln sollten gelten: - Backups werden regelmäßig und wann immer möglich automatisiert durchgeführt, - Backups werden getrennt von der Produktionsumgebung des KMU aufbewahrt, - Backups sind verschlüsselt, insbesondere wenn sie zwischen Standorten übertragen werden sollen, - die Fähigkeit zur regelmäßigen Wiederherstellung von Daten aus den Backups wird	rds-in-backup-plan	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon Relational Database Service (Amazon RDS) -Instances Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	getestet. Idealerweise sollte eine vollständ ige Wiederherstellung regelmäßig von Anfang bis Ende getestet werden.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
9_SICHERE BACKUPS	Für die Wiederherstellung von Schlüsselbildungen sollten Backups aufbewahrt werden, da sie eine effektive Methode zur Wiederherstellung nach Katastrophen wie einem Ransomware-Angriff darstellen. Die folgenden Backup-Regeln sollten gelten: - Backups werden regelmäßig und wann immer möglich automatisiert durchgeführt, - Backups werden getrennt von der Produktionsumgebung des KMU aufbewahrt, - Backups sind verschlüsselt, insbesondere wenn sie zwischen Standorten übertragen werden sollen, - die Fähigkeit zur regelmäßigen Wiederherstellung von Daten aus den Backups wird	rds-resources-protected-by-Backup-Plan	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon Relational Database Service (Amazon RDS) -Ressourcen Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	getestet. Idealerweise sollte eine vollständ ige Wiederherstellung regelmäßig von Anfang bis Ende getestet werden.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
9_SICHERE BACKUPS	Für die Wiederherstellung von Schlüsselbildungen sollten Backups aufbewahrt werden, da sie eine effektive Methode zur Wiederherstellung nach Katastrophen wie einem Ransomware-Angriff darstellen. Die folgenden Backup-Regeln sollten gelten: - Backups werden regelmäßig und wann immer möglich automatisiert durchgeführt, - Backups werden getrennt von der Produktionsumgebung des KMU aufbewahrt, - Backups sind verschlüsselt, insbesondere wenn sie zwischen Standorten übertragen werden sollen, - die Fähigkeit zur regelmäßigen Wiederherstellung von Daten aus den Backups wird	redshift-backup-enabled	Stellen Sie zur Unterstützung der Datensicherungsprozesse sicher, dass Ihre Amazon-Redshift-Cluster über automatisierte Snapshots verfügen. Wenn automatisierte Snapshots für einen Cluster aktiviert sind, erstellt Redshift in regelmäßigen Abständen Snapshots dieses Clusters. Standardmäßig erstellt Redshift alle acht Stunden oder alle 5 GB einen Snapshot für jeden Knoten mit Datenänderungen oder je nachdem, was zuerst eintritt.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	getestet. Idealerweise sollte eine vollständ ige Wiederherstellung regelmäßig von Anfang bis Ende getestet werden.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
9_SICHERE BACKUPS	Für die Wiederher stellung von Schlüssel bildungen sollten Backups aufbewahr t werden, da sie eine effektive Methode zur Wiederherstellung nach Katastrop hen wie einem Ransomware-Angriff darstellen. Die folgenden Backup-Regeln sollten gelten: - Backups werden regelmäßi g und wann immer möglich automatis iert durchgeführt, - Backups werden getrennt von der Produktionsumgebun g des KMU aufbewahr t, - Backups sind verschlüsselt, insbesondere wenn sie zwischen Standorten übertrage n werden sollen, - die Fähigkeit zur regelmäßigen Wiederherstellung von Daten aus den Backups wird	s3- bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) unterstützt die Aufrechterhaltung einer angemesse nen Kapazität und Verfügbarkeit. CRR ermöglicht das automatische, asynchrone Kopieren von Objekten in Amazon-S3-Buckets, um die Datenverf ügbarkeit sicherzus tellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	getestet. Idealerweise sollte eine vollständige Wiederherstellung regelmäßig von Anfang bis Ende getestet werden.		
11_SICHERE WEBSITES	Es ist wichtig SMEs sicherzustellen, dass ihre Online-Websites auf sichere Weise konfiguriert und verwaltet werden und dass alle persönlichen Daten oder Finanzdaten, wie Kreditkartendaten, angemessen geschützt sind. Dies beinhaltet regelmäßige Sicherheitstests anhand der Websites, um potenzielle Sicherheitsschwachstellen zu ermitteln, und die Durchführung regelmäßiger Überprüfungen, um sicherzustellen, dass die Website ordnungsgemäß gewartet und aktualisiert wird.	vuln-management-plan-exists(Prozessüberprüfung)	Stellen Sie sicher, dass ein Plan für das Schwachstellenmanagement entwickelt und implementiert wird, damit Sie über formell definierte Prozesse zur Behebung von Schwachstellen in Ihrer Umgebung verfügen.

Vorlage

Die Vorlage ist verfügbar unter GitHub: Leitfaden für bewährte Betriebspraktiken für die ENISA-Cybersicherheit für SMEs.

Bewährte Methoden für die Implementierung des Esquema Nacional de Seguridad (ENS) Low

Konformitätspakete bieten ein allgemeines Compliance-Framework, das es Ihnen ermöglicht, mithilfe verwalteter oder benutzerdefinierter Regeln und Abhilfemaßnahmen Kontrollen zur Sicherheit, zum Betrieb oder zur Kostenoptimierung durchzuführen. AWS Config AWS Config Conformance Packs dienen als Beispielvorlagen nicht dazu, die vollständige Einhaltung eines bestimmten Governance- oder Compliance-Standards sicherzustellen. Sie sind dafür verantwortlich, selbst zu beurteilen, ob Ihre Nutzung der Services den geltenden gesetzlichen und behördlichen Anforderungen entspricht.

Im Folgenden finden Sie ein Beispiel für eine Zuordnung zwischen Esquema Nacional de Seguridad (ENS) Low Framework-Steuerelementen in Spanien und verwalteten Konfigurationsregeln. AWS Jede Config-Regel gilt für eine bestimmte AWS -Ressource und bezieht sich auf eine oder mehrere Kontrollen des spanischen ENS Low. Eine Kontrolle des spanischen ENS kann mehreren Config-Regeln zugeordnet werden. In der folgenden Tabelle finden Sie weitere Informationen und Anleitungen zu diesen Zuordnungen.

Diese beispielhafte Conformance-Pack-Vorlage enthält Zuordnungen zu Kontrollen nach den Richtlinien des spanischen ENS Low, das zuletzt am 23.10.2020 aktualisiert wurde.

Kontroll-ID	AWS Config	Empfehlungen
Anexo II 4.1.2.a); b); c)	dynamodb-table-encrypted-kms	Stellen Sie sicher, dass die Verschlüsselung für Ihre Amazon-DynamoDB-Tabellen aktiviert ist. Um eventuell vorhandene sensible Daten im Ruhezustand in diesen Tabellen zu schützen, müssen Sie die Verschlüsselung von Daten im Ruhezustand aktivieren. Standardmäßig werden DynamoDB-Tabellen

Kontroll-ID	AWS Config	Empfehlungen
		mit einem AWS eigenen Kundenhauptschlüssel (CMK) verschlüsselt.
Anexo II 4.1.2.a); b); c)	ec2- ebs-encryption-by-default	Zum Schutz von Daten im Ruhezustand müssen Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon Elastic Block Store (Amazon EBS)-Volumes aktiviert ist. Da sensible Daten auch im Ruhezusta nd vorhanden sein können, sollten Sie die Verschlüs selung im Ruhezustand aktivieren, um diese Daten zu schützen.
Anexo II 4.1.2.a); b); c)	elasticsearch-node-to-node-Verschlüsselungsprüfung	Stellen Sie sicher, dass die node-to-node Verschlüsselung für Amazon OpenSearch Service aktiviert ist. Node-to-nodeVerschlüsselung ermöglicht die TLS 1.2-Versc hlüsselung für die gesamte Kommunikation innerhalb der Amazon Virtual Private Cloud (Amazon VPC). Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	AWS Config	Empfehlungen
Anexo II 4.1.2.a); b); c)	elb-cross-zone-load-Balancing aktiviert	Aktivieren Sie zonenüber greifendes Load Balancing für Ihre Elastic Load Balancer (ELBs), um eine angemesse ne Kapazität und Verfügbar keit aufrechtzuerhalten. Zonenübergreifendes Load Balancing reduziert die Notwendigkeit, die gleiche Anzahl von Instances in jeder aktivierten Availability Zone aufrechtzuerhalten. Es verbessert auch die Fähigkeit Ihrer Anwendung, den Verlust einer oder mehrerer Instances zu bewältigen.
Anexo II 4.1.2.a); b); c)	elb-tls-https-listeners-nur	Stellen Sie sicher, dass Ihre Elastic Load Balancer (ELBs) mit SSL- oder HTTPS-Lis tenern konfiguriert sind. Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	AWS Config	Empfehlungen
Anexo II 4.1.2.a); b); c)	rds-instance-deletion-protection-aktiviert	Stellen Sie sicher, dass Amazon Relational Database Service (Amazon RDS)-Instances den Löschschutz aktiviert haben. Verwenden Sie den Löschschutz, um zu verhindern, dass Ihre Amazon-RDS-Instances versehentlich oder böswillig gelöscht werden, was zum Verlust der Verfügbarkeit Ihrer Anwendungen führen kann.
Anexo II 4.1.2.a); b); c)	rds-snapshot-encrypted	Stellen Sie sicher, dass die Verschlüsselung für Ihre Amazon Relational Database Service (Amazon RDS)-Snapshots aktiviert ist. Da sensible Daten auch im Ruhezustand vorhanden sein können, sollten Sie die Verschlüsselung im Ruhezustand aktivieren, um diese Daten zu schützen.
Anexo II 4.1.2.a); b); c)	s3- bucket-default-lock-enabled	Stellen Sie sicher, dass für Ihren Amazon Simple Storage Service (Amazon S3)-Bucket standardmäßig eine Sperre aktiviert ist. Zum Schutz eventuell vorhandener sensibler Daten in S3-Buckets müssen Sie Objektsperren für Daten im Ruhezustand erzwingen.

Kontroll-ID	AWS Config	Empfehlungen
Anexo II 4.1.2.a); b); c)	s-3 default-encryption-kms	Stellen Sie sicher, dass die Verschlüsselung für Ihre Amazon Simple Storage Service (Amazon S3)-Buckets aktiviert ist. Um eventuell vorhandene sensible Daten im Ruhezustand in einem Amazon-S3-Bucket zu schützen, muss die Verschlüsselung aktiviert sein.
Anexo II 4.1.2.a); b); c)	sagemaker-notebook-instance-kms-key-konfiguriert	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass die Verschlüsselung mit dem AWS Key Management Service (AWS KMS) für Ihr Notebook aktiviert ist. SageMaker Da vertrauliche Daten im SageMaker Notebook gespeichert werden können, sollten Sie die Verschlüsselung im Ruhezustand aktivieren, um diese Daten zu schützen.

Kontroll-ID	AWS Config	Empfehlungen
Anexo II 4.1.2.a); b); c)	sns-encrypted-kms	Um Daten im Ruhezusta nd zu schützen, stellen Sie sicher, dass Ihre Amazon Simple Notification Service (Amazon SNS) -Themen mit dem AWS Key Management Service (AWS KMS) verschlüs selt werden müssen. Um eventuell vorhandene sensible Daten im Ruhezustand in veröffentlichten Nachricht en zu schützen, muss die Verschlüsselung von Daten im Ruhezustand aktiviert sein.
Anexo II 4.1.2.a); b); c)	alb-http-to-https-Umleitung sprüfung	Um Daten während der Übertragung zu schützen, stellen Sie sicher, dass Ihr Application Load Balancer unverschlüsselte HTTP-Anfragen automatisch an HTTPS umleitet. Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	AWS Config	Empfehlungen
Anexo II 4.1.2.a); b); c)	api-gw-cache-enabled-und-verschlüsselt	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass die Verschlüsselung für den Cache Ihrer API-Gateway-Stufe aktiviert ist. Da für die API-Methode sensible Daten erfasst werden können, sollten Sie die Verschlüsselung von Daten im Ruhezustand aktivieren, um diese Daten zu schützen.
Anexo II 4.1.2.a); b); c)	api-gw-ssl-enabled	Stellen Sie sicher, dass die REST-API-Stufen von Amazon API Gateway mit SSL-Zertifikaten konfiguriert sind, damit Backend-Systeme überprüfen können, ob Anforderungen von API Gateway stammen.
Anexo II 4.1.2.a); b); c)	cloud-trail-encryption-enabled	Da sensible Daten vorhanden sein können und um Daten im Ruhezustand zu schützen, sollten Sie sicherstellen, dass die Verschlüsselung für Ihre AWS CloudTrail Trails aktiviert ist.

Kontroll-ID	AWS Config	Empfehlungen
Anexo II 4.1.2.a); b); c)	cloud-trail-log-file-Validierung aktiviert	Verwenden Sie die AWS CloudTrail Protokolldateivalidierung, um die Integrität von Protokollen zu überprüfen. CloudTrail Mithilfe der Protokolldateivalidierung kann festgestellt werden, ob eine Protokolldatei geändert oder gelöscht wurde oder ob sie nach der Übermittlung CloudTrail unverändert geblieben ist. Dieses Feature wurde mit dem Branchenstandard entsprechenden Algorithmen entwickelt: SHA-256 für die Hashfunktion und SHA-256 mit RSA für digitale Signaturen. Aus diesem Grund ist es rechnerisch unmöglich, CloudTrail Protokolldateien unbemerkt zu ändern, zu löschen oder zu fälschen.
Anexo II 4.1.2.a); b); c)	cloudwatch-log-group-encrypted	Um sensible Daten im Ruhezustand zu schützen, stellen Sie sicher, dass die Verschlüsselung für Ihre Amazon CloudWatch Log Groups aktiviert ist.

Kontroll-ID	AWS Config	Empfehlungen
Anexo II 4.1.2.a); b); c)	dynamodb-autoscaling-enabled	Amazon DynamoDB Auto Scaling verwendet den AWS Application Auto Scaling-Service, um die bereitgestellte Durchsatzkapazität so anzupassen, dass sie automatisch auf tatsächliche Verkehrsmuster reagiert. Auf diese Weise kann eine Tabelle oder ein globaler sekundärer Index die bereitgestellte Lese-/Schreibkapazität erhöhen, um plötzliche Erhöhungen des Datenverkehrs ohne Drosselung zu bewältigen.
Anexo II 4.1.2.a); b); c)	efs-encrypted-check	Aktivieren Sie die Verschlüsselung für Ihr Amazon Elastic File System (EFS), um eventuell vorhandene sensible Daten sowie Daten im Ruhezustand zu schützen.
Anexo II 4.1.2.a); b); c)	elasticsearch-encrypted-at-rest	Da sensible Daten vorhanden sein können und um Daten im Ruhezustand zu schützen, sollten Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon OpenSearch Service (OpenSearch Service) -Domains aktiviert ist.

Kontroll-ID	AWS Config	Empfehlungen
Anexo II 4.1.2.a); b); c)	elb-acm-certificate-required	Zum Schutz von eventuell vorhandenen sensiblen Daten sowie von Daten während der Übertragung muss die Verschlüsselung für Ihr Elastic Load Balancing aktiviert sein. Verwenden Sie AWS Certifica te Manager, um öffentlic he und private SSL/TLS-Z ertifikate mit AWS Diensten und internen Ressourcen zu verwalten, bereitzustellen und bereitzustellen.
Anexo II 4.1.2.a); b); c)	elb-deletion-protection-ena bled	Diese Regel sorgt dafür, dass der Löschschutz für Elastic Load Balancing aktiviert ist. Verwenden Sie diese Funktion, um zu verhinder n, dass Ihr Load Balancer versehentlich oder böswillig gelöscht wird, was zum Verlust der Verfügbarkeit Ihrer Anwendungen führen kann.
Anexo II 4.1.2.a); b); c)	encrypted-volumes	Aktivieren Sie die Verschlüs selung für Ihre Amazon-El astic-Block-Store (Amazon-EBS)-Volumes, um eventuell vorhandene sensible Daten sowie Daten im Ruhezustand zu schützen.

Kontroll-ID	AWS Config	Empfehlungen
Anexo II 4.1.2.a); b); c)	opensearch-encrypted-at-rest	Da sensible Daten vorhanden sein können und um Daten im Ruhezustand zu schützen, sollten Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon OpenSearch Service-Domains aktiviert ist.
Anexo II 4.1.2.a); b); c)	opensearch-node-to-node-Verschlüsselungsprüfung	Stellen Sie sicher, dass die node-to-node Verschlüsselung für Amazon OpenSearch Service aktiviert ist. Node-to-nodeVerschlüsselung ermöglicht die TLS 1.2-Verschlüsselung für die gesamte Kommunikation innerhalb der Amazon Virtual Private Cloud (Amazon VPC). Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	AWS Config	Empfehlungen
Anexo II 4.1.2.a); b); c)	rds-multi-az-support	Die Multi-AZ-Unterstützung in Amazon Relational Database Service (Amazon RDS) bietet eine verbesserte Verfügbar keit und Beständigkeit von Datenbank-Instances. Wenn Sie eine Multi-AZ-Datenbank-Instance bereitstellen, erstellt Amazon RDS automatisch eine primäre Datenbank-Instance und repliziert die Daten synchron auf eine Standby-Instance in einer anderen Availability Zone. Jede Availability Zone läuft auf einer eigenen, physisch getrennten, unabhängigen Infrastruktur und ist auf eine hohe Verfügbarkeit ausgelegt . Im Falle eines Infrastru kturausfalls führt Amazon RDS einen automatischen Failover zum Standby-Modus durch, sodass Sie den Datenbank betrieb wieder aufnehmen können, sobald der Failover abgeschlossen ist.

Kontroll-ID	AWS Config	Empfehlungen
Anexo II 4.1.2.a); b); c)	rds-cluster-multi-az-aktiviert	Die Multi-AZ-Unterstützung in Amazon Relational Database Service (Amazon RDS) bietet eine verbesserte Verfügbar keit und Beständigkeit von Datenbank-Instances. Wenn Sie eine Multi-AZ-Datenbank-Instance bereitstellen, erstellt Amazon RDS automatisch eine primäre Datenbank-Instance und repliziert die Daten synchron auf eine Standby-Instance in einer anderen Availability Zone. Jede Availability Zone läuft auf einer eigenen, physisch getrennten, unabhängigen Infrastruktur und ist auf eine hohe Verfügbarkeit ausgelegt . Im Falle eines Infrastru kturausfalls führt Amazon RDS einen automatischen Failover zum Standby-Modus durch, sodass Sie den Datenbank betrieb wieder aufnehmen können, sobald der Failover abgeschlossen ist.

Kontroll-ID	AWS Config	Empfehlungen
Anexo II 4.1.2.a); b); c)	rds-storage-encrypted	Zum Schutz von Daten im Ruhezustand müssen Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon Relational Database Service (Amazon RDS)-Instances aktiviert ist. Um eventuell vorhandene sensible Daten im Ruhezustand in Amazon-RDS-Instanc es zu schützen, muss die Verschlüsselung von Daten im Ruhezustand aktiviert sein.

Kontroll-ID	AWS Config	Empfehlungen
Anexo II 4.1.2.a); b); c)	redshift-cluster-configuration-check	Um Daten im Ruhezustand zu schützen, muss die Verschlüsselung für Ihre Amazon-Redshift-Cluster aktiviert sein. Sie müssen auch sicherstellen, dass die erforderlichen Konfigurationen auf Amazon-Redshift-Clustern bereitgestellt werden. Die Prüfungsprotokollierung muss aktiviert sein, um Informationen zu Verbindungen und Benutzeraktivitäten in der Datenbank bereitzustellen. Diese Regel erfordert, dass ein Wert für clusterDbEncrypted (Config Default: TRUE) und LoggingEnabled (Config Default: TRUE) gesetzt ist. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	AWS Config	Empfehlungen
Anexo II 4.1.2.a); b); c)	redshift-cluster-kms-enabled	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass die Verschlüsselung mit AWS Key Management Service (AWS KMS) für Ihren Amazon Redshift Redshift-Cluster aktiviert ist. Um eventuell vorhandene sensible Daten im Ruhezustand in Redshift-Clustern zu schützen, muss die Verschlüsselung von Daten im Ruhezustand aktiviert sein.
Anexo II 4.1.2.a); b); c)	redshift-require-tls-ssl	Stellen Sie sicher, dass Ihre Amazon-Redshift-Cluster eine TLS/SSL-Verschlüsselung erfordern, um eine Verbindun g zu SQL-Clients herzustel len. Um eventuell vorhanden e sensible Daten zu schützen, sollten Sie die Verschlüs selung bei der Übertragung aktivieren.

Kontroll-ID	AWS Config	Empfehlungen
Anexo II 4.1.2.a); b); c)	s3- aktiviert bucket-server-side -encryption	Zum Schutz von Daten im Ruhezustand müssen Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon Simple Storage Service (Amazon S3)-Bucke ts aktiviert ist. Um eventuell vorhandene sensible Daten im Ruhezustand in Amazon-S3 -Buckets zu schützen, muss die Verschlüsselung aktiviert sein.
Anexo II 4.1.2.a); b); c)	s-3 bucket-ssl-requests-only	Um Daten während der Übertragung zu schützen, stellen Sie sicher, dass Ihre Amazon Simple Storage Service (Amazon S3)-Bucke ts Anfragen zur Verwendun g von Secure Socket Layer (SSL)-Buckets erfordern. Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	AWS Config	Empfehlungen
Anexo II 4.1.2.a); b); c)	sagemaker-endpoint-configuration-kms-key-konfiguriert	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass die Verschlüsselung mit dem AWS Key Management Service (AWS KMS) für Ihren Endpunkt aktiviert ist. SageMaker Da sensible Daten auf dem SageMaker Endgerät gespeichert werden können, sollten Sie die Verschlüsselung im Ruhezustand aktivieren, um diese Daten zu schützen.
Anexo II 4.1.2.a); b); c)	secretsmanager-using-cmk	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass die Verschlüsselung mit dem AWS Key Management Service (AWS KMS) für AWS Secrets Manager aktiviert ist. Aktivieren Sie die Verschlüsselung von Daten im Ruhezustand, um eventuell vorhandene sensible Daten im Ruhezustand im Secrets Manager zu schützen.

Kontroll-ID	AWS Config	Empfehlungen
Anexo II 4.1.2.a); b); c)	vpc-vpn-2-tunnels-up	Redundante Site-to-Site VPN-Tunnel können implement iert werden, um die Anforderu ngen an die Ausfallsicherheit zu erfüllen. Es verwendet zwei Tunnel, um die Konnektiv ität sicherzustellen, falls eine der Site-to-Site VPN-Verbi ndungen nicht verfügbar ist. Um sich vor einem Verbindun gsverlust zu schützen, können Sie für den Fall, dass Ihr Kunden-Gateway nicht verfügbar ist, eine zweite Site-to-Site VPN-Verbindung zu Ihrer Amazon Virtual Private Cloud (Amazon VPC) und Ihrem Virtual Private Gateway einrichten, indem Sie ein zweites Kunden-Gateway verwenden.
Anexo II 4.1.2.b)	ec2- -einperiodisch security-group-attached-to	Diese Regel stellt sicher, dass die Sicherheitsgruppen an eine Amazon Elastic Compute Cloud (Amazon EC2) - Instance oder an eine ENI angehängt sind. Diese Regel unterstützt die Überwachu ng ungenutzter Sicherhei tsgruppen im Bestand und die Verwaltung Ihrer Umgebung.

Kontroll-ID	AWS Config	Empfehlungen
Anexo II 4.1.2.b)	ec2-check managedinstance-association-compliance-status	Verwenden Sie AWS Systems Manager Associations, um bei der Inventarisierung von Softwareplattformen und Anwendungen innerhalb eines Unternehmens zu helfen. AWS Systems Manager weist Ihren verwalteten Instanzen einen Konfigurationsstatus zu und ermöglicht es Ihnen, Basiswerte für Betriebss ystem-Patch-Levels, Softwarei nstallationen, Anwendung skonfigurationen und andere Details zu Ihrer Umgebung festzulegen.
Anexo II 4.1.2.b)	ec2-stopped-instance	Aktivieren Sie diese Regel, um bei der Basiskonfiguration von Amazon Elastic Compute Cloud (Amazon EC2) - Instances zu helfen, indem Sie überprüfen, ob EC2 Amazon-Instances gemäß den Standards Ihrer Organisat ion für mehr als die zulässige Anzahl von Tagen gestoppt wurden.

Kontroll-ID	AWS Config	Empfehlungen
Anexo II 4.1.2.b)	ec2- volume-inuse-check	Diese Regel stellt sicher, dass Amazon Elastic Block Store-Volumes, die an Amazon Elastic Compute Cloud (Amazon EC2) -Instances angehängt sind, zum Löschen markiert werden, wenn eine Instance beendet wird. Wenn ein Amazon-EBS-Volume nicht gelöscht wird, wenn die Instance, an die es angehängt ist, beendet wird, kann dies gegen das Konzept der geringsten Funktionalität verstoßen.
Anexo II 4.1.2.b)	eip-attached	Diese Regel stellt sicher, dass Elastic, die einer Amazon Virtual Private Cloud (Amazon VPC) IPs zugewiesen sind, an Amazon Elastic Compute Cloud (Amazon EC2) - Instances oder verwendete Elastic Network Interfaces angehängt sind. Diese Regel hilft bei der Überwachung ungenutzter Inhalte EIPs in Ihrer Umgebung.

Kontroll-ID	AWS Config	Empfehlungen
Anexo II 4.1.2.b)	vpc-network-acl-unused-überprüfen	Diese Regel stellt sicher, dass Amazon Virtual Private Cloud (VPC)-Netzwerkzugriffskontrolllisten verwendet werden. Die Überwachung ungenutzter Netzwerkzugriffskontrolllisten kann zu einer genauen Inventarisierung und Verwaltung Ihrer Umgebung beitragen.
Anexo II 4.2.1.a)	iam-root-access-key-überprüfen	Der Zugriff auf Systeme und Ressourcen kann gesteuert werden, indem überprüft wird, ob der Root-Benutzer keine Zugriffsschlüssel mit seiner AWS Identity and Access Management (IAM) -Rolle verknüpft hat. Stellen Sie sicher, dass die Root-Zugriffsschlüssel gelöscht werden. Erstellen und verwenden Sie stattdessen rollenbasierte Funktionen, AWS-Konten um das Prinzip der geringsten Funktionalität zu berücksichtigen.

Kontroll-ID	AWS Config	Empfehlungen
Anexo II 4.2.1.a); b)	iam-root-access-key-überprüfen	Der Zugriff auf Systeme und Ressourcen kann gesteuert werden, indem überprüft wird, ob der Root-Benutzer keine Zugriffsschlüssel mit seiner AWS Identity and Access Management (IAM) -Rolle verknüpft hat. Stellen Sie sicher, dass die Root-Zugriffsschlüssel gelöscht werden. Erstellen und verwenden Sie stattdessen rollenbasierte Funktionen, AWS-Konten um das Prinzip der geringsten Funktionalität zu berücksichtigen.
Anexo II 4.2.4	ecs-task-definition-user-for-host-mode-check	Wenn für eine Aufgabendefinition erhöhte Berechtigungen gelten, liegt das daran, dass der Kunde diesen Konfigurationen ausdrücklich zugestimmt hat. Diese Kontrolle prüft, ob eine unerwartete Berechtigungseskalation vorliegt, wenn für eine Aufgabendefinition das Host-Netzwerk aktiviert ist, die Kunden aber keine erhöhten Berechtigungen aktiviert haben.

Kontroll-ID	AWS Config	Empfehlungen
Anexo II 4.2.4	iam-policy-no-statements-with-full-access	Stellen Sie sicher, dass IAM-Aktionen nur auf die benötigte n Aktionen beschränkt sind. Wenn Benutzern mehr Rechte eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und der Aufgabentrennung verstoßen.
Anexo II 4.2.4	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) kann Ihnen dabei helfen, die Prinzipien der geringsten Rechte und der Aufgabent rennung in Zugriffsberechtigu ngen und Autorisierungen zu integrieren und zu verhinder n, dass Richtlinien „Effect“: „Allow“ mit „Action“: „*“ anstelle von „Resource“: „*“ enthalten. Wenn Benutzern mehr Rechte eingeräumt werden, als für die Ausführun g einer Aufgabe erforderl ich sind, kann dies gegen das Prinzip der geringste n Berechtigung und der Aufgabentrennung verstoßen.

Kontroll-ID	AWS Config	Empfehlungen
Anexo II 4.2.4	s3- bucket-policy-grantee-check	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie s3_bucket_policy_grantee_check aktivieren. Diese Regel prüft, ob der vom Amazon S3 S3-Bucket gewährte Zugriff durch die von Ihnen bereitgestellten AWS Principals, Verbundbenutzer, Service Principals, IP-Adressen oder Amazon Virtual Private Cloud (Amazon VPC) IDs eingeschränkt ist.
Anexo II 4.2.5	iam-root-access-key-überprüfen	Der Zugriff auf Systeme und Ressourcen kann gesteuert werden, indem überprüft wird, ob der Root-Benutzer keine Zugriffsschlüssel mit seiner AWS Identity and Access Management (IAM) -Rolle verknüpft hat. Stellen Sie sicher, dass die Root-Zugriffsschlüssel gelöscht werden. Erstellen und verwenden Sie stattdessen rollenbasierte Funktionen, AWS-Konten um das Prinzip der geringsten Funktionalität zu berücksichtigen.

Kontroll-ID	AWS Config	Empfehlungen
Anexo II 4.2.5.BAJO.a)	iam-password-policy	Die Identitäten und Anmeldein formationen werden auf der Grundlage einer organisat orischen IAM-Passwortrichtl inie ausgestellt, verwaltet und verifiziert. Sie erfüllen oder übertreffen die Anforderungen von NIST SP 800-63 und dem Standard „Best Practices“ von AWS Foundational Security für die Passwortstärke. Mit dieser Regel können Sie optional RequireUppercaseCharacters (Wert für AWS grundlege nde Sicherheitsbewährte Methoden: wahr), RequireLo wercaseCharacters (Wert für bewährte Methoden für AWS grundlegende Sicherheit: wahr), RequireSymbols (Wert für bewährte Methoden für AWS grundlegende Sicherhei t: wahr), RequireNumbers (Wert für bewährte Methoden für AWS grundlegende Sicherheit: wahr), MinimumPa sswordLength (Wert für bewährte Methoden für AWS grundlegende Sicherheit: 14), PasswordReusePreve ntion (Wert für bewährte Methoden für AWS grundlege nde Sicherheit: 24) und MaxPasswordAge (Wert

Kontroll-ID	AWS Config	Empfehlungen
		für bewährte Methoden für AWS grundlegende Sicherheit: 90) für Ihr IAM festlegen . Kennwortrichtlinie. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	AWS Config	Empfehlungen
Anexo II 4.2.5.BAJO.c)	iam-password-policy	Die Identitäten und Anmeldein formationen werden auf der Grundlage einer organisat orischen IAM-Passwortrichtl inie ausgestellt, verwaltet und verifiziert. Sie erfüllen oder übertreffen die Anforderungen von NIST SP 800-63 und dem Standard „Best Practices“ von AWS Foundational Security für die Passwortstärke. Mit dieser Regel können Sie optional RequireUppercaseCharacters (Wert für AWS grundlege nde Sicherheitsbewährte Methoden: wahr), RequireLo wercaseCharacters (Wert für bewährte Methoden für AWS grundlegende Sicherheit: wahr), RequireSymbols (Wert für bewährte Methoden für AWS grundlegende Sicherhei t: wahr), RequireNumbers (Wert für bewährte Methoden für AWS grundlegende Sicherheit: wahr), MinimumPa sswordLength (Wert für bewährte Methoden für AWS grundlegende Sicherheit: 14), PasswordReusePreve ntion (Wert für bewährte Methoden für AWS grundlege nde Sicherheit: 24) und MaxPasswordAge (Wert

Kontroll-ID	AWS Config	Empfehlungen
		für bewährte Methoden für AWS grundlegende Sicherhei t: 90) für Ihr IAM festlegen . Kennwortrichtlinie. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisat ion entsprechen.
Anexo II 4.2.6.BAJO.c)	elasticsearch-logs-to-cloud watch	Stellen Sie sicher, dass für Amazon OpenSearch Service-Domains Fehlerprotokolle aktiviert und zur Aufbewahr ung und Beantwortung an Amazon CloudWatch Logs gestreamt werden. Domain-Fehlerprotokolle sind bei Sicherheits- und Zugriffsp rüfungen sowie bei der Diagnose von Verfügbar keitsproblemen nützlich.

Kontroll-ID	AWS Config	Empfehlungen
Anexo II 4.2.6.BAJO.c)	multi-region-cloudtrail-enabled	AWS CloudTrail zeichnet Aktionen und API-Aufrufe der AWS Management Console auf. Sie können feststellen, welche Benutzer und Konten angerufen wurden AWS, von welcher Quell-IP-Adresse aus die Anrufe getätigt wurden und wann die Anrufe erfolgten . CloudTrail übermittelt Protokolldateien aus allen AWS Regionen an Ihren S3-Bucket, wenn MULTI_REGION_CLOUD_TRAIL_ENABLED aktiviert ist. Außerdem wird beim AWS Start einer neuen Region derselbe Trail in der neuen Region erstellt. CloudTrail Dadurch erhalten Sie automatisch Protokoll dateien mit API-Aktivitäten für die neue Region.

Kontroll-ID	AWS Config	Empfehlungen
Anexo II 4.2.6.BAJO.c)	rds-logging-enabled	Um die Protokollierung und Überwachung in Ihrer Umgebung zu erleichtern, stellen Sie sicher, dass die Amazon Relational Database Service (Amazon RDS)-Protokollierung aktiviert ist. Mit der Amazon-RDS-Protokollierung können Sie Ereignisse wie Verbindungen, Verbindungsabbrüche, Abfragen oder abgefragte Tabellen erfassen.
Anexo II 4.2.6.BAJO.c)	wafv2-logging-enabled	Um die Protokollierung und Überwachung in Ihrer Umgebung zu erleichtern, aktivieren Sie die AWS WAF (V2) -Protokollierung im regionalen und globalen Web ACLs. AWS Die WAF-Protokollierung bietet detaillierte Informationen über den Datenverkehr, der von Ihrer Web-ACL analysiert wird. In den Protokollen werden die Uhrzeit aufgezeichnet, zu der die AWS WAF die Anfrage von Ihrer AWS Ressource erhalten hat, Informationen über die Anfrage und eine Aktion für die Regel, der jede Anfrage entsprach.

Kontroll-ID	AWS Config	Empfehlungen
Anexo II 4.2.6.BAJO.c)	api-gw-execution-logging-aktiviert	Die API-Gateway-Protokollierung zeigt detaillierte Ansichten der Benutzer, die auf die API zugegriffen haben, und wie diese Benutzer auf die API zugegriffen haben. Diese Einblicke ermöglichen die Transparenz von Benutzeraktivitäten.
Anexo II 4.2.6.BAJO.c)	cloud-trail-cloud-watch-logs-aktiviert	Verwenden Sie Amazon CloudWatch , um Protokollereignisaktivitäten zentral zu sammeln und zu verwalten . Die Aufnahme von AWS CloudTrail Daten liefert Einzelheiten zu den API-Aufrufaktivitäten in Ihrem AWS-Konto.

Kontroll-ID	AWS Config	Empfehlungen
Anexo II 4.2.6.BAJO.c)	cloudtrail-enabled	AWS CloudTrail kann bei der Nichtabstreitbarkeit helfen, indem Aktionen und API-Aufrufe der AWS Managemen t Console aufgezeichnet werden. Sie können die Benutzer und die Benutzer AWS-Konten , die einen AWS Dienst aufgerufen haben, die Quell-IP-Adresse, über die die Aufrufe generiert wurden, und den Zeitpunkt der Anrufe identifizieren. Einzelheiten zu den erfassten Daten finden Sie in den AWS CloudTrail Datensatzinhalten.
Anexo II 4.2.6.BAJO.c)	cloudtrail-s3-dataevents-en abled	Die Erfassung von Simple Storage Service (Amazon S3)-Datenereignissen unterstützt die Erkennung von ungewöhnl ichen Aktivitäten. Zu den Details gehören AWS-Konto Informationen über den Zugriff auf einen Amazon S3 S3-Bucket, die IP-Adresse und die Uhrzeit des Ereignisses.

Kontroll-ID	AWS Config	Empfehlungen
Anexo II 4.2.6.BAJO.c)	elb-logging-enabled	Die Elastic-Load-Balancing-Aktivität ist ein zentraler Kommunikationspunkt innerhalb einer Umgebung. Stellen Sie sicher, dass die ELB-Protokollierung aktiviert ist. Die gesammelten Daten enthalten detaillierte Informationen zu Anfragen, die an den ELB gesendet wurden. Jedes Protokoll enthält Informationen wie die Zeit, zu der die Anforderung einging, die Client-IP-Adresse, Latenzen, Anforderungspfade und Serverantworten.
Anexo II 4.2.6.BAJO.c)	opensearch-logs-to-cloudwatch	Stellen Sie sicher, dass für Amazon OpenSearch Service-Domains Fehlerprotokolle aktiviert und zur Aufbewahrung und Beantwortung an Amazon CloudWatch Logs gestreamt werden. OpenSearch Service-Fehlerprotokolle können bei Sicherheits- und Zugriffsprüfungen helfen und bei der Diagnose von Verfügbarkeitsproblemen helfen.

Kontroll-ID	AWS Config	Empfehlungen
Anexo II 4.2.6.BAJO.c)	s-3 bucket-logging-enabled	Die Amazon Simple Storage Service (Amazon S3)-Serve rzugriffsprotokollierung bietet eine Methode zur Überwachung des Netzwerks im Hinblick auf potenzielle Cybersicherheitsereignisse. Die Ereignisse werden überwacht, indem detaillie rte Aufzeichnungen über die Anfragen erfasst werden, die an einen Amazon-S3-Bucket gestellt wurden. Jeder Zugriffsprotokolleintrag enthält Details zu einer einzelnen Zugriffsanfrage. Zu den Details gehören Anfordere r, Bucket-Name, Anforderu ngszeit, Anforderungsaktion, Antwortstatus und Fehlercode, falls relevant.

Kontroll-ID	AWS Config	Empfehlungen
Anexo II 4.2.6.BAJO.c)	vpc-flow-logs-enabled	VPC-Flow-Protokolle erfassen detaillierte Informationsdatensätze über den IP-Datenverkehr, der zu und von Netzwerkschnittstellen in Ihrer Amazon Virtual Private Cloud (Amazon VPC) fließt. Standardmäßig enthalten Flow-Protokolldatensätze Werte für die verschiedenen Komponenten des IP-Flows, einschließlich Quelle, Ziel und Protokoll.
Anexo II 4.2.7.BAJO	iam-user-mfa-enabled	Aktivieren Sie diese Regel, um den Zugriff auf Ressourcen in der AWS Cloud einzuschränken. Diese Regel sorgt dafür, dass die Multi-Faktor-Authentifizierung (MFA) für alle Benutzer aktiviert ist. MFA sorgt für eine weitere Schutzebene zusätzlich zu den Anmeldeinformationen. Reduzieren Sie Fälle von kompromittierten Konten, indem Sie MFA für Benutzer vorschreiben.

Kontroll-ID	AWS Config	Empfehlungen
Anexo II 4.2.7.BAJO	mfa-enabled-for-iam-Konsolenzugriff	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass MFA für alle AWS Identity and Access Management (IAM) -Benutzer aktiviert ist, die über ein Konsolenkennwort verfügen. MFA sorgt für eine weitere Schutzebene zusätzlich zu den Anmeldeinformationen. Indem Sie MFA für Benutzer vorschreiben, können Sie Fälle kompromittierter Konten reduzieren und verhindern, dass unbefugte Benutzer auf vertrauliche Daten zugreifen.
Anexo II 4.2.7.BAJO	root-account-hardware-mfa-aktiviert	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Hardware-MFA für den Root-Benutzer aktiviert ist. Der Stammbenutzer ist der AWS-Konto-Benutzer mit den meisten Berechtigungen. MFA sorgt für eine weitere Schutzebene zusätzlich zu den Anmeldeinformationen. Indem Sie MFA für den Root-Benutzer vorschreiben, können Sie die Anzahl AWS-Konten kompromittierter Benutzer reduzieren.

Kontroll-ID	AWS Config	Empfehlungen
Anexo II 4.2.7.BAJO	root-account-mfa-enabled	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass MFA für den Root-Benutzer aktiviert ist. Der Stammbenutzer ist der AWS-Konto-Benutzer mit den meisten Berechtigungen. MFA sorgt für eine weitere Schutzebene zusätzlich zu den Anmeldeinformationen. Indem Sie MFA für den Root-Benutzer vorschreiben, können Sie die Anzahl AWS-Konten kompromittierter Benutzer reduzieren.
Anexo II 4.3.1	ec2-check managedinstance-association-compliance-status	Verwenden Sie AWS Systems Manager Associations, um bei der Inventarisierung von Softwareplattformen und Anwendungen innerhalb eines Unternehmens zu helfen. AWS Systems Manager weist Ihren verwalteten Instanzen einen Konfigurationsstatus zu und ermöglicht es Ihnen, Basiswerte für Betriebssystem-Patch-Levels, Softwareinstallationen, Anwendungskonfigurationen und andere Details zu Ihrer Umgebung festzulegen.

Kontroll-ID	AWS Config	Empfehlungen
Anexo II 4.3.1	ec2-stopped-instance	Aktivieren Sie diese Regel, um bei der Basiskonfiguration von Amazon Elastic Compute Cloud (Amazon EC2) - Instances zu helfen, indem Sie überprüfen, ob EC2 Amazon-Instances gemäß den Standards Ihrer Organisation für mehr als die zulässige Anzahl von Tagen gestoppt wurden.
Anexo II 4.3.1	ec2- volume-inuse-check	Diese Regel stellt sicher, dass Amazon Elastic Block Store-Volumes, die an Amazon Elastic Compute Cloud (Amazon EC2) -Instances angehängt sind, zum Löschen markiert werden, wenn eine Instance beendet wird. Wenn ein Amazon-EBS-Volume nicht gelöscht wird, wenn die Instance, an die es angehängt ist, beendet wird, kann dies gegen das Konzept der geringsten Funktionalität verstoßen.

Kontroll-ID	AWS Config	Empfehlungen
Anexo II 4.3.1	eip-attached	Diese Regel stellt sicher, dass Elastic, die einer Amazon Virtual Private Cloud (Amazon VPC) IPs zugewiesen sind, an Amazon Elastic Compute Cloud (Amazon EC2) - Instances oder verwendete Elastic Network Interfaces angehängt sind. Diese Regel hilft bei der Überwachung ungenutzter Inhalte EIPs in Ihrer Umgebung.
Anexo II 4.3.1	vpc-network-acl-unused-überprüfen	Diese Regel stellt sicher, dass Amazon Virtual Private Cloud (VPC)-Netzwerkzugriffskontrolllisten verwendet werden. Die Überwachung ungenutzter Netzwerkzugriffskontrolllisten kann zu einer genauen Inventarisierung und Verwaltung Ihrer Umgebung beitragen.

Kontroll-ID	AWS Config	Empfehlungen
Anexo II 4.3.2.b)	alb-waf-enabled	Stellen Sie sicher, dass AWS WAF auf Elastic Load Balancers (ELB) aktiviert ist, um Webanwendungen zu schützen. Eine WAF trägt zum Schutz Ihrer Webanwendungen oder APIs vor gängigen Web-Exploits bei. Diese Web-Exploits können sich auf die Verfügbarkeit auswirken, die Sicherheit gefährden oder übermäßige Ressourcen in Ihrer Umgebung verbrauchen.
Anexo II 4.3.2.b)	api-gw-associated-with-WAF	AWS Mit WAF können Sie eine Reihe von Regeln (als Web Access Control List (Web ACL) bezeichnet) konfigurieren, die Webanfragen auf der Grundlage von anpassbaren Websicherheitsregeln und -bedingungen, die Sie definieren, zulassen, blockieren oder zählen. Stellen Sie sicher, dass Ihre Amazon-API-Gateway-Stufe mit einer WAF-Web-ACL verknüpft ist, um sie vor böswilligen Angriffen zu schützen.

Kontroll-ID	AWS Config	Empfehlungen
Anexo II 4.3.2.b)	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) Security Groups können bei der Verwaltung des Netzwerkz ugriffs helfen, indem sie eine statusbehaftete Filterung von eingehendem und ausgehend em Netzwerkverkehr zu Ressourcen bereitstellen. AWS Wenn Sie eingehenden (oder entfernten) Datenverk ehr von 0.0.0.0/0 bis Port 22 auf Ihren Ressourcen nicht zulassen, können Sie den Remote-Zugriff einschränken.
Anexo II 4.3.2.b)	no-unrestricted-route-to-igw	Stellen Sie sicher, dass EC2 Amazon-Routentabellen keine uneingeschränkten Routen zu einem Internet-Gateway enthalten. Durch das Entfernen oder Beschränk en des Internetzugangs für Workloads innerhalb von Amazon VPCs können unbeabsichtigte Zugriffe in Ihrer Umgebung reduziert werden.

Kontroll-ID	AWS Config	Empfehlungen
Anexo II 4.3.2.b)	ssm-document-not-public	Stellen Sie sicher, dass AWS Systems Manager (SSM) - Dokumente nicht öffentlich sind, da dies einen unbeabsichtigten Zugriff auf Ihre SSM-Dokumente ermöglichen kann. Ein öffentliches SSM-Dokument kann Informationen über Ihr Konto, Ihre Ressourcen und internen Prozesse preisgeben.
Anexo II 4.3.2.b)	dms-replication-not-public	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass auf DMS-Replikationsinstanzen nicht öffentlich zugegriffen werden kann. DMS-Replikations-Instances können vertrauliche Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.
Anexo II 4.3.2.b)	ebs-snapshot-public-restorable-überprüfen	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass EBS-Snapshots nicht öffentlich wiederherstellbar sind. EBS-Volume-Snapshots können vertrauliche Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	AWS Config	Empfehlungen
Anexo II 4.3.2.b)	ec-2 instance-no-public-ip	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon Elastic Compute Cloud (Amazon EC2) -Instances nicht öffentlich zugänglich sind. EC2 Amazon-Instances können vertrauliche Informati onen enthalten, und für solche Konten ist eine Zugriffsk ontrolle erforderlich.
Anexo II 4.3.2.b)	elasticsearch-in-vpc-only	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass sich Amazon OpenSearch OpenSearch Service (Service) -Domains innerhalb einer Amazon Virtual Private Cloud (Amazon VPC) befinden. Eine OpenSearch Service-D omain innerhalb einer Amazon VPC ermöglicht die sichere Kommunikation zwischen OpenSearch Service und anderen Services innerhalb der Amazon VPC, ohne dass ein Internet-Gateway, ein NAT-Gerät oder eine VPN-Verbindung erforderlich ist.

Kontroll-ID	AWS Config	Empfehlungen
Anexo II 4.3.2.b)	emr-master-no-public-ip	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon EMR-Cluster-Masterknoten nicht öffentlich zugänglich sind. Amazon-EMR-Cluster-Hauptknoten können vertrauliche Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.
Anexo II 4.3.2.b)	internet-gateway-authorized-vpc-nur	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Internet-Gateways nur mit autorisierter Amazon Virtual Private Cloud (Amazon VPC) verbunden sind. Internet-Gateways ermöglichen den bidirektionalen Internetzugang zur und von der Amazon VPC, was möglicherweise zu einem unbefugten Zugriff auf Amazon-VPC-Ressourcen führen kann.

Kontroll-ID	AWS Config	Empfehlungen
Anexo II 4.3.2.b)	lambda-function-public-access-verboten	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass AWS Lambda-Funktionen nicht öffentlich zugänglich sind. Der öffentliche Zugriff kann möglicherweise die Verfügbarkeit von Ressourcen beeinträchtigen.

Kontroll-ID	AWS Config	Empfehlungen
Anexo II 4.3.2.b)	lambda-inside-vpc	Stellen Sie AWS Lambda-Funktionen in einer Amazon Virtual Private Cloud (Amazon VPC) bereit, um eine sichere Kommunikation zwischen einer Funktion und anderen Diensten innerhalb der Amazon VPC zu gewährleisten. Bei dieser Konfiguration sind kein Internet-Gateway, kein NAT-Gerät und keine VPN-Verbindung erforderlich. Der gesamte Datenverkehr bleibt sicher in der Cloud. AWS Domains, die sich innerhalb einer VPC befinden, verfügen aufgrund ihrer logischen Isolierung im Vergleich zu Domains mit öffentlichen Endpunkten über eine zusätzliche Sicherheitsebene. Um den Zugriff ordnungsgemäß zu verwalten, sollten AWS Lambda-Funktionen einer VPC zugewiesen werden.

Kontroll-ID	AWS Config	Empfehlungen
Anexo II 4.3.2.b)	opensearch-in-vpc-only	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass sich Amazon OpenSearch Service-Domains innerhalb einer Amazon Virtual Private Cloud (Amazon VPC) befinden. Eine Amazon OpenSearch Service-Domain innerhalb einer Amazon VPC ermöglich t die sichere Kommunika tion zwischen Amazon OpenSearch Service und anderen Services innerhalb der Amazon VPC, ohne dass ein Internet-Gateway, ein NAT-Gerät oder eine VPN-Verbindung erforderlich ist.
Anexo II 4.3.2.b)	rds-instance-public-access-überprüfen	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherste llen, dass Amazon Relationa l Database Service (Amazon RDS) -Instances nicht öffentlic h sind. Amazon-RDS-Datenba nk-Instances können vertrauli che Informationen enthalten und für solche Konten sind Prinzipien und Zugriffsk ontrollen erforderlich.

Kontroll-ID	AWS Config	Empfehlungen
Anexo II 4.3.2.b)	rds-snapshots-public-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Relational Database Service (Amazon RDS) -Instances nicht öffentlich sind. Amazon-RDS-Datenbank-Instances können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.
Anexo II 4.3.2.b)	redshift-cluster-public-access-überprüfen	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Redshift Redshift-Cluster nicht öffentlich sind. Amazon-Redshift-Cluster können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	AWS Config	Empfehlungen
Anexo II 4.3.2.b)	restricted-common-ports	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass gemeinsame Ports für Amazon Elastic Compute Cloud (Amazon EC2) - Sicherheitsgruppen eingeschränkt sind. Wenn der Zugriff auf Ports nicht auf vertrauenswürdige Quellen beschränkt wird, kann dies zu Angriffen auf die Verfügbarkeit, Integrität und Vertraulichkeit von Systemen führen. Mit dieser Regel können Sie optional die Parameter blockedPort1–blockedPort5 festlegen (Standardkonfigurationen: 20, 21, 3389, 3306, 4333). Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	AWS Config	Empfehlungen
Anexo II 4.3.2.b)	s3- account-level-public-access -blöcke-periodisch	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Simple Storage Service (Amazon S3) -Buckets nicht öffentlich zugänglich sind. Diese Regel trägt dazu bei, sensible Daten vor unbefugten Remote-Benutzern zu schützen, indem sie den öffentlichen Zugriff verhindert. Mit dieser Regel können Sie optional die Parameter ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) und restrictPublicBuckets Parameter (Config Default: True) festlegen. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	AWS Config	Empfehlungen
Anexo II 4.3.2.b)	s3 bucket-level-public-access -verboten	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Simple Storage Service (Amazon S3) -Buckets nicht öffentlich zugänglich sind. Diese Regel trägt dazu bei, sensible Daten vor unbefugten Remote-Benutzern zu schützen, indem sie den öffentlichen Zugriff auf Bucket-Ebene verhindert.
Anexo II 4.3.2.b)	s-3 bucket-public-read-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie nur autorisierten Benutzern, Prozessen und Geräten Zugriff auf Amazon Simple Storage Service (Amazon S3) -Buckets gewähren. Die Verwaltung des Zugriffs sollte mit der Klassifizierung der Daten übereinstimmen.

Kontroll-ID	AWS Config	Empfehlungen
Anexo II 4.3.2.b)	s3- bucket-public-write-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie nur autorisierten Benutzern, Prozessen und Geräten Zugriff auf Amazon Simple Storage Service (Amazon S3) -Buckets gewähren. Die Verwaltung des Zugriffs sollte mit der Klassifizierung der Daten übereinstimmen.
Anexo II 4.3.2.b)	sagemaker-notebook-no-direct-Internetzugang	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass SageMaker Amazon-Notebooks keinen direkten Internetzugang zulassen. Indem Sie direkten Internetzugang blockieren, vermeiden Sie, dass unbefugte Benutzer auf sensible Daten zugreifen.

Kontroll-ID	AWS Config	Empfehlungen
Anexo II 4.3.2.b)	subnet-auto-assign-public-ip-deaktiviert	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon Virtual Private Cloud (VPC) -Subnetzen nicht automatis ch eine öffentliche IP-Adress e zugewiesen wird. Amazon Elastic Compute Cloud (EC2) -Instances, die in Subnetzen gestartet werden, in denen dieses Attribut aktiviert ist, haben ihrer primären Netzwerkschnittste lle eine öffentliche IP-Adresse zugewiesen.
Anexo II 4.3.2.b)	vpc-default-security-group-geschlossen	Sicherheitsgruppen von Amazon Elastic Compute Cloud (Amazon EC2) können bei der Verwaltung des Netzwerkzugriffs helfen, indem sie eine statusbeh aftete Filterung des ein- und ausgehenden Netzwerkv erkehrs zu Ressourcen bereitstellen. AWS Die Beschränkung des gesamten Datenverkehrs auf die Standardsicherheitsgruppe hilft dabei, den Fernzugriff auf Ihre Ressourcen einzuschr änken. AWS

Kontroll-ID	AWS Config	Empfehlungen
Anexo II 4.3.2.b)	vpc-sg-open-only-to-authorized-ports	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass gemeinsame Ports für Amazon Elastic Compute Cloud (Amazon EC2) - Sicherheitsgruppen eingeschränkt sind. Wenn der Zugriff auf Ports nicht auf vertrauenswürdige Quellen beschränkt wird, kann dies zu Angriffen auf die Verfügbarkeit, Integrität und Vertraulichkeit von Systemen führen. Durch die Beschränkung des Zugriffs auf Ressourcen innerhalb einer Sicherheitsgruppe aus dem Internet (0.0.0.0/0) kann der Remote-Zugriff auf interne Systeme gesteuert werden.

Kontroll-ID	AWS Config	Empfehlungen
Anexo II 4.3.4.c)	vuln-management-plan-exists (Prozessüberprüfung)	Stellen Sie sicher, dass ein Plan für das Schwachst ellenmanagement entwickel t und implementiert wird, damit Sie über formell definiert e Prozesse zur Behebung von Schwachstellen in Ihrer Umgebung verfügen. Dazu zählen Tools für das Schwachstellenmanagement, regelmäßige Umgebungs scans sowie entsprechende Rollen und Verantwortlichkeit en.
Anexo II 4.3.8.BAJO	elasticsearch-logs-to-cloud watch	Stellen Sie sicher, dass für Amazon OpenSearch Service-Domains Fehlerprotokolle aktiviert und zur Aufbewahr ung und Beantwortung an Amazon CloudWatch Logs gestreamt werden. Domain-Fehlerprotokolle sind bei Sicherheits- und Zugriffsp rüfungen sowie bei der Diagnose von Verfügbar keitsproblemen nützlich.

Kontroll-ID	AWS Config	Empfehlungen
Anexo II 4.3.8.BAJO	multi-region-cloudtrail-enabled	AWS CloudTrail zeichnet Aktionen und API-Aufrufe der AWS Management Console auf. Sie können feststellen, welche Benutzer und Konten angerufen wurden AWS, von welcher Quell-IP-Adresse aus die Anrufe getätigt wurden und wann die Anrufe erfolgten . CloudTrail übermittelt Protokolldateien aus allen AWS Regionen an Ihren S3-Bucket, wenn MULTI_REGION_CLOUD_TRAIL_ENABLED aktiviert ist. Außerdem wird beim AWS Start einer neuen Region derselbe Trail in der neuen Region erstellt. CloudTrail Dadurch erhalten Sie automatisch Protokoll dateien mit API-Aktivitäten für die neue Region.

Kontroll-ID	AWS Config	Empfehlungen
Anexo II 4.3.8.BAJO	rds-logging-enabled	Um die Protokollierung und Überwachung in Ihrer Umgebung zu erleichtern, stellen Sie sicher, dass die Amazon Relational Database Service (Amazon RDS)-Protokollierung aktiviert ist. Mit der Amazon-RDS-Protokollierung können Sie Ereignisse wie Verbindungen, Verbindungsabbrüche, Abfragen oder abgefragte Tabellen erfassen.
Anexo II 4.3.8.BAJO	wafv2-logging-enabled	Um die Protokollierung und Überwachung in Ihrer Umgebung zu erleichtern, aktivieren Sie die AWS WAF (V2) -Protokollierung im regionalen und globalen Web ACLs. AWS Die WAF-Protokollierung bietet detaillierte Informationen über den Datenverkehr, der von Ihrer Web-ACL analysiert wird. In den Protokollen werden die Uhrzeit aufgezeichnet, zu der die AWS WAF die Anfrage von Ihrer AWS Ressource erhalten hat, Informationen über die Anfrage und eine Aktion für die Regel, der jede Anfrage entsprach.

Kontroll-ID	AWS Config	Empfehlungen
Anexo II 4.3.8.BAJO	api-gw-execution-logging-aktiviert	Die API-Gateway-Protokollierung zeigt detaillierte Ansichten der Benutzer, die auf die API zugegriffen haben, und wie diese Benutzer auf die API zugegriffen haben. Diese Einblicke ermöglichen die Transparenz von Benutzeraktivitäten.
Anexo II 4.3.8.BAJO	cloud-trail-cloud-watch-logs-aktiviert	Verwenden Sie Amazon CloudWatch , um Protokollereignisaktivitäten zentral zu sammeln und zu verwalten . Die Aufnahme von AWS CloudTrail Daten liefert Einzelheiten zu den API-Aufrufaktivitäten in Ihrem AWS-Konto.

Kontroll-ID	AWS Config	Empfehlungen
Anexo II 4.3.8.BAJO	cloudtrail-enabled	AWS CloudTrail kann bei der Nichtabstreitbarkeit helfen, indem Aktionen und API-Aufrufe der AWS Managemen t Console aufgezeichnet werden. Sie können die Benutzer und die Benutzer AWS-Konten , die einen AWS Dienst aufgerufen haben, die Quell-IP-Adresse, über die die Aufrufe generiert wurden, und den Zeitpunkt der Anrufe identifizieren. Einzelheiten zu den erfassten Daten finden Sie in den AWS CloudTrail Datensatzinhalten.
Anexo II 4.3.8.BAJO	cloudtrail-s3-dataevents-en abled	Die Erfassung von Simple Storage Service (Amazon S3)-Datenereignissen unterstützt die Erkennung von ungewöhnl ichen Aktivitäten. Zu den Details gehören AWS-Konto Informationen über den Zugriff auf einen Amazon S3 S3-Bucket, die IP-Adresse und die Uhrzeit des Ereignisses.

Kontroll-ID	AWS Config	Empfehlungen
Anexo II 4.3.8.BAJO	elb-logging-enabled	Die Elastic-Load-Balancing-Aktivität ist ein zentraler Kommunikationspunkt innerhalb einer Umgebung. Stellen Sie sicher, dass die ELB-Protokollierung aktiviert ist. Die gesammelten Daten enthalten detaillierte Informationen zu Anfragen, die an den ELB gesendet wurden. Jedes Protokoll enthält Informationen wie die Zeit, zu der die Anforderung einging, die Client-IP-Adresse, Latenzen, Anforderungspfade und Serverantworten.
Anexo II 4.3.8.BAJO	opensearch-logs-to-cloudwatch	Stellen Sie sicher, dass für Amazon OpenSearch Service-Domains Fehlerprotokolle aktiviert und zur Aufbewahrung und Beantwortung an Amazon CloudWatch Logs gestreamt werden. OpenSearch Service-Fehlerprotokolle können bei Sicherheits- und Zugriffsprüfungen helfen und bei der Diagnose von Verfügbarkeitsproblemen helfen.

Kontroll-ID	AWS Config	Empfehlungen
Anexo II 4.3.8.BAJO	s-3 bucket-logging-enabled	Die Amazon Simple Storage Service (Amazon S3)-Serverzugriffsprotokollierung bietet eine Methode zur Überwachung des Netzwerks im Hinblick auf potenzielle Cybersicherheitsereignisse. Die Ereignisse werden überwacht, indem detaillierte Aufzeichnungen über die Anfragen erfasst werden, die an einen Amazon-S3-Bucket gestellt wurden. Jeder Zugriffsprotokolleintrag enthält Details zu einer einzelnen Zugriffsanfrage. Zu den Details gehören Anforderer, Bucket-Name, Anforderungszeit, Anforderungsaktion, Antwortstatus und Fehlercode, falls relevant.

Kontroll-ID	AWS Config	Empfehlungen
Anexo II 4.3.8.BAJO	vpc-flow-logs-enabled	VPC-Flow-Protokolle erfassen detaillierte Informationsdatensätze über den IP-Datenverkehr, der zu und von Netzwerkschnittstellen in Ihrer Amazon Virtual Private Cloud (Amazon VPC) fließt. Standardmäßig enthalten Flow-Protokolldatensätze Werte für die verschiedenen Komponenten des IP-Flows, einschließlich Quelle, Ziel und Protokoll.
Anexo II 4.3.10.b)	cloud-trail-encryption-enabled	Da sensible Daten vorhanden sein können und um Daten im Ruhezustand zu schützen, sollten Sie sicherstellen, dass die Verschlüsselung für Ihre AWS CloudTrail Trails aktiviert ist.

Kontroll-ID	AWS Config	Empfehlungen
Anexo II 4.3.10.b)	cloud-trail-log-file-Validierung aktiviert	Verwenden Sie die AWS CloudTrail Protokolldateivalidierung, um die Integrität von Protokollen zu überprüfen. CloudTrail Mithilfe der Protokolldateivalidierung kann festgestellt werden, ob eine Protokolldatei geändert oder gelöscht wurde oder ob sie nach der Übermittlung CloudTrail unverändert geblieben ist. Dieses Feature wurde mit dem Branchenstandard entsprechenden Algorithmen entwickelt: SHA-256 für die Hashfunktion und SHA-256 mit RSA für digitale Signaturen. Aus diesem Grund ist es rechnerisch unmöglich, CloudTrail Protokolldateien unbemerkt zu ändern, zu löschen oder zu fälschen.

Kontroll-ID	AWS Config	Empfehlungen
Anexo II 4.3.10.d)	s-3 bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) unterstützt die Aufrechte rhaltung einer angemessenen Kapazität und Verfügbarkeit. CRR ermöglicht das automatis che, asynchrone Kopieren von Objekten in Amazon-S3 -Buckets, um die Datenverf ügbarkeit sicherzustellen.
Anexo II 4.6.1	guardduty-enabled-centralized	Amazon GuardDuty kann mithilfe von Threat Intellige nce Feeds helfen, potenzielle Cybersicherheitsereignisse zu überwachen und zu erkennen. Dazu gehören Listen mit bösartigen IPs und maschinel len Lernmethoden zur Identifiz ierung unerwarteter, nicht autorisierter und bösartige r Aktivitäten in Ihrer AWS Cloud-Umgebung.

Kontroll-ID	AWS Config	Empfehlungen
Anexo II 4.6.2.BASICA	securityhub-enabled	AWS Security Hub hilft bei der Überwachung von unbefugte m Personal, Verbindungen, Geräten und Software. AWS Security Hub aggregiert, organisiert und priorisiert die Sicherheitswarnungen oder Ergebnisse mehrerer Dienste. AWS Einige dieser Dienste sind Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer und AWS Firewall Manager sowie AWS Partnerlösungen.
Anexo II 5.2.3	security-awareness-program-exists (Prozessüberprüfung)	Etablieren und pflegen Sie ein Programm zur Förderung des Sicherheitsbewusst seins in Ihrer Organisation. Programme zur Förderung des Sicherheitsbewusstseins der Mitarbeiter vermitteln ihnen, wie sie ihre Organisation vor diversen Sicherheitsverletz ungen oder Sicherheitsvorfäll en schützen können.

Kontroll-ID	AWS Config	Empfehlungen
Anexo II 5.4.3.BAJO.a)	iam-password-policy	Die Identitäten und Anmeldein formationen werden auf der Grundlage einer organisat orischen IAM-Passwortrichtl inie ausgestellt, verwaltet und verifiziert. Sie erfüllen oder übertreffen die Anforderungen von NIST SP 800-63 und dem Standard „Best Practices“ von AWS Foundational Security für die Passwortstärke. Mit dieser Regel können Sie optional RequireUppercaseCharacters (Wert für AWS grundlege nde Sicherheitsbewährte Methoden: wahr), RequireLo wercaseCharacters (Wert für bewährte Methoden für AWS grundlegende Sicherheit: wahr), RequireSymbols (Wert für bewährte Methoden für AWS grundlegende Sicherhei t: wahr), RequireNumbers (Wert für bewährte Methoden für AWS grundlegende Sicherheit: wahr), MinimumPa sswordLength (Wert für bewährte Methoden für AWS grundlegende Sicherheit: 14), PasswordReusePreve ntion (Wert für bewährte Methoden für AWS grundlege nde Sicherheit: 24) und MaxPasswordAge (Wert

Kontroll-ID	AWS Config	Empfehlungen
		für bewährte Methoden für AWS grundlegende Sicherhei t: 90) für Ihr IAM festlegen . Kennwortrichtlinie. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisat ion entsprechen.
Anexo II 5.6.1.c)	codebuild-project-envvar-aw scred-überprüfen	Stellen Sie sicher, dass die Anmeldeinformationen AWS_ACCESS_KEY_ID AWS_SECRET_ACCESS_ KEY nicht in AWS Codebuild -Projektumgebungen vorhanden sind. Speichern Sie diese Variablen nicht als Klartext. Das Speichern dieser Variablen als Klartext bewirkt eine unbeabsichtigte Offenlegung von Daten sowie unberechtigte Zugriffe.

Kontroll-ID	AWS Config	Empfehlungen
Anexo II 5.6.1.c)	codebuild-project-source-repo-URL-Prüfung	Stellen Sie sicher, dass die URL des Quell-Repositorys GitHub oder des Bitbucket -Quell-Repositorys keine persönlichen Zugriffstoken oder Anmeldeinformation en in Codebuild-Projektu mgebungen enthält. AWS Verwende OAuth anstelle von persönlichen Zugriffst oken oder Anmeldedaten die Autorisierung für den Zugriff auf GitHub Bitbucket-Reposito rys.
Anexo II 5.7.3	dynamodb-table-encrypted-km s	Stellen Sie sicher, dass die Verschlüsselung für Ihre Amazon-DynamoDB-Tabellen aktiviert ist. Um eventuell vorhandene sensible Daten im Ruhezustand in diesen Tabellen zu schützen, müssen Sie die Verschlüsselung von Daten im Ruhezustand aktivieren. Standardmäßig werden DynamoDB-Tabellen mit einem AWS eigenen Kundenhauptschlüssel (CMK) verschlüsselt.

Kontroll-ID	AWS Config	Empfehlungen
Anexo II 5.7.3	ec2- ebs-encryption-by-default	Zum Schutz von Daten im Ruhezustand müssen Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon Elastic Block Store (Amazon EBS)-Volumes aktiviert ist. Da sensible Daten auch im Ruhezusta nd vorhanden sein können, sollten Sie die Verschlüs selung im Ruhezustand aktivieren, um diese Daten zu schützen.
Anexo II 5.7.3	elasticsearch-node-to-node-Verschlüsselungsprüfung	Stellen Sie sicher, dass die node-to-node Verschlüsselung für Amazon OpenSearch Service aktiviert ist. Node-to-nodeVerschlüsselung ermöglicht die TLS 1.2-Versc hlüsselung für die gesamte Kommunikation innerhalb der Amazon Virtual Private Cloud (Amazon VPC). Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	AWS Config	Empfehlungen
Anexo II 5.7.3	elb-tls-https-listeners-nur	Stellen Sie sicher, dass Ihre Elastic Load Balancer (ELBs) mit SSL- oder HTTPS-Listenern konfiguriert sind. Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.
Anexo II 5.7.3	rds-snapshot-encrypted	Stellen Sie sicher, dass die Verschlüsselung für Ihre Amazon Relational Database Service (Amazon RDS)-Snapshots aktiviert ist. Da sensible Daten auch im Ruhezustand vorhanden sein können, sollten Sie die Verschlüsselung im Ruhezustand aktivieren, um diese Daten zu schützen.
Anexo II 5.7.3	s-3 default-encryption-kms	Stellen Sie sicher, dass die Verschlüsselung für Ihre Amazon Simple Storage Service (Amazon S3)-Buckets aktiviert ist. Um eventuell vorhandene sensible Daten im Ruhezustand in einem Amazon-S3-Bucket zu schützen, muss die Verschlüsselung aktiviert sein.

Kontroll-ID	AWS Config	Empfehlungen
Anexo II 5.7.3	sagemaker-notebook-instance-kms-key-konfiguriert	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass die Verschlüsselung mit dem AWS Key Management Service (AWS KMS) für Ihr Notebook aktiviert ist. SageMaker Da vertrauliche Daten im SageMaker Notebook gespeichert werden können, sollten Sie die Verschlüsselung im Ruhezustand aktivieren, um diese Daten zu schützen.
Anexo II 5.7.3	sns-encrypted-kms	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass Ihre Amazon Simple Notification Service (Amazon SNS) -Themen mit dem AWS Key Management Service (AWS KMS) verschlüsselt werden müssen. Um eventuell vorhandene sensible Daten im Ruhezustand in veröffentlichten Nachrichten zu schützen, muss die Verschlüsselung von Daten im Ruhezustand aktiviert sein.

Kontroll-ID	AWS Config	Empfehlungen
Anexo II 5.7.3	alb-http-to-https-Umleitung sprüfung	Um Daten während der Übertragung zu schützen, stellen Sie sicher, dass Ihr Application Load Balancer unverschlüsselte HTTP-Anfragen automatisch an HTTPS umleitet. Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.
Anexo II 5.7.3	api-gw-cache-enabled-und-ve rschlüsselt	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass die Verschlüsselung für den Cache Ihrer API-Gatew ay-Stufe aktiviert ist. Da für die API-Methode sensible Daten erfasst werden können, sollten Sie die Verschlüsselung von Daten im Ruhezustand aktivieren, um diese Daten zu schützen.
Anexo II 5.7.3	api-gw-ssl-enabled	Stellen Sie sicher, dass die REST-API-Stufen von Amazon API Gateway mit SSL-Zerti fikaten konfiguriert sind, damit Backend-Systeme überprüfe n können, ob Anforderungen von API Gateway stammen.

Kontroll-ID	AWS Config	Empfehlungen
Anexo II 5.7.3	cloud-trail-encryption-enabled	Da sensible Daten vorhanden sein können und um Daten im Ruhezustand zu schützen, sollten Sie sicherstellen, dass die Verschlüsselung für Ihre AWS CloudTrail Trails aktiviert ist.
Anexo II 5.7.3	cloudwatch-log-group-encrypted	Um sensible Daten im Ruhezustand zu schützen, stellen Sie sicher, dass die Verschlüsselung für Ihre Amazon CloudWatch Log Groups aktiviert ist.
Anexo II 5.7.3	efs-encrypted-check	Aktivieren Sie die Verschlüsselung für Ihr Amazon Elastic File System (EFS), um eventuell vorhandene sensible Daten sowie Daten im Ruhezustand zu schützen.
Anexo II 5.7.3	elasticsearch-encrypted-at-rest	Da sensible Daten vorhanden sein können und um Daten im Ruhezustand zu schützen, sollten Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon OpenSearch Service (OpenSearch Service) -Domains aktiviert ist.

Kontroll-ID	AWS Config	Empfehlungen
Anexo II 5.7.3	elb-acm-certificate-required	Zum Schutz von eventuell vorhandenen sensiblen Daten sowie von Daten während der Übertragung muss die Verschlüsselung für Ihr Elastic Load Balancing aktiviert sein. Verwenden Sie AWS Certifica te Manager, um öffentlic he und private SSL/TLS-Z ertifikate mit AWS Diensten und internen Ressourcen zu verwalten, bereitzustellen und bereitzustellen.
Anexo II 5.7.3	encrypted-volumes	Aktivieren Sie die Verschlüs selung für Ihre Amazon-El astic-Block-Store (Amazon-EBS)-Volumes, um eventuell vorhandene sensible Daten sowie Daten im Ruhezustand zu schützen.
Anexo II 5.7.3	opensearch-encrypted-at-rest	Da sensible Daten vorhanden sein können und um Daten im Ruhezustand zu schützen, sollten Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon OpenSearch Service-Domains aktiviert ist.

Kontroll-ID	AWS Config	Empfehlungen
Anexo II 5.7.3	opensearch-node-to-node-Verschlüsselungsprüfung	Stellen Sie sicher, dass die node-to-node Verschlüsselung für Amazon OpenSearch Service aktiviert ist. Node-to-nodeVerschlüsselung ermöglicht die TLS 1.2-Verschlüsselung für die gesamte Kommunikation innerhalb der Amazon Virtual Private Cloud (Amazon VPC). Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.
Anexo II 5.7.3	rds-storage-encrypted	Zum Schutz von Daten im Ruhezustand müssen Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon Relational Database Service (Amazon RDS)-Instances aktiviert ist. Um eventuell vorhandene sensible Daten im Ruhezustand in Amazon-RDS-Instances zu schützen, muss die Verschlüsselung von Daten im Ruhezustand aktiviert sein.

Kontroll-ID	AWS Config	Empfehlungen
Anexo II 5.7.3	redshift-cluster-configuration-check	Um Daten im Ruhezustand zu schützen, muss die Verschlüsselung für Ihre Amazon-Redshift-Cluster aktiviert sein. Sie müssen auch sicherstellen, dass die erforderlichen Konfigurationen auf Amazon-Redshift-Clustern bereitgestellt werden. Die Prüfungsprotokollierung muss aktiviert sein, um Informationen zu Verbindungen und Benutzeraktivitäten in der Datenbank bereitzustellen. Diese Regel erfordert, dass ein Wert für clusterDbEncrypted (Config Default: TRUE) und LoggingEnabled (Config Default: TRUE) gesetzt ist. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	AWS Config	Empfehlungen
Anexo II 5.7.3	redshift-cluster-kms-enabled	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass die Verschlüsselung mit AWS Key Management Service (AWS KMS) für Ihren Amazon Redshift Redshift-Cluster aktiviert ist. Um eventuell vorhandene sensible Daten im Ruhezustand in Redshift-Clustern zu schützen, muss die Verschlüsselung von Daten im Ruhezustand aktiviert sein.
Anexo II 5.7.3	redshift-require-tls-ssl	Stellen Sie sicher, dass Ihre Amazon-Redshift-Cluster eine TLS/SSL-Verschlüsselung erfordern, um eine Verbindun g zu SQL-Clients herzustel len. Um eventuell vorhanden e sensible Daten zu schützen, sollten Sie die Verschlüs selung bei der Übertragung aktivieren.

Kontroll-ID	AWS Config	Empfehlungen
Anexo II 5.7.3	s3- aktiviert bucket-server-side -encryption	Zum Schutz von Daten im Ruhezustand müssen Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon Simple Storage Service (Amazon S3)-Bucke ts aktiviert ist. Um eventuell vorhandene sensible Daten im Ruhezustand in Amazon-S3 -Buckets zu schützen, muss die Verschlüsselung aktiviert sein.
Anexo II 5.7.3	s-3 bucket-ssl-requests-only	Um Daten während der Übertragung zu schützen, stellen Sie sicher, dass Ihre Amazon Simple Storage Service (Amazon S3)-Bucke ts Anfragen zur Verwendun g von Secure Socket Layer (SSL)-Buckets erfordern. Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	AWS Config	Empfehlungen
Anexo II 5.7.3	sagemaker-endpoint-configuration-kms-key-konfiguriert	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass die Verschlüsselung mit dem AWS Key Management Service (AWS KMS) für Ihren Endpunkt aktiviert ist. SageMaker Da sensible Daten auf dem SageMaker Endgerät gespeichert werden können, sollten Sie die Verschlüsselung im Ruhezustand aktivieren, um diese Daten zu schützen.
Anexo II 5.7.3	secretsmanager-using-cmk	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass die Verschlüsselung mit dem AWS Key Management Service (AWS KMS) für AWS Secrets Manager aktiviert ist. Aktivieren Sie die Verschlüsselung von Daten im Ruhezustand, um eventuell vorhandene sensible Daten im Ruhezustand im Secrets Manager zu schützen.
Anexo II 5.7.4	cmk-backing-key-rotation-aktiviert	Aktivieren Sie die Schlüssel rotation, um sicherzustellen, dass Schlüssel rotiert werden, nachdem sie das Ende ihrer Krypto-Periode erreicht haben.

Kontroll-ID	AWS Config	Empfehlungen
Anexo II 5.7.4	kms-cmk-not-scheduled-zum Löschen	Um Daten im Ruhezustand zu schützen, sollten Sie sicherstellen, dass die für den Kunden erforderlichen Masterschlüssel (CMKs) nicht für das Löschen im AWS Key Management Service (AWS KMS) vorgesehen sind. Da Schlüssel manchmal gelöscht werden müssen, können Sie mit dieser Regel alle zu löschenden Schlüssel überprüfen, falls ein Schlüssel versehentlich zur Löschung vorgemerkt wurde.
Anexo II 5.8.2	alb-waf-enabled	Stellen Sie sicher, dass AWS WAF auf Elastic Load Balancers (ELB) aktiviert ist, um Webanwendungen zu schützen. Eine WAF trägt zum Schutz Ihrer Webanwendungen oder APIs vor gängigen Web-Exploits bei. Diese Web-Exploits können sich auf die Verfügbarkeit auswirken, die Sicherheit gefährden oder übermäßige Ressourcen in Ihrer Umgebung verbrauchen.

Kontroll-ID	AWS Config	Empfehlungen
Anexo II 5.8.2	api-gw-associated-with-WAF	AWS Mit WAF können Sie eine Reihe von Regeln (als Web Access Control List (Web ACL) bezeichnet) konfiguri eren, die Webanfragen auf der Grundlage von anpassbar en Websicherheitsregeln und -bedingungen, die Sie definieren, zulassen, blockiere n oder zählen. Stellen Sie sicher, dass Ihre Amazon-API-Gateway-Stufe mit einer WAF-Web-ACL verknüpft ist, um sie vor böswilligen Angriffen zu schützen.
Art. 14.4	iam-root-access-key-überprü fen	Der Zugriff auf Systeme und Ressourcen kann gesteuert werden, indem überprüft wird, ob der Root-Benutzer keine Zugriffsschlüssel mit seiner AWS Identity and Access Management (IAM) -Rolle verknüpft hat. Stellen Sie sicher, dass die Root-Zugr iffsschlüssel gelöscht werden. Erstellen und verwenden Sie stattdessen rollenbasierte Funktionen, AWS-Konten um das Prinzip der geringsten Funktionalität zu berücksic htigen.

Kontroll-ID	AWS Config	Empfehlungen
Art. 16	ecs-task-definition-user-for-host-mode-check	Wenn für eine Aufgabend efinition erhöhte Berechtig ungen gelten, liegt das daran, dass der Kunde diesen Konfigurationen ausdrücklich zugestimmt hat. Diese Kontrolle prüft, ob eine unerwartete Berechtig ungseskalation vorliegt, wenn für eine Aufgabendefinition das Host-Netzwerk aktiviert ist, die Kunden aber keine erhöhten Berechtigungen aktiviert haben.
Art. 16	iam-policy-no-statements-with-full-access	Stellen Sie sicher, dass IAM-Aktionen nur auf die benötigte n Aktionen beschränkt sind. Wenn Benutzern mehr Rechte eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und der Aufgabentrennung verstoßen.

Kontroll-ID	AWS Config	Empfehlungen
Art. 16	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) kann Ihnen dabei helfen, die Prinzipien der geringsten Rechte und der Aufgabent rennung in Zugriffsberechtigu ngen und Autorisierungen zu integrieren und zu verhinder n, dass Richtlinien „Effect“: „Allow“ mit „Action“: „*“ anstelle von „Resource“: „*“ enthalten. Wenn Benutzern mehr Rechte eingeräumt werden, als für die Ausführun g einer Aufgabe erforderl ich sind, kann dies gegen das Prinzip der geringste n Berechtigung und der Aufgabentrennung verstoßen.
Art. 16	s3- bucket-policy-grantee-check	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie s3_ bucket_policy_grantee_check aktivieren. Diese Regel prüft, ob der vom Amazon S3 S3-Bucket gewährte Zugriff durch die von Ihnen bereitgestellten AWS Principals, Verbundbe nutzer, Service Principals, IP-Adressen oder Amazon Virtual Private Cloud (Amazon VPC) IDs eingeschränkt ist.

Kontroll-ID	AWS Config	Empfehlungen
Art. 20.2	rds-automatic-minor-version-Upgrade aktiviert	Aktivieren Sie automatische Unterversions-Upgrades auf Ihren Amazon-Relational-Database-Service (RDS)-Instances, um sicherzustellen, dass die aktuellen Updates für Unterversionen des Relational Database Management System (RDBMS) installiert sind, die Sicherheitspatches und Bugfixes enthalten können.
Art. 20.2	ec2- prüfen managedinstance-patch-compliance-status	Aktivieren Sie diese Regel, um bei der Identifizierung und Dokumentation von Sicherheitslücken in Amazon Elastic Compute Cloud (Amazon EC2) zu helfen. Die Regel prüft, ob die EC2 Amazon-Instance die Patch-Konformität im AWS Systems Manager gemäß den Richtlinien und Verfahren Ihrer Organisation einhält.

Kontroll-ID	AWS Config	Empfehlungen
Art. 20.2	elastic-beanstalk-managed-updates-aktiviert	Durch die Aktivierung verwalteter Plattformupdates für eine Amazon-Elastic-Beanstalk-Umgebung wird sichergestellt, dass die aktuellen verfügbaren Plattform-Fixes, -Updates und -Features für die Umgebung installiert sind. Eine bewährte Methode zur Sicherung von Systemen besteht darin, stets die aktuellen Patches zu installieren.
Art. 20.2	vuln-management-plan-exists (Prozessüberprüfung)	Stellen Sie sicher, dass ein Plan für das Schwachstellenmanagement entwickelt und implementiert wird, damit Sie über formell definierte Prozesse zur Behebung von Schwachstellen in Ihrer Umgebung verfügen. Dazu zählen Tools für das Schwachstellenmanagement, regelmäßige Umgebungsscans sowie entsprechende Rollen und Verantwortlichkeiten.

Kontroll-ID	AWS Config	Empfehlungen
Art. 21.1	dynamodb-table-encrypted-kms	Stellen Sie sicher, dass die Verschlüsselung für Ihre Amazon-DynamoDB-Tabellen aktiviert ist. Um eventuell vorhandene sensible Daten im Ruhezustand in diesen Tabellen zu schützen, müssen Sie die Verschlüsselung von Daten im Ruhezustand aktivieren. Standardmäßig werden DynamoDB-Tabellen mit einem AWS eigenen Kundenhauptschlüssel (CMK) verschlüsselt.
Art. 21.1	ec2- ebs-encryption-by-default	Zum Schutz von Daten im Ruhezustand müssen Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon Elastic Block Store (Amazon EBS)-Volumes aktiviert ist. Da sensible Daten auch im Ruhezustand vorhanden sein können, sollten Sie die Verschlüsselung im Ruhezustand aktivieren, um diese Daten zu schützen.

Kontroll-ID	AWS Config	Empfehlungen
Art. 21.1	elasticsearch-node-to-node-Verschlüsselungsprüfung	Stellen Sie sicher, dass die node-to-node Verschlüsselung für Amazon OpenSearch Service aktiviert ist. Node-to-nodeVerschlüsselung ermöglicht die TLS 1.2-Versc hlüsselung für die gesamte Kommunikation innerhalb der Amazon Virtual Private Cloud (Amazon VPC). Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.
Art. 21.1	elb-cross-zone-load-Balancing aktiviert	Aktivieren Sie zonenüber greifendes Load Balancing für Ihre Elastic Load Balancer (ELBs), um eine angemesse ne Kapazität und Verfügbar keit aufrechtzuerhalten. Zonenübergreifendes Load Balancing reduziert die Notwendigkeit, die gleiche Anzahl von Instances in jeder aktivierten Availability Zone aufrechtzuerhalten. Es verbessert auch die Fähigkeit Ihrer Anwendung, den Verlust einer oder mehrerer Instances zu bewältigen.

Kontroll-ID	AWS Config	Empfehlungen
Art. 21.1	elb-tls-https-listeners-nur	Stellen Sie sicher, dass Ihre Elastic Load Balancer (ELBs) mit SSL- oder HTTPS-Listenern konfiguriert sind. Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.
Art. 21.1	rds-instance-deletion-protection-aktiviert	Stellen Sie sicher, dass Amazon Relational Database Service (Amazon RDS)-Instances den Löschschutz aktiviert haben. Verwenden Sie den Löschschutz, um zu verhindern, dass Ihre Amazon-RDS-Instances versehentlich oder böswillig gelöscht werden, was zum Verlust der Verfügbarkeit Ihrer Anwendungen führen kann.
Art. 21.1	rds-snapshot-encrypted	Stellen Sie sicher, dass die Verschlüsselung für Ihre Amazon Relational Database Service (Amazon RDS)-Snapshots aktiviert ist. Da sensible Daten auch im Ruhezustand vorhanden sein können, sollten Sie die Verschlüsselung im Ruhezustand aktivieren, um diese Daten zu schützen.

Kontroll-ID	AWS Config	Empfehlungen
Art. 21.1	s3- bucket-default-lock-enabled	Stellen Sie sicher, dass für Ihren Amazon Simple Storage Service (Amazon S3)-Bucket standardmäßig eine Sperre aktiviert ist. Zum Schutz eventuell vorhandener sensibler Daten in S3-Bucket s müssen Sie Objektsperren für Daten im Ruhezustand erzwingen.
Art. 21.1	s-3 default-encryption-kms	Stellen Sie sicher, dass die Verschlüsselung für Ihre Amazon Simple Storage Service (Amazon S3)-Bucke ts aktiviert ist. Um eventuell vorhandene sensible Daten im Ruhezustand in einem Amazon-S3-Bucket zu schützen, muss die Verschlüs selung aktiviert sein.
Art. 21.1	sagemaker-notebook-instance -kms-key-konfiguriert	Um Daten im Ruhezusta nd zu schützen, stellen Sie sicher, dass die Verschlüs selung mit dem AWS Key Management Service (AWS KMS) für Ihr Notebook aktiviert ist. SageMaker Da vertrauli che Daten im SageMaker Notebook gespeichert werden können, sollten Sie die Verschlüsselung im Ruhezustand aktivieren, um diese Daten zu schützen.

Kontroll-ID	AWS Config	Empfehlungen
Art. 21.1	sns-encrypted-kms	Um Daten im Ruhezusta nd zu schützen, stellen Sie sicher, dass Ihre Amazon Simple Notification Service (Amazon SNS) -Themen mit dem AWS Key Management Service (AWS KMS) verschlüs selt werden müssen. Um eventuell vorhandene sensible Daten im Ruhezustand in veröffentlichten Nachricht en zu schützen, muss die Verschlüsselung von Daten im Ruhezustand aktiviert sein.
Art. 21.1	alb-http-to-https-Umleitung sprüfung	Um Daten während der Übertragung zu schützen, stellen Sie sicher, dass Ihr Application Load Balancer unverschlüsselte HTTP-Anfragen automatisch an HTTPS umleitet. Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	AWS Config	Empfehlungen
Art. 21.1	api-gw-cache-enabled-und-verschlüsselt	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass die Verschlüsselung für den Cache Ihrer API-Gateway-Stufe aktiviert ist. Da für die API-Methode sensible Daten erfasst werden können, sollten Sie die Verschlüsselung von Daten im Ruhezustand aktivieren, um diese Daten zu schützen.
Art. 21.1	api-gw-ssl-enabled	Stellen Sie sicher, dass die REST-API-Stufen von Amazon API Gateway mit SSL-Zertifikaten konfiguriert sind, damit Backend-Systeme überprüfen können, ob Anforderungen von API Gateway stammen.
Art. 21.1	cloud-trail-encryption-enabled	Da sensible Daten vorhanden sein können und um Daten im Ruhezustand zu schützen, sollten Sie sicherstellen, dass die Verschlüsselung für Ihre AWS CloudTrail Trails aktiviert ist.

Kontroll-ID	AWS Config	Empfehlungen
Art. 21.1	cloud-trail-log-file-Validierung aktiviert	Verwenden Sie die AWS CloudTrail Protokolldateivalidierung, um die Integrität von Protokollen zu überprüfen. CloudTrail Mithilfe der Protokolldateivalidierung kann festgestellt werden, ob eine Protokolldatei geändert oder gelöscht wurde oder ob sie nach der Übermittlung CloudTrail unverändert geblieben ist. Dieses Feature wurde mit dem Branchenstandard entsprechenden Algorithmen entwickelt: SHA-256 für die Hashfunktion und SHA-256 mit RSA für digitale Signaturen. Aus diesem Grund ist es rechnerisch unmöglich, CloudTrail Protokolldateien unbemerkt zu ändern, zu löschen oder zu fälschen.
Art. 21.1	cloudwatch-log-group-encrypted	Um sensible Daten im Ruhezustand zu schützen, stellen Sie sicher, dass die Verschlüsselung für Ihre Amazon CloudWatch Log Groups aktiviert ist.

Kontroll-ID	AWS Config	Empfehlungen
Art. 21.1	dynamodb-autoscaling-enabled	Amazon DynamoDB Auto Scaling verwendet den AWS Application Auto Scaling-Service, um die bereitgestellte Durchsatzkapazität so anzupassen, dass sie automatisch auf tatsächliche Verkehrsmuster reagiert. Auf diese Weise kann eine Tabelle oder ein globaler sekundärer Index die bereitgestellte Lese-/Schreibkapazität erhöhen, um plötzliche Erhöhungen des Datenverkehrs ohne Drosselung zu bewältigen.
Art. 21.1	efs-encrypted-check	Aktivieren Sie die Verschlüsselung für Ihr Amazon Elastic File System (EFS), um eventuell vorhandene sensible Daten sowie Daten im Ruhezustand zu schützen.
Art. 21.1	elasticsearch-encrypted-at-rest	Da sensible Daten vorhanden sein können und um Daten im Ruhezustand zu schützen, sollten Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon OpenSearch Service (OpenSearch Service) -Domains aktiviert ist.

Kontroll-ID	AWS Config	Empfehlungen
Art. 21.1	elb-acm-certificate-required	Zum Schutz von eventuell vorhandenen sensiblen Daten sowie von Daten während der Übertragung muss die Verschlüsselung für Ihr Elastic Load Balancing aktiviert sein. Verwenden Sie AWS Certifica te Manager, um öffentlic he und private SSL/TLS-Z ertifikate mit AWS Diensten und internen Ressourcen zu verwalten, bereitzustellen und bereitzustellen.
Art. 21.1	elb-deletion-protection-ena bled	Diese Regel sorgt dafür, dass der Löschschutz für Elastic Load Balancing aktiviert ist. Verwenden Sie diese Funktion, um zu verhinder n, dass Ihr Load Balancer versehentlich oder böswillig gelöscht wird, was zum Verlust der Verfügbarkeit Ihrer Anwendungen führen kann.
Art. 21.1	encrypted-volumes	Aktivieren Sie die Verschlüs selung für Ihre Amazon-El astic-Block-Store (Amazon-EBS)-Volumes, um eventuell vorhandene sensible Daten sowie Daten im Ruhezustand zu schützen.

Kontroll-ID	AWS Config	Empfehlungen
Art. 21.1	opensearch-encrypted-at-rest	Da sensible Daten vorhanden sein können und um Daten im Ruhezustand zu schützen, sollten Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon OpenSearch Service-Domains aktiviert ist.
Art. 21.1	opensearch-node-to-node-Verschlüsselungsprüfung	Stellen Sie sicher, dass die node-to-node Verschlüsselung für Amazon OpenSearch Service aktiviert ist. Node-to-nodeVerschlüsselung ermöglicht die TLS 1.2-Verschlüsselung für die gesamte Kommunikation innerhalb der Amazon Virtual Private Cloud (Amazon VPC). Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	AWS Config	Empfehlungen
Art. 21.1	rds-multi-az-support	Die Multi-AZ-Unterstützung in Amazon Relational Database Service (Amazon RDS) bietet eine verbesserte Verfügbar keit und Beständigkeit von Datenbank-Instances. Wenn Sie eine Multi-AZ-Datenbank-Instance bereitstellen, erstellt Amazon RDS automatisch eine primäre Datenbank-Instance und repliziert die Daten synchron auf eine Standby-Instance in einer anderen Availability Zone. Jede Availability Zone läuft auf einer eigenen, physisch getrennten, unabhängigen Infrastruktur und ist auf eine hohe Verfügbarkeit ausgelegt . Im Falle eines Infrastru kturausfalls führt Amazon RDS einen automatischen Failover zum Standby-Modus durch, sodass Sie den Datenbank betrieb wieder aufnehmen können, sobald der Failover abgeschlossen ist.

Kontroll-ID	AWS Config	Empfehlungen
Art. 21.1	rds-cluster-multi-az-aktiviert	Die Multi-AZ-Unterstützung in Amazon Relational Database Service (Amazon RDS) bietet eine verbesserte Verfügbar keit und Beständigkeit von Datenbank-Instances. Wenn Sie eine Multi-AZ-Datenbank-Instance bereitstellen, erstellt Amazon RDS automatisch eine primäre Datenbank-Instance und repliziert die Daten synchron auf eine Standby-Instance in einer anderen Availability Zone. Jede Availability Zone läuft auf einer eigenen, physisch getrennten, unabhängigen Infrastruktur und ist auf eine hohe Verfügbarkeit ausgelegt . Im Falle eines Infrastru kturausfalls führt Amazon RDS einen automatischen Failover zum Standby-Modus durch, sodass Sie den Datenbank betrieb wieder aufnehmen können, sobald der Failover abgeschlossen ist.

Kontroll-ID	AWS Config	Empfehlungen
Art. 21.1	rds-storage-encrypted	Zum Schutz von Daten im Ruhezustand müssen Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon Relational Database Service (Amazon RDS)-Instances aktiviert ist. Um eventuell vorhandene sensible Daten im Ruhezustand in Amazon-RDS-Instanc es zu schützen, muss die Verschlüsselung von Daten im Ruhezustand aktiviert sein.

Kontroll-ID	AWS Config	Empfehlungen
Art. 21.1	redshift-cluster-configuration-check	Um Daten im Ruhezustand zu schützen, muss die Verschlüsselung für Ihre Amazon-Redshift-Cluster aktiviert sein. Sie müssen auch sicherstellen, dass die erforderlichen Konfigurationen auf Amazon-Redshift-Clustern bereitgestellt werden. Die Prüfungsprotokollierung muss aktiviert sein, um Informationen zu Verbindungen und Benutzeraktivitäten in der Datenbank bereitzustellen. Diese Regel erfordert, dass ein Wert für clusterDbEncrypted (Config Default: TRUE) und LoggingEnabled (Config Default: TRUE) gesetzt ist. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	AWS Config	Empfehlungen
Art. 21.1	redshift-cluster-kms-enabled	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass die Verschlüsselung mit AWS Key Management Service (AWS KMS) für Ihren Amazon Redshift Redshift-Cluster aktiviert ist. Um eventuell vorhandene sensible Daten im Ruhezustand in Redshift-Clustern zu schützen, muss die Verschlüsselung von Daten im Ruhezustand aktiviert sein.
Art. 21.1	redshift-require-tls-ssl	Stellen Sie sicher, dass Ihre Amazon-Redshift-Cluster eine TLS/SSL-Verschlüsselung erfordern, um eine Verbindun g zu SQL-Clients herzustel len. Um eventuell vorhanden e sensible Daten zu schützen, sollten Sie die Verschlüs selung bei der Übertragung aktivieren.

Kontroll-ID	AWS Config	Empfehlungen
Art. 21.1	s3- aktiviert bucket-server-side-encryption	Zum Schutz von Daten im Ruhezustand müssen Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon Simple Storage Service (Amazon S3)-Buckets aktiviert ist. Um eventuell vorhandene sensible Daten im Ruhezustand in Amazon-S3-Buckets zu schützen, muss die Verschlüsselung aktiviert sein.
Art. 21.1	s-3 bucket-ssl-requests-only	Um Daten während der Übertragung zu schützen, stellen Sie sicher, dass Ihre Amazon Simple Storage Service (Amazon S3)-Buckets Anfragen zur Verwendung von Secure Socket Layer (SSL)-Buckets erfordern. Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	AWS Config	Empfehlungen
Art. 21.1	sagemaker-endpoint-configuration-kms-key-konfiguriert	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass die Verschlüsselung mit dem AWS Key Management Service (AWS KMS) für Ihren Endpunkt aktiviert ist. SageMaker Da sensible Daten auf dem SageMaker Endgerät gespeichert werden können, sollten Sie die Verschlüsselung im Ruhezustand aktivieren, um diese Daten zu schützen.
Art. 21.1	secretsmanager-using-cmk	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass die Verschlüsselung mit dem AWS Key Management Service (AWS KMS) für AWS Secrets Manager aktiviert ist. Aktivieren Sie die Verschlüsselung von Daten im Ruhezustand, um eventuell vorhandene sensible Daten im Ruhezustand im Secrets Manager zu schützen.

Kontroll-ID	AWS Config	Empfehlungen
Art. 21.1	vpc-vpn-2-tunnels-up	Redundante Site-to-Site VPN-Tunnel können implement iert werden, um die Anforderu ngen an die Ausfallsicherheit zu erfüllen. Es verwendet zwei Tunnel, um die Konnektiv ität sicherzustellen, falls eine der Site-to-Site VPN-Verbi ndungen nicht verfügbar ist. Um sich vor einem Verbindun gsverlust zu schützen, können Sie für den Fall, dass Ihr Kunden-Gateway nicht verfügbar ist, eine zweite Site-to-Site VPN-Verbindung zu Ihrer Amazon Virtual Private Cloud (Amazon VPC) und Ihrem Virtual Private Gateway einrichten, indem Sie ein zweites Kunden-Gateway verwenden.
Art. 22	autoscaling-launch-config-p ublic-ip-deaktiviert	Wenn Sie Ihre Netzwerks chnittstellen mit einer öffentlic hen IP-Adresse konfigurieren, sind die diesen Netzwerks chnittstellen zugehörigen Ressourcen über das Internet erreichbar. EC2 Ressource n sollten nicht öffentlich zugänglich sein, da dies einen unbeabsichtigten Zugriff auf Ihre Anwendungen oder Server ermöglichen kann.

Kontroll-ID	AWS Config	Empfehlungen
Art. 22	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) Security Groups können bei der Verwaltung des Netzwerkz ugriffs helfen, indem sie eine statusbehaftete Filterung von eingehendem und ausgehend em Netzwerkverkehr zu Ressourcen bereitstellen. AWS Wenn Sie eingehenden (oder entfernten) Datenverk ehr von 0.0.0.0/0 bis Port 22 auf Ihren Ressourcen nicht zulassen, können Sie den Remote-Zugriff einschränken.
Art. 22	ssm-document-not-public	Stellen Sie sicher, dass AWS Systems Manager (SSM) - Dokumente nicht öffentlich sind, da dies einen unbeabsic htigten Zugriff auf Ihre SSM-Dokumente ermöglichen kann. Ein öffentliches SSM-Dokum ent kann Informationen über Ihr Konto, Ihre Ressource n und internen Prozesse preisgeben.

Kontroll-ID	AWS Config	Empfehlungen
Art. 22	dms-replication-not-public	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass auf DMS-Replikationsinstanzen nicht öffentlich zugegriffen werden kann. DMS-Replikations-I nstances können vertrauli che Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.
Art. 22	ebs-snapshot-public-restora ble-überprüfen	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass EBS-Snaps hots nicht öffentlich wiederher stellbar sind. EBS-Volume-Snapshots können vertrauli che Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.
Art. 22	ec-2 instance-no-public-ip	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon Elastic Compute Cloud (Amazon EC2) -Instances nicht öffentlich zugänglich sind. EC2 Amazon-Instances können vertrauliche Informati onen enthalten, und für solche Konten ist eine Zugriffsk ontrolle erforderlich.

Kontroll-ID	AWS Config	Empfehlungen
Art. 22	elasticsearch-in-vpc-only	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass sich Amazon OpenSearch OpenSearch Service (Service) -Domains innerhalb einer Amazon Virtual Private Cloud (Amazon VPC) befinden. Eine OpenSearch Service-Domain innerhalb einer Amazon VPC ermöglicht die sichere Kommunikation zwischen OpenSearch Service und anderen Services innerhalb der Amazon VPC, ohne dass ein Internet-Gateway, ein NAT-Gerät oder eine VPN-Verbindung erforderlich ist.
Art. 22	emr-master-no-public-ip	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon EMR-Cluster-Masterknoten nicht öffentlich zugänglich sind. Amazon-EMR-Cluster-Hauptknoten können vertrauliche Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	AWS Config	Empfehlungen
Art. 22	internet-gateway-authorized-vpc-nur	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Internet-Gateways nur mit autorisierter Amazon Virtual Private Cloud (Amazon VPC) verbunden sind. Internet-Gateways ermöglichen den bidirekti onalen Internetzugang zur und von der Amazon VPC, was möglicherweise zu einem unbefugten Zugriff auf Amazon-VPC-Ressourcen führen kann.
Art. 22	lambda-function-public-acce ss-verboten	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherste llen, dass AWS Lambda-Funktionen nicht öffentlich zugänglich sind. Der öffentlic he Zugriff kann möglicher weise die Verfügbarkeit von Ressourcen beeinträchtigen.

Kontroll-ID	AWS Config	Empfehlungen
Art. 22	lambda-inside-vpc	Stellen Sie AWS Lambda-Funktionen in einer Amazon Virtual Private Cloud (Amazon VPC) bereit, um eine sichere Kommunikation zwischen einer Funktion und anderen Diensten innerhalb der Amazon VPC zu gewährleisten. Bei dieser Konfiguration sind kein Internet-Gateway, kein NAT-Gerät und keine VPN-Verbindung erforderlich. Der gesamte Datenverkehr bleibt sicher in der Cloud. AWS Domains, die sich innerhalb einer VPC befinden, verfügen aufgrund ihrer logischen Isolierung im Vergleich zu Domains mit öffentlichen Endpunkten über eine zusätzliche Sicherheitsebene. Um den Zugriff ordnungsgemäß zu verwalten, sollten AWS Lambda-Funktionen einer VPC zugewiesen werden.

Kontroll-ID	AWS Config	Empfehlungen
Art. 22	opensearch-in-vpc-only	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass sich Amazon OpenSearch Service-Domains innerhalb einer Amazon Virtual Private Cloud (Amazon VPC) befinden. Eine Amazon OpenSearch Service-Domain innerhalb einer Amazon VPC ermöglich t die sichere Kommunika tion zwischen Amazon OpenSearch Service und anderen Services innerhalb der Amazon VPC, ohne dass ein Internet-Gateway, ein NAT-Gerät oder eine VPN-Verbindung erforderlich ist.
Art. 22	rds-instance-public-access-überprüfen	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherste llen, dass Amazon Relationa l Database Service (Amazon RDS) -Instances nicht öffentlic h sind. Amazon-RDS-Datenba nk-Instances können vertrauli che Informationen enthalten und für solche Konten sind Prinzipien und Zugriffsk ontrollen erforderlich.

Kontroll-ID	AWS Config	Empfehlungen
Art. 22	rds-snapshots-public-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Relational Database Service (Amazon RDS) -Instances nicht öffentlich sind. Amazon-RDS-Datenbank-Instances können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.
Art. 22	redshift-cluster-public-access-überprüfen	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Redshift Redshift-Cluster nicht öffentlich sind. Amazon-Redshift-Cluster können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	AWS Config	Empfehlungen
Art. 22	restricted-common-ports	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass gemeinsame Ports für Amazon Elastic Compute Cloud (Amazon EC2) - Sicherheitsgruppen eingeschränkt sind. Wenn der Zugriff auf Ports nicht auf vertrauenswürdige Quellen beschränkt wird, kann dies zu Angriffen auf die Verfügbarkeit, Integrität und Vertraulichkeit von Systemen führen. Mit dieser Regel können Sie optional die Parameter blockedPort1–blockedPort5 festlegen (Standardkonfigurationen: 20, 21, 3389, 3306, 4333). Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	AWS Config	Empfehlungen
Art. 22	s3- account-level-public-access -blöcke-periodisch	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Simple Storage Service (Amazon S3) -Buckets nicht öffentlich zugänglich sind. Diese Regel trägt dazu bei, sensible Daten vor unbefugten Remote-Benutzern zu schützen, indem sie den öffentlichen Zugriff verhindert. Mit dieser Regel können Sie optional die Parameter ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) und restrictPublicBuckets Parameter (Config Default: True) festlegen. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	AWS Config	Empfehlungen
Art. 22	s3 bucket-level-public-access -verboten	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Simple Storage Service (Amazon S3) -Buckets nicht öffentlich zugänglich sind. Diese Regel trägt dazu bei, sensible Daten vor unbefugten Remote-Benutzern zu schützen, indem sie den öffentlichen Zugriff auf Bucket-Ebene verhindert.
Art. 22	s-3 bucket-public-read-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie nur autorisierten Benutzern, Prozessen und Geräten Zugriff auf Amazon Simple Storage Service (Amazon S3) -Buckets gewähren. Die Verwaltung des Zugriffs sollte mit der Klassifizierung der Daten übereinstimmen.

Kontroll-ID	AWS Config	Empfehlungen
Art. 22	s3- bucket-public-write-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie nur autorisierten Benutzern, Prozessen und Geräten Zugriff auf Amazon Simple Storage Service (Amazon S3) -Buckets gewähren. Die Verwaltung des Zugriffs sollte mit der Klassifizierung der Daten übereinstimmen.
Art. 22	sagemaker-notebook-no-direct-Internetzugang	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass SageMaker Amazon-Notebooks keinen direkten Internetzugang zulassen. Indem Sie direkten Internetzugang blockieren, vermeiden Sie, dass unbefugte Benutzer auf sensible Daten zugreifen.

Kontroll-ID	AWS Config	Empfehlungen
Art. 22	subnet-auto-assign-public-ip-deaktiviert	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon Virtual Private Cloud (VPC) -Subnetzen nicht automatis ch eine öffentliche IP-Adress e zugewiesen wird. Amazon Elastic Compute Cloud (EC2) -Instances, die in Subnetzen gestartet werden, in denen dieses Attribut aktiviert ist, haben ihrer primären Netzwerkschnittste lle eine öffentliche IP-Adresse zugewiesen.
Art. 22	vpc-default-security-group-geschlossen	Sicherheitsgruppen von Amazon Elastic Compute Cloud (Amazon EC2) können bei der Verwaltung des Netzwerkzugriffs helfen, indem sie eine statusbeh aftete Filterung des ein- und ausgehenden Netzwerkv erkehrs zu Ressourcen bereitstellen. AWS Die Beschränkung des gesamten Datenverkehrs auf die Standardsicherheitsgruppe hilft dabei, den Fernzugriff auf Ihre Ressourcen einzuschr änken. AWS

Kontroll-ID	AWS Config	Empfehlungen
Art. 22	vpc-sg-open-only-to-authorized-ports	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass gemeinsame Ports für Amazon Elastic Compute Cloud (Amazon EC2) - Sicherheitsgruppen eingeschränkt sind. Wenn der Zugriff auf Ports nicht auf vertrauenswürdige Quellen beschränkt wird, kann dies zu Angriffen auf die Verfügbarkeit, Integrität und Vertraulichkeit von Systemen führen. Durch die Beschränkung des Zugriffs auf Ressourcen innerhalb einer Sicherheitsgruppe aus dem Internet (0.0.0.0/0) kann der Remote-Zugriff auf interne Systeme gesteuert werden.
Art. 23	elasticsearch-logs-to-cloudwatch	Stellen Sie sicher, dass für Amazon OpenSearch Service-Domains Fehlerprotokolle aktiviert und zur Aufbewahrung und Beantwortung an Amazon CloudWatch Logs gestreamt werden. Domain-Fehlerprotokolle sind bei Sicherheits- und Zugriffsprüfungen sowie bei der Diagnose von Verfügbarkeitsproblemen nützlich.

Kontroll-ID	AWS Config	Empfehlungen
Art. 23	multi-region-cloudtrail-enabled	AWS CloudTrail zeichnet Aktionen und API-Aufrufe der AWS Management Console auf. Sie können feststellen, welche Benutzer und Konten angerufen wurden AWS, von welcher Quell-IP-Adresse aus die Anrufe getätigt wurden und wann die Anrufe erfolgten . CloudTrail übermittelt Protokolldateien aus allen AWS Regionen an Ihren S3-Bucket, wenn MULTI_REGION_CLOUD_TRAIL_ENABLED aktiviert ist. Außerdem wird beim AWS Start einer neuen Region derselbe Trail in der neuen Region erstellt. CloudTrail Dadurch erhalten Sie automatisch Protokoll dateien mit API-Aktivitäten für die neue Region.

Kontroll-ID	AWS Config	Empfehlungen
Art. 23	rds-logging-enabled	Um die Protokollierung und Überwachung in Ihrer Umgebung zu erleichtern, stellen Sie sicher, dass die Amazon Relational Database Service (Amazon RDS)-Protokollierung aktiviert ist. Mit der Amazon-RDS-Protokollierung können Sie Ereignisse wie Verbindungen, Verbindungsabbrüche, Abfragen oder abgefragte Tabellen erfassen.
Art. 23	wafv2-logging-enabled	Um die Protokollierung und Überwachung in Ihrer Umgebung zu erleichtern, aktivieren Sie die AWS WAF (V2) -Protokollierung im regionalen und globalen Web ACLs. AWS Die WAF-Protokollierung bietet detaillierte Informationen über den Datenverkehr, der von Ihrer Web-ACL analysiert wird. In den Protokollen werden die Uhrzeit aufgezeichnet, zu der die AWS WAF die Anfrage von Ihrer AWS Ressource erhalten hat, Informationen über die Anfrage und eine Aktion für die Regel, der jede Anfrage entsprach.

Kontroll-ID	AWS Config	Empfehlungen
Art. 23	api-gw-execution-logging-aktiviert	Die API-Gateway-Protokollierung zeigt detaillierte Ansichten der Benutzer, die auf die API zugegriffen haben, und wie diese Benutzer auf die API zugegriffen haben. Diese Einblicke ermöglichen die Transparenz von Benutzeraktivitäten.
Art. 23	cloud-trail-cloud-watch-logs-aktiviert	Verwenden Sie Amazon CloudWatch , um Protokollereignisaktivitäten zentral zu sammeln und zu verwalten . Die Aufnahme von AWS CloudTrail Daten liefert Einzelheiten zu den API-Aufrufaktivitäten in Ihrem AWS-Konto.

Kontroll-ID	AWS Config	Empfehlungen
Art. 23	cloudtrail-enabled	AWS CloudTrail kann bei der Nichtabstreitbarkeit helfen, indem Aktionen und API-Aufrufe der AWS Managemen t Console aufgezeichnet werden. Sie können die Benutzer und die Benutzer AWS-Konten , die einen AWS Dienst aufgerufen haben, die Quell-IP-Adresse, über die die Aufrufe generiert wurden, und den Zeitpunkt der Anrufe identifizieren. Einzelheiten zu den erfassten Daten finden Sie in den AWS CloudTrail Datensatzinhalten.
Art. 23	cloudtrail-s3-dataevents-en abled	Die Erfassung von Simple Storage Service (Amazon S3)-Datenereignissen unterstützt die Erkennung von ungewöhnl ichen Aktivitäten. Zu den Details gehören AWS-Konto Informationen über den Zugriff auf einen Amazon S3 S3-Bucket, die IP-Adresse und die Uhrzeit des Ereignisses.

Kontroll-ID	AWS Config	Empfehlungen
Art. 23	elb-logging-enabled	Die Elastic-Load-Balancing-Aktivität ist ein zentraler Kommunikationspunkt innerhalb einer Umgebung. Stellen Sie sicher, dass die ELB-Protokollierung aktiviert ist. Die gesammelten Daten enthalten detaillierte Informati onen zu Anfragen, die an den ELB gesendet wurden. Jedes Protokoll enthält Informati onen wie die Zeit, zu der die Anforderung einging, die Client-IP-Adresse, Latenzen, Anforderungspfade und Serverantworten.
Art. 23	opensearch-logs-to-cloudwat ch	Stellen Sie sicher, dass für Amazon OpenSearch Service-Domains Fehlerprotokolle aktiviert und zur Aufbewahr ung und Beantwortung an Amazon CloudWatch Logs gestreamt werden. OpenSearc h Service-Fehlerprotokolle können bei Sicherheits- und Zugriffsprüfungen helfen und bei der Diagnose von Verfügbarkeitsproblemen helfen.

Kontroll-ID	AWS Config	Empfehlungen
Art. 23	s-3 bucket-logging-enabled	Die Amazon Simple Storage Service (Amazon S3)-Serverzugriffsprotokollierung bietet eine Methode zur Überwachung des Netzwerks im Hinblick auf potenzielle Cybersicherheitsereignisse. Die Ereignisse werden überwacht, indem detaillierte Aufzeichnungen über die Anfragen erfasst werden, die an einen Amazon-S3-Bucket gestellt wurden. Jeder Zugriffsprotokolleintrag enthält Details zu einer einzelnen Zugriffsanfrage. Zu den Details gehören Anforderer, Bucket-Name, Anforderungszeit, Anforderungsaktion, Antwortstatus und Fehlercode, falls relevant.

Kontroll-ID	AWS Config	Empfehlungen
Art. 23	vpc-flow-logs-enabled	VPC-Flow-Protokolle erfassen detaillierte Informationsdatensätze über den IP-Datenverkehr, der zu und von Netzwerkschnittstellen in Ihrer Amazon Virtual Private Cloud (Amazon VPC) fließt. Standardmäßig enthalten Flow-Protokolldatensätze Werte für die verschiedenen Komponenten des IP-Flows, einschließlich Quelle, Ziel und Protokoll.
Art. 25	dynamodb-in-backup-plan	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon DynamoDB-Tabellen Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	AWS Config	Empfehlungen
Art. 25	ebs-in-backup-plan	Stellen Sie zur Unterstützung der Datensicherungsprozesse sicher, dass Ihre Amazon Elastic Block Store (Amazon EBS) -Volumes Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherung smanagement und erleichte rt Ihnen die Erfüllung von geschäftlichen und behördlic hen Compliance-Anforde rungen hinsichtlich Datensich erungen.

Kontroll-ID	AWS Config	Empfehlungen
Art. 25	efs-in-backup-plan	Um Sie bei Datensich erungsprozessen zu unterstüt zen, stellen Sie sicher, dass Ihre Amazon Elastic File System (Amazon EFS) - Dateisysteme Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherung smanagement und erleichte rt Ihnen die Erfüllung von geschäftlichen und behördlic hen Compliance-Anforde rungen hinsichtlich Datensich erungen.

Kontroll-ID	AWS Config	Empfehlungen
Art. 25	rds-in-backup-plan	Um Sie bei Datensich erungsprozessen zu unterstüt zen, stellen Sie sicher, dass Ihre Amazon Relational Database Service (Amazon RDS) -Instances Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherung smanagement und erleichte rt Ihnen die Erfüllung von geschäftlichen und behördlic hen Compliance-Anforde rungen hinsichtlich Datensich erungen.

Kontroll-ID	AWS Config	Empfehlungen
Art. 25	redshift-backup-enabled	Stellen Sie zur Unterstützung der Datensicherungsprozesse sicher, dass Ihre Amazon-Redshift-Cluster über automatisierte Snapshots verfügen. Wenn automatisierte Snapshots für einen Cluster aktiviert sind, erstellt Redshift in regelmäßigen Abständen Snapshots dieses Clusters. Standardmäßig erstellt Redshift alle acht Stunden oder alle 5 GB einen Snapshot für jeden Knoten mit Datenänderungen oder je nachdem, was zuerst eintritt.
Art. 25	db-instance-backup-enabled	Die Sicherungsfunktion von Amazon RDS erstellt Sicherungen Ihrer Datenbanken und Transaktionsprotokolle. Amazon RDS erstellt einen Snapshot für das Speichervolume Ihrer DB-Instance, sodass die gesamte DB-Instance gesichert wird. Sie können im System spezifische Aufbewahrungsfristen festlegen, um Ihre Ausfallsicherheitsanforderungen zu erfüllen.

Kontroll-ID	AWS Config	Empfehlungen
Art. 25	dynamodb-pitr-enabled	Aktivieren Sie diese Regel, um zu überprüfen, ob die Informationen gesichert wurden. Es verwaltet auch die Backups, indem es sicherstellt, dass die point-in-time Wiederherstellung in Amazon DynamoDB aktiviert ist. Bei der Wiederherstellung werden fortlaufende Backups Ihrer Tabelle für die letzten 35 Tage gespeichert.
Art. 25	ebs-optimized-instance	Eine optimierte Instance im Amazon Elastic Block Store (Amazon EBS) bietet zusätzliche, dedizierte Kapazität für Amazon-EBS-I/O-Vorgänge. Diese Optimierung bietet die beste Leistung für Ihr EBS-Volume, indem Konflikte zwischen Amazon-EBS-I/O und anderem Datenverkehr von Ihrer Instance minimiert werden.

Kontroll-ID	AWS Config	Empfehlungen
Art. 25	elasticache-redis-cluster-automatic-Backup-Prüfung	Wenn automatische Backups aktiviert sind, ElastiCache erstellt Amazon täglich ein Backup des Clusters. Die Sicherung kann für eine von Ihrer Organisation festgelegte Anzahl von Tagen aufbewahrt werden. Automatische Backups schützen vor Datenverlust. Bei einem Ausfall können Sie einen neuen Cluster erstellen, der Ihre Daten aus dem aktuellen Backup wiederherstellt.
Art. 25	s-3 bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) unterstützt die Aufrechterhaltung einer angemessenen Kapazität und Verfügbarkeit. CRR ermöglicht das automatische, asynchrone Kopieren von Objekten in Amazon-S3-Buckets, um die Datenverfügbarkeit sicherzustellen.

Kontroll-ID	AWS Config	Empfehlungen
Art. 25	s-3 bucket-versioning-enabled	Die Versionsverwaltung von Amazon Simple Storage Service (Amazon S3)-Buckets hilft dabei, mehrere Varianten eines Objekts im selben Amazon-S3-Bucket zu speichern. Verwenden Sie die Versionsverwaltung, um sämtliche Versionen aller Objekte in Ihrem Amazon-S3-Bucket zu speichern, abzurufen oder wiederher zustellen. Mit der Versionsv erwaltung können Sie Versionen sowohl nach unbeabsichtigten Benutzera ktionen als auch nach Anwendungsfehlern problemlo s wiederherstellen.

Vorlage

Die Vorlage ist verfügbar unter GitHub: Operational Best Practices for Esquema Nacional de Seguridad (ENS) Low.

Bewährte Methoden für die Implementierung des Esquema Nacional de Seguridad (ENS) Medium

Konformitätspakete bieten ein allgemeines Compliance-Framework, das es Ihnen ermöglicht, mithilfe verwalteter oder benutzerdefinierter Regeln und Abhilfemaßnahmen Kontrollen zur Sicherheit, zum Betrieb oder zur Kostenoptimierung durchzuführen. AWS Config AWS Config Conformance Packs dienen als Beispielvorlagen nicht dazu, die vollständige Einhaltung eines bestimmten Governance- oder Compliance-Standards sicherzustellen. Sie sind dafür verantwortlich, selbst zu beurteilen, ob Ihre Nutzung der Services den geltenden gesetzlichen und behördlichen Anforderungen entspricht.

Im Folgenden finden Sie ein Beispiel für eine Zuordnung zwischen Esquema Nacional de Seguridad (ENS) Medium Framework-Steuerelementen in Spanien und verwalteten Konfigurationsregeln. AWS Jede Config-Regel gilt für eine bestimmte AWS Ressource und bezieht sich auf eine oder mehrere Spanien ENS Medium-Steuerelemente. Eine Kontrolle des spanischen ENS kann mehreren Config-Regeln zugeordnet werden. In der folgenden Tabelle finden Sie weitere Informationen und Anleitungen zu diesen Zuordnungen.

Diese beispielhafte Conformance-Pack-Vorlage enthält Zuordnungen zu Kontrollen nach den Richtlinien des spanischen ENS Medium, das zuletzt am 23.10.2020 aktualisiert wurde.

Kontroll-ID	AWS Config	Empfehlungen
Anexo II 4.1.2.a); b); c)	dynamodb-table-encrypted-kms	Stellen Sie sicher, dass die Verschlüsselung für Ihre Amazon-DynamoDB-Tabellen aktiviert ist. Um eventuell vorhandene sensible Daten im Ruhezustand in diesen Tabellen zu schützen, müssen Sie die Verschlüsselung von Daten im Ruhezustand aktivieren. Standardmäßig werden DynamoDB-Tabellen mit einem AWS eigenen Kundenhauptschlüssel (CMK) verschlüsselt.
Anexo II 4.1.2.a); b); c)	ec2- ebs-encryption-by-default	Zum Schutz von Daten im Ruhezustand müssen Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon Elastic Block Store (Amazon EBS)-Volumes aktiviert ist. Da sensible Daten auch im Ruhezusta nd vorhanden sein können, sollten Sie die Verschlüs

Kontroll-ID	AWS Config	Empfehlungen
		selung im Ruhezustand aktivieren, um diese Daten zu schützen.
Anexo II 4.1.2.a); b); c)	elasticsearch-node-to-node-Verschlüsselungsprüfung	Stellen Sie sicher, dass die node-to-node Verschlüsselung für Amazon OpenSearch Service aktiviert ist. Node-to-nodeVerschlüsselung ermöglicht die TLS 1.2-Versc hlüsselung für die gesamte Kommunikation innerhalb der Amazon Virtual Private Cloud (Amazon VPC). Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.
Anexo II 4.1.2.a); b); c)	elb-cross-zone-load-Balancing aktiviert	Aktivieren Sie zonenüber greifendes Load Balancing für Ihre Elastic Load Balancer (ELBs), um eine angemesse ne Kapazität und Verfügbar keit aufrechtzuerhalten. Zonenübergreifendes Load Balancing reduziert die Notwendigkeit, die gleiche Anzahl von Instances in jeder aktivierten Availability Zone aufrechtzuerhalten. Es verbessert auch die Fähigkeit Ihrer Anwendung, den Verlust einer oder mehrerer Instances zu bewältigen.

Kontroll-ID	AWS Config	Empfehlungen
Anexo II 4.1.2.a); b); c)	elb-tls-https-listeners-nur	Stellen Sie sicher, dass Ihre Elastic Load Balancer (ELBs) mit SSL- oder HTTPS-Listenern konfiguriert sind. Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.
Anexo II 4.1.2.a); b); c)	rds-instance-deletion-protection-aktiviert	Stellen Sie sicher, dass Amazon Relational Database Service (Amazon RDS)-Instances den Löschschutz aktiviert haben. Verwenden Sie den Löschschutz, um zu verhindern, dass Ihre Amazon-RDS-Instances versehentlich oder böswillig gelöscht werden, was zum Verlust der Verfügbarkeit Ihrer Anwendungen führen kann.
Anexo II 4.1.2.a); b); c)	rds-snapshot-encrypted	Stellen Sie sicher, dass die Verschlüsselung für Ihre Amazon Relational Database Service (Amazon RDS)-Snapshots aktiviert ist. Da sensible Daten auch im Ruhezustand vorhanden sein können, sollten Sie die Verschlüsselung im Ruhezustand aktivieren, um diese Daten zu schützen.

Kontroll-ID	AWS Config	Empfehlungen
Anexo II 4.1.2.a); b); c)	s3- bucket-default-lock-enabled	Stellen Sie sicher, dass für Ihren Amazon Simple Storage Service (Amazon S3)-Bucket standardmäßig eine Sperre aktiviert ist. Zum Schutz eventuell vorhandener sensibler Daten in S3-Bucket s müssen Sie Objektsperren für Daten im Ruhezustand erzwingen.
Anexo II 4.1.2.a); b); c)	s-3 default-encryption-kms	Stellen Sie sicher, dass die Verschlüsselung für Ihre Amazon Simple Storage Service (Amazon S3)-Bucke ts aktiviert ist. Um eventuell vorhandene sensible Daten im Ruhezustand in einem Amazon-S3-Bucket zu schützen, muss die Verschlüs selung aktiviert sein.
Anexo II 4.1.2.a); b); c)	sagemaker-notebook-instance -kms-key-konfiguriert	Um Daten im Ruhezusta nd zu schützen, stellen Sie sicher, dass die Verschlüs selung mit dem AWS Key Management Service (AWS KMS) für Ihr Notebook aktiviert ist. SageMaker Da vertrauli che Daten im SageMaker Notebook gespeichert werden können, sollten Sie die Verschlüsselung im Ruhezustand aktivieren, um diese Daten zu schützen.

Kontroll-ID	AWS Config	Empfehlungen
Anexo II 4.1.2.a); b); c)	sns-encrypted-kms	Um Daten im Ruhezusta nd zu schützen, stellen Sie sicher, dass Ihre Amazon Simple Notification Service (Amazon SNS) -Themen mit dem AWS Key Management Service (AWS KMS) verschlüs selt werden müssen. Um eventuell vorhandene sensible Daten im Ruhezustand in veröffentlichten Nachricht en zu schützen, muss die Verschlüsselung von Daten im Ruhezustand aktiviert sein.
Anexo II 4.1.2.a); b); c)	alb-http-to-https-Umleitung sprüfung	Um Daten während der Übertragung zu schützen, stellen Sie sicher, dass Ihr Application Load Balancer unverschlüsselte HTTP-Anfragen automatisch an HTTPS umleitet. Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	AWS Config	Empfehlungen
Anexo II 4.1.2.a); b); c)	api-gw-cache-enabled-und-verschlüsselt	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass die Verschlüsselung für den Cache Ihrer API-Gateway-Stufe aktiviert ist. Da für die API-Methode sensible Daten erfasst werden können, sollten Sie die Verschlüsselung von Daten im Ruhezustand aktivieren, um diese Daten zu schützen.
Anexo II 4.1.2.a); b); c)	api-gw-ssl-enabled	Stellen Sie sicher, dass die REST-API-Stufen von Amazon API Gateway mit SSL-Zertifikaten konfiguriert sind, damit Backend-Systeme überprüfen können, ob Anforderungen von API Gateway stammen.
Anexo II 4.1.2.a); b); c)	cloud-trail-encryption-enabled	Da sensible Daten vorhanden sein können und um Daten im Ruhezustand zu schützen, sollten Sie sicherstellen, dass die Verschlüsselung für Ihre AWS CloudTrail Trails aktiviert ist.

Kontroll-ID	AWS Config	Empfehlungen
Anexo II 4.1.2.a); b); c)	cloud-trail-log-file-Validierung aktiviert	Verwenden Sie die AWS CloudTrail Protokolldateivalidierung, um die Integrität von Protokollen zu überprüfen. CloudTrail Mithilfe der Protokolldateivalidierung kann festgestellt werden, ob eine Protokolldatei geändert oder gelöscht wurde oder ob sie nach der Übermittlung CloudTrail unverändert geblieben ist. Dieses Feature wurde mit dem Branchenstandard entsprechenden Algorithmen entwickelt: SHA-256 für die Hashfunktion und SHA-256 mit RSA für digitale Signaturen. Aus diesem Grund ist es rechnerisch unmöglich, CloudTrail Protokolldateien unbemerkt zu ändern, zu löschen oder zu fälschen.
Anexo II 4.1.2.a); b); c)	cloudwatch-log-group-encrypted	Um sensible Daten im Speicher zu schützen, stellen Sie sicher, dass die Verschlüsselung für Ihre Amazon CloudWatch Log Groups aktiviert ist.

Kontroll-ID	AWS Config	Empfehlungen
Anexo II 4.1.2.a); b); c)	dynamodb-autoscaling-enabled	Amazon DynamoDB Auto Scaling verwendet den AWS Application Auto Scaling-Service, um die bereitgestellte Durchsatzkapazität so anzupassen, dass sie automatisch auf tatsächliche Verkehrsmuster reagiert. Auf diese Weise kann eine Tabelle oder ein globaler sekundärer Index die bereitgestellte Lese-/Schreibkapazität erhöhen, um plötzliche Erhöhungen des Datenverkehrs ohne Drosselung zu bewältigen.
Anexo II 4.1.2.a); b); c)	efs-encrypted-check	Aktivieren Sie die Verschlüsselung für Ihr Amazon Elastic File System (EFS), um eventuell vorhandene sensible Daten sowie Daten im Ruhezustand zu schützen.
Anexo II 4.1.2.a); b); c)	elasticsearch-encrypted-at-rest	Da sensible Daten vorhanden sein können und um Daten im Ruhezustand zu schützen, sollten Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon OpenSearch Service (OpenSearch Service) -Domains aktiviert ist.

Kontroll-ID	AWS Config	Empfehlungen
Anexo II 4.1.2.a); b); c)	elb-acm-certificate-required	Zum Schutz von eventuell vorhandenen sensiblen Daten sowie von Daten während der Übertragung muss die Verschlüsselung für Ihr Elastic Load Balancing aktiviert sein. Verwenden Sie AWS Certifica te Manager, um öffentlic he und private SSL/TLS-Z ertifikate mit AWS Diensten und internen Ressourcen zu verwalten, bereitzustellen und bereitzustellen.
Anexo II 4.1.2.a); b); c)	elb-deletion-protection-ena bled	Diese Regel sorgt dafür, dass der Löschschutz für Elastic Load Balancing aktiviert ist. Verwenden Sie diese Funktion, um zu verhinder n, dass Ihr Load Balancer versehentlich oder böswillig gelöscht wird, was zum Verlust der Verfügbarkeit Ihrer Anwendungen führen kann.
Anexo II 4.1.2.a); b); c)	encrypted-volumes	Aktivieren Sie die Verschlüs selung für Ihre Amazon-El astic-Block-Store (Amazon-EBS)-Volumes, um eventuell vorhandene sensible Daten sowie Daten im Ruhezustand zu schützen.

Kontroll-ID	AWS Config	Empfehlungen
Anexo II 4.1.2.a); b); c)	opensearch-encrypted-at-rest	Da sensible Daten vorhanden sein können und um Daten im Ruhezustand zu schützen, sollten Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon OpenSearch Service-Domains aktiviert ist.
Anexo II 4.1.2.a); b); c)	opensearch-node-to-node-Verschlüsselungsprüfung	Stellen Sie sicher, dass die node-to-node Verschlüsselung für Amazon OpenSearch Service aktiviert ist. Node-to-nodeVerschlüsselung ermöglicht die TLS 1.2-Verschlüsselung für die gesamte Kommunikation innerhalb der Amazon Virtual Private Cloud (Amazon VPC). Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	AWS Config	Empfehlungen
Anexo II 4.1.2.a); b); c)	rds-multi-az-support	Die Multi-AZ-Unterstützung in Amazon Relational Database Service (Amazon RDS) bietet eine verbesserte Verfügbar keit und Beständigkeit von Datenbank-Instances. Wenn Sie eine Multi-AZ-Datenbank-Instance bereitstellen, erstellt Amazon RDS automatisch eine primäre Datenbank-Instance und repliziert die Daten synchron auf eine Standby-Instance in einer anderen Availability Zone. Jede Availability Zone läuft auf einer eigenen, physisch getrennten, unabhängigen Infrastruktur und ist auf eine hohe Verfügbarkeit ausgelegt . Im Falle eines Infrastru kturausfalls führt Amazon RDS einen automatischen Failover zum Standby-Modus durch, sodass Sie den Datenbank betrieb wieder aufnehmen können, sobald der Failover abgeschlossen ist.

Kontroll-ID	AWS Config	Empfehlungen
Anexo II 4.1.2.a); b); c)	rds-cluster-multi-az-aktiviert	Die Multi-AZ-Unterstützung in Amazon Relational Database Service (Amazon RDS) bietet eine verbesserte Verfügbar keit und Beständigkeit von Datenbank-Instances. Wenn Sie eine Multi-AZ-Datenbank-Instance bereitstellen, erstellt Amazon RDS automatisch eine primäre Datenbank-Instance und repliziert die Daten synchron auf eine Standby-Instance in einer anderen Availability Zone. Jede Availability Zone läuft auf einer eigenen, physisch getrennten, unabhängigen Infrastruktur und ist auf eine hohe Verfügbarkeit ausgelegt . Im Falle eines Infrastru kturausfalls führt Amazon RDS einen automatischen Failover zum Standby-Modus durch, sodass Sie den Datenbank betrieb wieder aufnehmen können, sobald der Failover abgeschlossen ist.

Kontroll-ID	AWS Config	Empfehlungen
Anexo II 4.1.2.a); b); c)	rds-storage-encrypted	Zum Schutz von Daten im Ruhezustand müssen Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon Relational Database Service (Amazon RDS)-Instances aktiviert ist. Um eventuell vorhandene sensible Daten im Ruhezustand in Amazon-RDS-Instanc es zu schützen, muss die Verschlüsselung von Daten im Ruhezustand aktiviert sein.

Kontroll-ID	AWS Config	Empfehlungen
Anexo II 4.1.2.a); b); c)	redshift-cluster-configuration-check	Um Daten im Ruhezustand zu schützen, muss die Verschlüsselung für Ihre Amazon-Redshift-Cluster aktiviert sein. Sie müssen auch sicherstellen, dass die erforderlichen Konfigurationen auf Amazon-Redshift-Clustern bereitgestellt werden. Die Prüfungsprotokollierung muss aktiviert sein, um Informationen zu Verbindungen und Benutzeraktivitäten in der Datenbank bereitzustellen. Diese Regel erfordert, dass ein Wert für clusterDbEncrypted (Config Default: TRUE) und LoggingEnabled (Config Default: TRUE) gesetzt ist. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	AWS Config	Empfehlungen
Anexo II 4.1.2.a); b); c)	redshift-cluster-kms-enabled	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass die Verschlüsselung mit AWS Key Management Service (AWS KMS) für Ihren Amazon Redshift Redshift-Cluster aktiviert ist. Um eventuell vorhandene sensible Daten im Ruhezustand in Redshift-Clustern zu schützen, muss die Verschlüsselung von Daten im Ruhezustand aktiviert sein.
Anexo II 4.1.2.a); b); c)	redshift-require-tls-ssl	Stellen Sie sicher, dass Ihre Amazon-Redshift-Cluster eine TLS/SSL-Verschlüsselung erfordern, um eine Verbindun g zu SQL-Clients herzustel len. Um eventuell vorhanden e sensible Daten zu schützen, sollten Sie die Verschlüs selung bei der Übertragung aktivieren.

Kontroll-ID	AWS Config	Empfehlungen
Anexo II 4.1.2.a); b); c)	s3- aktiviert bucket-server-side -encryption	Zum Schutz von Daten im Ruhezustand müssen Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon Simple Storage Service (Amazon S3)-Bucke ts aktiviert ist. Um eventuell vorhandene sensible Daten im Ruhezustand in Amazon-S3 -Buckets zu schützen, muss die Verschlüsselung aktiviert sein.
Anexo II 4.1.2.a); b); c)	s-3 bucket-ssl-requests-only	Um Daten während der Übertragung zu schützen, stellen Sie sicher, dass Ihre Amazon Simple Storage Service (Amazon S3)-Bucke ts Anfragen zur Verwendun g von Secure Socket Layer (SSL)-Buckets erfordern. Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	AWS Config	Empfehlungen
Anexo II 4.1.2.a); b); c)	sagemaker-endpoint-configuration-kms-key-konfiguriert	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass die Verschlüsselung mit dem AWS Key Management Service (AWS KMS) für Ihren Endpunkt aktiviert ist. SageMaker Da sensible Daten auf dem SageMaker Endgerät gespeichert werden können, sollten Sie die Verschlüsselung im Ruhezustand aktivieren, um diese Daten zu schützen.
Anexo II 4.1.2.a); b); c)	secretsmanager-using-cmk	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass die Verschlüsselung mit dem AWS Key Management Service (AWS KMS) für AWS Secrets Manager aktiviert ist. Aktivieren Sie die Verschlüsselung von Daten im Ruhezustand, um eventuell vorhandene sensible Daten im Ruhezustand im Secrets Manager zu schützen.

Kontroll-ID	AWS Config	Empfehlungen
Anexo II 4.1.2.a); b); c)	vpc-vpn-2-tunnels-up	Redundante Site-to-Site VPN-Tunnel können implement iert werden, um die Anforderu ngen an die Ausfallsicherheit zu erfüllen. Es verwendet zwei Tunnel, um die Konnektiv ität sicherzustellen, falls eine der Site-to-Site VPN-Verbi ndungen nicht verfügbar ist. Um sich vor einem Verbindun gsverlust zu schützen, können Sie für den Fall, dass Ihr Kunden-Gateway nicht verfügbar ist, eine zweite Site-to-Site VPN-Verbindung zu Ihrer Amazon Virtual Private Cloud (Amazon VPC) und Ihrem Virtual Private Gateway einrichten, indem Sie ein zweites Kunden-Gateway verwenden.
Anexo II 4.1.2.b)	ec2- -eni-periodisch security-group-attached-to	Diese Regel stellt sicher, dass die Sicherheitsgruppen an eine Amazon Elastic Compute Cloud (Amazon EC2) - Instance oder an eine ENI angehängt sind. Diese Regel unterstützt die Überwachu ng ungenutzter Sicherhei tsgruppen im Bestand und die Verwaltung Ihrer Umgebung.

Kontroll-ID	AWS Config	Empfehlungen
Anexo II 4.1.2.b)	ec2-check managedinstance-association-compliance-status	Verwenden Sie AWS Systems Manager Associations, um bei der Inventarisierung von Softwareplattformen und Anwendungen innerhalb eines Unternehmens zu helfen. AWS Systems Manager weist Ihren verwalteten Instanzen einen Konfigurationsstatus zu und ermöglicht es Ihnen, Basiswerte für Betriebss ystem-Patch-Levels, Softwarei nstallationen, Anwendung skonfigurationen und andere Details zu Ihrer Umgebung festzulegen.
Anexo II 4.1.2.b)	ec2-stopped-instance	Aktivieren Sie diese Regel, um bei der Basiskonfiguration von Amazon Elastic Compute Cloud (Amazon EC2) - Instances zu helfen, indem Sie überprüfen, ob EC2 Amazon-Instances gemäß den Standards Ihrer Organisat ion für mehr als die zulässige Anzahl von Tagen gestoppt wurden.

Kontroll-ID	AWS Config	Empfehlungen
Anexo II 4.1.2.b)	ec2- volume-inuse-check	Diese Regel stellt sicher, dass Amazon Elastic Block Store-Volumes, die an Amazon Elastic Compute Cloud (Amazon EC2) -Instances angehängt sind, zum Löschen markiert werden, wenn eine Instance beendet wird. Wenn ein Amazon-EBS-Volume nicht gelöscht wird, wenn die Instance, an die es angehängt ist, beendet wird, kann dies gegen das Konzept der geringsten Funktionalität verstoßen.
Anexo II 4.1.2.b)	eip-attached	Diese Regel stellt sicher, dass Elastic, die einer Amazon Virtual Private Cloud (Amazon VPC) IPs zugewiesen sind, an Amazon Elastic Compute Cloud (Amazon EC2) - Instances oder verwendete Elastic Network Interfaces angehängt sind. Diese Regel hilft bei der Überwachung ungenutzter Inhalte EIPs in Ihrer Umgebung.

Kontroll-ID	AWS Config	Empfehlungen
Anexo II 4.1.2.b)	vpc-network-acl-unused-überprüfen	Diese Regel stellt sicher, dass Amazon Virtual Private Cloud (VPC)-Netzwerkzugriffskontrolllisten verwendet werden. Die Überwachung ungenutzter Netzwerkzugriffskontrolllisten kann zu einer genauen Inventarisierung und Verwaltung Ihrer Umgebung beitragen.
Anexo II 4.2.1.a)	iam-root-access-key-überprüfen	Der Zugriff auf Systeme und Ressourcen kann gesteuert werden, indem überprüft wird, ob der Root-Benutzer keine Zugriffsschlüssel mit seiner AWS Identity and Access Management (IAM) -Rolle verknüpft hat. Stellen Sie sicher, dass die Root-Zugriffsschlüssel gelöscht werden. Erstellen und verwenden Sie stattdessen rollenbasierte Funktionen, AWS-Konten um das Prinzip der geringsten Funktionalität zu berücksichtigen.

Kontroll-ID	AWS Config	Empfehlungen
Anexo II 4.2.1.a); 4.2.1.b)	iam-root-access-key-überprüfen	Der Zugriff auf Systeme und Ressourcen kann gesteuert werden, indem überprüft wird, ob der Root-Benutzer keine Zugriffsschlüssel mit seiner AWS Identity and Access Management (IAM) -Rolle verknüpft hat. Stellen Sie sicher, dass die Root-Zugriffsschlüssel gelöscht werden. Erstellen und verwenden Sie stattdessen rollenbasierte Funktionen, AWS-Konten um das Prinzip der geringsten Funktionalität zu berücksichtigen.
Anexo II 4.2.4	ecs-task-definition-user-for-host-mode-check	Wenn für eine Aufgabendefinition erhöhte Berechtigungen gelten, liegt das daran, dass der Kunde diesen Konfigurationen ausdrücklich zugestimmt hat. Diese Kontrolle prüft, ob eine unerwartete Berechtigungseskalation vorliegt, wenn für eine Aufgabendefinition das Host-Netzwerk aktiviert ist, die Kunden aber keine erhöhten Berechtigungen aktiviert haben.

Kontroll-ID	AWS Config	Empfehlungen
Anexo II 4.2.4	iam-policy-no-statements-with-full-access	Stellen Sie sicher, dass IAM-Aktionen nur auf die benötigte n Aktionen beschränkt sind. Wenn Benutzern mehr Rechte eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und der Aufgabentrennung verstoßen.
Anexo II 4.2.4	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) kann Ihnen dabei helfen, die Prinzipien der geringsten Rechte und der Aufgabent rennung in Zugriffsberechtigu ngen und Autorisierungen zu integrieren und so zu verhindern, dass Richtlinien „Effect“: „Allow“ mit „Action“: „*“ anstelle von „Resource“: „*“ enthalten. Wenn Benutzern mehr Rechte eingeräumt werden, als für die Ausführun g einer Aufgabe erforderl ich sind, kann dies gegen das Prinzip der geringste n Berechtigung und der Aufgabentrennung verstoßen.

Kontroll-ID	AWS Config	Empfehlungen
Anexo II 4.2.4	s3- bucket-policy-grantee-check	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie s3_bucket_policy_grantee_check aktivieren. Diese Regel prüft, ob der vom Amazon S3 S3-Bucket gewährte Zugriff durch die von Ihnen bereitgestellten AWS Principals, Verbundbenutzer, Service Principals, IP-Adressen oder Amazon Virtual Private Cloud (Amazon VPC) IDs eingeschränkt ist.
Anexo II 4.2.5	iam-root-access-key-überprüfen	Der Zugriff auf Systeme und Ressourcen kann gesteuert werden, indem überprüft wird, ob der Root-Benutzer keine Zugriffsschlüssel mit seiner AWS Identity and Access Management (IAM) -Rolle verknüpft hat. Stellen Sie sicher, dass die Root-Zugriffsschlüssel gelöscht werden. Erstellen und verwenden Sie stattdessen rollenbasierte Funktionen, AWS-Konten um das Prinzip der geringsten Funktionalität zu berücksichtigen.

Kontroll-ID	AWS Config	Empfehlungen
Anexo II 4.2.5.a)	iam-password-policy	Die Identitäten und Anmeldein formationen werden auf der Grundlage einer organisat orischen IAM-Passwortrichtl inie ausgestellt, verwaltet und verifiziert. Sie erfüllen oder übertreffen die Anforderungen von NIST SP 800-63 und dem Standard „Best Practices“ von AWS Foundational Security für die Passwortstärke. Mit dieser Regel können Sie optional RequireUppercaseCharacters (Wert für AWS grundlege nde Sicherheitsbewährte Methoden: wahr), RequireLo wercaseCharacters (Wert für bewährte Methoden für AWS grundlegende Sicherheit: wahr), RequireSymbols (Wert für bewährte Methoden für AWS grundlegende Sicherhei t: wahr), RequireNumbers (Wert für bewährte Methoden für AWS grundlegende Sicherheit: wahr), MinimumPa sswordLength (Wert für bewährte Methoden für AWS grundlegende Sicherheit: 14), PasswordReusePreve ntion (Wert für bewährte Methoden für AWS grundlege nde Sicherheit: 24) und MaxPasswordAge (Wert

Kontroll-ID	AWS Config	Empfehlungen
		für bewährte Methoden für AWS grundlegende Sicherheit: 90) für Ihr IAM festlegen Kennwortrichtlinie. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	AWS Config	Empfehlungen
Anexo II 4.2.5.c)	iam-password-policy	Die Identitäten und Anmeldein formationen werden auf der Grundlage einer organisat orischen IAM-Passwortrichtl inie ausgestellt, verwaltet und verifiziert. Sie erfüllen oder übertreffen die Anforderungen des NIST SP 800-63 und des AWS Foundational Security Best Practices-Standards für Passwortstärke. Mit dieser Regel können Sie optional RequireUppercaseCharacters (Wert für AWS grundlege nde Sicherheitsbewährte Methoden: wahr), RequireLo wercaseCharacters (Wert für bewährte Methoden für AWS grundlegende Sicherheit: wahr), RequireSymbols (Wert für bewährte Methoden für AWS grundlegende Sicherhei t: wahr), RequireNumbers (Wert für bewährte Methoden für AWS grundlegende Sicherheit: wahr), MinimumPa sswordLength (Wert für bewährte Methoden für AWS grundlegende Sicherheit: 14), PasswordReusePreve ntion (Wert für bewährte Methoden für AWS grundlege nde Sicherheit: 24) und MaxPasswordAge (Wert

Kontroll-ID	AWS Config	Empfehlungen
		für bewährte Methoden für AWS grundlegende Sicherhei t: 90) für Ihr IAM festlegen Kennwortrichtlinie. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisat ion entsprechen.
Anexo II 4.2.6.BAJO.c)	opensearch-logs-to-cloudwat ch	Stellen Sie sicher, dass für Amazon OpenSearch Service-Domains Fehlerprotokolle aktiviert und zur Aufbewahr ung und Beantwortung an Amazon CloudWatch Logs gestreamt werden. OpenSearc h Service-Fehlerprotokolle können bei Sicherheits- und Zugriffsprüfungen helfen und bei der Diagnose von Verfügbarkeitsproblemen helfen.
Anexo II 4.2.6.c)	elasticsearch-logs-to-cloud watch	Stellen Sie sicher, dass für Amazon OpenSearch Service-Domains Fehlerprotokolle aktiviert und zur Aufbewahr ung und Beantwortung an Amazon CloudWatch Logs gestreamt werden. Domain-Fehlerprotokolle sind bei Sicherheits- und Zugriffsp rüfungen sowie bei der Diagnose von Verfügbar keitsproblemen nützlich.

Kontroll-ID	AWS Config	Empfehlungen
Anexo II 4.2.6.c)	multi-region-cloudtrail-enabled	AWS CloudTrail zeichnet Aktionen und API-Aufrufe der AWS Management Console auf. Sie können feststellen, welche Benutzer und Konten angerufen wurden AWS, von welcher Quell-IP-Adresse aus die Anrufe getätigt wurden und wann die Anrufe erfolgten . CloudTrail übermittelt Protokolldateien aus allen AWS Regionen an Ihren S3-Bucket, wenn MULTI_REGION_CLOUD_TRAIL_ENABLED aktiviert ist. Außerdem wird beim AWS Start einer neuen Region derselbe Trail in der neuen Region erstellt. CloudTrail Dadurch erhalten Sie automatisch Protokoll dateien mit API-Aktivitäten für die neue Region.

Kontroll-ID	AWS Config	Empfehlungen
Anexo II 4.2.6.c)	rds-logging-enabled	Um die Protokollierung und Überwachung in Ihrer Umgebung zu erleichtern, stellen Sie sicher, dass die Amazon Relational Database Service (Amazon RDS)-Protokollierung aktiviert ist. Mit der Amazon-RDS-Protokollierung können Sie Ereignisse wie Verbindungen, Verbindungsabbrüche, Abfragen oder abgefragte Tabellen erfassen.
Anexo II 4.2.6.c)	wafv2-logging-enabled	Um die Protokollierung und Überwachung in Ihrer Umgebung zu erleichtern, aktivieren Sie die AWS WAF (V2) -Protokollierung im regionalen und globalen Web ACLs. AWS Die WAF-Protokollierung bietet detaillierte Informationen über den Datenverkehr, der von Ihrer Web-ACL analysiert wird. In den Protokollen werden die Uhrzeit aufgezeichnet, zu der die AWS WAF die Anfrage von Ihrer AWS Ressource erhalten hat, Informationen über die Anfrage und eine Aktion für die Regel, der jede Anfrage entsprach.

Kontroll-ID	AWS Config	Empfehlungen
Anexo II 4.2.6.c)	api-gw-execution-logging-aktiviert	Die API-Gateway-Protokollierung zeigt detaillierte Ansichten der Benutzer, die auf die API zugegriffen haben, und wie diese Benutzer auf die API zugegriffen haben. Diese Einblicke ermöglichen die Transparenz von Benutzeraktivitäten.
Anexo II 4.2.6.c)	cloud-trail-cloud-watch-logs-aktiviert	Verwenden Sie Amazon CloudWatch , um Protokollereignisaktivitäten zentral zu sammeln und zu verwalten . Die Aufnahme von AWS CloudTrail Daten liefert Einzelheiten zu den API-Aufrufaktivitäten in Ihrem AWS-Konto.

Kontroll-ID	AWS Config	Empfehlungen
Anexo II 4.2.6.c)	cloudtrail-enabled	AWS CloudTrail kann bei der Nichtabstreitbarkeit helfen, indem Aktionen und API-Aufrufe der AWS Managemen t Console aufgezeichnet werden. Sie können die Benutzer und die Benutzer AWS-Konten , die einen AWS Dienst aufgerufen haben, die Quell-IP-Adresse, über die die Aufrufe generiert wurden, und den Zeitpunkt der Anrufe identifizieren. Einzelheiten zu den erfassten Daten finden Sie in den AWS CloudTrail Datensatzinhalten.
Anexo II 4.2.6.c)	cloudtrail-s3-dataevents-en abled	Die Erfassung von Simple Storage Service (Amazon S3)-Datenereignissen unterstützt die Erkennung von ungewöhnl ichen Aktivitäten. Zu den Details gehören AWS-Konto Informationen über den Zugriff auf einen Amazon S3 S3-Bucket, die IP-Adresse und die Uhrzeit des Ereignisses.

Kontroll-ID	AWS Config	Empfehlungen
Anexo II 4.2.6.c)	elb-logging-enabled	Die Elastic-Load-Balancing-Aktivität ist ein zentraler Kommunikationspunkt innerhalb einer Umgebung. Stellen Sie sicher, dass die ELB-Protokollierung aktiviert ist. Die gesammelten Daten enthalten detaillierte Informati onen zu Anfragen, die an den ELB gesendet wurden. Jedes Protokoll enthält Informati onen wie die Zeit, zu der die Anforderung einging, die Client-IP-Adresse, Latenzen, Anforderungspfade und Serverantworten.

Kontroll-ID	AWS Config	Empfehlungen
Anexo II 4.2.6.c)	s-3 bucket-logging-enabled	Die Amazon Simple Storage Service (Amazon S3)-Serve rzugriffsprotokollierung bietet eine Methode zur Überwachung des Netzwerks im Hinblick auf potenzielle Cybersicherheitsereignisse. Die Ereignisse werden überwacht, indem detaillie rte Aufzeichnungen über die Anfragen erfasst werden, die an einen Amazon-S3-Bucket gestellt wurden. Jeder Zugriffsprotokolleintrag enthält Details zu einer einzelnen Zugriffsanfrage. Zu den Details gehören Anfordere r, Bucket-Name, Anforderu ngszeit, Anforderungsaktion, Antwortstatus und Fehlercode, falls relevant.

Kontroll-ID	AWS Config	Empfehlungen
Anexo II 4.2.6.c)	vpc-flow-logs-enabled	VPC-Flow-Protokolle erfassen detaillierte Informationsdatensätze über den IP-Datenverkehr, der zu und von Netzwerkschnittstellen in Ihrer Amazon Virtual Private Cloud (Amazon VPC) fließt. Standardmäßig enthalten Flow-Protokolldatensätze Werte für die verschiedenen Komponenten des IP-Flows, einschließlich Quelle, Ziel und Protokoll.
Anexo II 4.2.7	iam-user-mfa-enabled	Aktivieren Sie diese Regel, um den Zugriff auf Ressourcen in der AWS Cloud einzuschränken. Diese Regel sorgt dafür, dass die Multi-Faktor-Authentifizierung (MFA) für alle Benutzer aktiviert ist. MFA sorgt für eine weitere Schutzebene zusätzlich zu den Anmeldeinformationen. Reduzieren Sie Fälle von kompromittierten Konten, indem Sie MFA für Benutzer vorschreiben.

Kontroll-ID	AWS Config	Empfehlungen
Anexo II 4.2.7	mfa-enabled-for-iam-Konsolenzugriff	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass MFA für alle AWS Identity and Access Management (IAM) -Benutzer aktiviert ist, die über ein Konsolenkennwort verfügen. MFA sorgt für eine weitere Schutzebene zusätzlich zu den Anmeldeinformationen. Indem Sie MFA für Benutzer vorschreiben, können Sie Fälle kompromittierter Konten reduzieren und verhindern, dass unbefugte Benutzer auf vertrauliche Daten zugreifen.
Anexo II 4.2.7	root-account-hardware-mfa-aktiviert	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Hardware-MFA für den Root-Benutzer aktiviert ist. Der Stammbenutzer ist der AWS-Konto-Benutzer mit den meisten Berechtigungen. MFA sorgt für eine weitere Schutzebene zusätzlich zu den Anmeldeinformationen. Indem Sie MFA für den Root-Benutzer vorschreiben, können Sie die Anzahl AWS-Konten kompromittierter Benutzer reduzieren.

Kontroll-ID	AWS Config	Empfehlungen
Anexo II 4.2.7	root-account-mfa-enabled	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass MFA für den Root-Benutzer aktiviert ist. Der Stammbenutzer ist der AWS-Konto-Benutzer mit den meisten Berechtigungen. MFA sorgt für eine weitere Schutzebene zusätzlich zu den Anmeldeinformationen. Indem Sie MFA für den Root-Benutzer vorschreiben, können Sie die Anzahl AWS-Konten kompromittierter Benutzer reduzieren.
Anexo II 4.3.1	ec2- -eni-periodisch security-group-attached-to	Diese Regel stellt sicher, dass die Sicherheitsgruppen an eine Amazon Elastic Compute Cloud (Amazon EC2) - Instance oder an eine ENI angehängt sind. Diese Regel unterstützt die Überwachung ungenutzter Sicherheitsgruppen im Bestand und die Verwaltung Ihrer Umgebung.

Kontroll-ID	AWS Config	Empfehlungen
Anexo II 4.3.1	ec2-check managedinstance-association-compliance-status	Verwenden Sie AWS Systems Manager Associations, um bei der Inventarisierung von Softwareplattformen und Anwendungen innerhalb eines Unternehmens zu helfen. AWS Systems Manager weist Ihren verwalteten Instanzen einen Konfigurationsstatus zu und ermöglicht es Ihnen, Basiswerte für Betriebss ystem-Patch-Levels, Softwarei nstallationen, Anwendung skonfigurationen und andere Details zu Ihrer Umgebung festzulegen.
Anexo II 4.3.1	ec2-stopped-instance	Aktivieren Sie diese Regel, um bei der Basiskonfiguration von Amazon Elastic Compute Cloud (Amazon EC2) - Instances zu helfen, indem Sie überprüfen, ob EC2 Amazon-Instances gemäß den Standards Ihrer Organisat ion für mehr als die zulässige Anzahl von Tagen gestoppt wurden.

Kontroll-ID	AWS Config	Empfehlungen
Anexo II 4.3.1	ec2- volume-inuse-check	Diese Regel stellt sicher, dass Amazon Elastic Block Store-Volumes, die an Amazon Elastic Compute Cloud (Amazon EC2) -Instances angehängt sind, zum Löschen markiert werden, wenn eine Instance beendet wird. Wenn ein Amazon-EBS-Volume nicht gelöscht wird, wenn die Instance, an die es angehängt ist, beendet wird, kann dies gegen das Konzept der geringsten Funktionalität verstoßen.
Anexo II 4.3.1	eip-attached	Diese Regel stellt sicher, dass Elastic, die einer Amazon Virtual Private Cloud (Amazon VPC) IPs zugewiesen sind, an Amazon Elastic Compute Cloud (Amazon EC2) - Instances oder verwendete Elastic Network Interfaces angehängt sind. Diese Regel hilft bei der Überwachung ungenutzter Inhalte EIPs in Ihrer Umgebung.

Kontroll-ID	AWS Config	Empfehlungen
Anexo II 4.3.1	vpc-network-acl-unused-überprüfen	Diese Regel stellt sicher, dass Amazon Virtual Private Cloud (VPC)-Netzwerkzugriffskontrolllisten verwendet werden. Die Überwachung ungenutzter Netzwerkzugriffskontrolllisten kann zu einer genauen Inventarisierung und Verwaltung Ihrer Umgebung beitragen.
Anexo II 4.3.2.b)	alb-waf-enabled	Stellen Sie sicher, dass AWS WAF auf Elastic Load Balancers (ELB) aktiviert ist, um Webanwendungen zu schützen. Eine WAF trägt zum Schutz Ihrer Webanwendungen oder APIs vor gängigen Web-Exploits bei. Diese Web-Exploits können sich auf die Verfügbarkeit auswirken, die Sicherheit gefährden oder übermäßige Ressourcen in Ihrer Umgebung verbrauchen.

Kontroll-ID	AWS Config	Empfehlungen
Anexo II 4.3.2.b)	api-gw-associated-with-WAF	AWS Mit WAF können Sie eine Reihe von Regeln (als Web Access Control List (Web ACL) bezeichnet) konfiguri eren, die Webanfragen auf der Grundlage von anpassbar en Websicherheitsregeln und -bedingungen, die Sie definieren, zulassen, blockiere n oder zählen. Stellen Sie sicher, dass Ihre Amazon-API-Gateway-Stufe mit einer WAF-Web-ACL verknüpft ist, um sie vor böswilligen Angriffen zu schützen.
Anexo II 4.3.2.b)	no-unrestricted-route-to-igw	Stellen Sie sicher, dass EC2 Amazon-Routentabellen keine uneingeschränkten Routen zu einem Internet-Gateway enthalten. Durch das Entfernen oder Beschränk en des Internetzugangs für Workloads innerhalb von Amazon VPCs können unbeabsichtigte Zugriffe in Ihrer Umgebung reduziert werden.

Kontroll-ID	AWS Config	Empfehlungen
Anexo II 4.3.2.b)	ssm-document-not-public	Stellen Sie sicher, dass AWS Systems Manager (SSM) - Dokumente nicht öffentlich sind, da dies einen unbeabsichtigten Zugriff auf Ihre SSM-Dokumente ermöglichen kann. Ein öffentliches SSM-Dokument kann Informationen über Ihr Konto, Ihre Ressourcen und internen Prozesse preisgeben.
Anexo II 4.3.2.b)	dms-replication-not-public	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass auf DMS-Replikationsinstanzen nicht öffentlich zugegriffen werden kann. DMS-Replikations-Instances können vertrauliche Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.
Anexo II 4.3.2.b)	ebs-snapshot-public-restorable-überprüfen	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass EBS-Snapshots nicht öffentlich wiederherstellbar sind. EBS-Volume-Snapshots können vertrauliche Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	AWS Config	Empfehlungen
Anexo II 4.3.2.b)	ec-2 instance-no-public-ip	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon Elastic Compute Cloud (Amazon EC2) -Instances nicht öffentlich zugänglich sind. EC2 Amazon-Instances können vertrauliche Informati onen enthalten, und für solche Konten ist eine Zugriffsk ontrolle erforderlich.
Anexo II 4.3.2.b)	elasticsearch-in-vpc-only	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass sich Amazon OpenSearch OpenSearch Service (Service) -Domains innerhalb einer Amazon Virtual Private Cloud (Amazon VPC) befinden. Eine OpenSearch Service-D omain innerhalb einer Amazon VPC ermöglicht die sichere Kommunikation zwischen OpenSearch Service und anderen Services innerhalb der Amazon VPC, ohne dass ein Internet-Gateway, ein NAT-Gerät oder eine VPN-Verbindung erforderlich ist.

Kontroll-ID	AWS Config	Empfehlungen
Anexo II 4.3.2.b)	emr-master-no-public-ip	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon EMR-Cluster-Masterknoten nicht öffentlich zugänglich sind. Amazon-EMR-Cluster-Hauptknoten können vertrauliche Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.
Anexo II 4.3.2.b)	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) Security Groups können bei der Verwaltung des Netzwerkzugriffs helfen, indem sie eine statusbehaftete Filterung von eingehendem und ausgehendem Netzwerkverkehr zu Ressourcen bereitstellen. AWS Wenn Sie eingehenden (oder entfernten) Datenverkehr von 0.0.0.0/0 bis Port 22 auf Ihren Ressourcen nicht zulassen, können Sie den Remote-Zugriff einschränken.

Kontroll-ID	AWS Config	Empfehlungen
Anexo II 4.3.2.b)	internet-gateway-authorized-vpc-nur	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Internet-Gateways nur mit autorisierter Amazon Virtual Private Cloud (Amazon VPC) verbunden sind. Internet-Gateways ermöglichen den bidirekti onalen Internetzugang zur und von der Amazon VPC, was möglicherweise zu einem unbefugten Zugriff auf Amazon-VPC-Ressourcen führen kann.
Anexo II 4.3.2.b)	lambda-function-public-acce ss-verboten	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherste llen, dass AWS Lambda-Funktionen nicht öffentlich zugänglich sind. Der öffentlic he Zugriff kann möglicher weise die Verfügbarkeit von Ressourcen beeinträchtigen.

Kontroll-ID	AWS Config	Empfehlungen
Anexo II 4.3.2.b)	lambda-inside-vpc	Stellen Sie AWS Lambda-Funktionen in einer Amazon Virtual Private Cloud (Amazon VPC) bereit, um eine sichere Kommunikation zwischen einer Funktion und anderen Diensten innerhalb der Amazon VPC zu gewährleisten. Bei dieser Konfiguration sind kein Internet-Gateway, kein NAT-Gerät und keine VPN-Verbindung erforderlich. Der gesamte Datenverkehr bleibt sicher in der Cloud. AWS Domains, die sich innerhalb einer VPC befinden, verfügen aufgrund ihrer logischen Isolierung im Vergleich zu Domains mit öffentlichen Endpunkten über eine zusätzliche Sicherheitsebene. Um den Zugriff ordnungsgemäß zu verwalten, sollten AWS Lambda-Funktionen einer VPC zugewiesen werden.

Kontroll-ID	AWS Config	Empfehlungen
Anexo II 4.3.2.b)	opensearch-in-vpc-only	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass sich Amazon OpenSearch Service-Domains innerhalb einer Amazon Virtual Private Cloud (Amazon VPC) befinden. Eine Amazon OpenSearch Service-Domain innerhalb einer Amazon VPC ermöglich t die sichere Kommunika tion zwischen Amazon OpenSearch Service und anderen Services innerhalb der Amazon VPC, ohne dass ein Internet-Gateway, ein NAT-Gerät oder eine VPN-Verbindung erforderlich ist.
Anexo II 4.3.2.b)	rds-instance-public-access-überprüfen	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherste llen, dass Amazon Relationa l Database Service (Amazon RDS) -Instances nicht öffentlic h sind. Amazon-RDS-Datenba nk-Instances können vertrauli che Informationen enthalten und für solche Konten sind Prinzipien und Zugriffsk ontrollen erforderlich.

Kontroll-ID	AWS Config	Empfehlungen
Anexo II 4.3.2.b)	rds-snapshots-public-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Relational Database Service (Amazon RDS) -Instances nicht öffentlich sind. Amazon-RDS-Datenbank-Instances können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.
Anexo II 4.3.2.b)	redshift-cluster-public-access-überprüfen	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Redshift Redshift-Cluster nicht öffentlich sind. Amazon-Redshift-Cluster können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	AWS Config	Empfehlungen
Anexo II 4.3.2.b)	restricted-common-ports	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass gemeinsame Ports für Amazon Elastic Compute Cloud (Amazon EC2) - Sicherheitsgruppen eingeschränkt sind. Wenn der Zugriff auf Ports nicht auf vertrauenswürdige Quellen beschränkt wird, kann dies zu Angriffen auf die Verfügbarkeit, Integrität und Vertraulichkeit von Systemen führen. Mit dieser Regel können Sie optional die Parameter blockedPort1–blockedPort5 festlegen (Standardkonfigurationen: 20, 21, 3389, 3306, 4333). Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	AWS Config	Empfehlungen
Anexo II 4.3.2.b)	s3- account-level-public-access -Block-periodisch	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Simple Storage Service (Amazon S3) -Buckets nicht öffentlich zugänglich sind. Diese Regel trägt dazu bei, sensible Daten vor unbefugten Remote-Benutzern zu schützen, indem sie den öffentlichen Zugriff verhindert. Mit dieser Regel können Sie optional die Parameter ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) und restrictPublicBuckets Parameter (Config Default: True) festlegen. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	AWS Config	Empfehlungen
Anexo II 4.3.2.b)	s3 bucket-level-public-access -verboten	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Simple Storage Service (Amazon S3) -Buckets nicht öffentlich zugänglich sind. Diese Regel trägt dazu bei, sensible Daten vor unbefugten Remote-Benutzern zu schützen, indem sie den öffentlichen Zugriff auf Bucket-Ebene verhindert.
Anexo II 4.3.2.b)	s-3 bucket-public-read-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie nur autorisierten Benutzern, Prozessen und Geräten Zugriff auf Amazon Simple Storage Service (Amazon S3) -Buckets gewähren. Die Verwaltung des Zugriffs sollte mit der Klassifizierung der Daten übereinstimmen.

Kontroll-ID	AWS Config	Empfehlungen
Anexo II 4.3.2.b)	s3- bucket-public-write-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie nur autorisierten Benutzern, Prozessen und Geräten Zugriff auf Amazon Simple Storage Service (Amazon S3) -Buckets gewähren. Die Verwaltung des Zugriffs sollte mit der Klassifizierung der Daten übereinstimmen.
Anexo II 4.3.2.b)	sagemaker-notebook-no-direct-Internetzugang	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass SageMaker Amazon-Notebooks keinen direkten Internetzugang zulassen. Indem Sie direkten Internetzugang blockieren, vermeiden Sie, dass unbefugte Benutzer auf sensible Daten zugreifen.

Kontroll-ID	AWS Config	Empfehlungen
Anexo II 4.3.2.b)	subnet-auto-assign-public-ip-deaktiviert	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon Virtual Private Cloud (VPC) -Subnetzen nicht automatis ch eine öffentliche IP-Adress e zugewiesen wird. Amazon Elastic Compute Cloud (EC2) -Instances, die in Subnetzen gestartet werden, in denen dieses Attribut aktiviert ist, haben ihrer primären Netzwerkschnittste lle eine öffentliche IP-Adresse zugewiesen.
Anexo II 4.3.2.b)	vpc-default-security-group-geschlossen	Sicherheitsgruppen von Amazon Elastic Compute Cloud (Amazon EC2) können bei der Verwaltung des Netzwerkzugriffs helfen, indem sie eine statusbeh aftete Filterung des ein- und ausgehenden Netzwerkv erkehrs zu Ressourcen bereitstellen. AWS Die Beschränkung des gesamten Datenverkehrs auf die Standardsicherheitsgruppe hilft dabei, den Fernzugriff auf Ihre Ressourcen einzuschr änken. AWS

Kontroll-ID	AWS Config	Empfehlungen
Anexo II 4.3.2.b)	vpc-sg-open-only-to-authorized-ports	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass gemeinsame Ports für Amazon Elastic Compute Cloud (Amazon EC2) - Sicherheitsgruppen eingeschränkt sind. Wenn der Zugriff auf Ports nicht auf vertrauenswürdige Quellen beschränkt wird, kann dies zu Angriffen auf die Verfügbarkeit, Integrität und Vertraulichkeit von Systemen führen. Durch die Beschränkung des Zugriffs auf Ressourcen innerhalb einer Sicherheitsgruppe aus dem Internet (0.0.0.0/0) kann der Remote-Zugriff auf interne Systeme gesteuert werden.

Kontroll-ID	AWS Config	Empfehlungen
Anexo II 4.3.4.c)	vuln-management-plan-exists (Prozessüberprüfung)	Stellen Sie sicher, dass ein Plan für das Schwachst ellenmanagement entwickel t und implementiert wird, damit Sie über formell definiert e Prozesse zur Behebung von Schwachstellen in Ihrer Umgebung verfügen. Dazu zählen Tools für das Schwachstellenmanagement, regelmäßige Umgebungs scans sowie entsprechende Rollen und Verantwortlichkeit en.
Anexo II 4.3.6	guardduty-enabled-centralized	Amazon GuardDuty kann mithilfe von Threat Intellige nce Feeds helfen, potenzielle Cybersicherheitsereignisse zu überwachen und zu erkennen. Dazu gehören Listen mit bösartigen IPs und maschinel len Lernmethoden zur Identifiz ierung unerwarteter, nicht autorisierter und bösartige r Aktivitäten in Ihrer AWS Cloud-Umgebung.

Kontroll-ID	AWS Config	Empfehlungen
Anexo II 4.3.7.a)	response-plan-exists-maintained (Prozessüberprüfung)	Stellen Sie sicher, dass Vorfallreaktionspläne erstellt, verwaltet und an das verantwortliche Personal verteilt werden. Aktualisierte und formal dokumentierte Reaktionspläne können dazu beitragen, dass das zuständige Personal die Rollen, Verantwortlichkeiten und Prozesse versteht, die bei einem Vorfall einzuhalten sind.
Anexo II 4.3.8	elasticsearch-logs-to-cloudwatch	Stellen Sie sicher, dass für Amazon OpenSearch Service-Domains Fehlerprotokolle aktiviert und zur Aufbewahrung und Beantwortung an Amazon CloudWatch Logs gestreamt werden. Domain-Fehlerprotokolle sind bei Sicherheits- und Zugriffsprüfungen sowie bei der Diagnose von Verfügbarkeitsproblemen nützlich.

Kontroll-ID	AWS Config	Empfehlungen
Anexo II 4.3.8	multi-region-cloudtrail-enabled	AWS CloudTrail zeichnet Aktionen und API-Aufrufe der AWS Management Console auf. Sie können feststellen, welche Benutzer und Konten angerufen wurden AWS, von welcher Quell-IP-Adresse aus die Anrufe getätigt wurden und wann die Anrufe erfolgten . CloudTrail übermittelt Protokolldateien aus allen AWS Regionen an Ihren S3-Bucket, wenn MULTI_REGION_CLOUD_TRAIL_ENABLED aktiviert ist. Außerdem wird beim AWS Start einer neuen Region derselbe Trail in der neuen Region erstellt. CloudTrail Dadurch erhalten Sie automatisch Protokoll dateien mit API-Aktivitäten für die neue Region.

Kontroll-ID	AWS Config	Empfehlungen
Anexo II 4.3.8	rds-logging-enabled	Um die Protokollierung und Überwachung in Ihrer Umgebung zu erleichtern, stellen Sie sicher, dass die Amazon Relational Database Service (Amazon RDS)-Protokollierung aktiviert ist. Mit der Amazon-RDS-Protokollierung können Sie Ereignisse wie Verbindungen, Verbindungsabbrüche, Abfragen oder abgefragte Tabellen erfassen.
Anexo II 4.3.8	wafv2-logging-enabled	Um die Protokollierung und Überwachung in Ihrer Umgebung zu erleichtern, aktivieren Sie die AWS WAF (V2) -Protokollierung im regionalen und globalen Web ACLs. AWS Die WAF-Protokollierung bietet detaillierte Informationen über den Datenverkehr, der von Ihrer Web-ACL analysiert wird. In den Protokollen werden die Uhrzeit aufgezeichnet, zu der die AWS WAF die Anfrage von Ihrer AWS Ressource erhalten hat, Informationen über die Anfrage und eine Aktion für die Regel, der jede Anfrage entsprach.

Kontroll-ID	AWS Config	Empfehlungen
Anexo II 4.3.8	api-gw-execution-logging-aktiviert	Die API-Gateway-Protokollierung zeigt detaillierte Ansichten der Benutzer, die auf die API zugegriffen haben, und wie diese Benutzer auf die API zugegriffen haben. Diese Einblicke ermöglichen die Transparenz von Benutzeraktivitäten.
Anexo II 4.3.8	cloud-trail-cloud-watch-logs-aktiviert	Verwenden Sie Amazon CloudWatch , um Protokollereignisaktivitäten zentral zu sammeln und zu verwalten . Die Aufnahme von AWS CloudTrail Daten liefert Einzelheiten zu den API-Aufrufaktivitäten in Ihrem AWS-Konto.

Kontroll-ID	AWS Config	Empfehlungen
Anexo II 4.3.8	cloudtrail-enabled	AWS CloudTrail kann bei der Nichtabstreitbarkeit helfen, indem Aktionen und API-Aufrufe der AWS Managemen t Console aufgezeichnet werden. Sie können die Benutzer und die Benutzer AWS-Konten , die einen AWS Dienst aufgerufen haben, die Quell-IP-Adresse, über die die Aufrufe generiert wurden, und den Zeitpunkt der Anrufe identifizieren. Einzelheiten zu den erfassten Daten finden Sie in den AWS CloudTrail Datensatzinhalten.
Anexo II 4.3.8	cloudtrail-s3-dataevents-en abled	Die Erfassung von Simple Storage Service (Amazon S3)-Datenereignissen unterstützt die Erkennung von ungewöhnl ichen Aktivitäten. Zu den Details gehören AWS-Konto Informationen über den Zugriff auf einen Amazon S3 S3-Bucket, die IP-Adresse und die Uhrzeit des Ereignisses.

Kontroll-ID	AWS Config	Empfehlungen
Anexo II 4.3.8	elb-logging-enabled	Die Elastic-Load-Balancing-Aktivität ist ein zentraler Kommunikationspunkt innerhalb einer Umgebung. Stellen Sie sicher, dass die ELB-Protokollierung aktiviert ist. Die gesammelten Daten enthalten detaillierte Informati onen zu Anfragen, die an den ELB gesendet wurden. Jedes Protokoll enthält Informati onen wie die Zeit, zu der die Anforderung einging, die Client-IP-Adresse, Latenzen, Anforderungspfade und Serverantworten.

Kontroll-ID	AWS Config	Empfehlungen
Anexo II 4.3.8	s-3 bucket-logging-enabled	Die Amazon Simple Storage Service (Amazon S3)-Serve rzugriffsprotokollierung bietet eine Methode zur Überwachung des Netzwerks im Hinblick auf potenzielle Cybersicherheitsereignisse. Die Ereignisse werden überwacht, indem detaillie rte Aufzeichnungen über die Anfragen erfasst werden, die an einen Amazon-S3-Bucket gestellt wurden. Jeder Zugriffsprotokolleintrag enthält Details zu einer einzelnen Zugriffsanfrage. Zu den Details gehören Anfordere r, Bucket-Name, Anforderu ngszeit, Anforderungsaktion, Antwortstatus und Fehlercode, falls relevant.

Kontroll-ID	AWS Config	Empfehlungen
Anexo II 4.3.8	vpc-flow-logs-enabled	VPC-Flow-Protokolle erfassen detaillierte Informationsdatensätze über den IP-Datenverkehr, der zu und von Netzwerkschnittstellen in Ihrer Amazon Virtual Private Cloud (Amazon VPC) fließt. Standardmäßig enthalten Flow-Protokolldatensätze Werte für die verschiedenen Komponenten des IP-Flows, einschließlich Quelle, Ziel und Protokoll.
Anexo II 4.3.8.BAJO	opensearch-logs-to-cloudwatch	Stellen Sie sicher, dass für Amazon OpenSearch Service-Domains Fehlerprotokolle aktiviert und zur Aufbewahrung und Beantwortung an Amazon CloudWatch Logs gestreamt werden. OpenSearch Service-Fehlerprotokolle können bei Sicherheits- und Zugriffsprüfungen helfen und bei der Diagnose von Verfügbarkeitsproblemen helfen.

Kontroll-ID	AWS Config	Empfehlungen
Anexo II 4.3.8.MEDIO	opensearch-logs-to-cloudwatch	Stellen Sie sicher, dass für Amazon OpenSearch Service-Domains Fehlerprotokolle aktiviert und zur Aufbewahrung und Beantwortung an Amazon CloudWatch Logs gestreamt werden. OpenSearch Service-Fehlerprotokolle können bei Sicherheits- und Zugriffsprüfungen helfen und bei der Diagnose von Verfügbarkeitsproblemen helfen.
Anexo II 4.3.10.b)	cloud-trail-encryption-enabled	Da sensible Daten vorhanden sein können und um Daten im Speicher zu schützen, sollten Sie sicherstellen, dass die Verschlüsselung für Ihre AWS CloudTrail Trails aktiviert ist.

Kontroll-ID	AWS Config	Empfehlungen
Anexo II 4.3.10.b)	cloud-trail-log-file-Validierung aktiviert	Verwenden Sie die AWS CloudTrail Protokolldateivalidierung, um die Integrität von Protokollen zu überprüfen. CloudTrail Mithilfe der Protokolldateivalidierung kann festgestellt werden, ob eine Protokolldatei geändert oder gelöscht wurde oder ob sie nach der Übermittlung CloudTrail unverändert geblieben ist. Dieses Feature wurde mit dem Branchenstandard entsprechenden Algorithmen entwickelt: SHA-256 für die Hashfunktion und SHA-256 mit RSA für digitale Signaturen. Aus diesem Grund ist es rechnerisch unmöglich, CloudTrail Protokolldateien unbemerkt zu ändern, zu löschen oder zu fälschen.

Kontroll-ID	AWS Config	Empfehlungen
Anexo II 4.3.10.d)	s-3 bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) unterstützt die Aufrechte rhaltung einer angemessenen Kapazität und Verfügbarkeit. CRR ermöglicht das automatis che, asynchrone Kopieren von Objekten in Amazon-S3 -Buckets, um die Datenverf ügbarkeit sicherzustellen.
Anexo II 4.6.1	guardduty-enabled-centralized	Amazon GuardDuty kann mithilfe von Threat Intellige nce Feeds helfen, potenzielle Cybersicherheitsereignisse zu überwachen und zu erkennen. Dazu gehören Listen mit bösartigen IPs und maschinel len Lernmethoden zur Identifiz ierung unerwarteter, nicht autorisierter und bösartige r Aktivitäten in Ihrer AWS Cloud-Umgebung.

Kontroll-ID	AWS Config	Empfehlungen
Anexo II 4.6.2	securityhub-enabled	AWS Security Hub hilft bei der Überwachung von unbefugte m Personal, Verbindungen, Geräten und Software. AWS Security Hub aggregiert, organisiert und priorisiert die Sicherheitswarnungen oder Ergebnisse mehrerer Dienste. AWS Einige dieser Dienste sind Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer und AWS Firewall Manager sowie AWS Partnerlösungen.
Anexo II 4.6.2	guardduty-enabled-centralized	Amazon GuardDuty kann mithilfe von Threat Intellige nce Feeds helfen, potenzielle Cybersicherheitsereignisse zu überwachen und zu erkennen. Dazu gehören Listen mit bösartigen IPs und maschinel len Lernmethoden zur Identifiz ierung unerwarteter, nicht autorisierter und bösartige r Aktivitäten in Ihrer AWS Cloud-Umgebung.

Kontroll-ID	AWS Config	Empfehlungen
Anexo II 5.2.3	security-awareness-program-exists (Prozessüberprüfung)	Etablieren und pflegen Sie ein Programm zur Förderung des Sicherheitsbewusst seins in Ihrer Organisation. Programme zur Förderung des Sicherheitsbewusstseins der Mitarbeiter vermitteln ihnen, wie sie ihre Organisation vor diversen Sicherheitsverletz ungen oder Sicherheitsvorfäll en schützen können.
Anexo II 5.4.2	elasticsearch-node-to-node-Verschlüsselungsprüfung	Stellen Sie sicher, dass die node-to-node Verschlüsselung für Amazon OpenSearch Service aktiviert ist. Node-to-nodeVerschlüsselung ermöglicht die TLS 1.2-Versc hlüsselung für die gesamte Kommunikation innerhalb der Amazon Virtual Private Cloud (Amazon VPC). Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	AWS Config	Empfehlungen
Anexo II 5.4.2	elbv-2 acm-certificate-required	Zum Schutz von eventuell vorhandenen sensiblen Daten sowie von Daten während der Übertragung muss die Verschlüsselung für Ihr Elastic Load Balancing aktiviert sein. Verwenden Sie AWS Certifica te Manager, um öffentlic he und private SSL/TLS-Z ertifikate mit AWS Diensten und internen Ressourcen zu verwalten, bereitzustellen und bereitzustellen.
Anexo II 5.4.2	elb-tls-https-listeners-nur	Stellen Sie sicher, dass Ihre Elastic Load Balancer (ELBs) mit SSL- oder HTTPS-Lis tenern konfiguriert sind. Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.
Anexo II 5.4.2	alb-http-to-https-Umleitung sprüfung	Um Daten während der Übertragung zu schützen, stellen Sie sicher, dass Ihr Application Load Balancer unverschlüsselte HTTP-Anfragen automatisch an HTTPS umleitet. Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	AWS Config	Empfehlungen
Anexo II 5.4.2	api-gw-ssl-enabled	Stellen Sie sicher, dass die REST-API-Stufen von Amazon API Gateway mit SSL-Zerti fikaten konfiguriert sind, damit Backend-Systeme überprüfe n können, ob Anforderungen von API Gateway stammen.
Anexo II 5.4.2	elb-acm-certificate-required	Zum Schutz von eventuell vorhandenen sensiblen Daten sowie von Daten während der Übertragung muss die Verschlüsselung für Ihr Elastic Load Balancing aktiviert sein. Verwenden Sie AWS Certifica te Manager, um öffentlic he und private SSL/TLS-Z ertifikate mit AWS Diensten und internen Ressourcen zu verwalten, bereitzustellen und bereitzustellen.
Anexo II 5.4.2	redshift-require-tls-ssl	Stellen Sie sicher, dass Ihre Amazon-Redshift-Cluster eine TLS/SSL-Verschlüsselung erfordern, um eine Verbindun g zu SQL-Clients herzustel len. Um eventuell vorhanden e sensible Daten zu schützen, sollten Sie die Verschlüs selung bei der Übertragung aktivieren.

Kontroll-ID	AWS Config	Empfehlungen
Anexo II 5.4.2	s-3 bucket-ssl-requests-only	Um Daten während der Übertragung zu schützen, stellen Sie sicher, dass Ihre Amazon Simple Storage Service (Amazon S3)-Buckets Anfragen zur Verwendung von Secure Socket Layer (SSL)-Buckets erfordern. Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.
Anexo II 5.4.2.MEDIO	opensearch-logs-to-cloudwatch	Stellen Sie sicher, dass für Amazon OpenSearch Service-Domains Fehlerprotokolle aktiviert und zur Aufbewahrung und Beantwortung an Amazon CloudWatch Logs gestreamt werden. OpenSearch Service-Fehlerprotokolle können bei Sicherheits- und Zugriffsprüfungen helfen und bei der Diagnose von Verfügbarkeitsproblemen helfen.

Kontroll-ID	AWS Config	Empfehlungen
Anexo II 5.4.3	elasticsearch-node-to-node-Verschlüsselungsprüfung	Stellen Sie sicher, dass die node-to-node Verschlüsselung für Amazon OpenSearch Service aktiviert ist. Node-to-nodeVerschlüsselung ermöglicht die TLS 1.2-Versc hlüsselung für die gesamte Kommunikation innerhalb der Amazon Virtual Private Cloud (Amazon VPC). Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.
Anexo II 5.4.3	elbv-2 acm-certificate-required	Zum Schutz von eventuell vorhandenen sensiblen Daten sowie von Daten während der Übertragung muss die Verschlüsselung für Ihr Elastic Load Balancing aktiviert sein. Verwenden Sie AWS Certifica te Manager, um öffentlic he und private SSL/TLS-Z ertifikate mit AWS Diensten und internen Ressourcen zu verwalten, bereitzustellen und bereitzustellen.

Kontroll-ID	AWS Config	Empfehlungen
Anexo II 5.4.3	elb-tls-https-listeners-nur	Stellen Sie sicher, dass Ihre Elastic Load Balancer (ELBs) mit SSL- oder HTTPS-Listenern konfiguriert sind. Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.
Anexo II 5.4.3	alb-http-to-https-Umleitungsprüfung	Um Daten während der Übertragung zu schützen, stellen Sie sicher, dass Ihr Application Load Balancer unverschlüsselte HTTP-Anfragen automatisch an HTTPS umleitet. Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.
Anexo II 5.4.3	api-gw-ssl-enabled	Stellen Sie sicher, dass die REST-API-Stufen von Amazon API Gateway mit SSL-Zertifikaten konfiguriert sind, damit Backend-Systeme überprüfen können, ob Anforderungen von API Gateway stammen.

Kontroll-ID	AWS Config	Empfehlungen
Anexo II 5.4.3	elb-acm-certificate-required	Zum Schutz von eventuell vorhandenen sensiblen Daten sowie von Daten während der Übertragung muss die Verschlüsselung für Ihr Elastic Load Balancing aktiviert sein. Verwenden Sie AWS Certifica te Manager, um öffentlic he und private SSL/TLS-Z ertifikate mit AWS Diensten und internen Ressourcen zu verwalten, bereitzustellen und bereitzustellen.
Anexo II 5.4.3	redshift-require-tls-ssl	Stellen Sie sicher, dass Ihre Amazon-Redshift-Cluster eine TLS/SSL-Verschlüsselung erfordern, um eine Verbindun g zu SQL-Clients herzustel len. Um eventuell vorhanden e sensible Daten zu schützen, sollten Sie die Verschlüs selung bei der Übertragung aktivieren.

Kontroll-ID	AWS Config	Empfehlungen
Anexo II 5.4.3	s-3 bucket-ssl-requests-only	Um Daten während der Übertragung zu schützen, stellen Sie sicher, dass Ihre Amazon Simple Storage Service (Amazon S3)-Buckets Anfragen zur Verwendung von Secure Socket Layer (SSL)-Buckets erfordern. Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.
Anexo II 5.4.3.MEDIO	opensearch-logs-to-cloudwatch	Stellen Sie sicher, dass für Amazon OpenSearch Service-Domains Fehlerprotokolle aktiviert und zur Aufbewahrung und Beantwortung an Amazon CloudWatch Logs gestreamt werden. OpenSearch Service-Fehlerprotokolle können bei Sicherheits- und Zugriffsprüfungen helfen und bei der Diagnose von Verfügbarkeitsproblemen helfen.

Kontroll-ID	AWS Config	Empfehlungen
Anexo II 5.4.3.a)	iam-password-policy	Die Identitäten und Anmeldein formationen werden auf der Grundlage einer organisat orischen IAM-Passwortrichtl inie ausgestellt, verwaltet und verifiziert. Sie erfüllen oder übertreffen die Anforderungen von NIST SP 800-63 und dem Standard „Best Practices“ von AWS Foundational Security für die Passwortstärke. Mit dieser Regel können Sie optional RequireUppercaseCharacters (Wert für AWS grundlege nde Sicherheitsbewährte Methoden: wahr), RequireLo wercaseCharacters (Wert für bewährte Methoden für AWS grundlegende Sicherheit: wahr), RequireSymbols (Wert für bewährte Methoden für AWS grundlegende Sicherhei t: wahr), RequireNumbers (Wert für bewährte Methoden für AWS grundlegende Sicherheit: wahr), MinimumPa sswordLength (Wert für bewährte Methoden für AWS grundlegende Sicherheit: 14), PasswordReusePreve ntion (Wert für bewährte Methoden für AWS grundlege nde Sicherheit: 24) und MaxPasswordAge (Wert

Kontroll-ID	AWS Config	Empfehlungen
		für bewährte Methoden für AWS grundlegende Sicherhei t: 90) für Ihr IAM festlegen Kennwortrichtlinie. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisat ion entsprechen.
Anexo II 5.6.1.c)	codebuild-project-envvar-aw scred-überprüfen	Stellen Sie sicher, dass die Anmeldeinformationen AWS_ACCESS_KEY_ID AWS_SECRET_ACCESS_ KEY nicht in AWS Codebuild -Projektumgebungen vorhanden sind. Speichern Sie diese Variablen nicht als Klartext. Das Speichern dieser Variablen als Klartext bewirkt eine unbeabsichtigte Offenlegung von Daten sowie unberechtigte Zugriffe.

Kontroll-ID	AWS Config	Empfehlungen
Anexo II 5.6.1.c)	codebuild-project-source-repo-URL-Prüfung	Stellen Sie sicher, dass die URL des Quell-Repositorys GitHub oder des Bitbucket -Quell-Repositorys keine persönlichen Zugriffstoken oder Anmeldeinformationen in Codebuild-Projektumgebungen enthält. AWS Verwende OAuth anstelle von persönlichen Zugriffstoken oder Anmeldedaten die Autorisierung für den Zugriff auf GitHub Bitbucket-Repositorys.
Anexo II 5.7.3	dynamodb-table-encrypted-kms	Stellen Sie sicher, dass die Verschlüsselung für Ihre Amazon-DynamoDB-Tabellen aktiviert ist. Um eventuell vorhandene sensible Daten im Ruhezustand in diesen Tabellen zu schützen, müssen Sie die Verschlüsselung von Daten im Ruhezustand aktivieren. Standardmäßig werden DynamoDB-Tabellen mit einem AWS eigenen Kundenhauptschlüssel (CMK) verschlüsselt.

Kontroll-ID	AWS Config	Empfehlungen
Anexo II 5.7.3	ec2- ebs-encryption-by-default	Zum Schutz von Daten im Ruhezustand müssen Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon Elastic Block Store (Amazon EBS)-Volumes aktiviert ist. Da sensible Daten auch im Ruhezusta nd vorhanden sein können, sollten Sie die Verschlüs selung im Ruhezustand aktivieren, um diese Daten zu schützen.
Anexo II 5.7.3	elasticsearch-node-to-node-Verschlüsselungsprüfung	Stellen Sie sicher, dass die node-to-node Verschlüsselung für Amazon OpenSearch Service aktiviert ist. Node-to-nodeVerschlüsselung ermöglicht die TLS 1.2-Versc hlüsselung für die gesamte Kommunikation innerhalb der Amazon Virtual Private Cloud (Amazon VPC). Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	AWS Config	Empfehlungen
Anexo II 5.7.3	elb-tls-https-listeners-nur	Stellen Sie sicher, dass Ihre Elastic Load Balancer (ELBs) mit SSL- oder HTTPS-Listenern konfiguriert sind. Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.
Anexo II 5.7.3	rds-snapshot-encrypted	Stellen Sie sicher, dass die Verschlüsselung für Ihre Amazon Relational Database Service (Amazon RDS)-Snapshots aktiviert ist. Da sensible Daten auch im Ruhezustand vorhanden sein können, sollten Sie die Verschlüsselung im Ruhezustand aktivieren, um diese Daten zu schützen.
Anexo II 5.7.3	s-3 default-encryption-kms	Stellen Sie sicher, dass die Verschlüsselung für Ihre Amazon Simple Storage Service (Amazon S3)-Buckets aktiviert ist. Um eventuell vorhandene sensible Daten im Ruhezustand in einem Amazon-S3-Bucket zu schützen, muss die Verschlüsselung aktiviert sein.

Kontroll-ID	AWS Config	Empfehlungen
Anexo II 5.7.3	sagemaker-notebook-instance-kms-key-konfiguriert	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass die Verschlüsselung mit dem AWS Key Management Service (AWS KMS) für Ihr Notebook aktiviert ist. SageMaker Da vertrauliche Daten im SageMaker Notebook gespeichert werden können, sollten Sie die Verschlüsselung im Ruhezustand aktivieren, um diese Daten zu schützen.
Anexo II 5.7.3	sns-encrypted-kms	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass Ihre Amazon Simple Notification Service (Amazon SNS) -Themen mit dem AWS Key Management Service (AWS KMS) verschlüsselt werden müssen. Um eventuell vorhandene sensible Daten im Ruhezustand in veröffentlichten Nachrichten zu schützen, muss die Verschlüsselung von Daten im Ruhezustand aktiviert sein.

Kontroll-ID	AWS Config	Empfehlungen
Anexo II 5.7.3	alb-http-to-https-Umleitung sprüfung	Um Daten während der Übertragung zu schützen, stellen Sie sicher, dass Ihr Application Load Balancer unverschlüsselte HTTP-Anfragen automatisch an HTTPS umleitet. Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.
Anexo II 5.7.3	api-gw-cache-enabled-und-ve rschlüsselt	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass die Verschlüsselung für den Cache Ihrer API-Gatew ay-Stufe aktiviert ist. Da für die API-Methode sensible Daten erfasst werden können, sollten Sie die Verschlüsselung von Daten im Ruhezustand aktivieren, um diese Daten zu schützen.
Anexo II 5.7.3	api-gw-ssl-enabled	Stellen Sie sicher, dass die REST-API-Stufen von Amazon API Gateway mit SSL-Zerti fikaten konfiguriert sind, damit Backend-Systeme überprüfe n können, ob Anforderungen von API Gateway stammen.

Kontroll-ID	AWS Config	Empfehlungen
Anexo II 5.7.3	cloud-trail-encryption-enabled	Da sensible Daten vorhanden sein können und um Daten im Ruhezustand zu schützen, sollten Sie sicherstellen, dass die Verschlüsselung für Ihre AWS CloudTrail Trails aktiviert ist.
Anexo II 5.7.3	cloudwatch-log-group-encrypted	Um sensible Daten im Speicher zu schützen, stellen Sie sicher, dass die Verschlüsselung für Ihre Amazon CloudWatch Log Groups aktiviert ist.
Anexo II 5.7.3	efs-encrypted-check	Aktivieren Sie die Verschlüsselung für Ihr Amazon Elastic File System (EFS), um eventuell vorhandene sensible Daten sowie Daten im Ruhezustand zu schützen.
Anexo II 5.7.3	elasticsearch-encrypted-at-rest	Da sensible Daten vorhanden sein können und um Daten im Ruhezustand zu schützen, sollten Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon OpenSearch Service (OpenSearch Service) -Domains aktiviert ist.

Kontroll-ID	AWS Config	Empfehlungen
Anexo II 5.7.3	elb-acm-certificate-required	Zum Schutz von eventuell vorhandenen sensiblen Daten sowie von Daten während der Übertragung muss die Verschlüsselung für Ihr Elastic Load Balancing aktiviert sein. Verwenden Sie AWS Certifica te Manager, um öffentlic he und private SSL/TLS-Z ertifikate mit AWS Diensten und internen Ressourcen zu verwalten, bereitzustellen und bereitzustellen.
Anexo II 5.7.3	encrypted-volumes	Aktivieren Sie die Verschlüs selung für Ihre Amazon-El astic-Block-Store (Amazon-EBS)-Volumes, um eventuell vorhandene sensible Daten sowie Daten im Ruhezustand zu schützen.
Anexo II 5.7.3	opensearch-encrypted-at-rest	Da sensible Daten vorhanden sein können und um Daten im Ruhezustand zu schützen, sollten Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon OpenSearch Service-Domains aktiviert ist.

Kontroll-ID	AWS Config	Empfehlungen
Anexo II 5.7.3	opensearch-node-to-node-Verschlüsselungsprüfung	Stellen Sie sicher, dass die node-to-node Verschlüsselung für Amazon OpenSearch Service aktiviert ist. Node-to-nodeVerschlüsselung ermöglicht die TLS 1.2-Verschlüsselung für die gesamte Kommunikation innerhalb der Amazon Virtual Private Cloud (Amazon VPC). Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.
Anexo II 5.7.3	rds-storage-encrypted	Zum Schutz von Daten im Ruhezustand müssen Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon Relational Database Service (Amazon RDS)-Instances aktiviert ist. Um eventuell vorhandene sensible Daten im Ruhezustand in Amazon-RDS-Instances zu schützen, muss die Verschlüsselung von Daten im Ruhezustand aktiviert sein.

Kontroll-ID	AWS Config	Empfehlungen
Anexo II 5.7.3	redshift-cluster-configuration-check	Um Daten im Ruhezustand zu schützen, muss die Verschlüsselung für Ihre Amazon-Redshift-Cluster aktiviert sein. Sie müssen auch sicherstellen, dass die erforderlichen Konfigurationen auf Amazon-Redshift-Clustern bereitgestellt werden. Die Prüfungsprotokollierung muss aktiviert sein, um Informationen zu Verbindungen und Benutzeraktivitäten in der Datenbank bereitzustellen. Diese Regel erfordert, dass ein Wert für clusterDbEncrypted (Config Default: TRUE) und LoggingEnabled (Config Default: TRUE) gesetzt ist. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	AWS Config	Empfehlungen
Anexo II 5.7.3	redshift-cluster-kms-enabled	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass die Verschlüsselung mit AWS Key Management Service (AWS KMS) für Ihren Amazon Redshift Redshift-Cluster aktiviert ist. Um eventuell vorhandene sensible Daten im Ruhezustand in Redshift-Clustern zu schützen, muss die Verschlüsselung von Daten im Ruhezustand aktiviert sein.
Anexo II 5.7.3	redshift-require-tls-ssl	Stellen Sie sicher, dass Ihre Amazon-Redshift-Cluster eine TLS/SSL-Verschlüsselung erfordern, um eine Verbindun g zu SQL-Clients herzustel len. Um eventuell vorhanden e sensible Daten zu schützen, sollten Sie die Verschlüs selung bei der Übertragung aktivieren.

Kontroll-ID	AWS Config	Empfehlungen
Anexo II 5.7.3	s3- aktiviert bucket-server-side -encryption	Zum Schutz von Daten im Ruhezustand müssen Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon Simple Storage Service (Amazon S3)-Bucke ts aktiviert ist. Um eventuell vorhandene sensible Daten im Ruhezustand in Amazon-S3 -Buckets zu schützen, muss die Verschlüsselung aktiviert sein.
Anexo II 5.7.3	s-3 bucket-ssl-requests-only	Um Daten während der Übertragung zu schützen, stellen Sie sicher, dass Ihre Amazon Simple Storage Service (Amazon S3)-Bucke ts Anfragen zur Verwendun g von Secure Socket Layer (SSL)-Buckets erfordern. Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	AWS Config	Empfehlungen
Anexo II 5.7.3	sagemaker-endpoint-configuration-kms-key-konfiguriert	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass die Verschlüsselung mit dem AWS Key Management Service (AWS KMS) für Ihren Endpunkt aktiviert ist. SageMaker Da sensible Daten auf dem SageMaker Endgerät gespeichert werden können, sollten Sie die Verschlüsselung im Ruhezustand aktivieren, um diese Daten zu schützen.
Anexo II 5.7.3	secretsmanager-using-cmk	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass die Verschlüsselung mit dem AWS Key Management Service (AWS KMS) für AWS Secrets Manager aktiviert ist. Aktivieren Sie die Verschlüsselung von Daten im Ruhezustand, um eventuell vorhandene sensible Daten im Ruhezustand im Secrets Manager zu schützen.
Anexo II 5.7.4	cmk-backing-key-rotation-aktiviert	Aktivieren Sie die Schlüssel rotation, um sicherzustellen, dass Schlüssel rotiert werden, nachdem sie das Ende ihrer Krypto-Periode erreicht haben.

Kontroll-ID	AWS Config	Empfehlungen
Anexo II 5.7.4	kms-cmk-not-scheduled-zum Löschen	Um Daten im Ruhezustand zu schützen, sollten Sie sicherstellen, dass die für den Kunden erforderlichen Masterschlüssel (CMKs) nicht im AWS Key Management Service (AWS KMS) gelöscht werden. Da Schlüssel manchmal gelöscht werden müssen, können Sie mit dieser Regel alle zu löschenden Schlüssel überprüfen, falls ein Schlüssel versehentlich zur Löschung vorgemerkt wurde.
Anexo II 5.8.2	alb-waf-enabled	Stellen Sie sicher, dass AWS WAF auf Elastic Load Balancers (ELB) aktiviert ist, um Webanwendungen zu schützen. Eine WAF trägt zum Schutz Ihrer Webanwendungen oder APIs vor gängigen Web-Exploits bei. Diese Web-Exploits können sich auf die Verfügbarkeit auswirken, die Sicherheit gefährden oder übermäßige Ressourcen in Ihrer Umgebung verbrauchen.

Kontroll-ID	AWS Config	Empfehlungen
Anexo II 5.8.2	api-gw-associated-with-WAF	AWS Mit WAF können Sie eine Reihe von Regeln (als Web Access Control List (Web ACL) bezeichnet) konfiguri eren, die Webanfragen auf der Grundlage von anpassbar en Websicherheitsregeln und -bedingungen, die Sie definieren, zulassen, blockiere n oder zählen. Stellen Sie sicher, dass Ihre Amazon-API-Gateway-Stufe mit einer WAF-Web-ACL verknüpft ist, um sie vor böswilligen Angriffen zu schützen.
Anexo II 5.8.3.b)	alb-waf-enabled	Stellen Sie sicher, dass AWS WAF auf Elastic Load Balancers (ELB) aktiviert ist, um Webanwendungen zu schützen. Eine WAF trägt zum Schutz Ihrer Webanwend ungen oder APIs vor gängigen Web-Exploits bei. Diese Web-Exploits können sich auf die Verfügbarkeit auswirken, die Sicherheit gefährden oder übermäßige Ressourcen in Ihrer Umgebung verbrauchen.

Kontroll-ID	AWS Config	Empfehlungen
Anexo II 5.8.3.b)	api-gw-associated-with-WAF	AWS Mit WAF können Sie eine Reihe von Regeln (als Web Access Control List (Web ACL) bezeichnet) konfiguri eren, die Webanfragen auf der Grundlage von anpassbar en Websicherheitsregeln und -bedingungen, die Sie definieren, zulassen, blockiere n oder zählen. Stellen Sie sicher, dass Ihre Amazon-API-Gateway-Stufe mit einer WAF-Web-ACL verknüpft ist, um sie vor böswilligen Angriffen zu schützen.
Anexo II 5.8.3.b)	elb-cross-zone-load-Balancing aktiviert	Aktivieren Sie zonenüber greifendes Load Balancing für Ihre Elastic Load Balancer (ELBs), um eine angemesse ne Kapazität und Verfügbar keit aufrechtzuerhalten. Zonenübergreifendes Load Balancing reduziert die Notwendigkeit, die gleiche Anzahl von Instances in jeder aktivierten Availability Zone aufrechtzuerhalten. Es verbessert auch die Fähigkeit Ihrer Anwendung, den Verlust einer oder mehrerer Instances zu bewältigen.

Kontroll-ID	AWS Config	Empfehlungen
Anexo II 5.8.3.b)	rds-instance-deletion-protection-aktiviert	Stellen Sie sicher, dass Amazon Relational Database Service (Amazon RDS)-Instances den Löschschutz aktiviert haben. Verwenden Sie den Löschschutz, um zu verhindern, dass Ihre Amazon-RDS-Instances versehentlich oder böswillig gelöscht werden, was zum Verlust der Verfügbarkeit Ihrer Anwendungen führen kann.
Anexo II 5.8.3.b)	dynamodb-autoscaling-enabled	Amazon DynamoDB Auto Scaling verwendet den AWS Application Auto Scaling-Service, um die bereitgestellte Durchsatzkapazität so anzupassen, dass sie automatisch auf tatsächliche Verkehrsmuster reagiert. Auf diese Weise kann eine Tabelle oder ein globaler sekundärer Index die bereitgestellte Lese-/Schreibkapazität erhöhen, um plötzliche Erhöhungen des Datenverkehrs ohne Drosselung zu bewältigen.

Kontroll-ID	AWS Config	Empfehlungen
Anexo II 5.8.3.b)	elb-deletion-protection-enabled	Diese Regel sorgt dafür, dass der Löschschutz für Elastic Load Balancing aktiviert ist. Verwenden Sie diese Funktion, um zu verhindern, dass Ihr Load Balancer versehentlich oder böswillig gelöscht wird, was zum Verlust der Verfügbarkeit Ihrer Anwendungen führen kann.

Kontroll-ID	AWS Config	Empfehlungen
Anexo II 5.8.3.b)	rds-multi-az-support	Die Multi-AZ-Unterstützung in Amazon Relational Database Service (Amazon RDS) bietet eine verbesserte Verfügbar keit und Beständigkeit von Datenbank-Instances. Wenn Sie eine Multi-AZ-Datenbank-Instance bereitstellen, erstellt Amazon RDS automatisch eine primäre Datenbank-Instance und repliziert die Daten synchron auf eine Standby-Instance in einer anderen Availability Zone. Jede Availability Zone läuft auf einer eigenen, physisch getrennten, unabhängigen Infrastruktur und ist auf eine hohe Verfügbarkeit ausgelegt . Im Falle eines Infrastru kturausfalls führt Amazon RDS einen automatischen Failover zum Standby-Modus durch, sodass Sie den Datenbank betrieb wieder aufnehmen können, sobald der Failover abgeschlossen ist.

Kontroll-ID	AWS Config	Empfehlungen
Anexo II 5.8.3.b)	rds-cluster-multi-az-aktiviert	Die Multi-AZ-Unterstützung in Amazon Relational Database Service (Amazon RDS) bietet eine verbesserte Verfügbar keit und Beständigkeit von Datenbank-Instances. Wenn Sie eine Multi-AZ-Datenbank-Instance bereitstellen, erstellt Amazon RDS automatisch eine primäre Datenbank-Instance und repliziert die Daten synchron auf eine Standby-Instance in einer anderen Availability Zone. Jede Availability Zone läuft auf einer eigenen, physisch getrennten, unabhängigen Infrastruktur und ist auf eine hohe Verfügbarkeit ausgelegt . Im Falle eines Infrastru kturausfalls führt Amazon RDS einen automatischen Failover zum Standby-Modus durch, sodass Sie den Datenbank betrieb wieder aufnehmen können, sobald der Failover abgeschlossen ist.

Kontroll-ID	AWS Config	Empfehlungen
Anexo II 5.8.3.b)	vpc-vpn-2-tunnels-up	Redundante Site-to-Site VPN-Tunnel können implement iert werden, um die Anforderu ngen an die Ausfallsicherheit zu erfüllen. Es verwendet zwei Tunnel, um die Konnektiv ität sicherzustellen, falls eine der Site-to-Site VPN-Verbi ndungen nicht verfügbar ist. Um sich vor einem Verbindun gsverlust zu schützen, können Sie für den Fall, dass Ihr Kunden-Gateway nicht verfügbar ist, eine zweite Site-to-Site VPN-Verbindung zu Ihrer Amazon Virtual Private Cloud (Amazon VPC) und Ihrem Virtual Private Gateway einrichten, indem Sie ein zweites Kunden-Gateway verwenden.

Kontroll-ID	AWS Config	Empfehlungen
Art. 14.4	iam-root-access-key-überprüfen	Der Zugriff auf Systeme und Ressourcen kann gesteuert werden, indem überprüft wird, ob der Root-Benutzer keine Zugriffsschlüssel mit seiner AWS Identity and Access Management (IAM) -Rolle verknüpft hat. Stellen Sie sicher, dass die Root-Zugriffsschlüssel gelöscht werden. Erstellen und verwenden Sie stattdessen rollenbasierte Funktionen, AWS-Konten um das Prinzip der geringsten Funktionalität zu berücksichtigen.
Art. 16	ecs-task-definition-user-for-host-mode-check	Wenn für eine Aufgabendefinition erhöhte Berechtigungen gelten, liegt das daran, dass der Kunde diesen Konfigurationen ausdrücklich zugestimmt hat. Diese Kontrolle prüft, ob eine unerwartete Berechtigungseskalation vorliegt, wenn für eine Aufgabendefinition das Host-Netzwerk aktiviert ist, die Kunden aber keine erhöhten Berechtigungen aktiviert haben.

Kontroll-ID	AWS Config	Empfehlungen
Art. 16	iam-policy-no-statements-with-full-access	Stellen Sie sicher, dass IAM-Aktionen nur auf die benötigte n Aktionen beschränkt sind. Wenn Benutzern mehr Rechte eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und der Aufgabentrennung verstoßen.
Art. 16	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) kann Ihnen dabei helfen, die Prinzipien der geringsten Rechte und der Aufgabent rennung in Zugriffsberechtigu ngen und Autorisierungen zu integrieren und so zu verhindern, dass Richtlinien „Effect“: „Allow“ mit „Action“: „*“ anstelle von „Resource“: „*“ enthalten. Wenn Benutzern mehr Rechte eingeräumt werden, als für die Ausführun g einer Aufgabe erforderl ich sind, kann dies gegen das Prinzip der geringste n Berechtigung und der Aufgabentrennung verstoßen.

Kontroll-ID	AWS Config	Empfehlungen
Art. 16	s3- bucket-policy-grantee-check	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie s3_bucket_policy_grantee_check aktivieren. Diese Regel prüft, ob der vom Amazon S3 S3-Bucket gewährte Zugriff durch die von Ihnen bereitgestellten AWS Principals, Verbundbenutzer, Service Principals, IP-Adressen oder Amazon Virtual Private Cloud (Amazon VPC) IDs eingeschränkt ist.
Art. 20.2	rds-automatic-minor-version-Upgrade-fähig	Aktivieren Sie automatische Unterversions-Upgrades auf Ihren Amazon-Relational-Database-Service (RDS)-Instances, um sicherzustellen, dass die aktuellen Updates für Unterversionen des Relational Database Management System (RDBMS) installiert sind, die Sicherheitspatches und Bugfixes enthalten können.

Kontroll-ID	AWS Config	Empfehlungen
Art. 20.2	ec2- prüfen managedinstance-patch-compliance-status	Aktivieren Sie diese Regel, um bei der Identifizierung und Dokumentation von Sicherheitslücken in Amazon Elastic Compute Cloud (Amazon EC2) zu helfen. Die Regel prüft, ob die EC2 Amazon-Instance die Patch-Konformität im AWS Systems Manager gemäß den Richtlinien und Verfahren Ihrer Organisation einhält.
Art. 20.2	elastic-beanstalk-managed-updates-aktiviert	Durch die Aktivierung verwalteter Plattformupdates für eine Amazon-Elastic-Beanstalk-Umgebung wird sichergestellt, dass die aktuellen verfügbaren Plattform-Fixes, -Updates und -Features für die Umgebung installiert sind. Eine bewährte Methode zur Sicherung von Systemen besteht darin, stets die aktuellen Patches zu installieren.

Kontroll-ID	AWS Config	Empfehlungen
Art. 20.2	vuln-management-plan-exists (Prozessüberprüfung)	Stellen Sie sicher, dass ein Plan für das Schwachst ellenmanagement entwickel t und implementiert wird, damit Sie über formell definiert e Prozesse zur Behebung von Schwachstellen in Ihrer Umgebung verfügen. Dazu zählen Tools für das Schwachstellenmanagement, regelmäßige Umgebungs scans sowie entsprechende Rollen und Verantwortlichkeit en.
Art. 21.1	dynamodb-table-encrypted-km s	Stellen Sie sicher, dass die Verschlüsselung für Ihre Amazon-DynamoDB-Tabellen aktiviert ist. Um eventuell vorhandene sensible Daten im Ruhezustand in diesen Tabellen zu schützen, müssen Sie die Verschlüsselung von Daten im Ruhezustand aktivieren. Standardmäßig werden DynamoDB-Tabellen mit einem AWS eigenen Kundenhauptschlüssel (CMK) verschlüsselt.

Kontroll-ID	AWS Config	Empfehlungen
Art. 21.1	ec2- ebs-encryption-by-default	Zum Schutz von Daten im Ruhezustand müssen Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon Elastic Block Store (Amazon EBS)-Volumes aktiviert ist. Da sensible Daten auch im Ruhezusta nd vorhanden sein können, sollten Sie die Verschlüs selung im Ruhezustand aktivieren, um diese Daten zu schützen.
Art. 21.1	elasticsearch-node-to-node-Verschlüsselungsprüfung	Stellen Sie sicher, dass die node-to-node Verschlüsselung für Amazon OpenSearch Service aktiviert ist. Node-to-nodeVerschlüsselung ermöglicht die TLS 1.2-Versc hlüsselung für die gesamte Kommunikation innerhalb der Amazon Virtual Private Cloud (Amazon VPC). Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	AWS Config	Empfehlungen
Art. 21.1	elb-cross-zone-load-Balancing aktiviert	Aktivieren Sie zonenüber greifendes Load Balancing für Ihre Elastic Load Balancer (ELBs), um eine angemesse ne Kapazität und Verfügbar keit aufrechtzuerhalten. Zonenübergreifendes Load Balancing reduziert die Notwendigkeit, die gleiche Anzahl von Instances in jeder aktivierten Availability Zone aufrechtzuerhalten. Es verbessert auch die Fähigkeit Ihrer Anwendung, den Verlust einer oder mehrerer Instances zu bewältigen.
Art. 21.1	elb-tls-https-listeners-nur	Stellen Sie sicher, dass Ihre Elastic Load Balancer (ELBs) mit SSL- oder HTTPS-Lis tenern konfiguriert sind. Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	AWS Config	Empfehlungen
Art. 21.1	rds-instance-deletion-protection-aktiviert	Stellen Sie sicher, dass Amazon Relational Database Service (Amazon RDS)-Instances den Löschschutz aktiviert haben. Verwenden Sie den Löschschutz, um zu verhindern, dass Ihre Amazon-RDS-Instances versehentlich oder böswillig gelöscht werden, was zum Verlust der Verfügbarkeit Ihrer Anwendungen führen kann.
Art. 21.1	rds-snapshot-encrypted	Stellen Sie sicher, dass die Verschlüsselung für Ihre Amazon Relational Database Service (Amazon RDS)-Snapshots aktiviert ist. Da sensible Daten auch im Ruhezustand vorhanden sein können, sollten Sie die Verschlüsselung im Ruhezustand aktivieren, um diese Daten zu schützen.
Art. 21.1	s3- bucket-default-lock-enabled	Stellen Sie sicher, dass für Ihren Amazon Simple Storage Service (Amazon S3)-Bucket standardmäßig eine Sperre aktiviert ist. Zum Schutz eventuell vorhandener sensibler Daten in S3-Buckets müssen Sie Objektsperren für Daten im Ruhezustand erzwingen.

Kontroll-ID	AWS Config	Empfehlungen
Art. 21.1	s-3 default-encryption-kms	Stellen Sie sicher, dass die Verschlüsselung für Ihre Amazon Simple Storage Service (Amazon S3)-Bucke ts aktiviert ist. Um eventuell vorhandene sensible Daten im Ruhezustand in einem Amazon-S3-Bucket zu schützen, muss die Verschlüs selung aktiviert sein.
Art. 21.1	sagemaker-notebook-instance -kms-key-konfiguriert	Um Daten im Ruhezusta nd zu schützen, stellen Sie sicher, dass die Verschlüs selung mit dem AWS Key Management Service (AWS KMS) für Ihr Notebook aktiviert ist. SageMaker Da vertrauli che Daten im SageMaker Notebook gespeichert werden können, sollten Sie die Verschlüsselung im Ruhezustand aktivieren, um diese Daten zu schützen.

Kontroll-ID	AWS Config	Empfehlungen
Art. 21.1	sns-encrypted-kms	Um Daten im Ruhezusta nd zu schützen, stellen Sie sicher, dass Ihre Amazon Simple Notification Service (Amazon SNS) -Themen mit dem AWS Key Management Service (AWS KMS) verschlüs selt werden müssen. Um eventuell vorhandene sensible Daten im Ruhezustand in veröffentlichten Nachricht en zu schützen, muss die Verschlüsselung von Daten im Ruhezustand aktiviert sein.
Art. 21.1	alb-http-to-https-Umleitung sprüfung	Um Daten während der Übertragung zu schützen, stellen Sie sicher, dass Ihr Application Load Balancer unverschlüsselte HTTP-Anfragen automatisch an HTTPS umleitet. Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	AWS Config	Empfehlungen
Art. 21.1	api-gw-cache-enabled-und-verschlüsselt	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass die Verschlüsselung für den Cache Ihrer API-Gateway-Stufe aktiviert ist. Da für die API-Methode sensible Daten erfasst werden können, sollten Sie die Verschlüsselung von Daten im Ruhezustand aktivieren, um diese Daten zu schützen.
Art. 21.1	api-gw-ssl-enabled	Stellen Sie sicher, dass die REST-API-Stufen von Amazon API Gateway mit SSL-Zertifikaten konfiguriert sind, damit Backend-Systeme überprüfen können, ob Anforderungen von API Gateway stammen.
Art. 21.1	cloud-trail-encryption-enabled	Da sensible Daten vorhanden sein können und um Daten im Ruhezustand zu schützen, sollten Sie sicherstellen, dass die Verschlüsselung für Ihre AWS CloudTrail Trails aktiviert ist.

Kontroll-ID	AWS Config	Empfehlungen
Art. 21.1	cloud-trail-log-file-Validierung aktiviert	Verwenden Sie die AWS CloudTrail Protokolldateivalidierung, um die Integrität von Protokollen zu überprüfen. CloudTrail Mithilfe der Protokolldateivalidierung kann festgestellt werden, ob eine Protokolldatei geändert oder gelöscht wurde oder ob sie nach der Übermittlung CloudTrail unverändert geblieben ist. Dieses Feature wurde mit dem Branchenstandard entsprechenden Algorithmen entwickelt: SHA-256 für die Hashfunktion und SHA-256 mit RSA für digitale Signaturen. Aus diesem Grund ist es rechnerisch unmöglich, CloudTrail Protokolldateien unbemerkt zu ändern, zu löschen oder zu fälschen.
Art. 21.1	cloudwatch-log-group-encrypted	Um sensible Daten im Speicher zu schützen, stellen Sie sicher, dass die Verschlüsselung für Ihre Amazon CloudWatch Log Groups aktiviert ist.

Kontroll-ID	AWS Config	Empfehlungen
Art. 21.1	dynamodb-autoscaling-enabled	Amazon DynamoDB Auto Scaling verwendet den AWS Application Auto Scaling-Service, um die bereitgestellte Durchsatzkapazität so anzupassen, dass sie automatisch auf tatsächliche Verkehrsmuster reagiert. Auf diese Weise kann eine Tabelle oder ein globaler sekundärer Index die bereitgestellte Lese-/Schreibkapazität erhöhen, um plötzliche Erhöhungen des Datenverkehrs ohne Drosselung zu bewältigen.
Art. 21.1	efs-encrypted-check	Aktivieren Sie die Verschlüsselung für Ihr Amazon Elastic File System (EFS), um eventuell vorhandene sensible Daten sowie Daten im Ruhezustand zu schützen.
Art. 21.1	elasticsearch-encrypted-at-rest	Da sensible Daten vorhanden sein können und um Daten im Ruhezustand zu schützen, sollten Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon OpenSearch Service (OpenSearch Service) -Domains aktiviert ist.

Kontroll-ID	AWS Config	Empfehlungen
Art. 21.1	elb-acm-certificate-required	Zum Schutz von eventuell vorhandenen sensiblen Daten sowie von Daten während der Übertragung muss die Verschlüsselung für Ihr Elastic Load Balancing aktiviert sein. Verwenden Sie AWS Certifica te Manager, um öffentlic he und private SSL/TLS-Z ertifikate mit AWS Diensten und internen Ressourcen zu verwalten, bereitzustellen und bereitzustellen.
Art. 21.1	elb-deletion-protection-ena bled	Diese Regel sorgt dafür, dass der Löschschutz für Elastic Load Balancing aktiviert ist. Verwenden Sie diese Funktion, um zu verhinder n, dass Ihr Load Balancer versehentlich oder böswillig gelöscht wird, was zum Verlust der Verfügbarkeit Ihrer Anwendungen führen kann.
Art. 21.1	encrypted-volumes	Aktivieren Sie die Verschlüs selung für Ihre Amazon-El astic-Block-Store (Amazon-EBS)-Volumes, um eventuell vorhandene sensible Daten sowie Daten im Ruhezustand zu schützen.

Kontroll-ID	AWS Config	Empfehlungen
Art. 21.1	opensearch-encrypted-at-rest	Da sensible Daten vorhanden sein können und um Daten im Ruhezustand zu schützen, sollten Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon OpenSearch Service-Domains aktiviert ist.
Art. 21.1	opensearch-node-to-node-Verschlüsselungsprüfung	Stellen Sie sicher, dass die node-to-node Verschlüsselung für Amazon OpenSearch Service aktiviert ist. Node-to-nodeVerschlüsselung ermöglicht die TLS 1.2-Verschlüsselung für die gesamte Kommunikation innerhalb der Amazon Virtual Private Cloud (Amazon VPC). Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	AWS Config	Empfehlungen
Art. 21.1	rds-multi-az-support	Die Multi-AZ-Unterstützung in Amazon Relational Database Service (Amazon RDS) bietet eine verbesserte Verfügbar keit und Beständigkeit von Datenbank-Instances. Wenn Sie eine Multi-AZ-Datenbank-Instance bereitstellen, erstellt Amazon RDS automatisch eine primäre Datenbank-Instance und repliziert die Daten synchron auf eine Standby-Instance in einer anderen Availability Zone. Jede Availability Zone läuft auf einer eigenen, physisch getrennten, unabhängigen Infrastruktur und ist auf eine hohe Verfügbarkeit ausgelegt . Im Falle eines Infrastru kturausfalls führt Amazon RDS einen automatischen Failover zum Standby-Modus durch, sodass Sie den Datenbank betrieb wieder aufnehmen können, sobald der Failover abgeschlossen ist.

Kontroll-ID	AWS Config	Empfehlungen
Art. 21.1	rds-cluster-multi-az-aktiviert	Die Multi-AZ-Unterstützung in Amazon Relational Database Service (Amazon RDS) bietet eine verbesserte Verfügbar keit und Beständigkeit von Datenbank-Instances. Wenn Sie eine Multi-AZ-Datenbank-Instance bereitstellen, erstellt Amazon RDS automatisch eine primäre Datenbank-Instance und repliziert die Daten synchron auf eine Standby-Instance in einer anderen Availability Zone. Jede Availability Zone läuft auf einer eigenen, physisch getrennten, unabhängigen Infrastruktur und ist auf eine hohe Verfügbarkeit ausgelegt . Im Falle eines Infrastru kturausfalls führt Amazon RDS einen automatischen Failover zum Standby-Modus durch, sodass Sie den Datenbank betrieb wieder aufnehmen können, sobald der Failover abgeschlossen ist.

Kontroll-ID	AWS Config	Empfehlungen
Art. 21.1	rds-storage-encrypted	Zum Schutz von Daten im Ruhezustand müssen Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon Relational Database Service (Amazon RDS)-Instances aktiviert ist. Um eventuell vorhandene sensible Daten im Ruhezustand in Amazon-RDS-Instanc es zu schützen, muss die Verschlüsselung von Daten im Ruhezustand aktiviert sein.

Kontroll-ID	AWS Config	Empfehlungen
Art. 21.1	redshift-cluster-configuration-check	Um Daten im Ruhezustand zu schützen, muss die Verschlüsselung für Ihre Amazon-Redshift-Cluster aktiviert sein. Sie müssen auch sicherstellen, dass die erforderlichen Konfigurationen auf Amazon-Redshift-Clustern bereitgestellt werden. Die Prüfungsprotokollierung muss aktiviert sein, um Informationen zu Verbindungen und Benutzeraktivitäten in der Datenbank bereitzustellen. Diese Regel erfordert, dass ein Wert für clusterDbEncrypted (Config Default: TRUE) und LoggingEnabled (Config Default: TRUE) gesetzt ist. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	AWS Config	Empfehlungen
Art. 21.1	redshift-cluster-kms-enabled	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass die Verschlüsselung mit AWS Key Management Service (AWS KMS) für Ihren Amazon Redshift Redshift-Cluster aktiviert ist. Um eventuell vorhandene sensible Daten im Ruhezustand in Redshift-Clustern zu schützen, muss die Verschlüsselung von Daten im Ruhezustand aktiviert sein.
Art. 21.1	redshift-require-tls-ssl	Stellen Sie sicher, dass Ihre Amazon-Redshift-Cluster eine TLS/SSL-Verschlüsselung erfordern, um eine Verbindun g zu SQL-Clients herzustel len. Um eventuell vorhanden e sensible Daten zu schützen, sollten Sie die Verschlüs selung bei der Übertragung aktivieren.

Kontroll-ID	AWS Config	Empfehlungen
Art. 21.1	s3- aktiviert bucket-server-side-encryption	Zum Schutz von Daten im Ruhezustand müssen Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon Simple Storage Service (Amazon S3)-Buckets aktiviert ist. Um eventuell vorhandene sensible Daten im Ruhezustand in Amazon-S3-Buckets zu schützen, muss die Verschlüsselung aktiviert sein.
Art. 21.1	s-3 bucket-ssl-requests-only	Um Daten während der Übertragung zu schützen, stellen Sie sicher, dass Ihre Amazon Simple Storage Service (Amazon S3)-Buckets Anfragen zur Verwendung von Secure Socket Layer (SSL)-Buckets erfordern. Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	AWS Config	Empfehlungen
Art. 21.1	sagemaker-endpoint-configuration-kms-key-konfiguriert	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass die Verschlüsselung mit dem AWS Key Management Service (AWS KMS) für Ihren Endpunkt aktiviert ist. SageMaker Da sensible Daten auf dem SageMaker Endgerät gespeichert werden können, sollten Sie die Verschlüsselung im Ruhezustand aktivieren, um diese Daten zu schützen.
Art. 21.1	secretsmanager-using-cmk	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass die Verschlüsselung mit dem AWS Key Management Service (AWS KMS) für AWS Secrets Manager aktiviert ist. Aktivieren Sie die Verschlüsselung von Daten im Ruhezustand, um eventuell vorhandene sensible Daten im Ruhezustand im Secrets Manager zu schützen.

Kontroll-ID	AWS Config	Empfehlungen
Art. 21.1	vpc-vpn-2-tunnels-up	Redundante Site-to-Site VPN-Tunnel können implement iert werden, um die Anforderu ngen an die Ausfallsicherheit zu erfüllen. Es verwendet zwei Tunnel, um die Konnektiv ität sicherzustellen, falls eine der Site-to-Site VPN-Verbi ndungen nicht verfügbar ist. Um sich vor einem Verbindun gsverlust zu schützen, können Sie für den Fall, dass Ihr Kunden-Gateway nicht verfügbar ist, eine zweite Site-to-Site VPN-Verbindung zu Ihrer Amazon Virtual Private Cloud (Amazon VPC) und Ihrem Virtual Private Gateway einrichten, indem Sie ein zweites Kunden-Gateway verwenden.
Art. 22	autoscaling-launch-config-p ublic-ip-deaktiviert	Wenn Sie Ihre Netzwerks chnittstellen mit einer öffentlic hen IP-Adresse konfigurieren, sind die diesen Netzwerks chnittstellen zugehörigen Ressourcen über das Internet erreichbar. EC2 Ressource n sollten nicht öffentlich zugänglich sein, da dies einen unbeabsichtigten Zugriff auf Ihre Anwendungen oder Server ermöglichen kann.

Kontroll-ID	AWS Config	Empfehlungen
Art. 22	ssm-document-not-public	Stellen Sie sicher, dass AWS Systems Manager (SSM) - Dokumente nicht öffentlich sind, da dies einen unbeabsichtigten Zugriff auf Ihre SSM-Dokumente ermöglichen kann. Ein öffentliches SSM-Dokument kann Informationen über Ihr Konto, Ihre Ressourcen und internen Prozesse preisgeben.
Art. 22	dms-replication-not-public	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass auf DMS-Replikationsinstanzen nicht öffentlich zugegriffen werden kann. DMS-Replikations-Instances können vertrauliche Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.
Art. 22	ebs-snapshot-public-restorable-überprüfen	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass EBS-Snapshots nicht öffentlich wiederherstellbar sind. EBS-Volume-Snapshots können vertrauliche Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	AWS Config	Empfehlungen
Art. 22	ec-2 instance-no-public-ip	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon Elastic Compute Cloud (Amazon EC2) -Instances nicht öffentlich zugänglich sind. EC2 Amazon-Instances können vertrauliche Informati onen enthalten, und für solche Konten ist eine Zugriffsk ontrolle erforderlich.
Art. 22	elasticsearch-in-vpc-only	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass sich Amazon OpenSearch OpenSearch Service (Service) -Domains innerhalb einer Amazon Virtual Private Cloud (Amazon VPC) befinden. Eine OpenSearch Service-D omain innerhalb einer Amazon VPC ermöglicht die sichere Kommunikation zwischen OpenSearch Service und anderen Services innerhalb der Amazon VPC, ohne dass ein Internet-Gateway, ein NAT-Gerät oder eine VPN-Verbindung erforderlich ist.

Kontroll-ID	AWS Config	Empfehlungen
Art. 22	emr-master-no-public-ip	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon EMR-Cluster-Masterknoten nicht öffentlich zugänglich sind. Amazon-EMR-Cluster-Hauptknoten können vertrauliche Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.
Art. 22	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) Security Groups können bei der Verwaltung des Netzwerkzugriffs helfen, indem sie eine statusbehaftete Filterung von eingehendem und ausgehendem Netzwerkverkehr zu Ressourcen bereitstellen. AWS Wenn Sie eingehenden (oder entfernten) Datenverkehr von 0.0.0.0/0 bis Port 22 auf Ihren Ressourcen nicht zulassen, können Sie den Remote-Zugriff einschränken.

Kontroll-ID	AWS Config	Empfehlungen
Art. 22	internet-gateway-authorized-vpc-nur	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Internet-Gateways nur mit autorisierter Amazon Virtual Private Cloud (Amazon VPC) verbunden sind. Internet-Gateways ermöglichen den bidirekti onalen Internetzugang zur und von der Amazon VPC, was möglicherweise zu einem unbefugten Zugriff auf Amazon-VPC-Ressourcen führen kann.
Art. 22	lambda-function-public-acce ss-verboten	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherste llen, dass AWS Lambda-Funktionen nicht öffentlich zugänglich sind. Der öffentlic he Zugriff kann möglicher weise die Verfügbarkeit von Ressourcen beeinträchtigen.

Kontroll-ID	AWS Config	Empfehlungen
Art. 22	lambda-inside-vpc	Stellen Sie AWS Lambda-Funktionen in einer Amazon Virtual Private Cloud (Amazon VPC) bereit, um eine sichere Kommunikation zwischen einer Funktion und anderen Diensten innerhalb der Amazon VPC zu gewährleisten. Bei dieser Konfiguration sind kein Internet-Gateway, kein NAT-Gerät und keine VPN-Verbindung erforderlich. Der gesamte Datenverkehr bleibt sicher in der Cloud. AWS Domains, die sich innerhalb einer VPC befinden, verfügen aufgrund ihrer logischen Isolierung im Vergleich zu Domains mit öffentlichen Endpunkten über eine zusätzliche Sicherheitsebene. Um den Zugriff ordnungsgemäß zu verwalten, sollten AWS Lambda-Funktionen einer VPC zugewiesen werden.

Kontroll-ID	AWS Config	Empfehlungen
Art. 22	opensearch-in-vpc-only	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass sich Amazon OpenSearch Service-Domains innerhalb einer Amazon Virtual Private Cloud (Amazon VPC) befinden. Eine Amazon OpenSearch Service-Domain innerhalb einer Amazon VPC ermöglich t die sichere Kommunika tion zwischen Amazon OpenSearch Service und anderen Services innerhalb der Amazon VPC, ohne dass ein Internet-Gateway, ein NAT-Gerät oder eine VPN-Verbindung erforderlich ist.
Art. 22	rds-instance-public-access-überprüfen	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherste llen, dass Amazon Relationa l Database Service (Amazon RDS) -Instances nicht öffentlic h sind. Amazon-RDS-Datenba nk-Instances können vertrauli che Informationen enthalten und für solche Konten sind Prinzipien und Zugriffsk ontrollen erforderlich.

Kontroll-ID	AWS Config	Empfehlungen
Art. 22	rds-snapshots-public-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Relational Database Service (Amazon RDS) -Instances nicht öffentlich sind. Amazon-RDS-Datenbank-Instances können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.
Art. 22	redshift-cluster-public-access-überprüfen	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Redshift Redshift-Cluster nicht öffentlich sind. Amazon-Redshift-Cluster können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	AWS Config	Empfehlungen
Art. 22	restricted-common-ports	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass gemeinsame Ports für Amazon Elastic Compute Cloud (Amazon EC2) - Sicherheitsgruppen eingeschränkt sind. Wenn der Zugriff auf Ports nicht auf vertrauenswürdige Quellen beschränkt wird, kann dies zu Angriffen auf die Verfügbarkeit, Integrität und Vertraulichkeit von Systemen führen. Mit dieser Regel können Sie optional die Parameter blockedPort1–blockedPort5 festlegen (Standardkonfigurationen: 20, 21, 3389, 3306, 4333). Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	AWS Config	Empfehlungen
Art. 22	s3- account-level-public-access -Block-periodisch	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Simple Storage Service (Amazon S3) -Buckets nicht öffentlich zugänglich sind. Diese Regel trägt dazu bei, sensible Daten vor unbefugten Remote-Benutzern zu schützen, indem sie den öffentlichen Zugriff verhindert. Mit dieser Regel können Sie optional die Parameter ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) und restrictPublicBuckets Parameter (Config Default: True) festlegen. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	AWS Config	Empfehlungen
Art. 22	s3 bucket-level-public-access -verboten	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Simple Storage Service (Amazon S3) -Buckets nicht öffentlich zugänglich sind. Diese Regel trägt dazu bei, sensible Daten vor unbefugten Remote-Benutzern zu schützen, indem sie den öffentlichen Zugriff auf Bucket-Ebene verhindert.
Art. 22	s-3 bucket-public-read-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie nur autorisierten Benutzern, Prozessen und Geräten Zugriff auf Amazon Simple Storage Service (Amazon S3) -Buckets gewähren. Die Verwaltung des Zugriffs sollte mit der Klassifizierung der Daten übereinstimmen.

Kontroll-ID	AWS Config	Empfehlungen
Art. 22	s3- bucket-public-write-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie nur autorisierten Benutzern, Prozessen und Geräten Zugriff auf Amazon Simple Storage Service (Amazon S3) -Buckets gewähren. Die Verwaltung des Zugriffs sollte mit der Klassifizierung der Daten übereinstimmen.
Art. 22	sagemaker-notebook-no-direct-Internetzugang	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass SageMaker Amazon-Notebooks keinen direkten Internetzugang zulassen. Indem Sie direkten Internetzugang blockieren, vermeiden Sie, dass unbefugte Benutzer auf sensible Daten zugreifen.

Kontroll-ID	AWS Config	Empfehlungen
Art. 22	subnet-auto-assign-public-ip-deaktiviert	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon Virtual Private Cloud (VPC) -Subnetzen nicht automatis ch eine öffentliche IP-Adress e zugewiesen wird. Amazon Elastic Compute Cloud (EC2) -Instances, die in Subnetzen gestartet werden, in denen dieses Attribut aktiviert ist, haben ihrer primären Netzwerkschnittste lle eine öffentliche IP-Adresse zugewiesen.
Art. 22	vpc-default-security-group-geschlossen	Sicherheitsgruppen von Amazon Elastic Compute Cloud (Amazon EC2) können bei der Verwaltung des Netzwerkzugriffs helfen, indem sie eine statusbeh aftete Filterung des ein- und ausgehenden Netzwerkv erkehrs zu Ressourcen bereitstellen. AWS Die Beschränkung des gesamten Datenverkehrs auf die Standardsicherheitsgruppe hilft dabei, den Fernzugriff auf Ihre Ressourcen einzuschr änken. AWS

Kontroll-ID	AWS Config	Empfehlungen
Art. 22	vpc-sg-open-only-to-authorized-ports	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass gemeinsame Ports für Amazon Elastic Compute Cloud (Amazon EC2) - Sicherheitsgruppen eingeschränkt sind. Wenn der Zugriff auf Ports nicht auf vertrauenswürdige Quellen beschränkt wird, kann dies zu Angriffen auf die Verfügbarkeit, Integrität und Vertraulichkeit von Systemen führen. Durch die Beschränkung des Zugriffs auf Ressourcen innerhalb einer Sicherheitsgruppe aus dem Internet (0.0.0.0/0) kann der Remote-Zugriff auf interne Systeme gesteuert werden.
Art. 23	elasticsearch-logs-to-cloudwatch	Stellen Sie sicher, dass für Amazon OpenSearch Service-Domains Fehlerprotokolle aktiviert und zur Aufbewahrung und Beantwortung an Amazon CloudWatch Logs gestreamt werden. Domain-Fehlerprotokolle sind bei Sicherheits- und Zugriffsprüfungen sowie bei der Diagnose von Verfügbarkeitsproblemen nützlich.

Kontroll-ID	AWS Config	Empfehlungen
Art. 23	multi-region-cloudtrail-enabled	AWS CloudTrail zeichnet Aktionen und API-Aufrufe der AWS Management Console auf. Sie können feststellen, welche Benutzer und Konten angerufen wurden AWS, von welcher Quell-IP-Adresse aus die Anrufe getätigt wurden und wann die Anrufe erfolgten . CloudTrail übermittelt Protokolldateien aus allen AWS Regionen an Ihren S3-Bucket, wenn MULTI_REGION_CLOUD_TRAIL_ENABLED aktiviert ist. Außerdem wird beim AWS Start einer neuen Region derselbe Trail in der neuen Region erstellt. CloudTrail Dadurch erhalten Sie automatisch Protokoll dateien mit API-Aktivitäten für die neue Region.

Kontroll-ID	AWS Config	Empfehlungen
Art. 23	rds-logging-enabled	Um die Protokollierung und Überwachung in Ihrer Umgebung zu erleichtern, stellen Sie sicher, dass die Amazon Relational Database Service (Amazon RDS)-Protokollierung aktiviert ist. Mit der Amazon-RDS-Protokollierung können Sie Ereignisse wie Verbindungen, Verbindungsabbrüche, Abfragen oder abgefragte Tabellen erfassen.
Art. 23	wafv2-logging-enabled	Um die Protokollierung und Überwachung in Ihrer Umgebung zu erleichtern, aktivieren Sie die AWS WAF (V2) -Protokollierung im regionalen und globalen Web ACLs. AWS Die WAF-Protokollierung bietet detaillierte Informationen über den Datenverkehr, der von Ihrer Web-ACL analysiert wird. In den Protokollen werden die Uhrzeit aufgezeichnet, zu der die AWS WAF die Anfrage von Ihrer AWS Ressource erhalten hat, Informationen über die Anfrage und eine Aktion für die Regel, der jede Anfrage entsprach.

Kontroll-ID	AWS Config	Empfehlungen
Art. 23	api-gw-execution-logging-aktiviert	Die API-Gateway-Protokollierung zeigt detaillierte Ansichten der Benutzer, die auf die API zugegriffen haben, und wie diese Benutzer auf die API zugegriffen haben. Diese Einblicke ermöglichen die Transparenz von Benutzeraktivitäten.
Art. 23	cloud-trail-cloud-watch-logs-aktiviert	Verwenden Sie Amazon CloudWatch , um Protokollereignisaktivitäten zentral zu sammeln und zu verwalten . Die Aufnahme von AWS CloudTrail Daten liefert Einzelheiten zu den API-Aufrufaktivitäten in Ihrem AWS-Konto.

Kontroll-ID	AWS Config	Empfehlungen
Art. 23	cloudtrail-enabled	AWS CloudTrail kann bei der Nichtabstreitbarkeit helfen, indem Aktionen und API-Aufrufe der AWS Managemen t Console aufgezeichnet werden. Sie können die Benutzer und die Benutzer AWS-Konten , die einen AWS Dienst aufgerufen haben, die Quell-IP-Adresse, über die die Aufrufe generiert wurden, und den Zeitpunkt der Anrufe identifizieren. Einzelheiten zu den erfassten Daten finden Sie in den AWS CloudTrail Datensatzinhalten.
Art. 23	cloudtrail-s3-dataevents-en abled	Die Erfassung von Simple Storage Service (Amazon S3)-Datenereignissen unterstützt die Erkennung von ungewöhnl ichen Aktivitäten. Zu den Details gehören AWS-Konto Informationen über den Zugriff auf einen Amazon S3 S3-Bucket, die IP-Adresse und die Uhrzeit des Ereignisses.

Kontroll-ID	AWS Config	Empfehlungen
Art. 23	elb-logging-enabled	Die Elastic-Load-Balancing-Aktivität ist ein zentraler Kommunikationspunkt innerhalb einer Umgebung. Stellen Sie sicher, dass die ELB-Protokollierung aktiviert ist. Die gesammelten Daten enthalten detaillierte Informati onen zu Anfragen, die an den ELB gesendet wurden. Jedes Protokoll enthält Informati onen wie die Zeit, zu der die Anforderung einging, die Client-IP-Adresse, Latenzen, Anforderungspfade und Serverantworten.
Art. 23	opensearch-logs-to-cloudwat ch	Stellen Sie sicher, dass für Amazon OpenSearch Service-Domains Fehlerprotokolle aktiviert und zur Aufbewahr ung und Beantwortung an Amazon CloudWatch Logs gestreamt werden. OpenSearc h Service-Fehlerprotokolle können bei Sicherheits- und Zugriffsprüfungen helfen und bei der Diagnose von Verfügbarkeitsproblemen helfen.

Kontroll-ID	AWS Config	Empfehlungen
Art. 23	s-3 bucket-logging-enabled	Die Amazon Simple Storage Service (Amazon S3)-Serverzugriffsprotokollierung bietet eine Methode zur Überwachung des Netzwerks im Hinblick auf potenzielle Cybersicherheitsereignisse. Die Ereignisse werden überwacht, indem detaillierte Aufzeichnungen über die Anfragen erfasst werden, die an einen Amazon-S3-Bucket gestellt wurden. Jeder Zugriffsprotokolleintrag enthält Details zu einer einzelnen Zugriffsanfrage. Zu den Details gehören Anforderer, Bucket-Name, Anforderungszeit, Anforderungsaktion, Antwortstatus und Fehlercode, falls relevant.

Kontroll-ID	AWS Config	Empfehlungen
Art. 23	vpc-flow-logs-enabled	VPC-Flow-Protokolle erfassen detaillierte Informationsdatensätze über den IP-Datenverkehr, der zu und von Netzwerkschnittstellen in Ihrer Amazon Virtual Private Cloud (Amazon VPC) fließt. Standardmäßig enthalten Flow-Protokolldatensätze Werte für die verschiedenen Komponenten des IP-Flows, einschließlich Quelle, Ziel und Protokoll.
Artikel 24.1	guardduty-enabled-centralized	Amazon GuardDuty kann mithilfe von Threat Intelligence Feeds helfen, potenzielle Cybersicherheitsereignisse zu überwachen und zu erkennen. Dazu gehören Listen mit bösartigen IPs und maschinellen Lernmethoden zur Identifizierung unerwarteter, nicht autorisierter und bösartiger Aktivitäten in Ihrer AWS Cloud-Umgebung.

Kontroll-ID	AWS Config	Empfehlungen
Artikel 24.2	response-plan-exists-maintained (Prozessüberprüfung)	Stellen Sie sicher, dass Vorfallreaktionspläne erstellt, verwaltet und an das verantwortliche Personal verteilt werden. Aktualisierte und formal dokumentierte Reaktionspläne können dazu beitragen, dass das zuständige Personal die Rollen, Verantwortlichkeiten und Prozesse versteht, die bei einem Vorfall einzuhalten sind.
Art. 25	dynamodb-in-backup-plan	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon DynamoDB-Tabellen Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	AWS Config	Empfehlungen
Art. 25	ebs-in-backup-plan	Stellen Sie zur Unterstützung der Datensicherungsprozesse sicher, dass Ihre Amazon Elastic Block Store (Amazon EBS) -Volumes Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherung smanagement und erleichte rt Ihnen die Erfüllung von geschäftlichen und behördlic hen Compliance-Anforde rungen hinsichtlich Datensich erungen.

Kontroll-ID	AWS Config	Empfehlungen
Art. 25	efs-in-backup-plan	Um Sie bei Datensich erungsprozessen zu unterstüt zen, stellen Sie sicher, dass Ihre Amazon Elastic File System (Amazon EFS) - Dateisysteme Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherung smanagement und erleichte rt Ihnen die Erfüllung von geschäftlichen und behördlic hen Compliance-Anforde rungen hinsichtlich Datensich erungen.

Kontroll-ID	AWS Config	Empfehlungen
Art. 25	rds-in-backup-plan	Um Sie bei Datensich erungsprozessen zu unterstüt zen, stellen Sie sicher, dass Ihre Amazon Relational Database Service (Amazon RDS) -Instances Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherung smanagement und erleichte rt Ihnen die Erfüllung von geschäftlichen und behördlic hen Compliance-Anforde rungen hinsichtlich Datensich erungen.

Kontroll-ID	AWS Config	Empfehlungen
Art. 25	redshift-backup-enabled	Stellen Sie zur Unterstützung der Datensicherungsprozesse sicher, dass Ihre Amazon-Redshift-Cluster über automatisierte Snapshots verfügen. Wenn automatisierte Snapshots für einen Cluster aktiviert sind, erstellt Redshift in regelmäßigen Abständen Snapshots dieses Clusters. Standardmäßig erstellt Redshift alle acht Stunden oder alle 5 GB einen Snapshot für jeden Knoten mit Datenänderungen oder je nachdem, was zuerst eintritt.
Art. 25	db-instance-backup-enabled	Die Sicherungsfunktion von Amazon RDS erstellt Sicherungen Ihrer Datenbanken und Transaktionsprotokolle. Amazon RDS erstellt einen Snapshot für das Speichervolume Ihrer DB-Instance, sodass die gesamte DB-Instance gesichert wird. Sie können im System spezifische Aufbewahrungsfristen festlegen, um Ihre Ausfallsicherheitsanforderungen zu erfüllen.

Kontroll-ID	AWS Config	Empfehlungen
Art. 25	dynamodb-pitr-enabled	Aktivieren Sie diese Regel, um zu überprüfen, ob die Informationen gesichert wurden. Es verwaltet auch die Backups, indem es sicherstellt, dass die point-in-time Wiederherstellung in Amazon DynamoDB aktiviert ist. Bei der Wiederherstellung werden fortlaufende Backups Ihrer Tabelle für die letzten 35 Tage gespeichert.
Art. 25	ebs-optimized-instance	Eine optimierte Instance im Amazon Elastic Block Store (Amazon EBS) bietet zusätzliche, dedizierte Kapazität für Amazon-EBS-I/O-Vorgänge. Diese Optimierung bietet die beste Leistung für Ihr EBS-Volume, indem Konflikte zwischen Amazon-EBS-I/O und anderem Datenverkehr von Ihrer Instance minimiert werden.

Kontroll-ID	AWS Config	Empfehlungen
Art. 25	elasticache-redis-cluster-automatic-Backup-Prüfung	Wenn automatische Backups aktiviert sind, ElastiCache erstellt Amazon täglich ein Backup des Clusters. Die Sicherung kann für eine von Ihrer Organisation festgelegte Anzahl von Tagen aufbewahrt werden. Automatische Backups schützen vor Datenverlust. Bei einem Ausfall können Sie einen neuen Cluster erstellen, der Ihre Daten aus dem aktuellen Backup wiederherstellt.
Art. 25	s-3 bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) unterstützt die Aufrechterhaltung einer angemessenen Kapazität und Verfügbarkeit. CRR ermöglicht das automatische, asynchrone Kopieren von Objekten in Amazon-S3-Buckets, um die Datenverfügbarkeit sicherzustellen.

Kontroll-ID	AWS Config	Empfehlungen
Art. 25	s-3 bucket-versioning-enabled	Die Versionsverwaltung von Amazon Simple Storage Service (Amazon S3)-Buckets hilft dabei, mehrere Varianten eines Objekts im selben Amazon-S3-Bucket zu speichern. Verwenden Sie die Versionsverwaltung, um sämtliche Versionen aller Objekte in Ihrem Amazon-S3-Bucket zu speichern, abzurufen oder wiederher zustellen. Mit der Versionsv erwaltung können Sie Versionen sowohl nach unbeabsichtigten Benutzera ktionen als auch nach Anwendungsfehlern problemlo s wiederherstellen.

Vorlage

Die Vorlage ist verfügbar auf GitHub: Operational Best Practices for Esquema Nacional de Seguridad (ENS) Medium.

Bewährte Methoden für die Implementierung des Esquema Nacional de Seguridad (ENS) High

Konformitätspakete bieten ein allgemeines Compliance-Framework, das es Ihnen ermöglicht, mithilfe verwalteter oder benutzerdefinierter Regeln und Abhilfemaßnahmen Governance-Prüfungen zur Sicherheit, zum Betrieb oder zur Kostenoptimierung durchzuführen. AWS Config AWS Config Conformance Packs dienen als Beispielvorlagen nicht dazu, die vollständige Einhaltung eines bestimmten Governance- oder Compliance-Standards sicherzustellen. Sie sind dafür verantwortlich,

selbst zu beurteilen, ob Ihre Nutzung der Services den geltenden gesetzlichen und behördlichen Anforderungen entspricht.

Im Folgenden finden Sie ein Beispiel für eine Zuordnung zwischen Esquema Nacional de Seguridad (ENS) High Framework-Steuerelementen in Spanien und verwalteten Konfigurationsregeln. AWS Jede Config-Regel gilt für eine bestimmte AWS Ressource und bezieht sich auf eine oder mehrere Spanien ENS High-Kontrollen. Eine Kontrolle des spanischen ENS kann mehreren Config-Regeln zugeordnet werden. In der folgenden Tabelle finden Sie weitere Informationen und Anleitungen zu diesen Zuordnungen.

Diese beispielhafte Conformance-Pack-Vorlage enthält Zuordnungen zu Kontrollen nach den Richtlinien des spanischen ENS High, das zuletzt am 09.07.2021 aktualisiert wurde.

Kontroll-ID	AWS Config	Empfehlungen
Anexo II 4.1.1.ALTO	annual-risk-assessment-performed (Prozessprüfung)	Führen Sie eine jährliche Risikobewertung für Ihre Organisation durch. Risikowertungen können dabei helfen, die Wahrscheinlichkeit und Auswirkungen identifizierter Risiken und/oder Schwachstellen für eine Organisation zu ermitteln.
4.2.1.b)	iam-root-access-key-prüfen	Der Zugriff auf Systeme und Ressourcen kann gesteuert werden, indem überprüft wird, ob der Root-Benutzer keine Zugriffsschlüssel mit seiner AWS Identity and Access Management (IAM) -Rolle verknüpft hat. Stellen Sie sicher, dass die Root-Zugriffsschlüssel gelöscht werden. Erstellen und verwenden Sie stattdessen rollenbasierte Funktionen, AWS-Konten um

Kontroll-ID	AWS Config	Empfehlungen
		das Prinzip der geringsten Funktionalität zu berücksic htigen.
4.2.5.ALTO.a)	iam-root-access-key-überprü fen	Der Zugriff auf Systeme und Ressourcen kann gesteuert werden, indem überprüft wird, ob der Root-Benutzer keine Zugriffsschlüssel mit seiner AWS Identity and Access Management (IAM) -Rolle verknüpft hat. Stellen Sie sicher, dass die Root-Zugr iffsschlüssel gelöscht werden. Erstellen und verwenden Sie stattdessen rollenbasierte Funktionen, AWS-Konten um das Prinzip der geringsten Funktionalität zu berücksic htigen.
Anexo II 4.1.2.a); b); c)	dynamodb-table-encrypted-km s	Stellen Sie sicher, dass die Verschlüsselung für Ihre Amazon-DynamoDB-Tabellen aktiviert ist. Um eventuell vorhandene sensible Daten im Ruhezustand in diesen Tabellen zu schützen, müssen Sie die Verschlüsselung von Daten im Ruhezustand aktivieren. Standardmäßig werden DynamoDB-Tabellen mit einem AWS eigenen Kundenhauptschlüssel (CMK) verschlüsselt.

Kontroll-ID	AWS Config	Empfehlungen
Anexo II 4.1.2.a); b); c)	ec2- ebs-encryption-by-default	Zum Schutz von Daten im Ruhezustand müssen Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon Elastic Block Store (Amazon EBS)-Volumes aktiviert ist. Da sensible Daten auch im Ruhezusta nd vorhanden sein können, sollten Sie die Verschlüs selung im Ruhezustand aktivieren, um diese Daten zu schützen.
Anexo II 4.1.2.a); b); c)	elasticsearch-node-to-node-Verschlüsselungsprüfung	Stellen Sie sicher, dass die node-to-node Verschlüsselung für Amazon OpenSearch Service aktiviert ist. Node-to-nodeVerschlüsselung ermöglicht die TLS 1.2-Versc hlüsselung für die gesamte Kommunikation innerhalb der Amazon Virtual Private Cloud (Amazon VPC). Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	AWS Config	Empfehlungen
Anexo II 4.1.2.a); b); c)	elb-cross-zone-load-Balancing aktiviert	Aktivieren Sie zonenüber greifendes Load Balancing für Ihre Elastic Load Balancer (ELBs), um eine angemesse ne Kapazität und Verfügbar keit aufrechtzuerhalten. Zonenübergreifendes Load Balancing reduziert die Notwendigkeit, die gleiche Anzahl von Instances in jeder aktivierten Availability Zone aufrechtzuerhalten. Es verbessert auch die Fähigkeit Ihrer Anwendung, den Verlust einer oder mehrerer Instances zu bewältigen.
Anexo II 4.1.2.a); b); c)	elb-tls-https-listeners-nur	Stellen Sie sicher, dass Ihre Elastic Load Balancer (ELBs) mit SSL- oder HTTPS-Lis tenern konfiguriert sind. Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	AWS Config	Empfehlungen
Anexo II 4.1.2.a); b); c)	rds-instance-deletion-protection-aktiviert	Stellen Sie sicher, dass Amazon Relational Database Service (Amazon RDS)-Instances den Löschschutz aktiviert haben. Verwenden Sie den Löschschutz, um zu verhindern, dass Ihre Amazon-RDS-Instances versehentlich oder böswillig gelöscht werden, was zum Verlust der Verfügbarkeit Ihrer Anwendungen führen kann.
Anexo II 4.1.2.a); b); c)	rds-snapshot-encrypted	Stellen Sie sicher, dass die Verschlüsselung für Ihre Amazon Relational Database Service (Amazon RDS)-Snapshots aktiviert ist. Da sensible Daten auch im Ruhezustand vorhanden sein können, sollten Sie die Verschlüsselung im Ruhezustand aktivieren, um diese Daten zu schützen.
Anexo II 4.1.2.a); b); c)	s3- bucket-default-lock-enabled	Stellen Sie sicher, dass für Ihren Amazon Simple Storage Service (Amazon S3)-Bucket standardmäßig eine Sperre aktiviert ist. Zum Schutz eventuell vorhandener sensibler Daten in S3-Buckets müssen Sie Objektsperren für Daten im Ruhezustand erzwingen.

Kontroll-ID	AWS Config	Empfehlungen
Anexo II 4.1.2.a); b); c)	s-3 default-encryption-kms	Stellen Sie sicher, dass die Verschlüsselung für Ihre Amazon Simple Storage Service (Amazon S3)-Buckets aktiviert ist. Um eventuell vorhandene sensible Daten im Ruhezustand in einem Amazon-S3-Bucket zu schützen, muss die Verschlüsselung aktiviert sein.
Anexo II 4.1.2.a); b); c)	sagemaker-notebook-instance-kms-key-konfiguriert	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass die Verschlüsselung mit dem AWS Key Management Service (AWS KMS) für Ihr Notebook aktiviert ist. SageMaker Da vertrauliche Daten im SageMaker Notebook gespeichert werden können, sollten Sie die Verschlüsselung im Ruhezustand aktivieren, um diese Daten zu schützen.

Kontroll-ID	AWS Config	Empfehlungen
Anexo II 4.1.2.a); b); c)	sns-encrypted-kms	Um Daten im Ruhezusta nd zu schützen, stellen Sie sicher, dass Ihre Amazon Simple Notification Service (Amazon SNS) -Themen mit dem AWS Key Management Service (AWS KMS) verschlüs selt werden müssen. Um eventuell vorhandene sensible Daten im Ruhezustand in veröffentlichten Nachricht en zu schützen, muss die Verschlüsselung von Daten im Ruhezustand aktiviert sein.
Anexo II 4.1.2.a); b); c)	alb-http-to-https-Umleitung sprüfung	Um Daten während der Übertragung zu schützen, stellen Sie sicher, dass Ihr Application Load Balancer unverschlüsselte HTTP-Anfragen automatisch an HTTPS umleitet. Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	AWS Config	Empfehlungen
Anexo II 4.1.2.a); b); c)	api-gw-cache-enabled-und-verschlüsselt	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass die Verschlüsselung für den Cache Ihrer API-Gateway-Stufe aktiviert ist. Da für die API-Methode sensible Daten erfasst werden können, sollten Sie die Verschlüsselung von Daten im Ruhezustand aktivieren, um diese Daten zu schützen.
Anexo II 4.1.2.a); b); c)	api-gw-ssl-enabled	Stellen Sie sicher, dass die REST-API-Stufen von Amazon API Gateway mit SSL-Zertifikaten konfiguriert sind, damit Backend-Systeme überprüfen können, ob Anforderungen von API Gateway stammen.
Anexo II 4.1.2.a); b); c)	cloud-trail-encryption-enabled	Da sensible Daten vorhanden sein können und um Daten im Speicher zu schützen, sollten Sie sicherstellen, dass die Verschlüsselung für Ihre AWS CloudTrail Trails aktiviert ist.

Kontroll-ID	AWS Config	Empfehlungen
Anexo II 4.1.2.a); b); c)	cloud-trail-log-file-Validierung aktiviert	Verwenden Sie die AWS CloudTrail Protokolldateivalidierung, um die Integrität von Protokollen zu überprüfen. CloudTrail Mithilfe der Protokolldateivalidierung kann festgestellt werden, ob eine Protokolldatei geändert oder gelöscht wurde oder ob sie nach der Übermittlung CloudTrail unverändert geblieben ist. Dieses Feature wurde mit dem Branchenstandard entsprechenden Algorithmen entwickelt: SHA-256 für die Hashfunktion und SHA-256 mit RSA für digitale Signaturen. Aus diesem Grund ist es rechnerisch unmöglich, CloudTrail Protokolldateien unbemerkt zu ändern, zu löschen oder zu fälschen.
Anexo II 4.1.2.a); b); c)	cloudwatch-log-group-encrypted	Um sensible Daten im Speicher zu schützen, stellen Sie sicher, dass die Verschlüsselung für Ihre Amazon CloudWatch Log Groups aktiviert ist.

Kontroll-ID	AWS Config	Empfehlungen
Anexo II 4.1.2.a); b); c)	dynamodb-autoscaling-enabled	Amazon DynamoDB Auto Scaling verwendet den AWS Application Auto Scaling-Service, um die bereitgestellte Durchsatzkapazität so anzupassen, dass sie automatisch auf tatsächliche Verkehrsmuster reagiert. Auf diese Weise kann eine Tabelle oder ein globaler sekundärer Index die bereitgestellte Lese-/Schreibkapazität erhöhen, um plötzliche Erhöhungen des Datenverkehrs ohne Drosselung zu bewältigen.
Anexo II 4.1.2.a); b); c)	efs-encrypted-check	Aktivieren Sie die Verschlüsselung für Ihr Amazon Elastic File System (EFS), um eventuell vorhandene sensible Daten sowie Daten im Ruhezustand zu schützen.
Anexo II 4.1.2.a); b); c)	elasticsearch-encrypted-at-rest	Da sensible Daten vorhanden sein können und um Daten im Ruhezustand zu schützen, sollten Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon OpenSearch Service (OpenSearch Service) -Domains aktiviert ist.

Kontroll-ID	AWS Config	Empfehlungen
Anexo II 4.1.2.a); b); c)	elb-acm-certificate-required	Zum Schutz von eventuell vorhandenen sensiblen Daten sowie von Daten während der Übertragung muss die Verschlüsselung für Ihr Elastic Load Balancing aktiviert sein. Verwenden Sie AWS Certifica te Manager, um öffentlic he und private SSL/TLS-Z ertifikate mit AWS Diensten und internen Ressourcen zu verwalten, bereitzustellen und bereitzustellen.
Anexo II 4.1.2.a); b); c)	elb-deletion-protection-ena bled	Diese Regel sorgt dafür, dass der Löschschutz für Elastic Load Balancing aktiviert ist. Verwenden Sie diese Funktion, um zu verhinder n, dass Ihr Load Balancer versehentlich oder böswillig gelöscht wird, was zum Verlust der Verfügbarkeit Ihrer Anwendungen führen kann.
Anexo II 4.1.2.a); b); c)	encrypted-volumes	Aktivieren Sie die Verschlüs selung für Ihre Amazon-El astic-Block-Store (Amazon-EBS)-Volumes, um eventuell vorhandene sensible Daten sowie Daten im Ruhezustand zu schützen.

Kontroll-ID	AWS Config	Empfehlungen
Anexo II 4.1.2.a); b); c)	opensearch-encrypted-at-rest	Da sensible Daten vorhanden sein können und um Daten im Ruhezustand zu schützen, sollten Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon OpenSearch Service-Domains aktiviert ist.
Anexo II 4.1.2.a); b); c)	opensearch-node-to-node-Verschlüsselungsprüfung	Stellen Sie sicher, dass die node-to-node Verschlüsselung für Amazon OpenSearch Service aktiviert ist. Node-to-nodeVerschlüsselung ermöglicht die TLS 1.2-Verschlüsselung für die gesamte Kommunikation innerhalb der Amazon Virtual Private Cloud (Amazon VPC). Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	AWS Config	Empfehlungen
Anexo II 4.1.2.a); b); c)	rds-multi-az-support	Die Multi-AZ-Unterstützung in Amazon Relational Database Service (Amazon RDS) bietet eine verbesserte Verfügbar keit und Beständigkeit von Datenbank-Instances. Wenn Sie eine Multi-AZ-Datenbank-Instance bereitstellen, erstellt Amazon RDS automatisch eine primäre Datenbank-Instance und repliziert die Daten synchron auf eine Standby-Instance in einer anderen Availability Zone. Jede Availability Zone läuft auf einer eigenen, physisch getrennten, unabhängigen Infrastruktur und ist auf eine hohe Verfügbarkeit ausgelegt . Im Falle eines Infrastru kturausfalls führt Amazon RDS einen automatischen Failover zum Standby-Modus durch, sodass Sie den Datenbank betrieb wieder aufnehmen können, sobald der Failover abgeschlossen ist.

Kontroll-ID	AWS Config	Empfehlungen
Anexo II 4.1.2.a); b); c)	rds-cluster-multi-az-aktiviert	Die Multi-AZ-Unterstützung in Amazon Relational Database Service (Amazon RDS) bietet eine verbesserte Verfügbar keit und Beständigkeit von Datenbank-Instances. Wenn Sie eine Multi-AZ-Datenbank-Instance bereitstellen, erstellt Amazon RDS automatisch eine primäre Datenbank-Instance und repliziert die Daten synchron auf eine Standby-Instance in einer anderen Availability Zone. Jede Availability Zone läuft auf einer eigenen, physisch getrennten, unabhängigen Infrastruktur und ist auf eine hohe Verfügbarkeit ausgelegt . Im Falle eines Infrastru kturausfalls führt Amazon RDS einen automatischen Failover zum Standby-Modus durch, sodass Sie den Datenbank betrieb wieder aufnehmen können, sobald der Failover abgeschlossen ist.

Kontroll-ID	AWS Config	Empfehlungen
Anexo II 4.1.2.a); b); c)	rds-storage-encrypted	Zum Schutz von Daten im Ruhezustand müssen Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon Relational Database Service (Amazon RDS)-Instances aktiviert ist. Um eventuell vorhandene sensible Daten im Ruhezustand in Amazon-RDS-Instanc es zu schützen, muss die Verschlüsselung von Daten im Ruhezustand aktiviert sein.

Kontroll-ID	AWS Config	Empfehlungen
Anexo II 4.1.2.a); b); c)	redshift-cluster-configuration-check	Um Daten im Ruhezustand zu schützen, muss die Verschlüsselung für Ihre Amazon-Redshift-Cluster aktiviert sein. Sie müssen auch sicherstellen, dass die erforderlichen Konfigurationen auf Amazon-Redshift-Clustern bereitgestellt werden. Die Prüfungsprotokollierung muss aktiviert sein, um Informationen zu Verbindungen und Benutzeraktivitäten in der Datenbank bereitzustellen. Diese Regel erfordert, dass ein Wert für clusterDbEncrypted (Config Default: TRUE) und LoggingEnabled (Config Default: TRUE) gesetzt ist. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	AWS Config	Empfehlungen
Anexo II 4.1.2.a); b); c)	redshift-cluster-kms-enabled	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass die Verschlüsselung mit AWS Key Management Service (AWS KMS) für Ihren Amazon Redshift Redshift-Cluster aktiviert ist. Um eventuell vorhandene sensible Daten im Ruhezustand in Redshift-Clustern zu schützen, muss die Verschlüsselung von Daten im Ruhezustand aktiviert sein.
Anexo II 4.1.2.a); b); c)	redshift-require-tls-ssl	Stellen Sie sicher, dass Ihre Amazon-Redshift-Cluster eine TLS/SSL-Verschlüsselung erfordern, um eine Verbindun g zu SQL-Clients herzustel len. Um eventuell vorhanden e sensible Daten zu schützen, sollten Sie die Verschlüs selung bei der Übertragung aktivieren.

Kontroll-ID	AWS Config	Empfehlungen
Anexo II 4.1.2.a); b); c)	s3- aktiviert bucket-server-side -encryption	Zum Schutz von Daten im Ruhezustand müssen Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon Simple Storage Service (Amazon S3)-Bucke ts aktiviert ist. Um eventuell vorhandene sensible Daten im Ruhezustand in Amazon-S3 -Buckets zu schützen, muss die Verschlüsselung aktiviert sein.
Anexo II 4.1.2.a); b); c)	s-3 bucket-ssl-requests-only	Um Daten während der Übertragung zu schützen, stellen Sie sicher, dass Ihre Amazon Simple Storage Service (Amazon S3)-Bucke ts Anfragen zur Verwendun g von Secure Socket Layer (SSL)-Buckets erfordern. Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	AWS Config	Empfehlungen
Anexo II 4.1.2.a); b); c)	sagemaker-endpoint-configuration-kms-key-konfiguriert	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass die Verschlüsselung mit dem AWS Key Management Service (AWS KMS) für Ihren Endpunkt aktiviert ist. SageMaker Da sensible Daten auf dem SageMaker Endgerät gespeichert werden können, sollten Sie die Verschlüsselung im Ruhezustand aktivieren, um diese Daten zu schützen.
Anexo II 4.1.2.a); b); c)	secretsmanager-using-cmk	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass die Verschlüsselung mit dem AWS Key Management Service (AWS KMS) für AWS Secrets Manager aktiviert ist. Aktivieren Sie die Verschlüsselung von Daten im Ruhezustand, um eventuell vorhandene sensible Daten im Ruhezustand im Secrets Manager zu schützen.

Kontroll-ID	AWS Config	Empfehlungen
Anexo II 4.1.2.a); b); c)	vpc-vpn-2-tunnels-up	Redundante Site-to-Site VPN-Tunnel können implement iert werden, um die Anforderu ngen an die Ausfallsicherheit zu erfüllen. Es verwendet zwei Tunnel, um die Konnektiv ität sicherzustellen, falls eine der Site-to-Site VPN-Verbi ndungen nicht verfügbar ist. Um sich vor einem Verbindun gsverlust zu schützen, können Sie für den Fall, dass Ihr Kunden-Gateway nicht verfügbar ist, eine zweite Site-to-Site VPN-Verbindung zu Ihrer Amazon Virtual Private Cloud (Amazon VPC) und Ihrem Virtual Private Gateway einrichten, indem Sie ein zweites Kunden-Gateway verwenden.
Anexo II 4.1.2.b)	ec2- -eni-periodisch security-group-attached-to	Diese Regel stellt sicher, dass die Sicherheitsgruppen an eine Amazon Elastic Compute Cloud (Amazon EC2) - Instance oder an eine ENI angehängt sind. Diese Regel unterstützt die Überwachu ng ungenutzter Sicherhei tsgruppen im Bestand und die Verwaltung Ihrer Umgebung.

Kontroll-ID	AWS Config	Empfehlungen
Anexo II 4.1.2.b)	ec2-check managedinstance-association-compliance-status	Verwenden Sie AWS Systems Manager Associations, um bei der Inventarisierung von Softwareplattformen und Anwendungen innerhalb eines Unternehmens zu helfen. AWS Systems Manager weist Ihren verwalteten Instanzen einen Konfigurationsstatus zu und ermöglicht es Ihnen, Basiswerte für Betriebss ystem-Patch-Levels, Softwarei nstallationen, Anwendung skonfigurationen und andere Details zu Ihrer Umgebung festzulegen.
Anexo II 4.1.2.b)	ec2-stopped-instance	Aktivieren Sie diese Regel, um bei der Basiskonfiguration von Amazon Elastic Compute Cloud (Amazon EC2) - Instances zu helfen, indem Sie überprüfen, ob EC2 Amazon-Instances gemäß den Standards Ihrer Organisat ion für mehr als die zulässige Anzahl von Tagen gestoppt wurden.

Kontroll-ID	AWS Config	Empfehlungen
Anexo II 4.1.2.b)	ec2- volume-inuse-check	Diese Regel stellt sicher, dass Amazon Elastic Block Store-Volumes, die an Amazon Elastic Compute Cloud (Amazon EC2) -Instances angehängt sind, zum Löschen markiert werden, wenn eine Instance beendet wird. Wenn ein Amazon-EBS-Volume nicht gelöscht wird, wenn die Instance, an die es angehängt ist, beendet wird, kann dies gegen das Konzept der geringsten Funktionalität verstoßen.
Anexo II 4.1.2.b)	eip-attached	Diese Regel stellt sicher, dass Elastic, die einer Amazon Virtual Private Cloud (Amazon VPC) IPs zugewiesen sind, an Amazon Elastic Compute Cloud (Amazon EC2) - Instances oder verwendete Elastic Network Interfaces angehängt sind. Diese Regel hilft bei der Überwachung ungenutzter Inhalte EIPs in Ihrer Umgebung.

Kontroll-ID	AWS Config	Empfehlungen
Anexo II 4.1.2.b)	vpc-network-acl-unused-überprüfen	Diese Regel stellt sicher, dass Amazon Virtual Private Cloud (VPC)-Netzwerkzugriffskontrolllisten verwendet werden. Die Überwachung ungenutzter Netzwerkzugriffskontrolllisten kann zu einer genauen Inventarisierung und Verwaltung Ihrer Umgebung beitragen.
Anexo II 4.2.1.a)	iam-root-access-key-überprüfen	Der Zugriff auf Systeme und Ressourcen kann gesteuert werden, indem überprüft wird, ob der Root-Benutzer keine Zugriffsschlüssel mit seiner AWS Identity and Access Management (IAM) -Rolle verknüpft hat. Stellen Sie sicher, dass die Root-Zugriffsschlüssel gelöscht werden. Erstellen und verwenden Sie stattdessen rollenbasierte Funktionen, AWS-Konten um das Prinzip der geringsten Funktionalität zu berücksichtigen.

Kontroll-ID	AWS Config	Empfehlungen
Anexo II 4.2.4	ecs-task-definition-user-for-host-mode-check	Wenn für eine Aufgabend efinition erhöhte Berechtig ungen gelten, liegt das daran, dass der Kunde diesen Konfigurationen ausdrücklich zugestimmt hat. Diese Kontrolle prüft, ob eine unerwartete Berechtig ungseskalation vorliegt, wenn für eine Aufgabendefinition das Host-Netzwerk aktiviert ist, die Kunden aber keine erhöhten Berechtigungen aktiviert haben.
Anexo II 4.2.4	iam-policy-no-statements-with-full-access	Stellen Sie sicher, dass IAM-Aktionen nur auf die benötigte n Aktionen beschränkt sind. Wenn Benutzern mehr Rechte eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und der Aufgabentrennung verstoßen.

Kontroll-ID	AWS Config	Empfehlungen
Anexo II 4.2.4	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) kann Ihnen dabei helfen, die Prinzipien der geringsten Rechte und der Aufgabent rennung in Zugriffsberechtigu ngen und Autorisierungen zu integrieren und so zu verhindern, dass Richtlinien „Effect“: „Allow“ mit „Action“: „*“ anstelle von „Resource“: „*“ enthalten. Wenn Benutzern mehr Rechte eingeräumt werden, als für die Ausführun g einer Aufgabe erforderl ich sind, kann dies gegen das Prinzip der geringste n Berechtigung und der Aufgabentrennung verstoßen.
Anexo II 4.2.4	s3- bucket-policy-grantee-check	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie s3_ bucket_policy_grantee_check aktivieren. Diese Regel prüft, ob der vom Amazon S3 S3-Bucket gewährte Zugriff durch die von Ihnen bereitgestellten AWS Principals, Verbundbe nutzer, Service Principals, IP-Adressen oder Amazon Virtual Private Cloud (Amazon VPC) IDs eingeschränkt ist.

Kontroll-ID	AWS Config	Empfehlungen
Anexo II 4.2.5	iam-root-access-key-überprüfen	Der Zugriff auf Systeme und Ressourcen kann gesteuert werden, indem überprüft wird, ob der Root-Benutzer keine Zugriffsschlüssel mit seiner AWS Identity and Access Management (IAM) -Rolle verknüpft hat. Stellen Sie sicher, dass die Root-Zugriffsschlüssel gelöscht werden. Erstellen und verwenden Sie stattdessen rollenbasierte Funktionen, AWS-Konten um das Prinzip der geringsten Funktionalität zu berücksichtigen.

Kontroll-ID	AWS Config	Empfehlungen
Anexo II 4.2.5.BAJO.a)	iam-password-policy	Die Identitäten und Anmeldein formationen werden auf der Grundlage einer organisat orischen IAM-Passwortrichtl inie ausgestellt, verwaltet und verifiziert. Sie erfüllen oder übertreffen die Anforderu ngen, die von NIST SP 800-63 und dem Standard „Best Practices“ von AWS Foundational Security in Bezug auf die Passwortstärke festgelegt wurden. Mit dieser Regel können Sie optional RequireUppercaseCharacters (Wert für AWS grundlege nde Sicherheitsbewährte Methoden: wahr), RequireLo wercaseCharacters (Wert für bewährte Methoden für AWS grundlegende Sicherheit: wahr), RequireSymbols (Wert für bewährte Methoden für AWS grundlegende Sicherhei t: wahr), RequireNumbers (Wert für bewährte Methoden für AWS grundlegende Sicherheit: wahr), MinimumPa sswordLength (Wert für bewährte Methoden für AWS grundlegende Sicherheit: 14), PasswordReusePreve ntion (Wert für bewährte Methoden für AWS grundlege

Kontroll-ID	AWS Config	Empfehlungen
		nde Sicherheit: 24) und MaxPasswordAge (Wert für bewährte Methoden für AWS grundlegende Sicherhei t: 90) für Ihr IAM festlegen Kennwortrichtlinie. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisat ion entsprechen.

Kontroll-ID	AWS Config	Empfehlungen
Anexo II 4.2.5.BAJO.c)	iam-password-policy	Die Identitäten und Anmeldein formationen werden auf der Grundlage einer organisat orischen IAM-Passwortrichtl inie ausgestellt, verwaltet und verifiziert. Sie erfüllen oder übertreffen die Anforderungen des NIST SP 800-63 und des AWS Foundational Security Best Practices-Standards für Passwortstärke. Mit dieser Regel können Sie optional RequireUppercaseCharacters (Wert für AWS grundlege nde Sicherheitsbewährte Methoden: wahr), RequireLo wercaseCharacters (Wert für bewährte Methoden für AWS grundlegende Sicherheit: wahr), RequireSymbols (Wert für bewährte Methoden für AWS grundlegende Sicherhei t: wahr), RequireNumbers (Wert für bewährte Methoden für AWS grundlegende Sicherheit: wahr), MinimumPa sswordLength (Wert für bewährte Methoden für AWS grundlegende Sicherheit: 14), PasswordReusePreve ntion (Wert für bewährte Methoden für AWS grundlege nde Sicherheit: 24) und MaxPasswordAge (Wert

Kontroll-ID	AWS Config	Empfehlungen
		für bewährte Methoden für AWS grundlegende Sicherhei t: 90) für Ihr IAM festlegen Kennwortrichtlinie. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisat ion entsprechen.
Anexo II 4.2.6.ALTO.b)	iam-user-mfa-enabled	Aktivieren Sie diese Regel, um den Zugriff auf Ressourcen in der AWS Cloud einzuschr änken. Diese Regel sorgt dafür, dass die Multi-Faktor-Authentifizierung (MFA) für alle Benutzer aktiviert ist. MFA sorgt für eine weitere Schutzebene zusätzlich zu den Anmeldeinformationen. Reduzieren Sie Fälle von kompromittierten Konten, indem Sie MFA für Benutzer vorschreiben.

Kontroll-ID	AWS Config	Empfehlungen
Anexo II 4.2.6.ALTO.b)	mfa-enabled-for-iam-Konsolenzugriff	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass MFA für alle AWS Identity and Access Management (IAM) -Benutzer aktiviert ist, die über ein Konsolenkennwort verfügen. MFA sorgt für eine weitere Schutzebene zusätzlich zu den Anmeldeinformationen. Indem Sie MFA für Benutzer vorschreiben, können Sie Fälle kompromittierter Konten reduzieren und verhindern, dass unbefugte Benutzer auf vertrauliche Daten zugreifen.
Anexo II 4.2.6.ALTO.b)	root-account-hardware-mfa-aktiviert	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Hardware-MFA für den Root-Benutzer aktiviert ist. Der Stammbenutzer ist der AWS-Konto-Benutzer mit den meisten Berechtigungen. MFA sorgt für eine weitere Schutzebene zusätzlich zu den Anmeldeinformationen. Indem Sie MFA für den Root-Benutzer vorschreiben, können Sie die Anzahl AWS-Konten kompromittierter Benutzer reduzieren.

Kontroll-ID	AWS Config	Empfehlungen
Anexo II 4.2.6.ALTO.b)	root-account-mfa-enabled	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass MFA für den Root-Benutzer aktiviert ist. Der Stammbenutzer ist der AWS-Konto-Benutzer mit den meisten Berechtigungen. MFA sorgt für eine weitere Schutzebene zusätzlich zu den Anmeldeinformationen. Indem Sie MFA für den Root-Benutzer vorschreiben, können Sie die Anzahl AWS-Konten kompromittierter Benutzer reduzieren.
Anexo II 4.2.6.BAJO.c)	elasticsearch-logs-to-cloudwatch	Stellen Sie sicher, dass für Amazon OpenSearch Service-Domains Fehlerprotokolle aktiviert und zur Aufbewahrung und Beantwortung an Amazon CloudWatch Logs gestreamt werden. Domain-Fehlerprotokolle sind bei Sicherheits- und Zugriffsprüfungen sowie bei der Diagnose von Verfügbarkeitsproblemen nützlich.

Kontroll-ID	AWS Config	Empfehlungen
Anexo II 4.2.6.BAJO.c)	multi-region-cloudtrail-enabled	AWS CloudTrail zeichnet Aktionen und API-Aufrufe der AWS Management Console auf. Sie können feststellen, welche Benutzer und Konten angerufen wurden AWS, von welcher Quell-IP-Adresse aus die Anrufe getätigt wurden und wann die Anrufe erfolgten . CloudTrail übermittelt Protokolldateien aus allen AWS Regionen an Ihren S3-Bucket, wenn MULTI_REGION_CLOUD_TRAIL_ENABLED aktiviert ist. Außerdem wird beim AWS Start einer neuen Region derselbe Trail in der neuen Region erstellt. CloudTrail Dadurch erhalten Sie automatisch Protokoll dateien mit API-Aktivitäten für die neue Region.

Kontroll-ID	AWS Config	Empfehlungen
Anexo II 4.2.6.BAJO.c)	rds-logging-enabled	Um die Protokollierung und Überwachung in Ihrer Umgebung zu erleichtern, stellen Sie sicher, dass die Amazon Relational Database Service (Amazon RDS)-Protokollierung aktiviert ist. Mit der Amazon-RDS-Protokollierung können Sie Ereignisse wie Verbindungen, Verbindungsabbrüche, Abfragen oder abgefragte Tabellen erfassen.
Anexo II 4.2.6.BAJO.c)	wafv2-logging-enabled	Um die Protokollierung und Überwachung in Ihrer Umgebung zu erleichtern, aktivieren Sie die AWS WAF (V2) -Protokollierung im regionalen und globalen Web ACLs. AWS Die WAF-Protokollierung bietet detaillierte Informationen über den Datenverkehr, der von Ihrer Web-ACL analysiert wird. In den Protokollen werden die Uhrzeit aufgezeichnet, zu der die AWS WAF die Anfrage von Ihrer AWS Ressource erhalten hat, Informationen über die Anfrage und eine Aktion für die Regel, der jede Anfrage entsprach.

Kontroll-ID	AWS Config	Empfehlungen
Anexo II 4.2.6.BAJO.c)	api-gw-execution-logging-aktiviert	Die API-Gateway-Protokollierung zeigt detaillierte Ansichten der Benutzer, die auf die API zugegriffen haben, und wie diese Benutzer auf die API zugegriffen haben. Diese Einblicke ermöglichen die Transparenz von Benutzeraktivitäten.
Anexo II 4.2.6.BAJO.c)	cloud-trail-cloud-watch-logs-aktiviert	Verwenden Sie Amazon CloudWatch , um Protokollereignisaktivitäten zentral zu sammeln und zu verwalten . Die Aufnahme von AWS CloudTrail Daten liefert Einzelheiten zu den API-Aufrufaktivitäten in Ihrem AWS-Konto.

Kontroll-ID	AWS Config	Empfehlungen
Anexo II 4.2.6.BAJO.c)	cloudtrail-enabled	AWS CloudTrail kann bei der Nichtabstreitbarkeit helfen, indem Aktionen und API-Aufrufe der AWS Managemen t Console aufgezeichnet werden. Sie können die Benutzer und die Benutzer AWS-Konten , die einen AWS Dienst aufgerufen haben, die Quell-IP-Adresse, über die die Aufrufe generiert wurden, und den Zeitpunkt der Anrufe identifizieren. Einzelheiten zu den erfassten Daten finden Sie in den AWS CloudTrail Datensatzinhalten.
Anexo II 4.2.6.BAJO.c)	cloudtrail-s3-dataevents-en abled	Die Erfassung von Simple Storage Service (Amazon S3)-Datenereignissen unterstützt die Erkennung von ungewöhnl ichen Aktivitäten. Zu den Details gehören AWS-Konto Informationen über den Zugriff auf einen Amazon S3 S3-Bucket, die IP-Adresse und die Uhrzeit des Ereignisses.

Kontroll-ID	AWS Config	Empfehlungen
Anexo II 4.2.6.BAJO.c)	elb-logging-enabled	Die Elastic-Load-Balancing-Aktivität ist ein zentraler Kommunikationspunkt innerhalb einer Umgebung. Stellen Sie sicher, dass die ELB-Protokollierung aktiviert ist. Die gesammelten Daten enthalten detaillierte Informationen zu Anfragen, die an den ELB gesendet wurden. Jedes Protokoll enthält Informationen wie die Zeit, zu der die Anforderung einging, die Client-IP-Adresse, Latenzen, Anforderungspfade und Serverantworten.
Anexo II 4.2.6.BAJO.c)	opensearch-logs-to-cloudwatch	Stellen Sie sicher, dass für Amazon OpenSearch Service-Domains Fehlerprotokolle aktiviert und zur Aufbewahrung und Beantwortung an Amazon CloudWatch Logs gestreamt werden. OpenSearch Service-Fehlerprotokolle können bei Sicherheits- und Zugriffsprüfungen helfen und bei der Diagnose von Verfügbarkeitsproblemen helfen.

Kontroll-ID	AWS Config	Empfehlungen
Anexo II 4.2.6.BAJO.c)	s-3 bucket-logging-enabled	Die Amazon Simple Storage Service (Amazon S3)-Serve rzugriffsprotokollierung bietet eine Methode zur Überwachung des Netzwerks im Hinblick auf potenzielle Cybersicherheitsereignisse. Die Ereignisse werden überwacht, indem detaillie rte Aufzeichnungen über die Anfragen erfasst werden, die an einen Amazon-S3-Bucket gestellt wurden. Jeder Zugriffsprotokolleintrag enthält Details zu einer einzelnen Zugriffsanfrage. Zu den Details gehören Anfordere r, Bucket-Name, Anforderu ngszeit, Anforderungsaktion, Antwortstatus und Fehlercode, falls relevant.

Kontroll-ID	AWS Config	Empfehlungen
Anexo II 4.2.6.BAJO.c)	vpc-flow-logs-enabled	VPC-Flow-Protokolle erfassen detaillierte Informationsdatensätze über den IP-Datenverkehr, der zu und von Netzwerkschnittstellen in Ihrer Amazon Virtual Private Cloud (Amazon VPC) fließt. Standardmäßig enthalten Flow-Protokolldatensätze Werte für die verschiedenen Komponenten des IP-Flows, einschließlich Quelle, Ziel und Protokoll.
Anexo II 4.2.7.BAJO	iam-user-mfa-enabled	Aktivieren Sie diese Regel, um den Zugriff auf Ressourcen in der AWS Cloud einzuschränken. Diese Regel sorgt dafür, dass die Multi-Faktor-Authentifizierung (MFA) für alle Benutzer aktiviert ist. MFA sorgt für eine weitere Schutzebene zusätzlich zu den Anmeldeinformationen. Reduzieren Sie Fälle von kompromittierten Konten, indem Sie MFA für Benutzer vorschreiben.

Kontroll-ID	AWS Config	Empfehlungen
Anexo II 4.2.7.BAJO	mfa-enabled-for-iam-Konsolenzugriff	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass MFA für alle AWS Identity and Access Management (IAM) -Benutzer aktiviert ist, die über ein Konsolenkennwort verfügen. MFA sorgt für eine weitere Schutzebene zusätzlich zu den Anmeldeinformationen. Indem Sie MFA für Benutzer vorschreiben, können Sie Fälle kompromittierter Konten reduzieren und verhindern, dass unbefugte Benutzer auf vertrauliche Daten zugreifen.
Anexo II 4.2.7.BAJO	root-account-hardware-mfa-aktiviert	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Hardware-MFA für den Root-Benutzer aktiviert ist. Der Stammbenutzer ist der AWS-Konto-Benutzer mit den meisten Berechtigungen. MFA sorgt für eine weitere Schutzebene zusätzlich zu den Anmeldeinformationen. Indem Sie MFA für den Root-Benutzer vorschreiben, können Sie die Anzahl AWS-Konten kompromittierter Benutzer reduzieren.

Kontroll-ID	AWS Config	Empfehlungen
Anexo II 4.2.7.BAJO	root-account-mfa-enabled	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass MFA für den Root-Benutzer aktiviert ist. Der Stammbenutzer ist der AWS-Konto-Benutzer mit den meisten Berechtigungen. MFA sorgt für eine weitere Schutzebene zusätzlich zu den Anmeldeinformationen. Indem Sie MFA für den Root-Benutzer vorschreiben, können Sie die Anzahl AWS-Konten kompromittierter Benutzer reduzieren.
Anexo II 4.3.1	ec2- -eni-periodisch security-group-attached-to	Diese Regel stellt sicher, dass die Sicherheitsgruppen an eine Amazon Elastic Compute Cloud (Amazon EC2) - Instance oder an eine ENI angehängt sind. Diese Regel unterstützt die Überwachung ungenutzter Sicherheitsgruppen im Bestand und die Verwaltung Ihrer Umgebung.

Kontroll-ID	AWS Config	Empfehlungen
Anexo II 4.3.1	ec2-check managedinstance-association-compliance-status	Verwenden Sie AWS Systems Manager Associations, um bei der Inventarisierung von Softwareplattformen und Anwendungen innerhalb eines Unternehmens zu helfen. AWS Systems Manager weist Ihren verwalteten Instanzen einen Konfigurationsstatus zu und ermöglicht es Ihnen, Basiswerte für Betriebss ystem-Patch-Levels, Softwarei nstallationen, Anwendung skonfigurationen und andere Details zu Ihrer Umgebung festzulegen.
Anexo II 4.3.1	ec2-stopped-instance	Aktivieren Sie diese Regel, um bei der Basiskonfiguration von Amazon Elastic Compute Cloud (Amazon EC2) - Instances zu helfen, indem Sie überprüfen, ob EC2 Amazon-Instances gemäß den Standards Ihrer Organisat ion für mehr als die zulässige Anzahl von Tagen gestoppt wurden.

Kontroll-ID	AWS Config	Empfehlungen
Anexo II 4.3.1	ec2- volume-inuse-check	Diese Regel stellt sicher, dass Amazon Elastic Block Store-Volumes, die an Amazon Elastic Compute Cloud (Amazon EC2) -Instances angehängt sind, zum Löschen markiert werden, wenn eine Instance beendet wird. Wenn ein Amazon-EBS-Volume nicht gelöscht wird, wenn die Instance, an die es angehängt ist, beendet wird, kann dies gegen das Konzept der geringsten Funktionalität verstoßen.
Anexo II 4.3.1	eip-attached	Diese Regel stellt sicher, dass Elastic, die einer Amazon Virtual Private Cloud (Amazon VPC) IPs zugewiesen sind, an Amazon Elastic Compute Cloud (Amazon EC2) - Instances oder verwendete Elastic Network Interfaces angehängt sind. Diese Regel hilft bei der Überwachung ungenutzter Inhalte EIPs in Ihrer Umgebung.

Kontroll-ID	AWS Config	Empfehlungen
Anexo II 4.3.1	vpc-network-acl-unused-überprüfen	Diese Regel stellt sicher, dass Amazon Virtual Private Cloud (VPC)-Netzwerkzugriffskontrolllisten verwendet werden. Die Überwachung ungenutzter Netzwerkzugriffskontrolllisten kann zu einer genauen Inventarisierung und Verwaltung Ihrer Umgebung beitragen.
Anexo II 4.3.2.b)	alb-waf-enabled	Stellen Sie sicher, dass AWS WAF auf Elastic Load Balancers (ELB) aktiviert ist, um Webanwendungen zu schützen. Eine WAF trägt zum Schutz Ihrer Webanwendungen oder APIs vor gängigen Web-Exploits bei. Diese Web-Exploits können sich auf die Verfügbarkeit auswirken, die Sicherheit gefährden oder übermäßige Ressourcen in Ihrer Umgebung verbrauchen.

Kontroll-ID	AWS Config	Empfehlungen
Anexo II 4.3.2.b)	api-gw-associated-with-WAF	AWS Mit WAF können Sie eine Reihe von Regeln (als Web Access Control List (Web ACL) bezeichnet) konfiguri eren, die Webanfragen auf der Grundlage von anpassbar en Websicherheitsregeln und -bedingungen, die Sie definieren, zulassen, blockiere n oder zählen. Stellen Sie sicher, dass Ihre Amazon-API-Gateway-Stufe mit einer WAF-Web-ACL verknüpft ist, um sie vor böswilligen Angriffen zu schützen.
Anexo II 4.3.2.b)	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) Security Groups können bei der Verwaltung des Netzwerkz ugriffs helfen, indem sie eine statusbehaftete Filterung des ein- und ausgehend en Netzwerkverkehrs zu Ressourcen bereitstellen. AWS Wenn Sie eingehenden (oder entfernten) Datenverk ehr von 0.0.0.0/0 bis Port 22 auf Ihren Ressourcen nicht zulassen, können Sie den Remote-Zugriff einschränken.

Kontroll-ID	AWS Config	Empfehlungen
Anexo II 4.3.2.b)	no-unrestricted-route-to-igw	Stellen Sie sicher, dass EC2 Amazon-Routentabellen keine uneingeschränkten Routen zu einem Internet-Gateway enthalten. Durch das Entfernen oder Beschränken des Internetzugangs für Workloads innerhalb von Amazon VPCs können unbeabsichtigte Zugriffe in Ihrer Umgebung reduziert werden.

Kontroll-ID	AWS Config	Empfehlungen
Anexo II 4.3.2.b)	s3- -blöcke-periodisch account-level-public-access	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Simple Storage Service (Amazon S3) -Buckets nicht öffentlich zugänglich sind. Diese Regel trägt dazu bei, sensible Daten vor unbefugten Remote-Benutzern zu schützen, indem sie den öffentlichen Zugriff verhindert. Mit dieser Regel können Sie optional die Parameter ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) und restrictPublicBuckets Parameter (Config Default: True) festlegen. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	AWS Config	Empfehlungen
Anexo II 4.3.2.b)	ssm-document-not-public	Stellen Sie sicher, dass AWS Systems Manager (SSM) - Dokumente nicht öffentlich sind, da dies einen unbeabsichtigten Zugriff auf Ihre SSM-Dokumente ermöglichen kann. Ein öffentliches SSM-Dokument kann Informationen über Ihr Konto, Ihre Ressourcen und internen Prozesse preisgeben.
Anexo II 4.3.2.b)	dms-replication-not-public	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass auf DMS-Replikationsinstanzen nicht öffentlich zugegriffen werden kann. DMS-Replikations-Instances können vertrauliche Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.
Anexo II 4.3.2.b)	ebs-snapshot-public-restorable-überprüfen	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass EBS-Snapshots nicht öffentlich wiederherstellbar sind. EBS-Volume-Snapshots können vertrauliche Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	AWS Config	Empfehlungen
Anexo II 4.3.2.b)	ec-2 instance-no-public-ip	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon Elastic Compute Cloud (Amazon EC2) -Instances nicht öffentlich zugänglich sind. EC2 Amazon-Instances können vertrauliche Informati onen enthalten, und für solche Konten ist eine Zugriffsk ontrolle erforderlich.
Anexo II 4.3.2.b)	elasticsearch-in-vpc-only	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass sich Amazon OpenSearch OpenSearch Service (Service) -Domains innerhalb einer Amazon Virtual Private Cloud (Amazon VPC) befinden. Eine OpenSearch Service-D omain innerhalb einer Amazon VPC ermöglicht die sichere Kommunikation zwischen OpenSearch Service und anderen Services innerhalb der Amazon VPC, ohne dass ein Internet-Gateway, ein NAT-Gerät oder eine VPN-Verbindung erforderlich ist.

Kontroll-ID	AWS Config	Empfehlungen
Anexo II 4.3.2.b)	emr-master-no-public-ip	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon EMR-Cluster-Masterknoten nicht öffentlich zugänglich sind. Amazon-EMR-Cluster-Hauptknoten können vertrauliche Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.
Anexo II 4.3.2.b)	internet-gateway-authorized-vpc-nur	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Internet-Gateways nur mit autorisierter Amazon Virtual Private Cloud (Amazon VPC) verbunden sind. Internet-Gateways ermöglichen den bidirektionalen Internetzugang zur und von der Amazon VPC, was möglicherweise zu einem unbefugten Zugriff auf Amazon-VPC-Ressourcen führen kann.

Kontroll-ID	AWS Config	Empfehlungen
Anexo II 4.3.2.b)	lambda-function-public-access-verboten	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass AWS Lambda-Funktionen nicht öffentlich zugänglich sind. Der öffentliche Zugriff kann möglicherweise die Verfügbarkeit von Ressourcen beeinträchtigen.

Kontroll-ID	AWS Config	Empfehlungen
Anexo II 4.3.2.b)	lambda-inside-vpc	Stellen Sie AWS Lambda-Funktionen in einer Amazon Virtual Private Cloud (Amazon VPC) bereit, um eine sichere Kommunikation zwischen einer Funktion und anderen Diensten innerhalb der Amazon VPC zu gewährleisten. Bei dieser Konfiguration sind kein Internet-Gateway, kein NAT-Gerät und keine VPN-Verbindung erforderlich. Der gesamte Datenverkehr bleibt sicher in der Cloud. AWS Domains, die sich innerhalb einer VPC befinden, verfügen aufgrund ihrer logischen Isolierung im Vergleich zu Domains mit öffentlichen Endpunkten über eine zusätzliche Sicherheitsebene. Um den Zugriff ordnungsgemäß zu verwalten, sollten AWS Lambda-Funktionen einer VPC zugewiesen werden.

Kontroll-ID	AWS Config	Empfehlungen
Anexo II 4.3.2.b)	opensearch-in-vpc-only	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass sich Amazon OpenSearch Service-Domains innerhalb einer Amazon Virtual Private Cloud (Amazon VPC) befinden. Eine Amazon OpenSearch Service-Domain innerhalb einer Amazon VPC ermöglich t die sichere Kommunika tion zwischen Amazon OpenSearch Service und anderen Services innerhalb der Amazon VPC, ohne dass ein Internet-Gateway, ein NAT-Gerät oder eine VPN-Verbindung erforderlich ist.
Anexo II 4.3.2.b)	rds-instance-public-access-überprüfen	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherste llen, dass Amazon Relationa l Database Service (Amazon RDS) -Instances nicht öffentlic h sind. Amazon-RDS-Datenba nk-Instances können vertrauli che Informationen enthalten und für solche Konten sind Prinzipien und Zugriffsk ontrollen erforderlich.

Kontroll-ID	AWS Config	Empfehlungen
Anexo II 4.3.2.b)	rds-snapshots-public-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Relational Database Service (Amazon RDS) -Instances nicht öffentlich sind. Amazon-RDS-Datenbank-Instances können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.
Anexo II 4.3.2.b)	redshift-cluster-public-access-überprüfen	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Redshift Redshift-Cluster nicht öffentlich sind. Amazon-Redshift-Cluster können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	AWS Config	Empfehlungen
Anexo II 4.3.2.b)	restricted-common-ports	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass gemeinsame Ports für Amazon Elastic Compute Cloud (Amazon EC2) - Sicherheitsgruppen eingeschränkt sind. Wenn der Zugriff auf Ports nicht auf vertrauenswürdige Quellen beschränkt wird, kann dies zu Angriffen auf die Verfügbarkeit, Integrität und Vertraulichkeit von Systemen führen. Mit dieser Regel können Sie optional die Parameter blockedPort1–blockedPort5 festlegen (Standardkonfigurationen: 20, 21, 3389, 3306, 4333). Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	AWS Config	Empfehlungen
Anexo II 4.3.2.b)	s3 bucket-level-public-access - verboten	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherste llen, dass Amazon Simple Storage Service (Amazon S3) -Buckets nicht öffentlich zugänglich sind. Diese Regel trägt dazu bei, sensible Daten vor unbefugten Remote-Be nutzern zu schützen, indem sie den öffentlichen Zugriff auf Bucket-Ebene verhindert.
Anexo II 4.3.2.b)	s3- bucket-public-read-prohibit ed	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie nur autorisie rten Benutzern, Prozessen und Geräten Zugriff auf Amazon Simple Storage Service (Amazon S3) -Buckets gewähren. Die Verwaltung des Zugriffs sollte mit der Klassifiz ierung der Daten übereinst immen.

Kontroll-ID	AWS Config	Empfehlungen
Anexo II 4.3.2.b)	s3- bucket-public-write-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie nur autorisierten Benutzern, Prozessen und Geräten Zugriff auf Amazon Simple Storage Service (Amazon S3) -Buckets gewähren. Die Verwaltung des Zugriffs sollte mit der Klassifizierung der Daten übereinstimmen.
Anexo II 4.3.2.b)	sagemaker-notebook-no-direct-Internetzugang	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass SageMaker Amazon-Notebooks keinen direkten Internetzugang zulassen. Indem Sie direkten Internetzugang blockieren, vermeiden Sie, dass unbefugte Benutzer auf sensible Daten zugreifen.

Kontroll-ID	AWS Config	Empfehlungen
Anexo II 4.3.2.b)	subnet-auto-assign-public-ip-deaktiviert	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon Virtual Private Cloud (VPC) -Subnetzen nicht automatis ch eine öffentliche IP-Adress e zugewiesen wird. Amazon Elastic Compute Cloud (EC2) -Instances, die in Subnetzen gestartet werden, in denen dieses Attribut aktiviert ist, haben ihrer primären Netzwerkschnittste lle eine öffentliche IP-Adresse zugewiesen.
Anexo II 4.3.2.b)	vpc-default-security-group-geschlossen	Sicherheitsgruppen von Amazon Elastic Compute Cloud (Amazon EC2) können bei der Verwaltung des Netzwerkzugriffs helfen, indem sie eine statusbeh aftete Filterung des ein- und ausgehenden Netzwerkv erkehrs zu Ressourcen bereitstellen. AWS Die Beschränkung des gesamten Datenverkehrs auf die Standardsicherheitsgruppe hilft dabei, den Fernzugriff auf Ihre Ressourcen einzuschr änken. AWS

Kontroll-ID	AWS Config	Empfehlungen
Anexo II 4.3.2.b)	vpc-sg-open-only-to-authorized-ports	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass gemeinsame Ports für Amazon Elastic Compute Cloud (Amazon EC2) - Sicherheitsgruppen eingeschränkt sind. Wenn der Zugriff auf Ports nicht auf vertrauenswürdige Quellen beschränkt wird, kann dies zu Angriffen auf die Verfügbarkeit, Integrität und Vertraulichkeit von Systemen führen. Durch die Beschränkung des Zugriffs auf Ressourcen innerhalb einer Sicherheitsgruppe aus dem Internet (0.0.0.0/0) kann der Remote-Zugriff auf interne Systeme gesteuert werden.

Kontroll-ID	AWS Config	Empfehlungen
Anexo II 4.3.4.c)	vuln-management-plan-exists (Prozessüberprüfung)	Stellen Sie sicher, dass ein Plan für das Schwachst ellenmanagement entwickel t und implementiert wird, damit Sie über formell definiert e Prozesse zur Behebung von Schwachstellen in Ihrer Umgebung verfügen. Dazu zählen Tools für das Schwachstellenmanagement, regelmäßige Umgebungs scans sowie entsprechende Rollen und Verantwortlichkeit en.
Anexo II 4.3.6	guardduty-enabled-centralized	Amazon GuardDuty kann mithilfe von Threat Intellige nce Feeds helfen, potenzielle Cybersicherheitsereignisse zu überwachen und zu erkennen. Dazu gehören Listen mit bösartigen IPs und maschinel len Lernmethoden zur Identifiz ierung unerwarteter, nicht autorisierter und bösartige r Aktivitäten in Ihrer AWS Cloud-Umgebung.

Kontroll-ID	AWS Config	Empfehlungen
Anexo II 4.3.7.MEDIA.a)	response-plan-exists-maintained (Prozessüberprüfung)	Stellen Sie sicher, dass Vorfallreaktionspläne erstellt, verwaltet und an das verantwortliche Personal verteilt werden. Aktualisierte und formal dokumentierte Reaktionspläne können dazu beitragen, dass das zuständige Personal die Rollen, Verantwortlichkeiten und Prozesse versteht, die bei einem Vorfall einzuhalten sind.
Anexo II 4.3.8.BAJO	elasticsearch-logs-to-cloudwatch	Stellen Sie sicher, dass für Amazon OpenSearch Service-Domains Fehlerprotokolle aktiviert und zur Aufbewahrung und Beantwortung an Amazon CloudWatch Logs gestreamt werden. Domain-Fehlerprotokolle sind bei Sicherheits- und Zugriffsprüfungen sowie bei der Diagnose von Verfügbarkeitsproblemen nützlich.

Kontroll-ID	AWS Config	Empfehlungen
Anexo II 4.3.8.BAJO	multi-region-cloudtrail-enabled	AWS CloudTrail zeichnet Aktionen und API-Aufrufe der AWS Management Console auf. Sie können feststellen, welche Benutzer und Konten angerufen wurden AWS, von welcher Quell-IP-Adresse aus die Anrufe getätigt wurden und wann die Anrufe erfolgten . CloudTrail übermittelt Protokolldateien aus allen AWS Regionen an Ihren S3-Bucket, wenn MULTI_REGION_CLOUD_TRAIL_ENABLED aktiviert ist. Außerdem wird beim AWS Start einer neuen Region derselbe Trail in der neuen Region erstellt. CloudTrail Dadurch erhalten Sie automatisch Protokoll dateien mit API-Aktivitäten für die neue Region.

Kontroll-ID	AWS Config	Empfehlungen
Anexo II 4.3.8.BAJO	rds-logging-enabled	Um die Protokollierung und Überwachung in Ihrer Umgebung zu erleichtern, stellen Sie sicher, dass die Amazon Relational Database Service (Amazon RDS)-Protokollierung aktiviert ist. Mit der Amazon-RDS-Protokollierung können Sie Ereignisse wie Verbindungen, Verbindungsabbrüche, Abfragen oder abgefragte Tabellen erfassen.
Anexo II 4.3.8.BAJO	wafv2-logging-enabled	Um die Protokollierung und Überwachung in Ihrer Umgebung zu erleichtern, aktivieren Sie die AWS WAF (V2) -Protokollierung im regionalen und globalen Web ACLs. AWS Die WAF-Protokollierung bietet detaillierte Informationen über den Datenverkehr, der von Ihrer Web-ACL analysiert wird. In den Protokollen werden die Uhrzeit aufgezeichnet, zu der die AWS WAF die Anfrage von Ihrer AWS Ressource erhalten hat, Informationen über die Anfrage und eine Aktion für die Regel, der jede Anfrage entsprach.

Kontroll-ID	AWS Config	Empfehlungen
Anexo II 4.3.8.BAJO	api-gw-execution-logging-aktiviert	Die API-Gateway-Protokollierung zeigt detaillierte Ansichten der Benutzer, die auf die API zugegriffen haben, und wie diese Benutzer auf die API zugegriffen haben. Diese Einblicke ermöglichen die Transparenz von Benutzeraktivitäten.
Anexo II 4.3.8.BAJO	cloud-trail-cloud-watch-logs-aktiviert	Verwenden Sie Amazon CloudWatch , um Protokollereignisaktivitäten zentral zu sammeln und zu verwalten . Die Aufnahme von AWS CloudTrail Daten liefert Einzelheiten zu den API-Aufrufaktivitäten in Ihrem AWS-Konto.

Kontroll-ID	AWS Config	Empfehlungen
Anexo II 4.3.8.BAJO	cloudtrail-enabled	AWS CloudTrail kann bei der Nichtabstreitbarkeit helfen, indem Aktionen und API-Aufrufe der AWS Managemen t Console aufgezeichnet werden. Sie können die Benutzer und die Benutzer AWS-Konten , die einen AWS Dienst aufgerufen haben, die Quell-IP-Adresse, über die die Aufrufe generiert wurden, und den Zeitpunkt der Anrufe identifizieren. Einzelheiten zu den erfassten Daten finden Sie in den AWS CloudTrail Datensatzinhalten.
Anexo II 4.3.8.BAJO	cloudtrail-s3-dataevents-en abled	Die Erfassung von Simple Storage Service (Amazon S3)-Datenereignissen unterstützt die Erkennung von ungewöhnl ichen Aktivitäten. Zu den Details gehören AWS-Konto Informationen über den Zugriff auf einen Amazon S3 S3-Bucket, die IP-Adresse und die Uhrzeit des Ereignisses.

Kontroll-ID	AWS Config	Empfehlungen
Anexo II 4.3.8.BAJO	elb-logging-enabled	Die Elastic-Load-Balancing-Aktivität ist ein zentraler Kommunikationspunkt innerhalb einer Umgebung. Stellen Sie sicher, dass die ELB-Protokollierung aktiviert ist. Die gesammelten Daten enthalten detaillierte Informationen zu Anfragen, die an den ELB gesendet wurden. Jedes Protokoll enthält Informationen wie die Zeit, zu der die Anforderung einging, die Client-IP-Adresse, Latenzen, Anforderungspfade und Serverantworten.
Anexo II 4.3.8.BAJO	opensearch-logs-to-cloudwatch	Stellen Sie sicher, dass für Amazon OpenSearch Service-Domains Fehlerprotokolle aktiviert und zur Aufbewahrung und Beantwortung an Amazon CloudWatch Logs gestreamt werden. OpenSearch Service-Fehlerprotokolle können bei Sicherheits- und Zugriffsprüfungen helfen und bei der Diagnose von Verfügbarkeitsproblemen helfen.

Kontroll-ID	AWS Config	Empfehlungen
Anexo II 4.3.8.BAJO	s-3 bucket-logging-enabled	Die Amazon Simple Storage Service (Amazon S3)-Serverzugriffsprotokollierung bietet eine Methode zur Überwachung des Netzwerks im Hinblick auf potenzielle Cybersicherheitsereignisse. Die Ereignisse werden überwacht, indem detaillierte Aufzeichnungen über die Anfragen erfasst werden, die an einen Amazon-S3-Bucket gestellt wurden. Jeder Zugriffsprotokolleintrag enthält Details zu einer einzelnen Zugriffsanfrage. Zu den Details gehören Anforderer, Bucket-Name, Anforderungszeit, Anforderungsaktion, Antwortstatus und Fehlercode, falls relevant.

Kontroll-ID	AWS Config	Empfehlungen
Anexo II 4.3.8.BAJO	vpc-flow-logs-enabled	VPC-Flow-Protokolle erfassen detaillierte Informationsdatensätze über den IP-Datenverkehr, der zu und von Netzwerkschnittstellen in Ihrer Amazon Virtual Private Cloud (Amazon VPC) fließt. Standardmäßig enthalten Flow-Protokolldatensätze Werte für die verschiedenen Komponenten des IP-Flows, einschließlich Quelle, Ziel und Protokoll.
Anexo II 4.3.8.MEDIO	elasticsearch-logs-to-cloudwatch	Stellen Sie sicher, dass für Amazon OpenSearch Service-Domains Fehlerprotokolle aktiviert und zur Aufbewahrung und Beantwortung an Amazon CloudWatch Logs gestreamt werden. Domain-Fehlerprotokolle sind bei Sicherheits- und Zugriffsprüfungen sowie bei der Diagnose von Verfügbarkeitsproblemen nützlich.

Kontroll-ID	AWS Config	Empfehlungen
Anexo II 4.3.8.MEDIO	multi-region-cloudtrail-enabled	AWS CloudTrail zeichnet Aktionen und API-Aufrufe der AWS Management Console auf. Sie können feststellen, welche Benutzer und Konten angerufen wurden AWS, von welcher Quell-IP-Adresse aus die Anrufe getätigt wurden und wann die Anrufe erfolgten . CloudTrail übermittelt Protokolldateien aus allen AWS Regionen an Ihren S3-Bucket, wenn MULTI_REGION_CLOUD_TRAIL_ENABLED aktiviert ist. Außerdem wird beim AWS Start einer neuen Region derselbe Trail in der neuen Region erstellt. CloudTrail Dadurch erhalten Sie automatisch Protokoll dateien mit API-Aktivitäten für die neue Region.

Kontroll-ID	AWS Config	Empfehlungen
Anexo II 4.3.8.MEDIO	rds-logging-enabled	Um die Protokollierung und Überwachung in Ihrer Umgebung zu erleichtern, stellen Sie sicher, dass die Amazon Relational Database Service (Amazon RDS)-Protokollierung aktiviert ist. Mit der Amazon-RDS-Protokollierung können Sie Ereignisse wie Verbindungen, Verbindungsabbrüche, Abfragen oder abgefragte Tabellen erfassen.
Anexo II 4.3.8.MEDIO	wafv2-logging-enabled	Um die Protokollierung und Überwachung in Ihrer Umgebung zu erleichtern, aktivieren Sie die AWS WAF (V2) -Protokollierung im regionalen und globalen Web ACLs. AWS Die WAF-Protokollierung bietet detaillierte Informationen über den Datenverkehr, der von Ihrer Web-ACL analysiert wird. In den Protokollen werden die Uhrzeit aufgezeichnet, zu der die AWS WAF die Anfrage von Ihrer AWS Ressource erhalten hat, Informationen über die Anfrage und eine Aktion für die Regel, der jede Anfrage entsprach.

Kontroll-ID	AWS Config	Empfehlungen
Anexo II 4.3.8.MEDIO	api-gw-execution-logging-aktiviert	Die API-Gateway-Protokollierung zeigt detaillierte Ansichten der Benutzer, die auf die API zugegriffen haben, und wie diese Benutzer auf die API zugegriffen haben. Diese Einblicke ermöglichen die Transparenz von Benutzeraktivitäten.
Anexo II 4.3.8.MEDIO	cloud-trail-cloud-watch-logs-aktiviert	Verwenden Sie Amazon CloudWatch , um Protokollereignisaktivitäten zentral zu sammeln und zu verwalten . Die Aufnahme von AWS CloudTrail Daten liefert Einzelheiten zu den API-Aufrufaktivitäten in Ihrem AWS-Konto.

Kontroll-ID	AWS Config	Empfehlungen
Anexo II 4.3.8.MEDIO	cloudtrail-enabled	AWS CloudTrail kann bei der Nichtabstreitbarkeit helfen, indem Aktionen und API-Aufrufe der AWS Managemen t Console aufgezeichnet werden. Sie können die Benutzer und die Benutzer AWS-Konten , die einen AWS Dienst aufgerufen haben, die Quell-IP-Adresse, über die die Aufrufe generiert wurden, und den Zeitpunkt der Anrufe identifizieren. Einzelheiten zu den erfassten Daten finden Sie in den AWS CloudTrail Datensatzinhalten.
Anexo II 4.3.8.MEDIO	cloudtrail-s3-dataevents-en abled	Die Erfassung von Simple Storage Service (Amazon S3)-Datenereignissen unterstützt die Erkennung von ungewöhnl ichen Aktivitäten. Zu den Details gehören AWS-Konto Informationen über den Zugriff auf einen Amazon S3 S3-Bucket, die IP-Adresse und die Uhrzeit des Ereignisses.

Kontroll-ID	AWS Config	Empfehlungen
Anexo II 4.3.8.MEDIO	elb-logging-enabled	Die Elastic-Load-Balancing-Aktivität ist ein zentraler Kommunikationspunkt innerhalb einer Umgebung. Stellen Sie sicher, dass die ELB-Protokollierung aktiviert ist. Die gesammelten Daten enthalten detaillierte Informationen zu Anfragen, die an den ELB gesendet wurden. Jedes Protokoll enthält Informationen wie die Zeit, zu der die Anforderung einging, die Client-IP-Adresse, Latenzen, Anforderungspfade und Serverantworten.
Anexo II 4.3.8.MEDIO	opensearch-logs-to-cloudwatch	Stellen Sie sicher, dass für Amazon OpenSearch Service-Domains Fehlerprotokolle aktiviert und zur Aufbewahrung und Beantwortung an Amazon CloudWatch Logs gestreamt werden. OpenSearch Service-Fehlerprotokolle können bei Sicherheits- und Zugriffsprüfungen helfen und bei der Diagnose von Verfügbarkeitsproblemen helfen.

Kontroll-ID	AWS Config	Empfehlungen
Anexo II 4.3.8.MEDIO	s-3 bucket-logging-enabled	Die Amazon Simple Storage Service (Amazon S3)-Serverzugriffsprotokollierung bietet eine Methode zur Überwachung des Netzwerks im Hinblick auf potenzielle Cybersicherheitsereignisse. Die Ereignisse werden überwacht, indem detaillierte Aufzeichnungen über die Anfragen erfasst werden, die an einen Amazon-S3-Bucket gestellt wurden. Jeder Zugriffsprotokolleintrag enthält Details zu einer einzelnen Zugriffsanfrage. Zu den Details gehören Anforderer, Bucket-Name, Anforderungszeit, Anforderungsaktion, Antwortstatus und Fehlercode, falls relevant.

Kontroll-ID	AWS Config	Empfehlungen
Anexo II 4.3.8.MEDIO	vpc-flow-logs-enabled	VPC-Flow-Protokolle erfassen detaillierte Informationsdatensätze über den IP-Datenverkehr, der zu und von Netzwerkschnittstellen in Ihrer Amazon Virtual Private Cloud (Amazon VPC) fließt. Standardmäßig enthalten Flow-Protokolldatensätze Werte für die verschiedenen Komponenten des IP-Flows, einschließlich Quelle, Ziel und Protokoll.
Anexo II 4.3.10.b)	cloud-trail-encryption-enabled	Da sensible Daten vorhanden sein können und um Daten im Ruhezustand zu schützen, sollten Sie sicherstellen, dass die Verschlüsselung für Ihre AWS CloudTrail Trails aktiviert ist.

Kontroll-ID	AWS Config	Empfehlungen
Anexo II 4.3.10.b)	cloud-trail-log-file-Validierung aktiviert	Verwenden Sie die AWS CloudTrail Protokolldateivalidierung, um die Integrität von Protokollen zu überprüfen. CloudTrail Mithilfe der Protokolldateivalidierung kann festgestellt werden, ob eine Protokolldatei geändert oder gelöscht wurde oder ob sie nach der Übermittlung CloudTrail unverändert geblieben ist. Dieses Feature wurde mit dem Branchenstandard entsprechenden Algorithmen entwickelt: SHA-256 für die Hashfunktion und SHA-256 mit RSA für digitale Signaturen. Aus diesem Grund ist es rechnerisch unmöglich, CloudTrail Protokolldateien unbemerkt zu ändern, zu löschen oder zu fälschen.

Kontroll-ID	AWS Config	Empfehlungen
Anexo II 4.3.10.d)	s-3 bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) unterstützt die Aufrechte rhaltung einer angemessenen Kapazität und Verfügbarkeit. CRR ermöglicht das automatis che, asynchrone Kopieren von Objekten in Amazon-S3 -Buckets, um die Datenverf ügbarkeit sicherzustellen.
Anexo II 4.6.1	guardduty-enabled-centralized	Amazon GuardDuty kann mithilfe von Threat Intellige nce Feeds helfen, potenzielle Cybersicherheitsereignisse zu überwachen und zu erkennen. Dazu gehören Listen mit bösartigen IPs und maschinel len Lernmethoden zur Identifiz ierung unerwarteter, nicht autorisierter und bösartige r Aktivitäten in Ihrer AWS Cloud-Umgebung.

Kontroll-ID	AWS Config	Empfehlungen
Anexo II 4.6.2.ALTO	guardduty-non-archived-findings	Amazon GuardDuty hilft Ihnen dabei, die Auswirkungen eines Vorfalls zu verstehen, indem es die Ergebnisse nach Schweregrad klassifiziert: niedrig, mittel und hoch. Diese Klassifizierungen können Sie zur Festlegung von entsprechenden Strategien und Prioritäten zur Behebung solcher Vorfälle verwenden. Mit dieser Regel können Sie optional daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7) und daysHighSev (Config Default: 1) für nicht archivierte Ergebnisse festlegen, wie es die Richtlinien Ihrer Organisation erfordern.

Kontroll-ID	AWS Config	Empfehlungen
Anexo II 4.6.2.BASICA	securityhub-enabled	AWS Security Hub hilft bei der Überwachung von unbefugte m Personal, Verbindungen, Geräten und Software. AWS Security Hub aggregiert, organisiert und priorisiert die Sicherheitswarnungen oder Ergebnisse mehrerer Dienste. AWS Einige dieser Dienste sind Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer und AWS Firewall Manager sowie AWS Partnerlösungen.
Anexo II 4.6.2.MEDIA	guardduty-enabled-centralized	Amazon GuardDuty kann mithilfe von Threat Intellige nce Feeds helfen, potenzielle Cybersicherheitsereignisse zu überwachen und zu erkennen. Dazu gehören Listen mit bösartigen IPs und maschinel len Lernmethoden zur Identifiz ierung unerwarteter, nicht autorisierter und bösartige r Aktivitäten in Ihrer AWS Cloud-Umgebung.

Kontroll-ID	AWS Config	Empfehlungen
Anexo II 5.2.3	security-awareness-program-exists (Prozessüberprüfung)	Etablieren und pflegen Sie ein Programm zur Förderung des Sicherheitsbewusst seins in Ihrer Organisation. Programme zur Förderung des Sicherheitsbewusstseins der Mitarbeiter vermitteln ihnen, wie sie ihre Organisation vor diversen Sicherheitsverletz ungen oder Sicherheitsvorfäll en schützen können.
Anexo II 5.2.4	security-awareness-program-exists (Prozessüberprüfung)	Etablieren und pflegen Sie ein Programm zur Förderung des Sicherheitsbewusst seins in Ihrer Organisation. Programme zur Förderung des Sicherheitsbewusstseins der Mitarbeiter vermitteln ihnen, wie sie ihre Organisation vor diversen Sicherheitsverletz ungen oder Sicherheitsvorfäll en schützen können.
Anexo II 5.2.5	security-awareness-program-exists (Prozessüberprüfung)	Etablieren und pflegen Sie ein Programm zur Förderung des Sicherheitsbewusst seins in Ihrer Organisation. Programme zur Förderung des Sicherheitsbewusstseins der Mitarbeiter vermitteln ihnen, wie sie ihre Organisation vor diversen Sicherheitsverletz ungen oder Sicherheitsvorfäll en schützen können.

Kontroll-ID	AWS Config	Empfehlungen
Anexo II 5.4.2.MEDIO	elasticsearch-node-to-node-Verschlüsselungsprüfung	Stellen Sie sicher, dass die node-to-node Verschlüsselung für Amazon OpenSearch Service aktiviert ist. Node-to-nodeVerschlüsselung ermöglicht die TLS 1.2-Versc hlüsselung für die gesamte Kommunikation innerhalb der Amazon Virtual Private Cloud (Amazon VPC). Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.
Anexo II 5.4.2.MEDIO	elbv-2 acm-certificate-required	Zum Schutz von eventuell vorhandenen sensiblen Daten sowie von Daten während der Übertragung muss die Verschlüsselung für Ihr Elastic Load Balancing aktiviert sein. Verwenden Sie AWS Certifica te Manager, um öffentlic he und private SSL/TLS-Z ertifikate mit AWS Diensten und internen Ressourcen zu verwalten, bereitzustellen und bereitzustellen.

Kontroll-ID	AWS Config	Empfehlungen
Anexo II 5.4.2.MEDIO	elb-tls-https-listeners-nur	Stellen Sie sicher, dass Ihre Elastic Load Balancer (ELBs) mit SSL- oder HTTPS-Listenern konfiguriert sind. Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.
Anexo II 5.4.2.MEDIO	alb-http-to-https-Umleitungsprüfung	Um Daten während der Übertragung zu schützen, stellen Sie sicher, dass Ihr Application Load Balancer unverschlüsselte HTTP-Anfragen automatisch an HTTPS umleitet. Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.
Anexo II 5.4.2.MEDIO	api-gw-ssl-enabled	Stellen Sie sicher, dass die REST-API-Stufen von Amazon API Gateway mit SSL-Zertifikaten konfiguriert sind, damit Backend-Systeme überprüfen können, ob Anforderungen von API Gateway stammen.

Kontroll-ID	AWS Config	Empfehlungen
Anexo II 5.4.2.MEDIO	elb-acm-certificate-required	Zum Schutz von eventuell vorhandenen sensiblen Daten sowie von Daten während der Übertragung muss die Verschlüsselung für Ihr Elastic Load Balancing aktiviert sein. Verwenden Sie AWS Certifica te Manager, um öffentlic he und private SSL/TLS-Z ertifikate mit AWS Diensten und internen Ressourcen zu verwalten, bereitzustellen und bereitzustellen.
Anexo II 5.4.2.MEDIO	opensearch-logs-to-cloudwat ch	Stellen Sie sicher, dass für Amazon OpenSearch Service-Domains Fehlerprotokolle aktiviert und zur Aufbewahr ung und Beantwortung an Amazon CloudWatch Logs gestreamt werden. OpenSearc h Service-Fehlerprotokolle können bei Sicherheits- und Zugriffsprüfungen helfen und bei der Diagnose von Verfügbarkeitsproblemen helfen.

Kontroll-ID	AWS Config	Empfehlungen
Anexo II 5.4.2.MEDIO	redshift-require-tls-ssl	Stellen Sie sicher, dass Ihre Amazon-Redshift-Cluster eine TLS/SSL-Verschlüsselung erfordern, um eine Verbindun g zu SQL-Clients herzustel len. Um eventuell vorhanden e sensible Daten zu schützen, sollten Sie die Verschlüs selung bei der Übertragung aktivieren.
Anexo II 5.4.2.MEDIO	s-3 bucket-ssl-requests-only	Um Daten während der Übertragung zu schützen, stellen Sie sicher, dass Ihre Amazon Simple Storage Service (Amazon S3)-Bucke ts Anfragen zur Verwendun g von Secure Socket Layer (SSL)-Buckets erfordern. Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	AWS Config	Empfehlungen
Anexo II 5.4.3.BAJO.a)	iam-password-policy	Die Identitäten und Anmeldein formationen werden auf der Grundlage einer organisat orischen IAM-Passwortrichtl inie ausgestellt, verwaltet und verifiziert. Sie erfüllen oder übertreffen die Anforderungen des NIST SP 800-63 und des AWS Foundational Security Best Practices-Standards für Passwortstärke. Mit dieser Regel können Sie optional RequireUppercaseCharacters (Wert für AWS grundlege nde Sicherheitsbewährte Methoden: wahr), RequireLo wercaseCharacters (Wert für bewährte Methoden für AWS grundlegende Sicherheit: wahr), RequireSymbols (Wert für bewährte Methoden für AWS grundlegende Sicherhei t: wahr), RequireNumbers (Wert für bewährte Methoden für AWS grundlegende Sicherheit: wahr), MinimumPa sswordLength (Wert für bewährte Methoden für AWS grundlegende Sicherheit: 14), PasswordReusePreve ntion (Wert für bewährte Methoden für AWS grundlege nde Sicherheit: 24) und MaxPasswordAge (Wert

Kontroll-ID	AWS Config	Empfehlungen
		für bewährte Methoden für AWS grundlegende Sicherhei t: 90) für Ihr IAM festlegen Kennwortrichtlinie. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisat ion entsprechen.
Anexo II 5.4.3.MEDIO	elasticsearch-node-to-node-Verschlüsselungsprüfung	Stellen Sie sicher, dass die node-to-node Verschlüsselung für Amazon OpenSearch Service aktiviert ist. Node-to-nodeVerschlüsselung ermöglicht die TLS 1.2-Versc hlüsselung für die gesamte Kommunikation innerhalb der Amazon Virtual Private Cloud (Amazon VPC). Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	AWS Config	Empfehlungen
Anexo II 5.4.3.MEDIO	elbv-2 acm-certificate-required	Zum Schutz von eventuell vorhandenen sensiblen Daten sowie von Daten während der Übertragung muss die Verschlüsselung für Ihr Elastic Load Balancing aktiviert sein. Verwenden Sie AWS Certifica te Manager, um öffentlic he und private SSL/TLS-Z ertifikate mit AWS Diensten und internen Ressourcen zu verwalten, bereitzustellen und bereitzustellen.
Anexo II 5.4.3.MEDIO	elb-tls-https-listeners-nur	Stellen Sie sicher, dass Ihre Elastic Load Balancer (ELBs) mit SSL- oder HTTPS-Lis tenern konfiguriert sind. Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.
Anexo II 5.4.3.MEDIO	alb-http-to-https-Umleitung sprüfung	Um Daten während der Übertragung zu schützen, stellen Sie sicher, dass Ihr Application Load Balancer unverschlüsselte HTTP-Anfragen automatisch an HTTPS umleitet. Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	AWS Config	Empfehlungen
Anexo II 5.4.3.MEDIO	api-gw-ssl-enabled	Stellen Sie sicher, dass die REST-API-Stufen von Amazon API Gateway mit SSL-Zerti fikaten konfiguriert sind, damit Backend-Systeme überprüfe n können, ob Anforderungen von API Gateway stammen.
Anexo II 5.4.3.MEDIO	elb-acm-certificate-required	Zum Schutz von eventuell vorhandenen sensiblen Daten sowie von Daten während der Übertragung muss die Verschlüsselung für Ihr Elastic Load Balancing aktiviert sein. Verwenden Sie AWS Certifica te Manager, um öffentlic he und private SSL/TLS-Z ertifikate mit AWS Diensten und internen Ressourcen zu verwalten, bereitzustellen und bereitzustellen.
Anexo II 5.4.3.MEDIO	opensearch-logs-to-cloudwat ch	Stellen Sie sicher, dass für Amazon OpenSearch Service-Domains Fehlerprotokolle aktiviert und zur Aufbewahr ung und Beantwortung an Amazon CloudWatch Logs gestreamt werden. OpenSearc h Service-Fehlerprotokolle können bei Sicherheits- und Zugriffsprüfungen helfen und bei der Diagnose von Verfügbarkeitsproblemen helfen.

Kontroll-ID	AWS Config	Empfehlungen
Anexo II 5.4.3.MEDIO	redshift-require-tls-ssl	Stellen Sie sicher, dass Ihre Amazon-Redshift-Cluster eine TLS/SSL-Verschlüsselung erfordern, um eine Verbindun g zu SQL-Clients herzustel len. Um eventuell vorhanden e sensible Daten zu schützen, sollten Sie die Verschlüs selung bei der Übertragung aktivieren.
Anexo II 5.4.3.MEDIO	s-3 bucket-ssl-requests-only	Um Daten während der Übertragung zu schützen, stellen Sie sicher, dass Ihre Amazon Simple Storage Service (Amazon S3)-Bucke ts Anfragen zur Verwendun g von Secure Socket Layer (SSL)-Buckets erfordern. Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	AWS Config	Empfehlungen
Anexo II 5.6.1.c)	codebuild-project-envvar-awscred-überprüfen	Stellen Sie sicher, dass die Anmeldeinformationen AWS_ACCESS_KEY_ID AWS_SECRET_ACCESS_KEY nicht in AWS Codebuild -Projektumgebungen vorhanden sind. Speichern Sie diese Variablen nicht als Klartext. Das Speichern dieser Variablen als Klartext bewirkt eine unbeabsichtigte Offenlegung von Daten sowie unberechtigte Zugriffe.
Anexo II 5.6.1.c)	codebuild-project-source-repo-URL-Prüfung	Stellen Sie sicher, dass die URL des Quell-Repositorys GitHub oder des Bitbucket -Quell-Repositorys keine persönlichen Zugriffstoken oder Anmeldeinformationen in Codebuild-Projektumgebungen enthält. AWS Verwende OAuth anstelle von persönlichen Zugriffstoken oder Anmeldedaten die Autorisierung für den Zugriff auf GitHub Bitbucket-Repositorys.

Kontroll-ID	AWS Config	Empfehlungen
Anexo II 5.7.3	dynamodb-table-encrypted-kms	Stellen Sie sicher, dass die Verschlüsselung für Ihre Amazon-DynamoDB-Tabellen aktiviert ist. Um eventuell vorhandene sensible Daten im Ruhezustand in diesen Tabellen zu schützen, müssen Sie die Verschlüsselung von Daten im Ruhezustand aktivieren. Standardmäßig werden DynamoDB-Tabellen mit einem AWS eigenen Kundenhauptschlüssel (CMK) verschlüsselt.
Anexo II 5.7.3	ec2- ebs-encryption-by-default	Zum Schutz von Daten im Ruhezustand müssen Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon Elastic Block Store (Amazon EBS)-Volumes aktiviert ist. Da sensible Daten auch im Ruhezusta nd vorhanden sein können, sollten Sie die Verschlüs selung im Ruhezustand aktivieren, um diese Daten zu schützen.

Kontroll-ID	AWS Config	Empfehlungen
Anexo II 5.7.3	elasticsearch-node-to-node-Verschlüsselungsprüfung	Stellen Sie sicher, dass die node-to-node Verschlüsselung für Amazon OpenSearch Service aktiviert ist. Node-to-nodeVerschlüsselung ermöglicht die TLS 1.2-Versc hlüsselung für die gesamte Kommunikation innerhalb der Amazon Virtual Private Cloud (Amazon VPC). Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.
Anexo II 5.7.3	elb-tls-https-listeners-nur	Stellen Sie sicher, dass Ihre Elastic Load Balancer (ELBs) mit SSL- oder HTTPS-Lis tenern konfiguriert sind. Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.
Anexo II 5.7.3	rds-snapshot-encrypted	Stellen Sie sicher, dass die Verschlüsselung für Ihre Amazon Relational Database Service (Amazon RDS)-Snap shots aktiviert ist. Da sensible Daten auch im Ruhezusta nd vorhanden sein können, sollten Sie die Verschlüs selung im Ruhezustand aktivieren, um diese Daten zu schützen.

Kontroll-ID	AWS Config	Empfehlungen
Anexo II 5.7.3	s-3 default-encryption-kms	Stellen Sie sicher, dass die Verschlüsselung für Ihre Amazon Simple Storage Service (Amazon S3)-Bucke ts aktiviert ist. Um eventuell vorhandene sensible Daten im Ruhezustand in einem Amazon-S3-Bucket zu schützen, muss die Verschlüs selung aktiviert sein.
Anexo II 5.7.3	sagemaker-notebook-instance -kms-key-konfiguriert	Um Daten im Ruhezusta nd zu schützen, stellen Sie sicher, dass die Verschlüs selung mit dem AWS Key Management Service (AWS KMS) für Ihr Notebook aktiviert ist. SageMaker Da vertrauli che Daten im SageMaker Notebook gespeichert werden können, sollten Sie die Verschlüsselung im Ruhezustand aktivieren, um diese Daten zu schützen.

Kontroll-ID	AWS Config	Empfehlungen
Anexo II 5.7.3	sns-encrypted-kms	Um Daten im Ruhezusta nd zu schützen, stellen Sie sicher, dass Ihre Amazon Simple Notification Service (Amazon SNS) -Themen mit dem AWS Key Management Service (AWS KMS) verschlüs selt werden müssen. Um eventuell vorhandene sensible Daten im Ruhezustand in veröffentlichten Nachricht en zu schützen, muss die Verschlüsselung von Daten im Ruhezustand aktiviert sein.
Anexo II 5.7.3	alb-http-to-https-Umleitung sprüfung	Um Daten während der Übertragung zu schützen, stellen Sie sicher, dass Ihr Application Load Balancer unverschlüsselte HTTP-Anfragen automatisch an HTTPS umleitet. Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	AWS Config	Empfehlungen
Anexo II 5.7.3	api-gw-cache-enabled-und-verschlüsselt	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass die Verschlüsselung für den Cache Ihrer API-Gateway-Stufe aktiviert ist. Da für die API-Methode sensible Daten erfasst werden können, sollten Sie die Verschlüsselung von Daten im Ruhezustand aktivieren, um diese Daten zu schützen.
Anexo II 5.7.3	api-gw-ssl-enabled	Stellen Sie sicher, dass die REST-API-Stufen von Amazon API Gateway mit SSL-Zertifikaten konfiguriert sind, damit Backend-Systeme überprüfen können, ob Anforderungen von API Gateway stammen.
Anexo II 5.7.3	cloud-trail-encryption-enabled	Da sensible Daten vorhanden sein können und um Daten im Speicher zu schützen, sollten Sie sicherstellen, dass die Verschlüsselung für Ihre AWS CloudTrail Trails aktiviert ist.
Anexo II 5.7.3	cloudwatch-log-group-encrypted	Um sensible Daten im Speicher zu schützen, stellen Sie sicher, dass die Verschlüsselung für Ihre Amazon CloudWatch Log Groups aktiviert ist.

Kontroll-ID	AWS Config	Empfehlungen
Anexo II 5.7.3	efs-encrypted-check	Aktivieren Sie die Verschlüs selung für Ihr Amazon Elastic File System (EFS), um eventuell vorhandene sensible Daten sowie Daten im Ruhezustand zu schützen.
Anexo II 5.7.3	elasticsearch-encrypted-at-rest	Da sensible Daten vorhanden sein können und um Daten im Ruhezustand zu schützen, sollten Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon OpenSearch Service (OpenSearch Service) -Domains aktiviert ist.
Anexo II 5.7.3	elb-acm-certificate-required	Zum Schutz von eventuell vorhandenen sensiblen Daten sowie von Daten während der Übertragung muss die Verschlüsselung für Ihr Elastic Load Balancing aktiviert sein. Verwenden Sie AWS Certifica te Manager, um öffentlic he und private SSL/TLS-Z ertifikate mit AWS Diensten und internen Ressourcen zu verwalten, bereitzustellen und bereitzustellen.

Kontroll-ID	AWS Config	Empfehlungen
Anexo II 5.7.3	encrypted-volumes	Aktivieren Sie die Verschlüs selung für Ihre Amazon-El astic-Block-Store (Amazon-EBS)-Volumes, um eventuell vorhandene sensible Daten sowie Daten im Ruhezustand zu schützen.
Anexo II 5.7.3	opensearch-encrypted-at-rest	Da sensible Daten vorhanden sein können und um Daten im Ruhezustand zu schützen, sollten Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon OpenSearch Service-Domains aktiviert ist.
Anexo II 5.7.3	opensearch-node-to-node-Ver schlüsselungsprüfung	Stellen Sie sicher, dass die node-to-node Verschlüsselung für Amazon OpenSearch Service aktiviert ist. Node-to-nodeVerschlüsselung ermöglicht die TLS 1.2-Versc hlüsselung für die gesamte Kommunikation innerhalb der Amazon Virtual Private Cloud (Amazon VPC). Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	AWS Config	Empfehlungen
Anexo II 5.7.3	rds-storage-encrypted	Zum Schutz von Daten im Ruhezustand müssen Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon Relational Database Service (Amazon RDS)-Instances aktiviert ist. Um eventuell vorhandene sensible Daten im Ruhezustand in Amazon-RDS-Instanc es zu schützen, muss die Verschlüsselung von Daten im Ruhezustand aktiviert sein.

Kontroll-ID	AWS Config	Empfehlungen
Anexo II 5.7.3	redshift-cluster-configuration-check	Um Daten im Ruhezustand zu schützen, muss die Verschlüsselung für Ihre Amazon-Redshift-Cluster aktiviert sein. Sie müssen auch sicherstellen, dass die erforderlichen Konfigurationen auf Amazon-Redshift-Clustern bereitgestellt werden. Die Prüfungsprotokollierung muss aktiviert sein, um Informationen zu Verbindungen und Benutzeraktivitäten in der Datenbank bereitzustellen. Diese Regel erfordert, dass ein Wert für clusterDbEncrypted (Config Default: TRUE) und LoggingEnabled (Config Default: TRUE) gesetzt ist. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	AWS Config	Empfehlungen
Anexo II 5.7.3	redshift-cluster-kms-enabled	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass die Verschlüsselung mit AWS Key Management Service (AWS KMS) für Ihren Amazon Redshift Redshift-Cluster aktiviert ist. Um eventuell vorhandene sensible Daten im Ruhezustand in Redshift-Clustern zu schützen, muss die Verschlüsselung von Daten im Ruhezustand aktiviert sein.
Anexo II 5.7.3	redshift-require-tls-ssl	Stellen Sie sicher, dass Ihre Amazon-Redshift-Cluster eine TLS/SSL-Verschlüsselung erfordern, um eine Verbindun g zu SQL-Clients herzustel len. Um eventuell vorhanden e sensible Daten zu schützen, sollten Sie die Verschlüs selung bei der Übertragung aktivieren.

Kontroll-ID	AWS Config	Empfehlungen
Anexo II 5.7.3	s3- aktiviert bucket-server-side -encryption	Zum Schutz von Daten im Ruhezustand müssen Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon Simple Storage Service (Amazon S3)-Bucke ts aktiviert ist. Um eventuell vorhandene sensible Daten im Ruhezustand in Amazon-S3 -Buckets zu schützen, muss die Verschlüsselung aktiviert sein.
Anexo II 5.7.3	s-3 bucket-ssl-requests-only	Um Daten während der Übertragung zu schützen, stellen Sie sicher, dass Ihre Amazon Simple Storage Service (Amazon S3)-Bucke ts Anfragen zur Verwendun g von Secure Socket Layer (SSL)-Buckets erfordern. Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	AWS Config	Empfehlungen
Anexo II 5.7.3	sagemaker-endpoint-configuration-kms-key-konfiguriert	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass die Verschlüsselung mit dem AWS Key Management Service (AWS KMS) für Ihren Endpunkt aktiviert ist. SageMaker Da sensible Daten auf dem SageMaker Endgerät gespeichert werden können, sollten Sie die Verschlüsselung im Ruhezustand aktivieren, um diese Daten zu schützen.
Anexo II 5.7.3	secretsmanager-using-cmk	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass die Verschlüsselung mit dem AWS Key Management Service (AWS KMS) für AWS Secrets Manager aktiviert ist. Aktivieren Sie die Verschlüsselung von Daten im Ruhezustand, um eventuell vorhandene sensible Daten im Ruhezustand im Secrets Manager zu schützen.
Anexo II 5.7.4	cmk-backing-key-rotation-aktiviert	Aktivieren Sie die Schlüssel rotation, um sicherzustellen, dass Schlüssel rotiert werden, nachdem sie das Ende ihrer Krypto-Periode erreicht haben.

Kontroll-ID	AWS Config	Empfehlungen
Anexo II 5.7.4	kms-cmk-not-scheduled-zum Löschen	Um Daten im Ruhezustand zu schützen, sollten Sie sicherstellen, dass die für den Kunden erforderlichen Masterschlüssel (CMKs) nicht für das Löschen im AWS Key Management Service (AWS KMS) vorgesehen sind. Da Schlüssel manchmal gelöscht werden müssen, können Sie mit dieser Regel alle zu löschenden Schlüssel überprüfen, falls ein Schlüssel versehentlich zur Löschung vorgemerkt wurde.
Anexo II 5.8.2	alb-waf-enabled	Stellen Sie sicher, dass AWS WAF auf Elastic Load Balancers (ELB) aktiviert ist, um Webanwendungen zu schützen. Eine WAF trägt zum Schutz Ihrer Webanwendungen oder APIs vor gängigen Web-Exploits bei. Diese Web-Exploits können sich auf die Verfügbarkeit auswirken, die Sicherheit gefährden oder übermäßige Ressourcen in Ihrer Umgebung verbrauchen.

Kontroll-ID	AWS Config	Empfehlungen
Anexo II 5.8.2	api-gw-associated-with-WAF	AWS Mit WAF können Sie eine Reihe von Regeln (als Web Access Control List (Web ACL) bezeichnet) konfiguri eren, die Webanfragen auf der Grundlage von anpassbar en Websicherheitsregeln und -bedingungen, die Sie definieren, zulassen, blockiere n oder zählen. Stellen Sie sicher, dass Ihre Amazon-API-Gateway-Stufe mit einer WAF-Web-ACL verknüpft ist, um sie vor böswilligen Angriffen zu schützen.
Anexo II 5.8.3.MEDIO.b)	alb-waf-enabled	Stellen Sie sicher, dass AWS WAF auf Elastic Load Balancers (ELB) aktiviert ist, um Webanwendungen zu schützen. Eine WAF trägt zum Schutz Ihrer Webanwend ungen oder APIs vor gängigen Web-Exploits bei. Diese Web-Exploits können sich auf die Verfügbarkeit auswirken, die Sicherheit gefährden oder übermäßige Ressourcen in Ihrer Umgebung verbrauchen.

Kontroll-ID	AWS Config	Empfehlungen
Anexo II 5.8.3.MEDIO.b)	api-gw-associated-with-WAF	AWS Mit WAF können Sie eine Reihe von Regeln (als Web Access Control List (Web ACL) bezeichnet) konfiguri eren, die Webanfragen auf der Grundlage von anpassbar en Websicherheitsregeln und -bedingungen, die Sie definieren, zulassen, blockiere n oder zählen. Stellen Sie sicher, dass Ihre Amazon-API-Gateway-Stufe mit einer WAF-Web-ACL verknüpft ist, um sie vor böswilligen Angriffen zu schützen.
Anexo II 5.8.3.MEDIO.b)	elb-cross-zone-load-Balancing aktiviert	Aktivieren Sie zonenüber greifendes Load Balancing für Ihre Elastic Load Balancer (ELBs), um eine angemesse ne Kapazität und Verfügbar keit aufrechtzuerhalten. Zonenübergreifendes Load Balancing reduziert die Notwendigkeit, die gleiche Anzahl von Instances in jeder aktivierten Availability Zone aufrechtzuerhalten. Es verbessert auch die Fähigkeit Ihrer Anwendung, den Verlust einer oder mehrerer Instances zu bewältigen.

Kontroll-ID	AWS Config	Empfehlungen
Anexo II 5.8.3.MEDIO.b)	rds-instance-deletion-protection-aktiviert	Stellen Sie sicher, dass Amazon Relational Database Service (Amazon RDS)-Instances den Löschschutz aktiviert haben. Verwenden Sie den Löschschutz, um zu verhindern, dass Ihre Amazon-RDS-Instances versehentlich oder böswillig gelöscht werden, was zum Verlust der Verfügbarkeit Ihrer Anwendungen führen kann.
Anexo II 5.8.3.MEDIO.b)	dynamodb-autoscaling-enabled	Amazon DynamoDB Auto Scaling verwendet den AWS Application Auto Scaling-Service, um die bereitgestellte Durchsatzkapazität so anzupassen, dass sie automatisch auf tatsächliche Verkehrsmuster reagiert. Auf diese Weise kann eine Tabelle oder ein globaler sekundärer Index die bereitgestellte Lese-/Schreibkapazität erhöhen, um plötzliche Erhöhungen des Datenverkehrs ohne Drosselung zu bewältigen.

Kontroll-ID	AWS Config	Empfehlungen
Anexo II 5.8.3.MEDIO.b)	elb-deletion-protection-enabled	Diese Regel sorgt dafür, dass der Löschschutz für Elastic Load Balancing aktiviert ist. Verwenden Sie diese Funktion, um zu verhindern, dass Ihr Load Balancer versehentlich oder böswillig gelöscht wird, was zum Verlust der Verfügbarkeit Ihrer Anwendungen führen kann.

Kontroll-ID	AWS Config	Empfehlungen
Anexo II 5.8.3.MEDIO.b)	rds-multi-az-support	Die Multi-AZ-Unterstützung in Amazon Relational Database Service (Amazon RDS) bietet eine verbesserte Verfügbar keit und Beständigkeit von Datenbank-Instances. Wenn Sie eine Multi-AZ-Datenbank-Instance bereitstellen, erstellt Amazon RDS automatisch eine primäre Datenbank-Instance und repliziert die Daten synchron auf eine Standby-Instance in einer anderen Availability Zone. Jede Availability Zone läuft auf einer eigenen, physisch getrennten, unabhängigen Infrastruktur und ist auf eine hohe Verfügbarkeit ausgelegt . Im Falle eines Infrastru kturausfalls führt Amazon RDS einen automatischen Failover zum Standby-Modus durch, sodass Sie den Datenbank betrieb wieder aufnehmen können, sobald der Failover abgeschlossen ist.

Kontroll-ID	AWS Config	Empfehlungen
Anexo II 5.8.3.MEDIO.b)	rds-cluster-multi-az-aktiviert	Die Multi-AZ-Unterstützung in Amazon Relational Database Service (Amazon RDS) bietet eine verbesserte Verfügbar keit und Beständigkeit von Datenbank-Instances. Wenn Sie eine Multi-AZ-Datenbank-Instance bereitstellen, erstellt Amazon RDS automatisch eine primäre Datenbank-Instance und repliziert die Daten synchron auf eine Standby-Instance in einer anderen Availability Zone. Jede Availability Zone läuft auf einer eigenen, physisch getrennten, unabhängigen Infrastruktur und ist auf eine hohe Verfügbarkeit ausgelegt . Im Falle eines Infrastru kturausfalls führt Amazon RDS einen automatischen Failover zum Standby-Modus durch, sodass Sie den Datenbank betrieb wieder aufnehmen können, sobald der Failover abgeschlossen ist.

Kontroll-ID	AWS Config	Empfehlungen
Anexo II 5.8.3.MEDIO.b)	vpc-vpn-2-tunnels-up	Redundante Site-to-Site VPN-Tunnel können implementiert werden, um die Anforderungen an die Ausfallsicherheit zu erfüllen. Es verwendet zwei Tunnel, um die Konnektivität sicherzustellen, falls eine der Site-to-Site VPN-Verbindungen nicht verfügbar ist. Um sich vor einem Verbindungsverlust zu schützen, können Sie für den Fall, dass Ihr Kunden-Gateway nicht verfügbar ist, eine zweite Site-to-Site VPN-Verbindung zu Ihrer Amazon Virtual Private Cloud (Amazon VPC) und Ihrem Virtual Private Gateway einrichten, indem Sie ein zweites Kunden-Gateway verwenden.

Kontroll-ID	AWS Config	Empfehlungen
Art. 14.4	iam-root-access-key-überprüfen	Der Zugriff auf Systeme und Ressourcen kann gesteuert werden, indem überprüft wird, ob der Root-Benutzer keine Zugriffsschlüssel mit seiner AWS Identity and Access Management (IAM) -Rolle verknüpft hat. Stellen Sie sicher, dass die Root-Zugriffsschlüssel gelöscht werden. Erstellen und verwenden Sie stattdessen rollenbasierte Funktionen, AWS-Konten um das Prinzip der geringsten Funktionalität zu berücksichtigen.
Art. 16	ecs-task-definition-user-for-host-mode-check	Wenn für eine Aufgabendefinition erhöhte Berechtigungen gelten, liegt das daran, dass der Kunde diesen Konfigurationen ausdrücklich zugestimmt hat. Diese Kontrolle prüft, ob eine unerwartete Berechtigungseskalation vorliegt, wenn für eine Aufgabendefinition das Host-Netzwerk aktiviert ist, die Kunden aber keine erhöhten Berechtigungen aktiviert haben.

Kontroll-ID	AWS Config	Empfehlungen
Art. 16	iam-policy-no-statements-with-full-access	Stellen Sie sicher, dass IAM-Aktionen nur auf die benötigte n Aktionen beschränkt sind. Wenn Benutzern mehr Rechte eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und der Aufgabentrennung verstoßen.
Art. 16	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) kann Ihnen dabei helfen, die Prinzipien der geringsten Rechte und der Aufgabent rennung in Zugriffsberechtigu ngen und Autorisierungen zu integrieren und so zu verhindern, dass Richtlinien „Effect“: „Allow“ mit „Action“: „*“ anstelle von „Resource“: „*“ enthalten. Wenn Benutzern mehr Rechte eingeräumt werden, als für die Ausführun g einer Aufgabe erforderl ich sind, kann dies gegen das Prinzip der geringste n Berechtigung und der Aufgabentrennung verstoßen.

Kontroll-ID	AWS Config	Empfehlungen
Art. 16	s3- bucket-policy-grantee-check	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie s3_bucket_policy_grantee_check aktivieren. Diese Regel prüft, ob der vom Amazon S3 S3-Bucket gewährte Zugriff durch die von Ihnen bereitgestellten AWS Principals, Verbundbenutzer, Service Principals, IP-Adressen oder Amazon Virtual Private Cloud (Amazon VPC) IDs eingeschränkt ist.
Art. 20.2	rds-automatic-minor-version-Upgrade-fähig	Aktivieren Sie automatische Unterversions-Upgrades auf Ihren Amazon-Relational-Database-Service (RDS)-Instances, um sicherzustellen, dass die aktuellen Updates für Unterversionen des Relational Database Management System (RDBMS) installiert sind, die Sicherheitspatches und Bugfixes enthalten können.

Kontroll-ID	AWS Config	Empfehlungen
Art. 20.2	ec2- prüfen managedinstance-patch-compliance-status	Aktivieren Sie diese Regel, um bei der Identifizierung und Dokumentation von Sicherheitslücken in Amazon Elastic Compute Cloud (Amazon EC2) zu helfen. Die Regel prüft, ob die EC2 Amazon-Instance die Patch-Konformität im AWS Systems Manager gemäß den Richtlinien und Verfahren Ihrer Organisation einhält.
Art. 20.2	elastic-beanstalk-managed-updates-aktiviert	Durch die Aktivierung verwalteter Plattformupdates für eine Amazon-Elastic-Beanstalk-Umgebung wird sichergestellt, dass die aktuellen verfügbaren Plattform-Fixes, -Updates und -Features für die Umgebung installiert sind. Eine bewährte Methode zur Sicherung von Systemen besteht darin, stets die aktuellen Patches zu installieren.

Kontroll-ID	AWS Config	Empfehlungen
Art. 20.2	vuln-management-plan-exists (Prozessüberprüfung)	Stellen Sie sicher, dass ein Plan für das Schwachst ellenmanagement entwickel t und implementiert wird, damit Sie über formell definiert e Prozesse zur Behebung von Schwachstellen in Ihrer Umgebung verfügen. Dazu zählen Tools für das Schwachstellenmanagement, regelmäßige Umgebungs scans sowie entsprechende Rollen und Verantwortlichkeit en.
Art. 21.1	dynamodb-table-encrypted-km s	Stellen Sie sicher, dass die Verschlüsselung für Ihre Amazon-DynamoDB-Tabellen aktiviert ist. Um eventuell vorhandene sensible Daten im Ruhezustand in diesen Tabellen zu schützen, müssen Sie die Verschlüsselung von Daten im Ruhezustand aktivieren. Standardmäßig werden DynamoDB-Tabellen mit einem AWS eigenen Kundenhauptschlüssel (CMK) verschlüsselt.

Kontroll-ID	AWS Config	Empfehlungen
Art. 21.1	ec2- ebs-encryption-by-default	Zum Schutz von Daten im Ruhezustand müssen Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon Elastic Block Store (Amazon EBS)-Volumes aktiviert ist. Da sensible Daten auch im Ruhezusta nd vorhanden sein können, sollten Sie die Verschlüs selung im Ruhezustand aktivieren, um diese Daten zu schützen.
Art. 21.1	elasticsearch-node-to-node-Verschlüsselungsprüfung	Stellen Sie sicher, dass die node-to-node Verschlüsselung für Amazon OpenSearch Service aktiviert ist. Node-to-nodeVerschlüsselung ermöglicht die TLS 1.2-Versc hlüsselung für die gesamte Kommunikation innerhalb der Amazon Virtual Private Cloud (Amazon VPC). Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	AWS Config	Empfehlungen
Art. 21.1	elb-cross-zone-load-Balancing aktiviert	Aktivieren Sie zonenüber greifendes Load Balancing für Ihre Elastic Load Balancer (ELBs), um eine angemesse ne Kapazität und Verfügbar keit aufrechtzuerhalten. Zonenübergreifendes Load Balancing reduziert die Notwendigkeit, die gleiche Anzahl von Instances in jeder aktivierten Availability Zone aufrechtzuerhalten. Es verbessert auch die Fähigkeit Ihrer Anwendung, den Verlust einer oder mehrerer Instances zu bewältigen.
Art. 21.1	elb-tls-https-listeners-nur	Stellen Sie sicher, dass Ihre Elastic Load Balancer (ELBs) mit SSL- oder HTTPS-Lis tenern konfiguriert sind. Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	AWS Config	Empfehlungen
Art. 21.1	rds-instance-deletion-protection-aktiviert	Stellen Sie sicher, dass Amazon Relational Database Service (Amazon RDS)-Instances den Löschschutz aktiviert haben. Verwenden Sie den Löschschutz, um zu verhindern, dass Ihre Amazon-RDS-Instances versehentlich oder böswillig gelöscht werden, was zum Verlust der Verfügbarkeit Ihrer Anwendungen führen kann.
Art. 21.1	rds-snapshot-encrypted	Stellen Sie sicher, dass die Verschlüsselung für Ihre Amazon Relational Database Service (Amazon RDS)-Snapshots aktiviert ist. Da sensible Daten auch im Ruhezustand vorhanden sein können, sollten Sie die Verschlüsselung im Ruhezustand aktivieren, um diese Daten zu schützen.
Art. 21.1	s3- bucket-default-lock-enabled	Stellen Sie sicher, dass für Ihren Amazon Simple Storage Service (Amazon S3)-Bucket standardmäßig eine Sperre aktiviert ist. Zum Schutz eventuell vorhandener sensibler Daten in S3-Buckets müssen Sie Objektsperren für Daten im Ruhezustand erzwingen.

Kontroll-ID	AWS Config	Empfehlungen
Art. 21.1	s-3 default-encryption-kms	Stellen Sie sicher, dass die Verschlüsselung für Ihre Amazon Simple Storage Service (Amazon S3)-Bucke ts aktiviert ist. Um eventuell vorhandene sensible Daten im Ruhezustand in einem Amazon-S3-Bucket zu schützen, muss die Verschlüs selung aktiviert sein.
Art. 21.1	sagemaker-notebook-instance -kms-key-konfiguriert	Um Daten im Ruhezusta nd zu schützen, stellen Sie sicher, dass die Verschlüs selung mit dem AWS Key Management Service (AWS KMS) für Ihr Notebook aktiviert ist. SageMaker Da vertrauli che Daten im SageMaker Notebook gespeichert werden können, sollten Sie die Verschlüsselung im Ruhezustand aktivieren, um diese Daten zu schützen.

Kontroll-ID	AWS Config	Empfehlungen
Art. 21.1	sns-encrypted-kms	Um Daten im Ruhezusta nd zu schützen, stellen Sie sicher, dass Ihre Amazon Simple Notification Service (Amazon SNS) -Themen mit dem AWS Key Management Service (AWS KMS) verschlüs selt werden müssen. Um eventuell vorhandene sensible Daten im Ruhezustand in veröffentlichten Nachricht en zu schützen, muss die Verschlüsselung von Daten im Ruhezustand aktiviert sein.
Art. 21.1	alb-http-to-https-Umleitung sprüfung	Um Daten während der Übertragung zu schützen, stellen Sie sicher, dass Ihr Application Load Balancer unverschlüsselte HTTP-Anfragen automatisch an HTTPS umleitet. Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	AWS Config	Empfehlungen
Art. 21.1	api-gw-cache-enabled-und-verschlüsselt	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass die Verschlüsselung für den Cache Ihrer API-Gateway-Stufe aktiviert ist. Da für die API-Methode sensible Daten erfasst werden können, sollten Sie die Verschlüsselung von Daten im Ruhezustand aktivieren, um diese Daten zu schützen.
Art. 21.1	api-gw-ssl-enabled	Stellen Sie sicher, dass die REST-API-Stufen von Amazon API Gateway mit SSL-Zertifikaten konfiguriert sind, damit Backend-Systeme überprüfen können, ob Anforderungen von API Gateway stammen.
Art. 21.1	cloud-trail-encryption-enabled	Da sensible Daten vorhanden sein können und um Daten im Speicher zu schützen, sollten Sie sicherstellen, dass die Verschlüsselung für Ihre AWS CloudTrail Trails aktiviert ist.

Kontroll-ID	AWS Config	Empfehlungen
Art. 21.1	cloud-trail-log-file-Validierung aktiviert	Verwenden Sie die AWS CloudTrail Protokolldateivalidierung, um die Integrität von Protokollen zu überprüfen. CloudTrail Mithilfe der Protokolldateivalidierung kann festgestellt werden, ob eine Protokolldatei geändert oder gelöscht wurde oder ob sie nach der Übermittlung CloudTrail unverändert geblieben ist. Dieses Feature wurde mit dem Branchenstandard entsprechenden Algorithmen entwickelt: SHA-256 für die Hashfunktion und SHA-256 mit RSA für digitale Signaturen. Aus diesem Grund ist es rechnerisch unmöglich, CloudTrail Protokolldateien unbemerkt zu ändern, zu löschen oder zu fälschen.
Art. 21.1	cloudwatch-log-group-encrypted	Um sensible Daten im Speicher zu schützen, stellen Sie sicher, dass die Verschlüsselung für Ihre Amazon CloudWatch Log Groups aktiviert ist.

Kontroll-ID	AWS Config	Empfehlungen
Art. 21.1	dynamodb-autoscaling-enabled	Amazon DynamoDB Auto Scaling verwendet den AWS Application Auto Scaling-Service, um die bereitgestellte Durchsatzkapazität so anzupassen, dass sie automatisch auf tatsächliche Verkehrsmuster reagiert. Auf diese Weise kann eine Tabelle oder ein globaler sekundärer Index die bereitgestellte Lese-/Schreibkapazität erhöhen, um plötzliche Erhöhungen des Datenverkehrs ohne Drosselung zu bewältigen.
Art. 21.1	efs-encrypted-check	Aktivieren Sie die Verschlüsselung für Ihr Amazon Elastic File System (EFS), um eventuell vorhandene sensible Daten sowie Daten im Ruhezustand zu schützen.
Art. 21.1	elasticsearch-encrypted-at-rest	Da sensible Daten vorhanden sein können und um Daten im Ruhezustand zu schützen, sollten Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon OpenSearch Service (OpenSearch Service) -Domains aktiviert ist.

Kontroll-ID	AWS Config	Empfehlungen
Art. 21.1	elb-acm-certificate-required	Zum Schutz von eventuell vorhandenen sensiblen Daten sowie von Daten während der Übertragung muss die Verschlüsselung für Ihr Elastic Load Balancing aktiviert sein. Verwenden Sie AWS Certifica te Manager, um öffentlic he und private SSL/TLS-Z ertifikate mit AWS Diensten und internen Ressourcen zu verwalten, bereitzustellen und bereitzustellen.
Art. 21.1	elb-deletion-protection-ena bled	Diese Regel sorgt dafür, dass der Löschschutz für Elastic Load Balancing aktiviert ist. Verwenden Sie diese Funktion, um zu verhinder n, dass Ihr Load Balancer versehentlich oder böswillig gelöscht wird, was zum Verlust der Verfügbarkeit Ihrer Anwendungen führen kann.
Art. 21.1	encrypted-volumes	Aktivieren Sie die Verschlüs selung für Ihre Amazon-El astic-Block-Store (Amazon-EBS)-Volumes, um eventuell vorhandene sensible Daten sowie Daten im Ruhezustand zu schützen.

Kontroll-ID	AWS Config	Empfehlungen
Art. 21.1	opensearch-encrypted-at-rest	Da sensible Daten vorhanden sein können und um Daten im Ruhezustand zu schützen, sollten Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon OpenSearch Service-Domains aktiviert ist.
Art. 21.1	opensearch-node-to-node-Verschlüsselungsprüfung	Stellen Sie sicher, dass die node-to-node Verschlüsselung für Amazon OpenSearch Service aktiviert ist. Node-to-nodeVerschlüsselung ermöglicht die TLS 1.2-Verschlüsselung für die gesamte Kommunikation innerhalb der Amazon Virtual Private Cloud (Amazon VPC). Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	AWS Config	Empfehlungen
Art. 21.1	rds-multi-az-support	Die Multi-AZ-Unterstützung in Amazon Relational Database Service (Amazon RDS) bietet eine verbesserte Verfügbar keit und Beständigkeit von Datenbank-Instances. Wenn Sie eine Multi-AZ-Datenbank-Instance bereitstellen, erstellt Amazon RDS automatisch eine primäre Datenbank-Instance und repliziert die Daten synchron auf eine Standby-Instance in einer anderen Availability Zone. Jede Availability Zone läuft auf einer eigenen, physisch getrennten, unabhängigen Infrastruktur und ist auf eine hohe Verfügbarkeit ausgelegt . Im Falle eines Infrastru kturausfalls führt Amazon RDS einen automatischen Failover zum Standby-Modus durch, sodass Sie den Datenbank betrieb wieder aufnehmen können, sobald der Failover abgeschlossen ist.

Kontroll-ID	AWS Config	Empfehlungen
Art. 21.1	rds-cluster-multi-az-aktiviert	Die Multi-AZ-Unterstützung in Amazon Relational Database Service (Amazon RDS) bietet eine verbesserte Verfügbar keit und Beständigkeit von Datenbank-Instances. Wenn Sie eine Multi-AZ-Datenbank-Instance bereitstellen, erstellt Amazon RDS automatisch eine primäre Datenbank-Instance und repliziert die Daten synchron auf eine Standby-Instance in einer anderen Availability Zone. Jede Availability Zone läuft auf einer eigenen, physisch getrennten, unabhängigen Infrastruktur und ist auf eine hohe Verfügbarkeit ausgelegt . Im Falle eines Infrastru kturausfalls führt Amazon RDS einen automatischen Failover zum Standby-Modus durch, sodass Sie den Datenbank betrieb wieder aufnehmen können, sobald der Failover abgeschlossen ist.

Kontroll-ID	AWS Config	Empfehlungen
Art. 21.1	rds-storage-encrypted	Zum Schutz von Daten im Ruhezustand müssen Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon Relational Database Service (Amazon RDS)-Instances aktiviert ist. Um eventuell vorhandene sensible Daten im Ruhezustand in Amazon-RDS-Instanc es zu schützen, muss die Verschlüsselung von Daten im Ruhezustand aktiviert sein.

Kontroll-ID	AWS Config	Empfehlungen
Art. 21.1	redshift-cluster-configuration-check	Um Daten im Ruhezustand zu schützen, muss die Verschlüsselung für Ihre Amazon-Redshift-Cluster aktiviert sein. Sie müssen auch sicherstellen, dass die erforderlichen Konfigurationen auf Amazon-Redshift-Clustern bereitgestellt werden. Die Prüfungsprotokollierung muss aktiviert sein, um Informationen zu Verbindungen und Benutzeraktivitäten in der Datenbank bereitzustellen. Diese Regel erfordert, dass ein Wert für clusterDbEncrypted (Config Default: TRUE) und LoggingEnabled (Config Default: TRUE) gesetzt ist. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	AWS Config	Empfehlungen
Art. 21.1	redshift-cluster-kms-enabled	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass die Verschlüsselung mit AWS Key Management Service (AWS KMS) für Ihren Amazon Redshift Redshift-Cluster aktiviert ist. Um eventuell vorhandene sensible Daten im Ruhezustand in Redshift-Clustern zu schützen, muss die Verschlüsselung von Daten im Ruhezustand aktiviert sein.
Art. 21.1	redshift-require-tls-ssl	Stellen Sie sicher, dass Ihre Amazon-Redshift-Cluster eine TLS/SSL-Verschlüsselung erfordern, um eine Verbindun g zu SQL-Clients herzustel len. Um eventuell vorhanden e sensible Daten zu schützen, sollten Sie die Verschlüs selung bei der Übertragung aktivieren.

Kontroll-ID	AWS Config	Empfehlungen
Art. 21.1	s3- aktiviert bucket-server-side-encryption	Zum Schutz von Daten im Ruhezustand müssen Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon Simple Storage Service (Amazon S3)-Buckets aktiviert ist. Um eventuell vorhandene sensible Daten im Ruhezustand in Amazon-S3-Buckets zu schützen, muss die Verschlüsselung aktiviert sein.
Art. 21.1	s-3 bucket-ssl-requests-only	Um Daten während der Übertragung zu schützen, stellen Sie sicher, dass Ihre Amazon Simple Storage Service (Amazon S3)-Buckets Anfragen zur Verwendung von Secure Socket Layer (SSL)-Buckets erfordern. Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	AWS Config	Empfehlungen
Art. 21.1	sagemaker-endpoint-configuration-kms-key-konfiguriert	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass die Verschlüsselung mit dem AWS Key Management Service (AWS KMS) für Ihren Endpunkt aktiviert ist. SageMaker Da sensible Daten auf dem SageMaker Endgerät gespeichert werden können, sollten Sie die Verschlüsselung im Ruhezustand aktivieren, um diese Daten zu schützen.
Art. 21.1	secretsmanager-using-cmk	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass die Verschlüsselung mit dem AWS Key Management Service (AWS KMS) für AWS Secrets Manager aktiviert ist. Aktivieren Sie die Verschlüsselung von Daten im Ruhezustand, um eventuell vorhandene sensible Daten im Ruhezustand im Secrets Manager zu schützen.

Kontroll-ID	AWS Config	Empfehlungen
Art. 21.1	vpc-vpn-2-tunnels-up	Redundante Site-to-Site VPN-Tunnel können implement iert werden, um die Anforderu ngen an die Ausfallsicherheit zu erfüllen. Es verwendet zwei Tunnel, um die Konnektiv ität sicherzustellen, falls eine der Site-to-Site VPN-Verbi ndungen nicht verfügbar ist. Um sich vor einem Verbindun gsverlust zu schützen, können Sie für den Fall, dass Ihr Kunden-Gateway nicht verfügbar ist, eine zweite Site-to-Site VPN-Verbindung zu Ihrer Amazon Virtual Private Cloud (Amazon VPC) und Ihrem Virtual Private Gateway einrichten, indem Sie ein zweites Kunden-Gateway verwenden.
Art. 22	autoscaling-launch-config-p ublic-ip ist deaktiviert	Wenn Sie Ihre Netzwerks chnittstellen mit einer öffentlic hen IP-Adresse konfigurieren, sind die diesen Netzwerks chnittstellen zugehörigen Ressourcen über das Internet erreichbar. EC2 Ressource n sollten nicht öffentlich zugänglich sein, da dies einen unbeabsichtigten Zugriff auf Ihre Anwendungen oder Server ermöglichen kann.

Kontroll-ID	AWS Config	Empfehlungen
Art. 22	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) Security Groups können bei der Verwaltung des Netzwerkz ugriffs helfen, indem sie eine statusbehaftete Filterung des ein- und ausgehend en Netzwerkverkehrs zu Ressourcen bereitstellen. AWS Wenn Sie eingehenden (oder entfernten) Datenverk ehr von 0.0.0.0/0 bis Port 22 auf Ihren Ressourcen nicht zulassen, können Sie den Remote-Zugriff einschränken.

Kontroll-ID	AWS Config	Empfehlungen
Art. 22	s3-Blöcke, periodisch account-level-public-access	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Simple Storage Service (Amazon S3) -Buckets nicht öffentlich zugänglich sind. Diese Regel trägt dazu bei, sensible Daten vor unbefugten Remote-Benutzern zu schützen, indem sie den öffentlichen Zugriff verhindert. Mit dieser Regel können Sie optional die Parameter ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) und restrictPublicBuckets Parameter (Config Default: True) festlegen. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	AWS Config	Empfehlungen
Art. 22	ssm-document-not-public	Stellen Sie sicher, dass AWS Systems Manager (SSM) - Dokumente nicht öffentlich sind, da dies einen unbeabsichtigten Zugriff auf Ihre SSM-Dokumente ermöglichen kann. Ein öffentliches SSM-Dokument kann Informationen über Ihr Konto, Ihre Ressourcen und internen Prozesse preisgeben.
Art. 22	dms-replication-not-public	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass auf DMS-Replikationsinstanzen nicht öffentlich zugegriffen werden kann. DMS-Replikations-Instances können vertrauliche Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.
Art. 22	ebs-snapshot-public-restorable-überprüfen	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass EBS-Snapshots nicht öffentlich wiederherstellbar sind. EBS-Volume-Snapshots können vertrauliche Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	AWS Config	Empfehlungen
Art. 22	ec-2 instance-no-public-ip	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon Elastic Compute Cloud (Amazon EC2) -Instances nicht öffentlich zugänglich sind. EC2 Amazon-Instances können vertrauliche Informati onen enthalten, und für solche Konten ist eine Zugriffsk ontrolle erforderlich.
Art. 22	elasticsearch-in-vpc-only	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass sich Amazon OpenSearch OpenSearch Service (Service) -Domains innerhalb einer Amazon Virtual Private Cloud (Amazon VPC) befinden. Eine OpenSearch Service-D omain innerhalb einer Amazon VPC ermöglicht die sichere Kommunikation zwischen OpenSearch Service und anderen Services innerhalb der Amazon VPC, ohne dass ein Internet-Gateway, ein NAT-Gerät oder eine VPN-Verbindung erforderlich ist.

Kontroll-ID	AWS Config	Empfehlungen
Art. 22	emr-master-no-public-ip	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon EMR-Cluster-Masterknoten nicht öffentlich zugänglich sind. Amazon-EMR-Cluster-Hauptknoten können vertrauliche Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.
Art. 22	internet-gateway-authorized-vpc-nur	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Internet-Gateways nur mit autorisierter Amazon Virtual Private Cloud (Amazon VPC) verbunden sind. Internet-Gateways ermöglichen den bidirektionalen Internetzugang zur und von der Amazon VPC, was möglicherweise zu einem unbefugten Zugriff auf Amazon-VPC-Ressourcen führen kann.

Kontroll-ID	AWS Config	Empfehlungen
Art. 22	lambda-function-public-access-verboten	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass AWS Lambda-Funktionen nicht öffentlich zugänglich sind. Der öffentliche Zugriff kann möglicherweise die Verfügbarkeit von Ressourcen beeinträchtigen.

Kontroll-ID	AWS Config	Empfehlungen
Art. 22	lambda-inside-vpc	Stellen Sie AWS Lambda-Funktionen in einer Amazon Virtual Private Cloud (Amazon VPC) bereit, um eine sichere Kommunikation zwischen einer Funktion und anderen Diensten innerhalb der Amazon VPC zu gewährleisten. Bei dieser Konfiguration sind kein Internet-Gateway, kein NAT-Gerät und keine VPN-Verbindung erforderlich. Der gesamte Datenverkehr bleibt sicher in der Cloud. AWS Domains, die sich innerhalb einer VPC befinden, verfügen aufgrund ihrer logischen Isolierung im Vergleich zu Domains mit öffentlichen Endpunkten über eine zusätzliche Sicherheitsebene. Um den Zugriff ordnungsgemäß zu verwalten, sollten AWS Lambda-Funktionen einer VPC zugewiesen werden.

Kontroll-ID	AWS Config	Empfehlungen
Art. 22	opensearch-in-vpc-only	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass sich Amazon OpenSearch Service-Domains innerhalb einer Amazon Virtual Private Cloud (Amazon VPC) befinden. Eine Amazon OpenSearch Service-Domain innerhalb einer Amazon VPC ermöglich t die sichere Kommunika tion zwischen Amazon OpenSearch Service und anderen Services innerhalb der Amazon VPC, ohne dass ein Internet-Gateway, ein NAT-Gerät oder eine VPN-Verbindung erforderlich ist.
Art. 22	rds-instance-public-access-überprüfen	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherste llen, dass Amazon Relationa l Database Service (Amazon RDS) -Instances nicht öffentlic h sind. Amazon-RDS-Datenba nk-Instances können vertrauli che Informationen enthalten und für solche Konten sind Prinzipien und Zugriffsk ontrollen erforderlich.

Kontroll-ID	AWS Config	Empfehlungen
Art. 22	rds-snapshots-public-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Relational Database Service (Amazon RDS) -Instances nicht öffentlich sind. Amazon-RDS-Datenbank-Instances können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.
Art. 22	redshift-cluster-public-access-überprüfen	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Redshift Redshift-Cluster nicht öffentlich sind. Amazon-Redshift-Cluster können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	AWS Config	Empfehlungen
Art. 22	restricted-common-ports	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass gemeinsame Ports für Amazon Elastic Compute Cloud (Amazon EC2) - Sicherheitsgruppen eingeschränkt sind. Wenn der Zugriff auf Ports nicht auf vertrauenswürdige Quellen beschränkt wird, kann dies zu Angriffen auf die Verfügbarkeit, Integrität und Vertraulichkeit von Systemen führen. Mit dieser Regel können Sie optional die Parameter blockedPort1–blockedPort5 festlegen (Standardkonfigurationen: 20, 21, 3389, 3306, 4333). Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	AWS Config	Empfehlungen
Art. 22	s3 bucket-level-public-access -verboten	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Simple Storage Service (Amazon S3) -Buckets nicht öffentlich zugänglich sind. Diese Regel trägt dazu bei, sensible Daten vor unbefugten Remote-Benutzern zu schützen, indem sie den öffentlichen Zugriff auf Bucket-Ebene verhindert.
Art. 22	s3- bucket-public-read-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie nur autorisierten Benutzern, Prozessen und Geräten Zugriff auf Amazon Simple Storage Service (Amazon S3) -Buckets gewähren. Die Verwaltung des Zugriffs sollte mit der Klassifizierung der Daten übereinstimmen.

Kontroll-ID	AWS Config	Empfehlungen
Art. 22	s3- bucket-public-write-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie nur autorisierten Benutzern, Prozessen und Geräten Zugriff auf Amazon Simple Storage Service (Amazon S3) -Buckets gewähren. Die Verwaltung des Zugriffs sollte mit der Klassifizierung der Daten übereinstimmen.
Art. 22	sagemaker-notebook-no-direct-Internetzugang	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass SageMaker Amazon-Notebooks keinen direkten Internetzugang zulassen. Indem Sie direkten Internetzugang blockieren, vermeiden Sie, dass unbefugte Benutzer auf sensible Daten zugreifen.

Kontroll-ID	AWS Config	Empfehlungen
Art. 22	subnet-auto-assign-public-ip-deaktiviert	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon Virtual Private Cloud (VPC) -Subnetzen nicht automatis ch eine öffentliche IP-Adress e zugewiesen wird. Amazon Elastic Compute Cloud (EC2) -Instances, die in Subnetzen gestartet werden, in denen dieses Attribut aktiviert ist, haben ihrer primären Netzwerkschnittste lle eine öffentliche IP-Adresse zugewiesen.
Art. 22	vpc-default-security-group-geschlossen	Sicherheitsgruppen von Amazon Elastic Compute Cloud (Amazon EC2) können bei der Verwaltung des Netzwerkzugriffs helfen, indem sie eine statusbeh aftete Filterung des ein- und ausgehenden Netzwerkv erkehrs zu Ressourcen bereitstellen. AWS Die Beschränkung des gesamten Datenverkehrs auf die Standardsicherheitsgruppe hilft dabei, den Fernzugriff auf Ihre Ressourcen einzuschr änken. AWS

Kontroll-ID	AWS Config	Empfehlungen
Art. 22	vpc-sg-open-only-to-authorized-ports	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass gemeinsame Ports für Amazon Elastic Compute Cloud (Amazon EC2) - Sicherheitsgruppen eingeschränkt sind. Wenn der Zugriff auf Ports nicht auf vertrauenswürdige Quellen beschränkt wird, kann dies zu Angriffen auf die Verfügbarkeit, Integrität und Vertraulichkeit von Systemen führen. Durch die Beschränkung des Zugriffs auf Ressourcen innerhalb einer Sicherheitsgruppe aus dem Internet (0.0.0.0/0) kann der Remote-Zugriff auf interne Systeme gesteuert werden.
Art. 23	elasticsearch-logs-to-cloudwatch	Stellen Sie sicher, dass für Amazon OpenSearch Service-Domains Fehlerprotokolle aktiviert und zur Aufbewahrung und Beantwortung an Amazon CloudWatch Logs gestreamt werden. Domain-Fehlerprotokolle sind bei Sicherheits- und Zugriffsprüfungen sowie bei der Diagnose von Verfügbarkeitsproblemen nützlich.

Kontroll-ID	AWS Config	Empfehlungen
Art. 23	multi-region-cloudtrail-enabled	AWS CloudTrail zeichnet Aktionen und API-Aufrufe der AWS Management Console auf. Sie können feststellen, welche Benutzer und Konten angerufen wurden AWS, von welcher Quell-IP-Adresse aus die Anrufe getätigt wurden und wann die Anrufe erfolgten . CloudTrail übermittelt Protokolldateien aus allen AWS Regionen an Ihren S3-Bucket, wenn MULTI_REGION_CLOUD_TRAIL_ENABLED aktiviert ist. Außerdem wird beim AWS Start einer neuen Region derselbe Trail in der neuen Region erstellt. CloudTrail Dadurch erhalten Sie automatisch Protokoll dateien mit API-Aktivitäten für die neue Region.

Kontroll-ID	AWS Config	Empfehlungen
Art. 23	rds-logging-enabled	Um die Protokollierung und Überwachung in Ihrer Umgebung zu erleichtern, stellen Sie sicher, dass die Amazon Relational Database Service (Amazon RDS)-Protokollierung aktiviert ist. Mit der Amazon-RDS-Protokollierung können Sie Ereignisse wie Verbindungen, Verbindungsabbrüche, Abfragen oder abgefragte Tabellen erfassen.
Art. 23	wafv2-logging-enabled	Um die Protokollierung und Überwachung in Ihrer Umgebung zu erleichtern, aktivieren Sie die AWS WAF (V2) -Protokollierung im regionalen und globalen Web ACLs. AWS Die WAF-Protokollierung bietet detaillierte Informationen über den Datenverkehr, der von Ihrer Web-ACL analysiert wird. In den Protokollen werden die Uhrzeit aufgezeichnet, zu der die AWS WAF die Anfrage von Ihrer AWS Ressource erhalten hat, Informationen über die Anfrage und eine Aktion für die Regel, der jede Anfrage entsprach.

Kontroll-ID	AWS Config	Empfehlungen
Art. 23	api-gw-execution-logging-aktiviert	Die API-Gateway-Protokollierung zeigt detaillierte Ansichten der Benutzer, die auf die API zugegriffen haben, und wie diese Benutzer auf die API zugegriffen haben. Diese Einblicke ermöglichen die Transparenz von Benutzeraktivitäten.
Art. 23	cloud-trail-cloud-watch-logs-aktiviert	Verwenden Sie Amazon CloudWatch , um Protokollereignisaktivitäten zentral zu sammeln und zu verwalten . Die Aufnahme von AWS CloudTrail Daten liefert Einzelheiten zu den API-Aufrufaktivitäten in Ihrem AWS-Konto.

Kontroll-ID	AWS Config	Empfehlungen
Art. 23	cloudtrail-enabled	AWS CloudTrail kann bei der Nichtabstreitbarkeit helfen, indem Aktionen und API-Aufrufe der AWS Managemen t Console aufgezeichnet werden. Sie können die Benutzer und die Benutzer AWS-Konten , die einen AWS Dienst aufgerufen haben, die Quell-IP-Adresse, über die die Aufrufe generiert wurden, und den Zeitpunkt der Anrufe identifizieren. Einzelheiten zu den erfassten Daten finden Sie in den AWS CloudTrail Datensatzinhalten.
Art. 23	cloudtrail-s3-dataevents-en abled	Die Erfassung von Simple Storage Service (Amazon S3)-Datenereignissen unterstützt die Erkennung von ungewöhnl ichen Aktivitäten. Zu den Details gehören AWS-Konto Informationen über den Zugriff auf einen Amazon S3 S3-Bucket, die IP-Adresse und die Uhrzeit des Ereignisses.

Kontroll-ID	AWS Config	Empfehlungen
Art. 23	elb-logging-enabled	Die Elastic-Load-Balancing-Aktivität ist ein zentraler Kommunikationspunkt innerhalb einer Umgebung. Stellen Sie sicher, dass die ELB-Protokollierung aktiviert ist. Die gesammelten Daten enthalten detaillierte Informationen zu Anfragen, die an den ELB gesendet wurden. Jedes Protokoll enthält Informationen wie die Zeit, zu der die Anforderung einging, die Client-IP-Adresse, Latenzen, Anforderungspfade und Serverantworten.
Art. 23	opensearch-logs-to-cloudwatch	Stellen Sie sicher, dass für Amazon OpenSearch Service-Domains Fehlerprotokolle aktiviert und zur Aufbewahrung und Beantwortung an Amazon CloudWatch Logs gestreamt werden. OpenSearch Service-Fehlerprotokolle können bei Sicherheits- und Zugriffsprüfungen helfen und bei der Diagnose von Verfügbarkeitsproblemen helfen.

Kontroll-ID	AWS Config	Empfehlungen
Art. 23	s-3 bucket-logging-enabled	Die Amazon Simple Storage Service (Amazon S3)-Serverzugriffsprotokollierung bietet eine Methode zur Überwachung des Netzwerks im Hinblick auf potenzielle Cybersicherheitsereignisse. Die Ereignisse werden überwacht, indem detaillierte Aufzeichnungen über die Anfragen erfasst werden, die an einen Amazon-S3-Bucket gestellt wurden. Jeder Zugriffsprotokolleintrag enthält Details zu einer einzelnen Zugriffsanfrage. Zu den Details gehören Anforderer, Bucket-Name, Anforderungszeit, Anforderungsaktion, Antwortstatus und Fehlercode, falls relevant.

Kontroll-ID	AWS Config	Empfehlungen
Art. 23	vpc-flow-logs-enabled	VPC-Flow-Protokolle erfassen detaillierte Informationsdatensätze über den IP-Datenverkehr, der zu und von Netzwerkschnittstellen in Ihrer Amazon Virtual Private Cloud (Amazon VPC) fließt. Standardmäßig enthalten Flow-Protokolldatensätze Werte für die verschiedenen Komponenten des IP-Flows, einschließlich Quelle, Ziel und Protokoll.
Artikel 24.2	response-plan-exists-maintained (Prozessüberprüfung)	Stellen Sie sicher, dass Vorfallreaktionspläne erstellt, verwaltet und an das verantwortliche Personal verteilt werden. Aktualisierte und formal dokumentierte Reaktionspläne können dazu beitragen, dass das zuständige Personal die Rollen, Verantwortlichkeiten und Prozesse versteht, die bei einem Vorfall einzuhalten sind.

Kontroll-ID	AWS Config	Empfehlungen
Artikel 24.1	guardduty-enabled-centralized	Amazon GuardDuty kann mithilfe von Threat Intellige nce Feeds helfen, potenzielle Cybersicherheitsereignisse zu überwachen und zu erkennen. Dazu gehören Listen mit bösartigen IPs und maschinel len Lernmethoden zur Identifiz ierung unerwarteter, nicht autorisierter und bösartige r Aktivitäten in Ihrer AWS Cloud-Umgebung.
Art. 25	dynamodb-in-backup-plan	Um Sie bei Datensich erungsprozessen zu unterstüt zen, stellen Sie sicher, dass Ihre Amazon DynamoDB-Tabellen Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherung smanagement und erleichte rt Ihnen die Erfüllung von geschäftlichen und behördlic hen Compliance-Anforde rungen hinsichtlich Datensich erungen.

Kontroll-ID	AWS Config	Empfehlungen
Art. 25	ebs-in-backup-plan	Stellen Sie zur Unterstützung der Datensicherungsprozesse sicher, dass Ihre Amazon Elastic Block Store (Amazon EBS) -Volumes Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherung smanagement und erleichte rt Ihnen die Erfüllung von geschäftlichen und behördlic hen Compliance-Anforde rungen hinsichtlich Datensich erungen.

Kontroll-ID	AWS Config	Empfehlungen
Art. 25	efs-in-backup-plan	Um Sie bei Datensich erungsprozessen zu unterstüt zen, stellen Sie sicher, dass Ihre Amazon Elastic File System (Amazon EFS) - Dateisysteme Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherung smanagement und erleichte rt Ihnen die Erfüllung von geschäftlichen und behördlic hen Compliance-Anforde rungen hinsichtlich Datensich erungen.

Kontroll-ID	AWS Config	Empfehlungen
Art. 25	rds-in-backup-plan	Um Sie bei Datensich erungsprozessen zu unterstüt zen, stellen Sie sicher, dass Ihre Amazon Relational Database Service (Amazon RDS) -Instances Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherung smanagement und erleichte rt Ihnen die Erfüllung von geschäftlichen und behördlic hen Compliance-Anforde rungen hinsichtlich Datensich erungen.

Kontroll-ID	AWS Config	Empfehlungen
Art. 25	redshift-backup-enabled	Stellen Sie zur Unterstützung der Datensicherungsprozesse sicher, dass Ihre Amazon-Redshift-Cluster über automatisierte Snapshots verfügen. Wenn automatisierte Snapshots für einen Cluster aktiviert sind, erstellt Redshift in regelmäßigen Abständen Snapshots dieses Clusters. Standardmäßig erstellt Redshift alle acht Stunden oder alle 5 GB einen Snapshot für jeden Knoten mit Datenänderungen oder je nachdem, was zuerst eintritt.
Art. 25	db-instance-backup-enabled	Die Sicherungsfunktion von Amazon RDS erstellt Sicherungen Ihrer Datenbanken und Transaktionsprotokolle. Amazon RDS erstellt einen Snapshot für das Speichervolume Ihrer DB-Instance, sodass die gesamte DB-Instance gesichert wird. Sie können im System spezifische Aufbewahrungsfristen festlegen, um Ihre Ausfallsicherheitsanforderungen zu erfüllen.

Kontroll-ID	AWS Config	Empfehlungen
Art. 25	dynamodb-pitr-enabled	Aktivieren Sie diese Regel, um zu überprüfen, ob die Informationen gesichert wurden. Es verwaltet auch die Backups, indem es sicherste llt, dass die point-in-time Wiederherstellung in Amazon DynamoDB aktiviert ist. Bei der Wiederherstellung werden fortlaufende Backups Ihrer Tabelle für die letzten 35 Tage gespeichert.
Art. 25	ebs-optimized-instance	Eine optimierte Instance im Amazon Elastic Block Store (Amazon EBS) bietet zusätzlic he, dedizierte Kapazität für Amazon-EBS-I/O-Vorgänge. Diese Optimierung bietet die beste Leistung für Ihr EBS-Volume, indem Konflikte zwischen Amazon-EBS-I/O und anderem Datenverkehr von Ihrer Instance minimiert werden.

Kontroll-ID	AWS Config	Empfehlungen
Art. 25	elasticache-redis-cluster-automatic-Backup-Prüfung	Wenn automatische Backups aktiviert sind, ElastiCache erstellt Amazon täglich ein Backup des Clusters. Die Sicherung kann für eine von Ihrer Organisation festgelegte Anzahl von Tagen aufbewahrt werden. Automatische Backups schützen vor Datenverlust. Bei einem Ausfall können Sie einen neuen Cluster erstellen, der Ihre Daten aus dem aktuellen Backup wiederherstellt.
Art. 25	s-3 bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) unterstützt die Aufrechterhaltung einer angemessenen Kapazität und Verfügbarkeit. CRR ermöglicht das automatische, asynchrone Kopieren von Objekten in Amazon-S3-Buckets, um die Datenverfügbarkeit sicherzustellen.

Kontroll-ID	AWS Config	Empfehlungen
Art. 25	s-3 bucket-versioning-enabled	Die Versionsverwaltung von Amazon Simple Storage Service (Amazon S3)-Buckets hilft dabei, mehrere Varianten eines Objekts im selben Amazon-S3-Bucket zu speichern. Verwenden Sie die Versionsverwaltung, um sämtliche Versionen aller Objekte in Ihrem Amazon-S3-Bucket zu speichern, abzurufen oder wiederher zustellen. Mit der Versionsv erwaltung können Sie Versionen sowohl nach unbeabsichtigten Benutzera ktionen als auch nach Anwendungsfehlern problemlo s wiederherstellen.

Vorlage

Die Vorlage ist verfügbar unter GitHub: Operational Best Practices for Esquema Nacional de Seguridad (ENS) High.

Betriebliche bewährte Methoden für FDA Titel 21 CFR Teil 11

Konformitätspakete bieten ein allgemeines Compliance-Framework, das es Ihnen ermöglicht, mithilfe verwalteter oder benutzerdefinierter AWS Config Regeln und Abhilfemaßnahmen Kontrollen zur Sicherheits-, Betriebs- oder Kostenoptimierung durchzuführen. AWS Config Conformance Packs dienen als Beispielvorlagen nicht dazu, die vollständige Einhaltung eines bestimmten Governance- oder Compliance-Standards sicherzustellen. Sie sind dafür verantwortlich, selbst zu beurteilen, ob Ihre Nutzung der Services den geltenden gesetzlichen und behördlichen Anforderungen entspricht.

Im Folgenden finden Sie ein Beispiel für eine Zuordnung zwischen Titel 21 des Code of Federal Regulations (CFR) Teil 11 und AWS verwalteten Konfigurationsregeln. Jede AWS Config Regel gilt für eine bestimmte AWS Ressource und bezieht sich auf eine oder mehrere FDA-Kontrollen nach Titel 21 CFR Part 11. Eine Kontrolle nach FDA Title 21 CFR Part 11 kann sich auf mehrere Config-Regeln beziehen. In der folgenden Tabelle finden Sie weitere Informationen und Anleitungen zu diesen Zuordnungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
11.1	Personen, die geschlossene Systeme verwenden , um elektronische Aufzeichnungen zu erstellen, zu ändern, zu pflegen oder zu übertragen, müssen entsprech ende Verfahren und Kontrollen anwenden, um die Echtheit, Integritä t und gegebenen falls die Vertrauli chkeit elektronischer Aufzeichnungen sicherzustellen und dafür zu sorgen, dass die Unterzeic hneten die signierte Aufzeichnung nicht ohne Weiteres als unecht zurückwei sen können. Diese Verfahren und	db-instance-backup-enabled	Die Sicherung sfunktion von Amazon RDS erstellt Sicherung en Ihrer Datenbank en und Transakti onsprotokolle. Amazon RDS erstellt einen Snapshot für das Speichervolume Ihrer DB-Instance, sodass die gesamte DB-Instance gesichert wird. Sie können im System spezifische Aufbewahrungsfrist en festlegen, um Ihre Ausfallsicherheits anforderungen zu erfüllen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	Kontrollen müssen Folgendes umfassen:		
11.1	Personen, die geschlossene Systeme verwenden , um elektronische Aufzeichnungen zu erstellen, zu ändern, zu pflegen oder zu übertragen, müssen entsprech ende Verfahren und Kontrollen anwenden, um die Echtheit, Integritä t und gegebenen falls die Vertrauli chkeit elektronischer Aufzeichnungen sicherzustellen und dafür zu sorgen, dass die Unterzeic hneten die signierte Aufzeichnung nicht ohne Weiteres als unecht zurückwei sen können. Diese Verfahren und Kontrollen müssen Folgendes umfassen:	dynamodb-in-backup-plan	Um Sie bei Datensich erungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon DynamoDB-Tabellen Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwaltet er Backup-Service mit einer richtlini enbasierten Backup-Lösung. Diese Lösung vereinfac ht Ihr Sicherung smanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforde rungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
11.1	Personen, die geschlossene Systeme verwenden , um elektronische Aufzeichnungen zu erstellen, zu ändern, zu pflegen oder zu übertragen, müssen entsprech ende Verfahren und Kontrollen anwenden, um die Echtheit, Integritä t und gegebenen falls die Vertrauli chkeit elektronischer Aufzeichnungen sicherzustellen und dafür zu sorgen, dass die Unterzeic hneten die signierte Aufzeichnung nicht ohne Weiteres als unecht zurückwei sen können. Diese Verfahren und Kontrollen müssen Folgendes umfassen:	dynamodb-pitr-enab led	Aktivieren Sie diese Regel, um zu überprüfen, ob die Informationen gesichert wurden. Es verwaltet auch die Backups, indem es sicherstellt, dass die point-in-time Wiederherstellung in Amazon DynamoDB aktiviert ist. Bei der Wiederherstellung werden fortlaufende Backups Ihrer Tabelle für die letzten 35 Tage gespeichert.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
11.1	Personen, die geschlossene Systeme verwenden , um elektronische Aufzeichnungen zu erstellen, zu ändern, zu pflegen oder zu übertragen, müssen entsprech ende Verfahren und Kontrollen anwenden, um die Echtheit, Integritä t und gegebenen falls die Vertrauli chkeit elektronischer Aufzeichnungen sicherzustellen und dafür zu sorgen, dass die Unterzeic hneten die signierte Aufzeichnung nicht ohne Weiteres als unecht zurückwei sen können. Diese Verfahren und Kontrollen müssen Folgendes umfassen:	ebs-in-backup-plan	Stellen Sie zur Unterstützung der Datensicherungspro zesse sicher, dass Ihre Amazon Elastic Block Store (Amazon EBS) -Volumes Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwaltet er Backup-Service mit einer richtlini enbasierten Backup-Lösung. Diese Lösung vereinfac ht Ihr Sicherung smanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforde rungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
11.1	Personen, die geschlossene Systeme verwenden, um elektronische Aufzeichnungen zu erstellen, zu ändern, zu pflegen oder zu übertragen, müssen entsprechende Verfahren und Kontrollen anwenden, um die Echtheit, Integrität und gegebenenfalls die Vertraulichkeit elektronischer Aufzeichnungen sicherzustellen und dafür zu sorgen, dass die Unterzeichneten die signierte Aufzeichnung nicht ohne Weiteres als unecht zurückweisen können. Diese Verfahren und Kontrollen müssen Folgendes umfassen:	ebs-optimized-instance	Eine optimierte Instance im Amazon Elastic Block Store (Amazon EBS) bietet zusätzliche, dedizierte Kapazität für Amazon-EBS-I/O-Vorgänge. Diese Optimierung bietet die beste Leistung für Ihr EBS-Volume, indem Konflikte zwischen Amazon-EBS-I/O und anderem Datenverkehr von Ihrer Instance minimiert werden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
11.1	Personen, die geschlossene Systeme verwenden , um elektronische Aufzeichnungen zu erstellen, zu ändern, zu pflegen oder zu übertragen, müssen entsprech ende Verfahren und Kontrollen anwenden, um die Echtheit, Integritä t und gegebenen falls die Vertrauli chkeit elektronischer Aufzeichnungen sicherzustellen und dafür zu sorgen, dass die Unterzeic hneten die signierte Aufzeichnung nicht ohne Weiteres als unecht zurückwei sen können. Diese Verfahren und Kontrollen müssen Folgendes umfassen:	efs-in-backup-plan	Um Sie bei Datensich erungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon Elastic File System (Amazon EFS) -Dateisysteme Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwaltet er Backup-Service mit einer richtlini enbasierten Backup-Lösung. Diese Lösung vereinfac ht Ihr Sicherung smanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforde rungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
11.1	Personen, die geschlossene Systeme verwenden , um elektronische Aufzeichnungen zu erstellen, zu ändern, zu pflegen oder zu übertragen, müssen entsprech ende Verfahren und Kontrollen anwenden, um die Echtheit, Integritä t und gegebenen falls die Vertrauli chkeit elektronischer Aufzeichnungen sicherzustellen und dafür zu sorgen, dass die Unterzeic hneten die signierte Aufzeichnung nicht ohne Weiteres als unecht zurückwei sen können. Diese Verfahren und Kontrollen müssen Folgendes umfassen:	elasticache-redis-cluster-automatic-Backup-Check	Wenn automatische Backups aktiviert sind, ElastiCache erstellt Amazon täglich ein Backup des Clusters. Die Sicherung kann für eine von Ihrer Organisation festgelegte Anzahl von Tagen aufbewahrt werden. Automatische Backups schützen vor Datenverlust. Bei einem Ausfall können Sie einen neuen Cluster erstellen, der Ihre Daten aus dem aktuellen Backup wiederherstellt.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
11.1	Personen, die geschlossene Systeme verwenden , um elektronische Aufzeichnungen zu erstellen, zu ändern, zu pflegen oder zu übertragen, müssen entsprech ende Verfahren und Kontrollen anwenden, um die Echtheit, Integritä t und gegebenen falls die Vertrauli chkeit elektronischer Aufzeichnungen sicherzustellen und dafür zu sorgen, dass die Unterzeic hneten die signierte Aufzeichnung nicht ohne Weiteres als unecht zurückwei sen können. Diese Verfahren und Kontrollen müssen Folgendes umfassen:	rds-in-backup-plan	Um Sie bei Datensich erungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon Relational Database Service (Amazon RDS) -Instance s Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwaltet er Backup-Service mit einer richtlini enbasierten Backup-Lösung. Diese Lösung vereinfac ht Ihr Sicherung smanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforde rungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
11.1	Personen, die geschlossene Systeme verwenden, um elektronische Aufzeichnungen zu erstellen, zu ändern, zu pflegen oder zu übertragen, müssen entsprechende Verfahren und Kontrollen anwenden, um die Echtheit, Integrität und gegebenenfalls die Vertraulichkeit elektronischer Aufzeichnungen sicherzustellen und dafür zu sorgen, dass die Unterzeichneten die signierte Aufzeichnung nicht ohne Weiteres als unecht zurückweisen können. Diese Verfahren und Kontrollen müssen Folgendes umfassen:	redshift-backup-enabled	Stellen Sie zur Unterstützung der Datensicherungsprozesse sicher, dass Ihre Amazon-Redshift-Cluster über automatisierte Snapshots verfügen. Wenn automatisierte Snapshots für einen Cluster aktiviert sind, erstellt Redshift in regelmäßigen Abständen Snapshots dieses Clusters. Standardmäßig erstellt Redshift alle acht Stunden oder alle 5 GB einen Snapshot für jeden Knoten mit Datenänderungen oder je nachdem, was zuerst eintritt.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
11.1	Personen, die geschlossene Systeme verwenden , um elektronische Aufzeichnungen zu erstellen, zu ändern, zu pflegen oder zu übertragen, müssen entsprech ende Verfahren und Kontrollen anwenden, um die Echtheit, Integritä t und gegebenen falls die Vertrauli chkeit elektronischer Aufzeichnungen sicherzustellen und dafür zu sorgen, dass die Unterzeic hneten die signierte Aufzeichnung nicht ohne Weiteres als unecht zurückwei sen können. Diese Verfahren und Kontrollen müssen Folgendes umfassen:	s3- bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) unterstützt die Aufrechterhaltung einer angemesse nen Kapazität und Verfügbarkeit. CRR ermöglicht das automatische, asynchrone Kopieren von Objekten in Amazon-S3-Buckets, um die Datenverf ügbarkeit sicherzus tellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
11.1	Personen, die geschlossene Systeme verwenden , um elektronische Aufzeichnungen zu erstellen, zu ändern, zu pflegen oder zu übertragen, müssen entsprech ende Verfahren und Kontrollen anwenden, um die Echtheit, Integritä t und gegebenen falls die Vertrauli chkeit elektronischer Aufzeichnungen sicherzustellen und dafür zu sorgen, dass die Unterzeic hneten die signierte Aufzeichnung nicht ohne Weiteres als unecht zurückwei sen können. Diese Verfahren und Kontrollen müssen Folgendes umfassen:	s-3 bucket-versioning-enabled	Die Versionsv erwaltung von Amazon Simple Storage Service (Amazon S3)-Bucke ts hilft dabei, mehrere Varianten eines Objekts im selben Amazon-S3-Bucket zu speichern. Verwenden Sie die Versionsv erwaltung, um sämtliche Versionen aller Objekte in Ihrem Amazon-S3-Bucket zu speichern , abzurufen oder wiederherzustellen . Mit der Versionsv erwaltung können Sie Versionen sowohl nach unbeabsic htigten Benutzera ktionen als auch nach Anwendungsfehlern problemlos wiederher stellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
11.10(a)	Personen, die geschlossene Systeme verwenden, um elektronische Aufzeichnungen zu erstellen, zu ändern, zu pflegen oder zu übertragen, müssen entsprechende Verfahren und Kontrollen anwenden, um die Echtheit, Integrität und gegebenenfalls die Vertraulichkeit elektronischer Aufzeichnungen sicherzustellen und dafür zu sorgen, dass die Unterzeichneten die signierte Aufzeichnung nicht ohne Weiteres als unecht zurückweisen können. Diese Verfahren und Kontrollen müssen Folgendes umfassen: (a) Validierung von Systemen zur Sicherstellung von Genauigkeit, Zuverlässigkeit,	backup-plan-min-frequency-and-min-retention-check	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihr AWS Backup-Plan auf eine Mindestfrequenz und Aufbewahrung festgelegt ist. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen. Mit dieser Regel können Sie die Parameter requiredFrequencyValue (Config default: 1), requiredRetentionDays (Config default: 35) und requiredFrequencyUnit

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	gleichbleibender Leistung und der Fähigkeit zur Erkennung von ungültigen oder geänderten Aufzeichnungen.		(Config default: days) festlegen. Der tatsächliche Wert muss den Anforderungen Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
11.10(a)	Personen, die geschlossene Systeme verwenden , um elektronische Aufzeichnungen zu erstellen, zu ändern, zu pflegen oder zu übertragen, müssen entsprech ende Verfahren und Kontrollen anwenden, um die Echtheit, Integritä t und gegebenen falls die Vertrauli chkeit elektronischer Aufzeichnungen sicherzustellen und dafür zu sorgen, dass die Unterzeic hneten die signierte Aufzeichnung nicht ohne Weiteres als unecht zurückwei sen können. Diese Verfahren und Kontrollen müssen Folgendes umfassen: (a) Validierung von Systemen zur Sicherstellung von Genauigkeit, Zuverlässigkeit,	backup-recovery-point-encrypted	Stellen Sie sicher, dass die Verschlüs selung für Ihre AWS Backup-Wiederherst ellungspunkte aktiviert ist. Da sensible Daten auch im Ruhezusta nd vorhanden sein können, sollten Sie die Verschlüsselung im Ruhezustand aktivieren, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	gleichbleibender Leistung und der Fähigkeit zur Erkennung von ungültigen oder geänderten Aufzeichnungen.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
11.10(a)	Personen, die geschlossene Systeme verwenden , um elektronische Aufzeichnungen zu erstellen, zu ändern, zu pflegen oder zu übertragen, müssen entsprech ende Verfahren und Kontrollen anwenden, um die Echtheit, Integritä t und gegebenen falls die Vertrauli chkeit elektronischer Aufzeichnungen sicherzustellen und dafür zu sorgen, dass die Unterzeic hneten die signierte Aufzeichnung nicht ohne Weiteres als unecht zurückwei sen können. Diese Verfahren und Kontrollen müssen Folgendes umfassen: (a) Validierung von Systemen zur Sicherstellung von Genauigkeit, Zuverlässigkeit,	backup-recovery-point-manual-Löschen-deaktiviert	Stellen Sie sicher, dass Ihren AWS Backup-Wiederherstellungspunkten eine ressourcenbasierte Richtlinie zugeordnet ist, die das Löschen von Wiederherstellungspunkten verhindert. Die Verwendung einer ressourcenbasierten Richtlinie zur Verhinderung des Löschens von Wiederherstellungspunkten kann dazu beitragen, ein versehentliches oder absichtliches Löschen zu unterbinden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	gleichbleibender Leistung und der Fähigkeit zur Erkennung von ungültigen oder geänderten Aufzeichnungen.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
11.10(a)	Personen, die geschlossene Systeme verwenden , um elektronische Aufzeichnungen zu erstellen, zu ändern, zu pflegen oder zu übertragen, müssen entsprech ende Verfahren und Kontrollen anwenden, um die Echtheit, Integritä t und gegebenen falls die Vertrauli chkeit elektronischer Aufzeichnungen sicherzustellen und dafür zu sorgen, dass die Unterzeic hneten die signierte Aufzeichnung nicht ohne Weiteres als unecht zurückwei sen können. Diese Verfahren und Kontrollen müssen Folgendes umfassen: (a) Validierung von Systemen zur Sicherstellung von Genauigkeit, Zuverlässigkeit,	cloud-trail-log-file-Validierung aktiviert	Verwenden Sie die AWS CloudTrail Protokolldateivali dierung, um die Integrität von Protokoll en zu überprüfen. CloudTrail Mithilfe der Protokolldateivali dierung kann festgestellt werden, ob eine Protokoll datei geändert oder gelöscht wurde oder ob sie nach der Übermittlung CloudTrail unverände rt geblieben ist. Dieses Feature wurde mit dem Branchens tandard entsprech enden Algorithmen entwickelt: SHA-256 für die Hashfunktion und SHA-256 mit RSA für digitale Signature n. Aus diesem Grund ist es rechnerisch unmöglich, CloudTrai l Protokolldateien unbemerkt zu ändern, zu löschen oder zu fälschen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	gleichbleibender Leistung und der Fähigkeit zur Erkennung von ungültigen oder geänderten Aufzeichnungen.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
11.10(a)	Personen, die geschlossene Systeme verwenden , um elektronische Aufzeichnungen zu erstellen, zu ändern, zu pflegen oder zu übertragen, müssen entsprech ende Verfahren und Kontrollen anwenden, um die Echtheit, Integritä t und gegebenen falls die Vertrauli chkeit elektronischer Aufzeichnungen sicherzustellen und dafür zu sorgen, dass die Unterzeic hneten die signierte Aufzeichnung nicht ohne Weiteres als unecht zurückwei sen können. Diese Verfahren und Kontrollen müssen Folgendes umfassen: (a) Validierung von Systemen zur Sicherstellung von Genauigkeit, Zuverlässigkeit,	cloudtrail-security-trail-enabled	Diese Regel trägt dazu bei, die Verwendung der AWS empfohlenen bewährten Sicherhei tsmethoden für sicherzustellen AWS CloudTrai l, indem geprüft wird, ob mehrere Einstellungen aktiviert sind. Dazu gehören die Verwendun g von Protokoll verschlüsselung, Protokollvalidieru ng und Aktivierung AWS CloudTrail in mehreren Regionen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	gleichbleibender Leistung und der Fähigkeit zur Erkennung von ungültigen oder geänderten Aufzeichnungen.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
11.10(a)	Personen, die geschlossene Systeme verwenden , um elektronische Aufzeichnungen zu erstellen, zu ändern, zu pflegen oder zu übertragen, müssen entsprech ende Verfahren und Kontrollen anwenden, um die Echtheit, Integritä t und gegebenen falls die Vertrauli chkeit elektronischer Aufzeichnungen sicherzustellen und dafür zu sorgen, dass die Unterzeic hneten die signierte Aufzeichnung nicht ohne Weiteres als unecht zurückwei sen können. Diese Verfahren und Kontrollen müssen Folgendes umfassen: (a) Validierung von Systemen zur Sicherstellung von Genauigkeit, Zuverlässigkeit,	db-instance-backup-enabled	Die Sicherung sfunktion von Amazon RDS erstellt Sicherung en Ihrer Datenbank en und Transakti onsprotokolle. Amazon RDS erstellt einen Snapshot für das Speichervolume Ihrer DB-Instance, sodass die gesamte DB-Instance gesichert wird. Sie können im System spezifische Aufbewahrungsfrist en festlegen, um Ihre Ausfallsicherheits anforderungen zu erfüllen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	gleichbleibender Leistung und der Fähigkeit zur Erkennung von ungültigen oder geänderten Aufzeichnungen.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
11.10(a)	Personen, die geschlossene Systeme verwenden , um elektronische Aufzeichnungen zu erstellen, zu ändern, zu pflegen oder zu übertragen, müssen entsprech ende Verfahren und Kontrollen anwenden, um die Echtheit, Integritä t und gegebenen falls die Vertrauli chkeit elektronischer Aufzeichnungen sicherzustellen und dafür zu sorgen, dass die Unterzeic hneten die signierte Aufzeichnung nicht ohne Weiteres als unecht zurückwei sen können. Diese Verfahren und Kontrollen müssen Folgendes umfassen: (a) Validierung von Systemen zur Sicherstellung von Genauigkeit, Zuverlässigkeit,	dynamodb-autoscali ng-enabled	Amazon DynamoDB Auto Scaling verwendet den AWS Application Auto Scaling-Service, um die bereitgestellte Durchsatzkapazität so anzupassen, dass sie automatis ch auf tatsächli che Verkehrsm uster reagiert. Auf diese Weise kann eine Tabelle oder ein globaler sekundärer Index die bereitgestellte Lese-/Schreibkapaz ität erhöhen, um plötzliche Erhöhunge n des Datenverkehrs ohne Drosselung zu bewältigen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	gleichbleibender Leistung und der Fähigkeit zur Erkennung von ungültigen oder geänderten Aufzeichnungen.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
11.10(a)	Personen, die geschlossene Systeme verwenden , um elektronische Aufzeichnungen zu erstellen, zu ändern, zu pflegen oder zu übertragen, müssen entsprech ende Verfahren und Kontrollen anwenden, um die Echtheit, Integritä t und gegebenen falls die Vertrauli chkeit elektronischer Aufzeichnungen sicherzustellen und dafür zu sorgen, dass die Unterzeic hneten die signierte Aufzeichnung nicht ohne Weiteres als unecht zurückwei sen können. Diese Verfahren und Kontrollen müssen Folgendes umfassen: (a) Validierung von Systemen zur Sicherstellung von Genauigkeit, Zuverlässigkeit,	dynamodb-in-backup-plan	Um Sie bei Datensich erungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon DynamoDB-Tabellen Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwaltet er Backup-Service mit einer richtlini enbasierten Backup-Lösung. Diese Lösung vereinfac ht Ihr Sicherung smanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforde rungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	gleichbleibender Leistung und der Fähigkeit zur Erkennung von ungültigen oder geänderten Aufzeichnungen.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
11.10(a)	Personen, die geschlossene Systeme verwenden , um elektronische Aufzeichnungen zu erstellen, zu ändern, zu pflegen oder zu übertragen, müssen entsprech ende Verfahren und Kontrollen anwenden, um die Echtheit, Integritä t und gegebenen falls die Vertrauli chkeit elektronischer Aufzeichnungen sicherzustellen und dafür zu sorgen, dass die Unterzeic hneten die signierte Aufzeichnung nicht ohne Weiteres als unecht zurückwei sen können. Diese Verfahren und Kontrollen müssen Folgendes umfassen: (a) Validierung von Systemen zur Sicherstellung von Genauigkeit, Zuverlässigkeit,	dynamodb-pitr-enab led	Aktivieren Sie diese Regel, um zu überprüfen, ob die Informationen gesichert wurden. Es verwaltet auch die Backups, indem es sicherstellt, dass die point-in-time Wiederherstellung in Amazon DynamoDB aktiviert ist. Bei der Wiederherstellung werden fortlaufende Backups Ihrer Tabelle für die letzten 35 Tage gespeichert.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	gleichbleibender Leistung und der Fähigkeit zur Erkennung von ungültigen oder geänderten Aufzeichnungen.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
11.10(a)	Personen, die geschlossene Systeme verwenden , um elektronische Aufzeichnungen zu erstellen, zu ändern, zu pflegen oder zu übertragen, müssen entsprech ende Verfahren und Kontrollen anwenden, um die Echtheit, Integritä t und gegebenen falls die Vertrauli chkeit elektronischer Aufzeichnungen sicherzustellen und dafür zu sorgen, dass die Unterzeic hneten die signierte Aufzeichnung nicht ohne Weiteres als unecht zurückwei sen können. Diese Verfahren und Kontrollen müssen Folgendes umfassen: (a) Validierung von Systemen zur Sicherstellung von Genauigkeit, Zuverlässigkeit,	dynamodb-resources-protected-by-Backup-Plan	Um Sie bei Datensich erungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon DynamoDB DynamoDB-Ressourcen Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwaltet er Backup-Service mit einer richtlini enbasierten Backup-Lösung. Diese Lösung vereinfac ht Ihr Sicherung smanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforde rungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	gleichbleibender Leistung und der Fähigkeit zur Erkennung von ungültigen oder geänderten Aufzeichnungen.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
11.10(a)	Personen, die geschlossene Systeme verwenden , um elektronische Aufzeichnungen zu erstellen, zu ändern, zu pflegen oder zu übertragen, müssen entsprech ende Verfahren und Kontrollen anwenden, um die Echtheit, Integritä t und gegebenen falls die Vertrauli chkeit elektronischer Aufzeichnungen sicherzustellen und dafür zu sorgen, dass die Unterzeic hneten die signierte Aufzeichnung nicht ohne Weiteres als unecht zurückwei sen können. Diese Verfahren und Kontrollen müssen Folgendes umfassen: (a) Validierung von Systemen zur Sicherstellung von Genauigkeit, Zuverlässigkeit,	ebs-in-backup-plan	Stellen Sie zur Unterstützung der Datensicherungspro zesse sicher, dass Ihre Amazon Elastic Block Store (Amazon EBS) -Volumes Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwaltet er Backup-Service mit einer richtlini enbasierten Backup-Lösung. Diese Lösung vereinfac ht Ihr Sicherung smanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforde rungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	gleichbleibender Leistung und der Fähigkeit zur Erkennung von ungültigen oder geänderten Aufzeichnungen.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
11.10(a)	Personen, die geschlossene Systeme verwenden , um elektronische Aufzeichnungen zu erstellen, zu ändern, zu pflegen oder zu übertragen, müssen entsprech ende Verfahren und Kontrollen anwenden, um die Echtheit, Integritä t und gegebenen falls die Vertrauli chkeit elektronischer Aufzeichnungen sicherzustellen und dafür zu sorgen, dass die Unterzeic hneten die signierte Aufzeichnung nicht ohne Weiteres als unecht zurückwei sen können. Diese Verfahren und Kontrollen müssen Folgendes umfassen: (a) Validierung von Systemen zur Sicherstellung von Genauigkeit, Zuverlässigkeit,	ebs-optimized-inst ance	Eine optimierte Instance im Amazon Elastic Block Store (Amazon EBS) bietet zusätzliche, dedizierte Kapazität für Amazon-EBS-I/ O-Vorgänge. Diese Optimierung bietet die beste Leistung für Ihr EBS-Volume, indem Konflikte zwischen Amazon-EBS-I/O und anderem Datenverk ehr von Ihrer Instance minimiert werden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	gleichbleibender Leistung und der Fähigkeit zur Erkennung von ungültigen oder geänderten Aufzeichnungen.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
11.10(a)	Personen, die geschlossene Systeme verwenden, um elektronische Aufzeichnungen zu erstellen, zu ändern, zu pflegen oder zu übertragen, müssen entsprechende Verfahren und Kontrollen anwenden, um die Echtheit, Integrität und gegebenenfalls die Vertraulichkeit elektronischer Aufzeichnungen sicherzustellen und dafür zu sorgen, dass die Unterzeichneten die signierte Aufzeichnung nicht ohne Weiteres als unecht zurückweisen können. Diese Verfahren und Kontrollen müssen Folgendes umfassen: (a) Validierung von Systemen zur Sicherstellung von Genauigkeit, Zuverlässigkeit,	ec2-manager instance-managed-by-systems	Eine Bestandsaufnahme der Softwareplattformen und Anwendungen innerhalb des Unternehmens ist möglich, indem Amazon Elastic Compute Cloud (Amazon EC2) - Instances mit AWS Systems Manager verwaltet werden. Verwenden Sie AWS Systems Manager, um detaillierte Systemkonfigurationen, Betriebssystem-Patch-Levels, Namen und Typ der Dienste, Softwareinstallationen, Anwendungsname, Herausgeber und Version sowie andere Details zu Ihrer Umgebung bereitzustellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	gleichbleibender Leistung und der Fähigkeit zur Erkennung von ungültigen oder geänderten Aufzeichnungen.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
11.10(a)	Personen, die geschlossene Systeme verwenden, um elektronische Aufzeichnungen zu erstellen, zu ändern, zu pflegen oder zu übertragen, müssen entsprechende Verfahren und Kontrollen anwenden, um die Echtheit, Integrität und gegebenenfalls die Vertraulichkeit elektronischer Aufzeichnungen sicherzustellen und dafür zu sorgen, dass die Unterzeichneten die signierte Aufzeichnung nicht ohne Weiteres als unecht zurückweisen können. Diese Verfahren und Kontrollen müssen Folgendes umfassen: (a) Validierung von Systemen zur Sicherstellung von Genauigkeit, Zuverlässigkeit,	ec2-check managedinstance-association-compliance-status	Verwenden Sie AWS Systems Manager Associations, um bei der Inventarisierung von Softwareplattformen und Anwendungen innerhalb eines Unternehmens zu helfen. AWS Systems Manager weist Ihren verwalteten Instanzen einen Konfigurationsstatus zu und ermöglicht es Ihnen, Basiswerte für Betriebssystem-Patch-Levels, Softwareinstallationen, Anwendungskonfigurationen und andere Details zu Ihrer Umgebung festzulegen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	gleichbleibender Leistung und der Fähigkeit zur Erkennung von ungültigen oder geänderten Aufzeichnungen.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
11.10(a)	Personen, die geschlossene Systeme verwenden , um elektronische Aufzeichnungen zu erstellen, zu ändern, zu pflegen oder zu übertragen, müssen entsprech ende Verfahren und Kontrollen anwenden, um die Echtheit, Integritä t und gegebenen falls die Vertrauli chkeit elektronischer Aufzeichnungen sicherzustellen und dafür zu sorgen, dass die Unterzeic hneten die signierte Aufzeichnung nicht ohne Weiteres als unecht zurückwei sen können. Diese Verfahren und Kontrollen müssen Folgendes umfassen: (a) Validierung von Systemen zur Sicherstellung von Genauigkeit, Zuverlässigkeit,	ec2-check managedin stance-patch-compl iance-status	Aktivieren Sie diese Regel, um bei der Identifizierung und Dokumentation von Sicherheitslücken in Amazon Elastic Compute Cloud (Amazon EC2) zu helfen. Die Regel prüft, ob die EC2 Amazon-Instance die Patch-Konformität im AWS Systems Manager gemäß den Richtlinien und Verfahren Ihrer Organisation einhält.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	gleichbleibender Leistung und der Fähigkeit zur Erkennung von ungültigen oder geänderten Aufzeichnungen.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
11.10(a)	Personen, die geschlossene Systeme verwenden , um elektronische Aufzeichnungen zu erstellen, zu ändern, zu pflegen oder zu übertragen, müssen entsprech ende Verfahren und Kontrollen anwenden, um die Echtheit, Integritä t und gegebenen falls die Vertrauli chkeit elektronischer Aufzeichnungen sicherzustellen und dafür zu sorgen, dass die Unterzeic hneten die signierte Aufzeichnung nicht ohne Weiteres als unecht zurückwei sen können. Diese Verfahren und Kontrollen müssen Folgendes umfassen: (a) Validierung von Systemen zur Sicherstellung von Genauigkeit, Zuverlässigkeit,	ec2--Plan resources-protected-by-backup	Um Sie bei Datensich erungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon Elastic Compute Cloud (Amazon EC2) -Ressourc en Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwaltet er Backup-Service mit einer richtlini enbasierten Backup-Lösung. Diese Lösung vereinfac ht Ihr Sicherung smanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforde rungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	gleichbleibender Leistung und der Fähigkeit zur Erkennung von ungültigen oder geänderten Aufzeichnungen.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
11.10(a)	Personen, die geschlossene Systeme verwenden , um elektronische Aufzeichnungen zu erstellen, zu ändern, zu pflegen oder zu übertragen, müssen entsprech ende Verfahren und Kontrollen anwenden, um die Echtheit, Integritä t und gegebenen falls die Vertrauli chkeit elektronischer Aufzeichnungen sicherzustellen und dafür zu sorgen, dass die Unterzeic hneten die signierte Aufzeichnung nicht ohne Weiteres als unecht zurückwei sen können. Diese Verfahren und Kontrollen müssen Folgendes umfassen: (a) Validierung von Systemen zur Sicherstellung von Genauigkeit, Zuverlässigkeit,	ec2-stopped-instance	Aktivieren Sie diese Regel, um bei der Basiskonfiguration von Amazon Elastic Compute Cloud (Amazon EC2) - Instances zu helfen, indem Sie überprüfe n, ob EC2 Amazon-Instances gemäß den Standards Ihrer Organisation für mehr als die zulässige Anzahl von Tagen gestoppt wurden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	gleichbleibender Leistung und der Fähigkeit zur Erkennung von ungültigen oder geänderten Aufzeichnungen.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
11.10(a)	Personen, die geschlossene Systeme verwenden , um elektronische Aufzeichnungen zu erstellen, zu ändern, zu pflegen oder zu übertragen, müssen entsprech ende Verfahren und Kontrollen anwenden, um die Echtheit, Integritä t und gegebenen falls die Vertrauli chkeit elektronischer Aufzeichnungen sicherzustellen und dafür zu sorgen, dass die Unterzeic hneten die signierte Aufzeichnung nicht ohne Weiteres als unecht zurückwei sen können. Diese Verfahren und Kontrollen müssen Folgendes umfassen: (a) Validierung von Systemen zur Sicherstellung von Genauigkeit, Zuverlässigkeit,	ec2- volume-inuse-check	Diese Regel stellt sicher, dass Amazon Elastic Block Store-Volumes, die an Amazon Elastic Compute Cloud (Amazon EC2) - Instances angehängt sind, zum Löschen markiert werden, wenn eine Instance beendet wird. Wenn ein Amazon-EB S-Volume nicht gelöscht wird, wenn die Instance, an die es angehängt ist, beendet wird, kann dies gegen das Konzept der geringsten Funktiona lität verstoßen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	gleichbleibender Leistung und der Fähigkeit zur Erkennung von ungültigen oder geänderten Aufzeichnungen.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
11.10(a)	Personen, die geschlossene Systeme verwenden , um elektronische Aufzeichnungen zu erstellen, zu ändern, zu pflegen oder zu übertragen, müssen entsprech ende Verfahren und Kontrollen anwenden, um die Echtheit, Integritä t und gegebenen falls die Vertrauli chkeit elektronischer Aufzeichnungen sicherzustellen und dafür zu sorgen, dass die Unterzeic hneten die signierte Aufzeichnung nicht ohne Weiteres als unecht zurückwei sen können. Diese Verfahren und Kontrollen müssen Folgendes umfassen: (a) Validierung von Systemen zur Sicherstellung von Genauigkeit, Zuverlässigkeit,	efs-in-backup-plan	Um Sie bei Datensich erungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon Elastic File System (Amazon EFS) -Dateisysteme Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwaltet er Backup-Service mit einer richtlini enbasierten Backup-Lösung. Diese Lösung vereinfac ht Ihr Sicherung smanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforde rungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	gleichbleibender Leistung und der Fähigkeit zur Erkennung von ungültigen oder geänderten Aufzeichnungen.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
11.10(a)	Personen, die geschlossene Systeme verwenden , um elektronische Aufzeichnungen zu erstellen, zu ändern, zu pflegen oder zu übertragen, müssen entsprech ende Verfahren und Kontrollen anwenden, um die Echtheit, Integritä t und gegebenen falls die Vertrauli chkeit elektronischer Aufzeichnungen sicherzustellen und dafür zu sorgen, dass die Unterzeic hneten die signierte Aufzeichnung nicht ohne Weiteres als unecht zurückwei sen können. Diese Verfahren und Kontrollen müssen Folgendes umfassen: (a) Validierung von Systemen zur Sicherstellung von Genauigkeit, Zuverlässigkeit,	elasticache-redis-cluster-automatic-Backup-Check	Wenn automatische Backups aktiviert sind, ElastiCache erstellt Amazon täglich ein Backup des Clusters. Die Sicherung kann für eine von Ihrer Organisation festgelegte Anzahl von Tagen aufbewahrt werden. Automatische Backups schützen vor Datenverlust. Bei einem Ausfall können Sie einen neuen Cluster erstellen, der Ihre Daten aus dem aktuellen Backup wiederherstellt.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	gleichbleibender Leistung und der Fähigkeit zur Erkennung von ungültigen oder geänderten Aufzeichnungen.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
11.10(a)	Personen, die geschlossene Systeme verwenden , um elektronische Aufzeichnungen zu erstellen, zu ändern, zu pflegen oder zu übertragen, müssen entsprech ende Verfahren und Kontrollen anwenden, um die Echtheit, Integritä t und gegebenen falls die Vertrauli chkeit elektronischer Aufzeichnungen sicherzustellen und dafür zu sorgen, dass die Unterzeic hneten die signierte Aufzeichnung nicht ohne Weiteres als unecht zurückwei sen können. Diese Verfahren und Kontrollen müssen Folgendes umfassen: (a) Validierung von Systemen zur Sicherstellung von Genauigkeit, Zuverlässigkeit,	elb-cross-zone-load-Balancing aktiviert	Aktivieren Sie zonenübergreifende s Load Balancing für Ihre Elastic Load Balancer (ELBs), um eine angemesse ne Kapazität und Verfügbarkeit aufrechtzuerhalten. Zonenübergreifende s Load Balancing reduziert die Notwendigkeit, die gleiche Anzahl von Instances in jeder aktivierten Availability Zone aufrechtzuerhalten. Es verbessert auch die Fähigkeit Ihrer Anwendung, den Verlust einer oder mehrerer Instances zu bewältigen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	gleichbleibender Leistung und der Fähigkeit zur Erkennung von ungültigen oder geänderten Aufzeichnungen.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
11.10(a)	Personen, die geschlossene Systeme verwenden , um elektronische Aufzeichnungen zu erstellen, zu ändern, zu pflegen oder zu übertragen, müssen entsprech ende Verfahren und Kontrollen anwenden, um die Echtheit, Integritä t und gegebenen falls die Vertrauli chkeit elektronischer Aufzeichnungen sicherzustellen und dafür zu sorgen, dass die Unterzeic hneten die signierte Aufzeichnung nicht ohne Weiteres als unecht zurückwei sen können. Diese Verfahren und Kontrollen müssen Folgendes umfassen: (a) Validierung von Systemen zur Sicherstellung von Genauigkeit, Zuverlässigkeit,	elb-deletion-prote ction-enabled	Diese Regel sorgt dafür, dass der Löschschutz für Elastic Load Balancing aktiviert ist. Verwenden Sie diese Funktion, um zu verhindern, dass Ihr Load Balancer versehentlich oder böswillig gelöscht wird, was zum Verlust der Verfügbarkeit Ihrer Anwendungen führen kann.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	gleichbleibender Leistung und der Fähigkeit zur Erkennung von ungültigen oder geänderten Aufzeichnungen.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
11.10(a)	Personen, die geschlossene Systeme verwenden , um elektronische Aufzeichnungen zu erstellen, zu ändern, zu pflegen oder zu übertragen, müssen entsprech ende Verfahren und Kontrollen anwenden, um die Echtheit, Integritä t und gegebenen falls die Vertrauli chkeit elektronischer Aufzeichnungen sicherzustellen und dafür zu sorgen, dass die Unterzeic hneten die signierte Aufzeichnung nicht ohne Weiteres als unecht zurückwei sen können. Diese Verfahren und Kontrollen müssen Folgendes umfassen: (a) Validierung von Systemen zur Sicherstellung von Genauigkeit, Zuverlässigkeit,	rds-in-backup-plan	Um Sie bei Datensich erungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon Relational Database Service (Amazon RDS) -Instance s Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwaltet er Backup-Service mit einer richtlini enbasierten Backup-Lösung. Diese Lösung vereinfac ht Ihr Sicherung smanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforde rungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	gleichbleibender Leistung und der Fähigkeit zur Erkennung von ungültigen oder geänderten Aufzeichnungen.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
11.10(a)	Personen, die geschlossene Systeme verwenden , um elektronische Aufzeichnungen zu erstellen, zu ändern, zu pflegen oder zu übertragen, müssen entsprech ende Verfahren und Kontrollen anwenden, um die Echtheit, Integritä t und gegebenen falls die Vertrauli chkeit elektronischer Aufzeichnungen sicherzustellen und dafür zu sorgen, dass die Unterzeic hneten die signierte Aufzeichnung nicht ohne Weiteres als unecht zurückwei sen können. Diese Verfahren und Kontrollen müssen Folgendes umfassen: (a) Validierung von Systemen zur Sicherstellung von Genauigkeit, Zuverlässigkeit,	rds-multi-az-support	Die Multi-AZ-Unterstüt zung in Amazon Relational Database Service (Amazon RDS) bietet eine verbesserte Verfügbar keit und Beständig keit von Datenbank -Instances. Wenn Sie eine Multi-AZ-Datenbank-Instance bereitste llen, erstellt Amazon RDS automatisch eine primäre Datenbank-Instance und replizier t die Daten synchron auf eine Standby-Instance in einer anderen Availability Zone. Jede Availabil ity Zone läuft auf einer eigenen, physisch getrennte n, unabhängigen Infrastruktur und ist auf eine hohe Verfügbarkeit ausgelegt. Im Falle eines Infrastru kturausfalls führt Amazon RDS einen automatis

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	gleichbleibender Leistung und der Fähigkeit zur Erkennung von ungültigen oder geänderten Aufzeichnungen.		chen Failover zum Standby-Modus durch, sodass Sie den Datenbankbetrieb wieder aufnehmen können, sobald der Failover abgeschlossen ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
11.10(a)	Personen, die geschlossene Systeme verwenden, um elektronische Aufzeichnungen zu erstellen, zu ändern, zu pflegen oder zu übertragen, müssen entsprechende Verfahren und Kontrollen anwenden, um die Echtheit, Integrität und gegebenenfalls die Vertraulichkeit elektronischer Aufzeichnungen sicherzustellen und dafür zu sorgen, dass die Unterzeichneten die signierte Aufzeichnung nicht ohne Weiteres als unecht zurückweisen können. Diese Verfahren und Kontrollen müssen Folgendes umfassen: (a) Validierung von Systemen zur Sicherstellung von Genauigkeit, Zuverlässigkeit,	redshift-backup-enabled	Stellen Sie zur Unterstützung der Datensicherungsprozesse sicher, dass Ihre Amazon-Redshift-Cluster über automatisierte Snapshots verfügen. Wenn automatisierte Snapshots für einen Cluster aktiviert sind, erstellt Redshift in regelmäßigen Abständen Snapshots dieses Clusters. Standardmäßig erstellt Redshift alle acht Stunden oder alle 5 GB einen Snapshot für jeden Knoten mit Datenänderungen oder je nachdem, was zuerst eintritt.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	gleichbleibender Leistung und der Fähigkeit zur Erkennung von ungültigen oder geänderten Aufzeichnungen.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
11.10(a)	Personen, die geschlossene Systeme verwenden , um elektronische Aufzeichnungen zu erstellen, zu ändern, zu pflegen oder zu übertragen, müssen entsprech ende Verfahren und Kontrollen anwenden, um die Echtheit, Integritä t und gegebenen falls die Vertrauli chkeit elektronischer Aufzeichnungen sicherzustellen und dafür zu sorgen, dass die Unterzeic hneten die signierte Aufzeichnung nicht ohne Weiteres als unecht zurückwei sen können. Diese Verfahren und Kontrollen müssen Folgendes umfassen: (a) Validierung von Systemen zur Sicherstellung von Genauigkeit, Zuverlässigkeit,	s3- bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) unterstützt die Aufrechterhaltung einer angemesse nen Kapazität und Verfügbarkeit. CRR ermöglicht das automatische, asynchrone Kopieren von Objekten in Amazon-S3-Buckets, um die Datenverf ügbarkeit sicherzus tellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	gleichbleibender Leistung und der Fähigkeit zur Erkennung von ungültigen oder geänderten Aufzeichnungen.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
11.10(a)	Personen, die geschlossene Systeme verwenden , um elektronische Aufzeichnungen zu erstellen, zu ändern, zu pflegen oder zu übertragen, müssen entsprech ende Verfahren und Kontrollen anwenden, um die Echtheit, Integritä t und gegebenen falls die Vertrauli chkeit elektronischer Aufzeichnungen sicherzustellen und dafür zu sorgen, dass die Unterzeic hneten die signierte Aufzeichnung nicht ohne Weiteres als unecht zurückwei sen können. Diese Verfahren und Kontrollen müssen Folgendes umfassen: (a) Validierung von Systemen zur Sicherstellung von Genauigkeit, Zuverlässigkeit,	s-3 bucket-versioning-enabled	Die Versionsv erwaltung von Amazon Simple Storage Service (Amazon S3)-Bucke ts hilft dabei, mehrere Varianten eines Objekts im selben Amazon-S3-Bucket zu speichern. Verwenden Sie die Versionsv erwaltung, um sämtliche Versionen aller Objekte in Ihrem Amazon-S3-Bucket zu speichern , abzurufen oder wiederherzustellen . Mit der Versionsv erwaltung können Sie Versionen sowohl nach unbeabsic htigten Benutzera ktionen als auch nach Anwendungsfehlern problemlos wiederher stellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	gleichbleibender Leistung und der Fähigkeit zur Erkennung von ungültigen oder geänderten Aufzeichnungen.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
11.10(a)	Personen, die geschlossene Systeme verwenden, um elektronische Aufzeichnungen zu erstellen, zu ändern, zu pflegen oder zu übertragen, müssen entsprechende Verfahren und Kontrollen anwenden, um die Echtheit, Integrität und gegebenenfalls die Vertraulichkeit elektronischer Aufzeichnungen sicherzustellen und dafür zu sorgen, dass die Unterzeichneten die signierte Aufzeichnung nicht ohne Weiteres als unecht zurückweisen können. Diese Verfahren und Kontrollen müssen Folgendes umfassen: (a) Validierung von Systemen zur Sicherstellung von Genauigkeit, Zuverlässigkeit,	vpc-vpn-2-tunnels-up	Redundante Site-to-Site VPN-Tunnel können implementiert werden, um die Anforderungen an die Ausfallsicherheit zu erfüllen. Es verwendet zwei Tunnel, um die Konnektivität sicherzustellen, falls eine der Site-to-Site VPN-Verbindungen nicht verfügbar ist. Um sich vor einem Verbindungsverlust zu schützen, können Sie für den Fall, dass Ihr Kunden-Gateway nicht verfügbar ist, eine zweite Site-to-Site VPN-Verbindung zu Ihrer Amazon Virtual Private Cloud (Amazon VPC) und Ihrem Virtual Private Gateway einrichten, indem Sie ein zweites Kunden-Gateway verwenden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	gleichbleibender Leistung und der Fähigkeit zur Erkennung von ungültigen oder geänderten Aufzeichnungen.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
11.10(c)	Personen, die geschlossene Systeme verwenden , um elektronische Aufzeichnungen zu erstellen, zu ändern, zu pflegen oder zu übertragen, müssen entsprech ende Verfahren und Kontrollen anwenden, um die Echtheit, Integritä t und gegebenen falls die Vertrauli chkeit elektroni scher Aufzeichn ungen sicherzus tellen und dafür zu sorgen, dass die Unterzeichneten die signierte Aufzeichn ung nicht ohne Weiteres als unecht zurückweisen können. Diese Verfahren und Kontrollen müssen Folgendes umfassen: (c) Schutz der Aufzeichnungen, damit sie während der gesamten Aufbewahr ungsfrist fehlerfrei und	cloud-trail-encryption-enabled	Da sensible Daten vorhanden sein können und um Daten im Speicher zu schützen, sollten Sie sicherstellen, dass die Verschlüsselung für Ihre AWS CloudTrail Trails aktiviert ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	problemlos abgerufen werden können.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
11.10(c)	Personen, die geschlossene Systeme verwenden, um elektronische Aufzeichnungen zu erstellen, zu ändern, zu pflegen oder zu übertragen, müssen entsprechende Verfahren und Kontrollen anwenden, um die Echtheit, Integrität und gegebenenfalls die Vertraulichkeit elektronischer Aufzeichnungen sicherzustellen und dafür zu sorgen, dass die Unterzeichneten die signierte Aufzeichnung nicht ohne Weiteres als unecht zurückweisen können. Diese Verfahren und Kontrollen müssen Folgendes umfassen: (c) Schutz der Aufzeichnungen, damit sie während der gesamten Aufbewahrungsfrist fehlerfrei und	cw-loggroup-retention-period-überprüfen	Stellen Sie sicher, dass die Ereignisprotokolldaten für Ihre Protokollgruppen über eine Mindestdauer aufbewahrt werden, um die Fehlerbehebung und forensische Untersuchungen zu unterstützen. Fehlende frühere Ereignisprotokolldaten erschweren die Rekonstruierung und Identifizierung potenziell schädlicher Ereignisse.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	problemlos abgerufen werden können.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
11.10(c)	Personen, die geschlossene Systeme verwenden , um elektronische Aufzeichnungen zu erstellen, zu ändern, zu pflegen oder zu übertragen, müssen entsprech ende Verfahren und Kontrollen anwenden, um die Echtheit, Integritä t und gegebenen falls die Vertrauli chkeit elektroni scher Aufzeichn ungen sicherzus tellen und dafür zu sorgen, dass die Unterzeichneten die signierte Aufzeichn ung nicht ohne Weiteres als unecht zurückweisen können. Diese Verfahren und Kontrollen müssen Folgendes umfassen: (c) Schutz der Aufzeichnungen, damit sie während der gesamten Aufbewahr ungsfrist fehlerfrei und	ecr-private-lifecycle-policy-konfiguriert	Mit Lebenszyk lusrichtlinien des Amazon Elastic Container Repositor y (ECR) können Sie das Lebenszyk lusmanagement von Images in einem Repository festlegen . Dies ermöglicht die Automatisierung der Bereinigung ungenutzter Images, z. B. Images, die aufgrund von Alter oder Anzahl ablaufen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	problemlos abgerufen werden können.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
11.10(c)	Personen, die geschlossene Systeme verwenden, um elektronische Aufzeichnungen zu erstellen, zu ändern, zu pflegen oder zu übertragen, müssen entsprechende Verfahren und Kontrollen anwenden, um die Echtheit, Integrität und gegebenenfalls die Vertraulichkeit elektronischer Aufzeichnungen sicherzustellen und dafür zu sorgen, dass die Unterzeichneten die signierte Aufzeichnung nicht ohne Weiteres als unecht zurückweisen können. Diese Verfahren und Kontrollen müssen Folgendes umfassen: (c) Schutz der Aufzeichnungen, damit sie während der gesamten Aufbewahrungsfrist fehlerfrei und	rds-snapshot-encrypted	Stellen Sie sicher, dass die Verschlüsselung für Ihre Amazon Relational Database Service (Amazon RDS)-Snapshots aktiviert ist. Da sensible Daten auch im Ruhezustand vorhanden sein können, sollten Sie die Verschlüsselung im Ruhezustand aktivieren, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	problemlos abgerufen werden können.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
11.10(c)	Personen, die geschlossene Systeme verwenden , um elektronische Aufzeichnungen zu erstellen, zu ändern, zu pflegen oder zu übertragen, müssen entsprech ende Verfahren und Kontrollen anwenden, um die Echtheit, Integritä t und gegebenen falls die Vertrauli chkeit elektroni scher Aufzeichn ungen sicherzus tellen und dafür zu sorgen, dass die Unterzeichneten die signierte Aufzeichn ung nicht ohne Weiteres als unecht zurückweisen können. Diese Verfahren und Kontrollen müssen Folgendes umfassen: (c) Schutz der Aufzeichnungen, damit sie während der gesamten Aufbewahr ungsfrist fehlerfrei und	rds-snapshots-public-prohibited	Verwalten Sie den Zugriff auf Ressource n in der AWS Cloud, indem Sie sicherste llen, dass Amazon Relational Database Service (Amazon RDS) -Instance s nicht öffentlic h sind. Amazon-RDS-Datenbank-Instances können vertrauliche Informati onen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	problemlos abgerufen werden können.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
11.10(c)	Personen, die geschlossene Systeme verwenden, um elektronische Aufzeichnungen zu erstellen, zu ändern, zu pflegen oder zu übertragen, müssen entsprechende Verfahren und Kontrollen anwenden, um die Echtheit, Integrität und gegebenenfalls die Vertraulichkeit elektronischer Aufzeichnungen sicherzustellen und dafür zu sorgen, dass die Unterzeichneten die signierte Aufzeichnung nicht ohne Weiteres als unecht zurückweisen können. Diese Verfahren und Kontrollen müssen Folgendes umfassen: (c) Schutz der Aufzeichnungen, damit sie während der gesamten Aufbewahrungsfrist fehlerfrei und	rds-storage-encrypted	Zum Schutz von Daten im Ruhezustand müssen Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon Relational Database Service (Amazon RDS)-Instances aktiviert ist. Um eventuell vorhandene sensible Daten im Ruhezustand in Amazon-RDS-Instances zu schützen, muss die Verschlüsselung von Daten im Ruhezustand aktiviert sein.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	problemlos abgerufen werden können.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
11.10(c)	Personen, die geschlossene Systeme verwenden , um elektronische Aufzeichnungen zu erstellen, zu ändern, zu pflegen oder zu übertragen, müssen entsprech ende Verfahren und Kontrollen anwenden, um die Echtheit, Integritä t und gegebenen falls die Vertrauli chkeit elektroni scher Aufzeichn ungen sicherzus tellen und dafür zu sorgen, dass die Unterzeichneten die signierte Aufzeichn ung nicht ohne Weiteres als unecht zurückweisen können. Diese Verfahren und Kontrollen müssen Folgendes umfassen: (c) Schutz der Aufzeichnungen, damit sie während der gesamten Aufbewahr ungsfrist fehlerfrei und	redshift-cluster-c onfiguration-check	Um Daten im Ruhezustand zu schützen, muss die Verschlüsselung für Ihre Amazon-Re dshift-Cluster aktiviert sein. Sie müssen auch sicherstellen, dass die erforderl ichen Konfigurationen auf Amazon-Redshift-Clustern bereitges tellt werden. Die Prüfungsprotokolli erung muss aktiviert sein, um Informati onen zu Verbindun gen und Benutzera ktivitäten in der Datenbank bereitzus tellen. Diese Regel erfordert, dass ein Wert für clusterDb Encrypted (Config Default: TRUE) und LoggingEnabled (Config Default: TRUE) gesetzt ist. Die tatsächlichen Werte müssen den Richtlini en Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	problemlos abgerufen werden können.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
11.10(c)	Personen, die geschlossene Systeme verwenden , um elektronische Aufzeichnungen zu erstellen, zu ändern, zu pflegen oder zu übertragen, müssen entsprech ende Verfahren und Kontrollen anwenden, um die Echtheit, Integritä t und gegebenen falls die Vertrauli chkeit elektroni scher Aufzeichn ungen sicherzus tellen und dafür zu sorgen, dass die Unterzeichneten die signierte Aufzeichn ung nicht ohne Weiteres als unecht zurückweisen können. Diese Verfahren und Kontrollen müssen Folgendes umfassen: (c) Schutz der Aufzeichnungen, damit sie während der gesamten Aufbewahr ungsfrist fehlerfrei und	redshift-cluster-public-access-überprüfen	Verwalten Sie den Zugriff auf Ressource n in der AWS Cloud, indem Sie sicherste llen, dass Amazon Redshift Redshift-Cluster nicht öffentlic h sind. Amazon-Re dshift-Cluster können vertrauliche Informati onen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	problemlos abgerufen werden können.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
11.10(c)	Personen, die geschlossene Systeme verwenden , um elektronische Aufzeichnungen zu erstellen, zu ändern, zu pflegen oder zu übertragen, müssen entsprech ende Verfahren und Kontrollen anwenden, um die Echtheit, Integritä t und gegebenen falls die Vertrauli chkeit elektroni scher Aufzeichn ungen sicherzus tellen und dafür zu sorgen, dass die Unterzeichneten die signierte Aufzeichn ung nicht ohne Weiteres als unecht zurückweisen können. Diese Verfahren und Kontrollen müssen Folgendes umfassen: (c) Schutz der Aufzeichnungen, damit sie während der gesamten Aufbewahr ungsfrist fehlerfrei und	redshift-require-tls-ssl	Stellen Sie sicher, dass Ihre Amazon-Redshift-Cluster eine TLS/SSL-Verschlüss elung erfordern, um eine Verbindun g zu SQL-Clients herzustellen. Um eventuell vorhanden e sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	problemlos abgerufen werden können.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
11.10(c)	Personen, die geschlossene Systeme verwenden , um elektronische Aufzeichnungen zu erstellen, zu ändern, zu pflegen oder zu übertragen, müssen entsprech ende Verfahren und Kontrollen anwenden, um die Echtheit, Integritä t und gegebenen falls die Vertrauli chkeit elektroni scher Aufzeichn ungen sicherzus tellen und dafür zu sorgen, dass die Unterzeichneten die signierte Aufzeichn ung nicht ohne Weiteres als unecht zurückweisen können. Diese Verfahren und Kontrollen müssen Folgendes umfassen: (c) Schutz der Aufzeichnungen, damit sie während der gesamten Aufbewahr ungsfrist fehlerfrei und	s-3 bucket-public-read -prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie nur autorisierten Benutzern, Prozessen und Geräten Zugriff auf Amazon Simple Storage Service (Amazon S3) - Buckets gewähren. Die Verwaltung des Zugriffs sollte mit der Klassifizierung der Daten übereinst immen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	problemlos abgerufen werden können.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
11.10(c)	Personen, die geschlossene Systeme verwenden , um elektronische Aufzeichnungen zu erstellen, zu ändern, zu pflegen oder zu übertragen, müssen entsprech ende Verfahren und Kontrollen anwenden, um die Echtheit, Integritä t und gegebenen falls die Vertrauli chkeit elektroni scher Aufzeichn ungen sicherzus tellen und dafür zu sorgen, dass die Unterzeichneten die signierte Aufzeichn ung nicht ohne Weiteres als unecht zurückweisen können. Diese Verfahren und Kontrollen müssen Folgendes umfassen: (c) Schutz der Aufzeichnungen, damit sie während der gesamten Aufbewahr ungsfrist fehlerfrei und	s3- bucket-public-writ e-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie nur autorisierten Benutzern, Prozessen und Geräten Zugriff auf Amazon Simple Storage Service (Amazon S3) - Buckets gewähren. Die Verwaltung des Zugriffs sollte mit der Klassifizierung der Daten übereinst immen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	problemlos abgerufen werden können.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
11.10(c)	Personen, die geschlossene Systeme verwenden, um elektronische Aufzeichnungen zu erstellen, zu ändern, zu pflegen oder zu übertragen, müssen entsprechende Verfahren und Kontrollen anwenden, um die Echtheit, Integrität und gegebenenfalls die Vertraulichkeit elektronischer Aufzeichnungen sicherzustellen und dafür zu sorgen, dass die Unterzeichneten die signierte Aufzeichnung nicht ohne Weiteres als unecht zurückweisen können. Diese Verfahren und Kontrollen müssen Folgendes umfassen: (c) Schutz der Aufzeichnungen, damit sie während der gesamten Aufbewahrungsfrist fehlerfrei und	s3-fähig bucket-server-side-encryption	Zum Schutz von Daten im Ruhezustand müssen Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon Simple Storage Service (Amazon S3)-Buckets aktiviert ist. Um eventuell vorhandene sensible Daten im Ruhezustand in Amazon-S3-Buckets zu schützen, muss die Verschlüsselung aktiviert sein.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	problemlos abgerufen werden können.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
11.10(c)	Personen, die geschlossene Systeme verwenden , um elektronische Aufzeichnungen zu erstellen, zu ändern, zu pflegen oder zu übertragen, müssen entsprech ende Verfahren und Kontrollen anwenden, um die Echtheit, Integritä t und gegebenen falls die Vertrauli chkeit elektroni scher Aufzeichn ungen sicherzus tellen und dafür zu sorgen, dass die Unterzeichneten die signierte Aufzeichn ung nicht ohne Weiteres als unecht zurückweisen können. Diese Verfahren und Kontrollen müssen Folgendes umfassen: (c) Schutz der Aufzeichnungen, damit sie während der gesamten Aufbewahr ungsfrist fehlerfrei und	s-3 bucket-ssl-request s-only	Um Daten während der Übertragung zu schützen, stellen Sie sicher, dass Ihre Amazon Simple Storage Service (Amazon S3)-Bucke ts Anfragen zur Verwendung von Secure Socket Layer (SSL)-Buc kets erfordern. Um eventuell vorhanden e sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	problemlos abgerufen werden können.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
11.10(c)	Personen, die geschlossene Systeme verwenden , um elektronische Aufzeichnungen zu erstellen, zu ändern, zu pflegen oder zu übertragen, müssen entsprech ende Verfahren und Kontrollen anwenden, um die Echtheit, Integritä t und gegebenen falls die Vertrauli chkeit elektroni scher Aufzeichn ungen sicherzus tellen und dafür zu sorgen, dass die Unterzeichneten die signierte Aufzeichn ung nicht ohne Weiteres als unecht zurückweisen können. Diese Verfahren und Kontrollen müssen Folgendes umfassen: (c) Schutz der Aufzeichnungen, damit sie während der gesamten Aufbewahr ungsfrist fehlerfrei und	s-3 bucket-versioning-enabled	Die Versionsv erwaltung von Amazon Simple Storage Service (Amazon S3)-Bucke ts hilft dabei, mehrere Varianten eines Objekts im selben Amazon-S3-Bucket zu speichern. Verwenden Sie die Versionsv erwaltung, um sämtliche Versionen aller Objekte in Ihrem Amazon-S3-Bucket zu speichern , abzurufen oder wiederherzustellen . Mit der Versionsv erwaltung können Sie Versionen sowohl nach unbeabsic htigten Benutzera ktionen als auch nach Anwendungsfehlern problemlos wiederher stellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	problemlos abgerufen werden können.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
11.10(c)	Personen, die geschlossene Systeme verwenden , um elektronische Aufzeichnungen zu erstellen, zu ändern, zu pflegen oder zu übertragen, müssen entsprech ende Verfahren und Kontrollen anwenden, um die Echtheit, Integritä t und gegebenen falls die Vertrauli chkeit elektroni scher Aufzeichn ungen sicherzus tellen und dafür zu sorgen, dass die Unterzeichneten die signierte Aufzeichn ung nicht ohne Weiteres als unecht zurückweisen können. Diese Verfahren und Kontrollen müssen Folgendes umfassen: (c) Schutz der Aufzeichnungen, damit sie während der gesamten Aufbewahr ungsfrist fehlerfrei und	s-3 version-lifecycle-policy-check	Mit Amazon-S3-Lebenszyklusregeln können Sie Aktionen definieren, die Amazon S3 während der Lebensdau er eines Objekts ausführen soll (z. B. die Überführu ng von Objekten in eine andere Speicherklasse, ihre Archivierung oder Löschung nach einem bestimmten Zeitraum) .

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	problemlos abgerufen werden können.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
11.10(c)	Personen, die geschlossene Systeme verwenden , um elektronische Aufzeichnungen zu erstellen, zu ändern, zu pflegen oder zu übertragen, müssen entsprech ende Verfahren und Kontrollen anwenden, um die Echtheit, Integritä t und gegebenen falls die Vertrauli chkeit elektroni scher Aufzeichn ungen sicherzus tellen und dafür zu sorgen, dass die Unterzeichneten die signierte Aufzeichn ung nicht ohne Weiteres als unecht zurückweisen können. Diese Verfahren und Kontrollen müssen Folgendes umfassen: (c) Schutz der Aufzeichnungen, damit sie während der gesamten Aufbewahr ungsfrist fehlerfrei und	sagemaker-endpoint -configuration-kms- key-konfiguriert	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass die Verschlüsselung mit dem AWS Key Management Service (AWS KMS) für Ihren Endpunkt aktiviert ist. SageMaker Da sensible Daten auf dem SageMaker Endgerät gespeiche rt werden können, sollten Sie die Verschlüsselung im Ruhezustand aktiviere n, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	problemlos abgerufen werden können.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
11.10(c)	Personen, die geschlossene Systeme verwenden , um elektronische Aufzeichnungen zu erstellen, zu ändern, zu pflegen oder zu übertragen, müssen entsprech ende Verfahren und Kontrollen anwenden, um die Echtheit, Integritä t und gegebenen falls die Vertrauli chkeit elektroni scher Aufzeichn ungen sicherzus tellen und dafür zu sorgen, dass die Unterzeichneten die signierte Aufzeichn ung nicht ohne Weiteres als unecht zurückweisen können. Diese Verfahren und Kontrollen müssen Folgendes umfassen: (c) Schutz der Aufzeichnungen, damit sie während der gesamten Aufbewahr ungsfrist fehlerfrei und	sagemaker-notebook -instance-kms-schl üsselkonfiguriert	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass die Verschlüsselung mit dem AWS Key Management Service (AWS KMS) für Ihr Notebook aktiviert ist. SageMaker Da vertrauliche Daten im SageMaker Notebook gespeichert werden können, sollten Sie die Verschlüsselung im Ruhezustand aktivieren, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	problemlos abgerufen werden können.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
11.10(c)	Personen, die geschlossene Systeme verwenden, um elektronische Aufzeichnungen zu erstellen, zu ändern, zu pflegen oder zu übertragen, müssen entsprechende Verfahren und Kontrollen anwenden, um die Echtheit, Integrität und gegebenenfalls die Vertraulichkeit elektronischer Aufzeichnungen sicherzustellen und dafür zu sorgen, dass die Unterzeichneten die signierte Aufzeichnung nicht ohne Weiteres als unecht zurückweisen können. Diese Verfahren und Kontrollen müssen Folgendes umfassen: (c) Schutz der Aufzeichnungen, damit sie während der gesamten Aufbewahrungsfrist fehlerfrei und	sagemaker-notebook-no-direct-Internetzugang	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass SageMaker Amazon-Notebooks keinen direkten Internetzugang zulassen. Indem Sie direkten Internetzugang blockieren, vermeiden Sie, dass unbefugte Benutzer auf sensible Daten zugreifen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	problemlos abgerufen werden können.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
11.10(d)	Personen, die geschlossene Systeme verwenden , um elektronische Aufzeichnungen zu erstellen, zu ändern, zu pflegen oder zu übertragen, müssen entsprech ende Verfahren und Kontrollen anwenden, um die Echtheit, Integritä t und gegebenen falls die Vertrauli chkeit elektronischer Aufzeichnungen sicherzustellen und dafür zu sorgen, dass die Unterzeic hneten die signierte Aufzeichnung nicht ohne Weiteres als unecht zurückwei sen können. Diese Verfahren und Kontrollen müssen Folgendes umfassen: (d) Beschränkung des Systemzugriffs auf autorisierte Personen.	access-keys-rotated	Die Anmeldein formationen für autorisierte Geräte, Benutzer und Prozesse werden geprüft, indem sichergestellt wird, dass die IAM-Zugri ffsschlüssel entsprech end den Vorgaben der Unternehmensrichtl inie rotiert werden. Das regelmäßi ge Ändern der Zugriffsschlüssel ist eine bewährte Sicherheitsmethode . Es verkürzt den Zeitraum, in dem ein Zugriffsschlüssel aktiv ist, und reduziert die Auswirkungen auf das Unternehmen, wenn die Schlüssel kompromittiert werden. Diese Regel erfordert einen Wert für die Zugriffsschlüssel-Rotation (Standard konfiguration: 90). Der tatsächliche Wert muss den Richtlini

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			en Ihrer Organisation entsprechen.
11.10(d)	Personen, die geschlossene Systeme verwenden, um elektronische Aufzeichnungen zu erstellen, zu ändern, zu pflegen oder zu übertragen, müssen entsprechende Verfahren und Kontrollen anwenden, um die Echtheit, Integrität und gegebenenfalls die Vertraulichkeit elektronischer Aufzeichnungen sicherzustellen und dafür zu sorgen, dass die Unterzeichneten die signierte Aufzeichnung nicht ohne Weiteres als unecht zurückweisen können. Diese Verfahren und Kontrollen müssen Folgendes umfassen: (d) Beschränkung des Systemzugriffs auf autorisierte Personen.	account-part-of-organizations	Durch die zentrale Verwaltung AWS-Konten innerhalb von AWS Organizations wird sichergestellt, dass die Konten den Vorschriften entsprechen. Eine fehlende zentrale Kontoverwaltung kann zu inkonsistenten Kontokonfigurationen führen, wodurch Ressourcen und sensible Daten offengelegt werden können.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
11.10(d)	Personen, die geschlossene Systeme verwenden , um elektronische Aufzeichnungen zu erstellen, zu ändern, zu pflegen oder zu übertragen, müssen entsprech ende Verfahren und Kontrollen anwenden, um die Echtheit, Integritä t und gegebenen falls die Vertrauli chkeit elektronischer Aufzeichnungen sicherzustellen und dafür zu sorgen, dass die Unterzeic hneten die signierte Aufzeichnung nicht ohne Weiteres als unecht zurückwei sen können. Diese Verfahren und Kontrollen müssen Folgendes umfassen: (d) Beschränkung des Systemzugriffs auf autorisierte Personen.	dms-replication-not-public	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass auf DMS-Replikationsin stanzen nicht öffentlic h zugegriffen werden kann. DMS-Repli kations-Instances können vertrauli che Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
11.10(d)	Personen, die geschlossene Systeme verwenden, um elektronische Aufzeichnungen zu erstellen, zu ändern, zu pflegen oder zu übertragen, müssen entsprechende Verfahren und Kontrollen anwenden, um die Echtheit, Integrität und gegebenenfalls die Vertraulichkeit elektronischer Aufzeichnungen sicherzustellen und dafür zu sorgen, dass die Unterzeichneten die signierte Aufzeichnung nicht ohne Weiteres als unecht zurückweisen können. Diese Verfahren und Kontrollen müssen Folgendes umfassen: (d) Beschränkung des Systemzugriffs auf autorisierte Personen.	dynamodb-table-encrypted-kms	Stellen Sie sicher, dass die Verschlüsselung für Ihre Amazon-DynamoDB-Tabellen aktiviert ist. Um eventuell vorhandene sensible Daten im Ruhezustand in diesen Tabellen zu schützen, müssen Sie die Verschlüsselung von Daten im Ruhezustand aktivieren. Standardmäßig werden DynamoDB-Tabellen mit einem AWS eigenen Kundenhauptschlüssel (CMK) verschlüsselt.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
11.10(d)	Personen, die geschlossene Systeme verwenden , um elektronische Aufzeichnungen zu erstellen, zu ändern, zu pflegen oder zu übertragen, müssen entsprech ende Verfahren und Kontrollen anwenden, um die Echtheit, Integritä t und gegebenen falls die Vertrauli chkeit elektronischer Aufzeichnungen sicherzustellen und dafür zu sorgen, dass die Unterzeic hneten die signierte Aufzeichnung nicht ohne Weiteres als unecht zurückwei sen können. Diese Verfahren und Kontrollen müssen Folgendes umfassen: (d) Beschränkung des Systemzugriffs auf autorisierte Personen.	ebs-snapshot-public-restorable-überprüfen	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass EBS-Snapshots nicht öffentlich wiederher stellbar sind. EBS-Volume-Snapsho ts können vertrauli che Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
11.10(d)	Personen, die geschlossene Systeme verwenden, um elektronische Aufzeichnungen zu erstellen, zu ändern, zu pflegen oder zu übertragen, müssen entsprechende Verfahren und Kontrollen anwenden, um die Echtheit, Integrität und gegebenenfalls die Vertraulichkeit elektronischer Aufzeichnungen sicherzustellen und dafür zu sorgen, dass die Unterzeichneten die signierte Aufzeichnung nicht ohne Weiteres als unecht zurückweisen können. Diese Verfahren und Kontrollen müssen Folgendes umfassen: (d) Beschränkung des Systemzugriffs auf autorisierte Personen.	ec-2 ebs-encryption-by-default	Zum Schutz von Daten im Ruhezustand müssen Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon Elastic Block Store (Amazon EBS)-Volumes aktiviert ist. Da sensible Daten auch im Ruhezustand vorhanden sein können, sollten Sie die Verschlüsselung im Ruhezustand aktivieren, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
11.10(d)	Personen, die geschlossene Systeme verwenden , um elektronische Aufzeichnungen zu erstellen, zu ändern, zu pflegen oder zu übertragen, müssen entsprech ende Verfahren und Kontrollen anwenden, um die Echtheit, Integritä t und gegebenen falls die Vertrauli chkeit elektronischer Aufzeichnungen sicherzustellen und dafür zu sorgen, dass die Unterzeic hneten die signierte Aufzeichnung nicht ohne Weiteres als unecht zurückwei sen können. Diese Verfahren und Kontrollen müssen Folgendes umfassen: (d) Beschränkung des Systemzugriffs auf autorisierte Personen.	ec2-imdsv2-check	Stellen Sie sicher, dass die Methode Instance Metadata Service Version 2 (IMDSv2) aktiviert ist, um den Zugriff auf und die Kontrolle der Amazon Elastic Compute Cloud (Amazon EC2) - Instance-Metadate n zu schützen. Die IMDSv2 Methode verwendet sitzungsb asierte Kontrollen. Mit können Kontrolle n implementiert werden IMDSv2, um Änderungen an Instanzmetadaten einzuschränken.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
11.10(d)	Personen, die geschlossene Systeme verwenden , um elektronische Aufzeichnungen zu erstellen, zu ändern, zu pflegen oder zu übertragen, müssen entsprech ende Verfahren und Kontrollen anwenden, um die Echtheit, Integritä t und gegebenen falls die Vertrauli chkeit elektronischer Aufzeichnungen sicherzustellen und dafür zu sorgen, dass die Unterzeic hneten die signierte Aufzeichnung nicht ohne Weiteres als unecht zurückwei sen können. Diese Verfahren und Kontrollen müssen Folgendes umfassen: (d) Beschränkung des Systemzugriffs auf autorisierte Personen.	ec-2 instance-no-public-ip	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon Elastic Compute Cloud (Amazon EC2) - Instances nicht öffentlich zugänglich sind. EC2 Amazon-Instances können vertrauliche Informati onen enthalten, und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
11.10(d)	Personen, die geschlossene Systeme verwenden , um elektronische Aufzeichnungen zu erstellen, zu ändern, zu pflegen oder zu übertragen, müssen entsprech ende Verfahren und Kontrollen anwenden, um die Echtheit, Integritä t und gegebenen falls die Vertrauli chkeit elektronischer Aufzeichnungen sicherzustellen und dafür zu sorgen, dass die Unterzeic hneten die signierte Aufzeichnung nicht ohne Weiteres als unecht zurückwei sen können. Diese Verfahren und Kontrollen müssen Folgendes umfassen: (d) Beschränkung des Systemzugriffs auf autorisierte Personen.	ec2- instance-profile-a ttached	EC2 Instanzprofile übergeben eine IAM-Rolle an eine EC2 Instance. Das Anhängen eines Instance-Profils an Ihre Instances kann bei der Implement ierung von geringste n Berechtigungen und der Berechtig ungsverwaltung helfen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
11.10(d)	Personen, die geschlossene Systeme verwenden , um elektronische Aufzeichnungen zu erstellen, zu ändern, zu pflegen oder zu übertragen, müssen entsprech ende Verfahren und Kontrollen anwenden, um die Echtheit, Integritä t und gegebenen falls die Vertrauli chkeit elektronischer Aufzeichnungen sicherzustellen und dafür zu sorgen, dass die Unterzeic hneten die signierte Aufzeichnung nicht ohne Weiteres als unecht zurückwei sen können. Diese Verfahren und Kontrollen müssen Folgendes umfassen: (d) Beschränkung des Systemzugriffs auf autorisierte Personen.	ecs-task-definition-user-for-host-mode-check	Wenn für eine Aufgabendefinition erhöhte Berechtig ungen gelten, liegt das daran, dass der Kunde diesen Konfigura tionen ausdrücklich zugestimmt hat. Diese Kontrolle prüft, ob eine unerwartete Berechtigungseskal ation vorliegt, wenn für eine Aufgabend efinition das Host-Netzwerk aktiviert ist, die Kunden aber keine erhöhten Berechtigungen aktiviert haben.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
11.10(d)	Personen, die geschlossene Systeme verwenden , um elektronische Aufzeichnungen zu erstellen, zu ändern, zu pflegen oder zu übertragen, müssen entsprech ende Verfahren und Kontrollen anwenden, um die Echtheit, Integritä t und gegebenen falls die Vertrauli chkeit elektronischer Aufzeichnungen sicherzustellen und dafür zu sorgen, dass die Unterzeic hneten die signierte Aufzeichnung nicht ohne Weiteres als unecht zurückwei sen können. Diese Verfahren und Kontrollen müssen Folgendes umfassen: (d) Beschränkung des Systemzugriffs auf autorisierte Personen.	efs-encrypted-check	Aktivieren Sie die Verschlüsselung für Ihr Amazon Elastic File System (EFS), um eventuell vorhandene sensible Daten sowie Daten im Ruhezustand zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
11.10(d)	Personen, die geschlossene Systeme verwenden , um elektronische Aufzeichnungen zu erstellen, zu ändern, zu pflegen oder zu übertragen, müssen entsprech ende Verfahren und Kontrollen anwenden, um die Echtheit, Integritä t und gegebenen falls die Vertrauli chkeit elektronischer Aufzeichnungen sicherzustellen und dafür zu sorgen, dass die Unterzeic hneten die signierte Aufzeichnung nicht ohne Weiteres als unecht zurückwei sen können. Diese Verfahren und Kontrollen müssen Folgendes umfassen: (d) Beschränkung des Systemzugriffs auf autorisierte Personen.	elasticsearch-encr ypted-at-rest	Da sensible Daten vorhanden sein können und um Daten im Ruhezustand zu schützen, sollten Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon OpenSearch Service (OpenSearch Service) -Domains aktiviert ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
11.10(d)	Personen, die geschlossene Systeme verwenden , um elektronische Aufzeichnungen zu erstellen, zu ändern, zu pflegen oder zu übertragen, müssen entsprech ende Verfahren und Kontrollen anwenden, um die Echtheit, Integritä t und gegebenen falls die Vertrauli chkeit elektronischer Aufzeichnungen sicherzustellen und dafür zu sorgen, dass die Unterzeic hneten die signierte Aufzeichnung nicht ohne Weiteres als unecht zurückwei sen können. Diese Verfahren und Kontrollen müssen Folgendes umfassen: (d) Beschränkung des Systemzugriffs auf autorisierte Personen.	elasticsearch-in-vpc-only	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherste llen, dass sich Amazon OpenSearc h OpenSearch Service (Service) - Domains innerhalb einer Amazon Virtual Private Cloud (Amazon VPC) befinden. Eine OpenSearch Service-Domain innerhalb einer Amazon VPC ermöglicht die sichere Kommunikation zwischen OpenSearc h Service und anderen Services innerhalb der Amazon VPC, ohne dass ein Internet-Gateway, ein NAT-Gerät oder eine VPN-Verbindung erforderlich ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
11.10(d)	Personen, die geschlossene Systeme verwenden , um elektronische Aufzeichnungen zu erstellen, zu ändern, zu pflegen oder zu übertragen, müssen entsprech ende Verfahren und Kontrollen anwenden, um die Echtheit, Integritä t und gegebenen falls die Vertrauli chkeit elektronischer Aufzeichnungen sicherzustellen und dafür zu sorgen, dass die Unterzeic hneten die signierte Aufzeichnung nicht ohne Weiteres als unecht zurückwei sen können. Diese Verfahren und Kontrollen müssen Folgendes umfassen: (d) Beschränkung des Systemzugriffs auf autorisierte Personen.	elasticsearch-node -to-node-Verschlüs selungsprüfung	Stellen Sie sicher, dass die node-to-node Verschlüs selung für Amazon OpenSearch Service aktiviert ist. Node-to-nodeVerschlüsselung ermöglicht die TLS 1.2-Verschlüsselun g für die gesamte Kommunikation innerhalb der Amazon Virtual Private Cloud (Amazon VPC). Um eventuell vorhanden e sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
11.10(d)	Personen, die geschlossene Systeme verwenden , um elektronische Aufzeichnungen zu erstellen, zu ändern, zu pflegen oder zu übertragen, müssen entsprech ende Verfahren und Kontrollen anwenden, um die Echtheit, Integritä t und gegebenen falls die Vertrauli chkeit elektronischer Aufzeichnungen sicherzustellen und dafür zu sorgen, dass die Unterzeic hneten die signierte Aufzeichnung nicht ohne Weiteres als unecht zurückwei sen können. Diese Verfahren und Kontrollen müssen Folgendes umfassen: (d) Beschränkung des Systemzugriffs auf autorisierte Personen.	emr-kerberos-enabled	Die Zugriffsberechtigu ngen und -autorisi erungen können verwaltet und nach den Prinzipien der geringsten Berechtig ung und Aufgabent rennung integrier t werden, indem Kerberos für Amazon-EMR-Cluster aktiviert wird. In Kerberos werden Services und Benutzer, die sich authentif izieren müssen, als Prinzipale bezeichnet. Prinzipal e befinden sich in einem Kerberos-Bereich. Innerhalb dieses Bereichs wird ein Kerberos-Server als Key Distribution Center (KDC) bezeichnet. Über diesen Server können sich Prinzipal e authentifizieren. Die Authentifizierung im KDC erfolgt durch die Ausstellu ng von Authentif

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			izierungstickets. Das KDC unterhält eine Datenbank der Prinzipale in seinem Bereich mit ihren Passwörtern und anderen administr ativen Informationen zu jedem Prinzipal.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
11.10(d)	Personen, die geschlossene Systeme verwenden , um elektronische Aufzeichnungen zu erstellen, zu ändern, zu pflegen oder zu übertragen, müssen entsprech ende Verfahren und Kontrollen anwenden, um die Echtheit, Integritä t und gegebenen falls die Vertrauli chkeit elektronischer Aufzeichnungen sicherzustellen und dafür zu sorgen, dass die Unterzeic hneten die signierte Aufzeichnung nicht ohne Weiteres als unecht zurückwei sen können. Diese Verfahren und Kontrollen müssen Folgendes umfassen: (d) Beschränkung des Systemzugriffs auf autorisierte Personen.	emr-master-no-public-ip	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon EMR-Clust er-Masterknoten nicht öffentlich zugänglic h sind. Amazon-EM R-Cluster-Hauptkno ten können vertrauli che Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
11.10(d)	Personen, die geschlossene Systeme verwenden , um elektronische Aufzeichnungen zu erstellen, zu ändern, zu pflegen oder zu übertragen, müssen entsprech ende Verfahren und Kontrollen anwenden, um die Echtheit, Integritä t und gegebenen falls die Vertrauli chkeit elektronischer Aufzeichnungen sicherzustellen und dafür zu sorgen, dass die Unterzeic hneten die signierte Aufzeichnung nicht ohne Weiteres als unecht zurückwei sen können. Diese Verfahren und Kontrollen müssen Folgendes umfassen: (d) Beschränkung des Systemzugriffs auf autorisierte Personen.	encrypted-volumes	Aktivieren Sie die Verschlüsselung für Ihre Amazon-Elastic-Block-Store (Amazon-EBS)-Volumes, um eventuell vorhandene sensible Daten sowie Daten im Ruhezusta nd zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
11.10(d)	Personen, die geschlossene Systeme verwenden, um elektronische Aufzeichnungen zu erstellen, zu ändern, zu pflegen oder zu übertragen, müssen entsprechende Verfahren und Kontrollen anwenden, um die Echtheit, Integrität und gegebenenfalls die Vertraulichkeit elektronischer Aufzeichnungen sicherzustellen und dafür zu sorgen, dass die Unterzeichneten die signierte Aufzeichnung nicht ohne Weiteres als unecht zurückweisen können. Diese Verfahren und Kontrollen müssen Folgendes umfassen: (d) Beschränkung des Systemzugriffs auf autorisierte Personen.	iam-customer-policy-blocked-kms-Aktionen	AWS Identity and Access Management (IAM) kann Ihnen helfen, die Prinzipien der geringsten Rechte und der Aufgabentrennung in Zugriffsberechtigungen und Autorisierungen zu integrieren und so zu verhindern, dass Richtlinien blockierte Aktionen für alle AWS Schlüssel des Key Management Service enthalten. Wenn Benutzer mehr Rechte haben, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und Aufgabentrennung verstoßen. Mit dieser Regel können Sie den Parameter festlegen. blockedActionsPatterns (Wert „AWS Bewährte grundlegende Sicherheitsmethoden“: kms:

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			Decrypt, kms:ReEncryptFrom). Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
11.10(d)	Personen, die geschlossene Systeme verwenden, um elektronische Aufzeichnungen zu erstellen, zu ändern, zu pflegen oder zu übertragen, müssen entsprechende Verfahren und Kontrollen anwenden, um die Echtheit, Integrität und gegebenenfalls die Vertraulichkeit elektronischer Aufzeichnungen sicherzustellen und dafür zu sorgen, dass die Unterzeichneten die signierte Aufzeichnung nicht ohne Weiteres als unecht zurückweisen können. Diese Verfahren und Kontrollen müssen Folgendes umfassen: (d) Beschränkung des Systemzugriffs auf autorisierte Personen.	iam-group-has-users-überprüfen	AWS Identity and Access Management (IAM) kann Ihnen helfen, die Prinzipien der geringsten Rechte und der Aufgabentrennung mit Zugriffsberechtigungen und Autorisierungen zu integrieren, indem sichergestellt wird, dass IAM-Gruppen mindestens einen Benutzer haben. Die Einteilung von Benutzern in Gruppen auf der Grundlage der ihnen zugewiesenen Berechtigungen oder ihrer Funktion ist eine Möglichkeit, das Prinzip der geringsten Berechtigung zu implementieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
11.10(d)	Personen, die geschlossene Systeme verwenden , um elektronische Aufzeichnungen zu erstellen, zu ändern, zu pflegen oder zu übertragen, müssen entsprech ende Verfahren und Kontrollen anwenden, um die Echtheit, Integritä t und gegebenen falls die Vertrauli chkeit elektronischer Aufzeichnungen sicherzustellen und dafür zu sorgen, dass die Unterzeic hneten die signierte Aufzeichnung nicht ohne Weiteres als unecht zurückwei sen können. Diese Verfahren und Kontrollen müssen Folgendes umfassen: (d) Beschränkung des Systemzugriffs auf autorisierte Personen.	iam-inline-policy-blocked-kms-Aktionen	Stellen Sie sicher, dass ein Benutzer, eine IAM-Rolle oder eine IAM-Gruppe (AWS Identity and Access Management) nicht über eine Inline-Richtlinie verfügt, die blockierte Aktionen für alle AWS Schlüssel des Key Management Service zulässt. AWS empfiehlt, verwaltet e Richtlinien anstelle von Inline-Richtlinien zu verwenden. Verwaltete Richtlini en ermöglichen Wiederverwendbarke it, Versionsverwaltung , Rollback und Delegierung der Berechtigungsverwa ltung. Mit dieser Regel können Sie den blockedActionsPatt erns Parameter festlegen. (Wert „AWS Bewährte grundlege nde Sicherhei tsmethoden“: kms: Decrypt, kms:ReEnc ryptFrom). Die

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
11.10(d)	Personen, die geschlossene Systeme verwenden , um elektronische Aufzeichnungen zu erstellen, zu ändern, zu pflegen oder zu übertragen, müssen entsprech ende Verfahren und Kontrollen anwenden, um die Echtheit, Integritä t und gegebenen falls die Vertrauli chkeit elektronischer Aufzeichnungen sicherzustellen und dafür zu sorgen, dass die Unterzeic hneten die signierte Aufzeichnung nicht ohne Weiteres als unecht zurückwei sen können. Diese Verfahren und Kontrollen müssen Folgendes umfassen: (d) Beschränkung des Systemzugriffs auf autorisierte Personen.	iam-no-inline-policy-überprüfen	Stellen Sie sicher, dass ein Benutzer, eine IAM-Rolle oder eine IAM-Gruppe (AWS Identity and Access Management) nicht über eine Inline-Richtlinie zur Zugriffsk ontrolle auf Systeme und Ressource n verfügt. AWS empfiehlt, verwaltet e Richtlinien anstelle von Inline-Richtlinien zu verwenden. Verwaltete Richtlini en ermöglichen Wiederverwendbarke it, Versionsverwaltung , Rollback und Delegierung der Berechtigungsverwa ltung.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
11.10(d)	Personen, die geschlossene Systeme verwenden , um elektronische Aufzeichnungen zu erstellen, zu ändern, zu pflegen oder zu übertragen, müssen entsprech ende Verfahren und Kontrollen anwenden, um die Echtheit, Integritä t und gegebenen falls die Vertrauli chkeit elektronischer Aufzeichnungen sicherzustellen und dafür zu sorgen, dass die Unterzeic hneten die signierte Aufzeichnung nicht ohne Weiteres als unecht zurückwei sen können. Diese Verfahren und Kontrollen müssen Folgendes umfassen: (d) Beschränkung des Systemzugriffs auf autorisierte Personen.	iam-password-policy	Die Identitäten und Anmeldeinformation en werden auf der Grundlage einer organisatorischen IAM-Passwortrichtlinie ausgestellt, verwaltet und verifiziert. Sie erfüllen oder übertreff en die Anforderungen von NIST SP 800-63 und dem Standard „Best Practices“ von AWS Foundatio nal Security für die Passwortstärke. Mit dieser Regel können Sie optional RequireUppercaseCh aracters (Wert für AWS grundlegende Sicherheitsbewährt e Methoden: wahr), RequireLowercaseCh aracters (Wert für bewährte Methoden für AWS grundlege nde Sicherheit: wahr), RequireSy mbols (Wert für bewährte Methoden für AWS grundlege nde Sicherheit:

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			wahr), RequireNumbers (Wert für bewährte Methoden für AWS grundlegende Sicherheit: wahr), MinimumPasswordLength (Wert für bewährte Methoden für AWS grundlegende Sicherheit: 14), PasswordReusePrevention (Wert für bewährte Methoden für AWS grundlegende Sicherheit: 24) und MaxPasswordAge (Wert für bewährte Methoden für AWS grundlegende Sicherheit: 90) für Ihr IAM festlegen. Kennwortrichtlinie. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
11.10(d)	Personen, die geschlossene Systeme verwenden, um elektronische Aufzeichnungen zu erstellen, zu ändern, zu pflegen oder zu übertragen, müssen entsprechende Verfahren und Kontrollen anwenden, um die Echtheit, Integrität und gegebenenfalls die Vertraulichkeit elektronischer Aufzeichnungen sicherzustellen und dafür zu sorgen, dass die Unterzeichneten die signierte Aufzeichnung nicht ohne Weiteres als unecht zurückweisen können. Diese Verfahren und Kontrollen müssen Folgendes umfassen: (d) Beschränkung des Systemzugriffs auf autorisierte Personen.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) kann Ihnen dabei helfen, die Prinzipien der geringsten Rechte und der Aufgabentrennung in Zugriffsberechtigungen und Autorisierungen zu integrieren und so zu verhindern, dass Richtlinien „Effect“: „Allow“ mit „Action“: „*“ anstelle von „Resource“: „*“ enthalten. Wenn Benutzern mehr Rechte eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und der Aufgabentrennung verstoßen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
11.10(d)	Personen, die geschlossene Systeme verwenden, um elektronische Aufzeichnungen zu erstellen, zu ändern, zu pflegen oder zu übertragen, müssen entsprechende Verfahren und Kontrollen anwenden, um die Echtheit, Integrität und gegebenenfalls die Vertraulichkeit elektronischer Aufzeichnungen sicherzustellen und dafür zu sorgen, dass die Unterzeichneten die signierte Aufzeichnung nicht ohne Weiteres als unecht zurückweisen können. Diese Verfahren und Kontrollen müssen Folgendes umfassen: (d) Beschränkung des Systemzugriffs auf autorisierte Personen.	iam-policy-no-statements-with-full-access	Stellen Sie sicher, dass IAM-Aktionen nur auf die benötigten Aktionen beschränkt sind. Wenn Benutzern mehr Rechte eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und der Aufgabentrennung verstoßen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
11.10(d)	Personen, die geschlossene Systeme verwenden , um elektronische Aufzeichnungen zu erstellen, zu ändern, zu pflegen oder zu übertragen, müssen entsprech ende Verfahren und Kontrollen anwenden, um die Echtheit, Integritä t und gegebenen falls die Vertrauli chkeit elektronischer Aufzeichnungen sicherzustellen und dafür zu sorgen, dass die Unterzeic hneten die signierte Aufzeichnung nicht ohne Weiteres als unecht zurückwei sen können. Diese Verfahren und Kontrollen müssen Folgendes umfassen: (d) Beschränkung des Systemzugriffs auf autorisierte Personen.	iam-root-access-key-überprüfen	Der Zugriff auf Systeme und Ressourcen kann gesteuert werden, indem überprüft wird, ob der Root-Benu tzer keine Zugriffss chlüssel mit seiner AWS Identity and Access Management (IAM) -Rolle verknüpft hat. Stellen Sie sicher, dass die Root-Zugr iffsschlüssel gelöscht werden. Erstellen und verwenden Sie stattdessen rollenbas ierte Funktionen, AWS-Konten um das Prinzip der geringste n Funktionalität zu berücksichtigen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
11.10(d)	Personen, die geschlossene Systeme verwenden, um elektronische Aufzeichnungen zu erstellen, zu ändern, zu pflegen oder zu übertragen, müssen entsprechende Verfahren und Kontrollen anwenden, um die Echtheit, Integrität und gegebenenfalls die Vertraulichkeit elektronischer Aufzeichnungen sicherzustellen und dafür zu sorgen, dass die Unterzeichneten die signierte Aufzeichnung nicht ohne Weiteres als unecht zurückweisen können. Diese Verfahren und Kontrollen müssen Folgendes umfassen: (d) Beschränkung des Systemzugriffs auf autorisierte Personen.	iam-user-group-membership-überprüfen	AWS Identity and Access Management (IAM) kann Ihnen helfen, Zugriffsberechtigungen und Autorisierungen einzuschränken, indem sichergestellt wird, dass Benutzer Mitglieder mindestens einer Gruppe sind. Wenn Benutzern mehr Berechtigungen eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und Aufgabentrennung verstoßen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
11.10(d)	Personen, die geschlossene Systeme verwenden , um elektronische Aufzeichnungen zu erstellen, zu ändern, zu pflegen oder zu übertragen, müssen entsprech ende Verfahren und Kontrollen anwenden, um die Echtheit, Integritä t und gegebenen falls die Vertrauli chkeit elektronischer Aufzeichnungen sicherzustellen und dafür zu sorgen, dass die Unterzeic hneten die signierte Aufzeichnung nicht ohne Weiteres als unecht zurückwei sen können. Diese Verfahren und Kontrollen müssen Folgendes umfassen: (d) Beschränkung des Systemzugriffs auf autorisierte Personen.	iam-user-mfa-enabled	Aktivieren Sie diese Regel, um den Zugriff auf Ressourcen in der AWS Cloud einzuschr änken. Diese Regel sorgt dafür, dass die Multi-Faktor-Authe ntifizierung (MFA) für alle Benutzer aktiviert ist. MFA sorgt für eine weitere Schutzebe ne zusätzlich zu den Anmeldeinformation en. Reduzieren Sie Fälle von kompromit tierten Konten, indem Sie MFA für Benutzer vorschreiben.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
11.10(d)	Personen, die geschlossene Systeme verwenden , um elektronische Aufzeichnungen zu erstellen, zu ändern, zu pflegen oder zu übertragen, müssen entsprech ende Verfahren und Kontrollen anwenden, um die Echtheit, Integritä t und gegebenen falls die Vertrauli chkeit elektronischer Aufzeichnungen sicherzustellen und dafür zu sorgen, dass die Unterzeic hneten die signierte Aufzeichnung nicht ohne Weiteres als unecht zurückwei sen können. Diese Verfahren und Kontrollen müssen Folgendes umfassen: (d) Beschränkung des Systemzugriffs auf autorisierte Personen.	iam-user-no-policies-überprüfen	Diese Regel stellt sicher, dass AWS Identity and Access Management (IAM) -Richtlinien nur Gruppen oder Rollen zugewiese n werden, um den Zugriff auf Systeme und Ressourcen zu kontrollieren. Die Zuweisung von Berechtig ungen auf Gruppen- oder Rollenebene trägt dazu bei, die Wahrscheinlichkeit zu verringern, dass eine Identität übermäßige Berechtigungen erhält oder beibehält.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
11.10(d)	Personen, die geschlossene Systeme verwenden, um elektronische Aufzeichnungen zu erstellen, zu ändern, zu pflegen oder zu übertragen, müssen entsprechende Verfahren und Kontrollen anwenden, um die Echtheit, Integrität und gegebenenfalls die Vertraulichkeit elektronischer Aufzeichnungen sicherzustellen und dafür zu sorgen, dass die Unterzeichneten die signierte Aufzeichnung nicht ohne Weiteres als unecht zurückweisen können. Diese Verfahren und Kontrollen müssen Folgendes umfassen: (d) Beschränkung des Systemzugriffs auf autorisierte Personen.	iam-user-unused-credentials-überprüfen	AWS Identity and Access Management (IAM) kann Ihnen bei Zugriffsberechtigungen und Autorisierungen helfen, indem es nach IAM-Passwörtern und Zugriffsschlüsseln sucht, die für einen bestimmten Zeitraum nicht verwendet wurden. Wenn ungenutzte Anmeldeinformationen identifiziert werden, müssen Sie sie deaktivieren und/oder entfernen, da dies gegen das Prinzip der geringsten Berechtigung verstoßen könnte. Für diese Regel müssen Sie einen Wert für das maxCredentialUsage Alter festlegen (Standardkonfiguration: 90). Der tatsächliche Wert muss den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
11.10(d)	Personen, die geschlossene Systeme verwenden, um elektronische Aufzeichnungen zu erstellen, zu ändern, zu pflegen oder zu übertragen, müssen entsprechende Verfahren und Kontrollen anwenden, um die Echtheit, Integrität und gegebenenfalls die Vertraulichkeit elektronischer Aufzeichnungen sicherzustellen und dafür zu sorgen, dass die Unterzeichneten die signierte Aufzeichnung nicht ohne Weiteres als unecht zurückweisen können. Diese Verfahren und Kontrollen müssen Folgendes umfassen: (d) Beschränkung des Systemzugriffs auf autorisierte Personen.	iam-user-unused-credentials-überprüfen	AWS Identity and Access Management (IAM) kann Ihnen bei Zugriffsberechtigungen und Autorisierungen helfen, indem es nach IAM-Passwörtern und Zugriffsschlüsseln sucht, die für einen bestimmten Zeitraum nicht verwendet wurden. Wenn ungenutzte Anmeldeinformationen identifiziert werden, müssen Sie sie deaktivieren und/oder entfernen, da dies gegen das Prinzip der geringsten Berechtigung verstoßen könnte. Für diese Regel müssen Sie einen Wert für das maxCredentialUsage Alter festlegen (Standardkonfiguration: 90). Der tatsächliche Wert muss den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
11.10(d)	Personen, die geschlossene Systeme verwenden , um elektronische Aufzeichnungen zu erstellen, zu ändern, zu pflegen oder zu übertragen, müssen entsprech ende Verfahren und Kontrollen anwenden, um die Echtheit, Integritä t und gegebenen falls die Vertrauli chkeit elektronischer Aufzeichnungen sicherzustellen und dafür zu sorgen, dass die Unterzeic hneten die signierte Aufzeichnung nicht ohne Weiteres als unecht zurückwei sen können. Diese Verfahren und Kontrollen müssen Folgendes umfassen: (d) Beschränkung des Systemzugriffs auf autorisierte Personen.	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) Security Groups können bei der Verwaltung des Netzwerkzugriffs helfen, indem sie eine statusbeh aftete Filterung von eingehendem und ausgehendem Netzwerkverkehr zu Ressourcen bereitste llen. AWS Wenn Sie eingehenden (oder entfernten) Datenverk ehr von 0.0.0.0/0 bis Port 22 auf Ihren Ressourcen nicht zulassen, können Sie den Remote-Zugriff einschränken.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
11.10(d)	Personen, die geschlossene Systeme verwenden , um elektronische Aufzeichnungen zu erstellen, zu ändern, zu pflegen oder zu übertragen, müssen entsprech ende Verfahren und Kontrollen anwenden, um die Echtheit, Integritä t und gegebenen falls die Vertrauli chkeit elektronischer Aufzeichnungen sicherzustellen und dafür zu sorgen, dass die Unterzeic hneten die signierte Aufzeichnung nicht ohne Weiteres als unecht zurückwei sen können. Diese Verfahren und Kontrollen müssen Folgendes umfassen: (d) Beschränkung des Systemzugriffs auf autorisierte Personen.	ec-2 instances-in-vpc	Stellen Sie Amazon Elastic Compute Cloud (Amazon EC2) -Instances innerhalb einer Amazon Virtual Private Cloud (Amazon VPC) bereit, um eine sichere Kommunika tion zwischen einer Instance und anderen Services innerhalb der Amazon VPC zu ermöglichen, ohne dass ein Internet-Gateway, ein NAT-Gerät oder eine VPN-Verbindung erforderlich ist. Der gesamte Datenverk ehr bleibt sicher in der AWS Cloud. Domains, die sich innerhalb einer VPC befinden, verfügen aufgrund ihrer logischen Isolierun g im Vergleich zu Domains mit öffentlic hen Endpunkten über eine zusätzlic he Sicherheitsebene. Weisen Sie EC2

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			Amazon-Instances einer Amazon-VPC zu, um den Zugriff ordnungsgemäß zu verwalten.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
11.10(d)	Personen, die geschlossene Systeme verwenden, um elektronische Aufzeichnungen zu erstellen, zu ändern, zu pflegen oder zu übertragen, müssen entsprechende Verfahren und Kontrollen anwenden, um die Echtheit, Integrität und gegebenenfalls die Vertraulichkeit elektronischer Aufzeichnungen sicherzustellen und dafür zu sorgen, dass die Unterzeichneten die signierte Aufzeichnung nicht ohne Weiteres als unecht zurückweisen können. Diese Verfahren und Kontrollen müssen Folgendes umfassen: (d) Beschränkung des Systemzugriffs auf autorisierte Personen.	lambda-function-public-access-verboten	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass AWS Lambda-Funktionen nicht öffentlich zugänglich sind. Der öffentliche Zugriff kann möglicherweise die Verfügbarkeit von Ressourcen beeinträchtigen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
11.10(d)	Personen, die geschlossene Systeme verwenden , um elektronische Aufzeichnungen zu erstellen, zu ändern, zu pflegen oder zu übertragen, müssen entsprech ende Verfahren und Kontrollen anwenden, um die Echtheit, Integritä t und gegebenen falls die Vertrauli chkeit elektronischer Aufzeichnungen sicherzustellen und dafür zu sorgen, dass die Unterzeic hneten die signierte Aufzeichnung nicht ohne Weiteres als unecht zurückwei sen können. Diese Verfahren und Kontrollen müssen Folgendes umfassen: (d) Beschränkung des Systemzugriffs auf autorisierte Personen.	lambda-inside-vpc	Stellen Sie AWS Lambda-Funktionen in einer Amazon Virtual Private Cloud (Amazon VPC) bereit, um eine sichere Kommunika tion zwischen einer Funktion und anderen Diensten innerhalb der Amazon VPC zu gewährleisten. Bei dieser Konfiguration sind kein Internet-Gateway, kein NAT-Gerät und keine VPN-Verbindung erforderlich. Der gesamte Datenverk ehr bleibt sicher in der Cloud. AWS Domains, die sich innerhalb einer VPC befinden, verfügen aufgrund ihrer logischen Isolierun g im Vergleich zu Domains mit öffentlic hen Endpunkten über eine zusätzliche Sicherheitsebene. Um den Zugriff ordnungsg emäß zu verwalten,

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			sollten AWS Lambda-Funktionen einer VPC zugewiesen werden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
11.10(d)	Personen, die geschlossene Systeme verwenden , um elektronische Aufzeichnungen zu erstellen, zu ändern, zu pflegen oder zu übertragen, müssen entsprech ende Verfahren und Kontrollen anwenden, um die Echtheit, Integritä t und gegebenen falls die Vertrauli chkeit elektronischer Aufzeichnungen sicherzustellen und dafür zu sorgen, dass die Unterzeic hneten die signierte Aufzeichnung nicht ohne Weiteres als unecht zurückwei sen können. Diese Verfahren und Kontrollen müssen Folgendes umfassen: (d) Beschränkung des Systemzugriffs auf autorisierte Personen.	mfa-enabled-for-iam-Konsolenzugriff	Verwalten Sie den Zugriff auf Ressource n in der AWS Cloud, indem Sie sicherste llen, dass MFA für alle AWS Identity and Access Managemen t (IAM) -Benutzer aktiviert ist, die über ein Konsolenk ennwort verfügen. MFA sorgt für eine weitere Schutzebe ne zusätzlich zu den Anmeldeinformation en. Indem Sie MFA für Benutzer vorschrei ben, können Sie Fälle kompromittierter Konten reduzieren und verhindern, dass unbefugte Benutzer auf vertrauliche Daten zugreifen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
11.10(d)	Personen, die geschlossene Systeme verwenden , um elektronische Aufzeichnungen zu erstellen, zu ändern, zu pflegen oder zu übertragen, müssen entsprech ende Verfahren und Kontrollen anwenden, um die Echtheit, Integritä t und gegebenen falls die Vertrauli chkeit elektronischer Aufzeichnungen sicherzustellen und dafür zu sorgen, dass die Unterzeic hneten die signierte Aufzeichnung nicht ohne Weiteres als unecht zurückwei sen können. Diese Verfahren und Kontrollen müssen Folgendes umfassen: (d) Beschränkung des Systemzugriffs auf autorisierte Personen.	no-unrestricted-route-to-igw	Stellen Sie sicher, dass EC2 Amazon-Routentabellen keine uneingeschränkten Routen zu einem Internet-Gateway enthalten. Durch das Entfernen oder Beschränken des Internetzugangs für Workloads innerhalb von Amazon VPCs können unbeabsic htigte Zugriffe in Ihrer Umgebung reduziert werden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
11.10(d)	Personen, die geschlossene Systeme verwenden , um elektronische Aufzeichnungen zu erstellen, zu ändern, zu pflegen oder zu übertragen, müssen entsprech ende Verfahren und Kontrollen anwenden, um die Echtheit, Integritä t und gegebenen falls die Vertrauli chkeit elektronischer Aufzeichnungen sicherzustellen und dafür zu sorgen, dass die Unterzeic hneten die signierte Aufzeichnung nicht ohne Weiteres als unecht zurückwei sen können. Diese Verfahren und Kontrollen müssen Folgendes umfassen: (d) Beschränkung des Systemzugriffs auf autorisierte Personen.	rds-instance-public-access-überprüfen	Verwalten Sie den Zugriff auf Ressource n in der AWS Cloud, indem Sie sicherste llen, dass Amazon Relational Database Service (Amazon RDS) -Instance s nicht öffentlic h sind. Amazon-RDS-Datenbank-Instances können vertrauliche Informati onen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
11.10(d)	Personen, die geschlossene Systeme verwenden , um elektronische Aufzeichnungen zu erstellen, zu ändern, zu pflegen oder zu übertragen, müssen entsprech ende Verfahren und Kontrollen anwenden, um die Echtheit, Integritä t und gegebenen falls die Vertrauli chkeit elektronischer Aufzeichnungen sicherzustellen und dafür zu sorgen, dass die Unterzeic hneten die signierte Aufzeichnung nicht ohne Weiteres als unecht zurückwei sen können. Diese Verfahren und Kontrollen müssen Folgendes umfassen: (d) Beschränkung des Systemzugriffs auf autorisierte Personen.	rds-snapshots-public-prohibited	Verwalten Sie den Zugriff auf Ressource n in der AWS Cloud, indem Sie sicherste llen, dass Amazon Relational Database Service (Amazon RDS) -Instance s nicht öffentlic h sind. Amazon-RDS-Datenbank-Instances können vertrauliche Informati onen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
11.10(d)	Personen, die geschlossene Systeme verwenden , um elektronische Aufzeichnungen zu erstellen, zu ändern, zu pflegen oder zu übertragen, müssen entsprech ende Verfahren und Kontrollen anwenden, um die Echtheit, Integritä t und gegebenen falls die Vertrauli chkeit elektronischer Aufzeichnungen sicherzustellen und dafür zu sorgen, dass die Unterzeic hneten die signierte Aufzeichnung nicht ohne Weiteres als unecht zurückwei sen können. Diese Verfahren und Kontrollen müssen Folgendes umfassen: (d) Beschränkung des Systemzugriffs auf autorisierte Personen.	redshift-cluster-public-access-überprüfen	Verwalten Sie den Zugriff auf Ressource n in der AWS Cloud, indem Sie sicherste llen, dass Amazon Redshift Redshift-Cluster nicht öffentlic h sind. Amazon-Re dshift-Cluster können vertrauliche Informati onen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
11.10(d)	Personen, die geschlossene Systeme verwenden , um elektronische Aufzeichnungen zu erstellen, zu ändern, zu pflegen oder zu übertragen, müssen entsprech ende Verfahren und Kontrollen anwenden, um die Echtheit, Integritä t und gegebenen falls die Vertrauli chkeit elektronischer Aufzeichnungen sicherzustellen und dafür zu sorgen, dass die Unterzeic hneten die signierte Aufzeichnung nicht ohne Weiteres als unecht zurückwei sen können. Diese Verfahren und Kontrollen müssen Folgendes umfassen: (d) Beschränkung des Systemzugriffs auf autorisierte Personen.	restricted-common-ports	Verwalten Sie den Zugriff auf Ressource n in der AWS Cloud, indem Sie sicherste llen, dass gemeinsam e Ports für Amazon Elastic Compute Cloud (Amazon EC2) -Sicherhe itsgruppen eingeschr ränkt sind. Wenn der Zugriff auf Ports nicht auf vertrauen swürdige Quellen beschränkt wird, kann dies zu Angriffen auf die Verfügbar keit, Integrität und Vertraulichkeit von Systemen führen. Mit dieser Regel können Sie optional die Parameter blockedPo rt1–blockedPort5 festlegen (Standard konfigurationen: 20, 21, 3389, 3306, 4333). Die tatsächli chen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
11.10(d)	Personen, die geschlossene Systeme verwenden, um elektronische Aufzeichnungen zu erstellen, zu ändern, zu pflegen oder zu übertragen, müssen entsprechende Verfahren und Kontrollen anwenden, um die Echtheit, Integrität und gegebenenfalls die Vertraulichkeit elektronischer Aufzeichnungen sicherzustellen und dafür zu sorgen, dass die Unterzeichneten die signierte Aufzeichnung nicht ohne Weiteres als unecht zurückweisen können. Diese Verfahren und Kontrollen müssen Folgendes umfassen: (d) Beschränkung des Systemzugriffs auf autorisierte Personen.	root-account-hardware-mfa-aktiviert	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Hardware-MFA für den Root-Benutzer aktiviert ist. Der Stammbenutzer ist der AWS-Konto-Benutzer mit den meisten Berechtigungen. MFA sorgt für eine weitere Schutzebene zusätzlich zu den Anmeldeinformationen. Indem Sie MFA für den Root-Benutzer vorschreiben, können Sie die Anzahl AWS-Konten kompromittierter Benutzer reduzieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
11.10(d)	Personen, die geschlossene Systeme verwenden, um elektronische Aufzeichnungen zu erstellen, zu ändern, zu pflegen oder zu übertragen, müssen entsprechende Verfahren und Kontrollen anwenden, um die Echtheit, Integrität und gegebenenfalls die Vertraulichkeit elektronischer Aufzeichnungen sicherzustellen und dafür zu sorgen, dass die Unterzeichneten die signierte Aufzeichnung nicht ohne Weiteres als unecht zurückweisen können. Diese Verfahren und Kontrollen müssen Folgendes umfassen: (d) Beschränkung des Systemzugriffs auf autorisierte Personen.	root-account-mfa-enabled	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass MFA für den Root-Benutzer aktiviert ist. Der Stammbenutzer ist der AWS-Konto-Benutzer mit den meisten Berechtigungen. MFA sorgt für eine weitere Schutzebene zusätzlich zu den Anmeldeinformationen. Indem Sie MFA für den Root-Benutzer vorschreiben, können Sie die Anzahl AWS-Konten kompromittierter Benutzer reduzieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
11.10(d)	Personen, die geschlossene Systeme verwenden , um elektronische Aufzeichnungen zu erstellen, zu ändern, zu pflegen oder zu übertragen, müssen entsprech ende Verfahren und Kontrollen anwenden, um die Echtheit, Integritä t und gegebenen falls die Vertrauli chkeit elektronischer Aufzeichnungen sicherzustellen und dafür zu sorgen, dass die Unterzeic hneten die signierte Aufzeichnung nicht ohne Weiteres als unecht zurückwei sen können. Diese Verfahren und Kontrollen müssen Folgendes umfassen: (d) Beschränkung des Systemzugriffs auf autorisierte Personen.	s3- -blöcke-periodisch account-level-public-access	Verwalten Sie den Zugriff auf Ressource n in der AWS Cloud, indem Sie sicherste llen, dass Amazon Simple Storage Service (Amazon S3) -Buckets nicht öffentlich zugänglic h sind. Diese Regel trägt dazu bei, sensible Daten vor unbefugten Remote-Benutzern zu schützen, indem sie den öffentlichen Zugriff verhinder t. Mit dieser Regel können Sie optional die Parameter ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) und restrictPublicBuck ets Parameter (Config Default: True) festlegen. Die tatsächlichen Werte müssen den Richtlini

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			en Ihrer Organisation entsprechen.
11.10(d)	Personen, die geschlossene Systeme verwenden , um elektronische Aufzeichnungen zu erstellen, zu ändern, zu pflegen oder zu übertragen, müssen entsprech ende Verfahren und Kontrollen anwenden, um die Echtheit, Integritä t und gegebenen falls die Vertrauli chkeit elektronischer Aufzeichnungen sicherzustellen und dafür zu sorgen, dass die Unterzeic hneten die signierte Aufzeichnung nicht ohne Weiteres als unecht zurückwei sen können. Diese Verfahren und Kontrollen müssen Folgendes umfassen: (d) Beschränkung des Systemzugriffs auf autorisierte Personen.	s3 bucket-level-public-access - verboten	Verwalten Sie den Zugriff auf Ressource n in der AWS Cloud, indem Sie sicherste llen, dass Amazon Simple Storage Service (Amazon S3) -Buckets nicht öffentlich zugänglic h sind. Diese Regel trägt dazu bei, sensible Daten vor unbefugten Remote-Benutzern zu schützen, indem sie den öffentlichen Zugriff auf Bucket-Eb ene verhindert.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
11.10(d)	Personen, die geschlossene Systeme verwenden , um elektronische Aufzeichnungen zu erstellen, zu ändern, zu pflegen oder zu übertragen, müssen entsprech ende Verfahren und Kontrollen anwenden, um die Echtheit, Integritä t und gegebenen falls die Vertrauli chkeit elektronischer Aufzeichnungen sicherzustellen und dafür zu sorgen, dass die Unterzeic hneten die signierte Aufzeichnung nicht ohne Weiteres als unecht zurückwei sen können. Diese Verfahren und Kontrollen müssen Folgendes umfassen: (d) Beschränkung des Systemzugriffs auf autorisierte Personen.	s-3 bucket-public-read -prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie nur autorisierten Benutzern, Prozessen und Geräten Zugriff auf Amazon Simple Storage Service (Amazon S3) - Buckets gewähren. Die Verwaltung des Zugriffs sollte mit der Klassifizierung der Daten übereinst immen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
11.10(d)	Personen, die geschlossene Systeme verwenden , um elektronische Aufzeichnungen zu erstellen, zu ändern, zu pflegen oder zu übertragen, müssen entsprech ende Verfahren und Kontrollen anwenden, um die Echtheit, Integritä t und gegebenen falls die Vertrauli chkeit elektronischer Aufzeichnungen sicherzustellen und dafür zu sorgen, dass die Unterzeic hneten die signierte Aufzeichnung nicht ohne Weiteres als unecht zurückwei sen können. Diese Verfahren und Kontrollen müssen Folgendes umfassen: (d) Beschränkung des Systemzugriffs auf autorisierte Personen.	s3- bucket-public-writ e-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie nur autorisierten Benutzern, Prozessen und Geräten Zugriff auf Amazon Simple Storage Service (Amazon S3) - Buckets gewähren. Die Verwaltung des Zugriffs sollte mit der Klassifizierung der Daten übereinst immen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
11.10(d)	Personen, die geschlossene Systeme verwenden, um elektronische Aufzeichnungen zu erstellen, zu ändern, zu pflegen oder zu übertragen, müssen entsprechende Verfahren und Kontrollen anwenden, um die Echtheit, Integrität und gegebenenfalls die Vertraulichkeit elektronischer Aufzeichnungen sicherzustellen und dafür zu sorgen, dass die Unterzeichneten die signierte Aufzeichnung nicht ohne Weiteres als unecht zurückweisen können. Diese Verfahren und Kontrollen müssen Folgendes umfassen: (d) Beschränkung des Systemzugriffs auf autorisierte Personen.	sagemaker-notebook-no-direct-Internetzugang	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass SageMaker Amazon-Notebooks keinen direkten Internetzugang zulassen. Indem Sie direkten Internetzugang blockieren, vermeiden Sie, dass unbefugte Benutzer auf sensible Daten zugreifen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
11.10(d)	Personen, die geschlossene Systeme verwenden , um elektronische Aufzeichnungen zu erstellen, zu ändern, zu pflegen oder zu übertragen, müssen entsprech ende Verfahren und Kontrollen anwenden, um die Echtheit, Integritä t und gegebenen falls die Vertrauli chkeit elektronischer Aufzeichnungen sicherzustellen und dafür zu sorgen, dass die Unterzeic hneten die signierte Aufzeichnung nicht ohne Weiteres als unecht zurückwei sen können. Diese Verfahren und Kontrollen müssen Folgendes umfassen: (d) Beschränkung des Systemzugriffs auf autorisierte Personen.	secretsmanager-rot ation-enabled-check	Diese Regel stellt sicher, dass bei AWS Secrets Manager Manager-Geheimnissen die Rotation aktiviert ist. Die regelmäßige Rotation von Secrets kann den Zeitraum verkürzen, in dem ein Secret aktiv ist, und möglicherweise die Auswirkungen auf das Unternehmen verringern, falls das Secret kompromittiert wird.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
11.10(d)	Personen, die geschlossene Systeme verwenden, um elektronische Aufzeichnungen zu erstellen, zu ändern, zu pflegen oder zu übertragen, müssen entsprechende Verfahren und Kontrollen anwenden, um die Echtheit, Integrität und gegebenenfalls die Vertraulichkeit elektronischer Aufzeichnungen sicherzustellen und dafür zu sorgen, dass die Unterzeichneten die signierte Aufzeichnung nicht ohne Weiteres als unecht zurückweisen können. Diese Verfahren und Kontrollen müssen Folgendes umfassen: (d) Beschränkung des Systemzugriffs auf autorisierte Personen.	secretsmanager-scheduled-rotation-success-überprüfen	Diese Regel stellt sicher, dass AWS Secrets Manager Manager-Geheimnisse gemäß dem Rotationsplan erfolgreich rotiert wurden. Die regelmäßige Rotation von Secrets kann den Zeitraum verkürzen, in dem ein Secret aktiv ist, und möglicherweise die Auswirkungen auf das Unternehmen verringern, falls es kompromittiert wird.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
11.10(d)	Personen, die geschlossene Systeme verwenden , um elektronische Aufzeichnungen zu erstellen, zu ändern, zu pflegen oder zu übertragen, müssen entsprech ende Verfahren und Kontrollen anwenden, um die Echtheit, Integritä t und gegebenen falls die Vertrauli chkeit elektronischer Aufzeichnungen sicherzustellen und dafür zu sorgen, dass die Unterzeic hneten die signierte Aufzeichnung nicht ohne Weiteres als unecht zurückwei sen können. Diese Verfahren und Kontrollen müssen Folgendes umfassen: (d) Beschränkung des Systemzugriffs auf autorisierte Personen.	ssm-document-not-p ublic	Stellen Sie sicher, dass AWS Systems Manager (SSM) - Dokumente nicht öffentlich sind, da dies einen unbeabsic htigten Zugriff auf Ihre SSM-Dokum ente ermöglichen kann. Ein öffentlic hes SSM-Dokum ent kann Informati onen über Ihr Konto, Ihre Ressourcen und internen Prozesse preisgeben.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
11.10(d)	Personen, die geschlossene Systeme verwenden , um elektronische Aufzeichnungen zu erstellen, zu ändern, zu pflegen oder zu übertragen, müssen entsprech ende Verfahren und Kontrollen anwenden, um die Echtheit, Integritä t und gegebenen falls die Vertrauli chkeit elektronischer Aufzeichnungen sicherzustellen und dafür zu sorgen, dass die Unterzeic hneten die signierte Aufzeichnung nicht ohne Weiteres als unecht zurückwei sen können. Diese Verfahren und Kontrollen müssen Folgendes umfassen: (d) Beschränkung des Systemzugriffs auf autorisierte Personen.	subnet-auto-assign-public-ip-deaktiviert	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon Virtual Private Cloud (VPC) -Subnetzen nicht automatisch eine öffentliche IP-Adress e zugewiesen wird. Amazon Elastic Compute Cloud (EC2) -Instances, die in Subnetzen gestartet werden, in denen dieses Attribut aktiviert ist, haben ihrer primären Netzwerkschnittste lle eine öffentliche IP-Adresse zugewiesen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
11.10(d)	Personen, die geschlossene Systeme verwenden , um elektronische Aufzeichnungen zu erstellen, zu ändern, zu pflegen oder zu übertragen, müssen entsprech ende Verfahren und Kontrollen anwenden, um die Echtheit, Integritä t und gegebenen falls die Vertrauli chkeit elektronischer Aufzeichnungen sicherzustellen und dafür zu sorgen, dass die Unterzeic hneten die signierte Aufzeichnung nicht ohne Weiteres als unecht zurückwei sen können. Diese Verfahren und Kontrollen müssen Folgendes umfassen: (d) Beschränkung des Systemzugriffs auf autorisierte Personen.	vpc-default-security-group-geschlossen	Sicherheitsgruppen von Amazon Elastic Compute Cloud (Amazon EC2) können bei der Verwaltung des Netzwerkzugriffs helfen, indem sie eine statusbehaftete Filterung des ein- und ausgehenden Netzwerkverkehrs zu Ressourcen bereitstellen. AWS Die Beschränk ung des gesamten Datenverkehrs auf die Standardsicherheit sgruppe hilft dabei, den Fernzugriff auf Ihre Ressourcen einzuschränken. AWS

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
11.10(d)	Personen, die geschlossene Systeme verwenden , um elektronische Aufzeichnungen zu erstellen, zu ändern, zu pflegen oder zu übertragen, müssen entsprech ende Verfahren und Kontrollen anwenden, um die Echtheit, Integritä t und gegebenen falls die Vertrauli chkeit elektronischer Aufzeichnungen sicherzustellen und dafür zu sorgen, dass die Unterzeic hneten die signierte Aufzeichnung nicht ohne Weiteres als unecht zurückwei sen können. Diese Verfahren und Kontrollen müssen Folgendes umfassen: (d) Beschränkung des Systemzugriffs auf autorisierte Personen.	vpc-sg-open-only-to-authorized-ports	Verwalten Sie den Zugriff auf Ressource n in der AWS Cloud, indem Sie sicherste llen, dass gemeinsam e Ports für Amazon Elastic Compute Cloud (Amazon EC2) -Sicherhe itsgruppen eingeschr ränkt sind. Wenn der Zugriff auf Ports nicht auf vertrauen swürdige Quellen beschränkt wird, kann dies zu Angriffen auf die Verfügbar keit, Integrität und Vertraulichkeit von Systemen führen. Durch die Beschränk ung des Zugriffs auf Ressourcen innerhalb einer Sicherhei tsgruppe aus dem Internet (0.0.0.0/0) kann der Remote-Zugriff auf interne Systeme gesteuert werden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
11.10(e)	Personen, die geschlossene Systeme verwenden , um elektronische Aufzeichnungen zu erstellen, zu ändern, zu pflegen oder zu übertragen, müssen entsprech ende Verfahren und Kontrollen anwenden, um die Echtheit, Integritä t und gegebenen falls die Vertrauli chkeit elektronischer Aufzeichnungen sicherzustellen und dafür zu sorgen, dass die Unterzeic hneten die signierte Aufzeichnung nicht ohne Weiteres als unecht zurückwei sen können. Diese Verfahren und Kontrollen müssen Folgendes umfassen: (e) Verwendung sicherer, computerg enerierter Audit Trails mit Zeitstemp el zur unabhängi	access-keys-rotated	Die Anmeldein formationen für autorisierte Geräte, Benutzer und Prozesse werden geprüft, indem sichergestellt wird, dass die IAM-Zugri ffsschlüssel gemäß den Vorgaben der Unternehmensrichtl inie rotiert werden. Das regelmäßi ge Ändern der Zugriffsschlüssel ist eine bewährte Sicherheitsmethode . Es verkürzt den Zeitraum, in dem ein Zugriffsschlüssel aktiv ist, und reduziert die Auswirkungen auf das Unternehmen, wenn die Schlüssel kompromittiert werden. Diese Regel erfordert einen Wert für die Zugriffsschlüssel-Rotation (Standard konfiguration: 90). Der tatsächliche Wert muss den Richtlini

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	gen Aufzeichnung von Datum und Uhrzeit von Benutzere ingaben und Aktionen, mit denen elektroni sche Aufzeichnungen erstellt, geändert oder gelöscht werden. Änderungen an den Aufzeichn ungen dürfen zuvor aufgezeichnete Informationen nicht verdecken. Solche Audit Trails müssen mindestens so lange aufbewahrt werden, wie dies für die betreffenden elektroni schen Aufzeichn ungen erforderlich ist, und sie müssen der zuständigen Behörde zur Überprüfung und Vervielfältigung zur Verfügung gestellt werden.		en Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
11.10(e)	Personen, die geschlossene Systeme verwenden , um elektronische Aufzeichnungen zu erstellen, zu ändern, zu pflegen oder zu übertragen, müssen entsprech ende Verfahren und Kontrollen anwenden, um die Echtheit, Integritä t und gegebenen falls die Vertrauli chkeit elektronischer Aufzeichnungen sicherzustellen und dafür zu sorgen, dass die Unterzeic hneten die signierte Aufzeichnung nicht ohne Weiteres als unecht zurückwei sen können. Diese Verfahren und Kontrollen müssen Folgendes umfassen: (e) Verwendung sicherer, computerg enerierter Audit Trails mit Zeitstemp el zur unabhängi	api-gw-execution-l ogging-aktiviert	Die API-Gateway-Protokollierung zeigt detaillierte Ansichten der Benutzer, die auf die API zugegriff en haben, und wie diese Benutzer auf die API zugegriff en haben. Diese Einblicke ermöglichen die Transparenz von Benutzeraktivitäten.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	gen Aufzeichnung von Datum und Uhrzeit von Benutzere ingaben und Aktionen, mit denen elektroni sche Aufzeichnungen erstellt, geändert oder gelöscht werden. Änderungen an den Aufzeichn ungen dürfen zuvor aufgezeichnete Informationen nicht verdecken. Solche Audit Trails müssen mindestens so lange aufbewahrt werden, wie dies für die betreffenden elektroni schen Aufzeichn ungen erforderlich ist, und sie müssen der zuständigen Behörde zur Überprüfung und Vervielfältigung zur Verfügung gestellt werden.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
11.10(e)	Personen, die geschlossene Systeme verwenden , um elektronische Aufzeichnungen zu erstellen, zu ändern, zu pflegen oder zu übertragen, müssen entsprech ende Verfahren und Kontrollen anwenden, um die Echtheit, Integritä t und gegebenen falls die Vertrauli chkeit elektronischer Aufzeichnungen sicherzustellen und dafür zu sorgen, dass die Unterzeic hneten die signierte Aufzeichnung nicht ohne Weiteres als unecht zurückwei sen können. Diese Verfahren und Kontrollen müssen Folgendes umfassen: (e) Verwendung sicherer, computerg enerierter Audit Trails mit Zeitstemp el zur unabhängi	cloud-trail-cloud-watch-logs-aktiviert	Verwenden Sie Amazon CloudWatc h , um Protokoll ereignisaktivitäten zentral zu sammeln und zu verwalten. Die Aufnahme von AWS CloudTrail Daten liefert Einzelheiten zu den API-Aufrufaktivitä ten in Ihrem AWS-Konto.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	gen Aufzeichnung von Datum und Uhrzeit von Benutzere ingaben und Aktionen, mit denen elektroni sche Aufzeichnungen erstellt, geändert oder gelöscht werden. Änderungen an den Aufzeichn ungen dürfen zuvor aufgezeichnete Informationen nicht verdecken. Solche Audit Trails müssen mindestens so lange aufbewahrt werden, wie dies für die betreffenden elektroni schen Aufzeichn ungen erforderlich ist, und sie müssen der zuständigen Behörde zur Überprüfung und Vervielfältigung zur Verfügung gestellt werden.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
11.10(e)	Personen, die geschlossene Systeme verwenden , um elektronische Aufzeichnungen zu erstellen, zu ändern, zu pflegen oder zu übertragen, müssen entsprech ende Verfahren und Kontrollen anwenden, um die Echtheit, Integritä t und gegebenen falls die Vertrauli chkeit elektronischer Aufzeichnungen sicherzustellen und dafür zu sorgen, dass die Unterzeic hneten die signierte Aufzeichnung nicht ohne Weiteres als unecht zurückwei sen können. Diese Verfahren und Kontrollen müssen Folgendes umfassen: (e) Verwendung sicherer, computerg enerierter Audit Trails mit Zeitstemp el zur unabhängi	cloudtrail-enabled	AWS CloudTrail kann bei der Nichtabst reitbarkeit helfen, indem Aktionen und API-Aufrufe der AWS Management Console aufgezeic hnet werden. Sie können die Benutzer und die Benutzer AWS-Konten , die einen AWS Dienst aufgerufen haben, die Quell-IP-Adresse, über die die Aufrufe generiert wurden, und den Zeitpunkt der Anrufe identifiz ieren. Einzelheiten zu den erfassten Daten finden Sie unter Inhalt des AWS CloudTrail Datensatzes.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	gen Aufzeichnung von Datum und Uhrzeit von Benutzere ingaben und Aktionen, mit denen elektroni sche Aufzeichnungen erstellt, geändert oder gelöscht werden. Änderungen an den Aufzeichn ungen dürfen zuvor aufgezeichnete Informationen nicht verdecken. Solche Audit Trails müssen mindestens so lange aufbewahrt werden, wie dies für die betreffenden elektroni schen Aufzeichn ungen erforderlich ist, und sie müssen der zuständigen Behörde zur Überprüfung und Vervielfältigung zur Verfügung gestellt werden.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
11.10(e)	Personen, die geschlossene Systeme verwenden , um elektronische Aufzeichnungen zu erstellen, zu ändern, zu pflegen oder zu übertragen, müssen entsprech ende Verfahren und Kontrollen anwenden, um die Echtheit, Integritä t und gegebenen falls die Vertrauli chkeit elektronischer Aufzeichnungen sicherzustellen und dafür zu sorgen, dass die Unterzeic hneten die signierte Aufzeichnung nicht ohne Weiteres als unecht zurückwei sen können. Diese Verfahren und Kontrollen müssen Folgendes umfassen: (e) Verwendung sicherer, computerg enerierter Audit Trails mit Zeitstemp el zur unabhängi	cloudtrail-s3-data events-enabled	Die Erfassung von Simple Storage Service (Amazon S3)-Datenereigniss en unterstützt die Erkennung von ungewöhnlichen Aktivitäten. Zu den Details gehören AWS-Konto Informationen über den Zugriff auf einen Amazon S3 S3-Bucket, die IP-Adress e und die Uhrzeit des Ereignisses.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	gen Aufzeichnung von Datum und Uhrzeit von Benutzere ingaben und Aktionen, mit denen elektroni sche Aufzeichnungen erstellt, geändert oder gelöscht werden. Änderungen an den Aufzeichn ungen dürfen zuvor aufgezeichnete Informationen nicht verdecken. Solche Audit Trails müssen mindestens so lange aufbewahrt werden, wie dies für die betreffenden elektroni schen Aufzeichn ungen erforderlich ist, und sie müssen der zuständigen Behörde zur Überprüfung und Vervielfältigung zur Verfügung gestellt werden.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
11.10(e)	Personen, die geschlossene Systeme verwenden, um elektronische Aufzeichnungen zu erstellen, zu ändern, zu pflegen oder zu übertragen, müssen entsprechende Verfahren und Kontrollen anwenden, um die Echtheit, Integrität und gegebenenfalls die Vertraulichkeit elektronischer Aufzeichnungen sicherzustellen und dafür zu sorgen, dass die Unterzeichneten die signierte Aufzeichnung nicht ohne Weiteres als unecht zurückweisen können. Diese Verfahren und Kontrollen müssen Folgendes umfassen: (e) Verwendung sicherer, computergenerierter Audit Trails mit Zeitstempel zur unabhängi	cw-loggroup-retention-period-überprüfen	Stellen Sie sicher, dass die Ereignisprotokolldaten für Ihre Protokollgruppen über eine Mindestdauer aufbewahrt werden, um die Fehlerbehebung und forensische Untersuchungen zu unterstützen. Fehlende frühere Ereignisprotokolldaten erschweren die Rekonstruierung und Identifizierung potenziell schädlicher Ereignisse.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	gen Aufzeichnung von Datum und Uhrzeit von Benutzere ingaben und Aktionen, mit denen elektroni sche Aufzeichnungen erstellt, geändert oder gelöscht werden. Änderungen an den Aufzeichn ungen dürfen zuvor aufgezeichnete Informationen nicht verdecken. Solche Audit Trails müssen mindestens so lange aufbewahrt werden, wie dies für die betreffenden elektroni schen Aufzeichn ungen erforderlich ist, und sie müssen der zuständigen Behörde zur Überprüfung und Vervielfältigung zur Verfügung gestellt werden.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
11.10(e)	Personen, die geschlossene Systeme verwenden , um elektronische Aufzeichnungen zu erstellen, zu ändern, zu pflegen oder zu übertragen, müssen entsprech ende Verfahren und Kontrollen anwenden, um die Echtheit, Integritä t und gegebenen falls die Vertrauli chkeit elektronischer Aufzeichnungen sicherzustellen und dafür zu sorgen, dass die Unterzeic hneten die signierte Aufzeichnung nicht ohne Weiteres als unecht zurückwei sen können. Diese Verfahren und Kontrollen müssen Folgendes umfassen: (e) Verwendung sicherer, computerg enerierter Audit Trails mit Zeitstemp el zur unabhängi	ec2-imdsv2-check	Stellen Sie sicher, dass die Methode Instance Metadata Service Version 2 (IMDSv2) aktiviert ist, um den Zugriff auf und die Kontrolle der Amazon Elastic Compute Cloud (Amazon EC2) - Instance-Metadate n zu schützen. Die IMDSv2 Methode verwendet sitzungsb asierte Kontrollen. Mit können Kontrolle n implementiert werden IMDSv2, um Änderungen an Instanzmetadaten einzuschränken.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	gen Aufzeichnung von Datum und Uhrzeit von Benutzere ingaben und Aktionen, mit denen elektroni sche Aufzeichnungen erstellt, geändert oder gelöscht werden. Änderungen an den Aufzeichn ungen dürfen zuvor aufgezeichnete Informationen nicht verdecken. Solche Audit Trails müssen mindestens so lange aufbewahrt werden, wie dies für die betreffenden elektroni schen Aufzeichn ungen erforderlich ist, und sie müssen der zuständigen Behörde zur Überprüfung und Vervielfältigung zur Verfügung gestellt werden.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
11.10(e)	Personen, die geschlossene Systeme verwenden , um elektronische Aufzeichnungen zu erstellen, zu ändern, zu pflegen oder zu übertragen, müssen entsprech ende Verfahren und Kontrollen anwenden, um die Echtheit, Integritä t und gegebenen falls die Vertrauli chkeit elektronischer Aufzeichnungen sicherzustellen und dafür zu sorgen, dass die Unterzeic hneten die signierte Aufzeichnung nicht ohne Weiteres als unecht zurückwei sen können. Diese Verfahren und Kontrollen müssen Folgendes umfassen: (e) Verwendung sicherer, computerg enerierter Audit Trails mit Zeitstemp el zur unabhängi	elasticsearch-logs-to-cloudwatch	Stellen Sie sicher, dass für Amazon OpenSearch Service-Domains Fehlerpro tokolle aktiviert und zur Aufbewahrung und Beantwortung an Amazon CloudWatc h Logs gestreamt werden. Domain-Fehlerprotokolle sind bei Sicherhei ts- und Zugriffsp rüfungen sowie bei der Diagnose von Verfügbarkeitsprob lemen nützlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	gen Aufzeichnung von Datum und Uhrzeit von Benutzere ingaben und Aktionen, mit denen elektroni sche Aufzeichnungen erstellt, geändert oder gelöscht werden. Änderungen an den Aufzeichn ungen dürfen zuvor aufgezeichnete Informationen nicht verdecken. Solche Audit Trails müssen mindestens so lange aufbewahrt werden, wie dies für die betreffenden elektroni schen Aufzeichn ungen erforderlich ist, und sie müssen der zuständigen Behörde zur Überprüfung und Vervielfältigung zur Verfügung gestellt werden.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
11.10(e)	Personen, die geschlossene Systeme verwenden , um elektronische Aufzeichnungen zu erstellen, zu ändern, zu pflegen oder zu übertragen, müssen entsprech ende Verfahren und Kontrollen anwenden, um die Echtheit, Integritä t und gegebenen falls die Vertrauli chkeit elektronischer Aufzeichnungen sicherzustellen und dafür zu sorgen, dass die Unterzeic hneten die signierte Aufzeichnung nicht ohne Weiteres als unecht zurückwei sen können. Diese Verfahren und Kontrollen müssen Folgendes umfassen: (e) Verwendung sicherer, computerg enerierter Audit Trails mit Zeitstemp el zur unabhängi	elb-logging-enabled	Die Elastic-Load-Balancing-Aktivität ist ein zentraler Kommunikationspunk t innerhalb einer Umgebung. Stellen Sie sicher, dass die ELB-Protokollierun g aktiviert ist. Die gesammelten Daten enthalten detaillie rte Informationen zu Anfragen, die an den ELB gesendet wurden. Jedes Protokoll enthält Informationen wie die Zeit, zu der die Anforderung einging, die Client-IP -Adresse, Latenzen, Anforderungspfade und Serverantworten.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	gen Aufzeichnung von Datum und Uhrzeit von Benutzere ingaben und Aktionen, mit denen elektroni sche Aufzeichnungen erstellt, geändert oder gelöscht werden. Änderungen an den Aufzeichn ungen dürfen zuvor aufgezeichnete Informationen nicht verdecken. Solche Audit Trails müssen mindestens so lange aufbewahrt werden, wie dies für die betreffenden elektroni schen Aufzeichn ungen erforderlich ist, und sie müssen der zuständigen Behörde zur Überprüfung und Vervielfältigung zur Verfügung gestellt werden.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
11.10(e)	Personen, die geschlossene Systeme verwenden , um elektronische Aufzeichnungen zu erstellen, zu ändern, zu pflegen oder zu übertragen, müssen entsprech ende Verfahren und Kontrollen anwenden, um die Echtheit, Integritä t und gegebenen falls die Vertrauli chkeit elektronischer Aufzeichnungen sicherzustellen und dafür zu sorgen, dass die Unterzeic hneten die signierte Aufzeichnung nicht ohne Weiteres als unecht zurückwei sen können. Diese Verfahren und Kontrollen müssen Folgendes umfassen: (e) Verwendung sicherer, computerg enerierter Audit Trails mit Zeitstemp el zur unabhängi	emr-kerberos-enabled	Die Zugriffsberechtigu ngen und -autorisi erungen können verwaltet und nach den Prinzipien der geringsten Berechtig ung und Aufgabent rennung integrier t werden, indem Kerberos für Amazon-EMR-Cluster aktiviert wird. In Kerberos werden Services und Benutzer, die sich authentif izieren müssen, als Prinzipale bezeichnet. Prinzipal e befinden sich in einem Kerberos-Bereich. Innerhalb dieses Bereichs wird ein Kerberos-Server als Key Distribution Center (KDC) bezeichnet. Über diesen Server können sich Prinzipal e authentifizieren. Die Authentifizierung im KDC erfolgt durch die Ausstellu ng von Authentif

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	gen Aufzeichnung von Datum und Uhrzeit von Benutzere ingaben und Aktionen, mit denen elektroni sche Aufzeichnungen erstellt, geändert oder gelöscht werden. Änderungen an den Aufzeichn ungen dürfen zuvor aufgezeichnete Informationen nicht verdecken. Solche Audit Trails müssen mindestens so lange aufbewahrt werden, wie dies für die betreffenden elektroni schen Aufzeichn ungen erforderlich ist, und sie müssen der zuständigen Behörde zur Überprüfung und Vervielfältigung zur Verfügung gestellt werden.		izierungstickets. Das KDC unterhält eine Datenbank der Prinzipale in seinem Bereich mit ihren Passwörtern und anderen administr ativen Informationen zu jedem Prinzipal.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
11.10(e)	Personen, die geschlossene Systeme verwenden, um elektronische Aufzeichnungen zu erstellen, zu ändern, zu pflegen oder zu übertragen, müssen entsprechende Verfahren und Kontrollen anwenden, um die Echtheit, Integrität und gegebenenfalls die Vertraulichkeit elektronischer Aufzeichnungen sicherzustellen und dafür zu sorgen, dass die Unterzeichneten die signierte Aufzeichnung nicht ohne Weiteres als unecht zurückweisen können. Diese Verfahren und Kontrollen müssen Folgendes umfassen: (e) Verwendung sicherer, computergenerierter Audit Trails mit Zeitstempel zur unabhängi	iam-group-has-users-überprüfen	AWS Identity and Access Management (IAM) kann Ihnen helfen, die Prinzipien der geringsten Rechte und der Aufgabentrennung mit Zugriffsberechtigungen und Autorisierungen zu integrieren, indem sichergestellt wird, dass IAM-Gruppen mindestens einen Benutzer haben. Die Einteilung von Benutzern in Gruppen auf der Grundlage der ihnen zugewiesenen Berechtigungen oder ihrer Funktion ist eine Möglichkeit, das Prinzip der geringsten Berechtigung zu implementieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	gen Aufzeichnung von Datum und Uhrzeit von Benutzere ingaben und Aktionen, mit denen elektroni sche Aufzeichnungen erstellt, geändert oder gelöscht werden. Änderungen an den Aufzeichn ungen dürfen zuvor aufgezeichnete Informationen nicht verdecken. Solche Audit Trails müssen mindestens so lange aufbewahrt werden, wie dies für die betreffenden elektroni schen Aufzeichn ungen erforderlich ist, und sie müssen der zuständigen Behörde zur Überprüfung und Vervielfältigung zur Verfügung gestellt werden.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
11.10(e)	Personen, die geschlossene Systeme verwenden , um elektronische Aufzeichnungen zu erstellen, zu ändern, zu pflegen oder zu übertragen, müssen entsprech ende Verfahren und Kontrollen anwenden, um die Echtheit, Integritä t und gegebenen falls die Vertrauli chkeit elektronischer Aufzeichnungen sicherzustellen und dafür zu sorgen, dass die Unterzeic hneten die signierte Aufzeichnung nicht ohne Weiteres als unecht zurückwei sen können. Diese Verfahren und Kontrollen müssen Folgendes umfassen: (e) Verwendung sicherer, computerg enerierter Audit Trails mit Zeitstemp el zur unabhängi	iam-no-inline-policy-überprüfen	Stellen Sie sicher, dass ein Benutzer, eine IAM-Rolle oder eine IAM-Gruppe (AWS Identity and Access Management) nicht über eine Inline-Richtlinie zur Zugriffsk ontrolle auf Systeme und Ressource n verfügt. AWS empfiehlt, verwaltet e Richtlinien anstelle von Inline-Richtlinien zu verwenden. Verwaltete Richtlini en ermöglichen Wiederverwendbarke it, Versionsverwaltung , Rollback und Delegierung der Berechtigungsverwa ltung.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	gen Aufzeichnung von Datum und Uhrzeit von Benutzere ingaben und Aktionen, mit denen elektroni sche Aufzeichnungen erstellt, geändert oder gelöscht werden. Änderungen an den Aufzeichn ungen dürfen zuvor aufgezeichnete Informationen nicht verdecken. Solche Audit Trails müssen mindestens so lange aufbewahrt werden, wie dies für die betreffenden elektroni schen Aufzeichn ungen erforderlich ist, und sie müssen der zuständigen Behörde zur Überprüfung und Vervielfältigung zur Verfügung gestellt werden.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
11.10(e)	Personen, die geschlossene Systeme verwenden , um elektronische Aufzeichnungen zu erstellen, zu ändern, zu pflegen oder zu übertragen, müssen entsprech ende Verfahren und Kontrollen anwenden, um die Echtheit, Integritä t und gegebenen falls die Vertrauli chkeit elektronischer Aufzeichnungen sicherzustellen und dafür zu sorgen, dass die Unterzeic hneten die signierte Aufzeichnung nicht ohne Weiteres als unecht zurückwei sen können. Diese Verfahren und Kontrollen müssen Folgendes umfassen: (e) Verwendung sicherer, computerg enerierter Audit Trails mit Zeitstemp el zur unabhängi	iam-password-policy	Die Identitäten und Anmeldeinformation en werden auf der Grundlage einer organisatorischen IAM-Passwortrichtlinie ausgestellt, verwaltet und verifiziert. Sie erfüllen oder übertreff en die Anforderungen von NIST SP 800-63 und dem Standard „Best Practices“ von AWS Foundatio nal Security für die Passwortstärke. Mit dieser Regel können Sie optional RequireUppercaseCh aracters (Wert für AWS grundlegende Sicherheitsbewährt e Methoden: wahr), RequireLowercaseCh aracters (Wert für bewährte Methoden für AWS grundlege nde Sicherheit: wahr), RequireSy mbols (Wert für bewährte Methoden für AWS grundlege nde Sicherheit:

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	gen Aufzeichnung von Datum und Uhrzeit von Benutzere ingaben und Aktionen, mit denen elektroni sche Aufzeichnungen erstellt, geändert oder gelöscht werden. Änderungen an den Aufzeichn ungen dürfen zuvor aufgezeichnete Informationen nicht verdecken. Solche Audit Trails müssen mindestens so lange aufbewahrt werden, wie dies für die betreffenden elektroni schen Aufzeichn ungen erforderlich ist, und sie müssen der zuständigen Behörde zur Überprüfung und Vervielfältigung zur Verfügung gestellt werden.		wahr), RequireNu mbers (Wert für bewährte Methoden für AWS grundlege nde Sicherheit: wahr), MinimumPa sswordLength (Wert für bewährte Methoden für AWS grundlegende Sicherheit: 14), PasswordReusePreve ntion (Wert für bewährte Methoden für AWS grundlege nde Sicherheit: 24) und MaxPasswo rdAge (Wert für bewährte Methoden für AWS grundlege nde Sicherheit: 90) für Ihr IAM festlegen. Kennwortrichtlinie. Die tatsächlichen Werte müssen den Richtlini en Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
11.10(e)	Personen, die geschlossene Systeme verwenden, um elektronische Aufzeichnungen zu erstellen, zu ändern, zu pflegen oder zu übertragen, müssen entsprechende Verfahren und Kontrollen anwenden, um die Echtheit, Integrität und gegebenenfalls die Vertraulichkeit elektronischer Aufzeichnungen sicherzustellen und dafür zu sorgen, dass die Unterzeichneten die signierte Aufzeichnung nicht ohne Weiteres als unecht zurückweisen können. Diese Verfahren und Kontrollen müssen Folgendes umfassen: (e) Verwendung sicherer, computergenerierter Audit Trails mit Zeitstempel zur unabhängi	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) kann Ihnen dabei helfen, die Prinzipien der geringsten Rechte und der Aufgabentrennung in Zugriffsberechtigungen und Autorisierungen zu integrieren und so zu verhindern, dass Richtlinien „Effect“: „Allow“ mit „Action“: „*“ anstelle von „Resource“: „*“ enthalten. Wenn Benutzern mehr Rechte eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und der Aufgabentrennung verstoßen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	gen Aufzeichnung von Datum und Uhrzeit von Benutzere ingaben und Aktionen, mit denen elektroni sche Aufzeichnungen erstellt, geändert oder gelöscht werden. Änderungen an den Aufzeichn ungen dürfen zuvor aufgezeichnete Informationen nicht verdecken. Solche Audit Trails müssen mindestens so lange aufbewahrt werden, wie dies für die betreffenden elektroni schen Aufzeichn ungen erforderlich ist, und sie müssen der zuständigen Behörde zur Überprüfung und Vervielfältigung zur Verfügung gestellt werden.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
11.10(e)	Personen, die geschlossene Systeme verwenden , um elektronische Aufzeichnungen zu erstellen, zu ändern, zu pflegen oder zu übertragen, müssen entsprech ende Verfahren und Kontrollen anwenden, um die Echtheit, Integritä t und gegebenen falls die Vertrauli chkeit elektronischer Aufzeichnungen sicherzustellen und dafür zu sorgen, dass die Unterzeic hneten die signierte Aufzeichnung nicht ohne Weiteres als unecht zurückwei sen können. Diese Verfahren und Kontrollen müssen Folgendes umfassen: (e) Verwendung sicherer, computerg enerierter Audit Trails mit Zeitstemp el zur unabhängi	multi-region-cloudtrail-enabled	AWS CloudTrail zeichnet Aktionen und API-Aufrufe der AWS Management Console auf. Sie können feststellen, welche Benutzer und Konten angerufen wurden AWS, von welcher Quell-IP-Adresse aus die Anrufe getätigt wurden und wann die Anrufe erfolgten. CloudTrail übermittelt Protokolldateien aus allen AWS Regionen an Ihren S3-Bucket , wenn MULTI_REG ION_CLOUD _TRAIL_ENABLED aktiviert ist. Außerdem wird beim AWS Start einer neuen Region derselbe Trail in der neuen Region erstellt. CloudTrail Dadurch erhalten Sie automatis ch Protokolldateien mit API-Aktivitäten für die neue Region.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	gen Aufzeichnung von Datum und Uhrzeit von Benutzere ingaben und Aktionen, mit denen elektroni sche Aufzeichnungen erstellt, geändert oder gelöscht werden. Änderungen an den Aufzeichn ungen dürfen zuvor aufgezeichnete Informationen nicht verdecken. Solche Audit Trails müssen mindestens so lange aufbewahrt werden, wie dies für die betreffenden elektroni schen Aufzeichn ungen erforderlich ist, und sie müssen der zuständigen Behörde zur Überprüfung und Vervielfältigung zur Verfügung gestellt werden.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
11.10(e)	Personen, die geschlossene Systeme verwenden , um elektronische Aufzeichnungen zu erstellen, zu ändern, zu pflegen oder zu übertragen, müssen entsprech ende Verfahren und Kontrollen anwenden, um die Echtheit, Integritä t und gegebenen falls die Vertrauli chkeit elektronischer Aufzeichnungen sicherzustellen und dafür zu sorgen, dass die Unterzeic hneten die signierte Aufzeichnung nicht ohne Weiteres als unecht zurückwei sen können. Diese Verfahren und Kontrollen müssen Folgendes umfassen: (e) Verwendung sicherer, computerg enerierter Audit Trails mit Zeitstemp el zur unabhängi	opensearch-logs-to-cloudwatch	Stellen Sie sicher, dass für Amazon OpenSearch Service-Domains Fehlerpro tokolle aktiviert und zur Aufbewahr ung und Beantwort ung an Amazon CloudWatch Logs gestreamt werden. OpenSearch Service-Fehlerprotokolle können bei Sicherhei ts- und Zugriffsp rüfungen helfen und bei der Diagnose von Verfügbarkeitsprob lemen helfen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	gen Aufzeichnung von Datum und Uhrzeit von Benutzere ingaben und Aktionen, mit denen elektroni sche Aufzeichnungen erstellt, geändert oder gelöscht werden. Änderungen an den Aufzeichn ungen dürfen zuvor aufgezeichnete Informationen nicht verdecken. Solche Audit Trails müssen mindestens so lange aufbewahrt werden, wie dies für die betreffenden elektroni schen Aufzeichn ungen erforderlich ist, und sie müssen der zuständigen Behörde zur Überprüfung und Vervielfältigung zur Verfügung gestellt werden.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
11.10(e)	Personen, die geschlossene Systeme verwenden , um elektronische Aufzeichnungen zu erstellen, zu ändern, zu pflegen oder zu übertragen, müssen entsprech ende Verfahren und Kontrollen anwenden, um die Echtheit, Integritä t und gegebenen falls die Vertrauli chkeit elektronischer Aufzeichnungen sicherzustellen und dafür zu sorgen, dass die Unterzeic hneten die signierte Aufzeichnung nicht ohne Weiteres als unecht zurückwei sen können. Diese Verfahren und Kontrollen müssen Folgendes umfassen: (e) Verwendung sicherer, computerg enerierter Audit Trails mit Zeitstemp el zur unabhängi	rds-logging-enabled	Um die Protokoll ierung und Überwachung in Ihrer Umgebung zu erleichtern, stellen Sie sicher, dass die Amazon Relationa l Database Service (Amazon RDS)-Prot okollierung aktiviert ist. Mit der Amazon-RDS-Protokollierung können Sie Ereigniss e wie Verbindungen, Verbindungsabbrüch e, Abfragen oder abgefragte Tabellen erfassen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	gen Aufzeichnung von Datum und Uhrzeit von Benutzere ingaben und Aktionen, mit denen elektroni sche Aufzeichnungen erstellt, geändert oder gelöscht werden. Änderungen an den Aufzeichn ungen dürfen zuvor aufgezeichnete Informationen nicht verdecken. Solche Audit Trails müssen mindestens so lange aufbewahrt werden, wie dies für die betreffenden elektroni schen Aufzeichn ungen erforderlich ist, und sie müssen der zuständigen Behörde zur Überprüfung und Vervielfältigung zur Verfügung gestellt werden.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
11.10(e)	Personen, die geschlossene Systeme verwenden , um elektronische Aufzeichnungen zu erstellen, zu ändern, zu pflegen oder zu übertragen, müssen entsprech ende Verfahren und Kontrollen anwenden, um die Echtheit, Integritä t und gegebenen falls die Vertrauli chkeit elektronischer Aufzeichnungen sicherzustellen und dafür zu sorgen, dass die Unterzeic hneten die signierte Aufzeichnung nicht ohne Weiteres als unecht zurückwei sen können. Diese Verfahren und Kontrollen müssen Folgendes umfassen: (e) Verwendung sicherer, computerg enerierter Audit Trails mit Zeitstemp el zur unabhängi	redshift-audit-logging-enabled	Aktivieren Sie die Prüfungsprotokolli erung, um Informati onen über Verbindun gen und Benutzera ktivitäten in Ihrem Amazon-Redshift-Cl uster zu erfassen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	gen Aufzeichnung von Datum und Uhrzeit von Benutzere ingaben und Aktionen, mit denen elektroni sche Aufzeichnungen erstellt, geändert oder gelöscht werden. Änderungen an den Aufzeichn ungen dürfen zuvor aufgezeichnete Informationen nicht verdecken. Solche Audit Trails müssen mindestens so lange aufbewahrt werden, wie dies für die betreffenden elektroni schen Aufzeichn ungen erforderlich ist, und sie müssen der zuständigen Behörde zur Überprüfung und Vervielfältigung zur Verfügung gestellt werden.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
11.10(e)	Personen, die geschlossene Systeme verwenden , um elektronische Aufzeichnungen zu erstellen, zu ändern, zu pflegen oder zu übertragen, müssen entsprech ende Verfahren und Kontrollen anwenden, um die Echtheit, Integritä t und gegebenen falls die Vertrauli chkeit elektronischer Aufzeichnungen sicherzustellen und dafür zu sorgen, dass die Unterzeic hneten die signierte Aufzeichnung nicht ohne Weiteres als unecht zurückwei sen können. Diese Verfahren und Kontrollen müssen Folgendes umfassen: (e) Verwendung sicherer, computerg enerierter Audit Trails mit Zeitstemp el zur unabhängi	redshift-cluster-c onfiguration-check	Um Daten im Ruhezustand zu schützen, muss die Verschlüsselung für Ihre Amazon-Re dshift-Cluster aktiviert sein. Sie müssen auch sicherstellen, dass die erforderl ichen Konfigurationen auf Amazon-Redshift-Clustern bereitges tellt werden. Die Prüfungsprotokolli erung muss aktiviert sein, um Informati onen zu Verbindun gen und Benutzera ktivitäten in der Datenbank bereitzus tellen. Diese Regel erfordert, dass ein Wert für clusterDb Encrypted (Config Default: TRUE) und LoggingEnabled (Config Default: TRUE) gesetzt ist. Die tatsächlichen Werte müssen den Richtlini en Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	gen Aufzeichnung von Datum und Uhrzeit von Benutzere ingaben und Aktionen, mit denen elektroni sche Aufzeichnungen erstellt, geändert oder gelöscht werden. Änderungen an den Aufzeichn ungen dürfen zuvor aufgezeichnete Informationen nicht verdecken. Solche Audit Trails müssen mindestens so lange aufbewahrt werden, wie dies für die betreffenden elektroni schen Aufzeichn ungen erforderlich ist, und sie müssen der zuständigen Behörde zur Überprüfung und Vervielfältigung zur Verfügung gestellt werden.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
11.10(e)	Personen, die geschlossene Systeme verwenden , um elektronische Aufzeichnungen zu erstellen, zu ändern, zu pflegen oder zu übertragen, müssen entsprech ende Verfahren und Kontrollen anwenden, um die Echtheit, Integritä t und gegebenen falls die Vertrauli chkeit elektronischer Aufzeichnungen sicherzustellen und dafür zu sorgen, dass die Unterzeic hneten die signierte Aufzeichnung nicht ohne Weiteres als unecht zurückwei sen können. Diese Verfahren und Kontrollen müssen Folgendes umfassen: (e) Verwendung sicherer, computerg enerierter Audit Trails mit Zeitstemp el zur unabhängi	s3- bucket-logging-enabled	Die Amazon Simple Storage Service (Amazon S3)-Serverzugriffs protokollierung bietet eine Methode zur Überwachu ng des Netzwerks im Hinblick auf potenzielle Cybersich erheitsereignisse. Die Ereignisse werden überwacht, indem detaillierte Aufzeichn ungen über die Anfragen erfasst werden, die an einen Amazon-S3-Bucket gestellt wurden. Jeder Zugriffsprotokolle intrag enthält Details zu einer einzelnen Zugriffsanfrage. Zu den Details gehören Anforderer, Bucket-Name, Anforderu ngszeit, Anforderu ngsaktion, Antwortst atus und Fehlercode, falls relevant.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	gen Aufzeichnung von Datum und Uhrzeit von Benutzere ingaben und Aktionen, mit denen elektroni sche Aufzeichnungen erstellt, geändert oder gelöscht werden. Änderungen an den Aufzeichn ungen dürfen zuvor aufgezeichnete Informationen nicht verdecken. Solche Audit Trails müssen mindestens so lange aufbewahrt werden, wie dies für die betreffenden elektroni schen Aufzeichn ungen erforderlich ist, und sie müssen der zuständigen Behörde zur Überprüfung und Vervielfältigung zur Verfügung gestellt werden.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
11.10(e)	Personen, die geschlossene Systeme verwenden, um elektronische Aufzeichnungen zu erstellen, zu ändern, zu pflegen oder zu übertragen, müssen entsprechende Verfahren und Kontrollen anwenden, um die Echtheit, Integrität und gegebenenfalls die Vertraulichkeit elektronischer Aufzeichnungen sicherzustellen und dafür zu sorgen, dass die Unterzeichneten die signierte Aufzeichnung nicht ohne Weiteres als unecht zurückweisen können. Diese Verfahren und Kontrollen müssen Folgendes umfassen: (e) Verwendung sicherer, computergenerierter Audit Trails mit Zeitstempel zur unabhängi	vpc-flow-logs-enabled	VPC-Flow-Protokolle erfassen detaillierte Informationsdatensätze über den IP-Datenverkehr, der zu und von Netzwerkschnittstellen in Ihrer Amazon Virtual Private Cloud (Amazon VPC) fließt. Standardmäßig enthalten Flow-Protokolldatensätze Werte für die verschiedenen Komponenten des IP-Flows, einschließlich Quelle, Ziel und Protokoll.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	gen Aufzeichnung von Datum und Uhrzeit von Benutzere ingaben und Aktionen, mit denen elektroni sche Aufzeichnungen erstellt, geändert oder gelöscht werden. Änderungen an den Aufzeichn ungen dürfen zuvor aufgezeichnete Informationen nicht verdecken. Solche Audit Trails müssen mindestens so lange aufbewahrt werden, wie dies für die betreffenden elektroni schen Aufzeichn ungen erforderlich ist, und sie müssen der zuständigen Behörde zur Überprüfung und Vervielfältigung zur Verfügung gestellt werden.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
11.10(e)	Personen, die geschlossene Systeme verwenden, um elektronische Aufzeichnungen zu erstellen, zu ändern, zu pflegen oder zu übertragen, müssen entsprechende Verfahren und Kontrollen anwenden, um die Echtheit, Integrität und gegebenenfalls die Vertraulichkeit elektronischer Aufzeichnungen sicherzustellen und dafür zu sorgen, dass die Unterzeichneten die signierte Aufzeichnung nicht ohne Weiteres als unecht zurückweisen können. Diese Verfahren und Kontrollen müssen Folgendes umfassen: (e) Verwendung sicherer, computergenerierter Audit Trails mit Zeitstempel zur unabhängi	wafv2-logging-enabled	Um die Protokollierung und Überwachung in Ihrer Umgebung zu erleichtern, aktivieren Sie die AWS WAF (V2) -Protokollierung im regionalen und globalen Web ACLs. AWS Die WAF-Protokollierung bietet detaillierte Informationen über den Datenverkehr, der von Ihrer Web-ACL analysiert wird. In den Protokollen werden die Uhrzeit aufgezeichnet, zu der die AWS WAF die Anfrage von Ihrer AWS Ressource erhalten hat, Informationen über die Anfrage und eine Aktion für die Regel, der jede Anfrage entsprach.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	gen Aufzeichnung von Datum und Uhrzeit von Benutzere ingaben und Aktionen, mit denen elektroni sche Aufzeichnungen erstellt, geändert oder gelöscht werden. Änderungen an den Aufzeichn ungen dürfen zuvor aufgezeichnete Informationen nicht verdecken. Solche Audit Trails müssen mindestens so lange aufbewahrt werden, wie dies für die betreffenden elektroni schen Aufzeichn ungen erforderlich ist, und sie müssen der zuständigen Behörde zur Überprüfung und Vervielfältigung zur Verfügung gestellt werden.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
11.10(g)	Personen, die geschlossene Systeme verwenden , um elektronische Aufzeichnungen zu erstellen, zu ändern, zu pflegen oder zu übertragen, müssen entsprech ende Verfahren und Kontrollen anwenden, um die Echtheit, Integritä t und gegebenen falls die Vertrauli chkeit elektronischer Aufzeichnungen sicherzustellen und dafür zu sorgen, dass die Unterzeic hneten die signierte Aufzeichnung nicht ohne Weiteres als unecht zurückwei sen können. Diese Verfahren und Kontrollen müssen Folgendes umfassen: (g) Durchführung von behördlichen Kontrollen, damit ausschließlich befugte Personen das System	access-keys-rotated	Die Anmeldein formationen für autorisierte Geräte, Benutzer und Prozesse werden geprüft, indem sichergestellt wird, dass die IAM-Zugri ffsschlüssel gemäß den Vorgaben der Unternehmensrichtl inie rotiert werden. Das regelmäßi ge Ändern der Zugriffsschlüssel ist eine bewährte Sicherheitsmethode . Es verkürzt den Zeitraum, in dem ein Zugriffsschlüssel aktiv ist, und reduziert die Auswirkungen auf das Unternehmen, wenn die Schlüssel kompromittiert werden. Diese Regel erfordert einen Wert für die Zugriffsschlüssel-Rotation (Standard konfiguration: 90). Der tatsächliche Wert muss den Richtlini

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	nutzen, Aufzeichnungen elektronisch signieren, auf den Vorgang oder das Eingabe- oder Ausgabegerät des Computersystems zugreifen, Aufzeichnungen ändern oder den betreffenden Vorgang ausführen können.		en Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
11.10(g)	Personen, die geschlossene Systeme verwenden, um elektronische Aufzeichnungen zu erstellen, zu ändern, zu pflegen oder zu übertragen, müssen entsprechende Verfahren und Kontrollen anwenden, um die Echtheit, Integrität und gegebenenfalls die Vertraulichkeit elektronischer Aufzeichnungen sicherzustellen und dafür zu sorgen, dass die Unterzeichneten die signierte Aufzeichnung nicht ohne Weiteres als unecht zurückweisen können. Diese Verfahren und Kontrollen müssen Folgendes umfassen: (g) Durchführung von behördlichen Kontrollen, damit ausschließlich befugte Personen das System	account-part-of-organizations	Durch die zentrale Verwaltung AWS-Konten innerhalb von AWS Organizations wird sichergestellt, dass die Konten den Vorschriften entsprechen. Eine fehlende zentrale Kontoverwaltung kann zu inkonsistenten Kontokonfigurationen führen, wodurch Ressourcen und sensible Daten offengelegt werden können.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	nutzen, Aufzeichnungen elektronisch signieren, auf den Vorgang oder das Eingabe- oder Ausgabegerät des Computersystems zugreifen, Aufzeichnungen ändern oder den betreffenden Vorgang ausführen können.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
11.10(g)	Personen, die geschlossene Systeme verwenden , um elektronische Aufzeichnungen zu erstellen, zu ändern, zu pflegen oder zu übertragen, müssen entsprech ende Verfahren und Kontrollen anwenden, um die Echtheit, Integritä t und gegebenen falls die Vertrauli chkeit elektronischer Aufzeichnungen sicherzustellen und dafür zu sorgen, dass die Unterzeic hneten die signierte Aufzeichnung nicht ohne Weiteres als unecht zurückwei sen können. Diese Verfahren und Kontrollen müssen Folgendes umfassen: (g) Durchführung von behördlichen Kontrollen, damit ausschließlich befugte Personen das System	dms-replication-not-public	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass auf DMS-Replikationsin stanzen nicht öffentlic h zugegriffen werden kann. DMS-Repli kations-Instances können vertrauli che Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	nutzen, Aufzeichnungen elektronisch signieren, auf den Vorgang oder das Eingabe- oder Ausgabegerät des Computersystems zugreifen, Aufzeichnungen ändern oder den betreffenden Vorgang ausführen können.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
11.10(g)	Personen, die geschlossene Systeme verwenden, um elektronische Aufzeichnungen zu erstellen, zu ändern, zu pflegen oder zu übertragen, müssen entsprechende Verfahren und Kontrollen anwenden, um die Echtheit, Integrität und gegebenenfalls die Vertraulichkeit elektronischer Aufzeichnungen sicherzustellen und dafür zu sorgen, dass die Unterzeichneten die signierte Aufzeichnung nicht ohne Weiteres als unecht zurückweisen können. Diese Verfahren und Kontrollen müssen Folgendes umfassen: (g) Durchführung von behördlichen Kontrollen, damit ausschließlich befugte Personen das System	dynamodb-table-encrypted-kms	Stellen Sie sicher, dass die Verschlüsselung für Ihre Amazon-DynamoDB-Tabellen aktiviert ist. Um eventuell vorhandene sensible Daten im Ruhezustand in diesen Tabellen zu schützen, müssen Sie die Verschlüsselung von Daten im Ruhezustand aktivieren. Standardmäßig werden DynamoDB-Tabellen mit einem AWS eigenen Kundenhauptschlüssel (CMK) verschlüsselt.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	nutzen, Aufzeichnungen elektronisch signieren, auf den Vorgang oder das Eingabe- oder Ausgabegerät des Computersystems zugreifen, Aufzeichnungen ändern oder den betreffenden Vorgang ausführen können.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
11.10(g)	Personen, die geschlossene Systeme verwenden , um elektronische Aufzeichnungen zu erstellen, zu ändern, zu pflegen oder zu übertragen, müssen entsprech ende Verfahren und Kontrollen anwenden, um die Echtheit, Integritä t und gegebenen falls die Vertrauli chkeit elektronischer Aufzeichnungen sicherzustellen und dafür zu sorgen, dass die Unterzeic hneten die signierte Aufzeichnung nicht ohne Weiteres als unecht zurückwei sen können. Diese Verfahren und Kontrollen müssen Folgendes umfassen: (g) Durchführung von behördlichen Kontrollen, damit ausschließlich befugte Personen das System	ebs-snapshot-public-restorable-überprüfen	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass EBS-Snapshots nicht öffentlich wiederher stellbar sind. EBS-Volume-Snapsho ts können vertrauli che Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	nutzen, Aufzeichnungen elektronisch signieren, auf den Vorgang oder das Eingabe- oder Ausgabegerät des Computersystems zugreifen, Aufzeichnungen ändern oder den betreffenden Vorgang ausführen können.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
11.10(g)	Personen, die geschlossene Systeme verwenden , um elektronische Aufzeichnungen zu erstellen, zu ändern, zu pflegen oder zu übertragen, müssen entsprech ende Verfahren und Kontrollen anwenden, um die Echtheit, Integritä t und gegebenen falls die Vertrauli chkeit elektronischer Aufzeichnungen sicherzustellen und dafür zu sorgen, dass die Unterzeic hneten die signierte Aufzeichnung nicht ohne Weiteres als unecht zurückwei sen können. Diese Verfahren und Kontrollen müssen Folgendes umfassen: (g) Durchführung von behördlichen Kontrollen, damit ausschließlich befugte Personen das System	ec-2 ebs-encryption-by-default	Zum Schutz von Daten im Ruhezusta nd müssen Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon Elastic Block Store (Amazon EBS)-Volu mes aktiviert ist. Da sensible Daten auch im Ruhezusta nd vorhanden sein können, sollten Sie die Verschlüsselung im Ruhezustand aktivieren, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	nutzen, Aufzeichnungen elektronisch signieren, auf den Vorgang oder das Eingabe- oder Ausgabegerät des Computersystems zugreifen, Aufzeichnungen ändern oder den betreffenden Vorgang ausführen können.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
11.10(g)	Personen, die geschlossene Systeme verwenden , um elektronische Aufzeichnungen zu erstellen, zu ändern, zu pflegen oder zu übertragen, müssen entsprech ende Verfahren und Kontrollen anwenden, um die Echtheit, Integritä t und gegebenen falls die Vertrauli chkeit elektronischer Aufzeichnungen sicherzustellen und dafür zu sorgen, dass die Unterzeic hneten die signierte Aufzeichnung nicht ohne Weiteres als unecht zurückwei sen können. Diese Verfahren und Kontrollen müssen Folgendes umfassen: (g) Durchführung von behördlichen Kontrollen, damit ausschließlich befugte Personen das System	ec2-imdsv2-check	Stellen Sie sicher, dass die Methode Instance Metadata Service Version 2 (IMDSv2) aktiviert ist, um den Zugriff auf und die Kontrolle der Amazon Elastic Compute Cloud (Amazon EC2) - Instance-Metadate n zu schützen. Die IMDSv2 Methode verwendet sitzungsb asierte Kontrollen. Mit können Kontrolle n implementiert werden IMDSv2, um Änderungen an Instanzmetadaten einzuschränken.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	nutzen, Aufzeichnungen elektronisch signieren, auf den Vorgang oder das Eingabe- oder Ausgabegerät des Computersystems zugreifen, Aufzeichnungen ändern oder den betreffenden Vorgang ausführen können.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
11.10(g)	Personen, die geschlossene Systeme verwenden , um elektronische Aufzeichnungen zu erstellen, zu ändern, zu pflegen oder zu übertragen, müssen entsprech ende Verfahren und Kontrollen anwenden, um die Echtheit, Integritä t und gegebenen falls die Vertrauli chkeit elektronischer Aufzeichnungen sicherzustellen und dafür zu sorgen, dass die Unterzeic hneten die signierte Aufzeichnung nicht ohne Weiteres als unecht zurückwei sen können. Diese Verfahren und Kontrollen müssen Folgendes umfassen: (g) Durchführung von behördlichen Kontrollen, damit ausschließlich befugte Personen das System	ec-2 instance-no-public-ip	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon Elastic Compute Cloud (Amazon EC2) - Instances nicht öffentlich zugänglich sind. EC2 Amazon-Instances können vertrauliche Informati onen enthalten, und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	nutzen, Aufzeichnungen elektronisch signieren, auf den Vorgang oder das Eingabe- oder Ausgabegerät des Computersystems zugreifen, Aufzeichnungen ändern oder den betreffenden Vorgang ausführen können.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
11.10(g)	Personen, die geschlossene Systeme verwenden , um elektronische Aufzeichnungen zu erstellen, zu ändern, zu pflegen oder zu übertragen, müssen entsprech ende Verfahren und Kontrollen anwenden, um die Echtheit, Integritä t und gegebenen falls die Vertrauli chkeit elektronischer Aufzeichnungen sicherzustellen und dafür zu sorgen, dass die Unterzeic hneten die signierte Aufzeichnung nicht ohne Weiteres als unecht zurückwei sen können. Diese Verfahren und Kontrollen müssen Folgendes umfassen: (g) Durchführung von behördlichen Kontrollen, damit ausschließlich befugte Personen das System	ec2- instance-profile-a ttached	EC2 Instanzprofile übergeben eine IAM-Rolle an eine EC2 Instance. Das Anhängen eines Instance-Profils an Ihre Instances kann bei der Implement ierung von geringste n Berechtigungen und der Berechtig ungsverwaltung helfen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	nutzen, Aufzeichnungen elektronisch signieren, auf den Vorgang oder das Eingabe- oder Ausgabegerät des Computersystems zugreifen, Aufzeichnungen ändern oder den betreffenden Vorgang ausführen können.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
11.10(g)	Personen, die geschlossene Systeme verwenden , um elektronische Aufzeichnungen zu erstellen, zu ändern, zu pflegen oder zu übertragen, müssen entsprech ende Verfahren und Kontrollen anwenden, um die Echtheit, Integritä t und gegebenen falls die Vertrauli chkeit elektronischer Aufzeichnungen sicherzustellen und dafür zu sorgen, dass die Unterzeic hneten die signierte Aufzeichnung nicht ohne Weiteres als unecht zurückwei sen können. Diese Verfahren und Kontrollen müssen Folgendes umfassen: (g) Durchführung von behördlichen Kontrollen, damit ausschließlich befugte Personen das System	ecs-task-definition-user-for-host-mode-check	Wenn für eine Aufgabendefinition erhöhte Berechtig ungen gelten, liegt das daran, dass der Kunde diesen Konfigura tionen ausdrücklich zugestimmt hat. Diese Kontrolle prüft, ob eine unerwartete Berechtigungseskal ation vorliegt, wenn für eine Aufgabend efinition das Host-Netzwerk aktiviert ist, die Kunden aber keine erhöhten Berechtigungen aktiviert haben.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	nutzen, Aufzeichnungen elektronisch signieren, auf den Vorgang oder das Eingabe- oder Ausgabegerät des Computersystems zugreifen, Aufzeichnungen ändern oder den betreffenden Vorgang ausführen können.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
11.10(g)	Personen, die geschlossene Systeme verwenden , um elektronische Aufzeichnungen zu erstellen, zu ändern, zu pflegen oder zu übertragen, müssen entsprech ende Verfahren und Kontrollen anwenden, um die Echtheit, Integritä t und gegebenen falls die Vertrauli chkeit elektronischer Aufzeichnungen sicherzustellen und dafür zu sorgen, dass die Unterzeic hneten die signierte Aufzeichnung nicht ohne Weiteres als unecht zurückwei sen können. Diese Verfahren und Kontrollen müssen Folgendes umfassen: (g) Durchführung von behördlichen Kontrollen, damit ausschließlich befugte Personen das System	efs-encrypted-check	Aktivieren Sie die Verschlüsselung für Ihr Amazon Elastic File System (EFS), um eventuell vorhandene sensible Daten sowie Daten im Ruhezustand zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	nutzen, Aufzeichnungen elektronisch signieren, auf den Vorgang oder das Eingabe- oder Ausgabegerät des Computersystems zugreifen, Aufzeichnungen ändern oder den betreffenden Vorgang ausführen können.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
11.10(g)	Personen, die geschlossene Systeme verwenden , um elektronische Aufzeichnungen zu erstellen, zu ändern, zu pflegen oder zu übertragen, müssen entsprech ende Verfahren und Kontrollen anwenden, um die Echtheit, Integritä t und gegebenen falls die Vertrauli chkeit elektronischer Aufzeichnungen sicherzustellen und dafür zu sorgen, dass die Unterzeic hneten die signierte Aufzeichnung nicht ohne Weiteres als unecht zurückwei sen können. Diese Verfahren und Kontrollen müssen Folgendes umfassen: (g) Durchführung von behördlichen Kontrollen, damit ausschließlich befugte Personen das System	elasticsearch-encr ypted-at-rest	Da sensible Daten vorhanden sein können und um Daten im Ruhezustand zu schützen, sollten Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon OpenSearch Service (OpenSearch Service) -Domains aktiviert ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	nutzen, Aufzeichnungen elektronisch signieren, auf den Vorgang oder das Eingabe- oder Ausgabegerät des Computersystems zugreifen, Aufzeichnungen ändern oder den betreffenden Vorgang ausführen können.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
11.10(g)	Personen, die geschlossene Systeme verwenden , um elektronische Aufzeichnungen zu erstellen, zu ändern, zu pflegen oder zu übertragen, müssen entsprech ende Verfahren und Kontrollen anwenden, um die Echtheit, Integritä t und gegebenen falls die Vertrauli chkeit elektronischer Aufzeichnungen sicherzustellen und dafür zu sorgen, dass die Unterzeic hneten die signierte Aufzeichnung nicht ohne Weiteres als unecht zurückwei sen können. Diese Verfahren und Kontrollen müssen Folgendes umfassen: (g) Durchführung von behördlichen Kontrollen, damit ausschließlich befugte Personen das System	elasticsearch-in-vpc-only	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherste llen, dass sich Amazon OpenSearc h OpenSearch Service (Service) - Domains innerhalb einer Amazon Virtual Private Cloud (Amazon VPC) befinden. Eine OpenSearch Service-Domain innerhalb einer Amazon VPC ermöglicht die sichere Kommunikation zwischen OpenSearc h Service und anderen Services innerhalb der Amazon VPC, ohne dass ein Internet-Gateway, ein NAT-Gerät oder eine VPN-Verbindung erforderlich ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	nutzen, Aufzeichnungen elektronisch signieren, auf den Vorgang oder das Eingabe- oder Ausgabegerät des Computersystems zugreifen, Aufzeichnungen ändern oder den betreffenden Vorgang ausführen können.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
11.10(g)	Personen, die geschlossene Systeme verwenden , um elektronische Aufzeichnungen zu erstellen, zu ändern, zu pflegen oder zu übertragen, müssen entsprech ende Verfahren und Kontrollen anwenden, um die Echtheit, Integritä t und gegebenen falls die Vertrauli chkeit elektronischer Aufzeichnungen sicherzustellen und dafür zu sorgen, dass die Unterzeic hneten die signierte Aufzeichnung nicht ohne Weiteres als unecht zurückwei sen können. Diese Verfahren und Kontrollen müssen Folgendes umfassen: (g) Durchführung von behördlichen Kontrollen, damit ausschließlich befugte Personen das System	elasticsearch-node -to-node-Verschlüs selungsprüfung	Stellen Sie sicher, dass die node-to-node Verschlüs selung für Amazon OpenSearch Service aktiviert ist. Node-to-nodeVerschlüsselung ermöglicht die TLS 1.2-Verschlüsselun g für die gesamte Kommunikation innerhalb der Amazon Virtual Private Cloud (Amazon VPC). Um eventuell vorhanden e sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	nutzen, Aufzeichnungen elektronisch signieren, auf den Vorgang oder das Eingabe- oder Ausgabegerät des Computersystems zugreifen, Aufzeichnungen ändern oder den betreffenden Vorgang ausführen können.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
11.10(g)	Personen, die geschlossene Systeme verwenden , um elektronische Aufzeichnungen zu erstellen, zu ändern, zu pflegen oder zu übertragen, müssen entsprech ende Verfahren und Kontrollen anwenden, um die Echtheit, Integritä t und gegebenen falls die Vertrauli chkeit elektronischer Aufzeichnungen sicherzustellen und dafür zu sorgen, dass die Unterzeic hneten die signierte Aufzeichnung nicht ohne Weiteres als unecht zurückwei sen können. Diese Verfahren und Kontrollen müssen Folgendes umfassen: (g) Durchführung von behördlichen Kontrollen, damit ausschließlich befugte Personen das System	emr-kerberos-enabled	Die Zugriffsberechtigu ngen und -autorisi erungen können verwaltet und nach den Prinzipien der geringsten Berechtig ung und Aufgabent rennung integrier t werden, indem Kerberos für Amazon-EMR-Cluster aktiviert wird. In Kerberos werden Services und Benutzer, die sich authentif izieren müssen, als Prinzipale bezeichnet. Prinzipal e befinden sich in einem Kerberos-Bereich. Innerhalb dieses Bereichs wird ein Kerberos-Server als Key Distribution Center (KDC) bezeichnet. Über diesen Server können sich Prinzipal e authentifizieren. Die Authentifizierung im KDC erfolgt durch die Ausstellu ng von Authentif

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	nutzen, Aufzeichnungen elektronisch signieren, auf den Vorgang oder das Eingabe- oder Ausgabegerät des Computersystems zugreifen, Aufzeichnungen ändern oder den betreffenden Vorgang ausführen können.		izierungstickets. Das KDC unterhält eine Datenbank der Prinzipale in seinem Bereich mit ihren Passwörtern und anderen administrativen Informationen zu jedem Prinzipal.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
11.10(g)	Personen, die geschlossene Systeme verwenden , um elektronische Aufzeichnungen zu erstellen, zu ändern, zu pflegen oder zu übertragen, müssen entsprech ende Verfahren und Kontrollen anwenden, um die Echtheit, Integritä t und gegebenen falls die Vertrauli chkeit elektronischer Aufzeichnungen sicherzustellen und dafür zu sorgen, dass die Unterzeic hneten die signierte Aufzeichnung nicht ohne Weiteres als unecht zurückwei sen können. Diese Verfahren und Kontrollen müssen Folgendes umfassen: (g) Durchführung von behördlichen Kontrollen, damit ausschließlich befugte Personen das System	emr-master-no-public-ip	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon EMR-Clust er-Masterknoten nicht öffentlich zugänglic h sind. Amazon-EM R-Cluster-Hauptkno ten können vertrauli che Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	nutzen, Aufzeichnungen elektronisch signieren, auf den Vorgang oder das Eingabe- oder Ausgabegerät des Computersystems zugreifen, Aufzeichnungen ändern oder den betreffenden Vorgang ausführen können.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
11.10(g)	Personen, die geschlossene Systeme verwenden , um elektronische Aufzeichnungen zu erstellen, zu ändern, zu pflegen oder zu übertragen, müssen entsprech ende Verfahren und Kontrollen anwenden, um die Echtheit, Integritä t und gegebenen falls die Vertrauli chkeit elektronischer Aufzeichnungen sicherzustellen und dafür zu sorgen, dass die Unterzeic hneten die signierte Aufzeichnung nicht ohne Weiteres als unecht zurückwei sen können. Diese Verfahren und Kontrollen müssen Folgendes umfassen: (g) Durchführung von behördlichen Kontrollen, damit ausschließlich befugte Personen das System	encrypted-volumes	Aktivieren Sie die Verschlüsselung für Ihre Amazon-Elastic-Block-Store (Amazon-EBS)-Volumes, um eventuell vorhandene sensible Daten sowie Daten im Ruhezusta nd zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	nutzen, Aufzeichnungen elektronisch signieren, auf den Vorgang oder das Eingabe- oder Ausgabegerät des Computersystems zugreifen, Aufzeichnungen ändern oder den betreffenden Vorgang ausführen können.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
11.10(g)	Personen, die geschlossene Systeme verwenden, um elektronische Aufzeichnungen zu erstellen, zu ändern, zu pflegen oder zu übertragen, müssen entsprechende Verfahren und Kontrollen anwenden, um die Echtheit, Integrität und gegebenenfalls die Vertraulichkeit elektronischer Aufzeichnungen sicherzustellen und dafür zu sorgen, dass die Unterzeichneten die signierte Aufzeichnung nicht ohne Weiteres als unecht zurückweisen können. Diese Verfahren und Kontrollen müssen Folgendes umfassen: (g) Durchführung von behördlichen Kontrollen, damit ausschließlich befugte Personen das System	iam-customer-policy-blocked-kms-Aktionen	AWS Identity and Access Management (IAM) kann Ihnen helfen, die Prinzipien der geringsten Rechte und der Aufgabentrennung in Zugriffsberechtigungen und Autorisierungen zu integrieren und so zu verhindern, dass Richtlinien blockierte Aktionen für alle AWS Schlüssel des Key Management Service enthalten. Wenn Benutzer mehr Rechte haben, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und Aufgabentrennung verstoßen. Mit dieser Regel können Sie den Parameter festlegen. blockedActionsPatterns (Wert „AWS Bewährte grundlegende Sicherheitsmethoden“: kms:

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	nutzen, Aufzeichnungen elektronisch signieren, auf den Vorgang oder das Eingabe- oder Ausgabegerät des Computersystems zugreifen, Aufzeichnungen ändern oder den betreffenden Vorgang ausführen können.		Decrypt, kms:ReEncryptFrom). Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
11.10(g)	Personen, die geschlossene Systeme verwenden, um elektronische Aufzeichnungen zu erstellen, zu ändern, zu pflegen oder zu übertragen, müssen entsprechende Verfahren und Kontrollen anwenden, um die Echtheit, Integrität und gegebenenfalls die Vertraulichkeit elektronischer Aufzeichnungen sicherzustellen und dafür zu sorgen, dass die Unterzeichneten die signierte Aufzeichnung nicht ohne Weiteres als unecht zurückweisen können. Diese Verfahren und Kontrollen müssen Folgendes umfassen: (g) Durchführung von behördlichen Kontrollen, damit ausschließlich befugte Personen das System	iam-group-has-users-überprüfen	AWS Identity and Access Management (IAM) kann Ihnen helfen, die Prinzipien der geringsten Rechte und der Aufgabentrennung mit Zugriffsberechtigungen und Autorisierungen zu integrieren, indem sichergestellt wird, dass IAM-Gruppen mindestens einen Benutzer haben. Die Einteilung von Benutzern in Gruppen auf der Grundlage der ihnen zugewiesenen Berechtigungen oder ihrer Funktion ist eine Möglichkeit, das Prinzip der geringsten Berechtigung zu implementieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	nutzen, Aufzeichnungen elektronisch signieren, auf den Vorgang oder das Eingabe- oder Ausgabegerät des Computersystems zugreifen, Aufzeichnungen ändern oder den betreffenden Vorgang ausführen können.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
11.10(g)	Personen, die geschlossene Systeme verwenden , um elektronische Aufzeichnungen zu erstellen, zu ändern, zu pflegen oder zu übertragen, müssen entsprech ende Verfahren und Kontrollen anwenden, um die Echtheit, Integritä t und gegebenen falls die Vertrauli chkeit elektronischer Aufzeichnungen sicherzustellen und dafür zu sorgen, dass die Unterzeic hneten die signierte Aufzeichnung nicht ohne Weiteres als unecht zurückwei sen können. Diese Verfahren und Kontrollen müssen Folgendes umfassen: (g) Durchführung von behördlichen Kontrollen, damit ausschließlich befugte Personen das System	iam-inline-policy-blocked-kms-Aktionen	Stellen Sie sicher, dass ein Benutzer, eine IAM-Rolle oder eine IAM-Gruppe (AWS Identity and Access Management) nicht über eine Inline-Richtlinie verfügt, die blockierte Aktionen für alle AWS Schlüssel des Key Management Service zulässt. AWS empfiehlt, verwaltet e Richtlinien anstelle von Inline-Richtlinien zu verwenden. Verwaltete Richtlini en ermöglichen Wiederverwendbarke it, Versionsverwaltung , Rollback und Delegierung der Berechtigungsverwa ltung. Mit dieser Regel können Sie den blockedActionsPatt erns Parameter festlegen. (Wert „AWS Bewährte grundlege nde Sicherhei tsmethoden“: kms: Decrypt, kms:ReEnc ryptFrom). Die

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	nutzen, Aufzeichnungen elektronisch signieren, auf den Vorgang oder das Eingabe- oder Ausgabegerät des Computersystems zugreifen, Aufzeichnungen ändern oder den betreffenden Vorgang ausführen können.		tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
11.10(g)	Personen, die geschlossene Systeme verwenden , um elektronische Aufzeichnungen zu erstellen, zu ändern, zu pflegen oder zu übertragen, müssen entsprech ende Verfahren und Kontrollen anwenden, um die Echtheit, Integritä t und gegebenen falls die Vertrauli chkeit elektronischer Aufzeichnungen sicherzustellen und dafür zu sorgen, dass die Unterzeic hneten die signierte Aufzeichnung nicht ohne Weiteres als unecht zurückwei sen können. Diese Verfahren und Kontrollen müssen Folgendes umfassen: (g) Durchführung von behördlichen Kontrollen, damit ausschließlich befugte Personen das System	iam-no-inline-policy-überprüfen	Stellen Sie sicher, dass ein Benutzer, eine IAM-Rolle oder eine IAM-Gruppe (AWS Identity and Access Management) nicht über eine Inline-Richtlinie zur Zugriffsk ontrolle auf Systeme und Ressource n verfügt. AWS empfiehlt, verwaltet e Richtlinien anstelle von Inline-Richtlinien zu verwenden. Verwaltete Richtlini en ermöglichen Wiederverwendbarke it, Versionsverwaltung , Rollback und Delegierung der Berechtigungsverwa ltung.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	nutzen, Aufzeichnungen elektronisch signieren, auf den Vorgang oder das Eingabe- oder Ausgabegerät des Computersystems zugreifen, Aufzeichnungen ändern oder den betreffenden Vorgang ausführen können.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
11.10(g)	Personen, die geschlossene Systeme verwenden , um elektronische Aufzeichnungen zu erstellen, zu ändern, zu pflegen oder zu übertragen, müssen entsprech ende Verfahren und Kontrollen anwenden, um die Echtheit, Integritä t und gegebenen falls die Vertrauli chkeit elektronischer Aufzeichnungen sicherzustellen und dafür zu sorgen, dass die Unterzeic hneten die signierte Aufzeichnung nicht ohne Weiteres als unecht zurückwei sen können. Diese Verfahren und Kontrollen müssen Folgendes umfassen: (g) Durchführung von behördlichen Kontrollen, damit ausschließlich befugte Personen das System	iam-password-policy	Die Identitäten und Anmeldeinformation en werden auf der Grundlage einer organisatorischen IAM-Passwortrichtlinie ausgestellt, verwaltet und verifiziert. Sie erfüllen oder übertreff en die Anforderungen von NIST SP 800-63 und dem Standard „Best Practices“ von AWS Foundatio nal Security für die Passwortstärke. Mit dieser Regel können Sie optional RequireUppercaseCh aracters (Wert für AWS grundlegende Sicherheitsbewährt e Verfahren: wahr), RequireLowercaseCh aracters (Wert für bewährte Methoden für AWS grundlege nde Sicherheit: wahr), RequireSy mbols (Wert für bewährte Methoden für AWS grundlege nde Sicherheit:

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	nutzen, Aufzeichnungen elektronisch signieren, auf den Vorgang oder das Eingabe- oder Ausgabegerät des Computersystems zugreifen, Aufzeichnungen ändern oder den betreffenden Vorgang ausführen können.		wahr), RequireNumbers (Wert für bewährte Methoden für AWS grundlegende Sicherheit: wahr), MinimumPasswordLength (Wert für bewährte Methoden für AWS grundlegende Sicherheit: 14), PasswordReusePrevention (Wert für bewährte Methoden für AWS grundlegende Sicherheit: 24) und MaxPasswordAge (Wert für bewährte Methoden für AWS grundlegende Sicherheit: 90) für Ihr IAM festlegen Kennwortrichtlinie. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
11.10(g)	Personen, die geschlossene Systeme verwenden, um elektronische Aufzeichnungen zu erstellen, zu ändern, zu pflegen oder zu übertragen, müssen entsprechende Verfahren und Kontrollen anwenden, um die Echtheit, Integrität und gegebenenfalls die Vertraulichkeit elektronischer Aufzeichnungen sicherzustellen und dafür zu sorgen, dass die Unterzeichneten die signierte Aufzeichnung nicht ohne Weiteres als unecht zurückweisen können. Diese Verfahren und Kontrollen müssen Folgendes umfassen: (g) Durchführung von behördlichen Kontrollen, damit ausschließlich befugte Personen das System	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) kann Ihnen dabei helfen, die Prinzipien der geringsten Rechte und der Aufgabentrennung in Zugriffsberechtigungen und Autorisierungen zu integrieren und so zu verhindern, dass Richtlinien „Effect“: „Allow“ mit „Action“: „*“ anstelle von „Resource“: „*“ enthalten. Wenn Benutzern mehr Rechte eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und der Aufgabentrennung verstoßen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	nutzen, Aufzeichnungen elektronisch signieren, auf den Vorgang oder das Eingabe- oder Ausgabegerät des Computersystems zugreifen, Aufzeichnungen ändern oder den betreffenden Vorgang ausführen können.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
11.10(g)	Personen, die geschlossene Systeme verwenden, um elektronische Aufzeichnungen zu erstellen, zu ändern, zu pflegen oder zu übertragen, müssen entsprechende Verfahren und Kontrollen anwenden, um die Echtheit, Integrität und gegebenenfalls die Vertraulichkeit elektronischer Aufzeichnungen sicherzustellen und dafür zu sorgen, dass die Unterzeichneten die signierte Aufzeichnung nicht ohne Weiteres als unecht zurückweisen können. Diese Verfahren und Kontrollen müssen Folgendes umfassen: (g) Durchführung von behördlichen Kontrollen, damit ausschließlich befugte Personen das System	iam-policy-no-statements-with-full-access	Stellen Sie sicher, dass IAM-Aktionen nur auf die benötigten Aktionen beschränkt sind. Wenn Benutzern mehr Rechte eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und der Aufgabentrennung verstoßen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	nutzen, Aufzeichnungen elektronisch signieren, auf den Vorgang oder das Eingabe- oder Ausgabegerät des Computersystems zugreifen, Aufzeichnungen ändern oder den betreffenden Vorgang ausführen können.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
11.10(g)	Personen, die geschlossene Systeme verwenden , um elektronische Aufzeichnungen zu erstellen, zu ändern, zu pflegen oder zu übertragen, müssen entsprech ende Verfahren und Kontrollen anwenden, um die Echtheit, Integritä t und gegebenen falls die Vertrauli chkeit elektronischer Aufzeichnungen sicherzustellen und dafür zu sorgen, dass die Unterzeic hneten die signierte Aufzeichnung nicht ohne Weiteres als unecht zurückwei sen können. Diese Verfahren und Kontrollen müssen Folgendes umfassen: (g) Durchführung von behördlichen Kontrollen, damit ausschließlich befugte Personen das System	iam-root-access-key-überprüfen	Der Zugriff auf Systeme und Ressourcen kann gesteuert werden, indem überprüft wird, ob der Root-Benu tzer keine Zugriffss chlüssel mit seiner AWS Identity and Access Management (IAM) -Rolle verknüpft hat. Stellen Sie sicher, dass die Root-Zugr iffsschlüssel gelöscht werden. Erstellen und verwenden Sie stattdessen rollenbas ierte Funktionen, AWS-Konten um das Prinzip der geringste n Funktionalität zu berücksichtigen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	nutzen, Aufzeichnungen elektronisch signieren, auf den Vorgang oder das Eingabe- oder Ausgabegerät des Computersystems zugreifen, Aufzeichnungen ändern oder den betreffenden Vorgang ausführen können.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
11.10(g)	Personen, die geschlossene Systeme verwenden, um elektronische Aufzeichnungen zu erstellen, zu ändern, zu pflegen oder zu übertragen, müssen entsprechende Verfahren und Kontrollen anwenden, um die Echtheit, Integrität und gegebenenfalls die Vertraulichkeit elektronischer Aufzeichnungen sicherzustellen und dafür zu sorgen, dass die Unterzeichneten die signierte Aufzeichnung nicht ohne Weiteres als unecht zurückweisen können. Diese Verfahren und Kontrollen müssen Folgendes umfassen: (g) Durchführung von behördlichen Kontrollen, damit ausschließlich befugte Personen das System	iam-user-group-membership-überprüfen	AWS Identity and Access Management (IAM) kann Ihnen helfen, Zugriffsberechtigungen und Autorisierungen einzuschränken, indem sichergestellt wird, dass Benutzer Mitglieder mindestens einer Gruppe sind. Wenn Benutzern mehr Berechtigungen eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und Aufgabentrennung verstoßen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	nutzen, Aufzeichnungen elektronisch signieren, auf den Vorgang oder das Eingabe- oder Ausgabegerät des Computersystems zugreifen, Aufzeichnungen ändern oder den betreffenden Vorgang ausführen können.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
11.10(g)	Personen, die geschlossene Systeme verwenden , um elektronische Aufzeichnungen zu erstellen, zu ändern, zu pflegen oder zu übertragen, müssen entsprech ende Verfahren und Kontrollen anwenden, um die Echtheit, Integritä t und gegebenen falls die Vertrauli chkeit elektronischer Aufzeichnungen sicherzustellen und dafür zu sorgen, dass die Unterzeic hneten die signierte Aufzeichnung nicht ohne Weiteres als unecht zurückwei sen können. Diese Verfahren und Kontrollen müssen Folgendes umfassen: (g) Durchführung von behördlichen Kontrollen, damit ausschließlich befugte Personen das System	iam-user-mfa-enabled	Aktivieren Sie diese Regel, um den Zugriff auf Ressourcen in der AWS Cloud einzuschr änken. Diese Regel sorgt dafür, dass die Multi-Faktor-Authe ntifizierung (MFA) für alle Benutzer aktiviert ist. MFA sorgt für eine weitere Schutzebe ne zusätzlich zu den Anmeldeinformation en. Reduzieren Sie Fälle von kompromit tierten Konten, indem Sie MFA für Benutzer vorschreiben.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	nutzen, Aufzeichnungen elektronisch signieren, auf den Vorgang oder das Eingabe- oder Ausgabegerät des Computersystems zugreifen, Aufzeichnungen ändern oder den betreffenden Vorgang ausführen können.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
11.10(g)	Personen, die geschlossene Systeme verwenden , um elektronische Aufzeichnungen zu erstellen, zu ändern, zu pflegen oder zu übertragen, müssen entsprech ende Verfahren und Kontrollen anwenden, um die Echtheit, Integritä t und gegebenen falls die Vertrauli chkeit elektronischer Aufzeichnungen sicherzustellen und dafür zu sorgen, dass die Unterzeic hneten die signierte Aufzeichnung nicht ohne Weiteres als unecht zurückwei sen können. Diese Verfahren und Kontrollen müssen Folgendes umfassen: (g) Durchführung von behördlichen Kontrollen, damit ausschließlich befugte Personen das System	iam-user-no-policies-überprüfen	Diese Regel stellt sicher, dass AWS Identity and Access Management (IAM) -Richtlinien nur Gruppen oder Rollen zugewiese n werden, um den Zugriff auf Systeme und Ressourcen zu kontrollieren. Die Zuweisung von Berechtig ungen auf Gruppen- oder Rollenebene trägt dazu bei, die Wahrscheinlichkeit zu verringern, dass eine Identität übermäßige Berechtigungen erhält oder beibehält.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	nutzen, Aufzeichnungen elektronisch signieren, auf den Vorgang oder das Eingabe- oder Ausgabegerät des Computersystems zugreifen, Aufzeichnungen ändern oder den betreffenden Vorgang ausführen können.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
11.10(g)	Personen, die geschlossene Systeme verwenden , um elektronische Aufzeichnungen zu erstellen, zu ändern, zu pflegen oder zu übertragen, müssen entsprech ende Verfahren und Kontrollen anwenden, um die Echtheit, Integritä t und gegebenen falls die Vertrauli chkeit elektronischer Aufzeichnungen sicherzustellen und dafür zu sorgen, dass die Unterzeic hneten die signierte Aufzeichnung nicht ohne Weiteres als unecht zurückwei sen können. Diese Verfahren und Kontrollen müssen Folgendes umfassen: (g) Durchführung von behördlichen Kontrollen, damit ausschließlich befugte Personen das System	iam-user-no-policies-überprüfen	Diese Regel stellt sicher, dass AWS Identity and Access Management (IAM) -Richtlinien nur Gruppen oder Rollen zugewiese n werden, um den Zugriff auf Systeme und Ressourcen zu kontrollieren. Die Zuweisung von Berechtig ungen auf Gruppen- oder Rollenebene trägt dazu bei, die Wahrscheinlichkeit zu verringern, dass eine Identität übermäßige Berechtigungen erhält oder beibehält.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	nutzen, Aufzeichnungen elektronisch signieren, auf den Vorgang oder das Eingabe- oder Ausgabegerät des Computersystems zugreifen, Aufzeichnungen ändern oder den betreffenden Vorgang ausführen können.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
11.10(g)	Personen, die geschlossene Systeme verwenden, um elektronische Aufzeichnungen zu erstellen, zu ändern, zu pflegen oder zu übertragen, müssen entsprechende Verfahren und Kontrollen anwenden, um die Echtheit, Integrität und gegebenenfalls die Vertraulichkeit elektronischer Aufzeichnungen sicherzustellen und dafür zu sorgen, dass die Unterzeichneten die signierte Aufzeichnung nicht ohne Weiteres als unecht zurückweisen können. Diese Verfahren und Kontrollen müssen Folgendes umfassen: (g) Durchführung von behördlichen Kontrollen, damit ausschließlich befugte Personen das System	iam-user-unused-credentials-überprüfen	AWS Identity and Access Management (IAM) kann Ihnen bei Zugriffsberechtigungen und Autorisierungen helfen, indem es nach IAM-Passwörtern und Zugriffsschlüsseln sucht, die für einen bestimmten Zeitraum nicht verwendet wurden. Wenn ungenutzte Anmeldeinformationen identifiziert werden, müssen Sie sie deaktivieren und/oder entfernen, da dies gegen das Prinzip der geringsten Berechtigung verstoßen könnte. Für diese Regel müssen Sie einen Wert für das maxCredentialUsage Alter festlegen (Standardkonfiguration: 90). Der tatsächliche Wert muss den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	nutzen, Aufzeichnungen elektronisch signieren, auf den Vorgang oder das Eingabe- oder Ausgabegerät des Computersystems zugreifen, Aufzeichnungen ändern oder den betreffenden Vorgang ausführen können.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
11.10(g)	Personen, die geschlossene Systeme verwenden , um elektronische Aufzeichnungen zu erstellen, zu ändern, zu pflegen oder zu übertragen, müssen entsprech ende Verfahren und Kontrollen anwenden, um die Echtheit, Integritä t und gegebenen falls die Vertrauli chkeit elektronischer Aufzeichnungen sicherzustellen und dafür zu sorgen, dass die Unterzeic hneten die signierte Aufzeichnung nicht ohne Weiteres als unecht zurückwei sen können. Diese Verfahren und Kontrollen müssen Folgendes umfassen: (g) Durchführung von behördlichen Kontrollen, damit ausschließlich befugte Personen das System	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) Security Groups können bei der Verwaltung des Netzwerkzugriffs helfen, indem sie eine statusbeh aftete Filterung von eingehendem und ausgehendem Netzwerkverkehr zu Ressourcen bereitste llen. AWS Wenn Sie eingehenden (oder entfernten) Datenverk ehr von 0.0.0.0/0 bis Port 22 auf Ihren Ressourcen nicht zulassen, können Sie den Remote-Zugriff einschränken.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	nutzen, Aufzeichnungen elektronisch signieren, auf den Vorgang oder das Eingabe- oder Ausgabegerät des Computersystems zugreifen, Aufzeichnungen ändern oder den betreffenden Vorgang ausführen können.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
11.10(g)	Personen, die geschlossene Systeme verwenden , um elektronische Aufzeichnungen zu erstellen, zu ändern, zu pflegen oder zu übertragen, müssen entsprech ende Verfahren und Kontrollen anwenden, um die Echtheit, Integritä t und gegebenen falls die Vertrauli chkeit elektronischer Aufzeichnungen sicherzustellen und dafür zu sorgen, dass die Unterzeic hneten die signierte Aufzeichnung nicht ohne Weiteres als unecht zurückwei sen können. Diese Verfahren und Kontrollen müssen Folgendes umfassen: (g) Durchführung von behördlichen Kontrollen, damit ausschließlich befugte Personen das System	ec-2 instances-in-vpc	Stellen Sie Amazon Elastic Compute Cloud (Amazon EC2) -Instances innerhalb einer Amazon Virtual Private Cloud (Amazon VPC) bereit, um eine sichere Kommunika tion zwischen einer Instance und anderen Services innerhalb der Amazon VPC zu ermöglichen, ohne dass ein Internet-Gateway, ein NAT-Gerät oder eine VPN-Verbindung erforderlich ist. Der gesamte Datenverk ehr bleibt sicher in der AWS Cloud. Domains, die sich innerhalb einer VPC befinden, verfügen aufgrund ihrer logischen Isolierun g im Vergleich zu Domains mit öffentlic hen Endpunkten über eine zusätzlic he Sicherheitsebene. Weisen Sie EC2

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	nutzen, Aufzeichnungen elektronisch signieren, auf den Vorgang oder das Eingabe- oder Ausgabegerät des Computersystems zugreifen, Aufzeichnungen ändern oder den betreffenden Vorgang ausführen können.		Amazon-Instances einer Amazon-VPC zu, um den Zugriff ordnungsgemäß zu verwalten.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
11.10(g)	Personen, die geschlossene Systeme verwenden, um elektronische Aufzeichnungen zu erstellen, zu ändern, zu pflegen oder zu übertragen, müssen entsprechende Verfahren und Kontrollen anwenden, um die Echtheit, Integrität und gegebenenfalls die Vertraulichkeit elektronischer Aufzeichnungen sicherzustellen und dafür zu sorgen, dass die Unterzeichneten die signierte Aufzeichnung nicht ohne Weiteres als unecht zurückweisen können. Diese Verfahren und Kontrollen müssen Folgendes umfassen: (g) Durchführung von behördlichen Kontrollen, damit ausschließlich befugte Personen das System	lambda-function-public-access-verboten	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass AWS Lambda-Funktionen nicht öffentlich zugänglich sind. Der öffentliche Zugriff kann möglicherweise die Verfügbarkeit von Ressourcen beeinträchtigen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	nutzen, Aufzeichnungen elektronisch signieren, auf den Vorgang oder das Eingabe- oder Ausgabegerät des Computersystems zugreifen, Aufzeichnungen ändern oder den betreffenden Vorgang ausführen können.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
11.10(g)	Personen, die geschlossene Systeme verwenden , um elektronische Aufzeichnungen zu erstellen, zu ändern, zu pflegen oder zu übertragen, müssen entsprech ende Verfahren und Kontrollen anwenden, um die Echtheit, Integritä t und gegebenen falls die Vertrauli chkeit elektronischer Aufzeichnungen sicherzustellen und dafür zu sorgen, dass die Unterzeic hneten die signierte Aufzeichnung nicht ohne Weiteres als unecht zurückwei sen können. Diese Verfahren und Kontrollen müssen Folgendes umfassen: (g) Durchführung von behördlichen Kontrollen, damit ausschließlich befugte Personen das System	lambda-inside-vpc	Stellen Sie AWS Lambda-Funktionen in einer Amazon Virtual Private Cloud (Amazon VPC) bereit, um eine sichere Kommunika tion zwischen einer Funktion und anderen Diensten innerhalb der Amazon VPC zu gewährleisten. Bei dieser Konfiguration sind kein Internet-Gateway, kein NAT-Gerät und keine VPN-Verbindung erforderlich. Der gesamte Datenverk ehr bleibt sicher in der Cloud. AWS Domains, die sich innerhalb einer VPC befinden, verfügen aufgrund ihrer logischen Isolierun g im Vergleich zu Domains mit öffentlic hen Endpunkten über eine zusätzliche Sicherheitsebene. Um den Zugriff ordnungsg emäß zu verwalten,

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	nutzen, Aufzeichnungen elektronisch signieren, auf den Vorgang oder das Eingabe- oder Ausgabegerät des Computersystems zugreifen, Aufzeichnungen ändern oder den betreffenden Vorgang ausführen können.		sollten AWS Lambda-Funktionen einer VPC zugewiesen werden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
11.10(g)	Personen, die geschlossene Systeme verwenden , um elektronische Aufzeichnungen zu erstellen, zu ändern, zu pflegen oder zu übertragen, müssen entsprech ende Verfahren und Kontrollen anwenden, um die Echtheit, Integritä t und gegebenen falls die Vertrauli chkeit elektronischer Aufzeichnungen sicherzustellen und dafür zu sorgen, dass die Unterzeic hneten die signierte Aufzeichnung nicht ohne Weiteres als unecht zurückwei sen können. Diese Verfahren und Kontrollen müssen Folgendes umfassen: (g) Durchführung von behördlichen Kontrollen, damit ausschließlich befugte Personen das System	mfa-enabled-for-iam-Konsolenzugriff	Verwalten Sie den Zugriff auf Ressource n in der AWS Cloud, indem Sie sicherste llen, dass MFA für alle AWS Identity and Access Managemen t (IAM) -Benutzer aktiviert ist, die über ein Konsolenk ennwort verfügen. MFA sorgt für eine weitere Schutzebe ne zusätzlich zu den Anmeldeinformation en. Indem Sie MFA für Benutzer vorschrei ben, können Sie Fälle kompromittierter Konten reduzieren und verhindern, dass unbefugte Benutzer auf vertrauliche Daten zugreifen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	nutzen, Aufzeichnungen elektronisch signieren, auf den Vorgang oder das Eingabe- oder Ausgabegerät des Computersystems zugreifen, Aufzeichnungen ändern oder den betreffenden Vorgang ausführen können.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
11.10(g)	Personen, die geschlossene Systeme verwenden , um elektronische Aufzeichnungen zu erstellen, zu ändern, zu pflegen oder zu übertragen, müssen entsprech ende Verfahren und Kontrollen anwenden, um die Echtheit, Integritä t und gegebenen falls die Vertrauli chkeit elektronischer Aufzeichnungen sicherzustellen und dafür zu sorgen, dass die Unterzeic hneten die signierte Aufzeichnung nicht ohne Weiteres als unecht zurückwei sen können. Diese Verfahren und Kontrollen müssen Folgendes umfassen: (g) Durchführung von behördlichen Kontrollen, damit ausschließlich befugte Personen das System	no-unrestricted-route-to-igw	Stellen Sie sicher, dass EC2 Amazon-Routentabellen keine uneingeschränkten Routen zu einem Internet-Gateway enthalten. Durch das Entfernen oder Beschränken des Internetzugangs für Workloads innerhalb von Amazon VPCs können unbeabsic htigte Zugriffe in Ihrer Umgebung reduziert werden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	nutzen, Aufzeichnungen elektronisch signieren, auf den Vorgang oder das Eingabe- oder Ausgabegerät des Computersystems zugreifen, Aufzeichnungen ändern oder den betreffenden Vorgang ausführen können.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
11.10(g)	Personen, die geschlossene Systeme verwenden , um elektronische Aufzeichnungen zu erstellen, zu ändern, zu pflegen oder zu übertragen, müssen entsprech ende Verfahren und Kontrollen anwenden, um die Echtheit, Integritä t und gegebenen falls die Vertrauli chkeit elektronischer Aufzeichnungen sicherzustellen und dafür zu sorgen, dass die Unterzeic hneten die signierte Aufzeichnung nicht ohne Weiteres als unecht zurückwei sen können. Diese Verfahren und Kontrollen müssen Folgendes umfassen: (g) Durchführung von behördlichen Kontrollen, damit ausschließlich befugte Personen das System	rds-instance-public-access-überprüfen	Verwalten Sie den Zugriff auf Ressource n in der AWS Cloud, indem Sie sicherste llen, dass Amazon Relational Database Service (Amazon RDS) -Instance s nicht öffentlic h sind. Amazon-RDS-Datenbank-Instances können vertrauliche Informati onen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	nutzen, Aufzeichnungen elektronisch signieren, auf den Vorgang oder das Eingabe- oder Ausgabegerät des Computersystems zugreifen, Aufzeichnungen ändern oder den betreffenden Vorgang ausführen können.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
11.10(g)	Personen, die geschlossene Systeme verwenden , um elektronische Aufzeichnungen zu erstellen, zu ändern, zu pflegen oder zu übertragen, müssen entsprech ende Verfahren und Kontrollen anwenden, um die Echtheit, Integritä t und gegebenen falls die Vertrauli chkeit elektronischer Aufzeichnungen sicherzustellen und dafür zu sorgen, dass die Unterzeic hneten die signierte Aufzeichnung nicht ohne Weiteres als unecht zurückwei sen können. Diese Verfahren und Kontrollen müssen Folgendes umfassen: (g) Durchführung von behördlichen Kontrollen, damit ausschließlich befugte Personen das System	rds-snapshots-public-prohibited	Verwalten Sie den Zugriff auf Ressource n in der AWS Cloud, indem Sie sicherste llen, dass Amazon Relational Database Service (Amazon RDS) -Instance s nicht öffentlic h sind. Amazon-RDS-Datenbank-Instances können vertrauliche Informati onen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	nutzen, Aufzeichnungen elektronisch signieren, auf den Vorgang oder das Eingabe- oder Ausgabegerät des Computersystems zugreifen, Aufzeichnungen ändern oder den betreffenden Vorgang ausführen können.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
11.10(g)	Personen, die geschlossene Systeme verwenden , um elektronische Aufzeichnungen zu erstellen, zu ändern, zu pflegen oder zu übertragen, müssen entsprech ende Verfahren und Kontrollen anwenden, um die Echtheit, Integritä t und gegebenen falls die Vertrauli chkeit elektronischer Aufzeichnungen sicherzustellen und dafür zu sorgen, dass die Unterzeic hneten die signierte Aufzeichnung nicht ohne Weiteres als unecht zurückwei sen können. Diese Verfahren und Kontrollen müssen Folgendes umfassen: (g) Durchführung von behördlichen Kontrollen, damit ausschließlich befugte Personen das System	redshift-cluster-kms-enabled	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass die Verschlüs selung mit AWS Key Management Service (AWS KMS) für Ihren Amazon Redshift Redshift-Cluster aktiviert ist. Um eventuell vorhanden e sensible Daten im Ruhezustand in Redshift-Clustern zu schützen, muss die Verschlüsselung von Daten im Ruhezusta nd aktiviert sein.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	nutzen, Aufzeichnungen elektronisch signieren, auf den Vorgang oder das Eingabe- oder Ausgabegerät des Computersystems zugreifen, Aufzeichnungen ändern oder den betreffenden Vorgang ausführen können.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
11.10(g)	Personen, die geschlossene Systeme verwenden , um elektronische Aufzeichnungen zu erstellen, zu ändern, zu pflegen oder zu übertragen, müssen entsprech ende Verfahren und Kontrollen anwenden, um die Echtheit, Integritä t und gegebenen falls die Vertrauli chkeit elektronischer Aufzeichnungen sicherzustellen und dafür zu sorgen, dass die Unterzeic hneten die signierte Aufzeichnung nicht ohne Weiteres als unecht zurückwei sen können. Diese Verfahren und Kontrollen müssen Folgendes umfassen: (g) Durchführung von behördlichen Kontrollen, damit ausschließlich befugte Personen das System	redshift-cluster-public-access-überprüfen	Verwalten Sie den Zugriff auf Ressource n in der AWS Cloud, indem Sie sicherste llen, dass Amazon Redshift Redshift-Cluster nicht öffentlic h sind. Amazon-Re dshift-Cluster können vertrauliche Informati onen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	nutzen, Aufzeichnungen elektronisch signieren, auf den Vorgang oder das Eingabe- oder Ausgabegerät des Computersystems zugreifen, Aufzeichnungen ändern oder den betreffenden Vorgang ausführen können.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
11.10(g)	Personen, die geschlossene Systeme verwenden , um elektronische Aufzeichnungen zu erstellen, zu ändern, zu pflegen oder zu übertragen, müssen entsprech ende Verfahren und Kontrollen anwenden, um die Echtheit, Integritä t und gegebenen falls die Vertrauli chkeit elektronischer Aufzeichnungen sicherzustellen und dafür zu sorgen, dass die Unterzeic hneten die signierte Aufzeichnung nicht ohne Weiteres als unecht zurückwei sen können. Diese Verfahren und Kontrollen müssen Folgendes umfassen: (g) Durchführung von behördlichen Kontrollen, damit ausschließlich befugte Personen das System	redshift-enhanced-vpc-routing-aktiviert	Mit Enhanced-VPC-Routing wird erzwungen, dass der gesamte COPY- und UNLOAD-Da tenverkehr zwischen Ihrem Cluster und Datenrepositorys über Ihre Amazon VPC erfolgt. Anschließ end können Sie VPC-Features wie Sicherheitsgruppen und Netzwerkz ugriffskontrolllisten verwenden, um den Netzwerkverkehr zu schützen. Sie können auch VPC-Flow-Protokolle verwenden , um den Netzwerkv erkehr zu überwache n.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	nutzen, Aufzeichnungen elektronisch signieren, auf den Vorgang oder das Eingabe- oder Ausgabegerät des Computersystems zugreifen, Aufzeichnungen ändern oder den betreffenden Vorgang ausführen können.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
11.10(g)	Personen, die geschlossene Systeme verwenden , um elektronische Aufzeichnungen zu erstellen, zu ändern, zu pflegen oder zu übertragen, müssen entsprech ende Verfahren und Kontrollen anwenden, um die Echtheit, Integritä t und gegebenen falls die Vertrauli chkeit elektronischer Aufzeichnungen sicherzustellen und dafür zu sorgen, dass die Unterzeic hneten die signierte Aufzeichnung nicht ohne Weiteres als unecht zurückwei sen können. Diese Verfahren und Kontrollen müssen Folgendes umfassen: (g) Durchführung von behördlichen Kontrollen, damit ausschließlich befugte Personen das System	restricted-common-ports	Verwalten Sie den Zugriff auf Ressource n in der AWS Cloud, indem Sie sicherste llen, dass gemeinsam e Ports für Amazon Elastic Compute Cloud (Amazon EC2) -Sicherhe itsgruppen eingeschr ränkt sind. Wenn der Zugriff auf Ports nicht auf vertrauen swürdige Quellen beschränkt wird, kann dies zu Angriffen auf die Verfügbar keit, Integrität und Vertraulichkeit von Systemen führen. Mit dieser Regel können Sie optional die Parameter blockedPo rt1–blockedPort5 festlegen (Standard konfigurationen: 20, 21, 3389, 3306, 4333). Die tatsächli chen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	nutzen, Aufzeichnungen elektronisch signieren, auf den Vorgang oder das Eingabe- oder Ausgabegerät des Computersystems zugreifen, Aufzeichnungen ändern oder den betreffenden Vorgang ausführen können.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
11.10(g)	Personen, die geschlossene Systeme verwenden, um elektronische Aufzeichnungen zu erstellen, zu ändern, zu pflegen oder zu übertragen, müssen entsprechende Verfahren und Kontrollen anwenden, um die Echtheit, Integrität und gegebenenfalls die Vertraulichkeit elektronischer Aufzeichnungen sicherzustellen und dafür zu sorgen, dass die Unterzeichneten die signierte Aufzeichnung nicht ohne Weiteres als unecht zurückweisen können. Diese Verfahren und Kontrollen müssen Folgendes umfassen: (g) Durchführung von behördlichen Kontrollen, damit ausschließlich befugte Personen das System	root-account-hardware-mfa-aktiviert	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Hardware-MFA für den Root-Benutzer aktiviert ist. Der Stammbenutzer ist der AWS-Konto-Benutzer mit den meisten Berechtigungen. MFA sorgt für eine weitere Schutzebene zusätzlich zu den Anmeldeinformationen. Indem Sie MFA für den Root-Benutzer vorschreiben, können Sie die Anzahl AWS-Konten kompromittierter Benutzer reduzieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	nutzen, Aufzeichnungen elektronisch signieren, auf den Vorgang oder das Eingabe- oder Ausgabegerät des Computersystems zugreifen, Aufzeichnungen ändern oder den betreffenden Vorgang ausführen können.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
11.10(g)	Personen, die geschlossene Systeme verwenden, um elektronische Aufzeichnungen zu erstellen, zu ändern, zu pflegen oder zu übertragen, müssen entsprechende Verfahren und Kontrollen anwenden, um die Echtheit, Integrität und gegebenenfalls die Vertraulichkeit elektronischer Aufzeichnungen sicherzustellen und dafür zu sorgen, dass die Unterzeichneten die signierte Aufzeichnung nicht ohne Weiteres als unecht zurückweisen können. Diese Verfahren und Kontrollen müssen Folgendes umfassen: (g) Durchführung von behördlichen Kontrollen, damit ausschließlich befugte Personen das System	root-account-mfa-enabled	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass MFA für den Root-Benutzer aktiviert ist. Der Stammbenutzer ist der AWS-Konto-Benutzer mit den meisten Berechtigungen. MFA sorgt für eine weitere Schutzebene zusätzlich zu den Anmeldeinformationen. Indem Sie MFA für den Root-Benutzer vorschreiben, können Sie die Anzahl AWS-Konten kompromittierter Benutzer reduzieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	nutzen, Aufzeichnungen elektronisch signieren, auf den Vorgang oder das Eingabe- oder Ausgabegerät des Computersystems zugreifen, Aufzeichnungen ändern oder den betreffenden Vorgang ausführen können.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
11.10(g)	Personen, die geschlossene Systeme verwenden , um elektronische Aufzeichnungen zu erstellen, zu ändern, zu pflegen oder zu übertragen, müssen entsprech ende Verfahren und Kontrollen anwenden, um die Echtheit, Integritä t und gegebenen falls die Vertrauli chkeit elektronischer Aufzeichnungen sicherzustellen und dafür zu sorgen, dass die Unterzeic hneten die signierte Aufzeichnung nicht ohne Weiteres als unecht zurückwei sen können. Diese Verfahren und Kontrollen müssen Folgendes umfassen: (g) Durchführung von behördlichen Kontrollen, damit ausschließlich befugte Personen das System	s3- -blöcke-periodisch account-level-public-access	Verwalten Sie den Zugriff auf Ressource n in der AWS Cloud, indem Sie sicherste llen, dass Amazon Simple Storage Service (Amazon S3) -Buckets nicht öffentlich zugänglic h sind. Diese Regel trägt dazu bei, sensible Daten vor unbefugten Remote-Benutzern zu schützen, indem sie den öffentlichen Zugriff verhinder t. Mit dieser Regel können Sie optional die Parameter ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) und restrictPublicBuck ets Parameter (Config Default: True) festlegen. Die tatsächlichen Werte müssen den Richtlini

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	nutzen, Aufzeichnungen elektronisch signieren, auf den Vorgang oder das Eingabe- oder Ausgabegerät des Computersystems zugreifen, Aufzeichnungen ändern oder den betreffenden Vorgang ausführen können.		en Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
11.10(g)	Personen, die geschlossene Systeme verwenden , um elektronische Aufzeichnungen zu erstellen, zu ändern, zu pflegen oder zu übertragen, müssen entsprech ende Verfahren und Kontrollen anwenden, um die Echtheit, Integritä t und gegebenen falls die Vertrauli chkeit elektronischer Aufzeichnungen sicherzustellen und dafür zu sorgen, dass die Unterzeic hneten die signierte Aufzeichnung nicht ohne Weiteres als unecht zurückwei sen können. Diese Verfahren und Kontrollen müssen Folgendes umfassen: (g) Durchführung von behördlichen Kontrollen, damit ausschließlich befugte Personen das System	s3 bucket-level-public-access - verboten	Verwalten Sie den Zugriff auf Ressource n in der AWS Cloud, indem Sie sicherste llen, dass Amazon Simple Storage Service (Amazon S3) -Buckets nicht öffentlich zugänglic h sind. Diese Regel trägt dazu bei, sensible Daten vor unbefugten Remote-Benutzern zu schützen, indem sie den öffentlichen Zugriff auf Bucket-Eb ene verhindert.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	nutzen, Aufzeichnungen elektronisch signieren, auf den Vorgang oder das Eingabe- oder Ausgabegerät des Computersystems zugreifen, Aufzeichnungen ändern oder den betreffenden Vorgang ausführen können.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
11.10(g)	Personen, die geschlossene Systeme verwenden , um elektronische Aufzeichnungen zu erstellen, zu ändern, zu pflegen oder zu übertragen, müssen entsprech ende Verfahren und Kontrollen anwenden, um die Echtheit, Integritä t und gegebenen falls die Vertrauli chkeit elektronischer Aufzeichnungen sicherzustellen und dafür zu sorgen, dass die Unterzeic hneten die signierte Aufzeichnung nicht ohne Weiteres als unecht zurückwei sen können. Diese Verfahren und Kontrollen müssen Folgendes umfassen: (g) Durchführung von behördlichen Kontrollen, damit ausschließlich befugte Personen das System	s-3 bucket-public-read -prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie nur autorisierten Benutzern, Prozessen und Geräten Zugriff auf Amazon Simple Storage Service (Amazon S3) - Buckets gewähren. Die Verwaltung des Zugriffs sollte mit der Klassifizierung der Daten übereinst immen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	nutzen, Aufzeichnungen elektronisch signieren, auf den Vorgang oder das Eingabe- oder Ausgabegerät des Computersystems zugreifen, Aufzeichnungen ändern oder den betreffenden Vorgang ausführen können.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
11.10(g)	Personen, die geschlossene Systeme verwenden , um elektronische Aufzeichnungen zu erstellen, zu ändern, zu pflegen oder zu übertragen, müssen entsprech ende Verfahren und Kontrollen anwenden, um die Echtheit, Integritä t und gegebenen falls die Vertrauli chkeit elektronischer Aufzeichnungen sicherzustellen und dafür zu sorgen, dass die Unterzeic hneten die signierte Aufzeichnung nicht ohne Weiteres als unecht zurückwei sen können. Diese Verfahren und Kontrollen müssen Folgendes umfassen: (g) Durchführung von behördlichen Kontrollen, damit ausschließlich befugte Personen das System	s3- bucket-public-writ e-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie nur autorisierten Benutzern, Prozessen und Geräten Zugriff auf Amazon Simple Storage Service (Amazon S3) - Buckets gewähren. Die Verwaltung des Zugriffs sollte mit der Klassifizierung der Daten übereinst immen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	nutzen, Aufzeichnungen elektronisch signieren, auf den Vorgang oder das Eingabe- oder Ausgabegerät des Computersystems zugreifen, Aufzeichnungen ändern oder den betreffenden Vorgang ausführen können.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
11.10(g)	Personen, die geschlossene Systeme verwenden, um elektronische Aufzeichnungen zu erstellen, zu ändern, zu pflegen oder zu übertragen, müssen entsprechende Verfahren und Kontrollen anwenden, um die Echtheit, Integrität und gegebenenfalls die Vertraulichkeit elektronischer Aufzeichnungen sicherzustellen und dafür zu sorgen, dass die Unterzeichneten die signierte Aufzeichnung nicht ohne Weiteres als unecht zurückweisen können. Diese Verfahren und Kontrollen müssen Folgendes umfassen: (g) Durchführung von behördlichen Kontrollen, damit ausschließlich befugte Personen das System	sagemaker-notebook-no-direct-Internetzugang	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass SageMaker Amazon-Notebooks keinen direkten Internetzugang zulassen. Indem Sie direkten Internetzugang blockieren, vermeiden Sie, dass unbefugte Benutzer auf sensible Daten zugreifen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	nutzen, Aufzeichnungen elektronisch signieren, auf den Vorgang oder das Eingabe- oder Ausgabegerät des Computersystems zugreifen, Aufzeichnungen ändern oder den betreffenden Vorgang ausführen können.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
11.10(g)	Personen, die geschlossene Systeme verwenden , um elektronische Aufzeichnungen zu erstellen, zu ändern, zu pflegen oder zu übertragen, müssen entsprech ende Verfahren und Kontrollen anwenden, um die Echtheit, Integritä t und gegebenen falls die Vertrauli chkeit elektronischer Aufzeichnungen sicherzustellen und dafür zu sorgen, dass die Unterzeic hneten die signierte Aufzeichnung nicht ohne Weiteres als unecht zurückwei sen können. Diese Verfahren und Kontrollen müssen Folgendes umfassen: (g) Durchführung von behördlichen Kontrollen, damit ausschließlich befugte Personen das System	secretsmanager-rot ation-enabled-check	Diese Regel stellt sicher, dass bei AWS Secrets Manager Manager-Geheimnissen die Rotation aktiviert ist. Die regelmäßige Rotation von Secrets kann den Zeitraum verkürzen, in dem ein Secret aktiv ist, und möglicherweise die Auswirkungen auf das Unternehmen verringern, falls das Secret kompromittiert wird.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	nutzen, Aufzeichnungen elektronisch signieren, auf den Vorgang oder das Eingabe- oder Ausgabegerät des Computersystems zugreifen, Aufzeichnungen ändern oder den betreffenden Vorgang ausführen können.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
11.10(g)	Personen, die geschlossene Systeme verwenden , um elektronische Aufzeichnungen zu erstellen, zu ändern, zu pflegen oder zu übertragen, müssen entsprech ende Verfahren und Kontrollen anwenden, um die Echtheit, Integritä t und gegebenen falls die Vertrauli chkeit elektronischer Aufzeichnungen sicherzustellen und dafür zu sorgen, dass die Unterzeic hneten die signierte Aufzeichnung nicht ohne Weiteres als unecht zurückwei sen können. Diese Verfahren und Kontrollen müssen Folgendes umfassen: (g) Durchführung von behördlichen Kontrollen, damit ausschließlich befugte Personen das System	secretsmanager-sch eduled-rotation-su ccess-überprüfen	Diese Regel stellt sicher, dass AWS Secrets Manager Manager-Geheimnisse gemäß dem Rotations plan erfolgreich rotiert wurden. Die regelmäßige Rotation von Secrets kann den Zeitraum verkürzen, in dem ein Secret aktiv ist, und möglicherweise die Auswirkungen auf das Unternehm en verringern, falls es kompromittiert wird.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	nutzen, Aufzeichnungen elektronisch signieren, auf den Vorgang oder das Eingabe- oder Ausgabegerät des Computersystems zugreifen, Aufzeichnungen ändern oder den betreffenden Vorgang ausführen können.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
11.10(g)	Personen, die geschlossene Systeme verwenden , um elektronische Aufzeichnungen zu erstellen, zu ändern, zu pflegen oder zu übertragen, müssen entsprech ende Verfahren und Kontrollen anwenden, um die Echtheit, Integritä t und gegebenen falls die Vertrauli chkeit elektronischer Aufzeichnungen sicherzustellen und dafür zu sorgen, dass die Unterzeic hneten die signierte Aufzeichnung nicht ohne Weiteres als unecht zurückwei sen können. Diese Verfahren und Kontrollen müssen Folgendes umfassen: (g) Durchführung von behördlichen Kontrollen, damit ausschließlich befugte Personen das System	ssm-document-not-p ublic	Stellen Sie sicher, dass AWS Systems Manager (SSM) - Dokumente nicht öffentlich sind, da dies einen unbeabsic htigten Zugriff auf Ihre SSM-Dokum ente ermöglichen kann. Ein öffentlic hes SSM-Dokum ent kann Informati onen über Ihr Konto, Ihre Ressourcen und internen Prozesse preisgeben.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	nutzen, Aufzeichnungen elektronisch signieren, auf den Vorgang oder das Eingabe- oder Ausgabegerät des Computersystems zugreifen, Aufzeichnungen ändern oder den betreffenden Vorgang ausführen können.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
11.10(g)	Personen, die geschlossene Systeme verwenden , um elektronische Aufzeichnungen zu erstellen, zu ändern, zu pflegen oder zu übertragen, müssen entsprech ende Verfahren und Kontrollen anwenden, um die Echtheit, Integritä t und gegebenen falls die Vertrauli chkeit elektronischer Aufzeichnungen sicherzustellen und dafür zu sorgen, dass die Unterzeic hneten die signierte Aufzeichnung nicht ohne Weiteres als unecht zurückwei sen können. Diese Verfahren und Kontrollen müssen Folgendes umfassen: (g) Durchführung von behördlichen Kontrollen, damit ausschließlich befugte Personen das System	subnet-auto-assign-public-ip-deaktiviert	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon Virtual Private Cloud (VPC) -Subnetzen nicht automatisch eine öffentliche IP-Adress e zugewiesen wird. Amazon Elastic Compute Cloud (EC2) -Instances, die in Subnetzen gestartet werden, in denen dieses Attribut aktiviert ist, haben ihrer primären Netzwerkschnittste lle eine öffentliche IP-Adresse zugewiesen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	nutzen, Aufzeichnungen elektronisch signieren, auf den Vorgang oder das Eingabe- oder Ausgabegerät des Computersystems zugreifen, Aufzeichnungen ändern oder den betreffenden Vorgang ausführen können.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
11.10(g)	Personen, die geschlossene Systeme verwenden , um elektronische Aufzeichnungen zu erstellen, zu ändern, zu pflegen oder zu übertragen, müssen entsprech ende Verfahren und Kontrollen anwenden, um die Echtheit, Integritä t und gegebenen falls die Vertrauli chkeit elektronischer Aufzeichnungen sicherzustellen und dafür zu sorgen, dass die Unterzeic hneten die signierte Aufzeichnung nicht ohne Weiteres als unecht zurückwei sen können. Diese Verfahren und Kontrollen müssen Folgendes umfassen: (g) Durchführung von behördlichen Kontrollen, damit ausschließlich befugte Personen das System	vpc-default-security-group-geschlossen	Sicherheitsgruppen von Amazon Elastic Compute Cloud (Amazon EC2) können bei der Verwaltung des Netzwerkzugriffs helfen, indem sie eine statusbehaftete Filterung des ein- und ausgehenden Netzwerkverkehrs zu Ressourcen bereitstellen. AWS Die Beschränk ung des gesamten Datenverkehrs auf die Standardsicherheit sgruppe hilft dabei, den Fernzugriff auf Ihre Ressourcen einzuschränken. AWS

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	nutzen, Aufzeichnungen elektronisch signieren, auf den Vorgang oder das Eingabe- oder Ausgabegerät des Computersystems zugreifen, Aufzeichnungen ändern oder den betreffenden Vorgang ausführen können.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
11.10(g)	Personen, die geschlossene Systeme verwenden , um elektronische Aufzeichnungen zu erstellen, zu ändern, zu pflegen oder zu übertragen, müssen entsprech ende Verfahren und Kontrollen anwenden, um die Echtheit, Integritä t und gegebenen falls die Vertrauli chkeit elektronischer Aufzeichnungen sicherzustellen und dafür zu sorgen, dass die Unterzeic hneten die signierte Aufzeichnung nicht ohne Weiteres als unecht zurückwei sen können. Diese Verfahren und Kontrollen müssen Folgendes umfassen: (g) Durchführung von behördlichen Kontrollen, damit ausschließlich befugte Personen das System	vpc-sg-open-only-to-authorized-ports	Verwalten Sie den Zugriff auf Ressource n in der AWS Cloud, indem Sie sicherste llen, dass gemeinsam e Ports für Amazon Elastic Compute Cloud (Amazon EC2) -Sicherhe itsgruppen eingeschr ränkt sind. Wenn der Zugriff auf Ports nicht auf vertrauen swürdige Quellen beschränkt wird, kann dies zu Angriffen auf die Verfügbar keit, Integrität und Vertraulichkeit von Systemen führen. Durch die Beschränk ung des Zugriffs auf Ressourcen innerhalb einer Sicherhei tsgruppe aus dem Internet (0.0.0.0/0) kann der Remote-Zugriff auf interne Systeme gesteuert werden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	nutzen, Aufzeichnungen elektronisch signieren, auf den Vorgang oder das Eingabe- oder Ausgabegerät des Computersystems zugreifen, Aufzeichnungen ändern oder den betreffenden Vorgang ausführen können.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
11.10(h)	Personen, die geschlossene Systeme verwenden, um elektronische Aufzeichnungen zu erstellen, zu ändern, zu pflegen oder zu übertragen, müssen entsprechende Verfahren und Kontrollen anwenden, um die Echtheit, Integrität und gegebenenfalls die Vertraulichkeit elektronischer Aufzeichnungen sicherzustellen und dafür zu sorgen, dass die Unterzeichneten die signierte Aufzeichnung nicht ohne Weiteres als unecht zurückweisen können. Diese Verfahren und Kontrollen müssen Folgendes umfassen: (h) Verwendung von Geräteprüfungen (z. B. Endgeräten), um gegebenenfalls die Gültigkeit der Quelle	ec2-manager instance-managed-by-systems	Eine Bestandsaufnahme der Softwareplattformen und Anwendungen innerhalb des Unternehmens ist möglich, indem Amazon Elastic Compute Cloud (Amazon EC2) - Instances mit AWS Systems Manager verwaltet werden. Verwenden Sie AWS Systems Manager, um detaillierte Systemkonfigurationen, Betriebssystem-Patch-Levels, Namen und Typ der Dienste, Softwareinstallationen, Anwendungsname, Herausgeber und Version sowie andere Details zu Ihrer Umgebung bereitzustellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	der Dateneingabe oder der Betriebsanweisung festzustellen.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
11.10(h)	Personen, die geschlossene Systeme verwenden, um elektronische Aufzeichnungen zu erstellen, zu ändern, zu pflegen oder zu übertragen, müssen entsprechende Verfahren und Kontrollen anwenden, um die Echtheit, Integrität und gegebenenfalls die Vertraulichkeit elektronischer Aufzeichnungen sicherzustellen und dafür zu sorgen, dass die Unterzeichneten die signierte Aufzeichnung nicht ohne Weiteres als unecht zurückweisen können. Diese Verfahren und Kontrollen müssen Folgendes umfassen: (h) Verwendung von Geräteprüfungen (z. B. Endgeräten), um gegebenenfalls die Gültigkeit der Quelle	ec2-Check managedinstance-association-compliance-status	Verwenden Sie AWS Systems Manager Associations, um bei der Inventarisierung von Softwareplattformen und Anwendungen innerhalb eines Unternehmens zu helfen. AWS Systems Manager weist Ihren verwalteten Instanzen einen Konfigurationsstatus zu und ermöglicht es Ihnen, Basiswerte für Betriebssystem-Patch-Levels, Softwareinstallationen, Anwendungskonfigurationen und andere Details zu Ihrer Umgebung festzulegen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	der Dateneingabe oder der Betriebsanweisung festzustellen.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
11.10(h)	Personen, die geschlossene Systeme verwenden , um elektronische Aufzeichnungen zu erstellen, zu ändern, zu pflegen oder zu übertragen, müssen entsprech ende Verfahren und Kontrollen anwenden, um die Echtheit, Integritä t und gegebenen falls die Vertrauli chkeit elektronischer Aufzeichnungen sicherzustellen und dafür zu sorgen, dass die Unterzeic hneten die signierte Aufzeichnung nicht ohne Weiteres als unecht zurückwei sen können. Diese Verfahren und Kontrollen müssen Folgendes umfassen: (h) Verwendung von Geräteprüfungen (z. B. Endgeräten), um gegebenenfalls die Gültigkeit der Quelle	ec2-Check managedinstance-pa tch-compliance-status	Aktivieren Sie diese Regel, um bei der Identifizierung und Dokumentation von Sicherheitslücken in Amazon Elastic Compute Cloud (Amazon EC2) zu helfen. Die Regel prüft, ob die EC2 Amazon-Instance die Patch-Konformität im AWS Systems Manager gemäß den Richtlinien und Verfahren Ihrer Organisation einhält.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	der Dateneingabe oder der Betriebsanweisung festzustellen.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
11.10(i)	Personen, die geschlossene Systeme verwenden , um elektronische Aufzeichnungen zu erstellen, zu ändern, zu pflegen oder zu übertragen, müssen entsprech ende Verfahren und Kontrollen anwenden, um die Echtheit, Integritä t und gegebenen falls die Vertrauli chkeit elektronischer Aufzeichnungen sicherzustellen und dafür zu sorgen, dass die Unterzeic hneten die signierte Aufzeichnung nicht ohne Weiteres als unecht zurückwei sen können. Diese Verfahren und Kontrollen müssen Folgendes umfassen: i) Gewährleistung, dass Personen, die elektronische Aufzeichnungs- und Signatursysteme	security-awareness -program-exists (Prozessüberprüfung)	Etablieren und pflegen Sie ein Programm zur Förderung des Sicherheitsbewusst seins in Ihrer Organisation. Programme zur Förderung des Sicherheitsbewusst seins der Mitarbeiter vermitteln ihnen, wie sie ihre Organisation vor diversen Sicherhei tsverletzungen oder Sicherheitsvorfällen schützen können.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	entwickeln, pflegen oder verwenden, über die erforderliche Ausbildung, Schulung und Erfahrung verfügen, um die ihnen übertragenen Aufgaben zu erfüllen.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
11.10(k)	Personen, die geschlossene Systeme verwenden , um elektronische Aufzeichnungen zu erstellen, zu ändern, zu pflegen oder zu übertragen, müssen entsprech ende Verfahren und Kontrollen anwenden, um die Echtheit, Integritä t und gegebenen falls die Vertrauli chkeit elektronischer Aufzeichnungen sicherzustellen und dafür zu sorgen, dass die Unterzeic hneten die signierte Aufzeichnung nicht ohne Weiteres als unecht zurückwei sen können. Diese Verfahren und Kontrollen müssen Folgendes umfassen: (k) Anwendung geeigneter Kontrolle n der Systemdok umentation, darunter: (1) Angemesse	autoscaling-launch -config-public-ip- deaktiviert	Wenn Sie Ihre Netzwerkschnittstellen mit einer öffentlichen IP-Adresse konfiguri eren, sind die diesen Netzwerkschnittste llen zugehörigen Ressourcen über das Internet erreichba r. EC2 Ressourcen sollten nicht öffentlic h zugänglich sein, da dies einen unbeabsic htigten Zugriff auf Ihre Anwendungen oder Server ermöglichen kann.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	ne Kontrollen des Zugriffs auf und der Verteilung und Verwendun g von Unterlage n für den Betrieb und die Wartung des Systems; (2) Verfahren zur Überprüfung und Kontrolle von Änderungen, um ein Audit Trail anzulegen , in dem die Erstellun g und Änderung der Systemdokumentatio n in chronolog ischer Reihenfolge dokumentiert wird.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
11.10(k)	Personen, die geschlossene Systeme verwenden , um elektronische Aufzeichnungen zu erstellen, zu ändern, zu pflegen oder zu übertragen, müssen entsprech ende Verfahren und Kontrollen anwenden, um die Echtheit, Integritä t und gegebenen falls die Vertrauli chkeit elektronischer Aufzeichnungen sicherzustellen und dafür zu sorgen, dass die Unterzeic hneten die signierte Aufzeichnung nicht ohne Weiteres als unecht zurückwei sen können. Diese Verfahren und Kontrollen müssen Folgendes umfassen: (k) Anwendung geeigneter Kontrolle n der Systemdok umentation, darunter: (1) Angemesse	cloud-trail-cloud-watch-logs-aktiviert	Verwenden Sie Amazon CloudWatc h , um Protokoll ereignisaktivitäten zentral zu sammeln und zu verwalten. Die Aufnahme von AWS CloudTrail Daten liefert Einzelheiten zu den API-Aufrufaktivitä ten in Ihrem AWS-Konto.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	ne Kontrollen des Zugriffs auf und der Verteilung und Verwendun g von Unterlage n für den Betrieb und die Wartung des Systems; (2) Verfahren zur Überprüfung und Kontrolle von Änderungen, um ein Audit Trail anzulegen , in dem die Erstellun g und Änderung der Systemdokumentatio n in chronolog ischer Reihenfolge dokumentiert wird.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
11.10(k)	Personen, die geschlossene Systeme verwenden , um elektronische Aufzeichnungen zu erstellen, zu ändern, zu pflegen oder zu übertragen, müssen entsprech ende Verfahren und Kontrollen anwenden, um die Echtheit, Integritä t und gegebenen falls die Vertrauli chkeit elektronischer Aufzeichnungen sicherzustellen und dafür zu sorgen, dass die Unterzeic hneten die signierte Aufzeichnung nicht ohne Weiteres als unecht zurückwei sen können. Diese Verfahren und Kontrollen müssen Folgendes umfassen: (k) Anwendung geeigneter Kontrolle n der Systemdok umentation, darunter: (1) Angemesse	cloudtrail-enabled	AWS CloudTrail kann bei der Nichtabst reitbarkeit helfen, indem Aktionen und API-Aufrufe der AWS Management Console aufgezeic hnet werden. Sie können die Benutzer und die Benutzer AWS-Konten , die einen AWS Dienst aufgerufen haben, die Quell-IP-Adresse, über die die Aufrufe generiert wurden, und den Zeitpunkt der Anrufe identifiz ieren. Einzelheiten zu den erfassten Daten finden Sie unter Inhalt des AWS CloudTrail Datensatzes.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	ne Kontrollen des Zugriffs auf und der Verteilung und Verwendun g von Unterlage n für den Betrieb und die Wartung des Systems; (2) Verfahren zur Überprüfung und Kontrolle von Änderungen, um ein Audit Trail anzulegen , in dem die Erstellun g und Änderung der Systemdokumentatio n in chronolog ischer Reihenfolge dokumentiert wird.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
11.10(k)	Personen, die geschlossene Systeme verwenden , um elektronische Aufzeichnungen zu erstellen, zu ändern, zu pflegen oder zu übertragen, müssen entsprech ende Verfahren und Kontrollen anwenden, um die Echtheit, Integritä t und gegebenen falls die Vertrauli chkeit elektronischer Aufzeichnungen sicherzustellen und dafür zu sorgen, dass die Unterzeic hneten die signierte Aufzeichnung nicht ohne Weiteres als unecht zurückwei sen können. Diese Verfahren und Kontrollen müssen Folgendes umfassen: (k) Anwendung geeigneter Kontrolle n der Systemdok umentation, darunter: (1) Angemesse	cloudtrail-s3-data events-enabled	Die Erfassung von Simple Storage Service (Amazon S3)-Datenereigniss en unterstützt die Erkennung von ungewöhnlichen Aktivitäten. Zu den Details gehören AWS-Konto Informationen über den Zugriff auf einen Amazon S3 S3-Bucket, die IP-Adress e und die Uhrzeit des Ereignisses.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	ne Kontrollen des Zugriffs auf und der Verteilung und Verwendun g von Unterlage n für den Betrieb und die Wartung des Systems; (2) Verfahren zur Überprüfung und Kontrolle von Änderungen, um ein Audit Trail anzulegen , in dem die Erstellun g und Änderung der Systemdokumentatio n in chronolog ischer Reihenfolge dokumentiert wird.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
11.10(k)	Personen, die geschlossene Systeme verwenden , um elektronische Aufzeichnungen zu erstellen, zu ändern, zu pflegen oder zu übertragen, müssen entsprech ende Verfahren und Kontrollen anwenden, um die Echtheit, Integritä t und gegebenen falls die Vertrauli chkeit elektronischer Aufzeichnungen sicherzustellen und dafür zu sorgen, dass die Unterzeic hneten die signierte Aufzeichnung nicht ohne Weiteres als unecht zurückwei sen können. Diese Verfahren und Kontrollen müssen Folgendes umfassen: (k) Anwendung geeigneter Kontrolle n der Systemdok umentation, darunter: (1) Angemesse	dms-replication-not-public	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass auf DMS-Replikationsin stanzen nicht öffentlic h zugegriffen werden kann. DMS-Repli kations-Instances können vertrauli che Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	ne Kontrollen des Zugriffs auf und der Verteilung und Verwendun g von Unterlage n für den Betrieb und die Wartung des Systems; (2) Verfahren zur Überprüfung und Kontrolle von Änderungen, um ein Audit Trail anzulegen , in dem die Erstellun g und Änderung der Systemdokumentatio n in chronolog ischer Reihenfolge dokumentiert wird.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
11.10(k)	Personen, die geschlossene Systeme verwenden , um elektronische Aufzeichnungen zu erstellen, zu ändern, zu pflegen oder zu übertragen, müssen entsprech ende Verfahren und Kontrollen anwenden, um die Echtheit, Integritä t und gegebenen falls die Vertrauli chkeit elektronischer Aufzeichnungen sicherzustellen und dafür zu sorgen, dass die Unterzeic hneten die signierte Aufzeichnung nicht ohne Weiteres als unecht zurückwei sen können. Diese Verfahren und Kontrollen müssen Folgendes umfassen: (k) Anwendung geeigneter Kontrolle n der Systemdok umentation, darunter: (1) Angemesse	ebs-snapshot-public-restorable-überprüfen	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass EBS-Snapshots nicht öffentlich wiederher stellbar sind. EBS-Volume-Snapsho ts können vertrauli che Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	ne Kontrollen des Zugriffs auf und der Verteilung und Verwendun g von Unterlage n für den Betrieb und die Wartung des Systems; (2) Verfahren zur Überprüfung und Kontrolle von Änderungen, um ein Audit Trail anzulegen , in dem die Erstellun g und Änderung der Systemdokumentatio n in chronolog ischer Reihenfolge dokumentiert wird.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
11.10(k)	Personen, die geschlossene Systeme verwenden , um elektronische Aufzeichnungen zu erstellen, zu ändern, zu pflegen oder zu übertragen, müssen entsprech ende Verfahren und Kontrollen anwenden, um die Echtheit, Integritä t und gegebenen falls die Vertrauli chkeit elektronischer Aufzeichnungen sicherzustellen und dafür zu sorgen, dass die Unterzeic hneten die signierte Aufzeichnung nicht ohne Weiteres als unecht zurückwei sen können. Diese Verfahren und Kontrollen müssen Folgendes umfassen: (k) Anwendung geeigneter Kontrolle n der Systemdok umentation, darunter: (1) Angemesse	emr-master-no-public-ip	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon EMR-Clust er-Masterknoten nicht öffentlich zugänglic h sind. Amazon-EM R-Cluster-Hauptkno ten können vertrauli che Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	ne Kontrollen des Zugriffs auf und der Verteilung und Verwendun g von Unterlage n für den Betrieb und die Wartung des Systems; (2) Verfahren zur Überprüfung und Kontrolle von Änderungen, um ein Audit Trail anzulegen , in dem die Erstellun g und Änderung der Systemdokumentatio n in chronolog ischer Reihenfolge dokumentiert wird.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
11.10(k)	Personen, die geschlossene Systeme verwenden , um elektronische Aufzeichnungen zu erstellen, zu ändern, zu pflegen oder zu übertragen, müssen entsprech ende Verfahren und Kontrollen anwenden, um die Echtheit, Integritä t und gegebenen falls die Vertrauli chkeit elektronischer Aufzeichnungen sicherzustellen und dafür zu sorgen, dass die Unterzeic hneten die signierte Aufzeichnung nicht ohne Weiteres als unecht zurückwei sen können. Diese Verfahren und Kontrollen müssen Folgendes umfassen: (k) Anwendung geeigneter Kontrolle n der Systemdok umentation, darunter: (1) Angemesse	ec-2 instances-in-vpc	Stellen Sie Amazon Elastic Compute Cloud (Amazon EC2) -Instances innerhalb einer Amazon Virtual Private Cloud (Amazon VPC) bereit, um eine sichere Kommunika tion zwischen einer Instance und anderen Services innerhalb der Amazon VPC zu ermöglichen, ohne dass ein Internet-Gateway, ein NAT-Gerät oder eine VPN-Verbindung erforderlich ist. Der gesamte Datenverk ehr bleibt sicher in der AWS Cloud. Domains, die sich innerhalb einer VPC befinden, verfügen aufgrund ihrer logischen Isolierun g im Vergleich zu Domains mit öffentlic hen Endpunkten über eine zusätzlic he Sicherheitsebene. Weisen Sie EC2

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	ne Kontrollen des Zugriffs auf und der Verteilung und Verwendun g von Unterlage n für den Betrieb und die Wartung des Systems; (2) Verfahren zur Überprüfung und Kontrolle von Änderungen, um ein Audit Trail anzulegen , in dem die Erstellun g und Änderung der Systemdokumentatio n in chronolog ischer Reihenfolge dokumentiert wird.		Amazon-Instances einer Amazon-VPC zu, um den Zugriff ordnungsgemäß zu verwalten.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
11.10(k)	Personen, die geschlossene Systeme verwenden , um elektronische Aufzeichnungen zu erstellen, zu ändern, zu pflegen oder zu übertragen, müssen entsprech ende Verfahren und Kontrollen anwenden, um die Echtheit, Integritä t und gegebenen falls die Vertrauli chkeit elektronischer Aufzeichnungen sicherzustellen und dafür zu sorgen, dass die Unterzeic hneten die signierte Aufzeichnung nicht ohne Weiteres als unecht zurückwei sen können. Diese Verfahren und Kontrollen müssen Folgendes umfassen: (k) Anwendung geeigneter Kontrolle n der Systemdok umentation, darunter: (1) Angemesse	rds-instance-public-access-überprüfen	Verwalten Sie den Zugriff auf Ressource n in der AWS Cloud, indem Sie sicherste llen, dass Amazon Relational Database Service (Amazon RDS) -Instance s nicht öffentlic h sind. Amazon-RDS-Datenbank-Instances können vertrauliche Informati onen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	ne Kontrollen des Zugriffs auf und der Verteilung und Verwendun g von Unterlage n für den Betrieb und die Wartung des Systems; (2) Verfahren zur Überprüfung und Kontrolle von Änderungen, um ein Audit Trail anzulegen , in dem die Erstellun g und Änderung der Systemdokumentatio n in chronolog ischer Reihenfolge dokumentiert wird.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
11.10(k)	Personen, die geschlossene Systeme verwenden, um elektronische Aufzeichnungen zu erstellen, zu ändern, zu pflegen oder zu übertragen, müssen entsprechende Verfahren und Kontrollen anwenden, um die Echtheit, Integrität und gegebenenfalls die Vertraulichkeit elektronischer Aufzeichnungen sicherzustellen und dafür zu sorgen, dass die Unterzeichneten die signierte Aufzeichnung nicht ohne Weiteres als unecht zurückweisen können. Diese Verfahren und Kontrollen müssen Folgendes umfassen: (k) Anwendung geeigneter Kontrollen der Systemdokumentation, darunter: (1) Angemesse	rds-logging-enabled	Um die Protokollierung und Überwachung in Ihrer Umgebung zu erleichtern, stellen Sie sicher, dass die Amazon Relational Database Service (Amazon RDS)-Protokollierung aktiviert ist. Mit der Amazon-RDS-Protokollierung können Sie Ereignisse wie Verbindungen, Verbindungsabbrüche, Abfragen oder abgefragte Tabellen erfassen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	ne Kontrollen des Zugriffs auf und der Verteilung und Verwendun g von Unterlage n für den Betrieb und die Wartung des Systems; (2) Verfahren zur Überprüfung und Kontrolle von Änderungen, um ein Audit Trail anzulegen , in dem die Erstellun g und Änderung der Systemdokumentatio n in chronolog ischer Reihenfolge dokumentiert wird.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
11.10(k)	Personen, die geschlossene Systeme verwenden , um elektronische Aufzeichnungen zu erstellen, zu ändern, zu pflegen oder zu übertragen, müssen entsprech ende Verfahren und Kontrollen anwenden, um die Echtheit, Integritä t und gegebenen falls die Vertrauli chkeit elektronischer Aufzeichnungen sicherzustellen und dafür zu sorgen, dass die Unterzeic hneten die signierte Aufzeichnung nicht ohne Weiteres als unecht zurückwei sen können. Diese Verfahren und Kontrollen müssen Folgendes umfassen: (k) Anwendung geeigneter Kontrolle n der Systemdok umentation, darunter: (1) Angemesse	rds-snapshots-public-prohibited	Verwalten Sie den Zugriff auf Ressource n in der AWS Cloud, indem Sie sicherste llen, dass Amazon Relational Database Service (Amazon RDS) -Instance s nicht öffentlic h sind. Amazon-RDS-Datenbank-Instances können vertrauliche Informati onen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	ne Kontrollen des Zugriffs auf und der Verteilung und Verwendun g von Unterlage n für den Betrieb und die Wartung des Systems; (2) Verfahren zur Überprüfung und Kontrolle von Änderungen, um ein Audit Trail anzulegen , in dem die Erstellun g und Änderung der Systemdokumentatio n in chronolog ischer Reihenfolge dokumentiert wird.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
11.10(k)	Personen, die geschlossene Systeme verwenden , um elektronische Aufzeichnungen zu erstellen, zu ändern, zu pflegen oder zu übertragen, müssen entsprech ende Verfahren und Kontrollen anwenden, um die Echtheit, Integritä t und gegebenen falls die Vertrauli chkeit elektronischer Aufzeichnungen sicherzustellen und dafür zu sorgen, dass die Unterzeic hneten die signierte Aufzeichnung nicht ohne Weiteres als unecht zurückwei sen können. Diese Verfahren und Kontrollen müssen Folgendes umfassen: (k) Anwendung geeigneter Kontrolle n der Systemdok umentation, darunter: (1) Angemesse	redshift-cluster-public-access-überprüfen	Verwalten Sie den Zugriff auf Ressource n in der AWS Cloud, indem Sie sicherste llen, dass Amazon Redshift Redshift-Cluster nicht öffentlic h sind. Amazon-Re dshift-Cluster können vertrauliche Informati onen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	ne Kontrollen des Zugriffs auf und der Verteilung und Verwendun g von Unterlage n für den Betrieb und die Wartung des Systems; (2) Verfahren zur Überprüfung und Kontrolle von Änderungen, um ein Audit Trail anzulegen , in dem die Erstellun g und Änderung der Systemdokumentatio n in chronolog ischer Reihenfolge dokumentiert wird.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
11.10(k)	Personen, die geschlossene Systeme verwenden, um elektronische Aufzeichnungen zu erstellen, zu ändern, zu pflegen oder zu übertragen, müssen entsprechende Verfahren und Kontrollen anwenden, um die Echtheit, Integrität und gegebenenfalls die Vertraulichkeit elektronischer Aufzeichnungen sicherzustellen und dafür zu sorgen, dass die Unterzeichneten die signierte Aufzeichnung nicht ohne Weiteres als unecht zurückweisen können. Diese Verfahren und Kontrollen müssen Folgendes umfassen: (k) Anwendung geeigneter Kontrollen der Systemdokumentation, darunter: (1) Angemesse	restricted-common-ports	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass gemeinsame Ports für Amazon Elastic Compute Cloud (Amazon EC2) -Sicherheitsgruppen eingeschränkt sind. Wenn der Zugriff auf Ports nicht auf vertrauenswürdige Quellen beschränkt wird, kann dies zu Angriffen auf die Verfügbarkeit, Integrität und Vertraulichkeit von Systemen führen. Mit dieser Regel können Sie optional die Parameter blockedPort1–blockedPort5 festlegen (Standardkonfigurationen: 20, 21, 3389, 3306, 4333). Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	ne Kontrollen des Zugriffs auf und der Verteilung und Verwendun g von Unterlage n für den Betrieb und die Wartung des Systems; (2) Verfahren zur Überprüfung und Kontrolle von Änderungen, um ein Audit Trail anzulegen , in dem die Erstellun g und Änderung der Systemdokumentatio n in chronolog ischer Reihenfolge dokumentiert wird.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
11.10(k)	Personen, die geschlossene Systeme verwenden, um elektronische Aufzeichnungen zu erstellen, zu ändern, zu pflegen oder zu übertragen, müssen entsprechende Verfahren und Kontrollen anwenden, um die Echtheit, Integrität und gegebenenfalls die Vertraulichkeit elektronischer Aufzeichnungen sicherzustellen und dafür zu sorgen, dass die Unterzeichneten die signierte Aufzeichnung nicht ohne Weiteres als unecht zurückweisen können. Diese Verfahren und Kontrollen müssen Folgendes umfassen: (k) Anwendung geeigneter Kontrollen der Systemdokumentation, darunter: (1) Angemesse	s3- account-level-public-access -Block-periodisch	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Simple Storage Service (Amazon S3) -Buckets nicht öffentlich zugänglich sind. Diese Regel trägt dazu bei, sensible Daten vor unbefugten Remote-Benutzern zu schützen, indem sie den öffentlichen Zugriff verhindert. Mit dieser Regel können Sie optional die Parameter ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) und restrictPublicBuckets Parameter (Config Default: True) festlegen. Die tatsächlichen Werte müssen den Richtlini

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	ne Kontrollen des Zugriffs auf und der Verteilung und Verwendun g von Unterlage n für den Betrieb und die Wartung des Systems; (2) Verfahren zur Überprüfung und Kontrolle von Änderungen, um ein Audit Trail anzulegen , in dem die Erstellun g und Änderung der Systemdokumentatio n in chronolog ischer Reihenfolge dokumentiert wird.		en Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
11.10(k)	Personen, die geschlossene Systeme verwenden , um elektronische Aufzeichnungen zu erstellen, zu ändern, zu pflegen oder zu übertragen, müssen entsprech ende Verfahren und Kontrollen anwenden, um die Echtheit, Integritä t und gegebenen falls die Vertrauli chkeit elektronischer Aufzeichnungen sicherzustellen und dafür zu sorgen, dass die Unterzeic hneten die signierte Aufzeichnung nicht ohne Weiteres als unecht zurückwei sen können. Diese Verfahren und Kontrollen müssen Folgendes umfassen: (k) Anwendung geeigneter Kontrolle n der Systemdok umentation, darunter: (1) Angemesse	s3- bucket-logging-enabled	Die Amazon Simple Storage Service (Amazon S3)-Serverzugriffs protokollierung bietet eine Methode zur Überwachu ng des Netzwerks im Hinblick auf potenzielle Cybersich erheitsereignisse. Die Ereignisse werden überwacht, indem detaillierte Aufzeichn ungen über die Anfragen erfasst werden, die an einen Amazon-S3-Bucket gestellt wurden. Jeder Zugriffsprotokolle intrag enthält Details zu einer einzelnen Zugriffsanfrage. Zu den Details gehören Anforderer, Bucket-Name, Anforderu ngszeit, Anforderu ngsaktion, Antwortst atus und Fehlercode, falls relevant.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	ne Kontrollen des Zugriffs auf und der Verteilung und Verwendun g von Unterlage n für den Betrieb und die Wartung des Systems; (2) Verfahren zur Überprüfung und Kontrolle von Änderungen, um ein Audit Trail anzulegen , in dem die Erstellun g und Änderung der Systemdokumentatio n in chronolog ischer Reihenfolge dokumentiert wird.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
11.10(k)	Personen, die geschlossene Systeme verwenden , um elektronische Aufzeichnungen zu erstellen, zu ändern, zu pflegen oder zu übertragen, müssen entsprech ende Verfahren und Kontrollen anwenden, um die Echtheit, Integritä t und gegebenen falls die Vertrauli chkeit elektronischer Aufzeichnungen sicherzustellen und dafür zu sorgen, dass die Unterzeic hneten die signierte Aufzeichnung nicht ohne Weiteres als unecht zurückwei sen können. Diese Verfahren und Kontrollen müssen Folgendes umfassen: (k) Anwendung geeigneter Kontrolle n der Systemdok umentation, darunter: (1) Angemesse	s-3 bucket-public-read -prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie nur autorisierten Benutzern, Prozessen und Geräten Zugriff auf Amazon Simple Storage Service (Amazon S3) - Buckets gewähren. Die Verwaltung des Zugriffs sollte mit der Klassifizierung der Daten übereinst immen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	ne Kontrollen des Zugriffs auf und der Verteilung und Verwendun g von Unterlage n für den Betrieb und die Wartung des Systems; (2) Verfahren zur Überprüfung und Kontrolle von Änderungen, um ein Audit Trail anzulegen , in dem die Erstellun g und Änderung der Systemdokumentatio n in chronolog ischer Reihenfolge dokumentiert wird.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
11.10(k)	Personen, die geschlossene Systeme verwenden , um elektronische Aufzeichnungen zu erstellen, zu ändern, zu pflegen oder zu übertragen, müssen entsprech ende Verfahren und Kontrollen anwenden, um die Echtheit, Integritä t und gegebenen falls die Vertrauli chkeit elektronischer Aufzeichnungen sicherzustellen und dafür zu sorgen, dass die Unterzeic hneten die signierte Aufzeichnung nicht ohne Weiteres als unecht zurückwei sen können. Diese Verfahren und Kontrollen müssen Folgendes umfassen: (k) Anwendung geeigneter Kontrolle n der Systemdok umentation, darunter: (1) Angemesse	s3- bucket-public-writ e-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie nur autorisierten Benutzern, Prozessen und Geräten Zugriff auf Amazon Simple Storage Service (Amazon S3) - Buckets gewähren. Die Verwaltung des Zugriffs sollte mit der Klassifizierung der Daten übereinst immen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	ne Kontrollen des Zugriffs auf und der Verteilung und Verwendun g von Unterlage n für den Betrieb und die Wartung des Systems; (2) Verfahren zur Überprüfung und Kontrolle von Änderungen, um ein Audit Trail anzulegen , in dem die Erstellun g und Änderung der Systemdokumentatio n in chronolog ischer Reihenfolge dokumentiert wird.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
11.10(k)	Personen, die geschlossene Systeme verwenden, um elektronische Aufzeichnungen zu erstellen, zu ändern, zu pflegen oder zu übertragen, müssen entsprechende Verfahren und Kontrollen anwenden, um die Echtheit, Integrität und gegebenenfalls die Vertraulichkeit elektronischer Aufzeichnungen sicherzustellen und dafür zu sorgen, dass die Unterzeichneten die signierte Aufzeichnung nicht ohne Weiteres als unecht zurückweisen können. Diese Verfahren und Kontrollen müssen Folgendes umfassen: (k) Anwendung geeigneter Kontrollen der Systemdokumentation, darunter: (1) Angemesse	sagemaker-notebook-no-direct-Internetzugang	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass SageMaker Amazon-Notebooks keinen direkten Internetzugang zulassen. Indem Sie direkten Internetzugang blockieren, vermeiden Sie, dass unbefugte Benutzer auf sensible Daten zugreifen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	ne Kontrollen des Zugriffs auf und der Verteilung und Verwendun g von Unterlage n für den Betrieb und die Wartung des Systems; (2) Verfahren zur Überprüfung und Kontrolle von Änderungen, um ein Audit Trail anzulegen , in dem die Erstellun g und Änderung der Systemdokumentatio n in chronolog ischer Reihenfolge dokumentiert wird.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
11.10(k)	Personen, die geschlossene Systeme verwenden , um elektronische Aufzeichnungen zu erstellen, zu ändern, zu pflegen oder zu übertragen, müssen entsprech ende Verfahren und Kontrollen anwenden, um die Echtheit, Integritä t und gegebenen falls die Vertrauli chkeit elektronischer Aufzeichnungen sicherzustellen und dafür zu sorgen, dass die Unterzeic hneten die signierte Aufzeichnung nicht ohne Weiteres als unecht zurückwei sen können. Diese Verfahren und Kontrollen müssen Folgendes umfassen: (k) Anwendung geeigneter Kontrolle n der Systemdok umentation, darunter: (1) Angemesse	ssm-document-not-p ublic	Stellen Sie sicher, dass AWS Systems Manager (SSM) - Dokumente nicht öffentlich sind, da dies einen unbeabsic htigten Zugriff auf Ihre SSM-Dokum ente ermöglichen kann. Ein öffentlic hes SSM-Dokum ent kann Informati onen über Ihr Konto, Ihre Ressourcen und internen Prozesse preisgeben.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	ne Kontrollen des Zugriffs auf und der Verteilung und Verwendun g von Unterlage n für den Betrieb und die Wartung des Systems; (2) Verfahren zur Überprüfung und Kontrolle von Änderungen, um ein Audit Trail anzulegen , in dem die Erstellun g und Änderung der Systemdokumentatio n in chronolog ischer Reihenfolge dokumentiert wird.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
11.10(k)	Personen, die geschlossene Systeme verwenden , um elektronische Aufzeichnungen zu erstellen, zu ändern, zu pflegen oder zu übertragen, müssen entsprech ende Verfahren und Kontrollen anwenden, um die Echtheit, Integritä t und gegebenen falls die Vertrauli chkeit elektronischer Aufzeichnungen sicherzustellen und dafür zu sorgen, dass die Unterzeic hneten die signierte Aufzeichnung nicht ohne Weiteres als unecht zurückwei sen können. Diese Verfahren und Kontrollen müssen Folgendes umfassen: (k) Anwendung geeigneter Kontrolle n der Systemdok umentation, darunter: (1) Angemesse	vpc-default-security-group-geschlossen	Sicherheitsgruppen von Amazon Elastic Compute Cloud (Amazon EC2) können bei der Verwaltung des Netzwerkzugriffs helfen, indem sie eine statusbehaftete Filterung des ein- und ausgehenden Netzwerkverkehrs zu Ressourcen bereitstellen. AWS Die Beschränk ung des gesamten Datenverkehrs auf die Standardsicherheit sgruppe hilft dabei, den Fernzugriff auf Ihre Ressourcen einzuschränken. AWS

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	ne Kontrollen des Zugriffs auf und der Verteilung und Verwendun g von Unterlage n für den Betrieb und die Wartung des Systems; (2) Verfahren zur Überprüfung und Kontrolle von Änderungen, um ein Audit Trail anzulegen , in dem die Erstellun g und Änderung der Systemdokumentatio n in chronolog ischer Reihenfolge dokumentiert wird.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
11.10(k)	Personen, die geschlossene Systeme verwenden , um elektronische Aufzeichnungen zu erstellen, zu ändern, zu pflegen oder zu übertragen, müssen entsprech ende Verfahren und Kontrollen anwenden, um die Echtheit, Integritä t und gegebenen falls die Vertrauli chkeit elektronischer Aufzeichnungen sicherzustellen und dafür zu sorgen, dass die Unterzeic hneten die signierte Aufzeichnung nicht ohne Weiteres als unecht zurückwei sen können. Diese Verfahren und Kontrollen müssen Folgendes umfassen: (k) Anwendung geeigneter Kontrolle n der Systemdok umentation, darunter: (1) Angemesse	vpc-sg-open-only-to-authorized-ports	Verwalten Sie den Zugriff auf Ressource n in der AWS Cloud, indem Sie sicherste llen, dass gemeinsam e Ports für Amazon Elastic Compute Cloud (Amazon EC2) -Sicherhe itsgruppen eingeschr ränkt sind. Wenn der Zugriff auf Ports nicht auf vertrauen swürdige Quellen beschränkt wird, kann dies zu Angriffen auf die Verfügbar keit, Integrität und Vertraulichkeit von Systemen führen. Durch die Beschränk ung des Zugriffs auf Ressourcen innerhalb einer Sicherhei tsgruppe aus dem Internet (0.0.0.0/0) kann der Remote-Zugriff auf interne Systeme gesteuert werden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	ne Kontrollen des Zugriffs auf und der Verteilung und Verwendun g von Unterlage n für den Betrieb und die Wartung des Systems; (2) Verfahren zur Überprüfung und Kontrolle von Änderungen, um ein Audit Trail anzulegen , in dem die Erstellun g und Änderung der Systemdokumentatio n in chronolog ischer Reihenfolge dokumentiert wird.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
11.10(k)	Personen, die geschlossene Systeme verwenden , um elektronische Aufzeichnungen zu erstellen, zu ändern, zu pflegen oder zu übertragen, müssen entsprech ende Verfahren und Kontrollen anwenden, um die Echtheit, Integritä t und gegebenen falls die Vertrauli chkeit elektronischer Aufzeichnungen sicherzustellen und dafür zu sorgen, dass die Unterzeic hneten die signierte Aufzeichnung nicht ohne Weiteres als unecht zurückwei sen können. Diese Verfahren und Kontrollen müssen Folgendes umfassen: (k) Anwendung geeigneter Kontrolle n der Systemdok umentation, darunter: (1) Angemesse	s3 bucket-level-public-access - verboten	Verwalten Sie den Zugriff auf Ressource n in der AWS Cloud, indem Sie sicherste llen, dass Amazon Simple Storage Service (Amazon S3) -Buckets nicht öffentlich zugänglic h sind. Diese Regel trägt dazu bei, sensible Daten vor unbefugten Remote-Benutzern zu schützen, indem sie den öffentlichen Zugriff auf Bucket-Eb ene verhindert.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	ne Kontrollen des Zugriffs auf und der Verteilung und Verwendun g von Unterlage n für den Betrieb und die Wartung des Systems; (2) Verfahren zur Überprüfung und Kontrolle von Änderungen, um ein Audit Trail anzulegen , in dem die Erstellun g und Änderung der Systemdokumentatio n in chronolog ischer Reihenfolge dokumentiert wird.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
11.2	(a) Elektronische Signaturen, die nicht auf biometrischen Daten basieren: (1) müssen mindestens zwei unterschiedliche Identifikationskomponenten wie einen Identifikationscode und ein Passwort enthalten. (i) Wenn eine Person in einem einzigen, ununterbrochenen Zeitraum des kontrollierten Systemzugriffs mehrere Signaturen erstellt, muss die erste Signatur unter Verwendung aller elektronischen Signaturkomponenten erfolgen; nachfolgende Signaturen erfordern mindestens eine elektronische Signaturkomponente, die nur von dieser Person ausgeführt werden kann und auch nur von ihr verwendet werden soll. (ii) Wenn eine	access-keys-rotated	Die Anmeldeinformationen für autorisierte Geräte, Benutzer und Prozesse werden geprüft, indem sichergestellt wird, dass die IAM-Zugriffsschlüssel gemäß den Vorgaben der Unternehmensrichtlinie rotiert werden. Das regelmäßige Ändern der Zugriffsschlüssel ist eine bewährte Sicherheitsmethode. Es verkürzt den Zeitraum, in dem ein Zugriffsschlüssel aktiv ist, und reduziert die Auswirkungen auf das Unternehmen, wenn die Schlüssel kompromittiert werden. Diese Regel erfordert einen Wert für die Zugriffsschlüssel-Rotation (Standardkonfiguration: 90). Der tatsächliche Wert muss den Richtlini

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	Person eine oder mehrere Signature n erstellt, die nicht während eines einzigen, ununterbr ochenen Zeitraums des kontrollierten Systemzugriffs erfolgten, sind für jede Signatur alle elektronischen Signaturkomponente n erforderlich. (2) dürfen nur von ihren echten Eigentümern verwendet werden; und (3) müssen so verwaltet und ausgeführt werden, dass die versuchte Verwendung der elektronischen Signatur einer Person durch eine andere Person als ihren echten Eigentümer die Zusammenarbeit von mindestens zwei Personen erfordert.		en Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
11.2	(a) Elektronische Signaturen, die nicht auf biometrischen Daten basieren: (1) müssen mindestens zwei unterschiedliche Identifikationskomponenten wie einen Identifikationscode und ein Passwort enthalten. (i) Wenn eine Person in einem einzigen, ununterbrochenen Zeitraum des kontrollierten Systemzugriffs mehrere Signaturen erstellt, muss die erste Signatur unter Verwendung aller elektronischen Signaturkomponenten erfolgen; nachfolgende Signaturen erfordern mindestens eine elektronische Signaturkomponente, die nur von dieser Person ausgeführt werden kann und auch nur von ihr verwendet werden soll. (ii) Wenn eine	iam-password-policy	Die Identitäten und Anmeldeinformationen werden auf der Grundlage einer organisatorischen IAM-Passwortrichtlinie ausgestellt, verwaltet und verifiziert. Sie erfüllen oder übertreffen die Anforderungen von NIST SP 800-63 und dem Standard „Best Practices“ von AWS Foundational Security in Bezug auf die Passwortstärke. Mit dieser Regel können Sie optional RequireUppercaseCharacters (Wert für AWS grundlegende Sicherheitsbewährte Verfahren: wahr), RequireLowercaseCharacters (Wert für bewährte Methoden für AWS grundlegende Sicherheit: wahr), RequireSymbols (Wert für bewährte Methoden für AWS grundlegende Sicherheit:

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	Person eine oder mehrere Signaturen erstellt, die nicht während eines einzigen, ununterbrochenen Zeitraums des kontrollierten Systemzugriffs erfolgten, sind für jede Signatur alle elektronischen Signaturkomponenten erforderlich. (2) dürfen nur von ihren echten Eigentümern verwendet werden; und (3) müssen so verwaltet und ausgeführt werden, dass die versuchte Verwendung der elektronischen Signatur einer Person durch eine andere Person als ihren echten Eigentümer die Zusammenarbeit von mindestens zwei Personen erfordert.		wahr), RequireNumbers (Wert für bewährte Methoden für AWS grundlegende Sicherheit: wahr), MinimumPasswordLength (Wert für bewährte Methoden für AWS grundlegende Sicherheit: 14), PasswordReusePrevention (Wert für bewährte Methoden für AWS grundlegende Sicherheit: 24) und MaxPasswordAge (Wert für bewährte Methoden für AWS grundlegende Sicherheit: 90) für Ihr IAM festlegen Kennwortrichtlinie. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
11.2	(a) Elektronische Signaturen, die nicht auf biometrischen Daten basieren: (1) müssen mindestens zwei unterschiedliche Identifikationskomponenten wie einen Identifikationscode und ein Passwort enthalten. (i) Wenn eine Person in einem einzigen, ununterbrochenen Zeitraum des kontrollierten Systemzugriffs mehrere Signaturen erstellt, muss die erste Signatur unter Verwendung aller elektronischen Signaturkomponenten erfolgen; nachfolgende Signaturen erfordern mindestens eine elektronische Signaturkomponente, die nur von dieser Person ausgeführt werden kann und auch nur von ihr verwendet werden soll. (ii) Wenn eine	iam-root-access-key-überprüfen	Der Zugriff auf Systeme und Ressourcen kann gesteuert werden, indem überprüft wird, ob der Root-Benutzer keine Zugriffsschlüssel mit seiner AWS Identity and Access Management (IAM) -Rolle verknüpft hat. Stellen Sie sicher, dass die Root-Zugriffsschlüssel gelöscht werden. Erstellen und verwenden Sie stattdessen rollenbasierte Funktionen, AWS-Konten um das Prinzip der geringsten Funktionalität zu berücksichtigen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	Person eine oder mehrere Signature n erstellt, die nicht während eines einzigen, ununterbr ochenen Zeitraums des kontrollierten Systemzugriffs erfolgten, sind für jede Signatur alle elektronischen Signaturkomponente n erforderlich. (2) dürfen nur von ihren echten Eigentümern verwendet werden; und (3) müssen so verwaltet und ausgeführt werden, dass die versuchte Verwendung der elektronischen Signatur einer Person durch eine andere Person als ihren echten Eigentümer die Zusammenarbeit von mindestens zwei Personen erfordert.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
11.2	(a) Elektronische Signaturen, die nicht auf biometrischen Daten basieren: (1) müssen mindestens zwei unterschiedliche Identifikationskomponenten wie einen Identifikationscode und ein Passwort enthalten. (i) Wenn eine Person in einem einzigen, ununterbrochenen Zeitraum des kontrollierten Systemzugriffs mehrere Signaturen erstellt, muss die erste Signatur unter Verwendung aller elektronischen Signaturkomponenten erfolgen; nachfolgende Signaturen erfordern mindestens eine elektronische Signaturkomponente, die nur von dieser Person ausgeführt werden kann und auch nur von ihr verwendet werden soll. (ii) Wenn eine	iam-user-mfa-enabled	Aktivieren Sie diese Regel, um den Zugriff auf Ressourcen in der AWS Cloud einzuschränken. Diese Regel sorgt dafür, dass die Multi-Faktor-Authentifizierung (MFA) für alle Benutzer aktiviert ist. MFA sorgt für eine weitere Schutzebene zusätzlich zu den Anmeldeinformationen. Reduzieren Sie Fälle von kompromittierten Konten, indem Sie MFA für Benutzer vorschreiben.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	Person eine oder mehrere Signature n erstellt, die nicht während eines einzigen, ununterbr ochenen Zeitraums des kontrollierten Systemzugriffs erfolgten, sind für jede Signatur alle elektronischen Signaturkomponente n erforderlich. (2) dürfen nur von ihren echten Eigentümern verwendet werden; und (3) müssen so verwaltet und ausgeführt werden, dass die versuchte Verwendung der elektronischen Signatur einer Person durch eine andere Person als ihren echten Eigentümer die Zusammenarbeit von mindestens zwei Personen erfordert.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
11.2	(a) Elektronische Signaturen, die nicht auf biometrischen Daten basieren: (1) müssen mindestens zwei unterschiedliche Identifikationskomponenten wie einen Identifikationscode und ein Passwort enthalten. (i) Wenn eine Person in einem einzigen, ununterbrochenen Zeitraum des kontrollierten Systemzugriffs mehrere Signaturen erstellt, muss die erste Signatur unter Verwendung aller elektronischen Signaturkomponenten erfolgen; nachfolgende Signaturen erfordern mindestens eine elektronische Signaturkomponente, die nur von dieser Person ausgeführt werden kann und auch nur von ihr verwendet werden soll. (ii) Wenn eine	mfa-enabled-for-iam-Konsolenzugriff	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass MFA für alle AWS Identity and Access Management (IAM) -Benutzer aktiviert ist, die über ein Konsolenkennwort verfügen. MFA sorgt für eine weitere Schutzebene zusätzlich zu den Anmeldeinformationen. Indem Sie MFA für Benutzer vorschreiben, können Sie Fälle kompromittierter Konten reduzieren und verhindern, dass unbefugte Benutzer auf vertrauliche Daten zugreifen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	Person eine oder mehrere Signature n erstellt, die nicht während eines einzigen, ununterbr ochenen Zeitraums des kontrollierten Systemzugriffs erfolgten, sind für jede Signatur alle elektronischen Signaturkomponente n erforderlich. (2) dürfen nur von ihren echten Eigentümern verwendet werden; und (3) müssen so verwaltet und ausgeführt werden, dass die versuchte Verwendung der elektronischen Signatur einer Person durch eine andere Person als ihren echten Eigentümer die Zusammenarbeit von mindestens zwei Personen erfordert.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
11.2	(a) Elektronische Signaturen, die nicht auf biometrischen Daten basieren: (1) müssen mindestens zwei unterschiedliche Identifikationskomponenten wie einen Identifikationscode und ein Passwort enthalten. (i) Wenn eine Person in einem einzigen, ununterbrochenen Zeitraum des kontrollierten Systemzugriffs mehrere Signaturen erstellt, muss die erste Signatur unter Verwendung aller elektronischen Signaturkomponenten erfolgen; nachfolgende Signaturen erfordern mindestens eine elektronische Signaturkomponente, die nur von dieser Person ausgeführt werden kann und auch nur von ihr verwendet werden soll. (ii) Wenn eine	root-account-hardware-mfa-aktiviert	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Hardware-MFA für den Root-Benutzer aktiviert ist. Der Stammbenutzer ist der AWS-Konto-Benutzer mit den meisten Berechtigungen. MFA sorgt für eine weitere Schutzebene zusätzlich zu den Anmeldeinformationen. Indem Sie MFA für den Root-Benutzer vorschreiben, können Sie die Anzahl AWS-Konten kompromittierter Benutzer reduzieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	Person eine oder mehrere Signature n erstellt, die nicht während eines einzigen, ununterbr ochenen Zeitraums des kontrollierten Systemzugriffs erfolgten, sind für jede Signatur alle elektronischen Signaturkomponente n erforderlich. (2) dürfen nur von ihren echten Eigentümern verwendet werden; und (3) müssen so verwaltet und ausgeführt werden, dass die versuchte Verwendung der elektronischen Signatur einer Person durch eine andere Person als ihren echten Eigentümer die Zusammenarbeit von mindestens zwei Personen erfordert.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
11.2	(a) Elektronische Signaturen, die nicht auf biometrischen Daten basieren: (1) müssen mindestens zwei unterschiedliche Identifikationskomponenten wie einen Identifikationscode und ein Passwort enthalten. (i) Wenn eine Person in einem einzigen, ununterbrochenen Zeitraum des kontrollierten Systemzugriffs mehrere Signaturen erstellt, muss die erste Signatur unter Verwendung aller elektronischen Signaturkomponenten erfolgen; nachfolgende Signaturen erfordern mindestens eine elektronische Signaturkomponente, die nur von dieser Person ausgeführt werden kann und auch nur von ihr verwendet werden soll. (ii) Wenn eine	root-account-mfa-enabled	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass MFA für den Root-Benutzer aktiviert ist. Der Stammbenutzer ist der AWS-Konto-Benutzer mit den meisten Berechtigungen. MFA sorgt für eine weitere Schutzebene zusätzlich zu den Anmeldeinformationen. Indem Sie MFA für den Root-Benutzer vorschreiben, können Sie die Anzahl AWS-Konten kompromittierter Benutzer reduzieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	Person eine oder mehrere Signature n erstellt, die nicht während eines einzigen, ununterbr ochenen Zeitraums des kontrollierten Systemzugriffs erfolgten, sind für jede Signatur alle elektronischen Signaturkomponente n erforderlich. (2) dürfen nur von ihren echten Eigentümern verwendet werden; und (3) müssen so verwaltet und ausgeführt werden, dass die versuchte Verwendung der elektronischen Signatur einer Person durch eine andere Person als ihren echten Eigentümer die Zusammenarbeit von mindestens zwei Personen erfordert.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
11.3	Personen, die offene Systeme verwenden , um elektronische Aufzeichnungen zu erstellen, zu ändern, zu pflegen oder zu übertragen, müssen entsprech ende Verfahren und Kontrollen anwenden, um die Echtheit, Integritä t und gegebenen falls die Vertrauli chkeit elektronischer Aufzeichnungen ab dem Zeitpunkt ihrer Erstellung bis zu ihrem Empfang sicherzustellen. Zu diesen Verfahren und Kontrollen gehören gegebenen falls die in 11.10 genannten Verfahren und zusätzliche Maßnahmen wie die Verschlüsselung von Dokumenten und die Anwendung geeigneter Standards für digitale Signature n, um, soweit dies	alb-http-to-https-Umleitungsprüfung	Um Daten während der Übertragung zu schützen, stellen Sie sicher, dass Ihr Application Load Balancer unverschl üsselte HTTP-Anfr agen automatisch an HTTPS umleitet. Um eventuell vorhanden e sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	unter den gegebenen Umständen erforderlich ist, die Authentizität, Integrität und Vertraulichkeit der Aufzeichnungen sicherzustellen.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
11.3	Personen, die offene Systeme verwenden, um elektronische Aufzeichnungen zu erstellen, zu ändern, zu pflegen oder zu übertragen, müssen entsprechende Verfahren und Kontrollen anwenden, um die Echtheit, Integrität und gegebenenfalls die Vertraulichkeit elektronischer Aufzeichnungen ab dem Zeitpunkt ihrer Erstellung bis zu ihrem Empfang sicherzustellen. Zu diesen Verfahren und Kontrollen gehören gegebenenfalls die in 11.10 genannten Verfahren und zusätzliche Maßnahmen wie die Verschlüsselung von Dokumenten und die Anwendung geeigneter Standards für digitale Signaturen, um, soweit dies	api-gw-cache-enabled-und-verschlüsselt	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass die Verschlüsselung für den Cache Ihrer API-Gateway-Stufe aktiviert ist. Da für die API-Methode sensible Daten erfasst werden können, sollten Sie die Verschlüsselung von Daten im Ruhezustand aktivieren, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	unter den gegebenen Umständen erforderlich ist, die Authentizität, Integrität und Vertraulichkeit der Aufzeichnungen sicherzustellen.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
11.3	Personen, die offene Systeme verwenden , um elektronische Aufzeichnungen zu erstellen, zu ändern, zu pflegen oder zu übertragen, müssen entsprech ende Verfahren und Kontrollen anwenden, um die Echtheit, Integritä t und gegebenen falls die Vertrauli chkeit elektronischer Aufzeichnungen ab dem Zeitpunkt ihrer Erstellung bis zu ihrem Empfang sicherzustellen. Zu diesen Verfahren und Kontrollen gehören gegebenen falls die in 11.10 genannten Verfahren und zusätzliche Maßnahmen wie die Verschlüsselung von Dokumenten und die Anwendung geeigneter Standards für digitale Signature n, um, soweit dies	api-gw-ssl-enabled	Stellen Sie sicher, dass die REST-API-Stufen von Amazon API Gateway mit SSL-Zertifikaten konfiguri ert sind, damit Backend-Systeme überprüfen können, ob Anforderungen von API Gateway stammen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	unter den gegebenen Umständen erforderlich ist, die Authentizität, Integrität und Vertraulichkeit der Aufzeichnungen sicherzustellen.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
11,3	Personen, die offene Systeme verwenden , um elektronische Aufzeichnungen zu erstellen, zu ändern, zu pflegen oder zu übertragen, müssen entsprech ende Verfahren und Kontrollen anwenden, um die Echtheit, Integritä t und gegebenen falls die Vertrauli chkeit elektronischer Aufzeichnungen ab dem Zeitpunkt ihrer Erstellung bis zu ihrem Empfang sicherzustellen. Zu diesen Verfahren und Kontrollen gehören gegebenen falls die in 11.10 genannten Verfahren und zusätzliche Maßnahmen wie die Verschlüsselung von Dokumenten und die Anwendung geeigneter Standards für digitale Signature n, um, soweit dies	api-gw-ssl-enabled	Stellen Sie sicher, dass die REST-API-Stufen von Amazon API Gateway mit SSL-Zertifikaten konfiguri ert sind, damit Backend-Systeme überprüfen können, ob Anforderungen von API Gateway stammen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	unter den gegebenen Umständen erforderlich ist, die Authentizität, Integrität und Vertraulichkeit der Aufzeichnungen sicherzustellen.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
11,3	Personen, die offene Systeme verwenden, um elektronische Aufzeichnungen zu erstellen, zu ändern, zu pflegen oder zu übertragen, müssen entsprechende Verfahren und Kontrollen anwenden, um die Echtheit, Integrität und gegebenenfalls die Vertraulichkeit elektronischer Aufzeichnungen ab dem Zeitpunkt ihrer Erstellung bis zu ihrem Empfang sicherzustellen. Zu diesen Verfahren und Kontrollen gehören gegebenenfalls die in 11.10 genannten Verfahren und zusätzliche Maßnahmen wie die Verschlüsselung von Dokumenten und die Anwendung geeigneter Standards für digitale Signaturen, um, soweit dies	backup-recovery-point-encrypted	Stellen Sie sicher, dass die Verschlüsselung für Ihre AWS Backup-Wiederherstellungspunkte aktiviert ist. Da sensible Daten auch im Ruhezustand vorhanden sein können, sollten Sie die Verschlüsselung im Ruhezustand aktivieren, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	unter den gegebenen Umständen erforderlich ist, die Authentizität, Integrität und Vertraulichkeit der Aufzeichnungen sicherzustellen.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
11.3	Personen, die offene Systeme verwenden , um elektronische Aufzeichnungen zu erstellen, zu ändern, zu pflegen oder zu übertragen, müssen entsprech ende Verfahren und Kontrollen anwenden, um die Echtheit, Integritä t und gegebenen falls die Vertrauli chkeit elektronischer Aufzeichnungen ab dem Zeitpunkt ihrer Erstellung bis zu ihrem Empfang sicherzustellen. Zu diesen Verfahren und Kontrollen gehören gegebenen falls die in 11.10 genannten Verfahren und zusätzliche Maßnahmen wie die Verschlüsselung von Dokumenten und die Anwendung geeigneter Standards für digitale Signature n, um, soweit dies	cloud-trail-encryption-enabled	Da sensible Daten vorhanden sein können und um Daten im Ruhezustand zu schützen, sollten Sie sicherstellen, dass die Verschlüsselung für Ihre AWS CloudTrail Trails aktiviert ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	unter den gegebenen Umständen erforderlich ist, die Authentizität, Integrität und Vertraulichkeit der Aufzeichnungen sicherzustellen.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
11.3	Personen, die offene Systeme verwenden , um elektronische Aufzeichnungen zu erstellen, zu ändern, zu pflegen oder zu übertragen, müssen entsprech ende Verfahren und Kontrollen anwenden, um die Echtheit, Integritä t und gegebenen falls die Vertrauli chkeit elektronischer Aufzeichnungen ab dem Zeitpunkt ihrer Erstellung bis zu ihrem Empfang sicherzustellen. Zu diesen Verfahren und Kontrollen gehören gegebenen falls die in 11.10 genannten Verfahren und zusätzliche Maßnahmen wie die Verschlüsselung von Dokumenten und die Anwendung geeigneter Standards für digitale Signature n, um, soweit dies	cloud-trail-log-file-Validierung aktiviert	Verwenden Sie die AWS CloudTrail Protokolldateivali dierung, um die Integrität von Protokoll en zu überprüfen. CloudTrail Mithilfe der Protokolldateivali dierung kann festgestellt werden, ob eine Protokoll datei geändert oder gelöscht wurde oder ob sie nach der Übermittlung CloudTrail unverände rt geblieben ist. Dieses Feature wurde mit dem Branchens tandard entsprech enden Algorithmen entwickelt: SHA-256 für die Hashfunktion und SHA-256 mit RSA für digitale Signature n. Aus diesem Grund ist es rechnerisch unmöglich, CloudTrai l Protokolldateien unbemerkt zu ändern, zu löschen oder zu fälschen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	unter den gegebenen Umständen erforderl ich ist, die Authentiz ität, Integrität und Vertraulichkeit der Aufzeichnungen sicherzustellen.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
11.3	Personen, die offene Systeme verwenden , um elektronische Aufzeichnungen zu erstellen, zu ändern, zu pflegen oder zu übertragen, müssen entsprech ende Verfahren und Kontrollen anwenden, um die Echtheit, Integritä t und gegebenen falls die Vertrauli chkeit elektronischer Aufzeichnungen ab dem Zeitpunkt ihrer Erstellung bis zu ihrem Empfang sicherzustellen. Zu diesen Verfahren und Kontrollen gehören gegebenen falls die in 11.10 genannten Verfahren und zusätzliche Maßnahmen wie die Verschlüsselung von Dokumenten und die Anwendung geeigneter Standards für digitale Signature n, um, soweit dies	cloudwatch-log-group-encrypted	Um sensible Daten im Speicher zu schützen, stellen Sie sicher, dass die Verschlüs selung für Ihre Amazon CloudWatch Log Groups aktiviert ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	unter den gegebenen Umständen erforderlich ist, die Authentizität, Integrität und Vertraulichkeit der Aufzeichnungen sicherzustellen.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
11.3	Personen, die offene Systeme verwenden , um elektronische Aufzeichnungen zu erstellen, zu ändern, zu pflegen oder zu übertragen, müssen entsprech ende Verfahren und Kontrollen anwenden, um die Echtheit, Integritä t und gegebenen falls die Vertrauli chkeit elektronischer Aufzeichnungen ab dem Zeitpunkt ihrer Erstellung bis zu ihrem Empfang sicherzustellen. Zu diesen Verfahren und Kontrollen gehören gegebenen falls die in 11.10 genannten Verfahren und zusätzliche Maßnahmen wie die Verschlüsselung von Dokumenten und die Anwendung geeigneter Standards für digitale Signature n, um, soweit dies	cmk-backing-key-rotation-aktiviert	Aktivieren Sie die Schlüsselrotation, um sicherzustellen, dass Schlüssel rotiert werden, nachdem sie das Ende ihrer Krypto-Periode erreicht haben.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	unter den gegebenen Umständen erforderlich ist, die Authentizität, Integrität und Vertraulichkeit der Aufzeichnungen sicherzustellen.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
11.3	Personen, die offene Systeme verwenden , um elektronische Aufzeichnungen zu erstellen, zu ändern, zu pflegen oder zu übertragen, müssen entsprech ende Verfahren und Kontrollen anwenden, um die Echtheit, Integritä t und gegebenen falls die Vertrauli chkeit elektronischer Aufzeichnungen ab dem Zeitpunkt ihrer Erstellung bis zu ihrem Empfang sicherzustellen. Zu diesen Verfahren und Kontrollen gehören gegebenen falls die in 11.10 genannten Verfahren und zusätzliche Maßnahmen wie die Verschlüsselung von Dokumenten und die Anwendung geeigneter Standards für digitale Signature n, um, soweit dies	codebuild-project-artifact-encryption	Um sensible Daten im Speicher zu schützen, stellen Sie sicher, dass die Verschlüs selung für Ihre AWS CodeBuild Artefakte aktiviert ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	unter den gegebenen Umständen erforderlich ist, die Authentizität, Integrität und Vertraulichkeit der Aufzeichnungen sicherzustellen.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
11.3	Personen, die offene Systeme verwenden , um elektronische Aufzeichnungen zu erstellen, zu ändern, zu pflegen oder zu übertragen, müssen entsprech ende Verfahren und Kontrollen anwenden, um die Echtheit, Integritä t und gegebenen falls die Vertrauli chkeit elektronischer Aufzeichnungen ab dem Zeitpunkt ihrer Erstellung bis zu ihrem Empfang sicherzustellen. Zu diesen Verfahren und Kontrollen gehören gegebenen falls die in 11.10 genannten Verfahren und zusätzliche Maßnahmen wie die Verschlüsselung von Dokumenten und die Anwendung geeigneter Standards für digitale Signature n, um, soweit dies	codebuild-project-s3-Log-verschlüsselt	Um sensible Daten im Ruhezustand zu schützen, stellen Sie sicher, dass die Verschlüsselung für Ihre in Amazon S3 gespeicherten AWS CodeBuild Protokolle aktiviert ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	unter den gegebenen Umständen erforderlich ist, die Authentizität, Integrität und Vertraulichkeit der Aufzeichnungen sicherzustellen.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
11.3	Personen, die offene Systeme verwenden, um elektronische Aufzeichnungen zu erstellen, zu ändern, zu pflegen oder zu übertragen, müssen entsprechende Verfahren und Kontrollen anwenden, um die Echtheit, Integrität und gegebenenfalls die Vertraulichkeit elektronischer Aufzeichnungen ab dem Zeitpunkt ihrer Erstellung bis zu ihrem Empfang sicherzustellen. Zu diesen Verfahren und Kontrollen gehören gegebenenfalls die in 11.10 genannten Verfahren und zusätzliche Maßnahmen wie die Verschlüsselung von Dokumenten und die Anwendung geeigneter Standards für digitale Signaturen, um, soweit dies	dynamodb-table-encrypted-kms	Stellen Sie sicher, dass die Verschlüsselung für Ihre Amazon-DynamoDB-Tabellen aktiviert ist. Um eventuell vorhandene sensible Daten im Ruhezustand in diesen Tabellen zu schützen, müssen Sie die Verschlüsselung von Daten im Ruhezustand aktivieren. Standardmäßig werden DynamoDB-Tabellen mit einem AWS eigenen Kundenhauptschlüssel (CMK) verschlüselt.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	unter den gegebenen Umständen erforderlich ist, die Authentizität, Integrität und Vertraulichkeit der Aufzeichnungen sicherzustellen.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
11.3	Personen, die offene Systeme verwenden , um elektronische Aufzeichnungen zu erstellen, zu ändern, zu pflegen oder zu übertragen, müssen entsprech ende Verfahren und Kontrollen anwenden, um die Echtheit, Integritä t und gegebenen falls die Vertrauli chkeit elektronischer Aufzeichnungen ab dem Zeitpunkt ihrer Erstellung bis zu ihrem Empfang sicherzustellen. Zu diesen Verfahren und Kontrollen gehören gegebenen falls die in 11.10 genannten Verfahren und zusätzliche Maßnahmen wie die Verschlüsselung von Dokumenten und die Anwendung geeigneter Standards für digitale Signature n, um, soweit dies	ec-2 ebs-encryption-by-default	Zum Schutz von Daten im Ruhezusta nd müssen Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon Elastic Block Store (Amazon EBS)-Volu mes aktiviert ist. Da sensible Daten auch im Ruhezusta nd vorhanden sein können, sollten Sie die Verschlüsselung im Ruhezustand aktivieren, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	unter den gegebenen Umständen erforderlich ist, die Authentizität, Integrität und Vertraulichkeit der Aufzeichnungen sicherzustellen.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
11,3	Personen, die offene Systeme verwenden , um elektronische Aufzeichnungen zu erstellen, zu ändern, zu pflegen oder zu übertragen, müssen entsprech ende Verfahren und Kontrollen anwenden, um die Echtheit, Integritä t und gegebenen falls die Vertrauli chkeit elektronischer Aufzeichnungen ab dem Zeitpunkt ihrer Erstellung bis zu ihrem Empfang sicherzustellen. Zu diesen Verfahren und Kontrollen gehören gegebenen falls die in 11.10 genannten Verfahren und zusätzliche Maßnahmen wie die Verschlüsselung von Dokumenten und die Anwendung geeigneter Standards für digitale Signature n, um, soweit dies	efs-encrypted-check	Aktivieren Sie die Verschlüsselung für Ihr Amazon Elastic File System (EFS), um eventuell vorhandene sensible Daten sowie Daten im Ruhezustand zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	unter den gegebenen Umständen erforderlich ist, die Authentizität, Integrität und Vertraulichkeit der Aufzeichnungen sicherzustellen.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
11,3	Personen, die offene Systeme verwenden, um elektronische Aufzeichnungen zu erstellen, zu ändern, zu pflegen oder zu übertragen, müssen entsprechende Verfahren und Kontrollen anwenden, um die Echtheit, Integrität und gegebenenfalls die Vertraulichkeit elektronischer Aufzeichnungen ab dem Zeitpunkt ihrer Erstellung bis zu ihrem Empfang sicherzustellen. Zu diesen Verfahren und Kontrollen gehören gegebenenfalls die in 11.10 genannten Verfahren und zusätzliche Maßnahmen wie die Verschlüsselung von Dokumenten und die Anwendung geeigneter Standards für digitale Signaturen, um, soweit dies	elasticsearch-encrypted-at-rest	Da sensible Daten vorhanden sein können und um Daten im Ruhezustand zu schützen, sollten Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon OpenSearch Service (OpenSearch Service) -Domains aktiviert ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	unter den gegebenen Umständen erforderlich ist, die Authentizität, Integrität und Vertraulichkeit der Aufzeichnungen sicherzustellen.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
11.3	Personen, die offene Systeme verwenden, um elektronische Aufzeichnungen zu erstellen, zu ändern, zu pflegen oder zu übertragen, müssen entsprechende Verfahren und Kontrollen anwenden, um die Echtheit, Integrität und gegebenenfalls die Vertraulichkeit elektronischer Aufzeichnungen ab dem Zeitpunkt ihrer Erstellung bis zu ihrem Empfang sicherzustellen. Zu diesen Verfahren und Kontrollen gehören gegebenenfalls die in 11.10 genannten Verfahren und zusätzliche Maßnahmen wie die Verschlüsselung von Dokumenten und die Anwendung geeigneter Standards für digitale Signaturen, um, soweit dies	elasticsearch-encrypted-at-rest	Da sensible Daten vorhanden sein können und um Daten im Ruhezustand zu schützen, sollten Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon OpenSearch Service (OpenSearch Service) -Domains aktiviert ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	unter den gegebenen Umständen erforderlich ist, die Authentizität, Integrität und Vertraulichkeit der Aufzeichnungen sicherzustellen.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
11.3	Personen, die offene Systeme verwenden, um elektronische Aufzeichnungen zu erstellen, zu ändern, zu pflegen oder zu übertragen, müssen entsprechende Verfahren und Kontrollen anwenden, um die Echtheit, Integrität und gegebenenfalls die Vertraulichkeit elektronischer Aufzeichnungen ab dem Zeitpunkt ihrer Erstellung bis zu ihrem Empfang sicherzustellen. Zu diesen Verfahren und Kontrollen gehören gegebenenfalls die in 11.10 genannten Verfahren und zusätzliche Maßnahmen wie die Verschlüsselung von Dokumenten und die Anwendung geeigneter Standards für digitale Signaturen, um, soweit dies	elasticsearch-node-to-node-Verschlüsselungsprüfung	Stellen Sie sicher, dass die node-to-node Verschlüsselung für Amazon OpenSearch Service aktiviert ist. Node-to-nodeVerschlüsselung ermöglicht die TLS 1.2-Verschlüsselung für die gesamte Kommunikation innerhalb der Amazon Virtual Private Cloud (Amazon VPC). Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	unter den gegebenen Umständen erforderlich ist, die Authentizität, Integrität und Vertraulichkeit der Aufzeichnungen sicherzustellen.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
11.3	Personen, die offene Systeme verwenden , um elektronische Aufzeichnungen zu erstellen, zu ändern, zu pflegen oder zu übertragen, müssen entsprech ende Verfahren und Kontrollen anwenden, um die Echtheit, Integritä t und gegebenen falls die Vertrauli chkeit elektronischer Aufzeichnungen ab dem Zeitpunkt ihrer Erstellung bis zu ihrem Empfang sicherzustellen. Zu diesen Verfahren und Kontrollen gehören gegebenen falls die in 11.10 genannten Verfahren und zusätzliche Maßnahmen wie die Verschlüsselung von Dokumenten und die Anwendung geeigneter Standards für digitale Signature n, um, soweit dies	elb-acm-certificate-required	Zum Schutz von eventuell vorhanden en sensiblen Daten sowie von Daten während der Übertragung muss die Verschlüsselung für Ihr Elastic Load Balancing aktiviert sein. Verwenden Sie AWS Certificate Manager, um öffentlic he und private SSL/ TLS-Zertifikate mit AWS Diensten und internen Ressource n zu verwalten, bereitzustellen und bereitzustellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	unter den gegebenen Umständen erforderlich ist, die Authentizität, Integrität und Vertraulichkeit der Aufzeichnungen sicherzustellen.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
11.3	Personen, die offene Systeme verwenden , um elektronische Aufzeichnungen zu erstellen, zu ändern, zu pflegen oder zu übertragen, müssen entsprech ende Verfahren und Kontrollen anwenden, um die Echtheit, Integritä t und gegebenen falls die Vertrauli chkeit elektronischer Aufzeichnungen ab dem Zeitpunkt ihrer Erstellung bis zu ihrem Empfang sicherzustellen. Zu diesen Verfahren und Kontrollen gehören gegebenen falls die in 11.10 genannten Verfahren und zusätzliche Maßnahmen wie die Verschlüsselung von Dokumenten und die Anwendung geeigneter Standards für digitale Signature n, um, soweit dies	elb-acm-certificate-required	Zum Schutz von eventuell vorhanden en sensiblen Daten sowie von Daten während der Übertragung muss die Verschlüsselung für Ihr Elastic Load Balancing aktiviert sein. Verwenden Sie AWS Certificate Manager, um öffentlic he und private SSL/ TLS-Zertifikate mit AWS Diensten und internen Ressource n zu verwalten, bereitzustellen und bereitzustellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	unter den gegebenen Umständen erforderlich ist, die Authentizität, Integrität und Vertraulichkeit der Aufzeichnungen sicherzustellen.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
11.3	Personen, die offene Systeme verwenden , um elektronische Aufzeichnungen zu erstellen, zu ändern, zu pflegen oder zu übertragen, müssen entsprech ende Verfahren und Kontrollen anwenden, um die Echtheit, Integritä t und gegebenen falls die Vertrauli chkeit elektronischer Aufzeichnungen ab dem Zeitpunkt ihrer Erstellung bis zu ihrem Empfang sicherzustellen. Zu diesen Verfahren und Kontrollen gehören gegebenen falls die in 11.10 genannten Verfahren und zusätzliche Maßnahmen wie die Verschlüsselung von Dokumenten und die Anwendung geeigneter Standards für digitale Signature n, um, soweit dies	elb-tls-https-listeners-nur	Stellen Sie sicher, dass Ihre Elastic Load Balancer (ELBs) mit SSL- oder HTTPS-Listenern konfiguriert sind. Um eventuell vorhanden e sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	unter den gegebenen Umständen erforderlich ist, die Authentizität, Integrität und Vertraulichkeit der Aufzeichnungen sicherzustellen.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
11.3	Personen, die offene Systeme verwenden, um elektronische Aufzeichnungen zu erstellen, zu ändern, zu pflegen oder zu übertragen, müssen entsprechende Verfahren und Kontrollen anwenden, um die Echtheit, Integrität und gegebenenfalls die Vertraulichkeit elektronischer Aufzeichnungen ab dem Zeitpunkt ihrer Erstellung bis zu ihrem Empfang sicherzustellen. Zu diesen Verfahren und Kontrollen gehören gegebenenfalls die in 11.10 genannten Verfahren und zusätzliche Maßnahmen wie die Verschlüsselung von Dokumenten und die Anwendung geeigneter Standards für digitale Signaturen, um, soweit dies	Elb v 2 acm-certificate-required	Zum Schutz von eventuell vorhandenen sensiblen Daten sowie von Daten während der Übertragung muss die Verschlüsselung für Ihr Elastic Load Balancing aktiviert sein. Verwenden Sie AWS Certificate Manager, um öffentliche und private SSL/TLS-Zertifikate mit AWS Diensten und internen Ressourcen zu verwalten, bereitzustellen und bereitzustellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	unter den gegebenen Umständen erforderlich ist, die Authentizität, Integrität und Vertraulichkeit der Aufzeichnungen sicherzustellen.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
11.3	Personen, die offene Systeme verwenden , um elektronische Aufzeichnungen zu erstellen, zu ändern, zu pflegen oder zu übertragen, müssen entsprech ende Verfahren und Kontrollen anwenden, um die Echtheit, Integritä t und gegebenen falls die Vertrauli chkeit elektronischer Aufzeichnungen ab dem Zeitpunkt ihrer Erstellung bis zu ihrem Empfang sicherzustellen. Zu diesen Verfahren und Kontrollen gehören gegebenen falls die in 11.10 genannten Verfahren und zusätzliche Maßnahmen wie die Verschlüsselung von Dokumenten und die Anwendung geeigneter Standards für digitale Signature n, um, soweit dies	encrypted-volumes	Aktivieren Sie die Verschlüsselung für Ihre Amazon-Elastic-Block-Store (Amazon-EBS)-Volumes, um eventuell vorhandene sensible Daten sowie Daten im Ruhezusta nd zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	unter den gegebenen Umständen erforderl ich ist, die Authentiz ität, Integrität und Vertraulichkeit der Aufzeichnungen sicherzustellen.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
11,3	Personen, die offene Systeme verwenden , um elektronische Aufzeichnungen zu erstellen, zu ändern, zu pflegen oder zu übertragen, müssen entsprech ende Verfahren und Kontrollen anwenden, um die Echtheit, Integritä t und gegebenen falls die Vertrauli chkeit elektronischer Aufzeichnungen ab dem Zeitpunkt ihrer Erstellung bis zu ihrem Empfang sicherzustellen. Zu diesen Verfahren und Kontrollen gehören gegebenen falls die in 11.10 genannten Verfahren und zusätzliche Maßnahmen wie die Verschlüsselung von Dokumenten und die Anwendung geeigneter Standards für digitale Signature n, um, soweit dies	kinesis-stream-enc rypted	Aktivieren Sie die Verschlüsselung für Ihre Amazon-Kinesis-Streams, um eventuell vorhandene sensible Daten sowie Daten im Ruhezustand zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	unter den gegebenen Umständen erforderl ich ist, die Authentiz ität, Integrität und Vertraulichkeit der Aufzeichnungen sicherzustellen.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
11,3	Personen, die offene Systeme verwenden, um elektronische Aufzeichnungen zu erstellen, zu ändern, zu pflegen oder zu übertragen, müssen entsprechende Verfahren und Kontrollen anwenden, um die Echtheit, Integrität und gegebenenfalls die Vertraulichkeit elektronischer Aufzeichnungen ab dem Zeitpunkt ihrer Erstellung bis zu ihrem Empfang sicherzustellen. Zu diesen Verfahren und Kontrollen gehören gegebenenfalls die in 11.10 genannten Verfahren und zusätzliche Maßnahmen wie die Verschlüsselung von Dokumenten und die Anwendung geeigneter Standards für digitale Signaturen, um, soweit dies	kms-cmk-not-scheduled-zum Löschen	Um Daten im Ruhezustand zu schützen, sollten Sie sicherstellen, dass die für den Kunden erforderlichen Masterschlüssel (CMKs) nicht im AWS Key Management Service (AWS KMS) gelöscht werden. Da Schlüssel manchmal gelöscht werden müssen, können Sie mit dieser Regel alle zu löschenden Schlüssel überprüfen, falls ein Schlüssel versehentlich zur Löschung vorgemerkt wurde.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	unter den gegebenen Umständen erforderl ich ist, die Authentiz ität, Integrität und Vertraulichkeit der Aufzeichnungen sicherzustellen.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
11.3	Personen, die offene Systeme verwenden , um elektronische Aufzeichnungen zu erstellen, zu ändern, zu pflegen oder zu übertragen, müssen entsprech ende Verfahren und Kontrollen anwenden, um die Echtheit, Integritä t und gegebenen falls die Vertrauli chkeit elektronischer Aufzeichnungen ab dem Zeitpunkt ihrer Erstellung bis zu ihrem Empfang sicherzustellen. Zu diesen Verfahren und Kontrollen gehören gegebenen falls die in 11.10 genannten Verfahren und zusätzliche Maßnahmen wie die Verschlüsselung von Dokumenten und die Anwendung geeigneter Standards für digitale Signature n, um, soweit dies	opensearch-encrypt ed-at-rest	Da sensible Daten vorhanden sein können und um Daten im Ruhezustand zu schützen, sollten Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon OpenSearch Service-Domains aktiviert ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	unter den gegebenen Umständen erforderlich ist, die Authentizität, Integrität und Vertraulichkeit der Aufzeichnungen sicherzustellen.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
11.3	Personen, die offene Systeme verwenden , um elektronische Aufzeichnungen zu erstellen, zu ändern, zu pflegen oder zu übertragen, müssen entsprech ende Verfahren und Kontrollen anwenden, um die Echtheit, Integritä t und gegebenen falls die Vertrauli chkeit elektronischer Aufzeichnungen ab dem Zeitpunkt ihrer Erstellung bis zu ihrem Empfang sicherzustellen. Zu diesen Verfahren und Kontrollen gehören gegebenen falls die in 11.10 genannten Verfahren und zusätzliche Maßnahmen wie die Verschlüsselung von Dokumenten und die Anwendung geeigneter Standards für digitale Signature n, um, soweit dies	opensearch-node-to -node-Verschlüssel ungsprüfung	Stellen Sie sicher, dass die node-to-node Verschlüs selung für Amazon OpenSearch Service aktiviert ist. Node-to-nodeVerschlüsselung ermöglicht die TLS 1.2-Verschlüsselun g für die gesamte Kommunikation innerhalb der Amazon Virtual Private Cloud (Amazon VPC). Um eventuell vorhanden e sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	unter den gegebenen Umständen erforderlich ist, die Authentizität, Integrität und Vertraulichkeit der Aufzeichnungen sicherzustellen.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
11.3	Personen, die offene Systeme verwenden, um elektronische Aufzeichnungen zu erstellen, zu ändern, zu pflegen oder zu übertragen, müssen entsprechende Verfahren und Kontrollen anwenden, um die Echtheit, Integrität und gegebenenfalls die Vertraulichkeit elektronischer Aufzeichnungen ab dem Zeitpunkt ihrer Erstellung bis zu ihrem Empfang sicherzustellen. Zu diesen Verfahren und Kontrollen gehören gegebenenfalls die in 11.10 genannten Verfahren und zusätzliche Maßnahmen wie die Verschlüsselung von Dokumenten und die Anwendung geeigneter Standards für digitale Signaturen, um, soweit dies	rds-snapshot-encrypted	Stellen Sie sicher, dass die Verschlüsselung für Ihre Amazon Relational Database Service (Amazon RDS)-Snapshots aktiviert ist. Da sensible Daten auch im Ruhezustand vorhanden sein können, sollten Sie die Verschlüsselung im Ruhezustand aktivieren, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	unter den gegebenen Umständen erforderlich ist, die Authentizität, Integrität und Vertraulichkeit der Aufzeichnungen sicherzustellen.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
11,3	Personen, die offene Systeme verwenden , um elektronische Aufzeichnungen zu erstellen, zu ändern, zu pflegen oder zu übertragen, müssen entsprech ende Verfahren und Kontrollen anwenden, um die Echtheit, Integritä t und gegebenen falls die Vertrauli chkeit elektronischer Aufzeichnungen ab dem Zeitpunkt ihrer Erstellung bis zu ihrem Empfang sicherzustellen. Zu diesen Verfahren und Kontrollen gehören gegebenen falls die in 11.10 genannten Verfahren und zusätzliche Maßnahmen wie die Verschlüsselung von Dokumenten und die Anwendung geeigneter Standards für digitale Signature n, um, soweit dies	rds-storage-encrypted	Zum Schutz von Daten im Ruhezusta nd müssen Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon Relational Database Service (Amazon RDS)-Instances aktiviert ist. Um eventuell vorhanden e sensible Daten im Ruhezustand in Amazon-RDS-Instanc es zu schützen, muss die Verschlüs selung von Daten im Ruhezustand aktiviert sein.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	unter den gegebenen Umständen erforderlich ist, die Authentizität, Integrität und Vertraulichkeit der Aufzeichnungen sicherzustellen.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
11,3	Personen, die offene Systeme verwenden, um elektronische Aufzeichnungen zu erstellen, zu ändern, zu pflegen oder zu übertragen, müssen entsprechende Verfahren und Kontrollen anwenden, um die Echtheit, Integrität und gegebenenfalls die Vertraulichkeit elektronischer Aufzeichnungen ab dem Zeitpunkt ihrer Erstellung bis zu ihrem Empfang sicherzustellen. Zu diesen Verfahren und Kontrollen gehören gegebenenfalls die in 11.10 genannten Verfahren und zusätzliche Maßnahmen wie die Verschlüsselung von Dokumenten und die Anwendung geeigneter Standards für digitale Signaturen, um, soweit dies	redshift-cluster-configuration-check	Um Daten im Ruhezustand zu schützen, muss die Verschlüsselung für Ihre Amazon-Redshift-Cluster aktiviert sein. Sie müssen auch sicherstellen, dass die erforderlichen Konfigurationen auf Amazon-Redshift-Clustern bereitgestellt werden. Die Prüfungsprotokollierung muss aktiviert sein, um Informationen zu Verbindungen und Benutzeraktivitäten in der Datenbank bereitzustellen. Diese Regel erfordert, dass ein Wert für clusterDbEncrypted (Config Default: TRUE) und LoggingEnabled (Config Default: TRUE) gesetzt ist. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	unter den gegebenen Umständen erforderlich ist, die Authentizität, Integrität und Vertraulichkeit der Aufzeichnungen sicherzustellen.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
11.3	Personen, die offene Systeme verwenden , um elektronische Aufzeichnungen zu erstellen, zu ändern, zu pflegen oder zu übertragen, müssen entsprech ende Verfahren und Kontrollen anwenden, um die Echtheit, Integritä t und gegebenen falls die Vertrauli chkeit elektronischer Aufzeichnungen ab dem Zeitpunkt ihrer Erstellung bis zu ihrem Empfang sicherzustellen. Zu diesen Verfahren und Kontrollen gehören gegebenen falls die in 11.10 genannten Verfahren und zusätzliche Maßnahmen wie die Verschlüsselung von Dokumenten und die Anwendung geeigneter Standards für digitale Signature n, um, soweit dies	redshift-cluster-kms-enabled	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass die Verschlüs selung mit AWS Key Management Service (AWS KMS) für Ihren Amazon Redshift Redshift-Cluster aktiviert ist. Um eventuell vorhanden e sensible Daten im Ruhezustand in Redshift-Clustern zu schützen, muss die Verschlüsselung von Daten im Ruhezusta nd aktiviert sein.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	unter den gegebenen Umständen erforderlich ist, die Authentizität, Integrität und Vertraulichkeit der Aufzeichnungen sicherzustellen.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
11.3	Personen, die offene Systeme verwenden , um elektronische Aufzeichnungen zu erstellen, zu ändern, zu pflegen oder zu übertragen, müssen entsprech ende Verfahren und Kontrollen anwenden, um die Echtheit, Integritä t und gegebenen falls die Vertrauli chkeit elektronischer Aufzeichnungen ab dem Zeitpunkt ihrer Erstellung bis zu ihrem Empfang sicherzustellen. Zu diesen Verfahren und Kontrollen gehören gegebenen falls die in 11.10 genannten Verfahren und zusätzliche Maßnahmen wie die Verschlüsselung von Dokumenten und die Anwendung geeigneter Standards für digitale Signature n, um, soweit dies	redshift-require-tls-ssl	Stellen Sie sicher, dass Ihre Amazon-Redshift-Cluster eine TLS/SSL-Verschlüss elung erfordern, um eine Verbindun g zu SQL-Clients herzustellen. Um eventuell vorhanden e sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	unter den gegebenen Umständen erforderlich ist, die Authentizität, Integrität und Vertraulichkeit der Aufzeichnungen sicherzustellen.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
11,3	Personen, die offene Systeme verwenden, um elektronische Aufzeichnungen zu erstellen, zu ändern, zu pflegen oder zu übertragen, müssen entsprechende Verfahren und Kontrollen anwenden, um die Echtheit, Integrität und gegebenenfalls die Vertraulichkeit elektronischer Aufzeichnungen ab dem Zeitpunkt ihrer Erstellung bis zu ihrem Empfang sicherzustellen. Zu diesen Verfahren und Kontrollen gehören gegebenenfalls die in 11.10 genannten Verfahren und zusätzliche Maßnahmen wie die Verschlüsselung von Dokumenten und die Anwendung geeigneter Standards für digitale Signaturen, um, soweit dies	s3-fähig bucket-server-side-encryption	Zum Schutz von Daten im Ruhezustand müssen Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon Simple Storage Service (Amazon S3)-Buckets aktiviert ist. Um eventuell vorhandene sensible Daten im Ruhezustand in Amazon-S3-Buckets zu schützen, muss die Verschlüsselung aktiviert sein.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	unter den gegebenen Umständen erforderlich ist, die Authentizität, Integrität und Vertraulichkeit der Aufzeichnungen sicherzustellen.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
11.3	Personen, die offene Systeme verwenden, um elektronische Aufzeichnungen zu erstellen, zu ändern, zu pflegen oder zu übertragen, müssen entsprechende Verfahren und Kontrollen anwenden, um die Echtheit, Integrität und gegebenenfalls die Vertraulichkeit elektronischer Aufzeichnungen ab dem Zeitpunkt ihrer Erstellung bis zu ihrem Empfang sicherzustellen. Zu diesen Verfahren und Kontrollen gehören gegebenenfalls die in 11.10 genannten Verfahren und zusätzliche Maßnahmen wie die Verschlüsselung von Dokumenten und die Anwendung geeigneter Standards für digitale Signaturen, um, soweit dies	s-3 bucket-ssl-requests-only	Um Daten während der Übertragung zu schützen, stellen Sie sicher, dass Ihre Amazon Simple Storage Service (Amazon S3)-Buckets Anfragen zur Verwendung von Secure Socket Layer (SSL)-Buckets erfordern. Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	unter den gegebenen Umständen erforderl ich ist, die Authentiz ität, Integrität und Vertraulichkeit der Aufzeichnungen sicherzustellen.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
11,3	Personen, die offene Systeme verwenden, um elektronische Aufzeichnungen zu erstellen, zu ändern, zu pflegen oder zu übertragen, müssen entsprechende Verfahren und Kontrollen anwenden, um die Echtheit, Integrität und gegebenenfalls die Vertraulichkeit elektronischer Aufzeichnungen ab dem Zeitpunkt ihrer Erstellung bis zu ihrem Empfang sicherzustellen. Zu diesen Verfahren und Kontrollen gehören gegebenenfalls die in 11.10 genannten Verfahren und zusätzliche Maßnahmen wie die Verschlüsselung von Dokumenten und die Anwendung geeigneter Standards für digitale Signaturen, um, soweit dies	s-3 default-encryption-kms	Stellen Sie sicher, dass die Verschlüsselung für Ihre Amazon Simple Storage Service (Amazon S3)-Buckets aktiviert ist. Um eventuell vorhandene sensible Daten im Ruhezustand in einem Amazon-S3-Bucket zu schützen, muss die Verschlüsselung aktiviert sein.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	unter den gegebenen Umständen erforderlich ist, die Authentizität, Integrität und Vertraulichkeit der Aufzeichnungen sicherzustellen.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
11,3	Personen, die offene Systeme verwenden , um elektronische Aufzeichnungen zu erstellen, zu ändern, zu pflegen oder zu übertragen, müssen entsprech ende Verfahren und Kontrollen anwenden, um die Echtheit, Integritä t und gegebenen falls die Vertrauli chkeit elektronischer Aufzeichnungen ab dem Zeitpunkt ihrer Erstellung bis zu ihrem Empfang sicherzustellen. Zu diesen Verfahren und Kontrollen gehören gegebenen falls die in 11.10 genannten Verfahren und zusätzliche Maßnahmen wie die Verschlüsselung von Dokumenten und die Anwendung geeigneter Standards für digitale Signature n, um, soweit dies	sagemaker-endpoint -configuration-kms- schlüsselkonfiguriert	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass die Verschlüsselung mit dem AWS Key Management Service (AWS KMS) für Ihren Endpunkt aktiviert ist. SageMaker Da sensible Daten auf dem SageMaker Endgerät gespeiche rt werden können, sollten Sie die Verschlüsselung im Ruhezustand aktiviere n, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	unter den gegebenen Umständen erforderlich ist, die Authentizität, Integrität und Vertraulichkeit der Aufzeichnungen sicherzustellen.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
11.3	Personen, die offene Systeme verwenden, um elektronische Aufzeichnungen zu erstellen, zu ändern, zu pflegen oder zu übertragen, müssen entsprechende Verfahren und Kontrollen anwenden, um die Echtheit, Integrität und gegebenenfalls die Vertraulichkeit elektronischer Aufzeichnungen ab dem Zeitpunkt ihrer Erstellung bis zu ihrem Empfang sicherzustellen. Zu diesen Verfahren und Kontrollen gehören gegebenenfalls die in 11.10 genannten Verfahren und zusätzliche Maßnahmen wie die Verschlüsselung von Dokumenten und die Anwendung geeigneter Standards für digitale Signaturen, um, soweit dies	sagemaker-notebook-instance-kms-schlüsselkonfiguriert	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass die Verschlüsselung mit dem AWS Key Management Service (AWS KMS) für Ihr Notebook aktiviert ist. SageMaker Da vertrauliche Daten im SageMaker Notebook gespeichert werden können, sollten Sie die Verschlüsselung im Ruhezustand aktivieren, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	unter den gegebenen Umständen erforderlich ist, die Authentizität, Integrität und Vertraulichkeit der Aufzeichnungen sicherzustellen.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
11.3	Personen, die offene Systeme verwenden, um elektronische Aufzeichnungen zu erstellen, zu ändern, zu pflegen oder zu übertragen, müssen entsprechende Verfahren und Kontrollen anwenden, um die Echtheit, Integrität und gegebenenfalls die Vertraulichkeit elektronischer Aufzeichnungen ab dem Zeitpunkt ihrer Erstellung bis zu ihrem Empfang sicherzustellen. Zu diesen Verfahren und Kontrollen gehören gegebenenfalls die in 11.10 genannten Verfahren und zusätzliche Maßnahmen wie die Verschlüsselung von Dokumenten und die Anwendung geeigneter Standards für digitale Signaturen, um, soweit dies	secretsmanager-using-cmk	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass die Verschlüsselung mit dem AWS Key Management Service (AWS KMS) für AWS Secrets Manager aktiviert ist. Aktivieren Sie die Verschlüsselung von Daten im Ruhezustand, um eventuell vorhandene sensible Daten im Ruhezustand im Secrets Manager zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	unter den gegebenen Umständen erforderlich ist, die Authentizität, Integrität und Vertraulichkeit der Aufzeichnungen sicherzustellen.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
11.3	Personen, die offene Systeme verwenden , um elektronische Aufzeichnungen zu erstellen, zu ändern, zu pflegen oder zu übertragen, müssen entsprech ende Verfahren und Kontrollen anwenden, um die Echtheit, Integritä t und gegebenen falls die Vertrauli chkeit elektronischer Aufzeichnungen ab dem Zeitpunkt ihrer Erstellung bis zu ihrem Empfang sicherzustellen. Zu diesen Verfahren und Kontrollen gehören gegebenen falls die in 11.10 genannten Verfahren und zusätzliche Maßnahmen wie die Verschlüsselung von Dokumenten und die Anwendung geeigneter Standards für digitale Signature n, um, soweit dies	sns-encrypted-kms	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass Ihre Amazon Simple Notification Service (Amazon SNS) -Themen mit dem AWS Key Management Service (AWS KMS) verschlüsselt werden müssen. Um eventuell vorhandene sensible Daten im Ruhezusta nd in veröffentlichten Nachrichten zu schützen, muss die Verschlüsselung von Daten im Ruhezusta nd aktiviert sein.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	unter den gegebenen Umständen erforderlich ist, die Authentizität, Integrität und Vertraulichkeit der Aufzeichnungen sicherzustellen.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
11.300(b)	Personen, die elektronische Signaturen verwenden, die auf der Verwendung von Identifikationscodes in Kombination mit Passwörtern basieren, müssen entsprechende Kontrollen anwenden, um deren Sicherheit und Integrität zu gewährleisten. Zu diesen Kontrollen gehören: (b) Es muss sichergestellt werden, dass Identifizierungscodes und Passwörter regelmäßig überprüft, zurückgerufen oder überarbeitet werden (z. B. um Ereignisse wie das Altern von Passwörtern abzudecken).	access-keys-rotated	Die Anmeldeinformationen für autorisierte Geräte, Benutzer und Prozesse werden geprüft, indem sichergestellt wird, dass die IAM-Zugangsschlüssel entsprechend den Vorgaben der Unternehmensrichtlinie rotiert werden. Das regelmäßige Ändern der Zugriffsschlüssel ist eine bewährte Sicherheitsmethode. Es verkürzt den Zeitraum, in dem ein Zugriffsschlüssel aktiv ist, und reduziert die Auswirkungen auf das Unternehmen, wenn die Schlüssel kompromittiert werden. Diese Regel erfordert einen Wert für die Zugriffsschlüssel-Rotation (Standard konfiguration: 90). Der tatsächliche Wert muss den Richtlini

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			en Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
11.300(b)	Personen, die elektronische Signaturen verwenden, die auf der Verwendung von Identifikationscodes in Kombination mit Passwörtern basieren, müssen entsprechende Kontrollen anwenden, um deren Sicherheit und Integrität zu gewährleisten. Zu diesen Kontrollen gehören: (b) Es muss sichergestellt werden, dass Identifizierungscodes und Passwörter regelmäßig überprüft, zurückgerufen oder überarbeitet werden (z. B. um Ereignisse wie das Altern von Passwörtern abzudecken).	emr-kerberos-enabled	Die Zugriffsberechtigungen und -autorisierungen können verwaltet und nach den Prinzipien der geringsten Berechtigung und Aufgabentrennung integriert werden, indem Kerberos für Amazon-EMR-Cluster aktiviert wird. In Kerberos werden Services und Benutzer, die sich authentifizieren müssen, als Prinzipale bezeichnet. Prinzipale befinden sich in einem Kerberos-Bereich. Innerhalb dieses Bereichs wird ein Kerberos-Server als Key Distribution Center (KDC) bezeichnet. Über diesen Server können sich Prinzipale authentifizieren. Die Authentifizierung im KDC erfolgt durch die Ausstellung von Authentif

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			izierungstickets. Das KDC unterhält eine Datenbank der Prinzipale in seinem Bereich mit ihren Passwörtern und anderen administr ativen Informationen zu jedem Prinzipal.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
11.300(b)	Personen, die elektronische Signaturen verwenden, die auf der Verwendung von Identifikationscodes in Kombination mit Passwörtern basieren, müssen entsprechende Kontrollen anwenden, um deren Sicherheit und Integrität zu gewährleisten. Zu diesen Kontrollen gehören: (b) die Sicherstellung, dass die Ausgabeaufgaben von Identifikationscodes und Passwörtern regelmäßig überprüft, zurückgerufen oder überarbeitet werden (z. B. um Ereignisse wie das Altern von Passwörtern abzudecken).	iam-password-policy	Die Identitäten und Anmeldeinformationen werden auf der Grundlage einer organisatorischen IAM-Passwortrichtlinie ausgestellt, verwaltet und verifiziert. Sie erfüllen oder übertreffen die Anforderungen von NIST SP 800-63 und dem Standard „Best Practices“ von AWS Foundational Security für die Passwortstärke. Mit dieser Regel können Sie optional RequireUppercaseCharacters (Wert für AWS grundlegende Sicherheitsbewährte Verfahren: wahr), RequireLowercaseCharacters (Wert für bewährte Methoden für AWS grundlegende Sicherheit: wahr), RequireSymbols (Wert für bewährte Methoden für AWS grundlegende Sicherheit:

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			wahr), RequireNumbers (Wert für bewährte Methoden für AWS grundlegende Sicherheit: wahr), MinimumPasswordLength (Wert für bewährte Methoden für AWS grundlegende Sicherheit: 14), PasswordReusePrevention (Wert für bewährte Methoden für AWS grundlegende Sicherheit: 24) und MaxPasswordAge (Wert für bewährte Methoden für AWS grundlegende Sicherheit: 90) für Ihr IAM festlegen Kennwortrichtlinie. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
11.300(b)	Personen, die elektronische Signaturen verwenden, die auf der Verwendung von Identifikationscodes in Kombination mit Passwörtern basieren, müssen entsprechende Kontrollen anwenden, um deren Sicherheit und Integrität zu gewährleisten. Zu diesen Kontrollen gehören: (b) die Sicherstellung, dass die Herausgabe von Identifikationscodes und Passwörtern regelmäßig überprüft, zurückgerufen oder überarbeitet wird (z. B. um Ereignisse wie das Altern von Passwörtern abzudecken).	iam-user-unused-credentials-überprüfen	AWS Identity and Access Management (IAM) kann Ihnen bei Zugriffsberechtigungen und Autorisierungen helfen, indem es nach IAM-Passwörtern und Zugriffsschlüsseln sucht, die für einen bestimmten Zeitraum nicht verwendet wurden. Wenn ungenutzte Anmeldeinformationen identifiziert werden, müssen Sie sie deaktivieren und/oder entfernen, da dies gegen das Prinzip der geringsten Berechtigung verstoßen könnte. Für diese Regel müssen Sie einen Wert für das maxCredentialUsage Alter festlegen (Standardkonfiguration: 90). Der tatsächliche Wert muss den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
11.300(b)	Personen, die elektronische Signaturen verwenden, die auf der Verwendung von Identifikationscodes in Kombination mit Passwörtern basieren, müssen entsprechende Kontrollen anwenden, um deren Sicherheit und Integrität zu gewährleisten. Zu diesen Kontrollen gehören: (b) Die Sicherstellung, dass die Herausgabe von Identifikationscodes und Passwörtern regelmäßig überprüft, zurückgerufen oder überarbeitet wird (z. B. um Ereignisse wie das Altern von Passwörtern abzudecken).	secretsmanager-rotation-enabled-check	Diese Regel stellt sicher, dass bei AWS Secrets Manager Manager-Geheimnissen die Rotation aktiviert ist. Die regelmäßige Rotation von Secrets kann den Zeitraum verkürzen, in dem ein Secret aktiv ist, und möglicherweise die Auswirkungen auf das Unternehmen verringern, falls das Secret kompromittiert wird.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
11.300(b)	Personen, die elektronische Signaturen verwenden, die auf der Verwendung von Identifikationscodes in Kombination mit Passwörtern basieren, müssen entsprechende Kontrollen anwenden, um deren Sicherheit und Integrität zu gewährleisten. Zu diesen Kontrollen gehören: (b) die Sicherstellung, dass die Herausgabe von Identifikationscodes und Passwörtern regelmäßig überprüft, zurückgerufen oder überarbeitet wird (z. B. um Ereignisse wie das Altern von Passwörtern abzudecken).	secretsmanager-scheduled-rotation-success-überprüfen	Diese Regel stellt sicher, dass AWS Secrets Manager Manager-Geheimnisse gemäß dem Rotationsplan erfolgreich rotiert wurden. Die regelmäßige Rotation von Secrets kann den Zeitraum verkürzen, in dem ein Secret aktiv ist, und möglicherweise die Auswirkungen auf das Unternehmen verringern, falls es kompromittiert wird.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
11.300(d)	Personen, die elektronische Signaturen verwenden, die auf der Verwendung von Identifikationscodes in Kombination mit Passwörtern basieren, müssen entsprech ende Kontrolle n anwenden, um deren Sicherheit und Integrität zu gewährlei sten. Zu diesen Kontrollen gehören: (d) Maßnahmen zum Schutz von Transaktionen, um die unbefugte Verwendung von Passwörtern und/oder Identifikationscodes zu verhindern und jegliche Versuche einer unbefugte n Verwendung aufzudecken und der Systemsic herheitsabteilung und gegebenen falls der Geschäfts leitung dringend	cloud-trail-cloud-watch-logs-aktiviert	Verwenden Sie Amazon CloudWatc h , um Protokoll ereignisaktivitäten zentral zu sammeln und zu verwalten. Die Aufnahme von AWS CloudTrail Daten liefert Einzelheiten zu den API-Aufrufaktivitä ten in Ihrem AWS-Konto.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	und unverzüglich zu melden.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
11.300(d)	Personen, die elektronische Signaturen verwenden, die auf der Verwendung von Identifikationscodes in Kombination mit Passwörtern basieren, müssen entsprech ende Kontrolle n anwenden, um deren Sicherheit und Integrität zu gewährlei sten. Zu diesen Kontrollen gehören: (d) Maßnahmen zum Schutz von Transaktionen, um die unbefugte Verwendung von Passwörtern und/oder Identifikationscodes zu verhindern und jegliche Versuche einer unbefugte n Verwendung aufzudecken und der Systemsic herheitsabteilung und gegebenen falls der Geschäfts leitung dringend	cloudtrail-enabled	AWS CloudTrail kann bei der Nichtabst reitbarkeit helfen, indem Aktionen und API-Aufrufe der AWS Management Console aufgezeic hnet werden. Sie können die Benutzer und die Benutzer AWS-Konten , die einen AWS Dienst aufgerufen haben, die Quell-IP-Adresse, über die die Aufrufe generiert wurden, und den Zeitpunkt der Anrufe identifiz ieren. Einzelheiten zu den erfassten Daten finden Sie unter Inhalt des AWS CloudTrail Datensatzes.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	und unverzüglich zu melden.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
11.300(d)	Personen, die elektronische Signaturen verwenden, die auf der Verwendung von Identifikationscodes in Kombination mit Passwörtern basieren, müssen entsprech ende Kontrolle n anwenden, um deren Sicherheit und Integrität zu gewährlei sten. Zu diesen Kontrollen gehören: (d) Maßnahmen zum Schutz von Transaktionen, um die unbefugte Verwendung von Passwörtern und/oder Identifikationscodes zu verhindern und jegliche Versuche einer unbefugte n Verwendung aufzudecken und der Systemsic herheitsabteilung und gegebenen falls der Geschäfts leitung dringend	guardduty-enabled-centralized	Amazon GuardDuty kann mithilfe von Threat Intellige nce Feeds helfen, potenzielle Cybersich erheitsereignisse zu überwachen und zu erkennen. Dazu gehören Listen mit bösartigen IPs und maschinel len Lernmethoden zur Identifizierung unerwarteter, nicht autorisierter und bösartiger Aktivitäten in Ihrer AWS Cloud-Umgebung.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	und unverzüglich zu melden.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
11.300(d)	Personen, die elektronische Signaturen verwenden, die auf der Verwendung von Identifikationscodes in Kombination mit Passwörtern basieren, müssen entsprech ende Kontrolle n anwenden, um deren Sicherheit und Integrität zu gewährlei sten. Zu diesen Kontrollen gehören: (d) Maßnahmen zum Schutz von Transaktionen, um die unbefugte Verwendung von Passwörtern und/oder Identifikationscodes zu verhindern und jegliche Versuche einer unbefugte n Verwendung aufzudecken und der Systemsic herheitsabteilung und gegebenen falls der Geschäfts leitung dringend	securityhub-enabled	AWS Security Hub hilft bei der Überwachung von unbefugtem Personal, Verbindun gen, Geräten und Software. AWS Security Hub aggregiert, organisie rt und priorisie rt die Sicherhei tswarnungen oder Ergebnisse mehrerer Dienste. AWS Einige dieser Dienste sind Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer und AWS Firewall Manager sowie AWS Partnerlösungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	und unverzüglich zu melden.		

Vorlage

Die Vorlage ist verfügbar unter GitHub: Operational Best Practices for FDA Title 21 CFR Part 11.

Bewährte Methoden zur Implementierung von FedRAMP(Low)

Conformance Packs bieten ein allgemeines Compliance-Framework, das es Ihnen ermöglicht, mithilfe verwalteter oder benutzerdefinierter Regeln und Abhilfemaßnahmen Kontrollen zur Sicherheits-, Betriebs- oder Kostenoptimierung durchzuführen. AWS Config AWS Config Conformance Packs dienen als Beispielvorlagen nicht dazu, die vollständige Einhaltung eines bestimmten Governance- oder Compliance-Standards sicherzustellen. Sie sind dafür verantwortlich, selbst zu beurteilen, ob Ihre Nutzung der Services den geltenden gesetzlichen und behördlichen Anforderungen entspricht.

Im Folgenden finden Sie ein Beispiel für eine Zuordnung zwischen den Low Baseline Controls des Federal Risk and Authorization Management Program (FedRAMP) und den AWS verwalteten Konfigurationsregeln. Jede Config-Regel gilt für eine bestimmte AWS Ressource und bezieht sich auf ein oder mehrere FedRAMP-Steuerelemente. Eine FedRAMP-Kontrolle kann mehreren Config-Regeln zugeordnet werden. In der folgenden Tabelle finden Sie weitere Informationen und Anleitungen zu diesen Zuordnungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-2	KONTENVERWALTUNG	codebuild-project-logging-enabled	Stellen Sie sicher, dass die AWS CodeBuild Projektprotokollierung aktiviert ist, damit Ihre Build-Ausgabeprotokolle entweder an Amazon CloudWatc

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			h oder Amazon Simple Storage Service (Amazon S3) gesendet werden. Build-Ausgabeprotokolle enthalten detaillierte Informationen zu Ihrem Build-Projekt.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-2	KONTENVERWALTUNG	iam-customer-policy-blocked-kms-Aktionen	AWS Identity and Access Management (IAM) kann Ihnen helfen, die Prinzipien der geringsten Rechte und der Aufgabentrennung in Zugriffsberechtigungen und Autorisierungen zu integrieren und so zu verhindern, dass Richtlinien blockierte Aktionen für alle AWS Schlüssel des Key Management Service enthalten. Wenn Benutzer mehr Rechte haben, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und Aufgabentrennung verstoßen. Mit dieser Regel können Sie den Parameter festlegen. blockedActionsPatterns (Wert „AWS Bewährte grundlegende Sicherheitsmethode

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			n“: kms: Entschlüs seln, kms:ReEnc ryptFrom). Die tatsächlichen Werte müssen den Richtlini en Ihrer Organisation entsprechen.
AC-2	KONTENVER WALTUNG	iam-group-has-users-überprüfen	AWS Identity and Access Managemen t (IAM) kann Ihnen helfen, die Prinzipien der geringsten Rechte und der Aufgabent rennung mit Zugriffsb erechtigungen und Autorisierungen zu integrieren, indem sichergestellt wird, dass IAM-Gruppen mindestens einen Benutzer haben. Die Einteilung von Benutzern in Gruppen auf der Grundlage der ihnen zugewiese nen Berechtigungen oder ihrer Funktion ist eine Möglichkeit, das Prinzip der geringste n Berechtigung zu implementieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-2	KONTENVER WALTUNG	iam-inline-policy-blocked-kms-Aktionen	Stellen Sie sicher, dass ein Benutzer, eine IAM-Rolle oder eine IAM-Gruppe (AWS Identity and Access Management) nicht über eine Inline-Richtlinie verfügt, die blockierte Aktionen für alle AWS Schlüssel des Key Management Service zulässt. AWS empfiehlt, verwaltete Richtlinien anstelle von Inline-Richtlinien zu verwenden. Verwaltete Richtlinien ermöglichen Wiederverwendbarkeit, Versionsverwaltung, Rollback und Delegierung der Berechtigungsverwaltung. Mit dieser Regel können Sie den blockedActionsPatterns Parameter festlegen. (Wert „AWS Bewährte grundlegende Sicherheitsmethoden“: kms: Entschlüsseln, kms:ReEnc

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			ryptFrom). Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.
AC-2	KONTENVERWALTUNG	iam-no-inline-policy-überprüfen	Stellen Sie sicher, dass ein Benutzer, eine IAM-Rolle oder eine IAM-Gruppe (AWS Identity and Access Management) nicht über eine Inline-Richtlinie zur Zugriffskontrolle auf Systeme und Ressourcen verfügt. AWS empfiehlt, verwaltete Richtlinien anstelle von Inline-Richtlinien zu verwenden. Verwaltete Richtlinien ermöglichen Wiederverwendbarkeit, Versionsverwaltung, Rollback und Delegierung der Berechtigungsverwaltung.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-2	KONTENVERWALTUNG	iam-policy-no-statements-with-full-access	Stellen Sie sicher, dass IAM-Aktionen nur auf die benötigten Aktionen beschränkt sind. Wenn Benutzern mehr Rechte eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und der Aufgabentrennung verstoßen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-2	KONTENVERWALTUNG	multi-region-cloudtrail-enabled	AWS CloudTrail zeichnet Aktionen und API-Aufrufe der AWS Management Console auf. Sie können feststellen, welche Benutzer und Konten angerufen wurden AWS, von welcher Quell-IP-Adresse aus die Anrufe getätigt wurden und wann die Anrufe erfolgten. CloudTrail übermittelt Protokolldateien aus allen AWS Regionen an Ihren S3-Bucket , wenn MULTI_REGION_CLOUD_TRAIL_ENABLED aktiviert ist. Außerdem wird beim AWS Start einer neuen Region derselbe Trail in der neuen Region erstellt. CloudTrail Dadurch erhalten Sie automatisch Protokolldateien mit API-Aktivitäten für die neue Region.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-2	KONTENVERWALTUNG	rds-logging-enabled	Um die Protokollierung und Überwachung in Ihrer Umgebung zu erleichtern, stellen Sie sicher, dass die Amazon Relational Database Service (Amazon RDS)-Protokollierung aktiviert ist. Mit der Amazon-RDS-Protokollierung können Sie Ereignisse wie Verbindungen, Verbindungsabbrüche, Abfragen oder abgefragte Tabellen erfassen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-2	KONTENVERWALTUNG	securityhub-enabled	AWS Security Hub hilft bei der Überwachung von unbefugtem Personal, Verbindungen, Geräten und Software. AWS Security Hub aggregiert, organisiert und priorisiert die Sicherheitswarnungen oder Ergebnisse mehrerer Dienste. AWS Einige dieser Dienste sind Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer und AWS Firewall Manager sowie AWS Partnerlösungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-2	KONTENVERWALTUNG	access-keys-rotated	Die Anmeldeinformationen für autorisierte Geräte, Benutzer und Prozesse werden geprüft, indem sichergestellt wird, dass die IAM-Zugriffsschlüssel gemäß den Vorgaben der Unternehmensrichtlinie rotiert werden. Das regelmäßige Ändern der Zugriffsschlüssel ist eine bewährte Sicherheitsmethode. Es verkürzt den Zeitraum, in dem ein Zugriffsschlüssel aktiv ist, und reduziert die Auswirkungen auf das Unternehmen, wenn die Schlüssel kompromittiert werden. Diese Regel erfordert einen Wert für die Zugriffsschlüssel-Rotation (Standardkonfiguration: 90). Der tatsächliche Wert muss den Richtlini

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			en Ihrer Organisation entsprechen.
AC-2	KONTENVERWALTUNG	cloud-trail-cloud-watch-Logs aktiviert	Verwenden Sie Amazon CloudWatch , um Protokoll ereignisaktivitäten zentral zu sammeln und zu verwalten. Die Aufnahme von AWS CloudTrail Daten liefert Einzelheiten zu den API-Aufrufaktivitäten in Ihrem AWS-Konto.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-2	KONTENVERWALTUNG	cloudtrail-enabled	AWS CloudTrail kann bei der Nichtabstreitbarkeit helfen, indem Aktionen und API-Aufrufe der AWS Management Console aufgezeichnet werden. Sie können die Benutzer und die Benutzer AWS-Konten , die einen AWS Dienst aufgerufen haben, die Quell-IP-Adresse, über die die Aufrufe generiert wurden, und den Zeitpunkt der Anrufe identifizieren. Einzelheiten zu den erfassten Daten finden Sie unter Inhalt des AWS CloudTrail Datensatzes.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-2	KONTENVERWALTUNG	cloudtrail-s3-dataevents-enabled	Die Erfassung von Simple Storage Service (Amazon S3)-Datenereignissen unterstützt die Erkennung von ungewöhnlichen Aktivitäten. Zu den Details gehören AWS-Konto Informationen über den Zugriff auf einen Amazon S3 S3-Bucket, die IP-Adresse und die Uhrzeit des Ereignisses.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-2	KONTENVERWALTUNG	cloudwatch-alarm-action-check	Amazon CloudWatch alarmiert, wenn eine Metrik den Schwellenwert für eine bestimmte Anzahl von Bewertungszeiträumen überschreitet. Der Alarm führt eine oder mehrere Aktionen durch, die vom Wert der Metrik oder des Ausdrucks im Vergleich zu einem Schwellenwert in einer Reihe von Zeiträumen abhängt. Diese Regel erfordert einen Wert für alarmActionRequired (Config Default: True), insufficientDataAction Required (Config Default: True), okActionRequired (Config Default: False). Der tatsächliche Wert muss die Alarmaktionen für Ihre Umgebung widerspiegeln.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-2	KONTENVER WALTUNG	guardduty-enabled-centralized	Amazon GuardDuty kann mithilfe von Threat Intellige nce Feeds helfen, potenzielle Cybersich erheitsereignisse zu überwachen und zu erkennen. Dazu gehören Listen mit bösartigen IPs und maschinel len Lernmethoden zur Identifizierung unerwarteter, nicht autorisierter und bösartiger Aktivitäten in Ihrer AWS Cloud-Umgebung.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-2	KONTENVERWALTUNG	iam-password-policy	Die Identitäten und Anmeldeinformationen werden auf der Grundlage einer organisatorischen IAM-Passwortrichtlinie ausgestellt, verwaltet und verifiziert. Sie erfüllen oder übertreffen die Anforderungen von NIST SP 800-63 und dem Standard „Best Practices“ von AWS Foundational Security für die Passwortstärke. Mit dieser Regel können Sie optional RequireUppercaseCharacters (Wert für AWS grundlegende Sicherheitsbewährte Methoden: wahr), RequireLowercaseCharacters (Wert für bewährte Methoden für AWS grundlegende Sicherheit: wahr), RequireSymbols (Wert für bewährte Methoden für AWS grundlegende Sicherheit:

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			wahr), RequireNumbers (Wert für bewährte Methoden für AWS grundlegende Sicherheit: wahr), MinimumPasswordLength (Wert für bewährte Methoden für AWS grundlegende Sicherheit: 14), PasswordReusePrevention (Wert für bewährte Methoden für AWS grundlegende Sicherheit: 24) und MaxPasswordAge (Wert für bewährte Methoden für AWS grundlegende Sicherheit: 90) für Ihr IAM festlegen Kennwortrichtlinie. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-2	KONTENVERWALTUNG	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) kann Ihnen dabei helfen, die Prinzipien der geringsten Rechte und der Aufgabentrennung in Zugriffsberechtigungen und Autorisierungen zu integrieren und so zu verhindern, dass Richtlinien „Effect“: „Allow“ mit „Action“: „*“ anstelle von „Resource“: „*“ enthalten. Wenn Benutzern mehr Rechte eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und der Aufgabentrennung verstoßen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-2	KONTENVERWALTUNG	iam-root-access-key-überprüfen	Der Zugriff auf Systeme und Ressourcen kann gesteuert werden, indem überprüft wird, ob der Root-Benutzer keine Zugriffsschlüssel mit seiner AWS Identity and Access Management (IAM) -Rolle verknüpft hat. Stellen Sie sicher, dass die Root-Zugriffsschlüssel gelöscht werden. Erstellen und verwenden Sie stattdessen rollenbasierte Funktionen, AWS-Konten um das Prinzip der geringsten Funktionalität zu berücksichtigen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-2	KONTENVERWALTUNG	iam-user-group-membership-überprüfen	AWS Identity and Access Management (IAM) kann Ihnen helfen, Zugriffsberechtigungen und Autorisierungen einzuschränken, indem sichergestellt wird, dass Benutzer Mitglieder mindestens einer Gruppe sind. Wenn Benutzern mehr Berechtigungen eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und Aufgabentrennung verstoßen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-2	KONTENVERWALTUNG	iam-user-mfa-enabled	Aktivieren Sie diese Regel, um den Zugriff auf Ressourcen in der AWS Cloud einzuschränken. Diese Regel sorgt dafür, dass die Multi-Faktor-Authentifizierung (MFA) für alle Benutzer aktiviert ist. MFA sorgt für eine weitere Schutzebene zusätzlich zu den Anmeldeinformationen. Reduzieren Sie Fälle von kompromittierten Konten, indem Sie MFA für Benutzer vorschreiben.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-2	KONTENVERWALTUNG	iam-user-no-policies-überprüfen	Diese Regel stellt sicher, dass AWS Identity and Access Management (IAM) -Richtlinien nur Gruppen oder Rollen zugewiesen werden, um den Zugriff auf Systeme und Ressourcen zu kontrollieren. Die Zuweisung von Berechtigungen auf Gruppen- oder Rollenebene trägt dazu bei, die Wahrscheinlichkeit zu verringern, dass eine Identität übermäßige Berechtigungen erhält oder beibehält.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-2	KONTENVERWALTUNG	iam-user-unused-credentials-überprüfen	AWS Identity and Access Management (IAM) kann Ihnen bei Zugriffsberechtigungen und Autorisierungen helfen, indem es nach IAM-Passwörtern und Zugriffsschlüsseln sucht, die für einen bestimmten Zeitraum nicht verwendet wurden. Wenn ungenutzte Anmeldeinformationen identifiziert werden, müssen Sie sie deaktivieren und/oder entfernen, da dies gegen das Prinzip der geringsten Berechtigung verstoßen könnte. Für diese Regel müssen Sie einen Wert für das maxCredentialUsage Alter festlegen (Standardkonfiguration: 90). Der tatsächliche Wert muss den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-2	KONTENVERWALTUNG	mfa-enabled-for-iam-Konsolenzugriff	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass MFA für alle AWS Identity and Access Management (IAM) -Benutzer aktiviert ist, die über ein Konsolenkennwort verfügen. MFA sorgt für eine weitere Schutzebene zusätzlich zu den Anmeldeinformationen. Indem Sie MFA für Benutzer vorschreiben, können Sie Fälle kompromittierter Konten reduzieren und verhindern, dass unbefugte Benutzer auf vertrauliche Daten zugreifen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-2	KONTENVERWALTUNG	redshift-cluster-configuration-check	Um Daten im Ruhezustand zu schützen, muss die Verschlüsselung für Ihre Amazon-Redshift-Cluster aktiviert sein. Sie müssen auch sicherstellen, dass die erforderlichen Konfigurationen auf Amazon-Redshift-Clustern bereitgestellt werden. Die Prüfungsprotokollierung muss aktiviert sein, um Informationen zu Verbindungen und Benutzeraktivitäten in der Datenbank bereitzustellen. Diese Regel erfordert, dass ein Wert für clusterDbEncrypted (Config Default: TRUE) und LoggingEnabled (Config Default: TRUE) gesetzt ist. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-2	KONTENVERWALTUNG	root-account-hardware-mfa-aktiviert	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Hardware-MFA für den Root-Benutzer aktiviert ist. Der Stammbenutzer ist der AWS-Konto-Benutzer mit den meisten Berechtigungen. MFA sorgt für eine weitere Schutzebene zusätzlich zu den Anmeldeinformationen. Indem Sie MFA für den Root-Benutzer vorschreiben, können Sie die Anzahl AWS-Konten kompromittierter Benutzer reduzieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-2	KONTENVERWALTUNG	root-account-mfa-enabled	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass MFA für den Root-Benutzer aktiviert ist. Der Stammbenutzer ist der AWS-Konto-Benutzer mit den meisten Berechtigungen. MFA sorgt für eine weitere Schutzebene zusätzlich zu den Anmeldeinformationen. Indem Sie MFA für den Root-Benutzer vorschreiben, können Sie die Anzahl AWS-Konten kompromittierter Benutzer reduzieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-2	KONTENVERWALTUNG	s-3 bucket-logging-enabled	Die Amazon Simple Storage Service (Amazon S3)-Serverzugriffsprotokollierung bietet eine Methode zur Überwachung des Netzwerks im Hinblick auf potenzielle Cybersicherheitsereignisse. Die Ereignisse werden überwacht, indem detaillierte Aufzeichnungen über die Anfragen erfasst werden, die an einen Amazon-S3-Bucket gestellt wurden. Jeder Zugriffsprotokolleintrag enthält Details zu einer einzelnen Zugriffsanfrage. Zu den Details gehören Anforderer, Bucket-Name, Anforderungszeit, Anforderungsaktion, Antwortstatus und Fehlercode, falls relevant.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-3	DURCHSETZUNG DES ZUGRIFFS	autoscaling-launch-config-public-ip-deaktiviert	Wenn Sie Ihre Netzwerkschnittstellen mit einer öffentlichen IP-Adresse konfigurieren, sind die diesen Netzwerkschnittstellen zugehörigen Ressourcen über das Internet erreichbar. EC2 Ressourcen sollten nicht öffentlich zugänglich sein, da dies einen unbeabsichtigten Zugriff auf Ihre Anwendungen oder Server ermöglichen kann.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-3	DURCHSETZUNG DES ZUGRIFFS	ec2-imdsv2-check	Stellen Sie sicher, dass die Methode Instance Metadata Service Version 2 (IMDSv2) aktiviert ist, um den Zugriff auf und die Kontrolle der Amazon Elastic Compute Cloud (Amazon EC2) - Instance-Metadate n zu schützen. Die IMDSv2 Methode verwendet sitzungsb asierte Kontrollen. Mit können Kontrolle n implementiert werden IMDSv2, um Änderungen an Instanzmetadaten einzuschränken.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-3	DURCHSETZUNG DES ZUGRIFFS	ec-2 instance-profile-attached	EC2 Instanzprofile übergeben eine IAM-Rolle an eine EC2 Instance. Das Anhängen eines Instance-Profils an Ihre Instances kann bei der Implementierung von geringsten Berechtigungen und der Berechtigungsverwaltung helfen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-3	DURCHSETZUNG DES ZUGRIFFS	ecs-task-definition-user-for-host-mode-check	Wenn für eine Aufgabendefinition erhöhte Berechtigungen gelten, liegt das daran, dass der Kunde diesen Konfigurationen ausdrücklich zugestimmt hat. Diese Kontrolle prüft, ob eine unerwartete Berechtigungseskalation vorliegt, wenn für eine Aufgabendefinition das Host-Netzwerk aktiviert ist, die Kunden aber keine erhöhten Berechtigungen aktiviert haben.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-3	DURCHSETZUNG DES ZUGRIFFS	iam-no-inline-policy-überprüfen	Stellen Sie sicher, dass ein Benutzer, eine IAM-Rolle oder eine IAM-Gruppe (AWS Identity and Access Management) nicht über eine Inline-Richtlinie zur Zugriffskontrolle auf Systeme und Ressourcen verfügt. AWS empfiehlt, verwaltete Richtlinien anstelle von Inline-Richtlinien zu verwenden. Verwaltete Richtlinien ermöglichen Wiederverwendbarkeit, Versionsverwaltung, Rollback und Delegierung der Berechtigungsverwaltung.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-3	DURCHSETZUNG DES ZUGRIFFS	iam-policy-no-statements-with-full-access	Stellen Sie sicher, dass IAM-Aktionen nur auf die benötigten Aktionen beschränkt sind. Wenn Benutzern mehr Rechte eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und der Aufgabentrennung verstoßen.
AC-3	DURCHSETZUNG DES ZUGRIFFS	ssm-document-not-public	Stellen Sie sicher, dass AWS Systems Manager (SSM) - Dokumente nicht öffentlich sind, da dies einen unbeabsichtigten Zugriff auf Ihre SSM-Dokumente ermöglichen kann. Ein öffentliches SSM-Dokument kann Informationen über Ihr Konto, Ihre Ressourcen und internen Prozesse preisgeben.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-3	DURCHSETZUNG DES ZUGRIFFS	dms-replication-not-public	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass auf DMS-Replikationsin stanzen nicht öffentlic h zugegriffen werden kann. DMS-Repli kations-Instances können vertrauli che Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.
AC-3	DURCHSETZUNG DES ZUGRIFFS	ebs-snapshot-public-restorable-überprüfen	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass EBS-Snapshots nicht öffentlich wiederher stellbar sind. EBS-Volume-Snapsho ts können vertrauli che Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-3	DURCHSETZUNG DES ZUGRIFFS	ec-2 instance-no-public-ip	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon Elastic Compute Cloud (Amazon EC2) - Instances nicht öffentlich zugänglich sind. EC2 Amazon-Instances können vertrauliche Informationen enthalten, und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-3	DURCHSETZUNG DES ZUGRIFFS	elasticsearch-in-vpc-only	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass sich Amazon OpenSearch OpenSearch Service (Service) - Domains innerhalb einer Amazon Virtual Private Cloud (Amazon VPC) befinden. Eine OpenSearch Service-Domain innerhalb einer Amazon VPC ermöglicht die sichere Kommunikation zwischen OpenSearch Service und anderen Services innerhalb der Amazon VPC, ohne dass ein Internet-Gateway, ein NAT-Gerät oder eine VPN-Verbindung erforderlich ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-3	DURCHSETZUNG DES ZUGRIFFS	emr-master-no-public-ip	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon EMR-Cluster-Masterknoten nicht öffentlich zugänglich sind. Amazon-EMR-Cluster-Hauptknoten können vertrauliche Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-3	DURCHSETZUNG DES ZUGRIFFS	iam-group-has-users-überprüfen	AWS Identity and Access Managemen t (IAM) kann Ihnen helfen, die Prinzipien der geringsten Rechte und der Aufgabent rennung mit Zugriffsb erechtigungen und Autorisierungen zu integrieren, indem sichergestellt wird, dass IAM-Gruppen mindestens einen Benutzer haben. Die Einteilung von Benutzern in Gruppen auf der Grundlage der ihnen zugewiese nen Berechtigungen oder ihrer Funktion ist eine Möglichkeit, das Prinzip der geringste n Berechtigung zu implementieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-3	DURCHSETZUNG DES ZUGRIFFS	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) kann Ihnen dabei helfen, die Prinzipien der geringsten Rechte und der Aufgabentrennung in Zugriffsberechtigungen und Autorisierungen zu integrieren und so zu verhindern, dass Richtlinien „Effect“: „Allow“ mit „Action“: „*“ anstelle von „Resource“: „*“ enthalten. Wenn Benutzern mehr Rechte eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und der Aufgabentrennung verstoßen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-3	DURCHSETZUNG DES ZUGRIFFS	iam-root-access-key-überprüfen	Der Zugriff auf Systeme und Ressourcen kann gesteuert werden, indem überprüft wird, ob der Root-Benutzer keine Zugriffsschlüssel mit seiner AWS Identity and Access Management (IAM) -Rolle verknüpft hat. Stellen Sie sicher, dass die Root-Zugriffsschlüssel gelöscht werden. Erstellen und verwenden Sie stattdessen rollenbasierte Funktionen, AWS-Konten um das Prinzip der geringsten Funktionalität zu berücksichtigen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-3	DURCHSETZUNG DES ZUGRIFFS	iam-user-group-membership-überprüfen	AWS Identity and Access Management (IAM) kann Ihnen helfen, Zugriffsberechtigungen und Autorisierungen einzuschränken, indem sichergestellt wird, dass Benutzer Mitglieder mindestens einer Gruppe sind. Wenn Benutzern mehr Berechtigungen eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und Aufgabentrennung verstoßen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-3	DURCHSETZUNG DES ZUGRIFFS	iam-user-no-policies-überprüfen	Diese Regel stellt sicher, dass AWS Identity and Access Management (IAM) -Richtlinien nur Gruppen oder Rollen zugewiese n werden, um den Zugriff auf Systeme und Ressourcen zu kontrollieren. Die Zuweisung von Berechtig ungen auf Gruppen- oder Rollenebene trägt dazu bei, die Wahrscheinlichkeit zu verringern, dass eine Identität übermäßige Berechtigungen erhält oder beibehält.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-3	DURCHSETZUNG DES ZUGRIFFS	iam-user-unused-credentials-überprüfen	AWS Identity and Access Management (IAM) kann Ihnen bei Zugriffsberechtigungen und Autorisierungen helfen, indem es nach IAM-Passwörtern und Zugriffsschlüsseln sucht, die für einen bestimmten Zeitraum nicht verwendet wurden. Wenn ungenutzte Anmeldeinformationen identifiziert werden, müssen Sie sie deaktivieren und/oder entfernen, da dies gegen das Prinzip der geringsten Berechtigung verstoßen könnte. Für diese Regel müssen Sie einen Wert für das maxCredentialUsage Alter festlegen (Standardkonfiguration: 90). Der tatsächliche Wert muss den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-3	DURCHSETZUNG DES ZUGRIFFS	lambda-function-public-access-verboten	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass AWS Lambda-Funktionen nicht öffentlich zugänglich sind. Der öffentliche Zugriff kann möglicherweise die Verfügbarkeit von Ressourcen beeinträchtigen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-3	DURCHSETZUNG DES ZUGRIFFS	lambda-inside-vpc	Stellen Sie AWS Lambda-Funktionen in einer Amazon Virtual Private Cloud (Amazon VPC) bereit, um eine sichere Kommunika tion zwischen einer Funktion und anderen Diensten innerhalb der Amazon VPC zu gewährleisten. Bei dieser Konfiguration sind kein Internet-Gateway, kein NAT-Gerät und keine VPN-Verbindung erforderlich. Der gesamte Datenverk ehr bleibt sicher in der Cloud. AWS Domains, die sich innerhalb einer VPC befinden, verfügen aufgrund ihrer logischen Isolierun g im Vergleich zu Domains mit öffentlic hen Endpunkten über eine zusätzliche Sicherheitsebene. Um den Zugriff ordnungsg emäß zu verwalten,

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			sollten AWS Lambda-Funktionen einer VPC zugewiesen werden.
AC-3	DURCHSETZUNG DES ZUGRIFFS	opensearch-in-vpc-only	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass sich Amazon OpenSearch Service-Domains innerhalb einer Amazon Virtual Private Cloud (Amazon VPC) befinden. Eine Amazon OpenSearch Service-Domain innerhalb einer Amazon VPC ermöglicht die sichere Kommunikation zwischen Amazon OpenSearch Service und anderen Services innerhalb der Amazon VPC, ohne dass ein Internet-Gateway, ein NAT-Gerät oder eine VPN-Verbindung erforderlich ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-3	DURCHSETZUNG DES ZUGRIFFS	rds-instance-public-access-überprüfen	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Relational Database Service (Amazon RDS) -Instances nicht öffentlich sind. Amazon-RDS-Datenbank-Instances können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-3	DURCHSETZUNG DES ZUGRIFFS	rds-snapshots-public-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Relational Database Service (Amazon RDS) -Instances nicht öffentlich sind. Amazon-RDS-Datenbank-Instances können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-3	DURCHSETZUNG DES ZUGRIFFS	redshift-cluster-public-access-überprüfen	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Redshift Redshift-Cluster nicht öffentlich sind. Amazon-Redshift-Cluster können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-3	DURCHSETZUNG DES ZUGRIFFS	s3- -Block-periodisch account-level-public-access	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Simple Storage Service (Amazon S3) -Buckets nicht öffentlich zugänglich sind. Diese Regel trägt dazu bei, sensible Daten vor unbefugten Remote-Benutzern zu schützen, indem sie den öffentlichen Zugriff verhindert. Mit dieser Regel können Sie optional die Parameter ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) und restrictPublicBuckets Parameter (Config Default: True) festlegen. Die tatsächlichen Werte müssen den Richtlini

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			en Ihrer Organisation entsprechen.
AC-3	DURCHSETZUNG DES ZUGRIFFS	s3 bucket-level-public-access - verboten	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Simple Storage Service (Amazon S3) -Buckets nicht öffentlich zugänglich sind. Diese Regel trägt dazu bei, sensible Daten vor unbefugten Remote-Benutzern zu schützen, indem sie den öffentlichen Zugriff auf Bucket-Ebene verhindert.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-3	DURCHSETZUNG DES ZUGRIFFS	s3- bucket-public-read -prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie nur autorisierten Benutzern, Prozessen und Geräten Zugriff auf Amazon Simple Storage Service (Amazon S3) - Buckets gewähren. Die Verwaltung des Zugriffs sollte mit der Klassifizierung der Daten übereinst immen.
AC-3	DURCHSETZUNG DES ZUGRIFFS	s3- bucket-public-writ e-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie nur autorisierten Benutzern, Prozessen und Geräten Zugriff auf Amazon Simple Storage Service (Amazon S3) - Buckets gewähren. Die Verwaltung des Zugriffs sollte mit der Klassifizierung der Daten übereinst immen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-3	DURCHSETZUNG DES ZUGRIFFS	sagemaker-notebook-no-direct-Internetzugang	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass SageMaker Amazon-Notebooks keinen direkten Internetzugang zulassen. Indem Sie direkten Internetzugang blockieren, vermeiden Sie, dass unbefugte Benutzer auf sensible Daten zugreifen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-3	DURCHSETZUNG DES ZUGRIFFS	subnet-auto-assign-public-ip-deaktiviert	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon Virtual Private Cloud (VPC) -Subnetzen nicht automatisch eine öffentliche IP-Adresse zugewiesen wird. Amazon Elastic Compute Cloud (EC2) -Instances, die in Subnetzen gestartet werden, in denen dieses Attribut aktiviert ist, haben ihrer primären Netzwerkschnittstelle eine öffentliche IP-Adresse zugewiesen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-17	REMOTE-ZUGRIFF	elb-tls-https-listeners-nur	Stellen Sie sicher, dass Ihre Elastic Load Balancer (ELBs) mit SSL- oder HTTPS-Listenern konfiguriert sind. Um eventuell vorhanden e sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-17	REMOTE-ZUGRIFF	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) Security Groups können bei der Verwaltung des Netzwerkzugriffs helfen, indem sie eine statusbehaftete Filterung des ein- und ausgehenden Netzwerkverkehrs zu Ressourcen bereitstellen. AWS Wenn Sie eingehenden (oder entfernten) Datenverkehr von 0.0.0.0/0 bis Port 22 auf Ihren Ressourcen nicht zulassen, können Sie den Remote-Zugriff einschränken.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-17	REMOTE-ZUGRIFF	ec-2 instances-in-vpc	Stellen Sie Amazon Elastic Compute Cloud (Amazon EC2) -Instances innerhalb einer Amazon Virtual Private Cloud (Amazon VPC) bereit, um eine sichere Kommunika tion zwischen einer Instance und anderen Services innerhalb der Amazon VPC zu ermöglichen, ohne dass ein Internet-Gateway, ein NAT-Gerät oder eine VPN-Verbindung erforderlich ist. Der gesamte Datenverk ehr bleibt sicher in der AWS Cloud. Domains, die sich innerhalb einer VPC befinden, verfügen aufgrund ihrer logischen Isolierun g im Vergleich zu Domains mit öffentlic hen Endpunkten über eine zusätzlic he Sicherheitsebene. Weisen Sie EC2

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			Amazon-Instances einer Amazon-VPC zu, um den Zugriff ordnungsgemäß zu verwalten.
AC-17	REMOTE-ZUGRIFF	securityhub-enabled	AWS Security Hub hilft bei der Überwachung von unbefugtem Personal, Verbindungen, Geräten und Software. AWS Security Hub aggregiert, organisiert und priorisiert die Sicherheitswarnungen oder Ergebnisse mehrerer Dienste. AWS Einige dieser Dienste sind Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer und AWS Firewall Manager sowie AWS Partnerlösungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-17	REMOTE-ZUGRIFF	acm-certificate-expiration-check	Stellen Sie sicher, dass die Netzwerkintegrität geschützt ist, indem Sie sicherstellen, dass X509-Zertifikate von ACM ausgestellt werden. AWS Diese Zertifikate müssen gültig und dürfen nicht abgelaufen sein. Für diese Regel ist ein Wert für erforderlich daysToExpiration (Wert für bewährte AWS Grundregeln für Sicherheit: 90). Der tatsächliche Wert muss den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-17	REMOTE-ZUGRIFF	alb-http-to-https-Umleitungsprüfung	Um Daten während der Übertragung zu schützen, stellen Sie sicher, dass Ihr Application Load Balancer unverschlüsselte HTTP-Anfragen automatisch an HTTPS umleitet. Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.
AC-17	REMOTE-ZUGRIFF	dms-replication-not-public	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass auf DMS-Replikationsinstanzen nicht öffentlich zugegriffen werden kann. DMS-Replikations-Instances können vertrauliche Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-17	REMOTE-ZUGRIFF	ebs-snapshot-public-restorable-überprüfen	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass EBS-Snapshots nicht öffentlich wiederher stellbar sind. EBS-Volume-Snapsho ts können vertrauli che Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.
AC-17	REMOTE-ZUGRIFF	ec-2 instance-no-public-ip	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon Elastic Compute Cloud (Amazon EC2) - Instances nicht öffentlich zugänglich sind. EC2 Amazon-Instances können vertrauliche Informati onen enthalten, und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-17	REMOTE-ZUGRIFF	elasticsearch-in-vpc-only	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass sich Amazon OpenSearch OpenSearch Service (Service) - Domains innerhalb einer Amazon Virtual Private Cloud (Amazon VPC) befinden. Eine OpenSearch Service-Domain innerhalb einer Amazon VPC ermöglicht die sichere Kommunikation zwischen OpenSearch Service und anderen Services innerhalb der Amazon VPC, ohne dass ein Internet-Gateway, ein NAT-Gerät oder eine VPN-Verbindung erforderlich ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-17	REMOTE-ZUGRIFF	emr-master-no-public-ip	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon EMR-Cluster-Masterknoten nicht öffentlich zugänglich sind. Amazon-EMR-Cluster-Hauptknoten können vertrauliche Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-17	REMOTE-ZUGRIFF	guardduty-enabled-centralized	Amazon GuardDuty kann mithilfe von Threat Intellige nce Feeds helfen, potenzielle Cybersich erheitsereignisse zu überwachen und zu erkennen. Dazu gehören Listen mit bösartigen IPs und maschinel len Lernmethoden zur Identifizierung unerwarteter, nicht autorisierter und bösartiger Aktivitäten in Ihrer AWS Cloud-Umgebung.
AC-17	REMOTE-ZUGRIFF	lambda-function-public-access-verboten	Verwalten Sie den Zugriff auf Ressource n in der AWS Cloud, indem Sie sicherste llen, dass AWS Lambda-Funktionen nicht öffentlich zugänglich sind. Der öffentliche Zugriff kann möglicherweise die Verfügbarkeit von Ressourcen beeinträc htigen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-17	REMOTE-ZUGRIFF	lambda-inside-vpc	Stellen Sie AWS Lambda-Funktionen in einer Amazon Virtual Private Cloud (Amazon VPC) bereit, um eine sichere Kommunika tion zwischen einer Funktion und anderen Diensten innerhalb der Amazon VPC zu gewährleisten. Bei dieser Konfiguration sind kein Internet-Gateway, kein NAT-Gerät und keine VPN-Verbindung erforderlich. Der gesamte Datenverk ehr bleibt sicher in der Cloud. AWS Domains, die sich innerhalb einer VPC befinden, verfügen aufgrund ihrer logischen Isolierun g im Vergleich zu Domains mit öffentlic hen Endpunkten über eine zusätzliche Sicherheitsebene. Um den Zugriff ordnungsg emäß zu verwalten,

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			sollten AWS Lambda-Funktionen einer VPC zugewiesen werden.
AC-17	REMOTE-ZUGRIFF	opensearch-in-vpc-only	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass sich Amazon OpenSearch Service-Domains innerhalb einer Amazon Virtual Private Cloud (Amazon VPC) befinden. Eine Amazon OpenSearch Service-Domain innerhalb einer Amazon VPC ermöglicht die sichere Kommunikation zwischen Amazon OpenSearch Service und anderen Services innerhalb der Amazon VPC, ohne dass ein Internet-Gateway, ein NAT-Gerät oder eine VPN-Verbindung erforderlich ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-17	REMOTE-ZUGRIFF	rds-instance-public-access-überprüfen	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Relational Database Service (Amazon RDS) -Instances nicht öffentlich sind. Amazon-RDS-Datenbank-Instances können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-17	REMOTE-ZUGRIFF	rds-snapshots-public-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Relational Database Service (Amazon RDS) -Instances nicht öffentlich sind. Amazon-RDS-Datenbank-Instances können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-17	REMOTE-ZUGRIFF	redshift-cluster-public-access-überprüfen	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Redshift Redshift-Cluster nicht öffentlich sind. Amazon-Redshift-Cluster können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.
AC-17	REMOTE-ZUGRIFF	redshift-require-tls-ssl	Stellen Sie sicher, dass Ihre Amazon-Redshift-Cluster eine TLS/SSL-Verschlüsselung erfordern, um eine Verbindung zu SQL-Clients herzustellen. Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-17	REMOTE-ZUGRIFF	restricted-common-ports	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass gemeinsame Ports für Amazon Elastic Compute Cloud (Amazon EC2) -Sicherheitsgruppen eingeschränkt sind. Wenn der Zugriff auf Ports nicht auf vertrauenswürdige Quellen beschränkt wird, kann dies zu Angriffen auf die Verfügbarkeit, Integrität und Vertraulichkeit von Systemen führen. Mit dieser Regel können Sie optional die Parameter blockedPort1–blockedPort5 festlegen (Standardkonfigurationen: 20, 21, 3389, 3306, 4333). Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-17	REMOTE-ZUGRIFF	s3- account-level-public-access -Block-periodisch	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Simple Storage Service (Amazon S3) -Buckets nicht öffentlich zugänglich sind. Diese Regel trägt dazu bei, sensible Daten vor unbefugten Remote-Benutzern zu schützen, indem sie den öffentlichen Zugriff verhindert. Mit dieser Regel können Sie optional die Parameter ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) und restrictPublicBuckets Parameter (Config Default: True) festlegen. Die tatsächlichen Werte müssen den Richtlini

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			en Ihrer Organisation entsprechen.
AC-17	REMOTE-ZUGRIFF	s3 bucket-level-public-access - verboten	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Simple Storage Service (Amazon S3) -Buckets nicht öffentlich zugänglich sind. Diese Regel trägt dazu bei, sensible Daten vor unbefugten Remote-Benutzern zu schützen, indem sie den öffentlichen Zugriff auf Bucket-Ebene verhindert.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-17	REMOTE-ZUGRIFF	s3- bucket-public-read -prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie nur autorisierten Benutzern, Prozessen und Geräten Zugriff auf Amazon Simple Storage Service (Amazon S3) - Buckets gewähren. Die Verwaltung des Zugriffs sollte mit der Klassifizierung der Daten übereinst immen.
AC-17	REMOTE-ZUGRIFF	s3- bucket-public-writ e-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie nur autorisierten Benutzern, Prozessen und Geräten Zugriff auf Amazon Simple Storage Service (Amazon S3) - Buckets gewähren. Die Verwaltung des Zugriffs sollte mit der Klassifizierung der Daten übereinst immen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-17	REMOTE-ZUGRIFF	s3- bucket-ssl-requests-only	Um Daten während der Übertragung zu schützen, stellen Sie sicher, dass Ihre Amazon Simple Storage Service (Amazon S3)-Buckets Anfragen zur Verwendung von Secure Socket Layer (SSL)-Buckets erfordern. Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-17	REMOTE-ZUGRIFF	sagemaker-notebook-no-direct-Internetzugang	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass SageMaker Amazon-Notebooks keinen direkten Internetzugang zulassen. Indem Sie direkten Internetzugang blockieren, vermeiden Sie, dass unbefugte Benutzer auf sensible Daten zugreifen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-17	REMOTE-ZUGRIFF	subnet-auto-assign-public-ip-deaktiviert	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon Virtual Private Cloud (VPC) -Subnetzen nicht automatisch eine öffentliche IP-Adresse zugewiesen wird. Amazon Elastic Compute Cloud (EC2) -Instances, die in Subnetzen gestartet werden, in denen dieses Attribut aktiviert ist, haben ihrer primären Netzwerkschnittstelle eine öffentliche IP-Adresse zugewiesen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-17	REMOTE-ZUGRIFF	vpc-default-security-group-geschlossen	Sicherheitsgruppen von Amazon Elastic Compute Cloud (Amazon EC2) können bei der Verwaltung des Netzwerkzugriffs helfen, indem sie eine statusbehaftete Filterung des ein- und ausgehenden Netzwerkverkehrs zu Ressourcen bereitstellen. AWS Die Beschränk ung des gesamten Datenverkehrs auf die Standardsicherheit sgruppe hilft dabei, den Fernzugriff auf Ihre Ressourcen einzuschränken. AWS

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-17	REMOTE-ZUGRIFF	vpc-sg-open-only-to-authorized-ports	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass gemeinsame Ports für Amazon Elastic Compute Cloud (Amazon EC2) -Sicherheitsgruppen eingeschränkt sind. Wenn der Zugriff auf Ports nicht auf vertrauenswürdige Quellen beschränkt wird, kann dies zu Angriffen auf die Verfügbarkeit, Integrität und Vertraulichkeit von Systemen führen. Durch die Beschränkung des Zugriffs auf Ressourcen innerhalb einer Sicherheitsgruppe aus dem Internet (0.0.0.0/0) kann der Remote-Zugriff auf interne Systeme gesteuert werden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AU-2	PRÜFUNGSE REIGNISSE	codebuild-project-logging-enabled	Stellen Sie sicher, dass die AWS CodeBuild Projektprotokollierung aktiviert ist, damit Ihre Build-Ausgabeprotokolle entweder an Amazon CloudWatch oder Amazon Simple Storage Service (Amazon S3) gesendet werden. Build-Ausgabeprotokolle enthalten detaillierte Informationen zu Ihrem Build-Projekt.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AU-2	PRÜFUNGSE REIGNISSE	multi-region-cloudtrail-enabled	AWS CloudTrail zeichnet Aktionen und API-Aufrufe der AWS Management Console auf. Sie können feststellen, welche Benutzer und Konten angerufen wurden AWS, von welcher Quell-IP-Adresse aus die Anrufe getätigt wurden und wann die Anrufe erfolgten. CloudTrail übermittelt Protokolldateien aus allen AWS Regionen an Ihren S3-Bucket , wenn MULTI_REG ION_CLOUD _TRAIL_ENABLED aktiviert ist. Außerdem wird beim AWS Start einer neuen Region derselbe Trail in der neuen Region erstellt. CloudTrail Dadurch erhalten Sie automatis ch Protokolldateien mit API-Aktivitäten für die neue Region.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AU-2	PRÜFUNGSE REIGNISSE	rds-logging-enabled	Um die Protokoll ierung und Überwachung in Ihrer Umgebung zu erleichtern, stellen Sie sicher, dass die Amazon Relationa l Database Service (Amazon RDS)-Prot okollierung aktiviert ist. Mit der Amazon-RDS-Protokollierung können Sie Ereigniss e wie Verbindungen, Verbindungsabbrüch e, Abfragen oder abgefragte Tabellen erfassen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AU-2	PRÜFUNGSEREIGNISSE	wafv2-logging-enabled	Um die Protokollierung und Überwachung in Ihrer Umgebung zu erleichtern, aktivieren Sie die AWS WAF (V2) -Protokollierung im regionalen und globalen Web ACLs. AWS Die WAF-Protokollierung bietet detaillierte Informationen über den Datenverkehr, der von Ihrer Web-ACL analysiert wird. In den Protokollen werden die Uhrzeit aufgezeichnet, zu der die AWS WAF die Anfrage von Ihrer AWS Ressource erhalten hat, Informationen über die Anfrage und eine Aktion für die Regel, der jede Anfrage entsprach.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AU-2	PRÜFUNGSE REIGNISSE	api-gw-execution-logging-aktiviert	Die API-Gateway-Protokollierung zeigt detaillierte Ansichten der Benutzer, die auf die API zugegriff en haben, und wie diese Benutzer auf die API zugegriff en haben. Diese Einblicke ermöglichen die Transparenz von Benutzeraktivitäten.
AU-2	PRÜFUNGSE REIGNISSE	cloud-trail-cloud-watch-logs-aktiviert	Verwenden Sie Amazon CloudWatc h , um Protokoll ereignisaktivitäten zentral zu sammeln und zu verwalten. Die Aufnahme von AWS CloudTrail Daten liefert Einzelheiten zu den API-Aufrufaktivitä ten in Ihrem AWS-Konto.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AU-2	PRÜFUNGSE REIGNISSE	cloudtrail-enabled	AWS CloudTrail kann bei der Nichtabst reitbarkeit helfen, indem Aktionen und API-Aufrufe der AWS Management Console aufgezeic hnet werden. Sie können die Benutzer und die Benutzer AWS-Konten , die einen AWS Dienst aufgerufen haben, die Quell-IP-Adresse, über die die Aufrufe generiert wurden, und den Zeitpunkt der Anrufe identifiz ieren. Einzelheiten zu den erfassten Daten finden Sie unter Inhalt des AWS CloudTrail Datensatzes.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AU-2	PRÜFUNGSE REIGNISSE	cloudtrail-s3-data events-enabled	Die Erfassung von Simple Storage Service (Amazon S3)-Datenereigniss en unterstützt die Erkennung von ungewöhnlichen Aktivitäten. Zu den Details gehören AWS-Konto Informationen über den Zugriff auf einen Amazon S3 S3-Bucket, die IP-Adress e und die Uhrzeit des Ereignisses.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AU-2	PRÜFUNGSE REIGNISSE	elb-logging-enabled	Die Elastic-Load-Balancing-Aktivität ist ein zentraler Kommunikationspunk t innerhalb einer Umgebung. Stellen Sie sicher, dass die ELB-Protokollierun g aktiviert ist. Die gesammelten Daten enthalten detaillie rte Informationen zu Anfragen, die an den ELB gesendet wurden. Jedes Protokoll enthält Informationen wie die Zeit, zu der die Anforderung einging, die Client-IP -Adresse, Latenzen, Anforderungspfade und Serverantworten.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AU-2	PRÜFUNGSEREIGNISSE	redshift-cluster-configuration-check	Um Daten im Ruhezustand zu schützen, muss die Verschlüsselung für Ihre Amazon-Redshift-Cluster aktiviert sein. Sie müssen auch sicherstellen, dass die erforderlichen Konfigurationen auf Amazon-Redshift-Clustern bereitgestellt werden. Die Prüfungsprotokollierung muss aktiviert sein, um Informationen zu Verbindungen und Benutzeraktivitäten in der Datenbank bereitzustellen. Diese Regel erfordert, dass ein Wert für clusterDbEncrypted (Config Default: TRUE) und LoggingEnabled (Config Default: TRUE) gesetzt ist. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AU-2	PRÜFUNGSE REIGNISSE	s3- bucket-logging-enabled	Die Amazon Simple Storage Service (Amazon S3)-Serverzugriffs protokollierung bietet eine Methode zur Überwachu ng des Netzwerks im Hinblick auf potenzielle Cybersich erheitsereignisse. Die Ereignisse werden überwacht, indem detaillierte Aufzeichn ungen über die Anfragen erfasst werden, die an einen Amazon-S3-Bucket gestellt wurden. Jeder Zugriffsprotokolle intrag enthält Details zu einer einzelnen Zugriffsanfrage. Zu den Details gehören Anforderer, Bucket-Name, Anforderu ngszeit, Anforderu ngsaktion, Antwortst atus und Fehlercode, falls relevant.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AU-2	PRÜFUNGSE REIGNISSE	vpc-flow-logs-enabled	VPC-Flow-Protokolle erfassen detaillierte Informationsdatensätze über den IP-Datenverkehr, der zu und von Netzwerkschnittstellen in Ihrer Amazon Virtual Private Cloud (Amazon VPC) fließt. Standardmäßig enthalten Flow-Protokolldatensätze Werte für die verschiedenen Komponenten des IP-Flows, einschließlich Quelle, Ziel und Protokoll.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AU-3	INHALT DER PRÜFUNGSUNTERLAGEN	codebuild-project-logging-enabled	Stellen Sie sicher, dass die AWS CodeBuild Projektprotokollierung aktiviert ist, damit Ihre Build-Ausgabeprotokolle entweder an Amazon CloudWatch oder Amazon Simple Storage Service (Amazon S3) gesendet werden. Build-Ausgabeprotokolle enthalten detaillierte Informationen zu Ihrem Build-Projekt.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AU-3	INHALT DER PRÜFUNGSUNTERLAGEN	multi-region-cloudtrail-enabled	AWS CloudTrail zeichnet Aktionen und API-Aufrufe der AWS Management Console auf. Sie können feststellen, welche Benutzer und Konten angerufen wurden AWS, von welcher Quell-IP-Adresse aus die Anrufe getätigt wurden und wann die Anrufe erfolgten. CloudTrail übermittelt Protokolldateien aus allen AWS Regionen an Ihren S3-Bucket , wenn MULTI_REGION_CLOUD_TRAIL_ENABLED aktiviert ist. Außerdem wird beim AWS Start einer neuen Region derselbe Trail in der neuen Region erstellt. CloudTrail Dadurch erhalten Sie automatisch Protokolldateien mit API-Aktivitäten für die neue Region.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AU-3	INHALT DER PRÜFUNGSUNTERLAGEN	rds-logging-enabled	Um die Protokollierung und Überwachung in Ihrer Umgebung zu erleichtern, stellen Sie sicher, dass die Amazon Relational Database Service (Amazon RDS)-Protokollierung aktiviert ist. Mit der Amazon-RDS-Protokollierung können Sie Ereignisse wie Verbindungen, Verbindungsabbrüche, Abfragen oder abgefragte Tabellen erfassen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AU-3	INHALT DER PRÜFUNGSUNTERLAGEN	wafv2-logging-enabled	Um die Protokollierung und Überwachung in Ihrer Umgebung zu erleichtern, aktivieren Sie die AWS WAF (V2) -Protokollierung im regionalen und globalen Web ACLs. AWS Die WAF-Protokollierung bietet detaillierte Informationen über den Datenverkehr, der von Ihrer Web-ACL analysiert wird. In den Protokollen werden die Uhrzeit aufgezeichnet, zu der die AWS WAF die Anfrage von Ihrer AWS Ressource erhalten hat, Informationen über die Anfrage und eine Aktion für die Regel, der jede Anfrage entsprach.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AU-3	INHALT DER PRÜFUNGSUNTERLAGEN	api-gw-execution-logging-aktiviert	Die API-Gateway-Protokollierung zeigt detaillierte Ansichten der Benutzer, die auf die API zugegriffen haben, und wie diese Benutzer auf die API zugegriffen haben. Diese Einblicke ermöglichen die Transparenz von Benutzeraktivitäten.
AU-3	INHALT DER PRÜFUNGSUNTERLAGEN	cloud-trail-cloud-watch-logs-aktiviert	Verwenden Sie Amazon CloudWatch , um Protokoll ereignisaktivitäten zentral zu sammeln und zu verwalten. Die Aufnahme von AWS CloudTrail Daten liefert Einzelheiten zu den API-Aufrufaktivitäten in Ihrem AWS-Konto.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AU-3	INHALT DER PRÜFUNGSUNTERLAGEN	cloudtrail-enabled	AWS CloudTrail kann bei der Nichtabstreitbarkeit helfen, indem Aktionen und API-Aufrufe der AWS Management Console aufgezeichnet werden. Sie können die Benutzer und die Benutzer AWS-Konten , die einen AWS Dienst aufgerufen haben, die Quell-IP-Adresse, über die die Aufrufe generiert wurden, und den Zeitpunkt der Anrufe identifizieren. Einzelheiten zu den erfassten Daten finden Sie unter Inhalt des AWS CloudTrail Datensatzes.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AU-3	INHALT DER PRÜFUNGSUNTERLAGEN	cloudtrail-s3-dataevents-enabled	Die Erfassung von Simple Storage Service (Amazon S3)-Datenereignissen unterstützt die Erkennung von ungewöhnlichen Aktivitäten. Zu den Details gehören AWS-Konto Informationen über den Zugriff auf einen Amazon S3 S3-Bucket, die IP-Adresse und die Uhrzeit des Ereignisses.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AU-3	INHALT DER PRÜFUNGSUNTERLAGEN	elb-logging-enabled	Die Elastic-Load-Balancing-Aktivität ist ein zentraler Kommunikationspunkt innerhalb einer Umgebung. Stellen Sie sicher, dass die ELB-Protokollierung aktiviert ist. Die gesammelten Daten enthalten detaillierte Informationen zu Anfragen, die an den ELB gesendet wurden. Jedes Protokoll enthält Informationen wie die Zeit, zu der die Anforderung einging, die Client-IP-Adresse, Latenzen, Anforderungspfade und Serverantworten.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AU-3	INHALT DER PRÜFUNGSUNTERLAGEN	redshift-cluster-configuration-check	Um Daten im Ruhezustand zu schützen, muss die Verschlüsselung für Ihre Amazon-Redshift-Cluster aktiviert sein. Sie müssen auch sicherstellen, dass die erforderlichen Konfigurationen auf Amazon-Redshift-Clustern bereitgestellt werden. Die Prüfungsprotokollierung muss aktiviert sein, um Informationen zu Verbindungen und Benutzeraktivitäten in der Datenbank bereitzustellen. Diese Regel erfordert, dass ein Wert für clusterDbEncrypted (Config Default: TRUE) und LoggingEnabled (Config Default: TRUE) gesetzt ist. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AU-3	INHALT DER PRÜFUNGSUNTERLAGEN	s3- bucket-logging-enabled	Die Amazon Simple Storage Service (Amazon S3)-Serverzugriffsprotokollierung bietet eine Methode zur Überwachung des Netzwerks im Hinblick auf potenzielle Cybersicherheitsereignisse. Die Ereignisse werden überwacht, indem detaillierte Aufzeichnungen über die Anfragen erfasst werden, die an einen Amazon-S3-Bucket gestellt wurden. Jeder Zugriffsprotokolleintrag enthält Details zu einer einzelnen Zugriffsanfrage. Zu den Details gehören Anforderer, Bucket-Name, Anforderungszeit, Anforderungsaktion, Antwortstatus und Fehlercode, falls relevant.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AU-3	INHALT DER PRÜFUNGSUNTERLAGEN	vpc-flow-logs-enabled	VPC-Flow-Protokolle erfassen detaillierte Informationsdatensätze über den IP-Datenverkehr, der zu und von Netzwerkschnittstellen in Ihrer Amazon Virtual Private Cloud (Amazon VPC) fließt. Standardmäßig enthalten Flow-Protokolldatensätze Werte für die verschiedenen Komponenten des IP-Flows, einschließlich Quelle, Ziel und Protokoll.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AU-6	PRÜFUNG, ANALYSE UND BERICHTER STATTUNG	codebuild-project-logging-enabled	Stellen Sie sicher, dass die AWS CodeBuild Projektprotokollierung aktiviert ist, damit Ihre Build-Ausgabeprotokolle entweder an Amazon CloudWatch oder Amazon Simple Storage Service (Amazon S3) gesendet werden. Build-Ausgabeprotokolle enthalten detaillierte Informationen zu Ihrem Build-Projekt.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AU-6	PRÜFUNG, ANALYSE UND BERICHTER STATTUNG	cw-loggroup-retent ion-period-überprüfen	Stellen Sie sicher, dass die Ereignisp rotokolldaten für Ihre Protokollgruppen über eine Mindestdauer aufbewahrt werden, um die Fehlerbeh ebung und forensisc he Untersuchungen zu unterstützen. Fehlende frühere Ereignisprotokolld aten erschweren die Rekonstruierung und Identifizierung potenziell schädlicher Ereignisse.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AU-6	PRÜFUNG, ANALYSE UND BERICHTER STATTUNG	multi-region-cloudtrail-enabled	AWS CloudTrail zeichnet Aktionen und API-Aufrufe der AWS Management Console auf. Sie können feststellen, welche Benutzer und Konten angerufen wurden AWS, von welcher Quell-IP-Adresse aus die Anrufe getätigt wurden und wann die Anrufe erfolgten. CloudTrail übermittelt Protokolldateien aus allen AWS Regionen an Ihren S3-Bucket , wenn MULTI_REG ION_CLOUD _TRAIL_ENABLED aktiviert ist. Außerdem wird beim AWS Start einer neuen Region derselbe Trail in der neuen Region erstellt. CloudTrail Dadurch erhalten Sie automatis ch Protokolldateien mit API-Aktivitäten für die neue Region.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AU-6	PRÜFUNG, ANALYSE UND BERICHTER STATTUNG	securityhub-enabled	AWS Security Hub hilft bei der Überwachung von unbefugtem Personal, Verbindun gen, Geräten und Software. AWS Security Hub aggregiert, organisie rt und priorisie rt die Sicherhei tswarnungen oder Ergebnisse mehrerer Dienste. AWS Einige dieser Dienste sind Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer und AWS Firewall Manager sowie AWS Partnerlösungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AU-6	PRÜFUNG, ANALYSE UND BERICHTER STATTUNG	wafv2-logging-enabled	Um Ihnen bei der Protokollierung und Überwachung in Ihrer Umgebung zu helfen, aktivieren Sie die AWS WAF (V2) -Protokollierung im regionalen und globalen Web. ACLs AWS Die WAF-Protokollierung bietet detaillierte Informationen über den Datenverkehr, der von Ihrer Web-ACL analysiert wird. In den Protokollen werden die Uhrzeit aufgezeichnet, zu der die AWS WAF die Anfrage von Ihrer AWS Ressource erhalten hat, Informationen über die Anfrage und eine Aktion für die Regel, der jede Anfrage entsprach.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AU-6	PRÜFUNG, ANALYSE UND BERICHTER STATTUNG	api-gw-execution-logging-aktiviert	Die API-Gateway-Protokollierung zeigt detaillierte Ansichten der Benutzer, die auf die API zugegriff en haben, und wie diese Benutzer auf die API zugegriff en haben. Diese Einblicke ermöglichen die Transparenz von Benutzeraktivitäten.
AU-6	PRÜFUNG, ANALYSE UND BERICHTER STATTUNG	cloud-trail-cloud-watch-logs-aktiviert	Verwenden Sie Amazon CloudWatc h , um Protokoll ereignisaktivitäten zentral zu sammeln und zu verwalten. Die Aufnahme von AWS CloudTrail Daten liefert Einzelheiten zu den API-Aufrufaktivitä ten in Ihrem AWS-Konto.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AU-6	PRÜFUNG, ANALYSE UND BERICHTER STATTUNG	cloudtrail-enabled	AWS CloudTrail kann bei der Nichtabst reitbarkeit helfen, indem Aktionen und API-Aufrufe der AWS Management Console aufgezeic hnet werden. Sie können die Benutzer und die Benutzer AWS-Konten , die einen AWS Dienst aufgerufen haben, die Quell-IP-Adresse, über die die Aufrufe generiert wurden, und den Zeitpunkt der Anrufe identifiz ieren. Einzelheiten zu den erfassten Daten finden Sie unter Inhalt des AWS CloudTrail Datensatzes.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AU-6	PRÜFUNG, ANALYSE UND BERICHTER STATTUNG	cloudtrail-s3-data events-enabled	Die Erfassung von Simple Storage Service (Amazon S3)-Datenereigniss en unterstützt die Erkennung von ungewöhnlichen Aktivitäten. Zu den Details gehören AWS-Konto Informationen über den Zugriff auf einen Amazon S3 S3-Bucket, die IP-Adress e und die Uhrzeit des Ereignisses.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AU-6	PRÜFUNG, ANALYSE UND BERICHTER STATTUNG	cloudwatch-alarm-action-check	Amazon CloudWatch alarmiert, wenn eine Metrik den Schwellenwert für eine bestimmte Anzahl von Bewertungszeiträumen überschreitet. Der Alarm führt eine oder mehrere Aktionen durch, die vom Wert der Metrik oder des Ausdrucks im Vergleich zu einem Schwellenwert in einer Reihe von Zeiträumen abhängt. Diese Regel erfordert einen Wert für alarmActionRequired (Config Default: True), insufficientDataAction Required (Config Default: True), okActionRequired (Config Default: False). Der tatsächliche Wert muss die Alarmaktionen für Ihre Umgebung widerspiegeln.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AU-6	PRÜFUNG, ANALYSE UND BERICHTER STATTUNG	elb-logging-enabled	Die Elastic-Load-Balancing-Aktivität ist ein zentraler Kommunikationspunkt innerhalb einer Umgebung. Stellen Sie sicher, dass die ELB-Protokollierung aktiviert ist. Die gesammelten Daten enthalten detaillierte Informationen zu Anfragen, die an den ELB gesendet wurden. Jedes Protokoll enthält Informationen wie die Zeit, zu der die Anforderung einging, die Client-IP-Adresse, Latenzen, Anforderungspfade und Serverantworten.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AU-6	PRÜFUNG, ANALYSE UND BERICHTER STATTUNG	guardduty-enabled-centralized	Amazon GuardDuty kann mithilfe von Threat Intellige nce Feeds helfen, potenzielle Cybersich erheitsereignisse zu überwachen und zu erkennen. Dazu gehören Listen mit bösartigen IPs und maschinel len Lernmethoden zur Identifizierung unerwarteter, nicht autorisierter und bösartiger Aktivitäten in Ihrer AWS Cloud-Umgebung.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AU-6	PRÜFUNG, ANALYSE UND BERICHTER STATTUNG	rds-logging-enabled	Um die Protokoll ierung und Überwachung in Ihrer Umgebung zu erleichtern, stellen Sie sicher, dass die Amazon Relationa l Database Service (Amazon RDS)-Prot okollierung aktiviert ist. Mit der Amazon-RDS-Protokollierung können Sie Ereigniss e wie Verbindungen, Verbindungsabbrüch e, Abfragen oder abgefragte Tabellen erfassen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AU-6	PRÜFUNG, ANALYSE UND BERICHTER STATTUNG	redshift-cluster-configuration-check	Um Daten im Ruhezustand zu schützen, muss die Verschlüsselung für Ihre Amazon-Redshift-Cluster aktiviert sein. Sie müssen auch sicherstellen, dass die erforderlichen Konfigurationen auf Amazon-Redshift-Clustern bereitgestellt werden. Die Prüfungsprotokollierung muss aktiviert sein, um Informationen zu Verbindungen und Benutzeraktivitäten in der Datenbank bereitzustellen. Diese Regel erfordert, dass ein Wert für clusterDbEncrypted (Config Default: TRUE) und LoggingEnabled (Config Default: TRUE) gesetzt ist. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AU-6	PRÜFUNG, ANALYSE UND BERICHTER STATTUNG	s3- bucket-logging-enabled	Die Amazon Simple Storage Service (Amazon S3)-Serverzugriffs protokollierung bietet eine Methode zur Überwachu ng des Netzwerks im Hinblick auf potenzielle Cybersich erheitsereignisse. Die Ereignisse werden überwacht, indem detaillierte Aufzeichn ungen über die Anfragen erfasst werden, die an einen Amazon-S3-Bucket gestellt wurden. Jeder Zugriffsprotokolle intrag enthält Details zu einer einzelnen Zugriffsanfrage. Zu den Details gehören Anforderer, Bucket-Name, Anforderu ngszeit, Anforderu ngsaktion, Antwortst atus und Fehlercode, falls relevant.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AU-6	PRÜFUNG, ANALYSE UND BERICHTER STATTUNG	vpc-flow-logs-enabled	VPC-Flow-Protokolle erfassen detaillierte Informationsdatensätze über den IP-Datenverkehr, der zu und von Netzwerkschnittstellen in Ihrer Amazon Virtual Private Cloud (Amazon VPC) fließt. Standardmäßig enthalten Flow-Protokolldatensätze Werte für die verschiedenen Komponenten des IP-Flows, einschließlich Quelle, Ziel und Protokoll.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AU-9	SCHUTZ VON PRÜFUNGSI NFORMATIONEN	s-3 bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) unterstützt die Aufrechterhaltung einer angemesse nen Kapazität und Verfügbarkeit. CRR ermöglicht das automatische, asynchrone Kopieren von Objekten in Amazon-S3-Buckets, um die Datenverf ügbarkeit sicherzus tellen.
AU-9	SCHUTZ VON PRÜFUNGSI NFORMATIONEN	cloud-trail-encryption-enabled	Da sensible Daten vorhanden sein können und um Daten im Ruhezustand zu schützen, sollten Sie sicherstellen, dass die Verschlüsselung für Ihre AWS CloudTrail Trails aktiviert ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AU-9	SCHUTZ VON PRÜFUNGSINFORMATIONEN	cloud-trail-log-file-Validierung aktiviert	Verwenden Sie die AWS CloudTrail Protokolldateivalidierung, um die Integrität von Protokollen zu überprüfen. CloudTrail Mithilfe der Protokolldateivalidierung kann festgestellt werden, ob eine Protokolldatei geändert oder gelöscht wurde oder ob sie nach der Übermittlung CloudTrail unverändert geblieben ist. Dieses Feature wurde mit dem Branchenstandard entsprechenden Algorithmen entwickelt: SHA-256 für die Hashfunktion und SHA-256 mit RSA für digitale Signaturen. Aus diesem Grund ist es rechnerisch unmöglich, CloudTrail Protokolldateien unbemerkt zu ändern, zu löschen oder zu fälschen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AU-9	SCHUTZ VON PRÜFUNGSI NFORMATIONEN	cloudwatch-log-group-encrypted	Um sensible Daten im Speicher zu schützen, stellen Sie sicher, dass die Verschlüs selung für Ihre Amazon CloudWatch Log Groups aktiviert ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AU-9	SCHUTZ VON PRÜFUNGSINFORMATIONEN	s-3 bucket-versioning-enabled	Die Versionsverwaltung von Amazon Simple Storage Service (Amazon S3)-Buckets hilft dabei, mehrere Varianten eines Objekts im selben Amazon-S3-Bucket zu speichern. Verwenden Sie die Versionsverwaltung, um sämtliche Versionen aller Objekte in Ihrem Amazon-S3-Bucket zu speichern, abzurufen oder wiederherzustellen. Mit der Versionsverwaltung können Sie Versionen sowohl nach unbeabsichtigten Benutzeraktionen als auch nach Anwendungsfehlern problemlos wiederherstellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AU-11	AUFBEWAHRUNG VON PRÜFUNGSAUFZEICHNUNGEN	cw-loggroup-retention-period-überprüfen	Stellen Sie sicher, dass die Ereignisprotokolldaten für Ihre Protokollgruppen über eine Mindestdauer aufbewahrt werden, um die Fehlerbehebung und forensische Untersuchungen zu unterstützen. Fehlende frühere Ereignisprotokolldaten erschweren die Rekonstruierung und Identifizierung potenziell schädlicher Ereignisse.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AU-12	GENERIERUNG VON PRÜFUNGEN	codebuild-project-logging-enabled	Stellen Sie sicher, dass die AWS CodeBuild Projektprotokollierung aktiviert ist, damit Ihre Build-Ausgabeprotokolle entweder an Amazon CloudWatch oder Amazon Simple Storage Service (Amazon S3) gesendet werden. Build-Ausgabeprotokolle enthalten detaillierte Informationen zu Ihrem Build-Projekt.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AU-12	GENERIERUNG VON PRÜFUNGEN	multi-region-cloudtrail-enabled	AWS CloudTrail zeichnet Aktionen und API-Aufrufe der AWS Management Console auf. Sie können feststellen, welche Benutzer und Konten angerufen wurden AWS, von welcher Quell-IP-Adresse aus die Anrufe getätigt wurden und wann die Anrufe erfolgten. CloudTrail übermittelt Protokolldateien aus allen AWS Regionen an Ihren S3-Bucket , wenn MULTI_REGION_CLOUD_TRAIL_ENABLED aktiviert ist. Außerdem wird beim AWS Start einer neuen Region derselbe Trail in der neuen Region erstellt. CloudTrail Dadurch erhalten Sie automatisch Protokolldateien mit API-Aktivitäten für die neue Region.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AU-12	GENERIERUNG VON PRÜFUNGEN	rds-logging-enabled	Um die Protokollierung und Überwachung in Ihrer Umgebung zu erleichtern, stellen Sie sicher, dass die Amazon Relational Database Service (Amazon RDS)-Protokollierung aktiviert ist. Mit der Amazon-RDS-Protokollierung können Sie Ereignisse wie Verbindungen, Verbindungsabbrüche, Abfragen oder abgefragte Tabellen erfassen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AU-12	GENERIERUNG VON PRÜFUNGEN	wafv2-logging-enabled	Um die Protokollierung und Überwachung in Ihrer Umgebung zu erleichtern, aktivieren Sie die AWS WAF (V2) -Protokollierung im regionalen und globalen Web ACLs. AWS Die WAF-Protokollierung bietet detaillierte Informationen über den Datenverkehr, der von Ihrer Web-ACL analysiert wird. In den Protokollen werden die Uhrzeit aufgezeichnet, zu der die AWS WAF die Anfrage von Ihrer AWS Ressource erhalten hat, Informationen über die Anfrage und eine Aktion für die Regel, der jede Anfrage entsprach.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AU-12	GENERIERUNG VON PRÜFUNGEN	api-gw-execution-logging-aktiviert	Die API-Gateway-Protokollierung zeigt detaillierte Ansichten der Benutzer, die auf die API zugegriffen haben, und wie diese Benutzer auf die API zugegriffen haben. Diese Einblicke ermöglichen die Transparenz von Benutzeraktivitäten.
AU-12	GENERIERUNG VON PRÜFUNGEN	cloud-trail-cloud-watch-logs-aktiviert	Verwenden Sie Amazon CloudWatch , um Protokoll ereignisaktivitäten zentral zu sammeln und zu verwalten. Die Aufnahme von AWS CloudTrail Daten liefert Einzelheiten zu den API-Aufrufaktivitäten in Ihrem AWS-Konto.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AU-12	GENERIERUNG VON PRÜFUNGEN	cloudtrail-enabled	AWS CloudTrail kann bei der Nichtabstreitbarkeit helfen, indem Aktionen und API-Aufrufe der AWS Management Console aufgezeichnet werden. Sie können die Benutzer und die Benutzer AWS-Konten , die einen AWS Dienst aufgerufen haben, die Quell-IP-Adresse, über die die Aufrufe generiert wurden, und den Zeitpunkt der Anrufe identifizieren. Einzelheiten zu den erfassten Daten finden Sie unter Inhalt des AWS CloudTrail Datensatzes.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AU-12	GENERIERUNG VON PRÜFUNGEN	cloudtrail-s3-data events-enabled	Die Erfassung von Simple Storage Service (Amazon S3)-Datenereignissen unterstützt die Erkennung von ungewöhnlichen Aktivitäten. Zu den Details gehören AWS-Konto Informationen über den Zugriff auf einen Amazon S3 S3-Bucket, die IP-Adresse und die Uhrzeit des Ereignisses.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AU-12	GENERIERUNG VON PRÜFUNGEN	elb-logging-enabled	Die Elastic-Load-Balancing-Aktivität ist ein zentraler Kommunikationspunkt innerhalb einer Umgebung. Stellen Sie sicher, dass die ELB-Protokollierung aktiviert ist. Die gesammelten Daten enthalten detaillierte Informationen zu Anfragen, die an den ELB gesendet wurden. Jedes Protokoll enthält Informationen wie die Zeit, zu der die Anforderung einging, die Client-IP-Adresse, Latenzen, Anforderungspfade und Serverantworten.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AU-12	GENERIERUNG VON PRÜFUNGEN	redshift-cluster-configuration-check	Um Daten im Ruhezustand zu schützen, muss die Verschlüsselung für Ihre Amazon-Redshift-Cluster aktiviert sein. Sie müssen auch sicherstellen, dass die erforderlichen Konfigurationen auf Amazon-Redshift-Clustern bereitgestellt werden. Die Prüfungsprotokollierung muss aktiviert sein, um Informationen zu Verbindungen und Benutzeraktivitäten in der Datenbank bereitzustellen. Diese Regel erfordert, dass ein Wert für clusterDbEncrypted (Config Default: TRUE) und LoggingEnabled (Config Default: TRUE) gesetzt ist. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AU-12	GENERIERUNG VON PRÜFUNGEN	s3- bucket-logging-enabled	Die Amazon Simple Storage Service (Amazon S3)-Serverzugriffs protokollierung bietet eine Methode zur Überwachu ng des Netzwerks im Hinblick auf potenzielle Cybersich erheitsereignisse. Die Ereignisse werden überwacht, indem detaillierte Aufzeichn ungen über die Anfragen erfasst werden, die an einen Amazon-S3-Bucket gestellt wurden. Jeder Zugriffsprotokolle intrag enthält Details zu einer einzelnen Zugriffsanfrage. Zu den Details gehören Anforderer, Bucket-Name, Anforderu ngszeit, Anforderu ngsaktion, Antwortst atus und Fehlercode, falls relevant.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AU-12	GENERIERUNG VON PRÜFUNGEN	vpc-flow-logs-enabled	VPC-Flow-Protokolle erfassen detaillierte Informationsdatensätze über den IP-Datenverkehr, der zu und von Netzwerkschnittstellen in Ihrer Amazon Virtual Private Cloud (Amazon VPC) fließt. Standardmäßig enthalten Flow-Protokolldatensätze Werte für die verschiedenen Komponenten des IP-Flows, einschließlich Quelle, Ziel und Protokoll.
CA-7	KONTINUIERLICHE ÜBERWACHUNG	lambda-concurrency-check	Diese Regel stellt sicher, dass die Höchst- und Untergrenzen für die Gleichzeitigkeit einer Lambda-Funktion festgelegt werden. Dies kann Sie beim Baselining für die Anzahl der Anforderungen unterstützen, die Ihre Funktion zu einem bestimmten Zeitpunkt verarbeitet.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CA-7	KONTINUIERLICHE ÜBERWACHUNG	lambda-dlq-check	Aktivieren Sie diese Regel, um das entsprechende Personal über Amazon Simple Queue Service (Amazon SQS) oder Amazon Simple Notification Service (Amazon SNS) zu benachrichtigen, wenn eine Funktion ausgefallen ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CA-7	KONTINUIERLICHE ÜBERWACHUNG	multi-region-cloudtrail-enabled	AWS CloudTrail zeichnet Aktionen und API-Aufrufe der AWS Management Console auf. Sie können feststellen, welche Benutzer und Konten angerufen wurden AWS, von welcher Quell-IP-Adresse aus die Anrufe getätigt wurden und wann die Anrufe erfolgten. CloudTrail übermittelt Protokolldateien aus allen AWS Regionen an Ihren S3-Bucket , wenn MULTI_REG ION_CLOUD _TRAIL_ENABLED aktiviert ist. Außerdem wird beim AWS Start einer neuen Region derselbe Trail in der neuen Region erstellt. CloudTrail Dadurch erhalten Sie automatis ch Protokolldateien mit API-Aktivitäten für die neue Region.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CA-7	KONTINUIERLICHE ÜBERWACHUNG	rds-enhanced-monitoring-enabled	Aktivieren Sie Amazon Relational Database Service (Amazon RDS), um die Verfügbarkeit von Amazon RDS zu überwachen. Dies bietet einen detaillierten Einblick in den Zustand Ihrer Amazon-RDS-Datenbank-Instances. Wenn der Amazon-RDS-Speicher mehr als ein zugrunde liegendes physisches Gerät verwendet, erfasst Enhanced Monitoring die Daten für jedes Gerät. Wenn die Amazon-RDS-Datenbank-Instance in einer Multi-AZ-Bereitstellung ausgeführt wird, werden außerdem die Daten für jedes Gerät auf dem sekundären Host sowie die Metriken des sekundären Hosts erfasst.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CA-7	KONTINUIERLICHE ÜBERWACHUNG	securityhub-enabled	AWS Security Hub hilft bei der Überwachung von unbefugtem Personal, Verbindungen, Geräten und Software. AWS Security Hub aggregiert, organisiert und priorisiert die Sicherheitswarnungen oder Ergebnisse mehrerer Dienste. AWS Einige dieser Dienste sind Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer und AWS Firewall Manager sowie AWS Partnerlösungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CA-7	KONTINUIERLICHE ÜBERWACHUNG	autoscaling-group-elb-healthcheck-erforderlich	Die Elastic Load Balancer (ELB) - Zustandsprüfungen für Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling Scaling-Gruppen unterstützen die Aufrechterhaltung einer angemessenen Kapazität und Verfügbarkeit. Der Load Balancer sendet regelmäßig Pings, versucht Verbindungen herzustellen oder sendet Anfragen, um den Zustand der EC2 Amazon-Instances in einer Gruppe mit auto-scaling zu testen. Wenn eine Instance nicht zurückmeldet, wird der Traffic an eine neue EC2 Amazon-Instance gesendet.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CA-7	KONTINUIERLICHE ÜBERWACHUNG	beanstalk-enhanced-health-reporting-aktiviert	AWS Die verbesserte Zustandsberichterstattung von Elastic Beanstalk ermöglicht eine schnellere Reaktion auf Veränderungen im Zustand der zugrunde liegenden Infrastruktur. Diese Änderungen könnten zu einer mangelnden Verfügbarkeit der Anwendung führen. Die erweiterten Zustandsberichte von Elastic Beanstalk bieten eine Statusbeschreibung, um den Schweregrad der identifizierten Probleme einzuschätzen und mögliche Ursachen zu identifizieren, die untersucht werden müssen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CA-7	KONTINUIERLICHE ÜBERWACHUNG	cloudtrail-enabled	AWS CloudTrai l kann durch die Aufzeichnung von Aktionen und API-Aufrufen in der AWS Management Console bei der Nichtabst reitbarkeit helfen. Sie können die Benutzer und die Benutzer AWS-Konten , die einen AWS Dienst aufgerufen haben, die Quell-IP-Adresse, über die die Aufrufe generiert wurden, und den Zeitpunkt der Anrufe identifiz ieren. Einzelheiten zu den erfassten Daten finden Sie unter Inhalt des AWS CloudTrail Datensatzes.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CA-7	KONTINUIERLICHE ÜBERWACHUNG	cloudtrail-s3-data events-enabled	Die Erfassung von Simple Storage Service (Amazon S3)-Datenereignissen unterstützt die Erkennung von ungewöhnlichen Aktivitäten. Zu den Details gehören AWS-Konto Informationen über den Zugriff auf einen Amazon S3 S3-Bucket, die IP-Adresse und die Uhrzeit des Ereignisses.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CA-7	KONTINUIERLICHE ÜBERWACHUNG	cloudwatch-alarm-action-check	Amazon CloudWatch alarmiert, wenn eine Metrik den Schwellenwert für eine bestimmte Anzahl von Bewertungszeiträumen überschreitet. Der Alarm führt eine oder mehrere Aktionen durch, die vom Wert der Metrik oder des Ausdrucks im Vergleich zu einem Schwellenwert in einer Reihe von Zeiträumen abhängt. Diese Regel erfordert einen Wert für alarmActionRequired (Config Default: True), insufficientDataAction Required (Config Default: True), okActionRequired (Config Default: False). Der tatsächliche Wert muss die Alarmaktionen für Ihre Umgebung widerspiegeln.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CA-7	KONTINUIERLICHE ÜBERWACHUNG	dynamodb-throughput-limit-check	Aktivieren Sie diese Regel, um sicherzustellen, dass die bereitgestellte Durchsatzkapazität in Ihren Amazon-DynamoDB-Tabellen überprüft wird. Dies ist der Umfang der Lese- und Schreibaktivitäten, der von den jeweiligen Tabellen unterstützt werden kann. DynamoDB verwendet diese Informationen für das Reservieren ausreichender Systemressourcen, um Ihren Durchsatz anforderungen gerecht zu werden. Diese Regel generiert eine Warnung, wenn sich der Durchsatz dem Höchstlimit für ein Kundenkonto nähert. Mit dieser Regel können Sie optional die Parameter RCUThreshold Kontoprozentsatz

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			(Konfigurationsstandard: 80) und WCUThreshold Kontoprozentsatz (Konfigurationsstandard: 80) festlegen. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.
CA-7	KONTINUIERLICHE ÜBERWACHUNG	ec2- instance-detailed-monitoring-enabled	Aktivieren Sie diese Regel, um die Amazon Elastic Compute Cloud (Amazon EC2) - Instance-Überwachung auf der EC2 Amazon-Konsole zu verbessern, in der Monitoring-Diagramme mit einem Zeitraum von 1 Minute für die Instance angezeigt werden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CA-7	KONTINUIERLICHE ÜBERWACHUNG	guardduty-enabled-centralized	Amazon GuardDuty kann mithilfe von Threat Intellige nce Feeds helfen, potenzielle Cybersich erheitsereignisse zu überwachen und zu erkennen. Dazu gehören Listen mit bösartigen IPs und maschinel len Lernmethoden zur Identifizierung unerwarteter, nicht autorisierter und bösartiger Aktivitäten in Ihrer AWS Cloud-Umgebung.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CA-7	KONTINUIERLICHE ÜBERWACHUNG	redshift-cluster-configuration-check	Um Daten im Ruhezustand zu schützen, muss die Verschlüsselung für Ihre Amazon-Redshift-Cluster aktiviert sein. Sie müssen auch sicherstellen, dass die erforderlichen Konfigurationen auf Amazon-Redshift-Clustern bereitgestellt werden. Die Prüfungsprotokollierung muss aktiviert sein, um Informationen zu Verbindungen und Benutzeraktivitäten in der Datenbank bereitzustellen. Diese Regel erfordert, dass ein Wert für clusterDbEncrypted (Config Default: TRUE) und LoggingEnabled (Config Default: TRUE) gesetzt ist. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CM-2	BASISKONFIGURATION	alb-waf-enabled	Stellen Sie sicher, dass AWS WAF auf Elastic Load Balancers (ELB) aktiviert ist, um Webanwendungen zu schützen. Eine WAF trägt zum Schutz Ihrer Webanwendungen oder APIs vor gängigen Web-Exploits bei. Diese Web-Exploits können sich auf die Verfügbarkeit auswirken, die Sicherheit gefährden oder übermäßige Ressourcen in Ihrer Umgebung verbrauchen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CM-2	BASISKONFIGURATION	api-gw-associated-with-WAF	AWS Mit WAF können Sie eine Reihe von Regeln (als Web Access Control List (Web ACL) bezeichnet) konfigurieren, die Webanfragen auf der Grundlage von anpassbaren Websicherheitsregeln und -bedingungen, die Sie definieren, zulassen, blockieren oder zählen. Stellen Sie sicher, dass Ihre Amazon-API-Gateway-Stufe mit einer WAF-Web-ACL verknüpft ist, um sie vor böswilligen Angriffen zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CM-2	BASISKONFIGURATION	autoscaling-launch-config-public-ip-deaktiviert	Wenn Sie Ihre Netzwerkschnittstellen mit einer öffentlichen IP-Adresse konfigurieren, sind die diesen Netzwerkschnittstellen zugehörigen Ressourcen über das Internet erreichbar. EC2 Ressourcen sollten nicht öffentlich zugänglich sein, da dies einen unbeabsichtigten Zugriff auf Ihre Anwendungen oder Server ermöglichen kann.
CM-2	BASISKONFIGURATION	dms-replication-not-public	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass auf DMS-Replikationsinstanzen nicht öffentlich zugegriffen werden kann. DMS-Replikations-Instances können vertrauliche Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CM-2	BASISKONFIGURATION	ebs-snapshot-public-restorable-überprüfen	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass EBS-Snapshots nicht öffentlich wiederherstellbar sind. EBS-Volume-Snapshots können vertrauliche Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.
CM-2	BASISKONFIGURATION	ec-2 instance-no-public-ip	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon Elastic Compute Cloud (Amazon EC2) - Instances nicht öffentlich zugänglich sind. EC2 Amazon-Instances können vertrauliche Informationen enthalten, und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CM-2	BASISKONFIGURATION	elasticsearch-in-vpc-only	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass sich Amazon OpenSearch OpenSearch Service (Service) - Domains innerhalb einer Amazon Virtual Private Cloud (Amazon VPC) befinden. Eine OpenSearch Service-Domain innerhalb einer Amazon VPC ermöglicht die sichere Kommunikation zwischen OpenSearch Service und anderen Services innerhalb der Amazon VPC, ohne dass ein Internet-Gateway, ein NAT-Gerät oder eine VPN-Verbindung erforderlich ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CM-2	BASISKONFIGURATION	emr-master-no-public-ip	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon EMR-Cluster-Masterknoten nicht öffentlich zugänglich sind. Amazon-EMR-Cluster-Hauptknoten können vertrauliche Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CM-2	BASISKONFIGURATION	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) Security Groups können bei der Verwaltung des Netzwerkzugriffs helfen, indem sie eine statusbehaftete Filterung des ein- und ausgehenden Netzwerkverkehrs zu Ressourcen bereitstellen. AWS Wenn Sie eingehenden (oder entfernten) Datenverkehr von 0.0.0.0/0 bis Port 22 auf Ihren Ressourcen nicht zulassen, können Sie den Remote-Zugriff einschränken.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CM-2	BASISKONFIGURATION	ec-2 instances-in-vpc	Stellen Sie Amazon Elastic Compute Cloud (Amazon EC2) -Instances innerhalb einer Amazon Virtual Private Cloud (Amazon VPC) bereit, um eine sichere Kommunikation zwischen einer Instance und anderen Services innerhalb der Amazon VPC zu ermöglichen, ohne dass ein Internet-Gateway, ein NAT-Gerät oder eine VPN-Verbindung erforderlich ist. Der gesamte Datenverkehr bleibt sicher in der AWS Cloud. Domains, die sich innerhalb einer VPC befinden, verfügen aufgrund ihrer logischen Isolierung im Vergleich zu Domains mit öffentlichen Endpunkten über eine zusätzliche Sicherheitsebene. Weisen Sie EC2

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			Amazon-Instances einer Amazon-VPC zu, um den Zugriff ordnungsgemäß zu verwalten.
CM-2	BASISKONFIGURATION	lambda-function-public-access-verboten	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass AWS Lambda-Funktionen nicht öffentlich zugänglich sind. Der öffentliche Zugriff kann möglicherweise die Verfügbarkeit von Ressourcen beeinträchtigen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CM-2	BASISKONFIGURATION	lambda-inside-vpc	Stellen Sie AWS Lambda-Funktionen in einer Amazon Virtual Private Cloud (Amazon VPC) bereit, um eine sichere Kommunikation zwischen einer Funktion und anderen Diensten innerhalb der Amazon VPC zu gewährleisten. Bei dieser Konfiguration sind kein Internet-Gateway, kein NAT-Gerät und keine VPN-Verbindung erforderlich. Der gesamte Datenverkehr bleibt sicher in der Cloud. AWS Domains, die sich innerhalb einer VPC befinden, verfügen aufgrund ihrer logischen Isolierung im Vergleich zu Domains mit öffentlichen Endpunkten über eine zusätzliche Sicherheitsebene. Um den Zugriff ordnungsgemäß zu verwalten,

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			sollten AWS Lambda-Funktionen einer VPC zugewiesen werden.
CM-2	BASISKONFIGURATION	no-unrestricted-route-to-igw	Stellen Sie sicher, dass EC2 Amazon-Routentabellen keine uneingeschränkten Routen zu einem Internet-Gateway enthalten. Durch das Entfernen oder Beschränken des Internetzugangs für Workloads innerhalb von Amazon VPCs können unbeabsichtigte Zugriffe in Ihrer Umgebung reduziert werden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CM-2	BASISKONFIGURATION	rds-instance-public-access-überprüfen	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Relational Database Service (Amazon RDS) -Instances nicht öffentlich sind. Amazon-RDS-Datenbank-Instances können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CM-2	BASISKONFIGURATION	rds-snapshots-public-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Relational Database Service (Amazon RDS) -Instances nicht öffentlich sind. Amazon-RDS-Datenbank-Instances können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CM-2	BASISKONFIGURATION	redshift-cluster-public-access-überprüfen	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Redshift Redshift-Cluster nicht öffentlich sind. Amazon-Redshift-Cluster können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CM-2	BASISKONFIGURATION	s3- -Block-periodisch account-level-public-access	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Simple Storage Service (Amazon S3) -Buckets nicht öffentlich zugänglich sind. Diese Regel trägt dazu bei, sensible Daten vor unbefugten Remote-Benutzern zu schützen, indem sie den öffentlichen Zugriff verhindert. Mit dieser Regel können Sie optional die Parameter ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) und restrictPublicBuckets Parameter (Config Default: True) festlegen. Die tatsächlichen Werte müssen den Richtlini

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			en Ihrer Organisation entsprechen.
CM-2	BASISKONFIGURATION	s3- bucket-public-read-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie nur autorisierten Benutzern, Prozessen und Geräten Zugriff auf Amazon Simple Storage Service (Amazon S3) - Buckets gewähren. Die Verwaltung des Zugriffs sollte mit der Klassifizierung der Daten übereinstimmen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CM-2	BASISKONFIGURATION	s3- bucket-public-write-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie nur autorisierten Benutzern, Prozessen und Geräten Zugriff auf Amazon Simple Storage Service (Amazon S3) - Buckets gewähren. Die Verwaltung des Zugriffs sollte mit der Klassifizierung der Daten übereinstimmen.
CM-2	BASISKONFIGURATION	sagemaker-notebook-no-direct-Internetzugang	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass SageMaker Amazon-Notebooks keinen direkten Internetzugang zulassen. Indem Sie direkten Internetzugang blockieren, vermeiden Sie, dass unbefugte Benutzer auf sensible Daten zugreifen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CM-2	BASISKONFIGURATION	vpc-default-security-group-geschlossen	Sicherheitsgruppen von Amazon Elastic Compute Cloud (Amazon EC2) können bei der Verwaltung des Netzwerkzugriffs helfen, indem sie eine statusbehaftete Filterung des ein- und ausgehenden Netzwerkverkehrs zu Ressourcen bereitstellen. AWS Die Beschränkung des gesamten Datenverkehrs auf die Standardsicherheitsgruppe hilft dabei, den Fernzugriff auf Ihre Ressourcen einzuschränken. AWS

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CM-2	BASISKONFIGURATION	vpc-sg-open-only-to-authorized-ports	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass gemeinsame Ports für Amazon Elastic Compute Cloud (Amazon EC2) -Sicherheitsgruppen eingeschränkt sind. Wenn der Zugriff auf Ports nicht auf vertrauenswürdige Quellen beschränkt wird, kann dies zu Angriffen auf die Verfügbarkeit, Integrität und Vertraulichkeit von Systemen führen. Durch die Beschränkung des Zugriffs auf Ressourcen innerhalb einer Sicherheitsgruppe aus dem Internet (0.0.0.0/0) kann der Remote-Zugriff auf interne Systeme gesteuert werden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CM-2	BASISKONFIGURATION	ec2-managerinstance-managed-by-systems	Eine Bestandsaufnahme der Softwareplattformen und Anwendungen innerhalb des Unternehmens ist möglich, indem Amazon Elastic Compute Cloud (Amazon EC2) - Instances mit AWS Systems Manager verwaltet werden. Verwenden Sie AWS Systems Manager, um detaillierte Systemkonfigurationen, Betriebssystem-Patch-Levels, Namen und Typ der Dienste, Softwareinstallationen, Anwendungsname, Herausgeber und Version sowie andere Details zu Ihrer Umgebung bereitzustellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CM-2	BASISKONFIGURATION	ec2-check managedinstance-association-compliance-status	Verwenden Sie AWS Systems Manager Associations, um bei der Inventarisierung von Softwareplattformen und Anwendungen innerhalb eines Unternehmens zu helfen. AWS Systems Manager weist Ihren verwalteten Instanzen einen Konfigurationsstatus zu und ermöglicht es Ihnen, Basiswerte für Betriebssystem-Patch-Levels, Softwareinstallationen, Anwendungskonfigurationen und andere Details zu Ihrer Umgebung festzulegen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CM-2	BASISKONFIGURATION	ec2-stopped-instance	Aktivieren Sie diese Regel, um bei der Basiskonfiguration von Amazon Elastic Compute Cloud (Amazon EC2) - Instances zu helfen, indem Sie überprüfen, ob EC2 Amazon-Instances gemäß den Standards Ihrer Organisation für mehr als die zulässige Anzahl von Tagen gestoppt wurden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CM-2	BASISKONFIGURATION	ec2- volume-inuse-check	Diese Regel stellt sicher, dass Amazon Elastic Block Store-Volumes, die an Amazon Elastic Compute Cloud (Amazon EC2) - Instances angehängt sind, zum Löschen markiert werden, wenn eine Instance beendet wird. Wenn ein Amazon-EBS-Volume nicht gelöscht wird, wenn die Instance, an die es angehängt ist, beendet wird, kann dies gegen das Konzept der geringsten Funktionalität verstoßen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CM-2	BASISKONFIGURATION	elb-deletion-protection-enabled	Diese Regel sorgt dafür, dass der Löschschutz für Elastic Load Balancing aktiviert ist. Verwenden Sie diese Funktion, um zu verhindern, dass Ihr Load Balancer versehentlich oder böswillig gelöscht wird, was zum Verlust der Verfügbarkeit Ihrer Anwendungen führen kann.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CM-2	BASISKONFIGURATION	opensearch-in-vpc-only	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass sich Amazon OpenSearch Service-Domains innerhalb einer Amazon Virtual Private Cloud (Amazon VPC) befinden. Eine Amazon OpenSearch Service-Domain innerhalb einer Amazon VPC ermöglicht die sichere Kommunikation zwischen Amazon OpenSearch Service und anderen Services innerhalb der Amazon VPC, ohne dass ein Internet-Gateway, ein NAT-Gerät oder eine VPN-Verbindung erforderlich ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CM-2	BASISKONFIGURATION	restricted-common-ports	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass gemeinsame Ports für Amazon Elastic Compute Cloud (Amazon EC2) -Sicherheitsgruppen eingeschränkt sind. Wenn der Zugriff auf Ports nicht auf vertrauenswürdige Quellen beschränkt wird, kann dies zu Angriffen auf die Verfügbarkeit, Integrität und Vertraulichkeit von Systemen führen. Mit dieser Regel können Sie optional die Parameter blockedPort1–blockedPort5 festlegen (Standardkonfigurationen: 20, 21, 3389, 3306, 4333). Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CM-2	BASISKONFIGURATION	s3 bucket-level-public-access - verboten	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Simple Storage Service (Amazon S3) -Buckets nicht öffentlich zugänglich sind. Diese Regel trägt dazu bei, sensible Daten vor unbefugten Remote-Benutzern zu schützen, indem sie den öffentlichen Zugriff auf Bucket-Ebene verhindert.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CM-2	BASISKONFIGURATION	subnet-auto-assign-public-ip-deaktiviert	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon Virtual Private Cloud (VPC) -Subnetzen nicht automatisch eine öffentliche IP-Adresse zugewiesen wird. Amazon Elastic Compute Cloud (EC2) -Instances, die in Subnetzen gestartet werden, in denen dieses Attribut aktiviert ist, haben ihrer primären Netzwerkschnittstelle eine öffentliche IP-Adresse zugewiesen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CM-7	GERINGSTE FUNKTIONALITÄT	ec2- instance-profile-attached	EC2 Instanzprofile übergeben eine IAM-Rolle an eine EC2 Instance. Das Anhängen eines Instance-Profils an Ihre Instances kann bei der Implementierung von geringsten Berechtigungen und der Berechtigungsverwaltung helfen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CM-7	GERINGSTE FUNKTIONALITÄT	ec2-manager instance-managed-by-systems	Eine Bestandsaufnahme der Softwareplattformen und Anwendungen innerhalb des Unternehmens ist möglich, indem Amazon Elastic Compute Cloud (Amazon EC2) - Instances mit AWS Systems Manager verwaltet werden. Verwenden Sie AWS Systems Manager, um detaillierte Systemkonfigurationen, Betriebssystem-Patch-Levels, Namen und Typ der Dienste, Softwareinstallationen, Anwendungsname, Herausgeber und Version sowie andere Details zu Ihrer Umgebung bereitzustellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CM-7	GERINGSTE FUNKTIONALITÄT	ec2-check managedinstance-association-compliance-status	Verwenden Sie AWS Systems Manager Associations, um bei der Inventarisierung von Softwareplattformen und Anwendungen innerhalb eines Unternehmens zu helfen. AWS Systems Manager weist Ihren verwalteten Instanzen einen Konfigurationsstatus zu und ermöglicht es Ihnen, Basiswerte für Betriebssystem-Patch-Levels, Softwareinstallationen, Anwendungskonfigurationen und andere Details zu Ihrer Umgebung festzulegen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CM-8	INVENTAR DER INFORMATIONSSYSTEMKOMPONENTEN	ec2-manager instance-managed-by-systems	Eine Bestandsaufnahme der Softwareplattformen und Anwendungen innerhalb des Unternehmens ist möglich, indem Amazon Elastic Compute Cloud (Amazon EC2) - Instances mit AWS Systems Manager verwaltet werden. Verwenden Sie AWS Systems Manager, um detaillierte Systemkonfigurationen, Betriebssystem-Patch-Levels, Namen und Typ der Dienste, Softwareinstallationen, Anwendungsname, Herausgeber und Version sowie andere Details zu Ihrer Umgebung bereitzustellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CM-8	INVENTAR DER INFORMATIONSSYSTEM KOMPONENTEN	ec2-check managedinstance-association-compliance-status	Verwenden Sie AWS Systems Manager Associations, um bei der Inventarisierung von Softwareplattformen und Anwendungen innerhalb eines Unternehmens zu helfen. AWS Systems Manager weist Ihren verwalteten Instanzen einen Konfigurationsstatus zu und ermöglicht es Ihnen, Basiswerte für Betriebssystem-Patch-Levels, Softwareinstallationen, Anwendungskonfigurationen und andere Details zu Ihrer Umgebung festzulegen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CM-8	INVENTAR DER INFORMATIONSSYSTEM KOMPONENTEN	ec2-check managedinstance-patch-compliance-status	Aktivieren Sie diese Regel, um bei der Identifizierung und Dokumentation von Sicherheitslücken in Amazon Elastic Compute Cloud (Amazon EC2) zu helfen. Die Regel prüft, ob die EC2 Amazon-Instance die Patch-Konformität im AWS Systems Manager gemäß den Richtlinien und Verfahren Ihrer Organisation einhält.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CM-8	INVENTAR DER INFORMATI ONSSYSTEM KOMPONENTEN	guardduty-enabled-centralized	Amazon GuardDuty kann mithilfe von Threat Intellige nce Feeds helfen, potenzielle Cybersich erheitsereignisse zu überwachen und zu erkennen. Dazu gehören Listen mit bösartigen IPs und maschinel len Lernmethoden zur Identifizierung unerwarteter, nicht autorisierter und bösartiger Aktivitäten in Ihrer AWS Cloud-Umgebung.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CP-9	SICHERUNG DES INFORMATIONSSYSTEMS	aurora-resources-protected-by-Backup-Plan	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon Aurora Aurora-Ressourcen Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CP-9	SICHERUNG DES INFORMATIONSSYSTEMS	backup-plan-min-frequency-and-min-retention-check	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihr AWS Backup-Plan auf eine Mindestfrequenz und Aufbewahrung festgelegt ist. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen. Mit dieser Regel können Sie die Parameter requiredFrequencyValue (Config default: 1), requiredRetentionDays (Config default: 35) und requiredFrequencyUnit

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			(Config default: days) festlegen. Der tatsächliche Wert muss den Anforderungen Ihrer Organisation entsprechen.
CP-9	SICHERUNG DES INFORMATIONSSYSTEMS	dynamodb-resources-protected-by-Backup-Plan	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon DynamoDB DynamoDB-Ressourcen Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CP-9	SICHERUNG DES INFORMATIONSSYSTEMS	ebs-resources-protected-by-Backup-Plan	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon Elastic Block Store (Amazon EBS) -Ressourcen Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CP-9	SICHERUNG DES INFORMATIONSSYSTEMS	ec2--Plan resources-protected-by-backup	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon Elastic Compute Cloud (Amazon EC2) -Ressourcen Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CP-9	SICHERUNG DES INFORMATIONSSYSTEMS	efs-resources-protected-by-Backup-Plan	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon Elastic File System (Amazon EFS) -Dateisysteme Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CP-9	SICHERUNG DES INFORMATIONSSYSTEMS	fsx-resources-protected-by-Backup-Plan	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre FSx Amazon-Dateisysteme Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CP-9	SICHERUNG DES INFORMATIONSSYSTEMS	rds-resources-protected-by-Backup-Plan	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon Relational Database Service (Amazon RDS) -Ressourcen Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CP-9	SICHERUNG DES INFORMATIONSSYSTEMS	redshift-backup-enabled	Stellen Sie zur Unterstützung der Datensicherungsprozesse sicher, dass Ihre Amazon-Redshift-Cluster über automatisierte Snapshots verfügen. Wenn automatisierte Snapshots für einen Cluster aktiviert sind, erstellt Redshift in regelmäßigen Abständen Snapshots dieses Clusters. Standardmäßig erstellt Redshift alle acht Stunden oder alle 5 GB einen Snapshot für jeden Knoten mit Datenänderungen oder je nachdem, was zuerst eintritt.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CP-9	SICHERUNG DES INFORMATIONSSYSTEMS	db-instance-backup-enabled	Die Sicherungsfunktion von Amazon RDS erstellt Sicherungen Ihrer Datenbanken und Transaktionsprotokolle. Amazon RDS erstellt einen Snapshot für das Speichervolume Ihrer DB-Instance, sodass die gesamte DB-Instance gesichert wird. Sie können im System spezifische Aufbewahrungsfristen festlegen, um Ihre Ausfallsicherheitsanforderungen zu erfüllen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CP-9	SICHERUNG DES INFORMATIONSSYSTEMS	dynamodb-pitr-enabled	Aktivieren Sie diese Regel, um zu überprüfen, ob die Informationen gesichert wurden. Es verwaltet auch die Backups, indem es sicherstellt, dass die point-in-time Wiederherstellung in Amazon DynamoDB aktiviert ist. Bei der Wiederherstellung werden fortlaufende Backups Ihrer Tabelle für die letzten 35 Tage gespeichert.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CP-9	SICHERUNG DES INFORMATIONSSYSTEMS	elasticache-redis-cluster-automatic-Backup-Prüfung	Wenn automatische Backups aktiviert sind, ElastiCache erstellt Amazon täglich ein Backup des Clusters. Die Sicherung kann für eine von Ihrer Organisation festgelegte Anzahl von Tagen aufbewahrt werden. Automatische Backups schützen vor Datenverlust. Bei einem Ausfall können Sie einen neuen Cluster erstellen, der Ihre Daten aus dem aktuellen Backup wiederherstellt.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CP-9	SICHERUNG DES INFORMATIONSSYSTEMS	s-3 bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) unterstützt die Aufrechterhaltung einer angemessenen Kapazität und Verfügbarkeit. CRR ermöglicht das automatische, asynchrone Kopieren von Objekten in Amazon-S3-Buckets, um die Datenverfügbarkeit sicherzustellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CP-9	SICHERUNG DES INFORMATIONSSYSTEMS	s-3 bucket-versioning-enabled	Die Versionsverwaltung von Amazon Simple Storage Service (Amazon S3)-Buckets hilft dabei, mehrere Varianten eines Objekts im selben Amazon-S3-Bucket zu speichern. Verwenden Sie die Versionsverwaltung, um sämtliche Versionen aller Objekte in Ihrem Amazon-S3-Bucket zu speichern, abzurufen oder wiederherzustellen. Mit der Versionsverwaltung können Sie Versionen sowohl nach unbeabsichtigten Benutzeraktionen als auch nach Anwendungsfehlern problemlos wiederherstellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CP-10	WIEDERHERSTELLUNG UND REKONSTITUTION DES INFORMATIONSSYSTEMS	aurora-resources-protected-by-Backup-Plan	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon Aurora Aurora-Ressourcen Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CP-10	WIEDERHERSTELLUNG UND REKONSTITUTION DES INFORMATIONSSYSTEMS	backup-plan-min-frequency-and-min-retention-check	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihr AWS Backup-Plan auf eine Mindestfrequenz und Aufbewahrung festgelegt ist. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen. Mit dieser Regel können Sie die Parameter requiredFrequencyValue (Config default: 1), requiredRetentionDays (Config default: 35) und requiredFrequencyUnit

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			(Config default: days) festlegen. Der tatsächliche Wert muss den Anforderungen Ihrer Organisation entsprechen.
CP-10	WIEDERHERSTELLUNG UND REKONSTITUTION DES INFORMATIONSSYSTEMS	dynamodb-resources-protected-by-Backup-Plan	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon DynamoDB DynamoDB-Ressourcen Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CP-10	WIEDERHERSTELLUNG UND REKONSTITUTION DES INFORMATIONSSYSTEMS	ebs-resources-protected-by-Backup-Plan	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon Elastic Block Store (Amazon EBS) -Ressourcen Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CP-10	WIEDERHERSTELLUNG UND REKONSTITUTION DES INFORMATIONSSYSTEMS	ec2--Plan resources-protected-by-backup	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon Elastic Compute Cloud (Amazon EC2) -Ressourcen Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CP-10	WIEDERHERSTELLUNG UND REKONSTITUTION DES INFORMATIONSSYSTEMS	efs-resources-protected-by-Backup-Plan	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon Elastic File System (Amazon EFS) -Dateisysteme Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CP-10	WIEDERHERSTELLUNG UND REKONSTITUTION DES INFORMATIONSSYSTEMS	elb-cross-zone-load-Balancing aktiviert	Aktivieren Sie zonenübergreifendes Load Balancing für Ihre Elastic Load Balancer (ELBs), um eine angemessene Kapazität und Verfügbarkeit aufrechtzuerhalten. Zonenübergreifendes Load Balancing reduziert die Notwendigkeit, die gleiche Anzahl von Instances in jeder aktivierten Availability Zone aufrechtzuerhalten. Es verbessert auch die Fähigkeit Ihrer Anwendung, den Verlust einer oder mehrerer Instances zu bewältigen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CP-10	WIEDERHERSTELLUNG UND REKONSTITUTION DES INFORMATIONSSYSTEMS	fsx-resources-protected-by-Backup-Plan	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre FSx Amazon-Dateisysteme Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CP-10	WIEDERHERSTELLUNG UND REKONSTITUTION DES INFORMATIONSSYSTEMS	rds-resources-protected-by-Backup-Plan	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon Relational Database Service (Amazon RDS) -Ressourcen Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CP-10	WIEDERHERSTELLUNG UND REKONSTITUTION DES INFORMATIONSSYSTEMS	redshift-backup-enabled	Stellen Sie zur Unterstützung der Datensicherungsprozesse sicher, dass Ihre Amazon-Redshift-Cluster über automatisierte Snapshots verfügen. Wenn automatisierte Snapshots für einen Cluster aktiviert sind, erstellt Redshift in regelmäßigen Abständen Snapshots dieses Clusters. Standardmäßig erstellt Redshift alle acht Stunden oder alle 5 GB einen Snapshot für jeden Knoten mit Datenänderungen oder je nachdem, was zuerst eintritt.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CP-10	WIEDERHERSTELLUNG UND REKONSTITUTION DES INFORMATIONSSYSTEMS	db-instance-backup-enabled	Die Sicherungsfunktion von Amazon RDS erstellt Sicherungen Ihrer Datenbanken und Transaktionsprotokolle. Amazon RDS erstellt einen Snapshot für das Speichervolume Ihrer DB-Instance, sodass die gesamte DB-Instance gesichert wird. Sie können im System spezifische Aufbewahrungsfristen festlegen, um Ihre Ausfallsicherheitsanforderungen zu erfüllen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CP-10	WIEDERHERSTELLUNG UND REKONSTITUTION DES INFORMATIONSSYSTEMS	dynamodb-autoscaling-enabled	Amazon DynamoDB Auto Scaling verwendet den AWS Application Auto Scaling-Service, um die bereitgestellte Durchsatzkapazität so anzupassen, dass sie automatisch auf tatsächliche Verkehrsmuster reagiert. Auf diese Weise kann eine Tabelle oder ein globaler sekundärer Index die bereitgestellte Lese-/Schreibkapazität erhöhen, um plötzliche Erhöhungen des Datenverkehrs ohne Drosselung zu bewältigen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CP-10	WIEDERHERSTELLUNG UND REKONSTITUTION DES INFORMATIONSSYSTEMS	dynamodb-pitr-enabled	Aktivieren Sie diese Regel, um zu überprüfen, ob die Informationen gesichert wurden. Es verwaltet auch die Backups, indem es sicherstellt, dass die point-in-time Wiederherstellung in Amazon DynamoDB aktiviert ist. Bei der Wiederherstellung werden fortlaufende Backups Ihrer Tabelle für die letzten 35 Tage gespeichert.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CP-10	WIEDERHERSTELLUNG UND REKONSTITUTION DES INFORMATIONSSYSTEMS	ebs-optimized-instance	Eine optimierte Instance im Amazon Elastic Block Store (Amazon EBS) bietet zusätzliche, dedizierte Kapazität für Amazon-EBS-I/O-Vorgänge. Diese Optimierung bietet die beste Leistung für Ihr EBS-Volume, indem Konflikte zwischen Amazon-EBS-I/O und anderem Datenverkehr von Ihrer Instance minimiert werden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CP-10	WIEDERHER STELLUNG UND REKONSTITUTION DES INFORMATI ONSSYSTEMS	elasticache-redis-cluster-automatic-Backup-Prüfung	Wenn automatische Backups aktiviert sind, ElastiCache erstellt Amazon täglich ein Backup des Clusters. Die Sicherung kann für eine von Ihrer Organisation festgelegte Anzahl von Tagen aufbewahrt werden. Automatische Backups schützen vor Datenverlust. Bei einem Ausfall können Sie einen neuen Cluster erstellen, der Ihre Daten aus dem aktuellen Backup wiederherstellt.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CP-10	WIEDERHERSTELLUNG UND REKONSTITUTION DES INFORMATIONSSYSTEMS	elb-deletion-protection-enabled	Diese Regel sorgt dafür, dass der Löschschutz für Elastic Load Balancing aktiviert ist. Verwenden Sie diese Funktion, um zu verhindern, dass Ihr Load Balancer versehentlich oder böswillig gelöscht wird, was zum Verlust der Verfügbarkeit Ihrer Anwendungen führen kann.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CP-10	WIEDERHERSTELLUNG UND REKONSTITUTION DES INFORMATIONSSYSTEMS	rds-multi-az-support	Die Multi-AZ-Unterstützung in Amazon Relational Database Service (Amazon RDS) bietet eine verbesserte Verfügbarkeit und Beständigkeit von Datenbank-Instances. Wenn Sie eine Multi-AZ-Datenbank-Instance bereitstellen, erstellt Amazon RDS automatisch eine primäre Datenbank-Instance und repliziert die Daten synchron auf eine Standby-Instance in einer anderen Availability Zone. Jede Availability Zone läuft auf einer eigenen, physisch getrennten, unabhängigen Infrastruktur und ist auf eine hohe Verfügbarkeit ausgelegt. Im Falle eines Infrastrukturausfalls führt Amazon RDS einen automatis

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			chen Failover zum Standby-Modus durch, sodass Sie den Datenbankbetrieb wieder aufnehmen können, sobald der Failover abgeschlo ssen ist.
CP-10	WIEDERHER STELLUNG UND REKONSTITUTION DES INFORMATI ONSSYSTEMS	s-3 bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) unterstützt die Aufrechterhaltung einer angemesse nen Kapazität und Verfügbarkeit. CRR ermöglicht das automatische, asynchrone Kopieren von Objekten in Amazon-S3-Buckets, um die Datenverf ügbarkeit sicherzus tellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CP-10	WIEDERHERSTELLUNG UND REKONSTITUTION DES INFORMATIONSSYSTEMS	s-3 bucket-versioning-enabled	Die Versionsverwaltung von Amazon Simple Storage Service (Amazon S3)-Buckets hilft dabei, mehrere Varianten eines Objekts im selben Amazon-S3-Bucket zu speichern. Verwenden Sie die Versionsverwaltung, um sämtliche Versionen aller Objekte in Ihrem Amazon-S3-Bucket zu speichern, abzurufen oder wiederherzustellen. Mit der Versionsverwaltung können Sie Versionen sowohl nach unbeabsichtigten Benutzeraktionen als auch nach Anwendungsfehlern problemlos wiederherstellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CP-10	WIEDERHERSTELLUNG UND REKONSTITUTION DES INFORMATIONSSYSTEMS	vpc-vpn-2-tunnels-up	Redundante Site-to-Site VPN-Tunnel können implementiert werden, um die Anforderungen an die Ausfallsicherheit zu erfüllen. Es verwendet zwei Tunnel, um die Konnektivität sicherzustellen, falls eine der Site-to-Site VPN-Verbindungen nicht verfügbar ist. Um sich vor einem Verbindungsverlust zu schützen, können Sie für den Fall, dass Ihr Kunden-Gateway nicht verfügbar ist, eine zweite Site-to-Site VPN-Verbindung zu Ihrer Amazon Virtual Private Cloud (Amazon VPC) und Ihrem Virtual Private Gateway einrichten, indem Sie ein zweites Kunden-Gateway verwenden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
IA-2	IDENTIFIZIERUNG UND AUTHENTIFIZIERUNG (BENUTZER DER ORGANISATION)	iam-password-policy	Die Identitäten und Anmeldeinformationen werden auf der Grundlage einer organisatorischen IAM-Passwortrichtlinie ausgestellt, verwaltet und verifiziert. Sie erfüllen oder übertreffen die Anforderungen von NIST SP 800-63 und dem Standard „Best Practices“ von AWS Foundational Security für die Passwortstärke. Mit dieser Regel können Sie optional RequireUppercaseCharacters (Wert für AWS grundlegende Sicherheitsbewährte Methoden: wahr), RequireLowercaseCharacters (Wert für bewährte Methoden für AWS grundlegende Sicherheit: wahr), RequireSymbols (Wert für bewährte Methoden für AWS grundlegende Sicherheit:

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			wahr), RequireNumbers (Wert für bewährte Methoden für AWS grundlegende Sicherheit: wahr), MinimumPasswordLength (Wert für bewährte Methoden für AWS grundlegende Sicherheit: 14), PasswordReusePrevention (Wert für bewährte Methoden für AWS grundlegende Sicherheit: 24) und MaxPasswordAge (Wert für bewährte Methoden für AWS grundlegende Sicherheit: 90) für Ihr IAM festlegen Kennwortrichtlinie. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
IA-2	IDENTIFIZIERUNG UND AUTHENTIFIZIERUNG (BENUTZER DER ORGANISATION)	iam-root-access-key-überprüfen	Der Zugriff auf Systeme und Ressourcen kann gesteuert werden, indem überprüft wird, ob der Root-Benutzer keine Zugriffsschlüssel mit seiner AWS Identity and Access Management (IAM) -Rolle verknüpft hat. Stellen Sie sicher, dass die Root-Zugriffsschlüssel gelöscht werden. Erstellen und verwenden Sie stattdessen rollenbasierte Funktionen, AWS-Konten um das Prinzip der geringsten Funktionalität zu berücksichtigen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
IA-2	IDENTIFIZIERUNG UND AUTHENTIFIZIERUNG (BENUTZER DER ORGANISATION)	iam-user-mfa-enabled	Aktivieren Sie diese Regel, um den Zugriff auf Ressourcen in der AWS Cloud einzuschränken. Diese Regel sorgt dafür, dass die Multi-Faktor-Authentifizierung (MFA) für alle Benutzer aktiviert ist. MFA sorgt für eine weitere Schutzebene zusätzlich zu den Anmeldeinformationen. Reduzieren Sie Fälle von kompromittierten Konten, indem Sie MFA für Benutzer vorschreiben.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
IA-2	IDENTIFIZIERUNG UND AUTHENTIFIZIERUNG (BENUTZER DER ORGANISATION)	mfa-enabled-for-iam-Konsolenzugriff	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass MFA für alle AWS Identity and Access Management (IAM) -Benutzer aktiviert ist, die über ein Konsolenkennwort verfügen. MFA sorgt für eine weitere Schutzebene zusätzlich zu den Anmeldeinformationen. Indem Sie MFA für Benutzer vorschreiben, können Sie Fälle kompromittierter Konten reduzieren und verhindern, dass unbefugte Benutzer auf vertrauliche Daten zugreifen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
IA-2	IDENTIFIZIERUNG UND AUTHENTIFIZIERUNG (BENUTZER DER ORGANISATION)	root-account-hardware-mfa-aktiviert	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Hardware-MFA für den Root-Benutzer aktiviert ist. Der Stammbenutzer ist der AWS-Konto-Benutzer mit den meisten Berechtigungen. MFA sorgt für eine weitere Schutzebene zusätzlich zu den Anmeldeinformationen. Indem Sie MFA für den Root-Benutzer vorschreiben, können Sie die Anzahl AWS-Konten kompromittierter Benutzer reduzieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
IA-2	IDENTIFIZIERUNG UND AUTHENTIFIZIERUNG (BENUTZER DER ORGANISATION)	root-account-mfa-enabled	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass MFA für den Root-Benutzer aktiviert ist. Der Stammbenutzer ist der AWS-Konto-Benutzer mit den meisten Berechtigungen. MFA sorgt für eine weitere Schutzebene zusätzlich zu den Anmeldeinformationen. Indem Sie MFA für den Root-Benutzer vorschreiben, können Sie die Anzahl AWS-Konten kompromittierter Benutzer reduzieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
IA-5	VERWALTUNG VON AUTHENTIFIKATOREN	codebuild-project-envvar-awscred-überprüfen	Stellen Sie sicher, dass die Anmeldeinformationen AWS_ACCESS_KEY_ID AWS_SECRET_ACCESS_KEY nicht in AWS Codebuild-Projektumgebungen vorhanden sind. Speichern Sie diese Variablen nicht als Klartext. Das Speichern dieser Variablen als Klartext bewirkt eine unbeabsichtigte Offenlegung von Daten sowie unberechtigte Zugriffe.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
IA-5	VERWALTUNG VON AUTHENTIFIKATOREN	iam-password-policy	Die Identitäten und Anmeldeinformationen werden auf der Grundlage einer organisatorischen IAM-Passwortrichtlinie ausgestellt, verwaltet und verifiziert. Sie erfüllen oder übertreffen die Anforderungen von NIST SP 800-63 und dem Standard „Best Practices“ von AWS Foundational Security für die Passwortstärke. Mit dieser Regel können Sie optional RequireUppercaseCharacters (Wert für AWS grundlegende Sicherheitsbewährte Methoden: wahr), RequireLowercaseCharacters (Wert für bewährte Methoden für AWS grundlegende Sicherheit: wahr), RequireSymbols (Wert für bewährte Methoden für AWS grundlegende Sicherheit:

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			wahr), RequireNumbers (Wert für bewährte Methoden für AWS grundlegende Sicherheit: wahr), MinimumPasswordLength (Wert für bewährte Methoden für AWS grundlegende Sicherheit: 14), PasswordReusePrevention (Wert für bewährte Methoden für AWS grundlegende Sicherheit: 24) und MaxPasswordAge (Wert für bewährte Methoden für AWS grundlegende Sicherheit: 90) für Ihr IAM festlegen Kennwortrichtlinie. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
IR-4	VORFALLREAKTION	autoscaling-group-elb-healthcheck-erforderlich	Die Elastic Load Balancer (ELB) - Zustandsprüfungen für Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling Scaling-Gruppen unterstützen die Aufrechterhaltung einer angemessenen Kapazität und Verfügbarkeit. Der Load Balancer sendet regelmäßig Pings, versucht Verbindungen herzustellen oder sendet Anfragen, um den Zustand der EC2 Amazon-Instances in einer Gruppe mit auto-scaling zu testen. Wenn eine Instance nicht zurückmeldet, wird der Traffic an eine neue EC2 Amazon-Instance gesendet.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
IR-4	VORFALLREAKTION	guardduty-enabled-centralized	Amazon GuardDuty kann mithilfe von Threat Intellige nce Feeds helfen, potenzielle Cybersich erheitsereignisse zu überwachen und zu erkennen. Dazu gehören Listen mit bösartigen IPs und maschinel len Lernmethoden zur Identifizierung unerwarteter, nicht autorisierter und bösartiger Aktivitäten in Ihrer AWS Cloud-Umgebung.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
IR-4	VORFALLREAKTION	guardduty-non-archived-findings	Amazon GuardDuty hilft Ihnen dabei, die Auswirkungen eines Vorfalls zu verstehen, indem es die Ergebnisse nach Schweregrad klassifiziert: niedrig, mittel und hoch. Diese Klassifizierungen können Sie zur Festlegung von entsprechenden Strategien und Prioritäten zur Behebung solcher Vorfälle verwenden. Mit dieser Regel können Sie optional daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7) und daysHighSev (Config Default: 1) für nicht archivierte Ergebnisse festlegen, wie es die Richtlinien Ihrer Organisation erfordern.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
IR-4	VORFALLREAKTION	securityhub-enabled	AWS Security Hub hilft bei der Überwachung von unbefugtem Personal, Verbindungen, Geräten und Software. AWS Security Hub aggregiert, organisiert und priorisiert die Sicherheitswarnungen oder Ergebnisse mehrerer Dienste. AWS Einige dieser Dienste sind Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer und AWS Firewall Manager sowie AWS Partnerlösungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
IR-4	VORFALLREAKTION	cloudwatch-alarm-action-check	Amazon CloudWatch alarmiert, wenn eine Metrik den Schwellenwert für eine bestimmte Anzahl von Bewertungszeiträumen überschreitet. Der Alarm führt eine oder mehrere Aktionen durch, die vom Wert der Metrik oder des Ausdrucks im Vergleich zu einem Schwellenwert in einer Reihe von Zeiträumen abhängt. Diese Regel erfordert einen Wert für alarmActionRequired (Config Default: True), insufficientDataAction Required (Config Default: True), okActionRequired (Config Default: False). Der tatsächliche Wert muss die Alarmaktionen für Ihre Umgebung widerspiegeln.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
IR-6	ERSTELLUNG VON VORFALLBERICHTEN	guardduty-enabled-centralized	Amazon GuardDuty kann mithilfe von Threat Intelligence Feeds helfen, potenzielle Cybersicherheitsereignisse zu überwachen und zu erkennen. Dazu gehören Listen mit bösartigen IPs und maschinellen Lernmethoden zur Identifizierung unerwarteter, nicht autorisierter und bösartiger Aktivitäten in Ihrer AWS Cloud-Umgebung.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
IR-6	ERSTELLUNG VON VORFALLBERICHTEN	guardduty-non-archived-findings	Amazon GuardDuty hilft Ihnen dabei, die Auswirkungen eines Vorfalls zu verstehen, indem es die Ergebnisse nach Schweregrad klassifiziert: niedrig, mittel und hoch. Diese Klassifizierungen können Sie zur Festlegung von entsprechenden Strategien und Prioritäten zur Behebung solcher Vorfälle verwenden. Mit dieser Regel können Sie optional daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7) und daysHighSev (Config Default: 1) für nicht archivierte Ergebnisse festlegen, wie es die Richtlinien Ihrer Organisation erfordern.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
IR-6	ERSTELLUNG VON VORFALLBERICHTEN	securityhub-enabled	AWS Security Hub hilft bei der Überwachung von unbefugtem Personal, Verbindungen, Geräten und Software. AWS Security Hub aggregiert, organisiert und priorisiert die Sicherheitswarnungen oder Ergebnisse mehrerer Dienste. AWS Einige dieser Dienste sind Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer und AWS Firewall Manager sowie AWS Partnerlösungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
IR-7	UNTERSTÜTZUNG FÜR VORFALLRE AKTIONEN	guardduty-enabled-centralized	Amazon GuardDuty kann mithilfe von Threat Intellige nce Feeds helfen, potenzielle Cybersich erheitsereignisse zu überwachen und zu erkennen. Dazu gehören Listen mit bösartigen IPs und maschinel len Lernmethoden zur Identifizierung unerwarteter, nicht autorisierter und bösartiger Aktivitäten in Ihrer AWS Cloud-Umgebung.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
IR-7	UNTERSTÜTZUNG FÜR VORFALLRE AKTIONEN	guardduty-non-archived-findings	Amazon GuardDuty hilft Ihnen dabei, die Auswirkungen eines Vorfalls zu verstehen, indem es die Ergebnisse nach Schweregrad klassifiziert: niedrig, mittel und hoch. Diese Klassifizierungen können Sie zur Festlegung von entsprechenden Strategien und Prioritäten zur Behebung solcher Vorfälle verwenden. Mit dieser Regel können Sie optional daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7) und daysHighSev (Config Default: 1) für nicht archivierte Ergebnisse festlegen, wie es die Richtlinien Ihrer Organisation erfordern.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
IR-7	UNTERSTÜTZUNG FÜR VORFALLRE AKTIONEN	securityhub-enabled	AWS Security Hub hilft bei der Überwachung von unbefugtem Personal, Verbindun gen, Geräten und Software. AWS Security Hub aggregiert, organisie rt und priorisie rt die Sicherhei tswarnungen oder Ergebnisse mehrerer Dienste. AWS Einige dieser Dienste sind Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer und AWS Firewall Manager sowie AWS Partnerlösungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
RA-5	SCHWCHSTE LLENSCANS	guardduty-non-archived-findings	Amazon GuardDuty hilft Ihnen dabei, die Auswirkungen eines Vorfalls zu verstehen, indem es die Ergebnisse nach Schweregrad klassifiziert: niedrig, mittel und hoch. Diese Klassifizierungen können Sie zur Festlegung von entsprechenden Strategien und Prioritäten zur Behebung solcher Vorfälle verwenden. Mit dieser Regel können Sie optional daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7) und daysHighSev (Config Default: 1) für nicht archivierte Ergebnisse festlegen, wie es die Richtlinien Ihrer Organisation erfordern.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
RA-5	SCHWCHSTE LLENSCANS	securityhub-enabled	AWS Security Hub hilft bei der Überwachung von unbefugtem Personal, Verbindungen, Geräten und Software. AWS Security Hub aggregiert, organisiert und priorisiert die Sicherheitswarnungen oder Ergebnisse mehrerer Dienste. AWS Einige dieser Dienste sind Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer und AWS Firewall Manager sowie AWS Partnerlösungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
RA-5	SCHWCHSTE LLENSCANS	guardduty-enabled-centralized	Amazon GuardDuty kann mithilfe von Threat Intellige nce Feeds helfen, potenzielle Cybersich erheitsereignisse zu überwachen und zu erkennen. Dazu gehören Listen mit bösartigen IPs und maschinel len Lernmethoden zur Identifizierung unerwarteter, nicht autorisierter und bösartiger Aktivitäten in Ihrer AWS Cloud-Umgebung.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SA-3	LEBENSZYKLUS DER SYSTEMENTWICKLUNG	codebuild-project-envvar-awscred-überprüfen	Stellen Sie sicher, dass die Anmeldeinformationen AWS_ACCESS_KEY_ID AWS_SECRET_ACCESS_KEY nicht in AWS Codebuild-Projektumgebungen vorhanden sind. Speichern Sie diese Variablen nicht als Klartext. Das Speichern dieser Variablen als Klartext bewirkt eine unbeabsichtigte Offenlegung von Daten sowie unberechtigte Zugriffe.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SA-3	LEBENSZYKLUS DER SYSTEMENTWICKLUNG	codebuild-project-source-repo-URL-Prüfung	Stellen Sie sicher, dass die URL des Quell-Repositorys GitHub oder des Bitbucket-Quell-Repositorys keine persönlichen Zugriffstoken oder Anmeldeinformationen in Codebuild-Projektumgebungen enthält. AWS Verwende OAuth anstelle von persönlichen Zugriffstoken oder Anmeldedaten die Autorisierung für den Zugriff auf GitHub Bitbucket-Repositorys.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SA-3	LEBENSZYKLUS DER SYSTEMENTWICKLUNG	ec2-managerinstance-managed-by-systems	Eine Bestandsaufnahme der Softwareplattformen und Anwendungen innerhalb des Unternehmens ist möglich, indem Amazon Elastic Compute Cloud (Amazon EC2) - Instances mit AWS Systems Manager verwaltet werden. Verwenden Sie AWS Systems Manager, um detaillierte Systemkonfigurationen, Betriebssystem-Patch-Levels, Namen und Typ der Dienste, Softwareinstallationen, Anwendungsname, Herausgeber und Version sowie andere Details zu Ihrer Umgebung bereitzustellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-5	DENIAL-OF-SERVICE-SCHUTZ	elb-cross-zone-load-Balancing aktiviert	Aktivieren Sie zonenübergreifendes Load Balancing für Ihre Elastic Load Balancer (ELBs), um eine angemessene Kapazität und Verfügbarkeit aufrechtzuerhalten. Zonenübergreifendes Load Balancing reduziert die Notwendigkeit, die gleiche Anzahl von Instances in jeder aktivierten Availability Zone aufrechtzuerhalten. Es verbessert auch die Fähigkeit Ihrer Anwendung, den Verlust einer oder mehrerer Instances zu bewältigen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-5	DENIAL-OF-SERVICE-SCHUTZ	rds-instance-deletion-protection-aktiviert	Stellen Sie sicher, dass Amazon Relational Database Service (Amazon RDS)-Instances den Löschschutz aktiviert haben. Verwenden Sie den Löschschutz, um zu verhindern, dass Ihre Amazon-RDS-Instances versehentlich oder böswillig gelöscht werden, was zum Verlust der Verfügbarkeit Ihrer Anwendungen führen kann.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-5	DENIAL-OF-SERVICE-SCHUTZ	autoscaling-group-elb-healthcheck-erforderlich	Die Elastic Load Balancer (ELB) - Zustandsprüfungen für Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling Scaling-Gruppen unterstützen die Aufrechterhaltung einer angemessenen Kapazität und Verfügbarkeit. Der Load Balancer sendet regelmäßig Pings, versucht Verbindungen herzustellen oder sendet Anfragen, um den Zustand der EC2 Amazon-Instances in einer Gruppe mit auto-scaling zu testen. Wenn eine Instance nicht zurückmeldet, wird der Traffic an eine neue EC2 Amazon-Instance gesendet.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-5	DENIAL-OF-SERVICE-SCHUTZ	dynamodb-autoscaling-enabled	Amazon DynamoDB Auto Scaling verwendet den AWS Application Auto Scaling-Service, um die bereitgestellte Durchsatzkapazität so anzupassen, dass sie automatisch auf tatsächliche Verkehrsmuster reagiert. Auf diese Weise kann eine Tabelle oder ein globaler sekundärer Index die bereitgestellte Lese-/Schreibkapazität erhöhen, um plötzliche Erhöhungen des Datenverkehrs ohne Drosselung zu bewältigen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-5	DENIAL-OF-SERVICE-SCHUTZ	dynamodb-pitr-enabled	Aktivieren Sie diese Regel, um zu überprüfen, ob die Informationen gesichert wurden. Es verwaltet auch die Backups, indem es sicherstellt, dass die point-in-time Wiederherstellung in Amazon DynamoDB aktiviert ist. Bei der Wiederherstellung werden fortlaufende Backups Ihrer Tabelle für die letzten 35 Tage gespeichert.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-5	DENIAL-OF-SERVICE-SCHUTZ	ebs-optimized-instance	Eine optimierte Instance im Amazon Elastic Block Store (Amazon EBS) bietet zusätzliche, dedizierte Kapazität für Amazon-EBS-I/O-Vorgänge. Diese Optimierung bietet die beste Leistung für Ihr EBS-Volume, indem Konflikte zwischen Amazon-EBS-I/O und anderem Datenverkehr von Ihrer Instance minimiert werden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-5	DENIAL-OF-SERVICE-SCHUTZ	elasticache-redis-cluster-automatic-Backup-Prüfung	Wenn automatische Backups aktiviert sind, ElastiCache erstellt Amazon täglich ein Backup des Clusters. Die Sicherung kann für eine von Ihrer Organisation festgelegte Anzahl von Tagen aufbewahrt werden. Automatische Backups schützen vor Datenverlust. Bei einem Ausfall können Sie einen neuen Cluster erstellen, der Ihre Daten aus dem aktuellen Backup wiederherstellt.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-5	DENIAL-OF-SERVICE-SCHUTZ	elb-deletion-protection-enabled	Diese Regel sorgt dafür, dass der Löschschutz für Elastic Load Balancing aktiviert ist. Verwenden Sie diese Funktion, um zu verhindern, dass Ihr Load Balancer versehentlich oder böswillig gelöscht wird, was zum Verlust der Verfügbarkeit Ihrer Anwendungen führen kann.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-5	DENIAL-OF-SERVICE-SCHUTZ	guardduty-enabled-centralized	Amazon GuardDuty kann mithilfe von Threat Intellige nce Feeds helfen, potenzielle Cybersich erheitsereignisse zu überwachen und zu erkennen. Dazu gehören Listen mit bösartigen IPs und maschinel len Lernmethoden zur Identifizierung unerwarteter, nicht autorisierter und bösartiger Aktivitäten in Ihrer AWS Cloud-Umgebung.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-5	DENIAL-OF-SERVICE-SCHUTZ	rds-multi-az-support	Die Multi-AZ-Unterstützung in Amazon Relational Database Service (Amazon RDS) bietet eine verbesserte Verfügbarkeit und Beständigkeit von Datenbank-Instances. Wenn Sie eine Multi-AZ-Datenbank-Instance bereitstellen, erstellt Amazon RDS automatisch eine primäre Datenbank-Instance und repliziert die Daten synchron auf eine Standby-Instance in einer anderen Availability Zone. Jede Availability Zone läuft auf einer eigenen, physisch getrennten, unabhängigen Infrastruktur und ist auf eine hohe Verfügbarkeit ausgelegt. Im Falle eines Infrastrukturausfalls führt Amazon RDS einen automatis

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			chen Failover zum Standby-Modus durch, sodass Sie den Datenbankbetrieb wieder aufnehmen können, sobald der Failover abgeschlo ssen ist.
SC-5	DENIAL-OF-SERVICE-SCHUTZ	s-3 bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) unterstützt die Aufrechterhaltung einer angemesse nen Kapazität und Verfügbarkeit. CRR ermöglicht das automatische, asynchrone Kopieren von Objekten in Amazon-S3-Buckets, um die Datenverf ügbarkeit sicherzus tellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-5	DENIAL-OF-SERVICE-SCHUTZ	s-3 bucket-versioning-enabled	Die Versionsv erwaltung von Amazon Simple Storage Service (Amazon S3)-Bucke ts hilft dabei, mehrere Varianten eines Objekts im selben Amazon-S3-Bucket zu speichern. Verwenden Sie die Versionsv erwaltung, um sämtliche Versionen aller Objekte in Ihrem Amazon-S3-Bucket zu speichern , abzurufen oder wiederherzustellen . Mit der Versionsv erwaltung können Sie Versionen sowohl nach unbeabsic htigten Benutzera ktionen als auch nach Anwendungsfehlern problemlos wiederher stellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-5	DENIAL-OF-SERVICE-SCHUTZ	vpc-vpn-2-tunnels-up	Redundante Site-to-Site VPN-Tunnel können implementiert werden, um die Anforderungen an die Ausfallsicherheit zu erfüllen. Es verwendet zwei Tunnel, um die Konnektivität sicherzustellen, falls eine der Site-to-Site VPN-Verbindungen nicht verfügbar ist. Um sich vor einem Verbindungsverlust zu schützen, können Sie für den Fall, dass Ihr Kunden-Gateway nicht verfügbar ist, eine zweite Site-to-Site VPN-Verbindung zu Ihrer Amazon Virtual Private Cloud (Amazon VPC) und Ihrem Virtual Private Gateway einrichten, indem Sie ein zweites Kunden-Gateway verwenden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-7	GRENZSCHUTZ	alb-waf-enabled	Stellen Sie sicher, dass AWS WAF auf Elastic Load Balancers (ELB) aktiviert ist, um Webanwendungen zu schützen. Eine WAF trägt zum Schutz Ihrer Webanwend ungen oder APIs vor gängigen Web-Explo its bei. Diese Web-Exploits können sich auf die Verfügbar keit auswirken, die Sicherheit gefährden oder übermäßige Ressourcen in Ihrer Umgebung verbrauch en.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-7	GRENZSCHUTZ	autoscaling-launch-config-public-ip-deaktiviert	Wenn Sie Ihre Netzwerkschnittstellen mit einer öffentlichen IP-Adresse konfigurieren, sind die diesen Netzwerkschnittstellen zugehörigen Ressourcen über das Internet erreichbar. EC2 Ressourcen sollten nicht öffentlich zugänglich sein, da dies einen unbeabsichtigten Zugriff auf Ihre Anwendungen oder Server ermöglichen kann.
SC-7	GRENZSCHUTZ	elb-tls-https-listeners-nur	Stellen Sie sicher, dass Ihre Elastic Load Balancer (ELBs) mit SSL- oder HTTPS-Listenern konfiguriert sind. Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-7	GRENZSCHUTZ	ec-2 instances-in-vpc	Stellen Sie Amazon Elastic Compute Cloud (Amazon EC2) -Instances innerhalb einer Amazon Virtual Private Cloud (Amazon VPC) bereit, um eine sichere Kommunika tion zwischen einer Instance und anderen Services innerhalb der Amazon VPC zu ermöglichen, ohne dass ein Internet-Gateway, ein NAT-Gerät oder eine VPN-Verbindung erforderlich ist. Der gesamte Datenverk ehr bleibt sicher in der AWS Cloud. Domains, die sich innerhalb einer VPC befinden, verfügen aufgrund ihrer logischen Isolierun g im Vergleich zu Domains mit öffentlic hen Endpunkten über eine zusätzlic he Sicherheitsebene. Weisen Sie EC2

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			Amazon-Instances einer Amazon-VPC zu, um den Zugriff ordnungsgemäß zu verwalten.
SC-7	GRENZSCHUTZ	ssm-document-not-public	Stellen Sie sicher, dass AWS Systems Manager (SSM) - Dokumente nicht öffentlich sind, da dies einen unbeabsichtigten Zugriff auf Ihre SSM-Dokumente ermöglichen kann. Ein öffentliches SSM-Dokument kann Informationen über Ihr Konto, Ihre Ressourcen und internen Prozesse preisgeben.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-7	GRENZSCHUTZ	vpc-flow-logs-enabled	VPC-Flow-Protokolle erfassen detaillierte Informationsdatensätze über den IP-Datenverkehr, der zu und von Netzwerkschnittstellen in Ihrer Amazon Virtual Private Cloud (Amazon VPC) fließt. Standardmäßig enthalten Flow-Protokolldatensätze Werte für die verschiedenen Komponenten des IP-Flows, einschließlich Quelle, Ziel und Protokoll.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-7	GRENZSCHUTZ	wafv2-logging-enabled	Um die Protokollierung und Überwachung in Ihrer Umgebung zu erleichtern, aktivieren Sie die AWS WAF (V2) -Protokollierung im regionalen und globalen Web. ACLs AWS Die WAF-Protokollierung bietet detaillierte Informationen über den Datenverkehr, der von Ihrer Web-ACL analysiert wird. In den Protokollen werden die Uhrzeit aufgezeichnet, zu der die AWS WAF die Anfrage von Ihrer AWS Ressource erhalten hat, Informationen über die Anfrage und eine Aktion für die Regel, der jede Anfrage entsprach.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-7	GRENZSCHUTZ	alb-http-to-https-Umleitungsprüfung	Um Daten während der Übertragung zu schützen, stellen Sie sicher, dass Ihr Application Load Balancer unverschlüsselte HTTP-Anfragen automatisch an HTTPS umleitet. Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-7	GRENZSCHUTZ	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) Security Groups können bei der Verwaltung des Netzwerkzugriffs helfen, indem sie eine statusbehaftete Filterung des ein- und ausgehenden Netzwerkverkehrs zu Ressourcen bereitstellen. AWS Wenn Sie eingehenden (oder entfernten) Datenverkehr von 0.0.0.0/0 bis Port 22 auf Ihren Ressourcen nicht zulassen, können Sie den Remote-Zugriff einschränken.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-7	GRENZSCHUTZ	lambda-inside-vpc	Stellen Sie AWS Lambda-Funktionen in einer Amazon Virtual Private Cloud (Amazon VPC) bereit, um eine sichere Kommunika tion zwischen einer Funktion und anderen Diensten innerhalb der Amazon VPC zu gewährleisten. Bei dieser Konfiguration sind kein Internet-Gateway, kein NAT-Gerät und keine VPN-Verbindung erforderlich. Der gesamte Datenverk ehr bleibt sicher in der Cloud. AWS Domains, die sich innerhalb einer VPC befinden, verfügen aufgrund ihrer logischen Isolierun g im Vergleich zu Domains mit öffentlic hen Endpunkten über eine zusätzliche Sicherheitsebene. Um den Zugriff ordnungsg emäß zu verwalten,

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			sollten AWS Lambda-Funktionen einer VPC zugewiesen werden.
SC-7	GRENZSCHUTZ	rds-instance-public-access-überprüfen	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Relational Database Service (Amazon RDS) -Instances nicht öffentlich sind. Amazon-RDS-Datenbank-Instances können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-7	GRENZSCHUTZ	rds-snapshots-public-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Relational Database Service (Amazon RDS) -Instances nicht öffentlich sind. Amazon-RDS-Datenbank-Instances können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-7	GRENZSCHUTZ	redshift-cluster-public-access-überprüfen	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Redshift Redshift-Cluster nicht öffentlich sind. Amazon-Redshift-Cluster können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.
SC-7	GRENZSCHUTZ	redshift-require-tls-ssl	Stellen Sie sicher, dass Ihre Amazon-Redshift-Cluster eine TLS/SSL-Verschlüsselung erfordern, um eine Verbindung zu SQL-Clients herzustellen. Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-7	GRENZSCHUTZ	restricted-common-ports	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass gemeinsame Ports für Amazon Elastic Compute Cloud (Amazon EC2) -Sicherheitsgruppen eingeschränkt sind. Wenn der Zugriff auf Ports nicht auf vertrauenswürdige Quellen beschränkt wird, kann dies zu Angriffen auf die Verfügbarkeit, Integrität und Vertraulichkeit von Systemen führen. Mit dieser Regel können Sie optional die Parameter blockedPort1–blockedPort5 festlegen (Standardkonfigurationen: 20, 21, 3389, 3306, 4333). Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-7	GRENZSCHUTZ	s-3 bucket-public-read-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie nur autorisierten Benutzern, Prozessen und Geräten Zugriff auf Amazon Simple Storage Service (Amazon S3) - Buckets gewähren. Die Verwaltung des Zugriffs sollte mit der Klassifizierung der Daten übereinst immen.
SC-7	GRENZSCHUTZ	s3- bucket-public-write-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie nur autorisierten Benutzern, Prozessen und Geräten Zugriff auf Amazon Simple Storage Service (Amazon S3) - Buckets gewähren. Die Verwaltung des Zugriffs sollte mit der Klassifizierung der Daten übereinst immen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-7	GRENZSCHUTZ	s3- bucket-ssl-requests-only	Um Daten während der Übertragung zu schützen, stellen Sie sicher, dass Ihre Amazon Simple Storage Service (Amazon S3)-Buckets Anfragen zur Verwendung von Secure Socket Layer (SSL)-Buckets erfordern. Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-7	GRENZSCHUTZ	sagemaker-notebook-no-direct-Internetzugang	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass SageMaker Amazon-Notebooks keinen direkten Internetzugang zulassen. Indem Sie direkten Internetzugang blockieren, vermeiden Sie, dass unbefugte Benutzer auf sensible Daten zugreifen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-7	GRENZSCHUTZ	subnet-auto-assign-public-ip-deaktiviert	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon Virtual Private Cloud (VPC) -Subnetzen nicht automatisch eine öffentliche IP-Adresse zugewiesen wird. Amazon Elastic Compute Cloud (EC2) -Instances, die in Subnetzen gestartet werden, in denen dieses Attribut aktiviert ist, haben ihrer primären Netzwerkschnittstelle eine öffentliche IP-Adresse zugewiesen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-7	GRENZSCHUTZ	vpc-default-security-group-geschlossen	Sicherheitsgruppen von Amazon Elastic Compute Cloud (Amazon EC2) können bei der Verwaltung des Netzwerkzugriffs helfen, indem sie eine statusbehaftete Filterung des ein- und ausgehenden Netzwerkverkehrs zu Ressourcen bereitstellen. AWS Die Beschränk ung des gesamten Datenverkehrs auf die Standardsicherheit sgruppe hilft dabei, den Fernzugriff auf Ihre Ressourcen einzuschränken. AWS

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-7	GRENZSCHUTZ	vpc-sg-open-only-to-authorized-ports	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass gemeinsame Ports für Amazon Elastic Compute Cloud (Amazon EC2) -Sicherheitsgruppen eingeschränkt sind. Wenn der Zugriff auf Ports nicht auf vertrauenswürdige Quellen beschränkt wird, kann dies zu Angriffen auf die Verfügbarkeit, Integrität und Vertraulichkeit von Systemen führen. Durch die Beschränkung des Zugriffs auf Ressourcen innerhalb einer Sicherheitsgruppe aus dem Internet (0.0.0.0/0) kann der Remote-Zugriff auf interne Systeme gesteuert werden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-7	GRENZSCHUTZ	waf-regional-webacl-not-leer	Eine an eine AWS WAF angehängte Web-ACL kann eine Sammlung von Regeln und Regelgruppen zur Überprüfung und Steuerung von Webanfragen enthalten. Wenn eine Web-ACL leer ist, wird der Webdatenverkehr weitergeleitet, ohne von der WAF erkannt oder bearbeitet zu werden.
SC-12	EINRICHTUNG UND VERWALTUNG KRYPTOGRAFISCHER SCHLÜSSEL	cmk-backing-key-rotation-aktiviert	Aktivieren Sie die Schlüsselrotation, um sicherzustellen, dass Schlüssel rotiert werden, nachdem sie das Ende ihrer Krypto-Periode erreicht haben.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-12	EINRICHTUNG UND VERWALTUN G KRYPTOGRA FISCHER SCHLÜSSEL	acm-certificate-ex piration-check	Stellen Sie sicher, dass die Netzwerki ntegrität geschützt ist, indem Sie sicherste llen, dass X509-Zertifikate von AWS ACM ausgestel lt werden. Diese Zertifikate müssen gültig und dürfen nicht abgelaufen sein. Für diese Regel ist ein Wert für erforderlich daysToExpiration (Wert für bewährte AWS Grundregeln für Sicherheit: 90). Der tatsächliche Wert muss den Richtlini en Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-12	EINRICHTUNG UND VERWALTUNG KRYPTOGRAFISCHER SCHLÜSSEL	kms-cmk-not-scheduled-zum Löschen	Um Daten im Ruhezustand zu schützen, sollten Sie sicherstellen, dass die für den Kunden erforderlichen Masterschlüssel (CMKs) nicht im AWS Key Management Service (AWS KMS) gelöscht werden. Da Schlüssel manchmal gelöscht werden müssen, können Sie mit dieser Regel alle zu löschenden Schlüssel überprüfen, falls ein Schlüssel versehentlich zur Löschung vorgemerkt wurde.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-13	KRYPTOGRAFISCHER SCHUTZ	kms-cmk-not-scheduled-zum Löschen	Um Daten im Ruhezustand zu schützen, sollten Sie sicherstellen, dass die für den Kunden erforderlichen Masterschlüssel (CMKs) nicht im AWS Key Management Service (AWS KMS) gelöscht werden. Da Schlüssel manchmal gelöscht werden müssen, können Sie mit dieser Regel alle zu löschenden Schlüssel überprüfen, falls ein Schlüssel versehentlich zur Löschung vorgemerkt wurde.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-13	KRYPTOGRAFISCHER SCHUTZ	s3- default-encryption-kms	Stellen Sie sicher, dass die Verschlüsselung für Ihre Amazon Simple Storage Service (Amazon S3)-Buckets aktiviert ist. Um eventuell vorhandene sensible Daten im Ruhezustand in einem Amazon-S3-Bucket zu schützen, muss die Verschlüsselung aktiviert sein.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-13	KRYPTOGRA FISCHER SCHUTZ	sagemaker-endpoint-configuration-kms-key-konfiguriert	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass die Verschlüsselung mit dem AWS Key Management Service (AWS KMS) für Ihren Endpunkt aktiviert ist. SageMaker Da sensible Daten auf dem SageMaker Endgerät gespeiche rt werden können, sollten Sie die Verschlüsselung im Ruhezustand aktiviere n, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-13	KRYPTOGRA FISCHER SCHUTZ	sagemaker-notebook-instance-kms-schlüsselkonfiguriert	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass die Verschlüsselung mit dem AWS Key Management Service (AWS KMS) für Ihr Notebook aktiviert ist. SageMaker Da vertrauliche Daten im SageMaker Notebook gespeichert werden können, sollten Sie die Verschlüsselung im Ruhezustand aktivieren, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-13	KRYPTOGRAFISCHER SCHUTZ	sns-encrypted-kms	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass Ihre Amazon Simple Notification Service (Amazon SNS) -Themen mit dem AWS Key Management Service (AWS KMS) verschlüsselt werden müssen. Um eventuell vorhandene sensible Daten im Ruhezustand in veröffentlichten Nachrichten zu schützen, muss die Verschlüsselung von Daten im Ruhezustand aktiviert sein.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-13	KRYPTOGRA FISCHER SCHUTZ	redshift-cluster-kms-enabled	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass die Verschlüs selung mit AWS Key Management Service (AWS KMS) für Ihren Amazon Redshift Redshift-Cluster aktiviert ist. Um eventuell vorhanden e sensible Daten im Ruhezustand in Redshift-Clustern zu schützen, muss die Verschlüsselung von Daten im Ruhezusta nd aktiviert sein.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SI-2	FEHLERKORREKTUR	ec2-managerinstance-managed-by-systems	Eine Bestandsaufnahme der Softwareplattformen und Anwendungen innerhalb des Unternehmens ist möglich, indem Amazon Elastic Compute Cloud (Amazon EC2) - Instances mit AWS Systems Manager verwaltet werden. Verwenden Sie AWS Systems Manager, um detaillierte Systemkonfigurationen, Betriebssystem-Patch-Levels, Namen und Typ der Dienste, Softwareinstallationen, Anwendungsname, Herausgeber und Version sowie andere Details zu Ihrer Umgebung bereitzustellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SI-2	FEHLERKOR REKTUR	ec2-check managedin stance-association-compliance-status	Verwenden Sie AWS Systems Manager Associati ons, um bei der Inventarisierung von Softwareplattforme n und Anwendung en innerhalb eines Unternehmens zu helfen. AWS Systems Manager weist Ihren verwaltet en Instanzen einen Konfigurationsstat us zu und ermöglich t es Ihnen, Basiswert e für Betriebss ystem-Patch-Levels , Softwareinstallati onen, Anwendung skonfigurationen und andere Details zu Ihrer Umgebung festzulegen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SI-2	FEHLERKOR REKTUR	ec2-check managedin stance-patch-compl iance-status	Aktivieren Sie diese Regel, um bei der Identifizierung und Dokumentation von Sicherheitslücken in Amazon Elastic Compute Cloud (Amazon EC2) zu helfen. Die Regel prüft, ob die EC2 Amazon-Instance die Patch-Konformität im AWS Systems Manager gemäß den Richtlinien und Verfahren Ihrer Organisation einhält.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SI-2	FEHLERKORREKTUR	elastic-beanstalk-managed-updates-aktiviert	Durch die Aktivierung verwalteter Plattform updates für eine Amazon-Elastic-Beanstalk-Umgebung wird sichergestellt, dass die aktuellen verfügbaren Plattform -Fixes, -Updates und -Features für die Umgebung installiert sind. Eine bewährte Methode zur Sicherung von Systemen besteht darin, stets die aktuellen Patches zu installieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SI-3	FEHLERKOR REKTUR	codebuild-project-envvar-awscred-überprüfen	Stellen Sie sicher, dass die Anmeldeinformationen AWS_ACCESS_KEY_ID AWS_SECRET_ACCESS_KEY nicht in AWS Codebuild-Projektumgebungen vorhanden sind. Speichern Sie diese Variablen nicht als Klartext. Das Speichern dieser Variablen als Klartext bewirkt eine unbeabsichtigte Offenlegung von Daten sowie unberechtigte Zugriffe.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SI-3	FEHLERKORREKTUR	codebuild-project-source-repo-URL-Prüfung	Stellen Sie sicher, dass die URL des Quell-Repositorys GitHub oder des Bitbucket-Quell-Repositorys keine persönlichen Zugriffstoken oder Anmeldeinformationen in Codebuild-Projektumgebungen enthält. AWS Verwende OAuth anstelle von persönlichen Zugriffstoken oder Anmeldedaten die Autorisierung für den Zugriff auf GitHub Bitbucket-Repositorys.
SI-3	FEHLERKORREKTUR	ecs-task-definition-memory-hartes Limit	Durch die Begrenzung des Speichers, der Ihren Containern im Amazon Elastic Container Service (ECS) maximal zur Verfügung steht, verhindern Sie eine Ressourcenüberlastung im Falle eines schädlichen Zugriffs auf Ihre Container.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SI-4	ÜBERWACHUNG DES INFORMATIONSSYSTEMS	alb-waf-enabled	Stellen Sie sicher, dass AWS WAF auf Elastic Load Balancers (ELB) aktiviert ist, um Webanwendungen zu schützen. Eine WAF trägt zum Schutz Ihrer Webanwendungen oder APIs vor gängigen Web-Exploits bei. Diese Web-Exploits können sich auf die Verfügbarkeit auswirken, die Sicherheit gefährden oder übermäßige Ressourcen in Ihrer Umgebung verbrauchen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SI-4	ÜBERWACHUNG DES INFORMATIONSSYSTEMS	api-gw-associated-with-WAF	AWS Mit WAF können Sie eine Reihe von Regeln (als Web Access Control List (Web ACL) bezeichnet) konfigurieren, die Webanfragen auf der Grundlage von anpassbaren Websicherheitsregeln und -bedingungen, die Sie definieren, zulassen, blockieren oder zählen. Stellen Sie sicher, dass Ihre Amazon-API-Gateway-Stufe mit einer WAF-Web-ACL verknüpft ist, um sie vor böswilligen Angriffen zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SI-4	ÜBERWACHUNG DES INFORMATIONSSYSTEMS	guardduty-non-archived-findings	Amazon GuardDuty hilft Ihnen dabei, die Auswirkungen eines Vorfalls zu verstehen, indem es die Ergebnisse nach Schweregrad klassifiziert: niedrig, mittel und hoch. Diese Klassifizierungen können Sie zur Festlegung von entsprechenden Strategien und Prioritäten zur Behebung solcher Vorfälle verwenden. Mit dieser Regel können Sie optional daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7) und daysHighSev (Config Default: 1) für nicht archivierte Ergebnisse festlegen, wie es die Richtlinien Ihrer Organisation erfordern.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SI-4	ÜBERWACHUNG DES INFORMATIONSSYSTEMS	multi-region-cloudtrail-enabled	AWS CloudTrail zeichnet Aktionen und API-Aufrufe der AWS Management Console auf. Sie können feststellen, welche Benutzer und Konten angerufen wurden AWS, von welcher Quell-IP-Adresse aus die Anrufe getätigt wurden und wann die Anrufe erfolgten. CloudTrail übermittelt Protokolldateien aus allen AWS Regionen an Ihren S3-Bucket , wenn MULTI_REGION_CLOUD_TRAIL_ENABLED aktiviert ist. Außerdem wird beim AWS Start einer neuen Region derselbe Trail in der neuen Region erstellt. CloudTrail Dadurch erhalten Sie automatisch Protokolldateien mit API-Aktivitäten für die neue Region.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SI-4	ÜBERWACHUNG DES INFORMATIONSSYSTEMS	securityhub-enabled	AWS Security Hub hilft bei der Überwachung von unbefugtem Personal, Verbindungen, Geräten und Software. AWS Security Hub aggregiert, organisiert und priorisiert die Sicherheitswarnungen oder Ergebnisse mehrerer Dienste. AWS Einige dieser Dienste sind Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer und AWS Firewall Manager sowie AWS Partnerlösungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SI-4	ÜBERWACHUNG DES INFORMATIONSSYSTEMS	wafv2-logging-enabled	Um Ihnen bei der Protokollierung und Überwachung in Ihrer Umgebung zu helfen, aktivieren Sie die AWS WAF (V2) -Protokollierung im regionalen und globalen Web. ACLs AWS Die WAF-Protokollierung bietet detaillierte Informationen über den Datenverkehr, der von Ihrer Web-ACL analysiert wird. In den Protokollen werden die Uhrzeit aufgezeichnet, zu der die AWS WAF die Anfrage von Ihrer AWS Ressource erhalten hat, Informationen über die Anfrage und eine Aktion für die Regel, der jede Anfrage entsprach.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SI-4	ÜBERWACHUNG DES INFORMATIONSSYSTEMS	cloud-trail-cloud-watch-logs-aktiviert	Verwenden Sie Amazon CloudWatch , um Protokoll ereignisaktivitäten zentral zu sammeln und zu verwalten. Die Aufnahme von AWS CloudTrail Daten liefert Einzelheiten zu den API-Aufrufaktivitäten in Ihrem AWS-Konto.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SI-4	ÜBERWACHUNG DES INFORMATIONSSYSTEMS	cloudtrail-enabled	AWS CloudTrail kann bei der Nichtabstreitbarkeit helfen, indem Aktionen und API-Aufrufe der AWS Management Console aufgezeichnet werden. Sie können die Benutzer und die Benutzer AWS-Konten , die einen AWS Dienst aufgerufen haben, die Quell-IP-Adresse, über die die Aufrufe generiert wurden, und den Zeitpunkt der Anrufe identifizieren. Einzelheiten zu den erfassten Daten finden Sie unter Inhalt des AWS CloudTrail Datensatzes.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SI-4	ÜBERWACHUNG DES INFORMATIONSSYSTEMS	cloudtrail-s3-dataevents-enabled	Die Erfassung von Simple Storage Service (Amazon S3)-Datenereignissen unterstützt die Erkennung von ungewöhnlichen Aktivitäten. Zu den Details gehören AWS-Konto Informationen über den Zugriff auf einen Amazon S3 S3-Bucket, die IP-Adresse und die Uhrzeit des Ereignisses.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SI-4	ÜBERWACHUNG DES INFORMATIONSSYSTEMS	cloudwatch-alarm-action-check	Amazon CloudWatch alarmiert, wenn eine Metrik den Schwellenwert für eine bestimmte Anzahl von Bewertungszeiträumen überschreitet. Der Alarm führt eine oder mehrere Aktionen durch, die vom Wert der Metrik oder des Ausdrucks im Vergleich zu einem Schwellenwert in einer Reihe von Zeiträumen abhängt. Diese Regel erfordert einen Wert für alarmActionRequired (Config Default: True), insufficientDataAction Required (Config Default: True), okActionRequired (Config Default: False). Der tatsächliche Wert muss die Alarmaktionen für Ihre Umgebung widerspiegeln.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SI-4	ÜBERWACHUNG DES INFORMATIONSSYSTEMS	ec2- instance-detailed-monitoring-enabled	Aktivieren Sie diese Regel, um die Amazon Elastic Compute Cloud (Amazon EC2) - Instance-Überwachung auf der EC2 Amazon-Konsole zu verbessern, in der Monitoring-Diagramme mit einem Zeitraum von 1 Minute für die Instance angezeigt werden.
SI-4	ÜBERWACHUNG DES INFORMATIONSSYSTEMS	guardduty-enabled-centralized	Amazon GuardDuty kann mithilfe von Threat Intelligence Feeds helfen, potenzielle Cybersicherheitsereignisse zu überwachen und zu erkennen. Dazu gehören Listen mit bösartigen IPs und maschinellen Lernmethoden zur Identifizierung unerwarteter, nicht autorisierter und bösartiger Aktivitäten in Ihrer AWS Cloud-Umgebung.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SI-4	ÜBERWACHUNG DES INFORMATIONSSYSTEMS	redshift-cluster-configuration-check	Um Daten im Ruhezustand zu schützen, muss die Verschlüsselung für Ihre Amazon-Redshift-Cluster aktiviert sein. Sie müssen auch sicherstellen, dass die erforderlichen Konfigurationen auf Amazon-Redshift-Clustern bereitgestellt werden. Die Prüfungsprotokollierung muss aktiviert sein, um Informationen zu Verbindungen und Benutzeraktivitäten in der Datenbank bereitzustellen. Diese Regel erfordert, dass ein Wert für clusterDbEncrypted (Config Default: TRUE) und LoggingEnabled (Config Default: TRUE) gesetzt ist. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SI-5	SICHERHEITSWARNUNGEN, HINWEISE UND RICHTLINIEN	cloudwatch-alarm-action-check	Amazon CloudWatch alarmiert, wenn eine Metrik den Schwellenwert für eine bestimmte Anzahl von Bewertungszeiträumen überschreitet. Der Alarm führt eine oder mehrere Aktionen durch, die vom Wert der Metrik oder des Ausdrucks im Vergleich zu einem Schwellenwert in einer Reihe von Zeiträumen abhängt. Diese Regel erfordert einen Wert für alarmActionRequired (Config Default: True), insufficientDataAction Required (Config Default: True), okActionRequired (Config Default: False). Der tatsächliche Wert muss die Alarmaktionen für Ihre Umgebung widerspiegeln.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SI-5	SICHERHEITSWARNUNGEN, HINWEISE UND RICHTLINIEN	guardduty-enabled-centralized	Amazon GuardDuty kann mithilfe von Threat Intelligence Feeds helfen, potenzielle Cybersicherheitsereignisse zu überwachen und zu erkennen. Dazu gehören Listen mit bösartigen IPs und maschinellen Lernmethoden zur Identifizierung unerwarteter, nicht autorisierter und bösartiger Aktivitäten in Ihrer AWS Cloud-Umgebung.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SI-5	SICHERHEITSWARNUNGEN, HINWEISE UND RICHTLINIEN	guardduty-non-archived-findings	Amazon GuardDuty hilft Ihnen dabei, die Auswirkungen eines Vorfalls zu verstehen, indem es die Ergebnisse nach Schweregrad klassifiziert: niedrig, mittel und hoch. Diese Klassifizierungen können Sie zur Festlegung von entsprechenden Strategien und Prioritäten zur Behebung solcher Vorfälle verwenden. Mit dieser Regel können Sie optional daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7) und daysHighSev (Config Default: 1) für nicht archivierte Ergebnisse festlegen, wie es die Richtlinien Ihrer Organisation erfordern.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SI-5	SICHERHEITSWARNUNGEN, HINWEISE UND RICHTLINIEN	securityhub-enabled	AWS Security Hub hilft bei der Überwachung von unbefugtem Personal, Verbindungen, Geräten und Software. AWS Security Hub aggregiert, organisiert und priorisiert die Sicherheitswarnungen oder Ergebnisse mehrerer Dienste. AWS Einige dieser Dienste sind Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer und AWS Firewall Manager sowie AWS Partnerlösungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SI-12	VERARBEITUNG UND AUFBEWAHRUNG VON INFORMATIONEN	aurora-resources-protected-by-Backup-Plan	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon Aurora Aurora-Ressourcen Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SI-12	VERARBEITUNG UND AUFBEWAHRUNG VON INFORMATIONEN	backup-plan-min-frequency-and-min-retention-check	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihr AWS Backup-Plan auf eine Mindestfrequenz und Aufbewahrung festgelegt ist. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen. Mit dieser Regel können Sie die Parameter requiredFrequencyValue (Config default: 1), requiredRetentionDays (Config default: 35) und requiredFrequencyUnit

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			(Config default: days) festlegen. Der tatsächliche Wert muss den Anforderungen Ihrer Organisation entsprechen.
SI-12	VERARBEITUNG UND AUFBEWAHRUNG VON INFORMATIONEN	cw-loggroup-retention-period-überprüfen	Stellen Sie sicher, dass die Ereignisprotokolldaten für Ihre Protokollgruppen über eine Mindestdauer aufbewahrt werden, um die Fehlerbehebung und forensische Untersuchungen zu unterstützen. Fehlende frühere Ereignisprotokolldaten erschweren die Rekonstruierung und Identifizierung potenziell schädlicher Ereignisse.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SI-12	VERARBEITUNG UND AUFBEWAHRUNG VON INFORMATIONEN	dynamodb-resources-protected-by-Ersatzplan	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon DynamoDB DynamoDB-Ressourcen Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SI-12	VERARBEITUNG UND AUFBEWAHRUNG VON INFORMATIONEN	ebs-resources-protected-by-Backup-Plan	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon Elastic Block Store (Amazon EBS) -Ressourcen Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SI-12	VERARBEITUNG UND AUFBEWAHRUNG VON INFORMATIONEN	ec2--Plan resources-protected-by-backup	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon Elastic Compute Cloud (Amazon EC2) -Ressourcen Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SI-12	VERARBEITUNG UND AUFBEWAHRUNG VON INFORMATIONEN	efs-resources-protected-by-Backup-Plan	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon Elastic File System (Amazon EFS) -Dateisysteme Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SI-12	VERARBEITUNG UND AUFBEWAHRUNG VON INFORMATIONEN	fsx-resources-protected-by-Backup-Plan	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre FSx Amazon-Dateisysteme Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SI-12	VERARBEITUNG UND AUFBEWAHRUNG VON INFORMATIONEN	rds-resources-protected-by-Backup-Plan	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon Relational Database Service (Amazon RDS) -Ressourcen Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SI-12	VERARBEITUNG UND AUFBEWAHRUNG VON INFORMATIONEN	redshift-backup-enabled	Stellen Sie zur Unterstützung der Datensicherungsprozesse sicher, dass Ihre Amazon-Redshift-Cluster über automatisierte Snapshots verfügen. Wenn automatisierte Snapshots für einen Cluster aktiviert sind, erstellt Redshift in regelmäßigen Abständen Snapshots dieses Clusters. Standardmäßig erstellt Redshift alle acht Stunden oder alle 5 GB einen Snapshot für jeden Knoten mit Datenänderungen oder je nachdem, was zuerst eintritt.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SI-12	VERARBEITUNG UND AUFBEWAHRUNG VON INFORMATIONEN	db-instance-backup-enabled	Die Sicherungsfunktion von Amazon RDS erstellt Sicherungen Ihrer Datenbanken und Transaktionsprotokolle. Amazon RDS erstellt einen Snapshot für das Speichervolume Ihrer DB-Instance, sodass die gesamte DB-Instance gesichert wird. Sie können im System spezifische Aufbewahrungsfristen festlegen, um Ihre Ausfallsicherheitsanforderungen zu erfüllen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SI-12	VERARBEITUNG UND AUFBEWAHRUNG VON INFORMATIONEN	dynamodb-pitr-enabled	Aktivieren Sie diese Regel, um zu überprüfen, ob die Informationen gesichert wurden. Es verwaltet auch die Backups, indem es sicherstellt, dass die point-in-time Wiederherstellung in Amazon DynamoDB aktiviert ist. Bei der Wiederherstellung werden fortlaufende Backups Ihrer Tabelle für die letzten 35 Tage gespeichert.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SI-12	VERARBEITUNG UND AUFBEWAHRUNG VON INFORMATIONEN	elasticache-redis-cluster-automatic-Backup-Prüfung	Wenn automatische Backups aktiviert sind, ElastiCache erstellt Amazon täglich ein Backup des Clusters. Die Sicherung kann für eine von Ihrer Organisation festgelegte Anzahl von Tagen aufbewahrt werden. Automatische Backups schützen vor Datenverlust. Bei einem Ausfall können Sie einen neuen Cluster erstellen, der Ihre Daten aus dem aktuellen Backup wiederherstellt.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SI-12	VERARBEITUNG UND AUFBEWAHRUNG VON INFORMATIONEN	s-3 bucket-versioning-enabled	Die Versionsverwaltung von Amazon Simple Storage Service (Amazon S3)-Buckets hilft dabei, mehrere Varianten eines Objekts im selben Amazon-S3-Bucket zu speichern. Verwenden Sie die Versionsverwaltung, um sämtliche Versionen aller Objekte in Ihrem Amazon-S3-Bucket zu speichern, abzurufen oder wiederherzustellen. Mit der Versionsverwaltung können Sie Versionen sowohl nach unbeabsichtigten Benutzeraktionen als auch nach Anwendungsfehlern problemlos wiederherstellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SI-16	SPEICHERSCHUTZ	ecs-task-definition-memory-hartes Limit	Durch die Begrenzung des Speichers, der Ihren Container im Amazon Elastic Container Service (ECS) maximal zur Verfügung steht, verhindern Sie eine Ressourcenüberlastung im Falle eines schädlichen Zugriffs auf Ihre Container.

Vorlage

Die Vorlage ist verfügbar unter GitHub: Operational Best Practices for FedRAMP (Low).

Bewährte Methoden für die Ausführung von FedRAMP(Moderate)

Konformitätspakete bieten ein allgemeines Compliance-Framework, das es Ihnen ermöglicht, mithilfe verwalteter oder benutzerdefinierter Regeln und Abhilfemaßnahmen Kontrollen zur Sicherheits-, Betriebs- oder Kostenoptimierung durchzuführen. AWS Config AWS Config Conformance Packs dienen als Beispielvorlagen nicht dazu, die vollständige Einhaltung eines bestimmten Governance- oder Compliance-Standards sicherzustellen. Sie sind dafür verantwortlich, selbst zu beurteilen, ob Ihre Nutzung der Services den geltenden gesetzlichen und behördlichen Anforderungen entspricht.

Im Folgenden finden Sie ein Beispiel für eine Zuordnung zwischen dem Federal Risk and Authorization Management Program (FedRAMP) und AWS verwalteten Konfigurationsregeln. Jede Config-Regel gilt für eine bestimmte AWS Ressource und bezieht sich auf ein oder mehrere FedRAMP-Steuerelemente. Eine FedRAMP-Kontrolle kann mehreren Config-Regeln zugeordnet werden. In der folgenden Tabelle finden Sie weitere Informationen und Anleitungen zu diesen Zuordnungen.

Dieses Konformitätspaket wurde von AWS Security Assurance Services LLC (AWS SAS) validiert. Dabei handelt es sich um ein Team von qualifizierten Sicherheitsbewertern (QSAs) für die

Zahlungskartenbranche (), HITRUST-zertifizierten Common Security Framework Practitionern (CCSFPs) und Compliance-Experten, die für die Beratung und Bewertung verschiedener Branchen-Frameworks zertifiziert sind. AWS Die Experten von SAS haben dieses Conformance Pack so konzipiert, dass ein Kunde sich an einer Teilmenge der FedRAMP-Kontrollen orientieren kann.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
AC-2(1)	Die Organisation wendet automatisierte Mechanismen an, um die Verwaltung von Informationssystem konten zu unterstüt zen.	iam-no-inline-policy-überprüfen	Stellen Sie sicher, dass ein Benutzer, eine IAM-Rolle oder eine IAM-Gruppe (AWS Identity and Access Management) nicht über eine Inline-Richtlinie zur Zugriffsk ontrolle auf Systeme und Ressource n verfügt. AWS empfiehlt, verwaltet e Richtlinien anstelle von Inline-Richtlinien zu verwenden. Verwaltete Richtlini en ermöglichen Wiederverwendbarke it, Versionsverwaltung , Rollback und Delegierung der Berechtigungsverwa ltung.
AC-2(1)	Die Organisation wendet automatisierte Mechanismen an, um die Verwaltung von Informationssystem	securityhub-enabled	AWS Security Hub hilft bei der Überwachung von unbefugtem Personal, Verbindun

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
	konten zu unterstützen.		gen, Geräten und Software. AWS Security Hub aggregiert, organisiert und priorisiert die Sicherheitswarnungen oder Ergebnisse mehrerer Dienste. AWS Einige dieser Dienste sind Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer und AWS Firewall Manager sowie AWS Partnerlösungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
AC-2(1)	Die Organisation wendet automatisierte Mechanismen an, um die Verwaltung von Informationssystem konten zu unterstüt zen.	access-keys-rotated	Die Anmeldein formationen für autorisierte Geräte, Benutzer und Prozesse werden geprüft, indem sichergestellt wird, dass die IAM-Zugri ffsschlüssel gemäß den Vorgaben der Unternehmensrichtl inie rotiert werden. Das regelmäßi ge Ändern der Zugriffsschlüssel ist eine bewährte Sicherheitsmethode . Es verkürzt den Zeitraum, in dem ein Zugriffsschlüssel aktiv ist, und reduziert die Auswirkungen auf das Unternehmen, wenn die Schlüssel kompromittiert werden. Diese Regel erfordert einen Wert für die Zugriffsschlüssel-Rotation (Standard konfiguration: 90). Der tatsächliche Wert muss den Richtlini

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
			en Ihrer Organisation entsprechen.
AC-2(1)	Die Organisation wendet automatisierte Mechanismen an, um die Verwaltung von Informationssystem konten zu unterstüt zen.	guardduty-enabled-centralized	Amazon GuardDuty kann mithilfe von Threat Intellige nce Feeds helfen, potenzielle Cybersich erheitsereignisse zu überwachen und zu erkennen. Dazu gehören Listen mit bösartigen IPs und maschinellen Lernmethoden, um unerwartete, unbefugte und bösartige Aktivitäten in Ihrer AWS Cloud-Umgebung zu identifiz ieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
AC-2(1)	Die Organisation wendet automatisierte Mechanismen an, um die Verwaltung von Informationssystem konten zu unterstüt zen.	iam-password-policy	Die Identitäten und Anmeldeinformation en werden auf der Grundlage einer organisatorischen IAM-Passwortrichtlinie ausgestellt, verwaltet und verifiziert. Sie erfüllen oder übertreff en die Anforderungen von NIST SP 800-63 und dem Standard „Best Practices“ von AWS Foundatio nal Security für die Passwortstärke. Mit dieser Regel können Sie optional RequireUppercaseCh aracters (Wert für AWS grundlegende Sicherheitsbewährt e Methoden: wahr), RequireLowercaseCh aracters (Wert für bewährte Methoden für AWS grundlege nde Sicherheit: wahr), RequireSy mbols (Wert für bewährte Methoden für AWS grundlege nde Sicherheit:

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
			wahr), RequireNumbers (Wert für bewährte Methoden für AWS grundlegende Sicherheit: wahr), MinimumPasswordLength (Wert für bewährte Methoden für AWS grundlegende Sicherheit: 14), PasswordReusePrevention (Wert für bewährte Methoden für AWS grundlegende Sicherheit: 24) und MaxPasswordAge (Wert für bewährte Methoden für AWS grundlegende Sicherheit: 90) für Ihr IAM festlegen Kennwortrichtlinie. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
AC-2(1)	Die Organisation wendet automatisierte Mechanismen an, um die Verwaltung von Informationssystem konten zu unterstüt zen.	iam-policy-no-stat ements-with-admin-access	AWS Identity and Access Managemen t (IAM) kann Ihnen dabei helfen, die Prinzipien der geringsten Rechte und der Aufgabent rennung in Zugriffsb erechtigungen und Autorisierungen zu integrieren und so zu verhindern, dass Richtlinien „Effect“: „Allow“ mit „Action“: „*“ anstelle von „Resource“: „*“ enthalten. Wenn Benutzern mehr Rechte eingeräum t werden, als für die Ausführung einer Aufgabe erforderl ich sind, kann dies gegen das Prinzip der geringsten Berechtigung und der Aufgabentrennung verstoßen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
AC-2(1)	Die Organisation wendet automatisierte Mechanismen an, um die Verwaltung von Informationssystem konten zu unterstüt zen.	iam-root-access-key-überprüfen	Der Zugriff auf Systeme und Ressourcen kann gesteuert werden, indem überprüft wird, ob der Root-Benu tzer keine Zugriffss chlüssel mit seiner AWS Identity and Access Management (IAM) -Rolle verknüpft hat. Stellen Sie sicher, dass die Root-Zugr iffsschlüssel gelöscht werden. Erstellen und verwenden Sie stattdessen rollenbas ierte Funktionen, AWS-Konten um das Prinzip der geringste n Funktionalität zu berücksichtigen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
AC-2(1)	Die Organisation wendet automatisierte Mechanismen an, um die Verwaltung von Informationssystem konten zu unterstüt zen.	iam-user-group-mem bership-überprüfen	AWS Identity and Access Managemen t (IAM) kann Ihnen helfen, Zugriffsb erechtigungen und Autorisierungen einzuschränken, indem sichergestellt wird, dass Benutzer Mitglieder mindesten s einer Gruppe sind. Wenn Benutzern mehr Berechtigungen eingeräumt werden, als für die Ausführun g einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringste n Berechtigung und Aufgabentrennung verstoßen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
AC-2(1)	Die Organisation wendet automatisierte Mechanismen an, um die Verwaltung von Informationssystem konten zu unterstüt zen.	iam-user-mfa-enabled	Aktivieren Sie diese Regel, um den Zugriff auf Ressourcen in der AWS Cloud einzuschr änken. Diese Regel sorgt dafür, dass die Multi-Faktor-Authe ntifizierung (MFA) für alle Benutzer aktiviert ist. MFA sorgt für eine weitere Schutzebe ne zusätzlich zu den Anmeldeinformation en. Reduzieren Sie Fälle von kompromit tierten Konten, indem Sie MFA für Benutzer vorschreiben.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
AC-2(1)	Die Organisation wendet automatisierte Mechanismen an, um die Verwaltung von Informationssystem konten zu unterstüt zen.	iam-user-no-policies-überprüfen	Diese Regel stellt sicher, dass AWS Identity and Access Management (IAM) -Richtlinien nur Gruppen oder Rollen zugewiese n werden, um den Zugriff auf Systeme und Ressourcen zu kontrollieren. Die Zuweisung von Berechtig ungen auf Gruppen- oder Rollenebene trägt dazu bei, die Wahrscheinlichkeit zu verringern, dass eine Identität übermäßige Berechtigungen erhält oder beibehält.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
AC-2(1)	Die Organisation wendet automatisierte Mechanismen an, um die Verwaltung von Informationssystem konten zu unterstüt zen.	iam-user-unused-cr edentials-überprüfen	AWS Identity and Access Managemen t (IAM) kann Ihnen bei Zugriffsberechtigu ngen und Autorisie rungen helfen, indem es nach IAM-Passw örtern und Zugriffss chlüsseln sucht, die für einen bestimmte n Zeitraum nicht verwendet wurden. Wenn ungenutzte Anmeldeinformation en identifiziert werden, müssen Sie sie deaktivieren und/oder entfernen , da dies gegen das Prinzip der geringste n Berechtigung verstoßen könnte. Für diese Regel müssen Sie einen Wert für das maxCreden tialUsage Alter festlegen (Standard konfiguration: 90). Der tatsächliche Wert muss den Richtlini en Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
AC-2(1)	Die Organisation wendet automatisierte Mechanismen an, um die Verwaltung von Informationssystem konten zu unterstüt zen.	mfa-enabled-for-iam-Konsolenzugriff	Verwalten Sie den Zugriff auf Ressource n in der AWS Cloud, indem Sie sicherste llen, dass MFA für alle AWS Identity and Access Managemen t (IAM) -Benutzer aktiviert ist, die über ein Konsolenk ennwort verfügen. MFA sorgt für eine weitere Schutzebe ne zusätzlich zu den Anmeldeinformation en. Indem Sie MFA für Benutzer vorschrei ben, können Sie Fälle kompromittierter Konten reduzieren und verhindern, dass unbefugte Benutzer auf vertrauliche Daten zugreifen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
AC-2(1)	Die Organisation wendet automatisierte Mechanismen an, um die Verwaltung von Informationssystem konten zu unterstützen.	root-account-hardware-mfa-aktiviert	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Hardware-MFA für den Root-Benutzer aktiviert ist. Der Stammbenutzer ist der AWS-Konto-Benutzer mit den meisten Berechtigungen. MFA sorgt für eine weitere Schutzebene zusätzlich zu den Anmeldeinformationen. Indem Sie MFA für den Root-Benutzer vorschreiben, können Sie die Anzahl AWS-Konten kompromittierter Benutzer reduzieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
AC-2(1)	Die Organisation wendet automatisierte Mechanismen an, um die Verwaltung von Informationssystem konten zu unterstüt zen.	root-account-mfa-e nabled	Verwalten Sie den Zugriff auf Ressource n in der AWS Cloud, indem Sie sicherste llen, dass MFA für den Root-Benutzer aktiviert ist. Der Stammbenutzer ist der AWS-Konto-Benutzer mit den meisten Berechtig ungen. MFA sorgt für eine weitere Schutzebene zusätzlic h zu den Anmeldein formationen. Indem Sie MFA für den Root-Benutzer vorschrei ben, können Sie die Anzahl AWS-Konte n kompromittierter Benutzer reduzieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
AC-2(3)	Das Informati onssystem deaktiviert automatisch inaktive Konten von Benutzern nach 90 Tagen.	iam-password-policy	Die Identitäten und Anmeldeinformation en werden auf der Grundlage einer organisatorischen IAM-Passwortrichtl inie ausgestellt, verwaltet und verifizie rt. Sie erfüllen oder übertreffen die Anforderungen, die von NIST SP 800-63 und dem Standard „Best Practices“ von AWS Foundational Security in Bezug auf die Passworts tärke festgelegt sind. Mit dieser Regel können Sie optional RequireUppercaseCh aracters (Wert für AWS grundlegende Sicherheitsbewährt e Methoden: wahr), RequireLowercaseCh aracters (Wert für bewährte Methoden für AWS grundlege nde Sicherheit: wahr), RequireSy mbols (Wert für bewährte Methoden

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
			für AWS grundlegende Sicherheit: wahr), RequireNumbers (Wert für bewährte Methoden für AWS grundlegende Sicherheit: wahr), MinimumPasswordLength (Wert für bewährte Methoden für AWS grundlegende Sicherheit: 14), PasswordReusePrevention (Wert für bewährte Methoden für AWS grundlegende Sicherheit: 24) und MaxPasswordAge (Wert für bewährte Methoden für AWS grundlegende Sicherheit: 90) für Ihr IAM festlegen Kennwortrichtlinie. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
AC-2(3)	Das Informationssystem deaktiviert automatisch inaktive Konten von Benutzern nach 90 Tagen.	iam-user-unused-credentials-überprüfen	AWS Identity and Access Management (IAM) kann Ihnen bei Zugriffsberechtigungen und Autorisierungen helfen, indem es nach IAM-Passwörtern und Zugriffsschlüsseln sucht, die für einen bestimmten Zeitraum nicht verwendet wurden. Wenn ungenutzte Anmeldeinformationen identifiziert werden, müssen Sie sie deaktivieren und/oder entfernen, da dies gegen das Prinzip der geringsten Berechtigung verstoßen könnte. Für diese Regel müssen Sie einen Wert für das maxCredentialUsage Alter festlegen (Standardkonfiguration: 90). Der tatsächliche Wert muss den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
AC-2(4)	Das Informati onssystem prüft automatisch Aktionen wie die Erstellung, Änderung, Aktivieru ng, Deaktivierung und Entfernung von Konten und benachric htigt [Zuordnung: von der Organisation designierte Mitarbeiter oder Rollen].	codebuild-project-logging-enabled	Stellen Sie sicher, dass die AWS CodeBuild Projektpr otokollierung aktiviert ist, damit Ihre Build-Ausgabeproto kolle entweder an Amazon CloudWatc h oder Amazon Simple Storage Service (Amazon S3) gesendet werden. Build-Ausgabeproto kolle enthalten detaillierte Informati onen zu Ihrem Build-Projekt.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
AC-2(4)	Das Informati onssystem prüft automatisch Aktionen wie die Erstellung, Änderung, Aktivieru ng, Deaktivierung und Entfernung von Konten und benachric htigt [Zuordnung: von der Organisation designierte Mitarbeiter oder Rollen].	multi-region-cloudtrail-enabled	AWS CloudTrail zeichnet Aktionen und API-Aufrufe der AWS Management Console auf. Sie können feststellen, welche Benutzer und Konten angerufen wurden AWS, von welcher Quell-IP-Adresse aus die Anrufe getätigt wurden und wann die Anrufe erfolgten. CloudTrail übermittelt Protokolldateien aus allen AWS Regionen an Ihren S3-Bucket , wenn MULTI_REG ION_CLOUD _TRAIL_ENABLED aktiviert ist. Außerdem wird beim AWS Start einer neuen Region derselbe Trail in der neuen Region erstellt. CloudTrail Dadurch erhalten Sie automatis ch Protokolldateien mit API-Aktivitäten für die neue Region.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
AC-2(4)	Das Informati onssystem prüft automatisch Aktionen wie die Erstellung, Änderung, Aktivieru ng, Deaktivierung und Entfernung von Konten und benachric htigt [Zuordnung: von der Organisation designierte Mitarbeiter oder Rollen].	rds-logging-enabled	Um die Protokoll ierung und Überwachung in Ihrer Umgebung zu erleichtern, stellen Sie sicher, dass die Amazon Relationa l Database Service (Amazon RDS)-Prot okollierung aktiviert ist. Mit der Amazon-RDS-Protokollierung können Sie Ereigniss e wie Verbindungen, Verbindungsabbrüch e, Abfragen oder abgefragte Tabellen erfassen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
AC-2(4)	Das Informati onssystem prüft automatisch Aktionen wie die Erstellung, Änderung, Aktivieru ng, Deaktivierung und Entfernung von Konten und benachric htigt [Zuordnung: von der Organisation designierte Mitarbeiter oder Rollen].	securityhub-enabled	AWS Security Hub hilft bei der Überwachung von unbefugtem Personal, Verbindun gen, Geräten und Software. AWS Security Hub aggregiert, organisie rt und priorisie rt die Sicherhei tswarnungen oder Ergebnisse mehrerer Dienste. AWS Einige dieser Dienste sind Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer und AWS Firewall Manager sowie AWS Partnerlösungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
AC-2(4)	Das Informati onssystem prüft automatisch Aktionen wie die Erstellung, Änderung, Aktivieru ng, Deaktivierung und Entfernung von Konten und benachric htigt [Zuordnung: von der Organisation designierte Mitarbeiter oder Rollen].	cloud-trail-cloud-watch-logs-aktiviert	Verwenden Sie Amazon CloudWatc h , um Protokoll ereignisaktivitäten zentral zu sammeln und zu verwalten. Die Aufnahme von AWS CloudTrail Daten liefert Einzelheiten zu den API-Aufrufaktivitä ten in Ihrem AWS-Konto.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
AC-2(4)	Das Informati onssystem prüft automatisch Aktionen wie die Erstellung, Änderung, Aktivieru ng, Deaktivierung und Entfernung von Konten und benachric htigt [Zuordnung: von der Organisation designierte Mitarbeiter oder Rollen].	cloudtrail-enabled	AWS CloudTrail kann bei der Nichtabst reitbarkeit helfen, indem Aktionen und API-Aufrufe der AWS Management Console aufgezeic hnet werden. Sie können die Benutzer und die Benutzer AWS-Konten , die einen AWS Dienst aufgerufen haben, die Quell-IP-Adresse, über die die Aufrufe generiert wurden, und den Zeitpunkt der Anrufe identifiz ieren. Einzelheiten zu den erfassten Daten finden Sie in den AWS CloudTrail Datensatzinhalten.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
AC-2(4)	Das Informati onssystem prüft automatisch Aktionen wie die Erstellung, Änderung, Aktivieru ng, Deaktivierung und Entfernung von Konten und benachric htigt [Zuordnung: von der Organisation designierte Mitarbeiter oder Rollen].	cloudtrail-s3-data events-enabled	Die Erfassung von Simple Storage Service (Amazon S3)-Datenereigniss en unterstützt die Erkennung von ungewöhnlichen Aktivitäten. Zu den Details gehören AWS-Konto Informationen über den Zugriff auf einen Amazon S3 S3-Bucket, die IP-Adress e und die Uhrzeit des Ereignisses.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
AC-2(4)	Das Informati onssystem prüft automatisch Aktionen wie die Erstellung, Änderung, Aktivieru ng, Deaktivierung und Entfernung von Konten und benachric htigt [Zuordnung: von der Organisation designierte Mitarbeiter oder Rollen].	cloudwatch-alarm-a ction-check	Amazon CloudWatch alarmiert, wenn eine Metrik den Schwellen wert für eine bestimmte Anzahl von Bewertungszeiträum en überschreitet. Der Alarm führt eine oder mehrere Aktionen durch, die vom Wert der Metrik oder des Ausdrucks im Vergleich zu einem Schwellenwert in einer Reihe von Zeiträumen abhängt. Diese Regel erfordert einen Wert für alarmActionRequired (Config Default: True), insufficientDataAc tion Required (Config Default: True), okActionRequired (Config Default: False). Der tatsächli che Wert muss die Alarmaktionen für Ihre Umgebung widerspie geln.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
AC-2(4)	Das Informati onssystem prüft automatisch Aktionen wie die Erstellung, Änderung, Aktivieru ng, Deaktivierung und Entfernung von Konten und benachric htigt [Zuordnung: von der Organisation designierte Mitarbeiter oder Rollen].	guardduty-enabled-centralized	Amazon GuardDuty kann mithilfe von Threat Intellige nce Feeds helfen, potenzielle Cybersich erheitsereignisse zu überwachen und zu erkennen. Dazu gehören Listen mit bösartigen IPs und maschinellen Lernmethoden, um unerwartete, unbefugte und bösartige Aktivitäten in Ihrer AWS Cloud-Umgebung zu identifiz ieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
AC-2(4)	Das Informati onssystem prüft automatisch Aktionen wie die Erstellung, Änderung, Aktivieru ng, Deaktivierung und Entfernung von Konten und benachric htigt [Zuordnung: von der Organisation designierte Mitarbeiter oder Rollen].	redshift-cluster-c onfiguration-check	Um Daten im Ruhezustand zu schützen, muss die Verschlüsselung für Ihre Amazon-Re dshift-Cluster aktiviert sein. Sie müssen auch sicherstellen, dass die erforderl ichen Konfigurationen auf Amazon-Redshift-Clustern bereitges tellt werden. Die Prüfungsprotokolli erung muss aktiviert sein, um Informati onen zu Verbindun gen und Benutzera ktivitäten in der Datenbank bereitzus tellen. Diese Regel erfordert, dass ein Wert für clusterDb Encrypted (Config Default: TRUE) und LoggingEnabled (Config Default: TRUE) gesetzt ist. Die tatsächlichen Werte müssen den Richtlini en Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
AC-2(4)	Das Informati onssystem prüft automatisch Aktionen wie die Erstellung, Änderung, Aktivieru ng, Deaktivierung und Entfernung von Konten und benachric htigt [Zuordnung: von der Organisation designierte Mitarbeiter oder Rollen].	s3- bucket-logging-enabled	Die Amazon Simple Storage Service (Amazon S3)-Serverzugriffs protokollierung bietet eine Methode zur Überwachu ng des Netzwerks im Hinblick auf potenzielle Cybersich erheitsereignisse. Die Ereignisse werden überwacht, indem detaillierte Aufzeichn ungen über die Anfragen erfasst werden, die an einen Amazon-S3-Bucket gestellt wurden. Jeder Zugriffsprotokolle intrag enthält Details zu einer einzelnen Zugriffsanfrage. Zu den Details gehören Anforderer, Bucket-Name, Anforderu ngszeit, Anforderu ngsaktion, Antwortst atus und Fehlercode, falls relevant.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
AC-2(7)	Die Organisation: (a) richtet privilegierte Benutzer ein und verwaltet sie gemäß einem rollenbasierten Zugriffsschema, das den autorisierten Zugriff auf das Informationssystem und die Berechtigungen in Rollen organisiert; (b) überwacht privilegierte Rollenzuweisungen; und (c) ergreift [Zuweisung: von der Organisation festgelegte Aktionen], wenn privilegierte Rollenzuweisungen nicht mehr angemessen sind. Zusätzliche Empfehlungen: Privilegierte Rollen sind von der Organisation definierte Rollen, die Einzelpersonen zugewiesen werden, damit sie bestimmte sicherheitsrelevante Funktionen ausführen	iam-customer-policy-blocked-kms-Aktionen	AWS Identity and Access Management (IAM) kann Ihnen helfen, die Prinzipien der geringsten Rechte und der Aufgabentrennung in Zugriffsberechtigungen und Autorisierungen zu integrieren und so zu verhindern, dass Richtlinien blockierte Aktionen für alle AWS Schlüssel des Key Management Service enthalten. Wenn Benutzer mehr Rechte haben, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und Aufgabentrennung verstoßen. Mit dieser Regel können Sie den Parameter festlegen. blockedActionsPatterns (Wert „AWS Bewährte grundlegende Sicherheitsmethoden“: kms:

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
	können, zu denen normale Benutzer nicht berechtigt sind. Zu diesen privilegi erten Rollen gehört zum Beispiel die Verwaltung von Schlüsseln, Konten, Netzwerken und Systemen, Datenbank en und Websites.		Decrypt, kms:ReEnc ryptFrom). Die tatsächlichen Werte müssen den Richtlini en Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
AC-2(7)	Die Organisation: (a) richtet privilegierte Benutzer ein und verwaltet sie gemäß einem rollenbasierten Zugriffsschema, das den autorisierten Zugriff auf das Informationssystem und die Berechtigungen in Rollen organisiert; (b) überwacht privilegierte Rollenzuweisungen; und (c) ergreift [Zuweisung: von der Organisation festgelegte Aktionen], wenn privilegierte Rollenzuweisungen nicht mehr angemessen sind. Zusätzliche Empfehlungen: Privilegierte Rollen sind von der Organisation definierte Rollen, die Einzelpersonen zugewiesen werden, damit sie bestimmte sicherheitsrelevante Funktionen ausführen	iam-group-has-users-überprüfen	AWS Identity and Access Management (IAM) kann Ihnen helfen, die Prinzipien der geringsten Rechte und der Aufgabentrennung mit Zugriffsberechtigungen und Autorisierungen zu integrieren, indem sichergestellt wird, dass IAM-Gruppen mindestens einen Benutzer haben. Die Einteilung von Benutzern in Gruppen auf der Grundlage der ihnen zugewiesenen Berechtigungen oder ihrer Funktion ist eine Möglichkeit, das Prinzip der geringsten Berechtigung zu implementieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
	können, zu denen normale Benutzer nicht berechtigt sind. Zu diesen privilegi erten Rollen gehört zum Beispiel die Verwaltung von Schlüsseln, Konten, Netzwerken und Systemen, Datenbank en und Websites.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
AC-2(7)	Die Organisation: (a) richtet privilegi erte Benutzer ein und verwaltet sie gemäß einem rollenbas ierten Zugriffss chema, das den autorisierten Zugriff auf das Informati onssystem und die Berechtigungen in Rollen organisiert; (b) überwacht privilegi erte Rollenzuw eisungen; und (c) ergreift [Zuweisung: von der Organisation festgelegte Aktionen] , wenn privilegi erte Rollenzuw eisungen nicht mehr angemesse n sind. Zusätzlic he Empfehlun gen: Privilegierte Rollen sind von der Organisation definierte Rollen, die Einzelpersonen zugewiesen werden, damit sie bestimmte sicherheitsrelevante Funktionen ausführen	iam-inline-policy-blocked-kms-Aktionen	Stellen Sie sicher, dass ein Benutzer, eine IAM-Rolle oder eine IAM-Gruppe (AWS Identity and Access Management) nicht über eine Inline-Richtlinie verfügt, die blockierte Aktionen für alle AWS Schlüssel des Key Management Service zulässt. AWS empfiehlt, verwaltet e Richtlinien anstelle von Inline-Richtlinien zu verwenden. Verwaltete Richtlini en ermöglichen Wiederverwendbarke it, Versionsverwaltung , Rollback und Delegierung der Berechtigungsverwa ltung. Mit dieser Regel können Sie den blockedActionsPatt erns Parameter festlegen. (Wert „AWS Bewährte grundlege nde Sicherhei tsmethoden“: kms: Decrypt, kms:ReEnc ryptFrom). Die

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
	können, zu denen normale Benutzer nicht berechtigt sind. Zu diesen privilegi erten Rollen gehört zum Beispiel die Verwaltung von Schlüsseln, Konten, Netzwerken und Systemen, Datenbank en und Websites.		tatsächlichen Werte müssen den Richtlini en Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
AC-2(7)	Die Organisation: (a) richtet privilegierte Benutzer ein und verwaltet sie gemäß einem rollenbasierten Zugriffsschema, das den autorisierten Zugriff auf das Informationssystem und die Berechtigungen in Rollen organisiert; (b) überwacht privilegierte Rollenzuweisungen; und (c) ergreift [Zuweisung: von der Organisation festgelegte Aktionen], wenn privilegierte Rollenzuweisungen nicht mehr angemessen sind. Zusätzliche Empfehlungen: Privilegierte Rollen sind von der Organisation definierte Rollen, die Einzelpersonen zugewiesen werden, damit sie bestimmte sicherheitsrelevante Funktionen ausführen	iam-no-inline-policy-überprüfen	Stellen Sie sicher, dass ein Benutzer, eine IAM-Rolle oder eine IAM-Gruppe (AWS Identity and Access Management) nicht über eine Inline-Richtlinie zur Zugriffskontrolle auf Systeme und Ressourcen verfügt. AWS empfiehlt, verwaltete Richtlinien anstelle von Inline-Richtlinien zu verwenden. Verwaltete Richtlinien ermöglichen Wiederverwendbarkeit, Versionsverwaltung, Rollback und Delegierung der Berechtigungsverwaltung.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
	können, zu denen normale Benutzer nicht berechtigt sind. Zu diesen privilegi erten Rollen gehört zum Beispiel die Verwaltung von Schlüsseln, Konten, Netzwerken und Systemen, Datenbank en und Websites.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
AC-2(7)	Die Organisation: (a) richtet privilegierte Benutzer ein und verwaltet sie gemäß einem rollenbasierten Zugriffsschema, das den autorisierten Zugriff auf das Informationssystem und die Berechtigungen in Rollen organisiert; (b) überwacht privilegierte Rollenzuweisungen; und (c) ergreift [Zuweisung: von der Organisation festgelegte Aktionen], wenn privilegierte Rollenzuweisungen nicht mehr angemessen sind. Zusätzliche Empfehlungen: Privilegierte Rollen sind von der Organisation definierte Rollen, die Einzelpersonen zugewiesen werden, damit sie bestimmte sicherheitsrelevante Funktionen ausführen	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) kann Ihnen dabei helfen, die Prinzipien der geringsten Rechte und der Aufgabentrennung in Zugriffsberechtigungen und Autorisierungen zu integrieren und so zu verhindern, dass Richtlinien „Effect“: „Allow“ mit „Action“: „*“ anstelle von „Resource“: „*“ enthalten. Wenn Benutzern mehr Rechte eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und der Aufgabentrennung verstoßen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
	können, zu denen normale Benutzer nicht berechtigt sind. Zu diesen privilegi erten Rollen gehört zum Beispiel die Verwaltung von Schlüsseln, Konten, Netzwerken und Systemen, Datenbank en und Websites.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
AC-2(7)	Die Organisation: (a) richtet privilegierte Benutzer ein und verwaltet sie gemäß einem rollenbasierten Zugriffsschema, das den autorisierten Zugriff auf das Informationssystem und die Berechtigungen in Rollen organisiert; (b) überwacht privilegierte Rollenzuweisungen; und (c) ergreift [Zuweisung: von der Organisation festgelegte Aktionen], wenn privilegierte Rollenzuweisungen nicht mehr angemessen sind. Zusätzliche Empfehlungen: Privilegierte Rollen sind von der Organisation definierte Rollen, die Einzelpersonen zugewiesen werden, damit sie bestimmte sicherheitsrelevante Funktionen ausführen	iam-policy-no-statements-with-full-access	Stellen Sie sicher, dass IAM-Aktionen nur auf die benötigten Aktionen beschränkt sind. Wenn Benutzern mehr Rechte eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und der Aufgabentrennung verstoßen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
	können, zu denen normale Benutzer nicht berechtigt sind. Zu diesen privilegi erten Rollen gehört zum Beispiel die Verwaltung von Schlüsseln, Konten, Netzwerken und Systemen, Datenbank en und Websites.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
AC-2(12)(a)	Die Organisation: a. Überwacht die Konten des Informationssystems im Hinblick auf [Zuordnung: von der Organisation definierte untypische Nutzung].	securityhub-enabled	AWS Security Hub hilft bei der Überwachung von unbefugtem Personal, Verbindungen, Geräten und Software. AWS Security Hub aggregiert, organisiert und priorisiert die Sicherheitswarnungen oder Ergebnisse mehrerer Dienste. AWS Einige dieser Dienste sind Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer und AWS Firewall Manager sowie AWS Partnerlösungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
AC-2(12)(a)	Die Organisation: a. Überwacht die Konten des Informationssystems im Hinblick auf [Zuordnung: von der Organisation definierte untypische Nutzung].	guardduty-enabled-centralized	Amazon GuardDuty kann mithilfe von Threat Intelligence Feeds helfen, potenzielle Cybersicherheitsereignisse zu überwachen und zu erkennen. Dazu gehören Listen mit bösartigen IPs und maschinellen Lernmethoden, um unerwartete, unbefugte und bösartige Aktivitäten in Ihrer AWS Cloud-Umgebung zu identifizieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
AC-2(f)	Die Organisation: f. Erstellt, aktiviert, ändert, deaktiviert und entfernt Konten im Informationssystem gemäß [Zuweisung: von der Organisation definierte Verfahren oder Bedingungen].	iam-inline-policy-blocked-kms-Aktionen	Stellen Sie sicher, dass ein Benutzer, eine IAM-Rolle oder eine IAM-Gruppe (AWS Identity and Access Management) nicht über eine Inline-Richtlinie verfügt, die blockierte Aktionen für alle AWS Schlüssel des Key Management Service zulässt. AWS empfiehlt, verwaltete Richtlinien anstelle von Inline-Richtlinien zu verwenden. Verwaltete Richtlinien ermöglichen Wiederverwendbarkeit, Versionsverwaltung, Rollback und Delegierung der Berechtigungsverwaltung. Mit dieser Regel können Sie den blockedActionsPatterns Parameter festlegen. (Wert „AWS Bewährte grundlegende Sicherheitsmethoden“: kms:Decrypt, kms:ReEncryptFrom). Die

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
			tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.
AC-2(f)	Die Organisation: f. Erstellt, aktiviert, ändert, deaktiviert und entfernt Konten im Informationssystem gemäß [Zuweisung: von der Organisation definierte Verfahren oder Bedingungen].	iam-no-inline-policy-überprüfen	Stellen Sie sicher, dass ein Benutzer, eine IAM-Rolle oder eine IAM-Gruppe (AWS Identity and Access Management) nicht über eine Inline-Richtlinie zur Zugriffskontrolle auf Systeme und Ressourcen verfügt. AWS empfiehlt, verwaltete Richtlinien anstelle von Inline-Richtlinien zu verwenden. Verwaltete Richtlinien ermöglichen Wiederverwendbarkeit, Versionsverwaltung, Rollback und Delegierung der Berechtigungsverwaltung.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
AC-2(f)	Die Organisation: f. Erstellt, aktiviert, ändert, deaktiviert und entfernt Konten im Informationssystem gemäß [Zuweisung: von der Organisation definierte Verfahren oder Bedingungen].	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) kann Ihnen dabei helfen, die Prinzipien der geringsten Rechte und der Aufgabentrennung in Zugriffsberechtigungen und Autorisierungen zu integrieren und so zu verhindern, dass Richtlinien „Effect“: „Allow“ mit „Action“: „*“ anstelle von „Resource“: „*“ enthalten. Wenn Benutzern mehr Rechte eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und der Aufgabentrennung verstoßen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
AC-2(f)	Die Organisation: f. Erstellt, aktiviert, ändert, deaktiviert und entfernt Konten im Informationssystem gemäß [Zuweisung: von der Organisation definierte Verfahren oder Bedingungen].	iam-policy-no-statements-with-full-access	Stellen Sie sicher, dass IAM-Aktionen nur auf die benötigten Aktionen beschränkt sind. Wenn Benutzern mehr Rechte eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und der Aufgabentrennung verstoßen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
AC-2(f)	Die Organisation: f. Erstellt, aktiviert, ändert, deaktiviert und entfernt Konten im Informationssystem gemäß [Zuweisung: von der Organisation definierte Verfahren oder Bedingungen].	access-keys-rotated	Die Anmeldein formationen für autorisierte Geräte, Benutzer und Prozesse werden geprüft, indem sichergestellt wird, dass die IAM-Zugri ffsschlüssel entsprech end den Vorgaben der Unternehmensrichtl inie rotiert werden. Das regelmäßi ge Ändern der Zugriffsschlüssel ist eine bewährte Sicherheitsmethode . Es verkürzt den Zeitraum, in dem ein Zugriffsschlüssel aktiv ist, und reduziert die Auswirkungen auf das Unternehmen, wenn die Schlüssel kompromittiert werden. Diese Regel erfordert einen Wert für die Zugriffsschlüssel-Rotation (Standard konfiguration: 90). Der tatsächliche Wert muss den Richtlini

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
			en Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
AC-2(f)	Die Organisation: f. Erstellt, aktiviert, ändert, deaktiviert und entfernt Konten im Informationssystem gemäß [Zuweisung: von der Organisation definierte Verfahren oder Bedingungen].	iam-password-policy	Die Identitäten und Anmeldeinformationen werden auf der Grundlage einer organisatorischen IAM-Passwortrichtlinie ausgestellt, verwaltet und verifiziert. Sie erfüllen oder übertreffen die Anforderungen von NIST SP 800-63 und dem Standard „Best Practices“ von AWS Foundational Security in Bezug auf die Passwortstärke. Mit dieser Regel können Sie optional RequireUppercaseCharacters (Wert für AWS grundlegende Sicherheitsbewährte Methoden: wahr), RequireLowercaseCharacters (Wert für bewährte Methoden für AWS grundlegende Sicherheit: wahr), RequireSymbols (Wert für bewährte Methoden für AWS grundlegende Sicherheit:

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
			wahr), RequireNumbers (Wert für bewährte Methoden für AWS grundlegende Sicherheit: wahr), MinimumPasswordLength (Wert für bewährte Methoden für AWS grundlegende Sicherheit: 14), PasswordReusePrevention (Wert für bewährte Methoden für AWS grundlegende Sicherheit: 24) und MaxPasswordAge (Wert für bewährte Methoden für AWS grundlegende Sicherheit: 90) für Ihr IAM festlegen Kennwortrichtlinie. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
AC-2(f)	Die Organisation: f. Erstellt, aktiviert, ändert, deaktiviert und entfernt Konten im Informationssystem gemäß [Zuweisung: von der Organisation definierte Verfahren oder Bedingungen].	iam-root-access-key-überprüfen	Der Zugriff auf Systeme und Ressourcen kann gesteuert werden, indem überprüft wird, ob der Root-Benutzer keine Zugriffsschlüssel mit seiner AWS Identity and Access Management (IAM) -Rolle verknüpft hat. Stellen Sie sicher, dass die Root-Zugriffsschlüssel gelöscht werden. Erstellen und verwenden Sie stattdessen rollenbasierte Funktionen, AWS-Konten um das Prinzip der geringsten Funktionalität zu berücksichtigen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
AC-2(f)	Die Organisation: f. Erstellt, aktiviert, ändert, deaktiviert und entfernt Konten im Informationssystem gemäß [Zuweisung: von der Organisation definierte Verfahren oder Bedingungen].	iam-user-group-membership-überprüfen	AWS Identity and Access Management (IAM) kann Ihnen helfen, Zugriffsberechtigungen und Autorisierungen einzuschränken, indem sichergestellt wird, dass Benutzer Mitglieder mindestens einer Gruppe sind. Wenn Benutzern mehr Berechtigungen eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und Aufgabentrennung verstoßen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
AC-2(f)	Die Organisation: f. Erstellt, aktiviert, ändert, deaktiviert und entfernt Konten im Informationssystem gemäß [Zuweisung: von der Organisation definierte Verfahren oder Bedingungen].	iam-user-mfa-enabled	Aktivieren Sie diese Regel, um den Zugriff auf Ressourcen in der AWS Cloud einzuschränken. Diese Regel sorgt dafür, dass die Multi-Faktor-Authentifizierung (MFA) für alle Benutzer aktiviert ist. MFA sorgt für eine weitere Schutzebene zusätzlich zu den Anmeldeinformationen. Reduzieren Sie Fälle von kompromittierten Konten, indem Sie MFA für Benutzer vorschreiben.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
AC-2(f)	Die Organisation: f. Erstellt, aktiviert, ändert, deaktiviert und entfernt Konten im Informationssystem gemäß [Zuweisung: von der Organisation definierte Verfahren oder Bedingungen].	iam-user-no-policies-überprüfen	Diese Regel stellt sicher, dass AWS Identity and Access Management (IAM) -Richtlinien nur Gruppen oder Rollen zugewiese n werden, um den Zugriff auf Systeme und Ressourcen zu kontrollieren. Die Zuweisung von Berechtig ungen auf Gruppen- oder Rollenebene trägt dazu bei, die Wahrscheinlichkeit zu verringern, dass eine Identität übermäßige Berechtigungen erhält oder beibehält.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
AC-2(f)	Die Organisation: f. Erstellt, aktiviert, ändert, deaktiviert und entfernt Konten im Informationssystem gemäß [Zuweisung: von der Organisation definierte Verfahren oder Bedingungen].	iam-user-unused-credentials-überprüfen	AWS Identity and Access Management (IAM) kann Ihnen bei Zugriffsberechtigungen und Autorisierungen helfen, indem es nach IAM-Passwörtern und Zugriffsschlüsseln sucht, die für einen bestimmten Zeitraum nicht verwendet wurden. Wenn ungenutzte Anmeldeinformationen identifiziert werden, müssen Sie sie deaktivieren und/oder entfernen, da dies gegen das Prinzip der geringsten Berechtigung verstoßen könnte. Für diese Regel müssen Sie einen Wert für das maxCredentialUsage Alter festlegen (Standardkonfiguration: 90). Der tatsächliche Wert muss den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
AC-2(f)	Die Organisation: f. Erstellt, aktiviert, ändert, deaktiviert und entfernt Konten im Informationssystem gemäß [Zuweisung: von der Organisation definierte Verfahren oder Bedingungen].	mfa-enabled-for-iam-Konsolenzugriff	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass MFA für alle AWS Identity and Access Management (IAM) -Benutzer aktiviert ist, die über ein Konsolenkennwort verfügen. MFA sorgt für eine weitere Schutzebene zusätzlich zu den Anmeldeinformationen. Indem Sie MFA für Benutzer vorschreiben, können Sie Fälle kompromittierter Konten reduzieren und verhindern, dass unbefugte Benutzer auf vertrauliche Daten zugreifen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
AC-2(f)	Die Organisation: f. Erstellt, aktiviert, ändert, deaktiviert und entfernt Konten im Informationssystem gemäß [Zuweisung: von der Organisation definierte Verfahren oder Bedingungen].	root-account-hardware-mfa-aktiviert	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Hardware-MFA für den Root-Benutzer aktiviert ist. Der Stammbenutzer ist der AWS-Konto-Benutzer mit den meisten Berechtigungen. MFA sorgt für eine weitere Schutzebene zusätzlich zu den Anmeldeinformationen. Indem Sie MFA für den Root-Benutzer vorschreiben, können Sie die Anzahl AWS-Konten kompromittierter Benutzer reduzieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
AC-2(f)	Die Organisation: f. Erstellt, aktiviert, ändert, deaktiviert und entfernt Konten im Informationssystem gemäß [Zuweisung: von der Organisation definierte Verfahren oder Bedingungen].	root-account-mfa-enabled	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass MFA für den Root-Benutzer aktiviert ist. Der Stammbenutzer ist der AWS-Konto-Benutzer mit den meisten Berechtigungen. MFA sorgt für eine weitere Schutzebene zusätzlich zu den Anmeldeinformationen. Indem Sie MFA für den Root-Benutzer vorschreiben, können Sie die Anzahl AWS-Konten kompromittierter Benutzer reduzieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
AC-2(g)	Die Organisation: g. Überwacht die Verwendung von Konten im Informationssystem.	api-gw-execution-logging-aktiviert	Die API-Gateway-Protokollierung zeigt detaillierte Ansichten der Benutzer, die auf die API zugegriffen haben, und wie diese Benutzer auf die API zugegriffen haben. Diese Einblicke ermöglichen die Transparenz von Benutzeraktivitäten.
AC-2(g)	Die Organisation: g. Überwacht die Verwendung von Konten im Informationssystem.	codebuild-project-logging-enabled	Stellen Sie sicher, dass die AWS CodeBuild Projektprotokollierung aktiviert ist, damit Ihre Build-Ausgabeprotokolle entweder an Amazon CloudWatch oder Amazon Simple Storage Service (Amazon S3) gesendet werden. Build-Ausgabeprotokolle enthalten detaillierte Informationen zu Ihrem Build-Projekt.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
AC-2(g)	Die Organisation: g. Überwacht die Verwendung von Konten im Informati onssystem.	elasticsearch-logs-to-cloudwatch	Stellen Sie sicher, dass für Amazon OpenSearch Service-Domains Fehlerpro tokolle aktiviert und zur Aufbewahrung und Beantwortung an Amazon CloudWatc h Logs gestreamt werden. Domain-Fehlerprotokolle sind bei Sicherhei ts- und Zugriffsp rüfungen sowie bei der Diagnose von Verfügbarkeitsprob lemen nützlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
AC-2(g)	Die Organisation: g. Überwacht die Verwendung von Konten im Informati onssystem.	multi-region-cloudtrail-enabled	AWS CloudTrail zeichnet Aktionen und API-Aufrufe der AWS Management Console auf. Sie können feststellen, welche Benutzer und Konten angerufen wurden AWS, von welcher Quell-IP-Adresse aus die Anrufe getätigt wurden und wann die Anrufe erfolgten. CloudTrail übermittelt Protokolldateien aus allen AWS Regionen an Ihren S3-Bucket , wenn MULTI_REG ION_CLOUD _TRAIL_ENABLED aktiviert ist. Außerdem wird beim AWS Start einer neuen Region derselbe Trail in der neuen Region erstellt. CloudTrail Dadurch erhalten Sie automatis ch Protokolldateien mit API-Aktivitäten für die neue Region.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
AC-2(g)	Die Organisation: g. Überwacht die Verwendung von Konten im Informati onssystem.	rds-logging-enabled	Um die Protokoll ierung und Überwachung in Ihrer Umgebung zu erleichtern, stellen Sie sicher, dass die Amazon Relationa l Database Service (Amazon RDS)-Prot okollierung aktiviert ist. Mit der Amazon-RDS-Protokollierung können Sie Ereigniss e wie Verbindungen, Verbindungsabbrüch e, Abfragen oder abgefragte Tabellen erfassen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
AC-2(g)	Die Organisation: g. Überwacht die Verwendung von Konten im Informati onssystem.	securityhub-enabled	AWS Security Hub hilft bei der Überwachung von unbefugtem Personal, Verbindun gen, Geräten und Software. AWS Security Hub aggregiert, organisie rt und priorisie rt die Sicherhei tswarnungen oder Ergebnisse mehrerer Dienste. AWS Einige dieser Dienste sind Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer und AWS Firewall Manager sowie AWS Partnerlösungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
AC-2(g)	Die Organisation: g. Überwacht die Verwendung von Konten im Informationssystem.	wafv2-logging-enabled	Um Ihnen bei der Protokollierung und Überwachung in Ihrer Umgebung zu helfen, aktivieren Sie die AWS WAF (V2) -Protokollierung im regionalen und globalen Web. ACLs AWS Die WAF-Protokollierung bietet detaillierte Informationen über den Datenverkehr, der von Ihrer Web-ACL analysiert wird. In den Protokollen werden die Uhrzeit aufgezeichnet, zu der die AWS WAF die Anfrage von Ihrer AWS Ressource erhalten hat, Informationen zu der Anfrage und eine Aktion für die Regel, der jede Anfrage entsprach.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
AC-2(g)	Die Organisation: g. Überwacht die Verwendung von Konten im Informati onssystem.	cloud-trail-cloud-watch-logs-aktiviert	Verwenden Sie Amazon CloudWatc h , um Protokoll ereignisaktivitäten zentral zu sammeln und zu verwalten. Die Aufnahme von AWS CloudTrail Daten liefert Einzelheiten zu den API-Aufrufaktivitä ten in Ihrem AWS-Konto.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
AC-2(g)	Die Organisation: g. Überwacht die Verwendung von Konten im Informati onssystem.	cloudtrail-enabled	AWS CloudTrail kann bei der Nichtabst reitbarkeit helfen, indem Aktionen und API-Aufrufe der AWS Management Console aufgezeic hnet werden. Sie können die Benutzer und die Benutzer AWS-Konten , die einen AWS Dienst aufgerufen haben, die Quell-IP-Adresse, über die die Aufrufe generiert wurden, und den Zeitpunkt der Anrufe identifiz ieren. Einzelheiten zu den erfassten Daten finden Sie in den AWS CloudTrail Datensatzinhalten.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
AC-2(g)	Die Organisation: g. Überwacht die Verwendung von Konten im Informati onssystem.	cloudtrail-s3-data events-enabled	Die Erfassung von Simple Storage Service (Amazon S3)-Datenereigniss en unterstützt die Erkennung von ungewöhnlichen Aktivitäten. Zu den Details gehören AWS-Konto Informationen über den Zugriff auf einen Amazon S3 S3-Bucket, die IP-Adress e und die Uhrzeit des Ereignisses.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
AC-2(g)	Die Organisation: g. Überwacht die Verwendung von Konten im Informati onssystem.	guardduty-enabled-centralized	Amazon GuardDuty kann mithilfe von Threat Intellige nce Feeds helfen, potenzielle Cybersich erheitsereignisse zu überwachen und zu erkennen. Dazu gehören Listen mit bösartigen IPs und maschinellen Lernmethoden, um unerwartete, unbefugte und bösartige Aktivitäten in Ihrer AWS Cloud-Umgebung zu identifiz ieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
AC-2(g)	Die Organisation: g. Überwacht die Verwendung von Konten im Informati onssystem.	opensearch-logs-to-cloudwatch	Stellen Sie sicher, dass für Amazon OpenSearch Service-Domains Fehlerpro tokolle aktiviert und zur Aufbewahr ung und Beantwort ung an Amazon CloudWatch Logs gestreamt werden. OpenSearch Service-Fehlerprotokolle können bei Sicherhei ts- und Zugriffsp rüfungen helfen und bei der Diagnose von Verfügbarkeitsprob lemen helfen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
AC-2(g)	Die Organisation: g. Überwacht die Verwendung von Konten im Informationssystem.	redshift-cluster-configuration-check	Um Daten im Ruhezustand zu schützen, muss die Verschlüsselung für Ihre Amazon-Redshift-Cluster aktiviert sein. Sie müssen auch sicherstellen, dass die erforderlichen Konfigurationen auf Amazon-Redshift-Clustern bereitgestellt werden. Die Prüfungsprotokollierung muss aktiviert sein, um Informationen zu Verbindungen und Benutzeraktivitäten in der Datenbank bereitzustellen. Diese Regel erfordert, dass ein Wert für clusterDbEncrypted (Config Default: TRUE) und LoggingEnabled (Config Default: TRUE) gesetzt ist. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
AC-2(g)	Die Organisation: g. Überwacht die Verwendung von Konten im Informati onssystem.	s3- bucket-logging-enabled	Die Amazon Simple Storage Service (Amazon S3)-Serverzugriffs protokollierung bietet eine Methode zur Überwachu ng des Netzwerks im Hinblick auf potenzielle Cybersich erheitsereignisse. Die Ereignisse werden überwacht, indem detaillierte Aufzeichn ungen über die Anfragen erfasst werden, die an einen Amazon-S3-Bucket gestellt wurden. Jeder Zugriffsprotokolle intrag enthält Details zu einer einzelnen Zugriffsanfrage. Zu den Details gehören Anforderer, Bucket-Name, Anforderu ngszeit, Anforderu ngsaktion, Antwortst atus und Fehlercode, falls relevant.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
AC-2(j)	Die Organisation: j. Überprüft Konten auf deren Einhaltung der Kontoverwaltungsanforderungen [Zuweisung: von der Organisation festgelegte Häufigkeit].	ec2- instance-profile-attached	EC2 Instanzprofile übergeben eine IAM-Rolle an eine EC2 Instance. Das Anhängen eines Instance-Profils an Ihre Instances kann bei der Implementierung von geringsten Berechtigungen und der Berechtigungsverwaltung helfen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
AC-2(j)	Die Organisation: j. Überprüft Konten auf deren Einhaltung der Kontoverwaltungsanforderungen [Zuweisung: von der Organisation festgelegte Häufigkeit].	ecs-task-definition-user-for-host-mode-check	Wenn für eine Aufgabendefinition erhöhte Berechtigungen gelten, liegt das daran, dass der Kunde diesen Konfigurationen ausdrücklich zugestimmt hat. Diese Kontrolle prüft, ob eine unerwartete Berechtigungseskalation vorliegt, wenn für eine Aufgabendefinition das Host-Netzwerk aktiviert ist, die Kunden aber keine erhöhten Berechtigungen aktiviert haben.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
AC-2(j)	Die Organisation: j. Überprüft Konten auf deren Einhaltung der Kontoverwaltungsanforderungen [Zuweisung: von der Organisation festgelegte Häufigkeit].	iam-customer-policy-blocked-kms-Aktionen	AWS Identity and Access Management (IAM) kann Ihnen helfen, die Prinzipien der geringsten Rechte und der Aufgabentrennung in Zugriffsberechtigungen und Autorisierungen zu integrieren und so zu verhindern, dass Richtlinien blockierte Aktionen für alle AWS Schlüssel des Key Management Service enthalten. Wenn Benutzer mehr Rechte haben, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und Aufgabentrennung verstoßen. Mit dieser Regel können Sie den Parameter festlegen. blockedActionsPatterns (Wert „AWS Bewährte grundlegende Sicherheitsmethoden“: kms:

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
			Decrypt, kms:ReEncryptFrom). Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
AC-2(j)	Die Organisation: j. Überprüft Konten auf deren Einhaltung der Kontoverwaltungsanforderungen [Zuweisung: von der Organisation festgelegte Häufigkeit].	iam-inline-policy-blocked-kms-Aktionen	Stellen Sie sicher, dass ein Benutzer, eine IAM-Rolle oder eine IAM-Gruppe (AWS Identity and Access Management) nicht über eine Inline-Richtlinie verfügt, die blockierte Aktionen für alle AWS Schlüssel des Key Management Service zulässt. AWS empfiehlt, verwaltete Richtlinien anstelle von Inline-Richtlinien zu verwenden. Verwaltete Richtlinien ermöglichen Wiederverwendbarkeit, Versionsverwaltung, Rollback und Delegierung der Berechtigungsverwaltung. Mit dieser Regel können Sie den blockedActionsPatterns Parameter festlegen. (Wert „AWS Bewährte grundlegende Sicherheitsmethoden“: kms:Decrypt, kms:ReEncryptFrom). Die

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
			tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.
AC-2(j)	Die Organisation: j. Überprüft Konten auf deren Einhaltung der Kontoverwaltungsanforderungen [Zuweisung: von der Organisation festgelegte Häufigkeit].	iam-no-inline-policy-überprüfen	Stellen Sie sicher, dass ein Benutzer, eine IAM-Rolle oder eine IAM-Gruppe (AWS Identity and Access Management) nicht über eine Inline-Richtlinie zur Zugriffskontrolle auf Systeme und Ressourcen verfügt. AWS empfiehlt, verwaltete Richtlinien anstelle von Inline-Richtlinien zu verwenden. Verwaltete Richtlinien ermöglichen Wiederverwendbarkeit, Versionsverwaltung, Rollback und Delegierung der Berechtigungsverwaltung.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
AC-2(j)	Die Organisation: j. Überprüft Konten auf deren Einhaltung der Kontoverwaltungsanforderungen [Zuweisung: von der Organisation festgelegte Häufigkeit].	iam-policy-no-statements-with-full-access	Stellen Sie sicher, dass IAM-Aktionen nur auf die benötigten Aktionen beschränkt sind. Wenn Benutzern mehr Rechte eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und der Aufgabentrennung verstoßen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
AC-2(j)	Die Organisation: j. Überprüft Konten auf deren Einhaltung der Kontoverwaltungsanforderungen [Zuweisung: von der Organisation festgelegte Häufigkeit].	iam-user-mfa-enabled	Aktivieren Sie diese Regel, um den Zugriff auf Ressourcen in der AWS Cloud einzuschränken. Diese Regel sorgt dafür, dass die Multi-Faktor-Authentifizierung (MFA) für alle Benutzer aktiviert ist. MFA sorgt für eine weitere Schutzebene zusätzlich zu den Anmeldeinformationen. Reduzieren Sie Fälle von kompromittierten Konten, indem Sie MFA für Benutzer vorschreiben.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
AC-2(j)	Die Organisation: j. Überprüft Konten auf deren Einhaltung der Kontoverwaltungsanforderungen [Zuweisung: von der Organisation festgelegte Häufigkeit].	iam-user-unused-credentials-überprüfen	AWS Identity and Access Management (IAM) kann Ihnen bei Zugriffsberechtigungen und Autorisierungen helfen, indem es nach IAM-Passwörtern und Zugriffsschlüsseln sucht, die für einen bestimmten Zeitraum nicht verwendet wurden. Wenn ungenutzte Anmeldeinformationen identifiziert werden, müssen Sie sie deaktivieren und/oder entfernen, da dies gegen das Prinzip der geringsten Berechtigung verstoßen könnte. Für diese Regel müssen Sie einen Wert für das maxCredentialUsage Alter festlegen (Standardkonfiguration: 90). Der tatsächliche Wert muss den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
AC-2(j)	Die Organisation: j. Überprüft Konten auf deren Einhaltung der Kontoverwaltungsanforderungen [Zuweisung: von der Organisation festgelegte Häufigkeit].	mfa-enabled-for-iam-Konsolenzugriff	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass MFA für alle AWS Identity and Access Management (IAM) -Benutzer aktiviert ist, die über ein Konsolenkennwort verfügen. MFA sorgt für eine weitere Schutzebene zusätzlich zu den Anmeldeinformationen. Indem Sie MFA für Benutzer vorschreiben, können Sie Fälle kompromittierter Konten reduzieren und verhindern, dass unbefugte Benutzer auf vertrauliche Daten zugreifen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
AC-2(j)	Die Organisation: j. Überprüft Konten auf deren Einhaltung der Kontoverwaltungsanforderungen [Zuweisung: von der Organisation festgelegte Häufigkeit].	access-keys-rotated	Die Anmeldeinformationen für autorisierte Geräte, Benutzer und Prozesse werden geprüft, indem sichergestellt wird, dass die IAM-Zugriffsschlüssel gemäß den Vorgaben der Unternehmensrichtlinie rotiert werden. Das regelmäßige Ändern der Zugriffsschlüssel ist eine bewährte Sicherheitsmethode. Es verkürzt den Zeitraum, in dem ein Zugriffsschlüssel aktiv ist, und reduziert die Auswirkungen auf das Unternehmen, wenn die Schlüssel kompromittiert werden. Diese Regel erfordert einen Wert für die Zugriffsschlüssel-Rotation (Standardkonfiguration: 90). Der tatsächliche Wert muss den Richtlini

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
			en Ihrer Organisation entsprechen.
AC-2(j)	Die Organisation: j. Überprüft Konten auf deren Einhaltung der Kontoverwaltungsanforderungen [Zuweisung: von der Organisation festgelegte Häufigkeit].	iam-group-has-users-überprüfen	AWS Identity and Access Management (IAM) kann Ihnen helfen, die Prinzipien der geringsten Rechte und der Aufgabentrennung mit Zugriffsberechtigungen und Autorisierungen zu integrieren, indem sichergestellt wird, dass IAM-Gruppen mindestens einen Benutzer haben. Die Einteilung von Benutzern in Gruppen auf der Grundlage der ihnen zugewiesenen Berechtigungen oder ihrer Funktion ist eine Möglichkeit, das Prinzip der geringsten Berechtigung zu implementieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
AC-2(j)	Die Organisation: j. Überprüft Konten auf deren Einhaltung der Kontoverwaltungsanforderungen [Zuweisung: von der Organisation festgelegte Häufigkeit].	iam-password-policy	Die Identitäten und Anmeldeinformationen werden auf der Grundlage einer organisatorischen IAM-Passwortrichtlinie ausgestellt, verwaltet und verifiziert. Sie erfüllen oder übertreffen die Anforderungen von NIST SP 800-63 und dem Standard „Best Practices“ von AWS Foundational Security für die Passwortstärke. Mit dieser Regel können Sie optional RequireUppercaseCharacters (Wert für AWS grundlegende Sicherheitsbewährte Methoden: wahr), RequireLowercaseCharacters (Wert für bewährte Methoden für AWS grundlegende Sicherheit: wahr), RequireSymbols (Wert für bewährte Methoden für AWS grundlegende Sicherheit:

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
			wahr), RequireNumbers (Wert für bewährte Methoden für AWS grundlegende Sicherheit: wahr), MinimumPasswordLength (Wert für bewährte Methoden für AWS grundlegende Sicherheit: 14), PasswordReusePrevention (Wert für bewährte Methoden für AWS grundlegende Sicherheit: 24) und MaxPasswordAge (Wert für bewährte Methoden für AWS grundlegende Sicherheit: 90) für Ihr IAM festlegen Kennwortrichtlinie. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
AC-2(j)	Die Organisation: j. Überprüft Konten auf deren Einhaltung der Kontoverwaltungsanforderungen [Zuweisung: von der Organisation festgelegte Häufigkeit].	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) kann Ihnen dabei helfen, die Prinzipien der geringsten Rechte und der Aufgabentrennung in Zugriffsberechtigungen und Autorisierungen zu integrieren und so zu verhindern, dass Richtlinien „Effect“: „Allow“ mit „Action“: „*“ anstelle von „Resource“: „*“ enthalten. Wenn Benutzern mehr Rechte eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und der Aufgabentrennung verstoßen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
AC-2(j)	Die Organisation: j. Überprüft Konten auf deren Einhaltung der Kontoverwaltungsanforderungen [Zuweisung: von der Organisation festgelegte Häufigkeit].	iam-root-access-key-überprüfen	Der Zugriff auf Systeme und Ressourcen kann gesteuert werden, indem überprüft wird, ob der Root-Benutzer keine Zugriffsschlüssel mit seiner AWS Identity and Access Management (IAM) -Rolle verknüpft hat. Stellen Sie sicher, dass die Root-Zugriffsschlüssel gelöscht werden. Erstellen und verwenden Sie stattdessen rollenbasierte Funktionen, AWS-Konten um das Prinzip der geringsten Funktionalität zu berücksichtigen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
AC-2(j)	Die Organisation: j. Überprüft Konten auf deren Einhaltung der Kontoverwaltungsanforderungen [Zuweisung: von der Organisation festgelegte Häufigkeit].	iam-user-group-membership-überprüfen	AWS Identity and Access Management (IAM) kann Ihnen helfen, Zugriffsberechtigungen und Autorisierungen einzuschränken, indem sichergestellt wird, dass Benutzer Mitglieder mindestens einer Gruppe sind. Wenn Benutzern mehr Berechtigungen eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und Aufgabentrennung verstoßen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
AC-2(j)	Die Organisation: j. Überprüft Konten auf deren Einhaltung der Kontoverwaltungsanforderungen [Zuweisung: von der Organisation festgelegte Häufigkeit].	iam-user-no-policies-überprüfen	Diese Regel stellt sicher, dass AWS Identity and Access Management (IAM) -Richtlinien nur Gruppen oder Rollen zugewiesen werden, um den Zugriff auf Systeme und Ressourcen zu kontrollieren. Die Zuweisung von Berechtigungen auf Gruppen- oder Rollenebene trägt dazu bei, die Wahrscheinlichkeit zu verringern, dass eine Identität übermäßige Berechtigungen erhält oder beibehält.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
AC-2(j)	Die Organisation: j. Überprüft Konten auf deren Einhaltung der Kontoverwaltungsanforderungen [Zuweisung: von der Organisation festgelegte Häufigkeit].	root-account-mfa-enabled	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass MFA für den Root-Benutzer aktiviert ist. Der Stammbenutzer ist der AWS-Konto-Benutzer mit den meisten Berechtigungen. MFA sorgt für eine weitere Schutzebene zusätzlich zu den Anmeldeinformationen. Indem Sie MFA für den Root-Benutzer vorschreiben, können Sie die Anzahl AWS-Konten kompromittierter Benutzer reduzieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
AC-3	Das Informati onssystem setzt genehmigte Autorisie rungen für den logischen Zugriff auf Informationen und Systemressourcen gemäß den geltenden Zugriffskontrollri chtlinien durch.	autoscaling-launch -config-public-ip- deaktiviert	Wenn Sie Ihre Netzwerkschnittstellen mit einer öffentlichen IP-Adresse konfiguri eren, sind die diesen Netzwerkschnittste llen zugehörigen Ressourcen über das Internet erreichba r. EC2 Ressourcen sollten nicht öffentlic h zugänglich sein, da dies einen unbeabsic htigten Zugriff auf Ihre Anwendungen oder Server ermöglichen kann.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
AC-3	Das Informati onssystem setzt genehmigte Autorisie rungen für den logischen Zugriff auf Informationen und Systemressourcen gemäß den geltenden Zugriffskontrollri chtlinien durch.	ec2-imdsv2-check	Stellen Sie sicher, dass die Methode Instance Metadata Service Version 2 (IMDSv2) aktiviert ist, um den Zugriff auf und die Kontrolle der Amazon Elastic Compute Cloud (Amazon EC2) - Instance-Metadate n zu schützen. Die IMDSv2 Methode verwendet sitzungsb asierte Kontrollen. Mit können Kontrolle n implementiert werden IMDSv2, um Änderungen an Instanzmetadaten einzuschränken.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
AC-3	Das Informati onssystem setzt genehmigte Autorisie rungen für den logischen Zugriff auf Informationen und Systemressourcen gemäß den geltenden Zugriffskontrollri chtlinien durch.	ec-2 instance-profile-a ttached	EC2 Instanzprofile übergeben eine IAM-Rolle an eine EC2 Instance. Das Anhängen eines Instance-Profils an Ihre Instances kann bei der Implement ierung von geringste n Berechtigungen und der Berechtig ungsverwaltung helfen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
AC-3	Das Informati onssystem setzt genehmigte Autorisie rungen für den logischen Zugriff auf Informationen und Systemressourcen gemäß den geltenden Zugriffskontrollri chtlinien durch.	ecs-task-definition-user-for-host-mode-check	Wenn für eine Aufgabendefinition erhöhte Berechtig ungen gelten, liegt das daran, dass der Kunde diesen Konfigura tionen ausdrücklich zugestimmt hat. Diese Kontrolle prüft, ob eine unerwartete Berechtigungseskal ation vorliegt, wenn für eine Aufgabend efinition das Host-Netzwerk aktiviert ist, die Kunden aber keine erhöhten Berechtigungen aktiviert haben.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
AC-3	Das Informati onssystem setzt genehmigte Autorisie rungen für den logischen Zugriff auf Informationen und Systemressourcen gemäß den geltenden Zugriffskontrollri chtlinien durch.	iam-no-inline-policy-überprüfen	Stellen Sie sicher, dass ein Benutzer, eine IAM-Rolle oder eine IAM-Gruppe (AWS Identity and Access Management) nicht über eine Inline-Richtlinie zur Zugriffsk ontrolle auf Systeme und Ressource n verfügt. AWS empfiehlt, verwaltet e Richtlinien anstelle von Inline-Richtlinien zu verwenden. Verwaltete Richtlini en ermöglichen Wiederverwendbarke it, Versionsverwaltung , Rollback und Delegierung der Berechtigungsverwa ltung.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
AC-3	Das Informationssystem setzt genehmigte Autorisierungen für den logischen Zugriff auf Informationen und Systemressourcen gemäß den geltenden Zugriffskontrollrichtlinien durch.	iam-policy-no-statements-with-full-access	Stellen Sie sicher, dass IAM-Aktionen nur auf die benötigten Aktionen beschränkt sind. Wenn Benutzern mehr Rechte eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und der Aufgabentrennung verstoßen.
AC-3	Das Informationssystem setzt genehmigte Autorisierungen für den logischen Zugriff auf Informationen und Systemressourcen gemäß den geltenden Zugriffskontrollrichtlinien durch.	ssm-document-not-public	Stellen Sie sicher, dass AWS Systems Manager (SSM) - Dokumente nicht öffentlich sind, da dies einen unbeabsichtigten Zugriff auf Ihre SSM-Dokumente ermöglichen kann. Ein öffentliches SSM-Dokument kann Informationen über Ihr Konto, Ihre Ressourcen und internen Prozesse preisgeben.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
AC-3	Das Informati onssystem setzt genehmigte Autorisie rungen für den logischen Zugriff auf Informationen und Systemressourcen gemäß den geltenden Zugriffskontrollri chtlinien durch.	dms-replication-not-public	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass auf DMS-Replikationsin stanzen nicht öffentlic h zugegriffen werden kann. DMS-Repli kations-Instances können vertrauli che Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.
AC-3	Das Informati onssystem setzt genehmigte Autorisie rungen für den logischen Zugriff auf Informationen und Systemressourcen gemäß den geltenden Zugriffskontrollri chtlinien durch.	ebs-snapshot-public-restorable-überprüfen	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass EBS-Snapshots nicht öffentlich wiederher stellbar sind. EBS-Volume-Snapsho ts können vertrauli che Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
AC-3	Das Informati onssystem setzt genehmigte Autorisie rungen für den logischen Zugriff auf Informationen und Systemressourcen gemäß den geltenden Zugriffskontrollri chtlinien durch.	ec-2 instance-no-public-ip	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon Elastic Compute Cloud (Amazon EC2) - Instances nicht öffentlich zugänglich sind. EC2 Amazon-Instances können vertrauliche Informati onen enthalten, und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
AC-3	Das Informati onssystem setzt genehmigte Autorisie rungen für den logischen Zugriff auf Informationen und Systemressourcen gemäß den geltenden Zugriffskontrollri chtlinien durch.	elasticsearch-in-vpc-only	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherste llen, dass sich Amazon OpenSearc h OpenSearch Service (Service) - Domains innerhalb einer Amazon Virtual Private Cloud (Amazon VPC) befinden. Eine OpenSearch Service-Domain innerhalb einer Amazon VPC ermöglicht die sichere Kommunikation zwischen OpenSearc h Service und anderen Services innerhalb der Amazon VPC, ohne dass ein Internet-Gateway, ein NAT-Gerät oder eine VPN-Verbindung erforderlich ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
AC-3	Das Informati onssystem setzt genehmigte Autorisie rungen für den logischen Zugriff auf Informationen und Systemressourcen gemäß den geltenden Zugriffskontrollri chtlinien durch.	emr-master-no-public-ip	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon EMR-Clust er-Masterknoten nicht öffentlich zugänglic h sind. Amazon-EM R-Cluster-Hauptkno ten können vertrauli che Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
AC-3	Das Informationssystem setzt genehmigte Autorisierungen für den logischen Zugriff auf Informationen und Systemressourcen gemäß den geltenden Zugriffskontrollrichtlinien durch.	iam-group-has-users-überprüfen	AWS Identity and Access Management (IAM) kann Ihnen helfen, die Prinzipien der geringsten Rechte und der Aufgabentrennung mit Zugriffsberechtigungen und Autorisierungen zu integrieren, indem sichergestellt wird, dass IAM-Gruppen mindestens einen Benutzer haben. Die Einteilung von Benutzern in Gruppen auf der Grundlage der ihnen zugewiesenen Berechtigungen oder ihrer Funktion ist eine Möglichkeit, das Prinzip der geringsten Berechtigung zu implementieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
AC-3	Das Informationssystem setzt genehmigte Autorisierungen für den logischen Zugriff auf Informationen und Systemressourcen gemäß den geltenden Zugriffskontrollrichtlinien durch.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) kann Ihnen dabei helfen, die Prinzipien der geringsten Rechte und der Aufgabentrennung in Zugriffsberechtigungen und Autorisierungen zu integrieren und so zu verhindern, dass Richtlinien „Effect“: „Allow“ mit „Action“: „*“ anstelle von „Resource“: „*“ enthalten. Wenn Benutzern mehr Rechte eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und der Aufgabentrennung verstoßen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
AC-3	Das Informati onssystem setzt genehmigte Autorisie rungen für den logischen Zugriff auf Informationen und Systemressourcen gemäß den geltenden Zugriffskontrollri chtlinien durch.	iam-root-access-key-überprüfen	Der Zugriff auf Systeme und Ressourcen kann gesteuert werden, indem überprüft wird, ob der Root-Benu tzer keine Zugriffss chlüssel mit seiner AWS Identity and Access Management (IAM) -Rolle verknüpft hat. Stellen Sie sicher, dass die Root-Zugr iffsschlüssel gelöscht werden. Erstellen und verwenden Sie stattdessen rollenbas ierte Funktionen, AWS-Konten um das Prinzip der geringste n Funktionalität zu berücksichtigen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
AC-3	Das Informationssystem setzt genehmigte Autorisierungen für den logischen Zugriff auf Informationen und Systemressourcen gemäß den geltenden Zugriffskontrollrichtlinien durch.	iam-user-group-membership-überprüfen	AWS Identity and Access Management (IAM) kann Ihnen helfen, Zugriffsberechtigungen und Autorisierungen einzuschränken, indem sichergestellt wird, dass Benutzer Mitglieder mindestens einer Gruppe sind. Wenn Benutzern mehr Berechtigungen eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und Aufgabentrennung verstoßen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
AC-3	Das Informati onssystem setzt genehmigte Autorisie rungen für den logischen Zugriff auf Informationen und Systemressourcen gemäß den geltenden Zugriffskontrollri chtlinien durch.	iam-user-no-policies-überprüfen	Diese Regel stellt sicher, dass AWS Identity and Access Management (IAM) -Richtlinien nur Gruppen oder Rollen zugewiese n werden, um den Zugriff auf Systeme und Ressourcen zu kontrollieren. Die Zuweisung von Berechtig ungen auf Gruppen- oder Rollenebene trägt dazu bei, die Wahrscheinlichkeit zu verringern, dass eine Identität übermäßige Berechtigungen erhält oder beibehält.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
AC-3	Das Informationssystem setzt genehmigte Autorisierungen für den logischen Zugriff auf Informationen und Systemressourcen gemäß den geltenden Zugriffskontrollrichtlinien durch.	iam-user-unused-credentials-überprüfen	AWS Identity and Access Management (IAM) kann Ihnen bei Zugriffsberechtigungen und Autorisierungen helfen, indem es nach IAM-Passwörtern und Zugriffsschlüsseln sucht, die für einen bestimmten Zeitraum nicht verwendet wurden. Wenn ungenutzte Anmeldeinformationen identifiziert werden, müssen Sie sie deaktivieren und/oder entfernen, da dies gegen das Prinzip der geringsten Berechtigung verstoßen könnte. Für diese Regel müssen Sie einen Wert für das maxCredentialUsage Alter festlegen (Standardkonfiguration: 90). Der tatsächliche Wert muss den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
AC-3	Das Informationssystem setzt genehmigte Autorisierungen für den logischen Zugriff auf Informationen und Systemressourcen gemäß den geltenden Zugriffskontrollrichtlinien durch.	lambda-function-public-access-verboten	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass AWS Lambda-Funktionen nicht öffentlich zugänglich sind. Der öffentliche Zugriff kann möglicherweise die Verfügbarkeit von Ressourcen beeinträchtigen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
AC-3	Das Informati onssystem setzt genehmigte Autorisie rungen für den logischen Zugriff auf Informationen und Systemressourcen gemäß den geltenden Zugriffskontrollri chtlinien durch.	lambda-inside-vpc	Stellen Sie AWS Lambda-Funktionen in einer Amazon Virtual Private Cloud (Amazon VPC) bereit, um eine sichere Kommunika tion zwischen einer Funktion und anderen Diensten innerhalb der Amazon VPC zu gewährleisten. Bei dieser Konfiguration sind kein Internet-Gateway, kein NAT-Gerät und keine VPN-Verbindung erforderlich. Der gesamte Datenverk ehr bleibt sicher in der Cloud. AWS Domains, die sich innerhalb einer VPC befinden, verfügen aufgrund ihrer logischen Isolierun g im Vergleich zu Domains mit öffentlic hen Endpunkten über eine zusätzliche Sicherheitsebene. Um den Zugriff ordnungsg emäß zu verwalten,

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
			sollten AWS Lambda-Funktionen einer VPC zugewiesen werden.
AC-3	Das Informationssystem setzt genehmigte Autorisierungen für den logischen Zugriff auf Informationen und Systemressourcen gemäß den geltenden Zugriffskontrollrichtlinien durch.	rds-instance-public-access-überprüfen	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Relational Database Service (Amazon RDS) -Instances nicht öffentlich sind. Amazon-RDS-Datenbank-Instances können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
AC-3	Das Informati onssystem setzt genehmigte Autorisie rungen für den logischen Zugriff auf Informationen und Systemressourcen gemäß den geltenden Zugriffskontrollri chtlinien durch.	rds-snapshots-public-prohibited	Verwalten Sie den Zugriff auf Ressource n in der AWS Cloud, indem Sie sicherste llen, dass Amazon Relational Database Service (Amazon RDS) -Instance s nicht öffentlic h sind. Amazon-RDS-Datenbank-Instances können vertrauliche Informati onen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
AC-3	Das Informati onssystem setzt genehmigte Autorisie rungen für den logischen Zugriff auf Informationen und Systemressourcen gemäß den geltenden Zugriffskontrollri chtlinien durch.	redshift-cluster-public-access-überprüfen	Verwalten Sie den Zugriff auf Ressource n in der AWS Cloud, indem Sie sicherste llen, dass Amazon Redshift Redshift-Cluster nicht öffentlic h sind. Amazon-Re dshift-Cluster können vertrauliche Informati onen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
AC-3	Das Informati onssystem setzt genehmigte Autorisie rungen für den logischen Zugriff auf Informationen und Systemressourcen gemäß den geltenden Zugriffskontrollri chtlinien durch.	s3- -Block-periodisch account-level-public-access	Verwalten Sie den Zugriff auf Ressource n in der AWS Cloud, indem Sie sicherste llen, dass Amazon Simple Storage Service (Amazon S3) -Buckets nicht öffentlich zugänglic h sind. Diese Regel trägt dazu bei, sensible Daten vor unbefugten Remote-Benutzern zu schützen, indem sie den öffentlichen Zugriff verhinder t. Mit dieser Regel können Sie optional die Parameter ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) und restrictPublicBuck ets Parameter (Config Default: True) festlegen. Die tatsächlichen Werte müssen den Richtlini

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
			en Ihrer Organisation entsprechen.
AC-3	Das Informati onssystem setzt genehmigte Autorisie rungen für den logischen Zugriff auf Informationen und Systemressourcen gemäß den geltenden Zugriffskontrollri chtlinien durch.	s3 bucket-level-public-access - verboten	Verwalten Sie den Zugriff auf Ressource n in der AWS Cloud, indem Sie sicherste llen, dass Amazon Simple Storage Service (Amazon S3) -Buckets nicht öffentlich zugänglic h sind. Diese Regel trägt dazu bei, sensible Daten vor unbefugten Remote-Benutzern zu schützen, indem sie den öffentlichen Zugriff auf Bucket-Eb ene verhindert.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
AC-3	Das Informati onssystem setzt genehmigte Autorisie rungen für den logischen Zugriff auf Informationen und Systemressourcen gemäß den geltenden Zugriffskontrollri chtlinien durch.	s-3 bucket-public-read -prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie nur autorisierten Benutzern, Prozessen und Geräten Zugriff auf Amazon Simple Storage Service (Amazon S3) - Buckets gewähren. Die Verwaltung des Zugriffs sollte mit der Klassifizierung der Daten übereinst immen.
AC-3	Das Informati onssystem setzt genehmigte Autorisie rungen für den logischen Zugriff auf Informationen und Systemressourcen gemäß den geltenden Zugriffskontrollri chtlinien durch.	s3- bucket-public-writ e-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie nur autorisierten Benutzern, Prozessen und Geräten Zugriff auf Amazon Simple Storage Service (Amazon S3) - Buckets gewähren. Die Verwaltung des Zugriffs sollte mit der Klassifizierung der Daten übereinst immen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
AC-3	Das Informati onssystem setzt genehmigte Autorisie rungen für den logischen Zugriff auf Informationen und Systemressourcen gemäß den geltenden Zugriffskontrollri chtlinien durch.	sagemaker-notebook -no-direct-Interne tzugang	Verwalten Sie den Zugriff auf Ressource n in der AWS Cloud, indem Sie sicherste llen, dass SageMaker Amazon-Notebooks keinen direkten Internetzugang zulassen. Indem Sie direkten Internetz ugang blockieren, vermeiden Sie, dass unbefugte Benutzer auf sensible Daten zugreifen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
AC-3	Das Informati onssystem setzt genehmigte Autorisie rungen für den logischen Zugriff auf Informationen und Systemressourcen gemäß den geltenden Zugriffskontrollri chtlinien durch.	subnet-auto-assign-public-ip-deaktiviert	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon Virtual Private Cloud (VPC) -Subnetzen nicht automatisch eine öffentliche IP-Adress e zugewiesen wird. Amazon Elastic Compute Cloud (EC2) -Instances, die in Subnetzen gestartet werden, in denen dieses Attribut aktiviert ist, haben ihrer primären Netzwerkschnittste lle eine öffentliche IP-Adresse zugewiesen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
AC-4	Das Informati onssystem setzt genehmigte Autorisie rungen für die Kontrolle des Informationsflusse s innerhalb des Systems und zwischen miteinander vernetzten Systemen auf der Grundlage von [Zuweisung: von der Organisation definierte Richtlini en zur Kontrolle des Informationsflusses] durch.	ec2- instances-in-vpc	Stellen Sie Amazon Elastic Compute Cloud (Amazon EC2) -Instances innerhalb einer Amazon Virtual Private Cloud (Amazon VPC) bereit, um eine sichere Kommunika tion zwischen einer Instance und anderen Services innerhalb der Amazon VPC zu ermöglichen, ohne dass ein Internet-Gateway, ein NAT-Gerät oder eine VPN-Verbindung erforderlich ist. Der gesamte Datenverk ehr bleibt sicher in der AWS Cloud. Domains, die sich innerhalb einer VPC befinden, verfügen aufgrund ihrer logischen Isolierun g im Vergleich zu Domains mit öffentlic hen Endpunkten über eine zusätzlic he Sicherheitsebene. Weisen Sie EC2

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
			Amazon-Instances einer Amazon-VPC zu, um den Zugriff ordnungsgemäß zu verwalten.
AC-4	Das Informati onssystem setzt genehmigte Autorisie rungen für die Kontrolle des Informationsflusse s innerhalb des Systems und zwischen miteinander vernetzten Systemen auf der Grundlage von [Zuweisung: von der Organisation definierte Richtlini en zur Kontrolle des Informationsflusses] durch.	acm-certificate-ex piration-check	Stellen Sie sicher, dass die Netzwerki ntegrität geschützt ist, indem Sie sicherste llen, dass X509-Zertifikate von AWS ACM ausgestel lt werden. Diese Zertifikate müssen gültig und dürfen nicht abgelaufen sein. Für diese Regel ist ein Wert für erforderlich daysToExpiration (Wert für bewährte AWS Grundregeln für Sicherheit: 90). Der tatsächliche Wert muss den Richtlini en Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
AC-4	Das Informationssystem setzt genehmigte Autorisierungen für die Kontrolle des Informationsflusses innerhalb des Systems und zwischen miteinander vernetzten Systemen auf der Grundlage von [Zuweisung: von der Organisation definierte Richtlinien zur Kontrolle des Informationsflusses] durch.	dms-replication-not-public	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass auf DMS-Replikationsinstanzen nicht öffentlich zugegriffen werden kann. DMS-Replikations-Instances können vertrauliche Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
AC-4	Das Informati onssystem setzt genehmigte Autorisie rungen für die Kontrolle des Informationsflusse s innerhalb des Systems und zwischen miteinander vernetzten Systemen auf der Grundlage von [Zuweisung: von der Organisation definierte Richtlini en zur Kontrolle des Informationsflusses] durch.	ebs-snapshot-public-restorable-überprüfen	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass EBS-Snapshots nicht öffentlich wiederher stellbar sind. EBS-Volume-Snapsho ts können vertrauli che Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
AC-4	Das Informati onssystem setzt genehmigte Autorisie rungen für die Kontrolle des Informationsflusse s innerhalb des Systems und zwischen miteinander vernetzten Systemen auf der Grundlage von [Zuweisung: von der Organisation definierte Richtlini en zur Kontrolle des Informationsflusses] durch.	ec-2 instance-no-public-ip	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon Elastic Compute Cloud (Amazon EC2) - Instances nicht öffentlich zugänglich sind. EC2 Amazon-Instances können vertrauliche Informati onen enthalten, und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
AC-4	Das Informationssystem setzt genehmigte Autorisierungen für die Kontrolle des Informationsflusses innerhalb des Systems und zwischen miteinander vernetzten Systemen auf der Grundlage von [Zuweisung: von der Organisation definierte Richtlinien zur Kontrolle des Informationsflusses] durch.	elasticsearch-in-vpc-only	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass sich Amazon OpenSearch OpenSearch Service (Service) - Domains innerhalb einer Amazon Virtual Private Cloud (Amazon VPC) befinden. Eine OpenSearch Service-Domain innerhalb einer Amazon VPC ermöglicht die sichere Kommunikation zwischen OpenSearch Service und anderen Services innerhalb der Amazon VPC, ohne dass ein Internet-Gateway, ein NAT-Gerät oder eine VPN-Verbindung erforderlich ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
AC-4	Das Informationssystem setzt genehmigte Autorisierungen für die Kontrolle des Informationsflusses innerhalb des Systems und zwischen miteinander vernetzten Systemen auf der Grundlage von [Zuweisung: von der Organisation definierte Richtlinien zur Kontrolle des Informationsflusses] durch.	emr-master-no-public-ip	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon EMR-Cluster-Masterknoten nicht öffentlich zugänglich sind. Amazon-EMR-Cluster-Hauptknoten können vertrauliche Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
AC-4	Das Informati onssystem setzt genehmigte Autorisie rungen für die Kontrolle des Informationsflusse s innerhalb des Systems und zwischen miteinander vernetzten Systemen auf der Grundlage von [Zuweisung: von der Organisation definierte Richtlini en zur Kontrolle des Informationsflusses] durch.	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) Security Groups können bei der Verwaltung des Netzwerkzugriffs helfen, indem sie eine statusbeh aftete Filterung von eingehendem und ausgehendem Netzwerkverkehr zu Ressourcen bereitste llen. AWS Wenn Sie eingehenden (oder entfernten) Datenverk ehr von 0.0.0.0/0 bis Port 22 auf Ihren Ressourcen nicht zulassen, können Sie den Remote-Zugriff einschränken.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
AC-4	Das Informationssystem setzt genehmigte Autorisierungen für die Kontrolle des Informationsflusses innerhalb des Systems und zwischen miteinander vernetzten Systemen auf der Grundlage von [Zuweisung: von der Organisation definierte Richtlinien zur Kontrolle des Informationsflusses] durch.	lambda-function-public-access-verboten	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass AWS Lambda-Funktionen nicht öffentlich zugänglich sind. Der öffentliche Zugriff kann möglicherweise die Verfügbarkeit von Ressourcen beeinträchtigen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
AC-4	Das Informati onssystem setzt genehmigte Autorisie rungen für die Kontrolle des Informationsflusse s innerhalb des Systems und zwischen miteinander vernetzten Systemen auf der Grundlage von [Zuweisung: von der Organisation definierte Richtlini en zur Kontrolle des Informationsflusses] durch.	lambda-inside-vpc	Stellen Sie AWS Lambda-Funktionen in einer Amazon Virtual Private Cloud (Amazon VPC) bereit, um eine sichere Kommunika tion zwischen einer Funktion und anderen Diensten innerhalb der Amazon VPC zu gewährleisten. Bei dieser Konfiguration sind kein Internet-Gateway, kein NAT-Gerät und keine VPN-Verbindung erforderlich. Der gesamte Datenverk ehr bleibt sicher in der Cloud. AWS Domains, die sich innerhalb einer VPC befinden, verfügen aufgrund ihrer logischen Isolierun g im Vergleich zu Domains mit öffentlic hen Endpunkten über eine zusätzliche Sicherheitsebene. Um den Zugriff ordnungsg emäß zu verwalten,

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
			sollten AWS Lambda-Funktionen einer VPC zugewiesen werden.
AC-4	Das Informationssystem setzt genehmigte Autorisierungen für die Kontrolle des Informationsflusses innerhalb des Systems und zwischen miteinander vernetzten Systemen auf der Grundlage von [Zuweisung: von der Organisation definierte Richtlinien zur Kontrolle des Informationsflusses] durch.	rds-instance-public-access-überprüfen	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Relational Database Service (Amazon RDS) -Instances nicht öffentlich sind. Amazon-RDS-Datenbank-Instances können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
AC-4	Das Informationssystem setzt genehmigte Autorisierungen für die Kontrolle des Informationsflusses innerhalb des Systems und zwischen miteinander vernetzten Systemen auf der Grundlage von [Zuweisung: von der Organisation definierte Richtlinien zur Kontrolle des Informationsflusses] durch.	rds-snapshots-public-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Relational Database Service (Amazon RDS) -Instances nicht öffentlich sind. Amazon-RDS-Datenbank-Instances können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
AC-4	Das Informationssystem setzt genehmigte Autorisierungen für die Kontrolle des Informationsflusses innerhalb des Systems und zwischen miteinander vernetzten Systemen auf der Grundlage von [Zuweisung: von der Organisation definierte Richtlinien zur Kontrolle des Informationsflusses] durch.	redshift-cluster-public-access-überprüfen	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Redshift Redshift-Cluster nicht öffentlich sind. Amazon-Redshift-Cluster können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
AC-4	Das Informationssystem setzt genehmigte Autorisierungen für die Kontrolle des Informationsflusses innerhalb des Systems und zwischen miteinander vernetzten Systemen auf der Grundlage von [Zuweisung: von der Organisation definierte Richtlinien zur Kontrolle des Informationsflusses] durch.	restricted-common-ports	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass gemeinsame Ports für Amazon Elastic Compute Cloud (Amazon EC2) -Sicherheitsgruppen eingeschränkt sind. Wenn der Zugriff auf Ports nicht auf vertrauenswürdige Quellen beschränkt wird, kann dies zu Angriffen auf die Verfügbarkeit, Integrität und Vertraulichkeit von Systemen führen. Mit dieser Regel können Sie optional die Parameter blockedPort1–blockedPort5 festlegen (Standardkonfigurationen: 20, 21, 3389, 3306, 4333). Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
AC-4	Das Informationssystem setzt genehmigte Autorisierungen für die Kontrolle des Informationsflusses innerhalb des Systems und zwischen miteinander vernetzten Systemen auf der Grundlage von [Zuweisung: von der Organisation definierte Richtlinien zur Kontrolle des Informationsflusses] durch.	s-3 bucket-public-read-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie nur autorisierten Benutzern, Prozessen und Geräten Zugriff auf Amazon Simple Storage Service (Amazon S3) - Buckets gewähren. Die Verwaltung des Zugriffs sollte mit der Klassifizierung der Daten übereinstimmen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
AC-4	Das Informationssystem setzt genehmigte Autorisierungen für die Kontrolle des Informationsflusses innerhalb des Systems und zwischen miteinander vernetzten Systemen auf der Grundlage von [Zuweisung: von der Organisation definierte Richtlinien zur Kontrolle des Informationsflusses] durch.	s3- bucket-public-write-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie nur autorisierten Benutzern, Prozessen und Geräten Zugriff auf Amazon Simple Storage Service (Amazon S3) - Buckets gewähren. Die Verwaltung des Zugriffs sollte mit der Klassifizierung der Daten übereinstimmen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
AC-4	Das Informationssystem setzt genehmigte Autorisierungen für die Kontrolle des Informationsflusses innerhalb des Systems und zwischen miteinander vernetzten Systemen auf der Grundlage von [Zuweisung: von der Organisation definierte Richtlinien zur Kontrolle des Informationsflusses] durch.	sagemaker-notebook-no-direct-Internetzugang	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass SageMaker Amazon-Notebooks keinen direkten Internetzugang zulassen. Indem Sie direkten Internetzugang blockieren, vermeiden Sie, dass unbefugte Benutzer auf sensible Daten zugreifen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
AC-4	Das Informati onssystem setzt genehmigte Autorisie rungen für die Kontrolle des Informationsflusse s innerhalb des Systems und zwischen miteinander vernetzten Systemen auf der Grundlage von [Zuweisung: von der Organisation definierte Richtlini en zur Kontrolle des Informationsflusses] durch.	vpc-default-security-group-geschlossen	Sicherheitsgruppen von Amazon Elastic Compute Cloud (Amazon EC2) können bei der Verwaltung des Netzwerkzugriffs helfen, indem sie eine statusbehaftete Filterung des ein- und ausgehenden Netzwerkverkehrs zu Ressourcen bereitstellen. AWS Die Beschränk ung des gesamten Datenverkehrs auf die Standardsicherheit sgruppe hilft dabei, den Fernzugriff auf Ihre Ressourcen einzuschränken. AWS

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
AC-4	Das Informationssystem setzt genehmigte Autorisierungen für die Kontrolle des Informationsflusses innerhalb des Systems und zwischen miteinander vernetzten Systemen auf der Grundlage von [Zuweisung: von der Organisation definierte Richtlinien zur Kontrolle des Informationsflusses] durch.	vpc-sg-open-only-to-authorized-ports	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass gemeinsame Ports für Amazon Elastic Compute Cloud (Amazon EC2) -Sicherheitsgruppen eingeschränkt sind. Wenn der Zugriff auf Ports nicht auf vertrauenswürdige Quellen beschränkt wird, kann dies zu Angriffen auf die Verfügbarkeit, Integrität und Vertraulichkeit von Systemen führen. Durch die Beschränkung des Zugriffs auf Ressourcen innerhalb einer Sicherheitsgruppe aus dem Internet (0.0.0.0/0) kann der Remote-Zugriff auf interne Systeme gesteuert werden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
AC-5c	Die Organisation: c. Definiert Zugriffsb erechtigungen für das Informationssystem zur Unterstützung der Aufgabentrennung.	ecs-task-definition-user-for-host-mode-check	Wenn für eine Aufgabendefinition erhöhte Berechtig ungen gelten, liegt das daran, dass der Kunde diesen Konfigura tionen ausdrücklich zugestimmt hat. Diese Kontrolle prüft, ob eine unerwartete Berechtigungseskal ation vorliegt, wenn für eine Aufgabend efinition das Host-Netzwerk aktiviert ist, die Kunden aber keine erhöhten Berechtigungen aktiviert haben.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
AC-5c	Die Organisation: c. Definiert Zugriffsb erechtigungen für das Informationssystem zur Unterstützung der Aufgabentrennung.	iam-customer-policy-blocked-kms-Aktionen	AWS Identity and Access Managemen t (IAM) kann Ihnen helfen, die Prinzipien der geringsten Rechte und der Aufgabent rennung in Zugriffsb erechtigungen und Autorisierungen zu integrieren und so zu verhindern, dass Richtlinien blockiert e Aktionen für alle AWS Schlüssel des Key Management Service enthalten. Wenn Benutzer mehr Rechte haben, als für die Ausführung einer Aufgabe erforderl ich sind, kann dies gegen das Prinzip der geringsten Berechtig ung und Aufgabent rennung verstoßen . Mit dieser Regel können Sie den Parameter festlegen . blockedActionsPatt erns (Wert „AWS Bewährte grundlege nde Sicherhei tsmethoden“: kms:

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
			Decrypt, kms:ReEncryptFrom). Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
AC-5c	Die Organisation: c. Definiert Zugriffsb erechtigungen für das Informationssystem zur Unterstützung der Aufgabentrennung.	iam-inline-policy-blocked-kms-Aktionen	Stellen Sie sicher, dass ein Benutzer, eine IAM-Rolle oder eine IAM-Gruppe (AWS Identity and Access Management) nicht über eine Inline-Richtlinie verfügt, die blockierte Aktionen für alle AWS Schlüssel des Key Management Service zulässt. AWS empfiehlt, verwaltet e Richtlinien anstelle von Inline-Richtlinien zu verwenden. Verwaltete Richtlini en ermöglichen Wiederverwendbarke it, Versionsverwaltung , Rollback und Delegierung der Berechtigungsverwa ltung. Mit dieser Regel können Sie den blockedActionsPatt erns Parameter festlegen. (Wert „AWS Bewährte grundlege nde Sicherhei tsmethoden“: kms: Decrypt, kms:ReEnc ryptFrom). Die

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
			tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.
AC-5c	Die Organisation: c. Definiert Zugriffsberechtigungen für das Informationssystem zur Unterstützung der Aufgabentrennung.	iam-no-inline-policy-überprüfen	Stellen Sie sicher, dass ein Benutzer, eine IAM-Rolle oder eine IAM-Gruppe (AWS Identity and Access Management) nicht über eine Inline-Richtlinie zur Zugriffskontrolle auf Systeme und Ressourcen verfügt. AWS empfiehlt, verwaltete Richtlinien anstelle von Inline-Richtlinien zu verwenden. Verwaltete Richtlinien ermöglichen Wiederverwendbarkeit, Versionsverwaltung, Rollback und Delegierung der Berechtigungsverwaltung.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
AC-5c	Die Organisation: c. Definiert Zugriffsberechtigungen für das Informationssystem zur Unterstützung der Aufgabentrennung.	iam-password-policy	Die Identitäten und Anmeldeinformationen werden auf der Grundlage einer organisatorischen IAM-Passwortrichtlinie ausgestellt, verwaltet und verifiziert. Sie erfüllen oder übertreffen die Anforderungen von NIST SP 800-63 und dem Standard „Best Practices“ von AWS Foundational Security für die Passwortstärke. Mit dieser Regel können Sie optional RequireUppercaseCharacters (Wert für AWS grundlegende Sicherheitsbewährte Methoden: wahr), RequireLowercaseCharacters (Wert für bewährte Methoden für AWS grundlegende Sicherheit: wahr), RequireSymbols (Wert für bewährte Methoden für AWS grundlegende Sicherheit:

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
			wahr), RequireNumbers (Wert für bewährte Methoden für AWS grundlegende Sicherheit: wahr), MinimumPasswordLength (Wert für bewährte Methoden für AWS grundlegende Sicherheit: 14), PasswordReusePrevention (Wert für bewährte Methoden für AWS grundlegende Sicherheit: 24) und MaxPasswordAge (Wert für bewährte Methoden für AWS grundlegende Sicherheit: 90) für Ihr IAM festlegen Kennwortrichtlinie. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
AC-5c	Die Organisation: c. Definiert Zugriffsberechtigungen für das Informationssystem zur Unterstützung der Aufgabentrennung.	iam-policy-no-statements-with-full-access	Stellen Sie sicher, dass IAM-Aktionen nur auf die benötigten Aktionen beschränkt sind. Wenn Benutzern mehr Rechte eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und der Aufgabentrennung verstoßen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
AC-5c	Die Organisation: c. Definiert Zugriffsb erechtigungen für das Informationssystem zur Unterstützung der Aufgabentrennung.	iam-root-access-key-überprüfen	Der Zugriff auf Systeme und Ressourcen kann gesteuert werden, indem überprüft wird, ob der Root-Benu tzer keine Zugriffss chlüssel mit seiner AWS Identity and Access Management (IAM) -Rolle verknüpft hat. Stellen Sie sicher, dass die Root-Zugr iffsschlüssel gelöscht werden. Erstellen und verwenden Sie stattdessen rollenbas ierte Funktionen, AWS-Konten um das Prinzip der geringste n Funktionalität zu berücksichtigen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
AC-5c	Die Organisation: c. Definiert Zugriffsberechtigungen für das Informationssystem zur Unterstützung der Aufgabentrennung.	iam-user-group-membership-überprüfen	AWS Identity and Access Management (IAM) kann Ihnen helfen, Zugriffsberechtigungen und Autorisierungen einzuschränken, indem sichergestellt wird, dass Benutzer Mitglieder mindestens einer Gruppe sind. Wenn Benutzern mehr Berechtigungen eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und Aufgabentrennung verstoßen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
AC-5c	Die Organisation: c. Definiert Zugriffsberechtigungen für das Informationssystem zur Unterstützung der Aufgabentrennung.	iam-user-unused-credentials-überprüfen	AWS Identity and Access Management (IAM) kann Ihnen bei Zugriffsberechtigungen und Autorisierungen helfen, indem es nach IAM-Passwörtern und Zugriffsschlüsseln sucht, die für einen bestimmten Zeitraum nicht verwendet wurden. Wenn ungenutzte Anmeldeinformationen identifiziert werden, müssen Sie sie deaktivieren und/oder entfernen, da dies gegen das Prinzip der geringsten Berechtigung verstoßen könnte. Für diese Regel müssen Sie einen Wert für das maxCredentialUsage Alter festlegen (Standardkonfiguration: 90). Der tatsächliche Wert muss den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
AC-5c	Die Organisation: c. Definiert Zugriffsb erechtigungen für das Informationssystem zur Unterstützung der Aufgabentrennung.	iam-group-has-users-überprüfen	AWS Identity and Access Managemen t (IAM) kann Ihnen helfen, die Prinzipien der geringsten Rechte und der Aufgabent rennung mit Zugriffsb erechtigungen und Autorisierungen zu integrieren, indem sichergestellt wird, dass IAM-Gruppen mindestens einen Benutzer haben. Die Einteilung von Benutzern in Gruppen auf der Grundlage der ihnen zugewiese nen Berechtigungen oder ihrer Funktion ist eine Möglichkeit, das Prinzip der geringste n Berechtigung zu implementieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
AC-5c	Die Organisation: c. Definiert Zugriffsberechtigungen für das Informationssystem zur Unterstützung der Aufgabentrennung.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) kann Ihnen dabei helfen, die Prinzipien der geringsten Rechte und der Aufgabentrennung in Zugriffsberechtigungen und Autorisierungen zu integrieren und so zu verhindern, dass Richtlinien „Effect“: „Allow“ mit „Action“: „*“ anstelle von „Resource“: „*“ enthalten. Wenn Benutzern mehr Rechte eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und der Aufgabentrennung verstoßen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
AC-5c	Die Organisation: c. Definiert Zugriffsb erechtigungen für das Informationssystem zur Unterstützung der Aufgabentrennung.	iam-user-no-policies-überprüfen	Diese Regel stellt sicher, dass AWS Identity and Access Management (IAM) -Richtlinien nur Gruppen oder Rollen zugewiese n werden, um den Zugriff auf Systeme und Ressourcen zu kontrollieren. Die Zuweisung von Berechtig ungen auf Gruppen- oder Rollenebene trägt dazu bei, die Wahrscheinlichkeit zu verringern, dass eine Identität übermäßige Berechtigungen erhält oder beibehält.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
AC-6(10)	Das Informationssystem verhindert, dass nicht privilegierte Benutzer privilegierte Funktionen ausführen, einschließlich der Deaktivierung, Umgehung oder Änderung implementierter Sicherheitsvorkehrungen/Gegenmaßnahmen.	iam-policy-no-statements-with-full-access	Stellen Sie sicher, dass IAM-Aktionen nur auf die benötigten Aktionen beschränkt sind. Wenn Benutzern mehr Rechte eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und der Aufgabentrennung verstoßen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
AC-6(10)	Das Informationssystem verhindert, dass nicht privilegierte Benutzer privilegierte Funktionen ausführen, einschließlich der Deaktivierung, Umgehung oder Änderung implementierter Sicherheitsvorkehrungen/Gegenmaßnahmen.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) kann Ihnen dabei helfen, die Prinzipien der geringsten Rechte und der Aufgabentrennung in Zugriffsberechtigungen und Autorisierungen zu integrieren und so zu verhindern, dass Richtlinien „Effect“: „Allow“ mit „Action“: „*“ anstelle von „Resource“: „*“ enthalten. Wenn Benutzern mehr Rechte eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und der Aufgabentrennung verstoßen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
AC-6(10)	Das Informati onssystem verhinder t, dass nicht privilegi erte Benutzer privilegi erte Funktionen ausführen, einschlie ßlich der Deaktivie rung, Umgehung oder Änderung implement ierter Sicherhei tsvorkehrungen/Geg enmaßnahmen.	iam-root-access-key-überprüfen	Der Zugriff auf Systeme und Ressourcen kann gesteuert werden, indem überprüft wird, ob der Root-Benu tzer keine Zugriffss chlüssel mit seiner AWS Identity and Access Management (IAM) -Rolle verknüpft hat. Stellen Sie sicher, dass die Root-Zugr iffsschlüssel gelöscht werden. Erstellen und verwenden Sie stattdessen rollenbas ierte Funktionen, AWS-Konten um das Prinzip der geringste n Funktionalität zu berücksichtigen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
AC-6	Die Organisation wendet das Prinzip der geringsten Berechtigung an und erlaubt Benutzern (oder Prozessen , die im Namen von Benutzern handeln) nur dann den Zugriff, wenn dies für die Ausführun g zugewiesener Aufgaben gemäß den Unternehmenszielen und Geschäfts funktionen notwendig ist.	ec2-imdsv2-check	Stellen Sie sicher, dass die Methode Instance Metadata Service Version 2 (IMDSv2) aktiviert ist, um den Zugriff auf und die Kontrolle der Amazon Elastic Compute Cloud (Amazon EC2) - Instance-Metadate n zu schützen. Die IMDSv2 Methode verwendet sitzungsb asierte Kontrollen. Mit können Kontrolle n implementiert werden IMDSv2, um Änderungen an Instanzmetadaten einzuschränken.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
AC-6	Die Organisation wendet das Prinzip der geringsten Berechtigung an und erlaubt Benutzern (oder Prozessen , die im Namen von Benutzern handeln) nur dann den Zugriff, wenn dies für die Ausführun g zugewiesener Aufgaben gemäß den Unternehmenszielen und Geschäfts funktionen notwendig ist.	iam-no-inline-policy-überprüfen	Stellen Sie sicher, dass ein Benutzer, eine IAM-Rolle oder eine IAM-Gruppe (AWS Identity and Access Management) nicht über eine Inline-Richtlinie zur Zugriffsk ontrolle auf Systeme und Ressource n verfügt. AWS empfiehlt, verwaltet e Richtlinien anstelle von Inline-Richtlinien zu verwenden. Verwaltete Richtlini en ermöglichen Wiederverwendbarke it, Versionsverwaltung , Rollback und Delegierung der Berechtigungsverwa ltung.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
AC-6	Die Organisation wendet das Prinzip der geringsten Berechtigung an und erlaubt Benutzern (oder Prozessen , die im Namen von Benutzern handeln) nur dann den Zugriff, wenn dies für die Ausführun g zugewiesener Aufgaben gemäß den Unternehmenszielen und Geschäfts funktionen notwendig ist.	ec-2 instances-in-vpc	Stellen Sie Amazon Elastic Compute Cloud (Amazon EC2) -Instances innerhalb einer Amazon Virtual Private Cloud (Amazon VPC) bereit, um eine sichere Kommunika tion zwischen einer Instance und anderen Services innerhalb der Amazon VPC zu ermöglichen, ohne dass ein Internet-Gateway, ein NAT-Gerät oder eine VPN-Verbindung erforderlich ist. Der gesamte Datenverk ehr bleibt sicher in der AWS Cloud. Domains, die sich innerhalb einer VPC befinden, verfügen aufgrund ihrer logischen Isolierun g im Vergleich zu Domains mit öffentlic hen Endpunkten über eine zusätzlic he Sicherheitsebene. Weisen Sie EC2

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
			Amazon-Instances einer Amazon-VPC zu, um den Zugriff ordnungsgemäß zu verwalten.
AC-6	Die Organisation wendet das Prinzip der geringsten Berechtigung an und erlaubt Benutzern (oder Prozessen , die im Namen von Benutzern handeln) nur dann den Zugriff, wenn dies für die Ausführung zugewiesener Aufgaben gemäß den Unternehmenszielen und Geschäfts funktionen notwendig ist.	codebuild-project-envvar-awscred-überprüfen	Stellen Sie sicher, dass die Anmeldeinformationen AWS_ACCESS_KEY_ID AWS_SECRET_ACCESS_KEY nicht in AWS Codebuild-Projektumgebungen vorhanden sind. Speichern Sie diese Variablen nicht als Klartext. Das Speichern dieser Variablen als Klartext bewirkt eine unbeabsichtigte Offenlegung von Daten sowie unberechtigte Zugriffe.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
AC-6	Die Organisation wendet das Prinzip der geringsten Berechtigung an und erlaubt Benutzern (oder Prozessen , die im Namen von Benutzern handeln) nur dann den Zugriff, wenn dies für die Ausführun g zugewiesener Aufgaben gemäß den Unternehmenszielen und Geschäfts funktionen notwendig ist.	dms-replication-not-public	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass auf DMS-Replikationsin stanzen nicht öffentlic h zugegriffen werden kann. DMS-Repli kations-Instances können vertrauli che Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
AC-6	Die Organisation wendet das Prinzip der geringsten Berechtigung an und erlaubt Benutzern (oder Prozessen , die im Namen von Benutzern handeln) nur dann den Zugriff, wenn dies für die Ausführun g zugewiesener Aufgaben gemäß den Unternehmenszielen und Geschäfts funktionen notwendig ist.	ebs-snapshot-public-restorable-überprüfen	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass EBS-Snapshots nicht öffentlich wiederher stellbar sind. EBS-Volume-Snapsho ts können vertrauli che Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
AC-6	Die Organisation wendet das Prinzip der geringsten Berechtigung an und erlaubt Benutzern (oder Prozessen , die im Namen von Benutzern handeln) nur dann den Zugriff, wenn dies für die Ausführun g zugewiesener Aufgaben gemäß den Unternehmenszielen und Geschäfts funktionen notwendig ist.	ec-2 instance-no-public-ip	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon Elastic Compute Cloud (Amazon EC2) - Instances nicht öffentlich zugänglich sind. EC2 Amazon-Instances können vertrauliche Informati onen enthalten, und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
AC-6	Die Organisation wendet das Prinzip der geringsten Berechtigung an und erlaubt Benutzern (oder Prozessen , die im Namen von Benutzern handeln) nur dann den Zugriff, wenn dies für die Ausführun g zugewiesener Aufgaben gemäß den Unternehmenszielen und Geschäfts funktionen notwendig ist.	elasticsearch-in-vpc-only	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherste llen, dass sich Amazon OpenSearc h OpenSearch Service (Service) - Domains innerhalb einer Amazon Virtual Private Cloud (Amazon VPC) befinden. Eine OpenSearch Service-Domain innerhalb einer Amazon VPC ermöglicht die sichere Kommunikation zwischen OpenSearc h Service und anderen Services innerhalb der Amazon VPC, ohne dass ein Internet-Gateway, ein NAT-Gerät oder eine VPN-Verbindung erforderlich ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
AC-6	Die Organisation wendet das Prinzip der geringsten Berechtigung an und erlaubt Benutzern (oder Prozessen , die im Namen von Benutzern handeln) nur dann den Zugriff, wenn dies für die Ausführun g zugewiesener Aufgaben gemäß den Unternehmenszielen und Geschäfts funktionen notwendig ist.	emr-master-no-public-ip	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon EMR-Clust er-Masterknoten nicht öffentlich zugänglic h sind. Amazon-EM R-Cluster-Hauptkno ten können vertrauli che Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
AC-6	Die Organisation wendet das Prinzip der geringsten Berechtigung an und erlaubt Benutzern (oder Prozessen , die im Namen von Benutzern handeln) nur dann den Zugriff, wenn dies für die Ausführun g zugewiesener Aufgaben gemäß den Unternehmenszielen und Geschäfts funktionen notwendig ist.	iam-group-has-users-überprüfen	AWS Identity and Access Managemen t (IAM) kann Ihnen helfen, die Prinzipien der geringsten Rechte und der Aufgabent rennung mit Zugriffsb erechtigungen und Autorisierungen zu integrieren, indem sichergestellt wird, dass IAM-Gruppen mindestens einen Benutzer haben. Die Einteilung von Benutzern in Gruppen auf der Grundlage der ihnen zugewiese nen Berechtigungen oder ihrer Funktion ist eine Möglichkeit, das Prinzip der geringste n Berechtigung zu implementieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
AC-6	Die Organisation wendet das Prinzip der geringsten Berechtigung an und erlaubt Benutzern (oder Prozessen , die im Namen von Benutzern handeln) nur dann den Zugriff, wenn dies für die Ausführun g zugewiesener Aufgaben gemäß den Unternehmenszielen und Geschäfts funktionen notwendig ist.	iam-policy-no-stat ements-with-admin-access	AWS Identity and Access Managemen t (IAM) kann Ihnen dabei helfen, die Prinzipien der geringsten Rechte und der Aufgabent rennung in Zugriffsb erechtigungen und Autorisierungen zu integrieren und so zu verhindern, dass Richtlinien „Effect“: „Allow“ mit „Action“: „*“ anstelle von „Resource“: „*“ enthalten. Wenn Benutzern mehr Rechte eingeräum t werden, als für die Ausführung einer Aufgabe erforderl ich sind, kann dies gegen das Prinzip der geringsten Berechtigung und der Aufgabentrennung verstoßen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
AC-6	Die Organisation wendet das Prinzip der geringsten Berechtigung an und erlaubt Benutzern (oder Prozessen , die im Namen von Benutzern handeln) nur dann den Zugriff, wenn dies für die Ausführun g zugewiesener Aufgaben gemäß den Unternehmenszielen und Geschäfts funktionen notwendig ist.	iam-root-access-key-überprüfen	Der Zugriff auf Systeme und Ressourcen kann gesteuert werden, indem überprüft wird, ob der Root-Benu tzer keine Zugriffss chlüssel mit seiner AWS Identity and Access Management (IAM) -Rolle verknüpft hat. Stellen Sie sicher, dass die Root-Zugr iffsschlüssel gelöscht werden. Erstellen und verwenden Sie stattdessen rollenbas ierte Funktionen, AWS-Konten um das Prinzip der geringste n Funktionalität zu berücksichtigen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
AC-6	Die Organisation wendet das Prinzip der geringsten Berechtigung an und erlaubt Benutzern (oder Prozessen , die im Namen von Benutzern handeln) nur dann den Zugriff, wenn dies für die Ausführung zugewiesener Aufgaben gemäß den Unternehmenszielen und Geschäfts funktionen notwendig ist.	iam-user-group-membership-überprüfen	AWS Identity and Access Management (IAM) kann Ihnen helfen, Zugriffsberechtigungen und Autorisierungen einzuschränken, indem sichergestellt wird, dass Benutzer Mitglieder mindestens einer Gruppe sind. Wenn Benutzern mehr Berechtigungen eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und Aufgabentrennung verstoßen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
AC-6	Die Organisation wendet das Prinzip der geringsten Berechtigung an und erlaubt Benutzern (oder Prozessen , die im Namen von Benutzern handeln) nur dann den Zugriff, wenn dies für die Ausführun g zugewiesener Aufgaben gemäß den Unternehmenszielen und Geschäfts funktionen notwendig ist.	iam-user-no-policies-überprüfen	Diese Regel stellt sicher, dass AWS Identity and Access Management (IAM) -Richtlinien nur Gruppen oder Rollen zugewiese n werden, um den Zugriff auf Systeme und Ressourcen zu kontrollieren. Die Zuweisung von Berechtig ungen auf Gruppen- oder Rollenebene trägt dazu bei, die Wahrscheinlichkeit zu verringern, dass eine Identität übermäßige Berechtigungen erhält oder beibehält.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
AC-6	Die Organisation wendet das Prinzip der geringsten Berechtigung an und erlaubt Benutzern (oder Prozessen, die im Namen von Benutzern handeln) nur dann den Zugriff, wenn dies für die Ausführung zugewiesener Aufgaben gemäß den Unternehmenszielen und Geschäftsfunktionen notwendig ist.	iam-user-unused-credentials-überprüfen	AWS Identity and Access Management (IAM) kann Ihnen bei Zugriffsberechtigungen und Autorisierungen helfen, indem es nach IAM-Passwörtern und Zugriffsschlüsseln sucht, die für einen bestimmten Zeitraum nicht verwendet wurden. Wenn ungenutzte Anmeldeinformationen identifiziert werden, müssen Sie sie deaktivieren und/oder entfernen, da dies gegen das Prinzip der geringsten Berechtigung verstoßen könnte. Für diese Regel müssen Sie einen Wert für das maxCredentialUsage Alter festlegen (Standardkonfiguration: 90). Der tatsächliche Wert muss den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
AC-6	Die Organisation wendet das Prinzip der geringsten Berechtigung an und erlaubt Benutzern (oder Prozessen , die im Namen von Benutzern handeln) nur dann den Zugriff, wenn dies für die Ausführun g zugewiesener Aufgaben gemäß den Unternehmenszielen und Geschäfts funktionen notwendig ist.	lambda-function-pu blic-access-verboten	Verwalten Sie den Zugriff auf Ressource n in der AWS Cloud, indem Sie sicherste llen, dass AWS Lambda-Funktionen nicht öffentlich zugänglich sind. Der öffentliche Zugriff kann möglicherweise die Verfügbarkeit von Ressourcen beeinträc htigen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
AC-6	Die Organisation wendet das Prinzip der geringsten Berechtigung an und erlaubt Benutzern (oder Prozessen , die im Namen von Benutzern handeln) nur dann den Zugriff, wenn dies für die Ausführun g zugewiesener Aufgaben gemäß den Unternehmenszielen und Geschäfts funktionen notwendig ist.	lambda-inside-vpc	Stellen Sie AWS Lambda-Funktionen in einer Amazon Virtual Private Cloud (Amazon VPC) bereit, um eine sichere Kommunika tion zwischen einer Funktion und anderen Diensten innerhalb der Amazon VPC zu gewährleisten. Bei dieser Konfiguration sind kein Internet-Gateway, kein NAT-Gerät und keine VPN-Verbindung erforderlich. Der gesamte Datenverk ehr bleibt sicher in der Cloud. AWS Domains, die sich innerhalb einer VPC befinden, verfügen aufgrund ihrer logischen Isolierun g im Vergleich zu Domains mit öffentlic hen Endpunkten über eine zusätzliche Sicherheitsebene. Um den Zugriff ordnungsg emäß zu verwalten,

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
			sollten AWS Lambda-Funktionen einer VPC zugewiesen werden.
AC-6	Die Organisation wendet das Prinzip der geringsten Berechtigung an und erlaubt Benutzern (oder Prozessen , die im Namen von Benutzern handeln) nur dann den Zugriff, wenn dies für die Ausführun g zugewiesener Aufgaben gemäß den Unternehmenszielen und Geschäfts funktionen notwendig ist.	rds-instance-public-access-überprüfen	Verwalten Sie den Zugriff auf Ressource n in der AWS Cloud, indem Sie sicherste llen, dass Amazon Relational Database Service (Amazon RDS) -Instance s nicht öffentlic h sind. Amazon-RDS-Datenbank-Instances können vertrauliche Informati onen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
AC-6	Die Organisation wendet das Prinzip der geringsten Berechtigung an und erlaubt Benutzern (oder Prozessen , die im Namen von Benutzern handeln) nur dann den Zugriff, wenn dies für die Ausführun g zugewiesener Aufgaben gemäß den Unternehmenszielen und Geschäfts funktionen notwendig ist.	rds-snapshots-public-prohibited	Verwalten Sie den Zugriff auf Ressource n in der AWS Cloud, indem Sie sicherste llen, dass Amazon Relational Database Service (Amazon RDS) -Instance s nicht öffentlic h sind. Amazon-RDS-Datenbank-Instances können vertrauliche Informati onen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
AC-6	Die Organisation wendet das Prinzip der geringsten Berechtigung an und erlaubt Benutzern (oder Prozessen , die im Namen von Benutzern handeln) nur dann den Zugriff, wenn dies für die Ausführun g zugewiesener Aufgaben gemäß den Unternehmenszielen und Geschäfts funktionen notwendig ist.	redshift-cluster-public-access-überprüfen	Verwalten Sie den Zugriff auf Ressource n in der AWS Cloud, indem Sie sicherste llen, dass Amazon Redshift Redshift-Cluster nicht öffentlic h sind. Amazon-Re dshift-Cluster können vertrauliche Informati onen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
AC-6	Die Organisation wendet das Prinzip der geringsten Berechtigung an und erlaubt Benutzern (oder Prozessen , die im Namen von Benutzern handeln) nur dann den Zugriff, wenn dies für die Ausführun g zugewiesener Aufgaben gemäß den Unternehmenszielen und Geschäfts funktionen notwendig ist.	s3- -Block-periodisch account-level-public-access	Verwalten Sie den Zugriff auf Ressource n in der AWS Cloud, indem Sie sicherste llen, dass Amazon Simple Storage Service (Amazon S3) -Buckets nicht öffentlich zugänglic h sind. Diese Regel trägt dazu bei, sensible Daten vor unbefugten Remote-Benutzern zu schützen, indem sie den öffentlichen Zugriff verhinder t. Mit dieser Regel können Sie optional die Parameter ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) und restrictPublicBuck ets Parameter (Config Default: True) festlegen. Die tatsächlichen Werte müssen den Richtlini

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
			en Ihrer Organisation entsprechen.
AC-6	Die Organisation wendet das Prinzip der geringsten Berechtigung an und erlaubt Benutzern (oder Prozessen , die im Namen von Benutzern handeln) nur dann den Zugriff, wenn dies für die Ausführun g zugewiesener Aufgaben gemäß den Unternehmenszielen und Geschäfts funktionen notwendig ist.	s3 bucket-level-public-access - verboten	Verwalten Sie den Zugriff auf Ressource n in der AWS Cloud, indem Sie sicherste llen, dass Amazon Simple Storage Service (Amazon S3) -Buckets nicht öffentlich zugänglic h sind. Diese Regel trägt dazu bei, sensible Daten vor unbefugten Remote-Benutzern zu schützen, indem sie den öffentlichen Zugriff auf Bucket-Eb ene verhindert.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
AC-6	Die Organisation wendet das Prinzip der geringsten Berechtigung an und erlaubt Benutzern (oder Prozessen , die im Namen von Benutzern handeln) nur dann den Zugriff, wenn dies für die Ausführun g zugewiesener Aufgaben gemäß den Unternehmenszielen und Geschäfts funktionen notwendig ist.	s-3 bucket-public-read -prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie nur autorisierten Benutzern, Prozessen und Geräten Zugriff auf Amazon Simple Storage Service (Amazon S3) - Buckets gewähren. Die Verwaltung des Zugriffs sollte mit der Klassifizierung der Daten übereinst immen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
AC-6	Die Organisation wendet das Prinzip der geringsten Berechtigung an und erlaubt Benutzern (oder Prozessen , die im Namen von Benutzern handeln) nur dann den Zugriff, wenn dies für die Ausführun g zugewiesener Aufgaben gemäß den Unternehmenszielen und Geschäfts funktionen notwendig ist.	s3- bucket-public-writ e-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie nur autorisierten Benutzern, Prozessen und Geräten Zugriff auf Amazon Simple Storage Service (Amazon S3) - Buckets gewähren. Die Verwaltung des Zugriffs sollte mit der Klassifizierung der Daten übereinst immen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
AC-6	Die Organisation wendet das Prinzip der geringsten Berechtigung an und erlaubt Benutzern (oder Prozessen , die im Namen von Benutzern handeln) nur dann den Zugriff, wenn dies für die Ausführun g zugewiesener Aufgaben gemäß den Unternehmenszielen und Geschäfts funktionen notwendig ist.	sagemaker-notebook -no-direct-Interne tzugang	Verwalten Sie den Zugriff auf Ressource n in der AWS Cloud, indem Sie sicherste llen, dass SageMaker Amazon-Notebooks keinen direkten Internetzugang zulassen. Indem Sie direkten Internetz ugang blockieren, vermeiden Sie, dass unbefugte Benutzer auf sensible Daten zugreifen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
AC-6	Die Organisation wendet das Prinzip der geringsten Berechtigung an und erlaubt Benutzern (oder Prozessen , die im Namen von Benutzern handeln) nur dann den Zugriff, wenn dies für die Ausführun g zugewiesener Aufgaben gemäß den Unternehmenszielen und Geschäfts funktionen notwendig ist.	subnet-auto-assign-public-ip-deaktiviert	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon Virtual Private Cloud (VPC) -Subnetzen nicht automatisch eine öffentliche IP-Adress e zugewiesen wird. Amazon Elastic Compute Cloud (EC2) -Instances, die in Subnetzen gestartet werden, in denen dieses Attribut aktiviert ist, haben ihrer primären Netzwerkschnittste lle eine öffentliche IP-Adresse zugewiesen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
AC-17(1)	Das Informati onssystem überwacht und kontrolliert die Remote-Zugriffsmet hoden.	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) Security Groups können bei der Verwaltung des Netzwerkzugriffs helfen, indem sie eine statusbeh aftete Filterung von eingehendem und ausgehendem Netzwerkverkehr zu Ressourcen bereitste llen. AWS Wenn Sie eingehenden (oder entfernten) Datenverk ehr von 0.0.0.0/0 bis Port 22 auf Ihren Ressourcen nicht zulassen, können Sie den Remote-Zugriff einschränken.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
AC-17(1)	Das Informati onssystem überwacht und kontrolliert die Remote-Zugriffsmet hoden.	ec-2 instances-in-vpc	Stellen Sie Amazon Elastic Compute Cloud (Amazon EC2) -Instances innerhalb einer Amazon Virtual Private Cloud (Amazon VPC) bereit, um eine sichere Kommunika tion zwischen einer Instance und anderen Services innerhalb der Amazon VPC zu ermöglichen, ohne dass ein Internet-Gateway, ein NAT-Gerät oder eine VPN-Verbindung erforderlich ist. Der gesamte Datenverk ehr bleibt sicher in der AWS Cloud. Domains, die sich innerhalb einer VPC befinden, verfügen aufgrund ihrer logischen Isolierun g im Vergleich zu Domains mit öffentlic hen Endpunkten über eine zusätzlic he Sicherheitsebene. Weisen Sie EC2

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
			Amazon-Instances einer Amazon-VPC zu, um den Zugriff ordnungsgemäß zu verwalten.
AC-17(1)	Das Informati onssystem überwacht und kontrolliert die Remote-Zugriffsmet hoden.	securityhub-enabled	AWS Security Hub hilft bei der Überwachung von unbefugtem Personal, Verbindun gen, Geräten und Software. AWS Security Hub aggregiert, organisie rt und priorisie rt die Sicherhei tswarnungen oder Ergebnisse mehrerer Dienste. AWS Einige dieser Dienste sind Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer und AWS Firewall Manager sowie AWS Partnerlösungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
AC-17(1)	Das Informati onssystem überwacht und kontrolliert die Remote-Zugriffsmet hoden.	dms-replication-not-public	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass auf DMS-Replikationsin stanzen nicht öffentlic h zugegriffen werden kann. DMS-Repli kations-Instances können vertrauli che Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.
AC-17(1)	Das Informati onssystem überwacht und kontrolliert die Remote-Zugriffsmet hoden.	ebs-snapshot-public-restorable-überprüfen	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass EBS-Snapshots nicht öffentlich wiederher stellbar sind. EBS-Volume-Snapsho ts können vertrauli che Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
AC-17(1)	Das Informati onssystem überwacht und kontrolliert die Remote-Zugriffsmet hoden.	ec-2 instance-no-public-ip	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon Elastic Compute Cloud (Amazon EC2) - Instances nicht öffentlich zugänglich sind. EC2 Amazon-Instances können vertrauliche Informati onen enthalten, und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
AC-17(1)	Das Informati onssystem überwacht und kontrolliert die Remote-Zugriffsmet hoden.	elasticsearch-in-vpc-only	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherste llen, dass sich Amazon OpenSearc h OpenSearch Service (Service) - Domains innerhalb einer Amazon Virtual Private Cloud (Amazon VPC) befinden. Eine OpenSearch Service-Domain innerhalb einer Amazon VPC ermöglicht die sichere Kommunikation zwischen OpenSearc h Service und anderen Services innerhalb der Amazon VPC, ohne dass ein Internet-Gateway, ein NAT-Gerät oder eine VPN-Verbindung erforderlich ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
AC-17(1)	Das Informati onssystem überwacht und kontrolliert die Remote-Zugriffsmet hoden.	emr-master-no-public-ip	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon EMR-Clust er-Masterknoten nicht öffentlich zugänglic h sind. Amazon-EM R-Cluster-Hauptkno ten können vertrauli che Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
AC-17(1)	Das Informati onssystem überwacht und kontrolliert die Remote-Zugriffsmet hoden.	guardduty-enabled-centralized	Amazon GuardDuty kann mithilfe von Threat Intellige nce Feeds helfen, potenzielle Cybersich erheitsereignisse zu überwachen und zu erkennen. Dazu gehören Listen mit bösartigen IPs und maschinellen Lernmethoden, um unerwartete, unbefugte und bösartige Aktivitäten in Ihrer AWS Cloud-Umgebung zu identifiz ieren.
AC-17(1)	Das Informati onssystem überwacht und kontrolliert die Remote-Zugriffsmet hoden.	lambda-function-pu blic-access-verboten	Verwalten Sie den Zugriff auf Ressource n in der AWS Cloud, indem Sie sicherste llen, dass AWS Lambda-Funktionen nicht öffentlich zugänglich sind. Der öffentliche Zugriff kann möglicherweise die Verfügbarkeit von Ressourcen beeinträc htigen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
AC-17(1)	Das Informati onssystem überwacht und kontrolliert die Remote-Zugriffsmet hoden.	lambda-inside-vpc	Stellen Sie AWS Lambda-Funktionen in einer Amazon Virtual Private Cloud (Amazon VPC) bereit, um eine sichere Kommunika tion zwischen einer Funktion und anderen Diensten innerhalb der Amazon VPC zu gewährleisten. Bei dieser Konfiguration sind kein Internet-Gateway, kein NAT-Gerät und keine VPN-Verbindung erforderlich. Der gesamte Datenverk ehr bleibt sicher in der Cloud. AWS Domains, die sich innerhalb einer VPC befinden, verfügen aufgrund ihrer logischen Isolierun g im Vergleich zu Domains mit öffentlic hen Endpunkten über eine zusätzliche Sicherheitsebene. Um den Zugriff ordnungsg emäß zu verwalten,

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
			sollten AWS Lambda-Funktionen einer VPC zugewiesen werden.
AC-17(1)	Das Informationssystem überwacht und kontrolliert die Remote-Zugriffsmethoden.	rds-instance-public-access-überprüfen	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Relational Database Service (Amazon RDS) -Instances nicht öffentlich sind. Amazon-RDS-Datenbank-Instances können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
AC-17(1)	Das Informati onssystem überwacht und kontrolliert die Remote-Zugriffsmet hoden.	rds-snapshots-public-prohibited	Verwalten Sie den Zugriff auf Ressource n in der AWS Cloud, indem Sie sicherste llen, dass Amazon Relational Database Service (Amazon RDS) -Instance s nicht öffentlic h sind. Amazon-RDS-Datenbank-Instances können vertrauliche Informati onen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
AC-17(1)	Das Informati onssystem überwacht und kontrolliert die Remote-Zugriffsmet hoden.	redshift-cluster-public-access-überprüfen	Verwalten Sie den Zugriff auf Ressource n in der AWS Cloud, indem Sie sicherste llen, dass Amazon Redshift Redshift-Cluster nicht öffentlic h sind. Amazon-Re dshift-Cluster können vertrauliche Informati onen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
AC-17(1)	Das Informati onssystem überwacht und kontrolliert die Remote-Zugriffsmet hoden.	restricted-common-ports	Verwalten Sie den Zugriff auf Ressource n in der AWS Cloud, indem Sie sicherste llen, dass gemeinsam e Ports für Amazon Elastic Compute Cloud (Amazon EC2) -Sicherhe itsgruppen eingeschr ränkt sind. Wenn der Zugriff auf Ports nicht auf vertrauen swürdige Quellen beschränkt wird, kann dies zu Angriffen auf die Verfügbar keit, Integrität und Vertraulichkeit von Systemen führen. Mit dieser Regel können Sie optional die Parameter blockedPo rt1–blockedPort5 festlegen (Standard konfigurationen: 20, 21, 3389, 3306, 4333). Die tatsächli chen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
AC-17(1)	Das Informati onssystem überwacht und kontrolliert die Remote-Zugriffsmet hoden.	s3- account-level-publ ic-access -Block-pe riodisch	Verwalten Sie den Zugriff auf Ressource n in der AWS Cloud, indem Sie sicherste llen, dass Amazon Simple Storage Service (Amazon S3) -Buckets nicht öffentlich zugänglic h sind. Diese Regel trägt dazu bei, sensible Daten vor unbefugten Remote-Benutzern zu schützen, indem sie den öffentlichen Zugriff verhinder t. Mit dieser Regel können Sie optional die Parameter ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) und restrictPublicBuck ets Parameter (Config Default: True) festlegen. Die tatsächlichen Werte müssen den Richtlini

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
			en Ihrer Organisation entsprechen.
AC-17(1)	Das Informati onssystem überwacht und kontrolliert die Remote-Zugriffsmet hoden.	s3 bucket-level-public-access - verboten	Verwalten Sie den Zugriff auf Ressource n in der AWS Cloud, indem Sie sicherste llen, dass Amazon Simple Storage Service (Amazon S3) -Buckets nicht öffentlich zugänglic h sind. Diese Regel trägt dazu bei, sensible Daten vor unbefugten Remote-Benutzern zu schützen, indem sie den öffentlichen Zugriff auf Bucket-Eb ene verhindert.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
AC-17(1)	Das Informati onssystem überwacht und kontrolliert die Remote-Zugriffsmet hoden.	s-3 bucket-public-read -prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie nur autorisierten Benutzern, Prozessen und Geräten Zugriff auf Amazon Simple Storage Service (Amazon S3) - Buckets gewähren. Die Verwaltung des Zugriffs sollte mit der Klassifizierung der Daten übereinst immen.
AC-17(1)	Das Informati onssystem überwacht und kontrolliert die Remote-Zugriffsmet hoden.	s3- bucket-public-writ e-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie nur autorisierten Benutzern, Prozessen und Geräten Zugriff auf Amazon Simple Storage Service (Amazon S3) - Buckets gewähren. Die Verwaltung des Zugriffs sollte mit der Klassifizierung der Daten übereinst immen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
AC-17(1)	Das Informati onssystem überwacht und kontrolliert die Remote-Zugriffsmet hoden.	sagemaker-notebook -no-direct-Interne tzugang	Verwalten Sie den Zugriff auf Ressource n in der AWS Cloud, indem Sie sicherste llen, dass SageMaker Amazon-Notebooks keinen direkten Internetzugang zulassen. Indem Sie direkten Internetz ugang blockieren, vermeiden Sie, dass unbefugte Benutzer auf sensible Daten zugreifen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
AC-17(1)	Das Informati onssystem überwacht und kontrolliert die Remote-Zugriffsmet hoden.	subnet-auto-assign-public-ip-deaktiviert	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon Virtual Private Cloud (VPC) -Subnetzen nicht automatisch eine öffentliche IP-Adress e zugewiesen wird. Amazon Elastic Compute Cloud (EC2) -Instances, die in Subnetzen gestartet werden, in denen dieses Attribut aktiviert ist, haben ihrer primären Netzwerkschnittste lle eine öffentliche IP-Adresse zugewiesen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
AC-17(1)	Das Informati onssystem überwacht und kontrolliert die Remote-Zugriffsmet hoden.	vpc-default-security-group-geschlossen	Sicherheitsgruppen von Amazon Elastic Compute Cloud (Amazon EC2) können bei der Verwaltung des Netzwerkzugriffs helfen, indem sie eine statusbehaftete Filterung des ein- und ausgehenden Netzwerkverkehrs zu Ressourcen bereitstellen. AWS Die Beschränk ung des gesamten Datenverkehrs auf die Standardsicherheit sgruppe hilft dabei, den Fernzugriff auf Ihre Ressourcen einzuschränken. AWS

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
AC-17(1)	Das Informati onssystem überwacht und kontrolliert die Remote-Zugriffsmet hoden.	vpc-sg-open-only-to-authorized-ports	Verwalten Sie den Zugriff auf Ressource n in der AWS Cloud, indem Sie sicherste llen, dass gemeinsam e Ports für Amazon Elastic Compute Cloud (Amazon EC2) -Sicherhe itsgruppen eingeschr ränkt sind. Wenn der Zugriff auf Ports nicht auf vertrauen swürdige Quellen beschränkt wird, kann dies zu Angriffen auf die Verfügbar keit, Integrität und Vertraulichkeit von Systemen führen. Durch die Beschränk ung des Zugriffs auf Ressourcen innerhalb einer Sicherhei tsgruppe aus dem Internet (0.0.0.0/0) kann der Remote-Zugriff auf interne Systeme gesteuert werden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
AC-17(2)	Das Informati onssystem implement iert kryptografische Mechanismen, um die Vertraulichkeit und Integrität von Remote-Zugriffssitzungen zu schützen.	elb-tls-https-listeners-nur	Stellen Sie sicher, dass Ihre Elastic Load Balancer (ELBs) mit SSL- oder HTTPS-Listenern konfiguriert sind. Um eventuell vorhanden e sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
AC-17(2)	Das Informati onssystem implement iert kryptografische Mechanismen, um die Vertraulichkeit und Integrität von Remote-Zugriffssitzungen zu schützen.	acm-certificate-ex piration-check	Stellen Sie sicher, dass die Netzwerki ntegrität geschützt ist, indem Sie sicherste llen, dass X509-Zertifikate von ACM ausgestellt werden. AWS Diese Zertifika te müssen gültig und dürfen nicht abgelaufen sein. Für diese Regel ist ein Wert für erforderlich daysToExpiration (Wert für bewährte AWS Grundregeln für Sicherheit: 90). Der tatsächliche Wert muss den Richtlini en Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
AC-17(2)	Das Informati onssystem implement iert kryptografische Mechanismen, um die Vertraulichkeit und Integrität von Remote-Zugriffssitzungen zu schützen.	alb-http-to-https-Umleitungsprüfung	Um Daten während der Übertragung zu schützen, stellen Sie sicher, dass Ihr Application Load Balancer unverschl üsselte HTTP-Anfr agen automatisch an HTTPS umleitet. Um eventuell vorhanden e sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.
AC-17(2)	Das Informati onssystem implement iert kryptografische Mechanismen, um die Vertraulichkeit und Integrität von Remote-Zugriffssitzungen zu schützen.	redshift-require-tls-ssl	Stellen Sie sicher, dass Ihre Amazon-Redshift-Cluster eine TLS/SSL-Verschlüss elung erfordern, um eine Verbindun g zu SQL-Clients herzustellen. Um eventuell vorhanden e sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
AC-17(2)	Das Informati onssystem implement iert kryptografische Mechanismen, um die Vertraulichkeit und Integrität von Remote-Zugriffssitzungen zu schützen.	s3- bucket-ssl-request s-only	Um Daten während der Übertragung zu schützen, stellen Sie sicher, dass Ihre Amazon Simple Storage Service (Amazon S3)-Bucke ts Anfragen zur Verwendung von Secure Socket Layer (SSL)-Buc kets erfordern. Um eventuell vorhanden e sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
AC-21(b)	Die Organisation: b. Verwendet [Zuweisung: von der Organisation definierte automatisierte Mechanismen oder manuelle Prozesse], um Benutzer bei Entscheidungen hinsichtlich Informationsweitergabe/Zusammenarbeit zu unterstützen.	autoscaling-launch-config-public-ip-deaktiviert	Wenn Sie Ihre Netzwerkschnittstellen mit einer öffentlichen IP-Adresse konfigurieren, sind die diesen Netzwerkschnittstellen zugehörigen Ressourcen über das Internet erreichbar. EC2 Ressourcen sollten nicht öffentlich zugänglich sein, da dies einen unbeabsichtigten Zugriff auf Ihre Anwendungen oder Server ermöglichen kann.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
AC-21(b)	Die Organisation: b. Verwendet [Zuweisung: von der Organisation definierte automatisierte Mechanismen oder manuelle Prozesse], um Benutzer bei Entscheidungen hinsichtlich Informationsweitergabe/Zusammenarbeit zu unterstützen.	no-unrestricted-route-to-igw	Stellen Sie sicher, dass EC2 Amazon-Routentabellen keine uneingeschränkten Routen zu einem Internet-Gateway enthalten. Durch das Entfernen oder Beschränken des Internetzugangs für Workloads innerhalb von Amazon VPCs können unbeabsichtigte Zugriffe in Ihrer Umgebung reduziert werden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
AC-21(b)	Die Organisation: b. Verwendet [Zuweisung: von der Organisation definierte automatisierte Mechanismen oder manuelle Prozesse], um Benutzer bei Entscheidungen hinsichtlich Informationsweitergabe/Zusammenarbeit zu unterstützen.	restricted-common-ports	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass gemeinsame Ports für Amazon Elastic Compute Cloud (Amazon EC2) -Sicherheitsgruppen eingeschränkt sind. Wenn der Zugriff auf Ports nicht auf vertrauenswürdige Quellen beschränkt wird, kann dies zu Angriffen auf die Verfügbarkeit, Integrität und Vertraulichkeit von Systemen führen. Mit dieser Regel können Sie optional die Parameter blockedPort1–blockedPort5 festlegen (Standardkonfigurationen: 20, 21, 3389, 3306, 4333). Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
AC-21(b)	Die Organisation: b. Verwendet [Zuweisung: von der Organisation definierte automatisierte Mechanismen oder manuelle Prozesse], um Benutzer bei Entscheidungen hinsichtlich Informationsweitergabe/ Zusammenarbeit zu unterstützen.	s3- account-level-public-access -Block-periodisch	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Simple Storage Service (Amazon S3) -Buckets nicht öffentlich zugänglich sind. Diese Regel trägt dazu bei, sensible Daten vor unbefugten Remote-Benutzern zu schützen, indem sie den öffentlichen Zugriff verhindert. Mit dieser Regel können Sie optional die Parameter ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) und restrictPublicBuckets Parameter (Config Default: True) festlegen. Die tatsächlichen Werte müssen den Richtlini

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
			en Ihrer Organisation entsprechen.
AC-21(b)	Die Organisation: b. Verwendet [Zuweisung: von der Organisation definierte automatisierte Mechanismen oder manuelle Prozesse], um Benutzer bei Entscheidungen hinsichtlich Informationsweitergabe/Zusammenarbeit zu unterstützen.	vpc-default-security-group-geschlossen	Sicherheitsgruppen von Amazon Elastic Compute Cloud (Amazon EC2) können bei der Verwaltung des Netzwerkzugriffs helfen, indem sie eine statusbehaftete Filterung des ein- und ausgehenden Netzwerkverkehrs zu Ressourcen bereitstellen. AWS Die Beschränkung des gesamten Datenverkehrs auf die Standardsicherheitsgruppe hilft dabei, den Fernzugriff auf Ihre Ressourcen einzuschränken. AWS

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
AC-21(b)	Die Organisation: b. Verwendet [Zuweisung: von der Organisation definierte automatisierte Mechanismen oder manuelle Prozesse], um Benutzer bei Entscheidungen hinsichtlich Informationsweitergabe/Zusammenarbeit zu unterstützen.	vpc-sg-open-only-to-authorized-ports	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass gemeinsame Ports für Amazon Elastic Compute Cloud (Amazon EC2) -Sicherheitsgruppen eingeschränkt sind. Wenn der Zugriff auf Ports nicht auf vertrauenswürdige Quellen beschränkt wird, kann dies zu Angriffen auf die Verfügbarkeit, Integrität und Vertraulichkeit von Systemen führen. Durch die Beschränkung des Zugriffs auf Ressourcen innerhalb einer Sicherheitsgruppe aus dem Internet (0.0.0.0/0) kann der Remote-Zugriff auf interne Systeme gesteuert werden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
AC-21(b)	Die Organisation: b. Verwendet [Zuweisung: von der Organisation definierte automatisierte Mechanismen oder manuelle Prozesse], um Benutzer bei Entscheidungen hinsichtlich Informationsweitergabe/Zusammenarbeit zu unterstützen.	dms-replication-not-public	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass auf DMS-Replikationsinstanzen nicht öffentlich zugegriffen werden kann. DMS-Replikations-Instances können vertrauliche Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.
AC-21(b)	Die Organisation: b. Verwendet [Zuweisung: von der Organisation definierte automatisierte Mechanismen oder manuelle Prozesse], um Benutzer bei Entscheidungen hinsichtlich Informationsweitergabe/Zusammenarbeit zu unterstützen.	ebs-snapshot-public-restorable-überprüfen	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass EBS-Snapshots nicht öffentlich wiederherstellbar sind. EBS-Volume-Snapshots können vertrauliche Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
AC-21(b)	Die Organisation: b. Verwendet [Zuweisung: von der Organisation definierte automatisierte Mechanismen oder manuelle Prozesse], um Benutzer bei Entscheidungen hinsichtlich Informationsweitergabe/Zusammenarbeit zu unterstützen.	ec-2 instance-no-public-ip	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon Elastic Compute Cloud (Amazon EC2) - Instances nicht öffentlich zugänglich sind. EC2 Amazon-Instances können vertrauliche Informationen enthalten, und für solche Konten ist eine Zugriffskontrolle erforderlich.
AC-21(b)	Die Organisation: b. Verwendet [Zuweisung: von der Organisation definierte automatisierte Mechanismen oder manuelle Prozesse], um Benutzer bei Entscheidungen hinsichtlich Informationsweitergabe/Zusammenarbeit zu unterstützen.	emr-master-no-public-ip	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon EMR-Cluster-Masterknoten nicht öffentlich zugänglich sind. Amazon-EMR-Cluster-Hauptknoten können vertrauliche Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
AC-21(b)	Die Organisation: b. Verwendet [Zuweisung: von der Organisation definierte automatisierte Mechanismen oder manuelle Prozesse], um Benutzer bei Entscheidungen hinsichtlich Informationsweitergabe/Zusammenarbeit zu unterstützen.	lambda-function-public-access-verboten	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass AWS Lambda-Funktionen nicht öffentlich zugänglich sind. Der öffentliche Zugriff kann möglicherweise die Verfügbarkeit von Ressourcen beeinträchtigen.
AC-21(b)	Die Organisation: b. Verwendet [Zuweisung: von der Organisation definierte automatisierte Mechanismen oder manuelle Prozesse], um Benutzer bei Entscheidungen hinsichtlich Informationsweitergabe/Zusammenarbeit zu unterstützen.	rds-instance-public-access-überprüfen	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Relational Database Service (Amazon RDS) -Instances nicht öffentlich sind. Amazon-RDS-Datenbank-Instances können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
AC-21(b)	Die Organisation: b. Verwendet [Zuweisung: von der Organisation definierte automatisierte Mechanismen oder manuelle Prozesse], um Benutzer bei Entscheidungen hinsichtlich Informationsweitergabe/Zusammenarbeit zu unterstützen.	rds-snapshots-public-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Relational Database Service (Amazon RDS) -Instances nicht öffentlich sind. Amazon-RDS-Datenbank-Instances können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
AC-21(b)	Die Organisation: b. Verwendet [Zuweisung: von der Organisation definierte automatisierte Mechanismen oder manuelle Prozesse], um Benutzer bei Entscheidungen hinsichtlich Informationsweitergabe/Zusammenarbeit zu unterstützen.	redshift-cluster-public-access-überprüfen	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Redshift Redshift-Cluster nicht öffentlich sind. Amazon-Redshift-Cluster können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
AC-21(b)	Die Organisation: b. Verwendet [Zuweisung: von der Organisation definierte automatisierte Mechanismen oder manuelle Prozesse], um Benutzer bei Entscheidungen hinsichtlich Informationsweitergabe/Zusammenarbeit zu unterstützen.	s3- verboten bucket-level-public-access	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Simple Storage Service (Amazon S3) -Buckets nicht öffentlich zugänglich sind. Diese Regel trägt dazu bei, sensible Daten vor unbefugten Remote-Benutzern zu schützen, indem sie den öffentlichen Zugriff auf Bucket-Ebene verhindert.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
AC-21(b)	Die Organisation: b. Verwendet [Zuweisung: von der Organisation definierte automatisierte Mechanismen oder manuelle Prozesse], um Benutzer bei Entscheidungen hinsichtlich Informationsweitergabe/Zusammenarbeit zu unterstützen.	s-3 bucket-public-read-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie nur autorisierten Benutzern, Prozessen und Geräten Zugriff auf Amazon Simple Storage Service (Amazon S3) - Buckets gewähren. Die Verwaltung des Zugriffs sollte mit der Klassifizierung der Daten übereinstimmen.
AC-21(b)	Die Organisation: b. Verwendet [Zuweisung: von der Organisation definierte automatisierte Mechanismen oder manuelle Prozesse], um Benutzer bei Entscheidungen hinsichtlich Informationsweitergabe/Zusammenarbeit zu unterstützen.	s3- bucket-public-write-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie nur autorisierten Benutzern, Prozessen und Geräten Zugriff auf Amazon Simple Storage Service (Amazon S3) - Buckets gewähren. Die Verwaltung des Zugriffs sollte mit der Klassifizierung der Daten übereinstimmen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
AC-21(b)	Die Organisation: b. Verwendet [Zuweisung: von der Organisation definierte automatisierte Mechanismen oder manuelle Prozesse], um Benutzer bei Entscheidungen hinsichtlich Informationsweitergabe/Zusammenarbeit zu unterstützen.	sagemaker-notebook-no-direct-Internetzugang	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass SageMaker Amazon-Notebooks keinen direkten Internetzugang zulassen. Indem Sie direkten Internetzugang blockieren, vermeiden Sie, dass unbefugte Benutzer auf sensible Daten zugreifen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
AC-21(b)	Die Organisation: b. Verwendet [Zuweisung: von der Organisation definierte automatisierte Mechanismen oder manuelle Prozesse], um Benutzer bei Entscheidungen hinsichtlich Informationsweitergabe/Zusammenarbeit zu unterstützen.	subnet-auto-assign-public-ip-deaktiviert	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon Virtual Private Cloud (VPC) -Subnetzen nicht automatisch eine öffentliche IP-Adresse zugewiesen wird. Amazon Elastic Compute Cloud (EC2) -Instances, die in Subnetzen gestartet werden, in denen dieses Attribut aktiviert ist, haben ihrer primären Netzwerkschnittstelle eine öffentliche IP-Adresse zugewiesen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
AU-2(a)(d)	Die Organisation: a. Legt fest, dass das Informationssystem folgenden Ereignisse überprüfen kann: Erfolgreiche und erfolglose Kontoanmeldungen, Kontoverwaltungsereignisse, Objektzugriffe, Richtlinienänderungen, Berechtigungsfunktionen, Prozessnachverfolgung und Systemereignisse. Für Webanwendungen: sämtliche Administratoraktivitäten, Authentifizierungsprüfungen, Autorisierungsprüfungen, Datenlöschungen, Datenzugriffe, Datenänderungen und Berechtigungsänderungen. d. Legt fest, dass die folgenden Ereignisse innerhalb des Informationssystems geprüft werden müssen: [von der	codebuild-project-logging-enabled	Stellen Sie sicher, dass die AWS CodeBuild Projektprotokollierung aktiviert ist, damit Ihre Build-Ausgabeprotokolle entweder an Amazon CloudWatch oder Amazon Simple Storage Service (Amazon S3) gesendet werden. Build-Ausgabeprotokolle enthalten detaillierte Informationen zu Ihrem Build-Projekt.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
	Organisation definiert e Teilmenge der in AU-2(a) definierten prüffähigen Ereigniss e wird kontinuierlich für jedes identifizierte Ereignis geprüft].		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
AU-2(a)(d)	Die Organisation: a. Legt fest, dass das Informationssystem folgenden Ereignisse überprüfen kann: Erfolgreiche und erfolglose Kontoanmeldungen, Kontoverwaltungsereignisse, Objektzugriffe, Richtlinienänderungen, Berechtigungsfunktionen, Prozessnachverfolgung und Systemereignisse. Für Webanwendungen: sämtliche Administratoraktivitäten, Authentifizierungsprüfungen, Autorisierungsprüfungen, Datenlöschungen, Datenzugriffe, Datenänderungen und Berechtigungsänderungen. d. Legt fest, dass die folgenden Ereignisse innerhalb des Informationssystems geprüft werden müssen: [von der	multi-region-cloudtrail-enabled	AWS CloudTrail zeichnet Aktionen und API-Aufrufe der AWS Management Console auf. Sie können feststellen, welche Benutzer und Konten angerufen wurden AWS, von welcher Quell-IP-Adresse aus die Anrufe getätigt wurden und wann die Anrufe erfolgten. CloudTrail übermittelt Protokolldateien aus allen AWS Regionen an Ihren S3-Bucket, wenn MULTI_REGION_CLOUD_TRAIL_ENABLED aktiviert ist. Außerdem wird beim AWS Start einer neuen Region derselbe Trail in der neuen Region erstellt. CloudTrail Dadurch erhalten Sie automatisch Protokolldateien mit API-Aktivitäten für die neue Region.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
	Organisation definiert e Teilmenge der in AU-2(a) definierten prüffähigen Ereigniss e wird kontinuierlich für jedes identifizierte Ereignis geprüft].		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
AU-2(a)(d)	Die Organisation: a. Legt fest, dass das Informationssystem folgenden Ereignisse überprüfen kann: Erfolgreiche und erfolglose Kontoanmeldungen, Kontoverwaltungsereignisse, Objektzugriffe, Richtlinienänderungen, Berechtigungsfunktionen, Prozessnachverfolgung und Systemereignisse. Für Webanwendungen: sämtliche Administratoraktivitäten, Authentifizierungsprüfungen, Autorisierungsprüfungen, Datenlöschungen, Datenzugriffe, Datenänderungen und Berechtigungsänderungen. d. Legt fest, dass die folgenden Ereignisse innerhalb des Informationssystems geprüft werden müssen: [von der	rds-logging-enabled	Um die Protokollierung und Überwachung in Ihrer Umgebung zu erleichtern, stellen Sie sicher, dass die Amazon Relational Database Service (Amazon RDS)-Protokollierung aktiviert ist. Mit der Amazon-RDS-Protokollierung können Sie Ereignisse wie Verbindungen, Verbindungsabbrüche, Abfragen oder abgefragte Tabellen erfassen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
	Organisation definiert e Teilmenge der in AU-2(a) definierten prüffähigen Ereigniss e wird kontinuierlich für jedes identifizierte Ereignis geprüft].		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
AU-2(a)(d)	Die Organisation: a. Legt fest, dass das Informationssystem folgenden Ereignisse überprüfen kann: Erfolgreiche und erfolglose Kontoanmeldungen, Kontoverwaltungsereignisse, Objektzugriffe, Richtlinienänderungen, Berechtigungsfunktionen, Prozessnachverfolgung und Systemereignisse. Für Webanwendungen: sämtliche Administratoraktivitäten, Authentifizierungsprüfungen, Autorisierungsprüfungen, Datenlöschungen, Datenzugriffe, Datenänderungen und Berechtigungsänderungen. d. Legt fest, dass die folgenden Ereignisse innerhalb des Informationssystems geprüft werden müssen: [von der	wafv2-logging-enabled	Um die Protokollierung und Überwachung in Ihrer Umgebung zu erleichtern, aktivieren Sie die AWS WAF (V2) -Protokollierung im regionalen und globalen Web ACLs. AWS Die WAF-Protokollierung bietet detaillierte Informationen über den Datenverkehr, der von Ihrer Web-ACL analysiert wird. In den Protokollen werden die Uhrzeit aufgezeichnet, zu der die AWS WAF die Anfrage von Ihrer AWS Ressource erhalten hat, Informationen zu der Anfrage und eine Aktion für die Regel, der jede Anfrage entsprach.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
	Organisation definiert e Teilmenge der in AU-2(a) definierten prüffähigen Ereigniss e wird kontinuierlich für jedes identifizierte Ereignis geprüft].		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
AU-2(a)(d)	Die Organisation: a. Legt fest, dass das Informationssystem folgenden Ereignisse überprüfen kann: Erfolgreiche und erfolglose Kontoanmeldungen, Kontoverwaltungsereignisse, Objektzugriffe, Richtlinienänderungen, Berechtigungsfunktionen, Prozessnachverfolgung und Systemereignisse. Für Webanwendungen: sämtliche Administratoraktivitäten, Authentifizierungsprüfungen, Autorisierungsprüfungen, Datenlöschungen, Datenzugriffe, Datenänderungen und Berechtigungsänderungen. d. Legt fest, dass die folgenden Ereignisse innerhalb des Informationssystems geprüft werden müssen: [von der	api-gw-execution-logging-aktiviert	Die API-Gateway-Protokollierung zeigt detaillierte Ansichten der Benutzer, die auf die API zugegriffen haben, und wie diese Benutzer auf die API zugegriffen haben. Diese Einblicke ermöglichen die Transparenz von Benutzeraktivitäten.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
	Organisation definiert e Teilmenge der in AU-2(a) definierten prüffähigen Ereigniss e wird kontinuierlich für jedes identifizierte Ereignis geprüft].		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
AU-2(a)(d)	Die Organisation: a. Legt fest, dass das Informationssystem folgenden Ereignisse überprüfen kann: Erfolgreiche und erfolglose Kontoanmeldungen, Kontoverwaltungsereignisse, Objektzugriffe, Richtlinienänderungen, Berechtigungsfunktionen, Prozessnachverfolgung und Systemereignisse. Für Webanwendungen: sämtliche Administratoraktivitäten, Authentifizierungsprüfungen, Autorisierungsprüfungen, Datenlöschungen, Datenzugriffe, Datenänderungen und Berechtigungsänderungen. d. Legt fest, dass die folgenden Ereignisse innerhalb des Informationssystems geprüft werden müssen: [von der	cloud-trail-cloud-watch-logs-aktiviert	Verwenden Sie Amazon CloudWatch , um Protokollereignisaktivitäten zentral zu sammeln und zu verwalten. Die Aufnahme von AWS CloudTrail Daten liefert Einzelheiten zu den API-Aufrufaktivitäten in Ihrem AWS-Konto.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
	Organisation definiert e Teilmenge der in AU-2(a) definierten prüffähigen Ereigniss e wird kontinuierlich für jedes identifizierte Ereignis geprüft].		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
AU-2(a)(d)	Die Organisation: a. Legt fest, dass das Informationssystem folgenden Ereignisse überprüfen kann: Erfolgreiche und erfolglose Kontoanmeldungen, Kontoverwaltungsereignisse, Objektzugriffe, Richtlinienänderungen, Berechtigungsfunktionen, Prozessnachverfolgung und Systemereignisse. Für Webanwendungen: sämtliche Administratoraktivitäten, Authentifizierungsprüfungen, Autorisierungsprüfungen, Datenlöschungen, Datenzugriffe, Datenänderungen und Berechtigungsänderungen. d. Legt fest, dass die folgenden Ereignisse innerhalb des Informationssystems geprüft werden müssen: [von der	cloudtrail-enabled	AWS CloudTrail kann bei der Nichtabstreitbarkeit helfen, indem Aktionen und API-Aufrufe der AWS Management Console aufgezeichnet werden. Sie können die Benutzer und die Benutzer AWS-Konten , die einen AWS Dienst aufgerufen haben, die Quell-IP-Adresse, über die die Aufrufe generiert wurden, und den Zeitpunkt der Anrufe identifizieren. Einzelheiten zu den erfassten Daten finden Sie in den AWS CloudTrail Datensatzinhalten.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
	Organisation definiert e Teilmenge der in AU-2(a) definierten prüffähigen Ereigniss e wird kontinuierlich für jedes identifizierte Ereignis geprüft].		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
AU-2(a)(d)	Die Organisation: a. Legt fest, dass das Informationssystem folgenden Ereignisse überprüfen kann: Erfolgreiche und erfolglose Kontoanmeldungen, Kontoverwaltungsereignisse, Objektzugriffe, Richtlinienänderungen, Berechtigungsfunktionen, Prozessnachverfolgung und Systemereignisse. Für Webanwendungen: sämtliche Administratoraktivitäten, Authentifizierungsprüfungen, Autorisierungsprüfungen, Datenlöschungen, Datenzugriffe, Datenänderungen und Berechtigungsänderungen. d. Legt fest, dass die folgenden Ereignisse innerhalb des Informationssystems geprüft werden müssen: [von der	cloudtrail-s3-dataevents-enabled	Die Erfassung von Simple Storage Service (Amazon S3)-Datenereignissen unterstützt die Erkennung von ungewöhnlichen Aktivitäten. Zu den Details gehören AWS-Konto Informationen über den Zugriff auf einen Amazon S3 S3-Bucket, die IP-Adresse und die Uhrzeit des Ereignisses.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
	Organisation definiert e Teilmenge der in AU-2(a) definierten prüffähigen Ereigniss e wird kontinuierlich für jedes identifizierte Ereignis geprüft].		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
AU-2(a)(d)	Die Organisation: a. Legt fest, dass das Informationssystem folgenden Ereignisse überprüfen kann: Erfolgreiche und erfolglose Kontoanmeldungen, Kontoverwaltungsereignisse, Objektzugriffe, Richtlinienänderungen, Berechtigungsfunktionen, Prozessnachverfolgung und Systemereignisse. Für Webanwendungen: sämtliche Administratoraktivitäten, Authentifizierungsprüfungen, Autorisierungsprüfungen, Datenlöschungen, Datenzugriffe, Datenänderungen und Berechtigungsänderungen. d. Legt fest, dass die folgenden Ereignisse innerhalb des Informationssystems geprüft werden müssen: [von der	elb-logging-enabled	Die Elastic-Load-Balancing-Aktivität ist ein zentraler Kommunikationspunkt innerhalb einer Umgebung. Stellen Sie sicher, dass die ELB-Protokollierung aktiviert ist. Die gesammelten Daten enthalten detaillierte Informationen zu Anfragen, die an den ELB gesendet wurden. Jedes Protokoll enthält Informationen wie die Zeit, zu der die Anforderung einging, die Client-IP-Adresse, Latenzen, Anforderungspfade und Serverantworten.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
	Organisation definiert e Teilmenge der in AU-2(a) definierten prüffähigen Ereigniss e wird kontinuierlich für jedes identifizierte Ereignis geprüft].		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
AU-2(a)(d)	Die Organisation: a. Legt fest, dass das Informationssystem folgenden Ereignisse überprüfen kann: Erfolgreiche und erfolglose Kontoanmeldungen, Kontoverwaltungsereignisse, Objektzugriffe, Richtlinienänderungen, Berechtigungsfunktionen, Prozessnachverfolgung und Systemereignisse. Für Webanwendungen: sämtliche Administratoraktivitäten, Authentifizierungsprüfungen, Autorisierungsprüfungen, Datenlöschungen, Datenzugriffe, Datenänderungen und Berechtigungsänderungen. d. Legt fest, dass die folgenden Ereignisse innerhalb des Informationssystems geprüft werden müssen: [von der	redshift-cluster-configuration-check	Um Daten im Ruhezustand zu schützen, muss die Verschlüsselung für Ihre Amazon-Redshift-Cluster aktiviert sein. Sie müssen auch sicherstellen, dass die erforderlichen Konfigurationen auf Amazon-Redshift-Clustern bereitgestellt werden. Die Prüfungsprotokollierung muss aktiviert sein, um Informationen zu Verbindungen und Benutzeraktivitäten in der Datenbank bereitzustellen. Diese Regel erfordert, dass ein Wert für clusterDbEncrypted (Config Default: TRUE) und LoggingEnabled (Config Default: TRUE) gesetzt ist. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
	Organisation definiert e Teilmenge der in AU-2(a) definierten prüffähigen Ereigniss e wird kontinuierlich für jedes identifizierte Ereignis geprüft].		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
AU-2(a)(d)	Die Organisation: a. Legt fest, dass das Informationssystem folgenden Ereignisse überprüfen kann: Erfolgreiche und erfolglose Kontoanmeldungen, Kontoverwaltungsereignisse, Objektzugriffe, Richtlinienänderungen, Berechtigungsfunktionen, Prozessnachverfolgung und Systemereignisse. Für Webanwendungen: sämtliche Administratoraktivitäten, Authentifizierungsprüfungen, Autorisierungsprüfungen, Datenlöschungen, Datenzugriffe, Datenänderungen und Berechtigungsänderungen. d. Legt fest, dass die folgenden Ereignisse innerhalb des Informationssystems geprüft werden müssen: [von der	s3- bucket-logging-enabled	Die Amazon Simple Storage Service (Amazon S3)-Serverzugriffsprotokollierung bietet eine Methode zur Überwachung des Netzwerks im Hinblick auf potenzielle Cybersicherheitsereignisse. Die Ereignisse werden überwacht, indem detaillierte Aufzeichnungen über die Anfragen erfasst werden, die an einen Amazon-S3-Bucket gestellt wurden. Jeder Zugriffsprotokolleintrag enthält Details zu einer einzelnen Zugriffsanfrage. Zu den Details gehören Anforderer, Bucket-Name, Anforderungszeit, Anforderungsaktion, Antwortstatus und Fehlercode, falls relevant.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
	Organisation definiert e Teilmenge der in AU-2(a) definierten prüffähigen Ereigniss e wird kontinuierlich für jedes identifizierte Ereignis geprüft].		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
AU-2(a)(d)	Die Organisation: a. Legt fest, dass das Informationssystem folgenden Ereignisse überprüfen kann: Erfolgreiche und erfolglose Kontoanmeldungen, Kontoverwaltungsereignisse, Objektzugriffe, Richtlinienänderungen, Berechtigungsfunktionen, Prozessnachverfolgung und Systemereignisse. Für Webanwendungen: sämtliche Administratoraktivitäten, Authentifizierungsprüfungen, Autorisierungsprüfungen, Datenlöschungen, Datenzugriffe, Datenänderungen und Berechtigungsänderungen. d. Legt fest, dass die folgenden Ereignisse innerhalb des Informationssystems geprüft werden müssen: [von der	vpc-flow-logs-enabled	VPC-Flow-Protokolle erfassen detaillierte Informationsdatensätze über den IP-Datenverkehr, der zu und von Netzwerkschnittstellen in Ihrer Amazon Virtual Private Cloud (Amazon VPC) fließt. Standardmäßig enthalten Flow-Protokolldatensätze Werte für die verschiedenen Komponenten des IP-Flows, einschließlich Quelle, Ziel und Protokoll.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
	Organisation definiert e Teilmenge der in AU-2(a) definierten prüffähigen Ereigniss e wird kontinuierlich für jedes identifizierte Ereignis geprüft].		
AU-3	Das Informati onssystem generiert Prüfprotokolle mit Informationen, aus denen hervorgeh t, welche Art von Ereignis eingetret en ist, wann und wo das Ereignis stattgefunden hat, welchen Ursprung das Ereignis hat, wie es ausging und mit welchen Personen oder Subjekten das Ereignis in Verbindun g steht.	codebuild-project-logging-enabled	Stellen Sie sicher, dass die AWS CodeBuild Projektpr otokollierung aktiviert ist, damit Ihre Build-Ausgabeproto kolle entweder an Amazon CloudWatc h oder Amazon Simple Storage Service (Amazon S3) gesendet werden. Build-Ausgabeproto kolle enthalten detaillierte Informati onen zu Ihrem Build-Projekt.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
AU-3	Das Informati onssystem generiert Prüfprotokolle mit Informationen, aus denen hervorgeh t, welche Art von Ereignis eingetret en ist, wann und wo das Ereignis stattgefunden hat, welchen Ursprung das Ereignis hat, wie es ausging und mit welchen Personen oder Subjekten das Ereignis in Verbindun g steht.	multi-region-cloudtrail-enabled	AWS CloudTrail zeichnet Aktionen und API-Aufrufe der AWS Management Console auf. Sie können feststellen, welche Benutzer und Konten angerufen wurden AWS, von welcher Quell-IP-Adresse aus die Anrufe getätigt wurden und wann die Anrufe erfolgten. CloudTrail übermittelt Protokolldateien aus allen AWS Regionen an Ihren S3-Bucket , wenn MULTI_REG ION_CLOUD _TRAIL_ENABLED aktiviert ist. Außerdem wird beim AWS Start einer neuen Region derselbe Trail in der neuen Region erstellt. CloudTrail Dadurch erhalten Sie automatis ch Protokolldateien mit API-Aktivitäten für die neue Region.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
AU-3	Das Informationssystem generiert Prüfprotokolle mit Informationen, aus denen hervorgeht, welche Art von Ereignis eingetreten ist, wann und wo das Ereignis stattgefunden hat, welchen Ursprung das Ereignis hat, wie es ausging und mit welchen Personen oder Subjekten das Ereignis in Verbindung steht.	rds-logging-enabled	Um die Protokollierung und Überwachung in Ihrer Umgebung zu erleichtern, stellen Sie sicher, dass die Amazon Relational Database Service (Amazon RDS)-Protokollierung aktiviert ist. Mit der Amazon-RDS-Protokollierung können Sie Ereignisse wie Verbindungen, Verbindungsabbrüche, Abfragen oder abgefragte Tabellen erfassen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
AU-3	Das Informationssystem generiert Prüfprotokolle mit Informationen, aus denen hervorgeht, welche Art von Ereignis eingetreten ist, wann und wo das Ereignis stattgefunden hat, welchen Ursprung das Ereignis hat, wie es ausging und mit welchen Personen oder Subjekten das Ereignis in Verbindung steht.	wafv2-logging-enabled	Um die Protokollierung und Überwachung in Ihrer Umgebung zu erleichtern, aktivieren Sie die AWS WAF (V2) -Protokollierung im regionalen und globalen Web ACLs. AWS Die WAF-Protokollierung bietet detaillierte Informationen über den Datenverkehr, der von Ihrer Web-ACL analysiert wird. In den Protokollen werden die Uhrzeit aufgezeichnet, zu der die AWS WAF die Anfrage von Ihrer AWS Ressource erhalten hat, Informationen zu der Anfrage und eine Aktion für die Regel, der jede Anfrage entsprach.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
AU-3	Das Informati onssystem generiert Prüfprotokolle mit Informationen, aus denen hervorgeh t, welche Art von Ereignis eingetret en ist, wann und wo das Ereignis stattgefunden hat, welchen Ursprung das Ereignis hat, wie es ausging und mit welchen Personen oder Subjekten das Ereignis in Verbindun g steht.	api-gw-execution-l ogging-aktiviert	Die API-Gateway-Protokollierung zeigt detaillierte Ansichten der Benutzer, die auf die API zugegriff en haben, und wie diese Benutzer auf die API zugegriff en haben. Diese Einblicke ermöglichen die Transparenz von Benutzeraktivitäten.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
AU-3	Das Informati onssystem generiert Prüfprotokolle mit Informationen, aus denen hervorgeh t, welche Art von Ereignis eingetret en ist, wann und wo das Ereignis stattgefunden hat, welchen Ursprung das Ereignis hat, wie es ausging und mit welchen Personen oder Subjekten das Ereignis in Verbindun g steht.	cloud-trail-cloud-watch-logs-aktiviert	Verwenden Sie Amazon CloudWatc h , um Protokoll ereignisaktivitäten zentral zu sammeln und zu verwalten. Die Aufnahme von AWS CloudTrail Daten liefert Einzelheiten zu den API-Aufrufaktivitä ten in Ihrem AWS-Konto.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
AU-3	Das Informati onssystem generiert Prüfprotokolle mit Informationen, aus denen hervorgeh t, welche Art von Ereignis eingetret en ist, wann und wo das Ereignis stattgefunden hat, welchen Ursprung das Ereignis hat, wie es ausging und mit welchen Personen oder Subjekten das Ereignis in Verbindun g steht.	cloudtrail-enabled	AWS CloudTrail kann bei der Nichtabst reitbarkeit helfen, indem Aktionen und API-Aufrufe der AWS Management Console aufgezeic hnet werden. Sie können die Benutzer und die Benutzer AWS-Konten , die einen AWS Dienst aufgerufen haben, die Quell-IP-Adresse, über die die Aufrufe generiert wurden, und den Zeitpunkt der Anrufe identifiz ieren. Einzelheiten zu den erfassten Daten finden Sie in den AWS CloudTrail Datensatzinhalten.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
AU-3	Das Informati onssystem generiert Prüfprotokolle mit Informationen, aus denen hervorgeh t, welche Art von Ereignis eingetret en ist, wann und wo das Ereignis stattgefunden hat, welchen Ursprung das Ereignis hat, wie es ausging und mit welchen Personen oder Subjekten das Ereignis in Verbindun g steht.	cloudtrail-s3-data events-enabled	Die Erfassung von Simple Storage Service (Amazon S3)-Datenereigniss en unterstützt die Erkennung von ungewöhnlichen Aktivitäten. Zu den Details gehören AWS-Konto Informationen über den Zugriff auf einen Amazon S3 S3-Bucket, die IP-Adress e und die Uhrzeit des Ereignisses.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
AU-3	Das Informati onssystem generiert Prüfprotokolle mit Informationen, aus denen hervorgeh t, welche Art von Ereignis eingetret en ist, wann und wo das Ereignis stattgefunden hat, welchen Ursprung das Ereignis hat, wie es ausging und mit welchen Personen oder Subjekten das Ereignis in Verbindun g steht.	elb-logging-enabled	Die Elastic-Load-Balancing-Aktivität ist ein zentraler Kommunikationspunk t innerhalb einer Umgebung. Stellen Sie sicher, dass die ELB-Protokollierun g aktiviert ist. Die gesammelten Daten enthalten detaillie rte Informationen zu Anfragen, die an den ELB gesendet wurden. Jedes Protokoll enthält Informationen wie die Zeit, zu der die Anforderung einging, die Client-IP -Adresse, Latenzen, Anforderungspfade und Serverantworten.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
AU-3	Das Informationssystem generiert Prüfprotokolle mit Informationen, aus denen hervorgeht, welche Art von Ereignis eingetreten ist, wann und wo das Ereignis stattgefunden hat, welchen Ursprung das Ereignis hat, wie es ausging und mit welchen Personen oder Subjekten das Ereignis in Verbindung steht.	redshift-cluster-configuration-check	Um Daten im Ruhezustand zu schützen, muss die Verschlüsselung für Ihre Amazon-Redshift-Cluster aktiviert sein. Sie müssen auch sicherstellen, dass die erforderlichen Konfigurationen auf Amazon-Redshift-Clustern bereitgestellt werden. Die Prüfungsprotokollierung muss aktiviert sein, um Informationen zu Verbindungen und Benutzeraktivitäten in der Datenbank bereitzustellen. Diese Regel erfordert, dass ein Wert für clusterDbEncrypted (Config Default: TRUE) und LoggingEnabled (Config Default: TRUE) gesetzt ist. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
AU-3	Das Informati onssystem generiert Prüfprotokolle mit Informationen, aus denen hervorgeh t, welche Art von Ereignis eingetret en ist, wann und wo das Ereignis stattgefunden hat, welchen Ursprung das Ereignis hat, wie es ausging und mit welchen Personen oder Subjekten das Ereignis in Verbindun g steht.	s3- bucket-logging-enabled	Die Amazon Simple Storage Service (Amazon S3)-Serverzugriffs protokollierung bietet eine Methode zur Überwachu ng des Netzwerks im Hinblick auf potenzielle Cybersich erheitsereignisse. Die Ereignisse werden überwacht, indem detaillierte Aufzeichn ungen über die Anfragen erfasst werden, die an einen Amazon-S3-Bucket gestellt wurden. Jeder Zugriffsprotokolle intrag enthält Details zu einer einzelnen Zugriffsanfrage. Zu den Details gehören Anforderer, Bucket-Name, Anforderu ngszeit, Anforderu ngsaktion, Antwortst atus und Fehlercode, falls relevant.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
AU-3	Das Informationssystem generiert Prüfprotokolle mit Informationen, aus denen hervorgeht, welche Art von Ereignis eingetreten ist, wann und wo das Ereignis stattgefunden hat, welchen Ursprung das Ereignis hat, wie es ausging und mit welchen Personen oder Subjekten das Ereignis in Verbindung steht.	vpc-flow-logs-enabled	VPC-Flow-Protokolle erfassen detaillierte Informationsdatensätze über den IP-Datenverkehr, der zu und von Netzwerkschnittstellen in Ihrer Amazon Virtual Private Cloud (Amazon VPC) fließt. Standardmäßig enthalten Flow-Protokolldatensätze Werte für die verschiedenen Komponenten des IP-Flows, einschließlich Quelle, Ziel und Protokoll.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
AU-6(1)(3)	(1) Die Organisation setzt automatisierte Mechanismen zur Integration von Prüfungs-, Analyse- und Berichtsprozessen ein, um die Prozesse der Organisation zur Untersuchung und Reaktion auf verdächtige Aktivitäten zu unterstützen. (3) Die Organisation analysiert und korreliert Prüfungsunterlagen aus verschiedenen Repositorys, um sich ein Bild über die Situation in der gesamten Organisation zu verschaffen.	codebuild-project-logging-enabled	Stellen Sie sicher, dass die AWS CodeBuild Projektprotokollierung aktiviert ist, damit Ihre Build-Ausgabeprotokolle entweder an Amazon CloudWatch oder Amazon Simple Storage Service (Amazon S3) gesendet werden. Build-Ausgabeprotokolle enthalten detaillierte Informationen zu Ihrem Build-Projekt.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
AU-6(1)(3)	(1) Die Organisation setzt automatisierte Mechanismen zur Integration von Prüfungs-, Analyse- und Berichtsprozessen ein, um die Prozesse der Organisation zur Untersuchung und Reaktion auf verdächtige Aktivitäten zu unterstützen. (3) Die Organisation analysiert und korreliert Prüfungsunterlagen aus verschiedenen Repositorys, um sich ein Bild über die Situation in der gesamten Organisation zu verschaffen.	cw-loggroup-retention-period-überprüfen	Stellen Sie sicher, dass die Ereignisprotokolldaten für Ihre Protokollgruppen über eine Mindestdauer aufbewahrt werden, um die Fehlerbehebung und forensische Untersuchungen zu unterstützen. Fehlende frühere Ereignisprotokolldaten erschweren die Rekonstruierung und Identifizierung potenziell schädlicher Ereignisse.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
AU-6(1)(3)	(1) Die Organisation setzt automatisierte Mechanismen zur Integration von Prüfungs-, Analyse- und Berichtsprozessen ein, um die Prozesse der Organisation zur Untersuchung und Reaktion auf verdächtige Aktivitäten zu unterstützen. (3) Die Organisation analysiert und korreliert Prüfungsunterlagen aus verschiedenen Repositorys, um sich ein Bild über die Situation in der gesamten Organisation zu verschaffen.	multi-region-cloudtrail-enabled	AWS CloudTrail zeichnet Aktionen und API-Aufrufe der AWS Management Console auf. Sie können feststellen, welche Benutzer und Konten angerufen wurden AWS, von welcher Quell-IP-Adresse aus die Anrufe getätigt wurden und wann die Anrufe erfolgten. CloudTrail übermittelt Protokolldateien aus allen AWS Regionen an Ihren S3-Bucket, wenn MULTI_REGION_CLOUD_TRAIL_ENABLED aktiviert ist. Außerdem wird beim AWS Start einer neuen Region derselbe Trail in der neuen Region erstellt. CloudTrail Dadurch erhalten Sie automatisch Protokolldateien mit API-Aktivitäten für die neue Region.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
AU-6(1)(3)	(1) Die Organisation setzt automatisierte Mechanismen zur Integration von Prüfungs-, Analyse- und Berichtsprozessen ein, um die Prozesse der Organisation zur Untersuchung und Reaktion auf verdächtige Aktivitäten zu unterstützen. (3) Die Organisation analysiert und korreliert Prüfungsunterlagen aus verschiedenen Repositorys, um sich ein Bild über die Situation in der gesamten Organisation zu verschaffen.	securityhub-enabled	AWS Security Hub hilft bei der Überwachung von unbefugtem Personal, Verbindungen, Geräten und Software. AWS Security Hub aggregiert, organisiert und priorisiert die Sicherheitswarnungen oder Ergebnisse mehrerer Dienste. AWS Einige dieser Dienste sind Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer und AWS Firewall Manager sowie AWS Partnerlösungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
AU-6(1)(3)	(1) Die Organisation setzt automatisierte Mechanismen zur Integration von Prüfungs-, Analyse- und Berichtsprozessen ein, um die Prozesse der Organisation zur Untersuchung und Reaktion auf verdächtige Aktivitäten zu unterstützen. (3) Die Organisation analysiert und korreliert Prüfungsunterlagen aus verschiedenen Repositorys, um sich ein Bild über die Situation in der gesamten Organisation zu verschaffen.	wafv2-logging-enabled	Um Ihnen bei der Protokollierung und Überwachung in Ihrer Umgebung zu helfen, aktivieren Sie die AWS WAF (V2) -Protokollierung im regionalen und globalen Web. ACLs AWS Die WAF-Protokollierung bietet detaillierte Informationen über den Datenverkehr, der von Ihrer Web-ACL analysiert wird. In den Protokollen werden die Uhrzeit aufgezeichnet, zu der die AWS WAF die Anfrage von Ihrer AWS Ressource erhalten hat, Informationen zu der Anfrage und eine Aktion für die Regel, der jede Anfrage entsprach.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
AU-6(1)(3)	(1) Die Organisation setzt automatisierte Mechanismen zur Integration von Prüfungs-, Analyse- und Berichtsprozessen ein, um die Prozesse der Organisation zur Untersuchung und Reaktion auf verdächtige Aktivitäten zu unterstützen. (3) Die Organisation analysiert und korreliert Prüfungsunterlagen aus verschiedenen Repositorys, um sich ein Bild über die Situation in der gesamten Organisation zu verschaffen.	api-gw-execution-logging-aktiviert	Die API-Gateway-Protokollierung zeigt detaillierte Ansichten der Benutzer, die auf die API zugegriffen haben, und wie diese Benutzer auf die API zugegriffen haben. Diese Einblicke ermöglichen die Transparenz von Benutzeraktivitäten.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
AU-6(1)(3)	(1) Die Organisation setzt automatisierte Mechanismen zur Integration von Prüfungs-, Analyse- und Berichtsprozessen ein, um die Prozesse der Organisation zur Untersuchung und Reaktion auf verdächtige Aktivitäten zu unterstützen. (3) Die Organisation analysiert und korreliert Prüfungsunterlagen aus verschiedenen Repositorys, um sich ein Bild über die Situation in der gesamten Organisation zu verschaffen.	cloud-trail-cloud-watch-logs-aktiviert	Verwenden Sie Amazon CloudWatch , um Protokoll ereignisaktivitäten zentral zu sammeln und zu verwalten. Die Aufnahme von AWS CloudTrail Daten liefert Einzelheiten zu den API-Aufrufaktivitäten in Ihrem AWS-Konto.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
AU-6(1)(3)	(1) Die Organisation setzt automatisierte Mechanismen zur Integration von Prüfungs-, Analyse- und Berichtsprozessen ein, um die Prozesse der Organisation zur Untersuchung und Reaktion auf verdächtige Aktivitäten zu unterstützen. (3) Die Organisation analysiert und korreliert Prüfungsunterlagen aus verschiedenen Repositorys, um sich ein Bild über die Situation in der gesamten Organisation zu verschaffen.	cloudtrail-enabled	AWS CloudTrail kann bei der Nichtabstreitbarkeit helfen, indem Aktionen und API-Aufrufe der AWS Management Console aufgezeichnet werden. Sie können die Benutzer und die Benutzer AWS-Konten , die einen AWS Dienst aufgerufen haben, die Quell-IP-Adresse, über die die Aufrufe generiert wurden, und den Zeitpunkt der Anrufe identifizieren. Einzelheiten zu den erfassten Daten finden Sie in den AWS CloudTrail Datensatzinhalten.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
AU-6(1)(3)	(1) Die Organisation setzt automatisierte Mechanismen zur Integration von Prüfungs-, Analyse- und Berichtsprozessen ein, um die Prozesse der Organisation zur Untersuchung und Reaktion auf verdächtige Aktivitäten zu unterstützen. (3) Die Organisation analysiert und korreliert Prüfungsunterlagen aus verschiedenen Repositorys, um sich ein Bild über die Situation in der gesamten Organisation zu verschaffen.	cloudtrail-s3-dataevents-enabled	Die Erfassung von Simple Storage Service (Amazon S3)-Datenereignissen unterstützt die Erkennung von ungewöhnlichen Aktivitäten. Zu den Details gehören AWS-Konto Informationen über den Zugriff auf einen Amazon S3 S3-Bucket, die IP-Adresse und die Uhrzeit des Ereignisses.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
AU-6(1)(3)	(1) Die Organisation setzt automatisierte Mechanismen zur Integration von Prüfungs-, Analyse- und Berichtsprozessen ein, um die Prozesse der Organisation zur Untersuchung und Reaktion auf verdächtige Aktivitäten zu unterstützen. (3) Die Organisation analysiert und korreliert Prüfungsunterlagen aus verschiedenen Repositorys, um sich ein Bild über die Situation in der gesamten Organisation zu verschaffen.	cloudwatch-alarm-action-check	Amazon CloudWatch alarmiert, wenn eine Metrik den Schwellenwert für eine bestimmte Anzahl von Bewertungszeiträumen überschreitet. Der Alarm führt eine oder mehrere Aktionen durch, die vom Wert der Metrik oder des Ausdrucks im Vergleich zu einem Schwellenwert in einer Reihe von Zeiträumen abhängt. Diese Regel erfordert einen Wert für alarmActionRequired (Config Default: True), insufficientDataAction Required (Config Default: True), okActionRequired (Config Default: False). Der tatsächliche Wert muss die Alarmaktionen für Ihre Umgebung widerspiegeln.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
AU-6(1)(3)	(1) Die Organisation setzt automatisierte Mechanismen zur Integration von Prüfungs-, Analyse- und Berichtsprozessen ein, um die Prozesse der Organisation zur Untersuchung und Reaktion auf verdächtige Aktivitäten zu unterstützen. (3) Die Organisation analysiert und korreliert Prüfungsunterlagen aus verschiedenen Repositorys, um sich ein Bild über die Situation in der gesamten Organisation zu verschaffen.	elb-logging-enabled	Die Elastic-Load-Balancing-Aktivität ist ein zentraler Kommunikationspunkt innerhalb einer Umgebung. Stellen Sie sicher, dass die ELB-Protokollierung aktiviert ist. Die gesammelten Daten enthalten detaillierte Informationen zu Anfragen, die an den ELB gesendet wurden. Jedes Protokoll enthält Informationen wie die Zeit, zu der die Anforderung einging, die Client-IP-Adresse, Latenzen, Anforderungspfade und Serverantworten.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
AU-6(1)(3)	(1) Die Organisation setzt automatisierte Mechanismen zur Integration von Prüfungs-, Analyse- und Berichtsprozessen ein, um die Prozesse der Organisation zur Untersuchung und Reaktion auf verdächtige Aktivitäten zu unterstützen. (3) Die Organisation analysiert und korreliert Prüfungsunterlagen aus verschiedenen Repositorys, um sich ein Bild über die Situation in der gesamten Organisation zu verschaffen.	guardduty-enabled-centralized	Amazon GuardDuty kann mithilfe von Threat Intelligence Feeds helfen, potenzielle Cybersicherheitsereignisse zu überwachen und zu erkennen. Dazu gehören Listen mit bösartigen IPs und maschinellen Lernmethoden, um unerwartete, unbefugte und bösartige Aktivitäten in Ihrer AWS Cloud-Umgebung zu identifizieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
AU-6(1)(3)	(1) Die Organisation setzt automatisierte Mechanismen zur Integration von Prüfungs-, Analyse- und Berichtsprozessen ein, um die Prozesse der Organisation zur Untersuchung und Reaktion auf verdächtige Aktivitäten zu unterstützen. (3) Die Organisation analysiert und korreliert Prüfungsunterlagen aus verschiedenen Repositorys, um sich ein Bild über die Situation in der gesamten Organisation zu verschaffen.	rds-logging-enabled	Um die Protokollierung und Überwachung in Ihrer Umgebung zu erleichtern, stellen Sie sicher, dass die Amazon Relational Database Service (Amazon RDS)-Protokollierung aktiviert ist. Mit der Amazon-RDS-Protokollierung können Sie Ereignisse wie Verbindungen, Verbindungsabbrüche, Abfragen oder abgefragte Tabellen erfassen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
AU-6(1)(3)	(1) Die Organisation setzt automatisierte Mechanismen zur Integration von Prüfungs-, Analyse- und Berichtsprozessen ein, um die Prozesse der Organisation zur Untersuchung und Reaktion auf verdächtige Aktivitäten zu unterstützen. (3) Die Organisation analysiert und korreliert Prüfungsunterlagen aus verschiedenen Repositorys, um sich ein Bild über die Situation in der gesamten Organisation zu verschaffen.	redshift-cluster-configuration-check	Um Daten im Ruhezustand zu schützen, muss die Verschlüsselung für Ihre Amazon-Redshift-Cluster aktiviert sein. Sie müssen auch sicherstellen, dass die erforderlichen Konfigurationen auf Amazon-Redshift-Clustern bereitgestellt werden. Die Prüfungsprotokollierung muss aktiviert sein, um Informationen zu Verbindungen und Benutzeraktivitäten in der Datenbank bereitzustellen. Diese Regel erfordert, dass ein Wert für clusterDbEncrypted (Config Default: TRUE) und LoggingEnabled (Config Default: TRUE) gesetzt ist. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
AU-6(1)(3)	(1) Die Organisation setzt automatisierte Mechanismen zur Integration von Prüfungs-, Analyse- und Berichtsprozessen ein, um die Prozesse der Organisation zur Untersuchung und Reaktion auf verdächtige Aktivitäten zu unterstützen. (3) Die Organisation analysiert und korreliert Prüfungsunterlagen aus verschiedenen Repositorys, um sich ein Bild über die Situation in der gesamten Organisation zu verschaffen.	s3- bucket-logging-enabled	Die Amazon Simple Storage Service (Amazon S3)-Serverzugriffsprotokollierung bietet eine Methode zur Überwachung des Netzwerks im Hinblick auf potenzielle Cybersicherheitsereignisse. Die Ereignisse werden überwacht, indem detaillierte Aufzeichnungen über die Anfragen erfasst werden, die an einen Amazon-S3-Bucket gestellt wurden. Jeder Zugriffsprotokolleintrag enthält Details zu einer einzelnen Zugriffsanfrage. Zu den Details gehören Anforderer, Bucket-Name, Anforderungszeit, Anforderungsaktion, Antwortstatus und Fehlercode, falls relevant.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
AU-6(1)(3)	(1) Die Organisation setzt automatisierte Mechanismen zur Integration von Prüfungs-, Analyse- und Berichtsprozessen ein, um die Prozesse der Organisation zur Untersuchung und Reaktion auf verdächtige Aktivitäten zu unterstützen. (3) Die Organisation analysiert und korreliert Prüfungsunterlagen aus verschiedenen Repositorys, um sich ein Bild über die Situation in der gesamten Organisation zu verschaffen.	vpc-flow-logs-enabled	VPC-Flow-Protokolle erfassen detaillierte Informationsdatensätze über den IP-Datenverkehr, der zu und von Netzwerkschnittstellen in Ihrer Amazon Virtual Private Cloud (Amazon VPC) fließt. Standardmäßig enthalten Flow-Protokolldatensätze Werte für die verschiedenen Komponenten des IP-Flows, einschließlich Quelle, Ziel und Protokoll.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
AU-7(1)	Das Informationssystem bietet die Möglichkeit, Prüfungsunterlagen für Ereignisse von Interesse auf der Grundlage von [Zuweisung: von der Organisation definierte Prüfungsfelder in den Prüfungsunterlagen] zu verarbeiten.	cloud-trail-cloud-watch-logs-aktiviert	Verwenden Sie Amazon CloudWatch , um Protokollereignisaktivitäten zentral zu sammeln und zu verwalten. Die Aufnahme von AWS CloudTrail Daten liefert Einzelheiten zu den API-Aufrufaktivitäten in Ihrem AWS-Konto.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
AU-7(1)	Das Informationssystem bietet die Möglichkeit, Prüfungsunterlagen für Ereignisse von Interesse auf der Grundlage von [Zuweisung: von der Organisation definierte Prüfungsfelder in den Prüfungsunterlagen] zu verarbeiten.	cloudwatch-alarm-action-check	Amazon CloudWatch alarmiert, wenn eine Metrik den Schwellenwert für eine bestimmte Anzahl von Bewertungszeiträumen überschreitet. Der Alarm führt eine oder mehrere Aktionen durch, die vom Wert der Metrik oder des Ausdrucks im Vergleich zu einem Schwellenwert in einer Reihe von Zeiträumen abhängt. Diese Regel erfordert einen Wert für alarmActionRequired (Config Default: True), insufficientDataAction Required (Config Default: True), okActionRequired (Config Default: False). Der tatsächliche Wert muss die Alarmaktionen für Ihre Umgebung widerspiegeln.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
AU-9(2)	Das Informati onssystem sichert die Prüfungsu nterlagen mindestens wöchentlich auf einem anderen System bzw. einer anderen Systemkomponente als dem System/de r Komponente, das/ die Gegenstand der Prüfung ist.	s3- bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) unterstützt die Aufrechterhaltung einer angemesse nen Kapazität und Verfügbarkeit. CRR ermöglicht das automatische, asynchrone Kopieren von Objekten in Amazon-S3-Buckets, um die Datenverf ügbarkeit sicherzus tellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
AU-9(2)	Das Informationssystem sichert die Prüfungsunterlagen mindestens wöchentlich auf einem anderen System bzw. einer anderen Systemkomponente als dem System/der Komponente, das/die Gegenstand der Prüfung ist.	s-3 bucket-versioning-enabled	Die Versionsverwaltung von Amazon Simple Storage Service (Amazon S3)-Buckets hilft dabei, mehrere Varianten eines Objekts im selben Amazon-S3-Bucket zu speichern. Verwenden Sie die Versionsverwaltung, um sämtliche Versionen aller Objekte in Ihrem Amazon-S3-Bucket zu speichern, abzurufen oder wiederherzustellen. Mit der Versionsverwaltung können Sie Versionen sowohl nach unbeabsichtigten Benutzeraktionen als auch nach Anwendungsfehlern problemlos wiederherstellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
AU-9	Das Informati onssystem schützt Prüfungsinformatio nen und -tools vor unbefugtem Zugriff, Änderung und Löschung.	cloud-trail-encryption-enabled	Da sensible Daten vorhanden sein können und um Daten im Ruhezustand zu schützen, sollten Sie sicherstellen, dass die Verschlüsselung für Ihre AWS CloudTrail Trails aktiviert ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
AU-9	Das Informationssystem schützt Prüfungsinformationen und -tools vor unbefugtem Zugriff, Änderung und Löschung.	cloud-trail-log-file-Validierung aktiviert	Verwenden Sie die AWS CloudTrail Protokolldateivalidierung, um die Integrität von Protokollen zu überprüfen. CloudTrail Mithilfe der Protokolldateivalidierung kann festgestellt werden, ob eine Protokolldatei geändert oder gelöscht wurde oder ob sie nach der Übermittlung CloudTrail unverändert geblieben ist. Dieses Feature wurde mit dem Branchenstandard entsprechenden Algorithmen entwickelt: SHA-256 für die Hashfunktion und SHA-256 mit RSA für digitale Signaturen. Aus diesem Grund ist es rechnerisch unmöglich, CloudTrail Protokolldateien unbemerkt zu ändern, zu löschen oder zu fälschen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
AU-9	Das Informationssystem schützt Prüfungsinformationen und -tools vor unbefugtem Zugriff, Änderung und Löschung.	cloudwatch-log-group-encrypted	Um sensible Daten im Speicher zu schützen, stellen Sie sicher, dass die Verschlüsselung für Ihre Amazon CloudWatch Log Groups aktiviert ist.
AU-11	Die Organisation bewahrt die Prüfunterlagen mindestens 90 Tage lang auf, um die after-the-fact Untersuchung von Sicherheitsvorfällen zu unterstützen und die gesetzlichen und organisatorischen Anforderungen zur Aufbewahrung von Informationen zu erfüllen.	cw-loggroup-retention-period-überprüfen	Stellen Sie sicher, dass die Ereignisprotokolldaten für Ihre Protokollgruppen über eine Mindestdauer aufbewahrt werden, um die Fehlerbehebung und forensische Untersuchungen zu unterstützen. Fehlende frühere Ereignisprotokolldaten erschweren die Rekonstruierung und Identifizierung potenziell schädlicher Ereignisse.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
AU-12(a)(c)	Das Informati onssystem: a. Ermöglicht die Generierung von Prüfungsunterlagen für die in AU-2 a. definierten prüffähig en Ereignisse für alle Informationssystem - und Netzwerkk omponenten, bei denen Prüfungsf unktionen bereitges tellt/verfügbar sind c. Generiert Prüfungsu nterlagen für die in AU-2 d. definierten Ereignisse mit dem in AU-3 definierten Inhalt.	codebuild-project-logging-enabled	Stellen Sie sicher, dass die AWS CodeBuild Projektpr otokollierung aktiviert ist, damit Ihre Build-Ausgabeproto kolle entweder an Amazon CloudWatc h oder Amazon Simple Storage Service (Amazon S3) gesendet werden. Build-Ausgabeproto kolle enthalten detaillierte Informati onen zu Ihrem Build-Projekt.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
AU-12(a)(c)	Das Informati onssystem: a. Ermöglicht die Generierung von Prüfungsunterlagen für die in AU-2 a. definierten prüffähig en Ereignisse für alle Informationssystem - und Netzwerkk omponenten, bei denen Prüfungsf unktionen bereitges tellt/verfügbar sind c. Generiert Prüfungsu nterlagen für die in AU-2 d. definierten Ereignisse mit dem in AU-3 definierten Inhalt.	multi-region-cloudtrail-enabled	AWS CloudTrail zeichnet Aktionen und API-Aufrufe der AWS Management Console auf. Sie können feststellen, welche Benutzer und Konten angerufen wurden AWS, von welcher Quell-IP-Adresse aus die Anrufe getätigt wurden und wann die Anrufe erfolgten. CloudTrail übermittelt Protokolldateien aus allen AWS Regionen an Ihren S3-Bucket , wenn MULTI_REG ION_CLOUD _TRAIL_ENABLED aktiviert ist. Außerdem wird beim AWS Start einer neuen Region derselbe Trail in der neuen Region erstellt. CloudTrail Dadurch erhalten Sie automatis ch Protokolldateien mit API-Aktivitäten für die neue Region.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
AU-12(a)(c)	Das Informati onssystem: a. Ermöglicht die Generierung von Prüfungsunterlagen für die in AU-2 a. definierten prüffähig en Ereignisse für alle Informationssystem - und Netzwerkk omponenten, bei denen Prüfungsf unktionen bereitges tellt/verfügbar sind c. Generiert Prüfungsu nterlagen für die in AU-2 d. definierten Ereignisse mit dem in AU-3 definierten Inhalt.	rds-logging-enabled	Um die Protokoll ierung und Überwachung in Ihrer Umgebung zu erleichtern, stellen Sie sicher, dass die Amazon Relationa l Database Service (Amazon RDS)-Prot okollierung aktiviert ist. Mit der Amazon-RDS-Protokollierung können Sie Ereigniss e wie Verbindungen, Verbindungsabbrüch e, Abfragen oder abgefragte Tabellen erfassen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
AU-12(a)(c)	Das Informationssystem: a. Ermöglicht die Generierung von Prüfungsunterlagen für die in AU-2 a. definierten prüffähigen Ereignisse für alle Informationssystem- und Netzwerkkomponenten, bei denen Prüfungsfunktionen bereitgestellt/verfügbar sind c. Generiert Prüfungsunterlagen für die in AU-2 d. definierten Ereignisse mit dem in AU-3 definierten Inhalt.	wafv2-logging-enabled	Um die Protokollierung und Überwachung in Ihrer Umgebung zu erleichtern, aktivieren Sie die AWS WAF (V2) -Protokollierung im regionalen und globalen Web ACLs. AWS Die WAF-Protokollierung bietet detaillierte Informationen über den Datenverkehr, der von Ihrer Web-ACL analysiert wird. In den Protokollen werden die Uhrzeit aufgezeichnet, zu der die AWS WAF die Anfrage von Ihrer AWS Ressource erhalten hat, Informationen zu der Anfrage und eine Aktion für die Regel, der jede Anfrage entsprach.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
AU-12(a)(c)	Das Informati onssystem: a. Ermöglicht die Generierung von Prüfungsunterlagen für die in AU-2 a. definierten prüffähig en Ereignisse für alle Informationssystem - und Netzwerkk omponenten, bei denen Prüfungsf unktionen bereitges tellt/verfügbar sind c. Generiert Prüfungsu nterlagen für die in AU-2 d. definierten Ereignisse mit dem in AU-3 definierten Inhalt.	api-gw-execution-l ogging-aktiviert	Die API-Gateway-Protokollierung zeigt detaillierte Ansichten der Benutzer, die auf die API zugegriff en haben, und wie diese Benutzer auf die API zugegriff en haben. Diese Einblicke ermöglichen die Transparenz von Benutzeraktivitäten.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
AU-12(a)(c)	Das Informati onssystem: a. Ermöglicht die Generierung von Prüfungsunterlagen für die in AU-2 a. definierten prüffähig en Ereignisse für alle Informationssystem - und Netzwerkk omponenten, bei denen Prüfungsf unktionen bereitges tellt/verfügbar sind c. Generiert Prüfungsu nterlagen für die in AU-2 d. definierten Ereignisse mit dem in AU-3 definierten Inhalt.	cloud-trail-cloud-watch-logs-aktiviert	Verwenden Sie Amazon CloudWatc h , um Protokoll ereignisaktivitäten zentral zu sammeln und zu verwalten. Die Aufnahme von AWS CloudTrail Daten liefert Einzelheiten zu den API-Aufrufaktivitä ten in Ihrem AWS-Konto.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
AU-12(a)(c)	Das Informati onssystem: a. Ermöglicht die Generierung von Prüfungsunterlagen für die in AU-2 a. definierten prüffähig en Ereignisse für alle Informationssystem - und Netzwerkk omponenten, bei denen Prüfungsf unktionen bereitges tellt/verfügbar sind c. Generiert Prüfungsu nterlagen für die in AU-2 d. definierten Ereignisse mit dem in AU-3 definierten Inhalt.	cloudtrail-enabled	AWS CloudTrail kann bei der Nichtabst reitbarkeit helfen, indem Aktionen und API-Aufrufe der AWS Management Console aufgezeic hnet werden. Sie können die Benutzer und die Benutzer AWS-Konten , die einen AWS Dienst aufgerufen haben, die Quell-IP-Adresse, über die die Aufrufe generiert wurden, und den Zeitpunkt der Anrufe identifiz ieren. Einzelheiten zu den erfassten Daten finden Sie in den AWS CloudTrail Datensatzinhalten.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
AU-12(a)(c)	Das Informati onssystem: a. Ermöglicht die Generierung von Prüfungsunterlagen für die in AU-2 a. definierten prüffähig en Ereignisse für alle Informationssystem - und Netzwerkk omponenten, bei denen Prüfungsf unktionen bereitges tellt/verfügbar sind c. Generiert Prüfungsu nterlagen für die in AU-2 d. definierten Ereignisse mit dem in AU-3 definierten Inhalt.	cloudtrail-s3-data events-enabled	Die Erfassung von Simple Storage Service (Amazon S3)-Datenereigniss en unterstützt die Erkennung von ungewöhnlichen Aktivitäten. Zu den Details gehören AWS-Konto Informationen über den Zugriff auf einen Amazon S3 S3-Bucket, die IP-Adress e und die Uhrzeit des Ereignisses.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
AU-12(a)(c)	Das Informati onssystem: a. Ermöglicht die Generierung von Prüfungsunterlagen für die in AU-2 a. definierten prüffähig en Ereignisse für alle Informationssystem - und Netzwerkk omponenten, bei denen Prüfungsf unktionen bereitges tellt/verfügbar sind c. Generiert Prüfungsu nterlagen für die in AU-2 d. definierten Ereignisse mit dem in AU-3 definierten Inhalt.	elb-logging-enabled	Die Elastic-Load-Balancing-Aktivität ist ein zentraler Kommunikationspunk t innerhalb einer Umgebung. Stellen Sie sicher, dass die ELB-Protokollierun g aktiviert ist. Die gesammelten Daten enthalten detaillie rte Informationen zu Anfragen, die an den ELB gesendet wurden. Jedes Protokoll enthält Informationen wie die Zeit, zu der die Anforderung einging, die Client-IP -Adresse, Latenzen, Anforderungspfade und Serverantworten.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
AU-12(a)(c)	Das Informationssystem: a. Ermöglicht die Generierung von Prüfungsunterlagen für die in AU-2 a. definierten prüffähigen Ereignisse für alle Informationssystem- und Netzwerkkomponenten, bei denen Prüfungsfunktionen bereitgestellt/verfügbar sind c. Generiert Prüfungsunterlagen für die in AU-2 d. definierten Ereignisse mit dem in AU-3 definierten Inhalt.	redshift-cluster-configuration-check	Um Daten im Ruhezustand zu schützen, muss die Verschlüsselung für Ihre Amazon-Redshift-Cluster aktiviert sein. Sie müssen auch sicherstellen, dass die erforderlichen Konfigurationen auf Amazon-Redshift-Clustern bereitgestellt werden. Die Prüfungsprotokollierung muss aktiviert sein, um Informationen zu Verbindungen und Benutzeraktivitäten in der Datenbank bereitzustellen. Diese Regel erfordert, dass ein Wert für clusterDbEncrypted (Config Default: TRUE) und LoggingEnabled (Config Default: TRUE) gesetzt ist. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
AU-12(a)(c)	Das Informati onssystem: a. Ermöglicht die Generierung von Prüfungsunterlagen für die in AU-2 a. definierten prüffähig en Ereignisse für alle Informationssystem - und Netzwerkk omponenten, bei denen Prüfungsf unktionen bereitges tellt/verfügbar sind c. Generiert Prüfungsu nterlagen für die in AU-2 d. definierten Ereignisse mit dem in AU-3 definierten Inhalt.	s3- bucket-logging-enabled	Die Amazon Simple Storage Service (Amazon S3)-Serverzugriffs protokollierung bietet eine Methode zur Überwachu ng des Netzwerks im Hinblick auf potenzielle Cybersich erheitsereignisse. Die Ereignisse werden überwacht, indem detaillierte Aufzeichn ungen über die Anfragen erfasst werden, die an einen Amazon-S3-Bucket gestellt wurden. Jeder Zugriffsprotokolle intrag enthält Details zu einer einzelnen Zugriffsanfrage. Zu den Details gehören Anforderer, Bucket-Name, Anforderu ngszeit, Anforderu ngsaktion, Antwortst atus und Fehlercode, falls relevant.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
AU-12(a)(c)	Das Informationssystem: a. Ermöglicht die Generierung von Prüfungsunterlagen für die in AU-2 a. definierten prüffähigen Ereignisse für alle Informationssystem- und Netzwerkkomponenten, bei denen Prüfungsfunktionen bereitgestellt/verfügbar sind c. Generiert Prüfungsunterlagen für die in AU-2 d. definierten Ereignisse mit dem in AU-3 definierten Inhalt.	vpc-flow-logs-enabled	VPC-Flow-Protokolle erfassen detaillierte Informationsdatensätze über den IP-Datenverkehr, der zu und von Netzwerkschnittstellen in Ihrer Amazon Virtual Private Cloud (Amazon VPC) fließt. Standardmäßig enthalten Flow-Protokolldatensätze Werte für die verschiedenen Komponenten des IP-Flows, einschließlich Quelle, Ziel und Protokoll.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
CA-7(a)(b)	Die Organisation entwickelt eine Strategie zur kontinuierlichen Überwachung und implementiert ein kontinuierliches Überwachungsprogramm, das Folgendes umfasst: a. Festlegung von [Zuweisung: von der Organisation definierte Kennzahlen], die überwacht werden sollen; b. Festlegung von [Zuweisung: von der Organisation festgelegte Häufigkeiten] für die Überwachung und [Zuweisung: von der Organisation festgelegte Häufigkeiten] für Bewertungen, die diese Überwachung unterstützen.	lambda-concurrency-check	Diese Regel stellt sicher, dass die Höchst- und Untergrenzen für die Gleichzeitigkeit einer Lambda-Funktion festgelegt werden. Dies kann Sie beim Baselining für die Anzahl der Anforderungen unterstützen, die Ihre Funktion zu einem bestimmten Zeitpunkt verarbeitet.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
CA-7(a)(b)	Die Organisation entwickelt eine Strategie zur kontinuierlichen Überwachung und implementiert ein kontinuierliches Überwachungsprogramm, das Folgendes umfasst: a. Festlegung von [Zuweisung: von der Organisation definierte Kennzahlen], die überwacht werden sollen; b. Festlegung von [Zuweisung: von der Organisation festgelegte Häufigkeiten] für die Überwachung und [Zuweisung: von der Organisation festgelegte Häufigkeiten] für Bewertungen, die diese Überwachung unterstützen.	lambda-dlq-check	Aktivieren Sie diese Regel, um das entsprechende Personal über Amazon Simple Queue Service (Amazon SQS) oder Amazon Simple Notification Service (Amazon SNS) zu benachrichtigen, wenn eine Funktion ausgefallen ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
CA-7(a)(b)	Die Organisation entwickelt eine Strategie zur kontinuierlichen Überwachung und implementiert ein kontinuierliches Überwachungsprogramm, das Folgendes umfasst: a. Festlegung von [Zuweisung: von der Organisation definierte Kennzahlen], die überwacht werden sollen; b. Festlegung von [Zuweisung: von der Organisation festgelegte Häufigkeiten] für die Überwachung und [Zuweisung: von der Organisation festgelegte Häufigkeiten] für Bewertungen, die diese Überwachung unterstützen.	multi-region-cloudtrail-enabled	AWS CloudTrail zeichnet Aktionen und API-Aufrufe der AWS Management Console auf. Sie können feststellen, welche Benutzer und Konten angerufen wurden AWS, von welcher Quell-IP-Adresse aus die Anrufe getätigt wurden und wann die Anrufe erfolgten. CloudTrail übermittelt Protokolldateien aus allen AWS Regionen an Ihren S3-Bucket, wenn MULTI_REGION_CLOUD_TRAIL_ENABLED aktiviert ist. Außerdem wird beim AWS Start einer neuen Region derselbe Trail in der neuen Region erstellt. CloudTrail Dadurch erhalten Sie automatisch Protokolldateien mit API-Aktivitäten für die neue Region.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
CA-7(a)(b)	Die Organisation entwickelt eine Strategie zur kontinuierlichen Überwachung und implementiert ein kontinuierliches Überwachungsprogramm, das Folgendes umfasst: a. Festlegung von [Zuweisung: von der Organisation definierte Kennzahlen], die überwacht werden sollen; b. Festlegung von [Zuweisung: von der Organisation festgelegte Häufigkeiten] für die Überwachung und [Zuweisung: von der Organisation festgelegte Häufigkeiten] für Bewertungen, die diese Überwachung unterstützen.	rds-enhanced-monitoring-enabled	Aktivieren Sie Amazon Relational Database Service (Amazon RDS), um die Verfügbarkeit von Amazon RDS zu überwachen. Dies bietet einen detaillierten Einblick in den Zustand Ihrer Amazon-RDS-Datenbank-Instances. Wenn der Amazon-RDS-Speicher mehr als ein zugrunde liegendes physisches Gerät verwendet, erfasst Enhanced Monitoring die Daten für jedes Gerät. Wenn die Amazon-RDS-Datenbank-Instance in einer Multi-AZ-Bereitstellung ausgeführt wird, werden außerdem die Daten für jedes Gerät auf dem sekundären Host sowie die Metriken des sekundären Hosts erfasst.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
CA-7(a)(b)	Die Organisation entwickelt eine Strategie zur kontinuierlichen Überwachung und implementiert ein kontinuierliches Überwachungsprogramm, das Folgendes umfasst: a. Festlegung von [Zuweisung: von der Organisation definierte Kennzahlen], die überwacht werden sollen; b. Festlegung von [Zuweisung: von der Organisation festgelegte Häufigkeiten] für die Überwachung und [Zuweisung: von der Organisation festgelegte Häufigkeiten] für Bewertungen, die diese Überwachung unterstützen.	securityhub-enabled	AWS Security Hub hilft bei der Überwachung von unbefugtem Personal, Verbindungen, Geräten und Software. AWS Security Hub aggregiert, organisiert und priorisiert die Sicherheitswarnungen oder Ergebnisse mehrerer Dienste. AWS Einige dieser Dienste sind Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer und AWS Firewall Manager sowie AWS Partnerlösungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
CA-7(a)(b)	Die Organisation entwickelt eine Strategie zur kontinuierlichen Überwachung und implementiert ein kontinuierliches Überwachungsprogramm, das Folgendes umfasst: a. Festlegung von [Zuweisung: von der Organisation definierte Kennzahlen], die überwacht werden sollen; b. Festlegung von [Zuweisung: von der Organisation festgelegte Häufigkeiten] für die Überwachung und [Zuweisung: von der Organisation festgelegte Häufigkeiten] für Bewertungen, die diese Überwachung unterstützen.	autoscaling-group-elb-healthcheck-erforderlich	Die Elastic Load Balancer (ELB) - Zustandsprüfungen für Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling Scaling-Gruppen unterstützen die Aufrechterhaltung einer angemessenen Kapazität und Verfügbarkeit. Der Load Balancer sendet regelmäßig Pings, versucht Verbindungen herzustellen oder sendet Anfragen, um den Zustand der EC2 Amazon-Instances in einer Gruppe mit auto-scaling zu testen. Wenn eine Instance nicht zurückmeldet, wird der Traffic an eine neue EC2 Amazon-Instance gesendet.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
CA-7(a)(b)	Die Organisation entwickelt eine Strategie zur kontinuierlichen Überwachung und implementiert ein kontinuierliches Überwachungsprogramm, das Folgendes umfasst: a. Festlegung von [Zuweisung: von der Organisation definierte Kennzahlen], die überwacht werden sollen; b. Festlegung von [Zuweisung: von der Organisation festgelegte Häufigkeiten] für die Überwachung und [Zuweisung: von der Organisation festgelegte Häufigkeiten] für Bewertungen, die diese Überwachung unterstützen.	beanstalk-enhanced-health-reporting-aktiviert	AWS Die verbesserte Zustandsberichterstattung von Elastic Beanstalk ermöglicht eine schnellere Reaktion auf Veränderungen im Zustand der zugrunde liegenden Infrastruktur. Diese Änderungen könnten zu einer mangelnden Verfügbarkeit der Anwendung führen. Die erweiterten Zustandsberichte von Elastic Beanstalk bieten eine Statusbeschreibung, um den Schweregrad der identifizierten Probleme einzuschätzen und mögliche Ursachen zu identifizieren, die untersucht werden müssen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
CA-7(a)(b)	Die Organisation entwickelt eine Strategie zur kontinuierlichen Überwachung und implementiert ein kontinuierliches Überwachungsprogramm, das Folgendes umfasst: a. Festlegung von [Zuweisung: von der Organisation definierte Kennzahlen], die überwacht werden sollen; b. Festlegung von [Zuweisung: von der Organisation festgelegte Häufigkeiten] für die Überwachung und [Zuweisung: von der Organisation festgelegte Häufigkeiten] für Bewertungen, die diese Überwachung unterstützen.	cloudtrail-enabled	AWS CloudTrail kann durch die Aufzeichnung von Aktionen und API-Aufrufen in der AWS Management Console bei der Nichtabstreitbarkeit helfen. Sie können die Benutzer und die Benutzer AWS-Konten , die einen AWS Dienst aufgerufen haben, die Quell-IP-Adresse, über die die Aufrufe generiert wurden, und den Zeitpunkt der Anrufe identifizieren. Einzelheiten zu den erfassten Daten finden Sie in den AWS CloudTrail Datensatzinhalten.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
CA-7(a)(b)	Die Organisation entwickelt eine Strategie zur kontinuierlichen Überwachung und implementiert ein kontinuierliches Überwachungsprogramm, das Folgendes umfasst: a. Festlegung von [Zuweisung: von der Organisation definierte Kennzahlen], die überwacht werden sollen; b. Festlegung von [Zuweisung: von der Organisation festgelegte Häufigkeiten] für die Überwachung und [Zuweisung: von der Organisation festgelegte Häufigkeiten] für Bewertungen, die diese Überwachung unterstützen.	cloudtrail-s3-dataevents-enabled	Die Erfassung von Simple Storage Service (Amazon S3)-Datenereignissen unterstützt die Erkennung von ungewöhnlichen Aktivitäten. Zu den Details gehören AWS-Konto Informationen über den Zugriff auf einen Amazon S3 S3-Bucket, die IP-Adresse und die Uhrzeit des Ereignisses.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
CA-7(a)(b)	Die Organisation entwickelt eine Strategie zur kontinuierlichen Überwachung und implementiert ein kontinuierliches Überwachungsprogramm, das Folgendes umfasst: a. Festlegung von [Zuweisung: von der Organisation definierte Kennzahlen], die überwacht werden sollen; b. Festlegung von [Zuweisung: von der Organisation festgelegte Häufigkeiten] für die Überwachung und [Zuweisung: von der Organisation festgelegte Häufigkeiten] für Bewertungen, die diese Überwachung unterstützen.	cloudwatch-alarm-action-check	Amazon CloudWatch alarmiert, wenn eine Metrik den Schwellenwert für eine bestimmte Anzahl von Bewertungszeiträumen überschreitet. Der Alarm führt eine oder mehrere Aktionen durch, die vom Wert der Metrik oder des Ausdrucks im Vergleich zu einem Schwellenwert in einer Reihe von Zeiträumen abhängt. Diese Regel erfordert einen Wert für alarmActionRequired (Config Default: True), insufficientDataAction Required (Config Default: True), okActionRequired (Config Default: False). Der tatsächliche Wert muss die Alarmaktionen für Ihre Umgebung widerspiegeln.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
CA-7(a)(b)	Die Organisation entwickelt eine Strategie zur kontinuierlichen Überwachung und implementiert ein kontinuierliches Überwachungsprogramm, das Folgendes umfasst: a. Festlegung von [Zuweisung: von der Organisation definierte Kennzahlen], die überwacht werden sollen; b. Festlegung von [Zuweisung: von der Organisation festgelegte Häufigkeiten] für die Überwachung und [Zuweisung: von der Organisation festgelegte Häufigkeiten] für Bewertungen, die diese Überwachung unterstützen.	dynamodb-throughput-limit-check	Aktivieren Sie diese Regel, um sicherzustellen, dass die bereitgestellte Durchsatzkapazität in Ihren Amazon-DynamoDB-Tabellen überprüft wird. Dies ist der Umfang der Lese- und Schreibaktivitäten, der von den jeweiligen Tabellen unterstützt werden kann. DynamoDB verwendet diese Informationen für das Reservieren ausreichender Systemressourcen, um Ihren Durchsatzanforderungen gerecht zu werden. Diese Regel generiert eine Warnung, wenn sich der Durchsatz dem Höchstlimit für ein Kundenkonto nähert. Mit dieser Regel können Sie optional die Parameter RCUThreshold Kontoprozentsatz

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
			(Konfigurationsstandard: 80) und WCUThreshold Kontoprozentsatz (Konfigurationsstandard: 80) festlegen. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
CA-7(a)(b)	Die Organisation entwickelt eine Strategie zur kontinuierlichen Überwachung und implementiert ein kontinuierliches Überwachungsprogramm, das Folgendes umfasst: a. Festlegung von [Zuweisung: von der Organisation definierte Kennzahlen], die überwacht werden sollen; b. Festlegung von [Zuweisung: von der Organisation festgelegte Häufigkeiten] für die Überwachung und [Zuweisung: von der Organisation festgelegte Häufigkeiten] für Bewertungen, die diese Überwachung unterstützen.	ec2- instance-detailed-monitoring-enabled	Aktivieren Sie diese Regel, um die Amazon Elastic Compute Cloud (Amazon EC2) - Instance-Überwachung auf der EC2 Amazon-Konsole zu verbessern, in der Monitoring-Diagramme mit einem Zeitraum von 1 Minute für die Instance angezeigt werden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
CA-7(a)(b)	Die Organisation entwickelt eine Strategie zur kontinuierlichen Überwachung und implementiert ein kontinuierliches Überwachungsprogramm, das Folgendes umfasst: a. Festlegung von [Zuweisung: von der Organisation definierte Kennzahlen], die überwacht werden sollen; b. Festlegung von [Zuweisung: von der Organisation festgelegte Häufigkeiten] für die Überwachung und [Zuweisung: von der Organisation festgelegte Häufigkeiten] für Bewertungen, die diese Überwachung unterstützen.	guardduty-enabled-centralized	Amazon GuardDuty kann mithilfe von Threat Intelligence Feeds helfen, potenzielle Cybersicherheitsereignisse zu überwachen und zu erkennen. Dazu gehören Listen mit bösartigen IPs und maschinellen Lernmethoden, um unerwartete, unbefugte und bösartige Aktivitäten in Ihrer AWS Cloud-Umgebung zu identifizieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
CA-7(a)(b)	Die Organisation entwickelt eine Strategie zur kontinuierlichen Überwachung und implementiert ein kontinuierliches Überwachungsprogramm, das Folgendes umfasst: a. Festlegung von [Zuweisung: von der Organisation definierte Kennzahlen], die überwacht werden sollen; b. Festlegung von [Zuweisung: von der Organisation festgelegte Häufigkeiten] für die Überwachung und [Zuweisung: von der Organisation festgelegte Häufigkeiten] für Bewertungen, die diese Überwachung unterstützen.	redshift-cluster-configuration-check	Um Daten im Ruhezustand zu schützen, muss die Verschlüsselung für Ihre Amazon-Redshift-Cluster aktiviert sein. Sie müssen auch sicherstellen, dass die erforderlichen Konfigurationen auf Amazon-Redshift-Clustern bereitgestellt werden. Die Prüfungsprotokollierung muss aktiviert sein, um Informationen zu Verbindungen und Benutzeraktivitäten in der Datenbank bereitzustellen. Diese Regel erfordert, dass ein Wert für clusterDbEncrypted (Config Default: TRUE) und LoggingEnabled (Config Default: TRUE) gesetzt ist. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
CM-2	Die Organisation entwickelt, dokumentiert und verwaltet unter Konfigurationskontrolle eine aktuelle Basiskonfiguration des Informationssystems.	alb-waf-enabled	Stellen Sie sicher, dass AWS WAF auf Elastic Load Balancers (ELB) aktiviert ist, um Webanwendungen zu schützen. Eine WAF trägt zum Schutz Ihrer Webanwendungen oder APIs vor gängigen Web-Exploits bei. Diese Web-Exploits können sich auf die Verfügbarkeit auswirken, die Sicherheit gefährden oder übermäßige Ressourcen in Ihrer Umgebung verbrauchen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
CM-2	Die Organisation entwickelt, dokumentiert und verwaltet unter Konfigurationskontrolle eine aktuelle Basiskonfiguration des Informationssystems.	api-gw-associated-with-WAF	AWS Mit WAF können Sie eine Reihe von Regeln (als Web Access Control List (Web ACL) bezeichnet) konfigurieren, die Webanfragen auf der Grundlage von anpassbaren Websicherheitsregeln und -bedingungen, die Sie definieren, zulassen, blockieren oder zählen. Stellen Sie sicher, dass Ihre Amazon-API-Gateway-Stufe mit einer WAF-Web-ACL verknüpft ist, um sie vor böswilligen Angriffen zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
CM-2	Die Organisation entwickelt, dokumentiert und verwaltet unter Konfigurationskontrolle eine aktuelle Basiskonfiguration des Informationssystems.	autoscaling-launch-config-public-ip-deaktiviert	Wenn Sie Ihre Netzwerkschnittstellen mit einer öffentlichen IP-Adresse konfigurieren, sind die diesen Netzwerkschnittstellen zugehörigen Ressourcen über das Internet erreichbar. EC2 Ressourcen sollten nicht öffentlich zugänglich sein, da dies einen unbeabsichtigten Zugriff auf Ihre Anwendungen oder Server ermöglichen kann.
CM-2	Die Organisation entwickelt, dokumentiert und verwaltet unter Konfigurationskontrolle eine aktuelle Basiskonfiguration des Informationssystems.	dms-replication-not-public	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass auf DMS-Replikationsinstanzen nicht öffentlich zugegriffen werden kann. DMS-Replikations-Instances können vertrauliche Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
CM-2	Die Organisation entwickelt, dokumentiert und verwaltet unter Konfigurationskontrolle eine aktuelle Basiskonfiguration des Informationssystems.	ebs-snapshot-public-restorable-überprüfen	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass EBS-Snapshots nicht öffentlich wiederherstellbar sind. EBS-Volume-Snapshots können vertrauliche Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.
CM-2	Die Organisation entwickelt, dokumentiert und verwaltet unter Konfigurationskontrolle eine aktuelle Basiskonfiguration des Informationssystems.	ec-2 instance-no-public-ip	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon Elastic Compute Cloud (Amazon EC2) - Instances nicht öffentlich zugänglich sind. EC2 Amazon-Instances können vertrauliche Informationen enthalten, und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
CM-2	Die Organisation entwickelt, dokumentiert und verwaltet unter Konfigurationskontrolle eine aktuelle Basiskonfiguration des Informationssystems.	elasticsearch-in-vpc-only	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass sich Amazon OpenSearch OpenSearch Service (Service) - Domains innerhalb einer Amazon Virtual Private Cloud (Amazon VPC) befinden. Eine OpenSearch Service-Domain innerhalb einer Amazon VPC ermöglicht die sichere Kommunikation zwischen OpenSearch Service und anderen Services innerhalb der Amazon VPC, ohne dass ein Internet-Gateway, ein NAT-Gerät oder eine VPN-Verbindung erforderlich ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
CM-2	Die Organisation entwickelt, dokumentiert und verwaltet unter Konfigurationskontrolle eine aktuelle Basiskonfiguration des Informationssystems.	emr-master-no-public-ip	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon EMR-Cluster-Masterknoten nicht öffentlich zugänglich sind. Amazon-EMR-Cluster-Hauptknoten können vertrauliche Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
CM-2	Die Organisation entwickelt, dokumentiert und verwaltet unter Konfigurationskontrolle eine aktuelle Basiskonfiguration des Informationssystems.	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) Security Groups können bei der Verwaltung des Netzwerkzugriffs helfen, indem sie eine statusbehaftete Filterung von eingehendem und ausgehendem Netzwerkverkehr zu Ressourcen bereitstellen. AWS Wenn Sie eingehenden (oder entfernten) Datenverkehr von 0.0.0.0/0 bis Port 22 auf Ihren Ressourcen nicht zulassen, können Sie den Remote-Zugriff einschränken.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
CM-2	Die Organisation entwickelt, dokumentiert und verwaltet unter Konfigurationskontrolle eine aktuelle Basiskonfiguration des Informationssystems.	ec-2 instances-in-vpc	Stellen Sie Amazon Elastic Compute Cloud (Amazon EC2) -Instances innerhalb einer Amazon Virtual Private Cloud (Amazon VPC) bereit, um eine sichere Kommunikation zwischen einer Instance und anderen Services innerhalb der Amazon VPC zu ermöglichen, ohne dass ein Internet-Gateway, ein NAT-Gerät oder eine VPN-Verbindung erforderlich ist. Der gesamte Datenverkehr bleibt sicher in der AWS Cloud. Domains, die sich innerhalb einer VPC befinden, verfügen aufgrund ihrer logischen Isolierung im Vergleich zu Domains mit öffentlichen Endpunkten über eine zusätzliche Sicherheitsebene. Weisen Sie EC2

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
			Amazon-Instances einer Amazon-VPC zu, um den Zugriff ordnungsgemäß zu verwalten.
CM-2	Die Organisation entwickelt, dokumentiert und verwaltet unter Konfigurationskontrolle eine aktuelle Basiskonfiguration des Informationssystems.	lambda-function-public-access-verboten	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass AWS Lambda-Funktionen nicht öffentlich zugänglich sind. Der öffentliche Zugriff kann möglicherweise die Verfügbarkeit von Ressourcen beeinträchtigen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
CM-2	Die Organisation entwickelt, dokumentiert und verwaltet unter Konfigurationskontrolle eine aktuelle Basiskonfiguration des Informationssystems.	lambda-inside-vpc	Stellen Sie AWS Lambda-Funktionen in einer Amazon Virtual Private Cloud (Amazon VPC) bereit, um eine sichere Kommunikation zwischen einer Funktion und anderen Diensten innerhalb der Amazon VPC zu gewährleisten. Bei dieser Konfiguration sind kein Internet-Gateway, kein NAT-Gerät und keine VPN-Verbindung erforderlich. Der gesamte Datenverkehr bleibt sicher in der Cloud. AWS Domains, die sich innerhalb einer VPC befinden, verfügen aufgrund ihrer logischen Isolierung im Vergleich zu Domains mit öffentlichen Endpunkten über eine zusätzliche Sicherheitsebene. Um den Zugriff ordnungsgemäß zu verwalten,

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
			sollten AWS Lambda-Funktionen einer VPC zugewiesen werden.
CM-2	Die Organisation entwickelt, dokumentiert und verwaltet unter Konfigurationskontrolle eine aktuelle Basiskonfiguration des Informationssystems.	no-unrestricted-route-to-igw	Stellen Sie sicher, dass EC2 Amazon-Routentabellen keine uneingeschränkten Routen zu einem Internet-Gateway enthalten. Durch das Entfernen oder Beschränken des Internetzugangs für Workloads innerhalb von Amazon VPCs können unbeabsichtigte Zugriffe in Ihrer Umgebung reduziert werden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
CM-2	Die Organisation entwickelt, dokumentiert und verwaltet unter Konfigurationskontrolle eine aktuelle Basiskonfiguration des Informationssystems.	rds-instance-public-access-überprüfen	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Relational Database Service (Amazon RDS) -Instances nicht öffentlich sind. Amazon-RDS-Datenbank-Instances können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
CM-2	Die Organisation entwickelt, dokumentiert und verwaltet unter Konfigurationskontrolle eine aktuelle Basiskonfiguration des Informationssystems.	rds-snapshots-public-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Relational Database Service (Amazon RDS) -Instances nicht öffentlich sind. Amazon-RDS-Datenbank-Instances können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
CM-2	Die Organisation entwickelt, dokumentiert und verwaltet unter Konfigurationskontrolle eine aktuelle Basiskonfiguration des Informationssystems.	redshift-cluster-public-access-überprüfen	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Redshift Redshift-Cluster nicht öffentlich sind. Amazon-Redshift-Cluster können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
CM-2	Die Organisation entwickelt, dokumentiert und verwaltet unter Konfigurationskontrolle eine aktuelle Basiskonfiguration des Informationssystems.	s3- -Block-periodisch account-level-public-access	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Simple Storage Service (Amazon S3) -Buckets nicht öffentlich zugänglich sind. Diese Regel trägt dazu bei, sensible Daten vor unbefugten Remote-Benutzern zu schützen, indem sie den öffentlichen Zugriff verhindert. Mit dieser Regel können Sie optional die Parameter ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) und restrictPublicBuckets Parameter (Config Default: True) festlegen. Die tatsächlichen Werte müssen den Richtlini

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
			en Ihrer Organisation entsprechen.
CM-2	Die Organisation entwickelt, dokumentiert und verwaltet unter Konfigurationskontrolle eine aktuelle Basiskonfiguration des Informationssystems.	s3- bucket-public-read-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie nur autorisierten Benutzern, Prozessen und Geräten Zugriff auf Amazon Simple Storage Service (Amazon S3) - Buckets gewähren. Die Verwaltung des Zugriffs sollte mit der Klassifizierung der Daten übereinstimmen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
CM-2	Die Organisation entwickelt, dokumentiert und verwaltet unter Konfigurationskontrolle eine aktuelle Basiskonfiguration des Informationssystems.	s3- bucket-public-write-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie nur autorisierten Benutzern, Prozessen und Geräten Zugriff auf Amazon Simple Storage Service (Amazon S3) - Buckets gewähren. Die Verwaltung des Zugriffs sollte mit der Klassifizierung der Daten übereinstimmen.
CM-2	Die Organisation entwickelt, dokumentiert und verwaltet unter Konfigurationskontrolle eine aktuelle Basiskonfiguration des Informationssystems.	sagemaker-notebook-no-direct-Internetzugang	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass SageMaker Amazon-Notebooks keinen direkten Internetzugang zulassen. Indem Sie direkten Internetzugang blockieren, vermeiden Sie, dass unbefugte Benutzer auf sensible Daten zugreifen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
CM-2	Die Organisation entwickelt, dokumentiert und verwaltet unter Konfigurationskontrolle eine aktuelle Basiskonfiguration des Informationssystems.	vpc-default-security-group-geschlossen	Sicherheitsgruppen von Amazon Elastic Compute Cloud (Amazon EC2) können bei der Verwaltung des Netzwerkzugriffs helfen, indem sie eine statusbehaftete Filterung des ein- und ausgehenden Netzwerkverkehrs zu Ressourcen bereitstellen. AWS Die Beschränkung des gesamten Datenverkehrs auf die Standardsicherheitsgruppe hilft dabei, den Fernzugriff auf Ihre Ressourcen einzuschränken. AWS

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
CM-2	Die Organisation entwickelt, dokumentiert und verwaltet unter Konfigurationskontrolle eine aktuelle Basiskonfiguration des Informationssystems.	vpc-sg-open-only-to-authorized-ports	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass gemeinsame Ports für Amazon Elastic Compute Cloud (Amazon EC2) -Sicherheitsgruppen eingeschränkt sind. Wenn der Zugriff auf Ports nicht auf vertrauenswürdige Quellen beschränkt wird, kann dies zu Angriffen auf die Verfügbarkeit, Integrität und Vertraulichkeit von Systemen führen. Durch die Beschränkung des Zugriffs auf Ressourcen innerhalb einer Sicherheitsgruppe aus dem Internet (0.0.0.0/0) kann der Remote-Zugriff auf interne Systeme gesteuert werden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
CM-2	Die Organisation entwickelt, dokumentiert und verwaltet unter Konfigurationskontrolle eine aktuelle Basiskonfiguration des Informationssystems.	ec2-managed-instance-managed-by-systems	Eine Bestandsaufnahme der Softwareplattformen und Anwendungen innerhalb des Unternehmens ist möglich, indem Amazon Elastic Compute Cloud (Amazon EC2) - Instances mit AWS Systems Manager verwaltet werden. Verwenden Sie AWS Systems Manager, um detaillierte Systemkonfigurationen, Betriebssystem-Patch-Levels, Namen und Typ der Dienste, Softwareinstallationen, Anwendungsname, Herausgeber und Version sowie andere Details zu Ihrer Umgebung bereitzustellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
CM-2	Die Organisation entwickelt, dokumentiert und verwaltet unter Konfigurationskontrolle eine aktuelle Basiskonfiguration des Informationssystems.	ec2-check managedinstance-association-compliance-status	Verwenden Sie AWS Systems Manager Associations, um bei der Inventarisierung von Softwareplattformen und Anwendungen innerhalb eines Unternehmens zu helfen. AWS Systems Manager weist Ihren verwalteten Instanzen einen Konfigurationsstatus zu und ermöglicht es Ihnen, Basiswerte für Betriebssystem-Patch-Levels, Softwareinstallationen, Anwendungskonfigurationen und andere Details zu Ihrer Umgebung festzulegen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
CM-2	Die Organisation entwickelt, dokumentiert und verwaltet unter Konfigurationskontrolle eine aktuelle Basiskonfiguration des Informationssystems.	ec2-stopped-instance	Aktivieren Sie diese Regel, um bei der Basiskonfiguration von Amazon Elastic Compute Cloud (Amazon EC2) - Instances zu helfen, indem Sie überprüfen, ob EC2 Amazon-Instances gemäß den Standards Ihrer Organisation für mehr als die zulässige Anzahl von Tagen gestoppt wurden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
CM-2	Die Organisation entwickelt, dokumentiert und verwaltet unter Konfigurationskontrolle eine aktuelle Basiskonfiguration des Informationssystems.	ec2- volume-inuse-check	Diese Regel stellt sicher, dass Amazon Elastic Block Store-Volumes, die an Amazon Elastic Compute Cloud (Amazon EC2) - Instances angehängt sind, zum Löschen markiert werden, wenn eine Instance beendet wird. Wenn ein Amazon-EBS-Volume nicht gelöscht wird, wenn die Instance, an die es angehängt ist, beendet wird, kann dies gegen das Konzept der geringsten Funktionalität verstoßen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
CM-2	Die Organisation entwickelt, dokumentiert und verwaltet unter Konfigurationskontrolle eine aktuelle Basiskonfiguration des Informationssystems.	elb-deletion-protection-enabled	Diese Regel sorgt dafür, dass der Löschschutz für Elastic Load Balancing aktiviert ist. Verwenden Sie diese Funktion, um zu verhindern, dass Ihr Load Balancer versehentlich oder böswillig gelöscht wird, was zum Verlust der Verfügbarkeit Ihrer Anwendungen führen kann.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
CM-2	Die Organisation entwickelt, dokumentiert und verwaltet unter Konfigurationskontrolle eine aktuelle Basiskonfiguration des Informationssystems.	restricted-common-ports	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass gemeinsame Ports für Amazon Elastic Compute Cloud (Amazon EC2) -Sicherheitsgruppen eingeschränkt sind. Wenn der Zugriff auf Ports nicht auf vertrauenswürdige Quellen beschränkt wird, kann dies zu Angriffen auf die Verfügbarkeit, Integrität und Vertraulichkeit von Systemen führen. Mit dieser Regel können Sie optional die Parameter blockedPort1–blockedPort5 festlegen (Standardkonfigurationen: 20, 21, 3389, 3306, 4333). Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
CM-2	Die Organisation entwickelt, dokumentiert und verwaltet unter Konfigurationskontrolle eine aktuelle Basiskonfiguration des Informationssystems.	s3 bucket-level-public-access - verboten	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Simple Storage Service (Amazon S3) -Buckets nicht öffentlich zugänglich sind. Diese Regel trägt dazu bei, sensible Daten vor unbefugten Remote-Benutzern zu schützen, indem sie den öffentlichen Zugriff auf Bucket-Ebene verhindert.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
CM-2	Die Organisation entwickelt, dokumentiert und verwaltet unter Konfigurationskontrolle eine aktuelle Basiskonfiguration des Informationssystems.	subnet-auto-assign-public-ip-deaktiviert	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon Virtual Private Cloud (VPC) -Subnetzen nicht automatisch eine öffentliche IP-Adresse zugewiesen wird. Amazon Elastic Compute Cloud (EC2) -Instances, die in Subnetzen gestartet werden, in denen dieses Attribut aktiviert ist, haben ihrer primären Netzwerkschnittstelle eine öffentliche IP-Adresse zugewiesen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
CM-7(a)	Die Organisation: a. Konfiguriert das Informationssystem auf eine Weise, dass nur wesentliche Funktionen bereitgestellt werden.	ec2- instance-profile-attached	EC2 Instanzprofile übergeben eine IAM-Rolle an eine EC2 Instance. Das Anhängen eines Instance-Profils an Ihre Instances kann bei der Implementierung von geringsten Berechtigungen und der Berechtigungsverwaltung helfen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
CM-7(a)	Die Organisation: a. Konfiguriert das Informationssystem auf eine Weise, dass nur wesentliche Funktionen bereitgestellt werden.	ec2-manager instance-managed-by-systems	Eine Bestandsaufnahme der Softwareplattformen und Anwendungen innerhalb des Unternehmens ist möglich, indem Amazon Elastic Compute Cloud (Amazon EC2) - Instances mit AWS Systems Manager verwaltet werden. Verwenden Sie AWS Systems Manager, um detaillierte Systemkonfigurationen, Betriebssystem-Patch-Levels, Namen und Typ der Dienste, Softwareinstallationen, Anwendungsname, Herausgeber und Version sowie andere Details zu Ihrer Umgebung bereitzustellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
CM-7(a)	Die Organisation: a. Konfiguriert das Informationssystem auf eine Weise, dass nur wesentliche Funktionen bereitgestellt werden.	ec2-check managedinstance-association-compliance-status	Verwenden Sie AWS Systems Manager Associations, um bei der Inventarisierung von Softwareplattformen und Anwendungen innerhalb eines Unternehmens zu helfen. AWS Systems Manager weist Ihren verwalteten Instanzen einen Konfigurationsstatus zu und ermöglicht es Ihnen, Basiswerte für Betriebssystem-Patch-Levels, Softwareinstallationen, Anwendungskonfigurationen und andere Details zu Ihrer Umgebung festzulegen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
CM-8(1)	Die Organisation aktualisiert das Inventar der Informationssystemkomponenten als integralen Bestandteil der Installation und Demontage von Komponenten sowie der Aktualisierung von Informationssystemen.	ec2-managed-instance-managed-by-systems	Eine Bestandsaufnahme der Softwareplattformen und Anwendungen innerhalb des Unternehmens ist möglich, indem Amazon Elastic Compute Cloud (Amazon EC2) - Instances mit AWS Systems Manager verwaltet werden. Verwenden Sie AWS Systems Manager, um detaillierte Systemkonfigurationen, Betriebssystem-Patch-Levels, Namen und Typ der Dienste, Softwareinstallationen, Anwendungsname, Herausgeber und Version sowie andere Details zu Ihrer Umgebung bereitzustellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
CM-8(1)	Die Organisation aktualisiert das Inventar der Informationssystemkomponenten als integralen Bestandteil der Installation und Demontage von Komponenten sowie der Aktualisierung von Informationssystemen.	ec2-check managedinstance-association-compliance-status	Verwenden Sie AWS Systems Manager Associations, um bei der Inventarisierung von Softwareplattformen und Anwendungen innerhalb eines Unternehmens zu helfen. AWS Systems Manager weist Ihren verwalteten Instanzen einen Konfigurationsstatus zu und ermöglicht es Ihnen, Basiswerte für Betriebssystem-Patch-Levels, Softwareinstallationen, Anwendungskonfigurationen und andere Details zu Ihrer Umgebung festzulegen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
CM-8(3)(a)	Die Organisation: a. Setzt kontinuierlich automatisierte Mechanismen ein und verwendet automatisierte Mechanismen mit einer Erkennungsverzögerung von maximal fünf Minuten, um nicht autorisierte Hardware-, Software- und Firmware-Komponenten im Informationssystem zu erkennen.	ec2-manager instance-managed-by-systems	Eine Bestandsaufnahme der Softwareplattformen und Anwendungen innerhalb des Unternehmens ist möglich, indem Amazon Elastic Compute Cloud (Amazon EC2) - Instances mit AWS Systems Manager verwaltet werden. Verwenden Sie AWS Systems Manager, um detaillierte Systemkonfigurationen, Betriebssystem-Patch-Levels, Namen und Typ der Dienste, Softwareinstallationen, Anwendungsname, Herausgeber und Version sowie andere Details zu Ihrer Umgebung bereitzustellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
CM-8(3)(a)	Die Organisation: a. Setzt kontinuierlich automatisierte Mechanismen ein und verwendet automatisierte Mechanismen mit einer Erkennungsverzögerung von maximal fünf Minuten, um nicht autorisierte Hardware-, Software- und Firmware-Komponenten im Informationssystem zu erkennen.	ec2-check managedinstance-association-compliance-status	Verwenden Sie AWS Systems Manager Associations, um bei der Inventarisierung von Softwareplattformen und Anwendungen innerhalb eines Unternehmens zu helfen. AWS Systems Manager weist Ihren verwalteten Instanzen einen Konfigurationsstatus zu und ermöglicht es Ihnen, Basiswerte für Betriebssystem-Patch-Levels, Softwareinstallationen, Anwendungskonfigurationen und andere Details zu Ihrer Umgebung festzulegen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
CM-8(3)(a)	Die Organisation: a. Setzt kontinuierlich automatisierte Mechanismen ein und verwendet automatisierte Mechanismen mit einer Erkennungsverzögerung von maximal fünf Minuten, um nicht autorisierte Hardware-, Software- und Firmware-Komponenten im Informationssystem zu erkennen.	ec2-check managedinstance-patch-compliance-status	Aktivieren Sie diese Regel, um bei der Identifizierung und Dokumentation von Sicherheitslücken in Amazon Elastic Compute Cloud (Amazon EC2) zu helfen. Die Regel prüft, ob die EC2 Amazon-Instance die Patch-Konformität im AWS Systems Manager gemäß den Richtlinien und Verfahren Ihrer Organisation einhält.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
CM-8(3)(a)	Die Organisation: a. Setzt kontinuierlich automatisierte Mechanismen ein und verwendet automatisierte Mechanismen mit einer Erkennungsverzögerung von maximal fünf Minuten, um nicht autorisierte Hardware-, Software- und Firmware-Komponenten im Informationssystem zu erkennen.	guardduty-enabled-centralized	Amazon GuardDuty kann mithilfe von Threat Intelligence Feeds helfen, potenzielle Cybersicherheitsereignisse zu überwachen und zu erkennen. Dazu gehören Listen mit bösartigen IPs und maschinellen Lernmethoden, um unerwartete, unbefugte und bösartige Aktivitäten in Ihrer AWS Cloud-Umgebung zu identifizieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
CP-9(b)	Die Organisation: b. Führt Backups der im Informationssystem enthaltenen Informationen auf Systemebene durch (inkrementelles Backup täglich; vollständiges Backup wöchentlich).	aurora-resources-protected-by-Backup-Plan	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon Aurora Aurora-Ressourcen Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
CP-9(b)	Die Organisation: b. Führt Backups der im Informationssystem enthaltenen Informationen auf Systemebene durch (inkrementelles Backup täglich; vollständiges Backup wöchentlich).	backup-plan-min-frequency-and-min-retention-check	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihr AWS Backup-Plan auf eine Mindestfrequenz und Aufbewahrung festgelegt ist. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen. Mit dieser Regel können Sie die Parameter requiredFrequencyValue (Config default: 1), requiredRetentionDays (Config default: 35) und requiredFrequencyUnit

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
			(Config default: days) festlegen. Der tatsächliche Wert muss den Anforderungen Ihrer Organisation entsprechen.
CP-9(b)	Die Organisation: b. Führt Backups der im Informationssystem enthaltenen Informationen auf Systemebene durch (inkrementelles Backup täglich; vollständiges Backup wöchentlich).	dynamodb-resources-protected-by-Backup-Plan	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon DynamoDB DynamoDB-Ressourcen Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
CP-9(b)	Die Organisation: b. Führt Backups der im Informationssystem enthaltenen Informationen auf Systemebene durch (inkrementelles Backup täglich; vollständiges Backup wöchentlich).	ebs-resources-protected-by-Backup-Plan	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon Elastic Block Store (Amazon EBS) -Ressourcen Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
CP-9(b)	Die Organisation: b. Führt Backups der im Informationssystem enthaltenen Informationen auf Systemebene durch (inkrementelles Backup täglich; vollständiges Backup wöchentlich).	ec2--Plan resources-protected-by-backup	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon Elastic Compute Cloud (Amazon EC2) -Ressourcen Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
CP-9(b)	Die Organisation: b. Führt Backups der im Informationssystem enthaltenen Informationen auf Systemebene durch (inkrementelles Backup täglich; vollständiges Backup wöchentlich).	efs-resources-protected-by-Backup-Plan	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon Elastic File System (Amazon EFS) -Dateisysteme Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
CP-9(b)	Die Organisation: b. Führt Backups der im Informationssystem enthaltenen Informationen auf Systemebene durch (inkrementelles Backup täglich; vollständiges Backup wöchentlich).	fsx-resources-protected-by-Backup-Plan	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre FSx Amazon-Dateisysteme Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
CP-9(b)	Die Organisation: b. Führt Backups der im Informationssystem enthaltenen Informationen auf Systemebene durch (inkrementelles Backup täglich; vollständiges Backup wöchentlich).	rds-resources-protected-by-Backup-Plan	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon Relational Database Service (Amazon RDS) -Ressourcen Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
CP-9(b)	Die Organisation: b. Führt Backups der im Informationssystem enthaltenen Informationen auf Systemebene durch (inkrementelles Backup täglich; vollständiges Backup wöchentlich).	redshift-backup-enabled	Stellen Sie zur Unterstützung der Datensicherungsprozesse sicher, dass Ihre Amazon-Redshift-Cluster über automatisierte Snapshots verfügen. Wenn automatisierte Snapshots für einen Cluster aktiviert sind, erstellt Redshift in regelmäßigen Abständen Snapshots dieses Clusters. Standardmäßig erstellt Redshift alle acht Stunden oder alle 5 GB einen Snapshot für jeden Knoten mit Datenänderungen oder je nachdem, was zuerst eintritt.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
CP-9(b)	Die Organisation: b. Führt Backups der im Informationssystem enthaltenen Informationen auf Systemebene durch (inkrementelles Backup täglich; vollständiges Backup wöchentlich).	db-instance-backup-enabled	Die Sicherungsfunktion von Amazon RDS erstellt Sicherungen Ihrer Datenbanken und Transaktionsprotokolle. Amazon RDS erstellt einen Snapshot für das Speichervolume Ihrer DB-Instance, sodass die gesamte DB-Instance gesichert wird. Sie können im System spezifische Aufbewahrungsfristen festlegen, um Ihre Ausfallsicherheitsanforderungen zu erfüllen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
CP-9(b)	Die Organisation: b. Führt Backups der im Informationssystem enthaltenen Informationen auf Systemebene durch (inkrementelles Backup täglich; vollständiges Backup wöchentlich).	dynamodb-pitr-enabled	Aktivieren Sie diese Regel, um zu überprüfen, ob die Informationen gesichert wurden. Es verwaltet auch die Backups, indem es sicherstellt, dass die point-in-time Wiederherstellung in Amazon DynamoDB aktiviert ist. Bei der Wiederherstellung werden fortlaufende Backups Ihrer Tabelle für die letzten 35 Tage gespeichert.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
CP-9(b)	Die Organisation: b. Führt Backups der im Informationssystem enthaltenen Informationen auf Systemebene durch (inkrementelles Backup täglich; vollständiges Backup wöchentlich).	elasticache-redis-cluster-automatic-Backup-Prüfung	Wenn automatische Backups aktiviert sind, ElastiCache erstellt Amazon täglich ein Backup des Clusters. Die Sicherung kann für eine von Ihrer Organisation festgelegte Anzahl von Tagen aufbewahrt werden. Automatische Backups schützen vor Datenverlust. Bei einem Ausfall können Sie einen neuen Cluster erstellen, der Ihre Daten aus dem aktuellen Backup wiederherstellt.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
CP-9(b)	Die Organisation: b. Führt Backups der im Informationssystem enthaltenen Informationen auf Systemebene durch (inkrementelles Backup täglich; vollständiges Backup wöchentlich).	s-3 bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) unterstützt die Aufrechterhaltung einer angemessenen Kapazität und Verfügbarkeit. CRR ermöglicht das automatische, asynchrone Kopieren von Objekten in Amazon-S3-Buckets, um die Datenverfügbarkeit sicherzustellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
CP-9(b)	Die Organisation: b. Führt Backups der im Informationssystem enthaltenen Informationen auf Systemebene durch (inkrementelles Backup täglich; vollständiges Backup wöchentlich).	s-3 bucket-versioning-enabled	Die Versionsverwaltung von Amazon Simple Storage Service (Amazon S3)-Buckets hilft dabei, mehrere Varianten eines Objekts im selben Amazon-S3-Bucket zu speichern. Verwenden Sie die Versionsverwaltung, um sämtliche Versionen aller Objekte in Ihrem Amazon-S3-Bucket zu speichern, abzurufen oder wiederherzustellen. Mit der Versionsverwaltung können Sie Versionen sowohl nach unbeabsichtigten Benutzeraktionen als auch nach Anwendungsfehlern problemlos wiederherstellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
CP-10	Die Organisation sorgt dafür, dass das Informationssystem nach einer Unterbrechung, einer Beeinträchtigung oder einem Ausfall wiederhergestellt und wieder in einen bekannten Zustand versetzt wird.	aurora-resources-protected-by-Backup-Plan	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon Aurora Aurora-Ressourcen Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
CP-10	Die Organisation sorgt dafür, dass das Informationssystem nach einer Unterbrechung, einer Beeinträchtigung oder einem Ausfall wiederhergestellt und wieder in einen bekannten Zustand versetzt wird.	backup-plan-min-frequency-and-min-retention-check	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihr AWS Backup-Plan auf eine Mindestfrequenz und Aufbewahrung festgelegt ist. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen. Mit dieser Regel können Sie die Parameter requiredFrequencyValue (Config default: 1), requiredRetentionDays (Config default: 35) und requiredFrequencyUnit

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
			(Config default: days) festlegen. Der tatsächliche Wert muss den Anforderungen Ihrer Organisation entsprechen.
CP-10	Die Organisation sorgt dafür, dass das Informationssystem nach einer Unterbrechung, einer Beeinträchtigung oder einem Ausfall wiederhergestellt und wieder in einen bekannten Zustand versetzt wird.	dynamodb-resources-protected-by-Backup-Plan	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon DynamoDB DynamoDB-Ressourcen Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
CP-10	Die Organisation sorgt dafür, dass das Informationssystem nach einer Unterbrechung, einer Beeinträchtigung oder einem Ausfall wiederhergestellt und wieder in einen bekannten Zustand versetzt wird.	ebs-resources-protected-by-Backup-Plan	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon Elastic Block Store (Amazon EBS) -Ressourcen Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
CP-10	Die Organisation sorgt dafür, dass das Informationssystem nach einer Unterbrechung, einer Beeinträchtigung oder einem Ausfall wiederhergestellt und wieder in einen bekannten Zustand versetzt wird.	ec2--Plan resources-protected-by-backup	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon Elastic Compute Cloud (Amazon EC2) -Ressourcen Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
CP-10	Die Organisation sorgt dafür, dass das Informationssystem nach einer Unterbrechung, einer Beeinträchtigung oder einem Ausfall wiederhergestellt und wieder in einen bekannten Zustand versetzt wird.	efs-resources-protected-by-Backup-Plan	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon Elastic File System (Amazon EFS) -Dateisysteme Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
CP-10	Die Organisation sorgt dafür, dass das Informationssystem nach einer Unterbrechung, einer Beeinträchtigung oder einem Ausfall wiederhergestellt und wieder in einen bekannten Zustand versetzt wird.	elb-cross-zone-load-Balancing aktiviert	Aktivieren Sie zonenübergreifendes Load Balancing für Ihre Elastic Load Balancer (ELBs), um eine angemessene Kapazität und Verfügbarkeit aufrechtzuerhalten. Zonenübergreifendes Load Balancing reduziert die Notwendigkeit, die gleiche Anzahl von Instances in jeder aktivierten Availability Zone aufrechtzuerhalten. Es verbessert auch die Fähigkeit Ihrer Anwendung, den Verlust einer oder mehrerer Instances zu bewältigen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
CP-10	Die Organisation sorgt dafür, dass das Informationssystem nach einer Unterbrechung, einer Beeinträchtigung oder einem Ausfall wiederhergestellt und wieder in einen bekannten Zustand versetzt wird.	fsx-resources-protected-by-Backup-Plan	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre FSx Amazon-Dateisysteme Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
CP-10	Die Organisation sorgt dafür, dass das Informationssystem nach einer Unterbrechung, einer Beeinträchtigung oder einem Ausfall wiederhergestellt und wieder in einen bekannten Zustand versetzt wird.	rds-resources-protected-by-Backup-Plan	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon Relational Database Service (Amazon RDS) -Ressourcen Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
CP-10	Die Organisation sorgt dafür, dass das Informationssystem nach einer Unterbrechung, einer Beeinträchtigung oder einem Ausfall wiederhergestellt und wieder in einen bekannten Zustand versetzt wird.	redshift-backup-enabled	Stellen Sie zur Unterstützung der Datensicherungsprozesse sicher, dass Ihre Amazon-Redshift-Cluster über automatisierte Snapshots verfügen. Wenn automatisierte Snapshots für einen Cluster aktiviert sind, erstellt Redshift in regelmäßigen Abständen Snapshots dieses Clusters. Standardmäßig erstellt Redshift alle acht Stunden oder alle 5 GB einen Snapshot für jeden Knoten mit Datenänderungen oder je nachdem, was zuerst eintritt.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
CP-10	Die Organisation sorgt dafür, dass das Informationssystem nach einer Unterbrechung, einer Beeinträchtigung oder einem Ausfall wiederhergestellt und wieder in einen bekannten Zustand versetzt wird.	db-instance-backup-enabled	Die Sicherungsfunktion von Amazon RDS erstellt Sicherungen Ihrer Datenbanken und Transaktionsprotokolle. Amazon RDS erstellt einen Snapshot für das Speichervolume Ihrer DB-Instance, sodass die gesamte DB-Instance gesichert wird. Sie können im System spezifische Aufbewahrungsfristen festlegen, um Ihre Ausfallsicherheitsanforderungen zu erfüllen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
CP-10	Die Organisation sorgt dafür, dass das Informationssystem nach einer Unterbrechung, einer Beeinträchtigung oder einem Ausfall wiederhergestellt und wieder in einen bekannten Zustand versetzt wird.	dynamodb-autoscaling-enabled	Amazon DynamoDB Auto Scaling verwendet den AWS Application Auto Scaling-Service, um die bereitgestellte Durchsatzkapazität so anzupassen, dass sie automatisch auf tatsächliche Verkehrsmuster reagiert. Auf diese Weise kann eine Tabelle oder ein globaler sekundärer Index die bereitgestellte Lese-/Schreibkapazität erhöhen, um plötzliche Erhöhungen des Datenverkehrs ohne Drosselung zu bewältigen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
CP-10	Die Organisation sorgt dafür, dass das Informationssystem nach einer Unterbrechung, einer Beeinträchtigung oder einem Ausfall wiederhergestellt und wieder in einen bekannten Zustand versetzt wird.	dynamodb-pitr-enabled	Aktivieren Sie diese Regel, um zu überprüfen, ob die Informationen gesichert wurden. Es verwaltet auch die Backups, indem es sicherstellt, dass die point-in-time Wiederherstellung in Amazon DynamoDB aktiviert ist. Bei der Wiederherstellung werden fortlaufende Backups Ihrer Tabelle für die letzten 35 Tage gespeichert.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
CP-10	Die Organisation sorgt dafür, dass das Informationssystem nach einer Unterbrechung, einer Beeinträchtigung oder einem Ausfall wiederhergestellt und wieder in einen bekannten Zustand versetzt wird.	ebs-optimized-instance	Eine optimierte Instance im Amazon Elastic Block Store (Amazon EBS) bietet zusätzliche, dedizierte Kapazität für Amazon-EBS-I/O-Vorgänge. Diese Optimierung bietet die beste Leistung für Ihr EBS-Volume, indem Konflikte zwischen Amazon-EBS-I/O und anderem Datenverkehr von Ihrer Instance minimiert werden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
CP-10	Die Organisation sorgt dafür, dass das Informationssystem nach einer Unterbrechung, einer Beeinträchtigung oder einem Ausfall wiederhergestellt und wieder in einen bekannten Zustand versetzt wird.	elasticache-redis-cluster-automatic-Backup-Prüfung	Wenn automatische Backups aktiviert sind, ElastiCache erstellt Amazon täglich ein Backup des Clusters. Die Sicherung kann für eine von Ihrer Organisation festgelegte Anzahl von Tagen aufbewahrt werden. Automatische Backups schützen vor Datenverlust. Bei einem Ausfall können Sie einen neuen Cluster erstellen, der Ihre Daten aus dem aktuellen Backup wiederherstellt.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
CP-10	Die Organisation sorgt dafür, dass das Informationssystem nach einer Unterbrechung, einer Beeinträchtigung oder einem Ausfall wiederhergestellt und wieder in einen bekannten Zustand versetzt wird.	elb-deletion-protection-enabled	Diese Regel sorgt dafür, dass der Löschschutz für Elastic Load Balancing aktiviert ist. Verwenden Sie diese Funktion, um zu verhindern, dass Ihr Load Balancer versehentlich oder böswillig gelöscht wird, was zum Verlust der Verfügbarkeit Ihrer Anwendungen führen kann.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
CP-10	Die Organisation sorgt dafür, dass das Informationssystem nach einer Unterbrechung, einer Beeinträchtigung oder einem Ausfall wiederhergestellt und wieder in einen bekannten Zustand versetzt wird.	rds-multi-az-support	Die Multi-AZ-Unterstützung in Amazon Relational Database Service (Amazon RDS) bietet eine verbesserte Verfügbarkeit und Beständigkeit von Datenbank-Instances. Wenn Sie eine Multi-AZ-Datenbank-Instance bereitstellen, erstellt Amazon RDS automatisch eine primäre Datenbank-Instance und repliziert die Daten synchron auf eine Standby-Instance in einer anderen Availability Zone. Jede Availability Zone läuft auf einer eigenen, physisch getrennten, unabhängigen Infrastruktur und ist auf eine hohe Verfügbarkeit ausgelegt. Im Falle eines Infrastrukturausfalls führt Amazon RDS einen automatis

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
			chen Failover zum Standby-Modus durch, sodass Sie den Datenbankbetrieb wieder aufnehmen können, sobald der Failover abgeschlo ssen ist.
CP-10	Die Organisation sorgt dafür, dass das Informationssystem nach einer Unterbrec hung, einer Beeinträc htigung oder einem Ausfall wiederher gestellt und wieder in einen bekannten Zustand versetzt wird.	s-3 bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) unterstützt die Aufrechterhaltung einer angemesse nen Kapazität und Verfügbarkeit. CRR ermöglicht das automatische, asynchrone Kopieren von Objekten in Amazon-S3-Buckets, um die Datenverf ügbarkeit sicherzus tellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
CP-10	Die Organisation sorgt dafür, dass das Informationssystem nach einer Unterbrechung, einer Beeinträchtigung oder einem Ausfall wiederhergestellt und wieder in einen bekannten Zustand versetzt wird.	s-3 bucket-versioning-enabled	Die Versionsverwaltung von Amazon Simple Storage Service (Amazon S3)-Buckets hilft dabei, mehrere Varianten eines Objekts im selben Amazon-S3-Bucket zu speichern. Verwenden Sie die Versionsverwaltung, um sämtliche Versionen aller Objekte in Ihrem Amazon-S3-Bucket zu speichern, abzurufen oder wiederherzustellen. Mit der Versionsverwaltung können Sie Versionen sowohl nach unbeabsichtigten Benutzeraktionen als auch nach Anwendungsfehlern problemlos wiederherstellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
CP-10	Die Organisation sorgt dafür, dass das Informationssystem nach einer Unterbrechung, einer Beeinträchtigung oder einem Ausfall wiederhergestellt und wieder in einen bekannten Zustand versetzt wird.	vpc-vpn-2-tunnels-up	Redundante Site-to-Site VPN-Tunnel können implementiert werden, um die Anforderungen an die Ausfallsicherheit zu erfüllen. Es verwendet zwei Tunnel, um die Konnektivität sicherzustellen, falls eine der Site-to-Site VPN-Verbindungen nicht verfügbar ist. Um sich vor einem Verbindungsverlust zu schützen, können Sie für den Fall, dass Ihr Kunden-Gateway nicht verfügbar ist, eine zweite Site-to-Site VPN-Verbindung zu Ihrer Amazon Virtual Private Cloud (Amazon VPC) und Ihrem Virtual Private Gateway einrichten, indem Sie ein zweites Kunden-Gateway verwenden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
IA-2(1)(2)	(1) Das Informationssystem implementiert eine Multi-Faktor-Authentifizierung für den Netzwerkzugriff auf privilegierte Konten. (1) Das Informationssystem implementiert eine Multifaktor-Authentifizierung für den Netzwerkzugriff auf nicht privilegierte Konten.	root-account-mfa-enabled	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass MFA für den Root-Benutzer aktiviert ist. Der Stammbenutzer ist der AWS-Konto-Benutzer mit den meisten Berechtigungen. MFA sorgt für eine weitere Schutzebene zusätzlich zu den Anmeldeinformationen. Indem Sie MFA für den Root-Benutzer vorschreiben, können Sie die Anzahl AWS-Konten kompromittierter Benutzer reduzieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
IA-2(1)(2)	(1) Das Informationssystem implementiert eine Multi-Faktor-Authentifizierung für den Netzwerkzugriff auf privilegierte Konten. (1) Das Informationssystem implementiert eine Multifaktor-Authentifizierung für den Netzwerkzugriff auf nicht privilegierte Konten.	iam-user-mfa-enabled	Aktivieren Sie diese Regel, um den Zugriff auf Ressourcen in der AWS Cloud einzuschränken. Diese Regel sorgt dafür, dass die Multi-Faktor-Authentifizierung (MFA) für alle Benutzer aktiviert ist. MFA sorgt für eine weitere Schutzebene zusätzlich zu den Anmeldeinformationen. Reduzieren Sie Fälle von kompromittierten Konten, indem Sie MFA für Benutzer vorschreiben.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
IA-2(1)(2)	(1) Das Informationssystem implementiert eine Multi-Faktor-Authentifizierung für den Netzwerkzugriff auf privilegierte Konten. (1) Das Informationssystem implementiert eine Multifaktor-Authentifizierung für den Netzwerkzugriff auf nicht privilegierte Konten.	mfa-enabled-for-iam-Konsolenzugriff	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass MFA für alle AWS Identity and Access Management (IAM) -Benutzer aktiviert ist, die über ein Konsolenkennwort verfügen. MFA sorgt für eine weitere Schutzebene zusätzlich zu den Anmeldeinformationen. Indem Sie MFA für Benutzer vorschreiben, können Sie Fälle kompromittierter Konten reduzieren und verhindern, dass unbefugte Benutzer auf vertrauliche Daten zugreifen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
IA-2(1)(2)	(1) Das Informationssystem implementiert eine Multi-Faktor-Authentifizierung für den Netzwerkzugriff auf privilegierte Konten. (1) Das Informationssystem implementiert eine Multifaktor-Authentifizierung für den Netzwerkzugriff auf nicht privilegierte Konten.	root-account-hardware-mfa-aktiviert	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Hardware-MFA für den Root-Benutzer aktiviert ist. Der Stammbenutzer ist der AWS-Konto-Benutzer mit den meisten Berechtigungen. MFA sorgt für eine weitere Schutzebene zusätzlich zu den Anmeldeinformationen. Indem Sie MFA für den Root-Benutzer vorschreiben, können Sie die Anzahl AWS-Konten kompromittierter Benutzer reduzieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
IA-2(1)	(1) Das Informationssystem implementiert eine Multi-Faktor-Authentifizierung für den Netzwerkzugriff auf privilegierte Konten.	iam-user-mfa-enabled	Aktivieren Sie diese Regel, um den Zugriff auf Ressourcen in der AWS Cloud einzuschränken. Diese Regel sorgt dafür, dass die Multi-Faktor-Authentifizierung (MFA) für alle Benutzer aktiviert ist. MFA sorgt für eine weitere Schutzebene zusätzlich zu den Anmeldeinformationen. Reduzieren Sie Fälle von kompromittierten Konten, indem Sie MFA für Benutzer vorschreiben.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
IA-2(1)	(1) Das Informationssystem implementiert eine Multi-Faktor-Authentifizierung für den Netzwerkzugriff auf privilegierte Konten.	mfa-enabled-for-iam-Konsolenzugriff	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass MFA für alle AWS Identity and Access Management (IAM) -Benutzer aktiviert ist, die über ein Konsolenkennwort verfügen. MFA sorgt für eine weitere Schutzebene zusätzlich zu den Anmeldeinformationen. Indem Sie MFA für Benutzer vorschreiben, können Sie Fälle kompromittierter Konten reduzieren und verhindern, dass unbefugte Benutzer auf vertrauliche Daten zugreifen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
IA-2(1)	(1) Das Informationssystem implementiert eine Multi-Faktor-Authentifizierung für den Netzwerkzugriff auf privilegierte Konten.	root-account-hardware-mfa-aktiviert	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Hardware-MFA für den Root-Benutzer aktiviert ist. Der Stammbenutzer ist der AWS-Konto-Benutzer mit den meisten Berechtigungen. MFA sorgt für eine weitere Schutzebene zusätzlich zu den Anmeldeinformationen. Indem Sie MFA für den Root-Benutzer vorschreiben, können Sie die Anzahl AWS-Konten kompromittierter Benutzer reduzieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
IA-2(1)	(1) Das Informationssystem implementiert eine Multi-Faktor-Authentifizierung für den Netzwerkzugriff auf privilegierte Konten.	root-account-mfa-enabled	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass MFA für den Root-Benutzer aktiviert ist. Der Stammbenutzer ist der AWS-Konto-Benutzer mit den meisten Berechtigungen. MFA sorgt für eine weitere Schutzebene zusätzlich zu den Anmeldeinformationen. Indem Sie MFA für den Root-Benutzer vorschreiben, können Sie die Anzahl AWS-Konten kompromittierter Benutzer reduzieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
IA-2	Das Informati onssystem nimmt eine eindeutige Identifizierung und Authentifizierung der Benutzer (oder Prozesse, die im Namen von Benutzern der Organisation handeln) vor.	iam-password-policy	Die Identitäten und Anmeldeinformation en werden auf der Grundlage einer organisatorischen IAM-Passwortrichtl inie ausgestellt, verwaltet und verifizie rt. Sie erfüllen oder übertreffen die Anforderungen, die von NIST SP 800-63 und dem Standard „Best Practices“ von AWS Foundational Security in Bezug auf die Passworts tärke festgelegt sind. Mit dieser Regel können Sie optional RequireUppercaseCh aracters (Wert für AWS grundlegende Sicherheitsbewährt e Methoden: wahr), RequireLowercaseCh aracters (Wert für bewährte Methoden für AWS grundlege nde Sicherheit: wahr), RequireSy mbols (Wert für bewährte Methoden

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
			für AWS grundlegende Sicherheit: wahr), RequireNumbers (Wert für bewährte Methoden für AWS grundlegende Sicherheit: wahr), MinimumPasswordLength (Wert für bewährte Methoden für AWS grundlegende Sicherheit: 14), PasswordReusePrevention (Wert für bewährte Methoden für AWS grundlegende Sicherheit: 24) und MaxPasswordAge (Wert für bewährte Methoden für AWS grundlegende Sicherheit: 90) für Ihr IAM festlegen Kennwortrichtlinie. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
IA-2	Das Informati onssystem nimmt eine eindeutige Identifizierung und Authentifizierung der Benutzer (oder Prozesse, die im Namen von Benutzern der Organisation handeln) vor.	iam-root-access-key-überprüfen	Der Zugriff auf Systeme und Ressourcen kann gesteuert werden, indem überprüft wird, ob der Root-Benu tzer keine Zugriffss chlüssel mit seiner AWS Identity and Access Management (IAM) -Rolle verknüpft hat. Stellen Sie sicher, dass die Root-Zugr iffsschlüssel gelöscht werden. Erstellen und verwenden Sie stattdessen rollenbas ierte Funktionen, AWS-Konten um das Prinzip der geringste n Funktionalität zu berücksichtigen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
IA-5(1)(a)(d)(e)	Das Informati onssystem ergreift für die passwortgestützte Authentifizierung folgende Maßnahmen : a. Es erzwingt eine Mindestkomplexität von [Zuweisung: vom Unternehm en festgelegte Anforderungen an Groß- und Kleinschr eibung, Zeichenan zahl, Kombinati on aus Groß- und Kleinbuchstaben, Zahlen und Sonderzei chen, einschlie ßlich Mindestan forderungen für jeden Typ]; d. Es erzwingt die minimale und maximale Gültigkeitsdauer von Passwörtern von [Zuweisung: von der Organisat ion festgelegte Frist für die minimale und maximale Gültigkeitsdauer]; e. Verbietet die Wiederverwendung	iam-password-policy	Die Identitäten und Anmeldeinformation en werden auf der Grundlage einer organisatorischen IAM-Passwortrichtlinie ausgestellt, verwaltet und verifiziert. Sie erfüllen oder übertreff en die Anforderungen von NIST SP 800-63 und dem Standard „Best Practices“ von AWS Foundatio nal Security für die Passwortstärke. Mit dieser Regel können Sie optional RequireUppercaseCh aracters (Wert für AWS grundlegende Sicherheitsbewährt e Methoden: wahr), RequireLowercaseCh aracters (Wert für bewährte Methoden für AWS grundlege nde Sicherheit: wahr), RequireSy mbols (Wert für bewährte Methoden für AWS grundlege nde Sicherheit:

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
	von Passwörtern für die nächsten 24 Generationen.		wahr), RequireNumbers (Wert für bewährte Methoden für AWS grundlegende Sicherheit: wahr), MinimumPasswordLength (Wert für bewährte Methoden für AWS grundlegende Sicherheit: 14), PasswordReusePrevention (Wert für bewährte Methoden für AWS grundlegende Sicherheit: 24) und MaxPasswordAge (Wert für bewährte Methoden für AWS grundlegende Sicherheit: 90) für Ihr IAM festlegen Kennwortrichtlinie. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
IA-5(4)	Die Organisation verwendet automatisierte Tools, um festzustellen, ob Passwortauthentifikatoren stark genug sind, um [Zuweisung: von der Organisation definierte Anforderungen] zu erfüllen.	iam-password-policy	Die Identitäten und Anmeldeinformationen werden auf der Grundlage einer organisatorischen IAM-Passwortrichtlinie ausgestellt, verwaltet und verifiziert. Sie erfüllen oder übertreffen die Anforderungen des NIST SP 800-63 und des AWS Foundational Security Best Practices-Standards für Passwortstärke. Mit dieser Regel können Sie optional RequireUppercaseCharacters (Wert für AWS grundlegende Sicherheitsbewährte Methoden: wahr), RequireLowercaseCharacters (Wert für bewährte Methoden für AWS grundlegende Sicherheit: wahr), RequireSymbols (Wert für bewährte Methoden für AWS grundlegende Sicherheit:

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
			wahr), RequireNumbers (Wert für bewährte Methoden für AWS grundlegende Sicherheit: wahr), MinimumPasswordLength (Wert für bewährte Methoden für AWS grundlegende Sicherheit: 14), PasswordReusePrevention (Wert für bewährte Methoden für AWS grundlegende Sicherheit: 24) und MaxPasswordAge (Wert für bewährte Methoden für AWS grundlegende Sicherheit: 90) für Ihr IAM festlegen Kennwortrichtlinie. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
IA-5(7)	Die Organisation stellt sicher, dass unverschlüsselte statische Authentifikatoren nicht in Anwendungen oder Zugriffsskripts eingebettet oder in Funktionsschlüsseln gespeichert werden.	codebuild-project-envvar-awscred-überprüfen	Stellen Sie sicher, dass die Anmeldeinformationen AWS_ACCESS_KEY_ID AWS_SECRET_ACCESS_KEY nicht in AWS Codebuild-Projektumgebungen vorhanden sind. Speichern Sie diese Variablen nicht als Klartext. Das Speichern dieser Variablen als Klartext bewirkt eine unbeabsichtigte Offenlegung von Daten sowie unberechtigte Zugriffe.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
IR-4(1)	Die Organisation setzt automatisierte Mechanismen ein, um die Bearbeitung von Sicherheitsvorfällen zu unterstützen.	autoscaling-group-elb-healthcheck-erforderlich	Die Elastic Load Balancer (ELB) - Zustandsprüfungen für Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling Scaling-Gruppen unterstützen die Aufrechterhaltung einer angemessenen Kapazität und Verfügbarkeit. Der Load Balancer sendet regelmäßig Pings, versucht Verbindungen herzustellen oder sendet Anfragen, um den Zustand der EC2 Amazon-Instances in einer Gruppe mit auto-scaling zu testen. Wenn eine Instance nicht zurückmeldet, wird der Traffic an eine neue EC2 Amazon-Instance gesendet.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
IR-4(1)	Die Organisation setzt automatisierte Mechanismen ein, um die Bearbeitung von Sicherheitsvorfällen zu unterstützen.	guardduty-enabled-centralized	Amazon GuardDuty kann mithilfe von Threat Intellige nce Feeds helfen, potenzielle Cybersich erheitsereignisse zu überwachen und zu erkennen. Dazu gehören Listen mit bösartigen IPs und maschinellen Lernmethoden, um unerwartete, unbefugte und bösartige Aktivitäten in Ihrer AWS Cloud-Umgebung zu identifiz ieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
IR-4(1)	Die Organisation setzt automatisierte Mechanismen ein, um die Bearbeitung von Sicherheitsvorfällen zu unterstützen.	guardduty-non-archived-findings	Amazon GuardDuty hilft Ihnen dabei, die Auswirkungen eines Vorfalls zu verstehen, indem es die Ergebnisse nach Schweregrad klassifiziert: niedrig, mittel und hoch. Diese Klassifizierungen können Sie zur Festlegung von entsprechenden Strategien und Prioritäten zur Behebung solcher Vorfälle verwenden. Mit dieser Regel können Sie optional daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7) und daysHighSev (Config Default: 1) für nicht archivierte Ergebnisse festlegen, wie es die Richtlinien Ihrer Organisation erfordern.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
IR-4(1)	Die Organisation setzt automatisierte Mechanismen ein, um die Bearbeitung von Sicherheitsvorfällen zu unterstützen.	securityhub-enabled	AWS Security Hub hilft bei der Überwachung von unbefugtem Personal, Verbindungen, Geräten und Software. AWS Security Hub aggregiert, organisiert und priorisiert die Sicherheitswarnungen oder Ergebnisse mehrerer Dienste. AWS Einige dieser Dienste sind Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer und AWS Firewall Manager sowie AWS Partnerlösungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
IR-4(1)	Die Organisation setzt automatisierte Mechanismen ein, um die Bearbeitung von Sicherheitsvorfällen zu unterstützen.	cloudwatch-alarm-action-check	Amazon CloudWatch alarmiert, wenn eine Metrik den Schwellenwert für eine bestimmte Anzahl von Bewertungszeiträumen überschreitet. Der Alarm führt eine oder mehrere Aktionen durch, die vom Wert der Metrik oder des Ausdrucks im Vergleich zu einem Schwellenwert in einer Reihe von Zeiträumen abhängt. Diese Regel erfordert einen Wert für alarmActionRequired (Config Default: True), insufficientDataAction Required (Config Default: True), okActionRequired (Config Default: False). Der tatsächliche Wert muss die Alarmaktionen für Ihre Umgebung widerspiegeln.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
IR-6(1)	Die Organisation setzt automatisierte Mechanismen ein, um die Meldung von Sicherheitsvorfällen zu unterstützen.	guardduty-enabled-centralized	Amazon GuardDuty kann mithilfe von Threat Intellige nce Feeds helfen, potenzielle Cybersich erheitsereignisse zu überwachen und zu erkennen. Dazu gehören Listen mit bösartigen IPs und maschinellen Lernmethoden, um unerwartete, unbefugte und bösartige Aktivitäten in Ihrer AWS Cloud-Umgebung zu identifiz ieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
IR-6(1)	Die Organisation setzt automatisierte Mechanismen ein, um die Meldung von Sicherheitsvorfällen zu unterstützen.	guardduty-non-archived-findings	Amazon GuardDuty hilft Ihnen dabei, die Auswirkungen eines Vorfalls zu verstehen, indem es die Ergebnisse nach Schweregrad klassifiziert: niedrig, mittel und hoch. Diese Klassifizierungen können Sie zur Festlegung von entsprechenden Strategien und Prioritäten zur Behebung solcher Vorfälle verwenden. Mit dieser Regel können Sie optional daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7) und daysHighSev (Config Default: 1) für nicht archivierte Ergebnisse festlegen, wie es die Richtlinien Ihrer Organisation erfordern.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
IR-6(1)	Die Organisation setzt automatisierte Mechanismen ein, um die Meldung von Sicherheitsvorfällen zu unterstützen.	securityhub-enabled	AWS Security Hub hilft bei der Überwachung von unbefugtem Personal, Verbindungen, Geräten und Software. AWS Security Hub aggregiert, organisiert und priorisiert die Sicherheitswarnungen oder Ergebnisse mehrerer Dienste. AWS Einige dieser Dienste sind Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer und AWS Firewall Manager sowie AWS Partnerlösungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
IR-7(1)	Die Organisation setzt automatisierte Mechanismen ein, um die Verfügbarkeit von Informationen und Unterstützung im Zusammenhang mit der Reaktion auf Vorfälle zu erhöhen.	guardduty-enabled-centralized	Amazon GuardDuty kann mithilfe von Threat Intellige nce Feeds helfen, potenzielle Cybersich erheitsereignisse zu überwachen und zu erkennen. Dazu gehören Listen mit bösartigen IPs und maschinellen Lernmethoden, um unerwartete, unbefugte und bösartige Aktivitäten in Ihrer AWS Cloud-Umgebung zu identifiz ieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
IR-7(1)	Die Organisation setzt automatisierte Mechanismen ein, um die Verfügbarkeit von Informationen und Unterstützung im Zusammenhang mit der Reaktion auf Vorfälle zu erhöhen.	guardduty-non-archived-findings	Amazon GuardDuty hilft Ihnen dabei, die Auswirkungen eines Vorfalls zu verstehen, indem es die Ergebnisse nach Schweregrad klassifiziert: niedrig, mittel und hoch. Diese Klassifizierungen können Sie zur Festlegung von entsprechenden Strategien und Prioritäten zur Behebung solcher Vorfälle verwenden. Mit dieser Regel können Sie optional daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7) und daysHighSev (Config Default: 1) für nicht archivierte Ergebnisse festlegen, wie es die Richtlinien Ihrer Organisation erfordern.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
IR-7(1)	Die Organisation setzt automatisierte Mechanismen ein, um die Verfügbarkeit von Informationen und Unterstützung im Zusammenhang mit der Reaktion auf Vorfälle zu erhöhen.	securityhub-enabled	AWS Security Hub hilft bei der Überwachung von unbefugtem Personal, Verbindungen, Geräten und Software. AWS Security Hub aggregiert, organisiert und priorisiert die Sicherheitswarnungen oder Ergebnisse mehrerer Dienste. AWS Einige dieser Dienste sind Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer und AWS Firewall Manager sowie AWS Partnerlösungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
RA-5(1)	Das Unternehmen setzt Tools zum Scannen von Schwachstellen ein, mit denen die zu scannenden Schwachstellen im Informationssystem problemlos aktualisiert werden können. Zusätzliche Empfehlungen: Die zu scannenden Schwachstellen müssen umgehend aktualisiert werden, sobald neue Schwachstellen entdeckt, angekündigt und Scanmethoden entwickelt werden. Dieser Aktualisierungsprozess trägt dazu bei, dass potenzielle Schwachstellen im Informationssystem so schnell wie möglich identifiziert und behoben werden. Verwandte Kontrollen: SI-3, SI-7.	guardduty-enabled-centralized	Amazon GuardDuty kann mithilfe von Threat Intelligence Feeds helfen, potenzielle Cybersicherheitsereignisse zu überwachen und zu erkennen. Dazu gehören Listen mit bösartigen IPs und maschinellen Lernmethoden, um unerwartete, unbefugte und bösartige Aktivitäten in Ihrer AWS Cloud-Umgebung zu identifizieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
RA-5(1)	Das Unternehmen setzt Tools zum Scannen von Schwachstellen ein, mit denen die zu scannenden Schwachstellen im Informationssystem problemlos aktualisiert werden können. Zusätzliche Empfehlungen: Die zu scannenden Schwachstellen müssen umgehend aktualisiert werden, sobald neue Schwachstellen entdeckt, angekündigt und Scanmethoden entwickelt werden. Dieser Aktualisierungsprozess trägt dazu bei, dass potenzielle Schwachstellen im Informationssystem so schnell wie möglich identifiziert und behoben werden. Verwandte Kontrollen: SI-3, SI-7.	guardduty-non-archived-findings	Amazon GuardDuty hilft Ihnen dabei, die Auswirkungen eines Vorfalls zu verstehen, indem es die Ergebnisse nach Schweregrad klassifiziert: niedrig, mittel und hoch. Diese Klassifizierungen können Sie zur Festlegung von entsprechenden Strategien und Prioritäten zur Behebung solcher Vorfälle verwenden. Mit dieser Regel können Sie optional daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7) und daysHighSev (Config Default: 1) für nicht archivierte Ergebnisse festlegen, wie es die Richtlinien Ihrer Organisation erfordern.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
RA-5(1)	Das Unternehmen setzt Tools zum Scannen von Schwachstellen ein, mit denen die zu scannenden Schwachstellen im Informationssystem problemlos aktualisiert werden können. Zusätzliche Empfehlungen: Die zu scannenden Schwachstellen müssen umgehend aktualisiert werden, sobald neue Schwachstellen entdeckt, angekündigt und Scanmethoden entwickelt werden. Dieser Aktualisierungsprozess trägt dazu bei, dass potenzielle Schwachstellen im Informationssystem so schnell wie möglich identifiziert und behoben werden. Verwandte Kontrollen: SI-3, SI-7.	securityhub-enabled	AWS Security Hub hilft bei der Überwachung von unbefugtem Personal, Verbindungen, Geräten und Software. AWS Security Hub aggregiert, organisiert und priorisiert die Sicherheitswarnungen oder Ergebnisse mehrerer Dienste. AWS Einige dieser Dienste sind Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer und AWS Firewall Manager sowie AWS Partnerlösungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
RA-5	Die Organisation: a. Monatliche Scans nach Sicherheitslücken im Informationssystem und in den gehosteten Anwendungen [in Betrieb] system/infrastructure; monthly web applications and databases] and when new vulnerabilities potentially affecting the system/applications werden identifiziert und gemeldet; b. Wendet Tools und Techniken zum Scannen von Schwachstellen an, die die Interoperabilität zwischen den Tools erleichtern und Teile des Schwachstellenmanagements automatisieren, indem für folgende Aktivitäten Standards angewendet werden: 1. Aufzählung von Plattformen, Softwarefehlern und ungeeigneten Konfigurationen;	guardduty-non-archived-findings	Amazon GuardDuty hilft Ihnen dabei, die Auswirkungen eines Vorfalls zu verstehen, indem es die Ergebnisse nach Schweregrad klassifiziert: niedrig, mittel und hoch. Diese Klassifizierungen können Sie zur Festlegung von entsprechenden Strategien und Prioritäten zur Behebung solcher Vorfälle verwenden. Mit dieser Regel können Sie optional daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7) und daysHighSev (Config Default: 1) für nicht archivierte Ergebnisse festlegen, wie es die Richtlinien Ihrer Organisation erfordern.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
	2. Formatierung von Checklisten und Testverfahren; und 3. Messung der Auswirkungen von Schwachstellen; c. Analysiert Scanberichte über Schwachstellen und Ergebnisse von Sicherheitskontrollbewertungen; d. Behebt legitime Schwachstellen: Schwachstellen mit hohem Risiko, die innerhalb von dreißig (30) Tagen ab ihrer Feststellung behoben werden; Schwachstellen mit mäßigem Risiko, die innerhalb von neunzig (90) Tagen ab ihrer Feststellung behoben werden; Sicherheitslücken mit geringem Risiko, die innerhalb von einhundertachtzig (180) Tagen ab ihrer Feststellung behoben werden, gemäß einer Risikobewertung der Organisation; und e. Leitet die Informati		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
	onen aus dem Schwachstellenscan und den Sicherhei tskontrollbewertun gen an [Zuweisung: von der Organisation ernanntes Personal oder definierte Rollen] weiter, um ähnliche Schwachstellen in anderen Informati onssystemen (d. h. Systemschwächen oder -mängel) zu beseitigen.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
RA-5	Die Organisation: a. Sucht nach Sicherheitslücken im Informationssystem und in gehosteten Anwendungen [Zuordnung: Von der Organisation festgelegte Häufigkeit and/or randomly in accordance with organization-defined process] and when new vulnerabilities potentially affecting the system/applications der Identifizierung und Meldung; b. Wendet Tools und Techniken zum Scannen von Schwachstellen an, die die Interoperabilität zwischen den Tools erleichtern und Teile des Schwachstellenmanagements automatisieren, indem für folgende Aktivitäten Standards angewendet werden: 1. Aufzählung von Plattformen, Softwaref	guardduty-enabled-centralized	Amazon GuardDuty kann mithilfe von Threat Intelligence Feeds helfen, potenzielle Cybersicherheitsereignisse zu überwachen und zu erkennen. Dazu gehören Listen mit bösartigen IPs und maschinellen Lernmethoden, um unerwartete, unbefugte und bösartige Aktivitäten in Ihrer AWS Cloud-Umgebung zu identifizieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
	ehlern und ungeeigneten Konfigurationen; 2. Formatierung von Checklisten und Testverfahren; und 3. Messung der Auswirkungen von Schwachstellen; c. Analysiert Scanberichte über Schwachstellen und Ergebnisse von Sicherheitskontrollbewertungen; d. Behebt legitime Schwachstellen [Zuweisung: von der Organisation festgelegte Reaktionszeiten] gemäß einer Risikobewertung der Organisation; und e. Leitet die Informationen aus dem Schwachstellenscan und den Sicherheitskontrollbewertungen an [Zuweisung: von der Organisation ernanntes Personal oder definierte Rollen] weiter, um ähnliche Schwachstellen in anderen Informationssystemen (d. h.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
	Systemschwächen oder -mängel) zu beseitigen.		
SA-3(a)	Die Organisation: a. Verwaltet das Informationssystem mithilfe von [Zuweisung: von der Organisation definierter Lebenszyklus der Systementwicklung], dem Überlegungen zur Informationssicherheit zugrunde liegen.	codebuild-project-envvar-awscred-überprüfen	Stellen Sie sicher, dass die Anmeldeinformationen AWS_ACCESS_KEY_ID AWS_SECRET_ACCESS_KEY nicht in AWS Codebuild-Projektumgebungen vorhanden sind. Speichern Sie diese Variablen nicht als Klartext. Das Speichern dieser Variablen als Klartext bewirkt eine unbeabsichtigte Offenlegung von Daten sowie unberechtigte Zugriffe.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
SA-3(a)	Die Organisation: a. Verwaltet das Informationssystem mithilfe von [Zuweisung: von der Organisation definierter Lebenszyklus der Systementwicklung], dem Überlegungen zur Informationssicherheit zugrunde liegen.	codebuild-project-source-repo-URL-Prüfung	Stellen Sie sicher, dass die URL des Quell-Repositorys GitHub oder des Bitbucket-Quell-Repositorys keine persönlichen Zugriffstoken oder Anmeldeinformationen in Codebuild-Projektumgebungen enthält. AWS Verwende OAuth anstelle von persönlichen Zugriffstoken oder Anmeldedaten die Autorisierung für den Zugriff auf GitHub Bitbucket-Repositorys.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
SA-3(a)	Die Organisation: a. Verwaltet das Informationssystem mithilfe von [Zuweisung: von der Organisation definierter Lebenszyklus der Systementwicklung], dem Überlegungen zur Informationssicherheit zugrunde liegen.	ec2-manager instance-managed-by-systems	Eine Bestandsaufnahme der Softwareplattformen und Anwendungen innerhalb des Unternehmens ist möglich, indem Amazon Elastic Compute Cloud (Amazon EC2) - Instances mit AWS Systems Manager verwaltet werden. Verwenden Sie AWS Systems Manager, um detaillierte Systemkonfigurationen, Betriebssystem-Patch-Levels, Namen und Typ der Dienste, Softwareinstallationen, Anwendungsname, Herausgeber und Version sowie andere Details zu Ihrer Umgebung bereitzustellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
SA-10	Die Organisation verlangt von den Entwicklern des Informationssystems, der Systemkomponente oder des Informationssystemservices: a. Die Durchführung des Konfigurationsmanagements während der Entwicklung, Implementierung und des Betriebs von Systemen, Komponenten oder Services; b. Die Dokumentation, Verwaltung und Kontrolle der Integrität von Änderungen an [Zuweisung: von der Organisation definierte Konfigurationselemente im Rahmen der Konfigurationsverwaltung]; c. Die Implementierung von ausschließlich von der Organisation genehmigten Änderungen am System, der	guardduty-non-archived-findings	Amazon GuardDuty hilft Ihnen dabei, die Auswirkungen eines Vorfalls zu verstehen, indem es die Ergebnisse nach Schweregrad klassifiziert: niedrig, mittel und hoch. Diese Klassifizierungen können Sie zur Festlegung von entsprechenden Strategien und Prioritäten zur Behebung solcher Vorfälle verwenden. Mit dieser Regel können Sie optional daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7) und daysHighSev (Config Default: 1) für nicht archivierte Ergebnisse festlegen, wie es die Richtlinien Ihrer Organisation erfordern.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
	Komponente oder dem Service; d. Die Dokumentation von genehmigten Änderungen am System, der Komponente oder dem Service sowie der potenziellen Auswirkungen solcher Änderungen auf die Sicherheit; und e. Die Überwachung von Sicherheitslücken und deren Behebung innerhalb des Systems, der Komponente oder des Services und die Meldung der Ergebnisse an [Zuweisung: von der Organisation ernanntes Personal].		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
SA-10	Die Organisation verlangt von den Entwicklern des Informationssystems, der Systemkomponente oder des Informationssystemservices: a. Die Durchführung des Konfigurationsmanagements während der Entwicklung, Implementierung und des Betriebs von Systemen, Komponenten oder Services; b. Die Dokumentation, Verwaltung und Kontrolle der Integrität von Änderungen an [Zuweisung: von der Organisation definierte Konfigurationselemente im Rahmen der Konfigurationsverwaltung]; c. Die Implementierung von ausschließlich von der Organisation genehmigten Änderungen am System, der	securityhub-enabled	AWS Security Hub hilft bei der Überwachung von unbefugtem Personal, Verbindungen, Geräten und Software. AWS Security Hub aggregiert, organisiert und priorisiert die Sicherheitswarnungen oder Ergebnisse mehrerer Dienste. AWS Einige dieser Dienste sind Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer und AWS Firewall Manager sowie AWS Partnerlösungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
	Komponente oder dem Service; d. Die Dokumentation von genehmigten Änderungen am System, der Komponente oder dem Service sowie der potenziellen Auswirkungen solcher Änderungen auf die Sicherheit; und e. Die Überwachung von Sicherheitslücken und deren Behebung innerhalb des Systems, der Komponente oder des Services und die Meldung der Ergebnisse an [Zuweisung: von der Organisation ernanntes Personal].		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
SA-10	Die Organisation verlangt von den Entwicklern des Informationssystems, der Systemkomponente oder des Informationssystemservices: a. Die Durchführung des Konfigurationsmanagements während der Entwicklung, Implementierung und des Betriebs von Systemen, Komponenten oder Services; b. Die Dokumentation, Verwaltung und Kontrolle der Integrität von Änderungen an [Zuweisung: von der Organisation definierte Konfigurationselemente im Rahmen der Konfigurationsverwaltung]; c. Die Implementierung von ausschließlich von der Organisation genehmigten Änderungen am System, der	ec2-managed-instance-managed-by-systems	Eine Bestandsaufnahme der Softwareplattformen und Anwendungen innerhalb des Unternehmens ist möglich, indem Amazon Elastic Compute Cloud (Amazon EC2) - Instances mit AWS Systems Manager verwaltet werden. Verwenden Sie AWS Systems Manager, um detaillierte Systemkonfigurationen, Betriebssystem-Patch-Levels, Namen und Typ der Dienste, Softwareinstallationen, Anwendungsname, Herausgeber und Version sowie andere Details zu Ihrer Umgebung bereitzustellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
	Komponente oder dem Service; d. Die Dokumentation von genehmigten Änderungen am System, der Komponente oder dem Service sowie der potenziellen Auswirkungen solcher Änderungen auf die Sicherheit; und e. Die Überwachung von Sicherheitslücken und deren Behebung innerhalb des Systems, der Komponente oder des Services und die Meldung der Ergebnisse an [Zuweisung: von der Organisation ernanntes Personal].		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
SA-10	Die Organisation verlangt von den Entwicklern des Informationssystems, der Systemkomponente oder des Informationssystemservices: a. Die Durchführung des Konfigurationsmanagements während der Entwicklung, Implementierung und des Betriebs von Systemen, Komponenten oder Services; b. Die Dokumentation, Verwaltung und Kontrolle der Integrität von Änderungen an [Zuweisung: von der Organisation definierte Konfigurationselemente im Rahmen der Konfigurationsverwaltung]; c. Die Implementierung von ausschließlich von der Organisation genehmigten Änderungen am System, der	guardduty-enabled-centralized	Amazon GuardDuty kann mithilfe von Threat Intelligence Feeds helfen, potenzielle Cybersicherheitsereignisse zu überwachen und zu erkennen. Dazu gehören Listen mit bösartigen IPs und maschinellen Lernmethoden, um unerwartete, unbefugte und bösartige Aktivitäten in Ihrer AWS Cloud-Umgebung zu identifizieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
	Komponente oder dem Service; d. Die Dokumentation von genehmigten Änderungen am System, der Komponente oder dem Service sowie der potenziellen Auswirkungen solcher Änderungen auf die Sicherheit; und e. Die Überwachung von Sicherheitslücken und deren Behebung innerhalb des Systems, der Komponente oder des Services und die Meldung der Ergebnisse an [Zuweisung: von der Organisation ernanntes Personal].		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
SC-2	Das Informati onssystem trennt Benutzerfunktionen (einschließlich Benutzerschnittste llenservices) von den Verwaltungsfunktio nen des Informati onssystems.	iam-no-inline-policy-überprüfen	Stellen Sie sicher, dass ein Benutzer, eine IAM-Rolle oder eine IAM-Gruppe (AWS Identity and Access Management) nicht über eine Inline-Richtlinie zur Zugriffsk ontrolle auf Systeme und Ressource n verfügt. AWS empfiehlt, verwaltet e Richtlinien anstelle von Inline-Richtlinien zu verwenden. Verwaltete Richtlini en ermöglichen Wiederverwendbarke it, Versionsverwaltung , Rollback und Delegierung der Berechtigungsverwa ltung.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
SC-2	Das Informati onssystem trennt Benutzerfunktionen (einschließlich Benutzerschnittste llenservices) von den Verwaltungsfunktio nen des Informati onssystems.	iam-user-group-mem bership-überprüfen	AWS Identity and Access Managemen t (IAM) kann Ihnen helfen, Zugriffsb erechtigungen und Autorisierungen einzuschränken, indem sichergestellt wird, dass Benutzer Mitglieder mindesten s einer Gruppe sind. Wenn Benutzern mehr Berechtigungen eingeräumt werden, als für die Ausführun g einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringste n Berechtigung und Aufgabentrennung verstoßen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
SC-2	Das Informati onssystem trennt Benutzerfunktionen (einschließlich Benutzerschnittste llenservices) von den Verwaltungsfunktio nen des Informati onssystems.	iam-user-no-policies-überprüfen	Diese Regel stellt sicher, dass AWS Identity and Access Management (IAM) -Richtlinien nur Gruppen oder Rollen zugewiese n werden, um den Zugriff auf Systeme und Ressourcen zu kontrollieren. Die Zuweisung von Berechtig ungen auf Gruppen- oder Rollenebene trägt dazu bei, die Wahrscheinlichkeit zu verringern, dass eine Identität übermäßige Berechtigungen erhält oder beibehält.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
SC-2	Das Informati onssystem trennt Benutzerfunktionen (einschließlich Benutzerschnittste llenservices) von den Verwaltungsfunktio nen des Informati onssystems.	iam-group-has-users-überprüfen	AWS Identity and Access Managemen t (IAM) kann Ihnen helfen, die Prinzipien der geringsten Rechte und der Aufgabent rennung mit Zugriffsb erechtigungen und Autorisierungen zu integrieren, indem sichergestellt wird, dass IAM-Gruppen mindestens einen Benutzer haben. Die Einteilung von Benutzern in Gruppen auf der Grundlage der ihnen zugewiese nen Berechtigungen oder ihrer Funktion ist eine Möglichkeit, das Prinzip der geringste n Berechtigung zu implementieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
SC-2	Das Informationssystem trennt Benutzerfunktionen (einschließlich Benutzerschnittstellenservices) von den Verwaltungsfunktionen des Informationssystems.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) kann Ihnen dabei helfen, die Prinzipien der geringsten Rechte und der Aufgabentrennung in Zugriffsberechtigungen und Autorisierungen zu integrieren und so zu verhindern, dass Richtlinien „Effect“: „Allow“ mit „Action“: „*“ anstelle von „Resource“: „*“ enthalten. Wenn Benutzern mehr Rechte eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und der Aufgabentrennung verstoßen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
SC-4	Das Informati onssystem verhinder t die unbefugte und unbeabsichtigte Übertragung von Informationen aus gemeinsam genutzten Systemressourcen.	dms-replication-not-public	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass auf DMS-Replikationsin stanzen nicht öffentlic h zugegriffen werden kann. DMS-Repli kations-Instances können vertrauli che Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.
SC-4	Das Informati onssystem verhinder t die unbefugte und unbeabsichtigte Übertragung von Informationen aus gemeinsam genutzten Systemressourcen.	ebs-snapshot-public-restorable-überprüfen	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass EBS-Snapshots nicht öffentlich wiederher stellbar sind. EBS-Volume-Snapsho ts können vertrauli che Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
SC-4	Das Informati onssystem verhinder t die unbefugte und unbeabsichtigte Übertragung von Informationen aus gemeinsam genutzten Systemressourcen.	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) Security Groups können bei der Verwaltung des Netzwerkzugriffs helfen, indem sie eine statusbeh aftete Filterung von eingehendem und ausgehendem Netzwerkverkehr zu Ressourcen bereitste llen. AWS Wenn Sie eingehenden (oder entfernten) Datenverk ehr von 0.0.0.0/0 bis Port 22 auf Ihren Ressourcen nicht zulassen, können Sie den Remote-Zugriff einschränken.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
SC-4	Das Informationssystem verhindert die unbefugte und unbeabsichtigte Übertragung von Informationen aus gemeinsam genutzten Systemressourcen.	lambda-function-public-access-verboten	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass AWS Lambda-Funktionen nicht öffentlich zugänglich sind. Der öffentliche Zugriff kann möglicherweise die Verfügbarkeit von Ressourcen beeinträchtigen.
SC-4	Das Informationssystem verhindert die unbefugte und unbeabsichtigte Übertragung von Informationen aus gemeinsam genutzten Systemressourcen.	no-unrestricted-route-to-igw	Stellen Sie sicher, dass EC2 Amazon-Routentabellen keine uneingeschränkten Routen zu einem Internet-Gateway enthalten. Durch das Entfernen oder Beschränken des Internetzugangs für Workloads innerhalb von Amazon VPCs können unbeabsichtigte Zugriffe in Ihrer Umgebung reduziert werden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
SC-4	Das Informati onssystem verhinder t die unbefugte und unbeabsichtigte Übertragung von Informationen aus gemeinsam genutzten Systemressourcen.	rds-instance-public-access-überprüfen	Verwalten Sie den Zugriff auf Ressource n in der AWS Cloud, indem Sie sicherste llen, dass Amazon Relational Database Service (Amazon RDS) -Instance s nicht öffentlic h sind. Amazon-RDS-Datenbank-Instances können vertrauliche Informati onen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
SC-4	Das Informati onssystem verhinder t die unbefugte und unbeabsichtigte Übertragung von Informationen aus gemeinsam genutzten Systemressourcen.	rds-snapshots-public-prohibited	Verwalten Sie den Zugriff auf Ressource n in der AWS Cloud, indem Sie sicherste llen, dass Amazon Relational Database Service (Amazon RDS) -Instance s nicht öffentlic h sind. Amazon-RDS-Datenbank-Instances können vertrauliche Informati onen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
SC-4	Das Informati onssystem verhinder t die unbefugte und unbeabsichtigte Übertragung von Informationen aus gemeinsam genutzten Systemressourcen.	redshift-cluster-public-access-überprüfen	Verwalten Sie den Zugriff auf Ressource n in der AWS Cloud, indem Sie sicherste llen, dass Amazon Redshift Redshift-Cluster nicht öffentlic h sind. Amazon-Re dshift-Cluster können vertrauliche Informati onen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
SC-4	Das Informationssystem verhindert die unbefugte und unbeabsichtigte Übertragung von Informationen aus gemeinsam genutzten Systemressourcen.	restricted-common-ports	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass gemeinsame Ports für Amazon Elastic Compute Cloud (Amazon EC2) -Sicherheitsgruppen eingeschränkt sind. Wenn der Zugriff auf Ports nicht auf vertrauenswürdige Quellen beschränkt wird, kann dies zu Angriffen auf die Verfügbarkeit, Integrität und Vertraulichkeit von Systemen führen. Mit dieser Regel können Sie optional die Parameter blockedPort1–blockedPort5 festlegen (Standardkonfigurationen: 20, 21, 3389, 3306, 4333). Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
SC-4	Das Informati onssystem verhinder t die unbefugte und unbeabsichtigte Übertragung von Informationen aus gemeinsam genutzten Systemressourcen.	s3- -blöcke-periodisch account-level-public-access	Verwalten Sie den Zugriff auf Ressource n in der AWS Cloud, indem Sie sicherste llen, dass Amazon Simple Storage Service (Amazon S3) -Buckets nicht öffentlich zugänglic h sind. Diese Regel trägt dazu bei, sensible Daten vor unbefugten Remote-Benutzern zu schützen, indem sie den öffentlichen Zugriff verhinder t. Mit dieser Regel können Sie optional die Parameter ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) und restrictPublicBuck ets Parameter (Config Default: True) festlegen. Die tatsächlichen Werte müssen den Richtlini

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
			en Ihrer Organisation entsprechen.
SC-4	Das Informati onssystem verhinder t die unbefugte und unbeabsichtigte Übertragung von Informationen aus gemeinsam genutzten Systemressourcen.	s3- verboten bucket-le vel-public-access	Verwalten Sie den Zugriff auf Ressource n in der AWS Cloud, indem Sie sicherste llen, dass Amazon Simple Storage Service (Amazon S3) -Buckets nicht öffentlich zugänglic h sind. Diese Regel trägt dazu bei, sensible Daten vor unbefugten Remote-Benutzern zu schützen, indem sie den öffentlichen Zugriff auf Bucket-Eb ene verhindert.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
SC-4	Das Informati onssystem verhinder t die unbefugte und unbeabsichtigte Übertragung von Informationen aus gemeinsam genutzten Systemressourcen.	s-3 bucket-public-read -prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie nur autorisierten Benutzern, Prozessen und Geräten Zugriff auf Amazon Simple Storage Service (Amazon S3) - Buckets gewähren. Die Verwaltung des Zugriffs sollte mit der Klassifizierung der Daten übereinst immen.
SC-4	Das Informati onssystem verhinder t die unbefugte und unbeabsichtigte Übertragung von Informationen aus gemeinsam genutzten Systemressourcen.	s-3 bucket-public-writ e-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie nur autorisierten Benutzern, Prozessen und Geräten Zugriff auf Amazon Simple Storage Service (Amazon S3) - Buckets gewähren. Die Verwaltung des Zugriffs sollte mit der Klassifizierung der Daten übereinst immen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
SC-4	Das Informati onssystem verhinder t die unbefugte und unbeabsichtigte Übertragung von Informationen aus gemeinsam genutzten Systemressourcen.	sagemaker-notebook -no-direct-Interne tzugang	Verwalten Sie den Zugriff auf Ressource n in der AWS Cloud, indem Sie sicherste llen, dass SageMaker Amazon-Notebooks keinen direkten Internetzugang zulassen. Indem Sie direkten Internetz ugang blockieren, vermeiden Sie, dass unbefugte Benutzer auf sensible Daten zugreifen.
SC-4	Das Informati onssystem verhinder t die unbefugte und unbeabsichtigte Übertragung von Informationen aus gemeinsam genutzten Systemressourcen.	ssm-document-not-p ublic	Stellen Sie sicher, dass AWS Systems Manager (SSM) - Dokumente nicht öffentlich sind, da dies einen unbeabsic htigten Zugriff auf Ihre SSM-Dokum ente ermöglichen kann. Ein öffentlic hes SSM-Dokum ent kann Informati onen über Ihr Konto, Ihre Ressourcen und internen Prozesse preisgeben.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
SC-4	Das Informati onssystem verhinder t die unbefugte und unbeabsichtigte Übertragung von Informationen aus gemeinsam genutzten Systemressourcen.	vpc-default-security-group-geschlossen	Sicherheitsgruppen von Amazon Elastic Compute Cloud (Amazon EC2) können bei der Verwaltung des Netzwerkzugriffs helfen, indem sie eine statusbehaftete Filterung des ein- und ausgehenden Netzwerkverkehrs zu Ressourcen bereitstellen. AWS Die Beschränk ung des gesamten Datenverkehrs auf die Standardsicherheit sgruppe hilft dabei, den Fernzugriff auf Ihre Ressourcen einzuschränken. AWS

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
SC-4	Das Informati onssystem verhinder t die unbefugte und unbeabsichtigte Übertragung von Informationen aus gemeinsam genutzten Systemressourcen.	vpc-sg-open-only-to-authorized-ports	Verwalten Sie den Zugriff auf Ressource n in der AWS Cloud, indem Sie sicherste llen, dass gemeinsam e Ports für Amazon Elastic Compute Cloud (Amazon EC2) -Sicherhe itsgruppen eingeschr ränkt sind. Wenn der Zugriff auf Ports nicht auf vertrauen swürdige Quellen beschränkt wird, kann dies zu Angriffen auf die Verfügbar keit, Integrität und Vertraulichkeit von Systemen führen. Durch die Beschränk ung des Zugriffs auf Ressourcen innerhalb einer Sicherhei tsgruppe aus dem Internet (0.0.0.0/0) kann der Remote-Zugriff auf interne Systeme gesteuert werden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
SC-4	Das Informati onssystem verhinder t die unbefugte und unbeabsichtigte Übertragung von Informationen aus gemeinsam genutzten Systemressourcen.	ec2- volume-inuse-check	Diese Regel stellt sicher, dass Amazon Elastic Block Store-Volumes, die an Amazon Elastic Compute Cloud (Amazon EC2) - Instances angehängt sind, zum Löschen markiert werden, wenn eine Instance beendet wird. Wenn ein Amazon-EB S-Volume nicht gelöscht wird, wenn die Instance, an die es angehängt ist, beendet wird, kann dies gegen das Konzept der geringsten Funktiona lität verstoßen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
SC-5	Das Informationssystem schützt vor den folgenden Arten von Denial-of-Service-Angriffen oder begrenzt deren Auswirkungen: [Zuweisung: von der Organisation definierte Arten von Denial-of-Service-Angriffen oder Verweise auf Quellen für solche Informationen] durch den Einsatz von [Zuweisung: von der Organisation definierte Sicherheitsvorkehrungen].	elb-cross-zone-load-Balancing aktiviert	Aktivieren Sie zonenübergreifendes Load Balancing für Ihre Elastic Load Balancer (ELBs), um eine angemessene Kapazität und Verfügbarkeit aufrechtzuerhalten. Zonenübergreifendes Load Balancing reduziert die Notwendigkeit, die gleiche Anzahl von Instances in jeder aktivierten Availability Zone aufrechtzuerhalten. Es verbessert auch die Fähigkeit Ihrer Anwendung, den Verlust einer oder mehrerer Instances zu bewältigen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
SC-5	Das Informati onssystem schützt vor den folgenden Arten von Denial-of -Service-Angriffen oder begrenzt deren Auswirkungen: [Zuweisung: von der Organisation definiert e Arten von Denial-of-Service-Angriffen oder Verweise auf Quellen für solche Informationen] durch den Einsatz von [Zuweisung: von der Organisation definiert e Sicherheitsvorkehr ungen].	rds-instance-deletion-protection-aktiviert	Stellen Sie sicher, dass Amazon Relational Database Service (Amazon RDS)-Instances den Löschschutz aktiviert haben. Verwenden Sie den Löschschu tz, um zu verhindern, dass Ihre Amazon-RD S-Instances versehent lich oder böswillig gelöscht werden, was zum Verlust der Verfügbarkeit Ihrer Anwendungen führen kann.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
SC-5	Das Informationssystem schützt vor den folgenden Arten von Denial-of-Service-Angriffen oder begrenzt deren Auswirkungen: [Zuweisung: von der Organisation definierte Arten von Denial-of-Service-Angriffen oder Verweise auf Quellen für solche Informationen] durch den Einsatz von [Zuweisung: von der Organisation definierte Sicherheitsvorkehrungen].	autoscaling-group-elb-healthcheck-erforderlich	Die Elastic Load Balancer (ELB) - Zustandsprüfungen für Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling Scaling-Gruppen unterstützen die Aufrechterhaltung einer angemessenen Kapazität und Verfügbarkeit. Der Load Balancer sendet regelmäßig Pings, versucht Verbindungen herzustellen oder sendet Anfragen, um den Zustand der EC2 Amazon-Instances in einer Gruppe mit auto-scaling zu testen. Wenn eine Instance nicht zurückmeldet, wird der Traffic an eine neue EC2 Amazon-Instance gesendet.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
SC-5	Das Informationssystem schützt vor den folgenden Arten von Denial-of-Service-Angriffen oder begrenzt deren Auswirkungen: [Zuweisung: von der Organisation definierte Arten von Denial-of-Service-Angriffen oder Verweise auf Quellen für solche Informationen] durch den Einsatz von [Zuweisung: von der Organisation definierte Sicherheitsvorkehrungen].	dynamodb-autoscaling-enabled	Amazon DynamoDB Auto Scaling verwendet den AWS Application Auto Scaling-Service, um die bereitgestellte Durchsatzkapazität so anzupassen, dass sie automatisch auf tatsächliche Verkehrsmuster reagiert. Auf diese Weise kann eine Tabelle oder ein globaler sekundärer Index die bereitgestellte Lese-/Schreibkapazität erhöhen, um plötzliche Erhöhungen des Datenverkehrs ohne Drosselung zu bewältigen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
SC-5	Das Informationssystem schützt vor den folgenden Arten von Denial-of-Service-Angriffen oder begrenzt deren Auswirkungen: [Zuweisung: von der Organisation definierte Arten von Denial-of-Service-Angriffen oder Verweise auf Quellen für solche Informationen] durch den Einsatz von [Zuweisung: von der Organisation definierte Sicherheitsvorkehrungen].	dynamodb-pitr-enabled	Aktivieren Sie diese Regel, um zu überprüfen, ob die Informationen gesichert wurden. Es verwaltet auch die Backups, indem es sicherstellt, dass die point-in-time Wiederherstellung in Amazon DynamoDB aktiviert ist. Bei der Wiederherstellung werden fortlaufende Backups Ihrer Tabelle für die letzten 35 Tage gespeichert.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
SC-5	Das Informationssystem schützt vor den folgenden Arten von Denial-of-Service-Angriffen oder begrenzt deren Auswirkungen: [Zuweisung: von der Organisation definierte Arten von Denial-of-Service-Angriffen oder Verweise auf Quellen für solche Informationen] durch den Einsatz von [Zuweisung: von der Organisation definierte Sicherheitsvorkehrungen].	ebs-optimized-instance	Eine optimierte Instance im Amazon Elastic Block Store (Amazon EBS) bietet zusätzliche, dedizierte Kapazität für Amazon-EBS-I/O-Vorgänge. Diese Optimierung bietet die beste Leistung für Ihr EBS-Volume, indem Konflikte zwischen Amazon-EBS-I/O und anderem Datenverkehr von Ihrer Instance minimiert werden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
SC-5	Das Informati onssystem schützt vor den folgenden Arten von Denial-of -Service-Angriffen oder begrenzt deren Auswirkungen: [Zuweisung: von der Organisation definiert e Arten von Denial-of-Service-Angriffen oder Verweise auf Quellen für solche Informationen] durch den Einsatz von [Zuweisung: von der Organisation definiert e Sicherheitsvorkehr ungen].	elasticache-redis-cluster-automatic-Backup-Prüfung	Wenn automatische Backups aktiviert sind, ElastiCache erstellt Amazon täglich ein Backup des Clusters. Die Sicherung kann für eine von Ihrer Organisation festgelegte Anzahl von Tagen aufbewahrt werden. Automatische Backups schützen vor Datenverlust. Bei einem Ausfall können Sie einen neuen Cluster erstellen, der Ihre Daten aus dem aktuellen Backup wiederherstellt.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
SC-5	Das Informationssystem schützt vor den folgenden Arten von Denial-of-Service-Angriffen oder begrenzt deren Auswirkungen: [Zuweisung: von der Organisation definierte Arten von Denial-of-Service-Angriffen oder Verweise auf Quellen für solche Informationen] durch den Einsatz von [Zuweisung: von der Organisation definierte Sicherheitsvorkehrungen].	elb-deletion-protection-enabled	Diese Regel sorgt dafür, dass der Löschschutz für Elastic Load Balancing aktiviert ist. Verwenden Sie diese Funktion, um zu verhindern, dass Ihr Load Balancer versehentlich oder böswillig gelöscht wird, was zum Verlust der Verfügbarkeit Ihrer Anwendungen führen kann.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
SC-5	Das Informati onssystem schützt vor den folgenden Arten von Denial-of -Service-Angriffen oder begrenzt deren Auswirkungen: [Zuweisung: von der Organisation definiert e Arten von Denial-of-Service-Angriffen oder Verweise auf Quellen für solche Informationen] durch den Einsatz von [Zuweisung: von der Organisation definiert e Sicherheitsvorkehr ungen].	guardduty-enabled-centralized	Amazon GuardDuty kann mithilfe von Threat Intellige nce Feeds helfen, potenzielle Cybersich erheitsereignisse zu überwachen und zu erkennen. Dazu gehören Listen mit bösartigen IPs und maschinellen Lernmethoden, um unerwartete, unbefugte und bösartige Aktivitäten in Ihrer AWS Cloud-Umgebung zu identifiz ieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
SC-5	Das Informationssystem schützt vor den folgenden Arten von Denial-of-Service-Angriffen oder begrenzt deren Auswirkungen: [Zuweisung: von der Organisation definierte Arten von Denial-of-Service-Angriffen oder Verweise auf Quellen für solche Informationen] durch den Einsatz von [Zuweisung: von der Organisation definierte Sicherheitsvorkehrungen].	rds-multi-az-support	Die Multi-AZ-Unterstützung in Amazon Relational Database Service (Amazon RDS) bietet eine verbesserte Verfügbarkeit und Beständigkeit von Datenbank-Instances. Wenn Sie eine Multi-AZ-Datenbank-Instance bereitstellen, erstellt Amazon RDS automatisch eine primäre Datenbank-Instance und repliziert die Daten synchron auf eine Standby-Instance in einer anderen Availability Zone. Jede Availability Zone läuft auf einer eigenen, physisch getrennten, unabhängigen Infrastruktur und ist auf eine hohe Verfügbarkeit ausgelegt. Im Falle eines Infrastrukturausfalls führt Amazon RDS einen automatis

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
			chen Failover zum Standby-Modus durch, sodass Sie den Datenbankbetrieb wieder aufnehmen können, sobald der Failover abgeschlo ssen ist.
SC-5	Das Informati onssystem schützt vor den folgenden Arten von Denial-of -Service-Angriffen oder begrenzt deren Auswirkungen: [Zuweisung: von der Organisation definiert e Arten von Denial-of-Service-Angriffen oder Verweise auf Quellen für solche Informationen] durch den Einsatz von [Zuweisung: von der Organisation definiert e Sicherheitsvorkehr ungen].	s-3 bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) unterstützt die Aufrechterhaltung einer angemesse nen Kapazität und Verfügbarkeit. CRR ermöglicht das automatische, asynchrone Kopieren von Objekten in Amazon-S3-Buckets, um die Datenverf ügbarkeit sicherzus tellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
SC-5	Das Informationssystem schützt vor den folgenden Arten von Denial-of-Service-Angriffen oder begrenzt deren Auswirkungen: [Zuweisung: von der Organisation definierte Arten von Denial-of-Service-Angriffen oder Verweise auf Quellen für solche Informationen] durch den Einsatz von [Zuweisung: von der Organisation definierte Sicherheitsvorkehrungen].	s-3 bucket-versioning-enabled	Die Versionsverwaltung von Amazon Simple Storage Service (Amazon S3)-Buckets hilft dabei, mehrere Varianten eines Objekts im selben Amazon-S3-Bucket zu speichern. Verwenden Sie die Versionsverwaltung, um sämtliche Versionen aller Objekte in Ihrem Amazon-S3-Bucket zu speichern, abzurufen oder wiederherzustellen. Mit der Versionsverwaltung können Sie Versionen sowohl nach unbeabsichtigten Benutzeraktionen als auch nach Anwendungsfehlern problemlos wiederherstellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
SC-5	Das Informati onssystem schützt vor den folgenden Arten von Denial-of -Service-Angriffen oder begrenzt deren Auswirkungen: [Zuweisung: von der Organisation definiert e Arten von Denial-of-Service-Angriffen oder Verweise auf Quellen für solche Informationen] durch den Einsatz von [Zuweisung: von der Organisation definiert e Sicherheitsvorkehr ungen].	vpc-vpn-2-tunnels-up	Redundante Site-to-Site VPN-Tunne l können implement iert werden, um die Anforderungen an die Ausfallsicherheit zu erfüllen. Es verwendet zwei Tunnel, um die Konnektivität sicherzustellen, falls eine der Site-to-Site VPN-Verbindungen nicht verfügbar ist. Um sich vor einem Verbindungsverlust zu schützen, können Sie für den Fall, dass Ihr Kunden-Gateway nicht verfügbar ist, eine zweite Site-to-S ite VPN-Verbindung zu Ihrer Amazon Virtual Private Cloud (Amazon VPC) und Ihrem Virtual Private Gateway einrichten, indem Sie ein zweites Kunden-Gateway verwenden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
SC-7(3)	Die Organisation begrenzt die Anzahl der externen Netzwerkverbindungen zum Informationssystem.	autoscaling-launch-config-public-ip-deaktiviert	Wenn Sie Ihre Netzwerkschnittstellen mit einer öffentlichen IP-Adresse konfigurieren, sind die diesen Netzwerkschnittstellen zugehörigen Ressourcen über das Internet erreichbar. EC2 Ressourcen sollten nicht öffentlich zugänglich sein, da dies einen unbeabsichtigten Zugriff auf Ihre Anwendungen oder Server ermöglichen kann.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
SC-7(3)	Die Organisation begrenzt die Anzahl der externen Netzwerkverbindungen zum Informationssystem.	ec2- instances-in-vpc	Stellen Sie Amazon Elastic Compute Cloud (Amazon EC2) -Instances innerhalb einer Amazon Virtual Private Cloud (Amazon VPC) bereit, um eine sichere Kommunikation zwischen einer Instance und anderen Services innerhalb der Amazon VPC zu ermöglichen, ohne dass ein Internet-Gateway, ein NAT-Gerät oder eine VPN-Verbindung erforderlich ist. Der gesamte Datenverkehr bleibt sicher in der AWS Cloud. Domains, die sich innerhalb einer VPC befinden, verfügen aufgrund ihrer logischen Isolierung im Vergleich zu Domains mit öffentlichen Endpunkten über eine zusätzliche Sicherheitsebene. Weisen Sie EC2

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
			Amazon-Instances einer Amazon-VPC zu, um den Zugriff ordnungsgemäß zu verwalten.
SC-7(3)	Die Organisation begrenzt die Anzahl der externen Netzwerkverbindungen zum Informationssystem.	ssm-document-not-public	Stellen Sie sicher, dass AWS Systems Manager (SSM) - Dokumente nicht öffentlich sind, da dies einen unbeabsichtigten Zugriff auf Ihre SSM-Dokumente ermöglichen kann. Ein öffentliches SSM-Dokument kann Informationen über Ihr Konto, Ihre Ressourcen und internen Prozesse preisgeben.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
SC-7(3)	Die Organisation begrenzt die Anzahl der externen Netzwerkverbindungen zum Informationssystem.	dms-replication-not-public	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass auf DMS-Replikationsinstanzen nicht öffentlich zugegriffen werden kann. DMS-Replikations-Instances können vertrauliche Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.
SC-7(3)	Die Organisation begrenzt die Anzahl der externen Netzwerkverbindungen zum Informationssystem.	ebs-snapshot-public-restorable-überprüfen	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass EBS-Snapshots nicht öffentlich wiederherstellbar sind. EBS-Volume-Snapshots können vertrauliche Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
SC-7(3)	Die Organisation begrenzt die Anzahl der externen Netzwerkverbindungen zum Informationssystem.	ec-2 instance-no-public-ip	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon Elastic Compute Cloud (Amazon EC2) - Instances nicht öffentlich zugänglich sind. EC2 Amazon-Instances können vertrauliche Informationen enthalten, und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
SC-7(3)	Die Organisation begrenzt die Anzahl der externen Netzwerkverbindungen zum Informationssystem.	elasticsearch-in-vpc-only	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass sich Amazon OpenSearch OpenSearch Service (Service) - Domains innerhalb einer Amazon Virtual Private Cloud (Amazon VPC) befinden. Eine OpenSearch Service-Domain innerhalb einer Amazon VPC ermöglicht die sichere Kommunikation zwischen OpenSearch Service und anderen Services innerhalb der Amazon VPC, ohne dass ein Internet-Gateway, ein NAT-Gerät oder eine VPN-Verbindung erforderlich ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
SC-7(3)	Die Organisation begrenzt die Anzahl der externen Netzwerkverbindungen zum Informationssystem.	emr-master-no-public-ip	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon EMR-Cluster-Masterknoten nicht öffentlich zugänglich sind. Amazon-EMR-Cluster-Hauptknoten können vertrauliche Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
SC-7(3)	Die Organisat ion begrenzt die Anzahl der externen Netzwerkverbindung en zum Informati onssystem.	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) Security Groups können bei der Verwaltung des Netzwerkzugriffs helfen, indem sie eine statusbeh aftete Filterung von eingehendem und ausgehendem Netzwerkverkehr zu Ressourcen bereitste llen. AWS Wenn Sie eingehenden (oder entfernten) Datenverk ehr von 0.0.0.0/0 bis Port 22 auf Ihren Ressourcen nicht zulassen, können Sie den Remote-Zugriff einschränken.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
SC-7(3)	Die Organisation begrenzt die Anzahl der externen Netzwerkverbindungen zum Informationssystem.	lambda-function-public-access-verboten	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass AWS Lambda-Funktionen nicht öffentlich zugänglich sind. Der öffentliche Zugriff kann möglicherweise die Verfügbarkeit von Ressourcen beeinträchtigen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
SC-7(3)	Die Organisation begrenzt die Anzahl der externen Netzwerkverbindungen zum Informationssystem.	lambda-inside-vpc	Stellen Sie AWS Lambda-Funktionen in einer Amazon Virtual Private Cloud (Amazon VPC) bereit, um eine sichere Kommunikation zwischen einer Funktion und anderen Diensten innerhalb der Amazon VPC zu gewährleisten. Bei dieser Konfiguration sind kein Internet-Gateway, kein NAT-Gerät und keine VPN-Verbindung erforderlich. Der gesamte Datenverkehr bleibt sicher in der Cloud. AWS Domains, die sich innerhalb einer VPC befinden, verfügen aufgrund ihrer logischen Isolierung im Vergleich zu Domains mit öffentlichen Endpunkten über eine zusätzliche Sicherheitsebene. Um den Zugriff ordnungsgemäß zu verwalten,

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
			sollten AWS Lambda-Funktionen einer VPC zugewiesen werden.
SC-7(3)	Die Organisation begrenzt die Anzahl der externen Netzwerkverbindungen zum Informationssystem.	rds-instance-public-access-überprüfen	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Relational Database Service (Amazon RDS) -Instances nicht öffentlich sind. Amazon-RDS-Datenbank-Instances können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
SC-7(3)	Die Organisation begrenzt die Anzahl der externen Netzwerkverbindungen zum Informationssystem.	rds-snapshots-public-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Relational Database Service (Amazon RDS) -Instances nicht öffentlich sind. Amazon-RDS-Datenbank-Instances können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
SC-7(3)	Die Organisation begrenzt die Anzahl der externen Netzwerkverbindungen zum Informationssystem.	redshift-cluster-public-access-überprüfen	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Redshift Redshift-Cluster nicht öffentlich sind. Amazon-Redshift-Cluster können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
SC-7(3)	Die Organisation begrenzt die Anzahl der externen Netzwerkverbindungen zum Informationssystem.	restricted-common-ports	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass gemeinsame Ports für Amazon Elastic Compute Cloud (Amazon EC2) -Sicherheitsgruppen eingeschränkt sind. Wenn der Zugriff auf Ports nicht auf vertrauenswürdige Quellen beschränkt wird, kann dies zu Angriffen auf die Verfügbarkeit, Integrität und Vertraulichkeit von Systemen führen. Mit dieser Regel können Sie optional die Parameter blockedPort1–blockedPort5 festlegen (Standardkonfigurationen: 20, 21, 3389, 3306, 4333). Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
SC-7(3)	Die Organisation begrenzt die Anzahl der externen Netzwerkverbindungen zum Informationssystem.	s3- account-level-public-access -Block-periodisch	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Simple Storage Service (Amazon S3) -Buckets nicht öffentlich zugänglich sind. Diese Regel trägt dazu bei, sensible Daten vor unbefugten Remote-Benutzern zu schützen, indem sie den öffentlichen Zugriff verhindert. Mit dieser Regel können Sie optional die Parameter ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) und restrictPublicBuckets Parameter (Config Default: True) festlegen. Die tatsächlichen Werte müssen den Richtlini

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
			en Ihrer Organisation entsprechen.
SC-7(3)	Die Organisat ion begrenzt die Anzahl der externen Netzwerkverbindung en zum Informati onssystem.	s3 bucket-level-public-access - verboten	Verwalten Sie den Zugriff auf Ressource n in der AWS Cloud, indem Sie sicherste llen, dass Amazon Simple Storage Service (Amazon S3) -Buckets nicht öffentlich zugänglic h sind. Diese Regel trägt dazu bei, sensible Daten vor unbefugten Remote-Benutzern zu schützen, indem sie den öffentlichen Zugriff auf Bucket-Eb ene verhindert.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
SC-7(3)	Die Organisation begrenzt die Anzahl der externen Netzwerkverbindungen zum Informationssystem.	s-3 bucket-public-read-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie nur autorisierten Benutzern, Prozessen und Geräten Zugriff auf Amazon Simple Storage Service (Amazon S3) - Buckets gewähren. Die Verwaltung des Zugriffs sollte mit der Klassifizierung der Daten übereinstimmen.
SC-7(3)	Die Organisation begrenzt die Anzahl der externen Netzwerkverbindungen zum Informationssystem.	s3- bucket-public-write-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie nur autorisierten Benutzern, Prozessen und Geräten Zugriff auf Amazon Simple Storage Service (Amazon S3) - Buckets gewähren. Die Verwaltung des Zugriffs sollte mit der Klassifizierung der Daten übereinstimmen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
SC-7(3)	Die Organisation begrenzt die Anzahl der externen Netzwerkverbindungen zum Informationssystem.	sagemaker-notebook-no-direct-Internetzugang	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass SageMaker Amazon-Notebooks keinen direkten Internetzugang zulassen. Indem Sie direkten Internetzugang blockieren, vermeiden Sie, dass unbefugte Benutzer auf sensible Daten zugreifen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
SC-7(3)	Die Organisation begrenzt die Anzahl der externen Netzwerkverbindungen zum Informationssystem.	subnet-auto-assign-public-ip-deaktiviert	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon Virtual Private Cloud (VPC) -Subnetzen nicht automatisch eine öffentliche IP-Adresse zugewiesen wird. Amazon Elastic Compute Cloud (EC2) -Instances, die in Subnetzen gestartet werden, in denen dieses Attribut aktiviert ist, haben ihrer primären Netzwerkschnittstelle eine öffentliche IP-Adresse zugewiesen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
SC-7(3)	Die Organisation begrenzt die Anzahl der externen Netzwerkverbindungen zum Informationssystem.	vpc-default-security-group-geschlossen	Sicherheitsgruppen von Amazon Elastic Compute Cloud (Amazon EC2) können bei der Verwaltung des Netzwerkzugriffs helfen, indem sie eine statusbehaftete Filterung des ein- und ausgehenden Netzwerkverkehrs zu Ressourcen bereitstellen. AWS Die Beschränkung des gesamten Datenverkehrs auf die Standardsicherheitsgruppe hilft dabei, den Fernzugriff auf Ihre Ressourcen einzuschränken. AWS

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
SC-7(3)	Die Organisation begrenzt die Anzahl der externen Netzwerkverbindungen zum Informationssystem.	vpc-sg-open-only-to-authorized-ports	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass gemeinsame Ports für Amazon Elastic Compute Cloud (Amazon EC2) -Sicherheitsgruppen eingeschränkt sind. Wenn der Zugriff auf Ports nicht auf vertrauenswürdige Quellen beschränkt wird, kann dies zu Angriffen auf die Verfügbarkeit, Integrität und Vertraulichkeit von Systemen führen. Durch die Beschränkung des Zugriffs auf Ressourcen innerhalb einer Sicherheitsgruppe aus dem Internet (0.0.0.0/0) kann der Remote-Zugriff auf interne Systeme gesteuert werden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
SC-7(4)	Die Organisation: (a) Implementiert eine verwaltete Schnittstelle für jeden externen Telekommunikationsdienst; (b) legt eine Verkehrsflussrichtlinie für jede verwaltete Schnittstelle fest; (c) schützt die Vertraulichkeit und Integrität der Informationen, die über jede Schnittstelle übertragen werden; (d) dokumentiert jede Ausnahme von der Verkehrsflussrichtlinie mit unterstützendem mission/business need and duration of that need; and (e) Reviews exceptions to the traffic flow policy [Assignment: organization-defined frequency] and removes exceptions that are no longer supported by an explicit mission/business Bedarf. Zusätzliche Empfehlungen:	rds-snapshots-public-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Relational Database Service (Amazon RDS) -Instances nicht öffentlich sind. Amazon-RDS-Datenbank-Instances können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
	Verwandte Kontrolle: SC-8.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
SC-7(4)	Die Organisation: (a) Implementiert eine verwaltete Schnittstelle für jeden externen Telekommunikationsdienst; (b) legt eine Verkehrsflussrichtlinie für jede verwaltete Schnittstelle fest; (c) schützt die Vertraulichkeit und Integrität der Informationen, die über jede Schnittstelle übertragen werden; (d) dokumentiert jede Ausnahme von der Verkehrsflussrichtlinie mit mission/business need and duration of that need; and (e) Reviews exceptions to the traffic flow policy [Assignment: organization-defined frequency] and removes exceptions that are no longer supported by an explicit mission/business unterstützendem Bedarf. Zusätzliche Empfehlungen:	rds-snapshot-encrypted	Stellen Sie sicher, dass die Verschlüsselung für Ihre Amazon Relational Database Service (Amazon RDS)-Snapshots aktiviert ist. Da sensible Daten auch im Ruhezustand vorhanden sein können, sollten Sie die Verschlüsselung im Ruhezustand aktivieren, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
	Verwandte Kontrolle: SC-8.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
SC-7(4)	Die Organisation: (a) Implementiert eine verwaltete Schnittstelle für jeden externen Telekommunikationsdienst; (b) legt eine Verkehrsflussrichtlinie für jede verwaltete Schnittstelle fest; (c) schützt die Vertraulichkeit und Integrität der Informationen, die über jede Schnittstelle übertragen werden; (d) dokumentiert jede Ausnahme von der Verkehrsflussrichtlinie mit unterstützendem mission/business need and duration of that need; and (e) Reviews exceptions to the traffic flow policy [Assignment: organization-defined frequency] and removes exceptions that are no longer supported by an explicit mission/business Bedarf. Zusätzliche Empfehlungen:	rds-storage-encrypted	Zum Schutz von Daten im Ruhezustand müssen Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon Relational Database Service (Amazon RDS)-Instances aktiviert ist. Um eventuell vorhandene sensible Daten im Ruhezustand in Amazon-RDS-Instances zu schützen, muss die Verschlüsselung von Daten im Ruhezustand aktiviert sein.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
	Verwandte Kontrolle: SC-8.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
SC-7(4)	Die Organisation: (a) Implementiert eine verwaltete Schnittstelle für jeden externen Telekommunikationsdienst; (b) legt eine Verkehrsflussrichtlinie für jede verwaltete Schnittstelle fest; (c) schützt die Vertraulichkeit und Integrität der Informationen, die über jede Schnittstelle übertragen werden; (d) dokumentiert jede Ausnahme von der Verkehrsflussrichtlinie mit unterstützendem mission/business need and duration of that need; and (e) Reviews exceptions to the traffic flow policy [Assignment: organization-defined frequency] and removes exceptions that are no longer supported by an explicit mission/business Bedarf. Zusätzliche Empfehlungen:	vpc-default-security-group-geschlossen	Sicherheitsgruppen von Amazon Elastic Compute Cloud (Amazon EC2) können bei der Verwaltung des Netzwerkzugriffs helfen, indem sie eine statusbehaftete Filterung des ein- und ausgehenden Netzwerkverkehrs zu Ressourcen bereitstellen. AWS Die Beschränkung des gesamten Datenverkehrs auf die Standardsicherheitsgruppe hilft dabei, den Fernzugriff auf Ihre Ressourcen einzuschränken. AWS

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
	Verwandte Kontrolle: SC-8.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
SC-7(4)	Die Organisation: (a) Implementiert eine verwaltete Schnittstelle für jeden externen Telekommunikationsdienst; (b) legt eine Verkehrsflussrichtlinie für jede verwaltete Schnittstelle fest; (c) schützt die Vertraulichkeit und Integrität der Informationen, die über jede Schnittstelle übertragen werden; (d) dokumentiert jede Ausnahme von der Verkehrsflussrichtlinie mit unterstützendem Bedarf. mission/business need and duration of that need; and (e) Reviews exceptions to the traffic flow policy [Assignment: organization-defined frequency] and removes exceptions that are no longer supported by an explicit mission/business Zusätzliche Empfehlungen:	vpc-flow-logs-enabled	VPC-Flow-Protokolle erfassen detaillierte Informationsdatensätze über den IP-Datenverkehr, der zu und von Netzwerkschnittstellen in Ihrer Amazon Virtual Private Cloud (Amazon VPC) fließt. Standardmäßig enthalten Flow-Protokolldatensätze Werte für die verschiedenen Komponenten des IP-Flows, einschließlich Quelle, Ziel und Protokoll.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
	Verwandte Kontrolle: SC-8.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
SC-7(4)	Die Organisation: (a) Implementiert eine verwaltete Schnittstelle für jeden externen Telekommunikationsdienst; (b) legt eine Verkehrsflussrichtlinie für jede verwaltete Schnittstelle fest; (c) schützt die Vertraulichkeit und Integrität der Informationen, die über jede Schnittstelle übertragen werden; (d) dokumentiert jede Ausnahme von der Verkehrsflussrichtlinie mit unterstützendem mission/business need and duration of that need; and (e) Reviews exceptions to the traffic flow policy [Assignment: organization-defined frequency] and removes exceptions that are no longer supported by an explicit mission/business Bedarf. Zusätzliche Empfehlungen:	redshift-cluster-kms-enabled	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass die Verschlüsselung mit AWS Key Management Service (AWS KMS) für Ihren Amazon Redshift Redshift-Cluster aktiviert ist. Um eventuell vorhandene sensible Daten im Ruhezustand in Redshift-Clustern zu schützen, muss die Verschlüsselung von Daten im Ruhezustand aktiviert sein.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
	Verwandte Kontrolle: SC-8.		
SC-7(5)	Das Informationssystem lehnt Netzwerkverkehr an verwalteten Schnittstellen standardmäßig ab und lässt Netzwerkverkehr ausnahmsweise zu (d. h. alles verweigern, ausnahmsweise zulassen). Zusätzliche Empfehlungen: Diese Verbesserung der Kontrolle wirkt sich auf eingehenden und ausgehenden Netzwerkverkehr aus. Eine Richtlinie, die den gesamten permit-by-exception Netzwerkverkehr ablehnt, stellt sicher, dass nur Verbindungen zugelassen werden, die unbedingt erforderlich und genehmigt sind.	vpc-sg-open-only-to-authorized-ports	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass gemeinsame Ports für Amazon Elastic Compute Cloud (Amazon EC2) -Sicherheitsgruppen eingeschränkt sind. Wenn der Zugriff auf Ports nicht auf vertrauenswürdige Quellen beschränkt wird, kann dies zu Angriffen auf die Verfügbarkeit, Integrität und Vertraulichkeit von Systemen führen. Durch die Beschränkung des Zugriffs auf Ressourcen innerhalb einer Sicherheitsgruppe aus dem Internet (0.0.0.0/0) kann der Remote-Zugriff auf interne Systeme gesteuert werden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
SC-7	Das Informati onssystem: a. Überwacht und kontrolliert die Kommunikation an der Außengrenze des Systems und an wichtigen internen Grenzen innerhalb des Systems; b. Implementiert Subnetze für öffentlic h zugängliche Systemkomponenten, die [Auswahl: physisch; logisch] von internen Organisat ionsnetzen getrennt sind; und c. Stellt eine Verbindung zu externen Netzwerke n oder Informati onssystemen nur über verwaltete Schnittstellen her, die aus Grenzschu tzgeräten bestehen, die gemäß einer Sicherheitsarchite ktur der Organisation angeordnet sind.	alb-waf-enabled	Stellen Sie sicher, dass AWS WAF auf Elastic Load Balancers (ELB) aktiviert ist, um Webanwendungen zu schützen. Eine WAF trägt zum Schutz Ihrer Webanwend ungen oder APIs vor gängigen Web-Explo its bei. Diese Web-Exploits können sich auf die Verfügbar keit auswirken, die Sicherheit gefährden oder übermäßige Ressourcen in Ihrer Umgebung verbrauch en.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
SC-7	Das Informati onssystem: a. Überwacht und kontrolliert die Kommunikation an der Außengrenze des Systems und an wichtigen internen Grenzen innerhalb des Systems; b. Implementiert Subnetze für öffentlic h zugängliche Systemkomponenten, die [Auswahl: physisch; logisch] von internen Organisat ionsnetzen getrennt sind; und c. Stellt eine Verbindung zu externen Netzwerke n oder Informati onssystemen nur über verwaltete Schnittstellen her, die aus Grenzschu tzgeräten bestehen, die gemäß einer Sicherheitsarchite ktur der Organisation angeordnet sind.	elasticsearch-node -to-node-Verschlüs selungsprüfung	Stellen Sie sicher, dass die node-to-node Verschlüs selung für Amazon OpenSearch Service aktiviert ist. Node-to-nodeVerschlüsselung ermöglicht die TLS 1.2-Verschlüsselun g für die gesamte Kommunikation innerhalb der Amazon Virtual Private Cloud (Amazon VPC). Um eventuell vorhanden e sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
SC-7	Das Informati onssystem: a. Überwacht und kontrolliert die Kommunikation an der Außengrenze des Systems und an wichtigen internen Grenzen innerhalb des Systems; b. Implementiert Subnetze für öffentlic h zugängliche Systemkomponenten, die [Auswahl: physisch; logisch] von internen Organisat ionsnetzen getrennt sind; und c. Stellt eine Verbindung zu externen Netzwerke n oder Informati onssystemen nur über verwaltete Schnittstellen her, die aus Grenzschu tzgeräten bestehen, die gemäß einer Sicherheitsarchite ktur der Organisation angeordnet sind.	elb-tls-https-listeners-nur	Stellen Sie sicher, dass Ihre Elastic Load Balancer (ELBs) mit SSL- oder HTTPS-Listenern konfiguriert sind. Um eventuell vorhanden e sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
SC-7	Das Informati onssystem: a. Überwacht und kontrolliert die Kommunikation an der Außengrenze des Systems und an wichtigen internen Grenzen innerhalb des Systems; b. Implementiert Subnetze für öffentlic h zugängliche Systemkomponenten, die [Auswahl: physisch; logisch] von internen Organisat ionsnetzen getrennt sind; und c. Stellt eine Verbindung zu externen Netzwerke n oder Informati onssystemen nur über verwaltete Schnittstellen her, die aus Grenzschu tzgeräten bestehen, die gemäß einer Sicherheitsarchite ktur der Organisation angeordnet sind.	ec-2 instances-in-vpc	Stellen Sie Amazon Elastic Compute Cloud (Amazon EC2) -Instances innerhalb einer Amazon Virtual Private Cloud (Amazon VPC) bereit, um eine sichere Kommunika tion zwischen einer Instance und anderen Services innerhalb der Amazon VPC zu ermöglichen, ohne dass ein Internet-Gateway, ein NAT-Gerät oder eine VPN-Verbindung erforderlich ist. Der gesamte Datenverk ehr bleibt sicher in der AWS Cloud. Domains, die sich innerhalb einer VPC befinden, verfügen aufgrund ihrer logischen Isolierun g im Vergleich zu Domains mit öffentlic hen Endpunkten über eine zusätzlic he Sicherheitsebene. Weisen Sie EC2

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
			Amazon-Instances einer Amazon-VPC zu, um den Zugriff ordnungsgemäß zu verwalten.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
SC-7	Das Informationssystem: a. Überwacht und kontrolliert die Kommunikation an der Außengrenze des Systems und an wichtigen internen Grenzen innerhalb des Systems; b. Implementiert Subnetze für öffentlich zugängliche Systemkomponenten, die [Auswahl: physisch; logisch] von internen Organisationsnetzen getrennt sind; und c. Stellt eine Verbindung zu externen Netzwerken oder Informationssystemen nur über verwaltete Schnittstellen her, die aus Grenzschutzgeräten bestehen, die gemäß einer Sicherheitsarchitektur der Organisation angeordnet sind.	wafv2-logging-enabled	Um Ihnen bei der Protokollierung und Überwachung in Ihrer Umgebung zu helfen, aktivieren Sie die AWS WAF (V2) -Protokollierung im regionalen und globalen Web. ACLs AWS Die WAF-Protokollierung bietet detaillierte Informationen über den Datenverkehr, der von Ihrer Web-ACL analysiert wird. In den Protokollen werden die Uhrzeit aufgezeichnet, zu der die AWS WAF die Anfrage von Ihrer AWS Ressource erhalten hat, Informationen zu der Anfrage und eine Aktion für die Regel, der jede Anfrage entsprach.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
SC-7	Das Informati onssystem: a. Überwacht und kontrolliert die Kommunikation an der Außengrenze des Systems und an wichtigen internen Grenzen innerhalb des Systems; b. Implementiert Subnetze für öffentlic h zugängliche Systemkomponenten, die [Auswahl: physisch; logisch] von internen Organisat ionsnetzen getrennt sind; und c. Stellt eine Verbindung zu externen Netzwerke n oder Informati onssystemen nur über verwaltete Schnittstellen her, die aus Grenzschu tzgeräten bestehen, die gemäß einer Sicherheitsarchite ktur der Organisation angeordnet sind.	alb-http-to-https-Umleitungsprüfung	Um Daten während der Übertragung zu schützen, stellen Sie sicher, dass Ihr Application Load Balancer unverschl üsselte HTTP-Anfr agen automatisch an HTTPS umleitet. Um eventuell vorhanden e sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
SC-7	Das Informati onssystem: a. Überwacht und kontrolliert die Kommunikation an der Außengrenze des Systems und an wichtigen internen Grenzen innerhalb des Systems; b. Implementiert Subnetze für öffentlic h zugängliche Systemkomponenten, die [Auswahl: physisch; logisch] von internen Organisat ionsnetzen getrennt sind; und c. Stellt eine Verbindung zu externen Netzwerke n oder Informati onssystemen nur über verwaltete Schnittstellen her, die aus Grenzschu tzgeräten bestehen, die gemäß einer Sicherheitsarchite ktur der Organisation angeordnet sind.	dms-replication-not-public	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass auf DMS-Replikationsin stanzen nicht öffentlic h zugegriffen werden kann. DMS-Repli kations-Instances können vertrauli che Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
SC-7	Das Informati onssystem: a. Überwacht und kontrolliert die Kommunikation an der Außengrenze des Systems und an wichtigen internen Grenzen innerhalb des Systems; b. Implementiert Subnetze für öffentlic h zugängliche Systemkomponenten, die [Auswahl: physisch; logisch] von internen Organisat ionsnetzen getrennt sind; und c. Stellt eine Verbindung zu externen Netzwerke n oder Informati onssystemen nur über verwaltete Schnittstellen her, die aus Grenzschu tzgeräten bestehen, die gemäß einer Sicherheitsarchite ktur der Organisation angeordnet sind.	ebs-snapshot-public-restorable-überprüfen	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass EBS-Snapshots nicht öffentlich wiederher stellbar sind. EBS-Volume-Snapsho ts können vertrauli che Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
SC-7	Das Informati onssystem: a. Überwacht und kontrolliert die Kommunikation an der Außengrenze des Systems und an wichtigen internen Grenzen innerhalb des Systems; b. Implementiert Subnetze für öffentlic h zugängliche Systemkomponenten, die [Auswahl: physisch; logisch] von internen Organisat ionsnetzen getrennt sind; und c. Stellt eine Verbindung zu externen Netzwerke n oder Informati onssystemen nur über verwaltete Schnittstellen her, die aus Grenzschu tzgeräten bestehen, die gemäß einer Sicherheitsarchite ktur der Organisation angeordnet sind.	ec-2 instance-no-public-ip	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon Elastic Compute Cloud (Amazon EC2) - Instances nicht öffentlich zugänglich sind. EC2 Amazon-Instances können vertrauliche Informati onen enthalten, und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
SC-7	Das Informationssystem: a. Überwacht und kontrolliert die Kommunikation an der Außengrenze des Systems und an wichtigen internen Grenzen innerhalb des Systems; b. Implementiert Subnetze für öffentlich zugängliche Systemkomponenten, die [Auswahl: physisch; logisch] von internen Organisationsnetzen getrennt sind; und c. Stellt eine Verbindung zu externen Netzwerken oder Informationssystemen nur über verwaltete Schnittstellen her, die aus Grenzschutzgeräten bestehen, die gemäß einer Sicherheitsarchitektur der Organisation angeordnet sind.	elasticsearch-in-vpc-only	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass sich Amazon OpenSearch OpenSearch Service (Service) - Domains innerhalb einer Amazon Virtual Private Cloud (Amazon VPC) befinden. Eine OpenSearch Service-Domain innerhalb einer Amazon VPC ermöglicht die sichere Kommunikation zwischen OpenSearch Service und anderen Services innerhalb der Amazon VPC, ohne dass ein Internet-Gateway, ein NAT-Gerät oder eine VPN-Verbindung erforderlich ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
SC-7	Das Informationssystem: a. Überwacht und kontrolliert die Kommunikation an der Außengrenze des Systems und an wichtigen internen Grenzen innerhalb des Systems; b. Implementiert Subnetze für öffentlich zugängliche Systemkomponenten, die [Auswahl: physisch; logisch] von internen Organisationsnetzen getrennt sind; und c. Stellt eine Verbindung zu externen Netzwerken oder Informationssystemen nur über verwaltete Schnittstellen her, die aus Grenzschutzgeräten bestehen, die gemäß einer Sicherheitsarchitektur der Organisation angeordnet sind.	emr-master-no-public-ip	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon EMR-Cluster-Masterknoten nicht öffentlich zugänglich sind. Amazon-EMR-Cluster-Hauptknoten können vertrauliche Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
SC-7	Das Informati onssystem: a. Überwacht und kontrolliert die Kommunikation an der Außengrenze des Systems und an wichtigen internen Grenzen innerhalb des Systems; b. Implementiert Subnetze für öffentlic h zugängliche Systemkomponenten, die [Auswahl: physisch; logisch] von internen Organisat ionsnetzen getrennt sind; und c. Stellt eine Verbindung zu externen Netzwerke n oder Informati onssystemen nur über verwaltete Schnittstellen her, die aus Grenzschu tzgeräten bestehen, die gemäß einer Sicherheitsarchite ktur der Organisation angeordnet sind.	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) Security Groups können bei der Verwaltung des Netzwerkzugriffs helfen, indem sie eine statusbeh aftete Filterung von eingehendem und ausgehendem Netzwerkverkehr zu Ressourcen bereitste llen. AWS Wenn Sie eingehenden (oder entfernten) Datenverk ehr von 0.0.0.0/0 bis Port 22 auf Ihren Ressourcen nicht zulassen, können Sie den Remote-Zugriff einschränken.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
SC-7	Das Informationssystem: a. Überwacht und kontrolliert die Kommunikation an der Außengrenze des Systems und an wichtigen internen Grenzen innerhalb des Systems; b. Implementiert Subnetze für öffentlich zugängliche Systemkomponenten, die [Auswahl: physisch; logisch] von internen Organisationsnetzen getrennt sind; und c. Stellt eine Verbindung zu externen Netzwerken oder Informationssystemen nur über verwaltete Schnittstellen her, die aus Grenzschutzgeräten bestehen, die gemäß einer Sicherheitsarchitektur der Organisation angeordnet sind.	lambda-function-public-access-verboten	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass AWS Lambda-Funktionen nicht öffentlich zugänglich sind. Der öffentliche Zugriff kann möglicherweise die Verfügbarkeit von Ressourcen beeinträchtigen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
SC-7	Das Informati onssystem: a. Überwacht und kontrolliert die Kommunikation an der Außengrenze des Systems und an wichtigen internen Grenzen innerhalb des Systems; b. Implementiert Subnetze für öffentlic h zugängliche Systemkomponenten, die [Auswahl: physisch; logisch] von internen Organisat ionsnetzen getrennt sind; und c. Stellt eine Verbindung zu externen Netzwerke n oder Informati onssystemen nur über verwaltete Schnittstellen her, die aus Grenzschu tzgeräten bestehen, die gemäß einer Sicherheitsarchite ktur der Organisation angeordnet sind.	lambda-inside-vpc	Stellen Sie AWS Lambda-Funktionen in einer Amazon Virtual Private Cloud (Amazon VPC) bereit, um eine sichere Kommunika tion zwischen einer Funktion und anderen Diensten innerhalb der Amazon VPC zu gewährleisten. Bei dieser Konfiguration sind kein Internet-Gateway, kein NAT-Gerät und keine VPN-Verbindung erforderlich. Der gesamte Datenverk ehr bleibt sicher in der Cloud. AWS Domains, die sich innerhalb einer VPC befinden, verfügen aufgrund ihrer logischen Isolierun g im Vergleich zu Domains mit öffentlic hen Endpunkten über eine zusätzliche Sicherheitsebene. Um den Zugriff ordnungsg emäß zu verwalten,

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
			sollten AWS Lambda-Funktionen einer VPC zugewiesen werden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
SC-7	Das Informationssystem: a. Überwacht und kontrolliert die Kommunikation an der Außengrenze des Systems und an wichtigen internen Grenzen innerhalb des Systems; b. Implementiert Subnetze für öffentlich zugängliche Systemkomponenten, die [Auswahl: physisch; logisch] von internen Organisationsnetzen getrennt sind; und c. Stellt eine Verbindung zu externen Netzwerken oder Informationssystemen nur über verwaltete Schnittstellen her, die aus Grenzschutzgeräten bestehen, die gemäß einer Sicherheitsarchitektur der Organisation angeordnet sind.	rds-instance-public-access-überprüfen	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Relational Database Service (Amazon RDS) -Instances nicht öffentlich sind. Amazon-RDS-Datenbank-Instances können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
SC-7	Das Informationssystem: a. Überwacht und kontrolliert die Kommunikation an der Außengrenze des Systems und an wichtigen internen Grenzen innerhalb des Systems; b. Implementiert Subnetze für öffentlich zugängliche Systemkomponenten, die [Auswahl: physisch; logisch] von internen Organisationsnetzen getrennt sind; und c. Stellt eine Verbindung zu externen Netzwerken oder Informationssystemen nur über verwaltete Schnittstellen her, die aus Grenzschutzgeräten bestehen, die gemäß einer Sicherheitsarchitektur der Organisation angeordnet sind.	rds-snapshots-public-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Relational Database Service (Amazon RDS) -Instances nicht öffentlich sind. Amazon-RDS-Datenbank-Instances können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
SC-7	Das Informationssystem: a. Überwacht und kontrolliert die Kommunikation an der Außengrenze des Systems und an wichtigen internen Grenzen innerhalb des Systems; b. Implementiert Subnetze für öffentlich zugängliche Systemkomponenten, die [Auswahl: physisch; logisch] von internen Organisationsnetzen getrennt sind; und c. Stellt eine Verbindung zu externen Netzwerken oder Informationssystemen nur über verwaltete Schnittstellen her, die aus Grenzschutzgeräten bestehen, die gemäß einer Sicherheitsarchitektur der Organisation angeordnet sind.	redshift-cluster-public-access-überprüfen	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Redshift Redshift-Cluster nicht öffentlich sind. Amazon-Redshift-Cluster können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
SC-7	Das Informati onssystem: a. Überwacht und kontrolliert die Kommunikation an der Außengrenze des Systems und an wichtigen internen Grenzen innerhalb des Systems; b. Implementiert Subnetze für öffentlic h zugängliche Systemkomponenten, die [Auswahl: physisch; logisch] von internen Organisat ionsnetzen getrennt sind; und c. Stellt eine Verbindung zu externen Netzwerke n oder Informati onssystemen nur über verwaltete Schnittstellen her, die aus Grenzschu tzgeräten bestehen, die gemäß einer Sicherheitsarchite ktur der Organisation angeordnet sind.	redshift-require-tls-ssl	Stellen Sie sicher, dass Ihre Amazon-Redshift-Cluster eine TLS/SSL-Verschlüss elung erfordern, um eine Verbindun g zu SQL-Clients herzustellen. Um eventuell vorhanden e sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
SC-7	Das Informationssystem: a. Überwacht und kontrolliert die Kommunikation an der Außengrenze des Systems und an wichtigen internen Grenzen innerhalb des Systems; b. Implementiert Subnetze für öffentlich zugängliche Systemkomponenten, die [Auswahl: physisch; logisch] von internen Organisationsnetzen getrennt sind; und c. Stellt eine Verbindung zu externen Netzwerken oder Informationssystemen nur über verwaltete Schnittstellen her, die aus Grenzschutzgeräten bestehen, die gemäß einer Sicherheitsarchitektur der Organisation angeordnet sind.	restricted-common-ports	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass gemeinsame Ports für Amazon Elastic Compute Cloud (Amazon EC2) -Sicherheitsgruppen eingeschränkt sind. Wenn der Zugriff auf Ports nicht auf vertrauenswürdige Quellen beschränkt wird, kann dies zu Angriffen auf die Verfügbarkeit, Integrität und Vertraulichkeit von Systemen führen. Mit dieser Regel können Sie optional die Parameter blockedPort1–blockedPort5 festlegen (Standardkonfigurationen: 20, 21, 3389, 3306, 4333). Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
SC-7	Das Informationssystem: a. Überwacht und kontrolliert die Kommunikation an der Außengrenze des Systems und an wichtigen internen Grenzen innerhalb des Systems; b. Implementiert Subnetze für öffentlich zugängliche Systemkomponenten, die [Auswahl: physisch; logisch] von internen Organisationsnetzen getrennt sind; und c. Stellt eine Verbindung zu externen Netzwerken oder Informationssystemen nur über verwaltete Schnittstellen her, die aus Grenzschutzgeräten bestehen, die gemäß einer Sicherheitsarchitektur der Organisation angeordnet sind.	s3- account-level-public-access -Block-periodisch	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Simple Storage Service (Amazon S3) -Buckets nicht öffentlich zugänglich sind. Diese Regel trägt dazu bei, sensible Daten vor unbefugten Remote-Benutzern zu schützen, indem sie den öffentlichen Zugriff verhindert. Mit dieser Regel können Sie optional die Parameter ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) und restrictPublicBuckets Parameter (Config Default: True) festlegen. Die tatsächlichen Werte müssen den Richtlini

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
			en Ihrer Organisation entsprechen.
SC-7	Das Informati onssystem: a. Überwacht und kontrolliert die Kommunikation an der Außengrenze des Systems und an wichtigen internen Grenzen innerhalb des Systems; b. Implementiert Subnetze für öffentlic h zugängliche Systemkomponenten, die [Auswahl: physisch; logisch] von internen Organisat ionsnetzen getrennt sind; und c. Stellt eine Verbindung zu externen Netzwerke n oder Informati onssystemen nur über verwaltete Schnittstellen her, die aus Grenzschu tzgeräten bestehen, die gemäß einer Sicherheitsarchite ktur der Organisation angeordnet sind.	s3 bucket-level-public-access - verboten	Verwalten Sie den Zugriff auf Ressource n in der AWS Cloud, indem Sie sicherste llen, dass Amazon Simple Storage Service (Amazon S3) -Buckets nicht öffentlich zugänglic h sind. Diese Regel trägt dazu bei, sensible Daten vor unbefugten Remote-Benutzern zu schützen, indem sie den öffentlichen Zugriff auf Bucket-Eb ene verhindert.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
SC-7	Das Informati onssystem: a. Überwacht und kontrolliert die Kommunikation an der Außengrenze des Systems und an wichtigen internen Grenzen innerhalb des Systems; b. Implementiert Subnetze für öffentlic h zugängliche Systemkomponenten, die [Auswahl: physisch; logisch] von internen Organisat ionsnetzen getrennt sind; und c. Stellt eine Verbindung zu externen Netzwerke n oder Informati onssystemen nur über verwaltete Schnittstellen her, die aus Grenzschu tzgeräten bestehen, die gemäß einer Sicherheitsarchite ktur der Organisation angeordnet sind.	s-3 bucket-public-read -prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie nur autorisierten Benutzern, Prozessen und Geräten Zugriff auf Amazon Simple Storage Service (Amazon S3) - Buckets gewähren. Die Verwaltung des Zugriffs sollte mit der Klassifizierung der Daten übereinst immen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
SC-7	Das Informati onssystem: a. Überwacht und kontrolliert die Kommunikation an der Außengrenze des Systems und an wichtigen internen Grenzen innerhalb des Systems; b. Implementiert Subnetze für öffentlic h zugängliche Systemkomponenten, die [Auswahl: physisch; logisch] von internen Organisat ionsnetzen getrennt sind; und c. Stellt eine Verbindung zu externen Netzwerke n oder Informati onssystemen nur über verwaltete Schnittstellen her, die aus Grenzschu tzgeräten bestehen, die gemäß einer Sicherheitsarchite ktur der Organisation angeordnet sind.	s3- bucket-public-writ e-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie nur autorisierten Benutzern, Prozessen und Geräten Zugriff auf Amazon Simple Storage Service (Amazon S3) - Buckets gewähren. Die Verwaltung des Zugriffs sollte mit der Klassifizierung der Daten übereinst immen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
SC-7	Das Informati onssystem: a. Überwacht und kontrolliert die Kommunikation an der Außengrenze des Systems und an wichtigen internen Grenzen innerhalb des Systems; b. Implementiert Subnetze für öffentlic h zugängliche Systemkomponenten, die [Auswahl: physisch; logisch] von internen Organisat ionsnetzen getrennt sind; und c. Stellt eine Verbindung zu externen Netzwerke n oder Informati onssystemen nur über verwaltete Schnittstellen her, die aus Grenzschu tzgeräten bestehen, die gemäß einer Sicherheitsarchite ktur der Organisation angeordnet sind.	s3- bucket-ssl-request s-only	Um Daten während der Übertragung zu schützen, stellen Sie sicher, dass Ihre Amazon Simple Storage Service (Amazon S3)-Bucke ts Anfragen zur Verwendung von Secure Socket Layer (SSL)-Buc kets erfordern. Um eventuell vorhanden e sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
SC-7	Das Informationssystem: a. Überwacht und kontrolliert die Kommunikation an der Außengrenze des Systems und an wichtigen internen Grenzen innerhalb des Systems; b. Implementiert Subnetze für öffentlich zugängliche Systemkomponenten, die [Auswahl: physisch; logisch] von internen Organisationsnetzen getrennt sind; und c. Stellt eine Verbindung zu externen Netzwerken oder Informationssystemen nur über verwaltete Schnittstellen her, die aus Grenzschutzgeräten bestehen, die gemäß einer Sicherheitsarchitektur der Organisation angeordnet sind.	sagemaker-notebook-no-direct-Internetzugang	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass SageMaker Amazon-Notebooks keinen direkten Internetzugang zulassen. Indem Sie direkten Internetzugang blockieren, vermeiden Sie, dass unbefugte Benutzer auf sensible Daten zugreifen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
SC-7	Das Informationssystem: a. Überwacht und kontrolliert die Kommunikation an der Außengrenze des Systems und an wichtigen internen Grenzen innerhalb des Systems; b. Implementiert Subnetze für öffentlich zugängliche Systemkomponenten, die [Auswahl: physisch; logisch] von internen Organisationsnetzen getrennt sind; und c. Stellt eine Verbindung zu externen Netzwerken oder Informationssystemen nur über verwaltete Schnittstellen her, die aus Grenzschutzgeräten bestehen, die gemäß einer Sicherheitsarchitektur der Organisation angeordnet sind.	subnet-auto-assign-public-ip-deaktiviert	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon Virtual Private Cloud (VPC) -Subnetzen nicht automatisch eine öffentliche IP-Adresse zugewiesen wird. Amazon Elastic Compute Cloud (EC2) -Instances, die in Subnetzen gestartet werden, in denen dieses Attribut aktiviert ist, haben ihrer primären Netzwerkschnittstelle eine öffentliche IP-Adresse zugewiesen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
SC-7	Das Informati onssystem: a. Überwacht und kontrolliert die Kommunikation an der Außengrenze des Systems und an wichtigen internen Grenzen innerhalb des Systems; b. Implementiert Subnetze für öffentlic h zugängliche Systemkomponenten, die [Auswahl: physisch; logisch] von internen Organisat ionsnetzen getrennt sind; und c. Stellt eine Verbindung zu externen Netzwerke n oder Informati onssystemen nur über verwaltete Schnittstellen her, die aus Grenzschu tzgeräten bestehen, die gemäß einer Sicherheitsarchite ktur der Organisation angeordnet sind.	vpc-default-security-group-geschlossen	Sicherheitsgruppen von Amazon Elastic Compute Cloud (Amazon EC2) können bei der Verwaltung des Netzwerkzugriffs helfen, indem sie eine statusbehaftete Filterung des ein- und ausgehenden Netzwerkverkehrs zu Ressourcen bereitstellen. AWS Die Beschränk ung des gesamten Datenverkehrs auf die Standardsicherheit sgruppe hilft dabei, den Fernzugriff auf Ihre Ressourcen einzuschränken. AWS

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
SC-7	Das Informati onssystem: a. Überwacht und kontrolliert die Kommunikation an der Außengrenze des Systems und an wichtigen internen Grenzen innerhalb des Systems; b. Implementiert Subnetze für öffentlic h zugängliche Systemkomponenten, die [Auswahl: physisch; logisch] von internen Organisat ionsnetzen getrennt sind; und c. Stellt eine Verbindung zu externen Netzwerke n oder Informati onssystemen nur über verwaltete Schnittstellen her, die aus Grenzschu tzgeräten bestehen, die gemäß einer Sicherheitsarchite ktur der Organisation angeordnet sind.	vpc-sg-open-only-to-authorized-ports	Verwalten Sie den Zugriff auf Ressource n in der AWS Cloud, indem Sie sicherste llen, dass gemeinsam e Ports für Amazon Elastic Compute Cloud (Amazon EC2) -Sicherhe itsgruppen eingeschr änkt sind. Wenn der Zugriff auf Ports nicht auf vertrauen swürdige Quellen beschränkt wird, kann dies zu Angriffen auf die Verfügbar keit, Integrität und Vertraulichkeit von Systemen führen. Durch die Beschränk ung des Zugriffs auf Ressourcen innerhalb einer Sicherhei tsgruppe aus dem Internet (0.0.0.0/0) kann der Remote-Zugriff auf interne Systeme gesteuert werden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
SC-8(1)	Das Informationssystem setzt kryptographische Mechanismen ein, um während der Übertragung [Auswahl (eine oder mehrere Optionen): eine unbefugte Offenlegung von Informationen zu verhindern; Änderungen an Informationen zu erkennen], sofern sie nicht anderweitig durch [Zuweisung: von der Organisation definierte alternative physische Schutzmaßnahmen] geschützt sind.	elasticsearch-node-to-node-Verschlüsselungsprüfung	Stellen Sie sicher, dass die node-to-node Verschlüsselung für Amazon OpenSearch Service aktiviert ist. Node-to-nodeVerschlüsselung ermöglicht die TLS 1.2-Verschlüsselung für die gesamte Kommunikation innerhalb der Amazon Virtual Private Cloud (Amazon VPC). Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
SC-8(1)	Das Informationssystem setzt kryptographische Mechanismen ein, um während der Übertragung [Auswahl (eine oder mehrere Optionen): eine unbefugte Offenlegung von Informationen zu verhindern; Änderungen an Informationen zu erkennen], sofern sie nicht anderweitig durch [Zuweisung: von der Organisation definierte alternative physische Schutzmaßnahmen] geschützt sind.	elbv-2 acm-certificate-required	Zum Schutz von eventuell vorhandenen sensiblen Daten sowie von Daten während der Übertragung muss die Verschlüsselung für Ihr Elastic Load Balancing aktiviert sein. Verwenden Sie AWS Certificate Manager, um öffentliche und private SSL/TLS-Zertifikate mit AWS Diensten und internen Ressourcen zu verwalten, bereitzustellen und bereitzustellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
SC-8(1)	Das Informationssystem setzt kryptographische Mechanismen ein, um während der Übertragung [Auswahl (eine oder mehrere Optionen): eine unbefugte Offenlegung von Informationen zu verhindern; Änderungen an Informationen zu erkennen], sofern sie nicht anderweitig durch [Zuweisung: von der Organisation definierte alternative physische Schutzmaßnahmen] geschützt sind.	elb-tls-https-listeners-nur	Stellen Sie sicher, dass Ihre Elastic Load Balancer (ELBs) mit SSL- oder HTTPS-Listenern konfiguriert sind. Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
SC-8(1)	Das Informationssystem setzt kryptographische Mechanismen ein, um während der Übertragung [Auswahl (eine oder mehrere Optionen): eine unbefugte Offenlegung von Informationen zu verhindern; Änderungen an Informationen zu erkennen], sofern sie nicht anderweitig durch [Zuweisung: von der Organisation definierte alternative physische Schutzmaßnahmen] geschützt sind.	alb-http-to-https-Umleitungsprüfung	Um Daten während der Übertragung zu schützen, stellen Sie sicher, dass Ihr Application Load Balancer unverschlüsselte HTTP-Anfragen automatisch an HTTPS umleitet. Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
SC-8(1)	Das Informati onssystem setzt kryptographische Mechanismen ein, um während der Übertragung [Auswahl (eine oder mehrere Optionen): eine unbefugte Offenlegu ng von Informati onen zu verhinder n; Änderungen an Informationen zu erkennen], sofern sie nicht anderweit ig durch [Zuweisung: von der Organisation definierte alternative physische Schutzmaß nahmen] geschützt sind.	api-gw-ssl-enabled	Stellen Sie sicher, dass die REST-API-Stufen von Amazon API Gateway mit SSL-Zertifikaten konfiguri ert sind, damit Backend-Systeme überprüfen können, ob Anforderungen von API Gateway stammen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
SC-8(1)	Das Informationssystem setzt kryptographische Mechanismen ein, um während der Übertragung [Auswahl (eine oder mehrere Optionen): eine unbefugte Offenlegung von Informationen zu verhindern; Änderungen an Informationen zu erkennen], sofern sie nicht anderweitig durch [Zuweisung: von der Organisation definierte alternative physische Schutzmaßnahmen] geschützt sind.	redshift-require-tls-ssl	Stellen Sie sicher, dass Ihre Amazon-Redshift-Cluster eine TLS/SSL-Verschlüsselung erfordern, um eine Verbindung zu SQL-Clients herzustellen. Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
SC-8(1)	Das Informationssystem setzt kryptographische Mechanismen ein, um während der Übertragung [Auswahl (eine oder mehrere Optionen): eine unbefugte Offenlegung von Informationen zu verhindern; Änderungen an Informationen zu erkennen], sofern sie nicht anderweitig durch [Zuweisung: von der Organisation definierte alternative physische Schutzmaßnahmen] geschützt sind.	s3- bucket-ssl-requests-only	Um Daten während der Übertragung zu schützen, stellen Sie sicher, dass Ihre Amazon Simple Storage Service (Amazon S3)-Buckets Anfragen zur Verwendung von Secure Socket Layer (SSL)-Buckets erfordern. Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
SC-8	Das Informati onssystem schützt die Vertraulichkeit UND Integrität der übermittelten Informati onen.	elasticsearch-node -to-node-Verschlüs selungsprüfung	Stellen Sie sicher, dass die node-to-node Verschlüs selung für Amazon OpenSearch Service aktiviert ist. Node-to-nodeVerschlüsselung ermöglicht die TLS 1.2-Verschlüsselun g für die gesamte Kommunikation innerhalb der Amazon Virtual Private Cloud (Amazon VPC). Um eventuell vorhanden e sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
SC-8	Das Informationssystem schützt die Vertraulichkeit UND Integrität der übermittelten Informationen.	elbv-2 acm-certificate-required	Zum Schutz von eventuell vorhandenen sensiblen Daten sowie von Daten während der Übertragung muss die Verschlüsselung für Ihr Elastic Load Balancing aktiviert sein. Verwenden Sie AWS Certificate Manager, um öffentliche und private SSL/TLS-Zertifikate mit AWS Diensten und internen Ressourcen zu verwalten, bereitzustellen und bereitzustellen.
SC-8	Das Informationssystem schützt die Vertraulichkeit UND Integrität der übermittelten Informationen.	elb-tls-https-listeners-nur	Stellen Sie sicher, dass Ihre Elastic Load Balancer (ELBs) mit SSL- oder HTTPS-Listenern konfiguriert sind. Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
SC-8	Das Informationssystem schützt die Vertraulichkeit UND Integrität der übermittelten Informationen.	alb-http-to-https-Umleitungsprüfung	Um Daten während der Übertragung zu schützen, stellen Sie sicher, dass Ihr Application Load Balancer unverschlüsselte HTTP-Anfragen automatisch an HTTPS umleitet. Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.
SC-8	Das Informationssystem schützt die Vertraulichkeit UND Integrität der übermittelten Informationen.	api-gw-ssl-enabled	Stellen Sie sicher, dass die REST-API-Stufen von Amazon API Gateway mit SSL-Zertifikaten konfiguriert sind, damit Backend-Systeme überprüfen können, ob Anforderungen von API Gateway stammen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
SC-8	Das Informati onssystem schützt die Vertraulichkeit UND Integrität der übermittelten Informati onen.	redshift-require-tls-ssl	Stellen Sie sicher, dass Ihre Amazon-Redshift-Cluster eine TLS/SSL-Verschlüss elung erfordern, um eine Verbindun g zu SQL-Clients herzustellen. Um eventuell vorhanden e sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.
SC-8	Das Informati onssystem schützt die Vertraulichkeit UND Integrität der übermittelten Informati onen.	s3- bucket-ssl-request s-only	Um Daten während der Übertragung zu schützen, stellen Sie sicher, dass Ihre Amazon Simple Storage Service (Amazon S3)-Bucke ts Anfragen zur Verwendung von Secure Socket Layer (SSL)-Buc kets erfordern. Um eventuell vorhanden e sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
SC-12	Die Organisation erstellt und verwaltet kryptografische Schlüssel für die erforderliche Kryptografie, die innerhalb des Informationssystems eingesetzt wird, in Übereinstimmung mit [Zuordnung: von der Organisation festgelegte Anforderungen für die Erzeugung, Verteilung, Speicherung, den Zugriff und die Vernichtung von Schlüsseln].	cmk-backing-key-rotation-aktiviert	Aktivieren Sie die Schlüsselrotation, um sicherzustellen, dass Schlüssel rotiert werden, nachdem sie das Ende ihrer Krypto-Periode erreicht haben.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
SC-12	Die Organisation erstellt und verwaltet kryptografische Schlüssel für die erforderliche Kryptografie, die innerhalb des Informationssystems eingesetzt wird, in Übereinstimmung mit [Zuordnung: von der Organisation festgelegte Anforderungen für die Erzeugung, Verteilung, Speicherung, den Zugriff und die Vernichtung von Schlüsseln].	acm-certificate-expiration-check	Stellen Sie sicher, dass die Netzwerkintegrität geschützt ist, indem Sie sicherstellen, dass X509-Zertifikate von AWS ACM ausgestellt werden. Diese Zertifikate müssen gültig und dürfen nicht abgelaufen sein. Für diese Regel ist ein Wert für erforderlich daysToExpiration (Wert für bewährte AWS Grundregeln für Sicherheit: 90). Der tatsächliche Wert muss den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
SC-12	Die Organisation erstellt und verwaltet kryptografische Schlüssel für die erforderliche Kryptografie, die innerhalb des Informationssystems eingesetzt wird, in Übereinstimmung mit [Zuordnung: von der Organisation festgelegte Anforderungen für die Erzeugung, Verteilung, Speicherung, den Zugriff und die Vernichtung von Schlüsseln].	kms-cmk-not-scheduled-zum Löschen	Um Daten im Ruhezustand zu schützen, sollten Sie sicherstellen, dass die für den Kunden erforderlichen Masterschlüssel (CMKs) nicht im AWS Key Management Service (AWS KMS) gelöscht werden. Da Schlüssel manchmal gelöscht werden müssen, können Sie mit dieser Regel alle zu löschenden Schlüssel überprüfen, falls ein Schlüssel versehentlich zur Löschung vorgemerkt wurde.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
SC-13	Das Informationssystem setzt FIPS-validierte oder NSA-zugelassene Kryptographie in Übereinstimmung mit den geltenden Bundesgesetzen, Executive Orders, Direktiven, Richtlinien, Vorschriften und Standards ein.	kms-cmk-not-scheduled-zum Löschen	Um Daten im Ruhezustand zu schützen, sollten Sie sicherstellen, dass die für den Kunden erforderlichen Masterschlüssel (CMKs) nicht im AWS Key Management Service (AWS KMS) gelöscht werden. Da Schlüssel manchmal gelöscht werden müssen, können Sie mit dieser Regel alle zu löschenden Schlüssel überprüfen, falls ein Schlüssel versehentlich zur Löschung vorgemerkt wurde.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
SC-13	Das Informati onssystem setzt FIPS-validierte oder NSA-zugelassene Kryptographie in Übereinstimmung mit den geltenden Bundesgesetzen, Executive Orders, Direktiven, Richtlini en, Vorschriften und Standards ein.	s3- default-encryption -kms	Stellen Sie sicher, dass die Verschlüs selung für Ihre Amazon Simple Storage Service (Amazon S3)-Bucke ts aktiviert ist. Um eventuell vorhanden e sensible Daten im Ruhezustand in einem Amazon-S3-Bucket zu schützen, muss die Verschlüsselung aktiviert sein.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
SC-13	Das Informationssystem setzt FIPS-validierte oder NSA-zugelassene Kryptographie in Übereinstimmung mit den geltenden Bundesgesetzen, Executive Orders, Direktiven, Richtlinien, Vorschriften und Standards ein.	sagemaker-endpoint-configuration-kms-key-konfiguriert	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass die Verschlüsselung mit dem AWS Key Management Service (AWS KMS) für Ihren Endpunkt aktiviert ist. SageMaker Da sensible Daten auf dem SageMaker Endgerät gespeichert werden können, sollten Sie die Verschlüsselung im Ruhezustand aktivieren, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
SC-13	Das Informati onssystem setzt FIPS-validierte oder NSA-zugelassene Kryptographie in Übereinstimmung mit den geltenden Bundesgesetzen, Executive Orders, Direktiven, Richtlini en, Vorschriften und Standards ein.	sagemaker-notebook -instance-kms-schl üsselkonfiguriert	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass die Verschlüsselung mit dem AWS Key Management Service (AWS KMS) für Ihr Notebook aktiviert ist. SageMaker Da vertrauliche Daten im SageMaker Notebook gespeichert werden können, sollten Sie die Verschlüsselung im Ruhezustand aktivieren, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
SC-13	Das Informationssystem setzt FIPS-validierte oder NSA-zugelassene Kryptographie in Übereinstimmung mit den geltenden Bundesgesetzen, Executive Orders, Direktiven, Richtlinien, Vorschriften und Standards ein.	sns-encrypted-kms	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass Ihre Amazon Simple Notification Service (Amazon SNS) -Themen mit dem AWS Key Management Service (AWS KMS) verschlüsselt werden müssen. Um eventuell vorhandene sensible Daten im Ruhezustand in veröffentlichten Nachrichten zu schützen, muss die Verschlüsselung von Daten im Ruhezustand aktiviert sein.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
SC-13	Das Informati onssystem setzt FIPS-validierte oder NSA-zugelassene Kryptographie in Übereinstimmung mit den geltenden Bundesgesetzen, Executive Orders, Direktiven, Richtlini en, Vorschriften und Standards ein.	redshift-cluster-kms-enabled	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass die Verschlüs selung mit AWS Key Management Service (AWS KMS) für Ihren Amazon Redshift Redshift-Cluster aktiviert ist. Um eventuell vorhanden e sensible Daten im Ruhezustand in Redshift-Clustern zu schützen, muss die Verschlüsselung von Daten im Ruhezusta nd aktiviert sein.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
SC-23	Das Informati onssystem schützt die Authentizität der Kommunikationssitz ungen.	elasticsearch-node -to-node-Verschlüs selungsprüfung	Stellen Sie sicher, dass die node-to-node Verschlüs selung für Amazon OpenSearch Service aktiviert ist. Node-to-nodeVerschlüsselung ermöglicht die TLS 1.2-Verschlüsselun g für die gesamte Kommunikation innerhalb der Amazon Virtual Private Cloud (Amazon VPC). Um eventuell vorhanden e sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.
SC-23	Das Informati onssystem schützt die Authentizität der Kommunikationssitz ungen.	elb-tls-https-listeners-nur	Stellen Sie sicher, dass Ihre Elastic Load Balancer (ELBs) mit SSL- oder HTTPS-Listenern konfiguriert sind. Um eventuell vorhanden e sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
SC-23	Das Informati onssystem schützt die Authentizität der Kommunikationssitz ungen.	alb-http-to-https-Umleitungsprüfung	Um Daten während der Übertragung zu schützen, stellen Sie sicher, dass Ihr Application Load Balancer unverschl üsselte HTTP-Anfr agen automatisch an HTTPS umleitet. Um eventuell vorhanden e sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.
SC-23	Das Informati onssystem schützt die Authentizität der Kommunikationssitz ungen.	api-gw-ssl-enabled	Stellen Sie sicher, dass die REST-API-Stufen von Amazon API Gateway mit SSL-Zertifikaten konfiguri ert sind, damit Backend-Systeme überprüfen können, ob Anforderungen von API Gateway stammen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
SC-23	Das Informati onssystem schützt die Authentizität der Kommunikationssitz ungen.	redshift-require-tls-ssl	Stellen Sie sicher, dass Ihre Amazon-Redshift-Cluster eine TLS/SSL-Verschlüss elung erfordern, um eine Verbindun g zu SQL-Clients herzustellen. Um eventuell vorhanden e sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.
SC-23	Das Informati onssystem schützt die Authentizität der Kommunikationssitz ungen.	s3- bucket-ssl-request s-only	Um Daten während der Übertragung zu schützen, stellen Sie sicher, dass Ihre Amazon Simple Storage Service (Amazon S3)-Bucke ts Anfragen zur Verwendung von Secure Socket Layer (SSL)-Buc kets erfordern. Um eventuell vorhanden e sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
SC-28	Das Informationssystem schützt die Vertraulichkeit UND Integrität von [Zuweisung: von der Organisation definierte Informationen im Ruhestand].	s-3 bucket-default-lock-enabled	Stellen Sie sicher, dass für Ihren Amazon Simple Storage Service (Amazon S3)-Bucket standardmäßig eine Sperre aktiviert ist. Zum Schutz eventuell vorhandener sensibler Daten in S3-Buckets müssen Sie Objektsperren für Daten im Ruhezustand erzwingen.
SC-28	Das Informationssystem schützt die Vertraulichkeit UND Integrität von [Zuweisung: von der Organisation definierte Informationen im Ruhestand].	s-3 default-encryption-kms	Stellen Sie sicher, dass die Verschlüsselung für Ihre Amazon Simple Storage Service (Amazon S3)-Buckets aktiviert ist. Um eventuell vorhandene sensible Daten im Ruhezustand in einem Amazon-S3-Bucket zu schützen, muss die Verschlüsselung aktiviert sein.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
SC-28	Das Informati onssystem schützt die Vertraulichkeit UND Integrität von [Zuweisung: von der Organisation definiert e Informationen im Ruhestand].	sagemaker-notebook -instance-kms-key- konfiguriert	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass die Verschlüsselung mit dem AWS Key Management Service (AWS KMS) für Ihr Notebook aktiviert ist. SageMaker Da vertrauliche Daten im SageMaker Notebook gespeichert werden können, sollten Sie die Verschlüsselung im Ruhezustand aktivieren, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
SC-28	Das Informati onssystem schützt die Vertraulichkeit UND Integrität von [Zuweisung: von der Organisation definiert e Informationen im Ruhestand].	sns-encrypted-kms	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass Ihre Amazon Simple Notification Service (Amazon SNS) -Themen mit dem AWS Key Management Service (AWS KMS) verschlüsselt werden müssen. Um eventuell vorhandene sensible Daten im Ruhezusta nd in veröffentlichten Nachrichten zu schützen, muss die Verschlüsselung von Daten im Ruhezusta nd aktiviert sein.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
SC-28	Das Informationssystem schützt die Vertraulichkeit UND Integrität von [Zuweisung: von der Organisation definierte Informationen im Ruhestand].	api-gw-cache-enabled-und verschlüsselt	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass die Verschlüsselung für den Cache Ihrer API-Gateway-Stufe aktiviert ist. Da für die API-Methode sensible Daten erfasst werden können, sollten Sie die Verschlüsselung von Daten im Ruhezustand aktivieren, um diese Daten zu schützen.
SC-28	Das Informationssystem schützt die Vertraulichkeit UND Integrität von [Zuweisung: von der Organisation definierte Informationen im Ruhestand].	cloud-trail-encryption-enabled	Da sensible Daten vorhanden sein können und um Daten im Ruhezustand zu schützen, sollten Sie sicherstellen, dass die Verschlüsselung für Ihre AWS CloudTrail Trails aktiviert ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
SC-28	Das Informati onssystem schützt die Vertraulichkeit UND Integrität von [Zuweisung: von der Organisation definiert e Informationen im Ruhestand].	cloudwatch-log-group-encrypted	Um sensible Daten im Speicher zu schützen, stellen Sie sicher, dass die Verschlüs selung für Ihre Amazon CloudWatch Log Groups aktiviert ist.
SC-28	Das Informati onssystem schützt die Vertraulichkeit UND Integrität von [Zuweisung: von der Organisation definiert e Informationen im Ruhestand].	ec2- ebs-encryption-by-default	Zum Schutz von Daten im Ruhezusta nd müssen Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon Elastic Block Store (Amazon EBS)-Volu mes aktiviert ist. Da sensible Daten auch im Ruhezusta nd vorhanden sein können, sollten Sie die Verschlüsselung im Ruhezustand aktivieren, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
SC-28	Das Informationssystem schützt die Vertraulichkeit UND Integrität von [Zuweisung: von der Organisation definierte Informationen im Ruhestand].	efs-encrypted-check	Aktivieren Sie die Verschlüsselung für Ihr Amazon Elastic File System (EFS), um eventuell vorhandene sensible Daten sowie Daten im Ruhezustand zu schützen.
SC-28	Das Informationssystem schützt die Vertraulichkeit UND Integrität von [Zuweisung: von der Organisation definierte Informationen im Ruhestand].	elasticsearch-encrypted-at-rest	Da sensible Daten vorhanden sein können und um Daten im Ruhezustand zu schützen, sollten Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon OpenSearch Service (OpenSearch Service) -Domains aktiviert ist.
SC-28	Das Informationssystem schützt die Vertraulichkeit UND Integrität von [Zuweisung: von der Organisation definierte Informationen im Ruhestand].	encrypted-volumes	Aktivieren Sie die Verschlüsselung für Ihre Amazon-Elastic-Block-Store (Amazon-EBS)-Volumes, um eventuell vorhandene sensible Daten sowie Daten im Ruhezustand zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
SC-28	Das Informationssystem schützt die Vertraulichkeit UND Integrität von [Zuweisung: von der Organisation definierte Informationen im Ruhestand].	kms-cmk-not-scheduled-zum Löschen	Um Daten im Ruhezustand zu schützen, sollten Sie sicherstellen, dass die für den Kunden erforderlichen Masterschlüssel (CMKs) nicht im AWS Key Management Service (AWS KMS) gelöscht werden. Da Schlüssel manchmal gelöscht werden müssen, können Sie mit dieser Regel alle zu löschenden Schlüssel überprüfen, falls ein Schlüssel versehentlich zur Löschung vorgemerkt wurde.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
SC-28	Das Informati onssystem schützt die Vertraulichkeit UND Integrität von [Zuweisung: von der Organisation definiert e Informationen im Ruhestand].	rds-snapshot-encry pted	Stellen Sie sicher, dass die Verschlüs selung für Ihre Amazon Relationa l Database Service (Amazon RDS)-Snap shots aktiviert ist. Da sensible Daten auch im Ruhezusta nd vorhanden sein können, sollten Sie die Verschlüsselung im Ruhezustand aktivieren, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
SC-28	Das Informati onssystem schützt die Vertraulichkeit UND Integrität von [Zuweisung: von der Organisation definiert e Informationen im Ruhestand].	rds-storage-encrypted	Zum Schutz von Daten im Ruhezusta nd müssen Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon Relational Database Service (Amazon RDS)-Instances aktiviert ist. Um eventuell vorhanden e sensible Daten im Ruhezustand in Amazon-RDS-Instanc es zu schützen, muss die Verschlüs selung von Daten im Ruhezustand aktiviert sein.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
SC-28	Das Informationssystem schützt die Vertraulichkeit UND Integrität von [Zuweisung: von der Organisation definierte Informationen im Ruhestand].	redshift-cluster-configuration-check	Um Daten im Ruhezustand zu schützen, muss die Verschlüsselung für Ihre Amazon-Redshift-Cluster aktiviert sein. Sie müssen auch sicherstellen, dass die erforderlichen Konfigurationen auf Amazon-Redshift-Clustern bereitgestellt werden. Die Prüfungsprotokollierung muss aktiviert sein, um Informationen zu Verbindungen und Benutzeraktivitäten in der Datenbank bereitzustellen. Diese Regel erfordert, dass ein Wert für clusterDbEncrypted (Config Default: TRUE) und LoggingEnabled (Config Default: TRUE) gesetzt ist. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
SC-28	Das Informati onssystem schützt die Vertraulichkeit UND Integrität von [Zuweisung: von der Organisation definiert e Informationen im Ruhestand].	redshift-cluster-kms-enabled	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass die Verschlüs selung mit AWS Key Management Service (AWS KMS) für Ihren Amazon Redshift Redshift-Cluster aktiviert ist. Um eventuell vorhanden e sensible Daten im Ruhezustand in Redshift-Clustern zu schützen, muss die Verschlüsselung von Daten im Ruhezusta nd aktiviert sein.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
SC-28	Das Informati onssystem schützt die Vertraulichkeit UND Integrität von [Zuweisung: von der Organisation definiert e Informationen im Ruhestand].	s3- aktiviert bucket-se rver-side-encryption	Zum Schutz von Daten im Ruhezusta nd müssen Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon Simple Storage Service (Amazon S3)-Bucke ts aktiviert ist. Um eventuell vorhanden e sensible Daten im Ruhezustand in Amazon-S3-Buckets zu schützen, muss die Verschlüsselung aktiviert sein.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
SC-28	Das Informati onssystem schützt die Vertraulichkeit UND Integrität von [Zuweisung: von der Organisation definiert e Informationen im Ruhestand].	sagemaker-endpoint -configuration-kms-key-konfiguriert	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass die Verschlüsselung mit dem AWS Key Management Service (AWS KMS) für Ihren Endpunkt aktiviert ist. SageMaker Da sensible Daten auf dem SageMaker Endgerät gespeiche rt werden können, sollten Sie die Verschlüsselung im Ruhezustand aktiviere n, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
SI-2(2)	Die Organisation setzt automatisierte Mechanismen mindestens einmal im Monat ein, um den Zustand der Komponenten des Informationssystems im Hinblick auf die Behebung von Fehlern zu bestimmen.	ec2-manager instance-managed-by-systems	Eine Bestandsaufnahme der Softwareplattformen und Anwendungen innerhalb des Unternehmens ist möglich, indem Amazon Elastic Compute Cloud (Amazon EC2) - Instances mit AWS Systems Manager verwaltet werden. Verwenden Sie AWS Systems Manager, um detaillierte Systemkonfigurationen, Betriebssystem-Patch-Levels, Namen und Typ der Dienste, Softwareinstallationen, Anwendungsname, Herausgeber und Version sowie andere Details zu Ihrer Umgebung bereitzustellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
SI-2(2)	Die Organisation setzt automatisierte Mechanismen mindestens einmal im Monat ein, um den Zustand der Komponenten des Informationssystems im Hinblick auf die Behebung von Fehlern zu bestimmen.	ec2-check managedinstance-association-compliance-status	Verwenden Sie AWS Systems Manager Associations, um bei der Inventarisierung von Softwareplattformen und Anwendungen innerhalb eines Unternehmens zu helfen. AWS Systems Manager weist Ihren verwalteten Instanzen einen Konfigurationsstatus zu und ermöglicht es Ihnen, Basiswerte für Betriebssystem-Patch-Levels, Softwareinstallationen, Anwendungskonfigurationen und andere Details zu Ihrer Umgebung festzulegen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
SI-2(2)	Die Organisation setzt automatisierte Mechanismen mindestens einmal im Monat ein, um den Zustand der Komponenten des Informationssystems im Hinblick auf die Behebung von Fehlern zu bestimmen.	ec2-check managedinstance-patch-compliance-status	Aktivieren Sie diese Regel, um bei der Identifizierung und Dokumentation von Sicherheitslücken in Amazon Elastic Compute Cloud (Amazon EC2) zu helfen. Die Regel prüft, ob die EC2 Amazon-Instance die Patch-Konformität im AWS Systems Manager gemäß den Richtlinien und Verfahren Ihrer Organisation einhält.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
SI-2(2)	Die Organisation setzt automatisierte Mechanismen mindestens einmal im Monat ein, um den Zustand der Komponenten des Informationssystems im Hinblick auf die Behebung von Fehlern zu bestimmen.	elastic-beanstalk-managed-updates-aktiviert	Durch die Aktivierung verwalteter Plattformupdates für eine Amazon-Elastic-Beanstalk-Umgebung wird sichergestellt, dass die aktuellen verfügbaren Plattform-Fixes, -Updates und -Features für die Umgebung installiert sind. Eine bewährte Methode zur Sicherung von Systemen besteht darin, stets die aktuellen Patches zu installieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
SI-3	Die Organisation: a. Setzt Mechanismen zum Schutz vor schädlichem Code an Ein- und Austrittspunkten von Informationssystemen ein, um schädlichen Code zu erkennen und zu beseitigen; b. Aktualisiert die Schutzmechanismen gegen schädlichen Code, sobald neue Versionen verfügbar sind, gemäß den Richtlinien und Verfahren der Organisation für das Konfigurationsmanagement; c. Konfiguriert Schutzmechanismen gegen schädlichen Code zu folgenden Zwecken: 1. Führen Sie regelmäßige Scans des Informationssystems [Zuweisung: von der Organisation festgelegte Häufigkeit] und Echtzeitscans	codebuild-project-envvar-awscred-überprüfen	Stellen Sie sicher, dass die Anmeldeinformationen AWS_ACCESS_KEY_ID AWS_SECRET_ACCESS_KEY nicht in AWS Codebuild-Projektumgebungen vorhanden sind. Speichern Sie diese Variablen nicht als Klartext. Das Speichern dieser Variablen als Klartext bewirkt eine unbeabsichtigte Offenlegung von Daten sowie unberechtigte Zugriffe.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
	von Dateien aus externen Quellen an [Auswahl (eine oder mehrere); Endpunkt; entry/exit points] as the files are downloaded, opened, or executed in accordance with organizational security policy; and 2. [Selection(one or more): block malicious code; quarantine malicious code; send alert to administrator; [Assignment: organization-defined action]] in response to malicious code detection; and d. Addresses the receipt of false positives during malicious code detection and eradication and the resulting potential impact on the availability of the information system. Supplemental Guidance: Information system entry and exit points include, for example, firewalls		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
	, electronic mail servers, web servers, proxy servers, remote-access servers, workstations, notebook computers , and mobile devices. Malicious code includes, for example, viruses, worms, Trojan horses, and spyware. Malicious code can also be encoded in various formats(for example, UUENCODE, Unicode), contained within compresse d or hidden files, or hidden in files using steganogr aphy. Malicious code can be transport ed by different means including, for example, web accesses, electroni c mail, electronic mail attachments, and portable storage devices. Malicious code insertions occur through the exploitat ion of information		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
	system vulnerabi lities. Malicious code protection mechanisms include, for example, anti-viru s signature definitio ns and reputation-based technologies. A variety of technolog ies and methods exist to limit or eliminate the effects of malicious code. Pervasive configura tion management and comprehensive software integrity controls may be effective in preventing execution of unauthori zed code. In addition to commercial off-the-shelf software, malicious code may also be present in custom-built software. This could include, for example, logic bombs, back doors, and other types of cyber attacks that could affect organizational missions/business functions. Tradition		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
	al malicious code protection mechanism s cannot always detect such code. In these situations, organizations rely instead on other safeguards including , for example, secure coding practices, configura tion managemen t and control, trusted procureme nt processes, and monitoring practices to help ensure that software does not perform functions other than the functions intended. Organizations may determine that in response to the detection of malicious code, different actions may be warranted . For example, organizations can define actions in response to malicious code detection during periodic scans, actions in response to		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
	detection of malicious downloads, and/or Netzwerkaktionen als Reaktion auf die Erkennung böswillig er Absichten beim Versuch, Dateien zu öffnen oder auszuführ en, durch. Verwandte Kontrollen: CM-3, MP-2, SA-4, SA-8, SA-12, SA-13, SC-7, SC-26, SC-44, SI-2, SI-4, SI-7. Referenze n: NIST Sonderver öffentlichung 800-83.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
SI-3	Die Organisation: a. Setzt Mechanismen zum Schutz vor schädlichem Code an Ein- und Austrittspunkten von Informationssystemen ein, um schädlichen Code zu erkennen und zu beseitigen; b. Aktualisiert die Schutzmechanismen gegen schädlichen Code, sobald neue Versionen verfügbar sind, gemäß den Richtlinien und Verfahren der Organisation für das Konfigurationsmanagement; c. Konfiguriert Schutzmechanismen gegen schädlichen Code zu folgenden Zwecken: 1. Führen Sie regelmäßige Scans des Informationssystems [Zuweisung: von der Organisation festgelegte Häufigkeit] und Echtzeitscans	codebuild-project-source-repo-URL-Prüfung	Stellen Sie sicher, dass die URL des Quell-Repositorys GitHub oder des Bitbucket-Quell-Repositorys keine persönlichen Zugriffstoken oder Anmeldeinformationen in Codebuild-Projektumgebungen enthält. AWS Verwende OAuth anstelle von persönlichen Zugriffstoken oder Anmeldedaten die Autorisierung für den Zugriff auf GitHub Bitbucket-Repositorys.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
	von Dateien aus externen Quellen bei [Auswahl (eine oder mehrere); Endpunkt; entry/exit points] as the files are downloaded, opened, or executed in accordance with organizational security policy; and 2. [Selection(one or more): block malicious code; quarantine malicious code; send alert to administrator; [Assignment: organization-defined action]] in response to malicious code detection; and d. Addresses the receipt of false positives during malicious code detection and eradication and the resulting potential impact on the availability of the information system. Supplemental Guidance: Information system entry and exit points include, for example, firewalls		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
	, electronic mail servers, web servers, proxy servers, remote-access servers, workstations, notebook computers , and mobile devices. Malicious code includes, for example, viruses, worms, Trojan horses, and spyware. Malicious code can also be encoded in various formats(for example, UUENCODE, Unicode), contained within compresse d or hidden files, or hidden in files using steganogr aphy. Malicious code can be transport ed by different means including, for example, web accesses, electroni c mail, electronic mail attachments, and portable storage devices. Malicious code insertions occur through the exploitat ion of information		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
	system vulnerabi lities. Malicious code protection mechanisms include, for example, anti-viru s signature definitio ns and reputation-based technologies. A variety of technolog ies and methods exist to limit or eliminate the effects of malicious code. Pervasive configura tion management and comprehensive software integrity controls may be effective in preventing execution of unauthori zed code. In addition to commercial off-the-shelf software, malicious code may also be present in custom-built software. This could include, for example, logic bombs, back doors, and other types of cyber attacks that could affect organizational missions/business functions. Tradition		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
	al malicious code protection mechanism s cannot always detect such code. In these situations, organizations rely instead on other safeguards including , for example, secure coding practices, configura tion managemen t and control, trusted procureme nt processes, and monitoring practices to help ensure that software does not perform functions other than the functions intended. Organizations may determine that in response to the detection of malicious code, different actions may be warranted . For example, organizations can define actions in response to malicious code detection during periodic scans, actions in response to		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
	detection of malicious downloads, and/or Netzwerkaktionen als Reaktion auf die Erkennung böswillig er Absichten beim Versuch, Dateien zu öffnen oder auszuführ en, durch. Verwandte Kontrollen: CM-3, MP-2, SA-4, SA-8, SA-12, SA-13, SC-7, SC-26, SC-44, SI-2, SI-4, SI-7. Referenze n: NIST Sonderver öffentlichung 800-83.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
SI-3	Die Organisation: a. Setzt Mechanismen zum Schutz vor schädlichem Code an Ein- und Austrittspunkten von Informationssystemen ein, um schädlichen Code zu erkennen und zu beseitigen; b. Aktualisiert die Schutzmechanismen gegen schädlichen Code, sobald neue Versionen verfügbar sind, gemäß den Richtlinien und Verfahren der Organisation für das Konfigurationsmanagement; c. Konfiguriert Schutzmechanismen gegen schädlichen Code zu folgenden Zwecken: 1. Führen Sie regelmäßige Scans des Informationssystems durch [Zuweisung: von der Organisation festgelegte Häufigkeit] und Echtzeitscans	ecs-task-definition-memory-hartes Limit	Durch die Begrenzung des Speichers, der Ihren Container im Amazon Elastic Container Service (ECS) maximal zur Verfügung steht, verhindern Sie eine Ressourcenüberlastung im Falle eines schädlichen Zugriffs auf Ihre Container.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
	von Dateien aus externen Quellen an [Auswahl (eine oder mehrere); Endpunkt; entry/exit points] as the files are downloaded, opened, or executed in accordance with organizational security policy; and 2. [Selection(one or more): block malicious code; quarantine malicious code; send alert to administrator; [Assignment: organization-defined action]] in response to malicious code detection; and d. Addresses the receipt of false positives during malicious code detection and eradication and the resulting potential impact on the availability of the information system. Supplemental Guidance: Information system entry and exit points include, for example, firewalls		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
	, electronic mail servers, web servers, proxy servers, remote-access servers, workstations, notebook computers , and mobile devices. Malicious code includes, for example, viruses, worms, Trojan horses, and spyware. Malicious code can also be encoded in various formats(for example, UUENCODE, Unicode), contained within compresse d or hidden files, or hidden in files using steganogr aphy. Malicious code can be transport ed by different means including, for example, web accesses, electroni c mail, electronic mail attachments, and portable storage devices. Malicious code insertions occur through the exploitat ion of information		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
	system vulnerabi lities. Malicious code protection mechanisms include, for example, anti-viru s signature definitio ns and reputation-based technologies. A variety of technolog ies and methods exist to limit or eliminate the effects of malicious code. Pervasive configura tion management and comprehensive software integrity controls may be effective in preventing execution of unauthori zed code. In addition to commercial off-the-shelf software, malicious code may also be present in custom-built software. This could include, for example, logic bombs, back doors, and other types of cyber attacks that could affect organizational missions/business functions. Tradition		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
	al malicious code protection mechanism s cannot always detect such code. In these situations, organizations rely instead on other safeguards including , for example, secure coding practices, configura tion managemen t and control, trusted procureme nt processes, and monitoring practices to help ensure that software does not perform functions other than the functions intended. Organizations may determine that in response to the detection of malicious code, different actions may be warranted . For example, organizations can define actions in response to malicious code detection during periodic scans, actions in response to		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
	detection of malicious downloads, and/or Netzwerkaktionen als Reaktion auf die Erkennung böswillig er Absichten beim Versuch, Dateien zu öffnen oder auszuführ en. Verwandte Kontrollen: CM-3, MP-2, SA-4, SA-8, SA-12, SA-13, SC-7, SC-26, SC-44, SI-2, SI-4, SI-7. Referenze n: NIST Sonderver öffentlichung 800-83.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
SI-4(1)	Die Organisation verbindet und konfiguriert die einzelnen Intrusion-Detection-Tools zu einem informationssystemweiten Intrusion-Detection-System.	guardduty-enabled-centralized	Amazon GuardDuty kann mithilfe von Threat Intelligence Feeds helfen, potenzielle Cybersicherheitsereignisse zu überwachen und zu erkennen. Dazu gehören Listen mit bösartigen IPs und maschinellen Lernmethoden, um unerwartete, unbefugte und bösartige Aktivitäten in Ihrer AWS Cloud-Umgebung zu identifizieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
SI-4(2)	Die Organisation setzt automatisierte Tools ein, um die Analyse von Ereigniss en nahezu in Echtzeit zu unterstützen.	multi-region-cloudtrail-enabled	AWS CloudTrail zeichnet Aktionen und API-Aufrufe der AWS Management Console auf. Sie können feststellen, welche Benutzer und Konten angerufen wurden AWS, von welcher Quell-IP-Adresse aus die Anrufe getätigt wurden und wann die Anrufe erfolgten. CloudTrail übermittelt Protokolldateien aus allen AWS Regionen an Ihren S3-Bucket , wenn MULTI_REG ION_CLOUD _TRAIL_ENABLED aktiviert ist. Außerdem wird beim AWS Start einer neuen Region derselbe Trail in der neuen Region erstellt. CloudTrail Dadurch erhalten Sie automatis ch Protokolldateien mit API-Aktivitäten für die neue Region.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
SI-4(2)	Die Organisation setzt automatisierte Tools ein, um die Analyse von Ereignissen nahezu in Echtzeit zu unterstützen.	securityhub-enabled	AWS Security Hub hilft bei der Überwachung von unbefugtem Personal, Verbindungen, Geräten und Software. AWS Security Hub aggregiert, organisiert und priorisiert die Sicherheitswarnungen oder Ergebnisse mehrerer Dienste. AWS Einige dieser Dienste sind Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer und AWS Firewall Manager sowie AWS Partnerlösungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
SI-4(2)	Die Organisation setzt automatisierte Tools ein, um die Analyse von Ereignissen nahezu in Echtzeit zu unterstützen.	cloudtrail-enabled	AWS CloudTrail kann durch die Aufzeichnung von Aktionen und API-Aufrufen der AWS Management Console bei der Nichtabstreitbarkeit helfen. Sie können die Benutzer und die Benutzer AWS-Konten , die einen AWS Dienst aufgerufen haben, die Quell-IP-Adresse, über die die Aufrufe generiert wurden, und den Zeitpunkt der Anrufe identifizieren. Einzelheiten zu den erfassten Daten finden Sie in den AWS CloudTrail Datensatzinhalten.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
SI-4(2)	Die Organisation setzt automatisierte Tools ein, um die Analyse von Ereignissen nahezu in Echtzeit zu unterstützen.	cloudtrail-s3-dataevents-enabled	Die Erfassung von Simple Storage Service (Amazon S3)-Datenereignissen unterstützt die Erkennung von ungewöhnlichen Aktivitäten. Zu den Details gehören AWS-Konto Informationen über den Zugriff auf einen Amazon S3 S3-Bucket, die IP-Adresse und die Uhrzeit des Ereignisses.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
SI-4(2)	Die Organisation setzt automatisierte Tools ein, um die Analyse von Ereignissen nahezu in Echtzeit zu unterstützen.	cloudwatch-alarm-action-check	Amazon CloudWatch alarmiert, wenn eine Metrik den Schwellenwert für eine bestimmte Anzahl von Bewertungszeiträumen überschreitet. Der Alarm führt eine oder mehrere Aktionen durch, die vom Wert der Metrik oder des Ausdrucks im Vergleich zu einem Schwellenwert in einer Reihe von Zeiträumen abhängt. Diese Regel erfordert einen Wert für alarmActionRequired (Config Default: True), insufficientDataAction Required (Config Default: True), okActionRequired (Config Default: False). Der tatsächliche Wert muss die Alarmaktionen für Ihre Umgebung widerspiegeln.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
SI-4(2)	Die Organisation setzt automatisierte Tools ein, um die Analyse von Ereignissen nahezu in Echtzeit zu unterstützen.	ec2- instance-detailed-monitoring-enabled	Aktivieren Sie diese Regel, um die Amazon Elastic Compute Cloud (Amazon EC2) - Instance-Überwachung auf der EC2 Amazon-Konsole zu verbessern, in der Monitoring-Diagramme mit einem Zeitraum von 1 Minute für die Instance angezeigt werden.
SI-4(2)	Die Organisation setzt automatisierte Tools ein, um die Analyse von Ereignissen nahezu in Echtzeit zu unterstützen.	guardduty-enabled-centralized	Amazon GuardDuty kann mithilfe von Threat Intelligence Feeds helfen, potenzielle Cybersicherheitsereignisse zu überwachen und zu erkennen. Dazu gehören Listen mit bösartigen IPs und maschinellen Lernmethoden, um unerwartete, unbefugte und bösartige Aktivitäten in Ihrer AWS Cloud-Umgebung zu identifizieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
SI-4(2)	Die Organisation setzt automatisierte Tools ein, um die Analyse von Ereignissen nahezu in Echtzeit zu unterstützen.	redshift-cluster-configuration-check	Um Daten im Ruhezustand zu schützen, muss die Verschlüsselung für Ihre Amazon-Redshift-Cluster aktiviert sein. Sie müssen auch sicherstellen, dass die erforderlichen Konfigurationen auf Amazon-Redshift-Clustern bereitgestellt werden. Die Prüfungsprotokollierung muss aktiviert sein, um Informationen zu Verbindungen und Benutzeraktivitäten in der Datenbank bereitzustellen. Diese Regel erfordert, dass ein Wert für clusterDbEncrypted (Config Default: TRUE) und LoggingEnabled (Config Default: TRUE) gesetzt ist. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
SI-4(4)	Das Informationssystem überwacht den ein- und ausgehenden Kommunikationsverkehr kontinuierlich auf ungewöhnliche oder unzulässige Aktivitäten oder Bedingungen.	securityhub-enabled	AWS Security Hub hilft bei der Überwachung von unbefugtem Personal, Verbindungen, Geräten und Software. AWS Security Hub aggregiert, organisiert und priorisiert die Sicherheitswarnungen oder Ergebnisse mehrerer Dienste. AWS Einige dieser Dienste sind Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer und AWS Firewall Manager sowie AWS Partnerlösungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
SI-4(4)	Das Informati onssystem überwacht den ein- und ausgehenden Kommunikationsverk ehr kontinuierlich auf ungewöhnliche oder unzulässige Aktivität en oder Bedingungen.	cloud-trail-cloud-watch-logs-aktiviert	Verwenden Sie Amazon CloudWatc h , um Protokoll ereignisaktivitäten zentral zu sammeln und zu verwalten. Die Aufnahme von AWS CloudTrail Daten liefert Einzelheiten zu den API-Aufrufaktivitä ten in Ihrem AWS-Konto.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
SI-4(4)	Das Informati onssystem überwacht den ein- und ausgehenden Kommunikationsverk ehr kontinuierlich auf ungewöhnliche oder unzulässige Aktivität en oder Bedingungen.	cloudwatch-alarm-a ction-check	Amazon CloudWatch alarmiert, wenn eine Metrik den Schwellen wert für eine bestimmte Anzahl von Bewertungszeiträum en überschreitet. Der Alarm führt eine oder mehrere Aktionen durch, die vom Wert der Metrik oder des Ausdrucks im Vergleich zu einem Schwellenwert in einer Reihe von Zeiträumen abhängt. Diese Regel erfordert einen Wert für alarmActionRequired (Config Default: True), insufficientDataAc tion Required (Config Default: True), okActionRequired (Config Default: False). Der tatsächli che Wert muss die Alarmaktionen für Ihre Umgebung widerspie geln.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
SI-4(4)	Das Informati onssystem überwacht den ein- und ausgehenden Kommunikationsverk ehr kontinuierlich auf ungewöhnliche oder unzulässige Aktivität en oder Bedingungen.	guardduty-enabled-centralized	Amazon GuardDuty kann mithilfe von Threat Intellige nce Feeds helfen, potenzielle Cybersich erheitsereignisse zu überwachen und zu erkennen. Dazu gehören Listen mit bösartigen IPs und maschinel len Lernmethoden zur Identifizierung unerwarteter, nicht autorisierter und bösartiger Aktivitäten in Ihrer AWS Cloud-Umgebung.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
SI-4(5)	Das Informati onssystem alarmiert [Zuweisung: von der Organisation ernanntes Personal oder definierte Rollen], wenn die folgenden Anzeichen für eine bestehend e oder potenzielle Gefährdung auftreten : [Zuweisung: von der Organisation definiert e Gefährdungsindikat oren].	securityhub-enabled	AWS Security Hub hilft bei der Überwachung von unbefugtem Personal, Verbindun gen, Geräten und Software. AWS Security Hub aggregiert, organisie rt und priorisie rt die Sicherhei tswarnungen oder Ergebnisse mehrerer Dienste. AWS Einige dieser Dienste sind Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer und AWS Firewall Manager sowie AWS Partnerlösungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
SI-4(5)	Das Informati onssystem alarmiert [Zuweisung: von der Organisation ernanntes Personal oder definierte Rollen], wenn die folgenden Anzeichen für eine bestehend e oder potenzielle Gefährdung auftreten : [Zuweisung: von der Organisation definiert e Gefährdungsindikat oren].	cloud-trail-cloud-watch-logs-aktiviert	Verwenden Sie Amazon CloudWatc h , um Protokoll ereignisaktivitäten zentral zu sammeln und zu verwalten. Die Aufnahme von AWS CloudTrail Daten liefert Einzelheiten zu den API-Aufrufaktivitä ten in Ihrem AWS-Konto.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
SI-4(5)	Das Informationssystem alarmiert [Zuweisung: von der Organisation ernanntes Personal oder definierte Rollen], wenn die folgenden Anzeichen für eine bestehende oder potenzielle Gefährdung auftreten: [Zuweisung: von der Organisation definierte Gefährdungsindikatoren].	cloudwatch-alarm-action-check	Amazon CloudWatch alarmiert, wenn eine Metrik den Schwellenwert für eine bestimmte Anzahl von Bewertungszeiträumen überschreitet. Der Alarm führt eine oder mehrere Aktionen durch, die vom Wert der Metrik oder des Ausdrucks im Vergleich zu einem Schwellenwert in einer Reihe von Zeiträumen abhängt. Diese Regel erfordert einen Wert für alarmActionRequired (Config Default: True), insufficientDataAction Required (Config Default: True), okActionRequired (Config Default: False). Der tatsächliche Wert muss die Alarmaktionen für Ihre Umgebung widerspiegeln.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
SI-4(5)	Das Informati onssystem alarmiert [Zuweisung: von der Organisation ernanntes Personal oder definierte Rollen], wenn die folgenden Anzeichen für eine bestehend e oder potenzielle Gefährdung auftreten : [Zuweisung: von der Organisation definiert e Gefährdungsindikat oren].	guardduty-enabled-centralized	Amazon GuardDuty kann mithilfe von Threat Intellige nce Feeds helfen, potenzielle Cybersich erheitsereignisse zu überwachen und zu erkennen. Dazu gehören Listen mit bösartigen IPs und maschinel len Lernmethoden zur Identifizierung unerwarteter, nicht autorisierter und bösartiger Aktivitäten in Ihrer AWS Cloud-Umgebung.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
SI-4(16)	Die Organisation korreliert Informati onen aus Überwachu ngstools, die im gesamten Informati onssystem eingesetzt werden.	multi-region-cloudtrail-enabled	AWS CloudTrail zeichnet Aktionen und API-Aufrufe der AWS Management Console auf. Sie können feststellen, welche Benutzer und Konten angerufen wurden AWS, von welcher Quell-IP-Adresse aus die Anrufe getätigt wurden und wann die Anrufe erfolgten. CloudTrail übermittelt Protokolldateien aus allen AWS Regionen an Ihren S3-Bucket , wenn MULTI_REG ION_CLOUD _TRAIL_ENABLED aktiviert ist. Außerdem wird beim AWS Start einer neuen Region derselbe Trail in der neuen Region erstellt. CloudTrail Dadurch erhalten Sie automatis ch Protokolldateien mit API-Aktivitäten für die neue Region.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
SI-4(16)	Die Organisation korreliert Informati onen aus Überwachu ngstools, die im gesamten Informati onssystem eingesetzt werden.	securityhub-enabled	AWS Security Hub hilft bei der Überwachung von unbefugtem Personal, Verbindun gen, Geräten und Software. AWS Security Hub aggregiert, organisie rt und priorisie rt die Sicherhei tswarnungen oder Ergebnisse mehrerer Dienste. AWS Einige dieser Dienste sind Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer und AWS Firewall Manager sowie AWS Partnerlösungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
SI-4(16)	Die Organisation korreliert Informationen aus Überwachungstools, die im gesamten Informationssystem eingesetzt werden.	cloudtrail-enabled	AWS CloudTrail kann durch die Aufzeichnung von Aktionen und API-Aufrufen der AWS Management Console bei der Nichtabstreitbarkeit helfen. Sie können die Benutzer und die Benutzer AWS-Konten , die einen AWS Dienst aufgerufen haben, die Quell-IP-Adresse, über die die Aufrufe generiert wurden, und den Zeitpunkt der Anrufe identifizieren. Einzelheiten zu den erfassten Daten finden Sie in den AWS CloudTrail Datensatzinhalten.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
SI-4(16)	Die Organisation korreliert Informationen aus Überwachungstools, die im gesamten Informationssystem eingesetzt werden.	cloudtrail-s3-dataevents-enabled	Die Erfassung von Simple Storage Service (Amazon S3)-Datenereignissen unterstützt die Erkennung von ungewöhnlichen Aktivitäten. Zu den Details gehören AWS-Konto Informationen über den Zugriff auf einen Amazon S3 S3-Bucket, die IP-Adresse und die Uhrzeit des Ereignisses.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
SI-4(16)	Die Organisation korreliert Informati onen aus Überwachu ngstools, die im gesamten Informati onssystem eingesetzt werden.	guardduty-enabled-centralized	Amazon GuardDuty kann mithilfe von Threat Intellige nce Feeds helfen, potenzielle Cybersich erheitsereignisse zu überwachen und zu erkennen. Dazu gehören Listen mit bösartigen IPs und maschinel len Lernmethoden zur Identifizierung unerwarteter, nicht autorisierter und bösartiger Aktivitäten in Ihrer AWS Cloud-Umgebung.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
SI-4(16)	Die Organisation korreliert Informationen aus Überwachungstools, die im gesamten Informationssystem eingesetzt werden.	redshift-cluster-configuration-check	Um Daten im Ruhezustand zu schützen, muss die Verschlüsselung für Ihre Amazon-Redshift-Cluster aktiviert sein. Sie müssen auch sicherstellen, dass die erforderlichen Konfigurationen auf Amazon-Redshift-Clustern bereitgestellt werden. Die Prüfungsprotokollierung muss aktiviert sein, um Informationen zu Verbindungen und Benutzeraktivitäten in der Datenbank bereitzustellen. Diese Regel erfordert, dass ein Wert für clusterDbEncrypted (Config Default: TRUE) und LoggingEnabled (Config Default: TRUE) gesetzt ist. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
SI-4(a)(b)(c)	Die Organisation: a. Überwacht das Informationssystem und erkennt: 1. Angriffe und Indikatoren für potenzielle Angriffe in Übereinstimmung mit [Zuweisung: von der Organisation festgelegte Überwachungsziele]; und 2. Nicht autorisierte lokale Verbindungen sowie Netzwerk- und Remoteverbindungen; b. Identifiziert die unbefugte Nutzung des Informationssystems durch [Zuweisung: von der Organisation festgelegte Techniken und Methoden]; c. Verwendet Überwachungsgeräte: i. strategisch innerhalb des Informationssystems, um von der Organisation festgelegte wesentliche Informationen zu sammeln;	alb-waf-enabled	Stellen Sie sicher, dass AWS WAF auf Elastic Load Balancers (ELB) aktiviert ist, um Webanwendungen zu schützen. Eine WAF trägt zum Schutz Ihrer Webanwendungen oder APIs vor gängigen Web-Exploits bei. Diese Web-Exploits können sich auf die Verfügbarkeit auswirken, die Sicherheit gefährden oder übermäßige Ressourcen in Ihrer Umgebung verbrauchen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
	und ii) an Ad-hoc-St andorten innerhalb des Systems, um bestimmte Arten von Vorgängen zu verfolgen, die für die Organisation von Interesse sind.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
SI-4(a)(b)(c)	Die Organisation: a. Überwacht das Informationssystem und erkennt: 1. Angriffe und Indikatoren für potenzielle Angriffe in Übereinstimmung mit [Zuweisung: von der Organisation festgelegte Überwachungsziele]; und 2. Nicht autorisierte lokale Verbindungen sowie Netzwerk- und Remoteverbindungen; b. Identifiziert die unbefugte Nutzung des Informationssystems durch [Zuweisung: von der Organisation festgelegte Techniken und Methoden]; c. Verwendet Überwachungsgeräte: i. strategisch innerhalb des Informationssystems, um von der Organisation festgelegte wesentliche Informationen zu sammeln;	api-gw-associated-with-WAF	AWS Mit WAF können Sie eine Reihe von Regeln (als Web Access Control List (Web ACL) bezeichnet) konfigurieren, die Webanfragen auf der Grundlage von anpassbaren Websicherheitsregeln und -bedingungen, die Sie definieren, zulassen, blockieren oder zählen. Stellen Sie sicher, dass Ihre Amazon-API-Gateway-Stufe mit einer WAF-Web-ACL verknüpft ist, um sie vor böswilligen Angriffen zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
	und ii) an Ad-hoc-St andorten innerhalb des Systems, um bestimmte Arten von Vorgängen zu verfolgen, die für die Organisation von Interesse sind.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
SI-4(a)(b)(c)	Die Organisation: a. Überwacht das Informationssystem und erkennt: 1. Angriffe und Indikatoren für potenzielle Angriffe in Übereinstimmung mit [Zuweisung: von der Organisation festgelegte Überwachungsziele]; und 2. Nicht autorisierte lokale Verbindungen sowie Netzwerk- und Remoteverbindungen; b. Identifiziert die unbefugte Nutzung des Informationssystems durch [Zuweisung: von der Organisation festgelegte Techniken und Methoden]; c. Verwendet Überwachungsgeräte: i. strategisch innerhalb des Informationssystems, um von der Organisation festgelegte wesentliche Informationen zu sammeln;	guardduty-non-archived-findings	Amazon GuardDuty hilft Ihnen dabei, die Auswirkungen eines Vorfalls zu verstehen, indem es die Ergebnisse nach Schweregrad klassifiziert: niedrig, mittel und hoch. Diese Klassifizierungen können Sie zur Festlegung von entsprechenden Strategien und Prioritäten zur Behebung solcher Vorfälle verwenden. Mit dieser Regel können Sie optional daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7) und daysHighSev (Config Default: 1) für nicht archivierte Ergebnisse festlegen, wie es die Richtlinien Ihrer Organisation erfordern.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
	und ii) an Ad-hoc-St andorten innerhalb des Systems, um bestimmte Arten von Vorgängen zu verfolgen, die für die Organisation von Interesse sind.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
SI-4(a)(b)(c)	Die Organisation: a. Überwacht das Informationssystem und erkennt: 1. Angriffe und Indikatoren für potenzielle Angriffe in Übereinstimmung mit [Zuweisung: von der Organisation festgelegte Überwachungsziele]; und 2. Nicht autorisierte lokale Verbindungen sowie Netzwerk- und Remoteverbindungen; b. Identifiziert die unbefugte Nutzung des Informationssystems durch [Zuweisung: von der Organisation festgelegte Techniken und Methoden]; c. Verwendet Überwachungsgeräte: i. strategisch innerhalb des Informationssystems, um von der Organisation festgelegte wesentliche Informationen zu sammeln;	securityhub-enabled	AWS Security Hub hilft bei der Überwachung von unbefugtem Personal, Verbindungen, Geräten und Software. AWS Security Hub aggregiert, organisiert und priorisiert die Sicherheitswarnungen oder Ergebnisse mehrerer Dienste. AWS Einige dieser Dienste sind Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer und AWS Firewall Manager sowie AWS Partnerlösungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
	und ii) an Ad-hoc-St andorten innerhalb des Systems, um bestimmte Arten von Vorgängen zu verfolgen, die für die Organisation von Interesse sind.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
SI-4(a)(b)(c)	Die Organisation: a. Überwacht das Informationssystem und erkennt: 1. Angriffe und Indikatoren für potenzielle Angriffe in Übereinstimmung mit [Zuweisung: von der Organisation festgelegte Überwachungsziele]; und 2. Nicht autorisierte lokale Verbindungen sowie Netzwerk- und Remoteverbindungen; b. Identifiziert die unbefugte Nutzung des Informationssystems durch [Zuweisung: von der Organisation festgelegte Techniken und Methoden]; c. Verwendet Überwachungsgeräte: i. strategisch innerhalb des Informationssystems, um von der Organisation festgelegte wesentliche Informationen zu sammeln;	wafv2-logging-enabled	Um Ihnen bei der Protokollierung und Überwachung in Ihrer Umgebung zu helfen, aktivieren Sie die AWS WAF (V2) -Protokollierung im regionalen und globalen Web. ACLs AWS Die WAF-Protokollierung bietet detaillierte Informationen über den Datenverkehr, der von Ihrer Web-ACL analysiert wird. In den Protokollen werden die Uhrzeit aufgezeichnet, zu der die AWS WAF die Anfrage von Ihrer AWS Ressource erhalten hat, Informationen zu der Anfrage und eine Aktion für die Regel, der jede Anfrage entsprach.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
	und ii) an Ad-hoc-St andorten innerhalb des Systems, um bestimmte Arten von Vorgängen zu verfolgen, die für die Organisation von Interesse sind.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
SI-4(a)(b)(c)	Die Organisation: a. Überwacht das Informationssystem und erkennt: 1. Angriffe und Indikatoren für potenzielle Angriffe in Übereinstimmung mit [Zuweisung: von der Organisation festgelegte Überwachungsziele]; und 2. Nicht autorisierte lokale Verbindungen sowie Netzwerk- und Remoteverbindungen; b. Identifiziert die unbefugte Nutzung des Informationssystems durch [Zuweisung: von der Organisation festgelegte Techniken und Methoden]; c. Verwendet Überwachungsgeräte: i. strategisch innerhalb des Informationssystems, um von der Organisation festgelegte wesentliche Informationen zu sammeln;	cloud-trail-cloud-watch-logs-aktiviert	Verwenden Sie Amazon CloudWatch , um Protokoll ereignisaktivitäten zentral zu sammeln und zu verwalten. Die Aufnahme von AWS CloudTrail Daten liefert Einzelheiten zu den API-Aufrufaktivitäten in Ihrem AWS-Konto.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
	und ii) an Ad-hoc-St andorten innerhalb des Systems, um bestimmte Arten von Vorgängen zu verfolgen, die für die Organisation von Interesse sind.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
SI-4(a)(b)(c)	Die Organisation: a. Überwacht das Informationssystem und erkennt: 1. Angriffe und Indikatoren für potenzielle Angriffe in Übereinstimmung mit [Zuweisung: von der Organisation festgelegte Überwachungsziele]; und 2. Nicht autorisierte lokale Verbindungen sowie Netzwerk- und Remoteverbindungen; b. Identifiziert die unbefugte Nutzung des Informationssystems durch [Zuweisung: von der Organisation festgelegte Techniken und Methoden]; c. Verwendet Überwachungsgeräte: i. strategisch innerhalb des Informationssystems, um von der Organisation festgelegte wesentliche Informationen zu sammeln;	cloudwatch-alarm-action-check	Amazon CloudWatch alarmiert, wenn eine Metrik den Schwellenwert für eine bestimmte Anzahl von Bewertungszeiträumen überschreitet. Der Alarm führt eine oder mehrere Aktionen durch, die vom Wert der Metrik oder des Ausdrucks im Vergleich zu einem Schwellenwert in einer Reihe von Zeiträumen abhängt. Diese Regel erfordert einen Wert für alarmActionRequired (Config Default: True), insufficientDataAction Required (Config Default: True), okActionRequired (Config Default: False). Der tatsächliche Wert muss die Alarmaktionen für Ihre Umgebung widerspiegeln.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
	und ii) an Ad-hoc-St andorten innerhalb des Systems, um bestimmte Arten von Vorgängen zu verfolgen, die für die Organisation von Interesse sind.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
SI-4(a)(b)(c)	Die Organisation: a. Überwacht das Informationssystem und erkennt: 1. Angriffe und Indikatoren für potenzielle Angriffe in Übereinstimmung mit [Zuweisung: von der Organisation festgelegte Überwachungsziele]; und 2. Nicht autorisierte lokale Verbindungen sowie Netzwerk- und Remoteverbindungen; b. Identifiziert die unbefugte Nutzung des Informationssystems durch [Zuweisung: von der Organisation festgelegte Techniken und Methoden]; c. Verwendet Überwachungsgeräte: i. strategisch innerhalb des Informationssystems, um von der Organisation festgelegte wesentliche Informationen zu sammeln;	ec2- instance-detailed-monitoring-enabled	Aktivieren Sie diese Regel, um die Amazon Elastic Compute Cloud (Amazon EC2) - Instance-Überwachung auf der EC2 Amazon-Konsole zu verbessern, in der Monitoring-Diagramme mit einem Zeitraum von 1 Minute für die Instance angezeigt werden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
	und ii) an Ad-hoc-St andorten innerhalb des Systems, um bestimmte Arten von Vorgängen zu verfolgen, die für die Organisation von Interesse sind.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
SI-4(a)(b)(c)	Die Organisation: a. Überwacht das Informationssystem und erkennt: 1. Angriffe und Indikatoren für potenzielle Angriffe in Übereinstimmung mit [Zuweisung: von der Organisation festgelegte Überwachungsziele]; und 2. Nicht autorisierte lokale Verbindungen sowie Netzwerk- und Remoteverbindungen; b. Identifiziert die unbefugte Nutzung des Informationssystems durch [Zuweisung: von der Organisation festgelegte Techniken und Methoden]; c. Verwendet Überwachungsgeräte: i. strategisch innerhalb des Informationssystems, um von der Organisation festgelegte wesentliche Informationen zu sammeln;	guardduty-enabled-centralized	Amazon GuardDuty kann mithilfe von Threat Intelligence Feeds helfen, potenzielle Cybersicherheitsereignisse zu überwachen und zu erkennen. Dazu gehören Listen mit bösartigen IPs und maschinellen Lernmethoden zur Identifizierung unerwarteter, nicht autorisierter und bösartiger Aktivitäten in Ihrer AWS Cloud-Umgebung.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
	und ii) an Ad-hoc-St andorten innerhalb des Systems, um bestimmte Arten von Vorgängen zu verfolgen, die für die Organisation von Interesse sind.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
SI-5	Die Organisation: a. Erhält fortlaufend Warnmeldungen, Hinweise und Anweisungen zur Informationssystemsicherheit von [Zuweisung: von der Organisation definierte externe Organisationen]; b. Generiert nach Bedarf interne Sicherheitswarnungen, -hinweise und -anweisungen; c. Verteilt Sicherheitswarnungen, Hinweise und Anweisungen an: [Auswahl (eine oder mehrere Optionen): [Zuweisung: von der Organisation ernanntes Personal oder definierte Rollen]; [Zuweisung: von der Organisation definierte Elemente innerhalb der Organisation]; [Zuweisung: von der Organisation definierte externe	cloudwatch-alarm-action-check	Amazon CloudWatch alarmiert, wenn eine Metrik den Schwellenwert für eine bestimmte Anzahl von Bewertungszeiträumen überschreitet. Der Alarm führt eine oder mehrere Aktionen durch, die vom Wert der Metrik oder des Ausdrucks im Vergleich zu einem Schwellenwert in einer Reihe von Zeiträumen abhängt. Diese Regel erfordert einen Wert für alarmActionRequired (Config Default: True), insufficientDataAction Required (Config Default: True), okActionRequired (Config Default: False). Der tatsächliche Wert muss die Alarmaktionen für Ihre Umgebung widerspiegeln.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
	Organisationen]]; und d. Implement iert Sicherheitsrichtli nien gemäß den festgelegten Zeitpläne n oder benachric htigt die ausstellende Organisation über den Grad der Nichteinh altung. Zusätzlic he Empfehlungen: Das United States Computer Emergency Readiness Team (US-CERT) generiert Sicherheitswarnung en und -hinweise, um der Bundesregierung kontinuierlich situation sbedingte Informati onen zukommen zu lassen. Sicherhei tsrichtlinien werden von der OMB oder anderen benannten Organisationen herausgegeben, die für die Erstellun g solcher Richtlini en verantwortlich und befugt sind. Die Einhaltung von Sicherheitsrichtli nien ist aufgrund		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
	der Kritizität vieler dieser Richtlinien und der möglichen unmittelbaren negativen Auswirkun gen einer verspätet en Umsetzung der Richtlinien auf organisat orische Abläufe und Ressourcen, Einzelpersonen, andere Organisat ionen und die Nation von entscheidender Bedeutung. Zu den externen Organisat ionen gehören beispielsweise externe mission/b usiness partners, supply chain partners, external service providers, and other peer/supporting Organisationen. Verwandte Kontrolle : SI-2. Referenze n: NIST Sonderver öffentlichung 800-40.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
SI-5	Die Organisation: a. Erhält fortlaufe nd Warnmeldu ngen, Hinweise und Anweisungen zur Informationssystem sicherheit von [Zuweisung: von der Organisation definiert e externe Organisat ionen]; b. Generiert nach Bedarf interne Sicherheitswarnung en, -hinweise und -anweisungen; c. Verteilt Sicherhei tswarnungen, Hinweise und Anweisungen an: [Auswahl (eine oder mehrere Optionen) : [Zuweisung: von der Organisation ernanntes Personal oder definierte Rollen]; [Zuweisun g: von der Organisat ion definierte Elemente innerhalb der Organisation]; [Zuweisung: von der Organisation definierte externe	guardduty-enabled-centralized	Amazon GuardDuty kann mithilfe von Threat Intellige nce Feeds helfen, potenzielle Cybersich erheitsereignisse zu überwachen und zu erkennen. Dazu gehören Listen mit bösartigen IPs und maschinel len Lernmethoden zur Identifizierung unerwarteter, nicht autorisierter und bösartiger Aktivitäten in Ihrer AWS Cloud-Umgebung.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
	Organisationen]]; und d. Implement iert Sicherheitsrichtli nien gemäß den festgelegten Zeitpläne n oder benachric htigt die ausstellende Organisation über den Grad der Nichteinh altung. Zusätzlic he Empfehlungen: Das United States Computer Emergency Readiness Team (US-CERT) generiert Sicherheitswarnung en und -hinweise, um der Bundesregierung kontinuierlich situation sbedingte Informati onen zukommen zu lassen. Sicherhei tsrichtlinien werden von der OMB oder anderen benannten Organisationen herausgegeben, die für die Erstellun g solcher Richtlini en verantwortlich und befugt sind. Die Einhaltung von Sicherheitsrichtli nien ist aufgrund		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
	der Kritizität vieler dieser Richtlinien und der möglichen unmittelbaren negativen Auswirkun gen einer verspätet en Umsetzung der Richtlinien auf organisat orische Abläufe und Ressourcen, Einzelpersonen, andere Organisat ionen und die Nation von entscheidender Bedeutung. Zu den externen Organisat ionen gehören beispielsweise externe mission/b usiness partners, supply chain partners, external service providers, and other peer/supporting Organisationen. Verwandte Kontrolle : SI-2. Referenze n: NIST Sonderver öffentlichung 800-40.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
SI-5	Die Organisation: a. Erhält fortlaufend Warnmeldungen, Hinweise und Anweisungen zur Informationssystemsicherheit von [Zuweisung: von der Organisation definierte externe Organisationen]; b. Generiert nach Bedarf interne Sicherheitswarnungen, -hinweise und -anweisungen; c. Verteilt Sicherheitswarnungen, Hinweise und Anweisungen an: [Auswahl (eine oder mehrere Optionen): [Zuweisung: von der Organisation ernanntes Personal oder definierte Rollen]; [Zuweisung: von der Organisation definierte Elemente innerhalb der Organisation]; [Zuweisung: von der Organisation definierte externe	guardduty-non-archived-findings	Amazon GuardDuty hilft Ihnen dabei, die Auswirkungen eines Vorfalls zu verstehen, indem es die Ergebnisse nach Schweregrad klassifiziert: niedrig, mittel und hoch. Diese Klassifizierungen können Sie zur Festlegung von entsprechenden Strategien und Prioritäten zur Behebung solcher Vorfälle verwenden. Mit dieser Regel können Sie optional daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7) und daysHighSev (Config Default: 1) für nicht archivierte Ergebnisse festlegen, wie es die Richtlinien Ihrer Organisation erfordern.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
	Organisationen]]; und d. Implement iert Sicherheitsrichtli nien gemäß den festgelegten Zeitpläne n oder benachric htigt die ausstellende Organisation über den Grad der Nichteinh altung. Zusätzlic he Empfehlungen: Das United States Computer Emergency Readiness Team (US-CERT) generiert Sicherheitswarnung en und -hinweise, um der Bundesregierung kontinuierlich situation sbedingte Informati onen zukommen zu lassen. Sicherhei tsrichtlinien werden von der OMB oder anderen benannten Organisationen herausgegeben, die für die Erstellun g solcher Richtlini en verantwortlich und befugt sind. Die Einhaltung von Sicherheitsrichtli nien ist aufgrund		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
	der Kritizität vieler dieser Richtlinien und der möglichen unmittelbaren negativen Auswirkun gen einer verspätet en Umsetzung der Richtlinien auf organisat orische Abläufe und Ressourcen, Einzelpersonen, andere Organisat ionen und die Nation von entscheidender Bedeutung. Zu den externen Organisat ionen gehören beispielsweise externe mission/b usiness partners, supply chain partners, external service providers, and other peer/supporting Organisationen. Verwandte Kontrolle : SI-2. Referenze n: NIST Sonderver öffentlichung 800-40.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
SI-5	Die Organisation: a. Erhält fortlaufe nd Warnmeldu ngen, Hinweise und Anweisungen zur Informationssystem sicherheit von [Zuweisung: von der Organisation definiert e externe Organisat ionen]; b. Generiert nach Bedarf interne Sicherheitswarnung en, -hinweise und -anweisungen; c. Verteilt Sicherhei tswarnungen, Hinweise und Anweisungen an: [Auswahl (eine oder mehrere Optionen) : [Zuweisung: von der Organisation ernanntes Personal oder definierte Rollen]; [Zuweisun g: von der Organisat ion definierte Elemente innerhalb der Organisation]; [Zuweisung: von der Organisation definierte externe	securityhub-enabled	AWS Security Hub hilft bei der Überwachung von unbefugtem Personal, Verbindun gen, Geräten und Software. AWS Security Hub aggregiert, organisie rt und priorisie rt die Sicherhei tswarnungen oder Ergebnisse mehrerer Dienste. AWS Einige dieser Dienste sind Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer und AWS Firewall Manager sowie AWS Partnerlösungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
	Organisationen]]; und d. Implement iert Sicherheitsrichtli nien gemäß den festgelegten Zeitpläne n oder benachric htigt die ausstellende Organisation über den Grad der Nichteinh altung. Zusätzlic he Empfehlungen: Das United States Computer Emergency Readiness Team (US-CERT) generiert Sicherheitswarnung en und -hinweise, um der Bundesregierung kontinuierlich situation sbedingte Informati onen zukommen zu lassen. Sicherhei tsrichtlinien werden von der OMB oder anderen benannten Organisationen herausgegeben, die für die Erstellun g solcher Richtlini en verantwortlich und befugt sind. Die Einhaltung von Sicherheitsrichtli nien ist aufgrund		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
	der Kritizität vieler dieser Richtlinien und der möglichen unmittelbaren negativen Auswirkun gen einer verspätet en Umsetzung der Richtlinien auf organisat orische Abläufe und Ressourcen, Einzelpersonen, andere Organisat ionen und die Nation von entscheidender Bedeutung. Zu den externen Organisat ionen gehören beispielsweise externe mission/b usiness partners, supply chain partners, external service providers, and other peer/supporting Organisationen. Verwandte Kontrolle : SI-2. Referenze n: NIST Sonderver öffentlichung 800-40.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
SI-7(1)	Das Informati onssystem führt mindestens einmal im Monat eine Integritätsprüfung bei sicherheitsrelevanten Ereignissen durch.	cloud-trail-log-file-Validierung aktiviert	Verwenden Sie die AWS CloudTrail Protokolldateivali dierung, um die Integrität von Protokoll en zu überprüfen. CloudTrail Mithilfe der Protokolldateivali dierung kann festgestellt werden, ob eine Protokoll datei geändert oder gelöscht wurde oder ob sie nach der Übermittlung CloudTrail unverände rt geblieben ist. Dieses Feature wurde mit dem Branchens tandard entsprech enden Algorithmen entwickelt: SHA-256 für die Hashfunktion und SHA-256 mit RSA für digitale Signature n. Aus diesem Grund ist es rechnerisch unmöglich, CloudTrai l Protokolldateien unbemerkt zu ändern, zu löschen oder zu fälschen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
SI-7(1)	Das Informationssystem führt mindestens einmal im Monat eine Integritätsprüfung bei sicherheitsrelevanten Ereignissen durch.	ec2-managed-instance-managed-by-systems	Eine Bestandsaufnahme der Softwareplattformen und Anwendungen innerhalb des Unternehmens ist möglich, indem Amazon Elastic Compute Cloud (Amazon EC2) - Instances mit AWS Systems Manager verwaltet werden. Verwenden Sie AWS Systems Manager, um detaillierte Systemkonfigurationen, Betriebssystem-Patch-Levels, Namen und Typ der Dienste, Softwareinstallationen, Anwendungsname, Herausgeber und Version sowie andere Details zu Ihrer Umgebung bereitzustellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
SI-7(1)	Das Informati onssystem führt mindestens einmal im Monat eine Integritätsprüfung bei sicherheitsrelevanten Ereignissen durch.	ec2-check managedin stance-patch-compl iance-status	Aktivieren Sie diese Regel, um bei der Identifizierung und Dokumentation von Sicherheitslücken in Amazon Elastic Compute Cloud (Amazon EC2) zu helfen. Die Regel prüft, ob die EC2 Amazon-Instance die Patch-Konformität im AWS Systems Manager gemäß den Richtlinien und Verfahren Ihrer Organisation einhält.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
SI-7	Die Organisation verwendet Tools zur Integritätsprüfung , um unbefugte Änderungen an [Zuweisung: von der Organisation definiert e Software, Firmware und Informationen] zu erkennen.	cloud-trail-log-file-Validierung aktiviert	Verwenden Sie die AWS CloudTrail Protokolldateivali dierung, um die Integrität von Protokoll en zu überprüfen. CloudTrail Mithilfe der Protokolldateivali dierung kann festgestellt werden, ob eine Protokoll datei geändert oder gelöscht wurde oder ob sie nach der Übermittlung CloudTrail unverände rt geblieben ist. Dieses Feature wurde mit dem Branchens tandard entsprech enden Algorithmen entwickelt: SHA-256 für die Hashfunktion und SHA-256 mit RSA für digitale Signature n. Aus diesem Grund ist es rechnerisch unmöglich, CloudTrai l Protokolldateien unbemerkt zu ändern, zu löschen oder zu fälschen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
SI-11	Das Informati onssystem: a. Generiert Fehlermel dungen mit für Korrekturmaßnahmen erforderlichen Informationen, ohne Informationen preiszugeben, die von Angreifern ausgenutzt werden könnten; und b. Zeigt Fehlermeldungen nur für [Zuweisung: von der Organisation ernanntes Personal oder definierte Rollen] an. Zusätzliche Hinweise: Organizat ions prüfen sorgfälti g, welche structure /content of error messages. The extent to which information systems are able to identify and handle error conditions is guided by organizat ional policy and operational requireme nts. Information that could be exploited by adversaries	api-gw-execution-l ogging-aktiviert	Die API-Gateway-Protokollierung zeigt detaillierte Ansichten der Benutzer, die auf die API zugegriff en haben, und wie diese Benutzer auf die API zugegriff en haben. Diese Einblicke ermöglichen die Transparenz von Benutzeraktivitäten.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
	includes, for example, erroneous logon attempts with passwords entered by mistake as the username, mission/business Informationen aus aufgezeichneten Informationen und persönlichen Informationen wie Kontonummern, Sozialversicherungsnummern und Kreditkartennummern abgeleitet werden können (sofern nicht ausdrücklich angegeben). Darüber hinaus können Fehlermeldungen einen verdeckten Kanal für die Übertragung von Informationen bieten. Verwandte Kontrollen: AU-2, AU-3, SC-31. Verbesserungen der Kontrolle: Keine. Referenzen: Keine.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
SI-11	Das Informati onssystem: a. Generiert Fehlermel dungen mit für Korrekturmaßnahmen erforderlichen Informationen, ohne Informationen preiszugeben, die von Angreifern ausgenutzt werden könnten; und b. Zeigt Fehlermeldungen nur für [Zuweisung: von der Organisation ernanntes Personal oder definierte Rollen] an. Zusätzliche Hinweise: Organizat ions prüfen sorgfälti g, welche structure /content of error messages. The extent to which information systems are able to identify and handle error conditions is guided by organizat ional policy and operational requireme nts. Information that could be exploited by adversaries	cloud-trail-cloud-watch-Protokolle aktiviert	Verwenden Sie Amazon CloudWatc h , um Protokoll ereignisaktivitäten zentral zu sammeln und zu verwalten. Die Aufnahme von AWS CloudTrail Daten liefert Einzelheiten zu den API-Aufrufaktivitä ten in Ihrem AWS-Konto.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
	includes, for example, erroneous logon attempts with passwords entered by mistake as the username, mission/business Informationen aus aufgezeichneten Informationen und persönlichen Informationen wie Kontonummern, Sozialversicherungsnummern und Kreditkartennummern abgeleitet werden können (sofern nicht ausdrücklich angegeben). Darüber hinaus können Fehlermeldungen einen verdeckten Kanal für die Übertragung von Informationen bieten. Verwandte Kontrollen: AU-2, AU-3, SC-31. Verbesserungen der Kontrolle: Keine. Referenzen: Keine.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
SI-11	Das Informati onssystem: a. Generiert Fehlermel dungen mit für Korrekturmaßnahmen erforderlichen Informationen, ohne Informationen preiszugeben, die von Angreifern ausgenutzt werden könnten; und b. Zeigt Fehlermeldungen nur für [Zuweisung: von der Organisation ernanntes Personal oder definierte Rollen] an. Zusätzliche Hinweise: Organizat ions prüfen sorgfälti g, welche structure /content of error messages. The extent to which information systems are able to identify and handle error conditions is guided by organizat ional policy and operational requireme nts. Information that could be exploited by adversaries	codebuild-project-logging-enabled	Stellen Sie sicher, dass die AWS CodeBuild Projektpr otokollierung aktiviert ist, damit Ihre Build-Ausgabeproto kolle entweder an Amazon CloudWatc h oder Amazon Simple Storage Service (Amazon S3) gesendet werden. Build-Ausgabeproto kolle enthalten detaillierte Informati onen zu Ihrem Build-Projekt.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
	includes, for example, erroneous logon attempts with passwords entered by mistake as the username, mission/business Informationen aus aufgezeichneten Informationen und persönlichen Informationen wie Kontonummern, Sozialversicherungsnummern und Kreditkartennummern abgeleitet werden können (sofern nicht ausdrücklich angegeben). Darüber hinaus können Fehlermeldungen einen verdeckten Kanal für die Übertragung von Informationen bieten. Verwandte Kontrollen: AU-2, AU-3, SC-31. Verbesserungen der Kontrolle: Keine. Referenzen: Keine.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
SI-11	Das Informati onssystem: a. Generiert Fehlermel dungen mit für Korrekturmaßnahmen erforderlichen Informationen, ohne Informationen preiszugeben, die von Angreifern ausgenutzt werden könnten; und b. Zeigt Fehlermeldungen nur für [Zuweisung: von der Organisation ernanntes Personal oder definierte Rollen] an. Zusätzliche Hinweise: Organizat ions prüfen sorgfälti g, welche structure /content of error messages. The extent to which information systems are able to identify and handle error conditions is guided by organizat ional policy and operational requireme nts. Information that could be exploited by adversaries	elasticsearch-logs-to-cloudwatch	Stellen Sie sicher, dass für Amazon OpenSearch Service-Domains Fehlerpro tokolle aktiviert und zur Aufbewahrung und Beantwortung an Amazon CloudWatc h Logs gestreamt werden. Domain-Fehlerprotokolle sind bei Sicherhei ts- und Zugriffsp rüfungen sowie bei der Diagnose von Verfügbarkeitsprob lemen nützlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
	includes, for example, erroneous logon attempts with passwords entered by mistake as the username, mission/business Informationen aus aufgezeichneten Informationen und persönlichen Informationen wie Kontonummern, Sozialversicherungsnummern und Kreditkartennummern abgeleitet werden können (sofern nicht ausdrücklich angegeben). Darüber hinaus können Fehlermeldungen einen verdeckten Kanal für die Übertragung von Informationen bieten. Verwandte Kontrollen: AU-2, AU-3, SC-31. Verbesserungen der Kontrolle: Keine. Referenzen: Keine.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
SI-11	Das Informati onssystem: a. Generiert Fehlermel dungen mit für Korrekturmaßnahmen erforderlichen Informationen, ohne Informationen preiszugeben, die von Angreifern ausgenutzt werden könnten; und b. Zeigt Fehlermeldungen nur für [Zuweisung: von der Organisation ernanntes Personal oder definierte Rollen] an. Zusätzliche Hinweise: Organizat ions prüfen sorgfälti g, welche structure /content of error messages. The extent to which information systems are able to identify and handle error conditions is guided by organizat ional policy and operational requireme nts. Information that could be exploited by adversaries	s-3 bucket-logging-enabled	Die Amazon Simple Storage Service (Amazon S3)-Serverzugriffs protokollierung bietet eine Methode zur Überwachu ng des Netzwerks im Hinblick auf potenzielle Cybersich erheitsereignisse. Die Ereignisse werden überwacht, indem detaillierte Aufzeichn ungen über die Anfragen erfasst werden, die an einen Amazon-S3-Bucket gestellt wurden. Jeder Zugriffsprotokolle intrag enthält Details zu einer einzelnen Zugriffsanfrage. Zu den Details gehören Anforderer, Bucket-Name, Anforderu ngszeit, Anforderu ngsaktion, Antwortst atus und Fehlercode, falls relevant.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
	includes, for example, erroneous logon attempts with passwords entered by mistake as the username, mission/business Informationen aus aufgezeichneten Informationen und persönlichen Informationen wie Kontonummern, Sozialversicherungsnummern und Kreditkartennummern abgeleitet werden können (sofern nicht ausdrücklich angegeben). Darüber hinaus können Fehlermeldungen einen verdeckten Kanal für die Übertragung von Informationen bieten. Verwandte Kontrollen: AU-2, AU-3, SC-31. Verbesserungen der Kontrolle: Keine. Referenzen: Keine.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
SI-11	Das Informati onssystem: a. Generiert Fehlermel dungen mit für Korrekturmaßnahmen erforderlichen Informationen, ohne Informationen preiszugeben, die von Angreifern ausgenutzt werden könnten; und b. Zeigt Fehlermeldungen nur für [Zuweisung: von der Organisation ernanntes Personal oder definierte Rollen] an. Zusätzliche Hinweise: Organizat ions prüfen sorgfälti g, welche structure /content of error messages. The extent to which information systems are able to identify and handle error conditions is guided by organizat ional policy and operational requireme nts. Information that could be exploited by adversaries	vpc-flow-logs-enabled	VPC-Flow-Protokoll e erfassen detaillierte Informationsdatens ätze über den IP-Datenverkehr, der zu und von Netzwerkschnittste llen in Ihrer Amazon Virtual Private Cloud (Amazon VPC) fließt. Standardmäßig enthalten Flow-Prot okolldatensätze Werte für die verschiedenen Komponenten des IP-Flows, einschlie ßlich Quelle, Ziel und Protokoll.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
	includes, for example, erroneous logon attempts with passwords entered by mistake as the username, mission/business Informationen aus aufgezeichneten Informationen und persönlichen Informationen wie Kontonummern, Sozialversicherungsnummern und Kreditkartennummern abgeleitet werden können (sofern nicht ausdrücklich angegeben). Darüber hinaus können Fehlermeldungen einen verdeckten Kanal für die Übertragung von Informationen bieten. Verwandte Kontrollen: AU-2, AU-3, SC-31. Verbesserungen der Kontrolle: Keine. Referenzen: Keine.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
SI-11	Das Informationssystem: a. Generiert Fehlermeldungen mit für Korrekturmaßnahmen erforderlichen Informationen, ohne Informationen preiszugeben, die von Angreifern ausgenutzt werden könnten; und b. Zeigt Fehlermeldungen nur für [Zuweisung: von der Organisation ernanntes Personal oder definierte Rollen] an. Zusätzliche Hinweise: Organizations prüfen sorgfältig, welche structure /content of error messages. The extent to which information systems are able to identify and handle error conditions is guided by organizational policy and operational requirements. Information that could be exploited by adversaries	opensearch-logs-to-cloudwatch	Stellen Sie sicher, dass für Amazon OpenSearch Service-Domains Fehlerprotokolle aktiviert und zur Aufbewahrung und Beantwortung an Amazon CloudWatch Logs gestreamt werden. OpenSearch Service-Fehlerprotokolle können bei Sicherheits- und Zugriffsprüfungen helfen und bei der Diagnose von Verfügbarkeitsproblemen helfen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
	includes, for example, erroneous logon attempts with passwords entered by mistake as the username, mission/business Informationen aus aufgezeichneten Informationen und persönlichen Informationen wie Kontonummern, Sozialversicherungsnummern und Kreditkartennummern abgeleitet werden können (sofern nicht ausdrücklich angegeben). Darüber hinaus können Fehlermeldungen einen verdeckten Kanal für die Übertragung von Informationen bieten. Verwandte Kontrollen: AU-2, AU-3, SC-31. Verbesserungen der Kontrolle: Keine. Referenzen: Keine.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
SI-12	Die Organisation verarbeitet und speichert die Informationen innerhalb des Informationssystems und die aus dem System ausgegebenen Informationen gemäß den geltenden Bundesgesetzen, Verordnungen, Richtlinien, Richtlinien, Vorschriften, Standards und betrieblichen Anforderungen.	aurora-resources-protected-by-Backup-Plan	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon Aurora Aurora-Ressourcen Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
SI-12	Die Organisation verarbeitet und speichert die Informationen innerhalb des Informationssystems und die aus dem System ausgegebenen Informationen gemäß den geltenden Bundesgesetzen, Verordnungen, Richtlinien, Richtlinien, Vorschriften, Standards und betrieblichen Anforderungen.	backup-plan-min-frequency-and-min-retention-check	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihr AWS Backup-Plan auf eine Mindestfrequenz und Aufbewahrung festgelegt ist. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen. Mit dieser Regel können Sie die Parameter requiredFrequencyValue (Config default: 1), requiredRetentionDays (Config default: 35) und requiredFrequencyUnit

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
			(Config default: days) festlegen. Der tatsächliche Wert muss den Anforderungen Ihrer Organisation entsprechen.
SI-12	Die Organisation verarbeitet und speichert die Informationen innerhalb des Informationssystems und die aus dem System ausgegebenen Informationen gemäß den geltenden Bundesgesetzen, Verordnungen, Richtlinien, Richtlinien, Vorschriften, Standards und betrieblichen Anforderungen.	cw-loggroup-retention-period-überprüfen	Stellen Sie sicher, dass die Ereignisprotokolldaten für Ihre Protokollgruppen über eine Mindestdauer aufbewahrt werden, um die Fehlerbehebung und forensische Untersuchungen zu unterstützen. Fehlende frühere Ereignisprotokolldaten erschweren die Rekonstruierung und Identifizierung potenziell schädlicher Ereignisse.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
SI-12	Die Organisation verarbeitet und speichert die Informationen innerhalb des Informationssystems und die aus dem System ausgegebenen Informationen gemäß den geltenden Bundesgesetzen, Verordnungen, Richtlinien, Richtlinien, Vorschriften, Standards und betrieblichen Anforderungen.	dynamodb-resources-protected-by-Ersatzplan	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon DynamoDB DynamoDB-Ressourcen Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
SI-12	Die Organisation verarbeitet und speichert die Informationen innerhalb des Informationssystems und die aus dem System ausgegebenen Informationen gemäß den geltenden Bundesgesetzen, Verordnungen, Richtlinien, Richtlinien, Vorschriften, Standards und betrieblichen Anforderungen.	ebs-resources-protected-by-Backup-Plan	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon Elastic Block Store (Amazon EBS) -Ressourcen Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
SI-12	Die Organisation verarbeitet und speichert die Informationen innerhalb des Informationssysteme und die aus dem System ausgegebenen Informationen gemäß den geltenden Bundesgesetzen, Verordnungen, Richtlinien, Richtlinien, Vorschriften, Standards und betrieblichen Anforderungen.	ec2--Plan resources-protected-by-backup	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon Elastic Compute Cloud (Amazon EC2) -Ressourcen Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
SI-12	Die Organisation verarbeitet und speichert die Informationen innerhalb des Informationssystems und die aus dem System ausgegebenen Informationen gemäß den geltenden Bundesgesetzen, Verordnungen, Richtlinien, Richtlinien, Vorschriften, Standards und betrieblichen Anforderungen.	efs-resources-protected-by-Backup-Plan	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon Elastic File System (Amazon EFS) -Dateisysteme Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
SI-12	Die Organisation verarbeitet und speichert die Informationen innerhalb des Informationssystems und die aus dem System ausgegebenen Informationen gemäß den geltenden Bundesgesetzen, Verordnungen, Richtlinien, Richtlinien, Vorschriften, Standards und betrieblichen Anforderungen.	fsx-resources-protected-by-Backup-Plan	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre FSx Amazon-Dateisysteme Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
SI-12	Die Organisation verarbeitet und speichert die Informationen innerhalb des Informationssystems und die aus dem System ausgegebenen Informationen gemäß den geltenden Bundesgesetzen, Verordnungen, Richtlinien, Richtlinien, Vorschriften, Standards und betrieblichen Anforderungen.	rds-resources-protected-by-Backup-Plan	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon Relational Database Service (Amazon RDS) -Ressourcen Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
SI-12	Die Organisation verarbeitet und speichert die Informationen innerhalb des Informationssystems und die aus dem System ausgegebenen Informationen gemäß den geltenden Bundesgesetzen, Verordnungen, Richtlinien, Richtlinien, Vorschriften, Standards und betrieblichen Anforderungen.	redshift-backup-enabled	Stellen Sie zur Unterstützung der Datensicherungsprozesse sicher, dass Ihre Amazon-Redshift-Cluster über automatisierte Snapshots verfügen. Wenn automatisierte Snapshots für einen Cluster aktiviert sind, erstellt Redshift in regelmäßigen Abständen Snapshots dieses Clusters. Standardmäßig erstellt Redshift alle acht Stunden oder alle 5 GB einen Snapshot für jeden Knoten mit Datenänderungen oder je nachdem, was zuerst eintritt.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
SI-12	Die Organisation verarbeitet und speichert die Informationen innerhalb des Informationssystems und die aus dem System ausgegebenen Informationen gemäß den geltenden Bundesgesetzen, Verordnungen, Richtlinien, Richtlinien, Vorschriften, Standards und betrieblichen Anforderungen.	db-instance-backup-enabled	Die Sicherungsfunktion von Amazon RDS erstellt Sicherungen Ihrer Datenbanken und Transaktionsprotokolle. Amazon RDS erstellt einen Snapshot für das Speichervolume Ihrer DB-Instance, sodass die gesamte DB-Instance gesichert wird. Sie können im System spezifische Aufbewahrungsfristen festlegen, um Ihre Ausfallsicherheitsanforderungen zu erfüllen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
SI-12	Die Organisation verarbeitet und speichert die Informationen innerhalb des Informationssystems und die aus dem System ausgegebenen Informationen gemäß den geltenden Bundesgesetzen, Verordnungen, Richtlinien, Richtlinien, Vorschriften, Standards und betrieblichen Anforderungen.	dynamodb-pitr-enabled	Aktivieren Sie diese Regel, um zu überprüfen, ob die Informationen gesichert wurden. Es verwaltet auch die Backups, indem es sicherstellt, dass die point-in-time Wiederherstellung in Amazon DynamoDB aktiviert ist. Bei der Wiederherstellung werden fortlaufende Backups Ihrer Tabelle für die letzten 35 Tage gespeichert.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
SI-12	Die Organisation verarbeitet und speichert die Informationen innerhalb des Informationssysteme und die aus dem System ausgegebenen Informationen gemäß den geltenden Bundesgesetzen, Verordnungen, Richtlinien, Richtlinien, Vorschriften, Standards und betrieblichen Anforderungen.	elasticache-redis-cluster-automatic-Backup-Prüfung	Wenn automatische Backups aktiviert sind, ElastiCache erstellt Amazon täglich ein Backup des Clusters. Die Sicherung kann für eine von Ihrer Organisation festgelegte Anzahl von Tagen aufbewahrt werden. Automatische Backups schützen vor Datenverlust. Bei einem Ausfall können Sie einen neuen Cluster erstellen, der Ihre Daten aus dem aktuellen Backup wiederherstellt.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
SI-12	Die Organisation verarbeitet und speichert die Informationen innerhalb des Informationssysteme und die aus dem System ausgegebenen Informationen gemäß den geltenden Bundesgesetzen, Verordnungen, Richtlinien, Richtlinien, Vorschriften, Standards und betrieblichen Anforderungen.	s-3 bucket-versioning-enabled	Die Versionsverwaltung von Amazon Simple Storage Service (Amazon S3)-Buckets hilft dabei, mehrere Varianten eines Objekts im selben Amazon-S3-Bucket zu speichern. Verwenden Sie die Versionsverwaltung, um sämtliche Versionen aller Objekte in Ihrem Amazon-S3-Bucket zu speichern, abzurufen oder wiederherzustellen. Mit der Versionsverwaltung können Sie Versionen sowohl nach unbeabsichtigten Benutzeraktionen als auch nach Anwendungsfehlern problemlos wiederherstellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
SI-16	Das Informati onssystem implement iert [Zuweisung: von der Organisation festgelegte Sicherhei tsvorkehrungen], um seinen Speicher vor unberechtigten Codeausführungen zu schützen. Zusätzlic he Empfehlung: Einige Angreifer beabsichtigen, Code in nicht ausführbaren Speicherbereichen oder an untersagt en Speichero rten auszuführen. Mögliche Sicherhei tsmaßnahmen zum Schutz des Speichers sind beispielsweise die Verhinderung der Datenausf ührung und die zufällige Anordnung des Adressrau ms. Schutzmaß nahmen zur Verhinder ung der Datenausf ührung können entweder durch Hardware oder durch	ecs-task-definition-memory-hartes Limit	Durch die Begrenzun g des Speichers, der Ihren Container n im Amazon Elastic Container Service (ECS) maximal zur Verfügung steht, verhindern Sie eine Ressourcenüberlast ung im Falle eines schädlichen Zugriffs auf Ihre Container.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
	Software erzwungen werden, wobei die Hardware die effektive re Methode ist. Verwandte Kontrolle n: AC-25, SC-3. Verbesserungen der Kontrolle: Keine. Referenzen: Keine.		

Vorlage

Die Vorlage ist verfügbar unter GitHub: Operational Best Practices for FedRAMP (Moderate).

Bewährte Betriebspraktiken für FedRAMP (High Part 1)

Konformitätspakete bieten ein allgemeines Compliance-Framework, das es Ihnen ermöglicht, mithilfe verwalteter oder benutzerdefinierter Regeln und Abhilfemaßnahmen Kontrollen zur Sicherheits-, Betriebs- oder Kostenoptimierung durchzuführen. AWS Config AWS Config Conformance Packs dienen als Beispielvorlagen nicht dazu, die vollständige Einhaltung eines bestimmten Governance- oder Compliance-Standards sicherzustellen. Sie sind dafür verantwortlich, selbst zu beurteilen, ob Ihre Nutzung der Services den geltenden gesetzlichen und behördlichen Anforderungen entspricht.

Im Folgenden finden Sie ein Beispiel für eine Zuordnung zwischen dem Federal Risk and Authorization Management Program (FedRAMP) und AWS verwalteten Konfigurationsregeln. Jede Config-Regel gilt für eine bestimmte AWS Ressource und bezieht sich auf ein oder mehrere FedRAMP-Steuerelemente. Eine FedRAMP-Kontrolle kann mehreren Config-Regeln zugeordnet werden. In der folgenden Tabelle finden Sie weitere Informationen und Anleitungen zu diesen Zuordnungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-17(1)	Das Informati onssystem überwacht	securityhub-enabled	AWS Security Hub hilft bei der

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	und kontrolliert die Remote-Zugriffsmethoden.		Überwachung von unbefugtem Personal, Verbindungen, Geräten und Software. AWS Security Hub aggregiert, organisiert und priorisiert die Sicherheitswarnungen oder Ergebnisse mehrerer Dienste. AWS Einige dieser Dienste sind Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer und AWS Firewall Manager sowie AWS Partnerlösungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-17(1)	Das Informati onssystem überwacht und kontrolliert die Remote-Zugriffsmet hoden.	guardduty-enabled-centralized	Amazon GuardDuty kann mithilfe von Threat Intellige nce Feeds helfen, potenzielle Cybersich erheitsereignisse zu überwachen und zu erkennen. Dazu gehören Listen mit bösartigen IPs und maschinel len Lernmethoden zur Identifizierung unerwarteter, nicht autorisierter und bösartiger Aktivitäten in Ihrer AWS Cloud-Umgebung.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-17(1)	Das Informati onssystem überwacht und kontrolliert die Remote-Zugriffsmet hoden.	dms-replication-not-public	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass auf DMS-Replikationsin stanzen nicht öffentlic h zugegriffen werden kann. DMS-Repli kations-Instances können vertrauli che Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.
AC-17(1)	Das Informati onssystem überwacht und kontrolliert die Remote-Zugriffsmet hoden.	ebs-snapshot-public-restorable-überprüfen	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass EBS-Snapshots nicht öffentlich wiederher stellbar sind. EBS-Volume-Snapsho ts können vertrauli che Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-17(1)	Das Informati onssystem überwacht und kontrolliert die Remote-Zugriffsmet hoden.	ec2- instance-no-public-ip	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon Elastic Compute Cloud (Amazon EC2) - Instances nicht öffentlich zugänglich sind. EC2 Amazon-Instances können vertrauliche Informati onen enthalten, und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-17(1)	Das Informati onssystem überwacht und kontrolliert die Remote-Zugriffsmet hoden.	elasticsearch-in-vpc-only	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherste llen, dass sich Amazon OpenSearc h OpenSearch Service (Service) - Domains innerhalb einer Amazon Virtual Private Cloud (Amazon VPC) befinden. Eine OpenSearch Service-Domain innerhalb einer Amazon VPC ermöglicht die sichere Kommunikation zwischen OpenSearc h Service und anderen Services innerhalb der Amazon VPC, ohne dass ein Internet-Gateway, ein NAT-Gerät oder eine VPN-Verbindung erforderlich ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-17(1)	Das Informati onssystem überwacht und kontrolliert die Remote-Zugriffsmet hoden.	emr-master-no-public-ip	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon EMR-Clust er-Masterknoten nicht öffentlich zugänglic h sind. Amazon-EM R-Cluster-Hauptkno ten können vertrauli che Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-17(1)	Das Informati onssystem überwacht und kontrolliert die Remote-Zugriffsmet hoden.	ec2- instances-in-vpc	Stellen Sie Amazon Elastic Compute Cloud (Amazon EC2) -Instances innerhalb einer Amazon Virtual Private Cloud (Amazon VPC) bereit, um eine sichere Kommunika tion zwischen einer Instance und anderen Services innerhalb der Amazon VPC zu ermöglichen, ohne dass ein Internet-Gateway, ein NAT-Gerät oder eine VPN-Verbindung erforderlich ist. Der gesamte Datenverk ehr bleibt sicher in der AWS Cloud. Domains, die sich innerhalb einer VPC befinden, verfügen aufgrund ihrer logischen Isolierun g im Vergleich zu Domains mit öffentlic hen Endpunkten über eine zusätzlic he Sicherheitsebene. Weisen Sie EC2

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			Amazon-Instances einer Amazon-VPC zu, um den Zugriff ordnungsgemäß zu verwalten.
AC-17(1)	Das Informati onssystem überwacht und kontrolliert die Remote-Zugriffsmet hoden.	lambda-function-pu blic-access-verboten	Verwalten Sie den Zugriff auf Ressource n in der AWS Cloud, indem Sie sicherste llen, dass AWS Lambda-Funktionen nicht öffentlich zugänglich sind. Der öffentliche Zugriff kann möglicherweise die Verfügbarkeit von Ressourcen beeinträc htigen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-17(1)	Das Informati onssystem überwacht und kontrolliert die Remote-Zugriffsmet hoden.	lambda-inside-vpc	Stellen Sie AWS Lambda-Funktionen in einer Amazon Virtual Private Cloud (Amazon VPC) bereit, um eine sichere Kommunika tion zwischen einer Funktion und anderen Diensten innerhalb der Amazon VPC zu gewährleisten. Bei dieser Konfiguration sind kein Internet-Gateway, kein NAT-Gerät und keine VPN-Verbindung erforderlich. Der gesamte Datenverk ehr bleibt sicher in der Cloud. AWS Domains, die sich innerhalb einer VPC befinden, verfügen aufgrund ihrer logischen Isolierun g im Vergleich zu Domains mit öffentlic hen Endpunkten über eine zusätzliche Sicherheitsebene. Um den Zugriff ordnungsg emäß zu verwalten,

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			sollten AWS Lambda-Funktionen einer VPC zugewiesen werden.
AC-17(1)	Das Informationssystem überwacht und kontrolliert die Remote-Zugriffsmethoden.	rds-instance-public-access-überprüfen	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Relational Database Service (Amazon RDS) -Instances nicht öffentlich sind. Amazon-RDS-Datenbank-Instances können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-17(1)	Das Informati onssystem überwacht und kontrolliert die Remote-Zugriffsmet hoden.	rds-snapshots-public-prohibited	Verwalten Sie den Zugriff auf Ressource n in der AWS Cloud, indem Sie sicherste llen, dass Amazon Relational Database Service (Amazon RDS) -Instance s nicht öffentlic h sind. Amazon-RDS-Datenbank-Instances können vertrauliche Informati onen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-17(1)	Das Informati onssystem überwacht und kontrolliert die Remote-Zugriffsmet hoden.	redshift-cluster-public-access-überprüfen	Verwalten Sie den Zugriff auf Ressource n in der AWS Cloud, indem Sie sicherste llen, dass Amazon Redshift Redshift-Cluster nicht öffentlic h sind. Amazon-Re dshift-Cluster können vertrauliche Informati onen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-17(1)	Das Informati onssystem überwacht und kontrolliert die Remote-Zugriffsmet hoden.	restricted-common-ports	Verwalten Sie den Zugriff auf Ressource n in der AWS Cloud, indem Sie sicherste llen, dass gemeinsam e Ports für Amazon Elastic Compute Cloud (Amazon EC2) -Sicherhe itsgruppen eingeschr ränkt sind. Wenn der Zugriff auf Ports nicht auf vertrauen swürdige Quellen beschränkt wird, kann dies zu Angriffen auf die Verfügbar keit, Integrität und Vertraulichkeit von Systemen führen. Mit dieser Regel können Sie optional die Parameter blockedPo rt1–blockedPort5 festlegen (Standard konfigurationen: 20, 21, 3389, 3306, 4333). Die tatsächli chen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-17(1)	Das Informati onssystem überwacht und kontrolliert die Remote-Zugriffsmet hoden.	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) Security Groups können bei der Verwaltung des Netzwerkzugriffs helfen, indem sie eine statusbeh aftete Filterung von eingehendem und ausgehendem Netzwerkverkehr zu Ressourcen bereitste llen. AWS Wenn Sie eingehenden (oder entfernten) Datenverk ehr von 0.0.0.0/0 bis Port 22 auf Ihren Ressourcen nicht zulassen, können Sie den Remote-Zugriff einschränken.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-17(1)	Das Informati onssystem überwacht und kontrolliert die Remote-Zugriffsmet hoden.	account-level-publ ic-accesss3-Blöcke-periodisch	Verwalten Sie den Zugriff auf Ressource n in der AWS Cloud, indem Sie sicherste llen, dass Amazon Simple Storage Service (Amazon S3) -Buckets nicht öffentlich zugänglic h sind. Diese Regel trägt dazu bei, sensible Daten vor unbefugten Remote-Benutzern zu schützen, indem sie den öffentlichen Zugriff verhinder t. Mit dieser Regel können Sie optional die Parameter ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) und restrictPublicBuck ets Parameter (Config Default: True) festlegen. Die tatsächlichen Werte müssen den Richtlini

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			en Ihrer Organisation entsprechen.
AC-17(1)	Das Informati onssystem überwacht und kontrolliert die Remote-Zugriffsmet hoden.	s3 bucket-level-public-access - verboten	Verwalten Sie den Zugriff auf Ressource n in der AWS Cloud, indem Sie sicherste llen, dass Amazon Simple Storage Service (Amazon S3) -Buckets nicht öffentlich zugänglic h sind. Diese Regel trägt dazu bei, sensible Daten vor unbefugten Remote-Benutzern zu schützen, indem sie den öffentlichen Zugriff auf Bucket-Eb ene verhindert.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-17(1)	Das Informati onssystem überwacht und kontrolliert die Remote-Zugriffsmet hoden.	s-3 bucket-public-read -prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie nur autorisierten Benutzern, Prozessen und Geräten Zugriff auf Amazon Simple Storage Service (Amazon S3) - Buckets gewähren. Die Verwaltung des Zugriffs sollte mit der Klassifizierung der Daten übereinst immen.
AC-17(1)	Das Informati onssystem überwacht und kontrolliert die Remote-Zugriffsmet hoden.	s-3 bucket-public-writ e-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie nur autorisierten Benutzern, Prozessen und Geräten Zugriff auf Amazon Simple Storage Service (Amazon S3) - Buckets gewähren. Die Verwaltung des Zugriffs sollte mit der Klassifizierung der Daten übereinst immen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-17(1)	Das Informati onssystem überwacht und kontrolliert die Remote-Zugriffsmet hoden.	sagemaker-notebook -no-direct-Interne tzugang	Verwalten Sie den Zugriff auf Ressource n in der AWS Cloud, indem Sie sicherste llen, dass SageMaker Amazon-Notebooks keinen direkten Internetzugang zulassen. Indem Sie direkten Internetz ugang blockieren, vermeiden Sie, dass unbefugte Benutzer auf sensible Daten zugreifen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-17(1)	Das Informati onssystem überwacht und kontrolliert die Remote-Zugriffsmet hoden.	subnet-auto-assign-public-ip-deaktiviert	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon Virtual Private Cloud (VPC) -Subnetzen nicht automatisch eine öffentliche IP-Adress e zugewiesen wird. Amazon Elastic Compute Cloud (EC2) -Instances, die in Subnetzen gestartet werden, in denen dieses Attribut aktiviert ist, haben ihrer primären Netzwerkschnittste lle eine öffentliche IP-Adresse zugewiesen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-17(1)	Das Informati onssystem überwacht und kontrolliert die Remote-Zugriffsmet hoden.	vpc-default-security-group-geschlossen	Sicherheitsgruppen von Amazon Elastic Compute Cloud (Amazon EC2) können bei der Verwaltung des Netzwerkzugriffs helfen, indem sie eine statusbehaftete Filterung des ein- und ausgehenden Netzwerkverkehrs zu Ressourcen bereitstellen. AWS Die Beschränk ung des gesamten Datenverkehrs auf die Standardsicherheit sgruppe hilft dabei, den Fernzugriff auf Ihre Ressourcen einzuschränken. AWS

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-17(1)	Das Informati onssystem überwacht und kontrolliert die Remote-Zugriffsmet hoden.	vpc-sg-open-only-to-authorized-ports	Verwalten Sie den Zugriff auf Ressource n in der AWS Cloud, indem Sie sicherste llen, dass gemeinsam e Ports für Amazon Elastic Compute Cloud (Amazon EC2) -Sicherhe itsgruppen eingeschr änkt sind. Wenn der Zugriff auf Ports nicht auf vertrauen swürdige Quellen beschränkt wird, kann dies zu Angriffen auf die Verfügbar keit, Integrität und Vertraulichkeit von Systemen führen. Durch die Beschränk ung des Zugriffs auf Ressourcen innerhalb einer Sicherhei tsgruppe aus dem Internet (0.0.0.0/0) kann der Remote-Zugriff auf interne Systeme gesteuert werden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-17(2)	Das Informationssystem implementiert kryptografische Mechanismen, um die Vertraulichkeit und Integrität von Remote-Zugriffssitzungen zu schützen.	alb-http-to-https-Weiterleitungsprüfung	Um Daten während der Übertragung zu schützen, stellen Sie sicher, dass Ihr Application Load Balancer unverschlüsselte HTTP-Anfragen automatisch an HTTPS umleitet. Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.
AC-17(2)	Das Informationssystem implementiert kryptografische Mechanismen, um die Vertraulichkeit und Integrität von Remote-Zugriffssitzungen zu schützen.	redshift-require-tls-ssl	Stellen Sie sicher, dass Ihre Amazon-Redshift-Cluster eine TLS/SSL-Verschlüsselung erfordern, um eine Verbindung zu SQL-Clients herzustellen. Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-17(2)	Das Informati onssystem implement iert kryptografische Mechanismen, um die Vertraulichkeit und Integrität von Remote-Zugriffssitzungen zu schützen.	acm-certificate-ex piration-check	Stellen Sie sicher, dass die Netzwerki ntegrität geschützt ist, indem Sie sicherste llen, dass X509-Zertifikate von AWS ACM ausgestel lt werden. Diese Zertifikate müssen gültig und dürfen nicht abgelaufen sein. Für diese Regel ist ein Wert für erforderlich daysToExpiration (Wert für bewährte AWS Grundregeln für Sicherheit: 90). Der tatsächliche Wert muss den Richtlini en Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-17(2)	Das Informationssystem implementiert kryptografische Mechanismen, um die Vertraulichkeit und Integrität von Remote-Zugriffssitzungen zu schützen.	s-3 bucket-ssl-requests-only	Um Daten während der Übertragung zu schützen, stellen Sie sicher, dass Ihre Amazon Simple Storage Service (Amazon S3)-Buckets Anfragen zur Verwendung von Secure Socket Layer (SSL)-Buckets erfordern. Da sensible Daten vorhanden sein können, sollten Sie die Verschlüsselung bei der Übertragung aktivieren, um diese Daten zu schützen.
AC-17(2)	Das Informationssystem implementiert kryptografische Mechanismen, um die Vertraulichkeit und Integrität von Remote-Zugriffssitzungen zu schützen.	elb-tls-https-listeners-nur	Stellen Sie sicher, dass Ihre Elastic Load Balancer (ELBs) mit SSL- oder HTTPS-Listenern konfiguriert sind. Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-17(2)	Das Informati onssystem implement iert kryptografische Mechanismen, um die Vertraulichkeit und Integrität von Remote-Zugriffssitzungen zu schützen.	elb-acm-certificate-required	FÜLLEN SIE DAS
AC-17(2)	Das Informati onssystem implement iert kryptografische Mechanismen, um die Vertraulichkeit und Integrität von Remote-Zugriffssitzungen zu schützen.	api-gw-ssl-enabled	Stellen Sie sicher, dass die REST-API-Stufen von Amazon API Gateway mit SSL-Zertifikaten konfiguri ert sind, damit Backend-Systeme überprüfen können, ob Anforderungen von API Gateway stammen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-2(1)	Die Organisation wendet automatisierte Mechanismen an, um die Verwaltung von Informationssystem konten zu unterstüt zen.	iam-password-policy	Die Identitäten und Anmeldeinformation en werden auf der Grundlage einer organisatorischen IAM-Passwortrichtlinie ausgestellt, verwaltet und verifiziert. Sie erfüllen oder übertreff en die Anforderungen von NIST SP 800-63 und dem Standard „Best Practices“ von AWS Foundatio nal Security für die Passwortstärke. Mit dieser Regel können Sie optional RequireUppercaseCh aracters (Wert für AWS grundlegende Sicherheitsbewährt e Methoden: wahr), RequireLowercaseCh aracters (Wert für bewährte Methoden für AWS grundlege nde Sicherheit: wahr), RequireSy mbols (Wert für bewährte Methoden für AWS grundlege nde Sicherheit:

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			wahr), RequireNumbers (Wert für bewährte Methoden für AWS grundlegende Sicherheit: wahr), MinimumPasswordLength (Wert für bewährte Methoden für AWS grundlegende Sicherheit: 14), PasswordReusePrevention (Wert für bewährte Methoden für AWS grundlegende Sicherheit: 24) und MaxPasswordAge (Wert für bewährte Methoden für AWS grundlegende Sicherheit: 90) für Ihr IAM festlegen Kennwortrichtlinie. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-2(1)	Die Organisation wendet automatisierte Mechanismen an, um die Verwaltung von Informationssystem konten zu unterstüt zen.	access-keys-rotated	Die Anmeldein formationen für autorisierte Geräte, Benutzer und Prozesse werden geprüft, indem sichergestellt wird, dass die IAM-Zugri ffsschlüssel gemäß den Richtlinien der Organisation rotiert werden. Das regelmäßige Ändern der Zugriffsschlüssel ist eine bewährte Sicherheitsmethode . Es verkürzt den Zeitraum, in dem ein Zugriffsschlüssel aktiv ist, und reduziert die Auswirkungen auf das Unternehmen, wenn die Schlüssel kompromittiert werden. Diese Regel erfordert einen Wert für die Zugriffsschlüssel-Rotation (Standard konfiguration: 90). Der tatsächliche Wert muss den Richtlini

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			en Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-2(1)	Die Organisation wendet automatisierte Mechanismen an, um die Verwaltung von Informationssystem konten zu unterstüt zen.	iam-user-unused-cr edentials-überprüfen	AWS Identity and Access Managemen t (IAM) kann Ihnen bei Zugriffsberechtigu ngen und Autorisie rungen helfen, indem es nach IAM-Passw örtern und Zugriffss chlüsseln sucht, die für einen bestimmte n Zeitraum nicht verwendet wurden. Wenn ungenutzte Anmeldeinformation en identifiziert werden, müssen Sie sie deaktivieren und/oder entfernen , da dies gegen das Prinzip der geringste n Berechtigung verstoßen könnte. Für diese Regel müssen Sie einen Wert für das maxCreden tialUsage Alter festlegen (Standard konfiguration: 90). Der tatsächliche Wert muss den Richtlini en Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-2(1)	Die Organisation wendet automatisierte Mechanismen an, um die Verwaltung von Informationssystem konten zu unterstützen.	iam-user-group-membership-überprüfen	AWS Identity and Access Management (IAM) kann Ihnen helfen, Zugriffsberechtigungen und Autorisierungen einzuschränken, indem sichergestellt wird, dass IAM-Benutzer Mitglieder mindestens einer Gruppe sind. Wenn Benutzern mehr Berechtigungen eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und Aufgabentrennung verstoßen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-2(1)	Die Organisation wendet automatisierte Mechanismen an, um die Verwaltung von Informationssystem konten zu unterstüt zen.	securityhub-enabled	AWS Security Hub hilft bei der Überwachung von unbefugtem Personal, Verbindun gen, Geräten und Software. AWS Security Hub aggregiert, organisie rt und priorisie rt die Sicherhei tswarnungen oder Ergebnisse mehrerer Dienste. AWS Einige dieser Dienste sind Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer und AWS Firewall Manager sowie AWS Partnerlösungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-2(1)	Die Organisation wendet automatisierte Mechanismen an, um die Verwaltung von Informationssystem konten zu unterstüt zen.	guardduty-enabled-centralized	Amazon GuardDuty kann mithilfe von Threat Intellige nce Feeds helfen, potenzielle Cybersich erheitsereignisse zu überwachen und zu erkennen. Dazu gehören Listen mit bösartigen IPs und maschinel len Lernmethoden zur Identifizierung unerwarteter, nicht autorisierter und bösartiger Aktivitäten in Ihrer AWS Cloud-Umgebung.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-2(1)	Die Organisation wendet automatisierte Mechanismen an, um die Verwaltung von Informationssystem konten zu unterstüt zen.	iam-no-inline-policy-überprüfen	Stellen Sie sicher, dass ein Benutzer, eine IAM-Rolle oder eine IAM-Gruppe (AWS Identity and Access Management) nicht über eine Inline-Richtlinie zur Zugriffsk ontrolle auf Systeme und Ressource n verfügt. AWS empfiehlt, verwaltet e Richtlinien anstelle von Inline-Richtlinien zu verwenden. Verwaltete Richtlini en ermöglichen Wiederverwendbarke it, Versionsverwaltung , Rollback und Delegierung der Berechtigungsverwa ltung.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-2(1)	Die Organisation wendet automatisierte Mechanismen an, um die Verwaltung von Informationssystem konten zu unterstüt zen.	iam-policy-no-stat ements-with-admin-access	AWS Identity and Access Managemen t (IAM) kann Ihnen dabei helfen, die Prinzipien der geringsten Rechte und der Aufgabent rennung in Zugriffsb erechtigungen und Autorisierungen zu integrieren und so zu verhindern, dass Richtlinien „Effect“: „Allow“ mit „Action“: „*“ anstelle von „Resource“: „*“ enthalten. Wenn Benutzern mehr Rechte eingeräum t werden, als für die Ausführung einer Aufgabe erforderl ich sind, kann dies gegen das Prinzip der geringsten Berechtigung und der Aufgabentrennung verstoßen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-2(1)	Die Organisation wendet automatisierte Mechanismen an, um die Verwaltung von Informationssystem konten zu unterstüt zen.	iam-root-access-key-überprüfen	Der Zugriff auf Systeme und Ressourcen kann gesteuert werden, indem überprüft wird, ob der Root-Benu tzer keine Zugriffss chlüssel mit seiner AWS Identity and Access Management (IAM) -Rolle verknüpft hat. Stellen Sie sicher, dass die Root-Zugr iffsschlüssel gelöscht werden. Erstellen und verwenden Sie stattdessen rollenbas ierte AWS Konten, um dem Prinzip der geringsten Funktiona lität Rechnung zu tragen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-2(1)	Die Organisation wendet automatisierte Mechanismen an, um die Verwaltung von Informationssystem konten zu unterstüt zen.	iam-user-mfa-enabled	Aktivieren Sie diese Regel, um den Zugriff auf Ressourcen in der AWS Cloud einzuschr änken. Diese Regel stellt sicher, dass die Multi-Faktor-Authe ntifizierung (MFA) für alle IAM-Benut zer aktiviert ist. MFA bietet eine weitere Schutzebene zusätzlic h zum Benutzern amen und Passwort. Reduzieren Sie Fälle von kompromittierten Konten, indem Sie MFA für IAM-Benutzer vorschreiben.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-2(1)	Die Organisation wendet automatisierte Mechanismen an, um die Verwaltung von Informationssystem konten zu unterstüt zen.	iam-user-no-policies-überprüfen	Diese Regel stellt sicher, dass AWS Identity and Access Management (IAM) -Richtlinien nur Gruppen oder Rollen zugewiese n werden, um den Zugriff auf Systeme und Ressourcen zu kontrollieren. Die Zuweisung von Berechtig ungen auf Gruppen- oder Rollenebene trägt dazu bei, die Wahrscheinlichkeit zu verringern, dass eine Identität übermäßige Berechtigungen erhält oder beibehält.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-2(1)	Die Organisation wendet automatisierte Mechanismen an, um die Verwaltung von Informationssystem konten zu unterstüt zen.	mfa-enabled-for-iam-Konsolenzugriff	Verwalten Sie den Zugriff auf Ressource n in der AWS Cloud, indem Sie sicherste llen, dass MFA für alle AWS Identity and Access Managemen t (IAM) -Benutzer aktiviert ist, die über ein Konsolenk ennwort verfügen. MFA bietet eine weitere Schutzebe ne zusätzlich zum Benutzernamen und Passwort. Indem Sie MFA für IAM-Benut zer vorschreiben, können Sie Vorfälle kompromittierter Konten reduzieren und verhindern, dass unbefugte Benutzer auf vertrauliche Daten zugreifen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-2(12)(a)	Die Organisation: a. Überwacht die Konten des Informationssystems im Hinblick auf [Zuordnung: von der Organisation definierte untypische Nutzung].	securityhub-enabled	AWS Security Hub hilft bei der Überwachung von unbefugtem Personal, Verbindungen, Geräten und Software. AWS Security Hub aggregiert, organisiert und priorisiert die Sicherheitswarnungen oder Ergebnisse mehrerer Dienste. AWS Einige dieser Dienste sind Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer und AWS Firewall Manager sowie AWS Partnerlösungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-2(12)(a)	Die Organisation: a. Überwacht die Konten des Informationssystems im Hinblick auf [Zuordnung: von der Organisation definierte untypische Nutzung].	guardduty-enabled-centralized	Amazon GuardDuty kann mithilfe von Threat Intelligence Feeds helfen, potenzielle Cybersicherheitsereignisse zu überwachen und zu erkennen. Dazu gehören Listen mit bösartigen IPs und maschinellen Lernmethoden zur Identifizierung unerwarteter, nicht autorisierter und bösartiger Aktivitäten in Ihrer AWS Cloud-Umgebung.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-2(3)	Das Informationssystem deaktiviert inaktive Benutzerkonten automatisch nach 90 Tagen.	iam-user-unused-credentials-überprüfen	AWS Identity and Access Management (IAM) kann Ihnen bei Zugriffsberechtigungen und Autorisierungen helfen, indem es nach IAM-Passwörtern und Zugriffsschlüsseln sucht, die für einen bestimmten Zeitraum nicht verwendet wurden. Wenn ungenutzte Anmeldeinformationen identifiziert werden, müssen Sie sie deaktivieren und/oder entfernen, da dies gegen das Prinzip der geringsten Berechtigung verstoßen könnte. Für diese Regel müssen Sie einen Wert für das maxCredentialUsage Alter festlegen (Standardkonfiguration: 90). Der tatsächliche Wert muss den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-2(3)	Das Informati onssystem deaktiviert automatisch inaktive Benutzerkonten nach 90 Tagen.	iam-password-policy	Die Identitäten und Anmeldeinformation en werden auf der Grundlage einer organisatorischen IAM-Passwortrichtlinie ausgestellt, verwaltet und verifiziert. Sie erfüllen oder übertreff en die Anforderungen von NIST SP 800-63 und dem Standard „Best Practices“ von AWS Foundatio nal Security für die Passwortstärke. Mit dieser Regel können Sie optional RequireUppercaseCh aracters (Wert für AWS grundlegende Sicherheitsbewährt e Methoden: wahr), RequireLowercaseCh aracters (Wert für bewährte Methoden für AWS grundlege nde Sicherheit: wahr), RequireSy mbols (Wert für bewährte Methoden für AWS grundlege nde Sicherheit:

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			wahr), RequireNumbers (Wert für bewährte Methoden für AWS grundlegende Sicherheit: wahr), MinimumPasswordLength (Wert für bewährte Methoden für AWS grundlegende Sicherheit: 14), PasswordReusePrevention (Wert für bewährte Methoden für AWS grundlegende Sicherheit: 24) und MaxPasswordAge (Wert für bewährte Methoden für AWS grundlegende Sicherheit: 90) für Ihr IAM festlegen Kennwortrichtlinie. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-2(4)	Das Informati onssystem prüft automatisch Aktionen wie die Erstellung, Änderung, Aktivieru ng, Deaktivierung und Entfernung von Konten und benachric htigt [Zuordnung: von der Organisation designierte Mitarbeiter oder Rollen].	securityhub-enabled	AWS Security Hub hilft bei der Überwachung von unbefugtem Personal, Verbindun gen, Geräten und Software. AWS Security Hub aggregiert, organisie rt und priorisie rt die Sicherhei tswarnungen oder Ergebnisse mehrerer Dienste. AWS Einige dieser Dienste sind Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer und AWS Firewall Manager sowie AWS Partnerlösungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-2(4)	Das Informati onssystem prüft automatisch Aktionen wie die Erstellung, Änderung, Aktivieru ng, Deaktivierung und Entfernung von Konten und benachric htigt [Zuordnung: von der Organisation designierte Mitarbeiter oder Rollen].	guardduty-enabled-centralized	Amazon GuardDuty kann mithilfe von Threat Intellige nce Feeds helfen, potenzielle Cybersich erheitsereignisse zu überwachen und zu erkennen. Dazu gehören Listen mit bösartigen IPs und maschinel len Lernmethoden zur Identifizierung unerwarteter, nicht autorisierter und bösartiger Aktivitäten in Ihrer AWS Cloud-Umgebung.
AC-2(4)	Das Informati onssystem prüft automatisch Aktionen wie die Erstellung, Änderung, Aktivieru ng, Deaktivierung und Entfernung von Konten und benachric htigt [Zuordnung: von der Organisation designierte Mitarbeiter oder Rollen].	cloud-trail-cloud-watch-logs-aktiviert	Verwenden Sie Amazon CloudWatch , um Protokollereignisa ktivitäten zentral zu sammeln und zu verwalten. Durch die Aufnahme von AWS CloudTrail Daten erhalten Sie Einzelhei ten zu den API-Aufru faktivitäten innerhalb Ihres AWS Kontos.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-2(4)	Das Informati onssystem prüft automatisch Aktionen wie die Erstellung, Änderung, Aktivieru ng, Deaktivierung und Entfernung von Konten und benachric htigt [Zuordnung: von der Organisation designierte Mitarbeiter oder Rollen].	cloudtrail-enabled	AWS CloudTrail kann dabei helfen, die Ablehnung zu verhindern, indem die Aktionen und API-Aufrufe der AWS Management Console aufgezeic hnet werden. Sie können die Benutzer und AWS Konten, die einen AWS Dienst aufgerufen haben, die Quell-IP-Adresse, über die die Anrufe generiert wurden, und die Zeitpunkte der Anrufe identifiz ieren. Einzelheiten zu den erfassten Daten finden Sie in den AWS CloudTrail Datensatzinhalten.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-2(4)	Das Informati onssystem prüft automatisch Aktionen wie die Erstellung, Änderung, Aktivieru ng, Deaktivierung und Entfernung von Konten und benachric htigt [Zuordnung: von der Organisation designierte Mitarbeiter oder Rollen].	multi-region-cloudtrail-enabled	AWS CloudTrail zeichnet Aktionen und API-Aufrufe der AWS Management Console auf. Sie können feststellen, welche Benutzer und Konten angerufen wurden AWS, von welcher Quell-IP-Adresse aus die Anrufe getätigt wurden und wann die Anrufe erfolgten. CloudTrail übermittelt Protokolldateien aus allen AWS Regionen an Ihren S3-Bucket , wenn MULTI_REG ION_CLOUD _TRAIL_ENABLED aktiviert ist. Außerdem wird beim AWS Start einer neuen Region derselbe Trail in der neuen Region erstellt. CloudTrail Dadurch erhalten Sie automatis ch Protokolldateien mit API-Aktivitäten für die neue Region.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-2(4)	Das Informati onssystem prüft automatisch Aktionen wie die Erstellung, Änderung, Aktivieru ng, Deaktivierung und Entfernung von Konten und benachric htigt [Zuordnung: von der Organisation designierte Mitarbeiter oder Rollen].	rds-logging-enabled	Um die Protokoll ierung und Überwachung in Ihrer Umgebung zu erleichtern, stellen Sie sicher, dass die Amazon Relationa l Database Service (Amazon RDS)-Prot okollierung aktiviert ist. Mit der Amazon-RDS-Protokollierung können Sie Ereigniss e wie Verbindungen, Verbindungsabbrüch e, Abfragen oder abgefragte Tabellen erfassen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-2(4)	Das Informati onssystem prüft automatisch Aktionen wie die Erstellung, Änderung, Aktivieru ng, Deaktivierung und Entfernung von Konten und benachric htigt [Zuordnung: von der Organisation designierte Mitarbeiter oder Rollen].	cloudwatch-alarm-a ction-check	Amazon CloudWatch alarmiert, wenn eine Metrik den Schwellen wert für eine bestimmte Anzahl von Bewertungszeiträum en überschreitet. Der Alarm führt eine oder mehrere Aktionen durch, die vom Wert der Metrik oder des Ausdrucks im Vergleich zu einem Schwellenwert in einer Reihe von Zeiträumen abhängt. Diese Regel erfordert einen Wert für alarmActionRequired (Config Default: True), insufficientDataAc tion Required (Config Default: True), okActionRequired (Config Default: False). Der tatsächli che Wert muss die Alarmaktionen für Ihre Umgebung widerspie geln.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-2(4)	Das Informati onssystem prüft automatisch Aktionen wie die Erstellung, Änderung, Aktivieru ng, Deaktivierung und Entfernung von Konten und benachric htigt [Zuordnung: von der Organisation designierte Mitarbeiter oder Rollen].	redshift-cluster-c onfiguration-check	Um Daten im Ruhezustand zu schützen, muss die Verschlüsselung für Ihre Amazon-Re dshift-Cluster aktiviert sein. Sie müssen auch sicherstellen, dass die erforderl ichen Konfigurationen auf Amazon-Redshift-Clustern bereitges tellt werden. Die Prüfungsprotokolli erung muss aktiviert sein, um Informati onen zu Verbindun gen und Benutzera ktivitäten in der Datenbank bereitzus tellen. Diese Regel erfordert, dass ein Wert für clusterDb Encrypted (Config Default: TRUE) und LoggingEnabled (Config Default: TRUE) gesetzt ist. Die tatsächlichen Werte müssen den Richtlini en Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-2(4)	Das Informati onssystem prüft automatisch Aktionen wie die Erstellung, Änderung, Aktivieru ng, Deaktivierung und Entfernung von Konten und benachric htigt [Zuordnung: von der Organisation designierte Mitarbeiter oder Rollen].	s-3 bucket-logging-enabled	Die Amazon Simple Storage Service (Amazon S3)-Serverzugriffs protokollierung bietet eine Methode zur Überwachu ng des Netzwerks im Hinblick auf potenzielle Cybersich erheitsereignisse. Die Ereignisse werden überwacht, indem detaillierte Aufzeichn ungen über die Anfragen erfasst werden, die an einen Amazon-S3-Bucket gestellt wurden. Jeder Zugriffsprotokolle intrag enthält Details zu einer einzelnen Zugriffsanfrage. Zu den Details gehören Anforderer, Bucket-Name, Anforderu ngszeit, Anforderu ngsaktion, Antwortst atus und Fehlercode, falls relevant.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-2(4)	Das Informati onssystem prüft automatisch Aktionen wie die Erstellung, Änderung, Aktivieru ng, Deaktivierung und Entfernung von Konten und benachric htigt [Zuordnung: von der Organisation designierte Mitarbeiter oder Rollen].	cloudtrail-s3-data events-enabled	Die Erfassung von Simple Storage Service (Amazon S3)-Datenereigniss en unterstützt die Erkennung von ungewöhnlichen Aktivitäten. Zu den Details gehören AWS Kontoinformationen , über die auf einen Amazon S3 S3-Bucket zugegriffen wurde, die IP-Adress e und die Uhrzeit des Ereignisses.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-2(f)	Die Organisation: f. Erstellt, aktiviert, ändert, deaktiviert und entfernt Konten im Informationssystem gemäß [Zuweisung: von der Organisation definierte Verfahren oder Bedingungen].	iam-user-unused-credentials-überprüfen	AWS Identity and Access Management (IAM) kann Ihnen bei Zugriffsberechtigungen und Autorisierungen helfen, indem es nach IAM-Passwörtern und Zugriffsschlüsseln sucht, die für einen bestimmten Zeitraum nicht verwendet wurden. Wenn ungenutzte Anmeldeinformationen identifiziert werden, müssen Sie sie deaktivieren und/oder entfernen, da dies gegen das Prinzip der geringsten Berechtigung verstoßen könnte. Für diese Regel müssen Sie einen Wert für das maxCredentialUsage Alter festlegen (Standardkonfiguration: 90). Der tatsächliche Wert muss den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-2(f)	Die Organisation: f. Erstellt, aktiviert, ändert, deaktiviert und entfernt Konten im Informationssystem gemäß [Zuweisung: von der Organisation definierte Verfahren oder Bedingungen].	iam-password-policy	Die Identitäten und Anmeldeinformationen werden auf der Grundlage einer organisatorischen IAM-Passwortrichtlinie ausgestellt, verwaltet und verifiziert. Sie erfüllen oder übertreffen die Anforderungen von NIST SP 800-63 und dem Standard „Best Practices“ von AWS Foundational Security für die Passwortstärke. Mit dieser Regel können Sie optional RequireUppercaseCharacters (Wert für AWS grundlegende Sicherheitsbewährte Methoden: wahr), RequireLowercaseCharacters (Wert für bewährte Methoden für AWS grundlegende Sicherheit: wahr), RequireSymbols (Wert für bewährte Methoden für AWS grundlegende Sicherheit:

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			wahr), RequireNumbers (Wert für bewährte Methoden für AWS grundlegende Sicherheit: wahr), MinimumPasswordLength (Wert für bewährte Methoden für AWS grundlegende Sicherheit: 14), PasswordReusePrevention (Wert für bewährte Methoden für AWS grundlegende Sicherheit: 24) und MaxPasswordAge (Wert für bewährte Methoden für AWS grundlegende Sicherheit: 90) für Ihr IAM festlegen Kennwortrichtlinie. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-2(f)	Die Organisation: f. Erstellt, aktiviert, ändert, deaktiviert und entfernt Konten im Informationssystem gemäß [Zuweisung: von der Organisation definierte Verfahren oder Bedingungen].	iam-root-access-key-überprüfen	Der Zugriff auf Systeme und Ressourcen kann gesteuert werden, indem überprüft wird, ob der Root-Benutzer keine Zugriffsschlüssel mit seiner AWS Identity and Access Management (IAM) -Rolle verknüpft hat. Stellen Sie sicher, dass die Root-Zugriffsschlüssel gelöscht werden. Erstellen und verwenden Sie stattdessen rollenbasierte AWS Konten, um dem Prinzip der geringsten Funktionalität Rechnung zu tragen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-2(f)	Die Organisation: f. Erstellt, aktiviert, ändert, deaktiviert und entfernt Konten im Informationssystem gemäß [Zuweisung: von der Organisation definierte Verfahren oder Bedingungen].	iam-inline-policy-blocked-kms-Aktionen	Stellen Sie sicher, dass ein Benutzer, eine IAM-Rolle oder eine IAM-Gruppe (AWS Identity and Access Management) nicht über eine Inline-Richtlinie verfügt, die blockierte Aktionen für alle AWS Schlüssel des Key Management Service zulässt. AWS empfiehlt, verwaltete Richtlinien anstelle von Inline-Richtlinien zu verwenden. Verwaltete Richtlinien ermöglichen Wiederverwendbarkeit, Versionsverwaltung, Rollback und Delegierung der Berechtigungsverwaltung. Mit dieser Regel können Sie den blockedActionsPatterns Parameter festlegen. (Wert „AWS Bewährte grundlegende Sicherheitsmethoden“: kms:Decrypt, kms:ReEncryptFrom). Die

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.
AC-2(f)	Die Organisation: f. Erstellt, aktiviert, ändert, deaktiviert und entfernt Konten im Informationssystem gemäß [Zuweisung: von der Organisation definierte Verfahren oder Bedingungen].	iam-no-inline-policy-überprüfen	Stellen Sie sicher, dass ein Benutzer, eine IAM-Rolle oder eine IAM-Gruppe (AWS Identity and Access Management) nicht über eine Inline-Richtlinie zur Zugriffskontrolle auf Systeme und Ressourcen verfügt. AWS empfiehlt, verwaltete Richtlinien anstelle von Inline-Richtlinien zu verwenden. Verwaltete Richtlinien ermöglichen Wiederverwendbarkeit, Versionsverwaltung, Rollback und Delegierung der Berechtigungsverwaltung.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-2(f)	Die Organisation: f. Erstellt, aktiviert, ändert, deaktiviert und entfernt Konten im Informationssystem gemäß [Zuweisung: von der Organisation definierte Verfahren oder Bedingungen].	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) kann Ihnen dabei helfen, die Prinzipien der geringsten Rechte und der Aufgabentrennung in Zugriffsberechtigungen und Autorisierungen zu integrieren und so zu verhindern, dass Richtlinien „Effect“: „Allow“ mit „Action“: „*“ anstelle von „Resource“: „*“ enthalten. Wenn Benutzern mehr Rechte eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und der Aufgabentrennung verstoßen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-2(f)	Die Organisation: f. Erstellt, aktiviert, ändert, deaktiviert und entfernt Konten im Informationssystem gemäß [Zuweisung: von der Organisation definierte Verfahren oder Bedingungen].	access-keys-rotated	Die Anmeldein formationen für autorisierte Geräte, Benutzer und Prozesse werden geprüft, indem sichergestellt wird, dass die IAM-Zugri ffsschlüssel gemäß den Richtlinien der Organisation rotiert werden. Das regelmäßige Ändern der Zugriffsschlüssel ist eine bewährte Sicherheitsmethode . Es verkürzt den Zeitraum, in dem ein Zugriffsschlüssel aktiv ist, und reduziert die Auswirkungen auf das Unternehmen, wenn die Schlüssel kompromittiert werden. Diese Regel erfordert einen Wert für die Zugriffsschlüssel-Rotation (Standard konfiguration: 90). Der tatsächliche Wert muss den Richtlini

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			en Ihrer Organisation entsprechen.
AC-2(f)	Die Organisation: f. Erstellt, aktiviert, ändert, deaktiviert und entfernt Konten im Informationssystem gemäß [Zuweisung: von der Organisation definierte Verfahren oder Bedingungen].	iam-user-group-membership-überprüfen	AWS Identity and Access Management (IAM) kann Ihnen helfen, Zugriffsberechtigungen und Autorisierungen einzuschränken, indem sichergestellt wird, dass IAM-Benutzer Mitglieder mindestens einer Gruppe sind. Wenn Benutzern mehr Berechtigungen eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und Aufgabentrennung verstoßen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-2(f)	Die Organisation: f. Erstellt, aktiviert, ändert, deaktiviert und entfernt Konten im Informationssystem gemäß [Zuweisung: von der Organisation definierte Verfahren oder Bedingungen].	iam-user-mfa-enabled	Aktivieren Sie diese Regel, um den Zugriff auf Ressourcen in der Cloud einzuschränken. AWS Diese Regel stellt sicher, dass die Multi-Faktor-Authentifizierung (MFA) für alle IAM-Benutzer aktiviert ist. MFA bietet eine weitere Schutzebene zusätzlich zum Benutzernamen und Passwort. Reduzieren Sie Fälle von kompromittierten Konten, indem Sie MFA für IAM-Benutzer vorschreiben.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-2(f)	Die Organisation: f. Erstellt, aktiviert, ändert, deaktiviert und entfernt Konten im Informationssystem gemäß [Zuweisung: von der Organisation definierte Verfahren oder Bedingungen].	iam-user-no-policies-überprüfen	Diese Regel stellt sicher, dass AWS Identity and Access Management (IAM) -Richtlinien nur Gruppen oder Rollen zugewiese n werden, um den Zugriff auf Systeme und Ressourcen zu kontrollieren. Die Zuweisung von Berechtig ungen auf Gruppen- oder Rollenebene trägt dazu bei, die Wahrscheinlichkeit zu verringern, dass eine Identität übermäßige Berechtigungen erhält oder beibehält.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-2(f)	Die Organisation: f. Erstellt, aktiviert, ändert, deaktiviert und entfernt Konten im Informationssystem gemäß [Zuweisung: von der Organisation definierte Verfahren oder Bedingungen].	mfa-enabled-for-iam-Konsolenzugriff	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass MFA für alle AWS Identity and Access Management (IAM) -Benutzer aktiviert ist, die über ein Konsolenkennwort verfügen. MFA bietet eine weitere Schutzebene zusätzlich zum Benutzernamen und Passwort. Indem Sie MFA für IAM-Benutzer vorschreiben, können Sie Vorfälle kompromittierter Konten reduzieren und verhindern, dass unbefugte Benutzer auf vertrauliche Daten zugreifen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-2(f)	Die Organisation: f. Erstellt, aktiviert, ändert, deaktiviert und entfernt Konten im Informationssystem gemäß [Zuweisung: von der Organisation definierte Verfahren oder Bedingungen].	iam-policy-no-statements-with-full-access	Stellen Sie sicher, dass IAM-Aktionen nur auf die benötigten Aktionen beschränkt sind. Wenn Benutzern mehr Rechte eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und der Aufgabentrennung verstoßen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-2(g)	Die Organisation: g. Überwacht die Verwendung von Konten im Informationssystem.	redshift-cluster-configuration-check	Um Daten im Ruhezustand zu schützen, muss die Verschlüsselung für Ihre Amazon-Redshift-Cluster aktiviert sein. Sie müssen auch sicherstellen, dass die erforderlichen Konfigurationen auf Amazon-Redshift-Clustern bereitgestellt werden. Die Prüfungsprotokollierung muss aktiviert sein, um Informationen zu Verbindungen und Benutzeraktivitäten in der Datenbank bereitzustellen. Diese Regel erfordert, dass ein Wert für clusterDbEncrypted (Config Default: TRUE) und LoggingEnabled (Config Default: TRUE) gesetzt ist. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-2(g)	Die Organisation: g. Überwacht die Verwendung von Konten im Informati onssystem.	s-3 bucket-logging-enabled	Die Amazon Simple Storage Service (Amazon S3)-Serverzugriffs protokollierung bietet eine Methode zur Überwachu ng des Netzwerks im Hinblick auf potenzielle Cybersich erheitsereignisse. Die Ereignisse werden überwacht, indem detaillierte Aufzeichn ungen über die Anfragen erfasst werden, die an einen Amazon-S3-Bucket gestellt wurden. Jeder Zugriffsprotokolle intrag enthält Details zu einer einzelnen Zugriffsanfrage. Zu den Details gehören Anforderer, Bucket-Name, Anforderu ngszeit, Anforderu ngsaktion, Antwortst atus und Fehlercode, falls relevant.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-2(g)	Die Organisation: g. Überwacht die Verwendung von Konten im Informati onssystem.	cloudtrail-enabled	AWS CloudTrai l kann durch die Aufzeichnung AWS von Aktionen und API-Aufrufen der Management Console bei der Nichtabst reitbarkeit helfen. Sie können die Benutzer und AWS Konten, die einen AWS Dienst aufgerufen haben, die Quell-IP-Adresse, über die die Anrufe generiert wurden, und die Zeitpunkte der Anrufe identifiz ieren. Einzelheiten zu den erfassten Daten finden Sie in den AWS CloudTrail Datensatzinhalten.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-2(g)	Die Organisation: g. Überwacht die Verwendung von Konten im Informati onssystem.	cloudtrail-s3-data events-enabled	Die Erfassung von Simple Storage Service (Amazon S3)-Datenereigniss en unterstützt die Erkennung von ungewöhnlichen Aktivitäten. Zu den Details gehören AWS Kontoinformationen , über die auf einen Amazon S3 S3-Bucket zugegriffen wurde, die IP-Adress e und die Uhrzeit des Ereignisses.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-2(g)	Die Organisation: g. Überwacht die Verwendung von Konten im Informati onssystem.	securityhub-enabled	AWS Security Hub hilft bei der Überwachung von unbefugtem Personal, Verbindun gen, Geräten und Software. AWS Security Hub aggregiert, organisie rt und priorisie rt die Sicherhei tswarnungen oder Ergebnisse mehrerer Dienste. AWS Einige dieser Dienste sind Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer und AWS Firewall Manager sowie AWS Partnerlösungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-2(g)	Die Organisation: g. Überwacht die Verwendung von Konten im Informati onssystem.	guardduty-enabled-centralized	Amazon GuardDuty kann mithilfe von Threat Intellige nce Feeds helfen, potenzielle Cybersich erheitsereignisse zu überwachen und zu erkennen. Dazu gehören Listen mit bösartigen IPs und maschinel len Lernmethoden zur Identifizierung unerwarteter, nicht autorisierter und bösartiger Aktivitäten in Ihrer AWS Cloud-Umgebung.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-2(g)	Die Organisation: g. Überwacht die Verwendung von Konten im Informati onssystem.	rds-logging-enabled	Um die Protokoll ierung und Überwachung in Ihrer Umgebung zu erleichtern, stellen Sie sicher, dass die Amazon Relationa l Database Service (Amazon RDS)-Prot okollierung aktiviert ist. Mit der Amazon-RDS-Protokollierung können Sie Ereigniss e wie Verbindungen, Verbindungsabbrüch e, Abfragen oder abgefragte Tabellen erfassen.
AC-2(g)	Die Organisation: g. Überwacht die Verwendung von Konten im Informati onssystem.	cloud-trail-cloud-watch-logs-aktiviert	Verwenden Sie Amazon CloudWatch , um Protokollereignisa ktivitäten zentral zu sammeln und zu verwalten. Durch die Aufnahme von AWS CloudTrail Daten erhalten Sie Einzelhei ten zu den API-Aufru faktivitäten innerhalb Ihres AWS Kontos.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-2(g)	Die Organisation: g. Überwacht die Verwendung von Konten im Informati onssystem.	api-gw-execution-l ogging-aktiviert	Die API-Gateway-Protokollierung zeigt detaillierte Ansichten der Benutzer, die auf die API zugegriff en haben, und wie diese Benutzer auf die API zugegriff en haben. Diese Einblicke ermöglichen die Transparenz von Benutzeraktivitäten.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-2(g)	Die Organisation: g. Überwacht die Verwendung von Konten im Informati onssystem.	multi-region-cloudtrail-enabled	AWS CloudTrail zeichnet Aktionen und API-Aufrufe der AWS Management Console auf. Sie können feststellen, welche Benutzer und Konten angerufen wurden AWS, von welcher Quell-IP-Adresse aus die Anrufe getätigt wurden und wann die Anrufe erfolgten. CloudTrail übermittelt Protokolldateien aus allen AWS Regionen an Ihren S3-Bucket , wenn MULTI_REG ION_CLOUD _TRAIL_ENABLED aktiviert ist. Außerdem wird beim AWS Start einer neuen Region derselbe Trail in der neuen Region erstellt. CloudTrail Dadurch erhalten Sie automatis ch Protokolldateien mit API-Aktivitäten für die neue Region.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-2(g)	Die Organisation: g. Überwacht die Verwendung von Konten im Informationssystem.	wafv2-logging-enabled	Um die Protokollierung und Überwachung in Ihrer Umgebung zu erleichtern, aktivieren Sie die AWS WAF (V2) -Protokollierung im regionalen und globalen Web ACLs. AWS Die WAF-Protokollierung bietet detaillierte Informationen über den Datenverkehr, der von Ihrer Web-ACL analysiert wird. In den Protokollen werden die Uhrzeit aufgezeichnet, zu der die AWS WAF die Anfrage von Ihrer AWS Ressource erhalten hat, Informationen über die Anfrage und eine Aktion für die Regel, der jede Anfrage entsprach.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-2(g)	Die Organisation: g. Überwacht die Verwendung von Konten im Informati onssystem.	elasticsearch-logs-to-cloudwatch	Stellen Sie sicher, dass für Amazon OpenSearch Service-Domains Fehlerpro tokolle aktiviert und zur Aufbewahrung und Beantwortung an Amazon CloudWatc h Logs gestreamt werden. Domain-Fehlerprotokolle sind bei Sicherhei ts- und Zugriffsp rüfungen sowie bei der Diagnose von Verfügbarkeitsprob lemen nützlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-2(j)	Die Organisation: j. Überprüft Konten auf deren Einhaltung der Kontoverwaltungsanforderungen [Zuweisung: von der Organisation festgelegte Häufigkeit].	iam-user-group-membership-überprüfen	AWS Identity and Access Management (IAM) kann Ihnen helfen, Zugriffsberechtigungen und Autorisierungen einzuschränken, indem sichergestellt wird, dass IAM-Benutzer Mitglieder mindestens einer Gruppe sind. Wenn Benutzern mehr Berechtigungen eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und Aufgabentrennung verstoßen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-2(j)	Die Organisation: j. Überprüft Konten auf deren Einhaltung der Kontoverwaltungsanforderungen [Zuweisung: von der Organisation festgelegte Häufigkeit].	iam-password-policy	Die Identitäten und Anmeldeinformationen werden auf der Grundlage einer organisatorischen IAM-Passwortrichtlinie ausgestellt, verwaltet und verifiziert. Sie erfüllen oder übertreffen die Anforderungen von NIST SP 800-63 und dem Standard „Best Practices“ von AWS Foundational Security für die Passwortstärke. Mit dieser Regel können Sie optional RequireUppercaseCharacters (Wert für AWS grundlegende Sicherheitsbewährte Methoden: wahr), RequireLowercaseCharacters (Wert für bewährte Methoden für AWS grundlegende Sicherheit: wahr), RequireSymbols (Wert für bewährte Methoden für AWS grundlegende Sicherheit:

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			wahr), RequireNumbers (Wert für bewährte Methoden für AWS grundlegende Sicherheit: wahr), MinimumPasswordLength (Wert für bewährte Methoden für AWS grundlegende Sicherheit: 14), PasswordReusePrevention (Wert für bewährte Methoden für AWS grundlegende Sicherheit: 24) und MaxPasswordAge (Wert für bewährte Methoden für AWS grundlegende Sicherheit: 90) für Ihr IAM festlegen Kennwortrichtlinie. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-2(j)	Die Organisation: j. Überprüft Konten auf deren Einhaltung der Kontoverwaltungsanforderungen [Zuweisung: von der Organisation festgelegte Häufigkeit].	access-keys-rotated	Die Anmeldeinformationen für autorisierte Geräte, Benutzer und Prozesse werden geprüft, indem sichergestellt wird, dass die IAM-Zugriffsschlüssel gemäß den Richtlinien der Organisation rotiert werden. Das regelmäßige Ändern der Zugriffsschlüssel ist eine bewährte Sicherheitsmethode. Es verkürzt den Zeitraum, in dem ein Zugriffsschlüssel aktiv ist, und reduziert die Auswirkungen auf das Unternehmen, wenn die Schlüssel kompromittiert werden. Diese Regel erfordert einen Wert für die Zugriffsschlüssel-Rotation (Standard konfiguration: 90). Der tatsächliche Wert muss den Richtlini

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			en Ihrer Organisation entsprechen.
AC-2(j)	Die Organisation: j. Überprüft Konten auf deren Einhaltung der Kontoverwaltungsanforderungen [Zuweisung: von der Organisation festgelegte Häufigkeit].	iam-root-access-key-überprüfen	Der Zugriff auf Systeme und Ressourcen kann gesteuert werden, indem überprüft wird, ob der Root-Benutzer keine Zugriffsschlüssel mit seiner AWS Identity and Access Management (IAM) -Rolle verknüpft hat. Stellen Sie sicher, dass die Root-Zugriffsschlüssel gelöscht werden. Erstellen und verwenden Sie stattdessen rollenbasierte AWS Konten, um dem Prinzip der geringsten Funktionalität Rechnung zu tragen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-2(j)	Die Organisation: j. Überprüft Konten auf deren Einhaltung der Kontoverwaltungsanforderungen [Zuweisung: von der Organisation festgelegte Häufigkeit].	iam-group-has-users-überprüfen	AWS Identity and Access Management (IAM) kann Ihnen helfen, die Prinzipien der geringsten Rechte und der Aufgabentrennung mit Zugriffsberechtigungen und Autorisierungen zu integrieren, indem sichergestellt wird, dass IAM-Gruppen mindestens einen IAM-Benutzer haben. Die Einteilung von IAM-Benutzern in Gruppen auf der Grundlage der ihnen zugewiesenen Berechtigungen oder Aufgabenbereiche ist eine Möglichkeit, die geringsten Rechte zu berücksichtigen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-2(j)	Die Organisation: j. Überprüft Konten auf deren Einhaltung der Kontoverwaltungsanforderungen [Zuweisung: von der Organisation festgelegte Häufigkeit].	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) kann Ihnen dabei helfen, die Prinzipien der geringsten Rechte und der Aufgabentrennung in Zugriffsberechtigungen und Autorisierungen zu integrieren und so zu verhindern, dass Richtlinien „Effect“: „Allow“ mit „Action“: „*“ anstelle von „Resource“: „*“ enthalten. Wenn Benutzern mehr Rechte eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und der Aufgabentrennung verstoßen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-2(j)	Die Organisation: j. Überprüft Konten auf deren Einhaltung der Kontoverwaltungsanforderungen [Zuweisung: von der Organisation festgelegte Häufigkeit].	iam-user-no-policies-überprüfen	Diese Regel stellt sicher, dass AWS Identity and Access Management (IAM) -Richtlinien nur Gruppen oder Rollen zugewiesen werden, um den Zugriff auf Systeme und Ressourcen zu kontrollieren. Die Zuweisung von Berechtigungen auf Gruppen- oder Rollenebene trägt dazu bei, die Wahrscheinlichkeit zu verringern, dass eine Identität übermäßige Berechtigungen erhält oder beibehält.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-2(j)	Die Organisation: j. Überprüft Konten auf deren Einhaltung der Kontoverwaltungsanforderungen [Zuweisung: von der Organisation festgelegte Häufigkeit].	iam-customer-policy-blocked-kms-Aktionen	AWS Identity and Access Management (IAM) kann Ihnen helfen, die Prinzipien der geringsten Rechte und der Aufgabentrennung in Zugriffsberechtigungen und Autorisierungen zu integrieren und so zu verhindern, dass Richtlinien blockierte Aktionen für alle AWS Schlüssel des Key Management Service enthalten. Wenn Benutzer mehr Rechte haben, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und Aufgabentrennung verstoßen. Mit dieser Regel können Sie den Parameter festlegen. blockedActionsPatterns (Wert „AWS Bewährte grundlegende Sicherheitsmethoden“: kms:

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			Decrypt, kms:ReEncryptFrom). Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-2(j)	Die Organisation: j. Überprüft Konten auf deren Einhaltung der Kontoverwaltungsanforderungen [Zuweisung: von der Organisation festgelegte Häufigkeit].	iam-inline-policy-blocked-kms-Aktionen	Stellen Sie sicher, dass ein Benutzer, eine IAM-Rolle oder eine IAM-Gruppe (AWS Identity and Access Management) nicht über eine Inline-Richtlinie verfügt, die blockierte Aktionen für alle AWS Schlüssel des Key Management Service zulässt. AWS empfiehlt, verwaltete Richtlinien anstelle von Inline-Richtlinien zu verwenden. Verwaltete Richtlinien ermöglichen Wiederverwendbarkeit, Versionsverwaltung, Rollback und Delegierung der Berechtigungsverwaltung. Mit dieser Regel können Sie den blockedActionsPatterns Parameter festlegen. (Wert „AWS Bewährte grundlegende Sicherheitsmethoden“: kms:Decrypt, kms:ReEncryptFrom). Die

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.
AC-2(j)	Die Organisation: j. Überprüft Konten auf deren Einhaltung der Kontoverwaltungsanforderungen [Zuweisung: von der Organisation festgelegte Häufigkeit].	iam-no-inline-policy-überprüfen	Stellen Sie sicher, dass ein Benutzer, eine IAM-Rolle oder eine IAM-Gruppe (AWS Identity and Access Management) nicht über eine Inline-Richtlinie zur Zugriffskontrolle auf Systeme und Ressourcen verfügt. AWS empfiehlt, verwaltete Richtlinien anstelle von Inline-Richtlinien zu verwenden. Verwaltete Richtlinien ermöglichen Wiederverwendbarkeit, Versionsverwaltung, Rollback und Delegierung der Berechtigungsverwaltung.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-2(j)	Die Organisation: j. Überprüft Konten auf deren Einhaltung der Kontoverwaltungsanforderungen [Zuweisung: von der Organisation festgelegte Häufigkeit].	iam-user-mfa-enabled	Aktivieren Sie diese Regel, um den Zugriff auf Ressourcen in der AWS Cloud einzuschränken. Diese Regel stellt sicher, dass die Multi-Faktor-Authentifizierung (MFA) für alle IAM-Benutzer aktiviert ist. MFA bietet eine weitere Schutzebene zusätzlich zum Benutzernamen und Passwort. Reduzieren Sie Fälle von kompromittierten Konten, indem Sie MFA für IAM-Benutzer vorschreiben.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-2(j)	Die Organisation: j. Überprüft Konten auf deren Einhaltung der Kontoverwaltungsanforderungen [Zuweisung: von der Organisation festgelegte Häufigkeit].	iam-user-unused-credentials-überprüfen	AWS Identity and Access Management (IAM) kann Ihnen bei Zugriffsberechtigungen und Autorisierungen helfen, indem es nach IAM-Passwörtern und Zugriffsschlüsseln sucht, die für einen bestimmten Zeitraum nicht verwendet wurden. Wenn ungenutzte Anmeldeinformationen identifiziert werden, müssen Sie sie deaktivieren und/oder entfernen, da dies gegen das Prinzip der geringsten Berechtigung verstoßen könnte. Für diese Regel müssen Sie einen Wert für das maxCredentialUsage Alter festlegen (Standardkonfiguration: 90). Der tatsächliche Wert muss den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-2(j)	Die Organisation: j. Überprüft Konten auf deren Einhaltung der Kontoverwaltungsanforderungen [Zuweisung: von der Organisation festgelegte Häufigkeit].	mfa-enabled-for-iam-Konsolenzugriff	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass MFA für alle AWS Identity and Access Management (IAM) -Benutzer aktiviert ist, die über ein Konsolenkennwort verfügen. MFA bietet eine weitere Schutzebene zusätzlich zum Benutzernamen und Passwort. Indem Sie MFA für IAM-Benutzer vorschreiben, können Sie Vorfälle kompromittierter Konten reduzieren und verhindern, dass unbefugte Benutzer auf vertrauliche Daten zugreifen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-2(j)	Die Organisation: j. Überprüft Konten auf deren Einhaltung der Kontoverwaltungsanforderungen [Zuweisung: von der Organisation festgelegte Häufigkeit].	ec2- instance-profile-attached	EC2 Instanzprofile geben eine IAM-Rolle an eine Instanz weiter. EC2 Das Anhängen eines Instance-Profils an Ihre Instances kann bei der Implementierung von geringsten Berechtigungen und der Berechtigungsverwaltung helfen.
AC-2(j)	Die Organisation: j. Überprüft Konten auf deren Einhaltung der Kontoverwaltungsanforderungen [Zuweisung: von der Organisation festgelegte Häufigkeit].	iam-policy-no-statements-with-full-access	Stellen Sie sicher, dass IAM-Aktionen nur auf die benötigten Aktionen beschränkt sind. Wenn Benutzern mehr Rechte eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und der Aufgabentrennung verstoßen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-2(j)	Die Organisation: j. Überprüft Konten auf deren Einhaltung der Kontoverwaltungsanforderungen [Zuweisung: von der Organisation festgelegte Häufigkeit].	ecs-task-definition-user-for-host-mode-check	Wenn für eine Aufgabendefinition erhöhte Berechtigungen gelten, liegt das daran, dass der Kunde diesen Konfigurationen ausdrücklich zugestimmt hat. Diese Kontrolle prüft, ob eine unerwartete Berechtigungseskalation vorliegt, wenn für eine Aufgabendefinition das Host-Netzwerk aktiviert ist, die Kunden aber keine erhöhten Berechtigungen aktiviert haben.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-21(b)	Die Organisation: b. Verwendet [Zuweisung: von der Organisation definierte automatisierte Mechanismen oder manuelle Prozesse], um Benutzer bei Entscheidungen hinsichtlich Informationsweitergabe/Zusammenarbeit zu unterstützen.	sagemaker-notebook-no-direct-Internetzugang	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass SageMaker Amazon-Notebooks keinen direkten Internetzugang zulassen. Indem Sie direkten Internetzugang blockieren, vermeiden Sie, dass unbefugte Benutzer auf sensible Daten zugreifen.
AC-21(b)	Die Organisation: b. Verwendet [Zuweisung: von der Organisation definierte automatisierte Mechanismen oder manuelle Prozesse], um Benutzer bei Entscheidungen hinsichtlich Informationsweitergabe/Zusammenarbeit zu unterstützen.	dms-replication-not-public	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass auf DMS-Replikationsinstanzen nicht öffentlich zugegriffen werden kann. DMS-Replikations-Instances können vertrauliche Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-21(b)	Die Organisation: b. Verwendet [Zuweisung: von der Organisation definierte automatisierte Mechanismen oder manuelle Prozesse], um Benutzer bei Entscheidungen hinsichtlich Informationsweitergabe/Zusammenarbeit zu unterstützen.	ebs-snapshot-public-restorable-überprüfen	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass EBS-Snapshots nicht öffentlich wiederherstellbar sind. EBS-Volume-Snapshots können vertrauliche Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.
AC-21(b)	Die Organisation: b. Verwendet [Zuweisung: von der Organisation definierte automatisierte Mechanismen oder manuelle Prozesse], um Benutzer bei Entscheidungen hinsichtlich Informationsweitergabe/Zusammenarbeit zu unterstützen.	ec2- instance-no-public-ip	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon Elastic Compute Cloud (Amazon EC2) - Instances nicht öffentlich zugänglich sind. EC2 Amazon-Instances können vertrauliche Informationen enthalten, und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-21(b)	Die Organisation: b. Verwendet [Zuweisung: von der Organisation definierte automatisierte Mechanismen oder manuelle Prozesse], um Benutzer bei Entscheidungen hinsichtlich Informationsweitergabe/Zusammenarbeit zu unterstützen.	emr-master-no-public-ip	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon EMR-Cluster-Masterknoten nicht öffentlich zugänglich sind. Amazon-EMR-Cluster-Hauptknoten können vertrauliche Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.
AC-21(b)	Die Organisation: b. Verwendet [Zuweisung: von der Organisation definierte automatisierte Mechanismen oder manuelle Prozesse], um Benutzer bei Entscheidungen hinsichtlich Informationsweitergabe/Zusammenarbeit zu unterstützen.	lambda-function-public-access-verboten	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass AWS Lambda-Funktionen nicht öffentlich zugänglich sind. Der öffentliche Zugriff kann möglicherweise die Verfügbarkeit von Ressourcen beeinträchtigen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-21(b)	Die Organisation: b. Verwendet [Zuweisung: von der Organisation definierte automatisierte Mechanismen oder manuelle Prozesse], um Benutzer bei Entscheidungen hinsichtlich Informationsweitergabe/Zusammenarbeit zu unterstützen.	rds-instance-public-access-überprüfen	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Relational Database Service (Amazon RDS) -Instances nicht öffentlich sind. Amazon-RDS-Datenbank-Instances können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-21(b)	Die Organisation: b. Verwendet [Zuweisung: von der Organisation definierte automatisierte Mechanismen oder manuelle Prozesse], um Benutzer bei Entscheidungen hinsichtlich Informationsweitergabe/Zusammenarbeit zu unterstützen.	rds-snapshots-public-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Relational Database Service (Amazon RDS) -Instances nicht öffentlich sind. Amazon-RDS-Datenbank-Instances können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-21(b)	Die Organisation: b. Verwendet [Zuweisung: von der Organisation definierte automatisierte Mechanismen oder manuelle Prozesse], um Benutzer bei Entscheidungen hinsichtlich Informationsweitergabe/Zusammenarbeit zu unterstützen.	redshift-cluster-public-access-überprüfen	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Redshift Redshift-Cluster nicht öffentlich sind. Amazon-Redshift-Cluster können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.
AC-21(b)	Die Organisation: b. Verwendet [Zuweisung: von der Organisation definierte automatisierte Mechanismen oder manuelle Prozesse], um Benutzer bei Entscheidungen hinsichtlich Informationsweitergabe/Zusammenarbeit zu unterstützen.	s-3 bucket-public-read-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie nur autorisierten Benutzern, Prozessen und Geräten Zugriff auf Amazon Simple Storage Service (Amazon S3) - Buckets gewähren. Die Verwaltung des Zugriffs sollte mit der Klassifizierung der Daten übereinstimmen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-21(b)	Die Organisation: b. Verwendet [Zuweisung: von der Organisation definierte automatisierte Mechanismen oder manuelle Prozesse], um Benutzer bei Entscheidungen hinsichtlich Informationsweitergabe/Zusammenarbeit zu unterstützen.	s-3 bucket-public-write-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie nur autorisierten Benutzern, Prozessen und Geräten Zugriff auf Amazon Simple Storage Service (Amazon S3) - Buckets gewähren. Die Verwaltung des Zugriffs sollte mit der Klassifizierung der Daten übereinstimmen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-21(b)	Die Organisation: b. Verwendet [Zuweisung: von der Organisation definierte automatisierte Mechanismen oder manuelle Prozesse], um Benutzer bei Entscheidungen hinsichtlich Informationsweitergabe/Zusammenarbeit zu unterstützen.	restricted-common-ports	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass gemeinsame Ports für Amazon Elastic Compute Cloud (Amazon EC2) -Sicherheitsgruppen eingeschränkt sind. Wenn der Zugriff auf Ports nicht auf vertrauenswürdige Quellen beschränkt wird, kann dies zu Angriffen auf die Verfügbarkeit, Integrität und Vertraulichkeit von Systemen führen. Mit dieser Regel können Sie optional die Parameter blockedPort1–blockedPort5 festlegen (Standardkonfigurationen: 20, 21, 3389, 3306, 4333). Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-21(b)	Die Organisation: b. Verwendet [Zuweisung: von der Organisation definierte automatisierte Mechanismen oder manuelle Prozesse], um Benutzer bei Entscheidungen hinsichtlich Informationsweitergabe/Zusammenarbeit zu unterstützen.	vpc-default-security-group-geschlossen	Sicherheitsgruppen von Amazon Elastic Compute Cloud (Amazon EC2) können bei der Verwaltung des Netzwerkzugriffs helfen, indem sie eine statusbehaftete Filterung des ein- und ausgehenden Netzwerkverkehrs zu Ressourcen bereitstellen. AWS Die Beschränkung des gesamten Datenverkehrs auf die Standardsicherheitsgruppe hilft dabei, den Fernzugriff auf Ihre Ressourcen einzuschränken. AWS

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-21(b)	Die Organisation: b. Verwendet [Zuweisung: von der Organisation definierte automatisierte Mechanismen oder manuelle Prozesse], um Benutzer bei Entscheidungen hinsichtlich Informationsweitergabe/Zusammenarbeit zu unterstützen.	vpc-sg-open-only-to-authorized-ports	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass gemeinsame Ports für Amazon Elastic Compute Cloud (Amazon EC2) -Sicherheitsgruppen eingeschränkt sind. Wenn der Zugriff auf Ports nicht auf vertrauenswürdige Quellen beschränkt wird, kann dies zu Angriffen auf die Verfügbarkeit, Integrität und Vertraulichkeit von Systemen führen. Durch die Beschränkung des Zugriffs auf Ressourcen innerhalb einer Sicherheitsgruppe aus dem Internet (0.0.0.0/0) kann der Remote-Zugriff auf interne Systeme gesteuert werden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-21(b)	Die Organisation: b. Verwendet [Zuweisung: von der Organisation definierte automatisierte Mechanismen oder manuelle Prozesse], um Benutzer bei Entscheidungen hinsichtlich Informationsweitergabe/Zusammenarbeit zu unterstützen.	no-unrestricted-route-to-igw	Stellen Sie sicher, dass EC2 Amazon-Routentabellen keine uneingeschränkten Routen zu einem Internet-Gateway enthalten. Durch das Entfernen oder Beschränken des Internetzugangs für Workloads innerhalb von Amazon VPCs können unbeabsichtigte Zugriffe in Ihrer Umgebung reduziert werden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-21(b)	Die Organisation: b. Verwendet [Zuweisung: von der Organisation definierte automatisierte Mechanismen oder manuelle Prozesse], um Benutzer bei Entscheidungen hinsichtlich Informationsweitergabe/Zusammenarbeit zu unterstützen.	s3 bucket-level-public-access - verboten	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Simple Storage Service (Amazon S3) -Buckets nicht öffentlich zugänglich sind. Diese Regel trägt dazu bei, sensible Daten vor unbefugten Remote-Benutzern zu schützen, indem sie den öffentlichen Zugriff auf Bucket-Ebene verhindert.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-21(b)	Die Organisation: b. Verwendet [Zuweisung: von der Organisation definierte automatisierte Mechanismen oder manuelle Prozesse], um Benutzer bei Entscheidungen hinsichtlich Informationsweitergabe/Zusammenarbeit zu unterstützen.	subnet-auto-assign-public-ip-deaktiviert	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon Virtual Private Cloud (VPC) -Subnetzen nicht automatisch eine öffentliche IP-Adresse zugewiesen wird. Amazon Elastic Compute Cloud (EC2) -Instances, die in Subnetzen gestartet werden, in denen dieses Attribut aktiviert ist, haben ihrer primären Netzwerkschnittstelle eine öffentliche IP-Adresse zugewiesen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-21(b)	Die Organisation: b. Verwendet [Zuweisung: von der Organisation definierte automatisierte Mechanismen oder manuelle Prozesse], um Benutzer bei Entscheidungen hinsichtlich Informationsweitergabe/Zusammenarbeit zu unterstützen.	autoscaling-launch-config-public-ip-deaktiviert	Wenn Sie Ihre Netzwerkschnittstellen mit einer öffentlichen IP-Adresse konfigurieren, sind die diesen Netzwerkschnittstellen zugehörigen Ressourcen über das Internet erreichbar. EC2 Ressourcen sollten nicht öffentlich zugänglich sein, da dies einen unbeabsichtigten Zugriff auf Ihre Anwendungen oder Server ermöglichen kann.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-21(b)	Die Organisation: b. Verwendet [Zuweisung: von der Organisation definierte automatisierte Mechanismen oder manuelle Prozesse], um Benutzer bei Entscheidungen hinsichtlich Informationsweitergabe/Zusammenarbeit zu unterstützen.	account-level-public-accesss3-Blöcke-periodisch	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Simple Storage Service (Amazon S3) -Buckets nicht öffentlich zugänglich sind. Diese Regel trägt dazu bei, sensible Daten vor unbefugten Remote-Benutzern zu schützen, indem sie den öffentlichen Zugriff verhindert. Mit dieser Regel können Sie optional die Parameter ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) und restrictPublicBuckets Parameter (Config Default: True) festlegen. Die tatsächlichen Werte müssen den Richtlini

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			en Ihrer Organisation entsprechen.
AC-3	Das Informati onssystem setzt genehmigte Autorisie rungen für den logischen Zugriff auf Informationen und Systemressourcen gemäß den geltenden Zugriffskontrollri chtlinien durch.	s-3 bucket-public-writ e-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie nur autorisierten Benutzern, Prozessen und Geräten Zugriff auf Amazon Simple Storage Service (Amazon S3) - Buckets gewähren. Die Verwaltung des Zugriffs sollte mit der Klassifizierung der Daten übereinst immen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-3	Das Informati onssystem setzt genehmigte Autorisie rungen für den logischen Zugriff auf Informationen und Systemressourcen gemäß den geltenden Zugriffskontrollri chtlinien durch.	iam-user-no-policies-überprüfen	Diese Regel stellt sicher, dass AWS Identity and Access Management (IAM) -Richtlinien nur Gruppen oder Rollen zugewiese n werden, um den Zugriff auf Systeme und Ressourcen zu kontrollieren. Die Zuweisung von Berechtig ungen auf Gruppen- oder Rollenebene trägt dazu bei, die Wahrscheinlichkeit zu verringern, dass eine Identität übermäßige Berechtigungen erhält oder beibehält.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-3	Das Informationssystem setzt genehmigte Autorisierungen für den logischen Zugriff auf Informationen und Systemressourcen gemäß den geltenden Zugriffskontrollrichtlinien durch.	iam-user-unused-credentials-überprüfen	AWS Identity and Access Management (IAM) kann Ihnen bei Zugriffsberechtigungen und Autorisierungen helfen, indem es nach IAM-Passwörtern und Zugriffsschlüsseln sucht, die für einen bestimmten Zeitraum nicht verwendet wurden. Wenn ungenutzte Anmeldeinformationen identifiziert werden, müssen Sie sie deaktivieren und/oder entfernen, da dies gegen das Prinzip der geringsten Berechtigung verstoßen könnte. Für diese Regel müssen Sie einen Wert für das maxCredentialUsage Alter festlegen (Standardkonfiguration: 90). Der tatsächliche Wert muss den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-3	Das Informati onssystem setzt genehmigte Autorisie rungen für den logischen Zugriff auf Informationen und Systemressourcen gemäß den geltenden Zugriffskontrollri chtlinien durch.	lambda-function-pu blic-access-verboten	Verwalten Sie den Zugriff auf Ressource n in der AWS Cloud, indem Sie sicherste llen, dass AWS Lambda-Funktionen nicht öffentlich zugänglich sind. Der öffentliche Zugriff kann möglicherweise die Verfügbarkeit von Ressourcen beeinträc htigen.
AC-3	Das Informati onssystem setzt genehmigte Autorisie rungen für den logischen Zugriff auf Informationen und Systemressourcen gemäß den geltenden Zugriffskontrollri chtlinien durch.	rds-snapshots-public-prohibited	Verwalten Sie den Zugriff auf Ressource n in der AWS Cloud, indem Sie sicherste llen, dass Amazon Relational Database Service (Amazon RDS) -Instance s nicht öffentlic h sind. Amazon-RDS-Datenbank-Instances können vertrauliche Informati onen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-3	Das Informati onssystem setzt genehmigte Autorisie rungen für den logischen Zugriff auf Informationen und Systemressourcen gemäß den geltenden Zugriffskontrollri chtlinien durch.	redshift-cluster-public-access-überprüfen	Verwalten Sie den Zugriff auf Ressource n in der AWS Cloud, indem Sie sicherste llen, dass Amazon Redshift Redshift-Cluster nicht öffentlic h sind. Amazon-Re dshift-Cluster können vertrauliche Informati onen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-3	Das Informationssystem setzt genehmigte Autorisierungen für den logischen Zugriff auf Informationen und Systemressourcen gemäß den geltenden Zugriffskontrollrichtlinien durch.	iam-user-group-membership-überprüfen	AWS Identity and Access Management (IAM) kann Ihnen helfen, Zugriffsberechtigungen und Autorisierungen einzuschränken, indem sichergestellt wird, dass IAM-Benutzer Mitglieder mindestens einer Gruppe sind. Wenn Benutzern mehr Berechtigungen eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und Aufgabentrennung verstoßen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-3	Das Informati onssystem setzt genehmigte Autorisie rungen für den logischen Zugriff auf Informationen und Systemressourcen gemäß den geltenden Zugriffskontrollri chtlinien durch.	s-3 bucket-public-read -prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie nur autorisierten Benutzern, Prozessen und Geräten Zugriff auf Amazon Simple Storage Service (Amazon S3) - Buckets gewähren. Die Verwaltung des Zugriffs sollte mit der Klassifizierung der Daten übereinst immen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-3	Das Informati onssystem setzt genehmigte Autorisie rungen für den logischen Zugriff auf Informationen und Systemressourcen gemäß den geltenden Zugriffskontrollri chtlinien durch.	iam-root-access-key-überprüfen	Der Zugriff auf Systeme und Ressourcen kann gesteuert werden, indem überprüft wird, ob der Root-Benu tzer keine Zugriffss chlüssel mit seiner AWS Identity and Access Management (IAM) -Rolle verknüpft hat. Stellen Sie sicher, dass die Root-Zugr iffsschlüssel gelöscht werden. Erstellen und verwenden Sie stattdessen rollenbas ierte AWS Konten, um dem Prinzip der geringsten Funktiona lität Rechnung zu tragen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-3	Das Informati onssystem setzt genehmigte Autorisie rungen für den logischen Zugriff auf Informationen und Systemressourcen gemäß den geltenden Zugriffskontrollri chtlinien durch.	dms-replication-not-public	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass auf DMS-Replikationsin stanzen nicht öffentlic h zugegriffen werden kann. DMS-Repli kations-Instances können vertrauli che Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.
AC-3	Das Informati onssystem setzt genehmigte Autorisie rungen für den logischen Zugriff auf Informationen und Systemressourcen gemäß den geltenden Zugriffskontrollri chtlinien durch.	ebs-snapshot-public-restorable-überprüfen	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass EBS-Snapshots nicht öffentlich wiederher stellbar sind. EBS-Volume-Snapsho ts können vertrauli che Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-3	Das Informationssystem setzt genehmigte Autorisierungen für den logischen Zugriff auf Informationen und Systemressourcen gemäß den geltenden Zugriffskontrollrichtlinien durch.	iam-group-has-users-überprüfen	AWS Identity and Access Management (IAM) kann Ihnen helfen, die Prinzipien der geringsten Rechte und der Aufgabentrennung mit Zugriffsberechtigungen und Autorisierungen zu integrieren, indem sichergestellt wird, dass IAM-Gruppen mindestens einen IAM-Benutzer haben. Die Einteilung von IAM-Benutzern in Gruppen auf der Grundlage der ihnen zugewiesenen Berechtigungen oder Aufgabenbereiche ist eine Möglichkeit, die geringsten Rechte zu berücksichtigen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-3	Das Informationssystem setzt genehmigte Autorisierungen für den logischen Zugriff auf Informationen und Systemressourcen gemäß den geltenden Zugriffskontrollrichtlinien durch.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) kann Ihnen dabei helfen, die Prinzipien der geringsten Rechte und der Aufgabentrennung in Zugriffsberechtigungen und Autorisierungen zu integrieren und so zu verhindern, dass Richtlinien „Effect“: „Allow“ mit „Action“: „*“ anstelle von „Resource“: „*“ enthalten. Wenn Benutzern mehr Rechte eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und der Aufgabentrennung verstoßen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-3	Das Informati onssystem setzt genehmigte Autorisie rungen für den logischen Zugriff auf Informationen und Systemressourcen gemäß den geltenden Zugriffskontrollri chtlinien durch.	sagemaker-notebook -no-direct-Interne tzugang	Verwalten Sie den Zugriff auf Ressource n in der AWS Cloud, indem Sie sicherste llen, dass SageMaker Amazon-Notebooks keinen direkten Internetzugang zulassen. Indem Sie direkten Internetz ugang blockieren, vermeiden Sie, dass unbefugte Benutzer auf sensible Daten zugreifen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-3	Das Informati onssystem setzt genehmigte Autorisie rungen für den logischen Zugriff auf Informationen und Systemressourcen gemäß den geltenden Zugriffskontrollri chtlinien durch.	ec2-imdsv2-check	Stellen Sie sicher, dass die Methode Instance Metadata Service Version 2 (IMDSv2) aktiviert ist, um den Zugriff auf und die Kontrolle der Amazon Elastic Compute Cloud (Amazon EC2) - Instance-Metadate n zu schützen. Die IMDSv2 Methode verwendet sitzungsb asierte Kontrollen. Mit können Kontrolle n implementiert werden IMDSv2, um Änderungen an Instanzmetadaten einzuschränken.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-3	Das Informati onssystem setzt genehmigte Autorisie rungen für den logischen Zugriff auf Informationen und Systemressourcen gemäß den geltenden Zugriffskontrollri chtlinien durch.	ec2- instance-profile-a ttached	EC2 Instanzprofile übergeben eine IAM-Rolle an eine EC2 Instanz. Das Anhängen eines Instance-Profils an Ihre Instances kann bei der Implement ierung von geringste n Berechtigungen und der Berechtig ungsverwaltung helfen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-3	Das Informati onssystem setzt genehmigte Autorisie rungen für den logischen Zugriff auf Informationen und Systemressourcen gemäß den geltenden Zugriffskontrollri chtlinien durch.	iam-no-inline-policy-überprüfen	Stellen Sie sicher, dass ein Benutzer, eine IAM-Rolle oder eine IAM-Gruppe (AWS Identity and Access Management) nicht über eine Inline-Richtlinie zur Zugriffsk ontrolle auf Systeme und Ressource n verfügt. AWS empfiehlt, verwaltet e Richtlinien anstelle von Inline-Richtlinien zu verwenden. Verwaltete Richtlini en ermöglichen Wiederverwendbarke it, Versionsverwaltung , Rollback und Delegierung der Berechtigungsverwa ltung.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-3	Das Informati onssystem setzt genehmigte Autorisie rungen für den logischen Zugriff auf Informationen und Systemressourcen gemäß den geltenden Zugriffskontrollri chtlinien durch.	iam-policy-no-stat ements-with-full-a ccess	Stellen Sie sicher, dass IAM-Aktionen nur auf die benötigte n Aktionen beschränkt sind. Wenn Benutzern mehr Rechte eingeräumt werden, als für die Ausführun g einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringste n Berechtigung und der Aufgabentrennung verstoßen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-3	Das Informati onssystem setzt genehmigte Autorisie rungen für den logischen Zugriff auf Informationen und Systemressourcen gemäß den geltenden Zugriffskontrollri chtlinien durch.	ecs-task-definition-user-for-host-mode-check	Wenn für eine Aufgabendefinition erhöhte Berechtig ungen gelten, liegt das daran, dass der Kunde diesen Konfigura tionen ausdrücklich zugestimmt hat. Diese Kontrolle prüft, ob eine unerwartete Berechtigungseskal ation vorliegt, wenn für eine Aufgabend efinition das Host-Netzwerk aktiviert ist, die Kunden aber keine erhöhten Berechtigungen aktiviert haben.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-3	Das Informati onssystem setzt genehmigte Autorisie rungen für den logischen Zugriff auf Informationen und Systemressourcen gemäß den geltenden Zugriffskontrollri chtlinien durch.	ec2- instance-no-public-ip	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon Elastic Compute Cloud (Amazon EC2) - Instances nicht öffentlich zugänglich sind. EC2 Amazon-Instances können vertrauliche Informati onen enthalten, und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-3	Das Informati onssystem setzt genehmigte Autorisie rungen für den logischen Zugriff auf Informationen und Systemressourcen gemäß den geltenden Zugriffskontrollri chtlinien durch.	elasticsearch-in-vpc-only	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherste llen, dass sich Amazon OpenSearc h OpenSearch Service (Service) - Domains innerhalb einer Amazon Virtual Private Cloud (Amazon VPC) befinden. Eine OpenSearch Service-Domain innerhalb einer Amazon VPC ermöglicht die sichere Kommunikation zwischen OpenSearc h Service und anderen Services innerhalb der Amazon VPC, ohne dass ein Internet-Gateway, ein NAT-Gerät oder eine VPN-Verbindung erforderlich ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-3	Das Informati onssystem setzt genehmigte Autorisie rungen für den logischen Zugriff auf Informationen und Systemressourcen gemäß den geltenden Zugriffskontrollri chtlinien durch.	emr-master-no-public-ip	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon EMR-Clust er-Masterknoten nicht öffentlich zugänglic h sind. Amazon-EM R-Cluster-Hauptkno ten können vertrauli che Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-3	Das Informati onssystem setzt genehmigte Autorisie rungen für den logischen Zugriff auf Informationen und Systemressourcen gemäß den geltenden Zugriffskontrollri chtlinien durch.	lambda-inside-vpc	Stellen Sie AWS Lambda-Funktionen in einer Amazon Virtual Private Cloud (Amazon VPC) bereit, um eine sichere Kommunika tion zwischen einer Funktion und anderen Diensten innerhalb der Amazon VPC zu gewährleisten. Bei dieser Konfiguration sind kein Internet-Gateway, kein NAT-Gerät und keine VPN-Verbindung erforderlich. Der gesamte Datenverk ehr bleibt sicher in der Cloud. AWS Domains, die sich innerhalb einer VPC befinden, verfügen aufgrund ihrer logischen Isolierun g im Vergleich zu Domains mit öffentlic hen Endpunkten über eine zusätzliche Sicherheitsebene. Um den Zugriff ordnungsg emäß zu verwalten,

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			sollten AWS Lambda-Funktionen einer VPC zugewiesen werden.
AC-3	Das Informationssystem setzt genehmigte Autorisierungen für den logischen Zugriff auf Informationen und Systemressourcen gemäß den geltenden Zugriffskontrollrichtlinien durch.	rds-instance-public-access-überprüfen	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Relational Database Service (Amazon RDS) -Instances nicht öffentlich sind. Amazon-RDS-Datenbank-Instances können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-3	Das Informati onssystem setzt genehmigte Autorisie rungen für den logischen Zugriff auf Informationen und Systemressourcen gemäß den geltenden Zugriffskontrollri chtlinien durch.	account-level-publ ic-accesss3-Blöcke-periodisch	Verwalten Sie den Zugriff auf Ressource n in der AWS Cloud, indem Sie sicherste llen, dass Amazon Simple Storage Service (Amazon S3) -Buckets nicht öffentlich zugänglic h sind. Diese Regel trägt dazu bei, sensible Daten vor unbefugten Remote-Benutzern zu schützen, indem sie den öffentlichen Zugriff verhinder t. Mit dieser Regel können Sie optional die Parameter ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) und restrictPublicBuck ets Parameter (Config Default: True) festlegen. Die tatsächlichen Werte müssen den Richtlini

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			en Ihrer Organisation entsprechen.
AC-3	Das Informati onssystem setzt genehmigte Autorisie rungen für den logischen Zugriff auf Informationen und Systemressourcen gemäß den geltenden Zugriffskontrollri chtlinien durch.	s3 bucket-level-public-access - verboten	Verwalten Sie den Zugriff auf Ressource n in der AWS Cloud, indem Sie sicherste llen, dass Amazon Simple Storage Service (Amazon S3) -Buckets nicht öffentlich zugänglic h sind. Diese Regel trägt dazu bei, sensible Daten vor unbefugten Remote-Benutzern zu schützen, indem sie den öffentlichen Zugriff auf Bucket-Eb ene verhindert.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-3	Das Informati onssystem setzt genehmigte Autorisie rungen für den logischen Zugriff auf Informationen und Systemressourcen gemäß den geltenden Zugriffskontrollri chtlinien durch.	ssm-document-not-p ublic	Stellen Sie sicher, dass AWS Systems Manager (SSM) - Dokumente nicht öffentlich sind, da dies einen unbeabsic htigten Zugriff auf Ihre SSM-Dokum ente ermöglichen kann. Ein öffentlic hes SSM-Dokum ent kann Informati onen über Ihr Konto, Ihre Ressourcen und internen Prozesse preisgeben.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-3	Das Informati onssystem setzt genehmigte Autorisie rungen für den logischen Zugriff auf Informationen und Systemressourcen gemäß den geltenden Zugriffskontrollri chtlinien durch.	subnet-auto-assign-public-ip-deaktiviert	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon Virtual Private Cloud (VPC) -Subnetzen nicht automatisch eine öffentliche IP-Adress e zugewiesen wird. Amazon Elastic Compute Cloud (EC2) -Instances, die in Subnetzen gestartet werden, in denen dieses Attribut aktiviert ist, haben ihrer primären Netzwerkschnittste lle eine öffentliche IP-Adresse zugewiesen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-3	Das Informati onssystem setzt genehmigte Autorisie rungen für den logischen Zugriff auf Informationen und Systemressourcen gemäß den geltenden Zugriffskontrollri chtlinien durch.	autoscaling-launch -config-public-ip- deaktiviert	Wenn Sie Ihre Netzwerkschnittstellen mit einer öffentlichen IP-Adresse konfiguri eren, sind die diesen Netzwerkschnittste llen zugehörigen Ressourcen über das Internet erreichba r. EC2 Ressourcen sollten nicht öffentlic h zugänglich sein, da dies einen unbeabsic htigten Zugriff auf Ihre Anwendungen oder Server ermöglichen kann.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-4	Das Informationssystem setzt genehmigte Autorisierungen für die Kontrolle des Informationsflusses innerhalb des Systems und zwischen miteinander vernetzten Systemen auf der Grundlage von [Zuweisung: von der Organisation definierte Richtlinien zur Kontrolle des Informationsflusses] durch.	lambda-function-public-access-verboten	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass AWS Lambda-Funktionen nicht öffentlich zugänglich sind. Der öffentliche Zugriff kann möglicherweise die Verfügbarkeit von Ressourcen beeinträchtigen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-4	Das Informationssystem setzt genehmigte Autorisierungen für die Kontrolle des Informationsflusses innerhalb des Systems und zwischen miteinander vernetzten Systemen auf der Grundlage von [Zuweisung: von der Organisation definierte Richtlinien zur Kontrolle des Informationsflusses] durch.	redshift-cluster-public-access-überprüfen	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Redshift Redshift-Cluster nicht öffentlich sind. Amazon-Redshift-Cluster können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-4	Das Informationssystem setzt genehmigte Autorisierungen für die Kontrolle des Informationsflusses innerhalb des Systems und zwischen miteinander vernetzten Systemen auf der Grundlage von [Zuweisung: von der Organisation definierte Richtlinien zur Kontrolle des Informationsflusses] durch.	rds-snapshots-public-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Relational Database Service (Amazon RDS) -Instances nicht öffentlich sind. Amazon-RDS-Datenbank-Instances können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-4	Das Informationssystem setzt genehmigte Autorisierungen für die Kontrolle des Informationsflusses innerhalb des Systems und zwischen miteinander vernetzten Systemen auf der Grundlage von [Zuweisung: von der Organisation definierte Richtlinien zur Kontrolle des Informationsflusses] durch.	rds-instance-public-access-überprüfen	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Relational Database Service (Amazon RDS) -Instances nicht öffentlich sind. Amazon-RDS-Datenbank-Instances können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-4	Das Informati onssystem setzt genehmigte Autorisie rungen für die Kontrolle des Informationsflusse s innerhalb des Systems und zwischen miteinander vernetzten Systemen auf der Grundlage von [Zuweisung: von der Organisation definierte Richtlini en zur Kontrolle des Informationsflusses] durch.	lambda-inside-vpc	Stellen Sie AWS Lambda-Funktionen in einer Amazon Virtual Private Cloud (Amazon VPC) bereit, um eine sichere Kommunika tion zwischen einer Funktion und anderen Diensten innerhalb der Amazon VPC zu gewährleisten. Bei dieser Konfiguration sind kein Internet-Gateway, kein NAT-Gerät und keine VPN-Verbindung erforderlich. Der gesamte Datenverk ehr bleibt sicher in der Cloud. AWS Domains, die sich innerhalb einer VPC befinden, verfügen aufgrund ihrer logischen Isolierun g im Vergleich zu Domains mit öffentlic hen Endpunkten über eine zusätzliche Sicherheitsebene. Um den Zugriff ordnungsg emäß zu verwalten,

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			sollten AWS Lambda-Funktionen einer VPC zugewiesen werden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-4	Das Informati onssystem setzt genehmigte Autorisie rungen für die Kontrolle des Informationsflusse s innerhalb des Systems und zwischen miteinander vernetzten Systemen auf der Grundlage von [Zuweisung: von der Organisation definierte Richtlini en zur Kontrolle des Informationsflusses] durch.	ec2- instances-in-vpc	Stellen Sie Amazon Elastic Compute Cloud (Amazon EC2) -Instances innerhalb einer Amazon Virtual Private Cloud (Amazon VPC) bereit, um eine sichere Kommunika tion zwischen einer Instance und anderen Services innerhalb der Amazon VPC zu ermöglichen, ohne dass ein Internet-Gateway, ein NAT-Gerät oder eine VPN-Verbindung erforderlich ist. Der gesamte Datenverk ehr bleibt sicher in der AWS Cloud. Domains, die sich innerhalb einer VPC befinden, verfügen aufgrund ihrer logischen Isolierun g im Vergleich zu Domains mit öffentlic hen Endpunkten über eine zusätzlic he Sicherheitsebene. Weisen Sie EC2

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			Amazon-Instances einer Amazon-VPC zu, um den Zugriff ordnungsgemäß zu verwalten.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-4	Das Informationssystem setzt genehmigte Autorisierungen für die Kontrolle des Informationsflusses innerhalb des Systems und zwischen miteinander vernetzten Systemen auf der Grundlage von [Zuweisung: von der Organisation definierte Richtlinien zur Kontrolle des Informationsflusses] durch.	restricted-common-ports	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass gemeinsame Ports für Amazon Elastic Compute Cloud (Amazon EC2) -Sicherheitsgruppen eingeschränkt sind. Wenn der Zugriff auf Ports nicht auf vertrauenswürdige Quellen beschränkt wird, kann dies zu Angriffen auf die Verfügbarkeit, Integrität und Vertraulichkeit von Systemen führen. Mit dieser Regel können Sie optional die Parameter blockedPort1–blockedPort5 festlegen (Standardkonfigurationen: 20, 21, 3389, 3306, 4333). Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-4	Das Informati onssystem setzt genehmigte Autorisie rungen für die Kontrolle des Informationsflusse s innerhalb des Systems und zwischen miteinander vernetzten Systemen auf der Grundlage von [Zuweisung: von der Organisation definierte Richtlini en zur Kontrolle des Informationsflusses] durch.	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) Security Groups können bei der Verwaltung des Netzwerkzugriffs helfen, indem sie eine statusbeh aftete Filterung von eingehendem und ausgehendem Netzwerkverkehr zu Ressourcen bereitste llen. AWS Wenn Sie eingehenden (oder entfernten) Datenverk ehr von 0.0.0.0/0 bis Port 22 auf Ihren Ressourcen nicht zulassen, können Sie den Remote-Zugriff einschränken.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-4	Das Informationssystem setzt genehmigte Autorisierungen für die Kontrolle des Informationsflusses innerhalb des Systems und zwischen miteinander vernetzten Systemen auf der Grundlage von [Zuweisung: von der Organisation definierte Richtlinien zur Kontrolle des Informationsflusses] durch.	s-3 bucket-public-read-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie nur autorisierten Benutzern, Prozessen und Geräten Zugriff auf Amazon Simple Storage Service (Amazon S3) - Buckets gewähren. Die Verwaltung des Zugriffs sollte mit der Klassifizierung der Daten übereinstimmen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-4	Das Informationssystem setzt genehmigte Autorisierungen für die Kontrolle des Informationsflusses innerhalb des Systems und zwischen miteinander vernetzten Systemen auf der Grundlage von [Zuweisung: von der Organisation definierte Richtlinien zur Kontrolle des Informationsflusses] durch.	sagemaker-notebook-no-direct-Internetzugang	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass SageMaker Amazon-Notebooks keinen direkten Internetzugang zulassen. Indem Sie direkten Internetzugang blockieren, vermeiden Sie, dass unbefugte Benutzer auf sensible Daten zugreifen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-4	Das Informati onssystem setzt genehmigte Autorisie rungen für die Kontrolle des Informationsflusse s innerhalb des Systems und zwischen miteinander vernetzten Systemen auf der Grundlage von [Zuweisung: von der Organisation definierte Richtlini en zur Kontrolle des Informationsflusses] durch.	vpc-default-security-group-geschlossen	Sicherheitsgruppen von Amazon Elastic Compute Cloud (Amazon EC2) können bei der Verwaltung des Netzwerkzugriffs helfen, indem sie eine statusbehaftete Filterung des ein- und ausgehenden Netzwerkverkehrs zu Ressourcen bereitstellen. AWS Die Beschränk ung des gesamten Datenverkehrs auf die Standardsicherheit sgruppe hilft dabei, den Fernzugriff auf Ihre Ressourcen einzuschränken. AWS

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-4	Das Informationssystem setzt genehmigte Autorisierungen für die Kontrolle des Informationsflusses innerhalb des Systems und zwischen miteinander vernetzten Systemen auf der Grundlage von [Zuweisung: von der Organisation definierte Richtlinien zur Kontrolle des Informationsflusses] durch.	vpc-sg-open-only-to-authorized-ports	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass gemeinsame Ports für Amazon Elastic Compute Cloud (Amazon EC2) -Sicherheitsgruppen eingeschränkt sind. Wenn der Zugriff auf Ports nicht auf vertrauenswürdige Quellen beschränkt wird, kann dies zu Angriffen auf die Verfügbarkeit, Integrität und Vertraulichkeit von Systemen führen. Durch die Beschränkung des Zugriffs auf Ressourcen innerhalb einer Sicherheitsgruppe aus dem Internet (0.0.0.0/0) kann der Fernzugriff auf interne Systeme gesteuert werden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-4	Das Informationssystem setzt genehmigte Autorisierungen für die Kontrolle des Informationsflusses innerhalb des Systems und zwischen miteinander vernetzten Systemen auf der Grundlage von [Zuweisung: von der Organisation definierte Richtlinien zur Kontrolle des Informationsflusses] durch.	s-3 bucket-public-write-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie nur autorisierten Benutzern, Prozessen und Geräten Zugriff auf Amazon Simple Storage Service (Amazon S3) - Buckets gewähren. Die Verwaltung des Zugriffs sollte mit der Klassifizierung der Daten übereinstimmen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-4	Das Informati onssystem setzt genehmigte Autorisie rungen für die Kontrolle des Informationsflusse s innerhalb des Systems und zwischen miteinander vernetzten Systemen auf der Grundlage von [Zuweisung: von der Organisation definierte Richtlini en zur Kontrolle des Informationsflusses] durch.	acm-certificate-ex piration-check	Stellen Sie sicher, dass die Netzwerki ntegrität geschützt ist, indem Sie sicherste llen, dass X509-Zertifikate von AWS ACM ausgestel lt werden. Diese Zertifikate müssen gültig und dürfen nicht abgelaufen sein. Für diese Regel ist ein Wert für erforderlich daysToExpiration (Wert für bewährte AWS Grundregeln für Sicherheit: 90). Der tatsächliche Wert muss den Richtlini en Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-4	Das Informati onssystem setzt genehmigte Autorisie rungen für die Kontrolle des Informationsflusse s innerhalb des Systems und zwischen miteinander vernetzten Systemen auf der Grundlage von [Zuweisung: von der Organisation definierte Richtlini en zur Kontrolle des Informationsflusses] durch.	ec2- instance-no-public-ip	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon Elastic Compute Cloud (Amazon EC2) - Instances nicht öffentlich zugänglich sind. EC2 Amazon-Instances können vertrauliche Informati onen enthalten, und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-4	Das Informationssystem setzt genehmigte Autorisierungen für die Kontrolle des Informationsflusses innerhalb des Systems und zwischen miteinander vernetzten Systemen auf der Grundlage von [Zuweisung: von der Organisation definierte Richtlinien zur Kontrolle des Informationsflusses] durch.	elasticsearch-in-vpc-only	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass sich Amazon OpenSearch OpenSearch Service (Service) - Domains innerhalb einer Amazon Virtual Private Cloud (Amazon VPC) befinden. Eine OpenSearch Service-Domain innerhalb einer Amazon VPC ermöglicht die sichere Kommunikation zwischen OpenSearch Service und anderen Services innerhalb der Amazon VPC, ohne dass ein Internet-Gateway, ein NAT-Gerät oder eine VPN-Verbindung erforderlich ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-4	Das Informationssystem setzt genehmigte Autorisierungen für die Kontrolle des Informationsflusses innerhalb des Systems und zwischen miteinander vernetzten Systemen auf der Grundlage von [Zuweisung: von der Organisation definierte Richtlinien zur Kontrolle des Informationsflusses] durch.	dms-replication-not-public	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass auf DMS-Replikationsinstanzen nicht öffentlich zugegriffen werden kann. DMS-Replikations-Instances können vertrauliche Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-4	Das Informati onssystem setzt genehmigte Autorisie rungen für die Kontrolle des Informationsflusse s innerhalb des Systems und zwischen miteinander vernetzten Systemen auf der Grundlage von [Zuweisung: von der Organisation definierte Richtlini en zur Kontrolle des Informationsflusses] durch.	ebs-snapshot-public-restorable-überprüfen	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass EBS-Snapshots nicht öffentlich wiederher stellbar sind. EBS-Volume-Snapsho ts können vertrauli che Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-4	Das Informationssystem setzt genehmigte Autorisierungen für die Kontrolle des Informationsflusses innerhalb des Systems und zwischen miteinander vernetzten Systemen auf der Grundlage von [Zuweisung: von der Organisation definierte Richtlinien zur Kontrolle des Informationsflusses] durch.	emr-master-no-public-ip	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon EMR-Cluster-Masterknoten nicht öffentlich zugänglich sind. Amazon-EMR-Cluster-Hauptknoten können vertrauliche Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-5c	Die Organisation: c. Definiert Zugriffsberechtigungen für das Informationssystem zur Unterstützung der Aufgabentrennung.	iam-group-has-users-überprüfen	AWS Identity and Access Management (IAM) kann Ihnen helfen, die Prinzipien der geringsten Rechte und der Aufgabentrennung mit Zugriffsberechtigungen und Autorisierungen zu integrieren, indem sichergestellt wird, dass IAM-Gruppen mindestens einen IAM-Benutzer haben. Die Einteilung von IAM-Benutzern in Gruppen auf der Grundlage der ihnen zugewiesenen Berechtigungen oder Aufgabenbereiche ist eine Möglichkeit, die geringsten Rechte zu berücksichtigen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-5c	Die Organisation: c. Definiert Zugriffsberechtigungen für das Informationssystem zur Unterstützung der Aufgabentrennung.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) kann Ihnen dabei helfen, die Prinzipien der geringsten Rechte und der Aufgabentrennung in Zugriffsberechtigungen und Autorisierungen zu integrieren und so zu verhindern, dass Richtlinien „Effect“: „Allow“ mit „Action“: „*“ anstelle von „Resource“: „*“ enthalten. Wenn Benutzern mehr Rechte eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und der Aufgabentrennung verstoßen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-5c	Die Organisation: c. Definiert Zugriffsb erechtigungen für das Informationssystem zur Unterstützung der Aufgabentrennung.	iam-user-no-policies-überprüfen	Diese Regel stellt sicher, dass AWS Identity and Access Management (IAM) -Richtlinien nur Gruppen oder Rollen zugewiese n werden, um den Zugriff auf Systeme und Ressourcen zu kontrollieren. Die Zuweisung von Berechtig ungen auf Gruppen- oder Rollenebene trägt dazu bei, die Wahrscheinlichkeit zu verringern, dass eine Identität übermäßige Berechtigungen erhält oder beibehält.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-5c	Die Organisation: c. Definiert Zugriffsberechtigungen für das Informationssystem zur Unterstützung der Aufgabentrennung.	iam-policy-no-statements-with-full-access	Stellen Sie sicher, dass IAM-Aktionen nur auf die benötigten Aktionen beschränkt sind. Wenn Benutzern mehr Rechte eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und der Aufgabentrennung verstoßen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-5c	Die Organisation: c. Definiert Zugriffsb erechtigungen für das Informationssystem zur Unterstützung der Aufgabentrennung.	ecs-task-definition-user-for-host-mode-check	Wenn für eine Aufgabendefinition erhöhte Berechtig ungen gelten, liegt das daran, dass der Kunde diesen Konfigura tionen ausdrücklich zugestimmt hat. Diese Kontrolle prüft, ob eine unerwartete Berechtigungseskal ation vorliegt, wenn für eine Aufgabend efinition das Host-Netzwerk aktiviert ist, die Kunden aber keine erhöhten Berechtigungen aktiviert haben.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-5c	Die Organisation: c. Definiert Zugriffsb erechtigungen für das Informationssystem zur Unterstützung der Aufgabentrennung.	iam-customer-policy-blocked-kms-Aktionen	AWS Identity and Access Managemen t (IAM) kann Ihnen helfen, die Prinzipien der geringsten Rechte und der Aufgabent rennung in Zugriffsb erechtigungen und Autorisierungen zu integrieren und so zu verhindern, dass Richtlinien blockiert e Aktionen für alle AWS Schlüssel des Key Management Service enthalten. Wenn Benutzer mehr Rechte haben, als für die Ausführung einer Aufgabe erforderl ich sind, kann dies gegen das Prinzip der geringsten Berechtig ung und Aufgabent rennung verstoßen . Mit dieser Regel können Sie den Parameter festlegen . blockedActionsPatt erns (Wert „AWS Bewährte grundlege nde Sicherhei tsmethoden“: kms:

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			Decrypt, kms:ReEncryptFrom). Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-5c	Die Organisation: c. Definiert Zugriffsb erechtigungen für das Informationssystem zur Unterstützung der Aufgabentrennung.	iam-inline-policy-blocked-kms-Aktionen	Stellen Sie sicher, dass ein Benutzer, eine IAM-Rolle oder eine IAM-Gruppe (AWS Identity and Access Management) nicht über eine Inline-Richtlinie verfügt, die blockierte Aktionen für alle AWS Schlüssel des Key Management Service zulässt. AWS empfiehlt, verwaltet e Richtlinien anstelle von Inline-Richtlinien zu verwenden. Verwaltete Richtlini en ermöglichen Wiederverwendbarke it, Versionsverwaltung , Rollback und Delegierung der Berechtigungsverwa ltung. Mit dieser Regel können Sie den blockedActionsPatt erns Parameter festlegen. (Wert „AWS Bewährte grundlege nde Sicherhei tsmethoden“: kms: Decrypt, kms:ReEnc ryptFrom). Die

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.
AC-5c	Die Organisation: c. Definiert Zugriffsberechtigungen für das Informationssystem zur Unterstützung der Aufgabentrennung.	iam-no-inline-policy-überprüfen	Stellen Sie sicher, dass ein Benutzer, eine IAM-Rolle oder eine IAM-Gruppe (AWS Identity and Access Management) nicht über eine Inline-Richtlinie zur Zugriffskontrolle auf Systeme und Ressourcen verfügt. AWS empfiehlt, verwaltete Richtlinien anstelle von Inline-Richtlinien zu verwenden. Verwaltete Richtlinien ermöglichen Wiederverwendbarkeit, Versionsverwaltung, Rollback und Delegierung der Berechtigungsverwaltung.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-5c	Die Organisation: c. Definiert Zugriffsb erechtigungen für das Informationssystem zur Unterstützung der Aufgabentrennung.	iam-password-policy	Die Identitäten und Anmeldeinformation en werden auf der Grundlage einer organisatorischen IAM-Passwortrichtlinie ausgestellt, verwaltet und verifiziert. Sie erfüllen oder übertreff en die Anforderungen von NIST SP 800-63 und dem Standard „Best Practices“ von AWS Foundatio nal Security für die Passwortstärke. Mit dieser Regel können Sie optional RequireUppercaseCh aracters (Wert für AWS grundlegende Sicherheitsbewährt e Methoden: wahr), RequireLowercaseCh aracters (Wert für bewährte Methoden für AWS grundlege nde Sicherheit: wahr), RequireSy mbols (Wert für bewährte Methoden für AWS grundlege nde Sicherheit:

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			wahr), RequireNumbers (Wert für bewährte Methoden für AWS grundlegende Sicherheit: wahr), MinimumPasswordLength (Wert für bewährte Methoden für AWS grundlegende Sicherheit: 14), PasswordReusePrevention (Wert für bewährte Methoden für AWS grundlegende Sicherheit: 24) und MaxPasswordAge (Wert für bewährte Methoden für AWS grundlegende Sicherheit: 90) für Ihr IAM festlegen Kennwortrichtlinie. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-5c	Die Organisation: c. Definiert Zugriffsb erechtigungen für das Informationssystem zur Unterstützung der Aufgabentrennung.	iam-root-access-key-überprüfen	Der Zugriff auf Systeme und Ressourcen kann gesteuert werden, indem überprüft wird, ob der Root-Benu tzer keine Zugriffss chlüssel mit seiner AWS Identity and Access Management (IAM) -Rolle verknüpft hat. Stellen Sie sicher, dass die Root-Zugr iffsschlüssel gelöscht werden. Erstellen und verwenden Sie stattdessen rollenbas ierte AWS Konten, um dem Prinzip der geringsten Funktiona lität Rechnung zu tragen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-5c	Die Organisation: c. Definiert Zugriffsberechtigungen für das Informationssystem zur Unterstützung der Aufgabentrennung.	iam-user-group-membership-überprüfen	AWS Identity and Access Management (IAM) kann Ihnen helfen, Zugriffsberechtigungen und Autorisierungen einzuschränken, indem sichergestellt wird, dass IAM-Benutzer Mitglieder mindestens einer Gruppe sind. Wenn Benutzern mehr Berechtigungen eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und Aufgabentrennung verstoßen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-5c	Die Organisation: c. Definiert Zugriffsberechtigungen für das Informationssystem zur Unterstützung der Aufgabentrennung.	iam-user-unused-credentials-überprüfen	AWS Identity and Access Management (IAM) kann Ihnen bei Zugriffsberechtigungen und Autorisierungen helfen, indem es nach IAM-Passwörtern und Zugriffsschlüsseln sucht, die für einen bestimmten Zeitraum nicht verwendet wurden. Wenn ungenutzte Anmeldeinformationen identifiziert werden, müssen Sie sie deaktivieren und/oder entfernen, da dies gegen das Prinzip der geringsten Berechtigung verstoßen könnte. Für diese Regel müssen Sie einen Wert für das maxCredentialUsage Alter festlegen (Standardkonfiguration: 90). Der tatsächliche Wert muss den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-6	Die Organisation wendet das Prinzip der geringsten Berechtigung an und erlaubt Benutzern (oder Prozessen , die im Namen von Benutzern handeln) nur dann den Zugriff, wenn dies für die Ausführun g zugewiesener Aufgaben gemäß den Unternehmenszielen und Geschäfts funktionen notwendig ist.	rds-snapshots-public-prohibited	Verwalten Sie den Zugriff auf Ressource n in der AWS Cloud, indem Sie sicherste llen, dass Amazon Relational Database Service (Amazon RDS) -Instance s nicht öffentlic h sind. Amazon-RDS-Datenbank-Instances können vertrauliche Informati onen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-6	Die Organisation wendet das Prinzip der geringsten Berechtigung an und erlaubt Benutzern (oder Prozessen , die im Namen von Benutzern handeln) nur dann den Zugriff, wenn dies für die Ausführun g zugewiesener Aufgaben gemäß den Unternehmenszielen und Geschäfts funktionen notwendig ist.	redshift-cluster-public-access-überprüfen	Verwalten Sie den Zugriff auf Ressource n in der AWS Cloud, indem Sie sicherste llen, dass Amazon Redshift Redshift-Cluster nicht öffentlic h sind. Amazon-Re dshift-Cluster können vertrauliche Informati onen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-6	Die Organisation wendet das Prinzip der geringsten Berechtigung an und erlaubt Benutzern (oder Prozessen , die im Namen von Benutzern handeln) nur dann den Zugriff, wenn dies für die Ausführun g zugewiesener Aufgaben gemäß den Unternehmenszielen und Geschäfts funktionen notwendig ist.	s-3 bucket-public-read -prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie nur autorisierten Benutzern, Prozessen und Geräten Zugriff auf Amazon Simple Storage Service (Amazon S3) - Buckets gewähren. Die Verwaltung des Zugriffs sollte mit der Klassifizierung der Daten übereinst immen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-6	Die Organisation wendet das Prinzip der geringsten Berechtigung an und erlaubt Benutzern (oder Prozessen , die im Namen von Benutzern handeln) nur dann den Zugriff, wenn dies für die Ausführung zugewiesener Aufgaben gemäß den Unternehmenszielen und Geschäfts funktionen notwendig ist.	s-3 bucket-public-write-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie nur autorisierten Benutzern, Prozessen und Geräten Zugriff auf Amazon Simple Storage Service (Amazon S3) - Buckets gewähren. Die Verwaltung des Zugriffs sollte mit der Klassifizierung der Daten übereinstimmen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-6	Die Organisation wendet das Prinzip der geringsten Berechtigung an und erlaubt Benutzern (oder Prozessen , die im Namen von Benutzern handeln) nur dann den Zugriff, wenn dies für die Ausführun g zugewiesener Aufgaben gemäß den Unternehmenszielen und Geschäfts funktionen notwendig ist.	sagemaker-notebook -no-direct-Interne tzugang	Verwalten Sie den Zugriff auf Ressource n in der AWS Cloud, indem Sie sicherste llen, dass SageMaker Amazon-Notebooks keinen direkten Internetzugang zulassen. Indem Sie direkten Internetz ugang blockieren, vermeiden Sie, dass unbefugte Benutzer auf sensible Daten zugreifen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-6	Die Organisation wendet das Prinzip der geringsten Berechtigung an und erlaubt Benutzern (oder Prozessen , die im Namen von Benutzern handeln) nur dann den Zugriff, wenn dies für die Ausführun g zugewiesener Aufgaben gemäß den Unternehmenszielen und Geschäfts funktionen notwendig ist.	lambda-function-pu blic-access-verboten	Verwalten Sie den Zugriff auf Ressource n in der AWS Cloud, indem Sie sicherste llen, dass AWS Lambda-Funktionen nicht öffentlich zugänglich sind. Der öffentliche Zugriff kann möglicherweise die Verfügbarkeit von Ressourcen beeinträc htigen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-6	Die Organisation wendet das Prinzip der geringsten Berechtigung an und erlaubt Benutzern (oder Prozessen , die im Namen von Benutzern handeln) nur dann den Zugriff, wenn dies für die Ausführun g zugewiesener Aufgaben gemäß den Unternehmenszielen und Geschäfts funktionen notwendig ist.	codebuild-project-envvar-awscred-überprüfen	Stellen Sie sicher, dass die Anmeldein formationen AWS_ACCES S_KEY_ID AWS_SECRE T_ACCESS_ KEY nicht in den AWS Codebuild-Projektumgebungen vorhanden sind. Speichern Sie diese Variablen nicht als Klartext. Das Speichern dieser Variablen als Klartext bewirkt eine unbeabsic htigte Offenlegung von Daten sowie unberechtigte Zugriffe.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-6	Die Organisation wendet das Prinzip der geringsten Berechtigung an und erlaubt Benutzern (oder Prozessen , die im Namen von Benutzern handeln) nur dann den Zugriff, wenn dies für die Ausführun g zugewiesener Aufgaben gemäß den Unternehmenszielen und Geschäfts funktionen notwendig ist.	ebs-snapshot-public-restorable-überprüfen	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass EBS-Snapshots nicht öffentlich wiederher stellbar sind. EBS-Volume-Snapsho ts können vertrauli che Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-6	Die Organisation wendet das Prinzip der geringsten Berechtigung an und erlaubt Benutzern (oder Prozessen, die im Namen von Benutzern handeln) nur dann den Zugriff, wenn dies für die Ausführung zugewiesener Aufgaben gemäß den Unternehmenszielen und Geschäftsfunktionen notwendig ist.	iam-user-unused-credentials-überprüfen	AWS Identity and Access Management (IAM) kann Ihnen bei Zugriffsberechtigungen und Autorisierungen helfen, indem es nach IAM-Passwörtern und Zugriffsschlüsseln sucht, die für einen bestimmten Zeitraum nicht verwendet wurden. Wenn ungenutzte Anmeldeinformationen identifiziert werden, müssen Sie sie deaktivieren und/oder entfernen, da dies gegen das Prinzip der geringsten Berechtigung verstoßen könnte. Für diese Regel müssen Sie einen Wert für das maxCredentialUsage Alter festlegen (Standardkonfiguration: 90). Der tatsächliche Wert muss den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-6	Die Organisation wendet das Prinzip der geringsten Berechtigung an und erlaubt Benutzern (oder Prozessen , die im Namen von Benutzern handeln) nur dann den Zugriff, wenn dies für die Ausführun g zugewiesener Aufgaben gemäß den Unternehmenszielen und Geschäfts funktionen notwendig ist.	iam-group-has-users-überprüfen	AWS Identity and Access Managemen t (IAM) kann Ihnen helfen, die Prinzipie n der geringsten Rechte und der Aufgabentrennung mit Zugriffsberechtigu ngen und Autorisie rungen zu integrier en, indem sicherges tellt wird, dass IAM-Gruppen mindestens einen IAM-Benutzer haben. Die Einteilun g von IAM-Benut zern in Gruppen auf der Grundlage der ihnen zugewiesenen Berechtigungen oder Aufgabenbereiche ist eine Möglichkeit, die geringsten Rechte zu berücksichtigen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-6	Die Organisation wendet das Prinzip der geringsten Berechtigung an und erlaubt Benutzern (oder Prozessen , die im Namen von Benutzern handeln) nur dann den Zugriff, wenn dies für die Ausführun g zugewiesener Aufgaben gemäß den Unternehmenszielen und Geschäfts funktionen notwendig ist.	iam-policy-no-stat ements-with-admin-access	AWS Identity and Access Managemen t (IAM) kann Ihnen dabei helfen, die Prinzipien der geringsten Rechte und der Aufgabent rennung in Zugriffsb erechtigungen und Autorisierungen zu integrieren und so zu verhindern, dass Richtlinien „Effect“: „Allow“ mit „Action“: „*“ anstelle von „Resource“: „*“ enthalten. Wenn Benutzern mehr Rechte eingeräum t werden, als für die Ausführung einer Aufgabe erforderl ich sind, kann dies gegen das Prinzip der geringsten Berechtigung und der Aufgabentrennung verstoßen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-6	Die Organisation wendet das Prinzip der geringsten Berechtigung an und erlaubt Benutzern (oder Prozessen , die im Namen von Benutzern handeln) nur dann den Zugriff, wenn dies für die Ausführun g zugewiesener Aufgaben gemäß den Unternehmenszielen und Geschäfts funktionen notwendig ist.	iam-root-access-key-überprüfen	Der Zugriff auf Systeme und Ressourcen kann gesteuert werden, indem überprüft wird, ob der Root-Benu tzer keine Zugriffss chlüssel mit seiner AWS Identity and Access Management (IAM) -Rolle verknüpft hat. Stellen Sie sicher, dass die Root-Zugr iffsschlüssel gelöscht werden. Erstellen und verwenden Sie stattdessen rollenbas ierte AWS Konten, um dem Prinzip der geringsten Funktiona lität Rechnung zu tragen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-6	Die Organisation wendet das Prinzip der geringsten Berechtigung an und erlaubt Benutzern (oder Prozessen , die im Namen von Benutzern handeln) nur dann den Zugriff, wenn dies für die Ausführun g zugewiesener Aufgaben gemäß den Unternehmenszielen und Geschäfts funktionen notwendig ist.	iam-user-group-mem bership-überprüfen	AWS Identity and Access Managemen t (IAM) kann Ihnen helfen, Zugriffsb erechtigungen und Autorisierungen einzuschränken, indem sicherges tellt wird, dass IAM-Benutzer Mitgliede r mindestens einer Gruppe sind. Wenn Benutzern mehr Berechtigungen eingeräumt werden, als für die Ausführun g einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringste n Berechtigung und Aufgabentrennung verstoßen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-6	Die Organisation wendet das Prinzip der geringsten Berechtigung an und erlaubt Benutzern (oder Prozessen , die im Namen von Benutzern handeln) nur dann den Zugriff, wenn dies für die Ausführun g zugewiesener Aufgaben gemäß den Unternehmenszielen und Geschäfts funktionen notwendig ist.	iam-user-no-policies-überprüfen	Diese Regel stellt sicher, dass AWS Identity and Access Management (IAM) -Richtlinien nur Gruppen oder Rollen zugewiese n werden, um den Zugriff auf Systeme und Ressourcen zu kontrollieren. Die Zuweisung von Berechtig ungen auf Gruppen- oder Rollenebene trägt dazu bei, die Wahrscheinlichkeit zu verringern, dass eine Identität übermäßige Berechtigungen erhält oder beibehält.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-6	Die Organisation wendet das Prinzip der geringsten Berechtigung an und erlaubt Benutzern (oder Prozessen , die im Namen von Benutzern handeln) nur dann den Zugriff, wenn dies für die Ausführun g zugewiesener Aufgaben gemäß den Unternehmenszielen und Geschäfts funktionen notwendig ist.	dms-replication-not-public	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass auf DMS-Replikationsin stanzen nicht öffentlic h zugegriffen werden kann. DMS-Repli kations-Instances können vertrauli che Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-6	Die Organisation wendet das Prinzip der geringsten Berechtigung an und erlaubt Benutzern (oder Prozessen , die im Namen von Benutzern handeln) nur dann den Zugriff, wenn dies für die Ausführun g zugewiesener Aufgaben gemäß den Unternehmenszielen und Geschäfts funktionen notwendig ist.	rds-instance-public-access-überprüfen	Verwalten Sie den Zugriff auf Ressource n in der AWS Cloud, indem Sie sicherste llen, dass Amazon Relational Database Service (Amazon RDS) -Instance s nicht öffentlic h sind. Amazon-RDS-Datenbank-Instances können vertrauliche Informati onen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-6	Die Organisation wendet das Prinzip der geringsten Berechtigung an und erlaubt Benutzern (oder Prozessen , die im Namen von Benutzern handeln) nur dann den Zugriff, wenn dies für die Ausführun g zugewiesener Aufgaben gemäß den Unternehmenszielen und Geschäfts funktionen notwendig ist.	ec2- instance-no-public-ip	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon Elastic Compute Cloud (Amazon EC2) - Instances nicht öffentlich zugänglich sind. EC2 Amazon-Instances können vertrauliche Informati onen enthalten, und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-6	Die Organisation wendet das Prinzip der geringsten Berechtigung an und erlaubt Benutzern (oder Prozessen , die im Namen von Benutzern handeln) nur dann den Zugriff, wenn dies für die Ausführun g zugewiesener Aufgaben gemäß den Unternehmenszielen und Geschäfts funktionen notwendig ist.	ec2-imdsv2-check	Stellen Sie sicher, dass die Methode Instance Metadata Service Version 2 (IMDSv2) aktiviert ist, um den Zugriff auf und die Kontrolle der Amazon Elastic Compute Cloud (Amazon EC2) - Instance-Metadate n zu schützen. Die IMDSv2 Methode verwendet sitzungsb asierte Kontrollen. Mit können Kontrolle n implementiert werden IMDSv2, um Änderungen an Instanzmetadaten einzuschränken.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-6	Die Organisation wendet das Prinzip der geringsten Berechtigung an und erlaubt Benutzern (oder Prozessen , die im Namen von Benutzern handeln) nur dann den Zugriff, wenn dies für die Ausführun g zugewiesener Aufgaben gemäß den Unternehmenszielen und Geschäfts funktionen notwendig ist.	iam-no-inline-policy-überprüfen	Stellen Sie sicher, dass ein Benutzer, eine IAM-Rolle oder eine IAM-Gruppe (AWS Identity and Access Management) nicht über eine Inline-Richtlinie zur Zugriffsk ontrolle auf Systeme und Ressource n verfügt. AWS empfiehlt, verwaltet e Richtlinien anstelle von Inline-Richtlinien zu verwenden. Verwaltete Richtlini en ermöglichen Wiederverwendbarke it, Versionsverwaltung , Rollback und Delegierung der Berechtigungsverwa ltung.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-6	Die Organisation wendet das Prinzip der geringsten Berechtigung an und erlaubt Benutzern (oder Prozessen , die im Namen von Benutzern handeln) nur dann den Zugriff, wenn dies für die Ausführun g zugewiesener Aufgaben gemäß den Unternehmenszielen und Geschäfts funktionen notwendig ist.	elasticsearch-in-vpc-only	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherste llen, dass sich Amazon OpenSearc h OpenSearch Service (Service) - Domains innerhalb einer Amazon Virtual Private Cloud (Amazon VPC) befinden. Eine OpenSearch Service-Domain innerhalb einer Amazon VPC ermöglicht die sichere Kommunikation zwischen OpenSearc h Service und anderen Services innerhalb der Amazon VPC, ohne dass ein Internet-Gateway, ein NAT-Gerät oder eine VPN-Verbindung erforderlich ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-6	Die Organisation wendet das Prinzip der geringsten Berechtigung an und erlaubt Benutzern (oder Prozessen , die im Namen von Benutzern handeln) nur dann den Zugriff, wenn dies für die Ausführun g zugewiesener Aufgaben gemäß den Unternehmenszielen und Geschäfts funktionen notwendig ist.	emr-master-no-public-ip	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon EMR-Clust er-Masterknoten nicht öffentlich zugänglic h sind. Amazon-EM R-Cluster-Hauptkno ten können vertrauli che Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-6	Die Organisation wendet das Prinzip der geringsten Berechtigung an und erlaubt Benutzern (oder Prozessen , die im Namen von Benutzern handeln) nur dann den Zugriff, wenn dies für die Ausführun g zugewiesener Aufgaben gemäß den Unternehmenszielen und Geschäfts funktionen notwendig ist.	ec2- instances-in-vpc	Stellen Sie Amazon Elastic Compute Cloud (Amazon EC2) -Instances innerhalb einer Amazon Virtual Private Cloud (Amazon VPC) bereit, um eine sichere Kommunika tion zwischen einer Instance und anderen Services innerhalb der Amazon VPC zu ermöglichen, ohne dass ein Internet-Gateway, ein NAT-Gerät oder eine VPN-Verbindung erforderlich ist. Der gesamte Datenverk ehr bleibt sicher in der AWS Cloud. Domains, die sich innerhalb einer VPC befinden, verfügen aufgrund ihrer logischen Isolierun g im Vergleich zu Domains mit öffentlic hen Endpunkten über eine zusätzlic he Sicherheitsebene. Weisen Sie EC2

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			Amazon-Instances einer Amazon-VPC zu, um den Zugriff ordnungsgemäß zu verwalten.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-6	Die Organisation wendet das Prinzip der geringsten Berechtigung an und erlaubt Benutzern (oder Prozessen , die im Namen von Benutzern handeln) nur dann den Zugriff, wenn dies für die Ausführun g zugewiesener Aufgaben gemäß den Unternehmenszielen und Geschäfts funktionen notwendig ist.	lambda-inside-vpc	Stellen Sie AWS Lambda-Funktionen in einer Amazon Virtual Private Cloud (Amazon VPC) bereit, um eine sichere Kommunika tion zwischen einer Funktion und anderen Diensten innerhalb der Amazon VPC zu gewährleisten. Bei dieser Konfiguration sind kein Internet-Gateway, kein NAT-Gerät und keine VPN-Verbindung erforderlich. Der gesamte Datenverk ehr bleibt sicher in der Cloud. AWS Domains, die sich innerhalb einer VPC befinden, verfügen aufgrund ihrer logischen Isolierun g im Vergleich zu Domains mit öffentlic hen Endpunkten über eine zusätzliche Sicherheitsebene. Um den Zugriff ordnungsg emäß zu verwalten,

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			sollten AWS Lambda-Funktionen einer VPC zugewiesen werden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-6	Die Organisation wendet das Prinzip der geringsten Berechtigung an und erlaubt Benutzern (oder Prozessen , die im Namen von Benutzern handeln) nur dann den Zugriff, wenn dies für die Ausführun g zugewiesener Aufgaben gemäß den Unternehmenszielen und Geschäfts funktionen notwendig ist.	account-level-publ ic-accesss3-Blöcke-periodisch	Verwalten Sie den Zugriff auf Ressource n in der AWS Cloud, indem Sie sicherste llen, dass Amazon Simple Storage Service (Amazon S3) -Buckets nicht öffentlich zugänglic h sind. Diese Regel trägt dazu bei, sensible Daten vor unbefugten Remote-Benutzern zu schützen, indem sie den öffentlichen Zugriff verhinder t. Mit dieser Regel können Sie optional die Parameter ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) und restrictPublicBuck ets Parameter (Config Default: True) festlegen. Die tatsächlichen Werte müssen den Richtlini

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			en Ihrer Organisation entsprechen.
AC-6	Die Organisation wendet das Prinzip der geringsten Berechtigung an und erlaubt Benutzern (oder Prozessen , die im Namen von Benutzern handeln) nur dann den Zugriff, wenn dies für die Ausführun g zugewiesener Aufgaben gemäß den Unternehmenszielen und Geschäfts funktionen notwendig ist.	subnet-auto-assign-public-ip-deaktiviert	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon Virtual Private Cloud (VPC) -Subnetzen nicht automatisch eine öffentliche IP-Adress e zugewiesen wird. Amazon Elastic Compute Cloud (EC2) -Instances, die in Subnetzen gestartet werden, in denen dieses Attribut aktiviert ist, haben ihrer primären Netzwerkschnittste lle eine öffentliche IP-Adresse zugewiesen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-6	Die Organisation wendet das Prinzip der geringsten Berechtigung an und erlaubt Benutzern (oder Prozessen , die im Namen von Benutzern handeln) nur dann den Zugriff, wenn dies für die Ausführun g zugewiesener Aufgaben gemäß den Unternehmenszielen und Geschäfts funktionen notwendig ist.	s3 bucket-level-public-access - verboten	Verwalten Sie den Zugriff auf Ressource n in der AWS Cloud, indem Sie sicherste llen, dass Amazon Simple Storage Service (Amazon S3) -Buckets nicht öffentlich zugänglic h sind. Diese Regel trägt dazu bei, sensible Daten vor unbefugten Remote-Benutzern zu schützen, indem sie den öffentlichen Zugriff auf Bucket-Eb ene verhindert.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-6(2)	Das Informati onssystem erfordert die Verwendung nicht privilegierter Konten für den Zugriff auf nicht sicherhei tsrelevante Funktione n. Dadurch wird das Risiko begrenzt, wenn von privilegierten Konten oder Rollen aus gearbeitet wird	iam-policy-no-stat ements-with-full-a ccess	Stellen Sie sicher, dass IAM-Aktionen nur auf die benötigte n Aktionen beschränkt sind. Wenn Benutzern mehr Rechte eingeräumt werden, als für die Ausführun g einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringste n Berechtigung und der Aufgabentrennung verstoßen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-6(2)	Das Informationssystem verlangt für den Zugriff auf nicht sicherheitsrelevante Funktionen die Verwendung von Benutzerkonten ohne Benutzerrechte, wodurch die Gefahr begrenzt wird, wenn von privilegierten Konten oder Rollen aus operiert wird	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) kann Ihnen dabei helfen, die Prinzipien der geringsten Rechte und der Aufgabentrennung in Zugriffsberechtigungen und Autorisierungen zu integrieren und so zu verhindern, dass Richtlinien „Effect“: „Allow“ mit „Action“: „*“ anstelle von „Resource“: „*“ enthalten. Wenn Benutzern mehr Rechte eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und der Aufgabentrennung verstoßen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-6(2)	Das Informati onssystem erfordert die Verwendung von Konten ohne Zugriffsr echte für den Zugriff auf nicht sicherhei tsrelevante Funktione n. Dadurch wird das Risiko begrenzt, wenn von privilegierten Konten oder Rollen aus gearbeitet wird	iam-root-access-key-überprüfen	Der Zugriff auf Systeme und Ressourcen kann gesteuert werden, indem überprüft wird, ob der Root-Benu tzer keine Zugriffss chlüssel mit seiner AWS Identity and Access Management (IAM) -Rolle verknüpft hat. Stellen Sie sicher, dass die Root-Zugr iffsschlüssel gelöscht werden. Erstellen und verwenden Sie stattdessen rollenbas ierte AWS Konten, um dem Prinzip der geringsten Funktiona lität Rechnung zu tragen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-6(9)	Das Informati onssystem protokoll iert die Ausführun g privilegierter Funktionen.	cloud-trail-cloud-watch-logs-aktiviert	Verwenden Sie Amazon CloudWatch , um Protokollereignisa ktivitäten zentral zu sammeln und zu verwalten. Durch die Aufnahme von AWS CloudTrail Daten erhalten Sie Einzelhei ten zu den API-Aufru faktivitäten innerhalb Ihres AWS Kontos.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-6(9)	Das Informati onssystem protokoll iert die Ausführun g privilegierter Funktionen.	cloudtrail-enabled	AWS CloudTrail kann durch die Aufzeichn ung von Aktionen und API-Aufrufen der AWS Managemen t Console bei der Nichtabstreitbarkeit helfen. Sie können die Benutzer und AWS Konten, die einen AWS Dienst aufgerufen haben, die Quell-IP-Adresse, über die die Anrufe generiert wurden, und die Zeitpunkte der Anrufe identifiz ieren. Einzelheiten zu den erfassten Daten finden Sie in den AWS CloudTrail Datensatzinhalten.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-6(9)	Das Informati onssystem protokoll iert die Ausführun g privilegierter Funktionen.	multi-region-cloudtrail-enabled	AWS CloudTrail zeichnet Aktionen und API-Aufrufe der AWS Management Console auf. Sie können feststellen, welche Benutzer und Konten angerufen wurden AWS, von welcher Quell-IP-Adresse aus die Anrufe getätigt wurden und wann die Anrufe erfolgten. CloudTrail übermittelt Protokolldateien aus allen AWS Regionen an Ihren S3-Bucket , wenn MULTI_REG ION_CLOUD _TRAIL_ENABLED aktiviert ist. Außerdem wird beim AWS Start einer neuen Region derselbe Trail in der neuen Region erstellt. CloudTrail Dadurch erhalten Sie automatis ch Protokolldateien mit API-Aktivitäten für die neue Region.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-6(9)	Das Informati onssystem protokoll iert die Ausführun g privilegierter Funktionen.	elasticsearch-logs-to-cloudwatch	Stellen Sie sicher, dass für Amazon OpenSearch Service-Domains Fehlerpro tokolle aktiviert und zur Aufbewahrung und Beantwortung an Amazon CloudWatc h Logs gestreamt werden. Domain-Fehlerprotokolle sind bei Sicherhei ts- und Zugriffsp rüfungen sowie bei der Diagnose von Verfügbarkeitsprob lemen nützlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-6(9)	Das Informati onssystem protokoll iert die Ausführun g privilegierter Funktionen.	cloudtrail-s3-data events-enabled	Die Erfassung von Simple Storage Service (Amazon S3)-Datenereigniss en unterstützt die Erkennung von ungewöhnlichen Aktivitäten. Zu den Details gehören AWS Kontoinformationen , über die auf einen Amazon S3 S3-Bucket zugegriffen wurde, die IP-Adress e und die Uhrzeit des Ereignisses.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-6(9)	Das Informati onssystem protokoll iert die Ausführun g privilegierter Funktionen.	rds-logging-enabled	Um die Protokoll ierung und Überwachung in Ihrer Umgebung zu erleichtern, stellen Sie sicher, dass die Amazon Relationa l Database Service (Amazon RDS)-Prot okollierung aktiviert ist. Mit der Amazon-RDS-Protokollierung können Sie Ereigniss e wie Verbindungen, Verbindungsabbrüch e, Abfragen oder abgefragte Tabellen erfassen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-6(9)	Das Informationssystem protokolliert die Ausführung privilegierter Funktionen.	redshift-cluster-configuration-check	Um Daten im Ruhezustand zu schützen, muss die Verschlüsselung für Ihre Amazon-Redshift-Cluster aktiviert sein. Sie müssen auch sicherstellen, dass die erforderlichen Konfigurationen auf Amazon-Redshift-Clustern bereitgestellt werden. Die Prüfungsprotokollierung muss aktiviert sein, um Informationen zu Verbindungen und Benutzeraktivitäten in der Datenbank bereitzustellen. Diese Regel erfordert, dass ein Wert für clusterDbEncrypted (Config Default: TRUE) und LoggingEnabled (Config Default: TRUE) gesetzt ist. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-6(9)	Das Informati onssystem protokoll iert die Ausführun g privilegierter Funktionen.	s-3 bucket-logging-enabled	Die Amazon Simple Storage Service (Amazon S3)-Serverzugriffs protokollierung bietet eine Methode zur Überwachu ng des Netzwerks im Hinblick auf potenzielle Cybersich erheitsereignisse. Die Ereignisse werden überwacht, indem detaillierte Aufzeichn ungen über die Anfragen erfasst werden, die an einen Amazon-S3-Bucket gestellt wurden. Jeder Zugriffsprotokolle intrag enthält Details zu einer einzelnen Zugriffsanfrage. Zu den Details gehören Anforderer, Bucket-Name, Anforderu ngszeit, Anforderu ngsaktion, Antwortst atus und Fehlercode, falls relevant.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-6(10)	Das Informati onssystem verhinder t, dass nicht privilegi erte Benutzer privilegi erte Funktionen ausführen, einschlie ßlich der Deaktivie rung, Umgehung oder Änderung implement ierter Sicherhei tsvorkehrungen/Geg enmaßnahmen.	iam-root-access-key-überprüfen	Der Zugriff auf Systeme und Ressourcen kann gesteuert werden, indem überprüft wird, ob der Root-Benu tzer keine Zugriffss chlüssel mit seiner AWS Identity and Access Management (IAM) -Rolle verknüpft hat. Stellen Sie sicher, dass die Root-Zugr iffsschlüssel gelöscht werden. Erstellen und verwenden Sie stattdessen rollenbas ierte AWS Konten, um dem Prinzip der geringsten Funktiona lität Rechnung zu tragen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-6(10)	Das Informationssystem verhindert, dass nicht privilegierte Benutzer privilegierte Funktionen ausführen, einschließlich der Deaktivierung, Umgehung oder Änderung implementierter Sicherheitsvorkehrungen/Gegenmaßnahmen.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) kann Ihnen dabei helfen, die Prinzipien der geringsten Rechte und der Aufgabentrennung in Zugriffsberechtigungen und Autorisierungen zu integrieren und so zu verhindern, dass Richtlinien „Effect“: „Allow“ mit „Action“: „*“ anstelle von „Resource“: „*“ enthalten. Wenn Benutzern mehr Rechte eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und der Aufgabentrennung verstoßen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-6(10)	Das Informationssystem verhindert, dass nicht privilegierte Benutzer privilegierte Funktionen ausführen, einschließlich der Deaktivierung, Umgehung oder Änderung implementierter Sicherheitsvorkehrungen/Gegenmaßnahmen.	iam-policy-no-statements-with-full-access	Stellen Sie sicher, dass IAM-Aktionen nur auf die benötigten Aktionen beschränkt sind. Wenn Benutzern mehr Rechte eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und der Aufgabentrennung verstoßen.
AU-11	Das Unternehmen bewahrt die Auditaufzeichnungen mindestens 90 Tage lang auf, um die after-the-fact Untersuchung von Sicherheitsvorfällen zu unterstützen und die gesetzlichen und organisatorischen Anforderungen zur Aufbewahrung von Informationen zu erfüllen.	cw-loggroup-retention-period-überprüfen	Stellen Sie sicher, dass die Ereignisprotokolldaten für Ihre Protokollgruppen über eine Mindestdauer aufbewahrt werden, um die Fehlerbehebung und forensische Untersuchungen zu unterstützen. Fehlende frühere Ereignisprotokolldaten erschweren die Rekonstruierung und Identifizierung potenziell schädlicher Ereignisse.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AU-12(a)(c)	Das Informati onssystem: a. Ermöglicht die Generierung von Prüfungsunterlagen für die in AU-2 a. definierten prüffähig en Ereignisse für alle Informationssystem - und Netzwerkk omponenten, bei denen Prüfungsf unktionen bereitges tellt/verfügbar sind c. Generiert Prüfungsu nterlagen für die in AU-2 d. definierten Ereignisse mit dem in AU-3 definierten Inhalt.	api-gw-execution-l ogging-aktiviert	Die API-Gateway-Protokollierung zeigt detaillierte Ansichten der Benutzer, die auf die API zugegriff en haben, und wie diese Benutzer auf die API zugegriff en haben. Diese Einblicke ermöglichen die Transparenz von Benutzeraktivitäten.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AU-12(a)(c)	Das Informati onssystem: a. Ermöglicht die Generierung von Prüfungsunterlagen für die in AU-2 a. definierten prüffähig en Ereignisse für alle Informationssystem - und Netzwerkk omponenten, bei denen Prüfungsf unktionen bereitges tellt/verfügbar sind c. Generiert Prüfungsu nterlagen für die in AU-2 d. definierten Ereignisse mit dem in AU-3 definierten Inhalt.	cloud-trail-cloud-watch-logs-aktiviert	Verwenden Sie Amazon CloudWatch , um Protokollereignisa ktivitäten zentral zu sammeln und zu verwalten. Durch die Aufnahme von AWS CloudTrail Daten erhalten Sie Einzelhei ten zu den API-Aufru faktivitäten innerhalb Ihres AWS Kontos.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AU-12(a)(c)	Das Informati onssystem: a. Ermöglicht die Generierung von Prüfungsunterlagen für die in AU-2 a. definierten prüffähig en Ereignisse für alle Informationssystem - und Netzwerkk omponenten, bei denen Prüfungsf unktionen bereitges tellt/verfügbar sind c. Generiert Prüfungsu nterlagen für die in AU-2 d. definierten Ereignisse mit dem in AU-3 definierten Inhalt.	cloudtrail-s3-data events-enabled	Die Erfassung von Simple Storage Service (Amazon S3)-Datenereigniss en unterstützt die Erkennung von ungewöhnlichen Aktivitäten. Zu den Details gehören AWS Kontoinformationen , über die auf einen Amazon S3 S3-Bucket zugegriffen wurde, die IP-Adress e und die Uhrzeit des Ereignisses.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AU-12(a)(c)	Das Informationssystem: a. Ermöglicht die Generierung von Prüfungsunterlagen für die in AU-2 a. definierten prüffähigen Ereignisse für alle Informationssystem- und Netzwerkkomponenten, bei denen Prüfungsfunktionen bereitgestellt/verfügbar sind c. Generiert Prüfungsunterlagen für die in AU-2 d. definierten Ereignisse mit dem in AU-3 definierten Inhalt.	rds-logging-enabled	Um die Protokollierung und Überwachung in Ihrer Umgebung zu erleichtern, stellen Sie sicher, dass die Amazon Relational Database Service (Amazon RDS)-Protokollierung aktiviert ist. Mit der Amazon-RDS-Protokollierung können Sie Ereignisse wie Verbindungen, Verbindungsabbrüche, Abfragen oder abgefragte Tabellen erfassen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AU-12(a)(c)	Das Informati onssystem: a. Ermöglicht die Generierung von Prüfungsunterlagen für die in AU-2 a. definierten prüffähig en Ereignisse für alle Informationssystem - und Netzwerkk omponenten, bei denen Prüfungsf unktionen bereitges tellt/verfügbar sind c. Generiert Prüfungsu nterlagen für die in AU-2 d. definierten Ereignisse mit dem in AU-3 definierten Inhalt.	cloudtrail-enabled	AWS CloudTrail kann durch die Aufzeichn ung von Aktionen und API-Aufrufen in der AWS Managemen t Console bei der Nichtabstreitbarkeit helfen. Sie können die Benutzer und AWS Konten, die einen AWS Dienst aufgerufen haben, die Quell-IP-Adresse, über die die Anrufe generiert wurden, und die Zeitpunkte der Anrufe identifiz ieren. Einzelheiten zu den erfassten Daten finden Sie in den AWS CloudTrail Datensatzinhalten.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AU-12(a)(c)	Das Informati onssystem: a. Ermöglicht die Generierung von Prüfungsunterlagen für die in AU-2 a. definierten prüffähig en Ereignisse für alle Informationssystem - und Netzwerkk omponenten, bei denen Prüfungsf unktionen bereitges tellt/verfügbar sind c. Generiert Prüfungsu nterlagen für die in AU-2 d. definierten Ereignisse mit dem in AU-3 definierten Inhalt.	elb-logging-enabled	Die Elastic-Load-Balancing-Aktivität ist ein zentraler Kommunikationspunk t innerhalb einer Umgebung. Stellen Sie sicher, dass die ELB-Protokollierun g aktiviert ist. Die gesammelten Daten enthalten detaillie rte Informationen zu Anfragen, die an den ELB gesendet wurden. Jedes Protokoll enthält Informationen wie die Zeit, zu der die Anforderung einging, die Client-IP -Adresse, Latenzen, Anforderungspfade und Serverantworten.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AU-12(a)(c)	Das Informati onssystem: a. Ermöglicht die Generierung von Prüfungsunterlagen für die in AU-2 a. definierten prüffähig en Ereignisse für alle Informationssystem - und Netzwerkk omponenten, bei denen Prüfungsf unktionen bereitges tellt/verfügbar sind c. Generiert Prüfungsu nterlagen für die in AU-2 d. definierten Ereignisse mit dem in AU-3 definierten Inhalt.	multi-region-cloudtrail-enabled	AWS CloudTrail zeichnet Aktionen und API-Aufrufe der AWS Management Console auf. Sie können feststellen, welche Benutzer und Konten angerufen wurden AWS, von welcher Quell-IP-Adresse aus die Anrufe getätigt wurden und wann die Anrufe erfolgten. CloudTrail übermittelt Protokolldateien aus allen AWS Regionen an Ihren S3-Bucket , wenn MULTI_REG ION_CLOUD _TRAIL_ENABLED aktiviert ist. Außerdem wird beim AWS Start einer neuen Region derselbe Trail in der neuen Region erstellt. CloudTrail Dadurch erhalten Sie automatis ch Protokolldateien mit API-Aktivitäten für die neue Region.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AU-12(a)(c)	Das Informati onssystem: a. Ermöglicht die Generierung von Prüfungsunterlagen für die in AU-2 a. definierten prüffähig en Ereignisse für alle Informationssystem - und Netzwerkk omponenten, bei denen Prüfungsf unktionen bereitges tellt/verfügbar sind c. Generiert Prüfungsu nterlagen für die in AU-2 d. definierten Ereignisse mit dem in AU-3 definierten Inhalt.	s-3 bucket-logging-enabled	Die Amazon Simple Storage Service (Amazon S3)-Serverzugriffs protokollierung bietet eine Methode zur Überwachu ng des Netzwerks im Hinblick auf potenzielle Cybersich erheitsereignisse. Die Ereignisse werden überwacht, indem detaillierte Aufzeichn ungen über die Anfragen erfasst werden, die an einen Amazon-S3-Bucket gestellt wurden. Jeder Zugriffsprotokolle intrag enthält Details zu einer einzelnen Zugriffsanfrage. Zu den Details gehören Anforderer, Bucket-Name, Anforderu ngszeit, Anforderu ngsaktion, Antwortst atus und Fehlercode, falls relevant.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AU-12(a)(c)	Das Informationssystem: a. Ermöglicht die Generierung von Prüfungsunterlagen für die in AU-2 a. definierten prüffähigen Ereignisse für alle Informationssystem- und Netzwerkkomponenten, bei denen Prüfungsfunktionen bereitgestellt/verfügbar sind c. Generiert Prüfungsunterlagen für die in AU-2 d. definierten Ereignisse mit dem in AU-3 definierten Inhalt.	vpc-flow-logs-enabled	VPC-Flow-Protokolle erfassen detaillierte Informationsdatensätze über den IP-Datenverkehr, der zu und von Netzwerkschnittstellen in Ihrer Amazon Virtual Private Cloud (Amazon VPC) fließt. Standardmäßig enthalten Flow-Protokolldatensätze Werte für die verschiedenen Komponenten des IP-Flows, einschließlich Quelle, Ziel und Protokoll.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AU-12(a)(c)	Das Informationssystem: a. Ermöglicht die Generierung von Prüfungsunterlagen für die in AU-2 a. definierten prüffähigen Ereignisse für alle Informationssystem- und Netzwerkkomponenten, bei denen Prüfungsfunktionen bereitgestellt/verfügbar sind c. Generiert Prüfungsunterlagen für die in AU-2 d. definierten Ereignisse mit dem in AU-3 definierten Inhalt.	wafv2-logging-enabled	Um die Protokollierung und Überwachung in Ihrer Umgebung zu erleichtern, aktivieren Sie die AWS WAF (V2) -Protokollierung im regionalen und globalen Web ACLs. AWS Die WAF-Protokollierung bietet detaillierte Informationen über den Datenverkehr, der von Ihrer Web-ACL analysiert wird. In den Protokollen werden die Uhrzeit aufgezeichnet, zu der die AWS WAF die Anfrage von Ihrer AWS Ressource erhalten hat, Informationen über die Anfrage und eine Aktion für die Regel, der jede Anfrage entsprach.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AU-12(a)(c)	Das Informationssystem: a. Ermöglicht die Generierung von Prüfungsunterlagen für die in AU-2 a. definierten prüffähigen Ereignisse für alle Informationssystem- und Netzwerkkomponenten, bei denen Prüfungsfunktionen bereitgestellt/verfügbar sind c. Generiert Prüfungsunterlagen für die in AU-2 d. definierten Ereignisse mit dem in AU-3 definierten Inhalt.	redshift-cluster-configuration-check	Um Daten im Ruhezustand zu schützen, muss die Verschlüsselung für Ihre Amazon-Redshift-Cluster aktiviert sein. Sie müssen auch sicherstellen, dass die erforderlichen Konfigurationen auf Amazon-Redshift-Clustern bereitgestellt werden. Die Prüfungsprotokollierung muss aktiviert sein, um Informationen zu Verbindungen und Benutzeraktivitäten in der Datenbank bereitzustellen. Diese Regel erfordert, dass ein Wert für clusterDbEncrypted (Config Default: TRUE) und LoggingEnabled (Config Default: TRUE) gesetzt ist. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AU-2(a)(d)	Die Organisation: a. Legt fest, dass das Informationssystem folgenden Ereignisse überprüfen kann: Erfolgreiche und erfolglose Kontoanmeldungen, Kontoverwaltungsereignisse, Objektzugriffe, Richtlinienänderungen, Berechtigungsfunktionen, Prozessnachverfolgung und Systemereignisse. Für Webanwendungen: sämtliche Administratoraktivitäten, Authentifizierungsprüfungen, Autorisierungsprüfungen, Datenlöschungen, Datenzugriffe, Datenänderungen und Berechtigungsänderungen. d. Legt fest, dass die folgenden Ereignisse innerhalb des Informationssystems geprüft werden müssen: [von der	api-gw-execution-logging-aktiviert	Die API-Gateway-Protokollierung zeigt detaillierte Ansichten der Benutzer, die auf die API zugegriffen haben, und wie diese Benutzer auf die API zugegriffen haben. Diese Einblicke ermöglichen die Transparenz von Benutzeraktivitäten.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	Organisation definiert e Teilmenge der in AU-2(a) definierten prüffähigen Ereigniss e wird kontinuierlich für jedes identifizierte Ereignis geprüft].		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AU-2(a)(d)	Die Organisation: a. Legt fest, dass das Informationssystem folgenden Ereignisse überprüfen kann: Erfolgreiche und erfolglose Kontoanmeldungen, Kontoverwaltungsereignisse, Objektzugriffe, Richtlinienänderungen, Berechtigungsfunktionen, Prozessnachverfolgung und Systemereignisse. Für Webanwendungen: sämtliche Administratoraktivitäten, Authentifizierungsprüfungen, Autorisierungsprüfungen, Datenlöschungen, Datenzugriffe, Datenänderungen und Berechtigungsänderungen. d. Legt fest, dass die folgenden Ereignisse innerhalb des Informationssystems geprüft werden müssen: [von der	cloud-trail-cloud-watch-logs-aktiviert	Verwenden Sie Amazon CloudWatch , um Protokollereignisaktivitäten zentral zu sammeln und zu verwalten. Durch die Aufnahme von AWS CloudTrail Daten erhalten Sie Einzelheiten zu den API-Aufrufaktivitäten innerhalb Ihres AWS Kontos.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	Organisation definiert e Teilmenge der in AU-2(a) definierten prüffähigen Ereigniss e wird kontinuierlich für jedes identifizierte Ereignis geprüft].		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AU-2(a)(d)	Die Organisation: a. Legt fest, dass das Informationssystem folgenden Ereignisse überprüfen kann: Erfolgreiche und erfolglose Kontoanmeldungen, Kontoverwaltungsereignisse, Objektzugriffe, Richtlinienänderungen, Berechtigungsfunktionen, Prozessnachverfolgung und Systemereignisse. Für Webanwendungen: sämtliche Administratoraktivitäten, Authentifizierungsprüfungen, Autorisierungsprüfungen, Datenlöschungen, Datenzugriffe, Datenänderungen und Berechtigungsänderungen. d. Legt fest, dass die folgenden Ereignisse innerhalb des Informationssystems geprüft werden müssen: [von der	cloudtrail-s3-dataevents-enabled	Die Erfassung von Simple Storage Service (Amazon S3)-Datenereignissen unterstützt die Erkennung von ungewöhnlichen Aktivitäten. Zu den Details gehören AWS Kontoinformationen, über die auf einen Amazon S3 S3-Bucket zugegriffen wurde, die IP-Adresse und die Uhrzeit des Ereignisses.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	Organisation definiert e Teilmenge der in AU-2(a) definierten prüffähigen Ereigniss e wird kontinuierlich für jedes identifizierte Ereignis geprüft].		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AU-2(a)(d)	Die Organisation: a. Legt fest, dass das Informationssystem folgenden Ereignisse überprüfen kann: Erfolgreiche und erfolglose Kontoanmeldungen, Kontoverwaltungsereignisse, Objektzugriffe, Richtlinienänderungen, Berechtigungsfunktionen, Prozessnachverfolgung und Systemereignisse. Für Webanwendungen: sämtliche Administratoraktivitäten, Authentifizierungsprüfungen, Autorisierungsprüfungen, Datenlöschungen, Datenzugriffe, Datenänderungen und Berechtigungsänderungen. d. Legt fest, dass die folgenden Ereignisse innerhalb des Informationssystems geprüft werden müssen: [von der	cloudtrail-enabled	AWS CloudTrail kann durch die Aufzeichnung von Aktionen und API-Aufrufen in der AWS Management Console bei der Nichtabstreitbarkeit helfen. Sie können die Benutzer und AWS Konten, die einen AWS Dienst aufgerufen haben, die Quell-IP-Adresse, über die die Anrufe generiert wurden, und die Zeitpunkte der Anrufe identifizieren. Einzelheiten zu den erfassten Daten finden Sie in den AWS CloudTrail Datensatzinhalten.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	Organisation definiert e Teilmenge der in AU-2(a) definierten prüffähigen Ereigniss e wird kontinuierlich für jedes identifizierte Ereignis geprüft].		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AU-2(a)(d)	Die Organisation: a. Legt fest, dass das Informationssystem folgenden Ereignisse überprüfen kann: Erfolgreiche und erfolglose Kontoanmeldungen, Kontoverwaltungsereignisse, Objektzugriffe, Richtlinienänderungen, Berechtigungsfunktionen, Prozessnachverfolgung und Systemereignisse. Für Webanwendungen: sämtliche Administratoraktivitäten, Authentifizierungsprüfungen, Autorisierungsprüfungen, Datenlöschungen, Datenzugriffe, Datenänderungen und Berechtigungsänderungen. d. Legt fest, dass die folgenden Ereignisse innerhalb des Informationssystems geprüft werden müssen: [von der	elb-logging-enabled	Die Elastic-Load-Balancing-Aktivität ist ein zentraler Kommunikationspunkt innerhalb einer Umgebung. Stellen Sie sicher, dass die ELB-Protokollierung aktiviert ist. Die gesammelten Daten enthalten detaillierte Informationen zu Anfragen, die an den ELB gesendet wurden. Jedes Protokoll enthält Informationen wie die Zeit, zu der die Anforderung einging, die Client-IP-Adresse, Latenzen, Anforderungspfade und Serverantworten.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	Organisation definiert e Teilmenge der in AU-2(a) definierten prüffähigen Ereigniss e wird kontinuierlich für jedes identifizierte Ereignis geprüft].		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AU-2(a)(d)	Die Organisation: a. Legt fest, dass das Informationssystem folgenden Ereignisse überprüfen kann: Erfolgreiche und erfolglose Kontoanmeldungen, Kontoverwaltungsereignisse, Objektzugriffe, Richtlinienänderungen, Berechtigungsfunktionen, Prozessnachverfolgung und Systemereignisse. Für Webanwendungen: sämtliche Administratoraktivitäten, Authentifizierungsprüfungen, Autorisierungsprüfungen, Datenlöschungen, Datenzugriffe, Datenänderungen und Berechtigungsänderungen. d. Legt fest, dass die folgenden Ereignisse innerhalb des Informationssystems geprüft werden müssen: [von der	multi-region-cloudtrail-enabled	AWS CloudTrail zeichnet Aktionen und API-Aufrufe der AWS Management Console auf. Sie können feststellen, welche Benutzer und Konten angerufen wurden AWS, von welcher Quell-IP-Adresse aus die Anrufe getätigt wurden und wann die Anrufe erfolgten. CloudTrail übermittelt Protokolldateien aus allen AWS Regionen an Ihren S3-Bucket, wenn MULTI_REGION_CLOUD_TRAIL_ENABLED aktiviert ist. Außerdem wird beim AWS Start einer neuen Region derselbe Trail in der neuen Region erstellt. CloudTrail Dadurch erhalten Sie automatisch Protokolldateien mit API-Aktivitäten für die neue Region.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	Organisation definiert e Teilmenge der in AU-2(a) definierten prüffähigen Ereigniss e wird kontinuierlich für jedes identifizierte Ereignis geprüft].		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AU-2(a)(d)	Die Organisation: a. Legt fest, dass das Informationssystem folgenden Ereignisse überprüfen kann: Erfolgreiche und erfolglose Kontoanmeldungen, Kontoverwaltungsereignisse, Objektzugriffe, Richtlinienänderungen, Berechtigungsfunktionen, Prozessnachverfolgung und Systemereignisse. Für Webanwendungen: sämtliche Administratoraktivitäten, Authentifizierungsprüfungen, Autorisierungsprüfungen, Datenlöschungen, Datenzugriffe, Datenänderungen und Berechtigungsänderungen. d. Legt fest, dass die folgenden Ereignisse innerhalb des Informationssystems geprüft werden müssen: [von der	s-3 bucket-logging-enabled	Die Amazon Simple Storage Service (Amazon S3)-Serverzugriffsprotokollierung bietet eine Methode zur Überwachung des Netzwerks im Hinblick auf potenzielle Cybersicherheitsereignisse. Die Ereignisse werden überwacht, indem detaillierte Aufzeichnungen über die Anfragen erfasst werden, die an einen Amazon-S3-Bucket gestellt wurden. Jeder Zugriffsprotokolleintrag enthält Details zu einer einzelnen Zugriffsanfrage. Zu den Details gehören Anforderer, Bucket-Name, Anforderungszeit, Anforderungsaktion, Antwortstatus und Fehlercode, falls relevant.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	Organisation definiert e Teilmenge der in AU-2(a) definierten prüffähigen Ereigniss e wird kontinuierlich für jedes identifizierte Ereignis geprüft].		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AU-2(a)(d)	Die Organisation: a. Legt fest, dass das Informationssystem folgenden Ereignisse überprüfen kann: Erfolgreiche und erfolglose Kontoanmeldungen, Kontoverwaltungsereignisse, Objektzugriffe, Richtlinienänderungen, Berechtigungsfunktionen, Prozessnachverfolgung und Systemereignisse. Für Webanwendungen: sämtliche Administratoraktivitäten, Authentifizierungsprüfungen, Autorisierungsprüfungen, Datenlöschungen, Datenzugriffe, Datenänderungen und Berechtigungsänderungen. d. Legt fest, dass die folgenden Ereignisse innerhalb des Informationssystems geprüft werden müssen: [von der	vpc-flow-logs-enabled	VPC-Flow-Protokolle erfassen detaillierte Informationsdatensätze über den IP-Datenverkehr, der zu und von Netzwerkschnittstellen in Ihrer Amazon Virtual Private Cloud (Amazon VPC) fließt. Standardmäßig enthalten Flow-Protokolldatensätze Werte für die verschiedenen Komponenten des IP-Flows, einschließlich Quelle, Ziel und Protokoll.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	Organisation definiert e Teilmenge der in AU-2(a) definierten prüffähigen Ereigniss e wird kontinuierlich für jedes identifizierte Ereignis geprüft].		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AU-2(a)(d)	Die Organisation: a. Legt fest, dass das Informationssystem folgenden Ereignisse überprüfen kann: Erfolgreiche und erfolglose Kontoanmeldungen, Kontoverwaltungsereignisse, Objektzugriffe, Richtlinienänderungen, Berechtigungsfunktionen, Prozessnachverfolgung und Systemereignisse. Für Webanwendungen: sämtliche Administratoraktivitäten, Authentifizierungsprüfungen, Autorisierungsprüfungen, Datenlöschungen, Datenzugriffe, Datenänderungen und Berechtigungsänderungen. d. Legt fest, dass die folgenden Ereignisse innerhalb des Informationssystems geprüft werden müssen: [von der	rds-logging-enabled	Um die Protokollierung und Überwachung in Ihrer Umgebung zu erleichtern, stellen Sie sicher, dass die Amazon Relational Database Service (Amazon RDS)-Protokollierung aktiviert ist. Mit der Amazon-RDS-Protokollierung können Sie Ereignisse wie Verbindungen, Verbindungsabbrüche, Abfragen oder abgefragte Tabellen erfassen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	Organisation definiert e Teilmenge der in AU-2(a) definierten prüffähigen Ereigniss e wird kontinuierlich für jedes identifizierte Ereignis geprüft].		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AU-2(a)(d)	Die Organisation: a. Legt fest, dass das Informationssystem folgenden Ereignisse überprüfen kann: Erfolgreiche und erfolglose Kontoanmeldungen, Kontoverwaltungsereignisse, Objektzugriffe, Richtlinienänderungen, Berechtigungsfunktionen, Prozessnachverfolgung und Systemereignisse. Für Webanwendungen: sämtliche Administratoraktivitäten, Authentifizierungsprüfungen, Autorisierungsprüfungen, Datenlöschungen, Datenzugriffe, Datenänderungen und Berechtigungsänderungen. d. Legt fest, dass die folgenden Ereignisse innerhalb des Informationssystems geprüft werden müssen: [von der	wafv2-logging-enabled	Um die Protokollierung und Überwachung in Ihrer Umgebung zu erleichtern, aktivieren Sie die AWS WAF (V2) -Protokollierung im regionalen und globalen Web ACLs. AWS Die WAF-Protokollierung bietet detaillierte Informationen über den Datenverkehr, der von Ihrer Web-ACL analysiert wird. In den Protokollen werden die Uhrzeit aufgezeichnet, zu der die AWS WAF die Anfrage von Ihrer AWS Ressource erhalten hat, Informationen über die Anfrage und eine Aktion für die Regel, der jede Anfrage entsprach.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	Organisation definiert e Teilmenge der in AU-2(a) definierten prüffähigen Ereigniss e wird kontinuierlich für jedes identifizierte Ereignis geprüft].		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AU-2(a)(d)	Die Organisation: a. Legt fest, dass das Informationssystem folgenden Ereignisse überprüfen kann: Erfolgreiche und erfolglose Kontoanmeldungen, Kontoverwaltungsereignisse, Objektzugriffe, Richtlinienänderungen, Berechtigungsfunktionen, Prozessnachverfolgung und Systemereignisse. Für Webanwendungen: sämtliche Administratoraktivitäten, Authentifizierungsprüfungen, Autorisierungsprüfungen, Datenlöschungen, Datenzugriffe, Datenänderungen und Berechtigungsänderungen. d. Legt fest, dass die folgenden Ereignisse innerhalb des Informationssystems geprüft werden müssen: [von der	redshift-cluster-configuration-check	Um Daten im Ruhezustand zu schützen, muss die Verschlüsselung für Ihre Amazon-Redshift-Cluster aktiviert sein. Sie müssen auch sicherstellen, dass die erforderlichen Konfigurationen auf Amazon-Redshift-Clustern bereitgestellt werden. Die Prüfungsprotokollierung muss aktiviert sein, um Informationen zu Verbindungen und Benutzeraktivitäten in der Datenbank bereitzustellen. Diese Regel erfordert, dass ein Wert für clusterDbEncrypted (Config Default: TRUE) und LoggingEnabled (Config Default: TRUE) gesetzt ist. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	Organisation definiert e Teilmenge der in AU-2(a) definierten prüffähigen Ereigniss e wird kontinuierlich für jedes identifizierte Ereignis geprüft].		
AU-3	Das Informati onssystem generiert Prüfprotokolle mit Informationen, aus denen hervorgeh t, welche Art von Ereignis eingetret en ist, wann und wo das Ereignis stattgefunden hat, welchen Ursprung das Ereignis hat, wie es ausging und mit welchen Personen oder Subjekten das Ereignis in Verbindun g steht.	api-gw-execution-l ogging-aktiviert	Die API-Gateway-Protokollierung zeigt detaillierte Ansichten der Benutzer, die auf die API zugegriff en haben, und wie diese Benutzer auf die API zugegriff en haben. Diese Einblicke ermöglichen die Transparenz von Benutzeraktivitäten.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AU-3	Das Informati onssystem generiert Prüfprotokolle mit Informationen, aus denen hervorgeh t, welche Art von Ereignis eingetret en ist, wann und wo das Ereignis stattgefunden hat, welchen Ursprung das Ereignis hat, wie es ausging und mit welchen Personen oder Subjekten das Ereignis in Verbindun g steht.	cloud-trail-cloud-watch-logs-aktiviert	Verwenden Sie Amazon CloudWatch , um Protokollereignisa ktivitäten zentral zu sammeln und zu verwalten. Durch die Aufnahme von AWS CloudTrail Daten erhalten Sie Einzelhei ten zu den API-Aufru faktivitäten innerhalb Ihres AWS Kontos.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AU-3	Das Informati onssystem generiert Prüfprotokolle mit Informationen, aus denen hervorgeh t, welche Art von Ereignis eingetret en ist, wann und wo das Ereignis stattgefunden hat, welchen Ursprung das Ereignis hat, wie es ausging und mit welchen Personen oder Subjekten das Ereignis in Verbindun g steht.	cloudtrail-s3-data events-enabled	Die Erfassung von Simple Storage Service (Amazon S3)-Datenereigniss en unterstützt die Erkennung von ungewöhnlichen Aktivitäten. Zu den Details gehören AWS Kontoinformationen , über die auf einen Amazon S3 S3-Bucket zugegriffen wurde, die IP-Adress e und die Uhrzeit des Ereignisses.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AU-3	Das Informati onssystem generiert Prüfprotokolle mit Informationen, aus denen hervorgeh t, welche Art von Ereignis eingetret en ist, wann und wo das Ereignis stattgefunden hat, welchen Ursprung das Ereignis hat, wie es ausging und mit welchen Personen oder Subjekten das Ereignis in Verbindun g steht.	rds-logging-enabled	Um die Protokoll ierung und Überwachung in Ihrer Umgebung zu erleichtern, stellen Sie sicher, dass die Amazon Relationa l Database Service (Amazon RDS)-Prot okollierung aktiviert ist. Mit der Amazon-RDS-Protokollierung können Sie Ereigniss e wie Verbindungen, Verbindungsabbrüch e, Abfragen oder abgefragte Tabellen erfassen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AU-3	Das Informati onssystem generiert Prüfprotokolle mit Informationen, aus denen hervorgeh t, welche Art von Ereignis eingetret en ist, wann und wo das Ereignis stattgefunden hat, welchen Ursprung das Ereignis hat, wie es ausging und mit welchen Personen oder Subjekten das Ereignis in Verbindun g steht.	cloudtrail-enabled	AWS CloudTrail kann durch die Aufzeichn ung von Aktionen und API-Aufrufen in der AWS Managemen t Console bei der Nichtabstreitbarkeit helfen. Sie können die Benutzer und AWS Konten, die einen AWS Dienst aufgerufen haben, die Quell-IP-Adresse, über die die Anrufe generiert wurden, und die Zeitpunkte der Anrufe identifiz ieren. Einzelheiten zu den erfassten Daten finden Sie in den AWS CloudTrail Datensatzinhalten.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AU-3	Das Informati onssystem generiert Prüfprotokolle mit Informationen, aus denen hervorgeh t, welche Art von Ereignis eingetret en ist, wann und wo das Ereignis stattgefunden hat, welchen Ursprung das Ereignis hat, wie es ausging und mit welchen Personen oder Subjekten das Ereignis in Verbindun g steht.	elb-logging-enabled	Die Elastic-Load-Balancing-Aktivität ist ein zentraler Kommunikationspunk t innerhalb einer Umgebung. Stellen Sie sicher, dass die ELB-Protokollierun g aktiviert ist. Die gesammelten Daten enthalten detaillie rte Informationen zu Anfragen, die an den ELB gesendet wurden. Jedes Protokoll enthält Informationen wie die Zeit, zu der die Anforderung einging, die Client-IP -Adresse, Latenzen, Anforderungspfade und Serverantworten.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AU-3	Das Informati onssystem generiert Prüfprotokolle mit Informationen, aus denen hervorgeh t, welche Art von Ereignis eingetret en ist, wann und wo das Ereignis stattgefunden hat, welchen Ursprung das Ereignis hat, wie es ausging und mit welchen Personen oder Subjekten das Ereignis in Verbindun g steht.	multi-region-cloudtrail-enabled	AWS CloudTrail zeichnet Aktionen und API-Aufrufe der AWS Management Console auf. Sie können feststellen, welche Benutzer und Konten angerufen wurden AWS, von welcher Quell-IP-Adresse aus die Anrufe getätigt wurden und wann die Anrufe erfolgten. CloudTrail übermittelt Protokolldateien aus allen AWS Regionen an Ihren S3-Bucket , wenn MULTI_REG ION_CLOUD _TRAIL_ENABLED aktiviert ist. Außerdem wird beim AWS Start einer neuen Region derselbe Trail in der neuen Region erstellt. CloudTrail Dadurch erhalten Sie automatis ch Protokolldateien mit API-Aktivitäten für die neue Region.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AU-3	Das Informati onssystem generiert Prüfprotokolle mit Informationen, aus denen hervorgeh t, welche Art von Ereignis eingetret en ist, wann und wo das Ereignis stattgefunden hat, welchen Ursprung das Ereignis hat, wie es ausging und mit welchen Personen oder Subjekten das Ereignis in Verbindun g steht.	s-3 bucket-logging-enabled	Die Amazon Simple Storage Service (Amazon S3)-Serverzugriffs protokollierung bietet eine Methode zur Überwachu ng des Netzwerks im Hinblick auf potenzielle Cybersich erheitsereignisse. Die Ereignisse werden überwacht, indem detaillierte Aufzeichn ungen über die Anfragen erfasst werden, die an einen Amazon-S3-Bucket gestellt wurden. Jeder Zugriffsprotokolle intrag enthält Details zu einer einzelnen Zugriffsanfrage. Zu den Details gehören Anforderer, Bucket-Name, Anforderu ngszeit, Anforderu ngsaktion, Antwortst atus und Fehlercode, falls relevant.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AU-3	Das Informati onssystem generiert Prüfprotokolle mit Informationen, aus denen hervorgeh t, welche Art von Ereignis eingetret en ist, wann und wo das Ereignis stattgefunden hat, welchen Ursprung das Ereignis hat, wie es ausging und mit welchen Personen oder Subjekten das Ereignis in Verbindun g steht.	vpc-flow-logs-enabled	VPC-Flow-Protokoll e erfassen detaillierte Informationsdatens ätze über den IP-Datenverkehr, der zu und von Netzwerkschnittste llen in Ihrer Amazon Virtual Private Cloud (Amazon VPC) fließt. Standardmäßig enthalten Flow-Prot okolldatensätze Werte für die verschiedenen Komponenten des IP-Flows, einschlie ßlich Quelle, Ziel und Protokoll.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AU-3	Das Informationssystem generiert Prüfprotokolle mit Informationen, aus denen hervorgeht, welche Art von Ereignis eingetreten ist, wann und wo das Ereignis stattgefunden hat, welchen Ursprung das Ereignis hat, wie es ausging und mit welchen Personen oder Subjekten das Ereignis in Verbindung steht.	redshift-cluster-configuration-check	Um Daten im Ruhezustand zu schützen, muss die Verschlüsselung für Ihre Amazon-Redshift-Cluster aktiviert sein. Sie müssen auch sicherstellen, dass die erforderlichen Konfigurationen auf Amazon-Redshift-Clustern bereitgestellt werden. Die Prüfungsprotokollierung muss aktiviert sein, um Informationen zu Verbindungen und Benutzeraktivitäten in der Datenbank bereitzustellen. Diese Regel erfordert, dass ein Wert für clusterDbEncrypted (Config Default: TRUE) und LoggingEnabled (Config Default: TRUE) gesetzt ist. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AU-3	Das Informationssystem generiert Prüfprotokolle mit Informationen, aus denen hervorgeht, welche Art von Ereignis eingetreten ist, wann und wo das Ereignis stattgefunden hat, welchen Ursprung das Ereignis hat, wie es ausging und mit welchen Personen oder Subjekten das Ereignis in Verbindung steht.	wafv2-logging-enabled	Um die Protokollierung und Überwachung in Ihrer Umgebung zu erleichtern, aktivieren Sie die AWS WAF (V2) -Protokollierung im regionalen und globalen Web. ACLs AWS Die WAF-Protokollierung bietet detaillierte Informationen über den Datenverkehr, der von Ihrer Web-ACL analysiert wird. In den Protokollen werden die Uhrzeit aufgezeichnet, zu der die AWS WAF die Anfrage von Ihrer AWS Ressource erhalten hat, Informationen über die Anfrage und eine Aktion für die Regel, der jede Anfrage entsprach.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AU-6(1)(3)	(1) Die Organisation setzt automatisierte Mechanismen zur Integration von Prüfungs-, Analyse- und Berichtsprozessen ein, um die Prozesse der Organisation zur Untersuchung und Reaktion auf verdächtige Aktivitäten zu unterstützen. (3) Die Organisation analysiert und korreliert Prüfungsunterlagen aus verschiedenen Repositorys, um sich ein Bild über die Situation in der gesamten Organisation zu verschaffen.	cloudwatch-alarm-action-check	Amazon CloudWatch alarmiert, wenn eine Metrik den Schwellenwert für eine bestimmte Anzahl von Bewertungszeiträumen überschreitet. Der Alarm führt eine oder mehrere Aktionen durch, die vom Wert der Metrik oder des Ausdrucks im Vergleich zu einem Schwellenwert in einer Reihe von Zeiträumen abhängt. Diese Regel erfordert einen Wert für alarmActionRequired (Config Default: True), insufficientDataAction Required (Config Default: True), okActionRequired (Config Default: False). Der tatsächliche Wert muss die Alarmaktionen für Ihre Umgebung widerspiegeln.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AU-6(1)(3)	(1) Die Organisation setzt automatisierte Mechanismen zur Integration von Prüfungs-, Analyse- und Berichtsprozessen ein, um die Prozesse der Organisation zur Untersuchung und Reaktion auf verdächtige Aktivitäten zu unterstützen. (3) Die Organisation analysiert und korreliert Prüfungsunterlagen aus verschiedenen Repositorys, um sich ein Bild über die Situation in der gesamten Organisation zu verschaffen.	guardduty-enabled-centralized	Amazon GuardDuty kann mithilfe von Threat Intelligence Feeds helfen, potenzielle Cybersicherheitsereignisse zu überwachen und zu erkennen. Dazu gehören Listen mit bösartigen IPs und maschinellen Lernmethoden zur Identifizierung unerwarteter, nicht autorisierter und bösartiger Aktivitäten in Ihrer AWS Cloud-Umgebung.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AU-6(1)(3)	(1) Die Organisation setzt automatisierte Mechanismen zur Integration von Prüfungs-, Analyse- und Berichtsprozessen ein, um die Prozesse der Organisation zur Untersuchung und Reaktion auf verdächtige Aktivitäten zu unterstützen. (3) Die Organisation analysiert und korreliert Prüfungsunterlagen aus verschiedenen Repositorys, um sich ein Bild über die Situation in der gesamten Organisation zu verschaffen.	cloud-trail-cloud-watch-logs-aktiviert	Verwenden Sie Amazon CloudWatch , um Protokollereignisaktivitäten zentral zu sammeln und zu verwalten. Durch die Aufnahme von AWS CloudTrail Daten erhalten Sie Einzelheiten zu den API-Aufrufaktivitäten innerhalb Ihres AWS Kontos.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AU-6(1)(3)	(1) Die Organisation setzt automatisierte Mechanismen zur Integration von Prüfungs-, Analyse- und Berichtsprozessen ein, um die Prozesse der Organisation zur Untersuchung und Reaktion auf verdächtige Aktivitäten zu unterstützen. (3) Die Organisation analysiert und korreliert Prüfungsunterlagen aus verschiedenen Repositorys, um sich ein Bild über die Situation in der gesamten Organisation zu verschaffen.	securityhub-enabled	AWS Security Hub hilft bei der Überwachung von unbefugtem Personal, Verbindungen, Geräten und Software. AWS Security Hub aggregiert, organisiert und priorisiert die Sicherheitswarnungen oder Ergebnisse mehrerer Dienste. AWS Einige dieser Dienste sind Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer und AWS Firewall Manager sowie AWS Partnerlösungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AU-6(1)(3)	(1) Die Organisation setzt automatisierte Mechanismen zur Integration von Prüfungs-, Analyse- und Berichtsprozessen ein, um die Prozesse der Organisation zur Untersuchung und Reaktion auf verdächtige Aktivitäten zu unterstützen. (3) Die Organisation analysiert und korreliert Prüfungsunterlagen aus verschiedenen Repositorys, um sich ein Bild über die Situation in der gesamten Organisation zu verschaffen.	cloudtrail-s3-dataevents-enabled	Die Erfassung von Simple Storage Service (Amazon S3)-Datenereignissen unterstützt die Erkennung von ungewöhnlichen Aktivitäten. Zu den Details gehören AWS Kontoinformationen, über die auf einen Amazon S3 S3-Bucket zugegriffen wurde, die IP-Adresse und die Uhrzeit des Ereignisses.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AU-6(1)(3)	(1) Die Organisation setzt automatisierte Mechanismen zur Integration von Prüfungs-, Analyse- und Berichtsprozessen ein, um die Prozesse der Organisation zur Untersuchung und Reaktion auf verdächtige Aktivitäten zu unterstützen. (3) Die Organisation analysiert und korreliert Prüfungsunterlagen aus verschiedenen Repositorys, um sich ein Bild über die Situation in der gesamten Organisation zu verschaffen.	api-gw-execution-logging-aktiviert	Die API-Gateway-Protokollierung zeigt detaillierte Ansichten der Benutzer, die auf die API zugegriffen haben, und wie diese Benutzer auf die API zugegriffen haben. Diese Einblicke ermöglichen die Transparenz von Benutzeraktivitäten.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AU-6(1)(3)	(1) Die Organisation setzt automatisierte Mechanismen zur Integration von Prüfungs-, Analyse- und Berichtsprozessen ein, um die Prozesse der Organisation zur Untersuchung und Reaktion auf verdächtige Aktivitäten zu unterstützen. (3) Die Organisation analysiert und korreliert Prüfungsunterlagen aus verschiedenen Repositorys, um sich ein Bild über die Situation in der gesamten Organisation zu verschaffen.	multi-region-cloudtrail-enabled	AWS CloudTrail zeichnet Aktionen und API-Aufrufe der AWS Management Console auf. Sie können feststellen, welche Benutzer und Konten angerufen wurden AWS, von welcher Quell-IP-Adresse aus die Anrufe getätigt wurden und wann die Anrufe erfolgten. CloudTrail übermittelt Protokolldateien aus allen AWS Regionen an Ihren S3-Bucket, wenn MULTI_REGION_CLOUD_TRAIL_ENABLED aktiviert ist. Außerdem wird beim AWS Start einer neuen Region derselbe Trail in der neuen Region erstellt. CloudTrail Dadurch erhalten Sie automatisch Protokolldateien mit API-Aktivitäten für die neue Region.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AU-6(1)(3)	(1) Die Organisation setzt automatisierte Mechanismen zur Integration von Prüfungs-, Analyse- und Berichtsprozessen ein, um die Prozesse der Organisation zur Untersuchung und Reaktion auf verdächtige Aktivitäten zu unterstützen. (3) Die Organisation analysiert und korreliert Prüfungsunterlagen aus verschiedenen Repositorys, um sich ein Bild über die Situation in der gesamten Organisation zu verschaffen.	rds-logging-enabled	Um die Protokollierung und Überwachung in Ihrer Umgebung zu erleichtern, stellen Sie sicher, dass die Amazon Relational Database Service (Amazon RDS)-Protokollierung aktiviert ist. Mit der Amazon-RDS-Protokollierung können Sie Ereignisse wie Verbindungen, Verbindungsabbrüche, Abfragen oder abgefragte Tabellen erfassen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AU-6(1)(3)	(1) Die Organisation setzt automatisierte Mechanismen zur Integration von Prüfungs-, Analyse- und Berichtsprozessen ein, um die Prozesse der Organisation zur Untersuchung und Reaktion auf verdächtige Aktivitäten zu unterstützen. (3) Die Organisation analysiert und korreliert Prüfungsunterlagen aus verschiedenen Repositorys, um sich ein Bild über die Situation in der gesamten Organisation zu verschaffen.	cloudtrail-enabled	AWS CloudTrail kann durch die Aufzeichnung von Aktionen und API-Aufrufen in der AWS Management Console bei der Nichtabstreitbarkeit helfen. Sie können die Benutzer und AWS Konten, die einen AWS Dienst aufgerufen haben, die Quell-IP-Adresse, über die die Anrufe generiert wurden, und die Zeitpunkte der Anrufe identifizieren. Einzelheiten zu den erfassten Daten finden Sie in den AWS CloudTrail Datensatzinhalten.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AU-6(1)(3)	(1) Die Organisation setzt automatisierte Mechanismen zur Integration von Prüfungs-, Analyse- und Berichtsprozessen ein, um die Prozesse der Organisation zur Untersuchung und Reaktion auf verdächtige Aktivitäten zu unterstützen. (3) Die Organisation analysiert und korreliert Prüfungsunterlagen aus verschiedenen Repositorys, um sich ein Bild über die Situation in der gesamten Organisation zu verschaffen.	vpc-flow-logs-enabled	VPC-Flow-Protokolle erfassen detaillierte Informationsdatensätze über den IP-Datenverkehr, der zu und von Netzwerkschnittstellen in Ihrer Amazon Virtual Private Cloud (Amazon VPC) fließt. Standardmäßig enthalten Flow-Protokolldatensätze Werte für die verschiedenen Komponenten des IP-Flows, einschließlich Quelle, Ziel und Protokoll.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AU-6(1)(3)	(1) Die Organisation setzt automatisierte Mechanismen zur Integration von Prüfungs-, Analyse- und Berichtsprozessen ein, um die Prozesse der Organisation zur Untersuchung und Reaktion auf verdächtige Aktivitäten zu unterstützen. (3) Die Organisation analysiert und korreliert Prüfungsunterlagen aus verschiedenen Repositorys, um sich ein Bild über die Situation in der gesamten Organisation zu verschaffen.	elb-logging-enabled	Die Elastic-Load-Balancing-Aktivität ist ein zentraler Kommunikationspunkt innerhalb einer Umgebung. Stellen Sie sicher, dass die ELB-Protokollierung aktiviert ist. Die gesammelten Daten enthalten detaillierte Informationen zu Anfragen, die an den ELB gesendet wurden. Jedes Protokoll enthält Informationen wie die Zeit, zu der die Anforderung einging, die Client-IP-Adresse, Latenzen, Anforderungspfade und Serverantworten.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AU-6(1)(3)	(1) Die Organisation setzt automatisierte Mechanismen zur Integration von Prüfungs-, Analyse- und Berichtsprozessen ein, um die Prozesse der Organisation zur Untersuchung und Reaktion auf verdächtige Aktivitäten zu unterstützen. (3) Die Organisation analysiert und korreliert Prüfungsunterlagen aus verschiedenen Repositorys, um sich ein Bild über die Situation in der gesamten Organisation zu verschaffen.	redshift-cluster-configuration-check	Um Daten im Ruhezustand zu schützen, muss die Verschlüsselung für Ihre Amazon-Redshift-Cluster aktiviert sein. Sie müssen auch sicherstellen, dass die erforderlichen Konfigurationen auf Amazon-Redshift-Clustern bereitgestellt werden. Die Prüfungsprotokollierung muss aktiviert sein, um Informationen zu Verbindungen und Benutzeraktivitäten in der Datenbank bereitzustellen. Diese Regel erfordert, dass ein Wert für clusterDbEncrypted (Config Default: TRUE) und LoggingEnabled (Config Default: TRUE) gesetzt ist. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AU-6(1)(3)	(1) Die Organisation setzt automatisierte Mechanismen zur Integration von Prüfungs-, Analyse- und Berichtsprozessen ein, um die Prozesse der Organisation zur Untersuchung und Reaktion auf verdächtige Aktivitäten zu unterstützen. (3) Die Organisation analysiert und korreliert Prüfungsunterlagen aus verschiedenen Repositorys, um sich ein Bild über die Situation in der gesamten Organisation zu verschaffen.	s-3 bucket-logging-enabled	Die Amazon Simple Storage Service (Amazon S3)-Serverzugriffsprotokollierung bietet eine Methode zur Überwachung des Netzwerks im Hinblick auf potenzielle Cybersicherheitsereignisse. Die Ereignisse werden überwacht, indem detaillierte Aufzeichnungen über die Anfragen erfasst werden, die an einen Amazon-S3-Bucket gestellt wurden. Jeder Zugriffsprotokolleintrag enthält Details zu einer einzelnen Zugriffsanfrage. Zu den Details gehören Anforderer, Bucket-Name, Anforderungszeit, Anforderungsaktion, Antwortstatus und Fehlercode, falls relevant.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AU-6(1)(3)	(1) Die Organisation setzt automatisierte Mechanismen zur Integration von Prüfungs-, Analyse- und Berichtsprozessen ein, um die Prozesse der Organisation zur Untersuchung und Reaktion auf verdächtige Aktivitäten zu unterstützen. (3) Die Organisation analysiert und korreliert Prüfungsunterlagen aus verschiedenen Repositorys, um sich ein Bild über die Situation in der gesamten Organisation zu verschaffen.	wafv2-logging-enabled	Um die Protokollierung und Überwachung in Ihrer Umgebung zu erleichtern, aktivieren Sie die AWS WAF (V2) -Protokollierung im regionalen und globalen Web. ACLs AWS Die WAF-Protokollierung bietet detaillierte Informationen über den Datenverkehr, der von Ihrer Web-ACL analysiert wird. In den Protokollen werden die Uhrzeit aufgezeichnet, zu der die AWS WAF die Anfrage von Ihrer AWS Ressource erhalten hat, Informationen über die Anfrage und eine Aktion für die Regel, der jede Anfrage entsprach.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AU-6(1)(3)	(1) Die Organisation setzt automatisierte Mechanismen zur Integration von Prüfungs-, Analyse- und Berichtsprozessen ein, um die Prozesse der Organisation zur Untersuchung und Reaktion auf verdächtige Aktivitäten zu unterstützen. (3) Die Organisation analysiert und korreliert Prüfungsunterlagen aus verschiedenen Repositorys, um sich ein Bild über die Situation in der gesamten Organisation zu verschaffen.	cw-loggroup-retention-period-überprüfen	Stellen Sie sicher, dass die Ereignisprotokolldaten für Ihre Protokollgruppen über eine Mindestdauer aufbewahrt werden, um die Fehlerbehebung und forensische Untersuchungen zu unterstützen. Fehlende frühere Ereignisprotokolldaten erschweren die Rekonstruierung und Identifizierung potenziell schädlicher Ereignisse.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AU-6(3)	Die Organisation analysiert und korreliert Auditaufz eichnungen aus verschiedenen Repositorien, um ein unternehmensweites Situationsbewusstsein zu erlangen.	elasticsearch-logs-to-cloudwatch	Stellen Sie sicher, dass für Amazon OpenSearch Service-Domains Fehlerpro tokolle aktiviert und zur Aufbewahrung und Beantwortung an Amazon CloudWatc h Logs gestreamt werden. Domain-Fehlerprotokolle sind bei Sicherhei ts- und Zugriffsp rüfungen sowie bei der Diagnose von Verfügbarkeitsprob lemen nützlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AU-6(3)	Die Organisation analysiert und korreliert Auditaufz eichnungen aus verschiedenen Archiven, um ein unternehmensweites Situationsbewusstsein zu erlangen.	multi-region-cloudtrail-enabled	AWS CloudTrail zeichnet Aktionen und API-Aufrufe der AWS Management Console auf. Sie können feststellen, welche Benutzer und Konten angerufen wurden AWS, von welcher Quell-IP-Adresse aus die Anrufe getätigt wurden und wann die Anrufe erfolgten. CloudTrail übermittelt Protokolldateien aus allen AWS Regionen an Ihren S3-Bucket , wenn MULTI_REG ION_CLOUD _TRAIL_ENABLED aktiviert ist. Außerdem wird beim AWS Start einer neuen Region derselbe Trail in der neuen Region erstellt. CloudTrail Dadurch erhalten Sie automatis ch Protokolldateien mit API-Aktivitäten für die neue Region.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AU-6(3)	Die Organisation analysiert und korreliert die Auditdaten verschiedener Datenspeicher, um ein unternehmensweites Situationsbewusstsein zu erlangen.	wafv2-logging-enabled	Um die Protokollierung und Überwachung in Ihrer Umgebung zu erleichtern, aktivieren Sie die AWS WAF (V2) -Protokollierung im regionalen und globalen Internet. ACLs AWS Die WAF-Protokollierung bietet detaillierte Informationen über den Datenverkehr, der von Ihrer Web-ACL analysiert wird. In den Protokollen werden die Uhrzeit aufgezeichnet, zu der die AWS WAF die Anfrage von Ihrer AWS Ressource erhalten hat, Informationen über die Anfrage und eine Aktion für die Regel, der jede Anfrage entsprach.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AU-6(3)	Die Organisation analysiert und korreliert Auditaufzeichnungen aus verschiedenen Repositorien, um ein unternehmensweites Situationsbewusstsein zu erlangen.	api-gw-execution-logging-aktiviert	Die API-Gateway-Protokollierung zeigt detaillierte Ansichten der Benutzer, die auf die API zugegriffen haben, und wie diese Benutzer auf die API zugegriffen haben. Diese Einblicke ermöglichen die Transparenz von Benutzeraktivitäten.
AU-6(3)	Die Organisation analysiert und korreliert Auditaufzeichnungen aus verschiedenen Archiven, um ein unternehmensweites Situationsbewusstsein zu erlangen.	cloud-trail-cloud-watch-logs-aktiviert	Verwenden Sie Amazon CloudWatch , um Protokollereignisaktivitäten zentral zu sammeln und zu verwalten. Durch die Aufnahme von AWS CloudTrail Daten erhalten Sie Einzelheiten zu den API-Aufrufaktivitäten innerhalb Ihres AWS Kontos.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AU-6(3)	Die Organisation analysiert und korreliert die Auditaufzeichnungen verschiedener Datenspeicher, um ein unternehmensweites Situationsbewusstsein zu erlangen.	cloudtrail-enabled	AWS CloudTrail kann durch die Aufzeichnung von Aktionen und API-Aufrufen in der Management Console helfen, die Ablehnung zu verhindern. AWS Sie können die Benutzer und AWS Konten, die einen AWS Dienst aufgerufen haben, die Quell-IP-Adresse, über die die Anrufe generiert wurden, und die Zeitpunkte der Anrufe identifizieren. Einzelheiten zu den erfassten Daten finden Sie in den AWS CloudTrail Datensatzinhalten.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AU-6(3)	Die Organisation analysiert und korreliert Auditaufzeichnungen aus verschiedenen Archiven, um ein unternehmensweites Situationsbewusstsein zu erlangen.	cloudtrail-s3-dataevents-enabled	Die Erfassung von Simple Storage Service (Amazon S3)-Datenereignissen unterstützt die Erkennung von ungewöhnlichen Aktivitäten. Zu den Details gehören AWS Kontoinformationen, über die auf einen Amazon S3 S3-Bucket zugegriffen wurde, die IP-Adresse und die Uhrzeit des Ereignisses.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AU-6(3)	Die Organisation analysiert und korreliert Auditaufzeichnungen aus verschiedenen Repositorien, um ein unternehmensweites Situationsbewusstsein zu erlangen.	elb-logging-enabled	Die Elastic-Load-Balancing-Aktivität ist ein zentraler Kommunikationspunkt innerhalb einer Umgebung. Stellen Sie sicher, dass die ELB-Protokollierung aktiviert ist. Die gesammelten Daten enthalten detaillierte Informationen zu Anfragen, die an den ELB gesendet wurden. Jedes Protokoll enthält Informationen wie die Zeit, zu der die Anforderung einging, die Client-IP-Adresse, Latenzen, Anforderungspfade und Serverantworten.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AU-6(3)	Die Organisation analysiert und korreliert Auditaufzeichnungen aus verschiedenen Archiven, um ein unternehmensweites Situationsbewusstsein zu erlangen.	rds-logging-enabled	Um die Protokollierung und Überwachung in Ihrer Umgebung zu erleichtern, stellen Sie sicher, dass die Amazon Relational Database Service (Amazon RDS)-Protokollierung aktiviert ist. Mit der Amazon-RDS-Protokollierung können Sie Ereignisse wie Verbindungen, Verbindungsabbrüche, Abfragen oder abgefragte Tabellen erfassen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AU-6(3)	Die Organisation analysiert und korreliert Auditaufzeichnungen aus verschiedenen Archiven, um ein unternehmensweites Situationsbewusstsein zu erlangen.	redshift-cluster-configuration-check	Um Daten im Ruhezustand zu schützen, muss die Verschlüsselung für Ihre Amazon-Redshift-Cluster aktiviert sein. Sie müssen auch sicherstellen, dass die erforderlichen Konfigurationen auf Amazon-Redshift-Clustern bereitgestellt werden. Die Prüfungsprotokollierung muss aktiviert sein, um Informationen zu Verbindungen und Benutzeraktivitäten in der Datenbank bereitzustellen. Diese Regel erfordert, dass ein Wert für clusterDbEncrypted (Config Default: TRUE) und LoggingEnabled (Config Default: TRUE) gesetzt ist. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AU-6(3)	Die Organisation analysiert und korreliert Auditaufz eichnungen aus verschiedenen Repositorien, um ein unternehmensweites Situationsbewusstsein zu erlangen.	s-3 bucket-logging-enabled	Die Amazon Simple Storage Service (Amazon S3)-Serverzugriffs protokollierung bietet eine Methode zur Überwachu ng des Netzwerks im Hinblick auf potenzielle Cybersich erheitsereignisse. Die Ereignisse werden überwacht, indem detaillierte Aufzeichn ungen über die Anfragen erfasst werden, die an einen Amazon-S3-Bucket gestellt wurden. Jeder Zugriffsprotokolle intrag enthält Details zu einer einzelnen Zugriffsanfrage. Zu den Details gehören Anforderer, Bucket-Name, Anforderu ngszeit, Anforderu ngsaktion, Antwortst atus und Fehlercode, falls relevant.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AU-6(3)	Die Organisation analysiert und korreliert Auditaufzeichnungen aus verschiedenen Archiven, um ein unternehmensweites Situationsbewusstsein zu erlangen.	vpc-flow-logs-enabled	VPC-Flow-Protokolle erfassen detaillierte Informationsdatensätze über den IP-Datenverkehr, der zu und von Netzwerkschnittstellen in Ihrer Amazon Virtual Private Cloud (Amazon VPC) fließt. Standardmäßig enthalten Flow-Protokolldatensätze Werte für die verschiedenen Komponenten des IP-Flows, einschließlich Quelle, Ziel und Protokoll.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AU-7	Das Informati onssystem bietet und implement iert Funktionen zur Reduzierung von Prüfungsa ufzeichnungen und zur Erstellung von Berichten, die: a. Unterstützt die Prüfung, Analyse und Meldung von Prüfaufzeichnungen auf Abruf sowie die after-the-fact Untersuchung von Vorfällen; und b. Ändert weder den ursprünglichen Inhalt noch die zeitliche Reihenfolge der Prüfprotokolle.	cloud-trail-cloud-watch-logs-aktiviert	Verwenden Sie Amazon CloudWatch , um Protokollereignisa ktivitäten zentral zu sammeln und zu verwalten. Durch die Aufnahme von AWS CloudTrail Daten erhalten Sie Einzelhei ten zu den API-Aufru faktivitäten innerhalb Ihres AWS Kontos.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AU-7	Das Informati onssystem bietet und implement iert Funktionen zur Reduzierung von Prüfungsa ufzeichnungen und zur Erstellung von Berichten, die: a. Unterstützt die Prüfung, Analyse und Meldung von Prüfaufzeichnungen auf Abruf sowie die after-the-fact Untersuchung von Vorfällen; und b. Ändert weder den ursprünglichen Inhalt noch die zeitliche Reihenfolge der Prüfprotokolle.	cloud-trail-log-file-validierung aktiviert	Verwenden Sie die AWS CloudTrail Protokolldateivali dierung, um die Integrität von CloudTrail Protokoll en zu überprüfen. Mithilfe der Protokoll dateivalidierung kann festgestellt werden, ob eine Protokoll datei geändert oder gelöscht wurde oder ob sie nach der Übermittlung CloudTrail unverände rt geblieben ist. Dieses Feature wurde mit dem Branchens tandard entsprech enden Algorithmen entwickelt: SHA-256 für die Hashfunktion und SHA-256 mit RSA für digitale Signature n. Aus diesem Grund ist es rechnerisch unmöglich, CloudTrai l Protokolldateien unbemerkt zu ändern, zu löschen oder zu fälschen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AU-7(1)	Das Informationssystem bietet die Möglichkeit, Prüfungsunterlagen für Ereignisse von Interesse auf der Grundlage von [Zuweisung: von der Organisation definierte Prüfungsfelder in den Prüfungsunterlagen] zu verarbeiten.	cloudwatch-alarm-action-check	Amazon CloudWatch alarmiert, wenn eine Metrik den Schwellenwert für eine bestimmte Anzahl von Bewertungszeiträumen überschreitet. Der Alarm führt eine oder mehrere Aktionen durch, die vom Wert der Metrik oder des Ausdrucks im Vergleich zu einem Schwellenwert in einer Reihe von Zeiträumen abhängt. Diese Regel erfordert einen Wert für alarmActionRequired (Config Default: True), insufficientDataAction Required (Config Default: True), okActionRequired (Config Default: False). Der tatsächliche Wert muss die Alarmaktionen für Ihre Umgebung widerspiegeln.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AU-7(1)	Das Informati onssystem bietet die Möglichkeit, Prüfungsunterlagen für Ereignisse von Interesse auf der Grundlage von [Zuweisung: von der Organisation definiert e Prüfungsfelder in den Prüfungsu nterlagen] zu verarbeit en.	cloud-trail-cloud-watch-logs-aktiviert	Verwenden Sie Amazon CloudWatch , um Protokollereignisa ktivitäten zentral zu sammeln und zu verwalten. Durch die Aufnahme von AWS CloudTrail Daten erhalten Sie Einzelhei ten zu den API-Aufru faktivitäten innerhalb Ihres AWS Kontos.
AU-9	Das Informati onssystem schützt Prüfungsinformatio nen und -tools vor unbefugtem Zugriff, Änderung und Löschung.	cloud-trail-encryption-enabled	Da sensible Daten vorhanden sein können und um Daten im Speicher zu schützen, sollten Sie sicherstellen, dass die Verschlüsselung für Ihre AWS CloudTrail Trails aktiviert ist.
AU-9	Das Informati onssystem schützt Prüfungsinformatio nen und -tools vor unbefugtem Zugriff, Änderung und Löschung.	cloudwatch-log-group-encrypted	Um sensible Daten im Speicher zu schützen, stellen Sie sicher, dass die Verschlüs selung für Ihre Amazon CloudWatch Log Groups aktiviert ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AU-9	Das Informati onssystem schützt Prüfungsinformatio nen und -tools vor unbefugtem Zugriff, Änderung und Löschung.	cloud-trail-log-file-validierung aktiviert	Verwenden Sie die Validierung von AWS CloudTrail Protokolldateien, um die Integrität von CloudTrail Protokoll en zu überprüfen. Mithilfe der Protokoll dateivalidierung kann festgestellt werden, ob eine Protokoll datei geändert oder gelöscht wurde oder ob sie nach der Übermittlung CloudTrail unverände rt geblieben ist. Dieses Feature wurde mit dem Branchens tandard entsprech enden Algorithmen entwickelt: SHA-256 für die Hashfunktion und SHA-256 mit RSA für digitale Signature n. Aus diesem Grund ist es rechnerisch unmöglich, CloudTrai l Protokolldateien unbemerkt zu ändern, zu löschen oder zu fälschen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AU-9(2)	Das Informati onssystem sichert die Prüfungsu nterlagen mindestens wöchentlich auf einem anderen System bzw. einer anderen Systemkomponente als dem System/de r Komponente, das/ die Gegenstand der Prüfung ist.	s-3 bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) unterstützt die Aufrechterhaltung einer angemesse nen Kapazität und Verfügbarkeit. CRR ermöglicht das automatische, asynchrone Kopieren von Objekten in Amazon-S3-Buckets, um die Datenverf ügbarkeit sicherzus tellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AU-9(2)	Das Informationssystem sichert die Prüfungsunterlagen mindestens wöchentlich auf einem anderen System bzw. einer anderen Systemkomponente als dem System/der Komponente, das/die Gegenstand der Prüfung ist.	s-3 bucket-versioning-enabled	Die Versionsverwaltung von Amazon Simple Storage Service (Amazon S3)-Buckets hilft dabei, mehrere Varianten eines Objekts im selben Amazon-S3-Bucket zu speichern. Verwenden Sie die Versionsverwaltung, um sämtliche Versionen aller Objekte in Ihrem Amazon-S3-Bucket zu speichern, abzurufen oder wiederherzustellen. Mit der Versionsverwaltung können Sie Versionen sowohl nach unbeabsichtigten Benutzeraktionen als auch nach Anwendungsfehlern problemlos wiederherstellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AU-12	Das Informati onssystem bietet die Möglichkeit, Prüfproto kolle für die Ereignist ypen zu erstellen, die das System gemäß AU-2a unter [Aufgabe: organisationsdefin ierte Systemkom ponenten]; b) prüfen kann. [Zuordnung: organisationsdefin iertes Personal oder Rollen] die Auswahl der Ereignist ypen zulassen, die von bestimmte n Systemkom ponenten protokoll iert werden sollen; und c. Generieren Sie Prüfdatensätze für die in AU-2c definierten Ereignistypen, die den in AU-3 definierten Inhalt der Prüfdaten sätze enthalten.	elasticsearch-logs-to-cloudwatch	Stellen Sie sicher, dass für Amazon OpenSearch Service-Domains Fehlerpro tokolle aktiviert und zur Aufbewahrung und Beantwortung an Amazon CloudWatc h Logs gestreamt werden. Domain-Fehlerprotokolle sind bei Sicherhei ts- und Zugriffsp rüfungen sowie bei der Diagnose von Verfügbarkeitsprob lemen nützlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AU-12	Das Informati onssystem bietet die Möglichkeit, Prüfdaten sätze für die Ereignist ypen zu erstellen, die das System gemäß AU-2a unter [Aufgabe: organisationsdefin ierte Systemkom ponenten]; b) prüfen kann. [Zuordnung: organisationsdefin iertes Personal oder Rollen] die Auswahl der Ereignist ypen zulassen, die von bestimmte n Systemkom ponenten protokoll iert werden sollen; und c. Generieren Sie Prüfdatensätze für die in AU-2c definierten Ereignistypen, die den in AU-3 definierten Inhalt der Prüfdaten sätze enthalten.	multi-region-cloudtrail-enabled	AWS CloudTrail zeichnet Aktionen und API-Aufrufe der AWS Management Console auf. Sie können feststellen, welche Benutzer und Konten angerufen wurden AWS, von welcher Quell-IP-Adresse aus die Anrufe getätigt wurden und wann die Anrufe erfolgten. CloudTrail übermittelt Protokolldateien aus allen AWS Regionen an Ihren S3-Bucket , wenn MULTI_REG ION_CLOUD _TRAIL_ENABLED aktiviert ist. Außerdem wird beim AWS Start einer neuen Region derselbe Trail in der neuen Region erstellt. CloudTrail Dadurch erhalten Sie automatis ch Protokolldateien mit API-Aktivitäten für die neue Region.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AU-12	Das Informationssystem ermöglicht die Erstellung von Prüfprotokollen für die Ereignistypen, die das System gemäß AU-2a für [Aufgabe: organisationsdefinierte Systemkomponenten]; b) prüfen kann. [Zuordnung: organisationsdefiniertes Personal oder Rollen] die Auswahl der Ereignistypen zulassen, die von bestimmten Systemkomponenten protokolliert werden sollen; und c. Generieren Sie Prüfdatensätze für die in AU-2c definierten Ereignistypen, die den in AU-3 definierten Inhalt der Prüfdatensätze enthalten.	wafv2-logging-enabled	Um die Protokollierung und Überwachung in Ihrer Umgebung zu erleichtern, aktivieren Sie die AWS WAF (V2) -Protokollierung im regionalen und globalen Web. ACLs AWS Die WAF-Protokollierung bietet detaillierte Informationen über den Datenverkehr, der von Ihrer Web-ACL analysiert wird. In den Protokollen werden die Uhrzeit aufgezeichnet, zu der die AWS WAF die Anfrage von Ihrer AWS Ressource erhalten hat, Informationen über die Anfrage und eine Aktion für die Regel, der jede Anfrage entsprach.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AU-12	Das Informati onssystem bietet Funktionen zur Generierung von Prüfdatensätzen für die Ereignistypen, die das System gemäß AU-2a unter [Zuweisung: organisationsdefin ierte Systemkom ponenten]; b) prüfen kann. [Zuordnung: organisationsdefin iertes Personal oder Rollen] die Auswahl der Ereignist ypen zulassen, die von bestimmte n Systemkom ponenten protokoll iert werden sollen; und c. Generieren Sie Prüfdatensätze für die in AU-2c definierten Ereignistypen, die den in AU-3 definierten Inhalt der Prüfdaten sätze enthalten.	api-gw-execution-l ogging-aktiviert	Die API-Gateway-Protokollierung zeigt detaillierte Ansichten der Benutzer, die auf die API zugegriff en haben, und wie diese Benutzer auf die API zugegriff en haben. Diese Einblicke ermöglichen die Transparenz von Benutzeraktivitäten.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AU-12	Das Informati onssystem bietet die Möglichkeit, Prüfproto kolle für die Ereignist ypen zu erstellen, die das System gemäß AU-2a auf [Aufgabe: organisationsdefin ierte Systemkom ponenten] prüfen kann; b. [Zuordnun g: organisationsdefin iertes Personal oder Rollen] die Auswahl der Ereignist ypen zulassen, die von bestimmte n Systemkom ponenten protokoll iert werden sollen; und c. Generieren Sie Prüfdatensätze für die in AU-2c definierten Ereignistypen, die den in AU-3 definierten Inhalt der Prüfdaten sätze enthalten.	cloud-trail-cloud-watch-logs-aktiviert	Verwenden Sie Amazon CloudWatch , um Protokollereignisa ktivitäten zentral zu sammeln und zu verwalten. Durch die Aufnahme von AWS CloudTrail Daten erhalten Sie Einzelhei ten zu den API-Aufru faktivitäten innerhalb Ihres AWS Kontos.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AU-12	Das Informati onssystem ermöglich t die Erstellung von Prüfprotokollen für die Ereignistypen, die das System gemäß AU-2a unter [Aufgabe: organisationsdefin ierte Systemkom ponenten]; b) prüfen kann. [Zuordnung: organisationsdefin iertes Personal oder Rollen] die Auswahl der Ereignist ypen zulassen, die von bestimmte n Systemkom ponenten protokoll iert werden sollen; und c. Generieren Sie Prüfdatensätze für die in AU-2c definierten Ereignistypen, die den in AU-3 definierten Inhalt der Prüfdaten sätze enthalten.	cloudtrail-enabled	AWS CloudTrail kann durch die Aufzeichn ung von Aktionen und API-Aufrufen in der AWS Managemen t Console helfen, die Ablehnung zu verhindern. Sie können die Benutzer und AWS Konten, die einen AWS Dienst aufgerufen haben, die Quell-IP-Adresse, über die die Anrufe generiert wurden, und die Zeitpunkte der Anrufe identifiz ieren. Einzelheiten zu den erfassten Daten finden Sie in den AWS CloudTrail Datensatzinhalten.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AU-12	Das Informati onssystem bietet die Möglichkeit, Prüfproto kolle für die Ereignist ypen zu erstellen, die das System gemäß AU-2a für [Aufgabe: organisationsdefin ierte Systemkom ponenten] prüfen kann; b. [Zuordnun g: organisationsdefin iertes Personal oder Rollen] die Auswahl der Ereignist ypen zulassen, die von bestimmte n Systemkom ponenten protokoll iert werden sollen; und c. Generieren Sie Prüfdatensätze für die in AU-2c definierten Ereignistypen, die den in AU-3 definierten Inhalt der Prüfdaten sätze enthalten.	cloudtrail-s3-data events-enabled	Die Erfassung von Simple Storage Service (Amazon S3)-Datenereigniss en unterstützt die Erkennung von ungewöhnlichen Aktivitäten. Zu den Details gehören AWS Kontoinformationen , über die auf einen Amazon S3 S3-Bucket zugegriffen wurde, die IP-Adress e und die Uhrzeit des Ereignisses.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AU-12	Das Informati onssystem bietet Funktionen zur Generierung von Prüfdatensätzen für die Ereignistypen, die das System gemäß AU-2a unter [Zuweisung: organisationsdefin ierte Systemkom ponenten]; b) prüfen kann. [Zuordnung: organisationsdefin iertes Personal oder Rollen] die Auswahl der Ereignist ypen zulassen, die von bestimmte n Systemkom ponenten protokoll iert werden sollen; und c. Generieren Sie Prüfdatensätze für die in AU-2c definierten Ereignistypen, die den in AU-3 definierten Inhalt der Prüfdaten sätze enthalten.	elb-logging-enabled	Die Elastic-Load-Balancing-Aktivität ist ein zentraler Kommunikationspunk t innerhalb einer Umgebung. Stellen Sie sicher, dass die ELB-Protokollierun g aktiviert ist. Die gesammelten Daten enthalten detaillie rte Informationen zu Anfragen, die an den ELB gesendet wurden. Jedes Protokoll enthält Informationen wie die Zeit, zu der die Anforderung einging, die Client-IP -Adresse, Latenzen, Anforderungspfade und Serverantworten.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AU-12	Das Informationssystem bietet die Möglichkeit, Prüfprotokolle für die Ereignistypen zu erstellen, die das System gemäß AU-2a auf [Aufgabe: organisationsdefinierte Systemkomponenten] prüfen kann; b. [Zuordnung: organisationsdefiniertes Personal oder Rollen] die Auswahl der Ereignistypen zulassen, die von bestimmten Systemkomponenten protokolliert werden sollen; und c. Generieren Sie Prüfdatensätze für die in AU-2c definierten Ereignistypen, die den in AU-3 definierten Inhalt der Prüfdatensätze enthalten.	rds-logging-enabled	Um die Protokollierung und Überwachung in Ihrer Umgebung zu erleichtern, stellen Sie sicher, dass die Amazon Relational Database Service (Amazon RDS)-Protokollierung aktiviert ist. Mit der Amazon-RDS-Protokollierung können Sie Ereignisse wie Verbindungen, Verbindungsabbrüche, Abfragen oder abgefragte Tabellen erfassen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AU-12	Das Informationssystem bietet die Möglichkeit, Prüfprotokolle für die Ereignistypen zu erstellen, die das System gemäß AU-2a auf [Aufgabe: organisationsdefinierte Systemkomponenten] prüfen kann; b. [Zuordnung: organisationsdefiniertes Personal oder Rollen] die Auswahl der Ereignistypen zulassen, die von bestimmten Systemkomponenten protokolliert werden sollen; und c. Generieren Sie Prüfdatensätze für die in AU-2c definierten Ereignistypen, die den in AU-3 definierten Inhalt der Prüfdatensätze enthalten.	redshift-cluster-configuration-check	Um Daten im Ruhezustand zu schützen, muss die Verschlüsselung für Ihre Amazon-Redshift-Cluster aktiviert sein. Sie müssen auch sicherstellen, dass die erforderlichen Konfigurationen auf Amazon-Redshift-Clustern bereitgestellt werden. Die Prüfungsprotokollierung muss aktiviert sein, um Informationen zu Verbindungen und Benutzeraktivitäten in der Datenbank bereitzustellen. Diese Regel erfordert, dass ein Wert für clusterDbEncrypted (Config Default: TRUE) und LoggingEnabled (Config Default: TRUE) gesetzt ist. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AU-12	Das Informati onssystem bietet die Möglichkeit, Prüfdatensätze für die Ereignistypen zu erstellen, die das System gemäß AU-2a unter [Zuweisung: organisationsdefin ierte Systemkom ponenten]; b) prüfen kann. [Zuordnung: organisationsdefin iertes Personal oder Rollen] die Auswahl der Ereignist ypen zulassen, die von bestimmte n Systemkom ponenten protokoll iert werden sollen; und c. Generieren Sie Prüfdatensätze für die in AU-2c definierten Ereignistypen, die den in AU-3 definierten Inhalt der Prüfdaten sätze enthalten.	s-3 bucket-logging-enabled	Die Amazon Simple Storage Service (Amazon S3)-Serverzugriffs protokollierung bietet eine Methode zur Überwachu ng des Netzwerks im Hinblick auf potenzielle Cybersich erheitsereignisse. Die Ereignisse werden überwacht, indem detaillierte Aufzeichn ungen über die Anfragen erfasst werden, die an einen Amazon-S3-Bucket gestellt wurden. Jeder Zugriffsprotokolle intrag enthält Details zu einer einzelnen Zugriffsanfrage. Zu den Details gehören Anforderer, Bucket-Name, Anforderu ngszeit, Anforderu ngsaktion, Antwortst atus und Fehlercode, falls relevant.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AU-12	Das Informationssystem bietet die Möglichkeit, Prüfprotokolle für die Ereignistypen zu erstellen, die das System gemäß AU-2a auf [Aufgabe: organisationsdefinierte Systemkomponenten] prüfen kann; b. [Zuordnung: organisationsdefiniertes Personal oder Rollen] die Auswahl der Ereignistypen zulassen, die von bestimmten Systemkomponenten protokolliert werden sollen; und c. Generieren Sie Prüfdatensätze für die in AU-2c definierten Ereignistypen, die den in AU-3 definierten Inhalt der Prüfdatensätze enthalten.	vpc-flow-logs-enabled	VPC-Flow-Protokolle erfassen detaillierte Informationsdatensätze über den IP-Datenverkehr, der zu und von Netzwerkschnittstellen in Ihrer Amazon Virtual Private Cloud (Amazon VPC) fließt. Standardmäßig enthalten Flow-Protokolldatensätze Werte für die verschiedenen Komponenten des IP-Flows, einschließlich Quelle, Ziel und Protokoll.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CA-7(a)(b)	Die Organisation entwickelt eine Strategie zur kontinuierlichen Überwachung und implementiert ein kontinuierliches Überwachungsprogramm, das Folgendes umfasst: a. Festlegung von [Zuweisung: von der Organisation definierte Kennzahlen], die überwacht werden sollen; b. Festlegung von [Zuweisung: von der Organisation festgelegte Häufigkeiten] für die Überwachung und [Zuweisung: von der Organisation festgelegte Häufigkeiten] für Bewertungen, die diese Überwachung unterstützen.	cloudwatch-alarm-action-check	Amazon CloudWatch alarmiert, wenn eine Metrik den Schwellenwert für eine bestimmte Anzahl von Bewertungszeiträumen überschreitet. Der Alarm führt eine oder mehrere Aktionen durch, die vom Wert der Metrik oder des Ausdrucks im Vergleich zu einem Schwellenwert in einer Reihe von Zeiträumen abhängt. Diese Regel erfordert einen Wert für alarmActionRequired (Config Default: True), insufficientDataAction Required (Config Default: True), okActionRequired (Config Default: False). Der tatsächliche Wert muss die Alarmaktionen für Ihre Umgebung widerspiegeln.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CA-7(a)(b)	Die Organisation entwickelt eine Strategie zur kontinuierlichen Überwachung und implementiert ein kontinuierliches Überwachungsprogramm, das Folgendes umfasst: a. Festlegung von [Zuweisung: von der Organisation definierte Kennzahlen], die überwacht werden sollen; b. Festlegung von [Zuweisung: von der Organisation festgelegte Häufigkeiten] für die Überwachung und [Zuweisung: von der Organisation festgelegte Häufigkeiten] für Bewertungen, die diese Überwachung unterstützen.	ec2- instance-detailed-monitoring-enabled	Aktivieren Sie diese Regel, um die Amazon Elastic Compute Cloud (Amazon EC2) - Instance-Überwachung auf der EC2 Amazon-Konsole zu verbessern, in der Monitoring-Diagramme mit einem Zeitraum von 1 Minute für die Instance angezeigt werden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CA-7(a)(b)	Die Organisation entwickelt eine Strategie zur kontinuierlichen Überwachung und implementiert ein kontinuierliches Überwachungsprogramm, das Folgendes umfasst: a. Festlegung von [Zuweisung: von der Organisation definierte Kennzahlen], die überwacht werden sollen; b. Festlegung von [Zuweisung: von der Organisation festgelegte Häufigkeiten] für die Überwachung und [Zuweisung: von der Organisation festgelegte Häufigkeiten] für Bewertungen, die diese Überwachung unterstützen.	rds-enhanced-monitoring-enabled	Aktivieren Sie Amazon Relational Database Service (Amazon RDS), um die Verfügbarkeit von Amazon RDS zu überwachen. Dies bietet einen detaillierten Einblick in den Zustand Ihrer Amazon-RDS-Datenbank-Instances. Wenn der Amazon-RDS-Speicher mehr als ein zugrunde liegendes physisches Gerät verwendet, erfasst Enhanced Monitoring die Daten für jedes Gerät. Wenn die Amazon-RDS-Datenbank-Instance in einer Multi-AZ-Bereitstellung ausgeführt wird, werden außerdem die Daten für jedes Gerät auf dem sekundären Host sowie die Metriken des sekundären Hosts erfasst.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CA-7(a)(b)	Die Organisation entwickelt eine Strategie zur kontinuierlichen Überwachung und implementiert ein kontinuierliches Überwachungsprogramm, das Folgendes umfasst: a. Festlegung von [Zuweisung: von der Organisation definierte Kennzahlen], die überwacht werden sollen; b. Festlegung von [Zuweisung: von der Organisation festgelegte Häufigkeiten] für die Überwachung und [Zuweisung: von der Organisation festgelegte Häufigkeiten] für Bewertungen, die diese Überwachung unterstützen.	guardduty-enabled-centralized	Amazon GuardDuty kann mithilfe von Threat Intelligence Feeds helfen, potenzielle Cybersicherheitsereignisse zu überwachen und zu erkennen. Dazu gehören Listen mit bösartigen IPs und maschinellen Lernmethoden zur Identifizierung unerwarteter, nicht autorisierter und bösartiger Aktivitäten in Ihrer AWS Cloud-Umgebung.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CA-7(a)(b)	Die Organisation entwickelt eine Strategie zur kontinuierlichen Überwachung und implementiert ein kontinuierliches Überwachungsprogramm, das Folgendes umfasst: a. Festlegung von [Zuweisung: von der Organisation definierte Kennzahlen], die überwacht werden sollen; b. Festlegung von [Zuweisung: von der Organisation festgelegte Häufigkeiten] für die Überwachung und [Zuweisung: von der Organisation festgelegte Häufigkeiten] für Bewertungen, die diese Überwachung unterstützen.	securityhub-enabled	AWS Security Hub hilft bei der Überwachung von unbefugtem Personal, Verbindungen, Geräten und Software. AWS Security Hub aggregiert, organisiert und priorisiert die Sicherheitswarnungen oder Ergebnisse mehrerer Dienste. AWS Einige dieser Dienste sind Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer und AWS Firewall Manager sowie AWS Partnerlösungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CA-7(a)(b)	Die Organisation entwickelt eine Strategie zur kontinuierlichen Überwachung und implementiert ein kontinuierliches Überwachungsprogramm, das Folgendes umfasst: a. Festlegung von [Zuweisung: von der Organisation definierte Kennzahlen], die überwacht werden sollen; b. Festlegung von [Zuweisung: von der Organisation festgelegte Häufigkeiten] für die Überwachung und [Zuweisung: von der Organisation festgelegte Häufigkeiten] für Bewertungen, die diese Überwachung unterstützen.	autoscaling-group-elb-healthcheck-erforderlich	Die Elastic Load Balancer (ELB) - Zustandsprüfungen für Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling Scaling-Gruppen unterstützen die Aufrechterhaltung einer angemessenen Kapazität und Verfügbarkeit. Der Load Balancer sendet regelmäßig Pings, versucht Verbindungen herzustellen oder sendet Anfragen, um den Zustand der EC2 Amazon-Instances in einer Gruppe mit auto-scaling zu testen. Wenn eine Instance nicht zurückmeldet, wird der Traffic an eine neue EC2 Amazon-Instance gesendet.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CA-7(a)(b)	Die Organisation entwickelt eine Strategie zur kontinuierlichen Überwachung und implementiert ein kontinuierliches Überwachungsprogramm, das Folgendes umfasst: a. Festlegung von [Zuweisung: von der Organisation definierte Kennzahlen], die überwacht werden sollen; b. Festlegung von [Zuweisung: von der Organisation festgelegte Häufigkeiten] für die Überwachung und [Zuweisung: von der Organisation festgelegte Häufigkeiten] für Bewertungen, die diese Überwachung unterstützen.	beanstalk-enhanced-health-reporting-aktiviert	AWS Die verbesserte Zustandsberichterstattung von Elastic Beanstalk ermöglicht eine schnellere Reaktion auf Veränderungen im Zustand der zugrunde liegenden Infrastruktur. Diese Änderungen könnten zu einer mangelnden Verfügbarkeit der Anwendung führen. Die erweiterten Zustandsberichte von Elastic Beanstalk bieten eine Statusbeschreibung, um den Schweregrad der identifizierten Probleme einzuschätzen und mögliche Ursachen zu identifizieren, die untersucht werden müssen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CA-7(a)(b)	Die Organisation entwickelt eine Strategie zur kontinuierlichen Überwachung und implementiert ein kontinuierliches Überwachungsprogramm, das Folgendes umfasst: a. Festlegung von [Zuweisung: von der Organisation definierte Kennzahlen], die überwacht werden sollen; b. Festlegung von [Zuweisung: von der Organisation festgelegte Häufigkeiten] für die Überwachung und [Zuweisung: von der Organisation festgelegte Häufigkeiten] für Bewertungen, die diese Überwachung unterstützen.	cloudtrail-enabled	AWS CloudTrail kann durch die Aufzeichnung von Aktionen und API-Aufrufen in der AWS Management Console bei der Nichtabstreitbarkeit helfen. Sie können die Benutzer und AWS Konten, die einen AWS Dienst aufgerufen haben, die Quell-IP-Adresse, über die die Anrufe generiert wurden, und die Zeitpunkte der Anrufe identifizieren. Einzelheiten zu den erfassten Daten finden Sie in den AWS CloudTrail Datensatzinhalten.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CA-7(a)(b)	Die Organisation entwickelt eine Strategie zur kontinuierlichen Überwachung und implementiert ein kontinuierliches Überwachungsprogramm, das Folgendes umfasst: a. Festlegung von [Zuweisung: von der Organisation definierte Kennzahlen], die überwacht werden sollen; b. Festlegung von [Zuweisung: von der Organisation festgelegte Häufigkeiten] für die Überwachung und [Zuweisung: von der Organisation festgelegte Häufigkeiten] für Bewertungen, die diese Überwachung unterstützen.	cloudtrail-s3-dataevents-enabled	Die Erfassung von Simple Storage Service (Amazon S3)-Datenereignissen unterstützt die Erkennung von ungewöhnlichen Aktivitäten. Zu den Details gehören AWS Kontoinformationen, über die auf einen Amazon S3 S3-Bucket zugegriffen wurde, die IP-Adresse und die Uhrzeit des Ereignisses.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CA-7(a)(b)	Die Organisation entwickelt eine Strategie zur kontinuierlichen Überwachung und implementiert ein kontinuierliches Überwachungsprogramm, das Folgendes umfasst: a. Festlegung von [Zuweisung: von der Organisation definierte Kennzahlen], die überwacht werden sollen; b. Festlegung von [Zuweisung: von der Organisation festgelegte Häufigkeiten] für die Überwachung und [Zuweisung: von der Organisation festgelegte Häufigkeiten] für Bewertungen, die diese Überwachung unterstützen.	dynamodb-throughput-limit-check	Aktivieren Sie diese Regel, um sicherzustellen, dass die bereitgestellte Durchsatzkapazität in Ihren Amazon-DynamoDB-Tabellen überprüft wird. Dies ist der Umfang der Lese- und Schreibaktivitäten, der von den jeweiligen Tabellen unterstützt werden kann. DynamoDB verwendet diese Informationen für das Reservieren ausreichender Systemressourcen, um Ihren Durchsatzanforderungen gerecht zu werden. Diese Regel generiert eine Warnung, wenn sich der Durchsatz dem Höchstlimit für ein Kundenkonto nähert. Mit dieser Regel können Sie optional die Parameter RCUThreshold Kontoprozentsatz

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			(Konfigurationsstandard: 80) und WCUThreshold Kontoprozentsatz (Konfigurationsstandard: 80) festlegen. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CA-7(a)(b)	Die Organisation entwickelt eine Strategie zur kontinuierlichen Überwachung und implementiert ein kontinuierliches Überwachungsprogramm, das Folgendes umfasst: a. Festlegung von [Zuweisung: von der Organisation definierte Kennzahlen], die überwacht werden sollen; b. Festlegung von [Zuweisung: von der Organisation festgelegte Häufigkeiten] für die Überwachung und [Zuweisung: von der Organisation festgelegte Häufigkeiten] für Bewertungen, die diese Überwachung unterstützen.	lambda-concurrency-check	Diese Regel stellt sicher, dass die Höchst- und Untergrenzen für die Gleichzeitigkeit einer Lambda-Funktion festgelegt werden. Dies kann Sie beim Baselining für die Anzahl der Anforderungen unterstützen, die Ihre Funktion zu einem bestimmten Zeitpunkt verarbeitet.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CA-7(a)(b)	Die Organisation entwickelt eine Strategie zur kontinuierlichen Überwachung und implementiert ein kontinuierliches Überwachungsprogramm, das Folgendes umfasst: a. Festlegung von [Zuweisung: von der Organisation definierte Kennzahlen], die überwacht werden sollen; b. Festlegung von [Zuweisung: von der Organisation festgelegte Häufigkeiten] für die Überwachung und [Zuweisung: von der Organisation festgelegte Häufigkeiten] für Bewertungen, die diese Überwachung unterstützen.	lambda-dlq-check	Aktivieren Sie diese Regel, um das entsprechende Personal über Amazon Simple Queue Service (Amazon SQS) oder Amazon Simple Notification Service (Amazon SNS) zu benachrichtigen, wenn eine Funktion ausgefallen ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CA-7(a)(b)	Die Organisation entwickelt eine Strategie zur kontinuierlichen Überwachung und implementiert ein kontinuierliches Überwachungsprogramm, das Folgendes umfasst: a. Festlegung von [Zuweisung: von der Organisation definierte Kennzahlen], die überwacht werden sollen; b. Festlegung von [Zuweisung: von der Organisation festgelegte Häufigkeiten] für die Überwachung und [Zuweisung: von der Organisation festgelegte Häufigkeiten] für Bewertungen, die diese Überwachung unterstützen.	multi-region-cloudtrail-enabled	AWS CloudTrail zeichnet Aktionen und API-Aufrufe der AWS Management Console auf. Sie können feststellen, welche Benutzer und Konten angerufen wurden AWS, von welcher Quell-IP-Adresse aus die Anrufe getätigt wurden und wann die Anrufe erfolgten. CloudTrail übermittelt Protokolldateien aus allen AWS Regionen an Ihren S3-Bucket, wenn MULTI_REGION_CLOUD_TRAIL_ENABLED aktiviert ist. Außerdem wird beim AWS Start einer neuen Region derselbe Trail in der neuen Region erstellt. CloudTrail Dadurch erhalten Sie automatisch Protokolldateien mit API-Aktivitäten für die neue Region.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CA-7(a)(b)	Die Organisation entwickelt eine Strategie zur kontinuierlichen Überwachung und implementiert ein kontinuierliches Überwachungsprogramm, das Folgendes umfasst: a. Festlegung von [Zuweisung: von der Organisation definierte Kennzahlen], die überwacht werden sollen; b. Festlegung von [Zuweisung: von der Organisation festgelegte Häufigkeiten] für die Überwachung und [Zuweisung: von der Organisation festgelegte Häufigkeiten] für Bewertungen, die diese Überwachung unterstützen.	redshift-cluster-configuration-check	Um Daten im Ruhezustand zu schützen, muss die Verschlüsselung für Ihre Amazon-Redshift-Cluster aktiviert sein. Sie müssen auch sicherstellen, dass die erforderlichen Konfigurationen auf Amazon-Redshift-Clustern bereitgestellt werden. Die Prüfungsprotokollierung muss aktiviert sein, um Informationen zu Verbindungen und Benutzeraktivitäten in der Datenbank bereitzustellen. Diese Regel erfordert, dass ein Wert für clusterDbEncrypted (Config Default: TRUE) und LoggingEnabled (Config Default: TRUE) gesetzt ist. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CM-2	Die Organisation entwickelt, dokumentiert und verwaltet unter Konfigurationskontrolle eine aktuelle Basiskonfiguration des Informationssystems.	ec2-manager instance-managed-by-systems	Eine Bestandsaufnahme der Softwareplattformen und Anwendungen innerhalb des Unternehmens ist möglich, indem Amazon Elastic Compute Cloud (Amazon EC2) - Instances mit AWS Systems Manager verwaltet werden. Verwenden Sie AWS Systems Manager, um detaillierte Systemkonfigurationen, Betriebssystem-Patch-Levels, Namen und Typ der Dienste, Softwareinstallationen, Anwendungsname, Herausgeber und Version sowie andere Details zu Ihrer Umgebung bereitzustellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CM-2	Die Organisation entwickelt, dokumentiert und verwaltet unter Konfigurationskontrolle eine aktuelle Basiskonfiguration des Informationssystems.	ec2-prüfen managedinstance-association-compliance-status	Verwenden Sie AWS Systems Manager Associations, um bei der Inventarisierung von Softwareplattformen und Anwendungen innerhalb eines Unternehmens zu helfen. AWS Systems Manager weist Ihren verwalteten Instanzen einen Konfigurationsstatus zu und ermöglicht es Ihnen, Basiswerte für Betriebssystem-Patch-Levels, Softwareinstallationen, Anwendungskonfigurationen und andere Details zu Ihrer Umgebung festzulegen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CM-2	Die Organisation entwickelt, dokumentiert und verwaltet unter Konfigurationskontrolle eine aktuelle Basiskonfiguration des Informationssystems.	ec2-stopped-instance	Aktivieren Sie diese Regel, um bei der Basiskonfiguration von Amazon Elastic Compute Cloud (Amazon EC2) - Instances zu helfen, indem Sie überprüfen, ob EC2 Amazon-Instances gemäß den Standards Ihrer Organisation für mehr als die zulässige Anzahl von Tagen gestoppt wurden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CM-2	Die Organisation entwickelt, dokumentiert und verwaltet unter Konfigurationskontrolle eine aktuelle Basiskonfiguration des Informationssystems.	ec2- volume-inuse-check	Diese Regel stellt sicher, dass Amazon Elastic Block Store-Volumes, die an Amazon Elastic Compute Cloud (Amazon EC2) - Instances angehängt sind, zum Löschen markiert werden, wenn eine Instance beendet wird. Wenn ein Amazon-EBS-Volume nicht gelöscht wird, wenn die Instance, an die es angehängt ist, beendet wird, kann dies gegen das Konzept der geringsten Funktionalität verstoßen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CM-2	Die Organisation entwickelt, dokumentiert und verwaltet unter Konfigurationskontrolle eine aktuelle Basiskonfiguration des Informationssystems.	elb-deletion-protection-enabled	Diese Regel sorgt dafür, dass der Löschschutz für Elastic Load Balancing aktiviert ist. Verwenden Sie diese Funktion, um zu verhindern, dass Ihr Load Balancer versehentlich oder böswillig gelöscht wird, was zum Verlust der Verfügbarkeit Ihrer Anwendungen führen kann.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CM-2	Die Organisation entwickelt, dokumentiert und verwaltet unter Konfigurationskontrolle eine aktuelle Basiskonfiguration des Informationssystems.	restricted-common-ports	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass gemeinsame Ports für Amazon Elastic Compute Cloud (Amazon EC2) -Sicherheitsgruppen eingeschränkt sind. Wenn der Zugriff auf Ports nicht auf vertrauenswürdige Quellen beschränkt wird, kann dies zu Angriffen auf die Verfügbarkeit, Integrität und Vertraulichkeit von Systemen führen. Mit dieser Regel können Sie optional die Parameter blockedPort1–blockedPort5 festlegen (Standardkonfigurationen: 20, 21, 3389, 3306, 4333). Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CM-2	Die Organisation entwickelt, dokumentiert und verwaltet unter Konfigurationskontrolle eine aktuelle Basiskonfiguration des Informationssystems.	alb-waf-enabled	Stellen Sie sicher, dass AWS WAF auf Elastic Load Balancers (ELB) aktiviert ist, um Webanwendungen zu schützen. Eine WAF trägt zum Schutz Ihrer Webanwendungen oder APIs vor gängigen Web-Exploits bei. Diese Web-Exploits können sich auf die Verfügbarkeit auswirken, die Sicherheit gefährden oder übermäßige Ressourcen in Ihrer Umgebung verbrauchen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CM-2	Die Organisation entwickelt, dokumentiert und verwaltet unter Konfigurationskontrolle eine aktuelle Basiskonfiguration des Informationssystems.	dms-replication-not-public	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass auf DMS-Replikationsinstanzen nicht öffentlich zugegriffen werden kann. DMS-Replikations-Instances können vertrauliche Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.
CM-2	Die Organisation entwickelt, dokumentiert und verwaltet unter Konfigurationskontrolle eine aktuelle Basiskonfiguration des Informationssystems.	ebs-snapshot-public-restorable-überprüfen	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass EBS-Snapshots nicht öffentlich wiederherstellbar sind. EBS-Volume-Snapshots können vertrauliche Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CM-2	Die Organisation entwickelt, dokumentiert und verwaltet unter Konfigurationskontrolle eine aktuelle Basiskonfiguration des Informationssystems.	ec2- instance-no-public-ip	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon Elastic Compute Cloud (Amazon EC2) - Instances nicht öffentlich zugänglich sind. EC2 Amazon-Instances können vertrauliche Informationen enthalten, und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CM-2	Die Organisation entwickelt, dokumentiert und verwaltet unter Konfigurationskontrolle eine aktuelle Basiskonfiguration des Informationssystems.	elasticsearch-in-vpc-only	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass sich Amazon OpenSearch OpenSearch Service (Service) - Domains innerhalb einer Amazon Virtual Private Cloud (Amazon VPC) befinden. Eine OpenSearch Service-Domain innerhalb einer Amazon VPC ermöglicht die sichere Kommunikation zwischen OpenSearch Service und anderen Services innerhalb der Amazon VPC, ohne dass ein Internet-Gateway, ein NAT-Gerät oder eine VPN-Verbindung erforderlich ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CM-2	Die Organisation entwickelt, dokumentiert und verwaltet unter Konfigurationskontrolle eine aktuelle Basiskonfiguration des Informationssystems.	emr-master-no-public-ip	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon EMR-Cluster-Masterknoten nicht öffentlich zugänglich sind. Amazon-EMR-Cluster-Hauptknoten können vertrauliche Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CM-2	Die Organisation entwickelt, dokumentiert und verwaltet unter Konfigurationskontrolle eine aktuelle Basiskonfiguration des Informationssystems.	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) Security Groups können bei der Verwaltung des Netzwerkzugriffs helfen, indem sie eine statusbehaftete Filterung von eingehendem und ausgehendem Netzwerkverkehr zu Ressourcen bereitstellen. AWS Wenn Sie eingehenden (oder entfernten) Datenverkehr von 0.0.0.0/0 bis Port 22 auf Ihren Ressourcen nicht zulassen, können Sie den Remote-Zugriff einschränken.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CM-2	Die Organisation entwickelt, dokumentiert und verwaltet unter Konfigurationskontrolle eine aktuelle Basiskonfiguration des Informationssystems.	ec2- instances-in-vpc	Stellen Sie Amazon Elastic Compute Cloud (Amazon EC2) -Instances innerhalb einer Amazon Virtual Private Cloud (Amazon VPC) bereit, um eine sichere Kommunikation zwischen einer Instance und anderen Services innerhalb der Amazon VPC zu ermöglichen, ohne dass ein Internet-Gateway, ein NAT-Gerät oder eine VPN-Verbindung erforderlich ist. Der gesamte Datenverkehr bleibt sicher in der AWS Cloud. Domains, die sich innerhalb einer VPC befinden, verfügen aufgrund ihrer logischen Isolierung im Vergleich zu Domains mit öffentlichen Endpunkten über eine zusätzliche Sicherheitsebene. Weisen Sie EC2

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			Amazon-Instances einer Amazon-VPC zu, um den Zugriff ordnungsgemäß zu verwalten.
CM-2	Die Organisation entwickelt, dokumentiert und verwaltet unter Konfigurationskontrolle eine aktuelle Basiskonfiguration des Informationssystems.	lambda-function-public-access-verboten	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass AWS Lambda-Funktionen nicht öffentlich zugänglich sind. Der öffentliche Zugriff kann möglicherweise die Verfügbarkeit von Ressourcen beeinträchtigen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CM-2	Die Organisation entwickelt, dokumentiert und verwaltet unter Konfigurationskontrolle eine aktuelle Basiskonfiguration des Informationssystems.	lambda-inside-vpc	Stellen Sie AWS Lambda-Funktionen in einer Amazon Virtual Private Cloud (Amazon VPC) bereit, um eine sichere Kommunikation zwischen einer Funktion und anderen Diensten innerhalb der Amazon VPC zu gewährleisten. Bei dieser Konfiguration sind kein Internet-Gateway, kein NAT-Gerät und keine VPN-Verbindung erforderlich. Der gesamte Datenverkehr bleibt sicher in der Cloud. AWS Domains, die sich innerhalb einer VPC befinden, verfügen aufgrund ihrer logischen Isolierung im Vergleich zu Domains mit öffentlichen Endpunkten über eine zusätzliche Sicherheitsebene. Um den Zugriff ordnungsgemäß zu verwalten,

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			sollten AWS Lambda-Funktionen einer VPC zugewiesen werden.
CM-2	Die Organisation entwickelt, dokumentiert und verwaltet unter Konfigurationskontrolle eine aktuelle Basiskonfiguration des Informationssystems.	rds-instance-public-access-überprüfen	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Relational Database Service (Amazon RDS) -Instances nicht öffentlich sind. Amazon-RDS-Datenbank-Instances können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CM-2	Die Organisation entwickelt, dokumentiert und verwaltet unter Konfigurationskontrolle eine aktuelle Basiskonfiguration des Informationssystems.	rds-snapshots-public-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Relational Database Service (Amazon RDS) -Instances nicht öffentlich sind. Amazon-RDS-Datenbank-Instances können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CM-2	Die Organisation entwickelt, dokumentiert und verwaltet unter Konfigurationskontrolle eine aktuelle Basiskonfiguration des Informationssystems.	redshift-cluster-public-access-überprüfen	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Redshift Redshift-Cluster nicht öffentlich sind. Amazon-Redshift-Cluster können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.
CM-2	Die Organisation entwickelt, dokumentiert und verwaltet unter Konfigurationskontrolle eine aktuelle Basiskonfiguration des Informationssystems.	s-3 bucket-public-read-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie nur autorisierten Benutzern, Prozessen und Geräten Zugriff auf Amazon Simple Storage Service (Amazon S3) - Buckets gewähren. Die Verwaltung des Zugriffs sollte mit der Klassifizierung der Daten übereinstimmen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CM-2	Die Organisation entwickelt, dokumentiert und verwaltet unter Konfigurationskontrolle eine aktuelle Basiskonfiguration des Informationssystems.	s-3 bucket-public-write-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie nur autorisierten Benutzern, Prozessen und Geräten Zugriff auf Amazon Simple Storage Service (Amazon S3) - Buckets gewähren. Die Verwaltung des Zugriffs sollte mit der Klassifizierung der Daten übereinstimmen.
CM-2	Die Organisation entwickelt, dokumentiert und verwaltet unter Konfigurationskontrolle eine aktuelle Basiskonfiguration des Informationssystems.	sagemaker-notebook-no-direct-Internetzugang	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass SageMaker Amazon-Notebooks keinen direkten Internetzugang zulassen. Indem Sie direkten Internetzugang blockieren, vermeiden Sie, dass unbefugte Benutzer auf sensible Daten zugreifen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CM-2	Die Organisation entwickelt, dokumentiert und verwaltet unter Konfigurationskontrolle eine aktuelle Basiskonfiguration des Informationssystems.	vpc-default-security-group-geschlossen	Sicherheitsgruppen von Amazon Elastic Compute Cloud (Amazon EC2) können bei der Verwaltung des Netzwerkzugriffs helfen, indem sie eine statusbehaftete Filterung des ein- und ausgehenden Netzwerkverkehrs zu Ressourcen bereitstellen. AWS Die Beschränkung des gesamten Datenverkehrs auf die Standardsicherheitsgruppe hilft dabei, den Fernzugriff auf Ihre Ressourcen einzuschränken. AWS

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CM-2	Die Organisation entwickelt, dokumentiert und verwaltet unter Konfigurationskontrolle eine aktuelle Basiskonfiguration des Informationssystems.	vpc-sg-open-only-to-authorized-ports	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass gemeinsame Ports für Amazon Elastic Compute Cloud (Amazon EC2) -Sicherheitsgruppen eingeschränkt sind. Wenn der Zugriff auf Ports nicht auf vertrauenswürdige Quellen beschränkt wird, kann dies zu Angriffen auf die Verfügbarkeit, Integrität und Vertraulichkeit von Systemen führen. Durch die Beschränkung des Zugriffs auf Ressourcen innerhalb einer Sicherheitsgruppe aus dem Internet (0.0.0.0/0) kann der Remote-Zugriff auf interne Systeme gesteuert werden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CM-2	Die Organisation entwickelt, dokumentiert und verwaltet unter Konfigurationskontrolle eine aktuelle Basiskonfiguration des Informationssystems.	no-unrestricted-route-to-igw	Stellen Sie sicher, dass EC2 Amazon-Routentabellen keine uneingeschränkten Routen zu einem Internet-Gateway enthalten. Durch das Entfernen oder Beschränken des Internetzugangs für Workloads innerhalb von Amazon VPCs können unbeabsichtigte Zugriffe in Ihrer Umgebung reduziert werden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CM-2	Die Organisation entwickelt, dokumentiert und verwaltet unter Konfigurationskontrolle eine aktuelle Basiskonfiguration des Informationssystems.	s3 bucket-level-public-access - verboten	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Simple Storage Service (Amazon S3) -Buckets nicht öffentlich zugänglich sind. Diese Regel trägt dazu bei, sensible Daten vor unbefugten Remote-Benutzern zu schützen, indem sie den öffentlichen Zugriff auf Bucket-Ebene verhindert.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CM-2	Die Organisation entwickelt, dokumentiert und verwaltet unter Konfigurationskontrolle eine aktuelle Basiskonfiguration des Informationssystems.	subnet-auto-assign-public-ip-deaktiviert	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon Virtual Private Cloud (VPC) -Subnetzen nicht automatisch eine öffentliche IP-Adresse zugewiesen wird. Amazon Elastic Compute Cloud (EC2) -Instances, die in Subnetzen gestartet werden, in denen dieses Attribut aktiviert ist, haben ihrer primären Netzwerkschnittstelle eine öffentliche IP-Adresse zugewiesen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CM-2	Die Organisation entwickelt, dokumentiert und verwaltet unter Konfigurationskontrolle eine aktuelle Basiskonfiguration des Informationssystems.	autoscaling-launch-config-public-ip-deaktiviert	Wenn Sie Ihre Netzwerkschnittstellen mit einer öffentlichen IP-Adresse konfigurieren, sind die diesen Netzwerkschnittstellen zugehörigen Ressourcen über das Internet erreichbar. EC2 Ressourcen sollten nicht öffentlich zugänglich sein, da dies einen unbeabsichtigten Zugriff auf Ihre Anwendungen oder Server ermöglichen kann.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CM-2	Die Organisation entwickelt, dokumentiert und verwaltet unter Konfigurationskontrolle eine aktuelle Basiskonfiguration des Informationssystems.	api-gw-associated-with-WAF	AWS Mit WAF können Sie eine Reihe von Regeln (eine so genannte Web Access Control List (Web ACL)) konfigurieren, die Webanfragen auf der Grundlage von anpassbaren Websicherheitsregeln und -bedingungen, die Sie definieren, zulassen, blockieren oder zählen. Stellen Sie sicher, dass Ihre Amazon-API-Gateway-Stufe mit einer WAF-Web-ACL verknüpft ist, um sie vor böswilligen Angriffen zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CM-2	Die Organisation entwickelt, dokumentiert und verwaltet unter Konfigurationskontrolle eine aktuelle Basiskonfiguration des Informationssystems.	account-level-public-accesss3-Blöcke-periodisch	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Simple Storage Service (Amazon S3) -Buckets nicht öffentlich zugänglich sind. Diese Regel trägt dazu bei, sensible Daten vor unbefugten Remote-Benutzern zu schützen, indem sie den öffentlichen Zugriff verhindert. Mit dieser Regel können Sie optional die Parameter ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) und restrictPublicBuckets Parameter (Config Default: True) festlegen. Die tatsächlichen Werte müssen den Richtlini

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			en Ihrer Organisation entsprechen.
CM-7(a)	Die Organisation: a. Konfiguriert das Informationssystem auf eine Weise, dass nur wesentliche Funktionen bereitgestellt werden.	ec2-manager instance-managed-by-systems	Eine Bestandsaufnahme der Softwareplattformen und Anwendungen innerhalb des Unternehmens ist möglich, indem Amazon Elastic Compute Cloud (Amazon EC2) - Instances mit AWS Systems Manager verwaltet werden. Verwenden Sie AWS Systems Manager, um detaillierte Systemkonfigurationen, Betriebssystem-Patch-Levels, Namen und Typ der Dienste, Softwareinstallationen, Anwendungsname, Herausgeber und Version sowie andere Details zu Ihrer Umgebung bereitzustellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CM-7(a)	Die Organisation: a. Konfiguriert das Informationssystem auf eine Weise, dass nur wesentliche Funktionen bereitgestellt werden.	ec2-prüfen managedinstance-association-compliance-status	Verwenden Sie AWS Systems Manager Associations, um bei der Inventarisierung von Softwareplattformen und Anwendungen innerhalb eines Unternehmens zu helfen. AWS Systems Manager weist Ihren verwalteten Instanzen einen Konfigurationsstatus zu und ermöglicht es Ihnen, Basiswerte für Betriebssystem-Patch-Levels, Softwareinstallationen, Anwendungskonfigurationen und andere Details zu Ihrer Umgebung festzulegen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CM-7(a)	Die Organisation: a. Konfiguriert das Informationssystem auf eine Weise, dass nur wesentliche Funktionen bereitgestellt werden.	ec2- instance-profile-attached	EC2 Instanzprofile übergeben eine IAM-Rolle an eine Instanz. EC2 Das Anhängen eines Instance-Profils an Ihre Instances kann bei der Implementierung von geringsten Berechtigungen und der Berechtigungsverwaltung helfen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CM-8(1)	Die Organisation aktualisiert das Inventar der Informationssystemkomponenten als integralen Bestandteil der Installation und Demontage von Komponenten sowie der Aktualisierung von Informationssystemen.	ec2-manager instance-managed-by-systems	Eine Bestandsaufnahme der Softwareplattformen und Anwendungen innerhalb des Unternehmens ist möglich, indem Amazon Elastic Compute Cloud (Amazon EC2) - Instances mit AWS Systems Manager verwaltet werden. Verwenden Sie AWS Systems Manager, um detaillierte Systemkonfigurationen, Betriebssystem-Patch-Levels, Namen und Typ der Dienste, Softwareinstallationen, Anwendungsname, Herausgeber und Version sowie andere Details zu Ihrer Umgebung bereitzustellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CM-8(1)	Die Organisation aktualisiert das Inventar der Informationssystemkomponenten als integralen Bestandteil der Installation und Demontage von Komponenten sowie der Aktualisierung von Informationssystemen.	ec2-prüfen managedinstance-association-compliance-status	Verwenden Sie AWS Systems Manager Associations, um bei der Inventarisierung von Softwareplattformen und Anwendungen innerhalb eines Unternehmens zu helfen. AWS Systems Manager weist Ihren verwalteten Instanzen einen Konfigurationsstatus zu und ermöglicht es Ihnen, Basiswerte für Betriebssystem-Patch-Levels, Softwareinstallationen, Anwendungskonfigurationen und andere Details zu Ihrer Umgebung festzulegen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CM-8(3)(a)	Die Organisation: a. Setzt kontinuierlich automatisierte Mechanismen ein und verwendet automatisierte Mechanismen mit einer Erkennungsverzögerung von maximal fünf Minuten, um nicht autorisierte Hardware-, Software- und Firmware-Komponenten im Informationssystem zu erkennen.	ec2-manager instance-managed-by-systems	Eine Bestandsaufnahme der Softwareplattformen und Anwendungen innerhalb des Unternehmens ist möglich, indem Amazon Elastic Compute Cloud (Amazon EC2) - Instances mit AWS Systems Manager verwaltet werden. Verwenden Sie AWS Systems Manager, um detaillierte Systemkonfigurationen, Betriebssystem-Patch-Levels, Namen und Typ der Dienste, Softwareinstallationen, Anwendungsname, Herausgeber und Version sowie andere Details zu Ihrer Umgebung bereitzustellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CM-8(3)(a)	Die Organisation: a. Setzt kontinuierlich automatisierte Mechanismen ein und verwendet automatisierte Mechanismen mit einer Erkennungsverzögerung von maximal fünf Minuten, um nicht autorisierte Hardware-, Software- und Firmware-Komponenten im Informationssystem zu erkennen.	ec2-prüfen managedinstance-association-compliance-status	Verwenden Sie AWS Systems Manager Associations, um bei der Inventarisierung von Softwareplattformen und Anwendungen innerhalb eines Unternehmens zu helfen. AWS Systems Manager weist Ihren verwalteten Instanzen einen Konfigurationsstatus zu und ermöglicht es Ihnen, Basiswerte für Betriebssystem-Patch-Levels, Softwareinstallationen, Anwendungskonfigurationen und andere Details zu Ihrer Umgebung festzulegen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CM-8(3)(a)	Die Organisation: a. Setzt kontinuierlich automatisierte Mechanismen ein und verwendet automatisierte Mechanismen mit einer Erkennungsverzögerung von maximal fünf Minuten, um nicht autorisierte Hardware-, Software- und Firmware-Komponenten im Informationssystem zu erkennen.	ec2-prüfen managedinstance-patch-compliance-status	Aktivieren Sie diese Regel, um bei der Identifizierung und Dokumentation von Sicherheitslücken in Amazon Elastic Compute Cloud (Amazon EC2) zu helfen. Die Regel prüft, ob die EC2 Amazon-Instance die Patch-Konformität im AWS Systems Manager gemäß den Richtlinien und Verfahren Ihrer Organisation einhält.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CM-8(3)(a)	Die Organisation: a. Setzt kontinuierlich automatisierte Mechanismen ein und verwendet automatisierte Mechanismen mit einer Erkennungsverzögerung von maximal fünf Minuten, um nicht autorisierte Hardware-, Software- und Firmware-Komponenten im Informationssystem zu erkennen.	guardduty-enabled-centralized	Amazon GuardDuty kann mithilfe von Threat Intelligence Feeds helfen, potenzielle Cybersicherheitsereignisse zu überwachen und zu erkennen. Dazu gehören Listen mit bösartigen IPs und maschinellen Lernmethoden zur Identifizierung unerwarteter, nicht autorisierter und bösartiger Aktivitäten in Ihrer AWS Cloud-Umgebung.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CP-6 (1)	Das Unternehmen identifiziert einen alternativen Speichers tandort, der ausreiche nd vom primären Speicherort getrennt ist, um die Anfälligk eit für dieselben Bedrohungen zu verringern.	dynamodb-in-backup-plan	Um Sie bei Datensich erungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon DynamoDB-Tabellen Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwaltet er Backup-Service mit einer richtlini enbasierten Backup-Lösung. Diese Lösung vereinfac ht Ihr Sicherung smanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforde rungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CP-6 (1)	Das Unternehmen identifiziert einen alternativen Speichers tandort, der ausreiche nd vom primären Speicherort getrennt ist, um die Anfälligk eit für dieselben Bedrohungen zu verringern.	ebs-in-backup-plan	Um Sie bei Datensich erungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon Elastic Block Store (Amazon EBS) -Volumes Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwaltet er Backup-Service mit einer richtlini enbasierten Backup-Lösung. Diese Lösung vereinfac ht Ihr Sicherung smanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforde rungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CP-6 (1)	Das Unternehmen identifiziert einen alternativen Speichers tandort, der ausreiche nd vom primären Speicherort getrennt ist, um die Anfälligk eit für dieselben Bedrohungen zu verringern.	efs-in-backup-plan	Um Sie bei Datensich erungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon Elastic File System (Amazon EFS) -Dateisysteme Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwaltet er Backup-Service mit einer richtlini enbasierten Backup-Lösung. Diese Lösung vereinfac ht Ihr Sicherung smanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforde rungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CP-6 (1)	Das Unternehmen identifiziert einen alternativen Speichers tandort, der ausreiche nd vom primären Speicherort getrennt ist, um die Anfälligk eit für dieselben Bedrohungen zu verringern.	redshift-backup-en abled	Stellen Sie zur Unterstützung der Datensicherungspro zesse sicher, dass Ihre Amazon-Re dshift-Cluster über automatisierte Snapshots verfügen. Wenn automatis ierte Snapshots für einen Cluster aktiviert sind, erstellt Redshift in regelmäßi gen Abständen Snapshots dieses Clusters. Standardm äßig erzeugt Redshift ungefähr alle acht Stunden oder nach 5 GB geänderten Daten pro Knoten einen Snapshot, je nachdem, was zuerst auftritt.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CP-6 (1)	Das Unternehmen identifiziert einen alternativen Speichers tandort, der ausreiche nd vom primären Speicherort getrennt ist, um die Anfälligk eit für dieselben Bedrohungen zu verringern.	db-instance-backup-enabled	Die Sicherung sfunktion von Amazon RDS erstellt Sicherung en Ihrer Datenbank en und Transakti onsprotokolle. Amazon RDS erstellt einen Snapshot für das Speichervolume Ihrer DB-Instance, sodass die gesamte DB-Instance gesichert wird. Sie können im System spezifische Aufbewahrungsfrist en festlegen, um Ihre Ausfallsicherheits anforderungen zu erfüllen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CP-6 (1)	Das Unternehmen identifiziert einen alternativen Speichers tandort, der ausreiche nd vom primären Speicherort getrennt ist, um die Anfälligk eit für dieselben Bedrohungen zu verringern.	elasticache-redis-cluster-automatic-Backup-Check	Wenn automatische Backups aktiviert sind, ElastiCache erstellt Amazon täglich ein Backup des Clusters. Die Sicherung kann für eine von Ihrer Organisation festgelegte Anzahl von Tagen aufbewahrt werden. Automatische Backups schützen vor Datenverlust. Bei einem Ausfall können Sie einen neuen Cluster erstellen, der Ihre Daten aus dem aktuellen Backup wiederherstellt.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CP-6 (1)	Das Unternehmen identifiziert einen alternativen Speichers tandort, der ausreiche nd vom primären Speicherort getrennt ist, um die Anfälligk eit für dieselben Bedrohungen zu verringern.	s-3 bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) unterstützt die Aufrechterhaltung einer angemesse nen Kapazität und Verfügbarkeit. CRR ermöglicht das automatische, asynchrone Kopieren von Objekten in Amazon-S3-Buckets, um die Datenverf ügbarkeit sicherzus tellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CP-6 (1)	Das Unternehmen identifiziert einen alternativen Speichers tandort, der ausreiche nd vom primären Speicherort getrennt ist, um die Anfälligk eit für dieselben Bedrohungen zu verringern.	s-3 bucket-versioning-enabled	Die Versionsv erwaltung von Amazon Simple Storage Service (Amazon S3)-Bucke ts hilft dabei, mehrere Varianten eines Objekts im selben Amazon-S3-Bucket zu speichern. Verwenden Sie die Versionsv erwaltung, um sämtliche Versionen aller Objekte in Ihrem Amazon-S3-Bucket zu speichern , abzurufen oder wiederherzustellen . Mit der Versionsv erwaltung können Sie Versionen sowohl nach unbeabsic htigten Benutzera ktionen als auch nach Anwendungsfehlern problemlos wiederher stellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CP-9	Das Informati onssystem a. Führen Sie Backups von Informationen auf Benutzerebene durch, die in [Aufgabe: organisationsdefin ierte Systemkom ponenten] [Aufgabe: von der Organisation festgelegte Häufigkei t im Einklang mit den Zielen für Wiederher stellungszeit und Wiederherstellungs punkt] enthalten sind; b. Durchführung von Backups der im System enthalten en Informationen auf Systemebe ne [Aufgabe: vom Unternehmen festgelegte Häufigkei t im Einklang mit den Zielen für Wiederher stellungszeit und Wiederherstellungs punkt]; c. Durchführ ung von Backups der Systemdokumentatio n, einschließlich sicherheits- und	dynamodb-in-backup-plan	Um Sie bei Datensich erungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon DynamoDB-Tabellen Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwaltet er Backup-Service mit einer richtlini enbasierten Backup-Lösung. Diese Lösung vereinfac ht Ihr Sicherung smanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforde rungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	datenschutzrelevanter Dokumentation [Aufgabe: von der Organisation festgelegte Häufigkeit, die den Zielen für Wiederherstellungszeit und Wiederherstellungspunkt entsprich t]; und. Schützen Sie die Vertraulichkeit, Integrität und Verfügbarkeit von Backup-Informationen.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CP-9	Das Informationssystem a. Führen Sie Backups von Informationen auf Benutzerebene durch, die in [Aufgabe: organisationsdefinierte Systemkomponenten] [Aufgabe: von der Organisation festgelegte Häufigkeit im Einklang mit den Zielen für Wiederherstellungszeit und Wiederherstellungspunkt] enthalten sind; b. Durchführung von Backups der im System enthaltenen Informationen auf Systemebene [Aufgabe: vom Unternehmen festgelegte Häufigkeit im Einklang mit den Zielen für Wiederherstellungszeit und Wiederherstellungspunkt]; c. Durchführung von Backups der Systemdokumentation, einschließlich sicherheits- und	ebs-in-backup-plan	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon Elastic Block Store (Amazon EBS) -Volumes Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	datenschutzrelevanter Dokumentation [Aufgabe: von der Organisation festgelegte Häufigkeit, die den Zielen für Wiederherstellungszeit und Wiederherstellungspunkt entsprich t]; und. Schützen Sie die Vertraulichkeit, Integrität und Verfügbarkeit von Backup-Informationen.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CP-9	Das Informationssystem a. Führen Sie Backups von Informationen auf Benutzerebene durch, die in [Aufgabe: organisationsdefinierte Systemkomponenten] [Aufgabe: von der Organisation festgelegte Häufigkeit im Einklang mit den Zielen für Wiederherstellungszeit und Wiederherstellungspunkt] enthalten sind; b. Durchführung von Backups der im System enthaltenen Informationen auf Systemebene [Aufgabe: vom Unternehmen festgelegte Häufigkeit im Einklang mit den Zielen für Wiederherstellungszeit und Wiederherstellungspunkt]; c. Durchführung von Backups der Systemdokumentation, einschließlich sicherheits- und	efs-in-backup-plan	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon Elastic File System (Amazon EFS) -Dateisysteme Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	datenschutzrelevanter Dokumentation [Aufgabe: von der Organisation festgelegte Häufigkeit, die den Zielen für Wiederherstellungszeit und Wiederherstellungspunkt entsprich t]; und. Schützen Sie die Vertraulichkeit, Integrität und Verfügbarkeit von Backup-Informationen.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CP-9	Das Informationssystem a. Führen Sie Backups von Informationen auf Benutzerebene durch, die in [Aufgabe: organisationsdefinierte Systemkomponenten] [Aufgabe: von der Organisation festgelegte Häufigkeit im Einklang mit den Zielen für Wiederherstellungszeit und Wiederherstellungspunkt] enthalten sind; b. Durchführung von Backups der im System enthaltenen Informationen auf Systemebene [Aufgabe: vom Unternehmen festgelegte Häufigkeit im Einklang mit den Zielen für Wiederherstellungszeit und Wiederherstellungspunkt]; c. Durchführung von Backups der Systemdokumentation, einschließlich sicherheits- und	redshift-backup-enabled	Stellen Sie zur Unterstützung der Datensicherungsprozesse sicher, dass Ihre Amazon-Redshift-Cluster über automatisierte Snapshots verfügen. Wenn automatisierte Snapshots für einen Cluster aktiviert sind, erstellt Redshift in regelmäßigen Abständen Snapshots dieses Clusters. Standardmäßig erzeugt Redshift ungefähr alle acht Stunden oder nach 5 GB geänderten Daten pro Knoten einen Snapshot, je nachdem, was zuerst auftritt.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	datenschutzrelevanter Dokumentation [Aufgabe: von der Organisation festgelegte Häufigkeit, die den Zielen für Wiederherstellungszeit und Wiederherstellungspunkt entsprich t]; und. Schützen Sie die Vertraulichkeit, Integrität und Verfügbarkeit von Backup-Informationen.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CP-9	Das Informati onssystem a. Führen Sie Backups von Informationen auf Benutzerebene durch, die in [Aufgabe: organisationsdefin ierte Systemkom ponenten] [Aufgabe: von der Organisation festgelegte Häufigkei t im Einklang mit den Zielen für Wiederher stellungszeit und Wiederherstellungs punkt] enthalten sind; b. Durchführung von Backups der im System enthalten en Informationen auf Systemebe ne [Aufgabe: vom Unternehmen festgelegte Häufigkei t im Einklang mit den Zielen für Wiederher stellungszeit und Wiederherstellungs punkt]; c. Durchführ ung von Backups der Systemdokumentatio n, einschließlich sicherheits- und	s-3 version-lifecycle-policy-check	Mit Amazon-S3-Lebenszyklusregeln können Sie Aktionen definieren, die Amazon S3 während der Lebensdau er eines Objekts ausführen soll (z. B. die Überführu ng von Objekten in eine andere Speicherklasse, ihre Archivierung oder Löschung nach einem bestimmten Zeitraum) .

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	datenschutzrelevanter Dokumentation [Aufgabe: von der Organisation festgelegte Häufigkeit, die den Zielen für Wiederherstellungszeit und Wiederherstellungspunkt entsprich t]; und. Schützen Sie die Vertraulichkeit, Integrität und Verfügbarkeit von Backup-Informationen.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CP-9	Das Informati onssystem a. Führen Sie Backups von Informationen auf Benutzerebene durch, die in [Aufgabe: organisationsdefin ierte Systemkom ponenten] [Aufgabe: von der Organisation festgelegte Häufigkei t im Einklang mit den Zielen für Wiederher stellungszeit und Wiederherstellungs punkt] enthalten sind; b. Durchführung von Backups der im System enthalten en Informationen auf Systemebe ne [Aufgabe: vom Unternehmen festgelegte Häufigkei t im Einklang mit den Zielen für Wiederher stellungszeit und Wiederherstellungs punkt]; c. Durchführ ung von Backups der Systemdokumentatio n, einschließlich sicherheits- und	db-instance-backup-enabled	Die Sicherung sfunktion von Amazon RDS erstellt Sicherung en Ihrer Datenbank en und Transakti onsprotokolle. Amazon RDS erstellt einen Snapshot für das Speichervolume Ihrer DB-Instance, sodass die gesamte DB-Instance gesichert wird. Sie können im System spezifische Aufbewahrungsfrist en festlegen, um Ihre Ausfallsicherheits anforderungen zu erfüllen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	datenschutzrelevanter Dokumentation [Aufgabe: von der Organisation festgelegte Häufigkeit, die den Zielen für Wiederherstellungszeit und Wiederherstellungspunkt entsprich t]; und. Schützen Sie die Vertraulichkeit, Integrität und Verfügbarkeit von Backup-Informationen.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CP-9	Das Informati onssystem a. Führen Sie Backups von Informationen auf Benutzerebene durch, die in [Aufgabe: organisationsdefin ierte Systemkom ponenten] [Aufgabe: von der Organisation festgelegte Häufigkei t im Einklang mit den Zielen für Wiederher stellungszeit und Wiederherstellungs punkt] enthalten sind; b. Durchführung von Backups der im System enthalten en Informationen auf Systemebe ne [Aufgabe: vom Unternehmen festgelegte Häufigkei t im Einklang mit den Zielen für Wiederher stellungszeit und Wiederherstellungs punkt]; c. Durchführ ung von Backups der Systemdokumentatio n, einschließlich sicherheits- und	dynamodb-pitr-enab led	Aktivieren Sie diese Regel, um zu überprüfen, ob die Informationen gesichert wurden. Es verwaltet auch die Backups, indem es sicherstellt, dass die point-in-time Wiederherstellung in Amazon DynamoDB aktiviert ist. Bei der Wiederherstellung werden fortlaufende Backups Ihrer Tabelle für die letzten 35 Tage gespeichert.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	datenschutzrelevanter Dokumentation [Aufgabe: von der Organisation festgelegte Häufigkeit, die den Zielen für Wiederherstellungszeit und Wiederherstellungspunkt entsprich t]; und. Schützen Sie die Vertraulichkeit, Integrität und Verfügbarkeit von Backup-Informationen.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CP-9	Das Informationssystem a. Führen Sie Backups von Informationen auf Benutzerebene durch, die in [Aufgabe: organisationsdefinierte Systemkomponenten] [Aufgabe: von der Organisation festgelegte Häufigkeit im Einklang mit den Zielen für Wiederherstellungszeit und Wiederherstellungspunkt] enthalten sind; b. Durchführung von Backups der im System enthaltenen Informationen auf Systemebene [Aufgabe: vom Unternehmen festgelegte Häufigkeit im Einklang mit den Zielen für Wiederherstellungszeit und Wiederherstellungspunkt]; c. Durchführung von Backups der Systemdokumentation, einschließlich sicherheits- und	ebs-optimized-instance	Eine optimierte Instance im Amazon Elastic Block Store (Amazon EBS) bietet zusätzliche, dedizierte Kapazität für Amazon-EBS-I/O-Vorgänge. Diese Optimierung bietet die beste Leistung für Ihr EBS-Volume, indem Konflikte zwischen Amazon-EBS-I/O und anderem Datenverkehr von Ihrer Instance minimiert werden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	datenschutzrelevanter Dokumentation [Aufgabe: von der Organisation festgelegte Häufigkeit, die den Zielen für Wiederherstellungszeit und Wiederherstellungspunkt entsprich t]; und. Schützen Sie die Vertraulichkeit, Integrität und Verfügbarkeit von Backup-Informationen.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CP-9	Das Informati onssystem a. Führen Sie Backups von Informationen auf Benutzerebene durch, die in [Aufgabe: organisationsdefin ierte Systemkom ponenten] [Aufgabe: von der Organisation festgelegte Häufigkei t im Einklang mit den Zielen für Wiederher stellungszeit und Wiederherstellungs punkt] enthalten sind; b. Durchführung von Backups der im System enthalten en Informationen auf Systemebe ne [Aufgabe: vom Unternehmen festgelegte Häufigkei t im Einklang mit den Zielen für Wiederher stellungszeit und Wiederherstellungs punkt]; c. Durchführ ung von Backups der Systemdokumentatio n, einschließlich sicherheits- und	elasticache-redis-cluster-automatic-Backup-Check	Wenn automatische Backups aktiviert sind, ElastiCache erstellt Amazon täglich ein Backup des Clusters. Die Sicherung kann für eine von Ihrer Organisation festgelegte Anzahl von Tagen aufbewahrt werden. Automatische Backups schützen vor Datenverlust. Bei einem Ausfall können Sie einen neuen Cluster erstellen, der Ihre Daten aus dem aktuellen Backup wiederherstellt.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	datenschutzrelevanter Dokumentation [Aufgabe: von der Organisation festgelegte Häufigkeit, die den Zielen für Wiederherstellungszeit und Wiederherstellungspunkt entsprich t]; und. Schützen Sie die Vertraulichkeit, Integrität und Verfügbarkeit von Backup-Informationen.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CP-9	Das Informationssystem a. Führen Sie Backups von Informationen auf Benutzerebene durch, die in [Aufgabe: organisationsdefinierte Systemkomponenten] [Aufgabe: von der Organisation festgelegte Häufigkeit im Einklang mit den Zielen für Wiederherstellungszeit und Wiederherstellungspunkt] enthalten sind; b. Durchführung von Backups der im System enthaltenen Informationen auf Systemebene [Aufgabe: vom Unternehmen festgelegte Häufigkeit im Einklang mit den Zielen für Wiederherstellungszeit und Wiederherstellungspunkt]; c. Durchführung von Backups der Systemdokumentation, einschließlich sicherheits- und	redshift-cluster-maintenancesettings-check	Um Daten im Ruhezustand zu schützen, muss die Verschlüsselung für Ihre Amazon-Redshift-Cluster aktiviert sein. Sie müssen auch sicherstellen, dass die erforderlichen Konfigurationen auf Amazon-Redshift-Clustern bereitgestellt werden. Die Prüfungsprotokollierung muss aktiviert sein, um Informationen zu Verbindungen und Benutzeraktivitäten in der Datenbank bereitzustellen. Diese Regel erfordert, dass ein Wert für clusterDbEncrypted (Config Default: TRUE) und LoggingEnabled (Config Default: TRUE) gesetzt ist. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	datenschutzrelevanter Dokumentation [Aufgabe: von der Organisation festgelegte Häufigkeit, die den Zielen für Wiederherstellungszeit und Wiederherstellungspunkt entsprich t]; und. Schützen Sie die Vertraulichkeit, Integrität und Verfügbarkeit von Backup-Informationen.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CP-9	Das Informati onssystem a. Führen Sie Backups von Informationen auf Benutzerebene durch, die in [Aufgabe: organisationsdefin ierte Systemkom ponenten] [Aufgabe: von der Organisation festgelegte Häufigkei t im Einklang mit den Zielen für Wiederher stellungszeit und Wiederherstellungs punkt] enthalten sind; b. Durchführung von Backups der im System enthalten en Informationen auf Systemebe ne [Aufgabe: vom Unternehmen festgelegte Häufigkei t im Einklang mit den Zielen für Wiederher stellungszeit und Wiederherstellungs punkt]; c. Durchführ ung von Backups der Systemdokumentatio n, einschließlich sicherheits- und	s-3 bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) unterstützt die Aufrechterhaltung einer angemesse nen Kapazität und Verfügbarkeit. CRR ermöglicht das automatische, asynchrone Kopieren von Objekten in Amazon-S3-Buckets, um die Datenverf ügbarkeit sicherzus tellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	datenschutzrelevanter Dokumentation [Aufgabe: von der Organisation festgelegte Häufigkeit, die den Zielen für Wiederherstellungszeit und Wiederherstellungspunkt entsprich t]; und. Schützen Sie die Vertraulichkeit, Integrität und Verfügbarkeit von Backup-Informationen.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CP-9	Das Informati onssystem a. Führen Sie Backups von Informationen auf Benutzerebene durch, die in [Aufgabe: organisationsdefin ierte Systemkom ponenten] [Aufgabe: von der Organisation festgelegte Häufigkei t im Einklang mit den Zielen für Wiederher stellungszeit und Wiederherstellungs punkt] enthalten sind; b. Durchführung von Backups der im System enthalten en Informationen auf Systemebe ne [Aufgabe: vom Unternehmen festgelegte Häufigkei t im Einklang mit den Zielen für Wiederher stellungszeit und Wiederherstellungs punkt]; c. Durchführ ung von Backups der Systemdokumentatio n, einschließlich sicherheits- und	s-3 bucket-versioning-enabled	Die Versionsv erwaltung von Amazon Simple Storage Service (Amazon S3)-Bucke ts hilft dabei, mehrere Varianten eines Objekts im selben Amazon-S3-Bucket zu speichern. Verwenden Sie die Versionsv erwaltung, um sämtliche Versionen aller Objekte in Ihrem Amazon-S3-Bucket zu speichern , abzurufen oder wiederherzustellen . Mit der Versionsv erwaltung können Sie Versionen sowohl nach unbeabsic htigten Benutzera ktionen als auch nach Anwendungsfehlern problemlos wiederher stellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	datenschutzrelevanter Dokumentation [Aufgabe: von der Organisation festgelegte Häufigkeit, die den Zielen für Wiederherstellungszeit und Wiederherstellungspunkt entsprich t]; und. Schützen Sie die Vertraulichkeit, Integrität und Verfügbarkeit von Backup-Informationen.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CP-10	Die Organisation sorgt dafür, dass das Informationssystem nach einer Unterbrechung, einer Beeinträchtigung oder einem Ausfall wiederhergestellt und wieder in einen bekannten Zustand versetzt wird.	dynamodb-autoscaling-enabled	Amazon DynamoDB Auto Scaling verwendet den AWS Application Auto Scaling-Service, um die bereitgestellte Durchsatzkapazität so anzupassen, dass sie automatisch auf tatsächliche Verkehrsmuster reagiert. Auf diese Weise kann eine Tabelle oder ein globaler sekundärer Index die bereitgestellte Lese-/Schreibkapazität erhöhen, um plötzliche Erhöhungen des Datenverkehrs ohne Drosselung zu bewältigen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CP-10	Die Organisation sorgt dafür, dass das Informationssystem nach einer Unterbrechung, einer Beeinträchtigung oder einem Ausfall wiederhergestellt und wieder in einen bekannten Zustand versetzt wird.	rds-multi-az-support	Die Multi-AZ-Unterstützung in Amazon Relational Database Service (Amazon RDS) bietet eine verbesserte Verfügbarkeit und Beständigkeit von Datenbank-Instances. Wenn Sie eine Multi-AZ-Datenbank-Instance bereitstellen, erstellt Amazon RDS automatisch eine primäre Datenbank-Instance und repliziert die Daten synchron auf eine Standby-Instance in einer anderen Availability Zone. Jede Availability Zone läuft auf einer eigenen, physisch getrennten, unabhängigen Infrastruktur und ist auf eine hohe Verfügbarkeit ausgelegt. Im Falle eines Infrastrukturausfalls führt Amazon RDS einen automatis

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			chen Failover zum Standby-Modus durch, sodass Sie den Datenbankbetrieb wieder aufnehmen können, sobald der Failover abgeschlo ssen ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CP-10	Die Organisation sorgt dafür, dass das Informationssystem nach einer Unterbrechung, einer Beeinträchtigung oder einem Ausfall wiederhergestellt und wieder in einen bekannten Zustand versetzt wird.	s-3 bucket-versioning-enabled	Die Versionsverwaltung von Amazon Simple Storage Service (Amazon S3)-Buckets hilft dabei, mehrere Varianten eines Objekts im selben Amazon-S3-Bucket zu speichern. Verwenden Sie die Versionsverwaltung, um sämtliche Versionen aller Objekte in Ihrem Amazon-S3-Bucket zu speichern, abzurufen oder wiederherzustellen. Mit der Versionsverwaltung können Sie Versionen sowohl nach unbeabsichtigten Benutzeraktionen als auch nach Anwendungsfehlern problemlos wiederherstellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CP-10	Die Organisation sorgt dafür, dass das Informationssystem nach einer Unterbrechung, einer Beeinträchtigung oder einem Ausfall wiederhergestellt und wieder in einen bekannten Zustand versetzt wird.	db-instance-backup-enabled	Die Sicherungsfunktion von Amazon RDS erstellt Sicherungen Ihrer Datenbanken und Transaktionsprotokolle. Amazon RDS erstellt einen Snapshot für das Speichervolume Ihrer DB-Instance, sodass die gesamte DB-Instance gesichert wird. Sie können im System spezifische Aufbewahrungsfristen festlegen, um Ihre Ausfallsicherheitsanforderungen zu erfüllen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CP-10	Die Organisation sorgt dafür, dass das Informationssystem nach einer Unterbrechung, einer Beeinträchtigung oder einem Ausfall wiederhergestellt und wieder in einen bekannten Zustand versetzt wird.	dynamodb-pitr-enabled	Aktivieren Sie diese Regel, um zu überprüfen, ob die Informationen gesichert wurden. Es verwaltet auch die Backups, indem es sicherstellt, dass die point-in-time Wiederherstellung in Amazon DynamoDB aktiviert ist. Bei der Wiederherstellung werden fortlaufende Backups Ihrer Tabelle für die letzten 35 Tage gespeichert.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CP-10	Die Organisation sorgt dafür, dass das Informationssystem nach einer Unterbrechung, einer Beeinträchtigung oder einem Ausfall wiederhergestellt und wieder in einen bekannten Zustand versetzt wird.	elasticache-redis-cluster-automatic-Backup-Check	Wenn automatische Backups aktiviert sind, ElastiCache erstellt Amazon täglich ein Backup des Clusters. Die Sicherung kann für eine von Ihrer Organisation festgelegte Anzahl von Tagen aufbewahrt werden. Automatische Backups schützen vor Datenverlust. Bei einem Ausfall können Sie einen neuen Cluster erstellen, der Ihre Daten aus dem aktuellen Backup wiederherstellt.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CP-10	Die Organisation sorgt dafür, dass das Informationssystem nach einer Unterbrechung, einer Beeinträchtigung oder einem Ausfall wiederhergestellt und wieder in einen bekannten Zustand versetzt wird.	elb-deletion-protection-enabled	Diese Regel sorgt dafür, dass der Löschschutz für Elastic Load Balancing aktiviert ist. Verwenden Sie diese Funktion, um zu verhindern, dass Ihr Load Balancer versehentlich oder böswillig gelöscht wird, was zum Verlust der Verfügbarkeit Ihrer Anwendungen führen kann.
CP-10	Die Organisation sorgt dafür, dass das Informationssystem nach einer Unterbrechung, einer Beeinträchtigung oder einem Ausfall wiederhergestellt und wieder in einen bekannten Zustand versetzt wird.	s-3 bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) unterstützt die Aufrechterhaltung einer angemessenen Kapazität und Verfügbarkeit. CRR ermöglicht das automatische, asynchrone Kopieren von Objekten in Amazon-S3-Buckets, um die Datenverfügbarkeit sicherzustellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CP-10	Die Organisation sorgt dafür, dass das Informationssystem nach einer Unterbrechung, einer Beeinträchtigung oder einem Ausfall wiederhergestellt und wieder in einen bekannten Zustand versetzt wird.	vpc-vpn-2-tunnels-up	Redundante Site-to-Site VPN-Tunnel können implementiert werden, um die Anforderungen an die Ausfallsicherheit zu erfüllen. Es verwendet zwei Tunnel, um die Konnektivität sicherzustellen, falls eine der Site-to-Site VPN-Verbindungen nicht verfügbar ist. Um sich vor einem Verbindungsverlust zu schützen, können Sie für den Fall, dass Ihr Kunden-Gateway nicht verfügbar ist, eine zweite Site-to-Site VPN-Verbindung zu Ihrer Amazon Virtual Private Cloud (Amazon VPC) und Ihrem Virtual Private Gateway einrichten, indem Sie ein zweites Kunden-Gateway verwenden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CP-10	Die Organisation sorgt dafür, dass das Informationssystem nach einer Unterbrechung, einer Beeinträchtigung oder einem Ausfall wiederhergestellt und wieder in einen bekannten Zustand versetzt wird.	elb-cross-zone-load-Balancing aktiviert	Aktivieren Sie zonenübergreifendes Load Balancing für Ihre Elastic Load Balancer (ELBs), um eine angemessene Kapazität und Verfügbarkeit aufrechtzuerhalten. Zonenübergreifendes Load Balancing reduziert die Notwendigkeit, die gleiche Anzahl von Instances in jeder aktivierten Availability Zone aufrechtzuerhalten. Es verbessert auch die Fähigkeit Ihrer Anwendung, den Verlust einer oder mehrerer Instances zu bewältigen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CP-10	Die Organisation sorgt dafür, dass das Informationssystem nach einer Unterbrechung, einer Beeinträchtigung oder einem Ausfall wiederhergestellt und wieder in einen bekannten Zustand versetzt wird.	ebs-optimized-instance	Eine optimierte Instance im Amazon Elastic Block Store (Amazon EBS) bietet zusätzliche, dedizierte Kapazität für Amazon-EBS-I/O-Vorgänge. Diese Optimierung bietet die beste Leistung für Ihr EBS-Volume, indem Konflikte zwischen Amazon-EBS-I/O und anderem Datenverkehr von Ihrer Instance minimiert werden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CP-10	Die Organisation sorgt dafür, dass das Informationssystem nach einer Unterbrechung, einer Beeinträchtigung oder einem Ausfall wiederhergestellt und wieder in einen bekannten Zustand versetzt wird.	redshift-backup-enabled	Stellen Sie zur Unterstützung der Datensicherungsprozesse sicher, dass Ihre Amazon-Redshift-Cluster über automatisierte Snapshots verfügen. Wenn automatisierte Snapshots für einen Cluster aktiviert sind, erstellt Redshift in regelmäßigen Abständen Snapshots dieses Clusters. Standardmäßig erzeugt Redshift ungefähr alle acht Stunden oder nach 5 GB geänderten Daten pro Knoten einen Snapshot, je nachdem, was zuerst auftritt.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CP-10	Die Organisation sorgt dafür, dass das Informationssystem nach einer Unterbrechung, einer Beeinträchtigung oder einem Ausfall wiederhergestellt und wieder in einen bekannten Zustand versetzt wird.	backup-plan-min-frequency-and-min-retention-check	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihr AWS Backup-Plan auf eine Mindestfrequenz und Aufbewahrung festgelegt ist. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen. Mit dieser Regel können Sie die Parameter requiredFrequencyValue (Config default: 1), requiredRetentionDays (Config default: 35) und requiredFrequencyUnit

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			(Config default: days) festlegen. Der tatsächliche Wert muss den Anforderungen Ihrer Organisation entsprechen.
CP-10	Die Organisation sorgt dafür, dass das Informationssystem nach einer Unterbrechung, einer Beeinträchtigung oder einem Ausfall wiederhergestellt und wieder in einen bekannten Zustand versetzt wird.	fsx-resources-protected-by-Backup-Plan	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre FSx Amazon-Dateisysteme Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CP-10	Die Organisation sorgt dafür, dass das Informationssystem nach einer Unterbrechung, einer Beeinträchtigung oder einem Ausfall wiederhergestellt und wieder in einen bekannten Zustand versetzt wird.	ec2--Plan resources-protected-by-backup	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon Elastic Compute Cloud (Amazon EC2) -Ressourcen Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CP-10	Die Organisation sorgt dafür, dass das Informationssystem nach einer Unterbrechung, einer Beeinträchtigung oder einem Ausfall wiederhergestellt und wieder in einen bekannten Zustand versetzt wird.	aurora-resources-protected-by-Backup-Plan	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon Aurora Aurora-Ressourcen Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CP-10	Die Organisation sorgt dafür, dass das Informationssystem nach einer Unterbrechung, einer Beeinträchtigung oder einem Ausfall wiederhergestellt und wieder in einen bekannten Zustand versetzt wird.	dynamodb-resources-protected-by-Backup-Plan	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon DynamoDB DynamoDB-Ressourcen Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CP-10	Die Organisation sorgt dafür, dass das Informationssystem nach einer Unterbrechung, einer Beeinträchtigung oder einem Ausfall wiederhergestellt und wieder in einen bekannten Zustand versetzt wird.	ebs-resources-protected-by-Backup-Plan	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon Elastic Block Store (Amazon EBS) -Ressourcen Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CP-10	Die Organisation sorgt dafür, dass das Informationssystem nach einer Unterbrechung, einer Beeinträchtigung oder einem Ausfall wiederhergestellt und wieder in einen bekannten Zustand versetzt wird.	efs-resources-protected-by-Backup-Plan	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon Elastic File System (Amazon EFS) -Dateisysteme Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CP-10	Die Organisation sorgt dafür, dass das Informationssystem nach einer Unterbrechung, einer Beeinträchtigung oder einem Ausfall wiederhergestellt und wieder in einen bekannten Zustand versetzt wird.	rds-resources-protected-by-Backup-Plan	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon Relational Database Service (Amazon RDS) -Ressourcen Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CP-9(b)	Die Organisation: b. Führt Backups der im Informationssystem enthaltenen Informationen auf Systemebene durch (inkrementelles Backup täglich; vollständiges Backup wöchentlich).	db-instance-backup-enabled	Die Sicherungsfunktion von Amazon RDS erstellt Sicherungen Ihrer Datenbanken und Transaktionsprotokolle. Amazon RDS erstellt einen Snapshot für das Speichervolume Ihrer DB-Instance, sodass die gesamte DB-Instance gesichert wird. Sie können im System spezifische Aufbewahrungsfristen festlegen, um Ihre Ausfallsicherheitsanforderungen zu erfüllen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CP-9(b)	Die Organisation: b. Führt Backups der im Informationssystem enthaltenen Informationen auf Systemebene durch (inkrementelles Backup täglich; vollständiges Backup wöchentlich).	dynamodb-pitr-enabled	Aktivieren Sie diese Regel, um zu überprüfen, ob die Informationen gesichert wurden. Es verwaltet auch die Backups, indem es sicherstellt, dass die point-in-time Wiederherstellung in Amazon DynamoDB aktiviert ist. Bei der Wiederherstellung werden fortlaufende Backups Ihrer Tabelle für die letzten 35 Tage gespeichert.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CP-9(b)	Die Organisation: b. Führt Backups der im Informationssystem enthaltenen Informationen auf Systemebene durch (inkrementelles Backup täglich; vollständiges Backup wöchentlich).	elasticache-redis-cluster-automatic-Backup-Check	Wenn automatische Backups aktiviert sind, ElastiCache erstellt Amazon täglich ein Backup des Clusters. Die Sicherung kann für eine von Ihrer Organisation festgelegte Anzahl von Tagen aufbewahrt werden. Automatische Backups schützen vor Datenverlust. Bei einem Ausfall können Sie einen neuen Cluster erstellen, der Ihre Daten aus dem aktuellen Backup wiederherstellt.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CP-9(b)	Die Organisation: b. Führt Backups der im Informationssystem enthaltenen Informationen auf Systemebene durch (inkrementelles Backup täglich; vollständiges Backup wöchentlich).	s-3 bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) unterstützt die Aufrechterhaltung einer angemessenen Kapazität und Verfügbarkeit. CRR ermöglicht das automatische, asynchrone Kopieren von Objekten in Amazon-S3-Buckets, um die Datenverfügbarkeit sicherzustellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CP-9(b)	Die Organisation: b. Führt Backups der im Informationssystem enthaltenen Informationen auf Systemebene durch (inkrementelles Backup täglich; vollständiges Backup wöchentlich).	redshift-backup-enabled	Stellen Sie zur Unterstützung der Datensicherungsprozesse sicher, dass Ihre Amazon-Redshift-Cluster über automatisierte Snapshots verfügen. Wenn automatisierte Snapshots für einen Cluster aktiviert sind, erstellt Redshift in regelmäßigen Abständen Snapshots dieses Clusters. Standardmäßig erzeugt Redshift ungefähr alle acht Stunden oder nach 5 GB geänderten Daten pro Knoten einen Snapshot, je nachdem, was zuerst auftritt.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CP-9(b)	Die Organisation: b. Führt Backups der im Informationssystem enthaltenen Informationen auf Systemebene durch (inkrementelles Backup täglich; vollständiges Backup wöchentlich).	s-3 bucket-versioning-enabled	Die Versionsverwaltung von Amazon Simple Storage Service (Amazon S3)-Buckets hilft dabei, mehrere Varianten eines Objekts im selben Amazon-S3-Bucket zu speichern. Verwenden Sie die Versionsverwaltung, um sämtliche Versionen aller Objekte in Ihrem Amazon-S3-Bucket zu speichern, abzurufen oder wiederherzustellen. Mit der Versionsverwaltung können Sie Versionen sowohl nach unbeabsichtigten Benutzeraktionen als auch nach Anwendungsfehlern problemlos wiederherstellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CP-9(b)	Die Organisation: b. Führt Backups der im Informationssystem enthaltenen Informationen auf Systemebene durch (inkrementelles Backup täglich; vollständiges Backup wöchentlich).	backup-plan-min-frequency-and-min-retention-check	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihr AWS Backup-Plan auf eine Mindestfrequenz und Aufbewahrung festgelegt ist. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen. Mit dieser Regel können Sie die Parameter requiredFrequencyValue (Config default: 1), requiredRetentionDays (Config default: 35) und requiredFrequencyUnit

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			(Config default: days) festlegen. Der tatsächliche Wert muss den Anforderungen Ihrer Organisation entsprechen.
CP-9(b)	Die Organisation: b. Führt Backups der im Informationssystem enthaltenen Informationen auf Systemebene durch (inkrementelles Backup täglich; vollständiges Backup wöchentlich).	fsx-resources-protected-by-Backup-Plan	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre FSx Amazon-Dateisysteme Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CP-9(b)	Die Organisation: b. Führt Backups der im Informationssystem enthaltenen Informationen auf Systemebene durch (inkrementelles Backup täglich; vollständiges Backup wöchentlich).	ec2--Plan resources-protected-by-backup	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon Elastic Compute Cloud (Amazon EC2) -Ressourcen Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CP-9(b)	Die Organisation: b. Führt Backups der im Informationssystem enthaltenen Informationen auf Systemebene durch (inkrementelles Backup täglich; vollständiges Backup wöchentlich).	aurora-resources-protected-by-Backup-Plan	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon Aurora Aurora-Ressourcen Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CP-9(b)	Die Organisation: b. Führt Backups der im Informationssystem enthaltenen Informationen auf Systemebene durch (inkrementelles Backup täglich; vollständiges Backup wöchentlich).	dynamodb-resources-protected-by-Backup-Plan	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon DynamoDB DynamoDB-Ressourcen Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CP-9(b)	Die Organisation: b. Führt Backups der im Informationssystem enthaltenen Informationen auf Systemebene durch (inkrementelles Backup täglich; vollständiges Backup wöchentlich).	ebs-resources-protected-by-Backup-Plan	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon Elastic Block Store (Amazon EBS) -Ressourcen Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CP-9(b)	Die Organisation: b. Führt Backups der im Informationssystem enthaltenen Informationen auf Systemebene durch (inkrementelles Backup täglich; vollständiges Backup wöchentlich).	efs-resources-protected-by-Backup-Plan	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon Elastic File System (Amazon EFS) -Dateisysteme Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CP-9(b)	Die Organisation: b. Führt Backups der im Informationssystem enthaltenen Informationen auf Systemebene durch (inkrementelles Backup täglich; vollständiges Backup wöchentlich).	rds-resources-protected-by-Backup-Plan	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon Relational Database Service (Amazon RDS) -Ressourcen Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
IA-2	Das Informati onssystem nimmt eine eindeutige Identifizierung und Authentifizierung der Benutzer (oder Prozesse, die im Namen von Benutzern der Organisation handeln) vor.	iam-password-policy	Die Identitäten und Anmeldeinformation en werden auf der Grundlage einer organisatorischen IAM-Passwortrichtlinie ausgestellt, verwaltet und verifiziert. Sie erfüllen oder übertreff en die Anforderu ngen von NIST SP 800-63 und dem Standard „Best Practices“ von AWS Foundational Security für die Sicherheit von Passwörtern. Mit dieser Regel können Sie optional RequireUppercaseCh aracters (Wert für AWS grundlegende Sicherheitsbewährt e Methoden: wahr), RequireLowercaseCh aracters (Wert für bewährte Methoden für AWS grundlege nde Sicherheit: wahr), RequireSy mbols (Wert für bewährte Methoden für AWS grundlege

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			nde Sicherheit: wahr), RequireNumbers (Wert für bewährte Methoden für AWS grundlegende Sicherheit: wahr), MinimumPasswordLength (Wert für bewährte Methoden für AWS grundlegende Sicherheit: 14), PasswordReusePrevention (Wert für bewährte Methoden für AWS grundlegende Sicherheit: 24) und MaxPasswordAge (Wert für bewährte Methoden für AWS grundlegende Sicherheit: 90) für Ihr IAM festlegen Kennwortrichtlinie. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
IA-2	Das Informati onssystem nimmt eine eindeutige Identifizierung und Authentifizierung der Benutzer (oder Prozesse, die im Namen von Benutzern der Organisation handeln) vor.	iam-root-access-key-überprüfen	Der Zugriff auf Systeme und Ressourcen kann gesteuert werden, indem überprüft wird, ob der Root-Benu tzer keine Zugriffss chlüssel mit seiner AWS Identity and Access Management (IAM) -Rolle verknüpft hat. Stellen Sie sicher, dass die Root-Zugr iffsschlüssel gelöscht werden. Erstellen und verwenden Sie stattdessen rollenbas ierte AWS Konten, um dem Prinzip der geringsten Funktiona lität Rechnung zu tragen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
IA-2(1)	(1) Das Informati onssystem implement iert eine Multi-Fak tor-Authentifizierung für den Netzwerkz ugriff auf privilegierte Konten.	iam-user-mfa-enabled	Aktivieren Sie diese Regel, um den Zugriff auf Ressourcen in der AWS Cloud einzuschr änken. Diese Regel stellt sicher, dass die Multi-Faktor-Authe ntifizierung (MFA) für alle IAM-Benut zer aktiviert ist. MFA bietet eine weitere Schutzebene zusätzlic h zum Benutzern amen und Passwort. Reduzieren Sie Fälle von kompromittierten Konten, indem Sie MFA für IAM-Benutzer vorschreiben.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
IA-2(1)	(1) Das Informationssystem implementiert eine Multi-Faktor-Authentifizierung für den Netzwerkzugriff auf privilegierte Konten.	mfa-enabled-for-iam-Konsolenzugriff	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass MFA für alle AWS Identity and Access Management (IAM) -Benutzer aktiviert ist, die über ein Konsolenkennwort verfügen. MFA bietet eine weitere Schutzebene zusätzlich zum Benutzernamen und Passwort. Indem Sie MFA für IAM-Benutzer vorschreiben, können Sie Vorfälle kompromittierter Konten reduzieren und verhindern, dass unbefugte Benutzer auf vertrauliche Daten zugreifen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
IA-2(1)(2)	(1) Das Informationssystem implementiert eine Multi-Faktor-Authentifizierung für den Netzwerkzugriff auf privilegierte Konten. (1) Das Informationssystem implementiert eine Multifaktor-Authentifizierung für den Netzwerkzugriff auf nicht privilegierte Konten.	mfa-enabled-for-iam-Konsolenzugriff	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass MFA für alle AWS Identity and Access Management (IAM) -Benutzer aktiviert ist, die über ein Konsolenkennwort verfügen. MFA bietet eine weitere Schutzebene zusätzlich zum Benutzernamen und Passwort. Indem Sie MFA für IAM-Benutzer vorschreiben, können Sie Vorfälle kompromittierter Konten reduzieren und verhindern, dass unbefugte Benutzer auf vertrauliche Daten zugreifen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
IA-2(1)(2)	(1) Das Informationssystem implementiert eine Multi-Faktor-Authentifizierung für den Netzwerkzugriff auf privilegierte Konten. (1) Das Informationssystem implementiert eine Multifaktor-Authentifizierung für den Netzwerkzugriff auf nicht privilegierte Konten.	iam-user-mfa-enabled	Aktivieren Sie diese Regel, um den Zugriff auf Ressourcen in der Cloud einzuschränken. AWS Diese Regel stellt sicher, dass die Multi-Faktor-Authentifizierung (MFA) für alle IAM-Benutzer aktiviert ist. MFA bietet eine weitere Schutzebene zusätzlich zum Benutzernamen und Passwort. Reduzieren Sie Fälle von kompromittierten Konten, indem Sie MFA für IAM-Benutzer vorschreiben.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
IA-5(1)(a)(d)(e)	Das Informati onssystem ergreift für die passwortgestützte Authentifizierung folgende Maßnahmen : a. Es erzwingt eine Mindestkomplexität von [Zuweisung: vom Unternehm en festgelegte Anforderungen an Groß- und Kleinschr eibung, Zeichenan zahl, Kombinati on aus Groß- und Kleinbuchstaben, Zahlen und Sonderzei chen, einschlie ßlich Mindestan forderungen für jeden Typ]; d. Es erzwingt die minimale und maximale Gültigkeitsdauer von Passwörtern von [Zuweisung: von der Organisat ion festgelegte Frist für die minimale und maximale Gültigkeitsdauer]; e. Verbietet die Wiederverwendung	iam-password-policy	Die Identitäten und Anmeldeinformation en werden auf der Grundlage einer organisatorischen IAM-Passwortrichtlinie ausgestellt, verwaltet und verifiziert. Sie erfüllen oder übertreff en die Anforderungen von NIST SP 800-63 und dem Standard „Best Practices“ von AWS Foundatio nal Security für die Passwortstärke. Mit dieser Regel können Sie optional RequireUppercaseCh aracters (Wert für AWS grundlegende Sicherheitsbewährt e Methoden: wahr), RequireLowercaseCh aracters (Wert für bewährte Methoden für AWS grundlege nde Sicherheit: wahr), RequireSy mbols (Wert für bewährte Methoden für AWS grundlege nde Sicherheit:

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	von Passwörtern für die nächsten 24 Generationen.		wahr), RequireNumbers (Wert für bewährte Methoden für AWS grundlegende Sicherheit: wahr), MinimumPasswordLength (Wert für bewährte Methoden für AWS grundlegende Sicherheit: 14), PasswordReusePrevention (Wert für bewährte Methoden für AWS grundlegende Sicherheit: 24) und MaxPasswordAge (Wert für bewährte Methoden für AWS grundlegende Sicherheit: 90) für Ihr IAM festlegen Kennwortrichtlinie. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
IA-5(4)	Die Organisation verwendet automatisierte Tools, um festzustellen, ob Passwortauthentifikatoren stark genug sind, um [Zuweisung: von der Organisation definierte Anforderungen] zu erfüllen.	iam-password-policy	Die Identitäten und Anmeldeinformationen werden auf der Grundlage einer organisatorischen IAM-Passwortrichtlinie ausgestellt, verwaltet und verifiziert. Sie erfüllen oder übertreffen die Anforderungen des NIST SP 800-63 und des AWS Foundational Security Best Practices-Standards für Passwortstärke. Mit dieser Regel können Sie optional RequireUppercaseCharacters (Wert für AWS grundlegende Sicherheitsbewährte Methoden: wahr), RequireLowercaseCharacters (Wert für bewährte Methoden für AWS grundlegende Sicherheit: wahr), RequireSymbols (Wert für bewährte Methoden für AWS grundlegende Sicherheit:

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			wahr), RequireNumbers (Wert für bewährte Methoden für AWS grundlegende Sicherheit: wahr), MinimumPasswordLength (Wert für bewährte Methoden für AWS grundlegende Sicherheit: 14), PasswordReusePrevention (Wert für bewährte Methoden für AWS grundlegende Sicherheit: 24) und MaxPasswordAge (Wert für bewährte Methoden für AWS grundlegende Sicherheit: 90) für Ihr IAM festlegen Kennwortrichtlinie. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
IA-5(7)	Die Organisation stellt sicher, dass unverschlüsselte statische Authentifikatoren nicht in Anwendungen oder Zugriffsskripts eingebettet oder in Funktionsschlüsseln gespeichert werden.	codebuild-project-envvar-awscred-überprüfen	Stellen Sie sicher, dass die Anmeldeinformationen AWS_ACCESS_KEY_ID AWS_SECRET_ACCESS_KEY nicht in AWS Codebuild-Projektumgebungen vorhanden sind. Speichern Sie diese Variablen nicht als Klartext. Das Speichern dieser Variablen als Klartext bewirkt eine unbeabsichtigte Offenlegung von Daten sowie unberechtigte Zugriffe.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
IR-4(1)	Die Organisation setzt automatisierte Mechanismen ein, um die Bearbeitung von Sicherheitsvorfällen zu unterstützen.	cloudwatch-alarm-action-check	Amazon CloudWatch alarmiert, wenn eine Metrik den Schwellenwert für eine bestimmte Anzahl von Bewertungszeiträumen überschreitet. Der Alarm führt eine oder mehrere Aktionen durch, die vom Wert der Metrik oder des Ausdrucks im Vergleich zu einem Schwellenwert in einer Reihe von Zeiträumen abhängt. Diese Regel erfordert einen Wert für alarmActionRequired (Config Default: True), insufficientDataAction Required (Config Default: True), okActionRequired (Config Default: False). Der tatsächliche Wert muss die Alarmaktionen für Ihre Umgebung widerspiegeln.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
IR-4(1)	Die Organisation setzt automatisierte Mechanismen ein, um die Bearbeitung von Sicherheitsvorfällen zu unterstützen.	guardduty-non-archived-findings	Amazon GuardDuty hilft Ihnen dabei, die Auswirkungen eines Vorfalls zu verstehen, indem es die Ergebnisse nach Schweregrad klassifiziert: niedrig, mittel und hoch. Diese Klassifizierungen können Sie zur Festlegung von entsprechenden Strategien und Prioritäten zur Behebung solcher Vorfälle verwenden. Mit dieser Regel können Sie optional daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7) und daysHighSev (Config Default: 1) für nicht archivierte Ergebnisse festlegen, wie es die Richtlinien Ihrer Organisation erfordern.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
IR-4(1)	Die Organisation setzt automatisierte Mechanismen ein, um die Bearbeitung von Sicherheitsvorfällen zu unterstützen.	autoscaling-group-elb-healthcheck-erforderlich	Die Elastic Load Balancer (ELB) - Zustandsprüfungen für Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling Scaling-Gruppen unterstützen die Aufrechterhaltung einer angemessenen Kapazität und Verfügbarkeit. Der Load Balancer sendet regelmäßig Pings, versucht Verbindungen herzustellen oder sendet Anfragen, um den Zustand der EC2 Amazon-Instances in einer Gruppe mit auto-scaling zu testen. Wenn eine Instance nicht zurückmeldet, wird der Traffic an eine neue EC2 Amazon-Instance gesendet.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
IR-4(1)	Die Organisation setzt automatisierte Mechanismen ein, um die Bearbeitung von Sicherheitsvorfällen zu unterstützen.	guardduty-enabled-centralized	Amazon GuardDuty kann mithilfe von Threat Intellige nce Feeds helfen, potenzielle Cybersich erheitsereignisse zu überwachen und zu erkennen. Dazu gehören Listen mit bösartigen IPs und maschinel len Lernmethoden zur Identifizierung unerwarteter, nicht autorisierter und bösartiger Aktivitäten in Ihrer AWS Cloud-Umgebung.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
IR-4(1)	Die Organisation setzt automatisierte Mechanismen ein, um die Bearbeitung von Sicherheitsvorfällen zu unterstützen.	securityhub-enabled	AWS Security Hub hilft bei der Überwachung von unbefugtem Personal, Verbindungen, Geräten und Software. AWS Security Hub aggregiert, organisiert und priorisiert die Sicherheitswarnungen oder Ergebnisse mehrerer Dienste. AWS Einige dieser Dienste sind Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer und AWS Firewall Manager sowie AWS Partnerlösungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
IR-6(1)	Die Organisation setzt automatisierte Mechanismen ein, um die Meldung von Sicherheitsvorfällen zu unterstützen.	guardduty-non-archived-findings	Amazon GuardDuty hilft Ihnen dabei, die Auswirkungen eines Vorfalls zu verstehen, indem es die Ergebnisse nach Schweregrad klassifiziert: niedrig, mittel und hoch. Diese Klassifizierungen können Sie zur Festlegung von entsprechenden Strategien und Prioritäten zur Behebung solcher Vorfälle verwenden. Mit dieser Regel können Sie optional daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7) und daysHighSev (Config Default: 1) für nicht archivierte Ergebnisse festlegen, wie es die Richtlinien Ihrer Organisation erfordern.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
IR-6(1)	Die Organisation setzt automatisierte Mechanismen ein, um die Meldung von Sicherheitsvorfällen zu unterstützen.	guardduty-enabled-centralized	Amazon GuardDuty kann mithilfe von Threat Intellige nce Feeds helfen, potenzielle Cybersich erheitsereignisse zu überwachen und zu erkennen. Dazu gehören Listen mit bösartigen IPs und maschinel len Lernmethoden zur Identifizierung unerwarteter, nicht autorisierter und bösartiger Aktivitäten in Ihrer AWS Cloud-Umgebung.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
IR-6(1)	Die Organisation setzt automatisierte Mechanismen ein, um die Meldung von Sicherheitsvorfällen zu unterstützen.	securityhub-enabled	AWS Security Hub hilft bei der Überwachung von unbefugtem Personal, Verbindungen, Geräten und Software. AWS Security Hub aggregiert, organisiert und priorisiert die Sicherheitswarnungen oder Ergebnisse mehrerer Dienste. AWS Einige dieser Dienste sind Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer und AWS Firewall Manager sowie AWS Partnerlösungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
IR-7(1)	Die Organisation setzt automatisierte Mechanismen ein, um die Verfügbarkeit von Informationen und Unterstützung im Zusammenhang mit der Reaktion auf Vorfälle zu erhöhen.	guardduty-non-archived-findings	Amazon GuardDuty hilft Ihnen dabei, die Auswirkungen eines Vorfalls zu verstehen, indem es die Ergebnisse nach Schweregrad klassifiziert: niedrig, mittel und hoch. Diese Klassifizierungen können Sie zur Festlegung von entsprechenden Strategien und Prioritäten zur Behebung solcher Vorfälle verwenden. Mit dieser Regel können Sie optional daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7) und daysHighSev (Config Default: 1) für nicht archivierte Ergebnisse festlegen, wie es die Richtlinien Ihrer Organisation erfordern.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
IR-7(1)	Die Organisation setzt automatisierte Mechanismen ein, um die Verfügbarkeit von Informationen und Unterstützung im Zusammenhang mit der Reaktion auf Vorfälle zu erhöhen.	guardduty-enabled-centralized	Amazon GuardDuty kann mithilfe von Threat Intellige nce Feeds helfen, potenzielle Cybersich erheitsereignisse zu überwachen und zu erkennen. Dazu gehören Listen mit bösartigen IPs und maschinel len Lernmethoden zur Identifizierung unerwarteter, nicht autorisierter und bösartiger Aktivitäten in Ihrer AWS Cloud-Umgebung.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
IR-7(1)	Die Organisation setzt automatisierte Mechanismen ein, um die Verfügbarkeit von Informationen und Unterstützung im Zusammenhang mit der Reaktion auf Vorfälle zu erhöhen.	securityhub-enabled	AWS Security Hub hilft bei der Überwachung von unbefugtem Personal, Verbindungen, Geräten und Software. AWS Security Hub aggregiert, organisiert und priorisiert die Sicherheitswarnungen oder Ergebnisse mehrerer Dienste. AWS Einige dieser Dienste sind Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer und AWS Firewall Manager sowie AWS Partnerlösungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
RA-5	Die Organisation: a. Sucht nach Sicherheitslücken im Informationssystem und in gehosteten Anwendungen [Zuordnung: Von der Organisation festgelegte Häufigkeit and/or randomly in accordance with organization-defined process] and when new vulnerabilities potentially affecting the system/applications der Identifizierung und Meldung; b. Wendet Tools und Techniken zum Scannen von Schwachstellen an, die die Interoperabilität zwischen den Tools erleichtern und Teile des Schwachstellenmanagements automatisieren, indem für folgende Aktivitäten Standards angewendet werden: 1. Aufzählung von Plattformen, Softwaref	guardduty-enabled-centralized	Amazon GuardDuty kann mithilfe von Threat Intelligence Feeds helfen, potenzielle Cybersicherheitsereignisse zu überwachen und zu erkennen. Dazu gehören Listen mit bösartigen IPs und maschinellen Lernmethoden zur Identifizierung unerwarteter, nicht autorisierter und bösartiger Aktivitäten in Ihrer AWS Cloud-Umgebung.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	ehlern und ungeeigneten Konfigurationen; 2. Formatierung von Checklisten und Testverfahren; und 3. Messung der Auswirkungen von Schwachstellen; c. Analysiert Scanberichte über Schwachstellen und Ergebnisse von Sicherheitskontrollbewertungen; d. Behebt legitime Schwachstellen [Zuweisung: von der Organisation festgelegte Reaktionszeiten] gemäß einer Risikobewertung der Organisation; und e. Leitet die Informationen aus dem Schwachstellenscan und den Sicherheitskontrollbewertungen an [Zuweisung: von der Organisation ernanntes Personal oder definierte Rollen] weiter, um ähnliche Schwachstellen in anderen Informationssystemen (d. h.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	Systemschwächen oder -mängel) zu beseitigen.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
RA-5	Die Organisation: a. Monatliche Scans nach Sicherheitslücken im Informationssystem und in den gehosteten Anwendungen [Betrieb system/infrastructure; monthly web applications and databases] and when new vulnerabilities potentially affecting the system/applications werden identifiziert und gemeldet; b. Wendet Tools und Techniken zum Scannen von Schwachstellen an, die die Interoperabilität zwischen den Tools erleichtern und Teile des Schwachstellenmanagements automatisieren, indem für folgende Aktivitäten Standards angewendet werden: 1. Aufzählung von Plattformen, Softwarefehlern und ungeeigneten Konfigurationen;	guardduty-non-archived-findings	Amazon GuardDuty hilft Ihnen dabei, die Auswirkungen eines Vorfalls zu verstehen, indem es die Ergebnisse nach Schweregrad klassifiziert: niedrig, mittel und hoch. Diese Klassifizierungen können Sie zur Festlegung von entsprechenden Strategien und Prioritäten zur Behebung solcher Vorfälle verwenden. Mit dieser Regel können Sie optional daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7) und daysHighSev (Config Default: 1) für nicht archivierte Ergebnisse festlegen, wie es die Richtlinien Ihrer Organisation erfordern.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	2. Formatierung von Checklisten und Testverfahren; und 3. Messung der Auswirkungen von Schwachstellen; c. Analysiert Scanberichte über Schwachstellen und Ergebnisse von Sicherheitskontrollbewertungen; d. Behebt legitime Schwachstellen: Schwachstellen mit hohem Risiko, die innerhalb von dreißig (30) Tagen ab ihrer Feststellung behoben werden; Schwachstellen mit mäßigem Risiko, die innerhalb von neunzig (90) Tagen ab ihrer Feststellung behoben werden; Sicherheitslücken mit geringem Risiko, die innerhalb von einhundertachtzig (180) Tagen ab ihrer Feststellung behoben werden, gemäß einer Risikobewertung der Organisation; und e. Leitet die Informati		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	onen aus dem Schwachstellenscan und den Sicherhei tskontrollbewertun gen an [Zuweisung: von der Organisation ernanntes Personal oder definierte Rollen] weiter, um ähnliche Schwachstellen in anderen Informati onssystemen (d. h. Systemschwächen oder -mängel) zu beseitigen.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SA-10	Die Organisation verlangt von den Entwicklern des Informationssystems, der Systemkomponente oder des Informationssystemservices: a. Die Durchführung des Konfigurationsmanagements während der Entwicklung, Implementierung und des Betriebs von Systemen, Komponenten oder Services; b. Die Dokumentation, Verwaltung und Kontrolle der Integrität von Änderungen an [Zuweisung: von der Organisation definierte Konfigurationselemente im Rahmen der Konfigurationsverwaltung]; c. Die Implementierung von ausschließlich von der Organisation genehmigten Änderungen am System, der	guardduty-enabled-centralized	Amazon GuardDuty kann mithilfe von Threat Intelligence Feeds helfen, potenzielle Cybersicherheitsereignisse zu überwachen und zu erkennen. Dazu gehören Listen mit bösartigen IPs und maschinellen Lernmethoden zur Identifizierung unerwarteter, nicht autorisierter und bösartiger Aktivitäten in Ihrer AWS Cloud-Umgebung.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	Komponente oder dem Service; d. Die Dokumentation von genehmigten Änderungen am System, der Komponente oder dem Service sowie der potenziellen Auswirkungen solcher Änderungen auf die Sicherheit; und e. Die Überwachung von Sicherheitslücken und deren Behebung innerhalb des Systems, der Komponente oder des Services und die Meldung der Ergebnisse an [Zuweisung: von der Organisation ernanntes Personal].		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SA-10	Die Organisation verlangt von den Entwicklern des Informationssystems, der Systemkomponente oder des Informationssystemservices: a. Die Durchführung des Konfigurationsmanagements während der Entwicklung, Implementierung und des Betriebs von Systemen, Komponenten oder Services; b. Die Dokumentation, Verwaltung und Kontrolle der Integrität von Änderungen an [Zuweisung: von der Organisation definierte Konfigurationselemente im Rahmen der Konfigurationsverwaltung]; c. Die Implementierung von ausschließlich von der Organisation genehmigten Änderungen am System, der	guardduty-non-archived-findings	Amazon GuardDuty hilft Ihnen dabei, die Auswirkungen eines Vorfalls zu verstehen, indem es die Ergebnisse nach Schweregrad klassifiziert: niedrig, mittel und hoch. Diese Klassifizierungen können Sie zur Festlegung von entsprechenden Strategien und Prioritäten zur Behebung solcher Vorfälle verwenden. Mit dieser Regel können Sie optional daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7) und daysHighSev (Config Default: 1) für nicht archivierte Ergebnisse festlegen, wie es die Richtlinien Ihrer Organisation erfordern.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	Komponente oder dem Service; d. Die Dokumentation von genehmigten Änderungen am System, der Komponente oder dem Service sowie der potenziellen Auswirkungen solcher Änderungen auf die Sicherheit; und e. Die Überwachung von Sicherheitslücken und deren Behebung innerhalb des Systems, der Komponente oder des Services und die Meldung der Ergebnisse an [Zuweisung: von der Organisation ernanntes Personal].		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SA-10	Die Organisation verlangt von den Entwicklern des Informationssystems, der Systemkomponente oder des Informationssystemservices: a. Die Durchführung des Konfigurationsmanagements während der Entwicklung, Implementierung und des Betriebs von Systemen, Komponenten oder Services; b. Die Dokumentation, Verwaltung und Kontrolle der Integrität von Änderungen an [Zuweisung: von der Organisation definierte Konfigurationselemente im Rahmen der Konfigurationsverwaltung]; c. Die Implementierung von ausschließlich von der Organisation genehmigten Änderungen am System, der	securityhub-enabled	AWS Security Hub hilft bei der Überwachung von unbefugtem Personal, Verbindungen, Geräten und Software. AWS Security Hub aggregiert, organisiert und priorisiert die Sicherheitswarnungen oder Ergebnisse mehrerer Dienste. AWS Einige dieser Dienste sind Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer und AWS Firewall Manager sowie AWS Partnerlösungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	Komponente oder dem Service; d. Die Dokumentation von genehmigten Änderungen am System, der Komponente oder dem Service sowie der potenziellen Auswirkungen solcher Änderungen auf die Sicherheit; und e. Die Überwachung von Sicherheitslücken und deren Behebung innerhalb des Systems, der Komponente oder des Services und die Meldung der Ergebnisse an [Zuweisung: von der Organisation ernanntes Personal].		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SA-10	Die Organisation verlangt von den Entwicklern des Informationssystems, der Systemkomponente oder des Informationssystemservices: a. Die Durchführung des Konfigurationsmanagements während der Entwicklung, Implementierung und des Betriebs von Systemen, Komponenten oder Services; b. Die Dokumentation, Verwaltung und Kontrolle der Integrität von Änderungen an [Zuweisung: von der Organisation definierte Konfigurationselemente im Rahmen der Konfigurationsverwaltung]; c. Die Implementierung von ausschließlich von der Organisation genehmigten Änderungen am System, der	ec2-managed-instance-managed-by-systems	Eine Bestandsaufnahme der Softwareplattformen und Anwendungen innerhalb des Unternehmens ist möglich, indem Amazon Elastic Compute Cloud (Amazon EC2) - Instances mit AWS Systems Manager verwaltet werden. Verwenden Sie AWS Systems Manager, um detaillierte Systemkonfigurationen, Betriebssystem-Patch-Levels, Namen und Typ der Dienste, Softwareinstallationen, Anwendungsname, Herausgeber und Version sowie andere Details zu Ihrer Umgebung bereitzustellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	Komponente oder dem Service; d. Die Dokumentation von genehmigten Änderungen am System, der Komponente oder dem Service sowie der potenziellen Auswirkungen solcher Änderungen auf die Sicherheit; und e. Die Überwachung von Sicherheitslücken und deren Behebung innerhalb des Systems, der Komponente oder des Services und die Meldung der Ergebnisse an [Zuweisung: von der Organisation ernanntes Personal].		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SA-3(a)	Die Organisation: a. Verwaltet das Informationssystem mithilfe von [Zuweisung: von der Organisation definierter Lebenszyklus der Systementwicklung], dem Überlegungen zur Informationssicherheit zugrunde liegen.	codebuild-project-envvar-awscred-überprüfen	Stellen Sie sicher, dass die Anmeldeinformationen AWS_ACCESS_KEY_ID AWS_SECRET_ACCESS_KEY nicht in den AWS Codebuild-Projektumgebungen vorhanden sind. Speichern Sie diese Variablen nicht als Klartext. Das Speichern dieser Variablen als Klartext bewirkt eine unbeabsichtigte Offenlegung von Daten sowie unberechtigte Zugriffe.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SA-3(a)	Die Organisation: a. Verwaltet das Informationssystem mithilfe von [Zuweisung: von der Organisation definierter Lebenszyklus der Systementwicklung], dem Überlegungen zur Informationssicherheit zugrunde liegen.	ec2-manager instance-managed-by-systems	Eine Bestandsaufnahme der Softwareplattformen und Anwendungen innerhalb des Unternehmens ist möglich, indem Amazon Elastic Compute Cloud (Amazon EC2) - Instances mit AWS Systems Manager verwaltet werden. Verwenden Sie AWS Systems Manager, um detaillierte Systemkonfigurationen, Betriebssystem-Patch-Levels, Namen und Typ der Dienste, Softwareinstallationen, Anwendungsname, Herausgeber und Version sowie andere Details zu Ihrer Umgebung bereitzustellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SA-3(a)	Die Organisation: a. Verwaltet das Informationssystem mithilfe von [Zuweisung: von der Organisation definierter Lebenszyklus der Systementwicklung], dem Überlegungen zur Informationssicherheit zugrunde liegen.	codebuild-project-source-repo-URL-Prüfung	Stellen Sie sicher, dass die URL des Quell-Repositorys GitHub oder des Bitbucket-Quell-Repositorys keine persönlichen Zugriffstoken, Benutzernamen und Passwörter in AWS Codebuild-Projektumgebungen enthält. Verwende OAuth anstelle persönlicher Zugriffstoken oder einen Benutzernamen und ein Passwort, um die Autorisierung für den Zugriff auf GitHub Bitbucket-Repositorys zu gewähren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-12	Die Organisation erstellt und verwaltet kryptografische Schlüssel für die erforderliche Kryptografie, die innerhalb des Informationssystems eingesetzt wird, in Übereinstimmung mit [Zuordnung: von der Organisation festgelegte Anforderungen für die Erzeugung, Verteilung, Speicherung, den Zugriff und die Vernichtung von Schlüsseln].	cmk-backing-key-rotation-aktiviert	Aktivieren Sie die Schlüsselrotation, um sicherzustellen, dass Schlüssel rotiert werden, sobald sie das Ende ihrer Kryptoperiode erreicht haben.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-12	Die Organisation erstellt und verwaltet kryptografische Schlüssel für die erforderliche Kryptografie, die innerhalb des Informationssystems eingesetzt wird, in Übereinstimmung mit [Zuordnung: von der Organisation festgelegte Anforderungen für die Erzeugung, Verteilung, Speicherung, den Zugriff und die Vernichtung von Schlüsseln].	acm-certificate-expiration-check	Stelle sicher, dass die Netzwerkintegrität geschützt ist, indem du sicherstellst, dass X509-Zertifikate von ACM ausgestellt werden. AWS Diese Zertifikate müssen gültig und dürfen nicht abgelaufen sein. Für diese Regel ist ein Wert für erforderlich daysToExpiration (Wert für bewährte AWS Grundregeln für Sicherheit: 90). Der tatsächliche Wert muss den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-12	Die Organisation erstellt und verwaltet kryptografische Schlüssel für die erforderliche Kryptografie, die innerhalb des Informationssystems eingesetzt wird, in Übereinstimmung mit [Zuordnung: von der Organisation festgelegte Anforderungen für die Erzeugung, Verteilung, Speicherung, den Zugriff und die Vernichtung von Schlüsseln].	kms-cmk-not-scheduled-zum Löschen	Um Daten im Ruhezustand zu schützen, sollten Sie sicherstellen, dass die erforderlichen Masterschlüssel (CMKs) des Kunden nicht im AWS Key Management Service (AWS KMS) gelöscht werden. Da Schlüssel manchmal gelöscht werden müssen, können Sie mit dieser Regel alle zu löschenden Schlüssel überprüfen, falls ein Schlüssel versehentlich zur Löschung vorgemerkt wurde.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-13	Das Informati onssystem setzt FIPS-validierte oder NSA-zugelassene Kryptographie in Übereinstimmung mit den geltenden Bundesgesetzen, Executive Orders, Direktiven, Richtlini en, Vorschriften und Standards ein.	sagemaker-endpoint -configuration-kms- schlüsselkonfiguriert	Um Daten im Ruhezustand zu schützen, sollten Sie sicherstellen, dass die Verschlüs selung mit dem AWS Key Management Service (AWS KMS) für Ihren SageMaker Endpunkt aktiviert ist. Da sensible Daten auf dem SageMaker Endgerät gespeiche rt werden können, sollten Sie die Verschlüsselung im Ruhezustand aktiviere n, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-13	Das Informati onssystem setzt FIPS-validierte oder NSA-zugelassene Kryptographie in Übereinstimmung mit den geltenden Bundesgesetzen, Executive Orders, Direktiven, Richtlini en, Vorschriften und Standards ein.	sagemaker-notebook -instance-kms-schl üsselkonfiguriert	Um Daten im Ruhezustand zu schützen, sollten Sie sicherstellen, dass die Verschlüsselung mit dem AWS Key Management Service (AWS KMS) für Ihr SageMaker Notebook aktiviert ist. Da vertrauliche Daten im SageMaker Notebook gespeichert werden können, sollten Sie die Verschlüsselung im Ruhezustand aktivieren, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-13	Das Informationssystem setzt FIPS-validierte oder NSA-zugelassene Kryptographie in Übereinstimmung mit den geltenden Bundesgesetzen, Executive Orders, Direktiven, Richtlinien, Vorschriften und Standards ein.	sns-encrypted-kms	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass Ihre Amazon Simple Notification Service (Amazon SNS) -Themen mit dem AWS Key Management Service (AWS KMS) verschlüsselt werden müssen. Um eventuell vorhandene sensible Daten im Ruhezustand in veröffentlichten Nachrichten zu schützen, muss die Verschlüsselung von Daten im Ruhezustand aktiviert sein.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-13	Das Informationssystem setzt FIPS-validierte oder NSA-zugelassene Kryptographie in Übereinstimmung mit den geltenden Bundesgesetzen, Executive Orders, Direktiven, Richtlinien, Vorschriften und Standards ein.	kms-cmk-not-scheduled-zum Löschen	Stellen Sie zum Schutz der gespeicherten Daten sicher, dass die für den Kunden erforderlichen Masterschlüssel (CMKs) nicht für die Löschung im AWS Key Management Service (AWS KMS) vorgesehen sind. Da Schlüssel manchmal gelöscht werden müssen, können Sie mit dieser Regel alle zu löschenden Schlüssel überprüfen, falls ein Schlüssel versehentlich zur Löschung vorgemerkt wurde.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-13	Das Informati onssystem setzt FIPS-validierte oder NSA-zugelassene Kryptographie in Übereinstimmung mit den geltenden Bundesgesetzen, Executive Orders, Direktiven, Richtlini en, Vorschriften und Standards ein.	redshift-cluster-kms-enabled	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass die Verschlüs selung mit AWS Key Management Service (AWS KMS) für Ihren Amazon Redshift Redshift-Cluster aktiviert ist. Um eventuell vorhanden e sensible Daten im Ruhezustand in Redshift-Clustern zu schützen, muss die Verschlüsselung von Daten im Ruhezusta nd aktiviert sein.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-13	Das Informati onssystem setzt FIPS-validierte oder NSA-zugelassene Kryptographie in Übereinstimmung mit den geltenden Bundesgesetzen, Executive Orders, Direktiven, Richtlini en, Vorschriften und Standards ein.	s-3 default-encryption -kms	Stellen Sie sicher, dass die Verschlüs selung für Ihre Amazon Simple Storage Service (Amazon S3)-Bucke ts aktiviert ist. Um eventuell vorhanden e sensible Daten im Ruhezustand in einem Amazon-S3-Bucket zu schützen, muss die Verschlüsselung aktiviert sein.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-2	Das Informati onssystem trennt Benutzerfunktionen (einschließlich Benutzerschnittste llenservices) von den Verwaltungsfunktio nen des Informati onssystems.	iam-group-has-users-überprüfen	AWS Identity and Access Managemen t (IAM) kann Ihnen helfen, die Prinzipie n der geringsten Rechte und der Aufgabentrennung mit Zugriffsberechtigu ngen und Autorisie rungen zu integrier en, indem sicherges tellt wird, dass IAM-Gruppen mindestens einen IAM-Benutzer haben. Die Einteilun g von IAM-Benut zern in Gruppen auf der Grundlage der ihnen zugewiesenen Berechtigungen oder Aufgabenbereiche ist eine Möglichkeit, die geringsten Rechte zu berücksichtigen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-2	Das Informationssystem trennt Benutzerfunktionen (einschließlich Benutzerschnittstellenservices) von den Verwaltungsfunktionen des Informationssystems.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) kann Ihnen dabei helfen, die Prinzipien der geringsten Rechte und der Aufgabentrennung in Zugriffsberechtigungen und Autorisierungen zu integrieren und so zu verhindern, dass Richtlinien „Effect“: „Allow“ mit „Action“: „*“ anstelle von „Resource“: „*“ enthalten. Wenn Benutzern mehr Rechte eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und der Aufgabentrennung verstoßen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-2	Das Informati onssystem trennt Benutzerfunktionen (einschließlich Benutzerschnittste llenservices) von den Verwaltungsfunktio nen des Informati onssystems.	iam-no-inline-policy-überprüfen	Stellen Sie sicher, dass ein Benutzer, eine IAM-Rolle oder eine IAM-Gruppe (AWS Identity and Access Management) nicht über eine Inline-Richtlinie zur Zugriffsk ontrolle auf Systeme und Ressource n verfügt. AWS empfiehlt, verwaltet e Richtlinien anstelle von Inline-Richtlinien zu verwenden. Verwaltete Richtlini en ermöglichen Wiederverwendbarke it, Versionsverwaltung , Rollback und Delegierung der Berechtigungsverwa ltung.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-2	Das Informati onssystem trennt Benutzerfunktionen (einschließlich Benutzerschnittste llenservices) von den Verwaltungsfunktio nen des Informati onssystems.	iam-user-group-mem bership-überprüfen	AWS Identity and Access Managemen t (IAM) kann Ihnen helfen, Zugriffsb erechtigungen und Autorisierungen einzuschränken, indem sicherges tellt wird, dass IAM-Benutzer Mitgliede r mindestens einer Gruppe sind. Wenn Benutzern mehr Berechtigungen eingeräumt werden, als für die Ausführun g einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringste n Berechtigung und Aufgabentrennung verstoßen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-2	Das Informati onssystem trennt Benutzerfunktionen (einschließlich Benutzerschnittste llenservices) von den Verwaltungsfunktio nen des Informati onssystems.	iam-user-no-policies-überprüfen	Diese Regel stellt sicher, dass AWS Identity and Access Management (IAM) -Richtlinien nur Gruppen oder Rollen zugewiese n werden, um den Zugriff auf Systeme und Ressourcen zu kontrollieren. Die Zuweisung von Berechtig ungen auf Gruppen- oder Rollenebene trägt dazu bei, die Wahrscheinlichkeit zu verringern, dass eine Identität übermäßige Berechtigungen erhält oder beibehält.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-23	Das Informationssystem schützt die Authentizität der Kommunikationssitzungen.	alb-http-to-https-Weiterleitungsprüfung	Um Daten während der Übertragung zu schützen, stellen Sie sicher, dass Ihr Application Load Balancer unverschlüsselte HTTP-Anfragen automatisch an HTTPS umleitet. Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.
SC-23	Das Informationssystem schützt die Authentizität der Kommunikationssitzungen.	elb-tls-https-listeners-nur	Stellen Sie sicher, dass Ihre Elastic Load Balancer (ELBs) mit SSL- oder HTTPS-Listenern konfiguriert sind. Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-23	Das Informationssystem schützt die Authentizität der Kommunikationssitzungen.	api-gw-ssl-enabled	Stellen Sie sicher, dass die REST-API-Stufen von Amazon API Gateway mit SSL-Zertifikaten konfiguriert sind, damit Backend-Systeme überprüfen können, ob Anforderungen von API Gateway stammen.
SC-23	Das Informationssystem schützt die Authentizität der Kommunikationssitzungen.	elasticsearch-node-to-node-Verschlüsselungsprüfung	Stellen Sie sicher, dass die node-to-node Verschlüsselung für Amazon OpenSearch Service aktiviert ist. Node-to-nodeVerschlüsselung ermöglicht die TLS 1.2-Verschlüsselung für die gesamte Kommunikation innerhalb der Amazon Virtual Private Cloud (Amazon VPC). Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-23	Das Informationssystem schützt die Authentizität der Kommunikationssitzungen.	redshift-require-tls-ssl	Stellen Sie sicher, dass Ihre Amazon-Redshift-Cluster eine TLS/SSL-Verschlüsselung erfordern, um eine Verbindung zu SQL-Clients herzustellen. Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.
SC-23	Das Informationssystem schützt die Authentizität der Kommunikationssitzungen.	s-3 bucket-ssl-requests-only	Um Daten während der Übertragung zu schützen, stellen Sie sicher, dass Ihre Amazon Simple Storage Service (Amazon S3)-Buckets Anfragen zur Verwendung von Secure Socket Layer (SSL)-Buckets erfordern. Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-28	Das Informationssystem schützt die Vertraulichkeit UND Integrität von [Zuweisung: von der Organisation definierte Informationen im Ruhestand].	api-gw-cache-enabled-und-verschlüsselt	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass die Verschlüsselung für den Cache Ihrer API-Gateway-Stufe aktiviert ist. Da für die API-Methode sensible Daten erfasst werden können, sollten Sie die Verschlüsselung von Daten im Ruhezustand aktivieren, um diese Daten zu schützen.
SC-28	Das Informationssystem schützt die Vertraulichkeit UND Integrität von [Zuweisung: von der Organisation definierte Informationen im Ruhestand].	cloud-trail-encryption-enabled	Da sensible Daten vorhanden sein können und um Daten im Ruhezustand zu schützen, sollten Sie sicherstellen, dass die Verschlüsselung für Ihre AWS CloudTrail Trails aktiviert ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-28	Das Informationssystem schützt die Vertraulichkeit UND Integrität von [Zuweisung: von der Organisation definierte Informationen im Ruhestand].	cloudwatch-log-group-encrypted	Um sensible Daten im Speicher zu schützen, stellen Sie sicher, dass die Verschlüsselung für Ihre Amazon CloudWatch Log Groups aktiviert ist.
SC-28	Das Informationssystem schützt die Vertraulichkeit UND Integrität von [Zuweisung: von der Organisation definierte Informationen im Ruhestand].	efs-encrypted-check	Aktivieren Sie die Verschlüsselung für Ihr Amazon Elastic File System (EFS), um eventuell vorhandene sensible Daten sowie Daten im Ruhezustand zu schützen.
SC-28	Das Informationssystem schützt die Vertraulichkeit UND Integrität von [Zuweisung: von der Organisation definierte Informationen im Ruhestand].	elasticsearch-encrypted-at-rest	Da sensible Daten vorhanden sein können und um Daten im Ruhezustand zu schützen, sollten Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon OpenSearch Service (OpenSearch Service) -Domains aktiviert ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-28	Das Informati onssystem schützt die Vertraulichkeit UND Integrität von [Zuweisung: von der Organisation definiert e Informationen im Ruhestand].	encrypted-volumes	Aktivieren Sie die Verschlüsselung für Ihre Amazon-Elastic-Block-Store (Amazon-EBS)-Volumes, um eventuell vorhandene sensible Daten sowie Daten im Ruhezusta nd zu schützen.
SC-28	Das Informati onssystem schützt die Vertraulichkeit UND Integrität von [Zuweisung: von der Organisation definiert e Informationen im Ruhestand].	kms-cmk-not-schedu led-zum Löschen	Um Daten im Ruhezustand zu schützen, sollten Sie sicherstellen, dass die für den Kunden erforderl ichen Masterschlüssel (CMKs) nicht im AWS Key Management Service (AWS KMS) gelöscht werden. Da Schlüssel manchmal gelöscht werden müssen, können Sie mit dieser Regel alle zu löschenden Schlüssel überprüfe n, falls ein Schlüssel versehentlich zur Löschung vorgemerkt wurde.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-28	Das Informationssystem schützt die Vertraulichkeit UND Integrität von [Zuweisung: von der Organisation definierte Informationen im Ruhestand].	redshift-cluster-configuration-check	Um Daten im Ruhezustand zu schützen, muss die Verschlüsselung für Ihre Amazon-Redshift-Cluster aktiviert sein. Sie müssen auch sicherstellen, dass die erforderlichen Konfigurationen auf Amazon-Redshift-Clustern bereitgestellt werden. Die Prüfungsprotokollierung muss aktiviert sein, um Informationen zu Verbindungen und Benutzeraktivitäten in der Datenbank bereitzustellen. Diese Regel erfordert, dass ein Wert für clusterDbEncrypted (Config Default: TRUE) und LoggingEnabled (Config Default: TRUE) gesetzt ist. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-28	Das Informationssystem schützt die Vertraulichkeit UND Integrität von [Zuweisung: von der Organisation definierte Informationen im Ruhestand].	s-3 bucket-default-lock-enabled	Stellen Sie sicher, dass für Ihren Amazon Simple Storage Service (Amazon S3)-Bucket standardmäßig eine Sperre aktiviert ist. Zum Schutz eventuell vorhandener sensibler Daten in S3-Buckets müssen Sie Objektsperren für Daten im Ruhezustand erzwingen.
SC-28	Das Informationssystem schützt die Vertraulichkeit UND Integrität von [Zuweisung: von der Organisation definierte Informationen im Ruhestand].	bucket-server-side-encryptions3-fähig	Zum Schutz von Daten im Ruhezustand müssen Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon Simple Storage Service (Amazon S3)-Buckets aktiviert ist. Um eventuell vorhandene sensible Daten im Ruhezustand in Amazon-S3-Buckets zu schützen, muss die Verschlüsselung aktiviert sein.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-28	Das Informati onssystem schützt die Vertraulichkeit UND Integrität von [Zuweisung: von der Organisation definiert e Informationen im Ruhestand].	sagemaker-endpoint -configuration-kms- schlüsselkonfiguriert	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass die Verschlüsselung mit dem AWS Key Management Service (AWS KMS) für Ihren Endpunkt aktiviert ist. SageMaker Da sensible Daten auf dem SageMaker Endgerät gespeiche rt werden können, sollten Sie die Verschlüsselung im Ruhezustand aktiviere n, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-28	Das Informati onssystem schützt die Vertraulichkeit UND Integrität von [Zuweisung: von der Organisation definiert e Informationen im Ruhestand].	sagemaker-notebook -instance-kms-schl üsselkonfiguriert	Um Daten im Ruhezustand zu schützen, sollten Sie sicherstellen, dass die Verschlüsselung mit dem AWS Key Management Service (AWS KMS) für Ihr SageMaker Notebook aktiviert ist. Da vertrauliche Daten im SageMaker Notebook gespeichert werden können, sollten Sie die Verschlüsselung im Ruhezustand aktivieren, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-28	Das Informati onssystem schützt die Vertraulichkeit UND Integrität von [Zuweisung: von der Organisation definiert e Informationen im Ruhestand].	sns-encrypted-kms	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass Ihre Amazon Simple Notification Service (Amazon SNS) -Themen mit dem AWS Key Management Service (AWS KMS) verschlüsselt werden müssen. Um eventuell vorhandene sensible Daten im Ruhezusta nd in veröffentlichten Nachrichten zu schützen, muss die Verschlüsselung von Daten im Ruhezusta nd aktiviert sein.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-28	Das Informati onssystem schützt die Vertraulichkeit UND Integrität von [Zuweisung: von der Organisation definiert e Informationen im Ruhestand].	ec2- ebs-encryption-by-default	Zum Schutz von Daten im Ruhezusta nd müssen Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon Elastic Block Store (Amazon EBS)-Volu mes aktiviert ist. Da sensible Daten auch im Ruhezusta nd vorhanden sein können, sollten Sie die Verschlüsselung im Ruhezustand aktivieren, um diese Daten zu schützen.
SC-28	Das Informati onssystem schützt die Vertraulichkeit UND Integrität von [Zuweisung: von der Organisation definiert e Informationen im Ruhestand].	rds-snapshot-encry pted	Stellen Sie sicher, dass die Verschlüs selung für Ihre Amazon Relationa l Database Service (Amazon RDS)-Snap shots aktiviert ist. Da sensible Daten auch im Ruhezusta nd vorhanden sein können, sollten Sie die Verschlüsselung im Ruhezustand aktivieren, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-28	Das Informati onssystem schützt die Vertraulichkeit UND Integrität von [Zuweisung: von der Organisation definiert e Informationen im Ruhestand].	rds-storage-encrypted	Zum Schutz von Daten im Ruhezusta nd müssen Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon Relational Database Service (Amazon RDS)-Instances aktiviert ist. Um eventuell vorhanden e sensible Daten im Ruhezustand in Amazon-RDS-Instanc es zu schützen, muss die Verschlüs selung von Daten im Ruhezustand aktiviert sein.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-28	Das Informati onssystem schützt die Vertraulichkeit UND Integrität von [Zuweisung: von der Organisation definiert e Informationen im Ruhestand].	redshift-cluster-kms-enabled	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass die Verschlüs selung mit AWS Key Management Service (AWS KMS) für Ihren Amazon Redshift Redshift-Cluster aktiviert ist. Um eventuell vorhanden e sensible Daten im Ruhezustand in Redshift-Clustern zu schützen, muss die Verschlüsselung von Daten im Ruhezusta nd aktiviert sein.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-28	Das Informati onssystem schützt die Vertraulichkeit UND Integrität von [Zuweisung: von der Organisation definiert e Informationen im Ruhestand].	s-3 default-encryption -kms	Stellen Sie sicher, dass die Verschlüs selung für Ihre Amazon Simple Storage Service (Amazon S3)-Bucke ts aktiviert ist. Um eventuell vorhanden e sensible Daten im Ruhezustand in einem Amazon-S3-Bucket zu schützen, muss die Verschlüsselung aktiviert sein.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-4	Das Informati onssystem verhinder t die unbefugte und unbeabsichtigte Übertragung von Informationen über gemeinsam genutzte Systemressourcen.	ec2- volume-inuse-check	Diese Regel stellt sicher, dass Amazon Elastic Block Store-Volumes, die an Amazon Elastic Compute Cloud (Amazon EC2) - Instances angehängt sind, zum Löschen markiert werden, wenn eine Instance beendet wird. Wenn ein Amazon-EB S-Volume nicht gelöscht wird, wenn die Instance, an die es angehängt ist, beendet wird, kann dies gegen das Konzept der geringsten Funktiona lität verstoßen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-4	Das Informati onssystem verhinder t die unbefugte und unbeabsichtigte Übertragung von Informationen über gemeinsam genutzte Systemressourcen.	dms-replication-not-public	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass auf DMS-Replikationsin stanzen nicht öffentlic h zugegriffen werden kann. DMS-Repli kations-Instances können vertrauli che Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.
SC-4	Das Informati onssystem verhinder t die unbefugte und unbeabsichtigte Übertragung von Informationen über gemeinsam genutzte Systemressourcen.	ebs-snapshot-public-restorable-überprüfen	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass EBS-Snapshots nicht öffentlich wiederher stellbar sind. EBS-Volume-Snapsho ts können vertrauli che Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-4	Das Informati onssystem verhinder t die unbefugte und unbeabsichtigte Übertragung von Informationen über gemeinsam genutzte Systemressourcen.	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) Security Groups können bei der Verwaltung des Netzwerkzugriffs helfen, indem sie eine statusbeh aftete Filterung von eingehendem und ausgehendem Netzwerkverkehr zu Ressourcen bereitste llen. AWS Wenn Sie eingehenden (oder entfernten) Datenverk ehr von 0.0.0.0/0 bis Port 22 auf Ihren Ressourcen nicht zulassen, können Sie den Remote-Zugriff einschränken.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-4	Das Informati onssystem verhinder t die unbefugte und unbeabsichtigte Übertragung von Informationen über gemeinsam genutzte Systemressourcen.	lambda-function-pu blic-access-verboten	Verwalten Sie den Zugriff auf Ressource n in der AWS Cloud, indem Sie sicherste llen, dass AWS Lambda-Funktionen nicht öffentlich zugänglich sind. Der öffentliche Zugriff kann möglicherweise die Verfügbarkeit von Ressourcen beeinträc htigen.
SC-4	Das Informati onssystem verhinder t die unbefugte und unbeabsichtigte Übertragung von Informationen über gemeinsam genutzte Systemressourcen.	rds-instance-public-access-überprüfen	Verwalten Sie den Zugriff auf Ressource n in der AWS Cloud, indem Sie sicherste llen, dass Amazon Relational Database Service (Amazon RDS) -Instance s nicht öffentlic h sind. Amazon-RDS-Datenbank-Instances können vertrauliche Informati onen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-4	Das Informati onssystem verhinder t die unbefugte und unbeabsichtigte Übertragung von Informationen über gemeinsam genutzte Systemressourcen.	rds-snapshots-public-prohibited	Verwalten Sie den Zugriff auf Ressource n in der AWS Cloud, indem Sie sicherste llen, dass Amazon Relational Database Service (Amazon RDS) -Instance s nicht öffentlic h sind. Amazon-RDS-Datenbank-Instances können vertrauliche Informati onen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-4	Das Informati onssystem verhinder t die unbefugte und unbeabsichtigte Übertragung von Informationen über gemeinsam genutzte Systemressourcen.	redshift-cluster-public-access-überprüfen	Verwalten Sie den Zugriff auf Ressource n in der AWS Cloud, indem Sie sicherste llen, dass Amazon Redshift Redshift-Cluster nicht öffentlic h sind. Amazon-Re dshift-Cluster können vertrauliche Informati onen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-4	Das Informati onssystem verhinder t die unbefugte und unbeabsichtigte Übertragung von Informationen über gemeinsam genutzte Systemressourcen.	restricted-common-ports	Verwalten Sie den Zugriff auf Ressource n in der AWS Cloud, indem Sie sicherste llen, dass gemeinsam e Ports für Amazon Elastic Compute Cloud (Amazon EC2) -Sicherhe itsgruppen eingeschr ränkt sind. Wenn der Zugriff auf Ports nicht auf vertrauen swürdige Quellen beschränkt wird, kann dies zu Angriffen auf die Verfügbar keit, Integrität und Vertraulichkeit von Systemen führen. Mit dieser Regel können Sie optional die Parameter blockedPo rt1–blockedPort5 festlegen (Standard konfigurationen: 20, 21, 3389, 3306, 4333). Die tatsächli chen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-4	Das Informationssystem verhindert die unbefugte und unbeabsichtigte Übertragung von Informationen über gemeinsam genutzte Systemressourcen.	s-3 bucket-public-read-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie nur autorisierten Benutzern, Prozessen und Geräten Zugriff auf Amazon Simple Storage Service (Amazon S3) - Buckets gewähren. Die Verwaltung des Zugriffs sollte mit der Klassifizierung der Daten übereinstimmen.
SC-4	Das Informationssystem verhindert die unbefugte und unbeabsichtigte Übertragung von Informationen über gemeinsam genutzte Systemressourcen.	s-3 bucket-public-write-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie nur autorisierten Benutzern, Prozessen und Geräten Zugriff auf Amazon Simple Storage Service (Amazon S3) - Buckets gewähren. Die Verwaltung des Zugriffs sollte mit der Klassifizierung der Daten übereinstimmen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-4	Das Informati onssystem verhinder t die unbefugte und unbeabsichtigte Übertragung von Informationen über gemeinsam genutzte Systemressourcen.	sagemaker-notebook -no-direct-Interne tzugang	Verwalten Sie den Zugriff auf Ressource n in der AWS Cloud, indem Sie sicherste llen, dass SageMaker Amazon-Notebooks keinen direkten Internetzugang zulassen. Indem Sie direkten Internetz ugang blockieren, vermeiden Sie, dass unbefugte Benutzer auf sensible Daten zugreifen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-4	Das Informati onssystem verhinder t die unbefugte und unbeabsichtigte Übertragung von Informationen über gemeinsam genutzte Systemressourcen.	vpc-default-security-group-geschlossen	Sicherheitsgruppen von Amazon Elastic Compute Cloud (Amazon EC2) können bei der Verwaltung des Netzwerkzugriffs helfen, indem sie eine statusbehaftete Filterung des ein- und ausgehenden Netzwerkverkehrs zu Ressourcen bereitstellen. AWS Die Beschränk ung des gesamten Datenverkehrs auf die Standardsicherheit sgruppe hilft dabei, den Fernzugriff auf Ihre Ressourcen einzuschränken. AWS

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-4	Das Informati onssystem verhinder t die unbefugte und unbeabsichtigte Übertragung von Informationen über gemeinsam genutzte Systemressourcen.	vpc-sg-open-only-to-authorized-ports	Verwalten Sie den Zugriff auf Ressource n in der AWS Cloud, indem Sie sicherste llen, dass gemeinsam e Ports für Amazon Elastic Compute Cloud (Amazon EC2) -Sicherhe itsgruppen eingeschr ränkt sind. Wenn der Zugriff auf Ports nicht auf vertrauen swürdige Quellen beschränkt wird, kann dies zu Angriffen auf die Verfügbar keit, Integrität und Vertraulichkeit von Systemen führen. Durch die Beschränk ung des Zugriffs auf Ressourcen innerhalb einer Sicherhei tsgruppe aus dem Internet (0.0.0.0/0) kann der Remote-Zugriff auf interne Systeme gesteuert werden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-4	Das Informati onssystem verhinder t die unbefugte und unbeabsichtigte Übertragung von Informationen über gemeinsam genutzte Systemressourcen.	no-unrestricted-route-to-igw	Stellen Sie sicher, dass EC2 Amazon-Routentabellen keine uneingeschränkten Routen zu einem Internet-Gateway enthalten. Durch das Entfernen oder Beschränken des Internetzugangs für Workloads innerhalb von Amazon VPCs können unbeabsic htigte Zugriffe in Ihrer Umgebung reduziert werden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-4	Das Informati onssystem verhinder t die unbefugte und unbeabsichtigte Übertragung von Informationen über gemeinsam genutzte Systemressourcen.	s3 bucket-level-public-access - verboten	Verwalten Sie den Zugriff auf Ressource n in der AWS Cloud, indem Sie sicherste llen, dass Amazon Simple Storage Service (Amazon S3) -Buckets nicht öffentlich zugänglic h sind. Diese Regel trägt dazu bei, sensible Daten vor unbefugten Remote-Benutzern zu schützen, indem sie den öffentlichen Zugriff auf Bucket-Eb ene verhindert.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-4	Das Informati onssystem verhinder t die unbefugte und unbeabsichtigte Übertragung von Informationen über gemeinsam genutzte Systemressourcen.	account-level-publ ic-accesss3-Blöcke-periodisch	Verwalten Sie den Zugriff auf Ressource n in der AWS Cloud, indem Sie sicherste llen, dass Amazon Simple Storage Service (Amazon S3) -Buckets nicht öffentlich zugänglic h sind. Diese Regel trägt dazu bei, sensible Daten vor unbefugten Remote-Benutzern zu schützen, indem sie den öffentlichen Zugriff verhinder t. Mit dieser Regel können Sie optional die Parameter ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) und restrictPublicBuck ets Parameter (Config Default: True) festlegen. Die tatsächlichen Werte müssen den Richtlini

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			en Ihrer Organisation entsprechen.
SC-4	Das Informati onssystem verhinder t die unbefugte und unbeabsichtigte Übertragung von Informationen über gemeinsam genutzte Systemressourcen.	ssm-document-not-p ublic	Stellen Sie sicher, dass AWS Systems Manager (SSM) - Dokumente nicht öffentlich sind, da dies einen unbeabsic htigten Zugriff auf Ihre SSM-Dokum ente ermöglichen kann. Ein öffentlic hes SSM-Dokum ent kann Informati onen über Ihr Konto, Ihre Ressourcen und internen Prozesse preisgeben.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-5	Das Informati onssystem schützt vor den folgenden Arten von Denial-of -Service-Angriffen oder begrenzt deren Auswirkungen: [Zuweisung: von der Organisation definiert e Arten von Denial-of-Service-Angriffen oder Verweise auf Quellen für solche Informationen] durch den Einsatz von [Zuweisung: von der Organisation definiert e Sicherheitsvorkehr ungen].	autoscaling-group-elb-healthcheck-er forderlich	Die Elastic Load Balancer (ELB) - Zustandsprüfungen für Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling Scaling-G ruppen unterstützen die Aufrechterhaltung einer angemesse nen Kapazität und Verfügbarkeit. Der Load Balancer sendet regelmäßig Pings, versucht Verbindun gen herzustellen oder sendet Anfragen, um den Zustand der EC2 Amazon-Instances in einer Gruppe mit auto-scal ing zu testen. Wenn eine Instance nicht zurückmeldet, wird der Traffic an eine neue EC2 Amazon-In stance gesendet.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-5	Das Informationssystem schützt vor den folgenden Arten von Denial-of-Service-Angriffen oder begrenzt deren Auswirkungen: [Zuweisung: von der Organisation definierte Arten von Denial-of-Service-Angriffen oder Verweise auf Quellen für solche Informationen] durch den Einsatz von [Zuweisung: von der Organisation definierte Sicherheitsvorkehrungen].	dynamodb-autoscaling-enabled	Amazon DynamoDB Auto Scaling verwendet den AWS Application Auto Scaling-Service, um die bereitgestellte Durchsatzkapazität so anzupassen, dass sie automatisch auf tatsächliche Verkehrsmuster reagiert. Auf diese Weise kann eine Tabelle oder ein globaler sekundärer Index die bereitgestellte Lese-/Schreibkapazität erhöhen, um plötzliche Erhöhungen des Datenverkehrs ohne Drosselung zu bewältigen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-5	Das Informationssystem schützt vor den folgenden Arten von Denial-of-Service-Angriffen oder begrenzt deren Auswirkungen: [Zuweisung: von der Organisation definierte Arten von Denial-of-Service-Angriffen oder Verweise auf Quellen für solche Informationen] durch den Einsatz von [Zuweisung: von der Organisation definierte Sicherheitsvorkehrungen].	rds-multi-az-support	Die Multi-AZ-Unterstützung in Amazon Relational Database Service (Amazon RDS) bietet eine verbesserte Verfügbarkeit und Beständigkeit von Datenbank-Instances. Wenn Sie eine Multi-AZ-Datenbank-Instance bereitstellen, erstellt Amazon RDS automatisch eine primäre Datenbank-Instance und repliziert die Daten synchron auf eine Standby-Instance in einer anderen Availability Zone. Jede Availability Zone läuft auf einer eigenen, physisch getrennten, unabhängigen Infrastruktur und ist auf eine hohe Verfügbarkeit ausgelegt. Im Falle eines Infrastrukturausfalls führt Amazon RDS einen automatis

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			chen Failover zum Standby-Modus durch, sodass Sie den Datenbankbetrieb wieder aufnehmen können, sobald der Failover abgeschlo ssen ist.
SC-5	Das Informati onssystem schützt vor den folgenden Arten von Denial-of -Service-Angriffen oder begrenzt deren Auswirkungen: [Zuweisung: von der Organisation definiert e Arten von Denial-of-Service-Angriffen oder Verweise auf Quellen für solche Informationen] durch den Einsatz von [Zuweisung: von der Organisation definiert e Sicherheitsvorkehr ungen].	s-3 bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) unterstützt die Aufrechterhaltung einer angemesse nen Kapazität und Verfügbarkeit. CRR ermöglicht das automatische, asynchrone Kopieren von Objekten in Amazon-S3-Buckets, um die Datenverf ügbarkeit sicherzus tellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-5	Das Informati onssystem schützt vor den folgenden Arten von Denial-of -Service-Angriffen oder begrenzt deren Auswirkungen: [Zuweisung: von der Organisation definiert e Arten von Denial-of-Service-Angriffen oder Verweise auf Quellen für solche Informationen] durch den Einsatz von [Zuweisung: von der Organisation definiert e Sicherheitsvorkehr ungen].	elb-cross-zone-load-Balancing aktiviert	Aktivieren Sie den zonenübergreifende n Load Balancing für Ihre Elastic Load Balancer (ELBs), um eine angemesse ne Kapazität und Verfügbarkeit aufrechtzuerhalten. Zonenübergreifende s Load Balancing reduziert die Notwendigkeit, die gleiche Anzahl von Instances in jeder aktivierten Availability Zone aufrechtzuerhalten. Es verbessert auch die Fähigkeit Ihrer Anwendung, den Verlust einer oder mehrerer Instances zu bewältigen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-5	Das Informati onssystem schützt vor den folgenden Arten von Denial-of -Service-Angriffen oder begrenzt deren Auswirkungen: [Zuweisung: von der Organisation definiert e Arten von Denial-of-Service-Angriffen oder Verweise auf Quellen für solche Informationen] durch den Einsatz von [Zuweisung: von der Organisation definiert e Sicherheitsvorkehr ungen].	rds-instance-deletion-protection-aktiviert	Stellen Sie sicher, dass Amazon Relational Database Service (Amazon RDS)-Instances den Löschschutz aktiviert haben. Verwenden Sie den Löschschu tz, um zu verhindern, dass Ihre Amazon-RD S-Instances versehent lich oder böswillig gelöscht werden, was zum Verlust der Verfügbarkeit Ihrer Anwendungen führen kann.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-5	Das Informationssystem schützt vor den folgenden Arten von Denial-of-Service-Angriffen oder begrenzt deren Auswirkungen: [Zuweisung: von der Organisation definierte Arten von Denial-of-Service-Angriffen oder Verweise auf Quellen für solche Informationen] durch den Einsatz von [Zuweisung: von der Organisation definierte Sicherheitsvorkehrungen].	elb-deletion-protection-enabled	Diese Regel sorgt dafür, dass der Löschschutz für Elastic Load Balancing aktiviert ist. Verwenden Sie diese Funktion, um zu verhindern, dass Ihr Load Balancer versehentlich oder böswillig gelöscht wird, was zum Verlust der Verfügbarkeit Ihrer Anwendungen führen kann.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-5	Das Informati onssystem schützt vor den folgenden Arten von Denial-of -Service-Angriffen oder begrenzt deren Auswirkungen: [Zuweisung: von der Organisation definiert e Arten von Denial-of-Service-Angriffen oder Verweise auf Quellen für solche Informationen] durch den Einsatz von [Zuweisung: von der Organisation definiert e Sicherheitsvorkehr ungen].	vpc-vpn-2-tunnels-up	Redundante Site-to-Site VPN-Tunne l können implement iert werden, um die Anforderungen an die Ausfallsicherheit zu erfüllen. Es verwendet zwei Tunnel, um die Konnektivität sicherzustellen, falls eine der Site-to-Site VPN-Verbindungen nicht verfügbar ist. Um sich vor einem Verbindungsverlust zu schützen, können Sie für den Fall, dass Ihr Kunden-Gateway nicht verfügbar ist, eine zweite Site-to-S ite VPN-Verbindung zu Ihrer Amazon Virtual Private Cloud (Amazon VPC) und Ihrem Virtual Private Gateway einrichten, indem Sie ein zweites Kunden-Gateway verwenden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-5	Das Informationssystem schützt vor den folgenden Arten von Denial-of-Service-Angriffen oder begrenzt deren Auswirkungen: [Zuweisung: von der Organisation definierte Arten von Denial-of-Service-Angriffen oder Verweise auf Quellen für solche Informationen] durch den Einsatz von [Zuweisung: von der Organisation definierte Sicherheitsvorkehrungen].	dynamodb-pitr-enabled	Aktivieren Sie diese Regel, um zu überprüfen, ob die Informationen gesichert wurden. Es verwaltet auch die Backups, indem es sicherstellt, dass die point-in-time Wiederherstellung in Amazon DynamoDB aktiviert ist. Bei der Wiederherstellung werden fortlaufende Backups Ihrer Tabelle für die letzten 35 Tage gespeichert.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-5	Das Informationssystem schützt vor den folgenden Arten von Denial-of-Service-Angriffen oder begrenzt deren Auswirkungen: [Zuweisung: von der Organisation definierte Arten von Denial-of-Service-Angriffen oder Verweise auf Quellen für solche Informationen] durch den Einsatz von [Zuweisung: von der Organisation definierte Sicherheitsvorkehrungen].	ebs-optimized-instance	Eine optimierte Instance im Amazon Elastic Block Store (Amazon EBS) bietet zusätzliche, dedizierte Kapazität für Amazon-EBS-I/O-Vorgänge. Diese Optimierung bietet die beste Leistung für Ihr EBS-Volume, indem Konflikte zwischen Amazon-EBS-I/O und anderem Datenverkehr von Ihrer Instance minimiert werden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-5	Das Informati onssystem schützt vor den folgenden Arten von Denial-of -Service-Angriffen oder begrenzt deren Auswirkungen: [Zuweisung: von der Organisation definiert e Arten von Denial-of-Service-Angriffen oder Verweise auf Quellen für solche Informationen] durch den Einsatz von [Zuweisung: von der Organisation definiert e Sicherheitsvorkehr ungen].	elasticache-redis-cluster-automatic-Backup-Check	Wenn automatische Backups aktiviert sind, ElastiCache erstellt Amazon täglich ein Backup des Clusters. Die Sicherung kann für eine von Ihrer Organisation festgelegte Anzahl von Tagen aufbewahrt werden. Automatische Backups schützen vor Datenverlust. Bei einem Ausfall können Sie einen neuen Cluster erstellen, der Ihre Daten aus dem aktuellen Backup wiederherstellt.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-5	Das Informati onssystem schützt vor den folgenden Arten von Denial-of -Service-Angriffen oder begrenzt deren Auswirkungen: [Zuweisung: von der Organisation definiert e Arten von Denial-of-Service-Angriffen oder Verweise auf Quellen für solche Informationen] durch den Einsatz von [Zuweisung: von der Organisation definiert e Sicherheitsvorkehr ungen].	s-3 bucket-versioning-enabled	Die Versionsv erwaltung von Amazon Simple Storage Service (Amazon S3)-Bucke ts hilft dabei, mehrere Varianten eines Objekts im selben Amazon-S3-Bucket zu speichern. Verwenden Sie die Versionsv erwaltung, um sämtliche Versionen aller Objekte in Ihrem Amazon-S3-Bucket zu speichern , abzurufen oder wiederherzustellen . Mit der Versionsv erwaltung können Sie Versionen sowohl nach unbeabsic htigten Benutzera ktionen als auch nach Anwendungsfehlern problemlos wiederher stellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-5	Das Informati onssystem schützt vor den folgenden Arten von Denial-of -Service-Angriffen oder begrenzt deren Auswirkungen: [Zuweisung: von der Organisation definiert e Arten von Denial-of-Service-Angriffen oder Verweise auf Quellen für solche Informationen] durch den Einsatz von [Zuweisung: von der Organisation definiert e Sicherheitsvorkehr ungen].	guardduty-enabled-centralized	Amazon GuardDuty kann mithilfe von Threat Intellige nce Feeds helfen, potenzielle Cybersich erheitsereignisse zu überwachen und zu erkennen. Dazu gehören Listen mit bösartigen IPs und maschinel len Lernmethoden zur Identifizierung unerwarteter, nicht autorisierter und bösartiger Aktivitäten in Ihrer AWS Cloud-Umgebung.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-7	Das Informationssystem: a. Überwacht und kontrolliert die Kommunikation an der Außengrenze des Systems und an wichtigen internen Grenzen innerhalb des Systems; b. Implementiert Subnetze für öffentlich zugängliche Systemkomponenten, die [Auswahl: physisch; logisch] von internen Organisationsnetzen getrennt sind; und c. Stellt eine Verbindung zu externen Netzwerken oder Informationssystemen nur über verwaltete Schnittstellen her, die aus Grenzschutzgeräten bestehen, die gemäß einer Sicherheitsarchitektur der Organisation angeordnet sind.	wafv2-logging-enabled	Um die Protokollierung und Überwachung in Ihrer Umgebung zu erleichtern, aktivieren Sie die AWS WAF (V2) -Protokollierung im regionalen und globalen Web ACLs. AWS Die WAF-Protokollierung bietet detaillierte Informationen über den Datenverkehr, der von Ihrer Web-ACL analysiert wird. In den Protokollen werden die Uhrzeit aufgezeichnet, zu der die AWS WAF die Anfrage von Ihrer AWS Ressource erhalten hat, Informationen über die Anfrage und eine Aktion für die Regel, der jede Anfrage entsprach.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-7	Das Informati onssystem: a. Überwacht und kontrolliert die Kommunikation an der Außengrenze des Systems und an wichtigen internen Grenzen innerhalb des Systems; b. Implementiert Subnetze für öffentlic h zugängliche Systemkomponenten, die [Auswahl: physisch; logisch] von internen Organisat ionsnetzen getrennt sind; und c. Stellt eine Verbindung zu externen Netzwerke n oder Informati onssystemen nur über verwaltete Schnittstellen her, die aus Grenzschu tzgeräten bestehen, die gemäß einer Sicherheitsarchite ktur der Organisation angeordnet sind.	ec2- instances-in-vpc	Stellen Sie Amazon Elastic Compute Cloud (Amazon EC2) -Instances innerhalb einer Amazon Virtual Private Cloud (Amazon VPC) bereit, um eine sichere Kommunika tion zwischen einer Instance und anderen Services innerhalb der Amazon VPC zu ermöglichen, ohne dass ein Internet-Gateway, ein NAT-Gerät oder eine VPN-Verbindung erforderlich ist. Der gesamte Datenverk ehr bleibt sicher in der AWS Cloud. Domains, die sich innerhalb einer VPC befinden, verfügen aufgrund ihrer logischen Isolierun g im Vergleich zu Domains mit öffentlic hen Endpunkten über eine zusätzlic he Sicherheitsebene. Weisen Sie EC2

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			Amazon-Instances einer Amazon-VPC zu, um den Zugriff ordnungsgemäß zu verwalten.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-7	Das Informati onssystem: a. Überwacht und kontrolliert die Kommunikation an der Außengrenze des Systems und an wichtigen internen Grenzen innerhalb des Systems; b. Implementiert Subnetze für öffentlic h zugängliche Systemkomponenten, die [Auswahl: physisch; logisch] von internen Organisat ionsnetzen getrennt sind; und c. Stellt eine Verbindung zu externen Netzwerke n oder Informati onssystemen nur über verwaltete Schnittstellen her, die aus Grenzschu tzgeräten bestehen, die gemäß einer Sicherheitsarchite ktur der Organisation angeordnet sind.	dms-replication-not-public	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass auf DMS-Replikationsin stanzen nicht öffentlic h zugegriffen werden kann. DMS-Repli kations-Instances können vertrauli che Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-7	Das Informati onssystem: a. Überwacht und kontrolliert die Kommunikation an der Außengrenze des Systems und an wichtigen internen Grenzen innerhalb des Systems; b. Implementiert Subnetze für öffentlic h zugängliche Systemkomponenten, die [Auswahl: physisch; logisch] von internen Organisat ionsnetzen getrennt sind; und c. Stellt eine Verbindung zu externen Netzwerke n oder Informati onssystemen nur über verwaltete Schnittstellen her, die aus Grenzschu tzgeräten bestehen, die gemäß einer Sicherheitsarchite ktur der Organisation angeordnet sind.	ebs-snapshot-public-restorable-überprüfen	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass EBS-Snapshots nicht öffentlich wiederher stellbar sind. EBS-Volume-Snapsho ts können vertrauli che Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-7	Das Informati onssystem: a. Überwacht und kontrolliert die Kommunikation an der Außengrenze des Systems und an wichtigen internen Grenzen innerhalb des Systems; b. Implementiert Subnetze für öffentlic h zugängliche Systemkomponenten, die [Auswahl: physisch; logisch] von internen Organisat ionsnetzen getrennt sind; und c. Stellt eine Verbindung zu externen Netzwerke n oder Informati onssystemen nur über verwaltete Schnittstellen her, die aus Grenzschu tzgeräten bestehen, die gemäß einer Sicherheitsarchite ktur der Organisation angeordnet sind.	ec2- instance-no-public-ip	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon Elastic Compute Cloud (Amazon EC2) - Instances nicht öffentlich zugänglich sind. EC2 Amazon-Instances können vertrauliche Informati onen enthalten, und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-7	Das Informationssystem: a. Überwacht und kontrolliert die Kommunikation an der Außengrenze des Systems und an wichtigen internen Grenzen innerhalb des Systems; b. Implementiert Subnetze für öffentlich zugängliche Systemkomponenten, die [Auswahl: physisch; logisch] von internen Organisationsnetzen getrennt sind; und c. Stellt eine Verbindung zu externen Netzwerken oder Informationssystemen nur über verwaltete Schnittstellen her, die aus Grenzschutzgeräten bestehen, die gemäß einer Sicherheitsarchitektur der Organisation angeordnet sind.	elasticsearch-in-vpc-only	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass sich Amazon OpenSearch OpenSearch Service (Service) - Domains innerhalb einer Amazon Virtual Private Cloud (Amazon VPC) befinden. Eine OpenSearch Service-Domain innerhalb einer Amazon VPC ermöglicht die sichere Kommunikation zwischen OpenSearch Service und anderen Services innerhalb der Amazon VPC, ohne dass ein Internet-Gateway, ein NAT-Gerät oder eine VPN-Verbindung erforderlich ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-7	Das Informati onssystem: a. Überwacht und kontrolliert die Kommunikation an der Außengrenze des Systems und an wichtigen internen Grenzen innerhalb des Systems; b. Implementiert Subnetze für öffentlic h zugängliche Systemkomponenten, die [Auswahl: physisch; logisch] von internen Organisat ionsnetzen getrennt sind; und c. Stellt eine Verbindung zu externen Netzwerke n oder Informati onssystemen nur über verwaltete Schnittstellen her, die aus Grenzschu tzgeräten bestehen, die gemäß einer Sicherheitsarchite ktur der Organisation angeordnet sind.	emr-master-no-public-ip	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon EMR-Clust er-Masterknoten nicht öffentlich zugänglic h sind. Amazon-EM R-Cluster-Hauptkno ten können vertrauli che Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-7	Das Informati onssystem: a. Überwacht und kontrolliert die Kommunikation an der Außengrenze des Systems und an wichtigen internen Grenzen innerhalb des Systems; b. Implementiert Subnetze für öffentlic h zugängliche Systemkomponenten, die [Auswahl: physisch; logisch] von internen Organisat ionsnetzen getrennt sind; und c. Stellt eine Verbindung zu externen Netzwerke n oder Informati onssystemen nur über verwaltete Schnittstellen her, die aus Grenzschu tzgeräten bestehen, die gemäß einer Sicherheitsarchite ktur der Organisation angeordnet sind.	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) Security Groups können bei der Verwaltung des Netzwerkzugriffs helfen, indem sie eine statusbeh aftete Filterung von eingehendem und ausgehendem Netzwerkverkehr zu Ressourcen bereitste llen. AWS Wenn Sie eingehenden (oder entfernten) Datenverk ehr von 0.0.0.0/0 bis Port 22 auf Ihren Ressourcen nicht zulassen, können Sie den Remote-Zugriff einschränken.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-7	Das Informati onssystem: a. Überwacht und kontrolliert die Kommunikation an der Außengrenze des Systems und an wichtigen internen Grenzen innerhalb des Systems; b. Implementiert Subnetze für öffentlic h zugängliche Systemkomponenten, die [Auswahl: physisch; logisch] von internen Organisat ionsnetzen getrennt sind; und c. Stellt eine Verbindung zu externen Netzwerke n oder Informati onssystemen nur über verwaltete Schnittstellen her, die aus Grenzschu tzgeräten bestehen, die gemäß einer Sicherheitsarchite ktur der Organisation angeordnet sind.	lambda-function-pu blic-access-verboten	Verwalten Sie den Zugriff auf Ressource n in der AWS Cloud, indem Sie sicherste llen, dass AWS Lambda-Funktionen nicht öffentlich zugänglich sind. Der öffentliche Zugriff kann möglicherweise die Verfügbarkeit von Ressourcen beeinträc htigen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-7	Das Informati onssystem: a. Überwacht und kontrolliert die Kommunikation an der Außengrenze des Systems und an wichtigen internen Grenzen innerhalb des Systems; b. Implementiert Subnetze für öffentlic h zugängliche Systemkomponenten, die [Auswahl: physisch; logisch] von internen Organisat ionsnetzen getrennt sind; und c. Stellt eine Verbindung zu externen Netzwerke n oder Informati onssystemen nur über verwaltete Schnittstellen her, die aus Grenzschu tzgeräten bestehen, die gemäß einer Sicherheitsarchite ktur der Organisation angeordnet sind.	lambda-inside-vpc	Stellen Sie AWS Lambda-Funktionen in einer Amazon Virtual Private Cloud (Amazon VPC) bereit, um eine sichere Kommunika tion zwischen einer Funktion und anderen Diensten innerhalb der Amazon VPC zu gewährleisten. Bei dieser Konfiguration sind kein Internet-Gateway, kein NAT-Gerät und keine VPN-Verbindung erforderlich. Der gesamte Datenverk ehr bleibt sicher in der Cloud. AWS Domains, die sich innerhalb einer VPC befinden, verfügen aufgrund ihrer logischen Isolierun g im Vergleich zu Domains mit öffentlic hen Endpunkten über eine zusätzliche Sicherheitsebene. Um den Zugriff ordnungsg emäß zu verwalten,

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			sollten AWS Lambda-Funktionen einer VPC zugewiesen werden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-7	Das Informati onssystem: a. Überwacht und kontrolliert die Kommunikation an der Außengrenze des Systems und an wichtigen internen Grenzen innerhalb des Systems; b. Implementiert Subnetze für öffentlic h zugängliche Systemkomponenten, die [Auswahl: physisch; logisch] von internen Organisat ionsnetzen getrennt sind; und c. Stellt eine Verbindung zu externen Netzwerke n oder Informati onssystemen nur über verwaltete Schnittstellen her, die aus Grenzschu tzgeräten bestehen, die gemäß einer Sicherheitsarchite ktur der Organisation angeordnet sind.	rds-instance-public-access-überprüfen	Verwalten Sie den Zugriff auf Ressource n in der AWS Cloud, indem Sie sicherste llen, dass Amazon Relational Database Service (Amazon RDS) -Instance s nicht öffentlic h sind. Amazon-RDS-Datenbank-Instances können vertrauliche Informati onen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-7	Das Informationssystem: a. Überwacht und kontrolliert die Kommunikation an der Außengrenze des Systems und an wichtigen internen Grenzen innerhalb des Systems; b. Implementiert Subnetze für öffentlich zugängliche Systemkomponenten, die [Auswahl: physisch; logisch] von internen Organisationsnetzen getrennt sind; und c. Stellt eine Verbindung zu externen Netzwerken oder Informationssystemen nur über verwaltete Schnittstellen her, die aus Grenzschutzgeräten bestehen, die gemäß einer Sicherheitsarchitektur der Organisation angeordnet sind.	rds-snapshots-public-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Relational Database Service (Amazon RDS) -Instances nicht öffentlich sind. Amazon-RDS-Datenbank-Instances können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-7	Das Informationssystem: a. Überwacht und kontrolliert die Kommunikation an der Außengrenze des Systems und an wichtigen internen Grenzen innerhalb des Systems; b. Implementiert Subnetze für öffentlich zugängliche Systemkomponenten, die [Auswahl: physisch; logisch] von internen Organisationsnetzen getrennt sind; und c. Stellt eine Verbindung zu externen Netzwerken oder Informationssystemen nur über verwaltete Schnittstellen her, die aus Grenzschutzgeräten bestehen, die gemäß einer Sicherheitsarchitektur der Organisation angeordnet sind.	redshift-cluster-public-access-überprüfen	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Redshift Redshift-Cluster nicht öffentlich sind. Amazon-Redshift-Cluster können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-7	Das Informationssystem: a. Überwacht und kontrolliert die Kommunikation an der Außengrenze des Systems und an wichtigen internen Grenzen innerhalb des Systems; b. Implementiert Subnetze für öffentlich zugängliche Systemkomponenten, die [Auswahl: physisch; logisch] von internen Organisationsnetzen getrennt sind; und c. Stellt eine Verbindung zu externen Netzwerken oder Informationssystemen nur über verwaltete Schnittstellen her, die aus Grenzschutzgeräten bestehen, die gemäß einer Sicherheitsarchitektur der Organisation angeordnet sind.	restricted-common-ports	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass gemeinsame Ports für Amazon Elastic Compute Cloud (Amazon EC2) -Sicherheitsgruppen eingeschränkt sind. Wenn der Zugriff auf Ports nicht auf vertrauenswürdige Quellen beschränkt wird, kann dies zu Angriffen auf die Verfügbarkeit, Integrität und Vertraulichkeit von Systemen führen. Mit dieser Regel können Sie optional die Parameter blockedPort1–blockedPort5 festlegen (Standardkonfigurationen: 20, 21, 3389, 3306, 4333). Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-7	Das Informati onssystem: a. Überwacht und kontrolliert die Kommunikation an der Außengrenze des Systems und an wichtigen internen Grenzen innerhalb des Systems; b. Implementiert Subnetze für öffentlic h zugängliche Systemkomponenten, die [Auswahl: physisch; logisch] von internen Organisat ionsnetzen getrennt sind; und c. Stellt eine Verbindung zu externen Netzwerke n oder Informati onssystemen nur über verwaltete Schnittstellen her, die aus Grenzschu tzgeräten bestehen, die gemäß einer Sicherheitsarchite ktur der Organisation angeordnet sind.	s-3 bucket-public-read -prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie nur autorisierten Benutzern, Prozessen und Geräten Zugriff auf Amazon Simple Storage Service (Amazon S3) - Buckets gewähren. Die Verwaltung des Zugriffs sollte mit der Klassifizierung der Daten übereinst immen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-7	Das Informati onssystem: a. Überwacht und kontrolliert die Kommunikation an der Außengrenze des Systems und an wichtigen internen Grenzen innerhalb des Systems; b. Implementiert Subnetze für öffentlic h zugängliche Systemkomponenten, die [Auswahl: physisch; logisch] von internen Organisat ionsnetzen getrennt sind; und c. Stellt eine Verbindung zu externen Netzwerke n oder Informati onssystemen nur über verwaltete Schnittstellen her, die aus Grenzschu tzgeräten bestehen, die gemäß einer Sicherheitsarchite ktur der Organisation angeordnet sind.	s-3 bucket-public-writ e-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie nur autorisierten Benutzern, Prozessen und Geräten Zugriff auf Amazon Simple Storage Service (Amazon S3) - Buckets gewähren. Die Verwaltung des Zugriffs sollte mit der Klassifizierung der Daten übereinst immen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-7	Das Informationssystem: a. Überwacht und kontrolliert die Kommunikation an der Außengrenze des Systems und an wichtigen internen Grenzen innerhalb des Systems; b. Implementiert Subnetze für öffentlich zugängliche Systemkomponenten, die [Auswahl: physisch; logisch] von internen Organisationsnetzen getrennt sind; und c. Stellt eine Verbindung zu externen Netzwerken oder Informationssystemen nur über verwaltete Schnittstellen her, die aus Grenzschutzgeräten bestehen, die gemäß einer Sicherheitsarchitektur der Organisation angeordnet sind.	sagemaker-notebook-no-direct-Internetzugang	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass SageMaker Amazon-Notebooks keinen direkten Internetzugang zulassen. Indem Sie direkten Internetzugang blockieren, vermeiden Sie, dass unbefugte Benutzer auf sensible Daten zugreifen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-7	Das Informati onssystem: a. Überwacht und kontrolliert die Kommunikation an der Außengrenze des Systems und an wichtigen internen Grenzen innerhalb des Systems; b. Implementiert Subnetze für öffentlic h zugängliche Systemkomponenten, die [Auswahl: physisch; logisch] von internen Organisat ionsnetzen getrennt sind; und c. Stellt eine Verbindung zu externen Netzwerke n oder Informati onssystemen nur über verwaltete Schnittstellen her, die aus Grenzschu tzgeräten bestehen, die gemäß einer Sicherheitsarchite ktur der Organisation angeordnet sind.	vpc-default-security-group-geschlossen	Sicherheitsgruppen von Amazon Elastic Compute Cloud (Amazon EC2) können bei der Verwaltung des Netzwerkzugriffs helfen, indem sie eine statusbehaftete Filterung des ein- und ausgehenden Netzwerkverkehrs zu Ressourcen bereitstellen. AWS Die Beschränk ung des gesamten Datenverkehrs auf die Standardsicherheit sgruppe hilft dabei, den Fernzugriff auf Ihre Ressourcen einzuschränken. AWS

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-7	Das Informati onssystem: a. Überwacht und kontrolliert die Kommunikation an der Außengrenze des Systems und an wichtigen internen Grenzen innerhalb des Systems; b. Implementiert Subnetze für öffentlic h zugängliche Systemkomponenten, die [Auswahl: physisch; logisch] von internen Organisat ionsnetzen getrennt sind; und c. Stellt eine Verbindung zu externen Netzwerke n oder Informati onssystemen nur über verwaltete Schnittstellen her, die aus Grenzschu tzgeräten bestehen, die gemäß einer Sicherheitsarchite ktur der Organisation angeordnet sind.	alb-http-to-https-Weiterleitungsprüfung	Um Daten während der Übertragung zu schützen, stellen Sie sicher, dass Ihr Application Load Balancer unverschl üsselte HTTP-Anfr agen automatisch an HTTPS umleitet. Um eventuell vorhanden e sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-7	Das Informati onssystem: a. Überwacht und kontrolliert die Kommunikation an der Außengrenze des Systems und an wichtigen internen Grenzen innerhalb des Systems; b. Implementiert Subnetze für öffentlic h zugängliche Systemkomponenten, die [Auswahl: physisch; logisch] von internen Organisat ionsnetzen getrennt sind; und c. Stellt eine Verbindung zu externen Netzwerke n oder Informati onssystemen nur über verwaltete Schnittstellen her, die aus Grenzschu tzgeräten bestehen, die gemäß einer Sicherheitsarchite ktur der Organisation angeordnet sind.	elb-tls-https-listeners-nur	Stellen Sie sicher, dass Ihre Elastic Load Balancer (ELBs) mit SSL- oder HTTPS-Listenern konfiguriert sind. Um eventuell vorhanden e sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-7	Das Informationssystem: a. Überwacht und kontrolliert die Kommunikation an der Außengrenze des Systems und an wichtigen internen Grenzen innerhalb des Systems; b. Implementiert Subnetze für öffentlich zugängliche Systemkomponenten, die [Auswahl: physisch; logisch] von internen Organisationsnetzen getrennt sind; und c. Stellt eine Verbindung zu externen Netzwerken oder Informationssystemen nur über verwaltete Schnittstellen her, die aus Grenzschutzgeräten bestehen, die gemäß einer Sicherheitsarchitektur der Organisation angeordnet sind.	s-3 bucket-ssl-requests-only	Um Daten während der Übertragung zu schützen, stellen Sie sicher, dass Ihre Amazon Simple Storage Service (Amazon S3)-Buckets Anfragen zur Verwendung von Secure Socket Layer (SSL)-Buckets erfordern. Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-7	Das Informationssystem: a. Überwacht und kontrolliert die Kommunikation an der Außengrenze des Systems und an wichtigen internen Grenzen innerhalb des Systems; b. Implementiert Subnetze für öffentlich zugängliche Systemkomponenten, die [Auswahl: physisch; logisch] von internen Organisationsnetzen getrennt sind; und c. Stellt eine Verbindung zu externen Netzwerken oder Informationssystemen nur über verwaltete Schnittstellen her, die aus Grenzschutzgeräten bestehen, die gemäß einer Sicherheitsarchitektur der Organisation angeordnet sind.	redshift-require-tls-ssl	Stellen Sie sicher, dass Ihre Amazon-Redshift-Cluster eine TLS/SSL-Verschlüsselung erfordern, um eine Verbindung zu SQL-Clients herzustellen. Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-7	Das Informati onssystem: a. Überwacht und kontrolliert die Kommunikation an der Außengrenze des Systems und an wichtigen internen Grenzen innerhalb des Systems; b. Implementiert Subnetze für öffentlic h zugängliche Systemkomponenten, die [Auswahl: physisch; logisch] von internen Organisat ionsnetzen getrennt sind; und c. Stellt eine Verbindung zu externen Netzwerke n oder Informati onssystemen nur über verwaltete Schnittstellen her, die aus Grenzschu tzgeräten bestehen, die gemäß einer Sicherheitsarchite ktur der Organisation angeordnet sind.	alb-waf-enabled	Stellen Sie sicher, dass AWS WAF auf Elastic Load Balancers (ELB) aktiviert ist, um Webanwendungen zu schützen. Eine WAF trägt zum Schutz Ihrer Webanwend ungen oder APIs vor gängigen Web-Explo its bei. Diese Web-Exploits können sich auf die Verfügbar keit auswirken, die Sicherheit gefährden oder übermäßige Ressourcen in Ihrer Umgebung verbrauch en.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-7	Das Informationssystem: a. Überwacht und kontrolliert die Kommunikation an der Außengrenze des Systems und an wichtigen internen Grenzen innerhalb des Systems; b. Implementiert Subnetze für öffentlich zugängliche Systemkomponenten, die [Auswahl: physisch; logisch] von internen Organisationsnetzen getrennt sind; und c. Stellt eine Verbindung zu externen Netzwerken oder Informationssystemen nur über verwaltete Schnittstellen her, die aus Grenzschutzgeräten bestehen, die gemäß einer Sicherheitsarchitektur der Organisation angeordnet sind.	vpc-sg-open-only-to-authorized-ports	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass gemeinsame Ports für Amazon Elastic Compute Cloud (Amazon EC2) -Sicherheitsgruppen eingeschränkt sind. Wenn der Zugriff auf Ports nicht auf vertrauenswürdige Quellen beschränkt wird, kann dies zu Angriffen auf die Verfügbarkeit, Integrität und Vertraulichkeit von Systemen führen. Durch die Beschränkung des Zugriffs auf Ressourcen innerhalb einer Sicherheitsgruppe aus dem Internet (0.0.0.0/0) kann der Remote-Zugriff auf interne Systeme gesteuert werden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-7	Das Informationssystem: a. Überwacht und kontrolliert die Kommunikation an der Außengrenze des Systems und an wichtigen internen Grenzen innerhalb des Systems; b. Implementiert Subnetze für öffentlich zugängliche Systemkomponenten, die [Auswahl: physisch; logisch] von internen Organisationsnetzen getrennt sind; und c. Stellt eine Verbindung zu externen Netzwerken oder Informationssystemen nur über verwaltete Schnittstellen her, die aus Grenzschutzgeräten bestehen, die gemäß einer Sicherheitsarchitektur der Organisation angeordnet sind.	elasticsearch-node-to-node-Verschlüsselungsprüfung	Stellen Sie sicher, dass die node-to-node Verschlüsselung für Amazon OpenSearch Service aktiviert ist. Node-to-nodeVerschlüsselung ermöglicht die TLS 1.2-Verschlüsselung für die gesamte Kommunikation innerhalb der Amazon Virtual Private Cloud (Amazon VPC). Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-7	Das Informati onssystem: a. Überwacht und kontrolliert die Kommunikation an der Außengrenze des Systems und an wichtigen internen Grenzen innerhalb des Systems; b. Implementiert Subnetze für öffentlic h zugängliche Systemkomponenten, die [Auswahl: physisch; logisch] von internen Organisat ionsnetzen getrennt sind; und c. Stellt eine Verbindung zu externen Netzwerke n oder Informati onssystemen nur über verwaltete Schnittstellen her, die aus Grenzschu tzgeräten bestehen, die gemäß einer Sicherheitsarchite ktur der Organisation angeordnet sind.	account-level-publ ic-accesss3-Blöcke-periodisch	Verwalten Sie den Zugriff auf Ressource n in der AWS Cloud, indem Sie sicherste llen, dass Amazon Simple Storage Service (Amazon S3) -Buckets nicht öffentlich zugänglic h sind. Diese Regel trägt dazu bei, sensible Daten vor unbefugten Remote-Benutzern zu schützen, indem sie den öffentlichen Zugriff verhinder t. Mit dieser Regel können Sie optional die Parameter ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) und restrictPublicBuck ets Parameter (Config Default: True) festlegen. Die tatsächlichen Werte müssen den Richtlini

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			en Ihrer Organisation entsprechen.
SC-7	Das Informati onssystem: a. Überwacht und kontrolliert die Kommunikation an der Außengrenze des Systems und an wichtigen internen Grenzen innerhalb des Systems; b. Implementiert Subnetze für öffentlic h zugängliche Systemkomponenten, die [Auswahl: physisch; logisch] von internen Organisat ionsnetzen getrennt sind; und c. Stellt eine Verbindung zu externen Netzwerke n oder Informati onssystemen nur über verwaltete Schnittstellen her, die aus Grenzschu tzgeräten bestehen, die gemäß einer Sicherheitsarchite ktur der Organisation angeordnet sind.	subnet-auto-assign-public-ip-deaktiviert	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon Virtual Private Cloud (VPC) -Subnetzen nicht automatisch eine öffentliche IP-Adress e zugewiesen wird. Amazon Elastic Compute Cloud (EC2) -Instances, die in Subnetzen gestartet werden, in denen dieses Attribut aktiviert ist, haben ihrer primären Netzwerkschnittste lle eine öffentliche IP-Adresse zugewiesen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-7	Das Informati onssystem: a. Überwacht und kontrolliert die Kommunikation an der Außengrenze des Systems und an wichtigen internen Grenzen innerhalb des Systems; b. Implementiert Subnetze für öffentlic h zugängliche Systemkomponenten, die [Auswahl: physisch; logisch] von internen Organisat ionsnetzen getrennt sind; und c. Stellt eine Verbindung zu externen Netzwerke n oder Informati onssystemen nur über verwaltete Schnittstellen her, die aus Grenzschu tzgeräten bestehen, die gemäß einer Sicherheitsarchite ktur der Organisation angeordnet sind.	s3 bucket-level-public-access - verboten	Verwalten Sie den Zugriff auf Ressource n in der AWS Cloud, indem Sie sicherste llen, dass Amazon Simple Storage Service (Amazon S3) -Buckets nicht öffentlich zugänglic h sind. Diese Regel trägt dazu bei, sensible Daten vor unbefugten Remote-Benutzern zu schützen, indem sie den öffentlichen Zugriff auf Bucket-Eb ene verhindert.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-7(3)	Die Organisation begrenzt die Anzahl der externen Netzwerkverbindungen zum Informationssystem.	ec2- instances-in-vpc	Stellen Sie Amazon Elastic Compute Cloud (Amazon EC2) -Instances innerhalb einer Amazon Virtual Private Cloud (Amazon VPC) bereit, um eine sichere Kommunikation zwischen einer Instance und anderen Services innerhalb der Amazon VPC zu ermöglichen, ohne dass ein Internet-Gateway, ein NAT-Gerät oder eine VPN-Verbindung erforderlich ist. Der gesamte Datenverkehr bleibt sicher in der AWS Cloud. Domains, die sich innerhalb einer VPC befinden, verfügen aufgrund ihrer logischen Isolierung im Vergleich zu Domains mit öffentlichen Endpunkten über eine zusätzliche Sicherheitsebene. Weisen Sie EC2

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			Amazon-Instances einer Amazon-VPC zu, um den Zugriff ordnungsgemäß zu verwalten.
SC-7(3)	Die Organisation begrenzt die Anzahl der externen Netzwerkverbindungen zum Informationssystem.	dms-replication-not-public	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass auf DMS-Replikationsinstanzen nicht öffentlich zugegriffen werden kann. DMS-Replikations-Instances können vertrauliche Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-7(3)	Die Organisation begrenzt die Anzahl der externen Netzwerkverbindungen zum Informationssystem.	ebs-snapshot-public-restorable-überprüfen	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass EBS-Snapshots nicht öffentlich wiederherstellbar sind. EBS-Volume-Snapshots können vertrauliche Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.
SC-7(3)	Die Organisation begrenzt die Anzahl der externen Netzwerkverbindungen zum Informationssystem.	ec2- instance-no-public-ip	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon Elastic Compute Cloud (Amazon EC2) - Instances nicht öffentlich zugänglich sind. EC2 Amazon-Instances können vertrauliche Informationen enthalten, und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-7(3)	Die Organisation begrenzt die Anzahl der externen Netzwerkverbindungen zum Informationssystem.	elasticsearch-in-vpc-only	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass sich Amazon OpenSearch OpenSearch Service (Service) - Domains innerhalb einer Amazon Virtual Private Cloud (Amazon VPC) befinden. Eine OpenSearch Service-Domain innerhalb einer Amazon VPC ermöglicht die sichere Kommunikation zwischen OpenSearch Service und anderen Services innerhalb der Amazon VPC, ohne dass ein Internet-Gateway, ein NAT-Gerät oder eine VPN-Verbindung erforderlich ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-7(3)	Die Organisation begrenzt die Anzahl der externen Netzwerkverbindungen zum Informationssystem.	emr-master-no-public-ip	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon EMR-Cluster-Masterknoten nicht öffentlich zugänglich sind. Amazon-EMR-Cluster-Hauptknoten können vertrauliche Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-7(3)	Die Organisat ion begrenzt die Anzahl der externen Netzwerkverbindung en zum Informati onssystem.	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) Security Groups können bei der Verwaltung des Netzwerkzugriffs helfen, indem sie eine statusbeh aftete Filterung von eingehendem und ausgehendem Netzwerkverkehr zu Ressourcen bereitste llen. AWS Wenn Sie eingehenden (oder entfernten) Datenverk ehr von 0.0.0.0/0 bis Port 22 auf Ihren Ressourcen nicht zulassen, können Sie den Remote-Zugriff einschränken.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-7(3)	Die Organisation begrenzt die Anzahl der externen Netzwerkverbindungen zum Informationssystem.	lambda-function-public-access-verboten	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass AWS Lambda-Funktionen nicht öffentlich zugänglich sind. Der öffentliche Zugriff kann möglicherweise die Verfügbarkeit von Ressourcen beeinträchtigen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-7(3)	Die Organisation begrenzt die Anzahl der externen Netzwerkverbindungen zum Informationssystem.	lambda-inside-vpc	Stellen Sie AWS Lambda-Funktionen in einer Amazon Virtual Private Cloud (Amazon VPC) bereit, um eine sichere Kommunikation zwischen einer Funktion und anderen Diensten innerhalb der Amazon VPC zu gewährleisten. Bei dieser Konfiguration sind kein Internet-Gateway, kein NAT-Gerät und keine VPN-Verbindung erforderlich. Der gesamte Datenverkehr bleibt sicher in der Cloud. AWS Domains, die sich innerhalb einer VPC befinden, verfügen aufgrund ihrer logischen Isolierung im Vergleich zu Domains mit öffentlichen Endpunkten über eine zusätzliche Sicherheitsebene. Um den Zugriff ordnungsgemäß zu verwalten,

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			sollten AWS Lambda-Funktionen einer VPC zugewiesen werden.
SC-7(3)	Die Organisation begrenzt die Anzahl der externen Netzwerkverbindungen zum Informationssystem.	rds-instance-public-access-überprüfen	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Relational Database Service (Amazon RDS) -Instances nicht öffentlich sind. Amazon-RDS-Datenbank-Instances können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-7(3)	Die Organisation begrenzt die Anzahl der externen Netzwerkverbindungen zum Informationssystem.	rds-snapshots-public-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Relational Database Service (Amazon RDS) -Instances nicht öffentlich sind. Amazon-RDS-Datenbank-Instances können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-7(3)	Die Organisation begrenzt die Anzahl der externen Netzwerkverbindungen zum Informationssystem.	redshift-cluster-public-access-überprüfen	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Redshift Redshift-Cluster nicht öffentlich sind. Amazon-Redshift-Cluster können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-7(3)	Die Organisation begrenzt die Anzahl der externen Netzwerkverbindungen zum Informationssystem.	restricted-common-ports	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass gemeinsame Ports für Amazon Elastic Compute Cloud (Amazon EC2) -Sicherheitsgruppen eingeschränkt sind. Wenn der Zugriff auf Ports nicht auf vertrauenswürdige Quellen beschränkt wird, kann dies zu Angriffen auf die Verfügbarkeit, Integrität und Vertraulichkeit von Systemen führen. Mit dieser Regel können Sie optional die Parameter blockedPort1–blockedPort5 festlegen (Standardkonfigurationen: 20, 21, 3389, 3306, 4333). Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-7(3)	Die Organisation begrenzt die Anzahl der externen Netzwerkverbindungen zum Informationssystem.	s-3 bucket-public-read-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie nur autorisierten Benutzern, Prozessen und Geräten Zugriff auf Amazon Simple Storage Service (Amazon S3) - Buckets gewähren. Die Verwaltung des Zugriffs sollte mit der Klassifizierung der Daten übereinstimmen.
SC-7(3)	Die Organisation begrenzt die Anzahl der externen Netzwerkverbindungen zum Informationssystem.	s-3 bucket-public-write-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie nur autorisierten Benutzern, Prozessen und Geräten Zugriff auf Amazon Simple Storage Service (Amazon S3) - Buckets gewähren. Die Verwaltung des Zugriffs sollte mit der Klassifizierung der Daten übereinstimmen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-7(3)	Die Organisation begrenzt die Anzahl der externen Netzwerkverbindungen zum Informationssystem.	sagemaker-notebook-no-direct-Internetzugang	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass SageMaker Amazon-Notebooks keinen direkten Internetzugang zulassen. Indem Sie direkten Internetzugang blockieren, vermeiden Sie, dass unbefugte Benutzer auf sensible Daten zugreifen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-7(3)	Die Organisat ion begrenzt die Anzahl der externen Netzwerkverbindung en zum Informati onssystem.	vpc-default-security-group-geschlossen	Sicherheitsgruppen von Amazon Elastic Compute Cloud (Amazon EC2) können bei der Verwaltung des Netzwerkzugriffs helfen, indem sie eine statusbehaftete Filterung des ein- und ausgehenden Netzwerkverkehrs zu Ressourcen bereitstellen. AWS Die Beschränk ung des gesamten Datenverkehrs auf die Standardsicherheit sgruppe hilft dabei, den Fernzugriff auf Ihre Ressourcen einzuschränken. AWS

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-7(3)	Die Organisation begrenzt die Anzahl der externen Netzwerkverbindungen zum Informationssystem.	vpc-sg-open-only-to-authorized-ports	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass gemeinsame Ports für Amazon Elastic Compute Cloud (Amazon EC2) -Sicherheitsgruppen eingeschränkt sind. Wenn der Zugriff auf Ports nicht auf vertrauenswürdige Quellen beschränkt wird, kann dies zu Angriffen auf die Verfügbarkeit, Integrität und Vertraulichkeit von Systemen führen. Durch die Beschränkung des Zugriffs auf Ressourcen innerhalb einer Sicherheitsgruppe aus dem Internet (0.0.0.0/0) kann der Remote-Zugriff auf interne Systeme gesteuert werden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-7(3)	Die Organisation begrenzt die Anzahl der externen Netzwerkverbindungen zum Informationssystem.	account-level-public-accesss3-Blöcke-periodisch	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Simple Storage Service (Amazon S3) -Buckets nicht öffentlich zugänglich sind. Diese Regel trägt dazu bei, sensible Daten vor unbefugten Remote-Benutzern zu schützen, indem sie den öffentlichen Zugriff verhindert. Mit dieser Regel können Sie optional die Parameter ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) und restrictPublicBuckets Parameter (Config Default: True) festlegen. Die tatsächlichen Werte müssen den Richtlini

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			en Ihrer Organisation entsprechen.
SC-7(3)	Die Organisat ion begrenzt die Anzahl der externen Netzwerkverbindung en zum Informati onssystem.	s3 bucket-level-public-access - verboten	Verwalten Sie den Zugriff auf Ressource n in der AWS Cloud, indem Sie sicherste llen, dass Amazon Simple Storage Service (Amazon S3) -Buckets nicht öffentlich zugänglic h sind. Diese Regel trägt dazu bei, sensible Daten vor unbefugten Remote-Benutzern zu schützen, indem sie den öffentlichen Zugriff auf Bucket-Eb ene verhindert.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-7(3)	Die Organisation begrenzt die Anzahl der externen Netzwerkverbindungen zum Informationssystem.	ssm-document-not-public	Stellen Sie sicher, dass AWS Systems Manager (SSM) - Dokumente nicht öffentlich sind, da dies einen unbeabsichtigten Zugriff auf Ihre SSM-Dokumente ermöglichen kann. Ein öffentliches SSM-Dokument kann Informationen über Ihr Konto, Ihre Ressourcen und internen Prozesse preisgeben.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-7(3)	Die Organisation begrenzt die Anzahl der externen Netzwerkverbindungen zum Informationssystem.	subnet-auto-assign-public-ip-deaktiviert	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon Virtual Private Cloud (VPC) -Subnetzen nicht automatisch eine öffentliche IP-Adresse zugewiesen wird. Amazon Elastic Compute Cloud (EC2) -Instances, die in Subnetzen gestartet werden, in denen dieses Attribut aktiviert ist, haben ihrer primären Netzwerkschnittstelle eine öffentliche IP-Adresse zugewiesen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-7(3)	Die Organisat ion begrenzt die Anzahl der externen Netzwerkverbindung en zum Informati onssystem.	autoscaling-launch -config-public-ip- deaktiviert	Wenn Sie Ihre Netzwerkschnittstellen mit einer öffentlichen IP-Adresse konfiguri eren, sind die diesen Netzwerkschnittste llen zugehörigen Ressourcen über das Internet erreichba r. EC2 Ressourcen sollten nicht öffentlic h zugänglich sein, da dies einen unbeabsic htigten Zugriff auf Ihre Anwendungen oder Server ermöglichen kann.
SC-8	Das Informati onssystem schützt die Vertraulichkeit UND Integrität der übermittelten Informati onen.	alb-http-to-https- Weiterleitungsprüfung	Um Daten während der Übertragung zu schützen, stellen Sie sicher, dass Ihr Application Load Balancer unverschl üsselte HTTP-Anfr agen automatisch an HTTPS umleitet. Um eventuell vorhanden e sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-8	Das Informationssystem schützt die Vertraulichkeit UND Integrität der übermittelten Informationen.	elasticsearch-node-to-node-Verschlüsselungsprüfung	Stellen Sie sicher, dass die node-to-node Verschlüsselung für Amazon OpenSearch Service aktiviert ist. Node-to-nodeVerschlüsselung ermöglicht die TLS 1.2-Verschlüsselung für die gesamte Kommunikation innerhalb der Amazon Virtual Private Cloud (Amazon VPC). Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.
SC-8	Das Informationssystem schützt die Vertraulichkeit UND Integrität der übermittelten Informationen.	elb-tls-https-listeners-nur	Stellen Sie sicher, dass Ihre Elastic Load Balancer (ELBs) mit SSL- oder HTTPS-Listenern konfiguriert sind. Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-8	Das Informati onssystem schützt die Vertraulichkeit UND Integrität der übermittelten Informati onen.	redshift-require-tls-ssl	Stellen Sie sicher, dass Ihre Amazon-Redshift-Cluster eine TLS/SSL-Verschlüss elung erfordern, um eine Verbindun g zu SQL-Clients herzustellen. Um eventuell vorhanden e sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.
SC-8	Das Informati onssystem schützt die Vertraulichkeit UND Integrität der übermittelten Informati onen.	s-3 bucket-ssl-request s-only	Um Daten während der Übertragung zu schützen, stellen Sie sicher, dass Ihre Amazon Simple Storage Service (Amazon S3)-Bucke ts Anfragen zur Verwendung von Secure Socket Layer (SSL)-Buc kets erfordern. Um eventuell vorhanden e sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-8	Das Informati onssystem schützt die Vertraulichkeit UND Integrität der übermittelten Informati onen.	api-gw-ssl-enabled	Stellen Sie sicher, dass die REST-API-Stufen von Amazon API Gateway mit SSL-Zertifikaten konfiguri ert sind, damit Backend-Systeme überprüfen können, ob Anforderungen von API Gateway stammen.
SC-8(1)	Das Informati onssystem setzt kryptographische Mechanismen ein, um während der Übertragung [Auswahl (eine oder mehrere Optionen): eine unbefugte Offenlegu ng von Informati onen zu verhinder n; Änderungen an Informationen zu erkennen], sofern sie nicht anderweit ig durch [Zuweisung: von der Organisation definierte alternative physische Schutzmaß nahmen] geschützt sind.	alb-http-to-https-Weiterleitungsprüfung	Um Daten während der Übertragung zu schützen, stellen Sie sicher, dass Ihr Application Load Balancer unverschl üsselte HTTP-Anfr agen automatisch an HTTPS umleitet. Um eventuell vorhanden e sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-8(1)	Das Informationssystem setzt kryptographische Mechanismen ein, um während der Übertragung [Auswahl (eine oder mehrere Optionen): eine unbefugte Offenlegung von Informationen zu verhindern; Änderungen an Informationen zu erkennen], sofern sie nicht anderweitig durch [Zuweisung: von der Organisation definierte alternative physische Schutzmaßnahmen] geschützt sind.	elasticsearch-node-to-node-Verschlüsselungsprüfung	Stellen Sie sicher, dass die node-to-node Verschlüsselung für Amazon OpenSearch Service aktiviert ist. Node-to-nodeVerschlüsselung ermöglicht die TLS 1.2-Verschlüsselung für die gesamte Kommunikation innerhalb der Amazon Virtual Private Cloud (Amazon VPC). Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-8(1)	Das Informationssystem setzt kryptographische Mechanismen ein, um während der Übertragung [Auswahl (eine oder mehrere Optionen): eine unbefugte Offenlegung von Informationen zu verhindern; Änderungen an Informationen zu erkennen], sofern sie nicht anderweitig durch [Zuweisung: von der Organisation definierte alternative physische Schutzmaßnahmen] geschützt sind.	elb-tls-https-listeners-nur	Stellen Sie sicher, dass Ihre Elastic Load Balancer (ELBs) mit SSL- oder HTTPS-Listenern konfiguriert sind. Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-8(1)	Das Informationssystem setzt kryptographische Mechanismen ein, um während der Übertragung [Auswahl (eine oder mehrere Optionen): eine unbefugte Offenlegung von Informationen zu verhindern; Änderungen an Informationen zu erkennen], sofern sie nicht anderweitig durch [Zuweisung: von der Organisation definierte alternative physische Schutzmaßnahmen] geschützt sind.	redshift-require-tls-ssl	Stellen Sie sicher, dass Ihre Amazon-Redshift-Cluster eine TLS/SSL-Verschlüsselung erfordern, um eine Verbindung zu SQL-Clients herzustellen. Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-8(1)	Das Informationssystem setzt kryptographische Mechanismen ein, um während der Übertragung [Auswahl (eine oder mehrere Optionen): eine unbefugte Offenlegung von Informationen zu verhindern; Änderungen an Informationen zu erkennen], sofern sie nicht anderweitig durch [Zuweisung: von der Organisation definierte alternative physische Schutzmaßnahmen] geschützt sind.	s-3 bucket-ssl-requests-only	Um Daten während der Übertragung zu schützen, stellen Sie sicher, dass Ihre Amazon Simple Storage Service (Amazon S3)-Buckets Anfragen zur Verwendung von Secure Socket Layer (SSL)-Buckets erfordern. Da sensible Daten vorhanden sein können, sollten Sie die Verschlüsselung bei der Übertragung aktivieren, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-8(1)	Das Informati onssystem setzt kryptographische Mechanismen ein, um während der Übertragung [Auswahl (eine oder mehrere Optionen): eine unbefugte Offenlegu ng von Informati onen zu verhinder n; Änderungen an Informationen zu erkennen], sofern sie nicht anderweit ig durch [Zuweisung: von der Organisation definierte alternative physische Schutzmaß nahmen] geschützt sind.	api-gw-ssl-enabled	Stellen Sie sicher, dass die REST-API-Stufen von Amazon API Gateway mit SSL-Zertifikaten konfiguri ert sind, damit Backend-Systeme überprüfen können, ob Anforderungen von API Gateway stammen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SI-12	Die Organisation verarbeitet und speichert die Informationen innerhalb des Informationssysteme und die aus dem System ausgegebenen Informationen gemäß den geltenden Bundesgesetzen, Verordnungen, Richtlinien, Richtlinien, Vorschriften, Standards und betrieblichen Anforderungen.	s-3 bucket-versioning-enabled	Die Versionsverwaltung von Amazon Simple Storage Service (Amazon S3)-Buckets hilft dabei, mehrere Varianten eines Objekts im selben Amazon-S3-Bucket zu speichern. Verwenden Sie die Versionsverwaltung, um sämtliche Versionen aller Objekte in Ihrem Amazon-S3-Bucket zu speichern, abzurufen oder wiederherzustellen. Mit der Versionsverwaltung können Sie Versionen sowohl nach unbeabsichtigten Benutzeraktionen als auch nach Anwendungsfehlern problemlos wiederherstellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SI-12	Die Organisation verarbeitet und speichert die Informationen innerhalb des Informationssystems und die aus dem System ausgegebenen Informationen gemäß den geltenden Bundesgesetzen, Verordnungen, Richtlinien, Richtlinien, Vorschriften, Standards und betrieblichen Anforderungen.	db-instance-backup-enabled	Die Sicherungsfunktion von Amazon RDS erstellt Sicherungen Ihrer Datenbanken und Transaktionsprotokolle. Amazon RDS erstellt einen Snapshot für das Speichervolume Ihrer DB-Instance, sodass die gesamte DB-Instance gesichert wird. Sie können im System spezifische Aufbewahrungsfristen festlegen, um Ihre Ausfallsicherheitsanforderungen zu erfüllen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SI-12	Die Organisation verarbeitet und speichert die Informationen innerhalb des Informationssystems und die aus dem System ausgegebenen Informationen gemäß den geltenden Bundesgesetzen, Verordnungen, Richtlinien, Richtlinien, Vorschriften, Standards und betrieblichen Anforderungen.	dynamodb-pitr-enabled	Aktivieren Sie diese Regel, um zu überprüfen, ob die Informationen gesichert wurden. Es verwaltet auch die Backups, indem es sicherstellt, dass die point-in-time Wiederherstellung in Amazon DynamoDB aktiviert ist. Bei der Wiederherstellung werden fortlaufende Backups Ihrer Tabelle für die letzten 35 Tage gespeichert.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SI-12	Die Organisation verarbeitet und speichert die Informati onen innerhalb des Informationssystem s und die aus dem System ausgegebe nen Informati onen gemäß den geltenden Bundesges etzen, Verordnun gen, Richtlinien, Richtlinien, Vorschrif ten, Standards und betrieblichen Anforderungen.	elasticache-redis-cluster-automatic-Backup-Check	Wenn automatische Backups aktiviert sind, ElastiCache erstellt Amazon täglich ein Backup des Clusters. Die Sicherung kann für eine von Ihrer Organisation festgelegte Anzahl von Tagen aufbewahrt werden. Automatische Backups schützen vor Datenverlust. Bei einem Ausfall können Sie einen neuen Cluster erstellen, der Ihre Daten aus dem aktuellen Backup wiederherstellt.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SI-12	Die Organisation verarbeitet und speichert die Informationen innerhalb des Informationssystems und die aus dem System ausgegebenen Informationen gemäß den geltenden Bundesgesetzen, Verordnungen, Richtlinien, Richtlinien, Vorschriften, Standards und betrieblichen Anforderungen.	cw-loggroup-retention-period-überprüfen	Stellen Sie sicher, dass die Ereignisprotokolldaten für Ihre Protokollgruppen über eine Mindestdauer aufbewahrt werden, um die Fehlerbehebung und forensische Untersuchungen zu unterstützen. Fehlende frühere Ereignisprotokolldaten erschweren die Rekonstruierung und Identifizierung potenziell schädlicher Ereignisse.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SI-12	Die Organisation verarbeitet und speichert die Informationen innerhalb des Informationssystems und die aus dem System ausgegebenen Informationen gemäß den geltenden Bundesgesetzen, Verordnungen, Richtlinien, Richtlinien, Vorschriften, Standards und betrieblichen Anforderungen.	redshift-backup-enabled	Stellen Sie zur Unterstützung der Datensicherungsprozesse sicher, dass Ihre Amazon-Redshift-Cluster über automatisierte Snapshots verfügen. Wenn automatisierte Snapshots für einen Cluster aktiviert sind, erstellt Redshift in regelmäßigen Abständen Snapshots dieses Clusters. Standardmäßig erzeugt Redshift ungefähr alle acht Stunden oder nach 5 GB geänderten Daten pro Knoten einen Snapshot, je nachdem, was zuerst auftritt.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SI-12	Die Organisation verarbeitet und speichert die Informationen innerhalb des Informationssystems und die aus dem System ausgegebenen Informationen gemäß den geltenden Bundesgesetzen, Verordnungen, Richtlinien, Richtlinien, Vorschriften, Standards und betrieblichen Anforderungen.	backup-plan-min-frequency-and-min-retention-check	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihr AWS Backup-Plan auf eine Mindestfrequenz und Aufbewahrung festgelegt ist. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen. Mit dieser Regel können Sie die Parameter requiredFrequencyValue (Config default: 1), requiredRetentionDays (Config default: 35) und requiredFrequencyUnit

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			(Config default: days) festlegen. Der tatsächliche Wert muss den Anforderungen Ihrer Organisation entsprechen.
SI-12	Die Organisation verarbeitet und speichert die Informationen innerhalb des Informationssystems und die aus dem System ausgegebenen Informationen gemäß den geltenden Bundesgesetzen, Verordnungen, Richtlinien, Richtlinien, Vorschriften, Standards und betrieblichen Anforderungen.	fsx-resources-protected-by-Backup-Plan	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre FSx Amazon-Dateisysteme Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SI-12	Die Organisation verarbeitet und speichert die Informationen innerhalb des Informationssystems und die aus dem System ausgegebenen Informationen gemäß den geltenden Bundesgesetzen, Verordnungen, Richtlinien, Richtlinien, Vorschriften, Standards und betrieblichen Anforderungen.	ec2--Plan resources-protected-by-backup	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon Elastic Compute Cloud (Amazon EC2) -Ressourcen Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SI-12	Die Organisation verarbeitet und speichert die Informationen innerhalb des Informationssystems und die aus dem System ausgegebenen Informationen gemäß den geltenden Bundesgesetzen, Verordnungen, Richtlinien, Richtlinien, Vorschriften, Standards und betrieblichen Anforderungen.	aurora-resources-protected-by-Backup-Plan	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon Aurora Aurora-Ressourcen Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SI-12	Die Organisation verarbeitet und speichert die Informationen innerhalb des Informationssystems und die aus dem System ausgegebenen Informationen gemäß den geltenden Bundesgesetzen, Verordnungen, Richtlinien, Richtlinien, Vorschriften, Standards und betrieblichen Anforderungen.	dynamodb-resources-protected-by-Backup-Plan	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon DynamoDB DynamoDB-Ressourcen Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SI-12	Die Organisation verarbeitet und speichert die Informationen innerhalb des Informationssystems und die aus dem System ausgegebenen Informationen gemäß den geltenden Bundesgesetzen, Verordnungen, Richtlinien, Richtlinien, Vorschriften, Standards und betrieblichen Anforderungen.	ebs-resources-protected-by-Backup-Plan	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon Elastic Block Store (Amazon EBS) -Ressourcen Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SI-12	Die Organisation verarbeitet und speichert die Informationen innerhalb des Informationssystems und die aus dem System ausgegebenen Informationen gemäß den geltenden Bundesgesetzen, Verordnungen, Richtlinien, Richtlinien, Vorschriften, Standards und betrieblichen Anforderungen.	efs-resources-protected-by-Backup-Plan	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon Elastic File System (Amazon EFS) -Dateisysteme Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SI-12	Die Organisation verarbeitet und speichert die Informationen innerhalb des Informationssystems und die aus dem System ausgegebenen Informationen gemäß den geltenden Bundesgesetzen, Verordnungen, Richtlinien, Richtlinien, Vorschriften, Standards und betrieblichen Anforderungen.	rds-resources-protected-by-Backup-Plan	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon Relational Database Service (Amazon RDS) -Ressourcen Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SI-2(2)	Die Organisation setzt automatisierte Mechanismen mindestens einmal im Monat ein, um den Zustand der Komponenten des Informationssystems im Hinblick auf die Behebung von Fehlern zu bestimmen.	ec2-prüfen managedinstance-patch-compliance-status	Aktivieren Sie diese Regel, um bei der Identifizierung und Dokumentation von Sicherheitslücken in Amazon Elastic Compute Cloud (Amazon EC2) zu helfen. Die Regel prüft, ob die EC2 Amazon-Instance die Patch-Konformität im AWS Systems Manager gemäß den Richtlinien und Verfahren Ihrer Organisation einhält.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SI-2(2)	Die Organisation setzt automatisierte Mechanismen mindestens einmal im Monat ein, um den Zustand der Komponenten des Informationssystems im Hinblick auf die Behebung von Fehlern zu bestimmen.	ec2-managerinstance-managed-by-systems	Eine Bestandsaufnahme der Softwareplattformen und Anwendungen innerhalb des Unternehmens ist möglich, indem Amazon Elastic Compute Cloud (Amazon EC2) - Instances mit AWS Systems Manager verwaltet werden. Verwenden Sie AWS Systems Manager, um detaillierte Systemkonfigurationen, Betriebssystem-Patch-Levels, Namen und Typ der Dienste, Softwareinstallationen, Anwendungsname, Herausgeber und Version sowie andere Details zu Ihrer Umgebung bereitzustellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SI-2(2)	Die Organisation setzt automatisierte Mechanismen mindestens einmal im Monat ein, um den Zustand der Komponenten des Informationssystems im Hinblick auf die Behebung von Fehlern zu bestimmen.	ec2-prüfen managedinstance-association-compliance-status	Verwenden Sie AWS Systems Manager Associations, um bei der Inventarisierung von Softwareplattformen und Anwendungen innerhalb eines Unternehmens zu helfen. AWS Systems Manager weist Ihren verwalteten Instanzen einen Konfigurationsstatus zu und ermöglicht es Ihnen, Basiswerte für Betriebssystem-Patch-Levels, Softwareinstallationen, Anwendungskonfigurationen und andere Details zu Ihrer Umgebung festzulegen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SI-2(2)	Die Organisation setzt automatisierte Mechanismen mindestens einmal im Monat ein, um den Zustand der Komponenten des Informationssystems im Hinblick auf die Behebung von Fehlern zu bestimmen.	elastic-beanstalk-managed-updates-aktiviert	Durch die Aktivierung verwalteter Plattformupdates für eine Amazon-Elastic-Beanstalk-Umgebung wird sichergestellt, dass die aktuellen verfügbaren Plattform-Fixes, -Updates und -Features für die Umgebung installiert sind. Eine bewährte Methode zur Sicherung von Systemen besteht darin, stets die aktuellen Patches zu installieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SI-4(1)	Die Organisation verbindet und konfiguriert die einzelnen Intrusion-Detection-Tools zu einem informationssystemweiten Intrusion-Detection-System.	guardduty-enabled-centralized	Amazon GuardDuty kann mithilfe von Threat Intelligence Feeds helfen, potenzielle Cybersicherheitsereignisse zu überwachen und zu erkennen. Dazu gehören Listen mit bösartigen IPs und maschinellen Lernmethoden zur Identifizierung unerwarteter, nicht autorisierter und bösartiger Aktivitäten in Ihrer AWS Cloud-Umgebung.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SI-4(16)	Die Organisation korreliert Informati onen aus Überwachu ngstools, die im gesamten Informati onssystem eingesetzt werden.	guardduty-enabled-centralized	Amazon GuardDuty kann mithilfe von Threat Intellige nce Feeds helfen, potenzielle Cybersich erheitsereignisse zu überwachen und zu erkennen. Dazu gehören Listen mit bösartigen IPs und maschinel len Lernmethoden zur Identifizierung unerwarteter, nicht autorisierter und bösartiger Aktivitäten in Ihrer AWS Cloud-Umgebung.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SI-4(16)	Die Organisation korreliert Informati onen aus Überwachu ngstools, die im gesamten Informati onssystem eingesetzt werden.	securityhub-enabled	AWS Security Hub hilft bei der Überwachung von unbefugtem Personal, Verbindun gen, Geräten und Software. AWS Security Hub aggregiert, organisie rt und priorisie rt die Sicherhei tswarnungen oder Ergebnisse mehrerer Dienste. AWS Einige dieser Dienste sind Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer und AWS Firewall Manager sowie AWS Partnerlösungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SI-4(16)	Die Organisation korreliert Informati onen aus Überwachu ngstools, die im gesamten Informati onssystem eingesetzt werden.	cloudtrail-s3-data events-enabled	Die Erfassung von Simple Storage Service (Amazon S3)-Datenereigniss en unterstützt die Erkennung von ungewöhnlichen Aktivitäten. Zu den Details gehören AWS Kontoinformationen , über die auf einen Amazon S3 S3-Bucket zugegriffen wurde, die IP-Adress e und die Uhrzeit des Ereignisses.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SI-4(16)	Die Organisation korreliert Informati onen aus Überwachu ngstools, die im gesamten Informati onssystem eingesetzt werden.	multi-region-cloudtrail-enabled	AWS CloudTrail zeichnet Aktionen und API-Aufrufe der AWS Management Console auf. Sie können feststellen, welche Benutzer und Konten angerufen wurden AWS, von welcher Quell-IP-Adresse aus die Anrufe getätigt wurden und wann die Anrufe erfolgten. CloudTrail übermittelt Protokolldateien aus allen AWS Regionen an Ihren S3-Bucket , wenn MULTI_REG ION_CLOUD _TRAIL_ENABLED aktiviert ist. Außerdem wird beim AWS Start einer neuen Region derselbe Trail in der neuen Region erstellt. CloudTrail Dadurch erhalten Sie automatis ch Protokolldateien mit API-Aktivitäten für die neue Region.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SI-4(16)	Die Organisation korreliert Informati onen aus Überwachu ngstools, die im gesamten Informati onssystem eingesetzt werden.	cloudtrail-enabled	AWS CloudTrail kann durch die Aufzeichn ung von Aktionen und API-Aufrufen in der AWS Managemen t Console bei der Nichtabstreitbarkeit helfen. Sie können die Benutzer und AWS Konten, die einen AWS Dienst aufgerufen haben, die Quell-IP-Adresse, über die die Anrufe generiert wurden, und die Zeitpunkte der Anrufe identifiz ieren. Einzelheiten zu den erfassten Daten finden Sie in den AWS CloudTrail Datensatzinhalten.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SI-4(16)	Die Organisation korreliert Informationen aus Überwachungstools, die im gesamten Informationssystem eingesetzt werden.	redshift-cluster-configuration-check	Um Daten im Ruhezustand zu schützen, muss die Verschlüsselung für Ihre Amazon-Redshift-Cluster aktiviert sein. Sie müssen auch sicherstellen, dass die erforderlichen Konfigurationen auf Amazon-Redshift-Clustern bereitgestellt werden. Die Prüfungsprotokollierung muss aktiviert sein, um Informationen zu Verbindungen und Benutzeraktivitäten in der Datenbank bereitzustellen. Diese Regel erfordert, dass ein Wert für clusterDbEncrypted (Config Default: TRUE) und LoggingEnabled (Config Default: TRUE) gesetzt ist. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SI-4(2)	Die Organisation setzt automatisierte Tools ein, um die Analyse von Ereignissen nahezu in Echtzeit zu unterstützen.	guardduty-enabled-centralized	Amazon GuardDuty kann mithilfe von Threat Intelligence Feeds helfen, potenzielle Cybersicherheitsereignisse zu überwachen und zu erkennen. Dazu gehören Listen mit bösartigen IPs und maschinellen Lernmethoden zur Identifizierung unerwarteter, nicht autorisierter und bösartiger Aktivitäten in Ihrer AWS Cloud-Umgebung.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SI-4(2)	Die Organisation setzt automatisierte Tools ein, um die Analyse von Ereignissen nahezu in Echtzeit zu unterstützen.	securityhub-enabled	AWS Security Hub hilft bei der Überwachung von unbefugtem Personal, Verbindungen, Geräten und Software. AWS Security Hub aggregiert, organisiert und priorisiert die Sicherheitswarnungen oder Ergebnisse mehrerer Dienste. AWS Einige dieser Dienste sind Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer und AWS Firewall Manager sowie AWS Partnerlösungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SI-4(2)	Die Organisation setzt automatisierte Tools ein, um die Analyse von Ereignissen nahezu in Echtzeit zu unterstützen.	cloudwatch-alarm-action-check	Amazon CloudWatch alarmiert, wenn eine Metrik den Schwellenwert für eine bestimmte Anzahl von Bewertungszeiträumen überschreitet. Der Alarm führt eine oder mehrere Aktionen durch, die vom Wert der Metrik oder des Ausdrucks im Vergleich zu einem Schwellenwert in einer Reihe von Zeiträumen abhängt. Diese Regel erfordert einen Wert für alarmActionRequired (Config Default: True), insufficientDataAction Required (Config Default: True), okActionRequired (Config Default: False). Der tatsächliche Wert muss die Alarmaktionen für Ihre Umgebung widerspiegeln.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SI-4(2)	Die Organisation setzt automatisierte Tools ein, um die Analyse von Ereignissen nahezu in Echtzeit zu unterstützen.	ec2- instance-detailed-monitoring-enabled	Aktivieren Sie diese Regel, um die Amazon Elastic Compute Cloud (Amazon EC2) - Instance-Überwachung auf der EC2 Amazon-Konsole zu verbessern, in der Monitoring-Diagramme mit einem Zeitraum von 1 Minute für die Instance angezeigt werden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SI-4(2)	Die Organisation setzt automatisierte Tools ein, um die Analyse von Ereigniss en nahezu in Echtzeit zu unterstützen.	multi-region-cloudtrail-enabled	AWS CloudTrail zeichnet Aktionen und API-Aufrufe der AWS Management Console auf. Sie können feststellen, welche Benutzer und Konten angerufen wurden AWS, von welcher Quell-IP-Adresse aus die Anrufe getätigt wurden und wann die Anrufe erfolgten. CloudTrail übermittelt Protokolldateien aus allen AWS Regionen an Ihren S3-Bucket , wenn MULTI_REG ION_CLOUD _TRAIL_ENABLED aktiviert ist. Außerdem wird beim AWS Start einer neuen Region derselbe Trail in der neuen Region erstellt. CloudTrail Dadurch erhalten Sie automatis ch Protokolldateien mit API-Aktivitäten für die neue Region.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SI-4(2)	Die Organisation setzt automatisierte Tools ein, um die Analyse von Ereignissen nahezu in Echtzeit zu unterstützen.	cloudtrail-enabled	AWS CloudTrail kann durch die Aufzeichnung von Aktionen und API-Aufrufen in der AWS Management Console bei der Nichtabstreitbarkeit helfen. Sie können die Benutzer und AWS Konten, die einen AWS Dienst aufgerufen haben, die Quell-IP-Adresse, über die die Anrufe generiert wurden, und die Zeitpunkte der Anrufe identifizieren. Einzelheiten zu den erfassten Daten finden Sie in den AWS CloudTrail Datensatzinhalten.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SI-4(2)	Die Organisation setzt automatisierte Tools ein, um die Analyse von Ereignissen nahezu in Echtzeit zu unterstützen.	cloudtrail-s3-dataevents-enabled	Die Erfassung von Simple Storage Service (Amazon S3)-Datenereignissen unterstützt die Erkennung von ungewöhnlichen Aktivitäten. Zu den Details gehören AWS Kontoinformationen, über die auf einen Amazon S3 S3-Bucket zugegriffen wurde, die IP-Adresse und die Uhrzeit des Ereignisses.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SI-4(2)	Die Organisation setzt automatisierte Tools ein, um die Analyse von Ereignissen nahezu in Echtzeit zu unterstützen.	redshift-cluster-configuration-check	Um Daten im Ruhezustand zu schützen, muss die Verschlüsselung für Ihre Amazon-Redshift-Cluster aktiviert sein. Sie müssen auch sicherstellen, dass die erforderlichen Konfigurationen auf Amazon-Redshift-Clustern bereitgestellt werden. Die Prüfungsprotokollierung muss aktiviert sein, um Informationen zu Verbindungen und Benutzeraktivitäten in der Datenbank bereitzustellen. Diese Regel erfordert, dass ein Wert für clusterDbEncrypted (Config Default: TRUE) und LoggingEnabled (Config Default: TRUE) gesetzt ist. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SI-4(4)	Das Informati onssystem überwacht den ein- und ausgehenden Kommunikationsverk ehr kontinuierlich auf ungewöhnliche oder unzulässige Aktivität en oder Bedingungen.	guardduty-enabled-centralized	Amazon GuardDuty kann mithilfe von Threat Intellige nce Feeds helfen, potenzielle Cybersich erheitsereignisse zu überwachen und zu erkennen. Dazu gehören Listen mit bösartigen IPs und maschinel len Lernmethoden zur Identifizierung unerwarteter, nicht autorisierter und bösartiger Aktivitäten in Ihrer AWS Cloud-Umgebung.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SI-4(4)	Das Informati onssystem überwacht den ein- und ausgehenden Kommunikationsverk ehr kontinuierlich auf ungewöhnliche oder unzulässige Aktivität en oder Bedingungen.	securityhub-enabled	AWS Security Hub hilft bei der Überwachung von unbefugtem Personal, Verbindun gen, Geräten und Software. AWS Security Hub aggregiert, organisie rt und priorisie rt die Sicherhei tswarnungen oder Ergebnisse mehrerer Dienste. AWS Einige dieser Dienste sind Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer und AWS Firewall Manager sowie AWS Partnerlösungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SI-4(4)	Das Informationssystem überwacht den ein- und ausgehenden Kommunikationsverkehr kontinuierlich auf ungewöhnliche oder unzulässige Aktivitäten oder Bedingungen.	cloudwatch-alarm-action-check	Amazon CloudWatch alarmiert, wenn eine Metrik den Schwellenwert für eine bestimmte Anzahl von Bewertungszeiträumen überschreitet. Der Alarm führt eine oder mehrere Aktionen durch, die vom Wert der Metrik oder des Ausdrucks im Vergleich zu einem Schwellenwert in einer Reihe von Zeiträumen abhängt. Diese Regel erfordert einen Wert für alarmActionRequired (Config Default: True), insufficientDataAction Required (Config Default: True), okActionRequired (Config Default: False). Der tatsächliche Wert muss die Alarmaktionen für Ihre Umgebung widerspiegeln.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SI-4(4)	Das Informati onssystem überwacht den ein- und ausgehenden Kommunikationsverk ehr kontinuierlich auf ungewöhnliche oder unzulässige Aktivität en oder Bedingungen.	cloud-trail-cloud-watch-logs-aktiviert	Verwenden Sie Amazon CloudWatch , um Protokollereignisa ktivitäten zentral zu sammeln und zu verwalten. Durch die Aufnahme von AWS CloudTrail Daten erhalten Sie Einzelhei ten zu den API-Aufru faktivitäten innerhalb Ihres AWS Kontos.
SI-4(5)	Das Informati onssystem alarmiert [Zuweisung: von der Organisation ernanntes Personal oder definierte Rollen], wenn die folgenden Anzeichen für eine bestehend e oder potenzielle Gefährdung auftreten : [Zuweisung: von der Organisation definiert e Gefährdungsindikat oren].	guardduty-enabled-centralized	Amazon GuardDuty kann mithilfe von Threat Intellige nce Feeds helfen, potenzielle Cybersich erheitsereignisse zu überwachen und zu erkennen. Dazu gehören Listen mit bösartigen IPs und maschinel len Lernmethoden zur Identifizierung unerwarteter, nicht autorisierter und bösartiger Aktivitäten in Ihrer AWS Cloud-Umgebung.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SI-4(5)	Das Informati onssystem alarmiert [Zuweisung: von der Organisation ernanntes Personal oder definierte Rollen], wenn die folgenden Anzeichen für eine bestehend e oder potenzielle Gefährdung auftreten : [Zuweisung: von der Organisation definiert e Gefährdungsindikat oren].	securityhub-enabled	AWS Security Hub hilft bei der Überwachung von unbefugtem Personal, Verbindun gen, Geräten und Software. AWS Security Hub aggregiert, organisie rt und priorisie rt die Sicherhei tswarnungen oder Ergebnisse mehrerer Dienste. AWS Einige dieser Dienste sind Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer und AWS Firewall Manager sowie AWS Partnerlösungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SI-4(5)	Das Informationssystem alarmiert [Zuweisung: von der Organisation ernanntes Personal oder definierte Rollen], wenn die folgenden Anzeichen für eine bestehende oder potenzielle Gefährdung auftreten: [Zuweisung: von der Organisation definierte Gefährdungsindikatoren].	cloudwatch-alarm-action-check	Amazon CloudWatch alarmiert, wenn eine Metrik den Schwellenwert für eine bestimmte Anzahl von Bewertungszeiträumen überschreitet. Der Alarm führt eine oder mehrere Aktionen durch, die vom Wert der Metrik oder des Ausdrucks im Vergleich zu einem Schwellenwert in einer Reihe von Zeiträumen abhängt. Diese Regel erfordert einen Wert für alarmActionRequired (Config Default: True), insufficientDataAction Required (Config Default: True), okActionRequired (Config Default: False). Der tatsächliche Wert muss die Alarmaktionen für Ihre Umgebung widerspiegeln.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SI-4(5)	Das Informati onssystem alarmiert [Zuweisung: von der Organisation ernanntes Personal oder definierte Rollen], wenn die folgenden Anzeichen für eine bestehend e oder potenzielle Gefährdung auftreten : [Zuweisung: von der Organisation definiert e Gefährdungsindikat oren].	cloud-trail-cloud-watch-logs-aktiviert	Verwenden Sie Amazon CloudWatch , um Protokollereignisa ktivitäten zentral zu sammeln und zu verwalten. Durch die Aufnahme von AWS CloudTrail Daten erhalten Sie Einzelhei ten zu den API-Aufru faktivitäten innerhalb Ihres AWS Kontos.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SI-4(a)(b)(c)	Die Organisation: a. Überwacht das Informationssystem und erkennt: 1. Angriffe und Indikatoren für potenzielle Angriffe in Übereinstimmung mit [Zuweisung: von der Organisation festgelegte Überwachungsziele]; und 2. Nicht autorisierte lokale Verbindungen sowie Netzwerk- und Remoteverbindungen; b. Identifiziert die unbefugte Nutzung des Informationssystems durch [Zuweisung: von der Organisation festgelegte Techniken und Methoden]; c. Verwendet Überwachungsgeräte: i. strategisch innerhalb des Informationssystems, um von der Organisation festgelegte wesentliche Informationen zu sammeln;	guardduty-enabled-centralized	Amazon GuardDuty kann mithilfe von Threat Intelligence Feeds helfen, potenzielle Cybersicherheitsereignisse zu überwachen und zu erkennen. Dazu gehören Listen mit bösartigen IPs und maschinellen Lernmethoden zur Identifizierung unerwarteter, nicht autorisierter und bösartiger Aktivitäten in Ihrer AWS Cloud-Umgebung.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	und ii) an Ad-hoc-St andorten innerhalb des Systems, um bestimmte Arten von Vorgängen zu verfolgen, die für die Organisation von Interesse sind.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SI-4(a)(b)(c)	Die Organisation: a. Überwacht das Informationssystem und erkennt: 1. Angriffe und Indikatoren für potenzielle Angriffe in Übereinstimmung mit [Zuweisung: von der Organisation festgelegte Überwachungsziele]; und 2. Nicht autorisierte lokale Verbindungen sowie Netzwerk- und Remoteverbindungen; b. Identifiziert die unbefugte Nutzung des Informationssystems durch [Zuweisung: von der Organisation festgelegte Techniken und Methoden]; c. Verwendet Überwachungsgeräte: i. strategisch innerhalb des Informationssystems, um von der Organisation festgelegte wesentliche Informationen zu sammeln;	guardduty-non-archived-findings	Amazon GuardDuty hilft Ihnen dabei, die Auswirkungen eines Vorfalls zu verstehen, indem es die Ergebnisse nach Schweregrad klassifiziert: niedrig, mittel und hoch. Diese Klassifizierungen können Sie zur Festlegung von entsprechenden Strategien und Prioritäten zur Behebung solcher Vorfälle verwenden. Mit dieser Regel können Sie optional daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7) und daysHighSev (Config Default: 1) für nicht archivierte Ergebnisse festlegen, wie es die Richtlinien Ihrer Organisation erfordern.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	und ii) an Ad-hoc-St andorten innerhalb des Systems, um bestimmte Arten von Vorgängen zu verfolgen, die für die Organisation von Interesse sind.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SI-4(a)(b)(c)	Die Organisation: a. Überwacht das Informationssystem und erkennt: 1. Angriffe und Indikatoren für potenzielle Angriffe in Übereinstimmung mit [Zuweisung: von der Organisation festgelegte Überwachungsziele]; und 2. Nicht autorisierte lokale Verbindungen sowie Netzwerk- und Remoteverbindungen; b. Identifiziert die unbefugte Nutzung des Informationssystems durch [Zuweisung: von der Organisation festgelegte Techniken und Methoden]; c. Verwendet Überwachungsgeräte: i. strategisch innerhalb des Informationssystems, um von der Organisation festgelegte wesentliche Informationen zu sammeln;	alb-waf-enabled	Stellen Sie sicher, dass AWS WAF auf Elastic Load Balancers (ELB) aktiviert ist, um Webanwendungen zu schützen. Eine WAF trägt zum Schutz Ihrer Webanwendungen oder APIs vor gängigen Web-Exploits bei. Diese Web-Exploits können sich auf die Verfügbarkeit auswirken, die Sicherheit gefährden oder übermäßige Ressourcen in Ihrer Umgebung verbrauchen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	und ii) an Ad-hoc-St andorten innerhalb des Systems, um bestimmte Arten von Vorgängen zu verfolgen, die für die Organisation von Interesse sind.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SI-4(a)(b)(c)	Die Organisation: a. Überwacht das Informationssystem und erkennt: 1. Angriffe und Indikatoren für potenzielle Angriffe in Übereinstimmung mit [Zuweisung: von der Organisation festgelegte Überwachungsziele]; und 2. Nicht autorisierte lokale Verbindungen sowie Netzwerk- und Remoteverbindungen; b. Identifiziert die unbefugte Nutzung des Informationssystems durch [Zuweisung: von der Organisation festgelegte Techniken und Methoden]; c. Verwendet Überwachungsgeräte: i. strategisch innerhalb des Informationssystems, um von der Organisation festgelegte wesentliche Informationen zu sammeln;	wafv2-logging-enabled	Um die Protokollierung und Überwachung in Ihrer Umgebung zu erleichtern, aktivieren Sie die AWS WAF (V2) -Protokollierung im regionalen und globalen Web. ACLs AWS Die WAF-Protokollierung bietet detaillierte Informationen über den Datenverkehr, der von Ihrer Web-ACL analysiert wird. In den Protokollen werden die Uhrzeit aufgezeichnet, zu der die AWS WAF die Anfrage von Ihrer AWS Ressource erhalten hat, Informationen über die Anfrage und eine Aktion für die Regel, der jede Anfrage entsprach.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	und ii) an Ad-hoc-St andorten innerhalb des Systems, um bestimmte Arten von Vorgängen zu verfolgen, die für die Organisation von Interesse sind.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SI-4(a)(b)(c)	Die Organisation: a. Überwacht das Informationssystem und erkennt: 1. Angriffe und Indikatoren für potenzielle Angriffe in Übereinstimmung mit [Zuweisung: von der Organisation festgelegte Überwachungsziele]; und 2. Nicht autorisierte lokale Verbindungen sowie Netzwerk- und Remoteverbindungen; b. Identifiziert die unbefugte Nutzung des Informationssystems durch [Zuweisung: von der Organisation festgelegte Techniken und Methoden]; c. Verwendet Überwachungsgeräte: i. strategisch innerhalb des Informationssystems, um von der Organisation festgelegte wesentliche Informationen zu sammeln;	securityhub-enabled	AWS Security Hub hilft bei der Überwachung von unbefugtem Personal, Verbindungen, Geräten und Software. AWS Security Hub aggregiert, organisiert und priorisiert die Sicherheitswarnungen oder Ergebnisse mehrerer Dienste. AWS Einige dieser Dienste sind Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer und AWS Firewall Manager sowie AWS Partnerlösungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	und ii) an Ad-hoc-St andorten innerhalb des Systems, um bestimmte Arten von Vorgängen zu verfolgen, die für die Organisation von Interesse sind.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SI-4(a)(b)(c)	Die Organisation: a. Überwacht das Informationssystem und erkennt: 1. Angriffe und Indikatoren für potenzielle Angriffe in Übereinstimmung mit [Zuweisung: von der Organisation festgelegte Überwachungsziele]; und 2. Nicht autorisierte lokale Verbindungen sowie Netzwerk- und Remoteverbindungen; b. Identifiziert die unbefugte Nutzung des Informationssystems durch [Zuweisung: von der Organisation festgelegte Techniken und Methoden]; c. Verwendet Überwachungsgeräte: i. strategisch innerhalb des Informationssystems, um von der Organisation festgelegte wesentliche Informationen zu sammeln;	cloudwatch-alarm-action-check	Amazon CloudWatch alarmiert, wenn eine Metrik den Schwellenwert für eine bestimmte Anzahl von Bewertungszeiträumen überschreitet. Der Alarm führt eine oder mehrere Aktionen durch, die vom Wert der Metrik oder des Ausdrucks im Vergleich zu einem Schwellenwert in einer Reihe von Zeiträumen abhängt. Diese Regel erfordert einen Wert für alarmActionRequired (Config Default: True), insufficientDataAction Required (Config Default: True), okActionRequired (Config Default: False). Der tatsächliche Wert muss die Alarmaktionen für Ihre Umgebung widerspiegeln.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	und ii) an Ad-hoc-St andorten innerhalb des Systems, um bestimmte Arten von Vorgängen zu verfolgen, die für die Organisation von Interesse sind.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SI-4(a)(b)(c)	Die Organisation: a. Überwacht das Informationssystem und erkennt: 1. Angriffe und Indikatoren für potenzielle Angriffe in Übereinstimmung mit [Zuweisung: von der Organisation festgelegte Überwachungsziele]; und 2. Nicht autorisierte lokale Verbindungen sowie Netzwerk- und Remoteverbindungen; b. Identifiziert die unbefugte Nutzung des Informationssystems durch [Zuweisung: von der Organisation festgelegte Techniken und Methoden]; c. Verwendet Überwachungsgeräte: i. strategisch innerhalb des Informationssystems, um von der Organisation festgelegte wesentliche Informationen zu sammeln;	cloud-trail-cloud-watch-logs-aktiviert	Verwenden Sie Amazon CloudWatch , um Protokollereignisaktivitäten zentral zu sammeln und zu verwalten. Durch die Aufnahme von AWS CloudTrail Daten erhalten Sie Einzelheiten zu den API-Aufrufaktivitäten innerhalb Ihres AWS Kontos.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	und ii) an Ad-hoc-St andorten innerhalb des Systems, um bestimmte Arten von Vorgängen zu verfolgen, die für die Organisation von Interesse sind.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SI-4(a)(b)(c)	Die Organisation: a. Überwacht das Informationssystem und erkennt: 1. Angriffe und Indikatoren für potenzielle Angriffe in Übereinstimmung mit [Zuweisung: von der Organisation festgelegte Überwachungsziele]; und 2. Nicht autorisierte lokale Verbindungen sowie Netzwerk- und Remoteverbindungen; b. Identifiziert die unbefugte Nutzung des Informationssystems durch [Zuweisung: von der Organisation festgelegte Techniken und Methoden]; c. Verwendet Überwachungsgeräte: i. strategisch innerhalb des Informationssystems, um von der Organisation festgelegte wesentliche Informationen zu sammeln;	ec2- instance-detailed-monitoring-enabled	Aktivieren Sie diese Regel, um die Amazon Elastic Compute Cloud (Amazon EC2) - Instance-Überwachung auf der EC2 Amazon-Konsole zu verbessern, in der Monitoring-Diagramme mit einem Zeitraum von 1 Minute für die Instance angezeigt werden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	und ii) an Ad-hoc-St andorten innerhalb des Systems, um bestimmte Arten von Vorgängen zu verfolgen, die für die Organisation von Interesse sind.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SI-4(a)(b)(c)	Die Organisation: a. Überwacht das Informationssystem und erkennt: 1. Angriffe und Indikatoren für potenzielle Angriffe in Übereinstimmung mit [Zuweisung: von der Organisation festgelegte Überwachungsziele]; und 2. Nicht autorisierte lokale Verbindungen sowie Netzwerk- und Remoteverbindungen; b. Identifiziert die unbefugte Nutzung des Informationssystems durch [Zuweisung: von der Organisation festgelegte Techniken und Methoden]; c. Verwendet Überwachungsgeräte: i. strategisch innerhalb des Informationssystems, um von der Organisation festgelegte wesentliche Informationen zu sammeln;	api-gw-associated-with-WAF	AWS Mit WAF können Sie eine Reihe von Regeln (eine so genannte Web Access Control List (Web ACL)) konfigurieren, die Webanfragen auf der Grundlage von anpassbaren Websicherheitsregeln und -bedingungen, die Sie definieren, zulassen, blockieren oder zählen. Stellen Sie sicher, dass Ihre Amazon-API-Gateway-Stufe mit einer WAF-Web-ACL verknüpft ist, um sie vor böswilligen Angriffen zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	und ii) an Ad-hoc-St andorten innerhalb des Systems, um bestimmte Arten von Vorgängen zu verfolgen, die für die Organisation von Interesse sind.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SI-7	Die Organisation verwendet Tools zur Integritätsprüfung , um unbefugte Änderungen an [Zuweisung: von der Organisation definiert e Software, Firmware und Informationen] zu erkennen.	cloud-trail-log-file-validierung aktiviert	Verwenden Sie die Validierung von AWS CloudTrail Protokolldateien, um die Integrität von CloudTrail Protokoll en zu überprüfen. Mithilfe der Protokoll dateivalidierung kann festgestellt werden, ob eine Protokoll datei geändert oder gelöscht wurde oder ob sie nach der Übermittlung CloudTrail unverände rt geblieben ist. Dieses Feature wurde mit dem Branchens tandard entsprech enden Algorithmen entwickelt: SHA-256 für die Hashfunktion und SHA-256 mit RSA für digitale Signature n. Aus diesem Grund ist es rechnerisch unmöglich, CloudTrai l Protokolldateien unbemerkt zu ändern, zu löschen oder zu fälschen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SI-7(1)	Das Informationssystem führt mindestens einmal im Monat eine Integritätsprüfung bei sicherheitsrelevanten Ereignissen durch.	ec2-managed-instance-managed-by-systems	Eine Bestandsaufnahme der Softwareplattformen und Anwendungen innerhalb des Unternehmens ist möglich, indem Amazon Elastic Compute Cloud (Amazon EC2) - Instances mit AWS Systems Manager verwaltet werden. Verwenden Sie AWS Systems Manager, um detaillierte Systemkonfigurationen, Betriebssystem-Patch-Levels, Namen und Typ der Dienste, Softwareinstallationen, Anwendungsname, Herausgeber und Version sowie andere Details zu Ihrer Umgebung bereitzustellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SI-7(1)	Das Informati onssystem führt mindestens einmal im Monat eine Integritätsprüfung bei sicherheitsrelevanten Ereignissen durch.	ec2-prüfen managedinstance-pa tch-compliance-status	Aktivieren Sie diese Regel, um bei der Identifizierung und Dokumentation von Sicherheitslücken in Amazon Elastic Compute Cloud (Amazon EC2) zu helfen. Die Regel prüft, ob die EC2 Amazon-Instance die Patch-Konformität im AWS Systems Manager gemäß den Richtlinien und Verfahren Ihrer Organisation einhält.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SI-7(1)	Das Informati onssystem führt mindestens einmal im Monat eine Integritätsprüfung bei sicherheitsrelevanten Ereignissen durch.	cloud-trail-log-file-validierung aktiviert	Verwenden Sie die AWS CloudTrail Protokolldateivali dierung, um die Integrität der CloudTrail Protokoll e zu überprüfen. Mithilfe der Protokoll dateivalidierung kann festgestellt werden, ob eine Protokoll datei geändert oder gelöscht wurde oder ob sie nach der Übermittlung CloudTrail unverände rt geblieben ist. Dieses Feature wurde mit dem Branchens tandard entsprech enden Algorithmen entwickelt: SHA-256 für die Hashfunktion und SHA-256 mit RSA für digitale Signature n. Aus diesem Grund ist es rechnerisch unmöglich, CloudTrai l Protokolldateien unbemerkt zu ändern, zu löschen oder zu fälschen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
RA-5(1)	Das Unternehmen setzt Tools zum Scannen von Schwachstellen ein, mit denen die zu scannenden Schwachstellen im Informationssystem problemlos aktualisiert werden können. Zusätzliche Empfehlungen: Die zu scannenden Schwachstellen müssen umgehend aktualisiert werden, sobald neue Schwachstellen entdeckt, angekündigt und Scanmethoden entwickelt werden. Dieser Aktualisierungsprozess trägt dazu bei, dass potenzielle Schwachstellen im Informationssystem so schnell wie möglich identifiziert und behoben werden. Verwandte Kontrollen: SI-3, SI-7.	guardduty-enabled-centralized	Amazon GuardDuty kann mithilfe von Threat Intelligence Feeds helfen, potenzielle Cybersicherheitsereignisse zu überwachen und zu erkennen. Dazu gehören Listen mit bösartigen IPs und maschinellen Lernmethoden zur Identifizierung unerwarteter, nicht autorisierter und bösartiger Aktivitäten in Ihrer AWS Cloud-Umgebung.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
RA-5(1)	Das Unternehmen setzt Tools zum Scannen von Schwachstellen ein, mit denen die zu scannenden Schwachstellen im Informationssystem problemlos aktualisiert werden können. Zusätzliche Empfehlungen: Die zu scannenden Schwachstellen müssen umgehend aktualisiert werden, sobald neue Schwachstellen entdeckt, angekündigt und Scanmethoden entwickelt werden. Dieser Aktualisierungsprozess trägt dazu bei, dass potenzielle Schwachstellen im Informationssystem so schnell wie möglich identifiziert und behoben werden. Verwandte Kontrollen: SI-3, SI-7.	guardduty-non-archived-findings	Amazon GuardDuty hilft Ihnen dabei, die Auswirkungen eines Vorfalls zu verstehen, indem es die Ergebnisse nach Schweregrad klassifiziert: niedrig, mittel und hoch. Diese Klassifizierungen können Sie zur Festlegung von entsprechenden Strategien und Prioritäten zur Behebung solcher Vorfälle verwenden. Mit dieser Regel können Sie optional daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7) und daysHighSev (Config Default: 1) für nicht archivierte Ergebnisse festlegen, wie es die Richtlinien Ihrer Organisation erfordern.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
RA-5(1)	Das Unternehmen setzt Tools zum Scannen von Schwachstellen ein, mit denen die zu scannenden Schwachstellen im Informationssystem problemlos aktualisiert werden können. Zusätzliche Empfehlungen: Die zu scannenden Schwachstellen müssen umgehend aktualisiert werden, sobald neue Schwachstellen entdeckt, angekündigt und Scanmethoden entwickelt werden. Dieser Aktualisierungsprozess trägt dazu bei, dass potenzielle Schwachstellen im Informationssystem so schnell wie möglich identifiziert und behoben werden. Verwandte Kontrollen: SI-3, SI-7.	securityhub-enabled	AWS Security Hub hilft bei der Überwachung von unbefugtem Personal, Verbindungen, Geräten und Software. AWS Security Hub aggregiert, organisiert und priorisiert die Sicherheitswarnungen oder Ergebnisse mehrerer Dienste. AWS Einige dieser Dienste sind Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer und AWS Firewall Manager sowie AWS Partnerlösungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-7(4)	Die Organisation: (a) Implementiert eine verwaltete Schnittstelle für jeden externen Telekommunikationsdienst; (b) legt eine Verkehrsflussrichtlinie für jede verwaltete Schnittstelle fest; (c) schützt die Vertraulichkeit und Integrität der Informationen, die über jede Schnittstelle übertragen werden; (d) dokumentiert jede Ausnahme von der Verkehrsflussrichtlinie mit unterstützendem mission/business need and duration of that need; and (e) Reviews exceptions to the traffic flow policy [Assignment: organization-defined frequency] and removes exceptions that are no longer supported by an explicit mission/business Bedarf. Zusätzliche Empfehlungen:	vpc-default-security-group-geschlossen	Sicherheitsgruppen von Amazon Elastic Compute Cloud (Amazon EC2) können bei der Verwaltung des Netzwerkzugriffs helfen, indem sie eine statusbehaftete Filterung des ein- und ausgehenden Netzwerkverkehrs zu Ressourcen bereitstellen. AWS Die Beschränkung des gesamten Datenverkehrs auf die Standardsicherheitsgruppe hilft dabei, den Fernzugriff auf Ihre Ressourcen einzuschränken. AWS

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	Verwandte Kontrolle: SC-8.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-7(4)	Die Organisation: (a) Implementiert eine verwaltete Schnittstelle für jeden externen Telekommunikationsdienst; (b) legt eine Verkehrsflussrichtlinie für jede verwaltete Schnittstelle fest; (c) schützt die Vertraulichkeit und Integrität der Informationen, die über jede Schnittstelle übertragen werden; (d) dokumentiert jede Ausnahme von der Verkehrsflussrichtlinie mit unterstützendem Bedarf. mission/business need and duration of that need; and (e) Reviews exceptions to the traffic flow policy [Assignment: organization-defined frequency] and removes exceptions that are no longer supported by an explicit mission/business Zusätzliche Empfehlungen:	rds-snapshot-encrypted	Stellen Sie sicher, dass die Verschlüsselung für Ihre Amazon Relational Database Service (Amazon RDS)-Snapshots aktiviert ist. Da sensible Daten auch im Ruhezustand vorhanden sein können, sollten Sie die Verschlüsselung im Ruhezustand aktivieren, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	Verwandte Kontrolle: SC-8.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-7(4)	Die Organisation: (a) Implementiert eine verwaltete Schnittstelle für jeden externen Telekommunikationsdienst; (b) legt eine Verkehrsflussrichtlinie für jede verwaltete Schnittstelle fest; (c) schützt die Vertraulichkeit und Integrität der Informationen, die über jede Schnittstelle übertragen werden; (d) dokumentiert jede Ausnahme von der Verkehrsflussrichtlinie mit unterstützendem mission/business need and duration of that need; and (e) Reviews exceptions to the traffic flow policy [Assignment: organization-defined frequency] and removes exceptions that are no longer supported by an explicit mission/business Bedarf. Zusätzliche Empfehlungen:	rds-snapshots-public-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Relational Database Service (Amazon RDS) -Instances nicht öffentlich sind. Amazon-RDS-Datenbank-Instances können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	Verwandte Kontrolle: SC-8.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-7(4)	Die Organisation: (a) Implementiert eine verwaltete Schnittstelle für jeden externen Telekommunikationsdienst; (b) legt eine Verkehrsflussrichtlinie für jede verwaltete Schnittstelle fest; (c) schützt die Vertraulichkeit und Integrität der Informationen, die über jede Schnittstelle übertragen werden; (d) dokumentiert jede Ausnahme von der Verkehrsflussrichtlinie mit mission/business need and duration of that need; and (e) Reviews exceptions to the traffic flow policy [Assignment: organization-defined frequency] and removes exceptions that are no longer supported by an explicit mission/business unterstützendem Bedarf. Zusätzliche Empfehlungen:	rds-storage-encrypted	Zum Schutz von Daten im Ruhezustand müssen Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon Relational Database Service (Amazon RDS)-Instances aktiviert ist. Um eventuell vorhandene sensible Daten im Ruhezustand in Amazon-RDS-Instances zu schützen, muss die Verschlüsselung von Daten im Ruhezustand aktiviert sein.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	Verwandte Kontrolle: SC-8.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-7(4)	Die Organisation: (a) Implementiert eine verwaltete Schnittstelle für jeden externen Telekommunikationsdienst; (b) legt eine Verkehrsflussrichtlinie für jede verwaltete Schnittstelle fest; (c) schützt die Vertraulichkeit und Integrität der Informationen, die über jede Schnittstelle übertragen werden; (d) dokumentiert jede Ausnahme von der Verkehrsflussrichtlinie mit unterstützendem mission/business need and duration of that need; and (e) Reviews exceptions to the traffic flow policy [Assignment: organization-defined frequency] and removes exceptions that are no longer supported by an explicit mission/business Bedarf. Zusätzliche Empfehlungen:	redshift-cluster-kms-enabled	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass die Verschlüsselung mit AWS Key Management Service (AWS KMS) für Ihren Amazon Redshift Redshift-Cluster aktiviert ist. Um eventuell vorhandene sensible Daten im Ruhezustand in Redshift-Clustern zu schützen, muss die Verschlüsselung von Daten im Ruhezustand aktiviert sein.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	Verwandte Kontrolle: SC-8.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-7(4)	Die Organisation: (a) Implementiert eine verwaltete Schnittstelle für jeden externen Telekommunikationsdienst; (b) legt eine Verkehrsflussrichtlinie für jede verwaltete Schnittstelle fest; (c) schützt die Vertraulichkeit und Integrität der Informationen, die über jede Schnittstelle übertragen werden; (d) dokumentiert jede Ausnahme von der Verkehrsflussrichtlinie mit mission/business need and duration of that need; and (e) Reviews exceptions to the traffic flow policy [Assignment: organization-defined frequency] and removes exceptions that are no longer supported by an explicit mission/business unterstützendem Bedarf. Zusätzliche Empfehlungen:	vpc-flow-logs-enabled	VPC-Flow-Protokolle erfassen detaillierte Informationsdatensätze über den IP-Datenverkehr, der zu und von Netzwerkschnittstellen in Ihrer Amazon Virtual Private Cloud (Amazon VPC) fließt. Standardmäßig enthalten Flow-Protokolldatensätze Werte für die verschiedenen Komponenten des IP-Flows, einschließlich Quelle, Ziel und Protokoll.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	Verwandte Kontrolle: SC-8.		
SC-7(5)	Das Informati onssystem lehnt Netzwerkverkehr an verwalteten Schnittst ellen standardm äßig ab und lässt Netzwerkverkehr ausnahmsweise zu (d. h. alles verweiger n, ausnahmsweise zulassen). Zusätzlic he Empfehlungen: Diese Verbesserung der Kontrolle wirkt sich auf eingehend en und ausgehenden Netzwerkverkehr aus. Eine Richtlinie, bei der der permit-by-exceptio n Netzwerkverkehr generell verweiger t wird, stellt sicher, dass nur Verbindun gen zugelassen werden, die unbedingt erforderlich und zugelassen sind.	vpc-sg-open-only-to-authorized-ports	Verwalten Sie den Zugriff auf Ressource n in der AWS Cloud, indem Sie sicherste llen, dass gemeinsam e Ports für Amazon Elastic Compute Cloud (Amazon EC2) -Sicherhe itsgruppen eingeschr ränkt sind. Wenn der Zugriff auf Ports nicht auf vertrauen swürdige Quellen beschränkt wird, kann dies zu Angriffen auf die Verfügbar keit, Integrität und Vertraulichkeit von Systemen führen. Durch die Beschränk ung des Zugriffs auf Ressourcen innerhalb einer Sicherhei tsgruppe aus dem Internet (0.0.0.0/0) kann der Remote-Zugriff auf interne Systeme gesteuert werden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-2(7)	Die Organisation: (a) richtet privilegi erte Benutzerk onten gemäß einem rollenbasierten Zugriffsschema ein, das den erlaubten Zugriff auf das Informationssystem und die Rechte in Rollen organisiert; (b) überwacht privilegi erte Rollenzuw eisungen; und (c) ergreift [Zuweisung: organisationsdefin ierte Aktionen] , wenn privilegi erte Rollenzuw eisungen nicht mehr angemesse n sind. Zusätzlic he Empfehlun gen: Privilegierte Rollen sind von der Organisation definierte Rollen, die Einzelpersonen zugewiesen werden, damit sie bestimmte sicherheitsrelevante Funktionen ausführen können, zu denen	iam-customer-policy-blocked-kms-Aktionen	AWS Identity and Access Managemen t (IAM) kann Ihnen helfen, die Prinzipien der geringsten Rechte und der Aufgabent rennung in Zugriffsb erechtigungen und Autorisierungen zu integrieren und so zu verhindern, dass Richtlinien blockiert e Aktionen für alle AWS Schlüssel des Key Management Service enthalten. Wenn Benutzer mehr Rechte haben, als für die Ausführung einer Aufgabe erforderl ich sind, kann dies gegen das Prinzip der geringsten Berechtig ung und Aufgabent rennung verstoßen . Mit dieser Regel können Sie den Parameter festlegen . blockedActionsPatt erns (Wert „AWS Bewährte grundlege nde Sicherhei tsmethoden“: kms:

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	normale Benutzer nicht berechtigt sind. Zu diesen privilegi erten Rollen gehört zum Beispiel die Verwaltung von Schlüsseln, Konten, Netzwerken und Systemen, Datenbank en und Websites.		Decrypt, kms:ReEnc ryptFrom). Die tatsächlichen Werte müssen den Richtlini en Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-2(7)	Die Organisation: (a) richtet privilegierte Benutzerkonten gemäß einem rollenbasierten Zugriffsschema ein, das den erlaubten Zugriff auf das Informationssystem und die Rechte in Rollen organisiert; (b) überwacht privilegierte Rollenzuweisungen; und (c) ergreift [Zuweisung: organisationsdefinierte Aktionen], wenn privilegierte Rollenzuweisungen nicht mehr angemessen sind. Zusätzliche Empfehlungen: Privilegierte Rollen sind von der Organisation definierte Rollen, die Einzelpersonen zugewiesen werden, damit sie bestimmte sicherheitsrelevante Funktionen ausführen können, zu denen	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) kann Ihnen dabei helfen, die Prinzipien der geringsten Rechte und der Aufgabentrennung in Zugriffsberechtigungen und Autorisierungen zu integrieren und so zu verhindern, dass Richtlinien „Effect“: „Allow“ mit „Action“: „*“ anstelle von „Resource“: „*“ enthalten. Wenn Benutzern mehr Rechte eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und der Aufgabentrennung verstoßen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	normale Benutzer nicht berechtigt sind. Zu diesen privilegi erten Rollen gehört zum Beispiel die Verwaltung von Schlüsseln, Konten, Netzwerken und Systemen, Datenbank en und Websites.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-2(7)	Die Organisation: (a) richtet privilegierte Benutzerkonten ein und verwaltet sie gemäß einem rollenbasierten Zugriffsschema, das den erlaubten Zugriff auf das Informationssystem und die Rechte in Rollen organisiert; (b) überwacht privilegierte Rollenzuweisungen; und (c) ergreift [Zuweisung: organisationsdefinierte Aktionen], wenn privilegierte Rollenzuweisungen nicht mehr angemessen sind. Zusätzliche Empfehlungen: Privilegierte Rollen sind von der Organisation definierte Rollen, die Einzelpersonen zugewiesen werden, damit sie bestimmte sicherheitsrelevante Funktionen ausführen	iam-policy-no-statements-with-full-access	Stellen Sie sicher, dass IAM-Aktionen nur auf die benötigten Aktionen beschränkt sind. Wenn Benutzern mehr Rechte eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und der Aufgabentrennung verstoßen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	können, zu denen normale Benutzer nicht berechtigt sind. Zu diesen privilegi erten Rollen gehört zum Beispiel die Verwaltung von Schlüsseln, Konten, Netzwerken und Systemen, Datenbank en und Websites.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-2(7)	Die Organisation: (a) richtet privilegierte Benutzerkonten ein und verwaltet sie gemäß einem rollenbasierten Zugriffsschema, das den erlaubten Zugriff auf das Informationssystem und die Rechte in Rollen organisiert; (b) überwacht privilegierte Rollenzuweisungen; und (c) ergreift [Zuweisung: organisationsdefinierte Aktionen], wenn privilegierte Rollenzuweisungen nicht mehr angemessen sind. Zusätzliche Empfehlungen: Privilegierte Rollen sind von der Organisation definierte Rollen, die Einzelpersonen zugewiesen werden, damit sie bestimmte sicherheitsrelevante Funktionen ausführen	iam-group-has-users-überprüfen	AWS Identity and Access Management (IAM) kann Ihnen helfen, die Prinzipien der geringsten Rechte und der Aufgabentrennung mit Zugriffsberechtigungen und Autorisierungen zu integrieren, indem sichergestellt wird, dass IAM-Gruppen mindestens einen IAM-Benutzer haben. Die Einteilung von IAM-Benutzern in Gruppen auf der Grundlage der ihnen zugewiesenen Berechtigungen oder Aufgabenbereiche ist eine Möglichkeit, die geringsten Rechte zu berücksichtigen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	können, zu denen normale Benutzer nicht berechtigt sind. Zu diesen privilegi erten Rollen gehört zum Beispiel die Verwaltung von Schlüsseln, Konten, Netzwerken und Systemen, Datenbank en und Websites.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-2(7)	Die Organisation: (a) richtet privilegi erte Benutzerk onten gemäß einem rollenbasierten Zugriffsschema ein, das den erlaubten Zugriff auf das Informationssystem und die Rechte in Rollen organisiert; (b) überwacht privilegi erte Rollenzuw eisungen; und (c) ergreift [Zuweisung: organisationsdefin ierte Aktionen] , wenn privilegi erte Rollenzuw eisungen nicht mehr angemesse n sind. Zusätzlic he Empfehlun gen: Privilegierte Rollen sind von der Organisation definierte Rollen, die Einzelpersonen zugewiesen werden, damit sie bestimmte sicherheitsrelevante Funktionen ausführen können, zu denen	iam-inline-policy-blocked-kms-Aktionen	Stellen Sie sicher, dass ein Benutzer, eine IAM-Rolle oder eine IAM-Gruppe (AWS Identity and Access Management) nicht über eine Inline-Richtlinie verfügt, die blockierte Aktionen für alle AWS Schlüssel des Key Management Service zulässt. AWS empfiehlt, verwaltet e Richtlinien anstelle von Inline-Richtlinien zu verwenden. Verwaltete Richtlini en ermöglichen Wiederverwendbarke it, Versionsverwaltung , Rollback und Delegierung der Berechtigungsverwa ltung. Mit dieser Regel können Sie den blockedActionsPatt erns Parameter festlegen. (Wert „AWS Bewährte grundlege nde Sicherhei tsmethoden“: kms: Decrypt, kms:ReEnc ryptFrom). Die

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	normale Benutzer nicht berechtigt sind. Zu diesen privilegi erten Rollen gehört zum Beispiel die Verwaltung von Schlüsseln, Konten, Netzwerken und Systemen, Datenbank en und Websites.		tatsächlichen Werte müssen den Richtlini en Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-2(7)	Die Organisation: (a) richtet privilegi erte Benutzerk onten gemäß einem rollenbasierten Zugriffsschema ein, das den erlaubten Zugriff auf das Informationssystem und die Rechte in Rollen organisiert; (b) überwacht privilegi erte Rollenzuw eisungen; und (c) ergreift [Zuweisung: organisationsdefin ierte Aktionen] , wenn privilegi erte Rollenzuw eisungen nicht mehr angemesse n sind. Zusätzlic he Empfehlun gen: Privilegierte Rollen sind von der Organisation definierte Rollen, die Einzelpersonen zugewiesen werden, damit sie bestimmte sicherheitsrelevante Funktionen ausführen können, zu denen	iam-no-inline-policy-überprüfen	Stellen Sie sicher, dass ein Benutzer, eine IAM-Rolle oder eine IAM-Gruppe (AWS Identity and Access Management) nicht über eine Inline-Richtlinie zur Zugriffsk ontrolle auf Systeme und Ressource n verfügt. AWS empfiehlt, verwaltet e Richtlinien anstelle von Inline-Richtlinien zu verwenden. Verwaltete Richtlini en ermöglichen Wiederverwendbarke it, Versionsverwaltung , Rollback und Delegierung der Berechtigungsverwa ltung.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	normale Benutzer nicht berechtigt sind. Zu diesen privilegi erten Rollen gehört zum Beispiel die Verwaltung von Schlüsseln, Konten, Netzwerken und Systemen, Datenbank en und Websites.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SI-11	Das Informati onssystem: a. Generiert Fehlermel dungen mit für Korrekturmaßnahmen erforderlichen Informationen, ohne Informationen preiszugeben, die von Angreifern ausgenutzt werden könnten; und b. Zeigt Fehlermeldungen nur für [Zuweisung: von der Organisation ernanntes Personal oder definierte Rollen] an. Zusätzliche Hinweise: Organizat ions prüfen sorgfälti g, welche structure /content of error messages. The extent to which information systems are able to identify and handle error conditions is guided by organizat ional policy and operational requireme nts. Information that could be exploited by adversaries	s-3 bucket-logging-enabled	Die Amazon Simple Storage Service (Amazon S3)-Serverzugriffs protokollierung bietet eine Methode zur Überwachu ng des Netzwerks im Hinblick auf potenzielle Cybersich erheitsereignisse. Die Ereignisse werden überwacht, indem detaillierte Aufzeichn ungen über die Anfragen erfasst werden, die an einen Amazon-S3-Bucket gestellt wurden. Jeder Zugriffsprotokolle intrag enthält Details zu einer einzelnen Zugriffsanfrage. Zu den Details gehören Anforderer, Bucket-Name, Anforderu ngszeit, Anforderu ngsaktion, Antwortst atus und Fehlercode, falls relevant.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	includes, for example, erroneous logon attempts with passwords entered by mistake as the username, mission/business Informationen aus aufgezeichneten Informationen und persönlichen Informationen wie Kontonummern, Sozialversicherungsnummern und Kreditkartennummern abgeleitet werden können (sofern nicht ausdrücklich angegeben). Darüber hinaus können Fehlermeldungen einen verdeckten Kanal für die Übertragung von Informationen bieten. Verwandte Kontrollen: AU-2, AU-3, SC-31. Verbesserungen der Kontrolle: Keine. Referenzen: Keine.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SI-11	Das Informati onssystem: a. Generiert Fehlermel dungen mit für Korrekturmaßnahmen erforderlichen Informationen, ohne Informationen preiszugeben, die von Angreifern ausgenutzt werden könnten; und b. Zeigt Fehlermeldungen nur für [Zuweisung: von der Organisation ernanntes Personal oder definierte Rollen] an. Zusätzliche Hinweise: Organizat ions prüfen sorgfälti g, welche structure /content of error messages. The extent to which information systems are able to identify and handle error conditions is guided by organizat ional policy and operational requireme nts. Information that could be exploited by adversaries	codebuild-project-logging-enabled	Stellen Sie sicher, dass die AWS CodeBuild Projektpr otokollierung aktiviert ist, damit Ihre Build-Ausgabeproto kolle entweder an Amazon CloudWatc h oder Amazon Simple Storage Service (Amazon S3) gesendet werden. Build-Ausgabeproto kolle enthalten detaillierte Informati onen zu Ihrem Build-Projekt.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	includes, for example, erroneous logon attempts with passwords entered by mistake as the username, mission/business Informationen aus aufgezeichneten Informationen und persönlichen Informationen wie Kontonummern, Sozialversicherungsnummern und Kreditkartennummern abgeleitet werden können (sofern nicht ausdrücklich angegeben). Darüber hinaus können Fehlermeldungen einen verdeckten Kanal für die Übertragung von Informationen bieten. Verwandte Kontrollen: AU-2, AU-3, SC-31. Verbesserungen der Kontrolle: Keine. Referenzen: Keine.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SI-11	Das Informationssystem: a. Generiert Fehlermeldungen mit für Korrekturmaßnahmen erforderlichen Informationen, ohne Informationen preiszugeben, die von Angreifern ausgenutzt werden könnten; und b. Zeigt Fehlermeldungen nur für [Zuweisung: von der Organisation ernanntes Personal oder definierte Rollen] an. Zusätzliche Hinweise: Organizations prüfen sorgfältig, welche structure /content of error messages. The extent to which information systems are able to identify and handle error conditions is guided by organizational policy and operational requirements. Information that could be exploited by adversaries	vpc-flow-logs-enabled	VPC-Flow-Protokolle erfassen detaillierte Informationsdatensätze über den IP-Datenverkehr, der zu und von Netzwerkschnittstellen in Ihrer Amazon Virtual Private Cloud (Amazon VPC) fließt. Standardmäßig enthalten Flow-Protokolldatensätze Werte für die verschiedenen Komponenten des IP-Flows, einschließlich Quelle, Ziel und Protokoll.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	includes, for example, erroneous logon attempts with passwords entered by mistake as the username, mission/business Informationen aus aufgezeichneten Informationen und persönlichen Informationen wie Kontonummern, Sozialversicherungsnummern und Kreditkartennummern abgeleitet werden können (sofern nicht ausdrücklich angegeben). Darüber hinaus können Fehlermeldungen einen verdeckten Kanal für die Übertragung von Informationen bieten. Verwandte Kontrollen: AU-2, AU-3, SC-31. Verbesserungen der Kontrolle: Keine. Referenzen: Keine.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SI-11	Das Informati onssystem: a. Generiert Fehlermel dungen mit für Korrekturmaßnahmen erforderlichen Informationen, ohne Informationen preiszugeben, die von Angreifern ausgenutzt werden könnten; und b. Zeigt Fehlermeldungen nur für [Zuweisung: von der Organisation ernanntes Personal oder definierte Rollen] an. Zusätzliche Hinweise: Organizat ions prüfen sorgfälti g, welche structure /content of error messages. The extent to which information systems are able to identify and handle error conditions is guided by organizat ional policy and operational requireme nts. Information that could be exploited by adversaries	api-gw-execution-l ogging-aktiviert	Die API-Gateway-Protokollierung zeigt detaillierte Ansichten der Benutzer, die auf die API zugegriff en haben, und wie diese Benutzer auf die API zugegriff en haben. Diese Einblicke ermöglichen die Transparenz von Benutzeraktivitäten.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	includes, for example, erroneous logon attempts with passwords entered by mistake as the username, mission/business Informationen aus aufgezeichneten Informationen und persönlichen Informationen wie Kontonummern, Sozialversicherungsnummern und Kreditkartennummern abgeleitet werden können (sofern nicht ausdrücklich angegeben). Darüber hinaus können Fehlermeldungen einen verdeckten Kanal für die Übertragung von Informationen bieten. Verwandte Kontrollen: AU-2, AU-3, SC-31. Verbesserungen der Kontrolle: Keine. Referenzen: Keine.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SI-11	Das Informati onssystem: a. Generiert Fehlermel dungen mit für Korrekturmaßnahmen erforderlichen Informationen, ohne Informationen preiszugeben, die von Angreifern ausgenutzt werden könnten; und b. Zeigt Fehlermeldungen nur für [Zuweisung: von der Organisation ernanntes Personal oder definierte Rollen] an. Zusätzliche Hinweise: Organizat ions prüfen sorgfälti g, welche structure /content of error messages. The extent to which information systems are able to identify and handle error conditions is guided by organizat ional policy and operational requireme nts. Information that could be exploited by adversaries	cloud-trail-cloud-watch-logs-aktiviert	Verwenden Sie Amazon CloudWatch , um Protokollereignisa ktivitäten zentral zu sammeln und zu verwalten. Durch die Aufnahme von AWS CloudTrail Daten erhalten Sie Einzelhei ten zu den API-Aufru faktivitäten innerhalb Ihres AWS Kontos.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	includes, for example, erroneous logon attempts with passwords entered by mistake as the username, mission/business Informationen aus aufgezeichneten Informationen und persönlichen Informationen wie Kontonummern, Sozialversicherungsnummern und Kreditkartennummern abgeleitet werden können (sofern nicht ausdrücklich angegeben). Darüber hinaus können Fehlermeldungen einen verdeckten Kanal für die Übertragung von Informationen bieten. Verwandte Kontrollen: AU-2, AU-3, SC-31. Verbesserungen der Kontrolle: Keine. Referenzen: Keine.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SI-11	Das Informati onssystem: a. Generiert Fehlermel dungen mit für Korrekturmaßnahmen erforderlichen Informationen, ohne Informationen preiszugeben, die von Angreifern ausgenutzt werden könnten; und b. Zeigt Fehlermeldungen nur für [Zuweisung: von der Organisation ernanntes Personal oder definierte Rollen] an. Zusätzliche Hinweise: Organizat ions prüfen sorgfälti g, welche structure /content of error messages. The extent to which information systems are able to identify and handle error conditions is guided by organizat ional policy and operational requireme nts. Information that could be exploited by adversaries	elasticsearch-logs-to-cloudwatch	Stellen Sie sicher, dass für Amazon OpenSearch Service-Domains Fehlerpro tokolle aktiviert und zur Aufbewahrung und Beantwortung an Amazon CloudWatc h Logs gestreamt werden. Domain-Fehlerprotokolle sind bei Sicherhei ts- und Zugriffsp rüfungen sowie bei der Diagnose von Verfügbarkeitsprob lemen nützlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	includes, for example, erroneous logon attempts with passwords entered by mistake as the username, mission/business Informationen aus aufgezeichneten Informationen und persönlichen Informationen wie Kontonummern, Sozialversicherungsnummern und Kreditkartennummern abgeleitet werden können (sofern nicht ausdrücklich angegeben). Darüber hinaus können Fehlermeldungen einen verdeckten Kanal für die Übertragung von Informationen bieten. Verwandte Kontrollen: AU-2, AU-3, SC-31. Verbesserungen der Kontrolle: Keine. Referenzen: Keine.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SI-3	Die Organisation: a. Setzt Mechanismen zum Schutz vor schädlichem Code an Ein- und Austrittspunkten von Informationssystemen ein, um schädlichen Code zu erkennen und zu beseitigen; b. Aktualisiert die Schutzmechanismen gegen schädlichen Code, sobald neue Versionen verfügbar sind, gemäß den Richtlinien und Verfahren der Organisation für das Konfigurationsmanagement; c. Konfiguriert Schutzmechanismen gegen schädlichen Code zu folgenden Zwecken: 1. Führen Sie regelmäßige Scans des Informationssystems [Zuweisung: von der Organisation festgelegte Häufigkeit] und Echtzeitscans	codebuild-project-envvar-awscred-überprüfen	Stellen Sie sicher, dass die Anmeldeinformationen AWS_ACCESS_KEY_ID AWS_SECRET_ACCESS_KEY nicht in AWS den Codebuild-Projektumgebungen vorhanden sind. Speichern Sie diese Variablen nicht als Klartext. Das Speichern dieser Variablen als Klartext bewirkt eine unbeabsichtigte Offenlegung von Daten sowie unberechtigte Zugriffe.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	von Dateien aus externen Quellen an [Auswahl (eine oder mehrere); Endpunkt; entry/exit points] as the files are downloaded, opened, or executed in accordance with organizational security policy; and 2. [Selection(one or more): block malicious code; quarantine malicious code; send alert to administrator; [Assignment: organization-defined action]] in response to malicious code detection; and d. Addresses the receipt of false positives during malicious code detection and eradication and the resulting potential impact on the availability of the information system. Supplemental Guidance: Information system entry and exit points include, for example, firewalls		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	, electronic mail servers, web servers, proxy servers, remote-access servers, workstations, notebook computers , and mobile devices. Malicious code includes, for example, viruses, worms, Trojan horses, and spyware. Malicious code can also be encoded in various formats(e .g., UUENCODE, Unicode), contained within compresse d or hidden files, or hidden in files using steganogr aphy. Malicious code can be transport ed by different means including, for example, web accesses, electroni c mail, electronic mail attachments, and portable storage devices. Malicious code insertions occur through the exploitat ion of information		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	system vulnerabilities. Malicious code protection mechanisms include, for example, anti-virus signature definitions and reputation-based technologies. A variety of technologies and methods exist to limit or eliminate the effects of malicious code. Pervasive configuration management and comprehensive software integrity controls may be effective in preventing execution of unauthorized code. In addition to commercial off-the-shelf software, malicious code may also be present in custom-built software. This could include, for example, logic bombs, back doors, and other types of cyber attacks that could affect organizational missions/business functions. Tradition		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	al malicious code protection mechanisms cannot always detect such code. In these situations, organizations rely instead on other safeguards including, for example, secure coding practices, configuration management and control, trusted procurement processes, and monitoring practices to help ensure that software does not perform functions other than the functions intended. Organizations may determine that in response to the detection of malicious code, different actions may be warranted. For example, organizations can define actions in response to malicious code detection during periodic scans, actions in response to		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	detection of malicious downloads, and/or Netzwerkaktionen als Reaktion auf die Erkennung böswillig er Absichten beim Versuch, Dateien zu öffnen oder auszuführ en, durch. Verwandte Kontrollen: CM-3, MP-2, SA-4, SA-8, SA-12, SA-13, SC-7, SC-26, SC-44, SI-2, SI-4, SI-7. Referenze n: NIST Sonderver öffentlichung 800-83.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SI-3	Die Organisation: a. Setzt Mechanismen zum Schutz vor schädlichem Code an Ein- und Austrittspunkten von Informationssystemen ein, um schädlichen Code zu erkennen und zu beseitigen; b. Aktualisiert die Schutzmechanismen gegen schädlichen Code, sobald neue Versionen verfügbar sind, gemäß den Richtlinien und Verfahren der Organisation für das Konfigurationsmanagement; c. Konfiguriert Schutzmechanismen gegen schädlichen Code zu folgenden Zwecken: 1. Führen Sie regelmäßige Scans des Informationssystems [Zuweisung: von der Organisation festgelegte Häufigkeit] und Echtzeitscans	codebuild-project-source-repo-URL-Prüfung	Stellen Sie sicher, dass die URL des Quell-Repositorys GitHub oder des Bitbucket-Quell-Repositorys keine persönlichen Zugriffstoken, Benutzernamen und Passwörter in den Codebuild-Projektumgebungen enthält. AWS Verwende OAuth anstelle persönlicher Zugriffstoken oder einen Benutzernamen und ein Passwort, um die Autorisierung für den Zugriff auf GitHub Bitbucket-Repositorys zu gewähren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	von Dateien aus externen Quellen bei [Auswahl (eine oder mehrere); Endpunkt; entry/exit points] as the files are downloaded, opened, or executed in accordance with organizational security policy; and 2. [Selection(one or more): block malicious code; quarantine malicious code; send alert to administrator; [Assignment: organization-defined action]] in response to malicious code detection; and d. Addresses the receipt of false positives during malicious code detection and eradication and the resulting potential impact on the availability of the information system. Supplemental Guidance: Information system entry and exit points include, for example, firewalls		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	, electronic mail servers, web servers, proxy servers, remote-access servers, workstations, notebook computers , and mobile devices. Malicious code includes, for example, viruses, worms, Trojan horses, and spyware. Malicious code can also be encoded in various formats(e .g., UUENCODE, Unicode), contained within compresse d or hidden files, or hidden in files using steganogr aphy. Malicious code can be transport ed by different means including, for example, web accesses, electroni c mail, electronic mail attachments, and portable storage devices. Malicious code insertions occur through the exploitat ion of information		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	system vulnerabi lities. Malicious code protection mechanisms include, for example, anti-viru s signature definitio ns and reputation-based technologies. A variety of technolog ies and methods exist to limit or eliminate the effects of malicious code. Pervasive configura tion management and comprehensive software integrity controls may be effective in preventing execution of unauthori zed code. In addition to commercial off-the-shelf software, malicious code may also be present in custom-built software. This could include, for example, logic bombs, back doors, and other types of cyber attacks that could affect organizational missions/business functions. Tradition		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	al malicious code protection mechanisms cannot always detect such code. In these situations, organizations rely instead on other safeguards including, for example, secure coding practices, configuration management and control, trusted procurement processes, and monitoring practices to help ensure that software does not perform functions other than the functions intended. Organizations may determine that in response to the detection of malicious code, different actions may be warranted. For example, organizations can define actions in response to malicious code detection during periodic scans, actions in response to		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	detection of malicious downloads, and/or Netzwerkaktionen als Reaktion auf die Erkennung böswillig er Absichten beim Versuch, Dateien zu öffnen oder auszuführ en, durch. Verwandte Kontrollen: CM-3, MP-2, SA-4, SA-8, SA-12, SA-13, SC-7, SC-26, SC-44, SI-2, SI-4, SI-7. Referenze n: NIST Sonderver öffentlichung 800-83.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SI-5	Die Organisation: a. Erhält fortlaufe nd Warnmeldu ngen, Hinweise und Anweisungen zur Informationssystem sicherheit von [Zuweisung: von der Organisation definiert e externe Organisat ionen]; b. Generiert nach Bedarf interne Sicherheitswarnung en, -hinweise und -anweisungen; c. Verteilt Sicherhei tswarnungen, Hinweise und Anweisungen an: [Auswahl (eine oder mehrere Optionen) : [Zuweisung: von der Organisation ernanntes Personal oder definierte Rollen]; [Zuweisun g: von der Organisat ion definierte Elemente innerhalb der Organisation]; [Zuweisung: von der Organisation definierte externe	cloudwatch-alarm-a ction-check	Amazon CloudWatch alarmiert, wenn eine Metrik den Schwellen wert für eine bestimmte Anzahl von Bewertungszeiträum en überschreitet. Der Alarm führt eine oder mehrere Aktionen durch, die vom Wert der Metrik oder des Ausdrucks im Vergleich zu einem Schwellenwert in einer Reihe von Zeiträumen abhängt. Diese Regel erfordert einen Wert für alarmActionRequired (Config Default: True), insufficientDataAc tion Required (Config Default: True), okActionRequired (Config Default: False). Der tatsächli che Wert muss die Alarmaktionen für Ihre Umgebung widerspie geln.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	Organisationen]]; und d. Implement iert Sicherheitsrichtli nien gemäß den festgelegten Zeitpläne n oder benachric htigt die ausstellende Organisation über den Grad der Nichteinh altung. Zusätzlic he Empfehlungen: Das United States Computer Emergency Readiness Team (US-CERT) generiert Sicherheitswarnung en und -hinweise, um der Bundesregierung kontinuierlich situation sbedingte Informati onen zukommen zu lassen. Sicherhei tsrichtlinien werden von der OMB oder anderen benannten Organisationen herausgegeben, die für die Erstellun g solcher Richtlini en verantwortlich und befugt sind. Die Einhaltung von Sicherheitsrichtli nien ist aufgrund		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	der Kritizität vieler dieser Richtlinien und der möglichen unmittelbaren negativen Auswirkun gen einer verspätet en Umsetzung der Richtlinien auf organisat orische Abläufe und Ressourcen, Einzelpersonen, andere Organisat ionen und die Nation von entscheidender Bedeutung. Zu den externen Organisat ionen gehören beispielsweise externe mission/b usiness partners, supply chain partners, external service providers, and other peer/supporting Organisationen. Verwandte Kontrolle : SI-2. Referenze n: NIST Sonderver öffentlichung 800-40.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SI-5	Die Organisation: a. Erhält fortlaufe nd Warnmeldu ngen, Hinweise und Anweisungen zur Informationssystem sicherheit von [Zuweisung: von der Organisation definiert e externe Organisat ionen]; b. Generiert nach Bedarf interne Sicherheitswarnung en, -hinweise und -anweisungen; c. Verteilt Sicherhei tswarnungen, Hinweise und Anweisungen an: [Auswahl (eine oder mehrere Optionen) : [Zuweisung: von der Organisation ernanntes Personal oder definierte Rollen]; [Zuweisun g: von der Organisat ion definierte Elemente innerhalb der Organisation]; [Zuweisung: von der Organisation definierte externe	securityhub-enabled	AWS Security Hub hilft bei der Überwachung von unbefugtem Personal, Verbindun gen, Geräten und Software. AWS Security Hub aggregiert, organisie rt und priorisie rt die Sicherhei tswarnungen oder Ergebnisse mehrerer Dienste. AWS Einige dieser Dienste sind Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer und AWS Firewall Manager sowie AWS Partnerlösungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	Organisationen]]; und d. Implement iert Sicherheitsrichtli nien gemäß den festgelegten Zeitpläne n oder benachric htigt die ausstellende Organisation über den Grad der Nichteinh altung. Zusätzlic he Empfehlungen: Das United States Computer Emergency Readiness Team (US-CERT) generiert Sicherheitswarnung en und -hinweise, um der Bundesregierung kontinuierlich situation sbedingte Informati onen zukommen zu lassen. Sicherhei tsrichtlinien werden von der OMB oder anderen benannten Organisationen herausgegeben, die für die Erstellun g solcher Richtlini en verantwortlich und befugt sind. Die Einhaltung von Sicherheitsrichtli nien ist aufgrund		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	der Kritizität vieler dieser Richtlinien und der möglichen unmittelbaren negativen Auswirkun gen einer verspätet en Umsetzung der Richtlinien auf organisat orische Abläufe und Ressourcen, Einzelpersonen, andere Organisat ionen und die Nation von entscheidender Bedeutung. Zu den externen Organisat ionen gehören beispielsweise externe mission/b usiness partners, supply chain partners, external service providers, and other peer/supporting Organisationen. Verwandte Kontrolle : SI-2. Referenze n: NIST Sonderver öffentlichung 800-40.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SI-5	Die Organisation: a. Erhält fortlaufe nd Warnmeldu ngen, Hinweise und Anweisungen zur Informationssystem sicherheit von [Zuweisung: von der Organisation definiert e externe Organisat ionen]; b. Generiert nach Bedarf interne Sicherheitswarnung en, -hinweise und -anweisungen; c. Verteilt Sicherhei tswarnungen, Hinweise und Anweisungen an: [Auswahl (eine oder mehrere Optionen) : [Zuweisung: von der Organisation ernanntes Personal oder definierte Rollen]; [Zuweisun g: von der Organisat ion definierte Elemente innerhalb der Organisation]; [Zuweisung: von der Organisation definierte externe	guardduty-enabled-centralized	Amazon GuardDuty kann mithilfe von Threat Intellige nce Feeds helfen, potenzielle Cybersich erheitsereignisse zu überwachen und zu erkennen. Dazu gehören Listen mit bösartigen IPs und maschinel len Lernmethoden zur Identifizierung unerwarteter, nicht autorisierter und bösartiger Aktivitäten in Ihrer AWS Cloud-Umgebung.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	Organisationen]]; und d. Implement iert Sicherheitsrichtli nien gemäß den festgelegten Zeitpläne n oder benachric htigt die ausstellende Organisation über den Grad der Nichteinh altung. Zusätzlic he Empfehlungen: Das United States Computer Emergency Readiness Team (US-CERT) generiert Sicherheitswarnung en und -hinweise, um der Bundesregierung kontinuierlich situation sbedingte Informati onen zukommen zu lassen. Sicherhei tsrichtlinien werden von der OMB oder anderen benannten Organisationen herausgegeben, die für die Erstellun g solcher Richtlini en verantwortlich und befugt sind. Die Einhaltung von Sicherheitsrichtli nien ist aufgrund		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	der Kritizität vieler dieser Richtlinien und der möglichen unmittelbaren negativen Auswirkungen einer verspäteten Umsetzung der Richtlinien auf organisatorische Abläufe und Ressourcen, Einzelpersonen, andere Organisationen und die Nation von entscheidender Bedeutung. Zu den externen Organisationen gehören beispielsweise externe mission/business partners, supply chain partners, external service providers, and other peer/supporting Organisationen. Verwandte Kontrolle: SI-2. Referenzen: NIST Sonderveröffentlichung 800-40.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SI-5	Die Organisation: a. Erhält fortlaufend Warnmeldungen, Hinweise und Anweisungen zur Informationssystemsicherheit von [Zuweisung: von der Organisation definierte externe Organisationen]; b. Generiert nach Bedarf interne Sicherheitswarnungen, -hinweise und -anweisungen; c. Verteilt Sicherheitswarnungen, Hinweise und Anweisungen an: [Auswahl (eine oder mehrere Optionen): [Zuweisung: von der Organisation ernanntes Personal oder definierte Rollen]; [Zuweisung: von der Organisation definierte Elemente innerhalb der Organisation]; [Zuweisung: von der Organisation definierte externe	guardduty-non-archived-findings	Amazon GuardDuty hilft Ihnen dabei, die Auswirkungen eines Vorfalls zu verstehen, indem es die Ergebnisse nach Schweregrad klassifiziert: niedrig, mittel und hoch. Diese Klassifizierungen können Sie zur Festlegung von entsprechenden Strategien und Prioritäten zur Behebung solcher Vorfälle verwenden. Mit dieser Regel können Sie optional daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7) und daysHighSev (Config Default: 1) für nicht archivierte Ergebnisse festlegen, wie es die Richtlinien Ihrer Organisation erfordern.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	Organisationen]]; und d. Implement iert Sicherheitsrichtli nien gemäß den festgelegten Zeitpläne n oder benachric htigt die ausstellende Organisation über den Grad der Nichteinh altung. Zusätzlic he Empfehlungen: Das United States Computer Emergency Readiness Team (US-CERT) generiert Sicherheitswarnung en und -hinweise, um der Bundesregierung kontinuierlich situation sbedingte Informati onen zukommen zu lassen. Sicherhei tsrichtlinien werden von der OMB oder anderen benannten Organisationen herausgegeben, die für die Erstellun g solcher Richtlini en verantwortlich und befugt sind. Die Einhaltung von Sicherheitsrichtli nien ist aufgrund		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	der Kritizität vieler dieser Richtlinien und der möglichen unmittelbaren negativen Auswirkun gen einer verspätet en Umsetzung der Richtlinien auf organisat orische Abläufe und Ressourcen, Einzelpersonen, andere Organisat ionen und die Nation von entscheidender Bedeutung. Zu den externen Organisat ionen gehören beispielsweise externe mission/b usiness partners, supply chain partners, external service providers, and other peer/supporting Organisationen. Verwandte Kontrolle : SI-2. Referenze n: NIST Sonderver öffentlichung 800-40.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-2(4)	Das Informati onssystem prüft automatisch Aktionen wie die Erstellung, Änderung, Aktivieru ng, Deaktivierung und Entfernung von Konten und benachric htigt [Zuordnung: von der Organisation designierte Mitarbeiter oder Rollen].	codebuild-project-logging-enabled	Stellen Sie sicher, dass die AWS CodeBuild Projektpr otokollierung aktiviert ist, damit Ihre Build-Ausgabeproto kolle entweder an Amazon CloudWatc h oder Amazon Simple Storage Service (Amazon S3) gesendet werden. Build-Ausgabeproto kolle enthalten detaillierte Informati onen zu Ihrem Build-Projekt.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-2(g)	Die Organisation: g. Überwacht die Verwendung von Konten im Informationssystem.	codebuild-project-logging-enabled	Stellen Sie sicher, dass die AWS CodeBuild Projektprotokollierung aktiviert ist, damit Ihre Build-Ausgabeprotokolle entweder an Amazon CloudWatch oder Amazon Simple Storage Service (Amazon S3) gesendet werden. Build-Ausgabeprotokolle enthalten detaillierte Informationen zu Ihrem Build-Projekt.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AU-12(a)(c)	Das Informati onssystem: a. Ermöglicht die Generierung von Prüfungsunterlagen für die in AU-2 a. definierten prüffähig en Ereignisse für alle Informationssystem - und Netzwerkk omponenten, bei denen Prüfungsf unktionen bereitges tellt/verfügbar sind c. Generiert Prüfungsu nterlagen für die in AU-2 d. definierten Ereignisse mit dem in AU-3 definierten Inhalt.	codebuild-project-logging-enabled	Stellen Sie sicher, dass die AWS CodeBuild Projektpr otokollierung aktiviert ist, damit Ihre Build-Ausgabeproto kolle entweder an Amazon CloudWatc h oder Amazon Simple Storage Service (Amazon S3) gesendet werden. Build-Ausgabeproto kolle enthalten detaillierte Informati onen zu Ihrem Build-Projekt.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AU-2(a)(d)	Die Organisation: a. Legt fest, dass das Informationssystem folgenden Ereignisse überprüfen kann: Erfolgreiche und erfolglose Kontoanmeldungen, Kontoverwaltungsereignisse, Objektzugriffe, Richtlinienänderungen, Berechtigungsfunktionen, Prozessnachverfolgung und Systemereignisse. Für Webanwendungen: sämtliche Administratoraktivitäten, Authentifizierungsprüfungen, Autorisierungsprüfungen, Datenlöschungen, Datenzugriffe, Datenänderungen und Berechtigungsänderungen. d. Legt fest, dass die folgenden Ereignisse innerhalb des Informationssystems geprüft werden müssen: [von der	codebuild-project-logging-enabled	Stellen Sie sicher, dass die AWS CodeBuild Projektprotokollierung aktiviert ist, damit Ihre Build-Ausgabeprotokolle entweder an Amazon CloudWatch oder Amazon Simple Storage Service (Amazon S3) gesendet werden. Build-Ausgabeprotokolle enthalten detaillierte Informationen zu Ihrem Build-Projekt.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	Organisation definiert e Teilmenge der in AU-2(a) definierten prüffähigen Ereigniss e wird kontinuierlich für jedes identifizierte Ereignis geprüft].		
AU-3	Das Informati onssystem generiert Prüfprotokolle mit Informationen, aus denen hervorgeh t, welche Art von Ereignis eingetret en ist, wann und wo das Ereignis stattgefunden hat, welchen Ursprung das Ereignis hat, wie es ausging und mit welchen Personen oder Subjekten das Ereignis in Verbindun g steht.	codebuild-project-logging-enabled	Stellen Sie sicher, dass die AWS CodeBuild Projektpr otokollierung aktiviert ist, damit Ihre Build-Ausgabeproto kolle entweder an Amazon CloudWatc h oder Amazon Simple Storage Service (Amazon S3) gesendet werden. Build-Ausgabeproto kolle enthalten detaillierte Informati onen zu Ihrem Build-Projekt.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AU-6(1)(3)	(1) Die Organisation setzt automatisierte Mechanismen zur Integration von Prüfungs-, Analyse- und Berichtsprozessen ein, um die Prozesse der Organisation zur Untersuchung und Reaktion auf verdächtige Aktivitäten zu unterstützen. (3) Die Organisation analysiert und korreliert Prüfungsunterlagen aus verschiedenen Repositorys, um sich ein Bild über die Situation in der gesamten Organisation zu verschaffen.	codebuild-project-logging-enabled	Stellen Sie sicher, dass die AWS CodeBuild Projektprotokollierung aktiviert ist, damit Ihre Build-Ausgabeprotokolle entweder an Amazon CloudWatch oder Amazon Simple Storage Service (Amazon S3) gesendet werden. Build-Ausgabeprotokolle enthalten detaillierte Informationen zu Ihrem Build-Projekt.

Vorlage

Die Vorlage ist verfügbar unter GitHub: Operational Best Practices for FedRAMP (High Part 1).

Bewährte Betriebspraktiken für FedRAMP (High Part 2)

Konformitätspakete bieten ein allgemeines Compliance-Framework, das es Ihnen ermöglicht, mithilfe verwalteter oder benutzerdefinierter Regeln und Abhilfemaßnahmen Kontrollen zur Sicherheits-, Betriebs- oder Kostenoptimierung durchzuführen. AWS Config AWS Config Conformance Packs dienen als Beispielvorlagen nicht dazu, die vollständige Einhaltung eines bestimmten Governance-

oder Compliance-Standards sicherzustellen. Sie sind dafür verantwortlich, selbst zu beurteilen, ob Ihre Nutzung der Services den geltenden gesetzlichen und behördlichen Anforderungen entspricht.

Im Folgenden finden Sie ein Beispiel für eine Zuordnung zwischen dem Federal Risk and Authorization Management Program (FedRAMP) und AWS verwalteten Konfigurationsregeln. Jede Config-Regel gilt für eine bestimmte AWS Ressource und bezieht sich auf ein oder mehrere FedRAMP-Steuerelemente. Eine FedRAMP-Kontrolle kann mehreren Config-Regeln zugeordnet werden. In der folgenden Tabelle finden Sie weitere Informationen und Anleitungen zu diesen Zuordnungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-02 (11)	Das Informationssystem setzt organisationsdefinierte Umstände und/oder Nutzungsbedingungen für organisationsdefinierte Systemkonten durch.	guardduty-enabled-centralized	Verwenden Sie Amazon GuardDuty , um die Verwendung von kurzfristigen Anmeldeinformationen im Zusammenhang mit IAM-Instance-Rollen zu überwachen. Amazon kann GuardDuty mithilfe von Check überprüfen, ob Anmeldeinformationen in IAM-Instanzprofilen exfiltriert wurden. UnauthorizedAccess
AC-02 (12) (a)	Die Organisation: a. Überwacht die Konten des Informationssystems im Hinblick auf [Zuordnung: von der Organisation	cloudtrail-security-trail-enabled	AWS CloudTrail kann durch die Aufzeichnung von Aktionen und API-Aufrufen in der AWS Management Console bei der Nichtabstreitbarkeit

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	definierte untypische Nutzung].		helfen. Sie können die Benutzer und AWS Konten, die einen AWS Dienst aufgerufen haben, die Quell-IP-Adresse, über die die Anrufe generiert wurden, und die Zeitpunkte der Anrufe identifiz ieren. Einzelheiten zu den erfassten Daten finden Sie in den AWS CloudTrail Datensatzinhalten.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-06 (03)	Die Organisation autorisiert den Netzwerkzugriff für zugewiese nes Personal nur dann, wenn dies zur Erledigung der Aufgabe für den Zugriff auf den Sicherheitsplan erforderlich ist.	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) Security Groups können bei der Verwaltung des Netzwerkzugriffs helfen, indem sie eine statusbeh aftete Filterung von eingehendem und ausgehendem Netzwerkverkehr zu Ressourcen bereitste llen. AWS Wenn Sie eingehenden (oder entfernten) Datenverk ehr von 0.0.0.0/0 bis Port 22 auf Ihren Ressourcen nicht zulassen, können Sie den Remote-Zugriff einschränken.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-06 (03)	Die Organisation autorisiert den Netzwerkzugriff auf [Zuweisung: organisationsdefinierte privilegierte Befehle] nur für [Aufgabe: organisationsdefinierte zwingende betriebliche Anforderungen] und dokumentiert die Gründe für diesen Zugriff im Sicherheitsplan für das System.	vpc-default-security-group-geschlossen	Sicherheitsgruppen von Amazon Elastic Compute Cloud (Amazon EC2) können bei der Verwaltung des Netzwerkzugriffs helfen, indem sie eine statusbehaftete Filterung des ein- und ausgehenden Netzwerkverkehrs zu Ressourcen bereitstellen. AWS Die Beschränkung des gesamten Datenverkehrs auf die Standardsicherheitsgruppe hilft dabei, den Fernzugriff auf Ihre Ressourcen einzuschränken. AWS

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-06 (03)	Die Organisation autorisiert den Netzwerkzugriff auf [Zuweisung: organisationsdefinierte privilegierte Befehle] nur für [Aufgabe: organisationsdefinierte zwingende betriebliche Anforderungen] und dokumentiert die Gründe für diesen Zugriff im Sicherheitsplan für das System.	subnet-auto-assign-public-ip-deaktiviert	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon Virtual Private Cloud (VPC) -Subnetzen nicht automatisch eine öffentliche IP-Adresse zugewiesen wird. Amazon Elastic Compute Cloud (EC2) -Instances, die in Subnetzen gestartet werden, in denen dieses Attribut aktiviert ist, haben ihrer primären Netzwerkschnittstelle eine öffentliche IP-Adresse zugewiesen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-06 (03)	Die Organisation autorisiert den Netzwerkzugriff auf [Zuweisung: organisationsdefinierte privilegierte Befehle] nur für [Aufgabe: organisationsdefinierte zwingende betriebliche Anforderungen] und dokumentiert die Gründe für diesen Zugriff im Sicherheitsplan für das System.	autoscaling-launch-config-public-ip-deaktiviert	Wenn Sie Ihre Netzwerkschnittstellen mit einer öffentlichen IP-Adresse konfigurieren, sind die diesen Netzwerkschnittstellen zugehörigen Ressourcen über das Internet erreichbar. EC2 Ressourcen sollten nicht öffentlich zugänglich sein, da dies einen unbeabsichtigten Zugriff auf Ihre Anwendungen oder Server ermöglichen kann.
AC-06 (03)	Die Organisation autorisiert den Netzwerkzugriff auf [Zuweisung: organisationsdefinierte privilegierte Befehle] nur für [Aufgabe: organisationsdefinierte zwingende betriebliche Anforderungen] und dokumentiert die Gründe für diesen Zugriff im Sicherheitsplan für das System.	emr-master-no-public-ip	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon EMR-Cluster-Masterknoten nicht öffentlich zugänglich sind. Amazon-EMR-Cluster-Hauptknoten können vertrauliche Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-06 (03)	Die Organisation autorisiert den Netzwerkzugriff auf [Zuweisung: organisationsdefinierte privilegierte Befehle] nur für [Aufgabe: organisationsdefinierte zwingende betriebliche Anforderungen] und dokumentiert die Gründe für diesen Zugriff im Sicherheitsplan für das System.	lambda-function-public-access-verboten	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass AWS Lambda-Funktionen nicht öffentlich zugänglich sind. Der öffentliche Zugriff kann möglicherweise die Verfügbarkeit von Ressourcen beeinträchtigen.
AC-06 (03)	Die Organisation autorisiert den Netzwerkzugriff auf [Zuweisung: organisationsdefinierte privilegierte Befehle] nur für [Aufgabe: organisationsdefinierte zwingende betriebliche Anforderungen] und dokumentiert die Gründe für diesen Zugriff im Sicherheitsplan für das System.	rds-instance-public-access-überprüfen	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Relational Database Service (Amazon RDS) -Instances nicht öffentlich sind. Amazon-RDS-Datenbank-Instances können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-06 (03)	Die Organisation autorisiert den Netzwerkzugriff auf [Zuweisung: organisationsdefinierte privilegierte Befehle] nur für [Aufgabe: organisationsdefinierte zwingende betriebliche Anforderungen] und dokumentiert die Gründe für diesen Zugriff im Sicherheitsplan für das System.	redshift-cluster-public-access-überprüfen	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Redshift Redshift-Cluster nicht öffentlich sind. Amazon-Redshift-Cluster können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.
AC-06 (03)	Die Organisation autorisiert den Netzwerkzugriff auf [Zuweisung: organisationsdefinierte privilegierte Befehle] nur für [Aufgabe: organisationsdefinierte zwingende betriebliche Anforderungen] und dokumentiert die Gründe für diesen Zugriff im Sicherheitsplan für das System.	sagemaker-notebook-no-direct-Internetzugang	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass SageMaker Amazon-Notebooks keinen direkten Internetzugang zulassen. Indem Sie direkten Internetzugang blockieren, vermeiden Sie, dass unbefugte Benutzer auf sensible Daten zugreifen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-06 (03)	Die Organisation autorisiert den Netzwerkzugriff auf [Zuweisung: organisationsdefinierte privilegierte Befehle] nur für [Aufgabe: organisationsdefinierte zwingende betriebliche Anforderungen] und dokumentiert die Gründe für diesen Zugriff im Sicherheitsplan für das System.	eks-endpoint-no-public-Zugang	Verwalten Sie den Zugriff auf Ihren Amazon Elastic Kubernetes Service (Amazon EKS) - Cluster, indem Sie sicherstellen, dass der Kubernetes-API-Serverendpunkt nicht öffentlich zugänglich ist. Indem Sie den öffentlichen Zugriff auf den Kubernetes API-Serverendpunkt einschränken, können Sie das Risiko eines unbefugten Zugriffs auf Ihren EKS-Cluster und seine Ressourcen verringern.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AU-05 (02)	Das Informationssystem warnt wichtige Mitarbeiter innerhalb der festgelegten Zeit, wenn das zugewiesene Speichervolumen für Audit-Logs einen bestimmten Prozentsatz der maximalen Audit-Log-Speicherkapazität des Repositorys erreicht.	cloudwatch-alarm-action-check	Amazon CloudWatch alarmiert, wenn eine Metrik den Schwellenwert für eine bestimmte Anzahl von Bewertungszeiträumen überschreitet. Der Alarm führt eine oder mehrere Aktionen durch, die vom Wert der Metrik oder des Ausdrucks im Vergleich zu einem Schwellenwert in einer Reihe von Zeiträumen abhängt. Diese Regel erfordert einen Wert für alarmActionRequired (Config Default: True), insufficientDataAction Required (Config Default: True), okActionRequired (Config Default: False). Der tatsächliche Wert muss die Alarmaktionen für Ihre Umgebung widerspiegeln.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AU-06 (04)	Prüfung, Analyse und Berichterstattung von Prüfungsunterlagen | Zentrale Überprüfung und Analyse	elasticsearch-logs-to-cloudwatch	Stellen Sie sicher, dass für Amazon OpenSearch Service-Domains Fehlerprotokolle aktiviert und zur Aufbewahrung und Beantwortung an Amazon CloudWatch Logs gestreamt werden. Domain-Fehlerprotokolle sind bei Sicherheits- und Zugriffsprüfungen sowie bei der Diagnose von Verfügbarkeitsproblemen nützlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AU-06 (04)	Prüfung, Analyse und Berichterstattung von Prüfungsunterlagen | Zentrale Überprüfung und Analyse	multi-region-cloudtrail-enabled	AWS CloudTrail zeichnet Aktionen und API-Aufrufe der AWS Management Console auf. Sie können feststellen, welche Benutzer und Konten angerufen wurden AWS, von welcher Quell-IP-Adresse aus die Anrufe getätigt wurden und wann die Anrufe erfolgten. CloudTrail übermittelt Protokolldateien aus allen AWS Regionen an Ihren S3-Bucket , wenn MULTI_REG ION_CLOUD _TRAIL_ENABLED aktiviert ist. Außerdem wird beim AWS Start einer neuen Region derselbe Trail in der neuen Region erstellt. CloudTrail Dadurch erhalten Sie automatis ch Protokolldateien mit API-Aktivitäten für die neue Region.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AU-06 (04)	Prüfung, Analyse und Berichterstattung von Prüfungsunterlagen | Zentrale Überprüfung und Analyse	wafv2-logging-enabled	Um die Protokollierung und Überwachung in Ihrer Umgebung zu erleichtern, aktivieren Sie die AWS WAF (V2) -Protokollierung im regionalen und globalen Web. ACLs AWS Die WAF-Protokollierung bietet detaillierte Informationen über den Datenverkehr, der von Ihrer Web-ACL analysiert wird. In den Protokollen werden die Uhrzeit aufgezeichnet, zu der die AWS WAF die Anfrage von Ihrer AWS Ressource erhalten hat, Informationen über die Anfrage und eine Aktion für die Regel, der jede Anfrage entsprach.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AU-06 (04)	Prüfung, Analyse und Berichterstattung von Prüfungsunterlagen | Zentrale Überprüfung und Analyse	api-gw-execution-logging-aktiviert	Die API-Gateway-Protokollierung zeigt detaillierte Ansichten der Benutzer, die auf die API zugegriffen haben, und wie diese Benutzer auf die API zugegriffen haben. Diese Einblicke ermöglichen die Transparenz von Benutzeraktivitäten.
AU-06 (04)	Prüfung, Analyse und Berichterstattung von Prüfungsunterlagen | Zentrale Überprüfung und Analyse	cloud-trail-cloud-watch-logs-aktiviert	Verwenden Sie Amazon CloudWatch , um Protokollereignisaktivitäten zentral zu sammeln und zu verwalten. Durch die Aufnahme von AWS CloudTrail Daten erhalten Sie Einzelheiten zu den API-Aufrufaktivitäten innerhalb Ihres AWS Kontos.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AU-06 (04)	Prüfung, Analyse und Berichterstattung von Prüfungsunterlagen | Zentrale Überprüfung und Analyse	cloudtrail-enabled	AWS CloudTrail kann durch die Aufzeichnung von Aktionen und API-Aufrufen in der AWS Management Console bei der Nichtabstreitbarkeit helfen. Sie können die Benutzer und AWS Konten, die einen AWS Dienst aufgerufen haben, die Quell-IP-Adresse, über die die Anrufe generiert wurden, und die Zeitpunkte der Anrufe identifizieren. Einzelheiten zu den erfassten Daten finden Sie in den AWS CloudTrail Datensatzinhalten.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AU-06 (04)	Prüfung, Analyse und Berichterstattung von Prüfungsunterlagen | Zentrale Überprüfung und Analyse	cloudtrail-s3-data events-enabled	Die Erfassung von Simple Storage Service (Amazon S3)-Datenereignissen unterstützt die Erkennung von ungewöhnlichen Aktivitäten. Zu den Details gehören AWS Kontoinformationen, über die auf einen Amazon S3 S3-Bucket zugegriffen wurde, die IP-Adresse und die Uhrzeit des Ereignisses.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AU-06 (04)	Prüfung, Analyse und Berichterstattung von Prüfungsunterlagen | Zentrale Überprüfung und Analyse	elb-logging-enabled	Die Elastic-Load-Balancing-Aktivität ist ein zentraler Kommunikationspunkt innerhalb einer Umgebung. Stellen Sie sicher, dass die ELB-Protokollierung aktiviert ist. Die gesammelten Daten enthalten detaillierte Informationen zu Anfragen, die an den ELB gesendet wurden. Jedes Protokoll enthält Informationen wie die Zeit, zu der die Anforderung einging, die Client-IP-Adresse, Latenzen, Anforderungspfade und Serverantworten.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AU-06 (04)	Prüfung, Analyse und Berichterstattung von Prüfungsunterlagen | Zentrale Überprüfung und Analyse	rds-logging-enabled	Um die Protokollierung und Überwachung in Ihrer Umgebung zu erleichtern, stellen Sie sicher, dass die Amazon Relational Database Service (Amazon RDS)-Protokollierung aktiviert ist. Mit der Amazon-RDS-Protokollierung können Sie Ereignisse wie Verbindungen, Verbindungsabbrüche, Abfragen oder abgefragte Tabellen erfassen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AU-06 (04)	Prüfung, Analyse und Berichterstattung von Prüfungsunterlagen | Zentrale Überprüfung und Analyse	redshift-cluster-configuration-check	Um Daten im Ruhezustand zu schützen, muss die Verschlüsselung für Ihre Amazon-Redshift-Cluster aktiviert sein. Sie müssen auch sicherstellen, dass die erforderlichen Konfigurationen auf Amazon-Redshift-Clustern bereitgestellt werden. Die Prüfungsprotokollierung muss aktiviert sein, um Informationen zu Verbindungen und Benutzeraktivitäten in der Datenbank bereitzustellen. Diese Regel erfordert, dass ein Wert für clusterDbEncrypted (Config Default: TRUE) und LoggingEnabled (Config Default: TRUE) gesetzt ist. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AU-06 (04)	Prüfung, Analyse und Berichterstattung von Prüfungsunterlagen | Zentrale Überprüfung und Analyse	s-3 bucket-logging-enabled	Die Amazon Simple Storage Service (Amazon S3)-Serverzugriffs protokollierung bietet eine Methode zur Überwachu ng des Netzwerks im Hinblick auf potenzielle Cybersich erheitsereignisse. Die Ereignisse werden überwacht, indem detaillierte Aufzeichn ungen über die Anfragen erfasst werden, die an einen Amazon-S3-Bucket gestellt wurden. Jeder Zugriffsprotokolle intrag enthält Details zu einer einzelnen Zugriffsanfrage. Zu den Details gehören Anforderer, Bucket-Name, Anforderu ngszeit, Anforderu ngsaktion, Antwortst atus und Fehlercode, falls relevant.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AU-06 (04)	Prüfung, Analyse und Berichterstattung von Prüfungsunterlagen | Zentrale Überprüfung und Analyse	vpc-flow-logs-enabled	VPC-Flow-Protokolle erfassen detaillierte Informationsdatensätze über den IP-Datenverkehr, der zu und von Netzwerkschnittstellen in Ihrer Amazon Virtual Private Cloud (Amazon VPC) fließt. Standardmäßig enthalten Flow-Protokolldatensätze Werte für die verschiedenen Komponenten des IP-Flows, einschließlich Quelle, Ziel und Protokoll.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AU-06 (05)	Das Unternehm en kombiniert die Analyse von Auditaufz eichnungen mit der Analyse von Informati onen zum Schwachst ellen-Scanning, Leistungsdaten und Informationen zur Systemüberwachung, um die Fähigkeit , unangemessene oder ungewöhnl iche Aktivitäten zu identifizieren, weiter zu verbessern.	guardduty-enabled-centralized	Amazon GuardDuty kann mithilfe von Threat Intellige nce Feeds helfen, potenzielle Cybersich erheitsereignisse zu überwachen und zu erkennen. Dazu gehören Listen mit bösartigen IPs und maschinel len Lernmethoden zur Identifizierung unerwarteter, nicht autorisierter und bösartiger Aktivitäten in Ihrer AWS Cloud-Umgebung.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AU-06 (05)	Die Organisation kombiniert die Analyse von Auditaufzeichnungen mit der Analyse von [Auswahl (eine oder mehrere): Informationen zum Scannen von Sicherheitslücken; Leistungsdaten; Informationen zur Systemüberwachung; [Aufgabe: von der Organisation definierte Daten/Informationen aus anderen Quellen]], um die Fähigkeit, unangemessene oder ungewöhnliche Aktivitäten zu identifizieren, weiter zu verbessern.	securityhub-enabled	AWS Security Hub hilft bei der Überwachung von unbefugtem Personal, Verbindungen, Geräten und Software. AWS Security Hub aggregiert, organisiert und priorisiert die Sicherheitswarnungen oder Ergebnisse mehrerer Dienste. AWS Einige dieser Dienste sind Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer und AWS Firewall Manager sowie AWS Partnerlösungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AU-06 (07)	Die Organisation legt für jeden Systempro zess, jede Rolle und jeden Benutzer im Zusammenhang mit der Prüfung, Analyse und Berichterstattung von Prüfdatensätzen zulässige Aktionen fest.	iam-no-inline-policy-überprüfen	Stellen Sie sicher, dass ein Benutzer, eine IAM-Rolle oder eine IAM-Gruppe (AWS Identity and Access Management) nicht über eine Inline-Richtlinie zur Zugriffsk ontrolle auf Systeme und Ressource n verfügt. AWS empfiehlt, verwaltet e Richtlinien anstelle von Inline-Richtlinien zu verwenden. Verwaltete Richtlini en ermöglichen Wiederverwendbarke it, Versionsverwaltung , Rollback und Delegierung der Berechtigungsverwa ltung.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AU-06 (07)	Die Organisation legt die zulässige n Aktionen für jede [Auswahl (eine oder mehrere): Systempro zess; Rolle; Benutzer] fest, die mit der Prüfung, Analyse und Berichterstattung von Prüfdatensätzen in Verbindung stehen.	iam-user-no-policies-überprüfen	Diese Regel stellt sicher, dass AWS Identity and Access Management (IAM) -Richtlinien nur Gruppen oder Rollen zugewiese n werden, um den Zugriff auf Systeme und Ressourcen zu kontrollieren. Die Zuweisung von Berechtig ungen auf Gruppen- oder Rollenebene trägt dazu bei, die Wahrscheinlichkeit zu verringern, dass eine Identität übermäßige Berechtigungen erhält oder beibehält.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AU-09 (02)	Das Informationssystem implementiert kryptografische Mechanismen zum Schutz der Integrität von Prüfungsinformationen und Prüfungstools.	cloud-trail-log-file-validierung aktiviert	Verwenden Sie die Validierung von AWS CloudTrail Protokolldateien, um die Integrität von CloudTrail Protokollen zu überprüfen. Mithilfe der Protokolldateivalidierung kann festgestellt werden, ob eine Protokolldatei geändert oder gelöscht wurde oder ob sie nach der Übermittlung CloudTrail unverändert geblieben ist. Dieses Feature wurde mit dem Branchenstandard entsprechenden Algorithmen entwickelt: SHA-256 für die Hashfunktion und SHA-256 mit RSA für digitale Signaturen. Aus diesem Grund ist es rechnerisch unmöglich, CloudTrail Protokolldateien unbemerkt zu ändern, zu löschen oder zu fälschen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AU-09 (02)	Das Informati onssystem implement iert kryptografische Mechanismen zum Schutz der Integritä t von Prüfungsi nformationen und Prüfungstools.	cloud-trail-encryption-enabled	Da sensible Daten vorhanden sein können und um Daten im Ruhezustand zu schützen, sollten Sie sicherstellen, dass die Verschlüsselung für Ihre Protokoll e aktiviert ist AWS CloudTrail .
AU-09 (02)	Das Informati onssystem implement iert kryptografische Mechanismen zum Schutz der Integritä t von Prüfungsi nformationen und Prüfungstools.	cloudwatch-log-group-encrypted	Um sensible Daten im Speicher zu schützen, stellen Sie sicher, dass die Verschlüs selung für Ihre Amazon CloudWatch Log Groups aktiviert ist.
AU-09 (02)	Das Informati onssystem implement iert kryptografische Mechanismen zum Schutz der Integritä t von Prüfungsi nformationen und Prüfungstools.	s-3 default-encryption -kms	Stellen Sie sicher, dass die Verschlüs selung für Ihre Amazon Simple Storage Service (Amazon S3)-Bucke ts aktiviert ist. Um eventuell vorhanden e sensible Daten im Ruhezustand in einem Amazon-S3-Bucket zu schützen, muss die Verschlüsselung aktiviert sein.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AU-09 (03)	Das Informati onssystem liefert unwiderlegbare Beweise dafür, dass eine Person Leistunge n erbracht hat.	cloud-trail-log-file-validierung aktiviert	Verwenden Sie die Validierung von AWS CloudTrail Protokolldateien, um die Integrität von CloudTrail Protokoll en zu überprüfen. Mithilfe der Protokoll dateivalidierung kann festgestellt werden, ob eine Protokoll datei geändert oder gelöscht wurde oder ob sie nach der Übermittlung CloudTrail unverände rt geblieben ist. Dieses Feature wurde mit dem Branchens tandard entsprech enden Algorithmen entwickelt: SHA-256 für die Hashfunktion und SHA-256 mit RSA für digitale Signature n. Aus diesem Grund ist es rechnerisch unmöglich, CloudTrai l Protokolldateien unbemerkt zu ändern, zu löschen oder zu fälschen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AU-09 (03)	Das Informati onssystem schränkt den Netzwerkzugriff auf Auditprotokolldate n ein.	Wolkenspur-S3-bucket-public-access-prohibited	Stellt sicher, dass S3-Buckets, die zum Speichern von CloudTrail Protokoll en verwendet werden, nicht öffentlich zugänglich sind.
AU-10	Das Informati onssystem liefert unwiderlegbare Beweise dafür, dass eine Person (oder ein Prozess, der im Namen einer Einzelperson handelt) durchgeführt hat [Aufgabe: von der Organisation definiert e Maßnahmen, die unter die Nichtabst reitbarkeit fallen].	cloudtrail-enabled	AWS CloudTrail kann durch die Aufzeichn ung von Aktionen und API-Aufrufen der Managemen t Console bei der Nichtabstreitbarke it helfen. AWS Sie können die Benutzer und AWS Konten, die einen AWS Dienst aufgerufen haben, die Quell-IP-Adresse, über die die Anrufe generiert wurden, und die Zeitpunkte der Anrufe identifiz ieren. Einzelheiten zu den erfassten Daten finden Sie in den AWS CloudTrail Datensatzinhalten.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AU-10	Das Informati onssystem liefert unwiderlegbare Beweise dafür, dass eine Person (oder ein Prozess, der im Namen einer Einzelperson handelt) [Aufgabe: von der Organisation definiert e Maßnahmen, die unter die Nichtabst reitbarkeit fallen] durchgeführt hat.	cloud-trail-encryption-enabled	Da sensible Daten vorhanden sein können und um Daten im Speicher zu schützen, sollten Sie sicherstellen, dass die Verschlüsselung für Ihre Spuren aktiviert ist. AWS CloudTrail

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AU-10	Das Informati onssystem liefert unwiderlegbare Beweise dafür, dass eine Person (oder ein Prozess, der im Namen einer Person handelt) [Aufgabe: von der Organisation definiert e Maßnahmen, die unter die Nichtabst reitbarkeit fallen] durchgeführt hat.	multi-region-cloudtrail-enabled	AWS CloudTrail zeichnet Aktionen und API-Aufrufe der Management Console auf. AWS Sie können feststellen, welche Benutzer und Konten angerufen wurden AWS, von welcher Quell-IP-Adresse aus die Anrufe getätigt wurden und wann die Anrufe erfolgten. CloudTrail übermittelt Protokolldateien aus allen AWS Regionen an Ihren S3-Bucket , wenn MULTI_REG ION_CLOUD _TRAIL_ENABLED aktiviert ist. Außerdem wird beim AWS Start einer neuen Region derselbe Trail in der neuen Region erstellt. CloudTrail Dadurch erhalten Sie automatis ch Protokolldateien mit API-Aktivitäten für die neue Region.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AU-12	Die Organisation stellt Prüfdatensätze aus [Zuordnung: organisationsdefinierte Systemkomponenten] zu einem systemweiten (logischen oder physischen) Prüfpfad zusammen, der zeitlich mit [Zuordnung: organisationsdefiniertes Toleranzniveau für die Beziehung zwischen den Zeitstempeln einzelner Datensätze im Prüfpfad] korreliert.	s-3 bucket-logging-enabled	Die Amazon Simple Storage Service (Amazon S3)-Serverzugriffsprotokollierung bietet eine Methode zur Überwachung des Netzwerks im Hinblick auf potenzielle Cybersicherheitsereignisse. Die Ereignisse werden überwacht, indem detaillierte Aufzeichnungen über die Anfragen erfasst werden, die an einen Amazon-S3-Bucket gestellt wurden. Jeder Zugriffsprotokolleintrag enthält Details zu einer einzelnen Zugriffsanfrage. Zu den Details gehören Anforderer, Bucket-Name, Anforderungszeit, Anforderungsaktion, Antwortstatus und Fehlercode, falls relevant.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AU-12	Die Organisation stellt Prüfdatensätze aus [Zuordnung: organisationsdefinierte Systemkomponenten] in einem systemweiten (logischen oder physischen) Prüfpfad zusammen, der zeitlich mit [Aufgabe: organisationsdefiniertes Toleranzniveau für die Beziehung zwischen Zeitstempeln einzelner Datensätze im Prüfpfad] korreliert.	cloudtrail-s3-dataevents-enabled	Die Erfassung von Simple Storage Service (Amazon S3)-Datenereignissen unterstützt die Erkennung von ungewöhnlichen Aktivitäten. Zu den Details gehören AWS Kontoinformationen, über die auf einen Amazon S3 S3-Bucket zugegriffen wurde, die IP-Adresse und die Uhrzeit des Ereignisses.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AU-12	Die Organisation stellt Prüfaufze ichnungen aus [Zuordnung: organisat ionsdefinierte Systemkomponenten] zu einem systemwei ten (logischen oder physischen) Prüfpfad zusammen, der zeitlich mit [Zuordnung: organisat ionsdefiniertes Toleranzniveau für die Beziehung zwischen den Zeitstempeln einzelner Datensätze im Prüfpfad] korreliert.	cloud-trail-cloud-watch-logs-aktiviert	Verwenden Sie Amazon CloudWatch , um Protokollereignisa ktivitäten zentral zu sammeln und zu verwalten. Durch die Aufnahme von AWS CloudTrail Daten erhalten Sie Einzelhei ten zu den API-Aufru faktivitäten innerhalb Ihres AWS Kontos.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AU-12	Die Organisation stellt Prüfprotokolle aus [Aufgabe: organisationsdefinierte Systemkomponenten] zu einem systemweiten (logischen oder physischen) Prüfpfad zusammen, der zeitlich mit [Zuordnung: organisationsdefiniertes Toleranzniveau für die Beziehung zwischen den Zeitstempeln einzelner Datensätze im Prüfpfad] korreliert.	cloudtrail-enabled	AWS CloudTrail kann durch die Aufzeichnung von Aktionen und API-Aufrufen in der Management Console bei der Nichtabstreitbarkeit helfen. AWS Sie können die Benutzer und AWS Konten, die einen AWS Dienst aufgerufen haben, die Quell-IP-Adresse, über die die Anrufe generiert wurden, und die Zeitpunkte der Anrufe identifizieren. Einzelheiten zu den erfassten Daten finden Sie in den AWS CloudTrail Datensatzinhalten.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AU-12	Die Organisation stellt Prüfprotokolle aus [Aufgabe: organisationsdefinierte Systemkomponenten] zu einem systemweiten (logischen oder physischen) Prüfpfad zusammen, der zeitlich mit [Zuordnung: organisationsdefiniertes Toleranzniveau für die Beziehung zwischen den Zeitstempeln einzelner Datensätze im Prüfpfad] korreliert.	multi-region-cloudtrail-enabled	AWS CloudTrail AWS zeichnet Aktionen und API-Aufrufe der Management Console auf. Sie können feststellen, welche Benutzer und Konten angerufen wurden AWS, von welcher Quell-IP-Adresse aus die Anrufe getätigt wurden und wann die Anrufe erfolgten. CloudTrail übermittelt Protokolldateien aus allen AWS Regionen an Ihren S3-Bucket , wenn MULTI_REGION_CLOUD_TRAIL_ENABLED aktiviert ist. Außerdem wird beim AWS Start einer neuen Region derselbe Trail in der neuen Region erstellt. CloudTrail Dadurch erhalten Sie automatisch Protokolldateien mit API-Aktivitäten für die neue Region.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AU-12	Die Organisation stellt Prüfdatensätze aus [Zuordnung: organisationsdefinierte Systemkomponenten] zu einem systemweiten (logischen oder physischen) Prüfpfad zusammen, der zeitlich mit [Zuordnung: organisationsdefiniertes Toleranzniveau für die Beziehung zwischen den Zeitstempeln einzelner Datensätze im Prüfpfad] korreliert.	elb-logging-enabled	Die Elastic-Load-Balancing-Aktivität ist ein zentraler Kommunikationspunkt innerhalb einer Umgebung. Stellen Sie sicher, dass die ELB-Protokollierung aktiviert ist. Die gesammelten Daten enthalten detaillierte Informationen zu Anfragen, die an den ELB gesendet wurden. Jedes Protokoll enthält Informationen wie die Zeit, zu der die Anforderung einging, die Client-IP-Adresse, Latenzen, Anforderungspfade und Serverantworten.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AU-12	Die Organisation stellt Prüfdatensätze aus [Zuordnung: organisationsdefinierte Systemkomponenten] in einem systemweiten (logischen oder physischen) Prüfpfad zusammen, der zeitlich mit [Aufgabe: organisationsdefiniertes Toleranzniveau für die Beziehung zwischen Zeitstempeln einzelner Datensätze im Prüfpfad] korreliert.	vpc-flow-logs-enabled	VPC-Flow-Protokolle erfassen detaillierte Informationsdatensätze über den IP-Datenverkehr, der zu und von Netzwerkschnittstellen in Ihrer Amazon Virtual Private Cloud (Amazon VPC) fließt. Standardmäßig enthalten Flow-Protokolldatensätze Werte für die verschiedenen Komponenten des IP-Flows, einschließlich Quelle, Ziel und Protokoll.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AU-12	Die Organisation stellt Prüfdatensätze aus [Zuordnung: organisationsdefinierte Systemkomponenten] in einem systemweiten (logischen oder physischen) Prüfpfad zusammen, der zeitlich mit [Aufgabe: organisationsdefiniertes Toleranzniveau für die Beziehung zwischen Zeitstempeln einzelner Datensätze im Prüfpfad] korreliert.	rds-logging-enabled	Um die Protokollierung und Überwachung in Ihrer Umgebung zu erleichtern, stellen Sie sicher, dass die Amazon Relational Database Service (Amazon RDS)-Protokollierung aktiviert ist. Mit der Amazon-RDS-Protokollierung können Sie Ereignisse wie Verbindungen, Verbindungsabbrüche, Abfragen oder abgefragte Tabellen erfassen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AU-12	Die Organisation stellt Prüfdatensätze aus [Zuordnung: organisationsdefinierte Systemkomponenten] in einem systemweiten (logischen oder physischen) Prüfpfad zusammen, der zeitlich mit [Aufgabe: organisationsdefiniertes Toleranzniveau für die Beziehung zwischen Zeitstempeln einzelner Datensätze im Prüfpfad] korreliert.	wafv2-logging-enabled	Um die Protokollierung und Überwachung in Ihrer Umgebung zu erleichtern, aktivieren Sie die AWS WAF (V2) -Protokollierung im regionalen und globalen Web. ACLs AWS Die WAF-Protokollierung bietet detaillierte Informationen über den Datenverkehr, der von Ihrer Web-ACL analysiert wird. In den Protokollen werden die Uhrzeit aufgezeichnet, zu der die AWS WAF die Anfrage von Ihrer AWS Ressource erhalten hat, Informationen über die Anfrage und eine Aktion für die Regel, der jede Anfrage entsprach.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CM-03	Die Organisation bestimmt und dokumentiert die Arten von Änderungen am System, die konfigurationsgesteuert werden.	rds-instance-deletion-protection-aktiviert	Stellen Sie sicher, dass Amazon Relational Database Service (Amazon RDS)-Instances den Löschschutz aktiviert haben. Verwenden Sie den Löschschutz, um zu verhindern, dass Ihre Amazon-RDS-Instances versehentlich oder böswillig gelöscht werden, was zum Verlust der Verfügbarkeit Ihrer Anwendungen führen kann.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CM-08 (02)	Die Organisation gewährleistet die Aktualität, Vollständigkeit, Genauigkeit und Verfügbarkeit des Inventars der Systemkomponenten mithilfe von [Aufgabe: organisationsdefinierte automatisierte Mechanismen].	ec2-manager instance-managed-by-systems	Eine Bestandsaufnahme der Softwareplattformen und Anwendungen innerhalb des Unternehmens ist möglich, indem Amazon Elastic Compute Cloud (Amazon EC2) - Instances mit AWS Systems Manager verwaltet werden. Verwenden Sie AWS Systems Manager, um detaillierte Systemkonfigurationen, Betriebssystem-Patch-Levels, Namen und Typ der Dienste, Softwareinstallationen, Anwendungsname, Herausgeber und Version sowie andere Details zu Ihrer Umgebung bereitzustellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CM-08 (02)	Die Organisation gewährleistet die Aktualität, Vollständigkeit, Genauigkeit und Verfügbarkeit des Inventars der Systemkomponenten mithilfe von [Aufgabe: organisationsdefinierte automatisierte Mechanismen].	ec2-prüfen managedinstance-association-compliance-status	Verwenden Sie AWS Systems Manager Associations, um bei der Inventarisierung von Softwareplattformen und Anwendungen innerhalb eines Unternehmens zu helfen. AWS Systems Manager weist Ihren verwalteten Instanzen einen Konfigurationsstatus zu und ermöglicht es Ihnen, Basiswerte für Betriebssystem-Patch-Levels, Softwareinstallationen, Anwendungskonfigurationen und andere Details zu Ihrer Umgebung festzulegen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CM-08 (02)	Die Organisation gewährleistet die Aktualität, Vollständigkeit, Genauigkeit und Verfügbarkeit des Inventars der Systemkomponenten mithilfe von [Aufgabe: organisationsdefinierte automatisierte Mechanismen].	ec2-prüfen managedinstance-patch-compliance-status	Aktivieren Sie diese Regel, um bei der Identifizierung und Dokumentation von Sicherheitslücken in Amazon Elastic Compute Cloud (Amazon EC2) zu helfen. Die Regel prüft, ob die EC2 Amazon-Instance die Patch-Konformität im AWS Systems Manager gemäß den Richtlinien und Verfahren Ihrer Organisation einhält.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CP-02 (05)	Die Organisation erstellt einen Plan für die Fortführung der Mission und der Geschäftsfunktionen mit minimalem oder keinem Verlust der Betriebskontinuität und hält diese Kontinuität bis zur vollständigen Wiederherstellung des Systems an den primären Verarbeitungs- und/oder Speicherstandorten aufrecht.	rds-multi-az-support	Die Multi-AZ-Unterstützung in Amazon Relational Database Service (Amazon RDS) bietet eine verbesserte Verfügbarkeit und Beständigkeit von Datenbank-Instances. Wenn Sie eine Multi-AZ-Datenbank-Instance bereitstellen, erstellt Amazon RDS automatisch eine primäre Datenbank-Instance und repliziert die Daten synchron auf eine Standby-Instance in einer anderen Availability Zone. Jede Availability Zone läuft auf einer eigenen, physisch getrennten, unabhängigen Infrastruktur und ist auf eine hohe Verfügbarkeit ausgelegt. Im Falle eines Infrastrukturausfalls führt Amazon RDS einen automatis

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			chen Failover zum Standby-Modus durch, sodass Sie den Datenbankbetrieb wieder aufnehmen können, sobald der Failover abgeschlo ssen ist.
CP-06 (02)	Die Organisation konfiguriert den alternativen Speichers tandort so, dass die Wiederherstellungs vorgänge entsprech end den Zielen für Wiederherstellungs zeit und Wiederher stellungspunkt erleichtert werden.	backup-recovery-po int-minimum-Aufbew ahrungsprüfung	Prüft, ob ein Wiederherstellungs punkt frühestens nach Ablauf des angegebenen Zeitraums abläuft. Organizations legen im Rahmen der Notfallplanung Ziele für die Wiederher stellungszeit und den Erholungspunkt fest. Die Konfigura tion des alternativen Speicherstandorts umfasst die physische n Einrichtungen und die Systeme, die Wiederherstellungs vorgänge unterstüt zen und die Zugänglic hkeit und korrekte Ausführung sicherste llen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CP-06 (02)	Die Organisation konfiguriert den alternativen Speichers tandort so, dass die Wiederherstellungs vorgänge entsprech end den Zielen für Wiederherstellungs zeit und Wiederher stellungspunkt erleichtert werden.	s-3 bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) unterstützt die Aufrechterhaltung einer angemesse nen Kapazität und Verfügbarkeit. CRR ermöglicht das automatische, asynchrone Kopieren von Objekten in Amazon-S3-Buckets, um die Datenverf ügbarkeit sicherzus tellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CP-06 (02)	Die Organisation konfiguriert den alternativen Speichers tandort so, dass die Wiederherstellungs vorgänge entsprech end den Zielen für Wiederherstellungs zeit und Wiederher stellungspunkt erleichtert werden.	rds-in-backup-plan	Prüft, ob Amazon Relational Database Service (Amazon RDS) -Datenban ken in AWS Backup-Plänen vorhanden sind. Organizations legen im Rahmen der Notfallplanung Ziele für die Wiederher stellungszeit und den Erholungspunkt fest. Die Konfigura tion des alternativen Speicherstandorts umfasst die physische n Einrichtungen und die Systeme, die Wiederherstellungs vorgänge unterstüt zen und die Zugänglic hkeit und korrekte Ausführung sicherste llen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CP-06 (02)	Die Organisation konfiguriert den alternativen Speichers tandort so, dass die Wiederherstellungs vorgänge entsprech end den Zielen für Wiederherstellungs zeit und Wiederher stellungspunkt erleichtert werden.	dynamodb-in-backup-plan	Prüft, ob die Amazon DynamoDB-Tabelle in AWS Backup-Plänen vorhanden ist. Organizations legen im Rahmen der Notfallplanung Ziele für die Wiederher stellungszeit und den Erholungspunkt fest. Die Konfigura tion des alternativen Speicherstandorts umfasst die physische n Einrichtungen und die Systeme, die Wiederherstellungs vorgänge unterstüt zen und die Zugänglic hkeit und korrekte Ausführung sicherste llen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CP-06 (02)	Die Organisation konfiguriert den alternativen Speichers tandort so, dass die Wiederherstellungs vorgänge entsprech end den Zielen für Wiederherstellungs zeit und Wiederher stellungspunkt erleichtert werden.	ebs-in-backup-plan	Stellen Sie zur Unterstützung der Datensicherungspro zesse sicher, dass Ihre Amazon Elastic Block Store (Amazon EBS) -Volumes Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwaltet er Backup-Service mit einer richtlini enbasierten Backup-Lösung. Diese Lösung vereinfac ht Ihr Sicherung smanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforde rungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CP-06 (02)	Die Organisation konfiguriert den alternativen Speichers tandort so, dass die Wiederherstellungs vorgänge entsprech end den Zielen für Wiederherstellungs zeit und Wiederher stellungspunkt erleichtert werden.	efs-in-backup-plan	Um Sie bei Datensich erungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon Elastic File System (Amazon EFS) -Dateisysteme Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwaltet er Backup-Service mit einer richtlini enbasierten Backup-Lösung. Diese Lösung vereinfac ht Ihr Sicherung smanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforde rungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CP-06 (02)	Die Organisation konfiguriert den alternativen Speichers tandort so, dass die Wiederherstellungs vorgänge entsprech end den Zielen für Wiederherstellungs zeit und Wiederher stellungspunkt erleichtert werden.	elb-cross-zone-load-Balancing aktiviert	Aktivieren Sie zonenübergreifende s Load Balancing für Ihre Elastic Load Balancer (ELBs), um eine angemesse ne Kapazität und Verfügbarkeit aufrechtzuerhalten. Zonenübergreifende s Load Balancing reduziert die Notwendigkeit, die gleiche Anzahl von Instances in jeder aktivierten Availability Zone aufrechtzuerhalten. Es verbessert auch die Fähigkeit Ihrer Anwendung, den Verlust einer oder mehrerer Instances zu bewältigen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CP-06 (02)	Die Organisation konfiguriert den alternativen Speichers tandort so, dass die Wiederherstellungs vorgänge entsprech end den Zielen für Wiederherstellungs zeit und Wiederher stellungspunkt erleichtert werden.	redshift-backup-en abled	Stellen Sie zur Unterstützung der Datensicherungspro zesse sicher, dass Ihre Amazon-Re dshift-Cluster über automatisierte Snapshots verfügen. Wenn automatis ierte Snapshots für einen Cluster aktiviert sind, erstellt Redshift in regelmäßi gen Abständen Snapshots dieses Clusters. Standardm äßig erstellt Redshift alle acht Stunden oder alle 5 GB einen Snapshot für jeden Knoten mit Datenände rungen oder je nachdem, was zuerst eintritt.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CP-06 (02)	Die Organisation konfiguriert den alternativen Speichers tandort so, dass die Wiederherstellungs vorgänge entsprech end den Zielen für Wiederherstellungs zeit und Wiederher stellungspunkt erleichtert werden.	s-3 version-lifecycle-policy-check	Mit Amazon-S3-Lebenszyklusregeln können Sie Aktionen definieren, die Amazon S3 während der Lebensdau er eines Objekts ausführen soll (z. B. die Überführu ng von Objekten in eine andere Speicherklasse, ihre Archivierung oder Löschung nach einem bestimmten Zeitraum) .

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CP-06 (02)	Die Organisation konfiguriert den alternativen Speichers tandort so, dass die Wiederherstellungs vorgänge entsprech end den Zielen für Wiederherstellungs zeit und Wiederher stellungspunkt erleichtert werden.	db-instance-backup-enabled	Die Sicherung sfunktion von Amazon RDS erstellt Sicherung en Ihrer Datenbank en und Transakti onsprotokolle. Amazon RDS erstellt einen Snapshot für das Speichervolume Ihrer DB-Instance, sodass die gesamte DB-Instance gesichert wird. Sie können im System spezifische Aufbewahrungsfrist en festlegen, um Ihre Ausfallsicherheits anforderungen zu erfüllen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CP-06 (02)	Die Organisation konfiguriert den alternativen Speichers tandort so, dass die Wiederherstellungs vorgänge entsprech end den Zielen für Wiederherstellungs zeit und Wiederher stellungspunkt erleichtert werden.	dynamodb-autoscali ng-enabled	Amazon DynamoDB Auto Scaling verwendet den AWS Application Auto Scaling-Service, um die bereitgestellte Durchsatzkapazität so anzupassen, dass sie automatis ch auf tatsächli che Verkehrsm uster reagiert. Auf diese Weise kann eine Tabelle oder ein globaler sekundärer Index die bereitgestellte Lese-/Schreibkapaz ität erhöhen, um plötzliche Erhöhunge n des Datenverkehrs ohne Drosselung zu bewältigen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CP-06 (02)	Die Organisation konfiguriert den alternativen Speichers tandort so, dass die Wiederherstellungs vorgänge entsprech end den Zielen für Wiederherstellungs zeit und Wiederher stellungspunkt erleichtert werden.	dynamodb-pitr-enab led	Aktivieren Sie diese Regel, um zu überprüfen, ob die Informationen gesichert wurden. Es verwaltet auch die Backups, indem es sicherstellt, dass die point-in-time Wiederherstellung in Amazon DynamoDB aktiviert ist. Bei der Wiederherstellung werden fortlaufende Backups Ihrer Tabelle für die letzten 35 Tage gespeichert.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CP-06 (02)	Die Organisation konfiguriert den alternativen Speichers tandort so, dass die Wiederherstellungs vorgänge entsprech end den Zielen für Wiederherstellungs zeit und Wiederher stellungspunkt erleichtert werden.	elasticache-redis-cluster-automatic-Backup-Check	Wenn automatische Backups aktiviert sind, ElastiCache erstellt Amazon täglich ein Backup des Clusters. Die Sicherung kann für eine von Ihrer Organisation festgelegte Anzahl von Tagen aufbewahrt werden. Automatische Backups schützen vor Datenverlust. Bei einem Ausfall können Sie einen neuen Cluster erstellen, der Ihre Daten aus dem aktuellen Backup wiederherstellt.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CP-06 (02)	Die Organisation konfiguriert den alternativen Speichers tandort so, dass die Wiederherstellungs vorgänge entsprech end den Zielen für Wiederherstellungs zeit und Wiederher stellungspunkt erleichtert werden.	rds-multi-az-support	Die Multi-AZ-Unterstüt zung in Amazon Relational Database Service (Amazon RDS) bietet eine verbesserte Verfügbar keit und Beständig keit von Datenbank -Instances. Wenn Sie eine Multi-AZ-Datenbank-Instance bereitste llen, erstellt Amazon RDS automatisch eine primäre Datenbank-Instance und replizier t die Daten synchron auf eine Standby-Instance in einer anderen Availability Zone. Jede Availabil ity Zone läuft auf einer eigenen, physisch getrennte n, unabhängigen Infrastruktur und ist auf eine hohe Verfügbarkeit ausgelegt. Im Falle eines Infrastru kturausfalls führt Amazon RDS einen automatis

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			chen Failover zum Standby-Modus durch, sodass Sie den Datenbankbetrieb wieder aufnehmen können, sobald der Failover abgeschlo ssen ist.
CP-06 (02)	Die Organisation konfiguriert den alternativen Speichers tandort so, dass die Wiederherstellungs vorgänge entsprech end den Zielen für Wiederherstellungs zeit und Wiederher stellungspunkt erleichtert werden.	s-3 bucket-versioning-enabled	Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) unterstützt die Aufrechterhaltung einer angemesse nen Kapazität und Verfügbarkeit. CRR ermöglicht das automatische, asynchrone Kopieren von Objekten in Amazon-S3-Buckets, um die Datenverf ügbarkeit sicherzus tellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CP-06 (02)	Die Organisation konfiguriert den alternativen Speichers tandort so, dass die Wiederherstellungs vorgänge entsprech end den Zielen für Wiederherstellungs zeit und Wiederher stellungspunkt erleichtert werden.	vpc-vpn-2-tunnels-up	Redundante Site-to-Site VPN-Tunne l können implement iert werden, um die Anforderungen an die Ausfallsicherheit zu erfüllen. Es verwendet zwei Tunnel, um die Konnektivität sicherzustellen, falls eine der Site-to-Site VPN-Verbindungen nicht verfügbar ist. Um sich vor einem Verbindungsverlust zu schützen, können Sie für den Fall, dass Ihr Kunden-Gateway nicht verfügbar ist, eine zweite Site-to-S ite VPN-Verbindung zu Ihrer Amazon Virtual Private Cloud (Amazon VPC) und Ihrem Virtual Private Gateway einrichten, indem Sie ein zweites Kunden-Gateway verwenden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CP-07 (01)	Die Organisation identifiziert einen alternativen Verarbeitungsstandort, der ausreichend vom primären Verarbeitungsstandort getrennt ist, um die Anfälligkeit für dieselben Bedrohungen zu verringern.	rds-multi-az-support	Die Multi-AZ-Unterstützung in Amazon Relational Database Service (Amazon RDS) bietet eine verbesserte Verfügbarkeit und Beständigkeit von Datenbank-Instances. Wenn Sie eine Multi-AZ-Datenbank-Instance bereitstellen, erstellt Amazon RDS automatisch eine primäre Datenbank-Instance und repliziert die Daten synchron auf eine Standby-Instance in einer anderen Availability Zone. Jede Availability Zone läuft auf einer eigenen, physisch getrennten, unabhängigen Infrastruktur und ist auf eine hohe Verfügbarkeit ausgelegt. Im Falle eines Infrastrukturausfalls führt Amazon RDS einen automatis

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			chen Failover zum Standby-Modus durch, sodass Sie den Datenbankbetrieb wieder aufnehmen können, sobald der Failover abgeschlo ssen ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CP-07 (04)	Die Organisation bereitet den alternativen Verarbeitungsstandort so vor, dass der Standort als Betriebsstandort für wichtige Aufgaben und Geschäftsfunktionen dienen kann.	backup-plan-min-frequency-and-min-retention-check	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihr AWS Backup-Plan auf eine Mindestfrequenz und Aufbewahrung festgelegt ist. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen. Mit dieser Regel können Sie die Parameter requiredFrequencyValue (Config default: 1), requiredRetentionDays (Config default: 35) und requiredFrequencyUnit

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			(Config default: days) festlegen. Der tatsächliche Wert muss den Anforderungen Ihrer Organisation entsprechen.
CP-07 (04)	Die Organisation bereitet den alternativen Verarbeitungsstandort so vor, dass der Standort als Betriebsstandort für wichtige Aufgaben und Geschäftsfunktionen dienen kann.	backup-recovery-point-encrypted	Prüft, ob ein Wiederherstellungspunkt verschlüsselt ist. Die Vorbereitung des Standorts umfasst die Festlegung der Konfigurationseinstellungen für die Systeme am alternativen Verarbeitungsstandort, die den Anforderungen für diese Einstellungen am primären Standort entsprechen, und die Sicherstellung, dass die notwendigen Vorräte und logistischen Überlegungen vorhanden sind.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CP-07 (04)	Die Organisat ion bereitet den alternativen Verarbeit ungsstandort so vor, dass der Standort als Betriebsstandort für wichtige Aufgaben und Geschäfts funktionen dienen kann.	backup-recovery-po int-manual-Löschen-deaktiviert	Prüft, ob ein Backup-Tresor über eine zugeordnete ressourcenbasierte Richtlinie verfügt, die das Löschen von Wiederherstellungs punkten verhinder t. Zur Vorbereit ung des Standorts gehören die Festlegun g der Konfigura tionseinstellungen für die Systeme am alternativen Verarbeit ungsstandort, die den Anforderungen für diese Einstellungen am primären Standort entsprechen, und die Sicherstellung, dass die notwendigen Vorräte und logistisc hen Überlegungen eingehalten werden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CP-07 (04)	Die Organisat ion bereitet den alternativen Verarbeit ungsstandort so vor, dass der Standort als Betriebsstandort für wichtige Aufgaben und Geschäfts funktionen dienen kann.	bucket-cross-region-replications3-fähig	Überprüft, ob Sie die regionsübergreifen de S3-Replikation für Ihre Amazon S3 S3-Buckets aktiviert haben. Die Vorbereitung vor Ort umfasst die Einrichtu ng von Konfigura tionseinstellungen für Systeme am alternativen Verarbeit ungsstandort, die den Anforderungen für diese Einstellungen am primären Standort entsprechen, und die Sicherstellung, dass die notwendigen Vorräte und logistisc hen Überlegungen getroffen wurden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CP-09 (03)	Die Organisation speichert Sicherungskopien von [Auftrag: vom Unternehmen definierte kritische Systemsoftware und andere sicherheitsrelevante Informationen] in einer separaten Einrichtung oder in einem brandgeschützten Container, der sich nicht zusammen mit dem Betriebssystem befindet.	backup-recovery-point-minimum-Aufbewahrungsprüfung	Prüft, ob ein Wiederherstellungspunkt frühestens nach Ablauf des angegebenen Zeitraums abläuft. Der separate Speicher für wichtige Informationen gilt für alle wichtigen Informationen, unabhängig vom Typ des Backup-Speichermediums. Zu kritischer Systemsoftware gehören Betriebssysteme, Middleware, Systeme zur Verwaltung kryptografischer Schlüssel und Systeme zur Erkennung von Eindringlingen. Zu den sicherheitsrelevanten Informationen gehören Inventare von Systemhardware-, Software- und Firmware-Komponenten. Alternative Speicherstandorte, einschließlich

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			geografisch verteilte r Architekturen, dienen Organisat ionen als separate Speichereinrichtun gen. Organizations können separaten Speicher bereitstellen, indem sie automatis ierte Backup-Pr ozesse an alternati ven Speichers tandorten (z. B. Rechenzentren) implementieren. Die General Services Administration (GSA) legt Standards und Spezifikationen für Sicherheits- und Brandschutzcontainer fest.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CP-09 (03)	Die Organisation speichert Sicherungskopien von [Auftrag: vom Unternehmen definierte kritische Systemsoftware und andere sicherheitsrelevante Informationen] in einer separaten Einrichtung oder in einem brandgeschützten Container, der sich nicht zusammen mit dem Betriebssystem befindet.	aurora-resources-protected-by-Backup-Plan	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon Aurora Aurora-Ressourcen Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CP-09 (03)	Die Organisation speichert Sicherungskopien von [Auftrag: vom Unternehmen definierte kritische Systemsoftware und andere sicherheitsrelevante Informationen] in einer separaten Einrichtung oder in einem brandgeschützten Container, der sich nicht zusammen mit dem Betriebssystem befindet.	ebs-resources-protected-by-Backup-Plan	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon Elastic Block Store (Amazon EBS) -Ressourcen Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CP-09 (03)	Die Organisation speichert Sicherungskopien von [Auftrag: vom Unternehmen definierte kritische Systemsoftware und andere sicherheitsrelevante Informationen] in einer separaten Einrichtung oder in einem brandgeschützten Container, der sich nicht zusammen mit dem Betriebssystem befindet.	efs-resources-protected-by-Backup-Plan	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon Elastic File System (Amazon EFS) -Dateisysteme Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CP-09 (03)	Die Organisation speichert Sicherungskopien von [Auftrag: vom Unternehmen definierte kritische Systemsoftware und andere sicherheitsrelevante Informationen] in einer separaten Einrichtung oder in einem brandgeschützten Container, der sich nicht zusammen mit dem Betriebssystem befindet.	rds-resources-protected-by-Backup-Plan	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon Relational Database Service (Amazon RDS) -Ressourcen Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CP-09 (03)	Die Organisation speichert Sicherung skopien von [Auftrag: vom Unternehmen definierte kritische Systemsoftware und andere sicherhei tsrelevante Informati onen] in einer separaten Einrichtu ng oder in einem brandgeschützten Container, der sich nicht zusammen mit dem Betriebssystem befindet.	resources-protected-by-backups3-Plan	Um Sie bei Datensich erungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon Simple Storage Service (Amazon S3) -Buckets Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwaltet er Backup-Service mit einer richtlini enbasierten Backup-Lösung. Diese Lösung vereinfac ht Ihr Sicherung smanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforde rungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CP-09 (03)	Die Organisation speichert Sicherungskopien von [Auftrag: vom Unternehmen definierte kritische Systemsoftware und andere sicherheitsrelevante Informationen] in einer separaten Einrichtung oder in einem brandgeschützten Container, der sich nicht zusammen mit dem Betriebssystem befindet.	fsx-resources-protected-by-Backup-Plan	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre FSx Amazon-Dateisysteme Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CP-09 (03)	Die Organisation speichert Sicherungskopien von [Auftrag: vom Unternehmen definierte kritische Systemsoftware und andere sicherheitsrelevante Informationen] in einer separaten Einrichtung oder in einem brandgeschützten Container, der sich nicht zusammen mit dem Betriebssystem befindet.	dynamodb-resources-protected-by-Backup-Plan	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon DynamoDB DynamoDB-Ressourcen Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CP-09 (03)	Die Organisation speichert Sicherung skopien von [Auftrag: vom Unternehmen definierte kritische Systemsoftware und andere sicherhei tsrelevante Informati onen] in einer separaten Einrichtu ng oder in einem brandgeschützten Container, der sich nicht zusammen mit dem Betriebssystem befindet.	ec2--Plan resources-protected-by-backup	Um Sie bei Datensich erungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon Elastic Compute Cloud (Amazon EC2) -Ressourc en Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwaltet er Backup-Service mit einer richtlini enbasierten Backup-Lösung. Diese Lösung vereinfac ht Ihr Sicherung smanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforde rungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CP-09 (03)	Die Organisation speichert Sicherung skopien von [Auftrag: vom Unternehmen definierte kritische Systemsoftware und andere sicherhei tsrelevante Informati onen] in einer separaten Einrichtu ng oder in einem brandgeschützten Container, der sich nicht zusammen mit dem Betriebssystem befindet.	s-3 bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) unterstützt die Aufrechterhaltung einer angemesse nen Kapazität und Verfügbarkeit. CRR ermöglicht das automatische, asynchrone Kopieren von Objekten in Amazon-S3-Buckets, um die Datenverf ügbarkeit sicherzus tellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CP-09 (05)	Die Organisation überträgt die Systemsicherungsinformationen an den alternativen Speicherort [Zuweisung: organisationsdefinierter Zeitraum und Übertragungsrate, die den Zielen für Wiederherstellungszeit und Wiederherstellungspunkt entsprechen].	s-3 bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) unterstützt die Aufrechterhaltung einer angemessenen Kapazität und Verfügbarkeit. CRR ermöglicht das automatische, asynchrone Kopieren von Objekten in Amazon-S3-Buckets, um die Datenverfügbarkeit sicherzustellen.
CP-09 (05)	Die Organisation überträgt die Systemsicherungsinformationen an den alternativen Speicherort [Zuweisung: organisationsdefinierter Zeitraum und Übertragungsrate, die den Zielen für Wiederherstellungszeit und Wiederherstellungspunkt entsprechen].	backup-recovery-point-minimum-Aufbewahrungsprüfung	Prüft, ob ein Wiederherstellungspunkt frühestens nach Ablauf des angegebenen Zeitraums abläuft.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CP-09 (05)	Die Organisation überträgt die Systemsicherungsinformationen an den alternativen Speicherort [Zuweisung: organisationsdefinierter Zeitraum und Übertragungsrate, die den Zielen für Wiederherstellungszeit und Wiederherstellungspunkt entsprechen].	backup-plan-min-frequency-and-min-retention-check	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihr AWS Backup-Plan auf eine Mindestfrequenz und Aufbewahrung festgelegt ist. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen. Mit dieser Regel können Sie die Parameter requiredFrequencyValue (Config default: 1), requiredRetentionDays (Config default: 35) und requiredFrequencyUnit

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			(Config default: days) festlegen. Der tatsächliche Wert muss den Anforderungen Ihrer Organisation entsprechen.
CP-09 (05)	Die Organisation überträgt die Systemsicherungsinformationen an den alternativen Speicherort [Zuweisung: organisationsdefinierter Zeitraum und Übertragungsrate, die den Zielen für Wiederherstellungszeit und Wiederherstellungspunkt entsprechen].	dynamodb-pitr-enabled	Aktivieren Sie diese Regel, um zu überprüfen, ob die Informationen gesichert wurden. Es verwaltet auch die Backups, indem es sicherstellt, dass die point-in-time Wiederherstellung in Amazon DynamoDB aktiviert ist. Bei der Wiederherstellung werden fortlaufende Backups Ihrer Tabelle für die letzten 35 Tage gespeichert.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CP-09 (05)	Die Organisation überträgt die Systemsicherungsinformationen an den alternativen Speicherort [Zuweisung: organisationsdefinierter Zeitraum und Übertragungsrate, die den Zielen für Wiederherstellungszeit und Wiederherstellungspunkt entsprechen].	rds-multi-az-support	Die Multi-AZ-Unterstützung in Amazon Relational Database Service (Amazon RDS) bietet eine verbesserte Verfügbarkeit und Beständigkeit von Datenbank-Instances. Wenn Sie eine Multi-AZ-Datenbank-Instance bereitstellen, erstellt Amazon RDS automatisch eine primäre Datenbank-Instance und repliziert die Daten synchron auf eine Standby-Instance in einer anderen Availability Zone. Jede Availability Zone läuft auf einer eigenen, physisch getrennten, unabhängigen Infrastruktur und ist auf eine hohe Verfügbarkeit ausgelegt. Im Falle eines Infrastrukturausfalls führt Amazon RDS einen automatis

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			chen Failover zum Standby-Modus durch, sodass Sie den Datenbankbetrieb wieder aufnehmen können, sobald der Failover abgeschlo ssen ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CP-09 (08)	Die Organisation setzt kryptografische Mechanismen ein, um die unbefugte Offenlegung von Backup-Informationen zu verhindern.	backup-recovery-point-encrypted	Die Auswahl kryptografischer Mechanismen basiert auf der Notwendigkeit, die Vertraulichkeit und Integrität von Backup-Informationen zu schützen. Die Stärke der ausgewählten Mechanismen entspricht der Sicherheitskategorie oder Klassifizierung der Informationen. Der kryptografische Schutz gilt für System-Backup-Informationen, die sowohl an primären als auch an alternativen Speicherorten gespeichert sind. Organizations, die kryptografische Mechanismen zum Schutz von gespeicherten Informationen implementieren, ziehen auch Lösungen zur Verwaltung kryptografischer Schlüssel in Betracht.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CP-10 (04)	Die Organisation bietet die Möglichkeit, Systemkomponenten innerhalb von [Zuordnung: vom Unternehmen festgelegte Wiederherstellungszeiträume] anhand konfigurationsgesteuerter und integritätsgeschützter Informationen wiederherzustellen, die einen bekannten Betriebszustand der Komponenten darstellen.	backup-recovery-point-encrypted	Aktivieren Sie diese Regel, um zu überprüfen, ob ein Recovery Point verschlüsselt ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CP-10 (04)	Die Organisation bietet die Möglichkeit, Systemkomponenten innerhalb von [Zuordnung: vom Unternehmen festgelegte Wiederherstellungszeiträume] anhand konfigurationsgesteuerter und integritätsgeschützter Informationen wiederherzustellen, die einen bekannten Betriebszustand der Komponenten darstellen.	backup-recovery-point-minimum-Aufbewahrungsprüfung	Aktivieren Sie diese Regel, um zu überprüfen, ob ein Wiederherstellungspunkt nicht früher als nach dem angegebenen Zeitraum abläuft.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CP-10 (04)	Die Organisation bietet die Möglichkeit, Systemkomponenten innerhalb von [Zuordnung: vom Unternehmen festgelegte Wiederherstellungszeiträume] anhand konfigurationsgesteuerter und integritätsgeschützter Informationen wiederherzustellen, die einen bekannten Betriebszustand der Komponenten darstellen.	dynamodb-pitr-enabled	Aktivieren Sie diese Regel, um zu überprüfen, ob die Informationen gesichert wurden. Es verwaltet auch die Backups, indem es sicherstellt, dass die point-in-time Wiederherstellung in Amazon DynamoDB aktiviert ist. Bei der Wiederherstellung werden fortlaufende Backups Ihrer Tabelle für die letzten 35 Tage gespeichert.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CP-10 (04)	Die Organisation bietet die Möglichkeit, Systemkomponenten innerhalb von [Zuordnung: vom Unternehmen festgelegte Wiederherstellungszeiträume] anhand konfigurationsgesteuerter und integritätsgeschützter Informationen wiederherzustellen, die einen bekannten Betriebszustand der Komponenten darstellen.	rds-instance-deletion-protection-aktiviert	Stellen Sie sicher, dass Amazon Relational Database Service (Amazon RDS)-Instances den Löschschutz aktiviert haben. Verwenden Sie den Löschschutz, um zu verhindern, dass Ihre Amazon-RDS-Instances versehentlich oder böswillig gelöscht werden, was zum Verlust der Verfügbarkeit Ihrer Anwendungen führen kann.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CP-10 (04)	Die Organisation bietet die Möglichkeit, Systemkomponenten innerhalb von [Zuordnung: vom Unternehmen festgelegte Wiederherstellungszeiträume] anhand konfigurationsgesteuerter und integritätsgeschützter Informationen wiederherzustellen, die einen bekannten Betriebszustand der Komponenten darstellen.	s-3 bucket-versioning-enabled	Die Versionsverwaltung von Amazon Simple Storage Service (Amazon S3)-Buckets hilft dabei, mehrere Varianten eines Objekts im selben Amazon-S3-Bucket zu speichern. Verwenden Sie die Versionsverwaltung, um sämtliche Versionen aller Objekte in Ihrem Amazon-S3-Bucket zu speichern, abzurufen oder wiederherzustellen. Mit der Versionsverwaltung können Sie Versionen sowohl nach unbeabsichtigten Benutzeraktionen als auch nach Anwendungsfehlern problemlos wiederherstellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
IA-02 (02)	Implementieren Sie eine Multi-Faktor-Authentifizierung für den Zugriff auf nicht privilegierte Konten.	iam-user-mfa-enabled	Aktivieren Sie diese Regel, um den Zugriff auf Ressourcen in der AWS Cloud einzuschränken. Diese Regel sorgt dafür, dass die Multi-Faktor-Authentifizierung (MFA) für alle Benutzer aktiviert ist. MFA sorgt für eine weitere Schutzebene zusätzlich zu den Anmeldeinformationen. Reduzieren Sie Fälle von kompromittierten Konten, indem Sie MFA für Benutzer vorschreiben.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
IA-02 (02)	Implementieren Sie eine Multi-Faktor-Authentifizierung für den Zugriff auf nicht privilegierte Konten.	mfa-enabled-for-iam-Konsolenzugriff	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass MFA für alle AWS Identity and Access Management (IAM) -Benutzer aktiviert ist, die über ein Konsolenkennwort verfügen. MFA sorgt für eine weitere Schutzebene zusätzlich zu den Anmeldeinformationen. Indem Sie MFA für Benutzer vorschreiben, können Sie Fälle kompromittierter Konten reduzieren und verhindern, dass unbefugte Benutzer auf vertrauliche Daten zugreifen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
IA-02 (06)	Das Informati onssystem implement iert eine Multi-Fak tor-Authentifizierung für [Auswahl (eines oder mehrere): lokal; Netzwerk; Remote] Zugriff auf [Auswahl (eines oder mehrere): privilegierte Konten; nicht privilegierte Konten], sodass: (a) Einer der Faktoren durch ein vom System getrenntes Gerät bereitgestellt wird, das Zugriff erhält; und (b) das Gerät erfüllt [Aufgabe: organisationsdefin ierte Anforderungen an die Stärke des Mechanismus].	iam-user-mfa-enabled	Aktivieren Sie diese Regel, um den Zugriff auf Ressourcen in der Cloud einzuschr änken. AWS Diese Regel sorgt dafür, dass die Multi-Fak tor-Authentifizier ung (MFA) für alle Benutzer aktiviert ist. MFA sorgt für eine weitere Schutzebe ne zusätzlich zu den Anmeldeinformation en. Reduzieren Sie Fälle von kompromit tierten Konten, indem Sie MFA für Benutzer vorschreiben.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
IA-02 (06)	Das Informati onssystem implement iert eine Multi-Fak tor-Authentifizierung für [Auswahl (eines oder mehrere): lokal; Netzwerk; Remote] Zugriff auf [Auswahl (eines oder mehrere): privilegierte Konten; nicht privilegierte Konten], sodass: (a) Einer der Faktoren durch ein vom System getrenntes Gerät bereitgestellt wird, das Zugriff erhält; und (b) das Gerät erfüllt [Aufgabe: organisationsdefin ierte Anforderungen an die Stärke des Mechanismus].	mfa-enabled-for-iam-Konsolenzugriff	Verwalten Sie den Zugriff auf Ressource n in der AWS Cloud, indem Sie sicherste llen, dass MFA für alle AWS Identity and Access Managemen t (IAM) -Benutzer aktiviert ist, die über ein Konsolenk ennwort verfügen. MFA sorgt für eine weitere Schutzebe ne zusätzlich zu den Anmeldeinformation en. Indem Sie MFA für Benutzer vorschrei ben, können Sie Fälle kompromittierter Konten reduzieren und verhindern, dass unbefugte Benutzer auf vertrauliche Daten zugreifen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
IA-02 (08)	Das Informati onssystem implement iert replayresistente Authentifizierungs mechanismen für den Zugriff auf [Auswahl (eines oder mehrere): privilegierte Konten; nicht privilegierte Konten].	mfa-enabled-for-iam-Konsolenzugriff	Verwalten Sie den Zugriff auf Ressource n in der AWS Cloud, indem Sie sicherste llen, dass MFA für alle AWS Identity and Access Managemen t (IAM) -Benutzer aktiviert ist, die über ein Konsolenk ennwort verfügen. MFA sorgt für eine weitere Schutzebe ne zusätzlich zu den Anmeldeinformation en. Indem Sie MFA für Benutzer vorschrei ben, können Sie Fälle kompromittierter Konten reduzieren und verhindern, dass unbefugte Benutzer auf vertrauliche Daten zugreifen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
IA-05 (08)	Das Informati onssystem implement iert [Aufgabe: vom Unternehmen festgelegte Sicherhei tskontrollen], um das Risiko von Sicherheitslücken zu minimieren, die sich daraus ergeben, dass Benutzer Konten auf mehreren Systemen haben.	iam-password-policy	Die Identitäten und Anmeldeinformation en werden auf der Grundlage einer organisatorischen IAM-Passwortrichtlinie ausgestellt, verwaltet und verifiziert. Sie erfüllen oder übertreff en die Anforderungen von NIST SP 800-63 und dem Standard „Best Practices“ von AWS Foundational Security in Bezug auf die Passwortstärke. Mit dieser Regel können Sie optional RequireUppercaseCh aracters (Wert für AWS grundlegende Sicherheitsbewährt e Methoden: wahr), RequireLowercaseCh aracters (Wert für bewährte Methoden für AWS grundlege nde Sicherheit: wahr), RequireSy mbols (Wert für bewährte Methoden für AWS grundlege nde Sicherheit:

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			wahr), RequireNumbers (Wert für bewährte Methoden für AWS grundlegende Sicherheit: wahr), MinimumPasswordLength (Wert für bewährte Methoden für AWS grundlegende Sicherheit: 14), PasswordReusePrevention (Wert für bewährte Methoden für AWS grundlegende Sicherheit: 24) und MaxPasswordAge (Wert für bewährte Methoden für AWS grundlegende Sicherheit: 90) für Ihr IAM festlegen. Kennwortrichtlinie. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
IA-05 (08)	Das Informati onssystem implement iert [Aufgabe: vom Unternehmen festgelegte Sicherhei tskontrollen], um das Risiko von Sicherheitslücken zu minimieren, die sich daraus ergeben, dass Benutzer Konten auf mehreren Systemen haben.	iam-user-mfa-enabled	Aktivieren Sie diese Regel, um den Zugriff auf Ressourcen in der AWS Cloud einzuschr änken. Diese Regel stellt sicher, dass die Multi-Faktor-Authe ntifizierung (MFA) für alle IAM-Benut zer aktiviert ist. MFA bietet eine weitere Schutzebene zusätzlic h zum Benutzern amen und Passwort. Reduzieren Sie Fälle von kompromittierten Konten, indem Sie MFA für IAM-Benutzer vorschreiben.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
IA-05 (08)	Das Informati onssystem implement iert [Aufgabe: vom Unternehmen festgelegte Sicherhei tskontrollen], um das Risiko von Sicherheitslücken zu minimieren, die sich daraus ergeben, dass Benutzer Konten auf mehreren Systemen haben.	iam-root-access-key-überprüfen	Der Zugriff auf Systeme und Ressourcen kann gesteuert werden, indem überprüft wird, ob der Root-Benu tzer keine Zugriffss chlüssel mit seiner AWS Identity and Access Management (IAM) -Rolle verknüpft hat. Stellen Sie sicher, dass die Root-Zugr iffsschlüssel gelöscht werden. Erstellen und verwenden Sie stattdessen rollenbas ierte AWS Konten, um dem Prinzip der geringsten Funktiona lität Rechnung zu tragen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
IA-05 (08)	Das Informationssystem implementiert [Aufgabe: vom Unternehmen festgelegte Sicherheitskontrollen], um das Risiko von Sicherheitslücken zu minimieren, die sich daraus ergeben, dass Benutzer Konten auf mehreren Systemen haben.	iam-user-unused-credentials-überprüfen	AWS Identity and Access Management (IAM) kann Ihnen bei Zugriffsberechtigungen und Autorisierungen helfen, indem es nach IAM-Passwörtern und Zugriffsschlüsseln sucht, die für einen bestimmten Zeitraum nicht verwendet wurden. Wenn ungenutzte Anmeldeinformationen identifiziert werden, müssen Sie sie deaktivieren und/oder entfernen, da dies gegen das Prinzip der geringsten Berechtigung verstoßen könnte. Für diese Regel müssen Sie einen Wert für das maxCredentialUsage Alter festlegen (Standardkonfiguration: 90). Der tatsächliche Wert muss den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
IA-05 (08)	Das Informationssystem implementiert [Aufgabe: vom Unternehmen festgelegte Sicherheitskontrollen], um das Risiko von Sicherheitslücken zu minimieren, die sich daraus ergeben, dass Benutzer Konten auf mehreren Systemen haben.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) kann Ihnen dabei helfen, die Prinzipien der geringsten Rechte und der Aufgabentrennung in Zugriffsberechtigungen und Autorisierungen zu integrieren und so zu verhindern, dass Richtlinien „Effect“: „Allow“ mit „Action“: „*“ anstelle von „Resource“: „*“ enthalten. Wenn Benutzern mehr Rechte eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und der Aufgabentrennung verstoßen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
IA-05 (08)	Das Informationssystem implementiert [Aufgabe: vom Unternehmen festgelegte Sicherheitskontrollen], um das Risiko von Sicherheitslücken zu minimieren, die sich daraus ergeben, dass Benutzer Konten auf mehreren Systemen haben.	iam-user-group-membership-überprüfen	AWS Identity and Access Management (IAM) kann Ihnen helfen, Zugriffsberechtigungen und Autorisierungen einzuschränken, indem sichergestellt wird, dass IAM-Benutzer Mitglieder mindestens einer Gruppe sind. Wenn Benutzern mehr Berechtigungen eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und Aufgabentrennung verstoßen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
IR-04 (04)	Das Unternehmen setzt automatisierte Mechanismen ein, um Informationen zu Vorfällen und die Reaktion auf einzelne Vorfälle miteinander zu verknüpfen, um eine unternehmensweite Perspektive in Bezug auf die Sensibilisierung und Reaktion auf Vorfälle zu erhalten.	securityhub-enabled	AWS Security Hub hilft bei der Überwachung von unbefugtem Personal, Verbindungen, Geräten und Software. AWS Security Hub aggregiert, organisiert und priorisiert die Sicherheitswarnungen oder Ergebnisse mehrerer Dienste. AWS Einige dieser Dienste sind Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer und AWS Firewall Manager sowie AWS Partnerlösungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
IR-04 (04)	Das Unternehmen setzt automatisierte Mechanismen ein, um Informationen zu Vorfällen und die Reaktion auf einzelne Vorfälle miteinander zu verknüpfen, um eine unternehmensweite Perspektive in Bezug auf die Sensibilisierung und Reaktion auf Vorfälle zu erhalten.	guardduty-enabled-centralized	Amazon GuardDuty kann mithilfe von Threat Intelligence Feeds helfen, potenzielle Cybersicherheitsereignisse zu überwachen und zu erkennen. Dazu gehören Listen mit bösartigen IPs und maschinellen Lernmethoden zur Identifizierung unerwarteter, nicht autorisierter und bösartiger Aktivitäten in Ihrer AWS Cloud-Umgebung.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
IR-04 (04)	Das Unternehmen setzt automatisierte Mechanismen ein, um Informationen zu Vorfällen und die Reaktion auf einzelne Vorfälle miteinander zu verknüpfen, um eine unternehmensweite Perspektive in Bezug auf die Sensibilisierung und Reaktion auf Vorfälle zu erhalten.	cloudtrail-s3-dataevents-enabled	Die Erfassung von Simple Storage Service (Amazon S3)-Datenereignissen unterstützt die Erkennung von ungewöhnlichen Aktivitäten. Zu den Details gehören AWS Kontoinformationen, über die auf einen Amazon S3 S3-Bucket zugegriffen wurde, die IP-Adresse und die Uhrzeit des Ereignisses.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
IR-04 (04)	Das Unternehmen setzt automatisierte Mechanismen ein, um Informationen zu Vorfällen und die Reaktion auf einzelne Vorfälle miteinander zu verknüpfen, um eine unternehmensweite Perspektive in Bezug auf die Sensibilisierung und Reaktion auf Vorfälle zu erhalten.	cloudwatch-alarm-action-check	Amazon CloudWatch alarmiert, wenn eine Metrik den Schwellenwert für eine bestimmte Anzahl von Bewertungszeiträumen überschreitet. Der Alarm führt eine oder mehrere Aktionen durch, die vom Wert der Metrik oder des Ausdrucks im Vergleich zu einem Schwellenwert in einer Reihe von Zeiträumen abhängt. Diese Regel erfordert einen Wert für alarmActionRequired (Config Default: True), insufficientDataAction Required (Config Default: True), okActionRequired (Config Default: False). Der tatsächliche Wert muss die Alarmaktionen für Ihre Umgebung widerspiegeln.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
IR-04 (04)	Das Unternehmen setzt automatisierte Mechanismen ein, um Informationen zu Vorfällen und die Reaktion auf einzelne Vorfälle miteinander zu verknüpfen, um eine unternehmensweite Perspektive in Bezug auf die Sensibilisierung und Reaktion auf Vorfälle zu erhalten.	cloud-trail-cloud-watch-logs-aktiviert	Verwenden Sie Amazon CloudWatch , um Protokollereignisaktivitäten zentral zu sammeln und zu verwalten. Durch die Aufnahme von AWS CloudTrail Daten erhalten Sie Einzelheiten zu den API-Aufrufaktivitäten innerhalb Ihres AWS Kontos.
RA-05	Überwachung und Suche nach Sicherheitslücken, gehostete Anwendungen und wenn neue Sicherheitslücken identifiziert und gemeldet werden, die sich potenziell auf das System auswirken könnten	guardduty-enabled-centralized	Amazon GuardDuty kann mithilfe von Threat Intelligence Feeds helfen, potenzielle Cybersicherheitsereignisse zu überwachen und zu erkennen. Dazu gehören Listen mit bösartigen IPs und maschinellen Lernmethoden zur Identifizierung unerwarteter, nicht autorisierter und bösartiger Aktivitäten in Ihrer AWS Cloud-Umgebung.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
RA-05	Definieren Sie den Umfang und die Tiefe des Schutzes der Schwachstellen-Scans.	inspector-lambda-standard-scan-aktiviert	Überprüft, ob der Amazon Inspector V2 Lambda-Standardscan für Ihre Umgebung mit einem oder mehreren Konten aktiviert ist, um potenzielle Softwareschwachstellen zu erkennen. Die Regel lautet NON_COMPLIANT, wenn das Lambda-Standardscannen nicht aktiviert ist.
RA-05	Definieren Sie den Umfang und die Tiefe des Schutzes der Schwachstellen-Scans.	inspector-ec2-Scan aktiviert	Überprüft, ob der Amazon Inspector EC2 V2-Scan für Ihre Umgebung mit einem oder mehreren Konten aktiviert ist, um potenzielle Sicherheitslücken und Probleme mit der Netzwerkerreichbarkeit auf Ihren Instances zu erkennen. EC2 Die Regel lautet NON_COMPLIANT, wenn EC2 das Scannen nicht aktiviert ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
RA-05	Definieren Sie den Umfang und die Tiefe des Schutzes der Schwachstellen-Scans.	inspector-ecr-scan-enabled	Überprüft, ob der Amazon Inspector V2 ECR-Scan für Ihre Umgebung mit einem oder mehreren Konten aktiviert ist, um potenzielle Softwareschwachstellen in Ihren Container-Images zu erkennen. Die Regel lautet NON_COMPLIANT, wenn der ECR-Scan nicht aktiviert ist.
RA-05 (03)	Definieren Sie den Umfang und die Tiefe des Schutzes der Schwachstellen-Scans.	inspector-lambda-standard-scan-aktiviert	Überprüft, ob der Amazon Inspector V2 Lambda-Standardscan für Ihre Umgebung mit einem oder mehreren Konten aktiviert ist, um potenzielle Softwareschwachstellen zu erkennen. Die Regel lautet NON_COMPLIANT, wenn das Lambda-Standardscannen nicht aktiviert ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
RA-05 (03)	Definieren Sie den Umfang und die Tiefe des Schutzes der Schwachstellen-Scans.	inspector-ec2-Scan aktiviert	Überprüft, ob der Amazon Inspector EC2 V2-Scan für Ihre Umgebung mit einem oder mehreren Konten aktiviert ist, um potenzielle Sicherheitslücken und Probleme mit der Netzwerkerreichbarkeit auf Ihren Instances zu erkennen. EC2 Die Regel lautet NON_COMPLIANT, wenn EC2 das Scannen nicht aktiviert ist.
RA-05 (03)	Definieren Sie den Umfang und die Tiefe des Schutzes der Schwachstellen-Scans.	inspector-ecr-scan-enabled	Überprüft, ob der Amazon Inspector V2 ECR-Scan für Ihre Umgebung mit einem oder mehreren Konten aktiviert ist, um potenzielle Softwareschwachstellen in Ihren Container-Images zu erkennen. Die Regel lautet NON_COMPLIANT, wenn der ECR-Scan nicht aktiviert ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
RA-05 (05)	Implementieren Sie eine privilegi erte Zugriffsb erechtigung für [Zuweisung: organisat ionsdefinierte Systemkomponenten] zum Scannen der Organisation. (Spezifiziert alle Komponenten, die die Authentifizierung und alle Scans unterstüt zen)	inspector-ec2-Scan aktiviert	Überprüft, ob der Amazon Inspector EC2 V2-Scan für Ihre Umgebung mit einem oder mehreren Konten aktiviert ist, um potenzielle Sicherheitslücken und Probleme mit der Netzwerke rreichbarkeit auf Ihren Instances zu erkennen. EC2 Die Regel lautet NON_COMPL IANT, wenn EC2 das Scannen nicht aktiviert ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SA-10	Die Organisation verlangt vom Entwickler des Systems, der Systemkomponente oder des Systemdienstes: a. Durchführung des Konfigurationsmanagements während des Systems, der Komponente oder des Dienstes [Auswahl (eine oder mehrere): Entwurf; Entwicklung; Implementierung; Betrieb; Entsorgung]; b. Die Dokumentation, Verwaltung und Kontrolle der Integrität von Änderungen an [Zuweisung: von der Organisation definierte Konfigurationselemente im Rahmen der Konfigurationsverwaltung]; c. Die Implementierung von ausschließlich von der Organisation genehmigten Änderungen am System, der	ec2-managerinstance-managed-by-systems	Eine Bestandsaufnahme der Softwareplattformen und Anwendungen innerhalb des Unternehmens ist möglich, indem Amazon Elastic Compute Cloud (Amazon EC2) - Instances mit AWS Systems Manager verwaltet werden. Verwenden Sie AWS Systems Manager, um detaillierte Systemkonfigurationen, Betriebssystem-Patch-Levels, Namen und Typ der Dienste, Softwareinstallationen, Anwendungsname, Herausgeber und Version sowie andere Details zu Ihrer Umgebung bereitzustellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	Komponente oder dem Service; d. Dokumentieren Sie genehmigte Änderungen am System, an der Komponente oder am Dienst sowie die potenziellen Auswirkungen solcher Änderungen auf Sicherheit und Datenschutz; und e. Die Überwachung von Sicherheitslücken und deren Behebung innerhalb des Systems, der Komponente oder des Services und die Meldung der Ergebnisse an [Zuweisung: von der Organisation ernanntes Personal].		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-07 (12)	Die Organisation implementiert [Aufgabe: organisationsdefinierte hostbasierte Grenzschutzmechanismen] unter [Aufgabe: organisationsdefinierte Systemkomponenten].	vpc-sg-open-only-to-authorized-ports	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass gemeinsame Ports für Amazon Elastic Compute Cloud (Amazon EC2) -Sicherheitsgruppen eingeschränkt sind. Wenn der Zugriff auf Ports nicht auf vertrauenswürdige Quellen beschränkt wird, kann dies zu Angriffen auf die Verfügbarkeit, Integrität und Vertraulichkeit von Systemen führen. Durch die Beschränkung des Zugriffs auf Ressourcen innerhalb einer Sicherheitsgruppe aus dem Internet (0.0.0.0/0) kann der Remote-Zugriff auf interne Systeme gesteuert werden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-07 (20)	Bieten Sie die Möglichkeit, [Zuweisung: organisationsdefinierte Systemkomponenten] dynamisch von anderen Systemkomponenten zu isolieren.	wafv2-logging-enabled	Um die Protokollierung und Überwachung in Ihrer Umgebung zu erleichtern, aktivieren Sie die AWS WAF (V2) -Protokollierung im regionalen und globalen Web. ACLs AWS Die WAF-Protokollierung bietet detaillierte Informationen über den Datenverkehr, der von Ihrer Web-ACL analysiert wird. In den Protokollen werden die Uhrzeit aufgezeichnet, zu der die AWS WAF die Anfrage von Ihrer AWS Ressource erhalten hat, Informationen über die Anfrage und eine Aktion für die Regel, der jede Anfrage entsprach.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-07 (21)	Setzen Sie Grenzschutzmechanismen ein, um [Aufgabe: organisationsdefinierte Systemkomponenten] zu isolieren, die [Zuordnung: organisationsdefinierte Aufgaben und/oder Geschäftsfunktionen] unterstützen.	ec2- instances-in-vpc	Stellen Sie Amazon Elastic Compute Cloud (Amazon EC2) -Instances innerhalb einer Amazon Virtual Private Cloud (Amazon VPC) bereit, um eine sichere Kommunikation zwischen einer Instance und anderen Services innerhalb der Amazon VPC zu ermöglichen, ohne dass ein Internet-Gateway, ein NAT-Gerät oder eine VPN-Verbindung erforderlich ist. Der gesamte Datenverkehr bleibt sicher in der AWS Cloud. Domains, die sich innerhalb einer VPC befinden, verfügen aufgrund ihrer logischen Isolierung im Vergleich zu Domains mit öffentlichen Endpunkten über eine zusätzliche Sicherheitsebene. Weisen Sie EC2

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			Amazon-Instances einer Amazon-VPC zu, um den Zugriff ordnungsgemäß zu verwalten.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-07 (21)	Setzen Sie Grenzschutzmechanismen ein, um [Aufgabe: organisationsdefinierte Systemkomponenten] zu isolieren, die [Zuordnung: organisationsdefinierte Aufgaben und/oder Geschäftsfunktionen] unterstützen.	lambda-inside-vpc	Stellen Sie AWS Lambda-Funktionen in einer Amazon Virtual Private Cloud (Amazon VPC) bereit, um eine sichere Kommunikation zwischen einer Funktion und anderen Diensten innerhalb der Amazon VPC zu gewährleisten. Bei dieser Konfiguration sind kein Internet-Gateway, kein NAT-Gerät und keine VPN-Verbindung erforderlich. Der gesamte Datenverkehr bleibt sicher in der Cloud. AWS Domains, die sich innerhalb einer VPC befinden, verfügen aufgrund ihrer logischen Isolierung im Vergleich zu Domains mit öffentlichen Endpunkten über eine zusätzliche Sicherheitsebene. Um den Zugriff ordnungsgemäß zu verwalten,

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			sollten AWS Lambda-Funktionen einer VPC zugewiesen werden.
SC-12 (01)	Einrichtung und Verwaltung kryptografischer Schlüssel bei Verwendung von Kryptografie innerhalb des Systems gemäß den folgenden Schlüsselverwaltungsanforderungen: [Aufgabe: vom Unternehmen definierte Anforderungen für Schlüsselgenerierung, -verteilung, -speicherung, -zugriff und -vernichtung].	cloudtrail-enabled	AWS CloudTrail kann durch die Aufzeichnung von Aktionen und API-Aufrufen der Managementconsole bei der Nichtabstreitbarkeit helfen. AWS Sie können die Benutzer und AWS Konten, die einen AWS Dienst aufgerufen haben, die Quell-IP-Adresse, über die die Anrufe generiert wurden, und die Zeitpunkte der Anrufe identifizieren. Einzelheiten zu den erfassten Daten finden Sie in den AWS CloudTrail Datensatzinhalten.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-28 (01)	Die Organisation implementiert kryptografische Mechanismen, um die unbefugte Offenlegung und Änderung der folgenden Informationen zu verhindern, die sich auf [Zuordnung: organisationsdefinierte Systemkomponenten oder Medien] befinden: [Zuweisung: organisationsdefinierte Informationen].	dynamodb-table-encrypted-kms	Stellen Sie sicher, dass die Verschlüsselung für Ihre Amazon-DynamoDB-Tabellen aktiviert ist. Um eventuell vorhandene sensible Daten im Ruhezustand in diesen Tabellen zu schützen, müssen Sie die Verschlüsselung von Daten im Ruhezustand aktivieren. Standardmäßig werden DynamoDB-Tabellen mit einem AWS eigenen Kundenhauptschlüssel (CMK) verschlüsselt.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-28 (01)	Die Organisation implementiert kryptografische Mechanismen, um die unbefugte Offenlegung und Änderung der folgenden Informationen zu verhindern, die sich auf [Zuordnung: organisationsdefinierte Systemkomponenten oder Medien] befinden: [Zuweisung: organisationsdefinierte Informationen].	ec2- ebs-encryption-by-default	Zum Schutz von Daten im Ruhezustand müssen Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon Elastic Block Store (Amazon EBS)-Volumes aktiviert ist. Da sensible Daten auch im Ruhezustand vorhanden sein können, sollten Sie die Verschlüsselung im Ruhezustand aktivieren, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-28 (01)	Die Organisation implementiert kryptografische Mechanismen, um die unbefugte Offenlegung und Änderung der folgenden Informationen zu verhindern, die sich auf [Zuordnung: organisationsdefinierte Systemkomponenten oder Medien] befinden: [Zuweisung: organisationsdefinierte Informationen].	kinesis-stream-encrypted	Aktivieren Sie die Verschlüsselung für Ihre Amazon-Kinesis-Streams, um eventuell vorhandene sensible Daten sowie Daten im Ruhezustand zu schützen.
SC-28 (01)	Die Organisation implementiert kryptografische Mechanismen, um die unbefugte Offenlegung und Änderung der folgenden Informationen zu verhindern, die sich auf [Zuordnung: organisationsdefinierte Systemkomponenten oder Medien] befinden: [Zuweisung: organisationsdefinierte Informationen].	rds-snapshot-encrypted	Stellen Sie sicher, dass die Verschlüsselung für Ihre Amazon Relational Database Service (Amazon RDS)-Snapshots aktiviert ist. Da sensible Daten auch im Ruhezustand vorhanden sein können, sollten Sie die Verschlüsselung von Daten im Ruhezustand aktivieren, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-28 (01)	Die Organisation implementiert kryptografische Mechanismen, um die unbefugte Offenlegung und Änderung der folgenden Informationen zu verhindern, die sich auf [Zuordnung: organisationsdefinierte Systemkomponenten oder Medien] befinden: [Zuweisung: organisationsdefinierte Informationen].	s-3 default-encryption-kms	Stellen Sie sicher, dass die Verschlüsselung für Ihre Amazon Simple Storage Service (Amazon S3)-Buckets aktiviert ist. Um eventuell vorhandene sensible Daten im Ruhezustand in einem Amazon-S3-Bucket zu schützen, muss die Verschlüsselung aktiviert sein.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-28 (01)	Die Organisation implementiert kryptografische Mechanismen, um die unbefugte Offenlegung und Änderung der folgenden Informationen zu verhindern, die sich auf [Zuordnung: organisationsdefinierte Systemkomponenten oder Medien] befinden: [Zuweisung: organisationsdefinierte Informationen].	sagemaker-notebook-instance-kms-schlüsselkonfiguriert	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass die Verschlüsselung mit dem AWS Key Management Service (AWS KMS) für Ihr Notebook aktiviert ist. SageMaker Da vertrauliche Daten im SageMaker Notebook gespeichert werden können, sollten Sie die Verschlüsselung im Ruhezustand aktivieren, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-28 (01)	Die Organisation implementiert kryptografische Mechanismen, um die unbefugte Offenlegung und Änderung der folgenden Informationen zu verhindern, die sich auf [Zuordnung: organisationsdefinierte Systemkomponenten oder Medien] befinden: [Zuweisung: organisationsdefinierte Informationen].	sns-encrypted-kms	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass Ihre Amazon Simple Notification Service (Amazon SNS) -Themen mit dem AWS Key Management Service (AWS KMS) verschlüsselt werden müssen. Um eventuell vorhandene sensible Daten im Ruhezustand in veröffentlichten Nachrichten zu schützen, muss die Verschlüsselung von Daten im Ruhezustand aktiviert sein.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-28 (01)	Die Organisation implementiert kryptografische Mechanismen, um die unbefugte Offenlegung und Änderung der folgenden Informationen zu verhindern, die sich auf [Zuordnung: organisationsdefinierte Systemkomponenten oder Medien] befinden: [Zuweisung: organisationsdefinierte Informationen].	api-gw-cache-enabled-und-verschlüsselt	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass die Verschlüsselung für den Cache Ihrer API-Gateway-Stufe aktiviert ist. Da für die API-Methode sensible Daten erfasst werden können, sollten Sie die Verschlüsselung von Daten im Ruhezustand aktivieren, um diese Daten zu schützen.
SC-28 (01)	Die Organisation implementiert kryptografische Mechanismen, um die unbefugte Offenlegung und Änderung der folgenden Informationen zu verhindern, die sich auf [Zuordnung: organisationsdefinierte Systemkomponenten oder Medien] befinden: [Zuweisung: organisationsdefinierte Informationen].	cloud-trail-encryption-enabled	Da sensible Daten vorhanden sein können und um Daten im Speicher zu schützen, sollten Sie sicherstellen, dass die Verschlüsselung für Ihre Spuren aktiviert ist. AWS CloudTrail

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-28 (01)	Die Organisation implementiert kryptografische Mechanismen, um die unbefugte Offenlegung und Änderung der folgenden Informationen zu verhindern, die sich auf [Zuordnung: organisationsdefinierte Systemkomponenten oder Medien] befinden: [Zuweisung: organisationsdefinierte Informationen].	efs-encrypted-check	Aktivieren Sie die Verschlüsselung für Ihr Amazon Elastic File System (EFS), um eventuell vorhandene sensible Daten sowie Daten im Ruhezustand zu schützen.
SC-28 (01)	Die Organisation implementiert kryptografische Mechanismen, um die unbefugte Offenlegung und Änderung der folgenden Informationen zu verhindern, die sich auf [Zuordnung: organisationsdefinierte Systemkomponenten oder Medien] befinden: [Zuweisung: organisationsdefinierte Informationen].	elasticsearch-encrypted-at-rest	Da sensible Daten vorhanden sein können und um Daten im Ruhezustand zu schützen, sollten Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon OpenSearch Service (OpenSearch Service) -Domains aktiviert ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-28 (01)	Die Organisation implementiert kryptografische Mechanismen, um die unbefugte Offenlegung und Änderung der folgenden Informationen zu verhindern, die sich auf [Zuordnung: organisationsdefinierte Systemkomponenten oder Medien] befinden: [Zuweisung: organisationsdefinierte Informationen].	encrypted-volumes	Aktivieren Sie die Verschlüsselung für Ihre Amazon-Elastic-Block-Store (Amazon-EBS)-Volumes, um eventuell vorhandene sensible Daten sowie Daten im Ruhezustand zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-28 (01)	Die Organisation implementiert kryptografische Mechanismen, um die unbefugte Offenlegung und Änderung der folgenden Informationen zu verhindern, die sich auf [Zuordnung: organisationsdefinierte Systemkomponenten oder Medien] befinden: [Zuweisung: organisationsdefinierte Informationen].	rds-storage-encrypted	Zum Schutz von Daten im Ruhezustand müssen Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon Relational Database Service (Amazon RDS)-Instances aktiviert ist. Um eventuell vorhandene sensible Daten im Ruhezustand in Amazon-RDS-Instances zu schützen, muss die Verschlüsselung von Daten im Ruhezustand aktiviert sein.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-28 (01)	Die Organisation implementiert kryptografische Mechanismen, um die unbefugte Offenlegung und Änderung der folgenden Informationen zu verhindern, die sich auf [Zuordnung: organisationsdefinierte Systemkomponenten oder Medien] befinden: [Zuweisung: organisationsdefinierte Informationen].	redshift-cluster-configuration-check	Um Daten im Ruhezustand zu schützen, muss die Verschlüsselung für Ihre Amazon-Redshift-Cluster aktiviert sein. Sie müssen auch sicherstellen, dass die erforderlichen Konfigurationen auf Amazon-Redshift-Clustern bereitgestellt werden. Die Prüfungsprotokollierung muss aktiviert sein, um Informationen zu Verbindungen und Benutzeraktivitäten in der Datenbank bereitzustellen. Diese Regel erfordert, dass ein Wert für clusterDbEncrypted (Config Default: TRUE) und LoggingEnabled (Config Default: TRUE) gesetzt ist. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-28 (01)	Die Organisation implementiert kryptografische Mechanismen, um die unbefugte Offenlegung und Änderung der folgenden Informationen zu verhindern, die sich auf [Zuordnung: organisationsdefinierte Systemkomponenten oder Medien] befinden: [Zuweisung: organisationsdefinierte Informationen].	redshift-cluster-kms-enabled	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass die Verschlüsselung mit AWS Key Management Service (AWS KMS) für Ihren Amazon Redshift Redshift-Cluster aktiviert ist. Um eventuell vorhandene sensible Daten im Ruhezustand in Redshift-Clustern zu schützen, muss die Verschlüsselung von Daten im Ruhezustand aktiviert sein.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-28 (01)	Die Organisation implementiert kryptografische Mechanismen, um die unbefugte Offenlegung und Änderung der folgenden Informationen zu verhindern, die sich auf [Zuordnung: organisationsdefinierte Systemkomponenten oder Medien] befinden: [Zuweisung: organisationsdefinierte Informationen].	bucket-server-side-encryptions3-fähig	Zum Schutz von Daten im Ruhezustand müssen Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon Simple Storage Service (Amazon S3)-Buckets aktiviert ist. Um eventuell vorhandene sensible Daten im Ruhezustand in Amazon-S3-Buckets zu schützen, muss die Verschlüsselung aktiviert sein.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-28 (01)	Die Organisation implementiert kryptografische Mechanismen, um die unbefugte Offenlegung und Änderung der folgenden Informationen zu verhindern, die sich auf [Zuordnung: organisationsdefinierte Systemkomponenten oder Medien] befinden: [Zuweisung: organisationsdefinierte Informationen].	sagemaker-endpoint-configuration-kms-schlüsselkonfiguriert	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass die Verschlüsselung mit dem AWS Key Management Service (AWS KMS) für Ihren Endpunkt aktiviert ist. SageMaker Da sensible Daten auf dem SageMaker Endgerät gespeichert werden können, sollten Sie die Verschlüsselung im Ruhezustand aktivieren, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-28 (01)	Die Organisation implementiert kryptografische Mechanismen, um die unbefugte Offenlegung und Änderung der folgenden Informationen zu verhindern, die sich auf [Zuordnung: organisationsdefinierte Systemkomponenten oder Medien] befinden: [Zuweisung: organisationsdefinierte Informationen].	secretsmanager-using-cmk	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass die Verschlüsselung mit dem AWS Key Management Service (AWS KMS) für AWS Secrets Manager aktiviert ist. Aktivieren Sie die Verschlüsselung von Daten im Ruhezustand, um eventuell vorhandene sensible Daten im Ruhezustand im Secrets Manager zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SI-04 (12)	Warnung [Zuordnung: organisationsdefiniertes Personal oder Rollen] mithilfe von [Zuordnung: organisationsdefinierte automatisierte Mechanismen], wenn die folgenden Hinweise auf unangemessene oder ungewöhnliche Aktivitäten mit Auswirkungen auf die Sicherheit oder den Datenschutz auftreten: [Zuordnung: organisationsdefinierte Aktivitäten, die Warnmeldungen auslösen].	lambda-dlq-check	Aktivieren Sie diese Regel, um das entsprechende Personal über Amazon Simple Queue Service (Amazon SQS) oder Amazon Simple Notification Service (Amazon SNS) zu benachrichtigen, wenn eine Funktion ausgefallen ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SI-04 (20)	Implementieren Sie die folgende zusätzliche Überwachung für privilegierte Benutzer: [Zuweisung: vom Unternehmen definierte zusätzliche Überwachung].	s-3 bucket-logging-enabled	Die Amazon Simple Storage Service (Amazon S3)-Serverzugriffsprotokollierung bietet eine Methode zur Überwachung des Netzwerks im Hinblick auf potenzielle Cybersicherheitsereignisse. Die Ereignisse werden überwacht, indem detaillierte Aufzeichnungen über die Anfragen erfasst werden, die an einen Amazon-S3-Bucket gestellt wurden. Jeder Zugriffsprotokolleintrag enthält Details zu einer einzelnen Zugriffsanfrage. Zu den Details gehören Anforderer, Bucket-Name, Anforderungszeit, Anforderungsaktion, Antwortstatus und Fehlercode, falls relevant.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SI-04 (20)	Implementieren Sie die folgende zusätzliche Überwachung für privilegierte Benutzer: [Zuweisung: vom Unternehmen definierte zusätzliche Überwachung].	elasticsearch-logs-to-cloudwatch	Stellen Sie sicher, dass für Amazon OpenSearch Service-Domains Fehlerprotokolle aktiviert und zur Aufbewahrung und Beantwortung an Amazon CloudWatch Logs gestreamt werden. Domain-Fehlerprotokolle sind bei Sicherheits- und Zugriffsprüfungen sowie bei der Diagnose von Verfügbarkeitsproblemen nützlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SI-04 (20)	Implementieren Sie die folgende zusätzliche Überwachung für privilegierte Benutzer: [Zuweisung: vom Unternehmen definierte zusätzliche Überwachung].	multi-region-cloudtrail-enabled	AWS CloudTrail zeichnet Aktionen und API-Aufrufe der AWS Management Console auf. Sie können feststellen, welche Benutzer und Konten angerufen wurden AWS, von welcher Quell-IP-Adresse aus die Anrufe getätigt wurden und wann die Anrufe erfolgten. CloudTrail übermittelt Protokolldateien aus allen AWS Regionen an Ihren S3-Bucket, wenn MULTI_REGION_CLOUD_TRAIL_ENABLED aktiviert ist. Außerdem wird beim AWS Start einer neuen Region derselbe Trail in der neuen Region erstellt. CloudTrail Dadurch erhalten Sie automatisch Protokolldateien mit API-Aktivitäten für die neue Region.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SI-04 (20)	Implementieren Sie die folgende zusätzliche Überwachung für privilegierte Benutzer: [Zuweisung: vom Unternehmen definierte zusätzliche Überwachung].	cloud-trail-cloud-watch-logs-aktiviert	Verwenden Sie Amazon CloudWatch , um Protokollereignisaktivitäten zentral zu sammeln und zu verwalten. Durch die Aufnahme von AWS CloudTrail Daten erhalten Sie Einzelheiten zu den API-Aufrufaktivitäten innerhalb Ihres AWS Kontos.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SI-04 (20)	Implementieren Sie die folgende zusätzliche Überwachung für privilegierte Benutzer: [Zuweisung: vom Unternehmen definierte zusätzliche Überwachung].	cloudtrail-enabled	AWS CloudTrail kann durch die Aufzeichnung von Aktionen und API-Aufrufen in der AWS Management Console bei der Nichtabstreitbarkeit helfen. Sie können die Benutzer und AWS Konten, die einen AWS Dienst aufgerufen haben, die Quell-IP-Adresse, über die die Anrufe generiert wurden, und die Zeitpunkte der Anrufe identifizieren. Einzelheiten zu den erfassten Daten finden Sie in den AWS CloudTrail Datensatzinhalten.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SI-04 (20)	Implementieren Sie die folgende zusätzliche Überwachung für privilegierte Benutzer: [Zuweisung: vom Unternehmen definierte zusätzliche Überwachung].	cloudtrail-s3-dataevents-enabled	Die Erfassung von Simple Storage Service (Amazon S3)-Datenereignissen unterstützt die Erkennung von ungewöhnlichen Aktivitäten. Zu den Details gehören AWS Kontoinformationen, über die auf einen Amazon S3 S3-Bucket zugegriffen wurde, die IP-Adresse und die Uhrzeit des Ereignisses.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SI-04 (20)	Implementieren Sie die folgende zusätzliche Überwachung für privilegierte Benutzer: [Zuweisung: vom Unternehmen definierte zusätzliche Überwachung].	rds-logging-enabled	Um die Protokollierung und Überwachung in Ihrer Umgebung zu erleichtern, stellen Sie sicher, dass die Amazon Relational Database Service (Amazon RDS)-Protokollierung aktiviert ist. Mit der Amazon-RDS-Protokollierung können Sie Ereignisse wie Verbindungen, Verbindungsabbrüche, Abfragen oder abgefragte Tabellen erfassen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SI-04 (20)	Implementieren Sie die folgende zusätzliche Überwachung für privilegierte Benutzer: [Zuweisung: vom Unternehmen definierte zusätzliche Überwachung].	redshift-cluster-configuration-check	Um Daten im Ruhezustand zu schützen, muss die Verschlüsselung für Ihre Amazon-Redshift-Cluster aktiviert sein. Sie müssen auch sicherstellen, dass die erforderlichen Konfigurationen auf Amazon-Redshift-Clustern bereitgestellt werden. Die Prüfungsprotokollierung muss aktiviert sein, um Informationen zu Verbindungen und Benutzeraktivitäten in der Datenbank bereitzustellen. Diese Regel erfordert, dass ein Wert für clusterDbEncrypted (Config Default: TRUE) und LoggingEnabled (Config Default: TRUE) gesetzt ist. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SI-04 (20)	Implementieren Sie die folgende zusätzliche Überwachung für privilegierte Benutzer: [Zuweisung: vom Unternehmen definierte zusätzliche Überwachung].	s-3 bucket-logging-enabled	Die Amazon Simple Storage Service (Amazon S3)-Serverzugriffsprotokollierung bietet eine Methode zur Überwachung des Netzwerks im Hinblick auf potenzielle Cybersicherheitsereignisse. Die Ereignisse werden überwacht, indem detaillierte Aufzeichnungen über die Anfragen erfasst werden, die an einen Amazon-S3-Bucket gestellt wurden. Jeder Zugriffsprotokolleintrag enthält Details zu einer einzelnen Zugriffsanfrage. Zu den Details gehören Anforderer, Bucket-Name, Anforderungszeit, Anforderungsaktion, Antwortstatus und Fehlercode, falls relevant.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SI-04 (22)	(a) Erkennt Netzwerkdienste, die nicht durch [Zuweisung: organisationsdefinierte Autorisierungs- oder Genehmigungsprozesse] autorisiert oder genehmigt wurden; und (b) [Auswahl (einer oder mehrere): Audit; Warnung [Zuordnung: organisationsdefiniertes Personal oder Rollen]], wenn sie erkannt werden.	securityhub-enabled	(A) AWS Security Hub hilft bei der Überwachung von unbefugtem Personal, Verbindungen, Geräten und Software. AWS Security Hub aggregiert, organisiert und priorisiert die Sicherheitswarnungen oder Ergebnisse mehrerer Dienste. AWS Einige dieser Dienste sind Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer und AWS Firewall Manager sowie AWS Partnerlösungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SI-04 (22)	(a) Erkennt Netzwerkdienste, die nicht durch [Zuweisung: organisationsdefinierte Autorisierungs- oder Genehmigungsprozesse] autorisiert oder genehmigt wurden; und (b) [Auswahl (einer oder mehrere): Audit; Warnung [Zuordnung: organisationsdefiniertes Personal oder Rollen]], wenn sie erkannt werden.	vpc-flow-logs-enabled	VPC-Flow-Protokolle erfassen detaillierte Informationsdatensätze über den IP-Datenverkehr, der zu und von Netzwerkschnittstellen in Ihrer Amazon Virtual Private Cloud (Amazon VPC) fließt. Standardmäßig enthalten Flow-Protokolldatensätze Werte für die verschiedenen Komponenten des IP-Flows, einschließlich Quelle, Ziel und Protokoll.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SI-04 (22)	(a) Erkennt Netzwerkdienste, die nicht durch [Zuweisung: organisationsdefinierte Autorisierungs- oder Genehmigungsprozesse] autorisiert oder genehmigt wurden; und (b) [Auswahl (einer oder mehrere): Audit; Warnung [Zuordnung: organisationsdefiniertes Personal oder Rollen]], wenn sie erkannt werden.	guardduty-enabled-centralized	Amazon GuardDuty kann mithilfe von Threat Intelligence Feeds helfen, potenzielle Cybersicherheitsereignisse zu überwachen und zu erkennen. Dazu gehören Listen mit bösartigen IPs und maschinellen Lernmethoden zur Identifizierung unerwarteter, nicht autorisierter und bösartiger Aktivitäten in Ihrer AWS Cloud-Umgebung.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SI-05 (01)	Verbreiten Sie Sicherheitswarnungen und Warnhinweise im gesamten Unternehmen mithilfe von [Aufgabe: organisationsdefinierte automatisierte Mechanismen].	securityhub-enabled	AWS Security Hub hilft bei der Überwachung von unbefugtem Personal, Verbindungen, Geräten und Software. AWS Security Hub aggregiert, organisiert und priorisiert die Sicherheitswarnungen oder Ergebnisse mehrerer Dienste. AWS Einige dieser Dienste sind Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer und AWS Firewall Manager sowie AWS Partnerlösungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SI-05 (01)	Verbreiten Sie Sicherheitswarnungen und Warnhinweise im gesamten Unternehmen mithilfe von [Aufgabe: organisationsdefinierte automatisierte Mechanismen].	guardduty-enabled-centralized	Amazon GuardDuty kann mithilfe von Threat Intelligence Feeds helfen, potenzielle Cybersicherheitsereignisse zu überwachen und zu erkennen. Dazu gehören Listen mit bösartigen IPs und maschinellen Lernmethoden zur Identifizierung unerwarteter, nicht autorisierter und bösartiger Aktivitäten in Ihrer AWS Cloud-Umgebung.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SI-07 (02)	Setzen Sie automatisierte Tools ein, die [Zuordnung: vom Unternehmen festgelegte Mitarbeiter oder Rollen] benachrichtigen, wenn bei der Integritätsprüfung Unstimmigkeiten festgestellt werden.	cloudwatch-alarm-action-check	Amazon CloudWatch alarmiert, wenn eine Metrik den Schwellenwert für eine bestimmte Anzahl von Bewertungszeiträumen überschreitet. Der Alarm führt eine oder mehrere Aktionen durch, die vom Wert der Metrik oder des Ausdrucks im Vergleich zu einem Schwellenwert in einer Reihe von Zeiträumen abhängt. Diese Regel erfordert einen Wert für alarmActionRequired (Config Default: True), insufficientDataAction Required (Config Default: True), okActionRequired (Config Default: False). Der tatsächliche Wert muss die Alarmaktionen für Ihre Umgebung widerspiegeln.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SI-07 (02)	Setzen Sie automatisierte Tools ein, die [Zuordnung: vom Unternehmen festgelegte Mitarbeiter oder Rollen] benachrichtigen, wenn bei der Integritätsprüfung Unstimmigkeiten festgestellt werden.	cloudtrail-s3-dataevents-enabled	Die Erfassung von Simple Storage Service (Amazon S3)-Datenereignissen unterstützt die Erkennung von ungewöhnlichen Aktivitäten. Zu den Details gehören AWS Kontoinformationen, über die auf einen Amazon S3 S3-Bucket zugegriffen wurde, die IP-Adresse und die Uhrzeit des Ereignisses.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SI-07 (05)	Automatisch [Auswahl (eine oder mehrere): System herunterfahren; System neu starten; [Zuweisung: organisationsdefinierte Kontrollen]] implementieren, wenn Integritätsverletzungen entdeckt werden.	ec2-manager instance-managed-by-systems	Eine Bestandsaufnahme der Softwareplattformen und Anwendungen innerhalb des Unternehmens ist möglich, indem Amazon Elastic Compute Cloud (Amazon EC2) - Instances mit AWS Systems Manager verwaltet werden. Verwenden Sie AWS Systems Manager, um detaillierte Systemkonfigurationen, Betriebssystem-Patch-Levels, Namen und Typ der Dienste, Softwareinstallationen, Anwendungsname, Herausgeber und Version sowie andere Details zu Ihrer Umgebung bereitzustellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SI-07 (05)	Automatisch [Auswahl (eine oder mehrere): System herunterfahren; System neu starten; [Zuweisung: organisationsdefinierte Kontrollen]] implementieren, wenn Integritätsverletzungen entdeckt werden.	ec2-prüfen managedinstance-patch-compliance-status	Aktivieren Sie diese Regel, um bei der Identifizierung und Dokumentation von Sicherheitslücken in Amazon Elastic Compute Cloud (Amazon EC2) zu helfen. Die Regel prüft, ob die EC2 Amazon-Instance die Patch-Konformität im AWS Systems Manager gemäß den Richtlinien und Verfahren Ihrer Organisation einhält.
SI-07 (15)	Implementieren Sie kryptografische Mechanismen, um die folgenden Software- oder Firmware-Komponenten vor der Installation zu authentifizieren: [Aufgabe: organisationsdefinierte Software- oder Firmware-Komponenten].	api-gw-ssl-enabled	Stellen Sie sicher, dass die REST-API-Stufen von Amazon API Gateway mit SSL-Zertifikaten konfiguriert sind, damit Backend-Systeme überprüfen können, ob Anforderungen von API Gateway stammen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SI-07 (15)	Implementieren Sie kryptografische Mechanismen, um die folgenden Software- oder Firmware-Komponenten vor der Installation zu authentifizieren: [Aufgabe: organisationsdefinierte Software- oder Firmware-Komponenten].	acm-certificate-expiration-check	Stellen Sie sicher, dass die Netzwerkintegrität geschützt ist, indem Sie sicherstellen, dass X509-Zertifikate von ACM ausgestellt werden. AWS Diese Zertifikate müssen gültig und dürfen nicht abgelaufen sein. Für diese Regel ist ein Wert für erforderlich daysToExpiration (Wert für bewährte AWS Grundregeln für Sicherheit: 90). Der tatsächliche Wert muss den Richtlinien Ihrer Organisation entsprechen.

Vorlage

Die Vorlage ist verfügbar unter GitHub: Operational Best Practices for FedRAMP (High Part 2).

Betriebliche bewährte Methoden für FFIEC

Konformitätspakete bieten ein allgemeines Compliance-Framework, das es Ihnen ermöglicht, mithilfe verwalteter oder benutzerdefinierter AWS Config Regeln und Abhilfemaßnahmen Kontrollen zur Sicherheits-, Betriebs- oder Kostenoptimierung durchzuführen. AWS Config Conformance Packs dienen als Beispielvorlagen nicht dazu, die vollständige Einhaltung eines bestimmten Governance- oder Compliance-Standards sicherzustellen. Sie sind dafür verantwortlich, selbst zu beurteilen, ob Ihre Nutzung der Services den geltenden gesetzlichen und behördlichen Anforderungen entspricht.

Im Folgenden finden Sie ein Beispiel für eine Zuordnung zwischen den Domänen des Cyber Security Assessment Tool des Federal Financial Institutions Examination Council (FFIEC) und den AWS verwalteten Konfigurationsregeln. Jede Config-Regel gilt für eine bestimmte AWS Ressource und bezieht sich auf eine oder mehrere Steuerelemente des FFIEC Cyber Security Assessment Tool. Eine Kontrolle des FFIEC Cyber Security Assessment Tool kann mit mehreren Config-Regeln verknüpft werden. In der folgenden Tabelle finden Sie weitere Informationen und Anleitungen zu diesen Zuordnungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
D1.G.IT.B.1	Es wird ein Inventar der Unternehm ensressourcen (z. B. Hardware, Software, Daten und Systeme, die extern gehostet werden) geführt.	ec2-manager instance-managed-by-systems	Eine Bestandsa ufnahme der Softwareplattforme n und Anwendung en innerhalb des Unternehmens ist möglich, indem Amazon Elastic Compute Cloud (Amazon EC2) - Instances mit AWS Systems Manager verwaltet werden. Verwenden Sie AWS Systems Manager, um detaillierte Systemkonfiguratio nen, Betriebssystem-Patch-Levels, Namen und Typ der Dienste, Softwareinstallati onen, Anwendung sname, Herausgeb er und Version sowie andere Details zu

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			Ihrer Umgebung bereitzustellen.
D1.G.IT.B.1	Es wird ein Inventar der Unternehm ensressourcen (z. B. Hardware, Software, Daten und extern gehostete Systeme) geführt.	ec2-stopped-instance	Aktivieren Sie diese Regel, um bei der Basiskonfiguration von Amazon Elastic Compute Cloud (Amazon EC2) - Instances zu helfen, indem Sie überprüfe n, ob EC2 Amazon-Instances gemäß den Standards Ihrer Organisation für mehr als die zulässige Anzahl von Tagen gestoppt wurden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
D1.G.IT.B.1	Es wird ein Inventar der Unternehm ensressourcen (z. B. Hardware, Software, Daten und Systeme, die extern gehostet werden) geführt.	ec2- volume-inuse-check	Diese Regel stellt sicher, dass Amazon Elastic Block Store-Volumes, die an Amazon Elastic Compute Cloud (Amazon EC2) - Instances angehängt sind, zum Löschen markiert werden, wenn eine Instance beendet wird. Wenn ein Amazon-EB S-Volume nicht gelöscht wird, wenn die Instance, an die es angehängt ist, beendet wird, kann dies gegen das Konzept der geringsten Funktiona lität verstoßen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
D1.G.IT.B.1	Es wird ein Inventar der Unternehm ensressourcen (z. B. Hardware, Software, Daten und Systeme, die extern gehostet werden) geführt.	eip-attached	Diese Regel stellt sicher, dass Elastic, die einer Amazon Virtual Private Cloud (Amazon VPC) IPs zugewiesen sind, an Amazon Elastic Compute Cloud (Amazon EC2) - Instances oder verwendete Elastic Network Interface s angehängt sind. Diese Regel hilft bei der Überwachu ng ungenutzter Inhalte EIPs in Ihrer Umgebung.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
D1.RM.Rm.B.1	Innerhalb der Einrichtung gibt es mindestens eine Risikomanagementfunktion im Bereich Informationssicherheit und Geschäftskontinuität.	autoscaling-group-elb-healthcheck-erforderlich	Die Elastic Load Balancer (ELB) - Zustandsprüfungen für Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling Scaling-Gruppen unterstützen die Aufrechterhaltung einer angemessenen Kapazität und Verfügbarkeit. Der Load Balancer sendet regelmäßig Pings, versucht Verbindungen herzustellen oder sendet Anfragen, um den Zustand der EC2 Amazon-Instances in einer Gruppe mit auto-scaling zu testen. Wenn eine Instance nicht zurückmeldet, wird der Traffic an eine neue EC2 Amazon-Instance gesendet.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
D1.RM.Rm.B.1	Innerhalb der Einrichtung gibt es mindestens eine Risikomanagementfunktion im Bereich Informationssicherheit und Geschäftskontinuität.	s-3 bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) unterstützt die Aufrechterhaltung einer angemessenen Kapazität und Verfügbarkeit. CRR ermöglicht das automatische, asynchrone Kopieren von Objekten in Amazon-S3-Buckets, um die Datenverfügbarkeit sicherzustellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
D1.RM.Rm.B.1	Innerhalb der Einrichtung gibt es mindestens eine Risikomanagementfunktion im Bereich Informationssicherheit und Geschäftskontinuität.	rds-in-backup-plan	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon Relational Database Service (Amazon RDS) -Instances Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
D1.RM.Rm.B.1	Innerhalb der Einrichtung gibt es mindestens eine Risikomanagementfunktion im Bereich Informationssicherheit und Geschäftskontinuität.	efs-in-backup-plan	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon Elastic File System (Amazon EFS) -Dateisysteme Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
D1.RM.Rm.B.1	Innerhalb der Einrichtung gibt es mindestens eine Risikomanagementfunktion im Bereich Informationssicherheit und Geschäftskontinuität.	ebs-in-backup-plan	Stellen Sie zur Unterstützung der Datensicherungsprozesse sicher, dass Ihre Amazon Elastic Block Store (Amazon EBS) -Volumes Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
D1.RM.Rm.B.1	Innerhalb der Einrichtung gibt es mindestens eine Risikomanagementfunktion im Bereich Informationssicherheit und Geschäftskontinuität.	dynamodb-in-backup-plan	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon DynamoDB-Tabellen Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
D1.RM.Rm.B.1	Innerhalb der Einrichtung gibt es mindestens eine Risikomanagementfunktion im Bereich Informationssicherheit und Geschäftskontinuität.	elasticache-redis-cluster-automatic-Backup-Check	Wenn automatische Backups aktiviert sind, ElastiCache erstellt Amazon täglich ein Backup des Clusters. Die Sicherung kann für eine von Ihrer Organisation festgelegte Anzahl von Tagen aufbewahrt werden. Automatische Backups schützen vor Datenverlust. Bei einem Ausfall können Sie einen neuen Cluster erstellen, der Ihre Daten aus dem aktuellen Backup wiederherstellt.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
D1.RM.Rm.B.1	Innerhalb der Einrichtung gibt es mindestens eine Risikomanagementfunktion im Bereich Informationssicherheit und Geschäftskontinuität.	rds-multi-az-support	Die Multi-AZ-Unterstützung in Amazon Relational Database Service (Amazon RDS) bietet eine verbesserte Verfügbarkeit und Beständigkeit von Datenbank-Instances. Wenn Sie eine Multi-AZ-Datenbank-Instance bereitstellen, erstellt Amazon RDS automatisch eine primäre Datenbank-Instance und repliziert die Daten synchron auf eine Standby-Instance in einer anderen Availability Zone. Jede Availability Zone läuft auf einer eigenen, physisch getrennten, unabhängigen Infrastruktur und ist auf eine hohe Verfügbarkeit ausgelegt. Im Falle eines Infrastrukturausfalls führt Amazon RDS einen automatis

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			chen Failover zum Standby-Modus durch, sodass Sie den Datenbankbetrieb wieder aufnehmen können, sobald der Failover abgeschlo ssen ist.
D1.RM.Rm.B.1	Innerhalb der Einrichtung gibt es mindestens eine Risikomanagementfu nktion im Bereich Informationssicher heit und Geschäfts kontinuität.	db-instance-backup-enabled	Die Sicherung sfunktion von Amazon RDS erstellt Sicherung en Ihrer Datenbank en und Transakti onsprotokolle. Amazon RDS erstellt einen Snapshot für das Speichervolume Ihrer DB-Instance, sodass die gesamte DB-Instance gesichert wird. Sie können im System spezifische Aufbewahrungsfrist en festlegen, um Ihre Ausfallsicherheits anforderungen zu erfüllen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
D1.RM.Rm.B.1	Innerhalb der Einrichtung gibt es mindestens eine Risikomanagementfunktion im Bereich Informationssicherheit und Geschäftskontinuität.	aurora-resources-protected-by-Backup-Plan	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon Aurora Aurora-Ressourcen Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
D1.RM.Rm.B.1	Innerhalb der Einrichtung gibt es mindestens eine Risikomanagementfunktion im Bereich Informationssicherheit und Geschäftskontinuität.	backup-plan-min-frequency-and-min-retention-check	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihr AWS Backup-Plan auf eine Mindestfrequenz und Aufbewahrung festgelegt ist. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen. Mit dieser Regel können Sie die Parameter requiredFrequencyValue (Config default: 1), requiredRetentionDays (Config default: 35) und requiredFrequencyUnit

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			(Config default: days) festlegen. Der tatsächliche Wert muss den Anforderungen Ihrer Organisation entsprechen.
D1.RM.Rm.B.1	Innerhalb der Einrichtung gibt es mindestens eine Risikomanagementfunktion im Bereich Informationssicherheit und Geschäftskontinuität.	backup-recovery-point-manual-löschen-deaktiviert	Stellen Sie sicher, dass Ihren AWS Backup-Wiederherstellungspunkten eine ressourcenbasierte Richtlinie zugeordnet ist, die das Löschen von Wiederherstellungspunkten verhindert. Die Verwendung einer ressourcenbasierten Richtlinie zur Verhinderung des Löschens von Wiederherstellungspunkten kann dazu beitragen, ein versehentliches oder absichtliches Löschen zu unterbinden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
D1.RM.Rm.B.1	Innerhalb der Einrichtung gibt es mindestens eine Risikomanagementfunktion im Bereich Informationssicherheit und Geschäftskontinuität.	backup-recovery-point-minimum-Aufbewahrungsprüfung	Um bei Datensicherungsprozessen zu helfen, stellen Sie sicher, dass für Ihre AWS Backup-Wiederherstellungspunkte eine Mindestaufbewahrungsdauer festgelegt ist. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen. Mit dieser Regel können Sie den Parameter requiredRetentionDays (Config Default: 35) festlegen. Der tatsächliche Wert muss den Anforderu

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			ngen Ihrer Organisation entsprechen.
D1.RM.Rm.B.1	Innerhalb der Einrichtung gibt es mindestens eine Risikomanagementfunktion im Bereich Informationssicherheit und Geschäftskontinuität.	ec2--Plan resources-protected-by-backup	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon Elastic Compute Cloud (Amazon EC2) -Ressourcen Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
D1.RM.Rm.B.1	Innerhalb der Einrichtung gibt es mindestens eine Risikomanagementfunktion im Bereich Informationssicherheit und Geschäftskontinuität.	redshift-backup-enabled	Stellen Sie zur Unterstützung der Datensicherungsprozesse sicher, dass Ihre Amazon-Redshift-Cluster über automatisierte Snapshots verfügen. Wenn automatisierte Snapshots für einen Cluster aktiviert sind, erstellt Redshift in regelmäßigen Abständen Snapshots dieses Clusters. Standardmäßig erstellt Redshift alle acht Stunden oder alle 5 GB einen Snapshot für jeden Knoten mit Datenänderungen oder je nachdem, was zuerst eintritt.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
D1.RM.RA.B.2	Die Risikobewertung identifiziert internetb asierte Systeme und Transaktionen mit hohem Risiko, die zusätzliche Authentif izierungskontrollen erfordern.	guardduty-enabled-centralized	Amazon GuardDuty kann mithilfe von Threat Intellige nce Feeds helfen, potenzielle Cybersich erheitsereignisse zu überwachen und zu erkennen. Dazu gehören Listen mit bösartigen IPs und maschinel len Lernmethoden zur Identifizierung unerwarteter, nicht autorisierter und bösartiger Aktivitäten in Ihrer AWS Cloud-Umgebung.
D1.RM.RA.B.2	Die Risikobewertung identifiziert internetb asierte Systeme und Transaktionen mit hohem Risiko, die zusätzliche Authentif izierungskontrollen erfordern.	annual-risk-assess ment-performed (Prozessüberprüfung)	Führen Sie eine jährliche Risikobew ertung für Ihre Organisation durch. Risikowertungen können dabei helfen, die Wahrscheinlichkeit und Auswirkun gen identifizierter Risiken und/oder Schwachstellen für eine Organisation zu ermitteln.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
D1.TC.Tr.B.2	Die jährlichen Schulungen zur Informationssicherheit umfassen die Reaktion auf Vorfälle, aktuelle Cyberbedrohungen (z. B. Phishing, Spear-Phishing, Social Engineering und mobile Sicherheit) sowie neu auftretende Probleme.	security-awareness-program-exists (Prozessüberprüfung)	Etablieren und pflegen Sie ein Programm zur Förderung des Sicherheitsbewusstseins in Ihrer Organisation. Programme zur Förderung des Sicherheitsbewusstseins der Mitarbeiter vermitteln ihnen, wie sie ihre Organisation vor diversen Sicherheitsverletzungen oder Sicherheitsvorfällen schützen können.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
D2.IS.Is.B.1	Bedrohungen der Informationssicherheit werden erfasst und den zuständigen internen Mitarbeitern mitgeteilt.	guardduty-enabled-centralized	Amazon GuardDuty kann mithilfe von Threat Intelligence Feeds helfen, potenzielle Cybersicherheitsereignisse zu überwachen und zu erkennen. Dazu gehören Listen mit bösartigen IPs und maschinellen Lernmethoden zur Identifizierung unerwarteter, nicht autorisierter und bösartiger Aktivitäten in Ihrer AWS Cloud-Umgebung.
D2.IS.Is.B.1	Bedrohungen der Informationssicherheit werden erfasst und den zuständigen internen Mitarbeitern mitgeteilt.	cloud-trail-cloud-watch-Logs aktiviert	Verwenden Sie Amazon CloudWatch , um Protokollereignisaktivitäten zentral zu sammeln und zu verwalten. Die Aufnahme von AWS CloudTrail Daten liefert Einzelheiten zu den API-Aufrufaktivitäten in Ihrem AWS-Konto.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
D2.IS.Is.B.1	Bedrohungen der Informationssicherheit werden erfasst und den zuständigen internen Mitarbeitern mitgeteilt.	securityhub-enabled	AWS Security Hub hilft bei der Überwachung von unbefugtem Personal, Verbindungen, Geräten und Software. AWS Security Hub aggregiert, organisiert und priorisiert die Sicherheitswarnungen oder Ergebnisse mehrerer Dienste. AWS Einige dieser Dienste sind Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer und AWS Firewall Manager sowie AWS Partnerlösungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
D2.MA.Ma.B.1	Protokolle zu Prüfungen und anderen Sicherheitsereignissen werden überprüft und sicher aufbewahrt.	api-gw-execution-logging-aktiviert	Die API-Gateway-Protokollierung zeigt detaillierte Ansichten der Benutzer, die auf die API zugegriffen haben, und wie diese Benutzer auf die API zugegriffen haben. Diese Einblicke ermöglichen die Transparenz von Benutzeraktivitäten.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
D2.MA.Ma.B.1	Protokolle zu Prüfungen und anderen Sicherheitsereignissen werden überprüft und sicher aufbewahrt.	cloudtrail-enabled	AWS CloudTrail kann durch die Aufzeichnung von Aktionen und API-Aufrufen in der AWS Management Console bei der Nichtabstreitbarkeit helfen. Sie können die Benutzer und die Benutzer AWS-Konten , die einen AWS Dienst aufgerufen haben, die Quell-IP-Adresse, über die die Aufrufe generiert wurden, und den Zeitpunkt der Anrufe identifizieren. Einzelheiten zu den erfassten Daten finden Sie in den AWS CloudTrail Datensatzinhalten.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
D2.MA.Ma.B.1	Protokolle zu Prüfungen und anderen Sicherheitsereignissen werden überprüft und sicher aufbewahrt.	elb-logging-enabled	Die Elastic-Load-Balancing-Aktivität ist ein zentraler Kommunikationspunkt innerhalb einer Umgebung. Stellen Sie sicher, dass die ELB-Protokollierung aktiviert ist. Die gesammelten Daten enthalten detaillierte Informationen zu Anfragen, die an den ELB gesendet wurden. Jedes Protokoll enthält Informationen wie die Zeit, zu der die Anforderung einging, die Client-IP-Adresse, Latenzen, Anforderungspfade und Serverantworten.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
D2.MA.Ma.B.1	Protokolle zu Prüfungen und anderen Sicherheitsereignissen werden überprüft und sicher aufbewahrt.	multi-region-cloudtrail-enabled	AWS CloudTrail zeichnet Aktionen und API-Aufrufe der AWS Management Console auf. Sie können feststellen, welche Benutzer und Konten angerufen wurden AWS, von welcher Quell-IP-Adresse aus die Anrufe getätigt wurden und wann die Anrufe erfolgten. CloudTrail übermittelt Protokolldateien aus allen AWS Regionen an Ihren S3-Bucket , wenn MULTI_REGION_CLOUD_TRAIL_ENABLED aktiviert ist. Außerdem wird beim AWS Start einer neuen Region derselbe Trail in der neuen Region erstellt. CloudTrail Dadurch erhalten Sie automatisch Protokolldateien mit API-Aktivitäten für die neue Region.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
D2.MA.Ma.B.1	Protokolle zu Prüfungen und anderen Sicherheitsereignissen werden überprüft und sicher aufbewahrt.	s-3 bucket-logging-enabled	Die Amazon Simple Storage Service (Amazon S3)-Serverzugriffsprotokollierung bietet eine Methode zur Überwachung des Netzwerks im Hinblick auf potenzielle Cybersicherheitsereignisse. Die Ereignisse werden überwacht, indem detaillierte Aufzeichnungen über die Anfragen erfasst werden, die an einen Amazon-S3-Bucket gestellt wurden. Jeder Zugriffsprotokolleintrag enthält Details zu einer einzelnen Zugriffsanfrage. Zu den Details gehören Anforderer, Bucket-Name, Anforderungszeit, Anforderungsaktion, Antwortstatus und Fehlercode, falls relevant.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
D2.MA.Ma.B.1	Protokolle zu Prüfungen und anderen Sicherheitsereignissen werden überprüft und sicher aufbewahrt.	vpc-flow-logs-enabled	VPC-Flow-Protokolle erfassen detaillierte Informationsdatensätze über den IP-Datenverkehr, der zu und von Netzwerkschnittstellen in Ihrer Amazon Virtual Private Cloud (Amazon VPC) fließt. Standardmäßig enthalten Flow-Protokolldatensätze Werte für die verschiedenen Komponenten des IP-Flows, einschließlich Quelle, Ziel und Protokoll.
D2.MA.Ma.B.1	Protokolle zu Prüfungen und anderen Sicherheitsereignissen werden überprüft und sicher aufbewahrt.	s-3 bucket-default-lock-enabled	Stellen Sie sicher, dass für Ihren Amazon Simple Storage Service (Amazon S3)-Bucket standardmäßig eine Sperre aktiviert ist. Zum Schutz eventuell vorhandener sensibler Daten in S3-Buckets müssen Sie Objektsperren für Daten im Ruhezustand erzwingen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
D2.MA.Ma.B.1	Protokolle zu Prüfungen und anderen Sicherheitsereignissen werden überprüft und sicher aufbewahrt.	cloudtrail-s3-dataevents-enabled	Die Erfassung von Simple Storage Service (Amazon S3)-Datenereignissen unterstützt die Erkennung von ungewöhnlichen Aktivitäten. Zu den Details gehören AWS-Konto Informationen über den Zugriff auf einen Amazon S3 S3-Bucket, die IP-Adresse und die Uhrzeit des Ereignisses.
D2.MA.Ma.B.1	Protokolle zu Prüfungen und anderen Sicherheitsereignissen werden überprüft und sicher aufbewahrt.	cw-loggroup-retention-period-überprüfen	Stellen Sie sicher, dass die Ereignisprotokolldaten für Ihre Protokollgruppen über eine Mindestdauer aufbewahrt werden, um die Fehlerbehebung und forensische Untersuchungen zu unterstützen. Fehlende frühere Ereignisprotokolldaten erschweren die Rekonstruierung und Identifizierung potenziell schädlicher Ereignisse.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
D2.MA.Ma.B.1	Protokolle zu Prüfungen und anderen Sicherheitsereignissen werden überprüft und sicher aufbewahrt.	rds-logging-enabled	Um die Protokollierung und Überwachung in Ihrer Umgebung zu erleichtern, stellen Sie sicher, dass die Amazon Relational Database Service (Amazon RDS)-Protokollierung aktiviert ist. Mit der Amazon-RDS-Protokollierung können Sie Ereignisse wie Verbindungen, Verbindungsabbrüche, Abfragen oder abgefragte Tabellen erfassen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
D2.MA.Ma.B.1	Protokolle zu Prüfungen und anderen Sicherheitsereignissen werden überprüft und sicher aufbewahrt.	wafv2-logging-enabled	Um Ihnen bei der Protokollierung und Überwachung in Ihrer Umgebung zu helfen, aktivieren Sie die AWS WAF (V2) -Protokollierung im regionalen und globalen Web. ACLs AWS Die WAF-Protokollierung bietet detaillierte Informationen über den Datenverkehr, der von Ihrer Web-ACL analysiert wird. In den Protokollen werden die Uhrzeit aufgezeichnet, zu der die AWS WAF die Anfrage von Ihrer AWS Ressource erhalten hat, Informationen über die Anfrage und eine Aktion für die Regel, der jede Anfrage entsprach.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
D2.MA.Ma.B.1	Protokolle zu Prüfungen und anderen Sicherheitsereignissen werden überprüft und sicher aufbewahrt.	redshift-cluster-configuration-check	Um Daten im Ruhezustand zu schützen, muss die Verschlüsselung für Ihre Amazon-Redshift-Cluster aktiviert sein. Sie müssen auch sicherstellen, dass die erforderlichen Konfigurationen auf Amazon-Redshift-Clustern bereitgestellt werden. Die Prüfungsprotokollierung muss aktiviert sein, um Informationen zu Verbindungen und Benutzeraktivitäten in der Datenbank bereitzustellen. Diese Regel erfordert, dass ein Wert für clusterDbEncrypted (Config Default: TRUE) und LoggingEnabled (Config Default: TRUE) gesetzt ist. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
D2.MA.Ma.B.1	Protokolle zu Prüfungen und anderen Sicherheitsereignissen werden überprüft und sicher aufbewahrt.	cloud-trail-cloud-watch-logs-aktiviert	Verwenden Sie Amazon CloudWatch , um Protokollereignisaktivitäten zentral zu sammeln und zu verwalten. Die Aufnahme von AWS CloudTrail Daten liefert Einzelheiten zu den API-Aufrufaktivitäten in Ihrem AWS-Konto.
D2.MA.Ma.B.1	Protokolle zu Prüfungen und anderen Sicherheitsereignissen werden überprüft und sicher aufbewahrt.	elasticsearch-logs-to-cloudwatch	Stellen Sie sicher, dass für Amazon OpenSearch Service-Domains Fehlerprotokolle aktiviert und zur Aufbewahrung und Beantwortung an Amazon CloudWatch Logs gestreamt werden. Domain-Fehlerprotokolle sind bei Sicherheits- und Zugriffsprüfungen sowie bei der Diagnose von Verfügbarkeitsproblemen nützlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
D2.MA.Ma.B.2	Computerereignisprotokolle werden für Untersuchungen verwendet, nachdem ein Ereignis eingetreten ist.	api-gw-execution-logging-aktiviert	Die API-Gateway-Protokollierung zeigt detaillierte Ansichten der Benutzer, die auf die API zugegriffen haben, und wie diese Benutzer auf die API zugegriffen haben. Diese Einblicke ermöglichen die Transparenz von Benutzeraktivitäten.
D2.MA.Ma.B.2	Computerereignisprotokolle werden für Untersuchungen verwendet, nachdem ein Ereignis eingetreten ist.	cloud-trail-cloud-watch-Logs aktiviert	Verwenden Sie Amazon CloudWatch , um Protokoll ereignisaktivitäten zentral zu sammeln und zu verwalten. Die Aufnahme von AWS CloudTrail Daten liefert Einzelheiten zu den API-Aufrufaktivitäten in Ihrem AWS-Konto.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
D2.MA.Ma.B.2	Computerereignisprotokolle werden für Untersuchungen verwendet, nachdem ein Ereignis eingetreten ist.	cloudtrail-enabled	AWS CloudTrail kann durch die Aufzeichnung von Aktionen und API-Aufrufen in der AWS Management Console helfen, die Ablehnung zu verhindern. Sie können die Benutzer und die Benutzer AWS-Konten , die einen AWS Dienst aufgerufen haben, die Quell-IP-Adresse, über die die Aufrufe generiert wurden, und den Zeitpunkt der Anrufe identifizieren. Einzelheiten zu den erfassten Daten finden Sie in den AWS CloudTrail Datensatzinhalten.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
D2.MA.Ma.B.2	Computerereignisprotokolle werden für Untersuchungen verwendet, nachdem ein Ereignis eingetreten ist.	elb-logging-enabled	Die Elastic-Load-Balancing-Aktivität ist ein zentraler Kommunikationspunkt innerhalb einer Umgebung. Stellen Sie sicher, dass die ELB-Protokollierung aktiviert ist. Die gesammelten Daten enthalten detaillierte Informationen zu Anfragen, die an den ELB gesendet wurden. Jedes Protokoll enthält Informationen wie die Zeit, zu der die Anforderung einging, die Client-IP-Adresse, Latenzen, Anforderungspfade und Serverantworten.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
D2.MA.Ma.B.2	Computerereignisprotokolle werden für Untersuchungen verwendet, nachdem ein Ereignis eingetreten ist.	multi-region-cloudtrail-enabled	AWS CloudTrail zeichnet Aktionen und API-Aufrufe der AWS Management Console auf. Sie können feststellen, welche Benutzer und Konten angerufen wurden AWS, von welcher Quell-IP-Adresse aus die Anrufe getätigt wurden und wann die Anrufe erfolgten. CloudTrail übermittelt Protokolldateien aus allen AWS Regionen an Ihren S3-Bucket , wenn MULTI_REGION_CLOUD_TRAIL_ENABLED aktiviert ist. Außerdem wird beim AWS Start einer neuen Region derselbe Trail in der neuen Region erstellt. CloudTrail Dadurch erhalten Sie automatisch Protokolldateien mit API-Aktivitäten für die neue Region.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
D2.MA.Ma.B.2	Computerereignisprotokolle werden für Untersuchungen verwendet, nachdem ein Ereignis eingetreten ist.	s-3 bucket-logging-enabled	Die Amazon Simple Storage Service (Amazon S3)-Serverzugriffsprotokollierung bietet eine Methode zur Überwachung des Netzwerks im Hinblick auf potenzielle Cybersicherheitsereignisse. Die Ereignisse werden überwacht, indem detaillierte Aufzeichnungen über die Anfragen erfasst werden, die an einen Amazon-S3-Bucket gestellt wurden. Jeder Zugriffsprotokolleintrag enthält Details zu einer einzelnen Zugriffsanfrage. Zu den Details gehören Anforderer, Bucket-Name, Anforderungszeit, Anforderungsaktion, Antwortstatus und Fehlercode, falls relevant.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
D2.MA.Ma.B.2	Computerereignisprotokolle werden für Untersuchungen verwendet, nachdem ein Ereignis eingetreten ist.	vpc-flow-logs-enabled	VPC-Flow-Protokolle erfassen detaillierte Informationsdatensätze über den IP-Datenverkehr, der zu und von Netzwerkschnittstellen in Ihrer Amazon Virtual Private Cloud (Amazon VPC) fließt. Standardmäßig enthalten Flow-Protokolldatensätze Werte für die verschiedenen Komponenten des IP-Flows, einschließlich Quelle, Ziel und Protokoll.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
D2.MA.Ma.B.2	Computerereignisprotokolle werden für Untersuchungen verwendet, nachdem ein Ereignis eingetreten ist.	cloudtrail-s3-dataevents-enabled	Die Erfassung von Simple Storage Service (Amazon S3)-Datenereignissen unterstützt die Erkennung von ungewöhnlichen Aktivitäten. Zu den Details gehören AWS-Konto Informationen über den Zugriff auf einen Amazon S3 S3-Bucket, die IP-Adresse und die Uhrzeit des Ereignisses.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
D2.MA.Ma.B.2	Computerereignisprotokolle werden für Untersuchungen verwendet, nachdem ein Ereignis eingetreten ist.	redshift-cluster-configuration-check	Um Daten im Ruhezustand zu schützen, muss die Verschlüsselung für Ihre Amazon-Redshift-Cluster aktiviert sein. Sie müssen auch sicherstellen, dass die erforderlichen Konfigurationen auf Amazon-Redshift-Clustern bereitgestellt werden. Die Prüfungsprotokollierung muss aktiviert sein, um Informationen zu Verbindungen und Benutzeraktivitäten in der Datenbank bereitzustellen. Diese Regel erfordert, dass ein Wert für clusterDbEncrypted (Config Default: TRUE) und LoggingEnabled (Config Default: TRUE) gesetzt ist. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
D2.MA.Ma.B.2	Computerereignisprotokolle werden für Untersuchungen verwendet, nachdem ein Ereignis eingetreten ist.	elasticsearch-logs-to-cloudwatch	Stellen Sie sicher, dass für Amazon OpenSearch Service-Domains Fehlerprotokolle aktiviert und zur Aufbewahrung und Beantwortung an Amazon CloudWatch Logs gestreamt werden. Domain-Fehlerprotokolle sind bei Sicherheits- und Zugriffsprüfungen sowie bei der Diagnose von Verfügbarkeitsproblemen nützlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
D2.TI.Ti.B.1	Die Institution gehört einer oder mehreren Quellen zum Informati onsaustausch über Bedrohungen und Sicherheitslücken an, die Informationen über Bedrohungen bereitstellen (z. B. FS-ISAC, US-CERT).	securityhub-enabled	AWS Security Hub hilft bei der Überwachung von unbefugtem Personal, Verbindun gen, Geräten und Software. AWS Security Hub aggregiert, organisie rt und priorisie rt die Sicherhei tswarnungen oder Ergebnisse mehrerer Dienste. AWS Einige dieser Dienste sind Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer und AWS Firewall Manager sowie AWS Partnerlösungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
D2.TI.Ti.B.1	Die Institution gehört einer oder mehreren Quellen zum Informati onsaustausch über Bedrohungen und Sicherheitslücken an, die Informationen über Bedrohungen bereitstellen (z. B. FS-ISAC, US-CERT).	guardduty-enabled-centralized	Amazon GuardDuty kann mithilfe von Threat Intellige nce Feeds helfen, potenzielle Cybersich erheitsereignisse zu überwachen und zu erkennen. Dazu gehören Listen mit bösartigen IPs und maschinel len Lernmethoden zur Identifizierung unerwarteter, nicht autorisierter und bösartiger Aktivitäten in Ihrer AWS Cloud-Umgebung.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
D2.TI.Ti.B.2	Bedrohungsinformationen werden zur Überwachung von Bedrohungen und Schwachstellen verwendet.	ec2-check managedinstance-patch-compliance-status	Aktivieren Sie diese Regel, um bei der Identifizierung und Dokumentation von Sicherheitslücken in Amazon Elastic Compute Cloud (Amazon EC2) zu helfen. Die Regel prüft, ob die EC2 Amazon-Instance die Patch-Konformität im AWS Systems Manager gemäß den Richtlinien und Verfahren Ihrer Organisation einhält.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
D2.TI.Ti.B.2	Bedrohungsinformationen werden zur Überwachung von Bedrohungen und Schwachstellen verwendet.	guardduty-enabled-centralized	Amazon GuardDuty kann mithilfe von Threat Intelligence Feeds helfen, potenzielle Cybersicherheitsereignisse zu überwachen und zu erkennen. Dazu gehören Listen mit bösartigen IPs und maschinellen Lernmethoden zur Identifizierung unerwarteter, nicht autorisierter und bösartiger Aktivitäten in Ihrer AWS Cloud-Umgebung.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
D2.TI.Ti.B.2	Bedrohungsinformationen werden zur Überwachung von Bedrohungen und Schwachstellen verwendet.	securityhub-enabled	AWS Security Hub hilft bei der Überwachung von unbefugtem Personal, Verbindungen, Geräten und Software. AWS Security Hub aggregiert, organisiert und priorisiert die Sicherheitswarnungen oder Ergebnisse mehrerer Dienste. AWS Einige dieser Dienste sind Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer und AWS Firewall Manager sowie AWS Partnerlösungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
D2.TI.Ti.B.3	Bedrohungsinformationen werden zur Verbesserung des internen Risikomanagements und interner Kontrollen verwendet.	securityhub-enabled	AWS Security Hub hilft bei der Überwachung von unbefugtem Personal, Verbindungen, Geräten und Software. AWS Security Hub aggregiert, organisiert und priorisiert die Sicherheitswarnungen oder Ergebnisse mehrerer Dienste. AWS Einige dieser Dienste sind Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer und AWS Firewall Manager sowie AWS Partnerlösungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
D2.TI.Ti.B.3	Bedrohungsinformationen werden zur Verbesserung des internen Risikomanagements und interner Kontrollen verwendet.	guardduty-enabled-centralized	Amazon GuardDuty kann mithilfe von Threat Intelligence Feeds helfen, potenzielle Cybersicherheitsereignisse zu überwachen und zu erkennen. Dazu gehören Listen mit bösartigen IPs und maschinellen Lernmethoden zur Identifizierung unerwarteter, nicht autorisierter und bösartiger Aktivitäten in Ihrer AWS Cloud-Umgebung.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
D3.CC.PM.B.1	Ein Patch-Management-Programm wird implementiert, damit Software- und Firmware-Patches rechtzeitig installiert werden.	ec2-check managedinstance-patch-compliance-status	Aktivieren Sie diese Regel, um bei der Identifizierung und Dokumentation von Sicherheitslücken in Amazon Elastic Compute Cloud (Amazon EC2) zu helfen. Die Regel prüft, ob die EC2 Amazon-Instance die Patch-Konformität im AWS Systems Manager gemäß den Richtlinien und Verfahren Ihrer Organisation einhält.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
D3.CC.PM.B.1	Ein Patch-Management-Programm wird implementiert, damit Software- und Firmware-Patches rechtzeitig installiert werden.	elastic-beanstalk-managed-updates-aktiviert	Durch die Aktivierung verwalteter Plattformupdates für eine Amazon-Elastic-Beanstalk-Umgebung wird sichergestellt, dass die aktuellen verfügbaren Plattform-Fixes, -Updates und -Features für die Umgebung installiert sind. Eine bewährte Methode zur Sicherung von Systemen besteht darin, stets die aktuellen Patches zu installieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
D3.CC.PM.B.1	Ein Patch-Management-Programm wird implementiert, damit Software- und Firmware-Patches rechtzeitig installiert werden.	rds-automatic-minor-version-upgrade-fähig	Aktivieren Sie automatische Unterversions-Upgrades auf Ihren Amazon-Relational-Database-Service (RDS)-Instances, um sicherzustellen, dass die aktuellen Updates für Unterversionen des Relational Database Management System (RDBMS) installiert sind, die Sicherheitspatches und Bugfixes enthalten können.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
D3.CC.PM.B.1	Ein Patch-Management-Programm wird implementiert, damit Software- und Firmware-Patches rechtzeitig installiert werden.	redshift-cluster-maintenancesettings-check	Diese Regel stellt sicher, dass Amazon-Redshift-Cluster die bevorzugten Einstellungen für Ihre Organisation haben. Insbesondere sorgt sie dafür, dass Cluster bevorzugte Wartungsfenster und automatisierte Aufbewahrungsfristen für Snapshots für die Datenbank haben. Für diese Regel müssen Sie die festlegen. allowVersionUpgrade Der Standardwert ist „true“. Außerdem können Sie optional den Zeitraum preferredMaintenanceWindow (der Standardwert ist sa: 16:00 -sa: 16:30) und den automated SnapshotRetention Zeitraum (der Standardwert ist 1) festlegen. Die tatsächlichen Werte müssen den Richtlini

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			en Ihrer Organisation entsprechen.
D3.CC.PM.B.3	Die Patch-Management-Berichte werden geprüft und geben Auskunft über fehlende Sicherheitspatches.	ec2- -check managedinstance-patch-compliance-status	Aktivieren Sie diese Regel, um bei der Identifizierung und Dokumentation von Sicherheitslücken in Amazon Elastic Compute Cloud (Amazon EC2) zu helfen. Die Regel prüft, ob die EC2 Amazon-Instance die Patch-Konformität im AWS Systems Manager gemäß den Richtlinien und Verfahren Ihrer Organisation einhält.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
D3.CC.PM.B.3	Die Patch-Management-Berichte werden geprüft und geben Auskunft über fehlende Sicherheitspatches.	elastic-beanstalk-managed-updates-aktiviert	Durch die Aktivierung verwalteter Plattformupdates für eine Amazon-Elastic-Beanstalk-Umgebung wird sichergestellt, dass die aktuellen verfügbaren Plattform-Fixes, -Updates und -Features für die Umgebung installiert sind. Eine bewährte Methode zur Sicherung von Systemen besteht darin, stets die aktuellen Patches zu installieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
D3.CC.PM.B.3	Die Patch-Management-Berichte werden geprüft und geben Auskunft über fehlende Sicherheitspatches.	rds-automatic-minor-version-upgrade-fähig	Aktivieren Sie automatische Unterversions-Upgrades auf Ihren Amazon-Relational-Database-Service (RDS)-Instances, um sicherzustellen, dass die aktuellen Updates für Unterversionen des Relational Database Management System (RDBMS) installiert sind, die Sicherheitspatches und Bugfixes enthalten können.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
D3.CC.PM.B.3	Die Patch-Management-Berichte werden geprüft und geben Auskunft über fehlende Sicherheitspatches.	redshift-cluster-maintenancesettings-check	Diese Regel stellt sicher, dass Amazon-Redshift-Cluster die bevorzugten Einstellungen für Ihre Organisation haben. Insbesondere sorgt sie dafür, dass Cluster bevorzugte Wartungsfenster und automatisierte Aufbewahrungsfristen für Snapshots für die Datenbank haben. Für diese Regel müssen Sie die festlegen. allowVersionUpgrade Der Standardwert ist „true“. Außerdem können Sie optional den Zeitraum preferredMaintenanceWindow (der Standardwert ist sa: 16:00 -sa: 16:30) und den automated SnapshotRetention Zeitraum (der Standardwert ist 1) festlegen. Die tatsächlichen Werte müssen den Richtlini

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			en Ihrer Organisation entsprechen.
D3.DC.An.B.1	Die Einrichtung ist in der Lage, ungewöhnliche Aktivitäten durch Überwachung der gesamten Umgebung zu erkennen.	guardduty-non-archived-findings	Amazon GuardDuty hilft Ihnen dabei, die Auswirkungen eines Vorfalls zu verstehen, indem es die Ergebnisse nach Schweregrad klassifiziert: niedrig, mittel und hoch. Diese Klassifizierungen können Sie zur Festlegung von entsprechenden Strategien und Prioritäten zur Behebung solcher Vorfälle verwenden. Mit dieser Regel können Sie optional daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7) und daysHighSev (Config Default: 1) für nicht archivierte Ergebnisse festlegen, wie es die Richtlinien Ihrer Organisation erfordern.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
D3.DC.An.B.1	Die Einrichtung ist in der Lage, ungewöhnliche Aktivitäten durch Überwachung der gesamten Umgebung zu erkennen.	securityhub-enabled	AWS Security Hub hilft bei der Überwachung von unbefugtem Personal, Verbindungen, Geräten und Software. AWS Security Hub aggregiert, organisiert und priorisiert die Sicherheitswarnungen oder Ergebnisse mehrerer Dienste. AWS Einige dieser Dienste sind Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer und AWS Firewall Manager sowie AWS Partnerlösungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
D3.DC.An.B.1	Die Einrichtung ist in der Lage, ungewöhnliche Aktivitäten durch Überwachung der gesamten Umgebung zu erkennen.	guardduty-enabled-centralized	Amazon GuardDuty kann mithilfe von Threat Intelligence Feeds helfen, potenzielle Cybersicherheitsereignisse zu überwachen und zu erkennen. Dazu gehören Listen mit bösartigen IPs und maschinellen Lernmethoden zur Identifizierung unerwarteter, nicht autorisierter und bösartiger Aktivitäten in Ihrer AWS Cloud-Umgebung.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
D3.DC.An.B.2	Kundentransaktionen, die Warnmeldungen zu ungewöhnlichen Aktivitäten auslösen, werden überwacht und geprüft.	guardduty-enabled-centralized	Amazon GuardDuty kann mithilfe von Threat Intellige nce Feeds helfen, potenzielle Cybersich erheitsereignisse zu überwachen und zu erkennen. Dazu gehören Listen mit bösartigen IPs und maschinel len Lernmethoden zur Identifizierung unerwarteter, nicht autorisierter und bösartiger Aktivitäten in Ihrer AWS Cloud-Umgebung.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
D3.DC.An.B.2	Kundentransaktionen, die Warnmeldungen zu ungewöhnlichen Aktivitäten auslösen, werden überwacht und geprüft.	securityhub-enabled	AWS Security Hub hilft bei der Überwachung von unbefugtem Personal, Verbindungen, Geräten und Software. AWS Security Hub aggregiert, organisiert und priorisiert die Sicherheitswarnungen oder Ergebnisse mehrerer Dienste. AWS Einige dieser Dienste sind Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer und AWS Firewall Manager sowie AWS Partnerlösungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
D3.DC.An.B.3	Protokolle des physischen und/oder logischen Zugriffs werden nach Ereignissen überprüft.	cloudtrail-enabled	AWS CloudTrail kann durch die Aufzeichnung von Aktionen und API-Aufrufen in der AWS Management Console bei der Nichtabstreitbarkeit helfen. Sie können die Benutzer und die Benutzer AWS-Konten , die einen AWS Dienst aufgerufen haben, die Quell-IP-Adresse, über die die Aufrufe generiert wurden, und den Zeitpunkt der Anrufe identifizieren. Einzelheiten zu den erfassten Daten finden Sie in den AWS CloudTrail Datensatzinhalten.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
D3.DC.An.B.3	Protokolle des physischen und/oder logischen Zugriffs werden nach Ereignissen überprüft.	multi-region-cloudtrail-enabled	AWS CloudTrail zeichnet Aktionen und API-Aufrufe der AWS Management Console auf. Sie können feststellen, welche Benutzer und Konten angerufen wurden AWS, von welcher Quell-IP-Adresse aus die Anrufe getätigt wurden und wann die Anrufe erfolgten. CloudTrail übermittelt Protokolldateien aus allen AWS Regionen an Ihren S3-Bucket , wenn MULTI_REGION_CLOUD_TRAIL_ENABLED aktiviert ist. Außerdem wird beim AWS Start einer neuen Region derselbe Trail in der neuen Region erstellt. CloudTrail Dadurch erhalten Sie automatisch Protokolldateien mit API-Aktivitäten für die neue Region.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
D3.DC.An.B.3	Protokolle des physischen und/oder logischen Zugriffs werden nach Ereignissen überprüft.	s-3 bucket-logging-enabled	Die Amazon Simple Storage Service (Amazon S3)-Serverzugriffs protokollierung bietet eine Methode zur Überwachung des Netzwerks im Hinblick auf potenzielle Cybersicherheitsereignisse. Die Ereignisse werden überwacht, indem detaillierte Aufzeichnungen über die Anfragen erfasst werden, die an einen Amazon-S3-Bucket gestellt wurden. Jeder Zugriffsprotokolleintrag enthält Details zu einer einzelnen Zugriffsanfrage. Zu den Details gehören Anforderer, Bucket-Name, Anforderungszeit, Anforderungsaktion, Antwortstatus und Fehlercode, falls relevant.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
D3.DC.An.B.3	Protokolle des physischen und/oder logischen Zugriffs werden nach Ereignissen überprüft.	rds-logging-enabled	Um die Protokollierung und Überwachung in Ihrer Umgebung zu erleichtern, stellen Sie sicher, dass die Amazon Relational Database Service (Amazon RDS)-Protokollierung aktiviert ist. Mit der Amazon-RDS-Protokollierung können Sie Ereignisse wie Verbindungen, Verbindungsabbrüche, Abfragen oder abgefragte Tabellen erfassen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
D3.DC.An.B.3	Protokolle des physischen und/oder logischen Zugriffs werden nach Ereignissen überprüft.	wafv2-logging-enabled	Um die Protokollierung und Überwachung in Ihrer Umgebung zu erleichtern, aktivieren Sie die AWS WAF (V2) -Protokollierung im regionalen und globalen Web ACLs. AWS Die WAF-Protokollierung bietet detaillierte Informationen über den Datenverkehr, der von Ihrer Web-ACL analysiert wird. In den Protokollen werden die Uhrzeit aufgezeichnet, zu der die AWS WAF die Anfrage von Ihrer AWS Ressource erhalten hat, Informationen über die Anfrage und eine Aktion für die Regel, der jede Anfrage entsprach.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
D3.DC.An.B.3	Protokolle des physischen und/oder logischen Zugriffs werden nach Ereignissen überprüft.	cloud-trail-cloud-watch-logs-aktiviert	Verwenden Sie Amazon CloudWatch , um Protokoll ereignisaktivitäten zentral zu sammeln und zu verwalten. Die Aufnahme von AWS CloudTrail Daten liefert Einzelheiten zu den API-Aufrufaktivitäten in Ihrem AWS-Konto.
D3.DC.An.B.3	Protokolle des physischen und/oder logischen Zugriffs werden nach Ereignissen überprüft.	api-gw-execution-logging-aktiviert	Die API-Gateway-Protokollierung zeigt detaillierte Ansichten der Benutzer, die auf die API zugegriffen haben, und wie diese Benutzer auf die API zugegriffen haben. Diese Einblicke ermöglichen die Transparenz von Benutzeraktivitäten.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
D3.DC.An.B.3	Protokolle des physischen und/oder logischen Zugriffs werden nach Ereignissen überprüft.	elb-logging-enabled	Die Elastic-Load-Balancing-Aktivität ist ein zentraler Kommunikationspunkt innerhalb einer Umgebung. Stellen Sie sicher, dass die ELB-Protokollierung aktiviert ist. Die gesammelten Daten enthalten detaillierte Informationen zu Anfragen, die an den ELB gesendet wurden. Jedes Protokoll enthält Informationen wie die Zeit, zu der die Anforderung einging, die Client-IP-Adresse, Latenzen, Anforderungspfade und Serverantworten.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
D3.DC.An.B.3	Protokolle des physischen und/oder logischen Zugriffs werden nach Ereignissen überprüft.	vpc-flow-logs-enabled	VPC-Flow-Protokolle erfassen detaillierte Informationsdatensätze über den IP-Datenverkehr, der zu und von Netzwerkschnittstellen in Ihrer Amazon Virtual Private Cloud (Amazon VPC) fließt. Standardmäßig enthalten Flow-Protokolldatensätze Werte für die verschiedenen Komponenten des IP-Flows, einschließlich Quelle, Ziel und Protokoll.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
D3.DC.An.B.3	Protokolle des physischen und/oder logischen Zugriffs werden nach Ereignissen überprüft.	cloudtrail-s3-data events-enabled	Die Erfassung von Simple Storage Service (Amazon S3)-Datenereignissen unterstützt die Erkennung von ungewöhnlichen Aktivitäten. Zu den Details gehören AWS-Konto Informationen über den Zugriff auf einen Amazon S3 S3-Bucket, die IP-Adresse und die Uhrzeit des Ereignisses.
D3.DC.An.B.3	Protokolle des physischen und/oder logischen Zugriffs werden nach Ereignissen überprüft.	elasticsearch-logs-to-cloudwatch	Stellen Sie sicher, dass für Amazon OpenSearch Service-Domains Fehlerprotokolle aktiviert und zur Aufbewahrung und Beantwortung an Amazon CloudWatch Logs gestreamt werden. Domain-Fehlerprotokolle sind bei Sicherheits- und Zugriffsprüfungen sowie bei der Diagnose von Verfügbarkeitsproblemen nützlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
D3.DC.An.B.4	Der Zugriff Dritter auf kritische Systeme wird auf unbefugte oder ungewöhnliche Aktivitäten überwacht.	redshift-cluster-configuration-check	Um Daten im Ruhezustand zu schützen, muss die Verschlüsselung für Ihre Amazon-Redshift-Cluster aktiviert sein. Sie müssen auch sicherstellen, dass die erforderlichen Konfigurationen auf Amazon-Redshift-Clustern bereitgestellt werden. Die Prüfungsprotokollierung muss aktiviert sein, um Informationen zu Verbindungen und Benutzeraktivitäten in der Datenbank bereitzustellen. Diese Regel erfordert, dass ein Wert für clusterDbEncrypted (Config Default: TRUE) und LoggingEnabled (Config Default: TRUE) gesetzt ist. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
D3.DC.An.B.4	Der Zugriff Dritter auf kritische Systeme wird auf unbefugte oder ungewöhnliche Aktivitäten überwacht.	rds-logging-enabled	Um die Protokoll ierung und Überwachung in Ihrer Umgebung zu erleichtern, stellen Sie sicher, dass die Amazon Relationa l Database Service (Amazon RDS)-Prot okollierung aktiviert ist. Mit der Amazon-RDS-Protokollierung können Sie Ereigniss e wie Verbindungen, Verbindungsabbrüch e, Abfragen oder abgefragte Tabellen erfassen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
D3.DC.An.B.4	Der Zugriff Dritter auf kritische Systeme wird auf unbefugte oder ungewöhnliche Aktivitäten überwacht.	wafv2-logging-enabled	Um die Protokollierung und Überwachung in Ihrer Umgebung zu erleichtern, aktivieren Sie die AWS WAF (V2) -Protokollierung im regionalen und globalen Web. ACLs AWS Die WAF-Protokollierung bietet detaillierte Informationen über den Datenverkehr, der von Ihrer Web-ACL analysiert wird. In den Protokollen werden die Uhrzeit aufgezeichnet, zu der die AWS WAF die Anfrage von Ihrer AWS Ressource erhalten hat, Informationen über die Anfrage und eine Aktion für die Regel, der jede Anfrage entsprach.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
D3.DC.An.B.4	Der Zugriff Dritter auf kritische Systeme wird auf unbefugte oder ungewöhnliche Aktivitäten überwacht.	s3- bucket-logging-enabled	Die Amazon Simple Storage Service (Amazon S3)-Serverzugriffs protokollierung bietet eine Methode zur Überwachu ng des Netzwerks im Hinblick auf potenzielle Cybersich erheitsereignisse. Die Ereignisse werden überwacht, indem detaillierte Aufzeichn ungen über die Anfragen erfasst werden, die an einen Amazon-S3-Bucket gestellt wurden. Jeder Zugriffsprotokolle intrag enthält Details zu einer einzelnen Zugriffsanfrage. Zu den Details gehören Anforderer, Bucket-Name, Anforderu ngszeit, Anforderu ngsaktion, Antwortst atus und Fehlercode, falls relevant.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
D3.DC.An.B.4	Der Zugriff Dritter auf kritische Systeme wird auf unbefugte oder ungewöhnliche Aktivitäten überwacht.	api-gw-execution-logging-aktiviert	Die API-Gateway-Protokollierung zeigt detaillierte Ansichten der Benutzer, die auf die API zugegriff en haben, und wie diese Benutzer auf die API zugegriff en haben. Diese Einblicke ermöglichen die Transparenz von Benutzeraktivitäten.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
D3.DC.An.B.4	Der Zugriff Dritter auf kritische Systeme wird auf unbefugte oder ungewöhnliche Aktivitäten überwacht.	elb-logging-enabled	Die Elastic-Load-Balancing-Aktivität ist ein zentraler Kommunikationspunkt innerhalb einer Umgebung. Stellen Sie sicher, dass die ELB-Protokollierung aktiviert ist. Die gesammelten Daten enthalten detaillierte Informationen zu Anfragen, die an den ELB gesendet wurden. Jedes Protokoll enthält Informationen wie die Zeit, zu der die Anforderung einging, die Client-IP-Adresse, Latenzen, Anforderungspfade und Serverantworten.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
D3.DC.An.B.4	Der Zugriff Dritter auf kritische Systeme wird auf unbefugte oder ungewöhnliche Aktivitäten überwacht.	vpc-flow-logs-enabled	VPC-Flow-Protokolle erfassen detaillierte Informationsdatensätze über den IP-Datenverkehr, der zu und von Netzwerkschnittstellen in Ihrer Amazon Virtual Private Cloud (Amazon VPC) fließt. Standardmäßig enthalten Flow-Protokolldatensätze Werte für die verschiedenen Komponenten des IP-Flows, einschließlich Quelle, Ziel und Protokoll.
D3.DC.An.B.4	Der Zugriff Dritter auf kritische Systeme wird auf unbefugte oder ungewöhnliche Aktivitäten überwacht.	cloud-trail-cloud-watch-logs-aktiviert	Verwenden Sie Amazon CloudWatch , um Protokoll ereignisaktivitäten zentral zu sammeln und zu verwalten. Die Aufnahme von AWS CloudTrail Daten liefert Einzelheiten zu den API-Aufrufaktivitäten in Ihrem AWS-Konto.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
D3.DC.An.B.4	Der Zugriff Dritter auf kritische Systeme wird auf unbefugte oder ungewöhnliche Aktivitäten überwacht.	cloudtrail-enabled	AWS CloudTrail kann bei der Nichtabst reitbarkeit helfen, indem Aktionen und API-Aufrufe der AWS Management Console aufgezeic hnet werden. Sie können die Benutzer und die Benutzer AWS-Konten , die einen AWS Dienst aufgerufen haben, die Quell-IP-Adresse, über die die Aufrufe generiert wurden, und den Zeitpunkt der Anrufe identifiz ieren. Einzelheiten zu den erfassten Daten finden Sie in den AWS CloudTrail Datensatzinhalten.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
D3.DC.An.B.4	Der Zugriff Dritter auf kritische Systeme wird auf unbefugte oder ungewöhnliche Aktivitäten überwacht.	multi-region-cloudtrail-enabled	AWS CloudTrail zeichnet Aktionen und API-Aufrufe der AWS Management Console auf. Sie können feststellen, welche Benutzer und Konten angerufen wurden AWS, von welcher Quell-IP-Adresse aus die Anrufe getätigt wurden und wann die Anrufe erfolgten. CloudTrail übermittelt Protokolldateien aus allen AWS Regionen an Ihren S3-Bucket , wenn MULTI_REG ION_CLOUD _TRAIL_ENABLED aktiviert ist. Außerdem wird beim AWS Start einer neuen Region derselbe Trail in der neuen Region erstellt. CloudTrail Dadurch erhalten Sie automatis ch Protokolldateien mit API-Aktivitäten für die neue Region.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
D3.DC.An.B.4	Der Zugriff Dritter auf kritische Systeme wird auf unbefugte oder ungewöhnliche Aktivitäten überwacht.	cloudtrail-s3-data events-enabled	Die Erfassung von Simple Storage Service (Amazon S3)-Datenereignissen unterstützt die Erkennung von ungewöhnlichen Aktivitäten. Zu den Details gehören AWS-Konto Informationen über den Zugriff auf einen Amazon S3 S3-Bucket, die IP-Adresse und die Uhrzeit des Ereignisses.
D3.DC.An.B.4	Der Zugriff Dritter auf kritische Systeme wird auf unbefugte oder ungewöhnliche Aktivitäten überwacht.	elasticsearch-logs-to-cloudwatch	Stellen Sie sicher, dass für Amazon OpenSearch Service-Domains Fehlerprotokolle aktiviert und zur Aufbewahrung und Beantwortung an Amazon CloudWatch Logs gestreamt werden. Domain-Fehlerprotokolle sind bei Sicherheits- und Zugriffsprüfungen sowie bei der Diagnose von Verfügbarkeitsproblemen nützlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
D3.DC.An.B.5	Erhöhte Berechtigungen werden überwacht.	cloudtrail-enabled	AWS CloudTrail kann durch die Aufzeichnung von Aktionen und API-Aufrufen in der AWS Management Console bei der Nichtabstreitbarkeit helfen. Sie können die Benutzer und die Benutzer AWS-Konten , die einen AWS Dienst aufgerufen haben, die Quell-IP-Adresse, über die die Aufrufe generiert wurden, und den Zeitpunkt der Anrufe identifizieren. Einzelheiten zu den erfassten Daten finden Sie in den AWS CloudTrail Datensatzinhalten.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
D3.DC.An.B.5	Erhöhte Berechtigungen werden überwacht.	cloud-trail-cloud-watch-logs-aktiviert	Verwenden Sie Amazon CloudWatch , um Protokollereignisaktivitäten zentral zu sammeln und zu verwalten. Die Aufnahme von AWS CloudTrail Daten liefert Einzelheiten zu den API-Aufrufaktivitäten in Ihrem AWS-Konto.
D3.DC.Ev.B.1	Es wurde eine Baseline für normale Netzwerkaktivitäten eingerichtet.	lambda-concurrency-check	Diese Regel stellt sicher, dass die Höchst- und Untergrenzen für die Gleichzeitigkeit einer Lambda-Funktion festgelegt werden. Dies kann Sie beim Baselining für die Anzahl der Anforderungen unterstützen, die Ihre Funktion zu einem bestimmten Zeitpunkt verarbeitet.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
D3.DC.Ev.B.1	Es wurde eine Baseline für normale Netzwerkaktivitäten eingerichtet.	api-gw-execution-logging-aktiviert	Die API-Gateway-Protokollierung zeigt detaillierte Ansichten der Benutzer, die auf die API zugegriffen haben, und wie diese Benutzer auf die API zugegriffen haben. Diese Einblicke ermöglichen die Transparenz von Benutzeraktivitäten.
D3.DC.Ev.B.1	Es wurde eine Baseline für normale Netzwerkaktivitäten eingerichtet.	cloud-trail-cloud-watch-logs-aktiviert	Verwenden Sie Amazon CloudWatch , um Protokollereignisaktivitäten zentral zu sammeln und zu verwalten. Die Aufnahme von AWS CloudTrail Daten liefert Einzelheiten zu den API-Aufrufaktivitäten in Ihrem AWS-Konto.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
D3.DC.Ev.B.1	Es wurde eine Baseline für normale Netzwerkaktivitäten eingerichtet.	cloudtrail-enabled	AWS CloudTrail kann bei der Nichtabstreitbarkeit helfen, indem Aktionen und API-Aufrufe der AWS Management Console aufgezeichnet werden. Sie können die Benutzer und die Benutzer AWS-Konten , die einen AWS Dienst aufgerufen haben, die Quell-IP-Adresse, über die die Aufrufe generiert wurden, und den Zeitpunkt der Anrufe identifizieren. Einzelheiten zu den erfassten Daten finden Sie in den AWS CloudTrail Datensatzinhalten.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
D3.DC.Ev.B.1	Es wurde eine Baseline für normale Netzwerkaktivitäten eingerichtet.	elb-logging-enabled	Die Elastic-Load-Balancing-Aktivität ist ein zentraler Kommunikationspunkt innerhalb einer Umgebung. Stellen Sie sicher, dass die ELB-Protokollierung aktiviert ist. Die gesammelten Daten enthalten detaillierte Informationen zu Anfragen, die an den ELB gesendet wurden. Jedes Protokoll enthält Informationen wie die Zeit, zu der die Anforderung einging, die Client-IP-Adresse, Latenzen, Anforderungspfade und Serverantworten.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
D3.DC.Ev.B.1	Es wurde eine Baseline für normale Netzwerkaktivitäten eingerichtet.	cloudtrail-s3-data events-enabled	Die Erfassung von Simple Storage Service (Amazon S3)-Datenereignissen unterstützt die Erkennung von ungewöhnlichen Aktivitäten. Zu den Details gehören AWS-Konto Informationen über den Zugriff auf einen Amazon S3 S3-Bucket, die IP-Adresse und die Uhrzeit des Ereignisses.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
D3.DC.Ev.B.1	Es wurde eine Baseline für normale Netzwerkaktivitäten eingerichtet.	multi-region-cloudtrail-enabled	AWS CloudTrail zeichnet Aktionen und API-Aufrufe der AWS Management Console auf. Sie können feststellen, welche Benutzer und Konten angerufen wurden AWS, von welcher Quell-IP-Adresse aus die Anrufe getätigt wurden und wann die Anrufe erfolgten. CloudTrail übermittelt Protokolldateien aus allen AWS Regionen an Ihren S3-Bucket , wenn MULTI_REG ION_CLOUD _TRAIL_ENABLED aktiviert ist. Außerdem wird beim AWS Start einer neuen Region derselbe Trail in der neuen Region erstellt. CloudTrail Dadurch erhalten Sie automatis ch Protokolldateien mit API-Aktivitäten für die neue Region.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
D3.DC.Ev.B.1	Es wurde eine Baseline für normale Netzwerkaktivitäten eingerichtet.	redshift-cluster-configuration-check	Um Daten im Ruhezustand zu schützen, muss die Verschlüsselung für Ihre Amazon-Redshift-Cluster aktiviert sein. Sie müssen auch sicherstellen, dass die erforderlichen Konfigurationen auf Amazon-Redshift-Clustern bereitgestellt werden. Die Prüfungsprotokollierung muss aktiviert sein, um Informationen zu Verbindungen und Benutzeraktivitäten in der Datenbank bereitzustellen. Diese Regel erfordert, dass ein Wert für clusterDbEncrypted (Config Default: TRUE) und LoggingEnabled (Config Default: TRUE) gesetzt ist. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
D3.DC.Ev.B.1	Es wurde eine Baseline für normale Netzwerkaktivitäten eingerichtet.	vpc-flow-logs-enabled	VPC-Flow-Protokolle erfassen detaillierte Informationsdatensätze über den IP-Datenverkehr, der zu und von Netzwerkschnittstellen in Ihrer Amazon Virtual Private Cloud (Amazon VPC) fließt. Standardmäßig enthalten Flow-Protokolldatensätze Werte für die verschiedenen Komponenten des IP-Flows, einschließlich Quelle, Ziel und Protokoll.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
D3.DC.Ev.B.2	Es gibt Mechanismen (z. B. Antiviren warnungen, Warnmeldungen zur Protokollierung von Ereignissen), um vor potenziellen Angriffen zu warnen.	guardduty-enabled-centralized	Amazon GuardDuty kann mithilfe von Threat Intelligence Feeds helfen, potenzielle Cybersicherheitsereignisse zu überwachen und zu erkennen. Dazu gehören Listen mit bösartigen IPs und maschinellen Lernmethoden zur Identifizierung unerwarteter, nicht autorisierter und bösartiger Aktivitäten in Ihrer AWS Cloud-Umgebung.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
D3.DC.Ev.B.3	Es wurden Verfahren eingerichtet, um die Umgebung auf nicht autorisierte Benutzer, Geräte, Verbindungen und Software zu überwachen.	vpc-flow-logs-enabled	VPC-Flow-Protokolle erfassen detaillierte Informationsdatensätze über den IP-Datenverkehr, der zu und von Netzwerkschnittstellen in Ihrer Amazon Virtual Private Cloud (Amazon VPC) fließt. Standardmäßig enthalten Flow-Protokolldatensätze Werte für die verschiedenen Komponenten des IP-Flows, einschließlich Quelle, Ziel und Protokoll.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
D3.DC.Ev.B.3	Es wurden Verfahren eingerichtet, um die Umgebung auf nicht autorisierte Benutzer, Geräte, Verbindun gen und Software zu überwachen.	guardduty-enabled-centralized	Amazon GuardDuty kann mithilfe von Threat Intellige nce Feeds helfen, potenzielle Cybersich erheitsereignisse zu überwachen und zu erkennen. Dazu gehören Listen mit bösartigen IPs und maschinel len Lernmethoden zur Identifizierung unerwarteter, nicht autorisierter und bösartiger Aktivitäten in Ihrer AWS Cloud-Umgebung.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
D3.DC.Ev.B.3	Es wurden Verfahren eingerichtet, um die Umgebung auf nicht autorisierte Benutzer, Geräte, Verbindungen und Software zu überwachen.	securityhub-enabled	AWS Security Hub hilft bei der Überwachung von unbefugtem Personal, Verbindungen, Geräten und Software. AWS Security Hub aggregiert, organisiert und priorisiert die Sicherheitswarnungen oder Ergebnisse mehrerer Dienste. AWS Einige dieser Dienste sind Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer und AWS Firewall Manager sowie AWS Partnerlösungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
D3.DC.Ev.B.3	Es wurden Verfahren eingerichtet, um die Umgebung auf nicht autorisierte Benutzer, Geräte, Verbindungen und Software zu überwachen.	cloudtrail-enabled	AWS CloudTrail kann durch die Aufzeichnung von Aktionen und API-Aufrufen in der AWS Management Console bei der Nichtabstreitbarkeit helfen. Sie können die Benutzer und die Benutzer AWS-Konten , die einen AWS Dienst aufgerufen haben, die Quell-IP-Adresse, über die die Aufrufe generiert wurden, und den Zeitpunkt der Anrufe identifizieren. Einzelheiten zu den erfassten Daten finden Sie in den AWS CloudTrail Datensatzinhalten.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
D3.DC.Th.B.1	Unabhängige Tests (einschließlich Penetrationstests und Schwachstellenscans) werden basierend auf der Risikobewertung für externe Systeme und das interne Netzwerk durchgeführt.	guardduty-enabled-centralized	Amazon GuardDuty kann mithilfe von Threat Intelligence Feeds helfen, potenzielle Cybersicherheitsereignisse zu überwachen und zu erkennen. Dazu gehören Listen mit bösartigen IPs und maschinellen Lernmethoden zur Identifizierung unerwarteter, nicht autorisierter und bösartiger Aktivitäten in Ihrer AWS Cloud-Umgebung.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
D3.DC.Th.B.1	Unabhängige Tests (einschließlich Penetrationstests und Schwachstellenscans) werden basierend auf der Risikobewertung für externe Systeme und das interne Netzwerk durchgeführt.	securityhub-enabled	AWS Security Hub hilft bei der Überwachung von unbefugtem Personal, Verbindungen, Geräten und Software. AWS Security Hub aggregiert, organisiert und priorisiert die Sicherheitswarnungen oder Ergebnisse mehrerer Dienste. AWS Einige dieser Dienste sind Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer und AWS Firewall Manager sowie AWS Partnerlösungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
D3.DC.Th.B.1	Unabhängige Tests (einschließlich Penetrationstests und Schwachstellenscans) werden basierend auf der Risikobewertung für externe Systeme und das interne Netzwerk durchgeführt.	ec2-prüfen managedinstance-patch-compliance-status	Aktivieren Sie diese Regel, um bei der Identifizierung und Dokumentation von Sicherheitslücken in Amazon Elastic Compute Cloud (Amazon EC2) zu helfen. Die Regel prüft, ob die EC2 Amazon-Instance die Patch-Konformität im AWS Systems Manager gemäß den Richtlinien und Verfahren Ihrer Organisation einhält.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
D3.PC.Am.B.1	Der Mitarbeiterzugriff auf Systeme und vertrauliche Daten erfolgt basierend auf den beruflichen Pflichten und dem Grundsätz der geringsten Berechtigung.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) kann Ihnen dabei helfen, die Prinzipien der geringsten Rechte und der Aufgabentrennung in Zugriffsberechtigungen und Autorisierungen zu integrieren und so zu verhindern, dass Richtlinien „Effect“: „Allow“ mit „Action“: „*“ anstelle von „Resource“: „*“ enthalten. Wenn Benutzern mehr Rechte eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und der Aufgabentrennung verstoßen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
D3.PC.Am.B.1	Der Mitarbeiterzugriff auf Systeme und vertrauliche Daten erfolgt basierend auf den beruflich en Pflichten und dem Grundsätz der geringsten Berechtig ung.	iam-group-has-users-überprüfen	AWS Identity and Access Managemen t (IAM) kann Ihnen helfen, die Prinzipien der geringsten Rechte und der Aufgabent rennung mit Zugriffsb erechtigungen und Autorisierungen zu integrieren, indem sichergestellt wird, dass IAM-Gruppen mindestens einen Benutzer haben. Die Einteilung von Benutzern in Gruppen auf der Grundlage der ihnen zugewiese nen Berechtigungen oder ihrer Funktion ist eine Möglichkeit, das Prinzip der geringste n Berechtigung zu implementieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
D3.PC.Am.B.1	Der Mitarbeiterzugriff auf Systeme und vertrauliche Daten erfolgt basierend auf den beruflich en Pflichten und dem Grundsätz der geringsten Berechtig ung.	iam-root-access-key-überprüfen	Der Zugriff auf Systeme und Ressourcen kann gesteuert werden, indem überprüft wird, ob der Root-Benu tzer keine Zugriffss chlüssel mit seiner AWS Identity and Access Management (IAM) -Rolle verknüpft hat. Stellen Sie sicher, dass die Root-Zugr iffsschlüssel gelöscht werden. Erstellen und verwenden Sie stattdessen rollenbas ierte Funktionen, AWS-Konten um das Prinzip der geringste n Funktionalität zu berücksichtigen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
D3.PC.Am.B.1	Der Mitarbeiterzugriff auf Systeme und vertrauliche Daten erfolgt basierend auf den beruflichen Pflichten und dem Grundsätz der geringsten Berechtigung.	iam-user-group-membership-überprüfen	AWS Identity and Access Management (IAM) kann Ihnen helfen, Zugriffsberechtigungen und Autorisierungen einzuschränken, indem sichergestellt wird, dass Benutzer Mitglieder mindestens einer Gruppe sind. Wenn Benutzern mehr Berechtigungen eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und Aufgabentrennung verstoßen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
D3.PC.Am.B.1	Der Mitarbeiterzugriff auf Systeme und vertrauliche Daten erfolgt basierend auf den beruflich en Pflichten und dem Grundsätz der geringsten Berechtig ung.	iam-user-no-policies-überprüfen	Diese Regel stellt sicher, dass AWS Identity and Access Management (IAM) -Richtlinien nur Gruppen oder Rollen zugewiese n werden, um den Zugriff auf Systeme und Ressourcen zu kontrollieren. Die Zuweisung von Berechtig ungen auf Gruppen- oder Rollenebene trägt dazu bei, die Wahrscheinlichkeit zu verringern, dass eine Identität übermäßige Berechtigungen erhält oder beibehält.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
D3.PC.Am.B.1	Der Mitarbeiterzugriff auf Systeme und vertrauliche Daten erfolgt basierend auf den beruflich en Pflichten und dem Grundsätz der geringsten Berechtig ung.	iam-no-inline-policy-überprüfen	Stellen Sie sicher, dass ein Benutzer, eine IAM-Rolle oder eine IAM-Gruppe (AWS Identity and Access Management) nicht über eine Inline-Richtlinie zur Zugriffsk ontrolle auf Systeme und Ressource n verfügt. AWS empfiehlt, verwaltet e Richtlinien anstelle von Inline-Richtlinien zu verwenden. Verwaltete Richtlini en ermöglichen Wiederverwendbarke it, Versionsverwaltung , Rollback und Delegierung der Berechtigungsverwa ltung.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
D3.PC.Am.B.1	Der Mitarbeiterzugriff auf Systeme und vertrauliche Daten erfolgt basierend auf den beruflich en Pflichten und dem Grundsätz der geringsten Berechtig ung.	ec-2 instance-profile-a ttached	EC2 Instanzprofile übergeben eine IAM-Rolle an eine EC2 Instance. Das Anhängen eines Instance-Profils an Ihre Instances kann bei der Implement ierung von geringste n Berechtigungen und der Berechtig ungsverwaltung helfen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
D3.PC.Am.B.1	Der Mitarbeiterzugriff auf Systeme und vertrauliche Daten erfolgt basierend auf den beruflich en Pflichten und dem Grundsätz der geringsten Berechtig ung.	ecs-task-definition-user-for-host-mode-check	Wenn für eine Aufgabendefinition erhöhte Berechtig ungen gelten, liegt das daran, dass der Kunde diesen Konfigura tionen ausdrücklich zugestimmt hat. Diese Kontrolle prüft, ob eine unerwartete Berechtigungseskal ation vorliegt, wenn für eine Aufgabend efinition das Host-Netzwerk aktiviert ist, die Kunden aber keine erhöhten Berechtigungen aktiviert haben.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
D3.PC.Am.B.1	Der Mitarbeiterzugriff auf Systeme und vertrauliche Daten erfolgt basierend auf den beruflich en Pflichten und dem Grundsätz der geringsten Berechtig ung.	iam-customer-policy-blocked-kms-Aktionen	AWS Identity and Access Managemen t (IAM) kann Ihnen helfen, die Prinzipien der geringsten Rechte und der Aufgabent rennung in Zugriffsb erechtigungen und Autorisierungen zu integrieren und so zu verhindern, dass Richtlinien blockiert e Aktionen für alle AWS Schlüssel des Key Management Service enthalten. Wenn Benutzer mehr Rechte haben, als für die Ausführung einer Aufgabe erforderl ich sind, kann dies gegen das Prinzip der geringsten Berechtig ung und Aufgabent rennung verstoßen . Mit dieser Regel können Sie den Parameter festlegen . blockedActionsPatt erns (Wert „AWS Bewährte grundlege nde Sicherhei tsmethoden“: kms:

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			Decrypt, kms:ReEncryptFrom). Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
D3.PC.Am.B.1	Der Mitarbeiterzugriff auf Systeme und vertrauliche Daten erfolgt basierend auf den beruflich en Pflichten und dem Grundsätz der geringsten Berechtig ung.	iam-inline-policy-blocked-kms-Aktionen	Stellen Sie sicher, dass ein Benutzer, eine IAM-Rolle oder eine IAM-Gruppe (AWS Identity and Access Management) nicht über eine Inline-Richtlinie verfügt, die blockierte Aktionen für alle AWS Schlüssel des Key Management Service zulässt. AWS empfiehlt, verwaltet e Richtlinien anstelle von Inline-Richtlinien zu verwenden. Verwaltete Richtlini en ermöglichen Wiederverwendbarke it, Versionsverwaltung , Rollback und Delegierung der Berechtigungsverwa ltung. Mit dieser Regel können Sie den blockedActionsPatt erns Parameter festlegen. (Wert „AWS Bewährte grundlege nde Sicherhei tsmethoden“: kms: Decrypt, kms:ReEnc ryptFrom). Die

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.
D3.PC.Am.B.1	Der Mitarbeiterzugriff auf Systeme und vertrauliche Daten erfolgt basierend auf den beruflichen Pflichten und dem Grundsätz der geringsten Berechtigung.	iam-policy-no-statements-with-full-access	Stellen Sie sicher, dass IAM-Aktionen nur auf die benötigten Aktionen beschränkt sind. Wenn Benutzern mehr Rechte eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und der Aufgabentrennung verstoßen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
D3.PC.Am.B.10	Produktions- und Nichtproduktionsumgebungen sind segmentiert, um unbefugten Zugriff oder Änderungen an Informationsressourcen zu verhindern. (*N/A, wenn keine Produktionsumgebung in der Institution oder einem Drittanbieter der Institution vorhanden ist.)	ec2- instances-in-vpc	Stellen Sie Amazon Elastic Compute Cloud (Amazon EC2) -Instances innerhalb einer Amazon Virtual Private Cloud (Amazon VPC) bereit, um eine sichere Kommunikation zwischen einer Instance und anderen Services innerhalb der Amazon VPC zu ermöglichen, ohne dass ein Internet-Gateway, ein NAT-Gerät oder eine VPN-Verbindung erforderlich ist. Der gesamte Datenverkehr bleibt sicher in der AWS Cloud. Domains, die sich innerhalb einer VPC befinden, verfügen aufgrund ihrer logischen Isolierung im Vergleich zu Domains mit öffentlichen Endpunkten über eine zusätzliche Sicherheitsebene. Weisen Sie EC2

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			Amazon-Instances einer Amazon-VPC zu, um den Zugriff ordnungsgemäß zu verwalten.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
D3.PC.Am.B.10	Produktions- und Nichtproduktionsumgebungen sind segmentiert, um unbefugten Zugriff oder Änderungen an Informationsressourcen zu verhindern. (*N/A, wenn in der Institution oder bei einem Drittanbieter der Institution keine Produktionsumgebung vorhanden ist.)	vpc-sg-open-only-to-authorized-ports	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass gemeinsame Ports für Amazon Elastic Compute Cloud (Amazon EC2) -Sicherheitsgruppen eingeschränkt sind. Wenn der Zugriff auf Ports nicht auf vertrauenswürdige Quellen beschränkt wird, kann dies zu Angriffen auf die Verfügbarkeit, Integrität und Vertraulichkeit von Systemen führen. Durch die Beschränkung des Zugriffs auf Ressourcen innerhalb einer Sicherheitsgruppe aus dem Internet (0.0.0.0/0) kann der Remote-Zugriff auf interne Systeme gesteuert werden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
D3.PC.Am.B.10	Produktions- und Nichtproduktionsumgebungen sind segmentiert, um unbefugten Zugriff oder Änderungen an Informationsressourcen zu verhindern. (*N/A, wenn keine Produktionsumgebung in der Institution oder einem Drittanbieter der Institution vorhanden ist.)	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) Security Groups können bei der Verwaltung des Netzwerkzugriffs helfen, indem sie eine statusbehaftete Filterung von eingehendem und ausgehendem Netzwerkverkehr zu Ressourcen bereitstellen. AWS Wenn Sie eingehenden (oder entfernten) Datenverkehr von 0.0.0.0/0 bis Port 22 auf Ihren Ressourcen nicht zulassen, können Sie den Remote-Zugriff einschränken.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
D3.PC.Am.B.10	Produktions- und Nichtproduktionsumgebungen sind segmentiert, um unbefugten Zugriff oder Änderungen an Informationsressourcen zu verhindern. (*N/A, wenn keine Produktionsumgebung in der Institution oder einem Drittanbieter der Institution vorhanden ist.)	restricted-common-ports	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass gemeinsame Ports für Amazon Elastic Compute Cloud (Amazon EC2) -Sicherheitsgruppen eingeschränkt sind. Wenn der Zugriff auf Ports nicht auf vertrauenswürdige Quellen beschränkt wird, kann dies zu Angriffen auf die Verfügbarkeit, Integrität und Vertraulichkeit von Systemen führen. Mit dieser Regel können Sie optional die Parameter blockedPort1–blockedPort5 festlegen (Standardkonfigurationen: 20, 21, 3389, 3306, 4333). Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
D3.PC.Am.B.12	Alle Passwörter werden im Speicher und während der Übertragung verschlüsselt.	emr-kerberos-enabled	Die Zugriffsberechtigungen und -autorisierungen können verwaltet und nach den Prinzipien der geringsten Berechtigung und Aufgabentrennung integriert werden, indem Kerberos für Amazon-EMR-Cluster aktiviert wird. In Kerberos werden Services und Benutzer, die sich authentifizieren müssen, als Prinzipale bezeichnet. Prinzipale befinden sich in einem Kerberos-Bereich. Innerhalb dieses Bereichs wird ein Kerberos-Server als Key Distribution Center (KDC) bezeichnet. Über diesen Server können sich Prinzipale authentifizieren. Die Authentifizierung im KDC erfolgt durch die Ausstellung von Authentif

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			izierungstickets. Das KDC unterhält eine Datenbank der Prinzipale in seinem Bereich mit ihren Passwörtern und anderen administr ativen Informationen zu jedem Prinzipal.
D3.PC.Am.B.12	Alle Passwörter werden im Speicher und während der Übertragung verschlüsselt.	ec2- ebs-encryption-by-default	Zum Schutz von Daten im Ruhezusta nd müssen Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon Elastic Block Store (Amazon EBS)-Volu mes aktiviert ist. Da sensible Daten auch im Ruhezusta nd vorhanden sein können, sollten Sie die Verschlüsselung im Ruhezustand aktivieren, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
D3.PC.Am.B.12	Alle Passwörter werden im Speicher und während der Übertragung verschlüsselt.	s3- -aktiviert bucket-server-side-encryption	Zum Schutz von Daten im Ruhezustand müssen Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon Simple Storage Service (Amazon S3)-Buckets aktiviert ist. Um eventuell vorhandene sensible Daten im Ruhezustand in Amazon-S3-Buckets zu schützen, muss die Verschlüsselung aktiviert sein.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
D3.PC.Am.B.12	Alle Passwörter werden im Speicher und während der Übertragung verschlüsselt.	s-3 bucket-ssl-requests-only	Um Daten während der Übertragung zu schützen, stellen Sie sicher, dass Ihre Amazon Simple Storage Service (Amazon S3)-Buckets Anfragen zur Verwendung von Secure Socket Layer (SSL)-Buckets erfordern. Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
D3.PC.Am.B.12	Alle Passwörter werden im Speicher und während der Übertragung verschlüsselt.	rds-storage-encrypted	Zum Schutz von Daten im Ruhezustand müssen Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon Relational Database Service (Amazon RDS)-Instances aktiviert ist. Um eventuell vorhandene sensible Daten im Ruhezustand in Amazon-RDS-Instances zu schützen, muss die Verschlüsselung von Daten im Ruhezustand aktiviert sein.
D3.PC.Am.B.12	Alle Passwörter werden im Speicher und während der Übertragung verschlüsselt.	encrypted-volumes	Aktivieren Sie die Verschlüsselung für Ihre Amazon-Elastic-Block-Store (Amazon-EBS)-Volumes, um eventuell vorhandene sensible Daten sowie Daten im Ruhezustand zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
D3.PC.Am.B.12	Alle Passwörter werden im Speicher und während der Übertragung verschlüsselt.	opensearch-encrypted-at-rest	Da sensible Daten vorhanden sein können und um Daten im Ruhezustand zu schützen, sollten Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon OpenSearch Service-Domains aktiviert ist.
D3.PC.Am.B.12	Alle Passwörter werden im Speicher und während der Übertragung verschlüsselt.	opensearch-node-to-node-Verschlüsselungsprüfung	Stellen Sie sicher, dass die node-to-node Verschlüsselung für Amazon OpenSearch Service aktiviert ist. Node-to-nodeVerschlüsselung ermöglicht die TLS 1.2-Verschlüsselung für die gesamte Kommunikation innerhalb der Amazon Virtual Private Cloud (Amazon VPC). Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
D3.PC.Am.B.12	Alle Passwörter werden im Speicher und während der Übertragung verschlüsselt.	efs-encrypted-check	Aktivieren Sie die Verschlüsselung für Ihr Amazon Elastic File System (EFS), um eventuell vorhandene sensible Daten sowie Daten im Ruhezustand zu schützen.
D3.PC.Am.B.12	Alle Passwörter werden im Speicher und während der Übertragung verschlüsselt.	elasticsearch-encrypted-at-rest	Da sensible Daten vorhanden sein können und um Daten im Ruhezustand zu schützen, sollten Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon OpenSearch Service (OpenSearch Service) -Domains aktiviert ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
D3.PC.Am.B.12	Alle Passwörter werden im Speicher und während der Übertragung verschlüsselt.	elasticsearch-node-to-node-Verschlüsselungsprüfung	Stellen Sie sicher, dass die node-to-node Verschlüsselung für Amazon OpenSearch Service aktiviert ist. Node-to-nodeVerschlüsselung ermöglicht die TLS 1.2-Verschlüsselung für die gesamte Kommunikation innerhalb der Amazon Virtual Private Cloud (Amazon VPC). Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
D3.PC.Am.B.12	Alle Passwörter werden im Speicher und während der Übertragung verschlüsselt.	alb-http-to-https-Umleitungsprüfung	Um Daten während der Übertragung zu schützen, stellen Sie sicher, dass Ihr Application Load Balancer unverschlüsselte HTTP-Anfragen automatisch an HTTPS umleitet. Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.
D3.PC.Am.B.12	Alle Passwörter werden im Speicher und während der Übertragung verschlüsselt.	elb-tls-https-listeners-nur	Stellen Sie sicher, dass Ihre Elastic Load Balancer (ELBs) mit SSL- oder HTTPS-Listenern konfiguriert sind. Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
D3.PC.Am.B.12	Alle Passwörter werden im Speicher und während der Übertragung verschlüsselt.	redshift-require-tls-ssl	Stellen Sie sicher, dass Ihre Amazon-Redshift-Cluster eine TLS/SSL-Verschlüsselung erfordern, um eine Verbindung zu SQL-Clients herzustellen. Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
D3.PC.Am.B.12	Alle Passwörter werden im Speicher und während der Übertragung verschlüsselt.	redshift-cluster-configuration-check	Um Daten im Ruhezustand zu schützen, muss die Verschlüsselung für Ihre Amazon-Redshift-Cluster aktiviert sein. Sie müssen auch sicherstellen, dass die erforderlichen Konfigurationen auf Amazon-Redshift-Clustern bereitgestellt werden. Die Prüfungsprotokollierung muss aktiviert sein, um Informationen zu Verbindungen und Benutzeraktivitäten in der Datenbank bereitzustellen. Diese Regel erfordert, dass ein Wert für clusterDbEncrypted (Config Default: TRUE) und LoggingEnabled (Config Default: TRUE) gesetzt ist. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
D3.PC.Am.B.12	Alle Passwörter werden im Speicher und während der Übertragung verschlüsselt.	api-gw-ssl-enabled	Stellen Sie sicher, dass die REST-API-Stufen von Amazon API Gateway mit SSL-Zertifikaten konfiguriert sind, damit Backend-Systeme überprüfen können, ob Anforderungen von API Gateway stammen.
D3.PC.Am.B.12	Alle Passwörter werden im Speicher und während der Übertragung verschlüsselt.	backup-recovery-point-encrypted	Stellen Sie sicher, dass die Verschlüsselung für Ihre AWS Backup-Wiederherstellungspunkte aktiviert ist. Da sensible Daten auch im Ruhezustand vorhanden sein können, sollten Sie die Verschlüsselung im Ruhezustand aktivieren, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
D3.PC.Am.B.12	Alle Passwörter werden im Speicher und während der Übertragung verschlüsselt.	redshift-cluster-kms-enabled	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass die Verschlüs selung mit AWS Key Management Service (AWS KMS) für Ihren Amazon Redshift Redshift-Cluster aktiviert ist. Um eventuell vorhanden e sensible Daten im Ruhezustand in Redshift-Clustern zu schützen, muss die Verschlüsselung von Daten im Ruhezusta nd aktiviert sein.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
D3.PC.Am.B.12	Alle Passwörter werden im Speicher und während der Übertragung verschlüsselt.	s-3 default-encryption -kms	Stellen Sie sicher, dass die Verschlüs selung für Ihre Amazon Simple Storage Service (Amazon S3)-Bucke ts aktiviert ist. Um eventuell vorhanden e sensible Daten im Ruhezustand in einem Amazon-S3-Bucket zu schützen, muss die Verschlüsselung aktiviert sein.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
D3.PC.Am.B.13	Vertrauliche Daten werden verschlüs selt, wenn sie über öffentliche oder nicht vertrauenswürdige Netzwerke (z. B. Internet) übertragen werden.	elb-acm-certificate-required	Zum Schutz von eventuell vorhanden en sensiblen Daten sowie von Daten während der Übertragung muss die Verschlüsselung für Ihr Elastic Load Balancing aktiviert sein. Verwenden Sie AWS Certificate Manager, um öffentlic he und private SSL/ TLS-Zertifikate mit AWS Diensten und internen Ressource n zu verwalten, bereitzustellen und bereitzustellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
D3.PC.Am.B.13	Vertrauliche Daten werden verschlüs selt, wenn sie über öffentliche oder nicht vertrauenswürdige Netzwerke (z. B. das Internet) übertragen werden.	alb-http-to-https-Umleitungsprüfung	Um Daten während der Übertragung zu schützen, stellen Sie sicher, dass Ihr Application Load Balancer unverschl üsselte HTTP-Anfr agen automatisch an HTTPS umleitet. Um eventuell vorhanden e sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.
D3.PC.Am.B.13	Vertrauliche Daten werden verschlüs selt, wenn sie über öffentliche oder nicht vertrauenswürdige Netzwerke (z. B. das Internet) übertragen werden.	elb-tls-https-listeners-nur	Stellen Sie sicher, dass Ihre Elastic Load Balancer (ELBs) mit SSL- oder HTTPS-Listenern konfiguriert sind. Um eventuell vorhanden e sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
D3.PC.Am.B.13	Vertrauliche Daten werden verschlüs selt, wenn sie über öffentliche oder nicht vertrauenswürdige Netzwerke (z. B. das Internet) übertragen werden.	redshift-require-tls-ssl	Stellen Sie sicher, dass Ihre Amazon-Redshift-Cluster eine TLS/SSL-Verschlüss elung erfordern, um eine Verbindun g zu SQL-Clients herzustellen. Um eventuell vorhanden e sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.
D3.PC.Am.B.13	Vertrauliche Daten werden verschlüs selt, wenn sie über öffentliche oder nicht vertrauenswürdige Netzwerke (z. B. das Internet) übertragen werden.	s-3 bucket-ssl-request s-only	Um Daten während der Übertragung zu schützen, stellen Sie sicher, dass Ihre Amazon Simple Storage Service (Amazon S3)-Bucke ts Anfragen zur Verwendung von Secure Socket Layer (SSL)-Buc kets erfordern. Um eventuell vorhanden e sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
D3.PC.Am.B.13	Vertrauliche Daten werden verschlüs selt, wenn sie über öffentliche oder nicht vertrauenswürdige Netzwerke (z. B. Internet) übertragen werden.	api-gw-ssl-enabled	Stellen Sie sicher, dass die REST-API-Stufen von Amazon API Gateway mit SSL-Zertifikaten konfiguri ert sind, damit Backend-Systeme überprüfen können, ob Anforderungen von API Gateway stammen.
D3.PC.Am.B.13	Vertrauliche Daten werden verschlüs selt, wenn sie über öffentliche oder nicht vertrauenswürdige Netzwerke (z. B. das Internet) übertragen werden.	elbv2- acm-certificate-required	Zum Schutz von eventuell vorhanden en sensiblen Daten sowie von Daten während der Übertragung muss die Verschlüsselung für Ihr Elastic Load Balancing aktiviert sein. Verwenden Sie AWS Certificate Manager, um öffentlic he und private SSL/ TLS-Zertifikate mit AWS Diensten und internen Ressource n zu verwalten, bereitzustellen und bereitzustellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
D3.PC.Am.B.15	Der Remote-Zugriff auf kritische Systeme durch Mitarbeiter, Auftragnehmer und Dritte erfolgt über verschlüsselte Verbindungen und Multi-Faktor-Authentifizierung.	s-3 bucket-ssl-requests-only	Um Daten während der Übertragung zu schützen, stellen Sie sicher, dass Ihre Amazon Simple Storage Service (Amazon S3)-Buckets Anfragen zur Verwendung von Secure Socket Layer (SSL)-Buckets erfordern. Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
D3.PC.Am.B.15	Der Remote-Zugriff auf kritische Systeme durch Mitarbeiter, Auftragnehmer und Dritte erfolgt über verschlüsselte Verbindungen und Multi-Faktor-Authentifizierung.	root-account-hardware-mfa-aktiviert	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Hardware-MFA für den Root-Benutzer aktiviert ist. Der Stammbenutzer ist der AWS-Konto-Benutzer mit den meisten Berechtigungen. MFA sorgt für eine weitere Schutzebene zusätzlich zu den Anmeldeinformationen. Indem Sie MFA für den Root-Benutzer vorschreiben, können Sie die Anzahl AWS-Konten kompromittierter Benutzer reduzieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
D3.PC.Am.B.15	Der Remote-Zugriff auf kritische Systeme durch Mitarbeiter, Auftragnehmer und Dritte erfolgt über verschlüsselte Verbindungen und Multi-Faktor-Authentifizierung.	root-account-mfa-enabled	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass MFA für den Root-Benutzer aktiviert ist. Der Stammbenutzer ist der AWS-Konto-Benutzer mit den meisten Berechtigungen. MFA sorgt für eine weitere Schutzebene zusätzlich zu den Anmeldeinformationen. Indem Sie MFA für den Root-Benutzer vorschreiben, können Sie die Anzahl AWS-Konten kompromittierter Benutzer reduzieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
D3.PC.Am.B.15	Der Remote-Zugriff auf kritische Systeme durch Mitarbeiter, Auftragnehmer und Dritte erfolgt über verschlüsselte Verbindungen und Multi-Faktor-Authentifizierung.	mfa-enabled-for-iam-Konsolenzugriff	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass MFA für alle AWS Identity and Access Management (IAM) -Benutzer aktiviert ist, die über ein Konsolenkennwort verfügen. MFA sorgt für eine weitere Schutzebene zusätzlich zu den Anmeldeinformationen. Indem Sie MFA für Benutzer vorschreiben, können Sie Fälle kompromittierter Konten reduzieren und verhindern, dass unbefugte Benutzer auf vertrauliche Daten zugreifen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
D3.PC.Am.B.15	Der Remote-Zugriff auf kritische Systeme durch Mitarbeiter, Auftragnehmer und Dritte erfolgt über verschlüsselte Verbindungen und Multi-Faktor-Authentifizierung.	alb-http-to-https-Umleitungsprüfung	Um Daten während der Übertragung zu schützen, stellen Sie sicher, dass Ihr Application Load Balancer unverschlüsselte HTTP-Anfragen automatisch an HTTPS umleitet. Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.
D3.PC.Am.B.15	Der Remote-Zugriff auf kritische Systeme durch Mitarbeiter, Auftragnehmer und Dritte erfolgt über verschlüsselte Verbindungen und Multi-Faktor-Authentifizierung.	api-gw-ssl-enabled	Stellen Sie sicher, dass die REST-API-Stufen von Amazon API Gateway mit SSL-Zertifikaten konfiguriert sind, damit Backend-Systeme überprüfen können, ob Anforderungen von API Gateway stammen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
D3.PC.Am.B.15	Der Remote-Zugriff auf kritische Systeme durch Mitarbeiter, Auftragnehmer und Dritte erfolgt über verschlüsselte Verbindungen und Multi-Faktor-Authentifizierung.	redshift-require-tls-ssl	Stellen Sie sicher, dass Ihre Amazon-Redshift-Cluster eine TLS/SSL-Verschlüsselung erfordern, um eine Verbindung zu SQL-Clients herzustellen. Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
D3.PC.Am.B.16	Administrative, physische oder technische Kontrollen verhindern, dass Benutzer ohne administrative Aufgaben nicht autorisierte Software installieren.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) kann Ihnen dabei helfen, die Prinzipien der geringsten Rechte und der Aufgabentrennung in Zugriffsberechtigungen und Autorisierungen zu integrieren und so zu verhindern, dass Richtlinien „Effect“: „Allow“ mit „Action“: „*“ anstelle von „Resource“: „*“ enthalten. Wenn Benutzern mehr Rechte eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und der Aufgabentrennung verstoßen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
D3.PC.Am.B.16	Administrative, physische oder technische Kontrolle n verhindern, dass Benutzer ohne administrative Aufgaben nicht autorisierte Software installieren.	iam-group-has-users-überprüfen	AWS Identity and Access Managemen t (IAM) kann Ihnen helfen, die Prinzipien der geringsten Rechte und der Aufgabent rennung mit Zugriffsb erechtigungen und Autorisierungen zu integrieren, indem sichergestellt wird, dass IAM-Gruppen mindestens einen Benutzer haben. Die Einteilung von Benutzern in Gruppen auf der Grundlage der ihnen zugewiese nen Berechtigungen oder ihrer Funktion ist eine Möglichkeit, das Prinzip der geringste n Berechtigung zu implementieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
D3.PC.Am.B.16	Administrative, physische oder technische Kontrollen verhindern, dass Benutzer ohne administrative Aufgaben nicht autorisierte Software installieren.	iam-user-group-membership-überprüfen	AWS Identity and Access Management (IAM) kann Ihnen helfen, Zugriffsberechtigungen und Autorisierungen einzuschränken, indem sichergestellt wird, dass Benutzer Mitglieder mindestens einer Gruppe sind. Wenn Benutzern mehr Berechtigungen eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und Aufgabentrennung verstoßen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
D3.PC.Am.B.16	Administrative, physische oder technische Kontrollen verhindern, dass Benutzer ohne administrative Aufgaben nicht autorisierte Software installieren.	iam-policy-no-statements-with-full-access	Stellen Sie sicher, dass IAM-Aktionen nur auf die benötigten Aktionen beschränkt sind. Wenn Benutzern mehr Rechte eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und der Aufgabentrennung verstoßen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
D3.PC.Am.B.2	Der Mitarbeiterzugriff auf Systeme und vertrauliche Daten erfolgt nach dem Grundsatz der Aufgabentrennung.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) kann Ihnen dabei helfen, die Prinzipien der geringsten Rechte und der Aufgabentrennung in Zugriffsberechtigungen und Autorisierungen zu integrieren und so zu verhindern, dass Richtlinien „Effect“: „Allow“ mit „Action“: „*“ anstelle von „Resource“: „*“ enthalten. Wenn Benutzern mehr Rechte eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und der Aufgabentrennung verstoßen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
D3.PC.Am.B.2	Der Mitarbeiterzugriff auf Systeme und vertrauliche Daten erfolgt nach dem Grundsatz der Aufgabentrennung.	iam-user-group-membership-überprüfen	AWS Identity and Access Management (IAM) kann Ihnen helfen, Zugriffsberechtigungen und Autorisierungen einzuschränken, indem sichergestellt wird, dass Benutzer Mitglieder mindestens einer Gruppe sind. Wenn Benutzern mehr Berechtigungen eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und Aufgabentrennung verstoßen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
D3.PC.Am.B.2	Der Mitarbeiterzugriff auf Systeme und vertrauliche Daten erfolgt nach dem Grundsatz der Aufgabentrennung.	iam-policy-no-statements-with-full-access	Stellen Sie sicher, dass IAM-Aktionen nur auf die benötigten Aktionen beschränkt sind. Wenn Benutzern mehr Rechte eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und der Aufgabentrennung verstoßen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
D3.PC.Am.B.3	Erhöhte Rechte (z. B. Administratorrechte) sind begrenzt und werden streng kontrolliert (sie werden z. B. einzelnen Personen zugewiesen, nicht gemeinsam genutzt und erfordern strengere Kennwortkontrollen)	root-account-hardware-mfa-aktiviert	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Hardware-MFA für den Root-Benutzer aktiviert ist. Der Stammbenutzer ist der AWS-Konto-Benutzer mit den meisten Berechtigungen. MFA sorgt für eine weitere Schutzebene zusätzlich zu den Anmeldeinformationen. Indem Sie MFA für den Root-Benutzer vorschreiben, können Sie die Anzahl AWS-Konten kompromittierter Benutzer reduzieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
D3.PC.Am.B.3	Erhöhte Rechte (z. B. Administratorrechte) sind begrenzt und werden streng kontrolliert (sie werden z. B. einzelnen Personen zugewiesen, nicht gemeinsam genutzt und erfordern strengere Kennwortkontrollen)	root-account-mfa-enabled	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass MFA für den Root-Benutzer aktiviert ist. Der Stammbenutzer ist der AWS-Konto-Benutzer mit den meisten Berechtigungen. MFA sorgt für eine weitere Schutzebene zusätzlich zu den Anmeldeinformationen. Indem Sie MFA für den Root-Benutzer vorschreiben, können Sie die Anzahl AWS-Konten kompromittierter Benutzer reduzieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
D3.PC.Am.B.3	Erhöhte Rechte (z. B. Administratorrechte) sind begrenzt und werden streng kontrolliert (sie werden z. B. einzelnen Personen zugewiesen, nicht gemeinsam genutzt und erfordern strengere Kennwortkontrollen).	iam-group-has-users-überprüfen	AWS Identity and Access Management (IAM) kann Ihnen helfen, die Prinzipien der geringsten Rechte und der Aufgabentrennung mit Zugriffsberechtigungen und Autorisierungen zu integrieren, indem sichergestellt wird, dass IAM-Gruppen mindestens einen Benutzer haben. Die Einteilung von Benutzern in Gruppen auf der Grundlage der ihnen zugewiesenen Berechtigungen oder ihrer Funktion ist eine Möglichkeit, das Prinzip der geringsten Berechtigung zu implementieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
D3.PC.Am.B.3	Erhöhte Rechte (z. B. Administratorrechte) sind begrenzt und werden streng kontrolliert (sie werden z. B. einzelnen Personen zugewiesen, nicht gemeinsam genutzt und erfordern strengere Kennwortkontrollen)	iam-root-access-key-überprüfen	Der Zugriff auf Systeme und Ressourcen kann gesteuert werden, indem überprüft wird, ob der Root-Benutzer keine Zugriffsschlüssel mit seiner AWS Identity and Access Management (IAM) -Rolle verknüpft hat. Stellen Sie sicher, dass die Root-Zugriffsschlüssel gelöscht werden. Erstellen und verwenden Sie stattdessen rollenbasierte Funktionen, AWS-Konten um das Prinzip der geringsten Funktionalität zu berücksichtigen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
D3.PC.Am.B.3	Erhöhte Rechte (z. B. Administratorrechte) sind begrenzt und werden streng kontrolliert (sie werden z. B. einzelnen Personen zugewiesen, nicht gemeinsam genutzt und erfordern strengere Kennwortkontrollen)	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) kann Ihnen dabei helfen, die Prinzipien der geringsten Rechte und der Aufgabentrennung in Zugriffsberechtigungen und Autorisierungen zu integrieren und so zu verhindern, dass Richtlinien „Effect“: „Allow“ mit „Action“: „*“ anstelle von „Resource“: „*“ enthalten. Wenn Benutzern mehr Rechte eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und der Aufgabentrennung verstoßen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
D3.PC.Am.B.3	Erhöhte Rechte (z. B. Administratorrechte) sind begrenzt und werden streng kontrolliert (sie werden z. B. einzelnen Personen zugewiesen, nicht gemeinsam genutzt und erfordern strengere Kennwortkontrollen)	iam-policy-no-statements-with-full-access	Stellen Sie sicher, dass IAM-Aktionen nur auf die benötigten Aktionen beschränkt sind. Wenn Benutzern mehr Rechte eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und der Aufgabentrennung verstoßen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
D3.PC.Am.B.6	Für den Zugriff auf Systeme, Anwendungen und Hardware sind Identifikation und Authentifizierung erforderlich und werden verwaltet.	iam-user-unused-credentials-überprüfen	AWS Identity and Access Management (IAM) kann Ihnen bei Zugriffsberechtigungen und Autorisierungen helfen, indem es nach IAM-Passwörtern und Zugriffsschlüsseln sucht, die für einen bestimmten Zeitraum nicht verwendet wurden. Wenn ungenutzte Anmeldeinformationen identifiziert werden, müssen Sie sie deaktivieren und/oder entfernen, da dies gegen das Prinzip der geringsten Berechtigung verstoßen könnte. Für diese Regel müssen Sie einen Wert für das maxCredentialUsage Alter festlegen (Standardkonfiguration: 90). Der tatsächliche Wert muss den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
D3.PC.Am.B.6	Für den Zugriff auf Systeme, Anwendungen und Hardware sind Identifikation und Authentifizierung erforderlich und werden verwaltet.	iam-password-policy	Die Identitäten und Anmeldeinformationen werden auf der Grundlage einer organisatorischen IAM-Passwortrichtlinie ausgestellt, verwaltet und verifiziert. Sie erfüllen oder übertreffen die Anforderungen von NIST SP 800-63 und dem Standard „Best Practices“ von AWS Foundational Security für die Passwortstärke. Mit dieser Regel können Sie optional RequireUppercaseCharacters (Wert für AWS grundlegende Sicherheitsbewährte Methoden: wahr), RequireLowercaseCharacters (Wert für bewährte Methoden für AWS grundlegende Sicherheit: wahr), RequireSymbols (Wert für bewährte Methoden für AWS grundlegende Sicherheit:

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			wahr), RequireNumbers (Wert für bewährte Methoden für AWS grundlegende Sicherheit: wahr), MinimumPasswordLength (Wert für bewährte Methoden für AWS grundlegende Sicherheit: 14), PasswordReusePrevention (Wert für bewährte Methoden für AWS grundlegende Sicherheit: 24) und MaxPasswordAge (Wert für bewährte Methoden für AWS grundlegende Sicherheit: 90) für Ihr IAM festlegen Kennwortrichtlinie. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
D3.PC.Am.B.6	Für den Zugriff auf Systeme, Anwendungen und Hardware sind Identifikation und Authentifizierung erforderlich und werden verwaltet.	iam-user-mfa-enabled	Aktivieren Sie diese Regel, um den Zugriff auf Ressourcen in der AWS Cloud einzuschränken. Diese Regel sorgt dafür, dass die Multi-Faktor-Authentifizierung (MFA) für alle Benutzer aktiviert ist. MFA sorgt für eine weitere Schutzebene zusätzlich zu den Anmeldeinformationen. Reduzieren Sie Fälle von kompromittierten Konten, indem Sie MFA für Benutzer vorschreiben.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
D3.PC.Am.B.6	Für den Zugriff auf Systeme, Anwendungen und Hardware sind Identifikation und Authentifizierung erforderlich und werden verwaltet.	mfa-enabled-for-iam-Konsolenzugriff	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass MFA für alle AWS Identity and Access Management (IAM) -Benutzer aktiviert ist, die über ein Konsolenkennwort verfügen. MFA sorgt für eine weitere Schutzebene zusätzlich zu den Anmeldeinformationen. Indem Sie MFA für Benutzer vorschreiben, können Sie Fälle kompromittierter Konten reduzieren und verhindern, dass unbefugte Benutzer auf vertrauliche Daten zugreifen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
D3.PC.Am.B.6	Für den Zugriff auf Systeme, Anwendungen und Hardware sind Identifikation und Authentifizierung erforderlich und werden verwaltet.	root-account-hardware-mfa-aktiviert	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Hardware-MFA für den Root-Benutzer aktiviert ist. Der Stammbenutzer ist der AWS-Konto-Benutzer mit den meisten Berechtigungen. MFA sorgt für eine weitere Schutzebene zusätzlich zu den Anmeldeinformationen. Indem Sie MFA für den Root-Benutzer vorschreiben, können Sie die Anzahl AWS-Konten kompromittierter Benutzer reduzieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
D3.PC.Am.B.6	Für den Zugriff auf Systeme, Anwendungen und Hardware sind Identifikation und Authentifizierung erforderlich und werden verwaltet.	root-account-mfa-enabled	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass MFA für den Root-Benutzer aktiviert ist. Der Stammbenutzer ist der AWS-Konto-Benutzer mit den meisten Berechtigungen. MFA sorgt für eine weitere Schutzebene zusätzlich zu den Anmeldeinformationen. Indem Sie MFA für den Root-Benutzer vorschreiben, können Sie die Anzahl AWS-Konten kompromittierter Benutzer reduzieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
D3.PC.Am.B.6	Für den Zugriff auf Systeme, Anwendungen und Hardware sind Identifikation und Authentifizierung erforderlich und werden verwaltet.	iam-group-has-users-überprüfen	AWS Identity and Access Management (IAM) kann Ihnen helfen, die Prinzipien der geringsten Rechte und der Aufgabentrennung mit Zugriffsberechtigungen und Autorisierungen zu integrieren, indem sichergestellt wird, dass IAM-Gruppen mindestens einen Benutzer haben. Die Einteilung von Benutzern in Gruppen auf der Grundlage der ihnen zugewiesenen Berechtigungen oder ihrer Funktion ist eine Möglichkeit, das Prinzip der geringsten Berechtigung zu implementieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
D3.PC.Am.B.6	Für den Zugriff auf Systeme, Anwendungen und Hardware sind Identifikation und Authentifizierung erforderlich und werden verwaltet.	iam-user-group-membership-überprüfen	AWS Identity and Access Management (IAM) kann Ihnen helfen, Zugriffsberechtigungen und Autorisierungen einzuschränken, indem sichergestellt wird, dass Benutzer Mitglieder mindestens einer Gruppe sind. Wenn Benutzern mehr Berechtigungen eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und Aufgabentrennung verstoßen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
D3.PC.Am.B.6	Für den Zugriff auf Systeme, Anwendungen und Hardware sind Identifikation und Authentifizierung erforderlich und werden verwaltet.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) kann Ihnen dabei helfen, die Prinzipien der geringsten Rechte und der Aufgabentrennung in Zugriffsberechtigungen und Autorisierungen zu integrieren und so zu verhindern, dass Richtlinien „Effect“: „Allow“ mit „Action“: „*“ anstelle von „Resource“: „*“ enthalten. Wenn Benutzern mehr Rechte eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und der Aufgabentrennung verstoßen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
D3.PC.Am.B.6	Für den Zugriff auf Systeme, Anwendungen und Hardware sind Identifikation und Authentifizierung erforderlich und werden verwaltet.	iam-user-no-policies-überprüfen	Diese Regel stellt sicher, dass AWS Identity and Access Management (IAM) -Richtlinien nur Gruppen oder Rollen zugewiesen werden, um den Zugriff auf Systeme und Ressourcen zu kontrollieren. Die Zuweisung von Berechtigungen auf Gruppen- oder Rollenebene trägt dazu bei, die Wahrscheinlichkeit zu verringern, dass eine Identität übermäßige Berechtigungen erhält oder beibehält.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
D3.PC.Am.B.6	Für den Zugriff auf Systeme, Anwendungen und Hardware sind Identifikation und Authentifizierung erforderlich und werden verwaltet.	iam-policy-no-statements-with-full-access	Stellen Sie sicher, dass IAM-Aktionen nur auf die benötigten Aktionen beschränkt sind. Wenn Benutzern mehr Rechte eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und der Aufgabentrennung verstoßen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
D3.PC.Am.B.7	Zu den Zugriffskontrollen gehören die konfigurierte Passwortkomplexität und Beschränkungen für Passworteingabeversuche und die Wiederverwendung von Passwörtern.	iam-password-policy	Die Identitäten und Anmeldeinformationen werden auf der Grundlage einer organisatorischen IAM-Passwortrichtlinie ausgestellt, verwaltet und verifiziert. Sie erfüllen oder übertreffen die Anforderungen von NIST SP 800-63 und dem Standard „Best Practices“ von AWS Foundational Security für die Passwortstärke. Mit dieser Regel können Sie optional RequireUppercaseCharacters (Wert für AWS grundlegende Sicherheitsbewährte Methoden: wahr), RequireLowercaseCharacters (Wert für bewährte Methoden für AWS grundlegende Sicherheit: wahr), RequireSymbols (Wert für bewährte Methoden für AWS grundlegende Sicherheit:

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			wahr), RequireNumbers (Wert für bewährte Methoden für AWS grundlegende Sicherheit: wahr), MinimumPasswordLength (Wert für bewährte Methoden für AWS grundlegende Sicherheit: 14), PasswordReusePrevention (Wert für bewährte Methoden für AWS grundlegende Sicherheit: 24) und MaxPasswordAge (Wert für bewährte Methoden für AWS grundlegende Sicherheit: 90) für Ihr IAM festlegen Kennwortrichtlinie. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
D3.PC.Am.B.8	Alle Standardp asswörter und nicht benötigten Standardk onten werden vor der Systemimplementier ung geändert.	iam-root-access-key-überprüfen	Der Zugriff auf Systeme und Ressourcen kann gesteuert werden, indem überprüft wird, ob der Root-Benu tzer keine Zugriffss chlüssel mit seiner AWS Identity and Access Management (IAM) -Rolle verknüpft hat. Stellen Sie sicher, dass die Root-Zugr iffsschlüssel gelöscht werden. Erstellen und verwenden Sie stattdessen rollenbas ierte Funktionen, AWS-Konten um das Prinzip der geringste n Funktionalität zu berücksichtigen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
D3.PC.Im.B.1	Es werden Tools zum Schutz vor Netzwerkperimetern (z. B. Grenzrouter und Firewall) verwendet.	acm-certificate-expiration-check	Stellen Sie sicher, dass die Netzwerkintegrität geschützt ist, indem Sie sicherstellen, dass X509-Zertifikate von AWS ACM ausgestellt werden. Diese Zertifikate müssen gültig und dürfen nicht abgelaufen sein. Für diese Regel ist ein Wert für erforderlich daysToExpiration (Wert für bewährte AWS Grundregeln für Sicherheit: 90). Der tatsächliche Wert muss den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
D3.PC.Im.B.1	Es werden Tools zum Schutz vor Netzwerkperimetern (z. B. Grenzrouter und Firewall) verwendet.	dms-replication-not-public	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass auf DMS-Replikationsin stanzen nicht öffentlic h zugegriffen werden kann. DMS-Repli kations-Instances können vertrauli che Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.
D3.PC.Im.B.1	Tools zum Schutz vor Netzwerkperimetern (z. B. Grenzrouter und Firewall) werden verwendet.	ebs-snapshot-public-restorable-überprüfen	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass EBS-Snapshots nicht öffentlich wiederher stellbar sind. EBS-Volume-Snapsho ts können vertrauli che Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
D3.PC.Im.B.1	Es werden Tools zum Schutz vor Netzwerkperimetern (z. B. Grenzrouter und Firewall) verwendet.	ec2- instance-no-public-ip	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon Elastic Compute Cloud (Amazon EC2) - Instances nicht öffentlich zugänglich sind. EC2 Amazon-Instances können vertrauliche Informationen enthalten, und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
D3.PC.Im.B.1	Es werden Tools zum Schutz vor Netzwerkperimetern (z. B. Grenzrouter und Firewall) verwendet.	elasticsearch-in-vpc-only	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass sich Amazon OpenSearch OpenSearch Service (Service) - Domains innerhalb einer Amazon Virtual Private Cloud (Amazon VPC) befinden. Eine OpenSearch Service-Domain innerhalb einer Amazon VPC ermöglicht die sichere Kommunikation zwischen OpenSearch Service und anderen Services innerhalb der Amazon VPC, ohne dass ein Internet-Gateway, ein NAT-Gerät oder eine VPN-Verbindung erforderlich ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
D3.PC.Im.B.1	Es werden Tools zum Schutz vor Netzwerkperimetern (z. B. Grenzrouter und Firewall) verwendet.	emr-master-no-public-ip	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon EMR-Cluster-Masterknoten nicht öffentlich zugänglich sind. Amazon-EMR-Cluster-Hauptknoten können vertrauliche Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
D3.PC.Im.B.1	Tools zum Schutz vor Netzwerkperimetern (z. B. Grenzrouter und Firewall) werden verwendet.	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) Security Groups können bei der Verwaltung des Netzwerkzugriffs helfen, indem sie eine statusbeh aftete Filterung von eingehendem und ausgehendem Netzwerkverkehr zu Ressourcen bereitste llen. AWS Wenn Sie eingehenden (oder entfernten) Datenverk ehr von 0.0.0.0/0 bis Port 22 auf Ihren Ressourcen nicht zulassen, können Sie den Remote-Zugriff einschränken.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
D3.PC.Im.B.1	Es werden Tools zum Schutz vor Netzwerkperimetern (z. B. Grenzrouter und Firewall) verwendet.	ec2- instances-in-vpc	Stellen Sie Amazon Elastic Compute Cloud (Amazon EC2) -Instances innerhalb einer Amazon Virtual Private Cloud (Amazon VPC) bereit, um eine sichere Kommunika tion zwischen einer Instance und anderen Services innerhalb der Amazon VPC zu ermöglichen, ohne dass ein Internet-Gateway, ein NAT-Gerät oder eine VPN-Verbindung erforderlich ist. Der gesamte Datenverk ehr bleibt sicher in der AWS Cloud. Domains, die sich innerhalb einer VPC befinden, verfügen aufgrund ihrer logischen Isolierun g im Vergleich zu Domains mit öffentlic hen Endpunkten über eine zusätzlic he Sicherheitsebene. Weisen Sie EC2

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			Amazon-Instances einer Amazon-VPC zu, um den Zugriff ordnungsgemäß zu verwalten.
D3.PC.Im.B.1	Es werden Tools zum Schutz vor Netzwerkperimetern (z. B. Grenzrouter und Firewall) verwendet.	lambda-function-public-access-verboten	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass AWS Lambda-Funktionen nicht öffentlich zugänglich sind. Der öffentliche Zugriff kann möglicherweise die Verfügbarkeit von Ressourcen beeinträchtigen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
D3.PC.Im.B.1	Es werden Tools zur Abwehr von Netzwerkperimetern (z. B. Grenzrouter und Firewall) verwendet.	lambda-inside-vpc	Stellen Sie AWS Lambda-Funktionen in einer Amazon Virtual Private Cloud (Amazon VPC) bereit, um eine sichere Kommunika tion zwischen einer Funktion und anderen Diensten innerhalb der Amazon VPC zu gewährleisten. Bei dieser Konfiguration sind kein Internet-Gateway, kein NAT-Gerät und keine VPN-Verbindung erforderlich. Der gesamte Datenverk ehr bleibt sicher in der Cloud. AWS Domains, die sich innerhalb einer VPC befinden, verfügen aufgrund ihrer logischen Isolierun g im Vergleich zu Domains mit öffentlic hen Endpunkten über eine zusätzliche Sicherheitsebene. Um den Zugriff ordnungsg emäß zu verwalten,

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			sollten AWS Lambda-Funktionen einer VPC zugewiesen werden.
D3.PC.Im.B.1	Es werden Tools zum Schutz vor Netzwerkperimetern (z. B. Grenzrouter und Firewall) verwendet.	rds-instance-public-access-überprüfen	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Relational Database Service (Amazon RDS) -Instances nicht öffentlich sind. Amazon-RDS-Datenbank-Instances können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
D3.PC.Im.B.1	Es werden Tools zum Schutz vor Netzwerkperimetern (z. B. Grenzrouter und Firewall) verwendet.	rds-snapshots-public-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Relational Database Service (Amazon RDS) -Instances nicht öffentlich sind. Amazon-RDS-Datenbank-Instances können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
D3.PC.Im.B.1	Es werden Tools zum Schutz vor Netzwerkperimetern (z. B. Grenzrouter und Firewall) verwendet.	redshift-cluster-public-access-überprüfen	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Redshift Redshift-Cluster nicht öffentlich sind. Amazon-Redshift-Cluster können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
D3.PC.Im.B.1	Tools zum Schutz vor Netzwerkperimetern (z. B. Grenzrouter und Firewall) werden verwendet.	restricted-common-ports	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass gemeinsame Ports für Amazon Elastic Compute Cloud (Amazon EC2) -Sicherheitsgruppen eingeschränkt sind. Wenn der Zugriff auf Ports nicht auf vertrauenswürdige Quellen beschränkt wird, kann dies zu Angriffen auf die Verfügbarkeit, Integrität und Vertraulichkeit von Systemen führen. Mit dieser Regel können Sie optional die Parameter blockedPort1–blockedPort5 festlegen (Standardkonfigurationen: 20, 21, 3389, 3306, 4333). Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
D3.PC.Im.B.1	Es werden Tools zur Abwehr von Netzwerkperimetern (z. B. Grenzrouter und Firewall) verwendet.	s-3 bucket-public-read-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie nur autorisierten Benutzern, Prozessen und Geräten Zugriff auf Amazon Simple Storage Service (Amazon S3) - Buckets gewähren. Die Verwaltung des Zugriffs sollte mit der Klassifizierung der Daten übereinst immen.
D3.PC.Im.B.1	Es werden Tools zum Schutz vor Netzwerkperimetern (z. B. Grenzrouter und Firewall) verwendet.	s-3 bucket-public-write-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie nur autorisierten Benutzern, Prozessen und Geräten Zugriff auf Amazon Simple Storage Service (Amazon S3) - Buckets gewähren. Die Verwaltung des Zugriffs sollte mit der Klassifizierung der Daten übereinst immen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
D3.PC.Im.B.1	Es werden Tools zum Schutz vor Netzwerkperimetern (z. B. Grenzrouter und Firewall) verwendet.	sagemaker-notebook-no-direct-Internetzugang	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass SageMaker Amazon-Notebooks keinen direkten Internetzugang zulassen. Indem Sie direkten Internetzugang blockieren, vermeiden Sie, dass unbefugte Benutzer auf sensible Daten zugreifen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
D3.PC.Im.B.1	Es werden Tools zum Schutz vor Netzwerkperimetern (z. B. Grenzrouter und Firewall) verwendet.	vpc-default-security-group-geschlossen	Sicherheitsgruppen von Amazon Elastic Compute Cloud (Amazon EC2) können bei der Verwaltung des Netzwerkzugriffs helfen, indem sie eine statusbehaftete Filterung des ein- und ausgehenden Netzwerkverkehrs zu Ressourcen bereitstellen. AWS Die Beschränk ung des gesamten Datenverkehrs auf die Standardsicherheit sgruppe hilft dabei, den Fernzugriff auf Ihre Ressourcen einzuschränken. AWS

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
D3.PC.Im.B.1	Es werden Tools zum Schutz vor Netzwerkperimetern (z. B. Grenzrouter und Firewall) verwendet.	alb-waf-enabled	Stellen Sie sicher, dass AWS WAF auf Elastic Load Balancers (ELB) aktiviert ist, um Webanwendungen zu schützen. Eine WAF trägt zum Schutz Ihrer Webanwend ungen oder APIs vor gängigen Web-Explo its bei. Diese Web-Exploits können sich auf die Verfügbar keit auswirken, die Sicherheit gefährden oder übermäßige Ressourcen in Ihrer Umgebung verbrauch en.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
D3.PC.Im.B.1	Es werden Tools zum Schutz vor Netzwerkperimetern (z. B. Grenzrouter und Firewall) verwendet.	vpc-sg-open-only-to-authorized-ports	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass gemeinsame Ports für Amazon Elastic Compute Cloud (Amazon EC2) -Sicherheitsgruppen eingeschränkt sind. Wenn der Zugriff auf Ports nicht auf vertrauenswürdige Quellen beschränkt wird, kann dies zu Angriffen auf die Verfügbarkeit, Integrität und Vertraulichkeit von Systemen führen. Durch die Beschränkung des Zugriffs auf Ressourcen innerhalb einer Sicherheitsgruppe aus dem Internet (0.0.0.0/0) kann der Remote-Zugriff auf interne Systeme gesteuert werden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
D3.PC.Im.B.1	Es werden Tools zur Abwehr von Netzwerkperimetern (z. B. Grenzrouter und Firewall) verwendet.	api-gw-associated-with-WAF	AWS Mit WAF können Sie eine Reihe von Regeln (als Web Access Control List (Web ACL) bezeichnet) konfigurieren, die Webanfragen auf der Grundlage von anpassbaren Websicherheitsregeln und -bedingungen, die Sie definieren, zulassen, blockieren oder zählen. Stellen Sie sicher, dass Ihre Amazon-API-Gateway-Stufe mit einer WAF-Web-ACL verknüpft ist, um sie vor böswilligen Angriffen zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
D3.PC.Im.B.1	Es werden Tools zum Schutz vor Netzwerkperimetern (z. B. Grenzrouter und Firewall) verwendet.	autoscaling-launch-config-public-ip-deaktiviert	Wenn Sie Ihre Netzwerkschnittstellen mit einer öffentlichen IP-Adresse konfigurieren, sind die diesen Netzwerkschnittstellen zugehörigen Ressourcen über das Internet erreichbar. EC2 Ressourcen sollten nicht öffentlich zugänglich sein, da dies einen unbeabsichtigten Zugriff auf Ihre Anwendungen oder Server ermöglichen kann.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
D3.PC.Im.B.1	Es werden Tools zum Schutz vor Netzwerkperimetern (z. B. Grenzrouter und Firewall) verwendet.	no-unrestricted-route-to-igw	Stellen Sie sicher, dass EC2 Amazon-Routentabellen keine uneingeschränkten Routen zu einem Internet-Gateway enthalten. Durch das Entfernen oder Beschränken des Internetzugangs für Workloads innerhalb von Amazon VPCs können unbeabsic htigte Zugriffe in Ihrer Umgebung reduziert werden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
D3.PC.Im.B.1	Es werden Tools zum Schutz vor Netzwerkperimetern (z. B. Grenzrouter und Firewall) verwendet.	s3- -Block-periodisch account-level-public-access	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Simple Storage Service (Amazon S3) -Buckets nicht öffentlich zugänglich sind. Diese Regel trägt dazu bei, sensible Daten vor unbefugten Remote-Benutzern zu schützen, indem sie den öffentlichen Zugriff verhindert. Mit dieser Regel können Sie optional die Parameter ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) und restrictPublicBuckets Parameter (Config Default: True) festlegen. Die tatsächlichen Werte müssen den Richtlini

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			en Ihrer Organisation entsprechen.
D3.PC.Im.B.1	Es werden Tools zum Schutz vor Netzwerkperimetern (z. B. Grenzrouter und Firewall) verwendet.	s3- verboten bucket-level-public-access	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Simple Storage Service (Amazon S3) -Buckets nicht öffentlich zugänglich sind. Diese Regel trägt dazu bei, sensible Daten vor unbefugten Remote-Benutzern zu schützen, indem sie den öffentlichen Zugriff auf Bucket-Ebene verhindert.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
D3.PC.Im.B.1	Es werden Tools zum Schutz vor Netzwerkperimetern (z. B. Grenzrouter und Firewall) verwendet.	ssm-document-not-public	Stellen Sie sicher, dass AWS Systems Manager (SSM) - Dokumente nicht öffentlich sind, da dies einen unbeabsichtigten Zugriff auf Ihre SSM-Dokumente ermöglichen kann. Ein öffentliches SSM-Dokument kann Informationen über Ihr Konto, Ihre Ressourcen und internen Prozesse preisgeben.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
D3.PC.Im.B.1	Es werden Tools zum Schutz vor Netzwerkperimetern (z. B. Grenzrouter und Firewall) verwendet.	opensearch-in-vpc-only	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass sich Amazon OpenSearch Service-Domains innerhalb einer Amazon Virtual Private Cloud (Amazon VPC) befinden. Eine Amazon OpenSearch Service-Domain innerhalb einer Amazon VPC ermöglicht die sichere Kommunikation zwischen Amazon OpenSearch Service und anderen Services innerhalb der Amazon VPC, ohne dass ein Internet-Gateway, ein NAT-Gerät oder eine VPN-Verbindung erforderlich ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
D3.PC.Im.B.1	Tools zum Schutz vor Netzwerkperimetern (z. B. Grenzrouter und Firewall) werden verwendet.	subnet-auto-assign-public-ip-deaktiviert	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon Virtual Private Cloud (VPC) -Subnetzen nicht automatisch eine öffentliche IP-Adresse zugewiesen wird. Amazon Elastic Compute Cloud (EC2) -Instances, die in Subnetzen gestartet werden, in denen dieses Attribut aktiviert ist, haben ihrer primären Netzwerkschnittstelle eine öffentliche IP-Adresse zugewiesen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
D3.PC.Im.B.1	Tools zum Schutz vor Netzwerkperimetern (z. B. Grenzrouter und Firewall) werden verwendet.	redshift-enhanced-vpc-routing-aktiviert	Mit Enhanced-VPC-Routing wird erzwungen, dass der gesamte COPY- und UNLOAD-Datenverkehr zwischen Ihrem Cluster und Datenrepositorys über Ihre Amazon VPC erfolgt. Anschließend können Sie VPC-Features wie Sicherheitsgruppen und Netzwerkzugriffskontrolllisten verwenden, um den Netzwerkverkehr zu schützen. Sie können auch VPC-Flow-Protokolle verwenden, um den Netzwerkverkehr zu überwachen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
D3.PC.IM.B.2	Systeme, auf die über das Internet oder durch externe Parteien zugegriff en wird, sind durch Firewalls oder ähnliche Geräte geschützt.	vpc-default-security-group-geschlossen	Sicherheitsgruppen von Amazon Elastic Compute Cloud (Amazon EC2) können bei der Verwaltung des Netzwerkzugriffs helfen, indem sie eine statusbehaftete Filterung des ein- und ausgehenden Netzwerkverkehrs zu Ressourcen bereitstellen. AWS Die Beschränk ung des gesamten Datenverkehrs auf die Standardsicherheit sgruppe hilft dabei, den Fernzugriff auf Ihre Ressourcen einzuschränken. AWS

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
D3.PC.IM.B.2	Systeme, auf die über das Internet oder durch externe Parteien zugegriff en wird, sind durch Firewalls oder ähnliche Geräte geschützt.	vpc-sg-open-only-to-authorized-ports	Verwalten Sie den Zugriff auf Ressource n in der AWS Cloud, indem Sie sicherste llen, dass gemeinsam e Ports für Amazon Elastic Compute Cloud (Amazon EC2) -Sicherhe itsgruppen eingeschr ränkt sind. Wenn der Zugriff auf Ports nicht auf vertrauen swürdige Quellen beschränkt wird, kann dies zu Angriffen auf die Verfügbar keit, Integrität und Vertraulichkeit von Systemen führen. Durch die Beschränk ung des Zugriffs auf Ressourcen innerhalb einer Sicherhei tsgruppe aus dem Internet (0.0.0.0/0) kann der Remote-Zugriff auf interne Systeme gesteuert werden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
D3.PC.IM.B.2	Systeme, auf die über das Internet oder durch externe Parteien zugegriff en wird, sind durch Firewalls oder ähnliche Geräte geschützt.	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) Security Groups können bei der Verwaltung des Netzwerkzugriffs helfen, indem sie eine statusbeh aftete Filterung von eingehendem und ausgehendem Netzwerkverkehr zu Ressourcen bereitste llen. AWS Wenn Sie eingehenden (oder entfernten) Datenverk ehr von 0.0.0.0/0 bis Port 22 auf Ihren Ressourcen nicht zulassen, können Sie den Remote-Zugriff einschränken.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
D3.PC.IM.B.2	Systeme, auf die über das Internet oder durch externe Parteien zugegriff en wird, sind durch Firewalls oder ähnliche Geräte geschützt.	restricted-common-ports	Verwalten Sie den Zugriff auf Ressource n in der AWS Cloud, indem Sie sicherste llen, dass gemeinsam e Ports für Amazon Elastic Compute Cloud (Amazon EC2) -Sicherhe itsgruppen eingeschr ränkt sind. Wenn der Zugriff auf Ports nicht auf vertrauen swürdige Quellen beschränkt wird, kann dies zu Angriffen auf die Verfügbar keit, Integrität und Vertraulichkeit von Systemen führen. Mit dieser Regel können Sie optional die Parameter blockedPo rt1–blockedPort5 festlegen (Standard konfigurationen: 20, 21, 3389, 3306, 4333). Die tatsächli chen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
D3.PC.IM.B.2	Systeme, auf die über das Internet oder durch externe Parteien zugegriff en wird, sind durch Firewalls oder ähnliche Geräte geschützt.	api-gw-associated-with-WAF	AWS Mit WAF können Sie eine Reihe von Regeln (als Web Access Control List (Web ACL) bezeichne t) konfigurieren, die Webanfragen auf der Grundlage von anpassbaren Websicherheitsrege ln und -bedingungen, die Sie definieren, zulassen, blockieren oder zählen. Stellen Sie sicher, dass Ihre Amazon-API-Gateway-Stufe mit einer WAF-Web-A CL verknüpft ist, um sie vor böswilligen Angriffen zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
D3.PC.IM.B.2	Systeme, auf die über das Internet oder durch externe Parteien zugegriff en wird, sind durch Firewalls oder ähnliche Geräte geschützt.	alb-waf-enabled	Stellen Sie sicher, dass AWS WAF auf Elastic Load Balancers (ELB) aktiviert ist, um Webanwendungen zu schützen. Eine WAF trägt zum Schutz Ihrer Webanwend ungen oder APIs vor gängigen Web-Explo its bei. Diese Web-Exploits können sich auf die Verfügbar keit auswirken, die Sicherheit gefährden oder übermäßige Ressourcen in Ihrer Umgebung verbrauch en.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
D3.PC.IM.B.3	Alle Ports werden überwacht.	cloudtrail-enabled	AWS CloudTrail kann bei der Nichtabstreitbarkeit helfen, indem Aktionen und API-Aufrufe der AWS Management Console aufgezeichnet werden. Sie können die Benutzer und die Benutzer AWS-Konten , die einen AWS Dienst aufgerufen haben, die Quell-IP-Adresse, über die die Aufrufe generiert wurden, und den Zeitpunkt der Anrufe identifizieren. Einzelheiten zu den erfassten Daten finden Sie in den AWS CloudTrail Datensatzinhalten.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
D3.PC.IM.B.3	Alle Ports werden überwacht.	cloud-trail-cloud-watch-logs-aktiviert	Verwenden Sie Amazon CloudWatch , um Protokoll ereignisaktivitäten zentral zu sammeln und zu verwalten. Die Aufnahme von AWS CloudTrail Daten liefert Einzelheiten zu den API-Aufrufaktivitäten in Ihrem AWS-Konto.
D3.PC.IM.B.3	Alle Ports werden überwacht.	api-gw-execution-logging-aktiviert	Die API-Gateway-Protokollierung zeigt detaillierte Ansichten der Benutzer, die auf die API zugegriffen haben, und wie diese Benutzer auf die API zugegriffen haben. Diese Einblicke ermöglichen die Transparenz von Benutzeraktivitäten.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
D3.PC.IM.B.3	Alle Ports werden überwacht.	wafv2-logging-enabled	Um die Protokollierung und Überwachung in Ihrer Umgebung zu erleichtern, aktivieren Sie die AWS WAF (V2) -Protokollierung im regionalen und globalen Web. ACLs AWS Die WAF-Protokollierung bietet detaillierte Informationen über den Datenverkehr, der von Ihrer Web-ACL analysiert wird. In den Protokollen werden die Uhrzeit aufgezeichnet, zu der die AWS WAF die Anfrage von Ihrer AWS Ressource erhalten hat, Informationen über die Anfrage und eine Aktion für die Regel, der jede Anfrage entsprach.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
D3.PC.IM.B.3	Alle Ports werden überwacht.	elb-logging-enabled	Die Elastic-Load-Balancing-Aktivität ist ein zentraler Kommunikationspunkt innerhalb einer Umgebung. Stellen Sie sicher, dass die ELB-Protokollierung aktiviert ist. Die gesammelten Daten enthalten detaillierte Informationen zu Anfragen, die an den ELB gesendet wurden. Jedes Protokoll enthält Informationen wie die Zeit, zu der die Anforderung einging, die Client-IP-Adresse, Latenzen, Anforderungspfade und Serverantworten.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
D3.PC.IM.B.3	Alle Ports werden überwacht.	vpc-flow-logs-enabled	VPC-Flow-Protokolle erfassen detaillierte Informationsdatensätze über den IP-Datenverkehr, der zu und von Netzwerkschnittstellen in Ihrer Amazon Virtual Private Cloud (Amazon VPC) fließt. Standardmäßig enthalten Flow-Protokolldatensätze Werte für die verschiedenen Komponenten des IP-Flows, einschließlich Quelle, Ziel und Protokoll.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
D3.PC.Im.B.5	Systemkonfigurationen (für Server, Desktops, Router usw.) entsprechen Branchenstandards und werden durchgesetzt.	ec2-check managedinstance-association-compliance-status	Verwenden Sie AWS Systems Manager Associations, um bei der Inventarisierung von Softwareplattformen und Anwendungen innerhalb eines Unternehmens zu helfen. AWS Systems Manager weist Ihren verwalteten Instanzen einen Konfigurationsstatus zu und ermöglicht es Ihnen, Basiswerte für Betriebssystem-Patch-Levels, Softwareinstallationen, Anwendungskonfigurationen und andere Details zu Ihrer Umgebung festzulegen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
D3.PC.Im.B.5	Systemkonfigurationen (für Server, Desktops, Router usw.) entsprechen Branchenstandards und werden durchgesetzt.	ec2-managed-instance-managed-by-systems	Eine Bestandsaufnahme der Softwareplattformen und Anwendungen innerhalb des Unternehmens ist möglich, indem Amazon Elastic Compute Cloud (Amazon EC2) - Instances mit AWS Systems Manager verwaltet werden. Verwenden Sie AWS Systems Manager, um detaillierte Systemkonfigurationen, Betriebssystem-Patch-Levels, Namen und Typ der Dienste, Softwareinstallationen, Anwendungsname, Herausgeber und Version sowie andere Details zu Ihrer Umgebung bereitzustellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
D3.PC.Im.B.5	Systemkonfigurationen (für Server, Desktops, Router usw.) entsprechen Branchenstandards und werden durchgesetzt.	ec2-check managedinstance-patch-compliance-status	Aktivieren Sie diese Regel, um bei der Identifizierung und Dokumentation von Sicherheitslücken in Amazon Elastic Compute Cloud (Amazon EC2) zu helfen. Die Regel prüft, ob die EC2 Amazon-Instance die Patch-Konformität im AWS Systems Manager gemäß den Richtlinien und Verfahren Ihrer Organisation einhält.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
D3.PC.IM.B.6	Ports, Funktionen, Protokolle und Services werden verboten, wenn sie nicht mehr für geschäftliche Zwecke benötigt werden.	vpc-sg-open-only-to-authorized-ports	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass gemeinsame Ports für Amazon Elastic Compute Cloud (Amazon EC2) -Sicherheitsgruppen eingeschränkt sind. Wenn der Zugriff auf Ports nicht auf vertrauenswürdige Quellen beschränkt wird, kann dies zu Angriffen auf die Verfügbarkeit, Integrität und Vertraulichkeit von Systemen führen. Durch die Beschränkung des Zugriffs auf Ressourcen innerhalb einer Sicherheitsgruppe aus dem Internet (0.0.0.0/0) kann der Remote-Zugriff auf interne Systeme gesteuert werden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
D3.PC.IM.B.6	Ports, Funktione n, Protokolle und Services werden verboten, wenn sie nicht mehr für geschäftliche Zwecke benötigt werden.	vpc-default-security-group-geschlossen	Sicherheitsgruppen von Amazon Elastic Compute Cloud (Amazon EC2) können bei der Verwaltung des Netzwerkzugriffs helfen, indem sie eine statusbehaftete Filterung des ein- und ausgehenden Netzwerkverkehrs zu Ressourcen bereitstellen. AWS Die Beschränk ung des gesamten Datenverkehrs auf die Standardsicherheit sgruppe hilft dabei, den Fernzugriff auf Ihre Ressourcen einzuschränken. AWS

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
D3.PC.IM.B.6	Ports, Funktione n, Protokolle und Services werden verboten, wenn sie nicht mehr für geschäftliche Zwecke benötigt werden.	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) Security Groups können bei der Verwaltung des Netzwerkzugriffs helfen, indem sie eine statusbeh aftete Filterung von eingehendem und ausgehendem Netzwerkverkehr zu Ressourcen bereitste llen. AWS Wenn Sie eingehenden (oder entfernten) Datenverk ehr von 0.0.0.0/0 bis Port 22 auf Ihren Ressourcen nicht zulassen, können Sie den Remote-Zugriff einschränken.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
D3.PC.IM.B.6	Ports, Funktionen, Protokolle und Services werden verboten, wenn sie nicht mehr für geschäftliche Zwecke benötigt werden.	restricted-common-ports	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass gemeinsame Ports für Amazon Elastic Compute Cloud (Amazon EC2) -Sicherheitsgruppen eingeschränkt sind. Wenn der Zugriff auf Ports nicht auf vertrauenswürdige Quellen beschränkt wird, kann dies zu Angriffen auf die Verfügbarkeit, Integrität und Vertraulichkeit von Systemen führen. Mit dieser Regel können Sie optional die Parameter blockedPort1–blockedPort5 festlegen (Standardkonfigurationen: 20, 21, 3389, 3306, 4333). Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
D3.PC.Im.B.7	Änderungen an Systemkonfigurationen (einschließlich virtueller Maschinen und Hypervisoren) werden kontrolliert und überwacht.	iam-user-group-membership-überprüfen	AWS Identity and Access Management (IAM) kann Ihnen helfen, Zugriffsberechtigungen und Autorisierungen einzuschränken, indem sichergestellt wird, dass Benutzer Mitglieder mindestens einer Gruppe sind. Wenn Benutzern mehr Berechtigungen eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und Aufgabentrennung verstoßen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
D3.PC.Im.B.7	Änderungen an Systemkonfigurationen (einschließlich virtueller Maschinen und Hypervisoren) werden kontrolliert und überwacht.	iam-user-no-policies-überprüfen	Diese Regel stellt sicher, dass AWS Identity and Access Management (IAM) -Richtlinien nur Gruppen oder Rollen zugewiesen werden, um den Zugriff auf Systeme und Ressourcen zu kontrollieren. Die Zuweisung von Berechtigungen auf Gruppen- oder Rollenebene trägt dazu bei, die Wahrscheinlichkeit zu verringern, dass eine Identität übermäßige Berechtigungen erhält oder beibehält.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
D3.PC.Im.B.7	Änderungen an Systemkonfigurationen (einschließlich virtueller Maschinen und Hypervisoren) werden kontrolliert und überwacht.	iam-no-inline-policy-überprüfen	Stellen Sie sicher, dass ein Benutzer, eine IAM-Rolle oder eine IAM-Gruppe (AWS Identity and Access Management) nicht über eine Inline-Richtlinie zur Zugriffskontrolle auf Systeme und Ressourcen verfügt. AWS empfiehlt, verwaltete Richtlinien anstelle von Inline-Richtlinien zu verwenden. Verwaltete Richtlinien ermöglichen Wiederverwendbarkeit, Versionsverwaltung, Rollback und Delegierung der Berechtigungsverwaltung.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
D3.PC.Im.B.7	Änderungen an Systemkonfigurationen (einschließlich virtueller Maschinen und Hypervisoren) werden kontrolliert und überwacht.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) kann Ihnen dabei helfen, die Prinzipien der geringsten Rechte und der Aufgabentrennung in Zugriffsberechtigungen und Autorisierungen zu integrieren und so zu verhindern, dass Richtlinien „Effect“: „Allow“ mit „Action“: „*“ anstelle von „Resource“: „*“ enthalten. Wenn Benutzern mehr Rechte eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und der Aufgabentrennung verstoßen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
D3.PC.Im.B.7	Änderungen an Systemkonfigurationen (einschließlich virtueller Maschinen und Hypervisoren) werden kontrolliert und überwacht.	cloudtrail-enabled	AWS CloudTrail kann durch die Aufzeichnung AWS von Aktionen und API-Aufrufen der Management Console bei der Nichtabstreitbarkeit helfen. Sie können die Benutzer und die Benutzer AWS-Konten , die einen AWS Dienst aufgerufen haben, die Quell-IP-Adresse, über die die Aufrufe generiert wurden, und den Zeitpunkt der Anrufe identifizieren. Einzelheiten zu den erfassten Daten finden Sie in den AWS CloudTrail Datensatzinhalten.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
D3.PC.Im.B.7	Änderungen an Systemkonfigurationen (einschließlich virtueller Maschinen und Hypervisoren) werden kontrolliert und überwacht.	cloud-trail-cloud-watch-logs-aktiviert	Verwenden Sie Amazon CloudWatch , um Protokoll ereignisaktivitäten zentral zu sammeln und zu verwalten. Die Aufnahme von AWS CloudTrail Daten liefert Einzelheiten zu den API-Aufrufaktivitäten in Ihrem AWS-Konto.
D3.PC.Im.B.7	Änderungen an Systemkonfigurationen (einschließlich virtueller Maschinen und Hypervisoren) werden kontrolliert und überwacht.	iam-policy-no-statements-with-full-access	Stellen Sie sicher, dass IAM-Aktionen nur auf die benötigten Aktionen beschränkt sind. Wenn Benutzern mehr Rechte eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und der Aufgabentrennung verstoßen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
D3.PC.Se.B.1	Für die Einrichtung tätige Entwickler befolgen im Rahmen eines Lebenszyklus der Systementwicklung (System Development Life Cycle; SDLC) sichere Programmierungsmethoden, die den Branchenstandards entsprechen.	codebuild-project-envvar-awscred-überprüfen	Stellen Sie sicher, dass die Anmeldeinformationen AWS_ACCESS_KEY_ID AWS_SECRET_ACCESS_KEY nicht in AWS Codebuild-Projektumgebungen vorhanden sind. Speichern Sie diese Variablen nicht als Klartext. Das Speichern dieser Variablen als Klartext bewirkt eine unbeabsichtigte Offenlegung von Daten sowie unberechtigte Zugriffe.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
D3.PC.Se.B.1	Für die Einrichtung tätige Entwickler befolgen im Rahmen eines Lebenszyklus der Systementwicklung (System Development Life Cycle; SDLC) sichere Programmierungsmethoden, die den Branchenstandards entsprechen.	codebuild-project-source-repo-URL-Prüfung	Stellen Sie sicher, dass die URL des Quell-Repositorys GitHub oder des Bitbucket-Quell-Repositorys keine persönlichen Zugriffstoken oder Anmeldeinformationen in Codebuild-Projektumgebungen enthält. AWS Verwende OAuth anstelle von persönlichen Zugriffstoken oder Anmeldedaten die Autorisierung für den Zugriff auf GitHub Bitbucket-Repositorys.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
D4.C.Co.B.2	Die Einrichtung stellt sicher, dass Verbindungen von Drittanbietern autorisiert werden.	vpc-sg-open-only-to-authorized-ports	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass gemeinsame Ports für Amazon Elastic Compute Cloud (Amazon EC2) -Sicherheitsgruppen eingeschränkt sind. Wenn der Zugriff auf Ports nicht auf vertrauenswürdige Quellen beschränkt wird, kann dies zu Angriffen auf die Verfügbarkeit, Integrität und Vertraulichkeit von Systemen führen. Durch die Beschränkung des Zugriffs auf Ressourcen innerhalb einer Sicherheitsgruppe aus dem Internet (0.0.0.0/0) kann der Remote-Zugriff auf interne Systeme gesteuert werden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
D4.C.Co.B.2	Die Einrichtung stellt sicher, dass Verbindungen von Drittanbietern autorisiert werden.	vpc-default-security-group-geschlossen	Sicherheitsgruppen von Amazon Elastic Compute Cloud (Amazon EC2) können bei der Verwaltung des Netzwerkzugriffs helfen, indem sie eine statusbehaftete Filterung des ein- und ausgehenden Netzwerkverkehrs zu Ressourcen bereitstellen. AWS Die Beschränk ung des gesamten Datenverkehrs auf die Standardsicherheit sgruppe hilft dabei, den Fernzugriff auf Ihre Ressourcen einzuschränken. AWS

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
D4.C.Co.B.2	Die Einrichtung stellt sicher, dass Verbindungen von Drittanbietern autorisiert werden.	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) Security Groups können bei der Verwaltung des Netzwerkzugriffs helfen, indem sie eine statusbeh aftete Filterung von eingehendem und ausgehendem Netzwerkverkehr zu Ressourcen bereitste llen. AWS Wenn Sie eingehenden (oder entfernten) Datenverk ehr von 0.0.0.0/0 bis Port 22 auf Ihren Ressourcen nicht zulassen, können Sie den Remote-Zugriff einschränken.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
D4.C.Co.B.2	Die Einrichtung stellt sicher, dass Verbindungen von Drittanbietern autorisiert werden.	restricted-common-ports	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass gemeinsame Ports für Amazon Elastic Compute Cloud (Amazon EC2) -Sicherheitsgruppen eingeschränkt sind. Wenn der Zugriff auf Ports nicht auf vertrauenswürdige Quellen beschränkt wird, kann dies zu Angriffen auf die Verfügbarkeit, Integrität und Vertraulichkeit von Systemen führen. Mit dieser Regel können Sie optional die Parameter blockedPort1–blockedPort5 festlegen (Standardkonfigurationen: 20, 21, 3389, 3306, 4333). Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
D5.DR.De.B.1	Für die Erkennung von Vorfällen im Bereich der Informationssicherheit werden Warnparameter mit Aufforderungen zu entsprechenden Abhilfemaßnahmen eingerichtet.	cloudwatch-alarm-action-check	Amazon CloudWatch alarmiert, wenn eine Metrik den Schwellenwert für eine bestimmte Anzahl von Bewertungszeiträumen überschreitet. Der Alarm führt eine oder mehrere Aktionen durch, die vom Wert der Metrik oder des Ausdrucks im Vergleich zu einem Schwellenwert in einer Reihe von Zeiträumen abhängt. Diese Regel erfordert einen Wert für alarmActionRequired (Config Default: True), insufficientDataAction Required (Config Default: True), okActionRequired (Config Default: False). Der tatsächliche Wert muss die Alarmaktionen für Ihre Umgebung widerspiegeln.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
D5.DR.De.B.1	Für die Erkennung von Vorfällen im Bereich der Informationssicherheit werden Warnparameter mit Aufforderungen zu entsprechenden Abhilfemaßnahmen eingerichtet.	securityhub-enabled	AWS Security Hub hilft bei der Überwachung von unbefugtem Personal, Verbindungen, Geräten und Software. AWS Security Hub aggregiert, organisiert und priorisiert die Sicherheitswarnungen oder Ergebnisse mehrerer Dienste. AWS Einige dieser Dienste sind Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer und AWS Firewall Manager sowie AWS Partnerlösungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
D5.DR.De.B.1	Für die Erkennung von Vorfällen im Bereich der Informati onssicherheit werden Warnparameter mit Aufforderungen zu entsprechenden Abhilfemaßnahmen eingerichtet.	guardduty-enabled-centralized	Amazon GuardDuty kann mithilfe von Threat Intellige nce Feeds helfen, potenzielle Cybersich erheitsereignisse zu überwachen und zu erkennen. Dazu gehören Listen mit bösartigen IPs und maschinel len Lernmethoden zur Identifizierung unerwarteter, nicht autorisierter und bösartiger Aktivitäten in Ihrer AWS Cloud-Umgebung.
D5.DR.De.B.2	Systemleistungsber ichte enthalten Informationen, die als Risikoindikator zur Erkennung von Vorfällen im Bereich der Informationssicher heit verwendet werden können.	lambda-dlq-check	Aktivieren Sie diese Regel, um das entsprechende Personal über Amazon Simple Queue Service (Amazon SQS) oder Amazon Simple Notification Service (Amazon SNS) zu benachrichtigen, wenn eine Funktion ausgefallen ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
D5.DR.De.B.2	Systemleistungsberichte enthalten Informationen, die als Risikoindikator zur Erkennung von Vorfällen im Bereich der Informationssicherheit verwendet werden können.	dynamodb-throughput-limit-check	Aktivieren Sie diese Regel, um sicherzustellen, dass die bereitgestellte Durchsatzkapazität in Ihren Amazon-DynamoDB-Tabellen überprüft wird. Dies ist der Umfang der Lese- und Schreibaktivitäten, der von den jeweiligen Tabellen unterstützt werden kann. DynamoDB verwendet diese Informationen für das Reservieren ausreichender Systemressourcen, um Ihren Durchsatz anforderungen gerecht zu werden. Diese Regel generiert eine Warnung, wenn sich der Durchsatz dem Höchstlimit für ein Kundenkonto nähert. Mit dieser Regel können Sie optional die Parameter RCUThreshold Kontoprozentsatz

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			(Konfigurationsstandard: 80) und WCUThreshold Kontoprozentsatz (Konfigurationsstandard: 80) festlegen. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
D5.DR.De.B.3	Es sind Tools und Prozesse vorhanden , um das Programm zur Reaktion aus Vorfälle zu erkennen, zu alarmieren und auszulösen.	cloudtrail-enabled	AWS CloudTrail kann bei der Nichtabst reitbarkeit helfen, indem Aktionen und API-Aufrufe der AWS Management Console aufgezeic hnet werden. Sie können die Benutzer und die Benutzer AWS-Konten , die einen AWS Dienst aufgerufen haben, die Quell-IP-Adresse, über die die Aufrufe generiert wurden, und den Zeitpunkt der Anrufe identifiz ieren. Einzelheiten zu den erfassten Daten finden Sie in den AWS CloudTrail Datensatzinhalten.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
D5.DR.De.B.3	Es sind Tools und Prozesse vorhanden , um das Programm zur Reaktion aus Vorfälle zu erkennen, zu alarmieren und auszulösen.	elb-logging-enabled	Die Elastic-Load-Balancing-Aktivität ist ein zentraler Kommunikationspunk t innerhalb einer Umgebung. Stellen Sie sicher, dass die ELB-Protokollierun g aktiviert ist. Die gesammelten Daten enthalten detaillie rte Informationen zu Anfragen, die an den ELB gesendet wurden. Jedes Protokoll enthält Informationen wie die Zeit, zu der die Anforderung einging, die Client-IP -Adresse, Latenzen, Anforderungspfade und Serverantworten.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
D5.DR.De.B.3	Es sind Tools und Prozesse vorhanden , um das Programm zur Reaktion aus Vorfälle zu erkennen, zu alarmieren und auszulösen.	cloudtrail-s3-data events-enabled	Die Erfassung von Simple Storage Service (Amazon S3)-Datenereignisse n unterstützt die Erkennung von ungewöhnlichen Aktivitäten. Zu den Details gehören AWS-Konto Informationen über den Zugriff auf einen Amazon S3 S3-Bucket, die IP-Adresse und die Uhrzeit des Ereignisses.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
D5.DR.De.B.3	Es sind Tools und Prozesse vorhanden , um das Programm zur Reaktion aus Vorfälle zu erkennen, zu alarmieren und auszulösen.	multi-region-cloudtrail-enabled	AWS CloudTrail zeichnet Aktionen und API-Aufrufe der AWS Management Console auf. Sie können feststellen, welche Benutzer und Konten angerufen wurden AWS, von welcher Quell-IP-Adresse aus die Anrufe getätigt wurden und wann die Anrufe erfolgten. CloudTrail übermittelt Protokolldateien aus allen AWS Regionen an Ihren S3-Bucket , wenn MULTI_REG ION_CLOUD _TRAIL_ENABLED aktiviert ist. Außerdem wird beim AWS Start einer neuen Region derselbe Trail in der neuen Region erstellt. CloudTrail Dadurch erhalten Sie automatis ch Protokolldateien mit API-Aktivitäten für die neue Region.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
D5.DR.De.B.3	Es sind Tools und Prozesse vorhanden , um das Programm zur Reaktion aus Vorfälle zu erkennen, zu alarmieren und auszulösen.	redshift-cluster-configuration-check	Um Daten im Ruhezustand zu schützen, muss die Verschlüsselung für Ihre Amazon-Redshift-Cluster aktiviert sein. Sie müssen auch sicherstellen, dass die erforderlichen Konfigurationen auf Amazon-Redshift-Clustern bereitgestellt werden. Die Prüfungsprotokollierung muss aktiviert sein, um Informationen zu Verbindungen und Benutzeraktivitäten in der Datenbank bereitzustellen. Diese Regel erfordert, dass ein Wert für clusterDbEncrypted (Config Default: TRUE) und LoggingEnabled (Config Default: TRUE) gesetzt ist. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
D5.DR.De.B.3	Es sind Tools und Prozesse vorhanden , um das Programm zur Reaktion aus Vorfälle zu erkennen, zu alarmieren und auszulösen.	s3- bucket-logging-enabled	Die Amazon Simple Storage Service (Amazon S3)-Serverzugriffs protokollierung bietet eine Methode zur Überwachu ng des Netzwerks im Hinblick auf potenzielle Cybersich erheitsereignisse. Die Ereignisse werden überwacht, indem detaillierte Aufzeichn ungen über die Anfragen erfasst werden, die an einen Amazon-S3-Bucket gestellt wurden. Jeder Zugriffsprotokolle intrag enthält Details zu einer einzelnen Zugriffsanfrage. Zu den Details gehören Anforderer, Bucket-Name, Anforderu ngszeit, Anforderu ngsaktion, Antwortst atus und Fehlercode, falls relevant.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
D5.DR.De.B.3	Es sind Tools und Prozesse vorhanden , um das Programm zur Reaktion aus Vorfälle zu erkennen, zu alarmieren und auszulösen.	rds-logging-enabled	Um die Protokoll ierung und Überwachung in Ihrer Umgebung zu erleichtern, stellen Sie sicher, dass die Amazon Relationa l Database Service (Amazon RDS)-Prot okollierung aktiviert ist. Mit der Amazon-RDS-Protokollierung können Sie Ereigniss e wie Verbindungen, Verbindungsabbrüch e, Abfragen oder abgefragte Tabellen erfassen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
D5.DR.De.B.3	Es sind Tools und Prozesse vorhanden, um das Programm zur Reaktion aus Vorfälle zu erkennen, zu alarmieren und auszulösen.	wafv2-logging-enabled	Um die Protokollierung und Überwachung in Ihrer Umgebung zu erleichtern, aktivieren Sie die AWS WAF (V2) -Protokollierung im regionalen und globalen Web ACLs. AWS Die WAF-Protokollierung bietet detaillierte Informationen über den Datenverkehr, der von Ihrer Web-ACL analysiert wird. In den Protokollen werden die Uhrzeit aufgezeichnet, zu der die AWS WAF die Anfrage von Ihrer AWS Ressource erhalten hat, Informationen über die Anfrage und eine Aktion für die Regel, der jede Anfrage entsprach.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
D5.DR.De.B.3	Es sind Tools und Prozesse vorhanden , um das Programm zur Reaktion aus Vorfälle zu erkennen, zu alarmieren und auszulösen.	cloud-trail-cloud-watch-logs-aktiviert	Verwenden Sie Amazon CloudWatch , um Protokoll ereignisaktivitäten zentral zu sammeln und zu verwalten. Die Aufnahme von AWS CloudTrail Daten liefert Einzelheiten zu den API-Aufrufaktivitäten in Ihrem AWS-Konto.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
D5.DR.De.B.3	Es sind Tools und Prozesse vorhanden , um das Programm zur Reaktion aus Vorfälle zu erkennen, zu alarmieren und auszulösen.	cloudwatch-alarm-action-check	Amazon CloudWatch alarmiert, wenn eine Metrik den Schwellen wert für eine bestimmte Anzahl von Bewertungszeiträum en überschreitet. Der Alarm führt eine oder mehrere Aktionen durch, die vom Wert der Metrik oder des Ausdrucks im Vergleich zu einem Schwellenwert in einer Reihe von Zeiträumen abhängt. Diese Regel erfordert einen Wert für alarmActionRequired (Config Default: True), insufficientDataAc tion Required (Config Default: True), okActionRequired (Config Default: False). Der tatsächli che Wert muss die Alarmaktionen für Ihre Umgebung widerspie geln.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
D5.DR.De.B.3	Es sind Tools und Prozesse vorhanden , um das Programm zur Reaktion aus Vorfälle zu erkennen, zu alarmieren und auszulösen.	guardduty-enabled-centralized	Amazon GuardDuty kann mithilfe von Threat Intellige nce Feeds helfen, potenzielle Cybersich erheitsereignisse zu überwachen und zu erkennen. Dazu gehören Listen mit bösartigen IPs und maschinel len Lernmethoden zur Identifizierung unerwarteter, nicht autorisierter und bösartiger Aktivitäten in Ihrer AWS Cloud-Umgebung.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
D5.DR.De.B.3	Es sind Tools und Prozesse vorhanden , um das Programm zur Reaktion aus Vorfälle zu erkennen, zu alarmieren und auszulösen.	securityhub-enabled	AWS Security Hub hilft bei der Überwachung von unbefugtem Personal, Verbindun gen, Geräten und Software. AWS Security Hub aggregiert, organisie rt und priorisie rt die Sicherhei tswarnungen oder Ergebnisse mehrerer Dienste. AWS Einige dieser Dienste sind Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer und AWS Firewall Manager sowie AWS Partnerlösungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
D5.ER.Es.B.4	Vorfälle werden klassifiziert, protokolliert und nachverfolgt.	guardduty-non-archived-findings	Amazon GuardDuty hilft Ihnen dabei, die Auswirkungen eines Vorfalls zu verstehen, indem es die Ergebnisse nach Schweregrad klassifiziert: niedrig, mittel und hoch. Diese Klassifizierungen können Sie zur Festlegung von entsprechenden Strategien und Prioritäten zur Behebung solcher Vorfälle verwenden. Mit dieser Regel können Sie optional daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7) und daysHighSev (Config Default: 1) für nicht archivierte Ergebnisse festlegen, wie es die Richtlinien Ihrer Organisation erfordern.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
D5.IR.PI.B.1	Die Einrichtung verfügt über einen dokumentierten Plan, wie sie auf Cybervorf älle reagieren wird.	response-plan-exists-maintained (Prozessü berprüfung)	Stellen Sie sicher, dass Vorfallre aktionspläne erstellt, verwaltet und an das verantwortliche Personal verteilt werden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
D5.IR.PI.B.6	Die Einrichtung plant, Programme für Geschäftskontinuität, Notfallwiederherstellung und Datensicherung einzusetzen, um den Betrieb nach einem Vorfall wiederherzustellen.	s-3 bucket-versioning-enabled	Die Versionsverwaltung von Amazon Simple Storage Service (Amazon S3)-Buckets hilft dabei, mehrere Varianten eines Objekts im selben Amazon-S3-Bucket zu speichern. Verwenden Sie die Versionsverwaltung, um sämtliche Versionen aller Objekte in Ihrem Amazon-S3-Bucket zu speichern, abzurufen oder wiederherzustellen. Mit der Versionsverwaltung können Sie Versionen sowohl nach unbeabsichtigten Benutzeraktionen als auch nach Anwendungsfehlern problemlos wiederherstellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
D5.IR.PI.B.6	Die Einrichtung plant, Programme für Geschäftskontinuität, Notfallwiederherstellung und Datensicherung einzusetzen, um den Betrieb nach einem Vorfall wiederherzustellen.	dynamodb-autoscaling-enabled	Amazon DynamoDB Auto Scaling verwendet den AWS Application Auto Scaling-Service, um die bereitgestellte Durchsatzkapazität so anzupassen, dass sie automatisch auf tatsächliche Verkehrsmuster reagiert. Auf diese Weise kann eine Tabelle oder ein globaler sekundärer Index die bereitgestellte Lese-/Schreibkapazität erhöhen, um plötzliche Erhöhungen des Datenverkehrs ohne Drosselung zu bewältigen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
D5.IR.PI.B.6	Die Einrichtung plant, Programme für Geschäftskontinuität, Notfallwiederherstellung und Datensicherung einzusetzen, um den Betrieb nach einem Vorfall wiederherzustellen.	dynamodb-pitr-enabled	Aktivieren Sie diese Regel, um zu überprüfen, ob die Informationen gesichert wurden. Es verwaltet auch die Backups, indem es sicherstellt, dass die point-in-time Wiederherstellung in Amazon DynamoDB aktiviert ist. Bei der Wiederherstellung werden fortlaufende Backups Ihrer Tabelle für die letzten 35 Tage gespeichert.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
D5.IR.PI.B.6	Die Einrichtung plant, Programme für Geschäftskontinuität, Notfallwiederherstellung und Datensicherung einzusetzen, um den Betrieb nach einem Vorfall wiederherzustellen.	vpc-vpn-2-tunnels-up	Redundante Site-to-Site VPN-Tunnel können implementiert werden, um die Anforderungen an die Ausfallsicherheit zu erfüllen. Es verwendet zwei Tunnel, um die Konnektivität sicherzustellen, falls eine der Site-to-Site VPN-Verbindungen nicht verfügbar ist. Um sich vor einem Verbindungsverlust zu schützen, können Sie für den Fall, dass Ihr Kunden-Gateway nicht verfügbar ist, eine zweite Site-to-Site VPN-Verbindung zu Ihrer Amazon Virtual Private Cloud (Amazon VPC) und Ihrem Virtual Private Gateway einrichten, indem Sie ein zweites Kunden-Gateway verwenden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
D5.IR.PI.B.6	Die Einrichtung plant, Programme für Geschäftskontinuität, Notfallwiederherstellung und Datensicherung einzusetzen, um den Betrieb nach einem Vorfall wiederherzustellen.	dynamodb-throughput-limit-check	Aktivieren Sie diese Regel, um sicherzustellen, dass die bereitgestellte Durchsatzkapazität in Ihren Amazon-DynamoDB-Tabellen überprüft wird. Dies ist der Umfang der Lese- und Schreibaktivitäten, der von den jeweiligen Tabellen unterstützt werden kann. DynamoDB verwendet diese Informationen für das Reservieren ausreichender Systemressourcen, um Ihren Durchsatzanforderungen gerecht zu werden. Diese Regel generiert eine Warnung, wenn sich der Durchsatz dem Höchstlimit für ein Kundenkonto nähert. Mit dieser Regel können Sie optional die Parameter RCUThreshold Kontoprozentsatz

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			(Konfigurationsstandard: 80) und WCUThreshold Kontoprozentsatz (Konfigurationsstandard: 80) festlegen. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
D5.IR.PI.B.6	Die Einrichtung plant, Programme für Geschäftskontinuität, Notfallwiederherstellung und Datensicherung einzusetzen, um den Betrieb nach einem Vorfall wiederherzustellen.	rds-enhanced-monitoring-enabled	Aktivieren Sie Amazon Relational Database Service (Amazon RDS), um die Verfügbarkeit von Amazon RDS zu überwachen. Dies bietet einen detaillierten Einblick in den Zustand Ihrer Amazon-RDS-Datenbank-Instances. Wenn der Amazon-RDS-Speicher mehr als ein zugrunde liegendes physisches Gerät verwendet, erfasst Enhanced Monitoring die Daten für jedes Gerät. Wenn die Amazon-RDS-Datenbank-Instance in einer Multi-AZ-Bereitstellung ausgeführt wird, werden außerdem die Daten für jedes Gerät auf dem sekundären Host sowie die Metriken des sekundären Hosts erfasst.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
D5.IR.PI.B.6	Die Einrichtung plant, Programme für Geschäftskontinuität, Notfallwiederherstellung und Datensicherung einzusetzen, um den Betrieb nach einem Vorfall wiederherzustellen.	elb-cross-zone-load-Balancing aktiviert	Aktivieren Sie zonenübergreifendes Load Balancing für Ihre Elastic Load Balancer (ELBs), um eine angemessene Kapazität und Verfügbarkeit aufrechtzuerhalten. Zonenübergreifendes Load Balancing reduziert die Notwendigkeit, die gleiche Anzahl von Instances in jeder aktivierten Availability Zone aufrechtzuerhalten. Es verbessert auch die Fähigkeit Ihrer Anwendung, den Verlust einer oder mehrerer Instances zu bewältigen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
D5.IR.PI.B.6	Die Einrichtung plant, Programme für Geschäftskontinuität, Notfallwiederherstellung und Datensicherung einzusetzen, um den Betrieb nach einem Vorfall wiederherzustellen.	rds-instance-deletion-protection-aktiviert	Stellen Sie sicher, dass Amazon Relational Database Service (Amazon RDS)-Instances den Löschschutz aktiviert haben. Verwenden Sie den Löschschutz, um zu verhindern, dass Ihre Amazon-RDS-Instances versehentlich oder böswillig gelöscht werden, was zum Verlust der Verfügbarkeit Ihrer Anwendungen führen kann.
D5.IR.PI.B.6	Die Einrichtung plant, Programme für Geschäftskontinuität, Notfallwiederherstellung und Datensicherung einzusetzen, um den Betrieb nach einem Vorfall wiederherzustellen.	elb-deletion-protection-enabled	Diese Regel sorgt dafür, dass der Löschschutz für Elastic Load Balancing aktiviert ist. Verwenden Sie diese Funktion, um zu verhindern, dass Ihr Load Balancer versehentlich oder böswillig gelöscht wird, was zum Verlust der Verfügbarkeit Ihrer Anwendungen führen kann.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
D5.IR.PI.B.6	Die Einrichtung plant, Programme für Geschäftskontinuität, Notfallwiederherstellung und Datensicherung einzusetzen, um den Betrieb nach einem Vorfall wiederherzustellen.	autoscaling-group-elb-healthcheck-erforderlich	Die Elastic Load Balancer (ELB) - Zustandsprüfungen für Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling Scaling-Gruppen unterstützen die Aufrechterhaltung einer angemessenen Kapazität und Verfügbarkeit. Der Load Balancer sendet regelmäßig Pings, versucht Verbindungen herzustellen oder sendet Anfragen, um den Zustand der EC2 Amazon-Instances in einer Gruppe mit auto-scaling zu testen. Wenn eine Instance nicht zurückmeldet, wird der Traffic an eine neue EC2 Amazon-Instance gesendet.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
D5.IR.PI.B.6	Die Einrichtung plant, Programme für Geschäftskontinuität, Notfallwiederherstellung und Datensicherung einzusetzen, um den Betrieb nach einem Vorfall wiederherzustellen.	s-3 bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) unterstützt die Aufrechterhaltung einer angemessenen Kapazität und Verfügbarkeit. CRR ermöglicht das automatische, asynchrone Kopieren von Objekten in Amazon-S3-Buckets, um die Datenverfügbarkeit sicherzustellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
D5.IR.PI.B.6	Die Einrichtung plant, Programme für Geschäftskontinuität, Notfallwiederherstellung und Datensicherung einzusetzen, um den Betrieb nach einem Vorfall wiederherzustellen.	rds-in-backup-plan	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon Relational Database Service (Amazon RDS) -Instances Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
D5.IR.PI.B.6	Die Einrichtung plant, Programme für Geschäftskontinuität, Notfallwiederherstellung und Datensicherung einzusetzen, um den Betrieb nach einem Vorfall wiederherzustellen.	efs-in-backup-plan	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon Elastic File System (Amazon EFS) -Dateisysteme Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
D5.IR.PI.B.6	Die Einrichtung plant, Programme für Geschäftskontinuität, Notfallwiederherstellung und Datensicherung einzusetzen, um den Betrieb nach einem Vorfall wiederherzustellen.	ebs-in-backup-plan	Stellen Sie zur Unterstützung der Datensicherungsprozesse sicher, dass Ihre Amazon Elastic Block Store (Amazon EBS) -Volumes Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
D5.IR.PI.B.6	Die Einrichtung plant, Programme für Geschäftskontinuität, Notfallwiederherstellung und Datensicherung einzusetzen, um den Betrieb nach einem Vorfall wiederherzustellen.	dynamodb-in-backup-plan	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon DynamoDB-Tabellen Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
D5.IR.PI.B.6	Die Einrichtung plant, Programme für Geschäftskontinuität, Notfallwiederherstellung und Datensicherung einzusetzen, um den Betrieb nach einem Vorfall wiederherzustellen.	elasticache-redis-cluster-automatic-Backup-Check	Wenn automatische Backups aktiviert sind, ElastiCache erstellt Amazon täglich ein Backup des Clusters. Die Sicherung kann für eine von Ihrer Organisation festgelegte Anzahl von Tagen aufbewahrt werden. Automatische Backups schützen vor Datenverlust. Bei einem Ausfall können Sie einen neuen Cluster erstellen, der Ihre Daten aus dem aktuellen Backup wiederherstellt.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
D5.IR.PI.B.6	Die Einrichtung plant, Programme für Geschäftskontinuität, Notfallwiederherstellung und Datensicherung einzusetzen, um den Betrieb nach einem Vorfall wiederherzustellen.	rds-multi-az-support	Die Multi-AZ-Unterstützung in Amazon Relational Database Service (Amazon RDS) bietet eine verbesserte Verfügbarkeit und Beständigkeit von Datenbank-Instances. Wenn Sie eine Multi-AZ-Datenbank-Instance bereitstellen, erstellt Amazon RDS automatisch eine primäre Datenbank-Instance und repliziert die Daten synchron auf eine Standby-Instance in einer anderen Availability Zone. Jede Availability Zone läuft auf einer eigenen, physisch getrennten, unabhängigen Infrastruktur und ist auf eine hohe Verfügbarkeit ausgelegt. Im Falle eines Infrastrukturausfalls führt Amazon RDS einen automatis

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			chen Failover zum Standby-Modus durch, sodass Sie den Datenbankbetrieb wieder aufnehmen können, sobald der Failover abgeschlo ssen ist.
D5.IR.PI.B.6	Die Einrichtung plant, Programme für Geschäftskontinuit ät, Notfallwiederherst ellung und Datensich erung einzusetz en, um den Betrieb nach einem Vorfall wiederherzustellen.	db-instance-backup-enabled	Die Sicherung sfunktion von Amazon RDS erstellt Sicherung en Ihrer Datenbank en und Transakti onsprotokolle. Amazon RDS erstellt einen Snapshot für das Speichervolume Ihrer DB-Instance, sodass die gesamte DB-Instance gesichert wird. Sie können im System spezifische Aufbewahrungsfrist en festlegen, um Ihre Ausfallsicherheits anforderungen zu erfüllen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
D5.IR.PI.B.6	Die Einrichtung plant, Programme für Geschäftskontinuität, Notfallwiederherstellung und Datensicherung einzusetzen, um den Betrieb nach einem Vorfall wiederherzustellen.	lambda-concurrency-check	Diese Regel stellt sicher, dass die Höchst- und Untergrenzen für die Gleichzeitigkeit einer Lambda-Funktion festgelegt werden. Dies kann Sie beim Baselining für die Anzahl der Anforderungen unterstützen, die Ihre Funktion zu einem bestimmten Zeitpunkt verarbeitet.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
D5.IR.PI.B.6	Die Einrichtung plant, Programme für Geschäftskontinuität, Notfallwiederherstellung und Datensicherung einzusetzen, um den Betrieb nach einem Vorfall wiederherzustellen.	aurora-resources-protected-by-Backup-Plan	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon Aurora Aurora-Ressourcen Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
D5.IR.PI.B.6	Die Einrichtung plant, Programme für Geschäftskontinuität, Notfallwiederherstellung und Datensicherung einzusetzen, um den Betrieb nach einem Vorfall wiederherzustellen.	backup-plan-min-frequency-and-min-retention-check	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihr AWS Backup-Plan auf eine Mindestfrequenz und Aufbewahrung festgelegt ist. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen. Mit dieser Regel können Sie die Parameter requiredFrequencyValue (Config default: 1), requiredRetentionDays (Config default: 35) und requiredFrequencyUnit

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			(Config default: days) festlegen. Der tatsächliche Wert muss den Anforderungen Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
D5.IR.PI.B.6	Die Einrichtung plant, Programme für Geschäftskontinuität, Notfallwiederherstellung und Datensicherung einzusetzen, um den Betrieb nach einem Vorfall wiederherzustellen.	backup-recovery-point-minimum-Aufbewahrungsprüfung	Um bei Datensicherungsprozessen zu helfen, stellen Sie sicher, dass für Ihre AWS Backup-Wiederherstellungspunkte eine Mindestaufbewahrungsdauer festgelegt ist. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen. Mit dieser Regel können Sie den Parameter requiredRetentionDays (Config Default: 35) festlegen. Der tatsächliche Wert muss den Anforderu

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			ngen Ihrer Organisation entsprechen.
D5.IR.Pl.B.6	Die Einrichtung plant, Programme für Geschäftskontinuität, Notfallwiederherstellung und Datensicherung einzusetzen, um den Betrieb nach einem Vorfall wiederherzustellen.	ec2--Plan resources-protected-by-backup	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon Elastic Compute Cloud (Amazon EC2) -Ressourcen Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Vorlage

Die Vorlage ist verfügbar unter GitHub: Operational Best Practices for FFIEC.

Bewährte Methoden für die Implementierung des deutschen Kriterienkatalogs C5 (Cloud Computing Compliance Criteria Catalogue)

Konformitätspakete bieten ein allgemeines Compliance-Framework, das es Ihnen ermöglicht, mithilfe verwalteter oder benutzerdefinierter AWS Config Regeln und Abhilfemaßnahmen Kontrollen zur Sicherheits-, Betriebs- oder Kostenoptimierung durchzuführen. AWS Config Conformance Packs dienen als Beispielvorlagen nicht dazu, die vollständige Einhaltung eines bestimmten Governance- oder Compliance-Standards sicherzustellen. Sie sind dafür verantwortlich, selbst zu beurteilen, ob Ihre Nutzung der Services den geltenden gesetzlichen und behördlichen Anforderungen entspricht.

Im Folgenden finden Sie ein Beispiel für eine Zuordnung zwischen dem Deutschland Cloud Computing Compliance Criteria Catalog (C5) und AWS Managed Config-Regeln. Jede Config-Regel gilt für eine bestimmte AWS Ressource und bezieht sich auf eine oder mehrere Deutschland C5-Steuerelemente. Eine Kontrolle nach des deutschen C5 kann mehreren Config-Regeln zugeordnet werden. In der folgenden Tabelle finden Sie weitere Informationen und Anleitungen zu diesen Zuordnungen.

Kontroll-ID	AWS Config	Empfehlungen
COS-01	alb-waf-enabled	Stellen Sie sicher, dass AWS WAF auf Elastic Load Balancers (ELB) aktiviert ist, um Webanwendungen zu schützen. Eine WAF trägt zum Schutz Ihrer Webanwend ungen oder APIs vor gängigen Web-Exploits bei. Diese Web-Exploits können sich auf die Verfügbarkeit auswirken, die Sicherheit gefährden oder übermäßige Ressourcen in Ihrer Umgebung verbrauchen.
COS-01	api-gw-associated-with-WAF	AWS Mit WAF können Sie eine Reihe von Regeln (als Web Access Control List (Web ACL) bezeichnet) konfiguri

Kontroll-ID	AWS Config	Empfehlungen
		eren, die Webanfragen auf der Grundlage von anpassbar en Websicherheitsregeln und -bedingungen, die Sie definieren, zulassen, blockiere n oder zählen. Stellen Sie sicher, dass Ihre Amazon-API-Gateway-Stufe mit einer WAF-Web-ACL verknüpft ist, um sie vor böswilligen Angriffen zu schützen.
COS-01	waf-regional-rule-not-leer	Stellen Sie sicher, dass Ihre AWS WAF eine Regel hat, die nicht leer ist. Eine Regel ohne Bedingungen kann zu unbeabsichtigtem Verhalten führen.
COS-01	waf-regional-rulegroup-not-leer	Stellen Sie sicher, dass Ihre AWS WAF eine Regelgrup pe hat, die nicht leer ist. Eine leere Regelgruppe kann zu unbeabsichtigtem Verhalten führen.

Kontroll-ID	AWS Config	Empfehlungen
COS-01	waf-regional-webacl-not-leer	Eine an eine AWS WAF angehängte Web-ACL kann eine Sammlung von Regeln und Regelgruppen zur Überprüfung und Steuerung von Webanfragen enthalten . Wenn eine Web-ACL leer ist, wird der Webdatenverkehr weitergeleitet, ohne von der WAF erkannt oder bearbeitet zu werden.
COS-01	guardduty-enabled-centralized	Amazon GuardDuty kann mithilfe von Threat Intellige nce Feeds helfen, potenzielle Cybersicherheitsereignisse zu überwachen und zu erkennen. Dazu gehören Listen mit bösartigen IPs und maschinel len Lernmethoden zur Identifiz ierung unerwarteter, nicht autorisierter und bösartige r Aktivitäten in Ihrer AWS Cloud-Umgebung.

Kontroll-ID	AWS Config	Empfehlungen
COS-03	alb-waf-enabled	Stellen Sie sicher, dass AWS WAF auf Elastic Load Balancers (ELB) aktiviert ist, um Webanwendungen zu schützen. Eine WAF trägt zum Schutz Ihrer Webanwend ungen oder APIs vor gängigen Web-Exploits bei. Diese Web-Exploits können sich auf die Verfügbarkeit auswirken, die Sicherheit gefährden oder übermäßige Ressourcen in Ihrer Umgebung verbrauchen.
COS-03	dms-replication-not-public	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass auf DMS-Replikationsinstanzen nicht öffentlich zugegriffen werden kann. DMS-Replikations-I nstances können vertrauli che Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.
COS-03	ebs-snapshot-public-restora ble-überprüfen	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass EBS-Snaps hots nicht öffentlich wiederher stellbar sind. EBS-Volume-Snapshots können vertrauli che Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	AWS Config	Empfehlungen
COS-03	ec-2 instance-no-public-ip	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon Elastic Compute Cloud (Amazon EC2) -Instances nicht öffentlich zugänglich sind. EC2 Amazon-Instances können vertrauliche Informati onen enthalten, und für solche Konten ist eine Zugriffsk ontrolle erforderlich.

Kontroll-ID	AWS Config	Empfehlungen
COS-03	ec2- instances-in-vpc	Stellen Sie Amazon Elastic Compute Cloud (Amazon EC2) -Instances innerhalb einer Amazon Virtual Private Cloud (Amazon VPC) bereit, um eine sichere Kommunika tion zwischen einer Instance und anderen Services innerhalb der Amazon VPC zu ermöglichen, ohne dass ein Internet-Gateway, ein NAT-Gerät oder eine VPN-Verbi ndung erforderlich ist. Der gesamte Datenverkehr bleibt sicher in der AWS Cloud. Domains, die sich innerhalb einer VPC befinden, verfügen aufgrund ihrer logischen Isolierung im Vergleich zu Domains mit öffentlic hen Endpunkten über eine zusätzliche Sicherheitsebene. Weisen Sie EC2 Amazon-In stances einer Amazon-VPC zu, um den Zugriff ordnungsg emäß zu verwalten.

Kontroll-ID	AWS Config	Empfehlungen
COS-03	elasticsearch-in-vpc-only	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass sich Amazon OpenSearch OpenSearch Service (Service) -Domains innerhalb einer Amazon Virtual Private Cloud (Amazon VPC) befinden. Eine OpenSearch Service-Domain innerhalb einer Amazon VPC ermöglicht die sichere Kommunikation zwischen OpenSearch Service und anderen Services innerhalb der Amazon VPC, ohne dass ein Internet-Gateway, ein NAT-Gerät oder eine VPN-Verbindung erforderlich ist.

Kontroll-ID	AWS Config	Empfehlungen
COS-03	opensearch-in-vpc-only	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass sich Amazon OpenSearch Service-Domains innerhalb einer Amazon Virtual Private Cloud (Amazon VPC) befinden. Eine Amazon OpenSearch Service-Domain innerhalb einer Amazon VPC ermöglich t die sichere Kommunika tion zwischen Amazon OpenSearch Service und anderen Services innerhalb der Amazon VPC, ohne dass ein Internet-Gateway, ein NAT-Gerät oder eine VPN-Verbindung erforderlich ist.
COS-03	emr-master-no-public-ip	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon EMR-Cluster-Masterknoten nicht öffentlich zugänglich sind. Amazon-EMR-Cluster-Hauptknoten können vertrauli che Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	AWS Config	Empfehlungen
COS-03	internet-gateway-authorized-vpc-nur	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Internet-Gateways nur mit autorisierter Amazon Virtual Private Cloud (Amazon VPC) verbunden sind. Internet-Gateways ermöglichen den bidirekti onalen Internetzugang zur und von der Amazon VPC, was möglicherweise zu einem unbefugten Zugriff auf Amazon-VPC-Ressourcen führen kann.
COS-03	lambda-function-public-acce ss-verboten	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherste llen, dass AWS Lambda-Funktionen nicht öffentlich zugänglich sind. Der öffentlic he Zugriff kann möglicher weise die Verfügbarkeit von Ressourcen beeinträchtigen.

Kontroll-ID	AWS Config	Empfehlungen
COS-03	lambda-inside-vpc	Stellen Sie AWS Lambda-Funktionen in einer Amazon Virtual Private Cloud (Amazon VPC) bereit, um eine sichere Kommunikation zwischen einer Funktion und anderen Diensten innerhalb der Amazon VPC zu gewährleisten. Bei dieser Konfiguration sind kein Internet-Gateway, kein NAT-Gerät und keine VPN-Verbindung erforderlich. Der gesamte Datenverkehr bleibt sicher in der Cloud. AWS Domains, die sich innerhalb einer VPC befinden, verfügen aufgrund ihrer logischen Isolierung im Vergleich zu Domains mit öffentlichen Endpunkten über eine zusätzliche Sicherheitsebene. Um den Zugriff ordnungsgemäß zu verwalten, sollten AWS Lambda-Funktionen einer VPC zugewiesen werden.

Kontroll-ID	AWS Config	Empfehlungen
COS-03	rds-instance-public-access-überprüfen	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Relational Database Service (Amazon RDS) -Instances nicht öffentlich sind. Amazon-RDS-Datenbank-Instances können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.
COS-03	rds-snapshots-public-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Relational Database Service (Amazon RDS) -Instances nicht öffentlich sind. Amazon-RDS-Datenbank-Instances können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	AWS Config	Empfehlungen
COS-03	redshift-cluster-public-access-überprüfen	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Redshift Redshift-Cluster nicht öffentlich sind. Amazon-Redshift-Cluster können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.
COS-03	restricted-common-ports	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass gemeinsame Ports für Amazon Elastic Compute Cloud (Amazon EC2) - Sicherheitsgruppen eingeschränkt sind. Wenn der Zugriff auf Ports nicht auf vertrauenswürdige Quellen beschränkt wird, kann dies zu Angriffen auf die Verfügbarkeit, Integrität und Vertraulichkeit von Systemen führen. Mit dieser Regel können Sie optional die Parameter blockedPort1–blockedPort5 festlegen (Standardkonfigurationen: 20, 21, 3389, 3306, 4333). Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	AWS Config	Empfehlungen
COS-03	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) Security Groups können bei der Verwaltung des Netzwerkz ugriffs helfen, indem sie eine statusbehaftete Filterung von eingehendem und ausgehend em Netzwerkverkehr zu Ressourcen bereitstellen. AWS Wenn Sie eingehenden (oder entfernten) Datenverk ehr von 0.0.0.0/0 bis Port 22 auf Ihren Ressourcen nicht zulassen, können Sie den Remote-Zugriff einschränken.

Kontroll-ID	AWS Config	Empfehlungen
COS-03	s3-Blöcke, periodisch account-level-public-access	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Simple Storage Service (Amazon S3) -Buckets nicht öffentlich zugänglich sind. Diese Regel trägt dazu bei, sensible Daten vor unbefugten Remote-Benutzern zu schützen, indem sie den öffentlichen Zugriff verhindert. Mit dieser Regel können Sie optional die Parameter ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) und restrictPublicBuckets Parameter (Config Default: True) festlegen. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	AWS Config	Empfehlungen
COS-03	sagemaker-notebook-no-direct-Internetzugang	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass SageMaker Amazon-Notebooks keinen direkten Internetzugang zulassen. Indem Sie direkten Internetzugang blockieren, vermeiden Sie, dass unbefugte Benutzer auf sensible Daten zugreifen.
COS-03	vpc-default-security-group-geschlossen	Sicherheitsgruppen von Amazon Elastic Compute Cloud (Amazon EC2) können bei der Verwaltung des Netzwerkzugriffs helfen, indem sie eine statusbehaftete Filterung des ein- und ausgehenden Netzwerkverkehrs zu Ressourcen bereitstellen. AWS Die Beschränkung des gesamten Datenverkehrs auf die Standardsicherheitsgruppe hilft dabei, den Fernzugriff auf Ihre Ressourcen einzuschränken. AWS

Kontroll-ID	AWS Config	Empfehlungen
COS-03	vpc-sg-open-only-to-authorized-ports	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass gemeinsame Ports für Amazon Elastic Compute Cloud (Amazon EC2) - Sicherheitsgruppen eingeschränkt sind. Wenn der Zugriff auf Ports nicht auf vertrauenswürdige Quellen beschränkt wird, kann dies zu Angriffen auf die Verfügbarkeit, Integrität und Vertraulichkeit von Systemen führen. Durch die Beschränkung des Zugriffs auf Ressourcen innerhalb einer Sicherheitsgruppe aus dem Internet (0.0.0.0/0) kann der Remote-Zugriff auf interne Systeme gesteuert werden.
COS-03	alb-http-drop-invalid-Header-fähig	Stellen Sie sicher, dass Ihre Elastic Load Balancers (ELB) so konfiguriert sind, dass sie HTTP-Header löschen. Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	AWS Config	Empfehlungen
COS-05	iam-user-mfa-enabled	Aktivieren Sie diese Regel, um den Zugriff auf Ressource n in der Cloud einzuschr änken. AWS Diese Regel sorgt dafür, dass die Multi-Fak tor-Authentifizierung (MFA) für alle Benutzer aktiviert ist. MFA sorgt für eine weitere Schutzebene zusätzlich zu den Anmeldeinformationen. Reduzieren Sie Fälle von kompromittierten Konten, indem Sie MFA für Benutzer vorschreiben.
COS-05	mfa-enabled-for-iam-Konsole nzugriff	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherste llen, dass MFA für alle AWS Identity and Access Management (IAM) -Benutzer aktiviert ist, die über ein Konsolenkennwort verfügen. MFA sorgt für eine weitere Schutzebene zusätzlich zu den Anmeldeinformationen. Indem Sie MFA für Benutzer vorschreiben, können Sie Fälle kompromittierter Konten reduzieren und verhindern, dass unbefugte Benutzer auf vertrauliche Daten zugreifen.

Kontroll-ID	AWS Config	Empfehlungen
COS-05	root-account-hardware-mfa-aktiviert	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Hardware-MFA für den Root-Benutzer aktiviert ist. Der Stammbenutzer ist der AWS-Konto-Benutzer mit den meisten Berechtigungen. MFA sorgt für eine weitere Schutzebene zusätzlich zu den Anmeldeinformationen. Indem Sie MFA für den Root-Benutzer vorschreiben, können Sie die Anzahl AWS-Konten kompromittierter Benutzer reduzieren.
COS-05	root-account-mfa-enabled	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass MFA für den Root-Benutzer aktiviert ist. Der Stammbenutzer ist der AWS-Konto-Benutzer mit den meisten Berechtigungen. MFA sorgt für eine weitere Schutzebene zusätzlich zu den Anmeldeinformationen. Indem Sie MFA für den Root-Benutzer vorschreiben, können Sie die Anzahl AWS-Konten kompromittierter Benutzer reduzieren.

Kontroll-ID	AWS Config	Empfehlungen
COS-05	ec-2 instance-no-public-ip	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon Elastic Compute Cloud (Amazon EC2) -Instances nicht öffentlich zugänglich sind. EC2 Amazon-Instances können vertrauliche Informati onen enthalten, und für solche Konten ist eine Zugriffsk ontrolle erforderlich.
COS-05	emr-master-no-public-ip	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon EMR-Cluster-Masterknoten nicht öffentlich zugänglich sind. Amazon-EMR-Cluster-Hauptknoten können vertrauli che Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.
COS-05	rds-instance-public-access-überprüfen	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherste llen, dass Amazon Relationa l Database Service (Amazon RDS) -Instances nicht öffentlic h sind. Amazon-RDS-Datenba nk-Instances können vertrauli che Informationen enthalten und für solche Konten sind Prinzipien und Zugriffsk ontrollen erforderlich.

Kontroll-ID	AWS Config	Empfehlungen
COS-05	rds-snapshots-public-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Relational Database Service (Amazon RDS) -Instances nicht öffentlich sind. Amazon-RDS-Datenbank-Instances können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.
COS-05	redshift-cluster-public-access-überprüfen	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Redshift Redshift-Cluster nicht öffentlich sind. Amazon-Redshift-Cluster können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	AWS Config	Empfehlungen
COS-05	restricted-common-ports	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass gemeinsame Ports für Amazon Elastic Compute Cloud (Amazon EC2) - Sicherheitsgruppen eingeschränkt sind. Wenn der Zugriff auf Ports nicht auf vertrauenswürdige Quellen beschränkt wird, kann dies zu Angriffen auf die Verfügbarkeit, Integrität und Vertraulichkeit von Systemen führen. Mit dieser Regel können Sie optional die Parameter blockedPort1–blockedPort5 festlegen (Standardkonfigurationen: 20, 21, 3389, 3306, 4333). Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	AWS Config	Empfehlungen
COS-05	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) Security Groups können bei der Verwaltung des Netzwerkz ugriffs helfen, indem sie eine statusbehaftete Filterung von eingehendem und ausgehend em Netzwerkverkehr zu Ressourcen bereitstellen. AWS Wenn Sie eingehenden (oder entfernten) Datenverk ehr von 0.0.0.0/0 bis Port 22 auf Ihren Ressourcen nicht zulassen, können Sie den Remote-Zugriff einschränken.
COS-05	vpc-default-security-group-geschlossen	Sicherheitsgruppen von Amazon Elastic Compute Cloud (Amazon EC2) können bei der Verwaltung des Netzwerkzugriffs helfen, indem sie eine statusbeh aftete Filterung des ein- und ausgehenden Netzwerkv erkehrs zu Ressourcen bereitstellen. AWS Die Beschränkung des gesamten Datenverkehrs auf die Standardsicherheitsgruppe hilft dabei, den Fernzugriff auf Ihre Ressourcen einzuschr änken. AWS

Kontroll-ID	AWS Config	Empfehlungen
COS-05	vpc-sg-open-only-to-authorized-ports	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass gemeinsame Ports für Amazon Elastic Compute Cloud (Amazon EC2) - Sicherheitsgruppen eingeschränkt sind. Wenn der Zugriff auf Ports nicht auf vertrauenswürdige Quellen beschränkt wird, kann dies zu Angriffen auf die Verfügbarkeit, Integrität und Vertraulichkeit von Systemen führen. Durch die Beschränkung des Zugriffs auf Ressourcen innerhalb einer Sicherheitsgruppe aus dem Internet (0.0.0.0/0) kann der Remote-Zugriff auf interne Systeme gesteuert werden.
CRY-02	alb-http-to-https-Umleitungsprüfung	Um Daten während der Übertragung zu schützen, stellen Sie sicher, dass Ihr Application Load Balancer unverschlüsselte HTTP-Anfragen automatisch an HTTPS umleitet. Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	AWS Config	Empfehlungen
CRY-02	api-gw-ssl-enabled	Stellen Sie sicher, dass die REST-API-Stufen von Amazon API Gateway mit SSL-Zertifikaten konfiguriert sind, damit Backend-Systeme überprüfen können, ob Anforderungen von API Gateway stammen.

Kontroll-ID	AWS Config	Empfehlungen
CRY-02	elb-predefined-security-policy-ssl-Prüfung	Stellen Sie sicher, dass Ihre SSL-Listener von Classic Elastic Load Balancing eine vordefinierte Sicherheitsrichtlinie verwenden, um Daten während der Übertragung zu schützen. Elastic Load Balancing bietet vordefinierte Aushandlungskonfigurationen, die für die SSL-Aushandlung verwendet werden, wenn eine Verbindung zwischen einem Client und Ihrem Load Balancer hergestellt wurde. Die SSL-Aushandlungskonfigurationen sind mit einer breiten Palette von Clients kompatibel und verwenden hochfeste kryptografische Algorithmen. Diese Regel verlangt, dass Sie eine vordefinierte Sicherheitsrichtlinie für Ihre SSL-Listener festlegen. Die Standard-Sicherheitsrichtlinie lautet: Policy-TLS-1-2-2017-0. ELBSecurity Der tatsächliche Wert muss den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	AWS Config	Empfehlungen
CRY-02	opensearch-https-required	Da sensible Daten existiere n können und um Daten während der Übertragung zu schützen, sollten Sie sicherstellen, dass HTTPS für Verbindungen zu Ihren Amazon OpenSearch Service-Domains aktiviert ist.
CRY-02	elasticsearch-node-to-node-Verschlüsselungsprüfung	Stellen Sie sicher, dass die node-to-node Verschlüsselung für Amazon OpenSearch Service aktiviert ist. Node-to-nodeVerschlüsselung ermöglicht die TLS 1.2-Versc hlüsselung für die gesamte Kommunikation innerhalb der Amazon Virtual Private Cloud (Amazon VPC). Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.
CRY-02	elb-tls-https-listeners-nur	Stellen Sie sicher, dass Ihre Elastic Load Balancer (ELBs) mit SSL- oder HTTPS-Lis tenern konfiguriert sind. Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	AWS Config	Empfehlungen
CRY-02	redshift-require-tls-ssl	Stellen Sie sicher, dass Ihre Amazon-Redshift-Cluster eine TLS/SSL-Verschlüsselung erfordern, um eine Verbindun g zu SQL-Clients herzustel len. Um eventuell vorhanden e sensible Daten zu schützen, sollten Sie die Verschlüs selung bei der Übertragung aktivieren.
CRY-02	s-3 bucket-ssl-requests-only	Um Daten während der Übertragung zu schützen, stellen Sie sicher, dass Ihre Amazon Simple Storage Service (Amazon S3)-Bucke ts Anfragen zur Verwendun g von Secure Socket Layer (SSL)-Buckets erfordern. Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	AWS Config	Empfehlungen
CRY-02	opensearch-node-to-node-Verschlüsselungsprüfung	Stellen Sie sicher, dass die node-to-node Verschlüsselung für Amazon OpenSearch Service aktiviert ist. Node-to-nodeVerschlüsselung ermöglicht die TLS 1.2-Verschlüsselung für die gesamte Kommunikation innerhalb der Amazon Virtual Private Cloud (Amazon VPC). Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.
CRY-03	api-gw-cache-enabled-und verschlüsselt	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass die Verschlüsselung für den Cache Ihrer API-Gateway-Stufe aktiviert ist. Da für die API-Methode sensible Daten erfasst werden können, sollten Sie die Verschlüsselung von Daten im Ruhezustand aktivieren, um diese Daten zu schützen.
CRY-03	cloud-trail-encryption-enabled	Da sensible Daten vorhanden sein können und um Daten im Ruhezustand zu schützen, sollten Sie sicherstellen, dass die Verschlüsselung für Ihre AWS CloudTrail Trails aktiviert ist.

Kontroll-ID	AWS Config	Empfehlungen
CRY-03	cloudwatch-log-group-encrypted	Um sensible Daten im Speicher zu schützen, stellen Sie sicher, dass die Verschlüsselung für Ihre Amazon CloudWatch Log Groups aktiviert ist.
CRY-03	kinesis-stream-encrypted	Aktivieren Sie die Verschlüsselung für Ihre Amazon-Kinesis-Streams, um eventuell vorhandene sensible Daten sowie Daten im Ruhezustand zu schützen.
CRY-03	secretsmanager-using-cmk	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass die Verschlüsselung mit dem AWS Key Management Service (AWS KMS) für AWS Secrets Manager aktiviert ist. Aktivieren Sie die Verschlüsselung von Daten im Ruhezustand, um eventuell vorhandene sensible Daten im Ruhezustand im Secrets Manager zu schützen.

Kontroll-ID	AWS Config	Empfehlungen
CRY-03	dynamodb-table-encrypted-kms	Stellen Sie sicher, dass die Verschlüsselung für Ihre Amazon-DynamoDB-Tabellen aktiviert ist. Um eventuell vorhandene sensible Daten im Ruhezustand in diesen Tabellen zu schützen, müssen Sie die Verschlüsselung von Daten im Ruhezustand aktivieren. Standardmäßig werden DynamoDB-Tabellen mit einem AWS eigenen Kundenhauptschlüssel (CMK) verschlüsselt.
CRY-03	ebs-snapshot-public-restorable-überprüfen	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass EBS-Snapshots nicht öffentlich wiederherstellbar sind. EBS-Volume-Snapshots können vertrauliche Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	AWS Config	Empfehlungen
CRY-03	ec-2 ebs-encryption-by-default	Zum Schutz von Daten im Ruhezustand müssen Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon Elastic Block Store (Amazon EBS)-Volumes aktiviert ist. Da sensible Daten auch im Ruhezusta nd vorhanden sein können, sollten Sie die Verschlüs selung im Ruhezustand aktivieren, um diese Daten zu schützen.
CRY-03	efs-encrypted-check	Aktivieren Sie die Verschlüs selung für Ihr Amazon Elastic File System (EFS), um eventuell vorhandene sensible Daten sowie Daten im Ruhezustand zu schützen.
CRY-03	elasticsearch-encrypted-at-rest	Da sensible Daten vorhanden sein können und um Daten im Ruhezustand zu schützen, sollten Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon OpenSearch Service (OpenSearch Service) -Domains aktiviert ist.

Kontroll-ID	AWS Config	Empfehlungen
CRY-03	opensearch-encrypted-at-rest	Da sensible Daten vorhanden sein können und um Daten im Ruhezustand zu schützen, sollten Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon OpenSearch Service-Domains aktiviert ist.
CRY-03	encrypted-volumes	Aktivieren Sie die Verschlüs selung für Ihre Amazon-El astic-Block-Store (Amazon-EBS)-Volumes, um eventuell vorhandene sensible Daten sowie Daten im Ruhezustand zu schützen.
CRY-03	rds-snapshot-encrypted	Stellen Sie sicher, dass die Verschlüsselung für Ihre Amazon Relational Database Service (Amazon RDS)-Snap shots aktiviert ist. Da sensible Daten auch im Ruhezusta nd vorhanden sein können, sollten Sie die Verschlüs selung im Ruhezustand aktivieren, um diese Daten zu schützen.
CRY-03	codebuild-project-artifact-encryption	Um sensible Daten im Speicher zu schützen, stellen Sie sicher, dass die Verschlüsselung für Ihre AWS CodeBuild Artefakte aktiviert ist.

Kontroll-ID	AWS Config	Empfehlungen
CRY-03	rds-storage-encrypted	Zum Schutz von Daten im Ruhezustand müssen Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon Relational Database Service (Amazon RDS)-Instances aktiviert ist. Um eventuell vorhandene sensible Daten im Ruhezustand in Amazon-RDS-Instanc es zu schützen, muss die Verschlüsselung von Daten im Ruhezustand aktiviert sein.

Kontroll-ID	AWS Config	Empfehlungen
CRY-03	redshift-cluster-configuration-check	Um Daten im Ruhezustand zu schützen, muss die Verschlüsselung für Ihre Amazon-Redshift-Cluster aktiviert sein. Sie müssen auch sicherstellen, dass die erforderlichen Konfigurationen auf Amazon-Redshift-Clustern bereitgestellt werden. Die Prüfungsprotokollierung muss aktiviert sein, um Informationen zu Verbindungen und Benutzeraktivitäten in der Datenbank bereitzustellen. Diese Regel erfordert, dass ein Wert für clusterDbEncrypted (Config Default: TRUE) und LoggingEnabled (Config Default: TRUE) gesetzt ist. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.
CRY-03	s3- default-encryption-kms	Stellen Sie sicher, dass die Verschlüsselung für Ihre Amazon Simple Storage Service (Amazon S3)-Buckets aktiviert ist. Um eventuell vorhandene sensible Daten im Ruhezustand in einem Amazon-S3-Bucket zu schützen, muss die Verschlüsselung aktiviert sein.

Kontroll-ID	AWS Config	Empfehlungen
CRY-03	sagemaker-endpoint-configuration-kms-key-konfiguriert	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass die Verschlüsselung mit dem AWS Key Management Service (AWS KMS) für Ihren Endpunkt aktiviert ist. SageMaker Da sensible Daten auf dem SageMaker Endgerät gespeichert werden können, sollten Sie die Verschlüsselung im Ruhezustand aktivieren, um diese Daten zu schützen.
CRY-03	sagemaker-notebook-instance-kms-schlüsselkonfiguriert	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass die Verschlüsselung mit dem AWS Key Management Service (AWS KMS) für Ihr Notebook aktiviert ist. SageMaker Da vertrauliche Daten im SageMaker Notebook gespeichert werden können, sollten Sie die Verschlüsselung im Ruhezustand aktivieren, um diese Daten zu schützen.

Kontroll-ID	AWS Config	Empfehlungen
CRY-03	sns-encrypted-kms	Um Daten im Ruhezusta nd zu schützen, stellen Sie sicher, dass Ihre Amazon Simple Notification Service (Amazon SNS) -Themen mit dem AWS Key Management Service (AWS KMS) verschlüs selt werden müssen. Um eventuell vorhandene sensible Daten im Ruhezustand in veröffentlichten Nachricht en zu schützen, muss die Verschlüsselung von Daten im Ruhezustand aktiviert sein.
CRY-04	cmk-backing-key-rotation-ak tiviert	Aktivieren Sie die Schlüssel rotation, um sicherzustellen, dass Schlüssel rotiert werden, nachdem sie das Ende ihrer Krypto-Periode erreicht haben.
DEV-07	cloud-trail-cloud-watch-logs- aktiviert	Verwenden Sie Amazon CloudWatch , um Protokoll ereignisaktivitäten zentral zu sammeln und zu verwalten . Die Aufnahme von AWS CloudTrail Daten liefert Einzelheiten zu den API-Aufru faktivitäten in Ihrem AWS-Konto.

Kontroll-ID	AWS Config	Empfehlungen
DEV-07	codebuild-project-logging-enabled	Stellen Sie sicher, dass die AWS CodeBuild Projektprotokollierung aktiviert ist, damit Ihre Build-Ausgabeprotokolle entweder an Amazon CloudWatch oder Amazon Simple Storage Service (Amazon S3) gesendet werden. Build-Ausgabeprotokolle enthalten detaillierte Informationen zu Ihrem Build-Projekt.
DEV-07	s3- bucket-logging-enabled	Die Amazon Simple Storage Service (Amazon S3)-Serverzugriffsprotokollierung bietet eine Methode zur Überwachung des Netzwerks im Hinblick auf potenzielle Cybersicherheitsereignisse. Die Ereignisse werden überwacht, indem detaillierte Aufzeichnungen über die Anfragen erfasst werden, die an einen Amazon-S3-Bucket gestellt wurden. Jeder Zugriffsprotokolleintrag enthält Details zu einer einzelnen Zugriffsanfrage. Zu den Details gehören Anforderer, Bucket-Name, Anforderungszeit, Anforderungsaktion, Antwortstatus und Fehlercode, falls relevant.

Kontroll-ID	AWS Config	Empfehlungen
DEV-07	cloudtrail-enabled	AWS CloudTrail kann durch die Aufzeichnung von Aktionen und API-Aufrufen in der AWS Management Console bei der Nichtabst reitbarkeit helfen. Sie können die Benutzer und die Benutzer AWS-Konten , die einen AWS Dienst aufgerufen haben, die Quell-IP-Adresse, über die die Aufrufe generiert wurden, und den Zeitpunkt der Anrufe identifizieren. Einzelheiten zu den erfassten Daten finden Sie in den AWS CloudTrail Datensatzinhalten.
DEV-07	cloudtrail-s3-dataevents-en abled	Die Erfassung von Simple Storage Service (Amazon S3)-Datenereignissen unterstützt die Erkennung von ungewöhnl ichen Aktivitäten. Zu den Details gehören AWS-Konto Informationen über den Zugriff auf einen Amazon S3 S3-Bucket, die IP-Adresse und die Uhrzeit des Ereignisses.

Kontroll-ID	AWS Config	Empfehlungen
DEV-07	multi-region-cloudtrail-enabled	AWS CloudTrail zeichnet Aktionen und API-Aufrufe der AWS Management Console auf. Sie können feststellen, welche Benutzer und Konten angerufen wurden AWS, von welcher Quell-IP-Adresse aus die Anrufe getätigt wurden und wann die Anrufe erfolgten . CloudTrail übermittelt Protokolldateien aus allen AWS Regionen an Ihren S3-Bucket, wenn MULTI_REG ION_CLOUD_TRAIL_EN ABLED aktiviert ist. Außerdem wird beim AWS Start einer neuen Region derselbe Trail in der neuen Region erstellt. CloudTrail Dadurch erhalten Sie automatisch Protokoll dateien mit API-Aktivitäten für die neue Region.

Kontroll-ID	AWS Config	Empfehlungen
IDM-01	access-keys-rotated	Die Anmeldeinformationen für autorisierte Geräte, Benutzer und Prozesse werden geprüft, indem sichergestellt wird, dass die IAM-Zugriffsschlüssel entsprechend den Vorgaben der Unternehmensrichtlinie rotiert werden. Das regelmäßi ge Ändern der Zugriffss chlüssel ist eine bewährte Sicherheitsmethode. Es verkürzt den Zeitraum, in dem ein Zugriffsschlüssel aktiv ist, und reduziert die Auswirkun gen auf das Unternehmen, wenn die Schlüssel kompromit tiert werden. Diese Regel erfordert einen Wert für die Zugriffsschlüssel-Rotation (Standardkonfiguration: 90). Der tatsächliche Wert muss den Richtlinien Ihrer Organisat ion entsprechen.

Kontroll-ID	AWS Config	Empfehlungen
IDM-01	emr-kerberos-enabled	Die Zugriffsberechtigungen und -autorisierungen können verwaltet und nach den Prinzipien der geringsten Berechtigung und Aufgabent rennung integriert werden, indem Kerberos für Amazon-EMR-Cluster aktiviert wird. In Kerberos werden Services und Benutzer, die sich authentifizieren müssen, als Prinzipale bezeichnet. Prinzipale befinden sich in einem Kerberos-Bereich. Innerhalb dieses Bereichs wird ein Kerberos-Server als Key Distribution Center (KDC) bezeichnet. Über diesen Server können sich Prinzipale authentifizieren. Die Authentifizierung im KDC erfolgt durch die Ausstellu ng von Authentifizierungs tickets. Das KDC unterhält eine Datenbank der Prinzipal e in seinem Bereich mit ihren Passwörtern und anderen administrativen Informationen zu jedem Prinzipal.

Kontroll-ID	AWS Config	Empfehlungen
IDM-01	iam-password-policy	Die Identitäten und Anmeldein formationen werden auf der Grundlage einer organisat orischen IAM-Passwortrichtl inie ausgestellt, verwaltet und verifiziert. Sie erfüllen oder übertreffen die Anforderu ngen von NIST SP 800-63 und dem Standard „Best Practices“ von AWS Foundatio nal Security in Bezug auf die Passwortstärke. Mit dieser Regel können Sie optional RequireUppercaseCharacters (Wert für AWS grundlege nde Sicherheitsbewährte Methoden: wahr), RequireLo wercaseCharacters (Wert für bewährte Methoden für AWS grundlegende Sicherheit: wahr), RequireSymbols (Wert für bewährte Methoden für AWS grundlegende Sicherhei t: wahr), RequireNumbers (Wert für bewährte Methoden für AWS grundlegende Sicherheit: wahr), MinimumPa sswordLength (Wert für bewährte Methoden für AWS grundlegende Sicherheit: 14), PasswordReusePreve ntion (Wert für bewährte Methoden für AWS grundlege nde Sicherheit: 24) und

Kontroll-ID	AWS Config	Empfehlungen
		MaxPasswordAge (Wert für bewährte Methoden für AWS grundlegende Sicherhei t: 90) für Ihr IAM festlegen Kennwortrichtlinie. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisat ion entsprechen.
IDM-01	iam-root-access-key-überprü fen	Der Zugriff auf Systeme und Ressourcen kann gesteuert werden, indem überprüft wird, ob der Root-Benutzer keine Zugriffsschlüssel mit seiner AWS Identity and Access Management (IAM) -Rolle verknüpft hat. Stellen Sie sicher, dass die Root-Zugr iffsschlüssel gelöscht werden. Erstellen und verwenden Sie stattdessen rollenbasierte Funktionen, AWS-Konten um das Prinzip der geringsten Funktionalität zu berücksic htigen.

Kontroll-ID	AWS Config	Empfehlungen
IDM-01	iam-user-group-membership-überprüfen	AWS Identity and Access Management (IAM) kann Ihnen helfen, Zugriffsberechtigungen und Autorisierungen einzuschränken, indem sichergestellt wird, dass Benutzer Mitglieder mindestens einer Gruppe sind. Wenn Benutzern mehr Berechtigungen eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und Aufgabentrennung verstoßen.
IDM-01	iam-user-mfa-enabled	Aktivieren Sie diese Regel, um den Zugriff auf Ressourcen in der AWS Cloud einzuschränken. Diese Regel sorgt dafür, dass die Multi-Faktor-Authentifizierung (MFA) für alle Benutzer aktiviert ist. MFA sorgt für eine weitere Schutzebene zusätzlich zu den Anmeldeinformationen. Reduzieren Sie Fälle von kompromittierten Konten, indem Sie MFA für Benutzer vorschreiben.

Kontroll-ID	AWS Config	Empfehlungen
IDM-01	iam-user-unused-credentials-überprüfen	AWS Identity and Access Management (IAM) kann Ihnen bei Zugriffsberechtigungen und Autorisierungen helfen, indem es nach IAM-Passwörtern und Zugriffsschlüsseln sucht, die für einen bestimmten Zeitraum nicht verwendet wurden. Wenn ungenutzte Anmeldeinformationen identifiziert werden, müssen Sie sie deaktivieren und/oder entfernen, da dies gegen das Prinzip der geringsten Berechtigung verstoßen könnte. Für diese Regel müssen Sie einen Wert für das maxCredentialUsage Alter festlegen (Standardkonfiguration: 90). Der tatsächliche Wert muss den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	AWS Config	Empfehlungen
IDM-01	mfa-enabled-for-iam-Konsolenzugriff	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass MFA für alle AWS Identity and Access Management (IAM) -Benutzer aktiviert ist, die über ein Konsolenkennwort verfügen. MFA sorgt für eine weitere Schutzebene zusätzlich zu den Anmeldeinformationen. Indem Sie MFA für Benutzer vorschreiben, können Sie Fälle kompromittierter Konten reduzieren und verhindern, dass unbefugte Benutzer auf vertrauliche Daten zugreifen.
IDM-01	root-account-hardware-mfa-aktiviert	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Hardware-MFA für den Root-Benutzer aktiviert ist. Der Stammbenutzer ist der AWS-Konto-Benutzer mit den meisten Berechtigungen. MFA sorgt für eine weitere Schutzebene zusätzlich zu den Anmeldeinformationen. Indem Sie MFA für den Root-Benutzer vorschreiben, können Sie die Anzahl AWS-Konten kompromittierter Benutzer reduzieren.

Kontroll-ID	AWS Config	Empfehlungen
IDM-01	root-account-mfa-enabled	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass MFA für den Root-Benutzer aktiviert ist. Der Stammbenutzer ist der AWS-Konto-Benutzer mit den meisten Berechtigungen. MFA sorgt für eine weitere Schutzebene zusätzlich zu den Anmeldeinformationen. Indem Sie MFA für den Root-Benutzer vorschreiben, können Sie die Anzahl AWS-Konten kompromittierter Benutzer reduzieren.
IDM-01	secretsmanager-rotation-enabled-check	Diese Regel stellt sicher, dass bei AWS Secrets Manager Manager-Geheimnissen die Rotation aktiviert ist. Die regelmäßige Rotation von Secrets kann den Zeitraum verkürzen, in dem ein Secret aktiv ist, und möglicherweise die Auswirkungen auf das Unternehmen verringern, falls das Secret kompromittiert wird.

Kontroll-ID	AWS Config	Empfehlungen
IDM-01	secretsmanager-scheduled-rotation-success-überprüfen	Diese Regel stellt sicher, dass AWS Secrets Manager Manager-Geheimnisse gemäß dem Rotationsplan erfolgreich rotiert wurden. Die regelmäßige Rotation von Secrets kann den Zeitraum verkürzen, in dem ein Secret aktiv ist, und möglicherweise die Auswirkungen auf das Unternehmen verringern, falls es kompromittiert wird.
IDM-01	iam-group-has-users-überprüfen	AWS Identity and Access Management (IAM) kann Ihnen helfen, die Prinzipien der geringsten Rechte und der Aufgabentrennung mit Zugriffsberechtigungen und Autorisierungen zu integrieren, indem sichergestellt wird, dass IAM-Gruppen mindestens einen Benutzer haben. Die Einteilung von Benutzern in Gruppen auf der Grundlage der ihnen zugewiesenen Berechtigungen oder ihrer Funktion ist eine Möglichkeit, das Prinzip der geringsten Berechtigung zu implementieren.

Kontroll-ID	AWS Config	Empfehlungen
IDM-01	iam-user-no-policies-überprüfen	Diese Regel stellt sicher, dass AWS Identity and Access Management (IAM) -Richtlinien nur Gruppen oder Rollen zugewiesen werden, um den Zugriff auf Systeme und Ressourcen zu kontrollieren. Die Zuweisung von Berechtigungen auf Gruppen- oder Rollenebene trägt dazu bei, die Wahrscheinlichkeit zu verringern, dass eine Identität übermäßige Berechtigungen erhält oder beibehält.
IDM-01	codebuild-project-envvar-awscred-überprüfen	Stellen Sie sicher, dass die Anmeldeinformationen AWS_ACCESS_KEY_ID AWS_SECRET_ACCESS_KEY nicht in AWS Codebuild -Projektumgebungen vorhanden sind. Speichern Sie diese Variablen nicht als Klartext. Das Speichern dieser Variablen als Klartext bewirkt eine unbeabsichtigte Offenlegung von Daten sowie unberechtigte Zugriffe.

Kontroll-ID	AWS Config	Empfehlungen
IDM-01	ecs-containers-nonprivileged	Um die Implementierung des Prinzips der geringsten Berechtigung zu unterstützen, dürfen in Amazon Elastic Container Service (Amazon ECS)-Aufgabendefinitionen keine erhöhten Berechtigungen aktiviert sein. Wenn dieser Parameter den Wert „true“ aufweist, erhält der Container erhöhte Berechtigungen auf der Host-Container-Instance (ähnlich wie der Root-Benutzer).
IDM-01	ecs-containers-readonly-access	Die Aktivierung des schreibgeschützten Zugriffs auf Amazon Elastic Container Service (ECS)-Container kann dazu beitragen, das Prinzip der geringsten Berechtigung einzuhalten. Diese Option kann Angriffsvektoren reduzieren, da das Dateisystem der Container-Instance nur geändert werden kann, wenn es über ausdrückliche Lese- und Schreibberechtigungen verfügt.

Kontroll-ID	AWS Config	Empfehlungen
IDM-01	ecs-task-definition-user-for-host-mode-check	Wenn für eine Aufgabend efinition erhöhte Berechtig ungen gelten, liegt das daran, dass der Kunde diesen Konfigurationen ausdrücklich zugestimmt hat. Diese Kontrolle prüft, ob eine unerwartete Berechtig ungseskalation vorliegt, wenn für eine Aufgabendefinition das Host-Netzwerk aktiviert ist, die Kunden aber keine erhöhten Berechtigungen aktiviert haben.
IDM-01	efs-access-point-enforce-Stammverzeichnis	Die Durchsetzung eines Stammverzeichnisses für einen Amazon-Elastic-File-System (Amazon-EFS)-Zugan gspunkt trägt dazu bei, den Datenzugriff einzuschränken, indem sichergestellt wird, dass Benutzer des Zugangspu nkts nur auf Dateien des angegebenen Unterverz eichnisses zugreifen können.

Kontroll-ID	AWS Config	Empfehlungen
IDM-01	efs-access-point-enforce-Benutzeridentität	Um die Implementierung des Prinzips der geringsten Rechte zu unterstützen, stellen Sie sicher, dass die Benutzerdurchsetzung für Ihr Amazon Elastic File System (Amazon EFS) aktiviert ist. Wenn diese Option aktiviert ist, ersetzt Amazon EFS den Benutzer und die Gruppe IDs des NFS-Clients durch die Identität, die auf dem Access Point für alle Dateisystemoperationen konfiguriert ist, und gewährt nur Zugriff auf diese erzwungene Benutzeridentität.
IDM-01	iam-policy-no-statements-with-full-access	Stellen Sie sicher, dass IAM-Aktionen nur auf die benötigten Aktionen beschränkt sind. Wenn Benutzern mehr Rechte eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und der Aufgabentrennung verstoßen.

Kontroll-ID	AWS Config	Empfehlungen
IDM-01	opensearch-access-control-enabled	Stellen Sie sicher, dass eine differenzierte Zugriffskontrolle für Ihre Amazon OpenSearch Service-Domains aktiviert ist. Eine differenzierte Zugriffskontrolle bietet erweiterte Autorisierungsmechanismen, um den Zugriff auf Amazon Service-Domains mit den geringsten Rechten zu erreichen. OpenSearch Es ermöglicht eine rollenbasierte Zugriffskontrolle auf die Domain sowie Sicherheit auf Index-, Dokument- und Feldebene, Unterstützung für OpenSearch Service-Dashboards, Mehrmandantenfähigkeit und HTTP-Basisauthentifizierung für Service und Kibana. OpenSearch

Kontroll-ID	AWS Config	Empfehlungen
IDM-01	rds-instance-iam-authentication-aktiviert	Stellen Sie sicher, dass eine AWS Identity and Access Management (IAM) -Authentifizierung auf Amazon Relational Database Service (Amazon RDS) -Instances aktiviert ist, um den Zugriff auf Systeme und Ressourcen zu kontrollieren. Dadurch wird die Verschlüsselung von ausgehendem und eingehendem Netzwerkverkehr von und zur Datenbank anhand von Secure Sockets Layer (SSL) durchgesetzt. Da die Authentifizierung extern verwaltet wird, ist es nicht erforderlich, Benutzeranmeldeinformationen in der Datenbank zu speichern.

Kontroll-ID	AWS Config	Empfehlungen
IDM-01	s-3 bucket-acl-prohibited	Diese Regel prüft, ob Access Control Lists (ACLs) für die Zugriffskontrolle auf Amazon S3 S3-Buckets verwendet werden. ACLs sind veraltete Zugriffskontrollmechanismen für Amazon S3 S3-Buckets, die älter sind als AWS Identity and Access Management (IAM). Stattdessen empfiehlt es sich ACLs, IAM-Richtlinien oder S3-Bucket-Richtlinien zu verwenden, um den Zugriff auf Ihre S3-Buckets einfacher zu verwalten.

Kontroll-ID	AWS Config	Empfehlungen
IDM-03	iam-user-unused-credentials-überprüfen	AWS Identity and Access Management (IAM) kann Ihnen bei Zugriffsberechtigungen und Autorisierungen helfen, indem es nach IAM-Passwörtern und Zugriffsschlüsseln sucht, die für einen bestimmten Zeitraum nicht verwendet wurden. Wenn ungenutzte Anmeldeinformationen identifiziert werden, müssen Sie sie deaktivieren und/oder entfernen, da dies gegen das Prinzip der geringsten Berechtigung verstoßen könnte. Für diese Regel müssen Sie einen Wert für das maxCredentialUsage Alter festlegen (Standardkonfiguration: 90). Der tatsächliche Wert muss den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	AWS Config	Empfehlungen
IDM-03	secretsmanager-secret-unused	Wenn in AWS Secrets Manager unbenutzte Anmeldeinformationen vorhanden sind, sollten Sie die Anmeldeinformationen deaktivieren und/oder entfernen, da dies gegen das Prinzip der geringsten Rechte verstoßen kann. Mit dieser Regel können Sie einen Wert auf unusedForDays (Config Default: 90) setzen. Der tatsächliche Wert muss den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	AWS Config	Empfehlungen
IDM-08	iam-password-policy	Die Identitäten und Anmeldein formationen werden auf der Grundlage einer organisat orischen IAM-Passwortrichtl inie ausgestellt, verwaltet und verifiziert. Sie erfüllen oder übertreffen die Anforderungen von NIST SP 800-63 und dem Standard „Best Practices“ von AWS Foundational Security für die Passwortstärke. Mit dieser Regel können Sie optional RequireUppercaseCharacters (Wert für AWS grundlege nde Sicherheitsbewährte Methoden: wahr), RequireLo wercaseCharacters (Wert für bewährte Methoden für AWS grundlegende Sicherheit: wahr), RequireSymbols (Wert für bewährte Methoden für AWS grundlegende Sicherhei t: wahr), RequireNumbers (Wert für bewährte Methoden für AWS grundlegende Sicherheit: wahr), MinimumPa sswordLength (Wert für bewährte Methoden für AWS grundlegende Sicherheit: 14), PasswordReusePreve ntion (Wert für bewährte Methoden für AWS grundlege nde Sicherheit: 24) und MaxPasswordAge (Wert

Kontroll-ID	AWS Config	Empfehlungen
		für bewährte Methoden für AWS grundlegende Sicherheit: 90) für Ihr IAM festlegen Kennwortrichtlinie. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	AWS Config	Empfehlungen
CRY-01	iam-password-policy	Die Identitäten und Anmeldein formationen werden auf der Grundlage einer organisat orischen IAM-Passwortrichtl inie ausgestellt, verwaltet und verifiziert. Sie erfüllen oder übertreffen die Anforderungen des NIST SP 800-63 und des AWS Foundational Security Best Practices-Standards für Passwortstärke. Mit dieser Regel können Sie optional RequireUppercaseCharacters (Wert für AWS grundlege nde Sicherheitsbewährte Methoden: wahr), RequireLo wercaseCharacters (Wert für bewährte Methoden für AWS grundlegende Sicherheit: wahr), RequireSymbols (Wert für bewährte Methoden für AWS grundlegende Sicherhei t: wahr), RequireNumbers (Wert für bewährte Methoden für AWS grundlegende Sicherheit: wahr), MinimumPa sswordLength (Wert für bewährte Methoden für AWS grundlegende Sicherheit: 14), PasswordReusePreve ntion (Wert für bewährte Methoden für AWS grundlege nde Sicherheit: 24) und MaxPasswordAge (Wert

Kontroll-ID	AWS Config	Empfehlungen
		für bewährte Methoden für AWS grundlegende Sicherhei t: 90) für Ihr IAM festlegen Kennwortrichtlinie. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisat ion entsprechen.
IDM-09	iam-user-mfa-enabled	Aktivieren Sie diese Regel, um den Zugriff auf Ressourcen in der AWS Cloud einzuschr änken. Diese Regel sorgt dafür, dass die Multi-Faktor-Authentifizierung (MFA) für alle Benutzer aktiviert ist. MFA sorgt für eine weitere Schutzebene zusätzlich zu den Anmeldeinformationen. Reduzieren Sie Fälle von kompromittierten Konten, indem Sie MFA für Benutzer vorschreiben.

Kontroll-ID	AWS Config	Empfehlungen
IDM-09	mfa-enabled-for-iam-Konsolenzugriff	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass MFA für alle AWS Identity and Access Management (IAM) -Benutzer aktiviert ist, die über ein Konsolenkennwort verfügen. MFA sorgt für eine weitere Schutzebene zusätzlich zu den Anmeldeinformationen. Indem Sie MFA für Benutzer vorschreiben, können Sie Fälle kompromittierter Konten reduzieren und verhindern, dass unbefugte Benutzer auf vertrauliche Daten zugreifen.
IDM-09	root-account-hardware-mfa-aktiviert	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Hardware-MFA für den Root-Benutzer aktiviert ist. Der Stammbenutzer ist der AWS-Konto-Benutzer mit den meisten Berechtigungen. MFA sorgt für eine weitere Schutzebene zusätzlich zu den Anmeldeinformationen. Indem Sie MFA für den Root-Benutzer vorschreiben, können Sie die Anzahl AWS-Konten kompromittierter Benutzer reduzieren.

Kontroll-ID	AWS Config	Empfehlungen
IDM-09	root-account-mfa-enabled	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass MFA für den Root-Benutzer aktiviert ist. Der Stammbenutzer ist der AWS-Konto-Benutzer mit den meisten Berechtigungen. MFA sorgt für eine weitere Schutzebene zusätzlich zu den Anmeldeinformationen. Indem Sie MFA für den Root-Benutzer vorschreiben, können Sie die Anzahl AWS-Konten kompromittierter Benutzer reduzieren.
OPS-01	clb-multiple-az	Elastic Load Balancing (ELB) verteilt Ihren eingehenden Traffic automatisch auf mehrere Ziele wie EC2 Instances, Container und IP-Adressen in einer Availability Zone. Zur Gewährleistung einer hohen Verfügbarkeit stellen Sie sicher, dass Ihr ELB Instances aus mehreren Availability Zones registriert hat.

Kontroll-ID	AWS Config	Empfehlungen
OPS-01	elbv2-multiple-az	Elastic Load Balancing (ELB) verteilt Ihren eingehend en Traffic automatisch auf mehrere Ziele wie EC2 Instances, Container und IP-Adressen in einer Availabil ity Zone. Zur Gewährleistung einer hohen Verfügbarkeit stellen Sie sicher, dass Ihr ELB Instances aus mehreren Availability Zones registriert hat.
OPS-01	lambda-vpc-multi-az-überprü fen	Wenn Ihre AWS Lambda-Fu nktion so konfiguriert ist, dass sie eine Verbindung zu einer Virtual Private Cloud (VPC) in Ihrem Konto herstellt, stellen Sie die AWS Lambda-Funktion in mindestens zwei verschied enen Availability Zones bereit, um sicherzustellen, dass Ihre Funktion für die Verarbeitung von Ereignissen im Falle einer Dienstunterbrechung in einer einzigen Zone verfügbar ist.

Kontroll-ID	AWS Config	Empfehlungen
OPS-01	rds-cluster-multi-az-aktiviert	Für Cluster von Amazon Relational Database Service (Amazon RDS) sollte die Multi-AZ-Replikation aktiviert sein, um die Verfügbar keit der gespeicherten Daten zu gewährleisten. Availability Zones werden auf einer physisch getrennte n, unabhängigen Infrastru ktur ausgeführt und sind auf höchste Zuverlässigkeit ausgelegt. Im Falle eines Infrastrukturausfalls führt Amazon RDS einen automatis chen Failover zum Standby-Modus durch, sodass Sie den Datenbankbetrieb wieder aufnehmen können, sobald der Failover abgeschlossen ist.

Kontroll-ID	AWS Config	Empfehlungen
OPS-01	rds-multi-az-support	Die Multi-AZ-Unterstützung in Amazon Relational Database Service (Amazon RDS) bietet eine verbesserte Verfügbar keit und Beständigkeit von Datenbank-Instances. Wenn Sie eine Multi-AZ-Datenbank-Instance bereitstellen, erstellt Amazon RDS automatisch eine primäre Datenbank-Instance und repliziert die Daten synchron auf eine Standby-Instance in einer anderen Availability Zone. Jede Availability Zone läuft auf einer eigenen, physisch getrennten, unabhängigen Infrastruktur und ist auf eine hohe Verfügbarkeit ausgelegt . Im Falle eines Infrastru kturausfalls führt Amazon RDS einen automatischen Failover zum Standby-Modus durch, sodass Sie den Datenbank betrieb wieder aufnehmen können, sobald der Failover abgeschlossen ist.

Kontroll-ID	AWS Config	Empfehlungen
OPS-01	dynamodb-autoscaling-enabled	Amazon DynamoDB Auto Scaling verwendet den AWS Application Auto Scaling-Service, um die bereitgestellte Durchsatzkapazität so anzupassen, dass sie automatisch auf tatsächliche Verkehrsmuster reagiert. Auf diese Weise kann eine Tabelle oder ein globaler sekundärer Index die bereitgestellte Lese-/Schreibkapazität erhöhen, um plötzliche Erhöhungen des Datenverkehrs ohne Drosselung zu bewältigen.
OPS-01	elb-cross-zone-load-Balancing aktiviert	Aktivieren Sie zonenübergreifendes Load Balancing für Ihre Elastic Load Balancer (ELBs), um eine angemessene Kapazität und Verfügbarkeit aufrechtzuerhalten. Zonenübergreifendes Load Balancing reduziert die Notwendigkeit, die gleiche Anzahl von Instances in jeder aktivierten Availability Zone aufrechtzuerhalten. Es verbessert auch die Fähigkeit Ihrer Anwendung, den Verlust einer oder mehrerer Instances zu bewältigen.

Kontroll-ID	AWS Config	Empfehlungen
OPS-01	dynamodb-throughput-limit-check	Aktivieren Sie diese Regel, um sicherzustellen, dass die bereitgestellte Durchsatzkapazität in Ihren Amazon-DynamoDB-Tabellen überprüft wird. Dies ist der Umfang der Lese- und Schreibaktivitäten, der von den jeweiligen Tabellen unterstützt werden kann. DynamoDB verwendet diese Informationen für das Reservieren ausreichender Systemressourcen, um Ihren Durchsatzanforderungen gerecht zu werden. Diese Regel generiert eine Warnung, wenn sich der Durchsatz dem Höchstlimit für ein Kundenkonto nähert. Mit dieser Regel können Sie optional die Parameter RCUThreshold Kontoprozentsatz (Konfigurationsstandard: 80) und WCUThreshold Kontoprozentsatz (Konfigurationsstandard: 80) festlegen. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	AWS Config	Empfehlungen
OPS-02	clb-multiple-az	Elastic Load Balancing (ELB) verteilt Ihren eingehend en Traffic automatisch auf mehrere Ziele wie EC2 Instances, Container und IP-Adressen in einer Availabil ity Zone. Zur Gewährleistung einer hohen Verfügbarkeit stellen Sie sicher, dass Ihr ELB Instances aus mehreren Availability Zones registriert hat.
OPS-02	autoscaling-group-elb-healt hcheck-erforderlich	Die Elastic Load Balancer (ELB) -Zustandsprüfungen für Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling Scaling-Gruppen unterstützen die Aufrechte rhaltung einer angemessenen Kapazität und Verfügbarkeit. Der Load Balancer sendet regelmäßig Pings, versucht Verbindungen herzustellen oder sendet Anfragen, um den Zustand der EC2 Amazon-In stances in einer Gruppe mit auto-scaling zu testen. Wenn eine Instance nicht zurückmel det, wird der Traffic an eine neue EC2 Amazon-Instance gesendet.

Kontroll-ID	AWS Config	Empfehlungen
OPS-02	beanstalk-enhanced-health-reporting-aktiviert	AWS Die verbesserte Zustandsberichterstattung von Elastic Beanstalk ermöglicht eine schnellere Reaktion auf Veränderungen im Zustand der zugrunde liegenden Infrastruktur. Diese Änderungen könnten zu einer mangelnden Verfügbarkeit der Anwendung führen. Die erweiterten Zustandsberichte von Elastic Beanstalk bieten eine Statusbeschreibung, um den Schweregrad der identifizierten Probleme einzuschätzen und mögliche Ursachen zu identifizieren, die untersucht werden müssen.
OPS-02	elbv2-multiple-az	Elastic Load Balancing (ELB) verteilt Ihren eingehenden Traffic automatisch auf mehrere Ziele wie EC2 Instances, Container und IP-Adressen in einer Availability Zone. Zur Gewährleistung einer hohen Verfügbarkeit stellen Sie sicher, dass Ihr ELB Instances aus mehreren Availability Zones registriert hat.

Kontroll-ID	AWS Config	Empfehlungen
OPS-02	lambda-vpc-multi-az-überprüfen	Wenn Ihre AWS Lambda-Funktion so konfiguriert ist, dass sie eine Verbindung zu einer Virtual Private Cloud (VPC) in Ihrem Konto herstellt, stellen Sie die AWS Lambda-Funktion in mindestens zwei verschiedenen Availability Zones bereit, um sicherzustellen, dass Ihre Funktion für die Verarbeitung von Ereignissen im Falle einer Dienstunterbrechung in einer einzigen Zone verfügbar ist.

Kontroll-ID	AWS Config	Empfehlungen
OPS-02	rds-cluster-multi-az-aktiviert	Für Cluster von Amazon Relational Database Service (Amazon RDS) sollte die Multi-AZ-Replikation aktiviert sein, um die Verfügbar keit der gespeicherten Daten zu gewährleisten. Availability Zones werden auf einer physisch getrennte n, unabhängigen Infrastru ktur ausgeführt und sind auf höchste Zuverlässigkeit ausgelegt. Im Falle eines Infrastrukturausfalls führt Amazon RDS einen automatis chen Failover zum Standby-Modus durch, sodass Sie den Datenbankbetrieb wieder aufnehmen können, sobald der Failover abgeschlossen ist.

Kontroll-ID	AWS Config	Empfehlungen
OPS-02	rds-multi-az-support	Die Multi-AZ-Unterstützung in Amazon Relational Database Service (Amazon RDS) bietet eine verbesserte Verfügbar keit und Beständigkeit von Datenbank-Instances. Wenn Sie eine Multi-AZ-Datenbank-Instance bereitstellen, erstellt Amazon RDS automatisch eine primäre Datenbank-Instance und repliziert die Daten synchron auf eine Standby-Instance in einer anderen Availability Zone. Jede Availability Zone läuft auf einer eigenen, physisch getrennten, unabhängigen Infrastruktur und ist auf eine hohe Verfügbarkeit ausgelegt . Im Falle eines Infrastru kturausfalls führt Amazon RDS einen automatischen Failover zum Standby-Modus durch, sodass Sie den Datenbank betrieb wieder aufnehmen können, sobald der Failover abgeschlossen ist.

Kontroll-ID	AWS Config	Empfehlungen
OPS-02	dynamodb-autoscaling-enabled	Amazon DynamoDB Auto Scaling verwendet den AWS Application Auto Scaling-Service, um die bereitgestellte Durchsatzkapazität so anzupassen, dass sie automatisch auf tatsächliche Verkehrsmuster reagiert. Auf diese Weise kann eine Tabelle oder ein globaler sekundärer Index die bereitgestellte Lese-/Schreibkapazität erhöhen, um plötzliche Erhöhungen des Datenverkehrs ohne Drosselung zu bewältigen.
OPS-02	elb-cross-zone-load-Balancing aktiviert	Aktivieren Sie zonenübergreifendes Load Balancing für Ihre Elastic Load Balancer (ELBs), um eine angemessene Kapazität und Verfügbarkeit aufrechtzuerhalten. Zonenübergreifendes Load Balancing reduziert die Notwendigkeit, die gleiche Anzahl von Instances in jeder aktivierten Availability Zone aufrechtzuerhalten. Es verbessert auch die Fähigkeit Ihrer Anwendung, den Verlust einer oder mehrerer Instances zu bewältigen.

Kontroll-ID	AWS Config	Empfehlungen
OPS-02	dynamodb-throughput-limit-check	Aktivieren Sie diese Regel, um sicherzustellen, dass die bereitgestellte Durchsatzkapazität in Ihren Amazon-DynamoDB-Tabellen überprüft wird. Dies ist der Umfang der Lese- und Schreibaktivitäten, der von den jeweiligen Tabellen unterstützt werden kann. DynamoDB verwendet diese Informationen für das Reservieren ausreichender Systemressourcen, um Ihren Durchsatzanforderungen gerecht zu werden. Diese Regel generiert eine Warnung, wenn sich der Durchsatz dem Höchstlimit für ein Kundenkonto nähert. Mit dieser Regel können Sie optional die Parameter RCUThreshold Kontoprozentsatz (Konfigurationsstandard: 80) und WCUThreshold Kontoprozentsatz (Konfigurationsstandard: 80) festlegen. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	AWS Config	Empfehlungen
OPS-07	aurora-resources-protected-by-Backup-Plan	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon Aurora Aurora-Ressourcen Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	AWS Config	Empfehlungen
OPS-07	backup-plan-min-frequency-and-min-retention-check	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihr AWS Backup-Plan auf eine Mindestfrequenz und Aufbewahrung festgelegt ist. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen. Mit dieser Regel können Sie die Parameter requiredFrequencyValue (Config default: 1), requiredRetentionDays (Config default: 35) und requiredFrequencyUnit (Config default: days) festlegen. Der tatsächliche Wert muss den Anforderungen Ihrer Organisation entsprechen.

Kontroll-ID	AWS Config	Empfehlungen
OPS-07	backup-recovery-point-manual-löschen-deaktiviert	Stellen Sie sicher, dass Ihren AWS Backup-Wiederherstellungspunkten eine ressourcenbasierte Richtlinie zugeordnet ist, die das Löschen von Wiederherstellungspunkten verhindert. Die Verwendung einer ressourcenbasierten Richtlinie zur Verhinderung des Löschens von Wiederherstellungspunkten kann dazu beitragen, ein versehentliches oder absichtliches Löschen zu unterbinden.
OPS-07	dynamodb-pitr-enabled	Aktivieren Sie diese Regel, um zu überprüfen, ob die Informationen gesichert wurden. Es verwaltet auch die Backups, indem es sicherstellt, dass die point-in-time Wiederherstellung in Amazon DynamoDB aktiviert ist. Bei der Wiederherstellung werden fortlaufende Backups Ihrer Tabelle für die letzten 35 Tage gespeichert.

Kontroll-ID	AWS Config	Empfehlungen
OPS-07	opensearch-data-node-fault-Toleranz	Amazon OpenSearch Service (OpenSearch Service) benötigt mindestens drei Datenknoten für hohe Verfügbarkeit und Fehlertoleranz. Die Bereitstellung einer OpenSearch Service-Domain mit mindestens drei Datenknoten gewährleistet den Cluster-Betrieb, falls ein Knoten ausfällt.
OPS-07	backup-recovery-point-minimum-Aufbewahrungsprüfung	Um bei Datensicherungsprozessen zu helfen, stellen Sie sicher, dass für Ihre AWS Backup-Wiederherstellungspunkte eine Mindestaufbewahrungsdauer festgelegt ist. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen. Mit dieser Regel können Sie den Parameter requiredRetentionDays (Config Default: 35) festlegen. Der tatsächliche Wert muss den Anforderungen Ihrer Organisation entsprechen.

Kontroll-ID	AWS Config	Empfehlungen
OPS-07	db-instance-backup-enabled	Die Sicherungsfunktion von Amazon RDS erstellt Sicherungen Ihrer Datenbanken und Transaktionsprotokolle. Amazon RDS erstellt einen Snapshot für das Speichervolume Ihrer DB-Instance, sodass die gesamte DB-Instance gesichert wird. Sie können im System spezifische Aufbewahrungsfristen festlegen, um Ihre Ausfallsicherheitsanforderungen zu erfüllen.
OPS-07	dynamodb-in-backup-plan	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon DynamoDB-Tabellen Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	AWS Config	Empfehlungen
OPS-07	ebs-in-backup-plan	Stellen Sie zur Unterstützung der Datensicherungsprozesse sicher, dass Ihre Amazon Elastic Block Store (Amazon EBS) -Volumes Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherung smanagement und erleichte rt Ihnen die Erfüllung von geschäftlichen und behördlic hen Compliance-Anforde rungen hinsichtlich Datensich erungen.

Kontroll-ID	AWS Config	Empfehlungen
OPS-07	ec2--Plan resources-protected-by-backup	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon Elastic Compute Cloud (Amazon EC2) - Ressourcen Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	AWS Config	Empfehlungen
OPS-07	efs-in-backup-plan	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon Elastic File System (Amazon EFS) - Dateisysteme Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.
OPS-07	elasticache-redis-cluster-automatic-Backup-Check	Wenn automatische Backups aktiviert sind, ElastiCache erstellt Amazon täglich ein Backup des Clusters. Die Sicherung kann für eine von Ihrer Organisation festgelegte Anzahl von Tagen aufbewahrt werden. Automatische Backups schützen vor Datenverlust. Bei einem Ausfall können Sie einen neuen Cluster erstellen, der Ihre Daten aus dem aktuellen Backup wiederherstellt.

Kontroll-ID	AWS Config	Empfehlungen
OPS-07	fsx-resources-protected-by-Backup-Plan	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre FSx Amazon-Dateisysteme Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	AWS Config	Empfehlungen
OPS-07	rds-in-backup-plan	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon Relational Database Service (Amazon RDS) -Instances Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	AWS Config	Empfehlungen
OPS-07	redshift-backup-enabled	Stellen Sie zur Unterstützung der Datensicherungsprozesse sicher, dass Ihre Amazon-Redshift-Cluster über automatisierte Snapshots verfügen. Wenn automatisierte Snapshots für einen Cluster aktiviert sind, erstellt Redshift in regelmäßigen Abständen Snapshots dieses Clusters. Standardmäßig erstellt Redshift alle acht Stunden oder alle 5 GB einen Snapshot für jeden Knoten mit Datenänderungen oder je nachdem, was zuerst eintritt.
OPS-12	cw-loggroup-retention-period-überprüfen	Stellen Sie sicher, dass die Ereignisprotokolldaten für Ihre Protokollgruppen über eine Mindestdauer aufbewahrt werden, um die Fehlerbehebung und forensische Untersuchungen zu unterstützen. Fehlende frühere Ereignisprotokolldaten erschweren die Rekonstruierung und Identifizierung potenziell schädlicher Ereignisse.

Kontroll-ID	AWS Config	Empfehlungen
OPS-12	s3- lifecycle-policy-check	Mit Amazon-S3-Lebenszyklusregeln können Sie Aktionen definieren, die Amazon S3 während der Lebensdauer eines Objekts ausführen soll (z. B. die Überführung von Objekten in eine andere Speicherklasse, ihre Archivierung oder Löschung nach einem bestimmten Zeitraum).
OPS-13	guardduty-enabled-centralized	Amazon GuardDuty kann mithilfe von Threat Intelligence Feeds helfen, potenzielle Cybersicherheitsereignisse zu überwachen und zu erkennen. Dazu gehören Listen mit bösartigen IPs und maschinellen Lernmethoden zur Identifizierung unerwarteter, nicht autorisierter und bösartiger Aktivitäten in Ihrer AWS Cloud-Umgebung.

Kontroll-ID	AWS Config	Empfehlungen
OPS-13	redshift-cluster-configuration-check	Um Daten im Ruhezustand zu schützen, muss die Verschlüsselung für Ihre Amazon-Redshift-Cluster aktiviert sein. Sie müssen auch sicherstellen, dass die erforderlichen Konfigurationen auf Amazon-Redshift-Clustern bereitgestellt werden. Die Prüfungsprotokollierung muss aktiviert sein, um Informationen zu Verbindungen und Benutzeraktivitäten in der Datenbank bereitzustellen. Diese Regel erfordert, dass ein Wert für clusterDbEncrypted (Config Default: TRUE) und LoggingEnabled (Config Default: TRUE) gesetzt ist. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	AWS Config	Empfehlungen
OPS-13	securityhub-enabled	AWS Security Hub hilft bei der Überwachung von unbefugte m Personal, Verbindungen, Geräten und Software. AWS Security Hub aggregiert, organisiert und priorisiert die Sicherheitswarnungen oder Ergebnisse mehrerer Dienste. AWS Einige dieser Dienste sind Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer und AWS Firewall Manager sowie AWS Partnerlösungen.

Kontroll-ID	AWS Config	Empfehlungen
OPS-14	cloud-trail-log-file-Validierung aktiviert	Verwenden Sie die AWS CloudTrail Protokolldateivalidierung, um die Integrität von Protokollen zu überprüfen. CloudTrail Mithilfe der Protokolldateivalidierung kann festgestellt werden, ob eine Protokolldatei geändert oder gelöscht wurde oder ob sie nach der Übermittlung CloudTrail unverändert geblieben ist. Dieses Feature wurde mit dem Branchenstandard entsprechenden Algorithmen entwickelt: SHA-256 für die Hashfunktion und SHA-256 mit RSA für digitale Signaturen. Aus diesem Grund ist es rechnerisch unmöglich, CloudTrail Protokolldateien unbemerkt zu ändern, zu löschen oder zu fälschen.
OPS-14	cloud-trail-encryption-enabled	Da sensible Daten vorhanden sein können und um Daten im Speicher zu schützen, sollten Sie sicherstellen, dass die Verschlüsselung für Ihre Spuren aktiviert ist. AWS CloudTrail

Kontroll-ID	AWS Config	Empfehlungen
OPS-14	cw-loggroup-retention-period-überprüfen	Stellen Sie sicher, dass die Ereignisprotokolldaten für Ihre Protokollgruppen über eine Mindestdauer aufbewahrt werden, um die Fehlerbehebung und forensische Untersuch ungen zu unterstützen. Fehlende frühere Ereignisp rotokolldaten erschweren die Rekonstruierung und Identifiz ierung potenziell schädlicher Ereignisse.
OPS-14	s3- lifecycle-policy-check	Mit Amazon-S3-Lebenszy klusregeln können Sie Aktionen definieren, die Amazon S3 während der Lebensdauer eines Objekts ausführen soll (z. B. die Überführung von Objekten in eine andere Speicherk lasse, ihre Archivierung oder Löschung nach einem bestimmten Zeitraum).
OPS-15	api-gw-execution-logging-ak tiviert	Die API-Gateway-Protok ollierung zeigt detaillierte Ansichten der Benutzer, die auf die API zugegriffen haben, und wie diese Benutzer auf die API zugegriffen haben. Diese Einblicke ermöglichen die Transparenz von Benutzera ktivitäten.

Kontroll-ID	AWS Config	Empfehlungen
OPS-15	cloud-trail-cloud-watch-logs-aktiviert	Verwenden Sie Amazon CloudWatch , um Protokoll ereignisaktivitäten zentral zu sammeln und zu verwalten . Die Aufnahme von AWS CloudTrail Daten liefert Einzelheiten zu den API-Aufru faktivitäten in Ihrem AWS-Konto.
OPS-15	codebuild-project-logging-enabled	Stellen Sie sicher, dass die AWS CodeBuild Projektpr otokollierung aktiviert ist, damit Ihre Build-Ausgabeproto kolle entweder an Amazon CloudWatch oder Amazon Simple Storage Service (Amazon S3) gesendet werden. Build-Ausgabeproto kolle enthalten detaillierte Informationen zu Ihrem Build-Projekt.
OPS-15	elasticsearch-logs-to-cloudwatch	Stellen Sie sicher, dass für Amazon OpenSearch Service-Domains Fehlerprotokolle aktiviert und zur Aufbewahr ung und Beantwortung an Amazon CloudWatch Logs gestreamt werden. Domain-Fehlerprotokolle sind bei Sicherheits- und Zugriffsp rüfungen sowie bei der Diagnose von Verfügbar keitsproblemen nützlich.

Kontroll-ID	AWS Config	Empfehlungen
OPS-15	elb-logging-enabled	Die Elastic-Load-Balancing-Aktivität ist ein zentraler Kommunikationspunkt innerhalb einer Umgebung. Stellen Sie sicher, dass die ELB-Protokollierung aktiviert ist. Die gesammelten Daten enthalten detaillierte Informati onen zu Anfragen, die an den ELB gesendet wurden. Jedes Protokoll enthält Informati onen wie die Zeit, zu der die Anforderung einging, die Client-IP-Adresse, Latenzen, Anforderungspfade und Serverantworten.
OPS-15	opensearch-audit-logging-en abled	Stellen Sie sicher, dass die Audit-Protokollierung für Ihre Amazon OpenSearch Service-Domains aktiviert ist. Mit der Audit-Protokollierung können Sie Benutzeraktivitäten auf Ihren OpenSearch Domains verfolgen, einschließlich erfolgreicher und fehlgesch lagener Authentifizierunge n OpenSearch, Anfragen an, Indexänderungen und eingehende Suchanfragen.

Kontroll-ID	AWS Config	Empfehlungen
OPS-15	opensearch-logs-to-cloudwatch	Stellen Sie sicher, dass für Amazon OpenSearch Service-Domains Fehlerprotokolle aktiviert und zur Aufbewahrung und Beantwortung an Amazon CloudWatch Logs gestreamt werden. OpenSearch Service-Fehlerprotokolle können bei Sicherheits- und Zugriffsprüfungen helfen und bei der Diagnose von Verfügbarkeitsproblemen helfen.
OPS-15	rds-logging-enabled	Um die Protokollierung und Überwachung in Ihrer Umgebung zu erleichtern, stellen Sie sicher, dass die Amazon Relational Database Service (Amazon RDS)-Protokollierung aktiviert ist. Mit der Amazon-RDS-Protokollierung können Sie Ereignisse wie Verbindungen, Verbindungsabbrüche, Abfragen oder abgefragte Tabellen erfassen.
OPS-15	redshift-audit-logging-enabled	Aktivieren Sie die Prüfungsprotokollierung, um Informationen über Verbindungen und Benutzeraktivitäten in Ihrem Amazon-Redshift-Cluster zu erfassen.

Kontroll-ID	AWS Config	Empfehlungen
OPS-15	s-3 bucket-logging-enabled	Die Amazon Simple Storage Service (Amazon S3)-Serverzugriffsprotokollierung bietet eine Methode zur Überwachung des Netzwerks im Hinblick auf potenzielle Cybersicherheitsereignisse. Die Ereignisse werden überwacht, indem detaillierte Aufzeichnungen über die Anfragen erfasst werden, die an einen Amazon-S3-Bucket gestellt wurden. Jeder Zugriffsprotokolleintrag enthält Details zu einer einzelnen Zugriffsanfrage. Zu den Details gehören Anforderer, Bucket-Name, Anforderungszeit, Anforderungsaktion, Antwortstatus und Fehlercode, falls relevant.

Kontroll-ID	AWS Config	Empfehlungen
OPS-15	vpc-flow-logs-enabled	VPC-Flow-Protokolle erfassen detaillierte Informationsdatensätze über den IP-Datenverkehr, der zu und von Netzwerkschnittstellen in Ihrer Amazon Virtual Private Cloud (Amazon VPC) fließt. Standardmäßig enthalten Flow-Protokolldatensätze Werte für die verschiedenen Komponenten des IP-Flows, einschließlich Quelle, Ziel und Protokoll.
OPS-15	wafv2-logging-enabled	Um die Protokollierung und Überwachung in Ihrer Umgebung zu erleichtern, aktivieren Sie die AWS WAF (V2) -Protokollierung im regionalen und globalen Web ACLs. AWS Die WAF-Protokollierung bietet detaillierte Informationen über den Datenverkehr, der von Ihrer Web-ACL analysiert wird. In den Protokollen werden die Uhrzeit aufgezeichnet, zu der die AWS WAF die Anfrage von Ihrer AWS Ressource erhalten hat, Informationen über die Anfrage und eine Aktion für die Regel, der jede Anfrage entsprach.

Kontroll-ID	AWS Config	Empfehlungen
OPS-15	cloudtrail-enabled	AWS CloudTrail kann dabei helfen, die Ablehnung zu verhindern, indem Aktionen und API-Aufrufe der AWS Management Console aufgezeichnet werden. Sie können die Benutzer und die Benutzer AWS-Konten , die einen AWS Dienst aufgerufen haben, die Quell-IP-Adresse, über die die Aufrufe generiert wurden, und den Zeitpunkt der Anrufe identifizieren. Einzelheiten zu den erfassten Daten finden Sie in den AWS CloudTrail Datensatzinhalten.
OPS-15	cloudtrail-s3-dataevents-enabled	Die Erfassung von Simple Storage Service (Amazon S3)-Datenereignissen unterstützt die Erkennung von ungewöhnlichen Aktivitäten. Zu den Details gehören AWS-Konto Informationen über den Zugriff auf einen Amazon S3 S3-Bucket, die IP-Adresse und die Uhrzeit des Ereignisses.

Kontroll-ID	AWS Config	Empfehlungen
OPS-15	cloudtrail-security-trail-enabled	Diese Regel trägt dazu bei, die Verwendung der AWS empfohlenen bewährten Sicherheitsmethoden für sicherzustellen AWS CloudTrail, indem geprüft wird, ob mehrere Einstellungen aktiviert sind. Dazu gehören die Verwendung von Protokoll verschlüsselung, Protokoll validierung und Aktivierung AWS CloudTrail in mehreren Regionen.

Kontroll-ID	AWS Config	Empfehlungen
OPS-15	multi-region-cloudtrail-enabled	AWS CloudTrail zeichnet Aktionen und API-Aufrufe der AWS Management Console auf. Sie können feststellen, welche Benutzer und Konten angerufen wurden AWS, von welcher Quell-IP-Adresse aus die Anrufe getätigt wurden und wann die Anrufe erfolgten . CloudTrail übermittelt Protokolldateien aus allen AWS Regionen an Ihren S3-Bucket, wenn MULTI_REG ION_CLOUD_TRAIL_EN ABLED aktiviert ist. Außerdem wird beim AWS Start einer neuen Region derselbe Trail in der neuen Region erstellt. CloudTrail Dadurch erhalten Sie automatisch Protokoll dateien mit API-Aktivitäten für die neue Region.

Kontroll-ID	AWS Config	Empfehlungen
OPS-22	ecr-private-image-scanning-aktiviert	Der Amazon Elastic Container Repository (ECR)-Image-Scan unterstützt die Identifizierung von Software-Schwachstellen in Ihren Container-Images. Durch die Aktivierung von Image-Scans in ECR-Repos itorys werden die Integrität und Sicherheit der gespeicherten Images mit einer zusätzlichen Überprüfungsebene verbesser t.
PSS-05	iam-user-mfa-enabled	Aktivieren Sie diese Regel, um den Zugriff auf Ressourcen in der AWS Cloud einzuschr änken. Diese Regel sorgt dafür, dass die Multi-Faktor-Authentifizierung (MFA) für alle Benutzer aktiviert ist. MFA sorgt für eine weitere Schutzebene zusätzlich zu den Anmeldeinformationen. Reduzieren Sie Fälle von kompromittierten Konten, indem Sie MFA für Benutzer vorschreiben.

Kontroll-ID	AWS Config	Empfehlungen
PSS-05	mfa-enabled-for-iam-Konsolenzugriff	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass MFA für alle AWS Identity and Access Management (IAM) -Benutzer aktiviert ist, die über ein Konsolenkennwort verfügen. MFA sorgt für eine weitere Schutzebene zusätzlich zu den Anmeldeinformationen. Indem Sie MFA für Benutzer vorschreiben, können Sie Fälle kompromittierter Konten reduzieren und verhindern, dass unbefugte Benutzer auf vertrauliche Daten zugreifen.
PSS-05	root-account-hardware-mfa-aktiviert	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Hardware-MFA für den Root-Benutzer aktiviert ist. Der Stammbenutzer ist der AWS-Konto-Benutzer mit den meisten Berechtigungen. MFA sorgt für eine weitere Schutzebene zusätzlich zu den Anmeldeinformationen. Indem Sie MFA für den Root-Benutzer vorschreiben, können Sie die Anzahl AWS-Konten kompromittierter Benutzer reduzieren.

Kontroll-ID	AWS Config	Empfehlungen
PSS-05	root-account-mfa-enabled	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass MFA für den Root-Benutzer aktiviert ist. Der Stammbenutzer ist der AWS-Konto-Benutzer mit den meisten Berechtigungen. MFA sorgt für eine weitere Schutzebene zusätzlich zu den Anmeldeinformationen. Indem Sie MFA für den Root-Benutzer vorschreiben, können Sie die Anzahl AWS-Konten kompromittierter Benutzer reduzieren.

Kontroll-ID	AWS Config	Empfehlungen
PSS-07	iam-password-policy	Die Identitäten und Anmeldein formationen werden auf der Grundlage einer organisat orischen IAM-Passwortrichtl inie ausgestellt, verwaltet und verifiziert. Sie erfüllen oder übertreffen die Anforderungen von NIST SP 800-63 und dem Standard „Best Practices“ von AWS Foundational Security für die Passwortstärke. Mit dieser Regel können Sie optional RequireUppercaseCharacters (Wert für AWS grundlege nde Sicherheitsbewährte Methoden: wahr), RequireLo wercaseCharacters (Wert für bewährte Methoden für AWS grundlegende Sicherheit: wahr), RequireSymbols (Wert für bewährte Methoden für AWS grundlegende Sicherhei t: wahr), RequireNumbers (Wert für bewährte Methoden für AWS grundlegende Sicherheit: wahr), MinimumPa sswordLength (Wert für bewährte Methoden für AWS grundlegende Sicherheit: 14), PasswordReusePreve ntion (Wert für bewährte Methoden für AWS grundlege nde Sicherheit: 24) und MaxPasswordAge (Wert

Kontroll-ID	AWS Config	Empfehlungen
		für bewährte Methoden für AWS grundlegende Sicherhei t: 90) für Ihr IAM festlegen Kennwortrichtlinie. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisat ion entsprechen.

Vorlage

Die Vorlage ist verfügbar auf GitHub: Deutschland Cloud Computing Compliance Criteria Catalog (C5).

Bewährte Methoden für die Implementierung des Gramm Leach Bliley Act (GLBA)

Konformitätspakete bieten ein allgemeines Compliance-Framework, das es Ihnen ermöglicht, mithilfe verwalteter oder benutzerdefinierter Regeln und Abhilfemaßnahmen Kontrollen zur Sicherheits-, Betriebs- oder Kostenoptimierung durchzuführen. AWS Config AWS Config Conformance Packs dienen als Beispielvorlagen nicht dazu, die vollständige Einhaltung eines bestimmten Governance- oder Compliance-Standards sicherzustellen. Sie sind dafür verantwortlich, selbst zu beurteilen, ob Ihre Nutzung der Services den geltenden gesetzlichen und behördlichen Anforderungen entspricht.

Im Folgenden finden Sie ein Beispiel für eine Zuordnung zwischen den Gramm-Leach-Bliley Act- (GLBA) - und den AWS Managed Config-Regeln. Jede Config-Regel gilt für eine bestimmte AWS Ressource und bezieht sich auf eine oder mehrere GLBA-Steuerelemente. Eine CJIS-Kontrolle kann mehreren Config-Regeln zugeordnet werden. In der folgenden Tabelle finden Sie weitere Informationen und Anleitungen zu diesen Zuordnungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
GLBA-SEC.501(b)	Zur Förderung der in Unterabschnitt (a) dargelegten Richtlinie	dms-replication-not-public	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	legen alle in Abschnitt 505(a) beschriebenen Behörden angemessene Standards für die ihrer Gerichtsbarkeit unterstehenden Finanzinstitute in Bezug auf administrative, technische und physische Schutzmaßnahmen fest.		sicherstellen, dass auf DMS-Replikationsinstanzen nicht öffentlich zugegriffen werden kann. DMS-Replikations-Instances können vertrauliche Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.
GLBA-SEC.501(b)	Zur Förderung der in Unterabschnitt (a) dargelegten Richtlinie legen alle in Abschnitt 505(a) beschriebenen Behörden angemessene Standards für die ihrer Gerichtsbarkeit unterstehenden Finanzinstitute in Bezug auf administrative, technische und physische Schutzmaßnahmen fest.	ebs-snapshot-public-restorable-überprüfen	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass EBS-Snapshots nicht öffentlich wiederherstellbar sind. EBS-Volume-Snapshots können vertrauliche Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
GLBA-SEC.501(b)	Zur Förderung der in Unterabschnitt (a) dargelegten Richtlinie legen alle in Abschnitt 505(a) beschriebenen Behörden angemessene Standards für die ihrer Gerichtsbarkeit unterstehenden Finanzinstitute in Bezug auf administrative, technische und physische Schutzmaßnahmen fest.	ec-2 instance-no-public-ip	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon Elastic Compute Cloud (Amazon EC2) - Instances nicht öffentlich zugänglich sind. EC2Amazon -Instances können vertrauliche Informationen enthalten, und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
GLBA-SEC.501(b)	Zur Förderung der in Unterabschnitt (a) dargelegten Richtlinie legen alle in Abschnitt 505(a) beschriebenen Behörden angemessene Standards für die ihrer Gerichtsbarkeit unterstehenden Finanzinstitute in Bezug auf administrative, technische und physische Schutzmaßnahmen fest.	elasticsearch-in-vpc-only	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass sich Amazon OpenSearch OpenSearch Service (Service) - Domains innerhalb einer Amazon Virtual Private Cloud (Amazon VPC) befinden. Eine OpenSearch Service-Domain innerhalb einer Amazon VPC ermöglicht die sichere Kommunikation zwischen OpenSearch Service und anderen Services innerhalb der Amazon VPC, ohne dass ein Internet-Gateway, ein NAT-Gerät oder eine VPN-Verbindung erforderlich ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
GLBA-SEC.501(b)	Zur Förderung der in Unterabschnitt (a) dargelegten Richtlinie legen alle in Abschnitt 505(a) beschriebenen Behörden angemessene Standards für die ihrer Gerichtsbarkeit unterstehenden Finanzinstitute in Bezug auf administrative, technische und physische Schutzmaßnahmen fest.	emr-master-no-public-ip	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon EMR-Cluster-Masterknoten nicht öffentlich zugänglich sind. Amazon-EMR-Cluster-Hauptknoten können vertrauliche Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
GLBA-SEC.501(b)	Zur Förderung der in Unterabschnitt (a) dargelegten Richtlinie legen alle in Abschnitt 505(a) beschriebenen Behörden angemessene Standards für die ihrer Gerichtsbarkeit unterstehenden Finanzinstitute in Bezug auf administrative, technische und physische Schutzmaßnahmen fest.	ec-2 instances-in-vpc	Stellen Sie Amazon Elastic Compute Cloud (Amazon EC2) -Instances innerhalb einer Amazon Virtual Private Cloud (Amazon VPC) bereit, um eine sichere Kommunikation zwischen einer Instance und anderen Services innerhalb der Amazon VPC zu ermöglichen, ohne dass ein Internet-Gateway, ein NAT-Gerät oder eine VPN-Verbindung erforderlich ist. Der gesamte Datenverkehr bleibt sicher in der AWS Cloud. Domains, die sich innerhalb einer VPC befinden, verfügen aufgrund ihrer logischen Isolierung im Vergleich zu Domains mit öffentlichen Endpunkten über eine zusätzliche Sicherheitsebene. Weisen Sie EC2

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			Amazon-Instances einer Amazon-VPC zu, um den Zugriff ordnungsgemäß zu verwalten.
GLBA-SEC.501(b)	Zur Förderung der in Unterabschnitt (a) dargelegten Richtlinie legen alle in Abschnitt 505(a) beschriebenen Behörden angemessene Standards für die ihrer Gerichtsbarkeit unterstehenden Finanzinstitute in Bezug auf administrative, technische und physische Schutzmaßnahmen fest.	internet-gateway-authorized-vpc-nur	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Internet-Gateways nur mit autorisierter Amazon Virtual Private Cloud (Amazon VPC) verbunden sind. Internet-Gateways ermöglichen den bidirektionalen Internetzugang zur und von der Amazon VPC, was möglicherweise zu einem unbefugten Zugriff auf Amazon-VPC-Ressourcen führen kann.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
GLBA-SEC.501(b)	Zur Förderung der in Unterabschnitt (a) dargelegten Richtlinie legen alle in Abschnitt 505(a) beschriebenen Behörden angemessene Standards für die ihrer Gerichtsbarkeit unterstehenden Finanzinstitute in Bezug auf administrative, technische und physische Schutzmaßnahmen fest.	lambda-function-public-access-verboten	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass AWS Lambda-Funktionen nicht öffentlich zugänglich sind. Der öffentliche Zugriff kann möglicherweise die Verfügbarkeit von Ressourcen beeinträchtigen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
GLBA-SEC.501(b)	Zur Förderung der in Unterabschnitt (a) dargelegten Richtlinie legen alle in Abschnitt 505(a) beschriebenen Behörden angemessene Standards für die ihrer Gerichtsbarkeit unterstehenden Finanzinstitute in Bezug auf administrative, technische und physische Schutzmaßnahmen fest.	lambda-inside-vpc	Stellen Sie AWS Lambda-Funktionen in einer Amazon Virtual Private Cloud (Amazon VPC) bereit, um eine sichere Kommunikation zwischen einer Funktion und anderen Diensten innerhalb der Amazon VPC zu gewährleisten. Bei dieser Konfiguration sind kein Internet-Gateway, kein NAT-Gerät und keine VPN-Verbindung erforderlich. Der gesamte Datenverkehr bleibt sicher in der Cloud. AWS Domains, die sich innerhalb einer VPC befinden, verfügen aufgrund ihrer logischen Isolierung im Vergleich zu Domains mit öffentlichen Endpunkten über eine zusätzliche Sicherheitsebene. Um den Zugriff ordnungsgemäß zu verwalten,

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			sollten AWS Lambda-Funktionen einer VPC zugewiesen werden.
GLBA-SEC.501(b)	Zur Förderung der in Unterabschnitt (a) dargelegten Richtlinie legen alle in Abschnitt 505(a) beschriebenen Behörden angemessene Standards für die ihrer Gerichtsbarkeit unterstehenden Finanzinstitute in Bezug auf administrative, technische und physische Schutzmaßnahmen fest.	rds-instance-public-access-überprüfen	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Relational Database Service (Amazon RDS) -Instances nicht öffentlich sind. Amazon-RDS-Datenbank-Instances können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
GLBA-SEC.501(b)	Zur Förderung der in Unterabschnitt (a) dargelegten Richtlinie legen alle in Abschnitt 505(a) beschriebenen Behörden angemessene Standards für die ihrer Gerichtsbarkeit unterstehenden Finanzinstitute in Bezug auf administrative, technische und physische Schutzmaßnahmen fest.	rds-snapshots-public-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Relational Database Service (Amazon RDS) -Instances nicht öffentlich sind. Amazon-RDS-Datenbank-Instances können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
GLBA-SEC.501(b)	Zur Förderung der in Unterabschnitt (a) dargelegten Richtlinie legen alle in Abschnitt 505(a) beschriebenen Behörden angemessene Standards für die ihrer Gerichtsbarkeit unterstehenden Finanzinstitute in Bezug auf administrative, technische und physische Schutzmaßnahmen fest.	redshift-cluster-public-access-überprüfen	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Redshift Redshift-Cluster nicht öffentlich sind. Amazon-Redshift-Cluster können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
GLBA-SEC.501(b)	Zur Förderung der in Unterabschnitt (a) dargelegten Richtlinie legen alle in Abschnitt 505(a) beschriebenen Behörden angemessene Standards für die ihrer Gerichtsbarkeit unterstehenden Finanzinstitute in Bezug auf administrative, technische und physische Schutzmaßnahmen fest.	s3- -Block-periodisch account-level-public-access	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Simple Storage Service (Amazon S3) -Buckets nicht öffentlich zugänglich sind. Diese Regel trägt dazu bei, sensible Daten vor unbefugten Remote-Benutzern zu schützen, indem sie den öffentlichen Zugriff verhindert. Mit dieser Regel können Sie optional die Parameter ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) und restrictPublicBuckets Parameter (Config Default: True) festlegen. Die tatsächlichen Werte müssen den Richtlini

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			en Ihrer Organisation entsprechen.
GLBA-SEC.501(b)	Zur Förderung der in Unterabschnitt (a) dargelegten Richtlinie legen alle in Abschnitt 505(a) beschriebenen Behörden angemessene Standards für die ihrer Gerichtsbarkeit unterstehenden Finanzinstitute in Bezug auf administrative, technische und physische Schutzmaßnahmen fest.	s3- bucket-public-read-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie nur autorisierten Benutzern, Prozessen und Geräten Zugriff auf Amazon Simple Storage Service (Amazon S3) - Buckets gewähren. Die Verwaltung des Zugriffs sollte mit der Klassifizierung der Daten übereinstimmen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
GLBA-SEC.501(b)	Zur Förderung der in Unterabschnitt (a) dargelegten Richtlinie legen alle in Abschnitt 505(a) beschriebenen Behörden angemessene Standards für die ihrer Gerichtsbarkeit unterstehenden Finanzinstitute in Bezug auf administrative, technische und physische Schutzmaßnahmen fest.	sagemaker-notebook-no-direct-Internetzugang	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass SageMaker Amazon-Notebooks keinen direkten Internetzugang zulassen. Indem Sie direkten Internetzugang blockieren, vermeiden Sie, dass unbefugte Benutzer auf sensible Daten zugreifen.
GLBA-SEC.501(b)	Zur Förderung der in Unterabschnitt (a) dargelegten Richtlinie legen alle in Abschnitt 505(a) beschriebenen Behörden angemessene Standards für die ihrer Gerichtsbarkeit unterstehenden Finanzinstitute in Bezug auf administrative, technische und physische Schutzmaßnahmen fest.	autoscaling-launch-config-public-ip-deaktiviert	Wenn Sie Ihre Netzwerkschnittstellen mit einer öffentlichen IP-Adresse konfigurieren, sind die diesen Netzwerkschnittstellen zugehörigen Ressourcen über das Internet erreichbar. EC2 Ressourcen sollten nicht öffentlich zugänglich sein, da dies einen unbeabsichtigten Zugriff auf Ihre Anwendungen oder Server ermöglichen kann.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
GLBA-SEC.501(b)	Zur Förderung der in Unterabschnitt (a) dargelegten Richtlinie legen alle in Abschnitt 505(a) beschriebenen Behörden angemessene Standards für die ihrer Gerichtsbarkeit unterstehenden Finanzinstitute in Bezug auf administrative, technische und physische Schutzmaßnahmen fest.	s3- verboten bucket-level-public-access	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Simple Storage Service (Amazon S3) -Buckets nicht öffentlich zugänglich sind. Diese Regel trägt dazu bei, sensible Daten vor unbefugten Remote-Benutzern zu schützen, indem sie den öffentlichen Zugriff auf Bucket-Ebene verhindert.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
GLBA-SEC.501(b)	Zur Förderung der in Unterabschnitt (a) dargelegten Richtlinie legen alle in Abschnitt 505(a) beschriebenen Behörden angemessene Standards für die ihrer Gerichtsbarkeit unterstehenden Finanzinstitute in Bezug auf administrative, technische und physische Schutzmaßnahmen fest.	s-3 bucket-public-write-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie nur autorisierten Benutzern, Prozessen und Geräten Zugriff auf Amazon Simple Storage Service (Amazon S3) - Buckets gewähren. Die Verwaltung des Zugriffs sollte mit der Klassifizierung der Daten übereinstimmen.
GLBA-SEC.501(b)	Zur Förderung der in Unterabschnitt (a) dargelegten Richtlinie legen alle in Abschnitt 505(a) beschriebenen Behörden angemessene Standards für die ihrer Gerichtsbarkeit unterstehenden Finanzinstitute in Bezug auf administrative, technische und physische Schutzmaßnahmen fest.	ssm-document-not-public	Stellen Sie sicher, dass AWS Systems Manager (SSM) - Dokumente nicht öffentlich sind, da dies einen unbeabsichtigten Zugriff auf Ihre SSM-Dokumente ermöglichen kann. Ein öffentliches SSM-Dokument kann Informationen über Ihr Konto, Ihre Ressourcen und internen Prozesse preisgeben.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
GLBA-SEC.501(b)	Zur Förderung der in Unterabschnitt (a) dargelegten Richtlinie legen alle in Abschnitt 505(a) beschriebenen Behörden angemessene Standards für die ihrer Gerichtsbarkeit unterstehenden Finanzinstitute in Bezug auf administrative, technische und physische Schutzmaßnahmen fest.	subnet-auto-assign-public-ip-deaktiviert	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon Virtual Private Cloud (VPC) -Subnetzen nicht automatisch eine öffentliche IP-Adresse zugewiesen wird. Amazon Elastic Compute Cloud (EC2) -Instances, die in Subnetzen gestartet werden, in denen dieses Attribut aktiviert ist, haben ihrer primären Netzwerkschnittstelle eine öffentliche IP-Adresse zugewiesen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
GLBA-SEC.501(b)	Zur Förderung der in Unterabschnitt (a) dargelegten Richtlinie legen alle in Abschnitt 505(a) beschriebenen Behörden angemessene Standards für die ihrer Gerichtsbarkeit unterstehenden Finanzinstitute in Bezug auf administrative, technische und physische Schutzmaßnahmen fest.	vpc-sg-open-only-to-authorized-ports	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass gemeinsame Ports für Amazon Elastic Compute Cloud (Amazon EC2) -Sicherheitsgruppen eingeschränkt sind. Wenn der Zugriff auf Ports nicht auf vertrauenswürdige Quellen beschränkt wird, kann dies zu Angriffen auf die Verfügbarkeit, Integrität und Vertraulichkeit von Systemen führen. Durch die Beschränkung des Zugriffs auf Ressourcen innerhalb einer Sicherheitsgruppe aus dem Internet (0.0.0.0/0) kann der Remote-Zugriff auf interne Systeme gesteuert werden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
GLBA-SEC.501(b)	Zur Förderung der in Unterabschnitt (a) dargelegten Richtlinie legen alle in Abschnitt 505(a) beschriebenen Behörden angemessene Standards für die ihrer Gerichtsbarkeit unterstehenden Finanzinstitute in Bezug auf administrative, technische und physische Schutzmaßnahmen fest.	opensearch-in-vpc-only	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass sich Amazon OpenSearch Service-Domains innerhalb einer Amazon Virtual Private Cloud (Amazon VPC) befinden. Eine Amazon OpenSearch Service-Domain innerhalb einer Amazon VPC ermöglicht die sichere Kommunikation zwischen Amazon OpenSearch Service und anderen Services innerhalb der Amazon VPC, ohne dass ein Internet-Gateway, ein NAT-Gerät oder eine VPN-Verbindung erforderlich ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
GLBA-SEC.501(b)(1)	Zur Förderung der in Unterabschnitt (a) dargelegten Richtlinie legen alle in Abschnitt 505(a) beschriebenen Behörden angemessene Standards für die ihrer Gerichtsbarkeit unterstehenden Finanzinstitute in Bezug auf administrative, technische und physische Schutzmaßnahmen fest (1), um die Sicherheit und Vertraulichkeit von Kundendatensätzen und -informationen zu gewährleisten.	api-gw-cache-enabled-und verschlüsselt	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass die Verschlüsselung für den Cache Ihrer API-Gateway-Stufe aktiviert ist. Da für die API-Methode sensible Daten erfasst werden können, sollten Sie die Verschlüsselung von Daten im Ruhezustand aktivieren, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
GLBA-SEC.501(b)(1)	Zur Förderung der in Unterabschnitt (a) dargelegten Richtlinie legen alle in Abschnitt 505(a) beschriebenen Behörden angemessene Standards für die ihrer Gerichtsbarkeit unterstehenden Finanzinstitute in Bezug auf administrative, technische und physische Schutzmaßnahmen fest (1), um die Sicherheit und Vertraulichkeit von Kundendatensätzen und -informationen zu gewährleisten.	cloud-trail-encryption-enabled	Zum Schutz von eventuell vorhandenen sensiblen Daten sowie Daten im Ruhezustand müssen Sie sicherstellen, dass die Verschlüsselung für Ihre AWS CloudTrail aktiviert ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
GLBA-SEC.501(b)(1)	Zur Förderung der in Unterabschnitt (a) dargelegten Richtlinie legen alle in Abschnitt 505(a) beschriebenen Behörden angemessene Standards für die ihrer Gerichtsbarkeit unterstehenden Finanzinstitute in Bezug auf administrative, technische und physische Schutzmaßnahmen fest (1), um die Sicherheit und Vertraulichkeit von Kundendatensätzen und -informationen zu gewährleisten.	cloudwatch-log-group-encrypted	Um sensible Daten im Speicher zu schützen, stellen Sie sicher, dass die Verschlüsselung für Ihre Amazon CloudWatch Log Groups aktiviert ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
GLBA-SEC.501(b)(1)	Zur Förderung der in Unterabschnitt (a) dargelegten Richtlinie legen alle in Abschnitt 505(a) beschriebenen Behörden angemessene Standards für die ihrer Gerichtsbarkeit unterstehenden Finanzinstitute in Bezug auf administrative, technische und physische Schutzmaßnahmen fest (1), um die Sicherheit und Vertraulichkeit von Kundendatensätzen und -informationen zu gewährleisten.	efs-encrypted-check	Aktivieren Sie die Verschlüsselung für Ihr Amazon Elastic File System (EFS), um eventuell vorhandene sensible Daten sowie Daten im Ruhezustand zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
GLBA-SEC.501(b)(1)	Zur Förderung der in Unterabschnitt (a) dargelegten Richtlinie legen alle in Abschnitt 505(a) beschriebenen Behörden angemessene Standards für die ihrer Gerichtsbarkeit unterstehenden Finanzinstitute in Bezug auf administrative, technische und physische Schutzmaßnahmen fest (1), um die Sicherheit und Vertraulichkeit von Kundendatensätzen und -informationen zu gewährleisten.	elasticsearch-encrypted-at-rest	Da sensible Daten vorhanden sein können und um Daten im Ruhezustand zu schützen, sollten Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon OpenSearch Service (OpenSearch Service) -Domains aktiviert ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
GLBA-SEC.501(b)(1)	Zur Förderung der in Unterabschnitt (a) dargelegten Richtlinie legen alle in Abschnitt 505(a) beschriebenen Behörden angemessene Standards für die ihrer Gerichtsbarkeit unterstehenden Finanzinstitute in Bezug auf administrative, technische und physische Schutzmaßnahmen fest (1), um die Sicherheit und Vertraulichkeit von Kundendatensätzen und -informationen zu gewährleisten.	encrypted-volumes	Aktivieren Sie die Verschlüsselung für Ihre Amazon-Elastic-Block-Store (Amazon-EBS)-Volumes, um eventuell vorhandene sensible Daten sowie Daten im Ruhezustand zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
GLBA-SEC.501(b)(1)	Zur Förderung der in Unterabschnitt (a) dargelegten Richtlinie legen alle in Abschnitt 505(a) beschriebenen Behörden angemessene Standards für die ihrer Gerichtsbarkeit unterstehenden Finanzinstitute in Bezug auf administrative, technische und physische Schutzmaßnahmen fest (1), um die Sicherheit und Vertraulichkeit von Kundendatensätzen und -informationen zu gewährleisten.	rds-storage-encrypted	Zum Schutz von Daten im Ruhezustand müssen Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon Relational Database Service (Amazon RDS)-Instances aktiviert ist. Um eventuell vorhandene sensible Daten im Ruhezustand in Amazon-RDS-Instances zu schützen, muss die Verschlüsselung von Daten im Ruhezustand aktiviert sein.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
GLBA-SEC.501(b)(1)	Zur Förderung der in Unterabschnitt (a) dargelegten Richtlinie legen alle in Abschnitt 505(a) beschriebenen Behörden angemessene Standards für die ihrer Gerichtsbarkeit unterstehenden Finanzinstitute in Bezug auf administrative, technische und physische Schutzmaßnahmen fest (1), um die Sicherheit und Vertraulichkeit von Kundendatensätzen und -informationen zu gewährleisten.	redshift-cluster-configuration-check	Um Daten im Ruhezustand zu schützen, muss die Verschlüsselung für Ihre Amazon-Redshift-Cluster aktiviert sein. Sie müssen auch sicherstellen, dass die erforderlichen Konfigurationen auf Amazon-Redshift-Clustern bereitgestellt werden. Die Prüfungsprotokollierung muss aktiviert sein, um Informationen zu Verbindungen und Benutzeraktivitäten in der Datenbank bereitzustellen. Diese Regel erfordert, dass ein Wert für clusterDbEncrypted (Config Default: TRUE) und LoggingEnabled (Config Default: TRUE) gesetzt ist. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
GLBA-SEC.501(b)(1)	Zur Förderung der in Unterabschnitt (a) dargelegten Richtlinie legen alle in Abschnitt 505(a) beschriebenen Behörden angemessene Standards für die ihrer Gerichtsbarkeit unterstehenden Finanzinstitute in Bezug auf administrative, technische und physische Schutzmaßnahmen fest (1), um die Sicherheit und Vertraulichkeit von Kundendatensätzen und -informationen zu gewährleisten.	s3-aktiviert bucket-server-side-encryption	Zum Schutz von Daten im Ruhezustand müssen Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon Simple Storage Service (Amazon S3)-Buckets aktiviert ist. Um eventuell vorhandene sensible Daten im Ruhezustand in Amazon-S3-Buckets zu schützen, muss die Verschlüsselung aktiviert sein.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
GLBA-SEC.501(b)(1)	Zur Förderung der in Unterabschnitt (a) dargelegten Richtlinie legen alle in Abschnitt 505(a) beschriebenen Behörden angemessene Standards für die ihrer Gerichtsbarkeit unterstehenden Finanzinstitute in Bezug auf administrative, technische und physische Schutzmaßnahmen fest (1), um die Sicherheit und Vertraulichkeit von Kundendatensätzen und -informationen zu gewährleisten.	sagemaker-endpoint-configuration-kms-key-konfiguriert	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass die Verschlüsselung mit dem AWS Key Management Service (AWS KMS) für Ihren Endpunkt aktiviert ist. SageMaker Da sensible Daten auf dem SageMaker Endgerät gespeichert werden können, sollten Sie die Verschlüsselung im Ruhezustand aktivieren, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
GLBA-SEC.501(b)(1)	Zur Förderung der in Unterabschnitt (a) dargelegten Richtlinie legen alle in Abschnitt 505(a) beschriebenen Behörden angemessene Standards für die ihrer Gerichtsbarkeit unterstehenden Finanzinstitute in Bezug auf administrative, technische und physische Schutzmaßnahmen fest (1), um die Sicherheit und Vertraulichkeit von Kundendatensätzen und -informationen zu gewährleisten.	sagemaker-notebook-instance-kms-schlüsselkonfiguriert	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass die Verschlüsselung mit dem AWS Key Management Service (AWS KMS) für Ihr Notebook aktiviert ist. SageMaker Da vertrauliche Daten im SageMaker Notebook gespeichert werden können, sollten Sie die Verschlüsselung im Ruhezustand aktivieren, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
GLBA-SEC.501(b)(1)	Zur Förderung der in Unterabschnitt (a) dargelegten Richtlinie legen alle in Abschnitt 505(a) beschriebenen Behörden angemessene Standards für die ihrer Gerichtsbarkeit unterstehenden Finanzinstitute in Bezug auf administrative, technische und physische Schutzmaßnahmen fest (1), um die Sicherheit und Vertraulichkeit von Kundendatensätzen und -informationen zu gewährleisten.	sns-encrypted-kms	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass Ihre Amazon Simple Notification Service (Amazon SNS) -Themen mit dem AWS Key Management Service (AWS KMS) verschlüsselt werden müssen. Um eventuell vorhandene sensible Daten im Ruhezustand in veröffentlichten Nachrichten zu schützen, muss die Verschlüsselung von Daten im Ruhezustand aktiviert sein.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
GLBA-SEC.501(b)(1)	Zur Förderung der in Unterabschnitt (a) dargelegten Richtlinie legen alle in Abschnitt 505(a) beschriebenen Behörden angemessene Standards für die ihrer Gerichtsbarkeit unterstehenden Finanzinstitute in Bezug auf administrative, technische und physische Schutzmaßnahmen fest (1), um die Sicherheit und Vertraulichkeit von Kundendatensätzen und -informationen zu gewährleisten.	ec2- ebs-encryption-by-default	Zum Schutz von Daten im Ruhezustand müssen Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon Elastic Block Store (Amazon EBS)-Volumes aktiviert ist. Da sensible Daten auch im Ruhezustand vorhanden sein können, sollten Sie die Verschlüsselung im Ruhezustand aktivieren, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
GLBA-SEC.501(b)(1)	Zur Förderung der in Unterabschnitt (a) dargelegten Richtlinie legen alle in Abschnitt 505(a) beschriebenen Behörden angemessene Standards für die ihrer Gerichtsbarkeit unterstehenden Finanzinstitute in Bezug auf administrative, technische und physische Schutzmaßnahmen fest (1), um die Sicherheit und Vertraulichkeit von Kundendatensätzen und -informationen zu gewährleisten.	dynamodb-table-encrypted-kms	Stellen Sie sicher, dass die Verschlüsselung für Ihre Amazon-DynamoDB-Tabellen aktiviert ist. Um eventuell vorhandene sensible Daten im Ruhezustand in diesen Tabellen zu schützen, müssen Sie die Verschlüsselung von Daten im Ruhezustand aktivieren. Standardmäßig werden DynamoDB-Tabellen mit einem AWS eigenen Kundenhauptschlüssel (CMK) verschlüselt.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
GLBA-SEC.501(b)(1)	Zur Förderung der in Unterabschnitt (a) dargelegten Richtlinie legen alle in Abschnitt 505(a) beschriebenen Behörden angemessene Standards für die ihrer Gerichtsbarkeit unterstehenden Finanzinstitute in Bezug auf administrative, technische und physische Schutzmaßnahmen fest (1), um die Sicherheit und Vertraulichkeit von Kundendatensätzen und -informationen zu gewährleisten.	rds-snapshot-encrypted	Stellen Sie sicher, dass die Verschlüsselung für Ihre Amazon Relational Database Service (Amazon RDS)-Snapshots aktiviert ist. Da sensible Daten auch im Ruhezustand vorhanden sein können, sollten Sie die Verschlüsselung im Ruhezustand aktivieren, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
GLBA-SEC.501(b)(1)	Zur Förderung der in Unterabschnitt (a) dargelegten Richtlinie legen alle in Abschnitt 505(a) beschriebenen Behörden angemessene Standards für die ihrer Gerichtsbarkeit unterstehenden Finanzinstitute in Bezug auf administrative, technische und physische Schutzmaßnahmen fest (1), um die Sicherheit und Vertraulichkeit von Kundendatensätzen und -informationen zu gewährleisten.	s-3 default-encryption-kms	Stellen Sie sicher, dass die Verschlüsselung für Ihre Amazon Simple Storage Service (Amazon S3)-Buckets aktiviert ist. Um eventuell vorhandene sensible Daten im Ruhezustand in einem Amazon-S3-Bucket zu schützen, muss die Verschlüsselung aktiviert sein.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
GLBA-SEC.501(b)(1)	Zur Förderung der in Unterabschnitt (a) dargelegten Richtlinie legen alle in Abschnitt 505(a) beschriebenen Behörden angemessene Standards für die ihrer Gerichtsbarkeit unterstehenden Finanzinstitute in Bezug auf administrative, technische und physische Schutzmaßnahmen fest (1), um die Sicherheit und Vertraulichkeit von Kundendatensätzen und -informationen zu gewährleisten.	backup-recovery-point-encrypted	Stellen Sie sicher, dass die Verschlüsselung für Ihre AWS Backup-Wiederherstellungspunkte aktiviert ist. Da sensible Daten auch im Ruhezustand vorhanden sein können, sollten Sie die Verschlüsselung im Ruhezustand aktivieren, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
GLBA-SEC.501(b)(1)	Zur Förderung der in Unterabschnitt (a) dargelegten Richtlinie legen alle in Abschnitt 505(a) beschriebenen Behörden angemessene Standards für die ihrer Gerichtsbarkeit unterstehenden Finanzinstitute in Bezug auf administrative, technische und physische Schutzmaßnahmen fest (1), um die Sicherheit und Vertraulichkeit von Kundendatensätzen und -informationen zu gewährleisten.	elasticsearch-node-to-node-Verschlüsselungsprüfung	Stellen Sie sicher, dass die node-to-node Verschlüsselung für Amazon OpenSearch Service aktiviert ist. Node-to-nodeVerschlüsselung ermöglicht die TLS 1.2-Verschlüsselung für die gesamte Kommunikation innerhalb der Amazon Virtual Private Cloud (Amazon VPC). Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
GLBA-SEC.501(b)(1)	Zur Förderung der in Unterabschnitt (a) dargelegten Richtlinie legen alle in Abschnitt 505(a) beschriebenen Behörden angemessene Standards für die ihrer Gerichtsbarkeit unterstehenden Finanzinstitute in Bezug auf administrative, technische und physische Schutzmaßnahmen fest (1), um die Sicherheit und Vertraulichkeit von Kundendatensätzen und -informationen zu gewährleisten.	codebuild-project-s3-Log-verschlüsselt	Um sensible Daten im Ruhezustand zu schützen, stellen Sie sicher, dass die Verschlüsselung für Ihre in Amazon S3 gespeicherten AWS CodeBuild Protokolle aktiviert ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
GLBA-SEC.501(b)(1)	Zur Förderung der in Unterabschnitt (a) dargelegten Richtlinie legen alle in Abschnitt 505(a) beschriebenen Behörden angemessene Standards für die ihrer Gerichtsbarkeit unterstehenden Finanzinstitute in Bezug auf administrative, technische und physische Schutzmaßnahmen fest (1), um die Sicherheit und Vertraulichkeit von Kundendatensätzen und -informationen zu gewährleisten.	codebuild-project-artifact-encryption	Um sensible Daten im Speicher zu schützen, stellen Sie sicher, dass die Verschlüsselung für Ihre AWS CodeBuild Artefakte aktiviert ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
GLBA-SEC.501(b)(1)	Zur Förderung der in Unterabschnitt (a) dargelegten Richtlinie legen alle in Abschnitt 505(a) beschriebenen Behörden angemessene Standards für die ihrer Gerichtsbarkeit unterstehenden Finanzinstitute in Bezug auf administrative, technische und physische Schutzmaßnahmen fest (1), um die Sicherheit und Vertraulichkeit von Kundendatensätzen und -informationen zu gewährleisten.	opensearch-encrypted-at-rest	Da sensible Daten vorhanden sein können und um Daten im Ruhezustand zu schützen, sollten Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon OpenSearch Service-Domains aktiviert ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
GLBA-SEC.501(b)(1)	Zur Förderung der in Unterabschnitt (a) dargelegten Richtlinie legen alle in Abschnitt 505(a) beschriebenen Behörden angemessene Standards für die ihrer Gerichtsbarkeit unterstehenden Finanzinstitute in Bezug auf administrative, technische und physische Schutzmaßnahmen fest (1), um die Sicherheit und Vertraulichkeit von Kundendatensätzen und -informationen zu gewährleisten.	opensearch-node-to-node-Verschlüsselungsprüfung	Stellen Sie sicher, dass die node-to-node Verschlüsselung für Amazon OpenSearch Service aktiviert ist. Node-to-nodeVerschlüsselung ermöglicht die TLS 1.2-Verschlüsselung für die gesamte Kommunikation innerhalb der Amazon Virtual Private Cloud (Amazon VPC). Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
GLBA-SEC.501(b)(1)	Zur Förderung der in Unterabschnitt (a) dargelegten Richtlinie legen alle in Abschnitt 505(a) beschriebenen Behörden angemessene Standards für die ihrer Gerichtsbarkeit unterstehenden Finanzinstitute in Bezug auf administrative, technische und physische Schutzmaßnahmen fest (1), um die Sicherheit und Vertraulichkeit von Kundendatensätzen und -informationen zu gewährleisten.	kinesis-stream-encrypted	Aktivieren Sie die Verschlüsselung für Ihre Amazon-Kinesis-Streams, um eventuell vorhandene sensible Daten sowie Daten im Ruhezustand zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
GLBA-SEC.501(b)(2)	Zur Förderung der in Unterabschnitt (a) dargelegten Richtlinie legen alle in Abschnitt 505(a) beschriebenen Behörden angemessene Standards für die ihrer Gerichtsbarkeit unterstehenden Finanzinstitute in Bezug auf administrative, technische und physische Schutzmaßnahmen fest (2), um vorhersehbare Bedrohungen oder Gefahren für die Sicherheit und Vertraulichkeit solcher Datensätze abzuwenden.	guardduty-enabled-centralized	Amazon GuardDuty kann mithilfe von Threat Intelligence Feeds helfen, potenzielle Cybersicherheitsereignisse zu überwachen und zu erkennen. Dazu gehören Listen mit bösartigen IPs und maschinellen Lernmethoden zur Identifizierung unerwarteter, nicht autorisierter und bösartiger Aktivitäten in Ihrer AWS Cloud-Umgebung.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
GLBA-SEC.501(b)(2)	Zur Förderung der in Unterabschnitt (a) dargelegten Richtlinie legen alle in Abschnitt 505(a) beschriebenen Behörden angemessene Standards für die ihrer Gerichtsbarkeit unterstehenden Finanzinstitute in Bezug auf administrative, technische und physische Schutzmaßnahmen fest (2), um vorhersehbare Bedrohungen oder Gefahren für die Sicherheit und Vertraulichkeit solcher Datensätze abzuwenden.	securityhub-enabled	AWS Security Hub hilft bei der Überwachung von unbefugtem Personal, Verbindungen, Geräten und Software. AWS Security Hub aggregiert, organisiert und priorisiert die Sicherheitswarnungen oder Ergebnisse mehrerer Dienste. AWS Einige dieser Dienste sind Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer und AWS Firewall Manager sowie AWS Partnerlösungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
GLBA-SEC.501(b)(3)	Zur Förderung der in Unterabschnitt (a) dargelegten Richtlinie legen alle in Abschnitt 505(a) beschriebenen Behörden angemessene Standards für die ihrer Gerichtsbarkeit unterstehenden Finanzinstitute in Bezug auf administrative, technische und physische Schutzmaßnahmen fest (3), um den unerlaubten Zugriff oder die Verwendung solcher Datensätze oder Informationen und dadurch entstehende schwerwiegende Nachteile oder Unannehmlichkeiten für Kunden zu verhindern.	secretsmanager-rotation-enabled-check	Diese Regel stellt sicher, dass bei AWS Secrets Manager Manager-Geheimnissen die Rotation aktiviert ist. Die regelmäßige Rotation von Secrets kann den Zeitraum verkürzen, in dem ein Secret aktiv ist, und möglicherweise die Auswirkungen auf das Unternehmen verringern, falls das Secret kompromittiert wird.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
GLBA-SEC.501(b)(3)	Zur Förderung der in Unterabschnitt (a) dargelegten Richtlinie legen alle in Abschnitt 505(a) beschriebenen Behörden angemessene Standards für die ihrer Gerichtsbarkeit unterstehenden Finanzinstitute in Bezug auf administrative, technische und physische Schutzmaßnahmen fest (3), um den unerlaubten Zugriff oder die Verwendung solcher Datensätze oder Informationen und dadurch entstehende schwerwiegende Nachteile oder Unannehmlichkeiten für Kunden zu verhindern.	access-keys-rotated	Die Anmeldeinformationen für autorisierte Geräte, Benutzer und Prozesse werden geprüft, indem sichergestellt wird, dass die IAM-Zugriffsschlüssel gemäß den Vorgaben der Unternehmensrichtlinie rotiert werden. Das regelmäßige Ändern der Zugriffsschlüssel ist eine bewährte Sicherheitsmethode. Es verkürzt den Zeitraum, in dem ein Zugriffsschlüssel aktiv ist, und reduziert die Auswirkungen auf das Unternehmen, wenn die Schlüssel kompromittiert werden. Diese Regel erfordert einen Wert für die Zugriffsschlüssel-Rotation (Standardkonfiguration: 90). Der tatsächliche Wert muss den Richtlini

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			en Ihrer Organisation entsprechen.
GLBA-SEC.501(b)(3)	Zur Förderung der in Unterabschnitt (a) dargelegten Richtlinie legen alle in Abschnitt 505(a) beschriebenen Behörden angemessene Standards für die ihrer Gerichtsbarkeit unterstehenden Finanzinstitute in Bezug auf administrative, technische und physische Schutzmaßnahmen fest (3), um den unerlaubten Zugriff oder die Verwendung solcher Datensätze oder Informationen und dadurch entstehende schwerwiegende Nachteile oder Unannehmlichkeiten für Kunden zu verhindern.	iam-group-has-users-überprüfen	AWS Identity and Access Management (IAM) kann Ihnen helfen, die Prinzipien der geringsten Rechte und der Aufgabentrennung mit Zugriffsberechtigungen und Autorisierungen zu integrieren, indem sichergestellt wird, dass IAM-Gruppen mindestens einen Benutzer haben. Die Einteilung von Benutzern in Gruppen auf der Grundlage der ihnen zugewiesenen Berechtigungen oder ihrer Funktion ist eine Möglichkeit, das Prinzip der geringsten Berechtigung zu implementieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
GLBA-SEC.501(b)(3)	Zur Förderung der in Unterabschnitt (a) dargelegten Richtlinie legen alle in Abschnitt 505(a) beschriebenen Behörden angemessene Standards für die ihrer Gerichtsbarkeit unterstehenden Finanzinstitute in Bezug auf administrative, technische und physische Schutzmaßnahmen fest (3), um den unerlaubten Zugriff oder die Verwendung solcher Datensätze oder Informationen und dadurch entstehende schwerwiegende Nachteile oder Unannehmlichkeiten für Kunden zu verhindern.	iam-password-policy	Die Identitäten und Anmeldeinformationen werden auf der Grundlage einer organisatorischen IAM-Passwortrichtlinie ausgestellt, verwaltet und verifiziert. Sie erfüllen oder übertreffen die Anforderungen von NIST SP 800-63 und dem Standard „Best Practices“ von AWS Foundational Security für die Passwortstärke. Mit dieser Regel können Sie optional RequireUppercaseCharacters (Wert für AWS grundlegende Sicherheitsbewährte Methoden: wahr), RequireLowercaseCharacters (Wert für bewährte Methoden für AWS grundlegende Sicherheit: wahr), RequireSymbols (Wert für bewährte Methoden für AWS grundlegende Sicherheit:

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			wahr), RequireNumbers (Wert für bewährte Methoden für AWS grundlegende Sicherheit: wahr), MinimumPasswordLength (Wert für bewährte Methoden für AWS grundlegende Sicherheit: 14), PasswordReusePrevention (Wert für bewährte Methoden für AWS grundlegende Sicherheit: 24) und MaxPasswordAge (Wert für bewährte Methoden für AWS grundlegende Sicherheit: 90) für Ihr IAM festlegen. Kennwortrichtlinie. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
GLBA-SEC.501(b)(3)	Zur Förderung der in Unterabschnitt (a) dargelegten Richtlinie legen alle in Abschnitt 505(a) beschriebenen Behörden angemessene Standards für die ihrer Gerichtsbarkeit unterstehenden Finanzinstitute in Bezug auf administrative, technische und physische Schutzmaßnahmen fest (3), um den unerlaubten Zugriff oder die Verwendung solcher Datensätze oder Informationen und dadurch entstehende schwerwiegende Nachteile oder Unannehmlichkeiten für Kunden zu verhindern.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) kann Ihnen dabei helfen, die Prinzipien der geringsten Rechte und der Aufgabentrennung in Zugriffsberechtigungen und Autorisierungen zu integrieren und so zu verhindern, dass Richtlinien „Effect“: „Allow“ mit „Action“: „*“ anstelle von „Resource“: „*“ enthalten. Wenn Benutzern mehr Rechte eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und der Aufgabentrennung verstoßen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
GLBA-SEC.501(b)(3)	Zur Förderung der in Unterabschnitt (a) dargelegten Richtlinie legen alle in Abschnitt 505(a) beschriebenen Behörden angemessene Standards für die ihrer Gerichtsbarkeit unterstehenden Finanzinstitute in Bezug auf administrative, technische und physische Schutzmaßnahmen fest (3), um den unerlaubten Zugriff oder die Verwendung solcher Datensätze oder Informationen und dadurch entstehende schwerwiegende Nachteile oder Unannehmlichkeiten für Kunden zu verhindern.	iam-root-access-key-überprüfen	Der Zugriff auf Systeme und Ressourcen kann gesteuert werden, indem überprüft wird, ob der Root-Benutzer keine Zugriffsschlüssel mit seiner AWS Identity and Access Management (IAM) -Rolle verknüpft hat. Stellen Sie sicher, dass die Root-Zugriffsschlüssel gelöscht werden. Erstellen und verwenden Sie stattdessen rollenbasierte Funktionen, AWS-Konten um das Prinzip der geringsten Funktionalität zu berücksichtigen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
GLBA-SEC.501(b)(3)	Zur Förderung der in Unterabschnitt (a) dargelegten Richtlinie legen alle in Abschnitt 505(a) beschriebenen Behörden angemessene Standards für die ihrer Gerichtsbarkeit unterstehenden Finanzinstitute in Bezug auf administrative, technische und physische Schutzmaßnahmen fest (3), um den unerlaubten Zugriff oder die Verwendung solcher Datensätze oder Informationen und dadurch entstehende schwerwiegende Nachteile oder Unannehmlichkeiten für Kunden zu verhindern.	iam-user-group-membership-überprüfen	AWS Identity and Access Management (IAM) kann Ihnen helfen, Zugriffsberechtigungen und Autorisierungen einzuschränken, indem sichergestellt wird, dass Benutzer Mitglieder mindestens einer Gruppe sind. Wenn Benutzern mehr Berechtigungen eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und Aufgabentrennung verstoßen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
GLBA-SEC.501(b)(3)	Zur Förderung der in Unterabschnitt (a) dargelegten Richtlinie legen alle in Abschnitt 505(a) beschriebenen Behörden angemessene Standards für die ihrer Gerichtsbarkeit unterstehenden Finanzinstitute in Bezug auf administrative, technische und physische Schutzmaßnahmen fest (3), um den unerlaubten Zugriff oder die Verwendung solcher Datensätze oder Informationen und dadurch entstehende schwerwiegende Nachteile oder Unannehmlichkeiten für Kunden zu verhindern.	iam-user-no-policies-überprüfen	Diese Regel stellt sicher, dass AWS Identity and Access Management (IAM) -Richtlinien nur Gruppen oder Rollen zugewiesen werden, um den Zugriff auf Systeme und Ressourcen zu kontrollieren. Die Zuweisung von Berechtigungen auf Gruppen- oder Rollenebene trägt dazu bei, die Wahrscheinlichkeit zu verringern, dass eine Identität übermäßige Berechtigungen erhält oder beibehält.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
GLBA-SEC.501(b)(3)	Zur Förderung der in Unterabschnitt (a) dargelegten Richtlinie legen alle in Abschnitt 505(a) beschriebenen Behörden angemessene Standards für die ihrer Gerichtsbarkeit unterstehenden Finanzinstitute in Bezug auf administrative, technische und physische Schutzmaßnahmen fest (3), um den unerlaubten Zugriff oder die Verwendung solcher Datensätze oder Informationen und dadurch entstehende schwerwiegende Nachteile oder Unannehmlichkeiten für Kunden zu verhindern.	iam-user-unused-credentials-überprüfen	AWS Identity and Access Management (IAM) kann Ihnen bei Zugriffsberechtigungen und Autorisierungen helfen, indem es nach IAM-Passwörtern und Zugriffsschlüsseln sucht, die für einen bestimmten Zeitraum nicht verwendet wurden. Wenn ungenutzte Anmeldeinformationen identifiziert werden, müssen Sie sie deaktivieren und/oder entfernen, da dies gegen das Prinzip der geringsten Berechtigung verstoßen könnte. Für diese Regel müssen Sie einen Wert für das maxCredentialUsage Alter festlegen (Standardkonfiguration: 90). Der tatsächliche Wert muss den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
GLBA-SEC.501(b)(3)	Zur Förderung der in Unterabschnitt (a) dargelegten Richtlinie legen alle in Abschnitt 505(a) beschriebenen Behörden angemessene Standards für die ihrer Gerichtsbarkeit unterstehenden Finanzinstitute in Bezug auf administrative, technische und physische Schutzmaßnahmen fest (3), um den unerlaubten Zugriff oder die Verwendung solcher Datensätze oder Informationen und dadurch entstehende schwerwiegende Nachteile oder Unannehmlichkeiten für Kunden zu verhindern.	s-3 bucket-policy-grantee-check	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie s3_bucket_policy_grantee_check aktivieren. Diese Regel prüft, ob der vom Amazon S3 S3-Bucket gewährte Zugriff durch die von Ihnen bereitgestellten AWS Principals, Verbundbenutzer, Service Principals, IP-Adressen oder Amazon Virtual Private Cloud (Amazon VPC) IDs eingeschränkt ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
GLBA-SEC.501(b)(3)	Zur Förderung der in Unterabschnitt (a) dargelegten Richtlinie legen alle in Abschnitt 505(a) beschriebenen Behörden angemessene Standards für die ihrer Gerichtsbarkeit unterstehenden Finanzinstitute in Bezug auf administrative, technische und physische Schutzmaßnahmen fest (3), um den unerlaubten Zugriff oder die Verwendung solcher Datensätze oder Informationen und dadurch entstehende schwerwiegende Nachteile oder Unannehmlichkeiten für Kunden zu verhindern.	iam-policy-no-statements-with-full-access	Stellen Sie sicher, dass IAM-Aktionen nur auf die benötigten Aktionen beschränkt sind. Wenn Benutzern mehr Rechte eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und der Aufgabentrennung verstoßen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
GLBA-SEC.501(b)(3)	Zur Förderung der in Unterabschnitt (a) dargelegten Richtlinie legen alle in Abschnitt 505(a) beschriebenen Behörden angemessene Standards für die ihrer Gerichtsbarkeit unterstehenden Finanzinstitute in Bezug auf administrative, technische und physische Schutzmaßnahmen fest (3), um den unerlaubten Zugriff oder die Verwendung solcher Datensätze oder Informationen und dadurch entstehende schwerwiegende Nachteile oder Unannehmlichkeiten für Kunden zu verhindern.	mfa-enabled-for-iam-Konsolenzugriff	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass MFA für alle AWS Identity and Access Management (IAM) -Benutzer aktiviert ist, die über ein Konsolenkennwort verfügen. MFA sorgt für eine weitere Schutzebene zusätzlich zu den Anmeldeinformationen. Indem Sie MFA für Benutzer vorschreiben, können Sie Fälle kompromittierter Konten reduzieren und verhindern, dass unbefugte Benutzer auf vertrauliche Daten zugreifen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
GLBA-SEC.501(b)(3)	Zur Förderung der in Unterabschnitt (a) dargelegten Richtlinie legen alle in Abschnitt 505(a) beschriebenen Behörden angemessene Standards für die ihrer Gerichtsbarkeit unterstehenden Finanzinstitute in Bezug auf administrative, technische und physische Schutzmaßnahmen fest (3), um den unerlaubten Zugriff oder die Verwendung solcher Datensätze oder Informationen und dadurch entstehende schwerwiegende Nachteile oder Unannehmlichkeiten für Kunden zu verhindern.	opensearch-access-control-enabled	Stellen Sie sicher, dass eine differenzierte Zugriffskontrolle für Ihre Amazon OpenSearch Service-Domains aktiviert ist. Eine differenzierte Zugriffskontrolle bietet erweiterte Autorisierungsmechanismen, um den Zugriff auf Amazon Service-Domains mit den geringsten Rechten zu erreichen. OpenSearch Es ermöglicht eine rollenbasierte Zugriffskontrolle auf die Domain sowie Sicherheit auf Index-, Dokument- und Feldebene, Unterstützung für OpenSearch Service-Dashboards, Mehrmandantenfähigkeit und HTTP-Basisauthentifizierung für Service und Kibana. OpenSearch

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
GLBA-SEC.501(b)(3)	Zur Förderung der in Unterabschnitt (a) dargelegten Richtlinie legen alle in Abschnitt 505(a) beschriebenen Behörden angemessene Standards für die ihrer Gerichtsbarkeit unterstehenden Finanzinstitute in Bezug auf administrative, technische und physische Schutzmaßnahmen fest (3), um den unerlaubten Zugriff oder die Verwendung solcher Datensätze oder Informationen und dadurch entstehende schwerwiegende Nachteile oder Unannehmlichkeiten für Kunden zu verhindern.	ecs-containers-readonly-access	Die Aktivierung des schreibgeschützten Zugriffs auf Amazon Elastic Container Service (ECS)-Container kann dazu beitragen, das Prinzip der geringsten Berechtigung einzuhalten. Diese Option kann Angriffsvektoren reduzieren, da das Dateisystem der Container-Instance nur geändert werden kann, wenn es über ausdrückliche Lese- und Schreibberechtigungen verfügt.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
GLBA-SEC.501(b)(3)	Zur Förderung der in Unterabschnitt (a) dargelegten Richtlinie legen alle in Abschnitt 505(a) beschriebenen Behörden angemessene Standards für die ihrer Gerichtsbarkeit unterstehenden Finanzinstitute in Bezug auf administrative, technische und physische Schutzmaßnahmen fest (3), um den unerlaubten Zugriff oder die Verwendung solcher Datensätze oder Informationen und dadurch entstehende schwerwiegende Nachteile oder Unannehmlichkeiten für Kunden zu verhindern.	efs-access-point-enforce-Stammverzeichnis	Die Durchsetzung eines Stammverzeichnisses für einen Amazon-Elastic-File-System (Amazon-EFS)-Zugangspunkt trägt dazu bei, den Datenzugriff einzuschränken, indem sichergestellt wird, dass Benutzer des Zugangspunkts nur auf Dateien des angegebenen Unterverzeichnisses zugreifen können.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
GLBA-SEC.501(b)(3)	Zur Förderung der in Unterabschnitt (a) dargelegten Richtlinie legen alle in Abschnitt 505(a) beschriebenen Behörden angemessene Standards für die ihrer Gerichtsbarkeit unterstehenden Finanzinstitute in Bezug auf administrative, technische und physische Schutzmaßnahmen fest (3), um den unerlaubten Zugriff oder die Verwendung solcher Datensätze oder Informationen und dadurch entstehende schwerwiegende Nachteile oder Unannehmlichkeiten für Kunden zu verhindern.	efs-access-point-enforce-Benutzeridentität	Um die Implementierung des Prinzips der geringsten Rechte zu unterstützen, stellen Sie sicher, dass die Benutzerdurchsetzung für Ihr Amazon Elastic File System (Amazon EFS) aktiviert ist. Wenn diese Option aktiviert ist, ersetzt Amazon EFS den Benutzer und die Gruppe IDs des NFS-Clients durch die Identität, die auf dem Access Point für alle Dateisystemoperationen konfiguriert ist, und gewährt nur Zugriff auf diese erzwungene Benutzeridentität.

Vorlage

Die Vorlage ist verfügbar unter GitHub: Operational Best Practices for Gramm Leach Bliley Act (GLBA).

Bewährte Methoden für die Implementierung Anhang 11 zum EG-Leitfaden der Guten Herstellungspraxis

Konformitätspakete bieten ein allgemeines Compliance-Framework, das es Ihnen ermöglicht, mithilfe verwalteter oder benutzerdefinierter AWS Config Regeln und Abhilfemaßnahmen Kontrollen zur Sicherheits-, Betriebs- oder Kostenoptimierung durchzuführen. AWS Config Conformance Packs dienen als Beispielvorlagen nicht dazu, die vollständige Einhaltung eines bestimmten Governance- oder Compliance-Standards sicherzustellen. Sie sind dafür verantwortlich, selbst zu beurteilen, ob Ihre Nutzung der Services den geltenden gesetzlichen und behördlichen Anforderungen entspricht.

Im Folgenden finden Sie ein Beispiel für eine Zuordnung zwischen dem GxP EU Annex 11 und den AWS Managed Config-Regeln. Jede Config-Regel gilt für eine bestimmte AWS Ressource und bezieht sich auf eine oder mehrere GxP EU Annex 11-Kontrollen. Eine Kontrolle nach Anhang 11 zum EG-Leitfaden der Guten Herstellungspraxis kann mehreren Config-Regeln zugeordnet werden. In der folgenden Tabelle finden Sie weitere Informationen und Anleitungen zu diesen Zuordnungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
1. Risikomanagement	Das Risikomanagement sollte während des gesamten Lebenszyklus des computergestützten Systems angewendet werden, wobei die Patientensicherheit, Dateninteglität und Produktqualität im Vordergrund stehen. Entscheidungen über den Umfang der Validierungs- und Dateninteglitätskontrollen sollten als Teil eines Risikoman	cloudtrail-enabled	AWS CloudTrail kann bei der Nichtabstreitbarkeit helfen, indem Aktionen und API-Aufrufe der AWS Management Console aufgezeichnet werden. Sie können die Benutzer und die Benutzer AWS-Konten , die einen AWS Dienst aufgerufen haben, die Quell-IP-Adresse, über die die Aufrufe generiert wurden, und den Zeitpunkt der Anrufe identifiz

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	agementsystem auf einer begründeten und dokumentierten Risikobewertung des computergestützten Systems beruhen.		ieren. Einzelheiten zu den erfassten Daten finden Sie in den AWS CloudTrail Datensatzinhalten.
1. Risikomanagement	Das Risikoman agement sollte während des gesamten Lebenszyk lus des computerg estützten Systems angewendet werden, wobei die Patienten sicherheit, Dateninte grität und Produktqu alität im Vordergru nd stehen. Entscheid ungen über den Umfang der Validieru ngs- und Dateninte gritätskontrollen sollten als Teil eines Risikoman agementsystem auf einer begründeten und dokumentierten Risikobewertung des computergestützten Systems beruhen.	securityhub-enabled	AWS Security Hub hilft bei der Überwachung von unbefugtem Personal, Verbindun gen, Geräten und Software. AWS Security Hub aggregiert, organisie rt und priorisie rt die Sicherhei tswarnungen oder Ergebnisse mehrerer Dienste. AWS Einig e dieser Dienste sind Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer und AWS Firewall Manager sowie AWS Partnerlösungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
4.2. Validierung – Kontrolle der Änderungen an der Dokumentation	Die Validierungsdokumentation sollte Änderungskontrolleinträge (falls zutreffend) und Berichte über alle während des Validierungsprozesses festgestellten Abweichungen enthalten.	cloudtrail-enabled	AWS CloudTrail kann durch die Aufzeichnung von Aktionen und API-Aufrufen in der AWS Management Console bei der Nichtabstreitbarkeit helfen. Sie können die Benutzer und die Benutzer AWS-Konten , die einen AWS Dienst aufgerufen haben, die Quell-IP-Adresse, über die die Aufrufe generiert wurden, und den Zeitpunkt der Anrufe identifizieren. Einzelheiten zu den erfassten Daten finden Sie in den AWS CloudTrail Datensatzinhalten.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
4.3. Validierung – Inventar	Es sollte eine aktuelle Liste aller relevante n Systeme und ihrer GMP-Funkt ionen (Inventar) verfügbar sein. Für kritische Systeme sollte eine aktuelle Systembeschreibung verfügbar sein, in der die physischen und logischen Anordnung en, Datenflüsse und Schnittstellen zu anderen Systemen oder Prozessen, alle Hardware- und Softwarevoraussetz ungen und Sicherhei tsmaßnahmen detailliert beschrieben werden.	ec2-manager instance-managed-by-systems	Eine Bestandsa ufnahme der Softwareplattforme n und Anwendung en innerhalb des Unternehmens ist möglich, indem Amazon Elastic Compute Cloud (Amazon EC2) - Instances mit AWS Systems Manager verwaltet werden. Verwenden Sie AWS Systems Manager, um detaillierte Systemkonfiguratio nen, Betriebssystem-Patch-Levels, Namen und Typ der Dienste, Softwareinstallati onen, Anwendung sname, Herausgeb er und Version sowie andere Details zu Ihrer Umgebung bereitzustellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
4.3. Validierung – Inventar	Es sollte eine aktuelle Liste aller relevante n Systeme und ihrer GMP-Funkt ionen (Inventar) verfügbar sein. Für kritische Systeme sollte eine aktuelle Systembeschreibung verfügbar sein, in der die physischen und logischen Anordnung en, Datenflüsse und Schnittstellen zu anderen Systemen oder Prozessen, alle Hardware- und Softwarevoraussetz ungen und Sicherhei tsmaßnahmen detailliert beschrieben werden.	ec2-prüfen managedinstance-as sociation-compliance-status	Verwenden Sie AWS Systems Manager Associati ons, um bei der Inventarisierung von Softwareplattforme n und Anwendung en innerhalb eines Unternehmens zu helfen. AWS Syste ms Manager weist Ihren verwalteten Instances einen Konfigurationsstat us zu und ermöglich t es Ihnen, Basiswert e für Betriebss ystem-Patch-Levels , Softwareinstallati onen, Anwendung skonfigurationen und andere Details zu Ihrer Umgebung festzulegen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
4.3. Validierung – Inventar	Es sollte eine aktuelle Liste aller relevante n Systeme und ihrer GMP-Funkt ionen (Inventar) verfügbar sein. Für kritische Systeme sollte eine aktuelle Systembeschreibung verfügbar sein, in der die physischen und logischen Anordnung en, Datenflüsse und Schnittstellen zu anderen Systemen oder Prozessen, alle Hardware- und Softwarevoraussetz ungen und Sicherhei tsmaßnahmen detailliert beschrieben werden.	ec2- security-group-attached-to -einperio disch	Um Ihnen die Verwaltung Ihres Asset-Inventars zu erleichtern, prüft diese Regel, ob Sicherhei tsgruppen an Amazon Elastic Compute Cloud (Amazon EC2) -Instances oder an eine elastic network interface angehängt sind. Wenn Ihre Sicherhei tsgruppen nicht solchen Ressource ntypen angehängt sind, werden sie möglicherweise nicht genutzt und somit nicht mehr benötigt.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
4.3. Validierung – Inventar	Es sollte eine aktuelle Liste aller relevante n Systeme und ihrer GMP-Funkt ionen (Inventar) verfügbar sein. Für kritische Systeme sollte eine aktuelle Systembeschreibung verfügbar sein, in der die physischen und logischen Anordnung en, Datenflüsse und Schnittstellen zu anderen Systemen oder Prozessen, alle Hardware- und Softwarevoraussetz ungen und Sicherhei tsmaßnahmen detailliert beschrieben werden.	ec2-stopped-instance	Aktivieren Sie diese Regel, um bei der Basiskonfiguration von Amazon Elastic Compute Cloud (Amazon EC2) - Instances zu helfen, indem Sie überprüfe n, ob EC2 Amazon-Instances gemäß den Standards Ihrer Organisation für mehr als die zulässige Anzahl von Tagen gestoppt wurden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
4.3. Validierung – Inventar	Es sollte eine aktuelle Liste aller relevante n Systeme und ihrer GMP-Funkt ionen (Inventar) verfügbar sein. Für kritische Systeme sollte eine aktuelle Systembeschreibung verfügbar sein, in der die physischen und logischen Anordnung en, Datenflüsse und Schnittstellen zu anderen Systemen oder Prozessen, alle Hardware- und Softwarevoraussetz ungen und Sicherhei tsmaßnahmen detailliert beschrieben werden.	eip-attached	Diese Regel stellt sicher, dass Elastic, die einer Amazon Virtual Private Cloud (Amazon VPC) IPs zugewiesen sind, an Amazon Elastic Compute Cloud (Amazon EC2) - Instances oder verwendete Elastic Network Interface s angehängt sind. Diese Regel hilft bei der Überwachu ng ungenutzter Inhalte EIPs in Ihrer Umgebung.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
4.3. Validierung – Inventar	Es sollte eine aktuelle Liste aller relevante n Systeme und ihrer GMP-Funkt ionen (Inventar) verfügbar sein. Für kritische Systeme sollte eine aktuelle Systembeschreibung verfügbar sein, in der die physischen und logischen Anordnung en, Datenflüsse und Schnittstellen zu anderen Systemen oder Prozessen, alle Hardware- und Softwarevoraussetz ungen und Sicherhei tsmaßnahmen detailliert beschrieben werden.	vpc-network-acl-un used-überprüfen	Diese Regel stellt sicher, dass Amazon Virtual Private Cloud (VPC)-Netzwerkzugr iffskontrolllisten verwendet werden. Die Überwachu ng ungenutzter Netzwerkzugriffsko ntrolllisten kann zu einer genauen Inventarisierung und Verwaltung Ihrer Umgebung beitragen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
4.8. Validierung – Datenübertragung	Wenn Daten in ein anderes Datenformat oder System übertragen werden, sollte bei der Validierung auch geprüft werden, dass weder Wert noch Bedeutung der Daten während dieses Migrationsprozesses verändert wurden.	aurora-resources-protected-by-Backup-Plan	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon Aurora Aurora-Ressourcen Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
4.8. Validierung – Datenübertragung	Wenn Daten in ein anderes Datenformat oder System übertragen werden, sollte bei der Validierung auch geprüft werden, dass weder Wert noch Bedeutung der Daten während dieses Migrationsprozesses verändert wurden.	backup-plan-min-frequency-and-min-retention-check	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihr AWS Backup-Plan auf eine Mindestfrequenz und Aufbewahrung festgelegt ist. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen. Mit dieser Regel können Sie die Parameter requiredFrequencyValue (Config default: 1), requiredRetentionDays (Config default: 35) und requiredFrequencyUnit

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			(Config default: days) festlegen. Der tatsächliche Wert muss den Anforderungen Ihrer Organisation entsprechen.
4.8. Validierung – Datenübertragung	Wenn Daten in ein anderes Datenformat oder System übertragen werden, sollte bei der Validierung auch geprüft werden, dass weder Wert noch Bedeutung der Daten während dieses Migrationsprozesses verändert wurden.	backup-recovery-point-encrypted	Stellen Sie sicher, dass die Verschlüsselung für Ihre AWS Backup-Wiederherstellungspunkte aktiviert ist. Da sensible Daten auch im Ruhezustand vorhanden sein können, sollten Sie die Verschlüsselung im Ruhezustand aktivieren, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
4.8. Validierung – Datenübertragung	Wenn Daten in ein anderes Datenformat oder System übertragen werden, sollte bei der Validierung auch geprüft werden, dass weder Wert noch Bedeutung der Daten während dieses Migrationsprozesses verändert wurden.	backup-recovery-point-manual-Löschen-deaktiviert	Stellen Sie sicher, dass Ihren AWS Backup-Wiederherstellungspunkten eine ressourcenbasierte Richtlinie zugeordnet ist, die das Löschen von Wiederherstellungspunkten verhindert. Die Verwendung einer ressourcenbasierten Richtlinie zur Verhinderung des Löschens von Wiederherstellungspunkten kann dazu beitragen, ein versehentliches oder absichtliches Löschen zu unterbinden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
4.8. Validierung – Datenübertragung	Wenn Daten in ein anderes Datenformat oder System übertragen werden, sollte bei der Validierung auch geprüft werden, dass weder Wert noch Bedeutung der Daten während dieses Migrationsprozesses verändert wurden.	backup-recovery-point-minimum-Aufbewahrungsprüfung	Um bei Datensicherungsprozessen zu helfen, stellen Sie sicher, dass für Ihre AWS Backup-Wiederherstellungspunkte eine Mindestaufbewahrungsdauer festgelegt ist. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen. Mit dieser Regel können Sie den Parameter requiredRetentionDays (Standardkonfiguration: 35) festlegen. Der tatsächliche Wert muss den Anforderu

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			ngen Ihrer Organisat ion entsprechen.
4.8. Validierung – Datenübertragung	Wenn Daten in ein anderes Datenform at oder System übertragen werden, sollte bei der Validieru ng auch geprüft werden, dass weder Wert noch Bedeutung der Daten während dieses Migration sprozesses verändert wurden.	db-instance-backup-enabled	Die Sicherung sfunktion von Amazon RDS erstellt Sicherung en Ihrer Datenbank en und Transakti onsprotokolle. Amazon RDS erstellt einen Snapshot für das Speichervolume Ihrer DB-Instance, sodass die gesamte DB-Instance gesichert wird. Sie können im System spezifische Aufbewahrungsfrist en festlegen, um Ihre Ausfallsicherheits anforderungen zu erfüllen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
4,8. Validierung – Datenübertragung	Wenn Daten in ein anderes Datenformat oder System übertragen werden, sollte bei der Validierung auch geprüft werden, dass weder Wert noch Bedeutung der Daten während dieses Migrationsprozesses verändert wurden.	dynamodb-in-backup-plan	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon DynamoDB-Tabellen Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
4.8. Validierung – Datenübertragung	Wenn Daten in ein anderes Datenform at oder System übertragen werden, sollte bei der Validieru ng auch geprüft werden, dass weder Wert noch Bedeutung der Daten während dieses Migration sprozesses verändert wurden.	dynamodb-pitr-enab led	Aktivieren Sie diese Regel, um zu überprüfen, ob die Informationen gesichert wurden. Es verwaltet auch die Backups, indem es sicherstellt, dass die point-in-time Wiederherstellung in Amazon DynamoDB aktiviert ist. Bei der Wiederherstellung werden fortlaufende Backups Ihrer Tabelle für die letzten 35 Tage gespeichert.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
4.8. Validierung – Datenübertragung	Wenn Daten in ein anderes Datenform at oder System übertragen werden, sollte bei der Validieru ng auch geprüft werden, dass weder Wert noch Bedeutung der Daten während dieses Migration sprozesses verändert wurden.	ebs-in-backup-plan	Stellen Sie zur Unterstützung der Datensicherungspro zesse sicher, dass Ihre Amazon Elastic Block Store (Amazon EBS) -Volumes Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwaltet er Backup-Service mit einer richtlini enbasierten Backup-Lösung. Diese Lösung vereinfacht Ihre Backup-Verwaltung und ermöglicht es Ihnen, Ihre geschäftl ichen und behördlic hen Anforderungen bezüglich Backups zu erfüllen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
4.8. Validierung – Datenübertragung	Wenn Daten in ein anderes Datenformat oder System übertragen werden, sollte bei der Validierung auch geprüft werden, dass weder Wert noch Bedeutung der Daten während dieses Migrationsprozesses verändert wurden.	ebs-optimized-instance	Eine optimierte Instance im Amazon Elastic Block Store (Amazon EBS) bietet zusätzliche, dedizierte Kapazität für Amazon-EBS-I/O-Vorgänge. Diese Optimierung bietet die beste Leistung für Ihr EBS-Volume, indem Konflikte zwischen Amazon-EBS-I/O und anderem Datenverkehr von Ihrer Instance minimiert werden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
4,8. Validierung – Datenübertragung	Wenn Daten in ein anderes Datenformat oder System übertragen werden, sollte bei der Validierung auch geprüft werden, dass weder Wert noch Bedeutung der Daten während dieses Migrationsprozesses verändert wurden.	ebs-resources-protected-by-Backup-Plan	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon Elastic Block Store (Amazon EBS) -Ressourcen Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihre Backup-Verwaltung und ermöglicht es Ihnen, Ihre geschäftlichen und behördlichen Anforderungen bezüglich Backups zu erfüllen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
4.8. Validierung – Datenübertragung	Wenn Daten in ein anderes Datenformat oder System übertragen werden, sollte bei der Validierung auch geprüft werden, dass weder Wert noch Bedeutung der Daten während dieses Migrationsprozesses verändert wurden.	ec2--Plan resources-protected-by-backup	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon Elastic Compute Cloud (Amazon EC2) -Ressourcen Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
4.8. Validierung – Datenübertragung	Wenn Daten in ein anderes Datenformat oder System übertragen werden, sollte bei der Validierung auch geprüft werden, dass weder Wert noch Bedeutung der Daten während dieses Migrationsprozesses verändert wurden.	efs-in-backup-plan	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon Elastic File System (Amazon EFS) -Dateisysteme Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
4.8. Validierung – Datenübertragung	Wenn Daten in ein anderes Datenformat oder System übertragen werden, sollte bei der Validierung auch geprüft werden, dass weder Wert noch Bedeutung der Daten während dieses Migrationsprozesses verändert wurden.	efs-resources-protected-by-Backup-Plan	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon Elastic File System (Amazon EFS) -Dateisysteme Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
4.8. Validierung – Datenübertragung	Wenn Daten in ein anderes Datenform at oder System übertragen werden, sollte bei der Validieru ng auch geprüft werden, dass weder Wert noch Bedeutung der Daten während dieses Migration sprozesses verändert wurden.	elasticache-redis-cluster-automatic-Backup-Check	Wenn automatische Backups aktiviert sind, ElastiCache erstellt Amazon täglich ein Backup des Clusters. Die Sicherung kann für eine von Ihrer Organisation festgelegte Anzahl von Tagen aufbewahrt werden. Automatische Backups schützen vor Datenverlust. Bei einem Ausfall können Sie einen neuen Cluster erstellen, der Ihre Daten aus dem aktuellen Backup wiederherstellt.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
4.8. Validierung – Datenübertragung	Wenn Daten in ein anderes Datenformat oder System übertragen werden, sollte bei der Validierung auch geprüft werden, dass weder Wert noch Bedeutung der Daten während dieses Migrationsprozesses verändert wurden.	fsx-resources-protected-by-Backup-Plan	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre FSx Amazon-Dateisysteme Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
4.8. Validierung – Datenübertragung	Wenn Daten in ein anderes Datenformat oder System übertragen werden, sollte bei der Validierung auch geprüft werden, dass weder Wert noch Bedeutung der Daten während dieses Migrationsprozesses verändert wurden.	rds-in-backup-plan	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon Relational Database Service (Amazon RDS) -Instances Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
4.8. Validierung – Datenübertragung	Wenn Daten in ein anderes Datenformat oder System übertragen werden, sollte bei der Validierung auch geprüft werden, dass weder Wert noch Bedeutung der Daten während dieses Migrationsprozesses verändert wurden.	redshift-backup-enabled	Stellen Sie zur Unterstützung der Datensicherungsprozesse sicher, dass Ihre Amazon-Redshift-Cluster über automatisierte Snapshots verfügen. Wenn automatisierte Snapshots für einen Cluster aktiviert sind, erstellt Redshift in regelmäßigen Abständen Snapshots dieses Clusters. Standardmäßig erstellt Redshift alle acht Stunden oder alle 5 GB einen Snapshot für jeden Knoten mit Datenänderungen oder je nachdem, was zuerst eintritt.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
4.8. Validierung – Datenübertragung	Wenn Daten in ein anderes Datenform at oder System übertragen werden, sollte bei der Validieru ng auch geprüft werden, dass weder Wert noch Bedeutung der Daten während dieses Migration sprozesses verändert wurden.	s-3 bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) unterstützt die Aufrechterhaltung einer angemesse nen Kapazität und Verfügbarkeit. CRR ermöglicht das automatische, asynchrone Kopieren von Objekten in Amazon-S3-Buckets, um die Datenverf ügbarkeit sicherzus tellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
4,8. Validierung – Datenübertragung	Wenn Daten in ein anderes Datenform at oder System übertragen werden, sollte bei der Validieru ng auch geprüft werden, dass weder Wert noch Bedeutung der Daten während dieses Migration sprozesses verändert wurden.	s-3 bucket-versioning-enabled	Die Versionsv erwaltung von Amazon Simple Storage Service (Amazon S3)-Bucke ts hilft dabei, mehrere Varianten eines Objekts im selben Amazon-S3-Bucket zu speichern. Verwenden Sie die Versionsv erwaltung, um sämtliche Versionen aller Objekte in Ihrem Amazon-S3-Bucket zu speichern , abzurufen oder wiederherzustellen . Mit der Versionsv erwaltung können Sie Versionen sowohl nach unbeabsic htigten Benutzera ktionen als auch nach Anwendungsfehlern problemlos wiederher stellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
5. Daten	Computergestützte Systeme, die Daten elektronisch mit anderen Systemen austauschen, sollten geeignete integrierte Kontrollen für die korrekte und sichere Eingabe und Verarbeitung von Daten beinhalten, um die Risiken zu minimieren.	aurora-resources-protected-by-Backup-Plan	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon Aurora Aurora-Ressourcen Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
5. Daten	Computergestützte Systeme, die Daten elektronisch mit anderen Systemen austauschen, sollten geeignete integrierte Kontrollen für die korrekte und sichere Eingabe und Verarbeitung von Daten beinhalten, um die Risiken zu minimieren.	backup-plan-min-frequency-and-min-retention-check	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihr AWS Backup-Plan auf eine Mindestfrequenz und Aufbewahrung festgelegt ist. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen. Mit dieser Regel können Sie die Parameter requiredFrequencyValue (Config default: 1), requiredRetentionDays (Config default: 35) und requiredFrequencyUnit

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			(Config default: days) festlegen. Der tatsächliche Wert muss den Anforderungen Ihrer Organisation entsprechen.
5. Daten	Computergestützte Systeme, die Daten elektronisch mit anderen Systemen austauschen, sollten geeignete integrierte Kontrollen für die korrekte und sichere Eingabe und Verarbeitung von Daten beinhalten, um die Risiken zu minimieren.	backup-recovery-point-encrypted	Stellen Sie sicher, dass die Verschlüsselung für Ihre AWS Backup-Wiederherstellungspunkte aktiviert ist. Da sensible Daten auch im Ruhezustand vorhanden sein können, sollten Sie die Verschlüsselung im Ruhezustand aktivieren, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
5. Daten	Computergestützte Systeme, die Daten elektronisch mit anderen Systemen austauschen, sollten geeignete integrierte Kontrollen für die korrekte und sichere Eingabe und Verarbeitung von Daten beinhalten, um die Risiken zu minimieren.	backup-recovery-point-manual-Löschen-deaktiviert	Stellen Sie sicher, dass Ihren AWS Backup-Wiederherstellungspunkten eine ressourcenbasierte Richtlinie zugeordnet ist, die das Löschen von Wiederherstellungspunkten verhindert. Die Verwendung einer ressourcenbasierten Richtlinie zur Verhinderung des Löschens von Wiederherstellungspunkten kann dazu beitragen, ein versehentliches oder absichtliches Löschen zu unterbinden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
5. Daten	Computergestützte Systeme, die Daten elektronisch mit anderen Systemen austauschen, sollten geeignete integrierte Kontrollen für die korrekte und sichere Eingabe und Verarbeitung von Daten beinhalten, um die Risiken zu minimieren.	backup-recovery-point-minimum-Aufbewahrungsprüfung	Um bei Datensicherungsprozessen zu helfen, stellen Sie sicher, dass für Ihre AWS Backup-Wiederherstellungspunkte eine Mindestaufbewahrungsdauer festgelegt ist. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen. Mit dieser Regel können Sie den Parameter requiredRetentionDays (Standardkonfiguration: 35) festlegen. Der tatsächliche Wert muss den Anforderu

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			ngen Ihrer Organisat ion entsprechen.
5. Daten	Computergestützte Systeme, die Daten elektronisch mit anderen Systemen austauschen, sollten geeignete integrier te Kontrollen für die korrekte und sichere Eingabe und Verarbeitung von Daten beinhalten, um die Risiken zu minimieren.	db-instance-backup-enabled	Die Sicherung sfunktion von Amazon RDS erstellt Sicherung en Ihrer Datenbank en und Transakti onsprotokolle. Amazon RDS erstellt einen Snapshot für das Speichervolume Ihrer DB-Instance, sodass die gesamte DB-Instance gesichert wird. Sie können im System spezifische Aufbewahrungsfrist en festlegen, um Ihre Ausfallsicherheits anforderungen zu erfüllen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
5. Daten	Computergestützte Systeme, die Daten elektronisch mit anderen Systemen austauschen, sollten geeignete integrierte Kontrollen für die korrekte und sichere Eingabe und Verarbeitung von Daten beinhalten, um die Risiken zu minimieren.	dynamodb-in-backup-plan	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon DynamoDB-Tabellen Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
5. Daten	Computergestützte Systeme, die Daten elektronisch mit anderen Systemen austauschen, sollten geeignete integrierte Kontrollen für die korrekte und sichere Eingabe und Verarbeitung von Daten beinhalten, um die Risiken zu minimieren.	dynamodb-pitr-enabled	Aktivieren Sie diese Regel, um zu überprüfen, ob die Informationen gesichert wurden. Es verwaltet auch die Backups, indem es sicherstellt, dass die point-in-time Wiederherstellung in Amazon DynamoDB aktiviert ist. Bei der Wiederherstellung werden fortlaufende Backups Ihrer Tabelle für die letzten 35 Tage gespeichert.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
5. Daten	Computergestützte Systeme, die Daten elektronisch mit anderen Systemen austauschen, sollten geeignete integrierte Kontrollen für die korrekte und sichere Eingabe und Verarbeitung von Daten beinhalten, um die Risiken zu minimieren.	ebs-in-backup-plan	Stellen Sie zur Unterstützung der Datensicherungsprozesse sicher, dass Ihre Amazon Elastic Block Store (Amazon EBS) -Volumes Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihre Backup-Verwaltung und ermöglicht es Ihnen, Ihre geschäftlichen und behördlichen Anforderungen bezüglich Backups zu erfüllen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
5. Daten	Computergestützte Systeme, die Daten elektronisch mit anderen Systemen austauschen, sollten geeignete integrierte Kontrollen für die korrekte und sichere Eingabe und Verarbeitung von Daten beinhalten, um die Risiken zu minimieren.	ebs-optimized-instance	Eine optimierte Instance im Amazon Elastic Block Store (Amazon EBS) bietet zusätzliche, dedizierte Kapazität für Amazon-EBS-I/O-Vorgänge. Diese Optimierung bietet die beste Leistung für Ihr EBS-Volume, indem Konflikte zwischen Amazon-EBS-I/O und anderem Datenverkehr von Ihrer Instance minimiert werden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
5. Daten	Computergestützte Systeme, die Daten elektronisch mit anderen Systemen austauschen, sollten geeignete integrierte Kontrollen für die korrekte und sichere Eingabe und Verarbeitung von Daten beinhalten, um die Risiken zu minimieren.	ebs-resources-protected-by-Backup-Plan	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon Elastic Block Store (Amazon EBS) -Ressourcen Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihre Backup-Verwaltung und ermöglicht es Ihnen, Ihre geschäftlichen und behördlichen Anforderungen bezüglich Backups zu erfüllen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
5. Daten	Computergestützte Systeme, die Daten elektronisch mit anderen Systemen austauschen, sollten geeignete integrierte Kontrollen für die korrekte und sichere Eingabe und Verarbeitung von Daten beinhalten, um die Risiken zu minimieren.	ec2--Plan resources-protected-by-backup	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon Elastic Compute Cloud (Amazon EC2) -Ressourcen Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
5. Daten	Computergestützte Systeme, die Daten elektronisch mit anderen Systemen austauschen, sollten geeignete integrierte Kontrollen für die korrekte und sichere Eingabe und Verarbeitung von Daten beinhalten, um die Risiken zu minimieren.	efs-in-backup-plan	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon Elastic File System (Amazon EFS) -Dateisysteme Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
5. Daten	Computergestützte Systeme, die Daten elektronisch mit anderen Systemen austauschen, sollten geeignete integrierte Kontrollen für die korrekte und sichere Eingabe und Verarbeitung von Daten beinhalten, um die Risiken zu minimieren.	efs-resources-protected-by-Backup-Plan	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon Elastic File System (Amazon EFS) -Dateisysteme Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
5. Daten	Computergestützte Systeme, die Daten elektronisch mit anderen Systemen austauschen, sollten geeignete integrier te Kontrollen für die korrekte und sichere Eingabe und Verarbeitung von Daten beinhalten, um die Risiken zu minimieren.	elasticache-redis-cluster-automatic-Backup-Check	Wenn automatische Backups aktiviert sind, ElastiCache erstellt Amazon täglich ein Backup des Clusters. Die Sicherung kann für eine von Ihrer Organisation festgelegte Anzahl von Tagen aufbewahrt werden. Automatische Backups schützen vor Datenverlust. Bei einem Ausfall können Sie einen neuen Cluster erstellen, der Ihre Daten aus dem aktuellen Backup wiederherstellt.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
5. Daten	Computergestützte Systeme, die Daten elektronisch mit anderen Systemen austauschen, sollten geeignete integrierte Kontrollen für die korrekte und sichere Eingabe und Verarbeitung von Daten beinhalten, um die Risiken zu minimieren.	fsx-resources-protected-by-Backup-Plan	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre FSx Amazon-Dateisysteme Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
5. Daten	Computergestützte Systeme, die Daten elektronisch mit anderen Systemen austauschen, sollten geeignete integrierte Kontrollen für die korrekte und sichere Eingabe und Verarbeitung von Daten beinhalten, um die Risiken zu minimieren.	rds-in-backup-plan	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon Relational Database Service (Amazon RDS) -Instances Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
5. Daten	Computergestützte Systeme, die Daten elektronisch mit anderen Systemen austauschen, sollten geeignete integrierte Kontrollen für die korrekte und sichere Eingabe und Verarbeitung von Daten beinhalten, um die Risiken zu minimieren.	redshift-backup-enabled	Stellen Sie zur Unterstützung der Datensicherungsprozesse sicher, dass Ihre Amazon-Redshift-Cluster über automatisierte Snapshots verfügen. Wenn automatisierte Snapshots für einen Cluster aktiviert sind, erstellt Redshift in regelmäßigen Abständen Snapshots dieses Clusters. Standardmäßig erstellt Redshift alle acht Stunden oder alle 5 GB einen Snapshot für jeden Knoten mit Datenänderungen oder je nachdem, was zuerst eintritt.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
5. Daten	Computergestützte Systeme, die Daten elektronisch mit anderen Systemen austauschen, sollten geeignete integrier te Kontrollen für die korrekte und sichere Eingabe und Verarbeitung von Daten beinhalten, um die Risiken zu minimieren.	s3- bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) unterstützt die Aufrechterhaltung einer angemesse nen Kapazität und Verfügbarkeit. CRR ermöglicht das automatische, asynchrone Kopieren von Objekten in Amazon-S3-Buckets, um die Datenverf ügbarkeit sicherzus tellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
5. Daten	Computergestützte Systeme, die Daten elektronisch mit anderen Systemen austauschen, sollten geeignete integrierte Kontrollen für die korrekte und sichere Eingabe und Verarbeitung von Daten beinhalten, um die Risiken zu minimieren.	s-3 bucket-versioning-enabled	Die Versionsverwaltung von Amazon Simple Storage Service (Amazon S3)-Buckets hilft dabei, mehrere Varianten eines Objekts im selben Amazon-S3-Bucket zu speichern. Verwenden Sie die Versionsverwaltung, um sämtliche Versionen aller Objekte in Ihrem Amazon-S3-Bucket zu speichern, abzurufen oder wiederherzustellen. Mit der Versionsverwaltung können Sie Versionen sowohl nach unbeabsichtigten Benutzeraktionen als auch nach Anwendungsfehlern problemlos wiederherstellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
7.1. Datenspeicherung – Schutz vor Beschädigung	Daten sollten sowohl physisch als auch elektronisch vor Beschädigung geschützt werden. Gespeicherte Daten sollten auf Zugänglichkeit, Lesbarkeit und Richtigkeit überprüft werden. Der Datenzugriff sollte während der gesamten Aufbewahrungsdauer gewährleistet sein.	api-gw-cache-enabled-und-verschlüsselt	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass die Verschlüsselung für den Cache Ihrer API-Gateway-Stufe aktiviert ist. Da für die API-Methode sensible Daten erfasst werden können, sollten Sie die Verschlüsselung von Daten im Ruhezustand aktivieren, um diese Daten zu schützen.
7.1. Datenspeicherung – Schutz vor Beschädigung	Daten sollten sowohl physisch als auch elektronisch vor Beschädigung geschützt werden. Gespeicherte Daten sollten auf Zugänglichkeit, Lesbarkeit und Richtigkeit überprüft werden. Der Datenzugriff sollte während der gesamten Aufbewahrungsdauer gewährleistet sein.	cloudwatch-log-group-encrypted	Um sensible Daten im Speicher zu schützen, stellen Sie sicher, dass die Verschlüsselung für Ihre Amazon CloudWatch Log Groups aktiviert ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
7.1. Datenspei cherung – Schutz vor Beschädigung	Daten sollten sowohl physisch als auch elektronisch vor Beschädigung geschützt werden. Gespeicherte Daten sollten auf Zugänglic hkeit, Lesbarkei t und Richtigkeit überprüft werden. Der Datenzugriff sollte während der gesamten Aufbewahr ungsdauer gewährlei stet sein.	cloud-trail-encryption-enabled	Zum Schutz von eventuell vorhanden en sensiblen Daten sowie Daten im Ruhezustand müssen Sie sicherstellen, dass die Verschlüs selung für Ihre AWS CloudTrail aktiviert ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
7.1. Datenspei cherung – Schutz vor Beschädigung	Daten sollten sowohl physisch als auch elektronisch vor Beschädigung geschützt werden. Gespeicherte Daten sollten auf Zugänglic hkeit, Lesbarkei t und Richtigkeit überprüft werden. Der Datenzugriff sollte während der gesamten Aufbewahr ungsdauer gewährlei stet sein.	db-instance-backup-enabled	Die Sicherung sfunktion von Amazon RDS erstellt Sicherung en Ihrer Datenbank en und Transakti onsprotokolle. Amazon RDS erstellt einen Snapshot für das Speichervolume Ihrer DB-Instance, sodass die gesamte DB-Instance gesichert wird. Sie können im System spezifische Aufbewahrungsfrist en festlegen, um Ihre Ausfallsicherheits anforderungen zu erfüllen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
7.1. Datenspeicherung – Schutz vor Beschädigung	Daten sollten sowohl physisch als auch elektronisch vor Beschädigung geschützt werden. Gespeicherte Daten sollten auf Zugänglichkeit, Lesbarkeit und Richtigkeit überprüft werden. Der Datenzugriff sollte während der gesamten Aufbewahrungsdauer gewährleistet sein.	dynamodb-in-backup-plan	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon DynamoDB-Tabellen Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
7.1. Datenspei cherung – Schutz vor Beschädigung	Daten sollten sowohl physisch als auch elektronisch vor Beschädigung geschützt werden. Gespeicherte Daten sollten auf Zugänglic hkeit, Lesbarkei t und Richtigkeit überprüft werden. Der Datenzugriff sollte während der gesamten Aufbewahr ungsdauer gewährlei stet sein.	dynamodb-pitr-enab led	Aktivieren Sie diese Regel, um zu überprüfen, ob die Informationen gesichert wurden. Es verwaltet auch die Backups, indem es sicherstellt, dass die point-in-time Wiederherstellung in Amazon DynamoDB aktiviert ist. Bei der Wiederherstellung werden fortlaufende Backups Ihrer Tabelle für die letzten 35 Tage gespeichert.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
7.1. Datenspeicherung – Schutz vor Beschädigung	Daten sollten sowohl physisch als auch elektronisch vor Beschädigung geschützt werden. Gespeicherte Daten sollten auf Zugänglichkeit, Lesbarkeit und Richtigkeit überprüft werden. Der Datenzugriff sollte während der gesamten Aufbewahrungsdauer gewährleistet sein.	dynamodb-table-encrypted-kms	Stellen Sie sicher, dass die Verschlüsselung für Ihre Amazon-DynamoDB-Tabellen aktiviert ist. Um eventuell vorhandene sensible Daten im Ruhezustand in diesen Tabellen zu schützen, müssen Sie die Verschlüsselung von Daten im Ruhezustand aktivieren. Standardmäßig werden DynamoDB-Tabellen mit einem AWS eigenen Kundenhauptschlüssel (CMK) verschlüselt.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
7.1. Datenspei cherung – Schutz vor Beschädigung	Daten sollten sowohl physisch als auch elektronisch vor Beschädigung geschützt werden. Gespeicherte Daten sollten auf Zugänglic hkeit, Lesbarkei t und Richtigkeit überprüft werden. Der Datenzugriff sollte während der gesamten Aufbewahr ungsdauer gewährlei stet sein.	ebs-in-backup-plan	Stellen Sie zur Unterstützung der Datensicherungspro zesse sicher, dass Ihre Amazon Elastic Block Store (Amazon EBS) -Volumes Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwaltet er Backup-Service mit einer richtlini enbasierten Backup-Lösung. Diese Lösung vereinfacht Ihre Backup-Verwaltung und ermöglicht es Ihnen, Ihre geschäftl ichen und behördlic hen Anforderungen bezüglich Backups zu erfüllen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
7.1. Datenspei cherung – Schutz vor Beschädigung	Daten sollten sowohl physisch als auch elektronisch vor Beschädigung geschützt werden. Gespeicherte Daten sollten auf Zugänglic hkeit, Lesbarkei t und Richtigkeit überprüft werden. Der Datenzugriff sollte während der gesamten Aufbewahr ungsdauer gewährlei stet sein.	ebs-optimized-inst ance	Eine optimierte Instance im Amazon Elastic Block Store (Amazon EBS) bietet zusätzliche, dedizierte Kapazität für Amazon-EBS-I/ O-Vorgänge. Diese Optimierung bietet die beste Leistung für Ihr EBS-Volume, indem Konflikte zwischen Amazon-EBS-I/O und anderem Datenverk ehr von Ihrer Instance minimiert werden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
7.1. Datenspeicherung – Schutz vor Beschädigung	Daten sollten sowohl physisch als auch elektronisch vor Beschädigung geschützt werden. Gespeicherte Daten sollten auf Zugänglichkeit, Lesbarkeit und Richtigkeit überprüft werden. Der Datenzugriff sollte während der gesamten Aufbewahrungsdauer gewährleistet sein.	ec-2 ebs-encryption-by-default	Zum Schutz von Daten im Ruhezustand müssen Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon Elastic Block Store (Amazon EBS)-Volumes aktiviert ist. Da sensible Daten auch im Ruhezustand vorhanden sein können, sollten Sie die Verschlüsselung im Ruhezustand aktivieren, um diese Daten zu schützen.
7.1. Datenspeicherung – Schutz vor Beschädigung	Daten sollten sowohl physisch als auch elektronisch vor Beschädigung geschützt werden. Gespeicherte Daten sollten auf Zugänglichkeit, Lesbarkeit und Richtigkeit überprüft werden. Der Datenzugriff sollte während der gesamten Aufbewahrungsdauer gewährleistet sein.	efs-encrypted-check	Aktivieren Sie die Verschlüsselung für Ihr Amazon Elastic File System (EFS), um eventuell vorhandene sensible Daten sowie Daten im Ruhezustand zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
7.1. Datenspei cherung – Schutz vor Beschädigung	Daten sollten sowohl physisch als auch elektronisch vor Beschädigung geschützt werden. Gespeicherte Daten sollten auf Zugänglic hkeit, Lesbarkei t und Richtigkeit überprüft werden. Der Datenzugriff sollte während der gesamten Aufbewahr ungsdauer gewährlei stet sein.	efs-in-backup-plan	Um Sie bei Datensich erungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon Elastic File System (Amazon EFS) -Dateisysteme Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwaltet er Backup-Service mit einer richtlini enbasierten Backup-Lösung. Diese Lösung vereinfac ht Ihr Sicherung smanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforde rungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
7.1. Datenspei cherung – Schutz vor Beschädigung	Daten sollten sowohl physisch als auch elektronisch vor Beschädigung geschützt werden. Gespeicherte Daten sollten auf Zugänglic hkeit, Lesbarkei t und Richtigkeit überprüft werden. Der Datenzugriff sollte während der gesamten Aufbewahr ungsdauer gewährlei stet sein.	elasticache-redis-cluster-automatic-Backup-Check	Wenn automatische Backups aktiviert sind, ElastiCache erstellt Amazon täglich ein Backup des Clusters. Die Sicherung kann für eine von Ihrer Organisation festgelegte Anzahl von Tagen aufbewahrt werden. Automatische Backups schützen vor Datenverlust. Bei einem Ausfall können Sie einen neuen Cluster erstellen, der Ihre Daten aus dem aktuellen Backup wiederherstellt.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
7.1. Datenspeicherung – Schutz vor Beschädigung	Daten sollten sowohl physisch als auch elektronisch vor Beschädigung geschützt werden. Gespeicherte Daten sollten auf Zugänglichkeit, Lesbarkeit und Richtigkeit überprüft werden. Der Datenzugriff sollte während der gesamten Aufbewahrungsdauer gewährleistet sein.	elasticsearch-encrypted-at-rest	Da sensible Daten vorhanden sein können und um Daten im Ruhezustand zu schützen, sollten Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon OpenSearch Service (OpenSearch Service)-Domains aktiviert ist.
7.1. Datenspeicherung – Schutz vor Beschädigung	Daten sollten sowohl physisch als auch elektronisch vor Beschädigung geschützt werden. Gespeicherte Daten sollten auf Zugänglichkeit, Lesbarkeit und Richtigkeit überprüft werden. Der Datenzugriff sollte während der gesamten Aufbewahrungsdauer gewährleistet sein.	encrypted-volumes	Aktivieren Sie die Verschlüsselung für Ihre Amazon-Elastic-Block-Store (Amazon-EBS)-Volumes, um eventuell vorhandene sensible Daten sowie Daten im Ruhezustand zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
7.1. Datenspeicherung – Schutz vor Beschädigung	Daten sollten sowohl physisch als auch elektronisch vor Beschädigung geschützt werden. Gespeicherte Daten sollten auf Zugänglichkeit, Lesbarkeit und Richtigkeit überprüft werden. Der Datenzugriff sollte während der gesamten Aufbewahrungsdauer gewährleistet sein.	rds-in-backup-plan	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon Relational Database Service (Amazon RDS) -Instances Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
7.1. Datenspeicherung – Schutz vor Beschädigung	Daten sollten sowohl physisch als auch elektronisch vor Beschädigung geschützt werden. Gespeicherte Daten sollten auf Zugänglichkeit, Lesbarkeit und Richtigkeit überprüft werden. Der Datenzugriff sollte während der gesamten Aufbewahrungsdauer gewährleistet sein.	rds-snapshot-encrypted	Stellen Sie sicher, dass die Verschlüsselung für Ihre Amazon Relational Database Service (Amazon RDS)-Snapshots aktiviert ist. Da sensible Daten auch im Ruhezustand vorhanden sein können, sollten Sie die Verschlüsselung im Ruhezustand aktivieren, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
7.1. Datenspeicherung – Schutz vor Beschädigung	Daten sollten sowohl physisch als auch elektronisch vor Beschädigung geschützt werden. Gespeicherte Daten sollten auf Zugänglichkeit, Lesbarkeit und Richtigkeit überprüft werden. Der Datenzugriff sollte während der gesamten Aufbewahrungsdauer gewährleistet sein.	rds-storage-encrypted	Zum Schutz von Daten im Ruhezustand müssen Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon Relational Database Service (Amazon RDS)-Instances aktiviert ist. Um eventuell vorhandene sensible Daten im Ruhezustand in Amazon-RDS-Instances zu schützen, muss die Verschlüsselung von Daten im Ruhezustand aktiviert sein.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
7.1. Datenspei cherung – Schutz vor Beschädigung	Daten sollten sowohl physisch als auch elektronisch vor Beschädigung geschützt werden. Gespeicherte Daten sollten auf Zugänglic hkeit, Lesbarkei t und Richtigkeit überprüft werden. Der Datenzugriff sollte während der gesamten Aufbewahr ungsdauer gewährlei stet sein.	redshift-backup-en abled	Stellen Sie zur Unterstützung der Datensicherungspro zesse sicher, dass Ihre Amazon-Re dshift-Cluster über automatisierte Snapshots verfügen. Wenn automatis ierte Snapshots für einen Cluster aktiviert sind, erstellt Redshift in regelmäßi gen Abständen Snapshots dieses Clusters. Standardm äßig erstellt Redshift alle acht Stunden oder alle 5 GB einen Snapshot für jeden Knoten mit Datenände rungen oder je nachdem, was zuerst eintritt.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
7.1. Datenspei cherung – Schutz vor Beschädigung	Daten sollten sowohl physisch als auch elektronisch vor Beschädigung geschützt werden. Gespeicherte Daten sollten auf Zugänglic hkeit, Lesbarkei t und Richtigkeit überprüft werden. Der Datenzugriff sollte während der gesamten Aufbewahr ungsdauer gewährlei stet sein.	redshift-cluster-c onfiguration-check	Um Daten im Ruhezustand zu schützen, muss die Verschlüsselung für Ihre Amazon-Re dshift-Cluster aktiviert sein. Sie müssen auch sicherstellen, dass die erforderl ichen Konfigurationen auf Amazon-Redshift-Clustern bereitges tellt werden. Die Prüfungsprotokolli erung muss aktiviert sein, um Informati onen zu Verbindun gen und Benutzera ktivitäten in der Datenbank bereitzus tellen. Diese Regel erfordert, dass ein Wert für clusterDb Encrypted (Config Default: TRUE) und LoggingEnabled (Config Default: TRUE) gesetzt ist. Die tatsächlichen Werte müssen den Richtlini en Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
7.1. Datenspei cherung – Schutz vor Beschädigung	Daten sollten sowohl physisch als auch elektronisch vor Beschädigung geschützt werden. Gespeicherte Daten sollten auf Zugänglic hkeit, Lesbarkei t und Richtigkeit überprüft werden. Der Datenzugriff sollte während der gesamten Aufbewahr ungsdauer gewährlei stet sein.	s-3 bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) unterstützt die Aufrechterhaltung einer angemesse nen Kapazität und Verfügbarkeit. CRR ermöglicht das automatische, asynchrone Kopieren von Objekten in Amazon-S3-Buckets, um die Datenverf ügbarkeit sicherzus tellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
7.1. Datenspei cherung – Schutz vor Beschädigung	Daten sollten sowohl physisch als auch elektronisch vor Beschädigung geschützt werden. Gespeicherte Daten sollten auf Zugänglic hkeit, Lesbarkei t und Richtigkeit überprüft werden. Der Datenzugriff sollte während der gesamten Aufbewahr ungsdauer gewährlei stet sein.	bucket-server-side-encryptions3-fähig	Zum Schutz von Daten im Ruhezusta nd müssen Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon Simple Storage Service (Amazon S3)-Bucke ts aktiviert ist. Um eventuell vorhanden e sensible Daten im Ruhezustand in Amazon-S3-Buckets zu schützen, muss die Verschlüsselung aktiviert sein.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
7.1. Datenspei cherung – Schutz vor Beschädigung	Daten sollten sowohl physisch als auch elektronisch vor Beschädigung geschützt werden. Gespeicherte Daten sollten auf Zugänglic hkeit, Lesbarkei t und Richtigkeit überprüft werden. Der Datenzugriff sollte während der gesamten Aufbewahr ungsdauer gewährlei stet sein.	s-3 bucket-versioning-enabled	Die Versionsv erwaltung von Amazon Simple Storage Service (Amazon S3)-Bucke ts hilft dabei, mehrere Varianten eines Objekts im selben Amazon-S3-Bucket zu speichern. Verwenden Sie die Versionsv erwaltung, um sämtliche Versionen aller Objekte in Ihrem Amazon-S3-Bucket zu speichern , abzurufen oder wiederherzustellen . Mit der Versionsv erwaltung können Sie Versionen sowohl nach unbeabsic htigten Benutzera ktionen als auch nach Anwendungsfehlern problemlos wiederher stellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
7.1. Datenspei cherung – Schutz vor Beschädigung	Daten sollten sowohl physisch als auch elektronisch vor Beschädigung geschützt werden. Gespeicherte Daten sollten auf Zugänglic hkeit, Lesbarkei t und Richtigkeit überprüft werden. Der Datenzugriff sollte während der gesamten Aufbewahr ungsdauer gewährlei stet sein.	s-3 default-encryption -kms	Stellen Sie sicher, dass die Verschlüs selung für Ihre Amazon Simple Storage Service (Amazon S3)-Bucke ts aktiviert ist. Um eventuell vorhanden e sensible Daten im Ruhezustand in einem Amazon-S3-Bucket zu schützen, muss die Verschlüsselung aktiviert sein.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
7.1. Datenspei cherung – Schutz vor Beschädigung	Daten sollten sowohl physisch als auch elektronisch vor Beschädigung geschützt werden. Gespeicherte Daten sollten auf Zugänglic hkeit, Lesbarkei t und Richtigkeit überprüft werden. Der Datenzugriff sollte während der gesamten Aufbewahr ungsdauer gewährlei stet sein.	sagemaker-endpoint -configuration-kms- schlüsselkonfiguriert	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass die Verschlüsselung mit dem AWS Key Management Service (AWS KMS) für Ihren Endpunkt aktiviert ist. SageMaker Da sensible Daten auf dem SageMaker Endgerät gespeiche rt werden können, sollten Sie die Verschlüsselung im Ruhezustand aktiviere n, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
7.1. Datenspei cherung – Schutz vor Beschädigung	Daten sollten sowohl physisch als auch elektronisch vor Beschädigung geschützt werden. Gespeicherte Daten sollten auf Zugänglic hkeit, Lesbarkei t und Richtigkeit überprüft werden. Der Datenzugriff sollte während der gesamten Aufbewahr ungsdauer gewährlei stet sein.	sagemaker-notebook -instance-kms-schl üsselkonfiguriert	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass die Verschlüsselung mit dem AWS Key Management Service (AWS KMS) für Ihr Notebook aktiviert ist. SageMaker Da vertrauliche Daten im SageMaker Notebook gespeichert werden können, sollten Sie die Verschlüsselung im Ruhezustand aktivieren, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
7.1. Datenspei cherung – Schutz vor Beschädigung	Daten sollten sowohl physisch als auch elektronisch vor Beschädigung geschützt werden. Gespeicherte Daten sollten auf Zugänglic hkeit, Lesbarkei t und Richtigkeit überprüft werden. Der Datenzugriff sollte während der gesamten Aufbewahr ungsdauer gewährlei stet sein.	sns-encrypted-kms	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass Ihre Amazon Simple Notification Service (Amazon SNS) -Themen mit dem AWS Key Management Service (AWS KMS) verschlüsselt werden müssen. Um eventuell vorhandene sensible Daten im Ruhezusta nd in veröffentlichten Nachrichten zu schützen, muss die Verschlüsselung von Daten im Ruhezusta nd aktiviert sein.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
7.2. Datenspeicher – Backups	Es sollten regelmäßige Backups aller relevanten Daten durchgeführt werden. Die Integrität und Genauigkeit der Backup-Daten sowie die Fähigkeit, die Daten wiederher zustellen, sollten während der Validierung überprüft und regelmäßig überwacht werden.	aurora-resources-protected-by-Backup-Plan	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon Aurora Aurora-Ressourcen Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
7.2. Datenspeicher – Backups	Es sollten regelmäßige Backups aller relevanten Daten durchgeführt werden. Die Integrität und Genauigkeit der Backup-Daten sowie die Fähigkeit, die Daten wiederherzustellen, sollten während der Validierung überprüft und regelmäßig überwacht werden.	backup-plan-min-frequency-and-min-retention-check	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihr AWS Backup-Plan auf eine Mindestfrequenz und Aufbewahrung festgelegt ist. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen. Mit dieser Regel können Sie die Parameter requiredFrequencyValue (Config default: 1), requiredRetentionDays (Config default: 35) und requiredFrequencyUnit

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			(Config default: days) festlegen. Der tatsächliche Wert muss den Anforderungen Ihrer Organisation entsprechen.
7.2. Datenspeicher – Backups	Es sollten regelmäßige Backups aller relevanten Daten durchgeführt werden. Die Integrität und Genauigkeit der Backup-Daten sowie die Fähigkeit, die Daten wiederherzustellen, sollten während der Validierung überprüft und regelmäßig überwacht werden.	backup-recovery-point-encrypted	Stellen Sie sicher, dass die Verschlüsselung für Ihre AWS Backup-Wiederherstellungspunkte aktiviert ist. Da sensible Daten auch im Ruhezustand vorhanden sein können, sollten Sie die Verschlüsselung im Ruhezustand aktivieren, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
7.2. Datenspeicher – Backups	Es sollten regelmäßige Backups aller relevanten Daten durchgeführt werden. Die Integrität und Genauigkeit der Backup-Daten sowie die Fähigkeit, die Daten wiederherzustellen, sollten während der Validierung überprüft und regelmäßig überwacht werden.	backup-recovery-point-manual-Löschen-deaktiviert	Stellen Sie sicher, dass Ihren AWS Backup-Wiederherstellungspunkten eine ressourcenbasierte Richtlinie zugeordnet ist, die das Löschen von Wiederherstellungspunkten verhindert. Die Verwendung einer ressourcenbasierten Richtlinie zur Verhinderung des Löschens von Wiederherstellungspunkten kann dazu beitragen, ein versehentliches oder absichtliches Löschen zu unterbinden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
7.2. Datenspeicher – Backups	Es sollten regelmäßige Backups aller relevanten Daten durchgeführt werden. Die Integrität und Genauigkeit der Backup-Daten sowie die Fähigkeit, die Daten wiederher zustellen, sollten während der Validierung überprüft und regelmäßig überwacht werden.	backup-recovery-point-minimum-Aufbewahrungsprüfung	Um bei Datensicherungsprozessen zu helfen, stellen Sie sicher, dass für Ihre AWS Backup-Wiederherstellungspunkte eine Mindestaufbewahrungsdauer festgelegt ist. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen. Mit dieser Regel können Sie den Parameter requiredRetentionDays (Standardkonfiguration: 35) festlegen. Der tatsächliche Wert muss den Anforderu

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			ngen Ihrer Organisation entsprechen.
7.2. Datenspeicher – Backups	Es sollten regelmäßige Backups aller relevanten Daten durchgeführt werden. Die Integrität und Genauigkeit der Backup-Daten sowie die Fähigkeit, die Daten wiederherzustellen, sollten während der Validierung überprüft und regelmäßig überwacht werden.	db-instance-backup-enabled	Die Sicherungsfunktion von Amazon RDS erstellt Sicherungen Ihrer Datenbanken und Transaktionsprotokolle. Amazon RDS erstellt einen Snapshot für das Speichervolume Ihrer DB-Instance, sodass die gesamte DB-Instance gesichert wird. Sie können im System spezifische Aufbewahrungsfristen festlegen, um Ihre Ausfallsicherheitsanforderungen zu erfüllen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
7.2. Datenspeicher – Backups	Es sollten regelmäßige Backups aller relevanten Daten durchgeführt werden. Die Integrität und Genauigkeit der Backup-Daten sowie die Fähigkeit, die Daten wiederherzustellen, sollten während der Validierung überprüft und regelmäßig überwacht werden.	dynamodb-in-backup-plan	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon DynamoDB-Tabellen Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
7.2. Datenspeicher – Backups	Es sollten regelmäßige Backups aller relevanten Daten durchgeführt werden. Die Integrität und Genauigkeit der Backup-Daten sowie die Fähigkeit, die Daten wiederher zustellen, sollten während der Validierung überprüft und regelmäßig überwacht werden.	dynamodb-pitr-enabled	Aktivieren Sie diese Regel, um zu überprüfen, ob die Informationen gesichert wurden. Es verwaltet auch die Backups, indem es sicherstellt, dass die point-in-time Wiederherstellung in Amazon DynamoDB aktiviert ist. Bei der Wiederherstellung werden fortlaufende Backups Ihrer Tabelle für die letzten 35 Tage gespeichert.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
7.2. Datenspeicher – Backups	Es sollten regelmäßige Backups aller relevanten Daten durchgeführt werden. Die Integrität und Genauigkeit der Backup-Daten sowie die Fähigkeit, die Daten wiederher zustellen, sollten während der Validierung überprüft und regelmäßig überwacht werden.	ebs-in-backup-plan	Stellen Sie zur Unterstützung der Datensicherungsprozesse sicher, dass Ihre Amazon Elastic Block Store (Amazon EBS) -Volumes Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihre Backup-Verwaltung und ermöglicht es Ihnen, Ihre geschäftlichen und behördlichen Anforderungen bezüglich Backups zu erfüllen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
7.2. Datenspeicher – Backups	Es sollten regelmäßige Backups aller relevanten Daten durchgeführt werden. Die Integrität und Genauigkeit der Backup-Daten sowie die Fähigkeit, die Daten wiederher zustellen, sollten während der Validierung überprüft und regelmäßig überwacht werden.	ebs-optimized-instance	Eine optimierte Instance im Amazon Elastic Block Store (Amazon EBS) bietet zusätzliche, dedizierte Kapazität für Amazon-EBS-I/O-Vorgänge. Diese Optimierung bietet die beste Leistung für Ihr EBS-Volume, indem Konflikte zwischen Amazon-EBS-I/O und anderem Datenverkehr von Ihrer Instance minimiert werden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
7.2. Datenspeicher – Backups	Es sollten regelmäßige Backups aller relevanten Daten durchgeführt werden. Die Integrität und Genauigkeit der Backup-Daten sowie die Fähigkeit, die Daten wiederherzustellen, sollten während der Validierung überprüft und regelmäßig überwacht werden.	ebs-resources-protected-by-Backup-Plan	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon Elastic Block Store (Amazon EBS) -Ressourcen Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihre Backup-Verwaltung und ermöglicht es Ihnen, Ihre geschäftlichen und behördlichen Anforderungen bezüglich Backups zu erfüllen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
7.2. Datenspeicher – Backups	Es sollten regelmäßige Backups aller relevanten Daten durchgeführt werden. Die Integrität und Genauigkeit der Backup-Daten sowie die Fähigkeit, die Daten wiederherzustellen, sollten während der Validierung überprüft und regelmäßig überwacht werden.	ec2--Plan resources-protected-by-backup	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon Elastic Compute Cloud (Amazon EC2) -Ressourcen Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
7.2. Datenspeicher – Backups	Es sollten regelmäßige Backups aller relevanten Daten durchgeführt werden. Die Integrität und Genauigkeit der Backup-Daten sowie die Fähigkeit, die Daten wiederherzustellen, sollten während der Validierung überprüft und regelmäßig überwacht werden.	efs-in-backup-plan	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon Elastic File System (Amazon EFS) -Dateisysteme Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
7.2. Datenspeicher – Backups	Es sollten regelmäßige Backups aller relevanten Daten durchgeführt werden. Die Integrität und Genauigkeit der Backup-Daten sowie die Fähigkeit, die Daten wiederher zustellen, sollten während der Validierung überprüft und regelmäßig überwacht werden.	efs-resources-protected-by-Backup-Plan	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon Elastic File System (Amazon EFS) -Dateisysteme Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
7.2. Datenspeicher – Backups	Es sollten regelmäßige Backups aller relevanten Daten durchgeführt werden. Die Integrität und Genauigkeit der Backup-Daten sowie die Fähigkeit, die Daten wiederher zustellen, sollten während der Validierung überprüft und regelmäßig überwacht werden.	elasticache-redis-cluster-automatic-Backup-Check	Wenn automatische Backups aktiviert sind, ElastiCache erstellt Amazon täglich ein Backup des Clusters. Die Sicherung kann für eine von Ihrer Organisation festgelegte Anzahl von Tagen aufbewahrt werden. Automatische Backups schützen vor Datenverlust. Bei einem Ausfall können Sie einen neuen Cluster erstellen, der Ihre Daten aus dem aktuellen Backup wiederherstellt.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
7.2. Datenspeicher – Backups	Es sollten regelmäßige Backups aller relevanten Daten durchgeführt werden. Die Integrität und Genauigkeit der Backup-Daten sowie die Fähigkeit, die Daten wiederherzustellen, sollten während der Validierung überprüft und regelmäßig überwacht werden.	fsx-resources-protected-by-Backup-Plan	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre FSx Amazon-Dateisysteme Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
7.2. Datenspeicher – Backups	Es sollten regelmäßige Backups aller relevanten Daten durchgeführt werden. Die Integrität und Genauigkeit der Backup-Daten sowie die Fähigkeit, die Daten wiederherzustellen, sollten während der Validierung überprüft und regelmäßig überwacht werden.	rds-in-backup-plan	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon Relational Database Service (Amazon RDS) -Instances Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
7.2. Datenspeicher – Backups	Es sollten regelmäßige Backups aller relevanten Daten durchgeführt werden. Die Integrität und Genauigkeit der Backup-Daten sowie die Fähigkeit, die Daten wiederherzustellen, sollten während der Validierung überprüft und regelmäßig überwacht werden.	redshift-backup-enabled	Stellen Sie zur Unterstützung der Datensicherungsprozesse sicher, dass Ihre Amazon-Redshift-Cluster über automatisierte Snapshots verfügen. Wenn automatisierte Snapshots für einen Cluster aktiviert sind, erstellt Redshift in regelmäßigen Abständen Snapshots dieses Clusters. Standardmäßig erstellt Redshift alle acht Stunden oder alle 5 GB einen Snapshot für jeden Knoten mit Datenänderungen oder je nachdem, was zuerst eintritt.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
7.2. Datenspeicher – Backups	Es sollten regelmäßige Backups aller relevanten Daten durchgeführt werden. Die Integrität und Genauigkeit der Backup-Daten sowie die Fähigkeit, die Daten wiederherzustellen, sollten während der Validierung überprüft und regelmäßig überwacht werden.	s-3 bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) unterstützt die Aufrechterhaltung einer angemessenen Kapazität und Verfügbarkeit. CRR ermöglicht das automatische, asynchrone Kopieren von Objekten in Amazon-S3-Buckets, um die Datenverfügbarkeit sicherzustellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
7.2. Datenspeicher – Backups	Es sollten regelmäßige Backups aller relevanten Daten durchgeführt werden. Die Integrität und Genauigkeit der Backup-Daten sowie die Fähigkeit, die Daten wiederherzustellen, sollten während der Validierung überprüft und regelmäßig überwacht werden.	s-3 bucket-versioning-enabled	Die Versionsverwaltung von Amazon Simple Storage Service (Amazon S3)-Buckets hilft dabei, mehrere Varianten eines Objekts im selben Amazon-S3-Bucket zu speichern. Verwenden Sie die Versionsverwaltung, um sämtliche Versionen aller Objekte in Ihrem Amazon-S3-Bucket zu speichern, abzurufen oder wiederherzustellen. Mit der Versionsverwaltung können Sie Versionen sowohl nach unbeabsichtigten Benutzeraktionen als auch nach Anwendungsfehlern problemlos wiederherstellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
9. Audit Trails	Auf der Grundlage einer Risikobewertung sollte erwogen werden, in das System eine Aufzeichnung aller GMP-relevanten Änderungen und Löschungen aufzunehmen (ein vom System generierter „Audit Trail“). Für Änderungen oder Löschungen von GMP-relevanten Daten sollte der Grund dokumentiert werden. Audit Trails müssen verfügbar und in eine allgemein verständliche Form konvertierbar sein und regelmäßig überprüft werden.	cloudtrail-s3-dataevents-enabled	Die Erfassung von Simple Storage Service (Amazon S3)-Datenereignissen unterstützt die Erkennung von ungewöhnlichen Aktivitäten. Zu den Details gehören Informationen zu dem AWS -Konto, das auf einen Amazon-S3-Bucket zugegriffen hat, die IP-Adresse und die Uhrzeit des Ereignisses.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10. Änderungs- und Konfigurationsmanagement	Änderungen an einem computergestützten System, einschließlich Systemkonfigurationen, sollten nur kontrolliert und nach einem festgelegten Verfahren vorgenommen werden.	elb-deletion-protection-enabled	Diese Regel sorgt dafür, dass der Löschschutz für Elastic Load Balancing aktiviert ist. Verwenden Sie diese Funktion, um zu verhindern, dass Ihr Load Balancer versehentlich oder böswillig gelöscht wird, was zum Verlust der Verfügbarkeit Ihrer Anwendungen führen kann.
10. Änderungs- und Konfigurationsmanagement	Änderungen an einem computergestützten System, einschließlich Systemkonfigurationen, sollten nur kontrolliert und nach einem festgelegten Verfahren vorgenommen werden.	rds-cluster-deletion-protection-aktiviert	Stellen Sie sicher, dass Amazon Relational Database Service (Amazon RDS)-Instances den Löschschutz aktiviert haben. Verwenden Sie den Löschschutz, um zu verhindern, dass Ihre Amazon-RDS-Instances versehentlich oder böswillig gelöscht werden, was zum Verlust der Verfügbarkeit Ihrer Anwendungen führen kann.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10. Änderungs- und Konfigurationsmanagement	Änderungen an einem computergestützten System, einschließlich Systemkonfigurationen, sollten nur kontrolliert und nach einem festgelegten Verfahren vorgenommen werden.	rds-instance-deletion-protection-aktiviert	Stellen Sie sicher, dass Amazon Relational Database Service (Amazon RDS)-Instances den Löschschutz aktiviert haben. Verwenden Sie den Löschschutz, um zu verhindern, dass Ihre Amazon-RDS-Instances versehentlich oder böswillig gelöscht werden, was zum Verlust der Verfügbarkeit Ihrer Anwendungen führen kann.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
11. Regelmäßige Auswertung	Computergestützte Systeme sollten regelmäßig überprüft werden, um sicherzus tellen, dass sie sich weiterhin in einem gültigen Zustand befinden und GMP-konform sind. Solche Bewertungen sollten gegebenen falls den aktuellen Funktionsumfang, Aufzeichnungen über Abweichungen, Vorfälle, Probleme, Upgrade-Verlauf, Leistung, Zuverläss igkeit, Sicherheit und Validierungsstatus umfassen.	guardduty-enabled-centralized	Amazon GuardDuty kann mithilfe von Threat Intellige nce Feeds helfen, potenzielle Cybersich erheitsereignisse zu überwachen und zu erkennen. Dazu gehören Listen mit bösartigen IPs und maschinel len Lernmethoden zur Identifizierung unerwarteter, nicht autorisierter und bösartiger Aktivitäten in Ihrer AWS Cloud-Umgebung.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
12.1. Sicherheit – Autorisierte Personen	Es sollten physische und/oder logische Kontrollen implementiert werden, um den Zugriff auf das computergestützte System auf autorisierte Personen zu beschränken. Geeignete Methoden zur Verhinderung des unbefugten Zugriffs auf das System sind unter anderem die Verwendung von Schlüsseln, Ausweiskarten, persönlichen Codes mit Passwörtern, biometrische Daten sowie der eingeschränkte Zugang zu Computerausrüstung und Datenspeicherbereichen.	codebuild-project-environment-privileged-überprüfen	Um die Implementierung des Prinzips der geringsten Rechte zu unterstützen, stellen Sie sicher, dass in Ihrer CodeBuild Amazon-Projektumgebung der privilegierte Modus nicht aktiviert ist. Diese Einstellung sollte deaktiviert werden, um einen unbeabsichtigten Zugriff auf Docker APIs sowie auf die dem Container zugrundeliegende Hardware zu verhindern.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
12.1. Sicherheit – Autorisierte Personen	Es sollten physische und/oder logische Kontrollen implementiert werden, um den Zugriff auf das computergestützte System auf autorisierte Personen zu beschränken. Geeignete Methoden zur Verhinderung des unbefugten Zugriffs auf das System sind unter anderem die Verwendung von Schlüsseln, Ausweiskarten, persönlichen Codes mit Passwörtern, biometrische Daten sowie der eingeschränkte Zugang zu Computerausrüstung und Datenspeicherbereichen.	ec-2 instance-profile-attached	EC2 Instanzprofile übergeben eine IAM-Rolle an eine EC2 Instance. Das Anhängen eines Instance-Profils an Ihre Instances kann bei der Implementierung von geringsten Berechtigungen und der Berechtigungsverwaltung helfen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
12.1. Sicherheit – Autorisierte Personen	Es sollten physische und/oder logische Kontrollen implementiert werden, um den Zugriff auf das computergestützte System auf autorisierte Personen zu beschränken. Geeignete Methoden zur Verhinderung des unbefugten Zugriffs auf das System sind unter anderem die Verwendung von Schlüsseln, Ausweiskarten, persönlichen Codes mit Passwörtern, biometrische Daten sowie der eingeschränkte Zugang zu Computerausrüstung und Datenspeicherbereichen.	ecs-containers-nonprivileged	Um die Implementierung des Prinzips der geringsten Berechtigung zu unterstützen, dürfen in Amazon Elastic Container Service (Amazon ECS)-Aufgabendefinitionen keine erhöhten Berechtigungen aktiviert sein. Wenn dieser Parameter den Wert „true“ aufweist, erhält der Container erhöhte Berechtigungen auf der Host-Container-Instance (ähnlich wie der Root-Benutzer).

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
12,1. Sicherheit – Autorisierte Personen	Es sollten physische und/oder logische Kontrollen implementiert werden, um den Zugriff auf das computergestützte System auf autorisierte Personen zu beschränken. Geeignete Methoden zur Verhinderung des unbefugten Zugriffs auf das System sind unter anderem die Verwendung von Schlüsseln, Ausweiskarten, persönlichen Codes mit Passwörtern, biometrische Daten sowie der eingeschränkte Zugang zu Computerausrüstung und Datenspeicherbereichen.	ecs-containers-readonly-access	Die Aktivierung des schreibgeschützten Zugriffs auf Amazon Elastic Container Service (ECS)-Container kann dazu beitragen, das Prinzip der geringsten Berechtigung einzuhalten. Diese Option kann Angriffsvektoren reduzieren, da das Dateisystem der Container-Instance nur geändert werden kann, wenn es über ausdrückliche Lese- und Schreibberechtigungen verfügt.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
12,1. Sicherheit – Autorisierte Personen	Es sollten physische und/oder logische Kontrollen implement iert werden, um den Zugriff auf das computerg estützte System auf autorisierte Personen zu beschränken. Geeignete Methoden zur Verhinderung des unbefugten Zugriffs auf das System sind unter anderem die Verwendun g von Schlüssel n, Ausweiskarten, persönlichen Codes mit Passwörtern, biometrische Daten sowie der eingeschr änkte Zugang zu Computerausrüstung und Datenspei cherbereichen.	ecs-task-definition-nonroot-Benutzer	Sie bestimmen einen Nicht-Root-Benutzer für den Zugriff auf Ihre Aufgabendefinitionen des Amazon Elastic Container Service (Amazon ECS), um die Implementierung des Prinzips der geringsten Berechtig ung zu unterstützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
12.1. Sicherheit – Autorisierte Personen	Es sollten physische und/oder logische Kontrollen implementiert werden, um den Zugriff auf das computergestützte System auf autorisierte Personen zu beschränken. Geeignete Methoden zur Verhinderung des unbefugten Zugriffs auf das System sind unter anderem die Verwendung von Schlüsseln, Ausweiskarten, persönlichen Codes mit Passwörtern, biometrische Daten sowie der eingeschränkte Zugang zu Computerausrüstung und Datenspeicherbereichen.	ecs-task-definition-user-for-host-mode-check	Wenn für eine Aufgabendefinition erhöhte Berechtigungen gelten, liegt das daran, dass der Kunde diesen Konfigurationen ausdrücklich zugestimmt hat. Diese Kontrolle prüft, ob eine unerwartete Berechtigungseskalation vorliegt, wenn für eine Aufgabendefinition das Host-Netzwerk aktiviert ist, die Kunden aber keine erhöhten Berechtigungen aktiviert haben.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
12,1. Sicherheit – Autorisierte Personen	Es sollten physische und/oder logische Kontrollen implementiert werden, um den Zugriff auf das computergestützte System auf autorisierte Personen zu beschränken. Geeignete Methoden zur Verhinderung des unbefugten Zugriffs auf das System sind unter anderem die Verwendung von Schlüsseln, Ausweiskarten, persönlichen Codes mit Passwörtern, biometrische Daten sowie der eingeschränkte Zugang zu Computerausrüstung und Datenspeicherbereichen.	efs-access-point-enforce-root-Verzeichnis	Die Durchsetzung eines Stammverzeichnisses für einen Amazon-Elastic-File-System (Amazon-EFS)-Zugangspunkt trägt dazu bei, den Datenzugriff einzuschränken, indem sichergestellt wird, dass Benutzer des Zugangspunkts nur auf Dateien des angegebenen Unterverzeichnisses zugreifen können.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
12.1. Sicherheit – Autorisierte Personen	Es sollten physische und/oder logische Kontrollen implementiert werden, um den Zugriff auf das computergestützte System auf autorisierte Personen zu beschränken. Geeignete Methoden zur Verhinderung des unbefugten Zugriffs auf das System sind unter anderem die Verwendung von Schlüsseln, Ausweiskarten, persönlichen Codes mit Passwörtern, biometrische Daten sowie der eingeschränkte Zugang zu Computerausrüstung und Datenspeicherbereichen.	efs-access-point-enforce-Benutzeridentität	Um die Implementierung des Prinzips der geringsten Rechte zu unterstützen, stellen Sie sicher, dass die Benutzerdurchsetzung für Ihr Amazon Elastic File System (Amazon EFS) aktiviert ist. Wenn diese Option aktiviert ist, ersetzt Amazon EFS den Benutzer und die Gruppe IDs des NFS-Clients durch die Identität, die auf dem Access Point für alle Dateisystemoperationen konfiguriert ist, und gewährt nur Zugriff auf diese erzwungene Benutzeridentität.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
12.1. Sicherheit – Autorisierte Personen	Es sollten physische und/oder logische Kontrollen implementiert werden, um den Zugriff auf das computergestützte System auf autorisierte Personen zu beschränken. Geeignete Methoden zur Verhinderung des unbefugten Zugriffs auf das System sind unter anderem die Verwendung von Schlüsseln, Ausweiskarten, persönlichen Codes mit Passwörtern, biometrische Daten sowie der eingeschränkte Zugang zu Computerausrüstung und Datenspeicherbereichen.	iam-policy-no-statements-with-full-access	Stellen Sie sicher, dass IAM-Aktionen nur auf die benötigten Aktionen beschränkt sind. Wenn Benutzern mehr Rechte eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und der Aufgabentrennung verstoßen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
12,1. Sicherheit – Autorisierte Personen	Es sollten physische und/oder logische Kontrollen implementiert werden, um den Zugriff auf das computergestützte System auf autorisierte Personen zu beschränken. Geeignete Methoden zur Verhinderung des unbefugten Zugriffs auf das System sind unter anderem die Verwendung von Schlüsseln, Ausweiskarten, persönlichen Codes mit Passwörtern, biometrische Daten sowie der eingeschränkte Zugang zu Computerausrüstung und Datenspeicherbereichen.	opensearch-access-control-enabled	Stellen Sie sicher, dass eine detaillierte Zugriffskontrolle für Ihre Amazon OpenSearch Service-Domains aktiviert ist. Eine differenzierte Zugriffskontrolle bietet erweiterte Autorisierungsmechanismen, um den Zugriff auf Amazon Service-Domains mit den geringsten Rechten zu erreichen. OpenSearch Es ermöglicht eine rollenbasierte Zugriffskontrolle auf die Domain sowie Sicherheit auf Index-, Dokument- und Feldebene, Unterstützung für OpenSearch Service-Dashboards, Mehrmandantenfähigkeit und HTTP-Basisauthentifizierung für Service und Kibana. OpenSearch

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
12.1. Sicherheit – Autorisierte Personen	Es sollten physische und/oder logische Kontrollen implementiert werden, um den Zugriff auf das computergestützte System auf autorisierte Personen zu beschränken. Geeignete Methoden zur Verhinderung des unbefugten Zugriffs auf das System sind unter anderem die Verwendung von Schlüsseln, Ausweiskarten, persönlichen Codes mit Passwörtern, biometrische Daten sowie der eingeschränkte Zugang zu Computerausrüstung und Datenspeicherbereichen.	rds-instance-iam-authentication-aktiviert	Stellen Sie sicher, dass eine AWS Identity and Access Management (IAM) -Authentifizierung auf Amazon Relational Database Service (Amazon RDS) -Instances aktiviert ist, um den Zugriff auf Systeme und Ressourcen zu kontrollieren. Dadurch wird die Verschlüsselung von ausgehendem und eingehendem Netzwerkverkehr von und zur Datenbank anhand von Secure Sockets Layer (SSL) durchgesetzt. Da die Authentifizierung extern verwaltet wird, ist es nicht erforderlich, Benutzeranmeldeinformationen in der Datenbank zu speichern.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
12.1. Sicherheit – Autorisierte Personen	Es sollten physische und/oder logische Kontrollen implementiert werden, um den Zugriff auf das computergestützte System auf autorisierte Personen zu beschränken. Geeignete Methoden zur Verhinderung des unbefugten Zugriffs auf das System sind unter anderem die Verwendung von Schlüsseln, Ausweiskarten, persönlichen Codes mit Passwörtern, biometrische Daten sowie der eingeschränkte Zugang zu Computerausrüstung und Datenspeicherbereichen.	s-3 bucket-acl-prohibited	Diese Regel prüft, ob Access Control Lists (ACLs) für die Zugriffskontrolle auf Amazon S3 S3-Buckets verwendet werden. ACLs sind veraltete Zugriffskontrollmechanismen für Amazon S3 S3-Buckets, die älter sind als AWS Identity and Access Management (IAM). Stattdessen empfiehlt es sich ACLs, IAM-Richtlinien oder S3-Bucket-Richtlinien zu verwenden, um den Zugriff auf Ihre S3-Buckets einfacher zu verwalten.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
12.1. Sicherheit – Autorisierte Personen	Es sollten physische und/oder logische Kontrollen implementiert werden, um den Zugriff auf das computergestützte System auf autorisierte Personen zu beschränken. Geeignete Methoden zur Verhinderung des unbefugten Zugriffs auf das System sind unter anderem die Verwendung von Schlüsseln, Ausweiskarten, persönlichen Codes mit Passwörtern, biometrische Daten sowie der eingeschränkte Zugang zu Computerausrüstung und Datenspeicherbereichen.	ssm-document-not-public	Stellen Sie sicher, dass AWS Systems Manager (SSM) - Dokumente nicht öffentlich sind, da dies einen unbeabsichtigten Zugriff auf Ihre SSM-Dokumente ermöglichen kann. Ein öffentliches SSM-Dokument kann Informationen über Ihr Konto, Ihre Ressourcen und internen Prozesse preisgeben.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
12.1. Sicherheit – Autorisierte Personen	Es sollten physische und/oder logische Kontrollen implementiert werden, um den Zugriff auf das computergestützte System auf autorisierte Personen zu beschränken. Geeignete Methoden zur Verhinderung des unbefugten Zugriffs auf das System sind unter anderem die Verwendung von Schlüsseln, Ausweiskarten, persönlichen Codes mit Passwörtern, biometrische Daten sowie der eingeschränkte Zugang zu Computerausrüstung und Datenspeicherbereichen.	emr-kerberos-enabled	Die Zugriffsberechtigungen und -autorisierungen können verwaltet und nach den Prinzipien der geringsten Berechtigung und Aufgabentrennung integriert werden, indem Kerberos für Amazon-EMR-Cluster aktiviert wird. In Kerberos werden Services und Benutzer, die sich authentifizieren müssen, als Prinzipale bezeichnet. Prinzipale befinden sich in einem Kerberos-Bereich. Innerhalb dieses Bereichs wird ein Kerberos-Server als Key Distribution Center (KDC) bezeichnet. Über diesen Server können sich Prinzipale authentifizieren. Die Authentifizierung im KDC erfolgt durch die Ausstellung von Authentif

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			izierungstickets. Das KDC unterhält eine Datenbank der Prinzipale in seinem Bereich mit ihren Passwörtern und anderen administr ativen Informationen zu jedem Prinzipal.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
12,1. Sicherheit – Autorisierte Personen	Es sollten physische und/oder logische Kontrollen implementiert werden, um den Zugriff auf das computergestützte System auf autorisierte Personen zu beschränken. Geeignete Methoden zur Verhinderung des unbefugten Zugriffs auf das System sind unter anderem die Verwendung von Schlüsseln, Ausweiskarten, persönlichen Codes mit Passwörtern, biometrische Daten sowie der eingeschränkte Zugang zu Computerausrüstung und Datenspeicherbereichen.	iam-customer-policy-blocked-kms-Aktionen	AWS Identity and Access Management (IAM) kann Ihnen helfen, die Prinzipien der geringsten Rechte und der Aufgabentrennung in Zugriffsberechtigungen und Autorisierungen zu integrieren und so zu verhindern, dass Richtlinien blockierte Aktionen für alle AWS Schlüssel des Key Management Service enthalten. Wenn Benutzer mehr Rechte haben, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und Aufgabentrennung verstoßen. Mit dieser Regel können Sie den Parameter festlegen. blockedActionsPatterns (Wert „AWS Bewährte grundlegende Sicherheitsmethode

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			n“: kms: Entschlüs seln, kms:ReEnc ryptFrom). Die tatsächlichen Werte müssen den Richtlini en Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
12.1. Sicherheit – Autorisierte Personen	Es sollten physische und/oder logische Kontrollen implement iert werden, um den Zugriff auf das computerg estützte System auf autorisierte Personen zu beschränken. Geeignete Methoden zur Verhinderung des unbefugten Zugriffs auf das System sind unter anderem die Verwendun g von Schlüssel n, Ausweiskarten, persönlichen Codes mit Passwörtern, biometrische Daten sowie der eingeschr änkte Zugang zu Computerausrüstung und Datenspei cherbereichen.	iam-inline-policy-blocked-kms-Aktionen	Stellen Sie sicher, dass ein Benutzer, eine IAM-Rolle oder eine IAM-Gruppe (AWS Identity and Access Management) nicht über eine Inline-Richtlinie verfügt, die blockierte Aktionen für alle AWS Schlüssel des Key Management Service zulässt. AWS empfiehlt, verwaltet e Richtlinien anstelle von Inline-Richtlinien zu verwenden. Verwaltete Richtlini en ermöglichen Wiederverwendbarke it, Versionsverwaltung , Rollback und Delegierung der Berechtigungsverwa ltung. Mit dieser Regel können Sie den blockedActionsPatt erns Parameter festlegen. (Wert „AWS Bewährte grundlegende Sicherheitsmethode n“: kms: Entschlüs seln, kms:ReEnc

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			ryptFrom). Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.
12.1. Sicherheit – Autorisierte Personen	Es sollten physische und/oder logische Kontrollen implementiert werden, um den Zugriff auf das computergestützte System auf autorisierte Personen zu beschränken. Geeignete Methoden zur Verhinderung des unbefugten Zugriffs auf das System sind unter anderem die Verwendung von Schlüsseln, Ausweiskarten, persönlichen Codes mit Passwörtern, biometrische Daten sowie der eingeschränkte Zugang zu Computerausrüstung und Datenspeicherbereichen.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) kann Ihnen dabei helfen, die Prinzipien der geringsten Rechte und der Aufgabentrennung in Zugriffsberechtigungen und Autorisierungen zu integrieren und so zu verhindern, dass Richtlinien „Effect“: „Allow“ mit „Action“: „*“ anstelle von „Resource“: „*“ enthalten. Wenn Benutzern mehr Rechte eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und der Aufgabentrennung verstoßen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
12.1. Sicherheit – Autorisierte Personen	Es sollten physische und/oder logische Kontrollen implement iert werden, um den Zugriff auf das computerg estützte System auf autorisierte Personen zu beschränken. Geeignete Methoden zur Verhinderung des unbefugten Zugriffs auf das System sind unter anderem die Verwendun g von Schlüssel n, Ausweiskarten, persönlichen Codes mit Passwörtern, biometrische Daten sowie der eingeschr änkte Zugang zu Computerausrüstung und Datenspei cherbereichen.	iam-root-access-key-überprüfen	Der Zugriff auf Systeme und Ressourcen kann gesteuert werden, indem überprüft wird, ob der Root-Benu tzer keine Zugriffss chlüssel mit seiner AWS Identity and Access Management (IAM) -Rolle verknüpft hat. Stellen Sie sicher, dass die Root-Zugr iffsschlüssel gelöscht werden. Erstellen und verwenden Sie stattdessen rollenbas ierte Funktionen, AWS-Konten um das Prinzip der geringste n Funktionalität zu berücksichtigen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
12.1. Sicherheit – Autorisierte Personen	Es sollten physische und/oder logische Kontrollen implementiert werden, um den Zugriff auf das computergestützte System auf autorisierte Personen zu beschränken. Geeignete Methoden zur Verhinderung des unbefugten Zugriffs auf das System sind unter anderem die Verwendung von Schlüsseln, Ausweiskarten, persönlichen Codes mit Passwörtern, biometrische Daten sowie der eingeschränkte Zugang zu Computerausrüstung und Datenspeicherbereichen.	s-3 bucket-public-read-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie nur autorisierten Benutzern, Prozessen und Geräten Zugriff auf Amazon Simple Storage Service (Amazon S3) - Buckets gewähren. Die Verwaltung des Zugriffs sollte mit der Klassifizierung der Daten übereinstimmen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
12.1. Sicherheit – Autorisierte Personen	Es sollten physische und/oder logische Kontrollen implementiert werden, um den Zugriff auf das computergestützte System auf autorisierte Personen zu beschränken. Geeignete Methoden zur Verhinderung des unbefugten Zugriffs auf das System sind unter anderem die Verwendung von Schlüsseln, Ausweiskarten, persönlichen Codes mit Passwörtern, biometrische Daten sowie der eingeschränkte Zugang zu Computerausrüstung und Datenspeicherbereichen.	s-3 bucket-public-write-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie nur autorisierten Benutzern, Prozessen und Geräten Zugriff auf Amazon Simple Storage Service (Amazon S3) - Buckets gewähren. Die Verwaltung des Zugriffs sollte mit der Klassifizierung der Daten übereinstimmen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
12.1. Sicherheit – Autorisierte Personen	Es sollten physische und/oder logische Kontrollen implementiert werden, um den Zugriff auf das computergestützte System auf autorisierte Personen zu beschränken. Geeignete Methoden zur Verhinderung des unbefugten Zugriffs auf das System sind unter anderem die Verwendung von Schlüsseln, Ausweiskarten, persönlichen Codes mit Passwörtern, biometrische Daten sowie der eingeschränkte Zugang zu Computerausrüstung und Datenspeicherbereichen.	sagemaker-notebook-no-direct-Internetzugang	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass SageMaker Amazon-Notebooks keinen direkten Internetzugang zulassen. Indem Sie direkten Internetzugang blockieren, vermeiden Sie, dass unbefugte Benutzer auf sensible Daten zugreifen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
12.3. Sicherheit – Audit Trail zur Autorisierung	Die Erstellung, Änderung und der Widerruf von Zugriffsberechtigungen sollten aufgezeichnet werden.	cloudtrail-enabled	AWS CloudTrail kann durch die Aufzeichnung von Aktionen und API-Aufrufen in der AWS Management Console bei der Nichtabstreitbarkeit helfen. Sie können die Benutzer und die Benutzer AWS-Konten , die einen AWS Dienst aufgerufen haben, die Quell-IP-Adresse, über die die Aufrufe generiert wurden, und den Zeitpunkt der Anrufe identifizieren. Einzelheiten zu den erfassten Daten finden Sie in den AWS CloudTrail Datensatzinhalten.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
12.4. Sicherheit – Audit Trail	Managementsysteme für Daten und Dokumente sollten so konzipiert sein, dass sie die Identität der Betreiber aufzeichnen, die Daten wie Datum und Uhrzeit eingeben, ändern, bestätigen oder löschen.	cloudtrail-s3-dataevents-enabled	Die Erfassung von Simple Storage Service (Amazon S3)-Datenereignissen unterstützt die Erkennung von ungewöhnlichen Aktivitäten. Zu den Details gehören Informationen zu dem AWS -Konto, das auf einen Amazon-S3-Bucket zugegriffen hat, die IP-Adresse und die Uhrzeit des Ereignisses.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
12,4. Sicherheit – Audit Trail	Managementsysteme für Daten und Dokumente sollten so konzipiert sein, dass sie die Identität der Betreiber aufzeichnen, die Daten wie Datum und Uhrzeit eingeben, ändern, bestätigen oder löschen.	cloudtrail-enabled	AWS CloudTrail kann durch die Aufzeichnung von Aktionen und API-Aufrufen in der AWS Management Console bei der Nichtabstreitbarkeit helfen. Sie können die Benutzer und die Benutzer AWS-Konten , die einen AWS Dienst aufgerufen haben, die Quell-IP-Adresse, über die die Aufrufe generiert wurden, und den Zeitpunkt der Anrufe identifizieren. Einzelheiten zu den erfassten Daten finden Sie in den AWS CloudTrail Datensatzinhalten.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
12.4. Sicherheit – Audit Trail	Managementsysteme für Daten und Dokumente sollten so konzipiert sein, dass sie die Identität der Betreiber aufzeichnen, die Daten wie Datum und Uhrzeit eingeben, ändern, bestätigen oder löschen.	codebuild-project-logging-enabled	Stellen Sie sicher, dass die AWS CodeBuild Projektprotokollierung aktiviert ist, damit Ihre Build-Ausgabeprotokolle entweder an Amazon CloudWatch oder Amazon Simple Storage Service (Amazon S3) gesendet werden. Build-Ausgabeprotokolle enthalten detaillierte Informationen zu Ihrem Build-Projekt.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
12.4. Sicherheit – Audit Trail	Managementsysteme für Daten und Dokumente sollten so konzipiert sein, dass sie die Identität der Betreiber aufzeichnen, die Daten wie Datum und Uhrzeit eingeben, ändern, bestätigen oder löschen.	elasticsearch-logs-to-cloudwatch	Stellen Sie sicher, dass für Amazon OpenSearch Service-Domains Fehlerprotokolle aktiviert und zur Aufbewahrung und Beantwortung an Amazon CloudWatch Logs gestreamt werden. Domain-Fehlerprotokolle sind bei Sicherheits- und Zugriffsprüfungen sowie bei der Diagnose von Verfügbarkeitsproblemen nützlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
12.4. Sicherheit – Audit Trail	Managementsysteme für Daten und Dokumente sollten so konzipiert sein, dass sie die Identität der Betreiber aufzeichnen, die Daten wie Datum und Uhrzeit eingeben, ändern, bestätigen oder löschen.	multi-region-cloudtrail-enabled	AWS CloudTrail zeichnet Aktionen und API-Aufrufe der AWS Management Console auf. Sie können feststellen, welche Benutzer und Konten angerufen wurden AWS, von welcher Quell-IP-Adresse aus die Anrufe getätigt wurden und wann die Anrufe erfolgten. CloudTrail übermittelt Protokolldateien aus allen AWS Regionen an Ihren S3-Bucket, wenn MULTI_REGION_CLOUD_TRAIL_ENABLED aktiviert ist. Außerdem wird beim AWS Start einer neuen Region derselbe Trail in der neuen Region erstellt. CloudTrail Dadurch erhalten Sie automatisch Protokolldateien mit API-Aktivitäten für die neue Region.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
12.4. Sicherheit – Audit Trail	Managementsysteme für Daten und Dokumente sollten so konzipiert sein, dass sie die Identität der Betreiber aufzeichnen, die Daten wie Datum und Uhrzeit eingeben, ändern, bestätigen oder löschen.	opensearch-audit-logging-enabled	Stellen Sie sicher, dass die Audit-Protokollierung für Ihre Amazon OpenSearch Service-Domains aktiviert ist. Mit der Audit-Protokollierung können Sie Benutzeraktivitäten auf Ihren OpenSearch Domains verfolgen, einschließlich erfolgreicher und fehlgeschlagener Authentifizierungen OpenSearch, Anfragen an, Indexänderungen und eingehende Suchanfragen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
12.4. Sicherheit – Audit Trail	Managementsysteme für Daten und Dokumente sollten so konzipiert sein, dass sie die Identität der Betreiber aufzeichnen, die Daten wie Datum und Uhrzeit eingeben, ändern, bestätigen oder löschen.	opensearch-logs-to-cloudwatch	Stellen Sie sicher, dass für Amazon OpenSearch Service-Domains Fehlerprotokolle aktiviert und zur Aufbewahrung und Beantwortung an Amazon CloudWatch Logs gestreamt werden. OpenSearch Service-Fehlerprotokolle können bei Sicherheits- und Zugriffsprüfungen helfen und bei der Diagnose von Verfügbarkeitsproblemen helfen.
12.4. Sicherheit – Audit Trail	Managementsysteme für Daten und Dokumente sollten so konzipiert sein, dass sie die Identität der Betreiber aufzeichnen, die Daten wie Datum und Uhrzeit eingeben, ändern, bestätigen oder löschen.	redshift-audit-logging-enabled	Aktivieren Sie die Prüfungsprotokollierung, um Informationen über Verbindungen und Benutzeraktivitäten in Ihrem Amazon-Redshift-Cluster zu erfassen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
12,4. Sicherheit – Audit Trail	Managementsysteme für Daten und Dokumente sollten so konzipiert sein, dass sie die Identität der Betreiber aufzeichnen, die Daten wie Datum und Uhrzeit eingeben, ändern, bestätigen oder löschen.	cloud-trail-cloud-watch-logs-aktiviert	Verwenden Sie Amazon CloudWatch , um Protokoll ereignisaktivitäten zentral zu sammeln und zu verwalten. Die Aufnahme von AWS CloudTrail Daten liefert Einzelheiten zu den API-Aufrufaktivitäten in Ihrem AWS-Konto.
12.4. Sicherheit – Audit Trail	Managementsysteme für Daten und Dokumente sollten so konzipiert sein, dass sie die Identität der Betreiber aufzeichnen, die Daten wie Datum und Uhrzeit eingeben, ändern, bestätigen oder löschen.	rds-logging-enabled	Um die Protokollierung und Überwachung in Ihrer Umgebung zu erleichtern, stellen Sie sicher, dass die Amazon Relational Database Service (Amazon RDS)-Protokollierung aktiviert ist. Mit der Amazon-RDS-Protokollierung können Sie Ereignisse wie Verbindungen, Verbindungsabbrüche, Abfragen oder abgefragte Tabellen erfassen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
12,4. Sicherheit – Audit Trail	Managementsysteme für Daten und Dokumente sollten so konzipiert sein, dass sie die Identität der Betreiber aufzeichnen, die Daten wie Datum und Uhrzeit eingeben, ändern, bestätigen oder löschen.	redshift-cluster-configuration-check	Um Daten im Ruhezustand zu schützen, muss die Verschlüsselung für Ihre Amazon-Redshift-Cluster aktiviert sein. Sie müssen auch sicherstellen, dass die erforderlichen Konfigurationen auf Amazon-Redshift-Clustern bereitgestellt werden. Die Prüfungsprotokollierung muss aktiviert sein, um Informationen zu Verbindungen und Benutzeraktivitäten in der Datenbank bereitzustellen. Diese Regel erfordert, dass ein Wert für clusterDbEncrypted (Config Default: TRUE) und LoggingEnabled (Config Default: TRUE) gesetzt ist. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
12.4. Sicherheit – Audit Trail	Managementsysteme für Daten und Dokumente sollten so konzipiert sein, dass sie die Identität der Betreiber aufzeichnen, die Daten wie Datum und Uhrzeit eingeben, ändern, bestätigen oder löschen.	s-3 bucket-logging-enabled	Die Amazon Simple Storage Service (Amazon S3)-Serverzugriffsprotokollierung bietet eine Methode zur Überwachung des Netzwerks im Hinblick auf potenzielle Cybersicherheitsereignisse. Die Ereignisse werden überwacht, indem detaillierte Aufzeichnungen über die Anfragen erfasst werden, die an einen Amazon-S3-Bucket gestellt wurden. Jeder Zugriffsprotokolleintrag enthält Details zu einer einzelnen Zugriffsanfrage. Zu den Details gehören Anforderer, Bucket-Name, Anforderungszeit, Anforderungsaktion, Antwortstatus und Fehlercode, falls relevant.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
13. Vorfallmanagement	Alle Vorfälle, nicht nur System- und Datenfehler, sollten gemeldet und bewertet werden. Die Ursache eines kritischen Vorfalls sollte ermittelt werden und als Grundlage für Korrektur- und Präventivmaßnahmen dienen.	securityhub-enabled	AWS Security Hub hilft bei der Überwachung von unbefugtem Personal, Verbindungen, Geräten und Software. AWS Security Hub aggregiert, organisiert und priorisiert die Sicherheitswarnungen oder Ergebnisse mehrerer Dienste. AWS Einige dieser Dienste sind Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer und AWS Firewall Manager sowie AWS Partnerlösungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
13. Vorfallmanagement	Alle Vorfälle, nicht nur System- und Datenfehler, sollten gemeldet und bewertet werden. Die Ursache eines kritischen Vorfalls sollte ermittelt werden und als Grundlage für Korrektur- und Präventivmaßnahmen dienen.	guardduty-enabled-centralized	Amazon GuardDuty kann mithilfe von Threat Intelligence Feeds helfen, potenzielle Cybersicherheitsereignisse zu überwachen und zu erkennen. Dazu gehören Listen mit bösartigen IPs und maschinellen Lernmethoden zur Identifizierung unerwarteter, nicht autorisierter und bösartiger Aktivitäten in Ihrer AWS Cloud-Umgebung.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
16. Geschäftskontinuität	Für die Verfügbarkeit computergestützter Systeme zur Unterstützung kritischer Prozesse sollten Vorkehrungen getroffen werden, um die Kontinuität der Unterstützung dieser Prozesse im Falle eines Systemausfalls sicherzustellen (z. B. ein manuelles oder alternatives System). Der Zeitaufwand für die Implementierung der alternativen Vorkehrungen sollte sich nach dem Risiko richten und für das jeweilige System und den damit unterstützten Geschäftsprozess angemessen sein. Diese Vorkehrungen sollten angemessen dokumentiert und getestet werden.	aurora-resources-protected-by-Backup-Plan	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon Aurora Aurora-Ressourcen Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
16. Geschäftskontinuität	Für die Verfügbarkeit computergestützter Systeme zur Unterstützung kritischer Prozesse sollten Vorkehrungen getroffen werden, um die Kontinuität der Unterstützung dieser Prozesse im Falle eines Systemausfalls sicherzustellen (z. B. ein manuelles oder alternatives System). Der Zeitaufwand für die Implementierung der alternativen Vorkehrungen sollte sich nach dem Risiko richten und für das jeweilige System und den damit unterstützten Geschäftsprozess angemessen sein. Diese Vorkehrungen sollten angemessen dokumentiert und getestet werden.	backup-plan-min-frequency-and-min-retention-check	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihr AWS Backup-Plan auf eine Mindestfrequenz und Aufbewahrung festgelegt ist. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen. Mit dieser Regel können Sie die Parameter requiredFrequencyValue (Config default: 1), requiredRetentionDays (Config default: 35) und requiredFrequencyUnit

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			(Config default: days) festlegen. Der tatsächliche Wert muss den Anforderungen Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
16. Geschäftskontinuität	Für die Verfügbarkeit computergestützter Systeme zur Unterstützung kritischer Prozesse sollten Vorkehrungen getroffen werden, um die Kontinuität der Unterstützung dieser Prozesse im Falle eines Systemausfalls sicherzustellen (z. B. ein manuelles oder alternatives System). Der Zeitaufwand für die Implementierung der alternativen Vorkehrungen sollte sich nach dem Risiko richten und für das jeweilige System und den damit unterstützten Geschäftsprozess angemessen sein. Diese Vorkehrungen sollten angemessen dokumentiert und getestet werden.	backup-recovery-point-encrypted	Stellen Sie sicher, dass die Verschlüsselung für Ihre AWS Backup-Wiederherstellungspunkte aktiviert ist. Da sensible Daten auch im Ruhezustand vorhanden sein können, sollten Sie die Verschlüsselung im Ruhezustand aktivieren, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
16. Geschäftskontinuität	Für die Verfügbarkeit von Computersystemen, die kritische Prozesse unterstützen, sollten Vorkehrungen getroffen werden, um die Kontinuität der Unterstützung dieser Prozesse im Falle eines Systemausfalls sicherzustellen (z. B. ein manuelles oder alternatives System). Der Zeitaufwand für die Implementierung der alternativen Vorkehrungen sollte sich nach dem Risiko richten und für das jeweilige System und den damit unterstützten Geschäftsprozess angemessen sein. Diese Vorkehrungen sollten angemessen dokumentiert und getestet werden.	backup-recovery-point-manual-Löschung deaktiviert	Stellen Sie sicher, dass Ihren AWS Backup-Wiederherstellungspunkten eine ressourcenbasierte Richtlinie zugeordnet ist, die das Löschen von Wiederherstellungspunkten verhindert. Die Verwendung einer ressourcenbasierten Richtlinie zur Verhinderung des Löschens von Wiederherstellungspunkten kann dazu beitragen, ein versehentliches oder absichtliches Löschen zu unterbinden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
16. Geschäftskontinuität	Für die Verfügbarkeit computergestützter Systeme zur Unterstützung kritischer Prozesse sollten Vorkehrungen getroffen werden, um die Kontinuität der Unterstützung dieser Prozesse im Falle eines Systemausfalls sicherzustellen (z. B. ein manuelles oder alternatives System). Der Zeitaufwand für die Implementierung der alternativen Vorkehrungen sollte sich nach dem Risiko richten und für das jeweilige System und den damit unterstützten Geschäftsprozess angemessen sein. Diese Vorkehrungen sollten angemessen dokumentiert und getestet werden.	backup-recovery-point-minimum-Kontrolle der Aufbewahrung	Um bei Datensicherungsprozessen zu helfen, stellen Sie sicher, dass für Ihre AWS Backup-Wiederherstellungspunkte eine Mindestaufbewahrungsdauer festgelegt ist. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen. Mit dieser Regel können Sie den Parameter requiredRetentionDays (Standardkonfiguration: 35) festlegen. Der tatsächliche Wert muss den Anforderu

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			ngen Ihrer Organisation entsprechen.
16. Geschäftskontinuität	Für die Verfügbarkeit computergestützter Systeme zur Unterstützung kritischer Prozesse sollten Vorkehrungen getroffen werden, um die Kontinuität der Unterstützung dieser Prozesse im Falle eines Systemausfalls sicherzustellen (z. B. ein manuelles oder alternatives System). Der Zeitaufwand für die Implementierung der alternativen Vorkehrungen sollte sich nach dem Risiko richten und für das jeweilige System und den damit unterstützten Geschäftsprozess angemessen sein. Diese Vorkehrungen sollten angemessen dokumentiert und getestet werden.	db-instance-backup-enabled	Die Sicherungsfunktion von Amazon RDS erstellt Sicherungen Ihrer Datenbanken und Transaktionsprotokolle. Amazon RDS erstellt einen Snapshot für das Speichervolume Ihrer DB-Instance, sodass die gesamte DB-Instance gesichert wird. Sie können im System spezifische Aufbewahrungsfristen festlegen, um Ihre Ausfallsicherheitsanforderungen zu erfüllen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
16. Geschäftskontinuität	Für die Verfügbarkeit computergestützter Systeme zur Unterstützung kritischer Prozesse sollten Vorkehrungen getroffen werden, um die Kontinuität der Unterstützung dieser Prozesse im Falle eines Systemausfalls sicherzustellen (z. B. ein manuelles oder alternatives System). Der Zeitaufwand für die Implementierung der alternativen Vorkehrungen sollte sich nach dem Risiko richten und für das jeweilige System und den damit unterstützten Geschäftsprozess angemessen sein. Diese Vorkehrungen sollten angemessen dokumentiert und getestet werden.	dynamodb-in-backup-plan	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon DynamoDB-Tabellen Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
16. Geschäftskontinuität	Für die Verfügbarkeit computergestützter Systeme zur Unterstützung kritischer Prozesse sollten Vorkehrungen getroffen werden, um die Kontinuität der Unterstützung dieser Prozesse im Falle eines Systemausfalls sicherzustellen (z. B. ein manuelles oder alternatives System). Der Zeitaufwand für die Implementierung der alternativen Vorkehrungen sollte sich nach dem Risiko richten und für das jeweilige System und den damit unterstützten Geschäftsprozess angemessen sein. Diese Vorkehrungen sollten angemessen dokumentiert und getestet werden.	dynamodb-pitr-enabled	Aktivieren Sie diese Regel, um zu überprüfen, ob die Informationen gesichert wurden. Es verwaltet auch die Backups, indem es sicherstellt, dass die point-in-time Wiederherstellung in Amazon DynamoDB aktiviert ist. Bei der Wiederherstellung werden fortlaufende Backups Ihrer Tabelle für die letzten 35 Tage gespeichert.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
16. Geschäftskontinuität	Für die Verfügbarkeit computergestützter Systeme zur Unterstützung kritischer Prozesse sollten Vorkehrungen getroffen werden, um die Kontinuität der Unterstützung dieser Prozesse im Falle eines Systemausfalls sicherzustellen (z. B. ein manuelles oder alternatives System). Der Zeitaufwand für die Implementierung der alternativen Vorkehrungen sollte sich nach dem Risiko richten und für das jeweilige System und den damit unterstützten Geschäftsprozess angemessen sein. Diese Vorkehrungen sollten angemessen dokumentiert und getestet werden.	ebs-in-backup-plan	Stellen Sie zur Unterstützung der Datensicherungsprozesse sicher, dass Ihre Amazon Elastic Block Store (Amazon EBS) -Volumes Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihre Backup-Verwaltung und ermöglicht es Ihnen, Ihre geschäftlichen und behördlichen Anforderungen bezüglich Backups zu erfüllen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
16. Geschäftskontinuität	Für die Verfügbarkeit computergestützter Systeme zur Unterstützung kritischer Prozesse sollten Vorkehrungen getroffen werden, um die Kontinuität der Unterstützung dieser Prozesse im Falle eines Systemausfalls sicherzustellen (z. B. ein manuelles oder alternatives System). Der Zeitaufwand für die Implementierung der alternativen Vorkehrungen sollte sich nach dem Risiko richten und für das jeweilige System und den damit unterstützten Geschäftsprozess angemessen sein. Diese Vorkehrungen sollten angemessen dokumentiert und getestet werden.	ebs-optimized-instance	Eine optimierte Instance im Amazon Elastic Block Store (Amazon EBS) bietet zusätzliche, dedizierte Kapazität für Amazon-EBS-I/O-Vorgänge. Diese Optimierung bietet die beste Leistung für Ihr EBS-Volume, indem Konflikte zwischen Amazon-EBS-I/O und anderem Datenverkehr von Ihrer Instance minimiert werden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
16. Geschäftskontinuität	Für die Verfügbarkeit computergestützter Systeme zur Unterstützung kritischer Prozesse sollten Vorkehrungen getroffen werden, um die Kontinuität der Unterstützung dieser Prozesse im Falle eines Systemausfalls sicherzustellen (z. B. ein manuelles oder alternatives System). Der Zeitaufwand für die Implementierung der alternativen Vorkehrungen sollte sich nach dem Risiko richten und für das jeweilige System und den damit unterstützten Geschäftsprozess angemessen sein. Diese Vorkehrungen sollten angemessen dokumentiert und getestet werden.	ebs-resources-protected-by-Backup-Plan	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon Elastic Block Store (Amazon EBS) -Ressourcen Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihre Backup-Verwaltung und ermöglicht es Ihnen, Ihre geschäftlichen und behördlichen Anforderungen bezüglich Backups zu erfüllen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
16. Geschäftskontinuität	Für die Verfügbarkeit computergestützter Systeme zur Unterstützung kritischer Prozesse sollten Vorkehrungen getroffen werden, um die Kontinuität der Unterstützung dieser Prozesse im Falle eines Systemausfalls sicherzustellen (z. B. ein manuelles oder alternatives System). Der Zeitaufwand für die Implementierung der alternativen Vorkehrungen sollte sich nach dem Risiko richten und für das jeweilige System und den damit unterstützten Geschäftsprozess angemessen sein. Diese Vorkehrungen sollten angemessen dokumentiert und getestet werden.	ec2-Plan resources-protected-by-backup	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon Elastic Compute Cloud (Amazon EC2) -Ressourcen Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
16. Geschäftskontinuität	Für die Verfügbarkeit computergestützter Systeme zur Unterstützung kritischer Prozesse sollten Vorkehrungen getroffen werden, um die Kontinuität der Unterstützung dieser Prozesse im Falle eines Systemausfalls sicherzustellen (z. B. ein manuelles oder alternatives System). Der Zeitaufwand für die Implementierung der alternativen Vorkehrungen sollte sich nach dem Risiko richten und für das jeweilige System und den damit unterstützten Geschäftsprozess angemessen sein. Diese Vorkehrungen sollten angemessen dokumentiert und getestet werden.	efs-in-backup-plan	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon Elastic File System (Amazon EFS) -Dateisysteme Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
16. Geschäftskontinuität	Für die Verfügbarkeit computergestützter Systeme zur Unterstützung kritischer Prozesse sollten Vorkehrungen getroffen werden, um die Kontinuität der Unterstützung dieser Prozesse im Falle eines Systemausfalls sicherzustellen (z. B. ein manuelles oder alternatives System). Der Zeitaufwand für die Implementierung der alternativen Vorkehrungen sollte sich nach dem Risiko richten und für das jeweilige System und den damit unterstützten Geschäftsprozess angemessen sein. Diese Vorkehrungen sollten angemessen dokumentiert und getestet werden.	efs-resources-protected-by-Backup-Plan	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon Elastic File System (Amazon EFS) -Dateisysteme Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
16. Geschäftskontinuität	Für die Verfügbarkeit computergestützter Systeme zur Unterstützung kritischer Prozesse sollten Vorkehrungen getroffen werden, um die Kontinuität der Unterstützung dieser Prozesse im Falle eines Systemausfalls sicherzustellen (z. B. ein manuelles oder alternatives System). Der Zeitaufwand für die Implementierung der alternativen Vorkehrungen sollte sich nach dem Risiko richten und für das jeweilige System und den damit unterstützten Geschäftsprozess angemessen sein. Diese Vorkehrungen sollten angemessen dokumentiert und getestet werden.	elasticache-redis-cluster-automatic-Backup-Check	Wenn automatische Backups aktiviert sind, ElastiCache erstellt Amazon täglich ein Backup des Clusters. Die Sicherung kann für eine von Ihrer Organisation festgelegte Anzahl von Tagen aufbewahrt werden. Automatische Backups schützen vor Datenverlust. Bei einem Ausfall können Sie einen neuen Cluster erstellen, der Ihre Daten aus dem aktuellen Backup wiederherstellt.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
16. Geschäftskontinuität	Für die Verfügbarkeit computergestützter Systeme zur Unterstützung kritischer Prozesse sollten Vorkehrungen getroffen werden, um die Kontinuität der Unterstützung dieser Prozesse im Falle eines Systemausfalls sicherzustellen (z. B. ein manuelles oder alternatives System). Der Zeitaufwand für die Implementierung der alternativen Vorkehrungen sollte sich nach dem Risiko richten und für das jeweilige System und den damit unterstützten Geschäftsprozess angemessen sein. Diese Vorkehrungen sollten angemessen dokumentiert und getestet werden.	elbv2-multiple-az	Elastic Load Balancing (ELB) verteilt Ihren eingehenden Traffic automatisch auf mehrere Ziele wie EC2 Instances, Container und IP-Adressen in einer Availability Zone. Zur Gewährleistung einer hohen Verfügbarkeit stellen Sie sicher, dass Ihr ELB Instances aus mehreren Availability Zones registriert hat.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
16. Geschäftskontinuität	Für die Verfügbarkeit computergestützter Systeme zur Unterstützung kritischer Prozesse sollten Vorkehrungen getroffen werden, um die Kontinuität der Unterstützung dieser Prozesse im Falle eines Systemausfalls sicherzustellen (z. B. ein manuelles oder alternatives System). Der Zeitaufwand für die Implementierung der alternativen Vorkehrungen sollte sich nach dem Risiko richten und für das jeweilige System und den damit unterstützten Geschäftsprozess angemessen sein. Diese Vorkehrungen sollten angemessen dokumentiert und getestet werden.	elb-cross-zone-load-Balancing aktiviert	Aktivieren Sie zonenübergreifendes Load Balancing für Ihre Elastic Load Balancer (ELBs), um eine angemessene Kapazität und Verfügbarkeit aufrechtzuerhalten. Zonenübergreifendes Load Balancing reduziert die Notwendigkeit, die gleiche Anzahl von Instances in jeder aktivierten Availability Zone aufrechtzuerhalten. Es verbessert auch die Fähigkeit Ihrer Anwendung, den Verlust einer oder mehrerer Instances zu bewältigen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
16. Geschäftskontinuität	Für die Verfügbarkeit computergestützter Systeme zur Unterstützung kritischer Prozesse sollten Vorkehrungen getroffen werden, um die Kontinuität der Unterstützung dieser Prozesse im Falle eines Systemausfalls sicherzustellen (z. B. ein manuelles oder alternatives System). Der Zeitaufwand für die Implementierung der alternativen Vorkehrungen sollte sich nach dem Risiko richten und für das jeweilige System und den damit unterstützten Geschäftsprozess angemessen sein. Diese Vorkehrungen sollten angemessen dokumentiert und getestet werden.	fsx-resources-protected-by-Backup-Plan	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre FSx Amazon-Dateisysteme Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
16. Geschäftskontinuität	Für die Verfügbarkeit computergestützter Systeme zur Unterstützung kritischer Prozesse sollten Vorkehrungen getroffen werden, um die Kontinuität der Unterstützung dieser Prozesse im Falle eines Systemausfalls sicherzustellen (z. B. ein manuelles oder alternatives System). Der Zeitaufwand für die Implementierung der alternativen Vorkehrungen sollte sich nach dem Risiko richten und für das jeweilige System und den damit unterstützten Geschäftsprozess angemessen sein. Diese Vorkehrungen sollten angemessen dokumentiert und getestet werden.	lambda-vpc-multi-az-überprüfen	Wenn Ihre AWS Lambda-Funktion so konfiguriert ist, dass sie eine Verbindung zu einer Virtual Private Cloud (VPC) in Ihrem Konto herstellt, stellen Sie die AWS Lambda-Funktion in mindestens zwei verschiedenen Availability Zones bereit, um sicherzustellen, dass Ihre Funktion für die Verarbeitung von Ereignissen im Falle einer Dienstunterbrechung in einer einzigen Zone verfügbar ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
16. Geschäftskontinuität	Für die Verfügbarkeit computergestützter Systeme zur Unterstützung kritischer Prozesse sollten Vorkehrungen getroffen werden, um die Kontinuität der Unterstützung dieser Prozesse im Falle eines Systemausfalls sicherzustellen (z. B. ein manuelles oder alternatives System). Der Zeitaufwand für die Implementierung der alternativen Vorkehrungen sollte sich nach dem Risiko richten und für das jeweilige System und den damit unterstützten Geschäftsprozess angemessen sein. Diese Vorkehrungen sollten angemessen dokumentiert und getestet werden.	opensearch-data-node-fault-Toleranz	Amazon OpenSearch Service (OpenSearch Service) benötigt mindestens drei Datenknoten für hohe Verfügbarkeit und Fehlertoleranz. Durch die Bereitstellung einer OpenSearch Service-Domain mit mindestens drei Datenknoten wird der Cluster-Betrieb gewährleistet, falls ein Knoten ausfällt.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
16. Geschäftskontinuität	Für die Verfügbarkeit computergestützter Systeme zur Unterstützung kritischer Prozesse sollten Vorkehrungen getroffen werden, um die Kontinuität der Unterstützung dieser Prozesse im Falle eines Systemausfalls sicherzustellen (z. B. ein manuelles oder alternatives System). Der Zeitaufwand für die Implementierung der alternativen Vorkehrungen sollte sich nach dem Risiko richten und für das jeweilige System und den damit unterstützten Geschäftsprozess angemessen sein. Diese Vorkehrungen sollten angemessen dokumentiert und getestet werden.	rds-cluster-deletion-protection-aktiviert	Stellen Sie sicher, dass Amazon Relational Database Service (Amazon RDS)-Instances den Löschschutz aktiviert haben. Verwenden Sie den Löschschutz, um zu verhindern, dass Ihre Amazon-RDS-Instances versehentlich oder böswillig gelöscht werden, was zum Verlust der Verfügbarkeit Ihrer Anwendungen führen kann.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
16. Geschäftskontinuität	Für die Verfügbarkeit computergestützter Systeme zur Unterstützung kritischer Prozesse sollten Vorkehrungen getroffen werden, um die Kontinuität der Unterstützung dieser Prozesse im Falle eines Systemausfalls sicherzustellen (z. B. ein manuelles oder alternatives System). Der Zeitaufwand für die Implementierung der alternativen Vorkehrungen sollte sich nach dem Risiko richten und für das jeweilige System und den damit unterstützten Geschäftsprozess angemessen sein. Diese Vorkehrungen sollten angemessen dokumentiert und getestet werden.	rds-instance-deletion-protection-aktiviert	Stellen Sie sicher, dass Amazon Relational Database Service (Amazon RDS)-Instances den Löschschutz aktiviert haben. Verwenden Sie den Löschschutz, um zu verhindern, dass Ihre Amazon-RDS-Instances versehentlich oder böswillig gelöscht werden, was zum Verlust der Verfügbarkeit Ihrer Anwendungen führen kann.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
16. Geschäftskontinuität	Für die Verfügbarkeit computergestützter Systeme zur Unterstützung kritischer Prozesse sollten Vorkehrungen getroffen werden, um die Kontinuität der Unterstützung dieser Prozesse im Falle eines Systemausfalls sicherzustellen (z. B. ein manuelles oder alternatives System). Der Zeitaufwand für die Implementierung der alternativen Vorkehrungen sollte sich nach dem Risiko richten und für das jeweilige System und den damit unterstützten Geschäftsprozess angemessen sein. Diese Vorkehrungen sollten angemessen dokumentiert und getestet werden.	rds-in-backup-plan	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon Relational Database Service (Amazon RDS) -Instances Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
16. Geschäftskontinuität	Für die Verfügbarkeit computergestützter Systeme zur Unterstützung kritischer Prozesse sollten Vorkehrungen getroffen werden, um die Kontinuität der Unterstützung dieser Prozesse im Falle eines Systemausfalls sicherzustellen (z. B. ein manuelles oder alternatives System). Der Zeitaufwand für die Implementierung der alternativen Vorkehrungen sollte sich nach dem Risiko richten und für das jeweilige System und den damit unterstützten Geschäftsprozess angemessen sein. Diese Vorkehrungen sollten angemessen dokumentiert und getestet werden.	redshift-backup-enabled	Stellen Sie zur Unterstützung der Datensicherungsprozesse sicher, dass Ihre Amazon-Redshift-Cluster über automatisierte Snapshots verfügen. Wenn automatisierte Snapshots für einen Cluster aktiviert sind, erstellt Redshift in regelmäßigen Abständen Snapshots dieses Clusters. Standardmäßig erstellt Redshift alle acht Stunden oder alle 5 GB einen Snapshot für jeden Knoten mit Datenänderungen oder je nachdem, was zuerst eintritt.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
16. Geschäftskontinuität	Für die Verfügbarkeit computergestützter Systeme zur Unterstützung kritischer Prozesse sollten Vorkehrungen getroffen werden, um die Kontinuität der Unterstützung dieser Prozesse im Falle eines Systemausfalls sicherzustellen (z. B. ein manuelles oder alternatives System). Der Zeitaufwand für die Implementierung der alternativen Vorkehrungen sollte sich nach dem Risiko richten und für das jeweilige System und den damit unterstützten Geschäftsprozess angemessen sein. Diese Vorkehrungen sollten angemessen dokumentiert und getestet werden.	s3- bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) unterstützt die Aufrechterhaltung einer angemessenen Kapazität und Verfügbarkeit. CRR ermöglicht das automatische, asynchrone Kopieren von Objekten in Amazon-S3-Buckets, um die Datenverfügbarkeit sicherzustellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
16. Geschäftskontinuität	Für die Verfügbarkeit computergestützter Systeme zur Unterstützung kritischer Prozesse sollten Vorkehrungen getroffen werden, um die Kontinuität der Unterstützung dieser Prozesse im Falle eines Systemausfalls sicherzustellen (z. B. ein manuelles oder alternatives System). Der Zeitaufwand für die Implementierung der alternativen Vorkehrungen sollte sich nach dem Risiko richten und für das jeweilige System und den damit unterstützten Geschäftsprozess angemessen sein. Diese Vorkehrungen sollten angemessen dokumentiert und getestet werden.	s3- bucket-versioning-enabled	Die Versionsverwaltung von Amazon Simple Storage Service (Amazon S3)-Buckets hilft dabei, mehrere Varianten eines Objekts im selben Amazon-S3-Bucket zu speichern. Verwenden Sie die Versionsverwaltung, um sämtliche Versionen aller Objekte in Ihrem Amazon-S3-Bucket zu speichern, abzurufen oder wiederherzustellen. Mit der Versionsverwaltung können Sie Versionen sowohl nach unbeabsichtigten Benutzeraktionen als auch nach Anwendungsfehlern problemlos wiederherstellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
16. Geschäftskontinuität	Für die Verfügbarkeit computergestützter Systeme zur Unterstützung kritischer Prozesse sollten Vorkehrungen getroffen werden, um die Kontinuität der Unterstützung dieser Prozesse im Falle eines Systemausfalls sicherzustellen (z. B. ein manuelles oder alternatives System). Der Zeitaufwand für die Implementierung der alternativen Vorkehrungen sollte sich nach dem Risiko richten und für das jeweilige System und den damit unterstützten Geschäftsprozess angemessen sein. Diese Vorkehrungen sollten angemessen dokumentiert und getestet werden.	elb-deletion-protection-enabled	Diese Regel sorgt dafür, dass der Löschschutz für Elastic Load Balancing aktiviert ist. Verwenden Sie diese Funktion, um zu verhindern, dass Ihr Load Balancer versehentlich oder böswillig gelöscht wird, was zum Verlust der Verfügbarkeit Ihrer Anwendungen führen kann.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
16. Geschäftskontinuität	Für die Verfügbarkeit computergestützter Systeme zur Unterstützung kritischer Prozesse sollten Vorkehrungen getroffen werden, um die Kontinuität der Unterstützung dieser Prozesse im Falle eines Systemausfalls sicherzustellen (z. B. ein manuelles oder alternatives System). Der Zeitaufwand für die Implementierung der alternativen Vorkehrungen sollte sich nach dem Risiko richten und für das jeweilige System und den damit unterstützten Geschäftsprozess angemessen sein. Diese Vorkehrungen sollten angemessen dokumentiert und getestet werden.	rds-cluster-multi-az-aktiviert	Für Cluster von Amazon Relational Database Service (Amazon RDS) sollte die Multi-AZ-Replikation aktiviert sein, um die Verfügbarkeit der gespeicherten Daten zu gewährleisten. Availability Zones werden auf einer physisch getrennten, unabhängigen Infrastruktur ausgeführt und sind auf höchste Zuverlässigkeit ausgelegt. Im Falle eines Infrastrukturausfalls führt Amazon RDS einen automatischen Failover zum Standby-Modus durch, sodass Sie den Datenbankbetrieb wieder aufnehmen können, sobald der Failover abgeschlossen ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
16. Geschäftskontinuität	Für die Verfügbarkeit computergestützter Systeme zur Unterstützung kritischer Prozesse sollten Vorkehrungen getroffen werden, um die Kontinuität der Unterstützung dieser Prozesse im Falle eines Systemausfalls sicherzustellen (z. B. ein manuelles oder alternatives System). Der Zeitaufwand für die Implementierung der alternativen Vorkehrungen sollte sich nach dem Risiko richten und für das jeweilige System und den damit unterstützten Geschäftsprozess angemessen sein. Diese Vorkehrungen sollten angemessen dokumentiert und getestet werden.	rds-multi-az-support	Die Multi-AZ-Unterstützung in Amazon Relational Database Service (Amazon RDS) bietet eine verbesserte Verfügbarkeit und Beständigkeit von Datenbank-Instances. Wenn Sie eine Multi-AZ-Datenbank-Instance bereitstellen, erstellt Amazon RDS automatisch eine primäre Datenbank-Instance und repliziert die Daten synchron auf eine Standby-Instance in einer anderen Availability Zone. Jede Availability Zone läuft auf einer eigenen, physisch getrennten, unabhängigen Infrastruktur und ist auf eine hohe Verfügbarkeit ausgelegt. Im Falle eines Infrastrukturausfalls führt Amazon RDS einen automatis

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			chen Failover zum Standby-Modus durch, sodass Sie den Datenbankbetrieb wieder aufnehmen können, sobald der Failover abgeschlo ssen ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
16. Geschäftskontinuität	Für die Verfügbarkeit computergestützter Systeme zur Unterstützung kritischer Prozesse sollten Vorkehrungen getroffen werden, um die Kontinuität der Unterstützung dieser Prozesse im Falle eines Systemausfalls sicherzustellen (z. B. ein manuelles oder alternatives System). Der Zeitaufwand für die Implementierung der alternativen Vorkehrungen sollte sich nach dem Risiko richten und für das jeweilige System und den damit unterstützten Geschäftsprozess angemessen sein. Diese Vorkehrungen sollten angemessen dokumentiert und getestet werden.	vpc-vpn-2-tunnels-up	Um die Anforderungen an die Ausfallsicherheit zu erfüllen, können redundante Site-to-Site VPN-Tunnel eingerichtet werden. Es verwendet zwei Tunnel, um die Konnektivität sicherzustellen, falls eine der Site-to-Site VPN-Verbindungen nicht verfügbar ist. Um sich vor einem Verbindungsverlust zu schützen, können Sie für den Fall, dass Ihr Kunden-Gateway nicht verfügbar ist, eine zweite Site-to-Site VPN-Verbindung zu Ihrer Amazon Virtual Private Cloud (Amazon VPC) und Ihrem Virtual Private Gateway einrichten, indem Sie ein zweites Kunden-Gateway verwenden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
17. Archivierung	Daten können archiviert werden. Diese Daten sollten auf Zugänglichkeit, Lesbarkeit und Integrität überprüft werden. Wenn relevante Änderungen am System vorgenommen werden sollen (z. B. Computerausrüstung oder Programme), sollte die Fähigkeit, die Daten abzurufen, sichergestellt und getestet werden.	aurora-resources-protected-by-Backup-Plan	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon Aurora Aurora-Ressourcen Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
17. Archivierung	Daten können archiviert werden. Diese Daten sollten auf Zugänglichkeit, Lesbarkeit und Integrität überprüft werden. Wenn relevante Änderungen am System vorgenommen werden sollen (z. B. Computerausrüstung oder Programme), sollte die Fähigkeit, die Daten abzurufen, sichergestellt und getestet werden.	backup-plan-min-frequency-and-min-retention-check	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihr AWS Backup-Plan auf eine Mindestfrequenz und Aufbewahrung festgelegt ist. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen. Mit dieser Regel können Sie die Parameter requiredFrequencyValue (Config default: 1), requiredRetentionDays (Config default: 35) und requiredFrequencyUnit

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			(Config default: days) festlegen. Der tatsächliche Wert muss den Anforderungen Ihrer Organisation entsprechen.
17. Archivierung	Daten können archiviert werden. Diese Daten sollten auf Zugänglichkeit, Lesbarkeit und Integrität überprüft werden. Wenn relevante Änderungen am System vorgenommen werden sollen (z. B. Computerausrüstung oder Programme), sollte die Fähigkeit, die Daten abzurufen, sichergestellt und getestet werden.	backup-recovery-point-encrypted	Stellen Sie sicher, dass die Verschlüsselung für Ihre AWS Backup-Wiederherstellungspunkte aktiviert ist. Da sensible Daten auch im Ruhezustand vorhanden sein können, sollten Sie die Verschlüsselung im Ruhezustand aktivieren, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
17. Archivierung	Daten können archiviert werden. Diese Daten sollten auf Zugänglichkeit, Lesbarkeit und Integrität überprüft werden. Wenn relevante Änderungen am System vorgenommen werden sollen (z. B. Computerausrüstung oder Programme), sollte die Fähigkeit, die Daten abzurufen, sichergestellt und getestet werden.	backup-recovery-point-manual-Löschen-deaktiviert	Stellen Sie sicher, dass Ihren AWS Backup-Wiederherstellungspunkten eine ressourcenbasierte Richtlinie zugeordnet ist, die das Löschen von Wiederherstellungspunkten verhindert. Die Verwendung einer ressourcenbasierten Richtlinie zur Verhinderung des Löschens von Wiederherstellungspunkten kann dazu beitragen, ein versehentliches oder absichtliches Löschen zu unterbinden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
17. Archivierung	Daten können archiviert werden. Diese Daten sollten auf Zugänglichkeit, Lesbarkeit und Integrität überprüft werden. Wenn relevante Änderungen am System vorgenommen werden sollen (z. B. Computerausrüstung oder Programme), sollte die Fähigkeit, die Daten abzurufen, sichergestellt und getestet werden.	backup-recovery-point-minimum-Aufbewahrungsprüfung	Um bei Datensicherungsprozessen zu helfen, stellen Sie sicher, dass für Ihre AWS Backup-Wiederherstellungspunkte eine Mindestaufbewahrungsdauer festgelegt ist. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen. Mit dieser Regel können Sie den Parameter requiredRetentionDays (Standardkonfiguration: 35) festlegen. Der tatsächliche Wert muss den Anforderu

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			ngen Ihrer Organisat ion entsprechen.
17. Archivierung	Daten können archiviert werden. Diese Daten sollten auf Zugänglic hkeit, Lesbarkei t und Integrität überprüft werden. Wenn relevante Änderungen am System vorgenomm en werden sollen (z. B. Computera usrüstung oder Programme), sollte die Fähigkeit zum Abrufen der Daten sichergestellt und getestet werden.	db-instance-backup-enabled	Die Sicherung sfunktion von Amazon RDS erstellt Sicherung en Ihrer Datenbank en und Transakti onsprotokolle. Amazon RDS erstellt einen Snapshot für das Speichervolume Ihrer DB-Instance, sodass die gesamte DB-Instance gesichert wird. Sie können im System spezifische Aufbewahrungsfrist en festlegen, um Ihre Ausfallsicherheits anforderungen zu erfüllen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
17. Archivierung	Daten können archiviert werden. Diese Daten sollten auf Zugänglichkeit, Lesbarkeit und Integrität überprüft werden. Wenn relevante Änderungen am System vorgenommen werden sollen (z. B. Computerausrüstung oder Programme), sollte die Fähigkeit, die Daten abzurufen, sichergestellt und getestet werden.	dynamodb-in-backup-plan	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon DynamoDB-Tabellen Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
17. Archivierung	Daten können archiviert werden. Diese Daten sollten auf Zugänglichkeit, Lesbarkeit und Integrität überprüft werden. Wenn relevante Änderungen am System vorgenommen werden sollen (z. B. Computerausrüstung oder Programme), sollte die Fähigkeit, die Daten abzurufen, sichergestellt und getestet werden.	dynamodb-pitr-enabled	Aktivieren Sie diese Regel, um zu überprüfen, ob die Informationen gesichert wurden. Es verwaltet auch die Backups, indem es sicherstellt, dass die point-in-time Wiederherstellung in Amazon DynamoDB aktiviert ist. Bei der Wiederherstellung werden fortlaufende Backups Ihrer Tabelle für die letzten 35 Tage gespeichert.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
17. Archivierung	Daten können archiviert werden. Diese Daten sollten auf Zugänglichkeit, Lesbarkeit und Integrität überprüft werden. Wenn relevante Änderungen am System vorgenommen werden sollen (z. B. Computerausrüstung oder Programme), sollte die Fähigkeit, die Daten abzurufen, sichergestellt und getestet werden.	ebs-in-backup-plan	Stellen Sie zur Unterstützung der Datensicherungsprozesse sicher, dass Ihre Amazon Elastic Block Store (Amazon EBS) -Volumes Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihre Backup-Verwaltung und ermöglicht es Ihnen, Ihre geschäftlichen und behördlichen Anforderungen bezüglich Backups zu erfüllen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
17. Archivierung	Daten können archiviert werden. Diese Daten sollten auf Zugänglichkeit, Lesbarkeit und Integrität überprüft werden. Wenn relevante Änderungen am System vorgenommen werden sollen (z. B. Computerausrüstung oder Programme), sollte die Fähigkeit, die Daten abzurufen, sichergestellt und getestet werden.	ebs-optimized-instance	Eine optimierte Instance im Amazon Elastic Block Store (Amazon EBS) bietet zusätzliche, dedizierte Kapazität für Amazon-EBS-I/O-Vorgänge. Diese Optimierung bietet die beste Leistung für Ihr EBS-Volume, indem Konflikte zwischen Amazon-EBS-I/O und anderem Datenverkehr von Ihrer Instance minimiert werden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
17. Archivierung	Daten können archiviert werden. Diese Daten sollten auf Zugänglichkeit, Lesbarkeit und Integrität überprüft werden. Wenn relevante Änderungen am System vorgenommen werden sollen (z. B. Computerausrüstung oder Programme), sollte die Fähigkeit, die Daten abzurufen, sichergestellt und getestet werden.	ebs-resources-protected-by-Backup-Plan	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon Elastic Block Store (Amazon EBS) -Ressourcen Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihre Backup-Verwaltung und ermöglicht es Ihnen, Ihre geschäftlichen und behördlichen Anforderungen bezüglich Backups zu erfüllen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
17. Archivierung	Daten können archiviert werden. Diese Daten sollten auf Zugänglichkeit, Lesbarkeit und Integrität überprüft werden. Wenn relevante Änderungen am System vorgenommen werden sollen (z. B. Computerausrüstung oder Programme), sollte die Fähigkeit, die Daten abzurufen, sichergestellt und getestet werden.	ec2--Plan resources-protected-by-backup	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon Elastic Compute Cloud (Amazon EC2) -Ressourcen Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
17. Archivierung	Daten können archiviert werden. Diese Daten sollten auf Zugänglichkeit, Lesbarkeit und Integrität überprüft werden. Wenn relevante Änderungen am System vorgenommen werden sollen (z. B. Computerausrüstung oder Programme), sollte die Fähigkeit, die Daten abzurufen, sichergestellt und getestet werden.	efs-in-backup-plan	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon Elastic File System (Amazon EFS) -Dateisysteme Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
17. Archivierung	Daten können archiviert werden. Diese Daten sollten auf Zugänglichkeit, Lesbarkeit und Integrität überprüft werden. Wenn relevante Änderungen am System vorgenommen werden sollen (z. B. Computerausrüstung oder Programme), sollte die Fähigkeit, die Daten abzurufen, sichergestellt und getestet werden.	efs-resources-protected-by-Backup-Plan	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon Elastic File System (Amazon EFS) -Dateisysteme Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
17. Archivierung	Daten können archiviert werden. Diese Daten sollten auf Zugänglichkeit, Lesbarkeit und Integrität überprüft werden. Wenn relevante Änderungen am System vorgenommen werden sollen (z. B. Computerausrüstung oder Programme), sollte die Fähigkeit, die Daten abzurufen, sichergestellt und getestet werden.	elasticache-redis-cluster-automatic-Backup-Check	Wenn automatische Backups aktiviert sind, ElastiCache erstellt Amazon täglich ein Backup des Clusters. Die Sicherung kann für eine von Ihrer Organisation festgelegte Anzahl von Tagen aufbewahrt werden. Automatische Backups schützen vor Datenverlust. Bei einem Ausfall können Sie einen neuen Cluster erstellen, der Ihre Daten aus dem aktuellen Backup wiederherstellt.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
17. Archivierung	Daten können archiviert werden. Diese Daten sollten auf Zugänglichkeit, Lesbarkeit und Integrität überprüft werden. Wenn relevante Änderungen am System vorgenommen werden sollen (z. B. Computerausrüstung oder Programme), sollte die Fähigkeit, die Daten abzurufen, sichergestellt und getestet werden.	fsx-resources-protected-by-Backup-Plan	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre FSx Amazon-Dateisysteme Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
17. Archivierung	Daten können archiviert werden. Diese Daten sollten auf Zugänglichkeit, Lesbarkeit und Integrität überprüft werden. Wenn relevante Änderungen am System vorgenommen werden sollen (z. B. Computerausrüstung oder Programme), sollte die Fähigkeit, die Daten abzurufen, sichergestellt und getestet werden.	rds-in-backup-plan	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon Relational Database Service (Amazon RDS) -Instances Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
17. Archivierung	Daten können archiviert werden. Diese Daten sollten auf Zugänglichkeit, Lesbarkeit und Integrität überprüft werden. Wenn relevante Änderungen am System vorgenommen werden sollen (z. B. Computerausrüstung oder Programme), sollte die Fähigkeit, die Daten abzurufen, sichergestellt und getestet werden.	redshift-backup-enabled	Stellen Sie zur Unterstützung der Datensicherungsprozesse sicher, dass Ihre Amazon-Redshift-Cluster über automatisierte Snapshots verfügen. Wenn automatisierte Snapshots für einen Cluster aktiviert sind, erstellt Redshift in regelmäßigen Abständen Snapshots dieses Clusters. Standardmäßig erstellt Redshift alle acht Stunden oder alle 5 GB einen Snapshot für jeden Knoten mit Datenänderungen oder je nachdem, was zuerst eintritt.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
17. Archivierung	Daten können archiviert werden. Diese Daten sollten auf Zugänglichkeit, Lesbarkeit und Integrität überprüft werden. Wenn relevante Änderungen am System vorgenommen werden sollen (z. B. Computerausrüstung oder Programme), sollte die Fähigkeit, die Daten abzurufen, sichergestellt und getestet werden.	s-3 bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) unterstützt die Aufrechterhaltung einer angemessenen Kapazität und Verfügbarkeit. CRR ermöglicht das automatische, asynchrone Kopieren von Objekten in Amazon-S3-Buckets, um die Datenverfügbarkeit sicherzustellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
17. Archivierung	Daten können archiviert werden. Diese Daten sollten auf Zugänglichkeit, Lesbarkeit und Integrität überprüft werden. Wenn relevante Änderungen am System vorgenommen werden sollen (z. B. Computerausrüstung oder Programme), sollte die Fähigkeit zum Abrufen der Daten sichergestellt und getestet werden.	s-3 bucket-versioning-enabled	Die Versionsverwaltung von Amazon Simple Storage Service (Amazon S3)-Buckets hilft dabei, mehrere Varianten eines Objekts im selben Amazon-S3-Bucket zu speichern. Verwenden Sie die Versionsverwaltung, um sämtliche Versionen aller Objekte in Ihrem Amazon-S3-Bucket zu speichern, abzurufen oder wiederherzustellen. Mit der Versionsverwaltung können Sie Versionen sowohl nach unbeabsichtigten Benutzeraktionen als auch nach Anwendungsfehlern problemlos wiederherstellen.

Vorlage

Die Vorlage ist verfügbar unter GitHub: Operational Best Practices for GxP EU Annex 11.

Betriebliche bewährte Methoden für die HIPAA-Sicherheit

Konformitätspakete bieten ein allgemeines Compliance-Framework, das es Ihnen ermöglicht, mithilfe verwalteter oder benutzerdefinierter Regeln und Abhilfemaßnahmen Kontrollen zur Sicherheits-, Betriebs- oder Kostenoptimierung durchzuführen. AWS Config AWS Config Conformance Packs dienen als Beispielvorlagen nicht dazu, die vollständige Einhaltung eines bestimmten Governance- oder Compliance-Standards sicherzustellen. Sie sind dafür verantwortlich, selbst zu beurteilen, ob Ihre Nutzung der Services den geltenden gesetzlichen und behördlichen Anforderungen entspricht.

Im Folgenden finden Sie ein Beispiel für eine Zuordnung zwischen dem Health Insurance Portability and Accountability Act (HIPAA) und den AWS verwalteten Konfigurationsregeln. Jede Config-Regel gilt für eine bestimmte AWS Ressource und bezieht sich auf eine oder mehrere HIPAA-Kontrollen. Eine HIPAA-Kontrolle kann mehreren Config-Regeln zugeordnet werden. In der folgenden Tabelle finden Sie weitere Informationen und Anleitungen zu diesen Zuordnungen.

Dieses Konformitätspaket wurde von AWS Security Assurance Services LLC (AWS SAS) validiert. Dabei handelt es sich um ein Team von qualifizierten Sicherheitsbewertern () für die Zahlungskartenbranche (QSAs), HITRUST-zertifizierten Common Security Framework Practitionern (CCSFPs) und Compliance-Experten, die für die Bereitstellung von Leitlinien und Bewertungen für verschiedene Branchen-Frameworks zertifiziert sind. AWS Die Experten von SAS haben dieses Conformance Pack so konzipiert, dass sich ein Kunde an einen Teil des HIPAA anpassen kann.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.308(a)(1)(ii)(A)	(A) Risikoanalyse (erforderlich). Führen Sie eine genaue und gründliche Bewertung der potenziellen Risiken und Schwachst ellen in Bezug auf die Vertrauli chkeit, Integritä t und Verfügbar keit von elektroni sch geschützten	annual-risk-assess ment-performed (Prozessüberprüfung)	Führen Sie eine jährliche Risikobew ertung für Ihre Organisation durch. Risikowertungen können dabei helfen, die Wahrscheinlichkeit und Auswirkun gen identifizierter Risiken und/oder Schwachstellen für eine Organisation zu ermitteln.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	Gesundheitsinformationen durch, die sich im Besitz der jeweiligen Entität befinden.		
164.308(a)(1)(ii)(B)	(B) Risikomanagement (erforderlich). Implementieren Sie ausreichende Sicherheitsmaßnahmen, um Risiken und Schwachstellen auf ein angemessenes Maß zu reduzieren und die Vorgaben aus Abschnitt 164.306(a) zu erfüllen.	alb-http-to-https-Umleitungsprüfung	Um Daten während der Übertragung zu schützen, stellen Sie sicher, dass Ihr Application Load Balancer unverschlüsselte HTTP-Anfragen automatisch an HTTPS umleitet. Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.308(a)(1)(ii)(B)	(B) Risikomanagement (erforderlich). Implementieren Sie ausreichende Sicherheitsmaßnahmen, um Risiken und Schwachstellen auf ein angemessenes Maß zu reduzieren und die Vorgaben aus Abschnitt 164.306(a) zu erfüllen.	autoscaling-group-elb-healthcheck-erforderlich	Die Elastic Load Balancer (ELB) - Zustandsprüfungen für Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling Scaling-Gruppen unterstützen die Aufrechterhaltung einer angemessenen Kapazität und Verfügbarkeit. Der Load Balancer sendet regelmäßig Pings, versucht Verbindungen herzustellen oder sendet Anfragen, um den Zustand der EC2 Amazon-Instances in einer Gruppe mit auto-scaling zu testen. Wenn eine Instance nicht zurückmeldet, wird der Traffic an eine neue EC2 Amazon-Instance gesendet.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.308(a)(1)(ii)(B)	(B) Risikomanagement (erforderlich). Implementieren Sie ausreichende Sicherheitsmaßnahmen, um Risiken und Schwachstellen auf ein angemessenes Maß zu reduzieren und die Vorgaben aus Abschnitt 164.306(a) zu erfüllen.	cloud-trail-encryption-enabled	Da sensible Daten vorhanden sein können und um Daten im Ruhezustand zu schützen, sollten Sie sicherstellen, dass die Verschlüsselung für Ihre AWS CloudTrail Trails aktiviert ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.308(a)(1)(ii)(B)	(B) Risikoman agement (erforder lich). Implementieren Sie ausreichende Sicherheitsmaßnahm en, um Risiken und Schwachstellen auf ein angemessenes Maß zu reduzieren und die Vorgaben aus Abschnitt 164.306(a) zu erfüllen.	cloud-trail-log-file-Validierung aktiviert	Verwenden Sie die AWS CloudTrail Protokolldateivali dierung, um die Integrität von Protokoll en zu überprüfen. CloudTrail Mithilfe der Protokolldateivali dierung kann festgestellt werden, ob eine Protokoll datei geändert oder gelöscht wurde oder ob sie nach der Übermittlung CloudTrail unverände rt geblieben ist. Dieses Feature wurde mit dem Branchens tandard entsprech enden Algorithmen entwickelt: SHA-256 für die Hashfunkt ion und SHA-256 mit RSA für digitale Signaturen. Das macht es rechnerisch unmöglich, CloudTrai l Protokolldateien unbemerkt zu ändern, zu löschen oder zu fälschen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.308(a)(1)(ii)(B)	(B) Risikomanagement (erforderlich). Implementieren Sie ausreichende Sicherheitsmaßnahmen, um Risiken und Schwachstellen auf ein angemessenes Maß zu reduzieren und die Vorgaben aus Abschnitt 164.306(a) zu erfüllen.	codebuild-project-envvar-awscred-überprüfen	Stellen Sie sicher, dass die Anmeldeinformationen AWS_ACCESS_KEY_ID AWS_SECRET_ACCESS_KEY nicht in AWS Codebuild-Projektumgebungen vorhanden sind. Speichern Sie diese Variablen nicht als Klartext. Das Speichern dieser Variablen als Klartext bewirkt eine unbeabsichtigte Offenlegung von Daten sowie unberechtigte Zugriffe.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.308(a)(1)(ii)(B)	(B) Risikomanagement (erforderlich). Implementieren Sie ausreichende Sicherheitsmaßnahmen, um Risiken und Schwachstellen auf ein angemessenes Maß zu reduzieren und die Vorgaben aus Abschnitt 164.306(a) zu erfüllen.	codebuild-project-source-repo-URL-Prüfung	Stellen Sie sicher, dass die URL des Quell-Repositorys GitHub oder des Bitbucket-Quell-Repositorys keine persönlichen Zugriffstoken oder Anmeldeinformationen in Codebuild-Projektumgebungen enthält. AWS Verwende OAuth anstelle von persönlichen Zugriffstoken oder Anmeldedaten die Autorisierung für den Zugriff auf GitHub Bitbucket-Repositorys.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.308(a)(1)(ii)(B)	(B) Risikomanagement (erforderlich). Implementieren Sie ausreichende Sicherheitsmaßnahmen, um Risiken und Schwachstellen auf ein angemessenes Maß zu reduzieren und die Vorgaben aus Abschnitt 164.306(a) zu erfüllen.	db-instance-backup-enabled	Die Sicherungsfunktion von Amazon RDS erstellt Sicherungen Ihrer Datenbanken und Transaktionsprotokolle. Amazon RDS erstellt einen Snapshot für das Speichervolume Ihrer DB-Instance, sodass die gesamte DB-Instance gesichert wird. Sie können im System spezifische Aufbewahrungsfristen festlegen, um Ihre Ausfallsicherheitsanforderungen zu erfüllen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.308(a)(1)(ii)(B)	(B) Risikomanagement (erforderlich). Implementieren Sie ausreichende Sicherheitsmaßnahmen, um Risiken und Schwachstellen auf ein angemessenes Maß zu reduzieren und die Vorgaben aus Abschnitt 164.306(a) zu erfüllen.	dms-replication-not-public	Verwalte den Zugriff auf die AWS Cloud, indem du sicherstellst, dass auf DMS-Replikationsinstanzen nicht öffentlich zugegriffen werden kann. DMS-Replikations-Instances können vertrauliche Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.308(a)(1)(ii)(B)	(B) Risikomanagement (erforderlich). Implementieren Sie ausreichende Sicherheitsmaßnahmen, um Risiken und Schwachstellen auf ein angemessenes Maß zu reduzieren und die Vorgaben aus Abschnitt 164.306(a) zu erfüllen.	dynamodb-autoscaling-enabled	Amazon DynamoDB Auto Scaling verwendet den AWS Application Auto Scaling-Service, um die bereitgestellte Durchsatzkapazität so anzupassen, dass sie automatisch auf tatsächliche Verkehrsmuster reagiert. Auf diese Weise kann eine Tabelle oder ein globaler sekundärer Index die bereitgestellte Lese-/Schreibkapazität erhöhen, um plötzliche Erhöhungen des Datenverkehrs ohne Drosselung zu bewältigen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.308(a)(1)(ii)(B)	(B) Risikomanagement (erforderlich). Implementieren Sie ausreichende Sicherheitsmaßnahmen, um Risiken und Schwachstellen auf ein angemessenes Maß zu reduzieren und die Vorgaben aus Abschnitt 164.306(a) zu erfüllen.	dynamodb-pitr-enabled	Aktivieren Sie diese Regel, um zu überprüfen, ob die Informationen gesichert wurden. Es verwaltet auch die Backups, indem es sicherstellt, dass die point-in-time Wiederherstellung in Amazon DynamoDB aktiviert ist. Bei der Wiederherstellung werden fortlaufende Backups Ihrer Tabelle für die letzten 35 Tage gespeichert.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.308(a)(1)(ii)(B)	(B) Risikomanagement (erforderlich). Implementieren Sie ausreichende Sicherheitsmaßnahmen, um Risiken und Schwachstellen auf ein angemessenes Maß zu reduzieren und die Vorgaben aus Abschnitt 164.306(a) zu erfüllen.	dynamodb-throughput-limit-check	Aktivieren Sie diese Regel, um sicherzustellen, dass die bereitgestellte Durchsatzkapazität in Ihren Amazon-DynamoDB-Tabellen überprüft wird. Dies ist der Umfang der Lese- und Schreibaktivitäten, der von den jeweiligen Tabellen unterstützt werden kann. DynamoDB verwendet diese Informationen für das Reservieren ausreichender Systemressourcen, um Ihren Durchsatzanforderungen gerecht zu werden. Diese Regel generiert eine Warnung, wenn sich der Durchsatz dem Höchstlimit für ein Kundenkonto nähert. Mit dieser Regel können Sie optional die Parameter RCUThreshold Kontoprozentsatz

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			(Konfigurationsstandard: 80) und WCUThreshold Kontoprozentsatz (Konfigurationsstandard: 80) festlegen. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.
164.308(a)(1)(ii)(B)	(B) Risikomanagement (erforderlich). Implementieren Sie ausreichende Sicherheitsmaßnahmen, um Risiken und Schwachstellen auf ein angemessenes Maß zu reduzieren und die Vorgaben aus Abschnitt 164.306(a) zu erfüllen.	ebs-snapshot-public-restorable-überprüfen	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass EBS-Snapshots nicht öffentlich wiederherstellbar sind. EBS-Volume-Snapshots können vertrauliche Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.308(a)(1)(ii)(B)	(B) Risikomanagement (erforderlich). Implementieren Sie ausreichende Sicherheitsmaßnahmen, um Risiken und Schwachstellen auf ein angemessenes Maß zu reduzieren und die Vorgaben aus Abschnitt 164.306(a) zu erfüllen.	ec-2 ebs-encryption-by-default	Zum Schutz von Daten im Ruhezustand müssen Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon Elastic Block Store (Amazon EBS)-Volumes aktiviert ist. Da sensible Daten auch im Ruhezustand vorhanden sein können, sollten Sie die Verschlüsselung im Ruhezustand aktivieren, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.308(a)(1)(ii)(B)	(B) Risikoman agement (erforder lich). Implementieren Sie ausreichende Sicherheitsmaßnahm en, um Risiken und Schwachstellen auf ein angemessenes Maß zu reduzieren und die Vorgaben aus Abschnitt 164.306(a) zu erfüllen.	ec2- instance-no-public-ip	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon Elastic Compute Cloud (Amazon EC2) - Instances nicht öffentlich zugänglich sind. EC2 Amazon-Instances können vertrauliche Informati onen enthalten, und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.308(a)(1)(ii)(B)	(B) Risikoman agement (erforder lich). Implementieren Sie ausreichende Sicherheitsmaßnahm en, um Risiken und Schwachstellen auf ein angemessenes Maß zu reduzieren und die Vorgaben aus Abschnitt 164.306(a) zu erfüllen.	ec2- instances-in-vpc	Stellen Sie Amazon Elastic Compute Cloud (Amazon EC2) -Instances innerhalb einer Amazon Virtual Private Cloud (Amazon VPC) bereit, um eine sichere Kommunika tion zwischen einer Instance und anderen Services innerhalb der Amazon VPC zu ermöglichen, ohne dass ein Internet-Gateway, ein NAT-Gerät oder eine VPN-Verbindung erforderlich ist. Der gesamte Datenverk ehr bleibt sicher in der AWS Cloud. Domains, die sich innerhalb einer VPC befinden, verfügen aufgrund ihrer logischen Isolierun g im Vergleich zu Domains mit öffentlic hen Endpunkten über eine zusätzlic he Sicherheitsebene. Weisen Sie EC2

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			Amazon-Instances einer Amazon-VPC zu, um den Zugriff ordnungsgemäß zu verwalten.
164.308(a)(1)(ii)(B)	(B) Risikoman agement (erforder lich). Implementieren Sie ausreichende Sicherheitsmaßnahm en, um Risiken und Schwachstellen auf ein angemessenes Maß zu reduzieren und die Vorgaben aus Abschnitt 164.306(a) zu erfüllen.	ec2-stopped-instance	Aktivieren Sie diese Regel, um bei der Basiskonfiguration von Amazon Elastic Compute Cloud (Amazon EC2) - Instances zu helfen, indem Sie überprüfe n, ob EC2 Amazon-Instances gemäß den Standards Ihrer Organisation für mehr als die zulässige Anzahl von Tagen gestoppt wurden.
164.308(a)(1)(ii)(B)	(B) Risikoman agement (erforder lich). Implementieren Sie ausreichende Sicherheitsmaßnahm en, um Risiken und Schwachstellen auf ein angemessenes Maß zu reduzieren und die Vorgaben aus Abschnitt 164.306(a) zu erfüllen.	efs-encrypted-check	Aktivieren Sie die Verschlüsselung für Ihr Amazon Elastic File System (EFS), um eventuell vorhandene sensible Daten sowie Daten im Ruhezustand zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.308(a)(1)(ii)(B)	(B) Risikomanagement (erforderlich). Implementieren Sie ausreichende Sicherheitsmaßnahmen, um Risiken und Schwachstellen auf ein angemessenes Maß zu reduzieren und die Vorgaben aus Abschnitt 164.306(a) zu erfüllen.	elasticache-redis-cluster-automatic-Backup-Check	Wenn automatische Backups aktiviert sind, ElastiCache erstellt Amazon täglich ein Backup des Clusters. Die Sicherung kann für eine von Ihrer Organisation festgelegte Anzahl von Tagen aufbewahrt werden. Automatische Backups schützen vor Datenverlust. Bei einem Ausfall können Sie einen neuen Cluster erstellen, der Ihre Daten aus dem aktuellen Backup wiederherstellt.
164.308(a)(1)(ii)(B)	(B) Risikomanagement (erforderlich). Implementieren Sie ausreichende Sicherheitsmaßnahmen, um Risiken und Schwachstellen auf ein angemessenes Maß zu reduzieren und die Vorgaben aus Abschnitt 164.306(a) zu erfüllen.	elasticsearch-encrypted-at-rest	Da sensible Daten vorhanden sein können und um Daten im Ruhezustand zu schützen, sollten Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon OpenSearch Service (OpenSearch Service) -Domains aktiviert ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.308(a)(1)(ii)(B)	(B) Risikomanagement (erforderlich). Implementieren Sie ausreichende Sicherheitsmaßnahmen, um Risiken und Schwachstellen auf ein angemessenes Maß zu reduzieren und die Vorgaben aus Abschnitt 164.306(a) zu erfüllen.	elasticsearch-in-vpc-only	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass sich Amazon OpenSearch OpenSearch Service (Service) - Domains innerhalb einer Amazon Virtual Private Cloud (Amazon VPC) befinden. Eine OpenSearch Service-Domain innerhalb einer Amazon VPC ermöglicht die sichere Kommunikation zwischen OpenSearch Service und anderen Services innerhalb der Amazon VPC, ohne dass ein Internet-Gateway, ein NAT-Gerät oder eine VPN-Verbindung erforderlich ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.308(a)(1)(ii)(B)	(B) Risikomanagement (erforderlich). Implementieren Sie ausreichende Sicherheitsmaßnahmen, um Risiken und Schwachstellen auf ein angemessenes Maß zu reduzieren und die Vorgaben aus Abschnitt 164.306(a) zu erfüllen.	opensearch-encrypted-at-rest	Da sensible Daten vorhanden sein können und um Daten im Ruhezustand zu schützen, sollten Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon OpenSearch Service-Domains aktiviert ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.308(a)(1)(ii)(B)	(B) Risikomanagement (erforderlich). Implementieren Sie ausreichende Sicherheitsmaßnahmen, um Risiken und Schwachstellen auf ein angemessenes Maß zu reduzieren und die Vorgaben aus Abschnitt 164.306(a) zu erfüllen.	opensearch-in-vpc-only	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass sich Amazon OpenSearch Service-Domains innerhalb einer Amazon Virtual Private Cloud (Amazon VPC) befinden. Eine Amazon OpenSearch Service-Domain innerhalb einer Amazon VPC ermöglicht die sichere Kommunikation zwischen Amazon OpenSearch Service und anderen Services innerhalb der Amazon VPC, ohne dass ein Internet-Gateway, ein NAT-Gerät oder eine VPN-Verbindung erforderlich ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.308(a)(1)(ii)(B)	(B) Risikomanagement (erforderlich). Implementieren Sie ausreichende Sicherheitsmaßnahmen, um Risiken und Schwachstellen auf ein angemessenes Maß zu reduzieren und die Vorgaben aus Abschnitt 164.306(a) zu erfüllen.	elb-acm-certificate-required	Zum Schutz von eventuell vorhandenen sensiblen Daten sowie von Daten während der Übertragung muss die Verschlüsselung für Ihr Elastic Load Balancing aktiviert sein. Verwenden Sie AWS Certificate Manager, um öffentliche und private SSL/TLS-Zertifikate mit AWS Diensten und internen Ressourcen zu verwalten, bereitzustellen und bereitzustellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.308(a)(1)(ii)(B)	(B) Risikomanagement (erforderlich). Implementieren Sie ausreichende Sicherheitsmaßnahmen, um Risiken und Schwachstellen auf ein angemessenes Maß zu reduzieren und die Vorgaben aus Abschnitt 164.306(a) zu erfüllen.	elb-deletion-protection-enabled	Diese Regel sorgt dafür, dass der Löschschutz für Elastic Load Balancing aktiviert ist. Verwenden Sie diese Funktion, um zu verhindern, dass Ihr Load Balancer versehentlich oder böswillig gelöscht wird, was zum Verlust der Verfügbarkeit Ihrer Anwendungen führen kann.
164.308(a)(1)(ii)(B)	(B) Risikomanagement (erforderlich). Implementieren Sie ausreichende Sicherheitsmaßnahmen, um Risiken und Schwachstellen auf ein angemessenes Maß zu reduzieren und die Vorgaben aus Abschnitt 164.306(a) zu erfüllen.	emr-master-no-public-ip	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon EMR-Cluster-Masterknoten nicht öffentlich zugänglich sind. Amazon-EMR-Cluster-Hauptknoten können vertrauliche Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.308(a)(1)(ii)(B)	(B) Risikomanagement (erforderlich). Implementieren Sie ausreichende Sicherheitsmaßnahmen, um Risiken und Schwachstellen auf ein angemessenes Maß zu reduzieren und die Vorgaben aus Abschnitt 164.306(a) zu erfüllen.	encrypted-volumes	Aktivieren Sie die Verschlüsselung für Ihre Amazon-Elastic-Block-Store (Amazon-EBS)-Volumes, um eventuell vorhandene sensible Daten sowie Daten im Ruhezustand zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.308(a)(1)(ii)(B)	(B) Risikomanagement (erforderlich). Implementieren Sie ausreichende Sicherheitsmaßnahmen, um Risiken und Schwachstellen auf ein angemessenes Maß zu reduzieren und die Vorgaben aus Abschnitt 164.306(a) zu erfüllen.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) kann Ihnen dabei helfen, die Prinzipien der geringsten Rechte und der Aufgabentrennung in Zugriffsberechtigungen und Autorisierungen zu integrieren und so zu verhindern, dass Richtlinien „Effect“: „Allow“ mit „Action“: „*“ anstelle von „Resource“: „*“ enthalten. Wenn Benutzern mehr Rechte eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und der Aufgabentrennung verstoßen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.308(a)(1)(ii)(B)	(B) Risikoman agement (erforder lich). Implementieren Sie ausreichende Sicherheitsmaßnahm en, um Risiken und Schwachstellen auf ein angemessenes Maß zu reduzieren und die Vorgaben aus Abschnitt 164.306(a) zu erfüllen.	iam-root-access-key-überprüfen	Der Zugriff auf Systeme und Ressourcen kann gesteuert werden, indem überprüft wird, ob der Root-Benu tzer keine Zugriffss chlüssel mit seiner AWS Identity and Access Management (IAM) -Rolle verknüpft hat. Stellen Sie sicher, dass die Root-Zugr iffsschlüssel gelöscht werden. Erstellen und verwenden Sie stattdessen rollenbas ierte Funktionen, AWS-Konten um das Prinzip der geringste n Funktionalität zu berücksichtigen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.308(a)(1)(ii)(B)	(B) Risikoman agement (erforder lich). Implementieren Sie ausreichende Sicherheitsmaßnahm en, um Risiken und Schwachstellen auf ein angemessenes Maß zu reduzieren und die Vorgaben aus Abschnitt 164.306(a) zu erfüllen.	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) Security Groups können bei der Verwaltung des Netzwerkzugriffs helfen, indem sie eine statusbeh aftete Filterung von eingehendem und ausgehendem Netzwerkverkehr zu Ressourcen bereitste llen. AWS Wenn Sie eingehenden (oder entfernten) Datenverk ehr von 0.0.0.0/0 bis Port 22 auf Ihren Ressourcen nicht zulassen, können Sie den Remote-Zugriff einschränken.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.308(a)(1)(ii)(B)	(B) Risikomanagement (erforderlich). Implementieren Sie ausreichende Sicherheitsmaßnahmen, um Risiken und Schwachstellen auf ein angemessenes Maß zu reduzieren und die Vorgaben aus Abschnitt 164.306(a) zu erfüllen.	internet-gateway-authorized-vpc-nur	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Internet-Gateways nur mit autorisierter Amazon Virtual Private Cloud (Amazon VPC) verbunden sind. Internet-Gateways ermöglichen den bidirektionalen Internetzugang zur und von der Amazon VPC, was möglicherweise zu einem unbefugten Zugriff auf Amazon-VPC-Ressourcen führen kann.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.308(a)(1)(ii)(B)	(B) Risikomanagement (erforderlich). Implementieren Sie ausreichende Sicherheitsmaßnahmen, um Risiken und Schwachstellen auf ein angemessenes Maß zu reduzieren und die Vorgaben aus Abschnitt 164.306(a) zu erfüllen.	kms-cmk-not-scheduled-zum Löschen	Um Daten im Ruhezustand zu schützen, sollten Sie sicherstellen, dass die für den Kunden erforderlichen Masterschlüssel (CMKs) nicht im AWS Key Management Service (AWS KMS) gelöscht werden. Da Schlüssel manchmal gelöscht werden müssen, können Sie mit dieser Regel alle zu löschenden Schlüssel überprüfen, falls ein Schlüssel versehentlich zur Löschung vorgemerkt wurde.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.308(a)(1)(ii)(B)	(B) Risikomanagement (erforderlich). Implementieren Sie ausreichende Sicherheitsmaßnahmen, um Risiken und Schwachstellen auf ein angemessenes Maß zu reduzieren und die Vorgaben aus Abschnitt 164.306(a) zu erfüllen.	lambda-function-public-access-verboten	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass AWS Lambda-Funktionen nicht öffentlich zugänglich sind. Der öffentliche Zugriff kann möglicherweise die Verfügbarkeit von Ressourcen beeinträchtigen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.308(a)(1)(ii)(B)	(B) Risikomanagement (erforderlich). Implementieren Sie ausreichende Sicherheitsmaßnahmen, um Risiken und Schwachstellen auf ein angemessenes Maß zu reduzieren und die Vorgaben aus Abschnitt 164.306(a) zu erfüllen.	rds-multi-az-support	Die Multi-AZ-Unterstützung in Amazon Relational Database Service (Amazon RDS) bietet eine verbesserte Verfügbarkeit und Beständigkeit von Datenbank-Instances. Wenn Sie eine Multi-AZ-Datenbank-Instance bereitstellen, erstellt Amazon RDS automatisch eine primäre Datenbank-Instance und repliziert die Daten synchron auf eine Standby-Instance in einer anderen Availability Zone. Jede Availability Zone läuft auf einer eigenen, physisch getrennten, unabhängigen Infrastruktur und ist auf eine hohe Verfügbarkeit ausgelegt. Im Falle eines Infrastrukturausfalls führt Amazon RDS einen automatis

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			chen Failover zum Standby-Modus durch, sodass Sie den Datenbankbetrieb wieder aufnehmen können, sobald der Failover abgeschlo ssen ist.
164.308(a)(1)(ii)(B)	(B) Risikoman agement (erforder lich). Implementieren Sie ausreichende Sicherheitsmaßnahm en, um Risiken und Schwachstellen auf ein angemessenes Maß zu reduzieren und die Vorgaben aus Abschnitt 164.306(a) zu erfüllen.	rds-snapshot-encry pted	Stellen Sie sicher, dass die Verschlüs selung für Ihre Amazon Relationa l Database Service (Amazon RDS)-Snap shots aktiviert ist. Da sensible Daten auch im Ruhezusta nd vorhanden sein können, sollten Sie die Verschlüsselung im Ruhezustand aktivieren, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.308(a)(1)(ii)(B)	(B) Risikomanagement (erforderlich). Implementieren Sie ausreichende Sicherheitsmaßnahmen, um Risiken und Schwachstellen auf ein angemessenes Maß zu reduzieren und die Vorgaben aus Abschnitt 164.306(a) zu erfüllen.	rds-snapshots-public-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Relational Database Service (Amazon RDS) -Instances nicht öffentlich sind. Amazon-RDS-Datenbank-Instances können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.308(a)(1)(ii)(B)	(B) Risikomanagement (erforderlich). Implementieren Sie ausreichende Sicherheitsmaßnahmen, um Risiken und Schwachstellen auf ein angemessenes Maß zu reduzieren und die Vorgaben aus Abschnitt 164.306(a) zu erfüllen.	rds-storage-encrypted	Zum Schutz von Daten im Ruhezustand müssen Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon Relational Database Service (Amazon RDS)-Instances aktiviert ist. Um eventuell vorhandene sensible Daten im Ruhezustand in Amazon-RDS-Instances zu schützen, muss die Verschlüsselung von Daten im Ruhezustand aktiviert sein.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.308(a)(1)(ii)(B)	(B) Risikomanagement (erforderlich). Implementieren Sie ausreichende Sicherheitsmaßnahmen, um Risiken und Schwachstellen auf ein angemessenes Maß zu reduzieren und die Vorgaben aus Abschnitt 164.306(a) zu erfüllen.	redshift-cluster-configuration-check	Um Daten im Ruhezustand zu schützen, muss die Verschlüsselung für Ihre Amazon-Redshift-Cluster aktiviert sein. Sie müssen auch sicherstellen, dass die erforderlichen Konfigurationen auf Amazon-Redshift-Clustern bereitgestellt werden. Die Prüfungsprotokollierung muss aktiviert sein, um Informationen zu Verbindungen und Benutzeraktivitäten in der Datenbank bereitzustellen. Diese Regel erfordert, dass ein Wert für clusterDbEncrypted (Config Default: TRUE) und LoggingEnabled (Config Default: TRUE) gesetzt ist. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.308(a)(1)(ii)(B)	(B) Risikomanagement (erforderlich). Implementieren Sie ausreichende Sicherheitsmaßnahmen, um Risiken und Schwachstellen auf ein angemessenes Maß zu reduzieren und die Vorgaben aus Abschnitt 164.306(a) zu erfüllen.	redshift-cluster-public-access-überprüfen	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Redshift Redshift-Cluster nicht öffentlich sind. Amazon-Redshift-Cluster können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.
164.308(a)(1)(ii)(B)	(B) Risikomanagement (erforderlich). Implementieren Sie ausreichende Sicherheitsmaßnahmen, um Risiken und Schwachstellen auf ein angemessenes Maß zu reduzieren und die Vorgaben aus Abschnitt 164.306(a) zu erfüllen.	redshift-require-tls-ssl	Stellen Sie sicher, dass Ihre Amazon-Redshift-Cluster eine TLS/SSL-Verschlüsselung erfordern, um eine Verbindung zu SQL-Clients herzustellen. Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.308(a)(1)(ii)(B)	(B) Risikomanagement (erforderlich). Implementieren Sie ausreichende Sicherheitsmaßnahmen, um Risiken und Schwachstellen auf ein angemessenes Maß zu reduzieren und die Vorgaben aus Abschnitt 164.306(a) zu erfüllen.	restricted-common-ports	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass gemeinsame Ports für Amazon Elastic Compute Cloud (Amazon EC2) -Sicherheitsgruppen eingeschränkt sind. Wenn der Zugriff auf Ports nicht auf vertrauenswürdige Quellen beschränkt wird, kann dies zu Angriffen auf die Verfügbarkeit, Integrität und Vertraulichkeit von Systemen führen. Mit dieser Regel können Sie optional die Parameter blockedPort1–blockedPort5 festlegen (Standardkonfigurationen: 20, 21, 3389, 3306, 4333). Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.308(a)(1)(ii)(B)	(B) Risikomanagement (erforderlich). Implementieren Sie ausreichende Sicherheitsmaßnahmen, um Risiken und Schwachstellen auf ein angemessenes Maß zu reduzieren und die Vorgaben aus Abschnitt 164.306(a) zu erfüllen.	s-3 bucket-default-lock-enabled	Stellen Sie sicher, dass für Ihren Amazon Simple Storage Service (Amazon S3)-Bucket standardmäßig eine Sperre aktiviert ist. Zum Schutz eventuell vorhandener sensibler Daten in S3-Buckets müssen Sie Objektsperren für Daten im Ruhezustand erzwingen.
164.308(a)(1)(ii)(B)	(B) Risikomanagement (erforderlich). Implementieren Sie ausreichende Sicherheitsmaßnahmen, um Risiken und Schwachstellen auf ein angemessenes Maß zu reduzieren und die Vorgaben aus Abschnitt 164.306(a) zu erfüllen.	s-3 bucket-public-read-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie nur autorisierten Benutzern, Prozessen und Geräten Zugriff auf Amazon Simple Storage Service (Amazon S3) - Buckets gewähren. Die Verwaltung des Zugriffs sollte mit der Klassifizierung der Daten übereinstimmen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.308(a)(1)(ii)(B)	(B) Risikomanagement (erforderlich). Implementieren Sie ausreichende Sicherheitsmaßnahmen, um Risiken und Schwachstellen auf ein angemessenes Maß zu reduzieren und die Vorgaben aus Abschnitt 164.306(a) zu erfüllen.	s3- bucket-public-write-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie nur autorisierten Benutzern, Prozessen und Geräten Zugriff auf Amazon Simple Storage Service (Amazon S3) - Buckets gewähren. Die Verwaltung des Zugriffs sollte mit der Klassifizierung der Daten übereinstimmen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.308(a)(1)(ii)(B)	(B) Risikomanagement (erforderlich). Implementieren Sie ausreichende Sicherheitsmaßnahmen, um Risiken und Schwachstellen auf ein angemessenes Maß zu reduzieren und die Vorgaben aus Abschnitt 164.306(a) zu erfüllen.	s3- bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) unterstützt die Aufrechterhaltung einer angemessenen Kapazität und Verfügbarkeit. CRR ermöglicht das automatische, asynchrone Kopieren von Objekten in Amazon-S3-Buckets, um die Datenverfügbarkeit sicherzustellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.308(a)(1)(ii)(B)	(B) Risikomanagement (erforderlich). Implementieren Sie ausreichende Sicherheitsmaßnahmen, um Risiken und Schwachstellen auf ein angemessenes Maß zu reduzieren und die Vorgaben aus Abschnitt 164.306(a) zu erfüllen.	s3- bucket-server-side-encryption -aktiviert	Zum Schutz von Daten im Ruhezustand müssen Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon Simple Storage Service (Amazon S3)-Buckets aktiviert ist. Um eventuell vorhandene sensible Daten im Ruhezustand in Amazon-S3-Buckets zu schützen, muss die Verschlüsselung aktiviert sein.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.308(a)(1)(ii)(B)	(B) Risikomanagement (erforderlich). Implementieren Sie ausreichende Sicherheitsmaßnahmen, um Risiken und Schwachstellen auf ein angemessenes Maß zu reduzieren und die Vorgaben aus Abschnitt 164.306(a) zu erfüllen.	s-3 bucket-ssl-requests-only	Um Daten während der Übertragung zu schützen, stellen Sie sicher, dass Ihre Amazon Simple Storage Service (Amazon S3)-Buckets Anfragen zur Verwendung von Secure Socket Layer (SSL)-Buckets erfordern. Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.308(a)(1)(ii)(B)	(B) Risikomanagement (erforderlich). Implementieren Sie ausreichende Sicherheitsmaßnahmen, um Risiken und Schwachstellen auf ein angemessenes Maß zu reduzieren und die Vorgaben aus Abschnitt 164.306(a) zu erfüllen.	s-3 bucket-versioning-enabled	Die Versionsverwaltung von Amazon Simple Storage Service (Amazon S3)-Buckets hilft dabei, mehrere Varianten eines Objekts im selben Amazon-S3-Bucket zu speichern. Verwenden Sie die Versionsverwaltung, um sämtliche Versionen aller Objekte in Ihrem Amazon-S3-Bucket zu speichern, abzurufen oder wiederherzustellen. Mit der Versionsverwaltung können Sie Versionen sowohl nach unbeabsichtigten Benutzeraktionen als auch nach Anwendungsfehlern problemlos wiederherstellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.308(a)(1)(ii)(B)	(B) Risikomanagement (erforderlich). Implementieren Sie ausreichende Sicherheitsmaßnahmen, um Risiken und Schwachstellen auf ein angemessenes Maß zu reduzieren und die Vorgaben aus Abschnitt 164.306(a) zu erfüllen.	sagemaker-endpoint-configuration-kms-key-konfiguriert	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass die Verschlüsselung mit dem AWS Key Management Service (AWS KMS) für Ihren Endpunkt aktiviert ist. SageMaker Da sensible Daten auf dem SageMaker Endgerät gespeichert werden können, sollten Sie die Verschlüsselung im Ruhezustand aktivieren, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.308(a)(1)(ii)(B)	(B) Risikomanagement (erforderlich). Implementieren Sie ausreichende Sicherheitsmaßnahmen, um Risiken und Schwachstellen auf ein angemessenes Maß zu reduzieren und die Vorgaben aus Abschnitt 164.306(a) zu erfüllen.	sagemaker-notebook-instance-kms-schlüsselkonfiguriert	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass die Verschlüsselung mit dem AWS Key Management Service (AWS KMS) für Ihr Notebook aktiviert ist. SageMaker Da vertrauliche Daten im SageMaker Notebook gespeichert werden können, sollten Sie die Verschlüsselung im Ruhezustand aktivieren, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.308(a)(1)(ii)(B)	(B) Risikomanagement (erforderlich). Implementieren Sie ausreichende Sicherheitsmaßnahmen, um Risiken und Schwachstellen auf ein angemessenes Maß zu reduzieren und die Vorgaben aus Abschnitt 164.306(a) zu erfüllen.	sagemaker-notebook-no-direct-Internetzugang	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass SageMaker Amazon-Notebooks keinen direkten Internetzugang zulassen. Indem Sie direkten Internetzugang blockieren, vermeiden Sie, dass unbefugte Benutzer auf sensible Daten zugreifen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.308(a)(1)(ii)(B)	(B) Risikomanagement (erforderlich). Implementieren Sie ausreichende Sicherheitsmaßnahmen, um Risiken und Schwachstellen auf ein angemessenes Maß zu reduzieren und die Vorgaben aus Abschnitt 164.306(a) zu erfüllen.	sns-encrypted-kms	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass Ihre Amazon Simple Notification Service (Amazon SNS) -Themen mit dem AWS Key Management Service (AWS KMS) verschlüsselt werden müssen. Um eventuell vorhandene sensible Daten im Ruhezustand in veröffentlichten Nachrichten zu schützen, muss die Verschlüsselung von Daten im Ruhezustand aktiviert sein.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.308(a)(1)(ii)(B)	(B) Risikomanagement (erforderlich). Implementieren Sie ausreichende Sicherheitsmaßnahmen, um Risiken und Schwachstellen auf ein angemessenes Maß zu reduzieren und die Vorgaben aus Abschnitt 164.306(a) zu erfüllen.	vpc-sg-open-only-to-authorized-ports	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass gemeinsame Ports für Amazon Elastic Compute Cloud (Amazon EC2) -Sicherheitsgruppen eingeschränkt sind. Wenn der Zugriff auf Ports nicht auf vertrauenswürdige Quellen beschränkt wird, kann dies zu Angriffen auf die Verfügbarkeit, Integrität und Vertraulichkeit von Systemen führen. Durch die Beschränkung des Zugriffs auf Ressourcen innerhalb einer Sicherheitsgruppe aus dem Internet (0.0.0.0/0) kann der Remote-Zugriff auf interne Systeme gesteuert werden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.308(a)(1)(ii)(B)	(B) Risikomanagement (erforderlich). Implementieren Sie ausreichende Sicherheitsmaßnahmen, um Risiken und Schwachstellen auf ein angemessenes Maß zu reduzieren und die Vorgaben aus Abschnitt 164.306(a) zu erfüllen.	vpc-vpn-2-tunnels-up	Redundante Site-to-Site VPN-Tunnel können implementiert werden, um die Anforderungen an die Ausfallsicherheit zu erfüllen. Es verwendet zwei Tunnel, um die Konnektivität sicherzustellen, falls eine der Site-to-Site VPN-Verbindungen nicht verfügbar ist. Um sich vor einem Verbindungsverlust zu schützen, können Sie für den Fall, dass Ihr Kunden-Gateway nicht verfügbar ist, eine zweite Site-to-Site VPN-Verbindung zu Ihrer Amazon Virtual Private Cloud (Amazon VPC) und Ihrem Virtual Private Gateway einrichten, indem Sie ein zweites Kunden-Gateway verwenden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.308(a)(1)(ii)(B)	(B) Risikomanagement (erforderlich). Implementieren Sie ausreichende Sicherheitsmaßnahmen, um Risiken und Schwachstellen auf ein angemessenes Maß zu reduzieren und die Vorgaben aus Abschnitt 164.306(a) zu erfüllen.	ec2-managed-instance-managed-by-systems	Eine Bestandsaufnahme der Softwareplattformen und Anwendungen innerhalb des Unternehmens ist möglich, indem Amazon Elastic Compute Cloud (Amazon EC2) - Instances mit AWS Systems Manager verwaltet werden. Verwenden Sie AWS Systems Manager, um detaillierte Systemkonfigurationen, Betriebssystem-Patch-Levels, Namen und Typ der Dienste, Softwareinstallationen, Anwendungsname, Herausgeber und Version sowie andere Details zu Ihrer Umgebung bereitzustellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.308(a)(1)(ii)(B)	(B) Risikomanagement (erforderlich). Implementieren Sie ausreichende Sicherheitsmaßnahmen, um Risiken und Schwachstellen auf ein angemessenes Maß zu reduzieren und die Vorgaben aus Abschnitt 164.306(a) zu erfüllen.	ec2-check managedinstance-patch-compliance-status	Aktivieren Sie diese Regel, um bei der Identifizierung und Dokumentation von Sicherheitslücken in Amazon Elastic Compute Cloud (Amazon EC2) zu helfen. Die Regel prüft, ob die EC2 Amazon-Instance die Patch-Konformität im AWS Systems Manager gemäß den Richtlinien und Verfahren Ihrer Organisation einhält.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.308(a)(1)(ii)(B)	(B) Risikomanagement (erforderlich). Implementieren Sie ausreichende Sicherheitsmaßnahmen, um Risiken und Schwachstellen auf ein angemessenes Maß zu reduzieren und die Vorgaben aus Abschnitt 164.306(a) zu erfüllen.	ec2-check managedinstance-association-compliance-status	Verwenden Sie AWS Systems Manager Associations, um bei der Inventarisierung von Softwareplattformen und Anwendungen innerhalb eines Unternehmens zu helfen. AWS Systems Manager weist Ihren verwalteten Instanzen einen Konfigurationsstatus zu und ermöglicht es Ihnen, Basiswerte für Betriebssystem-Patch-Levels, Softwareinstallationen, Anwendungskonfigurationen und andere Details zu Ihrer Umgebung festzulegen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.308(a)(3)(i)	(3)(i) Standard: Sicherheit der Belegschaft. Implementieren Sie Richtlinien und Verfahren, um sicherzustellen, dass alle Mitarbeiter angemessen Zugriff auf elektronisch geschützte Gesundheitsinformationen haben, wie in Absatz (a)(4) dieses Abschnitts vorgesehen, und um zu verhindern, dass Mitarbeiter ohne Zugriff gemäß Absatz (a) (4) dieses Abschnitts Zugriff auf elektronisch geschützte Gesundheitsinformationen erhalten.	ec2-imdsv2-check	Stellen Sie sicher, dass die Methode Instance Metadata Service Version 2 (IMDSv2) aktiviert ist, um den Zugriff auf und die Kontrolle der Amazon Elastic Compute Cloud (Amazon EC2) - Instance-Metadaten zu schützen. Die IMDSv2 Methode verwendet sitzungsbasierte Kontrollen. Mit können Kontrollen implementiert werden IMDSv2, um Änderungen an Instanzmetadaten einzuschränken.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.308(a)(3)(i)	(3)(i) Standard: Sicherheit der Belegschaft. Implementieren Sie Richtlinien und Verfahren, um sicherzustellen, dass alle Mitarbeiter angemessen Zugriff auf elektronisch geschützte Gesundheitsinformationen haben, wie in Absatz (a)(4) dieses Abschnitts vorgesehen, und um zu verhindern, dass Mitarbeiter ohne Zugriff gemäß Absatz (a) (4) dieses Abschnitts Zugriff auf elektronisch geschützte Gesundheitsinformationen erhalten.	emr-kerberos-enabled	Die Zugriffsberechtigungen und -autorisierungen können verwaltet und nach den Prinzipien der geringsten Berechtigung und Aufgabentrennung integriert werden, indem Kerberos für Amazon-EMR-Cluster aktiviert wird. In Kerberos werden Services und Benutzer, die sich authentifizieren müssen, als Prinzipale bezeichnet. Prinzipale befinden sich in einem Kerberos-Bereich. Innerhalb dieses Bereichs wird ein Kerberos-Server als Key Distribution Center (KDC) bezeichnet. Über diesen Server können sich Prinzipale authentifizieren. Die Authentifizierung im KDC erfolgt durch die Ausstellung von Authentif

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			izierungstickets. Das KDC unterhält eine Datenbank der Prinzipale in seinem Bereich mit ihren Passwörtern und anderen administr ativen Informationen zu jedem Prinzipal.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.308(a)(3)(i)	(3)(i) Standard: Sicherheit der Belegschaft. Implementieren Sie Richtlinien und Verfahren, um sicherzustellen, dass alle Mitarbeiter angemessen Zugriff auf elektronisch geschützte Gesundheitsinformationen haben, wie in Absatz (a)(4) dieses Abschnitts vorgesehen, und um zu verhindern, dass Mitarbeiter ohne Zugriff gemäß Absatz (a) (4) dieses Abschnitts Zugriff auf elektronisch geschützte Gesundheitsinformationen erhalten.	iam-customer-policy-blocked-kms-Aktionen	AWS Identity and Access Management (IAM) kann Ihnen helfen, die Prinzipien der geringsten Rechte und der Aufgabentrennung in Zugriffsberechtigungen und Autorisierungen zu integrieren und so zu verhindern, dass Richtlinien blockierte Aktionen für alle AWS Schlüssel des Key Management Service enthalten. Wenn Benutzer mehr Rechte haben, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und Aufgabentrennung verstoßen. Mit dieser Regel können Sie den Parameter festlegen. blockedActionsPatterns (Wert „AWS Bewährte grundlegende Sicherheitsmethoden“: kms:

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			Decrypt, kms:ReEncryptFrom). Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.308(a)(3)(i)	(3)(i) Standard: Sicherheit der Belegschaft. Implementieren Sie Richtlinien und Verfahren, um sicherzustellen, dass alle Mitarbeiter angemessen Zugriff auf elektronisch geschützte Gesundheitsinformationen haben, wie in Absatz (a)(4) dieses Abschnitts vorgesehen, und um zu verhindern, dass Mitarbeiter ohne Zugriff gemäß Absatz (a) (4) dieses Abschnitts Zugriff auf elektronisch geschützte Gesundheitsinformationen erhalten.	iam-inline-policy-blocked-kms-Aktionen	Stellen Sie sicher, dass ein Benutzer, eine IAM-Rolle oder eine IAM-Gruppe (AWS Identity and Access Management) nicht über eine Inline-Richtlinie verfügt, die blockierte Aktionen für alle AWS Schlüssel des Key Management Service zulässt. AWS empfiehlt, verwaltete Richtlinien anstelle von Inline-Richtlinien zu verwenden. Verwaltete Richtlinien ermöglichen Wiederverwendbarkeit, Versionsverwaltung, Rollback und Delegierung der Berechtigungsverwaltung. Mit dieser Regel können Sie den blockedActionsPatterns Parameter festlegen. (Wert „AWS Bewährte grundlegende Sicherheitsmethoden“: kms:Decrypt, kms:ReEncryptFrom). Die

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.
164.308(a)(3)(i)	(3)(i) Standard: Sicherheit der Belegschaft. Implementieren Sie Richtlinien und Verfahren, um sicherzustellen, dass alle Mitarbeiter angemessen Zugriff auf elektronisch geschützte Gesundheitsinformationen haben, wie in Absatz (a)(4) dieses Abschnitts vorgesehen, und um zu verhindern, dass Mitarbeiter ohne Zugriff gemäß Absatz (a) (4) dieses Abschnitts Zugriff auf elektronisch geschützte Gesundheitsinformationen erhalten.	iam-no-inline-policy-überprüfen	Stellen Sie sicher, dass ein Benutzer, eine IAM-Rolle oder eine IAM-Gruppe (AWS Identity and Access Management) nicht über eine Inline-Richtlinie zur Zugriffskontrolle auf Systeme und Ressourcen verfügt. AWS empfiehlt, verwaltete Richtlinien anstelle von Inline-Richtlinien zu verwenden. Verwaltete Richtlinien ermöglichen Wiederverwendbarkeit, Versionsverwaltung, Rollback und Delegierung der Berechtigungsverwaltung.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.308(a)(3)(i)	(3)(i) Standard: Sicherheit der Belegschaft. Implementieren Sie Richtlinien und Verfahren, um sicherzustellen, dass alle Mitarbeiter angemessen Zugriff auf elektronisch geschützte Gesundheitsinformationen haben, wie in Absatz (a)(4) dieses Abschnitts vorgesehen, und um zu verhindern, dass Mitarbeiter ohne Zugriff gemäß Absatz (a) (4) dieses Abschnitts Zugriff auf elektronisch geschützte Gesundheitsinformationen erhalten.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) kann Ihnen dabei helfen, die Prinzipien der geringsten Rechte und der Aufgabentrennung in Zugriffsberechtigungen und Autorisierungen zu integrieren und so zu verhindern, dass Richtlinien „Effect“: „Allow“ mit „Action“: „*“ anstelle von „Resource“: „*“ enthalten. Wenn Benutzern mehr Rechte eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und der Aufgabentrennung verstoßen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.308(a)(3)(i)	(3)(i) Standard: Sicherheit der Belegschaft. Implementieren Sie Richtlinien und Verfahren, um sicherzustellen, dass alle Mitarbeiter angemessen Zugriff auf elektronisch geschützte Gesundheitsinformationen haben, wie in Absatz (a)(4) dieses Abschnitts vorgesehen, und um zu verhindern, dass Mitarbeiter ohne Zugriff gemäß Absatz (a) (4) dieses Abschnitts Zugriff auf elektronisch geschützte Gesundheitsinformationen erhalten.	iam-root-access-key-überprüfen	Der Zugriff auf Systeme und Ressourcen kann gesteuert werden, indem überprüft wird, ob der Root-Benutzer keine Zugriffsschlüssel mit seiner AWS Identity and Access Management (IAM) -Rolle verknüpft hat. Stellen Sie sicher, dass die Root-Zugriffsschlüssel gelöscht werden. Erstellen und verwenden Sie stattdessen rollenbasierte Funktionen, AWS-Konten um das Prinzip der geringsten Funktionalität zu berücksichtigen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.308(a)(3)(i)	(3)(i) Standard: Sicherheit der Belegschaft. Implementieren Sie Richtlinien und Verfahren, um sicherzustellen, dass alle Mitarbeiter angemessen Zugriff auf elektronisch geschützte Gesundheitsinformationen haben, wie in Absatz (a)(4) dieses Abschnitts vorgesehen, und um zu verhindern, dass Mitarbeiter ohne Zugriff gemäß Absatz (a) (4) dieses Abschnitts Zugriff auf elektronisch geschützte Gesundheitsinformationen erhalten.	iam-user-no-policies-überprüfen	Diese Regel stellt sicher, dass AWS Identity and Access Management (IAM) -Richtlinien nur Gruppen oder Rollen zugewiesen werden, um den Zugriff auf Systeme und Ressourcen zu kontrollieren. Die Zuweisung von Berechtigungen auf Gruppen- oder Rollenebene trägt dazu bei, die Wahrscheinlichkeit zu verringern, dass eine Identität übermäßige Berechtigungen erhält oder beibehält.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.308(a)(3)(i)	(3)(i) Standard: Sicherheit der Belegschaft. Implementieren Sie Richtlinien und Verfahren, um sicherzustellen, dass alle Mitarbeiter angemessen Zugriff auf elektronisch geschützte Gesundheitsinformationen haben, wie in Absatz (a)(4) dieses Abschnitts vorgesehen, und um zu verhindern, dass Mitarbeiter ohne Zugriff gemäß Absatz (a) (4) dieses Abschnitts Zugriff auf elektronisch geschützte Gesundheitsinformationen erhalten.	iam-user-unused-credentials-überprüfen	AWS Identity and Access Management (IAM) kann Ihnen bei Zugriffsberechtigungen und Autorisierungen helfen, indem es nach IAM-Passwörtern und Zugriffsschlüsseln sucht, die für einen bestimmten Zeitraum nicht verwendet wurden. Wenn ungenutzte Anmeldeinformationen identifiziert werden, müssen Sie sie deaktivieren und/oder entfernen, da dies gegen das Prinzip der geringsten Berechtigung verstoßen könnte. Für diese Regel müssen Sie einen Wert für das maxCredentialUsage Alter festlegen (Standardkonfiguration: 90). Der tatsächliche Wert muss den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.308(a)(3)(i)	(3)(i) Standard: Sicherheit der Belegschaft. Implementieren Sie Richtlinien und Verfahren, um sicherzustellen, dass alle Mitarbeiter angemessen Zugriff auf elektronisch geschützte Gesundheitsinformationen haben, wie in Absatz (a)(4) dieses Abschnitts vorgesehen, und um zu verhindern, dass Mitarbeiter ohne Zugriff gemäß Absatz (a) (4) dieses Abschnitts Zugriff auf elektronisch geschützte Gesundheitsinformationen erhalten.	iam-policy-no-statements-with-full-access	Stellen Sie sicher, dass IAM-Aktionen nur auf die benötigten Aktionen beschränkt sind. Wenn Benutzern mehr Rechte eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und der Aufgabentrennung verstoßen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.308(a)(3)(i)	(3)(i) Standard: Sicherheit der Belegschaft. Implementieren Sie Richtlinien und Verfahren, um sicherzustellen, dass alle Mitarbeiter angemessen Zugriff auf elektronisch geschützte Gesundheitsinformationen haben, wie in Absatz (a)(4) dieses Abschnitts vorgesehen, und um zu verhindern, dass Mitarbeiter ohne Zugriff gemäß Absatz (a) (4) dieses Abschnitts Zugriff auf elektronisch geschützte Gesundheitsinformationen erhalten.	ec2- instance-profile-attached	EC2 Instanzprofile übergeben eine IAM-Rolle an eine Instanz EC2 . Das Anhängen eines Instance-Profils an Ihre Instances kann bei der Implementierung von geringsten Berechtigungen und der Berechtigungsverwaltung helfen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.308(a)(3)(i)	(3)(i) Standard: Sicherheit der Belegschaft. Implementieren Sie Richtlinien und Verfahren, um sicherzustellen, dass alle Mitarbeiter angemessen Zugriff auf elektronisch geschützte Gesundheitsinformationen haben, wie in Absatz (a)(4) dieses Abschnitts vorgesehen, und um zu verhindern, dass Mitarbeiter ohne Zugriff gemäß Absatz (a) (4) dieses Abschnitts Zugriff auf elektronisch geschützte Gesundheitsinformationen erhalten.	dms-replication-not-public	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass auf DMS-Replikationsinstanzen nicht öffentlich zugegriffen werden kann. DMS-Replikations-Instances können vertrauliche Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.308(a)(3)(i)	(3)(i) Standard: Sicherheit der Belegschaft. Implementieren Sie Richtlinien und Verfahren, um sicherzustellen, dass alle Mitarbeiter angemessen Zugriff auf elektronisch geschützte Gesundheitsinformationen haben, wie in Absatz (a)(4) dieses Abschnitts vorgesehen, und um zu verhindern, dass Mitarbeiter ohne Zugriff gemäß Absatz (a) (4) dieses Abschnitts Zugriff auf elektronisch geschützte Gesundheitsinformationen erhalten.	ebs-snapshot-public-restorable-überprüfen	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass EBS-Snapshots nicht öffentlich wiederherstellbar sind. EBS-Volume-Snapshots können vertrauliche Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.308(a)(3)(i)	(3)(i) Standard: Sicherheit der Belegschaft. Implementieren Sie Richtlinien und Verfahren, um sicherzustellen, dass alle Mitarbeiter angemessen Zugriff auf elektronisch geschützte Gesundheitsinformationen haben, wie in Absatz (a)(4) dieses Abschnitts vorgesehen, und um zu verhindern, dass Mitarbeiter ohne Zugriff gemäß Absatz (a) (4) dieses Abschnitts Zugriff auf elektronisch geschützte Gesundheitsinformationen erhalten.	ec-2 instance-no-public-ip	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon Elastic Compute Cloud (Amazon EC2) - Instances nicht öffentlich zugänglich sind. EC2 Amazon-Instances können vertrauliche Informationen enthalten, und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.308(a)(3)(i)	(3)(i) Standard: Sicherheit der Belegschaft. Implementieren Sie Richtlinien und Verfahren, um sicherzustellen, dass alle Mitarbeiter angemessen Zugriff auf elektronisch geschützte Gesundheitsinformationen haben, wie in Absatz (a)(4) dieses Abschnitts vorgesehen, und um zu verhindern, dass Mitarbeiter ohne Zugriff gemäß Absatz (a) (4) dieses Abschnitts Zugriff auf elektronisch geschützte Gesundheitsinformationen erhalten.	elasticsearch-in-vpc-only	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass sich Amazon OpenSearch OpenSearch Service (Service) - Domains innerhalb einer Amazon Virtual Private Cloud (Amazon VPC) befinden. Eine OpenSearch Service-Domain innerhalb einer Amazon VPC ermöglicht die sichere Kommunikation zwischen OpenSearch Service und anderen Services innerhalb der Amazon VPC, ohne dass ein Internet-Gateway, ein NAT-Gerät oder eine VPN-Verbindung erforderlich ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.308(a)(3)(i)	(3)(i) Standard: Sicherheit der Belegschaft. Implementieren Sie Richtlinien und Verfahren, um sicherzustellen, dass alle Mitarbeiter angemessen Zugriff auf elektronisch geschützte Gesundheitsinformationen haben, wie in Absatz (a)(4) dieses Abschnitts vorgesehen, und um zu verhindern, dass Mitarbeiter ohne Zugriff gemäß Absatz (a) (4) dieses Abschnitts Zugriff auf elektronisch geschützte Gesundheitsinformationen erhalten.	emr-master-no-public-ip	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon EMR-Cluster-Masterknoten nicht öffentlich zugänglich sind. Amazon-EMR-Cluster-Hauptknoten können vertrauliche Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.308(a)(3)(i)	(3)(i) Standard: Sicherheit der Belegschaft. Implementieren Sie Richtlinien und Verfahren, um sicherzustellen, dass alle Mitarbeiter angemessen Zugriff auf elektronisch geschützte Gesundheitsinformationen haben, wie in Absatz (a)(4) dieses Abschnitts vorgesehen, und um zu verhindern, dass Mitarbeiter ohne Zugriff gemäß Absatz (a) (4) dieses Abschnitts Zugriff auf elektronisch geschützte Gesundheitsinformationen erhalten.	ec-2 instances-in-vpc	Stellen Sie Amazon Elastic Compute Cloud (Amazon EC2) -Instances innerhalb einer Amazon Virtual Private Cloud (Amazon VPC) bereit, um eine sichere Kommunikation zwischen einer Instance und anderen Services innerhalb der Amazon VPC zu ermöglichen, ohne dass ein Internet-Gateway, ein NAT-Gerät oder eine VPN-Verbindung erforderlich ist. Der gesamte Datenverkehr bleibt sicher in der AWS Cloud. Domains, die sich innerhalb einer VPC befinden, verfügen aufgrund ihrer logischen Isolierung im Vergleich zu Domains mit öffentlichen Endpunkten über eine zusätzliche Sicherheitsebene. Weisen Sie EC2

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			Amazon-Instances einer Amazon-VPC zu, um den Zugriff ordnungsgemäß zu verwalten.
164.308(a)(3)(i)	(3)(i) Standard: Sicherheit der Belegschaft. Implementieren Sie Richtlinien und Verfahren, um sicherzustellen, dass alle Mitarbeiter angemessen Zugriff auf elektronisch geschützte Gesundheitsinformationen haben, wie in Absatz (a)(4) dieses Abschnitts vorgesehen, und um zu verhindern, dass Mitarbeiter ohne Zugriff gemäß Absatz (a) (4) dieses Abschnitts Zugriff auf elektronisch geschützte Gesundheitsinformationen erhalten.	internet-gateway-authorized-vpc-nur	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Internet-Gateways nur mit autorisierter Amazon Virtual Private Cloud (Amazon VPC) verbunden sind. Internet-Gateways ermöglichen den bidirektionalen Internetzugang zur und von der Amazon VPC, was möglicher weise zu einem unbefugten Zugriff auf Amazon-VPC-Ressourcen führen kann.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.308(a)(3)(i)	(3)(i) Standard: Sicherheit der Belegschaft. Implementieren Sie Richtlinien und Verfahren, um sicherzustellen, dass alle Mitarbeiter angemessen Zugriff auf elektronisch geschützte Gesundheitsinformationen haben, wie in Absatz (a)(4) dieses Abschnitts vorgesehen, und um zu verhindern, dass Mitarbeiter ohne Zugriff gemäß Absatz (a) (4) dieses Abschnitts Zugriff auf elektronisch geschützte Gesundheitsinformationen erhalten.	lambda-function-public-access-verboten	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass AWS Lambda-Funktionen nicht öffentlich zugänglich sind. Der öffentliche Zugriff kann möglicherweise die Verfügbarkeit von Ressourcen beeinträchtigen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.308(a)(3)(i)	(3)(i) Standard: Sicherheit der Belegschaft. Implementieren Sie Richtlinien und Verfahren, um sicherzustellen, dass alle Mitarbeiter angemessen Zugriff auf elektronisch geschützte Gesundheitsinformationen haben, wie in Absatz (a)(4) dieses Abschnitts vorgesehen, und um zu verhindern, dass Mitarbeiter ohne Zugriff gemäß Absatz (a) (4) dieses Abschnitts Zugriff auf elektronisch geschützte Gesundheitsinformationen erhalten.	rds-instance-public-access-überprüfen	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Relational Database Service (Amazon RDS) -Instances nicht öffentlich sind. Amazon-RDS-Datenbank-Instances können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.308(a)(3)(i)	(3)(i) Standard: Sicherheit der Belegschaft. Implementieren Sie Richtlinien und Verfahren, um sicherzustellen, dass alle Mitarbeiter angemessen Zugriff auf elektronisch geschützte Gesundheitsinformationen haben, wie in Absatz (a)(4) dieses Abschnitts vorgesehen, und um zu verhindern, dass Mitarbeiter ohne Zugriff gemäß Absatz (a) (4) dieses Abschnitts Zugriff auf elektronisch geschützte Gesundheitsinformationen erhalten.	rds-snapshots-public-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Relational Database Service (Amazon RDS) -Instances nicht öffentlich sind. Amazon-RDS-Datenbank-Instances können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.308(a)(3)(i)	(3)(i) Standard: Sicherheit der Belegschaft. Implementieren Sie Richtlinien und Verfahren, um sicherzustellen, dass alle Mitarbeiter angemessen Zugriff auf elektronisch geschützte Gesundheitsinformationen haben, wie in Absatz (a)(4) dieses Abschnitts vorgesehen, und um zu verhindern, dass Mitarbeiter ohne Zugriff gemäß Absatz (a) (4) dieses Abschnitts Zugriff auf elektronisch geschützte Gesundheitsinformationen erhalten.	redshift-cluster-public-access-überprüfen	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Redshift Redshift-Cluster nicht öffentlich sind. Amazon-Redshift-Cluster können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.308(a)(3)(i)	(3)(i) Standard: Sicherheit der Belegschaft. Implementieren Sie Richtlinien und Verfahren, um sicherzustellen, dass alle Mitarbeiter angemessen Zugriff auf elektronisch geschützte Gesundheitsinformationen haben, wie in Absatz (a)(4) dieses Abschnitts vorgesehen, und um zu verhindern, dass Mitarbeiter ohne Zugriff gemäß Absatz (a) (4) dieses Abschnitts Zugriff auf elektronisch geschützte Gesundheitsinformationen erhalten.	s3- -Block-periodisch account-level-public-access	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Simple Storage Service (Amazon S3) -Buckets nicht öffentlich zugänglich sind. Diese Regel trägt dazu bei, sensible Daten vor unbefugten Remote-Benutzern zu schützen, indem sie den öffentlichen Zugriff verhindert. Mit dieser Regel können Sie optional die Parameter ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) und restrictPublicBuckets Parameter (Config Default: True) festlegen. Die tatsächlichen Werte müssen den Richtlini

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			en Ihrer Organisation entsprechen.
164.308(a)(3)(i)	(3)(i) Standard: Sicherheit der Belegschaft. Implementieren Sie Richtlinien und Verfahren, um sicherzustellen, dass alle Mitarbeiter angemessen Zugriff auf elektronisch geschützte Gesundheitsinformationen haben, wie in Absatz (a)(4) dieses Abschnitts vorgesehen, und um zu verhindern, dass Mitarbeiter ohne Zugriff gemäß Absatz (a) (4) dieses Abschnitts Zugriff auf elektronisch geschützte Gesundheitsinformationen erhalten.	s3- bucket-public-read-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie nur autorisierten Benutzern, Prozessen und Geräten Zugriff auf Amazon Simple Storage Service (Amazon S3) - Buckets gewähren. Die Verwaltung des Zugriffs sollte mit der Klassifizierung der Daten übereinstimmen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.308(a)(3)(i)	(3)(i) Standard: Sicherheit der Belegschaft. Implementieren Sie Richtlinien und Verfahren, um sicherzustellen, dass alle Mitarbeiter angemessen Zugriff auf elektronisch geschützte Gesundheitsinformationen haben, wie in Absatz (a)(4) dieses Abschnitts vorgesehen, und um zu verhindern, dass Mitarbeiter ohne Zugriff gemäß Absatz (a) (4) dieses Abschnitts Zugriff auf elektronisch geschützte Gesundheitsinformationen erhalten.	s3- bucket-public-write-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie nur autorisierten Benutzern, Prozessen und Geräten Zugriff auf Amazon Simple Storage Service (Amazon S3) - Buckets gewähren. Die Verwaltung des Zugriffs sollte mit der Klassifizierung der Daten übereinstimmen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.308(a)(3)(i)	(3)(i) Standard: Sicherheit der Belegschaft. Implementieren Sie Richtlinien und Verfahren, um sicherzustellen, dass alle Mitarbeiter angemessen Zugriff auf elektronisch geschützte Gesundheitsinformationen haben, wie in Absatz (a)(4) dieses Abschnitts vorgesehen, und um zu verhindern, dass Mitarbeiter ohne Zugriff gemäß Absatz (a) (4) dieses Abschnitts Zugriff auf elektronisch geschützte Gesundheitsinformationen erhalten.	sagemaker-notebook-no-direct-Internetzugang	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass SageMaker Amazon-Notebooks keinen direkten Internetzugang zulassen. Indem Sie direkten Internetzugang blockieren, vermeiden Sie, dass unbefugte Benutzer auf sensible Daten zugreifen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.308(a)(3)(i)	(3)(i) Standard: Sicherheit der Belegschaft. Implementieren Sie Richtlinien und Verfahren, um sicherzustellen, dass alle Mitarbeiter angemessen Zugriff auf elektronisch geschützte Gesundheitsinformationen haben, wie in Absatz (a)(4) dieses Abschnitts vorgesehen, und um zu verhindern, dass Mitarbeiter ohne Zugriff gemäß Absatz (a) (4) dieses Abschnitts Zugriff auf elektronisch geschützte Gesundheitsinformationen erhalten.	subnet-auto-assign-public-ip-deaktiviert	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon Virtual Private Cloud (VPC) -Subnetzen nicht automatisch eine öffentliche IP-Adresse zugewiesen wird. Amazon Elastic Compute Cloud (EC2) -Instances, die in Subnetzen gestartet werden, in denen dieses Attribut aktiviert ist, haben ihrer primären Netzwerkschnittstelle eine öffentliche IP-Adresse zugewiesen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.308(a)(3)(i)	(3)(i) Standard: Sicherheit der Belegschaft. Implementieren Sie Richtlinien und Verfahren, um sicherzustellen, dass alle Mitarbeiter angemessen Zugriff auf elektronisch geschützte Gesundheitsinformationen haben, wie in Absatz (a)(4) dieses Abschnitts vorgesehen, und um zu verhindern, dass Mitarbeiter ohne Zugriff gemäß Absatz (a) (4) dieses Abschnitts Zugriff auf elektronisch geschützte Gesundheitsinformationen erhalten.	ecs-task-definition-user-for-host-mode-check	Wenn für eine Aufgabendefinition erhöhte Berechtigungen gelten, liegt das daran, dass der Kunde diesen Konfigurationen ausdrücklich zugestimmt hat. Diese Kontrolle prüft, ob eine unerwartete Berechtigungseskalation vorliegt, wenn für eine Aufgabendefinition das Host-Netzwerk aktiviert ist, die Kunden aber keine erhöhten Berechtigungen aktiviert haben.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.308(a)(3)(i)	(3)(i) Standard: Sicherheit der Belegschaft. Implementieren Sie Richtlinien und Verfahren, um sicherzustellen, dass alle Mitarbeiter angemessen Zugriff auf elektronisch geschützte Gesundheitsinformationen haben, wie in Absatz (a)(4) dieses Abschnitts vorgesehen, und um zu verhindern, dass Mitarbeiter ohne Zugriff gemäß Absatz (a) (4) dieses Abschnitts Zugriff auf elektronisch geschützte Gesundheitsinformationen erhalten.	ecs-containers-readonly-access	Die Aktivierung des schreibgeschützten Zugriffs auf Amazon Elastic Container Service (ECS)-Container kann dazu beitragen, das Prinzip der geringsten Berechtigung einzuhalten. Diese Option kann Angriffsvektoren reduzieren, da das Dateisystem der Container-Instance nur geändert werden kann, wenn es über ausdrückliche Lese- und Schreibberechtigungen verfügt.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.308(a)(3)(i)	(3)(i) Standard: Sicherheit der Belegschaft. Implementieren Sie Richtlinien und Verfahren, um sicherzustellen, dass alle Mitarbeiter angemessen Zugriff auf elektronisch geschützte Gesundheitsinformationen haben, wie in Absatz (a)(4) dieses Abschnitts vorgesehen, und um zu verhindern, dass Mitarbeiter ohne Zugriff gemäß Absatz (a) (4) dieses Abschnitts Zugriff auf elektronisch geschützte Gesundheitsinformationen erhalten.	ssm-document-not-public	Stellen Sie sicher, dass AWS Systems Manager (SSM) - Dokumente nicht öffentlich sind, da dies einen unbeabsichtigten Zugriff auf Ihre SSM-Dokumente ermöglichen kann. Ein öffentliches SSM-Dokument kann Informationen über Ihr Konto, Ihre Ressourcen und internen Prozesse preisgeben.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.308(a)(3)(i)	(3)(i) Standard: Sicherheit der Belegschaft. Implementieren Sie Richtlinien und Verfahren, um sicherzustellen, dass alle Mitarbeiter angemessen Zugriff auf elektronisch geschützte Gesundheitsinformationen haben, wie in Absatz (a)(4) dieses Abschnitts vorgesehen, und um zu verhindern, dass Mitarbeiter ohne Zugriff gemäß Absatz (a) (4) dieses Abschnitts Zugriff auf elektronisch geschützte Gesundheitsinformationen erhalten.	s-3 bucket-acl-prohibited	Diese Regel prüft, ob Access Control Lists (ACLs) für die Zugriffskontrolle auf Amazon S3 S3-Buckets verwendet werden. ACLs sind veraltete Zugriffskontrollmechanismen für Amazon S3 S3-Buckets, die älter sind als AWS Identity and Access Management (IAM). Stattdessen empfiehlt es sich ACLs, IAM-Richtlinien oder S3-Bucket-Richtlinien zu verwenden, um den Zugriff auf Ihre S3-Buckets einfacher zu verwalten.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.308(a)(3)(i)	(3)(i) Standard: Sicherheit der Belegschaft. Implementieren Sie Richtlinien und Verfahren, um sicherzustellen, dass alle Mitarbeiter angemessen Zugriff auf elektronisch geschützte Gesundheitsinformationen haben, wie in Absatz (a)(4) dieses Abschnitts vorgesehen, und um zu verhindern, dass Mitarbeiter ohne Zugriff gemäß Absatz (a) (4) dieses Abschnitts Zugriff auf elektronisch geschützte Gesundheitsinformationen erhalten.	codebuild-project-envvar-awscred-überprüfen	Stellen Sie sicher, dass die Anmeldeinformationen AWS_ACCESS_KEY_ID AWS_SECRET_ACCESS_KEY nicht in AWS Codebuild-Projektumgebungen vorhanden sind. Speichern Sie diese Variablen nicht als Klartext. Das Speichern dieser Variablen als Klartext bewirkt eine unbeabsichtigte Offenlegung von Daten sowie unberechtigte Zugriffe.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.308(a)(3)(i)	(3)(i) Standard: Sicherheit der Belegschaft. Implementieren Sie Richtlinien und Verfahren, um sicherzustellen, dass alle Mitarbeiter angemessen Zugriff auf elektronisch geschützte Gesundheitsinformationen haben, wie in Absatz (a)(4) dieses Abschnitts vorgesehen, und um zu verhindern, dass Mitarbeiter ohne Zugriff gemäß Absatz (a) (4) dieses Abschnitts Zugriff auf elektronisch geschützte Gesundheitsinformationen erhalten.	codebuild-project-source-repo-URL-Prüfung	Stellen Sie sicher, dass die URL des Quell-Repositorys GitHub oder des Bitbucket-Quell-Repositorys keine persönlichen Zugriffstoken oder Anmeldeinformationen in Codebuild-Projektumgebungen enthält. AWS Verwende OAuth anstelle von persönlichen Zugriffstoken oder Anmeldedaten die Autorisierung für den Zugriff auf GitHub Bitbucket-Repositorys.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.308(a)(3)(i)	(3)(i) Standard: Sicherheit der Belegschaft. Implementieren Sie Richtlinien und Verfahren, um sicherzustellen, dass alle Mitarbeiter angemessen Zugriff auf elektronisch geschützte Gesundheitsinformationen haben, wie in Absatz (a)(4) dieses Abschnitts vorgesehen, und um zu verhindern, dass Mitarbeiter ohne Zugriff gemäß Absatz (a) (4) dieses Abschnitts Zugriff auf elektronisch geschützte Gesundheitsinformationen erhalten.	restricted-common-ports	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass gemeinsame Ports für Amazon Elastic Compute Cloud (Amazon EC2) -Sicherheitsgruppen eingeschränkt sind. Wenn der Zugriff auf Ports nicht auf vertrauenswürdige Quellen beschränkt wird, kann dies zu Angriffen auf die Verfügbarkeit, Integrität und Vertraulichkeit von Systemen führen. Mit dieser Regel können Sie optional die Parameter blockedPort1–blockedPort5 festlegen (Standardkonfigurationen: 20, 21, 3389, 3306, 4333). Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.308(a)(3)(i)	(3)(i) Standard: Sicherheit der Belegschaft. Implementieren Sie Richtlinien und Verfahren, um sicherzustellen, dass alle Mitarbeiter angemessen Zugriff auf elektronisch geschützte Gesundheitsinformationen haben, wie in Absatz (a)(4) dieses Abschnitts vorgesehen, und um zu verhindern, dass Mitarbeiter ohne Zugriff gemäß Absatz (a) (4) dieses Abschnitts Zugriff auf elektronisch geschützte Gesundheitsinformationen erhalten.	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) Security Groups können bei der Verwaltung des Netzwerkzugriffs helfen, indem sie eine statusbehaftete Filterung von eingehendem und ausgehendem Netzwerkverkehr zu Ressourcen bereitstellen. AWS Wenn Sie eingehenden (oder entfernten) Datenverkehr von 0.0.0.0/0 bis Port 22 auf Ihren Ressourcen nicht zulassen, können Sie den Remote-Zugriff einschränken.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.308(a)(3)(i)	(3)(i) Standard: Sicherheit der Belegschaft. Implementieren Sie Richtlinien und Verfahren, um sicherzustellen, dass alle Mitarbeiter angemessen Zugriff auf elektronisch geschützte Gesundheitsinformationen haben, wie in Absatz (a)(4) dieses Abschnitts vorgesehen, und um zu verhindern, dass Mitarbeiter ohne Zugriff gemäß Absatz (a) (4) dieses Abschnitts Zugriff auf elektronisch geschützte Gesundheitsinformationen erhalten.	autoscaling-launch-config-public-ip-deaktiviert	Wenn Sie Ihre Netzwerkschnittstellen mit einer öffentlichen IP-Adresse konfigurieren, sind die diesen Netzwerkschnittstellen zugehörigen Ressourcen über das Internet erreichbar. EC2 Ressourcen sollten nicht öffentlich zugänglich sein, da dies einen unbeabsichtigten Zugriff auf Ihre Anwendungen oder Server ermöglichen kann.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.308(a)(3)(i)	(3)(i) Standard: Sicherheit der Belegschaft. Implementieren Sie Richtlinien und Verfahren, um sicherzustellen, dass alle Mitarbeiter angemessen Zugriff auf elektronisch geschützte Gesundheitsinformationen haben, wie in Absatz (a)(4) dieses Abschnitts vorgesehen, und um zu verhindern, dass Mitarbeiter ohne Zugriff gemäß Absatz (a) (4) dieses Abschnitts Zugriff auf elektronisch geschützte Gesundheitsinformationen erhalten.	opensearch-in-vpc-only	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass sich Amazon OpenSearch Service-Domains innerhalb einer Amazon Virtual Private Cloud (Amazon VPC) befinden. Eine Amazon OpenSearch Service-Domain innerhalb einer Amazon VPC ermöglicht die sichere Kommunikation zwischen Amazon OpenSearch Service und anderen Services innerhalb der Amazon VPC, ohne dass ein Internet-Gateway, ein NAT-Gerät oder eine VPN-Verbindung erforderlich ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.308(a)(3)(ii)(A)	(A) and/or supervision (Addressable). Implement procedures for the authorization and/or Überwachung der Autorisierung von Mitarbeitern, die mit elektronisch geschützten Gesundheitsinformationen arbeiten oder an Orten, an denen auf diese zugegriffen werden kann.	emr-kerberos-enabled	Die Zugriffsberechtigungen und -autorisierungen können verwaltet und nach den Prinzipien der geringsten Berechtigung und Aufgabentrennung integriert werden, indem Kerberos für Amazon-EMR-Cluster aktiviert wird. In Kerberos werden Services und Benutzer, die sich authentifizieren müssen, als Prinzipale bezeichnet. Prinzipale befinden sich in einem Kerberos-Bereich. Innerhalb dieses Bereichs wird ein Kerberos-Server als Key Distribution Center (KDC) bezeichnet. Über diesen Server können sich Prinzipale authentifizieren. Die Authentifizierung im KDC erfolgt durch die Ausstellung von Authentif

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			izierungstickets. Das KDC unterhält eine Datenbank der Prinzipale in seinem Bereich mit ihren Passwörtern und anderen administr ativen Informationen zu jedem Prinzipal.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.308(a)(3)(ii)(A)	(A) and/or supervision (Addressable). Implement procedures for the authorization and/or Überwachung der Zulassung von Mitarbeitern, die mit elektronisch geschützten Gesundheitsinformationen arbeiten oder an Orten, an denen auf diese zugegriffen werden könnte.	iam-customer-policy-blocked-KMS-Aktionen	AWS Identity and Access Management (IAM) kann Ihnen helfen, die Prinzipien der geringsten Rechte und der Aufgabentrennung in Zugriffsberechtigungen und Autorisierungen zu integrieren und so zu verhindern, dass Richtlinien blockierte Aktionen für alle AWS Schlüssel des Key Management Service enthalten. Wenn Benutzer mehr Rechte haben, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und Aufgabentrennung verstoßen. Mit dieser Regel können Sie den Parameter festlegen. blockedActionsPatterns (Wert „AWS Bewährte grundlegende Sicherheitsmethoden“: kms:

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			Decrypt, kms:ReEncryptFrom). Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.308(a)(3)(ii)(A)	(A) and/or supervision (Addressable). Implement procedures for the authorization and/or Überwachung der Autorisierung von Mitarbeitern, die mit elektronisch geschützten Gesundheitsinformationen oder an Orten arbeiten, an denen auf diese zugegriffen werden könnte.	iam-inline-policy-blocked-KMS-Aktionen	Stellen Sie sicher, dass ein Benutzer, eine IAM-Rolle oder eine IAM-Gruppe (AWS Identity and Access Management) nicht über eine Inline-Richtlinie verfügt, die blockierte Aktionen für alle AWS Schlüssel des Key Management Service zulässt. AWS empfiehlt, verwaltete Richtlinien anstelle von Inline-Richtlinien zu verwenden. Verwaltete Richtlinien ermöglichen Wiederverwendbarkeit, Versionsverwaltung, Rollback und Delegierung der Berechtigungsverwaltung. Mit dieser Regel können Sie den blockedActionsPatterns Parameter festlegen. (Wert „AWS Bewährte grundlegende Sicherheitsmethoden“: kms:Decrypt, kms:ReEncryptFrom). Die

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.
164.308(a)(3)(ii)(A)	(A) and/or supervision (Addressable). Implement procedures for the authorization and/or Überwachung der Autorisierung von Mitarbeitern, die mit elektronisch geschützten Gesundheitsinformationen oder an Orten arbeiten, an denen auf diese zugegriffen werden könnte.	iam-no-inline-policy-überprüfen	Stellen Sie sicher, dass ein Benutzer, eine IAM-Rolle oder eine IAM-Gruppe (AWS Identity and Access Management) nicht über eine Inline-Richtlinie zur Zugriffskontrolle auf Systeme und Ressourcen verfügt. AWS empfiehlt, verwaltete Richtlinien anstelle von Inline-Richtlinien zu verwenden. Verwaltete Richtlinien ermöglichen Wiederverwendbarkeit, Versionsverwaltung, Rollback und Delegierung der Berechtigungsverwaltung.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.308(a)(3)(ii)(A)	(A) and/or supervision (Addressable). Implement procedures for the authorization and/or Überwachung der Autorisierung von Mitarbeitern, die mit elektronisch geschützten Gesundheitsinformationen arbeiten oder an Orten, an denen auf diese zugegriffen werden kann.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) kann Ihnen dabei helfen, die Prinzipien der geringsten Rechte und der Aufgabentrennung in Zugriffsberechtigungen und Autorisierungen zu integrieren und so zu verhindern, dass Richtlinien „Effect“: „Allow“ mit „Action“: „*“ anstelle von „Resource“: „*“ enthalten. Wenn Benutzern mehr Rechte eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und der Aufgabentrennung verstoßen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.308(a)(3)(ii)(A)	(A) and/or supervision (Addressable). Implement procedures for the authorization and/or Überwachung der Autorisierung von Mitarbeitern, die mit elektronisch geschützten Gesundheitsinformationen arbeiten oder sich an Orten befinden, an denen auf diese zugegriffen werden kann.	iam-user-no-policies-überprüfen	Diese Regel stellt sicher, dass AWS Identity and Access Management (IAM) -Richtlinien nur Gruppen oder Rollen zugewiesen werden, um den Zugriff auf Systeme und Ressourcen zu kontrollieren. Die Zuweisung von Berechtigungen auf Gruppen- oder Rollenebene trägt dazu bei, die Wahrscheinlichkeit zu verringern, dass eine Identität übermäßige Berechtigungen erhält oder beibehält.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.308(a)(3)(ii)(A)	(A) and/or supervision (Addressable). Implement procedures for the authorization and/or Überwachung der Autorisierung von Mitarbeitern, die mit elektronisch geschützten Gesundheitsinformationen arbeiten oder an Orten, an denen auf diese zugegriffen werden kann.	iam-policy-no-statements-with-full-access	Stellen Sie sicher, dass IAM-Aktionen nur auf die benötigten Aktionen beschränkt sind. Wenn Benutzern mehr Rechte eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und der Aufgabentrennung verstoßen.
164.308(a)(3)(ii)(A)	(A) and/or supervision (Addressable). Implement procedures for the authorization and/or Überwachung der Zulassung von Mitarbeitern, die mit elektronisch geschützten Gesundheitsinformationen arbeiten oder an Orten, an denen auf diese zugegriffen werden könnte.	ec2- instance-profile-attached	EC2 Instanzprofile übergeben eine IAM-Rolle an eine Instanz EC2 . Das Anhängen eines Instance-Profils an Ihre Instances kann bei der Implementierung von geringsten Berechtigungen und der Berechtigungsverwaltung helfen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.308(a)(3)(ii)(A)	(A) and/or supervision (Addressable). Implement procedures for the authorization and/or Überwachung der Autorisierung von Mitarbeitern, die mit elektronisch geschützten Gesundheitsinformationen arbeiten oder an Orten, an denen auf diese zugegriffen werden kann.	ecs-task-definition-user-for-host-mode-check	Wenn für eine Aufgabendefinition erhöhte Berechtigungen gelten, liegt das daran, dass der Kunde diesen Konfigurationen ausdrücklich zugestimmt hat. Diese Kontrolle prüft, ob eine unerwartete Berechtigungseskalation vorliegt, wenn für eine Aufgabendefinition das Host-Netzwerk aktiviert ist, die Kunden aber keine erhöhten Berechtigungen aktiviert haben.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.308(a)(3)(ii)(A)	(A) and/or supervision (Addressable). Implement procedures for the authorization and/or Überwachung der Zulassung von Mitarbeitern, die mit elektronisch geschützten Gesundheitsinformationen arbeiten oder an Orten, an denen auf diese zugegriffen werden könnte.	ecs-containers-readonly-access	Die Aktivierung des schreibgeschützten Zugriffs auf Amazon Elastic Container Service (ECS)-Container kann dazu beitragen, das Prinzip der geringsten Berechtigung einzuhalten. Diese Option kann Angriffsvektoren reduzieren, da das Dateisystem der Container-Instance nur geändert werden kann, wenn es über ausdrückliche Lese- und Schreibberechtigungen verfügt.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.308(a)(3)(ii)(A)	(A) and/or supervision (Addressable). Implement procedures for the authorization and/or Überwachung der Zulassung von Mitarbeitern, die mit elektronisch geschützten Gesundheitsinformationen arbeiten oder an Orten, an denen auf diese zugegriffen werden könnte.	cloud-trail-cloud-watch-Logs aktiviert	Verwenden Sie Amazon CloudWatch , um Protokoll ereignisaktivitäten zentral zu sammeln und zu verwalten. Die Aufnahme von AWS CloudTrail Daten liefert Einzelheiten zu den API-Aufrufaktivitäten in Ihrem AWS-Konto.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.308(a)(3)(ii)(A)	(A) and/or supervision (Addressable). Implement procedures for the authorization and/or Überwachung der Autorisierung von Mitarbeitern, die mit elektronisch geschützten Gesundheitsinformationen arbeiten oder an Orten, an denen auf diese zugegriffen werden kann.	cloudtrail-enabled	AWS CloudTrail kann durch die Aufzeichnung von Aktionen und API-Aufrufen in der AWS Management Console helfen, die Ablehnung zu verhindern. Sie können die Benutzer und die Benutzer AWS-Konten , die einen AWS Dienst aufgerufen haben, die Quell-IP-Adresse, über die die Aufrufe generiert wurden, und den Zeitpunkt der Anrufe identifizieren. Einzelheiten zu den erfassten Daten finden Sie unter Inhalt des AWS CloudTrail Datensatzes.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.308(a)(3)(ii)(A)	(A) and/or supervision (Addressable). Implement procedures for the authorization and/or Überwachung der Autorisierung von Mitarbeitern, die mit elektronisch geschützten Gesundheitsinformationen arbeiten oder an Orten, an denen auf diese zugegriffen werden kann.	cloudtrail-s3-dataevents-enabled	Die Erfassung von Simple Storage Service (Amazon S3)-Datenereignissen unterstützt die Erkennung von ungewöhnlichen Aktivitäten. Zu den Details gehören AWS-Konto Informationen über den Zugriff auf einen Amazon S3 S3-Bucket, die IP-Adresse und die Uhrzeit des Ereignisses.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.308(a)(3)(ii)(A)	(A) and/or supervision (Addressable). Implement procedures for the authorization and/or Überwachung der Autorisierung von Mitarbeitern, die mit elektronisch geschützten Gesundheitsinformationen arbeiten oder an Orten, an denen auf diese zugegriffen werden kann.	multi-region-cloudtrail-enabled	AWS CloudTrail zeichnet Aktionen und API-Aufrufe der AWS Management Console auf. Sie können feststellen, welche Benutzer und Konten angerufen wurden AWS, von welcher Quell-IP-Adresse aus die Anrufe getätigt wurden und wann die Anrufe erfolgten. CloudTrail übermittelt Protokolldateien aus allen AWS Regionen an Ihren S3-Bucket, wenn MULTI_REGION_CLOUD_TRAIL_ENABLED aktiviert ist. Außerdem wird beim AWS Start einer neuen Region derselbe Trail in der neuen Region erstellt. CloudTrail Dadurch erhalten Sie automatisch Protokolldateien mit API-Aktivitäten für die neue Region.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.308(a)(3)(ii)(A)	(A) and/or supervision (Addressable). Implement procedures for the authorization and/or Überwachung der Autorisierung von Mitarbeitern, die mit elektronisch geschützten Gesundheitsinformationen arbeiten oder sich an Orten befinden, an denen auf diese zugegriffen werden kann.	rds-logging-enabled	Um die Protokollierung und Überwachung in Ihrer Umgebung zu erleichtern, stellen Sie sicher, dass die Amazon Relational Database Service (Amazon RDS)-Protokollierung aktiviert ist. Mit der Amazon-RDS-Protokollierung können Sie Ereignisse wie Verbindungen, Verbindungsabbrüche, Abfragen oder abgefragte Tabellen erfassen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.308(a)(3)(ii)(A)	(A) and/or supervision (Addressable). Implement procedures for the authorization and/or Überwachung der Zulassung von Mitarbeitern, die mit elektronisch geschützten Gesundheitsinformationen arbeiten oder an Orten, an denen auf diese zugegriffen werden könnte.	s 3- bucket-logging-enabled	Die Amazon Simple Storage Service (Amazon S3)-Serverzugriffsprotokollierung bietet eine Methode zur Überwachung des Netzwerks im Hinblick auf potenzielle Cybersicherheitsereignisse. Die Ereignisse werden überwacht, indem detaillierte Aufzeichnungen über die Anfragen erfasst werden, die an einen Amazon-S3-Bucket gestellt wurden. Jeder Zugriffsprotokolleintrag enthält Details zu einer einzelnen Zugriffsanfrage. Zu den Details gehören Anforderer, Bucket-Name, Anforderungszeit, Anforderungsaktion, Antwortstatus und Fehlercode, falls relevant.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.308(a)(3)(ii)(A)	(A) and/or supervision (Addressable). Implement procedures for the authorization and/or Überwachung der Zulassung von Mitarbeitern, die mit elektronisch geschützten Gesundheitsinformationen arbeiten oder an Orten, an denen auf diese zugegriffen werden könnte.	vpc-flow-logs-enabled	VPC-Flow-Protokolle erfassen detaillierte Informationsdatensätze über den IP-Datenverkehr, der zu und von Netzwerkschnittstellen in Ihrer Amazon Virtual Private Cloud (Amazon VPC) fließt. Standardmäßig enthalten Flow-Protokolldatensätze Werte für die verschiedenen Komponenten des IP-Flows, einschließlich Quelle, Ziel und Protokoll.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.308(a)(3)(ii)(A)	(A) and/or supervision (Addressable). Implement procedures for the authorization and/or Überwachung der Zulassung von Mitarbeitern, die mit elektronisch geschützten Gesundheitsinformationen arbeiten oder an Orten, an denen auf diese zugegriffen werden könnte.	elasticsearch-logs-to-cloudwatch	Stellen Sie sicher, dass für Amazon OpenSearch Service-Domains Fehlerprotokolle aktiviert und zur Aufbewahrung und Beantwortung an Amazon CloudWatch Logs gestreamt werden. Domain-Fehlerprotokolle sind bei Sicherheits- und Zugriffsprüfungen sowie bei der Diagnose von Verfügbarkeitsproblemen nützlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.308(a)(3)(ii)(A)	(A) and/or supervision (Addressable). Implement procedures for the authorization and/or Überwachung der Autorisierung von Mitarbeitern, die mit elektronisch geschützten Gesundheitsinformationen arbeiten oder an Orten, an denen auf diese zugegriffen werden kann.	opensearch-logs-to-cloudwatch	Stellen Sie sicher, dass für Amazon OpenSearch Service-Domains Fehlerprotokolle aktiviert und zur Aufbewahrung und Beantwortung an Amazon CloudWatch Logs gestreamt werden. OpenSearch Service-Fehlerprotokolle können bei Sicherheits- und Zugriffsprüfungen helfen und bei der Diagnose von Verfügbarkeitsproblemen helfen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.308(a)(3)(ii)(B)	(B) Verfahren zur Freigabe am Personal (adressierbar). Implementiere Sie Verfahren, um festzustellen, ob der Zugriff von Mitarbeitern auf elektronisch geschützte Gesundheitsinformationen angemessen ist.	emr-kerberos-enabled	Die Zugriffsberechtigungen und -autorisierungen können verwaltet und nach den Prinzipien der geringsten Berechtigung und Aufgabentrennung integriert werden, indem Kerberos für Amazon-EMR-Cluster aktiviert wird. In Kerberos werden Services und Benutzer, die sich authentifizieren müssen, als Prinzipale bezeichnet. Prinzipale befinden sich in einem Kerberos-Bereich. Innerhalb dieses Bereichs wird ein Kerberos-Server als Key Distribution Center (KDC) bezeichnet. Über diesen Server können sich Prinzipale authentifizieren. Die Authentifizierung im KDC erfolgt durch die Ausstellung von Authentif

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			izierungstickets. Das KDC unterhält eine Datenbank der Prinzipale in seinem Bereich mit ihren Passwörtern und anderen administr ativen Informationen zu jedem Prinzipal.
164.308(a)(3)(ii)(B)	(B) Verfahren zur Freigabe am Personal (adressierbar). Implementiere Sie Verfahren, um festzustellen, ob der Zugriff von Mitarbeit ern auf elektronisch geschützte Gesundhei tsinformationen angemessen ist.	iam-no-inline-policy-überprüfen	Stellen Sie sicher, dass ein Benutzer, eine IAM-Rolle oder eine IAM-Gruppe (AWS Identity and Access Management) nicht über eine Inline-Richtlinie zur Zugriffsk ontrolle auf Systeme und Ressource n verfügt. AWS empfiehlt, verwaltet e Richtlinien anstelle von Inline-Richtlinien zu verwenden. Verwaltete Richtlini en ermöglichen Wiederverwendbarke it, Versionsverwaltung , Rollback und Delegierung der Berechtigungsverwa ltung.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.308(a)(3)(ii)(B)	(B) Verfahren zur Freigabe am Personal (adressierbar). Implementiere Sie Verfahren, um festzustellen, ob der Zugriff von Mitarbeitern auf elektronisch geschützte Gesundheitsinformationen angemessen ist.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) kann Ihnen dabei helfen, die Prinzipien der geringsten Rechte und der Aufgabentrennung in Zugriffsberechtigungen und Autorisierungen zu integrieren und so zu verhindern, dass Richtlinien „Effect“: „Allow“ mit „Action“: „*“ anstelle von „Resource“: „*“ enthalten. Wenn Benutzern mehr Rechte eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und der Aufgabentrennung verstoßen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.308(a)(3)(ii)(B)	(B) Verfahren zur Freigabe am Personal (adressierbar). Implementiere Sie Verfahren, um festzustellen, ob der Zugriff von Mitarbeit ern auf elektronisch geschützte Gesundhei tsinformationen angemessen ist.	iam-user-no-policies-überprüfen	Diese Regel stellt sicher, dass AWS Identity and Access Management (IAM) -Richtlinien nur Gruppen oder Rollen zugewiese n werden, um den Zugriff auf Systeme und Ressourcen zu kontrollieren. Die Zuweisung von Berechtig ungen auf Gruppen- oder Rollenebene trägt dazu bei, die Wahrscheinlichkeit zu verringern, dass eine Identität übermäßige Berechtigungen erhält oder beibehält.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.308(a)(3)(ii)(B)	(B) Verfahren zur Freigabe am Personal (adressierbar). Implementiere Sie Verfahren, um festzustellen, ob der Zugriff von Mitarbeitern auf elektronisch geschützte Gesundheitsinformationen angemessen ist.	iam-policy-no-statements-with-full-access	Stellen Sie sicher, dass IAM-Aktionen nur auf die benötigten Aktionen beschränkt sind. Wenn Benutzern mehr Rechte eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und der Aufgabentrennung verstoßen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.308(a)(3)(ii)(B)	(B) Verfahren zur Freigabe am Personal (adressierbar). Implementiere Sie Verfahren, um festzustellen, ob der Zugriff von Mitarbeitern auf elektronisch geschützte Gesundheitsinformationen angemessen ist.	restricted-common-ports	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass gemeinsame Ports für Amazon Elastic Compute Cloud (Amazon EC2) -Sicherheitsgruppen eingeschränkt sind. Wenn der Zugriff auf Ports nicht auf vertrauenswürdige Quellen beschränkt wird, kann dies zu Angriffen auf die Verfügbarkeit, Integrität und Vertraulichkeit von Systemen führen. Mit dieser Regel können Sie optional die Parameter blockedPort1–blockedPort5 festlegen (Standardkonfigurationen: 20, 21, 3389, 3306, 4333). Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.308(a)(3)(ii)(B)	(B) Verfahren zur Freigabe am Personal (adressierbar). Implementiere Sie Verfahren, um festzustellen, ob der Zugriff von Mitarbeit ern auf elektronisch geschützte Gesundhei tsinformationen angemessen ist.	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) Security Groups können bei der Verwaltung des Netzwerkzugriffs helfen, indem sie eine statusbeh aftete Filterung von eingehendem und ausgehendem Netzwerkverkehr zu Ressourcen bereitste llen. AWS Wenn Sie eingehenden (oder entfernten) Datenverk ehr von 0.0.0.0/0 bis Port 22 auf Ihren Ressourcen nicht zulassen, können Sie den Remote-Zugriff einschränken.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.308(a)(3)(ii)(B)	(B) Verfahren zur Freigabe am Personal (adressierbar). Implementiere Sie Verfahren, um festzustellen, ob der Zugriff von Mitarbeitern auf elektronisch geschützte Gesundheitsinformationen angemessen ist.	ssm-document-not-public	Stellen Sie sicher, dass AWS Systems Manager (SSM) - Dokumente nicht öffentlich sind, da dies einen unbeabsichtigten Zugriff auf Ihre SSM-Dokumente ermöglichen kann. Ein öffentliches SSM-Dokument kann Informationen über Ihr Konto, Ihre Ressourcen und internen Prozesse preisgeben.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.308(a)(3)(ii)(B)	(B) Verfahren zur Freigabe am Personal (adressierbar). Implementiere Sie Verfahren, um festzustellen, ob der Zugriff von Mitarbeitern auf elektronisch geschützte Gesundheitsinformationen angemessen ist.	ecs-containers-readonly-access	Die Aktivierung des schreibgeschützten Zugriffs auf Amazon Elastic Container Service (ECS)-Container kann dazu beitragen, das Prinzip der geringsten Berechtigung einzuhalten. Diese Option kann Angriffsvektoren reduzieren, da das Dateisystem der Container-Instance nur geändert werden kann, wenn es über ausdrückliche Lese- und Schreibberechtigungen verfügt.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.308(a)(3)(ii)(B)	(B) Verfahren zur Freigabe am Personal (adressierbar). Implementiere Sie Verfahren, um festzustellen, ob der Zugriff von Mitarbeitern auf elektronisch geschützte Gesundheitsinformationen angemessen ist.	autoscaling-launch-config-public-ip-deaktiviert	Wenn Sie Ihre Netzwerkschnittstellen mit einer öffentlichen IP-Adresse konfigurieren, sind die diesen Netzwerkschnittstellen zugehörigen Ressourcen über das Internet erreichbar. EC2 Ressourcen sollten nicht öffentlich zugänglich sein, da dies einen unbeabsichtigten Zugriff auf Ihre Anwendungen oder Server ermöglichen kann.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.308(a)(3)(ii)(B)	(B) Verfahren zur Freigabe am Personal (adressierbar). Implementiere Sie Verfahren, um festzustellen, ob der Zugriff von Mitarbeitern auf elektronisch geschützte Gesundheitsinformationen angemessen ist.	s-3 bucket-acl-prohibited	Diese Regel prüft, ob Access Control Lists (ACLs) für die Zugriffskontrolle auf Amazon S3 S3-Buckets verwendet werden. ACLs sind veraltete Zugriffskontrollmechanismen für Amazon S3 S3-Buckets, die älter sind als AWS Identity and Access Management (IAM). Stattdessen empfiehlt es sich ACLs, IAM-Richtlinien oder S3-Bucket-Richtlinien zu verwenden, um den Zugriff auf Ihre S3-Buckets einfacher zu verwalten.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.308(a)(3)(ii)(C)	(C) Verfahren zur Beendigung des Zugriffs (adressierbar). Implementieren Sie Verfahren, um den Zugriff auf elektronisch geschützte Gesundheitsinformationen einzustellen, wenn ein Beschäftigungsverhältnis endet oder dies aufgrund der Bestimmungen gemäß Absatz (a)(3)(ii)(B) dieses Abschnitts erforderlich ist.	access-keys-rotated	Die Anmeldeinformationen für autorisierte Geräte, Benutzer und Prozesse werden geprüft, indem sichergestellt wird, dass die IAM-Zugriffsschlüssel entsprechend den Vorgaben der Unternehmensrichtlinie rotiert werden. Das regelmäßige Ändern der Zugriffsschlüssel ist eine bewährte Sicherheitsmethode. Es verkürzt den Zeitraum, in dem ein Zugriffsschlüssel aktiv ist, und reduziert die Auswirkungen auf das Unternehmen, wenn die Schlüssel kompromittiert werden. Diese Regel erfordert einen Wert für die Zugriffsschlüssel-Rotation (Standardkonfiguration: 90). Der tatsächliche Wert muss den Richtlini

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			en Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.308(a)(4)(i)	(4)(i) Standard: Verwaltung des Informationszugriffs. Implementieren Sie Richtlinien und Verfahren für die Genehmigung des Zugriffs auf elektronisch geschützte Gesundheitsinformationen, die den geltenden Anforderungen in Unterabschnitt E dieses Abschnitts entsprechen.	emr-kerberos-enabled	Die Zugriffsberechtigungen und -autorisierungen können verwaltet und nach den Prinzipien der geringsten Berechtigung und Aufgabentrennung integriert werden, indem Kerberos für Amazon-EMR-Cluster aktiviert wird. In Kerberos werden Services und Benutzer, die sich authentifizieren müssen, als Prinzipale bezeichnet. Prinzipale befinden sich in einem Kerberos-Bereich. Innerhalb dieses Bereichs wird ein Kerberos-Server als Key Distribution Center (KDC) bezeichnet. Über diesen Server können sich Prinzipale authentifizieren. Die Authentifizierung im KDC erfolgt durch die Ausstellung von Authentif

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			izierungstickets. Das KDC unterhält eine Datenbank der Prinzipale in seinem Bereich mit ihren Passwörtern und anderen administr ativen Informationen zu jedem Prinzipal.
164.308(a)(4)(i)	(4)(i) Standard: Verwaltung des Informationszugrif fs. Implementieren Sie Richtlinien und Verfahren für die Genehmigu ng des Zugriffs auf elektronisch geschützte Gesundhei tsinformationen, die den geltenden Anforderungen in Unterabschnitt E dieses Abschnitts entsprechen.	iam-no-inline-policy-überprüfen	Stellen Sie sicher, dass ein Benutzer, eine IAM-Rolle oder eine IAM-Gruppe (AWS Identity and Access Management) nicht über eine Inline-Richtlinie zur Zugriffsk ontrolle auf Systeme und Ressource n verfügt. AWS empfiehlt, verwaltet e Richtlinien anstelle von Inline-Richtlinien zu verwenden. Verwaltete Richtlini en ermöglichen Wiederverwendbarke it, Versionsverwaltung , Rollback und Delegierung der Berechtigungsverwa ltung.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.308(a)(4)(i)	(4)(i) Standard: Verwaltung des Informationszugriffs. Implementieren Sie Richtlinien und Verfahren für die Genehmigung des Zugriffs auf elektronisch geschützte Gesundheitsinformationen, die den geltenden Anforderungen in Unterabschnitt E dieses Abschnitts entsprechen.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) kann Ihnen dabei helfen, die Prinzipien der geringsten Rechte und der Aufgabentrennung in Zugriffsberechtigungen und Autorisierungen zu integrieren und so zu verhindern, dass Richtlinien „Effect“: „Allow“ mit „Action“: „*“ anstelle von „Resource“: „*“ enthalten. Wenn Benutzern mehr Rechte eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und der Aufgabentrennung verstoßen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.308(a)(4)(i)	(4)(i) Standard: Verwaltung des Informationszugrif fs. Implementieren Sie Richtlinien und Verfahren für die Genehmigu ng des Zugriffs auf elektronisch geschützte Gesundhei tsinformationen, die den geltenden Anforderungen in Unterabschnitt E dieses Abschnitts entsprechen.	iam-user-no-policies-überprüfen	Diese Regel stellt sicher, dass AWS Identity and Access Management (IAM) -Richtlinien nur Gruppen oder Rollen zugewiese n werden, um den Zugriff auf Systeme und Ressourcen zu kontrollieren. Die Zuweisung von Berechtig ungen auf Gruppen- oder Rollenebene trägt dazu bei, die Wahrscheinlichkeit zu verringern, dass eine Identität übermäßige Berechtigungen erhält oder beibehält.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.308(a)(4)(i)	(4)(i) Standard: Verwaltung des Informationszugriffs. Implementieren Sie Richtlinien und Verfahren für die Genehmigung des Zugriffs auf elektronisch geschützte Gesundheitsinformationen, die den geltenden Anforderungen in Unterabschnitt E dieses Abschnitts entsprechen.	iam-policy-no-statements-with-full-access	Stellen Sie sicher, dass IAM-Aktionen nur auf die benötigten Aktionen beschränkt sind. Wenn Benutzern mehr Rechte eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und der Aufgabentrennung verstoßen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.308(a)(4)(i)	(4)(i) Standard: Verwaltung des Informationszugrif fs. Implementieren Sie Richtlinien und Verfahren für die Genehmigu ng des Zugriffs auf elektronisch geschützte Gesundhei tsinformationen, die den geltenden Anforderungen in Unterabschnitt E dieses Abschnitts entsprechen.	restricted-common-ports	Verwalten Sie den Zugriff auf Ressource n in der AWS Cloud, indem Sie sicherste llen, dass gemeinsam e Ports für Amazon Elastic Compute Cloud (Amazon EC2) -Sicherhe itsgruppen eingeschr ränkt sind. Wenn der Zugriff auf Ports nicht auf vertrauen swürdige Quellen beschränkt wird, kann dies zu Angriffen auf die Verfügbar keit, Integrität und Vertraulichkeit von Systemen führen. Mit dieser Regel können Sie optional die Parameter blockedPo rt1–blockedPort5 festlegen (Standard konfigurationen: 20, 21, 3389, 3306, 4333). Die tatsächli chen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.308(a)(4)(i)	(4)(i) Standard: Verwaltung des Informationszugrif fs. Implementieren Sie Richtlinien und Verfahren für die Genehmigu ng des Zugriffs auf elektronisch geschützte Gesundhei tsinformationen, die den geltenden Anforderungen in Unterabschnitt E dieses Abschnitts entsprechen.	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) Security Groups können bei der Verwaltung des Netzwerkzugriffs helfen, indem sie eine statusbeh aftete Filterung von eingehendem und ausgehendem Netzwerkverkehr zu Ressourcen bereitste llen. AWS Wenn Sie eingehenden (oder entfernten) Datenverk ehr von 0.0.0.0/0 bis Port 22 auf Ihren Ressourcen nicht zulassen, können Sie den Remote-Zugriff einschränken.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.308(a)(4)(i)	(4)(i) Standard: Verwaltung des Informationszugriffs. Implementieren Sie Richtlinien und Verfahren für die Genehmigung des Zugriffs auf elektronisch geschützte Gesundheitsinformationen, die den geltenden Anforderungen in Unterabschnitt E dieses Abschnitts entsprechen.	ssm-document-not-public	Stellen Sie sicher, dass AWS Systems Manager (SSM) - Dokumente nicht öffentlich sind, da dies einen unbeabsichtigten Zugriff auf Ihre SSM-Dokumente ermöglichen kann. Ein öffentliches SSM-Dokument kann Informationen über Ihr Konto, Ihre Ressourcen und internen Prozesse preisgeben.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.308(a)(4)(i)	(4)(i) Standard: Verwaltung des Informationszugriffs. Implementieren Sie Richtlinien und Verfahren für die Genehmigung des Zugriffs auf elektronisch geschützte Gesundheitsinformationen, die den geltenden Anforderungen in Unterabschnitt E dieses Abschnitts entsprechen.	ecs-containers-readonly-access	Die Aktivierung des schreibgeschützten Zugriffs auf Amazon Elastic Container Service (ECS)-Container kann dazu beitragen, das Prinzip der geringsten Berechtigung einzuhalten. Diese Option kann Angriffsvektoren reduzieren, da das Dateisystem der Container-Instance nur geändert werden kann, wenn es über ausdrückliche Lese- und Schreibberechtigungen verfügt.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.308(a)(4)(i)	(4)(i) Standard: Verwaltung des Informationszugriffs. Implementieren Sie Richtlinien und Verfahren für die Genehmigung des Zugriffs auf elektronisch geschützte Gesundheitsinformationen, die den geltenden Anforderungen in Unterabschnitt E dieses Abschnitts entsprechen.	s-3 bucket-acl-prohibited	Diese Regel prüft, ob Access Control Lists (ACLs) für die Zugriffskontrolle auf Amazon S3 S3-Buckets verwendet werden. ACLs sind veraltete Zugriffskontrollmechanismen für Amazon S3 S3-Buckets, die älter sind als AWS Identity and Access Management (IAM). Stattdessen empfiehlt es sich ACLs, IAM-Richtlinien oder S3-Bucket-Richtlinien zu verwenden, um den Zugriff auf Ihre S3-Buckets einfacher zu verwalten.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.308(a)(4)(ii)(A)	(A) Isolierung der Clearinghouse-Funktionen für Gesundheitsinformationen (erforderlich). Wenn ein Clearinghouse für Gesundheitsinformationen Teil einer größeren Organisation ist, muss das Clearinghouse Richtlinien und Verfahren einführen, die die elektronisch geschützten Gesundheitsinformationen des Clearinghouse vor unbefugtem Zugriff durch andere Teile der Organisation schützen.	ec2-imdsv2-check	Stellen Sie sicher, dass die Methode Instance Metadata Service Version 2 (IMDSv2) aktiviert ist, um den Zugriff auf und die Kontrolle der Amazon Elastic Compute Cloud (Amazon EC2) - Instance-Metadaten zu schützen. Die IMDSv2 Methode verwendet sitzungsbasierte Kontrollen. Mit können Kontrollen implementiert werden IMDSv2, um Änderungen an Instanzmetadaten einzuschränken.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.308(a)(4)(ii)(A)	(A) Isolierung der Clearinghouse-Funktionen für Gesundheitsinformationen (erforderlich). Wenn ein Clearinghouse für Gesundheitsinformationen Teil einer größeren Organisation ist, muss das Clearinghouse Richtlinien und Verfahren einführen, die die elektronisch geschützten Gesundheitsinformationen des Clearinghouse vor unbefugtem Zugriff durch andere Teile der Organisation schützen.	emr-kerberos-enabled	Die Zugriffsberechtigungen und -autorisierungen können verwaltet und nach den Prinzipien der geringsten Berechtigung und Aufgabentrennung integriert werden, indem Kerberos für Amazon-EMR-Cluster aktiviert wird. In Kerberos werden Services und Benutzer, die sich authentifizieren müssen, als Prinzipale bezeichnet. Prinzipale befinden sich in einem Kerberos-Bereich. Innerhalb dieses Bereichs wird ein Kerberos-Server als Key Distribution Center (KDC) bezeichnet. Über diesen Server können sich Prinzipale authentifizieren. Die Authentifizierung im KDC erfolgt durch die Ausstellung von Authentif

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			izierungstickets. Das KDC unterhält eine Datenbank der Prinzipale in seinem Bereich mit ihren Passwörtern und anderen administr ativen Informationen zu jedem Prinzipal.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.308(a)(4)(ii)(A)	(A) Isolierung der Clearinghouse-Funktionen für Gesundheitsinformationen (erforderlich). Wenn ein Clearinghouse für Gesundheitsinformationen Teil einer größeren Organisation ist, muss das Clearinghouse Richtlinien und Verfahren einführen, die die elektronisch geschützten Gesundheitsinformationen des Clearinghouse vor unbefugtem Zugriff durch andere Teile der Organisation schützen.	iam-customer-policy-blocked-kms-Aktionen	AWS Identity and Access Management (IAM) kann Ihnen helfen, die Prinzipien der geringsten Rechte und der Aufgabentrennung in Zugriffsberechtigungen und Autorisierungen zu integrieren und so zu verhindern, dass Richtlinien blockierte Aktionen für alle AWS Schlüssel des Key Management Service enthalten. Wenn Benutzer mehr Rechte haben, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und Aufgabentrennung verstoßen. Mit dieser Regel können Sie den Parameter festlegen. blockedActionsPatterns (Wert „AWS Bewährte grundlegende Sicherheitsmethoden“: kms:

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			Decrypt, kms:ReEncryptFrom). Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.308(a)(4)(ii)(A)	(A) Isolierung der Clearinghouse-Funktionen für Gesundheitsinformationen (erforderlich). Wenn ein Clearinghouse für Gesundheitsinformationen Teil einer größeren Organisation ist, muss das Clearinghouse Richtlinien und Verfahren einführen, die die elektronisch geschützten Gesundheitsinformationen des Clearinghouse vor unbefugtem Zugriff durch andere Teile der Organisation schützen.	iam-inline-policy-blocked-kms-Aktionen	Stellen Sie sicher, dass ein Benutzer, eine IAM-Rolle oder eine IAM-Gruppe (AWS Identity and Access Management) nicht über eine Inline-Richtlinie verfügt, die blockierte Aktionen für alle AWS Schlüssel des Key Management Service zulässt. AWS empfiehlt, verwaltete Richtlinien anstelle von Inline-Richtlinien zu verwenden. Verwaltete Richtlinien ermöglichen Wiederverwendbarkeit, Versionsverwaltung, Rollback und Delegierung der Berechtigungsverwaltung. Mit dieser Regel können Sie den blockedActionsPatterns Parameter festlegen. (Wert „AWS Bewährte grundlegende Sicherheitsmethoden“: kms:Decrypt, kms:ReEncryptFrom). Die

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.
164.308(a)(4)(ii)(A)	(A) Isolierung der Clearinghouse-Funktionen für Gesundheitsinformationen (erforderlich). Wenn ein Clearinghouse für Gesundheitsinformationen Teil einer größeren Organisation ist, muss das Clearinghouse Richtlinien und Verfahren einführen, die die elektronisch geschützten Gesundheitsinformationen des Clearinghouse vor unbefugtem Zugriff durch andere Teile der Organisation schützen.	iam-no-inline-policy-überprüfen	Stellen Sie sicher, dass ein Benutzer, eine IAM-Rolle oder eine IAM-Gruppe (AWS Identity and Access Management) nicht über eine Inline-Richtlinie zur Zugriffskontrolle auf Systeme und Ressourcen verfügt. AWS empfiehlt, verwaltete Richtlinien anstelle von Inline-Richtlinien zu verwenden. Verwaltete Richtlinien ermöglichen Wiederverwendbarkeit, Versionsverwaltung, Rollback und Delegierung der Berechtigungsverwaltung.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.308(a)(4)(ii)(A)	(A) Isolierung der Clearinghouse-Funktionen für Gesundheitsinformationen (erforderlich). Wenn ein Clearinghouse für Gesundheitsinformationen Teil einer größeren Organisation ist, muss das Clearinghouse Richtlinien und Verfahren einführen, die die elektronisch geschützten Gesundheitsinformationen des Clearinghouse vor unbefugtem Zugriff durch andere Teile der Organisation schützen.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) kann Ihnen dabei helfen, die Prinzipien der geringsten Rechte und der Aufgabentrennung in Zugriffsberechtigungen und Autorisierungen zu integrieren und so zu verhindern, dass Richtlinien „Effect“: „Allow“ mit „Action“: „*“ anstelle von „Resource“: „*“ enthalten. Wenn Benutzern mehr Rechte eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und der Aufgabentrennung verstoßen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.308(a)(4)(ii)(A)	(A) Isolierung der Clearinghouse-Funktionen für Gesundheitsinformationen (erforderlich). Wenn ein Clearinghouse für Gesundheitsinformationen Teil einer größeren Organisation ist, muss das Clearinghouse Richtlinien und Verfahren einführen, die die elektronisch geschützten Gesundheitsinformationen des Clearinghouse vor unbefugtem Zugriff durch andere Teile der Organisation schützen.	iam-root-access-key-überprüfen	Der Zugriff auf Systeme und Ressourcen kann gesteuert werden, indem überprüft wird, ob der Root-Benutzer keine Zugriffsschlüssel mit seiner AWS Identity and Access Management (IAM) -Rolle verknüpft hat. Stellen Sie sicher, dass die Root-Zugriffsschlüssel gelöscht werden. Erstellen und verwenden Sie stattdessen rollenbasierte Funktionen, AWS-Konten um das Prinzip der geringsten Funktionalität zu berücksichtigen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.308(a)(4)(ii)(A)	(A) Isolierung der Clearinghouse-Funktionen für Gesundheitsinformationen (erforderlich). Wenn ein Clearinghouse für Gesundheitsinformationen Teil einer größeren Organisation ist, muss das Clearinghouse Richtlinien und Verfahren einführen, die die elektronisch geschützten Gesundheitsinformationen des Clearinghouse vor unbefugtem Zugriff durch andere Teile der Organisation schützen.	iam-user-no-policies-überprüfen	Diese Regel stellt sicher, dass AWS Identity and Access Management (IAM)-Richtlinien nur Gruppen oder Rollen zugewiesen werden, um den Zugriff auf Systeme und Ressourcen zu kontrollieren. Die Zuweisung von Berechtigungen auf Gruppen- oder Rollenebene trägt dazu bei, die Wahrscheinlichkeit zu verringern, dass eine Identität übermäßige Berechtigungen erhält oder beibehält.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.308(a)(4)(ii)(A)	(A) Isolierung der Clearinghouse-Funktionen für Gesundheitsinformationen (erforderlich). Wenn ein Clearinghouse für Gesundheitsinformationen Teil einer größeren Organisation ist, muss das Clearinghouse Richtlinien und Verfahren einführen, die die elektronisch geschützten Gesundheitsinformationen des Clearinghouse vor unbefugtem Zugriff durch andere Teile der Organisation schützen.	iam-user-unused-credentials-überprüfen	AWS Identity and Access Management (IAM) kann Ihnen bei Zugriffsberechtigungen und Autorisierungen helfen, indem es nach IAM-Passwörtern und Zugriffsschlüsseln sucht, die für einen bestimmten Zeitraum nicht verwendet wurden. Wenn ungenutzte Anmeldeinformationen identifiziert werden, müssen Sie sie deaktivieren und/oder entfernen, da dies gegen das Prinzip der geringsten Berechtigung verstoßen könnte. Für diese Regel müssen Sie einen Wert für das maxCredentialUsage Alter festlegen (Standardkonfiguration: 90). Der tatsächliche Wert muss den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.308(a)(4)(ii)(A)	(A) Isolierung der Clearinghouse-Funktionen für Gesundheitsinformationen (erforderlich). Wenn ein Clearinghouse für Gesundheitsinformationen Teil einer größeren Organisation ist, muss das Clearinghouse Richtlinien und Verfahren einführen, die die elektronisch geschützten Gesundheitsinformationen des Clearinghouse vor unbefugtem Zugriff durch andere Teile der Organisation schützen.	iam-policy-no-statements-with-full-access	Stellen Sie sicher, dass IAM-Aktionen nur auf die benötigten Aktionen beschränkt sind. Wenn Benutzern mehr Rechte eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und der Aufgabentrennung verstoßen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.308(a)(4)(ii)(A)	(A) Isolierung der Clearinghouse-Funktionen für Gesundheitsinformationen (erforderlich). Wenn ein Clearinghouse für Gesundheitsinformationen Teil einer größeren Organisation ist, muss das Clearinghouse Richtlinien und Verfahren einführen, die die elektronisch geschützten Gesundheitsinformationen des Clearinghouse vor unbefugtem Zugriff durch andere Teile der Organisation schützen.	ec2- instance-profile-attached	EC2 Instanzprofile übergeben eine IAM-Rolle an eine Instanz EC2 . Das Anhängen eines Instance-Profils an Ihre Instances kann bei der Implementierung von geringsten Berechtigungen und der Berechtigungsverwaltung helfen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.308(a)(4)(ii)(A)	(A) Isolierung der Clearinghouse-Funktionen für Gesundheitsinformationen (erforderlich). Wenn ein Clearinghouse für Gesundheitsinformationen Teil einer größeren Organisation ist, muss das Clearinghouse Richtlinien und Verfahren einführen, die die elektronisch geschützten Gesundheitsinformationen des Clearinghouse vor unbefugtem Zugriff durch andere Teile der Organisation schützen.	dms-replication-not-public	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass auf DMS-Replikationsinstanzen nicht öffentlich zugegriffen werden kann. DMS-Replikations-Instances können vertrauliche Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.308(a)(4)(ii)(A)	(A) Isolierung der Clearinghouse-Funktionen für Gesundheitsinformationen (erforderlich). Wenn ein Clearinghouse für Gesundheitsinformationen Teil einer größeren Organisation ist, muss das Clearinghouse Richtlinien und Verfahren einführen, die die elektronisch geschützten Gesundheitsinformationen des Clearinghouse vor unbefugtem Zugriff durch andere Teile der Organisation schützen.	ebs-snapshot-public-restorable-überprüfen	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass EBS-Snapshots nicht öffentlich wiederherstellbar sind. EBS-Volume-Snapshots können vertrauliche Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.308(a)(4)(ii)(A)	(A) Isolierung der Clearinghouse-Funktionen für Gesundheitsinformationen (erforderlich). Wenn ein Clearinghouse für Gesundheitsinformationen Teil einer größeren Organisation ist, muss das Clearinghouse Richtlinien und Verfahren einführen, die die elektronisch geschützten Gesundheitsinformationen des Clearinghouse vor unbefugtem Zugriff durch andere Teile der Organisation schützen.	ec-2 instance-no-public-ip	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon Elastic Compute Cloud (Amazon EC2) - Instances nicht öffentlich zugänglich sind. EC2 Amazon-Instances können vertrauliche Informationen enthalten, und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.308(a)(4)(ii)(A)	(A) Isolierung der Clearinghouse-Funktionen für Gesundheitsinformationen (erforderlich). Wenn ein Clearinghouse für Gesundheitsinformationen Teil einer größeren Organisation ist, muss das Clearinghouse Richtlinien und Verfahren einführen, die die elektronisch geschützten Gesundheitsinformationen des Clearinghouse vor unbefugtem Zugriff durch andere Teile der Organisation schützen.	elasticsearch-in-vpc-only	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass sich Amazon OpenSearch OpenSearch Service (Service) - Domains innerhalb einer Amazon Virtual Private Cloud (Amazon VPC) befinden. Eine OpenSearch Service-Domain innerhalb einer Amazon VPC ermöglicht die sichere Kommunikation zwischen OpenSearch Service und anderen Services innerhalb der Amazon VPC, ohne dass ein Internet-Gateway, ein NAT-Gerät oder eine VPN-Verbindung erforderlich ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.308(a)(4)(ii)(A)	(A) Isolierung der Clearinghouse-Funktionen für Gesundheitsinformationen (erforderlich). Wenn ein Clearinghouse für Gesundheitsinformationen Teil einer größeren Organisation ist, muss das Clearinghouse Richtlinien und Verfahren einführen, die die elektronisch geschützten Gesundheitsinformationen des Clearinghouse vor unbefugtem Zugriff durch andere Teile der Organisation schützen.	emr-master-no-public-ip	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon EMR-Cluster-Masterknoten nicht öffentlich zugänglich sind. Amazon-EMR-Cluster-Hauptknoten können vertrauliche Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.308(a)(4)(ii)(A)	(A) Isolierung der Clearinghouse-Funktionen für Gesundheitsinformationen (erforderlich). Wenn ein Clearinghouse für Gesundheitsinformationen Teil einer größeren Organisation ist, muss das Clearinghouse Richtlinien und Verfahren einführen, die die elektronisch geschützten Gesundheitsinformationen des Clearinghouse vor unbefugtem Zugriff durch andere Teile der Organisation schützen.	ec-2 instances-in-vpc	Stellen Sie Amazon Elastic Compute Cloud (Amazon EC2) -Instances innerhalb einer Amazon Virtual Private Cloud (Amazon VPC) bereit, um eine sichere Kommunikation zwischen einer Instance und anderen Services innerhalb der Amazon VPC zu ermöglichen, ohne dass ein Internet-Gateway, ein NAT-Gerät oder eine VPN-Verbindung erforderlich ist. Der gesamte Datenverkehr bleibt sicher in der AWS Cloud. Domains, die sich innerhalb einer VPC befinden, verfügen aufgrund ihrer logischen Isolierung im Vergleich zu Domains mit öffentlichen Endpunkten über eine zusätzliche Sicherheitsebene. Weisen Sie EC2

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			Amazon-Instances einer Amazon-VPC zu, um den Zugriff ordnungsgemäß zu verwalten.
164.308(a)(4)(ii)(A)	(A) Isolierung der Clearinghouse-Funktionen für Gesundheitsinformationen (erforderlich). Wenn ein Clearinghouse für Gesundheitsinformationen Teil einer größeren Organisation ist, muss das Clearinghouse Richtlinien und Verfahren einführen, die die elektronisch geschützten Gesundheitsinformationen des Clearinghouse vor unbefugtem Zugriff durch andere Teile der Organisation schützen.	internet-gateway-authorized-vpc-nur	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Internet-Gateways nur mit autorisierter Amazon Virtual Private Cloud (Amazon VPC) verbunden sind. Internet-Gateways ermöglichen den bidirektionalen Internetzugang zur und von der Amazon VPC, was möglicher weise zu einem unbefugten Zugriff auf Amazon-VPC-Ressourcen führen kann.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.308(a)(4)(ii)(A)	(A) Isolierung der Clearinghouse-Funktionen für Gesundheitsinformationen (erforderlich). Wenn ein Clearinghouse für Gesundheitsinformationen Teil einer größeren Organisation ist, muss das Clearinghouse Richtlinien und Verfahren einführen, die die elektronisch geschützten Gesundheitsinformationen des Clearinghouse vor unbefugtem Zugriff durch andere Teile der Organisation schützen.	lambda-function-public-access-verboten	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass AWS Lambda-Funktionen nicht öffentlich zugänglich sind. Der öffentliche Zugriff kann möglicherweise die Verfügbarkeit von Ressourcen beeinträchtigen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.308(a)(4)(ii)(A)	(A) Isolierung der Clearinghouse-Funktionen für Gesundheitsinformationen (erforderlich). Wenn ein Clearinghouse für Gesundheitsinformationen Teil einer größeren Organisation ist, muss das Clearinghouse Richtlinien und Verfahren einführen, die die elektronisch geschützten Gesundheitsinformationen des Clearinghouse vor unbefugtem Zugriff durch andere Teile der Organisation schützen.	rds-instance-public-access-überprüfen	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Relational Database Service (Amazon RDS) -Instances nicht öffentlich sind. Amazon-RDS-Datenbank-Instances können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.308(a)(4)(ii)(A)	(A) Isolierung der Clearinghouse-Funktionen für Gesundheitsinformationen (erforderlich). Wenn ein Clearinghouse für Gesundheitsinformationen Teil einer größeren Organisation ist, muss das Clearinghouse Richtlinien und Verfahren einführen, die die elektronisch geschützten Gesundheitsinformationen des Clearinghouse vor unbefugtem Zugriff durch andere Teile der Organisation schützen.	rds-snapshots-public-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Relational Database Service (Amazon RDS) -Instances nicht öffentlich sind. Amazon-RDS-Datenbank-Instances können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.308(a)(4)(ii)(A)	(A) Isolierung der Clearinghouse-Funktionen für Gesundheitsinformationen (erforderlich). Wenn ein Clearinghouse für Gesundheitsinformationen Teil einer größeren Organisation ist, muss das Clearinghouse Richtlinien und Verfahren einführen, die die elektronisch geschützten Gesundheitsinformationen des Clearinghouse vor unbefugtem Zugriff durch andere Teile der Organisation schützen.	redshift-cluster-public-access-überprüfen	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Redshift Redshift-Cluster nicht öffentlich sind. Amazon-Redshift-Cluster können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.308(a)(4)(ii)(A)	(A) Isolierung der Clearinghouse-Funktionen für Gesundheitsinformationen (erforderlich). Wenn ein Clearinghouse für Gesundheitsinformationen Teil einer größeren Organisation ist, muss das Clearinghouse Richtlinien und Verfahren einführen, die die elektronisch geschützten Gesundheitsinformationen des Clearinghouse vor unbefugtem Zugriff durch andere Teile der Organisation schützen.	s3- -Block-periodisch account-level-public-access	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Simple Storage Service (Amazon S3) -Buckets nicht öffentlich zugänglich sind. Diese Regel trägt dazu bei, sensible Daten vor unbefugten Remote-Benutzern zu schützen, indem sie den öffentlichen Zugriff verhindert. Mit dieser Regel können Sie optional die Parameter ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) und restrictPublicBuckets Parameter (Config Default: True) festlegen. Die tatsächlichen Werte müssen den Richtlini

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			en Ihrer Organisation entsprechen.
164.308(a)(4)(ii)(A)	(A) Isolierung der Clearinghouse-Funktionen für Gesundheitsinformationen (erforderlich). Wenn ein Clearinghouse für Gesundheitsinformationen Teil einer größeren Organisation ist, muss das Clearinghouse Richtlinien und Verfahren einführen, die die elektronisch geschützten Gesundheitsinformationen des Clearinghouse vor unbefugtem Zugriff durch andere Teile der Organisation schützen.	s3- bucket-public-read-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie nur autorisierten Benutzern, Prozessen und Geräten Zugriff auf Amazon Simple Storage Service (Amazon S3) - Buckets gewähren. Die Verwaltung des Zugriffs sollte mit der Klassifizierung der Daten übereinstimmen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.308(a)(4)(ii)(A)	(A) Isolierung der Clearinghouse-Funktionen für Gesundheitsinformationen (erforderlich). Wenn ein Clearinghouse für Gesundheitsinformationen Teil einer größeren Organisation ist, muss das Clearinghouse Richtlinien und Verfahren einführen, die die elektronisch geschützten Gesundheitsinformationen des Clearinghouse vor unbefugtem Zugriff durch andere Teile der Organisation schützen.	s3- bucket-public-write-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie nur autorisierten Benutzern, Prozessen und Geräten Zugriff auf Amazon Simple Storage Service (Amazon S3) - Buckets gewähren. Die Verwaltung des Zugriffs sollte mit der Klassifizierung der Daten übereinstimmen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.308(a)(4)(ii)(A)	(A) Isolierung der Clearinghouse-Funktionen für Gesundheitsinformationen (erforderlich). Wenn ein Clearinghouse für Gesundheitsinformationen Teil einer größeren Organisation ist, muss das Clearinghouse Richtlinien und Verfahren einführen, die die elektronisch geschützten Gesundheitsinformationen des Clearinghouse vor unbefugtem Zugriff durch andere Teile der Organisation schützen.	sagemaker-notebook-no-direct-Internetzugang	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass SageMaker Amazon-Notebooks keinen direkten Internetzugang zulassen. Indem Sie direkten Internetzugang blockieren, vermeiden Sie, dass unbefugte Benutzer auf sensible Daten zugreifen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.308(a)(4)(ii)(A)	(A) Isolierung der Clearinghouse-Funktionen für Gesundheitsinformationen (erforderlich). Wenn ein Clearinghouse für Gesundheitsinformationen Teil einer größeren Organisation ist, muss das Clearinghouse Richtlinien und Verfahren einführen, die die elektronisch geschützten Gesundheitsinformationen des Clearinghouse vor unbefugtem Zugriff durch andere Teile der Organisation schützen.	subnet-auto-assign-public-ip-deaktiviert	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon Virtual Private Cloud (VPC) -Subnetzen nicht automatisch eine öffentliche IP-Adresse zugewiesen wird. Amazon Elastic Compute Cloud (EC2) -Instances, die in Subnetzen gestartet werden, in denen dieses Attribut aktiviert ist, haben ihrer primären Netzwerkschnittstelle eine öffentliche IP-Adresse zugewiesen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.308(a)(4)(ii)(A)	(A) Isolierung der Clearinghouse-Funktionen für Gesundheitsinformationen (erforderlich). Wenn ein Clearinghouse für Gesundheitsinformationen Teil einer größeren Organisation ist, muss das Clearinghouse Richtlinien und Verfahren einführen, die die elektronisch geschützten Gesundheitsinformationen des Clearinghouse vor unbefugtem Zugriff durch andere Teile der Organisation schützen.	ecs-task-definition-user-for-host-mode-check	Wenn für eine Aufgabendefinition erhöhte Berechtigungen gelten, liegt das daran, dass der Kunde diesen Konfigurationen ausdrücklich zugestimmt hat. Diese Kontrolle prüft, ob eine unerwartete Berechtigungseskalation vorliegt, wenn für eine Aufgabendefinition das Host-Netzwerk aktiviert ist, die Kunden aber keine erhöhten Berechtigungen aktiviert haben.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.308(a)(4)(ii)(A)	(A) Isolierung der Clearinghouse-Funktionen für Gesundheitsinformationen (erforderlich). Wenn ein Clearinghouse für Gesundheitsinformationen Teil einer größeren Organisation ist, muss das Clearinghouse Richtlinien und Verfahren einführen, die die elektronisch geschützten Gesundheitsinformationen des Clearinghouse vor unbefugtem Zugriff durch andere Teile der Organisation schützen.	codebuild-project-envvar-awscred-überprüfen	Stellen Sie sicher, dass die Anmeldeinformationen AWS_ACCESS_KEY_ID AWS_SECRET_ACCESS_KEY nicht in AWS Codebuild-Projektumgebungen vorhanden sind. Speichern Sie diese Variablen nicht als Klartext. Das Speichern dieser Variablen als Klartext bewirkt eine unbeabsichtigte Offenlegung von Daten sowie unberechtigte Zugriffe.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.308(a)(4)(ii)(A)	(A) Isolierung der Clearinghouse-Funktionen für Gesundheitsinformationen (erforderlich). Wenn ein Clearinghouse für Gesundheitsinformationen Teil einer größeren Organisation ist, muss das Clearinghouse Richtlinien und Verfahren einführen, die die elektronisch geschützten Gesundheitsinformationen des Clearinghouse vor unbefugtem Zugriff durch andere Teile der Organisation schützen.	codebuild-project-source-repo-URL-Prüfung	Stellen Sie sicher, dass die URL des Quell-Repositorys GitHub oder des Bitbucket-Quell-Repositorys keine persönlichen Zugriffstoken oder Anmeldeinformationen in Codebuild-Projektumgebungen enthält. AWS Verwende OAuth anstelle von persönlichen Zugriffstoken oder Anmeldedaten die Autorisierung für den Zugriff auf GitHub Bitbucket-Repositorys.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.308(a)(4)(ii)(A)	(A) Isolierung der Clearinghouse-Funktionen für Gesundheitsinformationen (erforderlich). Wenn ein Clearinghouse für Gesundheitsinformationen Teil einer größeren Organisation ist, muss das Clearinghouse Richtlinien und Verfahren einführen, die die elektronisch geschützten Gesundheitsinformationen des Clearinghouse vor unbefugtem Zugriff durch andere Teile der Organisation schützen.	restricted-common-ports	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass gemeinsame Ports für Amazon Elastic Compute Cloud (Amazon EC2) -Sicherheitsgruppen eingeschränkt sind. Wenn der Zugriff auf Ports nicht auf vertrauenswürdige Quellen beschränkt wird, kann dies zu Angriffen auf die Verfügbarkeit, Integrität und Vertraulichkeit von Systemen führen. Mit dieser Regel können Sie optional die Parameter blockedPort1–blockedPort5 festlegen (Standardkonfigurationen: 20, 21, 3389, 3306, 4333). Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.308(a)(4)(ii)(A)	(A) Isolierung der Clearinghouse-Funktionen für Gesundheitsinformationen (erforderlich). Wenn ein Clearinghouse für Gesundheitsinformationen Teil einer größeren Organisation ist, muss das Clearinghouse Richtlinien und Verfahren einführen, die die elektronisch geschützten Gesundheitsinformationen des Clearinghouse vor unbefugtem Zugriff durch andere Teile der Organisation schützen.	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) Security Groups können bei der Verwaltung des Netzwerkzugriffs helfen, indem sie eine statusbehaftete Filterung von eingehendem und ausgehendem Netzwerkverkehr zu Ressourcen bereitstellen. AWS Wenn Sie eingehenden (oder entfernten) Datenverkehr von 0.0.0.0/0 bis Port 22 auf Ihren Ressourcen nicht zulassen, können Sie den Remote-Zugriff einschränken.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.308(a)(4)(ii)(A)	(A) Isolierung der Clearinghouse-Funktionen für Gesundheitsinformationen (erforderlich). Wenn ein Clearinghouse für Gesundheitsinformationen Teil einer größeren Organisation ist, muss das Clearinghouse Richtlinien und Verfahren einführen, die die elektronisch geschützten Gesundheitsinformationen des Clearinghouse vor unbefugtem Zugriff durch andere Teile der Organisation schützen.	autoscaling-launch-config-public-ip-deaktiviert	Wenn Sie Ihre Netzwerkschnittstellen mit einer öffentlichen IP-Adresse konfigurieren, sind die diesen Netzwerkschnittstellen zugehörigen Ressourcen über das Internet erreichbar. EC2 Ressourcen sollten nicht öffentlich zugänglich sein, da dies einen unbeabsichtigten Zugriff auf Ihre Anwendungen oder Server ermöglichen kann.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.308(a)(4)(ii)(A)	(A) Isolierung der Clearinghouse-Funktionen für Gesundheitsinformationen (erforderlich). Wenn ein Clearinghouse für Gesundheitsinformationen Teil einer größeren Organisation ist, muss das Clearinghouse Richtlinien und Verfahren einführen, die die elektronisch geschützten Gesundheitsinformationen des Clearinghouse vor unbefugtem Zugriff durch andere Teile der Organisation schützen.	ecs-containers-readonly-access	Die Aktivierung des schreibgeschützten Zugriffs auf Amazon Elastic Container Service (ECS)-Container kann dazu beitragen, das Prinzip der geringsten Berechtigung einzuhalten. Diese Option kann Angriffsvektoren reduzieren, da das Dateisystem der Container-Instance nur geändert werden kann, wenn es über ausdrückliche Lese- und Schreibberechtigungen verfügt.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.308(a)(4)(ii)(A)	(A) Isolierung der Clearinghouse-Funktionen für Gesundheitsinformationen (erforderlich). Wenn ein Clearinghouse für Gesundheitsinformationen Teil einer größeren Organisation ist, muss das Clearinghouse Richtlinien und Verfahren einführen, die die elektronisch geschützten Gesundheitsinformationen des Clearinghouse vor unbefugtem Zugriff durch andere Teile der Organisation schützen.	ssm-document-not-public	Stellen Sie sicher, dass AWS Systems Manager (SSM) - Dokumente nicht öffentlich sind, da dies einen unbeabsichtigten Zugriff auf Ihre SSM-Dokumente ermöglichen kann. Ein öffentliches SSM-Dokument kann Informationen über Ihr Konto, Ihre Ressourcen und internen Prozesse preisgeben.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.308(a)(4)(ii)(A)	(A) Isolierung der Clearinghouse-Funktionen für Gesundheitsinformationen (erforderlich). Wenn ein Clearinghouse für Gesundheitsinformationen Teil einer größeren Organisation ist, muss das Clearinghouse Richtlinien und Verfahren einführen, die die elektronisch geschützten Gesundheitsinformationen des Clearinghouse vor unbefugtem Zugriff durch andere Teile der Organisation schützen.	s-3 bucket-acl-prohibited	Diese Regel prüft, ob Access Control Lists (ACLs) für die Zugriffskontrolle auf Amazon S3 S3-Buckets verwendet werden. ACLs sind veraltete Zugriffskontrollmechanismen für Amazon S3 S3-Buckets, die älter sind als AWS Identity and Access Management (IAM). Stattdessen empfiehlt es sich ACLs, IAM-Richtlinien oder S3-Bucket-Richtlinien zu verwenden, um den Zugriff auf Ihre S3-Buckets einfacher zu verwalten.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.308(a)(4)(ii)(A)	(A) Isolierung der Clearinghouse-Funktionen für Gesundheitsinformationen (erforderlich). Wenn ein Clearinghouse für Gesundheitsinformationen Teil einer größeren Organisation ist, muss das Clearinghouse Richtlinien und Verfahren einführen, die die elektronisch geschützten Gesundheitsinformationen des Clearinghouse vor unbefugtem Zugriff durch andere Teile der Organisation schützen.	opensearch-in-vpc-only	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass sich Amazon OpenSearch Service-Domains innerhalb einer Amazon Virtual Private Cloud (Amazon VPC) befinden. Eine Amazon OpenSearch Service-Domain innerhalb einer Amazon VPC ermöglicht die sichere Kommunikation zwischen Amazon OpenSearch Service und anderen Services innerhalb der Amazon VPC, ohne dass ein Internet-Gateway, ein NAT-Gerät oder eine VPN-Verbindung erforderlich ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.308(a)(4)(ii)(B)	(B) Zugriffsberechtigung (adressierbar). Implementieren Sie Richtlinien und Verfahren für die Gewährung des Zugriffs auf elektronisch geschützte Gesundheitsinformationen, z. B. durch den Zugriff auf eine Workstation, einen Vorgang, ein Programm, einen Prozess oder einen anderen Mechanismus.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) kann Ihnen dabei helfen, die Prinzipien der geringsten Rechte und der Aufgabentrennung in Zugriffsberechtigungen und Autorisierungen zu integrieren und so zu verhindern, dass Richtlinien „Effect“: „Allow“ mit „Action“: „*“ anstelle von „Resource“: „*“ enthalten. Wenn Benutzern mehr Rechte eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und der Aufgabentrennung verstoßen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.308(a)(4)(ii)(B)	(B) Zugriffsberechtigung (adressierbar). Implementieren Sie Richtlinien und Verfahren für die Gewährung des Zugriffs auf elektronisch geschützte Gesundheitsinformationen, z. B. durch den Zugriff auf eine Workstation, einen Vorgang, ein Programm, einen Prozess oder einen anderen Mechanismus.	iam-user-no-policies-überprüfen	Diese Regel stellt sicher, dass AWS Identity and Access Management (IAM) -Richtlinien nur Gruppen oder Rollen zugewiesen werden, um den Zugriff auf Systeme und Ressourcen zu kontrollieren. Die Zuweisung von Berechtigungen auf Gruppen- oder Rollenebene trägt dazu bei, die Wahrscheinlichkeit zu verringern, dass eine Identität übermäßige Berechtigungen erhält oder beibehält.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.308(a)(4)(ii)(B)	(B) Zugriffsberechtigung (adressierbar). Implementieren Sie Richtlinien und Verfahren für die Gewährung des Zugriffs auf elektronisch geschützte Gesundheitsinformationen, z. B. durch den Zugriff auf eine Workstation, einen Vorgang, ein Programm, einen Prozess oder einen anderen Mechanismus.	access-keys-rotated	Die Anmeldeinformationen für autorisierte Geräte, Benutzer und Prozesse werden geprüft, indem sichergestellt wird, dass die IAM-Zugriffsschlüssel entsprechend den Vorgaben der Unternehmensrichtlinie rotiert werden. Das regelmäßige Ändern der Zugriffsschlüssel ist eine bewährte Sicherheitsmethode. Es verkürzt den Zeitraum, in dem ein Zugriffsschlüssel aktiv ist, und reduziert die Auswirkungen auf das Unternehmen, wenn die Schlüssel kompromittiert werden. Diese Regel erfordert einen Wert für die Zugriffsschlüssel-Rotation (Standard konfiguration: 90). Der tatsächliche Wert muss den Richtlini

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			en Ihrer Organisation entsprechen.
164.308(a)(4)(ii)(B)	(B) Zugriffsberechtigung (adressierbar). Implementieren Sie Richtlinien und Verfahren für die Gewährung des Zugriffs auf elektronisch geschützte Gesundheitsinformationen, z. B. durch den Zugriff auf eine Workstation, einen Vorgang, ein Programm, einen Prozess oder einen anderen Mechanismus.	iam-root-access-key-überprüfen	Der Zugriff auf Systeme und Ressourcen kann gesteuert werden, indem überprüft wird, ob der Root-Benutzer keine Zugriffsschlüssel mit seiner AWS Identity and Access Management (IAM) -Rolle verknüpft hat. Stellen Sie sicher, dass die Root-Zugriffsschlüssel gelöscht werden. Erstellen und verwenden Sie stattdessen rollenbasierte Funktionen, AWS-Konten um das Prinzip der geringsten Funktionalität zu berücksichtigen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.308(a)(4)(ii)(B)	(B) Zugriffsberechtigung (adressierbar). Implementieren Sie Richtlinien und Verfahren für die Gewährung des Zugriffs auf elektronisch geschützte Gesundheitsinformationen, z. B. durch den Zugriff auf eine Workstation, einen Vorgang, ein Programm, einen Prozess oder einen anderen Mechanismus.	iam-password-policy	Die Identitäten und Anmeldeinformationen werden auf der Grundlage einer organisatorischen IAM-Passwortrichtlinie ausgestellt, verwaltet und verifiziert. Sie erfüllen oder übertreffen die Anforderungen von NIST SP 800-63 und dem Standard „Best Practices“ von AWS Foundational Security für die Passwortstärke. Mit dieser Regel können Sie optional RequireUppercaseCharacters (Wert für AWS grundlegende Sicherheitsbewährte Methoden: wahr), RequireLowercaseCharacters (Wert für bewährte Methoden für AWS grundlegende Sicherheit: wahr), RequireSymbols (Wert für bewährte Methoden für AWS grundlegende Sicherheit:

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			wahr), RequireNumbers (Wert für bewährte Methoden für AWS grundlegende Sicherheit: wahr), MinimumPasswordLength (Wert für bewährte Methoden für AWS grundlegende Sicherheit: 14), PasswordReusePrevention (Wert für bewährte Methoden für AWS grundlegende Sicherheit: 24) und MaxPasswordAge (Wert für bewährte Methoden für AWS grundlegende Sicherheit: 90) für Ihr IAM festlegen Kennwortrichtlinie. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.308(a)(4)(ii)(B)	(B) Zugriffsberechtigung (adressierbar). Implementieren Sie Richtlinien und Verfahren für die Gewährung des Zugriffs auf elektronisch geschützte Gesundheitsinformationen, z. B. durch den Zugriff auf eine Workstation, einen Vorgang, ein Programm, einen Prozess oder einen anderen Mechanismus.	iam-user-unused-credentials-überprüfen	AWS Identity and Access Management (IAM) kann Ihnen bei Zugriffsberechtigungen und Autorisierungen helfen, indem es nach IAM-Passwörtern und Zugriffsschlüsseln sucht, die für einen bestimmten Zeitraum nicht verwendet wurden. Wenn ungenutzte Anmeldeinformationen identifiziert werden, müssen Sie sie deaktivieren und/oder entfernen, da dies gegen das Prinzip der geringsten Berechtigung verstoßen könnte. Für diese Regel müssen Sie einen Wert für das maxCredentialUsage Alter festlegen (Standardkonfiguration: 90). Der tatsächliche Wert muss den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.308(a)(4)(ii)(B)	(B) Zugriffsberechtigung (adressierbar). Implementieren Sie Richtlinien und Verfahren für die Gewährung des Zugriffs auf elektronisch geschützte Gesundheitsinformationen, z. B. durch den Zugriff auf eine Workstation, einen Vorgang, ein Programm, einen Prozess oder einen anderen Mechanismus.	secretsmanager-rotation-enabled-check	Diese Regel stellt sicher, dass bei AWS Secrets Manager Manager-Geheimnissen die Rotation aktiviert ist. Die regelmäßige Rotation von Secrets kann den Zeitraum verkürzen, in dem ein Secret aktiv ist, und möglicherweise die Auswirkungen auf das Unternehmen verringern, falls das Secret kompromittiert wird.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.308(a)(4)(ii)(B)	(B) Zugriffsberechtigung (adressierbar). Implementieren Sie Richtlinien und Verfahren für die Gewährung des Zugriffs auf elektronisch geschützte Gesundheitsinformationen, z. B. durch den Zugriff auf eine Workstation, einen Vorgang, ein Programm, einen Prozess oder einen anderen Mechanismus.	emr-kerberos-enabled	Die Zugriffsberechtigungen und -autorisierungen können verwaltet und nach den Prinzipien der geringsten Berechtigung und Aufgabentrennung integriert werden, indem Kerberos für Amazon-EMR-Cluster aktiviert wird. In Kerberos werden Services und Benutzer, die sich authentifizieren müssen, als Prinzipale bezeichnet. Prinzipale befinden sich in einem Kerberos-Bereich. Innerhalb dieses Bereichs wird ein Kerberos-Server als Key Distribution Center (KDC) bezeichnet. Über diesen Server können sich Prinzipale authentifizieren. Die Authentifizierung im KDC erfolgt durch die Ausstellung von Authentif

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			izierungstickets. Das KDC unterhält eine Datenbank der Prinzipale in seinem Bereich mit ihren Passwörtern und anderen administr ativen Informationen zu jedem Prinzipal.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.308(a)(4)(ii)(B)	(B) Zugriffsberechtigung (adressierbar). Implementieren Sie Richtlinien und Verfahren für die Gewährung des Zugriffs auf elektronisch geschützte Gesundheitsinformationen, z. B. durch den Zugriff auf eine Workstation, einen Vorgang, ein Programm, einen Prozess oder einen anderen Mechanismus.	iam-customer-policy-blocked-kms-Aktionen	AWS Identity and Access Management (IAM) kann Ihnen helfen, die Prinzipien der geringsten Rechte und der Aufgabentrennung in Zugriffsberechtigungen und Autorisierungen zu integrieren und so zu verhindern, dass Richtlinien blockierte Aktionen für alle AWS Schlüssel des Key Management Service enthalten. Wenn Benutzer mehr Rechte haben, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und Aufgabentrennung verstoßen. Mit dieser Regel können Sie den Parameter festlegen. blockedActionsPatterns (Wert „AWS Bewährte grundlegende Sicherheitsmethoden“: kms:

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			Decrypt, kms:ReEncryptFrom). Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.308(a)(4)(ii)(B)	(B) Zugriffsberechtigung (adressierbar). Implementieren Sie Richtlinien und Verfahren für die Gewährung des Zugriffs auf elektronisch geschützte Gesundheitsinformationen, z. B. durch den Zugriff auf eine Workstation, einen Vorgang, ein Programm, einen Prozess oder einen anderen Mechanismus.	iam-inline-policy-blocked-kms-Aktionen	Stellen Sie sicher, dass ein Benutzer, eine IAM-Rolle oder eine IAM-Gruppe (AWS Identity and Access Management) nicht über eine Inline-Richtlinie verfügt, die blockierte Aktionen für alle AWS Schlüssel des Key Management Service zulässt. AWS empfiehlt, verwaltete Richtlinien anstelle von Inline-Richtlinien zu verwenden. Verwaltete Richtlinien ermöglichen Wiederverwendbarkeit, Versionsverwaltung, Rollback und Delegierung der Berechtigungsverwaltung. Mit dieser Regel können Sie den blockedActionsPatterns Parameter festlegen. (Wert „AWS Bewährte grundlegende Sicherheitsmethoden“: kms:Decrypt, kms:ReEncryptFrom). Die

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.
164.308(a)(4)(ii)(B)	(B) Zugriffsberechtigung (adressierbar). Implementieren Sie Richtlinien und Verfahren für die Gewährung des Zugriffs auf elektronisch geschützte Gesundheitsinformationen, z. B. durch den Zugriff auf eine Workstation, einen Vorgang, ein Programm, einen Prozess oder einen anderen Mechanismus.	iam-no-inline-policy-überprüfen	Stellen Sie sicher, dass ein Benutzer, eine IAM-Rolle oder eine IAM-Gruppe (AWS Identity and Access Management) nicht über eine Inline-Richtlinie zur Zugriffskontrolle auf Systeme und Ressourcen verfügt. AWS empfiehlt, verwaltete Richtlinien anstelle von Inline-Richtlinien zu verwenden. Verwaltete Richtlinien ermöglichen Wiederverwendbarkeit, Versionsverwaltung, Rollback und Delegierung der Berechtigungsverwaltung.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.308(a)(4)(ii)(B)	(B) Zugriffsberechtigung (adressierbar). Implementieren Sie Richtlinien und Verfahren für die Gewährung des Zugriffs auf elektronisch geschützte Gesundheitsinformationen, z. B. durch den Zugriff auf eine Workstation, einen Vorgang, ein Programm, einen Prozess oder einen anderen Mechanismus.	iam-user-mfa-enabled	Aktivieren Sie diese Regel, um den Zugriff auf Ressourcen in der AWS Cloud einzuschränken. Diese Regel sorgt dafür, dass die Multi-Faktor-Authentifizierung (MFA) für alle Benutzer aktiviert ist. MFA sorgt für eine weitere Schutzebene zusätzlich zu den Anmeldeinformationen. Reduzieren Sie Fälle von kompromittierten Konten, indem Sie MFA für Benutzer vorschreiben.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.308(a)(4)(ii)(B)	(B) Zugriffsberechtigung (adressierbar). Implementieren Sie Richtlinien und Verfahren für die Gewährung des Zugriffs auf elektronisch geschützte Gesundheitsinformationen, z. B. durch den Zugriff auf eine Workstation, einen Vorgang, ein Programm, einen Prozess oder einen anderen Mechanismus.	iam-policy-no-statements-with-full-access	Stellen Sie sicher, dass IAM-Aktionen nur auf die benötigten Aktionen beschränkt sind. Wenn Benutzern mehr Rechte eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und der Aufgabentrennung verstoßen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.308(a)(4)(ii)(B)	(B) Zugriffsberechtigung (adressierbar). Implementieren Sie Richtlinien und Verfahren für die Gewährung des Zugriffs auf elektronisch geschützte Gesundheitsinformationen, z. B. durch den Zugriff auf eine Workstation, einen Vorgang, ein Programm, einen Prozess oder einen anderen Mechanismus.	ec-2 instance-profile-attached	EC2 Instanzprofile übergeben eine IAM-Rolle an eine Instanz EC2 . Das Anhängen eines Instance-Profils an Ihre Instances kann bei der Implementierung von geringsten Berechtigungen und der Berechtigungsverwaltung helfen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.308(a)(4)(ii)(B)	(B) Zugriffsberechtigung (adressierbar). Implementieren Sie Richtlinien und Verfahren für die Gewährung des Zugriffs auf elektronisch geschützte Gesundheitsinformationen, z. B. durch den Zugriff auf eine Workstation, einen Vorgang, ein Programm, einen Prozess oder einen anderen Mechanismus.	restricted-common-ports	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass gemeinsame Ports für Amazon Elastic Compute Cloud (Amazon EC2) -Sicherheitsgruppen eingeschränkt sind. Wenn der Zugriff auf Ports nicht auf vertrauenswürdige Quellen beschränkt wird, kann dies zu Angriffen auf die Verfügbarkeit, Integrität und Vertraulichkeit von Systemen führen. Mit dieser Regel können Sie optional die Parameter blockedPort1–blockedPort5 festlegen (Standardkonfigurationen: 20, 21, 3389, 3306, 4333). Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.308(a)(4)(ii)(B)	(B) Zugriffsberechtigung (adressierbar). Implementieren Sie Richtlinien und Verfahren für die Gewährung des Zugriffs auf elektronisch geschützte Gesundheitsinformationen, z. B. durch den Zugriff auf eine Workstation, einen Vorgang, ein Programm, einen Prozess oder einen anderen Mechanismus.	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) Security Groups können bei der Verwaltung des Netzwerkzugriffs helfen, indem sie eine statusbehaftete Filterung von eingehendem und ausgehendem Netzwerkverkehr zu Ressourcen bereitstellen. AWS Wenn Sie eingehenden (oder entfernten) Datenverkehr von 0.0.0.0/0 bis Port 22 auf Ihren Ressourcen nicht zulassen, können Sie den Remote-Zugriff einschränken.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.308(a)(4)(ii)(B)	(B) Zugriffsberechtigung (adressierbar). Implementieren Sie Richtlinien und Verfahren für die Gewährung des Zugriffs auf elektronisch geschützte Gesundheitsinformationen, z. B. durch den Zugriff auf eine Workstation, einen Vorgang, ein Programm, einen Prozess oder einen anderen Mechanismus.	ssm-document-not-public	Stellen Sie sicher, dass AWS Systems Manager (SSM) - Dokumente nicht öffentlich sind, da dies einen unbeabsichtigten Zugriff auf Ihre SSM-Dokumente ermöglichen kann. Ein öffentliches SSM-Dokument kann Informationen über Ihr Konto, Ihre Ressourcen und internen Prozesse preisgeben.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.308(a)(4)(ii)(B)	(B) Zugriffsberechtigung (adressierbar). Implementieren Sie Richtlinien und Verfahren für die Gewährung des Zugriffs auf elektronisch geschützte Gesundheitsinformationen, z. B. durch den Zugriff auf eine Workstation, einen Vorgang, ein Programm, einen Prozess oder einen anderen Mechanismus.	ecs-containers-readonly-access	Die Aktivierung des schreibgeschützten Zugriffs auf Amazon Elastic Container Service (ECS)-Container kann dazu beitragen, das Prinzip der geringsten Berechtigung einzuhalten. Diese Option kann Angriffsvektoren reduzieren, da das Dateisystem der Container-Instance nur geändert werden kann, wenn es über ausdrückliche Lese- und Schreibberechtigungen verfügt.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.308(a)(4)(ii)(B)	(B) Zugriffsberechtigung (adressierbar). Implementieren Sie Richtlinien und Verfahren für die Gewährung des Zugriffs auf elektronisch geschützte Gesundheitsinformationen, z. B. durch den Zugriff auf eine Workstation, einen Vorgang, ein Programm, einen Prozess oder einen anderen Mechanismus.	s-3 bucket-acl-prohibited	Diese Regel prüft, ob Access Control Lists (ACLs) für die Zugriffskontrolle auf Amazon S3 S3-Buckets verwendet werden. ACLs sind veraltete Zugriffskontrollmechanismen für Amazon S3 S3-Buckets, die älter sind als AWS Identity and Access Management (IAM). Stattdessen empfiehlt es sich ACLs, IAM-Richtlinien oder S3-Bucket-Richtlinien zu verwenden, um den Zugriff auf Ihre S3-Buckets einfacher zu verwalten.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.308(a)(4)(ii)(C)	(C) Einrichtung und Änderung des Zugriffs (adressierbar). Implementieren Sie Richtlinien und Verfahren, mit denen auf der Grundlage der Zugriffsberechtigungsrichtlinien der Entität die Zugriffsrechte von Benutzern auf eine Workstation, einen Vorgang, ein Programm oder einen Prozess festgelegt, dokumentiert, überprüft und geändert werden.	ec2-imdsv2-check	Stellen Sie sicher, dass die Methode Instance Metadata Service Version 2 (IMDSv2) aktiviert ist, um den Zugriff auf und die Kontrolle der Amazon Elastic Compute Cloud (Amazon EC2) - Instance-Metadaten zu schützen. Die IMDSv2 Methode verwendet sitzungsbasierte Kontrollen. Mit können Kontrollen implementiert werden IMDSv2, um Änderungen an Instanzmetadaten einzuschränken.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.308(a)(4)(ii)(C)	(C) Einrichtung und Änderung des Zugriffs (adressierbar). Implementieren Sie Richtlinien und Verfahren, mit denen auf der Grundlage der Zugriffsberechtigungsrichtlinien der Entität die Zugriffsrechte von Benutzern auf eine Workstation, einen Vorgang, ein Programm oder einen Prozess festgelegt, dokumentiert, überprüft und geändert werden.	emr-kerberos-enabled	Die Zugriffsberechtigungen und -autorisierungen können verwaltet und nach den Prinzipien der geringsten Berechtigung und Aufgabentrennung integriert werden, indem Kerberos für Amazon-EMR-Cluster aktiviert wird. In Kerberos werden Services und Benutzer, die sich authentifizieren müssen, als Prinzipale bezeichnet. Prinzipale befinden sich in einem Kerberos-Bereich. Innerhalb dieses Bereichs wird ein Kerberos-Server als Key Distribution Center (KDC) bezeichnet. Über diesen Server können sich Prinzipale authentifizieren. Die Authentifizierung im KDC erfolgt durch die Ausstellung von Authentif

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			izierungstickets. Das KDC unterhält eine Datenbank der Prinzipale in seinem Bereich mit ihren Passwörtern und anderen administr ativen Informationen zu jedem Prinzipal.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.308(a)(4)(ii)(C)	(C) Einrichtung und Änderung des Zugriffs (adressierbar). Implementieren Sie Richtlinien und Verfahren, mit denen auf der Grundlage der Zugriffsberechtigungsrichtlinien der Entität die Zugriffsrechte von Benutzern auf eine Workstation, einen Vorgang, ein Programm oder einen Prozess festgelegt, dokumentiert, überprüft und geändert werden.	iam-customer-policy-blocked-kms-Aktionen	AWS Identity and Access Management (IAM) kann Ihnen helfen, die Prinzipien der geringsten Rechte und der Aufgabentrennung in Zugriffsberechtigungen und Autorisierungen zu integrieren und so zu verhindern, dass Richtlinien blockierte Aktionen für alle AWS Schlüssel des Key Management Service enthalten. Wenn Benutzer mehr Rechte haben, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und Aufgabentrennung verstoßen. Mit dieser Regel können Sie den Parameter festlegen. blockedActionsPatterns (Wert „AWS Bewährte grundlegende Sicherheitsmethoden“: kms:

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			Decrypt, kms:ReEncryptFrom). Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.308(a)(4)(ii)(C)	(C) Einrichtung und Änderung des Zugriffs (adressierbar). Implementieren Sie Richtlinien und Verfahren, mit denen auf der Grundlage der Zugriffsberechtigungsrichtlinien der Entität die Zugriffsrechte von Benutzern auf eine Workstation, einen Vorgang, ein Programm oder einen Prozess festgelegt, dokumentiert, überprüft und geändert werden.	iam-inline-policy-blocked-kms-Aktionen	Stellen Sie sicher, dass ein Benutzer, eine IAM-Rolle oder eine IAM-Gruppe (AWS Identity and Access Management) nicht über eine Inline-Richtlinie verfügt, die blockierte Aktionen für alle AWS Schlüssel des Key Management Service zulässt. AWS empfiehlt, verwaltete Richtlinien anstelle von Inline-Richtlinien zu verwenden. Verwaltete Richtlinien ermöglichen Wiederverwendbarkeit, Versionsverwaltung, Rollback und Delegierung der Berechtigungsverwaltung. Mit dieser Regel können Sie den blockedActionsPatterns Parameter festlegen. (Wert „AWS Bewährte grundlegende Sicherheitsmethoden“: kms:Decrypt, kms:ReEncryptFrom). Die

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.
164.308(a)(4)(ii)(C)	(C) Einrichtung und Änderung des Zugriffs (adressierbar). Implementieren Sie Richtlinien und Verfahren, mit denen auf der Grundlage der Zugriffsberechtigungsrichtlinien der Entität die Zugriffsrechte von Benutzern auf eine Workstation, einen Vorgang, ein Programm oder einen Prozess festgelegt, dokumentiert, überprüft und geändert werden.	iam-no-inline-policy-überprüfen	Stellen Sie sicher, dass ein Benutzer, eine IAM-Rolle oder eine IAM-Gruppe (AWS Identity and Access Management) nicht über eine Inline-Richtlinie zur Zugriffskontrolle auf Systeme und Ressourcen verfügt. AWS empfiehlt, verwaltete Richtlinien anstelle von Inline-Richtlinien zu verwenden. Verwaltete Richtlinien ermöglichen Wiederverwendbarkeit, Versionsverwaltung, Rollback und Delegierung der Berechtigungsverwaltung.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.308(a)(4)(ii)(C)	(C) Einrichtung und Änderung des Zugriffs (adressierbar). Implementieren Sie Richtlinien und Verfahren, mit denen auf der Grundlage der Zugriffsberechtigungsrichtlinien der Entität die Zugriffsrechte von Benutzern auf eine Workstation, einen Vorgang, ein Programm oder einen Prozess festgelegt, dokumentiert, überprüft und geändert werden.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) kann Ihnen dabei helfen, die Prinzipien der geringsten Rechte und der Aufgabentrennung in Zugriffsberechtigungen und Autorisierungen zu integrieren und so zu verhindern, dass Richtlinien „Effect“: „Allow“ mit „Action“: „*“ anstelle von „Resource“: „*“ enthalten. Wenn Benutzern mehr Rechte eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und der Aufgabentrennung verstoßen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.308(a)(4)(ii)(C)	(C) Einrichtung und Änderung des Zugriffs (adressierbar). Implementieren Sie Richtlinien und Verfahren, mit denen auf der Grundlage der Zugriffsberechtigungsrichtlinien der Entität die Zugriffsrechte von Benutzern auf eine Workstation, einen Vorgang, ein Programm oder einen Prozess festgelegt, dokumentiert, überprüft und geändert werden.	iam-root-access-key-überprüfen	Der Zugriff auf Systeme und Ressourcen kann gesteuert werden, indem überprüft wird, ob der Root-Benutzer keine Zugriffsschlüssel mit seiner AWS Identity and Access Management (IAM) -Rolle verknüpft hat. Stellen Sie sicher, dass die Root-Zugriffsschlüssel gelöscht werden. Erstellen und verwenden Sie stattdessen rollenbasierte Funktionen, AWS-Konten um das Prinzip der geringsten Funktionalität zu berücksichtigen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.308(a)(4)(ii)(C)	(C) Einrichtung und Änderung des Zugriffs (adressierbar). Implementieren Sie Richtlinien und Verfahren, mit denen auf der Grundlage der Zugriffsberechtigungsrichtlinien der Entität die Zugriffsrechte von Benutzern auf eine Workstation, einen Vorgang, ein Programm oder einen Prozess festgelegt, dokumentiert, überprüft und geändert werden.	iam-user-no-policies-überprüfen	Diese Regel stellt sicher, dass AWS Identity and Access Management (IAM) -Richtlinien nur Gruppen oder Rollen zugewiesen werden, um den Zugriff auf Systeme und Ressourcen zu kontrollieren. Die Zuweisung von Berechtigungen auf Gruppen- oder Rollenebene trägt dazu bei, die Wahrscheinlichkeit zu verringern, dass eine Identität übermäßige Berechtigungen erhält oder beibehält.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.308(a)(4)(ii)(C)	(C) Einrichtung und Änderung des Zugriffs (adressierbar). Implementieren Sie Richtlinien und Verfahren, mit denen auf der Grundlage der Zugriffsberechtigungsrichtlinien der Entität die Zugriffsrechte von Benutzern auf eine Workstation, einen Vorgang, ein Programm oder einen Prozess festgelegt, dokumentiert, überprüft und geändert werden.	iam-user-unused-credentials-überprüfen	AWS Identity and Access Management (IAM) kann Ihnen bei Zugriffsberechtigungen und Autorisierungen helfen, indem es nach IAM-Passwörtern und Zugriffsschlüsseln sucht, die für einen bestimmten Zeitraum nicht verwendet wurden. Wenn ungenutzte Anmeldeinformationen identifiziert werden, müssen Sie sie deaktivieren und/oder entfernen, da dies gegen das Prinzip der geringsten Berechtigung verstoßen könnte. Für diese Regel müssen Sie einen Wert für das maxCredentialUsage Alter festlegen (Standardkonfiguration: 90). Der tatsächliche Wert muss den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.308(a)(4)(ii)(C)	(C) Einrichtung und Änderung des Zugriffs (adressierbar). Implementieren Sie Richtlinien und Verfahren, mit denen auf der Grundlage der Zugriffsberechtigungsrichtlinien der Entität die Zugriffsrechte von Benutzern auf eine Workstation, einen Vorgang, ein Programm oder einen Prozess festgelegt, dokumentiert, überprüft und geändert werden.	iam-policy-no-statements-with-full-access	Stellen Sie sicher, dass IAM-Aktionen nur auf die benötigten Aktionen beschränkt sind. Wenn Benutzern mehr Rechte eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und der Aufgabentrennung verstoßen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.308(a)(4)(ii)(C)	(C) Einrichtung und Änderung des Zugriffs (adressierbar). Implementieren Sie Richtlinien und Verfahren, mit denen auf der Grundlage der Zugriffsberechtigungsrichtlinien der Entität die Zugriffsrechte von Benutzern auf eine Workstation, einen Vorgang, ein Programm oder einen Prozess festgelegt, dokumentiert, überprüft und geändert werden.	ec2- instance-profile-attached	EC2 Instanzprofile übergeben eine IAM-Rolle an eine Instanz EC2 . Das Anhängen eines Instance-Profils an Ihre Instances kann bei der Implementierung von geringsten Berechtigungen und der Berechtigungsverwaltung helfen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.308(a)(4)(ii)(C)	(C) Einrichtung und Änderung des Zugriffs (adressierbar). Implementieren Sie Richtlinien und Verfahren, mit denen auf der Grundlage der Zugriffsberechtigungsrichtlinien der Entität die Zugriffsrechte von Benutzern auf eine Workstation, einen Vorgang, ein Programm oder einen Prozess festgelegt, dokumentiert, überprüft und geändert werden.	dms-replication-not-public	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass auf DMS-Replikationsinstanzen nicht öffentlich zugegriffen werden kann. DMS-Replikations-Instances können vertrauliche Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.308(a)(4)(ii)(C)	(C) Einrichtung und Änderung des Zugriffs (adressierbar). Implementieren Sie Richtlinien und Verfahren, mit denen auf der Grundlage der Zugriffsberechtigungsrichtlinien der Entität die Zugriffsrechte von Benutzern auf eine Workstation, einen Vorgang, ein Programm oder einen Prozess festgelegt, dokumentiert, überprüft und geändert werden.	ebs-snapshot-public-restorable-überprüfen	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass EBS-Snapshots nicht öffentlich wiederherstellbar sind. EBS-Volume-Snapshots können vertrauliche Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.308(a)(4)(ii)(C)	(C) Einrichtung und Änderung des Zugriffs (adressierbar). Implementieren Sie Richtlinien und Verfahren, mit denen auf der Grundlage der Zugriffsberechtigungsrichtlinien der Entität die Zugriffsrechte von Benutzern auf eine Workstation, einen Vorgang, ein Programm oder einen Prozess festgelegt, dokumentiert, überprüft und geändert werden.	ec-2 instance-no-public-ip	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon Elastic Compute Cloud (Amazon EC2) - Instances nicht öffentlich zugänglich sind. EC2 Amazon-Instances können vertrauliche Informationen enthalten, und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.308(a)(4)(ii)(C)	(C) Einrichtung und Änderung des Zugriffs (adressierbar). Implementieren Sie Richtlinien und Verfahren, mit denen auf der Grundlage der Zugriffsberechtigungsrichtlinien der Entität die Zugriffsrechte von Benutzern auf eine Workstation, einen Vorgang, ein Programm oder einen Prozess festgelegt, dokumentiert, überprüft und geändert werden.	elasticsearch-in-vpc-only	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass sich Amazon OpenSearch OpenSearch Service (Service) - Domains innerhalb einer Amazon Virtual Private Cloud (Amazon VPC) befinden. Eine OpenSearch Service-Domain innerhalb einer Amazon VPC ermöglicht die sichere Kommunikation zwischen OpenSearch Service und anderen Services innerhalb der Amazon VPC, ohne dass ein Internet-Gateway, ein NAT-Gerät oder eine VPN-Verbindung erforderlich ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.308(a)(4)(ii)(C)	(C) Einrichtung und Änderung des Zugriffs (adressierbar). Implementieren Sie Richtlinien und Verfahren, mit denen auf der Grundlage der Zugriffsberechtigungsrichtlinien der Entität die Zugriffsrechte von Benutzern auf eine Workstation, einen Vorgang, ein Programm oder einen Prozess festgelegt, dokumentiert, überprüft und geändert werden.	emr-master-no-public-ip	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon EMR-Cluster-Masterknoten nicht öffentlich zugänglich sind. Amazon-EMR-Cluster-Hauptknoten können vertrauliche Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.308(a)(4)(ii)(C)	(C) Einrichtung und Änderung des Zugriffs (adressierbar). Implementieren Sie Richtlinien und Verfahren, mit denen auf der Grundlage der Zugriffsberechtigungsrichtlinien der Entität die Zugriffsrechte von Benutzern auf eine Workstation, einen Vorgang, ein Programm oder einen Prozess festgelegt, dokumentiert, überprüft und geändert werden.	ec-2 instances-in-vpc	Stellen Sie Amazon Elastic Compute Cloud (Amazon EC2) -Instances innerhalb einer Amazon Virtual Private Cloud (Amazon VPC) bereit, um eine sichere Kommunikation zwischen einer Instance und anderen Services innerhalb der Amazon VPC zu ermöglichen, ohne dass ein Internet-Gateway, ein NAT-Gerät oder eine VPN-Verbindung erforderlich ist. Der gesamte Datenverkehr bleibt sicher in der AWS Cloud. Domains, die sich innerhalb einer VPC befinden, verfügen aufgrund ihrer logischen Isolierung im Vergleich zu Domains mit öffentlichen Endpunkten über eine zusätzliche Sicherheitsebene. Weisen Sie EC2

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			Amazon-Instances einer Amazon-VPC zu, um den Zugriff ordnungsgemäß zu verwalten.
164.308(a)(4)(ii)(C)	(C) Einrichtung und Änderung des Zugriffs (adressierbar). Implementieren Sie Richtlinien und Verfahren, mit denen auf der Grundlage der Zugriffsberechtigungsrichtlinien der Entität die Zugriffsrechte von Benutzern auf eine Workstation, einen Vorgang, ein Programm oder einen Prozess festgelegt, dokumentiert, überprüft und geändert werden.	internet-gateway-authorized-vpc-nur	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Internet-Gateways nur mit autorisierter Amazon Virtual Private Cloud (Amazon VPC) verbunden sind. Internet-Gateways ermöglichen den bidirektionalen Internetzugang zur und von der Amazon VPC, was möglicherweise zu einem unbefugten Zugriff auf Amazon-VPC-Ressourcen führen kann.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.308(a)(4)(ii)(C)	(C) Einrichtung und Änderung des Zugriffs (adressierbar). Implementieren Sie Richtlinien und Verfahren, mit denen auf der Grundlage der Zugriffsberechtigungsrichtlinien der Entität die Zugriffsrechte von Benutzern auf eine Workstation, einen Vorgang, ein Programm oder einen Prozess festgelegt, dokumentiert, überprüft und geändert werden.	lambda-function-public-access-verboten	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass AWS Lambda-Funktionen nicht öffentlich zugänglich sind. Der öffentliche Zugriff kann möglicherweise die Verfügbarkeit von Ressourcen beeinträchtigen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.308(a)(4)(ii)(C)	(C) Einrichtung und Änderung des Zugriffs (adressierbar). Implementieren Sie Richtlinien und Verfahren, mit denen auf der Grundlage der Zugriffsberechtigungsrichtlinien der Entität die Zugriffsrechte von Benutzern auf eine Workstation, einen Vorgang, ein Programm oder einen Prozess festgelegt, dokumentiert, überprüft und geändert werden.	rds-instance-public-access-überprüfen	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Relational Database Service (Amazon RDS) -Instances nicht öffentlich sind. Amazon-RDS-Datenbank-Instances können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.308(a)(4)(ii)(C)	(C) Einrichtung und Änderung des Zugriffs (adressierbar). Implementieren Sie Richtlinien und Verfahren, mit denen auf der Grundlage der Zugriffsberechtigungsrichtlinien der Entität die Zugriffsrechte von Benutzern auf eine Workstation, einen Vorgang, ein Programm oder einen Prozess festgelegt, dokumentiert, überprüft und geändert werden.	rds-snapshots-public-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Relational Database Service (Amazon RDS) -Instances nicht öffentlich sind. Amazon-RDS-Datenbank-Instances können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.308(a)(4)(ii)(C)	(C) Einrichtung und Änderung des Zugriffs (adressierbar). Implementieren Sie Richtlinien und Verfahren, mit denen auf der Grundlage der Zugriffsberechtigungsrichtlinien der Entität die Zugriffsrechte von Benutzern auf eine Workstation, einen Vorgang, ein Programm oder einen Prozess festgelegt, dokumentiert, überprüft und geändert werden.	redshift-cluster-public-access-überprüfen	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Redshift Redshift-Cluster nicht öffentlich sind. Amazon-Redshift-Cluster können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.308(a)(4)(ii)(C)	(C) Einrichtung und Änderung des Zugriffs (adressierbar). Implementieren Sie Richtlinien und Verfahren, mit denen auf der Grundlage der Zugriffsberechtigungsrichtlinien der Entität die Zugriffsrechte von Benutzern auf eine Workstation, einen Vorgang, ein Programm oder einen Prozess festgelegt, dokumentiert, überprüft und geändert werden.	s3- -Block-periodisch account-level-public-access	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Simple Storage Service (Amazon S3) -Buckets nicht öffentlich zugänglich sind. Diese Regel trägt dazu bei, sensible Daten vor unbefugten Remote-Benutzern zu schützen, indem sie den öffentlichen Zugriff verhindert. Mit dieser Regel können Sie optional die Parameter ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) und restrictPublicBuckets Parameter (Config Default: True) festlegen. Die tatsächlichen Werte müssen den Richtlini

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			en Ihrer Organisation entsprechen.
164.308(a)(4)(ii)(C)	(C) Einrichtung und Änderung des Zugriffs (adressierbar). Implementieren Sie Richtlinien und Verfahren, mit denen auf der Grundlage der Zugriffsberechtigungsrichtlinien der Entität die Zugriffsrechte von Benutzern auf eine Workstation, einen Vorgang, ein Programm oder einen Prozess festgelegt, dokumentiert, überprüft und geändert werden.	s3- bucket-public-read-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie nur autorisierten Benutzern, Prozessen und Geräten Zugriff auf Amazon Simple Storage Service (Amazon S3) - Buckets gewähren. Die Verwaltung des Zugriffs sollte mit der Klassifizierung der Daten übereinstimmen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.308(a)(4)(ii)(C)	(C) Einrichtung und Änderung des Zugriffs (adressierbar). Implementieren Sie Richtlinien und Verfahren, mit denen auf der Grundlage der Zugriffsberechtigungsrichtlinien der Entität die Zugriffsrechte von Benutzern auf eine Workstation, einen Vorgang, ein Programm oder einen Prozess festgelegt, dokumentiert, überprüft und geändert werden.	s3- bucket-public-write-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie nur autorisierten Benutzern, Prozessen und Geräten Zugriff auf Amazon Simple Storage Service (Amazon S3) - Buckets gewähren. Die Verwaltung des Zugriffs sollte mit der Klassifizierung der Daten übereinstimmen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.308(a)(4)(ii)(C)	(C) Einrichtung und Änderung des Zugriffs (adressierbar). Implementieren Sie Richtlinien und Verfahren, mit denen auf der Grundlage der Zugriffsberechtigungsrichtlinien der Entität die Zugriffsrechte von Benutzern auf eine Workstation, einen Vorgang, ein Programm oder einen Prozess festgelegt, dokumentiert, überprüft und geändert werden.	sagemaker-notebook-no-direct-Internetzugang	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass SageMaker Amazon-Notebooks keinen direkten Internetzugang zulassen. Indem Sie direkten Internetzugang blockieren, vermeiden Sie, dass unbefugte Benutzer auf sensible Daten zugreifen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.308(a)(4)(ii)(C)	(C) Einrichtung und Änderung des Zugriffs (adressierbar). Implementieren Sie Richtlinien und Verfahren, mit denen auf der Grundlage der Zugriffsberechtigungsrichtlinien der Entität die Zugriffsrechte von Benutzern auf eine Workstation, einen Vorgang, ein Programm oder einen Prozess festgelegt, dokumentiert, überprüft und geändert werden.	subnet-auto-assign-public-ip-deaktiviert	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon Virtual Private Cloud (VPC) -Subnetzen nicht automatisch eine öffentliche IP-Adresse zugewiesen wird. Amazon Elastic Compute Cloud (EC2) -Instances, die in Subnetzen gestartet werden, in denen dieses Attribut aktiviert ist, haben ihrer primären Netzwerkschnittstelle eine öffentliche IP-Adresse zugewiesen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.308(a)(4)(ii)(C)	(C) Einrichtung und Änderung des Zugriffs (adressierbar). Implementieren Sie Richtlinien und Verfahren, mit denen auf der Grundlage der Zugriffsberechtigungsrichtlinien der Entität die Zugriffsrechte von Benutzern auf eine Workstation, einen Vorgang, ein Programm oder einen Prozess festgelegt, dokumentiert, überprüft und geändert werden.	ecs-task-definition-user-for-host-mode-check	Wenn für eine Aufgabendefinition erhöhte Berechtigungen gelten, liegt das daran, dass der Kunde diesen Konfigurationen ausdrücklich zugestimmt hat. Diese Kontrolle prüft, ob eine unerwartete Berechtigungseskalation vorliegt, wenn für eine Aufgabendefinition das Host-Netzwerk aktiviert ist, die Kunden aber keine erhöhten Berechtigungen aktiviert haben.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.308(a)(4)(ii)(C)	(C) Einrichtung und Änderung des Zugriffs (adressierbar). Implementieren Sie Richtlinien und Verfahren, mit denen auf der Grundlage der Zugriffsberechtigungsrichtlinien der Entität die Zugriffsrechte von Benutzern auf eine Workstation, einen Vorgang, ein Programm oder einen Prozess festgelegt, dokumentiert, überprüft und geändert werden.	codebuild-project-envvar-awscred-überprüfen	Stellen Sie sicher, dass die Anmeldeinformationen AWS_ACCESS_KEY_ID AWS_SECRET_ACCESS_KEY nicht in AWS Codebuild-Projektumgebungen vorhanden sind. Speichern Sie diese Variablen nicht als Klartext. Das Speichern dieser Variablen als Klartext bewirkt eine unbeabsichtigte Offenlegung von Daten sowie unberechtigte Zugriffe.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.308(a)(4)(ii)(C)	(C) Einrichtung und Änderung des Zugriffs (adressierbar). Implementieren Sie Richtlinien und Verfahren, mit denen auf der Grundlage der Zugriffsberechtigungsrichtlinien der Entität die Zugriffsrechte von Benutzern auf eine Workstation, einen Vorgang, ein Programm oder einen Prozess festgelegt, dokumentiert, überprüft und geändert werden.	codebuild-project-source-repo-URL-Prüfung	Stellen Sie sicher, dass die URL des Quell-Repositorys GitHub oder des Bitbucket-Quell-Repositorys keine persönlichen Zugriffstoken oder Anmeldeinformationen in Codebuild-Projektumgebungen enthält. AWS Verwende OAuth anstelle von persönlichen Zugriffstoken oder Anmeldedaten die Autorisierung für den Zugriff auf GitHub Bitbucket-Repositorys.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.308(a)(4)(ii)(C)	(C) Einrichtung und Änderung des Zugriffs (adressierbar). Implementieren Sie Richtlinien und Verfahren, mit denen auf der Grundlage der Zugriffsberechtigungsrichtlinien der Entität die Zugriffsrechte von Benutzern auf eine Workstation, einen Vorgang, ein Programm oder einen Prozess festgelegt, dokumentiert, überprüft und geändert werden.	restricted-common-ports	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass gemeinsame Ports für Amazon Elastic Compute Cloud (Amazon EC2) -Sicherheitsgruppen eingeschränkt sind. Wenn der Zugriff auf Ports nicht auf vertrauenswürdige Quellen beschränkt wird, kann dies zu Angriffen auf die Verfügbarkeit, Integrität und Vertraulichkeit von Systemen führen. Mit dieser Regel können Sie optional die Parameter blockedPort1–blockedPort5 festlegen (Standardkonfigurationen: 20, 21, 3389, 3306, 4333). Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.308(a)(4)(ii)(C)	(C) Einrichtung und Änderung des Zugriffs (adressierbar). Implementieren Sie Richtlinien und Verfahren, mit denen auf der Grundlage der Zugriffsberechtigungsrichtlinien der Entität die Zugriffsrechte von Benutzern auf eine Workstation, einen Vorgang, ein Programm oder einen Prozess festgelegt, dokumentiert, überprüft und geändert werden.	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) Security Groups können bei der Verwaltung des Netzwerkzugriffs helfen, indem sie eine statusbehaftete Filterung von eingehendem und ausgehendem Netzwerkverkehr zu Ressourcen bereitstellen. AWS Wenn Sie eingehenden (oder entfernten) Datenverkehr von 0.0.0.0/0 bis Port 22 auf Ihren Ressourcen nicht zulassen, können Sie den Remote-Zugriff einschränken.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.308(a)(4)(ii)(C)	(C) Einrichtung und Änderung des Zugriffs (adressierbar). Implementieren Sie Richtlinien und Verfahren, mit denen auf der Grundlage der Zugriffsberechtigungsrichtlinien der Entität die Zugriffsrechte von Benutzern auf eine Workstation, einen Vorgang, ein Programm oder einen Prozess festgelegt, dokumentiert, überprüft und geändert werden.	autoscaling-launch-config-public-ip-deaktiviert	Wenn Sie Ihre Netzwerkschnittstellen mit einer öffentlichen IP-Adresse konfigurieren, sind die diesen Netzwerkschnittstellen zugehörigen Ressourcen über das Internet erreichbar. EC2 Ressourcen sollten nicht öffentlich zugänglich sein, da dies einen unbeabsichtigten Zugriff auf Ihre Anwendungen oder Server ermöglichen kann.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.308(a)(4)(ii)(C)	(C) Einrichtung und Änderung des Zugriffs (adressierbar). Implementieren Sie Richtlinien und Verfahren, mit denen auf der Grundlage der Zugriffsberechtigungsrichtlinien der Entität die Zugriffsrechte von Benutzern auf eine Workstation, einen Vorgang, ein Programm oder einen Prozess festgelegt, dokumentiert, überprüft und geändert werden.	ecs-containers-readonly-access	Die Aktivierung des schreibgeschützten Zugriffs auf Amazon Elastic Container Service (ECS)-Container kann dazu beitragen, das Prinzip der geringsten Berechtigung einzuhalten. Diese Option kann Angriffsvektoren reduzieren, da das Dateisystem der Container-Instance nur geändert werden kann, wenn es über ausdrückliche Lese- und Schreibberechtigungen verfügt.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.308(a)(4)(ii)(C)	(C) Einrichtung und Änderung des Zugriffs (adressierbar). Implementieren Sie Richtlinien und Verfahren, mit denen auf der Grundlage der Zugriffsberechtigungsrichtlinien der Entität die Zugriffsrechte von Benutzern auf eine Workstation, einen Vorgang, ein Programm oder einen Prozess festgelegt, dokumentiert, überprüft und geändert werden.	ssm-document-not-public	Stellen Sie sicher, dass AWS Systems Manager (SSM) - Dokumente nicht öffentlich sind, da dies einen unbeabsichtigten Zugriff auf Ihre SSM-Dokumente ermöglichen kann. Ein öffentliches SSM-Dokument kann Informationen über Ihr Konto, Ihre Ressourcen und internen Prozesse preisgeben.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.308(a)(4)(ii)(C)	(C) Einrichtung und Änderung des Zugriffs (adressierbar). Implementieren Sie Richtlinien und Verfahren, mit denen auf der Grundlage der Zugriffsberechtigungsrichtlinien der Entität die Zugriffsrechte von Benutzern auf eine Workstation, einen Vorgang, ein Programm oder einen Prozess festgelegt, dokumentiert, überprüft und geändert werden.	s-3 bucket-acl-prohibited	Diese Regel prüft, ob Access Control Lists (ACLs) für die Zugriffskontrolle auf Amazon S3 S3-Buckets verwendet werden. ACLs sind veraltete Zugriffskontrollmechanismen für Amazon S3 S3-Buckets, die älter sind als AWS Identity and Access Management (IAM). Stattdessen empfiehlt es sich ACLs, IAM-Richtlinien oder S3-Bucket-Richtlinien zu verwenden, um den Zugriff auf Ihre S3-Buckets einfacher zu verwalten.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.308(a)(4)(ii)(C)	(C) Einrichtung und Änderung des Zugriffs (adressierbar). Implementieren Sie Richtlinien und Verfahren, mit denen auf der Grundlage der Zugriffsberechtigungsrichtlinien der Entität die Zugriffsrechte von Benutzern auf eine Workstation, einen Vorgang, ein Programm oder einen Prozess festgelegt, dokumentiert, überprüft und geändert werden.	opensearch-in-vpc-only	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass sich Amazon OpenSearch Service-Domains innerhalb einer Amazon Virtual Private Cloud (Amazon VPC) befinden. Eine Amazon OpenSearch Service-Domain innerhalb einer Amazon VPC ermöglicht die sichere Kommunikation zwischen Amazon OpenSearch Service und anderen Services innerhalb der Amazon VPC, ohne dass ein Internet-Gateway, ein NAT-Gerät oder eine VPN-Verbindung erforderlich ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.308(a)(5)(ii)(A)	(A) Sicherheitserinnerungen (adressierbar). Regelmäßige Sicherheitsupdates.	ec2-check managedinstance-patch-compliance-status	Aktivieren Sie diese Regel, um bei der Identifizierung und Dokumentation von Sicherheitslücken in Amazon Elastic Compute Cloud (Amazon EC2) zu helfen. Die Regel prüft, ob die EC2 Amazon-Instance die Patch-Konformität im AWS Systems Manager gemäß den Richtlinien und Verfahren Ihrer Organisation einhält.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.308(a)(5)(ii)(A)	(A) Sicherheitserinnerungen (adressierbar). Regelmäßige Sicherheitsupdates.	elastic-beanstalk-managed-updates-aktiviert	Durch die Aktivierung verwalteter Plattformupdates für eine Amazon-Elastic-Beanstalk-Umgebung wird sichergestellt, dass die aktuellen verfügbaren Plattform-Fixes, -Updates und -Features für die Umgebung installiert sind. Eine bewährte Methode zur Sicherung von Systemen besteht darin, stets die aktuellen Patches zu installieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.308(a)(5)(ii)(A)	(A) Sicherheitserinnerungen (adressierbar). Regelmäßige Sicherheitsupdates.	redshift-cluster-maintenancesettings-check	Diese Regel stellt sicher, dass Amazon-Redshift-Cluster die bevorzugten Einstellungen für Ihre Organisation haben. Insbesondere sorgt sie dafür, dass Cluster bevorzugte Wartungsfenster und automatisierte Aufbewahrungsfristen für Snapshots für die Datenbank haben. Für diese Regel müssen Sie die allowVersionUpgrade festlegen. Der Standardwert ist „true“. Außerdem können Sie optional den Zeitraum preferredMaintenanceWindow (der Standardwert ist sa: 16:00 -sa: 16:30) und den automated SnapshotRetention Zeitraum (der Standardwert ist 1) festlegen. Die tatsächlichen Werte müssen den Richtlini

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			en Ihrer Organisation entsprechen.
164.308(a)(5)(ii)(A)	(A) Sicherheitserinnerungen (adressierbar). Regelmäßige Sicherheitsupdates.	rds-automatic-minor-version-Upgrade aktiviert	Aktivieren Sie automatische Unterversions-Upgrades auf Ihren Amazon-Relational-Database-Service (RDS)-Instances, um sicherzustellen, dass die aktuellen Updates für Unterversionen des Relational Database Management System (RDBMS) installiert sind, die Sicherheitspatches und Bugfixes enthalten können.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.308(a)(5)(ii)(B)	(B) Schutz vor Malware (adressierbar). Verfahren zum Schutz vor Malware sowie zur Erkennung und Meldung von Malware.	ec2-managerinstance-managed-by-systems	Eine Bestandsaufnahme der Softwareplattformen und Anwendungen innerhalb des Unternehmens ist möglich, indem Amazon Elastic Compute Cloud (Amazon EC2) - Instances mit AWS Systems Manager verwaltet werden. Verwenden Sie AWS Systems Manager, um detaillierte Systemkonfigurationen, Betriebssystem-Patch-Levels, Namen und Typ der Dienste, Softwareinstallationen, Anwendungsname, Herausgeber und Version sowie andere Details zu Ihrer Umgebung bereitzustellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.308(a)(5)(ii)(B)	(B) Schutz vor Malware (adressierbar). Verfahren zum Schutz vor Malware sowie zur Erkennung und Meldung von Malware.	ec2-check managedinstance-association-compliance-status	Verwenden Sie AWS Systems Manager Associations, um bei der Inventarisierung von Softwareplattformen und Anwendungen innerhalb eines Unternehmens zu helfen. AWS Systems Manager weist Ihren verwalteten Instanzen einen Konfigurationsstatus zu und ermöglicht es Ihnen, Basiswerte für Betriebssystem-Patch-Levels, Softwareinstallationen, Anwendungskonfigurationen und andere Details zu Ihrer Umgebung festzulegen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.308(a)(5)(ii)(B)	(B) Schutz vor Malware (adressierbar). Verfahren zum Schutz vor Malware sowie zur Erkennung und Meldung von Malware.	ec2-check managedinstance-patch-compliance-status	Aktivieren Sie diese Regel, um bei der Identifizierung und Dokumentation von Sicherheitslücken in Amazon Elastic Compute Cloud (Amazon EC2) zu helfen. Die Regel prüft, ob die EC2 Amazon-Instance die Patch-Konformität im AWS Systems Manager gemäß den Richtlinien und Verfahren Ihrer Organisation einhält.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.308(a)(5)(ii)(C)	(C) Überwachung der Anmeldung (adressierbar). Verfahren zur Überwachung von Anmeldeversuchen und zur Meldung von Unstimmigkeiten.	guardduty-enabled-centralized	Amazon GuardDuty kann mithilfe von Threat Intelligence Feeds helfen, potenzielle Cybersicherheitsereignisse zu überwachen und zu erkennen. Dazu gehören Listen mit bösartigen IPs und maschinellen Lernmethoden zur Identifizierung unerwarteter, nicht autorisierter und bösartiger Aktivitäten in Ihrer AWS Cloud-Umgebung.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.308(a)(5)(ii)(C)	(C) Überwachung der Anmeldung (adressierbar). Verfahren zur Überwachung von Anmeldeversuchen und zur Meldung von Unstimmigkeiten.	cloudtrail-enabled	AWS CloudTrail kann durch die Aufzeichnung von Aktionen und API-Aufrufen in der AWS Management Console dazu beitragen, dass die Daten nicht zurückgewiesen werden können. Sie können die Benutzer und die Benutzer AWS-Konten , die einen AWS Dienst aufgerufen haben, die Quell-IP-Adresse, über die die Aufrufe generiert wurden, und den Zeitpunkt der Anrufe identifizieren. Einzelheiten zu den erfassten Daten finden Sie unter Inhalt des AWS CloudTrail Datensatzes.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.308(a)(5)(ii)(C)	(C) Überwachung der Anmeldung (adressierbar). Verfahren zur Überwachung von Anmeldeversuchen und zur Meldung von Unstimmigkeiten.	rds-logging-enabled	Um die Protokollierung und Überwachung in Ihrer Umgebung zu erleichtern, stellen Sie sicher, dass die Amazon Relational Database Service (Amazon RDS)-Protokollierung aktiviert ist. Mit der Amazon-RDS-Protokollierung können Sie Ereignisse wie Verbindungen, Verbindungsabbrüche, Abfragen oder abgefragte Tabellen erfassen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.308(a)(5)(ii)(D)	(D) Passwortv erwaltung (adressie rbar). Verfahren zum Erstellen, Ändern und Schützen von Passwörtern.	iam-password-policy	Die Identitäten und Anmeldeinformation en werden auf der Grundlage einer organisatorischen IAM-Passwortrichtlinie ausgestellt, verwaltet und verifiziert. Sie erfüllen oder übertreff en die Anforderungen von NIST SP 800-63 und dem Standard „Best Practices“ von AWS Foundatio nal Security für die Passwortstärke. Mit dieser Regel können Sie optional RequireUppercaseCh aracters (Wert für AWS grundlegende Sicherheitsbewährt e Methoden: wahr), RequireLowercaseCh aracters (Wert für bewährte Methoden für AWS grundlege nde Sicherheit: wahr), RequireSy mbols (Wert für bewährte Methoden für AWS grundlege nde Sicherheit:

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			wahr), RequireNumbers (Wert für bewährte Methoden für AWS grundlegende Sicherheit: wahr), MinimumPasswordLength (Wert für bewährte Methoden für AWS grundlegende Sicherheit: 14), PasswordReusePrevention (Wert für bewährte Methoden für AWS grundlegende Sicherheit: 24) und MaxPasswordAge (Wert für bewährte Methoden für AWS grundlegende Sicherheit: 90) für Ihr IAM festlegen Kennwortrichtlinie. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.308(a)(6)(i)	(6)(i) Standard: Verfahren für Sicherheitsvorfäll e. Implementieren Sie Richtlinien und Verfahren zur Behebung von Sicherheitsvorfällen.	securityhub-enabled	AWS Security Hub hilft bei der Überwachung von unbefugtem Personal, Verbindun gen, Geräten und Software. AWS Security Hub aggregiert, organisie rt und priorisie rt die Sicherhei tswarnungen oder Ergebnisse mehrerer Dienste. AWS Einige dieser Dienste sind Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer und AWS Firewall Manager sowie AWS Partnerlösungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.308(a)(6)(ii)	(ii) Spezifikation der Implementierung: Reaktion und Berichterstattung (erforderlich). Identifizieren Sie vermutete oder bekannte Sicherheitsvorfälle und reagieren Sie darauf; mindern Sie, soweit möglich, schädliche Auswirkungen von Sicherheitsvorfällen, die der betroffenen Entität bekannt sind, und dokumentieren Sie Sicherheitsvorfälle und ihre Folgen.	guardduty-enabled-centralized	Amazon GuardDuty kann mithilfe von Threat Intelligence Feeds helfen, potenzielle Cybersicherheitsereignisse zu überwachen und zu erkennen. Dazu gehören Listen mit bösartigen IPs und maschinellen Lernmethoden zur Identifizierung unerwarteter, nicht autorisierter und bösartiger Aktivitäten in Ihrer AWS Cloud-Umgebung.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.308(a)(7)(i)	(7) (i) Standard: Notfallplan. Festlegung (und nach Bedarf Umsetzung) von Richtlinien und Verfahren zur Reaktion auf Notfälle oder andere Ereignisse (z. B. Brand, Vandalismus, Systemausfall und Naturkatastrophe), durch die Systeme beschädigt werden, die elektronischegeschützte Gesundheitsinformationen enthalten.	dynamodb-autoscaling-enabled	Amazon DynamoDB Auto Scaling verwendet den AWS Application Auto Scaling-Service, um die bereitgestellte Durchsatzkapazität so anzupassen, dass sie automatisch auf tatsächliche Verkehrsmuster reagiert. Auf diese Weise kann eine Tabelle oder ein globaler sekundärer Index die bereitgestellte Lese-/Schreibkapazität erhöhen, um plötzliche Erhöhungen des Datenverkehrs ohne Drosselung zu bewältigen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.308(a)(7)(i)	(7) (i) Standard: Notfallplan. Festlegung (und nach Bedarf Umsetzung) von Richtlinien und Verfahren zur Reaktion auf Notfälle oder andere Ereignisse (z. B. Brand, Vandalismus, Systemausfall und Naturkatastrophe), durch die Systeme beschädigt werden, die elektronischegeschützte Gesundheitsinformationen enthalten.	elb-cross-zone-load-Balancing aktiviert	Aktivieren Sie zonenübergreifendes Load Balancing für Ihre Elastic Load Balancer (ELBs), um eine angemessene Kapazität und Verfügbarkeit aufrechtzuerhalten. Zonenübergreifendes Load Balancing reduziert die Notwendigkeit, die gleiche Anzahl von Instances in jeder aktivierten Availability Zone aufrechtzuerhalten. Es verbessert auch die Fähigkeit Ihrer Anwendung, den Verlust einer oder mehrerer Instances zu bewältigen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.308(a)(7)(i)	(7) (i) Standard: Notfallplan. Festlegung (und nach Bedarf Umsetzung) von Richtlinien und Verfahren zur Reaktion auf Notfälle oder andere Ereignisse (z. B. Brand, Vandalismus, Systemausfall und Naturkatastrophe), durch die Systeme beschädigt werden, die elektronischegeschützte Gesundheitsinformationen enthalten.	elb-deletion-protection-enabled	Diese Regel sorgt dafür, dass der Löschschutz für Elastic Load Balancing aktiviert ist. Verwenden Sie diese Funktion, um zu verhindern, dass Ihr Load Balancer versehentlich oder böswillig gelöscht wird, was zum Verlust der Verfügbarkeit Ihrer Anwendungen führen kann.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.308(a)(7)(i)	(7) (i) Standard: Notfallplan. Festlegung (und nach Bedarf Umsetzung) von Richtlinien und Verfahren zur Reaktion auf Notfälle oder andere Ereignisse (z. B. Brand, Vandalismus, Systemausfall und Naturkatastrophe), durch die Systeme beschädigt werden, die elektronischegeschützte Gesundheitsinformationen enthalten.	rds-cluster-deletion-protection-aktiviert	Stellen Sie sicher, dass Amazon Relational Database Service (Amazon RDS)-Instances den Löschschutz aktiviert haben. Verwenden Sie den Löschschutz, um zu verhindern, dass Ihre Amazon-RDS-Instances versehentlich oder böswillig gelöscht werden, was zum Verlust der Verfügbarkeit Ihrer Anwendungen führen kann.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.308(a)(7)(i)	(7) (i) Standard: Notfallplan. Festlegung (und nach Bedarf Umsetzung) von Richtlinien und Verfahren zur Reaktion auf Notfälle oder andere Ereignisse (z. B. Brand, Vandalismus, Systemausfall und Naturkatastrophe), durch die Systeme beschädigt werden, die elektronischegeschützte Gesundheitsinformationen enthalten.	rds-multi-az-support	Die Multi-AZ-Unterstützung in Amazon Relational Database Service (Amazon RDS) bietet eine verbesserte Verfügbarkeit und Beständigkeit von Datenbank-Instances. Wenn Sie eine Multi-AZ-Datenbank-Instance bereitstellen, erstellt Amazon RDS automatisch eine primäre Datenbank-Instance und repliziert die Daten synchron auf eine Standby-Instance in einer anderen Availability Zone. Jede Availability Zone läuft auf einer eigenen, physisch getrennten, unabhängigen Infrastruktur und ist auf eine hohe Verfügbarkeit ausgelegt. Im Falle eines Infrastrukturausfalls führt Amazon RDS einen automatis

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			chen Failover zum Standby-Modus durch, sodass Sie den Datenbankbetrieb wieder aufnehmen können, sobald der Failover abgeschlo ssen ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.308(a)(7)(i)	(7) (i) Standard: Notfallplan. Festlegung (und nach Bedarf Umsetzung) von Richtlinien und Verfahren zur Reaktion auf Notfälle oder andere Ereignisse (z. B. Brand, Vandalismus, Systemausfall und Naturkatastrophe), durch die Systeme beschädigt werden, die elektronischegeschützte Gesundheitsinformationen enthalten.	vpc-vpn-2-tunnels-up	Redundante Site-to-Site VPN-Tunnel können implementiert werden, um die Anforderungen an die Ausfallsicherheit zu erfüllen. Es verwendet zwei Tunnel, um die Konnektivität sicherzustellen, falls eine der Site-to-Site VPN-Verbindungen nicht verfügbar ist. Um sich vor einem Verbindungsverlust zu schützen, können Sie für den Fall, dass Ihr Kunden-Gateway nicht verfügbar ist, eine zweite Site-to-Site VPN-Verbindung zu Ihrer Amazon Virtual Private Cloud (Amazon VPC) und Ihrem Virtual Private Gateway einrichten, indem Sie ein zweites Kunden-Gateway verwenden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.308(a)(7)(i)	(7) (i) Standard: Notfallplan. Festlegung (und nach Bedarf Umsetzung) von Richtlinien und Verfahren zur Reaktion auf Notfälle oder andere Ereignisse (z. B. Brand, Vandalismus, Systemausfall und Naturkatastrophe), durch die Systeme beschädigt werden, die elektronischegeschützte Gesundheitsinformationen enthalten.	db-instance-backup-enabled	Die Sicherungsfunktion von Amazon RDS erstellt Sicherungen Ihrer Datenbanken und Transaktionsprotokolle. Amazon RDS erstellt einen Snapshot für das Speichervolume Ihrer DB-Instance, sodass die gesamte DB-Instance gesichert wird. Sie können im System spezifische Aufbewahrungsfristen festlegen, um Ihre Ausfallsicherheitsanforderungen zu erfüllen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.308(a)(7)(i)	(7) (i) Standard: Notfallplan. Festlegung (und nach Bedarf Umsetzung) von Richtlinien und Verfahren zur Reaktion auf Notfälle oder andere Ereignisse (z. B. Brand, Vandalismus, Systemausfall und Naturkatastrophe), durch die Systeme beschädigt werden, die elektronischegeschützte Gesundheitsinformationen enthalten.	dynamodb-in-backup-plan	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon DynamoDB-Tabellen Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.308(a)(7)(i)	(7) (i) Standard: Notfallplan. Festlegung (und nach Bedarf Umsetzung) von Richtlinien und Verfahren zur Reaktion auf Notfälle oder andere Ereignisse (z. B. Brand, Vandalismus, Systemausfall und Naturkatastrophe), durch die Systeme beschädigt werden, die elektronischegeschützte Gesundheitsinformationen enthalten.	dynamodb-pitr-enabled	Aktivieren Sie diese Regel, um zu überprüfen, ob die Informationen gesichert wurden. Es verwaltet auch die Backups, indem es sicherstellt, dass die point-in-time Wiederherstellung in Amazon DynamoDB aktiviert ist. Bei der Wiederherstellung werden fortlaufende Backups Ihrer Tabelle für die letzten 35 Tage gespeichert.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.308(a)(7)(i)	(7) (i) Standard: Notfallplan. Festlegung (und nach Bedarf Umsetzung) von Richtlinien und Verfahren zur Reaktion auf Notfälle oder andere Ereignisse (z. B. Brand, Vandalismus, Systemausfall und Naturkatastrophe), durch die Systeme beschädigt werden, die elektronischegeschützte Gesundheitsinformationen enthalten.	ebs-in-backup-plan	Stellen Sie zur Unterstützung der Datensicherungsprozesse sicher, dass Ihre Amazon Elastic Block Store (Amazon EBS) -Volumes Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.308(a)(7)(i)	(7) (i) Standard: Notfallplan. Festlegung (und nach Bedarf Umsetzung) von Richtlinien und Verfahren zur Reaktion auf Notfälle oder andere Ereignisse (z. B. Brand, Vandalismus, Systemausfall und Naturkatastrophe), durch die Systeme beschädigt werden, die elektronischegeschützte Gesundheitsinformationen enthalten.	efs-in-backup-plan	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon Elastic File System (Amazon EFS) -Dateisysteme Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.308(a)(7)(i)	(7) (i) Standard: Notfallplan. Festlegung (und nach Bedarf Umsetzung) von Richtlinien und Verfahren zur Reaktion auf Notfälle oder andere Ereignisse (z. B. Brand, Vandalismus, Systemausfall und Naturkatastrophe), durch die Systeme beschädigt werden, die elektronischegeschützte Gesundheitsinformationen enthalten.	elasticache-redis-cluster-automatic-Backup-Check	Wenn automatische Backups aktiviert sind, ElastiCache erstellt Amazon täglich ein Backup des Clusters. Die Sicherung kann für eine von Ihrer Organisation festgelegte Anzahl von Tagen aufbewahrt werden. Automatische Backups schützen vor Datenverlust. Bei einem Ausfall können Sie einen neuen Cluster erstellen, der Ihre Daten aus dem aktuellen Backup wiederherstellt.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.308(a)(7)(i)	(7) (i) Standard: Notfallplan. Festlegung (und nach Bedarf Umsetzung) von Richtlinien und Verfahren zur Reaktion auf Notfälle oder andere Ereignisse (z. B. Brand, Vandalismus, Systemausfall und Naturkatastrophe), durch die Systeme beschädigt werden, die elektronischegeschützte Gesundheitsinformationen enthalten.	rds-in-backup-plan	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon Relational Database Service (Amazon RDS) -Instances Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.308(a)(7)(i)	(7) (i) Standard: Notfallplan. Festlegung (und nach Bedarf Umsetzung) von Richtlinien und Verfahren zur Reaktion auf Notfälle oder andere Ereignisse (z. B. Brand, Vandalismus, Systemausfall und Naturkatastrophe), durch die Systeme beschädigt werden, die elektronischegeschützte Gesundheitsinformationen enthalten.	redshift-backup-enabled	Stellen Sie zur Unterstützung der Datensicherungsprozesse sicher, dass Ihre Amazon-Redshift-Cluster über automatisierte Snapshots verfügen. Wenn automatisierte Snapshots für einen Cluster aktiviert sind, erstellt Redshift in regelmäßigen Abständen Snapshots dieses Clusters. Standardmäßig erstellt Redshift alle acht Stunden oder alle 5 GB einen Snapshot für jeden Knoten mit Datenänderungen oder je nachdem, was zuerst eintritt.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.308(a)(7)(i)	(7) (i) Standard: Notfallplan. Festlegung (und nach Bedarf Umsetzung) von Richtlinien und Verfahren zur Reaktion auf Notfälle oder andere Ereignisse (z. B. Brand, Vandalismus, Systemausfall und Naturkatastrophe), durch die Systeme beschädigt werden, die elektronischegeschützte Gesundheitsinformationen enthalten.	s3- bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) unterstützt die Aufrechterhaltung einer angemessenen Kapazität und Verfügbarkeit. CRR ermöglicht das automatische, asynchrone Kopieren von Objekten in Amazon-S3-Buckets, um die Datenverfügbarkeit sicherzustellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.308(a)(7)(i)	(7) (i) Standard: Notfallplan. Festlegung (und nach Bedarf Umsetzung) von Richtlinien und Verfahren zur Reaktion auf Notfälle oder andere Ereignisse (z. B. Brand, Vandalismus, Systemausfall und Naturkatastrophe), durch die Systeme beschädigt werden, die elektronischegeschützte Gesundheitsinformationen enthalten.	s-3 bucket-versioning-enabled	Die Versionsverwaltung von Amazon Simple Storage Service (Amazon S3)-Buckets hilft dabei, mehrere Varianten eines Objekts im selben Amazon-S3-Bucket zu speichern. Verwenden Sie die Versionsverwaltung, um sämtliche Versionen aller Objekte in Ihrem Amazon-S3-Bucket zu speichern, abzurufen oder wiederherzustellen. Mit der Versionsverwaltung können Sie Versionen sowohl nach unbeabsichtigten Benutzeraktionen als auch nach Anwendungsfehlern problemlos wiederherstellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.308(a)(7)(i)	(7) (i) Standard: Notfallplan. Festlegung (und nach Bedarf Umsetzung) von Richtlinien und Verfahren zur Reaktion auf Notfälle oder andere Ereignisse (z. B. Brand, Vandalismus, Systemausfall und Naturkatastrophe), durch die Systeme beschädigt werden, die elektronischegeschützte Gesundheitsinformationen enthalten.	s-3 version-lifecycle-policy-check	Mit Amazon-S3-Lebenszyklusregeln können Sie Aktionen definieren, die Amazon S3 während der Lebensdauer eines Objekts ausführen soll (z. B. die Überführung von Objekten in eine andere Speicherklasse, ihre Archivierung oder Löschung nach einem bestimmten Zeitraum).

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.308(a)(7)(ii)(A)	(A) Datensicherungsplan (erforderlich). Einrichtung und Implementierung von Verfahren zur Erstellung und Aufbewahrung exakter, abrufbarer Kopien elektronisch geschützter Gesundheitsinformationen.	db-instance-backup-enabled	Die Sicherungsfunktion von Amazon RDS erstellt Sicherungen Ihrer Datenbanken und Transaktionsprotokolle. Amazon RDS erstellt einen Snapshot für das Speichervolume Ihrer DB-Instance, sodass die gesamte DB-Instance gesichert wird. Sie können im System spezifische Aufbewahrungsfristen festlegen, um Ihre Ausfallsicherheitsanforderungen zu erfüllen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.308(a)(7)(ii)(A)	(A) Datensich erungsplan (erforder lich). Einrichtung und Implement ierung von Verfahren zur Erstellung und Aufbewahrung exakter, abrufbare r Kopien elektroni sch geschützter Gesundheitsinforma tionen.	dynamodb-in-backup-plan	Um Sie bei Datensich erungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon DynamoDB-Tabellen Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwaltet er Backup-Service mit einer richtlini enbasierten Backup-Lösung. Diese Lösung vereinfac ht Ihr Sicherung smanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforde rungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.308(a)(7)(ii)(A)	(A) Datensicherungsplan (erforderlich). Einrichtung und Implementierung von Verfahren zur Erstellung und Aufbewahrung exakter, abrufbarer Kopien elektronisch geschützter Gesundheitsinformationen.	dynamodb-pitr-enabled	Aktivieren Sie diese Regel, um zu überprüfen, ob die Informationen gesichert wurden. Es verwaltet auch die Backups, indem es sicherstellt, dass die point-in-time Wiederherstellung in Amazon DynamoDB aktiviert ist. Bei der Wiederherstellung werden fortlaufende Backups Ihrer Tabelle für die letzten 35 Tage gespeichert.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.308(a)(7)(ii)(A)	(A) Datensicherungsplan (erforderlich). Einrichtung und Implementierung von Verfahren zur Erstellung und Aufbewahrung exakter, abrufbarer Kopien elektronisch geschützter Gesundheitsinformationen.	ebs-in-backup-plan	Stellen Sie zur Unterstützung der Datensicherungsprozesse sicher, dass Ihre Amazon Elastic Block Store (Amazon EBS) -Volumes Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.308(a)(7)(ii)(A)	(A) Datensicherungsplan (erforderlich). Einrichtung und Implementierung von Verfahren zur Erstellung und Aufbewahrung exakter, abrufbarer Kopien elektronisch geschützter Gesundheitsinformationen.	efs-in-backup-plan	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon Elastic File System (Amazon EFS) -Dateisysteme Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.308(a)(7)(ii)(A)	(A) Datensicherungsplan (erforderlich). Einrichtung und Implementierung von Verfahren zur Erstellung und Aufbewahrung exakter, abrufbarer Kopien elektronisch geschützter Gesundheitsinformationen.	elasticache-redis-cluster-automatic-Backup-Check	Wenn automatische Backups aktiviert sind, ElastiCache erstellt Amazon täglich ein Backup des Clusters. Die Sicherung kann für eine von Ihrer Organisation festgelegte Anzahl von Tagen aufbewahrt werden. Automatische Backups schützen vor Datenverlust. Bei einem Ausfall können Sie einen neuen Cluster erstellen, der Ihre Daten aus dem aktuellen Backup wiederherstellt.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.308(a)(7)(ii)(A)	(A) Datensicherungsplan (erforderlich). Einrichtung und Implementierung von Verfahren zur Erstellung und Aufbewahrung exakter, abrufbarer Kopien elektronisch geschützter Gesundheitsinformationen.	rds-in-backup-plan	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon Relational Database Service (Amazon RDS) -Instances Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.308(a)(7)(ii)(A)	(A) Datensicherungsplan (erforderlich). Einrichtung und Implementierung von Verfahren zur Erstellung und Aufbewahrung exakter, abrufbarer Kopien elektronisch geschützter Gesundheitsinformationen.	redshift-backup-enabled	Stellen Sie zur Unterstützung der Datensicherungsprozesse sicher, dass Ihre Amazon-Redshift-Cluster über automatisierte Snapshots verfügen. Wenn automatisierte Snapshots für einen Cluster aktiviert sind, erstellt Redshift in regelmäßigen Abständen Snapshots dieses Clusters. Standardmäßig erstellt Redshift alle acht Stunden oder alle 5 GB einen Snapshot für jeden Knoten mit Datenänderungen oder je nachdem, was zuerst eintritt.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.308(a)(7)(ii)(A)	(A) Datensicherungsplan (erforderlich). Einrichtung und Implementierung von Verfahren zur Erstellung und Aufbewahrung exakter, abrufbarer Kopien elektronisch geschützter Gesundheitsinformationen.	s3- bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) unterstützt die Aufrechterhaltung einer angemessenen Kapazität und Verfügbarkeit. CRR ermöglicht das automatische, asynchrone Kopieren von Objekten in Amazon-S3-Buckets, um die Datenverfügbarkeit sicherzustellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.308(a)(7)(ii)(A)	(A) Datensicherungsplan (erforderlich). Einrichtung und Implementierung von Verfahren zur Erstellung und Aufbewahrung exakter, abrufbarer Kopien elektronisch geschützter Gesundheitsinformationen.	s-3 bucket-versioning-enabled	Die Versionsverwaltung von Amazon Simple Storage Service (Amazon S3)-Buckets hilft dabei, mehrere Varianten eines Objekts im selben Amazon-S3-Bucket zu speichern. Verwenden Sie die Versionsverwaltung, um sämtliche Versionen aller Objekte in Ihrem Amazon-S3-Bucket zu speichern, abzurufen oder wiederherzustellen. Mit der Versionsverwaltung können Sie Versionen sowohl nach unbeabsichtigten Benutzeraktionen als auch nach Anwendungsfehlern problemlos wiederherstellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.308(a)(7)(ii)(A)	(A) Datensicherungsplan (erforderlich). Einrichtung und Implementierung von Verfahren zur Erstellung und Aufbewahrung exakter, abrufbarer Kopien elektronisch geschützter Gesundheitsinformationen.	s-3 version-lifecycle-policy-check	Mit Amazon-S3-Lebenszyklusregeln können Sie Aktionen definieren, die Amazon S3 während der Lebensdauer eines Objekts ausführen soll (z. B. die Überführung von Objekten in eine andere Speicherklasse, ihre Archivierung oder Löschung nach einem bestimmten Zeitraum).

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.308(a)(7)(ii)(A)	(A) Datensicherungsplan (erforderlich). Einrichtung und Implementierung von Verfahren zur Erstellung und Aufbewahrung exakter, abrufbarer Kopien elektronisch geschützter Gesundheitsinformationen.	redshift-cluster-maintenancesettings-check	Diese Regel stellt sicher, dass Amazon-Redshift-Cluster die bevorzugten Einstellungen für Ihre Organisation haben. Insbesondere sorgt sie dafür, dass Cluster bevorzugte Wartungsfenster und automatisierte Aufbewahrungsfristen für Snapshots für die Datenbank haben. Für diese Regel müssen Sie die festlegen allowVersionUpgrade. Der Standardwert ist „true“. Außerdem können Sie optional den Zeitraum preferredMaintenanceWindow (der Standardwert ist sa: 16:00 -sa: 16:30) und den automated SnapshotRetention Zeitraum (der Standardwert ist 1) festlegen. Die tatsächlichen Werte müssen den Richtlini

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			en Ihrer Organisation entsprechen.
164.308(a)(7)(ii)(B)	(B) Notfallwiederherstellungsplan (erforderlich). Etablieren Sie Verfahren zur Wiederherstellung von Datenverlusten (und implementieren Sie sie nach Bedarf).	db-instance-backup-enabled	Die Sicherungsfunktion von Amazon RDS erstellt Sicherungen Ihrer Datenbanken und Transaktionsprotokolle. Amazon RDS erstellt einen Snapshot für das Speichervolume Ihrer DB-Instance, sodass die gesamte DB-Instance gesichert wird. Sie können im System spezifische Aufbewahrungsfristen festlegen, um Ihre Ausfallsicherheitsanforderungen zu erfüllen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.308(a)(7)(ii)(B)	(B) Notfallwiederherstellungsplan (erforderlich). Etablieren Sie Verfahren zur Wiederherstellung von Datenverlusten (und implementieren Sie sie nach Bedarf).	dynamodb-in-backup-plan	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon DynamoDB-Tabellen Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.308(a)(7)(ii)(B)	(B) Notfallwiederherstellungsplan (erforderlich). Etablieren Sie Verfahren zur Wiederherstellung von Datenverlusten (und implementieren Sie sie nach Bedarf).	dynamodb-pitr-enabled	Aktivieren Sie diese Regel, um zu überprüfen, ob die Informationen gesichert wurden. Es verwaltet auch die Backups, indem es sicherstellt, dass die point-in-time Wiederherstellung in Amazon DynamoDB aktiviert ist. Bei der Wiederherstellung werden fortlaufende Backups Ihrer Tabelle für die letzten 35 Tage gespeichert.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.308(a)(7)(ii)(B)	(B) Notfallwiederherstellungsplan (erforderlich). Etablieren Sie Verfahren zur Wiederherstellung von Datenverlusten (und implementieren Sie sie nach Bedarf).	ebs-in-backup-plan	Stellen Sie zur Unterstützung der Datensicherungsprozesse sicher, dass Ihre Amazon Elastic Block Store (Amazon EBS) -Volumes Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.308(a)(7)(ii)(B)	(B) Notfallwiederherstellungsplan (erforderlich). Etablieren Sie Verfahren zur Wiederherstellung von Datenverlusten (und implementieren Sie sie nach Bedarf).	efs-in-backup-plan	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon Elastic File System (Amazon EFS) -Dateisysteme Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.308(a)(7)(ii)(B)	(B) Notfallwiederherstellungsplan (erforderlich). Etablieren Sie Verfahren zur Wiederherstellung von Datenverlusten (und implementieren Sie sie nach Bedarf).	elasticache-redis-cluster-automatic-Backup-Check	Wenn automatische Backups aktiviert sind, ElastiCache erstellt Amazon täglich ein Backup des Clusters. Die Sicherung kann für eine von Ihrer Organisation festgelegte Anzahl von Tagen aufbewahrt werden. Automatische Backups schützen vor Datenverlust. Bei einem Ausfall können Sie einen neuen Cluster erstellen, der Ihre Daten aus dem aktuellen Backup wiederherstellt.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.308(a)(7)(ii)(B)	(B) Notfallwiederherstellungsplan (erforderlich). Etablieren Sie Verfahren zur Wiederherstellung von Datenverlusten (und implementieren Sie sie nach Bedarf).	rds-in-backup-plan	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon Relational Database Service (Amazon RDS) -Instances Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.308(a)(7)(ii)(B)	(B) Notfallwiederherstellungsplan (erforderlich). Etablieren Sie Verfahren zur Wiederherstellung von Datenverlusten (und implementieren Sie sie nach Bedarf).	redshift-backup-enabled	Stellen Sie zur Unterstützung der Datensicherungsprozesse sicher, dass Ihre Amazon-Redshift-Cluster über automatisierte Snapshots verfügen. Wenn automatisierte Snapshots für einen Cluster aktiviert sind, erstellt Redshift in regelmäßigen Abständen Snapshots dieses Clusters. Standardmäßig erstellt Redshift alle acht Stunden oder alle 5 GB einen Snapshot für jeden Knoten mit Datenänderungen oder je nachdem, was zuerst eintritt.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.308(a)(7)(ii)(B)	(B) Notfallwiederherstellungsplan (erforderlich). Etablieren Sie Verfahren zur Wiederherstellung von Datenverlusten (und implementieren Sie sie nach Bedarf).	s3- bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) unterstützt die Aufrechterhaltung einer angemessenen Kapazität und Verfügbarkeit. CRR ermöglicht das automatische, asynchrone Kopieren von Objekten in Amazon-S3-Buckets, um die Datenverfügbarkeit sicherzustellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.308(a)(7)(ii)(B)	(B) Notfallwiederherstellungsplan (erforderlich). Etablieren Sie Verfahren zur Wiederherstellung von Datenverlusten (und implementieren Sie sie nach Bedarf).	s-3 bucket-versioning-enabled	Die Versionsverwaltung von Amazon Simple Storage Service (Amazon S3)-Buckets hilft dabei, mehrere Varianten eines Objekts im selben Amazon-S3-Bucket zu speichern. Verwenden Sie die Versionsverwaltung, um sämtliche Versionen aller Objekte in Ihrem Amazon-S3-Bucket zu speichern, abzurufen oder wiederherzustellen. Mit der Versionsverwaltung können Sie Versionen sowohl nach unbeabsichtigten Benutzeraktionen als auch nach Anwendungsfehlern problemlos wiederherstellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.308(a)(7)(ii)(B)	(B) Notfallwiederherstellungsplan (erforderlich). Etablieren Sie Verfahren zur Wiederherstellung von Datenverlusten (und implementieren Sie sie nach Bedarf).	s-3 version-lifecycle-policy-check	Mit Amazon-S3-Lebenszyklusregeln können Sie Aktionen definieren, die Amazon S3 während der Lebensdauer eines Objekts ausführen soll (z. B. die Überführung von Objekten in eine andere Speicherklasse, ihre Archivierung oder Löschung nach einem bestimmten Zeitraum).

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.308(a)(7)(ii)(C)	(C) Betriebsplan für den Notfallmodus (erforderlich). Etablieren (und nach Bedarf implementieren) Sie Verfahren, um die Fortführung kritischer Geschäftsprozesse zum Schutz von elektronisch geschützten Gesundheitsinformationen im Notfallmodus zu ermöglichen.	dynamodb-autoscaling-enabled	Amazon DynamoDB Auto Scaling verwendet den AWS Application Auto Scaling-Service, um die bereitgestellte Durchsatzkapazität so anzupassen, dass sie automatisch auf tatsächliche Verkehrsmuster reagiert. Auf diese Weise kann eine Tabelle oder ein globaler sekundärer Index die bereitgestellte Lese-/Schreibkapazität erhöhen, um plötzliche Erhöhungen des Datenverkehrs ohne Drosselung zu bewältigen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.308(a)(7)(ii)(C)	(C) Betriebsplan für den Notfallmodus (erforderlich). Etablieren (und nach Bedarf implementieren) Sie Verfahren, um die Fortführung kritischer Geschäftsprozesse zum Schutz von elektronisch geschützten Gesundheitsinformationen im Notfallmodus zu ermöglichen.	elb-cross-zone-load-Balancing aktiviert	Aktivieren Sie zonenübergreifendes Load Balancing für Ihre Elastic Load Balancer (ELBs), um eine angemessene Kapazität und Verfügbarkeit aufrechtzuerhalten. Zonenübergreifendes Load Balancing reduziert die Notwendigkeit, die gleiche Anzahl von Instances in jeder aktivierten Availability Zone aufrechtzuerhalten. Es verbessert auch die Fähigkeit Ihrer Anwendung, den Verlust einer oder mehrerer Instances zu bewältigen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.308(a)(7)(ii)(C)	(C) Betriebsplan für den Notfallmodus (erforderlich). Etablieren (und nach Bedarf implementieren) Sie Verfahren, um die Fortführung kritischer Geschäftsprozesse zum Schutz von elektronisch geschützten Gesundheitsinformationen im Notfallmodus zu ermöglichen.	elb-deletion-protection-enabled	Diese Regel sorgt dafür, dass der Löschschutz für Elastic Load Balancing aktiviert ist. Verwenden Sie diese Funktion, um zu verhindern, dass Ihr Load Balancer versehentlich oder böswillig gelöscht wird, was zum Verlust der Verfügbarkeit Ihrer Anwendungen führen kann.
164.308(a)(7)(ii)(C)	(C) Betriebsplan für den Notfallmodus (erforderlich). Etablieren (und nach Bedarf implementieren) Sie Verfahren, um die Fortführung kritischer Geschäftsprozesse zum Schutz von elektronisch geschützten Gesundheitsinformationen im Notfallmodus zu ermöglichen.	rds-cluster-deletion-protection-aktiviert	Stellen Sie sicher, dass Amazon Relational Database Service (Amazon RDS)-Instances den Löschschutz aktiviert haben. Verwenden Sie den Löschschutz, um zu verhindern, dass Ihre Amazon-RDS-Instances versehentlich oder böswillig gelöscht werden, was zum Verlust der Verfügbarkeit Ihrer Anwendungen führen kann.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.308(a)(7)(ii)(C)	(C) Betriebsplan für den Notfallmodus (erforderlich). Etablieren (und nach Bedarf implementieren) Sie Verfahren, um die Fortführung kritischer Geschäftsprozesse zum Schutz von elektronisch geschützten Gesundheitsinformationen im Notfallmodus zu ermöglichen.	rds-multi-az-support	Die Multi-AZ-Unterstützung in Amazon Relational Database Service (Amazon RDS) bietet eine verbesserte Verfügbarkeit und Beständigkeit von Datenbank-Instances. Wenn Sie eine Multi-AZ-Datenbank-Instance bereitstellen, erstellt Amazon RDS automatisch eine primäre Datenbank-Instance und repliziert die Daten synchron auf eine Standby-Instance in einer anderen Availability Zone. Jede Availability Zone läuft auf einer eigenen, physisch getrennten, unabhängigen Infrastruktur und ist auf eine hohe Verfügbarkeit ausgelegt. Im Falle eines Infrastrukturausfalls führt Amazon RDS einen automatis

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			chen Failover zum Standby-Modus durch, sodass Sie den Datenbankbetrieb wieder aufnehmen können, sobald der Failover abgeschlo ssen ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.308(a)(7)(ii)(C)	(C) Betriebsplan für den Notfallmodus (erforderlich). Etablieren (und nach Bedarf implementieren) Sie Verfahren, um die Fortführung kritischer Geschäftsprozesse zum Schutz von elektronisch geschützten Gesundheitsinformationen im Notfallmodus zu ermöglichen.	vpc-vpn-2-tunnels-up	Redundante Site-to-Site VPN-Tunnel können implementiert werden, um die Anforderungen an die Ausfallsicherheit zu erfüllen. Es verwendet zwei Tunnel, um die Konnektivität sicherzustellen, falls eine der Site-to-Site VPN-Verbindungen nicht verfügbar ist. Um sich vor einem Verbindungsverlust zu schützen, können Sie für den Fall, dass Ihr Kunden-Gateway nicht verfügbar ist, eine zweite Site-to-Site VPN-Verbindung zu Ihrer Amazon Virtual Private Cloud (Amazon VPC) und Ihrem Virtual Private Gateway einrichten, indem Sie ein zweites Kunden-Gateway verwenden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.308(a)(8)	(8) Standard: Bewertung. Führen Sie eine regelmäßige technische und nichttechnische Bewertung durch, die zunächst auf den im Rahmen dieser Regel eingeführten Standards basiert und anschließend als Reaktion auf Umgebungs- oder Verfahrensänderungen mit Auswirkungen auf die Sicherheit elektronisch geschützter Gesundheitsinformationen und feststellt, inwieweit die Sicherheitsrichtlinien und -verfahren einer Entität den Anforderungen dieses Unterabschnitts entsprechen.	securityhub-enabled	AWS Security Hub hilft bei der Überwachung von unbefugtem Personal, Verbindungen, Geräten und Software. AWS Security Hub aggregiert, organisiert und priorisiert die Sicherheitswarnungen oder Ergebnisse mehrerer Dienste. AWS Einige dieser Dienste sind Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer und AWS Firewall Manager sowie AWS Partnerlösungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.308(a)(8)	(8) Standard: Bewertung. Führen Sie eine regelmäßige technische und nichttechnische Bewertung durch, die zunächst auf den im Rahmen dieser Regel eingeführten Standards basiert und anschließend als Reaktion auf Umgebungs- oder Verfahrensänderungen mit Auswirkungen auf die Sicherheit elektronisch geschützter Gesundheitsinformationen und feststellt, inwieweit die Sicherheitsrichtlinien und -verfahren einer Entität den Anforderungen dieses Unterabschnitts entsprechen.	guardduty-enabled-centralized	Amazon GuardDuty kann mithilfe von Threat Intelligence Feeds helfen, potenzielle Cybersicherheitsereignisse zu überwachen und zu erkennen. Dazu gehören Listen mit bösartigen IPs und maschinellen Lernmethoden zur Identifizierung unerwarteter, nicht autorisierter und bösartiger Aktivitäten in Ihrer AWS Cloud-Umgebung.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.312(a)(1)	(a) (1) Standard: Zugriffskontrolle. Implementieren Sie technische Richtlinien und Verfahren für elektronische Informationssysteme, in denen elektronisch geschützte Gesundheitsinformationen gespeichert werden, sodass nur Personen oder Softwareprogramme darauf zugreifen können, denen Zugriffsrechte gemäß 164.308(a)(4) gewährt wurden.	ec2-imdsv2-check	Stellen Sie sicher, dass die Methode Instance Metadata Service Version 2 (IMDSv2) aktiviert ist, um den Zugriff auf und die Kontrolle der Amazon Elastic Compute Cloud (Amazon EC2) - Instance-Metadaten zu schützen. Die IMDSv2 Methode verwendet sitzungsbasierte Kontrollen. Mit können Kontrollen implementiert werden IMDSv2, um Änderungen an Instanzmetadaten einzuschränken.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.312(a)(1)	(a) (1) Standard: Zugriffskontrolle. Implementieren Sie technische Richtlinien und Verfahren für elektronische Informationssysteme, in denen elektronisch geschützte Gesundheitsinformationen gespeichert werden, sodass nur Personen oder Softwareprogramme darauf zugreifen können, denen Zugriffsrechte gemäß 164.308(a)(4) gewährt wurden.	emr-kerberos-enabled	Die Zugriffsberechtigungen und -autorisierungen können verwaltet und nach den Prinzipien der geringsten Berechtigung und Aufgabentrennung integriert werden, indem Kerberos für Amazon-EMR-Cluster aktiviert wird. In Kerberos werden Services und Benutzer, die sich authentifizieren müssen, als Prinzipale bezeichnet. Prinzipale befinden sich in einem Kerberos-Bereich. Innerhalb dieses Bereichs wird ein Kerberos-Server als Key Distribution Center (KDC) bezeichnet. Über diesen Server können sich Prinzipale authentifizieren. Die Authentifizierung im KDC erfolgt durch die Ausstellung von Authentif

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			izierungstickets. Das KDC unterhält eine Datenbank der Prinzipale in seinem Bereich mit ihren Passwörtern und anderen administr ativen Informationen zu jedem Prinzipal.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.312(a)(1)	(a) (1) Standard: Zugriffskontrolle. Implementieren Sie technische Richtlinien und Verfahren für elektronische Informationssysteme, in denen elektronisch geschützte Gesundheitsinformationen gespeichert werden, sodass nur Personen oder Softwareprogramme darauf zugreifen können, denen Zugriffsrechte gemäß 164.308(a)(4) gewährt wurden.	iam-customer-policy-blocked-kms-Aktionen	AWS Identity and Access Management (IAM) kann Ihnen helfen, die Prinzipien der geringsten Rechte und der Aufgabentrennung in Zugriffsberechtigungen und Autorisierungen zu integrieren und so zu verhindern, dass Richtlinien blockierte Aktionen für alle AWS Schlüssel des Key Management Service enthalten. Wenn Benutzer mehr Rechte haben, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und Aufgabentrennung verstoßen. Mit dieser Regel können Sie den Parameter festlegen. blockedActionsPatterns (Wert „AWS Bewährte grundlegende Sicherheitsmethoden“: kms:

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			Decrypt, kms:ReEncryptFrom). Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.312(a)(1)	(a) (1) Standard: Zugriffskontrolle. Implementieren Sie technische Richtlinien und Verfahren für elektronische Informationssysteme, in denen elektronisch geschützte Gesundheitsinformationen gespeichert werden, sodass nur Personen oder Softwareprogramme darauf zugreifen können, denen Zugriffsrechte gemäß 164.308(a)(4) gewährt wurden.	iam-inline-policy-blocked-kms-Aktionen	Stellen Sie sicher, dass ein Benutzer, eine IAM-Rolle oder eine IAM-Gruppe (AWS Identity and Access Management) nicht über eine Inline-Richtlinie verfügt, die blockierte Aktionen für alle AWS Schlüssel des Key Management Service zulässt. AWS empfiehlt, verwaltete Richtlinien anstelle von Inline-Richtlinien zu verwenden. Verwaltete Richtlinien ermöglichen Wiederverwendbarkeit, Versionsverwaltung, Rollback und Delegierung der Berechtigungsverwaltung. Mit dieser Regel können Sie den blockedActionsPatterns Parameter festlegen. (Wert „AWS Bewährte grundlegende Sicherheitsmethoden“: kms:Decrypt, kms:ReEncryptFrom). Die

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.
164.312(a)(1)	(a) (1) Standard: Zugriffskontrolle. Implementieren Sie technische Richtlinien und Verfahren für elektronische Informationssysteme, in denen elektronisch geschützte Gesundheitsinformationen gespeichert werden, sodass nur Personen oder Softwareprogramme darauf zugreifen können, denen Zugriffsrechte gemäß 164.308(a)(4) gewährt wurden.	iam-no-inline-policy-überprüfen	Stellen Sie sicher, dass ein Benutzer, eine IAM-Rolle oder eine IAM-Gruppe (AWS Identity and Access Management) nicht über eine Inline-Richtlinie zur Zugriffskontrolle auf Systeme und Ressourcen verfügt. AWS empfiehlt, verwaltete Richtlinien anstelle von Inline-Richtlinien zu verwenden. Verwaltete Richtlinien ermöglichen Wiederverwendbarkeit, Versionsverwaltung, Rollback und Delegierung der Berechtigungsverwaltung.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.312(a)(1)	(a) (1) Standard: Zugriffskontrolle. Implementieren Sie technische Richtlinien und Verfahren für elektronische Informationssysteme, in denen elektronisch geschützte Gesundheitsinformationen gespeichert werden, sodass nur Personen oder Softwareprogramme darauf zugreifen können, denen Zugriffsrechte gemäß 164.308(a)(4) gewährt wurden.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) kann Ihnen dabei helfen, die Prinzipien der geringsten Rechte und der Aufgabentrennung in Zugriffsberechtigungen und Autorisierungen zu integrieren und so zu verhindern, dass Richtlinien „Effect“: „Allow“ mit „Action“: „*“ anstelle von „Resource“: „*“ enthalten. Wenn Benutzern mehr Rechte eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und der Aufgabentrennung verstoßen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.312(a)(1)	(a) (1) Standard: Zugriffskontrolle. Implementieren Sie technische Richtlinien und Verfahren für elektronische Informationssysteme, in denen elektronisch geschützte Gesundheitsinformationen gespeichert werden, sodass nur Personen oder Softwareprogramme darauf zugreifen können, denen Zugriffsrechte gemäß 164.308(a)(4) gewährt wurden.	iam-root-access-key-überprüfen	Der Zugriff auf Systeme und Ressourcen kann gesteuert werden, indem überprüft wird, ob der Root-Benutzer keine Zugriffsschlüssel mit seiner AWS Identity and Access Management (IAM) -Rolle verknüpft hat. Stellen Sie sicher, dass die Root-Zugriffsschlüssel gelöscht werden. Erstellen und verwenden Sie stattdessen rollenbasierte Funktionen, AWS-Konten um das Prinzip der geringsten Funktionalität zu berücksichtigen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.312(a)(1)	(a) (1) Standard: Zugriffskontrolle. Implementieren Sie technische Richtlinien und Verfahren für elektronische Informationssysteme, in denen elektronisch geschützte Gesundheitsinformationen gespeichert werden, sodass nur Personen oder Softwareprogramme darauf zugreifen können, denen Zugriffsrechte gemäß 164.308(a)(4) gewährt wurden.	iam-user-no-policies-überprüfen	Diese Regel stellt sicher, dass AWS Identity and Access Management (IAM) -Richtlinien nur Gruppen oder Rollen zugewiesen werden, um den Zugriff auf Systeme und Ressourcen zu kontrollieren. Die Zuweisung von Berechtigungen auf Gruppen- oder Rollenebene trägt dazu bei, die Wahrscheinlichkeit zu verringern, dass eine Identität übermäßige Berechtigungen erhält oder beibehält.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.312(a)(1)	(a) (1) Standard: Zugriffskontrolle. Implementieren Sie technische Richtlinien und Verfahren für elektronische Informationssysteme, in denen elektronisch geschützte Gesundheitsinformationen gespeichert werden, sodass nur Personen oder Softwareprogramme darauf zugreifen können, denen Zugriffsrechte gemäß 164.308(a)(4) gewährt wurden.	iam-user-unused-credentials-überprüfen	AWS Identity and Access Management (IAM) kann Ihnen bei Zugriffsberechtigungen und Autorisierungen helfen, indem es nach IAM-Passwörtern und Zugriffsschlüsseln sucht, die für einen bestimmten Zeitraum nicht verwendet wurden. Wenn ungenutzte Anmeldeinformationen identifiziert werden, müssen Sie sie deaktivieren und/oder entfernen, da dies gegen das Prinzip der geringsten Berechtigung verstoßen könnte. Für diese Regel müssen Sie einen Wert für das maxCredentialUsage Alter festlegen (Standardkonfiguration: 90). Der tatsächliche Wert muss den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.312(a)(1)	(a) (1) Standard: Zugriffskontrolle. Implementieren Sie technische Richtlinien und Verfahren für elektronische Informationssysteme, in denen elektronisch geschützte Gesundheitsinformationen gespeichert werden, sodass nur Personen oder Softwareprogramme darauf zugreifen können, denen Zugriffsrechte gemäß 164.308(a)(4) gewährt wurden.	iam-policy-no-statements-with-full-access	Stellen Sie sicher, dass IAM-Aktionen nur auf die benötigten Aktionen beschränkt sind. Wenn Benutzern mehr Rechte eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und der Aufgabentrennung verstoßen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.312(a)(1)	(a) (1) Standard: Zugriffskontrolle. Implementieren Sie technische Richtlinien und Verfahren für elektronische Informationssysteme, in denen elektronisch geschützte Gesundheitsinformationen gespeichert werden, sodass nur Personen oder Softwareprogramme darauf zugreifen können, denen Zugriffsrechte gemäß 164.308(a)(4) gewährt wurden.	ec2- instance-profile-attached	EC2 Instanzprofile übergeben eine IAM-Rolle an eine Instanz EC2 . Das Anhängen eines Instance-Profils an Ihre Instances kann bei der Implementierung von geringsten Berechtigungen und der Berechtigungsverwaltung helfen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.312(a)(1)	(a) (1) Standard: Zugriffskontrolle. Implementieren Sie technische Richtlinien und Verfahren für elektronische Informationssysteme, in denen elektronisch geschützte Gesundheitsinformationen gespeichert werden, sodass nur Personen oder Softwareprogramme darauf zugreifen können, denen Zugriffsrechte gemäß 164.308(a)(4) gewährt wurden.	dms-replication-not-public	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass auf DMS-Replikationsinstanzen nicht öffentlich zugegriffen werden kann. DMS-Replikations-Instances können vertrauliche Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.312(a)(1)	(a) (1) Standard: Zugriffskontrolle. Implementieren Sie technische Richtlinien und Verfahren für elektronische Informationssysteme, in denen elektronisch geschützte Gesundheitsinformationen gespeichert werden, sodass nur Personen oder Softwareprogramme darauf zugreifen können, denen Zugriffsrechte gemäß 164.308(a)(4) gewährt wurden.	ebs-snapshot-public-restorable-überprüfen	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass EBS-Snapshots nicht öffentlich wiederherstellbar sind. EBS-Volume-Snapshots können vertrauliche Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.312(a)(1)	(a) (1) Standard: Zugriffskontrolle. Implementieren Sie technische Richtlinien und Verfahren für elektronische Informationssysteme, in denen elektronisch geschützte Gesundheitsinformationen gespeichert werden, sodass nur Personen oder Softwareprogramme darauf zugreifen können, denen Zugriffsrechte gemäß 164.308(a)(4) gewährt wurden.	ec-2 instance-no-public-ip	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon Elastic Compute Cloud (Amazon EC2) - Instances nicht öffentlich zugänglich sind. EC2 Amazon-Instances können vertrauliche Informationen enthalten, und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.312(a)(1)	(a) (1) Standard: Zugriffskontrolle. Implementieren Sie technische Richtlinien und Verfahren für elektronische Informationssysteme, in denen elektronisch geschützte Gesundheitsinformationen gespeichert werden, sodass nur Personen oder Softwareprogramme darauf zugreifen können, denen Zugriffsrechte gemäß 164.308(a)(4) gewährt wurden.	elasticsearch-in-vpc-only	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass sich Amazon OpenSearch OpenSearch Service (Service) - Domains innerhalb einer Amazon Virtual Private Cloud (Amazon VPC) befinden. Eine OpenSearch Service-Domain innerhalb einer Amazon VPC ermöglicht die sichere Kommunikation zwischen OpenSearch Service und anderen Services innerhalb der Amazon VPC, ohne dass ein Internet-Gateway, ein NAT-Gerät oder eine VPN-Verbindung erforderlich ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.312(a)(1)	(a) (1) Standard: Zugriffskontrolle. Implementieren Sie technische Richtlinien und Verfahren für elektronische Informationssysteme, in denen elektronisch geschützte Gesundheitsinformationen gespeichert werden, sodass nur Personen oder Softwareprogramme darauf zugreifen können, denen Zugriffsrechte gemäß 164.308(a)(4) gewährt wurden.	emr-master-no-public-ip	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon EMR-Cluster-Masterknoten nicht öffentlich zugänglich sind. Amazon-EMR-Cluster-Hauptknoten können vertrauliche Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.312(a)(1)	(a) (1) Standard: Zugriffskontrolle. Implementieren Sie technische Richtlinien und Verfahren für elektronische Informationssysteme, in denen elektronisch geschützte Gesundheitsinformationen gespeichert werden, sodass nur Personen oder Softwareprogramme darauf zugreifen können, denen Zugriffsrechte gemäß 164.308(a)(4) gewährt wurden.	ec-2 instances-in-vpc	Stellen Sie Amazon Elastic Compute Cloud (Amazon EC2) -Instances innerhalb einer Amazon Virtual Private Cloud (Amazon VPC) bereit, um eine sichere Kommunikation zwischen einer Instance und anderen Services innerhalb der Amazon VPC zu ermöglichen, ohne dass ein Internet-Gateway, ein NAT-Gerät oder eine VPN-Verbindung erforderlich ist. Der gesamte Datenverkehr bleibt sicher in der AWS Cloud. Domains, die sich innerhalb einer VPC befinden, verfügen aufgrund ihrer logischen Isolierung im Vergleich zu Domains mit öffentlichen Endpunkten über eine zusätzliche Sicherheitsebene. Weisen Sie EC2

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			Amazon-Instances einer Amazon-VPC zu, um den Zugriff ordnungsgemäß zu verwalten.
164.312(a)(1)	(a) (1) Standard: Zugriffskontrolle. Implementieren Sie technische Richtlinien und Verfahren für elektronische Informationssysteme, in denen elektronisch geschützte Gesundheitsinformationen gespeichert werden, sodass nur Personen oder Softwareprogramme darauf zugreifen können, denen Zugriffsrechte gemäß 164.308(a)(4) gewährt wurden.	internet-gateway-authorized-vpc-nur	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Internet-Gateways nur mit autorisierter Amazon Virtual Private Cloud (Amazon VPC) verbunden sind. Internet-Gateways ermöglichen den bidirektionalen Internetzugang zur und von der Amazon VPC, was möglicherweise zu einem unbefugten Zugriff auf Amazon-VPC-Ressourcen führen kann.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.312(a)(1)	(a) (1) Standard: Zugriffskontrolle. Implementieren Sie technische Richtlinien und Verfahren für elektronische Informationssysteme, in denen elektronisch geschützte Gesundheitsinformationen gespeichert werden, sodass nur Personen oder Softwareprogramme darauf zugreifen können, denen Zugriffsrechte gemäß 164.308(a)(4) gewährt wurden.	lambda-function-public-access-verboten	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass AWS Lambda-Funktionen nicht öffentlich zugänglich sind. Der öffentliche Zugriff kann möglicherweise die Verfügbarkeit von Ressourcen beeinträchtigen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.312(a)(1)	(a) (1) Standard: Zugriffskontrolle. Implementieren Sie technische Richtlinien und Verfahren für elektronische Informationssysteme, in denen elektronisch geschützte Gesundheitsinformationen gespeichert werden, sodass nur Personen oder Softwareprogramme darauf zugreifen können, denen Zugriffsrechte gemäß 164.308(a)(4) gewährt wurden.	rds-instance-public-access-überprüfen	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Relational Database Service (Amazon RDS) -Instances nicht öffentlich sind. Amazon-RDS-Datenbank-Instances können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.312(a)(1)	(a) (1) Standard: Zugriffskontrolle. Implementieren Sie technische Richtlinien und Verfahren für elektronische Informationssysteme, in denen elektronisch geschützte Gesundheitsinformationen gespeichert werden, sodass nur Personen oder Softwareprogramme darauf zugreifen können, denen Zugriffsrechte gemäß 164.308(a)(4) gewährt wurden.	rds-snapshots-public-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Relational Database Service (Amazon RDS) -Instances nicht öffentlich sind. Amazon-RDS-Datenbank-Instances können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.312(a)(1)	(a) (1) Standard: Zugriffskontrolle. Implementieren Sie technische Richtlinien und Verfahren für elektronische Informationssysteme, in denen elektronisch geschützte Gesundheitsinformationen gespeichert werden, sodass nur Personen oder Softwareprogramme darauf zugreifen können, denen Zugriffsrechte gemäß 164.308(a)(4) gewährt wurden.	redshift-cluster-public-access-überprüfen	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Redshift Redshift-Cluster nicht öffentlich sind. Amazon-Redshift-Cluster können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.312(a)(1)	(a) (1) Standard: Zugriffskontrolle. Implementieren Sie technische Richtlinien und Verfahren für elektronische Informationssysteme, in denen elektronisch geschützte Gesundheitsinformationen gespeichert werden, sodass nur Personen oder Softwareprogramme darauf zugreifen können, denen Zugriffsrechte gemäß 164.308(a)(4) gewährt wurden.	s3- -Block-periodisch account-level-public-access	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Simple Storage Service (Amazon S3) -Buckets nicht öffentlich zugänglich sind. Diese Regel trägt dazu bei, sensible Daten vor unbefugten Remote-Benutzern zu schützen, indem sie den öffentlichen Zugriff verhindert. Mit dieser Regel können Sie optional die Parameter ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) und restrictPublicBuckets Parameter (Config Default: True) festlegen. Die tatsächlichen Werte müssen den Richtlini

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			en Ihrer Organisation entsprechen.
164.312(a)(1)	(a) (1) Standard: Zugriffskontrolle. Implementieren Sie technische Richtlini en und Verfahren für elektronische Informationssysteme, in denen elektronisch geschützte Gesundhei tsinformationen gespeichert werden, sodass nur Personen oder Softwarep rogramme darauf zugreifen können, denen Zugriffsrechte gemäß 164.308(a)(4) gewährt wurden.	s3- bucket-public-read -prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie nur autorisierten Benutzern, Prozessen und Geräten Zugriff auf Amazon Simple Storage Service (Amazon S3) - Buckets gewähren. Die Verwaltung des Zugriffs sollte mit der Klassifizierung der Daten übereinst immen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.312(a)(1)	(a) (1) Standard: Zugriffskontrolle. Implementieren Sie technische Richtlinien und Verfahren für elektronische Informationssysteme, in denen elektronisch geschützte Gesundheitsinformationen gespeichert werden, sodass nur Personen oder Softwareprogramme darauf zugreifen können, denen Zugriffsrechte gemäß 164.308(a)(4) gewährt wurden.	s3- bucket-public-write-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie nur autorisierten Benutzern, Prozessen und Geräten Zugriff auf Amazon Simple Storage Service (Amazon S3) - Buckets gewähren. Die Verwaltung des Zugriffs sollte mit der Klassifizierung der Daten übereinstimmen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.312(a)(1)	(a) (1) Standard: Zugriffskontrolle. Implementieren Sie technische Richtlinien und Verfahren für elektronische Informationssysteme, in denen elektronisch geschützte Gesundheitsinformationen gespeichert werden, sodass nur Personen oder Softwareprogramme darauf zugreifen können, denen Zugriffsrechte gemäß 164.308(a)(4) gewährt wurden.	sagemaker-notebook-no-direct-Internetzugang	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass SageMaker Amazon-Notebooks keinen direkten Internetzugang zulassen. Indem Sie direkten Internetzugang blockieren, vermeiden Sie, dass unbefugte Benutzer auf sensible Daten zugreifen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.312(a)(1)	(a) (1) Standard: Zugriffskontrolle. Implementieren Sie technische Richtlinien und Verfahren für elektronische Informationssysteme, in denen elektronisch geschützte Gesundheitsinformationen gespeichert werden, sodass nur Personen oder Softwareprogramme darauf zugreifen können, denen Zugriffsrechte gemäß 164.308(a)(4) gewährt wurden.	subnet-auto-assign-public-ip-deaktiviert	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon Virtual Private Cloud (VPC) -Subnetzen nicht automatisch eine öffentliche IP-Adresse zugewiesen wird. Amazon Elastic Compute Cloud (EC2) -Instances, die in Subnetzen gestartet werden, in denen dieses Attribut aktiviert ist, haben ihrer primären Netzwerkschnittstelle eine öffentliche IP-Adresse zugewiesen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.312(a)(1)	(a) (1) Standard: Zugriffskontrolle. Implementieren Sie technische Richtlinien und Verfahren für elektronische Informationssysteme, in denen elektronisch geschützte Gesundheitsinformationen gespeichert werden, sodass nur Personen oder Softwareprogramme darauf zugreifen können, denen Zugriffsrechte gemäß 164.308(a)(4) gewährt wurden.	ecs-task-definition-user-for-host-mode-check	Wenn für eine Aufgabendefinition erhöhte Berechtigungen gelten, liegt das daran, dass der Kunde diesen Konfigurationen ausdrücklich zugestimmt hat. Diese Kontrolle prüft, ob eine unerwartete Berechtigungseskalation vorliegt, wenn für eine Aufgabendefinition das Host-Netzwerk aktiviert ist, die Kunden aber keine erhöhten Berechtigungen aktiviert haben.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.312(a)(1)	(a) (1) Standard: Zugriffskontrolle. Implementieren Sie technische Richtlinien und Verfahren für elektronische Informationssysteme, in denen elektronisch geschützte Gesundheitsinformationen gespeichert werden, sodass nur Personen oder Softwareprogramme darauf zugreifen können, denen Zugriffsrechte gemäß 164.308(a)(4) gewährt wurden.	codebuild-project-envvar-awscred-überprüfen	Stellen Sie sicher, dass die Anmeldeinformationen AWS_ACCESS_KEY_ID AWS_SECRET_ACCESS_KEY nicht in AWS Codebuild-Projektumgebungen vorhanden sind. Speichern Sie diese Variablen nicht als Klartext. Das Speichern dieser Variablen als Klartext bewirkt eine unbeabsichtigte Offenlegung von Daten sowie unberechtigte Zugriffe.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.312(a)(1)	(a) (1) Standard: Zugriffskontrolle. Implementieren Sie technische Richtlinien und Verfahren für elektronische Informationssysteme, in denen elektronisch geschützte Gesundheitsinformationen gespeichert werden, sodass nur Personen oder Softwareprogramme darauf zugreifen können, denen Zugriffsrechte gemäß 164.308(a)(4) gewährt wurden.	codebuild-project-source-repo-URL-Prüfung	Stellen Sie sicher, dass die URL des Quell-Repositorys GitHub oder des Bitbucket-Quell-Repositorys keine persönlichen Zugriffstoken oder Anmeldeinformationen in Codebuild-Projektumgebungen enthält. AWS Verwende OAuth anstelle von persönlichen Zugriffstoken oder Anmeldedaten die Autorisierung für den Zugriff auf GitHub Bitbucket-Repositorys.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.312(a)(1)	(a) (1) Standard: Zugriffskontrolle. Implementieren Sie technische Richtlinien und Verfahren für elektronische Informationssysteme, in denen elektronisch geschützte Gesundheitsinformationen gespeichert werden, sodass nur Personen oder Softwareprogramme darauf zugreifen können, denen Zugriffsrechte gemäß 164.308(a)(4) gewährt wurden.	restricted-common-ports	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass gemeinsame Ports für Amazon Elastic Compute Cloud (Amazon EC2) -Sicherheitsgruppen eingeschränkt sind. Wenn der Zugriff auf Ports nicht auf vertrauenswürdige Quellen beschränkt wird, kann dies zu Angriffen auf die Verfügbarkeit, Integrität und Vertraulichkeit von Systemen führen. Mit dieser Regel können Sie optional die Parameter blockedPort1–blockedPort5 festlegen (Standardkonfigurationen: 20, 21, 3389, 3306, 4333). Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.312(a)(1)	(a) (1) Standard: Zugriffskontrolle. Implementieren Sie technische Richtlini en und Verfahren für elektronische Informationssysteme, in denen elektronisch geschützte Gesundhei tsinformationen gespeichert werden, sodass nur Personen oder Softwarep rogramme darauf zugreifen können, denen Zugriffsrechte gemäß 164.308(a)(4) gewährt wurden.	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) Security Groups können bei der Verwaltung des Netzwerkzugriffs helfen, indem sie eine statusbeh aftete Filterung von eingehendem und ausgehendem Netzwerkverkehr zu Ressourcen bereitste llen. AWS Wenn Sie eingehenden (oder entfernten) Datenverk ehr von 0.0.0.0/0 bis Port 22 auf Ihren Ressourcen nicht zulassen, können Sie den Remote-Zugriff einschränken.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.312(a)(1)	(a) (1) Standard: Zugriffskontrolle. Implementieren Sie technische Richtlinien und Verfahren für elektronische Informationssysteme, in denen elektronisch geschützte Gesundheitsinformationen gespeichert werden, sodass nur Personen oder Softwareprogramme darauf zugreifen können, denen Zugriffsrechte gemäß 164.308(a)(4) gewährt wurden.	autoscaling-launch-config-public-ip-deaktiviert	Wenn Sie Ihre Netzwerkschnittstellen mit einer öffentlichen IP-Adresse konfigurieren, sind die diesen Netzwerkschnittstellen zugehörigen Ressourcen über das Internet erreichbar. EC2 Ressourcen sollten nicht öffentlich zugänglich sein, da dies einen unbeabsichtigten Zugriff auf Ihre Anwendungen oder Server ermöglichen kann.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.312(a)(1)	(a) (1) Standard: Zugriffskontrolle. Implementieren Sie technische Richtlinien und Verfahren für elektronische Informationssysteme, in denen elektronisch geschützte Gesundheitsinformationen gespeichert werden, sodass nur Personen oder Softwareprogramme darauf zugreifen können, denen Zugriffsrechte gemäß 164.308(a)(4) gewährt wurden.	ecs-containers-readonly-access	Die Aktivierung des schreibgeschützten Zugriffs auf Amazon Elastic Container Service (ECS)-Container kann dazu beitragen, das Prinzip der geringsten Berechtigung einzuhalten. Diese Option kann Angriffsvektoren reduzieren, da das Dateisystem der Container-Instance nur geändert werden kann, wenn es über ausdrückliche Lese- und Schreibberechtigungen verfügt.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.312(a)(1)	(a) (1) Standard: Zugriffskontrolle. Implementieren Sie technische Richtlinien und Verfahren für elektronische Informationssysteme, in denen elektronisch geschützte Gesundheitsinformationen gespeichert werden, sodass nur Personen oder Softwareprogramme darauf zugreifen können, denen Zugriffsrechte gemäß 164.308(a)(4) gewährt wurden.	ssm-document-not-public	Stellen Sie sicher, dass AWS Systems Manager (SSM) - Dokumente nicht öffentlich sind, da dies einen unbeabsichtigten Zugriff auf Ihre SSM-Dokumente ermöglichen kann. Ein öffentliches SSM-Dokument kann Informationen über Ihr Konto, Ihre Ressourcen und internen Prozesse preisgeben.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.312(a)(1)	(a) (1) Standard: Zugriffskontrolle. Implementieren Sie technische Richtlinien und Verfahren für elektronische Informationssysteme, in denen elektronisch geschützte Gesundheitsinformationen gespeichert werden, sodass nur Personen oder Softwareprogramme darauf zugreifen können, denen Zugriffsrechte gemäß 164.308(a)(4) gewährt wurden.	s-3 bucket-acl-prohibited	Diese Regel prüft, ob Access Control Lists (ACLs) für die Zugriffskontrolle auf Amazon S3 S3-Buckets verwendet werden. ACLs sind veraltete Zugriffskontrollmechanismen für Amazon S3 S3-Buckets, die älter sind als AWS Identity and Access Management (IAM). Stattdessen empfiehlt es sich ACLs, IAM-Richtlinien oder S3-Bucket-Richtlinien zu verwenden, um den Zugriff auf Ihre S3-Buckets einfacher zu verwalten.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.312(a)(1)	(a) (1) Standard: Zugriffskontrolle. Implementieren Sie technische Richtlinien und Verfahren für elektronische Informationssysteme, in denen elektronisch geschützte Gesundheitsinformationen gespeichert werden, sodass nur Personen oder Softwareprogramme darauf zugreifen können, denen Zugriffsrechte gemäß 164.308(a)(4) gewährt wurden.	opensearch-in-vpc-only	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass sich Amazon OpenSearch Service-Domains innerhalb einer Amazon Virtual Private Cloud (Amazon VPC) befinden. Eine Amazon OpenSearch Service-Domain innerhalb einer Amazon VPC ermöglicht die sichere Kommunikation zwischen Amazon OpenSearch Service und anderen Services innerhalb der Amazon VPC, ohne dass ein Internet-Gateway, ein NAT-Gerät oder eine VPN-Verbindung erforderlich ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.312(a)(2)(i)	(2) Spezifikationen der Implement ierung: (i) Eindeutige Benutzeridentifikation (erforderlich). Weisen Sie einen eindeutigen Namen und/oder eine eindeutige Nummer zur Identifizierung und Nachverfolgung der Benutzeridentität zu.	iam-root-access-key-überprüfen	Der Zugriff auf Systeme und Ressourcen kann gesteuert werden, indem überprüft wird, ob der Root-Benu tzer keine Zugriffss chlüssel mit seiner AWS Identity and Access Management (IAM) -Rolle verknüpft hat. Stellen Sie sicher, dass die Root-Zugr iffsschlüssel gelöscht werden. Erstellen und verwenden Sie stattdessen rollenbas ierte Funktionen, AWS-Konten um das Prinzip der geringste n Funktionalität zu berücksichtigen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.312(a)(2)(ii)	(ii) Zugriffsverfahren für Notfälle (erforderlich). Etablieren (und nach Bedarf implementieren) Sie Verfahren zur Beschaffung der in einem Notfall erforderlichen elektronisch geschützten Gesundheitsinformationen.	db-instance-backup-enabled	Die Sicherungsfunktion von Amazon RDS erstellt Sicherungen Ihrer Datenbanken und Transaktionsprotokolle. Amazon RDS erstellt einen Snapshot für das Speichervolume Ihrer DB-Instance, sodass die gesamte DB-Instance gesichert wird. Sie können im System spezifische Aufbewahrungsfristen festlegen, um Ihre Ausfallsicherheitsanforderungen zu erfüllen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.312(a)(2)(ii)	(ii) Zugriffsverfahren für Notfälle (erforderlich). Etablieren (und nach Bedarf implementieren) Sie Verfahren zur Beschaffung der in einem Notfall erforderlichen elektronisch geschützten Gesundheitsinformationen.	dynamodb-pitr-enabled	Aktivieren Sie diese Regel, um zu überprüfen, ob die Informationen gesichert wurden. Es verwaltet auch die Backups, indem es sicherstellt, dass die point-in-time Wiederherstellung in Amazon DynamoDB aktiviert ist. Bei der Wiederherstellung werden fortlaufende Backups Ihrer Tabelle für die letzten 35 Tage gespeichert.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.312(a)(2)(ii)	(ii) Zugriffsverfahren für Notfälle (erforderlich). Etablieren (und nach Bedarf implementieren) Sie Verfahren zur Beschaffung der in einem Notfall erforderlichen elektronisch geschützten Gesundheitsinformationen.	elasticache-redis-cluster-automatic-Backup-Prüfung	Wenn automatische Backups aktiviert sind, ElastiCache erstellt Amazon täglich ein Backup des Clusters. Die Sicherung kann für eine von Ihrer Organisation festgelegte Anzahl von Tagen aufbewahrt werden. Automatische Backups schützen vor Datenverlust. Bei einem Ausfall können Sie einen neuen Cluster erstellen, der Ihre Daten aus dem aktuellen Backup wiederherstellt.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.312(a)(2)(ii)	(ii) Zugriffsverfahren für Notfälle (erforderlich). Etablieren (und nach Bedarf implementieren) Sie Verfahren zur Beschaffung der in einem Notfall erforderlichen elektronisch geschützten Gesundheitsinformationen.	s-3 bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) unterstützt die Aufrechterhaltung einer angemessenen Kapazität und Verfügbarkeit. CRR ermöglicht das automatische, asynchrone Kopieren von Objekten in Amazon-S3-Buckets, um die Datenverfügbarkeit sicherzustellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.312(a)(2)(ii)	(ii) Zugriffsverfahren für Notfälle (erforderlich). Etablieren (und nach Bedarf implementieren) Sie Verfahren zur Beschaffung der in einem Notfall erforderlichen elektronisch geschützten Gesundheitsinformationen.	s-3 bucket-versioning-enabled	Die Versionsverwaltung von Amazon Simple Storage Service (Amazon S3)-Buckets hilft dabei, mehrere Varianten eines Objekts im selben Amazon-S3-Bucket zu speichern. Verwenden Sie die Versionsverwaltung, um sämtliche Versionen aller Objekte in Ihrem Amazon-S3-Bucket zu speichern, abzurufen oder wiederherzustellen. Mit der Versionsverwaltung können Sie Versionen sowohl nach unbeabsichtigten Benutzeraktionen als auch nach Anwendungsfehlern problemlos wiederherstellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.312(a)(2)(ii)	(ii) Zugriffsverfahren für Notfälle (erforderlich). Etablieren (und nach Bedarf implementieren) Sie Verfahren zur Beschaffung der in einem Notfall erforderlichen elektronisch geschützten Gesundheitsinformationen.	dynamodb-in-backup-plan	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon DynamoDB-Tabellen Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.312(a)(2)(ii)	(ii) Zugriffsverfahren für Notfälle (erforderlich). Etablieren (und nach Bedarf implementieren) Sie Verfahren zur Beschaffung der in einem Notfall erforderlichen elektronisch geschützten Gesundheitsinformationen.	ebs-in-backup-plan	Stellen Sie zur Unterstützung der Datensicherungsprozesse sicher, dass Ihre Amazon Elastic Block Store (Amazon EBS) -Volumes Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.312(a)(2)(ii)	(ii) Zugriffsverfahren für Notfälle (erforderlich). Etablieren (und nach Bedarf implementieren) Sie Verfahren zur Beschaffung der in einem Notfall erforderlichen elektronisch geschützten Gesundheitsinformationen.	efs-in-backup-plan	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon Elastic File System (Amazon EFS) -Dateisysteme Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.312(a)(2)(ii)	(ii) Zugriffsverfahren für Notfälle (erforderlich). Etablieren (und nach Bedarf implementieren) Sie Verfahren zur Beschaffung der in einem Notfall erforderlichen elektronisch geschützten Gesundheitsinformationen.	redshift-backup-enabled	Stellen Sie zur Unterstützung der Datensicherungsprozesse sicher, dass Ihre Amazon-Redshift-Cluster über automatisierte Snapshots verfügen. Wenn automatisierte Snapshots für einen Cluster aktiviert sind, erstellt Redshift in regelmäßigen Abständen Snapshots dieses Clusters. Standardmäßig erstellt Redshift alle acht Stunden oder alle 5 GB einen Snapshot für jeden Knoten mit Datenänderungen oder je nachdem, was zuerst eintritt.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.312(a)(2)(ii)	(ii) Zugriffsverfahren für Notfälle (erforderlich). Etablieren (und nach Bedarf implementieren) Sie Verfahren zur Beschaffung der in einem Notfall erforderlichen elektronisch geschützten Gesundheitsinformationen.	rds-in-backup-plan	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon Relational Database Service (Amazon RDS) -Instances Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.312(a)(2)(ii)	(ii) Zugriffsverfahren für Notfälle (erforderlich). Etablieren (und nach Bedarf implementieren) Sie Verfahren zur Beschaffung der in einem Notfall erforderlichen elektronisch geschützten Gesundheitsinformationen.	ec2--Plan resources-protected-by-backup	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon Elastic Compute Cloud (Amazon EC2) -Ressourcen Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.312(a)(2)(ii)	(ii) Zugriffsverfahren für Notfälle (erforderlich). Etablieren (und nach Bedarf implementieren) Sie Verfahren zur Beschaffung der in einem Notfall erforderlichen elektronisch geschützten Gesundheitsinformationen.	aurora-resources-protected-by-Backup-Plan	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon Aurora Aurora-Ressourcen Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.312(a)(2)(ii)	(ii) Zugriffsverfahren für Notfälle (erforderlich). Etablieren (und nach Bedarf implementieren) Sie Verfahren zur Beschaffung der in einem Notfall erforderlichen elektronisch geschützten Gesundheitsinformationen.	backup-plan-min-frequency-and-min-retention-check	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihr AWS Backup-Plan auf eine Mindestfrequenz und Aufbewahrung festgelegt ist. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen. Mit dieser Regel können Sie die Parameter requiredFrequencyValue (Config default: 1), requiredRetentionDays (Config default: 35) und requiredFrequencyUnit

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			(Config default: days) festlegen. Der tatsächliche Wert muss den Anforderungen Ihrer Organisation entsprechen.
164.312(a)(2)(ii)	(ii) Zugriffsverfahren für Notfälle (erforderlich). Etablieren (und nach Bedarf implementieren) Sie Verfahren zur Beschaffung der in einem Notfall erforderlichen elektronisch geschützten Gesundheitsinformationen.	backup-recovery-point-manual-löschen-deaktiviert	Stellen Sie sicher, dass Ihren AWS Backup-Wiederherstellungspunkten eine ressourcenbasierte Richtlinie zugeordnet ist, die das Löschen von Wiederherstellungspunkten verhindert. Die Verwendung einer ressourcenbasierten Richtlinie zur Verhinderung des Löschens von Wiederherstellungspunkten kann dazu beitragen, ein versehentliches oder absichtliches Löschen zu unterbinden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.312(a)(2)(ii)	(ii) Zugriffsverfahren für Notfälle (erforderlich). Etablieren (und nach Bedarf implementieren) Sie Verfahren zur Beschaffung der in einem Notfall erforderlichen elektronisch geschützten Gesundheitsinformationen.	backup-recovery-point-encrypted	Stellen Sie sicher, dass die Verschlüsselung für Ihre AWS Backup-Wiederherstellungspunkte aktiviert ist. Da sensible Daten auch im Ruhezustand vorhanden sein können, sollten Sie die Verschlüsselung im Ruhezustand aktivieren, um diese Daten zu schützen.
164.312(a)(2)(iv)	(iv) Verschlüsselung und Entschlüsselung (adressierbar). Implementieren Sie einen Mechanismus zur Ver- und Entschlüsselung elektronisch geschützter Gesundheitsinformationen.	alb-http-to-https-Umleitungsprüfung	Um Daten während der Übertragung zu schützen, stellen Sie sicher, dass Ihr Application Load Balancer unverschlüsselte HTTP-Anfragen automatisch an HTTPS umleitet. Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.312(a)(2)(iv)	(iv) Verschlüsselung und Entschlüs selung (adressie rbar). Implement ieren Sie einen Mechanismus zur Ver- und Entschlüs selung elektroni sch geschützter Gesundheitsinforma tionen.	api-gw-ssl-enabled	Stellen Sie sicher, dass die REST-API-Stufen von Amazon API Gateway mit SSL-Zertifikaten konfiguri ert sind, damit Backend-Systeme überprüfen können, ob Anforderungen von API Gateway stammen.
164.312(a)(2)(iv)	(iv) Verschlüsselung und Entschlüs selung (adressie rbar). Implement ieren Sie einen Mechanismus zur Ver- und Entschlüs selung elektroni sch geschützter Gesundheitsinforma tionen.	cloud-trail-encryption-enabled	Da sensible Daten vorhanden sein können und um Daten im Speicher zu schützen, sollten Sie sicherstellen, dass die Verschlüsselung für Ihre Trails aktiviert ist. AWS CloudTrail

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.312(a)(2)(iv)	(iv) Verschlüsselung und Entschlüs selung (adressie rbar). Implement ieren Sie einen Mechanismus zur Ver- und Entschlüs selung elektroni sch geschützter Gesundheitsinforma tionen.	ec-2 ebs-encryption-by-default	Zum Schutz von Daten im Ruhezusta nd müssen Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon Elastic Block Store (Amazon EBS)-Volu mes aktiviert ist. Da sensible Daten auch im Ruhezusta nd vorhanden sein können, sollten Sie die Verschlüsselung im Ruhezustand aktivieren, um diese Daten zu schützen.
164.312(a)(2)(iv)	(iv) Verschlüsselung und Entschlüs selung (adressie rbar). Implement ieren Sie einen Mechanismus zur Ver- und Entschlüs selung elektroni sch geschützter Gesundheitsinforma tionen.	efs-encrypted-check	Aktivieren Sie die Verschlüsselung für Ihr Amazon Elastic File System (EFS), um eventuell vorhandene sensible Daten sowie Daten im Ruhezustand zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.312(a)(2)(iv)	(iv) Verschlüsselung und Entschlüs selung (adressie rbar). Implement ieren Sie einen Mechanismus zur Ver- und Entschlüs selung elektroni sch geschützter Gesundheitsinforma tionen.	elasticsearch-encr ypted-at-rest	Da sensible Daten vorhanden sein können und um Daten im Ruhezustand zu schützen, sollten Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon OpenSearch Service (OpenSearch Service) -Domains aktiviert ist.
164.312(a)(2)(iv)	(iv) Verschlüsselung und Entschlüs selung (adressie rbar). Implement ieren Sie einen Mechanismus zur Ver- und Entschlüs selung elektroni sch geschützter Gesundheitsinforma tionen.	elasticsearch-node -to-node-Verschlüs selungsprüfung	Stellen Sie sicher, dass die node-to-node Verschlüs selung für Amazon OpenSearch Service aktiviert ist. Node-to-nodeVerschlüsselung ermöglicht die TLS 1.2-Verschlüsselun g für die gesamte Kommunikation innerhalb der Amazon Virtual Private Cloud (Amazon VPC). Um eventuell vorhanden e sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.312(a)(2)(iv)	(iv) Verschlüsselung und Entschlüs selung (adressie rbar). Implement ieren Sie einen Mechanismus zur Ver- und Entschlüs selung elektroni sch geschützter Gesundheitsinforma tionen.	elb-acm-certificate-required	Zum Schutz von eventuell vorhanden en sensiblen Daten sowie von Daten während der Übertragung muss die Verschlüsselung für Ihr Elastic Load Balancing aktiviert sein. Verwenden Sie AWS Certificate Manager, um öffentlic he und private SSL/ TLS-Zertifikate mit AWS Diensten und internen Ressource n zu verwalten, bereitzustellen und bereitzustellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.312(a)(2)(iv)	(iv) Verschlüsselung und Entschlüs selung (adressie rbar). Implement ieren Sie einen Mechanismus zur Ver- und Entschlüs selung elektroni sch geschützter Gesundheitsinforma tionen.	elb-predefined-sec urity-policy-ssl-check	Stellen Sie sicher, dass Ihre SSL-Liste ner von Classic Elastic Load Balancing eine vordefinierte Sicherhei tsrichtlinie verwenden , um Daten während der Übertragung zu schützen. Elastic Load Balancing bietet vordefinierte Aushandlungskonfig urationen, die für die SSL-Aushandlung verwendet werden, wenn eine Verbindun g zwischen einem Client und Ihrem Load Balancer hergestel lt wurde. Die SSL-Aushandlungsko nfigurationen sind mit einer breiten Palette von Clients kompatibe l und verwenden hochfeste kryptogra fische Algorithm en. Diese Regel verlangt, dass Sie eine vordefinierte Sicherheitsrichtlinie für Ihre SSL-Liste

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			ner festlegen. Die Standard-Sicherheitsrichtlinie lautet: Policy-TLS-1-2-2017-0. ELBSecurity Der tatsächliche Wert muss den Richtlinien Ihrer Organisation entsprechen.
164.312(a)(2)(iv)	(iv) Verschlüsselung und Entschlüsselung (adressierbar). Implementieren Sie einen Mechanismus zur Ver- und Entschlüsselung elektronisch geschützter Gesundheitsinformationen.	elb-tls-https-listeners-nur	Stellen Sie sicher, dass Ihre Elastic Load Balancer (ELBs) mit SSL- oder HTTPS-Listenern konfiguriert sind. Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.
164.312(a)(2)(iv)	(iv) Verschlüsselung und Entschlüsselung (adressierbar). Implementieren Sie einen Mechanismus zur Ver- und Entschlüsselung elektronisch geschützter Gesundheitsinformationen.	encrypted-volumes	Aktivieren Sie die Verschlüsselung für Ihre Amazon-Elastic-Block-Store (Amazon-EBS)-Volumes, um eventuell vorhandene sensible Daten sowie Daten im Ruhezustand zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.312(a)(2)(iv)	(iv) Verschlüsselung und Entschlüs selung (adressie rbar). Implement ieren Sie einen Mechanismus zur Ver- und Entschlüs selung elektroni sch geschützter Gesundheitsinforma tionen.	rds-snapshot-encry pted	Stellen Sie sicher, dass die Verschlüs selung für Ihre Amazon Relationa l Database Service (Amazon RDS)-Snap shots aktiviert ist. Da sensible Daten auch im Ruhezusta nd vorhanden sein können, sollten Sie die Verschlüsselung im Ruhezustand aktivieren, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.312(a)(2)(iv)	(iv) Verschlüsselung und Entschlüs selung (adressie rbar). Implement ieren Sie einen Mechanismus zur Ver- und Entschlüs selung elektroni sch geschützter Gesundheitsinforma tionen.	rds-storage-encrypted	Zum Schutz von Daten im Ruhezusta nd müssen Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon Relational Database Service (Amazon RDS)-Instances aktiviert ist. Um eventuell vorhanden e sensible Daten im Ruhezustand in Amazon-RDS-Instanc es zu schützen, muss die Verschlüs selung von Daten im Ruhezustand aktiviert sein.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.312(a)(2)(iv)	(iv) Verschlüsselung und Entschlüs selung (adressie rbar). Implement ieren Sie einen Mechanismus zur Ver- und Entschlüs selung elektroni sch geschützter Gesundheitsinforma tionen.	redshift-cluster-c onfiguration-check	Um Daten im Ruhezustand zu schützen, muss die Verschlüsselung für Ihre Amazon-Re dshift-Cluster aktiviert sein. Sie müssen auch sicherstellen, dass die erforderl ichen Konfigurationen auf Amazon-Redshift-Clustern bereitges tellt werden. Die Prüfungsprotokolli erung muss aktiviert sein, um Informati onen zu Verbindun gen und Benutzera ktivitäten in der Datenbank bereitzus tellen. Diese Regel erfordert, dass ein Wert für clusterDb Encrypted (Config Default: TRUE) und LoggingEnabled (Config Default: TRUE) gesetzt ist. Die tatsächlichen Werte müssen den Richtlini en Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.312(a)(2)(iv)	(iv) Verschlüsselung und Entschlüs selung (adressie rbar). Implement ieren Sie einen Mechanismus zur Ver- und Entschlüs selung elektroni sch geschützter Gesundheitsinforma tionen.	redshift-require-tls-ssl	Stellen Sie sicher, dass Ihre Amazon-Redshift-Cluster eine TLS/SSL-Verschlüss elung erfordern, um eine Verbindun g zu SQL-Clients herzustellen. Um eventuell vorhanden e sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.
164.312(a)(2)(iv)	(iv) Verschlüsselung und Entschlüs selung (adressie rbar). Implement ieren Sie einen Mechanismus zur Ver- und Entschlüs selung elektroni sch geschützter Gesundheitsinforma tionen.	s3-aktiviert bucket-se rver-side-encryption	Zum Schutz von Daten im Ruhezusta nd müssen Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon Simple Storage Service (Amazon S3)-Bucke ts aktiviert ist. Um eventuell vorhanden e sensible Daten im Ruhezustand in Amazon-S3-Buckets zu schützen, muss die Verschlüsselung aktiviert sein.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.312(a)(2)(iv)	(iv) Verschlüsselung und Entschlüs selung (adressie rbar). Implement ieren Sie einen Mechanismus zur Ver- und Entschlüs selung elektroni sch geschützter Gesundheitsinforma tionen.	s-3 bucket-ssl-request s-only	Um Daten während der Übertragung zu schützen, stellen Sie sicher, dass Ihre Amazon Simple Storage Service (Amazon S3)-Bucke ts Anfragen zur Verwendung von Secure Socket Layer (SSL)-Buc kets erfordern. Um eventuell vorhanden e sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.
164.312(a)(2)(iv)	(iv) Verschlüsselung und Entschlüs selung (adressie rbar). Implement ieren Sie einen Mechanismus zur Ver- und Entschlüs selung elektroni sch geschützter Gesundheitsinforma tionen.	s-3 default-encryption -kms	Stellen Sie sicher, dass die Verschlüs selung für Ihre Amazon Simple Storage Service (Amazon S3)-Bucke ts aktiviert ist. Um eventuell vorhanden e sensible Daten im Ruhezustand in einem Amazon-S3-Bucket zu schützen, muss die Verschlüsselung aktiviert sein.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.312(a)(2)(iv)	(iv) Verschlüsselung und Entschlüs selung (adressie rbar). Implement ieren Sie einen Mechanismus zur Ver- und Entschlüs selung elektroni sch geschützter Gesundheitsinforma tionen.	sagemaker-endpoint -configuration-kms-key-konfiguriert	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass die Verschlüsselung mit dem AWS Key Management Service (AWS KMS) für Ihren Endpunkt aktiviert ist. SageMaker Da sensible Daten auf dem SageMaker Endgerät gespeiche rt werden können, sollten Sie die Verschlüsselung im Ruhezustand aktiviere n, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.312(a)(2)(iv)	(iv) Verschlüsselung und Entschlüs selung (adressie rbar). Implement ieren Sie einen Mechanismus zur Ver- und Entschlüs selung elektroni sch geschützter Gesundheitsinforma tionen.	sagemaker-notebook -instance-kms-schl üsselkonfiguriert	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass die Verschlüsselung mit dem AWS Key Management Service (AWS KMS) für Ihr Notebook aktiviert ist. SageMaker Da vertrauliche Daten im SageMaker Notebook gespeichert werden können, sollten Sie die Verschlüsselung im Ruhezustand aktivieren, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.312(a)(2)(iv)	(iv) Verschlüsselung und Entschlüs selung (adressie rbar). Implement ieren Sie einen Mechanismus zur Ver- und Entschlüs selung elektroni sch geschützter Gesundheitsinforma tionen.	sns-encrypted-kms	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass Ihre Amazon Simple Notification Service (Amazon SNS) -Themen mit dem AWS Key Management Service (AWS KMS) verschlüsselt werden müssen. Um eventuell vorhandene sensible Daten im Ruhezusta nd in veröffentlichten Nachrichten zu schützen, muss die Verschlüsselung von Daten im Ruhezusta nd aktiviert sein.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.312(a)(2)(iv)	(iv) Verschlüsselung und Entschlüs selung (adressie rbar). Implement ieren Sie einen Mechanismus zur Ver- und Entschlüs selung elektroni sch geschützter Gesundheitsinforma tionen.	secretsmanager-usi ng-cmk	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass die Verschlüsselung mit dem AWS Key Management Service (AWS KMS) für AWS Secrets Manager aktiviert ist. Aktiviere n Sie die Verschlüs selung von Daten im Ruhezustand, um eventuell vorhanden e sensible Daten im Ruhezustand im Secrets Manager zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.312(a)(2)(iv)	(iv) Verschlüsselung und Entschlüs selung (adressie rbar). Implement ieren Sie einen Mechanismus zur Ver- und Entschlüs selung elektroni sch geschützter Gesundheitsinforma tionen.	elbv2- acm-certificate-required	Zum Schutz von eventuell vorhanden en sensiblen Daten sowie von Daten während der Übertragung muss die Verschlüsselung für Ihr Elastic Load Balancing aktiviert sein. Verwenden Sie AWS Certificate Manager, um öffentlic he und private SSL/ TLS-Zertifikate mit AWS Diensten und internen Ressource n zu verwalten, bereitzustellen und bereitzustellen.
164.312(a)(2)(iv)	(iv) Verschlüsselung und Entschlüs selung (adressie rbar). Implement ieren Sie einen Mechanismus zur Ver- und Entschlüs selung elektroni sch geschützter Gesundheitsinforma tionen.	opensearch-encrypt ed-at-rest	Da sensible Daten vorhanden sein können und um Daten im Ruhezustand zu schützen, sollten Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon OpenSearch Service-Domains aktiviert ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.312(a)(2)(iv)	(iv) Verschlüsselung und Entschlüs selung (adressie rbar). Implement ieren Sie einen Mechanismus zur Ver- und Entschlüs selung elektroni sch geschützter Gesundheitsinforma tionen.	opensearch-https-r equired	Da sensible Daten existieren können und um Daten während der Übertragung zu schützen, sollten Sie sicherstellen, dass HTTPS für Verbindun gen zu Ihren Amazon OpenSearch Service-Domains aktiviert ist.
164.312(a)(2)(iv)	(iv) Verschlüsselung und Entschlüs selung (adressie rbar). Implement ieren Sie einen Mechanismus zur Ver- und Entschlüs selung elektroni sch geschützter Gesundheitsinforma tionen.	opensearch-node-to -node-Verschlüssel ungsprüfung	Stellen Sie sicher, dass die node-to-node Verschlüs selung für Amazon OpenSearch Service aktiviert ist. Node-to-nodeVerschlüsselung ermöglicht die TLS 1.2-Verschlüsselun g für die gesamte Kommunikation innerhalb der Amazon Virtual Private Cloud (Amazon VPC). Um eventuell vorhanden e sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.312(a)(2)(iv)	(iv) Verschlüsselung und Entschlüs selung (adressie rbar). Implement ieren Sie einen Mechanismus zur Ver- und Entschlüs selung elektroni sch geschützter Gesundheitsinforma tionen.	kinesis-stream-enc rypted	Aktivieren Sie die Verschlüsselung für Ihre Amazon-Kinesis-Streams, um eventuell vorhandene sensible Daten sowie Daten im Ruhezustand zu schützen.
164.312(b)	(b) Standard: Prüfungskontrollen. Implementieren Sie Hardware-, Software- und/oder Verfahren smechanismen, die Aktivitäten in Informationssystem en aufzeichnen und untersuchen, die elektronisch geschützt e Gesundheitsinforma tionen enthalten oder verwenden.	api-gw-execution-l ogging-aktiviert	Die API-Gateway-Protokollierung zeigt detaillierte Ansichten der Benutzer, die auf die API zugegriff en haben, und wie diese Benutzer auf die API zugegriff en haben. Diese Einblicke ermöglichen die Transparenz von Benutzeraktivitäten.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.312(b)	(b) Standard: Prüfungskontrollen. Implementieren Sie Hardware-, Software- und/oder Verfahren smechanismen, die Aktivitäten in Informationssystem en aufzeichnen und untersuchen, die elektronisch geschützt e Gesundheitsinforma tionen enthalten oder verwenden.	autoscaling-group-elb-healthcheck-erforderlich	Die Elastic Load Balancer (ELB) - Zustandsprüfungen für Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling Scaling-G ruppen unterstützen die Aufrechterhaltung einer angemesse nen Kapazität und Verfügbarkeit. Der Load Balancer sendet regelmäßig Pings, versucht Verbindun gen herzustellen oder sendet Anfragen, um den Zustand der EC2 Amazon-Instances in einer Gruppe mit auto-scal ing zu testen. Wenn eine Instance nicht zurückmeldet, wird der Traffic an eine neue EC2 Amazon-In stance gesendet.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.312(b)	(b) Standard: Prüfungskontrollen. Implementieren Sie Hardware-, Software- und/oder Verfahren smechanismen, die Aktivitäten in Informationssystem en aufzeichnen und untersuchen, die elektronisch geschützt e Gesundheitsinforma tionen enthalten oder verwenden.	cloud-trail-cloud-watch-logs-aktiviert	Verwenden Sie Amazon CloudWatc h , um Protokoll ereignisaktivitäten zentral zu sammeln und zu verwalten. Die Aufnahme von AWS CloudTrail Daten liefert Einzelheiten zu den API-Aufrufaktivitä ten in Ihrem AWS-Konto.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.312(b)	(b) Standard: Prüfungskontrollen. Implementieren Sie Hardware-, Software- und/oder Verfahren smechanismen, die Aktivitäten in Informationssystem en aufzeichnen und untersuchen, die elektronisch geschützt e Gesundheitsinforma tionen enthalten oder verwenden.	cloudtrail-enabled	AWS CloudTrail kann bei der Nichtabst reitbarkeit helfen, indem Aktionen und API-Aufrufe der AWS Management Console aufgezeic hnet werden. Sie können die Benutzer und die Benutzer AWS-Konten , die einen AWS Dienst aufgerufen haben, die Quell-IP-Adresse, über die die Aufrufe generiert wurden, und den Zeitpunkt der Anrufe identifiz ieren. Einzelheiten zu den erfassten Daten finden Sie unter Inhalt des AWS CloudTrail Datensatzes.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.312(b)	(b) Standard: Prüfungskontrollen. Implementieren Sie Hardware-, Software- und/oder Verfahren smechanismen, die Aktivitäten in Informationssystem en aufzeichnen und untersuchen, die elektronisch geschützt e Gesundheitsinforma tionen enthalten oder verwenden.	cloudtrail-s3-data events-enabled	Die Erfassung von Simple Storage Service (Amazon S3)-Datenereigniss en unterstützt die Erkennung von ungewöhnlichen Aktivitäten. Zu den Details gehören AWS-Konto Informationen über den Zugriff auf einen Amazon S3 S3-Bucket, die IP-Adress e und die Uhrzeit des Ereignisses.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.312(b)	(b) Standard: Prüfungskontrollen. Implementieren Sie Hardware-, Software- und/oder Verfahren smechanismen, die Aktivitäten in Informationssystem en aufzeichnen und untersuchen, die elektronisch geschützt e Gesundheitsinforma tionen enthalten oder verwenden.	cloudwatch-alarm-a ction-check	Amazon CloudWatch alarmiert, wenn eine Metrik den Schwellen wert für eine bestimmte Anzahl von Bewertungszeiträum en überschreitet. Der Alarm führt eine oder mehrere Aktionen durch, die vom Wert der Metrik oder des Ausdrucks im Vergleich zu einem Schwellenwert in einer Reihe von Zeiträumen abhängt. Diese Regel erfordert einen Wert für alarmActionRequired (Config Default: True), insufficientDataAc tion Required (Config Default: True), okActionRequired (Config Default: False). Der tatsächli che Wert muss die Alarmaktionen für Ihre Umgebung widerspie geln.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.312(b)	(b) Standard: Prüfungskontrollen. Implementieren Sie Hardware-, Software- und/oder Verfahren smechanismen, die Aktivitäten in Informationssystem en aufzeichnen und untersuchen, die elektronisch geschützt e Gesundheitsinforma tionen enthalten oder verwenden.	dynamodb-throughpu t-limit-check	Aktivieren Sie diese Regel, um sicherzustellen, dass die bereitgestellte Durchsatzkapazität in Ihren Amazon-Dy namoDB-Tabellen überprüft wird. Dies ist der Umfang der Lese- und Schreibak tivitäten, der von den jeweiligen Tabellen unterstützt werden kann. DynamoDB verwendet diese Informationen für das Reservieren ausreichender Systemressourcen, um Ihren Durchsatz anforderungen gerecht zu werden. Diese Regel generiert eine Warnung, wenn sich der Durchsatz dem Höchstlimit für ein Kundenkonto nähert. Mit dieser Regel können Sie optional die Parameter RCUThreshold Kontoprozentsatz

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			(Konfigurationsstandard: 80) und WCUThreshold Kontoprozentsatz (Konfigurationsstandard: 80) festlegen. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.312(b)	(b) Standard: Prüfungskontrollen. Implementieren Sie Hardware-, Software- und/oder Verfahren smechanismen, die Aktivitäten in Informationssystem en aufzeichnen und untersuchen, die elektronisch geschützt e Gesundheitsinforma tionen enthalten oder verwenden.	elb-logging-enabled	Die Elastic-Load-Balancing-Aktivität ist ein zentraler Kommunikationspunk t innerhalb einer Umgebung. Stellen Sie sicher, dass die ELB-Protokollierun g aktiviert ist. Die gesammelten Daten enthalten detaillie rte Informationen zu Anfragen, die an den ELB gesendet wurden. Jedes Protokoll enthält Informationen wie die Zeit, zu der die Anforderung einging, die Client-IP -Adresse, Latenzen, Anforderungspfade und Serverantworten.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.312(b)	(b) Standard: Prüfungskontrollen. Implementieren Sie Hardware-, Software- und/oder Verfahren smechanismen, die Aktivitäten in Informationssystem en aufzeichnen und untersuchen, die elektronisch geschützt e Gesundheitsinforma tionen enthalten oder verwenden.	guardduty-enabled-centralized	Amazon GuardDuty kann mithilfe von Threat Intellige nce Feeds helfen, potenzielle Cybersich erheitsereignisse zu überwachen und zu erkennen. Dazu gehören Listen mit bösartigen IPs und maschinel len Lernmethoden zur Identifizierung unerwarteter, nicht autorisierter und bösartiger Aktivitäten in Ihrer AWS Cloud-Umgebung.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.312(b)	(b) Standard: Prüfungskontrollen. Implementieren Sie Hardware-, Software- und/oder Verfahren smechanismen, die Aktivitäten in Informationssystem en aufzeichnen und untersuchen, die elektronisch geschützt e Gesundheitsinforma tionen enthalten oder verwenden.	multi-region-cloudtrail-enabled	AWS CloudTrail zeichnet Aktionen und API-Aufrufe der AWS Management Console auf. Sie können feststellen, welche Benutzer und Konten angerufen wurden AWS, von welcher Quell-IP-Adresse aus die Anrufe getätigt wurden und wann die Anrufe erfolgten. CloudTrail übermittelt Protokolldateien aus allen AWS Regionen an Ihren S3-Bucket , wenn MULTI_REG ION_CLOUD _TRAIL_ENABLED aktiviert ist. Außerdem wird beim AWS Start einer neuen Region derselbe Trail in der neuen Region erstellt. CloudTrail Dadurch erhalten Sie automatis ch Protokolldateien mit API-Aktivitäten für die neue Region.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.312(b)	(b) Standard: Prüfungskontrollen. Implementieren Sie Hardware-, Software- und/oder Verfahrensmechanismen, die Aktivitäten in Informationssystemen aufzeichnen und untersuchen, die elektronisch geschützte Gesundheitsinformationen enthalten oder verwenden.	rds-enhanced-monitoring-enabled	Aktivieren Sie Amazon Relational Database Service (Amazon RDS), um die Verfügbarkeit von Amazon RDS zu überwachen. Dies bietet einen detaillierten Einblick in den Zustand Ihrer Amazon-RDS-Datenbank-Instances. Wenn der Amazon-RDS-Speicher mehr als ein zugrunde liegendes physisches Gerät verwendet, erfasst Enhanced Monitoring die Daten für jedes Gerät. Wenn die Amazon-RDS-Datenbank-Instance in einer Multi-AZ-Bereitstellung ausgeführt wird, werden außerdem die Daten für jedes Gerät auf dem sekundären Host sowie die Metriken des sekundären Hosts erfasst.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.312(b)	(b) Standard: Prüfungskontrollen. Implementieren Sie Hardware-, Software- und/oder Verfahren smechanismen, die Aktivitäten in Informationssystem en aufzeichnen und untersuchen, die elektronisch geschützt e Gesundheitsinforma tionen enthalten oder verwenden.	rds-logging-enabled	Um die Protokoll ierung und Überwachung in Ihrer Umgebung zu erleichtern, stellen Sie sicher, dass die Amazon Relationa l Database Service (Amazon RDS)-Prot okollierung aktiviert ist. Mit der Amazon-RDS-Protokollierung können Sie Ereigniss e wie Verbindungen, Verbindungsabbrüch e, Abfragen oder abgefragte Tabellen erfassen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.312(b)	(b) Standard: Prüfungskontrollen. Implementieren Sie Hardware-, Software- und/oder Verfahren smechanismen, die Aktivitäten in Informationssystem en aufzeichnen und untersuchen, die elektronisch geschützt e Gesundheitsinforma tionen enthalten oder verwenden.	s-3 bucket-logging-enabled	Die Amazon Simple Storage Service (Amazon S3)-Serverzugriffs protokollierung bietet eine Methode zur Überwachu ng des Netzwerks im Hinblick auf potenzielle Cybersich erheitsereignisse. Die Ereignisse werden überwacht, indem detaillierte Aufzeichn ungen über die Anfragen erfasst werden, die an einen Amazon-S3-Bucket gestellt wurden. Jeder Zugriffsprotokolle intrag enthält Details zu einer einzelnen Zugriffsanfrage. Zu den Details gehören Anforderer, Bucket-Name, Anforderu ngszeit, Anforderu ngsaktion, Antwortst atus und Fehlercode, falls relevant.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.312(b)	(b) Standard: Prüfungskontrollen. Implementieren Sie Hardware-, Software- und/oder Verfahren smechanismen, die Aktivitäten in Informationssystem en aufzeichnen und untersuchen, die elektronisch geschützt e Gesundheitsinforma tionen enthalten oder verwenden.	securityhub-enabled	AWS Security Hub hilft bei der Überwachung von unbefugtem Personal, Verbindun gen, Geräten und Software. AWS Security Hub aggregiert, organisie rt und priorisie rt die Sicherhei tswarnungen oder Ergebnisse mehrerer Dienste. AWS Einige dieser Dienste sind Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer und AWS Firewall Manager sowie AWS Partnerlösungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.312(b)	(b) Standard: Prüfungskontrollen. Implementieren Sie Hardware-, Software- und/oder Verfahren smechanismen, die Aktivitäten in Informationssystem en aufzeichnen und untersuchen, die elektronisch geschützt e Gesundheitsinforma tionen enthalten oder verwenden.	vpc-flow-logs-enabled	VPC-Flow-Protokoll e erfassen detaillierte Informationsdatens ätze über den IP-Datenverkehr, der zu und von Netzwerkschnittste llen in Ihrer Amazon Virtual Private Cloud (Amazon VPC) fließt. Standardmäßig enthalten Flow-Prot okolldatensätze Werte für die verschiedenen Komponenten des IP-Flows, einschlie ßlich Quelle, Ziel und Protokoll.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.312(b)	(b) Standard: Prüfungskontrollen. Implementieren Sie Hardware-, Software- und/oder Verfahren smechanismen, die Aktivitäten in Informationssystem en aufzeichnen und untersuchen, die elektronisch geschützt e Gesundheitsinforma tionen enthalten oder verwenden.	wafv2-logging-enab led	Um Ihnen bei der Protokollierung und Überwachung in Ihrer Umgebung zu helfen, aktivieren Sie die AWS WAF (V2) -Protokollierung im regionalen und globalen Web. ACLs AWS Die WAF-Protokollierung bietet detaillierte Informationen über den Datenverkehr, der von Ihrer Web-ACL analysiert wird. In den Protokollen werden die Uhrzeit aufgezeic hnet, zu der die AWS WAF die Anfrage von Ihrer AWS Ressource erhalten hat, Informati onen über die Anfrage und eine Aktion für die Regel, der jede Anfrage entsprach.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.312(b)	(b) Standard: Prüfungskontrollen. Implementieren Sie Hardware-, Software- und/oder Verfahrensmechanismen, die Aktivitäten in Informationssystemen aufzeichnen und untersuchen, die elektronisch geschützte Gesundheitsinformationen enthalten oder verwenden.	elasticsearch-logs-to-cloudwatch	Stellen Sie sicher, dass für Amazon OpenSearch Service-Domains Fehlerprotokolle aktiviert und zur Aufbewahrung und Beantwortung an Amazon CloudWatch Logs gestreamt werden. Domain-Fehlerprotokolle sind bei Sicherheits- und Zugriffsprüfungen sowie bei der Diagnose von Verfügbarkeitsproblemen nützlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.312(b)	(b) Standard: Prüfungskontrollen. Implementieren Sie Hardware-, Software- und/oder Verfahren smechanismen, die Aktivitäten in Informationssystem en aufzeichnen und untersuchen, die elektronisch geschützt e Gesundheitsinforma tionen enthalten oder verwenden.	redshift-cluster-c onfiguration-check	Um Daten im Ruhezustand zu schützen, muss die Verschlüsselung für Ihre Amazon-Re dshift-Cluster aktiviert sein. Sie müssen auch sicherstellen, dass die erforderl ichen Konfigurationen auf Amazon-Redshift-Clustern bereitges tellt werden. Die Prüfungsprotokolli erung muss aktiviert sein, um Informati onen zu Verbindun gen und Benutzera ktivitäten in der Datenbank bereitzus tellen. Diese Regel erfordert, dass ein Wert für clusterDb Encrypted (Config Default: TRUE) und LoggingEnabled (Config Default: TRUE) gesetzt ist. Die tatsächlichen Werte müssen den Richtlini en Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.312(b)	(b) Standard: Prüfungskontrollen. Implementieren Sie Hardware-, Software- und/oder Verfahren smechanismen, die Aktivitäten in Informationssystem en aufzeichnen und untersuchen, die elektronisch geschützt e Gesundheitsinforma tionen enthalten oder verwenden.	s3- event-notification s-enabled	Amazon-S3-Ereignis benachrichtigungen können das zuständig e Personal über versehentliche oder vorsätzliche Änderungen an Ihren Bucket-Ob jekten informieren. Zu den Warnen gehören beispiels weise: Erstellung eines neuen Objekts, Entfernung eines Objekts, Wiederher stellung eines Objekts, verloren gegangene und replizierte Objekte.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.312(b)	(b) Standard: Prüfungskontrollen. Implementieren Sie Hardware-, Software- und/oder Verfahrensmechanismen, die Aktivitäten in Informationssystemen aufzeichnen und untersuchen, die elektronisch geschützte Gesundheitsinformationen enthalten oder verwenden.	opensearch-logs-to-cloudwatch	Stellen Sie sicher, dass für Amazon OpenSearch Service-Domains Fehlerprotokolle aktiviert und zur Aufbewahrung und Beantwortung an Amazon CloudWatch Logs gestreamt werden. OpenSearch Service-Fehlerprotokolle können bei Sicherheits- und Zugriffsprüfungen helfen und bei der Diagnose von Verfügbarkeitsproblemen helfen.
164.312(c)(1)	(c)(1) Standard: Integrität. Implementieren Sie Richtlinien und Verfahren zum Schutz elektronisch geschützter Gesundheitsinformationen vor unsachgemäßer Änderung oder Vernichtung.	s-3 bucket-default-lock-enabled	Stellen Sie sicher, dass für Ihren Amazon Simple Storage Service (Amazon S3)-Bucket standardmäßig eine Sperre aktiviert ist. Zum Schutz eventuell vorhandener sensibler Daten in S3-Buckets müssen Sie Objektsperren für Daten im Ruhezustand erzwingen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.312(c)(1)	(c)(1) Standard: Integrität. Implementieren Sie Richtlinien und Verfahren zum Schutz elektronisch geschützter Gesundheitsinformationen vor unsachgemäßer Änderung oder Vernichtung.	s-3 bucket-versioning-enabled	Die Versionsverwaltung von Amazon Simple Storage Service (Amazon S3)-Buckets hilft dabei, mehrere Varianten eines Objekts im selben Amazon-S3-Bucket zu speichern. Verwenden Sie die Versionsverwaltung, um sämtliche Versionen aller Objekte in Ihrem Amazon-S3-Bucket zu speichern, abzurufen oder wiederherzustellen. Mit der Versionsverwaltung können Sie Versionen sowohl nach unbeabsichtigten Benutzeraktionen als auch nach Anwendungsfehlern problemlos wiederherstellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.312(c)(1)	(c)(1) Standard: Integrität. Implementieren Sie Richtlinien und Verfahren zum Schutz elektronisch geschützter Gesundheitsinformationen vor unsachgemäßer Änderung oder Vernichtung.	cloud-trail-log-file-validierung aktiviert	Verwenden Sie die AWS CloudTrail Protokolldateivalidierung, um die Integrität von Protokollen zu überprüfen. CloudTrail Mithilfe der Protokolldateivalidierung kann festgestellt werden, ob eine Protokolldatei geändert oder gelöscht wurde oder ob sie nach der Übermittlung CloudTrail unverändert geblieben ist. Dieses Feature wurde mit dem Branchenstandard entsprechenden Algorithmen entwickelt: SHA-256 für die Hashfunktion und SHA-256 mit RSA für digitale Signaturen. Das macht es rechnerisch unmöglich, CloudTrail Protokolldateien unbemerkt zu ändern, zu löschen oder zu fälschen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.312(c)(1)	(c)(1) Standard: Integrität. Implementieren Sie Richtlinien und Verfahren zum Schutz elektronisch geschützter Gesundheitsinformationen vor unsachgemäßer Änderung oder Vernichtung.	opensearch-https-required	Da sensible Daten existieren können und um Daten während der Übertragung zu schützen, sollten Sie sicherstellen, dass HTTPS für Verbindungen zu Ihren Amazon OpenSearch Service-Domains aktiviert ist.
164.312(c)(1)	(c)(1) Standard: Integrität. Implementieren Sie Richtlinien und Verfahren zum Schutz elektronisch geschützter Gesundheitsinformationen vor unsachgemäßer Änderung oder Vernichtung.	opensearch-node-to-node-Verschlüsselungsprüfung	Stellen Sie sicher, dass die node-to-node Verschlüsselung für Amazon OpenSearch Service aktiviert ist. Node-to-nodeVerschlüsselung ermöglicht die TLS 1.2-Verschlüsselung für die gesamte Kommunikation innerhalb der Amazon Virtual Private Cloud (Amazon VPC). Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.312(c)(2)	(2) Spezifikation der Implementierung: Mechanismus zur Authentifizierung elektronisch geschützter Gesundheitsinformationen (adressierbar). Implementieren Sie elektronische Mechanismen zur Bestätigung, dass elektronisch geschützte Gesundheitsinformationen nicht auf unbefugte Weise verändert oder vernichtet wurden.	cloud-trail-log-file-Validierung aktiviert	Verwenden Sie die AWS CloudTrail Protokolldateivalidierung, um die Integrität von Protokollen zu überprüfen. CloudTrail Mithilfe der Protokolldateivalidierung kann festgestellt werden, ob eine Protokolldatei geändert oder gelöscht wurde oder ob sie nach der Übermittlung CloudTrail unverändert geblieben ist. Dieses Feature wurde mit dem Branchenstandard entsprechenden Algorithmen entwickelt: SHA-256 für die Hashfunktion und SHA-256 mit RSA für digitale Signaturen. Das macht es rechnerisch unmöglich, CloudTrail Protokolldateien unbemerkt zu ändern, zu löschen oder zu fälschen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.312(c)(2)	(2) Spezifikation der Implementierung: Mechanismus zur Authentifizierung elektronisch geschützter Gesundheitsinformationen (adressierbar). Implementieren Sie elektronische Mechanismen zur Bestätigung, dass elektronisch geschützte Gesundheitsinformationen nicht auf unbefugte Weise verändert oder vernichtet wurden.	s-3 bucket-default-lock-enabled	Stellen Sie sicher, dass für Ihren Amazon Simple Storage Service (Amazon S3)-Bucket standardmäßig eine Sperre aktiviert ist. Zum Schutz eventuell vorhandener sensibler Daten in S3-Buckets müssen Sie Objektsperren für Daten im Ruhezustand erzwingen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.312(c)(2)	(2) Spezifikation der Implementierung: Mechanismus zur Authentifizierung elektronisch geschützter Gesundheitsinformationen (adressierbar). Implementieren Sie elektronische Mechanismen zur Bestätigung, dass elektronisch geschützte Gesundheitsinformationen nicht auf unbefugte Weise verändert oder vernichtet wurden.	s3- bucket-server-side-encryption -aktiviert	Zum Schutz von Daten im Ruhezustand müssen Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon Simple Storage Service (Amazon S3)-Buckets aktiviert ist. Um eventuell vorhandene sensible Daten im Ruhezustand in Amazon-S3-Buckets zu schützen, muss die Verschlüsselung aktiviert sein.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.312(c)(2)	(2) Spezifikation der Implementierung: Mechanismus zur Authentifizierung elektronisch geschützter Gesundheitsinformationen (adressierbar). Implementieren Sie elektronische Mechanismen zur Bestätigung, dass elektronisch geschützte Gesundheitsinformationen nicht auf unbefugte Weise verändert oder vernichtet wurden.	s-3 bucket-ssl-requests-only	Um Daten während der Übertragung zu schützen, stellen Sie sicher, dass Ihre Amazon Simple Storage Service (Amazon S3)-Buckets Anfragen zur Verwendung von Secure Socket Layer (SSL)-Buckets erfordern. Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.312(c)(2)	(2) Spezifikation der Implementierung: Mechanismus zur Authentifizierung elektronisch geschützter Gesundheitsinformationen (adressierbar). Implementieren Sie elektronische Mechanismen zur Bestätigung, dass elektronisch geschützte Gesundheitsinformationen nicht auf unbefugte Weise verändert oder vernichtet wurden.	s-3 bucket-versioning-enabled	Die Versionsverwaltung von Amazon Simple Storage Service (Amazon S3)-Buckets hilft dabei, mehrere Varianten eines Objekts im selben Amazon-S3-Bucket zu speichern. Verwenden Sie die Versionsverwaltung, um sämtliche Versionen aller Objekte in Ihrem Amazon-S3-Bucket zu speichern, abzurufen oder wiederherzustellen. Mit der Versionsverwaltung können Sie Versionen sowohl nach unbeabsichtigten Benutzeraktionen als auch nach Anwendungsfehlern problemlos wiederherstellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.312(d)	(d) Standard: Authentifizierung von Personen oder Entitäten. Implementieren Sie Verfahren, um zu überprüfen, ob es sich bei einer Person oder Entität, die Zugriff auf elektronisch geschützte Gesundheitsinformationen anfordert, tatsächlich um die behauptete Person oder Entität handelt.	iam-password-policy	Die Identitäten und Anmeldeinformationen werden auf der Grundlage einer organisatorischen IAM-Passwortrichtlinie ausgestellt, verwaltet und verifiziert. Sie erfüllen oder übertreffen die Anforderungen des NIST SP 800-63 und des AWS Foundational Security Best Practices-Standards für Passwortstärke. Mit dieser Regel können Sie optional RequireUppercaseCharacters (Wert für AWS grundlegende Sicherheitsbewährte Methoden: wahr), RequireLowercaseCharacters (Wert für bewährte Methoden für AWS grundlegende Sicherheit: wahr), RequireSymbols (Wert für bewährte Methoden für AWS grundlegende Sicherheit:

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			wahr), RequireNumbers (Wert für bewährte Methoden für AWS grundlegende Sicherheit: wahr), MinimumPasswordLength (Wert für bewährte Methoden für AWS grundlegende Sicherheit: 14), PasswordReusePrevention (Wert für bewährte Methoden für AWS grundlegende Sicherheit: 24) und MaxPasswordAge (Wert für bewährte Methoden für AWS grundlegende Sicherheit: 90) für Ihr IAM festlegen Kennwortrichtlinie. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.312(d)	(d) Standard: Authentifizierung von Personen oder Entitäten. Implementieren Sie Verfahren, um zu überprüfen, ob es sich bei einer Person oder Entität, die Zugriff auf elektronisch geschützte Gesundheitsinformationen anfordert, tatsächlich um die behauptete Person oder Entität handelt.	iam-user-mfa-enabled	Aktivieren Sie diese Regel, um den Zugriff auf Ressourcen in der AWS Cloud einzuschränken. Diese Regel sorgt dafür, dass die Multi-Faktor-Authentifizierung (MFA) für alle Benutzer aktiviert ist. MFA sorgt für eine weitere Schutzebene zusätzlich zu den Anmeldeinformationen. Reduzieren Sie Fälle von kompromittierten Konten, indem Sie MFA für Benutzer vorschreiben.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.312(d)	(d) Standard: Authentifizierung von Personen oder Entitäten. Implementieren Sie Verfahren, um zu überprüfen, ob es sich bei einer Person oder Entität, die Zugriff auf elektronisch geschützte Gesundheitsinformationen anfordert, tatsächlich um die behauptete Person oder Entität handelt.	mfa-enabled-for-iam-Konsolenzugriff	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass MFA für alle AWS Identity and Access Management (IAM) -Benutzer aktiviert ist, die über ein Konsolenkennwort verfügen. MFA sorgt für eine weitere Schutzebene zusätzlich zu den Anmeldeinformationen. Indem Sie MFA für Benutzer vorschreiben, können Sie Fälle kompromittierter Konten reduzieren und verhindern, dass unbefugte Benutzer auf vertrauliche Daten zugreifen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.312(d)	(d) Standard: Authentifizierung von Personen oder Entitäten. Implementieren Sie Verfahren, um zu überprüfen, ob es sich bei einer Person oder Entität, die Zugriff auf elektronisch geschützte Gesundheitsinformationen anfordert, tatsächlich um die behauptete Person oder Entität handelt.	root-account-hardware-mfa-aktiviert	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Hardware-MFA für den Root-Benutzer aktiviert ist. Der Stammbenutzer ist der AWS-Konto-Benutzer mit den meisten Berechtigungen. MFA sorgt für eine weitere Schutzebene zusätzlich zu den Anmeldeinformationen. Indem Sie MFA für den Root-Benutzer vorschreiben, können Sie die Anzahl AWS-Konten kompromittierter Benutzer reduzieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.312(d)	(d) Standard: Authentifizierung von Personen oder Entitäten. Implementieren Sie Verfahren, um zu überprüfen, ob es sich bei einer Person oder Entität, die Zugriff auf elektronisch geschützte Gesundheitsinformationen anfordert, tatsächlich um die behauptete Person oder Entität handelt.	root-account-mfa-enabled	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass MFA für den Root-Benutzer aktiviert ist. Der Stammbenutzer ist der AWS-Konto-Benutzer mit den meisten Berechtigungen. MFA sorgt für eine weitere Schutzebene zusätzlich zu den Anmeldeinformationen. Indem Sie MFA für den Root-Benutzer vorschreiben, können Sie die Anzahl AWS-Konten kompromittierter Benutzer reduzieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.312(e)(1)	(e)(1) Standard: Übertragungssicherheit. Implementieren Sie technische Sicherheitsmaßnahmen zum Schutz vor unbefugtem Zugriff auf elektronisch geschützte Gesundheitsinformationen, die über ein elektronisches Kommunikationsnetz übertragen werden.	alb-http-to-https-Umleitungsprüfung	Um Daten während der Übertragung zu schützen, stellen Sie sicher, dass Ihr Application Load Balancer unverschlüsselte HTTP-Anfragen automatisch an HTTPS umleitet. Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.
164.312(e)(1)	(e)(1) Standard: Übertragungssicherheit. Implementieren Sie technische Sicherheitsmaßnahmen zum Schutz vor unbefugtem Zugriff auf elektronisch geschützte Gesundheitsinformationen, die über ein elektronisches Kommunikationsnetz übertragen werden.	api-gw-ssl-enabled	Stellen Sie sicher, dass die REST-API-Stufen von Amazon API Gateway mit SSL-Zertifikaten konfiguriert sind, damit Backend-Systeme überprüfen können, ob Anforderungen von API Gateway stammen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.312(e)(1)	(e)(1) Standard: Übertragungssicherheit. Implementieren Sie technische Sicherheitsmaßnahmen zum Schutz vor unbefugtem Zugriff auf elektronisch geschützte Gesundheitsinformationen, die über ein elektronisches Kommunikationsnetz übertragen werden.	elasticsearch-node-to-node-Verschlüsselungsprüfung	Stellen Sie sicher, dass die node-to-node Verschlüsselung für Amazon OpenSearch Service aktiviert ist. Node-to-nodeVerschlüsselung ermöglicht die TLS 1.2-Verschlüsselung für die gesamte Kommunikation innerhalb der Amazon Virtual Private Cloud (Amazon VPC). Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.312(e)(1)	(e)(1) Standard: Übertragungssicherheit. Implementieren Sie technische Sicherheitsmaßnahmen zum Schutz vor unbefugtem Zugriff auf elektronisch geschützte Gesundheitsinformationen, die über ein elektronisches Kommunikationsnetz übertragen werden.	elb-acm-certificate-required	Zum Schutz von eventuell vorhanden en sensiblen Daten sowie von Daten während der Übertragung muss die Verschlüsselung für Ihr Elastic Load Balancing aktiviert sein. Verwenden Sie AWS Certificate Manager, um öffentliche und private SSL/TLS-Zertifikate mit AWS Diensten und internen Ressourcen zu verwalten, bereitzustellen und bereitzustellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.312(e)(1)	(e)(1) Standard: Übertragungssicherheit. Implementieren Sie technische Sicherheitsmaßnahmen zum Schutz vor unbefugtem Zugriff auf elektronisch geschützte Gesundheitsinformationen, die über ein elektronisches Kommunikationsnetz übertragen werden.	elb-predefined-security-policy-ssl-check	Stellen Sie sicher, dass Ihre SSL-Listener von Classic Elastic Load Balancing eine vordefinierte Sicherheitsrichtlinie verwenden, um Daten während der Übertragung zu schützen. Elastic Load Balancing bietet vordefinierte Aushandlungskonfigurationen, die für die SSL-Aushandlung verwendet werden, wenn eine Verbindung zwischen einem Client und Ihrem Load Balancer hergestellt wurde. Die SSL-Aushandlungskonfigurationen sind mit einer breiten Palette von Clients kompatibel und verwenden hochfeste kryptografische Algorithmen. Diese Regel verlangt, dass Sie eine vordefinierte Sicherheitsrichtlinie für Ihre SSL-Liste

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			ner festlegen. Die Standard-Sicherheitsrichtlinie lautet: Policy-TLS-1-2-2017-0. ELBSecurity Der tatsächliche Wert muss den Richtlinien Ihrer Organisation entsprechen.
164.312(e)(1)	(e)(1) Standard: Übertragungssicherheit. Implementieren Sie technische Sicherheitsmaßnahmen zum Schutz vor unbefugtem Zugriff auf elektronisch geschützte Gesundheitsinformationen, die über ein elektronisches Kommunikationsnetz übertragen werden.	elb-tls-https-listeners-nur	Stellen Sie sicher, dass Ihre Elastic Load Balancer (ELBs) mit SSL- oder HTTPS-Listenern konfiguriert sind. Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.312(e)(1)	(e)(1) Standard: Übertragungssicherheit. Implementieren Sie technische Sicherheitsmaßnahmen zum Schutz vor unbefugtem Zugriff auf elektronisch geschützte Gesundheitsinformationen, die über ein elektronisches Kommunikationsnetz übertragen werden.	redshift-require-tls-ssl	Stellen Sie sicher, dass Ihre Amazon-Redshift-Cluster eine TLS/SSL-Verschlüsselung erfordern, um eine Verbindung zu SQL-Clients herzustellen. Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.
164.312(e)(1)	(e)(1) Standard: Übertragungssicherheit. Implementieren Sie technische Sicherheitsmaßnahmen zum Schutz vor unbefugtem Zugriff auf elektronisch geschützte Gesundheitsinformationen, die über ein elektronisches Kommunikationsnetz übertragen werden.	s-3 bucket-ssl-requests-only	Um Daten während der Übertragung zu schützen, stellen Sie sicher, dass Ihre Amazon Simple Storage Service (Amazon S3)-Buckets Anfragen zur Verwendung von Secure Socket Layer (SSL)-Buckets erfordern. Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.312(e)(1)	(e)(1) Standard: Übertragungssicherheit. Implementieren Sie technische Sicherheitsmaßnahmen zum Schutz vor unbefugtem Zugriff auf elektronisch geschützte Gesundheitsinformationen, die über ein elektronisches Kommunikationsnetz übertragen werden.	dms-replication-not-public	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass auf DMS-Replikationsinstanzen nicht öffentlich zugegriffen werden kann. DMS-Replikations-Instances können vertrauliche Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.
164.312(e)(1)	(e)(1) Standard: Übertragungssicherheit. Implementieren Sie technische Sicherheitsmaßnahmen zum Schutz vor unbefugtem Zugriff auf elektronisch geschützte Gesundheitsinformationen, die über ein elektronisches Kommunikationsnetz übertragen werden.	ebs-snapshot-public-restorable-überprüfen	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass EBS-Snapshots nicht öffentlich wiederherstellbar sind. EBS-Volume-Snapshots können vertrauliche Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.312(e)(1)	(e)(1) Standard: Übertragungssicherheit. Implementieren Sie technische Sicherheitsmaßnahmen zum Schutz vor unbefugtem Zugriff auf elektronisch geschützte Gesundheitsinformationen, die über ein elektronisches Kommunikationsnetz übertragen werden.	ec-2 instance-no-public-ip	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon Elastic Compute Cloud (Amazon EC2) - Instances nicht öffentlich zugänglich sind. EC2 Amazon-Instances können vertrauliche Informationen enthalten, und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.312(e)(1)	(e)(1) Standard: Übertragungssicherheit. Implementieren Sie technische Sicherheitsmaßnahmen zum Schutz vor unbefugtem Zugriff auf elektronisch geschützte Gesundheitsinformationen, die über ein elektronisches Kommunikationsnetz übertragen werden.	elasticsearch-in-vpc-only	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass sich Amazon OpenSearch OpenSearch Service (Service) - Domains innerhalb einer Amazon Virtual Private Cloud (Amazon VPC) befinden. Eine OpenSearch Service-Domain innerhalb einer Amazon VPC ermöglicht die sichere Kommunikation zwischen OpenSearch Service und anderen Services innerhalb der Amazon VPC, ohne dass ein Internet-Gateway, ein NAT-Gerät oder eine VPN-Verbindung erforderlich ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.312(e)(1)	(e)(1) Standard: Übertragungssicherheit. Implementieren Sie technische Sicherheitsmaßnahmen zum Schutz vor unbefugtem Zugriff auf elektronisch geschützte Gesundheitsinformationen, die über ein elektronisches Kommunikationsnetz übertragen werden.	emr-master-no-public-ip	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon EMR-Cluster-Masterknoten nicht öffentlich zugänglich sind. Amazon-EMR-Cluster-Hauptknoten können vertrauliche Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.312(e)(1)	(e)(1) Standard: Übertragungssicherheit. Implementieren Sie technische Sicherheitsmaßnahmen zum Schutz vor unbefugtem Zugriff auf elektronisch geschützte Gesundheitsinformationen, die über ein elektronisches Kommunikationsnetz übertragen werden.	ec-2 instances-in-vpc	Stellen Sie Amazon Elastic Compute Cloud (Amazon EC2) -Instances innerhalb einer Amazon Virtual Private Cloud (Amazon VPC) bereit, um eine sichere Kommunikation zwischen einer Instance und anderen Services innerhalb der Amazon VPC zu ermöglichen, ohne dass ein Internet-Gateway, ein NAT-Gerät oder eine VPN-Verbindung erforderlich ist. Der gesamte Datenverkehr bleibt sicher in der AWS Cloud. Domains, die sich innerhalb einer VPC befinden, verfügen aufgrund ihrer logischen Isolierung im Vergleich zu Domains mit öffentlichen Endpunkten über eine zusätzliche Sicherheitsebene. Weisen Sie EC2

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			Amazon-Instances einer Amazon-VPC zu, um den Zugriff ordnungsgemäß zu verwalten.
164.312(e)(1)	(e)(1) Standard: Übertragungssicherheit. Implementieren Sie technische Sicherheitsmaßnahmen zum Schutz vor unbefugtem Zugriff auf elektronisch geschützte Gesundheitsinformationen, die über ein elektronisches Kommunikationsnetz übertragen werden.	internet-gateway-authorized-vpc-nur	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Internet-Gateways nur mit autorisierter Amazon Virtual Private Cloud (Amazon VPC) verbunden sind. Internet-Gateways ermöglichen den bidirektionalen Internetzugang zur und von der Amazon VPC, was möglicherweise zu einem unbefugten Zugriff auf Amazon-VPC-Ressourcen führen kann.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.312(e)(1)	(e)(1) Standard: Übertragungssicherheit. Implementieren Sie technische Sicherheitsmaßnahmen zum Schutz vor unbefugtem Zugriff auf elektronisch geschützte Gesundheitsinformationen, die über ein elektronisches Kommunikationsnetz übertragen werden.	lambda-function-public-access-verboten	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass AWS Lambda-Funktionen nicht öffentlich zugänglich sind. Der öffentliche Zugriff kann möglicherweise die Verfügbarkeit von Ressourcen beeinträchtigen.
164.312(e)(1)	(e)(1) Standard: Übertragungssicherheit. Implementieren Sie technische Sicherheitsmaßnahmen zum Schutz vor unbefugtem Zugriff auf elektronisch geschützte Gesundheitsinformationen, die über ein elektronisches Kommunikationsnetz übertragen werden.	no-unrestricted-route-to-igw	Stellen Sie sicher, dass EC2 Amazon-Routentabellen keine uneingeschränkten Routen zu einem Internet-Gateway enthalten. Durch das Entfernen oder Beschränken des Internetzugangs für Workloads innerhalb von Amazon VPCs können unbeabsichtigte Zugriffe in Ihrer Umgebung reduziert werden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.312(e)(1)	(e)(1) Standard: Übertragungssicherheit. Implementieren Sie technische Sicherheitsmaßnahmen zum Schutz vor unbefugtem Zugriff auf elektronisch geschützte Gesundheitsinformationen, die über ein elektronisches Kommunikationsnetz übertragen werden.	rds-instance-public-access-überprüfen	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Relational Database Service (Amazon RDS) -Instances nicht öffentlich sind. Amazon-RDS-Datenbank-Instances können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.312(e)(1)	(e)(1) Standard: Übertragungssicherheit. Implementieren Sie technische Sicherheitsmaßnahmen zum Schutz vor unbefugtem Zugriff auf elektronisch geschützte Gesundheitsinformationen, die über ein elektronisches Kommunikationsnetz übertragen werden.	rds-snapshots-public-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Relational Database Service (Amazon RDS) -Instances nicht öffentlich sind. Amazon-RDS-Datenbank-Instances können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.312(e)(1)	(e)(1) Standard: Übertragungssicherheit. Implementieren Sie technische Sicherheitsmaßnahmen zum Schutz vor unbefugtem Zugriff auf elektronisch geschützte Gesundheitsinformationen, die über ein elektronisches Kommunikationsnetz übertragen werden.	redshift-cluster-public-access-überprüfen	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Redshift Redshift-Cluster nicht öffentlich sind. Amazon-Redshift-Cluster können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.312(e)(1)	(e)(1) Standard: Übertragungssicherheit. Implementieren Sie technische Sicherheitsmaßnahmen zum Schutz vor unbefugtem Zugriff auf elektronisch geschützte Gesundheitsinformationen, die über ein elektronisches Kommunikationsnetz übertragen werden.	restricted-common-ports	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass gemeinsame Ports für Amazon Elastic Compute Cloud (Amazon EC2) -Sicherheitsgruppen eingeschränkt sind. Wenn der Zugriff auf Ports nicht auf vertrauenswürdige Quellen beschränkt wird, kann dies zu Angriffen auf die Verfügbarkeit, Integrität und Vertraulichkeit von Systemen führen. Mit dieser Regel können Sie optional die Parameter blockedPort1–blockedPort5 festlegen (Standardkonfigurationen: 20, 21, 3389, 3306, 4333). Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.312(e)(1)	(e)(1) Standard: Übertragungssicherheit. Implementieren Sie technische Sicherheitsmaßnahmen zum Schutz vor unbefugtem Zugriff auf elektronisch geschützte Gesundheitsinformationen, die über ein elektronisches Kommunikationsnetz übertragen werden.	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) Security Groups können bei der Verwaltung des Netzwerkzugriffs helfen, indem sie eine statusbehaftete Filterung von eingehendem und ausgehendem Netzwerkverkehr zu Ressourcen bereitstellen. AWS Wenn Sie eingehenden (oder entfernten) Datenverkehr von 0.0.0.0/0 bis Port 22 auf Ihren Ressourcen nicht zulassen, können Sie den Remote-Zugriff einschränken.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.312(e)(1)	(e)(1) Standard: Übertragungssicherheit. Implementieren Sie technische Sicherheitsmaßnahmen zum Schutz vor unbefugtem Zugriff auf elektronisch geschützte Gesundheitsinformationen, die über ein elektronisches Kommunikationsnetz übertragen werden.	s3-Blöcke, periodisch account-level-public-access	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Simple Storage Service (Amazon S3) -Buckets nicht öffentlich zugänglich sind. Diese Regel trägt dazu bei, sensible Daten vor unbefugten Remote-Benutzern zu schützen, indem sie den öffentlichen Zugriff verhindert. Mit dieser Regel können Sie optional die Parameter ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) und restrictPublicBuckets Parameter (Config Default: True) festlegen. Die tatsächlichen Werte müssen den Richtlini

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			en Ihrer Organisation entsprechen.
164.312(e)(1)	(e)(1) Standard: Übertragungssicherheit. Implementieren Sie technische Sicherheitsmaßnahmen zum Schutz vor unbefugtem Zugriff auf elektronisch geschützte Gesundheitsinformationen, die über ein elektronisches Kommunikationsnetz übertragen werden.	s3- bucket-public-read-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie nur autorisierten Benutzern, Prozessen und Geräten Zugriff auf Amazon Simple Storage Service (Amazon S3) - Buckets gewähren. Die Verwaltung des Zugriffs sollte mit der Klassifizierung der Daten übereinstimmen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.312(e)(1)	(e)(1) Standard: Übertragungssicherheit. Implementieren Sie technische Sicherheitsmaßnahmen zum Schutz vor unbefugtem Zugriff auf elektronisch geschützte Gesundheitsinformationen, die über ein elektronisches Kommunikationsnetz übertragen werden.	s3- bucket-public-write-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie nur autorisierten Benutzern, Prozessen und Geräten Zugriff auf Amazon Simple Storage Service (Amazon S3) - Buckets gewähren. Die Verwaltung des Zugriffs sollte mit der Klassifizierung der Daten übereinstimmen.
164.312(e)(1)	(e)(1) Standard: Übertragungssicherheit. Implementieren Sie technische Sicherheitsmaßnahmen zum Schutz vor unbefugtem Zugriff auf elektronisch geschützte Gesundheitsinformationen, die über ein elektronisches Kommunikationsnetz übertragen werden.	sagemaker-notebook-no-direct-Internetzugang	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass SageMaker Amazon-Notebooks keinen direkten Internetzugang zulassen. Indem Sie direkten Internetzugang blockieren, vermeiden Sie, dass unbefugte Benutzer auf sensible Daten zugreifen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.312(e)(1)	(e)(1) Standard: Übertragungssicherheit. Implementieren Sie technische Sicherheitsmaßnahmen zum Schutz vor unbefugtem Zugriff auf elektronisch geschützte Gesundheitsinformationen, die über ein elektronisches Kommunikationsnetz übertragen werden.	ssm-document-not-public	Stellen Sie sicher, dass AWS Systems Manager (SSM) - Dokumente nicht öffentlich sind, da dies einen unbeabsichtigten Zugriff auf Ihre SSM-Dokumente ermöglichen kann. Ein öffentliches SSM-Dokument kann Informationen über Ihr Konto, Ihre Ressourcen und internen Prozesse preisgeben.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.312(e)(1)	(e)(1) Standard: Übertragungssicherheit. Implementieren Sie technische Sicherheitsmaßnahmen zum Schutz vor unbefugtem Zugriff auf elektronisch geschützte Gesundheitsinformationen, die über ein elektronisches Kommunikationsnetz übertragen werden.	subnet-auto-assign-public-ip-deaktiviert	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon Virtual Private Cloud (VPC) -Subnetzen nicht automatisch eine öffentliche IP-Adresse zugewiesen wird. Amazon Elastic Compute Cloud (EC2) -Instances, die in Subnetzen gestartet werden, in denen dieses Attribut aktiviert ist, haben ihrer primären Netzwerkschnittstelle eine öffentliche IP-Adresse zugewiesen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.312(e)(1)	(e)(1) Standard: Übertragungssicherheit. Implementieren Sie technische Sicherheitsmaßnahmen zum Schutz vor unbefugtem Zugriff auf elektronisch geschützte Gesundheitsinformationen, die über ein elektronisches Kommunikationsnetz übertragen werden.	alb-waf-enabled	Stellen Sie sicher, dass AWS WAF auf Elastic Load Balancers (ELB) aktiviert ist, um Webanwendungen zu schützen. Eine WAF trägt zum Schutz Ihrer Webanwendungen oder APIs vor gängigen Web-Exploits bei. Diese Web-Exploits können sich auf die Verfügbarkeit auswirken, die Sicherheit gefährden oder übermäßige Ressourcen in Ihrer Umgebung verbrauchen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.312(e)(1)	(e)(1) Standard: Übertragungssicherheit. Implementieren Sie technische Sicherheitsmaßnahmen zum Schutz vor unbefugtem Zugriff auf elektronisch geschützte Gesundheitsinformationen, die über ein elektronisches Kommunikationsnetz übertragen werden.	api-gw-associated-with-WAF	AWS Mit WAF können Sie eine Reihe von Regeln (als Web Access Control List (Web ACL) bezeichnet) konfigurieren, die Webanfragen auf der Grundlage von anpassbaren Websicherheitsregeln und -bedingungen, die Sie definieren, zulassen, blockieren oder zählen. Stellen Sie sicher, dass Ihre Amazon-API-Gateway-Stufe mit einer WAF-Web-ACL verknüpft ist, um sie vor böswilligen Angriffen zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.312(e)(1)	(e)(1) Standard: Übertragungssicherheit. Implementieren Sie technische Sicherheitsmaßnahmen zum Schutz vor unbefugtem Zugriff auf elektronisch geschützte Gesundheitsinformationen, die über ein elektronisches Kommunikationsnetz übertragen werden.	vpc-default-security-group-geschlossen	Sicherheitsgruppen von Amazon Elastic Compute Cloud (Amazon EC2) können bei der Verwaltung des Netzwerkzugriffs helfen, indem sie eine statusbehaftete Filterung des ein- und ausgehenden Netzwerkverkehrs zu Ressourcen bereitstellen. AWS Die Beschränkung des gesamten Datenverkehrs auf die Standardsicherheitsgruppe hilft dabei, den Fernzugriff auf Ihre Ressourcen einzuschränken. AWS

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.312(e)(1)	(e)(1) Standard: Übertragungssicherheit. Implementieren Sie technische Sicherheitsmaßnahmen zum Schutz vor unbefugtem Zugriff auf elektronisch geschützte Gesundheitsinformationen, die über ein elektronisches Kommunikationsnetz übertragen werden.	vpc-sg-open-only-to-authorized-ports	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass gemeinsame Ports für Amazon Elastic Compute Cloud (Amazon EC2) -Sicherheitsgruppen eingeschränkt sind. Wenn der Zugriff auf Ports nicht auf vertrauenswürdige Quellen beschränkt wird, kann dies zu Angriffen auf die Verfügbarkeit, Integrität und Vertraulichkeit von Systemen führen. Durch die Beschränkung des Zugriffs auf Ressourcen innerhalb einer Sicherheitsgruppe aus dem Internet (0.0.0.0/0) kann der Remote-Zugriff auf interne Systeme gesteuert werden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.312(e)(1)	(e)(1) Standard: Übertragungssicherheit. Implementieren Sie technische Sicherheitsmaßnahmen zum Schutz vor unbefugtem Zugriff auf elektronisch geschützte Gesundheitsinformationen, die über ein elektronisches Kommunikationsnetz übertragen werden.	autoscaling-launch-config-public-ip-deaktiviert	Wenn Sie Ihre Netzwerkschnittstellen mit einer öffentlichen IP-Adresse konfigurieren, sind die diesen Netzwerkschnittstellen zugehörigen Ressourcen über das Internet erreichbar. EC2 Ressourcen sollten nicht öffentlich zugänglich sein, da dies einen unbeabsichtigten Zugriff auf Ihre Anwendungen oder Server ermöglichen kann.
164.312(e)(1)	(e)(1) Standard: Übertragungssicherheit. Implementieren Sie technische Sicherheitsmaßnahmen zum Schutz vor unbefugtem Zugriff auf elektronisch geschützte Gesundheitsinformationen, die über ein elektronisches Kommunikationsnetz übertragen werden.	opensearch-https-required	Da sensible Daten existieren können und um Daten während der Übertragung zu schützen, sollten Sie sicherstellen, dass HTTPS für Verbindungen zu Ihren Amazon OpenSearch Service-Domains aktiviert ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.312(e)(1)	(e)(1) Standard: Übertragungssicherheit. Implementieren Sie technische Sicherheitsmaßnahmen zum Schutz vor unbefugtem Zugriff auf elektronisch geschützte Gesundheitsinformationen, die über ein elektronisches Kommunikationsnetz übertragen werden.	opensearch-in-vpc-only	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass sich Amazon OpenSearch Service-Domains innerhalb einer Amazon Virtual Private Cloud (Amazon VPC) befinden. Eine Amazon OpenSearch Service-Domain innerhalb einer Amazon VPC ermöglicht die sichere Kommunikation zwischen Amazon OpenSearch Service und anderen Services innerhalb der Amazon VPC, ohne dass ein Internet-Gateway, ein NAT-Gerät oder eine VPN-Verbindung erforderlich ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.312(e)(1)	(e)(1) Standard: Übertragungssicherheit. Implementieren Sie technische Sicherheitsmaßnahmen zum Schutz vor unbefugtem Zugriff auf elektronisch geschützte Gesundheitsinformationen, die über ein elektronisches Kommunikationsnetz übertragen werden.	opensearch-node-to-node-Verschlüsselungsprüfung	Stellen Sie sicher, dass die node-to-node Verschlüsselung für Amazon OpenSearch Service aktiviert ist. Node-to-nodeVerschlüsselung ermöglicht die TLS 1.2-Verschlüsselung für die gesamte Kommunikation innerhalb der Amazon Virtual Private Cloud (Amazon VPC). Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.312(e)(2)(i)	(i) Integritätskontrollen (adressierbar). Implementieren Sie Sicherheitsmaßnahmen, um dafür zu sorgen, dass elektronisch übertragene und elektronisch geschützte Gesundheitsinformationen bis zu ihrer Löschung nicht unbemerkt verändert werden.	alb-http-to-https-Umleitungsprüfung	Um Daten während der Übertragung zu schützen, stellen Sie sicher, dass Ihr Application Load Balancer unverschlüsselte HTTP-Anfragen automatisch an HTTPS umleitet. Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.
164.312(e)(2)(i)	(i) Integritätskontrollen (adressierbar). Implementieren Sie Sicherheitsmaßnahmen, um dafür zu sorgen, dass elektronisch übertragene und elektronisch geschützte Gesundheitsinformationen bis zu ihrer Löschung nicht unbemerkt verändert werden.	api-gw-ssl-enabled	Stellen Sie sicher, dass die REST-API-Stufen von Amazon API Gateway mit SSL-Zertifikaten konfiguriert sind, damit Backend-Systeme überprüfen können, ob Anforderungen von API Gateway stammen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.312(e)(2)(i)	(i) Integritätskontrollen (adressierbar). Implementieren Sie Sicherheitsmaßnahmen, um dafür zu sorgen, dass elektronisch übertragene und elektronisch geschützte Gesundheitsinformationen bis zu ihrer Löschung nicht unbemerkt verändert werden.	elasticsearch-node-to-node-Verschlüsselungsprüfung	Stellen Sie sicher, dass die node-to-node Verschlüsselung für Amazon OpenSearch Service aktiviert ist. Node-to-nodeVerschlüsselung ermöglicht die TLS 1.2-Verschlüsselung für die gesamte Kommunikation innerhalb der Amazon Virtual Private Cloud (Amazon VPC). Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.312(e)(2)(i)	(i) Integritätskontrollen (adressierbar). Implementieren Sie Sicherheitsmaßnahmen, um dafür zu sorgen, dass elektronisch übertragene und elektronisch geschützte Gesundheitsinformationen bis zu ihrer Löschung nicht unbemerkt verändert werden.	elb-acm-certificate-required	Zum Schutz von eventuell vorhandenen sensiblen Daten sowie von Daten während der Übertragung muss die Verschlüsselung für Ihr Elastic Load Balancing aktiviert sein. Verwenden Sie AWS Certificate Manager, um öffentliche und private SSL/TLS-Zertifikate mit AWS Diensten und internen Ressourcen zu verwalten, bereitzustellen und bereitzustellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.312(e)(2)(i)	(i) Integritätskontrollen (adressierbar). Implementieren Sie Sicherheitsmaßnahmen, um dafür zu sorgen, dass elektronisch übertragene und elektronisch geschützte Gesundheitsinformationen bis zu ihrer Löschung nicht unbemerkt verändert werden.	elb-predefined-security-policy-ssl-check	Stellen Sie sicher, dass Ihre SSL-Listener von Classic Elastic Load Balancing eine vordefinierte Sicherheitsrichtlinie verwenden, um Daten während der Übertragung zu schützen. Elastic Load Balancing bietet vordefinierte Aushandlungskonfigurationen, die für die SSL-Aushandlung verwendet werden, wenn eine Verbindung zwischen einem Client und Ihrem Load Balancer hergestellt wurde. Die SSL-Aushandlungskonfigurationen sind mit einer breiten Palette von Clients kompatibel und verwenden hochfeste kryptografische Algorithmen. Diese Regel verlangt, dass Sie eine vordefinierte Sicherheitsrichtlinie für Ihre SSL-Liste

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			ner festlegen. Die Standard-Sicherheitsrichtlinie lautet: Policy-TLS-1-2-2017-0. ELBSecurity Der tatsächliche Wert muss den Richtlinien Ihrer Organisation entsprechen.
164.312(e)(2)(i)	(i) Integritätskontrollen (adressierbar). Implementieren Sie Sicherheitsmaßnahmen, um dafür zu sorgen, dass elektronisch übertragene und elektronisch geschützte Gesundheitsinformationen bis zu ihrer Löschung nicht unbemerkt verändert werden.	elb-tls-https-listeners-nur	Stellen Sie sicher, dass Ihre Elastic Load Balancer (ELBs) mit SSL- oder HTTPS-Listenern konfiguriert sind. Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.312(e)(2)(i)	(i) Integritätskontrollen (adressierbar). Implementieren Sie Sicherheitsmaßnahmen, um dafür zu sorgen, dass elektronisch übertragene und elektronisch geschützte Gesundheitsinformationen bis zu ihrer Löschung nicht unbemerkt verändert werden.	redshift-require-tls-ssl	Stellen Sie sicher, dass Ihre Amazon-Redshift-Cluster eine TLS/SSL-Verschlüsselung erfordern, um eine Verbindung zu SQL-Clients herzustellen. Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.
164.312(e)(2)(i)	(i) Integritätskontrollen (adressierbar). Implementieren Sie Sicherheitsmaßnahmen, um dafür zu sorgen, dass elektronisch übertragene und elektronisch geschützte Gesundheitsinformationen bis zu ihrer Löschung nicht unbemerkt verändert werden.	s-3 bucket-ssl-requests-only	Um Daten während der Übertragung zu schützen, stellen Sie sicher, dass Ihre Amazon Simple Storage Service (Amazon S3)-Buckets Anfragen zur Verwendung von Secure Socket Layer (SSL)-Buckets erfordern. Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.312(e)(2)(i)	(i) Integritätskontrollen (adressierbar). Implementieren Sie Sicherheitsmaßnahmen, um dafür zu sorgen, dass elektronisch übertragene und elektronisch geschützte Gesundheitsinformationen bis zu ihrer Löschung nicht unbemerkt verändert werden.	opensearch-https-required	Da sensible Daten existieren können und um Daten während der Übertragung zu schützen, sollten Sie sicherstellen, dass HTTPS für Verbindungen zu Ihren Amazon OpenSearch Service-Domains aktiviert ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.312(e)(2)(i)	(i) Integritätskontrollen (adressierbar). Implementieren Sie Sicherheitsmaßnahmen, um dafür zu sorgen, dass elektronisch übertragene und elektronisch geschützte Gesundheitsinformationen bis zu ihrer Löschung nicht unbemerkt verändert werden.	opensearch-node-to-node-Verschlüsselungsprüfung	Stellen Sie sicher, dass die node-to-node Verschlüsselung für Amazon OpenSearch Service aktiviert ist. Node-to-nodeVerschlüsselung ermöglicht die TLS 1.2-Verschlüsselung für die gesamte Kommunikation innerhalb der Amazon Virtual Private Cloud (Amazon VPC). Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.312(e)(2)(ii)	(ii) Verschlüsselung (adressierbar). Implementieren Sie einen Mechanismus zur bedarfswe isen Verschlüs selung elektroni sch geschützter Gesundheitsinforma tionen.	alb-http-to-https-Umleitungsprüfung	Um Daten während der Übertragung zu schützen, stellen Sie sicher, dass Ihr Application Load Balancer unverschl üsselte HTTP-Anfr agen automatisch an HTTPS umleitet. Um eventuell vorhanden e sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.
164.312(e)(2)(ii)	(ii) Verschlüsselung (adressierbar). Implementieren Sie einen Mechanismus zur bedarfswe isen Verschlüs selung elektroni sch geschützter Gesundheitsinforma tionen.	api-gw-ssl-enabled	Stellen Sie sicher, dass die REST-API-Stufen von Amazon API Gateway mit SSL-Zertifikaten konfiguri ert sind, damit Backend-Systeme überprüfen können, ob Anforderungen von API Gateway stammen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.312(e)(2)(ii)	(ii) Verschlüsselung (adressierbar). Implementieren Sie einen Mechanismus zur bedarfswe isen Verschlüs selung elektroni sch geschützter Gesundheitsinforma tionen.	cloud-trail-encryption-enabled	Da sensible Daten vorhanden sein können und um Daten im Speicher zu schützen, sollten Sie sicherstellen, dass die Verschlüsselung für Ihre Trails aktiviert ist. AWS CloudTrail
164.312(e)(2)(ii)	(ii) Verschlüsselung (adressierbar). Implementieren Sie einen Mechanismus zur bedarfswe isen Verschlüs selung elektroni sch geschützter Gesundheitsinforma tionen.	ec-2 ebs-encryption-by-default	Zum Schutz von Daten im Ruhezustand müssen Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon Elastic Block Store (Amazon EBS)-Volumes aktiviert ist. Da sensible Daten auch im Ruhezustand vorhanden sein können, sollten Sie die Verschlüsselung im Ruhezustand aktivieren, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.312(e)(2)(ii)	(ii) Verschlüsselung (adressierbar). Implementieren Sie einen Mechanismus zur bedarfswe isen Verschlüs selung elektroni sch geschützter Gesundheitsinforma tionen.	efs-encrypted-check	Aktivieren Sie die Verschlüsselung für Ihr Amazon Elastic File System (EFS), um eventuell vorhandene sensible Daten sowie Daten im Ruhezustand zu schützen.
164.312(e)(2)(ii)	(ii) Verschlüsselung (adressierbar). Implementieren Sie einen Mechanismus zur bedarfswe isen Verschlüs selung elektroni sch geschützter Gesundheitsinforma tionen.	elasticsearch-encr ypted-at-rest	Da sensible Daten vorhanden sein können und um Daten im Ruhezustand zu schützen, sollten Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon OpenSearch Service (OpenSearch Service) -Domains aktiviert ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.312(e)(2)(ii)	(ii) Verschlüsselung (adressierbar). Implementieren Sie einen Mechanismus zur bedarfswe isen Verschlüs selung elektroni sch geschützter Gesundheitsinforma tionen.	elasticsearch-node -to-node-Verschlüs selungsprüfung	Stellen Sie sicher, dass die node-to-node Verschlüs selung für Amazon OpenSearch Service aktiviert ist. Node-to-nodeVerschlüsselung ermöglicht die TLS 1.2-Verschlüsselun g für die gesamte Kommunikation innerhalb der Amazon Virtual Private Cloud (Amazon VPC). Um eventuell vorhanden e sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.312(e)(2)(ii)	(ii) Verschlüsselung (adressierbar). Implementieren Sie einen Mechanismus zur bedarfswe isen Verschlüs selung elektroni sch geschützter Gesundheitsinforma tionen.	elb-acm-certificate-required	Zum Schutz von eventuell vorhanden en sensiblen Daten sowie von Daten während der Übertragung muss die Verschlüsselung für Ihr Elastic Load Balancing aktiviert sein. Verwenden Sie AWS Certificate Manager, um öffentlic he und private SSL/ TLS-Zertifikate mit AWS Diensten und internen Ressource n zu verwalten, bereitzustellen und bereitzustellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.312(e)(2)(ii)	(ii) Verschlüsselung (adressierbar). Implementieren Sie einen Mechanismus zur bedarfswe isen Verschlüs selung elektroni sch geschützter Gesundheitsinforma tionen.	elb-predefined-security-policy-ssl-check	Stellen Sie sicher, dass Ihre SSL-Listener von Classic Elastic Load Balancing eine vordefinierte Sicherheitsrichtlinie verwenden, um Daten während der Übertragung zu schützen. Elastic Load Balancing bietet vordefinierte Aushandlungskonfigurationen, die für die SSL-Aushandlung verwendet werden, wenn eine Verbindung zwischen einem Client und Ihrem Load Balancer hergestellt wurde. Die SSL-Aushandlungskonfigurationen sind mit einer breiten Palette von Clients kompatibel und verwenden hochfeste kryptografische Algorithmen. Diese Regel verlangt, dass Sie eine vordefinierte Sicherheitsrichtlinie für Ihre SSL-Liste

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			ner festlegen. Die Standard-Sicherheitsrichtlinie lautet: Policy-TLS-1-2-2017-0. ELBSecurity Der tatsächliche Wert muss den Richtlinien Ihrer Organisation entsprechen.
164.312(e)(2)(ii)	(ii) Verschlüsselung (adressierbar). Implementieren Sie einen Mechanismus zur bedarfswe isen Verschlüsselung elektronisch geschützter Gesundheitsinformationen.	elb-tls-https-listeners-nur	Stellen Sie sicher, dass Ihre Elastic Load Balancer (ELBs) mit SSL- oder HTTPS-Listenern konfiguriert sind. Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.
164.312(e)(2)(ii)	(ii) Verschlüsselung (adressierbar). Implementieren Sie einen Mechanismus zur bedarfswe isen Verschlüsselung elektronisch geschützter Gesundheitsinformationen.	encrypted-volumes	Aktivieren Sie die Verschlüsselung für Ihre Amazon-Elastic-Block-Store (Amazon-EBS)-Volumes, um eventuell vorhandene sensible Daten sowie Daten im Ruhezustand zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.312(e)(2)(ii)	(ii) Verschlüsselung (adressierbar). Implementieren Sie einen Mechanismus zur bedarfswe isen Verschlüs selung elektroni sch geschützter Gesundheitsinforma tionen.	rds-snapshot-encry pted	Stellen Sie sicher, dass die Verschlüs selung für Ihre Amazon Relationa l Database Service (Amazon RDS)-Snap shots aktiviert ist. Da sensible Daten auch im Ruhezusta nd vorhanden sein können, sollten Sie die Verschlüsselung im Ruhezustand aktivieren, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.312(e)(2)(ii)	(ii) Verschlüsselung (adressierbar). Implementieren Sie einen Mechanismus zur bedarfswe isen Verschlüs selung elektroni sch geschützter Gesundheitsinforma tionen.	rds-storage-encrypted	Zum Schutz von Daten im Ruhezusta nd müssen Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon Relational Database Service (Amazon RDS)-Instances aktiviert ist. Um eventuell vorhanden e sensible Daten im Ruhezustand in Amazon-RDS-Instanc es zu schützen, muss die Verschlüs selung von Daten im Ruhezustand aktiviert sein.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.312(e)(2)(ii)	(ii) Verschlüsselung (adressierbar). Implementieren Sie einen Mechanismus zur bedarfswe isen Verschlüs selung elektroni sch geschützter Gesundheitsinforma tionen.	redshift-cluster-c onfiguration-check	Um Daten im Ruhezustand zu schützen, muss die Verschlüsselung für Ihre Amazon-Re dshift-Cluster aktiviert sein. Sie müssen auch sicherstellen, dass die erforderl ichen Konfigurationen auf Amazon-Redshift-Clustern bereitges tellt werden. Die Prüfungsprotokolli erung muss aktiviert sein, um Informati onen zu Verbindun gen und Benutzera ktivitäten in der Datenbank bereitzus tellen. Diese Regel erfordert, dass ein Wert für clusterDb Encrypted (Config Default: TRUE) und LoggingEnabled (Config Default: TRUE) gesetzt ist. Die tatsächlichen Werte müssen den Richtlini en Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.312(e)(2)(ii)	(ii) Verschlüsselung (adressierbar). Implementieren Sie einen Mechanismus zur bedarfswe isen Verschlüs selung elektroni sch geschützter Gesundheitsinforma tionen.	redshift-require-tls-ssl	Stellen Sie sicher, dass Ihre Amazon-Redshift-Cluster eine TLS/SSL-Verschlüss elung erfordern, um eine Verbindun g zu SQL-Clients herzustellen. Um eventuell vorhanden e sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.
164.312(e)(2)(ii)	(ii) Verschlüsselung (adressierbar). Implementieren Sie einen Mechanismus zur bedarfswe isen Verschlüs selung elektroni sch geschützter Gesundheitsinforma tionen.	s3-aktiviert bucket-se rver-side-encryption	Zum Schutz von Daten im Ruhezusta nd müssen Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon Simple Storage Service (Amazon S3)-Bucke ts aktiviert ist. Um eventuell vorhanden e sensible Daten im Ruhezustand in Amazon-S3-Buckets zu schützen, muss die Verschlüsselung aktiviert sein.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.312(e)(2)(ii)	(ii) Verschlüsselung (adressierbar). Implementieren Sie einen Mechanismus zur bedarfswe isen Verschlüs selung elektroni sch geschützter Gesundheitsinforma tionen.	s-3 bucket-ssl-requests-only	Um Daten während der Übertragung zu schützen, stellen Sie sicher, dass Ihre Amazon Simple Storage Service (Amazon S3)-Buckets Anfragen zur Verwendung von Secure Socket Layer (SSL)-Buckets erfordern. Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.
164.312(e)(2)(ii)	(ii) Verschlüsselung (adressierbar). Implementieren Sie einen Mechanismus zur bedarfswe isen Verschlüs selung elektroni sch geschützter Gesundheitsinforma tionen.	s-3 default-encryption-kms	Stellen Sie sicher, dass die Verschlüs selung für Ihre Amazon Simple Storage Service (Amazon S3)-Buckets aktiviert ist. Um eventuell vorhandene sensible Daten im Ruhezustand in einem Amazon-S3-Bucket zu schützen, muss die Verschlüsselung aktiviert sein.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.312(e)(2)(ii)	(ii) Verschlüsselung (adressierbar). Implementieren Sie einen Mechanismus zur bedarfswe isen Verschlüs selung elektroni sch geschützter Gesundheitsinforma tionen.	sagemaker-endpoint -configuration-kms-key-konfiguriert	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass die Verschlüsselung mit dem AWS Key Management Service (AWS KMS) für Ihren Endpunkt aktiviert ist. SageMaker Da sensible Daten auf dem SageMaker Endgerät gespeiche rt werden können, sollten Sie die Verschlüsselung im Ruhezustand aktiviere n, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.312(e)(2)(ii)	(ii) Verschlüsselung (adressierbar). Implementieren Sie einen Mechanismus zur bedarfswe isen Verschlüs selung elektroni sch geschützter Gesundheitsinforma tionen.	sagemaker-notebook-instance-kms-schlüsselkonfiguriert	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass die Verschlüsselung mit dem AWS Key Management Service (AWS KMS) für Ihr Notebook aktiviert ist. SageMaker Da vertrauliche Daten im SageMaker Notebook gespeichert werden können, sollten Sie die Verschlüsselung im Ruhezustand aktivieren, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.312(e)(2)(ii)	(ii) Verschlüsselung (adressierbar). Implementieren Sie einen Mechanismus zur bedarfswe isen Verschlüs selung elektroni sch geschützter Gesundheitsinforma tionen.	sns-encrypted-kms	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass Ihre Amazon Simple Notification Service (Amazon SNS) -Themen mit dem AWS Key Management Service (AWS KMS) verschlüsselt werden müssen. Um eventuell vorhandene sensible Daten im Ruhezusta nd in veröffentlichten Nachrichten zu schützen, muss die Verschlüsselung von Daten im Ruhezusta nd aktiviert sein.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.312(e)(2)(ii)	(ii) Verschlüsselung (adressierbar). Implementieren Sie einen Mechanismus zur bedarfswe isen Verschlüs selung elektroni sch geschützter Gesundheitsinforma tionen.	secretsmanager-using-cmk	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass die Verschlüsselung mit dem AWS Key Management Service (AWS KMS) für AWS Secrets Manager aktiviert ist. Aktiviere n Sie die Verschlüs selung von Daten im Ruhezustand, um eventuell vorhanden e sensible Daten im Ruhezustand im Secrets Manager zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.312(e)(2)(ii)	(ii) Verschlüsselung (adressierbar). Implementieren Sie einen Mechanismus zur bedarfswe isen Verschlüs selung elektroni sch geschützter Gesundheitsinforma tionen.	elbv2- acm-certificate-required	Zum Schutz von eventuell vorhanden en sensiblen Daten sowie von Daten während der Übertragung muss die Verschlüsselung für Ihr Elastic Load Balancing aktiviert sein. Verwenden Sie AWS Certificate Manager, um öffentlic he und private SSL/ TLS-Zertifikate mit AWS Diensten und internen Ressource n zu verwalten, bereitzustellen und bereitzustellen.
164.312(e)(2)(ii)	(ii) Verschlüsselung (adressierbar). Implementieren Sie einen Mechanismus zur bedarfswe isen Verschlüs selung elektroni sch geschützter Gesundheitsinforma tionen.	opensearch-encrypt ed-at-rest	Da sensible Daten vorhanden sein können und um Daten im Ruhezustand zu schützen, sollten Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon OpenSearch Service-Domains aktiviert ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.312(e)(2)(ii)	(ii) Verschlüsselung (adressierbar). Implementieren Sie einen Mechanismus zur bedarfswe isen Verschlüs selung elektroni sch geschützter Gesundheitsinforma tionen.	opensearch-https-required	Da sensible Daten existieren können und um Daten während der Übertragung zu schützen, sollten Sie sicherstellen, dass HTTPS für Verbindungen zu Ihren Amazon OpenSearch Service-Domains aktiviert ist.
164.312(e)(2)(ii)	(ii) Verschlüsselung (adressierbar). Implementieren Sie einen Mechanismus zur bedarfswe isen Verschlüs selung elektroni sch geschützter Gesundheitsinforma tionen.	opensearch-node-to-node-Verschlüsselungsprüfung	Stellen Sie sicher, dass die node-to-node Verschlüs selung für Amazon OpenSearch Service aktiviert ist. Node-to-nodeVerschlüsselung ermöglicht die TLS 1.2-Verschlüsselung für die gesamte Kommunikation innerhalb der Amazon Virtual Private Cloud (Amazon VPC). Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.312(e)(2)(ii)	(ii) Verschlüsselung (adressierbar). Implementieren Sie einen Mechanismus zur bedarfswe isen Verschlüs selung elektroni sch geschützter Gesundheitsinforma tionen.	kinesis-stream-encrypted	Aktivieren Sie die Verschlüsselung für Ihre Amazon-Kinesis-Streams, um eventuell vorhandene sensible Daten sowie Daten im Ruhezustand zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.314(b)(1)	(b)(1) Standard: Anforderungen an kollektive Gesundheitspläne. Sofern die einzigen elektronisch geschützten Gesundheitsinformationen nicht gemäß 164.504(f)(1)(ii) oder (iii) oder gemäß 164.508 an einen Versicherer weitergegeben werden, muss in den Versicherungsunterlagen eines kollektiven Gesundheitsplans festgelegt sein, dass der Versicherer elektronisch geschützte Gesundheitsinformationen, die für den kollektiven Gesundheitsplan erstellt, empfangen, verwaltet oder von oder an diesen übermittelt werden, angemessen schützt.	cloud-trail-encryption-enabled	Da sensible Daten vorhanden sein können und um Daten im Ruhezustand zu schützen, sollten Sie sicherstellen, dass die Verschlüsselung für Ihre AWS CloudTrail Trails aktiviert ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.314(b)(1)	(b)(1) Standard: Anforderungen an kollektive Gesundheitspläne. Sofern die einzigen elektronisch geschützten Gesundheitsinformationen nicht gemäß 164.504(f)(1)(ii) oder (iii) oder gemäß 164.508 an einen Versicherer weitergegeben werden, muss in den Versicherungsunterlagen eines kollektiven Gesundheitsplans festgelegt sein, dass der Versicherer elektronisch geschützte Gesundheitsinformationen, die für den kollektiven Gesundheitsplan erstellt, empfangen, verwaltet oder von oder an diesen übermittelt werden, angemessen schützt.	ec-2 ebs-encryption-by-default	Zum Schutz von Daten im Ruhezustand müssen Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon Elastic Block Store (Amazon EBS)-Volumes aktiviert ist. Da sensible Daten auch im Ruhezustand vorhanden sein können, sollten Sie die Verschlüsselung im Ruhezustand aktivieren, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.314(b)(1)	(b)(1) Standard: Anforderungen an kollektive Gesundheitspläne. Sofern die einzigen elektronisch geschützten Gesundheitsinformationen nicht gemäß 164.504(f)(1)(ii) oder (iii) oder gemäß 164.508 an einen Versicherer weitergegeben werden, muss in den Versicherungsunterlagen eines kollektiven Gesundheitsplans festgelegt sein, dass der Versicherer elektronisch geschützte Gesundheitsinformationen, die für den kollektiven Gesundheitsplan erstellt, empfangen, verwaltet oder von oder an diesen übermittelt werden, angemessen schützt.	elasticsearch-encrypted-at-rest	Da sensible Daten vorhanden sein können und um Daten im Ruhezustand zu schützen, sollten Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon OpenSearch Service (OpenSearch Service)-Domains aktiviert ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.314(b)(1)	(b)(1) Standard: Anforderungen an kollektive Gesundheitspläne. Sofern die einzigen elektronisch geschützten Gesundheitsinformationen nicht gemäß 164.504(f)(1)(ii) oder (iii) oder gemäß 164.508 an einen Versicherer weitergegeben werden, muss in den Versicherungsunterlagen eines kollektiven Gesundheitsplans festgelegt sein, dass der Versicherer elektronisch geschützte Gesundheitsinformationen, die für den kollektiven Gesundheitsplan erstellt, empfangen, verwaltet oder von oder an diesen übermittelt werden, angemessen schützt.	elasticsearch-node-to-node-Verschlüsselungsprüfung	Stellen Sie sicher, dass die node-to-node Verschlüsselung für Amazon OpenSearch Service aktiviert ist. Node-to-nodeVerschlüsselung ermöglicht die TLS 1.2-Verschlüsselung für die gesamte Kommunikation innerhalb der Amazon Virtual Private Cloud (Amazon VPC). Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.314(b)(1)	(b)(1) Standard: Anforderungen an kollektive Gesundheitspläne. Sofern die einzigen elektronisch geschützten Gesundheitsinformationen nicht gemäß 164.504(f)(1)(ii) oder (iii) oder gemäß 164.508 an einen Versicherer weitergegeben werden, muss in den Versicherungsunterlagen eines kollektiven Gesundheitsplans festgelegt sein, dass der Versicherer elektronisch geschützte Gesundheitsinformationen, die für den kollektiven Gesundheitsplan erstellt, empfangen, verwaltet oder von oder an diesen übermittelt werden, angemessen schützt.	elb-tls-https-listeners-nur	Stellen Sie sicher, dass Ihre Elastic Load Balancer (ELBs) mit SSL- oder HTTPS-Listenern konfiguriert sind. Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.314(b)(1)	(b)(1) Standard: Anforderungen an kollektive Gesundheitspläne. Sofern die einzigen elektronisch geschützten Gesundheitsinformationen nicht gemäß 164.504(f)(1)(ii) oder (iii) oder gemäß 164.508 an einen Versicherer weitergegeben werden, muss in den Versicherungsunterlagen eines kollektiven Gesundheitsplans festgelegt sein, dass der Versicherer elektronisch geschützte Gesundheitsinformationen, die für den kollektiven Gesundheitsplan erstellt, empfangen, verwaltet oder von oder an diesen übermittelt werden, angemessen schützt.	encrypted-volumes	Aktivieren Sie die Verschlüsselung für Ihre Amazon-Elastic-Block-Store (Amazon-EBS)-Volumes, um eventuell vorhandene sensible Daten sowie Daten im Ruhezustand zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.314(b)(1)	(b)(1) Standard: Anforderungen an kollektive Gesundheitspläne. Sofern die einzigen elektronisch geschützten Gesundheitsinformationen nicht gemäß 164.504(f)(1)(ii) oder (iii) oder gemäß 164.508 an einen Versicherer weitergegeben werden, muss in den Versicherungsunterlagen eines kollektiven Gesundheitsplans festgelegt sein, dass der Versicherer elektronisch geschützte Gesundheitsinformationen, die für den kollektiven Gesundheitsplan erstellt, empfangen, verwaltet oder von oder an diesen übermittelt werden, angemessen schützt.	opensearch-encrypted-at-rest	Da sensible Daten vorhanden sein können und um Daten im Ruhezustand zu schützen, sollten Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon OpenSearch Service-Domains aktiviert ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.314(b)(1)	(b)(1) Standard: Anforderungen an kollektive Gesundheitspläne. Sofern die einzigen elektronisch geschützten Gesundheitsinformationen nicht gemäß 164.504(f)(1)(ii) oder (iii) oder gemäß 164.508 an einen Versicherer weitergegeben werden, muss in den Versicherungsunterlagen eines kollektiven Gesundheitsplans festgelegt sein, dass der Versicherer elektronisch geschützte Gesundheitsinformationen, die für den kollektiven Gesundheitsplan erstellt, empfangen, verwaltet oder von oder an diesen übermittelt werden, angemessen schützt.	opensearch-https-required	Da sensible Daten existieren können und um Daten während der Übertragung zu schützen, sollten Sie sicherstellen, dass HTTPS für Verbindungen zu Ihren Amazon OpenSearch Service-Domains aktiviert ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.314(b)(1)	(b)(1) Standard: Anforderungen an kollektive Gesundheitspläne. Sofern die einzigen elektronisch geschützten Gesundheitsinformationen nicht gemäß 164.504(f)(1)(ii) oder (iii) oder gemäß 164.508 an einen Versicherer weitergegeben werden, muss in den Versicherungsunterlagen eines kollektiven Gesundheitsplans festgelegt sein, dass der Versicherer elektronisch geschützte Gesundheitsinformationen, die für den kollektiven Gesundheitsplan erstellt, empfangen, verwaltet oder von oder an diesen übermittelt werden, angemessen schützt.	opensearch-node-to-node-Verschlüsselungsprüfung	Stellen Sie sicher, dass die node-to-node Verschlüsselung für Amazon OpenSearch Service aktiviert ist. Node-to-nodeVerschlüsselung ermöglicht die TLS 1.2-Verschlüsselung für die gesamte Kommunikation innerhalb der Amazon Virtual Private Cloud (Amazon VPC). Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.314(b)(1)	(b)(1) Standard: Anforderungen an kollektive Gesundheitspläne. Sofern die einzigen elektronisch geschützten Gesundheitsinformationen nicht gemäß 164.504(f)(1)(ii) oder (iii) oder gemäß 164.508 an einen Versicherer weitergegeben werden, muss in den Versicherungsunterlagen eines kollektiven Gesundheitsplans festgelegt sein, dass der Versicherer elektronisch geschützte Gesundheitsinformationen, die für den kollektiven Gesundheitsplan erstellt, empfangen, verwaltet oder von oder an diesen übermittelt werden, angemessen schützt.	rds-snapshot-encrypted	Stellen Sie sicher, dass die Verschlüsselung für Ihre Amazon Relational Database Service (Amazon RDS)-Snapshots aktiviert ist. Da sensible Daten auch im Ruhezustand vorhanden sein können, sollten Sie die Verschlüsselung im Ruhezustand aktivieren, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.314(b)(1)	(b)(1) Standard: Anforderungen an kollektive Gesundheitspläne. Sofern die einzigen elektronisch geschützten Gesundheitsinformationen nicht gemäß 164.504(f)(1)(ii) oder (iii) oder gemäß 164.508 an einen Versicherer weitergegeben werden, muss in den Versicherungsunterlagen eines kollektiven Gesundheitsplans festgelegt sein, dass der Versicherer elektronisch geschützte Gesundheitsinformationen, die für den kollektiven Gesundheitsplan erstellt, empfangen, verwaltet oder von oder an diesen übermittelt werden, angemessen schützt.	rds-storage-encrypted	Zum Schutz von Daten im Ruhezustand müssen Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon Relational Database Service (Amazon RDS)-Instances aktiviert ist. Um eventuell vorhandene sensible Daten im Ruhezustand in Amazon-RDS-Instances zu schützen, muss die Verschlüsselung von Daten im Ruhezustand aktiviert sein.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.314(b)(1)	(b)(1) Standard: Anforderungen an kollektive Gesundheitspläne. Sofern die einzigen elektronisch geschützten Gesundheitsinformationen nicht gemäß 164.504(f)(1)(ii) oder (iii) oder gemäß 164.508 an einen Versicherer weitergegeben werden, muss in den Versicherungsunterlagen eines kollektiven Gesundheitsplans festgelegt sein, dass der Versicherer elektronisch geschützte Gesundheitsinformationen, die für den kollektiven Gesundheitsplan erstellt, empfangen, verwaltet oder von oder an diesen übermittelt werden, angemessen schützt.	redshift-cluster-public-access-überprüfen	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Redshift Redshift-Cluster nicht öffentlich sind. Amazon-Redshift-Cluster können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.314(b)(1)	(b)(1) Standard: Anforderungen an kollektive Gesundheitspläne. Sofern die einzigen elektronisch geschützten Gesundheitsinformationen nicht gemäß 164.504(f)(1)(ii) oder (iii) oder gemäß 164.508 an einen Versicherer weitergegeben werden, muss in den Versicherungsunterlagen eines kollektiven Gesundheitsplans festgelegt sein, dass der Versicherer elektronisch geschützte Gesundheitsinformationen, die für den kollektiven Gesundheitsplan erstellt, empfangen, verwaltet oder von oder an diesen übermittelt werden, angemessen schützt.	redshift-require-tls-ssl	Stellen Sie sicher, dass Ihre Amazon-Redshift-Cluster eine TLS/SSL-Verschlüsselung erfordern, um eine Verbindung zu SQL-Clients herzustellen. Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.314(b)(1)	(b)(1) Standard: Anforderungen an kollektive Gesundheitspläne. Sofern die einzigen elektronisch geschützten Gesundheitsinformationen nicht gemäß 164.504(f)(1)(ii) oder (iii) oder gemäß 164.508 an einen Versicherer weitergegeben werden, muss in den Versicherungsunterlagen eines kollektiven Gesundheitsplans festgelegt sein, dass der Versicherer elektronisch geschützte Gesundheitsinformationen, die für den kollektiven Gesundheitsplan erstellt, empfangen, verwaltet oder von oder an diesen übermittelt werden, angemessen schützt.	s-3 bucket-public-read-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie nur autorisierten Benutzern, Prozessen und Geräten Zugriff auf Amazon Simple Storage Service (Amazon S3) - Buckets gewähren. Die Verwaltung des Zugriffs sollte mit der Klassifizierung der Daten übereinstimmen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.314(b)(1)	(b)(1) Standard: Anforderungen an kollektive Gesundheitspläne. Sofern die einzigen elektronisch geschützten Gesundheitsinformationen nicht gemäß 164.504(f)(1)(ii) oder (iii) oder gemäß 164.508 an einen Versicherer weitergegeben werden, muss in den Versicherungsunterlagen eines kollektiven Gesundheitsplans festgelegt sein, dass der Versicherer elektronisch geschützte Gesundheitsinformationen, die für den kollektiven Gesundheitsplan erstellt, empfangen, verwaltet oder von oder an diesen übermittelt werden, angemessen schützt.	s3- bucket-public-write-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie nur autorisierten Benutzern, Prozessen und Geräten Zugriff auf Amazon Simple Storage Service (Amazon S3) - Buckets gewähren. Die Verwaltung des Zugriffs sollte mit der Klassifizierung der Daten übereinstimmen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.314(b)(1)	(b)(1) Standard: Anforderungen an kollektive Gesundheitspläne. Sofern die einzigen elektronisch geschützten Gesundheitsinformationen nicht gemäß 164.504(f)(1)(ii) oder (iii) oder gemäß 164.508 an einen Versicherer weitergegeben werden, muss in den Versicherungsunterlagen eines kollektiven Gesundheitsplans festgelegt sein, dass der Versicherer elektronisch geschützte Gesundheitsinformationen, die für den kollektiven Gesundheitsplan erstellt, empfangen, verwaltet oder von oder an diesen übermittelt werden, angemessen schützt.	s3-fähig bucket-server-side-encryption	Zum Schutz von Daten im Ruhezustand müssen Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon Simple Storage Service (Amazon S3)-Buckets aktiviert ist. Um eventuell vorhandene sensible Daten im Ruhezustand in Amazon-S3-Buckets zu schützen, muss die Verschlüsselung aktiviert sein.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.314(b)(1)	(b)(1) Standard: Anforderungen an kollektive Gesundheitspläne. Sofern die einzigen elektronisch geschützten Gesundheitsinformationen nicht gemäß 164.504(f)(1)(ii) oder (iii) oder gemäß 164.508 an einen Versicherer weitergegeben werden, muss in den Versicherungsunterlagen eines kollektiven Gesundheitsplans festgelegt sein, dass der Versicherer elektronisch geschützte Gesundheitsinformationen, die für den kollektiven Gesundheitsplan erstellt, empfangen, verwaltet oder von oder an diesen übermittelt werden, angemessen schützt.	s-3 bucket-ssl-requests-only	Um Daten während der Übertragung zu schützen, stellen Sie sicher, dass Ihre Amazon Simple Storage Service (Amazon S3)-Buckets Anfragen zur Verwendung von Secure Socket Layer (SSL)-Buckets erfordern. Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.314(b)(1)	(b)(1) Standard: Anforderungen an kollektive Gesundheitspläne. Sofern die einzigen elektronisch geschützten Gesundheitsinformationen nicht gemäß 164.504(f)(1)(ii) oder (iii) oder gemäß 164.508 an einen Versicherer weitergegeben werden, muss in den Versicherungsunterlagen eines kollektiven Gesundheitsplans festgelegt sein, dass der Versicherer elektronisch geschützte Gesundheitsinformationen, die für den kollektiven Gesundheitsplan erstellt, empfangen, verwaltet oder von oder an diesen übermittelt werden, angemessen schützt.	s-3 default-encryption-kms	Stellen Sie sicher, dass die Verschlüsselung für Ihre Amazon Simple Storage Service (Amazon S3)-Buckets aktiviert ist. Um eventuell vorhandene sensible Daten im Ruhezustand in einem Amazon-S3-Bucket zu schützen, muss die Verschlüsselung aktiviert sein.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.314(b)(1)	(b)(1) Standard: Anforderungen an kollektive Gesundheitspläne. Sofern die einzigen elektronisch geschützten Gesundheitsinformationen nicht gemäß 164.504(f)(1)(ii) oder (iii) oder gemäß 164.508 an einen Versicherer weitergegeben werden, muss in den Versicherungsunterlagen eines kollektiven Gesundheitsplans festgelegt sein, dass der Versicherer elektronisch geschützte Gesundheitsinformationen, die für den kollektiven Gesundheitsplan erstellt, empfangen, verwaltet oder von oder an diesen übermittelt werden, angemessen schützt.	sagemaker-endpoint-configuration-kms-key-konfiguriert	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass die Verschlüsselung mit dem AWS Key Management Service (AWS KMS) für Ihren Endpunkt aktiviert ist. SageMaker Da sensible Daten auf dem SageMaker Endgerät gespeichert werden können, sollten Sie die Verschlüsselung im Ruhezustand aktivieren, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.314(b)(1)	(b)(1) Standard: Anforderungen an kollektive Gesundheitspläne. Sofern die einzigen elektronisch geschützten Gesundheitsinformationen nicht gemäß 164.504(f)(1)(ii) oder (iii) oder gemäß 164.508 an einen Versicherer weitergegeben werden, muss in den Versicherungsunterlagen eines kollektiven Gesundheitsplans festgelegt sein, dass der Versicherer elektronisch geschützte Gesundheitsinformationen, die für den kollektiven Gesundheitsplan erstellt, empfangen, verwaltet oder von oder an diesen übermittelt werden, angemessen schützt.	sagemaker-notebook-instance-kms-schlüsselkonfiguriert	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass die Verschlüsselung mit dem AWS Key Management Service (AWS KMS) für Ihr Notebook aktiviert ist. SageMaker Da vertrauliche Daten im SageMaker Notebook gespeichert werden können, sollten Sie die Verschlüsselung im Ruhezustand aktivieren, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.314(b)(2)	(2) Implementierungsspezifikationen (erforderlich). Die Dokumente des kollektiven Gesundheitsplans müssen dahingehend geändert werden, dass der Versicherungsträger: (i) administrative, physische und technische Sicherheitsvorkehrungen trifft, die die Vertraulichkeit, Integrität und Verfügbarkeit der elektronisch geschützten Gesundheitsinformationen, die er im Namen des kollektiven Gesundheitsplans erstellt, empfängt, verwaltet oder übermittelt, sinnvoll und angemessen schützt; (ii) sicherstellt, dass die in 164.504(f)(2)(iii) vorgeschriebene angemessene Trennung durch sinnvolle und	cloud-trail-encryption-enabled	Da sensible Daten vorhanden sein können und um Daten im Speicher zu schützen, sollten Sie sicherstellen, dass die Verschlüsselung für Ihre AWS CloudTrail Spuren aktiviert ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	angemessene Sicherheitsmaßnahmen unterstützt wird; (iii) sicherstellt, dass sich der Beauftragte, einschließlich eines Unterauftragnehmers, dem er diese Informationen zur Verfügung stellt, damit einverstanden erklärt, sinnvolle und angemessene Sicherheitsmaßnahmen zum Schutz der Informationen zu ergreifen; und (iv) dem kollektiven Gesundheitsplan alle Sicherheitsvorfälle meldet, von dem er Kenntnis erlangt.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.314(b)(2)	(2) Implementierungsspezifikationen (erforderlich). Die Dokumente des kollektiven Gesundheitsplans müssen dahingehend geändert werden, dass der Versicherungsträger: (i) administrative, physische und technische Sicherheitsvorkehrungen trifft, die die Vertraulichkeit, Integrität und Verfügbarkeit der elektronisch geschützten Gesundheitsinformationen, die er im Namen des kollektiven Gesundheitsplans erstellt, empfängt, verwaltet oder übermittelt, sinnvoll und angemessen schützt; (ii) sicherstellt, dass die in 164.504(f)(2)(iii) vorgeschriebene angemessene Trennung durch sinnvolle und	ec-2 ebs-encryption-by-default	Zum Schutz von Daten im Ruhezustand müssen Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon Elastic Block Store (Amazon EBS)-Volumes aktiviert ist. Da sensible Daten auch im Ruhezustand vorhanden sein können, sollten Sie die Verschlüsselung im Ruhezustand aktivieren, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	angemessene Sicherheitsmaßnahmen unterstützt wird; (iii) sicherstellt, dass sich der Beauftragte, einschließlich eines Unterauftragnehmers, dem er diese Informationen zur Verfügung stellt, damit einverstanden erklärt, sinnvolle und angemessene Sicherheitsmaßnahmen zum Schutz der Informationen zu ergreifen; und (iv) dem kollektiven Gesundheitsplan alle Sicherheitsvorfälle meldet, von dem er Kenntnis erlangt.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.314(b)(2)	(2) Implementierungsspezifikationen (erforderlich). Die Dokumente des kollektiven Gesundheitsplans müssen dahingehend geändert werden, dass der Versicherungsträger: (i) administrative, physische und technische Sicherheitsvorkehrungen trifft, die die Vertraulichkeit, Integrität und Verfügbarkeit der elektronisch geschützten Gesundheitsinformationen, die er im Namen des kollektiven Gesundheitsplans erstellt, empfängt, verwaltet oder übermittelt, sinnvoll und angemessen schützt; (ii) sicherstellt, dass die in 164.504(f)(2)(iii) vorgeschriebene angemessene Trennung durch sinnvolle und	elasticsearch-encrypted-at-rest	Da sensible Daten vorhanden sein können und um Daten im Ruhezustand zu schützen, sollten Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon OpenSearch Service (OpenSearch Service) -Domains aktiviert ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	angemessene Sicherheitsmaßnahmen unterstützt wird; (iii) sicherstellt, dass sich der Beauftragte, einschließlich eines Unterauftragnehmers, dem er diese Informationen zur Verfügung stellt, damit einverstanden erklärt, sinnvolle und angemessene Sicherheitsmaßnahmen zum Schutz der Informationen zu ergreifen; und (iv) dem kollektiven Gesundheitsplan alle Sicherheitsvorfälle meldet, von dem er Kenntnis erlangt.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.314(b)(2)	(2) Implementierungsspezifikationen (erforderlich). Die Dokumente des kollektiven Gesundheitsplans müssen dahingehend geändert werden, dass der Versicherungsträger: (i) administrative, physische und technische Sicherheitsvorkehrungen trifft, die die Vertraulichkeit, Integrität und Verfügbarkeit der elektronisch geschützten Gesundheitsinformationen, die er im Namen des kollektiven Gesundheitsplans erstellt, empfängt, verwaltet oder übermittelt, sinnvoll und angemessen schützt; (ii) sicherstellt, dass die in 164.504(f)(2)(iii) vorgeschriebene angemessene Trennung durch sinnvolle und	elasticsearch-node-to-node-Verschlüsselungsprüfung	Stellen Sie sicher, dass die node-to-node Verschlüsselung für Amazon OpenSearch Service aktiviert ist. Node-to-nodeVerschlüsselung ermöglicht die TLS 1.2-Verschlüsselung für die gesamte Kommunikation innerhalb der Amazon Virtual Private Cloud (Amazon VPC). Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	angemessene Sicherheitsmaßnahmen unterstützt wird; (iii) sicherstellt, dass sich der Beauftragte, einschließlich eines Unterauftragnehmers, dem er diese Informationen zur Verfügung stellt, damit einverstanden erklärt, sinnvolle und angemessene Sicherheitsmaßnahmen zum Schutz der Informationen zu ergreifen; und (iv) dem kollektiven Gesundheitsplan alle Sicherheitsvorfälle meldet, von dem er Kenntnis erlangt.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.314(b)(2)	(2) Implementierungsspezifikationen (erforderlich). Die Dokumente des kollektiven Gesundheitsplans müssen dahingehend geändert werden, dass der Versicherungsträger: (i) administrative, physische und technische Sicherheitsvorkehrungen trifft, die die Vertraulichkeit, Integrität und Verfügbarkeit der elektronisch geschützten Gesundheitsinformationen, die er im Namen des kollektiven Gesundheitsplans erstellt, empfängt, verwaltet oder übermittelt, sinnvoll und angemessen schützt; (ii) sicherstellt, dass die in 164.504(f)(2)(iii) vorgeschriebene angemessene Trennung durch sinnvolle und	elb-tls-https-listeners-nur	Stellen Sie sicher, dass Ihre Elastic Load Balancer (ELBs) mit SSL- oder HTTPS-Listenern konfiguriert sind. Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	angemessene Sicherheitsmaßnahmen unterstützt wird; (iii) sicherstellt, dass sich der Beauftragte, einschließlich eines Unterauftragnehmers, dem er diese Informationen zur Verfügung stellt, damit einverstanden erklärt, sinnvolle und angemessene Sicherheitsmaßnahmen zum Schutz der Informationen zu ergreifen; und (iv) dem kollektiven Gesundheitsplan alle Sicherheitsvorfälle meldet, von dem er Kenntnis erlangt.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.314(b)(2)	(2) Implementierungsspezifikationen (erforderlich). Die Dokumente des kollektiven Gesundheitsplans müssen dahingehend geändert werden, dass der Versicherungsträger: (i) administrative, physische und technische Sicherheitsvorkehrungen trifft, die die Vertraulichkeit, Integrität und Verfügbarkeit der elektronisch geschützten Gesundheitsinformationen, die er im Namen des kollektiven Gesundheitsplans erstellt, empfängt, verwaltet oder übermittelt, sinnvoll und angemessen schützt; (ii) sicherstellt, dass die in 164.504(f)(2)(iii) vorgeschriebene angemessene Trennung durch sinnvolle und	encrypted-volumes	Aktivieren Sie die Verschlüsselung für Ihre Amazon-Elastic-Block-Store (Amazon-EBS)-Volumes, um eventuell vorhandene sensible Daten sowie Daten im Ruhezustand zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	angemessene Sicherheitsmaßnahmen unterstützt wird; (iii) sicherstellt, dass sich der Beauftragte, einschließlich eines Unterauftragnehmers, dem er diese Informationen zur Verfügung stellt, damit einverstanden erklärt, sinnvolle und angemessene Sicherheitsmaßnahmen zum Schutz der Informationen zu ergreifen; und (iv) dem kollektiven Gesundheitsplan alle Sicherheitsvorfälle meldet, von dem er Kenntnis erlangt.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.314(b)(2)	(2) Implementierungsspezifikationen (erforderlich). Die Dokumente des kollektiven Gesundheitsplans müssen dahingehend geändert werden, dass der Versicherungsträger: (i) administrative, physische und technische Sicherheitsvorkehrungen trifft, die die Vertraulichkeit, Integrität und Verfügbarkeit der elektronisch geschützten Gesundheitsinformationen, die er im Namen des kollektiven Gesundheitsplans erstellt, empfängt, verwaltet oder übermittelt, sinnvoll und angemessen schützt; (ii) sicherstellt, dass die in 164.504(f)(2)(iii) vorgeschriebene angemessene Trennung durch sinnvolle und	opensearch-encrypted-at-rest	Da sensible Daten vorhanden sein können und um Daten im Ruhezustand zu schützen, sollten Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon OpenSearch Service-Domains aktiviert ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	angemessene Sicherheitsmaßnahmen unterstützt wird; (iii) sicherstellt, dass sich der Beauftragte, einschließlich eines Unterauftragnehmers, dem er diese Informationen zur Verfügung stellt, damit einverstanden erklärt, sinnvolle und angemessene Sicherheitsmaßnahmen zum Schutz der Informationen zu ergreifen; und (iv) dem kollektiven Gesundheitsplan alle Sicherheitsvorfälle meldet, von dem er Kenntnis erlangt.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.314(b)(2)	(2) Implementierungsspezifikationen (erforderlich). Die Dokumente des kollektiven Gesundheitsplans müssen dahingehend geändert werden, dass der Versicherungsträger: (i) administrative, physische und technische Sicherheitsvorkehrungen trifft, die die Vertraulichkeit, Integrität und Verfügbarkeit der elektronisch geschützten Gesundheitsinformationen, die er im Namen des kollektiven Gesundheitsplans erstellt, empfängt, verwaltet oder übermittelt, sinnvoll und angemessen schützt; (ii) sicherstellt, dass die in 164.504(f)(2)(iii) vorgeschriebene angemessene Trennung durch sinnvolle und	opensearch-https-required	Da sensible Daten existieren können und um Daten während der Übertragung zu schützen, sollten Sie sicherstellen, dass HTTPS für Verbindungen zu Ihren Amazon OpenSearch Service-Domains aktiviert ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	angemessene Sicherheitsmaßnahmen unterstützt wird; (iii) sicherstellt, dass sich der Beauftragte, einschließlich eines Unterauftragnehmers, dem er diese Informationen zur Verfügung stellt, damit einverstanden erklärt, sinnvolle und angemessene Sicherheitsmaßnahmen zum Schutz der Informationen zu ergreifen; und (iv) dem kollektiven Gesundheitsplan alle Sicherheitsvorfälle meldet, von dem er Kenntnis erlangt.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.314(b)(2)	(2) Implementierungsspezifikationen (erforderlich). Die Dokumente des kollektiven Gesundheitsplans müssen dahingehend geändert werden, dass der Versicherungsträger: (i) administrative, physische und technische Sicherheitsvorkehrungen trifft, die die Vertraulichkeit, Integrität und Verfügbarkeit der elektronisch geschützten Gesundheitsinformationen, die er im Namen des kollektiven Gesundheitsplans erstellt, empfängt, verwaltet oder übermittelt, sinnvoll und angemessen schützt; (ii) sicherstellt, dass die in 164.504(f)(2)(iii) vorgeschriebene angemessene Trennung durch sinnvolle und	opensearch-node-to-node-Verschlüsselungsprüfung	Stellen Sie sicher, dass die node-to-node Verschlüsselung für Amazon OpenSearch Service aktiviert ist. Node-to-nodeVerschlüsselung ermöglicht die TLS 1.2-Verschlüsselung für die gesamte Kommunikation innerhalb der Amazon Virtual Private Cloud (Amazon VPC). Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	angemessene Sicherheitsmaßnahmen unterstützt wird; (iii) sicherstellt, dass sich der Beauftragte, einschließlich eines Unterauftragnehmers, dem er diese Informationen zur Verfügung stellt, damit einverstanden erklärt, sinnvolle und angemessene Sicherheitsmaßnahmen zum Schutz der Informationen zu ergreifen; und (iv) dem kollektiven Gesundheitsplan alle Sicherheitsvorfälle meldet, von dem er Kenntnis erlangt.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.314(b)(2)	(2) Implementierungsspezifikationen (erforderlich). Die Dokumente des kollektiven Gesundheitsplans müssen dahingehend geändert werden, dass der Versicherungsträger: (i) administrative, physische und technische Sicherheitsvorkehrungen trifft, die die Vertraulichkeit, Integrität und Verfügbarkeit der elektronisch geschützten Gesundheitsinformationen, die er im Namen des kollektiven Gesundheitsplans erstellt, empfängt, verwaltet oder übermittelt, sinnvoll und angemessen schützt; (ii) sicherstellt, dass die in 164.504(f)(2)(iii) vorgeschriebene angemessene Trennung durch sinnvolle und	rds-snapshot-encrypted	Stellen Sie sicher, dass die Verschlüsselung für Ihre Amazon Relational Database Service (Amazon RDS)-Snapshots aktiviert ist. Da sensible Daten auch im Ruhezustand vorhanden sein können, sollten Sie die Verschlüsselung im Ruhezustand aktivieren, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	angemessene Sicherheitsmaßnahmen unterstützt wird; (iii) sicherstellt, dass sich der Beauftragte, einschließlich eines Unterauftragnehmers, dem er diese Informationen zur Verfügung stellt, damit einverstanden erklärt, sinnvolle und angemessene Sicherheitsmaßnahmen zum Schutz der Informationen zu ergreifen; und (iv) dem kollektiven Gesundheitsplan alle Sicherheitsvorfälle meldet, von dem er Kenntnis erlangt.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.314(b)(2)	(2) Implementierungsspezifikationen (erforderlich). Die Dokumente des kollektiven Gesundheitsplans müssen dahingehend geändert werden, dass der Versicherungsträger: (i) administrative, physische und technische Sicherheitsvorkehrungen trifft, die die Vertraulichkeit, Integrität und Verfügbarkeit der elektronisch geschützten Gesundheitsinformationen, die er im Namen des kollektiven Gesundheitsplans erstellt, empfängt, verwaltet oder übermittelt, sinnvoll und angemessen schützt; (ii) sicherstellt, dass die in 164.504(f)(2)(iii) vorgeschriebene angemessene Trennung durch sinnvolle und	rds-storage-encrypted	Zum Schutz von Daten im Ruhezustand müssen Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon Relational Database Service (Amazon RDS)-Instances aktiviert ist. Um eventuell vorhandene sensible Daten im Ruhezustand in Amazon-RDS-Instances zu schützen, muss die Verschlüsselung von Daten im Ruhezustand aktiviert sein.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	angemessene Sicherheitsmaßnahmen unterstützt wird; (iii) sicherstellt, dass sich der Beauftragte, einschließlich eines Unterauftragnehmers, dem er diese Informationen zur Verfügung stellt, damit einverstanden erklärt, sinnvolle und angemessene Sicherheitsmaßnahmen zum Schutz der Informationen zu ergreifen; und (iv) dem kollektiven Gesundheitsplan alle Sicherheitsvorfälle meldet, von dem er Kenntnis erlangt.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.314(b)(2)	(2) Implementierungsspezifikationen (erforderlich). Die Dokumente des kollektiven Gesundheitsplans müssen dahingehend geändert werden, dass der Versicherungsträger: (i) administrative, physische und technische Sicherheitsvorkehrungen trifft, die die Vertraulichkeit, Integrität und Verfügbarkeit der elektronisch geschützten Gesundheitsinformationen, die er im Namen des kollektiven Gesundheitsplans erstellt, empfängt, verwaltet oder übermittelt, sinnvoll und angemessen schützt; (ii) sicherstellt, dass die in 164.504(f)(2)(iii) vorgeschriebene angemessene Trennung durch sinnvolle und	redshift-cluster-public-access-überprüfen	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Redshift Redshift-Cluster nicht öffentlich sind. Amazon-Redshift-Cluster können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	angemessene Sicherheitsmaßnahmen unterstützt wird; (iii) sicherstellt, dass sich der Beauftragte, einschließlich eines Unterauftragnehmers, dem er diese Informationen zur Verfügung stellt, damit einverstanden erklärt, sinnvolle und angemessene Sicherheitsmaßnahmen zum Schutz der Informationen zu ergreifen; und (iv) dem kollektiven Gesundheitsplan alle Sicherheitsvorfälle meldet, von dem er Kenntnis erlangt.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.314(b)(2)	(2) Implementierungsspezifikationen (erforderlich). Die Dokumente des kollektiven Gesundheitsplans müssen dahingehend geändert werden, dass der Versicherungsträger: (i) administrative, physische und technische Sicherheitsvorkehrungen trifft, die die Vertraulichkeit, Integrität und Verfügbarkeit der elektronisch geschützten Gesundheitsinformationen, die er im Namen des kollektiven Gesundheitsplans erstellt, empfängt, verwaltet oder übermittelt, sinnvoll und angemessen schützt; (ii) sicherstellt, dass die in 164.504(f)(2)(iii) vorgeschriebene angemessene Trennung durch sinnvolle und	redshift-require-tls-ssl	Stellen Sie sicher, dass Ihre Amazon-Redshift-Cluster eine TLS/SSL-Verschlüsselung erfordern, um eine Verbindung zu SQL-Clients herzustellen. Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	angemessene Sicherheitsmaßnahmen unterstützt wird; (iii) sicherstellt, dass sich der Beauftragte, einschließlich eines Unterauftragnehmers, dem er diese Informationen zur Verfügung stellt, damit einverstanden erklärt, sinnvolle und angemessene Sicherheitsmaßnahmen zum Schutz der Informationen zu ergreifen; und (iv) dem kollektiven Gesundheitsplan alle Sicherheitsvorfälle meldet, von dem er Kenntnis erlangt.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.314(b)(2)	(2) Implementierungsspezifikationen (erforderlich). Die Dokumente des kollektiven Gesundheitsplans müssen dahingehend geändert werden, dass der Versicherungsträger: (i) administrative, physische und technische Sicherheitsvorkehrungen trifft, die die Vertraulichkeit, Integrität und Verfügbarkeit der elektronisch geschützten Gesundheitsinformationen, die er im Namen des kollektiven Gesundheitsplans erstellt, empfängt, verwaltet oder übermittelt, sinnvoll und angemessen schützt; (ii) sicherstellt, dass die in 164.504(f)(2)(iii) vorgeschriebene angemessene Trennung durch sinnvolle und	s-3 bucket-public-read-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie nur autorisierten Benutzern, Prozessen und Geräten Zugriff auf Amazon Simple Storage Service (Amazon S3) - Buckets gewähren. Die Verwaltung des Zugriffs sollte mit der Klassifizierung der Daten übereinstimmen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	angemessene Sicherheitsmaßnahmen unterstützt wird; (iii) sicherstellt, dass sich der Beauftragte, einschließlich eines Unterauftragnehmers, dem er diese Informationen zur Verfügung stellt, damit einverstanden erklärt, sinnvolle und angemessene Sicherheitsmaßnahmen zum Schutz der Informationen zu ergreifen; und (iv) dem kollektiven Gesundheitsplan alle Sicherheitsvorfälle meldet, von dem er Kenntnis erlangt.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.314(b)(2)	(2) Implementierungsspezifikationen (erforderlich). Die Dokumente des kollektiven Gesundheitsplans müssen dahingehend geändert werden, dass der Versicherungsträger: (i) administrative, physische und technische Sicherheitsvorkehrungen trifft, die die Vertraulichkeit, Integrität und Verfügbarkeit der elektronisch geschützten Gesundheitsinformationen, die er im Namen des kollektiven Gesundheitsplans erstellt, empfängt, verwaltet oder übermittelt, sinnvoll und angemessen schützt; (ii) sicherstellt, dass die in 164.504(f)(2)(iii) vorgeschriebene angemessene Trennung durch sinnvolle und	s3- bucket-public-write-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie nur autorisierten Benutzern, Prozessen und Geräten Zugriff auf Amazon Simple Storage Service (Amazon S3) - Buckets gewähren. Die Verwaltung des Zugriffs sollte mit der Klassifizierung der Daten übereinstimmen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	angemessene Sicherheitsmaßnahmen unterstützt wird; (iii) sicherstellt, dass sich der Beauftragte, einschließlich eines Unterauftragnehmers, dem er diese Informationen zur Verfügung stellt, damit einverstanden erklärt, sinnvolle und angemessene Sicherheitsmaßnahmen zum Schutz der Informationen zu ergreifen; und (iv) dem kollektiven Gesundheitsplan alle Sicherheitsvorfälle meldet, von dem er Kenntnis erlangt.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.314(b)(2)	(2) Implementierungsspezifikationen (erforderlich). Die Dokumente des kollektiven Gesundheitsplans müssen dahingehend geändert werden, dass der Versicherungsträger: (i) administrative, physische und technische Sicherheitsvorkehrungen trifft, die die Vertraulichkeit, Integrität und Verfügbarkeit der elektronisch geschützten Gesundheitsinformationen, die er im Namen des kollektiven Gesundheitsplans erstellt, empfängt, verwaltet oder übermittelt, sinnvoll und angemessen schützt; (ii) sicherstellt, dass die in 164.504(f)(2)(iii) vorgeschriebene angemessene Trennung durch sinnvolle und	s3-fähig bucket-server-side-encryption	Zum Schutz von Daten im Ruhezustand müssen Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon Simple Storage Service (Amazon S3)-Buckets aktiviert ist. Um eventuell vorhandene sensible Daten im Ruhezustand in Amazon-S3-Buckets zu schützen, muss die Verschlüsselung aktiviert sein.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	angemessene Sicherheitsmaßnahmen unterstützt wird; (iii) sicherstellt, dass sich der Beauftragte, einschließlich eines Unterauftragnehmers, dem er diese Informationen zur Verfügung stellt, damit einverstanden erklärt, sinnvolle und angemessene Sicherheitsmaßnahmen zum Schutz der Informationen zu ergreifen; und (iv) dem kollektiven Gesundheitsplan alle Sicherheitsvorfälle meldet, von dem er Kenntnis erlangt.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.314(b)(2)	(2) Implementierungsspezifikationen (erforderlich). Die Dokumente des kollektiven Gesundheitsplans müssen dahingehend geändert werden, dass der Versicherungsträger: (i) administrative, physische und technische Sicherheitsvorkehrungen trifft, die die Vertraulichkeit, Integrität und Verfügbarkeit der elektronisch geschützten Gesundheitsinformationen, die er im Namen des kollektiven Gesundheitsplans erstellt, empfängt, verwaltet oder übermittelt, sinnvoll und angemessen schützt; (ii) sicherstellt, dass die in 164.504(f)(2)(iii) vorgeschriebene angemessene Trennung durch sinnvolle und	s-3 bucket-ssl-requests-only	Um Daten während der Übertragung zu schützen, stellen Sie sicher, dass Ihre Amazon Simple Storage Service (Amazon S3)-Buckets Anfragen zur Verwendung von Secure Socket Layer (SSL)-Buckets erfordern. Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	angemessene Sicherheitsmaßnahmen unterstützt wird; (iii) sicherstellt, dass sich der Beauftragte, einschließlich eines Unterauftragnehmers, dem er diese Informationen zur Verfügung stellt, damit einverstanden erklärt, sinnvolle und angemessene Sicherheitsmaßnahmen zum Schutz der Informationen zu ergreifen; und (iv) dem kollektiven Gesundheitsplan alle Sicherheitsvorfälle meldet, von dem er Kenntnis erlangt.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.314(b)(2)	(2) Implementierungsspezifikationen (erforderlich). Die Dokumente des kollektiven Gesundheitsplans müssen dahingehend geändert werden, dass der Versicherungsträger: (i) administrative, physische und technische Sicherheitsvorkehrungen trifft, die die Vertraulichkeit, Integrität und Verfügbarkeit der elektronisch geschützten Gesundheitsinformationen, die er im Namen des kollektiven Gesundheitsplans erstellt, empfängt, verwaltet oder übermittelt, sinnvoll und angemessen schützt; (ii) sicherstellt, dass die in 164.504(f)(2)(iii) vorgeschriebene angemessene Trennung durch sinnvolle und	s-3 default-encryption-kms	Stellen Sie sicher, dass die Verschlüsselung für Ihre Amazon Simple Storage Service (Amazon S3)-Buckets aktiviert ist. Um eventuell vorhandene sensible Daten im Ruhezustand in einem Amazon-S3-Bucket zu schützen, muss die Verschlüsselung aktiviert sein.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	angemessene Sicherheitsmaßnahmen unterstützt wird; (iii) sicherstellt, dass sich der Beauftragte, einschließlich eines Unterauftragnehmers, dem er diese Informationen zur Verfügung stellt, damit einverstanden erklärt, sinnvolle und angemessene Sicherheitsmaßnahmen zum Schutz der Informationen zu ergreifen; und (iv) dem kollektiven Gesundheitsplan alle Sicherheitsvorfälle meldet, von dem er Kenntnis erlangt.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.314(b)(2)	(2) Implementierungsspezifikationen (erforderlich). Die Dokumente des kollektiven Gesundheitsplans müssen dahingehend geändert werden, dass der Versicherungsträger: (i) administrative, physische und technische Sicherheitsvorkehrungen trifft, die die Vertraulichkeit, Integrität und Verfügbarkeit der elektronisch geschützten Gesundheitsinformationen, die er im Namen des kollektiven Gesundheitsplans erstellt, empfängt, verwaltet oder übermittelt, sinnvoll und angemessen schützt; (ii) sicherstellt, dass die in 164.504(f)(2)(iii) vorgeschriebene angemessene Trennung durch sinnvolle und	sagemaker-endpoint-configuration-kms-key-konfiguriert	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass die Verschlüsselung mit dem AWS Key Management Service (AWS KMS) für Ihren Endpunkt aktiviert ist. SageMaker Da sensible Daten auf dem SageMaker Endgerät gespeichert werden können, sollten Sie die Verschlüsselung im Ruhezustand aktivieren, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	angemessene Sicherheitsmaßnahmen unterstützt wird; (iii) sicherstellt, dass sich der Beauftragte, einschließlich eines Unterauftragnehmers, dem er diese Informationen zur Verfügung stellt, damit einverstanden erklärt, sinnvolle und angemessene Sicherheitsmaßnahmen zum Schutz der Informationen zu ergreifen; und (iv) dem kollektiven Gesundheitsplan alle Sicherheitsvorfälle meldet, von dem er Kenntnis erlangt.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.314(b)(2)	(2) Implementierungsspezifikationen (erforderlich). Die Dokumente des kollektiven Gesundheitsplans müssen dahingehend geändert werden, dass der Versicherungsträger: (i) administrative, physische und technische Sicherheitsvorkehrungen trifft, die die Vertraulichkeit, Integrität und Verfügbarkeit der elektronisch geschützten Gesundheitsinformationen, die er im Namen des kollektiven Gesundheitsplans erstellt, empfängt, verwaltet oder übermittelt, sinnvoll und angemessen schützt; (ii) sicherstellt, dass die in 164.504(f)(2)(iii) vorgeschriebene angemessene Trennung durch sinnvolle und	sagemaker-notebook-instance-kms-schlüsselkonfiguriert	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass die Verschlüsselung mit dem AWS Key Management Service (AWS KMS) für Ihr Notebook aktiviert ist. SageMaker Da vertrauliche Daten im SageMaker Notebook gespeichert werden können, sollten Sie die Verschlüsselung im Ruhezustand aktivieren, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	angemessene Sicherheitsmaßnahmen unterstützt wird; (iii) sicherstellt, dass sich der Beauftragte, einschließlich eines Unterauftragnehmers, dem er diese Informationen zur Verfügung stellt, damit einverstanden erklärt, sinnvolle und angemessene Sicherheitsmaßnahmen zum Schutz der Informationen zu ergreifen; und (iv) dem kollektiven Gesundheitsplan alle Sicherheitsvorfälle meldet, von dem er Kenntnis erlangt.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.314(b)(2)(i)	(2) Implementierungsspezifikationen (erforderlich). Die Plandokumente des kollektiven Gesundheitsplans müssen um Bestimmungen ergänzt werden, nach denen der Versicherungsträger: (i) administrative, physische und technische Sicherheitsvorkehrungen treffen muss, die die Vertraulichkeit, Integrität und Verfügbarkeit der elektronisch geschützten Gesundheitsinformationen, die er im Namen des kollektiven Gesundheitsplans erstellt, empfängt, verwaltet oder übermittelt, sinnvoll und angemessen schützt;	iam-customer-policy-blocked-kms-Aktionen	AWS Identity and Access Management (IAM) kann Ihnen helfen, die Prinzipien der geringsten Rechte und der Aufgabentrennung in Zugriffsberechtigungen und Autorisierungen zu integrieren und so zu verhindern, dass Richtlinien blockierte Aktionen für alle AWS Schlüssel des Key Management Service enthalten. Wenn Benutzer mehr Rechte haben, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und Aufgabentrennung verstoßen. Mit dieser Regel können Sie den Parameter festlegen. blockedActionsPatterns (Wert „AWS Bewährte grundlegende Sicherheitsmethoden“: kms:

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			Decrypt, kms:ReEncryptFrom). Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.314(b)(2)(i)	(2) Implementierungsspezifikationen (erforderlich). Die Plandokumente des kollektiven Gesundheitsplans müssen um Bestimmungen ergänzt werden, nach denen der Versicherungsträger: (i) administrative, physische und technische Sicherheitsvorkehrungen treffen muss, die die Vertraulichkeit, Integrität und Verfügbarkeit der elektronisch geschützten Gesundheitsinformationen, die er im Namen des kollektiven Gesundheitsplans erstellt, empfängt, verwaltet oder übermittelt, sinnvoll und angemessen schützt;	iam-inline-policy-blocked-kms-Aktionen	Stellen Sie sicher, dass ein Benutzer, eine IAM-Rolle oder eine IAM-Gruppe (AWS Identity and Access Management) nicht über eine Inline-Richtlinie verfügt, die blockierte Aktionen für alle AWS Schlüssel des Key Management Service zulässt. AWS empfiehlt, verwaltete Richtlinien anstelle von Inline-Richtlinien zu verwenden. Verwaltete Richtlinien ermöglichen Wiederverwendbarkeit, Versionsverwaltung, Rollback und Delegierung der Berechtigungsverwaltung. Mit dieser Regel können Sie den blockedActionsPatterns Parameter festlegen. (Wert „AWS Bewährte grundlegende Sicherheitsmethoden“: kms:Decrypt, kms:ReEncryptFrom). Die

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.
164.314(b)(2)(i)	(2) Implementierungsspezifikationen (erforderlich). Die Plandokumente des kollektiven Gesundheitsplans müssen um Bestimmungen ergänzt werden, nach denen der Versicherungsträger: (i) administrative, physische und technische Sicherheitsvorkehrungen treffen muss, die die Vertraulichkeit, Integrität und Verfügbarkeit der elektronisch geschützten Gesundheitsinformationen, die er im Namen des kollektiven Gesundheitsplans erstellt, empfängt, verwaltet oder übermittelt, sinnvoll und angemessen schützt;	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) kann Ihnen dabei helfen, die Prinzipien der geringsten Rechte und der Aufgabentrennung in Zugriffsberechtigungen und Autorisierungen zu integrieren und so zu verhindern, dass Richtlinien „Effect“: „Allow“ mit „Action“: „*“ anstelle von „Resource“: „*“ enthalten. Wenn Benutzern mehr Rechte eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und der Aufgabentrennung verstoßen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.314(b)(2)(i)	(2) Implementierungsspezifikationen (erforderlich). Die Plandokumente des kollektiven Gesundheitsplans müssen um Bestimmungen ergänzt werden, nach denen der Versicherungsträger: (i) administrative, physische und technische Sicherheitsvorkehrungen treffen muss, die die Vertraulichkeit, Integrität und Verfügbarkeit der elektronisch geschützten Gesundheitsinformationen, die er im Namen des kollektiven Gesundheitsplans erstellt, empfängt, verwaltet oder übermittelt, sinnvoll und angemessen schützt;	iam-root-access-key-überprüfen	Der Zugriff auf Systeme und Ressourcen kann gesteuert werden, indem überprüft wird, ob der Root-Benutzer keine Zugriffsschlüssel mit seiner AWS Identity and Access Management (IAM) -Rolle verknüpft hat. Stellen Sie sicher, dass die Root-Zugriffsschlüssel gelöscht werden. Erstellen und verwenden Sie stattdessen rollenbasierte Funktionen, AWS-Konten um das Prinzip der geringsten Funktionalität zu berücksichtigen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.314(b)(2)(i)	(2) Implementierungsspezifikationen (erforderlich). Die Plandokumente des kollektiven Gesundheitsplans müssen um Bestimmungen ergänzt werden, nach denen der Versicherungsträger: (i) administrative, physische und technische Sicherheitsvorkehrungen treffen muss, die die Vertraulichkeit, Integrität und Verfügbarkeit der elektronisch geschützten Gesundheitsinformationen, die er im Namen des kollektiven Gesundheitsplans erstellt, empfängt, verwaltet oder übermittelt, sinnvoll und angemessen schützt;	iam-user-no-policies-überprüfen	Diese Regel stellt sicher, dass AWS Identity and Access Management (IAM)-Richtlinien nur Gruppen oder Rollen zugewiesen werden, um den Zugriff auf Systeme und Ressourcen zu kontrollieren. Die Zuweisung von Berechtigungen auf Gruppen- oder Rollenebene trägt dazu bei, die Wahrscheinlichkeit zu verringern, dass eine Identität übermäßige Berechtigungen erhält oder beibehält.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.314(b)(2)(i)	(2) Implementierungsspezifikationen (erforderlich). Die Plandokumente des kollektiven Gesundheitsplans müssen um Bestimmungen ergänzt werden, nach denen der Versicherungsträger: (i) administrative, physische und technische Sicherheitsvorkehrungen treffen muss, die die Vertraulichkeit, Integrität und Verfügbarkeit der elektronisch geschützten Gesundheitsinformationen, die er im Namen des kollektiven Gesundheitsplans erstellt, empfängt, verwaltet oder übermittelt, sinnvoll und angemessen schützt;	iam-policy-no-statements-with-full-access	Stellen Sie sicher, dass IAM-Aktionen nur auf die benötigten Aktionen beschränkt sind. Wenn Benutzern mehr Rechte eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und der Aufgabentrennung verstoßen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.314(b)(2)(i)	(2) Implementierungsspezifikationen (erforderlich). Die Plandokumente des kollektiven Gesundheitsplans müssen um Bestimmungen ergänzt werden, nach denen der Versicherungsträger: (i) administrative, physische und technische Sicherheitsvorkehrungen treffen muss, die die Vertraulichkeit, Integrität und Verfügbarkeit der elektronisch geschützten Gesundheitsinformationen, die er im Namen des kollektiven Gesundheitsplans erstellt, empfängt, verwaltet oder übermittelt, sinnvoll und angemessen schützt;	ecs-task-definition-user-for-host-mode-check	Wenn für eine Aufgabendefinition erhöhte Berechtigungen gelten, liegt das daran, dass der Kunde diesen Konfigurationen ausdrücklich zugestimmt hat. Diese Kontrolle prüft, ob eine unerwartete Berechtigungseskalation vorliegt, wenn für eine Aufgabendefinition das Host-Netzwerk aktiviert ist, die Kunden aber keine erhöhten Berechtigungen aktiviert haben.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.314(b)(2)(i)	(2) Implementierungsspezifikationen (erforderlich). Die Plandokumente des kollektiven Gesundheitsplans müssen um Bestimmungen ergänzt werden, nach denen der Versicherungsträger: (i) administrative, physische und technische Sicherheitsvorkehrungen treffen muss, die die Vertraulichkeit, Integrität und Verfügbarkeit der elektronisch geschützten Gesundheitsinformationen, die er im Namen des kollektiven Gesundheitsplans erstellt, empfängt, verwaltet oder übermittelt, sinnvoll und angemessen schützt;	ecs-containers-readonly-access	Die Aktivierung des schreibgeschützten Zugriffs auf Amazon Elastic Container Service (ECS)-Container kann dazu beitragen, das Prinzip der geringsten Berechtigung einzuhalten. Diese Option kann Angriffsvektoren reduzieren, da das Dateisystem der Container-Instance nur geändert werden kann, wenn es über ausdrückliche Lese- und Schreibberechtigungen verfügt.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.314(b)(2)(i)	(2) Implementierungsspezifikationen (erforderlich). Die Plandokumente des kollektiven Gesundheitsplans müssen um Bestimmungen ergänzt werden, nach denen der Versicherungsträger: (i) administrative, physische und technische Sicherheitsvorkehrungen treffen muss, die die Vertraulichkeit, Integrität und Verfügbarkeit der elektronisch geschützten Gesundheitsinformationen, die er im Namen des kollektiven Gesundheitsplans erstellt, empfängt, verwaltet oder übermittelt, sinnvoll und angemessen schützt;	s3- bucket-acl-prohibited	Diese Regel prüft, ob Access Control Lists (ACLs) für die Zugriffskontrolle auf Amazon S3 S3-Buckets verwendet werden. ACLs sind veraltete Zugriffskontrollmechanismen für Amazon S3 S3-Buckets, die älter sind als AWS Identity and Access Management (IAM). Stattdessen empfiehlt es sich ACLs, IAM-Richtlinien oder S3-Bucket-Richtlinien zu verwenden, um den Zugriff auf Ihre S3-Buckets einfacher zu verwalten.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.314(b)(2)(i)	(2) Implementierungsspezifikationen (erforderlich). Die Plandokumente des kollektiven Gesundheitsplans müssen um Bestimmungen ergänzt werden, nach denen der Versicherungsträger: (i) administrative, physische und technische Sicherheitsvorkehrungen treffen muss, die die Vertraulichkeit, Integrität und Verfügbarkeit der elektronisch geschützten Gesundheitsinformationen, die er im Namen des kollektiven Gesundheitsplans erstellt, empfängt, verwaltet oder übermittelt, sinnvoll und angemessen schützt;	iam-password-policy	Die Identitäten und Anmeldeinformationen werden auf der Grundlage einer organisatorischen IAM-Passwortrichtlinie ausgestellt, verwaltet und verifiziert. Sie erfüllen oder übertreffen die Anforderungen von NIST SP 800-63 und dem Standard „Best Practices“ von AWS Foundational Security für die Passwortstärke. Mit dieser Regel können Sie optional RequireUppercaseCharacters (Wert für AWS grundlegende Sicherheitsbewährte Methoden: wahr), RequireLowercaseCharacters (Wert für bewährte Methoden für AWS grundlegende Sicherheit: wahr), RequireSymbols (Wert für bewährte Methoden für AWS grundlegende Sicherheit:

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			wahr), RequireNumbers (Wert für bewährte Methoden für AWS grundlegende Sicherheit: wahr), MinimumPasswordLength (Wert für bewährte Methoden für AWS grundlegende Sicherheit: 14), PasswordReusePrevention (Wert für bewährte Methoden für AWS grundlegende Sicherheit: 24) und MaxPasswordAge (Wert für bewährte Methoden für AWS grundlegende Sicherheit: 90) für Ihr IAM festlegen Kennwortrichtlinie. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.314(b)(2)(i)	(2) Implementierungsspezifikationen (erforderlich). Die Plandokumente des kollektiven Gesundheitsplans müssen um Bestimmungen ergänzt werden, nach denen der Versicherungsträger: (i) administrative, physische und technische Sicherheitsvorkehrungen treffen muss, die die Vertraulichkeit, Integrität und Verfügbarkeit der elektronisch geschützten Gesundheitsinformationen, die er im Namen des kollektiven Gesundheitsplans erstellt, empfängt, verwaltet oder übermittelt, sinnvoll und angemessen schützt;	acm-certificate-expiration-check	Stellen Sie sicher, dass die Netzwerkintegrität geschützt ist, indem Sie sicherstellen, dass X509-Zertifikate von AWS ACM ausgestellt werden. Diese Zertifikate müssen gültig und dürfen nicht abgelaufen sein. Für diese Regel ist ein Wert für erforderlich daysToExpiration (Wert für bewährte AWS Grundregeln für Sicherheit: 90). Der tatsächliche Wert muss den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.314(b)(2)(i)	(2) Implementierungsspezifikationen (erforderlich). Die Plandokumente des kollektiven Gesundheitsplans müssen um Bestimmungen ergänzt werden, nach denen der Versicherungsträger: (i) administrative, physische und technische Sicherheitsvorkehrungen treffen muss, die die Vertraulichkeit, Integrität und Verfügbarkeit der elektronisch geschützten Gesundheitsinformationen, die er im Namen des kollektiven Gesundheitsplans erstellt, empfängt, verwaltet oder übermittelt, sinnvoll und angemessen schützt;	alb-http-to-https-Umleitungsprüfung	Um Daten während der Übertragung zu schützen, stellen Sie sicher, dass Ihr Application Load Balancer unverschlüsselte HTTP-Anfragen automatisch an HTTPS umleitet. Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.314(b)(2)(i)	(2) Implementierungsspezifikationen (erforderlich). Die Plandokumente des kollektiven Gesundheitsplans müssen um Bestimmungen ergänzt werden, nach denen der Versicherungsträger: (i) administrative, physische und technische Sicherheitsvorkehrungen treffen muss, die die Vertraulichkeit, Integrität und Verfügbarkeit der elektronisch geschützten Gesundheitsinformationen, die er im Namen des kollektiven Gesundheitsplans erstellt, empfängt, verwaltet oder übermittelt, sinnvoll und angemessen schützt;	api-gw-ssl-enabled	Stellen Sie sicher, dass die REST-API-Stufen von Amazon API Gateway mit SSL-Zertifikaten konfiguriert sind, damit Backend-Systeme überprüfen können, ob Anforderungen von API Gateway stammen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.314(b)(2)(i)	(2) Implementierungsspezifikationen (erforderlich). Die Plandokumente des kollektiven Gesundheitsplans müssen um Bestimmungen ergänzt werden, nach denen der Versicherungsträger: (i) administrative, physische und technische Sicherheitsvorkehrungen treffen muss, die die Vertraulichkeit, Integrität und Verfügbarkeit der elektronisch geschützten Gesundheitsinformationen, die er im Namen des kollektiven Gesundheitsplans erstellt, empfängt, verwaltet oder übermittelt, sinnvoll und angemessen schützt;	elb-acm-certificate-required	Zum Schutz von eventuell vorhandenen sensiblen Daten sowie von Daten während der Übertragung muss die Verschlüsselung für Ihr Elastic Load Balancing aktiviert sein. Verwenden Sie AWS Certificate Manager, um öffentliche und private SSL/TLS-Zertifikate mit AWS Diensten und internen Ressourcen zu verwalten, bereitzustellen und bereitzustellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.314(b)(2)(i)	(2) Implementierungsspezifikationen (erforderlich). Die Plandokumente des kollektiven Gesundheitsplans müssen um Bestimmungen ergänzt werden, nach denen der Versicherungsträger: (i) administrative, physische und technische Sicherheitsvorkehrungen treffen muss, die die Vertraulichkeit, Integrität und Verfügbarkeit der elektronisch geschützten Gesundheitsinformationen, die er im Namen des kollektiven Gesundheitsplans erstellt, empfängt, verwaltet oder übermittelt, sinnvoll und angemessen schützt;	elb-predefined-security-policy-ssl-check	Stellen Sie sicher, dass Ihre SSL-Listener von Classic Elastic Load Balancing eine vordefinierte Sicherheitsrichtlinie verwenden, um Daten während der Übertragung zu schützen. Elastic Load Balancing bietet vordefinierte Aushandlungskonfigurationen, die für die SSL-Aushandlung verwendet werden, wenn eine Verbindung zwischen einem Client und Ihrem Load Balancer hergestellt wurde. Die SSL-Aushandlungskonfigurationen sind mit einer breiten Palette von Clients kompatibel und verwenden hochfeste kryptografische Algorithmen. Diese Regel verlangt, dass Sie eine vordefinierte Sicherheitsrichtlinie für Ihre SSL-Liste

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			ner festlegen. Die Standard-Sicherheitsrichtlinie lautet: Policy-TLS-1-2-2017-0. ELBSecurity Der tatsächliche Wert muss den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.314(b)(2)(i)	(2) Implementierungsspezifikationen (erforderlich). Die Plandokumente des kollektiven Gesundheitsplans müssen um Bestimmungen ergänzt werden, nach denen der Versicherungsträger: (i) administrative, physische und technische Sicherheitsvorkehrungen treffen muss, die die Vertraulichkeit, Integrität und Verfügbarkeit der elektronisch geschützten Gesundheitsinformationen, die er im Namen des kollektiven Gesundheitsplans erstellt, empfängt, verwaltet oder übermittelt, sinnvoll und angemessen schützt;	elb-tls-https-listeners-nur	Stellen Sie sicher, dass Ihre Elastic Load Balancer (ELBs) mit SSL- oder HTTPS-Listenern konfiguriert sind. Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.314(b)(2)(i)	(2) Implementierungsspezifikationen (erforderlich). Die Plandokumente des kollektiven Gesundheitsplans müssen um Bestimmungen ergänzt werden, nach denen der Versicherungsträger: (i) administrative, physische und technische Sicherheitsvorkehrungen treffen muss, die die Vertraulichkeit, Integrität und Verfügbarkeit der elektronisch geschützten Gesundheitsinformationen, die er im Namen des kollektiven Gesundheitsplans erstellt, empfängt, verwaltet oder übermittelt, sinnvoll und angemessen schützt;	s-3 bucket-ssl-requests-only	Um Daten während der Übertragung zu schützen, stellen Sie sicher, dass Ihre Amazon Simple Storage Service (Amazon S3)-Buckets Anfragen zur Verwendung von Secure Socket Layer (SSL)-Buckets erfordern. Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.314(b)(2)(i)	(2) Implementierungsspezifikationen (erforderlich). Die Plandokumente des kollektiven Gesundheitsplans müssen um Bestimmungen ergänzt werden, nach denen der Versicherungsträger: (i) administrative, physische und technische Sicherheitsvorkehrungen treffen muss, die die Vertraulichkeit, Integrität und Verfügbarkeit der elektronisch geschützten Gesundheitsinformationen, die er im Namen des kollektiven Gesundheitsplans erstellt, empfängt, verwaltet oder übermittelt, sinnvoll und angemessen schützt;	Elb v 2- acm-certificate-required	Zum Schutz von eventuell vorhandenen sensiblen Daten sowie von Daten während der Übertragung muss die Verschlüsselung für Ihr Elastic Load Balancing aktiviert sein. Verwenden Sie AWS Certificate Manager, um öffentliche und private SSL/TLS-Zertifikate mit AWS Diensten und internen Ressourcen zu verwalten, bereitzustellen und bereitzustellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.314(b)(2)(i)	(2) Implementierungsspezifikationen (erforderlich). Die Plandokumente des kollektiven Gesundheitsplans müssen um Bestimmungen ergänzt werden, nach denen der Versicherungsträger: (i) administrative, physische und technische Sicherheitsvorkehrungen treffen muss, die die Vertraulichkeit, Integrität und Verfügbarkeit der elektronisch geschützten Gesundheitsinformationen, die er im Namen des kollektiven Gesundheitsplans erstellt, empfängt, verwaltet oder übermittelt, sinnvoll und angemessen schützt;	cloud-trail-encryption-enabled	Da sensible Daten vorhanden sein können und um Daten im Speicher zu schützen, sollten Sie sicherstellen, dass die Verschlüsselung für Ihre AWS CloudTrail Trails aktiviert ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.314(b)(2)(i)	(2) Implementierungsspezifikationen (erforderlich). Die Plandokumente des kollektiven Gesundheitsplans müssen um Bestimmungen ergänzt werden, nach denen der Versicherungsträger: (i) administrative, physische und technische Sicherheitsvorkehrungen treffen muss, die die Vertraulichkeit, Integrität und Verfügbarkeit der elektronisch geschützten Gesundheitsinformationen, die er im Namen des kollektiven Gesundheitsplans erstellt, empfängt, verwaltet oder übermittelt, sinnvoll und angemessen schützt;	ec-2 ebs-encryption-by-default	Zum Schutz von Daten im Ruhezustand müssen Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon Elastic Block Store (Amazon EBS)-Volumes aktiviert ist. Da sensible Daten auch im Ruhezustand vorhanden sein können, sollten Sie die Verschlüsselung im Ruhezustand aktivieren, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.314(b)(2)(i)	(2) Implementierungsspezifikationen (erforderlich). Die Plandokumente des kollektiven Gesundheitsplans müssen um Bestimmungen ergänzt werden, nach denen der Versicherungsträger: (i) administrative, physische und technische Sicherheitsvorkehrungen treffen muss, die die Vertraulichkeit, Integrität und Verfügbarkeit der elektronisch geschützten Gesundheitsinformationen, die er im Namen des kollektiven Gesundheitsplans erstellt, empfängt, verwaltet oder übermittelt, sinnvoll und angemessen schützt;	efs-encrypted-check	Aktivieren Sie die Verschlüsselung für Ihr Amazon Elastic File System (EFS), um eventuell vorhandene sensible Daten sowie Daten im Ruhezustand zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.314(b)(2)(i)	(2) Implementierungsspezifikationen (erforderlich). Die Plandokumente des kollektiven Gesundheitsplans müssen um Bestimmungen ergänzt werden, nach denen der Versicherungsträger: (i) administrative, physische und technische Sicherheitsvorkehrungen treffen muss, die die Vertraulichkeit, Integrität und Verfügbarkeit der elektronisch geschützten Gesundheitsinformationen, die er im Namen des kollektiven Gesundheitsplans erstellt, empfängt, verwaltet oder übermittelt, sinnvoll und angemessen schützt;	elasticsearch-encrypted-at-rest	Da sensible Daten vorhanden sein können und um Daten im Ruhezustand zu schützen, sollten Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon OpenSearch Service (OpenSearch Service) -Domains aktiviert ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.314(b)(2)(i)	(2) Implementierungsspezifikationen (erforderlich). Die Plandokumente des kollektiven Gesundheitsplans müssen um Bestimmungen ergänzt werden, nach denen der Versicherungsträger: (i) administrative, physische und technische Sicherheitsvorkehrungen treffen muss, die die Vertraulichkeit, Integrität und Verfügbarkeit der elektronisch geschützten Gesundheitsinformationen, die er im Namen des kollektiven Gesundheitsplans erstellt, empfängt, verwaltet oder übermittelt, sinnvoll und angemessen schützt;	elasticsearch-node-to-node-Verschlüsselungsprüfung	Stellen Sie sicher, dass die node-to-node Verschlüsselung für Amazon OpenSearch Service aktiviert ist. Node-to-nodeVerschlüsselung ermöglicht die TLS 1.2-Verschlüsselung für die gesamte Kommunikation innerhalb der Amazon Virtual Private Cloud (Amazon VPC). Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.314(b)(2)(i)	(2) Implementierungsspezifikationen (erforderlich). Die Plandokumente des kollektiven Gesundheitsplans müssen um Bestimmungen ergänzt werden, nach denen der Versicherungsträger: (i) administrative, physische und technische Sicherheitsvorkehrungen treffen muss, die die Vertraulichkeit, Integrität und Verfügbarkeit der elektronisch geschützten Gesundheitsinformationen, die er im Namen des kollektiven Gesundheitsplans erstellt, empfängt, verwaltet oder übermittelt, sinnvoll und angemessen schützt;	encrypted-volumes	Aktivieren Sie die Verschlüsselung für Ihre Amazon-Elastic-Block-Store (Amazon-EBS)-Volumes, um eventuell vorhandene sensible Daten sowie Daten im Ruhezustand zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.314(b)(2)(i)	(2) Implementierungsspezifikationen (erforderlich). Die Plandokumente des kollektiven Gesundheitsplans müssen um Bestimmungen ergänzt werden, nach denen der Versicherungsträger: (i) administrative, physische und technische Sicherheitsvorkehrungen treffen muss, die die Vertraulichkeit, Integrität und Verfügbarkeit der elektronisch geschützten Gesundheitsinformationen, die er im Namen des kollektiven Gesundheitsplans erstellt, empfängt, verwaltet oder übermittelt, sinnvoll und angemessen schützt;	rds-snapshot-encrypted	Stellen Sie sicher, dass die Verschlüsselung für Ihre Amazon Relational Database Service (Amazon RDS)-Snapshots aktiviert ist. Da sensible Daten auch im Ruhezustand vorhanden sein können, sollten Sie die Verschlüsselung im Ruhezustand aktivieren, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.314(b)(2)(i)	(2) Implementierungsspezifikationen (erforderlich). Die Plandokumente des kollektiven Gesundheitsplans müssen um Bestimmungen ergänzt werden, nach denen der Versicherungsträger: (i) administrative, physische und technische Sicherheitsvorkehrungen treffen muss, die die Vertraulichkeit, Integrität und Verfügbarkeit der elektronisch geschützten Gesundheitsinformationen, die er im Namen des kollektiven Gesundheitsplans erstellt, empfängt, verwaltet oder übermittelt, sinnvoll und angemessen schützt;	rds-storage-encrypted	Zum Schutz von Daten im Ruhezustand müssen Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon Relational Database Service (Amazon RDS)-Instances aktiviert ist. Um eventuell vorhandene sensible Daten im Ruhezustand in Amazon-RDS-Instances zu schützen, muss die Verschlüsselung von Daten im Ruhezustand aktiviert sein.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.314(b)(2)(i)	(2) Implementierungsspezifikationen (erforderlich). Die Plandokumente des kollektiven Gesundheitsplans müssen um Bestimmungen ergänzt werden, nach denen der Versicherungsträger: (i) administrative, physische und technische Sicherheitsvorkehrungen treffen muss, die die Vertraulichkeit, Integrität und Verfügbarkeit der elektronisch geschützten Gesundheitsinformationen, die er im Namen des kollektiven Gesundheitsplans erstellt, empfängt, verwaltet oder übermittelt, sinnvoll und angemessen schützt;	redshift-cluster-configuration-check	Um Daten im Ruhezustand zu schützen, muss die Verschlüsselung für Ihre Amazon-Redshift-Cluster aktiviert sein. Sie müssen auch sicherstellen, dass die erforderlichen Konfigurationen auf Amazon-Redshift-Clustern bereitgestellt werden. Die Prüfungsprotokollierung muss aktiviert sein, um Informationen zu Verbindungen und Benutzeraktivitäten in der Datenbank bereitzustellen. Diese Regel erfordert, dass ein Wert für clusterDbEncrypted (Config Default: TRUE) und LoggingEnabled (Config Default: TRUE) gesetzt ist. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.314(b)(2)(i)	(2) Implementierungsspezifikationen (erforderlich). Die Plandokumente des kollektiven Gesundheitsplans müssen um Bestimmungen ergänzt werden, nach denen der Versicherungsträger: (i) administrative, physische und technische Sicherheitsvorkehrungen treffen muss, die die Vertraulichkeit, Integrität und Verfügbarkeit der elektronisch geschützten Gesundheitsinformationen, die er im Namen des kollektiven Gesundheitsplans erstellt, empfängt, verwaltet oder übermittelt, sinnvoll und angemessen schützt;	redshift-require-tls-ssl	Stellen Sie sicher, dass Ihre Amazon-Redshift-Cluster eine TLS/SSL-Verschlüsselung erfordern, um eine Verbindung zu SQL-Clients herzustellen. Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.314(b)(2)(i)	(2) Implementierungsspezifikationen (erforderlich). Die Plandokumente des kollektiven Gesundheitsplans müssen um Bestimmungen ergänzt werden, nach denen der Versicherungsträger: (i) administrative, physische und technische Sicherheitsvorkehrungen treffen muss, die die Vertraulichkeit, Integrität und Verfügbarkeit der elektronisch geschützten Gesundheitsinformationen, die er im Namen des kollektiven Gesundheitsplans erstellt, empfängt, verwaltet oder übermittelt, sinnvoll und angemessen schützt;	s3-aktiviert bucket-server-side-encryption	Zum Schutz von Daten im Ruhezustand müssen Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon Simple Storage Service (Amazon S3)-Buckets aktiviert ist. Um eventuell vorhandene sensible Daten im Ruhezustand in Amazon-S3-Buckets zu schützen, muss die Verschlüsselung aktiviert sein.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.314(b)(2)(i)	(2) Implementierungsspezifikationen (erforderlich). Die Plandokumente des kollektiven Gesundheitsplans müssen um Bestimmungen ergänzt werden, nach denen der Versicherungsträger: (i) administrative, physische und technische Sicherheitsvorkehrungen treffen muss, die die Vertraulichkeit, Integrität und Verfügbarkeit der elektronisch geschützten Gesundheitsinformationen, die er im Namen des kollektiven Gesundheitsplans erstellt, empfängt, verwaltet oder übermittelt, sinnvoll und angemessen schützt;	s-3 default-encryption-kms	Stellen Sie sicher, dass die Verschlüsselung für Ihre Amazon Simple Storage Service (Amazon S3)-Buckets aktiviert ist. Um eventuell vorhandene sensible Daten im Ruhezustand in einem Amazon-S3-Bucket zu schützen, muss die Verschlüsselung aktiviert sein.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.314(b)(2)(i)	(2) Implementierungsspezifikationen (erforderlich). Die Plandokumente des kollektiven Gesundheitsplans müssen um Bestimmungen ergänzt werden, nach denen der Versicherungsträger: (i) administrative, physische und technische Sicherheitsvorkehrungen treffen muss, die die Vertraulichkeit, Integrität und Verfügbarkeit der elektronisch geschützten Gesundheitsinformationen, die er im Namen des kollektiven Gesundheitsplans erstellt, empfängt, verwaltet oder übermittelt, sinnvoll und angemessen schützt;	sagemaker-endpoint-configuration-kms-key-konfiguriert	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass die Verschlüsselung mit dem AWS Key Management Service (AWS KMS) für Ihren Endpunkt aktiviert ist. SageMaker Da sensible Daten auf dem SageMaker Endgerät gespeichert werden können, sollten Sie die Verschlüsselung im Ruhezustand aktivieren, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.314(b)(2)(i)	(2) Implementierungsspezifikationen (erforderlich). Die Plandokumente des kollektiven Gesundheitsplans müssen um Bestimmungen ergänzt werden, nach denen der Versicherungsträger: (i) administrative, physische und technische Sicherheitsvorkehrungen treffen muss, die die Vertraulichkeit, Integrität und Verfügbarkeit der elektronisch geschützten Gesundheitsinformationen, die er im Namen des kollektiven Gesundheitsplans erstellt, empfängt, verwaltet oder übermittelt, sinnvoll und angemessen schützt;	sagemaker-notebook-instance-kms-schlüsselkonfiguriert	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass die Verschlüsselung mit dem AWS Key Management Service (AWS KMS) für Ihr Notebook aktiviert ist. SageMaker Da vertrauliche Daten im SageMaker Notebook gespeichert werden können, sollten Sie die Verschlüsselung im Ruhezustand aktivieren, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.314(b)(2)(i)	(2) Implementierungsspezifikationen (erforderlich). Die Plandokumente des kollektiven Gesundheitsplans müssen um Bestimmungen ergänzt werden, nach denen der Versicherungsträger: (i) administrative, physische und technische Sicherheitsvorkehrungen treffen muss, die die Vertraulichkeit, Integrität und Verfügbarkeit der elektronisch geschützten Gesundheitsinformationen, die er im Namen des kollektiven Gesundheitsplans erstellt, empfängt, verwaltet oder übermittelt, sinnvoll und angemessen schützt;	sns-encrypted-kms	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass Ihre Amazon Simple Notification Service (Amazon SNS) -Themen mit dem AWS Key Management Service (AWS KMS) verschlüsselt werden müssen. Um eventuell vorhandene sensible Daten im Ruhezustand in veröffentlichten Nachrichten zu schützen, muss die Verschlüsselung von Daten im Ruhezustand aktiviert sein.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.314(b)(2)(i)	(2) Implementierungsspezifikationen (erforderlich). Die Plandokumente des kollektiven Gesundheitsplans müssen um Bestimmungen ergänzt werden, nach denen der Versicherungsträger: (i) administrative, physische und technische Sicherheitsvorkehrungen treffen muss, die die Vertraulichkeit, Integrität und Verfügbarkeit der elektronisch geschützten Gesundheitsinformationen, die er im Namen des kollektiven Gesundheitsplans erstellt, empfängt, verwaltet oder übermittelt, sinnvoll und angemessen schützt;	dynamodb-autoscaling-enabled	Amazon DynamoDB Auto Scaling verwendet den AWS Application Auto Scaling-Service, um die bereitgestellte Durchsatzkapazität so anzupassen, dass sie automatisch auf tatsächliche Verkehrsmuster reagiert. Auf diese Weise kann eine Tabelle oder ein globaler sekundärer Index die bereitgestellte Lese-/Schreibkapazität erhöhen, um plötzliche Erhöhungen des Datenverkehrs ohne Drosselung zu bewältigen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.314(b)(2)(i)	(2) Implementierungsspezifikationen (erforderlich). Die Plandokumente des kollektiven Gesundheitsplans müssen um Bestimmungen ergänzt werden, nach denen der Versicherungsträger: (i) administrative, physische und technische Sicherheitsvorkehrungen treffen muss, die die Vertraulichkeit, Integrität und Verfügbarkeit der elektronisch geschützten Gesundheitsinformationen, die er im Namen des kollektiven Gesundheitsplans erstellt, empfängt, verwaltet oder übermittelt, sinnvoll und angemessen schützt;	dynamodb-pitr-enabled	Aktivieren Sie diese Regel, um zu überprüfen, ob die Informationen gesichert wurden. Es verwaltet auch die Backups, indem es sicherstellt, dass die point-in-time Wiederherstellung in Amazon DynamoDB aktiviert ist. Bei der Wiederherstellung werden fortlaufende Backups Ihrer Tabelle für die letzten 35 Tage gespeichert.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.314(b)(2)(i)	(2) Implementierungsspezifikationen (erforderlich). Die Plandokumente des kollektiven Gesundheitsplans müssen um Bestimmungen ergänzt werden, nach denen der Versicherungsträger: (i) administrative, physische und technische Sicherheitsvorkehrungen treffen muss, die die Vertraulichkeit, Integrität und Verfügbarkeit der elektronisch geschützten Gesundheitsinformationen, die er im Namen des kollektiven Gesundheitsplans erstellt, empfängt, verwaltet oder übermittelt, sinnvoll und angemessen schützt;	elb-cross-zone-load-Balancing aktiviert	Aktivieren Sie zonenübergreifendes Load Balancing für Ihre Elastic Load Balancer (ELBs), um eine angemessene Kapazität und Verfügbarkeit aufrechtzuerhalten. Zonenübergreifendes Load Balancing reduziert die Notwendigkeit, die gleiche Anzahl von Instances in jeder aktivierten Availability Zone aufrechtzuerhalten. Es verbessert auch die Fähigkeit Ihrer Anwendung, den Verlust einer oder mehrerer Instances zu bewältigen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.314(b)(2)(i)	(2) Implementierungsspezifikationen (erforderlich). Die Plandokumente des kollektiven Gesundheitsplans müssen um Bestimmungen ergänzt werden, nach denen der Versicherungsträger: (i) administrative, physische und technische Sicherheitsvorkehrungen treffen muss, die die Vertraulichkeit, Integrität und Verfügbarkeit der elektronisch geschützten Gesundheitsinformationen, die er im Namen des kollektiven Gesundheitsplans erstellt, empfängt, verwaltet oder übermittelt, sinnvoll und angemessen schützt;	elb-deletion-protection-enabled	Diese Regel sorgt dafür, dass der Löschschutz für Elastic Load Balancing aktiviert ist. Verwenden Sie diese Funktion, um zu verhindern, dass Ihr Load Balancer versehentlich oder böswillig gelöscht wird, was zum Verlust der Verfügbarkeit Ihrer Anwendungen führen kann.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.314(b)(2)(i)	(2) Implementierungsspezifikationen (erforderlich). Die Plandokumente des kollektiven Gesundheitsplans müssen um Bestimmungen ergänzt werden, nach denen der Versicherungsträger: (i) administrative, physische und technische Sicherheitsvorkehrungen treffen muss, die die Vertraulichkeit, Integrität und Verfügbarkeit der elektronisch geschützten Gesundheitsinformationen, die er im Namen des kollektiven Gesundheitsplans erstellt, empfängt, verwaltet oder übermittelt, sinnvoll und angemessen schützt;	rds-cluster-deletion-protection-aktiviert	Stellen Sie sicher, dass Amazon Relational Database Service (Amazon RDS)-Instances den Löschschutz aktiviert haben. Verwenden Sie den Löschschutz, um zu verhindern, dass Ihre Amazon-RDS-Instances versehentlich oder böswillig gelöscht werden, was zum Verlust der Verfügbarkeit Ihrer Anwendungen führen kann.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.314(b)(2)(i)	(2) Implementierungsspezifikationen (erforderlich). Die Plandokumente des kollektiven Gesundheitsplans müssen um Bestimmungen ergänzt werden, nach denen der Versicherungsträger: (i) administrative, physische und technische Sicherheitsvorkehrungen treffen muss, die die Vertraulichkeit, Integrität und Verfügbarkeit der elektronisch geschützten Gesundheitsinformationen, die er im Namen des kollektiven Gesundheitsplans erstellt, empfängt, verwaltet oder übermittelt, sinnvoll und angemessen schützt;	rds-multi-az-support	Die Multi-AZ-Unterstützung in Amazon Relational Database Service (Amazon RDS) bietet eine verbesserte Verfügbarkeit und Beständigkeit von Datenbank-Instances. Wenn Sie eine Multi-AZ-Datenbank-Instance bereitstellen, erstellt Amazon RDS automatisch eine primäre Datenbank-Instance und repliziert die Daten synchron auf eine Standby-Instance in einer anderen Availability Zone. Jede Availability Zone läuft auf einer eigenen, physisch getrennten, unabhängigen Infrastruktur und ist auf eine hohe Verfügbarkeit ausgelegt. Im Falle eines Infrastrukturausfalls führt Amazon RDS einen automatis

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			chen Failover zum Standby-Modus durch, sodass Sie den Datenbankbetrieb wieder aufnehmen können, sobald der Failover abgeschlo ssen ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.314(b)(2)(i)	(2) Implementierungsspezifikationen (erforderlich). Die Plandokumente des kollektiven Gesundheitsplans müssen um Bestimmungen ergänzt werden, nach denen der Versicherungsträger: (i) administrative, physische und technische Sicherheitsvorkehrungen treffen muss, die die Vertraulichkeit, Integrität und Verfügbarkeit der elektronisch geschützten Gesundheitsinformationen, die er im Namen des kollektiven Gesundheitsplans erstellt, empfängt, verwaltet oder übermittelt, sinnvoll und angemessen schützt;	s3- bucket-default-lock-enabled	Stellen Sie sicher, dass für Ihren Amazon Simple Storage Service (Amazon S3)-Bucket standardmäßig eine Sperre aktiviert ist. Zum Schutz eventuell vorhanden er sensibler Daten in S3-Buckets müssen Sie Objektsperren für Daten im Ruhezustand erzwingen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.314(b)(2)(i)	(2) Implementierungsspezifikationen (erforderlich). Die Plandokumente des kollektiven Gesundheitsplans müssen um Bestimmungen ergänzt werden, nach denen der Versicherungsträger: (i) administrative, physische und technische Sicherheitsvorkehrungen treffen muss, die die Vertraulichkeit, Integrität und Verfügbarkeit der elektronisch geschützten Gesundheitsinformationen, die er im Namen des kollektiven Gesundheitsplans erstellt, empfängt, verwaltet oder übermittelt, sinnvoll und angemessen schützt;	vpc-vpn-2-tunnels-up	Redundante Site-to-Site VPN-Tunnel können implementiert werden, um die Anforderungen an die Ausfallsicherheit zu erfüllen. Es verwendet zwei Tunnel, um die Konnektivität sicherzustellen, falls eine der Site-to-Site VPN-Verbindungen nicht verfügbar ist. Um sich vor einem Verbindungsverlust zu schützen, können Sie für den Fall, dass Ihr Kunden-Gateway nicht verfügbar ist, eine zweite Site-to-Site VPN-Verbindung zu Ihrer Amazon Virtual Private Cloud (Amazon VPC) und Ihrem Virtual Private Gateway einrichten, indem Sie ein zweites Kunden-Gateway verwenden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.314(b)(2)(i)	(2) Implementierungsspezifikationen (erforderlich). Die Plandokumente des kollektiven Gesundheitsplans müssen um Bestimmungen ergänzt werden, nach denen der Versicherungsträger: (i) administrative, physische und technische Sicherheitsvorkehrungen treffen muss, die die Vertraulichkeit, Integrität und Verfügbarkeit der elektronisch geschützten Gesundheitsinformationen, die er im Namen des kollektiven Gesundheitsplans erstellt, empfängt, verwaltet oder übermittelt, sinnvoll und angemessen schützt;	no-unrestricted-route-to-igw	Stellen Sie sicher, dass EC2 Amazon-Routentabellen keine uneingeschränkten Routen zu einem Internet-Gateway enthalten. Durch das Entfernen oder Beschränken des Internetzugangs für Workloads innerhalb von Amazon VPCs können unbeabsichtigte Zugriffe in Ihrer Umgebung reduziert werden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.314(b)(2)(i)	(2) Implementierungsspezifikationen (erforderlich). Die Plandokumente des kollektiven Gesundheitsplans müssen um Bestimmungen ergänzt werden, nach denen der Versicherungsträger: (i) administrative, physische und technische Sicherheitsvorkehrungen treffen muss, die die Vertraulichkeit, Integrität und Verfügbarkeit der elektronisch geschützten Gesundheitsinformationen, die er im Namen des kollektiven Gesundheitsplans erstellt, empfängt, verwaltet oder übermittelt, sinnvoll und angemessen schützt;	opensearch-encrypted-at-rest	Da sensible Daten vorhanden sein können und um Daten im Ruhezustand zu schützen, sollten Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon OpenSearch Service-Domains aktiviert ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.314(b)(2)(i)	(2) Implementierungsspezifikationen (erforderlich). Die Plandokumente des kollektiven Gesundheitsplans müssen um Bestimmungen ergänzt werden, nach denen der Versicherungsträger: (i) administrative, physische und technische Sicherheitsvorkehrungen treffen muss, die die Vertraulichkeit, Integrität und Verfügbarkeit der elektronisch geschützten Gesundheitsinformationen, die er im Namen des kollektiven Gesundheitsplans erstellt, empfängt, verwaltet oder übermittelt, sinnvoll und angemessen schützt;	opensearch-https-required	Da sensible Daten existieren können und um Daten während der Übertragung zu schützen, sollten Sie sicherstellen, dass HTTPS für Verbindungen zu Ihren Amazon OpenSearch Service-Domains aktiviert ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.314(b)(2)(i)	(2) Implementierungsspezifikationen (erforderlich). Die Plandokumente des kollektiven Gesundheitsplans müssen um Bestimmungen ergänzt werden, nach denen der Versicherungsträger: (i) administrative, physische und technische Sicherheitsvorkehrungen treffen muss, die die Vertraulichkeit, Integrität und Verfügbarkeit der elektronisch geschützten Gesundheitsinformationen, die er im Namen des kollektiven Gesundheitsplans erstellt, empfängt, verwaltet oder übermittelt, sinnvoll und angemessen schützt;	opensearch-in-vpc-only	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass sich Amazon OpenSearch Service-Domains innerhalb einer Amazon Virtual Private Cloud (Amazon VPC) befinden. Eine Amazon OpenSearch Service-Domain innerhalb einer Amazon VPC ermöglicht die sichere Kommunikation zwischen Amazon OpenSearch Service und anderen Services innerhalb der Amazon VPC, ohne dass ein Internet-Gateway, ein NAT-Gerät oder eine VPN-Verbindung erforderlich ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.314(b)(2)(i)	(2) Implementierungsspezifikationen (erforderlich). Die Plandokumente des kollektiven Gesundheitsplans müssen um Bestimmungen ergänzt werden, nach denen der Versicherungsträger: (i) administrative, physische und technische Sicherheitsvorkehrungen treffen muss, die die Vertraulichkeit, Integrität und Verfügbarkeit der elektronisch geschützten Gesundheitsinformationen, die er im Namen des kollektiven Gesundheitsplans erstellt, empfängt, verwaltet oder übermittelt, sinnvoll und angemessen schützt;	opensearch-node-to-node-Verschlüsselungsprüfung	Stellen Sie sicher, dass die node-to-node Verschlüsselung für Amazon OpenSearch Service aktiviert ist. Node-to-nodeVerschlüsselung ermöglicht die TLS 1.2-Verschlüsselung für die gesamte Kommunikation innerhalb der Amazon Virtual Private Cloud (Amazon VPC). Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
164.314(b)(2)(i)	(2) Implementierungsspezifikationen (erforderlich). Die Plandokumente des kollektiven Gesundheitsplans müssen um Bestimmungen ergänzt werden, nach denen der Versicherungsträger: (i) administrative, physische und technische Sicherheitsvorkehrungen treffen muss, die die Vertraulichkeit, Integrität und Verfügbarkeit der elektronisch geschützten Gesundheitsinformationen, die er im Namen des kollektiven Gesundheitsplans erstellt, empfängt, verwaltet oder übermittelt, sinnvoll und angemessen schützt;	kinesis-stream-encrypted	Aktivieren Sie die Verschlüsselung für Ihre Amazon-Kinesis-Streams, um eventuell vorhandene sensible Daten sowie Daten im Ruhezustand zu schützen.

Vorlage

Die Vorlage ist verfügbar unter GitHub: Operational Best Practices for HIPAA Security.

Bewährte Methoden für die Ausführung von IRS 1075

Konformitätspakete bieten ein allgemeines Compliance-Framework, das es Ihnen ermöglicht, mithilfe verwalteter oder benutzerdefinierter AWS Config Regeln und Abhilfemaßnahmen Kontrollen zur Sicherheits-, Betriebs- oder Kostenoptimierung durchzuführen. AWS Config Conformance Packs dienen als Beispielvorlagen nicht dazu, die vollständige Einhaltung eines bestimmten Governance- oder Compliance-Standards sicherzustellen. Sie sind dafür verantwortlich, selbst zu beurteilen, ob Ihre Nutzung der Services den geltenden gesetzlichen und behördlichen Anforderungen entspricht.

Im Folgenden finden Sie ein Beispiel für eine Zuordnung zwischen den IRS 1075- und AWS verwalteten Konfigurationsregeln. Jede Config-Regel gilt für eine bestimmte AWS Ressource und bezieht sich auf eine oder mehrere IRS 1075-Steuerelemente. Eine IRS-1075-Kontrolle kann mehreren Config-Regeln zugeordnet werden. In der folgenden Tabelle finden Sie weitere Informationen und Anleitungen zu diesen Zuordnungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3,3.1 Cloud-Computing d. Datenverschlüsselung während der Übertragung	FTI muss während der Übertragung innerhalb der Cloud-Umgebung verschlüsselt werden. Alle zur Verschlüsselung von FTI verwendeten Mechanismen müssen FIPS-140-zertifiziert sein und mit den aktuellen FIPS-140-kompatiblen Modulen betrieben werden. Diese Anforderung muss in der SLA enthalten sein.	alb-http-to-https-Umleitungsprüfung	Um Daten während der Übertragung zu schützen, stellen Sie sicher, dass Ihr Application Load Balancer unverschlüsselte HTTP-Anfragen automatisch an HTTPS umleitet. Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3,3.1 Cloud-Computing d. Datenverschlüsselung während der Übertragung	FTI muss während der Übertragung innerhalb der Cloud-Umgebung verschlüsselt werden. Alle zur Verschlüsselung von FTI verwendeten Mechanismen müssen FIPS-140-zertifiziert sein und mit den aktuellen FIPS-140-kompatiblen Modulen betrieben werden. Diese Anforderung muss in der SLA enthalten sein.	elasticsearch-node-to-node-Verschlüsselungsprüfung	Stellen Sie sicher, dass die node-to-node Verschlüsselung für Amazon OpenSearch Service aktiviert ist. Node-to-nodeVerschlüsselung ermöglicht die TLS 1.2-Verschlüsselung für die gesamte Kommunikation innerhalb der Amazon Virtual Private Cloud (Amazon VPC). Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3,3.1 Cloud-Computing d. Datenverschlüsselung während der Übertragung	FTI muss während der Übertragung innerhalb der Cloud-Umgebung verschlüsselt werden. Alle zur Verschlüsselung von FTI verwendeten Mechanismen müssen FIPS-140-zertifiziert sein und mit den aktuellen FIPS-140-kompatiblen Modulen betrieben werden. Diese Anforderung muss in der SLA enthalten sein.	elb-tls-https-listeners-nur	Stellen Sie sicher, dass Ihre Elastic Load Balancer (ELBs) mit SSL- oder HTTPS-Listenern konfiguriert sind. Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3,3.1 Cloud-Computing d. Datenverschlüsselung während der Übertragung	FTI muss während der Übertragung innerhalb der Cloud-Umgebung verschlüsselt werden. Alle zur Verschlüsselung von FTI verwendeten Mechanismen müssen FIPS-140-zertifiziert sein und mit den aktuellen FIPS-140-kompatiblen Modulen betrieben werden. Diese Anforderung muss in der SLA enthalten sein.	opensearch-https-required	Da sensible Daten existieren können und um Daten während der Übertragung zu schützen, sollten Sie sicherstellen, dass HTTPS für Verbindungen zu Ihren Amazon OpenSearch Service-Domains aktiviert ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3,3.1 Cloud-Computing d. Datenverschlüsselung während der Übertragung	FTI muss während der Übertragung innerhalb der Cloud-Umgebung verschlüsselt werden. Alle zur Verschlüsselung von FTI verwendeten Mechanismen müssen FIPS-140-zertifiziert sein und mit den aktuellen FIPS-140-kompatiblen Modulen betrieben werden. Diese Anforderung muss in der SLA enthalten sein.	opensearch-node-to-node-Verschlüsselungsprüfung	Stellen Sie sicher, dass die node-to-node Verschlüsselung für Amazon OpenSearch Service aktiviert ist. Node-to-nodeVerschlüsselung ermöglicht die TLS 1.2-Verschlüsselung für die gesamte Kommunikation innerhalb der Amazon Virtual Private Cloud (Amazon VPC). Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3,3.1 Cloud-Computing d. Datenverschlüsselung während der Übertragung	FTI muss während der Übertragung innerhalb der Cloud-Umgebung verschlüsselt werden. Alle zur Verschlüsselung von FTI verwendeten Mechanismen müssen FIPS-140-zertifiziert sein und mit den aktuellen FIPS-140-kompatiblen Modulen betrieben werden. Diese Anforderung muss in der SLA enthalten sein.	redshift-require-tls-ssl	Stellen Sie sicher, dass Ihre Amazon-Redshift-Cluster eine TLS/SSL-Verschlüsselung erfordern, um eine Verbindung zu SQL-Clients herzustellen. Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3,3.1 Cloud-Computing d. Datenverschlüsselung während der Übertragung	FTI muss während der Übertragung innerhalb der Cloud-Umgebung verschlüsselt werden. Alle zur Verschlüsselung von FTI verwendeten Mechanismen müssen FIPS-140-zertifiziert sein und mit den aktuellen FIPS-140-kompatiblen Modulen betrieben werden. Diese Anforderung muss in der SLA enthalten sein.	s-3 bucket-ssl-requests-only	Um Daten während der Übertragung zu schützen, stellen Sie sicher, dass Ihre Amazon Simple Storage Service (Amazon S3)-Buckets Anfragen zur Verwendung von Secure Socket Layer (SSL)-Buckets erfordern. Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3,3.1 Cloud-Computing e. Datenverschlüsselung im Ruhezustand	Datenverschlüsselung im Ruhezustand: FTI muss im Ruhezustand in der Cloud mit dem aktuellen FIPS-140-zertifizierten Verschlüsselungsmechanismus verschlüsselt werden. Diese Anforderung muss in der SLA enthalten sein.	api-gw-cache-enabled-und-verschlüsselt	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass die Verschlüsselung für den Cache Ihrer API-Gateway-Stufe aktiviert ist. Da für die API-Methode sensible Daten erfasst werden können, sollten Sie die Verschlüsselung von Daten im Ruhezustand aktivieren, um diese Daten zu schützen.
3,3.1 Cloud-Computing e. Datenverschlüsselung im Ruhezustand	Datenverschlüsselung im Ruhezustand: FTI muss im Ruhezustand in der Cloud mit dem aktuellen FIPS-140-zertifizierten Verschlüsselungsmechanismus verschlüsselt werden. Diese Anforderung muss in der SLA enthalten sein.	backup-recovery-point-encrypted	Stellen Sie sicher, dass die Verschlüsselung für Ihre AWS Backup-Wiederherstellungspunkte aktiviert ist. Da sensible Daten auch im Ruhezustand vorhanden sein können, sollten Sie die Verschlüsselung im Ruhezustand aktivieren, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3,3.1 Cloud-Computing e. Datenverschlüsselung im Ruhezustand	Datenverschlüsselung im Ruhezustand: FTI muss im Ruhezustand in der Cloud mit dem aktuellen FIPS-140-zertifizierten Verschlüsselungsmechanismus verschlüsselt werden. Diese Anforderung muss in der SLA enthalten sein.	cloud-trail-encryption-enabled	Da sensible Daten vorhanden sein können und um Daten im Ruhezustand zu schützen, sollten Sie sicherstellen, dass die Verschlüsselung für Ihre AWS CloudTrail Trails aktiviert ist.
3,3.1 Cloud-Computing e. Datenverschlüsselung im Ruhezustand	Datenverschlüsselung im Ruhezustand: FTI muss im Ruhezustand in der Cloud mit dem aktuellen FIPS-140-zertifizierten Verschlüsselungsmechanismus verschlüsselt werden. Diese Anforderung muss in der SLA enthalten sein.	dynamodb-table-encrypted-kms	Stellen Sie sicher, dass die Verschlüsselung für Ihre Amazon-DynamoDB-Tabellen aktiviert ist. Um eventuell vorhandene sensible Daten im Ruhezustand in diesen Tabellen zu schützen, müssen Sie die Verschlüsselung von Daten im Ruhezustand aktivieren. Standardmäßig werden DynamoDB-Tabellen mit einem AWS eigenen Kundenhauptschlüssel (CMK) verschlüsselt.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3,3.1 Cloud-Computing e. Datenverschlüsselung im Ruhezustand	Datenverschlüsselung im Ruhezustand: FTI muss im Ruhezustand in der Cloud mit dem aktuellen FIPS-140-zertifizierten Verschlüsselungsmechanismus verschlüsselt werden. Diese Anforderung muss in der SLA enthalten sein.	ec2- ebs-encryption-by-default	Zum Schutz von Daten im Ruhezustand müssen Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon Elastic Block Store (Amazon EBS)-Volumes aktiviert ist. Da sensible Daten auch im Ruhezustand vorhanden sein können, sollten Sie die Verschlüsselung im Ruhezustand aktivieren, um diese Daten zu schützen.
3,3.1 Cloud-Computing e. Datenverschlüsselung im Ruhezustand	Datenverschlüsselung im Ruhezustand: FTI muss im Ruhezustand in der Cloud mit dem aktuellen FIPS-140-zertifizierten Verschlüsselungsmechanismus verschlüsselt werden. Diese Anforderung muss in der SLA enthalten sein.	efs-encrypted-check	Aktivieren Sie die Verschlüsselung für Ihr Amazon Elastic File System (EFS), um eventuell vorhandene sensible Daten sowie Daten im Ruhezustand zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3,3.1 Cloud-Computing e. Datenverschlüsselung im Ruhezustand	Datenverschlüsselung im Ruhezustand: FTI muss im Ruhezustand in der Cloud mit dem aktuellen FIPS-140-zertifizierten Verschlüsselungsmechanismus verschlüsselt werden. Diese Anforderung muss in der SLA enthalten sein.	elasticsearch-encrypted-at-rest	Da sensible Daten vorhanden sein können und um Daten im Ruhezustand zu schützen, sollten Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon OpenSearch Service (OpenSearch Service) -Domains aktiviert ist.
3,3.1 Cloud-Computing e. Datenverschlüsselung im Ruhezustand	Datenverschlüsselung im Ruhezustand: FTI muss im Ruhezustand in der Cloud mit dem aktuellen FIPS-140-zertifizierten Verschlüsselungsmechanismus verschlüsselt werden. Diese Anforderung muss in der SLA enthalten sein.	encrypted-volumes	Aktivieren Sie die Verschlüsselung für Ihre Amazon-Elastic-Block-Store (Amazon-EBS)-Volumes, um eventuell vorhandene sensible Daten sowie Daten im Ruhezustand zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3,3.1 Cloud-Computing e. Datenverschlüsselung im Ruhezustand	Datenverschlüsselung im Ruhezustand: FTI muss im Ruhezustand in der Cloud mit dem aktuellen FIPS-140-zertifizierten Verschlüsselungsmechanismus verschlüsselt werden. Diese Anforderung muss in der SLA enthalten sein.	kinesis-stream-encrypted	Aktivieren Sie die Verschlüsselung für Ihre Amazon-Kinesis-Streams, um eventuell vorhandene sensible Daten sowie Daten im Ruhezustand zu schützen.
3,3.1 Cloud-Computing e. Datenverschlüsselung im Ruhezustand	Datenverschlüsselung im Ruhezustand: FTI muss im Ruhezustand in der Cloud mit dem aktuellen FIPS-140-zertifizierten Verschlüsselungsmechanismus verschlüsselt werden. Diese Anforderung muss in der SLA enthalten sein.	opensearch-encrypted-at-rest	Da sensible Daten vorhanden sein können und um Daten im Ruhezustand zu schützen, sollten Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon OpenSearch Service-Domains aktiviert ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3,3.1 Cloud-Computing e. Datenverschlüsselung im Ruhezustand	Datenverschlüsselung im Ruhezustand: FTI muss im Ruhezustand in der Cloud mit dem aktuellen FIPS-140-zertifizierten Verschlüsselungsmechanismus verschlüsselt werden. Diese Anforderung muss in der SLA enthalten sein.	rds-snapshot-encrypted	Stellen Sie sicher, dass die Verschlüsselung für Ihre Amazon Relational Database Service (Amazon RDS)-Snapshots aktiviert ist. Da sensible Daten auch im Ruhezustand vorhanden sein können, sollten Sie die Verschlüsselung im Ruhezustand aktivieren, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3,3.1 Cloud-Computing e. Datenverschlüsselung im Ruhezustand	Datenverschlüsselung im Ruhezustand: FTI muss im Ruhezustand in der Cloud mit dem aktuellen FIPS-140-zertifizierten Verschlüsselungsmechanismus verschlüsselt werden. Diese Anforderung muss in der SLA enthalten sein.	rds-storage-encrypted	Zum Schutz von Daten im Ruhezustand müssen Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon Relational Database Service (Amazon RDS)-Instances aktiviert ist. Um eventuell vorhandene sensible Daten im Ruhezustand in Amazon-RDS-Instances zu schützen, muss die Verschlüsselung von Daten im Ruhezustand aktiviert sein.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3,3.1 Cloud-Computing e. Datenverschlüsselung im Ruhezustand	Datenverschlüsselung im Ruhezustand: FTI muss im Ruhezustand in der Cloud mit dem aktuellen FIPS-140-zertifizierten Verschlüsselungsmechanismus verschlüsselt werden. Diese Anforderung muss in der SLA enthalten sein.	redshift-cluster-configuration-check	Um Daten im Ruhezustand zu schützen, muss die Verschlüsselung für Ihre Amazon-Redshift-Cluster aktiviert sein. Sie müssen auch sicherstellen, dass die erforderlichen Konfigurationen auf Amazon-Redshift-Clustern bereitgestellt werden. Die Prüfungsprotokollierung muss aktiviert sein, um Informationen zu Verbindungen und Benutzeraktivitäten in der Datenbank bereitzustellen. Diese Regel erfordert, dass ein Wert für clusterDbEncrypted (Config Default: TRUE) und LoggingEnabled (Config Default: TRUE) gesetzt ist. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3,3.1 Cloud-Computing e. Datenverschlüsselung im Ruhezustand	Datenverschlüsselung im Ruhezustand: FTI muss im Ruhezustand in der Cloud mit dem aktuellen FIPS-140-zertifizierten Verschlüsselungsmechanismus verschlüsselt werden. Diese Anforderung muss in der SLA enthalten sein.	redshift-cluster-kms-enabled	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass die Verschlüsselung mit AWS Key Management Service (AWS KMS) für Ihren Amazon Redshift Redshift-Cluster aktiviert ist. Um eventuell vorhandene sensible Daten im Ruhezustand in Redshift-Clustern zu schützen, muss die Verschlüsselung von Daten im Ruhezustand aktiviert sein.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3,3.1 Cloud-Computing e. Datenverschlüsselung im Ruhezustand	Datenverschlüsselung im Ruhezustand: FTI muss im Ruhezustand in der Cloud mit dem aktuellen FIPS-140-zertifizierten Verschlüsselungsmechanismus verschlüsselt werden. Diese Anforderung muss in der SLA enthalten sein.	s3- aktiviert bucket-server-side-encryption	Zum Schutz von Daten im Ruhezustand müssen Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon Simple Storage Service (Amazon S3)-Buckets aktiviert ist. Um eventuell vorhandene sensible Daten im Ruhezustand in Amazon-S3-Buckets zu schützen, muss die Verschlüsselung aktiviert sein.
3,3.1 Cloud-Computing e. Datenverschlüsselung im Ruhezustand	Datenverschlüsselung im Ruhezustand: FTI muss im Ruhezustand in der Cloud mit dem aktuellen FIPS-140-zertifizierten Verschlüsselungsmechanismus verschlüsselt werden. Diese Anforderung muss in der SLA enthalten sein.	s-3 default-encryption-kms	Stellen Sie sicher, dass die Verschlüsselung für Ihre Amazon Simple Storage Service (Amazon S3)-Buckets aktiviert ist. Um eventuell vorhandene sensible Daten im Ruhezustand in einem Amazon-S3-Bucket zu schützen, muss die Verschlüsselung aktiviert sein.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3,3.1 Cloud-Computing e. Datenverschlüsselung im Ruhezustand	Datenverschlüsselung im Ruhezustand: FTI muss im Ruhezustand in der Cloud mit dem aktuellen FIPS-140-zertifizierten Verschlüsselungsmechanismus verschlüsselt werden. Diese Anforderung muss in der SLA enthalten sein.	sagemaker-endpoint-configuration-kms-key-konfiguriert	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass die Verschlüsselung mit dem AWS Key Management Service (AWS KMS) für Ihren Endpunkt aktiviert ist. SageMaker Da sensible Daten auf dem SageMaker Endgerät gespeichert werden können, sollten Sie die Verschlüsselung im Ruhezustand aktivieren, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3,3.1 Cloud-Computing e. Datenverschlüsselung im Ruhezustand	Datenverschlüsselung im Ruhezustand: FTI muss im Ruhezustand in der Cloud mit dem aktuellen FIPS-140-zertifizierten Verschlüsselungsmechanismus verschlüsselt werden. Diese Anforderung muss in der SLA enthalten sein.	sagemaker-notebook-instance-kms-schlüsselkonfiguriert	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass die Verschlüsselung mit dem AWS Key Management Service (AWS KMS) für Ihr Notebook aktiviert ist. SageMaker Da vertrauliche Daten im SageMaker Notebook gespeichert werden können, sollten Sie die Verschlüsselung im Ruhezustand aktivieren, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3,3.1 Cloud-Computing e. Datenverschlüsselung im Ruhezustand	Datenverschlüsselung im Ruhezustand: FTI muss im Ruhezustand in der Cloud mit dem aktuellen FIPS-140-zertifizierten Verschlüsselungsmechanismus verschlüsselt werden. Diese Anforderung muss in der SLA enthalten sein.	secretsmanager-using-cmk	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass die Verschlüsselung mit dem AWS Key Management Service (AWS KMS) für AWS Secrets Manager aktiviert ist. Aktivieren Sie die Verschlüsselung von Daten im Ruhezustand, um eventuell vorhandene sensible Daten im Ruhezustand im Secrets Manager zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3,3.1 Cloud-Computing k. Multi-Faktor-Authentifizierung	Behörden müssen eine ausreichende Multi-Faktor-Authentifizierung implementieren, wenn ihre Cloud-Lösungen über das Internet verfügbar sind (d. h., wenn der Zugriff auf die Cloud-Lösung von außerhalb des vertrauenswürdigen Netzwerks der Behörde erfolgt).	iam-user-mfa-enabled	Aktivieren Sie diese Regel, um den Zugriff auf Ressourcen in der AWS Cloud einzuschränken. Diese Regel sorgt dafür, dass die Multi-Faktor-Authentifizierung (MFA) für alle Benutzer aktiviert ist. MFA sorgt für eine weitere Schutzebene zusätzlich zu den Anmeldeinformationen. Reduzieren Sie Fälle von kompromittierten Konten, indem Sie MFA für Benutzer vorschreiben.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3,3.1 Cloud-Computing k. Multi-Faktor-Authentifizierung	Behörden müssen eine ausreichende Multi-Faktor-Authentifizierung implementieren, wenn ihre Cloud-Lösungen über das Internet verfügbar sind (d. h., wenn der Zugriff auf die Cloud-Lösung von außerhalb des vertrauenswürdigen Netzwerks der Behörde erfolgt).	mfa-enabled-for-iam-Konsolenzugriff	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass MFA für alle AWS Identity and Access Management (IAM) -Benutzer aktiviert ist, die über ein Konsolenkennwort verfügen. MFA sorgt für eine weitere Schutzebene zusätzlich zu den Anmeldeinformationen. Indem Sie MFA für Benutzer vorschreiben, können Sie Fälle kompromittierter Konten reduzieren und verhindern, dass unbefugte Benutzer auf vertrauliche Daten zugreifen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3,3.1 Cloud-Computing k. Multi-Faktor-Authentifizierung	Behörden müssen eine ausreichende Multi-Faktor-Authentifizierung implementieren, wenn ihre Cloud-Lösungen über das Internet verfügbar sind (d. h., wenn der Zugriff auf die Cloud-Lösung von außerhalb des vertrauenswürdigen Netzwerks der Behörde erfolgt).	root-account-hardware-mfa-aktiviert	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Hardware-MFA für den Root-Benutzer aktiviert ist. Der Stammbenutzer ist der AWS-Konto-Benutzer mit den meisten Berechtigungen. MFA sorgt für eine weitere Schutzebene zusätzlich zu den Anmeldeinformationen. Indem Sie MFA für den Root-Benutzer vorschreiben, können Sie die Anzahl AWS-Konten kompromittierter Benutzer reduzieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3,3.1 Cloud-Computing k. Multi-Faktor-Authentifizierung	Behörden müssen eine ausreichende Multi-Faktor-Authentifizierung implementieren, wenn ihre Cloud-Lösungen über das Internet verfügbar sind (d. h., wenn der Zugriff auf die Cloud-Lösung von außerhalb des vertrauenswürdigen Netzwerks der Behörde erfolgt).	root-account-mfa-enabled	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass MFA für den Root-Benutzer aktiviert ist. Der Stammbenutzer ist der AWS-Konto-Benutzer mit den meisten Berechtigungen. MFA sorgt für eine weitere Schutzebene zusätzlich zu den Anmeldeinformationen. Indem Sie MFA für den Root-Benutzer vorschreiben, können Sie die Anzahl AWS-Konten kompromittierter Benutzer reduzieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3,3.1 Cloud-Computing i. Risikobewertung:	Die Behörde muss jährlich eine Bewertung der Sicherheits- und Datenschutzkontrollen durchführen, die für alle Informationssysteme gelten, die für den Empfang, die Verarbeitung, die Speicherung, den Zugriff, den Schutz und/oder die Übertragung von FTI verwendet werden.	annual-risk-assessment-performed(Prozessüberprüfung)	Führen Sie eine jährliche Risikobewertung für Ihre Organisation durch. Risikowertungen können dabei helfen, die Wahrscheinlichkeit und Auswirkungen identifizierter Risiken und/oder Schwachstellen für eine Organisation zu ermitteln.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.3.6 Netzwerkgrenze und Infrastruktur	Die Behörden müssen in ihrer gesamten Systemarchitektur Grenzschutzeinrich tungen einsetzen, einschließlich Router, Firewalls, Switches und Systeme zur Angriffserkennung, um FTI sowie FTI-Systeme zu schützen.	guardduty-enabled-centralized	Amazon GuardDuty kann mithilfe von Threat Intellige nce Feeds helfen, potenzielle Cybersich erheitsereignisse zu überwachen und zu erkennen. Dazu gehören Listen mit bösartigen IPs und maschinel len Lernmethoden zur Identifizierung unerwarteter, nicht autorisierter und bösartiger Aktivitäten in Ihrer AWS Cloud-Umgebung.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.3.6 Netzwerkgrenze und Infrastruktur	Die Behörden müssen in ihrer gesamten Systemarchitektur Grenzschutzeinrichtungen einsetzen, einschließlich Router, Firewalls, Switches und Systeme zur Angriffserkennung, um FTI sowie FTI-Systeme zu schützen.	guardduty-non-archived-findings	Amazon GuardDuty hilft Ihnen dabei, die Auswirkungen eines Vorfalls zu verstehen, indem es die Ergebnisse nach Schweregrad klassifiziert: niedrig, mittel und hoch. Diese Klassifizierungen können Sie zur Festlegung von entsprechenden Strategien und Prioritäten zur Behebung solcher Vorfälle verwenden. Mit dieser Regel können Sie optional daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7) und daysHighSev (Config Default: 1) für nicht archivierte Ergebnisse festlegen, wie es die Richtlinien Ihrer Organisation erfordern.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.3.6 Netzwerkgrenze und Infrastruktur	Die Behörden müssen in ihrer gesamten Systemarchitektur Grenzschutzeinrich tungen einsetzen, einschließlich Router, Firewalls, Switches und Systeme zur Angriffserkennung, um FTI sowie FTI-Systeme zu schützen.	netfw-policy-rule-group-verknüpft	Eine AWS Netzwerk-Firewall-Richtlinie definiert, wie Ihre Firewall den Verkehr in einer Amazon VPC überwacht und verarbeitet. Sie konfigurieren statusfre ie und statusbehaftete Regelgruppen, um Pakete und Datenverk ehrsströme zu filtern, und Sie definiere n den standardm äßigen Umgang mit Datenverkehr.
3.3.6 Netzwerkgrenze und Infrastruktur	Die Behörden müssen in ihrer gesamten Systemarchitektur Grenzschutzeinrich tungen einsetzen, einschließlich Router, Firewalls, Switches und Systeme zur Angriffserkennung, um FTI sowie FTI-Systeme zu schützen.	netfw-stateless-rule-group-nicht leer	Eine AWS Netzwerkf irewall-Regelgrupp e enthält Regeln, die definieren, wie Ihre Firewall den Verkehr in Ihrer VPC verarbeit et. Wenn eine leere statuslose Regelgrup pe in einer Firewall-Richtlinie vorhanden ist, verarbeitet sie keinen Datenverkehr.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.3.6 Netzwerkgrenze und Infrastruktur	Die Behörden müssen in ihrer gesamten Systemarchitektur Grenzschutzeinrich tungen einsetzen, einschließlich Router, Firewalls, Switches und Systeme zur Angriffserkennung, um FTI sowie FTI-Systeme zu schützen.	securityhub-enabled	AWS Security Hub hilft bei der Überwachung von unbefugtem Personal, Verbindun gen, Geräten und Software. AWS Security Hub aggregiert, organisie rt und priorisie rt die Sicherhei tswarnungen oder Ergebnisse mehrerer Dienste. AWS Einige dieser Dienste sind Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer und AWS Firewall Manager sowie AWS Partnerlösungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.3.6 Netzwerkgrenze und Infrastruktur	Die Behörden müssen in ihrer gesamten Systemarchitektur Grenzschutzeinrich tungen einsetzen, einschließlich Router, Firewalls, Switches und Systeme zur Angriffserkennung, um FTI sowie FTI-Systeme zu schützen.	waf-regional-rule-not-leer	Stellen Sie sicher, dass Ihre AWS WAF eine Regel hat, die nicht leer ist. Eine Regel ohne Bedingungen kann zu unbeabsichtigtem Verhalten führen.
3.3.6 Netzwerkgrenze und Infrastruktur	Die Behörden müssen in ihrer gesamten Systemarchitektur Grenzschutzeinrich tungen einsetzen, einschließlich Router, Firewalls, Switches und Systeme zur Angriffserkennung, um FTI sowie FTI-Systeme zu schützen.	waf-regional-rulegroup-not-leer	Stellen Sie sicher, dass Ihre AWS WAF eine Regelgruppe hat, die nicht leer ist. Eine leere Regelgruppe kann zu unbeabsichtigtem Verhalten führen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.3.6 Netzwerkgrenze und Infrastruktur	Die Behörden müssen in ihrer gesamten Systemarchitektur Grenzschutzeinrich tungen einsetzen, einschließlich Router, Firewalls, Switches und Systeme zur Angriffserkennung, um FTI sowie FTI-Systeme zu schützen.	waf-regional-webacl-not-leer	Eine an eine AWS WAF angehängt e Web-ACL kann eine Sammlung von Regeln und Regelgruppen zur Überprüfung und Steuerung von Webanfragen enthalten. Wenn eine Web-ACL leer ist, wird der Webdatenverkehr weitergeleitet, ohne von der WAF erkannt oder bearbeitet zu werden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.3.6 Netzwerkgrenze und Infrastruktur	Die Behörden müssen in ihrer gesamten Systemarchitektur Grenzschutzeinrich tungen einsetzen, einschließlich Router, Firewalls, Switches und Systeme zur Angriffserkennung, um FTI sowie FTI-Systeme zu schützen.	alb-waf-enabled	Stellen Sie sicher, dass AWS WAF auf Elastic Load Balancers (ELB) aktiviert ist, um Webanwendungen zu schützen. Eine WAF trägt zum Schutz Ihrer Webanwend ungen oder APIs vor gängigen Web-Explo its bei. Diese Web-Exploits können sich auf die Verfügbar keit auswirken, die Sicherheit gefährden oder übermäßige Ressourcen in Ihrer Umgebung verbrauch en.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.3.6 Netzwerkgrenze und Infrastruktur	Die Behörden müssen in ihrer gesamten Systemarchitektur Grenzschutzeinrich tungen einsetzen, einschließlich Router, Firewalls, Switches und Systeme zur Angriffserkennung, um FTI sowie FTI-Systeme zu schützen.	api-gw-associated-with-WAF	AWS Mit WAF können Sie eine Reihe von Regeln (als Web Access Control List (Web ACL) bezeichne t) konfigurieren, die Webanfragen auf der Grundlage von anpassbaren Websicherheitsrege ln und -bedingungen, die Sie definieren, zulassen, blockieren oder zählen. Stellen Sie sicher, dass Ihre Amazon-API-Gateway-Stufe mit einer WAF-Web-A CL verknüpft ist, um sie vor böswilligen Angriffen zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-2 Kontoverwaltung (f)	Konten müssen gemäß den behördlichen Anforderungen für die Kontoverwaltung erstellt, aktiviert, geändert, deaktiviert und entfernt werden;	iam-user-unused-credentials-überprüfen	AWS Identity and Access Management (IAM) kann Ihnen bei Zugriffsberechtigungen und Autorisierungen helfen, indem es nach IAM-Passwörtern und Zugriffsschlüsseln sucht, die für einen bestimmten Zeitraum nicht verwendet wurden. Wenn ungenutzte Anmeldeinformationen identifiziert werden, müssen Sie sie deaktivieren und/oder entfernen, da dies gegen das Prinzip der geringsten Berechtigung verstoßen könnte. Für diese Regel müssen Sie einen Wert für das maxCredentialUsage Alter festlegen (Standardkonfiguration: 90). Der tatsächliche Wert muss den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-2 Kontoverwaltung (f)	Konten müssen gemäß den behördlichen Anforderungen für die Kontoverwaltung erstellt, aktiviert, geändert, deaktiviert und entfernt werden;	account-part-of-organizations	Durch die zentrale Verwaltung AWS-Konten innerhalb von AWS Organizations wird sichergestellt, dass die Konten den Vorschriften entsprechen. Eine fehlende zentrale Kontoverwaltung kann zu inkonsistenten Kontokonfigurationen führen, wodurch Ressourcen und sensible Daten offengelegt werden können.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-2 Kontoverwaltung (f)	Konten müssen gemäß den behördlichen Anforderungen für die Kontoverwaltung erstellt, aktiviert, geändert, deaktiviert und entfernt werden;	iam-root-access-key-überprüfen	Der Zugriff auf Systeme und Ressourcen kann gesteuert werden, indem überprüft wird, ob der Root-Benutzer keine Zugriffsschlüssel mit seiner AWS Identity and Access Management (IAM) -Rolle verknüpft hat. Stellen Sie sicher, dass die Root-Zugriffsschlüssel gelöscht werden. Erstellen und verwenden Sie stattdessen rollenbasierte Funktionen, AWS-Konten um das Prinzip der geringsten Funktionalität zu berücksichtigen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-2 Kontoverwaltung (f)	Konten müssen gemäß den behördlichen Anforderungen für die Kontoverwaltung erstellt, aktiviert, geändert, deaktiviert und entfernt werden;	iam-user-mfa-enabled	Aktivieren Sie diese Regel, um den Zugriff auf Ressourcen in der AWS Cloud einzuschränken. Diese Regel sorgt dafür, dass die Multi-Faktor-Authentifizierung (MFA) für alle Benutzer aktiviert ist. MFA sorgt für eine weitere Schutzebene zusätzlich zu den Anmeldeinformationen. Reduzieren Sie Fälle von kompromittierten Konten, indem Sie MFA für Benutzer vorschreiben.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-2 Kontoverwaltung (f)	Konten müssen gemäß den behördlichen Anforderungen für die Kontoverwaltung erstellt, aktiviert, geändert, deaktiviert und entfernt werden;	iam-user-no-policies-überprüfen	Diese Regel stellt sicher, dass AWS Identity and Access Management (IAM)-Richtlinien nur Gruppen oder Rollen zugewiesen werden, um den Zugriff auf Systeme und Ressourcen zu kontrollieren. Die Zuweisung von Berechtigungen auf Gruppen- oder Rollenebene trägt dazu bei, die Wahrscheinlichkeit zu verringern, dass eine Identität übermäßige Berechtigungen erhält oder beibehält.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-2 Kontoverwaltung (g)	Überwachen Sie die Verwendung von Konten.	cloudtrail-enabled	AWS CloudTrail kann durch die Aufzeichnung von Aktionen und API-Aufrufen in der AWS Management Console helfen, die Ablehnung zu verhindern. Sie können die Benutzer und die Benutzer AWS-Konten , die einen AWS Dienst aufgerufen haben, die Quell-IP-Adresse, über die die Aufrufe generiert wurden, und den Zeitpunkt der Anrufe identifizieren. Einzelheiten zu den erfassten Daten finden Sie in den AWS CloudTrail Datensatzinhalten.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-2 Kontoverwaltung (g)	Überwachen Sie die Verwendung von Konten.	cloud-trail-cloud-watch-logs-aktiviert	Verwenden Sie Amazon CloudWatch , um Protokoll ereignisaktivitäten zentral zu sammeln und zu verwalten. Die Aufnahme von AWS CloudTrail Daten liefert Einzelheiten zu den API-Aufrufaktivitäten in Ihrem AWS-Konto.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-2 Kontoverwaltung (g)	Überwachen Sie die Verwendung von Konten.	cloud-trail-log-file-Validierung aktiviert	Verwenden Sie die AWS CloudTrail Protokolldateivalidierung, um die Integrität von Protokollen zu überprüfen. CloudTrail Mithilfe der Protokolldateivalidierung kann festgestellt werden, ob eine Protokolldatei geändert oder gelöscht wurde oder ob sie nach der Übermittlung CloudTrail unverändert geblieben ist. Dieses Feature wurde mit dem Branchenstandard entsprechenden Algorithmen entwickelt: SHA-256 für die Hashfunktion und SHA-256 mit RSA für digitale Signaturen. Aus diesem Grund ist es rechnerisch unmöglich, CloudTrail Protokolldateien unbemerkt zu ändern, zu löschen oder zu fälschen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-2 Kontoverwaltung (g)	Überwachen Sie die Verwendung von Konten.	guardduty-enabled-centralized	Amazon GuardDuty kann mithilfe von Threat Intelligence Feeds helfen, potenzielle Cybersicherheitsereignisse zu überwachen und zu erkennen. Dazu gehören Listen mit bösartigen IPs und maschinellen Lernmethoden zur Identifizierung unerwarteter, nicht autorisierter und bösartiger Aktivitäten in Ihrer AWS Cloud-Umgebung.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-2 Kontoverwaltung (g)	Überwachen Sie die Verwendung von Konten.	rds-logging-enabled	Um die Protokollierung und Überwachung in Ihrer Umgebung zu erleichtern, stellen Sie sicher, dass die Amazon Relational Database Service (Amazon RDS)-Protokollierung aktiviert ist. Mit der Amazon-RDS-Protokollierung können Sie Ereignisse wie Verbindungen, Verbindungsabbrüche, Abfragen oder abgefragte Tabellen erfassen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-2 Kontoverwaltung (g)	Überwachen Sie die Verwendung von Konten.	redshift-cluster-configuration-check	Um Daten im Ruhezustand zu schützen, muss die Verschlüsselung für Ihre Amazon-Redshift-Cluster aktiviert sein. Sie müssen auch sicherstellen, dass die erforderlichen Konfigurationen auf Amazon-Redshift-Clustern bereitgestellt werden. Die Prüfungsprotokollierung muss aktiviert sein, um Informationen zu Verbindungen und Benutzeraktivitäten in der Datenbank bereitzustellen. Diese Regel erfordert, dass ein Wert für clusterDbEncrypted (Config Default: TRUE) und LoggingEnabled (Config Default: TRUE) gesetzt ist. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-2 Kontoverwaltung (g)	Überwachen Sie die Verwendung von Konten.	s3- bucket-logging-enabled	Die Amazon Simple Storage Service (Amazon S3)-Serverzugriffsprotokollierung bietet eine Methode zur Überwachung des Netzwerks im Hinblick auf potenzielle Cybersicherheitsereignisse. Die Ereignisse werden überwacht, indem detaillierte Aufzeichnungen über die Anfragen erfasst werden, die an einen Amazon-S3-Bucket gestellt wurden. Jeder Zugriffsprotokolleintrag enthält Details zu einer einzelnen Zugriffsanfrage. Zu den Details gehören Anforderer, Bucket-Name, Anforderungszeit, Anforderungsaktion, Antwortstatus und Fehlercode, falls relevant.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-2 Kontoverwaltung (g)	Überwachen Sie die Verwendung von Konten.	securityhub-enabled	AWS Security Hub hilft bei der Überwachung von unbefugtem Personal, Verbindungen, Geräten und Software. AWS Security Hub aggregiert, organisiert und priorisiert die Sicherheitswarnungen oder Ergebnisse mehrerer Dienste. AWS Einige dieser Dienste sind Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer und AWS Firewall Manager sowie AWS Partnerlösungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-2 Kontoverwaltung (j)	Überprüfen Sie die Konten auf die Einhaltung der Anforderungen an die Kontoverwaltung.	root-account-mfa-enabled	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass MFA für den Root-Benutzer aktiviert ist. Der Stammbenutzer ist der AWS-Konto-Benutzer mit den meisten Berechtigungen. MFA sorgt für eine weitere Schutzebene zusätzlich zu den Anmeldeinformationen. Indem Sie MFA für den Root-Benutzer vorschreiben, können Sie die Anzahl AWS-Konten kompromittierter Benutzer reduzieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-2 Kontoverwaltung (j)	Überprüfen Sie die Konten auf die Einhaltung der Anforderungen an die Kontoverwaltung.	secretsmanager-scheduled-rotation-success-überprüfen	Diese Regel stellt sicher, dass AWS Secrets Manager Manager-Geheimnisse gemäß dem Rotationsplan erfolgreich rotiert wurden. Die regelmäßige Rotation von Secrets kann den Zeitraum verkürzen, in dem ein Secret aktiv ist, und möglicherweise die Auswirkungen auf das Unternehmen verringern, falls es kompromittiert wird.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-2 Kontoverwaltung (j)	Überprüfen Sie die Konten auf die Einhaltung der Anforderungen an die Kontoverwaltung.	secretsmanager-secret-periodic-rotation	Diese Regel stellt sicher, dass bei AWS Secrets Manager Manager-Geheimnissen die regelmäßige Rotation aktiviert ist. Die regelmäßige Rotation von Secrets kann den Zeitraum verkürzen, in dem ein Secret aktiv ist, und möglicherweise die Auswirkungen auf das Unternehmen verringern, falls das Secret kompromittiert wird. Der Standardwert lautet 90 Tage.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-2 Kontoverwaltung (j)	Überprüfen Sie die Konten auf die Einhaltung der Anforderungen an die Kontoverwaltung.	secretsmanager-secret-unused	Wenn in AWS Secrets Manager unbenutzte Anmeldeinformationen vorhanden sind, sollten Sie die Anmeldeinformationen deaktivieren und/oder entfernen, da dies gegen das Prinzip der geringsten Rechte verstoßen kann. Mit dieser Regel können Sie einen Wert auf unusedForDays (Config Default: 90) setzen. Der tatsächliche Wert muss den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-2 Kontoverwaltung (j)	Überprüfen Sie die Konten auf die Einhaltung der Anforderungen an die Kontoverwaltung.	iam-password-policy	Die Identitäten und Anmeldeinformationen werden auf der Grundlage einer organisatorischen IAM-Passwortrichtlinie ausgestellt, verwaltet und verifiziert. Sie erfüllen oder übertreffen die Anforderungen, die von NIST SP 800-63 und dem Standard „Best Practices“ von AWS Foundational Security für die Passwortstärke festgelegt wurden. Mit dieser Regel können Sie optional RequireUppercaseCharacters (Wert für AWS grundlegende Sicherheitsbewährte Methoden: wahr), RequireLowercaseCharacters (Wert für bewährte Methoden für AWS grundlegende Sicherheit: wahr), RequireSymbols (Wert für bewährte Methoden für AWS grundlege

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			nde Sicherheit: wahr), RequireNumbers (Wert für bewährte Methoden für AWS grundlegende Sicherheit: wahr), MinimumPasswordLength (Wert für bewährte Methoden für AWS grundlegende Sicherheit: 14), PasswordReusePrevention (Wert für bewährte Methoden für AWS grundlegende Sicherheit: 24) und MaxPasswordAge (Wert für bewährte Methoden für AWS grundlegende Sicherheit: 90) für Ihr IAM festlegen Kennwortrichtlinie. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-2 Kontoverwaltung (j)	Überprüfen Sie die Konten auf die Einhaltung der Anforderungen an die Kontoverwaltung.	access-keys-rotated	Die Anmeldeinformationen für autorisierte Geräte, Benutzer und Prozesse werden geprüft, indem sichergestellt wird, dass die IAM-Zugriffsschlüssel gemäß den Vorgaben der Unternehmensrichtlinie rotiert werden. Das regelmäßige Ändern der Zugriffsschlüssel ist eine bewährte Sicherheitsmethode. Es verkürzt den Zeitraum, in dem ein Zugriffsschlüssel aktiv ist, und reduziert die Auswirkungen auf das Unternehmen, wenn die Schlüssel kompromittiert werden. Diese Regel erfordert einen Wert für die Zugriffsschlüssel-Rotation (Standardkonfiguration: 90). Der tatsächliche Wert muss den Richtlini

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			en Ihrer Organisation entsprechen.
AC-2 Kontoverwaltung (j)	Überprüfen Sie die Konten auf die Einhaltung der Anforderungen an die Kontoverwaltung.	iam-policy-no-statements-with-full-access	Stellen Sie sicher, dass IAM-Aktionen nur auf die benötigten Aktionen beschränkt sind. Wenn Benutzern mehr Rechte eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und der Aufgabentrennung verstoßen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-2 Kontoverwaltung (j)	Überprüfen Sie die Konten auf die Einhaltung der Anforderungen an die Kontoverwaltung.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) kann Ihnen dabei helfen, die Prinzipien der geringsten Rechte und der Aufgabentrennung in Zugriffsberechtigungen und Autorisierungen zu integrieren und so zu verhindern, dass Richtlinien „Effect“: „Allow“ mit „Action“: „*“ anstelle von „Resource“: „*“ enthalten. Wenn Benutzern mehr Rechte eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und der Aufgabentrennung verstoßen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-2 Kontoverwaltung (j)	Überprüfen Sie die Konten auf die Einhaltung der Anforderungen an die Kontoverwaltung.	iam-root-access-key-überprüfen	Der Zugriff auf Systeme und Ressourcen kann gesteuert werden, indem überprüft wird, ob der Root-Benutzer keine Zugriffsschlüssel mit seiner AWS Identity and Access Management (IAM) -Rolle verknüpft hat. Stellen Sie sicher, dass die Root-Zugriffsschlüssel gelöscht werden. Erstellen und verwenden Sie stattdessen rollenbasierte Funktionen, AWS-Konten um das Prinzip der geringsten Funktionalität zu berücksichtigen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-2 Kontoverwaltung (j)	Überprüfen Sie die Konten auf die Einhaltung der Anforderungen an die Kontoverwaltung.	iam-user-no-policies-überprüfen	Diese Regel stellt sicher, dass AWS Identity and Access Management (IAM) -Richtlinien nur Gruppen oder Rollen zugewiesen werden, um den Zugriff auf Systeme und Ressourcen zu kontrollieren. Die Zuweisung von Berechtigungen auf Gruppen- oder Rollenebene trägt dazu bei, die Wahrscheinlichkeit zu verringern, dass eine Identität übermäßige Berechtigungen erhält oder beibehält.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-2 Kontoverwaltung (j)	Überprüfen Sie die Konten auf die Einhaltung der Anforderungen an die Kontoverwaltung.	iam-user-unused-credentials-überprüfen	AWS Identity and Access Management (IAM) kann Ihnen bei Zugriffsberechtigungen und Autorisierungen helfen, indem es nach IAM-Passwörtern und Zugriffsschlüsseln sucht, die für einen bestimmten Zeitraum nicht verwendet wurden. Wenn ungenutzte Anmeldeinformationen identifiziert werden, müssen Sie sie deaktivieren und/oder entfernen, da dies gegen das Prinzip der geringsten Berechtigung verstoßen könnte. Für diese Regel müssen Sie einen Wert für das maxCredentialUsage Alter festlegen (Standardkonfiguration: 90). Der tatsächliche Wert muss den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
(CE-1) Automatisierte Systemkontenverwaltung	Unterstützen Sie die Verwaltung von Systemkonten mithilfe automatisierter Mechanismen.	iam-password-policy	Die Identitäten und Anmeldeinformationen werden auf der Grundlage einer organisatorischen IAM-Passwortrichtlinie ausgestellt, verwaltet und verifiziert. Sie erfüllen oder übertreffen die Anforderungen, die von NIST SP 800-63 und dem Standard „Best Practices“ von AWS Foundational Security in Bezug auf die Passwortstärke festgelegt wurden. Mit dieser Regel können Sie optional RequireUppercaseCharacters (Wert für AWS grundlegende Sicherheitsbewährte Methoden: wahr), RequireLowercaseCharacters (Wert für bewährte Methoden für AWS grundlegende Sicherheit: wahr), RequireSymbols (Wert für bewährte Methoden

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			für AWS grundlegende Sicherheit: wahr), RequireNumbers (Wert für bewährte Methoden für AWS grundlegende Sicherheit: wahr), MinimumPasswordLength (Wert für bewährte Methoden für AWS grundlegende Sicherheit: 14), PasswordReusePrevention (Wert für bewährte Methoden für AWS grundlegende Sicherheit: 24) und MaxPasswordAge (Wert für bewährte Methoden für AWS grundlegende Sicherheit: 90) für Ihr IAM festlegen Kennwortrichtlinie. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
(CE-1) Automatisierte Systemkontenverwaltung	Unterstützen Sie die Verwaltung von Systemkonten mithilfe automatisierter Mechanismen.	access-keys-rotated	Die Anmeldeinformationen für autorisierte Geräte, Benutzer und Prozesse werden geprüft, indem sichergestellt wird, dass die IAM-Zugriffsschlüssel gemäß den Vorgaben der Unternehmensrichtlinie rotiert werden. Das regelmäßige Ändern der Zugriffsschlüssel ist eine bewährte Sicherheitsmethode. Es verkürzt den Zeitraum, in dem ein Zugriffsschlüssel aktiv ist, und reduziert die Auswirkungen auf das Unternehmen, wenn die Schlüssel kompromittiert werden. Diese Regel erfordert einen Wert für die Zugriffsschlüssel-Rotation (Standardkonfiguration: 90). Der tatsächliche Wert muss den Richtlini

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			en Ihrer Organisation entsprechen.
(CE-1) Automatisierte Systemkontenverwaltung	Unterstützen Sie die Verwaltung von Systemkonten mithilfe automatisierter Mechanismen.	secretsmanager-scheduled-rotation-success-überprüfen	Diese Regel stellt sicher, dass AWS Secrets Manager Manager-Geheimnisse gemäß dem Rotationsplan erfolgreich rotiert wurden. Die regelmäßige Rotation von Secrets kann den Zeitraum verkürzen, in dem ein Secret aktiv ist, und möglicherweise die Auswirkungen auf das Unternehmen verringern, falls es kompromittiert wird.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
(CE-3): Konten deaktivieren	Deaktivieren Sie Konten innerhalb von 120 Tagen, wenn die Konten: a. abgelaufen sind; b. keinen Benutzern oder Einzelpersonen mehr zugeordnet sind; c. gegen die Richtlinien der Organisation verstoßen; oder d. bei nicht privilegierten Konten 120 Tage und bei privilegierten Konten 60 Tage inaktiv waren.	iam-user-unused-credentials-überprüfen	AWS Identity and Access Management (IAM) kann Ihnen bei Zugriffsberechtigungen und Autorisierungen helfen, indem es nach IAM-Passwörtern und Zugriffsschlüsseln sucht, die für einen bestimmten Zeitraum nicht verwendet wurden. Wenn ungenutzte Anmeldeinformationen identifiziert werden, müssen Sie sie deaktivieren und/oder entfernen, da dies gegen das Prinzip der geringsten Berechtigung verstoßen könnte. Für diese Regel müssen Sie einen Wert für das maxCredentialUsage Alter festlegen (Standardkonfiguration: 90). Der tatsächliche Wert muss den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
(CE-12) Kontoüber wachung auf untypische Nutzung	Überwachen Sie Systemkonten auf von der Behörde definiert e untypische Nutzung und melden Sie die untypische Nutzung von Systemkonten an von der Behörde ernannte Mitarbeiter oder definierte Rollen.	guardduty-enabled-centralized	Amazon GuardDuty kann mithilfe von Threat Intellige nce Feeds helfen, potenzielle Cybersich erheitsereignisse zu überwachen und zu erkennen. Dazu gehören Listen mit bösartigen IPs und maschinel len Lernmethoden zur Identifizierung unerwarteter, nicht autorisierter und bösartiger Aktivitäten in Ihrer AWS Cloud-Umgebung.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-6 Geringste Berechtigung	Wenden Sie das Prinzip der geringsten Berechtigung an und erlauben Sie Benutzern (oder Prozessen, die im Namen von Benutzern handeln) nur dann den Zugriff, wenn dies für die Ausführung zugewiesener Aufgaben durch die Organisation notwendig ist.	iam-customer-policy-blocked-kms-Aktionen	AWS Identity and Access Management (IAM) kann Ihnen helfen, die Prinzipien der geringsten Rechte und der Aufgabentrennung in Zugriffsberechtigungen und Autorisierungen zu integrieren und so zu verhindern, dass Richtlinien blockierte Aktionen für alle AWS Schlüssel des Key Management Service enthalten. Wenn Benutzer mehr Rechte haben, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und Aufgabentrennung verstoßen. Mit dieser Regel können Sie den Parameter festlegen. blockedActionsPatterns (Wert „AWS Bewährte grundlegende Sicherheitsmethoden“: kms:

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			Decrypt, kms:ReEncryptFrom). Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-6 Geringste Berechtigung	Wenden Sie das Prinzip der geringsten Berechtigung an und erlauben Sie Benutzern (oder Prozessen, die im Namen von Benutzern handeln) nur dann den Zugriff, wenn dies für die Ausführung zugewiesener Aufgaben durch die Organisation notwendig ist.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) kann Ihnen dabei helfen, die Prinzipien der geringsten Rechte und der Aufgabentrennung in Zugriffsberechtigungen und Autorisierungen zu integrieren und so zu verhindern, dass Richtlinien „Effect“: „Allow“ mit „Action“: „*“ anstelle von „Resource“: „*“ enthalten. Wenn Benutzern mehr Rechte eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und der Aufgabentrennung verstoßen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-6 Geringste Berechtigung	Wenden Sie das Prinzip der geringsten Berechtigung an und erlauben Sie Benutzern (oder Prozessen, die im Namen von Benutzern handeln) nur dann den Zugriff, wenn dies für die Ausführung zugewiesener Aufgaben durch die Organisation notwendig ist.	iam-policy-no-statements-with-full-access	Stellen Sie sicher, dass IAM-Aktionen nur auf die benötigten Aktionen beschränkt sind. Wenn Benutzern mehr Rechte eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und der Aufgabentrennung verstoßen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-6 Geringste Berechtigung	Wenden Sie das Prinzip der geringsten Berechtigung an und erlauben Sie Benutzern (oder Prozessen, die im Namen von Benutzern handeln) nur dann den Zugriff, wenn dies für die Ausführung zugewiesener Aufgaben durch die Organisation notwendig ist.	iam-user-unused-credentials-überprüfen	AWS Identity and Access Management (IAM) kann Ihnen bei Zugriffsberechtigungen und Autorisierungen helfen, indem es nach IAM-Passwörtern und Zugriffsschlüsseln sucht, die für einen bestimmten Zeitraum nicht verwendet wurden. Wenn ungenutzte Anmeldeinformationen identifiziert werden, müssen Sie sie deaktivieren und/oder entfernen, da dies gegen das Prinzip der geringsten Berechtigung verstoßen könnte. Für diese Regel müssen Sie einen Wert für das maxCredentialUsage Alter festlegen (Standardkonfiguration: 90). Der tatsächliche Wert muss den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-6 Geringste Berechtigung	Wenden Sie das Prinzip der geringsten Berechtigung an und erlauben Sie Benutzern (oder Prozessen, die im Namen von Benutzern handeln) nur dann den Zugriff, wenn dies für die Ausführung zugewiesener Aufgaben durch die Organisation notwendig ist.	opensearch-access-control-enabled	Stellen Sie sicher, dass eine differenzierte Zugriffskontrolle für Ihre Amazon OpenSearch Service-Domains aktiviert ist. Eine differenzierte Zugriffskontrolle bietet erweiterte Autorisierungsmechanismen, um den Zugriff auf Amazon Service-Domains mit den geringsten Rechten zu erreichen. OpenSearch Es ermöglicht eine rollenbasierte Zugriffskontrolle auf die Domain sowie Sicherheit auf Index-, Dokument- und Feldebene, Unterstützung für OpenSearch Service-Dashboards, Mehrmandantenfähigkeit und HTTP-Basisauthentifizierung für Service und Kibana. OpenSearch

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-6 Geringste Berechtigung	Wenden Sie das Prinzip der geringsten Berechtigung an und erlauben Sie Benutzern (oder Prozessen, die im Namen von Benutzern handeln) nur dann den Zugriff, wenn dies für die Ausführung zugewiesener Aufgaben durch die Organisation notwendig ist.	secretsmanager-secret-unused	Wenn in AWS Secrets Manager unbenutzte Anmeldeinformationen vorhanden sind, sollten Sie die Anmeldeinformationen deaktivieren und/oder entfernen, da dies gegen das Prinzip der geringsten Rechte verstoßen kann. Mit dieser Regel können Sie einen Wert auf unusedForDays (Config Default: 90) setzen. Der tatsächliche Wert muss den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-6 Geringste Berechtigung	Wenden Sie das Prinzip der geringsten Berechtigung an und erlauben Sie Benutzern (oder Prozessen, die im Namen von Benutzern handeln) nur dann den Zugriff, wenn dies für die Ausführung zugewiesener Aufgaben durch die Organisation notwendig ist.	codebuild-project-environment-privileged-überprüfen	Um Sie bei der Implementierung des Prinzips der geringsten Rechte zu unterstützen, stellen Sie sicher, dass in Ihrer CodeBuild Amazon-Projektumgebung der privilegierte Modus nicht aktiviert ist. Diese Einstellung sollte deaktiviert werden, um unbeabsichtigten Zugriff auf Docker APIs sowie auf die dem Container zugrunde liegende Hardware zu verhindern.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-6 Geringste Berechtigung	Wenden Sie das Prinzip der geringsten Berechtigung an und erlauben Sie Benutzern (oder Prozessen, die im Namen von Benutzern handeln) nur dann den Zugriff, wenn dies für die Ausführung zugewiesener Aufgaben durch die Organisation notwendig ist.	ec2- instance-profile-attached	EC2 Instanzprofile übergeben eine IAM-Rolle an eine Instanz EC2 . Das Anhängen eines Instance-Profils an Ihre Instances kann bei der Implementierung von geringsten Berechtigungen und der Berechtigungsverwaltung helfen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-6 Geringste Berechtigung	Wenden Sie das Prinzip der geringsten Berechtigung an und erlauben Sie Benutzern (oder Prozessen, die im Namen von Benutzern handeln) nur dann den Zugriff, wenn dies für die Ausführung zugewiesener Aufgaben durch die Organisation notwendig ist.	ecs-containers-nonprivileged	Um die Implementierung des Prinzips der geringsten Berechtigung zu unterstützen, dürfen in Amazon Elastic Container Service (Amazon ECS)-Aufgabendefinitionen keine erhöhten Berechtigungen aktiviert sein. Wenn dieser Parameter den Wert „true“ aufweist, erhält der Container erhöhte Berechtigungen auf der Host-Container-Instance (ähnlich wie der Root-Benutzer).

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-6 Geringste Berechtigung	Wenden Sie das Prinzip der geringsten Berechtigung an und erlauben Sie Benutzern (oder Prozessen, die im Namen von Benutzern handeln) nur dann den Zugriff, wenn dies für die Ausführung zugewiesener Aufgaben durch die Organisation notwendig ist.	ecs-containers-readonly-access	Die Aktivierung des schreibgeschützten Zugriffs auf Amazon Elastic Container Service (ECS)-Container kann dazu beitragen, das Prinzip der geringsten Berechtigung einzuhalten. Diese Option kann Angriffsvektoren reduzieren, da das Dateisystem der Container-Instance nur geändert werden kann, wenn es über ausdrückliche Lese- und Schreibberechtigungen verfügt.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-6 Geringste Berechtigung	Wenden Sie das Prinzip der geringsten Berechtigung an und erlauben Sie Benutzern (oder Prozessen, die im Namen von Benutzern handeln) nur dann den Zugriff, wenn dies für die Ausführung zugewiesener Aufgaben durch die Organisation notwendig ist.	ecs-task-definition-nonroot-Benutzer	Sie bestimmen einen Nicht-Root-Benutzer für den Zugriff auf Ihre Aufgabendefinitionen des Amazon Elastic Container Service (Amazon ECS), um die Implementierung des Prinzips der geringsten Berechtigung zu unterstützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-6 Geringste Berechtigung	Wenden Sie das Prinzip der geringsten Berechtigung an und erlauben Sie Benutzern (oder Prozessen, die im Namen von Benutzern handeln) nur dann den Zugriff, wenn dies für die Ausführung zugewiesener Aufgaben durch die Organisation notwendig ist.	efs-access-point-enforce-Benutzeridentität	Um die Implementierung des Prinzips der geringsten Rechte zu unterstützen, stellen Sie sicher, dass die Benutzerdurchsetzung für Ihr Amazon Elastic File System (Amazon EFS) aktiviert ist. Wenn diese Option aktiviert ist, ersetzt Amazon EFS den Benutzer und die Gruppe IDs des NFS-Clients durch die Identität, die auf dem Access Point für alle Dateisystemoperationen konfiguriert ist, und gewährt nur Zugriff auf diese erzwungene Benutzeridentität.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-6 Geringste Berechtigung	Wenden Sie das Prinzip der geringsten Berechtigung an und erlauben Sie Benutzern (oder Prozessen, die im Namen von Benutzern handeln) nur dann den Zugriff, wenn dies für die Ausführung zugewiesener Aufgaben durch die Organisation notwendig ist.	emr-kerberos-enabled	Die Zugriffsberechtigungen und -autorisierungen können verwaltet und nach den Prinzipien der geringsten Berechtigung und Aufgabentrennung integriert werden, indem Kerberos für Amazon-EMR-Cluster aktiviert wird. In Kerberos werden Services und Benutzer, die sich authentifizieren müssen, als Prinzipale bezeichnet. Prinzipale befinden sich in einem Kerberos-Bereich. Innerhalb dieses Bereichs wird ein Kerberos-Server als Key Distribution Center (KDC) bezeichnet. Über diesen Server können sich Prinzipale authentifizieren. Die Authentifizierung im KDC erfolgt durch die Ausstellung von Authentif

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			izierungstickets. Das KDC unterhält eine Datenbank der Prinzipale in seinem Bereich mit ihren Passwörtern und anderen administr ativen Informationen zu jedem Prinzipal.
AC-6 Geringste Berechtigung	Wenden Sie das Prinzip der geringste n Berechtigung an und erlauben Sie Benutzern (oder Prozessen, die im Namen von Benutzern handeln) nur dann den Zugriff, wenn dies für die Ausführun g zugewiesener Aufgaben durch die Organisation notwendig ist.	iam-user-no-policies-überprüfen	Diese Regel stellt sicher, dass AWS Identity and Access Management (IAM) -Richtlinien nur Gruppen oder Rollen zugewiese n werden, um den Zugriff auf Systeme und Ressourcen zu kontrollieren. Die Zuweisung von Berechtig ungen auf Gruppen- oder Rollenebene trägt dazu bei, die Wahrscheinlichkeit zu verringern, dass eine Identität übermäßige Berechtigungen erhält oder beibehält.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-17: Remote-Zugriff	Definieren und dokumentieren Sie Nutzungsbeschränkungen, Konfigurations-/Verbindungsanforderungen und Implementierungsrichtlinien für jeden erlaubten Remote-Zugriffstyp. Autorisieren Sie jede Art von Remote-Zugriff auf das System, bevor Sie solche Verbindungen zulassen.	iam-password-policy	Die Identitäten und Anmeldeinformationen werden auf der Grundlage einer organisatorischen IAM-Passwortrichtlinie ausgestellt, verwaltet und verifiziert. Sie erfüllen oder übertreffen die Anforderungen von NIST SP 800-63 und dem Standard „Best Practices“ von AWS Foundational Security in Bezug auf die Passwortstärke. Mit dieser Regel können Sie optional RequireUppercaseCharacters (Wert für AWS grundlegende Sicherheitsbewährte Methoden: wahr), RequireLowercaseCharacters (Wert für bewährte Methoden für AWS grundlegende Sicherheit: wahr), RequireSymbols (Wert für bewährte Methoden für AWS grundlegende Sicherheit:

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			wahr), RequireNumbers (Wert für bewährte Methoden für AWS grundlegende Sicherheit: wahr), MinimumPasswordLength (Wert für bewährte Methoden für AWS grundlegende Sicherheit: 14), PasswordReusePrevention (Wert für bewährte Methoden für AWS grundlegende Sicherheit: 24) und MaxPasswordAge (Wert für bewährte Methoden für AWS grundlegende Sicherheit: 90) für Ihr IAM festlegen Kennwortrichtlinie. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-17: Remote-Zugriff	Definieren und dokumentieren Sie Nutzungsbeschränkungen, Konfigurations-/Verbindungsanforderungen und Implementierungsrichtlinien für jeden erlaubten Remote-Zugriffstyp. Autorisieren Sie jede Art von Remote-Zugriff auf das System, bevor Sie solche Verbindungen zulassen.	iam-user-mfa-enabled	Aktivieren Sie diese Regel, um den Zugriff auf Ressourcen in der AWS Cloud einzuschränken. Diese Regel sorgt dafür, dass die Multi-Faktor-Authentifizierung (MFA) für alle Benutzer aktiviert ist. MFA sorgt für eine weitere Schutzebene zusätzlich zu den Anmeldeinformationen. Reduzieren Sie Fälle von kompromittierten Konten, indem Sie MFA für Benutzer vorschreiben.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-17: Remote-Zugriff	Definieren und dokumentieren Sie Nutzungsbeschränkungen, Konfigurations-/Verbindungsanforderungen und Implementierungsrichtlinien für jeden erlaubten Remote-Zugriffstyp. Autorisieren Sie jede Art von Remote-Zugriff auf das System, bevor Sie solche Verbindungen zulassen.	mfa-enabled-for-iam-Konsolenzugriff	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass MFA für alle AWS Identity and Access Management (IAM) -Benutzer aktiviert ist, die über ein Konsolenkennwort verfügen. MFA sorgt für eine weitere Schutzebene zusätzlich zu den Anmeldeinformationen. Indem Sie MFA für Benutzer vorschreiben, können Sie Fälle kompromittierter Konten reduzieren und verhindern, dass unbefugte Benutzer auf vertrauliche Daten zugreifen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-17: Remote-Zugriff	Definieren und dokumentieren Sie Nutzungsbeschränkungen, Konfigurations-/Verbindungsanforderungen und Implementierungsrichtlinien für jeden erlaubten Remote-Zugriffstyp. Autorisieren Sie jede Art von Remote-Zugriff auf das System, bevor Sie solche Verbindungen zulassen.	root-account-hardware-mfa-aktiviert	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Hardware-MFA für den Root-Benutzer aktiviert ist. Der Stammbenutzer ist der AWS-Konto-Benutzer mit den meisten Berechtigungen. MFA sorgt für eine weitere Schutzebene zusätzlich zu den Anmeldeinformationen. Indem Sie MFA für den Root-Benutzer vorschreiben, können Sie die Anzahl AWS-Konten kompromittierter Benutzer reduzieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-17: Remote-Zugriff	Definieren und dokumentieren Sie Nutzungsbeschränkungen, Konfigurations-/Verbindungsanforderungen und Implementierungsrichtlinien für jeden erlaubten Remote-Zugriffstyp. Autorisieren Sie jede Art von Remote-Zugriff auf das System, bevor Sie solche Verbindungen zulassen.	root-account-mfa-enabled	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass MFA für den Root-Benutzer aktiviert ist. Der Stammbenutzer ist der AWS-Konto-Benutzer mit den meisten Berechtigungen. MFA sorgt für eine weitere Schutzebene zusätzlich zu den Anmeldeinformationen. Indem Sie MFA für den Root-Benutzer vorschreiben, können Sie die Anzahl AWS-Konten kompromittierter Benutzer reduzieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-17: Remote-Zugriff	Definieren und dokumentieren Sie Nutzungsbeschränkungen, Konfigurations-/Verbindungsanforderungen und Implementierungsrichtlinien für jeden erlaubten Remote-Zugriffstyp. Autorisieren Sie jede Art von Remote-Zugriff auf das System, bevor Sie solche Verbindungen zulassen.	api-gw-execution-logging-aktiviert	Die API-Gateway-Protokollierung zeigt detaillierte Ansichten der Benutzer, die auf die API zugegriffen haben, und wie diese Benutzer auf die API zugegriffen haben. Diese Einblicke ermöglichen die Transparenz von Benutzeraktivitäten.
AC-17: Remote-Zugriff	Definieren und dokumentieren Sie Nutzungsbeschränkungen, Konfigurations-/Verbindungsanforderungen und Implementierungsrichtlinien für jeden erlaubten Remote-Zugriffstyp. Autorisieren Sie jede Art von Remote-Zugriff auf das System, bevor Sie solche Verbindungen zulassen.	cloud-trail-cloud-watch-logs-aktiviert	Verwenden Sie Amazon CloudWatch , um Protokollereignisaktivitäten zentral zu sammeln und zu verwalten. Die Aufnahme von AWS CloudTrail Daten liefert Einzelheiten zu den API-Aufrufaktivitäten in Ihrem AWS-Konto.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-17: Remote-Zugriff	Definieren und dokumentieren Sie Nutzungsbeschränkungen, Konfigurations-/Verbindungsanforderungen und Implementierungsrichtlinien für jeden erlaubten Remote-Zugriffstyp. Autorisieren Sie jede Art von Remote-Zugriff auf das System, bevor Sie solche Verbindungen zulassen.	elasticsearch-logs-to-cloudwatch	Stellen Sie sicher, dass für Amazon OpenSearch Service-Domains Fehlerprotokolle aktiviert und zur Aufbewahrung und Beantwortung an Amazon CloudWatch Logs gestreamt werden. Domain-Fehlerprotokolle sind bei Sicherheits- und Zugriffsprüfungen sowie bei der Diagnose von Verfügbarkeitsproblemen nützlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-17: Remote-Zugriff	Definieren und dokumentieren Sie Nutzungsbeschränkungen, Konfigurations-/Verbindungsanforderungen und Implementierungsrichtlinien für jeden erlaubten Remote-Zugriffstyp. Autorisieren Sie jede Art von Remote-Zugriff auf das System, bevor Sie solche Verbindungen zulassen.	cloudtrail-enabled	AWS CloudTrail kann durch die Aufzeichnung von Aktionen und API-Aufrufen in der AWS Management Console bei der Nichtabstreitbarkeit helfen. Sie können die Benutzer und die Benutzer AWS-Konten , die einen AWS Dienst aufgerufen haben, die Quell-IP-Adresse, über die die Aufrufe generiert wurden, und den Zeitpunkt der Anrufe identifizieren. Einzelheiten zu den erfassten Daten finden Sie in den AWS CloudTrail Datensatzinhalten.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-17: Remote-Zugriff	Definieren und dokumentieren Sie Nutzungsbeschränkungen, Konfigurations-/Verbindungsanforderungen und Implementierungsrichtlinien für jeden erlaubten Remote-Zugriffstyp. Autorisieren Sie jede Art von Remote-Zugriff auf das System, bevor Sie solche Verbindungen zulassen.	opensearch-logs-to-cloudwatch	Stellen Sie sicher, dass für Amazon OpenSearch Service-Domains Fehlerprotokolle aktiviert und zur Aufbewahrung und Beantwortung an Amazon CloudWatch Logs gestreamt werden. OpenSearch Service-Fehlerprotokolle können bei Sicherheits- und Zugriffsprüfungen helfen und bei der Diagnose von Verfügbarkeitsproblemen helfen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-17: Remote-Zugriff	Definieren und dokumentieren Sie Nutzungsbeschränkungen, Konfigurations-/Verbindungsanforderungen und Implementierungsrichtlinien für jeden erlaubten Remote-Zugriffstyp. Autorisieren Sie jede Art von Remote-Zugriff auf das System, bevor Sie solche Verbindungen zulassen.	elb-logging-enabled	Die Elastic-Load-Balancing-Aktivität ist ein zentraler Kommunikationspunkt innerhalb einer Umgebung. Stellen Sie sicher, dass die ELB-Protokollierung aktiviert ist. Die gesammelten Daten enthalten detaillierte Informationen zu Anfragen, die an den ELB gesendet wurden. Jedes Protokoll enthält Informationen wie die Zeit, zu der die Anforderung einging, die Client-IP-Adresse, Latenzen, Anforderungspfade und Serverantworten.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-17: Remote-Zugriff	Definieren und dokumentieren Sie Nutzungsbeschränkungen, Konfigurations-/Verbindungsanforderungen und Implementierungsrichtlinien für jeden erlaubten Remote-Zugriffstyp. Autorisieren Sie jede Art von Remote-Zugriff auf das System, bevor Sie solche Verbindungen zulassen.	rds-logging-enabled	Um die Protokollierung und Überwachung in Ihrer Umgebung zu erleichtern, stellen Sie sicher, dass die Amazon Relational Database Service (Amazon RDS)-Protokollierung aktiviert ist. Mit der Amazon-RDS-Protokollierung können Sie Ereignisse wie Verbindungen, Verbindungsabbrüche, Abfragen oder abgefragte Tabellen erfassen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-17: Remote-Zugriff	Definieren und dokumentieren Sie Nutzungsbeschränkungen, Konfigurations-/Verbindungsanforderungen und Implementierungsrichtlinien für jeden erlaubten Remote-Zugriffstyp. Autorisieren Sie jede Art von Remote-Zugriff auf das System, bevor Sie solche Verbindungen zulassen.	s-3 bucket-logging-enabled	Die Amazon Simple Storage Service (Amazon S3)-Serverzugriffsprotokollierung bietet eine Methode zur Überwachung des Netzwerks im Hinblick auf potenzielle Cybersicherheitsereignisse. Die Ereignisse werden überwacht, indem detaillierte Aufzeichnungen über die Anfragen erfasst werden, die an einen Amazon-S3-Bucket gestellt wurden. Jeder Zugriffsprotokolleintrag enthält Details zu einer einzelnen Zugriffsanfrage. Zu den Details gehören Anforderer, Bucket-Name, Anforderungszeit, Anforderungsaktion, Antwortstatus und Fehlercode, falls relevant.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-17: Remote-Zugriff	Definieren und dokumentieren Sie Nutzungsbeschränkungen, Konfigurations-/Verbindungsanforderungen und Implementierungsrichtlinien für jeden erlaubten Remote-Zugriffstyp. Autorisieren Sie jede Art von Remote-Zugriff auf das System, bevor Sie solche Verbindungen zulassen.	securityhub-enabled	AWS Security Hub hilft bei der Überwachung von unbefugtem Personal, Verbindungen, Geräten und Software. AWS Security Hub aggregiert, organisiert und priorisiert die Sicherheitswarnungen oder Ergebnisse mehrerer Dienste. AWS Einige dieser Dienste sind Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer und AWS Firewall Manager sowie AWS Partnerlösungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-17: Remote-Zugriff	Definieren und dokumentieren Sie Nutzungsbeschränkungen, Konfigurations-/Verbindungsanforderungen und Implementierungsrichtlinien für jeden erlaubten Remote-Zugriffstyp. Autorisieren Sie jede Art von Remote-Zugriff auf das System, bevor Sie solche Verbindungen zulassen.	vpc-flow-logs-enabled	VPC-Flow-Protokolle erfassen detaillierte Informationsdatensätze über den IP-Datenverkehr, der zu und von Netzwerkschnittstellen in Ihrer Amazon Virtual Private Cloud (Amazon VPC) fließt. Standardmäßig enthalten Flow-Protokolldatensätze Werte für die verschiedenen Komponenten des IP-Flows, einschließlich Quelle, Ziel und Protokoll.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-17: Remote-Zugriff	Definieren und dokumentieren Sie Nutzungsbeschränkungen, Konfigurations-/Verbindungsanforderungen und Implementierungsrichtlinien für jeden erlaubten Remote-Zugriffstyp. Autorisieren Sie jede Art von Remote-Zugriff auf das System, bevor Sie solche Verbindungen zulassen.	wafv2-logging-enabled	Um Ihnen bei der Protokollierung und Überwachung in Ihrer Umgebung zu helfen, aktivieren Sie die AWS WAF (V2) -Protokollierung im regionalen und globalen Web. ACLs AWS Die WAF-Protokollierung bietet detaillierte Informationen über den Datenverkehr, der von Ihrer Web-ACL analysiert wird. In den Protokollen werden die Uhrzeit aufgezeichnet, zu der die AWS WAF die Anfrage von Ihrer AWS Ressource erhalten hat, Informationen über die Anfrage und eine Aktion für die Regel, der jede Anfrage entsprach.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-17: Remote-Zugriff	Definieren und dokumentieren Sie Nutzungsbeschränkungen, Konfigurations-/Verbindungsanforderungen und Implementierungsrichtlinien für jeden erlaubten Remote-Zugriffstyp. Autorisieren Sie jede Art von Remote-Zugriff auf das System, bevor Sie solche Verbindungen zulassen.	cloudwatch-alarm-action-check	Amazon CloudWatch alarmiert, wenn eine Metrik den Schwellenwert für eine bestimmte Anzahl von Bewertungszeiträumen überschreitet. Der Alarm führt eine oder mehrere Aktionen durch, die vom Wert der Metrik oder des Ausdrucks im Vergleich zu einem Schwellenwert in einer Reihe von Zeiträumen abhängt. Diese Regel erfordert einen Wert für alarmActionRequired (Config Default: True), insufficientDataAction Required (Config Default: True), okActionRequired (Config Default: False). Der tatsächliche Wert muss die Alarmaktionen für Ihre Umgebung widerspiegeln.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-17: Remote-Zugriff	Definieren und dokumentieren Sie Nutzungsbeschränkungen, Konfigurations-/Verbindungsanforderungen und Implementierungsrichtlinien für jeden erlaubten Remote-Zugriffstyp. Autorisieren Sie jede Art von Remote-Zugriff auf das System, bevor Sie solche Verbindungen zulassen.	redshift-cluster-configuration-check	Um Daten im Ruhezustand zu schützen, muss die Verschlüsselung für Ihre Amazon-Redshift-Cluster aktiviert sein. Sie müssen auch sicherstellen, dass die erforderlichen Konfigurationen auf Amazon-Redshift-Clustern bereitgestellt werden. Die Prüfungsprotokollierung muss aktiviert sein, um Informationen zu Verbindungen und Benutzeraktivitäten in der Datenbank bereitzustellen. Diese Regel erfordert, dass ein Wert für clusterDbEncrypted (Config Default: TRUE) und LoggingEnabled (Config Default: TRUE) gesetzt ist. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-17: Remote-Zugriff	Definieren und dokumentieren Sie Nutzungsbeschränkungen, Konfigurations-/Verbindungsanforderungen und Implementierungsrichtlinien für jeden erlaubten Remote-Zugriffstyp. Autorisieren Sie jede Art von Remote-Zugriff auf das System, bevor Sie solche Verbindungen zulassen.	redshift-enhanced-vpc-routing-aktiviert	Mit Enhanced-VPC-Routing wird erzwungen, dass der gesamte COPY- und UNLOAD-Datenverkehr zwischen Ihrem Cluster und Datenrepositorys über Ihre Amazon VPC erfolgt. Anschließend können Sie VPC-Features wie Sicherheitsgruppen und Netzwerkzugriffskontrolllisten verwenden, um den Netzwerkverkehr zu schützen. Sie können auch VPC-Flow-Protokolle verwenden, um den Netzwerkverkehr zu überwachen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AT-1: Sensibilisierung und Schulung	Bieten Sie Systembenutzern (einschließlich Managern, Führungskräften und Auftragnehmern) Schulungen zum Thema Sicherheit und Datenschutz an.	security-awareness-program-exists(Prozessüberprüfung)	Etablieren und pflegen Sie ein Programm zur Förderung des Sicherheitsbewusstseins in Ihrer Organisation. Programme zur Förderung des Sicherheitsbewusstseins der Mitarbeiter vermitteln ihnen, wie sie ihre Organisation vor diversen Sicherheitsverletzungen oder Sicherheitsvorfällen schützen können.
AU-2: Prüfungsereignisse	Identifizieren Sie die Arten von Ereignissen, die das System zur Unterstützung der Prüfungsfunktion protokollieren kann.	audit-log-policy-exists(Prozessüberprüfung)	Richten Sie eine Richtlinie zur Verwaltung von Prüfprotokollen ein, in der die Protokollierungsanforderungen Ihres Unternehmens definiert sind, und pflegen Sie diese Richtlinie. Dies beinhaltet, ist aber nicht beschränkt auf die Überprüfung und Aufbewahrung von Prüfprotokollen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AU-16: Organisationsübergreifende Protokollierung von Prüfungen	Wenden Sie behördlich definierte Methoden zur Koordinierung behördlich definierter Prüfungsinformationen zwischen externen Organisationen an, wenn Prüfungsinformationen außerhalb der Organisation übertragen werden.	audit-log-policy-exists(Prozessüberprüfung)	Richten Sie eine Richtlinie zur Verwaltung von Prüfprotokollen ein, in der die Protokollierungsanforderungen Ihres Unternehmens definiert sind, und pflegen Sie diese Richtlinie. Dies beinhaltet, ist aber nicht beschränkt auf die Überprüfung und Aufbewahrung von Prüfprotokollen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CA-7: Kontinuierliche Überwachung	Entwickeln Sie eine Strategie zur kontinuierlichen Überwachung auf Systemebene und Umsetzung einer kontinuierlichen Überwachung gemäß der Strategie zur kontinuierlichen Überwachung auf Organisationsebene: Bestimmen Sie behördlich definierte Kennzahlen, die überwacht werden sollen; Laufende Kontrollbewertungen gemäß der Strategie zur kontinuierlichen Überwachung; Kontinuierliche Überwachung der system- und organisationseitig definierten Kennzahlen gemäß der Strategie zur kontinuierlichen Überwachung; Korrelation und Analyse der durch Kontrollbewertungen und Überwachung generierten Informati	securityhub-enabled	AWS Security Hub hilft bei der Überwachung von unbefugtem Personal, Verbindungen, Geräten und Software. AWS Security Hub aggregiert, organisiert und priorisiert die Sicherheitswarnungen oder Ergebnisse mehrerer Dienste. AWS Einige dieser Dienste sind Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer und AWS Firewall Manager sowie AWS Partnerlösungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	onen; Reaktions maßnahmen zur Bearbeitung der Ergebnisse der Kontrollanalyse; Bewertung und Überwachung von Informationen und mindestens jährliche Berichterstattung über den Sicherheits- und Datenschutzstatus des Systems an von der Behörde ernannte Mitarbeiter.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CP-9: Systemsicherung	a. Führen Sie wöchentlich Backups von Informationen auf Benutzerebene durch, die in der Systemdokumentation enthalten sind, einschließlich sicherheitsrelevanter Dokumente; b. Führen Sie wöchentlich Backups von Informationen auf Systemebene durch; c. Führen Sie wöchentlich Backups der Systemdokumentation durch, einschließlich sicherheits- und datenschutzrelevanter Unterlagen; und d. Schützen Sie die Vertraulichkeit, Integrität und Verfügbarkeit von Backup-Informationen.	aurora-resources-protected-by-Backup-Plan	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon Aurora Aurora-Ressourcen Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CP-9: Systemsicherung	a. Führen Sie wöchentlich Backups von Informationen auf Benutzerebene durch, die in der Systemdokumentation enthalten sind, einschließlich sicherheitsrelevanter Dokumente; b. Führen Sie wöchentlich Backups von Informationen auf Systemebene durch; c. Führen Sie wöchentlich Backups der Systemdokumentation durch, einschließlich sicherheits- und datenschutzrelevanter Unterlagen; und d. Schützen Sie die Vertraulichkeit, Integrität und Verfügbarkeit von Backup-Informationen.	backup-plan-min-frequency-and-min-retention-check	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihr AWS Backup-Plan auf eine Mindestfrequenz und Aufbewahrung festgelegt ist. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen. Mit dieser Regel können Sie die Parameter requiredFrequencyValue (Config default: 1), requiredRetentionDays (Config default: 35) und requiredFrequencyUnit

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			(Config default: days) festlegen. Der tatsächliche Wert muss den Anforderungen Ihrer Organisation entsprechen.
CP-9: Systemsicherung	a. Führen Sie wöchentlich Backups von Informationen auf Benutzerebene durch, die in der Systemdokumentation enthalten sind, einschließlich sicherheitsrelevanter Dokumente; b. Führen Sie wöchentlich Backups von Informationen auf Systemebene durch; c. Führen Sie wöchentlich Backups der Systemdokumentation durch, einschließlich sicherheits- und datenschutzrelevanter Unterlagen; und d. Schützen Sie die Vertraulichkeit, Integrität und Verfügbarkeit von Backup-Informationen.	backup-recovery-point-encrypted	Stellen Sie sicher, dass die Verschlüsselung für Ihre AWS Backup-Wiederherstellungspunkte aktiviert ist. Da sensible Daten auch im Ruhezustand vorhanden sein können, sollten Sie die Verschlüsselung im Ruhezustand aktivieren, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CP-9: Systemsicherung	a. Führen Sie wöchentlich Backups von Informationen auf Benutzerebene durch, die in der Systemdokumentation enthalten sind, einschließlich sicherheitsrelevanter Dokumente; b. Führen Sie wöchentlich Backups von Informationen auf Systemebene durch; c. Führen Sie wöchentlich Backups der Systemdokumentation durch, einschließlich sicherheits- und datenschutzrelevanter Unterlagen; und d. Schützen Sie die Vertraulichkeit, Integrität und Verfügbarkeit von Backup-Informationen.	backup-recovery-point-manual-Löschen-deaktiviert	Stellen Sie sicher, dass Ihren AWS Backup-Wiederherstellungspunkten eine ressourcenbasierte Richtlinie zugeordnet ist, die das Löschen von Wiederherstellungspunkten verhindert. Die Verwendung einer ressourcenbasierten Richtlinie zur Verhinderung des Löschens von Wiederherstellungspunkten kann dazu beitragen, ein versehentliches oder absichtliches Löschen zu unterbinden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CP-9: Systemsicherung	a. Führen Sie wöchentlich Backups von Informationen auf Benutzerebene durch, die in der Systemdokumentation enthalten sind, einschließlich sicherheitsrelevanter Dokumente; b. Führen Sie wöchentlich Backups von Informationen auf Systemebene durch; c. Führen Sie wöchentlich Backups der Systemdokumentation durch, einschließlich sicherheits- und datenschutzrelevanter Unterlagen; und d. Schützen Sie die Vertraulichkeit, Integrität und Verfügbarkeit von Backup-Informationen.	backup-recovery-point-minimum-Aufbewahrungsprüfung	Um bei Datensicherungsprozessen zu helfen, stellen Sie sicher, dass für Ihre AWS Backup-Wiederherstellungspunkte eine Mindestaufbewahrungsdauer festgelegt ist. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen. Mit dieser Regel können Sie den Parameter requiredRetentionDays (Config Default: 35) festlegen. Der tatsächliche Wert muss den Anforderu

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			ngen Ihrer Organisation entsprechen.
CP-9: Systemsicherung	a. Führen Sie wöchentlich Backups von Informationen auf Benutzerebene durch, die in der Systemdokumentation enthalten sind, einschließlich sicherheitsrelevanter Dokumente; b. Führen Sie wöchentlich Backups von Informationen auf Systemebene durch; c. Führen Sie wöchentlich Backups der Systemdokumentation durch, einschließlich sicherheits- und datenschutzrelevanter Unterlagen; und d. Schützen Sie die Vertraulichkeit, Integrität und Verfügbarkeit von Backup-Informationen.	db-instance-backup-enabled	Die Sicherungsfunktion von Amazon RDS erstellt Sicherungen Ihrer Datenbanken und Transaktionsprotokolle. Amazon RDS erstellt einen Snapshot für das Speichervolume Ihrer DB-Instance, sodass die gesamte DB-Instance gesichert wird. Sie können im System spezifische Aufbewahrungsfristen festlegen, um Ihre Ausfallsicherheitsanforderungen zu erfüllen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CP-9: Systemsicherung	a. Führen Sie wöchentlich Backups von Informationen auf Benutzerebene durch, die in der Systemdokumentation enthalten sind, einschließlich sicherheitsrelevanter Dokumente; b. Führen Sie wöchentlich Backups von Informationen auf Systemebene durch; c. Führen Sie wöchentlich Backups der Systemdokumentation durch, einschließlich sicherheits- und datenschutzrelevanter Unterlagen; und d. Schützen Sie die Vertraulichkeit, Integrität und Verfügbarkeit von Backup-Informationen.	dynamodb-in-backup-plan	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon DynamoDB-Tabellen Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CP-9: Systemsicherung	a. Führen Sie wöchentlich Backups von Informationen auf Benutzerebene durch, die in der Systemdokumentation enthalten sind, einschließlich sicherheitsrelevanter Dokumente; b. Führen Sie wöchentlich Backups von Informationen auf Systemebene durch; c. Führen Sie wöchentlich Backups der Systemdokumentation durch, einschließlich sicherheits- und datenschutzrelevanter Unterlagen; und d. Schützen Sie die Vertraulichkeit, Integrität und Verfügbarkeit von Backup-Informationen.	dynamodb-pitr-enabled	Aktivieren Sie diese Regel, um zu überprüfen, ob die Informationen gesichert wurden. Es verwaltet auch die Backups, indem es sicherstellt, dass die point-in-time Wiederherstellung in Amazon DynamoDB aktiviert ist. Bei der Wiederherstellung werden fortlaufende Backups Ihrer Tabelle für die letzten 35 Tage gespeichert.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CP-9: Systemsicherung	a. Führen Sie wöchentlich Backups von Informationen auf Benutzerebene durch, die in der Systemdokumentation enthalten sind, einschließlich sicherheitsrelevanter Dokumente; b. Führen Sie wöchentlich Backups von Informationen auf Systemebene durch; c. Führen Sie wöchentlich Backups der Systemdokumentation durch, einschließlich sicherheits- und datenschutzrelevanter Unterlagen; und d. Schützen Sie die Vertraulichkeit, Integrität und Verfügbarkeit von Backup-Informationen.	ebs-in-backup-plan	Stellen Sie zur Unterstützung der Datensicherungsprozesse sicher, dass Ihre Amazon Elastic Block Store (Amazon EBS) -Volumes Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CP-9: Systemsicherung	a. Führen Sie wöchentlich Backups von Informationen auf Benutzerebene durch, die in der Systemdokumentation enthalten sind, einschließlich sicherheitsrelevanter Dokumente; b. Führen Sie wöchentlich Backups von Informationen auf Systemebene durch; c. Führen Sie wöchentlich Backups der Systemdokumentation durch, einschließlich sicherheits- und datenschutzrelevanter Unterlagen; und d. Schützen Sie die Vertraulichkeit, Integrität und Verfügbarkeit von Backup-Informationen.	ec2--Plan resources-protected-by-backup	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon Elastic Compute Cloud (Amazon EC2) -Ressourcen Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CP-9: Systemsicherung	a. Führen Sie wöchentlich Backups von Informationen auf Benutzerebene durch, die in der Systemdokumentation enthalten sind, einschließlich sicherheitsrelevanter Dokumente; b. Führen Sie wöchentlich Backups von Informationen auf Systemebene durch; c. Führen Sie wöchentlich Backups der Systemdokumentation durch, einschließlich sicherheits- und datenschutzrelevanter Unterlagen; und d. Schützen Sie die Vertraulichkeit, Integrität und Verfügbarkeit von Backup-Informationen.	efs-in-backup-plan	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon Elastic File System (Amazon EFS) -Dateisysteme Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CP-9: Systemsicherung	a. Führen Sie wöchentlich Backups von Informationen auf Benutzerebene durch, die in der Systemdokumentation enthalten sind, einschließlich sicherheitsrelevanter Dokumente; b. Führen Sie wöchentlich Backups von Informationen auf Systemebene durch; c. Führen Sie wöchentlich Backups der Systemdokumentation durch, einschließlich sicherheits- und datenschutzrelevanter Unterlagen; und d. Schützen Sie die Vertraulichkeit, Integrität und Verfügbarkeit von Backup-Informationen.	elasticache-redis-cluster-automatic-Backup-Check	Wenn automatische Backups aktiviert sind, ElastiCache erstellt Amazon täglich ein Backup des Clusters. Die Sicherung kann für eine von Ihrer Organisation festgelegte Anzahl von Tagen aufbewahrt werden. Automatische Backups schützen vor Datenverlust. Bei einem Ausfall können Sie einen neuen Cluster erstellen, der Ihre Daten aus dem aktuellen Backup wiederherstellt.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CP-9: Systemsicherung	a. Führen Sie wöchentlich Backups von Informationen auf Benutzerebene durch, die in der Systemdokumentation enthalten sind, einschließlich sicherheitsrelevanter Dokumente; b. Führen Sie wöchentlich Backups von Informationen auf Systemebene durch; c. Führen Sie wöchentlich Backups der Systemdokumentation durch, einschließlich sicherheits- und datenschutzrelevanter Unterlagen; und d. Schützen Sie die Vertraulichkeit, Integrität und Verfügbarkeit von Backup-Informationen.	fsx-resources-protected-by-Backup-Plan	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre FSx Amazon-Dateisysteme Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CP-9: Systemsicherung	a. Führen Sie wöchentlich Backups von Informationen auf Benutzerebene durch, die in der Systemdokumentation enthalten sind, einschließlich sicherheitsrelevanter Dokumente; b. Führen Sie wöchentlich Backups von Informationen auf Systemebene durch; c. Führen Sie wöchentlich Backups der Systemdokumentation durch, einschließlich sicherheits- und datenschutzrelevanter Unterlagen; und d. Schützen Sie die Vertraulichkeit, Integrität und Verfügbarkeit von Backup-Informationen.	rds-in-backup-plan	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon Relational Database Service (Amazon RDS) -Instances Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CP-9: Systemsicherung	a. Führen Sie wöchentlich Backups von Informationen auf Benutzerebene durch, die in der Systemdokumentation enthalten sind, einschließlich sicherheitsrelevanter Dokumente; b. Führen Sie wöchentlich Backups von Informationen auf Systemebene durch; c. Führen Sie wöchentlich Backups der Systemdokumentation durch, einschließlich sicherheits- und datenschutzrelevanter Unterlagen; und d. Schützen Sie die Vertraulichkeit, Integrität und Verfügbarkeit von Backup-Informationen.	rds-resources-protected-by-Backup-Plan	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon Relational Database Service (Amazon RDS) -Ressourcen Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CP-9: Systemsicherung	a. Führen Sie wöchentlich Backups von Informationen auf Benutzerebene durch, die in der Systemdokumentation enthalten sind, einschließlich sicherheitsrelevanter Dokumente; b. Führen Sie wöchentlich Backups von Informationen auf Systemebene durch; c. Führen Sie wöchentlich Backups der Systemdokumentation durch, einschließlich sicherheits- und datenschutzrelevanter Unterlagen; und d. Schützen Sie die Vertraulichkeit, Integrität und Verfügbarkeit von Backup-Informationen.	redshift-backup-enabled	Stellen Sie zur Unterstützung der Datensicherungsprozesse sicher, dass Ihre Amazon-Redshift-Cluster über automatisierte Snapshots verfügen. Wenn automatisierte Snapshots für einen Cluster aktiviert sind, erstellt Redshift in regelmäßigen Abständen Snapshots dieses Clusters. Standardmäßig erstellt Redshift alle acht Stunden oder alle 5 GB einen Snapshot für jeden Knoten mit Datenänderungen oder je nachdem, was zuerst eintritt.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CP-9: Systemsicherung	a. Führen Sie wöchentlich Backups von Informationen auf Benutzerebene durch, die in der Systemdokumentation enthalten sind, einschließlich sicherheitsrelevanter Dokumente; b. Führen Sie wöchentlich Backups von Informationen auf Systemebene durch; c. Führen Sie wöchentlich Backups der Systemdokumentation durch, einschließlich sicherheits- und datenschutzrelevanter Unterlagen; und d. Schützen Sie die Vertraulichkeit, Integrität und Verfügbarkeit von Backup-Informationen.	s3- bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) unterstützt die Aufrechterhaltung einer angemessenen Kapazität und Verfügbarkeit. CRR ermöglicht das automatische, asynchrone Kopieren von Objekten in Amazon-S3-Buckets, um die Datenverfügbarkeit sicherzustellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
IA-2: Identifizierung und Authentifizierung (Benutzer der Organisation) (CE-1) | Multi-Faktor-Authentifizierung für privilegierte Konten	Implementieren Sie eine Multi-Faktor-Authentifizierung für den Zugriff auf privilegierte Konten.	root-account-mfa-enabled	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass MFA für den Root-Benutzer aktiviert ist. Der Stammbenutzer ist der AWS-Konto-Benutzer mit den meisten Berechtigungen. MFA sorgt für eine weitere Schutzebene zusätzlich zu den Anmeldeinformationen. Indem Sie MFA für den Root-Benutzer vorschreiben, können Sie die Anzahl AWS-Konten kompromittierter Benutzer reduzieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
IA-2: Identifizierung und Authentifizierung (Benutzer der Organisation) (CE-1) | Multi-Faktor-Authentifizierung für privilegierte Konten	Implementieren Sie eine Multi-Faktor-Authentifizierung für den Zugriff auf privilegierte Konten.	root-account-hardware-mfa-aktiviert	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Hardware-MFA für den Root-Benutzer aktiviert ist. Der Stammbenutzer ist der AWS-Konto-Benutzer mit den meisten Berechtigungen. MFA sorgt für eine weitere Schutzebene zusätzlich zu den Anmeldeinformationen. Indem Sie MFA für den Root-Benutzer vorschreiben, können Sie die Anzahl AWS-Konten kompromittierter Benutzer reduzieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
IA-2: Identifizierung und Authentifizierung (Benutzer der Organisation) (CE-2) Multi-Faktor-Authentifizierung für nicht privilegierte Konten	Implementieren Sie eine Multi-Faktor-Authentifizierung für den Zugriff auf nicht privilegierte Konten.	mfa-enabled-for-iam-Konsolenzugriff	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass MFA für alle AWS Identity and Access Management (IAM) -Benutzer aktiviert ist, die über ein Konsolenkennwort verfügen. MFA sorgt für eine weitere Schutzebene zusätzlich zu den Anmeldeinformationen. Indem Sie MFA für Benutzer vorschreiben, können Sie Fälle kompromittierter Konten reduzieren und verhindern, dass unbefugte Benutzer auf vertrauliche Daten zugreifen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
IA-5: Verwaltung von Authentifikatoren: (CE-1) Passwortbasierte Authentifizierung: Für passwortbasierte Authentifizierung	Setzen Sie die folgenden Regeln hinsichtlich Zusammensetzung und Komplexität durch: 1. Erzwingen Sie eine Mindestpasswortlänge von vierzehn (14) Zeichen. 2. Erzwingen Sie eine Mindestkomplexität von Kennwörtern, damit sie eine Kombination aus Zahlen, Großbuchstaben, Kleinbuchstaben und Sonderzeichen enthalten. 3. Erzwingen Sie bei der Auswahl neuer Passwörter, dass mindestens ein (1) Zeichen geändert wird. 4. Speichern und übertragen Sie nur kryptografisch geschützte Passwörter. 5. Setzen Sie Einschränkungen für die Gültigkeitsdauer von Passwörtern durch: i. Mindestens ein (1) Tag und	iam-password-policy	Die Identitäten und Anmeldeinformationen werden auf der Grundlage einer organisatorischen IAM-Passwortrichtlinie ausgestellt, verwaltet und verifiziert. Sie erfüllen oder übertreffen die Anforderungen von NIST SP 800-63 und dem Standard „Best Practices“ von AWS Foundational Security für die Passwortstärke. Mit dieser Regel können Sie optional RequireUppercaseCharacters (Wert für AWS grundlegende Sicherheitsbewährte Methoden: wahr), RequireLowercaseCharacters (Wert für bewährte Methoden für AWS grundlegende Sicherheit: wahr), RequireSymbols (Wert für bewährte Methoden für AWS grundlegende Sicherheit:

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	maximal 90 Tage. ii. Passwörter für Servicekonten müssen innerhalb von 366 Tagen (inklusive) ablaufen.		wahr), RequireNumbers (Wert für bewährte Methoden für AWS grundlegende Sicherheit: wahr), MinimumPasswordLength (Wert für bewährte Methoden für AWS grundlegende Sicherheit: 14), PasswordReusePrevention (Wert für bewährte Methoden für AWS grundlegende Sicherheit: 24) und MaxPasswordAge (Wert für bewährte Methoden für AWS grundlegende Sicherheit: 90) für Ihr IAM festlegen Kennwortrichtlinie. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PM-5: Systeminventar	Erstellen und aktualisieren Sie kontinuierlich ein Inventar der Organisationssysteme.	ec2-managerinstance-managed-by-systems	Eine Bestandsaufnahme der Softwareplattformen und Anwendungen innerhalb des Unternehmens ist möglich, indem Amazon Elastic Compute Cloud (Amazon EC2) - Instances mit AWS Systems Manager verwaltet werden. Verwenden Sie AWS Systems Manager, um detaillierte Systemkonfigurationen, Betriebssystem-Patch-Levels, Namen und Typ der Dienste, Softwareinstallationen, Anwendungsname, Herausgeber und Version sowie andere Details zu Ihrer Umgebung bereitzustellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PM-5: Systeminventar	Erstellen und aktualisieren Sie kontinuierlich ein Inventar der Organisationssysteme.	ec2-check managedinstance-association-compliance-status	Verwenden Sie AWS Systems Manager Associations, um bei der Inventarisierung von Softwareplattformen und Anwendungen innerhalb eines Unternehmens zu helfen. AWS Systems Manager weist Ihren verwalteten Instanzen einen Konfigurationsstatus zu und ermöglicht es Ihnen, Basiswerte für Betriebssystem-Patch-Levels, Softwareinstallationen, Anwendungskonfigurationen und andere Details zu Ihrer Umgebung festzulegen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PM-5: Systeminventar	Erstellen und aktualisieren Sie kontinuierlich ein Inventar der Organisationssysteme.	vpc-network-acl-unused-überprüfen	Diese Regel stellt sicher, dass Amazon Virtual Private Cloud (VPC)-Netzwerkzugriffskontrolllisten verwendet werden. Die Überwachung ungenutzter Netzwerkzugriffskontrolllisten kann zu einer genauen Inventarisierung und Verwaltung Ihrer Umgebung beitragen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PM-5: Systeminventar	Erstellen und aktualisieren Sie kontinuierlich ein Inventar der Organisationssysteme.	ec2- volume-inuse-check	Diese Regel stellt sicher, dass Amazon Elastic Block Store-Volumes, die an Amazon Elastic Compute Cloud (Amazon EC2) - Instances angehängt sind, zum Löschen markiert werden, wenn eine Instance beendet wird. Wenn ein Amazon-EBS-Volume nicht gelöscht wird, wenn die Instance, an die es angehängt ist, beendet wird, kann dies gegen das Konzept der geringsten Funktionalität verstoßen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
RA-5: Überwachen und Scannen von Schwachstellen	Führen Sie alle dreißig (30) Tage Überwachungen und Scans auf Schwachstellen im System und in den gehosteten Anwendungen durch, bevor Sie ein neues Informationssystem in das Behördennetzwerk aufnehmen, um die Abhilfemaßnahmen zu verifizieren und wenn neue Sicherheitslücken, identifiziert und gemeldet werden, die möglicherweise das System betreffen.	vuln-scans-performed(Prozessüberprüfung)	Stellen Sie sicher, dass Schwachstellenscans gemäß Ihren Compliance-Anforderungen durchgeführt werden. Die Häufigkeit der Scans, die verwendeten Tools und die Verwendung der Ergebnisse sollten von Ihrer Organisation festgelegt werden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SA-10: Konfigurationsmanagement für Entwickler (e.)	Die Überwachung von Sicherheitslücken und deren Behebung innerhalb des Systems, der Komponente oder des Services und die Meldung der Ergebnisse an [Zuweisung: von der Organisation ernanntes Personal].	guardduty-enabled-centralized	Amazon GuardDuty kann mithilfe von Threat Intelligence Feeds helfen, potenzielle Cybersicherheitsereignisse zu überwachen und zu erkennen. Dazu gehören Listen mit bösartigen IPs und maschinellen Lernmethoden zur Identifizierung unerwarteter, nicht autorisierter und bösartiger Aktivitäten in Ihrer AWS Cloud-Umgebung.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SA-10: Konfigurationsmanagement für Entwickler (e.)	Die Überwachung von Sicherheitslücken und deren Behebung innerhalb des Systems, der Komponente oder des Services und die Meldung der Ergebnisse an [Zuweisung: von der Organisation ernanntes Personal].	guardduty-non-archived-findings	Amazon GuardDuty hilft Ihnen dabei, die Auswirkungen eines Vorfalls zu verstehen, indem es die Ergebnisse nach Schweregrad klassifiziert: niedrig, mittel und hoch. Diese Klassifizierungen können Sie zur Festlegung von entsprechenden Strategien und Prioritäten zur Behebung solcher Vorfälle verwenden. Mit dieser Regel können Sie optional daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7) und daysHighSev (Config Default: 1) für nicht archivierte Ergebnisse festlegen, wie es die Richtlinien Ihrer Organisation erfordern.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SA-10: Konfigurationsmanagement für Entwickler (e.)	Die Überwachung von Sicherheitslücken und deren Behebung innerhalb des Systems, der Komponente oder des Services und die Meldung der Ergebnisse an [Zuweisung: von der Organisation ernanntes Personal].	securityhub-enabled	AWS Security Hub hilft bei der Überwachung von unbefugtem Personal, Verbindungen, Geräten und Software. AWS Security Hub aggregiert, organisiert und priorisiert die Sicherheitswarnungen oder Ergebnisse mehrerer Dienste. AWS Einige dieser Dienste sind Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer und AWS Firewall Manager sowie AWS Partnerlösungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SA-10: Konfigurationsmanagement für Entwickler (a) (c.)	Führen Sie das Konfigurationsmanagement während des Entwurfs, der Entwicklung, der Implementierung und des Betriebs des Systems, der Komponenten oder des Services durch. Implementieren Sie nur von der Organisation genehmigte Änderungen am System, an der Komponente oder am Service;	ec2-manager instance-managed-by-systems	Eine Bestandsaufnahme der Softwareplattformen und Anwendungen innerhalb des Unternehmens ist möglich, indem Amazon Elastic Compute Cloud (Amazon EC2) - Instances mit AWS Systems Manager verwaltet werden. Verwenden Sie AWS Systems Manager, um detaillierte Systemkonfigurationen, Betriebssystem-Patch-Levels, Namen und Typ der Dienste, Softwareinstallationen, Anwendungsname, Herausgeber und Version sowie andere Details zu Ihrer Umgebung bereitzustellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-4: Informati onen in gemeinsam genutzten Systemres sourcen	Verhindern Sie die unbefugte und unbeabsichtigte Übertragung von Informationen aus gemeinsam genutzten Systemressourcen	ec2- volume-inuse-check	Diese Regel stellt sicher, dass Amazon Elastic Block Store-Volumes, die an Amazon Elastic Compute Cloud (Amazon EC2) - Instances angehängt sind, zum Löschen markiert werden, wenn eine Instance beendet wird. Wenn ein Amazon-EB S-Volume nicht gelöscht wird, wenn die Instance, an die es angehängt ist, beendet wird, kann dies gegen das Konzept der geringsten Funktiona lität verstoßen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-7: Grenzschutz	Überwachen und kontrollieren Sie die Kommunikation an der Außengrenze des Systems und an wichtigen internen Grenzen innerhalb des Systems; Implementieren Sie Subnetzwerke für öffentlich zugängliche Systemkomponenten, die von internen Organisationsnetzwerken getrennt sind; und stellen Sie Verbindungen zu externen Netzwerken oder Informationssystemen nur über verwaltete Schnittstellen her, die aus Grenzschutzvorrichtungen gemäß einer Sicherheitsarchitektur der Organisation angeordnet sind.	rds-instance-public-access-überprüfen	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Relational Database Service (Amazon RDS) -Instances nicht öffentlich sind. Amazon-RDS-Datenbank-Instances können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-7: Grenzschutz	Überwachen und kontrollieren Sie die Kommunikation an der Außengrenze des Systems und an wichtigen internen Grenzen innerhalb des Systems; Implementieren Sie Subnetzwerke für öffentlich zugängliche Systemkomponenten, die von internen Organisationsnetzwerken getrennt sind; und stellen Sie Verbindungen zu externen Netzwerken oder Informationssystemen nur über verwaltete Schnittstellen her, die aus Grenzschutzvorrichtungen gemäß einer Sicherheitsarchitektur der Organisation angeordnet sind.	rds-snapshots-public-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Relational Database Service (Amazon RDS) -Instances nicht öffentlich sind. Amazon-RDS-Datenbank-Instances können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-7: Grenzschutz	Überwachen und kontrollieren Sie die Kommunikation an der Außengrenze des Systems und an wichtigen internen Grenzen innerhalb des Systems; Implementieren Sie Subnetzwerke für öffentlich zugängliche Systemkomponenten, die von internen Organisationsnetzwerken getrennt sind; und stellen Sie Verbindungen zu externen Netzwerken oder Informationssystemen nur über verwaltete Schnittstellen her, die aus Grenzschutzvorrichtungen gemäß einer Sicherheitsarchitektur der Organisation angeordnet sind.	redshift-cluster-public-access-überprüfen	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Redshift Redshift-Cluster nicht öffentlich sind. Amazon-Redshift-Cluster können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-7: Grenzschutz	Überwachen und kontrollieren Sie die Kommunikation an der Außengrenze des Systems und an wichtigen internen Grenzen innerhalb des Systems; Implementieren Sie Subnetzwerke für öffentlich zugängliche Systemkomponenten, die von internen Organisationsnetzwerken getrennt sind; und stellen Sie Verbindungen zu externen Netzwerken oder Informationssystemen nur über verwaltete Schnittstellen her, die aus Grenzschutzvorrichtungen gemäß einer Sicherheitsarchitektur der Organisation angeordnet sind.	ebs-snapshot-public-restorable-überprüfen	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass EBS-Snapshots nicht öffentlich wiederherstellbar sind. EBS-Volume-Snapshots können vertrauliche Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-7: Grenzschutz	Überwachen und kontrollieren Sie die Kommunikation an der Außengrenze des Systems und an wichtigen internen Grenzen innerhalb des Systems; Implementieren Sie Subnetzwerke für öffentlich zugängliche Systemkomponenten, die von internen Organisationsnetzwerken getrennt sind; und stellen Sie Verbindungen zu externen Netzwerken oder Informationssystemen nur über verwaltete Schnittstellen her, die aus Grenzschutzvorrichtungen gemäß einer Sicherheitsarchitektur der Organisation angeordnet sind.	ec-2 instance-no-public-ip	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon Elastic Compute Cloud (Amazon EC2) - Instances nicht öffentlich zugänglich sind. EC2 Amazon-Instances können vertrauliche Informationen enthalten, und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-7: Grenzschutz	Überwachen und kontrollieren Sie die Kommunikation an der Außengrenze des Systems und an wichtigen internen Grenzen innerhalb des Systems; Implementieren Sie Subnetzwerke für öffentlich zugängliche Systemkomponenten, die von internen Organisationsnetzwerken getrennt sind; und stellen Sie Verbindungen zu externen Netzwerken oder Informationssystemen nur über verwaltete Schnittstellen her, die aus Grenzschutzvorrichtungen gemäß einer Sicherheitsarchitektur der Organisation angeordnet sind.	lambda-function-public-access-verboten	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass AWS Lambda-Funktionen nicht öffentlich zugänglich sind. Der öffentliche Zugriff kann möglicherweise die Verfügbarkeit von Ressourcen beeinträchtigen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-7: Grenzschutz	Überwachen und kontrollieren Sie die Kommunikation an der Außengrenze des Systems und an wichtigen internen Grenzen innerhalb des Systems; Implementieren Sie Subnetzwerke für öffentlich zugängliche Systemkomponenten, die von internen Organisationsnetzwerken getrennt sind; und stellen Sie Verbindungen zu externen Netzwerken oder Informationssystemen nur über verwaltete Schnittstellen her, die aus Grenzschutzvorrichtungen gemäß einer Sicherheitsarchitektur der Organisation angeordnet sind.	s3- -Block-periodisch account-level-public-access	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Simple Storage Service (Amazon S3) -Buckets nicht öffentlich zugänglich sind. Diese Regel trägt dazu bei, sensible Daten vor unbefugten Remote-Benutzern zu schützen, indem sie den öffentlichen Zugriff verhindert. Mit dieser Regel können Sie optional die Parameter ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) und restrictPublicBuckets Parameter (Config Default: True) festlegen. Die tatsächlichen Werte müssen den Richtlini

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			en Ihrer Organisation entsprechen.
SC-7: Grenzschutz	Überwachen und kontrollieren Sie die Kommunikation an der Außengrenze des Systems und an wichtigen internen Grenzen innerhalb des Systems; Implementieren Sie Subnetzwerke für öffentlich zugängliche Systemkomponenten, die von internen Organisationsnetzwerken getrennt sind; und stellen Sie Verbindungen zu externen Netzwerken oder Informationssystemen nur über verwaltete Schnittstellen her, die aus Grenzschutzvorrichtungen gemäß einer Sicherheitsarchitektur der Organisation angeordnet sind.	s3- bucket-policy-grantee-check	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie s3_bucket_policy_grantee_check aktivieren. Diese Regel prüft, ob der vom Amazon S3 S3-Bucket gewährte Zugriff durch die von Ihnen bereitgestellten AWS Principals, Verbundbenutzer, Service Principals, IP-Adressen oder Amazon Virtual Private Cloud (Amazon VPC) IDs eingeschränkt ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-7: Grenzschutz	Überwachen und kontrollieren Sie die Kommunikation an der Außengrenze des Systems und an wichtigen internen Grenzen innerhalb des Systems; Implementieren Sie Subnetzwerke für öffentlich zugängliche Systemkomponenten, die von internen Organisationsnetzwerken getrennt sind; und stellen Sie Verbindungen zu externen Netzwerken oder Informationssystemen nur über verwaltete Schnittstellen her, die aus Grenzschutzvorrichtungen gemäß einer Sicherheitsarchitektur der Organisation angeordnet sind.	s-3 bucket-public-read-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie nur autorisierten Benutzern, Prozessen und Geräten Zugriff auf Amazon Simple Storage Service (Amazon S3) - Buckets gewähren. Die Verwaltung des Zugriffs sollte mit der Klassifizierung der Daten übereinstimmen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-7: Grenzschutz	Überwachen und kontrollieren Sie die Kommunikation an der Außengrenze des Systems und an wichtigen internen Grenzen innerhalb des Systems; Implementieren Sie Subnetzwerke für öffentlich zugängliche Systemkomponenten, die von internen Organisationsnetzwerken getrennt sind; und stellen Sie Verbindungen zu externen Netzwerken oder Informationssystemen nur über verwaltete Schnittstellen her, die aus Grenzschutzvorrichtungen gemäß einer Sicherheitsarchitektur der Organisation angeordnet sind.	s3- bucket-public-write-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie nur autorisierten Benutzern, Prozessen und Geräten Zugriff auf Amazon Simple Storage Service (Amazon S3) - Buckets gewähren. Die Verwaltung des Zugriffs sollte mit der Klassifizierung der Daten übereinstimmen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-7: Grenzschutz	Überwachen und kontrollieren Sie die Kommunikation an der Außengrenze des Systems und an wichtigen internen Grenzen innerhalb des Systems; Implementieren Sie Subnetzwerke für öffentlich zugängliche Systemkomponenten, die von internen Organisationsnetzwerken getrennt sind; und stellen Sie Verbindungen zu externen Netzwerken oder Informationssystemen nur über verwaltete Schnittstellen her, die aus Grenzschutzvorrichtungen gemäß einer Sicherheitsarchitektur der Organisation angeordnet sind.	sagemaker-notebook-no-direct-Internetzugang	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass SageMaker Amazon-Notebooks keinen direkten Internetzugang zulassen. Indem Sie direkten Internetzugang blockieren, vermeiden Sie, dass unbefugte Benutzer auf sensible Daten zugreifen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-7: Grenzschutz	Überwachen und kontrollieren Sie die Kommunikation an der Außengrenze des Systems und an wichtigen internen Grenzen innerhalb des Systems; Implementieren Sie Subnetzwerke für öffentlich zugängliche Systemkomponenten, die von internen Organisationsnetzwerken getrennt sind; und stellen Sie Verbindungen zu externen Netzwerken oder Informationssystemen nur über verwaltete Schnittstellen her, die aus Grenzschutzvorrichtungen gemäß einer Sicherheitsarchitektur der Organisation angeordnet sind.	vpc-sg-open-only-to-authorized-ports	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass gemeinsame Ports für Amazon Elastic Compute Cloud (Amazon EC2) -Sicherheitsgruppen eingeschränkt sind. Wenn der Zugriff auf Ports nicht auf vertrauenswürdige Quellen beschränkt wird, kann dies zu Angriffen auf die Verfügbarkeit, Integrität und Vertraulichkeit von Systemen führen. Durch die Beschränkung des Zugriffs auf Ressourcen innerhalb einer Sicherheitsgruppe aus dem Internet (0.0.0.0/0) kann der Remote-Zugriff auf interne Systeme gesteuert werden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-7: Grenzschutz (CE-9) | Beschränkung von bedrohlichem ausgehendem Kommunikationsverkehr	Erkennen und blockieren Sie ausgehenden Kommunikationsverkehr, der eine Bedrohung für externe Systeme darstellt, und überprüfen Sie die Identität interner Benutzer, die mit verweigertem Kommunikationsverkehr in Verbindung gebracht werden.	wafv2-logging-enabled	Um die Protokollierung und Überwachung in Ihrer Umgebung zu erleichtern, aktivieren Sie die AWS WAF (V2) -Protokollierung im regionalen und globalen Web ACLs. AWS Die WAF-Protokollierung bietet detaillierte Informationen über den Datenverkehr, der von Ihrer Web-ACL analysiert wird. In den Protokollen werden die Uhrzeit aufgezeichnet, zu der die AWS WAF die Anfrage von Ihrer AWS Ressource erhalten hat, Informationen über die Anfrage und eine Aktion für die Regel, der jede Anfrage entsprach.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-7: Grenzschutz (CE-9) | Beschränkung von bedrohlichem ausgehendem Kommunikationsverkehr	Erkennen und blockieren Sie ausgehenden Kommunikationsverkehr, der eine Bedrohung für externe Systeme darstellt, und überprüfen Sie die Identität interner Benutzer, die mit verweigertem Kommunikationsverkehr in Verbindung gebracht werden.	alb-waf-enabled	Stellen Sie sicher, dass AWS WAF auf Elastic Load Balancers (ELB) aktiviert ist, um Webanwendungen zu schützen. Eine WAF trägt zum Schutz Ihrer Webanwendungen oder APIs vor gängigen Web-Exploits bei. Diese Web-Exploits können sich auf die Verfügbarkeit auswirken, die Sicherheit gefährden oder übermäßige Ressourcen in Ihrer Umgebung verbrauchen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-7: Grenzschutz (CE-9) | Beschränkung von bedrohlichem ausgehendem Kommunikationsverkehr	Erkennen und blockieren Sie ausgehenden Kommunikationsverkehr, der eine Bedrohung für externe Systeme darstellt, und überprüfen Sie die Identität interner Benutzer, die mit verweigertem Kommunikationsverkehr in Verbindung gebracht werden.	api-gw-associated-with-WAF	AWS Mit WAF können Sie eine Reihe von Regeln (als Web Access Control List (Web ACL) bezeichnet) konfigurieren, die Webanfragen auf der Grundlage von anpassbaren Websicherheitsregeln und -bedingungen, die Sie definieren, zulassen, blockieren oder zählen. Stellen Sie sicher, dass Ihre Amazon-API-Gateway-Stufe mit einer WAF-Web-ACL verknüpft ist, um sie vor böswilligen Angriffen zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-7: Grenzschutz (IRS-definiert)	Behörden müssen den Grenzschutz (in der Regel mithilfe von Firewalls) an Vertrauensgrenzen implementieren und verwalten . Alle Vertrauen sgrenzen werden überwacht und der grenzüberschreitende Kommunikationsverk ehr muss kontrolliert werden.	netfw-policy-rule-group-verknüpft	Eine AWS Netzwerk-Firewall-Richtlinie definiert, wie Ihre Firewall den Verkehr in einer Amazon VPC überwacht und verarbeitet. Sie konfigurieren statusfre ie und statusbehaftete Regelgruppen, um Pakete und Datenverk ehrsströme zu filtern, und Sie definiere n den standardm äßigen Umgang mit Datenverkehr.
SC-7: Grenzschutz (IRS-definiert)	Behörden müssen den Grenzschutz (in der Regel mithilfe von Firewalls) an Vertrauensgrenzen implementieren und verwalten . Alle Vertrauen sgrenzen werden überwacht und der grenzüberschreitende Kommunikationsverk ehr muss kontrolliert werden.	netfw-stateless-rule-group-nicht leer	Eine AWS Netzwerkf irewall-Regelgrupp e enthält Regeln, die definieren, wie Ihre Firewall den Verkehr in Ihrer VPC verarbeit et. Wenn eine leere statuslose Regelgrup pe in einer Firewall-Richtlinie vorhanden ist, verarbeitet sie keinen Datenverkehr.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-8: Vertraulichkeit und Integrität von Übertragungen (CE-1) Kryptografischer Schutz	Implementieren Sie kryptografische Mechanismen, um die unbefugte Offenlegung von Informationen zu verhindern und Änderungen an Informationen während der Übertragung zu erkennen.	alb-http-to-https-Umleitungsprüfung	Um Daten während der Übertragung zu schützen, stellen Sie sicher, dass Ihr Application Load Balancer unverschlüsselte HTTP-Anfragen automatisch an HTTPS umleitet. Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-8: Vertraulichkeit und Integrität von Übertragungen (CE-1) Kryptografischer Schutz	Implementieren Sie kryptografische Mechanismen, um die unbefugte Offenlegung von Informationen zu verhindern und Änderungen an Informationen während der Übertragung zu erkennen.	elasticsearch-node-to-node-Verschlüsselungsprüfung	Stellen Sie sicher, dass die node-to-node Verschlüsselung für Amazon OpenSearch Service aktiviert ist. Node-to-nodeVerschlüsselung ermöglicht die TLS 1.2-Verschlüsselung für die gesamte Kommunikation innerhalb der Amazon Virtual Private Cloud (Amazon VPC). Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.
SC-8: Vertraulichkeit und Integrität von Übertragungen (CE-1) Kryptografischer Schutz	Implementieren Sie kryptografische Mechanismen, um die unbefugte Offenlegung von Informationen zu verhindern und Änderungen an Informationen während der Übertragung zu erkennen.	elb-tls-https-listeners-nur	Stellen Sie sicher, dass Ihre Elastic Load Balancer (ELBs) mit SSL- oder HTTPS-Listenern konfiguriert sind. Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-8: Vertraulichkeit und Integrität von Übertragungen (CE-1) Kryptografischer Schutz	Implementieren Sie kryptografische Mechanismen, um die unbefugte Offenlegung von Informationen zu verhindern und Änderungen an Informationen während der Übertragung zu erkennen.	opensearch-https-required	Da sensible Daten existieren können und um Daten während der Übertragung zu schützen, sollten Sie sicherstellen, dass HTTPS für Verbindungen zu Ihren Amazon OpenSearch Service-Domains aktiviert ist.
SC-8: Vertraulichkeit und Integrität von Übertragungen (CE-1) Kryptografischer Schutz	Implementieren Sie kryptografische Mechanismen, um die unbefugte Offenlegung von Informationen zu verhindern und Änderungen an Informationen während der Übertragung zu erkennen.	opensearch-node-to-node-Verschlüsselungsprüfung	Stellen Sie sicher, dass die node-to-node Verschlüsselung für Amazon OpenSearch Service aktiviert ist. Node-to-nodeVerschlüsselung ermöglicht die TLS 1.2-Verschlüsselung für die gesamte Kommunikation innerhalb der Amazon Virtual Private Cloud (Amazon VPC). Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-8: Vertraulichkeit und Integrität von Übertragungen (CE-1) Kryptografischer Schutz	Implementieren Sie kryptografische Mechanismen, um die unbefugte Offenlegung von Informationen zu verhindern und Änderungen an Informationen während der Übertragung zu erkennen.	redshift-require-tls-ssl	Stellen Sie sicher, dass Ihre Amazon-Redshift-Cluster eine TLS/SSL-Verschlüsselung erfordern, um eine Verbindung zu SQL-Clients herzustellen. Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.
SC-8: Vertraulichkeit und Integrität von Übertragungen (CE-1) Kryptografischer Schutz	Implementieren Sie kryptografische Mechanismen, um die unbefugte Offenlegung von Informationen zu verhindern und Änderungen an Informationen während der Übertragung zu erkennen.	s-3 bucket-ssl-requests-only	Um Daten während der Übertragung zu schützen, stellen Sie sicher, dass Ihre Amazon Simple Storage Service (Amazon S3)-Buckets Anfragen zur Verwendung von Secure Socket Layer (SSL)-Buckets erfordern. Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-12: Einrichtung und Verwaltung kryptografischer Schlüssel	Wenn Kryptografie innerhalb des Systems eingesetzt wird, muss die Behörde kryptografische Schlüssel gemäß den folgenden zentralen Verwaltungsanforderungen einrichten und verwalten: NIST SP 800-57, Empfehlung für die Schlüsselmanagement und die Generierung, Verteilung, Speicherung, den Zugriff auf und die Vernichtung von Schlüsseln.	kms-cmk-not-scheduled-zum Löschen	Um Daten im Ruhezustand zu schützen, sollten Sie sicherstellen, dass die für den Kunden erforderlichen Masterschlüssel (CMKs) nicht für das Löschen im AWS Key Management Service (AWS KMS) vorgesehen sind. Da Schlüssel manchmal gelöscht werden müssen, können Sie mit dieser Regel alle zu löschenden Schlüssel überprüfen, falls ein Schlüssel versehentlich zur Löschung vorgemerkt wurde.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-12: Einrichtung und Verwaltung kryptografischer Schlüssel	Wenn Kryptografie innerhalb des Systems eingesetzt wird, muss die Behörde kryptografische Schlüssel gemäß den folgenden zentralen Verwaltungsanforderungen einrichten und verwalten: NIST SP 800-57, Empfehlung für die Schlüsselmanagement und die Generierung, Verteilung, Speicherung, den Zugriff auf und die Vernichtung von Schlüsseln.	cmk-backing-key-rotation-aktiviert	Aktivieren Sie die Schlüsselrotation, um sicherzustellen, dass Schlüssel rotiert werden, nachdem sie das Ende ihrer Krypto-Periode erreicht haben.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-13: Kryptografischer Schutz	Implementieren Sie die folgenden Kryptografietypen, die für jede bestimmte kryptografische Verwendung erforderlich sind: Der neueste FIPS-140-validierte Verschlüsselungsmechanismus NIST 800-52, Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations, Encryption in transit (payload encryption). Use of SHA-1 für digitale Signaturen ist verboten.	elb-acm-certificate-required	Zum Schutz von eventuell vorhandenen sensiblen Daten sowie von Daten während der Übertragung muss die Verschlüsselung für Ihr Elastic Load Balancing aktiviert sein. Verwenden Sie AWS Certificate Manager, um öffentliche und private SSL/TLS-Zertifikate mit AWS Diensten und internen Ressourcen zu verwalten, bereitzustellen und bereitzustellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-13: Kryptografischer Schutz	Implementieren Sie die folgenden Kryptografietypen, die für jede bestimmte kryptografische Verwendung erforderlich sind: Der neueste FIPS-140-validierte Verschlüsselungsmechanismus für digitale Signaturen ist verboten. NIST 800-52, Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations, Encryption in transit (payload encryption). Use of SHA-1	alb-http-to-https-Umleitungsprüfung	Um Daten während der Übertragung zu schützen, stellen Sie sicher, dass Ihr Application Load Balancer unverschlüsselte HTTP-Anfragen automatisch an HTTPS umleitet. Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-13: Kryptografischer Schutz	Implementieren Sie die folgenden Kryptografietypen, die für jede bestimmte kryptografische Verwendung erforderlich sind: Der neueste FIPS-140-validierte Verschlüsselungsmechanismus für digitale Signaturen ist verboten. NIST 800-52, Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations, Encryption in transit (payload encryption). Use of SHA-1	api-gw-cache-enabled-und-verschlüsselt	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass die Verschlüsselung für den Cache Ihrer API-Gateway-Stufe aktiviert ist. Da für die API-Methode sensible Daten erfasst werden können, sollten Sie die Verschlüsselung von Daten im Ruhezustand aktivieren, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-13: Kryptografischer Schutz	Implementieren Sie die folgenden Kryptografietypen, die für jede bestimmte kryptografische Verwendung erforderlich sind: Der neueste FIPS-140-validierte Verschlüsselungsmechanismus für digitale Signaturen ist verboten. NIST 800-52, Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations, Encryption in transit (payload encryption). Use of SHA-1	elasticsearch-node-to-node-Verschlüsselungsprüfung	Stellen Sie sicher, dass die node-to-node Verschlüsselung für Amazon OpenSearch Service aktiviert ist. Node-to-nodeVerschlüsselung ermöglicht die TLS 1.2-Verschlüsselung für die gesamte Kommunikation innerhalb der Amazon Virtual Private Cloud (Amazon VPC). Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-13: Kryptografischer Schutz	Implementieren Sie die folgenden Kryptografietypen, die für jede bestimmte kryptografische Verwendung erforderlich sind: Der neueste FIPS-140-validierte Verschlüsselungsmechanismus für digitale Signaturen ist verboten. NIST 800-52, Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations, Encryption in transit (payload encryption). Use of SHA-1	elb-tls-https-listeners-nur	Stellen Sie sicher, dass Ihre Elastic Load Balancer (ELBs) mit SSL- oder HTTPS-Listenern konfiguriert sind. Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-13: Kryptografischer Schutz	Implementieren Sie die folgenden Kryptografietypen, die für jede bestimmte kryptografische Verwendung erforderlich sind: Der neueste FIPS-140-validierte Verschlüsselungsmechanismus für digitale Signaturen ist verboten. NIST 800-52, Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations, Encryption in transit (payload encryption). Use of SHA-1	opensearch-https-required	Da sensible Daten existieren können und um Daten während der Übertragung zu schützen, sollten Sie sicherstellen, dass HTTPS für Verbindungen zu Ihren Amazon OpenSearch Service-Domains aktiviert ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-13: Kryptografischer Schutz	Implementieren Sie die folgenden Arten von Kryptografie, die für jede bestimmte kryptografische Verwendung erforderlich sind: Der neueste FIPS-140-validierte Verschlüsselungsmechanismus NIST 800-52, Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations, Encryption in transit (payload encryption). Use of SHA-1 für digitale Signaturen ist verboten.	opensearch-node-to-node-Verschlüsselungsprüfung	Stellen Sie sicher, dass die node-to-node Verschlüsselung für Amazon OpenSearch Service aktiviert ist. Node-to-nodeVerschlüsselung ermöglicht die TLS 1.2-Verschlüsselung für die gesamte Kommunikation innerhalb der Amazon Virtual Private Cloud (Amazon VPC). Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-13: Kryptografischer Schutz	Implementieren Sie die folgenden Kryptografietypen, die für jede bestimmte kryptografische Verwendung erforderlich sind: Der neueste FIPS-140-validierte Verschlüsselungsmechanismus für digitale Signaturen ist verboten. NIST 800-52, Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations, Encryption in transit (payload encryption). Use of SHA-1	backup-recovery-point-encrypted	Stellen Sie sicher, dass die Verschlüsselung für Ihre AWS Backup-Wiederherstellungspunkte aktiviert ist. Da sensible Daten auch im Ruhezustand vorhanden sein können, sollten Sie die Verschlüsselung im Ruhezustand aktivieren, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-13: Kryptografischer Schutz	Implementieren Sie die folgenden Kryptografietypen, die für jede bestimmte kryptografische Verwendung erforderlich sind: Der neueste FIPS-140-validierte Verschlüsselungsmechanismus NIST 800-52, Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations, Encryption in transit (payload encryption). Use of SHA-1 für digitale Signaturen ist verboten.	dynamodb-table-encrypted-kms	Stellen Sie sicher, dass die Verschlüsselung für Ihre Amazon-DynamoDB-Tabellen aktiviert ist. Um eventuell vorhandene sensible Daten im Ruhezustand in diesen Tabellen zu schützen, müssen Sie die Verschlüsselung von Daten im Ruhezustand aktivieren. Standardmäßig werden DynamoDB-Tabellen mit einem AWS eigenen Kundenhauptschlüssel (CMK) verschlüselt.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-13: Kryptografischer Schutz	Implementieren Sie die folgenden Kryptografietypen, die für jede bestimmte kryptografische Verwendung erforderlich sind: Der neueste FIPS-140-validierte Verschlüsselungsmechanismus für digitale Signaturen ist verboten. NIST 800-52, Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations, Encryption in transit (payload encryption). Use of SHA-1	ec2- ebs-encryption-by-default	Zum Schutz von Daten im Ruhezustand müssen Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon Elastic Block Store (Amazon EBS)-Volumes aktiviert ist. Da sensible Daten auch im Ruhezustand vorhanden sein können, sollten Sie die Verschlüsselung im Ruhezustand aktivieren, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-13: Kryptografischer Schutz	Implementieren Sie die folgenden Kryptografietypen, die für jede bestimmte kryptografische Verwendung erforderlich sind: Der neueste FIPS-140-validierte Verschlüsselungsmechanismus für digitale Signaturen ist verboten. NIST 800-52, Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations, Encryption in transit (payload encryption). Use of SHA-1	kinesis-stream-encrypted	Aktivieren Sie die Verschlüsselung für Ihre Amazon-Kinesis-Streams, um eventuell vorhandene sensible Daten sowie Daten im Ruhezustand zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-13: Kryptografischer Schutz	Implementieren Sie die folgenden Kryptografietypen, die für jede bestimmte kryptografische Verwendung erforderlich sind: Der neueste FIPS-140-validierte Verschlüsselungsmechanismus für digitale Signaturen ist verboten. NIST 800-52, Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations, Encryption in transit (payload encryption). Use of SHA-1	opensearch-encrypted-at-rest	Da sensible Daten vorhanden sein können und um Daten im Ruhezustand zu schützen, sollten Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon OpenSearch Service-Domains aktiviert ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-13: Kryptografischer Schutz	Implementieren Sie die folgenden Arten von Kryptografie, die für jede bestimmte kryptografische Verwendung erforderlich sind: Der neueste FIPS-140-validierte Verschlüsselungsmechanismus NIST 800-52, Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations, Encryption in transit (payload encryption). Use of SHA-1 für digitale Signaturen ist verboten.	rds-snapshot-encrypted	Stellen Sie sicher, dass die Verschlüsselung für Ihre Amazon Relational Database Service (Amazon RDS)-Snapshots aktiviert ist. Da sensible Daten auch im Ruhezustand vorhanden sein können, sollten Sie die Verschlüsselung im Ruhezustand aktivieren, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-13: Kryptografischer Schutz	Implementieren Sie die folgenden Kryptografietypen, die für jede bestimmte kryptografische Verwendung erforderlich sind: Der neueste FIPS-140-validierte Verschlüsselungsmechanismus für digitale Signaturen ist verboten. NIST 800-52, Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations, Encryption in transit (payload encryption). Use of SHA-1	redshift-cluster-kms-enabled	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass die Verschlüsselung mit AWS Key Management Service (AWS KMS) für Ihren Amazon Redshift Redshift-Cluster aktiviert ist. Um eventuell vorhandene sensible Daten im Ruhezustand in Redshift-Clustern zu schützen, muss die Verschlüsselung von Daten im Ruhezustand aktiviert sein.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-13: Kryptografischer Schutz	Implementieren Sie die folgenden Kryptografietypen, die für jede bestimmte kryptografische Verwendung erforderlich sind: Der neueste FIPS-140-validierte Verschlüsselungsmechanismus für digitale Signaturen ist verboten. NIST 800-52, Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations, Encryption in transit (payload encryption). Use of SHA-1	s3- default-encryption-kms	Stellen Sie sicher, dass die Verschlüsselung für Ihre Amazon Simple Storage Service (Amazon S3)-Buckets aktiviert ist. Um eventuell vorhandene sensible Daten im Ruhezustand in einem Amazon-S3-Bucket zu schützen, muss die Verschlüsselung aktiviert sein.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-13: Kryptografischer Schutz	Implementieren Sie die folgenden Kryptografietypen, die für jede bestimmte kryptografische Verwendung erforderlich sind: Der neueste FIPS-140-validierte Verschlüsselungsmechanismus NIST 800-52, Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations, Encryption in transit (payload encryption). Use of SHA-1 für digitale Signaturen ist verboten.	secretsmanager-using-cmk	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass die Verschlüsselung mit dem AWS Key Management Service (AWS KMS) für AWS Secrets Manager aktiviert ist. Aktivieren Sie die Verschlüsselung von Daten im Ruhezustand, um eventuell vorhandene sensible Daten im Ruhezustand im Secrets Manager zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-13: Kryptografischer Schutz	Implementieren Sie die folgenden Kryptografietypen, die für jede bestimmte kryptografische Verwendung erforderlich sind: Der neueste FIPS-140-validierte Verschlüsselungsmechanismus NIST 800-52, Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations, Encryption in transit (payload encryption). Use of SHA-1 für digitale Signaturen ist verboten.	cloudwatch-log-group-encrypted	Um sensible Daten im Speicher zu schützen, stellen Sie sicher, dass die Verschlüsselung für Ihre Amazon CloudWatch Log Groups aktiviert ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-13: Kryptografischer Schutz	Implementieren Sie die folgenden Kryptografietypen, die für jede bestimmte kryptografische Verwendung erforderlich sind: Der neueste FIPS-140-validierte Verschlüsselungsmechanismus NIST 800-52, Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations, Encryption in transit (payload encryption). Use of SHA-1 für digitale Signaturen ist verboten.	efs-encrypted-check	Aktivieren Sie die Verschlüsselung für Ihr Amazon Elastic File System (EFS), um eventuell vorhandene sensible Daten sowie Daten im Ruhezustand zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-13: Kryptografischer Schutz	Implementieren Sie die folgenden Kryptografietypen, die für jede bestimmte kryptografische Verwendung erforderlich sind: Der neueste FIPS-140-validierte Verschlüsselungsmechanismus für digitale Signaturen ist verboten. NIST 800-52, Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations, Encryption in transit (payload encryption). Use of SHA-1	elasticsearch-encrypted-at-rest	Da sensible Daten vorhanden sein können und um Daten im Ruhezustand zu schützen, sollten Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon OpenSearch Service (OpenSearch Service) -Domains aktiviert ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-13: Kryptografischer Schutz	Implementieren Sie die folgenden Arten von Kryptografie, die für jede bestimmte kryptografische Verwendung erforderlich sind: Der neueste FIPS-140-validierte Verschlüsselungsmechanismus NIST 800-52, Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations, Encryption in transit (payload encryption). Use of SHA-1 für digitale Signaturen ist verboten.	encrypted-volumes	Aktivieren Sie die Verschlüsselung für Ihre Amazon-Elastic-Block-Store (Amazon-EBS)-Volumes, um eventuell vorhandene sensible Daten sowie Daten im Ruhezustand zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-13: Kryptografischer Schutz	Implementieren Sie die folgenden Kryptografietypen, die für jede bestimmte kryptografische Verwendung erforderlich sind: Der neueste FIPS-140-validierte Verschlüsselungsmechanismus für digitale Signaturen ist verboten. NIST 800-52, Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations, Encryption in transit (payload encryption). Use of SHA-1	rds-storage-encrypted	Zum Schutz von Daten im Ruhezustand müssen Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon Relational Database Service (Amazon RDS)-Instances aktiviert ist. Um eventuell vorhandene sensible Daten im Ruhezustand in Amazon-RDS-Instances zu schützen, muss die Verschlüsselung von Daten im Ruhezustand aktiviert sein.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-13: Kryptografischer Schutz	Implementieren Sie die folgenden Kryptografietypen, die für jede bestimmte kryptografische Verwendung erforderlich sind: Der neueste FIPS-140-validierte Verschlüsselungsmechanismus für digitale Signaturen ist verboten. NIST 800-52, Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations, Encryption in transit (payload encryption). Use of SHA-1	redshift-cluster-configuration-check	Um Daten im Ruhezustand zu schützen, muss die Verschlüsselung für Ihre Amazon-Redshift-Cluster aktiviert sein. Sie müssen auch sicherstellen, dass die erforderlichen Konfigurationen auf Amazon-Redshift-Clustern bereitgestellt werden. Die Prüfungsprotokollierung muss aktiviert sein, um Informationen zu Verbindungen und Benutzeraktivitäten in der Datenbank bereitzustellen. Diese Regel erfordert, dass ein Wert für clusterDbEncrypted (Config Default: TRUE) und LoggingEnabled (Config Default: TRUE) gesetzt ist. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-13: Kryptografischer Schutz	Implementieren Sie die folgenden Kryptografietypen, die für jede angegebene kryptografische Verwendung erforderlich sind: Der neueste FIPS-140-validierte Verschlüsselungsmechanismus für digitale Signaturen ist verboten. NIST 800-52, Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations, Encryption in transit (payload encryption). Use of SHA-1	redshift-require-tls-ssl	Stellen Sie sicher, dass Ihre Amazon-Redshift-Cluster eine TLS/SSL-Verschlüsselung erfordern, um eine Verbindung zu SQL-Clients herzustellen. Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-13: Kryptografischer Schutz	Implementieren Sie die folgenden Kryptografietypen, die für jede bestimmte kryptografische Verwendung erforderlich sind: Der neueste FIPS-140-validierte Verschlüsselungsmechanismus für digitale Signaturen ist verboten. NIST 800-52, Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations, Encryption in transit (payload encryption). Use of SHA-1	s3- aktiviert bucket-server-side-encryption	Zum Schutz von Daten im Ruhezustand müssen Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon Simple Storage Service (Amazon S3)-Buckets aktiviert ist. Um eventuell vorhandene sensible Daten im Ruhezustand in Amazon-S3-Buckets zu schützen, muss die Verschlüsselung aktiviert sein.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-13: Kryptografischer Schutz	Implementieren Sie die folgenden Kryptografietypen, die für jede bestimmte kryptografische Verwendung erforderlich sind: Der neueste FIPS-140-validierte Verschlüsselungsmechanismus für digitale Signaturen ist verboten. NIST 800-52, Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations, Encryption in transit (payload encryption). Use of SHA-1	s3- bucket-ssl-requests-only	Um Daten während der Übertragung zu schützen, stellen Sie sicher, dass Ihre Amazon Simple Storage Service (Amazon S3)-Buckets Anfragen zur Verwendung von Secure Socket Layer (SSL)-Buckets erfordern. Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-13: Kryptografischer Schutz	Implementieren Sie die folgenden Kryptografietypen, die für jede bestimmte kryptografische Verwendung erforderlich sind: Der neueste FIPS-140-validierte Verschlüsselungsmechanismus NIST 800-52, Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations, Encryption in transit (payload encryption). Use of SHA-1 für digitale Signaturen ist verboten.	sagemaker-endpoint-configuration-kms-key-konfiguriert	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass die Verschlüsselung mit dem AWS Key Management Service (AWS KMS) für Ihren Endpunkt aktiviert ist. SageMaker Da sensible Daten auf dem SageMaker Endgerät gespeichert werden können, sollten Sie die Verschlüsselung im Ruhezustand aktivieren, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-13: Kryptografischer Schutz	Implementieren Sie die folgenden Kryptografietypen, die für jede bestimmte kryptografische Verwendung erforderlich sind: Der neueste FIPS-140-validierte Verschlüsselungsmechanismus NIST 800-52, Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations, Encryption in transit (payload encryption). Use of SHA-1 für digitale Signaturen ist verboten.	sagemaker-notebook-instance-kms-key-konfiguriert	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass die Verschlüsselung mit dem AWS Key Management Service (AWS KMS) für Ihr Notebook aktiviert ist. SageMaker Da vertrauliche Daten im SageMaker Notebook gespeichert werden können, sollten Sie die Verschlüsselung im Ruhezustand aktivieren, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-13: Kryptografischer Schutz	Implementieren Sie die folgenden Kryptografietypen, die für jede bestimmte kryptografische Verwendung erforderlich sind: Der neueste FIPS-140-validierte Verschlüsselungsmechanismus NIST 800-52, Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations, Encryption in transit (payload encryption). Use of SHA-1 für digitale Signaturen ist verboten.	sns-encrypted-kms	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass Ihre Amazon Simple Notification Service (Amazon SNS) -Themen mit dem AWS Key Management Service (AWS KMS) verschlüsselt werden müssen. Um eventuell vorhandene sensible Daten im Ruhezustand in veröffentlichten Nachrichten zu schützen, muss die Verschlüsselung von Daten im Ruhezustand aktiviert sein.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-23: Sitzungsauthentizität	Schützen Sie die Authentizität von Kommunikationssitzungen.	ec2-imdsv2-check	Stellen Sie sicher, dass die Methode Instance Metadata Service Version 2 (IMDSv2) aktiviert ist, um den Zugriff auf und die Kontrolle der Amazon Elastic Compute Cloud (Amazon EC2) - Instance-Metadaten zu schützen. Die IMDSv2 Methode verwendet sitzungsbasierte Kontrollen. Mit können Kontrollen implementiert werden IMDSv2, um Änderungen an Instanzmetadaten einzuschränken.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-28: Schutz von Informationen im Ruhezustand (CE-1) Kryptografischer Schutz	Implementieren Sie kryptografische Mechanismen, um die unbefugte Offenlegung und Änderung von FTI im Ruhezustand auf Computersystemen von Endbenutzern (d. h. Desktop-Computern, Laptops, Mobilgeräten, mobilen Wechseldatenträgern) in nichtflüchtigen Speichern zu verhindern.	api-gw-cache-enabled-und-verschlüsselt	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass die Verschlüsselung für den Cache Ihrer API-Gateway-Stufe aktiviert ist. Da für die API-Methode sensible Daten erfasst werden können, sollten Sie die Verschlüsselung von Daten im Ruhezustand aktivieren, um diese Daten zu schützen.
SC-28: Schutz von Informationen im Ruhezustand (CE-1) Kryptografischer Schutz	Implementieren Sie kryptografische Mechanismen, um die unbefugte Offenlegung und Änderung von FTI im Ruhezustand auf Computersystemen von Endbenutzern (d. h. Desktop-Computern, Laptops, Mobilgeräten, mobilen Wechseldatenträgern) in nichtflüchtigen Speichern zu verhindern.	backup-recovery-point-encrypted	Stellen Sie sicher, dass die Verschlüsselung für Ihre AWS Backup-Wiederherstellungspunkte aktiviert ist. Da sensible Daten auch im Ruhezustand vorhanden sein können, sollten Sie die Verschlüsselung im Ruhezustand aktivieren, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-28: Schutz von Informationen im Ruhezustand (CE-1) Kryptografischer Schutz	Implementieren Sie kryptografische Mechanismen, um die unbefugte Offenlegung und Änderung von FTI im Ruhezustand auf Computersystemen von Endbenutzern (d. h. Desktop-Computern, Laptops, Mobilgeräten, mobilen Wechseldatenträgern) in nichtflüchtigen Speichern zu verhindern.	cloud-trail-encryption-enabled	Da sensible Daten vorhanden sein können und um Daten im Ruhezustand zu schützen, sollten Sie sicherstellen, dass die Verschlüsselung für Ihre AWS CloudTrail Trails aktiviert ist.
SC-28: Schutz von Informationen im Ruhezustand (CE-1) Kryptografischer Schutz	Implementieren Sie kryptografische Mechanismen, um die unbefugte Offenlegung und Änderung von FTI im Ruhezustand auf Computersystemen von Endbenutzern (d. h. Desktop-Computern, Laptops, Mobilgeräten, mobilen Wechseldatenträgern) in nichtflüchtigen Speichern zu verhindern.	cloudwatch-log-group-encrypted	Um sensible Daten im Speicher zu schützen, stellen Sie sicher, dass die Verschlüsselung für Ihre Amazon CloudWatch Log Groups aktiviert ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-28: Schutz von Informationen im Ruhezustand (CE-1) Kryptografischer Schutz	Implementieren Sie kryptografische Mechanismen, um die unbefugte Offenlegung und Änderung von FTI im Ruhezustand auf Computersystemen von Endbenutzern (d. h. Desktop-Computern, Laptops, Mobilgeräten, mobilen Wechseldatenträgern) in nichtflüchtigen Speichern zu verhindern.	sns-encrypted-kms	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass Ihre Amazon Simple Notification Service (Amazon SNS) -Themen mit dem AWS Key Management Service (AWS KMS) verschlüsselt werden müssen. Um eventuell vorhandene sensible Daten im Ruhezustand in veröffentlichten Nachrichten zu schützen, muss die Verschlüsselung von Daten im Ruhezustand aktiviert sein.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-28: Schutz von Informationen im Ruhezustand (CE-1) Kryptografischer Schutz	Implementieren Sie kryptografische Mechanismen, um die unbefugte Offenlegung und Änderung von FTI im Ruhezustand auf Computersystemen von Endbenutzern (d. h. Desktop-Computern, Laptops, Mobilgeräten, mobilen Wechseldatenträgern) in nichtflüchtigen Speichern zu verhindern.	dynamodb-table-encrypted-kms	Stellen Sie sicher, dass die Verschlüsselung für Ihre Amazon-DynamoDB-Tabellen aktiviert ist. Um eventuell vorhandene sensible Daten im Ruhezustand in diesen Tabellen zu schützen, müssen Sie die Verschlüsselung von Daten im Ruhezustand aktivieren. Standardmäßig werden DynamoDB-Tabellen mit einem AWS eigenen Kundenhauptschlüssel (CMK) verschlüsselt.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-28: Schutz von Informationen im Ruhezustand (CE-1) Kryptografischer Schutz	Implementieren Sie kryptografische Mechanismen, um die unbefugte Offenlegung und Änderung von FTI im Ruhezustand auf Computersystemen von Endbenutzern (d. h. Desktop-Computern, Laptops, Mobilgeräten, mobilen Wechseldatenträgern) in nichtflüchtigen Speichern zu verhindern.	ec2- ebs-encryption-by-default	Zum Schutz von Daten im Ruhezustand müssen Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon Elastic Block Store (Amazon EBS)-Volumes aktiviert ist. Da sensible Daten auch im Ruhezustand vorhanden sein können, sollten Sie die Verschlüsselung im Ruhezustand aktivieren, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-28: Schutz von Informationen im Ruhezustand (CE-1) Kryptografischer Schutz	Implementieren Sie kryptografische Mechanismen, um die unbefugte Offenlegung und Änderung von FTI im Ruhezustand auf Computersystemen von Endbenutzern (d. h. Desktop-Computern, Laptops, Mobilgeräten, mobilen Wechseldatenträgern) in nichtflüchtigen Speichern zu verhindern.	efs-encrypted-check	Aktivieren Sie die Verschlüsselung für Ihr Amazon Elastic File System (EFS), um eventuell vorhandene sensible Daten sowie Daten im Ruhezustand zu schützen.
SC-28: Schutz von Informationen im Ruhezustand (CE-1) Kryptografischer Schutz	Implementieren Sie kryptografische Mechanismen, um die unbefugte Offenlegung und Änderung von FTI im Ruhezustand auf Computersystemen von Endbenutzern (d. h. Desktop-Computern, Laptops, Mobilgeräten, mobilen Wechseldatenträgern) in nichtflüchtigen Speichern zu verhindern.	elasticsearch-encrypted-at-rest	Da sensible Daten vorhanden sein können und um Daten im Ruhezustand zu schützen, sollten Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon OpenSearch Service (OpenSearch Service) -Domains aktiviert ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-28: Schutz von Informationen im Ruhezustand (CE-1) Kryptografischer Schutz	Implementieren Sie kryptografische Mechanismen, um die unbefugte Offenlegung und Änderung von FTI im Ruhezustand auf Computersystemen von Endbenutzern (d. h. Desktop-Computern, Laptops, Mobilgeräten, mobilen Wechseldatenträgern) in nichtflüchtigen Speichern zu verhindern.	encrypted-volumes	Aktivieren Sie die Verschlüsselung für Ihre Amazon-Elastic-Block-Store (Amazon-EBS)-Volumes, um eventuell vorhandene sensible Daten sowie Daten im Ruhezustand zu schützen.
SC-28: Schutz von Informationen im Ruhezustand (CE-1) Kryptografischer Schutz	Implementieren Sie kryptografische Mechanismen, um die unbefugte Offenlegung und Änderung von FTI im Ruhezustand auf Computersystemen von Endbenutzern (d. h. Desktop-Computern, Laptops, Mobilgeräten, mobilen Wechseldatenträgern) in nichtflüchtigen Speichern zu verhindern.	kinesis-stream-encrypted	Aktivieren Sie die Verschlüsselung für Ihre Amazon-Kinesis-Streams, um eventuell vorhandene sensible Daten sowie Daten im Ruhezustand zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-28: Schutz von Informationen im Ruhezustand (CE-1) Kryptografischer Schutz	Implementieren Sie kryptografische Mechanismen, um die unbefugte Offenlegung und Änderung von FTI im Ruhezustand auf Computersystemen von Endbenutzern (d. h. Desktop-Computern, Laptops, Mobilgeräten, mobilen Wechseldatenträgern) in nichtflüchtigen Speichern zu verhindern.	opensearch-encrypted-at-rest	Da sensible Daten vorhanden sein können und um Daten im Ruhezustand zu schützen, sollten Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon OpenSearch Service-Domains aktiviert ist.
SC-28: Schutz von Informationen im Ruhezustand (CE-1) Kryptografischer Schutz	Implementieren Sie kryptografische Mechanismen, um die unbefugte Offenlegung und Änderung von FTI im Ruhezustand auf Computersystemen von Endbenutzern (d. h. Desktop-Computern, Laptops, Mobilgeräten, mobilen Wechseldatenträgern) in nichtflüchtigen Speichern zu verhindern.	rds-snapshot-encrypted	Stellen Sie sicher, dass die Verschlüsselung für Ihre Amazon Relational Database Service (Amazon RDS)-Snapshots aktiviert ist. Da sensible Daten auch im Ruhezustand vorhanden sein können, sollten Sie die Verschlüsselung im Ruhezustand aktivieren, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-28: Schutz von Informationen im Ruhezustand (CE-1) Kryptografischer Schutz	Implementieren Sie kryptografische Mechanismen, um die unbefugte Offenlegung und Änderung von FTI im Ruhezustand auf Computersystemen von Endbenutzern (d. h. Desktop-Computern, Laptops, Mobilgeräten, mobilen Wechseldatenträgern) in nichtflüchtigen Speichern zu verhindern.	rds-storage-encrypted	Zum Schutz von Daten im Ruhezustand müssen Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon Relational Database Service (Amazon RDS)-Instances aktiviert ist. Um eventuell vorhandene sensible Daten im Ruhezustand in Amazon-RDS-Instances zu schützen, muss die Verschlüsselung von Daten im Ruhezustand aktiviert sein.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-28: Schutz von Informationen im Ruhezustand (CE-1) Kryptografischer Schutz	Implementieren Sie kryptografische Mechanismen, um die unbefugte Offenlegung und Änderung von FTI im Ruhezustand auf Computersystemen von Endbenutzern (d. h. Desktop-Computern, Laptops, Mobilgeräten, mobilen Wechseldatenträgern) in nichtflüchtigen Speichern zu verhindern.	redshift-cluster-configuration-check	Um Daten im Ruhezustand zu schützen, muss die Verschlüsselung für Ihre Amazon-Redshift-Cluster aktiviert sein. Sie müssen auch sicherstellen, dass die erforderlichen Konfigurationen auf Amazon-Redshift-Clustern bereitgestellt werden. Die Prüfungsprotokollierung muss aktiviert sein, um Informationen zu Verbindungen und Benutzeraktivitäten in der Datenbank bereitzustellen. Diese Regel erfordert, dass ein Wert für clusterDbEncrypted (Config Default: TRUE) und LoggingEnabled (Config Default: TRUE) gesetzt ist. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-28: Schutz von Informationen im Ruhezustand (CE-1) Kryptografischer Schutz	Implementieren Sie kryptografische Mechanismen, um die unbefugte Offenlegung und Änderung von FTI im Ruhezustand auf Computersystemen von Endbenutzern (d. h. Desktop-Computern, Laptops, Mobilgeräten, mobilen Wechseldatenträgern) in nichtflüchtigen Speichern zu verhindern.	redshift-cluster-kms-enabled	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass die Verschlüsselung mit AWS Key Management Service (AWS KMS) für Ihren Amazon Redshift Redshift-Cluster aktiviert ist. Um eventuell vorhandene sensible Daten im Ruhezustand in Redshift-Clustern zu schützen, muss die Verschlüsselung von Daten im Ruhezustand aktiviert sein.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-28: Schutz von Informationen im Ruhezustand (CE-1) Kryptografischer Schutz	Implementieren Sie kryptografische Mechanismen, um die unbefugte Offenlegung und Änderung von FTI im Ruhezustand auf Computersystemen von Endbenutzern (d. h. Desktop-Computern, Laptops, Mobilgeräten, mobilen Wechseldatenträgern) in nichtflüchtigen Speichern zu verhindern.	s3- aktiviert bucket-server-side-encryption	Zum Schutz von Daten im Ruhezustand müssen Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon Simple Storage Service (Amazon S3)-Buckets aktiviert ist. Um eventuell vorhandene sensible Daten im Ruhezustand in Amazon-S3-Buckets zu schützen, muss die Verschlüsselung aktiviert sein.
SC-28: Schutz von Informationen im Ruhezustand (CE-1) Kryptografischer Schutz	Implementieren Sie kryptografische Mechanismen, um die unbefugte Offenlegung und Änderung von FTI im Ruhezustand auf Computersystemen von Endbenutzern (d. h. Desktop-Computern, Laptops, Mobilgeräten, mobilen Wechseldatenträgern) in nichtflüchtigen Speichern zu verhindern.	s-3 default-encryption-kms	Stellen Sie sicher, dass die Verschlüsselung für Ihre Amazon Simple Storage Service (Amazon S3)-Buckets aktiviert ist. Um eventuell vorhandene sensible Daten im Ruhezustand in einem Amazon-S3-Bucket zu schützen, muss die Verschlüsselung aktiviert sein.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-28: Schutz von Informationen im Ruhezustand (CE-1) Kryptografischer Schutz	Implementieren Sie kryptografische Mechanismen, um die unbefugte Offenlegung und Änderung von FTI im Ruhezustand auf Computersystemen von Endbenutzern (d. h. Desktop-C omputern, Laptops, Mobilgeräten, mobilen Wechselda tenträgern) in nichtflüc htigen Speichern zu verhindern.	sagemaker-endpoint -configuration-kms- key-konfiguriert	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass die Verschlüsselung mit dem AWS Key Management Service (AWS KMS) für Ihren Endpunkt aktiviert ist. SageMaker Da sensible Daten auf dem SageMaker Endgerät gespeiche rt werden können, sollten Sie die Verschlüsselung im Ruhezustand aktiviere n, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-28: Schutz von Informationen im Ruhezustand (CE-1) Kryptografischer Schutz	Implementieren Sie kryptografische Mechanismen, um die unbefugte Offenlegung und Änderung von FTI im Ruhezustand auf Computersystemen von Endbenutzern (d. h. Desktop-Computern, Laptops, Mobilgeräten, mobilen Wechseldatenträgern) in nichtflüchtigen Speichern zu verhindern.	sagemaker-notebook-instance-kms-schlüsselkonfiguriert	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass die Verschlüsselung mit dem AWS Key Management Service (AWS KMS) für Ihr Notebook aktiviert ist. SageMaker Da vertrauliche Daten im SageMaker Notebook gespeichert werden können, sollten Sie die Verschlüsselung im Ruhezustand aktivieren, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-28: Schutz von Informationen im Ruhezustand (CE-1) Kryptografischer Schutz	Implementieren Sie kryptografische Mechanismen, um die unbefugte Offenlegung und Änderung von FTI im Ruhezustand auf Computersystemen von Endbenutzern (d. h. Desktop-Computern, Laptops, Mobilgeräten, mobilen Wechseldatenträgern) in nichtflüchtigen Speichern zu verhindern.	secretsmanager-using-cmk	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass die Verschlüsselung mit dem AWS Key Management Service (AWS KMS) für AWS Secrets Manager aktiviert ist. Aktivieren Sie die Verschlüsselung von Daten im Ruhezustand, um eventuell vorhandene sensible Daten im Ruhezustand im Secrets Manager zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SI-2: Behebung von Fehlern (IRS-definiert)	Die Agentur stellt sicher, dass beim täglichen Einschalten und beim Anschluss an das Netzwerk der Agentur die Arbeitsstationen (wie in den Richtlinien definiert, einschließlich Fernverbindungen über GFE-Workstations) überprüft werden, um sicherzustellen, dass die neuesten von der Behörde genehmigten Patches installiert wurden und dass alle fehlenden oder neuen Patches bei Bedarf installiert oder auf andere Weise überprüft werden, mindestens alle 24 Stunden (außer an Wochenenden, Feiertagen usw.).	instance-managed-by-systemsec2- -Manager	Eine Bestandsaufnahme der Softwareplattformen und Anwendungen innerhalb des Unternehmens ist möglich, indem Amazon Elastic Compute Cloud (Amazon EC2) - Instances mit AWS Systems Manager verwaltet werden. Verwenden Sie AWS Systems Manager, um detaillierte Systemkonfigurationen, Betriebssystem-Patch-Levels, Namen und Typ der Dienste, Softwareinstallationen, Anwendungsname, Herausgeber und Version sowie andere Details zu Ihrer Umgebung bereitzustellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SI-2: Behebung von Fehlern (IRS-definiert)	Die Agentur stellt sicher, dass beim täglichen Einschalten und beim Anschluss an das Netzwerk der Agentur die Arbeitsstationen (wie in den Richtlinien definiert, einschließlich Fernverbindungen über GFE-Workstations) überprüft werden, um sicherzustellen, dass die neuesten von der Behörde genehmigten Patches installiert wurden und dass alle fehlenden oder neuen Patches bei Bedarf installiert oder auf andere Weise überprüft werden, mindestens alle 24 Stunden (außer an Wochenenden, Feiertagen usw.).	managedinstance-association-compliance-statusec2- -check	Verwenden Sie AWS Systems Manager Associations, um bei der Inventarisierung von Softwareplattformen und Anwendungen innerhalb eines Unternehmens zu helfen. AWS Systems Manager weist Ihren verwalteten Instanzen einen Konfigurationsstatus zu und ermöglicht es Ihnen, Basiswerte für Betriebssystem-Patch-Levels, Softwareinstallationen, Anwendungskonfigurationen und andere Details zu Ihrer Umgebung festzulegen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SI-2: Behebung von Fehlern (IRS-definiert)	Die Agentur stellt sicher, dass beim täglichen Einschalten und beim Anschluss an das Netzwerk der Agentur die Arbeitsstationen (wie in den Richtlinien definiert, einschließlich Fernverbindungen über GFE-Workstations) überprüft werden, um sicherzustellen, dass die neuesten von der Behörde genehmigten Patches installiert wurden und dass alle fehlenden oder neuen Patches bei Bedarf installiert oder auf andere Weise überprüft werden, mindestens alle 24 Stunden (außer an Wochenenden, Feiertagen usw.).	managedinstance-patch-compliance-statusec2- -check	Aktivieren Sie diese Regel, um bei der Identifizierung und Dokumentation von Sicherheitslücken in Amazon Elastic Compute Cloud (Amazon EC2) zu helfen. Die Regel prüft, ob die EC2 Amazon-Instance die Patch-Konformität im AWS Systems Manager gemäß den Richtlinien und Verfahren Ihrer Organisation einhält.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SI-2: Behebung von Fehlern (IRS-definiert)	Die Agentur stellt sicher, dass beim täglichen Einschalten und beim Anschluss an das Netzwerk der Agentur die Arbeitsstationen (wie in den Richtlinien definiert, einschließlich Fernverbindungen über GFE-Workstations) überprüft werden, um sicherzustellen, dass die neuesten von der Behörde genehmigten Patches installiert wurden und dass alle fehlenden oder neuen Patches bei Bedarf installiert oder auf andere Weise überprüft werden, mindestens alle 24 Stunden (außer an Wochenenden, Feiertagen usw.).	ecs-fargate-latest-platform-Version	Sicherheitsupdates und Patches werden automatisch für Ihre AWS Fargate-Aufgaben bereitgestellt. Wenn ein Sicherheitsproblem gefunden wird, das eine AWS Fargate-Plattformversion betrifft, AWS wird die Plattformversion gepatcht. Um Sie bei der Patchverwaltung Ihrer Amazon Elastic Container Service (ECS) - Aufgaben zu unterstützen, auf denen AWS Fargate ausgeführt wird, aktualisieren Sie Ihre eigenständigen Service-Aufgaben, sodass sie die neueste Plattformversion verwenden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SI-2: Behebung von Fehlern (IRS-definiert)	Die Agentur stellt sicher, dass beim täglichen Einschalten und beim Anschluss an das Netzwerk der Agentur die Arbeitsstationen (wie in den Richtlinien definiert, einschließlich Fernverbindungen über GFE-Workstations) überprüft werden, um sicherzustellen, dass die neuesten von der Behörde genehmigten Patches installiert wurden und dass alle fehlenden oder neuen Patches bei Bedarf installiert oder auf andere Weise überprüft werden, mindestens alle 24 Stunden (außer an Wochenenden, Feiertagen usw.).	elastic-beanstalk-managed-updates-aktiviert	Durch die Aktivierung verwalteter Plattform updates für eine Amazon-Elastic-Beanstalk-Umgebung wird sichergestellt, dass die aktuellen verfügbaren Plattform-Fixes, -Updates und -Features für die Umgebung installiert sind. Eine bewährte Methode zur Sicherung von Systemen besteht darin, stets die aktuellen Patches zu installieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SI-2: Behebung von Fehlern (IRS-definiert)	Die Agentur stellt sicher, dass bei täglichem Einschalten und Anschluss an das Netzwerk der Agentur die Arbeitsstationen (wie in den Richtlinien definiert, einschließlich Fernverbindungen über GFE-Workstations) überprüft werden, um sicherzustellen, dass die neuesten von der Behörde genehmigten Patches installiert wurden und dass alle fehlenden oder neuen Patches bei Bedarf installiert oder auf andere Weise überprüft werden, und zwar mindestens alle 24 Stunden (außer an Wochenenden, Feiertagen usw.)	rds-automatic-minor-version-Upgrade-fähig	Aktivieren Sie automatische Unterversions-Upgrades auf Ihren Amazon-Relational-Database-Service (RDS)-Instances, um sicherzustellen, dass die aktuellen Updates für Unterversionen des Relational Database Management System (RDBMS) installiert sind, die Sicherheitspatches und Bugfixes enthalten können.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SI-4: Systemüberwachung	Die Organisation: a. Überwacht das Informationssystem und erkennt: 1. Angriffe und Anzeichen für potenzielle Angriffe gemäß [Zuordnung: von der Organisation festgelegte Überwachungsziele]; und 2. nicht autorisierte lokale Verbindungen, Netzwerkverbindungen und Remoteverbindungen; b. Sie identifiziert die unbefugte Nutzung des Informationssystems durch [Zuordnung: von der Organisation festgelegte Techniken und Methoden]; c. Sie verwendet Überwachungsgeräte: 1. Strategisch innerhalb des Informationssystems, um von der Organisation festgelegte wichtige Informationen zu sammeln;	guardduty-enabled-centralized	Amazon GuardDuty kann mithilfe von Threat Intelligence Feeds helfen, potenzielle Cybersicherheitsereignisse zu überwachen und zu erkennen. Dazu gehören Listen mit bösartigen IPs und maschinellen Lernmethoden zur Identifizierung unerwarteter, nicht autorisierter und bösartiger Aktivitäten in Ihrer AWS Cloud-Umgebung.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	und 2. An Ad-hoc-Stellen innerhalb des Systems, um bestimmte Arten von Vorgängen zu verfolgen, die für das Unternehmen von Interesse sind; d. Schützt Informati onen, die mit Tools zur Überwachung von Angriffen gewonnen werden, vor unbefugte m Zugriff, Änderung und Löschung;		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SI-4: Systemüberwachung	Die Organisation: a. Überwacht das Informationssystem und erkennt: 1. Angriffe und Anzeichen für potenzielle Angriffe gemäß [Zuordnung: von der Organisation festgelegte Überwachungsziele]; und 2. nicht autorisierte lokale Verbindungen, Netzwerkverbindungen und Remoteverbindungen; b. Sie identifiziert die unbefugte Nutzung des Informationssystems durch [Zuordnung: von der Organisation festgelegte Techniken und Methoden]; c. Sie verwendet Überwachungsgeräte: 1. Strategisch innerhalb des Informationssystems, um von der Organisation festgelegte wichtige Informationen zu sammeln;	securityhub-enabled	AWS Security Hub hilft bei der Überwachung von unbefugtem Personal, Verbindungen, Geräten und Software. AWS Security Hub aggregiert, organisiert und priorisiert die Sicherheitswarnungen oder Ergebnisse mehrerer Dienste. AWS Einige dieser Dienste sind Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer und AWS Firewall Manager sowie AWS Partnerlösungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	und 2. An Ad-hoc-Stellen innerhalb des Systems, um bestimmte Arten von Vorgängen zu verfolgen, die für das Unternehmen von Interesse sind; d. Schützt Informati onen, die mit Tools zur Überwachung von Angriffen gewonnen werden, vor unbefugte m Zugriff, Änderung und Löschung;		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SI-4: Systemüberwachung	Die Organisation: a. Überwacht das Informationssystem und erkennt: 1. Angriffe und Anzeichen für potenzielle Angriffe gemäß [Zuordnung: von der Organisation festgelegte Überwachungsziele]; und 2. nicht autorisierte lokale Verbindungen, Netzwerkverbindungen und Remoteverbindungen; b. Sie identifiziert die unbefugte Nutzung des Informationssystems durch [Zuordnung: von der Organisation festgelegte Techniken und Methoden]; c. Sie verwendet Überwachungsgeräte: 1. Strategisch innerhalb des Informationssystems, um von der Organisation festgelegte wichtige Informationen zu sammeln;	cloudwatch-alarm-action-check	Amazon CloudWatch alarmiert, wenn eine Metrik den Schwellenwert für eine bestimmte Anzahl von Bewertungszeiträumen überschreitet. Der Alarm führt eine oder mehrere Aktionen durch, die vom Wert der Metrik oder des Ausdrucks im Vergleich zu einem Schwellenwert in einer Reihe von Zeiträumen abhängt. Diese Regel erfordert einen Wert für alarmActionRequired (Config Default: True), insufficientDataAction Required (Config Default: True), okActionRequired (Config Default: False). Der tatsächliche Wert muss die Alarmaktionen für Ihre Umgebung widerspiegeln.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	und 2. An Ad-hoc-Stellen innerhalb des Systems, um bestimmte Arten von Vorgängen zu verfolgen, die für das Unternehmen von Interesse sind; d. Schützt Informati onen, die mit Tools zur Überwachung von Angriffen gewonnen werden, vor unbefugte m Zugriff, Änderung und Löschung;		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SI-4: Systemüberwachung	Die Organisation: a. Überwacht das Informationssystem und erkennt: 1. Angriffe und Anzeichen für potenzielle Angriffe gemäß [Zuordnung: von der Organisation festgelegte Überwachungsziele]; und 2. nicht autorisierte lokale Verbindungen, Netzwerkverbindungen und Remoteverbindungen; b. Sie identifiziert die unbefugte Nutzung des Informationssystems durch [Zuordnung: von der Organisation festgelegte Techniken und Methoden]; c. Sie verwendet Überwachungsgeräte: 1. Strategisch innerhalb des Informationssystems, um von der Organisation festgelegte wichtige Informationen zu sammeln;	cloud-trail-cloud-watch-logs-aktiviert	Verwenden Sie Amazon CloudWatch , um Protokollereignisaktivitäten zentral zu sammeln und zu verwalten. Die Aufnahme von AWS CloudTrail Daten liefert Einzelheiten zu den API-Aufrufaktivitäten in Ihrem AWS-Konto.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	und 2. An Ad-hoc-Stellen innerhalb des Systems, um bestimmte Arten von Vorgängen zu verfolgen, die für das Unternehmen von Interesse sind; d. Schützt Informati onen, die mit Tools zur Überwachung von Angriffen gewonnen werden, vor unbefugte m Zugriff, Änderung und Löschung;		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SI-4: Systemüberwachung	Die Organisation: a. Überwacht das Informationssystem und erkennt: 1. Angriffe und Anzeichen für potenzielle Angriffe gemäß [Zuordnung: von der Organisation festgelegte Überwachungsziele]; und 2. nicht autorisierte lokale Verbindungen, Netzwerkverbindungen und Remoteverbindungen; b. Sie identifiziert die unbefugte Nutzung des Informationssystems durch [Zuordnung: von der Organisation festgelegte Techniken und Methoden]; c. Sie verwendet Überwachungsgeräte: 1. Strategisch innerhalb des Informationssystems, um von der Organisation festgelegte wichtige Informationen zu sammeln;	ec-2 instance-detailed-monitoring-enabled	Aktivieren Sie diese Regel, um die Amazon Elastic Compute Cloud (Amazon EC2) - Instance-Überwachung auf der EC2 Amazon-Konsole zu verbessern, in der Monitoring-Diagramme mit einem Zeitraum von 1 Minute für die Instance angezeigt werden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	und 2. An Ad-hoc-Stellen innerhalb des Systems, um bestimmte Arten von Vorgängen zu verfolgen, die für das Unternehmen von Interesse sind; d. Schützt Informati onen, die mit Tools zur Überwachung von Angriffen gewonnen werden, vor unbefugte m Zugriff, Änderung und Löschung;		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SI-4: Systemübe rwachung (IRS-defi niert)	Alle Internetz ugangspunkte/ Portale müssen Header-Information en über eingehend en und ausgehend en Datenverk ehr erfassen und mindestens ein Jahr lang speichern, mit Ausnahme zugelasse ner „anonymer“ Internetverbindung en, die vom CISO der Behörde genehmigt werden können.	elb-logging-enabled	Die Elastic-Load-Balancing-Aktivität ist ein zentraler Kommunikationspunk t innerhalb einer Umgebung. Stellen Sie sicher, dass die ELB-Protokollierun g aktiviert ist. Die gesammelten Daten enthalten detaillie rte Informationen zu Anfragen, die an den ELB gesendet wurden. Jedes Protokoll enthält Informationen wie die Zeit, zu der die Anforderung einging, die Client-IP -Adresse, Latenzen, Anforderungspfade und Serverantworten.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SI-4: Systemüberwachung (IRS-definiert)	Alle Internetzugangspunkte/Portale müssen Header-Informationen über eingehenden und ausgehenden Datenverkehr erfassen und mindestens ein Jahr lang speichern, mit Ausnahme zugelassener „anonymer“ Internetverbindungen, die vom CISO der Behörde genehmigt werden können.	opensearch-audit-logging-enabled	Stellen Sie sicher, dass die Audit-Protokollierung für Ihre Amazon OpenSearch Service-Domains aktiviert ist. Mit der Audit-Protokollierung können Sie Benutzeraktivitäten auf Ihren OpenSearch Domains verfolgen, einschließlich erfolgreicher und fehlgeschlagener Authentifizierungen OpenSearch, Anfragen an, Indexänderungen und eingehende Suchanfragen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SI-4: Systemübe rwachung (IRS-defi niert)	Alle Internetz ugangspunkte/ Portale müssen Header-Information en über eingehend en und ausgehend en Datenverk ehr erfassen und mindestens ein Jahr lang speichern, mit Ausnahme zugelasse ner „anonymer“ Internetverbindung en, die vom CISO der Behörde genehmigt werden können.	redshift-audit-logging-enabled	Aktivieren Sie die Prüfungsprotokolli erung, um Informati onen über Verbindun gen und Benutzera ktivitäten in Ihrem Amazon-Redshift-Cl uster zu erfassen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SI-4: Systemüberwachung (IRS-definiert)	Alle Internetzugangspunkte/Portale müssen Header-Informationen über eingehende und ausgehende Datenverkehr erfassen und mindestens ein Jahr lang speichern, mit Ausnahme zugelassener „anonymer“ Internetverbindungen, die vom CISO der Behörde genehmigt werden können.	s3- bucket-logging-enabled	Die Amazon Simple Storage Service (Amazon S3)-Serverzugriffsprotokollierung bietet eine Methode zur Überwachung des Netzwerks im Hinblick auf potenzielle Cybersicherheitsereignisse. Die Ereignisse werden überwacht, indem detaillierte Aufzeichnungen über die Anfragen erfasst werden, die an einen Amazon-S3-Bucket gestellt wurden. Jeder Zugriffsprotokolleintrag enthält Details zu einer einzelnen Zugriffsanfrage. Zu den Details gehören Anforderer, Bucket-Name, Anforderungszeit, Anforderungsaktion, Antwortstatus und Fehlercode, falls relevant.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SI-4: Systemübe rwachung (IRS-defi niert)	Alle Internetz ugangspunkte/ Portale müssen Header-Information en über eingehend en und ausgehend en Datenverk ehr erfassen und mindestens ein Jahr lang speichern, mit Ausnahme zugelasse ner „anonymer“ Internetverbindung en, die vom CISO der Behörde genehmigt werden können.	wafv2-logging-enab led	Um die Protokoll ierung und Überwachung in Ihrer Umgebung zu erleichtern, aktiviere n Sie die AWS WAF (V2) -Protokol lierung im regionale n und globalen Web ACLs. AWS Die WAF-Protokollierun g bietet detaillierte Informationen über den Datenverkehr, der von Ihrer Web-ACL analysiert wird. In den Protokollen werden die Uhrzeit aufgezeic hnet, zu der die AWS WAF die Anfrage von Ihrer AWS Ressource erhalten hat, Informati onen über die Anfrage und eine Aktion für die Regel, der jede Anfrage entsprach.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SI-4: Systemüberwachung (IRS-definiert)	Alle Internetzugangspunkte/Portale müssen Header-Informationen über eingehenden und ausgehenden Datenverkehr erfassen und mindestens ein Jahr lang speichern, mit Ausnahme zugelassener „anonymer“ Internetverbindungen, die vom CISO der Behörde genehmigt werden können.	vpc-flow-logs-enabled	VPC-Flow-Protokolle erfassen detaillierte Informationsdatensätze über den IP-Datenverkehr, der zu und von Netzwerkschnittstellen in Ihrer Amazon Virtual Private Cloud (Amazon VPC) fließt. Standardmäßig enthalten Flow-Protokolldatensätze Werte für die verschiedenen Komponenten des IP-Flows, einschließlich Quelle, Ziel und Protokoll.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SI-4: Systemüberwachung (IRS-definiert)	Alle Internetzugangspunkte/Portale müssen Header-Informationen über eingehende und ausgehende Datenverkehr erfassen und mindestens ein Jahr lang speichern, mit Ausnahme zugelassener „anonymer“ Internetverbindungen, die vom CISO der Behörde genehmigt werden können.	api-gw-execution-logging-aktiviert	Die API-Gateway-Protokollierung zeigt detaillierte Ansichten der Benutzer, die auf die API zugegriffen haben, und wie diese Benutzer auf die API zugegriffen haben. Diese Einblicke ermöglichen die Transparenz von Benutzeraktivitäten.
SI-4: Systemüberwachung (IRS-definiert)	Alle Internetzugangspunkte/Portale müssen Header-Informationen über eingehende und ausgehende Datenverkehr erfassen und mindestens ein Jahr lang speichern, mit Ausnahme zugelassener „anonymer“ Internetverbindungen, die vom CISO der Behörde genehmigt werden können.	cloud-trail-cloud-watch-logs-aktiviert	Verwenden Sie Amazon CloudWatch , um Protokollereignisaktivitäten zentral zu sammeln und zu verwalten. Die Aufnahme von AWS CloudTrail Daten liefert Einzelheiten zu den API-Aufrufaktivitäten in Ihrem AWS-Konto.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SI-4: Systemüberwachung (IRS-definiert)	Alle Internetzugangspunkte/Portale müssen Header-Informationen über eingehende und ausgehende Datenverkehr erfassen und mindestens ein Jahr lang speichern, mit Ausnahme zugelassener „anonymer“ Internetverbindungen, die vom CISO der Behörde genehmigt werden können.	cloudtrail-enabled	AWS CloudTrail kann bei der Nichtabstreitbarkeit helfen, indem Aktionen und API-Aufrufe der AWS Management Console aufgezeichnet werden. Sie können die Benutzer und die Benutzer AWS-Konten , die einen AWS Dienst aufgerufen haben, die Quell-IP-Adresse, über die die Aufrufe generiert wurden, und den Zeitpunkt der Anrufe identifizieren. Einzelheiten zu den erfassten Daten finden Sie in den AWS CloudTrail Datensatzinhalten.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SI-4: Systemübe rwachung (IRS-defi niert)	Alle Internetz ugangspunkte/ Portale müssen Header-Information en über eingehend en und ausgehend en Datenverk ehr erfassen und mindestens ein Jahr lang speichern, mit Ausnahme zugelasse ner „anonymer“ Internetverbindung en, die vom CISO der Behörde genehmigt werden können.	cloud-trail-log-file-Validierung aktiviert	Verwenden Sie die AWS CloudTrail Protokolldateivali dierung, um die Integrität von Protokoll en zu überprüfen. CloudTrail Mithilfe der Protokolldateivali dierung kann festgestellt werden, ob eine Protokoll datei geändert oder gelöscht wurde oder ob sie nach der Übermittlung CloudTrail unverände rt geblieben ist. Dieses Feature wurde mit dem Branchens tandard entsprech enden Algorithmen entwickelt: SHA-256 für die Hashfunktion und SHA-256 mit RSA für digitale Signature n. Aus diesem Grund ist es rechnerisch unmöglich, CloudTrai l Protokolldateien unbemerkt zu ändern, zu löschen oder zu fälschen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SI-4: Systemüberwachung (IRS-definiert)	Alle Internetzugangspunkte/Portale müssen Header-Informationen über eingehende und ausgehende Datenverkehr erfassen und mindestens ein Jahr lang speichern, mit Ausnahme zugelassener „anonymer“ Internetverbindungen, die vom CISO der Behörde genehmigt werden können.	cw-loggroup-retention-period-überprüfen	Stellen Sie sicher, dass die Ereignisprotokolldaten für Ihre Protokollgruppen über eine Mindestdauer aufbewahrt werden, um die Fehlerbehebung und forensische Untersuchungen zu unterstützen. Fehlende frühere Ereignisprotokolldaten erschweren die Rekonstruierung und Identifizierung potenziell schädlicher Ereignisse.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SI-7: Software-, Firmware- und Informationsintegrität	Verwenden Sie Tools zur Integritätsprüfung, um unbefugte Änderungen an der folgenden Software, Firmware und Informationen zu erkennen: Systemkernel, Treiber, Firmware (z. B. BIOS, UEFI), Software (z. B. Betriebssystem, Anwendungen, Middleware) und Sicherheitsattributen.	ec2-manager instance-managed-by-systems	Eine Bestandsaufnahme der Softwareplattformen und Anwendungen innerhalb des Unternehmens ist möglich, indem Amazon Elastic Compute Cloud (Amazon EC2) - Instances mit AWS Systems Manager verwaltet werden. Verwenden Sie AWS Systems Manager, um detaillierte Systemkonfigurationen, Betriebssystem-Patch-Levels, Namen und Typ der Dienste, Softwareinstallationen, Anwendungsname, Herausgeber und Version sowie andere Details zu Ihrer Umgebung bereitzustellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SI-7: Software-, Firmware- und Informationsintegrität	Verwenden Sie Tools zur Integritätsprüfung, um unbefugte Änderungen an der folgenden Software, Firmware und Informationen zu erkennen: Systemkernel, Treiber, Firmware (z. B. BIOS, UEFI), Software (z. B. Betriebssystem, Anwendungen, Middleware) und Sicherheitsattributen.	ec2- -check managedinstance-patch-compliance-status	Aktivieren Sie diese Regel, um bei der Identifizierung und Dokumentation von Sicherheitslücken in Amazon Elastic Compute Cloud (Amazon EC2) zu helfen. Die Regel prüft, ob die EC2 Amazon-Instance die Patch-Konformität im AWS Systems Manager gemäß den Richtlinien und Verfahren Ihrer Organisation einhält.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SI-7: Software-, Firmware- und Informationsintegrität	Verwenden Sie Tools zur Integritätsprüfung, um unbefugte Änderungen an der folgenden Software, Firmware und Informationen zu erkennen: Systemkerne, Treiber, Firmware (z. B. BIOS, UEFI), Software (z. B. Betriebssystem, Anwendungen, Middleware) und Sicherheitsattributen.	cloud-trail-log-file-Validierung aktiviert	Verwenden Sie die AWS CloudTrail Protokolldateivalidierung, um die Integrität von Protokollen zu überprüfen. CloudTrail Mithilfe der Protokolldateivalidierung kann festgestellt werden, ob eine Protokolldatei geändert oder gelöscht wurde oder ob sie nach der Übermittlung CloudTrail unverändert geblieben ist. Dieses Feature wurde mit dem Branchenstandard entsprechenden Algorithmen entwickelt: SHA-256 für die Hashfunktion und SHA-256 mit RSA für digitale Signaturen. Aus diesem Grund ist es rechnerisch unmöglich, CloudTrail Protokolldateien unbemerkt zu ändern, zu löschen oder zu fälschen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SI-12: Informati onsmanagement und Aufbewahrung	Verarbeiten und speichern Sie die Informationen innerhalb des Informationssystem s und die aus dem System ausgegebe nen Informati onen gemäß den geltenden Bundesges etzen, Verordnun gen, Richtlinien, Richtlinien, Vorschrif ten, Standards und betrieblichen Anforderungen.	db-instance-backup-enabled	Die Sicherung sfunktion von Amazon RDS erstellt Sicherung en Ihrer Datenbank en und Transakti onsprotokolle. Amazon RDS erstellt einen Snapshot für das Speichervolume Ihrer DB-Instance, sodass die gesamte DB-Instance gesichert wird. Sie können im System spezifische Aufbewahrungsfrist en festlegen, um Ihre Ausfallsicherheits anforderungen zu erfüllen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SI-12: Informati onsmanagement und Aufbewahrung	Verarbeiten und speichern Sie die Informationen innerhalb des Informationssystem s und die aus dem System ausgegebe nen Informati onen gemäß den geltenden Bundesges etzen, Verordnun gen, Richtlinien, Richtlinien, Vorschrif ten, Standards und betrieblichen Anforderungen.	dynamodb-in-backup-plan	Um Sie bei Datensich erungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon DynamoDB-Tabellen Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwaltet er Backup-Service mit einer richtlini enbasierten Backup-Lösung. Diese Lösung vereinfac ht Ihr Sicherung smanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforde rungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SI-12: Informati onsmanagement und Aufbewahrung	Verarbeiten und speichern Sie die Informationen innerhalb des Informationssystem s und die aus dem System ausgegebe nen Informati onen gemäß den geltenden Bundesges etzen, Verordnun gen, Richtlinien, Richtlinien, Vorschrif ten, Standards und betrieblichen Anforderungen.	dynamodb-pitr-enab led	Aktivieren Sie diese Regel, um zu überprüfen, ob die Informationen gesichert wurden. Es verwaltet auch die Backups, indem es sicherstellt, dass die point-in-time Wiederherstellung in Amazon DynamoDB aktiviert ist. Bei der Wiederherstellung werden fortlaufende Backups Ihrer Tabelle für die letzten 35 Tage gespeichert.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SI-12: Informati onsmanagement und Aufbewahrung	Verarbeiten und speichern Sie die Informationen innerhalb des Informationssystem s und die aus dem System ausgegebe nen Informati onen gemäß den geltenden Bundesges etzen, Verordnun gen, Richtlinien, Richtlinien, Vorschrif ten, Standards und betrieblichen Anforderungen.	dynamodb-resources-protected-by-Backup-Plan	Um Sie bei Datensich erungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon DynamoDB DynamoDB-Ressourcen Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwaltet er Backup-Service mit einer richtlini enbasierten Backup-Lösung. Diese Lösung vereinfac ht Ihr Sicherung smanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforde rungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SI-12: Informati onsmanagement und Aufbewahrung	Verarbeiten und speichern Sie die Informationen innerhalb des Informationssystem s und die aus dem System ausgegebe nen Informati onen gemäß den geltenden Bundesges etzen, Verordnun gen, Richtlinien, Richtlinien, Vorschrif ten, Standards und betrieblichen Anforderungen.	ebs-in-backup-plan	Stellen Sie zur Unterstützung der Datensicherungspro zesse sicher, dass Ihre Amazon Elastic Block Store (Amazon EBS) -Volumes Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwaltet er Backup-Service mit einer richtlini enbasierten Backup-Lösung. Diese Lösung vereinfac ht Ihr Sicherung smanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforde rungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SI-12: Informati onsmanagement und Aufbewahrung	Verarbeiten und speichern Sie die Informationen innerhalb des Informationssystem s und die aus dem System ausgegebe nen Informati onen gemäß den geltenden Bundesges etzen, Verordnun gen, Richtlinien, Richtlinien, Vorschrif ten, Standards und betrieblichen Anforderungen.	ebs-resources-prot ected-by-Backup-Plan	Um Sie bei Datensich erungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon Elastic Block Store (Amazon EBS) -Ressourc en Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwaltet er Backup-Service mit einer richtlini enbasierten Backup-Lösung. Diese Lösung vereinfac ht Ihr Sicherung smanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforde rungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SI-12: Informati onsmanagement und Aufbewahrung	Verarbeiten und speichern Sie die Informationen innerhalb des Informationssystem s und die aus dem System ausgegebe nen Informati onen gemäß den geltenden Bundesges etzen, Verordnun gen, Richtlinien, Richtlinien, Vorschrif ten, Standards und betrieblichen Anforderungen.	ec2--Plan resources-protected-by-backup	Um Sie bei Datensich erungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon Elastic Compute Cloud (Amazon EC2) -Ressourc en Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwaltet er Backup-Service mit einer richtlini enbasierten Backup-Lösung. Diese Lösung vereinfac ht Ihr Sicherung smanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforde rungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SI-12: Informati onsmanagement und Aufbewahrung	Verarbeiten und speichern Sie die Informationen innerhalb des Informationssystem s und die aus dem System ausgegebe nen Informati onen gemäß den geltenden Bundesges etzen, Verordnun gen, Richtlinien, Richtlinien, Vorschrif ten, Standards und betrieblichen Anforderungen.	efs-in-backup-plan	Um Sie bei Datensich erungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon Elastic File System (Amazon EFS) -Dateisysteme Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwaltet er Backup-Service mit einer richtlini enbasierten Backup-Lösung. Diese Lösung vereinfac ht Ihr Sicherung smanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforde rungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SI-12: Informati onsmanagement und Aufbewahrung	Verarbeiten und speichern Sie die Informationen innerhalb des Informationssystem s und die aus dem System ausgegebe nen Informati onen gemäß den geltenden Bundesges etzen, Verordnun gen, Richtlinien, Richtlinien, Vorschrif ten, Standards und betrieblichen Anforderungen.	efs-resources-prot ected-by-Backup-Plan	Um Sie bei Datensich erungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon Elastic File System (Amazon EFS) -Dateisysteme Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwaltet er Backup-Service mit einer richtlini enbasierten Backup-Lösung. Diese Lösung vereinfac ht Ihr Sicherung smanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforde rungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SI-12: Informati onsmanagement und Aufbewahrung	Verarbeiten und speichern Sie die Informationen innerhalb des Informationssystem s und die aus dem System ausgegebe nen Informati onen gemäß den geltenden Bundesges etzen, Verordnun gen, Richtlinien, Richtlinien, Vorschrif ten, Standards und betrieblichen Anforderungen.	elasticache-redis-cluster-automatic-Backup-Check	Wenn automatische Backups aktiviert sind, ElastiCache erstellt Amazon täglich ein Backup des Clusters. Die Sicherung kann für eine von Ihrer Organisation festgelegte Anzahl von Tagen aufbewahrt werden. Automatische Backups schützen vor Datenverlust. Bei einem Ausfall können Sie einen neuen Cluster erstellen, der Ihre Daten aus dem aktuellen Backup wiederherstellt.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SI-12: Informati onsmanagement und Aufbewahrung	Verarbeiten und speichern Sie die Informationen innerhalb des Informationssystem s und die aus dem System ausgegebe nen Informati onen gemäß den geltenden Bundesges etzen, Verordnun gen, Richtlinien, Richtlinien, Vorschrif ten, Standards und betrieblichen Anforderungen.	fsx-resources-prot ected-by-Backup-Plan	Um Sie bei Datensich erungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre FSx Amazon-Dateisysteme Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwaltet er Backup-Service mit einer richtlini enbasierten Backup-Lösung. Diese Lösung vereinfac ht Ihr Sicherung smanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforde rungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SI-12: Informati onsmanagement und Aufbewahrung	Verarbeiten und speichern Sie die Informationen innerhalb des Informationssystem s und die aus dem System ausgegebe nen Informati onen gemäß den geltenden Bundesges etzen, Verordnun gen, Richtlinien, Richtlinien, Vorschrif ten, Standards und betrieblichen Anforderungen.	rds-in-backup-plan	Um Sie bei Datensich erungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon Relational Database Service (Amazon RDS) -Instance s Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwaltet er Backup-Service mit einer richtlini enbasierten Backup-Lösung. Diese Lösung vereinfac ht Ihr Sicherung smanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforde rungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SI-12: Informati onsmanagement und Aufbewahrung	Verarbeiten und speichern Sie die Informationen innerhalb des Informationssystem s und die aus dem System ausgegebe nen Informati onen gemäß den geltenden Bundesges etzen, Verordnun gen, Richtlinien, Richtlinien, Vorschrif ten, Standards und betrieblichen Anforderungen.	rds-resources-prot ected-by-Backup-Plan	Um Sie bei Datensich erungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon Relational Database Service (Amazon RDS) -Ressourc en Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwaltet er Backup-Service mit einer richtlini enbasierten Backup-Lösung. Diese Lösung vereinfac ht Ihr Sicherung smanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforde rungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SI-12: Informati onsmanagement und Aufbewahrung	Verarbeiten und speichern Sie die Informationen innerhalb des Informationssystem s und die aus dem System ausgegebe nen Informati onen gemäß den geltenden Bundesges etzen, Verordnun gen, Richtlinien, Richtlinien, Vorschrif ten, Standards und betrieblichen Anforderungen.	redshift-backup-en abled	Stellen Sie zur Unterstützung der Datensicherungspro zesse sicher, dass Ihre Amazon-Re dshift-Cluster über automatisierte Snapshots verfügen. Wenn automatis ierte Snapshots für einen Cluster aktiviert sind, erstellt Redshift in regelmäßi gen Abständen Snapshots dieses Clusters. Standardm äßig erstellt Redshift alle acht Stunden oder alle 5 GB einen Snapshot für jeden Knoten mit Datenände rungen oder je nachdem, was zuerst eintritt.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SI-12: Informati onsmanagement und Aufbewahrung	Verarbeiten und speichern Sie die Informationen innerhalb des Informationssystem s und die aus dem System ausgegebe nen Informati onen gemäß den geltenden Bundesges etzen, Verordnun gen, Richtlinien, Richtlinien, Vorschrif ten, Standards und betrieblichen Anforderungen.	aurora-resources-p rotected-by-Backup-Plan	Um Sie bei Datensich erungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon Aurora Aurora-Ressourcen Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwaltet er Backup-Service mit einer richtlini enbasierten Backup-Lösung. Diese Lösung vereinfac ht Ihr Sicherung smanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforde rungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SI-12: Informati onsmanagement und Aufbewahrung	Verarbeiten und speichern Sie die Informationen innerhalb des Informationssystem s und die aus dem System ausgegebe nen Informati onen gemäß den geltenden Bundesges etzen, Verordnun gen, Richtlinien, Richtlinien, Vorschrif ten, Standards und betrieblichen Anforderungen.	backup-plan-min-fr equency-and-min-re tention-check	Um Sie bei Datensich erungsprozessen zu unterstützen, stellen Sie sicher, dass Ihr AWS Backup-Plan auf eine Mindestfrequenz und Aufbewahr ung festgelegt ist. AWS Backup ist ein vollständig verwaltet er Backup-Service mit einer richtlini enbasierten Backup-Lösung. Diese Lösung vereinfac ht Ihr Sicherung smanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforde rungen hinsichtlich Datensicherungen. Mit dieser Regel können Sie die Parameter requiredF requencyValue (Config default: 1), requiredRetentionD ays (Config default: 35) und requiredF requencyUnit

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			(Config default: days) festlegen. Der tatsächliche Wert muss den Anforderungen Ihrer Organisation entsprechen.
SI-12: Informationsmanagement und Aufbewahrung	Verarbeiten und speichern Sie die Informationen innerhalb des Informationssystems und die aus dem System ausgegebenen Informationen gemäß den geltenden Bundesgesetzen, Verordnungen, Richtlinien, Richtlinien, Vorschriften, Standards und betrieblichen Anforderungen.	backup-recovery-point-manual-löschen-deaktiviert	Stellen Sie sicher, dass Ihren AWS Backup-Wiederherstellungspunkten eine ressourcenbasierte Richtlinie zugeordnet ist, die das Löschen von Wiederherstellungspunkten verhindert. Die Verwendung einer ressourcenbasierten Richtlinie zur Verhinderung des Löschens von Wiederherstellungspunkten kann dazu beitragen, ein versehentliches oder absichtliches Löschen zu unterbinden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SI-12: Informati onsmanagement und Aufbewahrung	Verarbeiten und speichern Sie die Informationen innerhalb des Informationssystem s und die aus dem System ausgegebe nen Informati onen gemäß den geltenden Bundesges etzen, Verordnun gen, Richtlinien, Richtlinien, Vorschrif ten, Standards und betrieblichen Anforderungen.	backup-recovery-po int-minimum-Aufbew ahrungsprüfung	Um bei Datensich erungsprozessen zu helfen, stellen Sie sicher, dass für Ihre AWS Backup-Wi ederherstellungspu nkte eine Mindestau fbewahrungsdauer festgelegt ist. AWS Backup ist ein vollständig verwaltet er Backup-Service mit einer richtlini enbasierten Backup-Lösung. Diese Lösung vereinfac ht Ihr Sicherung smanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforde rungen hinsichtlich Datensicherungen. Mit dieser Regel können Sie den Parameter requiredR etentionDays (Config Default: 35) festlegen. Der tatsächliche Wert muss den Anforderu

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			ngen Ihrer Organisat ion entsprechen.
SI-12: Informati onsmanagement und Aufbewahrung	Verarbeiten und speichern Sie die Informationen innerhalb des Informationssystem s und die aus dem System ausgegebe nen Informati onen gemäß den geltenden Bundesges etzen, Verordnun gen, Richtlinien, Richtlinien, Vorschrif ten, Standards und betrieblichen Anforderungen.	s-3 lifecycle-policy-c heck	Mit Amazon-S3-Lebenszyklusregeln können Sie Aktionen definieren, die Amazon S3 während der Lebensdau er eines Objekts ausführen soll (z. B. die Überführu ng von Objekten in eine andere Speicherklasse, ihre Archivierung oder Löschung nach einem bestimmten Zeitraum) .

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SI-12: Informati onsmanagement und Aufbewahrung	Verarbeiten und speichern Sie die Informationen innerhalb des Informationssystem s und die aus dem System ausgegebe nen Informati onen gemäß den geltenden Bundesges etzen, Verordnun gen, Richtlinien, Richtlinien, Vorschrif ten, Standards und betrieblichen Anforderungen.	s-3 version-lifecycle-policy-check	Mit Amazon-S3-Lebenszyklusregeln können Sie Aktionen definieren, die Amazon S3 während der Lebensdau er eines Objekts ausführen soll (z. B. die Überführu ng von Objekten in eine andere Speicherklasse, ihre Archivierung oder Löschung nach einem bestimmten Zeitraum) .

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SI-12: Informati onsmanagement und Aufbewahrung	Verarbeiten und speichern Sie die Informationen innerhalb des Informationssystem s und die aus dem System ausgegebe nen Informati onen gemäß den geltenden Bundesges etzen, Verordnun gen, Richtlinien, Richtlinien, Vorschrif ten, Standards und betrieblichen Anforderungen.	s-3 bucket-versioning-enabled	Die Versionsv erwaltung von Amazon Simple Storage Service (Amazon S3)-Bucke ts hilft dabei, mehrere Varianten eines Objekts im selben Amazon-S3-Bucket zu speichern. Verwenden Sie die Versionsv erwaltung, um sämtliche Versionen aller Objekte in Ihrem Amazon-S3-Bucket zu speichern , abzurufen oder wiederherzustellen . Mit der Versionsv erwaltung können Sie Versionen sowohl nach unbeabsic htigten Benutzera ktionen als auch nach Anwendungsfehlern problemlos wiederher stellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SI-12: Informati onsmanagement und Aufbewahrung	Verarbeiten und speichern Sie die Informationen innerhalb des Informationssystem s und die aus dem System ausgegebe nen Informati onen gemäß den geltenden Bundesges etzen, Verordnun gen, Richtlinien, Richtlinien, Vorschrif ten, Standards und betrieblichen Anforderungen.	s-3 bucket-default-loc k-enabled	Stellen Sie sicher, dass für Ihren Amazon Simple Storage Service (Amazon S3)-Bucke t standardmäßig eine Sperre aktiviert ist. Zum Schutz eventuell vorhanden er sensibler Daten in S3-Buckets müssen Sie Objektsperren für Daten im Ruhezusta nd erzwingen.

Vorlage

Die Vorlage ist verfügbar unter GitHub: Operational Best Practices for IRS 1075.

Bewährte Methoden zur Ausführung von K-ISMS

Konformitätspakete bieten ein allgemeines Compliance-Framework, das es Ihnen ermöglicht, mithilfe verwalteter oder benutzerdefinierter AWS Config Regeln und Abhilfemaßnahmen Kontrollen zur Sicherheits-, Betriebs- oder Kostenoptimierung durchzuführen. AWS Config Conformance Packs dienen als Beispielvorlagen nicht dazu, die vollständige Einhaltung eines bestimmten Governance- oder Compliance-Standards sicherzustellen. Sie sind dafür verantwortlich, selbst zu beurteilen, ob Ihre Nutzung der Services den geltenden gesetzlichen und behördlichen Anforderungen entspricht.

Im Folgenden finden Sie ein Beispiel für eine Zuordnung zwischen Korea — Information Security Management System (ISMS) und AWS verwalteten Konfigurationsregeln. Jede Config-Regel gilt für eine bestimmte AWS -Ressource und bezieht sich auf eine oder mehrere Korea-ISMS-Kontrollen.

Eine Korea-ISMS-Kontrolle kann mehreren Config-Regeln zugeordnet werden. In der folgenden Tabelle finden Sie weitere Informationen und Anleitungen zu diesen Zuordnungen.

Kontroll-ID	AWS Config	Empfehlungen
1.2.1	ec2-check managedinstance-association-compliance-status	Verwenden Sie AWS Systems Manager Associations, um bei der Inventarisierung von Softwareplattformen und Anwendungen innerhalb eines Unternehmens zu helfen. AWS Systems Manager weist Ihren verwalteten Instanzen einen Konfigurationsstatus zu und ermöglicht es Ihnen, Basiswerte für Betriebss ystem-Patch-Levels, Softwarei nstallationen, Anwendung skonfigurationen und andere Details zu Ihrer Umgebung festzulegen.
1.2.1	ec2- volume-inuse-check	Diese Regel stellt sicher, dass Amazon Elastic Block Store-Volumes, die an Amazon Elastic Compute Cloud (Amazon EC2) -Instances angehängt sind, zum Löschen markiert werden, wenn eine Instance beendet wird. Wenn ein Amazon-EBS-Volume nicht gelöscht wird, wenn die Instance, an die es angehängt ist, beendet wird, kann dies gegen das Konzept der geringsten Funktionalität verstoßen.

Kontroll-ID	AWS Config	Empfehlungen
2.1.3	ec2-check managedinstance-association-compliance-status	Verwenden Sie AWS Systems Manager Associations, um bei der Inventarisierung von Softwareplattformen und Anwendungen innerhalb eines Unternehmens zu helfen. AWS Systems Manager weist Ihren verwalteten Instanzen einen Konfigurationsstatus zu und ermöglicht es Ihnen, Basiswerte für Betriebss ystem-Patch-Levels, Softwarei nstallationen, Anwendung skonfigurationen und andere Details zu Ihrer Umgebung festzulegen.
2.1.3	ec2- volume-inuse-check	Diese Regel stellt sicher, dass Amazon Elastic Block Store-Volumes, die an Amazon Elastic Compute Cloud (Amazon EC2) -Instances angehängt sind, zum Löschen markiert werden, wenn eine Instance beendet wird. Wenn ein Amazon-EBS-Volume nicht gelöscht wird, wenn die Instance, an die es angehängt ist, beendet wird, kann dies gegen das Konzept der geringsten Funktionalität verstoßen.

Kontroll-ID	AWS Config	Empfehlungen
2.3.3	cloud-trail-cloud-watch-logs-aktiviert	Verwenden Sie Amazon CloudWatch , um Protokoll ereignisaktivitäten zentral zu sammeln und zu verwalten . Die Aufnahme von AWS CloudTrail Daten liefert Einzelheiten zu den API-Aufru faktivitäten in Ihrem AWS-Konto.
2.3.3	cloudtrail-enabled	AWS CloudTrail kann bei der Nichtabstreitbarkeit helfen, indem Aktionen und API-Aufrufe der AWS Managemen t Console aufgezeichnet werden. Sie können die Benutzer und die Benutzer AWS-Konten , die einen AWS Dienst aufgerufen haben, die Quell-IP-Adresse, über die die Aufrufe generiert wurden, und den Zeitpunkt der Anrufe identifizieren. Einzelheiten zu den erfassten Daten finden Sie in den AWS CloudTrail Datensatzinhalten.

Kontroll-ID	AWS Config	Empfehlungen
2.5.1	access-keys-rotated	Die Anmeldeinformationen für autorisierte Geräte, Benutzer und Prozesse werden geprüft, indem sichergestellt wird, dass die IAM-Zugriffsschlüssel entsprechend den Vorgaben der Unternehmensrichtlinie rotiert werden. Das regelmäßi ge Ändern der Zugriffss chlüssel ist eine bewährte Sicherheitsmethode. Es verkürzt den Zeitraum, in dem ein Zugriffsschlüssel aktiv ist, und reduziert die Auswirkun gen auf das Unternehmen, wenn die Schlüssel kompromit tiert werden. Diese Regel erfordert einen Wert für die Zugriffsschlüssel-Rotation (Standardkonfiguration: 90). Der tatsächliche Wert muss den Richtlinien Ihrer Organisat ion entsprechen.

Kontroll-ID	AWS Config	Empfehlungen
2.5.1	emr-kerberos-enabled	Die Zugriffsberechtigungen und -autorisierungen können verwaltet und nach den Prinzipien der geringsten Berechtigung und Aufgabent rennung integriert werden, indem Kerberos für Amazon-EMR-Cluster aktiviert wird. In Kerberos werden Services und Benutzer, die sich authentifizieren müssen, als Prinzipale bezeichnet. Prinzipale befinden sich in einem Kerberos-Bereich. Innerhalb dieses Bereichs wird ein Kerberos-Server als Key Distribution Center (KDC) bezeichnet. Über diesen Server können sich Prinzipale authentifizieren. Die Authentifizierung im KDC erfolgt durch die Ausstellu ng von Authentifizierungs tickets. Das KDC unterhält eine Datenbank der Prinzipal e in seinem Bereich mit ihren Passwörtern und anderen administrativen Informationen zu jedem Prinzipal.

Kontroll-ID	AWS Config	Empfehlungen
2.5.1	iam-customer-policy-blocked-kms-Aktionen	AWS Identity and Access Management (IAM) kann Ihnen helfen, die Prinzipien der geringsten Rechte und der Aufgabentrennung in Zugriffsberechtigungen und Autorisierungen zu integrier en und so zu verhindern, dass Richtlinien blockierte Aktionen für alle AWS Schlüssel des Key Management Service enthalten. Wenn Benutzer mehr Rechte haben, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtig ung und Aufgabentrennung verstoßen. Mit dieser Regel können Sie den Parameter festlegen. blockedActionsPatt erns (Wert „AWS Bewährte grundlegende Sicherhei tsmethoden“: kms: Decrypt, kms:ReEncryptFrom). Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisat ion entsprechen.

Kontroll-ID	AWS Config	Empfehlungen
2.5.1	iam-group-has-users-überprüfen	AWS Identity and Access Management (IAM) kann Ihnen helfen, die Prinzipien der geringsten Rechte und der Aufgabentrennung mit Zugriffsberechtigungen und Autorisierungen zu integrieren, indem sichergestellt wird, dass IAM-Gruppen mindestens einen Benutzer haben. Die Einteilung von Benutzern in Gruppen auf der Grundlage der ihnen zugewiesenen Berechtigungen oder ihrer Funktion ist eine Möglichkeit, das Prinzip der geringsten Berechtigung zu implementieren.

Kontroll-ID	AWS Config	Empfehlungen
2.5.1	iam-inline-policy-blocked-kms-Aktionen	Stellen Sie sicher, dass ein Benutzer, eine IAM-Rolle oder eine IAM-Grupp e (AWS Identity and Access Management) nicht über eine Inline-Richtlinie verfügt, die blockierte Aktionen für alle AWS Schlüssel des Key Management Service zulässt. AWS empfiehlt, verwaltete Richtlinien anstelle von Inline-Richtlinien zu verwenden . Verwaltete Richtlinien ermöglichen Wiederver wendbarkeit, Versionsv erwaltung, Rollback und Delegierung der Berechtig ungsverwaltung. Mit dieser Regel können Sie den blockedActionsPatterns Parameter festlegen. (Wert „AWS Bewährte grundlege nde Sicherheitsmethoden“: kms: Decrypt, kms:ReEnc ryptFrom). Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprech en.

Kontroll-ID	AWS Config	Empfehlungen
2.5.1	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) kann Ihnen dabei helfen, die Prinzipien der geringsten Rechte und der Aufgabent rennung in Zugriffsberechtigu ngen und Autorisierungen zu integrieren und zu verhinder n, dass Richtlinien „Effect“: „Allow“ mit „Action“: „*“ anstelle von „Resource“: „*“ enthalten. Wenn Benutzern mehr Rechte eingeräumt werden, als für die Ausführun g einer Aufgabe erforderl ich sind, kann dies gegen das Prinzip der geringste n Berechtigung und der Aufgabentrennung verstoßen.
2.5.1	iam-policy-no-statements-with-full-access	Stellen Sie sicher, dass IAM-Aktionen nur auf die benötigte n Aktionen beschränkt sind. Wenn Benutzern mehr Rechte eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und der Aufgabentrennung verstoßen.

Kontroll-ID	AWS Config	Empfehlungen
2.5.1	iam-root-access-key-überprüfen	Der Zugriff auf Systeme und Ressourcen kann gesteuert werden, indem überprüft wird, ob der Root-Benutzer keine Zugriffsschlüssel mit seiner AWS Identity and Access Management (IAM) -Rolle verknüpft hat. Stellen Sie sicher, dass die Root-Zugriffsschlüssel gelöscht werden. Erstellen und verwenden Sie stattdessen rollenbasierte Funktionen, AWS-Konten um das Prinzip der geringsten Funktionalität zu berücksichtigen.
2.5.1	iam-user-mfa-enabled	Aktivieren Sie diese Regel, um den Zugriff auf Ressourcen in der AWS Cloud einzuschränken. Diese Regel sorgt dafür, dass die Multi-Faktor-Authentifizierung (MFA) für alle Benutzer aktiviert ist. MFA sorgt für eine weitere Schutzebene zusätzlich zu den Anmeldeinformationen. Reduzieren Sie Fälle von kompromittierten Konten, indem Sie MFA für Benutzer vorschreiben.

Kontroll-ID	AWS Config	Empfehlungen
2.5.1	iam-user-no-policies-überprüfen	Diese Regel stellt sicher, dass AWS Identity and Access Management (IAM) -Richtlinien nur Gruppen oder Rollen zugewiesen werden, um den Zugriff auf Systeme und Ressourcen zu kontrollieren. Die Zuweisung von Berechtigungen auf Gruppen- oder Rollenebene trägt dazu bei, die Wahrscheinlichkeit zu verringern, dass eine Identität übermäßige Berechtigungen erhält oder beibehält.

Kontroll-ID	AWS Config	Empfehlungen
2.5.1	iam-user-unused-credentials-überprüfen	AWS Identity and Access Management (IAM) kann Ihnen bei Zugriffsberechtigungen und Autorisierungen helfen, indem es nach IAM-Passwörtern und Zugriffsschlüsseln sucht, die für einen bestimmten Zeitraum nicht verwendet wurden. Wenn ungenutzte Anmeldeinformationen identifiziert werden, müssen Sie sie deaktivieren und/oder entfernen, da dies gegen das Prinzip der geringsten Berechtigung verstoßen könnte. Für diese Regel müssen Sie einen Wert für das maxCredentialUsage Alter festlegen (Standardkonfiguration: 90). Der tatsächliche Wert muss den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	AWS Config	Empfehlungen
2.5.1	mfa-enabled-for-iam-Konsolenzugriff	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass MFA für alle AWS Identity and Access Management (IAM) -Benutzer aktiviert ist, die über ein Konsolenkennwort verfügen. MFA sorgt für eine weitere Schutzebene zusätzlich zu den Anmeldeinformationen. Indem Sie MFA für Benutzer vorschreiben, können Sie Fälle kompromittierter Konten reduzieren und verhindern, dass unbefugte Benutzer auf vertrauliche Daten zugreifen.
2.5.1	root-account-mfa-enabled	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass MFA für den Root-Benutzer aktiviert ist. Der Stammbenutzer ist der AWS-Konto-Benutzer mit den meisten Berechtigungen. MFA sorgt für eine weitere Schutzebene zusätzlich zu den Anmeldeinformationen. Indem Sie MFA für den Root-Benutzer vorschreiben, können Sie die Anzahl AWS-Konten kompromittierter Benutzer reduzieren.

Kontroll-ID	AWS Config	Empfehlungen
2.5.1	secretsmanager-using-cmk	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass die Verschlüsselung mit dem AWS Key Managemen t Service (AWS KMS) für AWS Secrets Manager aktiviert ist. Aktivieren Sie die Verschlüsselung von Daten im Ruhezustand, um eventuell vorhandene sensible Daten im Ruhezustand im Secrets Manager zu schützen.
2.5.3	iam-user-mfa-enabled	Aktivieren Sie diese Regel, um den Zugriff auf Ressourcen in der AWS Cloud einzuschr änken. Diese Regel sorgt dafür, dass die Multi-Faktor-Authentifizierung (MFA) für alle Benutzer aktiviert ist. MFA sorgt für eine weitere Schutzebene zusätzlich zu den Anmeldeinformationen. Reduzieren Sie Fälle von kompromittierten Konten, indem Sie MFA für Benutzer vorschreiben.

Kontroll-ID	AWS Config	Empfehlungen
2.5.3	mfa-enabled-for-iam-Konsolenzugriff	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass MFA für alle AWS Identity and Access Management (IAM) -Benutzer aktiviert ist, die über ein Konsolenkennwort verfügen. MFA sorgt für eine weitere Schutzebene zusätzlich zu den Anmeldeinformationen. Indem Sie MFA für Benutzer vorschreiben, können Sie Fälle kompromittierter Konten reduzieren und verhindern, dass unbefugte Benutzer auf vertrauliche Daten zugreifen.
2.5.3	root-account-mfa-enabled	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass MFA für den Root-Benutzer aktiviert ist. Der Stammbenutzer ist der AWS-Konto-Benutzer mit den meisten Berechtigungen. MFA sorgt für eine weitere Schutzebene zusätzlich zu den Anmeldeinformationen. Indem Sie MFA für den Root-Benutzer vorschreiben, können Sie die Anzahl AWS-Konten kompromittierter Benutzer reduzieren.

Kontroll-ID	AWS Config	Empfehlungen
2.5.4	iam-password-policy	Die Identitäten und Anmeldein formationen werden auf der Grundlage einer organisat orischen IAM-Passwortrichtl inie ausgestellt, verwaltet und verifiziert. Sie erfüllen oder übertreffen die Anforderungen von NIST SP 800-63 und dem Standard „Best Practices“ von AWS Foundational Security für die Passwortstärke. Mit dieser Regel können Sie optional RequireUppercaseCharacters (Wert für AWS grundlege nde Sicherheitsbewährte Methoden: wahr), RequireLo wercaseCharacters (Wert für bewährte Methoden für AWS grundlegende Sicherheit: wahr), RequireSymbols (Wert für bewährte Methoden für AWS grundlegende Sicherhei t: wahr), RequireNumbers (Wert für bewährte Methoden für AWS grundlegende Sicherheit: wahr), MinimumPa sswordLength (Wert für bewährte Methoden für AWS grundlegende Sicherheit: 14), PasswordReusePreve ntion (Wert für bewährte Methoden für AWS grundlege nde Sicherheit: 24) und MaxPasswordAge (Wert

Kontroll-ID	AWS Config	Empfehlungen
		für bewährte Methoden für AWS grundlegende Sicherhei t: 90) für Ihr IAM festlegen Kennwortrichtlinie. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisat ion entsprechen.
2.5.5	ec-2 instance-profile-attached	EC2 Instanzprofile übergeben eine IAM-Rolle an eine EC2 Instance. Das Anhängen eines Instance-Profils an Ihre Instances kann bei der Implementierung von geringsten Berechtigungen und der Berechtigungsverwa ltung helfen.
2.5.5	iam-root-access-key-überprü fen	Der Zugriff auf Systeme und Ressourcen kann gesteuert werden, indem überprüft wird, ob der Root-Benutzer keine Zugriffsschlüssel mit seiner AWS Identity and Access Management (IAM) -Rolle verknüpft hat. Stellen Sie sicher, dass die Root-Zugr iffsschlüssel gelöscht werden. Erstellen und verwenden Sie stattdessen rollenbasierte Funktionen, AWS-Konten um das Prinzip der geringsten Funktionalität zu berücksic htigen.

Kontroll-ID	AWS Config	Empfehlungen
2.5.5	root-account-mfa-enabled	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass MFA für den Root-Benutzer aktiviert ist. Der Stammbenutzer ist der AWS-Konto-Benutzer mit den meisten Berechtigungen. MFA sorgt für eine weitere Schutzebene zusätzlich zu den Anmeldeinformationen. Indem Sie MFA für den Root-Benutzer vorschreiben, können Sie die Anzahl AWS-Konten kompromittierter Benutzer reduzieren.
2.6	alb-waf-enabled	Stellen Sie sicher, dass AWS WAF auf Elastic Load Balancers (ELB) aktiviert ist, um Webanwendungen zu schützen. Eine WAF trägt zum Schutz Ihrer Webanwendungen oder APIs vor gängigen Web-Exploits bei. Diese Web-Exploits können sich auf die Verfügbarkeit auswirken, die Sicherheit gefährden oder übermäßige Ressourcen in Ihrer Umgebung verbrauchen.

Kontroll-ID	AWS Config	Empfehlungen
2.6	ec-2 instances-in-vpc	Stellen Sie Amazon Elastic Compute Cloud (Amazon EC2) -Instances innerhalb einer Amazon Virtual Private Cloud (Amazon VPC) bereit, um eine sichere Kommunika tion zwischen einer Instance und anderen Services innerhalb der Amazon VPC zu ermöglichen, ohne dass ein Internet-Gateway, ein NAT-Gerät oder eine VPN-Verbi ndung erforderlich ist. Der gesamte Datenverkehr bleibt sicher in der AWS Cloud. Domains, die sich innerhalb einer VPC befinden, verfügen aufgrund ihrer logischen Isolierung im Vergleich zu Domains mit öffentlic hen Endpunkten über eine zusätzliche Sicherheitsebene. Weisen Sie EC2 Amazon-In stances einer Amazon-VPC zu, um den Zugriff ordnungsg emäß zu verwalten.

Kontroll-ID	AWS Config	Empfehlungen
2.6	ebs-snapshot-public-restorable-überprüfen	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass EBS-Snapshots nicht öffentlich wiederherstellbar sind. EBS-Volume-Snapshots können vertrauliche Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.
2.6	ec-2 instance-no-public-ip	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon Elastic Compute Cloud (Amazon EC2) -Instances nicht öffentlich zugänglich sind. EC2 Amazon-Instances können vertrauliche Informationen enthalten, und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	AWS Config	Empfehlungen
2.6	iam-user-mfa-enabled	Aktivieren Sie diese Regel, um den Zugriff auf Ressourcen in der AWS Cloud einzuschränken. Diese Regel sorgt dafür, dass die Multi-Faktor-Authentifizierung (MFA) für alle Benutzer aktiviert ist. MFA sorgt für eine weitere Schutzebene zusätzlich zu den Anmeldeinformationen. Reduzieren Sie Fälle von kompromittierten Konten, indem Sie MFA für Benutzer vorschreiben.
2.6	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) Security Groups können bei der Verwaltung des Netzwerkzugriffs helfen, indem sie eine statusbehaftete Filterung von eingehendem und ausgehendem Netzwerkverkehr zu Ressourcen bereitstellen. AWS Wenn Sie eingehenden (oder entfernten) Datenverkehr von 0.0.0.0/0 bis Port 22 auf Ihren Ressourcen nicht zulassen, können Sie den Remote-Zugriff einschränken.

Kontroll-ID	AWS Config	Empfehlungen
2.6	lambda-function-public-access-verboten	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass AWS Lambda-Funktionen nicht öffentlich zugänglich sind. Der öffentliche Zugriff kann möglicherweise die Verfügbarkeit von Ressourcen beeinträchtigen.

Kontroll-ID	AWS Config	Empfehlungen
2.6	lambda-inside-vpc	Stellen Sie AWS Lambda-Funktionen in einer Amazon Virtual Private Cloud (Amazon VPC) bereit, um eine sichere Kommunikation zwischen einer Funktion und anderen Diensten innerhalb der Amazon VPC zu gewährleisten. Bei dieser Konfiguration sind kein Internet-Gateway, kein NAT-Gerät und keine VPN-Verbindung erforderlich. Der gesamte Datenverkehr bleibt sicher in der Cloud. AWS Domains, die sich innerhalb einer VPC befinden, verfügen aufgrund ihrer logischen Isolierung im Vergleich zu Domains mit öffentlichen Endpunkten über eine zusätzliche Sicherheitsebene. Um den Zugriff ordnungsgemäß zu verwalten, sollten AWS Lambda-Funktionen einer VPC zugewiesen werden.

Kontroll-ID	AWS Config	Empfehlungen
2.6	mfa-enabled-for-iam-Konsolenzugriff	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass MFA für alle AWS Identity and Access Management (IAM) -Benutzer aktiviert ist, die über ein Konsolenkennwort verfügen. MFA sorgt für eine weitere Schutzebene zusätzlich zu den Anmeldeinformationen. Indem Sie MFA für Benutzer vorschreiben, können Sie Fälle kompromittierter Konten reduzieren und verhindern, dass unbefugte Benutzer auf vertrauliche Daten zugreifen.
2.6	rds-instance-public-access-überprüfen	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Relational Database Service (Amazon RDS) -Instances nicht öffentlich sind. Amazon-RDS-Datenbank-Instances können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	AWS Config	Empfehlungen
2.6	rds-snapshots-public-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Relational Database Service (Amazon RDS) -Instances nicht öffentlich sind. Amazon-RDS-Datenbank-Instances können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.
2.6	redshift-cluster-public-access-überprüfen	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Redshift Redshift-Cluster nicht öffentlich sind. Amazon-Redshift-Cluster können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	AWS Config	Empfehlungen
2.6	restricted-common-ports	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass gemeinsame Ports für Amazon Elastic Compute Cloud (Amazon EC2) - Sicherheitsgruppen eingeschränkt sind. Wenn der Zugriff auf Ports nicht auf vertrauenswürdige Quellen beschränkt wird, kann dies zu Angriffen auf die Verfügbarkeit, Integrität und Vertraulichkeit von Systemen führen. Mit dieser Regel können Sie optional die Parameter blockedPort1–blockedPort5 festlegen (Standardkonfigurationen: 20, 21, 3389, 3306, 4333). Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	AWS Config	Empfehlungen
2.6	root-account-mfa-enabled	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass MFA für den Root-Benutzer aktiviert ist. Der Stammbenutzer ist der AWS-Konto-Benutzer mit den meisten Berechtigungen. MFA sorgt für eine weitere Schutzebene zusätzlich zu den Anmeldeinformationen. Indem Sie MFA für den Root-Benutzer vorschreiben, können Sie die Anzahl AWS-Konten kompromittierter Benutzer reduzieren.

Kontroll-ID	AWS Config	Empfehlungen
2.6	s3- -blöcke-periodisch account-level-public-access	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Simple Storage Service (Amazon S3) -Buckets nicht öffentlich zugänglich sind. Diese Regel trägt dazu bei, sensible Daten vor unbefugten Remote-Benutzern zu schützen, indem sie den öffentlichen Zugriff verhindert. Mit dieser Regel können Sie optional die Parameter ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) und restrictPublicBuckets Parameter (Config Default: True) festlegen. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	AWS Config	Empfehlungen
2.6	s3- bucket-public-read-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie nur autorisierten Benutzern, Prozessen und Geräten Zugriff auf Amazon Simple Storage Service (Amazon S3) -Buckets gewähren. Die Verwaltung des Zugriffs sollte mit der Klassifizierung der Daten übereinstimmen.
2.6	s3- bucket-public-write-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie nur autorisierten Benutzern, Prozessen und Geräten Zugriff auf Amazon Simple Storage Service (Amazon S3) -Buckets gewähren. Die Verwaltung des Zugriffs sollte mit der Klassifizierung der Daten übereinstimmen.
2.6	sagemaker-notebook-no-direct-Internetzugang	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass SageMaker Amazon-Notebooks keinen direkten Internetzugang zulassen. Indem Sie direkten Internetzugang blockieren, vermeiden Sie, dass unbefugte Benutzer auf sensible Daten zugreifen.

Kontroll-ID	AWS Config	Empfehlungen
2.6	vpc-default-security-group-geschlossen	Sicherheitsgruppen von Amazon Elastic Compute Cloud (Amazon EC2) können bei der Verwaltung des Netzwerkzugriffs helfen, indem sie eine statusbeh aftete Filterung des ein- und ausgehenden Netzwerkv erkehrs zu Ressourcen bereitstellen. AWS Die Beschränkung des gesamten Datenverkehrs auf die Standardsicherheitsgruppe hilft dabei, den Fernzugriff auf Ihre Ressourcen einzuschr änken. AWS

Kontroll-ID	AWS Config	Empfehlungen
2.6	vpc-sg-open-only-to-authorized-ports	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass gemeinsame Ports für Amazon Elastic Compute Cloud (Amazon EC2) - Sicherheitsgruppen eingeschränkt sind. Wenn der Zugriff auf Ports nicht auf vertrauenswürdige Quellen beschränkt wird, kann dies zu Angriffen auf die Verfügbarkeit, Integrität und Vertraulichkeit von Systemen führen. Durch die Beschränkung des Zugriffs auf Ressourcen innerhalb einer Sicherheitsgruppe aus dem Internet (0.0.0.0/0) kann der Remote-Zugriff auf interne Systeme gesteuert werden.

Kontroll-ID	AWS Config	Empfehlungen
2.6.6	api-gw-associated-with-WAF	AWS Mit WAF können Sie eine Reihe von Regeln (als Web Access Control List (Web ACL) bezeichnet) konfiguri eren, die Webanfragen auf der Grundlage von anpassbar en Websicherheitsregeln und -bedingungen, die Sie definieren, zulassen, blockiere n oder zählen. Stellen Sie sicher, dass Ihre Amazon-API-Gateway-Stufe mit einer WAF-Web-ACL verknüpft ist, um sie vor böswilligen Angriffen zu schützen.
2.6.6	elv 2 acm-certificate-required	Zum Schutz von eventuell vorhandenen sensiblen Daten sowie von Daten während der Übertragung muss die Verschlüsselung für Ihr Elastic Load Balancing aktiviert sein. Verwenden Sie AWS Certifica te Manager, um öffentlic he und private SSL/TLS-Z ertifikate mit AWS Diensten und internen Ressourcen zu verwalten, bereitzustellen und bereitzustellen.

Kontroll-ID	AWS Config	Empfehlungen
2.6.6	lambda-function-public-access-verboten	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass AWS Lambda-Funktionen nicht öffentlich zugänglich sind. Der öffentliche Zugriff kann möglicherweise die Verfügbarkeit von Ressourcen beeinträchtigen.
2.6.6	rds-instance-public-access-überprüfen	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Relational Database Service (Amazon RDS) -Instances nicht öffentlich sind. Amazon-RDS-Datenbank-Instances können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.
2.6.6	redshift-cluster-public-access-überprüfen	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Redshift Redshift-Cluster nicht öffentlich sind. Amazon-Redshift-Cluster können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	AWS Config	Empfehlungen
2.6.6	restricted-common-ports	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass gemeinsame Ports für Amazon Elastic Compute Cloud (Amazon EC2) - Sicherheitsgruppen eingeschränkt sind. Wenn der Zugriff auf Ports nicht auf vertrauenswürdige Quellen beschränkt wird, kann dies zu Angriffen auf die Verfügbarkeit, Integrität und Vertraulichkeit von Systemen führen. Mit dieser Regel können Sie optional die Parameter blockedPort1–blockedPort5 festlegen (Standardkonfigurationen: 20, 21, 3389, 3306, 4333). Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	AWS Config	Empfehlungen
2.6.6	s3-Blöcke-periodisch account-level-public-access	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Simple Storage Service (Amazon S3) -Buckets nicht öffentlich zugänglich sind. Diese Regel trägt dazu bei, sensible Daten vor unbefugten Remote-Benutzern zu schützen, indem sie den öffentlichen Zugriff verhindert. Mit dieser Regel können Sie optional die Parameter ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) und restrictPublicBuckets Parameter (Config Default: True) festlegen. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	AWS Config	Empfehlungen
2.6.6	s-3 bucket-public-read-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie nur autorisierten Benutzern, Prozessen und Geräten Zugriff auf Amazon Simple Storage Service (Amazon S3) -Buckets gewähren. Die Verwaltung des Zugriffs sollte mit der Klassifizierung der Daten übereinstimmen.
2.6.6	s-3 bucket-public-write-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie nur autorisierten Benutzern, Prozessen und Geräten Zugriff auf Amazon Simple Storage Service (Amazon S3) -Buckets gewähren. Die Verwaltung des Zugriffs sollte mit der Klassifizierung der Daten übereinstimmen.
2.6.6	sagemaker-notebook-no-direct-Internetzugang	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass SageMaker Amazon-Notebooks keinen direkten Internetzugang zulassen. Indem Sie direkten Internetzugang blockieren, vermeiden Sie, dass unbefugte Benutzer auf sensible Daten zugreifen.

Kontroll-ID	AWS Config	Empfehlungen
2.6.6	vpc-default-security-group-geschlossen	Sicherheitsgruppen von Amazon Elastic Compute Cloud (Amazon EC2) können bei der Verwaltung des Netzwerkzugriffs helfen, indem sie eine statusbeh aftete Filterung des ein- und ausgehenden Netzwerkv erkehrs zu Ressourcen bereitstellen. AWS Die Beschränkung des gesamten Datenverkehrs auf die Standardsicherheitsgruppe hilft dabei, den Fernzugriff auf Ihre Ressourcen einzuschr änken. AWS

Kontroll-ID	AWS Config	Empfehlungen
2.6.6	vpc-sg-open-only-to-authorized-ports	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass gemeinsame Ports für Amazon Elastic Compute Cloud (Amazon EC2) - Sicherheitsgruppen eingeschränkt sind. Wenn der Zugriff auf Ports nicht auf vertrauenswürdige Quellen beschränkt wird, kann dies zu Angriffen auf die Verfügbarkeit, Integrität und Vertraulichkeit von Systemen führen. Durch die Beschränkung des Zugriffs auf Ressourcen innerhalb einer Sicherheitsgruppe aus dem Internet (0.0.0.0/0) kann der Remote-Zugriff auf interne Systeme gesteuert werden.
2.6.7	no-unrestricted-route-to-igw	Stellen Sie sicher, dass EC2 Amazon-Routentabellen keine uneingeschränkten Routen zu einem Internet-Gateway enthalten. Durch das Entfernen oder Beschränken des Internetzugangs für Workloads innerhalb von Amazon VPCs können unbeabsichtigte Zugriffe in Ihrer Umgebung reduziert werden.

Kontroll-ID	AWS Config	Empfehlungen
2.7	acm-certificate-expiration-check	Stellen Sie sicher, dass die Netzwerkintegrität geschützt ist, indem Sie sicherstellen, dass X509-Zertifikate von ACM ausgestellt werden. AWS Diese Zertifikate müssen gültig und dürfen nicht abgelaufe n sein. Für diese Regel ist ein Wert für erforderlich daysToExpiration (Wert für bewährte AWS Grundrege ln für Sicherheit: 90). Der tatsächliche Wert muss den Richtlinien Ihrer Organisation entsprechen.
2.7	alb-http-drop-invalid-Header-aktiviert	Stellen Sie sicher, dass Ihre Elastic Load Balancers (ELB) so konfiguriert sind, dass sie HTTP-Header löschen. Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	AWS Config	Empfehlungen
2.7	alb-http-to-https-Umleitung sprüfung	Um Daten während der Übertragung zu schützen, stellen Sie sicher, dass Ihr Application Load Balancer unverschlüsselte HTTP-Anfragen automatisch an HTTPS umleitet. Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.
2.7	api-gw-cache-enabled-und-ve rschlüsselt	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass die Verschlüsselung für den Cache Ihrer API-Gatew ay-Stufe aktiviert ist. Da für die API-Methode sensible Daten erfasst werden können, sollten Sie die Verschlüsselung von Daten im Ruhezustand aktivieren, um diese Daten zu schützen.
2.7	cloudwatch-log-group-encryp ted	Um sensible Daten im Speicher zu schützen, stellen Sie sicher, dass die Verschlüs selung für Ihre Amazon CloudWatch Log Groups aktiviert ist.

Kontroll-ID	AWS Config	Empfehlungen
2.7	cloud-trail-encryption-enabled	Da sensible Daten vorhanden sein können und um Daten im Speicher zu schützen, sollten Sie sicherstellen, dass die Verschlüsselung für Ihre AWS CloudTrail Trails aktiviert ist.
2.7	dynamodb-table-encrypted-kms	Stellen Sie sicher, dass die Verschlüsselung für Ihre Amazon-DynamoDB-Tabellen aktiviert ist. Um eventuell vorhandene sensible Daten im Ruhezustand in diesen Tabellen zu schützen, müssen Sie die Verschlüsselung von Daten im Ruhezustand aktivieren. Standardmäßig werden DynamoDB-Tabellen mit einem AWS eigenen Kundenhauptschlüssel (CMK) verschlüsselt.
2.7	ec2- ebs-encryption-by-default	Zum Schutz von Daten im Ruhezustand müssen Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon Elastic Block Store (Amazon EBS)-Volumes aktiviert ist. Da sensible Daten auch im Ruhezusta nd vorhanden sein können, sollten Sie die Verschlüs selung im Ruhezustand aktivieren, um diese Daten zu schützen.

Kontroll-ID	AWS Config	Empfehlungen
2.7	efs-encrypted-check	Aktivieren Sie die Verschlüs selung für Ihr Amazon Elastic File System (EFS), um eventuell vorhandene sensible Daten sowie Daten im Ruhezustand zu schützen.
2.7	elasticsearch-encrypted-at-rest	Da sensible Daten vorhanden sein können und um Daten im Ruhezustand zu schützen, sollten Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon OpenSearch Service (OpenSearch Service) -Domains aktiviert ist.
2.7	elasticsearch-node-to-node-Verschlüsselungsprüfung	Stellen Sie sicher, dass die node-to-node Verschlüsselung für Amazon OpenSearch Service aktiviert ist. Node-to-nodeVerschlüsselung ermöglicht die TLS 1.2-Versc hlüsselung für die gesamte Kommunikation innerhalb der Amazon Virtual Private Cloud (Amazon VPC). Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	AWS Config	Empfehlungen
2.7	elb-acm-certificate-required	Zum Schutz von eventuell vorhandenen sensiblen Daten sowie von Daten während der Übertragung muss die Verschlüsselung für Ihr Elastic Load Balancing aktiviert sein. Verwenden Sie AWS Certifica te Manager, um öffentlic he und private SSL/TLS-Z ertifikate mit AWS Diensten und internen Ressourcen zu verwalten, bereitzustellen und bereitzustellen.
2.7	elb-tls-https-listeners-nur	Stellen Sie sicher, dass Ihre Elastic Load Balancer (ELBs) mit SSL- oder HTTPS-Lis tenern konfiguriert sind. Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.
2.7	encrypted-volumes	Aktivieren Sie die Verschlüs selung für Ihre Amazon-El astic-Block-Store (Amazon-EBS)-Volumes, um eventuell vorhandene sensible Daten sowie Daten im Ruhezustand zu schützen.

Kontroll-ID	AWS Config	Empfehlungen
2.7	rds-snapshot-encrypted	Stellen Sie sicher, dass die Verschlüsselung für Ihre Amazon Relational Database Service (Amazon RDS)-Snap shots aktiviert ist. Da sensible Daten auch im Ruhezusta nd vorhanden sein können, sollten Sie die Verschlüs selung im Ruhezustand aktivieren, um diese Daten zu schützen.
2.7	rds-storage-encrypted	Zum Schutz von Daten im Ruhezustand müssen Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon Relational Database Service (Amazon RDS)-Instances aktiviert ist. Um eventuell vorhandene sensible Daten im Ruhezustand in Amazon-RDS-Instanc es zu schützen, muss die Verschlüsselung von Daten im Ruhezustand aktiviert sein.

Kontroll-ID	AWS Config	Empfehlungen
2.7	redshift-cluster-configuration-check	Um Daten im Ruhezustand zu schützen, muss die Verschlüsselung für Ihre Amazon-Redshift-Cluster aktiviert sein. Sie müssen auch sicherstellen, dass die erforderlichen Konfigurationen auf Amazon-Redshift-Clustern bereitgestellt werden. Die Prüfungsprotokollierung muss aktiviert sein, um Informationen zu Verbindungen und Benutzeraktivitäten in der Datenbank bereitzustellen. Diese Regel erfordert, dass ein Wert für clusterDbEncrypted (Config Default: TRUE) und LoggingEnabled (Config Default: TRUE) gesetzt ist. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.
2.7	redshift-require-tls-ssl	Stellen Sie sicher, dass Ihre Amazon-Redshift-Cluster eine TLS/SSL-Verschlüsselung erfordern, um eine Verbindung zu SQL-Clients herzustellen. Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	AWS Config	Empfehlungen
2.7	s3-aktiviert bucket-server-side-encryption	Zum Schutz von Daten im Ruhezustand müssen Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon Simple Storage Service (Amazon S3)-Buckets aktiviert ist. Um eventuell vorhandene sensible Daten im Ruhezustand in Amazon-S3-Buckets zu schützen, muss die Verschlüsselung aktiviert sein.
2.7	s-3 bucket-ssl-requests-only	Um Daten während der Übertragung zu schützen, stellen Sie sicher, dass Ihre Amazon Simple Storage Service (Amazon S3)-Buckets Anfragen zur Verwendung von Secure Socket Layer (SSL)-Buckets erfordern. Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	AWS Config	Empfehlungen
2.7	sagemaker-endpoint-configuration-kms-key-konfiguriert	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass die Verschlüsselung mit dem AWS Key Management Service (AWS KMS) für Ihren Endpunkt aktiviert ist. SageMaker Da sensible Daten auf dem SageMaker Endgerät gespeichert werden können, sollten Sie die Verschlüsselung im Ruhezustand aktivieren, um diese Daten zu schützen.
2.7	sagemaker-notebook-instance-kms-schlüsselkonfiguriert	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass die Verschlüsselung mit dem AWS Key Management Service (AWS KMS) für Ihr Notebook aktiviert ist. SageMaker Da vertrauliche Daten im SageMaker Notebook gespeichert werden können, sollten Sie die Verschlüsselung im Ruhezustand aktivieren, um diese Daten zu schützen.

Kontroll-ID	AWS Config	Empfehlungen
2.7	sns-encrypted-kms	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass Ihre Amazon Simple Notification Service (Amazon SNS) -Themen mit dem AWS Key Management Service (AWS KMS) verschlüsselt werden müssen. Um eventuell vorhandene sensible Daten im Ruhezustand in veröffentlichten Nachrichten zu schützen, muss die Verschlüsselung von Daten im Ruhezustand aktiviert sein.
2.7	opensearch-encrypted-at-rest	Da sensible Daten vorhanden sein können und um Daten im Ruhezustand zu schützen, sollten Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon OpenSearch Service-Domains aktiviert ist.

Kontroll-ID	AWS Config	Empfehlungen
2.7	opensearch-node-to-node-Verschlüsselungsprüfung	Stellen Sie sicher, dass die node-to-node Verschlüsselung für Amazon OpenSearch Service aktiviert ist. Node-to-nodeVerschlüsselung ermöglicht die TLS 1.2-Verschlüsselung für die gesamte Kommunikation innerhalb der Amazon Virtual Private Cloud (Amazon VPC). Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.
2.7.1	api-gw-ssl-enabled	Stellen Sie sicher, dass die REST-API-Stufen von Amazon API Gateway mit SSL-Zertifikaten konfiguriert sind, damit Backend-Systeme überprüfen können, ob Anforderungen von API Gateway stammen.

Kontroll-ID	AWS Config	Empfehlungen
2.7.1	elb-predefined-security-policy-SSL-Prüfung	Stellen Sie sicher, dass Ihre SSL-Listener von Classic Elastic Load Balancing eine vordefinierte Sicherheitsrichtlinie verwenden, um Daten während der Übertragung zu schützen. Elastic Load Balancing bietet vordefinierte Aushandlungskonfigurationen, die für die SSL-Aushandlung verwendet werden, wenn eine Verbindung zwischen einem Client und Ihrem Load Balancer hergestellt wurde. Die SSL-Aushandlungskonfigurationen sind mit einer breiten Palette von Clients kompatibel und verwenden hochfeste kryptografische Algorithmen. Diese Regel verlangt, dass Sie eine vordefinierte Sicherheitsrichtlinie für Ihre SSL-Listener festlegen. Die Standard-Sicherheitsrichtlinie lautet: Policy-TLS-1-2-2017-0. ELBSecurity Der tatsächliche Wert muss den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	AWS Config	Empfehlungen
2.7.2	cmk-backing-key-rotation-aktiviert	Aktivieren Sie die Schlüssel rotation, um sicherzustellen, dass Schlüssel rotiert werden, nachdem sie das Ende ihrer Krypto-Periode erreicht haben.
2.7.2	kms-cmk-not-scheduled-zum Löschen	Um Daten im Ruhezustand zu schützen, sollten Sie sicherstellen, dass die für den Kunden erforderlichen Masterschlüssel (CMKs) nicht im AWS Key Management Service (AWS KMS) gelöscht werden. Da Schlüssel manchmal gelöscht werden müssen, können Sie mit dieser Regel alle zu löschenden Schlüssel überprüfen, falls ein Schlüssel versehentlich zur Löschung vorgemerkt wurde.
2.8.5	codebuild-project-envvar-awscred-überprüfen	Stellen Sie sicher, dass die Anmeldeinformationen AWS_ACCESS_KEY_ID AWS_SECRET_ACCESS_KEY nicht in AWS Codebuild -Projektumgebungen vorhanden sind. Speichern Sie diese Variablen nicht als Klartext. Das Speichern dieser Variablen als Klartext bewirkt eine unbeabsichtigte Offenlegung von Daten sowie unberechtigte Zugriffe.

Kontroll-ID	AWS Config	Empfehlungen
2.8.5	codebuild-project-source-repo-URL-Prüfung	Stellen Sie sicher, dass die URL des Quell-Repositorys GitHub oder des Bitbucket -Quell-Repositorys keine persönlichen Zugriffstoken oder Anmeldeinformationen in Codebuild-Projektumgebungen enthält. AWS Verwende OAuth anstelle von persönlichen Zugriffstoken oder Anmeldedaten die Autorisierung für den Zugriff auf GitHub Bitbucket-Repositorys.
2.8.6	codebuild-project-envvar-awscred-überprüfen	Stellen Sie sicher, dass die Anmeldeinformationen AWS_ACCESS_KEY_ID AWS_SECRET_ACCESS_KEY nicht in AWS Codebuild -Projektumgebungen vorhanden sind. Speichern Sie diese Variablen nicht als Klartext. Das Speichern dieser Variablen als Klartext bewirkt eine unbeabsichtigte Offenlegung von Daten sowie unberechtigte Zugriffe.

Kontroll-ID	AWS Config	Empfehlungen
2.8.6	codebuild-project-source-repo-URL-Prüfung	Stellen Sie sicher, dass die URL des Quell-Repositorys GitHub oder des Bitbucket -Quell-Repositorys keine persönlichen Zugriffstoken oder Anmeldeinformation en in Codebuild-Projektu mgebungen enthält. AWS Verwende OAuth anstelle von persönlichen Zugriffst oken oder Anmeldedaten die Autorisierung für den Zugriff auf GitHub Bitbucket-Reposito rys.
2.9.1	account-part-of-organizations	Durch die zentrale Verwaltun g AWS-Konten innerhalb von AWS Organizations wird sichergestellt, dass die Konten den Vorschriften entsprech en. Eine fehlende zentrale Kontoverwaltung kann zu inkonsistenten Kontokonf igurationen führen, wodurch Ressourcen und sensible Daten offengelegt werden können.

Kontroll-ID	AWS Config	Empfehlungen
2.9.1	cloudtrail-security-trail-enabled	Diese Regel trägt dazu bei, die Verwendung der AWS empfohlenen bewährten Sicherheitsmethoden für sicherzustellen AWS CloudTrail, indem geprüft wird, ob mehrere Einstellungen aktiviert sind. Dazu gehören die Verwendung von Protokoll verschlüsselung, Protokoll validierung und Aktivierung AWS CloudTrail in mehreren Regionen.

Kontroll-ID	AWS Config	Empfehlungen
2.9.1	cloud-trail-log-file-Validierung aktiviert	Verwenden Sie die AWS CloudTrail Protokolldateivalidierung, um die Integrität von Protokollen zu überprüfen. CloudTrail Mithilfe der Protokolldateivalidierung kann festgestellt werden, ob eine Protokolldatei geändert oder gelöscht wurde oder ob sie nach der Übermittlung CloudTrail unverändert geblieben ist. Dieses Feature wurde mit dem Branchenstandard entsprechenden Algorithmen entwickelt: SHA-256 für die Hashfunktion und SHA-256 mit RSA für digitale Signaturen. Aus diesem Grund ist es rechnerisch unmöglich, CloudTrail Protokolldateien unbemerkt zu ändern, zu löschen oder zu fälschen.

Kontroll-ID	AWS Config	Empfehlungen
2.9.1	redshift-cluster-maintenancesettings-check	Diese Regel stellt sicher, dass Amazon-Redshift-Cluster die bevorzugten Einstellungen für Ihre Organisation haben. Insbesondere sorgt sie dafür, dass Cluster bevorzugte Wartungsfenster und automatisierte Aufbewahrungsfristen für Snapshots für die Datenbank haben. Für diese Regel müssen Sie die allowVersionUpgrade festlegen. Der Standardwert ist „true“. Außerdem können Sie optional den Zeitraum preferredMaintenanceWindow (der Standardwert ist sa: 16:00 -sa: 16:30) und den automatedSnapshotRetention Zeitraum (der Standardwert ist 1) festlegen. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	AWS Config	Empfehlungen
2.9.2	autoscaling-group-elb-healthcheck-erforderlich	Die Elastic Load Balancer (ELB) -Zustandsprüfungen für Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling Scaling-Gruppen unterstützen die Aufrechterhaltung einer angemessenen Kapazität und Verfügbarkeit. Der Load Balancer sendet regelmäßig Pings, versucht Verbindungen herzustellen oder sendet Anfragen, um den Zustand der EC2 Amazon-Instances in einer Gruppe mit auto-scaling zu testen. Wenn eine Instance nicht zurückmeldet, wird der Traffic an eine neue EC2 Amazon-Instance gesendet.

Kontroll-ID	AWS Config	Empfehlungen
2.9.2	cloudwatch-alarm-action-check	Amazon CloudWatch alarmiert, wenn eine Metrik den Schwellenwert für eine bestimmte Anzahl von Bewertungszeiträumen überschreitet. Der Alarm führt eine oder mehrere Aktionen durch, die vom Wert der Metrik oder des Ausdrucks im Vergleich zu einem Schwellenwert in einer Reihe von Zeiträumen abhängt. Diese Regel erfordert einen Wert für alarmActionRequired (Config Default: True), insufficientDataActionRequired (Config Default: True), okActionRequired (Config Default: False). Der tatsächliche Wert muss die Alarmaktionen für Ihre Umgebung widerspiegeln.

Kontroll-ID	AWS Config	Empfehlungen
2.9.2	dynamodb-throughput-limit-check	Aktivieren Sie diese Regel, um sicherzustellen, dass die bereitgestellte Durchsatzkapazität in Ihren Amazon-DynamoDB-Tabellen überprüft wird. Dies ist der Umfang der Lese- und Schreibaktivitäten, der von den jeweiligen Tabellen unterstützt werden kann. DynamoDB verwendet diese Informationen für das Reservieren ausreichender Systemressourcen, um Ihren Durchsatzanforderungen gerecht zu werden. Diese Regel generiert eine Warnung, wenn sich der Durchsatz dem Höchstlimit für ein Kundenkonto nähert. Mit dieser Regel können Sie optional die Parameter RCUThreshold Kontoprozentsatz (Konfigurationsstandard: 80) und WCUThreshold Kontoprozentsatz (Konfigurationsstandard: 80) festlegen. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	AWS Config	Empfehlungen
2.9.2	ec-2 instance-detailed-monitoring-enabled	Aktivieren Sie diese Regel, um die Amazon Elastic Compute Cloud (Amazon EC2) -Instance-Überwachung auf der EC2 Amazon-Konsole zu verbessern, in der Monitoring-Diagramme mit einem Zeitraum von 1 Minute für die Instance angezeigt werden.
2.9.2	lambda-concurrency-check	Diese Regel stellt sicher, dass die Höchst- und Untergrenzen für die Gleichzeitigkeit einer Lambda-Funktion festgelegt werden. Dies kann Sie beim Baselining für die Anzahl der Anforderungen unterstützen, die Ihre Funktion zu einem bestimmten Zeitpunkt verarbeitet.

Kontroll-ID	AWS Config	Empfehlungen
2.9.2	rds-enhanced-monitoring-enabled	Aktivieren Sie Amazon Relational Database Service (Amazon RDS), um die Verfügbarkeit von Amazon RDS zu überwachen. Dies bietet einen detaillierten Einblick in den Zustand Ihrer Amazon-RDS-Datenbank-Instances. Wenn der Amazon-RDS-Speicher mehr als ein zugrunde liegendes physisches Gerät verwendet, erfasst Enhanced Monitoring die Daten für jedes Gerät. Wenn die Amazon-RDS-Datenbank-Instance in einer Multi-AZ-Bereitstellung ausgeführt wird, werden außerdem die Daten für jedes Gerät auf dem sekundären Host sowie die Metriken des sekundären Hosts erfasst.

Kontroll-ID	AWS Config	Empfehlungen
2.9.3	db-instance-backup-enabled	Die Sicherungsfunktion von Amazon RDS erstellt Sicherungen Ihrer Datenbank en und Transaktionsprotokolle. Amazon RDS erstellt einen Snapshot für das Speicherv olume Ihrer DB-Instance, sodass die gesamte DB-Instance gesichert wird. Sie können im System spezifisc he Aufbewahrungsfristen festlegen, um Ihre Ausfallsi cherheitsanforderungen zu erfüllen.
2.9.3	dynamodb-autoscaling-enable d	Amazon DynamoDB Auto Scaling verwendet den AWS Application Auto Scaling-Service, um die bereitges tellte Durchsatzkapazität so anzupassen, dass sie automatisch auf tatsächliche Verkehrsmuster reagiert. Auf diese Weise kann eine Tabelle oder ein globaler sekundärer Index die bereitgestellte Lese-/ Schreibkapazität erhöhen, um plötzliche Erhöhunge n des Datenverkehrs ohne Drosselung zu bewältigen.

Kontroll-ID	AWS Config	Empfehlungen
2.9.3	dynamodb-in-backup-plan	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon DynamoDB-Tabellen Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	AWS Config	Empfehlungen
2.9.3	ebs-in-backup-plan	Stellen Sie zur Unterstützung der Datensicherungsprozesse sicher, dass Ihre Amazon Elastic Block Store (Amazon EBS) -Volumes Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherung smanagement und erleichte rt Ihnen die Erfüllung von geschäftlichen und behördlic hen Compliance-Anforde rungen hinsichtlich Datensich erungen.

Kontroll-ID	AWS Config	Empfehlungen
2.9.3	efs-in-backup-plan	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon Elastic File System (Amazon EFS) - Dateisysteme Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.
2.9.3	elasticache-redis-cluster-automatic-Backup-Check	Wenn automatische Backups aktiviert sind, ElastiCache erstellt Amazon täglich ein Backup des Clusters. Die Sicherung kann für eine von Ihrer Organisation festgelegte Anzahl von Tagen aufbewahrt werden. Automatische Backups schützen vor Datenverlust. Bei einem Ausfall können Sie einen neuen Cluster erstellen, der Ihre Daten aus dem aktuellen Backup wiederherstellt.

Kontroll-ID	AWS Config	Empfehlungen
2.9.3	elb-cross-zone-load-Balancing aktiviert	Aktivieren Sie zonenüber greifendes Load Balancing für Ihre Elastic Load Balancer (ELBs), um eine angemesse ne Kapazität und Verfügbar keit aufrechtzuerhalten. Zonenübergreifendes Load Balancing reduziert die Notwendigkeit, die gleiche Anzahl von Instances in jeder aktivierten Availability Zone aufrechtzuerhalten. Es verbessert auch die Fähigkeit Ihrer Anwendung, den Verlust einer oder mehrerer Instances zu bewältigen.
2.9.3	elb-deletion-protection-ena bled	Diese Regel sorgt dafür, dass der Löschschutz für Elastic Load Balancing aktiviert ist. Verwenden Sie diese Funktion, um zu verhinder n, dass Ihr Load Balancer versehentlich oder böswillig gelöscht wird, was zum Verlust der Verfügbarkeit Ihrer Anwendungen führen kann.

Kontroll-ID	AWS Config	Empfehlungen
2.9.3	rds-instance-deletion-protection-aktiviert	Stellen Sie sicher, dass Amazon Relational Database Service (Amazon RDS)-Instances den Löschschutz aktiviert haben. Verwenden Sie den Löschschutz, um zu verhindern, dass Ihre Amazon-RDS-Instances versehentlich oder böswillig gelöscht werden, was zum Verlust der Verfügbarkeit Ihrer Anwendungen führen kann.
2.9.3	rds-in-backup-plan	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon Relational Database Service (Amazon RDS) -Instances Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	AWS Config	Empfehlungen
2.9.3	rds-multi-az-support	Die Multi-AZ-Unterstützung in Amazon Relational Database Service (Amazon RDS) bietet eine verbesserte Verfügbar keit und Beständigkeit von Datenbank-Instances. Wenn Sie eine Multi-AZ-Datenbank-Instance bereitstellen, erstellt Amazon RDS automatisch eine primäre Datenbank-Instance und repliziert die Daten synchron auf eine Standby-Instance in einer anderen Availability Zone. Jede Availability Zone läuft auf einer eigenen, physisch getrennten, unabhängigen Infrastruktur und ist auf eine hohe Verfügbarkeit ausgelegt . Im Falle eines Infrastru kturausfalls führt Amazon RDS einen automatischen Failover zum Standby-Modus durch, sodass Sie den Datenbank betrieb wieder aufnehmen können, sobald der Failover abgeschlossen ist.

Kontroll-ID	AWS Config	Empfehlungen
2.9.3	s-3 bucket-default-lock-enabled	Stellen Sie sicher, dass für Ihren Amazon Simple Storage Service (Amazon S3)-Bucket standardmäßig eine Sperre aktiviert ist. Zum Schutz eventuell vorhandener sensibler Daten in S3-Bucket s müssen Sie Objektsperren für Daten im Ruhezustand erzwingen.
2.9.3	s-3 bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) unterstützt die Aufrechte rhaltung einer angemessenen Kapazität und Verfügbarkeit. CRR ermöglicht das automatis che, asynchrone Kopieren von Objekten in Amazon-S3 -Buckets, um die Datenverf ügbarkeit sicherzustellen.

Kontroll-ID	AWS Config	Empfehlungen
2.9.3	s-3 bucket-versioning-enabled	Die Versionsverwaltung von Amazon Simple Storage Service (Amazon S3)-Buckets hilft dabei, mehrere Varianten eines Objekts im selben Amazon-S3-Bucket zu speichern. Verwenden Sie die Versionsverwaltung, um sämtliche Versionen aller Objekte in Ihrem Amazon-S3-Bucket zu speichern, abzurufen oder wiederher zustellen. Mit der Versionsv erwaltung können Sie Versionen sowohl nach unbeabsichtigten Benutzera ktionen als auch nach Anwendungsfehlern problemlo s wiederherstellen.

Kontroll-ID	AWS Config	Empfehlungen
2.9.3	vpc-vpn-2-tunnels-up	Redundante Site-to-Site VPN-Tunnel können implement iert werden, um die Anforderu ngen an die Ausfallsicherheit zu erfüllen. Es verwendet zwei Tunnel, um die Konnektiv ität sicherzustellen, falls eine der Site-to-Site VPN-Verbi ndungen nicht verfügbar ist. Um sich vor einem Verbindun gsverlust zu schützen, können Sie für den Fall, dass Ihr Kunden-Gateway nicht verfügbar ist, eine zweite Site-to-Site VPN-Verbindung zu Ihrer Amazon Virtual Private Cloud (Amazon VPC) und Ihrem Virtual Private Gateway einrichten, indem Sie ein zweites Kunden-Gateway verwenden.

Kontroll-ID	AWS Config	Empfehlungen
2.9.3	ec2--Plan resources-protected-by-backup	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon Elastic Compute Cloud (Amazon EC2) - Ressourcen Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	AWS Config	Empfehlungen
2.9.3	fsx-resources-protected-by-Backup-Plan	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre FSx Amazon-Dateisysteme Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.
2.9.4	api-gw-execution-logging-aktiviert	Die API-Gateway-Protokollierung zeigt detaillierte Ansichten der Benutzer, die auf die API zugegriffen haben, und wie diese Benutzer auf die API zugegriffen haben. Diese Einblicke ermöglichen die Transparenz von Benutzeraktivitäten.

Kontroll-ID	AWS Config	Empfehlungen
2.9.4	cloudtrail-s3-dataevents-enabled	Die Erfassung von Simple Storage Service (Amazon S3)-Datenereignissen unterstützt die Erkennung von ungewöhnlichen Aktivitäten. Zu den Details gehören AWS-Konto Informationen über den Zugriff auf einen Amazon S3 S3-Bucket, die IP-Adresse und die Uhrzeit des Ereignisses.
2.9.4	cloud-trail-cloud-watch-logs-aktiviert	Verwenden Sie Amazon CloudWatch , um Protokoll ereignisaktivitäten zentral zu sammeln und zu verwalten . Die Aufnahme von AWS CloudTrail Daten liefert Einzelheiten zu den API-Aufrufaktivitäten in Ihrem AWS-Konto.

Kontroll-ID	AWS Config	Empfehlungen
2.9.4	cloudtrail-enabled	AWS CloudTrail kann durch die Aufzeichnung von Aktionen und API-Aufrufen in der AWS Management Console bei der Nichtabst reitbarkeit helfen. Sie können die Benutzer und die Benutzer AWS-Konten , die einen AWS Dienst aufgerufen haben, die Quell-IP-Adresse, über die die Aufrufe generiert wurden, und den Zeitpunkt der Anrufe identifizieren. Einzelheiten zu den erfassten Daten finden Sie in den AWS CloudTrail Datensatzinhalten.
2.9.4	cw-loggroup-retention-period-überprüfen	Stellen Sie sicher, dass die Ereignisprotokolldaten für Ihre Protokollgruppen über eine Mindestdauer aufbewahrt werden, um die Fehlerbehebung und forensische Untersuch ungen zu unterstützen. Fehlende frühere Ereignisp rotokolldaten erschweren die Rekonstruierung und Identifiz ierung potenziell schädlicher Ereignisse.

Kontroll-ID	AWS Config	Empfehlungen
2.9.4	elb-logging-enabled	Die Elastic-Load-Balancing-Aktivität ist ein zentraler Kommunikationspunkt innerhalb einer Umgebung. Stellen Sie sicher, dass die ELB-Protokollierung aktiviert ist. Die gesammelten Daten enthalten detaillierte Informati onen zu Anfragen, die an den ELB gesendet wurden. Jedes Protokoll enthält Informati onen wie die Zeit, zu der die Anforderung einging, die Client-IP-Adresse, Latenzen, Anforderungspfade und Serverantworten.

Kontroll-ID	AWS Config	Empfehlungen
2.9.4	multi-region-cloudtrail-enabled	AWS CloudTrail zeichnet Aktionen und API-Aufrufe der AWS Management Console auf. Sie können feststellen, welche Benutzer und Konten angerufen wurden AWS, von welcher Quell-IP-Adresse aus die Anrufe getätigt wurden und wann die Anrufe erfolgten . CloudTrail übermittelt Protokolldateien aus allen AWS Regionen an Ihren S3-Bucket, wenn MULTI_REGION_CLOUD_TRAIL_ENABLED aktiviert ist. Außerdem wird beim AWS Start einer neuen Region derselbe Trail in der neuen Region erstellt. CloudTrail Dadurch erhalten Sie automatisch Protokoll dateien mit API-Aktivitäten für die neue Region.

Kontroll-ID	AWS Config	Empfehlungen
2.9.4	rds-logging-enabled	Um die Protokollierung und Überwachung in Ihrer Umgebung zu erleichtern, stellen Sie sicher, dass die Amazon Relational Database Service (Amazon RDS)-Protokollierung aktiviert ist. Mit der Amazon-RDS-Protokollierung können Sie Ereignisse wie Verbindungen, Verbindungsabbrüche, Abfragen oder abgefragte Tabellen erfassen.
2.9.4	s-3 bucket-logging-enabled	Die Amazon Simple Storage Service (Amazon S3)-Serverzugriffsprotokollierung bietet eine Methode zur Überwachung des Netzwerks im Hinblick auf potenzielle Cybersicherheitsereignisse. Die Ereignisse werden überwacht, indem detaillierte Aufzeichnungen über die Anfragen erfasst werden, die an einen Amazon-S3-Bucket gestellt wurden. Jeder Zugriffsprotokolleintrag enthält Details zu einer einzelnen Zugriffsanfrage. Zu den Details gehören Anforderer, Bucket-Name, Anforderungszeit, Anforderungsaktion, Antwortstatus und Fehlercode, falls relevant.

Kontroll-ID	AWS Config	Empfehlungen
2.9.4	vpc-flow-logs-enabled	VPC-Flow-Protokolle erfassen detaillierte Informationsdatensätze über den IP-Datenverkehr, der zu und von Netzwerkschnittstellen in Ihrer Amazon Virtual Private Cloud (Amazon VPC) fließt. Standardmäßig enthalten Flow-Protokolldatensätze Werte für die verschiedenen Komponenten des IP-Flows, einschließlich Quelle, Ziel und Protokoll.
2.9.4	wafv2-logging-enabled	Um die Protokollierung und Überwachung in Ihrer Umgebung zu erleichtern, aktivieren Sie die AWS WAF (V2) -Protokollierung im regionalen und globalen Web. ACLs AWS Die WAF-Protokollierung bietet detaillierte Informationen über den Datenverkehr, der von Ihrer Web-ACL analysiert wird. In den Protokollen werden die Uhrzeit aufgezeichnet, zu der die AWS WAF die Anfrage von Ihrer AWS Ressource erhalten hat, Informationen über die Anfrage und eine Aktion für die Regel, der jede Anfrage entsprach.

Kontroll-ID	AWS Config	Empfehlungen
2.10.3	ec-2 volume-inuse-check	Diese Regel stellt sicher, dass Amazon Elastic Block Store-Volumes, die an Amazon Elastic Compute Cloud (Amazon EC2) -Instances angehängt sind, zum Löschen markiert werden, wenn eine Instance beendet wird. Wenn ein Amazon-EBS-Volume nicht gelöscht wird, wenn die Instance, an die es angehängt ist, beendet wird, kann dies gegen das Konzept der geringsten Funktionalität verstoßen.
2.10.3	guardduty-enabled-centralized	Amazon GuardDuty kann mithilfe von Threat Intellige nce Feeds helfen, potenzielle Cybersicherheitsereignisse zu überwachen und zu erkennen. Dazu gehören Listen mit bösartigen IPs und maschinel len Lernmethoden zur Identifiz ierung unerwarteter, nicht autorisierter und bösartige r Aktivitäten in Ihrer AWS Cloud-Umgebung.

Kontroll-ID	AWS Config	Empfehlungen
2.10.3	guardduty-non-archived-findings	Amazon GuardDuty hilft Ihnen dabei, die Auswirkungen eines Vorfalls zu verstehen, indem es die Ergebnisse nach Schweregrad klassifiziert: niedrig, mittel und hoch. Diese Klassifizierungen können Sie zur Festlegung von entsprechenden Strategien und Prioritäten zur Behebung solcher Vorfälle verwenden. Mit dieser Regel können Sie optional daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7) und daysHighSev (Config Default: 1) für nicht archivierte Ergebnisse festlegen, wie es die Richtlinien Ihrer Organisation erfordern.

Kontroll-ID	AWS Config	Empfehlungen
2.10.3	ec2-prüfen managedinstance-association-compliance-status	Verwenden Sie AWS Systems Manager Associations, um bei der Inventarisierung von Softwareplattformen und Anwendungen innerhalb eines Unternehmens zu helfen. AWS Systems Manager weist Ihren verwalteten Instanzen einen Konfigurationsstatus zu und ermöglicht es Ihnen, Basiswerte für Betriebss ystem-Patch-Levels, Softwarei nstallationen, Anwendung skonfigurationen und andere Details zu Ihrer Umgebung festzulegen.
2.10.3	ec2-stopped-instance	Aktivieren Sie diese Regel, um bei der Basiskonfiguration von Amazon Elastic Compute Cloud (Amazon EC2) - Instances zu helfen, indem Sie überprüfen, ob EC2 Amazon-Instances gemäß den Standards Ihrer Organisat ion für mehr als die zulässige Anzahl von Tagen gestoppt wurden.

Kontroll-ID	AWS Config	Empfehlungen
2.10.5	alb-http-drop-invalid-Header-fähig	Stellen Sie sicher, dass Ihre Elastic Load Balancers (ELB) so konfiguriert sind, dass sie HTTP-Header löschen. Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.
2.10.5	alb-http-to-https-Umleitung sprüfung	Um Daten während der Übertragung zu schützen, stellen Sie sicher, dass Ihr Application Load Balancer unverschlüsselte HTTP-Anfragen automatisch an HTTPS umleitet. Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.
2.10.5	elasticsearch-node-to-node-Verschlüsselungsprüfung	Stellen Sie sicher, dass die node-to-node Verschlüsselung für Amazon OpenSearch Service aktiviert ist. Node-to-nodeVerschlüsselung ermöglicht die TLS 1.2-Versc hlüsselung für die gesamte Kommunikation innerhalb der Amazon Virtual Private Cloud (Amazon VPC). Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	AWS Config	Empfehlungen
2.10.5	elb-acm-certificate-required	Zum Schutz von eventuell vorhandenen sensiblen Daten sowie von Daten während der Übertragung muss die Verschlüsselung für Ihr Elastic Load Balancing aktiviert sein. Verwenden Sie AWS Certifica te Manager, um öffentlic he und private SSL/TLS-Z ertifikate mit AWS Diensten und internen Ressourcen zu verwalten, bereitzustellen und bereitzustellen.
2.10.5	elb-tls-https-listeners-nur	Stellen Sie sicher, dass Ihre Elastic Load Balancer (ELBs) mit SSL- oder HTTPS-Lis tenern konfiguriert sind. Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.
2.10.5	redshift-require-tls-ssl	Stellen Sie sicher, dass Ihre Amazon-Redshift-Cluster eine TLS/SSL-Verschlüsselung erfordern, um eine Verbindun g zu SQL-Clients herzustel len. Um eventuell vorhanden e sensible Daten zu schützen, sollten Sie die Verschlüs selung bei der Übertragung aktivieren.

Kontroll-ID	AWS Config	Empfehlungen
2.10,5	s-3 bucket-ssl-requests-only	Um Daten während der Übertragung zu schützen, stellen Sie sicher, dass Ihre Amazon Simple Storage Service (Amazon S3)-Bucke ts Anfragen zur Verwendun g von Secure Socket Layer (SSL)-Buckets erfordern. Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.
2,1,5	opensearch-node-to-node-Ver schlüsselungsprüfung	Stellen Sie sicher, dass die node-to-node Verschlüsselung für Amazon OpenSearch Service aktiviert ist. Node-to-nodeVerschlüsselung ermöglicht die TLS 1.2-Versc hlüsselung für die gesamte Kommunikation innerhalb der Amazon Virtual Private Cloud (Amazon VPC). Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	AWS Config	Empfehlungen
2.10.8	ec2-prüfen managedinstance-association-compliance-status	Verwenden Sie AWS Systems Manager Associations, um bei der Inventarisierung von Softwareplattformen und Anwendungen innerhalb eines Unternehmens zu helfen. AWS Systems Manager weist Ihren verwalteten Instanzen einen Konfigurationsstatus zu und ermöglicht es Ihnen, Basiswerte für Betriebss ystem-Patch-Levels, Softwarei nstallationen, Anwendung skonfigurationen und andere Details zu Ihrer Umgebung festzulegen.
2.10.8	ec2-prüfen managedinstance-patch-compliance-status	Aktivieren Sie diese Regel, um bei der Identifizierung und Dokumentation von Sicherhei tslücken in Amazon Elastic Compute Cloud (Amazon EC2) zu helfen. Die Regel prüft, ob die EC2 Amazon-In stance die Patch-Konformität im AWS Systems Manager gemäß den Richtlinien und Verfahren Ihrer Organisation einhält.

Kontroll-ID	AWS Config	Empfehlungen
2.11.2	guardduty-non-archived-findings	Amazon GuardDuty hilft Ihnen dabei, die Auswirkungen eines Vorfalls zu verstehen, indem es die Ergebnisse nach Schweregrad klassifiziert: niedrig, mittel und hoch. Diese Klassifizierungen können Sie zur Festlegung von entsprechenden Strategien und Prioritäten zur Behebung solcher Vorfälle verwenden. Mit dieser Regel können Sie optional daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7) und daysHighSev (Config Default: 1) für nicht archivierte Ergebnisse festlegen, wie es die Richtlinien Ihrer Organisation erfordern.

Kontroll-ID	AWS Config	Empfehlungen
2.11.3	cloudwatch-alarm-action-check	Amazon CloudWatch alarmiert, wenn eine Metrik den Schwellenwert für eine bestimmte Anzahl von Bewertungszeiträumen überschreitet. Der Alarm führt eine oder mehrere Aktionen durch, die vom Wert der Metrik oder des Ausdrucks im Vergleich zu einem Schwellenwert in einer Reihe von Zeiträumen abhängt. Diese Regel erfordert einen Wert für alarmActionRequired (Config Default: True), insufficientDataActionRequired (Config Default: True), okActionRequired (Config Default: False). Der tatsächliche Wert muss die Alarmaktionen für Ihre Umgebung widerspiegeln.
2.11.3	ec-2 instance-detailed-monitoring-enabled	Aktivieren Sie diese Regel, um die Amazon Elastic Compute Cloud (Amazon EC2) -Instance-Überwachung auf der EC2 Amazon-Konsole zu verbessern, in der Monitoring-Diagramme mit einem Zeitraum von 1 Minute für die Instance angezeigt werden.

Kontroll-ID	AWS Config	Empfehlungen
2.11.3	guardduty-enabled-centralized	Amazon GuardDuty kann mithilfe von Threat Intellige nce Feeds helfen, potenzielle Cybersicherheitsereignisse zu überwachen und zu erkennen. Dazu gehören Listen mit bösartigen IPs und maschinel len Lernmethoden zur Identifiz ierung unerwarteter, nicht autorisierter und bösartige r Aktivitäten in Ihrer AWS Cloud-Umgebung.
2.11.3	lambda-concurrency-check	Diese Regel stellt sicher, dass die Höchst- und Untergrenzen für die Gleichzeitigkeit einer Lambda-Funktion festgelegt werden. Dies kann Sie beim Baselining für die Anzahl der Anforderungen unterstüt zen, die Ihre Funktion zu einem bestimmten Zeitpunkt verarbeitet.

Kontroll-ID	AWS Config	Empfehlungen
2.11.3	rds-enhanced-monitoring-enabled	Aktivieren Sie Amazon Relational Database Service (Amazon RDS), um die Verfügbarkeit von Amazon RDS zu überwachen. Dies bietet einen detaillierten Einblick in den Zustand Ihrer Amazon-RDS-Datenbank-Instances. Wenn der Amazon-RDS-Speicher mehr als ein zugrunde liegendes physisches Gerät verwendet, erfasst Enhanced Monitoring die Daten für jedes Gerät. Wenn die Amazon-RDS-Datenbank-Instance in einer Multi-AZ-Bereitstellung ausgeführt wird, werden außerdem die Daten für jedes Gerät auf dem sekundären Host sowie die Metriken des sekundären Hosts erfasst.

Kontroll-ID	AWS Config	Empfehlungen
2.11.3	securityhub-enabled	AWS Security Hub hilft bei der Überwachung von unbefugte m Personal, Verbindungen, Geräten und Software. AWS Security Hub aggregiert, organisiert und priorisiert die Sicherheitswarnungen oder Ergebnisse mehrerer Dienste. AWS Einige dieser Dienste sind Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer und AWS Firewall Manager sowie AWS Partnerlösungen.
2.12	db-instance-backup-enabled	Die Sicherungsfunktion von Amazon RDS erstellt Sicherungen Ihrer Datenbank en und Transaktionsprotokolle. Amazon RDS erstellt einen Snapshot für das Speicherv olume Ihrer DB-Instance, sodass die gesamte DB-Instance gesichert wird. Sie können im System spezifisc he Aufbewahrungsfristen festlegen, um Ihre Ausfallsi cherheitsanforderungen zu erfüllen.

Kontroll-ID	AWS Config	Empfehlungen
2.12	dynamodb-autoscaling-enabled	Amazon DynamoDB Auto Scaling verwendet den AWS Application Auto Scaling-Service, um die bereitgestellte Durchsatzkapazität so anzupassen, dass sie automatisch auf tatsächliche Verkehrsmuster reagiert. Auf diese Weise kann eine Tabelle oder ein globaler sekundärer Index die bereitgestellte Lese-/Schreibkapazität erhöhen, um plötzliche Erhöhungen des Datenverkehrs ohne Drosselung zu bewältigen.
2.12	dynamodb-in-backup-plan	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon DynamoDB-Tabellen Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	AWS Config	Empfehlungen
2.12	ebs-in-backup-plan	Stellen Sie zur Unterstützung der Datensicherungsprozesse sicher, dass Ihre Amazon Elastic Block Store (Amazon EBS) -Volumes Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherung smanagement und erleichte rt Ihnen die Erfüllung von geschäftlichen und behördlic hen Compliance-Anforde rungen hinsichtlich Datensich erungen.

Kontroll-ID	AWS Config	Empfehlungen
2.12	efs-in-backup-plan	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon Elastic File System (Amazon EFS) - Dateisysteme Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.
2.12	elasticache-redis-cluster-automatic-Backup-Check	Wenn automatische Backups aktiviert sind, ElastiCache erstellt Amazon täglich ein Backup des Clusters. Die Sicherung kann für eine von Ihrer Organisation festgelegte Anzahl von Tagen aufbewahrt werden. Automatische Backups schützen vor Datenverlust. Bei einem Ausfall können Sie einen neuen Cluster erstellen, der Ihre Daten aus dem aktuellen Backup wiederherstellt.

Kontroll-ID	AWS Config	Empfehlungen
2.12	elb-cross-zone-load-Balancing aktiviert	Aktivieren Sie zonenüber greifendes Load Balancing für Ihre Elastic Load Balancer (ELBs), um eine angemesse ne Kapazität und Verfügbar keit aufrechtzuerhalten. Zonenübergreifendes Load Balancing reduziert die Notwendigkeit, die gleiche Anzahl von Instances in jeder aktivierten Availability Zone aufrechtzuerhalten. Es verbessert auch die Fähigkeit Ihrer Anwendung, den Verlust einer oder mehrerer Instances zu bewältigen.
2.12	elb-deletion-protection-ena bled	Diese Regel sorgt dafür, dass der Löschschutz für Elastic Load Balancing aktiviert ist. Verwenden Sie diese Funktion, um zu verhinder n, dass Ihr Load Balancer versehentlich oder böswillig gelöscht wird, was zum Verlust der Verfügbarkeit Ihrer Anwendungen führen kann.

Kontroll-ID	AWS Config	Empfehlungen
2.12	rds-instance-deletion-protection-aktiviert	Stellen Sie sicher, dass Amazon Relational Database Service (Amazon RDS)-Instances den Löschschutz aktiviert haben. Verwenden Sie den Löschschutz, um zu verhindern, dass Ihre Amazon-RDS-Instances versehentlich oder böswillig gelöscht werden, was zum Verlust der Verfügbarkeit Ihrer Anwendungen führen kann.
2.12	rds-in-backup-plan	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon Relational Database Service (Amazon RDS) -Instances Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	AWS Config	Empfehlungen
2.12	rds-multi-az-support	Die Multi-AZ-Unterstützung in Amazon Relational Database Service (Amazon RDS) bietet eine verbesserte Verfügbar keit und Beständigkeit von Datenbank-Instances. Wenn Sie eine Multi-AZ-Datenbank-Instance bereitstellen, erstellt Amazon RDS automatisch eine primäre Datenbank-Instance und repliziert die Daten synchron auf eine Standby-Instance in einer anderen Availability Zone. Jede Availability Zone läuft auf einer eigenen, physisch getrennten, unabhängigen Infrastruktur und ist auf eine hohe Verfügbarkeit ausgelegt . Im Falle eines Infrastru kturausfalls führt Amazon RDS einen automatischen Failover zum Standby-Modus durch, sodass Sie den Datenbank betrieb wieder aufnehmen können, sobald der Failover abgeschlossen ist.

Kontroll-ID	AWS Config	Empfehlungen
2.12	redshift-backup-enabled	Stellen Sie zur Unterstützung der Datensicherungsprozesse sicher, dass Ihre Amazon-Redshift-Cluster über automatisierte Snapshots verfügen. Wenn automatisierte Snapshots für einen Cluster aktiviert sind, erstellt Redshift in regelmäßigen Abständen Snapshots dieses Clusters. Standardmäßig erstellt Redshift alle acht Stunden oder alle 5 GB einen Snapshot für jeden Knoten mit Datenänderungen oder je nachdem, was zuerst eintritt.
2.12	s3- bucket-default-lock-enabled	Stellen Sie sicher, dass für Ihren Amazon Simple Storage Service (Amazon S3)-Bucket standardmäßig eine Sperre aktiviert ist. Zum Schutz eventuell vorhandener sensibler Daten in S3-Buckets müssen Sie Objektsperren für Daten im Ruhezustand erzwingen.

Kontroll-ID	AWS Config	Empfehlungen
2.12	s-3 bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) unterstützt die Aufrechte rhaltung einer angemessenen Kapazität und Verfügbarkeit. CRR ermöglicht das automatis che, asynchrone Kopieren von Objekten in Amazon-S3 -Buckets, um die Datenverf ügbarkeit sicherzustellen.
2.12	s-3 bucket-versioning-enabled	Die Versionsverwaltung von Amazon Simple Storage Service (Amazon S3)-Buckets hilft dabei, mehrere Varianten eines Objekts im selben Amazon-S3-Bucket zu speichern. Verwenden Sie die Versionsverwaltung, um sämtliche Versionen aller Objekte in Ihrem Amazon-S3-Bucket zu speichern, abzurufen oder wiederher zustellen. Mit der Versionsv erwaltung können Sie Versionen sowohl nach unbeabsichtigten Benutzera ktionen als auch nach Anwendungsfehlern problemlo s wiederherstellen.

Kontroll-ID	AWS Config	Empfehlungen
2.12	vpc-vpn-2-tunnels-up	Redundante Site-to-Site VPN-Tunnel können implement iert werden, um die Anforderu ngen an die Ausfallsicherheit zu erfüllen. Es verwendet zwei Tunnel, um die Konnektiv ität sicherzustellen, falls eine der Site-to-Site VPN-Verbi ndungen nicht verfügbar ist. Um sich vor einem Verbindun gsverlust zu schützen, können Sie für den Fall, dass Ihr Kunden-Gateway nicht verfügbar ist, eine zweite Site-to-Site VPN-Verbindung zu Ihrer Amazon Virtual Private Cloud (Amazon VPC) und Ihrem Virtual Private Gateway einrichten, indem Sie ein zweites Kunden-Gateway verwenden.

Kontroll-ID	AWS Config	Empfehlungen
2.12	aurora-resources-protected-by-Backup-Plan	Um Sie bei Datensich erungsprozessen zu unterstüt zen, stellen Sie sicher, dass Ihre Amazon Aurora Aurora-Ressourcen Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherung smanagement und erleichte rt Ihnen die Erfüllung von geschäftlichen und behördlic hen Compliance-Anforde rungen hinsichtlich Datensich erungen.

Kontroll-ID	AWS Config	Empfehlungen
2.12	backup-plan-min-frequency-and-min-retention-check	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihr AWS Backup-Plan auf eine Mindestfrequenz und Aufbewahrung festgelegt ist. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen. Mit dieser Regel können Sie die Parameter requiredFrequencyValue (Config default: 1), requiredRetentionDays (Config default: 35) und requiredFrequencyUnit (Config default: days) festlegen. Der tatsächliche Wert muss den Anforderungen Ihrer Organisation entsprechen.

Vorlage

Die Vorlage ist verfügbar unter GitHub: Operational Best Practices for K-ISMS.

Bewährte Methoden für die Ausführung von Load Balancing

Dieses Konformitätspaket enthält AWS Config Regeln, die auf dem internen AWS Lastenausgleich basieren. Eine Liste aller verwalteten Regeln, die von unterstützt werden AWS Config, finden Sie unter Liste der AWS Config verwalteten Regeln.

Die Namen und Beschreibungen der erforderlichen Parameter finden Sie im `Parameters` Abschnitt der folgenden Vorlage.

Die Vorlage ist verfügbar unter GitHub: Operational Best Practices for Load Balancing.

Betriebliche bewährte Methoden für die Protokollierung

Dieses Konformitätspaket enthält AWS Config Regeln, die auf der internen AWS Protokollierung basieren. Eine Liste aller verwalteten Regeln, die von unterstützt werden AWS Config, finden Sie unter Liste der AWS Config verwalteten Regeln.

Die Namen und Beschreibungen der erforderlichen Parameter finden Sie im `Parameters` Abschnitt der folgenden Vorlage.

Die Vorlage ist verfügbar unter GitHub: Operational Best Practices for Logging.

Bewährte Methoden für die Ausführung von Management- und Governance-Services

Dieses Konformitätspaket enthält AWS Config Regeln, die auf Management and Governance Services basieren. Weitere Informationen finden Sie unter Management and Governance unter AWS. Eine Liste aller verwalteten Regeln, die von unterstützt werden AWS Config, finden Sie unter Liste der AWS Config verwalteten Regeln.

Die Namen und Beschreibungen der erforderlichen Parameter finden Sie im `Parameters` Abschnitt der folgenden Vorlage.

Die Vorlage ist verfügbar unter GitHub: Operative Best Practices für Management- und Governance-Dienste.

Bewährte Methoden für die Verwendung der MAS Notice 655

Konformitätspakete bieten ein allgemeines Compliance-Framework, das es Ihnen ermöglicht, mithilfe verwalteter oder benutzerdefinierter AWS Config Regeln und Abhilfemaßnahmen Kontrollen zur

Sicherheits-, Betriebs- oder Kostenoptimierung durchzuführen. AWS Config Conformance Packs dienen als Beispielvorlagen nicht dazu, die vollständige Einhaltung eines bestimmten Governance- oder Compliance-Standards sicherzustellen. Sie sind dafür verantwortlich, selbst zu beurteilen, ob Ihre Nutzung der Services den geltenden gesetzlichen und behördlichen Anforderungen entspricht.

Im Folgenden finden Sie ein Beispiel für eine Zuordnung zwischen der Mitteilung 655 — Cyberhygiene der Monetary Authority of Singapur (MAS) und den AWS verwalteten Konfigurationsregeln. Jede Config-Regel gilt für eine bestimmte AWS Ressource und bezieht sich auf eine oder mehrere MAS-Mitteilung 655 — Cyber Hygiene Controls. Eine Kontrolle gemäß der MAS Notice 655 – Cyberhygiene kann sich auf mehrere Config-Regeln beziehen. In der folgenden Tabelle finden Sie weitere Informationen und Anleitungen zu diesen Zuordnungen.

Kontroll-ID	AWS Config	Empfehlungen
4.1	iam-user-no-policies-überprüfen	Diese Regel stellt sicher, dass AWS Identity and Access Management (IAM) -Richtlinien nur Gruppen oder Rollen zugewiesen werden, um den Zugriff auf Systeme und Ressourcen zu kontrollieren. Die Zuweisung von Berechtigungen auf Gruppen- oder Rollenebene trägt dazu bei, die Wahrscheinlichkeit zu verringern, dass eine Identität übermäßige Berechtigungen erhält oder beibehält.
4.1	access-keys-rotated	Die Anmeldeinformationen für autorisierte Geräte, Benutzer und Prozesse werden geprüft, indem sichergestellt wird, dass die IAM-Zugriffsschlüssel entsprechend den Vorgaben der Unternehmensrichtlinie rotiert werden. Das regelmäßi

Kontroll-ID	AWS Config	Empfehlungen
		ge Ändern der Zugriffss chlüssel ist eine bewährte Sicherheitsmethode. Es verkürzt den Zeitraum, in dem ein Zugriffsschlüssel aktiv ist, und reduziert die Auswirkun gen auf das Unternehmen, wenn die Schlüssel kompromit tiert werden. Diese Regel erfordert einen Wert für die Zugriffsschlüssel-Rotation (Standardkonfiguration: 90). Der tatsächliche Wert muss den Richtlinien Ihrer Organisat ion entsprechen.

Kontroll-ID	AWS Config	Empfehlungen
4.1	iam-user-unused-credentials-überprüfen	AWS Identity and Access Management (IAM) kann Ihnen bei Zugriffsberechtigungen und Autorisierungen helfen, indem es nach IAM-Passwörtern und Zugriffsschlüsseln sucht, die für einen bestimmten Zeitraum nicht verwendet wurden. Wenn ungenutzte Anmeldeinformationen identifiziert werden, müssen Sie sie deaktivieren und/oder entfernen, da dies gegen das Prinzip der geringsten Berechtigung verstoßen könnte. Für diese Regel müssen Sie einen Wert für das maxCredentialUsage Alter festlegen (Standardkonfiguration: 90). Der tatsächliche Wert muss den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	AWS Config	Empfehlungen
4.1	iam-password-policy	Die Identitäten und Anmeldein formationen werden auf der Grundlage einer organisat orischen IAM-Passwortrichtl inie ausgestellt, verwaltet und verifiziert. Sie erfüllen oder übertreffen die Anforderu ngen, die von NIST SP 800-63 und dem Standard „Best Practices“ von AWS Foundational Security in Bezug auf die Passwortstärke festgelegt wurden. Mit dieser Regel können Sie optional RequireUppercaseCharacters (Wert für AWS grundlege nde Sicherheitsbewährte Methoden: wahr), RequireLo wercaseCharacters (Wert für bewährte Methoden für AWS grundlegende Sicherheit: wahr), RequireSymbols (Wert für bewährte Methoden für AWS grundlegende Sicherhei t: wahr), RequireNumbers (Wert für bewährte Methoden für AWS grundlegende Sicherheit: wahr), MinimumPa sswordLength (Wert für bewährte Methoden für AWS grundlegende Sicherheit: 14), PasswordReusePreve ntion (Wert für bewährte Methoden für AWS grundlege

Kontroll-ID	AWS Config	Empfehlungen
		nde Sicherheit: 24) und MaxPasswordAge (Wert für bewährte Methoden für AWS grundlegende Sicherhei t: 90) für Ihr IAM festlegen Kennwortrichtlinie. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisat ion entsprechen.
4.1	root-account-mfa-enabled	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherste llen, dass MFA für den Root-Benutzer aktiviert ist. Der Stammbenutzer ist der AWS-Konto-Benutzer mit den meisten Berechtigungen. MFA sorgt für eine weitere Schutzebene zusätzlich zu den Anmeldeinformation en. Indem Sie MFA für den Root-Benutzer vorschrei ben, können Sie die Anzahl AWS-Konten kompromittierter Benutzer reduzieren.

Kontroll-ID	AWS Config	Empfehlungen
4.1	ec-2 instance-profile-attached	EC2 Instanzprofile übergeben eine IAM-Rolle an eine EC2 Instance. Das Anhängen eines Instance-Profils an Ihre Instances kann bei der Implementierung von geringsten Berechtigungen und der Berechtigungsverwa ltung helfen.

Kontroll-ID	AWS Config	Empfehlungen
4.1	iam-customer-policy-blocked-kms-Aktionen	AWS Identity and Access Management (IAM) kann Ihnen helfen, die Prinzipien der geringsten Rechte und der Aufgabentrennung in Zugriffsberechtigungen und Autorisierungen zu integrier en und so zu verhindern, dass Richtlinien blockierte Aktionen für alle AWS Schlüssel des Key Management Service enthalten. Wenn Benutzer mehr Rechte haben, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtig ung und Aufgabentrennung verstoßen. Mit dieser Regel können Sie den Parameter festlegen. blockedActionsPatt erns (Wert „AWS Bewährte grundlegende Sicherhei tsmethoden“: kms: Decrypt, kms:ReEncryptFrom). Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisat ion entsprechen.

Kontroll-ID	AWS Config	Empfehlungen
4.1	iam-inline-policy-blocked-kms-Aktionen	Stellen Sie sicher, dass ein Benutzer, eine IAM-Rolle oder eine IAM-Gruppe (AWS Identity and Access Management) nicht über eine Inline-Richtlinie verfügt, die blockierte Aktionen für alle AWS Schlüssel des Key Management Service zulässt. AWS empfiehlt, verwaltete Richtlinien anstelle von Inline-Richtlinien zu verwenden . Verwaltete Richtlinien ermöglichen Wiederverwendbarkeit, Versionsverwaltung, Rollback und Delegierung der Berechtigungsverwaltung. Mit dieser Regel können Sie den blockedActionsPatterns Parameter festlegen. (Wert „AWS Bewährte grundlegende Sicherheitsmethoden“: kms: Decrypt, kms:ReEncryptFrom). Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	AWS Config	Empfehlungen
4.1	iam-root-access-key-überprüfen	Der Zugriff auf Systeme und Ressourcen kann gesteuert werden, indem überprüft wird, ob der Root-Benutzer keine Zugriffsschlüssel mit seiner AWS Identity and Access Management (IAM) -Rolle verknüpft hat. Stellen Sie sicher, dass die Root-Zugriffsschlüssel gelöscht werden. Erstellen und verwenden Sie stattdessen rollenbasierte Funktionen, AWS-Konten um das Prinzip der geringsten Funktionalität zu berücksichtigen.
4.1	root-account-hardware-mfa-aktiviert	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Hardware-MFA für den Root-Benutzer aktiviert ist. Der Stammbenutzer ist der AWS-Konto-Benutzer mit den meisten Berechtigungen. MFA sorgt für eine weitere Schutzebene zusätzlich zu den Anmeldeinformationen. Indem Sie MFA für den Root-Benutzer vorschreiben, können Sie die Anzahl AWS-Konten kompromittierter Benutzer reduzieren.

Kontroll-ID	AWS Config	Empfehlungen
4.1	mfa-enabled-for-iam-Konsolenzugriff	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass MFA für alle AWS Identity and Access Management (IAM) -Benutzer aktiviert ist, die über ein Konsolenkennwort verfügen. MFA sorgt für eine weitere Schutzebene zusätzlich zu den Anmeldeinformationen. Indem Sie MFA für Benutzer vorschreiben, können Sie Fälle kompromittierter Konten reduzieren und verhindern, dass unbefugte Benutzer auf vertrauliche Daten zugreifen.
4.1	iam-user-mfa-enabled	Aktivieren Sie diese Regel, um den Zugriff auf Ressourcen in der AWS Cloud einzuschränken. Diese Regel sorgt dafür, dass die Multi-Faktor-Authentifizierung (MFA) für alle Benutzer aktiviert ist. MFA sorgt für eine weitere Schutzebene zusätzlich zu den Anmeldeinformationen. Reduzieren Sie Fälle von kompromittierten Konten, indem Sie MFA für Benutzer vorschreiben.

Kontroll-ID	AWS Config	Empfehlungen
4.1	emr-kerberos-enabled	Die Zugriffsberechtigungen und -autorisierungen können verwaltet und nach den Prinzipien der geringsten Berechtigung und Aufgabent rennung integriert werden, indem Kerberos für Amazon-EMR-Cluster aktiviert wird. In Kerberos werden Services und Benutzer, die sich authentifizieren müssen, als Prinzipale bezeichnet. Prinzipale befinden sich in einem Kerberos-Bereich. Innerhalb dieses Bereichs wird ein Kerberos-Server als Key Distribution Center (KDC) bezeichnet. Über diesen Server können sich Prinzipale authentifizieren. Die Authentifizierung im KDC erfolgt durch die Ausstellu ng von Authentifizierungs tickets. Das KDC unterhält eine Datenbank der Prinzipal e in seinem Bereich mit ihren Passwörtern und anderen administrativen Informationen zu jedem Prinzipal.

Kontroll-ID	AWS Config	Empfehlungen
4.1	iam-user-group-membership-überprüfen	AWS Identity and Access Management (IAM) kann Ihnen helfen, Zugriffsberechtigungen und Autorisierungen einzuschränken, indem sichergestellt wird, dass Benutzer Mitglieder mindestens einer Gruppe sind. Wenn Benutzern mehr Berechtigungen eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und Aufgabentrennung verstoßen.

Kontroll-ID	AWS Config	Empfehlungen
4.1	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) kann Ihnen dabei helfen, die Prinzipien der geringsten Rechte und der Aufgabent rennung in Zugriffsberechtigu ngen und Autorisierungen zu integrieren und so zu verhindern, dass Richtlinien „Effect“: „Allow“ mit „Action“: „*“ anstelle von „Resource“: „*“ enthalten. Wenn Benutzern mehr Rechte eingeräumt werden, als für die Ausführun g einer Aufgabe erforderl ich sind, kann dies gegen das Prinzip der geringste n Berechtigung und der Aufgabentrennung verstoßen.

Kontroll-ID	AWS Config	Empfehlungen
4.1	iam-no-inline-policy-überprüfen	Stellen Sie sicher, dass ein Benutzer, eine IAM-Rolle oder eine IAM-Gruppe (AWS Identity and Access Management) nicht über eine Inline-Richtlinie zur Zugriffskontrolle auf Systeme und Ressourcen verfügt. AWS empfiehlt, verwaltete Richtlinien anstelle von Inline-Richtlinien zu verwenden . Verwaltete Richtlinien ermöglichen Wiederverwendbarkeit, Versionsverwaltung, Rollback und Delegierung der Berechtigungsverwaltung.

Kontroll-ID	AWS Config	Empfehlungen
4.1	iam-group-has-users-überprüfen	AWS Identity and Access Management (IAM) kann Ihnen helfen, die Prinzipien der geringsten Rechte und der Aufgabentrennung mit Zugriffsberechtigungen und Autorisierungen zu integrieren, indem sichergestellt wird, dass IAM-Gruppen mindestens einen Benutzer haben. Die Einteilung von Benutzern in Gruppen auf der Grundlage der ihnen zugewiesenen Berechtigungen oder ihrer Funktion ist eine Möglichkeit, das Prinzip der geringsten Berechtigung zu implementieren.
4.1	secretsmanager-rotation-enabled-check	Diese Regel stellt sicher, dass bei AWS Secrets Manager Manager-Geheimnissen die Rotation aktiviert ist. Die regelmäßige Rotation von Secrets kann den Zeitraum verkürzen, in dem ein Secret aktiv ist, und möglicherweise die Auswirkungen auf das Unternehmen verringern, falls das Secret kompromittiert wird.

Kontroll-ID	AWS Config	Empfehlungen
4.1	secretsmanager-scheduled-rotation-success-überprüfen	Diese Regel stellt sicher, dass AWS Secrets Manager Manager-Geheimnisse gemäß dem Rotationsplan erfolgreich rotiert wurden. Die regelmäßige Rotation von Secrets kann den Zeitraum verkürzen, in dem ein Secret aktiv ist, und möglicherweise die Auswirkungen auf das Unternehmen verringern, falls es kompromittiert wird.
4.1	iam-policy-no-statements-with-full-access	Stellen Sie sicher, dass IAM-Aktionen nur auf die benötigten Aktionen beschränkt sind. Wenn Benutzern mehr Rechte eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und der Aufgabentrennung verstoßen.

Kontroll-ID	AWS Config	Empfehlungen
4.2	ec2-manager instance-managed-by-systems	Eine Bestandsaufnahme der Softwareplattformen und Anwendungen innerhalb des Unternehmens ist möglich, indem Amazon Elastic Compute Cloud (Amazon EC2) -Instances mit AWS Systems Manager verwaltet werden. Verwenden Sie AWS Systems Manager, um detaillierte Systemkonfigurationen, Betriebssystem-Patch-Levels, Namen und Typ der Dienste, Softwareinstallationen, Anwendungsname, Herausgeber und Version sowie andere Details zu Ihrer Umgebung bereitzustellen.
4.2	ec2-prüfen managedinstance-patch-compliance-status	Aktivieren Sie diese Regel, um bei der Identifizierung und Dokumentation von Sicherheitslücken in Amazon Elastic Compute Cloud (Amazon EC2) zu helfen. Die Regel prüft, ob die EC2 Amazon-Instance die Patch-Konformität im AWS Systems Manager gemäß den Richtlinien und Verfahren Ihrer Organisation einhält.

Kontroll-ID	AWS Config	Empfehlungen
4.2	ec2-prüfen managedinstance-association-compliance-status	Verwenden Sie AWS Systems Manager Associations, um bei der Inventarisierung von Softwareplattformen und Anwendungen innerhalb eines Unternehmens zu helfen. AWS Systems Manager weist Ihren verwalteten Instanzen einen Konfigurationsstatus zu und ermöglicht es Ihnen, Basiswerte für Betriebss ystem-Patch-Levels, Softwarei nstallationen, Anwendung skonfigurationen und andere Details zu Ihrer Umgebung festzulegen.

Kontroll-ID	AWS Config	Empfehlungen
4.2	redshift-cluster-maintenancesettings-check	Diese Regel stellt sicher, dass Amazon-Redshift-Cluster die bevorzugten Einstellungen für Ihre Organisation haben. Insbesondere sorgt sie dafür, dass Cluster bevorzugte Wartungsfenster und automatisierte Aufbewahrungsfristen für Snapshots für die Datenbank haben. Für diese Regel müssen Sie die festlegen allowVersionUpgrade. Der Standardwert ist „true“. Außerdem können Sie optional den Zeitraum preferredMaintenanceWindow (der Standardwert ist sa: 16:00 -sa: 16:30) und den automatedSnapshotRetention Zeitraum (der Standardwert ist 1) festlegen. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	AWS Config	Empfehlungen
4.2	ec2-imdsv2-check	Stellen Sie sicher, dass die Methode Instance Metadata Service Version 2 (IMDSv2) aktiviert ist, um den Zugriff auf und die Kontrolle der Amazon Elastic Compute Cloud (Amazon EC2) -Instance-Metadaten zu schützen. Die IMDSv2 Methode verwendet sitzungsbasierte Kontrolle n. Mit können Kontrollen implementiert werden IMDSv2, um Änderungen an Instanzme tadaten einzuschränken.
4.2	elastic-beanstalk-managed-updates-aktiviert	Durch die Aktivierung verwalteter Plattformupdates für eine Amazon-Elastic-Beanstalk-Umgebung wird sichergestellt, dass die aktuellen verfügbaren Plattform-Fixes, -Updates und -Features für die Umgebung installiert sind. Eine bewährte Methode zur Sicherung von Systemen besteht darin, stets die aktuellen Patches zu installieren.

Kontroll-ID	AWS Config	Empfehlungen
4.2	rds-automatic-minor-version-upgrade-fähig	Aktivieren Sie automatische Unterversions-Upgrades auf Ihren Amazon-Relational-Database-Service (RDS)-Instances, um sicherzustellen, dass die aktuellen Updates für Unterversionen des Relational Database Management System (RDBMS) installiert sind, die Sicherheitspatches und Bugfixes enthalten können.
4.2	ecr-private-image-scanning-aktiviert	Der Amazon Elastic Container Repository (ECR)-Image-Scan unterstützt die Identifizierung von Software-Schwachstellen in Ihren Container-Images. Durch die Aktivierung von Image-Scans in ECR-Repositorys werden die Integrität und Sicherheit der gespeicherten Images mit einer zusätzlichen Überprüfungsebene verbessert.

Kontroll-ID	AWS Config	Empfehlungen
4.3	ec2- -Manager instance-managed-by-systems	Eine Bestandsaufnahme der Softwareplattformen und Anwendungen innerhalb des Unternehmens ist möglich, indem Amazon Elastic Compute Cloud (Amazon EC2) -Instances mit AWS Systems Manager verwaltet werden. Verwenden Sie AWS Systems Manager, um detaillierte Systemkonfigurationen, Betriebssystem-Patch-Levels, Namen und Typ der Dienste, Softwareinstallationen, Anwendungsname, Herausgeber und Version sowie andere Details zu Ihrer Umgebung bereitzustellen.

Kontroll-ID	AWS Config	Empfehlungen
4.3	securityhub-enabled	AWS Security Hub hilft bei der Überwachung von unbefugte m Personal, Verbindungen, Geräten und Software. AWS Security Hub aggregiert, organisiert und priorisiert die Sicherheitswarnungen oder Ergebnisse mehrerer Dienste. AWS Einige dieser Dienste sind Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer und AWS Firewall Manager sowie AWS Partnerlösungen.
4.3	ec2-prüfen managedinstance-association-compliance-status	Verwenden Sie AWS Systems Manager Associations, um bei der Inventarisierung von Softwareplattformen und Anwendungen innerhalb eines Unternehmens zu helfen. AWS Systems Manager weist Ihren verwalteten Instanzen einen Konfigurationsstatus zu und ermöglicht es Ihnen, Basiswerte für Betriebss ystem-Patch-Levels, Softwarei nstallationen, Anwendung skonfigurationen und andere Details zu Ihrer Umgebung festzulegen.

Kontroll-ID	AWS Config	Empfehlungen
4.3	account-part-of-organizations	Durch die zentrale Verwaltung AWS-Konten innerhalb von AWS Organizations wird sichergestellt, dass die Konten den Vorschriften entsprechen. Eine fehlende zentrale Kontoverwaltung kann zu inkonsistenten Kontokonfigurationen führen, wodurch Ressourcen und sensible Daten offengelegt werden können.
4.4	alb-waf-enabled	Stellen Sie sicher, dass AWS WAF auf Elastic Load Balancers (ELB) aktiviert ist, um Webanwendungen zu schützen. Eine WAF trägt zum Schutz Ihrer Webanwendungen oder APIs vor gängigen Web-Exploits bei. Diese Web-Exploits können sich auf die Verfügbarkeit auswirken, die Sicherheit gefährden oder übermäßige Ressourcen in Ihrer Umgebung verbrauchen.

Kontroll-ID	AWS Config	Empfehlungen
4.4	dms-replication-not-public	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass auf DMS-Replikationsinstanzen nicht öffentlich zugegriffen werden kann. DMS-Replikations-I nstances können vertrauli che Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.
4.4	ebs-snapshot-public-restora ble-überprüfen	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass EBS-Snaps hots nicht öffentlich wiederher stellbar sind. EBS-Volume-Snapshots können vertrauli che Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.
4.4	ec-2 instance-no-public-ip	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon Elastic Compute Cloud (Amazon EC2) -Instances nicht öffentlich zugänglich sind. EC2 Amazon-Instances können vertrauliche Informati onen enthalten, und für solche Konten ist eine Zugriffsk ontrolle erforderlich.

Kontroll-ID	AWS Config	Empfehlungen
4.4	ec2- security-group-attached-to -einperiodisch	Diese Regel stellt sicher, dass die Sicherheitsgruppen an eine Amazon Elastic Compute Cloud (Amazon EC2) - Instance oder an eine ENI angehängt sind. Diese Regel unterstützt die Überwachu ng ungenutzter Sicherhei tsgruppen im Bestand und die Verwaltung Ihrer Umgebung.
4.4	elasticsearch-in-vpc-only	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass sich Amazon OpenSearch OpenSearch Service (Service) -Domains innerhalb einer Amazon Virtual Private Cloud (Amazon VPC) befinden. Eine OpenSearch Service-D omain innerhalb einer Amazon VPC ermöglicht die sichere Kommunikation zwischen OpenSearch Service und anderen Services innerhalb der Amazon VPC, ohne dass ein Internet-Gateway, ein NAT-Gerät oder eine VPN-Verbindung erforderlich ist.

Kontroll-ID	AWS Config	Empfehlungen
4.4	emr-master-no-public-ip	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon EMR-Cluster-Masterknoten nicht öffentlich zugänglich sind. Amazon-EMR-Cluster-Hauptknoten können vertrauliche Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.
4.4	guardduty-enabled-centralized	Amazon GuardDuty kann mithilfe von Threat Intelligence Feeds helfen, potenzielle Cybersicherheitsereignisse zu überwachen und zu erkennen. Dazu gehören Listen mit bösartigen IPs und maschinellen Lernmethoden zur Identifizierung unerwarteter, nicht autorisierter und bösartiger Aktivitäten in Ihrer AWS Cloud-Umgebung.

Kontroll-ID	AWS Config	Empfehlungen
4.4	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) Security Groups können bei der Verwaltung des Netzwerkz ugriffs helfen, indem sie eine statusbehaftete Filterung von eingehendem und ausgehend em Netzwerkverkehr zu Ressourcen bereitstellen. AWS Wenn Sie eingehenden (oder entfernten) Datenverk ehr von 0.0.0.0/0 bis Port 22 auf Ihren Ressourcen nicht zulassen, können Sie den Remote-Zugriff einschränken.

Kontroll-ID	AWS Config	Empfehlungen
4.4	ec-2 instances-in-vpc	Stellen Sie Amazon Elastic Compute Cloud (Amazon EC2) -Instances innerhalb einer Amazon Virtual Private Cloud (Amazon VPC) bereit, um eine sichere Kommunika tion zwischen einer Instance und anderen Services innerhalb der Amazon VPC zu ermöglichen, ohne dass ein Internet-Gateway, ein NAT-Gerät oder eine VPN-Verbi ndung erforderlich ist. Der gesamte Datenverkehr bleibt sicher in der AWS Cloud. Domains, die sich innerhalb einer VPC befinden, verfügen aufgrund ihrer logischen Isolierung im Vergleich zu Domains mit öffentlic hen Endpunkten über eine zusätzliche Sicherheitsebene. Weisen Sie EC2 Amazon-In stances einer Amazon VPC zu, um den Zugriff ordnungsg emäß zu verwalten.

Kontroll-ID	AWS Config	Empfehlungen
4.4	internet-gateway-authorized-vpc-nur	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Internet-Gateways nur mit autorisierter Amazon Virtual Private Cloud (Amazon VPC) verbunden sind. Internet-Gateways ermöglichen den bidirekti onalen Internetzugang zur und von der Amazon VPC, was möglicherweise zu einem unbefugten Zugriff auf Amazon-VPC-Ressourcen führen kann.
4.4	lambda-function-public-acce ss-verboten	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherste llen, dass AWS Lambda-Funktionen nicht öffentlich zugänglich sind. Der öffentlic he Zugriff kann möglicher weise die Verfügbarkeit von Ressourcen beeinträchtigen.

Kontroll-ID	AWS Config	Empfehlungen
4.4	lambda-inside-vpc	Stellen Sie AWS Lambda-Funktionen in einer Amazon Virtual Private Cloud (Amazon VPC) bereit, um eine sichere Kommunikation zwischen einer Funktion und anderen Diensten innerhalb der Amazon VPC zu gewährleisten. Bei dieser Konfiguration sind kein Internet-Gateway, kein NAT-Gerät und keine VPN-Verbindung erforderlich. Der gesamte Datenverkehr bleibt sicher in der Cloud. AWS Domains, die sich innerhalb einer VPC befinden, verfügen aufgrund ihrer logischen Isolierung im Vergleich zu Domains mit öffentlichen Endpunkten über eine zusätzliche Sicherheitsebene. Um den Zugriff ordnungsgemäß zu verwalten, sollten AWS Lambda-Funktionen einer VPC zugewiesen werden.

Kontroll-ID	AWS Config	Empfehlungen
4.4	rds-instance-public-access-überprüfen	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Relational Database Service (Amazon RDS) -Instances nicht öffentlich sind. Amazon-RDS-Datenbank-Instances können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.
4.4	rds-snapshots-public-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Relational Database Service (Amazon RDS) -Instances nicht öffentlich sind. Amazon-RDS-Datenbank-Instances können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.
4.4	waf-regional-rule-not-leer	Stellen Sie sicher, dass Ihre AWS WAF eine Regel hat, die nicht leer ist. Eine Regel ohne Bedingungen kann zu unbeabsichtigtem Verhalten führen.

Kontroll-ID	AWS Config	Empfehlungen
4.4	waf-regional-rulegroup-not-leer	Stellen Sie sicher, dass Ihre AWS WAF eine Regelgrup pe hat, die nicht leer ist. Eine leere Regelgruppe kann zu unbeabsichtigtem Verhalten führen.
4.4	waf-regional-webacl-not-leer	Eine an eine AWS WAF angehängte Web-ACL kann eine Sammlung von Regeln und Regelgruppen zur Überprüfung und Steuerung von Webanfragen enthalten . Wenn eine Web-ACL leer ist, wird der Webdatenverkehr weitergeleitet, ohne von der WAF erkannt oder bearbeitet zu werden.
4.4	netfw-policy-default-action-fragment-Pakete	Eine AWS Netzwerk-Firewall-Richtlinie definiert, wie Ihre Firewall den Verkehr in einer Amazon VPC überwacht und verarbeitet. Sie konfigurieren statusfreie und statusbeh aftete Regelgruppen, um Pakete und Datenverk ehrsströme zu filtern. Wenn Sie standardmäßig die Pass-Aktion verwenden, kann dies zu unbeabsichtigtem Datenverkehr führen.

Kontroll-ID	AWS Config	Empfehlungen
4.4	netfw-policy-default-action-vollständige Pakete	Eine AWS Netzwerk-Firewall-Richtlinie definiert, wie Ihre Firewall den Verkehr in einer Amazon VPC überwacht und verarbeitet. Sie konfigurieren statusfreie und statusbeh aftete Regelgruppen, um Pakete und Datenverk ehrsströme zu filtern. Wenn Sie standardmäßig die Pass-Aktion verwenden, kann dies zu unbeabsichtigtem Datenverkehr führen.
4.4	netfw-policy-rule-group-ass oziiert	Eine AWS Netzwerk-Firewall-Richtlinie definiert, wie Ihre Firewall den Verkehr in einer Amazon VPC überwacht und verarbeitet. Sie konfigurieren statusfreie und statusbehaftete Regelgruppen, um Pakete und Datenverkehrsströme zu filtern, und Sie definieren den standardmäßigen Umgang mit Datenverkehr.
4.4	netfw-stateless-rule-group-nicht leer	Eine AWS Netzwerkfirewall-R egelgruppe enthält Regeln, die definieren, wie Ihre Firewall den Verkehr in Ihrer VPC verarbeitet. Wenn eine leere statuslose Regelgruppe in einer Firewall-Richtlinie vorhanden ist, verarbeitet sie keinen Datenverkehr.

Kontroll-ID	AWS Config	Empfehlungen
4.4	redshift-cluster-public-access-überprüfen	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Redshift Redshift-Cluster nicht öffentlich sind. Amazon-Redshift-Cluster können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.
4.4	restricted-common-ports	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass gemeinsame Ports für Amazon Elastic Compute Cloud (Amazon EC2) - Sicherheitsgruppen eingeschränkt sind. Wenn der Zugriff auf Ports nicht auf vertrauenswürdige Quellen beschränkt wird, kann dies zu Angriffen auf die Verfügbarkeit, Integrität und Vertraulichkeit von Systemen führen. Mit dieser Regel können Sie optional die Parameter blockedPort1–blockedPort5 festlegen (Standardkonfigurationen: 20, 21, 3389, 3306, 4333). Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	AWS Config	Empfehlungen
4.4	account-level-public-accesss3-Blöcke-periodisch	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Simple Storage Service (Amazon S3) -Buckets nicht öffentlich zugänglich sind. Diese Regel trägt dazu bei, sensible Daten vor unbefugten Remote-Benutzern zu schützen, indem sie den öffentlichen Zugriff verhindert. Mit dieser Regel können Sie optional die Parameter ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) und restrictPublicBuckets Parameter (Config Default: True) festlegen. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	AWS Config	Empfehlungen
4.4	sagemaker-notebook-no-direct-Internetzugang	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass SageMaker Amazon-Notebooks keinen direkten Internetzugang zulassen. Indem Sie direkten Internetzugang blockieren, vermeiden Sie, dass unbefugte Benutzer auf sensible Daten zugreifen.
4.4	vpc-default-security-group-geschlossen	Sicherheitsgruppen von Amazon Elastic Compute Cloud (Amazon EC2) können bei der Verwaltung des Netzwerkzugriffs helfen, indem sie eine statusbehaftete Filterung des ein- und ausgehenden Netzwerkverkehrs zu Ressourcen bereitstellen. AWS Die Beschränkung des gesamten Datenverkehrs auf die Standardsicherheitsgruppe hilft dabei, den Fernzugriff auf Ihre Ressourcen einzuschränken. AWS

Kontroll-ID	AWS Config	Empfehlungen
4.4	vpc-sg-open-only-to-authorized-ports	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass gemeinsame Ports für Amazon Elastic Compute Cloud (Amazon EC2) - Sicherheitsgruppen eingeschränkt sind. Wenn der Zugriff auf Ports nicht auf vertrauenswürdige Quellen beschränkt wird, kann dies zu Angriffen auf die Verfügbarkeit, Integrität und Vertraulichkeit von Systemen führen. Durch die Beschränkung des Zugriffs auf Ressourcen innerhalb einer Sicherheitsgruppe aus dem Internet (0.0.0.0/0) kann der Remote-Zugriff auf interne Systeme gesteuert werden.
4.4	s-3 bucket-public-read-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie nur autorisierten Benutzern, Prozessen und Geräten Zugriff auf Amazon Simple Storage Service (Amazon S3) -Buckets gewähren. Die Verwaltung des Zugriffs sollte mit der Klassifizierung der Daten übereinstimmen.

Kontroll-ID	AWS Config	Empfehlungen
4.4	s-3 bucket-public-write-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie nur autorisierten Benutzern, Prozessen und Geräten Zugriff auf Amazon Simple Storage Service (Amazon S3) -Buckets gewähren. Die Verwaltung des Zugriffs sollte mit der Klassifizierung der Daten übereinstimmen.
4.4	no-unrestricted-route-to-igw	Stellen Sie sicher, dass EC2 Amazon-Routentabellen keine uneingeschränkten Routen zu einem Internet-Gateway enthalten. Durch das Entfernen oder Beschränken des Internetzugangs für Workloads innerhalb von Amazon VPCs können unbeabsichtigte Zugriffe in Ihrer Umgebung reduziert werden.

Kontroll-ID	AWS Config	Empfehlungen
4.4	s3 bucket-level-public-access -verboten	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Simple Storage Service (Amazon S3) -Buckets nicht öffentlich zugänglich sind. Diese Regel trägt dazu bei, sensible Daten vor unbefugten Remote-Benutzern zu schützen, indem sie den öffentlichen Zugriff auf Bucket-Ebene verhindert.
4.4	subnet-auto-assign-public-ip-deaktiviert	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon Virtual Private Cloud (VPC) -Subnetzen nicht automatisch eine öffentliche IP-Adresse zugewiesen wird. Amazon Elastic Compute Cloud (EC2) -Instances, die in Subnetzen gestartet werden, in denen dieses Attribut aktiviert ist, haben ihrer primären Netzwerkschnittstelle eine öffentliche IP-Adresse zugewiesen.

Kontroll-ID	AWS Config	Empfehlungen
4.4	autoscaling-launch-config-public-ip-deaktiviert	Wenn Sie Ihre Netzwerkschnittstellen mit einer öffentlichen IP-Adresse konfigurieren, sind die diesen Netzwerkschnittstellen zugehörigen Ressourcen über das Internet erreichbar. EC2 Ressourcen sollten nicht öffentlich zugänglich sein, da dies einen unbeabsichtigten Zugriff auf Ihre Anwendungen oder Server ermöglichen kann.
4.4	redshift-enhanced-vpc-routing-aktiviert	Mit Enhanced-VPC-Routing wird erzwungen, dass der gesamte COPY- und UNLOAD-Datenverkehr zwischen Ihrem Cluster und Datenrepositorys über Ihre Amazon VPC erfolgt. Anschließend können Sie VPC-Features wie Sicherheitsgruppen und Netzwerkzugriffskontrollllisten verwenden, um den Netzwerkverkehr zu schützen. Sie können auch VPC-Flow-Protokolle verwenden, um den Netzwerkverkehr zu überwachen.

Kontroll-ID	AWS Config	Empfehlungen
4.4	ssm-document-not-public	Stellen Sie sicher, dass AWS Systems Manager (SSM) - Dokumente nicht öffentlich sind, da dies einen unbeabsichtigten Zugriff auf Ihre SSM-Dokumente ermöglichen kann. Ein öffentliches SSM-Dokument kann Informationen über Ihr Konto, Ihre Ressourcen und internen Prozesse preisgeben.
4.4	api-gw-associated-with-WAF	AWS Mit WAF können Sie eine Reihe von Regeln (als Web Access Control List (Web ACL) bezeichnet) konfigurieren, die Webanfragen auf der Grundlage von anpassbaren Websicherheitsregeln und -bedingungen, die Sie definieren, zulassen, blockieren oder zählen. Stellen Sie sicher, dass Ihre Amazon-API-Gateway-Stufe mit einer WAF-Web-ACL verknüpft ist, um sie vor böswilligen Angriffen zu schützen.

Kontroll-ID	AWS Config	Empfehlungen
4.4	opensearch-in-vpc-only	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass sich Amazon OpenSearch Service-Domains innerhalb einer Amazon Virtual Private Cloud (Amazon VPC) befinden. Eine Amazon OpenSearch Service-Domain innerhalb einer Amazon VPC ermöglich t die sichere Kommunika tion zwischen Amazon OpenSearch Service und anderen Services innerhalb der Amazon VPC, ohne dass ein Internet-Gateway, ein NAT-Gerät oder eine VPN-Verbindung erforderlich ist.

Kontroll-ID	AWS Config	Empfehlungen
4.5	ec2-manager instance-managed-by-systems	Eine Bestandsaufnahme der Softwareplattformen und Anwendungen innerhalb des Unternehmens ist möglich, indem Amazon Elastic Compute Cloud (Amazon EC2) -Instances mit AWS Systems Manager verwaltet werden. Verwenden Sie AWS Systems Manager, um detaillierte Systemkonfigurationen, Betriebssystem-Patch-Levels, Namen und Typ der Dienste, Softwareinstallationen, Anwendungsname, Herausgeber und Version sowie andere Details zu Ihrer Umgebung bereitzustellen.
4.5	ec2-prüfen managedinstance-patch-compliance-status	Aktivieren Sie diese Regel, um bei der Identifizierung und Dokumentation von Sicherheitslücken in Amazon Elastic Compute Cloud (Amazon EC2) zu helfen. Die Regel prüft, ob die EC2 Amazon-Instance die Patch-Konformität im AWS Systems Manager gemäß den Richtlinien und Verfahren Ihrer Organisation einhält.

Kontroll-ID	AWS Config	Empfehlungen
4.5	ec2-prüfen managedinstance-association-compliance-status	Verwenden Sie AWS Systems Manager Associations, um bei der Inventarisierung von Softwareplattformen und Anwendungen innerhalb eines Unternehmens zu helfen. AWS Systems Manager weist Ihren verwalteten Instanzen einen Konfigurationsstatus zu und ermöglicht es Ihnen, Basiswerte für Betriebss ystem-Patch-Levels, Softwarei nstallationen, Anwendung skonfigurationen und andere Details zu Ihrer Umgebung festzulegen.
4.5	guardduty-enabled-centralized	Amazon GuardDuty kann mithilfe von Threat Intellige nce Feeds helfen, potenzielle Cybersicherheitsereignisse zu überwachen und zu erkennen. Dazu gehören Listen mit bösartigen IPs und maschinel len Lernmethoden zur Identifiz ierung unerwarteter, nicht autorisierter und bösartige r Aktivitäten in Ihrer AWS Cloud-Umgebung.

Kontroll-ID	AWS Config	Empfehlungen
4.6	iam-password-policy	Die Identitäten und Anmeldein formationen werden auf der Grundlage einer organisat orischen IAM-Passwortrichtl inie ausgestellt, verwaltet und verifiziert. Sie erfüllen oder übertreffen die Anforderungen des NIST SP 800-63 und des AWS Foundational Security Best Practices-Standards für die Passwortstärke. Mit dieser Regel können Sie optional RequireUppercaseCharacters (Wert für AWS grundlege nde Sicherheitsbewährte Methoden: wahr), RequireLo wercaseCharacters (Wert für bewährte Methoden für AWS grundlegende Sicherheit: wahr), RequireSymbols (Wert für bewährte Methoden für AWS grundlegende Sicherhei t: wahr), RequireNumbers (Wert für bewährte Methoden für AWS grundlegende Sicherheit: wahr), MinimumPa sswordLength (Wert für bewährte Methoden für AWS grundlegende Sicherheit: 14), PasswordReusePreve ntion (Wert für bewährte Methoden für AWS grundlege nde Sicherheit: 24) und MaxPasswordAge (Wert

Kontroll-ID	AWS Config	Empfehlungen
		für bewährte Methoden für AWS grundlegende Sicherhei t: 90) für Ihr IAM festlegen Kennwortrichtlinie. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisat ion entsprechen.
4.6	root-account-mfa-enabled	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherste llen, dass MFA für den Root-Benutzer aktiviert ist. Der Stammbenutzer ist der AWS-Konto-Benutzer mit den meisten Berechtigungen. MFA sorgt für eine weitere Schutzebene zusätzlich zu den Anmeldeinformation en. Indem Sie MFA für den Root-Benutzer vorschrei ben, können Sie die Anzahl AWS-Konten kompromittierter Benutzer reduzieren.

Kontroll-ID	AWS Config	Empfehlungen
4.6	iam-root-access-key-überprüfen	Der Zugriff auf Systeme und Ressourcen kann gesteuert werden, indem überprüft wird, ob der Root-Benutzer keine Zugriffsschlüssel mit seiner AWS Identity and Access Management (IAM) -Rolle verknüpft hat. Stellen Sie sicher, dass die Root-Zugriffsschlüssel gelöscht werden. Erstellen und verwenden Sie stattdessen rollenbasierte Funktionen, AWS-Konten um das Prinzip der geringsten Funktionalität zu berücksichtigen.
4.6	root-account-hardware-mfa-aktiviert	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Hardware-MFA für den Root-Benutzer aktiviert ist. Der Stammbenutzer ist der AWS-Konto-Benutzer mit den meisten Berechtigungen. MFA sorgt für eine weitere Schutzebene zusätzlich zu den Anmeldeinformationen. Indem Sie MFA für den Root-Benutzer vorschreiben, können Sie die Anzahl AWS-Konten kompromittierter Benutzer reduzieren.

Kontroll-ID	AWS Config	Empfehlungen
4.6	mfa-enabled-for-iam-Konsolenzugriff	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass MFA für alle AWS Identity and Access Management (IAM) -Benutzer aktiviert ist, die über ein Konsolenkennwort verfügen. MFA sorgt für eine weitere Schutzebene zusätzlich zu den Anmeldeinformationen. Indem Sie MFA für Benutzer vorschreiben, können Sie Fälle kompromittierter Konten reduzieren und verhindern, dass unbefugte Benutzer auf vertrauliche Daten zugreifen.
4.6	iam-user-mfa-enabled	Aktivieren Sie diese Regel, um den Zugriff auf Ressourcen in der AWS Cloud einzuschränken. Diese Regel sorgt dafür, dass die Multi-Faktor-Authentifizierung (MFA) für alle Benutzer aktiviert ist. MFA sorgt für eine weitere Schutzebene zusätzlich zu den Anmeldeinformationen. Reduzieren Sie Fälle von kompromittierten Konten, indem Sie MFA für Benutzer vorschreiben.

Vorlage

Die Vorlage ist verfügbar unter GitHub: Operational Best Practices for MAS Notice 655.

Bewährte Methoden für die Ausführung von MAS TRMG

Konformitätspakete bieten ein allgemeines Compliance-Framework, das es Ihnen ermöglicht, mithilfe verwalteter oder benutzerdefinierter AWS Config Regeln und Abhilfemaßnahmen Kontrollen zur Sicherheits-, Betriebs- oder Kostenoptimierung durchzuführen. AWS Config Conformance Packs dienen als Beispielvorlagen nicht dazu, die vollständige Einhaltung eines bestimmten Governance- oder Compliance-Standards sicherzustellen. Sie sind dafür verantwortlich, selbst zu beurteilen, ob Ihre Nutzung der Services den geltenden gesetzlichen und behördlichen Anforderungen entspricht.

Im Folgenden finden Sie ein Beispiel für eine Zuordnung zwischen den Technology Risk Management Guidelines (TRMG) der Monetary Authority of Singapur (MAS) vom Januar 2021 und den AWS Managed Config-Regeln. Jede AWS Config-Regel gilt für eine bestimmte AWS Ressource und bezieht sich auf ein oder mehrere MAS TRMG-Steuerelemente. Eine Kontrolle gemäß den TRMG der MAS vom Januar 2021 kann mehreren Config-Regeln zugeordnet werden. In der folgenden Tabelle finden Sie weitere Informationen und Anleitungen zu diesen Zuordnungen.

Kontroll-ID	AWS Config	Empfehlungen
3.3.1	account-part-of-organizations	Durch die zentrale Verwaltun g AWS-Konten innerhalb von AWS Organizations wird sichergestellt, dass die Konten den Vorschriften entsprech en. Eine fehlende zentrale Kontoverwaltung kann zu inkonsistenten Kontokonf igurationen führen, wodurch Ressourcen und sensible Daten offengelegt werden können.
5.4.3	codebuild-project-envvar-aw scred-überprüfen	Stellen Sie sicher, dass die Anmeldeinformationen AWS_ACCESS_KEY_ID

Kontroll-ID	AWS Config	Empfehlungen
		AWS_SECRET_ACCESS_KEY nicht in AWS Codebuild -Projektumgebungen vorhanden sind. Speichern Sie diese Variablen nicht als Klartext. Das Speichern dieser Variablen als Klartext bewirkt eine unbeabsichtigte Offenlegung von Daten sowie unberechtigte Zugriffe.
5.4.3	codebuild-project-source-repo-URL-Prüfung	Stellen Sie sicher, dass die URL des Quell-Repositorys GitHub oder des Bitbucket -Quell-Repositorys keine persönlichen Zugriffstoken oder Anmeldeinformationen in Codebuild-Projektumgebungen enthält. AWS Verwende OAuth anstelle von persönlichen Zugriffstoken oder Anmeldedaten die Autorisierung für den Zugriff auf GitHub Bitbucket-Repositorys.

Kontroll-ID	AWS Config	Empfehlungen
6.1.1	codebuild-project-envvar-awscred-überprüfen	Stellen Sie sicher, dass die Anmeldeinformationen AWS_ACCESS_KEY_ID AWS_SECRET_ACCESS_KEY nicht in AWS Codebuild -Projektumgebungen vorhanden sind. Speichern Sie diese Variablen nicht als Klartext. Das Speichern dieser Variablen als Klartext bewirkt eine unbeabsichtigte Offenlegung von Daten sowie unberechtigte Zugriffe.
6.1.2	codebuild-project-envvar-awscred-überprüfen	Stellen Sie sicher, dass die Anmeldeinformationen AWS_ACCESS_KEY_ID AWS_SECRET_ACCESS_KEY nicht in AWS Codebuild -Projektumgebungen vorhanden sind. Speichern Sie diese Variablen nicht als Klartext. Das Speichern dieser Variablen als Klartext bewirkt eine unbeabsichtigte Offenlegung von Daten sowie unberechtigte Zugriffe.

Kontroll-ID	AWS Config	Empfehlungen
6.1.4	ec2-manager instance-managed-by-systems	Eine Bestandsaufnahme der Softwareplattformen und Anwendungen innerhalb des Unternehmens ist möglich, indem Amazon Elastic Compute Cloud (Amazon EC2) -Instances mit AWS Systems Manager verwaltet werden. Verwenden Sie AWS Systems Manager, um detaillierte Systemkonfigurationen, Betriebssystem-Patch-Levels, Namen und Typ der Dienste, Softwareinstallationen, Anwendungsname, Herausgeber und Version sowie andere Details zu Ihrer Umgebung bereitzustellen.

Kontroll-ID	AWS Config	Empfehlungen
6.1.4	ec2-prüfen managedinstance-association-compliance-status	Verwenden Sie AWS Systems Manager Associations, um bei der Inventarisierung von Softwareplattformen und Anwendungen innerhalb eines Unternehmens zu helfen. AWS Systems Manager weist Ihren verwalteten Instanzen einen Konfigurationsstatus zu und ermöglicht es Ihnen, Basiswerte für Betriebss ystem-Patch-Levels, Softwarei nstallationen, Anwendung skonfigurationen und andere Details zu Ihrer Umgebung festzulegen.
6.1.4	ec2-prüfen managedinstance-patch-compliance-status	Aktivieren Sie diese Regel, um bei der Identifizierung und Dokumentation von Sicherhei tslücken in Amazon Elastic Compute Cloud (Amazon EC2) zu helfen. Die Regel prüft, ob die EC2 Amazon-In stance die Patch-Konformität im AWS Systems Manager gemäß den Richtlinien und Verfahren Ihrer Organisation einhält.

Kontroll-ID	AWS Config	Empfehlungen
6.2.1	elastic-beanstalk-managed-updates-aktiviert	Durch die Aktivierung verwalteter Plattformupdates für eine Amazon-Elastic-Beanstalk-Umgebung wird sichergestellt, dass die aktuellen verfügbaren Plattform-Fixes, -Updates und -Features für die Umgebung installiert sind. Eine bewährte Methode zur Sicherung von Systemen besteht darin, stets die aktuellen Patches zu installieren.
6.3.1	elastic-beanstalk-managed-updates-aktiviert	Durch die Aktivierung verwalteter Plattformupdates für eine Amazon-Elastic-Beanstalk-Umgebung wird sichergestellt, dass die aktuellen verfügbaren Plattform-Fixes, -Updates und -Features für die Umgebung installiert sind. Eine bewährte Methode zur Sicherung von Systemen besteht darin, stets die aktuellen Patches zu installieren.

Kontroll-ID	AWS Config	Empfehlungen
6.4.5	acm-certificate-expiration-check	Stellen Sie sicher, dass die Netzwerkintegrität geschützt ist, indem Sie sicherstellen, dass X509-Zertifikate von AWS ACM ausgestellt werden. Diese Zertifikate müssen gültig und dürfen nicht abgelaufe n sein. Für diese Regel ist ein Wert für erforderlich daysToExpiration (Wert für bewährte AWS Grundrege ln für Sicherheit: 90). Der tatsächliche Wert muss den Richtlinien Ihrer Organisation entsprechen.
6.4.5	alb-http-to-https-Umleitung sprüfung	Um Daten während der Übertragung zu schützen, stellen Sie sicher, dass Ihr Application Load Balancer unverschlüsselte HTTP-Anfragen automatisch an HTTPS umleitet. Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.
6.4.5	api-gw-ssl-enabled	Stellen Sie sicher, dass die REST-API-Stufen von Amazon API Gateway mit SSL-Zerti fikaten konfiguriert sind, damit Backend-Systeme überprüfe n können, ob Anforderungen von API Gateway stammen.

Kontroll-ID	AWS Config	Empfehlungen
6.4.5	cmk-backing-key-rotation-aktiviert	Aktivieren Sie die Schlüssel rotation, um sicherzustellen, dass Schlüssel rotiert werden, nachdem sie das Ende ihrer Krypto-Periode erreicht haben.
6.4.5	elasticsearch-node-to-node-Verschlüsselungsprüfung	Stellen Sie sicher, dass die node-to-node Verschlüsselung für Amazon OpenSearch Service aktiviert ist. Node-to-nodeVerschlüsselung ermöglicht die TLS 1.2-Verschlüsselung für die gesamte Kommunikation innerhalb der Amazon Virtual Private Cloud (Amazon VPC). Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.
6.4.5	opensearch-node-to-node-Verschlüsselungsprüfung	Stellen Sie sicher, dass die node-to-node Verschlüsselung für Amazon OpenSearch Service aktiviert ist. Node-to-nodeVerschlüsselung ermöglicht die TLS 1.2-Verschlüsselung für die gesamte Kommunikation innerhalb der Amazon Virtual Private Cloud (Amazon VPC). Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	AWS Config	Empfehlungen
6.4.5	opensearch-https-required	Da sensible Daten existiere n können und um Daten während der Übertragung zu schützen, sollten Sie sicherstellen, dass HTTPS für Verbindungen zu Ihren Amazon OpenSearch Service-Domains aktiviert ist.
6.4.5	elb-acm-certificate-required	Zum Schutz von eventuell vorhandenen sensiblen Daten sowie von Daten während der Übertragung muss die Verschlüsselung für Ihr Elastic Load Balancing aktiviert sein. Verwenden Sie AWS Certifica te Manager, um öffentlic he und private SSL/TLS-Z ertifikate mit AWS Diensten und internen Ressourcen zu verwalten, bereitzustellen und bereitzustellen.
6.4.5	elb-tls-https-listeners-nur	Stellen Sie sicher, dass Ihre Elastic Load Balancer (ELBs) mit SSL- oder HTTPS-Lis tenern konfiguriert sind. Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	AWS Config	Empfehlungen
6.4.5	elv 2 acm-certificate-required	Zum Schutz von eventuell vorhandenen sensiblen Daten sowie von Daten während der Übertragung muss die Verschlüsselung für Ihr Elastic Load Balancing aktiviert sein. Verwenden Sie AWS Certifica te Manager, um öffentlic he und private SSL/TLS-Z ertifikate mit AWS Diensten und internen Ressourcen zu verwalten, bereitzustellen und bereitzustellen.
6.4.5	redshift-require-tls-ssl	Stellen Sie sicher, dass Ihre Amazon-Redshift-Cluster eine TLS/SSL-Verschlüsselung erfordern, um eine Verbindun g zu SQL-Clients herzustel len. Um eventuell vorhanden e sensible Daten zu schützen, sollten Sie die Verschlüs selung bei der Übertragung aktivieren.

Kontroll-ID	AWS Config	Empfehlungen
6.4.5	s-3 bucket-ssl-requests-only	Um Daten während der Übertragung zu schützen, stellen Sie sicher, dass Ihre Amazon Simple Storage Service (Amazon S3)-Bucke ts Anfragen zur Verwendun g von Secure Socket Layer (SSL)-Buckets erfordern. Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.
6.4.6	api-gw-execution-logging-ak tiviert	Die API-Gateway-Protok ollierung zeigt detaillierte Ansichten der Benutzer, die auf die API zugegriffen haben, und wie diese Benutzer auf die API zugegriffen haben. Diese Einblicke ermöglichen die Transparenz von Benutzera ktivitäten.
6.4.6	cloud-trail-cloud-watch-logs-aktiviert	Verwenden Sie Amazon CloudWatch , um Protokoll ereignisaktivitäten zentral zu sammeln und zu verwalten . Die Aufnahme von AWS CloudTrail Daten liefert Einzelheiten zu den API-Aufru faktivitäten in Ihrem AWS-Konto.

Kontroll-ID	AWS Config	Empfehlungen
6.4.6	cloudtrail-enabled	AWS CloudTrail kann durch die Aufzeichnung von Aktionen und API-Aufrufen in der AWS Management Console bei der Nichtabst reitbarkeit helfen. Sie können die Benutzer und die Benutzer AWS-Konten , die einen AWS Dienst aufgerufen haben, die Quell-IP-Adresse, über die die Aufrufe generiert wurden, und den Zeitpunkt der Anrufe identifizieren. Einzelheiten zu den erfassten Daten finden Sie in den AWS CloudTrail Datensatzinhalten.

Kontroll-ID	AWS Config	Empfehlungen
6.4.6	cloud-trail-log-file-Validierung aktiviert	Verwenden Sie die AWS CloudTrail Protokolldateivalidierung, um die Integrität von Protokollen zu überprüfen. CloudTrail Mithilfe der Protokolldateivalidierung kann festgestellt werden, ob eine Protokolldatei geändert oder gelöscht wurde oder ob sie nach der Übermittlung CloudTrail unverändert geblieben ist. Dieses Feature wurde mit dem Branchenstandard entsprechenden Algorithmen entwickelt: SHA-256 für die Hashfunktion und SHA-256 mit RSA für digitale Signaturen. Aus diesem Grund ist es rechnerisch unmöglich, CloudTrail Protokolldateien unbemerkt zu ändern, zu löschen oder zu fälschen.

Kontroll-ID	AWS Config	Empfehlungen
6.4.6	elb-logging-enabled	Die Elastic-Load-Balancing-Aktivität ist ein zentraler Kommunikationspunkt innerhalb einer Umgebung. Stellen Sie sicher, dass die ELB-Protokollierung aktiviert ist. Die gesammelten Daten enthalten detaillierte Informati onen zu Anfragen, die an den ELB gesendet wurden. Jedes Protokoll enthält Informati onen wie die Zeit, zu der die Anforderung einging, die Client-IP-Adresse, Latenzen, Anforderungspfade und Serverantworten.

Kontroll-ID	AWS Config	Empfehlungen
6.4.6	multi-region-cloudtrail-enabled	AWS CloudTrail zeichnet Aktionen und API-Aufrufe der AWS Management Console auf. Sie können feststellen, welche Benutzer und Konten angerufen wurden AWS, von welcher Quell-IP-Adresse aus die Anrufe getätigt wurden und wann die Anrufe erfolgten . CloudTrail übermittelt Protokolldateien aus allen AWS Regionen an Ihren S3-Bucket, wenn MULTI_REGION_CLOUD_TRAIL_ENABLED aktiviert ist. Außerdem wird beim AWS Start einer neuen Region derselbe Trail in der neuen Region erstellt. CloudTrail Dadurch erhalten Sie automatisch Protokoll dateien mit API-Aktivitäten für die neue Region.

Kontroll-ID	AWS Config	Empfehlungen
6.4.6	rds-logging-enabled	Um die Protokollierung und Überwachung in Ihrer Umgebung zu erleichtern, stellen Sie sicher, dass die Amazon Relational Database Service (Amazon RDS)-Protokollierung aktiviert ist. Mit der Amazon-RDS-Protokollierung können Sie Ereignisse wie Verbindungen, Verbindungsabbrüche, Abfragen oder abgefragte Tabellen erfassen.

Kontroll-ID	AWS Config	Empfehlungen
6.4.6	redshift-cluster-configuration-check	Um Daten im Ruhezustand zu schützen, muss die Verschlüsselung für Ihre Amazon-Redshift-Cluster aktiviert sein. Sie müssen auch sicherstellen, dass die erforderlichen Konfigurationen auf Amazon-Redshift-Clustern bereitgestellt werden. Die Prüfungsprotokollierung muss aktiviert sein, um Informationen zu Verbindungen und Benutzeraktivitäten in der Datenbank bereitzustellen. Diese Regel erfordert, dass ein Wert für clusterDbEncrypted (Config Default: TRUE) und LoggingEnabled (Config Default: TRUE) gesetzt ist. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	AWS Config	Empfehlungen
6.4.6	s-3 bucket-logging-enabled	Die Amazon Simple Storage Service (Amazon S3)-Serverzugriffsprotokollierung bietet eine Methode zur Überwachung des Netzwerks im Hinblick auf potenzielle Cybersicherheitsereignisse. Die Ereignisse werden überwacht, indem detaillierte Aufzeichnungen über die Anfragen erfasst werden, die an einen Amazon-S3-Bucket gestellt wurden. Jeder Zugriffsprotokolleintrag enthält Details zu einer einzelnen Zugriffsanfrage. Zu den Details gehören Anforderer, Bucket-Name, Anforderungszeit, Anforderungsaktion, Antwortstatus und Fehlercode, falls relevant.

Kontroll-ID	AWS Config	Empfehlungen
6.4.6	wafv2-logging-enabled	Um die Protokollierung und Überwachung in Ihrer Umgebung zu erleichte rn, aktivieren Sie die AWS WAF (V2) -Protokollierung im regionalen und globalen Web. ACLs AWS Die WAF-Protokollierung bietet detaillie rte Informationen über den Datenverkehr, der von Ihrer Web-ACL analysiert wird. In den Protokollen werden die Uhrzeit aufgezeichnet, zu der die AWS WAF die Anfrage von Ihrer AWS Ressource erhalten hat, Informationen zu der Anfrage und eine Aktion für die Regel, der jede Anfrage entsprach.
6.4.7	api-gw-execution-logging-ak tiviert	Die API-Gateway-Protok ollierung zeigt detaillierte Ansichten der Benutzer, die auf die API zugegriffen haben, und wie diese Benutzer auf die API zugegriffen haben. Diese Einblicke ermöglichen die Transparenz von Benutzera ktivitäten.

Kontroll-ID	AWS Config	Empfehlungen
6.4.7	cloud-trail-cloud-watch-logs-aktiviert	Verwenden Sie Amazon CloudWatch , um Protokoll ereignisaktivitäten zentral zu sammeln und zu verwalten . Die Aufnahme von AWS CloudTrail Daten liefert Einzelheiten zu den API-Aufru faktivitäten in Ihrem AWS-Konto.
6.4.7	cloudtrail-enabled	AWS CloudTrail kann durch die Aufzeichnung von Aktionen und API-Aufrufen in der AWS Management Console bei der Nichtabst reitbarkeit helfen. Sie können die Benutzer und die Benutzer AWS-Konten , die einen AWS Dienst aufgerufen haben, die Quell-IP-Adresse, über die die Aufrufe generiert wurden, und den Zeitpunkt der Anrufe identifizieren. Einzelheiten zu den erfassten Daten finden Sie in den AWS CloudTrail Datensatzinhalten.

Kontroll-ID	AWS Config	Empfehlungen
6.4.7	cloud-trail-log-file-Validierung aktiviert	Verwenden Sie die AWS CloudTrail Protokolldateivalidierung, um die Integrität von Protokollen zu überprüfen. CloudTrail Mithilfe der Protokolldateivalidierung kann festgestellt werden, ob eine Protokolldatei geändert oder gelöscht wurde oder ob sie nach der Übermittlung CloudTrail unverändert geblieben ist. Dieses Feature wurde mit dem Branchenstandard entsprechenden Algorithmen entwickelt: SHA-256 für die Hashfunktion und SHA-256 mit RSA für digitale Signaturen. Aus diesem Grund ist es rechnerisch unmöglich, CloudTrail Protokolldateien unbemerkt zu ändern, zu löschen oder zu fälschen.
6.4.7	cloudtrail-s3-dataevents-enabled	Die Erfassung von Simple Storage Service (Amazon S3)-Datenereignissen unterstützt die Erkennung von ungewöhnlichen Aktivitäten. Zu den Details gehören AWS-Konto Informationen über den Zugriff auf einen Amazon S3 S3-Bucket, die IP-Adresse und die Uhrzeit des Ereignisses.

Kontroll-ID	AWS Config	Empfehlungen
6.4.7	cloudtrail-security-trail-enabled	Diese Regel trägt dazu bei, die Verwendung der AWS empfohlenen bewährten Sicherheitsmethoden für sicherzustellen AWS CloudTrail, indem geprüft wird, ob mehrere Einstellungen aktiviert sind. Dazu gehören die Verwendung von Protokoll verschlüsselung, Protokoll validierung und Aktivierung AWS CloudTrail in mehreren Regionen.
6.4.7	cw-loggroup-retention-period-überprüfen	Stellen Sie sicher, dass die Ereignisprotokolldaten für Ihre Protokollgruppen über eine Mindestdauer aufbewahrt werden, um die Fehlerbehebung und forensische Untersuch ungen zu unterstützen. Fehlende frühere Ereignisp rotokolldaten erschweren die Rekonstruierung und Identifiz ierung potenziell schädlicher Ereignisse.

Kontroll-ID	AWS Config	Empfehlungen
6.4.7	elb-logging-enabled	Die Elastic-Load-Balancing-Aktivität ist ein zentraler Kommunikationspunkt innerhalb einer Umgebung. Stellen Sie sicher, dass die ELB-Protokollierung aktiviert ist. Die gesammelten Daten enthalten detaillierte Informati onen zu Anfragen, die an den ELB gesendet wurden. Jedes Protokoll enthält Informati onen wie die Zeit, zu der die Anforderung einging, die Client-IP-Adresse, Latenzen, Anforderungspfade und Serverantworten.
6.4.7	guardduty-enabled-centralized	Amazon GuardDuty kann mithilfe von Threat Intellige nce Feeds helfen, potenzielle Cybersicherheitsereignisse zu überwachen und zu erkennen. Dazu gehören Listen mit bösartigen IPs und maschinel len Lernmethoden zur Identifiz ierung unerwarteter, nicht autorisierter und bösartige r Aktivitäten in Ihrer AWS Cloud-Umgebung.

Kontroll-ID	AWS Config	Empfehlungen
6.4.7	multi-region-cloudtrail-enabled	AWS CloudTrail zeichnet Aktionen und API-Aufrufe der AWS Management Console auf. Sie können feststellen, welche Benutzer und Konten angerufen wurden AWS, von welcher Quell-IP-Adresse aus die Anrufe getätigt wurden und wann die Anrufe erfolgten . CloudTrail übermittelt Protokolldateien aus allen AWS Regionen an Ihren S3-Bucket, wenn MULTI_REG ION_CLOUD_TRAIL_EN ABLED aktiviert ist. Außerdem wird beim AWS Start einer neuen Region derselbe Trail in der neuen Region erstellt. CloudTrail Dadurch erhalten Sie automatisch Protokoll dateien mit API-Aktivitäten für die neue Region.

Kontroll-ID	AWS Config	Empfehlungen
6.4.7	rds-logging-enabled	Um die Protokollierung und Überwachung in Ihrer Umgebung zu erleichtern, stellen Sie sicher, dass die Amazon Relational Database Service (Amazon RDS)-Protokollierung aktiviert ist. Mit der Amazon-RDS-Protokollierung können Sie Ereignisse wie Verbindungen, Verbindungsabbrüche, Abfragen oder abgefragte Tabellen erfassen.

Kontroll-ID	AWS Config	Empfehlungen
6.4.7	redshift-cluster-configuration-check	Um Daten im Ruhezustand zu schützen, muss die Verschlüsselung für Ihre Amazon-Redshift-Cluster aktiviert sein. Sie müssen auch sicherstellen, dass die erforderlichen Konfigurationen auf Amazon-Redshift-Clustern bereitgestellt werden. Die Prüfungsprotokollierung muss aktiviert sein, um Informationen zu Verbindungen und Benutzeraktivitäten in der Datenbank bereitzustellen. Diese Regel erfordert, dass ein Wert für clusterDbEncrypted (Config Default: TRUE) und LoggingEnabled (Config Default: TRUE) gesetzt ist. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	AWS Config	Empfehlungen
6.4.7	s-3 bucket-logging-enabled	Die Amazon Simple Storage Service (Amazon S3)-Serverzugriffsprotokollierung bietet eine Methode zur Überwachung des Netzwerks im Hinblick auf potenzielle Cybersicherheitsereignisse. Die Ereignisse werden überwacht, indem detaillierte Aufzeichnungen über die Anfragen erfasst werden, die an einen Amazon-S3-Bucket gestellt wurden. Jeder Zugriffsprotokolleintrag enthält Details zu einer einzelnen Zugriffsanfrage. Zu den Details gehören Anforderer, Bucket-Name, Anforderungszeit, Anforderungsaktion, Antwortstatus und Fehlercode, falls relevant.

Kontroll-ID	AWS Config	Empfehlungen
6.4.7	securityhub-enabled	AWS Security Hub hilft bei der Überwachung von unbefugte m Personal, Verbindungen, Geräten und Software. AWS Security Hub aggregiert, organisiert und priorisiert die Sicherheitswarnungen oder Ergebnisse mehrerer Dienste. AWS Einige dieser Dienste sind Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer und AWS Firewall Manager sowie AWS Partnerlösungen.

Kontroll-ID	AWS Config	Empfehlungen
6.4.7	wafv2-logging-enabled	Um die Protokollierung und Überwachung in Ihrer Umgebung zu erleichte rn, aktivieren Sie die AWS WAF (V2) -Protokollierung im regionalen und globalen Web. ACLs AWS Die WAF-Protokollierung bietet detaillie rte Informationen über den Datenverkehr, der von Ihrer Web-ACL analysiert wird. In den Protokollen werden die Uhrzeit aufgezeichnet, zu der die AWS WAF die Anfrage von Ihrer AWS Ressource erhalten hat, Informationen zu der Anfrage und eine Aktion für die Regel, der jede Anfrage entsprach.

Kontroll-ID	AWS Config	Empfehlungen
6.4.8	dynamodb-autoscaling-enabled	Amazon DynamoDB Auto Scaling verwendet den AWS Application Auto Scaling-Service, um die bereitgestellte Durchsatzkapazität so anzupassen, dass sie automatisch auf tatsächliche Verkehrsmuster reagiert. Auf diese Weise kann eine Tabelle oder ein globaler sekundärer Index die bereitgestellte Lese-/Schreibkapazität erhöhen, um plötzliche Erhöhungen des Datenverkehrs ohne Drosselung zu bewältigen.
6.4.8	s-3 bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) unterstützt die Aufrechterhaltung einer angemessenen Kapazität und Verfügbarkeit. CRR ermöglicht das automatische, asynchrone Kopieren von Objekten in Amazon-S3-Buckets, um die Datenverfügbarkeit sicherzustellen.

Kontroll-ID	AWS Config	Empfehlungen
6.4.8	autoscaling-group-elb-healthcheck-erforderlich	Die Elastic Load Balancer (ELB) -Zustandsprüfungen für Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling Scaling-Gruppen unterstützen die Aufrechterhaltung einer angemessenen Kapazität und Verfügbarkeit. Der Load Balancer sendet regelmäßig Pings, versucht Verbindungen herzustellen oder sendet Anfragen, um den Zustand der EC2 Amazon-Instances in einer Gruppe mit auto-scaling zu testen. Wenn eine Instance nicht zurückmeldet, wird der Traffic an eine neue EC2 Amazon-Instance gesendet.

Kontroll-ID	AWS Config	Empfehlungen
6.4.8	elb-cross-zone-load-Balancing aktiviert	Aktivieren Sie zonenüber greifendes Load Balancing für Ihre Elastic Load Balancer (ELBs), um eine angemesse ne Kapazität und Verfügbar keit aufrechtzuerhalten. Zonenübergreifendes Load Balancing reduziert die Notwendigkeit, die gleiche Anzahl von Instances in jeder aktivierten Availability Zone aufrechtzuerhalten. Es verbessert auch die Fähigkeit Ihrer Anwendung, den Verlust einer oder mehrerer Instances zu bewältigen.
6.4.8	elb-deletion-protection-ena bled	Diese Regel sorgt dafür, dass der Löschschutz für Elastic Load Balancing aktiviert ist. Verwenden Sie diese Funktion, um zu verhinder n, dass Ihr Load Balancer versehentlich oder böswillig gelöscht wird, was zum Verlust der Verfügbarkeit Ihrer Anwendungen führen kann.

Kontroll-ID	AWS Config	Empfehlungen
6.4.8	rds-instance-deletion-protection-aktiviert	Stellen Sie sicher, dass Amazon Relational Database Service (Amazon RDS)-Instances den Löschschutz aktiviert haben. Verwenden Sie den Löschschutz, um zu verhindern, dass Ihre Amazon-RDS-Instances versehentlich oder böswillig gelöscht werden, was zum Verlust der Verfügbarkeit Ihrer Anwendungen führen kann.

Kontroll-ID	AWS Config	Empfehlungen
6.4.8	rds-multi-az-support	Die Multi-AZ-Unterstützung in Amazon Relational Database Service (Amazon RDS) bietet eine verbesserte Verfügbar keit und Beständigkeit von Datenbank-Instances. Wenn Sie eine Multi-AZ-Datenbank-Instance bereitstellen, erstellt Amazon RDS automatisch eine primäre Datenbank-Instance und repliziert die Daten synchron auf eine Standby-Instance in einer anderen Availability Zone. Jede Availability Zone läuft auf einer eigenen, physisch getrennten, unabhängigen Infrastruktur und ist auf eine hohe Verfügbarkeit ausgelegt . Im Falle eines Infrastru kturausfalls führt Amazon RDS einen automatischen Failover zum Standby-Modus durch, sodass Sie den Datenbank betrieb wieder aufnehmen können, sobald der Failover abgeschlossen ist.

Kontroll-ID	AWS Config	Empfehlungen
6.4.8	vpc-vpn-2-tunnels-up	Redundante Site-to-Site VPN-Tunnel können implement iert werden, um die Anforderu ngen an die Ausfallsicherheit zu erfüllen. Es verwendet zwei Tunnel, um die Konnektiv ität sicherzustellen, falls eine der Site-to-Site VPN-Verbi ndungen nicht verfügbar ist. Um sich vor einem Verbindun gsverlust zu schützen, können Sie für den Fall, dass Ihr Kunden-Gateway nicht verfügbar ist, eine zweite Site-to-Site VPN-Verbindung zu Ihrer Amazon Virtual Private Cloud (Amazon VPC) und Ihrem Virtual Private Gateway einrichten, indem Sie ein zweites Kunden-Gateway verwenden.

Kontroll-ID	AWS Config	Empfehlungen
7.2.1	ec2-manager instance-managed-by-systems	Eine Bestandsaufnahme der Softwareplattformen und Anwendungen innerhalb des Unternehmens ist möglich, indem Amazon Elastic Compute Cloud (Amazon EC2) -Instances mit AWS Systems Manager verwaltet werden. Verwenden Sie AWS Systems Manager, um detaillierte Systemkonfigurationen, Betriebssystem-Patch-Levels, Namen und Typ der Dienste, Softwareinstallationen, Anwendungsname, Herausgeber und Version sowie andere Details zu Ihrer Umgebung bereitzustellen.

Kontroll-ID	AWS Config	Empfehlungen
7.2.1	ec2-check managedinstance-association-compliance-status	Verwenden Sie AWS Systems Manager Associations, um bei der Inventarisierung von Softwareplattformen und Anwendungen innerhalb eines Unternehmens zu helfen. AWS Systems Manager weist Ihren verwalteten Instanzen einen Konfigurationsstatus zu und ermöglicht es Ihnen, Basiswerte für Betriebss ystem-Patch-Levels, Softwarei nstallationen, Anwendung skonfigurationen und andere Details zu Ihrer Umgebung festzulegen.

Kontroll-ID	AWS Config	Empfehlungen
7.4.1	ec2-manager instance-managed-by-systems	Eine Bestandsaufnahme der Softwareplattformen und Anwendungen innerhalb des Unternehmens ist möglich, indem Amazon Elastic Compute Cloud (Amazon EC2) -Instances mit AWS Systems Manager verwaltet werden. Verwenden Sie AWS Systems Manager, um detaillierte Systemkonfigurationen, Betriebssystem-Patch-Levels, Namen und Typ der Dienste, Softwareinstallationen, Anwendungsname, Herausgeber und Version sowie andere Details zu Ihrer Umgebung bereitzustellen.

Kontroll-ID	AWS Config	Empfehlungen
7.4.1	ec2-check managedinstance-association-compliance-status	Verwenden Sie AWS Systems Manager Associations, um bei der Inventarisierung von Softwareplattformen und Anwendungen innerhalb eines Unternehmens zu helfen. AWS Systems Manager weist Ihren verwalteten Instanzen einen Konfigurationsstatus zu und ermöglicht es Ihnen, Basiswerte für Betriebss ystem-Patch-Levels, Softwarei nstallationen, Anwendung skonfigurationen und andere Details zu Ihrer Umgebung festzulegen.
7.4.1	ec2-check managedinstance-patch-compliance-status	Aktivieren Sie diese Regel, um bei der Identifizierung und Dokumentation von Sicherhei tslücken in Amazon Elastic Compute Cloud (Amazon EC2) zu helfen. Die Regel prüft, ob die EC2 Amazon-In stance die Patch-Konformität im AWS Systems Manager gemäß den Richtlinien und Verfahren Ihrer Organisation einhält.

Kontroll-ID	AWS Config	Empfehlungen
7.4.1	elastic-beanstalk-managed-updates-aktiviert	Durch die Aktivierung verwalteter Plattformupdates für eine Amazon-Elastic-Beanstalk-Umgebung wird sichergestellt, dass die aktuellen verfügbaren Plattform-Fixes, -Updates und -Features für die Umgebung installiert sind. Eine bewährte Methode zur Sicherung von Systemen besteht darin, stets die aktuellen Patches zu installieren.
7.4.1	rds-automatic-minor-version-upgrade-fähig	Aktivieren Sie automatische Unterversions-Upgrades auf Ihren Amazon-Relational-Database-Service (RDS)-Instances, um sicherzustellen, dass die aktuellen Updates für Unterversionen des Relational Database Management System (RDBMS) installiert sind, die Sicherheitspatches und Bugfixes enthalten können.

Kontroll-ID	AWS Config	Empfehlungen
7.4.1	redshift-cluster-maintenancesettings-check	Diese Regel stellt sicher, dass Amazon-Redshift-Cluster die bevorzugten Einstellungen für Ihre Organisation haben. Insbesondere sorgt sie dafür, dass Cluster bevorzugte Wartungsfenster und automatisierte Aufbewahrungsfristen für Snapshots für die Datenbank haben. Für diese Regel müssen Sie die festlegen. allowVersionUpgrade Der Standardwert ist „true“. Außerdem können Sie optional den Zeitraum preferredMaintenanceWindow (der Standardwert ist sa: 16:00 -sa: 16:30) und den automatedSnapshotRetention Zeitraum (der Standardwert ist 1) festlegen. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	AWS Config	Empfehlungen
7.5.5	db-instance-backup-enabled	Die Sicherungsfunktion von Amazon RDS erstellt Sicherungen Ihrer Datenbank en und Transaktionsprotokolle. Amazon RDS erstellt einen Snapshot für das Speicherv olume Ihrer DB-Instance, sodass die gesamte DB-Instance gesichert wird. Sie können im System spezifisc he Aufbewahrungsfristen festlegen, um Ihre Ausfallsi cherheitsanforderungen zu erfüllen.
7.5.5	dynamodb-in-backup-plan	Um Sie bei Datensich erungsprozessen zu unterstüt zen, stellen Sie sicher, dass Ihre Amazon DynamoDB-Tabellen Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherung smanagement und erleichte rt Ihnen die Erfüllung von geschäftlichen und behördlic hen Compliance-Anforde rungen hinsichtlich Datensich erungen.

Kontroll-ID	AWS Config	Empfehlungen
7.5.5	dynamodb-pitr-enabled	Aktivieren Sie diese Regel, um zu überprüfen, ob die Informationen gesichert wurden. Es verwaltet auch die Backups, indem es sicherste llt, dass die point-in-time Wiederherstellung in Amazon DynamoDB aktiviert ist. Bei der Wiederherstellung werden fortlaufende Backups Ihrer Tabelle für die letzten 35 Tage gespeichert.
7.5.5	ebs-in-backup-plan	Stellen Sie zur Unterstützung der Datensicherungsprozesse sicher, dass Ihre Amazon Elastic Block Store (Amazon EBS) -Volumes Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherung smanagement und erleichte rt Ihnen die Erfüllung von geschäftlichen und behördlic hen Compliance-Anforde rungen hinsichtlich Datensich erungen.

Kontroll-ID	AWS Config	Empfehlungen
7.5.5	efs-in-backup-plan	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon Elastic File System (Amazon EFS) - Dateisysteme Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.
7.5.5	elasticache-redis-cluster-automatic-Backup-Check	Wenn automatische Backups aktiviert sind, ElastiCache erstellt Amazon täglich ein Backup des Clusters. Die Sicherung kann für eine von Ihrer Organisation festgelegte Anzahl von Tagen aufbewahrt werden. Automatische Backups schützen vor Datenverlust. Bei einem Ausfall können Sie einen neuen Cluster erstellen, der Ihre Daten aus dem aktuellen Backup wiederherstellt.

Kontroll-ID	AWS Config	Empfehlungen
7.5.5	rds-in-backup-plan	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon Relational Database Service (Amazon RDS) -Instances Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	AWS Config	Empfehlungen
7.5.5	redshift-backup-enabled	Stellen Sie zur Unterstützung der Datensicherungsprozesse sicher, dass Ihre Amazon-Redshift-Cluster über automatisierte Snapshots verfügen. Wenn automatisierte Snapshots für einen Cluster aktiviert sind, erstellt Redshift in regelmäßigen Abständen Snapshots dieses Clusters. Standardmäßig erstellt Redshift alle acht Stunden oder alle 5 GB einen Snapshot für jeden Knoten mit Datenänderungen oder je nachdem, was zuerst eintritt.
7.5.5	s-3 bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) unterstützt die Aufrechterhaltung einer angemessenen Kapazität und Verfügbarkeit. CRR ermöglicht das automatische, asynchrone Kopieren von Objekten in Amazon-S3-Buckets, um die Datenverfügbarkeit sicherzustellen.

Kontroll-ID	AWS Config	Empfehlungen
7.5.5	s-3 bucket-versioning-enabled	Die Versionsverwaltung von Amazon Simple Storage Service (Amazon S3)-Buckets hilft dabei, mehrere Varianten eines Objekts im selben Amazon-S3-Bucket zu speichern. Verwenden Sie die Versionsverwaltung, um sämtliche Versionen aller Objekte in Ihrem Amazon-S3-Bucket zu speichern, abzurufen oder wiederher zustellen. Mit der Versionsv erwaltung können Sie Versionen sowohl nach unbeabsichtigten Benutzera ktionen als auch nach Anwendungsfehlern problemlo s wiederherstellen.
7.5.7	api-gw-execution-logging-ak tiviert	Die API-Gateway-Protok ollierung zeigt detaillierte Ansichten der Benutzer, die auf die API zugegriffen haben, und wie diese Benutzer auf die API zugegriffen haben. Diese Einblicke ermöglichen die Transparenz von Benutzera ktivitäten.

Kontroll-ID	AWS Config	Empfehlungen
7.5.7	cloud-trail-cloud-watch-logs-aktiviert	Verwenden Sie Amazon CloudWatch , um Protokoll ereignisaktivitäten zentral zu sammeln und zu verwalten . Die Aufnahme von AWS CloudTrail Daten liefert Einzelheiten zu den API-Aufru faktivitäten in Ihrem AWS-Konto.
7.5.7	cloudtrail-enabled	AWS CloudTrail kann bei der Nichtabstreitbarkeit helfen, indem Aktionen und API-Aufrufe der AWS Managemen t Console aufgezeichnet werden. Sie können die Benutzer und die Benutzer AWS-Konten , die einen AWS Dienst aufgerufen haben, die Quell-IP-Adresse, über die die Aufrufe generiert wurden, und den Zeitpunkt der Anrufe identifizieren. Einzelheiten zu den erfassten Daten finden Sie in den AWS CloudTrail Datensatzinhalten.

Kontroll-ID	AWS Config	Empfehlungen
7.5.7	cloudtrail-s3-dataevents-enabled	Die Erfassung von Simple Storage Service (Amazon S3)-Datenereignissen unterstützt die Erkennung von ungewöhnlichen Aktivitäten. Zu den Details gehören AWS-Konto Informationen über den Zugriff auf einen Amazon S3 S3-Bucket, die IP-Adresse und die Uhrzeit des Ereignisses.
7.5.7	elasticsearch-logs-to-cloudwatch	Stellen Sie sicher, dass für Amazon OpenSearch Service-Domains Fehlerprotokolle aktiviert und zur Aufbewahrung und Beantwortung an Amazon CloudWatch Logs gestreamt werden. Domain-Fehlerprotokolle sind bei Sicherheits- und Zugriffsprüfungen sowie bei der Diagnose von Verfügbarkeitsproblemen nützlich.

Kontroll-ID	AWS Config	Empfehlungen
7.5.7	opensearch-logs-to-cloudwatch	Stellen Sie sicher, dass für Amazon OpenSearch Service-Domains Fehlerprotokolle aktiviert und zur Aufbewahrung und Beantwortung an Amazon CloudWatch Logs gestreamt werden. OpenSearch Service-Fehlerprotokolle können bei Sicherheits- und Zugriffsprüfungen helfen und bei der Diagnose von Verfügbarkeitsproblemen helfen.
7.5.7	rds-logging-enabled	Um die Protokollierung und Überwachung in Ihrer Umgebung zu erleichtern, stellen Sie sicher, dass die Amazon Relational Database Service (Amazon RDS)-Protokollierung aktiviert ist. Mit der Amazon-RDS-Protokollierung können Sie Ereignisse wie Verbindungen, Verbindungsabbrüche, Abfragen oder abgefragte Tabellen erfassen.

Kontroll-ID	AWS Config	Empfehlungen
7.5.7	elb-logging-enabled	Die Elastic-Load-Balancing-Aktivität ist ein zentraler Kommunikationspunkt innerhalb einer Umgebung. Stellen Sie sicher, dass die ELB-Protokollierung aktiviert ist. Die gesammelten Daten enthalten detaillierte Informati onen zu Anfragen, die an den ELB gesendet wurden. Jedes Protokoll enthält Informati onen wie die Zeit, zu der die Anforderung einging, die Client-IP-Adresse, Latenzen, Anforderungspfade und Serverantworten.

Kontroll-ID	AWS Config	Empfehlungen
7.5.7	redshift-cluster-configuration-check	Um Daten im Ruhezustand zu schützen, muss die Verschlüsselung für Ihre Amazon-Redshift-Cluster aktiviert sein. Sie müssen auch sicherstellen, dass die erforderlichen Konfigurationen auf Amazon-Redshift-Clustern bereitgestellt werden. Die Prüfungsprotokollierung muss aktiviert sein, um Informationen zu Verbindungen und Benutzeraktivitäten in der Datenbank bereitzustellen. Diese Regel erfordert, dass ein Wert für clusterDbEncrypted (Config Default: TRUE) und LoggingEnabled (Config Default: TRUE) gesetzt ist. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	AWS Config	Empfehlungen
7.5.7	s-3 bucket-logging-enabled	Die Amazon Simple Storage Service (Amazon S3)-Serverzugriffsprotokollierung bietet eine Methode zur Überwachung des Netzwerks im Hinblick auf potenzielle Cybersicherheitsereignisse. Die Ereignisse werden überwacht, indem detaillierte Aufzeichnungen über die Anfragen erfasst werden, die an einen Amazon-S3-Bucket gestellt wurden. Jeder Zugriffsprotokolleintrag enthält Details zu einer einzelnen Zugriffsanfrage. Zu den Details gehören Anforderer, Bucket-Name, Anforderungszeit, Anforderungsaktion, Antwortstatus und Fehlercode, falls relevant.

Kontroll-ID	AWS Config	Empfehlungen
7.5.7	vpc-flow-logs-enabled	VPC-Flow-Protokolle erfassen detaillierte Informationsdatensätze über den IP-Datenverkehr, der zu und von Netzwerkschnittstellen in Ihrer Amazon Virtual Private Cloud (Amazon VPC) fließt. Standardmäßig enthalten Flow-Protokolldatensätze Werte für die verschiedenen Komponenten des IP-Flows, einschließlich Quelle, Ziel und Protokoll.
7.5.7	wafv2-logging-enabled	Um die Protokollierung und Überwachung in Ihrer Umgebung zu erleichtern, aktivieren Sie die AWS WAF (V2) -Protokollierung im regionalen und globalen Web. ACLs AWS Die WAF-Protokollierung bietet detaillierte Informationen über den Datenverkehr, der von Ihrer Web-ACL analysiert wird. In den Protokollen werden die Uhrzeit aufgezeichnet, zu der die AWS WAF die Anfrage von Ihrer AWS Ressource erhalten hat, Informationen zu der Anfrage und eine Aktion für die Regel, der jede Anfrage entsprach.

Kontroll-ID	AWS Config	Empfehlungen
8.1.1	s-3 bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) unterstützt die Aufrechte rhaltung einer angemessenen Kapazität und Verfügbarkeit. CRR ermöglicht das automatis che, asynchrone Kopieren von Objekten in Amazon-S3 -Buckets, um die Datenverf ügbarkeit sicherzustellen.
8.1.1	autoscaling-group-elb-healt hcheck-erforderlich	Die Elastic Load Balancer (ELB) -Zustandsprüfungen für Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling Scaling-Gruppen unterstützen die Aufrechte rhaltung einer angemessenen Kapazität und Verfügbarkeit. Der Load Balancer sendet regelmäßig Pings, versucht Verbindungen herzustellen oder sendet Anfragen, um den Zustand der EC2 Amazon-In stances in einer Gruppe mit auto-scaling zu testen. Wenn eine Instance nicht zurückmel det, wird der Traffic an eine neue EC2 Amazon-Instance gesendet.

Kontroll-ID	AWS Config	Empfehlungen
8.1.1	dynamodb-autoscaling-enabled	Amazon DynamoDB Auto Scaling verwendet den AWS Application Auto Scaling-Service, um die bereitgestellte Durchsatzkapazität so anzupassen, dass sie automatisch auf tatsächliche Verkehrsmuster reagiert. Auf diese Weise kann eine Tabelle oder ein globaler sekundärer Index die bereitgestellte Lese-/Schreibkapazität erhöhen, um plötzliche Erhöhungen des Datenverkehrs ohne Drosselung zu bewältigen.
8.1.1	elb-cross-zone-load-Balancing aktiviert	Aktivieren Sie zonenübergreifendes Load Balancing für Ihre Elastic Load Balancer (ELBs), um eine angemessene Kapazität und Verfügbarkeit aufrechtzuerhalten. Zonenübergreifendes Load Balancing reduziert die Notwendigkeit, die gleiche Anzahl von Instances in jeder aktivierten Availability Zone aufrechtzuerhalten. Es verbessert auch die Fähigkeit Ihrer Anwendung, den Verlust einer oder mehrerer Instances zu bewältigen.

Kontroll-ID	AWS Config	Empfehlungen
8.1.1	elb-deletion-protection-enabled	Diese Regel sorgt dafür, dass der Löschschutz für Elastic Load Balancing aktiviert ist. Verwenden Sie diese Funktion, um zu verhindern, dass Ihr Load Balancer versehentlich oder böswillig gelöscht wird, was zum Verlust der Verfügbarkeit Ihrer Anwendungen führen kann.
8.1.1	rds-instance-deletion-protection-aktiviert	Stellen Sie sicher, dass Amazon Relational Database Service (Amazon RDS)-Instances den Löschschutz aktiviert haben. Verwenden Sie den Löschschutz, um zu verhindern, dass Ihre Amazon-RDS-Instances versehentlich oder böswillig gelöscht werden, was zum Verlust der Verfügbarkeit Ihrer Anwendungen führen kann.

Kontroll-ID	AWS Config	Empfehlungen
8.1.1	rds-multi-az-support	Die Multi-AZ-Unterstützung in Amazon Relational Database Service (Amazon RDS) bietet eine verbesserte Verfügbar keit und Beständigkeit von Datenbank-Instances. Wenn Sie eine Multi-AZ-Datenbank-Instance bereitstellen, erstellt Amazon RDS automatisch eine primäre Datenbank-Instance und repliziert die Daten synchron auf eine Standby-Instance in einer anderen Availability Zone. Jede Availability Zone läuft auf einer eigenen, physisch getrennten, unabhängigen Infrastruktur und ist auf eine hohe Verfügbarkeit ausgelegt . Im Falle eines Infrastru kturausfalls führt Amazon RDS einen automatischen Failover zum Standby-Modus durch, sodass Sie den Datenbank betrieb wieder aufnehmen können, sobald der Failover abgeschlossen ist.

Kontroll-ID	AWS Config	Empfehlungen
8.1.1	vpc-vpn-2-tunnels-up	Redundante Site-to-Site VPN-Tunnel können implement iert werden, um die Anforderu ngen an die Ausfallsicherheit zu erfüllen. Es verwendet zwei Tunnel, um die Konnektiv ität sicherzustellen, falls eine der Site-to-Site VPN-Verbi ndungen nicht verfügbar ist. Um sich vor einem Verbindun gsverlust zu schützen, können Sie für den Fall, dass Ihr Kunden-Gateway nicht verfügbar ist, eine zweite Site-to-Site VPN-Verbindung zu Ihrer Amazon Virtual Private Cloud (Amazon VPC) und Ihrem Virtual Private Gateway einrichten, indem Sie ein zweites Kunden-Gateway verwenden.

Kontroll-ID	AWS Config	Empfehlungen
8.1.2	dynamodb-autoscaling-enabled	Amazon DynamoDB Auto Scaling verwendet den AWS Application Auto Scaling-Service, um die bereitgestellte Durchsatzkapazität so anzupassen, dass sie automatisch auf tatsächliche Verkehrsmuster reagiert. Auf diese Weise kann eine Tabelle oder ein globaler sekundärer Index die bereitgestellte Lese-/Schreibkapazität erhöhen, um plötzliche Erhöhungen des Datenverkehrs ohne Drosselung zu bewältigen.

Kontroll-ID	AWS Config	Empfehlungen
8.1.2	rds-multi-az-support	Die Multi-AZ-Unterstützung in Amazon Relational Database Service (Amazon RDS) bietet eine verbesserte Verfügbar keit und Beständigkeit von Datenbank-Instances. Wenn Sie eine Multi-AZ-Datenbank-Instance bereitstellen, erstellt Amazon RDS automatisch eine primäre Datenbank-Instance und repliziert die Daten synchron auf eine Standby-Instance in einer anderen Availability Zone. Jede Availability Zone läuft auf einer eigenen, physisch getrennten, unabhängigen Infrastruktur und ist auf eine hohe Verfügbarkeit ausgelegt . Im Falle eines Infrastru kturausfalls führt Amazon RDS einen automatischen Failover zum Standby-Modus durch, sodass Sie den Datenbank betrieb wieder aufnehmen können, sobald der Failover abgeschlossen ist.

Kontroll-ID	AWS Config	Empfehlungen
8.1.2	s-3 bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) unterstützt die Aufrechte rhaltung einer angemessenen Kapazität und Verfügbarkeit. CRR ermöglicht das automatis che, asynchrone Kopieren von Objekten in Amazon-S3 -Buckets, um die Datenverf ügbarkeit sicherzustellen.
8.1.2	opensearch-data-node-fault-Toleranz	Amazon OpenSearch Service (OpenSearch Service) benötigt mindestens drei Datenknoten für hohe Verfügbarkeit und Fehlertol eranz. Die Bereitstellung einer OpenSearch Service-Domain mit mindestens drei Datenknot en gewährleistet den Cluster-B etrieb, falls ein Knoten ausfällt.

Kontroll-ID	AWS Config	Empfehlungen
8.1.2	elb-cross-zone-load-Balancing aktiviert	Aktivieren Sie zonenüber greifendes Load Balancing für Ihre Elastic Load Balancer (ELBs), um eine angemesse ne Kapazität und Verfügbar keit aufrechtzuerhalten. Zonenübergreifendes Load Balancing reduziert die Notwendigkeit, die gleiche Anzahl von Instances in jeder aktivierten Availability Zone aufrechtzuerhalten. Es verbessert auch die Fähigkeit Ihrer Anwendung, den Verlust einer oder mehrerer Instances zu bewältigen.

Kontroll-ID	AWS Config	Empfehlungen
8.1.3	autoscaling-group-elb-healthcheck-erforderlich	Die Elastic Load Balancer (ELB) -Zustandsprüfungen für Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling Scaling-Gruppen unterstützen die Aufrechterhaltung einer angemessenen Kapazität und Verfügbarkeit. Der Load Balancer sendet regelmäßig Pings, versucht Verbindungen herzustellen oder sendet Anfragen, um den Zustand der EC2 Amazon-Instances in einer Gruppe mit auto-scaling zu testen. Wenn eine Instance nicht zurückmeldet, wird der Traffic an eine neue EC2 Amazon-Instance gesendet.

Kontroll-ID	AWS Config	Empfehlungen
8.1.3	beanstalk-enhanced-health-reporting-aktiviert	AWS Die verbesserte Zustandsberichterstattung von Elastic Beanstalk ermöglicht eine schnellere Reaktion auf Veränderungen im Zustand der zugrunde liegenden Infrastruktur. Diese Änderungen könnten zu einer mangelnden Verfügbarkeit der Anwendung führen. Die erweiterten Zustandsberichte von Elastic Beanstalk bieten eine Statusbeschreibung, um den Schweregrad der identifizierten Probleme einzuschätzen und mögliche Ursachen zu identifizieren, die untersucht werden müssen.
8.1.3	cloud-trail-cloud-watch-logs-aktiviert	Verwenden Sie Amazon CloudWatch , um Protokollereignisaktivitäten zentral zu sammeln und zu verwalten . Die Aufnahme von AWS CloudTrail Daten liefert Einzelheiten zu den API-Aufrufaktivitäten in Ihrem AWS-Konto.

Kontroll-ID	AWS Config	Empfehlungen
8.1.3	cloudtrail-enabled	AWS CloudTrail kann bei der Nichtabstreitbarkeit helfen, indem Aktionen und API-Aufrufe der AWS Managemen t Console aufgezeichnet werden. Sie können die Benutzer und die Benutzer AWS-Konten , die einen AWS Dienst aufgerufen haben, die Quell-IP-Adresse, über die die Aufrufe generiert wurden, und den Zeitpunkt der Anrufe identifizieren. Einzelheiten zu den erfassten Daten finden Sie in den AWS CloudTrail Datensatzinhalten.
8.4.1	db-instance-backup-enabled	Die Sicherungsfunktion von Amazon RDS erstellt Sicherungen Ihrer Datenbank en und Transaktionsprotokolle. Amazon RDS erstellt einen Snapshot für das Speicherv olume Ihrer DB-Instance, sodass die gesamte DB-Instance gesichert wird. Sie können im System spezifisc he Aufbewahrungsfristen festlegen, um Ihre Ausfallsi cherheitsanforderungen zu erfüllen.

Kontroll-ID	AWS Config	Empfehlungen
8.4.1	dynamodb-in-backup-plan	Um Sie bei Datensich erungsprozessen zu unterstüt zen, stellen Sie sicher, dass Ihre Amazon DynamoDB-Tabellen Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherung smanagement und erleichte rt Ihnen die Erfüllung von geschäftlichen und behördlic hen Compliance-Anforde rungen hinsichtlich Datensich erungen.
8.4.1	dynamodb-pitr-enabled	Aktivieren Sie diese Regel, um zu überprüfen, ob die Informationen gesichert wurden. Es verwaltet auch die Backups, indem es sicherste llt, dass die point-in-time Wiederherstellung in Amazon DynamoDB aktiviert ist. Bei der Wiederherstellung werden fortlaufende Backups Ihrer Tabelle für die letzten 35 Tage gespeichert.

Kontroll-ID	AWS Config	Empfehlungen
8.4.1	ebs-in-backup-plan	Stellen Sie zur Unterstützung der Datensicherungsprozesse sicher, dass Ihre Amazon Elastic Block Store (Amazon EBS) -Volumes Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherung smanagement und erleichte rt Ihnen die Erfüllung von geschäftlichen und behördlic hen Compliance-Anforde rungen hinsichtlich Datensich erungen.
8.4.1	ebs-optimized-instance	Eine optimierte Instance im Amazon Elastic Block Store (Amazon EBS) bietet zusätzlic he, dedizierte Kapazität für Amazon-EBS-I/O-Vorgänge. Diese Optimierung bietet die beste Leistung für Ihr EBS-Volume, indem Konflikte zwischen Amazon-EBS-I/O und anderem Datenverkehr von Ihrer Instance minimiert werden.

Kontroll-ID	AWS Config	Empfehlungen
8.4.1	efs-in-backup-plan	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon Elastic File System (Amazon EFS) - Dateisysteme Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	AWS Config	Empfehlungen
8.4.1	rds-in-backup-plan	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon Relational Database Service (Amazon RDS) -Instances Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	AWS Config	Empfehlungen
8.4.1	redshift-backup-enabled	Stellen Sie zur Unterstützung der Datensicherungsprozesse sicher, dass Ihre Amazon-Redshift-Cluster über automatisierte Snapshots verfügen. Wenn automatisierte Snapshots für einen Cluster aktiviert sind, erstellt Redshift in regelmäßigen Abständen Snapshots dieses Clusters. Standardmäßig erstellt Redshift alle acht Stunden oder alle 5 GB einen Snapshot für jeden Knoten mit Datenänderungen oder je nachdem, was zuerst eintritt.
8.4.1	elasticache-redis-cluster-automatic-Backup-Check	Wenn automatische Backups aktiviert sind, ElastiCache erstellt Amazon täglich ein Backup des Clusters. Die Sicherung kann für eine von Ihrer Organisation festgelegte Anzahl von Tagen aufbewahrt werden. Automatische Backups schützen vor Datenverlust. Bei einem Ausfall können Sie einen neuen Cluster erstellen, der Ihre Daten aus dem aktuellen Backup wiederherstellt.

Kontroll-ID	AWS Config	Empfehlungen
8.4.1	s-3 bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) unterstützt die Aufrechte rhaltung einer angemessenen Kapazität und Verfügbarkeit. CRR ermöglicht das automatis che, asynchrone Kopieren von Objekten in Amazon-S3 -Buckets, um die Datenverf ügbarkeit sicherzustellen.
8.4.1	s-3 bucket-versioning-enabled	Die Versionsverwaltung von Amazon Simple Storage Service (Amazon S3)-Buckets hilft dabei, mehrere Varianten eines Objekts im selben Amazon-S3-Bucket zu speichern. Verwenden Sie die Versionsverwaltung, um sämtliche Versionen aller Objekte in Ihrem Amazon-S3-Bucket zu speichern, abzurufen oder wiederher zustellen. Mit der Versionsv erwaltung können Sie Versionen sowohl nach unbeabsichtigten Benutzera ktionen als auch nach Anwendungsfehlern problemlo s wiederherstellen.

Kontroll-ID	AWS Config	Empfehlungen
8.4.2	db-instance-backup-enabled	Die Sicherungsfunktion von Amazon RDS erstellt Sicherungen Ihrer Datenbank en und Transaktionsprotokolle. Amazon RDS erstellt einen Snapshot für das Speicherv olume Ihrer DB-Instance, sodass die gesamte DB-Instance gesichert wird. Sie können im System spezifisc he Aufbewahrungsfristen festlegen, um Ihre Ausfallsi cherheitsanforderungen zu erfüllen.
8.4.2	dynamodb-in-backup-plan	Um Sie bei Datensich erungsprozessen zu unterstüt zen, stellen Sie sicher, dass Ihre Amazon DynamoDB-Tabellen Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherung smanagement und erleichte rt Ihnen die Erfüllung von geschäftlichen und behördlic hen Compliance-Anforde rungen hinsichtlich Datensich erungen.

Kontroll-ID	AWS Config	Empfehlungen
8.4.2	dynamodb-pitr-enabled	Aktivieren Sie diese Regel, um zu überprüfen, ob die Informationen gesichert wurden. Es verwaltet auch die Backups, indem es sicherste llt, dass die point-in-time Wiederherstellung in Amazon DynamoDB aktiviert ist. Bei der Wiederherstellung werden fortlaufende Backups Ihrer Tabelle für die letzten 35 Tage gespeichert.
8.4.2	ebs-in-backup-plan	Stellen Sie zur Unterstützung der Datensicherungsprozesse sicher, dass Ihre Amazon Elastic Block Store (Amazon EBS) -Volumes Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherung smanagement und erleichte rt Ihnen die Erfüllung von geschäftlichen und behördlic hen Compliance-Anforde rungen hinsichtlich Datensich erungen.

Kontroll-ID	AWS Config	Empfehlungen
8.4.2	ebs-optimized-instance	Eine optimierte Instance im Amazon Elastic Block Store (Amazon EBS) bietet zusätzliche, dedizierte Kapazität für Amazon-EBS-I/O-Vorgänge. Diese Optimierung bietet die beste Leistung für Ihr EBS-Volume, indem Konflikte zwischen Amazon-EBS-I/O und anderem Datenverkehr von Ihrer Instance minimiert werden.
8.4.2	efs-in-backup-plan	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon Elastic File System (Amazon EFS) - Dateisysteme Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	AWS Config	Empfehlungen
8.4.2	elasticache-redis-cluster-automatic-Backup-Check	Wenn automatische Backups aktiviert sind, ElastiCache erstellt Amazon täglich ein Backup des Clusters. Die Sicherung kann für eine von Ihrer Organisation festgelegte Anzahl von Tagen aufbewahrt werden. Automatische Backups schützen vor Datenverlust. Bei einem Ausfall können Sie einen neuen Cluster erstellen, der Ihre Daten aus dem aktuellen Backup wiederherstellt.
8.4.2	rds-in-backup-plan	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon Relational Database Service (Amazon RDS) -Instances Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	AWS Config	Empfehlungen
8.4.2	redshift-backup-enabled	Stellen Sie zur Unterstützung der Datensicherungsprozesse sicher, dass Ihre Amazon-Redshift-Cluster über automatisierte Snapshots verfügen. Wenn automatisierte Snapshots für einen Cluster aktiviert sind, erstellt Redshift in regelmäßigen Abständen Snapshots dieses Clusters. Standardmäßig erstellt Redshift alle acht Stunden oder alle 5 GB einen Snapshot für jeden Knoten mit Datenänderungen oder je nachdem, was zuerst eintritt.
8.4.2	s-3 bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) unterstützt die Aufrechterhaltung einer angemessenen Kapazität und Verfügbarkeit. CRR ermöglicht das automatische, asynchrone Kopieren von Objekten in Amazon-S3-Buckets, um die Datenverfügbarkeit sicherzustellen.

Kontroll-ID	AWS Config	Empfehlungen
8.4.2	s-3 bucket-versioning-enabled	Die Versionsverwaltung von Amazon Simple Storage Service (Amazon S3)-Buckets hilft dabei, mehrere Varianten eines Objekts im selben Amazon-S3-Bucket zu speichern. Verwenden Sie die Versionsverwaltung, um sämtliche Versionen aller Objekte in Ihrem Amazon-S3-Bucket zu speichern, abzurufen oder wiederher zustellen. Mit der Versionsv erwaltung können Sie Versionen sowohl nach unbeabsichtigten Benutzera ktionen als auch nach Anwendungsfehlern problemlo s wiederherstellen.
8.4.4	rds-snapshot-encrypted	Stellen Sie sicher, dass die Verschlüsselung für Ihre Amazon Relational Database Service (Amazon RDS)-Snap shots aktiviert ist. Da sensible Daten auch im Ruhezusta nd vorhanden sein können, sollten Sie die Verschlüs selung im Ruhezustand aktivieren, um diese Daten zu schützen.

Kontroll-ID	AWS Config	Empfehlungen
8.5.4	rds-multi-az-support	Die Multi-AZ-Unterstützung in Amazon Relational Database Service (Amazon RDS) bietet eine verbesserte Verfügbar keit und Beständigkeit von Datenbank-Instances. Wenn Sie eine Multi-AZ-Datenbank-Instance bereitstellen, erstellt Amazon RDS automatisch eine primäre Datenbank-Instance und repliziert die Daten synchron auf eine Standby-Instance in einer anderen Availability Zone. Jede Availability Zone läuft auf einer eigenen, physisch getrennten, unabhängigen Infrastruktur und ist auf eine hohe Verfügbarkeit ausgelegt . Im Falle eines Infrastru kturausfalls führt Amazon RDS einen automatischen Failover zum Standby-Modus durch, sodass Sie den Datenbank betrieb wieder aufnehmen können, sobald der Failover abgeschlossen ist.

Kontroll-ID	AWS Config	Empfehlungen
8.5.4	s-3 bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) unterstützt die Aufrechte rhaltung einer angemessenen Kapazität und Verfügbarkeit. CRR ermöglicht das automatis che, asynchrone Kopieren von Objekten in Amazon-S3 -Buckets, um die Datenverf ügbarkeit sicherzustellen.
9.1.1	ec-2 instance-profile-attached	EC2 Instanzprofile übergeben eine IAM-Rolle an eine EC2 Instance. Das Anhängen eines Instance-Profils an Ihre Instances kann bei der Implementierung von geringsten Berechtigungen und der Berechtigungsverwa ltung helfen.

Kontroll-ID	AWS Config	Empfehlungen
9.1.1	ecs-task-definition-user-for-host-mode-check	Wenn für eine Aufgabend efinition erhöhte Berechtig ungen gelten, liegt das daran, dass der Kunde diesen Konfigurationen ausdrücklich zugestimmt hat. Diese Kontrolle prüft, ob eine unerwartete Berechtig ungseskalation vorliegt, wenn für eine Aufgabendefinition das Host-Netzwerk aktiviert ist, die Kunden aber keine erhöhten Berechtigungen aktiviert haben.

Kontroll-ID	AWS Config	Empfehlungen
9.1.1	emr-kerberos-enabled	Die Zugriffsberechtigungen und -autorisierungen können verwaltet und nach den Prinzipien der geringsten Berechtigung und Aufgabent rennung integriert werden, indem Kerberos für Amazon-EMR-Cluster aktiviert wird. In Kerberos werden Services und Benutzer, die sich authentifizieren müssen, als Prinzipale bezeichnet. Prinzipale befinden sich in einem Kerberos-Bereich. Innerhalb dieses Bereichs wird ein Kerberos-Server als Key Distribution Center (KDC) bezeichnet. Über diesen Server können sich Prinzipale authentifizieren. Die Authentifizierung im KDC erfolgt durch die Ausstellu ng von Authentifizierungs tickets. Das KDC unterhält eine Datenbank der Prinzipal e in seinem Bereich mit ihren Passwörtern und anderen administrativen Informationen zu jedem Prinzipal.

Kontroll-ID	AWS Config	Empfehlungen
9.1.1	iam-customer-policy-blocked-kms-Aktionen	AWS Identity and Access Management (IAM) kann Ihnen helfen, die Prinzipien der geringsten Rechte und der Aufgabentrennung in Zugriffsberechtigungen und Autorisierungen zu integrier en und so zu verhindern, dass Richtlinien blockierte Aktionen für alle AWS Schlüssel des Key Management Service enthalten. Wenn Benutzer mehr Rechte haben, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und Aufgabentrennung verstoßen . Mit dieser Regel können Sie den Parameter festlegen. blockedActionsPatterns (Wert „AWS Bewährte grundlegende Sicherheitsmethoden“: kms: Entschlüsseln, kms:ReEnc ryptFrom). Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprech en.

Kontroll-ID	AWS Config	Empfehlungen
9.1.1	iam-group-has-users-überprüfen	AWS Identity and Access Management (IAM) kann Ihnen helfen, die Prinzipien der geringsten Rechte und der Aufgabentrennung mit Zugriffsberechtigungen und Autorisierungen zu integrieren, indem sichergestellt wird, dass IAM-Gruppen mindestens einen Benutzer haben. Die Einteilung von Benutzern in Gruppen auf der Grundlage der ihnen zugewiesenen Berechtigungen oder ihrer Funktion ist eine Möglichkeit, das Prinzip der geringsten Berechtigung zu implementieren.

Kontroll-ID	AWS Config	Empfehlungen
9.1.1	iam-inline-policy-blocked-kms-Aktionen	Stellen Sie sicher, dass ein Benutzer, eine IAM-Rolle oder eine IAM-Grupp e (AWS Identity and Access Management) nicht über eine Inline-Richtlinie verfügt, die blockierte Aktionen für alle AWS Schlüssel des Key Management Service zulässt. AWS empfiehlt, verwaltete Richtlinien anstelle von Inline-Richtlinien zu verwenden . Verwaltete Richtlinien ermöglichen Wiederver wendbarkeit, Versionsv erwaltung, Rollback und Delegierung der Berechtig ungsverwaltung. Mit dieser Regel können Sie den blockedActionsPatterns Parameter festlegen. (Wert „AWS Bewährte grundlegende Sicherheitsmethoden“: kms: Entschlüsseln, kms:ReEnc ryptFrom). Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprech en.

Kontroll-ID	AWS Config	Empfehlungen
9.1.1	iam-no-inline-policy-überprüfen	Stellen Sie sicher, dass ein Benutzer, eine IAM-Rolle oder eine IAM-Gruppe (AWS Identity and Access Management) nicht über eine Inline-Richtlinie zur Zugriffskontrolle auf Systeme und Ressourcen verfügt. AWS empfiehlt, verwaltete Richtlinien anstelle von Inline-Richtlinien zu verwenden . Verwaltete Richtlinien ermöglichen Wiederverwendbarkeit, Versionsverwaltung, Rollback und Delegierung der Berechtigungsverwaltung.

Kontroll-ID	AWS Config	Empfehlungen
9.1.1	iam-password-policy	Die Identitäten und Anmeldein formationen werden auf der Grundlage einer organisat orischen IAM-Passwortrichtl inie ausgestellt, verwaltet und verifiziert. Sie erfüllen oder übertreffen die Anforderungen von NIST SP 800-63 und dem Standard „Best Practices“ von AWS Foundational Security für die Passwortstärke. Mit dieser Regel können Sie optional RequireUppercaseCharacters (Wert für AWS grundlege nde Sicherheitsbewährte Verfahren: wahr), RequireLo wercaseCharacters (Wert für bewährte Methoden für AWS grundlegende Sicherheit: wahr), RequireSymbols (Wert für bewährte Methoden für AWS grundlegende Sicherhei t: wahr), RequireNumbers (Wert für bewährte Methoden für AWS grundlegende Sicherheit: wahr), MinimumPa sswordLength (Wert für bewährte Methoden für AWS grundlegende Sicherheit: 14), PasswordReusePreve ntion (Wert für bewährte Methoden für AWS grundlege nde Sicherheit: 24) und MaxPasswordAge (Wert

Kontroll-ID	AWS Config	Empfehlungen
		für bewährte Methoden für AWS grundlegende Sicherhei t: 90) für Ihr IAM festlegen Kennwortrichtlinie. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisat ion entsprechen.
9.1.1	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) kann Ihnen dabei helfen, die Prinzipien der geringsten Rechte und der Aufgabent rennung in Zugriffsberechtigu ngen und Autorisierungen zu integrieren und so zu verhindern, dass Richtlinien „Effect“: „Allow“ mit „Action“: „*“ anstelle von „Resource“: „*“ enthalten. Wenn Benutzern mehr Rechte eingeräumt werden, als für die Ausführun g einer Aufgabe erforderl ich sind, kann dies gegen das Prinzip der geringste n Berechtigung und der Aufgabentrennung verstoßen.

Kontroll-ID	AWS Config	Empfehlungen
9.1.1	iam-policy-no-statements-with-full-access	Stellen Sie sicher, dass IAM-Aktionen nur auf die benötigte n Aktionen beschränkt sind. Wenn Benutzern mehr Rechte eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und der Aufgabentrennung verstoßen.
9.1.1	iam-root-access-key-überprüfen	Der Zugriff auf Systeme und Ressourcen kann gesteuert werden, indem überprüft wird, ob der Root-Benutzer keine Zugriffsschlüssel mit seiner AWS Identity and Access Management (IAM) -Rolle verknüpft hat. Stellen Sie sicher, dass die Root-Zugr iffsschlüssel gelöscht werden. Erstellen und verwenden Sie stattdessen rollenbasierte Funktionen, AWS-Konten um das Prinzip der geringsten Funktionalität zu berücksic htigen.

Kontroll-ID	AWS Config	Empfehlungen
9.1.1	iam-user-group-membership-überprüfen	AWS Identity and Access Management (IAM) kann Ihnen helfen, Zugriffsberechtigungen und Autorisierungen einzuschränken, indem sichergestellt wird, dass Benutzer Mitglieder mindestens einer Gruppe sind. Wenn Benutzern mehr Berechtigungen eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und Aufgabentrennung verstoßen.
9.1.1	iam-user-mfa-enabled	Aktivieren Sie diese Regel, um den Zugriff auf Ressourcen in der AWS Cloud einzuschränken. Diese Regel sorgt dafür, dass die Multi-Faktor-Authentifizierung (MFA) für alle Benutzer aktiviert ist. MFA sorgt für eine weitere Schutzebene zusätzlich zu den Anmeldeinformationen. Reduzieren Sie Fälle von kompromittierten Konten, indem Sie MFA für Benutzer vorschreiben.

Kontroll-ID	AWS Config	Empfehlungen
9.1.1	iam-user-no-policies-überprüfen	Diese Regel stellt sicher, dass AWS Identity and Access Management (IAM) -Richtlinien nur Gruppen oder Rollen zugewiesen werden, um den Zugriff auf Systeme und Ressourcen zu kontrollieren. Die Zuweisung von Berechtigungen auf Gruppen- oder Rollenebene trägt dazu bei, die Wahrscheinlichkeit zu verringern, dass eine Identität übermäßige Berechtigungen erhält oder beibehält.

Kontroll-ID	AWS Config	Empfehlungen
9.1.1	iam-user-unused-credentials-überprüfen	AWS Identity and Access Management (IAM) kann Ihnen bei Zugriffsberechtigungen und Autorisierungen helfen, indem es nach IAM-Passwörtern und Zugriffsschlüsseln sucht, die für einen bestimmten Zeitraum nicht verwendet wurden. Wenn ungenutzte Anmeldeinformationen identifiziert werden, müssen Sie sie deaktivieren und/oder entfernen, da dies gegen das Prinzip der geringsten Berechtigung verstoßen könnte. Für diese Regel müssen Sie einen Wert für das maxCredentialUsage Alter festlegen (Standardkonfiguration: 90). Der tatsächliche Wert muss den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	AWS Config	Empfehlungen
9.1.1	mfa-enabled-for-iam-Konsolenzugriff	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass MFA für alle AWS Identity and Access Management (IAM) -Benutzer aktiviert ist, die über ein Konsolenkennwort verfügen. MFA sorgt für eine weitere Schutzebene zusätzlich zu den Anmeldeinformationen. Indem Sie MFA für Benutzer vorschreiben, können Sie Fälle kompromittierter Konten reduzieren und verhindern, dass unbefugte Benutzer auf vertrauliche Daten zugreifen.
9.1.1	root-account-hardware-mfa-aktiviert	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Hardware-MFA für den Root-Benutzer aktiviert ist. Der Stammbenutzer ist der AWS-Konto-Benutzer mit den meisten Berechtigungen. MFA sorgt für eine weitere Schutzebene zusätzlich zu den Anmeldeinformationen. Indem Sie MFA für den Root-Benutzer vorschreiben, können Sie die Anzahl AWS-Konten kompromittierter Benutzer reduzieren.

Kontroll-ID	AWS Config	Empfehlungen
9.1.1	root-account-mfa-enabled	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass MFA für den Root-Benutzer aktiviert ist. Der Stammbenutzer ist der AWS-Konto-Benutzer mit den meisten Berechtigungen. MFA sorgt für eine weitere Schutzebene zusätzlich zu den Anmeldeinformationen. Indem Sie MFA für den Root-Benutzer vorschreiben, können Sie die Anzahl AWS-Konten kompromittierter Benutzer reduzieren.
9.1.1	secretsmanager-rotation-enabled-check	Diese Regel stellt sicher, dass bei AWS Secrets Manager Manager-Geheimnissen die Rotation aktiviert ist. Die regelmäßige Rotation von Secrets kann den Zeitraum verkürzen, in dem ein Secret aktiv ist, und möglicherweise die Auswirkungen auf das Unternehmen verringern, falls das Secret kompromittiert wird.

Kontroll-ID	AWS Config	Empfehlungen
9.1.1	secretsmanager-scheduled-rotation-success-überprüfen	Diese Regel stellt sicher, dass AWS Secrets Manager Manager-Geheimnisse gemäß dem Rotationsplan erfolgreich rotiert wurden. Die regelmäßige Rotation von Secrets kann den Zeitraum verkürzen, in dem ein Secret aktiv ist, und möglicherweise die Auswirkungen auf das Unternehmen verringern, falls es kompromittiert wird.
9.1.1	s-3 bucket-policy-grantee-check	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie s3_bucket_policy_grantee_check aktivieren. Diese Regel prüft, ob der vom Amazon S3 S3-Bucket gewährte Zugriff durch die von Ihnen bereitgestellten AWS Principals, Verbundbenutzer, Service Principals, IP-Adressen oder Amazon Virtual Private Cloud (Amazon VPC) IDs eingeschränkt ist.

Kontroll-ID	AWS Config	Empfehlungen
9.1.1	secretsmanager-secret-periodic-rotation	Diese Regel stellt sicher, dass bei AWS Secrets Manager Manager-Geheimnissen die regelmäßige Rotation aktiviert ist. Die regelmäßige Rotation von Secrets kann den Zeitraum verkürzen, in dem ein Secret aktiv ist, und möglicherweise die Auswirkungen auf das Unternehmen verringern, falls das Secret kompromittiert wird. Der Standardwert lautet 90 Tage.
9.1.1	secretsmanager-secret-unused	Wenn in AWS Secrets Manager unbenutzte Anmeldeinformationen vorhanden sind, sollten Sie die Anmeldeinformationen deaktivieren und/oder entfernen, da dies gegen das Prinzip der geringsten Rechte verstoßen kann. Mit dieser Regel können Sie einen Wert auf unusedForDays (Config Default: 90) setzen. Der tatsächliche Wert muss den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	AWS Config	Empfehlungen
9.1.2	iam-customer-policy-blocked-kms-Aktionen	AWS Identity and Access Management (IAM) kann Ihnen helfen, die Prinzipien der geringsten Rechte und der Aufgabentrennung in Zugriffsberechtigungen und Autorisierungen zu integrier en und so zu verhindern, dass Richtlinien blockierte Aktionen für alle AWS Schlüssel des Key Management Service enthalten. Wenn Benutzer mehr Rechte haben, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und Aufgabentrennung verstoßen . Mit dieser Regel können Sie den Parameter festlegen. blockedActionsPatterns (Wert „AWS Bewährte grundlegende Sicherheitsmethoden“: kms: Entschlüsseln, kms:ReEnc ryptFrom). Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprech en.

Kontroll-ID	AWS Config	Empfehlungen
9.1.2	iam-group-has-users-überprüfen	AWS Identity and Access Management (IAM) kann Ihnen helfen, die Prinzipien der geringsten Rechte und der Aufgabentrennung mit Zugriffsberechtigungen und Autorisierungen zu integrieren, indem sichergestellt wird, dass IAM-Gruppen mindestens einen Benutzer haben. Die Einteilung von Benutzern in Gruppen auf der Grundlage der ihnen zugewiesenen Berechtigungen oder ihrer Funktion ist eine Möglichkeit, das Prinzip der geringsten Berechtigung zu implementieren.

Kontroll-ID	AWS Config	Empfehlungen
9.1.2	iam-inline-policy-blocked-kms-Aktionen	Stellen Sie sicher, dass ein Benutzer, eine IAM-Rolle oder eine IAM-Grupp e (AWS Identity and Access Management) nicht über eine Inline-Richtlinie verfügt, die blockierte Aktionen für alle AWS Schlüssel des Key Management Service zulässt. AWS empfiehlt, verwaltete Richtlinien anstelle von Inline-Richtlinien zu verwenden . Verwaltete Richtlinien ermöglichen Wiederver wendbarkeit, Versionsv erwaltung, Rollback und Delegierung der Berechtig ungsverwaltung. Mit dieser Regel können Sie den blockedActionsPatterns Parameter festlegen. (Wert „AWS Bewährte grundlegende Sicherheitsmethoden“: kms: Entschlüsseln, kms:ReEnc ryptFrom). Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprech en.

Kontroll-ID	AWS Config	Empfehlungen
9.1.2	iam-no-inline-policy-überprüfen	Stellen Sie sicher, dass ein Benutzer, eine IAM-Rolle oder eine IAM-Gruppe (AWS Identity and Access Management) nicht über eine Inline-Richtlinie zur Zugriffskontrolle auf Systeme und Ressourcen verfügt. AWS empfiehlt, verwaltete Richtlinien anstelle von Inline-Richtlinien zu verwenden . Verwaltete Richtlinien ermöglichen Wiederverwendbarkeit, Versionsverwaltung, Rollback und Delegierung der Berechtigungsverwaltung.

Kontroll-ID	AWS Config	Empfehlungen
9.1.2	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) kann Ihnen dabei helfen, die Prinzipien der geringsten Rechte und der Aufgabent rennung in Zugriffsberechtigu ngen und Autorisierungen zu integrieren und so zu verhindern, dass Richtlinien „Effect“: „Allow“ mit „Action“: „*“ anstelle von „Resource“: „*“ enthalten. Wenn Benutzern mehr Rechte eingeräumt werden, als für die Ausführun g einer Aufgabe erforderl ich sind, kann dies gegen das Prinzip der geringste n Berechtigung und der Aufgabentrennung verstoßen.
9.1.2	iam-policy-no-statements-with-full-access	Stellen Sie sicher, dass IAM-Aktionen nur auf die benötigte n Aktionen beschränkt sind. Wenn Benutzern mehr Rechte eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und der Aufgabentrennung verstoßen.

Kontroll-ID	AWS Config	Empfehlungen
9.1.3	api-gw-execution-logging-aktiviert	Die API-Gateway-Protokollierung zeigt detaillierte Ansichten der Benutzer, die auf die API zugegriffen haben, und wie diese Benutzer auf die API zugegriffen haben. Diese Einblicke ermöglichen die Transparenz von Benutzeraktivitäten.
9.1.3	cloud-trail-cloud-watch-logs-aktiviert	Verwenden Sie Amazon CloudWatch , um Protokollereignisaktivitäten zentral zu sammeln und zu verwalten . Die Aufnahme von AWS CloudTrail Daten liefert Einzelheiten zu den API-Aufrufaktivitäten in Ihrem AWS-Konto.

Kontroll-ID	AWS Config	Empfehlungen
9.1.3	cloudtrail-enabled	AWS CloudTrail kann durch die Aufzeichnung von Aktionen und API-Aufrufen in der AWS Management Console bei der Nichtabst reitbarkeit helfen. Sie können die Benutzer und die Benutzer AWS-Konten , die einen AWS Dienst aufgerufen haben, die Quell-IP-Adresse, über die die Aufrufe generiert wurden, und den Zeitpunkt der Anrufe identifizieren. Einzelheiten zu den erfassten Daten finden Sie in den AWS CloudTrail Datensatzinhalten.

Kontroll-ID	AWS Config	Empfehlungen
9.1.3	cloud-trail-log-file-Validierung aktiviert	Verwenden Sie die AWS CloudTrail Protokolldateivalidierung, um die Integrität von Protokollen zu überprüfen. CloudTrail Mithilfe der Protokolldateivalidierung kann festgestellt werden, ob eine Protokolldatei geändert oder gelöscht wurde oder ob sie nach der Übermittlung CloudTrail unverändert geblieben ist. Dieses Feature wurde mit dem Branchenstandard entsprechenden Algorithmen entwickelt: SHA-256 für die Hashfunktion und SHA-256 mit RSA für digitale Signaturen. Aus diesem Grund ist es rechnerisch unmöglich, CloudTrail Protokolldateien unbemerkt zu ändern, zu löschen oder zu fälschen.
9.1.3	cloudtrail-s3-dataevents-enabled	Die Erfassung von Simple Storage Service (Amazon S3)-Datenereignissen unterstützt die Erkennung von ungewöhnlichen Aktivitäten. Zu den Details gehören AWS-Konto Informationen über den Zugriff auf einen Amazon S3 S3-Bucket, die IP-Adresse und die Uhrzeit des Ereignisses.

Kontroll-ID	AWS Config	Empfehlungen
9.1.3	cloudtrail-security-trail-enabled	Diese Regel trägt dazu bei, die Verwendung der AWS empfohlenen bewährten Sicherheitsmethoden für sicherzustellen AWS CloudTrail, indem geprüft wird, ob mehrere Einstellungen aktiviert sind. Dazu gehören die Verwendung von Protokoll verschlüsselung, Protokoll validierung und Aktivierung AWS CloudTrail in mehreren Regionen.
9.1.3	cw-loggroup-retention-period-überprüfen	Stellen Sie sicher, dass die Ereignisprotokolldaten für Ihre Protokollgruppen über eine Mindestdauer aufbewahrt werden, um die Fehlerbehebung und forensische Untersuch ungen zu unterstützen. Fehlende frühere Ereignisp rotokolldaten erschweren die Rekonstruierung und Identifiz ierung potenziell schädlicher Ereignisse.

Kontroll-ID	AWS Config	Empfehlungen
9.1.3	elasticsearch-logs-to-cloudwatch	Stellen Sie sicher, dass für Amazon OpenSearch Service-Domains Fehlerprotokolle aktiviert und zur Aufbewahrung und Beantwortung an Amazon CloudWatch Logs gestreamt werden. Domain-Fehlerprotokolle sind bei Sicherheits- und Zugriffsprüfungen sowie bei der Diagnose von Verfügbarkeitsproblemen nützlich.
9.1.3	opensearch-logs-to-cloudwatch	Stellen Sie sicher, dass für Amazon OpenSearch Service-Domains Fehlerprotokolle aktiviert und zur Aufbewahrung und Beantwortung an Amazon CloudWatch Logs gestreamt werden. OpenSearch Service-Fehlerprotokolle können bei Sicherheits- und Zugriffsprüfungen helfen und bei der Diagnose von Verfügbarkeitsproblemen helfen.

Kontroll-ID	AWS Config	Empfehlungen
9.1.3	elb-logging-enabled	Die Elastic-Load-Balancing-Aktivität ist ein zentraler Kommunikationspunkt innerhalb einer Umgebung. Stellen Sie sicher, dass die ELB-Protokollierung aktiviert ist. Die gesammelten Daten enthalten detaillierte Informati onen zu Anfragen, die an den ELB gesendet wurden. Jedes Protokoll enthält Informati onen wie die Zeit, zu der die Anforderung einging, die Client-IP-Adresse, Latenzen, Anforderungspfade und Serverantworten.
9.1.3	guardduty-enabled-centralized	Amazon GuardDuty kann mithilfe von Threat Intellige nce Feeds helfen, potenzielle Cybersicherheitsereignisse zu überwachen und zu erkennen. Dazu gehören Listen mit bösartigen IPs und maschinel len Lernmethoden zur Identifiz ierung unerwarteter, nicht autorisierter und bösartige r Aktivitäten in Ihrer AWS Cloud-Umgebung.

Kontroll-ID	AWS Config	Empfehlungen
9.1.3	multi-region-cloudtrail-enabled	AWS CloudTrail zeichnet Aktionen und API-Aufrufe der AWS Management Console auf. Sie können feststellen, welche Benutzer und Konten angerufen wurden AWS, von welcher Quell-IP-Adresse aus die Anrufe getätigt wurden und wann die Anrufe erfolgten . CloudTrail übermittelt Protokolldateien aus allen AWS Regionen an Ihren S3-Bucket, wenn MULTI_REG ION_CLOUD_TRAIL_EN ABLED aktiviert ist. Außerdem wird beim AWS Start einer neuen Region derselbe Trail in der neuen Region erstellt. CloudTrail Dadurch erhalten Sie automatisch Protokoll dateien mit API-Aktivitäten für die neue Region.

Kontroll-ID	AWS Config	Empfehlungen
9.1.3	rds-logging-enabled	Um die Protokollierung und Überwachung in Ihrer Umgebung zu erleichtern, stellen Sie sicher, dass die Amazon Relational Database Service (Amazon RDS)-Protokollierung aktiviert ist. Mit der Amazon-RDS-Protokollierung können Sie Ereignisse wie Verbindungen, Verbindungsabbrüche, Abfragen oder abgefragte Tabellen erfassen.

Kontroll-ID	AWS Config	Empfehlungen
9.1.3	redshift-cluster-configuration-check	Um Daten im Ruhezustand zu schützen, muss die Verschlüsselung für Ihre Amazon-Redshift-Cluster aktiviert sein. Sie müssen auch sicherstellen, dass die erforderlichen Konfigurationen auf Amazon-Redshift-Clustern bereitgestellt werden. Die Prüfungsprotokollierung muss aktiviert sein, um Informationen zu Verbindungen und Benutzeraktivitäten in der Datenbank bereitzustellen. Diese Regel erfordert, dass ein Wert für clusterDbEncrypted (Config Default: TRUE) und LoggingEnabled (Config Default: TRUE) gesetzt ist. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	AWS Config	Empfehlungen
9.1.3	s-3 bucket-logging-enabled	Die Amazon Simple Storage Service (Amazon S3)-Serverzugriffsprotokollierung bietet eine Methode zur Überwachung des Netzwerks im Hinblick auf potenzielle Cybersicherheitsereignisse. Die Ereignisse werden überwacht, indem detaillierte Aufzeichnungen über die Anfragen erfasst werden, die an einen Amazon-S3-Bucket gestellt wurden. Jeder Zugriffsprotokolleintrag enthält Details zu einer einzelnen Zugriffsanfrage. Zu den Details gehören Anforderer, Bucket-Name, Anforderungszeit, Anforderungsaktion, Antwortstatus und Fehlercode, falls relevant.

Kontroll-ID	AWS Config	Empfehlungen
9.1.3	securityhub-enabled	AWS Security Hub hilft bei der Überwachung von unbefugte m Personal, Verbindungen, Geräten und Software. AWS Security Hub aggregiert, organisiert und priorisiert die Sicherheitswarnungen oder Ergebnisse mehrerer Dienste. AWS Einige dieser Dienste sind Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer und AWS Firewall Manager sowie AWS Partnerlösungen.
9.1.3	vpc-flow-logs-enabled	VPC-Flow-Protokolle erfassen detaillierte Informationsdatens ätze über den IP-Datenv erkehr, der zu und von Netzwerkschnittstellen in Ihrer Amazon Virtual Private Cloud (Amazon VPC) fließt. Standardmäßig enthalten Flow-Protokolldatensätze Werte für die verschiedenen Komponenten des IP-Flows, einschließlich Quelle, Ziel und Protokoll.

Kontroll-ID	AWS Config	Empfehlungen
9.1.3	wafv2-logging-enabled	Um die Protokollierung und Überwachung in Ihrer Umgebung zu erleichte rn, aktivieren Sie die AWS WAF (V2) -Protokollierung im regionalen und globalen Web. ACLs AWS Die WAF-Protokollierung bietet detaillie rte Informationen über den Datenverkehr, der von Ihrer Web-ACL analysiert wird. In den Protokollen werden die Uhrzeit aufgezeichnet, zu der die AWS WAF die Anfrage von Ihrer AWS Ressource erhalten hat, Informationen zu der Anfrage und eine Aktion für die Regel, der jede Anfrage entsprach.

Kontroll-ID	AWS Config	Empfehlungen
9.1.4	iam-password-policy	Die Identitäten und Anmeldein formationen werden auf der Grundlage einer organisat orischen IAM-Passwortrichtl inie ausgestellt, verwaltet und verifiziert. Sie erfüllen oder übertreffen die Anforderungen von NIST SP 800-63 und dem Standard „Best Practices“ von AWS Foundational Security für die Passwortstärke. Mit dieser Regel können Sie optional RequireUppercaseCharacters (Wert für AWS grundlege nde Sicherheitsbewährte Verfahren: wahr), RequireLo wercaseCharacters (Wert für bewährte Methoden für AWS grundlegende Sicherheit: wahr), RequireSymbols (Wert für bewährte Methoden für AWS grundlegende Sicherhei t: wahr), RequireNumbers (Wert für bewährte Methoden für AWS grundlegende Sicherheit: wahr), MinimumPa sswordLength (Wert für bewährte Methoden für AWS grundlegende Sicherheit: 14), PasswordReusePreve ntion (Wert für bewährte Methoden für AWS grundlege nde Sicherheit: 24) und MaxPasswordAge (Wert

Kontroll-ID	AWS Config	Empfehlungen
		für bewährte Methoden für AWS grundlegende Sicherhei t: 90) für Ihr IAM festlegen Kennwortrichtlinie. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisat ion entsprechen.
9.1.5	iam-user-mfa-enabled	Aktivieren Sie diese Regel, um den Zugriff auf Ressourcen in der AWS Cloud einzuschr änken. Diese Regel sorgt dafür, dass die Multi-Faktor-Authentifizierung (MFA) für alle Benutzer aktiviert ist. MFA sorgt für eine weitere Schutzebene zusätzlich zu den Anmeldeinformationen. Reduzieren Sie Fälle von kompromittierten Konten, indem Sie MFA für Benutzer vorschreiben.

Kontroll-ID	AWS Config	Empfehlungen
9.1.5	mfa-enabled-for-iam-Konsolenzugriff	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass MFA für alle AWS Identity and Access Management (IAM) -Benutzer aktiviert ist, die über ein Konsolenkennwort verfügen. MFA sorgt für eine weitere Schutzebene zusätzlich zu den Anmeldeinformationen. Indem Sie MFA für Benutzer vorschreiben, können Sie Fälle kompromittierter Konten reduzieren und verhindern, dass unbefugte Benutzer auf vertrauliche Daten zugreifen.
9.1.5	root-account-hardware-mfa-aktiviert	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Hardware-MFA für den Root-Benutzer aktiviert ist. Der Stammbenutzer ist der AWS-Konto-Benutzer mit den meisten Berechtigungen. MFA sorgt für eine weitere Schutzebene zusätzlich zu den Anmeldeinformationen. Indem Sie MFA für den Root-Benutzer vorschreiben, können Sie die Anzahl AWS-Konten kompromittierter Benutzer reduzieren.

Kontroll-ID	AWS Config	Empfehlungen
9.1.5	root-account-mfa-enabled	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass MFA für den Root-Benutzer aktiviert ist. Der Stammbenutzer ist der AWS-Konto-Benutzer mit den meisten Berechtigungen. MFA sorgt für eine weitere Schutzebene zusätzlich zu den Anmeldeinformationen. Indem Sie MFA für den Root-Benutzer vorschreiben, können Sie die Anzahl AWS-Konten kompromittierter Benutzer reduzieren.

Kontroll-ID	AWS Config	Empfehlungen
9.1.6	iam-user-unused-credentials-überprüfen	AWS Identity and Access Management (IAM) kann Ihnen bei Zugriffsberechtigungen und Autorisierungen helfen, indem es nach IAM-Passwörtern und Zugriffsschlüsseln sucht, die für einen bestimmten Zeitraum nicht verwendet wurden. Wenn ungenutzte Anmeldeinformationen identifiziert werden, müssen Sie sie deaktivieren und/oder entfernen, da dies gegen das Prinzip der geringsten Berechtigung verstoßen könnte. Für diese Regel müssen Sie einen Wert für das maxCredentialUsage Alter festlegen (Standardkonfiguration: 90). Der tatsächliche Wert muss den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	AWS Config	Empfehlungen
9.1.7	emr-kerberos-enabled	Die Zugriffsberechtigungen und -autorisierungen können verwaltet und nach den Prinzipien der geringsten Berechtigung und Aufgabent rennung integriert werden, indem Kerberos für Amazon-EMR-Cluster aktiviert wird. In Kerberos werden Services und Benutzer, die sich authentifizieren müssen, als Prinzipale bezeichnet. Prinzipale befinden sich in einem Kerberos-Bereich. Innerhalb dieses Bereichs wird ein Kerberos-Server als Key Distribution Center (KDC) bezeichnet. Über diesen Server können sich Prinzipale authentifizieren. Die Authentifizierung im KDC erfolgt durch die Ausstellu ng von Authentifizierungs tickets. Das KDC unterhält eine Datenbank der Prinzipal e in seinem Bereich mit ihren Passwörtern und anderen administrativen Informationen zu jedem Prinzipal.

Kontroll-ID	AWS Config	Empfehlungen
9.1.7	iam-customer-policy-blocked-kms-Aktionen	AWS Identity and Access Management (IAM) kann Ihnen helfen, die Prinzipien der geringsten Rechte und der Aufgabentrennung in Zugriffsberechtigungen und Autorisierungen zu integrier en und so zu verhindern, dass Richtlinien blockierte Aktionen für alle AWS Schlüssel des Key Management Service enthalten. Wenn Benutzer mehr Rechte haben, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und Aufgabentrennung verstoßen . Mit dieser Regel können Sie den Parameter festlegen. blockedActionsPatterns (Wert „AWS Bewährte grundlegende Sicherheitsmethoden“: kms: Entschlüsseln, kms:ReEnc ryptFrom). Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprech en.

Kontroll-ID	AWS Config	Empfehlungen
9.1.7	iam-group-has-users-überprüfen	AWS Identity and Access Management (IAM) kann Ihnen helfen, die Prinzipien der geringsten Rechte und der Aufgabentrennung mit Zugriffsberechtigungen und Autorisierungen zu integrieren, indem sichergestellt wird, dass IAM-Gruppen mindestens einen Benutzer haben. Die Einteilung von Benutzern in Gruppen auf der Grundlage der ihnen zugewiesenen Berechtigungen oder ihrer Funktion ist eine Möglichkeit, das Prinzip der geringsten Berechtigung zu implementieren.

Kontroll-ID	AWS Config	Empfehlungen
9.1.7	iam-inline-policy-blocked-kms-Aktionen	Stellen Sie sicher, dass ein Benutzer, eine IAM-Rolle oder eine IAM-Grupp e (AWS Identity and Access Management) nicht über eine Inline-Richtlinie verfügt, die blockierte Aktionen für alle AWS Schlüssel des Key Management Service zulässt. AWS empfiehlt, verwaltete Richtlinien anstelle von Inline-Richtlinien zu verwenden . Verwaltete Richtlinien ermöglichen Wiederver wendbarkeit, Versionsv erwaltung, Rollback und Delegierung der Berechtig ungsverwaltung. Mit dieser Regel können Sie den blockedActionsPatterns Parameter festlegen. (Wert „AWS Bewährte grundlegende Sicherheitsmethoden“: kms: Entschlüsseln, kms:ReEnc ryptFrom). Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprech en.

Kontroll-ID	AWS Config	Empfehlungen
9.1.7	iam-no-inline-policy-überprüfen	Stellen Sie sicher, dass ein Benutzer, eine IAM-Rolle oder eine IAM-Gruppe (AWS Identity and Access Management) nicht über eine Inline-Richtlinie zur Zugriffskontrolle auf Systeme und Ressourcen verfügt. AWS empfiehlt, verwaltete Richtlinien anstelle von Inline-Richtlinien zu verwenden . Verwaltete Richtlinien ermöglichen Wiederverwendbarkeit, Versionsverwaltung, Rollback und Delegierung der Berechtigungsverwaltung.

Kontroll-ID	AWS Config	Empfehlungen
9.1.7	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) kann Ihnen dabei helfen, die Prinzipien der geringsten Rechte und der Aufgabent rennung in Zugriffsberechtigu ngen und Autorisierungen zu integrieren und so zu verhindern, dass Richtlinien „Effect“: „Allow“ mit „Action“: „*“ anstelle von „Resource“: „*“ enthalten. Wenn Benutzern mehr Rechte eingeräumt werden, als für die Ausführun g einer Aufgabe erforderl ich sind, kann dies gegen das Prinzip der geringste n Berechtigung und der Aufgabentrennung verstoßen.
9.2.1	api-gw-execution-logging-ak tiviert	Die API-Gateway-Protok ollierung zeigt detaillierte Ansichten der Benutzer, die auf die API zugegriffen haben, und wie diese Benutzer auf die API zugegriffen haben. Diese Einblicke ermöglichen die Transparenz von Benutzera ktivitäten.

Kontroll-ID	AWS Config	Empfehlungen
9.2.1	cloud-trail-cloud-watch-logs-aktiviert	Verwenden Sie Amazon CloudWatch , um Protokoll ereignisaktivitäten zentral zu sammeln und zu verwalten . Die Aufnahme von AWS CloudTrail Daten liefert Einzelheiten zu den API-Aufru faktivitäten in Ihrem AWS-Konto.
9.2.1	iam-policy-no-statements-with-full-access	Stellen Sie sicher, dass IAM-Aktionen nur auf die benötigte n Aktionen beschränkt sind. Wenn Benutzern mehr Rechte eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und der Aufgabentrennung verstoßen.

Kontroll-ID	AWS Config	Empfehlungen
9.2.1	cloudtrail-enabled	AWS CloudTrail kann durch die Aufzeichnung von Aktionen und API-Aufrufen in der AWS Management Console bei der Nichtabst reitbarkeit helfen. Sie können die Benutzer und die Benutzer AWS-Konten , die einen AWS Dienst aufgerufen haben, die Quell-IP-Adresse, über die die Aufrufe generiert wurden, und den Zeitpunkt der Anrufe identifizieren. Einzelheiten zu den erfassten Daten finden Sie in den AWS CloudTrail Datensatzinhalten.
9.2.1	cloud-trail-encryption-enabled	Da sensible Daten vorhanden sein können und um Daten im Ruhezustand zu schützen, sollten Sie sicherstellen, dass die Verschlüsselung für Ihre AWS CloudTrail Trails aktiviert ist.

Kontroll-ID	AWS Config	Empfehlungen
9.2.1	cloud-trail-log-file-Validierung aktiviert	Verwenden Sie die AWS CloudTrail Protokolldateivalidierung, um die Integrität von Protokollen zu überprüfen. CloudTrail Mithilfe der Protokolldateivalidierung kann festgestellt werden, ob eine Protokolldatei geändert oder gelöscht wurde oder ob sie nach der Übermittlung CloudTrail unverändert geblieben ist. Dieses Feature wurde mit dem Branchenstandard entsprechenden Algorithmen entwickelt: SHA-256 für die Hashfunktion und SHA-256 mit RSA für digitale Signaturen. Aus diesem Grund ist es rechnerisch unmöglich, CloudTrail Protokolldateien unbemerkt zu ändern, zu löschen oder zu fälschen.

Kontroll-ID	AWS Config	Empfehlungen
9.2.1	cw-loggroup-retention-period-überprüfen	Stellen Sie sicher, dass die Ereignisprotokolldaten für Ihre Protokollgruppen über eine Mindestdauer aufbewahrt werden, um die Fehlerbehebung und forensische Untersuch ungen zu unterstützen. Fehlende frühere Ereignisp rotokolldaten erschweren die Rekonstruierung und Identifiz ierung potenziell schädlicher Ereignisse.
9.2.1	iam-root-access-key-überprü fen	Der Zugriff auf Systeme und Ressourcen kann gesteuert werden, indem überprüft wird, ob der Root-Benutzer keine Zugriffsschlüssel mit seiner AWS Identity and Access Management (IAM) -Rolle verknüpft hat. Stellen Sie sicher, dass die Root-Zugr iffsschlüssel gelöscht werden. Erstellen und verwenden Sie stattdessen rollenbasierte Funktionen, AWS-Konten um das Prinzip der geringsten Funktionalität zu berücksic htigen.

Kontroll-ID	AWS Config	Empfehlungen
9.2.1	multi-region-cloudtrail-enabled	AWS CloudTrail zeichnet Aktionen und API-Aufrufe der AWS Management Console auf. Sie können feststellen, welche Benutzer und Konten angerufen wurden AWS, von welcher Quell-IP-Adresse aus die Anrufe getätigt wurden und wann die Anrufe erfolgten . CloudTrail übermittelt Protokolldateien aus allen AWS Regionen an Ihren S3-Bucket, wenn MULTI_REGION_CLOUD_TRAIL_ENABLED aktiviert ist. Außerdem wird beim AWS Start einer neuen Region derselbe Trail in der neuen Region erstellt. CloudTrail Dadurch erhalten Sie automatisch Protokoll dateien mit API-Aktivitäten für die neue Region.

Kontroll-ID	AWS Config	Empfehlungen
9.2.1	redshift-cluster-configuration-check	Um Daten im Ruhezustand zu schützen, muss die Verschlüsselung für Ihre Amazon-Redshift-Cluster aktiviert sein. Sie müssen auch sicherstellen, dass die erforderlichen Konfigurationen auf Amazon-Redshift-Clustern bereitgestellt werden. Die Prüfungsprotokollierung muss aktiviert sein, um Informationen zu Verbindungen und Benutzeraktivitäten in der Datenbank bereitzustellen. Diese Regel erfordert, dass ein Wert für clusterDbEncrypted (Config Default: TRUE) und LoggingEnabled (Config Default: TRUE) gesetzt ist. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	AWS Config	Empfehlungen
9.2.1	securityhub-enabled	AWS Security Hub hilft bei der Überwachung von unbefugte m Personal, Verbindungen, Geräten und Software. AWS Security Hub aggregiert, organisiert und priorisiert die Sicherheitswarnungen oder Ergebnisse mehrerer Dienste. AWS Einige dieser Dienste sind Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer und AWS Firewall Manager sowie AWS Partnerlösungen.
9.2.2	api-gw-execution-logging-aktiviert	Die API-Gateway-Protokollierung zeigt detaillierte Ansichten der Benutzer, die auf die API zugegriffen haben, und wie diese Benutzer auf die API zugegriffen haben. Diese Einblicke ermöglichen die Transparenz von Benutzeraktivitäten.

Kontroll-ID	AWS Config	Empfehlungen
9.2.2	cloud-trail-cloud-watch-logs-aktiviert	Verwenden Sie Amazon CloudWatch , um Protokoll ereignisaktivitäten zentral zu sammeln und zu verwalten . Die Aufnahme von AWS CloudTrail Daten liefert Einzelheiten zu den API-Aufru faktivitäten in Ihrem AWS-Konto.
9.2.2	cloudtrail-enabled	AWS CloudTrail kann durch die Aufzeichnung von Aktionen und API-Aufrufen in der AWS Management Console bei der Nichtabst reitbarkeit helfen. Sie können die Benutzer und die Benutzer AWS-Konten , die einen AWS Dienst aufgerufen haben, die Quell-IP-Adresse, über die die Aufrufe generiert wurden, und den Zeitpunkt der Anrufe identifizieren. Einzelheiten zu den erfassten Daten finden Sie in den AWS CloudTrail Datensatzinhalten.
9.2.2	cloud-trail-encryption-enabled	Da sensible Daten vorhanden sein können und um Daten im Ruhezustand zu schützen, sollten Sie sicherstellen, dass die Verschlüsselung für Ihre AWS CloudTrail Trails aktiviert ist.

Kontroll-ID	AWS Config	Empfehlungen
9.2.2	cloud-trail-log-file-Validierung aktiviert	Verwenden Sie die AWS CloudTrail Protokolldateivalidierung, um die Integrität von Protokollen zu überprüfen. CloudTrail Mithilfe der Protokolldateivalidierung kann festgestellt werden, ob eine Protokolldatei geändert oder gelöscht wurde oder ob sie nach der Übermittlung CloudTrail unverändert geblieben ist. Dieses Feature wurde mit dem Branchenstandard entsprechenden Algorithmen entwickelt: SHA-256 für die Hashfunktion und SHA-256 mit RSA für digitale Signaturen. Aus diesem Grund ist es rechnerisch unmöglich, CloudTrail Protokolldateien unbemerkt zu ändern, zu löschen oder zu fälschen.

Kontroll-ID	AWS Config	Empfehlungen
9.2.2	cw-loggroup-retention-period-überprüfen	Stellen Sie sicher, dass die Ereignisprotokolldaten für Ihre Protokollgruppen über eine Mindestdauer aufbewahrt werden, um die Fehlerbehebung und forensische Untersuch ungen zu unterstützen. Fehlende frühere Ereignisp rotokolldaten erschweren die Rekonstruierung und Identifiz ierung potenziell schädlicher Ereignisse.
9.2.2	ec2-manager instance-managed-by-systems	Eine Bestandsaufnahme der Softwareplattformen und Anwendungen innerhalb des Unternehmens ist möglich, indem Amazon Elastic Compute Cloud (Amazon EC2) -Instances mit AWS Systems Manager verwaltet werden. Verwenden Sie AWS Systems Manager, um detaillierte Systemkonfiguratio nen, Betriebssystem-Patch-Levels, Namen und Typ der Dienste, Softwareinstallati onen, Anwendungsname, Herausgeber und Version sowie andere Details zu Ihrer Umgebung bereitzustellen.

Kontroll-ID	AWS Config	Empfehlungen
9.2.2	guardduty-enabled-centralized	Amazon GuardDuty kann mithilfe von Threat Intelligence Feeds helfen, potenzielle Cybersicherheitsereignisse zu überwachen und zu erkennen. Dazu gehören Listen mit bösartigen IPs und maschinellen Lernmethoden zur Identifizierung unerwarteter, nicht autorisierter und bösartiger Aktivitäten in Ihrer AWS Cloud-Umgebung.

Kontroll-ID	AWS Config	Empfehlungen
9.2.2	multi-region-cloudtrail-enabled	AWS CloudTrail zeichnet Aktionen und API-Aufrufe der AWS Management Console auf. Sie können feststellen, welche Benutzer und Konten angerufen wurden AWS, von welcher Quell-IP-Adresse aus die Anrufe getätigt wurden und wann die Anrufe erfolgten . CloudTrail übermittelt Protokolldateien aus allen AWS Regionen an Ihren S3-Bucket, wenn MULTI_REG ION_CLOUD_TRAIL_EN ABLED aktiviert ist. Außerdem wird beim AWS Start einer neuen Region derselbe Trail in der neuen Region erstellt. CloudTrail Dadurch erhalten Sie automatisch Protokoll dateien mit API-Aktivitäten für die neue Region.

Kontroll-ID	AWS Config	Empfehlungen
9.2.2	redshift-cluster-configuration-check	Um Daten im Ruhezustand zu schützen, muss die Verschlüsselung für Ihre Amazon-Redshift-Cluster aktiviert sein. Sie müssen auch sicherstellen, dass die erforderlichen Konfigurationen auf Amazon-Redshift-Clustern bereitgestellt werden. Die Prüfungsprotokollierung muss aktiviert sein, um Informationen zu Verbindungen und Benutzeraktivitäten in der Datenbank bereitzustellen. Diese Regel erfordert, dass ein Wert für clusterDbEncrypted (Config Default: TRUE) und LoggingEnabled (Config Default: TRUE) gesetzt ist. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	AWS Config	Empfehlungen
9.2.2	securityhub-enabled	AWS Security Hub hilft bei der Überwachung von unbefugte m Personal, Verbindungen, Geräten und Software. AWS Security Hub aggregiert, organisiert und priorisiert die Sicherheitswarnungen oder Ergebnisse mehrerer Dienste. AWS Einige dieser Dienste sind Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer und AWS Firewall Manager sowie AWS Partnerlösungen.
9.3.1	alb-http-to-https-Umleitung sprüfung	Um Daten während der Übertragung zu schützen, stellen Sie sicher, dass Ihr Application Load Balancer unverschlüsselte HTTP-Anfragen automatisch an HTTPS umleitet. Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	AWS Config	Empfehlungen
9.3.1	api-gw-ssl-enabled	Stellen Sie sicher, dass die REST-API-Stufen von Amazon API Gateway mit SSL-Zerti fikaten konfiguriert sind, damit Backend-Systeme überprüfe n können, ob Anforderungen von API Gateway stammen.
9.3.1	elasticsearch-node-to-node-Verschlüsselungsprüfung	Stellen Sie sicher, dass die node-to-node Verschlüsselung für Amazon OpenSearch Service aktiviert ist. Node-to-nodeVerschlüsselung ermöglicht die TLS 1.2-Versc hlüsselung für die gesamte Kommunikation innerhalb der Amazon Virtual Private Cloud (Amazon VPC). Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	AWS Config	Empfehlungen
9.3.1	opensearch-node-to-node-Verschlüsselungsprüfung	Stellen Sie sicher, dass die node-to-node Verschlüsselung für Amazon OpenSearch Service aktiviert ist. Node-to-nodeVerschlüsselung ermöglicht die TLS 1.2-Verschlüsselung für die gesamte Kommunikation innerhalb der Amazon Virtual Private Cloud (Amazon VPC). Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.
9.3.1	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) Security Groups können bei der Verwaltung des Netzwerkzugriffs helfen, indem sie eine statusbehaftete Filterung des ein- und ausgehenden Netzwerkverkehrs zu Ressourcen bereitstellen. AWS Wenn Sie eingehenden (oder entfernten) Datenverkehr von 0.0.0.0/0 bis Port 22 auf Ihren Ressourcen nicht zulassen, können Sie den Remote-Zugriff einschränken.

Kontroll-ID	AWS Config	Empfehlungen
9.3.1	vpc-default-security-group-geschlossen	Sicherheitsgruppen von Amazon Elastic Compute Cloud (Amazon EC2) können bei der Verwaltung des Netzwerkzugriffs helfen, indem sie eine statusbeh aftete Filterung des ein- und ausgehenden Netzwerkv erkehrs zu Ressourcen bereitstellen. AWS Die Beschränkung des gesamten Datenverkehrs auf die Standardsicherheitsgruppe hilft dabei, den Fernzugriff auf Ihre Ressourcen einzuschr änken. AWS

Kontroll-ID	AWS Config	Empfehlungen
9.3.1	vpc-sg-open-only-to-authorized-ports	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass gemeinsame Ports für Amazon Elastic Compute Cloud (Amazon EC2) - Sicherheitsgruppen eingeschränkt sind. Wenn der Zugriff auf Ports nicht auf vertrauenswürdige Quellen beschränkt wird, kann dies zu Angriffen auf die Verfügbarkeit, Integrität und Vertraulichkeit von Systemen führen. Durch die Beschränkung des Zugriffs auf Ressourcen innerhalb einer Sicherheitsgruppe aus dem Internet (0.0.0.0/0) kann der Remote-Zugriff auf interne Systeme gesteuert werden.
9.3.1	elb-acm-certificate-required	Zum Schutz von eventuell vorhandenen sensiblen Daten sowie von Daten während der Übertragung muss die Verschlüsselung für Ihr Elastic Load Balancing aktiviert sein. Verwenden Sie AWS Certificate Manager, um öffentliche und private SSL/TLS-Zertifikate mit AWS Diensten und internen Ressourcen zu verwalten, bereitzustellen und bereitzustellen.

Kontroll-ID	AWS Config	Empfehlungen
9.3.1	elb-tls-https-listeners-nur	Stellen Sie sicher, dass Ihre Elastic Load Balancer (ELBs) mit SSL- oder HTTPS-Listenern konfiguriert sind. Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.
9.3.1	iam-user-unused-credentials-überprüfen	AWS Identity and Access Management (IAM) kann Ihnen bei Zugriffsberechtigungen und Autorisierungen helfen, indem es nach IAM-Passwörtern und Zugriffsschlüsseln sucht, die für einen bestimmten Zeitraum nicht verwendet wurden. Wenn ungenutzte Anmeldeinformationen identifiziert werden, müssen Sie sie deaktivieren und/oder entfernen, da dies gegen das Prinzip der geringsten Berechtigung verstoßen könnte. Für diese Regel müssen Sie einen Wert für das maxCredentialUsage Alter festlegen (Standardkonfiguration: 90). Der tatsächliche Wert muss den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	AWS Config	Empfehlungen
9.3.1	mfa-enabled-for-iam-Konsolenzugriff	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass MFA für alle AWS Identity and Access Management (IAM) -Benutzer aktiviert ist, die über ein Konsolenkennwort verfügen. MFA sorgt für eine weitere Schutzebene zusätzlich zu den Anmeldeinformationen. Indem Sie MFA für Benutzer vorschreiben, können Sie Fälle kompromittierter Konten reduzieren und verhindern, dass unbefugte Benutzer auf vertrauliche Daten zugreifen.
9.3.1	redshift-require-tls-ssl	Stellen Sie sicher, dass Ihre Amazon-Redshift-Cluster eine TLS/SSL-Verschlüsselung erfordern, um eine Verbindung zu SQL-Clients herzustellen. Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	AWS Config	Empfehlungen
9.3.1	root-account-hardware-mfa-aktiviert	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Hardware-MFA für den Root-Benutzer aktiviert ist. Der Stammbenutzer ist der AWS-Konto-Benutzer mit den meisten Berechtigungen. MFA sorgt für eine weitere Schutzebene zusätzlich zu den Anmeldeinformationen. Indem Sie MFA für den Root-Benutzer vorschreiben, können Sie die Anzahl AWS-Konten kompromittierter Benutzer reduzieren.
9.3.1	root-account-mfa-enabled	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass MFA für den Root-Benutzer aktiviert ist. Der Stammbenutzer ist der AWS-Konto-Benutzer mit den meisten Berechtigungen. MFA sorgt für eine weitere Schutzebene zusätzlich zu den Anmeldeinformationen. Indem Sie MFA für den Root-Benutzer vorschreiben, können Sie die Anzahl AWS-Konten kompromittierter Benutzer reduzieren.

Kontroll-ID	AWS Config	Empfehlungen
9.3.1	s-3 bucket-ssl-requests-only	Um Daten während der Übertragung zu schützen, stellen Sie sicher, dass Ihre Amazon Simple Storage Service (Amazon S3)-Bucke ts Anfragen zur Verwendun g von Secure Socket Layer (SSL)-Buckets erfordern. Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.
10.1.1	acm-certificate-expiration-check	Stellen Sie sicher, dass die Netzwerkintegrität geschützt ist, indem Sie sicherstellen, dass X509-Zertifikate von AWS ACM ausgestellt werden. Diese Zertifikate müssen gültig und dürfen nicht abgelaufe n sein. Für diese Regel ist ein Wert für erforderlich daysToExpiration (Wert für bewährte AWS Grundrege ln für Sicherheit: 90). Der tatsächliche Wert muss den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	AWS Config	Empfehlungen
10.1.1	alb-http-to-https-Umleitung sprüfung	Um Daten während der Übertragung zu schützen, stellen Sie sicher, dass Ihr Application Load Balancer unverschlüsselte HTTP-Anfragen automatisch an HTTPS umleitet. Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.
10.1.1	api-gw-cache-enabled-und-ve rschlüsselt	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass die Verschlüsselung für den Cache Ihrer API-Gatew ay-Stufe aktiviert ist. Da für die API-Methode sensible Daten erfasst werden können, sollten Sie die Verschlüsselung von Daten im Ruhezustand aktivieren, um diese Daten zu schützen.
10.1.1	api-gw-ssl-enabled	Stellen Sie sicher, dass die REST-API-Stufen von Amazon API Gateway mit SSL-Zerti fikaten konfiguriert sind, damit Backend-Systeme überprüfe n können, ob Anforderungen von API Gateway stammen.

Kontroll-ID	AWS Config	Empfehlungen
10.1.1	cloud-trail-encryption-enabled	Da sensible Daten vorhanden sein können und um Daten im Ruhezustand zu schützen, sollten Sie sicherstellen, dass die Verschlüsselung für Ihre AWS CloudTrail Trails aktiviert ist.
10.1.1	cloudwatch-log-group-encrypted	Um sensible Daten im Speicher zu schützen, stellen Sie sicher, dass die Verschlüsselung für Ihre Amazon CloudWatch Log Groups aktiviert ist.
10.1.1	dynamodb-table-encrypted-kms	Stellen Sie sicher, dass die Verschlüsselung für Ihre Amazon-DynamoDB-Tabellen aktiviert ist. Um eventuell vorhandene sensible Daten im Ruhezustand in diesen Tabellen zu schützen, müssen Sie die Verschlüsselung von Daten im Ruhezustand aktivieren. Standardmäßig werden DynamoDB-Tabellen mit einem AWS eigenen Kundenhauptschlüssel (CMK) verschlüsselt.

Kontroll-ID	AWS Config	Empfehlungen
10.1.1	ec-2 ebs-encryption-by-default	Zum Schutz von Daten im Ruhezustand müssen Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon Elastic Block Store (Amazon EBS)-Volumes aktiviert ist. Da sensible Daten auch im Ruhezusta nd vorhanden sein können, sollten Sie die Verschlüs selung im Ruhezustand aktivieren, um diese Daten zu schützen.
10.1.1	efs-encrypted-check	Aktivieren Sie die Verschlüs selung für Ihr Amazon Elastic File System (EFS), um eventuell vorhandene sensible Daten sowie Daten im Ruhezustand zu schützen.
10.1.1	elasticsearch-encrypted-at-rest	Da sensible Daten vorhanden sein können und um Daten im Ruhezustand zu schützen, sollten Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon OpenSearch Service (OpenSearch Service) -Domains aktiviert ist.

Kontroll-ID	AWS Config	Empfehlungen
10.1.1	opensearch-encrypted-at-rest	Da sensible Daten vorhanden sein können und um Daten im Ruhezustand zu schützen, sollten Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon OpenSearch Service-Domains aktiviert ist.
10.1.1	elasticsearch-node-to-node-Verschlüsselungsprüfung	Stellen Sie sicher, dass die node-to-node Verschlüsselung für Amazon OpenSearch Service aktiviert ist. Node-to-nodeVerschlüsselung ermöglicht die TLS 1.2-Versc hlüsselung für die gesamte Kommunikation innerhalb der Amazon Virtual Private Cloud (Amazon VPC). Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	AWS Config	Empfehlungen
10.1.1	opensearch-node-to-node-Verschlüsselungsprüfung	Stellen Sie sicher, dass die node-to-node Verschlüsselung für Amazon OpenSearch Service aktiviert ist. Node-to-nodeVerschlüsselung ermöglicht die TLS 1.2-Verschlüsselung für die gesamte Kommunikation innerhalb der Amazon Virtual Private Cloud (Amazon VPC). Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.
10.1.1	elb-acm-certificate-required	Zum Schutz von eventuell vorhandenen sensiblen Daten sowie von Daten während der Übertragung muss die Verschlüsselung für Ihr Elastic Load Balancing aktiviert sein. Verwenden Sie AWS Certificate Manager, um öffentliche und private SSL/TLS-Zertifikate mit AWS Diensten und internen Ressourcen zu verwalten, bereitzustellen und bereitzustellen.

Kontroll-ID	AWS Config	Empfehlungen
10.1.1	elb-tls-https-listeners-nur	Stellen Sie sicher, dass Ihre Elastic Load Balancer (ELBs) mit SSL- oder HTTPS-Listenern konfiguriert sind. Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.
10.1.1	elv 2 acm-certificate-required	Zum Schutz von eventuell vorhandenen sensiblen Daten sowie von Daten während der Übertragung muss die Verschlüsselung für Ihr Elastic Load Balancing aktiviert sein. Verwenden Sie AWS Certificate Manager, um öffentliche und private SSL/TLS-Zertifikate mit AWS Diensten und internen Ressourcen zu verwalten, bereitzustellen und bereitzustellen.
10.1.1	encrypted-volumes	Aktivieren Sie die Verschlüsselung für Ihre Amazon-Elastic-Block-Store (Amazon-EBS)-Volumes, um eventuell vorhandene sensible Daten sowie Daten im Ruhezustand zu schützen.

Kontroll-ID	AWS Config	Empfehlungen
10.1.1	rds-snapshot-encrypted	Stellen Sie sicher, dass die Verschlüsselung für Ihre Amazon Relational Database Service (Amazon RDS)-Snap shots aktiviert ist. Da sensible Daten auch im Ruhezusta nd vorhanden sein können, sollten Sie die Verschlüs selung im Ruhezustand aktivieren, um diese Daten zu schützen.
10.1.1	rds-storage-encrypted	Zum Schutz von Daten im Ruhezustand müssen Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon Relational Database Service (Amazon RDS)-Instances aktiviert ist. Um eventuell vorhandene sensible Daten im Ruhezustand in Amazon-RDS-Instanc es zu schützen, muss die Verschlüsselung von Daten im Ruhezustand aktiviert sein.

Kontroll-ID	AWS Config	Empfehlungen
10.1.1	redshift-cluster-configuration-check	Um Daten im Ruhezustand zu schützen, muss die Verschlüsselung für Ihre Amazon-Redshift-Cluster aktiviert sein. Sie müssen auch sicherstellen, dass die erforderlichen Konfigurationen auf Amazon-Redshift-Clustern bereitgestellt werden. Die Prüfungsprotokollierung muss aktiviert sein, um Informationen zu Verbindungen und Benutzeraktivitäten in der Datenbank bereitzustellen. Diese Regel erfordert, dass ein Wert für clusterDbEncrypted (Config Default: TRUE) und LoggingEnabled (Config Default: TRUE) gesetzt ist. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	AWS Config	Empfehlungen
10.1.1	redshift-cluster-kms-enabled	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass die Verschlüsselung mit AWS Key Management Service (AWS KMS) für Ihren Amazon Redshift Redshift-Cluster aktiviert ist. Um eventuell vorhandene sensible Daten im Ruhezustand in Redshift-Clustern zu schützen, muss die Verschlüsselung von Daten im Ruhezustand aktiviert sein.
10.1.1	redshift-require-tls-ssl	Stellen Sie sicher, dass Ihre Amazon-Redshift-Cluster eine TLS/SSL-Verschlüsselung erfordern, um eine Verbindun g zu SQL-Clients herzustel len. Um eventuell vorhanden e sensible Daten zu schützen, sollten Sie die Verschlüs selung bei der Übertragung aktivieren.

Kontroll-ID	AWS Config	Empfehlungen
10.1.1	s3-fähig bucket-server-side-encryption	Zum Schutz von Daten im Ruhezustand müssen Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon Simple Storage Service (Amazon S3)-Buckets aktiviert ist. Um eventuell vorhandene sensible Daten im Ruhezustand in Amazon-S3-Buckets zu schützen, muss die Verschlüsselung aktiviert sein.
10.1.1	s-3 bucket-ssl-requests-only	Um Daten während der Übertragung zu schützen, stellen Sie sicher, dass Ihre Amazon Simple Storage Service (Amazon S3)-Buckets Anfragen zur Verwendung von Secure Socket Layer (SSL)-Buckets erfordern. Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	AWS Config	Empfehlungen
10.1.1	s-3 default-encryption-kms	Stellen Sie sicher, dass die Verschlüsselung für Ihre Amazon Simple Storage Service (Amazon S3)-Buckets aktiviert ist. Um eventuell vorhandene sensible Daten im Ruhezustand in einem Amazon-S3-Bucket zu schützen, muss die Verschlüsselung aktiviert sein.
10.1.1	sagemaker-endpoint-configuration-kms-schlüsselkonfiguriert	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass die Verschlüsselung mit dem AWS Key Management Service (AWS KMS) für Ihren Endpunkt aktiviert ist. SageMaker Da sensible Daten auf dem SageMaker Endgerät gespeichert werden können, sollten Sie die Verschlüsselung im Ruhezustand aktivieren, um diese Daten zu schützen.

Kontroll-ID	AWS Config	Empfehlungen
10.1.1	sagemaker-notebook-instance-kms-schlüsselkonfiguriert	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass die Verschlüsselung mit dem AWS Key Management Service (AWS KMS) für Ihr Notebook aktiviert ist. SageMaker Da vertrauliche Daten im SageMaker Notebook gespeichert werden können, sollten Sie die Verschlüsselung im Ruhezustand aktivieren, um diese Daten zu schützen.
10.1.1	secretsmanager-using-cmk	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass die Verschlüsselung mit dem AWS Key Management Service (AWS KMS) für AWS Secrets Manager aktiviert ist. Aktivieren Sie die Verschlüsselung von Daten im Ruhezustand, um eventuell vorhandene sensible Daten im Ruhezustand im Secrets Manager zu schützen.

Kontroll-ID	AWS Config	Empfehlungen
10.1.1	sns-encrypted-kms	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass Ihre Amazon Simple Notification Service (Amazon SNS) -Themen mit dem AWS Key Management Service (AWS KMS) verschlüsselt werden müssen. Um eventuell vorhandene sensible Daten im Ruhezustand in veröffentlichten Nachrichten zu schützen, muss die Verschlüsselung von Daten im Ruhezustand aktiviert sein.
10.2.1	acm-certificate-expiration-check	Stellen Sie sicher, dass die Netzwerkintegrität geschützt ist, indem Sie sicherstellen, dass X509-Zertifikate von AWS ACM ausgestellt werden. Diese Zertifikate müssen gültig und dürfen nicht abgelaufen sein. Für diese Regel ist ein Wert für erforderlich daysToExpiration (Wert für bewährte AWS Grundregeln für Sicherheit: 90). Der tatsächliche Wert muss den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	AWS Config	Empfehlungen
10.2.1	cmk-backing-key-rotation-aktiviert	Aktivieren Sie die Schlüssel rotation, um sicherzustellen, dass Schlüssel rotiert werden, nachdem sie das Ende ihrer Krypto-Periode erreicht haben.
10.2.1	kms-cmk-not-scheduled-zum Löschen	Um Daten im Ruhezustand zu schützen, sollten Sie sicherstellen, dass die für den Kunden erforderlichen Masterschlüssel (CMKs) nicht für das Löschen im AWS Key Management Service (AWS KMS) vorgesehen sind. Da Schlüssel manchmal gelöscht werden müssen, können Sie mit dieser Regel alle zu löschenden Schlüssel überprüfen, falls ein Schlüssel versehentlich zur Löschung vorgemerkt wurde.

Kontroll-ID	AWS Config	Empfehlungen
10.2.2	kms-cmk-not-scheduled-zum Löschen	Um Daten im Ruhezustand zu schützen, sollten Sie sicherstellen, dass die für den Kunden erforderlichen Masterschlüssel (CMKs) nicht für das Löschen im AWS Key Management Service (AWS KMS) vorgesehen sind. Da Schlüssel manchmal gelöscht werden müssen, können Sie mit dieser Regel alle zu löschenden Schlüssel überprüfen, falls ein Schlüssel versehentlich zur Löschung vorgemerkt wurde.

Kontroll-ID	AWS Config	Empfehlungen
10.2.3	access-keys-rotated	Die Anmeldeinformationen für autorisierte Geräte, Benutzer und Prozesse werden geprüft, indem sichergestellt wird, dass die IAM-Zugriffsschlüssel entsprechend den Vorgaben der Unternehmensrichtlinie rotiert werden. Das regelmäßi ge Ändern der Zugriffss chlüssel ist eine bewährte Sicherheitsmethode. Es verkürzt den Zeitraum, in dem ein Zugriffsschlüssel aktiv ist, und reduziert die Auswirkun gen auf das Unternehmen, wenn die Schlüssel kompromit tiert werden. Diese Regel erfordert einen Wert für die Zugriffsschlüssel-Rotation (Standardkonfiguration: 90). Der tatsächliche Wert muss den Richtlinien Ihrer Organisat ion entsprechen.
10.2.3	cmk-backing-key-rotation-ak tiviert	Aktivieren Sie die Schlüssel rotation, um sicherzustellen, dass Schlüssel rotiert werden, nachdem sie das Ende ihrer Krypto-Periode erreicht haben.

Kontroll-ID	AWS Config	Empfehlungen
10.2.3	kms-cmk-not-scheduled-zum Löschen	Um Daten im Ruhezusta nd zu schützen, sollten Sie sicherstellen, dass die für den Kunden erforderlichen Masterschlüssel (CMKs) nicht für das Löschen im AWS Key Management Service (AWS KMS) vorgesehen sind. Da Schlüssel manchmal gelöscht werden müssen, können Sie mit dieser Regel alle zu löschenden Schlüssel überprüfen, falls ein Schlüssel versehentlich zur Löschung vorgemerkt wurde.
11.1.1 (a)	acm-certificate-expiration-check	Stellen Sie sicher, dass die Netzwerkintegrität geschützt ist, indem Sie sicherstellen, dass X509-Zertifikate von AWS ACM ausgestellt werden. Diese Zertifikate müssen gültig und dürfen nicht abgelaufe n sein. Für diese Regel ist ein Wert für erforderlich daysToExpiration (Wert für bewährte AWS Grundrege ln für Sicherheit: 90). Der tatsächliche Wert muss den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	AWS Config	Empfehlungen
11.1.1 (a)	alb-http-to-https-Umleitung sprüfung	Um Daten während der Übertragung zu schützen, stellen Sie sicher, dass Ihr Application Load Balancer unverschlüsselte HTTP-Anfragen automatisch an HTTPS umleitet. Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.
11.1.1 (a)	api-gw-cache-enabled-und-ve rschlüsselt	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass die Verschlüsselung für den Cache Ihrer API-Gatew ay-Stufe aktiviert ist. Da für die API-Methode sensible Daten erfasst werden können, sollten Sie die Verschlüsselung von Daten im Ruhezustand aktivieren, um diese Daten zu schützen.
11.1.1 (a)	api-gw-ssl-enabled	Stellen Sie sicher, dass die REST-API-Stufen von Amazon API Gateway mit SSL-Zerti fikaten konfiguriert sind, damit Backend-Systeme überprüfe n können, ob Anforderungen von API Gateway stammen.

Kontroll-ID	AWS Config	Empfehlungen
11.1.1 (a)	elasticsearch-node-to-node-Verschlüsselungsprüfung	Stellen Sie sicher, dass die node-to-node Verschlüsselung für Amazon OpenSearch Service aktiviert ist. Node-to-nodeVerschlüsselung ermöglicht die TLS 1.2-Versc hlüsselung für die gesamte Kommunikation innerhalb der Amazon Virtual Private Cloud (Amazon VPC). Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.
11.1.1 (a)	opensearch-node-to-node-Verschlüsselungsprüfung	Stellen Sie sicher, dass die node-to-node Verschlüsselung für Amazon OpenSearch Service aktiviert ist. Node-to-nodeVerschlüsselung ermöglicht die TLS 1.2-Versc hlüsselung für die gesamte Kommunikation innerhalb der Amazon Virtual Private Cloud (Amazon VPC). Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	AWS Config	Empfehlungen
11.1.1 (a)	elbv-2 acm-certificate-required	Zum Schutz von eventuell vorhandenen sensiblen Daten sowie von Daten während der Übertragung muss die Verschlüsselung für Ihr Elastic Load Balancing aktiviert sein. Verwenden Sie AWS Certifica te Manager, um öffentlic he und private SSL/TLS-Z ertifikate mit AWS Diensten und internen Ressourcen zu verwalten, bereitzustellen und bereitzustellen.
11.1.1 (a)	guardduty-enabled-centralized	Amazon GuardDuty kann mithilfe von Threat Intellige nce Feeds helfen, potenzielle Cybersicherheitsereignisse zu überwachen und zu erkennen. Dazu gehören Listen mit bösartigen IPs und maschinel len Lernmethoden zur Identifiz ierung unerwarteter, nicht autorisierter und bösartige r Aktivitäten in Ihrer AWS Cloud-Umgebung.

Kontroll-ID	AWS Config	Empfehlungen
11.1.1 (a)	redshift-require-tls-ssl	Stellen Sie sicher, dass Ihre Amazon-Redshift-Cluster eine TLS/SSL-Verschlüsselung erfordern, um eine Verbindung zu SQL-Clients herzustellen. Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.
11.1.1 (a)	s-3 bucket-ssl-requests-only	Um Daten während der Übertragung zu schützen, stellen Sie sicher, dass Ihre Amazon Simple Storage Service (Amazon S3)-Buckets Anfragen zur Verwendung von Secure Socket Layer (SSL)-Buckets erfordern. Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.
11.1.1 (b)	api-gw-cache-enabled-und-verschlüsselt	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass die Verschlüsselung für den Cache Ihrer API-Gateway-Stufe aktiviert ist. Da für die API-Methode sensible Daten erfasst werden können, sollten Sie die Verschlüsselung von Daten im Ruhezustand aktivieren, um diese Daten zu schützen.

Kontroll-ID	AWS Config	Empfehlungen
11.1.1 (b)	autoscaling-launch-config-public-ip-deaktiviert	Wenn Sie Ihre Netzwerkschnittstellen mit einer öffentlichen IP-Adresse konfigurieren, sind die diesen Netzwerkschnittstellen zugehörigen Ressourcen über das Internet erreichbar. EC2 Ressourcen sollten nicht öffentlich zugänglich sein, da dies einen unbeabsichtigten Zugriff auf Ihre Anwendungen oder Server ermöglichen kann.
11.1.1 (b)	cloud-trail-encryption-enabled	Da sensible Daten vorhanden sein können und um Daten im Speicher zu schützen, sollten Sie sicherstellen, dass die Verschlüsselung für Ihre AWS CloudTrail Trails aktiviert ist.
11.1.1 (b)	cloudwatch-log-group-encrypted	Um sensible Daten im Speicher zu schützen, stellen Sie sicher, dass die Verschlüsselung für Ihre Amazon CloudWatch Log Groups aktiviert ist.

Kontroll-ID	AWS Config	Empfehlungen
11.1.1 (b)	dms-replication-not-public	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass auf DMS-Replikationsinstanzen nicht öffentlich zugegriffen werden kann. DMS-Replikations-Instances können vertrauliche Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.
11.1.1 (b)	dynamodb-table-encrypted-kms	Stellen Sie sicher, dass die Verschlüsselung für Ihre Amazon-DynamoDB-Tabellen aktiviert ist. Um eventuell vorhandene sensible Daten im Ruhezustand in diesen Tabellen zu schützen, müssen Sie die Verschlüsselung von Daten im Ruhezustand aktivieren. Standardmäßig werden DynamoDB-Tabellen mit einem AWS eigenen Kundenhauptschlüssel (CMK) verschlüsselt.
11.1.1 (b)	ebs-snapshot-public-restorable-überprüfen	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass EBS-Snapshots nicht öffentlich wiederherstellbar sind. EBS-Volume-Snapshots können vertrauliche Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	AWS Config	Empfehlungen
11.1.1 (b)	ec-2 ebs-encryption-by-default	Zum Schutz von Daten im Ruhezustand müssen Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon Elastic Block Store (Amazon EBS)-Volumes aktiviert ist. Da sensible Daten auch im Ruhezusta nd vorhanden sein können, sollten Sie die Verschlüs selung im Ruhezustand aktivieren, um diese Daten zu schützen.
11.1.1 (b)	ec2- instance-no-public-ip	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon Elastic Compute Cloud (Amazon EC2) -Instances nicht öffentlich zugänglich sind. EC2 Amazon-Instances können vertrauliche Informati onen enthalten, und für solche Konten ist eine Zugriffsk ontrolle erforderlich.
11.1.1 (b)	efs-encrypted-check	Aktivieren Sie die Verschlüs selung für Ihr Amazon Elastic File System (EFS), um eventuell vorhandene sensible Daten sowie Daten im Ruhezustand zu schützen.

Kontroll-ID	AWS Config	Empfehlungen
11.1.1 (b)	elasticsearch-encrypted-at-rest	Da sensible Daten vorhanden sein können und um Daten im Ruhezustand zu schützen, sollten Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon OpenSearch Service (OpenSearch Service) -Domains aktiviert ist.
11.1.1 (b)	opensearch-encrypted-at-rest	Da sensible Daten vorhanden sein können und um Daten im Ruhezustand zu schützen, sollten Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon OpenSearch Service-Domains aktiviert ist.
11.1.1 (b)	elasticsearch-in-vpc-only	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass sich Amazon OpenSearch OpenSearch Service (Service) -Domains innerhalb einer Amazon Virtual Private Cloud (Amazon VPC) befinden. Eine OpenSearch Service-D omain innerhalb einer Amazon VPC ermöglicht die sichere Kommunikation zwischen OpenSearch Service und anderen Services innerhalb der Amazon VPC, ohne dass ein Internet-Gateway, ein NAT-Gerät oder eine VPN-Verbindung erforderlich ist.

Kontroll-ID	AWS Config	Empfehlungen
11.1.1 (b)	opensearch-in-vpc-only	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass sich Amazon OpenSearch Service-Domains innerhalb einer Amazon Virtual Private Cloud (Amazon VPC) befinden. Eine Amazon OpenSearch Service-Domain innerhalb einer Amazon VPC ermöglich t die sichere Kommunika tion zwischen Amazon OpenSearch Service und anderen Services innerhalb der Amazon VPC, ohne dass ein Internet-Gateway, ein NAT-Gerät oder eine VPN-Verbindung erforderlich ist.
11.1.1 (b)	emr-master-no-public-ip	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon EMR-Cluster-Masterknoten nicht öffentlich zugänglich sind. Amazon-EMR-Cluster-Hauptknoten können vertrauli che Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	AWS Config	Empfehlungen
11.1.1 (b)	encrypted-volumes	Aktivieren Sie die Verschlüs selung für Ihre Amazon-El astic-Block-Store (Amazon-EBS)-Volumes, um eventuell vorhandene sensible Daten sowie Daten im Ruhezustand zu schützen.
11.1.1 (b)	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) Security Groups können bei der Verwaltung des Netzwerkz ugriffs helfen, indem sie eine statusbehaftete Filterung des ein- und ausgehend en Netzwerkverkehrs zu Ressourcen bereitstellen. AWS Wenn Sie eingehenden (oder entfernten) Datenverk ehr von 0.0.0.0/0 bis Port 22 auf Ihren Ressourcen nicht zulassen, können Sie den Remote-Zugriff einschränken.

Kontroll-ID	AWS Config	Empfehlungen
11.1.1 (b)	ec2- instances-in-vpc	Stellen Sie Amazon Elastic Compute Cloud (Amazon EC2) -Instances innerhalb einer Amazon Virtual Private Cloud (Amazon VPC) bereit, um eine sichere Kommunika tion zwischen einer Instance und anderen Services innerhalb der Amazon VPC zu ermöglichen, ohne dass ein Internet-Gateway, ein NAT-Gerät oder eine VPN-Verbi ndung erforderlich ist. Der gesamte Datenverkehr bleibt sicher in der AWS Cloud. Domains, die sich innerhalb einer VPC befinden, verfügen aufgrund ihrer logischen Isolierung im Vergleich zu Domains mit öffentlic hen Endpunkten über eine zusätzliche Sicherheitsebene. Weisen Sie EC2 Amazon-In stances einer Amazon-VPC zu, um den Zugriff ordnungsg emäß zu verwalten.

Kontroll-ID	AWS Config	Empfehlungen
11.1.1 (b)	lambda-function-public-access-verboten	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass AWS Lambda-Funktionen nicht öffentlich zugänglich sind. Der öffentliche Zugriff kann möglicherweise die Verfügbarkeit von Ressourcen beeinträchtigen.

Kontroll-ID	AWS Config	Empfehlungen
11.1.1 (b)	lambda-inside-vpc	Stellen Sie AWS Lambda-Funktionen in einer Amazon Virtual Private Cloud (Amazon VPC) bereit, um eine sichere Kommunikation zwischen einer Funktion und anderen Diensten innerhalb der Amazon VPC zu gewährleisten. Bei dieser Konfiguration sind kein Internet-Gateway, kein NAT-Gerät und keine VPN-Verbindung erforderlich. Der gesamte Datenverkehr bleibt sicher in der Cloud. AWS Domains, die sich innerhalb einer VPC befinden, verfügen aufgrund ihrer logischen Isolierung im Vergleich zu Domains mit öffentlichen Endpunkten über eine zusätzliche Sicherheitsebene. Um den Zugriff ordnungsgemäß zu verwalten, sollten AWS Lambda-Funktionen einer VPC zugewiesen werden.

Kontroll-ID	AWS Config	Empfehlungen
11.1.1 (b)	no-unrestricted-route-to-igw	Stellen Sie sicher, dass EC2 Amazon-Routentabellen keine uneingeschränkten Routen zu einem Internet-Gateway enthalten. Durch das Entfernen oder Beschränken des Internetzugangs für Workloads innerhalb von Amazon VPCs können unbeabsichtigte Zugriffe in Ihrer Umgebung reduziert werden.
11.1.1 (b)	rds-instance-public-access-überprüfen	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Relational Database Service (Amazon RDS) -Instances nicht öffentlich sind. Amazon-RDS-Datenbank-Instances können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	AWS Config	Empfehlungen
11.1.1 (b)	rds-snapshot-encrypted	Stellen Sie sicher, dass die Verschlüsselung für Ihre Amazon Relational Database Service (Amazon RDS)-Snapshots aktiviert ist. Da sensible Daten auch im Ruhezustand vorhanden sein können, sollten Sie die Verschlüsselung im Ruhezustand aktivieren, um diese Daten zu schützen.
11.1.1 (b)	rds-snapshots-public-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Relational Database Service (Amazon RDS) -Instances nicht öffentlich sind. Amazon-RDS-Datenbank-Instances können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	AWS Config	Empfehlungen
11.1.1 (b)	rds-storage-encrypted	Zum Schutz von Daten im Ruhezustand müssen Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon Relational Database Service (Amazon RDS)-Instances aktiviert ist. Um eventuell vorhandene sensible Daten im Ruhezustand in Amazon-RDS-Instanc es zu schützen, muss die Verschlüsselung von Daten im Ruhezustand aktiviert sein.

Kontroll-ID	AWS Config	Empfehlungen
11.1.1 (b)	redshift-cluster-configuration-check	Um Daten im Ruhezustand zu schützen, muss die Verschlüsselung für Ihre Amazon-Redshift-Cluster aktiviert sein. Sie müssen auch sicherstellen, dass die erforderlichen Konfigurationen auf Amazon-Redshift-Clustern bereitgestellt werden. Die Prüfungsprotokollierung muss aktiviert sein, um Informationen zu Verbindungen und Benutzeraktivitäten in der Datenbank bereitzustellen. Diese Regel erfordert, dass ein Wert für clusterDbEncrypted (Config Default: TRUE) und LoggingEnabled (Config Default: TRUE) gesetzt ist. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	AWS Config	Empfehlungen
11.1.1 (b)	redshift-cluster-kms-enabled	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass die Verschlüsselung mit AWS Key Management Service (AWS KMS) für Ihren Amazon Redshift Redshift-Cluster aktiviert ist. Um eventuell vorhandene sensible Daten im Ruhezustand in Redshift-Clustern zu schützen, muss die Verschlüsselung von Daten im Ruhezustand aktiviert sein.
11.1.1 (b)	redshift-cluster-public-access-überprüfen	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherste llen, dass Amazon Redshift Redshift-Cluster nicht öffentlic h sind. Amazon-Redshift-Cluster können vertrauli che Informationen enthalten und für solche Konten sind Prinzipien und Zugriffsk ontrollen erforderlich.

Kontroll-ID	AWS Config	Empfehlungen
11.1.1 (b)	restricted-common-ports	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass gemeinsame Ports für Amazon Elastic Compute Cloud (Amazon EC2) - Sicherheitsgruppen eingeschränkt sind. Wenn der Zugriff auf Ports nicht auf vertrauenswürdige Quellen beschränkt wird, kann dies zu Angriffen auf die Verfügbarkeit, Integrität und Vertraulichkeit von Systemen führen. Mit dieser Regel können Sie optional die Parameter blockedPort1–blockedPort5 festlegen (Standardkonfigurationen: 20, 21, 3389, 3306, 4333). Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	AWS Config	Empfehlungen
11.1.1 (b)	s3- account-level-public-access -blöcke-periodisch	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Simple Storage Service (Amazon S3) -Buckets nicht öffentlich zugänglich sind. Diese Regel trägt dazu bei, sensible Daten vor unbefugten Remote-Benutzern zu schützen, indem sie den öffentlichen Zugriff verhindert. Mit dieser Regel können Sie optional die Parameter ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) und restrictPublicBuckets Parameter (Config Default: True) festlegen. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	AWS Config	Empfehlungen
11.1.1 (b)	s3- bucket-public-read-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie nur autorisierten Benutzern, Prozessen und Geräten Zugriff auf Amazon Simple Storage Service (Amazon S3) -Buckets gewähren. Die Verwaltung des Zugriffs sollte mit der Klassifizierung der Daten übereinstimmen.
11.1.1 (b)	s3- bucket-public-write-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie nur autorisierten Benutzern, Prozessen und Geräten Zugriff auf Amazon Simple Storage Service (Amazon S3) -Buckets gewähren. Die Verwaltung des Zugriffs sollte mit der Klassifizierung der Daten übereinstimmen.

Kontroll-ID	AWS Config	Empfehlungen
11.1.1 (b)	s3-fähig bucket-server-side-encryption	Zum Schutz von Daten im Ruhezustand müssen Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon Simple Storage Service (Amazon S3)-Buckets aktiviert ist. Um eventuell vorhandene sensible Daten im Ruhezustand in Amazon-S3-Buckets zu schützen, muss die Verschlüsselung aktiviert sein.
11.1.1 (b)	s-3 default-encryption-kms	Stellen Sie sicher, dass die Verschlüsselung für Ihre Amazon Simple Storage Service (Amazon S3)-Buckets aktiviert ist. Um eventuell vorhandene sensible Daten im Ruhezustand in einem Amazon-S3-Bucket zu schützen, muss die Verschlüsselung aktiviert sein.

Kontroll-ID	AWS Config	Empfehlungen
11.1.1 (b)	sagemaker-endpoint-configuration-kms-key-konfiguriert	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass die Verschlüsselung mit dem AWS Key Management Service (AWS KMS) für Ihren Endpunkt aktiviert ist. SageMaker Da sensible Daten auf dem SageMaker Endgerät gespeichert werden können, sollten Sie die Verschlüsselung im Ruhezustand aktivieren, um diese Daten zu schützen.
11.1.1 (b)	sagemaker-notebook-instance-kms-schlüsselkonfiguriert	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass die Verschlüsselung mit dem AWS Key Management Service (AWS KMS) für Ihr Notebook aktiviert ist. SageMaker Da vertrauliche Daten im SageMaker Notebook gespeichert werden können, sollten Sie die Verschlüsselung im Ruhezustand aktivieren, um diese Daten zu schützen.

Kontroll-ID	AWS Config	Empfehlungen
11.1.1 (b)	sagemaker-notebook-no-direct-Internetzugang	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass SageMaker Amazon-Notebooks keinen direkten Internetzugang zulassen. Indem Sie direkten Internetzugang blockieren, vermeiden Sie, dass unbefugte Benutzer auf sensible Daten zugreifen.
11.1.1 (b)	secretsmanager-using-cmk	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass die Verschlüsselung mit dem AWS Key Management Service (AWS KMS) für AWS Secrets Manager aktiviert ist. Aktivieren Sie die Verschlüsselung von Daten im Ruhezustand, um eventuell vorhandene sensible Daten im Ruhezustand im Secrets Manager zu schützen.

Kontroll-ID	AWS Config	Empfehlungen
11.1.1 (b)	sns-encrypted-kms	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass Ihre Amazon Simple Notification Service (Amazon SNS) -Themen mit dem AWS Key Management Service (AWS KMS) verschlüsselt werden müssen. Um eventuell vorhandene sensible Daten im Ruhezustand in veröffentlichten Nachrichten zu schützen, muss die Verschlüsselung von Daten im Ruhezustand aktiviert sein.
11.1.1 (b)	ssm-document-not-public	Stellen Sie sicher, dass AWS Systems Manager (SSM) -Dokumente nicht öffentlich sind, da dies einen unbeabsichtigten Zugriff auf Ihre SSM-Dokumente ermöglichen kann. Ein öffentliches SSM-Dokument kann Informationen über Ihr Konto, Ihre Ressourcen und internen Prozesse preisgeben.

Kontroll-ID	AWS Config	Empfehlungen
11.1.1 (b)	vpc-sg-open-only-to-authorized-ports	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass gemeinsame Ports für Amazon Elastic Compute Cloud (Amazon EC2) - Sicherheitsgruppen eingeschränkt sind. Wenn der Zugriff auf Ports nicht auf vertrauenswürdige Quellen beschränkt wird, kann dies zu Angriffen auf die Verfügbarkeit, Integrität und Vertraulichkeit von Systemen führen. Durch die Beschränkung des Zugriffs auf Ressourcen innerhalb einer Sicherheitsgruppe aus dem Internet (0.0.0.0/0) kann der Remote-Zugriff auf interne Systeme gesteuert werden.
11.1.3	api-gw-cache-enabled-und-verschlüsselt	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass die Verschlüsselung für den Cache Ihrer API-Gateway-Stufe aktiviert ist. Da für die API-Methode sensible Daten erfasst werden können, sollten Sie die Verschlüsselung von Daten im Ruhezustand aktivieren, um diese Daten zu schützen.

Kontroll-ID	AWS Config	Empfehlungen
11.1.3	cloud-trail-encryption-enabled	Da sensible Daten vorhanden sein können und um Daten im Ruhezustand zu schützen, sollten Sie sicherstellen, dass die Verschlüsselung für Ihre AWS CloudTrail Trails aktiviert ist.
11.1.3	cloudwatch-log-group-encrypted	Um sensible Daten im Speicher zu schützen, stellen Sie sicher, dass die Verschlüsselung für Ihre Amazon CloudWatch Log Groups aktiviert ist.
11.1.3	dynamodb-table-encrypted-kms	Stellen Sie sicher, dass die Verschlüsselung für Ihre Amazon-DynamoDB-Tabellen aktiviert ist. Um eventuell vorhandene sensible Daten im Ruhezustand in diesen Tabellen zu schützen, müssen Sie die Verschlüsselung von Daten im Ruhezustand aktivieren. Standardmäßig werden DynamoDB-Tabellen mit einem AWS eigenen Kundenhauptschlüssel (CMK) verschlüsselt.

Kontroll-ID	AWS Config	Empfehlungen
11.1.3	ebs-snapshot-public-restorable-überprüfen	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass EBS-Snapshots nicht öffentlich wiederherstellbar sind. EBS-Volume-Snapshots können vertrauliche Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.
11.1.3	ec-2 ebs-encryption-by-default	Zum Schutz von Daten im Ruhezustand müssen Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon Elastic Block Store (Amazon EBS)-Volumes aktiviert ist. Da sensible Daten auch im Ruhezustand vorhanden sein können, sollten Sie die Verschlüsselung im Ruhezustand aktivieren, um diese Daten zu schützen.
11.1.3	ec-2 instance-profile-attached	EC2 Instanzprofile übergeben eine IAM-Rolle an eine EC2 Instance. Das Anhängen eines Instance-Profils an Ihre Instances kann bei der Implementierung von geringsten Berechtigungen und der Berechtigungsverwaltung helfen.

Kontroll-ID	AWS Config	Empfehlungen
11.1.3	ecs-task-definition-user-for-host-mode-check	Wenn für eine Aufgabend efinition erhöhte Berechtig ungen gelten, liegt das daran, dass der Kunde diesen Konfigurationen ausdrücklich zugestimmt hat. Diese Kontrolle prüft, ob eine unerwartete Berechtig ungseskalation vorliegt, wenn für eine Aufgabendefinition das Host-Netzwerk aktiviert ist, die Kunden aber keine erhöhten Berechtigungen aktiviert haben.
11.1.3	efs-encrypted-check	Aktivieren Sie die Verschlüs selung für Ihr Amazon Elastic File System (EFS), um eventuell vorhandene sensible Daten sowie Daten im Ruhezustand zu schützen.
11.1.3	elasticsearch-encrypted-at-rest	Da sensible Daten vorhanden sein können und um Daten im Ruhezustand zu schützen, sollten Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon OpenSearch Service (OpenSearch Service) -Domains aktiviert ist.

Kontroll-ID	AWS Config	Empfehlungen
11.1.3	opensearch-encrypted-at-rest	Da sensible Daten vorhanden sein können und um Daten im Ruhezustand zu schützen, sollten Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon OpenSearch Service-Domains aktiviert ist.

Kontroll-ID	AWS Config	Empfehlungen
11.1.3	emr-kerberos-enabled	Die Zugriffsberechtigungen und -autorisierungen können verwaltet und nach den Prinzipien der geringsten Berechtigung und Aufgabent rennung integriert werden, indem Kerberos für Amazon-EMR-Cluster aktiviert wird. In Kerberos werden Services und Benutzer, die sich authentifizieren müssen, als Prinzipale bezeichnet. Prinzipale befinden sich in einem Kerberos-Bereich. Innerhalb dieses Bereichs wird ein Kerberos-Server als Key Distribution Center (KDC) bezeichnet. Über diesen Server können sich Prinzipale authentifizieren. Die Authentifizierung im KDC erfolgt durch die Ausstellu ng von Authentifizierungs tickets. Das KDC unterhält eine Datenbank der Prinzipal e in seinem Bereich mit ihren Passwörtern und anderen administrativen Informationen zu jedem Prinzipal.

Kontroll-ID	AWS Config	Empfehlungen
11.1.3	iam-customer-policy-blocked-kms-Aktionen	AWS Identity and Access Management (IAM) kann Ihnen helfen, die Prinzipien der geringsten Rechte und der Aufgabentrennung in Zugriffsberechtigungen und Autorisierungen zu integrier en und so zu verhindern, dass Richtlinien blockierte Aktionen für alle AWS Schlüssel des Key Management Service enthalten. Wenn Benutzer mehr Rechte haben, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und Aufgabentrennung verstoßen . Mit dieser Regel können Sie den Parameter festlegen. blockedActionsPatterns (Wert „AWS Bewährte grundlegende Sicherheitsmethoden“: kms: Entschlüsseln, kms:ReEnc ryptFrom). Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprech en.

Kontroll-ID	AWS Config	Empfehlungen
11.1.3	iam-group-has-users-überprüfen	AWS Identity and Access Management (IAM) kann Ihnen helfen, die Prinzipien der geringsten Rechte und der Aufgabentrennung mit Zugriffsberechtigungen und Autorisierungen zu integrieren, indem sichergestellt wird, dass IAM-Gruppen mindestens einen Benutzer haben. Die Einteilung von Benutzern in Gruppen auf der Grundlage der ihnen zugewiesenen Berechtigungen oder ihrer Funktion ist eine Möglichkeit, das Prinzip der geringsten Berechtigung zu implementieren.

Kontroll-ID	AWS Config	Empfehlungen
11.1.3	iam-inline-policy-blocked-kms-Aktionen	Stellen Sie sicher, dass ein Benutzer, eine IAM-Rolle oder eine IAM-Grupp e (AWS Identity and Access Management) nicht über eine Inline-Richtlinie verfügt, die blockierte Aktionen für alle AWS Schlüssel des Key Management Service zulässt. AWS empfiehlt, verwaltete Richtlinien anstelle von Inline-Richtlinien zu verwenden . Verwaltete Richtlinien ermöglichen Wiederver wendbarkeit, Versionsv erwaltung, Rollback und Delegierung der Berechtig ungsverwaltung. Mit dieser Regel können Sie den blockedActionsPatterns Parameter festlegen. (Wert „AWS Bewährte grundlege nde Sicherheitsmethoden“: kms: Decrypt, kms:ReEnc ryptFrom). Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprech en.

Kontroll-ID	AWS Config	Empfehlungen
11.1.3	iam-no-inline-policy-überprüfen	Stellen Sie sicher, dass ein Benutzer, eine IAM-Rolle oder eine IAM-Gruppe (AWS Identity and Access Management) nicht über eine Inline-Richtlinie zur Zugriffskontrolle auf Systeme und Ressourcen verfügt. AWS empfiehlt, verwaltete Richtlinien anstelle von Inline-Richtlinien zu verwenden . Verwaltete Richtlinien ermöglichen Wiederverwendbarkeit, Versionsverwaltung, Rollback und Delegierung der Berechtigungsverwaltung.

Kontroll-ID	AWS Config	Empfehlungen
11.1.3	iam-password-policy	Die Identitäten und Anmeldein formationen werden auf der Grundlage einer organisat orischen IAM-Passwortrichtl inie ausgestellt, verwaltet und verifiziert. Sie erfüllen oder übertreffen die Anforderungen von NIST SP 800-63 und dem Standard „Best Practices“ von AWS Foundational Security für die Passwortstärke. Mit dieser Regel können Sie optional RequireUppercaseCharacters (Wert für AWS grundlege nde Sicherheitsbewährte Verfahren: wahr), RequireLo wercaseCharacters (Wert für bewährte Methoden für AWS grundlegende Sicherheit: wahr), RequireSymbols (Wert für bewährte Methoden für AWS grundlegende Sicherhei t: wahr), RequireNumbers (Wert für bewährte Methoden für AWS grundlegende Sicherheit: wahr), MinimumPa sswordLength (Wert für bewährte Methoden für AWS grundlegende Sicherheit: 14), PasswordReusePreve ntion (Wert für bewährte Methoden für AWS grundlege nde Sicherheit: 24) und MaxPasswordAge (Wert

Kontroll-ID	AWS Config	Empfehlungen
		für bewährte Methoden für AWS grundlegende Sicherhei t: 90) für Ihr IAM festlegen Kennwortrichtlinie. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisat ion entsprechen.
11.1.3	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) kann Ihnen dabei helfen, die Prinzipien der geringsten Rechte und der Aufgabent rennung in Zugriffsberechtigu ngen und Autorisierungen zu integrieren und so zu verhindern, dass Richtlinien „Effect“: „Allow“ mit „Action“: „*“ anstelle von „Resource“: „*“ enthalten. Wenn Benutzern mehr Rechte eingeräumt werden, als für die Ausführun g einer Aufgabe erforderl ich sind, kann dies gegen das Prinzip der geringste n Berechtigung und der Aufgabentrennung verstoßen.

Kontroll-ID	AWS Config	Empfehlungen
11.1.3	iam-policy-no-statements-with-full-access	Stellen Sie sicher, dass IAM-Aktionen nur auf die benötigte n Aktionen beschränkt sind. Wenn Benutzern mehr Rechte eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und der Aufgabentrennung verstoßen.
11.1.3	iam-user-group-membership-überprüfen	AWS Identity and Access Management (IAM) kann Ihnen helfen, Zugriffsb erechtigungen und Autorisie rungen einzuschränken, indem sichergestellt wird, dass Benutzer Mitglieder mindesten s einer Gruppe sind. Wenn Benutzern mehr Berechtig ungen eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtig ung und Aufgabentrennung verstoßen.

Kontroll-ID	AWS Config	Empfehlungen
11.1.3	iam-user-mfa-enabled	Aktivieren Sie diese Regel, um den Zugriff auf Ressourcen in der AWS Cloud einzuschränken. Diese Regel sorgt dafür, dass die Multi-Faktor-Authentifizierung (MFA) für alle Benutzer aktiviert ist. MFA sorgt für eine weitere Schutzebene zusätzlich zu den Anmeldeinformationen. Reduzieren Sie Fälle von kompromittierten Konten, indem Sie MFA für Benutzer vorschreiben.
11.1.3	iam-user-no-policies-überprüfen	Diese Regel stellt sicher, dass AWS Identity and Access Management (IAM) -Richtlinien nur Gruppen oder Rollen zugewiesen werden, um den Zugriff auf Systeme und Ressourcen zu kontrollieren. Die Zuweisung von Berechtigungen auf Gruppen- oder Rollenebene trägt dazu bei, die Wahrscheinlichkeit zu verringern, dass eine Identität übermäßige Berechtigungen erhält oder beibehält.

Kontroll-ID	AWS Config	Empfehlungen
11.1.3	iam-user-unused-credentials-überprüfen	AWS Identity and Access Management (IAM) kann Ihnen bei Zugriffsberechtigungen und Autorisierungen helfen, indem es nach IAM-Passwörtern und Zugriffsschlüsseln sucht, die für einen bestimmten Zeitraum nicht verwendet wurden. Wenn ungenutzte Anmeldeinformationen identifiziert werden, müssen Sie sie deaktivieren und/oder entfernen, da dies gegen das Prinzip der geringsten Berechtigung verstoßen könnte. Für diese Regel müssen Sie einen Wert für das maxCredentialUsage Alter festlegen (Standardkonfiguration: 90). Der tatsächliche Wert muss den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	AWS Config	Empfehlungen
11.1.3	mfa-enabled-for-iam-Konsolenzugriff	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass MFA für alle AWS Identity and Access Management (IAM) -Benutzer aktiviert ist, die über ein Konsolenkennwort verfügen. MFA sorgt für eine weitere Schutzebene zusätzlich zu den Anmeldeinformationen. Indem Sie MFA für Benutzer vorschreiben, können Sie Fälle kompromittierter Konten reduzieren und verhindern, dass unbefugte Benutzer auf vertrauliche Daten zugreifen.
11.1.3	rds-snapshot-encrypted	Stellen Sie sicher, dass die Verschlüsselung für Ihre Amazon Relational Database Service (Amazon RDS)-Snapshots aktiviert ist. Da sensible Daten auch im Ruhezustand vorhanden sein können, sollten Sie die Verschlüsselung im Ruhezustand aktivieren, um diese Daten zu schützen.

Kontroll-ID	AWS Config	Empfehlungen
11.1.3	rds-storage-encrypted	Zum Schutz von Daten im Ruhezustand müssen Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon Relational Database Service (Amazon RDS)-Instances aktiviert ist. Um eventuell vorhandene sensible Daten im Ruhezustand in Amazon-RDS-Instanc es zu schützen, muss die Verschlüsselung von Daten im Ruhezustand aktiviert sein.

Kontroll-ID	AWS Config	Empfehlungen
11.1.3	redshift-cluster-configuration-check	Um Daten im Ruhezustand zu schützen, muss die Verschlüsselung für Ihre Amazon-Redshift-Cluster aktiviert sein. Sie müssen auch sicherstellen, dass die erforderlichen Konfigurationen auf Amazon-Redshift-Clustern bereitgestellt werden. Die Prüfungsprotokollierung muss aktiviert sein, um Informationen zu Verbindungen und Benutzeraktivitäten in der Datenbank bereitzustellen. Diese Regel erfordert, dass ein Wert für clusterDbEncrypted (Config Default: TRUE) und LoggingEnabled (Config Default: TRUE) gesetzt ist. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	AWS Config	Empfehlungen
11.1.3	redshift-cluster-kms-enabled	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass die Verschlüsselung mit AWS Key Management Service (AWS KMS) für Ihren Amazon Redshift Redshift-Cluster aktiviert ist. Um eventuell vorhandene sensible Daten im Ruhezustand in Redshift-Clustern zu schützen, muss die Verschlüsselung von Daten im Ruhezustand aktiviert sein.
11.1.3	root-account-hardware-mfa-aktiviert	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Hardware-MFA für den Root-Benutzer aktiviert ist. Der Stammbenutzer ist der AWS-Konto-Benutzer mit den meisten Berechtigungen. MFA sorgt für eine weitere Schutzebene zusätzlich zu den Anmeldeinformationen. Indem Sie MFA für den Root-Benutzer vorschreiben, können Sie die Anzahl AWS-Konten kompromittierter Benutzer reduzieren.

Kontroll-ID	AWS Config	Empfehlungen
11.1.3	root-account-mfa-enabled	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass MFA für den Root-Benutzer aktiviert ist. Der Stammbenutzer ist der AWS-Konto-Benutzer mit den meisten Berechtigungen. MFA sorgt für eine weitere Schutzebene zusätzlich zu den Anmeldeinformationen. Indem Sie MFA für den Root-Benutzer vorschreiben, können Sie die Anzahl AWS-Konten kompromittierter Benutzer reduzieren.
11.1.3	s3-fähig bucket-server-side-encryption	Zum Schutz von Daten im Ruhezustand müssen Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon Simple Storage Service (Amazon S3)-Buckets aktiviert ist. Um eventuell vorhandene sensible Daten im Ruhezustand in Amazon-S3-Buckets zu schützen, muss die Verschlüsselung aktiviert sein.

Kontroll-ID	AWS Config	Empfehlungen
11.1.3	s-3 default-encryption-kms	Stellen Sie sicher, dass die Verschlüsselung für Ihre Amazon Simple Storage Service (Amazon S3)-Buckets aktiviert ist. Um eventuell vorhandene sensible Daten im Ruhezustand in einem Amazon-S3-Bucket zu schützen, muss die Verschlüsselung aktiviert sein.
11.1.3	sagemaker-endpoint-configuration-kms-schlüsselkonfiguriert	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass die Verschlüsselung mit dem AWS Key Management Service (AWS KMS) für Ihren Endpunkt aktiviert ist. SageMaker Da sensible Daten auf dem SageMaker Endgerät gespeichert werden können, sollten Sie die Verschlüsselung im Ruhezustand aktivieren, um diese Daten zu schützen.

Kontroll-ID	AWS Config	Empfehlungen
11.1.3	sagemaker-notebook-instance-kms-schlüsselkonfiguriert	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass die Verschlüsselung mit dem AWS Key Management Service (AWS KMS) für Ihr Notebook aktiviert ist. SageMaker Da vertrauliche Daten im SageMaker Notebook gespeichert werden können, sollten Sie die Verschlüsselung im Ruhezustand aktivieren, um diese Daten zu schützen.
11.1.3	secretsmanager-using-cmk	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass die Verschlüsselung mit dem AWS Key Management Service (AWS KMS) für AWS Secrets Manager aktiviert ist. Aktivieren Sie die Verschlüsselung von Daten im Ruhezustand, um eventuell vorhandene sensible Daten im Ruhezustand im Secrets Manager zu schützen.

Kontroll-ID	AWS Config	Empfehlungen
11.1.3	sns-encrypted-kms	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass Ihre Amazon Simple Notification Service (Amazon SNS) -Themen mit dem AWS Key Management Service (AWS KMS) verschlüsselt werden müssen. Um eventuell vorhandene sensible Daten im Ruhezustand in veröffentlichten Nachrichten zu schützen, muss die Verschlüsselung von Daten im Ruhezustand aktiviert sein.
11.2.1	alb-waf-enabled	Stellen Sie sicher, dass AWS WAF auf Elastic Load Balancers (ELB) aktiviert ist, um Webanwendungen zu schützen. Eine WAF trägt zum Schutz Ihrer Webanwendungen oder APIs vor gängigen Web-Exploits bei. Diese Web-Exploits können sich auf die Verfügbarkeit auswirken, die Sicherheit gefährden oder übermäßige Ressourcen in Ihrer Umgebung verbrauchen.

Kontroll-ID	AWS Config	Empfehlungen
11.2.2	autoscaling-launch-config-public-ip-deaktiviert	Wenn Sie Ihre Netzwerkschnittstellen mit einer öffentlichen IP-Adresse konfigurieren, sind die diesen Netzwerkschnittstellen zugehörigen Ressourcen über das Internet erreichbar. EC2 Ressourcen sollten nicht öffentlich zugänglich sein, da dies einen unbeabsichtigten Zugriff auf Ihre Anwendungen oder Server ermöglichen kann.
11.2.2	dms-replication-not-public	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass auf DMS-Replikationsinstanzen nicht öffentlich zugegriffen werden kann. DMS-Replikations-Instances können vertrauliche Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.
11.2.2	ebs-snapshot-public-restorable-überprüfen	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass EBS-Snapshots nicht öffentlich wiederherstellbar sind. EBS-Volume-Snapshots können vertrauliche Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	AWS Config	Empfehlungen
11.2.2	ec-2 instance-no-public-ip	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon Elastic Compute Cloud (Amazon EC2) -Instances nicht öffentlich zugänglich sind. EC2 Amazon-Instances können vertrauliche Informati onen enthalten, und für solche Konten ist eine Zugriffsk ontrolle erforderlich.
11.2.2	elasticsearch-in-vpc-only	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass sich Amazon OpenSearch OpenSearch Service (Service) -Domains innerhalb einer Amazon Virtual Private Cloud (Amazon VPC) befinden. Eine OpenSearch Service-D omain innerhalb einer Amazon VPC ermöglicht die sichere Kommunikation zwischen OpenSearch Service und anderen Services innerhalb der Amazon VPC, ohne dass ein Internet-Gateway, ein NAT-Gerät oder eine VPN-Verbindung erforderlich ist.

Kontroll-ID	AWS Config	Empfehlungen
11.2.2	opensearch-in-vpc-only	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass sich Amazon OpenSearch Service-Domains innerhalb einer Amazon Virtual Private Cloud (Amazon VPC) befinden. Eine Amazon OpenSearch Service-Domain innerhalb einer Amazon VPC ermöglich t die sichere Kommunika tion zwischen Amazon OpenSearch Service und anderen Services innerhalb der Amazon VPC, ohne dass ein Internet-Gateway, ein NAT-Gerät oder eine VPN-Verbindung erforderlich ist.
11.2.2	emr-master-no-public-ip	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon EMR-Cluster-Masterknoten nicht öffentlich zugänglich sind. Amazon-EMR-Cluster-Hauptknoten können vertrauli che Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	AWS Config	Empfehlungen
11.2.2	guardduty-enabled-centralized	Amazon GuardDuty kann mithilfe von Threat Intellige nce Feeds helfen, potenzielle Cybersicherheitsereignisse zu überwachen und zu erkennen. Dazu gehören Listen mit bösartigen IPs und maschinel len Lernmethoden zur Identifiz ierung unerwarteter, nicht autorisierter und bösartige r Aktivitäten in Ihrer AWS Cloud-Umgebung.
11.2.2	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) Security Groups können bei der Verwaltung des Netzwerkz ugriffs helfen, indem sie eine statusbehaftete Filterung des ein- und ausgehend en Netzwerkverkehrs zu Ressourcen bereitstellen. AWS Wenn Sie eingehenden (oder entfernten) Datenverk ehr von 0.0.0.0/0 bis Port 22 auf Ihren Ressourcen nicht zulassen, können Sie den Remote-Zugriff einschränken.

Kontroll-ID	AWS Config	Empfehlungen
11.2.2	ec-2 instances-in-vpc	Stellen Sie Amazon Elastic Compute Cloud (Amazon EC2) -Instances innerhalb einer Amazon Virtual Private Cloud (Amazon VPC) bereit, um eine sichere Kommunika tion zwischen einer Instance und anderen Services innerhalb der Amazon VPC zu ermöglichen, ohne dass ein Internet-Gateway, ein NAT-Gerät oder eine VPN-Verbi ndung erforderlich ist. Der gesamte Datenverkehr bleibt sicher in der AWS Cloud. Domains, die sich innerhalb einer VPC befinden, verfügen aufgrund ihrer logischen Isolierung im Vergleich zu Domains mit öffentlic hen Endpunkten über eine zusätzliche Sicherheitsebene. Weisen Sie EC2 Amazon-In stances einer Amazon-VPC zu, um den Zugriff ordnungsg emäß zu verwalten.

Kontroll-ID	AWS Config	Empfehlungen
11.2.2	lambda-function-public-access-verboten	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass AWS Lambda-Funktionen nicht öffentlich zugänglich sind. Der öffentliche Zugriff kann möglicherweise die Verfügbarkeit von Ressourcen beeinträchtigen.

Kontroll-ID	AWS Config	Empfehlungen
11.2.2	lambda-inside-vpc	Stellen Sie AWS Lambda-Funktionen in einer Amazon Virtual Private Cloud (Amazon VPC) bereit, um eine sichere Kommunikation zwischen einer Funktion und anderen Diensten innerhalb der Amazon VPC zu gewährleisten. Bei dieser Konfiguration sind kein Internet-Gateway, kein NAT-Gerät und keine VPN-Verbindung erforderlich. Der gesamte Datenverkehr bleibt sicher in der Cloud. AWS Domains, die sich innerhalb einer VPC befinden, verfügen aufgrund ihrer logischen Isolierung im Vergleich zu Domains mit öffentlichen Endpunkten über eine zusätzliche Sicherheitsebene. Um den Zugriff ordnungsgemäß zu verwalten, sollten AWS Lambda-Funktionen einer VPC zugewiesen werden.

Kontroll-ID	AWS Config	Empfehlungen
11.2.2	rds-instance-public-access-überprüfen	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Relational Database Service (Amazon RDS) -Instances nicht öffentlich sind. Amazon-RDS-Datenbank-Instances können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.
11.2.2	rds-snapshots-public-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Relational Database Service (Amazon RDS) -Instances nicht öffentlich sind. Amazon-RDS-Datenbank-Instances können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	AWS Config	Empfehlungen
11.2.2	redshift-cluster-public-access-überprüfen	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Redshift Redshift-Cluster nicht öffentlich sind. Amazon-Redshift-Cluster können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.
11.2.2	restricted-common-ports	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass gemeinsame Ports für Amazon Elastic Compute Cloud (Amazon EC2) - Sicherheitsgruppen eingeschränkt sind. Wenn der Zugriff auf Ports nicht auf vertrauenswürdige Quellen beschränkt wird, kann dies zu Angriffen auf die Verfügbarkeit, Integrität und Vertraulichkeit von Systemen führen. Mit dieser Regel können Sie optional die Parameter blockedPort1–blockedPort5 festlegen (Standardkonfigurationen: 20, 21, 3389, 3306, 4333). Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	AWS Config	Empfehlungen
11.2.2	s3-Blöcke-periodisch account-level-public-access	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Simple Storage Service (Amazon S3) -Buckets nicht öffentlich zugänglich sind. Diese Regel trägt dazu bei, sensible Daten vor unbefugten Remote-Benutzern zu schützen, indem sie den öffentlichen Zugriff verhindert. Mit dieser Regel können Sie optional die Parameter ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) und restrictPublicBuckets Parameter (Config Default: True) festlegen. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	AWS Config	Empfehlungen
11.2.2	s-3 bucket-public-read-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie nur autorisierten Benutzern, Prozessen und Geräten Zugriff auf Amazon Simple Storage Service (Amazon S3) -Buckets gewähren. Die Verwaltung des Zugriffs sollte mit der Klassifizierung der Daten übereinstimmen.
11.2.2	s-3 bucket-public-write-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie nur autorisierten Benutzern, Prozessen und Geräten Zugriff auf Amazon Simple Storage Service (Amazon S3) -Buckets gewähren. Die Verwaltung des Zugriffs sollte mit der Klassifizierung der Daten übereinstimmen.
11.2.2	sagemaker-notebook-no-direct-Internetzugang	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass SageMaker Amazon-Notebooks keinen direkten Internetzugang zulassen. Indem Sie direkten Internetzugang blockieren, vermeiden Sie, dass unbefugte Benutzer auf sensible Daten zugreifen.

Kontroll-ID	AWS Config	Empfehlungen
11.2.2	subnet-auto-assign-public-ip-deaktiviert	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon Virtual Private Cloud (VPC) -Subnetzen nicht automatis ch eine öffentliche IP-Adress e zugewiesen wird. Amazon Elastic Compute Cloud (EC2) -Instances, die in Subnetzen gestartet werden, in denen dieses Attribut aktiviert ist, haben ihrer primären Netzwerkschnittste lle eine öffentliche IP-Adresse zugewiesen.
11.2.2	vpc-default-security-group-geschlossen	Sicherheitsgruppen von Amazon Elastic Compute Cloud (Amazon EC2) können bei der Verwaltung des Netzwerkzugriffs helfen, indem sie eine statusbeh aftete Filterung des ein- und ausgehenden Netzwerkv erkehrs zu Ressourcen bereitstellen. AWS Die Beschränkung des gesamten Datenverkehrs auf die Standardsicherheitsgruppe hilft dabei, den Fernzugriff auf Ihre Ressourcen einzuschr änken. AWS

Kontroll-ID	AWS Config	Empfehlungen
11.2.2	vpc-sg-open-only-to-authorized-ports	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass gemeinsame Ports für Amazon Elastic Compute Cloud (Amazon EC2) - Sicherheitsgruppen eingeschränkt sind. Wenn der Zugriff auf Ports nicht auf vertrauenswürdige Quellen beschränkt wird, kann dies zu Angriffen auf die Verfügbarkeit, Integrität und Vertraulichkeit von Systemen führen. Durch die Beschränkung des Zugriffs auf Ressourcen innerhalb einer Sicherheitsgruppe aus dem Internet (0.0.0.0/0) kann der Remote-Zugriff auf interne Systeme gesteuert werden.
11.2.4	autoscaling-launch-config-public-ip-deaktiviert	Wenn Sie Ihre Netzwerkschnittstellen mit einer öffentlichen IP-Adresse konfigurieren, sind die diesen Netzwerkschnittstellen zugehörigen Ressourcen über das Internet erreichbar. EC2 Ressourcen sollten nicht öffentlich zugänglich sein, da dies einen unbeabsichtigten Zugriff auf Ihre Anwendungen oder Server ermöglichen kann.

Kontroll-ID	AWS Config	Empfehlungen
11.2.4	dms-replication-not-public	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass auf DMS-Replikationsinstanzen nicht öffentlich zugegriffen werden kann. DMS-Replikations-I nstances können vertrauli che Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.
11.2.4	ebs-snapshot-public-restora ble-überprüfen	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass EBS-Snaps hots nicht öffentlich wiederher stellbar sind. EBS-Volume-Snapshots können vertrauli che Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.
11.2.4	ec-2 instance-no-public-ip	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon Elastic Compute Cloud (Amazon EC2) -Instances nicht öffentlich zugänglich sind. EC2 Amazon-Instances können vertrauliche Informati onen enthalten, und für solche Konten ist eine Zugriffsk ontrolle erforderlich.

Kontroll-ID	AWS Config	Empfehlungen
11.2.4	emr-master-no-public-ip	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon EMR-Cluster-Masterknoten nicht öffentlich zugänglich sind. Amazon-EMR-Cluster-Hauptknoten können vertrauliche Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.
11.2.4	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) Security Groups können bei der Verwaltung des Netzwerkzugriffs helfen, indem sie eine statusbehaftete Filterung des ein- und ausgehenden Netzwerkverkehrs zu Ressourcen bereitstellen. AWS Wenn Sie eingehenden (oder entfernten) Datenverkehr von 0.0.0.0/0 bis Port 22 auf Ihren Ressourcen nicht zulassen, können Sie den Remote-Zugriff einschränken.

Kontroll-ID	AWS Config	Empfehlungen
11.2.4	ec-2 instances-in-vpc	Stellen Sie Amazon Elastic Compute Cloud (Amazon EC2) -Instances innerhalb einer Amazon Virtual Private Cloud (Amazon VPC) bereit, um eine sichere Kommunika tion zwischen einer Instance und anderen Services innerhalb der Amazon VPC zu ermöglichen, ohne dass ein Internet-Gateway, ein NAT-Gerät oder eine VPN-Verbi ndung erforderlich ist. Der gesamte Datenverkehr bleibt sicher in der AWS Cloud. Domains, die sich innerhalb einer VPC befinden, verfügen aufgrund ihrer logischen Isolierung im Vergleich zu Domains mit öffentlic hen Endpunkten über eine zusätzliche Sicherheitsebene. Weisen Sie EC2 Amazon-In stances einer Amazon-VPC zu, um den Zugriff ordnungsg emäß zu verwalten.

Kontroll-ID	AWS Config	Empfehlungen
11.2.4	guardduty-enabled-centralized	Amazon GuardDuty kann mithilfe von Threat Intellige nce Feeds helfen, potenzielle Cybersicherheitsereignisse zu überwachen und zu erkennen. Dazu gehören Listen mit bösartigen IPs und maschinel len Lernmethoden zur Identifiz ierung unerwarteter, nicht autorisierter und bösartige r Aktivitäten in Ihrer AWS Cloud-Umgebung.
11.2.4	api-gw-associated-with-WAF	AWS Mit WAF können Sie eine Reihe von Regeln (als Web Access Control List (Web ACL) bezeichnet) konfiguri eren, die Webanfragen auf der Grundlage von anpassbar en Websicherheitsregeln und -bedingungen, die Sie definieren, zulassen, blockiere n oder zählen. Stellen Sie sicher, dass Ihre Amazon-API-Gateway-Stufe mit einer WAF-Web-ACL verknüpft ist, um sie vor böswilligen Angriffen zu schützen.

Kontroll-ID	AWS Config	Empfehlungen
11.2.4	lambda-function-public-access-verboten	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass AWS Lambda-Funktionen nicht öffentlich zugänglich sind. Der öffentliche Zugriff kann möglicherweise die Verfügbarkeit von Ressourcen beeinträchtigen.

Kontroll-ID	AWS Config	Empfehlungen
11.2.4	lambda-inside-vpc	Stellen Sie AWS Lambda-Funktionen in einer Amazon Virtual Private Cloud (Amazon VPC) bereit, um eine sichere Kommunikation zwischen einer Funktion und anderen Diensten innerhalb der Amazon VPC zu gewährleisten. Bei dieser Konfiguration sind kein Internet-Gateway, kein NAT-Gerät und keine VPN-Verbindung erforderlich. Der gesamte Datenverkehr bleibt sicher in der Cloud. AWS Domains, die sich innerhalb einer VPC befinden, verfügen aufgrund ihrer logischen Isolierung im Vergleich zu Domains mit öffentlichen Endpunkten über eine zusätzliche Sicherheitsebene. Um den Zugriff ordnungsgemäß zu verwalten, sollten AWS Lambda-Funktionen einer VPC zugewiesen werden.

Kontroll-ID	AWS Config	Empfehlungen
11.2.4	rds-instance-public-access-überprüfen	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Relational Database Service (Amazon RDS) -Instances nicht öffentlich sind. Amazon-RDS-Datenbank-Instances können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.
11.2.4	rds-snapshots-public-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Relational Database Service (Amazon RDS) -Instances nicht öffentlich sind. Amazon-RDS-Datenbank-Instances können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	AWS Config	Empfehlungen
11.2.4	redshift-cluster-public-access-überprüfen	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Redshift Redshift-Cluster nicht öffentlich sind. Amazon-Redshift-Cluster können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.
11.2.4	restricted-common-ports	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass gemeinsame Ports für Amazon Elastic Compute Cloud (Amazon EC2) - Sicherheitsgruppen eingeschränkt sind. Wenn der Zugriff auf Ports nicht auf vertrauenswürdige Quellen beschränkt wird, kann dies zu Angriffen auf die Verfügbarkeit, Integrität und Vertraulichkeit von Systemen führen. Mit dieser Regel können Sie optional die Parameter blockedPort1–blockedPort5 festlegen (Standardkonfigurationen: 20, 21, 3389, 3306, 4333). Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	AWS Config	Empfehlungen
11.2.4	s3-Blöcke-periodisch account-level-public-access	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Simple Storage Service (Amazon S3) -Buckets nicht öffentlich zugänglich sind. Diese Regel trägt dazu bei, sensible Daten vor unbefugten Remote-Benutzern zu schützen, indem sie den öffentlichen Zugriff verhindert. Mit dieser Regel können Sie optional die Parameter ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) und restrictPublicBuckets Parameter (Config Default: True) festlegen. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	AWS Config	Empfehlungen
11.2.4	s-3 bucket-public-write-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie nur autorisierten Benutzern, Prozessen und Geräten Zugriff auf Amazon Simple Storage Service (Amazon S3) -Buckets gewähren. Die Verwaltung des Zugriffs sollte mit der Klassifizierung der Daten übereinstimmen.
11.2.4	sagemaker-notebook-no-direct-Internetzugang	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass SageMaker Amazon-Notebooks keinen direkten Internetzugang zulassen. Indem Sie direkten Internetzugang blockieren, vermeiden Sie, dass unbefugte Benutzer auf sensible Daten zugreifen.

Kontroll-ID	AWS Config	Empfehlungen
11.2.4	subnet-auto-assign-public-ip-deaktiviert	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon Virtual Private Cloud (VPC) -Subnetzen nicht automatis ch eine öffentliche IP-Adress e zugewiesen wird. Amazon Elastic Compute Cloud (EC2) -Instances, die in Subnetzen gestartet werden, in denen dieses Attribut aktiviert ist, haben ihrer primären Netzwerkschnittste lle eine öffentliche IP-Adresse zugewiesen.
11.2.4	vpc-default-security-group-geschlossen	Sicherheitsgruppen von Amazon Elastic Compute Cloud (Amazon EC2) können bei der Verwaltung des Netzwerkzugriffs helfen, indem sie eine statusbeh aftete Filterung des ein- und ausgehenden Netzwerkv erkehrs zu Ressourcen bereitstellen. AWS Die Beschränkung des gesamten Datenverkehrs auf die Standardsicherheitsgruppe hilft dabei, den Fernzugriff auf Ihre Ressourcen einzuschr änken. AWS

Kontroll-ID	AWS Config	Empfehlungen
11.2.4	vpc-sg-open-only-to-authorized-ports	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass gemeinsame Ports für Amazon Elastic Compute Cloud (Amazon EC2) - Sicherheitsgruppen eingeschränkt sind. Wenn der Zugriff auf Ports nicht auf vertrauenswürdige Quellen beschränkt wird, kann dies zu Angriffen auf die Verfügbarkeit, Integrität und Vertraulichkeit von Systemen führen. Durch die Beschränkung des Zugriffs auf Ressourcen innerhalb einer Sicherheitsgruppe aus dem Internet (0.0.0.0/0) kann der Remote-Zugriff auf interne Systeme gesteuert werden.

Kontroll-ID	AWS Config	Empfehlungen
11.3.1	ec2-imdsv2-check	Stellen Sie sicher, dass die Methode Instance Metadata Service Version 2 (IMDSv2) aktiviert ist, um den Zugriff auf und die Kontrolle der Amazon Elastic Compute Cloud (Amazon EC2) -Instance-Metadaten zu schützen. Die IMDSv2 Methode verwendet sitzungsbasierte Kontrolle n. Mit können Kontrollen implementiert werden IMDSv2, um Änderungen an Instanzme tadaten einzuschränken.
11.3.5	cloudtrail-enabled	AWS CloudTrail kann durch die Aufzeichnung von Aktionen und API-Aufrufen in der AWS Management Console bei der Nichtabst reitbarkeit helfen. Sie können die Benutzer und die Benutzer AWS-Konten , die einen AWS Dienst aufgerufen haben, die Quell-IP-Adresse, über die die Aufrufe generiert wurden, und den Zeitpunkt der Anrufe identifizieren. Einzelheiten zu den erfassten Daten finden Sie in den AWS CloudTrail Datensatzinhalten.

Kontroll-ID	AWS Config	Empfehlungen
11.3.5	guardduty-enabled-centralized	Amazon GuardDuty kann mithilfe von Threat Intellige nce Feeds helfen, potenzielle Cybersicherheitsereignisse zu überwachen und zu erkennen. Dazu gehören Listen mit bösartigen IPs und maschinel len Lernmethoden zur Identifiz ierung unerwarteter, nicht autorisierter und bösartige r Aktivitäten in Ihrer AWS Cloud-Umgebung.

Kontroll-ID	AWS Config	Empfehlungen
11.3.5	multi-region-cloudtrail-enabled	AWS CloudTrail zeichnet Aktionen und API-Aufrufe der AWS Management Console auf. Sie können feststellen, welche Benutzer und Konten angerufen wurden AWS, von welcher Quell-IP-Adresse aus die Anrufe getätigt wurden und wann die Anrufe erfolgten . CloudTrail übermittelt Protokolldateien aus allen AWS Regionen an Ihren S3-Bucket, wenn MULTI_REGION_CLOUD_TRAIL_ENABLED aktiviert ist. Außerdem wird beim AWS Start einer neuen Region derselbe Trail in der neuen Region erstellt. CloudTrail Dadurch erhalten Sie automatisch Protokoll dateien mit API-Aktivitäten für die neue Region.

Kontroll-ID	AWS Config	Empfehlungen
11.3.5	securityhub-enabled	AWS Security Hub hilft bei der Überwachung von unbefugte m Personal, Verbindungen, Geräten und Software. AWS Security Hub aggregiert, organisiert und priorisiert die Sicherheitswarnungen oder Ergebnisse mehrerer Dienste. AWS Einige dieser Dienste sind Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer und AWS Firewall Manager sowie AWS Partnerlösungen.
11.4.2	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) Security Groups können bei der Verwaltung des Netzwerkz ugriffs helfen, indem sie eine statusbehaftete Filterung des ein- und ausgehend en Netzwerkverkehrs zu Ressourcen bereitstellen. AWS Wenn Sie eingehenden (oder entfernten) Datenverk ehr von 0.0.0.0/0 bis Port 22 auf Ihren Ressourcen nicht zulassen, können Sie den Remote-Zugriff einschränken.

Kontroll-ID	AWS Config	Empfehlungen
11.4.2	restricted-common-ports	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass gemeinsame Ports für Amazon Elastic Compute Cloud (Amazon EC2) - Sicherheitsgruppen eingeschränkt sind. Wenn der Zugriff auf Ports nicht auf vertrauenswürdige Quellen beschränkt wird, kann dies zu Angriffen auf die Verfügbarkeit, Integrität und Vertraulichkeit von Systemen führen. Mit dieser Regel können Sie optional die Parameter blockedPort1–blockedPort5 festlegen (Standardkonfigurationen: 20, 21, 3389, 3306, 4333). Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	AWS Config	Empfehlungen
11.4.2	vpc-default-security-group-geschlossen	Sicherheitsgruppen von Amazon Elastic Compute Cloud (Amazon EC2) können bei der Verwaltung des Netzwerkzugriffs helfen, indem sie eine statusbeh aftete Filterung des ein- und ausgehenden Netzwerkv erkehrs zu Ressourcen bereitstellen. AWS Die Beschränkung des gesamten Datenverkehrs auf die Standardsicherheitsgruppe hilft dabei, den Fernzugriff auf Ihre Ressourcen einzuschr änken. AWS

Kontroll-ID	AWS Config	Empfehlungen
11.4.2	vpc-sg-open-only-to-authorized-ports	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass gemeinsame Ports für Amazon Elastic Compute Cloud (Amazon EC2) - Sicherheitsgruppen eingeschränkt sind. Wenn der Zugriff auf Ports nicht auf vertrauenswürdige Quellen beschränkt wird, kann dies zu Angriffen auf die Verfügbarkeit, Integrität und Vertraulichkeit von Systemen führen. Durch die Beschränkung des Zugriffs auf Ressourcen innerhalb einer Sicherheitsgruppe aus dem Internet (0.0.0.0/0) kann der Remote-Zugriff auf interne Systeme gesteuert werden.

Kontroll-ID	AWS Config	Empfehlungen
11.5.2	securityhub-enabled	AWS Security Hub hilft bei der Überwachung von unbefugte m Personal, Verbindungen, Geräten und Software. AWS Security Hub aggregiert, organisiert und priorisiert die Sicherheitswarnungen oder Ergebnisse mehrerer Dienste. AWS Einige dieser Dienste sind Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer und AWS Firewall Manager sowie AWS Partnerlösungen.
12.1.1	cloudtrail-enabled	AWS CloudTrail kann bei der Nichtabstreitbarkeit helfen, indem Aktionen und API-Aufrufe der AWS Managemen t Console aufgezeichnet werden. Sie können die Benutzer und die Benutzer AWS-Konten , die einen AWS Dienst aufgerufen haben, die Quell-IP-Adresse, über die die Aufrufe generiert wurden, und den Zeitpunkt der Anrufe identifizieren. Einzelheiten zu den erfassten Daten finden Sie in den AWS CloudTrail Datensatzinhalten.

Kontroll-ID	AWS Config	Empfehlungen
12.1.1	guardduty-enabled-centralized	Amazon GuardDuty kann mithilfe von Threat Intelligence Feeds helfen, potenzielle Cybersicherheitsereignisse zu überwachen und zu erkennen. Dazu gehören Listen mit bösartigen IPs und maschinellen Lernmethoden zur Identifizierung unerwarteter, nicht autorisierter und bösartiger Aktivitäten in Ihrer AWS Cloud-Umgebung.

Kontroll-ID	AWS Config	Empfehlungen
12.1.1	multi-region-cloudtrail-enabled	AWS CloudTrail zeichnet Aktionen und API-Aufrufe der AWS Management Console auf. Sie können feststellen, welche Benutzer und Konten angerufen wurden AWS, von welcher Quell-IP-Adresse aus die Anrufe getätigt wurden und wann die Anrufe erfolgten . CloudTrail übermittelt Protokolldateien aus allen AWS Regionen an Ihren S3-Bucket, wenn MULTI_REG ION_CLOUD_TRAIL_EN ABLED aktiviert ist. Außerdem wird beim AWS Start einer neuen Region derselbe Trail in der neuen Region erstellt. CloudTrail Dadurch erhalten Sie automatisch Protokoll dateien mit API-Aktivitäten für die neue Region.

Kontroll-ID	AWS Config	Empfehlungen
12.1.1	securityhub-enabled	AWS Security Hub hilft bei der Überwachung von unbefugte m Personal, Verbindungen, Geräten und Software. AWS Security Hub aggregiert, organisiert und priorisiert die Sicherheitswarnungen oder Ergebnisse mehrerer Dienste. AWS Einige dieser Dienste sind Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer und AWS Firewall Manager sowie AWS Partnerlösungen.
12.2.2	api-gw-execution-logging-aktiviert	Die API-Gateway-Protokollierung zeigt detaillierte Ansichten der Benutzer, die auf die API zugegriffen haben, und wie diese Benutzer auf die API zugegriffen haben. Diese Einblicke ermöglichen die Transparenz von Benutzeraktivitäten.

Kontroll-ID	AWS Config	Empfehlungen
12.2.2	cloud-trail-cloud-watch-logs-aktiviert	Verwenden Sie Amazon CloudWatch , um Protokoll ereignisaktivitäten zentral zu sammeln und zu verwalten . Die Aufnahme von AWS CloudTrail Daten liefert Einzelheiten zu den API-Aufru faktivitäten in Ihrem AWS-Konto.
12.2.2	cloud-trail-encryption-enabled	Da sensible Daten vorhanden sein können und um Daten im Ruhezustand zu schützen, sollten Sie sicherstellen, dass die Verschlüsselung für Ihre AWS CloudTrail Trails aktiviert ist.

Kontroll-ID	AWS Config	Empfehlungen
12.2.2	cloud-trail-log-file-Validierung aktiviert	Verwenden Sie die AWS CloudTrail Protokolldateivalidierung, um die Integrität von Protokollen zu überprüfen. CloudTrail Mithilfe der Protokolldateivalidierung kann festgestellt werden, ob eine Protokolldatei geändert oder gelöscht wurde oder ob sie nach der Übermittlung CloudTrail unverändert geblieben ist. Dieses Feature wurde mit dem Branchenstandard entsprechenden Algorithmen entwickelt: SHA-256 für die Hashfunktion und SHA-256 mit RSA für digitale Signaturen. Aus diesem Grund ist es rechnerisch unmöglich, CloudTrail Protokolldateien unbemerkt zu ändern, zu löschen oder zu fälschen.
12.2.2	cloudtrail-s3-dataevents-enabled	Die Erfassung von Simple Storage Service (Amazon S3)-Datenereignissen unterstützt die Erkennung von ungewöhnlichen Aktivitäten. Zu den Details gehören AWS-Konto Informationen über den Zugriff auf einen Amazon S3 S3-Bucket, die IP-Adresse und die Uhrzeit des Ereignisses.

Kontroll-ID	AWS Config	Empfehlungen
12.2.2	cloudwatch-log-group-encrypted	Um sensible Daten im Speicher zu schützen, stellen Sie sicher, dass die Verschlüsselung für Ihre Amazon CloudWatch Log Groups aktiviert ist.
12.2.2	cw-loggroup-retention-period-überprüfen	Stellen Sie sicher, dass die Ereignisprotokolldaten für Ihre Protokollgruppen über eine Mindestdauer aufbewahrt werden, um die Fehlerbehebung und forensische Untersuchungen zu unterstützen. Fehlende frühere Ereignisprotokolldaten erschweren die Rekonstruierung und Identifizierung potenziell schädlicher Ereignisse.

Kontroll-ID	AWS Config	Empfehlungen
12.2.2	elb-logging-enabled	Die Elastic-Load-Balancing-Aktivität ist ein zentraler Kommunikationspunkt innerhalb einer Umgebung. Stellen Sie sicher, dass die ELB-Protokollierung aktiviert ist. Die gesammelten Daten enthalten detaillierte Informati onen zu Anfragen, die an den ELB gesendet wurden. Jedes Protokoll enthält Informati onen wie die Zeit, zu der die Anforderung einging, die Client-IP-Adresse, Latenzen, Anforderungspfade und Serverantworten.
12.2.2	guardduty-enabled-centralized	Amazon GuardDuty kann mithilfe von Threat Intellige nce Feeds helfen, potenzielle Cybersicherheitsereignisse zu überwachen und zu erkennen. Dazu gehören Listen mit bösartigen IPs und maschinel len Lernmethoden zur Identifiz ierung unerwarteter, nicht autorisierter und bösartige r Aktivitäten in Ihrer AWS Cloud-Umgebung.

Kontroll-ID	AWS Config	Empfehlungen
12.2.2	multi-region-cloudtrail-enabled	AWS CloudTrail zeichnet Aktionen und API-Aufrufe der AWS Management Console auf. Sie können feststellen, welche Benutzer und Konten angerufen wurden AWS, von welcher Quell-IP-Adresse aus die Anrufe getätigt wurden und wann die Anrufe erfolgten . CloudTrail übermittelt Protokolldateien aus allen AWS Regionen an Ihren S3-Bucket, wenn MULTI_REG ION_CLOUD_TRAIL_EN ABLED aktiviert ist. Außerdem wird beim AWS Start einer neuen Region derselbe Trail in der neuen Region erstellt. CloudTrail Dadurch erhalten Sie automatisch Protokoll dateien mit API-Aktivitäten für die neue Region.

Kontroll-ID	AWS Config	Empfehlungen
12.2.2	rds-logging-enabled	Um die Protokollierung und Überwachung in Ihrer Umgebung zu erleichtern, stellen Sie sicher, dass die Amazon Relational Database Service (Amazon RDS)-Protokollierung aktiviert ist. Mit der Amazon-RDS-Protokollierung können Sie Ereignisse wie Verbindungen, Verbindungsabbrüche, Abfragen oder abgefragte Tabellen erfassen.

Kontroll-ID	AWS Config	Empfehlungen
12.2.2	redshift-cluster-configuration-check	Um Daten im Ruhezustand zu schützen, muss die Verschlüsselung für Ihre Amazon-Redshift-Cluster aktiviert sein. Sie müssen auch sicherstellen, dass die erforderlichen Konfigurationen auf Amazon-Redshift-Clustern bereitgestellt werden. Die Prüfungsprotokollierung muss aktiviert sein, um Informationen zu Verbindungen und Benutzeraktivitäten in der Datenbank bereitzustellen. Diese Regel erfordert, dass ein Wert für clusterDb Encrypted (Config Default: TRUE) und LoggingEnabled (Config Default: TRUE) gesetzt ist. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	AWS Config	Empfehlungen
12.2.2	s-3 bucket-logging-enabled	Die Amazon Simple Storage Service (Amazon S3)-Serverzugriffsprotokollierung bietet eine Methode zur Überwachung des Netzwerks im Hinblick auf potenzielle Cybersicherheitsereignisse. Die Ereignisse werden überwacht, indem detaillierte Aufzeichnungen über die Anfragen erfasst werden, die an einen Amazon-S3-Bucket gestellt wurden. Jeder Zugriffsprotokolleintrag enthält Details zu einer einzelnen Zugriffsanfrage. Zu den Details gehören Anforderer, Bucket-Name, Anforderungszeit, Anforderungsaktion, Antwortstatus und Fehlercode, falls relevant.

Kontroll-ID	AWS Config	Empfehlungen
12.2.2	securityhub-enabled	AWS Security Hub hilft bei der Überwachung von unbefugte m Personal, Verbindungen, Geräten und Software. AWS Security Hub aggregiert, organisiert und priorisiert die Sicherheitswarnungen oder Ergebnisse mehrerer Dienste. AWS Einige dieser Dienste sind Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer und AWS Firewall Manager sowie AWS Partnerlösungen.
12.2.2	vpc-flow-logs-enabled	VPC-Flow-Protokolle erfassen detaillierte Informationsdatens ätze über den IP-Datenv erkehr, der zu und von Netzwerkschnittstellen in Ihrer Amazon Virtual Private Cloud (Amazon VPC) fließt. Standardmäßig enthalten Flow-Protokolldatensätze Werte für die verschiedenen Komponenten des IP-Flows, einschließlich Quelle, Ziel und Protokoll.

Kontroll-ID	AWS Config	Empfehlungen
12.2.2	wafv2-logging-enabled	Um die Protokollierung und Überwachung in Ihrer Umgebung zu erleichte rn, aktivieren Sie die AWS WAF (V2) -Protokollierung im regionalen und globalen Web. ACLs AWS Die WAF-Protokollierung bietet detaillie rte Informationen über den Datenverkehr, der von Ihrer Web-ACL analysiert wird. In den Protokollen werden die Uhrzeit aufgezeichnet, zu der die AWS WAF die Anfrage von Ihrer AWS Ressource erhalten hat, Informationen zu der Anfrage und eine Aktion für die Regel, der jede Anfrage entsprach.
12.2.4	guardduty-enabled-centralized	Amazon GuardDuty kann mithilfe von Threat Intellige nce Feeds helfen, potenzielle Cybersicherheitsereignisse zu überwachen und zu erkennen. Dazu gehören Listen mit bösartigen IPs und maschinel len Lernmethoden zur Identifiz ierung unerwarteter, nicht autorisierter und bösartige r Aktivitäten in Ihrer AWS Cloud-Umgebung.

Kontroll-ID	AWS Config	Empfehlungen
12.2.4	securityhub-enabled	AWS Security Hub hilft bei der Überwachung von unbefugte m Personal, Verbindungen, Geräten und Software. AWS Security Hub aggregiert, organisiert und priorisiert die Sicherheitswarnungen oder Ergebnisse mehrerer Dienste. AWS Einige dieser Dienste sind Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer und AWS Firewall Manager sowie AWS Partnerlösungen.
12.2.5	cloudtrail-enabled	AWS CloudTrail kann durch die Aufzeichnung von Aktionen und API-Aufrufen in der AWS Management Console bei der Nichtabst reitbarkeit helfen. Sie können die Benutzer und die Benutzer AWS-Konten , die einen AWS Dienst aufgerufen haben, die Quell-IP-Adresse, über die die Aufrufe generiert wurden, und den Zeitpunkt der Anrufe identifizieren. Einzelheiten zu den erfassten Daten finden Sie in den AWS CloudTrail Datensatzinhalten.

Kontroll-ID	AWS Config	Empfehlungen
12.2.5	guardduty-enabled-centralized	Amazon GuardDuty kann mithilfe von Threat Intellige nce Feeds helfen, potenzielle Cybersicherheitsereignisse zu überwachen und zu erkennen. Dazu gehören Listen mit bösartigen IPs und maschinel len Lernmethoden zur Identifiz ierung unerwarteter, nicht autorisierter und bösartige r Aktivitäten in Ihrer AWS Cloud-Umgebung.

Kontroll-ID	AWS Config	Empfehlungen
12.2.5	multi-region-cloudtrail-enabled	AWS CloudTrail zeichnet Aktionen und API-Aufrufe der AWS Management Console auf. Sie können feststellen, welche Benutzer und Konten angerufen wurden AWS, von welcher Quell-IP-Adresse aus die Anrufe getätigt wurden und wann die Anrufe erfolgten . CloudTrail übermittelt Protokolldateien aus allen AWS Regionen an Ihren S3-Bucket, wenn MULTI_REG ION_CLOUD_TRAIL_EN ABLED aktiviert ist. Außerdem wird beim AWS Start einer neuen Region derselbe Trail in der neuen Region erstellt. CloudTrail Dadurch erhalten Sie automatisch Protokoll dateien mit API-Aktivitäten für die neue Region.

Kontroll-ID	AWS Config	Empfehlungen
12.2.5	securityhub-enabled	AWS Security Hub hilft bei der Überwachung von unbefugte m Personal, Verbindungen, Geräten und Software. AWS Security Hub aggregiert, organisiert und priorisiert die Sicherheitswarnungen oder Ergebnisse mehrerer Dienste. AWS Einige dieser Dienste sind Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer und AWS Firewall Manager sowie AWS Partnerlösungen.
12.3.2	guardduty-enabled-centralized	Amazon GuardDuty kann mithilfe von Threat Intellige nce Feeds helfen, potenzielle Cybersicherheitsereignisse zu überwachen und zu erkennen. Dazu gehören Listen mit bösartigen IPs und maschinel len Lernmethoden zur Identifiz ierung unerwarteter, nicht autorisierter und bösartige r Aktivitäten in Ihrer AWS Cloud-Umgebung.

Kontroll-ID	AWS Config	Empfehlungen
12.3.2	multi-region-cloudtrail-enabled	AWS CloudTrail zeichnet Aktionen und API-Aufrufe der AWS Management Console auf. Sie können feststellen, welche Benutzer und Konten angerufen wurden AWS, von welcher Quell-IP-Adresse aus die Anrufe getätigt wurden und wann die Anrufe erfolgten . CloudTrail übermittelt Protokolldateien aus allen AWS Regionen an Ihren S3-Bucket, wenn MULTI_REG ION_CLOUD_TRAIL_EN ABLED aktiviert ist. Außerdem wird beim AWS Start einer neuen Region derselbe Trail in der neuen Region erstellt. CloudTrail Dadurch erhalten Sie automatisch Protokoll dateien mit API-Aktivitäten für die neue Region.

Kontroll-ID	AWS Config	Empfehlungen
12.3.2	securityhub-enabled	AWS Security Hub hilft bei der Überwachung von unbefugte m Personal, Verbindungen, Geräten und Software. AWS Security Hub aggregiert, organisiert und priorisiert die Sicherheitswarnungen oder Ergebnisse mehrerer Dienste. AWS Einige dieser Dienste sind Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer und AWS Firewall Manager sowie AWS Partnerlösungen.
14.1.2	alb-http-to-https-Umleitung sprüfung	Um Daten während der Übertragung zu schützen, stellen Sie sicher, dass Ihr Application Load Balancer unverschlüsselte HTTP-Anfragen automatisch an HTTPS umleitet. Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	AWS Config	Empfehlungen
14.1.2	api-gw-ssl-enabled	Stellen Sie sicher, dass die REST-API-Stufen von Amazon API Gateway mit SSL-Zerti fikaten konfiguriert sind, damit Backend-Systeme überprüfe n können, ob Anforderungen von API Gateway stammen.
14.1.2	elasticsearch-node-to-node-Verschlüsselungsprüfung	Stellen Sie sicher, dass die node-to-node Verschlüsselung für Amazon OpenSearch Service aktiviert ist. Node-to-nodeVerschlüsselung ermöglicht die TLS 1.2-Versc hlüsselung für die gesamte Kommunikation innerhalb der Amazon Virtual Private Cloud (Amazon VPC). Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	AWS Config	Empfehlungen
14.1.2	opensearch-node-to-node-Verschlüsselungsprüfung	Stellen Sie sicher, dass die node-to-node Verschlüsselung für Amazon OpenSearch Service aktiviert ist. Node-to-nodeVerschlüsselung ermöglicht die TLS 1.2-Verschlüsselung für die gesamte Kommunikation innerhalb der Amazon Virtual Private Cloud (Amazon VPC). Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.
14.1.2	elb-acm-certificate-required	Zum Schutz von eventuell vorhandenen sensiblen Daten sowie von Daten während der Übertragung muss die Verschlüsselung für Ihr Elastic Load Balancing aktiviert sein. Verwenden Sie AWS Certificate Manager, um öffentliche und private SSL/TLS-Zertifikate mit AWS Diensten und internen Ressourcen zu verwalten, bereitzustellen und bereitzustellen.

Kontroll-ID	AWS Config	Empfehlungen
14.1.2	elb-tls-https-listeners-nur	Stellen Sie sicher, dass Ihre Elastic Load Balancer (ELBs) mit SSL- oder HTTPS-Listenern konfiguriert sind. Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.
14.1.2	elv 2 acm-certificate-required	Zum Schutz von eventuell vorhandenen sensiblen Daten sowie von Daten während der Übertragung muss die Verschlüsselung für Ihr Elastic Load Balancing aktiviert sein. Verwenden Sie AWS Certificate Manager, um öffentliche und private SSL/TLS-Zertifikate mit AWS Diensten und internen Ressourcen zu verwalten, bereitzustellen und bereitzustellen.
14.1.2	redshift-require-tls-ssl	Stellen Sie sicher, dass Ihre Amazon-Redshift-Cluster eine TLS/SSL-Verschlüsselung erfordern, um eine Verbindung zu SQL-Clients herzustellen. Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	AWS Config	Empfehlungen
14.1.2	s-3 bucket-ssl-requests-only	Um Daten während der Übertragung zu schützen, stellen Sie sicher, dass Ihre Amazon Simple Storage Service (Amazon S3)-Bucke ts Anfragen zur Verwendun g von Secure Socket Layer (SSL)-Buckets erfordern. Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.
14.1.3	alb-waf-enabled	Stellen Sie sicher, dass AWS WAF auf Elastic Load Balancers (ELB) aktiviert ist, um Webanwendungen zu schützen. Eine WAF trägt zum Schutz Ihrer Webanwend ungen oder APIs vor gängigen Web-Exploits bei. Diese Web-Exploits können sich auf die Verfügbarkeit auswirken, die Sicherheit gefährden oder übermäßige Ressourcen in Ihrer Umgebung verbrauchen.

Kontroll-ID	AWS Config	Empfehlungen
14.1.3	api-gw-associated-with-WAF	AWS Mit WAF können Sie eine Reihe von Regeln (als Web Access Control List (Web ACL) bezeichnet) konfiguri eren, die Webanfragen auf der Grundlage von anpassbar en Websicherheitsregeln und -bedingungen, die Sie definieren, zulassen, blockiere n oder zählen. Stellen Sie sicher, dass Ihre Amazon-API-Gateway-Stufe mit einer WAF-Web-ACL verknüpft ist, um sie vor böswilligen Angriffen zu schützen.
14.1.3	guardduty-enabled-centralized	Amazon GuardDuty kann mithilfe von Threat Intellige nce Feeds helfen, potenzielle Cybersicherheitsereignisse zu überwachen und zu erkennen. Dazu gehören Listen mit bösartigen IPs und maschinel len Lernmethoden zur Identifiz ierung unerwarteter, nicht autorisierter und bösartige r Aktivitäten in Ihrer AWS Cloud-Umgebung.

Kontroll-ID	AWS Config	Empfehlungen
14.1.3	securityhub-enabled	AWS Security Hub hilft bei der Überwachung von unbefugte m Personal, Verbindungen, Geräten und Software. AWS Security Hub aggregiert, organisiert und priorisiert die Sicherheitswarnungen oder Ergebnisse mehrerer Dienste. AWS Einige dieser Dienste sind Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer und AWS Firewall Manager sowie AWS Partnerlösungen.
14.2.2	acm-certificate-expiration-check	Stellen Sie sicher, dass die Netzwerkintegrität geschützt ist, indem Sie sicherstellen, dass X509-Zertifikate von AWS ACM ausgestellt werden. Diese Zertifikate müssen gültig und dürfen nicht abgelaufe n sein. Für diese Regel ist ein Wert für erforderlich daysToExpiration (Wert für bewährte AWS Grundrege ln für Sicherheit: 90). Der tatsächliche Wert muss den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	AWS Config	Empfehlungen
14.2.2	alb-http-to-https-Umleitung sprüfung	Um Daten während der Übertragung zu schützen, stellen Sie sicher, dass Ihr Application Load Balancer unverschlüsselte HTTP-Anfragen automatisch an HTTPS umleitet. Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.
14.2.2	api-gw-cache-enabled-und-ve rschlüsselt	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass die Verschlüsselung für den Cache Ihrer API-Gatew ay-Stufe aktiviert ist. Da für die API-Methode sensible Daten erfasst werden können, sollten Sie die Verschlüsselung von Daten im Ruhezustand aktivieren, um diese Daten zu schützen.
14.2.2	api-gw-ssl-enabled	Stellen Sie sicher, dass die REST-API-Stufen von Amazon API Gateway mit SSL-Zerti fikaten konfiguriert sind, damit Backend-Systeme überprüfe n können, ob Anforderungen von API Gateway stammen.

Kontroll-ID	AWS Config	Empfehlungen
14.2.2	dynamodb-table-encrypted-kms	Stellen Sie sicher, dass die Verschlüsselung für Ihre Amazon-DynamoDB-Tabellen aktiviert ist. Um eventuell vorhandene sensible Daten im Ruhezustand in diesen Tabellen zu schützen, müssen Sie die Verschlüsselung von Daten im Ruhezustand aktivieren. Standardmäßig werden DynamoDB-Tabellen mit einem AWS eigenen Kundenhauptschlüssel (CMK) verschlüsselt.
14.2.2	ec-2 ebs-encryption-by-default	Zum Schutz von Daten im Ruhezustand müssen Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon Elastic Block Store (Amazon EBS)-Volumes aktiviert ist. Da sensible Daten auch im Ruhezustand vorhanden sein können, sollten Sie die Verschlüsselung im Ruhezustand aktivieren, um diese Daten zu schützen.
14.2.2	efs-encrypted-check	Aktivieren Sie die Verschlüsselung für Ihr Amazon Elastic File System (EFS), um eventuell vorhandene sensible Daten sowie Daten im Ruhezustand zu schützen.

Kontroll-ID	AWS Config	Empfehlungen
14.2.2	elasticsearch-encrypted-at-rest	Da sensible Daten vorhanden sein können und um Daten im Ruhezustand zu schützen, sollten Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon OpenSearch Service (OpenSearch Service) -Domains aktiviert ist.
14.2.2	opensearch-encrypted-at-rest	Da sensible Daten vorhanden sein können und um Daten im Ruhezustand zu schützen, sollten Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon OpenSearch Service-Domains aktiviert ist.
14.2.2	encrypted-volumes	Aktivieren Sie die Verschlüs selung für Ihre Amazon-El astic-Block-Store (Amazon-EBS)-Volumes, um eventuell vorhandene sensible Daten sowie Daten im Ruhezustand zu schützen.

Kontroll-ID	AWS Config	Empfehlungen
14.2.2	ec-2 instances-in-vpc	Stellen Sie Amazon Elastic Compute Cloud (Amazon EC2) -Instances innerhalb einer Amazon Virtual Private Cloud (Amazon VPC) bereit, um eine sichere Kommunika tion zwischen einer Instance und anderen Services innerhalb der Amazon VPC zu ermöglichen, ohne dass ein Internet-Gateway, ein NAT-Gerät oder eine VPN-Verbi ndung erforderlich ist. Der gesamte Datenverkehr bleibt sicher in der AWS Cloud. Domains, die sich innerhalb einer VPC befinden, verfügen aufgrund ihrer logischen Isolierung im Vergleich zu Domains mit öffentlic hen Endpunkten über eine zusätzliche Sicherheitsebene. Weisen Sie EC2 Amazon-In stances einer Amazon-VPC zu, um den Zugriff ordnungsg emäß zu verwalten.

Kontroll-ID	AWS Config	Empfehlungen
14.2.2	redshift-cluster-configuration-check	Um Daten im Ruhezustand zu schützen, muss die Verschlüsselung für Ihre Amazon-Redshift-Cluster aktiviert sein. Sie müssen auch sicherstellen, dass die erforderlichen Konfigurationen auf Amazon-Redshift-Clustern bereitgestellt werden. Die Prüfungsprotokollierung muss aktiviert sein, um Informationen zu Verbindungen und Benutzeraktivitäten in der Datenbank bereitzustellen. Diese Regel erfordert, dass ein Wert für clusterDbEncrypted (Config Default: TRUE) und LoggingEnabled (Config Default: TRUE) gesetzt ist. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	AWS Config	Empfehlungen
14.2.6	dynamodb-table-encrypted-kms	Stellen Sie sicher, dass die Verschlüsselung für Ihre Amazon-DynamoDB-Tabellen aktiviert ist. Um eventuell vorhandene sensible Daten im Ruhezustand in diesen Tabellen zu schützen, müssen Sie die Verschlüsselung von Daten im Ruhezustand aktivieren. Standardmäßig werden DynamoDB-Tabellen mit einem AWS eigenen Kundenhauptschlüssel (CMK) verschlüsselt.
14.2.6	ec-2 ebs-encryption-by-default	Zum Schutz von Daten im Ruhezustand müssen Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon Elastic Block Store (Amazon EBS)-Volumes aktiviert ist. Da sensible Daten auch im Ruhezustand vorhanden sein können, sollten Sie die Verschlüsselung im Ruhezustand aktivieren, um diese Daten zu schützen.
14.2.6	efs-encrypted-check	Aktivieren Sie die Verschlüsselung für Ihr Amazon Elastic File System (EFS), um eventuell vorhandene sensible Daten sowie Daten im Ruhezustand zu schützen.

Kontroll-ID	AWS Config	Empfehlungen
14.2.6	elasticsearch-encrypted-at-rest	Da sensible Daten vorhanden sein können und um Daten im Ruhezustand zu schützen, sollten Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon OpenSearch Service (OpenSearch Service) -Domains aktiviert ist.
14.2.6	opensearch-encrypted-at-rest	Da sensible Daten vorhanden sein können und um Daten im Ruhezustand zu schützen, sollten Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon OpenSearch Service-Domains aktiviert ist.
14.2.6	rds-storage-encrypted	Zum Schutz von Daten im Ruhezustand müssen Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon Relational Database Service (Amazon RDS)-Instances aktiviert ist. Um eventuell vorhandene sensible Daten im Ruhezustand in Amazon-RDS-Instanc es zu schützen, muss die Verschlüsselung von Daten im Ruhezustand aktiviert sein.

Kontroll-ID	AWS Config	Empfehlungen
14.2.6	encrypted-volumes	Aktivieren Sie die Verschlüs selung für Ihre Amazon-El astic-Block-Store (Amazon-EBS)-Volumes, um eventuell vorhandene sensible Daten sowie Daten im Ruhezustand zu schützen.
14.2.6	redshift-cluster-configuration-check	Um Daten im Ruhezustand zu schützen, muss die Verschlüs selung für Ihre Amazon-Re dshift-Cluster aktiviert sein. Sie müssen auch sicherste llen, dass die erforderlichen Konfigurationen auf Amazon-Redshift-Clustern bereitgestellt werden. Die Prüfungsprotokolli erung muss aktiviert sein, um Informationen zu Verbindun gen und Benutzeraktivitäten in der Datenbank bereitzus tellen. Diese Regel erfordert , dass ein Wert für clusterDb Encrypted (Config Default: TRUE) und LoggingEnabled (Config Default: TRUE) gesetzt ist. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprech en.

Vorlage

Die Vorlage ist verfügbar unter GitHub: Operational Best Practices for MAS TRMG.

Bewährte Methoden für die Überwachung

Dieses Konformitätspaket enthält AWS Config Regeln, die auf der internen AWSÜberwachung basieren. Eine Liste aller verwalteten Regeln, die von unterstützt werden AWS Config, finden Sie unter Liste der AWS Config verwalteten Regeln.

Die Namen und Beschreibungen der erforderlichen Parameter finden Sie im `Parameters` Abschnitt der folgenden Vorlage.

Die Vorlage ist verfügbar unter GitHub: Bewährte Betriebspraktiken für die Überwachung.

Bewährte Methoden für die Implementierung von NBC TRMG

Konformitätspakete bieten ein allgemeines Compliance-Framework, das es Ihnen ermöglicht, mithilfe verwalteter oder benutzerdefinierter Regeln und Abhilfemaßnahmen Kontrollen zur Sicherheits-, Betriebs- oder Kostenoptimierung durchzuführen. AWS Config AWS Config Conformance Packs dienen als Beispielvorlagen nicht dazu, die vollständige Einhaltung eines bestimmten Governance- oder Compliance-Standards sicherzustellen. Sie sind dafür verantwortlich, selbst zu beurteilen, ob Ihre Nutzung der Services den geltenden gesetzlichen und behördlichen Anforderungen entspricht.

Im Folgenden finden Sie ein Beispiel für eine Zuordnung zwischen dem Framework der Technology Risk Management (TRM) Guidelines der National Bank of Cambodia (NBC) und den AWS Managed Config-Regeln. Jede Config-Regel gilt für eine bestimmte AWS Ressource und bezieht sich auf eine oder mehrere NBC TRM-Richtlinien. Eine NBC TRM Guideline kann sich auf mehrere Konfigurationsregeln beziehen. In der folgenden Tabelle finden Sie weitere Informationen und Anleitungen zu diesen Zuordnungen.

Diese Vorlage für ein Konformitätspaket enthält Zuordnungen zu Kontrollen innerhalb der Richtlinien der National Bank of Kambodscha (NBC) für Technologierisikomanagement (TRM), auf die Sie hier zugreifen können: National Bank of Cambodia: Technology Risk Management Guidelines.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
3.1.1(d)	d) Zu den wichtigen Kontrollen, die berücksichtigt werden müssen, gehören: - Ein systemati	iam-root-access-key-überprüfen	Der Zugriff auf Systeme und Ressourcen kann gesteuert werden, indem überprüft wird,

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
	scher Prozess zur Beantragung und Genehmigung der Erstellung von Benutzern IDs und der Zugangskontrollmatrix - Durchführung einer Risikobewertung und auf deren Grundlage die Gewährung von Zugriffsrechten. - Implementierung einer rollenbasierten Zugriffskontrolle zur Sicherstellung einer effektiven Aufgabentrennung - Änderung von Standardbenutzernamen and/or passwords of systems and prohibiting sharing of user IDs and passwords of generic accounts - Modification of access rights whenever there is a change in role or responsibility and removal of access rights on cessation of employment/contract - Verfahren zur rechtzeitigen		ob der Root-Benutzer keine Zugriffsschlüssel mit seiner AWS Identity and Access Management (IAM) -Rolle verknüpft hat. Stellen Sie sicher, dass die Root-Zugriffsschlüssel gelöscht werden. Erstellen und verwenden Sie stattdessen rollenbasierte Funktionen, AWS-Konten um das Prinzip der geringsten Funktionalität zu berücksichtigen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
	Benachrichtigung der Informationssicher heitsfunktion über hinzugefügte, gelöschte und Rollenänderungen von Benutzern - Regelmäßiger Abgleich von Benutzern IDs in einem System und tatsächlichen Benutzern, die Zugriff benötigen, und Löschung aller unnötigen IDs, falls vorhanden - Prüfung, Protokollierung und Überwachung des Zugriffs aller Benutzer auf IT-Ressourcen durch alle Benutzer und - Prüfung, Protokollierung und Überwachung des Zugriffs aller Benutzer auf IT-Ressourcen und - Prüfung der Deaktivierung IDs von Benutzern kritische r Anwendungen, die sind für längere Zeit beurlaubt		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
3.1.1(d)	d) Zu den wichtigen Kontrollen, die berücksichtigt werden müssen, gehören: - ein systematischer Prozess zur Beantragung und Genehmigung der Einrichtung von Benutzern IDs und der Zugriffskontrollmatrix - Durchführung einer Risikobewertung und Gewährung von Zugriffsrechten auf der Grundlage derselben. - Implementierung einer rollenbasierten Zugriffskontrolle zur Sicherstellung einer effektiven Aufgabentrennung - Änderung von Standardbenutzernamen and/or passwords of systems and prohibiting sharing of user IDs and passwords of generic accounts - Modification of access rights whenever there is a change in role	api-gw-execution-logging-aktiviert	Die API-Gateway-Protokollierung zeigt detaillierte Ansichten der Benutzer, die auf die API zugegriffen haben, und wie diese Benutzer auf die API zugegriffen haben. Diese Insights ermöglichen die Einsicht in Benutzeraktivitäten.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
	or responsibility and removal of access rights on cessation of employment/ contract - Verfahren zur rechtzeitigen Benachrichtigung der Informationssicher heitsfunktion über hinzugefügte, gelöschte und Rollenänderungen von Benutzern - Regelmäßiger Abgleich von Benutzern IDs in einem System und tatsächlichen Benutzern, die Zugriff benötigen, und Löschung aller unnötigen IDs, falls vorhanden - Prüfung, Protokollierung und Überwachung des Zugriffs aller Benutzer auf IT-Ressourcen durch alle Benutzer und - Prüfung, Protokollierung und Überwachung des Zugriffs aller Benutzer auf IT-Ressourcen und - Prüfung der		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
	Deaktivierung IDs von Benutzern kritische r Anwendungen, die sind für längere Zeit beurlaubt		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
3.1.1(d)	d) Zu den wichtigen Kontrollen, die in Betracht gezogen werden müssen, gehören: - ein systematischer Prozess zur Beantragung und Genehmigung der Einrichtung von Benutzern IDs und der Zugangskontrollmatrix - Durchführung einer Risikobewertung und Gewährung von Zugriffsrechten auf dieser Grundlage. - Implementierung einer rollenbasierten Zugriffskontrolle zur Sicherstellung einer effektiven Aufgabentrennung - Änderung von Standardbenutzernamen and/or passwords of systems and prohibiting sharing of user IDs and passwords of generic accounts - Modification of access rights whenever there	cloud-trail-cloud-watch-logs-aktiviert	Verwenden Sie Amazon CloudWatch , um Protokoll ereignisaktivitäten zentral zu sammeln und zu verwalten. Die Aufnahme von AWS CloudTrail Daten liefert Einzelheiten zu den API-Aufrufaktivitäten in Ihrem AWS-Konto.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
	is a change in role or responsibility and removal of access rights on cessation of employment/ contract - Verfahren zur rechtzeitigen Benachrichtigung der Informationssicher heitsfunktion über hinzugefügte, gelöschte und Rollenänderungen von Benutzern - Regelmäßiger Abgleich von Benutzern IDs in einem System und tatsächlichen Benutzern, die Zugriff benötigen, und Löschung aller unnötigen IDs, falls vorhanden - Prüfung, Protokollierung und Überwachung des Zugriffs aller Benutzer auf IT-Ressourcen durch alle Benutzer und - Prüfung, Protokollierung und Überwachung des Zugriffs aller Benutzer auf IT-Ressourcen		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
	und - Prüfung der Deaktivierung IDs von Benutzern kritische r Anwendungen, die sind für längere Zeit beurlaubt		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
3.1.1(d)	d) Zu den wichtigen Kontrollen, die berücksichtigt werden müssen, gehören: - Ein systematischer Prozess zur Beantragung und Genehmigung der Erstellung von Benutzer IDs - und Zugriffskontrollmatrizen - Durchführung einer Risikobewertung und Gewährung von Zugriffsrechten auf dieser Grundlage. - Implementierung einer rollenbasierten Zugriffskontrolle zur Sicherstellung einer effektiven Aufgabentrennung - Änderung von Standardbenutzernamen and/or passwords of systems and prohibiting sharing of user IDs and passwords of generic accounts - Modification of access rights whenever there is a change in role or responsibility and	cloudtrail-enabled	AWS CloudTrail kann durch die Aufzeichnung von Aktionen und API-Aufrufen in der AWS Management Console bei der Nichtabstreitbarkeit helfen. Sie können die Benutzer und die Benutzer AWS-Konten , die einen AWS Dienst aufgerufen haben, die Quell-IP-Adresse, über die die Aufrufe generiert wurden, und den Zeitpunkt der Anrufe identifizieren. Einzelheiten zu den erfassten Daten finden Sie in den AWS CloudTrail Datensatzinhalten.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
	removal of access rights on cessation of employment/ contract - Verfahren zur rechtzeitigen Benachrichtigung der Informationssicher heitsfunktion über hinzugefügte, gelöschte und Rollenänderungen von Benutzern - Regelmäßiger Abgleich von Benutzern IDs in einem System und tatsächlichen Benutzern, die Zugriff benötigen, und Löschung aller unnötigen IDs, falls vorhanden - Prüfung, Protokollierung und Überwachung des Zugriffs aller Benutzer auf IT-Ressourcen durch alle Benutzer und - Prüfung, Protokollierung und Überwachung des Zugriffs aller Benutzer auf IT-Ressourcen und - Prüfung der Deaktivierung IDs von		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
	Benutzern kritische r Anwendungen, die sind für längere Zeit beurlaubt		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
3.1.1(d)	d) Zu den wichtigen Kontrollen, die berücksichtigt werden müssen, gehören: - ein systematischer Prozess zur Beantragung und Genehmigung der Einrichtung von Benutzern IDs und der Zugriffskontrollmatrix - Durchführung einer Risikobewertung und Gewährung von Zugriffsrechten auf dieser Grundlage. - Implementierung einer rollenbasierten Zugriffskontrolle zur Sicherstellung einer effektiven Aufgabentrennung - Änderung von Standardbenutzernamen and/or passwords of systems and prohibiting sharing of user IDs and passwords of generic accounts - Modification of access rights whenever there is a change in role or responsibility and	cloudtrail-s3-dataevents-enabled	Die Erfassung von Simple Storage Service (Amazon S3)-Datenereignissen unterstützt die Erkennung von ungewöhnlichen Aktivitäten. Zu den Details gehören AWS-Konto Informationen über den Zugriff auf einen Amazon S3 S3-Bucket, die IP-Adresse und die Uhrzeit des Ereignisses.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
	removal of access rights on cessation of employment/ contract - Verfahren zur rechtzeitigen Benachrichtigung der Informationssicher heitsfunktion über hinzugefügte, gelöschte und Rollenänderungen von Benutzern - Regelmäßiger Abgleich von Benutzern IDs in einem System und tatsächlichen Benutzern, die Zugriff benötigen, und Löschung aller unnötigen IDs, falls vorhanden - Prüfung, Protokollierung und Überwachung des Zugriffs aller Benutzer auf IT-Ressourcen durch alle Benutzer und - Prüfung, Protokollierung und Überwachung des Zugriffs aller Benutzer auf IT-Ressourcen und - Prüfung der Deaktivierung IDs von		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
	Benutzern kritische r Anwendungen, die sind für längere Zeit beurlaubt		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
3.1.1(d)	d) Zu den wichtigen Kontrollen, die berücksichtigt werden müssen, gehören: - Ein systematischer Prozess zur Beantragung und Genehmigung der Erstellung von Benutzern IDs und der Zugriffskontrollmatrix - Durchführung einer Risikobewertung und Gewährung von Zugriffsrechten auf dieser Grundlage. - Implementierung einer rollenbasierten Zugriffskontrolle zur Sicherstellung einer effektiven Aufgabentrennung - Änderung von Standardbenutzernamen and/or passwords of systems and prohibiting sharing of user IDs and passwords of generic accounts - Modification of access rights whenever there is a change in role or responsibility and	cloudwatch-alarm-action-check	Amazon CloudWatch alarmiert, wenn eine Metrik den Schwellenwert für eine bestimmte Anzahl von Bewertungszeiträumen überschreitet. Der Alarm führt eine oder mehrere Aktionen durch, die vom Wert der Metrik oder des Ausdrucks im Vergleich zu einem Schwellenwert in einer Reihe von Zeiträumen abhängt. Diese Regel erfordert einen Wert für alarmActionRequired (Config Default: True), insufficientDataAction Required (Config Default: True), okActionRequired (Config Default: False). Der tatsächliche Wert muss die Alarmaktionen für Ihre Umgebung widerspiegeln.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
	removal of access rights on cessation of employment/ contract - Verfahren zur rechtzeitigen Benachrichtigung der Informationssicher heitsfunktion über hinzugefügte, gelöschte und Rollenänderungen von Benutzern - Regelmäßiger Abgleich von Benutzern IDs in einem System und tatsächlichen Benutzern, die Zugriff benötigen, und Löschung aller unnötigen IDs, falls vorhanden - Prüfung, Protokollierung und Überwachung des Zugriffs aller Benutzer auf IT-Ressourcen durch alle Benutzer und - Prüfung, Protokollierung und Überwachung des Zugriffs aller Benutzer auf IT-Ressourcen und - Prüfung der Deaktivierung IDs von		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
	Benutzern kritische r Anwendungen, die sind für längere Zeit beurlaubt		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
3.1.1(d)	d) Zu den wichtigen Kontrollen, die berücksichtigt werden müssen, gehören: - Ein systematischer Prozess zur Beantragung und Genehmigung der Erstellung von Benutzern IDs und der Zugriffskontrollmatrix - Durchführung einer Risikobewertung und Gewährung von Zugriffsrechten auf dieser Grundlage. - Implementierung einer rollenbasierten Zugriffskontrolle zur Sicherstellung einer effektiven Aufgabentrennung - Änderung von Standardbenutzernamen and/or passwords of systems and prohibiting sharing of user IDs and passwords of generic accounts - Modification of access rights whenever there is a change in role or responsibility and	elb-logging-enabled	Die Elastic-Load-Balancing-Aktivität ist ein zentraler Kommunikationspunkt innerhalb einer Umgebung. Stellen Sie sicher, dass die ELB-Protokollierung aktiviert ist. Die gesammelten Daten enthalten detaillierte Informationen zu Anfragen, die an den ELB gesendet wurden. Jedes Protokoll enthält Informationen wie die Zeit, zu der die Anforderung einging, die Client-IP-Adresse, Latenzen, Anforderungspfade und Serverantworten.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
	removal of access rights on cessation of employment/ contract - Verfahren zur rechtzeitigen Benachrichtigung der Informationssicher heitsfunktion über hinzugefügte, gelöschte und Rollenänderungen von Benutzern - Regelmäßiger Abgleich von Benutzern IDs in einem System und tatsächlichen Benutzern, die Zugriff benötigen, und Löschung aller unnötigen IDs, falls vorhanden - Prüfung, Protokollierung und Überwachung des Zugriffs aller Benutzer auf IT-Ressourcen durch alle Benutzer und - Prüfung, Protokollierung und Überwachung des Zugriffs aller Benutzer auf IT-Ressourcen und - Prüfung der Deaktivierung IDs von		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
	Benutzern kritische r Anwendungen, die sind für längere Zeit beurlaubt		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
3.1.1(d)	d) Zu den wichtigen Kontrollen, die in Betracht gezogen werden müssen, gehören: - ein systematischer Prozess zur Beantragung und Genehmigung der Einrichtung von Benutzern IDs und der Zugangsko ntrollmatrix - Durchführung einer Risikobewertung und auf deren Grundlage die Gewährung von Zugriffsrechten. - Implementierung einer rollenbasierten Zugriffskontrolle zur Sicherstellung einer effektiven Aufgabent rennung - Änderung von Standardb enutzernamen and/ or passwords of systems and prohibiti ng sharing of user IDs and passwords of generic accounts - Modification of access rights whenever there	guardduty-enabled-centralized	Amazon GuardDuty kann mithilfe von Threat Intellige nce Feeds helfen, potenzielle Cybersich erheitsereignisse zu überwachen und zu erkennen. Dazu gehören Listen mit bösartigen IPs und maschinel len Lernmethoden zur Identifizierung unerwarteter, nicht autorisierter und bösartiger Aktivitäten in Ihrer AWS Cloud-Umgebung.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
	is a change in role or responsibility and removal of access rights on cessation of employment/ contract - Verfahren zur rechtzeitigen Benachrichtigung der Informationssicher heitsfunktion über hinzugefügte, gelöschte und Rollenänderungen von Benutzern - Regelmäßiger Abgleich von Benutzern IDs in einem System und tatsächlichen Benutzern, die Zugriff benötigen, und Löschung aller unnötigen IDs, falls vorhanden - Prüfung, Protokollierung und Überwachung des Zugriffs aller Benutzer auf IT-Ressourcen durch alle Benutzer und - Prüfung, Protokollierung und Überwachung des Zugriffs aller Benutzer auf IT-Ressourcen		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
	und - Prüfung der Deaktivierung IDs von Benutzern kritische r Anwendungen, die sind für längere Zeit beurlaubt		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
3.1.1(d)	d) Zu den wichtigen Kontrollen, die berücksichtigt werden müssen, gehören: - Ein systemati scher Prozess zur Beantragung und Genehmigung der Erstellung von Benutzern IDs und der Zugriffskontrollma trix - Durchführung einer Risikobewertung und Gewährung von Zugriffsrechten auf dieser Grundlage. - Implementierung einer rollenbasierten Zugriffskontrolle zur Sicherstellung einer effektiven Aufgabent rennung - Änderung von Standardb enutzernamen and/ or passwords of systems and prohibiti ng sharing of user IDs and passwords of generic accounts - Modification of access rights whenever there is a change in role or responsibility and	lambda-dlq-check	Aktivieren Sie diese Regel, um das entsprechende Personal über Amazon Simple Queue Service (Amazon SQS) oder Amazon Simple Notification Service (Amazon SNS) zu benachrichtigen, wenn eine Funktion ausgefallen ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
	removal of access rights on cessation of employment/ contract - Verfahren zur rechtzeitigen Benachrichtigung der Informationssicher heitsfunktion über hinzugefügte, gelöschte und Rollenänderungen von Benutzern - Regelmäßiger Abgleich von Benutzern IDs in einem System und tatsächlichen Benutzern, die Zugriff benötigen, und Löschung aller unnötigen IDs, falls vorhanden - Prüfung, Protokollierung und Überwachung des Zugriffs aller Benutzer auf IT-Ressourcen durch alle Benutzer und - Prüfung, Protokollierung und Überwachung des Zugriffs aller Benutzer auf IT-Ressourcen und - Prüfung der Deaktivierung IDs von		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
	Benutzern kritische r Anwendungen, die sind für längere Zeit beurlaubt		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
3.1.1(d)	d) Zu den wichtigen Kontrollen, die in Betracht gezogen werden müssen, gehören: - ein systematischer Prozess zur Beantragung und Genehmigung der Einrichtung von Benutzern IDs und der Zugangsko ntrollmatrix - Durchführung einer Risikobewertung und auf deren Grundlage die Gewährung von Zugriffsrechten. - Implementierung einer rollenbasierten Zugriffskontrolle zur Sicherstellung einer effektiven Aufgabent rennung - Änderung von Standardb enutzernamen and/ or passwords of systems and prohibiti ng sharing of user IDs and passwords of generic accounts - Modification of access rights whenever there	multi-region-cloudtrail-enabled	AWS CloudTrail zeichnet Aktionen und API-Aufrufe der AWS Management Console auf. Sie können feststellen, welche Benutzer und Konten angerufen wurden AWS, von welcher Quell-IP-Adresse aus die Anrufe getätigt wurden und wann die Anrufe erfolgten. CloudTrail übermittelt Protokolldateien aus allen AWS Regionen an Ihren S3-Bucket , wenn MULTI_REG ION_CLOUD _TRAIL_ENABLED aktiviert ist. Außerdem wird beim AWS Start einer neuen Region derselbe Trail in der neuen Region erstellt. CloudTrail Dadurch erhalten Sie automatis ch Protokolldateien mit API-Aktivitäten für die neue Region.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
	is a change in role or responsibility and removal of access rights on cessation of employment/ contract - Verfahren zur rechtzeitigen Benachrichtigung der Informationssicher heitsfunktion über hinzugefügte, gelöschte und Rollenänderungen von Benutzern - Regelmäßiger Abgleich von Benutzern IDs in einem System und tatsächlichen Benutzern, die Zugriff benötigen, und Löschung aller unnötigen IDs, falls vorhanden - Prüfung, Protokollierung und Überwachung des Zugriffs aller Benutzer auf IT-Ressourcen durch alle Benutzer und - Prüfung, Protokollierung und Überwachung des Zugriffs aller Benutzer auf IT-Ressourcen		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
	und - Prüfung der Deaktivierung IDs von Benutzern kritische r Anwendungen, die sind für längere Zeit beurlaubt		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
3.1.1(d)	d) Zu den wichtigen Kontrollen, die berücksichtigt werden müssen, gehören: - ein systemati scher Prozess zur Beantragung und Genehmigung der Einrichtung von Benutzern IDs und der Zugangsko ntrollmatrix - Durchführung einer Risikobewertung und Gewährung von Zugriffsrechten auf dieser Grundlage. - Implementierung einer rollenbasierten Zugriffskontrolle zur Sicherstellung einer effektiven Aufgabent rennung - Änderung von Standardb enutzernamen and/ or passwords of systems and prohibiti ng sharing of user IDs and passwords of generic accounts - Modification of access rights whenever there is a change in role	s-3 bucket-logging-enabled	Die Amazon Simple Storage Service (Amazon S3)-Serverzugriffs protokollierung bietet eine Methode zur Überwachu ng des Netzwerks im Hinblick auf potenzielle Cybersich erheitsereignisse. Die Ereignisse werden überwacht, indem detaillierte Aufzeichn ungen über die Anfragen erfasst werden, die an einen Amazon-S3-Bucket gestellt wurden. Jeder Zugriffsprotokolle intrag enthält Details zu einer einzelnen Zugriffsanfrage. Zu den Details gehören Anforderer, Bucket-Name, Anforderu ngszeit, Anforderu ngsaktion, Antwortst atus und Fehlercode, falls relevant.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
	or responsibility and removal of access rights on cessation of employment/ contract - Verfahren zur rechtzeitigen Benachrichtigung der Informationssicher heitsfunktion über hinzugefügte, gelöschte und Rollenänderungen von Benutzern - Regelmäßiger Abgleich von Benutzern IDs in einem System und tatsächlichen Benutzern, die Zugriff benötigen, und Löschung aller unnötigen IDs, falls vorhanden - Prüfung, Protokollierung und Überwachung des Zugriffs aller Benutzer auf IT-Ressourcen durch alle Benutzer und - Prüfung, Protokollierung und Überwachung des Zugriffs aller Benutzer auf IT-Ressourcen und - Prüfung der		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
	Deaktivierung IDs von Benutzern kritische r Anwendungen, die sind für längere Zeit beurlaubt		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
3.1.1(d)	d) Zu den wichtigen Kontrollen, die in Betracht gezogen werden müssen, gehören: - ein systematischer Prozess zur Beantragung und Genehmigung der Einrichtung von Benutzern IDs und der Zugangsko ntrollmatrix - Durchführung einer Risikobewertung und Gewährung von Zugriffsrechten auf dieser Grundlage. - Implementierung einer rollenbasierten Zugriffskontrolle zur Sicherstellung einer effektiven Aufgabent rennung - Änderung von Standardb enutzernamen and/ or passwords of systems and prohibiti ng sharing of user IDs and passwords of generic accounts - Modification of access rights whenever there	securityhub-enabled	AWS Security Hub hilft bei der Überwachung von unbefugtem Personal, Verbindun gen, Geräten und Software. AWS Security Hub aggregiert, organisie rt und priorisie rt die Sicherhei tswarnungen oder Ergebnisse mehrerer Dienste. AWS Einige dieser Dienste sind Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer und AWS Firewall Manager sowie AWS Partnerlösungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
	is a change in role or responsibility and removal of access rights on cessation of employment/ contract - Verfahren zur rechtzeitigen Benachrichtigung der Informationssicher heitsfunktion über hinzugefügte, gelöschte und Rollenänderungen von Benutzern - Regelmäßiger Abgleich von Benutzern IDs in einem System und tatsächlichen Benutzern, die Zugriff benötigen, und Löschung aller unnötigen IDs, falls vorhanden - Prüfung, Protokollierung und Überwachung des Zugriffs aller Benutzer auf IT-Ressourcen durch alle Benutzer und - Prüfung, Protokollierung und Überwachung des Zugriffs aller Benutzer auf IT-Ressourcen		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
	und - Prüfung der Deaktivierung IDs von Benutzern kritische r Anwendungen, die sind für längere Zeit beurlaubt		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
3.1.1(d)	d) Zu den wichtigen Kontrollen, die berücksichtigt werden müssen, gehören: - Ein systematischer Prozess zur Beantragung und Genehmigung der Erstellung von Benutzern IDs und der Zugriffskontrollmatrix - Durchführung einer Risikobewertung und Gewährung von Zugriffsrechten auf dieser Grundlage. - Implementierung einer rollenbasierten Zugriffskontrolle zur Sicherstellung einer effektiven Aufgabentrennung - Änderung von Standardbenutzernamen and/or passwords of systems and prohibiting sharing of user IDs and passwords of generic accounts - Modification of access rights whenever there is a change in role or responsibility and	vpc-flow-logs-enabled	VPC-Flow-Protokolle erfassen detaillierte Informationsdatensätze über den IP-Datenverkehr, der zu und von Netzwerkschnittstellen in Ihrer Amazon Virtual Private Cloud (Amazon VPC) fließt. Standardmäßig enthalten Flow-Protokolldatensätze Werte für die verschiedenen Komponenten des IP-Flows, einschließlich Quelle, Ziel und Protokoll.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
	removal of access rights on cessation of employment/ contract - Verfahren zur rechtzeitigen Benachrichtigung der Informationssicher heitsfunktion über hinzugefügte, gelöschte und Rollenänderungen von Benutzern - Regelmäßiger Abgleich von Benutzern IDs in einem System und tatsächlichen Benutzern, die Zugriff benötigen, und Löschung aller unnötigen IDs, falls vorhanden - Prüfung, Protokollierung und Überwachung des Zugriffs aller Benutzer auf IT-Ressourcen durch alle Benutzer und - Prüfung, Protokollierung und Überwachung des Zugriffs aller Benutzer auf IT-Ressourcen und - Prüfung der Deaktivierung IDs von		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
	Benutzern kritische r Anwendungen, die sind für längere Zeit beurlaubt		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
3.1.1(d)	d) Zu den wichtigen Kontrollen, die in Betracht gezogen werden müssen, gehören: - ein systematischer Prozess zur Beantragung und Genehmigung der Einrichtung von Benutzern IDs und der Zugangskontrollmatrix - Durchführung einer Risikobewertung und auf deren Grundlage die Gewährung von Zugriffsrechten. - Implementierung einer rollenbasierten Zugriffskontrolle zur Sicherstellung einer effektiven Aufgabentrennung - Änderung von Standardbenutzernamen and/or passwords of systems and prohibiting sharing of user IDs and passwords of generic accounts - Modification of access rights whenever there	cw-loggroup-retention-period-überprüfen	Stellen Sie sicher, dass die Ereignisprotokolldaten für Ihre Protokollgruppen über eine Mindestdauer aufbewahrt werden, um die Fehlerbehebung und forensische Untersuchungen zu unterstützen. Fehlende frühere Ereignisprotokolldaten erschweren die Rekonstruierung und Identifizierung potenziell schädlicher Ereignisse.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
	is a change in role or responsibility and removal of access rights on cessation of employment/ contract - Verfahren zur rechtzeitigen Benachrichtigung der Informationssicher heitsfunktion über hinzugefügte, gelöschte und Rollenänderungen von Benutzern - Regelmäßiger Abgleich von Benutzern IDs in einem System und tatsächlichen Benutzern, die Zugriff benötigen, und Löschung aller unnötigen IDs, falls vorhanden - Prüfung, Protokollierung und Überwachung des Zugriffs aller Benutzer auf IT-Ressourcen durch alle Benutzer und - Prüfung, Protokollierung und Überwachung des Zugriffs aller Benutzer auf IT-Ressourcen		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
	und - Prüfung der Deaktivierung IDs von Benutzern kritische r Anwendungen, die sind für längere Zeit beurlaubt		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
3.1.1(d)	d) Zu den wichtigen Kontrollen, die berücksichtigt werden müssen, gehören: - ein systematischer Prozess zur Beantragung und Genehmigung der Einrichtung von Benutzern IDs und der Zugangskontrollmatrix - Durchführung einer Risikobewertung und auf deren Grundlage die Gewährung von Zugriffsrechten. - Implementierung einer rollenbasierten Zugriffskontrolle zur Sicherstellung einer effektiven Aufgabentrennung - Änderung von Standardbenutzernamen and/or passwords of systems and prohibiting sharing of user IDs and passwords of generic accounts - Modification of access rights whenever there is a change in role	rds-logging-enabled	Um die Protokollierung und Überwachung in Ihrer Umgebung zu erleichtern, stellen Sie sicher, dass die Amazon Relational Database Service (Amazon RDS)-Protokollierung aktiviert ist. Mit der Amazon-RDS-Protokollierung können Sie Ereignisse wie Verbindungen, Verbindungsabbrüche, Abfragen oder abgefragte Tabellen erfassen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
	or responsibility and removal of access rights on cessation of employment/ contract - Verfahren zur rechtzeitigen Benachrichtigung der Informationssicher heitsfunktion über hinzugefügte, gelöschte und Rollenänderungen von Benutzern - Regelmäßiger Abgleich von Benutzern IDs in einem System und tatsächlichen Benutzern, die Zugriff benötigen, und Löschung aller unnötigen IDs, falls vorhanden - Prüfung, Protokollierung und Überwachung des Zugriffs aller Benutzer auf IT-Ressourcen durch alle Benutzer und - Prüfung, Protokollierung und Überwachung des Zugriffs aller Benutzer auf IT-Ressourcen und - Prüfung der		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
	Deaktivierung IDs von Benutzern kritische r Anwendungen, die sind für längere Zeit beurlaubt		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
3.1.1(d)	d) Zu den wichtigen Kontrollen, die in Betracht gezogen werden müssen, gehören: - ein systematischer Prozess zur Beantragung und Genehmigung der Einrichtung von Benutzern IDs und der Zugangskontrollmatrix - Durchführung einer Risikobewertung und auf deren Grundlage die Gewährung von Zugriffsrechten. - Implementierung einer rollenbasierten Zugriffskontrolle zur Sicherstellung einer effektiven Aufgabentrennung - Änderung von Standardbenutzernamen and/or passwords of systems and prohibiting sharing of user IDs and passwords of generic accounts - Modification of access rights whenever there	wafv2-logging-enabled	Um die Protokollierung und Überwachung in Ihrer Umgebung zu erleichtern, aktivieren Sie die AWS WAF (V2) -Protokollierung im regionalen und globalen Web ACLs. AWS Die WAF-Protokollierung bietet detaillierte Informationen über den Datenverkehr, der von Ihrer Web-ACL analysiert wird. In den Protokollen werden die Uhrzeit aufgezeichnet, zu der die AWS WAF die Anfrage von Ihrer AWS Ressource erhalten hat, Informationen zu der Anfrage und eine Aktion für die Regel, der jede Anfrage entsprach.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
	is a change in role or responsibility and removal of access rights on cessation of employment/ contract - Verfahren zur rechtzeitigen Benachrichtigung der Informationssicher heitsfunktion über hinzugefügte, gelöschte und Rollenänderungen von Benutzern - Regelmäßiger Abgleich von Benutzern IDs in einem System und tatsächlichen Benutzern, die Zugriff benötigen, und Löschung aller unnötigen IDs, falls vorhanden - Prüfung, Protokollierung und Überwachung des Zugriffs aller Benutzer auf IT-Ressourcen durch alle Benutzer und - Prüfung, Protokollierung und Überwachung des Zugriffs aller Benutzer auf IT-Ressourcen		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
	und - Prüfung der Deaktivierung IDs von Benutzern kritische r Anwendungen, die sind für längere Zeit beurlaubt		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
3.1.1(d)	d) Zu den wichtigen Kontrollen, die berücksichtigt werden müssen, gehören: - Ein systematischer Prozess zur Beantragung und Genehmigung der Erstellung von Benutzern IDs und der Zugriffskontrollmatrix - Durchführung einer Risikobewertung und Gewährung von Zugriffsrechten auf dieser Grundlage. - Implementierung einer rollenbasierten Zugriffskontrolle zur Sicherstellung einer effektiven Aufgabentrennung - Änderung von Standardbenutzernamen and/or passwords of systems and prohibiting sharing of user IDs and passwords of generic accounts - Modification of access rights whenever there is a change in role or responsibility and	redshift-cluster-configuration-check	Um Daten im Ruhezustand zu schützen, muss die Verschlüsselung für Ihre Amazon-Redshift-Cluster aktiviert sein. Sie müssen auch sicherstellen, dass die erforderlichen Konfigurationen auf Amazon-Redshift-Clustern bereitgestellt werden. Die Prüfungsprotokollierung muss aktiviert sein, um Informationen zu Verbindungen und Benutzeraktivitäten in der Datenbank bereitzustellen. Diese Regel erfordert, dass ein Wert für clusterDbEncrypted (Config Default: TRUE) und LoggingEnabled (Config Default: TRUE) gesetzt ist. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
	removal of access rights on cessation of employment/ contract - Verfahren zur rechtzeitigen Benachrichtigung der Informationssicher heitsfunktion über hinzugefügte, gelöschte und Rollenänderungen von Benutzern - Regelmäßiger Abgleich von Benutzern IDs in einem System und tatsächlichen Benutzern, die Zugriff benötigen, und Löschung aller unnötigen IDs, falls vorhanden - Prüfung, Protokollierung und Überwachung des Zugriffs aller Benutzer auf IT-Ressourcen durch alle Benutzer und - Prüfung, Protokollierung und Überwachung des Zugriffs aller Benutzer auf IT-Ressourcen und - Prüfung der Deaktivierung IDs von		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
	Benutzern kritische r Anwendungen, die sind für längere Zeit beurlaubt		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
3.1.1(d)	d) Zu den wichtigen Kontrollen, die berücksichtigt werden müssen, gehören: - Ein systematischer Prozess zur Beantragung und Genehmigung der Erstellung von Benutzern IDs und der Zugriffskontrollmatrix - Durchführung einer Risikobewertung und Gewährung von Zugriffsrechten auf dieser Grundlage. - Implementierung einer rollenbasierten Zugriffskontrolle zur Sicherstellung einer effektiven Aufgabentrennung - Änderung von Standardbenutzernamen and/or passwords of systems and prohibiting sharing of user IDs and passwords of generic accounts - Modification of access rights whenever there is a change in role or responsibility and	iam-user-unused-credentials-überprüfen	AWS Identity and Access Management (IAM) kann Ihnen bei Zugriffsberechtigungen und Autorisierungen helfen, indem es nach IAM-Passwörtern und Zugriffsschlüsseln sucht, die für einen bestimmten Zeitraum nicht verwendet wurden. Wenn ungenutzte Anmeldeinformationen identifiziert werden, müssen Sie sie deaktivieren und/oder entfernen, da dies gegen das Prinzip der geringsten Berechtigung verstoßen könnte. Für diese Regel müssen Sie einen Wert für das maxCredentialUsage Alter festlegen (Standardkonfiguration: 90). Der tatsächliche Wert muss den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
	removal of access rights on cessation of employment/ contract - Verfahren zur rechtzeitigen Benachrichtigung der Informationssicher heitsfunktion über hinzugefügte, gelöschte und Rollenänderungen von Benutzern - Regelmäßiger Abgleich von Benutzern IDs in einem System und tatsächlichen Benutzern, die Zugriff benötigen, und Löschung aller unnötigen IDs, falls vorhanden - Prüfung, Protokollierung und Überwachung des Zugriffs aller Benutzer auf IT-Ressourcen durch alle Benutzer und - Prüfung, Protokollierung und Überwachung des Zugriffs aller Benutzer auf IT-Ressourcen und - Prüfung der Deaktivierung IDs von		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
	Benutzern kritische r Anwendungen, die sind für längere Zeit beurlaubt		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
3.1.1(d)	d) Zu den wichtigen Kontrollen, die berücksichtigt werden müssen, gehören: - Ein systematischer Prozess zur Beantragung und Genehmigung der Erstellung von Benutzern IDs und der Zugriffskontrollmatrix - Durchführung einer Risikobewertung und Gewährung von Zugriffsrechten auf dieser Grundlage. - Implementierung einer rollenbasierten Zugriffskontrolle zur Sicherstellung einer effektiven Aufgabentrennung - Änderung von Standardbenutzernamen and/or passwords of systems and prohibiting sharing of user IDs and passwords of generic accounts - Modification of access rights whenever there is a change in role or responsibility and	account-part-of-organizations	Durch die zentrale Verwaltung AWS-Konten innerhalb von AWS Organizations wird sichergestellt, dass die Konten den Vorschriften entsprechen. Eine fehlende zentrale Kontoverwaltung kann zu inkonsistenten Kontokonfigurationen führen, wodurch Ressourcen und sensible Daten offengelegt werden können.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
	removal of access rights on cessation of employment/ contract - Verfahren zur rechtzeitigen Benachrichtigung der Informationssicher heitsfunktion über hinzugefügte, gelöschte und Rollenänderungen von Benutzern - Regelmäßiger Abgleich von Benutzern IDs in einem System und tatsächlichen Benutzern, die Zugriff benötigen, und Löschung aller unnötigen IDs, falls vorhanden - Prüfung, Protokollierung und Überwachung des Zugriffs aller Benutzer auf IT-Ressourcen durch alle Benutzer und - Prüfung, Protokollierung und Überwachung des Zugriffs aller Benutzer auf IT-Ressourcen und - Prüfung der Deaktivierung IDs von		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
	Benutzern kritische r Anwendungen, die sind für längere Zeit beurlaubt		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
3.1.1(d)	d) Zu den wichtigen Kontrollen, die berücksichtigt werden müssen, gehören: - ein systematischer Prozess, bei dem die Erstellung einer Benutzer- und Zugriffskontrollmatrix beantragt IDs und genehmigt wird - die Durchführung einer Risikobewertung und die darauf basierende Gewährung von Zugriffsrechten. - Implementierung einer rollenbasierten Zugriffskontrolle zur Sicherstellung einer effektiven Aufgabentrennung - Änderung von Standardbenutzernamen and/or passwords of systems and prohibiting sharing of user IDs and passwords of generic accounts - Modification of access rights whenever there is a change in role or responsibility and	iam-customer-policy-blocked-KMS-Aktionen	AWS Identity and Access Management (IAM) kann Ihnen helfen, die Prinzipien der geringsten Rechte und der Aufgabentrennung in Zugriffsberechtigungen und Autorisierungen zu integrieren und so zu verhindern, dass Richtlinien blockierte Aktionen für alle AWS Schlüssel des Key Management Service enthalten. Wenn Benutzer mehr Rechte haben, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und Aufgabentrennung verstoßen. Mit dieser Regel können Sie den Parameter festlegen. blockedActionsPatterns (Wert „AWS Bewährte grundlegende Sicherheitsmethode

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
	removal of access rights on cessation of employment/ contract - Verfahren zur rechtzeitigen Benachrichtigung der Informationssicher heitsfunktion über hinzugefügte, gelöschte und Rollenänderungen von Benutzern - Regelmäßiger Abgleich von Benutzern IDs in einem System und tatsächlichen Benutzern, die Zugriff benötigen, und Löschung aller unnötigen IDs, falls vorhanden - Prüfung, Protokollierung und Überwachung des Zugriffs aller Benutzer auf IT-Ressourcen durch alle Benutzer und - Prüfung, Protokollierung und Überwachung des Zugriffs aller Benutzer auf IT-Ressourcen und - Prüfung der Deaktivierung IDs von		n“: kms: Entschlüs seln, kms:ReEnc ryptFrom). Die tatsächlichen Werte müssen den Richtlini en Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
	Benutzern kritische r Anwendungen, die sind für längere Zeit beurlaubt		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
3.1.1(d)	d) Zu den wichtigen Kontrollen, die berücksichtigt werden müssen, gehören: - ein systematischer Prozess, bei dem die Erstellung einer Benutzer- und Zugriffskontrollmatrix beantragt IDs und genehmigt wird - die Durchführung einer Risikobewertung und die Gewährung von Zugriffsrechten auf dieser Grundlage. - Implementierung einer rollenbasierten Zugriffskontrolle zur Sicherstellung einer effektiven Aufgabentrennung - Änderung von Standardbenutzernamen and/or passwords of systems and prohibiting sharing of user IDs and passwords of generic accounts - Modification of access rights whenever there is a change in role or responsibility and	iam-group-has-users-überprüfen	AWS Identity and Access Management (IAM) kann Ihnen helfen, die Prinzipien der geringsten Rechte und der Aufgabentrennung mit Zugriffsberechtigungen und Autorisierungen zu integrieren, indem sichergestellt wird, dass IAM-Gruppen mindestens einen Benutzer haben. Die Einteilung von Benutzern in Gruppen auf der Grundlage der ihnen zugewiesenen Berechtigungen oder ihrer Funktion ist eine Möglichkeit, das Prinzip der geringsten Berechtigung zu implementieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
	removal of access rights on cessation of employment/ contract - Verfahren zur rechtzeitigen Benachrichtigung der Informationssicher heitsfunktion über hinzugefügte, gelöschte und Rollenänderungen von Benutzern - Regelmäßiger Abgleich von Benutzern IDs in einem System und tatsächlichen Benutzern, die Zugriff benötigen, und Löschung aller unnötigen IDs, falls vorhanden - Prüfung, Protokollierung und Überwachung des Zugriffs aller Benutzer auf IT-Ressourcen durch alle Benutzer und - Prüfung, Protokollierung und Überwachung des Zugriffs aller Benutzer auf IT-Ressourcen und - Prüfung der Deaktivierung IDs von		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
	Benutzern kritische r Anwendungen, die sind für längere Zeit beurlaubt		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
3.1.1(d)	d) Zu den wichtigen Kontrollen, die berücksichtigt werden müssen, gehören: - Ein systematischer Prozess, bei dem die Erstellung von Benutzern und der Zugriffskontrollmatrix beantragt IDs und autorisiert wird. - Durchführung einer Risikobewertung und Gewährung von Zugriffsrechten auf dieser Grundlage. - Implementierung einer rollenbasierten Zugriffskontrolle zur Sicherstellung einer effektiven Aufgabentrennung - Änderung von Standardbenutzernamen and/or passwords of systems and prohibiting sharing of user IDs and passwords of generic accounts - Modification of access rights whenever there is a change in role or responsibility and	iam-inline-policy-blocked-KMS-Aktionen	Stellen Sie sicher, dass ein Benutzer, eine IAM-Rolle oder eine IAM-Gruppe (AWS Identity and Access Management) nicht über eine Inline-Richtlinie verfügt, die blockierte Aktionen für alle AWS Schlüssel des Key Management Service zulässt. AWS empfiehlt, verwaltete Richtlinien anstelle von Inline-Richtlinien zu verwenden. Verwaltete Richtlinien ermöglichen Wiederverwendbarkeit, Versionsverwaltung, Rollback und Delegierung der Berechtigungsverwaltung. Mit dieser Regel können Sie den blockedActionsPatterns Parameter festlegen. (Wert „AWS Bewährte grundlegende Sicherheitsmethoden“: kms: Entschlüsseln, kms:ReEnc

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
	removal of access rights on cessation of employment/ contract - Verfahren zur rechtzeitigen Benachrichtigung der Informationssicher heitsfunktion über hinzugefügte, gelöschte und Rollenänderungen von Benutzern - Regelmäßiger Abgleich von Benutzern IDs in einem System und tatsächlichen Benutzern, die Zugriff benötigen, und Löschung aller unnötigen IDs, falls vorhanden - Prüfung, Protokollierung und Überwachung des Zugriffs aller Benutzer auf IT-Ressourcen durch alle Benutzer und - Prüfung, Protokollierung und Überwachung des Zugriffs aller Benutzer auf IT-Ressourcen und - Prüfung der Deaktivierung IDs von		ryptFrom). Die tatsächlichen Werte müssen den Richtlini en Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
	Benutzern kritische r Anwendungen, die sind für längere Zeit beurlaubt		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
3.1.1(d)	d) Zu den wichtigen Kontrollen, die berücksichtigt werden müssen, gehören: - ein systematischer Prozess, bei dem die Erstellung einer Benutzer- und Zugriffskontrollmatrix beantragt IDs und genehmigt wird - die Durchführung einer Risikobewertung und die Gewährung von Zugriffsrechten auf dieser Grundlage. - Implementierung einer rollenbasierten Zugriffskontrolle zur Sicherstellung einer effektiven Aufgabentrennung - Änderung von Standardbenutzernamen and/or passwords of systems and prohibiting sharing of user IDs and passwords of generic accounts - Modification of access rights whenever there is a change in role or responsibility and	iam-user-group-membership-überprüfen	AWS Identity and Access Management (IAM) kann Ihnen helfen, Zugriffsberechtigungen und Autorisierungen einzuschränken, indem sichergestellt wird, dass Benutzer Mitglieder mindestens einer Gruppe sind. Wenn Benutzern mehr Berechtigungen eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und Aufgabentrennung verstoßen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
	removal of access rights on cessation of employment/ contract - Verfahren zur rechtzeitigen Benachrichtigung der Informationssicher heitsfunktion über hinzugefügte, gelöschte und Rollenänderungen von Benutzern - Regelmäßiger Abgleich von Benutzern IDs in einem System und tatsächlichen Benutzern, die Zugriff benötigen, und Löschung aller unnötigen IDs, falls vorhanden - Prüfung, Protokollierung und Überwachung des Zugriffs aller Benutzer auf IT-Ressourcen durch alle Benutzer und - Prüfung, Protokollierung und Überwachung des Zugriffs aller Benutzer auf IT-Ressourcen und - Prüfung der Deaktivierung IDs von		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
	Benutzern kritische r Anwendungen, die sind für längere Zeit beurlaubt		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
3.1.1(d)	d) Zu den wichtigen Kontrollen, die berücksichtigt werden müssen, gehören: - Ein systematischer Prozess zur Beantragung und Autorisierung der Erstellung von Benutzern IDs und der Zugriffskontrollmatrix - Durchführung einer Risikobewertung und Gewährung von Zugriffsrechten auf dieser Grundlage. - Implementierung einer rollenbasierten Zugriffskontrolle zur Sicherstellung einer effektiven Aufgabentrennung - Änderung von Standardbenutzernamen and/or passwords of systems and prohibiting sharing of user IDs and passwords of generic accounts - Modification of access rights whenever there is a change in role or responsibility and	ec-2 instance-profile-attached	EC2 Instanzprofile übergeben eine IAM-Rolle an eine EC2 Instance. Das Anhängen eines Instance-Profils an Ihre Instances kann bei der Implementierung von geringsten Berechtigungen und der Berechtigungsverwaltung helfen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
	removal of access rights on cessation of employment/ contract - Verfahren zur rechtzeitigen Benachrichtigung der Informationssicher heitsfunktion über hinzugefügte, gelöschte und Rollenänderungen von Benutzern - Regelmäßiger Abgleich von Benutzern IDs in einem System und tatsächlichen Benutzern, die Zugriff benötigen, und Löschung aller unnötigen IDs, falls vorhanden - Prüfung, Protokollierung und Überwachung des Zugriffs aller Benutzer auf IT-Ressourcen durch alle Benutzer und - Prüfung, Protokollierung und Überwachung des Zugriffs aller Benutzer auf IT-Ressourcen und - Prüfung der Deaktivierung IDs von		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
	Benutzern kritische r Anwendungen, die sind für längere Zeit beurlaubt		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
3.1.1(d)	d) Zu den wichtigen Kontrollen, die berücksichtigt werden müssen, gehören: - ein systematischer Prozess zur Beantragung und Genehmigung der Erstellung von Benutzern IDs und der Zugriffskontrollmatrix - Durchführung einer Risikobewertung und Gewährung von Zugriffsrechten auf dieser Grundlage. - Implementierung einer rollenbasierten Zugriffskontrolle zur Sicherstellung einer effektiven Aufgabentrennung - Änderung von Standardbenutzernamen and/or passwords of systems and prohibiting sharing of user IDs and passwords of generic accounts - Modification of access rights whenever there is a change in role or responsibility and	iam-policy-no-statements-with-full-access	Stellen Sie sicher, dass IAM-Aktionen nur auf die benötigten Aktionen beschränkt sind. Wenn Benutzern mehr Rechte eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Rechte und der Aufgabentrennung verstoßen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
	removal of access rights on cessation of employment/ contract - Verfahren zur rechtzeitigen Benachrichtigung der Informationssicher heitsfunktion über hinzugefügte, gelöschte und Rollenänderungen von Benutzern - Regelmäßiger Abgleich von Benutzern IDs in einem System und tatsächlichen Benutzern, die Zugriff benötigen, und Löschung aller unnötigen IDs, falls vorhanden - Prüfung, Protokollierung und Überwachung des Zugriffs aller Benutzer auf IT-Ressourcen durch alle Benutzer und - Prüfung, Protokollierung und Überwachung des Zugriffs aller Benutzer auf IT-Ressourcen und - Prüfung der Deaktivierung IDs von		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
	Benutzern kritische r Anwendungen, die sind für längere Zeit beurlaubt		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
3.1.1(d)	d) Zu den wichtigen Kontrollen, die in Betracht gezogen werden müssen, gehören: - ein systematischer Prozess zur Beantragung und Genehmigung der Einrichtung von Benutzern IDs und der Zugangskontrollmatrix - Durchführung einer Risikobewertung und auf deren Grundlage die Gewährung von Zugriffsrechten. - Implementierung einer rollenbasierten Zugriffskontrolle zur Sicherstellung einer effektiven Aufgabentrennung - Änderung von Standardbenutzernamen and/or passwords of systems and prohibiting sharing of user IDs and passwords of generic accounts - Modification of access rights whenever there	ecs-task-definition-user-for-host-mode-check	Wenn für eine Aufgabendefinition erhöhte Berechtigungen gelten, liegt das daran, dass der Kunde diesen Konfigurationen ausdrücklich zugestimmt hat. Diese Kontrolle prüft, ob eine unerwartete Berechtigungseskalation vorliegt, wenn für eine Aufgabendefinition das Host-Netzwerk aktiviert ist, die Kunden aber keine erhöhten Berechtigungen aktiviert haben.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
	is a change in role or responsibility and removal of access rights on cessation of employment/ contract - Verfahren zur rechtzeitigen Benachrichtigung der Informationssicher heitsfunktion über hinzugefügte, gelöschte und Rollenänderungen von Benutzern - Regelmäßiger Abgleich von Benutzern IDs in einem System und tatsächlichen Benutzern, die Zugriff benötigen, und Löschung aller unnötigen IDs, falls vorhanden - Prüfung, Protokollierung und Überwachung des Zugriffs aller Benutzer auf IT-Ressourcen durch alle Benutzer und - Prüfung, Protokollierung und Überwachung des Zugriffs aller Benutzer auf IT-Ressourcen		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
	und - Prüfung der Deaktivierung IDs von Benutzern kritische r Anwendungen, die sind für längere Zeit beurlaubt		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
3.1.1(d)	d) Zu den wichtigen Kontrollen, die in Betracht gezogen werden müssen, gehören: - ein systematischer Prozess zur Beantragung und Genehmigung der Einrichtung von Benutzern IDs und der Zugangskontrollmatrix - Durchführung einer Risikobewertung und auf deren Grundlage die Gewährung von Zugriffsrechten. - Implementierung einer rollenbasierten Zugriffskontrolle zur Sicherstellung einer effektiven Aufgabentrennung - Änderung von Standardbenutzernamen and/or passwords of systems and prohibiting sharing of user IDs and passwords of generic accounts - Modification of access rights whenever there	elasticsearch-logs-to-cloudwatch	Stellen Sie sicher, dass für Amazon OpenSearch Service-Domains Fehlerprotokolle aktiviert und zur Aufbewahrung und Beantwortung an Amazon CloudWatch Logs gestreamt werden. Domain-Fehlerprotokolle sind bei Sicherheits- und Zugriffsprüfungen sowie bei der Diagnose von Verfügbarkeitsproblemen nützlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
	is a change in role or responsibility and removal of access rights on cessation of employment/ contract - Verfahren zur rechtzeitigen Benachrichtigung der Informationssicher heitsfunktion über hinzugefügte, gelöschte und Rollenänderungen von Benutzern - Regelmäßiger Abgleich von Benutzern IDs in einem System und tatsächlichen Benutzern, die Zugriff benötigen, und Löschung aller unnötigen IDs, falls vorhanden - Prüfung, Protokollierung und Überwachung des Zugriffs aller Benutzer auf IT-Ressourcen durch alle Benutzer und - Prüfung, Protokollierung und Überwachung des Zugriffs aller Benutzer auf IT-Ressourcen		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
	und - Prüfung der Deaktivierung IDs von Benutzern kritische r Anwendungen, die sind für längere Zeit beurlaubt		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
3.1.1(d)	d) Zu den wichtigen Kontrollen, die berücksichtigt werden müssen, gehören: - Ein systematischer Prozess zur Beantragung und Genehmigung der Erstellung von Benutzern IDs und der Zugriffskontrollmatrix - Durchführung einer Risikobewertung und Gewährung von Zugriffsrechten auf dieser Grundlage. - Implementierung einer rollenbasierten Zugriffskontrolle zur Sicherstellung einer effektiven Aufgabentrennung - Änderung von Standardbenutzernamen and/or passwords of systems and prohibiting sharing of user IDs and passwords of generic accounts - Modification of access rights whenever there is a change in role or responsibility and	opensearch-logs-to-cloudwatch	Stellen Sie sicher, dass für Amazon OpenSearch Service-Domains Fehlerprotokolle aktiviert und zur Aufbewahrung und Beantwortung an Amazon CloudWatch Logs gestreamt werden. OpenSearch Service-Fehlerprotokolle können bei Sicherheits- und Zugriffsprüfungen helfen und bei der Diagnose von Verfügbarkeitsproblemen helfen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
	removal of access rights on cessation of employment/ contract - Verfahren zur rechtzeitigen Benachrichtigung der Informationssicher heitsfunktion über hinzugefügte, gelöschte und Rollenänderungen von Benutzern - Regelmäßiger Abgleich von Benutzern IDs in einem System und tatsächlichen Benutzern, die Zugriff benötigen, und Löschung aller unnötigen IDs, falls vorhanden - Prüfung, Protokollierung und Überwachung des Zugriffs aller Benutzer auf IT-Ressourcen durch alle Benutzer und - Prüfung, Protokollierung und Überwachung des Zugriffs aller Benutzer auf IT-Ressourcen und - Prüfung der Deaktivierung IDs von		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
	Benutzern kritische r Anwendungen, die sind für längere Zeit beurlaubt		
3.1.1(f)	f) Stellen Sie zur Erfüllung der Rechenschaftspflicht sicher, dass Benutzer und IT-Ressourcen eindeutig identifiz iert werden und ihre Aktionen überprüfbar sind.	cloudtrail-enabled	AWS CloudTrai l kann durch die Aufzeichnung von Aktionen und API-Aufrufen in der AWS Management Console bei der Nichtabst reitbarkeit helfen. Sie können die Benutzer und die Benutzer AWS-Konten , die einen AWS Dienst aufgerufen haben, die Quell-IP-Adresse, über die die Aufrufe generiert wurden, und den Zeitpunkt der Anrufe identifiz ieren. Einzelheiten zu den erfassten Daten finden Sie in den AWS CloudTrail Datensatzinhalten.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
3.1.1(f)	f) Stellen Sie zur Erfüllung der Rechenschaftspflicht sicher, dass Benutzer und IT-Ressourcen eindeutig identifiz iert werden und ihre Aktionen überprüfbar sind.	multi-region-cloudtrail-enabled	AWS CloudTrail zeichnet Aktionen und API-Aufrufe der AWS Management Console auf. Sie können feststellen, welche Benutzer und Konten angerufen wurden AWS, von welcher Quell-IP-Adresse aus die Anrufe getätigt wurden und wann die Anrufe erfolgten. CloudTrail übermittelt Protokolldateien aus allen AWS Regionen an Ihren S3-Bucket , wenn MULTI_REG ION_CLOUD _TRAIL_ENABLED aktiviert ist. Außerdem wird beim AWS Start einer neuen Region derselbe Trail in der neuen Region erstellt. CloudTrail Dadurch erhalten Sie automatis ch Protokolldateien mit API-Aktivitäten für die neue Region.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
3.1.1(f)	f) Stellen Sie zur Erfüllung der Rechenschaftspflicht sicher, dass Benutzer und IT-Ressourcen eindeutig identifiziert werden und ihre Aktionen überprüfbar sind.	opensearch-audit-logging-enabled	Stellen Sie sicher, dass die Audit-Protokollierung für Ihre Amazon OpenSearch Service-Domains aktiviert ist. Mit der Audit-Protokollierung können Sie Benutzeraktivitäten auf Ihren OpenSearch Domains verfolgen, einschließlich erfolgreicher und fehlgeschlagener Authentifizierungen OpenSearch, Anfragen an, Indexänderungen und eingehende Suchanfragen.
3.1.1(f)	f) Stellen Sie zur Erfüllung der Rechenschaftspflicht sicher, dass Benutzer und IT-Ressourcen eindeutig identifiziert werden und ihre Aktionen überprüfbar sind.	redshift-audit-logging-enabled	Aktivieren Sie die Prüfungsprotokollierung, um Informationen über Verbindungen und Benutzeraktivitäten in Ihrem Amazon-Redshift-Cluster zu erfassen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
3.1.1(f)	f) Stellen Sie zur Erfüllung der Rechenschaftspflicht sicher, dass Benutzer und IT-Ressourcen eindeutig identifiz iert werden und ihre Aktionen überprüfbar sind.	redshift-cluster-c onfiguration-check	Um Daten im Ruhezustand zu schützen, muss die Verschlüsselung für Ihre Amazon-Re dshift-Cluster aktiviert sein. Sie müssen auch sicherstellen, dass die erforderl ichen Konfigurationen auf Amazon-Redshift-Clustern bereitges tellt werden. Die Prüfungsprotokolli erung muss aktiviert sein, um Informati onen zu Verbindun gen und Benutzera ktivitäten in der Datenbank bereitzus tellen. Diese Regel erfordert, dass ein Wert für clusterDb Encrypted (Config Default: TRUE) und LoggingEnabled (Config Default: TRUE) gesetzt ist. Die tatsächlichen Werte müssen den Richtlini en Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
3.1.1(f)	f) Stellen Sie zur Erfüllung der Rechenschaftspflicht sicher, dass Benutzer und IT-Ressourcen eindeutig identifiz iert werden und ihre Aktionen überprüfbar sind.	elasticsearch-logs-to-cloudwatch	Stellen Sie sicher, dass für Amazon OpenSearch Service-Domains Fehlerpro tokolle aktiviert und zur Aufbewahrung und Beantwortung an Amazon CloudWatc h Logs gestreamt werden. Domain-Fehlerprotokolle sind bei Sicherhei ts- und Zugriffsp rüfungen sowie bei der Diagnose von Verfügbarkeitsprob lemen nützlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
3.1.1(f)	f) Stellen Sie zur Erfüllung der Rechenschaftspflicht sicher, dass Benutzer und IT-Ressourcen eindeutig identifiziert werden und ihre Aktionen überprüfbar sind.	opensearch-logs-to-cloudwatch	Stellen Sie sicher, dass für Amazon OpenSearch Service-Domains Fehlerprotokolle aktiviert und zur Aufbewahrung und Beantwortung an Amazon CloudWatch Logs gestreamt werden. OpenSearch Service-Fehlerprotokolle können bei Sicherheits- und Zugriffsprüfungen helfen und bei der Diagnose von Verfügbarkeitsproblemen helfen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
3.1.1(h)	h) Systemadministratoren, Sicherheitsbeauftragte, Programmierer und Mitarbeiter, die kritische Vorgänge durchführen, können aufgrund ihrer Aufgaben und ihres privilegierten Zugriffs den von ihnen unterhaltenen oder betriebenen Finanzsystemen schweren Schaden zuzufügen. Mitarbeiter mit erhöhten Systemzugriffsberechtigungen sollten engmaschig beaufsichtigt und alle ihre Systemaktivitäten protokolliert werden, da sie über Insiderwissen und die nötigen Ressourcen verfügen, um Systemkontrollen und Sicherheitsverfahren zu umgehen. Einige der unten aufgeführten Kontroll- und Sicherheitspraktiken	access-keys-rotated	Die Anmeldeinformationen für autorisierte Geräte, Benutzer und Prozesse werden geprüft, indem sichergestellt wird, dass die IAM-Zugriffsschlüssel entsprechend den Vorgaben der Unternehmensrichtlinien rotiert werden. Das regelmäßige Ändern der Zugriffsschlüssel ist eine bewährte Sicherheitsmethode. Es verkürzt den Zeitraum, in dem ein Zugriffsschlüssel aktiv ist, und reduziert die Auswirkungen auf das Unternehmen, wenn die Schlüssel kompromittiert werden. Diese Regel erfordert einen Wert für die Zugriffsschlüssel-Rotation (Standardkonfiguration: 90). Der tatsächliche Wert muss den Richtlini

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
	müssen berücksichtigt werden: - Implementierung einer Zwei-Faktor-Authentifizierung für privilegierte Benutzer - Einführung strenger Kontrollen des Fernzugriffs durch privilegierte Benutzer - Beschränkung der Anzahl privilegierter Benutzer - Gewährung von privilegierten Zugriffen auf „" oder "need-to-haveneed-to-do“ -Basis - Aufrechterhaltung der Audit-Protokollierung der von privilegierten Benutzern ausgeführten Systemaktivitäten - Sicherstellung, dass privilegierte Benutzer keinen Zugriff auf Systemprotokolle haben, in denen ihre Aktivitäten erfasst werden - Durchführung regelmäßiger Audits oder Managementüberprüfungen der Protokolle — Verbot		en Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
	der Weitergabe von privilegierten Daten IDs und deren Zugangsco des — Verbot des privilegierten Zugriffs auf Systeme ohne genaue Überwachu ng und Überwachu ng und _ Schutz von Backup-Daten vor unbefugtem Zugriff		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
3.1.1(h)	h) Systemadm inistratoren, Sicherhei tsbeauftragte, Programmierer und Mitarbeiter, die kritische Vorgänge durchführen, können aufgrund ihrer Aufgaben und ihres privilegierten Zugriffs den von ihnen unterhaltenen oder betriebenen Finanzsystemen schweren Schaden zuzufügen. Mitarbeit er mit erhöhten Systemzugriffsbere chtigungen sollten engmaschig beaufsich tigt und alle ihre Systemaktivitäten protokolliert werden, da sie über Insiderwi ssen und die nötigen Ressourcen verfügen, um Systemkon trollen und Sicherhei tsverfahren zu umgehen. Einige der unten aufgeführ ten Kontroll- und Sicherheitspraktiken	emr-kerberos-enabled	Die Zugriffsberechtigu ngen und -autorisi erungen können verwaltet und nach den Prinzipien der geringsten Berechtig ung und Aufgabent rennung integrier t werden, indem Kerberos für Amazon-EMR-Cluster aktiviert wird. In Kerberos werden Services und Benutzer, die sich authentif izieren müssen, als Prinzipale bezeichnet. Prinzipal e befinden sich in einem Kerberos-Bereich. Innerhalb dieses Bereichs wird ein Kerberos-Server als Key Distribution Center (KDC) bezeichnet. Über diesen Server können sich Prinzipal e authentifizieren. Die Authentifizierung im KDC erfolgt durch die Ausstellu ng von Authentif

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
	müssen berücksichtigt werden: - Implementierung einer Zwei-Faktor-Authentifizierung für privilegierte Benutzer - Einführung strenger Kontrollen des Fernzugriffs durch privilegierte Benutzer - Beschränkung der Anzahl privilegierter Benutzer - Gewährung von privilegierten Zugriffen auf „" oder "need-to-haveneed-to-do“ -Basis - Aufrechterhaltung der Audit-Protokollierung der von privilegierten Benutzern ausgeführten Systemaktivitäten - Sicherstellung, dass privilegierte Benutzer keinen Zugriff auf Systemprotokolle haben, in denen ihre Aktivitäten erfasst werden - Durchführung regelmäßiger Audits oder Managementüberprüfungen der Protokolle — Verbot		izierungstickets. Das KDC unterhält eine Datenbank der Prinzipale in seinem Bereich mit ihren Passwörtern und anderen administrativen Informationen zu jedem Prinzipal.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
	der Weitergabe von privilegierten Daten IDs und deren Zugangsco des — Verbot des privilegierten Zugriffs auf Systeme ohne genaue Überwachu ng und Überwachu ng und _ Schutz von Backup-Daten vor unbefugtem Zugriff		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
3.1.1(h)	h) Systemadm inistratoren, Sicherhei tsbeauftragte, Programmierer und Mitarbeiter, die kritische Vorgänge durchführen, können aufgrund ihrer Aufgaben und ihres privilegierten Zugriffs den von ihnen unterhaltenen oder betriebenen Finanzsystemen schweren Schaden zuzufügen. Mitarbeit er mit erhöhten Systemzugriffsbere chtigungen sollten engmaschig beaufsich tigt und alle ihre Systemaktivitäten protokolliert werden, da sie über Insiderwi ssen und die nötigen Ressourcen verfügen, um Systemkon trollen und Sicherhei tsverfahren zu umgehen. Einige der unten aufgeführ ten Kontroll- und Sicherheitspraktiken	iam-password-policy	Die Identitäten und Anmeldeinformation en werden auf der Grundlage einer organisatorischen IAM-Passwortrichtlinie ausgestellt, verwaltet und verifiziert. Sie erfüllen oder übertreff en die Anforderungen von NIST SP 800-63 und dem Standard AWS Foundatio nal Security Best Practices für die Passwortstärke. Mit dieser Regel können Sie optional RequireUppercaseCh aracters (Wert für AWS grundlegende Sicherheitsbewährt e Methoden: wahr), RequireLowercaseCh aracters (Wert für bewährte Methoden für AWS grundlege nde Sicherheit: wahr), RequireSy mbols (Wert für bewährte Methoden für AWS grundlege nde Sicherheit:

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
	müssen berücksichtigt werden: - Implementierung einer Zwei-Faktor-Authentifizierung für privilegierte Benutzer - Einführung strenger Kontrollen des Fernzugriffs durch privilegierte Benutzer - Beschränkung der Anzahl privilegierter Benutzer - Gewährung von privilegierten Zugriffen auf „" oder "need-to-haveneed-to-do“ -Basis - Aufrechterhaltung der Audit-Protokollierung der von privilegierten Benutzern ausgeführten Systemaktivitäten - Sicherstellung, dass privilegierte Benutzer keinen Zugriff auf Systemprotokolle haben, in denen ihre Aktivitäten erfasst werden - Durchführung regelmäßiger Audits oder Managementüberprüfungen der Protokolle — Verbot		wahr), RequireNumbers (Wert für bewährte Methoden für AWS grundlegende Sicherheit: wahr), MinimumPasswordLength (Wert für bewährte Methoden für AWS grundlegende Sicherheit: 14), PasswordReusePrevention (Wert für bewährte Methoden für AWS grundlegende Sicherheit: 24) und MaxPasswordAge (Wert für bewährte Methoden für AWS grundlegende Sicherheit: 90) für Ihr IAM festlegen Kennwortrichtlinie. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
	der Weitergabe von privilegierten Daten IDs und deren Zugangsco des — Verbot des privilegierten Zugriffs auf Systeme ohne genaue Überwachu ng und Überwachu ng und _ Schutz von Backup-Daten vor unbefugtem Zugriff		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
3.1.1(h)	h) Systemadministratoren, Sicherheitsbeauftragte, Programmierer und Mitarbeiter, die kritische Vorgänge durchführen, können aufgrund ihrer Aufgaben und ihres privilegierten Zugriffs den von ihnen unterhaltenen oder betriebenen Finanzsystemen schweren Schaden zuzufügen. Mitarbeiter mit erhöhten Systemzugriffsberechtigungen sollten engmaschig beaufsichtigt und alle ihre Systemaktivitäten protokolliert werden, da sie über Insiderwissen und die nötigen Ressourcen verfügen, um Systemkontrollen und Sicherheitsverfahren zu umgehen. Einige der unten aufgeführten Kontroll- und Sicherheitspraktiken	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) kann Ihnen dabei helfen, die Prinzipien der geringsten Rechte und der Aufgabentrennung in Zugriffsberechtigungen und Autorisierungen zu integrieren und so zu verhindern, dass Richtlinien „Effect“: „Allow“ mit „Action“: „*“ anstelle von „Resource“: „*“ enthalten. Wenn Benutzern mehr Rechte eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und der Aufgabentrennung verstoßen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
	müssen berücksichtigt werden: - Implementierung einer Zwei-Faktor-Authentifizierung für privilegierte Benutzer - Einführung strenger Kontrollen des Fernzugriffs durch privilegierte Benutzer - Beschränkung der Anzahl privilegierter Benutzer - Gewährung von privilegierten Zugriffen auf „" oder "need-to-haveneed-to-do“ -Basis - Aufrechterhaltung der Audit-Protokollierung der von privilegierten Benutzern ausgeführten Systemaktivitäten - Sicherstellung, dass privilegierte Benutzer keinen Zugriff auf Systemprotokolle haben, in denen ihre Aktivitäten erfasst werden - Durchführung regelmäßiger Audits oder Managementüberprüfungen der Protokolle — Verbot		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
	der Weitergabe von privilegierten Daten IDs und deren Zugangsco des — Verbot des privilegierten Zugriffs auf Systeme ohne genaue Überwachu ng und Überwachu ng und _ Schutz von Backup-Daten vor unbefugtem Zugriff		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
3.1.1(h)	h) Systemadministratoren, Sicherheitsbeauftragte, Programmierer und Mitarbeiter, die kritische Vorgänge durchführen, können aufgrund ihrer Aufgaben und ihres privilegierten Zugriffs den von ihnen unterhaltenen oder betriebenen Finanzsystemen schweren Schaden zuzufügen. Mitarbeiter mit erhöhten Systemzugriffsberechtigungen sollten engmaschig beaufsichtigt und alle ihre Systemaktivitäten protokolliert werden, da sie über Insiderwissen und die nötigen Ressourcen verfügen, um Systemkontrollen und Sicherheitsverfahren zu umgehen. Einige der unten aufgeführten Kontroll- und Sicherheitspraktiken	iam-root-access-key-überprüfen	Der Zugriff auf Systeme und Ressourcen kann gesteuert werden, indem überprüft wird, ob der Root-Benutzer keine Zugriffsschlüssel mit seiner AWS Identity and Access Management (IAM) -Rolle verknüpft hat. Stellen Sie sicher, dass die Root-Zugriffsschlüssel gelöscht werden. Erstellen und verwenden Sie stattdessen rollenbasierte Funktionen, AWS-Konten um das Prinzip der geringsten Funktionalität zu berücksichtigen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
	müssen berücksichtigt werden: - Implementierung einer Zwei-Faktor-Authentifizierung für privilegierte Benutzer - Einführung strenger Kontrollen des Fernzugriffs durch privilegierte Benutzer - Beschränkung der Anzahl privilegierter Benutzer - Gewährung von privilegierten Zugriffen auf „" oder "need-to-haveneed-to-do“ -Basis - Aufrechterhaltung der Audit-Protokollierung der von privilegierten Benutzern ausgeführten Systemaktivitäten - Sicherstellung, dass privilegierte Benutzer keinen Zugriff auf Systemprotokolle haben, in denen ihre Aktivitäten erfasst werden - Durchführung regelmäßiger Audits oder Managementüberprüfungen der Protokolle — Verbot		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
	der Weitergabe von privilegierten Daten IDs und deren Zugangsco des — Verbot des privilegierten Zugriffs auf Systeme ohne genaue Überwachu ng und Überwachu ng und _ Schutz von Backup-Daten vor unbefugtem Zugriff		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
3.1.1(h)	h) Systemadm inistratoren, Sicherhei tsbeauftragte, Programmierer und Mitarbeiter, die kritische Vorgänge durchführen, können aufgrund ihrer Aufgaben und ihres privilegierten Zugriffs den von ihnen unterhaltenen oder betriebenen Finanzsystemen schweren Schaden zuzufügen. Mitarbeit er mit erhöhten Systemzugriffsbere chtigungen sollten engmaschig beaufsich tigt und alle ihre Systemaktivitäten protokolliert werden, da sie über Insiderwi ssen und die nötigen Ressourcen verfügen, um Systemkon trollen und Sicherhei tsverfahren zu umgehen. Einige der unten aufgeführ ten Kontroll- und Sicherheitspraktiken	iam-user-mfa-enabled	Aktivieren Sie diese Regel, um den Zugriff auf Ressourcen in der Cloud einzuschr änken. AWS Diese Regel sorgt dafür, dass die Multi-Fak tor-Authentifizier ung (MFA) für alle Benutzer aktiviert ist. MFA sorgt für eine weitere Schutzebe ne zusätzlich zu den Anmeldeinformation en. Reduzieren Sie Fälle von kompromit tierten Konten, indem Sie MFA für Benutzer vorschreiben.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
	müssen berücksichtigt werden: - Implementierung einer Zwei-Faktor-Authentifizierung für privilegierte Benutzer - Einführung strenger Kontrollen des Fernzugriffs durch privilegierte Benutzer - Beschränkung der Anzahl privilegierter Benutzer - Gewährung von privilegierten Zugriffen auf „" oder "need-to-haveneed-to-do“ -Basis - Aufrechterhaltung der Audit-Protokollierung der von privilegierten Benutzern ausgeführten Systemaktivitäten - Sicherstellung, dass privilegierte Benutzer keinen Zugriff auf Systemprotokolle haben, in denen ihre Aktivitäten erfasst werden - Durchführung regelmäßiger Audits oder Managementüberprüfungen der Protokolle — Verbot		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
	der Weitergabe von privilegierten Daten IDs und deren Zugangsco des — Verbot des privilegierten Zugriffs auf Systeme ohne genaue Überwachu ng und Überwachu ng und _ Schutz von Backup-Daten vor unbefugtem Zugriff		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
3.1.1(h)	h) Systemadm inistratoren, Sicherhei tsbeauftragte, Programmierer und Mitarbeiter, die kritische Vorgänge durchführen, können aufgrund ihrer Aufgaben und ihres privilegierten Zugriffs den von ihnen unterhaltenen oder betriebenen Finanzsystemen schweren Schaden zuzufügen. Mitarbeit er mit erhöhten Systemzugriffsbere chtigungen sollten engmaschig beaufsich tigt und alle ihre Systemaktivitäten protokolliert werden, da sie über Insiderwi ssen und die nötigen Ressourcen verfügen, um Systemkon trollen und Sicherhei tsverfahren zu umgehen. Einige der unten aufgeführ ten Kontroll- und Sicherheitspraktiken	iam-user-no-policies-überprüfen	Diese Regel stellt sicher, dass AWS Identity and Access Management (IAM) -Richtlinien nur Gruppen oder Rollen zugewiese n werden, um den Zugriff auf Systeme und Ressourcen zu kontrollieren. Die Zuweisung von Berechtig ungen auf Gruppen- oder Rollenebene trägt dazu bei, die Wahrscheinlichkeit zu verringern, dass eine Identität übermäßige Berechtigungen erhält oder beibehält.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
	müssen berücksichtigt werden: - Implementierung einer Zwei-Faktor-Authentifizierung für privilegierte Benutzer - Einführung strenger Kontrollen des Fernzugriffs durch privilegierte Benutzer - Beschränkung der Anzahl privilegierter Benutzer - Gewährung von privilegierten Zugriffen auf „" oder "need-to-haveneed-to-do“ -Basis - Aufrechterhaltung der Audit-Protokollierung der von privilegierten Benutzern ausgeführten Systemaktivitäten - Sicherstellung, dass privilegierte Benutzer keinen Zugriff auf Systemprotokolle haben, in denen ihre Aktivitäten erfasst werden - Durchführung regelmäßiger Audits oder Managementüberprüfungen der Protokolle — Verbot		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
	der Weitergabe von privilegierten Daten IDs und deren Zugangsco des — Verbot des privilegierten Zugriffs auf Systeme ohne genaue Überwachu ng und Überwachu ng und _ Schutz von Backup-Daten vor unbefugtem Zugriff		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
3.1.1(h)	h) Systemadministratoren, Sicherheitsbeauftragte, Programmierer und Mitarbeiter, die kritische Vorgänge durchführen, können aufgrund ihrer Aufgaben und ihres privilegierten Zugriffs den von ihnen unterhaltenen oder betriebenen Finanzsystemen schweren Schaden zuzufügen. Mitarbeiter mit erhöhten Systemzugriffsberechtigungen sollten engmaschig beaufsichtigt und alle ihre Systemaktivitäten protokolliert werden, da sie über Insiderwissen und die nötigen Ressourcen verfügen, um Systemkontrollen und Sicherheitsverfahren zu umgehen. Einige der unten aufgeführten Kontroll- und Sicherheitspraktiken	iam-user-unused-credentials-überprüfen	AWS Identity and Access Management (IAM) kann Ihnen bei Zugriffsberechtigungen und Autorisierungen helfen, indem es nach IAM-Passwörtern und Zugriffsschlüsseln sucht, die für einen bestimmten Zeitraum nicht verwendet wurden. Wenn ungenutzte Anmeldeinformationen identifiziert werden, müssen Sie sie deaktivieren und/oder entfernen, da dies gegen das Prinzip der geringsten Berechtigung verstoßen könnte. Für diese Regel müssen Sie einen Wert für das maxCredentialUsage Alter festlegen (Standardkonfiguration: 90). Der tatsächliche Wert muss den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
	müssen berücksichtigt werden: - Implementierung einer Zwei-Faktor-Authentifizierung für privilegierte Benutzer - Einführung strenger Kontrollen des Fernzugriffs durch privilegierte Benutzer - Beschränkung der Anzahl privilegierter Benutzer - Gewährung von privilegierten Zugriffen auf „" oder "need-to-haveneed-to-do“ -Basis - Aufrechterhaltung der Audit-Protokollierung der von privilegierten Benutzern ausgeführten Systemaktivitäten - Sicherstellung, dass privilegierte Benutzer keinen Zugriff auf Systemprotokolle haben, in denen ihre Aktivitäten erfasst werden - Durchführung regelmäßiger Audits oder Managementüberprüfungen der Protokolle — Verbot		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
	der Weitergabe von privilegierten Daten IDs und deren Zugangsco des — Verbot des privilegierten Zugriffs auf Systeme ohne genaue Überwachu ng und Überwachu ng und _ Schutz von Backup-Daten vor unbefugtem Zugriff		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
3.1.1(h)	h) Systemadm inistratoren, Sicherhei tsbeauftragte, Programmierer und Mitarbeiter, die kritische Vorgänge durchführen, können aufgrund ihrer Aufgaben und ihres privilegierten Zugriffs den von ihnen unterhaltenen oder betriebenen Finanzsystemen schweren Schaden zuzufügen. Mitarbeit er mit erhöhten Systemzugriffsbere chtigungen sollten engmaschig beaufsich tigt und alle ihre Systemaktivitäten protokolliert werden, da sie über Insiderwi ssen und die nötigen Ressourcen verfügen, um Systemkon trollen und Sicherhei tsverfahren zu umgehen. Einige der unten aufgeführ ten Kontroll- und Sicherheitspraktiken	mfa-enabled-for-iam-Konsolenzugriff	Verwalten Sie den Zugriff auf Ressource n in der AWS Cloud, indem Sie sicherste llen, dass MFA für alle AWS Identity and Access Managemen t (IAM) -Benutzer aktiviert ist, die über ein Konsolenk ennwort verfügen. MFA sorgt für eine weitere Schutzebe ne zusätzlich zu den Anmeldeinformation en. Indem Sie MFA für Benutzer vorschrei ben, können Sie Fälle kompromittierter Konten reduzieren und verhindern, dass unbefugte Benutzer auf vertrauliche Daten zugreifen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
	müssen berücksichtigt werden: - Implementierung einer Zwei-Faktor-Authentifizierung für privilegierte Benutzer - Einführung strenger Kontrollen des Fernzugriffs durch privilegierte Benutzer - Beschränkung der Anzahl privilegierter Benutzer - Gewährung von privilegierten Zugriffen auf „" oder "need-to-haveneed-to-do“ -Basis - Aufrechterhaltung der Audit-Protokollierung der von privilegierten Benutzern ausgeführten Systemaktivitäten - Sicherstellung, dass privilegierte Benutzer keinen Zugriff auf Systemprotokolle haben, in denen ihre Aktivitäten erfasst werden - Durchführung regelmäßiger Audits oder Managementüberprüfungen der Protokolle — Verbot		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
	der Weitergabe von privilegierten Daten IDs und deren Zugangsco des — Verbot des privilegierten Zugriffs auf Systeme ohne genaue Überwachu ng und Überwachu ng und _ Schutz von Backup-Daten vor unbefugtem Zugriff		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
3.1.1(h)	h) Systemadministratoren, Sicherheitsbeauftragte, Programmierer und Mitarbeiter, die kritische Vorgänge durchführen, können aufgrund ihrer Aufgaben und ihres privilegierten Zugriffs den von ihnen unterhaltenen oder betriebenen Finanzsystemen schweren Schaden zuzufügen. Mitarbeiter mit erhöhten Systemzugriffsberechtigungen sollten engmaschig beaufsichtigt und alle ihre Systemaktivitäten protokolliert werden, da sie über Insiderwissen und die nötigen Ressourcen verfügen, um Systemkontrollen und Sicherheitsverfahren zu umgehen. Einige der unten aufgeführten Kontroll- und Sicherheitspraktiken	root-account-hardware-mfa-aktiviert	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Hardware-MFA für den Root-Benutzer aktiviert ist. Der Stammbenutzer ist der AWS-Konto-Benutzer mit den meisten Berechtigungen. MFA sorgt für eine weitere Schutzebene zusätzlich zu den Anmeldeinformationen. Indem Sie MFA für den Root-Benutzer vorschreiben, können Sie die Anzahl AWS-Konten kompromittierter Benutzer reduzieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
	müssen berücksichtigt werden: - Implementierung einer Zwei-Faktor-Authentifizierung für privilegierte Benutzer - Einführung strenger Kontrollen des Fernzugriffs durch privilegierte Benutzer - Beschränkung der Anzahl privilegierter Benutzer - Gewährung von privilegierten Zugriffen auf „" oder "need-to-haveneed-to-do“ -Basis - Aufrechterhaltung der Audit-Protokollierung der von privilegierten Benutzern ausgeführten Systemaktivitäten - Sicherstellung, dass privilegierte Benutzer keinen Zugriff auf Systemprotokolle haben, in denen ihre Aktivitäten erfasst werden - Durchführung regelmäßiger Audits oder Managementüberprüfungen der Protokolle — Verbot		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
	der Weitergabe von privilegierten Daten IDs und deren Zugangsco des — Verbot des privilegierten Zugriffs auf Systeme ohne genaue Überwachu ng und Überwachu ng und _ Schutz von Backup-Daten vor unbefugtem Zugriff		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
3.1.1(h)	h) Systemadministratoren, Sicherheitsbeauftragte, Programmierer und Mitarbeiter, die kritische Vorgänge durchführen, können aufgrund ihrer Aufgaben und ihres privilegierten Zugriffs den von ihnen unterhaltenen oder betriebenen Finanzsystemen schweren Schaden zuzufügen. Mitarbeiter mit erhöhten Systemzugriffsberechtigungen sollten engmaschig beaufsichtigt und alle ihre Systemaktivitäten protokolliert werden, da sie über Insiderwissen und die nötigen Ressourcen verfügen, um Systemkontrollen und Sicherheitsverfahren zu umgehen. Einige der unten aufgeführten Kontroll- und Sicherheitspraktiken	root-account-mfa-enabled	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass MFA für den Root-Benutzer aktiviert ist. Der Stammbenutzer ist der AWS-Konto-Benutzer mit den meisten Berechtigungen. MFA sorgt für eine weitere Schutzebene zusätzlich zu den Anmeldeinformationen. Indem Sie MFA für den Root-Benutzer vorschreiben, können Sie die Anzahl AWS-Konten kompromittierter Benutzer reduzieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
	müssen berücksichtigt werden: - Implementierung einer Zwei-Faktor-Authentifizierung für privilegierte Benutzer - Einführung strenger Kontrollen des Fernzugriffs durch privilegierte Benutzer - Beschränkung der Anzahl privilegierter Benutzer - Gewährung von privilegierten Zugriffen auf „" oder "need-to-haveneed-to-do“ -Basis - Aufrechterhaltung der Audit-Protokollierung der von privilegierten Benutzern ausgeführten Systemaktivitäten - Sicherstellung, dass privilegierte Benutzer keinen Zugriff auf Systemprotokolle haben, in denen ihre Aktivitäten erfasst werden - Durchführung regelmäßiger Audits oder Managementüberprüfungen der Protokolle — Verbot		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
	der Weitergabe von privilegierten Daten IDs und deren Zugangsco des — Verbot des privilegierten Zugriffs auf Systeme ohne genaue Überwachu ng und Überwachu ng und _ Schutz von Backup-Daten vor unbefugtem Zugriff		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
3.1.1(h)	h) Systemadm inistratoren, Sicherhei tsbeauftragte, Programmierer und Mitarbeiter, die kritische Vorgänge durchführen, können aufgrund ihrer Aufgaben und ihres privilegierten Zugriffs den von ihnen unterhaltenen oder betriebenen Finanzsystemen schweren Schaden zuzufügen. Mitarbeit er mit erhöhten Systemzugriffsbere chtigungen sollten engmaschig beaufsich tigt und alle ihre Systemaktivitäten protokolliert werden, da sie über Insiderwi ssen und die nötigen Ressourcen verfügen, um Systemkon trollen und Sicherhei tsverfahren zu umgehen. Einige der unten aufgeführ ten Kontroll- und Sicherheitspraktiken	iam-no-inline-policy-überprüfen	Stellen Sie sicher, dass ein Benutzer, eine IAM-Rolle oder eine IAM-Gruppe (AWS Identity and Access Management) nicht über eine Inline-Richtlinie zur Zugriffsk ontrolle auf Systeme und Ressource n verfügt. AWS empfiehlt, verwaltet e Richtlinien anstelle von Inline-Richtlinien zu verwenden. Verwaltete Richtlini en ermöglichen Wiederverwendbarke it, Versionsverwaltung , Rollback und Delegierung der Berechtigungsverwa ltung.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
	müssen berücksichtigt werden: - Implementierung einer Zwei-Faktor-Authentifizierung für privilegierte Benutzer - Einführung strenger Kontrollen des Fernzugriffs durch privilegierte Benutzer - Beschränkung der Anzahl privilegierter Benutzer - Gewährung von privilegierten Zugriffen auf „" oder "need-to-haveneed-to-do“ -Basis - Aufrechterhaltung der Audit-Protokollierung der von privilegierten Benutzern ausgeführten Systemaktivitäten - Sicherstellung, dass privilegierte Benutzer keinen Zugriff auf Systemprotokolle haben, in denen ihre Aktivitäten erfasst werden - Durchführung regelmäßiger Audits oder Managementüberprüfungen der Protokolle — Verbot		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
	der Weitergabe von privilegierten Daten IDs und deren Zugangsco des — Verbot des privilegierten Zugriffs auf Systeme ohne genaue Überwachu ng und Überwachu ng und _ Schutz von Backup-Daten vor unbefugtem Zugriff		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
3.1.1(h)	h) Systemadministratoren, Sicherheitsbeauftragte, Programmierer und Mitarbeiter, die kritische Vorgänge durchführen, können aufgrund ihrer Aufgaben und ihres privilegierten Zugriffs den von ihnen unterhaltenen oder betriebenen Finanzsystemen schweren Schaden zuzufügen. Mitarbeiter mit erhöhten Systemzugriffsberechtigungen sollten engmaschig beaufsichtigt und alle ihre Systemaktivitäten protokolliert werden, da sie über Insiderwissen und die nötigen Ressourcen verfügen, um Systemkontrollen und Sicherheitsverfahren zu umgehen. Einige der unten aufgeführten Kontroll- und Sicherheitspraktiken	api-gw-execution-logging-aktiviert	Die API-Gateway-Protokollierung zeigt detaillierte Ansichten der Benutzer, die auf die API zugegriffen haben, und wie diese Benutzer auf die API zugegriffen haben. Diese Insights ermöglichen die Einsicht in Benutzeraktivitäten.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
	müssen berücksichtigt werden: - Implementierung einer Zwei-Faktor-Authentifizierung für privilegierte Benutzer - Einführung strenger Kontrollen des Fernzugriffs durch privilegierte Benutzer - Beschränkung der Anzahl privilegierter Benutzer - Gewährung von privilegierten Zugriffen auf „" oder "need-to-haveneed-to-do“ -Basis - Aufrechterhaltung der Audit-Protokollierung der von privilegierten Benutzern ausgeführten Systemaktivitäten - Sicherstellung, dass privilegierte Benutzer keinen Zugriff auf Systemprotokolle haben, in denen ihre Aktivitäten erfasst werden - Durchführung regelmäßiger Audits oder Managementüberprüfungen der Protokolle — Verbot		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
	der Weitergabe von privilegierten Daten IDs und deren Zugangsco des — Verbot des privilegierten Zugriffs auf Systeme ohne genaue Überwachu ng und Überwachu ng und _ Schutz von Backup-Daten vor unbefugtem Zugriff		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
3.1.1(h)	h) Systemadm inistratoren, Sicherhei tsbeauftragte, Programmierer und Mitarbeiter, die kritische Vorgänge durchführen, können aufgrund ihrer Aufgaben und ihres privilegierten Zugriffs den von ihnen unterhaltenen oder betriebenen Finanzsystemen schweren Schaden zuzufügen. Mitarbeit er mit erhöhten Systemzugriffsbere chtigungen sollten engmaschig beaufsich tigt und alle ihre Systemaktivitäten protokolliert werden, da sie über Insiderwi ssen und die nötigen Ressourcen verfügen, um Systemkon trollen und Sicherhei tsverfahren zu umgehen. Einige der unten aufgeführ ten Kontroll- und Sicherheitspraktiken	cloud-trail-cloud-watch-Logs aktiviert	Verwenden Sie Amazon CloudWatc h , um Protokoll ereignisaktivitäten zentral zu sammeln und zu verwalten. Die Aufnahme von AWS CloudTrail Daten liefert Einzelheiten zu den API-Aufrufaktivitä ten in Ihrem AWS-Konto.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
	müssen berücksichtigt werden: - Implementierung einer Zwei-Faktor-Authentifizierung für privilegierte Benutzer - Einführung strenger Kontrollen des Fernzugriffs durch privilegierte Benutzer - Beschränkung der Anzahl privilegierter Benutzer - Gewährung von privilegierten Zugriffen auf „" oder "need-to-haveneed-to-do“ -Basis - Aufrechterhaltung der Audit-Protokollierung der von privilegierten Benutzern ausgeführten Systemaktivitäten - Sicherstellung, dass privilegierte Benutzer keinen Zugriff auf Systemprotokolle haben, in denen ihre Aktivitäten erfasst werden - Durchführung regelmäßiger Audits oder Managementüberprüfungen der Protokolle — Verbot		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
	der Weitergabe von privilegierten Daten IDs und deren Zugangsco des — Verbot des privilegierten Zugriffs auf Systeme ohne genaue Überwachu ng und Überwachu ng und _ Schutz von Backup-Daten vor unbefugtem Zugriff		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
3.1.1(h)	h) Systemadm inistratoren, Sicherhei tsbeauftragte, Programmierer und Mitarbeiter, die kritische Vorgänge durchführen, können aufgrund ihrer Aufgaben und ihres privilegierten Zugriffs den von ihnen unterhaltenen oder betriebenen Finanzsystemen schweren Schaden zuzufügen. Mitarbeit er mit erhöhten Systemzugriffsbere chtigungen sollten engmaschig beaufsich tigt und alle ihre Systemaktivitäten protokolliert werden, da sie über Insiderwi ssen und die nötigen Ressourcen verfügen, um Systemkon trollen und Sicherhei tsverfahren zu umgehen. Einige der unten aufgeführ ten Kontroll- und Sicherheitspraktiken	cloudtrail-enabled	AWS CloudTrail kann durch die Aufzeichn ung von Aktionen und API-Aufrufen der Managemen t Console bei der Nichtabstreitbarke it helfen. AWS Sie können die Benutzer und die Benutzer AWS-Konten , die einen AWS Dienst aufgerufen haben, die Quell-IP-Adresse, über die die Aufrufe generiert wurden, und den Zeitpunkt der Anrufe identifiz ieren. Einzelheiten zu den erfassten Daten finden Sie in den AWS CloudTrail Datensatzinhalten.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
	müssen berücksichtigt werden: - Implementierung einer Zwei-Faktor-Authentifizierung für privilegierte Benutzer - Einführung strenger Kontrollen des Fernzugriffs durch privilegierte Benutzer - Beschränkung der Anzahl privilegierter Benutzer - Gewährung von privilegierten Zugriffen auf „" oder "need-to-haveneed-to-do“ -Basis - Aufrechterhaltung der Audit-Protokollierung der von privilegierten Benutzern ausgeführten Systemaktivitäten - Sicherstellung, dass privilegierte Benutzer keinen Zugriff auf Systemprotokolle haben, in denen ihre Aktivitäten erfasst werden - Durchführung regelmäßiger Audits oder Managementüberprüfungen der Protokolle — Verbot		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
	der Weitergabe von privilegierten Daten IDs und deren Zugangsco des — Verbot des privilegierten Zugriffs auf Systeme ohne genaue Überwachu ng und Überwachu ng und _ Schutz von Backup-Daten vor unbefugtem Zugriff		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
3.1.1(h)	h) Systemadm inistratoren, Sicherhei tsbeauftragte, Programmierer und Mitarbeiter, die kritische Vorgänge durchführen, können aufgrund ihrer Aufgaben und ihres privilegierten Zugriffs den von ihnen unterhaltenen oder betriebenen Finanzsystemen schweren Schaden zuzufügen. Mitarbeit er mit erhöhten Systemzugriffsbere chtigungen sollten engmaschig beaufsich tigt und alle ihre Systemaktivitäten protokolliert werden, da sie über Insiderwi ssen und die nötigen Ressourcen verfügen, um Systemkon trollen und Sicherhei tsverfahren zu umgehen. Einige der unten aufgeführ ten Kontroll- und Sicherheitspraktiken	cloudtrail-s3-data events-enabled	Die Erfassung von Simple Storage Service (Amazon S3)-Datenereigniss en unterstützt die Erkennung von ungewöhnlichen Aktivitäten. Zu den Details gehören AWS-Konto Informationen über den Zugriff auf einen Amazon S3 S3-Bucket, die IP-Adress e und die Uhrzeit des Ereignisses.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
	müssen berücksichtigt werden: - Implementierung einer Zwei-Faktor-Authentifizierung für privilegierte Benutzer - Einführung strenger Kontrollen des Fernzugriffs durch privilegierte Benutzer - Beschränkung der Anzahl privilegierter Benutzer - Gewährung von privilegierten Zugriffen auf „" oder "need-to-haveneed-to-do“ -Basis - Aufrechterhaltung der Audit-Protokollierung der von privilegierten Benutzern ausgeführten Systemaktivitäten - Sicherstellung, dass privilegierte Benutzer keinen Zugriff auf Systemprotokolle haben, in denen ihre Aktivitäten erfasst werden - Durchführung regelmäßiger Audits oder Managementüberprüfungen der Protokolle — Verbot		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
	der Weitergabe von privilegierten Daten IDs und deren Zugangsco des — Verbot des privilegierten Zugriffs auf Systeme ohne genaue Überwachu ng und Überwachu ng und _ Schutz von Backup-Daten vor unbefugtem Zugriff		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
3.1.1(h)	h) Systemadministratoren, Sicherheitsbeauftragte, Programmierer und Mitarbeiter, die kritische Vorgänge durchführen, können aufgrund ihrer Aufgaben und ihres privilegierten Zugriffs den von ihnen unterhaltenen oder betriebenen Finanzsystemen schweren Schaden zuzufügen. Mitarbeiter mit erhöhten Systemzugriffsberechtigungen sollten engmaschig beaufsichtigt und alle ihre Systemaktivitäten protokolliert werden, da sie über Insiderwissen und die nötigen Ressourcen verfügen, um Systemkontrollen und Sicherheitsverfahren zu umgehen. Einige der unten aufgeführten Kontroll- und Sicherheitspraktiken	elb-logging-enabled	Die Elastic-Load-Balancing-Aktivität ist ein zentraler Kommunikationspunkt innerhalb einer Umgebung. Stellen Sie sicher, dass die ELB-Protokollierung aktiviert ist. Die gesammelten Daten enthalten detaillierte Informationen zu Anfragen, die an den ELB gesendet wurden. Jedes Protokoll enthält Informationen wie die Zeit, zu der die Anforderung einging, die Client-IP-Adresse, Latenzen, Anforderungspfade und Serverantworten.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
	müssen berücksichtigt werden: - Implementierung einer Zwei-Faktor-Authentifizierung für privilegierte Benutzer - Einführung strenger Kontrollen des Fernzugriffs durch privilegierte Benutzer - Beschränkung der Anzahl privilegierter Benutzer - Gewährung von privilegierten Zugriffen auf „" oder "need-to-haveneed-to-do“ -Basis - Aufrechterhaltung der Audit-Protokollierung der von privilegierten Benutzern ausgeführten Systemaktivitäten - Sicherstellung, dass privilegierte Benutzer keinen Zugriff auf Systemprotokolle haben, in denen ihre Aktivitäten erfasst werden - Durchführung regelmäßiger Audits oder Managementüberprüfungen der Protokolle — Verbot		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
	der Weitergabe von privilegierten Daten IDs und deren Zugangsco des — Verbot des privilegierten Zugriffs auf Systeme ohne genaue Überwachu ng und Überwachu ng und _ Schutz von Backup-Daten vor unbefugtem Zugriff		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
3.1.1(h)	h) Systemadm inistratoren, Sicherhei tsbeauftragte, Programmierer und Mitarbeiter, die kritische Vorgänge durchführen, können aufgrund ihrer Aufgaben und ihres privilegierten Zugriffs den von ihnen unterhaltenen oder betriebenen Finanzsystemen schweren Schaden zuzufügen. Mitarbeit er mit erhöhten Systemzugriffsbere chtigungen sollten engmaschig beaufsich tigt und alle ihre Systemaktivitäten protokolliert werden, da sie über Insiderwi ssen und die nötigen Ressourcen verfügen, um Systemkon trollen und Sicherhei tsverfahren zu umgehen. Einige der unten aufgeführ ten Kontroll- und Sicherheitspraktiken	multi-region-cloudtrail-enabled	AWS CloudTrail zeichnet Aktionen und API-Aufrufe der AWS Management Console auf. Sie können feststellen, welche Benutzer und Konten angerufen wurden AWS, von welcher Quell-IP-Adresse aus die Anrufe getätigt wurden und wann die Anrufe erfolgten. CloudTrail übermittelt Protokolldateien aus allen AWS Regionen an Ihren S3-Bucket , wenn MULTI_REG ION_CLOUD _TRAIL_ENABLED aktiviert ist. Außerdem wird beim AWS Start einer neuen Region derselbe Trail in der neuen Region erstellt. CloudTrail Dadurch erhalten Sie automatis ch Protokolldateien mit API-Aktivitäten für die neue Region.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
	müssen berücksichtigt werden: - Implementierung einer Zwei-Faktor-Authentifizierung für privilegierte Benutzer - Einführung strenger Kontrollen des Fernzugriffs durch privilegierte Benutzer - Beschränkung der Anzahl privilegierter Benutzer - Gewährung von privilegierten Zugriffen auf „" oder "need-to-haveneed-to-do“ -Basis - Aufrechterhaltung der Audit-Protokollierung der von privilegierten Benutzern ausgeführten Systemaktivitäten - Sicherstellung, dass privilegierte Benutzer keinen Zugriff auf Systemprotokolle haben, in denen ihre Aktivitäten erfasst werden - Durchführung regelmäßiger Audits oder Managementüberprüfungen der Protokolle — Verbot		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
	der Weitergabe von privilegierten Daten IDs und deren Zugangsco des — Verbot des privilegierten Zugriffs auf Systeme ohne genaue Überwachu ng und Überwachu ng und _ Schutz von Backup-Daten vor unbefugtem Zugriff		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
3.1.1(h)	h) Systemadm inistratoren, Sicherhei tsbeauftragte, Programmierer und Mitarbeiter, die kritische Vorgänge durchführen, können aufgrund ihrer Aufgaben und ihres privilegierten Zugriffs den von ihnen unterhaltenen oder betriebenen Finanzsystemen schweren Schaden zuzufügen. Mitarbeit er mit erhöhten Systemzugriffsbere chtigungen sollten engmaschig beaufsich tigt und alle ihre Systemaktivitäten protokolliert werden, da sie über Insiderwi ssen und die nötigen Ressourcen verfügen, um Systemkon trollen und Sicherhei tsverfahren zu umgehen. Einige der unten aufgeführ ten Kontroll- und Sicherheitspraktiken	s3- bucket-logging-enabled	Die Amazon Simple Storage Service (Amazon S3)-Serverzugriffs protokollierung bietet eine Methode zur Überwachu ng des Netzwerks im Hinblick auf potenzielle Cybersich erheitsereignisse. Die Ereignisse werden überwacht, indem detaillierte Aufzeichn ungen über die Anfragen erfasst werden, die an einen Amazon-S3-Bucket gestellt wurden. Jeder Zugriffsprotokolle intrag enthält Details zu einer einzelnen Zugriffsanfrage. Zu den Details gehören Anforderer, Bucket-Name, Anforderu ngszeit, Anforderu ngsaktion, Antwortst atus und Fehlercode, falls relevant.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
	müssen berücksichtigt werden: - Implementierung einer Zwei-Faktor-Authentifizierung für privilegierte Benutzer - Einführung strenger Kontrollen des Fernzugriffs durch privilegierte Benutzer - Beschränkung der Anzahl privilegierter Benutzer - Gewährung von privilegierten Zugriffen auf „" oder "need-to-haveneed-to-do“ -Basis - Aufrechterhaltung der Audit-Protokollierung der von privilegierten Benutzern ausgeführten Systemaktivitäten - Sicherstellung, dass privilegierte Benutzer keinen Zugriff auf Systemprotokolle haben, in denen ihre Aktivitäten erfasst werden - Durchführung regelmäßiger Audits oder Managementüberprüfungen der Protokolle — Verbot		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
	der Weitergabe von privilegierten Daten IDs und deren Zugangsco des — Verbot des privilegierten Zugriffs auf Systeme ohne genaue Überwachu ng und Überwachu ng und _ Schutz von Backup-Daten vor unbefugtem Zugriff		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
3.1.1(h)	h) Systemadministratoren, Sicherheitsbeauftragte, Programmierer und Mitarbeiter, die kritische Vorgänge durchführen, können aufgrund ihrer Aufgaben und ihres privilegierten Zugriffs den von ihnen unterhaltenen oder betriebenen Finanzsystemen schweren Schaden zuzufügen. Mitarbeiter mit erhöhten Systemzugriffsberechtigungen sollten engmaschig beaufsichtigt und alle ihre Systemaktivitäten protokolliert werden, da sie über Insiderwissen und die nötigen Ressourcen verfügen, um Systemkontrollen und Sicherheitsverfahren zu umgehen. Einige der unten aufgeführten Kontroll- und Sicherheitspraktiken	vpc-flow-logs-enabled	VPC-Flow-Protokolle erfassen detaillierte Informationsdatensätze über den IP-Datenverkehr, der zu und von Netzwerkschnittstellen in Ihrer Amazon Virtual Private Cloud (Amazon VPC) fließt. Standardmäßig enthalten Flow-Protokolldatensätze Werte für die verschiedenen Komponenten des IP-Flows, einschließlich Quelle, Ziel und Protokoll.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
	müssen berücksichtigt werden: - Implementierung einer Zwei-Faktor-Authentifizierung für privilegierte Benutzer - Einführung strenger Kontrollen des Fernzugriffs durch privilegierte Benutzer - Beschränkung der Anzahl privilegierter Benutzer - Gewährung von privilegierten Zugriffen auf „" oder "need-to-haveneed-to-do“ -Basis - Aufrechterhaltung der Audit-Protokollierung der von privilegierten Benutzern ausgeführten Systemaktivitäten - Sicherstellung, dass privilegierte Benutzer keinen Zugriff auf Systemprotokolle haben, in denen ihre Aktivitäten erfasst werden - Durchführung regelmäßiger Audits oder Managementüberprüfungen der Protokolle — Verbot		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
	der Weitergabe von privilegierten Daten IDs und deren Zugangsco des — Verbot des privilegierten Zugriffs auf Systeme ohne genaue Überwachu ng und Überwachu ng und _ Schutz von Backup-Daten vor unbefugtem Zugriff		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
3.1.1(h)	h) Systemadm inistratoren, Sicherhei tsbeauftragte, Programmierer und Mitarbeiter, die kritische Vorgänge durchführen, können aufgrund ihrer Aufgaben und ihres privilegierten Zugriffs den von ihnen unterhaltenen oder betriebenen Finanzsystemen schweren Schaden zuzufügen. Mitarbeit er mit erhöhten Systemzugriffsbere chtigungen sollten engmaschig beaufsich tigt und alle ihre Systemaktivitäten protokolliert werden, da sie über Insiderwi ssen und die nötigen Ressourcen verfügen, um Systemkon trollen und Sicherhei tsverfahren zu umgehen. Einige der unten aufgeführ ten Kontroll- und Sicherheitspraktiken	cw-loggroup-retent ion-period-überprüfen	Stellen Sie sicher, dass die Ereignisp rotokolldaten für Ihre Protokollgruppen über eine Mindestdauer aufbewahrt werden, um die Fehlerbeh ebung und forensisc he Untersuchungen zu unterstützen. Fehlende frühere Ereignisprotokolld aten erschweren die Rekonstruierung und Identifizierung potenziell schädlicher Ereignisse.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
	müssen berücksichtigt werden: - Implementierung einer Zwei-Faktor-Authentifizierung für privilegierte Benutzer - Einführung strenger Kontrollen des Fernzugriffs durch privilegierte Benutzer - Beschränkung der Anzahl privilegierter Benutzer - Gewährung von privilegierten Zugriffen auf „" oder "need-to-haveneed-to-do“ -Basis - Aufrechterhaltung der Audit-Protokollierung der von privilegierten Benutzern ausgeführten Systemaktivitäten - Sicherstellung, dass privilegierte Benutzer keinen Zugriff auf Systemprotokolle haben, in denen ihre Aktivitäten erfasst werden - Durchführung regelmäßiger Audits oder Managementüberprüfungen der Protokolle — Verbot		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
	der Weitergabe von privilegierten Daten IDs und deren Zugangsco des — Verbot des privilegierten Zugriffs auf Systeme ohne genaue Überwachu ng und Überwachu ng und _ Schutz von Backup-Daten vor unbefugtem Zugriff		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
3.1.1(h)	h) Systemadm inistratoren, Sicherhei tsbeauftragte, Programmierer und Mitarbeiter, die kritische Vorgänge durchführen, können aufgrund ihrer Aufgaben und ihres privilegierten Zugriffs den von ihnen unterhaltenen oder betriebenen Finanzsystemen schweren Schaden zuzufügen. Mitarbeit er mit erhöhten Systemzugriffsbere chtigungen sollten engmaschig beaufsich tigt und alle ihre Systemaktivitäten protokolliert werden, da sie über Insiderwi ssen und die nötigen Ressourcen verfügen, um Systemkon trollen und Sicherhei tsverfahren zu umgehen. Einige der unten aufgeführ ten Kontroll- und Sicherheitspraktiken	rds-logging-enabled	Um die Protokoll ierung und Überwachung in Ihrer Umgebung zu erleichtern, stellen Sie sicher, dass die Amazon Relationa l Database Service (Amazon RDS)-Prot okollierung aktiviert ist. Mit der Amazon-RDS-Protokollierung können Sie Ereigniss e wie Verbindungen, Verbindungsabbrüch e, Abfragen oder abgefragte Tabellen erfassen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
	müssen berücksichtigt werden: - Implementierung einer Zwei-Faktor-Authentifizierung für privilegierte Benutzer - Einführung strenger Kontrollen des Fernzugriffs durch privilegierte Benutzer - Beschränkung der Anzahl privilegierter Benutzer - Gewährung von privilegierten Zugriffen auf „" oder "need-to-haveneed-to-do“ -Basis - Aufrechterhaltung der Audit-Protokollierung der von privilegierten Benutzern ausgeführten Systemaktivitäten - Sicherstellung, dass privilegierte Benutzer keinen Zugriff auf Systemprotokolle haben, in denen ihre Aktivitäten erfasst werden - Durchführung regelmäßiger Audits oder Managementüberprüfungen der Protokolle — Verbot		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
	der Weitergabe von privilegierten Daten IDs und deren Zugangsco des — Verbot des privilegierten Zugriffs auf Systeme ohne genaue Überwachu ng und Überwachu ng und _ Schutz von Backup-Daten vor unbefugtem Zugriff		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
3.1.1(h)	h) Systemadministratoren, Sicherheitsbeauftragte, Programmierer und Mitarbeiter, die kritische Vorgänge durchführen, können aufgrund ihrer Aufgaben und ihres privilegierten Zugriffs den von ihnen unterhaltenen oder betriebenen Finanzsystemen schweren Schaden zuzufügen. Mitarbeiter mit erhöhten Systemzugriffsberechtigungen sollten engmaschig beaufsichtigt und alle ihre Systemaktivitäten protokolliert werden, da sie über Insiderwissen und die nötigen Ressourcen verfügen, um Systemkontrollen und Sicherheitsverfahren zu umgehen. Einige der unten aufgeführten Kontroll- und Sicherheitspraktiken	wafv2-logging-enabled	Um die Protokollierung und Überwachung in Ihrer Umgebung zu erleichtern, aktivieren Sie die AWS WAF (V2) -Protokollierung im regionalen und globalen Internet. ACLs AWS Die WAF-Protokollierung bietet detaillierte Informationen über den Datenverkehr, der von Ihrer Web-ACL analysiert wird. In den Protokollen werden die Uhrzeit aufgezeichnet, zu der die AWS WAF die Anfrage von Ihrer AWS Ressource erhalten hat, Informationen zu der Anfrage und eine Aktion für die Regel, der jede Anfrage entsprach.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
	müssen berücksichtigt werden: - Implementierung einer Zwei-Faktor-Authentifizierung für privilegierte Benutzer - Einführung strenger Kontrollen des Fernzugriffs durch privilegierte Benutzer - Beschränkung der Anzahl privilegierter Benutzer - Gewährung von privilegierten Zugriffen auf „" oder "need-to-haveneed-to-do“ -Basis - Aufrechterhaltung der Audit-Protokollierung der von privilegierten Benutzern ausgeführten Systemaktivitäten - Sicherstellung, dass privilegierte Benutzer keinen Zugriff auf Systemprotokolle haben, in denen ihre Aktivitäten erfasst werden - Durchführung regelmäßiger Audits oder Managementüberprüfungen der Protokolle — Verbot		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
	der Weitergabe von privilegierten Daten IDs und deren Zugangsco des — Verbot des privilegierten Zugriffs auf Systeme ohne genaue Überwachu ng und Überwachu ng und _ Schutz von Backup-Daten vor unbefugtem Zugriff		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
3.1.1(h)	h) Systemadministratoren, Sicherheitsbeauftragte, Programmierer und Mitarbeiter, die kritische Vorgänge durchführen, können aufgrund ihrer Aufgaben und ihres privilegierten Zugriffs den von ihnen unterhaltenen oder betriebenen Finanzsystemen schweren Schaden zuzufügen. Mitarbeiter mit erhöhten Systemzugriffsberechtigungen sollten engmaschig beaufsichtigt und alle ihre Systemaktivitäten protokolliert werden, da sie über Insiderwissen und die nötigen Ressourcen verfügen, um Systemkontrollen und Sicherheitsverfahren zu umgehen. Einige der unten aufgeführten Kontroll- und Sicherheitspraktiken	redshift-cluster-configuration-check	Um Daten im Ruhezustand zu schützen, muss die Verschlüsselung für Ihre Amazon-Redshift-Cluster aktiviert sein. Sie müssen auch sicherstellen, dass die erforderlichen Konfigurationen auf Amazon-Redshift-Clustern bereitgestellt werden. Die Prüfungsprotokollierung muss aktiviert sein, um Informationen zu Verbindungen und Benutzeraktivitäten in der Datenbank bereitzustellen. Diese Regel erfordert, dass ein Wert für clusterDbEncrypted (Config Default: TRUE) und LoggingEnabled (Config Default: TRUE) gesetzt ist. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
	müssen berücksichtigt werden: - Implementierung einer Zwei-Faktor-Authentifizierung für privilegierte Benutzer - Einführung strenger Kontrollen des Fernzugriffs durch privilegierte Benutzer - Beschränkung der Anzahl privilegierter Benutzer - Gewährung von privilegierten Zugriffen auf „" oder "need-to-haveneed-to-do“ -Basis - Aufrechterhaltung der Audit-Protokollierung der von privilegierten Benutzern ausgeführten Systemaktivitäten - Sicherstellung, dass privilegierte Benutzer keinen Zugriff auf Systemprotokolle haben, in denen ihre Aktivitäten erfasst werden - Durchführung regelmäßiger Audits oder Managementüberprüfungen der Protokolle — Verbot		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
	der Weitergabe von privilegierten Daten IDs und deren Zugangsco des — Verbot des privilegierten Zugriffs auf Systeme ohne genaue Überwachu ng und Überwachu ng und _ Schutz von Backup-Daten vor unbefugtem Zugriff		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
3.1.1(h)	h) Systemadministratoren, Sicherheitsbeauftragte, Programmierer und Mitarbeiter, die kritische Vorgänge durchführen, können aufgrund ihrer Aufgaben und ihres privilegierten Zugriffs den von ihnen unterhaltenen oder betriebenen Finanzsystemen schweren Schaden zuzufügen. Mitarbeiter mit erhöhten Systemzugriffsberechtigungen sollten engmaschig beaufsichtigt und alle ihre Systemaktivitäten protokolliert werden, da sie über Insiderwissen und die nötigen Ressourcen verfügen, um Systemkontrollen und Sicherheitsverfahren zu umgehen. Einige der unten aufgeführten Kontroll- und Sicherheitspraktiken	account-part-of-organizations	Durch die zentrale Verwaltung AWS-Konten innerhalb von AWS Organizations wird sichergestellt, dass die Konten den Vorschriften entsprechen. Eine fehlende zentrale Kontoverwaltung kann zu inkonsistenten Kontokonfigurationen führen, wodurch Ressourcen und sensible Daten offengelegt werden können.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
	müssen berücksichtigt werden: - Implementierung einer Zwei-Faktor-Authentifizierung für privilegierte Benutzer - Einführung strenger Kontrollen des Fernzugriffs durch privilegierte Benutzer - Beschränkung der Anzahl privilegierter Benutzer - Gewährung von privilegierten Zugriffen auf „" oder "need-to-haveneed-to-do“ -Basis - Aufrechterhaltung der Audit-Protokollierung der von privilegierten Benutzern ausgeführten Systemaktivitäten - Sicherstellung, dass privilegierte Benutzer keinen Zugriff auf Systemprotokolle haben, in denen ihre Aktivitäten erfasst werden - Durchführung regelmäßiger Audits oder Managementüberprüfungen der Protokolle — Verbot		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
	der Weitergabe von privilegierten Daten IDs und deren Zugangsco des — Verbot des privilegierten Zugriffs auf Systeme ohne genaue Überwachu ng und Überwachu ng und _ Schutz von Backup-Daten vor unbefugtem Zugriff		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
3.1.1(h)	h) Systemadministratoren, Sicherheitsbeauftragte, Programmierer und Mitarbeiter, die kritische Vorgänge durchführen, können aufgrund ihrer Aufgaben und ihres privilegierten Zugriffs den von ihnen unterhaltenen oder betriebenen Finanzsystemen schweren Schaden zuzufügen. Mitarbeiter mit erhöhten Systemzugriffsberechtigungen sollten engmaschig beaufsichtigt und alle ihre Systemaktivitäten protokolliert werden, da sie über Insiderwissen und die nötigen Ressourcen verfügen, um Systemkontrollen und Sicherheitsverfahren zu umgehen. Einige der unten aufgeführten Kontroll- und Sicherheitspraktiken	iam-customer-policy-blocked-kms-Aktionen	AWS Identity and Access Management (IAM) kann Ihnen helfen, die Prinzipien der geringsten Rechte und der Aufgabentrennung in Zugriffsberechtigungen und Autorisierungen zu integrieren und so zu verhindern, dass Richtlinien blockierte Aktionen für alle AWS Schlüssel des Key Management Service enthalten. Wenn Benutzer mehr Rechte haben, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und Aufgabentrennung verstoßen. Mit dieser Regel können Sie den Parameter festlegen. blockedActionsPatterns (Wert „AWS Bewährte grundlegende Sicherheitsmethode

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
	müssen berücksichtigt werden: - Implementierung einer Zwei-Faktor-Authentifizierung für privilegierte Benutzer - Einführung strenger Kontrollen des Fernzugriffs durch privilegierte Benutzer - Beschränkung der Anzahl privilegierter Benutzer - Gewährung von privilegierten Zugriffen auf „" oder "need-to-haveneed-to-do“ -Basis - Aufrechterhaltung der Audit-Protokollierung der von privilegierten Benutzern ausgeführten Systemaktivitäten - Sicherstellung, dass privilegierte Benutzer keinen Zugriff auf Systemprotokolle haben, in denen ihre Aktivitäten erfasst werden - Durchführung regelmäßiger Audits oder Managementüberprüfungen der Protokolle — Verbot		n“: kms: Entschlüsseln, kms:ReEncryptFrom). Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
	der Weitergabe von privilegierten Daten IDs und deren Zugangsco des — Verbot des privilegierten Zugriffs auf Systeme ohne genaue Überwachu ng und Überwachu ng und _ Schutz von Backup-Daten vor unbefugtem Zugriff		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
3.1.1(h)	h) Systemadministratoren, Sicherheitsbeauftragte, Programmierer und Mitarbeiter, die kritische Vorgänge durchführen, können aufgrund ihrer Aufgaben und ihres privilegierten Zugriffs den von ihnen unterhaltenen oder betriebenen Finanzsystemen schweren Schaden zuzufügen. Mitarbeiter mit erhöhten Systemzugriffsberechtigungen sollten engmaschig beaufsichtigt und alle ihre Systemaktivitäten protokolliert werden, da sie über Insiderwissen und die nötigen Ressourcen verfügen, um Systemkontrollen und Sicherheitsverfahren zu umgehen. Einige der unten aufgeführten Kontroll- und Sicherheitspraktiken	iam-group-has-users-überprüfen	AWS Identity and Access Management (IAM) kann Ihnen helfen, die Prinzipien der geringsten Rechte und der Aufgabentrennung mit Zugriffsberechtigungen und Autorisierungen zu integrieren, indem sichergestellt wird, dass IAM-Gruppen mindestens einen Benutzer haben. Die Einteilung von Benutzern in Gruppen auf der Grundlage der ihnen zugewiesenen Berechtigungen oder ihrer Funktion ist eine Möglichkeit, das Prinzip der geringsten Berechtigung zu implementieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
	müssen berücksichtigt werden: - Implementierung einer Zwei-Faktor-Authentifizierung für privilegierte Benutzer - Einführung strenger Kontrollen des Fernzugriffs durch privilegierte Benutzer - Beschränkung der Anzahl privilegierter Benutzer - Gewährung von privilegierten Zugriffen auf „" oder "need-to-haveneed-to-do“ -Basis - Aufrechterhaltung der Audit-Protokollierung der von privilegierten Benutzern ausgeführten Systemaktivitäten - Sicherstellung, dass privilegierte Benutzer keinen Zugriff auf Systemprotokolle haben, in denen ihre Aktivitäten erfasst werden - Durchführung regelmäßiger Audits oder Managementüberprüfungen der Protokolle — Verbot		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
	der Weitergabe von privilegierten Daten IDs und deren Zugangsco des — Verbot des privilegierten Zugriffs auf Systeme ohne genaue Überwachu ng und Überwachu ng und _ Schutz von Backup-Daten vor unbefugtem Zugriff		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
3.1.1(h)	h) Systemadm inistratoren, Sicherhei tsbeauftragte, Programmierer und Mitarbeiter, die kritische Vorgänge durchführen, können aufgrund ihrer Aufgaben und ihres privilegierten Zugriffs den von ihnen unterhaltenen oder betriebenen Finanzsystemen schweren Schaden zuzufügen. Mitarbeit er mit erhöhten Systemzugriffsbere chtigungen sollten engmaschig beaufsich tigt und alle ihre Systemaktivitäten protokolliert werden, da sie über Insiderwi ssen und die nötigen Ressourcen verfügen, um Systemkon trollen und Sicherhei tsverfahren zu umgehen. Einige der unten aufgeführ ten Kontroll- und Sicherheitspraktiken	iam-inline-policy-blocked-kms-Aktionen	Stellen Sie sicher, dass ein Benutzer, eine IAM-Rolle oder eine IAM-Gruppe (AWS Identity and Access Management) nicht über eine Inline-Richtlinie verfügt, die blockierte Aktionen für alle AWS Schlüssel des Key Management Service zulässt. AWS empfiehlt, verwaltet e Richtlinien anstelle von Inline-Richtlinien zu verwenden. Verwaltete Richtlini en ermöglichen Wiederverwendbarke it, Versionsverwaltung , Rollback und Delegierung der Berechtigungsverwa ltung. Mit dieser Regel können Sie den blockedActionsPatt erns Parameter festlegen. (Wert „AWS Bewährte grundlegende Sicherheitsmethode n“: kms: Entschlüs seln, kms:ReEnc

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
	müssen berücksichtigt werden: - Implementierung einer Zwei-Faktor-Authentifizierung für privilegierte Benutzer - Einführung strenger Kontrollen des Fernzugriffs durch privilegierte Benutzer - Beschränkung der Anzahl privilegierter Benutzer - Gewährung von privilegierten Zugriffen auf „" oder "need-to-haveneed-to-do“ -Basis - Aufrechterhaltung der Audit-Protokollierung der von privilegierten Benutzern ausgeführten Systemaktivitäten - Sicherstellung, dass privilegierte Benutzer keinen Zugriff auf Systemprotokolle haben, in denen ihre Aktivitäten erfasst werden - Durchführung regelmäßiger Audits oder Managementüberprüfungen der Protokolle — Verbot		ryptFrom). Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
	der Weitergabe von privilegierten Daten IDs und deren Zugangsco des — Verbot des privilegierten Zugriffs auf Systeme ohne genaue Überwachu ng und Überwachu ng und _ Schutz von Backup-Daten vor unbefugtem Zugriff		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
3.1.1(h)	h) Systemadministratoren, Sicherheitsbeauftragte, Programmierer und Mitarbeiter, die kritische Vorgänge durchführen, können aufgrund ihrer Aufgaben und ihres privilegierten Zugriffs den von ihnen unterhaltenen oder betriebenen Finanzsystemen schweren Schaden zuzufügen. Mitarbeiter mit erhöhten Systemzugriffsberechtigungen sollten engmaschig beaufsichtigt und alle ihre Systemaktivitäten protokolliert werden, da sie über Insiderwissen und die nötigen Ressourcen verfügen, um Systemkontrollen und Sicherheitsverfahren zu umgehen. Einige der unten aufgeführten Kontroll- und Sicherheitspraktiken	iam-user-group-membership-überprüfen	AWS Identity and Access Management (IAM) kann Ihnen helfen, Zugriffsberechtigungen und Autorisierungen einzuschränken, indem sichergestellt wird, dass Benutzer Mitglieder mindestens einer Gruppe sind. Wenn Benutzern mehr Berechtigungen eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und Aufgabentrennung verstoßen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
	müssen berücksichtigt werden: - Implementierung einer Zwei-Faktor-Authentifizierung für privilegierte Benutzer - Einführung strenger Kontrollen des Fernzugriffs durch privilegierte Benutzer - Beschränkung der Anzahl privilegierter Benutzer - Gewährung von privilegierten Zugriffen auf „" oder "need-to-haveneed-to-do“ -Basis - Aufrechterhaltung der Audit-Protokollierung der von privilegierten Benutzern ausgeführten Systemaktivitäten - Sicherstellung, dass privilegierte Benutzer keinen Zugriff auf Systemprotokolle haben, in denen ihre Aktivitäten erfasst werden - Durchführung regelmäßiger Audits oder Managementüberprüfungen der Protokolle — Verbot		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
	der Weitergabe von privilegierten Daten IDs und deren Zugangsco des — Verbot des privilegierten Zugriffs auf Systeme ohne genaue Überwachu ng und Überwachu ng und _ Schutz von Backup-Daten vor unbefugtem Zugriff		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
3.1.1(h)	h) Systemadm inistratoren, Sicherhei tsbeauftragte, Programmierer und Mitarbeiter, die kritische Vorgänge durchführen, können aufgrund ihrer Aufgaben und ihres privilegierten Zugriffs den von ihnen unterhaltenen oder betriebenen Finanzsystemen schweren Schaden zuzufügen. Mitarbeit er mit erhöhten Systemzugriffsbere chtigungen sollten engmaschig beaufsich tigt und alle ihre Systemaktivitäten protokolliert werden, da sie über Insiderwi ssen und die nötigen Ressourcen verfügen, um Systemkon trollen und Sicherhei tsverfahren zu umgehen. Einige der unten aufgeführ ten Kontroll- und Sicherheitspraktiken	ec2- instance-profile-a ttached	EC2 Instanzprofile übergeben eine IAM-Rolle an eine EC2 Instance. Das Anhängen eines Instance-Profils an Ihre Instances kann bei der Implement ierung von geringste n Berechtigungen und der Berechtig ungsverwaltung helfen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
	müssen berücksichtigt werden: - Implementierung einer Zwei-Faktor-Authentifizierung für privilegierte Benutzer - Einführung strenger Kontrollen des Fernzugriffs durch privilegierte Benutzer - Beschränkung der Anzahl privilegierter Benutzer - Gewährung von privilegierten Zugriffen auf „" oder "need-to-haveneed-to-do“ -Basis - Aufrechterhaltung der Audit-Protokollierung der von privilegierten Benutzern ausgeführten Systemaktivitäten - Sicherstellung, dass privilegierte Benutzer keinen Zugriff auf Systemprotokolle haben, in denen ihre Aktivitäten erfasst werden - Durchführung regelmäßiger Audits oder Managementüberprüfungen der Protokolle — Verbot		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
	der Weitergabe von privilegierten Daten IDs und deren Zugangsco des — Verbot des privilegierten Zugriffs auf Systeme ohne genaue Überwachu ng und Überwachu ng und _ Schutz von Backup-Daten vor unbefugtem Zugriff		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
3.1.1(h)	h) Systemadministratoren, Sicherheitsbeauftragte, Programmierer und Mitarbeiter, die kritische Vorgänge durchführen, können aufgrund ihrer Aufgaben und ihres privilegierten Zugriffs den von ihnen unterhaltenen oder betriebenen Finanzsystemen schweren Schaden zuzufügen. Mitarbeiter mit erhöhten Systemzugriffsberechtigungen sollten engmaschig beaufsichtigt und alle ihre Systemaktivitäten protokolliert werden, da sie über Insiderwissen und die nötigen Ressourcen verfügen, um Systemkontrollen und Sicherheitsverfahren zu umgehen. Einige der unten aufgeführten Kontroll- und Sicherheitspraktiken	iam-policy-no-statements-with-full-access	Stellen Sie sicher, dass IAM-Aktionen nur auf die benötigten Aktionen beschränkt sind. Wenn Benutzern mehr Rechte eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Rechte und der Aufgabentrennung verstoßen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
	müssen berücksichtigt werden: - Implementierung einer Zwei-Faktor-Authentifizierung für privilegierte Benutzer - Einführung strenger Kontrollen des Fernzugriffs durch privilegierte Benutzer - Beschränkung der Anzahl privilegierter Benutzer - Gewährung von privilegierten Zugriffen auf „" oder "need-to-haveneed-to-do“ -Basis - Aufrechterhaltung der Audit-Protokollierung der von privilegierten Benutzern ausgeführten Systemaktivitäten - Sicherstellung, dass privilegierte Benutzer keinen Zugriff auf Systemprotokolle haben, in denen ihre Aktivitäten erfasst werden - Durchführung regelmäßiger Audits oder Managementüberprüfungen der Protokolle — Verbot		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
	der Weitergabe von privilegierten Daten IDs und deren Zugangsco des — Verbot des privilegierten Zugriffs auf Systeme ohne genaue Überwachu ng und Überwachu ng und _ Schutz von Backup-Daten vor unbefugtem Zugriff		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
3.1.1(h)	h) Systemadm inistratoren, Sicherhei tsbeauftragte, Programmierer und Mitarbeiter, die kritische Vorgänge durchführen, können aufgrund ihrer Aufgaben und ihres privilegierten Zugriffs den von ihnen unterhaltenen oder betriebenen Finanzsystemen schweren Schaden zuzufügen. Mitarbeit er mit erhöhten Systemzugriffsbere chtigungen sollten engmaschig beaufsich tigt und alle ihre Systemaktivitäten protokolliert werden, da sie über Insiderwi ssen und die nötigen Ressourcen verfügen, um Systemkon trollen und Sicherhei tsverfahren zu umgehen. Einige der unten aufgeführ ten Kontroll- und Sicherheitspraktiken	ecs-task-definition-user-for-host-mode-check	Wenn für eine Aufgabendefinition erhöhte Berechtig ungen gelten, liegt das daran, dass der Kunde diesen Konfigura tionen ausdrücklich zugestimmt hat. Diese Kontrolle prüft, ob eine unerwartete Berechtigungseskal ation vorliegt, wenn für eine Aufgabend efinition das Host-Netzwerk aktiviert ist, die Kunden aber keine erhöhten Berechtigungen aktiviert haben.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
	müssen berücksichtigt werden: - Implementierung einer Zwei-Faktor-Authentifizierung für privilegierte Benutzer - Einführung strenger Kontrollen des Fernzugriffs durch privilegierte Benutzer - Beschränkung der Anzahl privilegierter Benutzer - Gewährung von privilegierten Zugriffen auf „" oder "need-to-haveneed-to-do“ -Basis - Aufrechterhaltung der Audit-Protokollierung der von privilegierten Benutzern ausgeführten Systemaktivitäten - Sicherstellung, dass privilegierte Benutzer keinen Zugriff auf Systemprotokolle haben, in denen ihre Aktivitäten erfasst werden - Durchführung regelmäßiger Audits oder Managementüberprüfungen der Protokolle — Verbot		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
	der Weitergabe von privilegierten Daten IDs und deren Zugangsco des — Verbot des privilegierten Zugriffs auf Systeme ohne genaue Überwachu ng und Überwachu ng und _ Schutz von Backup-Daten vor unbefugtem Zugriff		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
3.1.1(h)	h) Systemadministratoren, Sicherheitsbeauftragte, Programmierer und Mitarbeiter, die kritische Vorgänge durchführen, können aufgrund ihrer Aufgaben und ihres privilegierten Zugriffs den von ihnen unterhaltenen oder betriebenen Finanzsystemen schweren Schaden zuzufügen. Mitarbeiter mit erhöhten Systemzugriffsberechtigungen sollten engmaschig beaufsichtigt und alle ihre Systemaktivitäten protokolliert werden, da sie über Insiderwissen und die nötigen Ressourcen verfügen, um Systemkontrollen und Sicherheitsverfahren zu umgehen. Einige der unten aufgeführten Kontroll- und Sicherheitspraktiken	elasticsearch-logs-to-cloudwatch	Stellen Sie sicher, dass für Amazon OpenSearch Service-Domains Fehlerprotokolle aktiviert und zur Aufbewahrung und Beantwortung an Amazon CloudWatch Logs gestreamt werden. Domain-Fehlerprotokolle sind bei Sicherheits- und Zugriffsprüfungen sowie bei der Diagnose von Verfügbarkeitsproblemen nützlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
	müssen berücksichtigt werden: - Implementierung einer Zwei-Faktor-Authentifizierung für privilegierte Benutzer - Einführung strenger Kontrollen des Fernzugriffs durch privilegierte Benutzer - Beschränkung der Anzahl privilegierter Benutzer - Gewährung von privilegierten Zugriffen auf „" oder "need-to-haveneed-to-do“ -Basis - Aufrechterhaltung der Audit-Protokollierung der von privilegierten Benutzern ausgeführten Systemaktivitäten - Sicherstellung, dass privilegierte Benutzer keinen Zugriff auf Systemprotokolle haben, in denen ihre Aktivitäten erfasst werden - Durchführung regelmäßiger Audits oder Managementüberprüfungen der Protokolle — Verbot		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
	der Weitergabe von privilegierten Daten IDs und deren Zugangsco des — Verbot des privilegierten Zugriffs auf Systeme ohne genaue Überwachu ng und Überwachu ng und _ Schutz von Backup-Daten vor unbefugtem Zugriff		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
3.1.1(h)	h) Systemadm inistratoren, Sicherhei tsbeauftragte, Programmierer und Mitarbeiter, die kritische Vorgänge durchführen, können aufgrund ihrer Aufgaben und ihres privilegierten Zugriffs den von ihnen unterhaltenen oder betriebenen Finanzsystemen schweren Schaden zuzufügen. Mitarbeit er mit erhöhten Systemzugriffsbere chtigungen sollten engmaschig beaufsich tigt und alle ihre Systemaktivitäten protokolliert werden, da sie über Insiderwi ssen und die nötigen Ressourcen verfügen, um Systemkon trollen und Sicherhei tsverfahren zu umgehen. Einige der unten aufgeführ ten Kontroll- und Sicherheitspraktiken	opensearch-logs-to-cloudwatch	Stellen Sie sicher, dass für Amazon OpenSearch Service-Domains Fehlerpro tokolle aktiviert und zur Aufbewahr ung und Beantwort ung an Amazon CloudWatch Logs gestreamt werden. OpenSearch Service-Fehlerprotokolle können bei Sicherhei ts- und Zugriffsp rüfungen helfen und bei der Diagnose von Verfügbarkeitsprob lemen helfen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
	müssen berücksichtigt werden: - Implementierung einer Zwei-Faktor-Authentifizierung für privilegierte Benutzer - Einführung strenger Kontrollen des Fernzugriffs durch privilegierte Benutzer - Beschränkung der Anzahl privilegierter Benutzer - Gewährung von privilegierten Zugriffen auf „" oder "need-to-haveneed-to-do“ -Basis - Aufrechterhaltung der Audit-Protokollierung der von privilegierten Benutzern ausgeführten Systemaktivitäten - Sicherstellung, dass privilegierte Benutzer keinen Zugriff auf Systemprotokolle haben, in denen ihre Aktivitäten erfasst werden - Durchführung regelmäßiger Audits oder Managementüberprüfungen der Protokolle — Verbot		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
	der Weitergabe von privilegierten Daten IDs und deren Zugangsco des — Verbot des privilegierten Zugriffs auf Systeme ohne genaue Überwachu ng und Überwachu ng und _ Schutz von Backup-Daten vor unbefugtem Zugriff		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
3.1.1(h)	h) Systemadministratoren, Sicherheitsbeauftragte, Programmierer und Mitarbeiter, die kritische Vorgänge durchführen, können aufgrund ihrer Aufgaben und ihres privilegierten Zugriffs den von ihnen unterhaltenen oder betriebenen Finanzsystemen schweren Schaden zuzufügen. Mitarbeiter mit erhöhten Systemzugriffsberechtigungen sollten engmaschig beaufsichtigt und alle ihre Systemaktivitäten protokolliert werden, da sie über Insiderwissen und die nötigen Ressourcen verfügen, um Systemkontrollen und Sicherheitsverfahren zu umgehen. Einige der unten aufgeführten Kontroll- und Sicherheitspraktiken	rds-snapshot-encrypted	Stellen Sie sicher, dass die Verschlüsselung für Ihre Amazon Relational Database Service (Amazon RDS)-Snapshots aktiviert ist. Da sensible Daten auch im Ruhezustand vorhanden sein können, sollten Sie die Verschlüsselung von Daten im Ruhezustand aktivieren, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
	müssen berücksichtigt werden: - Implementierung einer Zwei-Faktor-Authentifizierung für privilegierte Benutzer - Einführung strenger Kontrollen des Fernzugriffs durch privilegierte Benutzer - Beschränkung der Anzahl privilegierter Benutzer - Gewährung von privilegierten Zugriffen auf „" oder "need-to-haveneed-to-do“ -Basis - Aufrechterhaltung der Audit-Protokollierung der von privilegierten Benutzern ausgeführten Systemaktivitäten - Sicherstellung, dass privilegierte Benutzer keinen Zugriff auf Systemprotokolle haben, in denen ihre Aktivitäten erfasst werden - Durchführung regelmäßiger Audits oder Managementüberprüfungen der Protokolle — Verbot		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
	der Weitergabe von privilegierten Daten IDs und deren Zugangsco des — Verbot des privilegierten Zugriffs auf Systeme ohne genaue Überwachu ng und Überwachu ng und _ Schutz von Backup-Daten vor unbefugtem Zugriff		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
3.1.1(h)	h) Systemadm inistratoren, Sicherhei tsbeauftragte, Programmierer und Mitarbeiter, die kritische Vorgänge durchführen, können aufgrund ihrer Aufgaben und ihres privilegierten Zugriffs den von ihnen unterhaltenen oder betriebenen Finanzsystemen schweren Schaden zuzufügen. Mitarbeit er mit erhöhten Systemzugriffsbere chtigungen sollten engmaschig beaufsich tigt und alle ihre Systemaktivitäten protokolliert werden, da sie über Insiderwi ssen und die nötigen Ressourcen verfügen, um Systemkon trollen und Sicherhei tsverfahren zu umgehen. Einige der unten aufgeführ ten Kontroll- und Sicherheitspraktiken	rds-storage-encrypted	Zum Schutz von Daten im Ruhezusta nd müssen Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon Relational Database Service (Amazon RDS)-Instances aktiviert ist. Da sensible Daten in Amazon-RDS-Instances gespeiche rt werden können, sollten Sie die Verschlüsselung von Daten im Ruhezusta nd aktivieren, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
	müssen berücksichtigt werden: - Implementierung einer Zwei-Faktor-Authentifizierung für privilegierte Benutzer - Einführung strenger Kontrollen des Fernzugriffs durch privilegierte Benutzer - Beschränkung der Anzahl privilegierter Benutzer - Gewährung von privilegierten Zugriffen auf „" oder "need-to-haveneed-to-do“ -Basis - Aufrechterhaltung der Audit-Protokollierung der von privilegierten Benutzern ausgeführten Systemaktivitäten - Sicherstellung, dass privilegierte Benutzer keinen Zugriff auf Systemprotokolle haben, in denen ihre Aktivitäten erfasst werden - Durchführung regelmäßiger Audits oder Managementüberprüfungen der Protokolle — Verbot		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
	der Weitergabe von privilegierten Daten IDs und deren Zugangsco des — Verbot des privilegierten Zugriffs auf Systeme ohne genaue Überwachu ng und Überwachu ng und _ Schutz von Backup-Daten vor unbefugtem Zugriff		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
3.1.1(h)	h) Systemadm inistratoren, Sicherhei tsbeauftragte, Programmierer und Mitarbeiter, die kritische Vorgänge durchführen, können aufgrund ihrer Aufgaben und ihres privilegierten Zugriffs den von ihnen unterhaltenen oder betriebenen Finanzsystemen schweren Schaden zuzufügen. Mitarbeit er mit erhöhten Systemzugriffsbere chtigungen sollten engmaschig beaufsich tigt und alle ihre Systemaktivitäten protokolliert werden, da sie über Insiderwi ssen und die nötigen Ressourcen verfügen, um Systemkon trollen und Sicherhei tsverfahren zu umgehen. Einige der unten aufgeführ ten Kontroll- und Sicherheitspraktiken	ec2- ebs-encryption-by-default	Zum Schutz von Daten im Ruhezusta nd müssen Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon Elastic Block Store (Amazon EBS)-Volu mes aktiviert ist. Da sensible Daten in diesen Volumes gespeichert werden können, sollten Sie die Verschlüs selung von Daten im Ruhezustand aktiviere n, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
	müssen berücksichtigt werden: - Implementierung einer Zwei-Faktor-Authentifizierung für privilegierte Benutzer - Einführung strenger Kontrollen des Fernzugriffs durch privilegierte Benutzer - Beschränkung der Anzahl privilegierter Benutzer - Gewährung von privilegierten Zugriffen auf „" oder "need-to-haveneed-to-do“ -Basis - Aufrechterhaltung der Audit-Protokollierung der von privilegierten Benutzern ausgeführten Systemaktivitäten - Sicherstellung, dass privilegierte Benutzer keinen Zugriff auf Systemprotokolle haben, in denen ihre Aktivitäten erfasst werden - Durchführung regelmäßiger Audits oder Managementüberprüfungen der Protokolle — Verbot		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
	der Weitergabe von privilegierten Daten IDs und deren Zugangsco des — Verbot des privilegierten Zugriffs auf Systeme ohne genaue Überwachu ng und Überwachu ng und _ Schutz von Backup-Daten vor unbefugtem Zugriff		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
3.1.1(h)	h) Systemadm inistratoren, Sicherhei tsbeauftragte, Programmierer und Mitarbeiter, die kritische Vorgänge durchführen, können aufgrund ihrer Aufgaben und ihres privilegierten Zugriffs den von ihnen unterhaltenen oder betriebenen Finanzsystemen schweren Schaden zuzufügen. Mitarbeit er mit erhöhten Systemzugriffsbere chtigungen sollten engmaschig beaufsich tigt und alle ihre Systemaktivitäten protokolliert werden, da sie über Insiderwi ssen und die nötigen Ressourcen verfügen, um Systemkon trollen und Sicherhei tsverfahren zu umgehen. Einige der unten aufgeführ ten Kontroll- und Sicherheitspraktiken	efs-encrypted-check	Aktivieren Sie die Verschlüsselung für Ihr Amazon Elastic File System (EFS), um eventuell vorhandene sensible Daten sowie Daten im Ruhezustand zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
	müssen berücksichtigt werden: - Implementierung einer Zwei-Faktor-Authentifizierung für privilegierte Benutzer - Einführung strenger Kontrollen des Fernzugriffs durch privilegierte Benutzer - Beschränkung der Anzahl privilegierter Benutzer - Gewährung von privilegierten Zugriffen auf „" oder "need-to-haveneed-to-do“ -Basis - Aufrechterhaltung der Audit-Protokollierung der von privilegierten Benutzern ausgeführten Systemaktivitäten - Sicherstellung, dass privilegierte Benutzer keinen Zugriff auf Systemprotokolle haben, in denen ihre Aktivitäten erfasst werden - Durchführung regelmäßiger Audits oder Managementüberprüfungen der Protokolle — Verbot		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
	der Weitergabe von privilegierten Daten IDs und deren Zugangsco des — Verbot des privilegierten Zugriffs auf Systeme ohne genaue Überwachu ng und Überwachu ng und _ Schutz von Backup-Daten vor unbefugtem Zugriff		
3.1.2(a)	a) Das BFI sollte an kritischen Stellen seiner IT-Infrastruktur Netzwerksicherheit seinrichtungen wie Firewalls, Antiviren -/Anti-Malware-Sof tware sowie Systeme zur Erkennung und Verhinderung von Angriffen installieren, um die Netzwerkg renzen zu schützen.	alb-waf-enabled	Stellen Sie sicher, dass AWS WAF auf Elastic Load Balancers (ELB) aktiviert ist, um Webanwendungen zu schützen. Eine WAF trägt zum Schutz Ihrer Webanwend ungen oder APIs vor gängigen Web-Explo its bei. Diese Web-Exploits können sich auf die Verfügbar keit auswirken, die Sicherheit gefährden oder übermäßige Ressourcen in Ihrer Umgebung verbrauch en.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
3.1.2(a)	a) Das BFI sollte an kritischen Stellen seiner IT-Infrastruktur Netzwerksicherheit seinrichtungen wie Firewalls, Antiviren -/Anti-Malware-Sof tware sowie Systeme zur Erkennung und Verhinderung von Angriffen installieren, um die Netzwerkg renzen zu schützen.	guardduty-enabled-centralized	Amazon GuardDuty kann mithilfe von Threat Intellige nce Feeds helfen, potenzielle Cybersich erheitsereignisse zu überwachen und zu erkennen. Dazu gehören Listen mit bösartigen IPs und maschinel len Lernmethoden zur Identifizierung unerwarteter, nicht autorisierter und bösartiger Aktivitäten in Ihrer AWS Cloud-Umgebung.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
3.1.2(a)	a) Das BFI sollte an kritischen Stellen seiner IT-Infrastruktur Netzwerksicherheit seinrichtungen wie Firewalls, Antiviren -/Anti-Malware-Sof tware sowie Systeme zur Erkennung und Verhinderung von Angriffen installieren, um die Netzwerkg renzen zu schützen.	api-gw-associated-with-WAF	AWS Mit WAF können Sie eine Reihe von Regeln (als Web Access Control List (Web ACL) bezeichne t) konfigurieren, die Webanfragen auf der Grundlage von anpassbaren Websicherheitsrege ln und -bedingungen, die Sie definieren, zulassen, blockieren oder zählen. Stellen Sie sicher, dass Ihre Amazon-API-Gateway-Stufe mit einer WAF-Web-A CL verknüpft ist, um sie vor böswilligen Angriffen zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
3.1.2(c)	c) Es sollten Kontrollen eingeführt werden, um die Informationssicherheit in Netzwerken und den Schutz vernetzter Services vor unbefugtem Zugriff zu gewährleisten. Insbesondere sollten die folgenden Punkte in Erwägung gezogen werden: - Für die Verwaltung von Netzwerkgeräten sollten Zuständigkeiten und Verfahren festgelegt werden; - Die operative Verantwortung für Netzwerke sollte gegebenenfalls von den Computerorgängen getrennt werden; - Es sollten spezifische Kontrollen eingeführt werden, um die Vertraulichkeit und Integrität von Daten zu gewährleisten, die über öffentliche oder drahtlose Netzwerke übertrage	acm-certificate-expiration-check	Stellen Sie sicher, dass die Netzwerkintegrität geschützt ist, indem Sie sicherstellen, dass X509-Zertifikate von AWS ACM ausgestellt werden. Diese Zertifikate müssen gültig und dürfen nicht abgelaufen sein. Für diese Regel ist ein Wert für erforderlich daysToExpiration (Wert für bewährte AWS Grundregeln für Sicherheit: 90). Der tatsächliche Wert muss den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
	n werden, und um die vernetzten Systeme und Anwendung en zu schützen (einschließlich Netzwerkverschlüss elungsprotokollen bei Verbindungen zu nicht vertrauenswürdigen Systemen/Netzwerke n); - Es sollten eine angemesse ne Protokollierung und Überwachung durchgeführt werden, um die Aufzeichn ung und Erkennung von Aktionen zu ermöglichen, die die Informationssicher heit beeinträchtigen könnten oder für sie relevant sind; - Die Verwaltun gsaktivitäten sollten eng koordiniert werden, um einerseit s den Service für die Organisat ion zu optimieren und andererseits sicherzustellen, dass die Kontrollen in der gesamten Informati		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
	onsverarbeitungsin frastruktur einheitlich angewendet werden; - Die Systeme im Netzwerk sollten authentifiziert werden; und - Nicht vertrauen swürdige Systemver bindungen zum Netzwerk sollten eingeschränkt werden.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
3.1.2(c)	c) Es sollten Kontrollen eingeführt werden, um die Informationssicherheit in Netzwerken und den Schutz vernetzter Services vor unbefugtem Zugriff zu gewährleisten. Insbesondere sollten die folgenden Punkte in Erwägung gezogen werden: - Für die Verwaltung von Netzwerkgeräten sollten Zuständigkeiten und Verfahren festgelegt werden; - Die operative Verantwortung für Netzwerke sollte gegebenenfalls von den Computerorgängen getrennt werden; - Es sollten spezifische Kontrollen eingeführt werden, um die Vertraulichkeit und Integrität von Daten zu gewährleisten, die über öffentliche oder drahtlose Netzwerke übertrage	alb-http-to-https-Umleitungsprüfung	Um Daten während der Übertragung zu schützen, stellen Sie sicher, dass Ihr Application Load Balancer unverschlüsselte HTTP-Anfragen automatisch an HTTPS umleitet. Da sensible Daten vorhanden sein können, sollten Sie die Verschlüsselung bei der Übertragung aktivieren, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
	n werden, und um die vernetzten Systeme und Anwendung en zu schützen (einschließlich Netzwerkverschlüss elungsprotokollen bei Verbindungen zu nicht vertrauenswürdigen Systemen/Netzwerke n); - Es sollten eine angemesse ne Protokollierung und Überwachung durchgeführt werden, um die Aufzeichn ung und Erkennung von Aktionen zu ermöglichen, die die Informationssicher heit beeinträchtigen könnten oder für sie relevant sind; - Die Verwaltun gsaktivitäten sollten eng koordiniert werden, um einerseit s den Service für die Organisat ion zu optimieren und andererseits sicherzustellen, dass die Kontrollen in der gesamten Informati		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
	onsverarbeitungsin frastruktur einheitlich angewendet werden; - Die Systeme im Netzwerk sollten authentifiziert werden; und - Nicht vertrauen swürdige Systemver bindungen zum Netzwerk sollten eingeschränkt werden.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
3.1.2(c)	c) Es sollten Kontrollen eingeführt werden, um die Informationssicherheit in Netzwerken und den Schutz vernetzter Services vor unbefugtem Zugriff zu gewährleisten. Insbesondere sollten die folgenden Punkte in Erwägung gezogen werden: - Für die Verwaltung von Netzwerkgeräten sollten Zuständigkeiten und Verfahren festgelegt werden; - Die operative Verantwortung für Netzwerke sollte gegebenenfalls von den Computerorgängen getrennt werden; - Es sollten spezifische Kontrollen eingeführt werden, um die Vertraulichkeit und Integrität von Daten zu gewährleisten, die über öffentliche oder drahtlose Netzwerke übertrage	elb-acm-certificate-required	Zum Schutz von eventuell vorhandenen sensiblen Daten sowie von Daten während der Übertragung muss die Verschlüsselung für Ihr Elastic Load Balancing aktiviert sein. Verwenden Sie AWS Certificate Manager, um öffentliche und private SSL/TLS-Zertifikate mit AWS Diensten und internen Ressourcen zu verwalten, bereitzustellen und bereitzustellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
	n werden, und um die vernetzten Systeme und Anwendung en zu schützen (einschließlich Netzwerkverschlüss elungsprotokollen bei Verbindungen zu nicht vertrauenswürdigen Systemen/Netzwerke n); - Es sollten eine angemesse ne Protokollierung und Überwachung durchgeführt werden, um die Aufzeichn ung und Erkennung von Aktionen zu ermöglichen, die die Informationssicher heit beeinträchtigen könnten oder für sie relevant sind; - Die Verwaltun gsaktivitäten sollten eng koordiniert werden, um einerseit s den Service für die Organisat ion zu optimieren und andererseits sicherzustellen, dass die Kontrollen in der gesamten Informati		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
	onsverarbeitungsin frastruktur einheitlich angewendet werden; - Die Systeme im Netzwerk sollten authentifiziert werden; und - Nicht vertrauen swürdige Systemver bindungen zum Netzwerk sollten eingeschränkt werden.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
3.1.2(c)	c) Es sollten Kontrollen eingeführt werden, um die Informationssicherheit in Netzwerken und den Schutz vernetzter Services vor unbefugtem Zugriff zu gewährleisten. Insbesondere sollten die folgenden Punkte in Erwägung gezogen werden: - Für die Verwaltung von Netzwerkgeräten sollten Zuständigkeiten und Verfahren festgelegt werden; - Die operative Verantwortung für Netzwerke sollte gegebenenfalls von den Computerorgängen getrennt werden; - Es sollten spezifische Kontrollen eingeführt werden, um die Vertraulichkeit und Integrität von Daten zu gewährleisten, die über öffentliche oder drahtlose Netzwerke übertrage	redshift-require-tls-ssl	Stellen Sie sicher, dass Ihre Amazon-Redshift-Cluster eine TLS/SSL-Verschlüsselung erfordern, um eine Verbindung zu SQL-Clients herzustellen. Da sensible Daten vorhanden sein können, sollten Sie die Verschlüsselung bei der Übertragung aktivieren, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
	n werden, und um die vernetzten Systeme und Anwendung en zu schützen (einschließlich Netzwerkverschlüss elungsprotokollen bei Verbindungen zu nicht vertrauenswürdigen Systemen/Netzwerke n); - Es sollten eine angemesse ne Protokollierung und Überwachung durchgeführt werden, um die Aufzeichn ung und Erkennung von Aktionen zu ermöglichen, die die Informationssicher heit beeinträchtigen könnten oder für sie relevant sind; - Die Verwaltun gsaktivitäten sollten eng koordiniert werden, um einerseit s den Service für die Organisat ion zu optimieren und andererseits sicherzustellen, dass die Kontrollen in der gesamten Informati		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
	onsverarbeitungsin frastruktur einheitlich angewendet werden; - Die Systeme im Netzwerk sollten authentifiziert werden; und - Nicht vertrauen swürdige Systemver bindungen zum Netzwerk sollten eingeschränkt werden.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
3.1.2(c)	c) Es sollten Kontrollen eingeführt werden, um die Informationssicherheit in Netzwerken und den Schutz vernetzter Services vor unbefugtem Zugriff zu gewährleisten. Insbesondere sollten die folgenden Punkte in Erwägung gezogen werden: - Für die Verwaltung von Netzwerkgeräten sollten Zuständigkeiten und Verfahren festgelegt werden; - Die operative Verantwortung für Netzwerke sollte gegebenenfalls von den Computerorgängen getrennt werden; - Es sollten spezifische Kontrollen eingeführt werden, um die Vertraulichkeit und Integrität von Daten zu gewährleisten, die über öffentliche oder drahtlose Netzwerke übertrage	s-3 bucket-ssl-requests-only	Um Daten während der Übertragung zu schützen, stellen Sie sicher, dass Ihre Amazon Simple Storage Service (Amazon S3)-Buckets Anfragen zur Verwendung von Secure Socket Layer (SSL)-Buckets erfordern. Da sensible Daten vorhanden sein können, sollten Sie die Verschlüsselung bei der Übertragung aktivieren, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
	n werden, und um die vernetzten Systeme und Anwendung en zu schützen (einschließlich Netzwerkverschlüss elungsprotokollen bei Verbindungen zu nicht vertrauenswürdigen Systemen/Netzwerke n); - Es sollten eine angemesse ne Protokollierung und Überwachung durchgeführt werden, um die Aufzeichn ung und Erkennung von Aktionen zu ermöglichen, die die Informationssicher heit beeinträchtigen könnten oder für sie relevant sind; - Die Verwaltun gsaktivitäten sollten eng koordiniert werden, um einerseit s den Service für die Organisat ion zu optimieren und andererseits sicherzustellen, dass die Kontrollen in der gesamten Informati		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
	onsverarbeitungsin frastruktur einheitlich angewendet werden; - Die Systeme im Netzwerk sollten authentifiziert werden; und - Nicht vertrauen swürdige Systemver bindungen zum Netzwerk sollten eingeschränkt werden.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
3.1.2(c)	c) Es sollten Kontrolle n eingeführt werden, um die Informati onssicherheit in Netzwerken und den Schutz vernetzte r Services vor unbefugtem Zugriff zu gewährleisten. Insbesondere sollten die folgenden Punkte in Erwägung gezogen werden: - Für die Verwaltung von Netzwerkgeräten sollten Zuständig keiten und Verfahren festgelegt werden; - Die operative Verantwortung für Netzwerke sollte gegebenenfalls von den Computerv orgängen getrennt werden; - Es sollten spezifische Kontrolle n eingeführt werden, um die Vertraulichkeit und Integrität von Daten zu gewährlei sten, die über öffentlic he oder drahtlose Netzwerke übertrage	alb-http-drop-invalid-Header-fähig	Stellen Sie sicher, dass Ihre Elastic Load Balancers (ELB) so konfiguriert sind, dass sie HTTP-Header löschen. Da sensible Daten vorhanden sein können, sollten Sie die Verschlüsselung bei der Übertragung aktivieren, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
	n werden, und um die vernetzten Systeme und Anwendung en zu schützen (einschließlich Netzwerkverschlüss elungsprotokollen bei Verbindungen zu nicht vertrauenswürdigen Systemen/Netzwerke n); - Es sollten eine angemesse ne Protokollierung und Überwachung durchgeführt werden, um die Aufzeichn ung und Erkennung von Aktionen zu ermöglichen, die die Informationssicher heit beeinträchtigen könnten oder für sie relevant sind; - Die Verwaltun gsaktivitäten sollten eng koordiniert werden, um einerseit s den Service für die Organisat ion zu optimieren und andererseits sicherzustellen, dass die Kontrollen in der gesamten Informati		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
	onsverarbeitungsin frastruktur einheitlich angewendet werden; - Die Systeme im Netzwerk sollten authentifiziert werden; und - Nicht vertrauen swürdige Systemver bindungen zum Netzwerk sollten eingeschränkt werden.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
3.1.2(c)	c) Es sollten Kontrollen eingeführt werden, um die Informationssicherheit in Netzwerken und den Schutz vernetzter Services vor unbefugtem Zugriff zu gewährleisten. Insbesondere sollten die folgenden Punkte in Erwägung gezogen werden: - Für die Verwaltung von Netzwerkgeräten sollten Zuständigkeiten und Verfahren festgelegt werden; - Die operative Verantwortung für Netzwerke sollte gegebenenfalls von den Computerorgängen getrennt werden; - Es sollten spezifische Kontrollen eingeführt werden, um die Vertraulichkeit und Integrität von Daten zu gewährleisten, die über öffentliche oder drahtlose Netzwerke übertrage	elasticsearch-node-to-node-Verschlüsselungsprüfung	Stellen Sie sicher, dass die node-to-node Verschlüsselung für Amazon OpenSearch Service aktiviert ist. Node-to-nodeVerschlüsselung ermöglicht die TLS 1.2-Verschlüsselung für die gesamte Kommunikation innerhalb der Amazon Virtual Private Cloud (Amazon VPC). Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
	n werden, und um die vernetzten Systeme und Anwendung en zu schützen (einschließlich Netzwerkverschlüss elungsprotokollen bei Verbindungen zu nicht vertrauenswürdigen Systemen/Netzwerke n); - Es sollten eine angemesse ne Protokollierung und Überwachung durchgeführt werden, um die Aufzeichn ung und Erkennung von Aktionen zu ermöglichen, die die Informationssicher heit beeinträchtigen könnten oder für sie relevant sind; - Die Verwaltun gsaktivitäten sollten eng koordiniert werden, um einerseit s den Service für die Organisat ion zu optimieren und andererseits sicherzustellen, dass die Kontrollen in der gesamten Informati		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
	onsverarbeitungsin frastruktur einheitlich angewendet werden; - Die Systeme im Netzwerk sollten authentifiziert werden; und - Nicht vertrauen swürdige Systemver bindungen zum Netzwerk sollten eingeschränkt werden.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
3.1.2(c)	c) Es sollten Kontrollen eingeführt werden, um die Informationssicherheit in Netzwerken und den Schutz vernetzter Services vor unbefugtem Zugriff zu gewährleisten. Insbesondere sollten die folgenden Punkte in Erwägung gezogen werden: - Für die Verwaltung von Netzwerkgeräten sollten Zuständigkeiten und Verfahren festgelegt werden; - Die operative Verantwortung für Netzwerke sollte gegebenenfalls von den Computerorgängen getrennt werden; - Es sollten spezifische Kontrollen eingeführt werden, um die Vertraulichkeit und Integrität von Daten zu gewährleisten, die über öffentliche oder drahtlose Netzwerke übertrage	opensearch-node-to-node-Verschlüsselungsprüfung	Stellen Sie sicher, dass die node-to-node Verschlüsselung für Amazon OpenSearch Service aktiviert ist. Node-to-nodeVerschlüsselung ermöglicht die TLS 1.2-Verschlüsselung für die gesamte Kommunikation innerhalb der Amazon Virtual Private Cloud (Amazon VPC). Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
	n werden, und um die vernetzten Systeme und Anwendung en zu schützen (einschließlich Netzwerkverschlüss elungsprotokollen bei Verbindungen zu nicht vertrauenswürdigen Systemen/Netzwerke n); - Es sollten eine angemesse ne Protokollierung und Überwachung durchgeführt werden, um die Aufzeichn ung und Erkennung von Aktionen zu ermöglichen, die die Informationssicher heit beeinträchtigen könnten oder für sie relevant sind; - Die Verwaltun gsaktivitäten sollten eng koordiniert werden, um einerseit s den Service für die Organisat ion zu optimieren und andererseits sicherzustellen, dass die Kontrollen in der gesamten Informati		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
	onsverarbeitungsin frastruktur einheitlich angewendet werden; - Die Systeme im Netzwerk sollten authentifiziert werden; und - Nicht vertrauen swürdige Systemver bindungen zum Netzwerk sollten eingeschränkt werden.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
3.1.2(c)	c) Es sollten Kontrolle n eingeführt werden, um die Informati onssicherheit in Netzwerken und den Schutz vernetzte r Services vor unbefugtem Zugriff zu gewährleisten. Insbesondere sollten die folgenden Punkte in Erwägung gezogen werden: - Für die Verwaltung von Netzwerkgeräten sollten Zuständig keiten und Verfahren festgelegt werden; - Die operative Verantwortung für Netzwerke sollte gegebenenfalls von den Computerv orgängen getrennt werden; - Es sollten spezifische Kontrolle n eingeführt werden, um die Vertraulichkeit und Integrität von Daten zu gewährlei sten, die über öffentlic he oder drahtlose Netzwerke übertrage	elb-tls-https-listeners-nur	Stellen Sie sicher, dass Ihre Elastic Load Balancer (ELBs) mit SSL- oder HTTPS-Listenern konfiguriert sind. Um eventuell vorhanden e sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
	n werden, und um die vernetzten Systeme und Anwendung en zu schützen (einschließlich Netzwerkverschlüss elungsprotokollen bei Verbindungen zu nicht vertrauenswürdigen Systemen/Netzwerke n); - Es sollten eine angemesse ne Protokollierung und Überwachung durchgeführt werden, um die Aufzeichn ung und Erkennung von Aktionen zu ermöglichen, die die Informationssicher heit beeinträchtigen könnten oder für sie relevant sind; - Die Verwaltun gsaktivitäten sollten eng koordiniert werden, um einerseit s den Service für die Organisat ion zu optimieren und andererseits sicherzustellen, dass die Kontrollen in der gesamten Informati		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
	onsverarbeitungsin frastruktur einheitlich angewendet werden; - Die Systeme im Netzwerk sollten authentifiziert werden; und - Nicht vertrauen swürdige Systemver bindungen zum Netzwerk sollten eingeschränkt werden.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
3.1.2(c)	c) Es sollten Kontrollen eingeführt werden, um die Informationssicherheit in Netzwerken und den Schutz vernetzter Services vor unbefugtem Zugriff zu gewährleisten. Insbesondere sollten die folgenden Punkte in Erwägung gezogen werden: - Für die Verwaltung von Netzwerkgeräten sollten Zuständigkeiten und Verfahren festgelegt werden; - Die operative Verantwortung für Netzwerke sollte gegebenenfalls von den Computerorgängen getrennt werden; - Es sollten spezifische Kontrollen eingeführt werden, um die Vertraulichkeit und Integrität von Daten zu gewährleisten, die über öffentliche oder drahtlose Netzwerke übertrage	api-gw-execution-logging-aktiviert	Die API-Gateway-Protokollierung zeigt detaillierte Ansichten der Benutzer, die auf die API zugegriffen haben, und wie diese Benutzer auf die API zugegriffen haben. Diese Insights ermöglichen die Einsicht in Benutzeraktivitäten.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
	n werden, und um die vernetzten Systeme und Anwendung en zu schützen (einschließlich Netzwerkverschlüss elungsprotokollen bei Verbindungen zu nicht vertrauenswürdigen Systemen/Netzwerke n); - Es sollten eine angemesse ne Protokollierung und Überwachung durchgeführt werden, um die Aufzeichn ung und Erkennung von Aktionen zu ermöglichen, die die Informationssicher heit beeinträchtigen könnten oder für sie relevant sind; - Die Verwaltun gsaktivitäten sollten eng koordiniert werden, um einerseit s den Service für die Organisat ion zu optimieren und andererseits sicherzustellen, dass die Kontrollen in der gesamten Informati		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
	onsverarbeitungsin frastruktur einheitlich angewendet werden; - Die Systeme im Netzwerk sollten authentifiziert werden; und - Nicht vertrauen swürdige Systemver bindungen zum Netzwerk sollten eingeschränkt werden.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
3.1.2(c)	c) Es sollten Kontrollen eingeführt werden, um die Informationssicherheit in Netzwerken und den Schutz vernetzter Services vor unbefugtem Zugriff zu gewährleisten. Insbesondere sollten die folgenden Punkte in Erwägung gezogen werden: - Für die Verwaltung von Netzwerkgeräten sollten Zuständigkeiten und Verfahren festgelegt werden; - Die operative Verantwortung für Netzwerke sollte gegebenenfalls von den Computerorgängen getrennt werden; - Es sollten spezifische Kontrollen eingeführt werden, um die Vertraulichkeit und Integrität von Daten zu gewährleisten, die über öffentliche oder drahtlose Netzwerke übertrage	cloud-trail-cloud-watch-logs-aktiviert	Verwenden Sie Amazon CloudWatch , um Protokollereignisaktivitäten zentral zu sammeln und zu verwalten. Die Aufnahme von AWS CloudTrail Daten liefert Einzelheiten zu den API-Aufrufaktivitäten in Ihrem AWS-Konto.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
	n werden, und um die vernetzten Systeme und Anwendung en zu schützen (einschließlich Netzwerkverschlüss elungsprotokollen bei Verbindungen zu nicht vertrauenswürdigen Systemen/Netzwerke n); - Es sollten eine angemesse ne Protokollierung und Überwachung durchgeführt werden, um die Aufzeichn ung und Erkennung von Aktionen zu ermöglichen, die die Informationssicher heit beeinträchtigen könnten oder für sie relevant sind; - Die Verwaltun gsaktivitäten sollten eng koordiniert werden, um einerseit s den Service für die Organisat ion zu optimieren und andererseits sicherzustellen, dass die Kontrollen in der gesamten Informati		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
	onsverarbeitungsin frastruktur einheitlich angewendet werden; - Die Systeme im Netzwerk sollten authentifiziert werden; und - Nicht vertrauen swürdige Systemver bindungen zum Netzwerk sollten eingeschränkt werden.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
3.1.2(c)	c) Es sollten Kontrollen eingeführt werden, um die Informationssicherheit in Netzwerken und den Schutz vernetzter Services vor unbefugtem Zugriff zu gewährleisten. Insbesondere sollten die folgenden Punkte in Erwägung gezogen werden: - Für die Verwaltung von Netzwerkgeräten sollten Zuständigkeiten und Verfahren festgelegt werden; - Die operative Verantwortung für Netzwerke sollte gegebenenfalls von den Computerorgängen getrennt werden; - Es sollten spezifische Kontrollen eingeführt werden, um die Vertraulichkeit und Integrität von Daten zu gewährleisten, die über öffentliche oder drahtlose Netzwerke übertrage	cloudtrail-enabled	AWS CloudTrail kann bei der Nichtabstreitbarkeit helfen, indem Aktionen und API-Aufrufe der AWS Management Console aufgezeichnet werden. Sie können die Benutzer und die Benutzer AWS-Konten , die einen AWS Dienst aufgerufen haben, die Quell-IP-Adresse, über die die Aufrufe generiert wurden, und den Zeitpunkt der Anrufe identifizieren. Einzelheiten zu den erfassten Daten finden Sie in den AWS CloudTrail Datensatzinhalten.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
	n werden, und um die vernetzten Systeme und Anwendung en zu schützen (einschließlich Netzwerkverschlüss elungsprotokollen bei Verbindungen zu nicht vertrauenswürdigen Systemen/Netzwerke n); - Es sollten eine angemesse ne Protokollierung und Überwachung durchgeführt werden, um die Aufzeichn ung und Erkennung von Aktionen zu ermöglichen, die die Informationssicher heit beeinträchtigen könnten oder für sie relevant sind; - Die Verwaltun gsaktivitäten sollten eng koordiniert werden, um einerseit s den Service für die Organisat ion zu optimieren und andererseits sicherzustellen, dass die Kontrollen in der gesamten Informati		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
	onsverarbeitungsin frastruktur einheitlich angewendet werden; - Die Systeme im Netzwerk sollten authentifiziert werden; und - Nicht vertrauen swürdige Systemver bindungen zum Netzwerk sollten eingeschränkt werden.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
3.1.2(c)	c) Es sollten Kontrollen eingeführt werden, um die Informationssicherheit in Netzwerken und den Schutz vernetzter Services vor unbefugtem Zugriff zu gewährleisten. Insbesondere sollten die folgenden Punkte in Erwägung gezogen werden: - Für die Verwaltung von Netzwerkgeräten sollten Zuständigkeiten und Verfahren festgelegt werden; - Die operative Verantwortung für Netzwerke sollte gegebenenfalls von den Computerorgängen getrennt werden; - Es sollten spezifische Kontrollen eingeführt werden, um die Vertraulichkeit und Integrität von Daten zu gewährleisten, die über öffentliche oder drahtlose Netzwerke übertrage	cloudtrail-s3-dataevents-enabled	Die Erfassung von Simple Storage Service (Amazon S3)-Datenereignissen unterstützt die Erkennung von ungewöhnlichen Aktivitäten. Zu den Details gehören AWS-Konto Informationen über den Zugriff auf einen Amazon S3 S3-Bucket, die IP-Adresse und die Uhrzeit des Ereignisses.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
	n werden, und um die vernetzten Systeme und Anwendung en zu schützen (einschließlich Netzwerkverschlüss elungsprotokollen bei Verbindungen zu nicht vertrauenswürdigen Systemen/Netzwerke n); - Es sollten eine angemesse ne Protokollierung und Überwachung durchgeführt werden, um die Aufzeichn ung und Erkennung von Aktionen zu ermöglichen, die die Informationssicher heit beeinträchtigen könnten oder für sie relevant sind; - Die Verwaltun gsaktivitäten sollten eng koordiniert werden, um einerseit s den Service für die Organisat ion zu optimieren und andererseits sicherzustellen, dass die Kontrollen in der gesamten Informati		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
	onsverarbeitungsin frastruktur einheitlich angewendet werden; - Die Systeme im Netzwerk sollten authentifiziert werden; und - Nicht vertrauen swürdige Systemver bindungen zum Netzwerk sollten eingeschränkt werden.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
3.1.2(c)	c) Es sollten Kontrollen eingeführt werden, um die Informationssicherheit in Netzwerken und den Schutz vernetzter Services vor unbefugtem Zugriff zu gewährleisten. Insbesondere sollten die folgenden Punkte in Erwägung gezogen werden: - Für die Verwaltung von Netzwerkgeräten sollten Zuständigkeiten und Verfahren festgelegt werden; - Die operative Verantwortung für Netzwerke sollte gegebenenfalls von den Computerorgängen getrennt werden; - Es sollten spezifische Kontrollen eingeführt werden, um die Vertraulichkeit und Integrität von Daten zu gewährleisten, die über öffentliche oder drahtlose Netzwerke übertrage	cloudwatch-alarm-action-check	Amazon CloudWatch alarmiert, wenn eine Metrik den Schwellenwert für eine bestimmte Anzahl von Bewertungszeiträumen überschreitet. Der Alarm führt eine oder mehrere Aktionen durch, die vom Wert der Metrik oder des Ausdrucks im Vergleich zu einem Schwellenwert in einer Reihe von Zeiträumen abhängt. Diese Regel erfordert einen Wert für alarmActionRequired (Config Default: True), insufficientDataAction Required (Config Default: True), okActionRequired (Config Default: False). Der tatsächliche Wert muss die Alarmaktionen für Ihre Umgebung widerspiegeln.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
	n werden, und um die vernetzten Systeme und Anwendung en zu schützen (einschließlich Netzwerkverschlüss elungsprotokollen bei Verbindungen zu nicht vertrauenswürdigen Systemen/Netzwerke n); - Es sollten eine angemesse ne Protokollierung und Überwachung durchgeführt werden, um die Aufzeichn ung und Erkennung von Aktionen zu ermöglichen, die die Informationssicher heit beeinträchtigen könnten oder für sie relevant sind; - Die Verwaltun gsaktivitäten sollten eng koordiniert werden, um einerseit s den Service für die Organisat ion zu optimieren und andererseits sicherzustellen, dass die Kontrollen in der gesamten Informati		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
	onsverarbeitungsin frastruktur einheitlich angewendet werden; - Die Systeme im Netzwerk sollten authentifiziert werden; und - Nicht vertrauen swürdige Systemver bindungen zum Netzwerk sollten eingeschränkt werden.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
3.1.2(c)	c) Es sollten Kontrollen eingeführt werden, um die Informationssicherheit in Netzwerken und den Schutz vernetzter Services vor unbefugtem Zugriff zu gewährleisten. Insbesondere sollten die folgenden Punkte in Erwägung gezogen werden: - Für die Verwaltung von Netzwerkgeräten sollten Zuständigkeiten und Verfahren festgelegt werden; - Die operative Verantwortung für Netzwerke sollte gegebenenfalls von den Computerorgängen getrennt werden; - Es sollten spezifische Kontrollen eingeführt werden, um die Vertraulichkeit und Integrität von Daten zu gewährleisten, die über öffentliche oder drahtlose Netzwerke übertrage	elb-logging-enabled	Die Elastic-Load-Balancing-Aktivität ist ein zentraler Kommunikationspunkt innerhalb einer Umgebung. Stellen Sie sicher, dass die ELB-Protokollierung aktiviert ist. Die gesammelten Daten enthalten detaillierte Informationen zu Anfragen, die an den ELB gesendet wurden. Jedes Protokoll enthält Informationen wie die Zeit, zu der die Anforderung einging, die Client-IP-Adresse, Latenzen, Anforderungspfade und Serverantworten.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
	n werden, und um die vernetzten Systeme und Anwendung en zu schützen (einschließlich Netzwerkverschlüss elungsprotokollen bei Verbindungen zu nicht vertrauenswürdigen Systemen/Netzwerke n); - Es sollten eine angemesse ne Protokollierung und Überwachung durchgeführt werden, um die Aufzeichn ung und Erkennung von Aktionen zu ermöglichen, die die Informationssicher heit beeinträchtigen könnten oder für sie relevant sind; - Die Verwaltun gsaktivitäten sollten eng koordiniert werden, um einerseit s den Service für die Organisat ion zu optimieren und andererseits sicherzustellen, dass die Kontrollen in der gesamten Informati		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
	onsverarbeitungsin frastruktur einheitlich angewendet werden; - Die Systeme im Netzwerk sollten authentifiziert werden; und - Nicht vertrauen swürdige Systemver bindungen zum Netzwerk sollten eingeschränkt werden.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
3.1.2(c)	c) Es sollten Kontrolle n eingeführt werden, um die Informati onssicherheit in Netzwerken und den Schutz vernetzte r Services vor unbefugtem Zugriff zu gewährleisten. Insbesondere sollten die folgenden Punkte in Erwägung gezogen werden: - Für die Verwaltung von Netzwerkgeräten sollten Zuständig keiten und Verfahren festgelegt werden; - Die operative Verantwortung für Netzwerke sollte gegebenenfalls von den Computerv orgängen getrennt werden; - Es sollten spezifische Kontrolle n eingeführt werden, um die Vertraulichkeit und Integrität von Daten zu gewährlei sten, die über öffentlic he oder drahtlose Netzwerke übertrage	guardduty-enabled-centralized	Amazon GuardDuty kann mithilfe von Threat Intellige nce Feeds helfen, potenzielle Cybersich erheitsereignisse zu überwachen und zu erkennen. Dazu gehören Listen mit bösartigen IPs und maschinel len Lernmethoden zur Identifizierung unerwarteter, nicht autorisierter und bösartiger Aktivitäten in Ihrer AWS Cloud-Umgebung.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
	n werden, und um die vernetzten Systeme und Anwendung en zu schützen (einschließlich Netzwerkverschlüss elungsprotokollen bei Verbindungen zu nicht vertrauenswürdigen Systemen/Netzwerke n); - Es sollten eine angemesse ne Protokollierung und Überwachung durchgeführt werden, um die Aufzeichn ung und Erkennung von Aktionen zu ermöglichen, die die Informationssicher heit beeinträchtigen könnten oder für sie relevant sind; - Die Verwaltun gsaktivitäten sollten eng koordiniert werden, um einerseit s den Service für die Organisat ion zu optimieren und andererseits sicherzustellen, dass die Kontrollen in der gesamten Informati		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
	onsverarbeitungsin frastruktur einheitlich angewendet werden; - Die Systeme im Netzwerk sollten authentifiziert werden; und - Nicht vertrauen swürdige Systemver bindungen zum Netzwerk sollten eingeschränkt werden.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
3.1.2(c)	c) Es sollten Kontrolle n eingeführt werden, um die Informati onssicherheit in Netzwerken und den Schutz vernetzte r Services vor unbefugtem Zugriff zu gewährleisten. Insbesondere sollten die folgenden Punkte in Erwägung gezogen werden: - Für die Verwaltung von Netzwerkgeräten sollten Zuständig keiten und Verfahren festgelegt werden; - Die operative Verantwortung für Netzwerke sollte gegebenenfalls von den Computerv orgängen getrennt werden; - Es sollten spezifische Kontrolle n eingeführt werden, um die Vertraulichkeit und Integrität von Daten zu gewährlei sten, die über öffentlic he oder drahtlose Netzwerke übertrage	lambda-dlq-check	Aktivieren Sie diese Regel, um das entsprechende Personal über Amazon Simple Queue Service (Amazon SQS) oder Amazon Simple Notification Service (Amazon SNS) zu benachrichtigen, wenn eine Funktion ausgefallen ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
	n werden, und um die vernetzten Systeme und Anwendung en zu schützen (einschließlich Netzwerkverschlüss elungsprotokollen bei Verbindungen zu nicht vertrauenswürdigen Systemen/Netzwerke n); - Es sollten eine angemesse ne Protokollierung und Überwachung durchgeführt werden, um die Aufzeichn ung und Erkennung von Aktionen zu ermöglichen, die die Informationssicher heit beeinträchtigen könnten oder für sie relevant sind; - Die Verwaltun gsaktivitäten sollten eng koordiniert werden, um einerseit s den Service für die Organisat ion zu optimieren und andererseits sicherzustellen, dass die Kontrollen in der gesamten Informati		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
	onsverarbeitungsin frastruktur einheitlich angewendet werden; - Die Systeme im Netzwerk sollten authentifiziert werden; und - Nicht vertrauen swürdige Systemver bindungen zum Netzwerk sollten eingeschränkt werden.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
3.1.2(c)	c) Es sollten Kontrolle n eingeführt werden, um die Informati onssicherheit in Netzwerken und den Schutz vernetzte r Services vor unbefugtem Zugriff zu gewährleisten. Insbesondere sollten die folgenden Punkte in Erwägung gezogen werden: - Für die Verwaltung von Netzwerkgeräten sollten Zuständig keiten und Verfahren festgelegt werden; - Die operative Verantwortung für Netzwerke sollte gegebenenfalls von den Computerv orgängen getrennt werden; - Es sollten spezifische Kontrolle n eingeführt werden, um die Vertraulichkeit und Integrität von Daten zu gewährlei sten, die über öffentlic he oder drahtlose Netzwerke übertrage	multi-region-cloudtrail-enabled	AWS CloudTrail zeichnet Aktionen und API-Aufrufe der AWS Management Console auf. Sie können feststellen, welche Benutzer und Konten angerufen wurden AWS, von welcher Quell-IP-Adresse aus die Anrufe getätigt wurden und wann die Anrufe erfolgten. CloudTrail übermittelt Protokolldateien aus allen AWS Regionen an Ihren S3-Bucket , wenn MULTI_REG ION_CLOUD _TRAIL_ENABLED aktiviert ist. Außerdem wird beim AWS Start einer neuen Region derselbe Trail in der neuen Region erstellt. CloudTrail Dadurch erhalten Sie automatis ch Protokolldateien mit API-Aktivitäten für die neue Region.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
	n werden, und um die vernetzten Systeme und Anwendung en zu schützen (einschließlich Netzwerkverschlüss elungsprotokollen bei Verbindungen zu nicht vertrauenswürdigen Systemen/Netzwerke n); - Es sollten eine angemesse ne Protokollierung und Überwachung durchgeführt werden, um die Aufzeichn ung und Erkennung von Aktionen zu ermöglichen, die die Informationssicher heit beeinträchtigen könnten oder für sie relevant sind; - Die Verwaltun gsaktivitäten sollten eng koordiniert werden, um einerseit s den Service für die Organisat ion zu optimieren und andererseits sicherzustellen, dass die Kontrollen in der gesamten Informati		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
	onsverarbeitungsin frastruktur einheitlich angewendet werden; - Die Systeme im Netzwerk sollten authentifiziert werden; und - Nicht vertrauen swürdige Systemver bindungen zum Netzwerk sollten eingeschränkt werden.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
3.1.2(c)	c) Es sollten Kontrolle n eingeführt werden, um die Informati onssicherheit in Netzwerken und den Schutz vernetzte r Services vor unbefugtem Zugriff zu gewährleisten. Insbesondere sollten die folgenden Punkte in Erwägung gezogen werden: - Für die Verwaltung von Netzwerkgeräten sollten Zuständig keiten und Verfahren festgelegt werden; - Die operative Verantwortung für Netzwerke sollte gegebenenfalls von den Computerv orgängen getrennt werden; - Es sollten spezifische Kontrolle n eingeführt werden, um die Vertraulichkeit und Integrität von Daten zu gewährlei sten, die über öffentlic he oder drahtlose Netzwerke übertrage	s-3 bucket-logging-enabled	Die Amazon Simple Storage Service (Amazon S3)-Serverzugriffs protokollierung bietet eine Methode zur Überwachu ng des Netzwerks im Hinblick auf potenzielle Cybersich erheitsereignisse. Die Ereignisse werden überwacht, indem detaillierte Aufzeichn ungen über die Anfragen erfasst werden, die an einen Amazon-S3-Bucket gestellt wurden. Jeder Zugriffsprotokolle intrag enthält Details zu einer einzelnen Zugriffsanfrage. Zu den Details gehören Anforderer, Bucket-Name, Anforderu ngszeit, Anforderu ngsaktion, Antwortst atus und Fehlercode, falls relevant.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
	n werden, und um die vernetzten Systeme und Anwendung en zu schützen (einschließlich Netzwerkverschlüss elungsprotokollen bei Verbindungen zu nicht vertrauenswürdigen Systemen/Netzwerke n); - Es sollten eine angemesse ne Protokollierung und Überwachung durchgeführt werden, um die Aufzeichn ung und Erkennung von Aktionen zu ermöglichen, die die Informationssicher heit beeinträchtigen könnten oder für sie relevant sind; - Die Verwaltun gsaktivitäten sollten eng koordiniert werden, um einerseit s den Service für die Organisat ion zu optimieren und andererseits sicherzustellen, dass die Kontrollen in der gesamten Informati		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
	onsverarbeitungsin frastruktur einheitlich angewendet werden; - Die Systeme im Netzwerk sollten authentifiziert werden; und - Nicht vertrauen swürdige Systemver bindungen zum Netzwerk sollten eingeschränkt werden.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
3.1.2(c)	c) Es sollten Kontrollen eingeführt werden, um die Informationssicherheit in Netzwerken und den Schutz vernetzter Services vor unbefugtem Zugriff zu gewährleisten. Insbesondere sollten die folgenden Punkte in Erwägung gezogen werden: - Für die Verwaltung von Netzwerkgeräten sollten Zuständigkeiten und Verfahren festgelegt werden; - Die operative Verantwortung für Netzwerke sollte gegebenenfalls von den Computerorgängen getrennt werden; - Es sollten spezifische Kontrollen eingeführt werden, um die Vertraulichkeit und Integrität von Daten zu gewährleisten, die über öffentliche oder drahtlose Netzwerke übertrage	securityhub-enabled	AWS Security Hub hilft bei der Überwachung von unbefugtem Personal, Verbindungen, Geräten und Software. AWS Security Hub aggregiert, organisiert und priorisiert die Sicherheitswarnungen oder Ergebnisse mehrerer Dienste. AWS Einige dieser Dienste sind Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer und AWS Firewall Manager sowie AWS Partnerlösungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
	n werden, und um die vernetzten Systeme und Anwendung en zu schützen (einschließlich Netzwerkverschlüss elungsprotokollen bei Verbindungen zu nicht vertrauenswürdigen Systemen/Netzwerke n); - Es sollten eine angemesse ne Protokollierung und Überwachung durchgeführt werden, um die Aufzeichn ung und Erkennung von Aktionen zu ermöglichen, die die Informationssicher heit beeinträchtigen könnten oder für sie relevant sind; - Die Verwaltun gsaktivitäten sollten eng koordiniert werden, um einerseit s den Service für die Organisat ion zu optimieren und andererseits sicherzustellen, dass die Kontrollen in der gesamten Informati		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
	onsverarbeitungsin frastruktur einheitlich angewendet werden; - Die Systeme im Netzwerk sollten authentifiziert werden; und - Nicht vertrauen swürdige Systemver bindungen zum Netzwerk sollten eingeschränkt werden.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
3.1.2(c)	c) Es sollten Kontrollen eingeführt werden, um die Informationssicherheit in Netzwerken und den Schutz vernetzter Services vor unbefugtem Zugriff zu gewährleisten. Insbesondere sollten die folgenden Punkte in Erwägung gezogen werden: - Für die Verwaltung von Netzwerkgeräten sollten Zuständigkeiten und Verfahren festgelegt werden; - Die operative Verantwortung für Netzwerke sollte gegebenenfalls von den Computerorgängen getrennt werden; - Es sollten spezifische Kontrollen eingeführt werden, um die Vertraulichkeit und Integrität von Daten zu gewährleisten, die über öffentliche oder drahtlose Netzwerke übertrage	rds-logging-enabled	Um die Protokollierung und Überwachung in Ihrer Umgebung zu erleichtern, stellen Sie sicher, dass die Amazon Relational Database Service (Amazon RDS)-Protokollierung aktiviert ist. Mit der Amazon-RDS-Protokollierung können Sie Ereignisse wie Verbindungen, Verbindungsabbrüche, Abfragen oder abgefragte Tabellen erfassen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
	n werden, und um die vernetzten Systeme und Anwendung en zu schützen (einschließlich Netzwerkverschlüss elungsprotokollen bei Verbindungen zu nicht vertrauenswürdigen Systemen/Netzwerke n); - Es sollten eine angemesse ne Protokollierung und Überwachung durchgeführt werden, um die Aufzeichn ung und Erkennung von Aktionen zu ermöglichen, die die Informationssicher heit beeinträchtigen könnten oder für sie relevant sind; - Die Verwaltun gsaktivitäten sollten eng koordiniert werden, um einerseit s den Service für die Organisat ion zu optimieren und andererseits sicherzustellen, dass die Kontrollen in der gesamten Informati		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
	onsverarbeitungsin frastruktur einheitlich angewendet werden; - Die Systeme im Netzwerk sollten authentifiziert werden; und - Nicht vertrauen swürdige Systemver bindungen zum Netzwerk sollten eingeschränkt werden.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
3.1.2(c)	c) Es sollten Kontrollen eingeführt werden, um die Informationssicherheit in Netzwerken und den Schutz vernetzter Services vor unbefugtem Zugriff zu gewährleisten. Insbesondere sollten die folgenden Punkte in Erwägung gezogen werden: - Für die Verwaltung von Netzwerkgeräten sollten Zuständigkeiten und Verfahren festgelegt werden; - Die operative Verantwortung für Netzwerke sollte gegebenenfalls von den Computerorgängen getrennt werden; - Es sollten spezifische Kontrollen eingeführt werden, um die Vertraulichkeit und Integrität von Daten zu gewährleisten, die über öffentliche oder drahtlose Netzwerke übertrage	wafv2-logging-enabled	Um Ihnen bei der Protokollierung und Überwachung in Ihrer Umgebung zu helfen, aktivieren Sie die AWS WAF (V2) -Protokollierung im regionalen und globalen Web. ACLs AWS Die WAF-Protokollierung bietet detaillierte Informationen über den Datenverkehr, der von Ihrer Web-ACL analysiert wird. In den Protokollen werden die Uhrzeit aufgezeichnet, zu der die AWS WAF die Anfrage von Ihrer AWS Ressource erhalten hat, Informationen zu der Anfrage und eine Aktion für die Regel, der jede Anfrage entsprach.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
	n werden, und um die vernetzten Systeme und Anwendung en zu schützen (einschließlich Netzwerkverschlüss elungsprotokollen bei Verbindungen zu nicht vertrauenswürdigen Systemen/Netzwerke n); - Es sollten eine angemesse ne Protokollierung und Überwachung durchgeführt werden, um die Aufzeichn ung und Erkennung von Aktionen zu ermöglichen, die die Informationssicher heit beeinträchtigen könnten oder für sie relevant sind; - Die Verwaltun gsaktivitäten sollten eng koordiniert werden, um einerseit s den Service für die Organisat ion zu optimieren und andererseits sicherzustellen, dass die Kontrollen in der gesamten Informati		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
	onsverarbeitungsin frastruktur einheitlich angewendet werden; - Die Systeme im Netzwerk sollten authentifiziert werden; und - Nicht vertrauen swürdige Systemver bindungen zum Netzwerk sollten eingeschränkt werden.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
3.1.2(c)	c) Es sollten Kontrollen eingeführt werden, um die Informationssicherheit in Netzwerken und den Schutz vernetzter Services vor unbefugtem Zugriff zu gewährleisten. Insbesondere sollten die folgenden Punkte in Erwägung gezogen werden: - Für die Verwaltung von Netzwerkgeräten sollten Zuständigkeiten und Verfahren festgelegt werden; - Die operative Verantwortung für Netzwerke sollte gegebenenfalls von den Computerorgängen getrennt werden; - Es sollten spezifische Kontrollen eingeführt werden, um die Vertraulichkeit und Integrität von Daten zu gewährleisten, die über öffentliche oder drahtlose Netzwerke übertrage	redshift-cluster-configuration-check	Um Daten im Ruhezustand zu schützen, muss die Verschlüsselung für Ihre Amazon-Redshift-Cluster aktiviert sein. Sie müssen auch sicherstellen, dass die erforderlichen Konfigurationen auf Amazon-Redshift-Clustern bereitgestellt werden. Die Prüfungsprotokollierung muss aktiviert sein, um Informationen zu Verbindungen und Benutzeraktivitäten in der Datenbank bereitzustellen. Diese Regel erfordert, dass ein Wert für clusterDbEncrypted (Config Default: TRUE) und LoggingEnabled (Config Default: TRUE) gesetzt ist. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
	n werden, und um die vernetzten Systeme und Anwendung en zu schützen (einschließlich Netzwerkverschlüss elungsprotokollen bei Verbindungen zu nicht vertrauenswürdigen Systemen/Netzwerke n); - Es sollten eine angemesse ne Protokollierung und Überwachung durchgeführt werden, um die Aufzeichn ung und Erkennung von Aktionen zu ermöglichen, die die Informationssicher heit beeinträchtigen könnten oder für sie relevant sind; - Die Verwaltun gsaktivitäten sollten eng koordiniert werden, um einerseit s den Service für die Organisat ion zu optimieren und andererseits sicherzustellen, dass die Kontrollen in der gesamten Informati		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
	onsverarbeitungsin frastruktur einheitlich angewendet werden; - Die Systeme im Netzwerk sollten authentifiziert werden; und - Nicht vertrauen swürdige Systemver bindungen zum Netzwerk sollten eingeschränkt werden.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
3.1.2(c)	c) Es sollten Kontrollen eingeführt werden, um die Informationssicherheit in Netzwerken und den Schutz vernetzter Services vor unbefugtem Zugriff zu gewährleisten. Insbesondere sollten die folgenden Punkte in Erwägung gezogen werden: - Für die Verwaltung von Netzwerkgeräten sollten Zuständigkeiten und Verfahren festgelegt werden; - Die operative Verantwortung für Netzwerke sollte gegebenenfalls von den Computerorgängen getrennt werden; - Es sollten spezifische Kontrollen eingeführt werden, um die Vertraulichkeit und Integrität von Daten zu gewährleisten, die über öffentliche oder drahtlose Netzwerke übertrage	dms-replication-not-public	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass auf DMS-Replikationsinstanzen nicht öffentlich zugegriffen werden kann. DMS-Replikations-Instances können vertrauliche Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
	n werden, und um die vernetzten Systeme und Anwendung en zu schützen (einschließlich Netzwerkverschlüss elungsprotokollen bei Verbindungen zu nicht vertrauenswürdigen Systemen/Netzwerke n); - Es sollten eine angemesse ne Protokollierung und Überwachung durchgeführt werden, um die Aufzeichn ung und Erkennung von Aktionen zu ermöglichen, die die Informationssicher heit beeinträchtigen könnten oder für sie relevant sind; - Die Verwaltun gsaktivitäten sollten eng koordiniert werden, um einerseit s den Service für die Organisat ion zu optimieren und andererseits sicherzustellen, dass die Kontrollen in der gesamten Informati		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
	onsverarbeitungsin frastruktur einheitlich angewendet werden; - Die Systeme im Netzwerk sollten authentifiziert werden; und - Nicht vertrauen swürdige Systemver bindungen zum Netzwerk sollten eingeschränkt werden.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
3.1.2(c)	c) Es sollten Kontrolle n eingeführt werden, um die Informati onssicherheit in Netzwerken und den Schutz vernetzte r Services vor unbefugtem Zugriff zu gewährleisten. Insbesondere sollten die folgenden Punkte in Erwägung gezogen werden: - Für die Verwaltung von Netzwerkgeräten sollten Zuständig keiten und Verfahren festgelegt werden; - Die operative Verantwortung für Netzwerke sollte gegebenenfalls von den Computerv orgängen getrennt werden; - Es sollten spezifische Kontrolle n eingeführt werden, um die Vertraulichkeit und Integrität von Daten zu gewährlei sten, die über öffentlic he oder drahtlose Netzwerke übertrage	ebs-snapshot-public-restorable-überprüfen	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass EBS-Snapshots nicht öffentlich wiederher stellbar sind. EBS-Volume-Snapsho ts können vertrauli che Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
	n werden, und um die vernetzten Systeme und Anwendung en zu schützen (einschließlich Netzwerkverschlüss elungsprotokollen bei Verbindungen zu nicht vertrauenswürdigen Systemen/Netzwerke n); - Es sollten eine angemesse ne Protokollierung und Überwachung durchgeführt werden, um die Aufzeichn ung und Erkennung von Aktionen zu ermöglichen, die die Informationssicher heit beeinträchtigen könnten oder für sie relevant sind; - Die Verwaltun gsaktivitäten sollten eng koordiniert werden, um einerseit s den Service für die Organisat ion zu optimieren und andererseits sicherzustellen, dass die Kontrollen in der gesamten Informati		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
	onsverarbeitungsin frastruktur einheitlich angewendet werden; - Die Systeme im Netzwerk sollten authentifiziert werden; und - Nicht vertrauen swürdige Systemver bindungen zum Netzwerk sollten eingeschränkt werden.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
3.1.2(c)	c) Es sollten Kontrollen eingeführt werden, um die Informationssicherheit in Netzwerken und den Schutz vernetzter Services vor unbefugtem Zugriff zu gewährleisten. Insbesondere sollten die folgenden Punkte in Erwägung gezogen werden: - Für die Verwaltung von Netzwerkgeräten sollten Zuständigkeiten und Verfahren festgelegt werden; - Die operative Verantwortung für Netzwerke sollte gegebenenfalls von den Computerorgängen getrennt werden; - Es sollten spezifische Kontrollen eingeführt werden, um die Vertraulichkeit und Integrität von Daten zu gewährleisten, die über öffentliche oder drahtlose Netzwerke übertrage	ec-2 instance-no-public-ip	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon Elastic Compute Cloud (Amazon EC2) - Instances nicht öffentlich zugänglich sind. EC2 Amazon-Instances können vertrauliche Informationen enthalten, und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
	n werden, und um die vernetzten Systeme und Anwendung en zu schützen (einschließlich Netzwerkverschlüss elungsprotokollen bei Verbindungen zu nicht vertrauenswürdigen Systemen/Netzwerke n); - Es sollten eine angemesse ne Protokollierung und Überwachung durchgeführt werden, um die Aufzeichn ung und Erkennung von Aktionen zu ermöglichen, die die Informationssicher heit beeinträchtigen könnten oder für sie relevant sind; - Die Verwaltun gsaktivitäten sollten eng koordiniert werden, um einerseit s den Service für die Organisat ion zu optimieren und andererseits sicherzustellen, dass die Kontrollen in der gesamten Informati		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
	onsverarbeitungsin frastruktur einheitlich angewendet werden; - Die Systeme im Netzwerk sollten authentifiziert werden; und - Nicht vertrauen swürdige Systemver bindungen zum Netzwerk sollten eingeschränkt werden.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
3.1.2(c)	c) Es sollten Kontrollen eingeführt werden, um die Informationssicherheit in Netzwerken und den Schutz vernetzter Services vor unbefugtem Zugriff zu gewährleisten. Insbesondere sollten die folgenden Punkte in Erwägung gezogen werden: - Für die Verwaltung von Netzwerkgeräten sollten Zuständigkeiten und Verfahren festgelegt werden; - Die operative Verantwortung für Netzwerke sollte gegebenenfalls von den Computerorgängen getrennt werden; - Es sollten spezifische Kontrollen eingeführt werden, um die Vertraulichkeit und Integrität von Daten zu gewährleisten, die über öffentliche oder drahtlose Netzwerke übertrage	elasticsearch-in-vpc-only	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass sich Amazon OpenSearch OpenSearch Service (Service) - Domains innerhalb einer Amazon Virtual Private Cloud (Amazon VPC) befinden. Eine OpenSearch Service-Domain innerhalb einer Amazon VPC ermöglicht die sichere Kommunikation zwischen OpenSearch Service und anderen Services innerhalb der Amazon VPC, ohne dass ein Internet-Gateway, ein NAT-Gerät oder eine VPN-Verbindung erforderlich ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
	n werden, und um die vernetzten Systeme und Anwendung en zu schützen (einschließlich Netzwerkverschlüss elungsprotokollen bei Verbindungen zu nicht vertrauenswürdigen Systemen/Netzwerke n); - Es sollten eine angemesse ne Protokollierung und Überwachung durchgeführt werden, um die Aufzeichn ung und Erkennung von Aktionen zu ermöglichen, die die Informationssicher heit beeinträchtigen könnten oder für sie relevant sind; - Die Verwaltun gsaktivitäten sollten eng koordiniert werden, um einerseit s den Service für die Organisat ion zu optimieren und andererseits sicherzustellen, dass die Kontrollen in der gesamten Informati		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
	onsverarbeitungsin frastruktur einheitlich angewendet werden; - Die Systeme im Netzwerk sollten authentifiziert werden; und - Nicht vertrauen swürdige Systemver bindungen zum Netzwerk sollten eingeschränkt werden.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
3.1.2(c)	c) Es sollten Kontrollen eingeführt werden, um die Informationssicherheit in Netzwerken und den Schutz vernetzter Services vor unbefugtem Zugriff zu gewährleisten. Insbesondere sollten die folgenden Punkte in Erwägung gezogen werden: - Für die Verwaltung von Netzwerkgeräten sollten Zuständigkeiten und Verfahren festgelegt werden; - Die operative Verantwortung für Netzwerke sollte gegebenenfalls von den Computerorgängen getrennt werden; - Es sollten spezifische Kontrollen eingeführt werden, um die Vertraulichkeit und Integrität von Daten zu gewährleisten, die über öffentliche oder drahtlose Netzwerke übertrage	opensearch-in-vpc-only	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass sich Amazon OpenSearch Service-Domains innerhalb einer Amazon Virtual Private Cloud (Amazon VPC) befinden. Eine Amazon OpenSearch Service-Domain innerhalb einer Amazon VPC ermöglicht die sichere Kommunikation zwischen Amazon OpenSearch Service und anderen Services innerhalb der Amazon VPC, ohne dass ein Internet-Gateway, ein NAT-Gerät oder eine VPN-Verbindung erforderlich ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
	n werden, und um die vernetzten Systeme und Anwendung en zu schützen (einschließlich Netzwerkverschlüss elungsprotokollen bei Verbindungen zu nicht vertrauenswürdigen Systemen/Netzwerke n); - Es sollten eine angemesse ne Protokollierung und Überwachung durchgeführt werden, um die Aufzeichn ung und Erkennung von Aktionen zu ermöglichen, die die Informationssicher heit beeinträchtigen könnten oder für sie relevant sind; - Die Verwaltun gsaktivitäten sollten eng koordiniert werden, um einerseit s den Service für die Organisat ion zu optimieren und andererseits sicherzustellen, dass die Kontrollen in der gesamten Informati		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
	onsverarbeitungsin frastruktur einheitlich angewendet werden; - Die Systeme im Netzwerk sollten authentifiziert werden; und - Nicht vertrauen swürdige Systemver bindungen zum Netzwerk sollten eingeschränkt werden.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
3.1.2(c)	c) Es sollten Kontrollen eingeführt werden, um die Informationssicherheit in Netzwerken und den Schutz vernetzter Services vor unbefugtem Zugriff zu gewährleisten. Insbesondere sollten die folgenden Punkte in Erwägung gezogen werden: - Für die Verwaltung von Netzwerkgeräten sollten Zuständigkeiten und Verfahren festgelegt werden; - Die operative Verantwortung für Netzwerke sollte gegebenenfalls von den Computerorgängen getrennt werden; - Es sollten spezifische Kontrollen eingeführt werden, um die Vertraulichkeit und Integrität von Daten zu gewährleisten, die über öffentliche oder drahtlose Netzwerke übertrage	emr-master-no-public-ip	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon EMR-Cluster-Masterknoten nicht öffentlich zugänglich sind. Amazon-EMR-Cluster-Hauptknoten können vertrauliche Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
	n werden, und um die vernetzten Systeme und Anwendung en zu schützen (einschließlich Netzwerkverschlüss elungsprotokollen bei Verbindungen zu nicht vertrauenswürdigen Systemen/Netzwerke n); - Es sollten eine angemesse ne Protokollierung und Überwachung durchgeführt werden, um die Aufzeichn ung und Erkennung von Aktionen zu ermöglichen, die die Informationssicher heit beeinträchtigen könnten oder für sie relevant sind; - Die Verwaltun gsaktivitäten sollten eng koordiniert werden, um einerseit s den Service für die Organisat ion zu optimieren und andererseits sicherzustellen, dass die Kontrollen in der gesamten Informati		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
	onsverarbeitungsin frastruktur einheitlich angewendet werden; - Die Systeme im Netzwerk sollten authentifiziert werden; und - Nicht vertrauen swürdige Systemver bindungen zum Netzwerk sollten eingeschränkt werden.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
3.1.2(c)	c) Es sollten Kontrolle n eingeführt werden, um die Informati onssicherheit in Netzwerken und den Schutz vernetzte r Services vor unbefugtem Zugriff zu gewährleisten. Insbesondere sollten die folgenden Punkte in Erwägung gezogen werden: - Für die Verwaltung von Netzwerkgeräten sollten Zuständig keiten und Verfahren festgelegt werden; - Die operative Verantwortung für Netzwerke sollte gegebenenfalls von den Computerv orgängen getrennt werden; - Es sollten spezifische Kontrolle n eingeführt werden, um die Vertraulichkeit und Integrität von Daten zu gewährlei sten, die über öffentlic he oder drahtlose Netzwerke übertrage	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) Security Groups können bei der Verwaltung des Netzwerkzugriffs helfen, indem sie eine statusbeh aftete Filterung von eingehendem und ausgehendem Netzwerkverkehr zu Ressourcen bereitste llen. AWS Wenn Sie eingehenden (oder entfernten) Datenverk ehr von 0.0.0.0/0 bis Port 22 auf Ihren Ressourcen nicht zulassen, können Sie den Remote-Zugriff einschränken.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
	n werden, und um die vernetzten Systeme und Anwendung en zu schützen (einschließlich Netzwerkverschlüss elungsprotokollen bei Verbindungen zu nicht vertrauenswürdigen Systemen/Netzwerke n); - Es sollten eine angemesse ne Protokollierung und Überwachung durchgeführt werden, um die Aufzeichn ung und Erkennung von Aktionen zu ermöglichen, die die Informationssicher heit beeinträchtigen könnten oder für sie relevant sind; - Die Verwaltun gsaktivitäten sollten eng koordiniert werden, um einerseit s den Service für die Organisat ion zu optimieren und andererseits sicherzustellen, dass die Kontrollen in der gesamten Informati		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
	onsverarbeitungsin frastruktur einheitlich angewendet werden; - Die Systeme im Netzwerk sollten authentifiziert werden; und - Nicht vertrauen swürdige Systemver bindungen zum Netzwerk sollten eingeschränkt werden.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
3.1.2(c)	c) Es sollten Kontrollen eingeführt werden, um die Informationssicherheit in Netzwerken und den Schutz vernetzter Services vor unbefugtem Zugriff zu gewährleisten. Insbesondere sollten die folgenden Punkte in Erwägung gezogen werden: - Für die Verwaltung von Netzwerkgeräten sollten Zuständigkeiten und Verfahren festgelegt werden; - Die operative Verantwortung für Netzwerke sollte gegebenenfalls von den Computerorgängen getrennt werden; - Es sollten spezifische Kontrollen eingeführt werden, um die Vertraulichkeit und Integrität von Daten zu gewährleisten, die über öffentliche oder drahtlose Netzwerke übertrage	ec-2 instances-in-vpc	Stellen Sie Amazon Elastic Compute Cloud (Amazon EC2) -Instances innerhalb einer Amazon Virtual Private Cloud (Amazon VPC) bereit, um eine sichere Kommunikation zwischen einer Instance und anderen Services innerhalb der Amazon VPC zu ermöglichen, ohne dass ein Internet-Gateway, ein NAT-Gerät oder eine VPN-Verbindung erforderlich ist. Der gesamte Datenverkehr bleibt sicher in der AWS Cloud. Domains, die sich innerhalb einer VPC befinden, verfügen aufgrund ihrer logischen Isolierung im Vergleich zu Domains mit öffentlichen Endpunkten über eine zusätzliche Sicherheitsebene. Weisen Sie EC2

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
	n werden, und um die vernetzten Systeme und Anwendung en zu schützen (einschließlich Netzwerkverschlüss elungsprotokollen bei Verbindungen zu nicht vertrauenswürdigen Systemen/Netzwerke n); - Es sollten eine angemesse ne Protokollierung und Überwachung durchgeführt werden, um die Aufzeichn ung und Erkennung von Aktionen zu ermöglichen, die die Informationssicher heit beeinträchtigen könnten oder für sie relevant sind; - Die Verwaltun gsaktivitäten sollten eng koordiniert werden, um einerseit s den Service für die Organisat ion zu optimieren und andererseits sicherzustellen, dass die Kontrollen in der gesamten Informati		Amazon-Instances einer Amazon-VPC zu, um den Zugriff ordnungsgemäß zu verwalten.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
	onsverarbeitungsin frastruktur einheitlich angewendet werden; - Die Systeme im Netzwerk sollten authentifiziert werden; und - Nicht vertrauen swürdige Systemver bindungen zum Netzwerk sollten eingeschränkt werden.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
3.1.2(c)	c) Es sollten Kontrollen eingeführt werden, um die Informationssicherheit in Netzwerken und den Schutz vernetzter Services vor unbefugtem Zugriff zu gewährleisten. Insbesondere sollten die folgenden Punkte in Erwägung gezogen werden: - Für die Verwaltung von Netzwerkgeräten sollten Zuständigkeiten und Verfahren festgelegt werden; - Die operative Verantwortung für Netzwerke sollte gegebenenfalls von den Computerorgängen getrennt werden; - Es sollten spezifische Kontrollen eingeführt werden, um die Vertraulichkeit und Integrität von Daten zu gewährleisten, die über öffentliche oder drahtlose Netzwerke übertrage	internet-gateway-authorized-vpc-nur	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Internet-Gateways nur mit autorisierter Amazon Virtual Private Cloud (Amazon VPC) verbunden sind. Internet-Gateways ermöglichen den bidirektionalen Internetzugang zur und von der Amazon VPC, was möglicherweise zu einem unbefugten Zugriff auf Amazon-VPC-Ressourcen führen kann.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
	n werden, und um die vernetzten Systeme und Anwendung en zu schützen (einschließlich Netzwerkverschlüss elungsprotokollen bei Verbindungen zu nicht vertrauenswürdigen Systemen/Netzwerke n); - Es sollten eine angemesse ne Protokollierung und Überwachung durchgeführt werden, um die Aufzeichn ung und Erkennung von Aktionen zu ermöglichen, die die Informationssicher heit beeinträchtigen könnten oder für sie relevant sind; - Die Verwaltun gsaktivitäten sollten eng koordiniert werden, um einerseit s den Service für die Organisat ion zu optimieren und andererseits sicherzustellen, dass die Kontrollen in der gesamten Informati		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
	onsverarbeitungsin frastruktur einheitlich angewendet werden; - Die Systeme im Netzwerk sollten authentifiziert werden; und - Nicht vertrauen swürdige Systemver bindungen zum Netzwerk sollten eingeschränkt werden.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
3.1.2(c)	c) Es sollten Kontrollen eingeführt werden, um die Informationssicherheit in Netzwerken und den Schutz vernetzter Services vor unbefugtem Zugriff zu gewährleisten. Insbesondere sollten die folgenden Punkte in Erwägung gezogen werden: - Für die Verwaltung von Netzwerkgeräten sollten Zuständigkeiten und Verfahren festgelegt werden; - Die operative Verantwortung für Netzwerke sollte gegebenenfalls von den Computerorgängen getrennt werden; - Es sollten spezifische Kontrollen eingeführt werden, um die Vertraulichkeit und Integrität von Daten zu gewährleisten, die über öffentliche oder drahtlose Netzwerke übertrage	lambda-function-public-access-verboten	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass AWS Lambda-Funktionen nicht öffentlich zugänglich sind. Der öffentliche Zugriff kann möglicherweise die Verfügbarkeit von Ressourcen beeinträchtigen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
	n werden, und um die vernetzten Systeme und Anwendung en zu schützen (einschließlich Netzwerkverschlüss elungsprotokollen bei Verbindungen zu nicht vertrauenswürdigen Systemen/Netzwerke n); - Es sollten eine angemesse ne Protokollierung und Überwachung durchgeführt werden, um die Aufzeichn ung und Erkennung von Aktionen zu ermöglichen, die die Informationssicher heit beeinträchtigen könnten oder für sie relevant sind; - Die Verwaltun gsaktivitäten sollten eng koordiniert werden, um einerseit s den Service für die Organisat ion zu optimieren und andererseits sicherzustellen, dass die Kontrollen in der gesamten Informati		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
	onsverarbeitungsin frastruktur einheitlich angewendet werden; - Die Systeme im Netzwerk sollten authentifiziert werden; und - Nicht vertrauen swürdige Systemver bindungen zum Netzwerk sollten eingeschränkt werden.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
3.1.2(c)	c) Es sollten Kontrollen eingeführt werden, um die Informationssicherheit in Netzwerken und den Schutz vernetzter Services vor unbefugtem Zugriff zu gewährleisten. Insbesondere sollten die folgenden Punkte in Erwägung gezogen werden: - Für die Verwaltung von Netzwerkgeräten sollten Zuständigkeiten und Verfahren festgelegt werden; - Die operative Verantwortung für Netzwerke sollte gegebenenfalls von den Computerorgängen getrennt werden; - Es sollten spezifische Kontrollen eingeführt werden, um die Vertraulichkeit und Integrität von Daten zu gewährleisten, die über öffentliche oder drahtlose Netzwerke übertrage	lambda-inside-vpc	Stellen Sie AWS Lambda-Funktionen in einer Amazon Virtual Private Cloud (Amazon VPC) bereit, um eine sichere Kommunikation zwischen einer Funktion und anderen Diensten innerhalb der Amazon VPC zu gewährleisten. Bei dieser Konfiguration sind kein Internet-Gateway, kein NAT-Gerät und keine VPN-Verbindung erforderlich. Der gesamte Datenverkehr bleibt sicher in der Cloud. AWS Domains, die sich innerhalb einer VPC befinden, verfügen aufgrund ihrer logischen Isolierung im Vergleich zu Domains mit öffentlichen Endpunkten über eine zusätzliche Sicherheitsebene. Um den Zugriff ordnungsgemäß zu verwalten,

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
	n werden, und um die vernetzten Systeme und Anwendung en zu schützen (einschließlich Netzwerkverschlüss elungsprotokollen bei Verbindungen zu nicht vertrauenswürdigen Systemen/Netzwerke n); - Es sollten eine angemesse ne Protokollierung und Überwachung durchgeführt werden, um die Aufzeichn ung und Erkennung von Aktionen zu ermöglichen, die die Informationssicher heit beeinträchtigen könnten oder für sie relevant sind; - Die Verwaltun gsaktivitäten sollten eng koordiniert werden, um einerseit s den Service für die Organisat ion zu optimieren und andererseits sicherzustellen, dass die Kontrollen in der gesamten Informati		sollten AWS Lambda-Funktionen einer VPC zugewiesen werden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
	onsverarbeitungsin frastruktur einheitlich angewendet werden; - Die Systeme im Netzwerk sollten authentifiziert werden; und - Nicht vertrauen swürdige Systemver bindungen zum Netzwerk sollten eingeschränkt werden.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
3.1.2(c)	c) Es sollten Kontrollen eingeführt werden, um die Informationssicherheit in Netzwerken und den Schutz vernetzter Services vor unbefugtem Zugriff zu gewährleisten. Insbesondere sollten die folgenden Punkte in Erwägung gezogen werden: - Für die Verwaltung von Netzwerkgeräten sollten Zuständigkeiten und Verfahren festgelegt werden; - Die operative Verantwortung für Netzwerke sollte gegebenenfalls von den Computerorgängen getrennt werden; - Es sollten spezifische Kontrollen eingeführt werden, um die Vertraulichkeit und Integrität von Daten zu gewährleisten, die über öffentliche oder drahtlose Netzwerke übertrage	rds-instance-public-access-überprüfen	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Relational Database Service (Amazon RDS) -Instances nicht öffentlich sind. Amazon-RDS-Datenbank-Instances können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
	n werden, und um die vernetzten Systeme und Anwendung en zu schützen (einschließlich Netzwerkverschlüss elungsprotokollen bei Verbindungen zu nicht vertrauenswürdigen Systemen/Netzwerke n); - Es sollten eine angemesse ne Protokollierung und Überwachung durchgeführt werden, um die Aufzeichn ung und Erkennung von Aktionen zu ermöglichen, die die Informationssicher heit beeinträchtigen könnten oder für sie relevant sind; - Die Verwaltun gsaktivitäten sollten eng koordiniert werden, um einerseit s den Service für die Organisat ion zu optimieren und andererseits sicherzustellen, dass die Kontrollen in der gesamten Informati		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
	onsverarbeitungsin frastruktur einheitlich angewendet werden; - Die Systeme im Netzwerk sollten authentifiziert werden; und - Nicht vertrauen swürdige Systemver bindungen zum Netzwerk sollten eingeschränkt werden.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
3.1.2(c)	c) Es sollten Kontrollen eingeführt werden, um die Informationssicherheit in Netzwerken und den Schutz vernetzter Services vor unbefugtem Zugriff zu gewährleisten. Insbesondere sollten die folgenden Punkte in Erwägung gezogen werden: - Für die Verwaltung von Netzwerkgeräten sollten Zuständigkeiten und Verfahren festgelegt werden; - Die operative Verantwortung für Netzwerke sollte gegebenenfalls von den Computerorgängen getrennt werden; - Es sollten spezifische Kontrollen eingeführt werden, um die Vertraulichkeit und Integrität von Daten zu gewährleisten, die über öffentliche oder drahtlose Netzwerke übertrage	rds-snapshots-public-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Relational Database Service (Amazon RDS) -Instances nicht öffentlich sind. Amazon-RDS-Datenbank-Instances können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
	n werden, und um die vernetzten Systeme und Anwendung en zu schützen (einschließlich Netzwerkverschlüss elungsprotokollen bei Verbindungen zu nicht vertrauenswürdigen Systemen/Netzwerke n); - Es sollten eine angemesse ne Protokollierung und Überwachung durchgeführt werden, um die Aufzeichn ung und Erkennung von Aktionen zu ermöglichen, die die Informationssicher heit beeinträchtigen könnten oder für sie relevant sind; - Die Verwaltun gsaktivitäten sollten eng koordiniert werden, um einerseit s den Service für die Organisat ion zu optimieren und andererseits sicherzustellen, dass die Kontrollen in der gesamten Informati		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
	onsverarbeitungsin frastruktur einheitlich angewendet werden; - Die Systeme im Netzwerk sollten authentifiziert werden; und - Nicht vertrauen swürdige Systemver bindungen zum Netzwerk sollten eingeschränkt werden.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
3.1.2(c)	c) Es sollten Kontrollen eingeführt werden, um die Informationssicherheit in Netzwerken und den Schutz vernetzter Services vor unbefugtem Zugriff zu gewährleisten. Insbesondere sollten die folgenden Punkte in Erwägung gezogen werden: - Für die Verwaltung von Netzwerkgeräten sollten Zuständigkeiten und Verfahren festgelegt werden; - Die operative Verantwortung für Netzwerke sollte gegebenenfalls von den Computerorgängen getrennt werden; - Es sollten spezifische Kontrollen eingeführt werden, um die Vertraulichkeit und Integrität von Daten zu gewährleisten, die über öffentliche oder drahtlose Netzwerke übertrage	redshift-cluster-public-access-überprüfen	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Redshift Redshift-Cluster nicht öffentlich sind. Amazon-Redshift-Cluster können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
	n werden, und um die vernetzten Systeme und Anwendung en zu schützen (einschließlich Netzwerkverschlüss elungsprotokollen bei Verbindungen zu nicht vertrauenswürdigen Systemen/Netzwerke n); - Es sollten eine angemesse ne Protokollierung und Überwachung durchgeführt werden, um die Aufzeichn ung und Erkennung von Aktionen zu ermöglichen, die die Informationssicher heit beeinträchtigen könnten oder für sie relevant sind; - Die Verwaltun gsaktivitäten sollten eng koordiniert werden, um einerseit s den Service für die Organisat ion zu optimieren und andererseits sicherzustellen, dass die Kontrollen in der gesamten Informati		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
	onsverarbeitungsin frastruktur einheitlich angewendet werden; - Die Systeme im Netzwerk sollten authentifiziert werden; und - Nicht vertrauen swürdige Systemver bindungen zum Netzwerk sollten eingeschränkt werden.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
3.1.2(c)	c) Es sollten Kontrollen eingeführt werden, um die Informationssicherheit in Netzwerken und den Schutz vernetzter Services vor unbefugtem Zugriff zu gewährleisten. Insbesondere sollten die folgenden Punkte in Erwägung gezogen werden: - Für die Verwaltung von Netzwerkgeräten sollten Zuständigkeiten und Verfahren festgelegt werden; - Die operative Verantwortung für Netzwerke sollte gegebenenfalls von den Computerorgängen getrennt werden; - Es sollten spezifische Kontrollen eingeführt werden, um die Vertraulichkeit und Integrität von Daten zu gewährleisten, die über öffentliche oder drahtlose Netzwerke übertrage	restricted-common-ports	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass gemeinsame Ports für Amazon Elastic Compute Cloud (Amazon EC2) -Sicherheitsgruppen eingeschränkt sind. Wenn der Zugriff auf Ports nicht auf vertrauenswürdige Quellen beschränkt wird, kann dies zu Angriffen auf die Verfügbarkeit, Integrität und Vertraulichkeit von Systemen führen. Mit dieser Regel können Sie optional die Parameter blockedPort1–blockedPort5 festlegen (Standardkonfigurationen: 20, 21, 3389, 3306, 4333). Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
	n werden, und um die vernetzten Systeme und Anwendung en zu schützen (einschließlich Netzwerkverschlüss elungsprotokollen bei Verbindungen zu nicht vertrauenswürdigen Systemen/Netzwerke n); - Es sollten eine angemesse ne Protokollierung und Überwachung durchgeführt werden, um die Aufzeichn ung und Erkennung von Aktionen zu ermöglichen, die die Informationssicher heit beeinträchtigen könnten oder für sie relevant sind; - Die Verwaltun gsaktivitäten sollten eng koordiniert werden, um einerseit s den Service für die Organisat ion zu optimieren und andererseits sicherzustellen, dass die Kontrollen in der gesamten Informati		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
	onsverarbeitungsin frastruktur einheitlich angewendet werden; - Die Systeme im Netzwerk sollten authentifiziert werden; und - Nicht vertrauen swürdige Systemver bindungen zum Netzwerk sollten eingeschränkt werden.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
3.1.2(c)	c) Es sollten Kontrollen eingeführt werden, um die Informationssicherheit in Netzwerken und den Schutz vernetzter Services vor unbefugtem Zugriff zu gewährleisten. Insbesondere sollten die folgenden Punkte in Erwägung gezogen werden: - Für die Verwaltung von Netzwerkgeräten sollten Zuständigkeiten und Verfahren festgelegt werden; - Die operative Verantwortung für Netzwerke sollte gegebenenfalls von den Computerorgängen getrennt werden; - Es sollten spezifische Kontrollen eingeführt werden, um die Vertraulichkeit und Integrität von Daten zu gewährleisten, die über öffentliche oder drahtlose Netzwerke übertrage	s-3 bucket-public-read-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie nur autorisierten Benutzern, Prozessen und Geräten Zugriff auf Amazon Simple Storage Service (Amazon S3) - Buckets gewähren. Die Verwaltung des Zugriffs sollte mit der Klassifizierung der Daten übereinstimmen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
	n werden, und um die vernetzten Systeme und Anwendung en zu schützen (einschließlich Netzwerkverschlüss elungsprotokollen bei Verbindungen zu nicht vertrauenswürdigen Systemen/Netzwerke n); - Es sollten eine angemesse ne Protokollierung und Überwachung durchgeführt werden, um die Aufzeichn ung und Erkennung von Aktionen zu ermöglichen, die die Informationssicher heit beeinträchtigen könnten oder für sie relevant sind; - Die Verwaltun gsaktivitäten sollten eng koordiniert werden, um einerseit s den Service für die Organisat ion zu optimieren und andererseits sicherzustellen, dass die Kontrollen in der gesamten Informati		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
	onsverarbeitungsin frastruktur einheitlich angewendet werden; - Die Systeme im Netzwerk sollten authentifiziert werden; und - Nicht vertrauen swürdige Systemver bindungen zum Netzwerk sollten eingeschränkt werden.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
3.1.2(c)	c) Es sollten Kontrollen eingeführt werden, um die Informationssicherheit in Netzwerken und den Schutz vernetzter Services vor unbefugtem Zugriff zu gewährleisten. Insbesondere sollten die folgenden Punkte in Erwägung gezogen werden: - Für die Verwaltung von Netzwerkgeräten sollten Zuständigkeiten und Verfahren festgelegt werden; - Die operative Verantwortung für Netzwerke sollte gegebenenfalls von den Computerorgängen getrennt werden; - Es sollten spezifische Kontrollen eingeführt werden, um die Vertraulichkeit und Integrität von Daten zu gewährleisten, die über öffentliche oder drahtlose Netzwerke übertrage	s3- bucket-public-write-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie nur autorisierten Benutzern, Prozessen und Geräten Zugriff auf Amazon Simple Storage Service (Amazon S3) - Buckets gewähren. Die Verwaltung des Zugriffs sollte mit der Klassifizierung der Daten übereinstimmen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
	n werden, und um die vernetzten Systeme und Anwendung en zu schützen (einschließlich Netzwerkverschlüss elungsprotokollen bei Verbindungen zu nicht vertrauenswürdigen Systemen/Netzwerke n); - Es sollten eine angemesse ne Protokollierung und Überwachung durchgeführt werden, um die Aufzeichn ung und Erkennung von Aktionen zu ermöglichen, die die Informationssicher heit beeinträchtigen könnten oder für sie relevant sind; - Die Verwaltun gsaktivitäten sollten eng koordiniert werden, um einerseit s den Service für die Organisat ion zu optimieren und andererseits sicherzustellen, dass die Kontrollen in der gesamten Informati		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
	onsverarbeitungsin frastruktur einheitlich angewendet werden; - Die Systeme im Netzwerk sollten authentifiziert werden; und - Nicht vertrauen swürdige Systemver bindungen zum Netzwerk sollten eingeschränkt werden.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
3.1.2(c)	c) Es sollten Kontrollen eingeführt werden, um die Informationssicherheit in Netzwerken und den Schutz vernetzter Services vor unbefugtem Zugriff zu gewährleisten. Insbesondere sollten die folgenden Punkte in Erwägung gezogen werden: - Für die Verwaltung von Netzwerkgeräten sollten Zuständigkeiten und Verfahren festgelegt werden; - Die operative Verantwortung für Netzwerke sollte gegebenenfalls von den Computerorgängen getrennt werden; - Es sollten spezifische Kontrollen eingeführt werden, um die Vertraulichkeit und Integrität von Daten zu gewährleisten, die über öffentliche oder drahtlose Netzwerke übertrage	sagemaker-notebook-no-direct-Internetzugang	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass SageMaker Amazon-Notebooks keinen direkten Internetzugang zulassen. Indem Sie direkten Internetzugang blockieren, vermeiden Sie, dass unbefugte Benutzer auf sensible Daten zugreifen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
	n werden, und um die vernetzten Systeme und Anwendung en zu schützen (einschließlich Netzwerkverschlüss elungsprotokollen bei Verbindungen zu nicht vertrauenswürdigen Systemen/Netzwerke n); - Es sollten eine angemesse ne Protokollierung und Überwachung durchgeführt werden, um die Aufzeichn ung und Erkennung von Aktionen zu ermöglichen, die die Informationssicher heit beeinträchtigen könnten oder für sie relevant sind; - Die Verwaltun gsaktivitäten sollten eng koordiniert werden, um einerseit s den Service für die Organisat ion zu optimieren und andererseits sicherzustellen, dass die Kontrollen in der gesamten Informati		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
	onsverarbeitungsin frastruktur einheitlich angewendet werden; - Die Systeme im Netzwerk sollten authentifiziert werden; und - Nicht vertrauen swürdige Systemver bindungen zum Netzwerk sollten eingeschränkt werden.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
3.1.2(c)	c) Es sollten Kontrolle n eingeführt werden, um die Informati onssicherheit in Netzwerken und den Schutz vernetzte r Services vor unbefugtem Zugriff zu gewährleisten. Insbesondere sollten die folgenden Punkte in Erwägung gezogen werden: - Für die Verwaltung von Netzwerkgeräten sollten Zuständig keiten und Verfahren festgelegt werden; - Die operative Verantwortung für Netzwerke sollte gegebenenfalls von den Computerv orgängen getrennt werden; - Es sollten spezifische Kontrolle n eingeführt werden, um die Vertraulichkeit und Integrität von Daten zu gewährlei sten, die über öffentlic he oder drahtlose Netzwerke übertrage	vpc-default-security-group-geschlossen	Sicherheitsgruppen von Amazon Elastic Compute Cloud (Amazon EC2) können bei der Verwaltung des Netzwerkzugriffs helfen, indem sie eine statusbehaftete Filterung des ein- und ausgehenden Netzwerkverkehrs zu Ressourcen bereitstellen. AWS Die Beschränk ung des gesamten Datenverkehrs auf die Standardsicherheit sgruppe hilft dabei, den Fernzugriff auf Ihre Ressourcen einzuschränken. AWS

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
	n werden, und um die vernetzten Systeme und Anwendung en zu schützen (einschließlich Netzwerkverschlüss elungsprotokollen bei Verbindungen zu nicht vertrauenswürdigen Systemen/Netzwerke n); - Es sollten eine angemesse ne Protokollierung und Überwachung durchgeführt werden, um die Aufzeichn ung und Erkennung von Aktionen zu ermöglichen, die die Informationssicher heit beeinträchtigen könnten oder für sie relevant sind; - Die Verwaltun gsaktivitäten sollten eng koordiniert werden, um einerseit s den Service für die Organisat ion zu optimieren und andererseits sicherzustellen, dass die Kontrollen in der gesamten Informati		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
	onsverarbeitungsin frastruktur einheitlich angewendet werden; - Die Systeme im Netzwerk sollten authentifiziert werden; und - Nicht vertrauen swürdige Systemver bindungen zum Netzwerk sollten eingeschränkt werden.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
3.1.2(c)	c) Es sollten Kontrollen eingeführt werden, um die Informationssicherheit in Netzwerken und den Schutz vernetzter Services vor unbefugtem Zugriff zu gewährleisten. Insbesondere sollten die folgenden Punkte in Erwägung gezogen werden: - Für die Verwaltung von Netzwerkgeräten sollten Zuständigkeiten und Verfahren festgelegt werden; - Die operative Verantwortung für Netzwerke sollte gegebenenfalls von den Computerorgängen getrennt werden; - Es sollten spezifische Kontrollen eingeführt werden, um die Vertraulichkeit und Integrität von Daten zu gewährleisten, die über öffentliche oder drahtlose Netzwerke übertrage	vpc-sg-open-only-to-authorized-ports	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass gemeinsame Ports für Amazon Elastic Compute Cloud (Amazon EC2) -Sicherheitsgruppen eingeschränkt sind. Wenn der Zugriff auf Ports nicht auf vertrauenswürdige Quellen beschränkt wird, kann dies zu Angriffen auf die Verfügbarkeit, Integrität und Vertraulichkeit von Systemen führen. Durch die Beschränkung des Zugriffs auf Ressourcen innerhalb einer Sicherheitsgruppe aus dem Internet (0.0.0.0/0) kann der Fernzugriff auf interne Systeme gesteuert werden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
	n werden, und um die vernetzten Systeme und Anwendung en zu schützen (einschließlich Netzwerkverschlüss elungsprotokollen bei Verbindungen zu nicht vertrauenswürdigen Systemen/Netzwerke n); - Es sollten eine angemesse ne Protokollierung und Überwachung durchgeführt werden, um die Aufzeichn ung und Erkennung von Aktionen zu ermöglichen, die die Informationssicher heit beeinträchtigen könnten oder für sie relevant sind; - Die Verwaltun gsaktivitäten sollten eng koordiniert werden, um einerseit s den Service für die Organisat ion zu optimieren und andererseits sicherzustellen, dass die Kontrollen in der gesamten Informati		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
	onsverarbeitungsin frastruktur einheitlich angewendet werden; - Die Systeme im Netzwerk sollten authentifiziert werden; und - Nicht vertrauen swürdige Systemver bindungen zum Netzwerk sollten eingeschränkt werden.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
3.1.2(c)	c) Es sollten Kontrollen eingeführt werden, um die Informationssicherheit in Netzwerken und den Schutz vernetzter Services vor unbefugtem Zugriff zu gewährleisten. Insbesondere sollten die folgenden Punkte in Erwägung gezogen werden: - Für die Verwaltung von Netzwerkgeräten sollten Zuständigkeiten und Verfahren festgelegt werden; - Die operative Verantwortung für Netzwerke sollte gegebenenfalls von den Computerorgängen getrennt werden; - Es sollten spezifische Kontrollen eingeführt werden, um die Vertraulichkeit und Integrität von Daten zu gewährleisten, die über öffentliche oder drahtlose Netzwerke übertrage	no-unrestricted-route-to-igw	Stellen Sie sicher, dass EC2 Amazon-Routentabellen keine uneingeschränkten Routen zu einem Internet-Gateway enthalten. Durch das Entfernen oder Beschränken des Internetzugangs für Workloads innerhalb von Amazon VPCs können unbeabsichtigte Zugriffe in Ihrer Umgebung reduziert werden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
	n werden, und um die vernetzten Systeme und Anwendung en zu schützen (einschließlich Netzwerkverschlüss elungsprotokollen bei Verbindungen zu nicht vertrauenswürdigen Systemen/Netzwerke n); - Es sollten eine angemesse ne Protokollierung und Überwachung durchgeführt werden, um die Aufzeichn ung und Erkennung von Aktionen zu ermöglichen, die die Informationssicher heit beeinträchtigen könnten oder für sie relevant sind; - Die Verwaltun gsaktivitäten sollten eng koordiniert werden, um einerseit s den Service für die Organisat ion zu optimieren und andererseits sicherzustellen, dass die Kontrollen in der gesamten Informati		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
	onsverarbeitungsin frastruktur einheitlich angewendet werden; - Die Systeme im Netzwerk sollten authentifiziert werden; und - Nicht vertrauen swürdige Systemver bindungen zum Netzwerk sollten eingeschränkt werden.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
3.1.2(c)	c) Es sollten Kontrollen eingeführt werden, um die Informationssicherheit in Netzwerken und den Schutz vernetzter Services vor unbefugtem Zugriff zu gewährleisten. Insbesondere sollten die folgenden Punkte in Erwägung gezogen werden: - Für die Verwaltung von Netzwerkgeräten sollten Zuständigkeiten und Verfahren festgelegt werden; - Die operative Verantwortung für Netzwerke sollte gegebenenfalls von den Computerorgängen getrennt werden; - Es sollten spezifische Kontrollen eingeführt werden, um die Vertraulichkeit und Integrität von Daten zu gewährleisten, die über öffentliche oder drahtlose Netzwerke übertrage	subnet-auto-assign-public-ip-deaktiviert	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon Virtual Private Cloud (VPC) -Subnetzen nicht automatisch eine öffentliche IP-Adresse zugewiesen wird. Amazon Elastic Compute Cloud (EC2) -Instances, die in Subnetzen gestartet werden, in denen dieses Attribut aktiviert ist, haben ihrer primären Netzwerkschnittstelle eine öffentliche IP-Adresse zugewiesen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
	n werden, und um die vernetzten Systeme und Anwendung en zu schützen (einschließlich Netzwerkverschlüss elungsprotokollen bei Verbindungen zu nicht vertrauenswürdigen Systemen/Netzwerke n); - Es sollten eine angemesse ne Protokollierung und Überwachung durchgeführt werden, um die Aufzeichn ung und Erkennung von Aktionen zu ermöglichen, die die Informationssicher heit beeinträchtigen könnten oder für sie relevant sind; - Die Verwaltun gsaktivitäten sollten eng koordiniert werden, um einerseit s den Service für die Organisat ion zu optimieren und andererseits sicherzustellen, dass die Kontrollen in der gesamten Informati		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
	onsverarbeitungsin frastruktur einheitlich angewendet werden; - Die Systeme im Netzwerk sollten authentifiziert werden; und - Nicht vertrauen swürdige Systemver bindungen zum Netzwerk sollten eingeschränkt werden.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
3.1.2(c)	c) Es sollten Kontrolle n eingeführt werden, um die Informati onssicherheit in Netzwerken und den Schutz vernetzte r Services vor unbefugtem Zugriff zu gewährleisten. Insbesondere sollten die folgenden Punkte in Erwägung gezogen werden: - Für die Verwaltung von Netzwerkgeräten sollten Zuständig keiten und Verfahren festgelegt werden; - Die operative Verantwortung für Netzwerke sollte gegebenenfalls von den Computerv orgängen getrennt werden; - Es sollten spezifische Kontrolle n eingeführt werden, um die Vertraulichkeit und Integrität von Daten zu gewährlei sten, die über öffentlic he oder drahtlose Netzwerke übertrage	autoscaling-launch -config-public-ip- deaktiviert	Wenn Sie Ihre Netzwerkschnittstellen mit einer öffentlichen IP-Adresse konfiguri eren, sind die diesen Netzwerkschnittste llen zugehörigen Ressourcen über das Internet erreichba r. EC2 Ressourcen sollten nicht öffentlic h zugänglich sein, da dies einen unbeabsic htigten Zugriff auf Ihre Anwendungen oder Server ermöglichen kann.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
	n werden, und um die vernetzten Systeme und Anwendung en zu schützen (einschließlich Netzwerkverschlüss elungsprotokollen bei Verbindungen zu nicht vertrauenswürdigen Systemen/Netzwerke n); - Es sollten eine angemesse ne Protokollierung und Überwachung durchgeführt werden, um die Aufzeichn ung und Erkennung von Aktionen zu ermöglichen, die die Informationssicher heit beeinträchtigen könnten oder für sie relevant sind; - Die Verwaltun gsaktivitäten sollten eng koordiniert werden, um einerseit s den Service für die Organisat ion zu optimieren und andererseits sicherzustellen, dass die Kontrollen in der gesamten Informati		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
	onsverarbeitungsin frastruktur einheitlich angewendet werden; - Die Systeme im Netzwerk sollten authentifiziert werden; und - Nicht vertrauen swürdige Systemver bindungen zum Netzwerk sollten eingeschränkt werden.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
3.1.2(c)	c) Es sollten Kontrollen eingeführt werden, um die Informationssicherheit in Netzwerken und den Schutz vernetzter Services vor unbefugtem Zugriff zu gewährleisten. Insbesondere sollten die folgenden Punkte in Erwägung gezogen werden: - Für die Verwaltung von Netzwerkgeräten sollten Zuständigkeiten und Verfahren festgelegt werden; - Die operative Verantwortung für Netzwerke sollte gegebenenfalls von den Computerorgängen getrennt werden; - Es sollten spezifische Kontrollen eingeführt werden, um die Vertraulichkeit und Integrität von Daten zu gewährleisten, die über öffentliche oder drahtlose Netzwerke übertrage	redshift-enhanced-vpc-routing-aktiviert	Mit Enhanced-VPC-Routing wird erzwungen, dass der gesamte COPY- und UNLOAD-Datenverkehr zwischen Ihrem Cluster und Datenrepositorys über Ihre Amazon VPC erfolgt. Anschließend können Sie VPC-Features wie Sicherheitsgruppen und Netzwerkzugriffskontrolllisten verwenden, um den Netzwerkverkehr zu schützen. Sie können auch VPC-Flow-Logs verwenden, um den Netzwerkverkehr zu überwachen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
	n werden, und um die vernetzten Systeme und Anwendung en zu schützen (einschließlich Netzwerkverschlüss elungsprotokollen bei Verbindungen zu nicht vertrauenswürdigen Systemen/Netzwerke n); - Es sollten eine angemesse ne Protokollierung und Überwachung durchgeführt werden, um die Aufzeichn ung und Erkennung von Aktionen zu ermöglichen, die die Informationssicher heit beeinträchtigen könnten oder für sie relevant sind; - Die Verwaltun gsaktivitäten sollten eng koordiniert werden, um einerseit s den Service für die Organisat ion zu optimieren und andererseits sicherzustellen, dass die Kontrollen in der gesamten Informati		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
	onsverarbeitungsin frastruktur einheitlich angewendet werden; - Die Systeme im Netzwerk sollten authentifiziert werden; und - Nicht vertrauen swürdige Systemver bindungen zum Netzwerk sollten eingeschränkt werden.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
3.1.2(c)	c) Es sollten Kontrolle n eingeführt werden, um die Informati onssicherheit in Netzwerken und den Schutz vernetzte r Services vor unbefugtem Zugriff zu gewährleisten. Insbesondere sollten die folgenden Punkte in Erwägung gezogen werden: - Für die Verwaltung von Netzwerkgeräten sollten Zuständig keiten und Verfahren festgelegt werden; - Die operative Verantwortung für Netzwerke sollte gegebenenfalls von den Computerv orgängen getrennt werden; - Es sollten spezifische Kontrolle n eingeführt werden, um die Vertraulichkeit und Integrität von Daten zu gewährlei sten, die über öffentlic he oder drahtlose Netzwerke übertrage	api-gw-ssl-enabled	Stellen Sie sicher, dass die REST-API-Stufen von Amazon API Gateway mit SSL-Zertifikaten konfiguri ert sind, damit Backend-Systeme überprüfen können, ob Anforderungen von API Gateway stammen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
	n werden, und um die vernetzten Systeme und Anwendung en zu schützen (einschließlich Netzwerkverschlüss elungsprotokollen bei Verbindungen zu nicht vertrauenswürdigen Systemen/Netzwerke n); - Es sollten eine angemesse ne Protokollierung und Überwachung durchgeführt werden, um die Aufzeichn ung und Erkennung von Aktionen zu ermöglichen, die die Informationssicher heit beeinträchtigen könnten oder für sie relevant sind; - Die Verwaltun gsaktivitäten sollten eng koordiniert werden, um einerseit s den Service für die Organisat ion zu optimieren und andererseits sicherzustellen, dass die Kontrollen in der gesamten Informati		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
	onsverarbeitungsin frastruktur einheitlich angewendet werden; - Die Systeme im Netzwerk sollten authentifiziert werden; und - Nicht vertrauen swürdige Systemver bindungen zum Netzwerk sollten eingeschränkt werden.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
3.1.2(c)	c) Es sollten Kontrollen eingeführt werden, um die Informationssicherheit in Netzwerken und den Schutz vernetzter Services vor unbefugtem Zugriff zu gewährleisten. Insbesondere sollten die folgenden Punkte in Erwägung gezogen werden: - Für die Verwaltung von Netzwerkgeräten sollten Zuständigkeiten und Verfahren festgelegt werden; - Die operative Verantwortung für Netzwerke sollte gegebenenfalls von den Computerorgängen getrennt werden; - Es sollten spezifische Kontrollen eingeführt werden, um die Vertraulichkeit und Integrität von Daten zu gewährleisten, die über öffentliche oder drahtlose Netzwerke übertrage	elbv2- acm-certificate-required	Zum Schutz von eventuell vorhandenen sensiblen Daten sowie von Daten während der Übertragung muss die Verschlüsselung für Ihr Elastic Load Balancing aktiviert sein. Verwenden Sie AWS Certificate Manager, um öffentliche und private SSL/TLS-Zertifikate mit AWS Diensten und internen Ressourcen zu verwalten, bereitzustellen und bereitzustellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
	n werden, und um die vernetzten Systeme und Anwendung en zu schützen (einschließlich Netzwerkverschlüss elungsprotokollen bei Verbindungen zu nicht vertrauenswürdigen Systemen/Netzwerke n); - Es sollten eine angemesse ne Protokollierung und Überwachung durchgeführt werden, um die Aufzeichn ung und Erkennung von Aktionen zu ermöglichen, die die Informationssicher heit beeinträchtigen könnten oder für sie relevant sind; - Die Verwaltun gsaktivitäten sollten eng koordiniert werden, um einerseit s den Service für die Organisat ion zu optimieren und andererseits sicherzustellen, dass die Kontrollen in der gesamten Informati		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
	onsverarbeitungsin frastruktur einheitlich angewendet werden; - Die Systeme im Netzwerk sollten authentifiziert werden; und - Nicht vertrauen swürdige Systemver bindungen zum Netzwerk sollten eingeschränkt werden.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
3.1.2(c)	c) Es sollten Kontrollen eingeführt werden, um die Informationssicherheit in Netzwerken und den Schutz vernetzter Services vor unbefugtem Zugriff zu gewährleisten. Insbesondere sollten die folgenden Punkte in Erwägung gezogen werden: - Für die Verwaltung von Netzwerkgeräten sollten Zuständigkeiten und Verfahren festgelegt werden; - Die operative Verantwortung für Netzwerke sollte gegebenenfalls von den Computerorgängen getrennt werden; - Es sollten spezifische Kontrollen eingeführt werden, um die Vertraulichkeit und Integrität von Daten zu gewährleisten, die über öffentliche oder drahtlose Netzwerke übertrage	elasticsearch-logs-to-cloudwatch	Stellen Sie sicher, dass für Amazon OpenSearch Service-Domains Fehlerprotokolle aktiviert und zur Aufbewahrung und Beantwortung an Amazon CloudWatch Logs gestreamt werden. Domain-Fehlerprotokolle sind bei Sicherheits- und Zugriffsprüfungen sowie bei der Diagnose von Verfügbarkeitsproblemen nützlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
	n werden, und um die vernetzten Systeme und Anwendung en zu schützen (einschließlich Netzwerkverschlüss elungsprotokollen bei Verbindungen zu nicht vertrauenswürdigen Systemen/Netzwerke n); - Es sollten eine angemesse ne Protokollierung und Überwachung durchgeführt werden, um die Aufzeichn ung und Erkennung von Aktionen zu ermöglichen, die die Informationssicher heit beeinträchtigen könnten oder für sie relevant sind; - Die Verwaltun gsaktivitäten sollten eng koordiniert werden, um einerseit s den Service für die Organisat ion zu optimieren und andererseits sicherzustellen, dass die Kontrollen in der gesamten Informati		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
	onsverarbeitungsin frastruktur einheitlich angewendet werden; - Die Systeme im Netzwerk sollten authentifiziert werden; und - Nicht vertrauen swürdige Systemver bindungen zum Netzwerk sollten eingeschränkt werden.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
3.1.2(c)	c) Es sollten Kontrollen eingeführt werden, um die Informationssicherheit in Netzwerken und den Schutz vernetzter Services vor unbefugtem Zugriff zu gewährleisten. Insbesondere sollten die folgenden Punkte in Erwägung gezogen werden: - Für die Verwaltung von Netzwerkgeräten sollten Zuständigkeiten und Verfahren festgelegt werden; - Die operative Verantwortung für Netzwerke sollte gegebenenfalls von den Computerorgängen getrennt werden; - Es sollten spezifische Kontrollen eingeführt werden, um die Vertraulichkeit und Integrität von Daten zu gewährleisten, die über öffentliche oder drahtlose Netzwerke übertrage	opensearch-logs-to-cloudwatch	Stellen Sie sicher, dass für Amazon OpenSearch Service-Domains Fehlerprotokolle aktiviert und zur Aufbewahrung und Beantwortung an Amazon CloudWatch Logs gestreamt werden. OpenSearch Service-Fehlerprotokolle können bei Sicherheits- und Zugriffsprüfungen helfen und bei der Diagnose von Verfügbarkeitsproblemen helfen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
	n werden, und um die vernetzten Systeme und Anwendung en zu schützen (einschließlich Netzwerkverschlüss elungsprotokollen bei Verbindungen zu nicht vertrauenswürdigen Systemen/Netzwerke n); - Es sollten eine angemesse ne Protokollierung und Überwachung durchgeführt werden, um die Aufzeichn ung und Erkennung von Aktionen zu ermöglichen, die die Informationssicher heit beeinträchtigen könnten oder für sie relevant sind; - Die Verwaltun gsaktivitäten sollten eng koordiniert werden, um einerseit s den Service für die Organisat ion zu optimieren und andererseits sicherzustellen, dass die Kontrollen in der gesamten Informati		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
	onsverarbeitungsin frastruktur einheitlich angewendet werden; - Die Systeme im Netzwerk sollten authentifiziert werden; und - Nicht vertrauen swürdige Systemver bindungen zum Netzwerk sollten eingeschränkt werden.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
3.1.2(c)	c) Es sollten Kontrollen eingeführt werden, um die Informationssicherheit in Netzwerken und den Schutz vernetzter Services vor unbefugtem Zugriff zu gewährleisten. Insbesondere sollten die folgenden Punkte in Erwägung gezogen werden: - Für die Verwaltung von Netzwerkgeräten sollten Zuständigkeiten und Verfahren festgelegt werden; - Die operative Verantwortung für Netzwerke sollte gegebenenfalls von den Computerorgängen getrennt werden; - Es sollten spezifische Kontrollen eingeführt werden, um die Vertraulichkeit und Integrität von Daten zu gewährleisten, die über öffentliche oder drahtlose Netzwerke übertrage	s3- account-level-public-access -blöcke-periodisch	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Simple Storage Service (Amazon S3) -Buckets nicht öffentlich zugänglich sind. Diese Regel trägt dazu bei, sensible Daten vor unbefugten Remote-Benutzern zu schützen, indem sie den öffentlichen Zugriff verhindert. Mit dieser Regel können Sie optional die Parameter ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) und restrictPublicBuckets Parameter (Config Default: True) festlegen. Die tatsächlichen Werte müssen den Richtlini

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
	n werden, und um die vernetzten Systeme und Anwendung en zu schützen (einschließlich Netzwerkverschlüss elungsprotokollen bei Verbindungen zu nicht vertrauenswürdigen Systemen/Netzwerke n); - Es sollten eine angemesse ne Protokollierung und Überwachung durchgeführt werden, um die Aufzeichn ung und Erkennung von Aktionen zu ermöglichen, die die Informationssicher heit beeinträchtigen könnten oder für sie relevant sind; - Die Verwaltun gsaktivitäten sollten eng koordiniert werden, um einerseit s den Service für die Organisat ion zu optimieren und andererseits sicherzustellen, dass die Kontrollen in der gesamten Informati		en Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
	onsverarbeitungsin frastruktur einheitlich angewendet werden; - Die Systeme im Netzwerk sollten authentifiziert werden; und - Nicht vertrauen swürdige Systemver bindungen zum Netzwerk sollten eingeschränkt werden.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
3.1.2(c)	c) Es sollten Kontrollen eingeführt werden, um die Informationssicherheit in Netzwerken und den Schutz vernetzter Services vor unbefugtem Zugriff zu gewährleisten. Insbesondere sollten die folgenden Punkte in Erwägung gezogen werden: - Für die Verwaltung von Netzwerkgeräten sollten Zuständigkeiten und Verfahren festgelegt werden; - Die operative Verantwortung für Netzwerke sollte gegebenenfalls von den Computerorgängen getrennt werden; - Es sollten spezifische Kontrollen eingeführt werden, um die Vertraulichkeit und Integrität von Daten zu gewährleisten, die über öffentliche oder drahtlose Netzwerke übertrage	ssm-document-not-public	Stellen Sie sicher, dass AWS Systems Manager (SSM) - Dokumente nicht öffentlich sind, da dies einen unbeabsichtigten Zugriff auf Ihre SSM-Dokumente ermöglichen kann. Ein öffentliches SSM-Dokument kann Informationen über Ihr Konto, Ihre Ressourcen und internen Prozesse preisgeben.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
	n werden, und um die vernetzten Systeme und Anwendung en zu schützen (einschließlich Netzwerkverschlüss elungsprotokollen bei Verbindungen zu nicht vertrauenswürdigen Systemen/Netzwerke n); - Es sollten eine angemesse ne Protokollierung und Überwachung durchgeführt werden, um die Aufzeichn ung und Erkennung von Aktionen zu ermöglichen, die die Informationssicher heit beeinträchtigen könnten oder für sie relevant sind; - Die Verwaltun gsaktivitäten sollten eng koordiniert werden, um einerseit s den Service für die Organisat ion zu optimieren und andererseits sicherzustellen, dass die Kontrollen in der gesamten Informati		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
	onsverarbeitungsin frastruktur einheitlich angewendet werden; - Die Systeme im Netzwerk sollten authentifiziert werden; und - Nicht vertrauen swürdige Systemver bindungen zum Netzwerk sollten eingeschränkt werden.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
3.1.2(e)	e) Netzwerkservices können von einfacher , nicht verwaltet er Bandbreite bis hin zu anspruchs vollen Services wie VPN, Voice over IP, VSAT usw. reichen. Netzwerkservices sollten folgende Sicherheitsmerkmal e aufweisen: - Technologien zum Schutz von Netzwerks ervices, z. B. Authentifizierung, Verschlüsselung und Kontrolle der Netzwerkverbindung ; - Technische Parameter für eine sichere Verbindung mit den Netzwerks ervices gemäß den Sicherheits- und Netzwerkv erbindungsregeln; und - Verfahren für die Nutzung von Netzwerkservices, um gegebenen falls den Zugriff auf Netzwerkservices	acm-certificate-ex piration-check	Stellen Sie sicher, dass die Netzwerki ntegrität geschützt ist, indem Sie sicherste llen, dass X509-Zertifikate von ACM ausgestellt werden. AWS Diese Zertifika te müssen gültig und dürfen nicht abgelaufen sein. Für diese Regel ist ein Wert für erforderlich daysToExpiration (Wert für bewährte AWS Grundregeln für Sicherheit: 90). Der tatsächliche Wert muss den Richtlini en Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
	oder -anwendungen einzuschränken.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
3.1.2(e)	e) Netzwerkservices können von einfacher , nicht verwaltet er Bandbreite bis hin zu anspruchs vollen Services wie VPN, Voice over IP, VSAT usw. reichen. Netzwerkservices sollten folgende Sicherheitsmerkmal e aufweisen: - Technologien zum Schutz von Netzwerks ervices, z. B. Authentifizierung, Verschlüsselung und Kontrolle der Netzwerkverbindung ; - Technische Parameter für eine sichere Verbindung mit den Netzwerks ervices gemäß den Sicherheits- und Netzwerkv erbindungsregeln; und - Verfahren für die Nutzung von Netzwerkservices, um gegebenen falls den Zugriff auf Netzwerkservices	alb-http-to-https-Umleitungsprüfung	Um Daten während der Übertragung zu schützen, stellen Sie sicher, dass Ihr Application Load Balancer unverschl üsselte HTTP-Anfr agen automatisch an HTTPS umleitet. Da sensible Daten vorhanden sein können, sollten Sie die Verschlüsselung bei der Übertragung aktivieren, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
	oder -anwendungen einzuschränken.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
3.1.2(e)	e) Netzwerkservices können von einfacher , nicht verwaltet er Bandbreite bis hin zu anspruchs vollen Services wie VPN, Voice over IP, VSAT usw. reichen. Netzwerkservices sollten folgende Sicherheitsmerkmal e aufweisen: - Technologien zum Schutz von Netzwerks ervices, z. B. Authentifizierung, Verschlüsselung und Kontrolle der Netzwerkverbindung ; - Technische Parameter für eine sichere Verbindung mit den Netzwerks ervices gemäß den Sicherheits- und Netzwerkv erbindungsregeln; und - Verfahren für die Nutzung von Netzwerkservices, um gegebenen falls den Zugriff auf Netzwerkservices	elb-acm-certificate-required	Zum Schutz von eventuell vorhanden en sensiblen Daten sowie von Daten während der Übertragung muss die Verschlüsselung für Ihr Elastic Load Balancing aktiviert sein. Verwenden Sie AWS Certificate Manager, um öffentlic he und private SSL/ TLS-Zertifikate mit AWS Diensten und internen Ressource n zu verwalten, bereitzustellen und bereitzustellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
	oder -anwendungen einzuschränken.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
3.1.2(e)	e) Netzwerkservices können von einfacher , nicht verwaltet er Bandbreite bis hin zu anspruchs vollen Services wie VPN, Voice over IP, VSAT usw. reichen. Netzwerkservices sollten folgende Sicherheitsmerkmal e aufweisen: - Technologien zum Schutz von Netzwerks ervices, z. B. Authentifizierung, Verschlüsselung und Kontrolle der Netzwerkverbindung ; - Technische Parameter für eine sichere Verbindung mit den Netzwerks ervices gemäß den Sicherheits- und Netzwerkv erbindungsregeln; und - Verfahren für die Nutzung von Netzwerkservices, um gegebenen falls den Zugriff auf Netzwerkservices	redshift-require-tls-ssl	Stellen Sie sicher, dass Ihre Amazon-Redshift-Cluster eine TLS/SSL-Verschlüss elung erfordern, um eine Verbindung zu SQL-Clients herzustel len. Da sensible Daten vorhanden sein können, sollten Sie die Verschlüsselung bei der Übertragung aktivieren, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
	oder -anwendungen einzuschränken.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
3.1.2(e)	e) Netzwerkservices können von einfacher , nicht verwaltet er Bandbreite bis hin zu anspruchs vollen Services wie VPN, Voice over IP, VSAT usw. reichen. Netzwerkservices sollten folgende Sicherheitsmerkmal e aufweisen: - Technologien zum Schutz von Netzwerks ervices, z. B. Authentifizierung, Verschlüsselung und Kontrolle der Netzwerkverbindung ; - Technische Parameter für eine sichere Verbindung mit den Netzwerks ervices gemäß den Sicherheits- und Netzwerkv erbindungsregeln; und - Verfahren für die Nutzung von Netzwerkservices, um gegebenen falls den Zugriff auf Netzwerkservices	s-3 bucket-ssl-request s-only	Um Daten während der Übertragung zu schützen, stellen Sie sicher, dass Ihre Amazon Simple Storage Service (Amazon S3)-Bucke ts Anfragen zur Verwendung von Secure Socket Layer (SSL)-Buckets erfordern. Da sensible Daten vorhanden sein können, sollten Sie die Verschlüsselung bei der Übertragung aktivieren, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
	oder -anwendungen einzuschränken.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
3.1.2(e)	e) Netzwerkservices können von einfacher , nicht verwaltet er Bandbreite bis hin zu anspruchs vollen Services wie VPN, Voice over IP, VSAT usw. reichen. Netzwerkservices sollten folgende Sicherheitsmerkmal e aufweisen: - Technologien zum Schutz von Netzwerks ervices, z. B. Authentifizierung, Verschlüsselung und Kontrolle der Netzwerkverbindung ; - Technische Parameter für eine sichere Verbindung mit den Netzwerks ervices gemäß den Sicherheits- und Netzwerkv erbindungsregeln; und - Verfahren für die Nutzung von Netzwerkservices, um gegebenen falls den Zugriff auf Netzwerkservices	alb-http-drop-invalid-Header-fähig	Stellen Sie sicher, dass Ihre Elastic Load Balancers (ELB) so konfiguriert sind, dass sie HTTP-Header löschen. Da sensible Daten vorhanden sein können, sollten Sie die Verschlüsselung bei der Übertragung aktivieren, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
	oder -anwendungen einzuschränken.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
3.1.2(e)	e) Netzwerkservices können von einfacher , nicht verwaltet er Bandbreite bis hin zu anspruchs vollen Services wie VPN, Voice over IP, VSAT usw. reichen. Netzwerkservices sollten folgende Sicherheitsmerkmal e aufweisen: - Technologien zum Schutz von Netzwerks ervices, z. B. Authentifizierung, Verschlüsselung und Kontrolle der Netzwerkverbindung ; - Technische Parameter für eine sichere Verbindung mit den Netzwerks ervices gemäß den Sicherheits- und Netzwerkv erbindungsregeln; und - Verfahren für die Nutzung von Netzwerkservices, um gegebenen falls den Zugriff auf Netzwerkservices	elasticsearch-node -to-node-Verschlüs selungsprüfung	Stellen Sie sicher, dass die node-to-node Verschlüs selung für Amazon OpenSearch Service aktiviert ist. Node-to-nodeVerschlüsselung ermöglicht die TLS 1.2-Verschlüsselun g für die gesamte Kommunikation innerhalb der Amazon Virtual Private Cloud (Amazon VPC). Um eventuell vorhanden e sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
	oder -anwendungen einzuschränken.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
3.1.2(e)	e) Netzwerkservices können von einfacher , nicht verwaltet er Bandbreite bis hin zu anspruchs vollen Services wie VPN, Voice over IP, VSAT usw. reichen. Netzwerkservices sollten folgende Sicherheitsmerkmal e aufweisen: - Technologien zum Schutz von Netzwerks ervices, z. B. Authentifizierung, Verschlüsselung und Kontrolle der Netzwerkverbindung ; - Technische Parameter für eine sichere Verbindung mit den Netzwerks ervices gemäß den Sicherheits- und Netzwerkv erbindungsregeln; und - Verfahren für die Nutzung von Netzwerkservices, um gegebenen falls den Zugriff auf Netzwerkservices	opensearch-node-to-node-Verschlüsselungsprüfung	Stellen Sie sicher, dass die node-to-node Verschlüs selung für Amazon OpenSearch Service aktiviert ist. Node-to-nodeVerschlüsselung ermöglicht die TLS 1.2-Verschlüsselun g für die gesamte Kommunikation innerhalb der Amazon Virtual Private Cloud (Amazon VPC). Um eventuell vorhanden e sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
	oder -anwendungen einzuschränken.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
3.1.2(e)	e) Netzwerkservices können von einfacher , nicht verwaltet er Bandbreite bis hin zu anspruchs vollen Services wie VPN, Voice over IP, VSAT usw. reichen. Netzwerkservices sollten folgende Sicherheitsmerkmal e aufweisen: - Technologien zum Schutz von Netzwerks ervices, z. B. Authentifizierung, Verschlüsselung und Kontrolle der Netzwerkverbindung ; - Technische Parameter für eine sichere Verbindung mit den Netzwerks ervices gemäß den Sicherheits- und Netzwerkv erbindungsregeln; und - Verfahren für die Nutzung von Netzwerkservices, um gegebenen falls den Zugriff auf Netzwerkservices	elb-tls-https-listeners-nur	Stellen Sie sicher, dass Ihre Elastic Load Balancer (ELBs) mit SSL- oder HTTPS-Listenern konfiguriert sind. Um eventuell vorhanden e sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
	oder -anwendungen einzuschränken.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
3.1.2(e)	e) Netzwerkservices können von einfacher , nicht verwaltet er Bandbreite bis hin zu anspruchs vollen Services wie VPN, Voice over IP, VSAT usw. reichen. Netzwerkservices sollten folgende Sicherheitsmerkmal e aufweisen: - Technologien zum Schutz von Netzwerks ervices, z. B. Authentifizierung, Verschlüsselung und Kontrolle der Netzwerkverbindung ; - Technische Parameter für eine sichere Verbindung mit den Netzwerks ervices gemäß den Sicherheits- und Netzwerkv erbindungsregeln; und - Verfahren für die Nutzung von Netzwerkservices, um gegebenen falls den Zugriff auf Netzwerkservices	api-gw-ssl-enabled	Stellen Sie sicher, dass die REST-API-Stufen von Amazon API Gateway mit SSL-Zertifikaten konfiguri ert sind, damit Backend-Systeme überprüfen können, ob Anforderungen von API Gateway stammen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
	oder -anwendungen einzuschränken.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
3.1.2(e)	e) Netzwerkservices können von einfacher , nicht verwaltet er Bandbreite bis hin zu anspruchs vollen Services wie VPN, Voice over IP, VSAT usw. reichen. Netzwerkservices sollten folgende Sicherheitsmerkmal e aufweisen: - Technologien zum Schutz von Netzwerks ervices, z. B. Authentifizierung, Verschlüsselung und Kontrolle der Netzwerkverbindung ; - Technische Parameter für eine sichere Verbindung mit den Netzwerks ervices gemäß den Sicherheits- und Netzwerkv erbindungsregeln; und - Verfahren für die Nutzung von Netzwerkservices, um gegebenen falls den Zugriff auf Netzwerkservices	elbv-2 acm-certificate-required	Zum Schutz von eventuell vorhanden en sensiblen Daten sowie von Daten während der Übertragung muss die Verschlüsselung für Ihr Elastic Load Balancing aktiviert sein. Verwenden Sie AWS Certificate Manager, um öffentlic he und private SSL/ TLS-Zertifikate mit AWS Diensten und internen Ressource n zu verwalten, bereitzustellen und bereitzustellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
	oder -anwendungen einzuschränken.		
3.1.3(e)	e) Schützen Sie die Kommunikationskanäle zwischen dem Remotezugriffsgerät und der Einrichtung durch Verschlüsselung, um die mit Netzwerk-Spoofing verbundenen Risiken zu begrenzen.	acm-certificate-expiration-check	Stellen Sie sicher, dass die Netzwerkintegrität geschützt ist, indem Sie sicherstellen, dass X509-Zertifikate von ACM ausgestellt werden. AWS Diese Zertifikate müssen gültig und dürfen nicht abgelaufen sein. Für diese Regel ist ein Wert für erforderlich daysToExpiration (Wert für bewährte AWS Grundregeln für Sicherheit: 90). Der tatsächliche Wert muss den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
3.1.3(e)	e) Schützen Sie die Kommunikationskanäle zwischen dem Remotezugriffsgerät und der Einrichtung durch Verschlüsselung, um die mit Netzwerk-Spoofing verbundenen Risiken zu begrenzen.	alb-http-to-https-Umleitungsprüfung	Um Daten während der Übertragung zu schützen, stellen Sie sicher, dass Ihr Application Load Balancer unverschlüsselte HTTP-Anfragen automatisch an HTTPS umleitet. Da sensible Daten vorhanden sein können, sollten Sie die Verschlüsselung bei der Übertragung aktivieren, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
3.1.3(e)	e) Schützen Sie die Kommunikationskanäle zwischen dem Remotezugriffsgerät und der Einrichtung durch Verschlüsselung, um die mit Netzwerk-Spoofing verbundenen Risiken zu begrenzen.	elb-acm-certificate-required	Zum Schutz von eventuell vorhandenen sensiblen Daten sowie von Daten während der Übertragung muss die Verschlüsselung für Ihr Elastic Load Balancing aktiviert sein. Verwenden Sie AWS Certificate Manager, um öffentliche und private SSL/TLS-Zertifikate mit AWS Diensten und internen Ressourcen zu verwalten, bereitzustellen und bereitzustellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
3.1.3(e)	e) Schützen Sie die Kommunikationskanäle zwischen dem Remotezugriffsgerät und der Einrichtung durch Verschlüsselung, um die mit Netzwerk-Spoofing verbundenen Risiken zu begrenzen.	redshift-require-tls-ssl	Stellen Sie sicher, dass Ihre Amazon-Redshift-Cluster eine TLS/SSL-Verschlüsselung erfordern, um eine Verbindung zu SQL-Clients herzustellen. Da sensible Daten vorhanden sein können, sollten Sie die Verschlüsselung bei der Übertragung aktivieren, um diese Daten zu schützen.
3.1.3(e)	e) Schützen Sie die Kommunikationskanäle zwischen dem Remotezugriffsgerät und der Einrichtung durch Verschlüsselung, um die mit Netzwerk-Spoofing verbundenen Risiken zu begrenzen.	s-3 bucket-ssl-requests-only	Um Daten während der Übertragung zu schützen, stellen Sie sicher, dass Ihre Amazon Simple Storage Service (Amazon S3)-Buckets Anfragen zur Verwendung von Secure Socket Layer (SSL)-Buckets erfordern. Da sensible Daten vorhanden sein können, sollten Sie die Verschlüsselung bei der Übertragung aktivieren, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
3.1.3(e)	e) Schützen Sie die Kommunikationskanäle zwischen dem Remotezugriffsgerät und der Einrichtung durch Verschlüsselung, um die mit Netzwerk-Spoofing verbundenen Risiken zu begrenzen.	alb-http-drop-invalid-Header-fähig	Stellen Sie sicher, dass Ihre Elastic Load Balancers (ELB) so konfiguriert sind, dass sie HTTP-Header löschen. Da sensible Daten vorhanden sein können, sollten Sie die Verschlüsselung bei der Übertragung aktivieren, um diese Daten zu schützen.
3.1.3(e)	e) Schützen Sie die Kommunikationskanäle zwischen dem Remotezugriffsgerät und der Einrichtung durch Verschlüsselung, um die mit Netzwerk-Spoofing verbundenen Risiken zu begrenzen.	elasticsearch-node-to-node-Verschlüsselungsprüfung	Stellen Sie sicher, dass die node-to-node Verschlüsselung für Amazon OpenSearch Service aktiviert ist. Node-to-nodeVerschlüsselung ermöglicht die TLS 1.2-Verschlüsselung für die gesamte Kommunikation innerhalb der Amazon Virtual Private Cloud (Amazon VPC). Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
3.1.3(e)	e) Schützen Sie die Kommunikationskanäle zwischen dem Remotezugriffsgerät und der Einrichtung durch Verschlüsselung, um die mit Netzwerk-Spoofing verbundenen Risiken zu begrenzen.	opensearch-node-to-node-Verschlüsselungsprüfung	Stellen Sie sicher, dass die node-to-node Verschlüsselung für Amazon OpenSearch Service aktiviert ist. Node-to-nodeVerschlüsselung ermöglicht die TLS 1.2-Verschlüsselung für die gesamte Kommunikation innerhalb der Amazon Virtual Private Cloud (Amazon VPC). Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.
3.1.3(e)	e) Schützen Sie die Kommunikationskanäle zwischen dem Remotezugriffsgerät und der Einrichtung durch Verschlüsselung, um die mit Netzwerk-Spoofing verbundenen Risiken zu begrenzen.	elb-tls-https-listeners-nur	Stellen Sie sicher, dass Ihre Elastic Load Balancer (ELBs) mit SSL- oder HTTPS-Listenern konfiguriert sind. Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
3.1.3(e)	e) Schützen Sie die Kommunikationskanäle zwischen dem Remotezugriffsgerät und der Einrichtung durch Verschlüsselung, um die mit Netzwerk-Spoofing verbundenen Risiken zu begrenzen.	api-gw-ssl-enabled	Stellen Sie sicher, dass die REST-API-Stufen von Amazon API Gateway mit SSL-Zertifikaten konfiguriert sind, damit Backend-Systeme überprüfen können, ob Anforderungen von API Gateway stammen.
3.1.3(e)	e) Schützen Sie die Kommunikationskanäle zwischen dem Remotezugriffsgerät und der Einrichtung durch Verschlüsselung, um die mit Netzwerk-Spoofing verbundenen Risiken zu begrenzen.	elbv-2 acm-certificate-required	Zum Schutz von eventuell vorhanden en sensiblen Daten sowie von Daten während der Übertragung muss die Verschlüsselung für Ihr Elastic Load Balancing aktiviert sein. Verwenden Sie AWS Certificate Manager, um öffentliche und private SSL/TLS-Zertifikate mit AWS Diensten und internen Ressourcen zu verwalten, bereitzustellen und bereitzustellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
3.1.3(g)	g) Führen Sie Protokolle für die Kommunikation per Remotezugriff. Die Protokolle sollten Datum, Uhrzeit, Benutzer, Standort, Dauer und Zweck sämtlicher Remotezugriffe enthalten, einschließlich aller per Remotezugriff ausgeführten Aktivitäten.	api-gw-execution-logging-aktiviert	Die API-Gateway-Protokollierung zeigt detaillierte Ansichten der Benutzer, die auf die API zugegriffen haben, und wie diese Benutzer auf die API zugegriffen haben. Diese Insights ermöglichen die Einsicht in Benutzeraktivitäten.
3.1.3(g)	g) Führen Sie Protokolle für die Kommunikation per Remotezugriff. Die Protokolle sollten Datum, Uhrzeit, Benutzer, Standort, Dauer und Zweck sämtlicher Remotezugriffe enthalten, einschließlich aller per Remotezugriff ausgeführten Aktivitäten.	cloud-trail-cloud-watch-logs-aktiviert	Verwenden Sie Amazon CloudWatch , um Protokoll ereignisaktivitäten zentral zu sammeln und zu verwalten. Die Aufnahme von AWS CloudTrail Daten liefert Einzelheiten zu den API-Aufrufaktivitäten in Ihrem AWS-Konto.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
3.1.3(g)	g) Führen Sie Protokolle für die Kommunikation per Remotezugriff. Die Protokolle sollten Datum, Uhrzeit, Benutzer, Standort, Dauer und Zweck sämtlicher Remotezugriffe enthalten, einschließlich aller per Remotezugriff ausgeführten Aktivitäten.	cloudtrail-enabled	AWS CloudTrail kann bei der Nichtabstreitbarkeit helfen, indem Aktionen und API-Aufrufe der AWS Management Console aufgezeichnet werden. Sie können die Benutzer und die Benutzer AWS-Konten , die einen AWS Dienst aufgerufen haben, die Quell-IP-Adresse, über die die Aufrufe generiert wurden, und den Zeitpunkt der Anrufe identifizieren. Einzelheiten zu den erfassten Daten finden Sie in den AWS CloudTrail Datensatzinhalten.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
3.1.3(g)	g) Führen Sie Protokolle für die Kommunikation per Remotezugriff. Die Protokolle sollten Datum, Uhrzeit, Benutzer, Standort, Dauer und Zweck sämtlicher Remotezugriffe enthalten, einschließlich aller per Remotezugriff ausgeführten Aktivitäten.	cloudtrail-s3-dataevents-enabled	Die Erfassung von Simple Storage Service (Amazon S3)-Datenereignissen unterstützt die Erkennung von ungewöhnlichen Aktivitäten. Zu den Details gehören AWS-Konto Informationen über den Zugriff auf einen Amazon S3 S3-Bucket, die IP-Adresse und die Uhrzeit des Ereignisses.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
3.1.3(g)	g) Führen Sie Protokolle für die Kommunikation per Remotezugriff. Die Protokolle sollten Datum, Uhrzeit, Benutzer, Standort, Dauer und Zweck sämtlicher Remotezugriffe enthalten, einschließlich aller per Remotezugriff ausgeführten Aktivitäten.	elb-logging-enabled	Die Elastic-Load-Balancing-Aktivität ist ein zentraler Kommunikationspunkt innerhalb einer Umgebung. Stellen Sie sicher, dass die ELB-Protokollierung aktiviert ist. Die gesammelten Daten enthalten detaillierte Informationen zu Anfragen, die an den ELB gesendet wurden. Jedes Protokoll enthält Informationen wie die Zeit, zu der die Anforderung einging, die Client-IP-Adresse, Latenzen, Anforderungspfade und Serverantworten.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
3.1.3(g)	g) Führen Sie Protokolle für die Kommunikation per Remotezugriff. Die Protokolle sollten Datum, Uhrzeit, Benutzer, Standort, Dauer und Zweck sämtlicher Remotezugriffe enthalten, einschließlich aller per Remotezugriff ausgeführten Aktivitäten.	multi-region-cloudtrail-enabled	AWS CloudTrail zeichnet Aktionen und API-Aufrufe der AWS Management Console auf. Sie können feststellen, welche Benutzer und Konten angerufen wurden AWS, von welcher Quell-IP-Adresse aus die Anrufe getätigt wurden und wann die Anrufe erfolgten. CloudTrail übermittelt Protokolldateien aus allen AWS Regionen an Ihren S3-Bucket, wenn MULTI_REGION_CLOUD_TRAIL_ENABLED aktiviert ist. Außerdem wird beim AWS Start einer neuen Region derselbe Trail in der neuen Region erstellt. CloudTrail Dadurch erhalten Sie automatisch Protokolldateien mit API-Aktivitäten für die neue Region.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
3.1.3(g)	g) Führen Sie Protokolle für die Kommunikation per Remotezugriff. Die Protokolle sollten Datum, Uhrzeit, Benutzer, Standort, Dauer und Zweck sämtlicher Remotezugriffe enthalten, einschließlich aller per Remotezugriff ausgeführten Aktivitäten.	s-3 bucket-logging-enabled	Die Amazon Simple Storage Service (Amazon S3)-Serverzugriffsprotokollierung bietet eine Methode zur Überwachung des Netzwerks im Hinblick auf potenzielle Cybersicherheitsereignisse. Die Ereignisse werden überwacht, indem detaillierte Aufzeichnungen über die Anfragen erfasst werden, die an einen Amazon-S3-Bucket gestellt wurden. Jeder Zugriffsprotokolleintrag enthält Details zu einer einzelnen Zugriffsanfrage. Zu den Details gehören Anforderer, Bucket-Name, Anforderungszeit, Anforderungsaktion, Antwortstatus und Fehlercode, falls relevant.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
3.1.3(g)	g) Führen Sie Protokolle für die Kommunikation per Remotezugriff. Die Protokolle sollten Datum, Uhrzeit, Benutzer, Standort, Dauer und Zweck sämtlicher Remotezugriffe enthalten, einschließlich aller per Remotezugriff ausgeführten Aktivitäten.	vpc-flow-logs-enabled	VPC-Flow-Protokolle erfassen detaillierte Informationsdatensätze über den IP-Datenverkehr, der zu und von Netzwerkschnittstellen in Ihrer Amazon Virtual Private Cloud (Amazon VPC) fließt. Standardmäßig enthalten Flow-Protokolldatensätze Werte für die verschiedenen Komponenten des IP-Flows, einschließlich Quelle, Ziel und Protokoll.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
3.1.3(g)	g) Führen Sie Protokolle für die Kommunikation per Remotezugriff. Die Protokolle sollten Datum, Uhrzeit, Benutzer, Standort, Dauer und Zweck sämtlicher Remotezugriffe enthalten, einschließlich aller per Remotezugriff ausgeführten Aktivitäten.	cw-loggroup-retention-period-überprüfen	Stellen Sie sicher, dass die Ereignisprotokolldaten für Ihre Protokollgruppen über eine Mindestdauer aufbewahrt werden, um die Fehlerbehebung und forensische Untersuchungen zu unterstützen. Fehlende frühere Ereignisprotokolldaten erschweren die Rekonstruierung und Identifizierung potenziell schädlicher Ereignisse.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
3.1.3(g)	g) Führen Sie Protokolle für die Kommunikation per Remotezugriff. Die Protokolle sollten Datum, Uhrzeit, Benutzer, Standort, Dauer und Zweck sämtlicher Remotezugriffe enthalten, einschließlich aller per Remotezugriff ausgeführten Aktivitäten.	rds-logging-enabled	Um die Protokollierung und Überwachung in Ihrer Umgebung zu erleichtern, stellen Sie sicher, dass die Amazon Relational Database Service (Amazon RDS)-Protokollierung aktiviert ist. Mit der Amazon-RDS-Protokollierung können Sie Ereignisse wie Verbindungen, Verbindungsabbrüche, Abfragen oder abgefragte Tabellen erfassen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
3.1.3(g)	g) Führen Sie Protokolle für die Kommunikation per Remotezugriff. Die Protokolle sollten Datum, Uhrzeit, Benutzer, Standort, Dauer und Zweck sämtlicher Remotezugriffe enthalten, einschließlich aller per Remotezugriff ausgeführten Aktivitäten.	wafv2-logging-enabled	Um Ihnen bei der Protokollierung und Überwachung in Ihrer Umgebung zu helfen, aktivieren Sie die AWS WAF (V2) -Protokollierung im regionalen und globalen Web. ACLs AWS Die WAF-Protokollierung bietet detaillierte Informationen über den Datenverkehr, der von Ihrer Web-ACL analysiert wird. In den Protokollen werden die Uhrzeit aufgezeichnet, zu der die AWS WAF die Anfrage von Ihrer AWS Ressource erhalten hat, Informationen zu der Anfrage und eine Aktion für die Regel, der jede Anfrage entsprach.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
3.1.3(g)	g) Führen Sie Protokolle für die Kommunikation per Remotezugriff. Die Protokolle sollten Datum, Uhrzeit, Benutzer, Standort, Dauer und Zweck sämtlicher Remotezugriffe enthalten, einschließlich aller per Remotezugriff ausgeführten Aktivitäten.	redshift-cluster-configuration-check	Um Daten im Ruhezustand zu schützen, muss die Verschlüsselung für Ihre Amazon-Redshift-Cluster aktiviert sein. Sie müssen auch sicherstellen, dass die erforderlichen Konfigurationen auf Amazon-Redshift-Clustern bereitgestellt werden. Die Prüfungsprotokollierung muss aktiviert sein, um Informationen zu Verbindungen und Benutzeraktivitäten in der Datenbank bereitzustellen. Diese Regel erfordert, dass ein Wert für clusterDbEncrypted (Config Default: TRUE) und LoggingEnabled (Config Default: TRUE) gesetzt ist. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
3.1.3(g)	g) Führen Sie Protokolle für die Kommunikation per Remotezugriff. Die Protokolle sollten Datum, Uhrzeit, Benutzer, Standort, Dauer und Zweck sämtlicher Remotezugriffe enthalten, einschließlich aller per Remotezugriff ausgeführten Aktivitäten.	elasticsearch-logs-to-cloudwatch	Stellen Sie sicher, dass für Amazon OpenSearch Service-Domains Fehlerprotokolle aktiviert und zur Aufbewahrung und Beantwortung an Amazon CloudWatch Logs gestreamt werden. Domain-Fehlerprotokolle sind bei Sicherheits- und Zugriffsprüfungen sowie bei der Diagnose von Verfügbarkeitsproblemen nützlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
3.1.3(g)	g) Führen Sie Protokolle für die Kommunikation per Remotezugriff. Die Protokolle sollten Datum, Uhrzeit, Benutzer, Standort, Dauer und Zweck sämtlicher Remotezugriffe enthalten, einschließlich aller per Remotezugriff ausgeführten Aktivitäten.	opensearch-logs-to-cloudwatch	Stellen Sie sicher, dass für Amazon OpenSearch Service-Domains Fehlerprotokolle aktiviert und zur Aufbewahrung und Beantwortung an Amazon CloudWatch Logs gestreamt werden. OpenSearch Service-Fehlerprotokolle können bei Sicherheits- und Zugriffsprüfungen helfen und bei der Diagnose von Verfügbarkeitsproblemen helfen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
3.1.3(i)	i) Erzwingen Sie eine Zwei-Faktor-Authentifizierung für den Fernzugriff (z. B. eine PIN-basierte Token-Karte mit einem einmaligen Zufallsknnwortgenerator oder eine Token-basierte PKI)	iam-user-mfa-enabled	Aktivieren Sie diese Regel, um den Zugriff auf Ressourcen in der AWS Cloud einzuschränken. Diese Regel sorgt dafür, dass die Multi-Faktor-Authentifizierung (MFA) für alle Benutzer aktiviert ist. MFA sorgt für eine weitere Schutzebene zusätzlich zu den Anmeldeinformationen. Reduzieren Sie Fälle von kompromittierten Konten, indem Sie MFA für Benutzer vorschreiben.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
3.1.3(i)	i) Erzwingen Sie eine Zwei-Faktor-Authentifizierung für den Fernzugriff (z. B. eine PIN-basierte Token-Karte mit einem einmaligen zufälligen Passwortgenerator oder eine tokenbasierte PKI)	mfa-enabled-for-iam-Konsolenzugriff	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass MFA für alle AWS Identity and Access Management (IAM) -Benutzer aktiviert ist, die über ein Konsolenkennwort verfügen. MFA sorgt für eine weitere Schutzebene zusätzlich zu den Anmeldeinformationen. Indem Sie MFA für Benutzer vorschreiben, können Sie Fälle kompromittierter Konten reduzieren und verhindern, dass unbefugte Benutzer auf vertrauliche Daten zugreifen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
3.1.3(i)	i) Erzwingen Sie eine Zwei-Faktor-Authentifizierung für den Fernzugriff (z. B. eine PIN-basierte Token-Karte mit einem einmaligen zufälligen Passwortgenerator oder eine tokenbasierte PKI)	root-account-hardware-mfa-aktiviert	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Hardware-MFA für den Root-Benutzer aktiviert ist. Der Stammbenutzer ist der AWS-Konto-Benutzer mit den meisten Berechtigungen. MFA sorgt für eine weitere Schutzebene zusätzlich zu den Anmeldeinformationen. Indem Sie MFA für den Root-Benutzer vorschreiben, können Sie die Anzahl AWS-Konten kompromittierter Benutzer reduzieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
3.1.3(i)	i) Erzwingen Sie eine Zwei-Faktor-Authentifizierung für den Fernzugriff (z. B. eine PIN-basierte Token-Karte mit einem zufälligen Einmalpasswortgenerator oder eine Token-basierte PKI)	root-account-mfa-enabled	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass MFA für den Root-Benutzer aktiviert ist. Der Stammbenutzer ist der AWS-Konto-Benutzer mit den meisten Berechtigungen. MFA sorgt für eine weitere Schutzebene zusätzlich zu den Anmeldeinformationen. Indem Sie MFA für den Root-Benutzer vorschreiben, können Sie die Anzahl AWS-Konten kompromittierter Benutzer reduzieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
3.1.4(c)(e)	c) Der Patch-Management-Prozess sollte folgende Aspekte beinhalten: - Festlegung von Methoden zur Beschaffung und Validierung von Patches, um sicherzustellen, dass der Patch von einer autorisierten Quelle stammt - Identifizierung von Sicherheitslücken, die für von der Organisation verwendete Anwendungen und Systeme gelten - Bewertung der geschäftlichen Auswirkungen der Implementierung von Patches (oder der Nichtimplementierung eines bestimmten Patches) - Sicherstellung, dass Patches getestet werden - Beschreibung von Methoden für die automatische Bereitstellung	ec2-manager instance-managed-by-systems	Eine Bestandsaufnahme der Softwareplattformen und Anwendungen innerhalb des Unternehmens ist möglich, indem Amazon Elastic Compute Cloud (Amazon EC2) - Instances mit AWS Systems Manager verwaltet werden. Verwenden Sie AWS Systems Manager, um detaillierte Systemkonfigurationen, Betriebssystem-Patch-Levels, Namen und Typ der Dienste, Softwareinstallationen, Anwendungsname, Herausgeber und Version sowie andere Details zu Ihrer Umgebung bereitzustellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
	von Patches, z. B. automatisch - Berichterstattung über den Status der Patch-Bereitstellung im gesamten Unternehmen und - Einbeziehen von Methoden für den Umgang mit der fehlgeschlagenen Bereitstellung eines Patches (z. B. erneutes Bereitstellen des Patches). e) BFIs sollte automatisierte Patch-Management-Tools und Softwareupdate-Tools für alle Systeme bereitstellen, für die solche Tools verfügbar und sicher sind		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
3.1.4(c)(e)	c) Der Patch-Management-Prozess sollte folgende Aspekte beinhalten: - Festlegung von Methoden zur Beschaffung und Validierung von Patches, um sicherzustellen, dass der Patch von einer autorisierten Quelle stammt - Identifizierung von Sicherheitslücken, die für von der Organisation verwendete Anwendungen und Systeme gelten - Bewertung der geschäftlichen Auswirkungen der Implementierung von Patches (oder der Nichtimplementierung eines bestimmten Patches) - Sicherstellung, dass Patches getestet werden - Beschreibung von Methoden für die automatische Bereitstellung	ec2-check managedinstance-association-compliance-status	Verwenden Sie AWS Systems Manager Associations, um bei der Inventarisierung von Softwareplattformen und Anwendungen innerhalb eines Unternehmens zu helfen. AWS Systems Manager weist Ihren verwalteten Instanzen einen Konfigurationsstatus zu und ermöglicht es Ihnen, Basiswerte für Betriebssystem-Patch-Levels, Softwareinstallationen, Anwendungskonfigurationen und andere Details zu Ihrer Umgebung festzulegen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
	von Patches, z. B. automatisch - Berichterstattung über den Status der Patch-Bereitstellung im gesamten Unternehmen und - Einbeziehen von Methoden für den Umgang mit der fehlgeschlagenen Bereitstellung eines Patches (z. B. erneutes Bereitstellen des Patches). e) BFIs sollte automatisierte Patch-Management-Tools und Softwareupdate-Tools für alle Systeme bereitstellen, für die solche Tools verfügbar und sicher sind		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
3.1.4(c)(e)	c) Der Patch-Management-Prozess sollte folgende Aspekte beinhalten: - Festlegung von Methoden zur Beschaffung und Validierung von Patches, um sicherzustellen, dass der Patch von einer autorisierten Quelle stammt - Identifizierung von Sicherheitslücken, die für von der Organisation verwendete Anwendungen und Systeme gelten - Bewertung der geschäftlichen Auswirkungen der Implementierung von Patches (oder der Nichtimplementierung eines bestimmten Patches) - Sicherstellung, dass Patches getestet werden - Beschreibung von Methoden für die automatische Bereitstellung	ec2-check managedinstance-patch-compliance-status	Aktivieren Sie diese Regel, um bei der Identifizierung und Dokumentation von Sicherheitslücken in Amazon Elastic Compute Cloud (Amazon EC2) zu helfen. Die Regel prüft, ob die EC2 Amazon-Instance die Patch-Konformität im AWS Systems Manager gemäß den Richtlinien und Verfahren Ihrer Organisation einhält.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
	von Patches, z. B. automatisch - Berichterstattung über den Status der Patch-Bereitstellung im gesamten Unternehmen und - Einbeziehen von Methoden für den Umgang mit der fehlgeschlagenen Bereitstellung eines Patches (z. B. erneutes Bereitstellen des Patches). e) BFIs sollte automatisierte Patch-Management-Tools und Softwareupdate-Tools für alle Systeme bereitstellen, für die solche Tools verfügbar und sicher sind		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
3.1.4(c)(e)	c) Der Patch-Management-Prozess sollte folgende Aspekte beinhalten: - Festlegung von Methoden zur Beschaffung und Validierung von Patches, um sicherzustellen, dass der Patch von einer autorisierten Quelle stammt - Identifizierung von Sicherheitslücken, die für von der Organisation verwendete Anwendungen und Systeme gelten - Bewertung der geschäftlichen Auswirkungen der Implementierung von Patches (oder der Nichtimplementierung eines bestimmten Patches) - Sicherstellung, dass Patches getestet werden - Beschreibung von Methoden für die automatische Bereitstellung	redshift-cluster-maintenancesettings-check	Diese Regel stellt sicher, dass Amazon-Redshift-Cluster die bevorzugten Einstellungen für Ihre Organisation haben. Insbesondere sorgt sie dafür, dass Cluster bevorzugte Wartungsfenster und automatisierte Aufbewahrungsfristen für Snapshots für die Datenbank haben. Für diese Regel müssen Sie die allowVersionUpgrade festlegen. Der Standardwert ist „true“. Außerdem können Sie optional den Zeitraum preferredMaintenanceWindow (der Standardwert ist sa: 16:00 -sa: 16:30) und den automated SnapshotRetention Zeitraum (der Standardwert ist 1) festlegen. Die tatsächlichen Werte müssen den Richtlini

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
	von Patches, z. B. automatisch - Berichterstattung über den Status der Patch-Bereitstellung im gesamten Unternehmen und - Einbeziehen von Methoden für den Umgang mit der fehlgeschlagenen Bereitstellung eines Patches (z. B. erneutes Bereitstellen des Patches). e) BFIs sollte automatisierte Patch-Management-Tools und Softwareupdate-Tools für alle Systeme bereitstellen, für die solche Tools verfügbar und sicher sind		en Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
3.1.4(c)(e)	c) Der Patch-Management-Prozess sollte folgende Aspekte beinhalten: - Festlegung von Methoden zur Beschaffung und Validierung von Patches, um sicherzustellen, dass der Patch von einer autorisierten Quelle stammt - Identifizierung von Sicherheitslücken, die für von der Organisation verwendete Anwendungen und Systeme gelten - Bewertung der geschäftlichen Auswirkungen der Implementierung von Patches (oder der Nichtimplementierung eines bestimmten Patches) - Sicherstellung, dass Patches getestet werden - Beschreibung von Methoden für die automatische Bereitstellung	elastic-beanstalk-managed-updates-aktiviert	Durch die Aktivierung verwalteter Plattformupdates für eine Amazon-Elastic-Beanstalk-Umgebung wird sichergestellt, dass die aktuellen verfügbaren Plattform-Fixes, -Updates und -Features für die Umgebung installiert sind. Eine bewährte Methode zur Sicherung von Systemen besteht darin, stets die aktuellen Patches zu installieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
	von Patches, z. B. automatisch - Berichterstattung über den Status der Patch-Bereitstellung im gesamten Unternehmen und - Einbeziehen von Methoden für den Umgang mit der fehlgeschlagenen Bereitstellung eines Patches (z. B. erneutes Bereitstellen des Patches). e) BFIs sollte automatisierte Patch-Management-Tools und Softwareupdate-Tools für alle Systeme bereitstellen, für die solche Tools verfügbar und sicher sind		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
3.1.4(c)(e)	c) Der Patch-Management-Prozess sollte folgende Aspekte beinhalten: - Festlegung von Methoden für den Bezug und die Validierung von Patches, um sicherzustellen, dass der Patch von einer autorisierten Quelle stammt - Identifizierung von Sicherheitslücken, die für die von der Organisation verwendeten Anwendungen und Systeme gelten - Bewertung der geschäftlichen Auswirkungen der Implementierung von Patches (oder der Nichtimplementierung eines bestimmten Patches) - Sicherstellung, dass Patches getestet werden - Beschreibung von Methoden für die automatische Bereitstellung	rds-automatic-minor-version-Upgrade-fähig	Aktivieren Sie automatische Unterversions-Upgrades auf Ihren Amazon-Relational-Database-Service-(RDS-)Instances, um sicherzustellen, dass die aktuellen Updates für Unterversionen des Relational Database Management System (RDBMS) installiert sind, die Sicherheitspatches und Bugfixes enthalten können.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
	von Patches, z. B. automatisch - Berichterstattung über den Status der Patch-Bereitstellung im gesamten Unternehmen und - Einbeziehen von Methoden für den Umgang mit der fehlgeschlagenen Bereitstellung eines Patches (z. B. erneutes Bereitstellen des Patches). e) BFIs sollte automatisierte Patch-Management-Tools und Softwareupdate-Tools für alle Systeme bereitstellen, für die solche Tools verfügbar und sicher sind		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
3.1.5(d)(e)	d) Eine angemessene Schlüsselverwaltung erfordert sichere Verfahren für Generierung, Speicherung, Archivierung, Abruf, Verteilung, Außerbetriebnahme und Vernichtung kryptografischer Schlüssel. e) Alle kryptografischen Schlüssel sollten vor Änderung und Verlust geschützt werden. Darüber hinaus müssen geheime und private Schlüssel vor unbefugter Verwendung und Offenlegung geschützt werden. Geräte, die zum Generieren, Speichern und Archivieren von Schlüsseln verwendet werden, sollten physisch geschützt werden.	kms-cmk-not-scheduled-zum Löschen	Um Daten im Ruhezustand zu schützen, sollten Sie sicherstellen, dass die für den Kunden erforderlichen Masterschlüssel (CMKs) nicht im AWS Key Management Service (AWS KMS) gelöscht werden. Da Schlüssel manchmal gelöscht werden müssen, können Sie mit dieser Regel alle zu löschenden Schlüssel überprüfen, falls ein Schlüssel versehentlich zur Löschung vorgemerkt wurde.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
3.1.5(d)(e)	d) Eine angemessene Schlüsselverwaltung erfordert sichere Verfahren für Generierung, Speicherung, Archivierung, Abruf, Verteilung, Außerbetriebnahme und Vernichtung kryptografischer Schlüssel. e) Alle kryptografischen Schlüssel sollten vor Änderung und Verlust geschützt werden. Darüber hinaus müssen geheime und private Schlüssel vor unbefugter Verwendung und Offenlegung geschützt werden. Geräte, die zum Generieren, Speichern und Archivieren von Schlüsseln verwendet werden, sollten physisch geschützt werden.	cmk-backing-key-rotation-aktiviert	Aktivieren Sie die Schlüsselrotation, um sicherzustellen, dass Schlüssel rotiert werden, nachdem sie das Ende ihrer Krypto-Periode erreicht haben.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
3.1.5(d)(e)	d) Eine angemessene Schlüsselverwaltung erfordert sichere Verfahren für Generierung, Speicherung, Archivierung, Abruf, Verteilung, Außerbetriebnahme und Vernichtung kryptografischer Schlüssel. e) Alle kryptografischen Schlüssel sollten vor Änderung und Verlust geschützt werden. Darüber hinaus müssen geheime und private Schlüssel vor unbefugter Verwendung und Offenlegung geschützt werden. Geräte, die zum Generieren, Speichern und Archivieren von Schlüsseln verwendet werden, sollten physisch geschützt werden.	iam-customer-policy-blocked-kms-Aktionen	AWS Identity and Access Management (IAM) kann Ihnen helfen, die Prinzipien der geringsten Rechte und der Aufgabentrennung in Zugriffsberechtigungen und Autorisierungen zu integrieren und so zu verhindern, dass Richtlinien blockierte Aktionen für alle AWS Schlüssel des Key Management Service enthalten. Wenn Benutzer mehr Rechte haben, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und Aufgabentrennung verstoßen. Mit dieser Regel können Sie den Parameter festlegen. blockedActionsPatterns (Wert „AWS Bewährte grundlegende Sicherheitsmethode

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
			n“: kms: Entschlüs seln, kms:ReEnc ryptFrom). Die tatsächlichen Werte müssen den Richtlini en Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
3.1.5(d)(e)	d) Eine angemessene Schlüsselverwaltung erfordert sichere Verfahren für Generierung, Speicherung, Archivierung, Abruf, Verteilung, Außerbetriebnahme und Vernichtung kryptografischer Schlüssel. e) Alle kryptografischen Schlüssel sollten vor Änderung und Verlust geschützt werden. Darüber hinaus müssen geheime und private Schlüssel vor unbefugter Verwendung und Offenlegung geschützt werden. Geräte, die zum Generieren, Speichern und Archivieren von Schlüsseln verwendet werden, sollten physisch geschützt werden.	iam-inline-policy-blocked-kms-Aktionen	Stellen Sie sicher, dass ein Benutzer, eine IAM-Rolle oder eine IAM-Gruppe (AWS Identity and Access Management) nicht über eine Inline-Richtlinie verfügt, die blockierte Aktionen für alle AWS Schlüssel des Key Management Service zulässt. AWS empfiehlt, verwaltete Richtlinien anstelle von Inline-Richtlinien zu verwenden. Verwaltete Richtlinien ermöglichen Wiederverwendbarkeit, Versionsverwaltung, Rollback und Delegierung der Berechtigungsverwaltung. Mit dieser Regel können Sie den blockedActionsPatterns Parameter festlegen. (Wert „AWS Bewährte grundlegende Sicherheitsmethoden“: kms: Entschlüsseln, kms:ReEnc

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
			ryptFrom). Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
3.1.5(f)	f) Ein Schlüssel verwaltungssystem sollte auf vereinbarten Standards , Verfahren und sicheren Methoden basieren für: - Generierung von Schlüsseln für verschiedene kryptografische Systeme und verschiedene Anwendungen - Ausstellung und Beschaffung von Zertifikaten für öffentliche Schlüssel - Verteilung von Schlüsseln an vorgesehene Einrichtungen, einschließlich der Art und Weise, wie Schlüssel beim Empfang aktiviert werden sollten - Speicherung von Schlüsseln, einschließlich der Art und Weise, wie autorisierte Benutzer Zugriff auf Schlüssel erhalten - Änderung oder	kms-cmk-not-scheduled-zum Löschen	Um Daten im Ruhezustand zu schützen, sollten Sie sicherstellen, dass die für den Kunden erforderlichen Masterschlüssel (CMKs) nicht im AWS Key Management Service (AWS KMS) gelöscht werden. Da Schlüssel manchmal gelöscht werden müssen, können Sie mit dieser Regel alle zu löschenden Schlüssel überprüfen, falls ein Schlüssel versehentlich zur Löschung vorgemerkt wurde.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
	Aktualisierung von Schlüsseln, einschließlich Regeln darüber, wann Schlüssel geändert werden sollten und wie dies geschehen soll - Umgang mit kompromittierten Schlüsseln - Widerruf Schlüssel, einschließlich How-Schlüssel sollte zurückgezogen oder deaktiviert werden, beispielsweise wenn Schlüssel kompromittiert wurden oder wenn ein Benutzer eine Organisation verlässt (in diesem Fall sollten Schlüssel auch archiviert werden) — Wiederherstellung verloren gegangener oder beschädigter Schlüssel — Sicherung oder Archivierung von Schlüsseln — Zerstörung von Schlüsseln und — Protokollierung und Prüfung von Aktivität		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
	en im Zusammenh ang mit der Schlüssel verwaltung.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
3.1.5(f)	f) Ein Schlüssel verwaltungssystem sollte auf vereinbarten Standards , Verfahren und sicheren Methoden basieren für: - Generierung von Schlüsseln für verschiedene kryptografische Systeme und verschiedene Anwendungen - Ausstellung und Beschaffung von Zertifikaten für öffentliche Schlüssel - Verteilung von Schlüsseln an vorgesehene Einrichtungen, einschließlich der Art und Weise, wie Schlüssel beim Empfang aktiviert werden sollten - Speicherung von Schlüsseln, einschließlich der Art und Weise, wie autorisierte Benutzer Zugriff auf Schlüssel erhalten - Änderung oder	cmk-backing-key-rotation-aktiviert	Aktivieren Sie die Schlüsselrotation, um sicherzustellen, dass Schlüssel rotiert werden, nachdem sie das Ende ihrer Krypto-Periode erreicht haben.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
	Aktualisierung von Schlüsseln, einschließlich Regeln darüber, wann Schlüssel geändert werden sollten und wie dies geschehen soll - Umgang mit kompromittierten Schlüsseln - Widerruf Schlüssel, einschließlich How-Schlüssel sollte zurückgezogen oder deaktiviert werden, beispielsweise wenn Schlüssel kompromittiert wurden oder wenn ein Benutzer eine Organisation verlässt (in diesem Fall sollten Schlüssel auch archiviert werden) — Wiederherstellung verloren gegangener oder beschädigter Schlüssel — Sicherung oder Archivierung von Schlüsseln — Zerstörung von Schlüsseln und — Protokollierung und Prüfung von Aktivität		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
	en im Zusammenh ang mit der Schlüssel verwaltung.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
3.1.5(f)	f) Ein Schlüssel verwaltungssystem sollte auf vereinbarten Standards , Verfahren und sicheren Methoden basieren für: - Generierung von Schlüsseln für verschiedene kryptografische Systeme und verschiedene Anwendungen - Ausstellung und Beschaffung von Zertifikaten für öffentliche Schlüssel - Verteilung von Schlüsseln an vorgesehene Einrichtungen, einschließlich der Art und Weise, wie Schlüssel beim Empfang aktiviert werden sollten - Speicherung von Schlüsseln, einschließlich der Art und Weise, wie autorisierte Benutzer Zugriff auf Schlüssel erhalten - Änderung oder	acm-certificate-expiration-check	Stellen Sie sicher, dass die Netzwerkintegrität geschützt ist, indem Sie sicherstellen, dass X509-Zertifikate von ACM ausgestellt werden. AWS Diese Zertifikate müssen gültig und dürfen nicht abgelaufen sein. Für diese Regel ist ein Wert für erforderlich daysToExpiration (Wert für bewährte AWS Grundregeln für Sicherheit: 90). Der tatsächliche Wert muss den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
	Aktualisierung von Schlüsseln, einschließlich Regeln darüber, wann Schlüssel geändert werden sollten und wie dies geschehen soll - Umgang mit kompromittierten Schlüsseln - Widerruf Schlüssel, einschließlich How-Schlüssel sollte zurückgezogen oder deaktiviert werden, beispielsweise wenn Schlüssel kompromittiert wurden oder wenn ein Benutzer eine Organisation verlässt (in diesem Fall sollten Schlüssel auch archiviert werden) — Wiederherstellung verloren gegangener oder beschädigter Schlüssel — Sicherung oder Archivierung von Schlüsseln — Zerstörung von Schlüsseln und — Protokollierung und Prüfung von Aktivität		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
	en im Zusammenh ang mit der Schlüssel verwaltung.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
3.1.5(f)	f) Ein Schlüssel verwaltungssystem sollte auf vereinbarten Standards, Verfahren und sicheren Methoden basieren für: - Generierung von Schlüsseln für verschiedene kryptografische Systeme und verschiedene Anwendungen - Ausstellung und Beschaffung von Zertifikaten für öffentliche Schlüssel - Verteilung von Schlüsseln an vorgesehene Einrichtungen, einschließlich der Art und Weise, wie Schlüssel beim Empfang aktiviert werden sollten - Speicherung von Schlüsseln, einschließlich der Art und Weise, wie autorisierte Benutzer Zugriff auf Schlüssel erhalten - Änderung oder	elb-acm-certificate-required	Zum Schutz von eventuell vorhandenen sensiblen Daten sowie von Daten während der Übertragung muss die Verschlüsselung für Ihr Elastic Load Balancing aktiviert sein. Verwenden Sie AWS Certificate Manager, um öffentliche und private SSL/TLS-Zertifikate mit AWS Diensten und internen Ressourcen zu verwalten, bereitzustellen und bereitzustellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
	Aktualisierung von Schlüsseln, einschließlich Regeln darüber, wann Schlüssel geändert werden sollten und wie dies geschehen soll - Umgang mit kompromittierten Schlüsseln - Widerruf Schlüssel, einschließlich How-Schlüssel sollte zurückgezogen oder deaktiviert werden, beispielsweise wenn Schlüssel kompromittiert wurden oder wenn ein Benutzer eine Organisation verlässt (in diesem Fall sollten Schlüssel auch archiviert werden) — Wiederherstellung verloren gegangener oder beschädigter Schlüssel — Sicherung oder Archivierung von Schlüsseln — Zerstörung von Schlüsseln und — Protokollierung und Prüfung von Aktivität		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
	en im Zusammenh ang mit der Schlüssel verwaltung.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
3.1.5(f)	f) Ein Schlüssel verwaltungssystem sollte auf vereinbar ten Standards , Verfahren und sicheren Methoden basieren für: - Generierung von Schlüsseln für verschiedene kryptografische Systeme und verschiedene Anwendungen - Ausstellung und Beschaffung von Zertifikaten für öffentliche Schlüssel - Verteilung von Schlüsseln an vorgesehene Einrichtu ngen, einschließlich der Art und Weise, wie Schlüssel beim Empfang aktiviert werden sollten - Speicherung von Schlüsseln, einschlie ßlich der Art und Weise, wie autorisie rte Benutzer Zugriff auf Schlüssel erhalten - Änderung oder	cloudtrail-enabled	AWS CloudTrai l kann durch die Aufzeichnung von Aktionen und API-Aufrufen der AWS Management Console bei der Nichtabst reitbarkeit helfen. Sie können die Benutzer und die Benutzer AWS-Konten , die einen AWS Dienst aufgerufen haben, die Quell-IP-Adresse, über die die Aufrufe generiert wurden, und den Zeitpunkt der Anrufe identifiz ieren. Einzelheiten zu den erfassten Daten finden Sie in den AWS CloudTrail Datensatzinhalten.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
	Aktualisierung von Schlüsseln, einschließlich Regeln darüber, wann Schlüssel geändert werden sollten und wie dies geschehen soll - Umgang mit kompromittierten Schlüsseln - Widerruf Schlüssel, einschließlich How-Schlüssel sollte zurückgezogen oder deaktiviert werden, beispielsweise wenn Schlüssel kompromittiert wurden oder wenn ein Benutzer eine Organisation verlässt (in diesem Fall sollten Schlüssel auch archiviert werden) — Wiederherstellung verloren gegangener oder beschädigter Schlüssel — Sicherung oder Archivierung von Schlüsseln — Zerstörung von Schlüsseln und — Protokollierung und Prüfung von Aktivität		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
	en im Zusammenh ang mit der Schlüssel verwaltung.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
3.1.5(f)	f) Ein Schlüssel verwaltungssystem sollte auf vereinbar ten Standards , Verfahren und sicheren Methoden basieren für: - Generierung von Schlüsseln für verschiedene kryptografische Systeme und verschiedene Anwendungen - Ausstellung und Beschaffung von Zertifikaten für öffentliche Schlüssel - Verteilung von Schlüsseln an vorgesehene Einrichtu ngen, einschließlich der Art und Weise, wie Schlüssel beim Empfang aktiviert werden sollten - Speicherung von Schlüsseln, einschlie ßlich der Art und Weise, wie autorisie rte Benutzer Zugriff auf Schlüssel erhalten - Änderung oder	multi-region-cloudtrail-enabled	AWS CloudTrail zeichnet Aktionen und API-Aufrufe der AWS Management Console auf. Sie können feststellen, welche Benutzer und Konten angerufen wurden AWS, von welcher Quell-IP-Adresse aus die Anrufe getätigt wurden und wann die Anrufe erfolgten. CloudTrail übermittelt Protokolldateien aus allen AWS Regionen an Ihren S3-Bucket , wenn MULTI_REG ION_CLOUD _TRAIL_ENABLED aktiviert ist. Außerdem wird beim AWS Start einer neuen Region derselbe Trail in der neuen Region erstellt. CloudTrail Dadurch erhalten Sie automatis ch Protokolldateien mit API-Aktivitäten für die neue Region.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
	Aktualisierung von Schlüsseln, einschließlich Regeln darüber, wann Schlüssel geändert werden sollten und wie dies geschehen soll - Umgang mit kompromittierten Schlüsseln - Widerruf Schlüssel, einschließlich How-Schlüssel sollte zurückgezogen oder deaktiviert werden, beispielsweise wenn Schlüssel kompromittiert wurden oder wenn ein Benutzer eine Organisation verlässt (in diesem Fall sollten Schlüssel auch archiviert werden) — Wiederherstellung verloren gegangener oder beschädigter Schlüssel — Sicherung oder Archivierung von Schlüsseln — Zerstörung von Schlüsseln und — Protokollierung und Prüfung von Aktivität		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
	en im Zusammenh ang mit der Schlüssel verwaltung.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
3.1.5(f)	f) Ein Schlüssel verwaltungssystem sollte auf vereinbarten Standards , Verfahren und sicheren Methoden basieren für: - Generierung von Schlüsseln für verschiedene kryptografische Systeme und verschiedene Anwendungen - Ausstellung und Beschaffung von Zertifikaten für öffentliche Schlüssel - Verteilung von Schlüsseln an vorgesehene Einrichtungen, einschließlich der Art und Weise, wie Schlüssel beim Empfang aktiviert werden sollten - Speicherung von Schlüsseln, einschließlich der Art und Weise, wie autorisierte Benutzer Zugriff auf Schlüssel erhalten - Änderung oder	elbv-2 acm-certificate-required	Zum Schutz von eventuell vorhandenen sensiblen Daten sowie von Daten während der Übertragung muss die Verschlüsselung für Ihr Elastic Load Balancing aktiviert sein. Verwenden Sie AWS Certificate Manager, um öffentliche und private SSL/TLS-Zertifikate mit AWS Diensten und internen Ressourcen zu verwalten, bereitzustellen und bereitzustellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
	Aktualisierung von Schlüsseln, einschließlich Regeln darüber, wann Schlüssel geändert werden sollten und wie dies geschehen soll - Umgang mit kompromittierten Schlüsseln - Widerruf Schlüssel, einschließlich How-Schlüssel sollte zurückgezogen oder deaktiviert werden, beispielsweise wenn Schlüssel kompromittiert wurden oder wenn ein Benutzer eine Organisation verlässt (in diesem Fall sollten Schlüssel auch archiviert werden) — Wiederherstellung verloren gegangener oder beschädigter Schlüssel — Sicherung oder Archivierung von Schlüsseln — Zerstörung von Schlüsseln und — Protokollierung und Prüfung von Aktivität		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
	en im Zusammenh ang mit der Schlüssel verwaltung.		
3.1.6(a)	a) Das BFI sollte eine Kombination aus automatisierten Tools und manuellen Techniken anwenden, um regelmäßig eine umfassende VA durchzuführen. Für webbasierte externe Systeme sollte der Anwendungsbereich von VA allgemeine Web-Schwachstellen wie SQL-Injection und Cross-Site-Scripting beinhalten.	guardduty-enabled-centralized	Amazon GuardDuty kann mithilfe von Threat Intellige nce Feeds helfen, potenzielle Cybersich erheitsereignisse zu überwachen und zu erkennen. Dazu gehören Listen mit bösartigen IPs und maschinel len Lernmethoden zur Identifizierung unerwarteter, nicht autorisierter und bösartiger Aktivitäten in Ihrer AWS Cloud-Umgebung.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
3.1.6(a)	a) Das BFI sollte eine Kombination aus automatisierten Tools und manuellen Techniken anwenden, um regelmäßig eine umfassende VA durchzuführen. Für webbasierte externe Systeme sollte der Anwendungsbereich von VA allgemeine Web-Schwachstellen wie SQL-Injection und Cross-Site-Scripting beinhalten.	alb-waf-enabled	Stellen Sie sicher, dass AWS WAF auf Elastic Load Balancers (ELB) aktiviert ist, um Webanwendungen zu schützen. Eine WAF trägt zum Schutz Ihrer Webanwend ungen oder APIs vor gängigen Web-Explo its bei. Diese Web-Exploits können sich auf die Verfügbar keit auswirken, die Sicherheit gefährden oder übermäßige Ressourcen in Ihrer Umgebung verbrauch en.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
3.1.6(a)	a) Das BFI sollte eine Kombination aus automatisierten Tools und manuellen Techniken anwenden, um regelmäßig eine umfassende VA durchzuführen. Für webbasierte externe Systeme sollte der Anwendungsbereich von VA allgemeine Web-Schwachstellen wie SQL-Injection und Cross-Site-Scripting beinhalten.	api-gw-associated-with-WAF	AWS Mit WAF können Sie eine Reihe von Regeln (als Web Access Control List (Web ACL) bezeichnet) konfigurieren, die Webanfragen auf der Grundlage von anpassbaren Websicherheitsregeln und -bedingungen, die Sie definieren, zulassen, blockieren oder zählen. Stellen Sie sicher, dass Ihre Amazon-API-Gateway-Stufe mit einer WAF-Web-ACL verknüpft ist, um sie vor böswilligen Angriffen zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
3.1.6(c)	c) Das BFI sollte ein Verfahren zur Behebung der in VA und PT festgestellten Probleme einrichten und anschließend die Abhilfemaßnahmen erneut überprüfen, um sicherzustellen, dass die Lücken vollständig behoben wurden.	vuln-mitigated-accepted(Prozessüberprüfung)	Stellen Sie sicher, dass neu identifizierte Schwachstellen behoben oder als akzeptierte Risiken dokumentiert werden. Schwachstellen sollten entsprechend den Compliance-Anforderungen Ihrer Organisation behoben oder als Risiken akzeptiert werden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
3.1.6(f)	f) Die Sicherheitsabteilung sollte für jede Abteilung/Division Statusmeldungen über die Anzahl der nicht behobenen, kritischen Schwachstellen bereitstellen und für die Geschäftsleitung in regelmäßigen Abständen Pläne zu deren Behebung erstellen.	guardduty-non-archived-findings	Amazon GuardDuty hilft Ihnen dabei, die Auswirkungen eines Vorfalls zu verstehen, indem es die Ergebnisse nach Schweregrad klassifiziert: niedrig, mittel und hoch. Diese Klassifizierungen können Sie zur Festlegung von entsprechenden Strategien und Prioritäten zur Behebung solcher Vorfälle verwenden. Mit dieser Regel können Sie optional daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7) und daysHighSev (Config Default: 1) für nicht archivierte Ergebnisse festlegen, wie es die Richtlinien Ihrer Organisation erfordern.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
3.1.8	Training und Sensibilisierung von Benutzern	security-awareness-program-exists(Prozessüberprüfung)	Etablieren und pflegen Sie ein Programm zur Förderung des Sicherheitsbewusstseins in Ihrer Organisation. Programme zur Förderung des Sicherheitsbewusstseins der Mitarbeiter vermitteln ihnen, wie sie die Organisation vor diversen Sicherheitsverletzungen oder Sicherheitsvorfällen schützen können.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
3.1.10(b)	b) Vertrauliche Informationen wie Systemdokumentation, Anwendungsquellcode und Produktionstransaktionsdaten sollten umfangreicher kontrolliert werden, um sie vor Änderungen zu schützen (z. B. Integritätsprüfungen, kryptografische Hashes). Darüber hinaus sollten Richtlinien die Verbreitung sensibler Informationen, einschließlich Ausdrucken mit solchen Informationen, auf ein Mindestmaß beschränken.	cloud-trail-encryption-enabled	Da sensible Daten vorhanden sein können und um Daten im Ruhezustand zu schützen, sollten Sie sicherstellen, dass die Verschlüsselung für Ihre Trails aktiviert ist. AWS CloudTrail

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
3.1.10(b)	b) Vertrauliche Informationen wie Systemdokumentation, Anwendungsquellcode und Produktionstransaktionsdaten sollten umfassenderen Kontrollen zum Schutz vor Änderungen unterliegen (z. B. Integritätsprüfungen, kryptografische Hashes). Darüber hinaus sollten Richtlinien die Verbreitung sensibler Informationen, einschließlich Ausdrucken mit solchen Informationen, auf ein Mindestmaß beschränken.	cloudwatch-log-group-encrypted	Um sensible Daten im Speicher zu schützen, stellen Sie sicher, dass die Verschlüsselung für Ihre Amazon CloudWatch Log Groups aktiviert ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
3.1.10(b)	b) Vertrauliche Informationen wie Systemdokumentation, Anwendungsquellcode und Produktionstransaktionsdaten sollten umfassenderen Kontrollen zum Schutz vor Änderungen unterliegen (z. B. Integritätsprüfungen, kryptografische Hashes). Darüber hinaus sollten Richtlinien die Verbreitung sensibler Informationen, einschließlich Ausdrucken mit solchen Informationen, auf ein Mindestmaß beschränken.	cloud-trail-log-file-Validierung aktiviert	Verwenden Sie die AWS CloudTrail Protokolldateivalidierung, um die Integrität von Protokollen zu überprüfen. CloudTrail Mithilfe der Protokolldateivalidierung kann festgestellt werden, ob eine Protokolldatei geändert oder gelöscht wurde oder ob sie nach der Übermittlung CloudTrail unverändert geblieben ist. Dieses Feature wurde mit dem Branchenstandard entsprechenden Algorithmen entwickelt: SHA-256 für die Hashfunktion und SHA-256 mit RSA für digitale Signaturen. Das macht es rechnerisch unmöglich, CloudTrail Protokolldateien unbemerkt zu ändern, zu löschen oder zu fälschen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
3.1.10(b)	b) Vertrauliche Informationen wie Systemdokumentation, Anwendungsquellcode und Daten zu Produktionstransaktionen sollten umfassenderen Kontrollen zum Schutz vor Änderungen unterliegen (z. B. Integritätsprüfungen, kryptografische Hashes). Darüber hinaus sollten Richtlinien die Verbreitung sensibler Informationen, einschließlich Ausdrucken mit solchen Informationen, auf ein Mindestmaß beschränken.	efs-encrypted-check	Aktivieren Sie die Verschlüsselung für Ihr Amazon Elastic File System (EFS), um eventuell vorhandene sensible Daten sowie Daten im Ruhezustand zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
3.1.10(b)	b) Bei sensiblen Informationen wie Systemdokumentation, Anwendungsquellcode und Produktionstransaktionsdaten sollten umfassendere Kontrollen zum Schutz vor Änderungen vorgenommen werden (z. B. Integritätsprüfungen, kryptografische Hashes). Darüber hinaus sollten Richtlinien die Verbreitung sensibler Informationen, einschließlich Ausdrucken mit solchen Informationen, auf ein Mindestmaß beschränken.	elasticsearch-encrypted-at-rest	Da sensible Daten vorhanden sein können und um Daten im Ruhezustand zu schützen, sollten Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon OpenSearch Service (OpenSearch Service)-Domains aktiviert ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
3.1.10(b)	b) Vertrauliche Informationen wie Systemdokumentation, Anwendungsquellcode und Produktionstransaktionsdaten sollten umfassenderen Kontrollen zum Schutz vor Änderungen unterliegen (z. B. Integritätsprüfungen, kryptografische Hashes). Darüber hinaus sollten Richtlinien die Verbreitung sensibler Informationen, einschließlich Ausdrucken mit solchen Informationen, auf ein Mindestmaß beschränken.	opensearch-encrypted-at-rest	Da sensible Daten vorhanden sein können und um Daten im Ruhezustand zu schützen, sollten Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon OpenSearch Service-Domains aktiviert ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
3.1.10(b)	b) Vertrauliche Informationen wie Systemdokumentation, Anwendungsquellcode und Produktionstransaktionsdaten sollten umfassenderen Kontrollen zum Schutz vor Änderungen unterliegen (z. B. Integritätsprüfungen, kryptografische Hashes). Darüber hinaus sollten Richtlinien die Verbreitung sensibler Informationen, einschließlich Ausdrucken mit solchen Informationen, auf ein Mindestmaß beschränken.	encrypted-volumes	Aktivieren Sie die Verschlüsselung für Ihre Amazon-Elastic-Block-Store-(Amazon-EBS-)Volumes, um eventuell vorhandene sensible Daten sowie Daten im Ruhezustand zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
3.1.10(b)	b) Bei sensiblen Informationen wie Systemdokumentation, Anwendungsquellcode und Produktionstransaktionsdaten sollten umfassendere Kontrollen zum Schutz vor Änderungen vorgenommen werden (z. B. Integritätsprüfungen, kryptografische Hashes). Darüber hinaus sollten Richtlinien die Verbreitung sensibler Informationen, einschließlich Ausdrucken mit solchen Informationen, auf ein Mindestmaß beschränken.	rds-storage-encrypted	Zum Schutz von Daten im Ruhezustand müssen Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon Relational Database Service (Amazon RDS)-Instances aktiviert ist. Da sensible Daten in Amazon-RDS-Instances gespeichert werden können, sollten Sie die Verschlüsselung von Daten im Ruhezustand aktivieren, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
3.1.10(b)	b) Bei sensiblen Informationen wie Systemdokumentation, Anwendungsquellcode und Produktionstransaktionsdaten sollten umfassendere Kontrollen zum Schutz vor Änderungen vorgenommen werden (z. B. Integritätsprüfungen, kryptografische Hashes). Darüber hinaus sollten Richtlinien die Verbreitung sensibler Informationen, einschließlich Ausdrucken mit solchen Informationen, auf ein Mindestmaß beschränken.	redshift-cluster-configuration-check	Um Daten im Ruhezustand zu schützen, muss die Verschlüsselung für Ihre Amazon-Redshift-Cluster aktiviert sein. Sie müssen auch sicherstellen, dass die erforderlichen Konfigurationen auf Amazon-Redshift-Clustern bereitgestellt werden. Die Prüfungsprotokollierung muss aktiviert sein, um Informationen zu Verbindungen und Benutzeraktivitäten in der Datenbank bereitzustellen. Diese Regel erfordert, dass ein Wert für clusterDbEncrypted (Config Default: TRUE) und LoggingEnabled (Config Default: TRUE) gesetzt ist. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
3.1.10(b)	b) Vertrauliche Informationen wie Systemdokumentation, Anwendungsquellcode und Produktionstransaktionsdaten sollten umfassendere Kontrollen zum Schutz vor Änderungen haben (z. B. Integritätsprüfungen, kryptografische Hashes). Darüber hinaus sollten Richtlinien die Verbreitung sensibler Informationen, einschließlich Ausdrucken mit solchen Informationen, auf ein Mindestmaß beschränken.	s3-fähig bucket-server-side-encryption	Zum Schutz von Daten im Ruhezustand müssen Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon Simple Storage Service (Amazon S3)-Buckets aktiviert ist. Da sensible Daten in Amazon S3 Buckets gespeichert werden können, sollten Sie die Verschlüsselung aktivieren, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
3.1.10(b)	b) Vertrauliche Informationen wie Systemdokumentation, Anwendungsquellcode und Produktionstransaktionsdaten sollten umfangreicher kontrolliert werden, um sie vor Änderungen zu schützen (z. B. Integritätsprüfungen, kryptografische Hashes). Darüber hinaus sollten Richtlinien die Verbreitung sensibler Informationen, einschließlich Ausdrucken mit solchen Informationen, auf ein Mindestmaß beschränken.	sagemaker-endpoint-configuration-kms-schlüsselkonfiguriert	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass die Verschlüsselung mit dem AWS Key Management Service (AWS KMS) für Ihren Endpunkt aktiviert ist. SageMaker Da sensible Daten auf dem SageMaker Endgerät gespeichert werden können, sollten Sie die Verschlüsselung im Ruhezustand aktivieren, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
3.1.10(b)	b) Vertrauliche Informationen wie Systemdokumentation, Anwendungsquellcode und Produktionstransaktionsdaten sollten umfassenderen Kontrollen zum Schutz vor Änderungen unterliegen (z. B. Integritätsprüfungen, kryptografische Hashes). Darüber hinaus sollten Richtlinien die Verbreitung sensibler Informationen, einschließlich Ausdrucken mit solchen Informationen, auf ein Mindestmaß beschränken.	sagemaker-notebook-instance-kms-schlüsselkonfiguriert	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass die Verschlüsselung mit dem AWS Key Management Service (AWS KMS) für Ihr Notebook aktiviert ist. SageMaker Da vertrauliche Daten im SageMaker Notebook gespeichert werden können, sollten Sie die Verschlüsselung im Ruhezustand aktivieren, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
3.1.10(b)	b) Vertrauliche Informationen wie Systemdokumentation, Anwendungsquellcode und Produktionstransaktionsdaten sollten umfassenderen Kontrollen zum Schutz vor Änderungen unterliegen (z. B. Integritätsprüfungen, kryptografische Hashes). Darüber hinaus sollten Richtlinien die Verbreitung sensibler Informationen, einschließlich Ausdrucken mit solchen Informationen, auf ein Mindestmaß beschränken.	sns-encrypted-kms	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass Ihre Amazon Simple Notification Service (Amazon SNS) -Themen mit dem AWS Key Management Service (AWS KMS) verschlüsselt werden müssen. Um eventuell vorhandene sensible Daten im Ruhezustand in veröffentlichten Nachrichten zu schützen, muss die Verschlüsselung von Daten im Ruhezustand aktiviert sein.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
3.1.10(b)	b) Vertrauliche Informationen wie Systemdokumentation, Anwendungsquellcode und Daten zu Produktionstransaktionen sollten umfassenderen Kontrollen zum Schutz vor Änderungen unterliegen (z. B. Integritätsprüfungen, kryptografische Hashes). Darüber hinaus sollten Richtlinien die Verbreitung sensibler Informationen, einschließlich Ausdrucken mit solchen Informationen, auf ein Mindestmaß beschränken.	ec2- ebs-encryption-by-default	Zum Schutz von Daten im Ruhezustand müssen Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon Elastic Block Store (Amazon EBS)-Volumes aktiviert ist. Da sensible Daten in diesen Volumes gespeichert werden können, sollten Sie die Verschlüsselung von Daten im Ruhezustand aktivieren, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
3.1.10(b)	b) Vertrauliche Informationen wie Systemdokumentation, Anwendungsquellcode und Daten zu Produktionstransaktionen sollten umfassenderen Kontrollen zum Schutz vor Änderungen unterliegen (z. B. Integritätsprüfungen, kryptografische Hashes). Darüber hinaus sollten Richtlinien die Verbreitung sensibler Informationen, einschließlich Ausdrucken mit solchen Informationen, auf ein Mindestmaß beschränken.	rds-snapshot-encrypted	Stellen Sie sicher, dass die Verschlüsselung für Ihre Amazon Relational Database Service (Amazon RDS)-Snapshots aktiviert ist. Da sensible Daten auch im Ruhezustand vorhanden sein können, sollten Sie die Verschlüsselung von Daten im Ruhezustand aktivieren, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
3.1.10(b)	b) Bei sensiblen Informationen wie Systemdokumentation, Anwendungsquellcode und Produktionstransaktionsdaten sollten umfassendere Kontrollen zum Schutz vor Änderungen vorgenommen werden (z. B. Integritätsprüfungen, kryptografische Hashes). Darüber hinaus sollten Richtlinien die Verbreitung sensibler Informationen, einschließlich Ausdrucken mit solchen Informationen, auf ein Mindestmaß beschränken.	s-3 default-encryption-kms	Stellen Sie sicher, dass die Verschlüsselung für Ihre Amazon Simple Storage Service (Amazon S3)-Buckets aktiviert ist. Da sensible Daten in einem Amazon S3 Bucket gespeichert werden können, sollten Sie die Verschlüsselung im Ruhezustand aktivieren, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
3.1.10(b)	b) Vertrauliche Informationen wie Systemdokumentation, Anwendungsquellcode und Produktionstransaktionsdaten sollten umfassenderen Kontrollen zum Schutz vor Änderungen unterliegen (z. B. Integritätsprüfungen, kryptografische Hashes). Darüber hinaus sollten Richtlinien die Verbreitung sensibler Informationen, einschließlich Ausdrucken mit solchen Informationen, auf ein Mindestmaß beschränken.	api-gw-cache-enabled-und verschlüsselt	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass die Verschlüsselung für den Cache Ihrer API-Gateway-Stufe aktiviert ist. Da für die API-Methode sensible Daten erfasst werden können, sollten Sie die Verschlüsselung von Daten im Ruhezustand aktivieren, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
3.1.10(b)	b) Vertrauliche Informationen wie Systemdokumentation, Anwendungsquellcode und Produktionstransaktionsdaten sollten umfassenderen Kontrollen zum Schutz vor Änderungen unterliegen (z. B. Integritätsprüfungen, kryptografische Hashes). Darüber hinaus sollten Richtlinien die Verbreitung sensibler Informationen, einschließlich Ausdrucken mit solchen Informationen, auf ein Mindestmaß beschränken.	dynamodb-table-encrypted-kms	Stellen Sie sicher, dass die Verschlüsselung für Ihre Amazon-DynamoDB-Tabellen aktiviert ist. Um eventuell vorhandene sensible Daten im Ruhezustand in diesen Tabellen zu schützen, müssen Sie die Verschlüsselung von Daten im Ruhezustand aktivieren. Standardmäßig werden DynamoDB-Tabellen mit einem AWS eigenen Kundenhauptschlüssel (CMK) verschlüselt.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
3.1.10(b)	b) Vertrauliche Informationen wie Systemdokumentation, Anwendungsquellcode und Produktionstransaktionsdaten sollten umfassenderen Kontrollen zum Schutz vor Änderungen unterliegen (z. B. Integritätsprüfungen, kryptografische Hashes). Darüber hinaus sollten Richtlinien die Verbreitung sensibler Informationen, einschließlich Ausdrucken mit solchen Informationen, auf ein Mindestmaß beschränken.	redshift-cluster-kms-enabled	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass die Verschlüsselung mit AWS Key Management Service (AWS KMS) für Ihren Amazon Redshift Redshift-Cluster aktiviert ist. Um eventuell vorhandene sensible Daten im Ruhezustand in Redshift-Clustern zu schützen, muss die Verschlüsselung von Daten im Ruhezustand aktiviert sein.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
3.1.10(b)	b) Vertrauliche Informationen wie Systemdokumentation, Anwendungsquellcode und Produktionstransaktionsdaten sollten umfassenderen Kontrollen zum Schutz vor Änderungen unterliegen (z. B. Integritätsprüfungen, kryptografische Hashes). Darüber hinaus sollten Richtlinien die Verbreitung sensibler Informationen, einschließlich Ausdrucken mit solchen Informationen, auf ein Mindestmaß beschränken.	secretsmanager-using-cmk	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass die Verschlüsselung mit dem AWS Key Management Service (AWS KMS) für AWS Secrets Manager aktiviert ist. Aktivieren Sie die Verschlüsselung von Daten im Ruhezustand, um eventuell vorhandene sensible Daten im Ruhezustand im Secrets Manager zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
3.2.1(h)	h) Um die mit Änderungen verbundenen Risiken zu minimieren, BFIs sollten Sie vor der Änderung Backups der betroffen en Systeme oder Anwendungen erstellen. BFIs sollte einen Rollback-Plan erstellen, um zu einer früheren Version des Systems oder der Anwendung zurückzukehren, falls während oder nach der Bereitstellung ein Problem auftritt.	db-instance-backup-enabled	Die Sicherung sfunktion von Amazon RDS erstellt Sicherung en Ihrer Datenbank en und Transakti onsprotokolle. Amazon RDS erstellt einen Snapshot für das Speichervolume Ihrer DB-Instance, sodass die gesamte DB-Instance gesichert wird. Sie können im System spezifische Aufbewahrungsfrist en festlegen, um Ihre Ausfallsicherheits anforderungen zu erfüllen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
3.2.1(h)	h) Um die mit Änderungen verbundenen Risiken zu minimieren, BFIs sollten vor der Änderung Backups der betroffenen Systeme oder Anwendungen durchgeführt werden. BFIs sollte einen Rollback-Plan erstellen, um zu einer früheren Version des Systems oder der Anwendung zurückzukehren, falls während oder nach der Bereitstellung ein Problem auftritt.	dynamodb-pitr-enabled	Aktivieren Sie diese Regel, um zu überprüfen, ob die Informationen gesichert wurden. Es verwaltet auch die Backups, indem es sicherstellt, dass die point-in-time Wiederherstellung in Amazon DynamoDB aktiviert ist. Bei der Wiederherstellung werden fortlaufende Backups Ihrer Tabelle für die letzten 35 Tage gespeichert.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
3.2.1(h)	h) Um die mit Änderungen verbundenen Risiken zu minimieren, BFIs sollten Sie vor der Änderung Backups der betroffenen Systeme oder Anwendungen durchführen. BFIs sollte einen Rollback-Plan erstellen, um zu einer früheren Version des Systems oder der Anwendung zurückzukehren, falls während oder nach der Bereitstellung ein Problem auftritt.	ebs-optimized-instance	Eine optimierte Instance im Amazon Elastic Block Store (Amazon EBS) bietet zusätzliche, dedizierte Kapazität für Amazon-EBS-I/O-Vorgänge. Diese Optimierung bietet die beste Leistung für Ihr EBS-Volume, indem Konflikte zwischen Amazon-EBS-I/O und anderem Datenverkehr von Ihrer Instance minimiert werden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
3.2.1(h)	h) Um die mit Änderungen verbundenen Risiken zu minimieren, BFIs sollten vor der Änderung Backups der betroffenen Systeme oder Anwendungen durchgeführt werden. BFIs sollte einen Rollback-Plan erstellen, um zu einer früheren Version des Systems oder der Anwendung zurückzukehren, falls während oder nach der Bereitstellung ein Problem auftritt.	elasticache-redis-cluster-automatic-Backup-Check	Wenn automatische Backups aktiviert sind, ElastiCache erstellt Amazon täglich ein Backup des Clusters. Die Sicherung kann für eine von Ihrer Organisation festgelegte Anzahl von Tagen aufbewahrt werden. Automatische Backups schützen vor Datenverlust. Bei einem Ausfall können Sie einen neuen Cluster erstellen, der Ihre Daten aus dem aktuellen Backup wiederherstellt.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
3.2.1(h)	h) Um die mit Änderungen verbundenen Risiken zu minimieren, BFIs sollten Sie vor der Änderung Backups der betroffen en Systeme oder Anwendungen durchführen. BFIs sollte einen Rollback-Plan erstellen, um zu einer früheren Version des Systems oder der Anwendung zurückzukehren, falls während oder nach der Bereitstellung ein Problem auftritt.	s3- bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) unterstützt die Aufrechterhaltung einer angemesse nen Kapazität und Verfügbarkeit. CRR ermöglicht das automatische, asynchrone Kopieren von Objekten in Amazon S3 Buckets, um die Datenverf ügbarkeit sicherzus tellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
3.2.1(h)	h) Um die mit Änderungen verbundenen Risiken zu minimieren, BFIs sollten vor der Änderung Backups der betroffenen Systeme oder Anwendungen durchgeführt werden. BFIs sollte einen Rollback-Plan erstellen, um zu einer früheren Version des Systems oder der Anwendung zurückzukehren, falls während oder nach der Bereitstellung ein Problem auftritt.	s3- bucket-versioning-enabled	Die Versionsv erwaltung von Amazon Simple Storage Service (Amazon S3)-Bucke ts hilft dabei, mehrere Varianten eines Objekts im selben Amazon-S3-Bucket zu speichern. Verwenden Sie die Versionsv erwaltung, um sämtliche Versionen aller Objekte in Ihrem Amazon-S3-Bucket zu speichern , abzurufen oder wiederherzustellen . Mit der Versionsv erwaltung können Sie Versionen sowohl nach unbeabsic htigten Benutzera ktionen als auch nach Anwendungsfehlern problemlos wiederher stellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
3.2.1(h)	h) Um die mit Änderungen verbundenen Risiken zu minimieren, BFIs sollten vor der Änderung Backups der betroffenen Systeme oder Anwendungen durchgeführt werden. BFIs sollte einen Rollback-Plan erstellen, um zu einer früheren Version des Systems oder der Anwendung zurückzukehren, falls während oder nach der Bereitstellung ein Problem auftritt.	dynamodb-in-backup-plan	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon DynamoDB-Tabellen Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
3.2.1(h)	h) Um die mit Änderungen verbundenen Risiken zu minimieren, BFIs sollten vor der Änderung Backups der betroffenen Systeme oder Anwendungen durchgeführt werden. BFIs sollte einen Rollback-Plan erstellen, um zu einer früheren Version des Systems oder der Anwendung zurückzukehren, falls während oder nach der Bereitstellung ein Problem auftritt.	ebs-in-backup-plan	Stellen Sie zur Unterstützung der Datensicherungspro zesse sicher, dass Ihre Amazon Elastic Block Store (Amazon EBS) -Volumes Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwaltet er Backup-Service mit einer richtlini enbasierten Backup-Lösung. Diese Lösung vereinfac ht Ihr Sicherung smanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforde rungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
3.2.1(h)	h) Um die mit Änderungen verbundenen Risiken zu minimieren, BFIs sollten vor der Änderung Backups der betroffenen Systeme oder Anwendungen durchgeführt werden. BFIs sollte einen Rollback-Plan erstellen, um zu einer früheren Version des Systems oder der Anwendung zurückzukehren, falls während oder nach der Bereitstellung ein Problem auftritt.	efs-in-backup-plan	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon Elastic File System (Amazon EFS) -Dateisysteme Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
3.2.1(h)	h) Um die mit Änderungen verbundenen Risiken zu minimieren, BFIs sollten vor der Änderung Backups der betroffenen Systeme oder Anwendungen durchgeführt werden. BFIs sollte einen Rollback-Plan erstellen, um zu einer früheren Version des Systems oder der Anwendung zurückzukehren, falls während oder nach der Bereitstellung ein Problem auftritt.	rds-in-backup-plan	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon Relational Database Service (Amazon RDS) -Instances Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
3.2.1(h)	h) Um die mit Änderungen verbundenen Risiken zu minimieren, BFIs sollten vor der Änderung Backups der betroffenen Systeme oder Anwendungen durchgeführt werden. BFIs sollte einen Rollback-Plan erstellen, um zu einer früheren Version des Systems oder der Anwendung zurückzukehren, falls während oder nach der Bereitstellung ein Problem auftritt.	redshift-backup-enabled	Stellen Sie zur Unterstützung der Datensicherungsprozesse sicher, dass Ihre Amazon-Redshift-Cluster über automatisierte Snapshots verfügen. Wenn automatisierte Snapshots für einen Cluster aktiviert sind, erstellt Redshift in regelmäßigen Abständen Snapshots dieses Clusters. Standardmäßig erstellt Redshift alle acht Stunden oder alle 5 GB einen Snapshot für jeden Knoten mit Datenänderungen oder je nachdem, was zuerst eintritt.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
3.2.1(k)	k) Prüfungs- und Sicherheitsprotokolle sind nützliche Informationen, die Untersuchungen und die Behebung von Problemen erleichtern. Das BFI sollte sicherstellen, dass die Protokollierungseinrichtung in der Lage ist, während des Migrationsprozess stattgefundene Aktivitäten aufzuzeichnen.	api-gw-execution-logging-aktiviert	Die API-Gateway-Protokollierung zeigt detaillierte Ansichten der Benutzer, die auf die API zugegriffen haben, und wie diese Benutzer auf die API zugegriffen haben. Diese Insights ermöglichen die Einsicht in Benutzeraktivitäten.
3.2.1(k)	k) Prüfungs- und Sicherheitsprotokolle sind nützliche Informationen, die Untersuchungen und die Behebung von Problemen erleichtern. Das BFI sollte sicherstellen, dass die Protokollierungseinrichtung in der Lage ist, während des Migrationsprozess stattgefundene Aktivitäten aufzuzeichnen.	cloud-trail-cloud-watch-logs-aktiviert	Verwenden Sie Amazon CloudWatch , um Protokollereignisaktivitäten zentral zu sammeln und zu verwalten. Die Aufnahme von AWS CloudTrail Daten liefert Einzelheiten zu den API-Aufrufaktivitäten in Ihrem AWS-Konto.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
3.2.1(k)	k) Prüfungs- und Sicherheitsprotokolle sind nützliche Informationen, die Untersuchungen und die Behebung von Problemen erleichtern. Das BFI sollte sicherstellen, dass die Protokollierungseinrichtung in der Lage ist, während des Migrationsprozess stattgefundene Aktivitäten aufzuzeichnen.	cloudtrail-enabled	AWS CloudTrail kann bei der Nichtabstreitbarkeit helfen, indem Aktionen und API-Aufrufe der AWS Management Console aufgezeichnet werden. Sie können die Benutzer und die Benutzer AWS-Konten , die einen AWS Dienst aufgerufen haben, die Quell-IP-Adresse, über die die Aufrufe generiert wurden, und den Zeitpunkt der Anrufe identifizieren. Einzelheiten zu den erfassten Daten finden Sie in den AWS CloudTrail Datensatzinhalten.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
3.2.1(k)	k) Prüfungs- und Sicherheitsprotokolle sind nützliche Informationen, die Untersuchungen und die Behebung von Problemen erleichtern. Das BFI sollte sicherstellen, dass die Protokollierungseinrichtung in der Lage ist, während des Migrationsprozess stattgefundene Aktivitäten aufzuzeichnen.	cloudtrail-s3-dataevents-enabled	Die Erfassung von Simple Storage Service (Amazon S3)-Datenereignissen unterstützt die Erkennung von ungewöhnlichen Aktivitäten. Zu den Details gehören AWS-Konto Informationen über den Zugriff auf einen Amazon S3 S3-Bucket, die IP-Adresse und die Uhrzeit des Ereignisses.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
3.2.1(k)	k) Prüfungs- und Sicherheitsprotokolle sind nützliche Informationen, die Untersuchungen und die Behebung von Problemen erleichtern. Das BFI sollte sicherstellen, dass die Protokollierungseinrichtung in der Lage ist, während des Migrationsprozess stattgefundene Aktivitäten aufzuzeichnen.	elb-logging-enabled	Die Elastic-Load-Balancing-Aktivität ist ein zentraler Kommunikationspunkt innerhalb einer Umgebung. Stellen Sie sicher, dass die ELB-Protokollierung aktiviert ist. Die gesammelten Daten enthalten detaillierte Informationen zu Anfragen, die an den ELB gesendet wurden. Jedes Protokoll enthält Informationen wie die Zeit, zu der die Anforderung einging, die Client-IP-Adresse, Latenzen, Anforderungspfade und Serverantworten.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
3.2.1(k)	k) Prüfungs- und Sicherheitsprotokolle sind nützliche Informationen, die Untersuchungen und die Behebung von Problemen erleichtern. Das BFI sollte sicherstellen, dass die Protokollierungseinrichtung in der Lage ist, während des Migrationsprozess stattgefundene Aktivitäten aufzuzeichnen.	multi-region-cloudtrail-enabled	AWS CloudTrail zeichnet Aktionen und API-Aufrufe der AWS Management Console auf. Sie können feststellen, welche Benutzer und Konten angerufen wurden AWS, von welcher Quell-IP-Adresse aus die Anrufe getätigt wurden und wann die Anrufe erfolgten. CloudTrail übermittelt Protokolldateien aus allen AWS Regionen an Ihren S3-Bucket, wenn MULTI_REGION_CLOUD_TRAIL_ENABLED aktiviert ist. Außerdem wird beim AWS Start einer neuen Region derselbe Trail in der neuen Region erstellt. CloudTrail Dadurch erhalten Sie automatisch Protokolldateien mit API-Aktivitäten für die neue Region.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
3.2.1(k)	k) Prüfungs- und Sicherheitsprotokolle sind nützliche Informationen, die Untersuchungen und die Behebung von Problemen erleichtern. Das BFI sollte sicherstellen, dass die Protokollierungseinrichtung in der Lage ist, während des Migrationsprozess stattgefundene Aktivitäten aufzuzeichnen.	s-3 bucket-logging-enabled	Die Amazon Simple Storage Service (Amazon S3)-Serverzugriffsprotokollierung bietet eine Methode zur Überwachung des Netzwerks im Hinblick auf potenzielle Cybersicherheitsereignisse. Die Ereignisse werden überwacht, indem detaillierte Aufzeichnungen über die Anfragen erfasst werden, die an einen Amazon-S3-Bucket gestellt wurden. Jeder Zugriffsprotokolleintrag enthält Details zu einer einzelnen Zugriffsanfrage. Zu den Details gehören Anforderer, Bucket-Name, Anforderungszeit, Anforderungsaktion, Antwortstatus und Fehlercode, falls relevant.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
3.2.1(k)	k) Prüfungs- und Sicherheitsprotokolle sind nützliche Informationen, die Untersuchungen und die Behebung von Problemen erleichtern. Das BFI sollte sicherstellen, dass die Protokollierungseinrichtung in der Lage ist, während des Migrationsprozess stattgefundene Aktivitäten aufzuzeichnen.	vpc-flow-logs-enabled	VPC-Flow-Protokolle erfassen detaillierte Informationsdatensätze über den IP-Datenverkehr, der zu und von Netzwerkschnittstellen in Ihrer Amazon Virtual Private Cloud (Amazon VPC) fließt. Standardmäßig enthalten Flow-Protokolldatensätze Werte für die verschiedenen Komponenten des IP-Flows, einschließlich Quelle, Ziel und Protokoll.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
3.2.1(k)	k) Prüfungs- und Sicherheitsprotokolle sind nützliche Informationen, die Untersuchungen und die Behebung von Problemen erleichtern. Das BFI sollte sicherstellen, dass die Protokollierungseinrichtung in der Lage ist, während des Migrationsprozess stattgefundene Aktivitäten aufzuzeichnen.	cw-loggroup-retention-period-überprüfen	Stellen Sie sicher, dass die Ereignisprotokolldaten für Ihre Protokollgruppen über eine Mindestdauer aufbewahrt werden, um die Fehlerbehebung und forensische Untersuchungen zu unterstützen. Fehlende frühere Ereignisprotokolldaten erschweren die Rekonstruierung und Identifizierung potenziell schädlicher Ereignisse.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
3.2.1(k)	k) Prüfungs- und Sicherheitsprotokolle sind nützliche Informationen, die Untersuchungen und die Behebung von Problemen erleichtern. Das BFI sollte sicherstellen, dass die Protokollierungseinrichtung in der Lage ist, während des Migrationsprozess stattgefundene Aktivitäten aufzuzeichnen.	rds-logging-enabled	Um die Protokollierung und Überwachung in Ihrer Umgebung zu erleichtern, stellen Sie sicher, dass die Amazon Relational Database Service (Amazon RDS)-Protokollierung aktiviert ist. Mit der Amazon-RDS-Protokollierung können Sie Ereignisse wie Verbindungen, Verbindungsabbrüche, Abfragen oder abgefragte Tabellen erfassen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
3.2.1(k)	k) Prüfungs- und Sicherheitsprotokolle sind nützliche Informationen, die Untersuchungen und die Behebung von Problemen erleichtern. Das BFI sollte sicherstellen, dass die Protokollierungseinrichtung in der Lage ist, während des Migrationsprozess stattgefundene Aktivitäten aufzuzeichnen.	wafv2-logging-enabled	Um Ihnen bei der Protokollierung und Überwachung in Ihrer Umgebung zu helfen, aktivieren Sie die AWS WAF (V2) -Protokollierung im regionalen und globalen Web. ACLs AWS Die WAF-Protokollierung bietet detaillierte Informationen über den Datenverkehr, der von Ihrer Web-ACL analysiert wird. In den Protokollen werden die Uhrzeit aufgezeichnet, zu der die AWS WAF die Anfrage von Ihrer AWS Ressource erhalten hat, Informationen zu der Anfrage und eine Aktion für die Regel, der jede Anfrage entsprach.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
3.2.1(k)	k) Prüfungs- und Sicherheitsprotokolle sind nützliche Informationen, die Untersuchungen und die Behebung von Problemen erleichtern. Das BFI sollte sicherstellen, dass die Protokollierungseinrichtung in der Lage ist, während des Migrationsprozess stattgefundene Aktivitäten aufzuzeichnen.	redshift-cluster-configuration-check	Um Daten im Ruhezustand zu schützen, muss die Verschlüsselung für Ihre Amazon-Redshift-Cluster aktiviert sein. Sie müssen auch sicherstellen, dass die erforderlichen Konfigurationen auf Amazon-Redshift-Clustern bereitgestellt werden. Die Prüfungsprotokollierung muss aktiviert sein, um Informationen zu Verbindungen und Benutzeraktivitäten in der Datenbank bereitzustellen. Diese Regel erfordert, dass ein Wert für clusterDbEncrypted (Config Default: TRUE) und LoggingEnabled (Config Default: TRUE) gesetzt ist. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
3.2.1(k)	k) Prüfungs- und Sicherheitsprotokolle sind nützliche Informationen, die Untersuchungen und die Behebung von Problemen erleichtern. Das BFI sollte sicherstellen, dass die Protokollierungseinrichtung in der Lage ist, während des Migrationsprozess stattgefundene Aktivitäten aufzuzeichnen.	elasticsearch-logs-to-cloudwatch	Stellen Sie sicher, dass für Amazon OpenSearch Service-Domains Fehlerprotokolle aktiviert und zur Aufbewahrung und Beantwortung an Amazon CloudWatch Logs gestreamt werden. Domain-Fehlerprotokolle sind bei Sicherheits- und Zugriffsprüfungen sowie bei der Diagnose von Verfügbarkeitsproblemen nützlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
3.2.1(k)	k) Prüfungs- und Sicherheitsprotokolle sind nützliche Informationen, die Untersuchungen und die Behebung von Problemen erleichtern. Das BFI sollte sicherstellen, dass die Protokollierungseinrichtung in der Lage ist, während des Migrationsprozess stattgefundene Aktivitäten aufzuzeichnen.	opensearch-logs-to-cloudwatch	Stellen Sie sicher, dass für Amazon OpenSearch Service-Domains Fehlerprotokolle aktiviert und zur Aufbewahrung und Beantwortung an Amazon CloudWatch Logs gestreamt werden. OpenSearch Service-Fehlerprotokolle können bei Sicherheits- und Zugriffsprüfungen helfen und bei der Diagnose von Verfügbarkeitsproblemen helfen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
3.2.3(a)	a) Entwickeln und implementieren Sie Verfahren zur Prävention, Erkennung, Analyse und Reaktion auf Informationssicherheitsvorfälle.	guardduty-enabled-centralized	Amazon GuardDuty kann mithilfe von Threat Intelligence Feeds helfen, potenzielle Cybersicherheitsereignisse zu überwachen und zu erkennen. Dazu gehören Listen mit bösartigen IPs und maschinellen Lernmethoden zur Identifizierung unerwarteter, nicht autorisierter und bösartiger Aktivitäten in Ihrer AWS Cloud-Umgebung.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
3.2.3(a)	a) Entwickeln und implementieren Sie Verfahren zur Prävention, Erkennung, Analyse und Reaktion auf Informationssicherheitsvorfälle.	securityhub-enabled	AWS Security Hub hilft bei der Überwachung von unbefugtem Personal, Verbindungen, Geräten und Software. AWS Security Hub aggregiert, organisiert und priorisiert die Sicherheitswarnungen oder Ergebnisse mehrerer Dienste. AWS Einige dieser Dienste sind Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer und AWS Firewall Manager sowie AWS Partnerlösungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
3.3.1(a)	a) Berücksichtigen Sie wichtige Faktoren im Zusammenhang mit der Aufrechterhaltung einer hohen Systemverfügbarkeit, einer angemessenen Kapazität, einer zuverlässigen Leistung, einer schnellen Reaktionszeit und Skalierbarkeit als Teil des Systemdesigns.	dynamodb-autoscaling-enabled	Amazon DynamoDB Auto Scaling verwendet den AWS Application Auto Scaling-Service, um die bereitgestellte Durchsatzkapazität so anzupassen, dass sie automatisch auf tatsächliche Verkehrsmuster reagiert. Auf diese Weise kann eine Tabelle oder ein globaler sekundärer Index die bereitgestellte Lese-/Schreibkapazität erhöhen, um plötzliche Erhöhungen des Datenverkehrs ohne Drosselung zu bewältigen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
3.3.1(a)	a) Berücksichtigen Sie wichtige Faktoren im Zusammenhang mit der Aufrechterhaltung einer hohen Systemverfügbarkeit, einer angemessenen Kapazität, einer zuverlässigen Leistung, einer schnellen Reaktionszeit und Skalierbarkeit als Teil des Systemdesigns.	dynamodb-pitr-enabled	Aktivieren Sie diese Regel, um zu überprüfen, ob die Informationen gesichert wurden. Es verwaltet auch die Backups, indem es sicherstellt, dass die point-in-time Wiederherstellung in Amazon DynamoDB aktiviert ist. Bei der Wiederherstellung werden fortlaufende Backups Ihrer Tabelle für die letzten 35 Tage gespeichert.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
3.3.1(a)	a) Berücksichtigen Sie wichtige Faktoren im Zusammenhang mit der Aufrechterhaltung einer hohen Systemverfügbarkeit, einer angemessenen Kapazität, einer zuverlässigen Leistung, einer schnellen Reaktionszeit und Skalierbarkeit als Teil des Systemdesigns.	ebs-optimized-instance	Eine optimierte Instance im Amazon Elastic Block Store (Amazon EBS) bietet zusätzliche, dedizierte Kapazität für Amazon-EBS-I/O-Vorgänge. Diese Optimierung bietet die beste Leistung für Ihr EBS-Volume, indem Konflikte zwischen Amazon-EBS-I/O und anderem Datenverkehr von Ihrer Instance minimiert werden.
3.3.1(a)	a) Berücksichtigen Sie wichtige Faktoren im Zusammenhang mit der Aufrechterhaltung einer hohen Systemverfügbarkeit, einer angemessenen Kapazität, einer zuverlässigen Leistung, einer schnellen Reaktionszeit und Skalierbarkeit als Teil des Systemdesigns.	elb-deletion-protection-enabled	Diese Regel sorgt dafür, dass der Löschschutz für Elastic Load Balancing aktiviert ist. Verwenden Sie diese Funktion, um zu verhindern, dass Ihr Load Balancer versehentlich oder böswillig gelöscht wird, was zum Verlust der Verfügbarkeit Ihrer Anwendungen führen kann.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
3.3.1(a)	a) Berücksichtigen Sie wichtige Faktoren im Zusammenhang mit der Aufrechterhaltung einer hohen Systemverfügbarkeit, einer angemessenen Kapazität, einer zuverlässigen Leistung, einer schnellen Reaktionszeit und Skalierbarkeit als Teil des Systemdesigns.	rds-multi-az-support	Die Multi-AZ-Unterstützung in Amazon Relational Database Service (Amazon RDS) bietet eine verbesserte Verfügbarkeit und Beständigkeit von Datenbank-Instances. Wenn Sie eine Multi-AZ-Datenbank-Instance bereitstellen, erstellt Amazon RDS automatisch eine primäre Datenbank-Instance und repliziert die Daten synchron auf eine Standby-Instance in einer anderen Availability Zone. Jede Availability Zone läuft auf einer eigenen, physisch getrennten, unabhängigen Infrastruktur und ist auf eine hohe Verfügbarkeit ausgelegt. Im Falle eines Infrastrukturausfalls führt Amazon RDS einen automatis

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
			chen Failover zum Standby-Modus durch, sodass Sie den Datenbankbetrieb wieder aufnehmen können, sobald der Failover abgeschlo ssen ist.
3.3.1(a)	a) Berücksichtigen Sie wichtige Faktoren im Zusammenhang mit der Aufrechte rhaltung einer hohen Systemverfügbarkei t, einer angemesse nen Kapazität, einer zuverläss igen Leistung, einer schnellen Reaktions zeit und Skalierba rkeit als Teil des Systemdesigns.	s-3 bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) unterstützt die Aufrechterhaltung einer angemesse nen Kapazität und Verfügbarkeit. CRR ermöglicht das automatische, asynchrone Kopieren von Objekten in Amazon S3 Buckets, um die Datenverf ügbarkeit sicherzus tellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
3.3.1(a)	a) Berücksichtigen Sie wichtige Faktoren im Zusammenhang mit der Aufrechterhaltung einer hohen Systemverfügbarkeit, einer angemessenen Kapazität, einer zuverlässigen Leistung, einer schnellen Reaktionszeit und Skalierbarkeit als Teil des Systemdesigns.	s-3 bucket-versioning-enabled	Die Versionsverwaltung von Amazon Simple Storage Service (Amazon S3)-Buckets hilft dabei, mehrere Varianten eines Objekts im selben Amazon-S3-Bucket zu speichern. Verwenden Sie die Versionsverwaltung, um sämtliche Versionen aller Objekte in Ihrem Amazon-S3-Bucket zu speichern, abzurufen oder wiederherzustellen. Mit der Versionsverwaltung können Sie Versionen sowohl nach unbeabsichtigten Benutzeraktionen als auch nach Anwendungsfehlern problemlos wiederherstellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
3.3.1(a)	a) Berücksichtigen Sie wichtige Faktoren im Zusammenhang mit der Aufrechterhaltung einer hohen Systemverfügbarkeit, einer angemessenen Kapazität, einer zuverlässigen Leistung, einer schnellen Reaktionszeit und Skalierbarkeit als Teil des Systemdesigns.	vpc-vpn-2-tunnels-up	Redundante Site-to-Site VPN-Tunnel können implementiert werden, um die Anforderungen an die Ausfallsicherheit zu erfüllen. Es verwendet zwei Tunnel, um die Konnektivität sicherzustellen, falls eine der Site-to-Site VPN-Verbindungen nicht verfügbar ist. Um sich vor einem Verbindungsverlust zu schützen, können Sie für den Fall, dass Ihr Kunden-Gateway nicht verfügbar ist, eine zweite Site-to-Site VPN-Verbindung zu Ihrer Amazon Virtual Private Cloud (Amazon VPC) und Ihrem Virtual Private Gateway einrichten, indem Sie ein zweites Kunden-Gateway verwenden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
3.3.1(a)	a) Berücksichtigen Sie wichtige Faktoren im Zusammenhang mit der Aufrechterhaltung einer hohen Systemverfügbarkeit, einer angemessenen Kapazität, einer zuverlässigen Leistung, einer schnellen Reaktionszeit und Skalierbarkeit als Teil des Systemdesigns.	elb-cross-zone-load-Balancing aktiviert	Aktivieren Sie zonenübergreifendes Load Balancing für Ihre Elastic Load Balancer (ELBs), um eine angemessene Kapazität und Verfügbarkeit aufrechtzuerhalten. Zonenübergreifendes Load Balancing reduziert die Notwendigkeit, die gleiche Anzahl von Instances in jeder aktivierten Availability Zone aufrechtzuerhalten. Es verbessert auch die Fähigkeit Ihrer Anwendung, den Verlust einer oder mehrerer Instances zu bewältigen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
3.3.1(a)	a) Berücksichtigen Sie wichtige Faktoren im Zusammenhang mit der Aufrechte rhaltung einer hohen Systemverfügbarkei t, einer angemesse nen Kapazität, einer zuverläss igen Leistung, einer schnellen Reaktions zeit und Skalierba rkeit als Teil des Systemdesigns.	rds-instance-deletion-protection-aktiviert	Stellen Sie sicher, dass Amazon Relational Database Service (Amazon RDS)-Instances den Löschschutz aktiviert haben. Verwenden Sie den Löschschu tz, um zu verhindern, dass Ihre Amazon-RD S-Instances versehent lich oder böswillig gelöscht werden, was zum Verlust der Verfügbarkeit Ihrer Anwendungen führen kann.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
3.3.1(a)	a) Berücksichtigen Sie wichtige Faktoren im Zusammenhang mit der Aufrechte rhaltung einer hohen Systemverfügbarkei t, einer angemesse nen Kapazität, einer zuverläss igen Leistung, einer schnellen Reaktions zeit und Skalierba rkeit als Teil des Systemdesigns.	autoscaling-group-elb-healthcheck-erforderlich	Die Elastic Load Balancer (ELB) - Zustandsprüfungen für Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling Scaling-G ruppen unterstützen die Aufrechterhaltung einer angemesse nen Kapazität und Verfügbarkeit. Der Load Balancer sendet regelmäßig Pings, versucht Verbindun gen herzustellen oder sendet Anfragen, um den Zustand der EC2 Amazon-Instances in einer Gruppe mit auto-scal ing zu testen. Wenn eine Instance nicht zurückmeldet, wird der Traffic an eine neue EC2 Amazon-In stance gesendet.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
3.3.1(a)	a) Berücksichtigen Sie wichtige Faktoren im Zusammenhang mit der Aufrechterhaltung einer hohen Systemverfügbarkeit, einer angemessenen Kapazität, einer zuverlässigen Leistung, einer schnellen Reaktionszeit und Skalierbarkeit als Teil des Systemdesigns.	dynamodb-throughput-limit-check	Aktivieren Sie diese Regel, um sicherzustellen, dass die bereitgestellte Durchsatzkapazität in Ihren Amazon-DynamoDB-Tabellen überprüft wird. Dies ist der Umfang der Lese- und Schreibaktivitäten, der von den jeweiligen Tabellen unterstützt werden kann. DynamoDB verwendet diese Informationen für das Reservieren ausreichender Systemressourcen, um Ihren Durchsatzanforderungen gerecht zu werden. Diese Regel generiert eine Warnung, wenn sich der Durchsatz dem Höchstlimit für ein Kundenkonto nähert. Mit dieser Regel können Sie optional die Parameter RCUThreshold Kontoprozentsatz

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
			(Konfigurationsstandard: 80) und WCUThreshold Kontoprozentsatz (Konfigurationsstandard: 80) festlegen. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.
3.3.1(a)	a) Berücksichtigen Sie wichtige Faktoren im Zusammenhang mit der Aufrechterhaltung einer hohen Systemverfügbarkeit, einer angemessenen Kapazität, einer zuverlässigen Leistung, einer schnellen Reaktionszeit und Skalierbarkeit als Teil des Systemdesigns.	lambda-concurrency-check	Diese Regel stellt sicher, dass die Höchst- und Untergrenzen für die Gleichzeitigkeit einer Lambda-Funktion festgelegt werden. Dies kann Sie beim Baselining für die Anzahl der Anforderungen unterstützen, die Ihre Funktion zu einem bestimmten Zeitpunkt verarbeitet.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
3.4(a)(b)(c)(f)(j)	a) Stellen Sie sicher, dass Aufzeichnungen über Benutzerzugriffe eindeutig identifiziert und zu Prüfungs- und Kontrollzwecken protokolliert werden; b) Sorgen Sie dafür, dass die Rechenschaftspflicht und die Identifizierung von unbefugten Zugriffen dokumentiert werden; c) Ermöglichen Sie die Prüfungsprotokollierung von Systemaktivitäten, die von privilegierten Benutzern ausgeführt werden; f) Stellen Sie sicher, dass die Ereignisprotokollierung die Grundlage für automatisierte Überwachungssysteme bildet, die konsolidierte Berichte und Warnmeldungen zur Systemsicherheit generieren können.	api-gw-execution-logging-aktiviert	Die API-Gateway-Protokollierung zeigt detaillierte Ansichten der Benutzer, die auf die API zugegriffen haben, und wie diese Benutzer auf die API zugegriffen haben. Diese Insights ermöglichen die Einsicht in Benutzeraktivitäten.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
3.4(a)(b)(c)(f)(j)	a) Stellen Sie sicher, dass Aufzeichnungen über Benutzerzugriffe eindeutig identifiziert und zu Prüfungs- und Kontrollzwecken protokolliert werden; b) Sorgen Sie dafür, dass die Rechenschaftspflicht und die Identifizierung von unbefugten Zugriffen dokumentiert werden; c) Ermöglichen Sie die Prüfungsprotokollierung von Systemaktivitäten, die von privilegierten Benutzern ausgeführt werden; f) Stellen Sie sicher, dass die Ereignisprotokollierung die Grundlage für automatisierte Überwachungssysteme bildet, die konsolidierte Berichte und Warnmeldungen zur Systemsicherheit generieren können.	cloud-trail-cloud-watch-logs-aktiviert	Verwenden Sie Amazon CloudWatch , um Protokoll ereignisaktivitäten zentral zu sammeln und zu verwalten. Die Aufnahme von AWS CloudTrail Daten liefert Einzelheiten zu den API-Aufrufaktivitäten in Ihrem AWS-Konto.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
3.4(a)(b)(c)(f)(j)	a) Stellen Sie sicher, dass Aufzeichnungen über Benutzerzugriffe eindeutig identifiz iert und zu Prüfungs- und Kontrollzwecken protokolliert werden; b) Sorgen Sie dafür, dass die Rechensch aftspflicht und die Identifizierung von unbefugten Zugriffen dokumentiert werden; c) Ermöglichen Sie die Prüfungsp rotokollierung von Systemaktivitäten, die von privilegierten Benutzern ausgeführ t werden; f) Stellen Sie sicher, dass die Ereignisprotokolli erung die Grundlage für automatisierte Überwachungssystem e bildet, die konsolidi erte Berichte und Warnmeldungen zur Systemsicherheit generieren können.	cloudtrail-enabled	AWS CloudTrail kann bei der Nichtabst reitbarkeit helfen, indem Aktionen und API-Aufrufe der AWS Management Console aufgezeic hnet werden. Sie können die Benutzer und die Benutzer AWS-Konten , die einen AWS Dienst aufgerufen haben, die Quell-IP-Adresse, über die die Aufrufe generiert wurden, und den Zeitpunkt der Anrufe identifiz ieren. Einzelheiten zu den erfassten Daten finden Sie in den AWS CloudTrail Datensatzinhalten.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
3.4(a)(b)(c)(f)(j)	a) Stellen Sie sicher, dass Aufzeichnungen über Benutzerzugriffe eindeutig identifiziert und zu Prüfungs- und Kontrollzwecken protokolliert werden; b) Sorgen Sie dafür, dass die Rechenschaftspflicht und die Identifizierung von unbefugten Zugriffen dokumentiert werden; c) Ermöglichen Sie die Prüfungsprotokollierung von Systemaktivitäten, die von privilegierten Benutzern ausgeführt werden; f) Stellen Sie sicher, dass die Ereignisprotokollierung die Grundlage für automatisierte Überwachungssysteme bildet, die konsolidierte Berichte und Warnmeldungen zur Systemsicherheit generieren können.	cloudtrail-s3-dataevents-enabled	Die Erfassung von Simple Storage Service (Amazon S3)-Datenereignissen unterstützt die Erkennung von ungewöhnlichen Aktivitäten. Zu den Details gehören AWS-Konto Informationen über den Zugriff auf einen Amazon S3 S3-Bucket, die IP-Adresse und die Uhrzeit des Ereignisses.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
3.4(a)(b)(c)(f)(j)	a) Stellen Sie sicher, dass Aufzeichnungen über Benutzerzugriffe eindeutig identifiziert und zu Prüfungs- und Kontrollzwecken protokolliert werden; b) Sorgen Sie dafür, dass die Rechenschaftspflicht und die Identifizierung von unbefugten Zugriffen dokumentiert werden; c) Ermöglichen Sie die Prüfungsprotokollierung von Systemaktivitäten, die von privilegierten Benutzern ausgeführt werden; f) Stellen Sie sicher, dass die Ereignisprotokollierung die Grundlage für automatisierte Überwachungssysteme bildet, die konsolidierte Berichte und Warnmeldungen zur Systemsicherheit generieren können.	cloud-trail-log-file-Validierung aktiviert	Verwenden Sie die AWS CloudTrail Protokolldateivalidierung, um die Integrität von Protokollen zu überprüfen. CloudTrail Mithilfe der Protokolldateivalidierung kann festgestellt werden, ob eine Protokolldatei geändert oder gelöscht wurde oder ob sie nach der Übermittlung CloudTrail unverändert geblieben ist. Dieses Feature wurde mit dem Branchenstandard entsprechenden Algorithmen entwickelt: SHA-256 für die Hashfunktion und SHA-256 mit RSA für digitale Signaturen. Das macht es rechnerisch unmöglich, CloudTrail Protokolldateien unbemerkt zu ändern, zu löschen oder zu fälschen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
3.4(a)(b)(c)(f)(j)	a) Stellen Sie sicher, dass Aufzeichnungen über Benutzerzugriffe eindeutig identifiziert und zu Prüfungs- und Kontrollzwecken protokolliert werden; b) Sorgen Sie dafür, dass die Rechenschaftspflicht und die Identifizierung von unbefugten Zugriffen dokumentiert werden; c) Ermöglichen Sie die Prüfungsprotokollierung von Systemaktivitäten, die von privilegierten Benutzern ausgeführt werden; f) Stellen Sie sicher, dass die Ereignisprotokollierung die Grundlage für automatisierte Überwachungssysteme bildet, die konsolidierte Berichte und Warnmeldungen zur Systemsicherheit generieren können.	elb-logging-enabled	Die Elastic-Load-Balancing-Aktivität ist ein zentraler Kommunikationspunkt innerhalb einer Umgebung. Stellen Sie sicher, dass die ELB-Protokollierung aktiviert ist. Die gesammelten Daten enthalten detaillierte Informationen zu Anfragen, die an den ELB gesendet wurden. Jedes Protokoll enthält Informationen wie die Zeit, zu der die Anforderung einging, die Client-IP-Adresse, Latenzen, Anforderungspfade und Serverantworten.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
3.4(a)(b)(c)(f)(j)	a) Stellen Sie sicher, dass Aufzeichnungen über Benutzerzugriffe eindeutig identifiz iert und zu Prüfungs- und Kontrollzwecken protokolliert werden; b) Sorgen Sie dafür, dass die Rechensch aftspflicht und die Identifizierung von unbefugten Zugriffen dokumentiert werden; c) Ermöglichen Sie die Prüfungsp rotokollierung von Systemaktivitäten, die von privilegierten Benutzern ausgeführ t werden; f) Stellen Sie sicher, dass die Ereignisprotokolli erung die Grundlage für automatisierte Überwachungssystem e bildet, die konsolidi erte Berichte und Warnmeldungen zur Systemsicherheit generieren können.	multi-region-cloudtrail-enabled	AWS CloudTrail zeichnet Aktionen und API-Aufrufe der AWS Management Console auf. Sie können feststellen, welche Benutzer und Konten angerufen wurden AWS, von welcher Quell-IP-Adresse aus die Anrufe getätigt wurden und wann die Anrufe erfolgten. CloudTrail übermittelt Protokolldateien aus allen AWS Regionen an Ihren S3-Bucket , wenn MULTI_REG ION_CLOUD _TRAIL_ENABLED aktiviert ist. Außerdem wird beim AWS Start einer neuen Region derselbe Trail in der neuen Region erstellt. CloudTrail Dadurch erhalten Sie automatis ch Protokolldateien mit API-Aktivitäten für die neue Region.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
3.4(a)(b)(c)(f)(j)	a) Stellen Sie sicher, dass Aufzeichnungen über Benutzerzugriffe eindeutig identifiz iert und zu Prüfungs- und Kontrollzwecken protokolliert werden; b) Sorgen Sie dafür, dass die Rechensch aftspflicht und die Identifizierung von unbefugten Zugriffen dokumentiert werden; c) Ermöglichen Sie die Prüfungsp rotokollierung von Systemaktivitäten, die von privilegierten Benutzern ausgeführ t werden; f) Stellen Sie sicher, dass die Ereignisprotokolli erung die Grundlage für automatisierte Überwachungssystem e bildet, die konsolidi erte Berichte und Warnmeldungen zur Systemsicherheit generieren können.	s-3 bucket-logging-enabled	Die Amazon Simple Storage Service (Amazon S3)-Serverzugriffs protokollierung bietet eine Methode zur Überwachu ng des Netzwerks im Hinblick auf potenzielle Cybersich erheitsereignisse. Die Ereignisse werden überwacht, indem detaillierte Aufzeichn ungen über die Anfragen erfasst werden, die an einen Amazon-S3-Bucket gestellt wurden. Jeder Zugriffsprotokolle intrag enthält Details zu einer einzelnen Zugriffsanfrage. Zu den Details gehören Anforderer, Bucket-Name, Anforderu ngszeit, Anforderu ngsaktion, Antwortst atus und Fehlercode, falls relevant.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
3.4(a)(b)(c)(f)(j)	a) Stellen Sie sicher, dass Aufzeichnungen über Benutzerzugriffe eindeutig identifiziert und zu Prüfungs- und Kontrollzwecken protokolliert werden; b) Sorgen Sie dafür, dass die Rechenschaftspflicht und die Identifizierung von unbefugten Zugriffen dokumentiert werden; c) Ermöglichen Sie die Prüfungsprotokollierung von Systemaktivitäten, die von privilegierten Benutzern ausgeführt werden; f) Stellen Sie sicher, dass die Ereignisprotokollierung die Grundlage für automatisierte Überwachungssysteme bildet, die konsolidierte Berichte und Warnmeldungen zur Systemsicherheit generieren können.	vpc-flow-logs-enabled	VPC-Flow-Protokolle erfassen detaillierte Informationsdatensätze über den IP-Datenverkehr, der zu und von Netzwerkschnittstellen in Ihrer Amazon Virtual Private Cloud (Amazon VPC) fließt. Standardmäßig enthalten Flow-Protokolldatensätze Werte für die verschiedenen Komponenten des IP-Flows, einschließlich Quelle, Ziel und Protokoll.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
3.4(a)(b)(c)(f)(j)	a) Stellen Sie sicher, dass Aufzeichnungen über Benutzerzugriffe eindeutig identifiziert und zu Prüfungs- und Kontrollzwecken protokolliert werden; b) Sorgen Sie dafür, dass die Rechenschaftspflicht und die Identifizierung von unbefugten Zugriffen dokumentiert werden; c) Ermöglichen Sie die Prüfungsprotokollierung von Systemaktivitäten, die von privilegierten Benutzern ausgeführt werden; f) Stellen Sie sicher, dass die Ereignisprotokollierung die Grundlage für automatisierte Überwachungssysteme bildet, die konsolidierte Berichte und Warnmeldungen zur Systemsicherheit generieren können.	rds-logging-enabled	Um die Protokollierung und Überwachung in Ihrer Umgebung zu erleichtern, stellen Sie sicher, dass die Amazon Relational Database Service (Amazon RDS)-Protokollierung aktiviert ist. Mit der Amazon-RDS-Protokollierung können Sie Ereignisse wie Verbindungen, Verbindungsabbrüche, Abfragen oder abgefragte Tabellen erfassen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
3.4(a)(b)(c)(f)(j)	a) Stellen Sie sicher, dass Aufzeichnungen über Benutzerzugriffe eindeutig identifiziert und zu Prüfungs- und Kontrollzwecken protokolliert werden; b) Sorgen Sie dafür, dass die Rechenschaftspflicht und die Identifizierung von unbefugten Zugriffen dokumentiert werden; c) Ermöglichen Sie die Prüfungsprotokollierung von Systemaktivitäten, die von privilegierten Benutzern ausgeführt werden; f) Stellen Sie sicher, dass die Ereignisprotokollierung die Grundlage für automatisierte Überwachungssysteme bildet, die konsolidierte Berichte und Warnmeldungen zur Systemsicherheit generieren können.	wafv2-logging-enabled	Um die Protokollierung und Überwachung in Ihrer Umgebung zu erleichtern, aktivieren Sie die AWS WAF (V2) -Protokollierung im regionalen und globalen Web ACLs. AWS Die WAF-Protokollierung bietet detaillierte Informationen über den Datenverkehr, der von Ihrer Web-ACL analysiert wird. In den Protokollen werden die Uhrzeit aufgezeichnet, zu der die AWS WAF die Anfrage von Ihrer AWS Ressource erhalten hat, Informationen zu der Anfrage und eine Aktion für die Regel, der jede Anfrage entsprach.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
3.4(a)(b)(c)(f)(j)	a) Stellen Sie sicher, dass Aufzeichnungen über Benutzerzugriffe eindeutig identifiziert und zu Prüfungs- und Kontrollzwecken protokolliert werden; b) Sorgen Sie dafür, dass die Rechenschaftspflicht und die Identifizierung von unbefugten Zugriffen dokumentiert werden; c) Ermöglichen Sie die Prüfungsprotokollierung von Systemaktivitäten, die von privilegierten Benutzern ausgeführt werden; f) Stellen Sie sicher, dass die Ereignisprotokollierung die Grundlage für automatisierte Überwachungssysteme bildet, die konsolidierte Berichte und Warnmeldungen zur Systemsicherheit generieren können.	redshift-cluster-configuration-check	Um Daten im Ruhezustand zu schützen, muss die Verschlüsselung für Ihre Amazon-Redshift-Cluster aktiviert sein. Sie müssen auch sicherstellen, dass die erforderlichen Konfigurationen auf Amazon-Redshift-Clustern bereitgestellt werden. Die Prüfungsprotokollierung muss aktiviert sein, um Informationen zu Verbindungen und Benutzeraktivitäten in der Datenbank bereitzustellen. Diese Regel erfordert, dass ein Wert für clusterDbEncrypted (Config Default: TRUE) und LoggingEnabled (Config Default: TRUE) gesetzt ist. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
3.4(a)(b)(c)(f)(j)	a) Stellen Sie sicher, dass Aufzeichnungen über Benutzerzugriffe eindeutig identifiziert und zu Prüfungs- und Kontrollzwecken protokolliert werden; b) Sorgen Sie dafür, dass die Rechenschaftspflicht und die Identifizierung von unbefugten Zugriffen dokumentiert werden; c) Ermöglichen Sie die Prüfungsprotokollierung von Systemaktivitäten, die von privilegierten Benutzern ausgeführt werden; f) Stellen Sie sicher, dass die Ereignisprotokollierung die Grundlage für automatisierte Überwachungssysteme bildet, die konsolidierte Berichte und Warnmeldungen zur Systemsicherheit generieren können.	elasticsearch-logs-to-cloudwatch	Stellen Sie sicher, dass für Amazon OpenSearch Service-Domains Fehlerprotokolle aktiviert und zur Aufbewahrung und Beantwortung an Amazon CloudWatch Logs gestreamt werden. Domain-Fehlerprotokolle sind bei Sicherheits- und Zugriffsprüfungen sowie bei der Diagnose von Verfügbarkeitsproblemen nützlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
3.4(a)(b)(c)(f)(j)	a) Stellen Sie sicher, dass Aufzeichnungen über Benutzerzugriffe eindeutig identifiziert und zu Prüfungs- und Kontrollzwecken protokolliert werden; b) Sorgen Sie dafür, dass die Rechenschaftspflicht und die Identifizierung von unbefugten Zugriffen dokumentiert werden; c) Ermöglichen Sie die Prüfungsprotokollierung von Systemaktivitäten, die von privilegierten Benutzern ausgeführt werden; f) Stellen Sie sicher, dass die Ereignisprotokollierung die Grundlage für automatisierte Überwachungssysteme bildet, die konsolidierte Berichte und Warnmeldungen zur Systemsicherheit generieren können.	opensearch-logs-to-cloudwatch	Stellen Sie sicher, dass für Amazon OpenSearch Service-Domains Fehlerprotokolle aktiviert und zur Aufbewahrung und Beantwortung an Amazon CloudWatch Logs gestreamt werden. OpenSearch Service-Fehlerprotokolle können bei Sicherheits- und Zugriffsprüfungen helfen und bei der Diagnose von Verfügbarkeitsproblemen helfen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
3.4(f)	f) Stellen Sie sicher, dass eine angemessene Protokollierung und Überwachung erfolgt, damit Aktionen aufgezeichnet und erkannt werden, die für die Informationssicherheit relevant sind oder sich darauf auswirken können.	securityhub-enabled	AWS Security Hub hilft bei der Überwachung von unbefugtem Personal, Verbindungen, Geräten und Software. AWS Security Hub aggregiert, organisiert und priorisiert die Sicherheitswarnungen oder Ergebnisse mehrerer Dienste. AWS Einige dieser Dienste sind Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer und AWS Firewall Manager sowie AWS Partnerlösungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
3.4(g)	g) Stellen Sie sicher, dass die Ereignisprotokolle gegebenenfalls Folgendes enthalten : IDs - Benutzer - Systemaktivitäten - Datum, Uhrzeit und Einzelheiten wichtiger Ereignisse, z. B. An- und Abmeldung - Geräteidentität oder Standort, falls möglich, und System-ID - Aufzeichnungen über erfolgreiche und abgelehnte Systemzugriffsversuche - Aufzeichnungen über erfolgreiche und abgelehnte Daten und andere Ressourcenzugriffsversuche - Änderungen der Systemkonfiguration - Verwendung von Rechten - Verwendung von Systemdienstprogrammen und Anwendungen - Zugriffsarten und Art des Zugriffs -	cloudtrail-s3-dataevents-enabled	Die Erfassung von Simple Storage Service (Amazon S3)-Datenereignissen unterstützt die Erkennung von ungewöhnlichen Aktivitäten. Zu den Details gehören AWS-Konto Informationen über den Zugriff auf einen Amazon S3 S3-Bucket, die IP-Adresse und die Uhrzeit des Ereignisses.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
	Netzwerkadressen und Protokolle - Ausgelöste Alarme durch die Zugriffsk ontrolle System und - Aufzeichnungen von Transaktionen, die von Benutzern in Anwendungen ausgeführt wurden, und Online-Ku ndentransaktionen		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
3.4(g)	g) Stellen Sie sicher, dass die Ereignisprotokolle gegebenenfalls Folgendes enthalten : IDs - Benutzer - Systemaktivitäten - Datum, Uhrzeit und Einzelheiten wichtiger Ereignisse, z. B. An- und Abmeldung - Geräteidentität oder Standort, falls möglich, und System-ID - Aufzeichnungen über erfolgreiche und abgelehnte Systemzugriffsversuche - Aufzeichnungen über erfolgreiche und abgelehnte Daten und andere Ressourcenzugriffsversuche - Änderungen der Systemkonfiguration - Verwendung von Rechten - Verwendung von Systemdienstprogrammen und Anwendungen - Zugriffsarten und Art des Zugriffs -	multi-region-cloudtrail-enabled	AWS CloudTrail zeichnet Aktionen und API-Aufrufe der AWS Management Console auf. Sie können feststellen, welche Benutzer und Konten angerufen wurden AWS, von welcher Quell-IP-Adresse aus die Anrufe getätigt wurden und wann die Anrufe erfolgten. CloudTrail übermittelt Protokolldateien aus allen AWS Regionen an Ihren S3-Bucket , wenn MULTI_REGION_CLOUD_TRAIL_ENABLED aktiviert ist. Außerdem wird beim AWS Start einer neuen Region derselbe Trail in der neuen Region erstellt. CloudTrail Dadurch erhalten Sie automatisch Protokolldateien mit API-Aktivitäten für die neue Region.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
	Netzwerkadressen und Protokolle - Ausgelöste Alarme durch die Zugriffsk ontrolle System und - Aufzeichnungen von Transaktionen, die von Benutzern in Anwendungen ausgeführt wurden, und Online-Ku ndentransaktionen		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
3.4(g)	g) Stellen Sie sicher, dass die Ereignisprotokolle gegebenenfalls Folgendes enthalten : IDs - Benutzer - Systemaktivitäten - Datum, Uhrzeit und Einzelheiten wichtiger Ereignisse, z. B. An- und Abmeldung - Geräteidentität oder Standort, falls möglich, und System-ID - Aufzeichnungen über erfolgreiche und abgelehnte Systemzugriffsversuche - Aufzeichnungen über erfolgreiche und abgelehnte Daten und andere Ressourcenzugriffsversuche - Änderungen der Systemkonfiguration - Verwendung von Rechten - Verwendung von Systemdienstprogrammen und Anwendungen - Zugriffsarten und Art des Zugriffs -	s-3 bucket-logging-enabled	Die Amazon Simple Storage Service (Amazon S3)-Serverzugriffsprotokollierung bietet eine Methode zur Überwachung des Netzwerks im Hinblick auf potenzielle Cybersicherheitsereignisse. Die Ereignisse werden überwacht, indem detaillierte Aufzeichnungen über die Anfragen erfasst werden, die an einen Amazon-S3-Bucket gestellt wurden. Jeder Zugriffsprotokolleintrag enthält Details zu einer einzelnen Zugriffsanfrage. Zu den Details gehören Anforderer, Bucket-Name, Anforderungszeit, Anforderungsaktion, Antwortstatus und Fehlercode, falls relevant.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
	Netzwerkadressen und Protokolle - Ausgelöste Alarme durch die Zugriffsk ontrolle System und - Aufzeichnungen von Transaktionen, die von Benutzern in Anwendungen ausgeführt wurden, und Online-Ku ndentransaktionen		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
3.4(g)	g) Stellen Sie sicher, dass die Ereignisprotokolle gegebenenfalls Folgendes enthalten : IDs - Benutzer - Systemaktivitäten - Datum, Uhrzeit und Einzelheiten wichtiger Ereignisse, z. B. An- und Abmeldung - Geräteidentität oder Standort, falls möglich, und System-ID - Aufzeichnungen über erfolgreiche und abgelehnte Systemzugriffsversuche - Aufzeichnungen über erfolgreiche und abgelehnte Daten und andere Ressourcenzugriffsversuche - Änderungen der Systemkonfiguration - Verwendung von Rechten - Verwendung von Systemdienstprogrammen und Anwendungen - Zugriffsarten und Art des Zugriffs -	rds-logging-enabled	Um die Protokollierung und Überwachung in Ihrer Umgebung zu erleichtern, stellen Sie sicher, dass die Amazon Relational Database Service (Amazon RDS)-Protokollierung aktiviert ist. Mit der Amazon-RDS-Protokollierung können Sie Ereignisse wie Verbindungen, Verbindungsabbrüche, Abfragen oder abgefragte Tabellen erfassen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
	Netzwerkadressen und Protokolle - Ausgelöste Alarme durch die Zugriffsk ontrolle System und - Aufzeichnungen von Transaktionen, die von Benutzern in Anwendungen ausgeführt wurden, und Online-Ku ndentransaktionen		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
3.4(g)	g) Stellen Sie sicher, dass die Ereignisprotokolle gegebenenfalls Folgendes enthalten : IDs - Benutzer - Systemaktivitäten - Datum, Uhrzeit und Einzelheiten wichtiger Ereignisse, z. B. An- und Abmeldung - Geräteidentität oder Standort, falls möglich, und System-ID - Aufzeichnungen über erfolgreiche und abgelehnte Systemzugriffsversuche - Aufzeichnungen über erfolgreiche und abgelehnte Daten und andere Ressourcenzugriffsversuche - Änderungen der Systemkonfiguration - Verwendung von Rechten - Verwendung von Systemdienstprogrammen und Anwendungen - Zugriffsarten und Art des Zugriffs -	redshift-cluster-configuration-check	Um Daten im Ruhezustand zu schützen, muss die Verschlüsselung für Ihre Amazon-Redshift-Cluster aktiviert sein. Sie müssen auch sicherstellen, dass die erforderlichen Konfigurationen auf Amazon-Redshift-Clustern bereitgestellt werden. Die Prüfungsprotokollierung muss aktiviert sein, um Informationen zu Verbindungen und Benutzeraktivitäten in der Datenbank bereitzustellen. Diese Regel erfordert, dass ein Wert für clusterDbEncrypted (Config Default: TRUE) und LoggingEnabled (Config Default: TRUE) gesetzt ist. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
	Netzwerkadressen und Protokolle - Ausgelöste Alarme durch die Zugriffsk ontrolle System und - Aufzeichnungen von Transaktionen, die von Benutzern in Anwendungen ausgeführt wurden, und Online-Ku ndentransaktionen		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
3.4(g)	g) Stellen Sie sicher, dass die Ereignisprotokolle gegebenenfalls Folgendes enthalten : IDs - Benutzer - Systemaktivitäten - Datum, Uhrzeit und Einzelheiten wichtiger Ereignisse, z. B. An- und Abmeldung - Geräteidentität oder Standort, falls möglich, und System-ID - Aufzeichnungen über erfolgreiche und abgelehnte Systemzugriffsversuche - Aufzeichnungen über erfolgreiche und abgelehnte Daten und andere Ressourcenzugriffsversuche - Änderungen der Systemkonfiguration - Verwendung von Rechten - Verwendung von Systemdienstprogrammen und Anwendungen - Zugriffsarten und Art des Zugriffs -	wafv2-logging-enabled	Um die Protokollierung und Überwachung in Ihrer Umgebung zu erleichtern, aktivieren Sie die AWS WAF (V2) -Protokollierung im regionalen und globalen Web ACLs. AWS Die WAF-Protokollierung bietet detaillierte Informationen über den Datenverkehr, der von Ihrer Web-ACL analysiert wird. In den Protokollen werden die Uhrzeit aufgezeichnet, zu der die AWS WAF die Anfrage von Ihrer AWS Ressource erhalten hat, Informationen zu der Anfrage und eine Aktion für die Regel, der jede Anfrage entsprach.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
	Netzwerkadressen und Protokolle - Ausgelöste Alarme durch die Zugriffsk ontrolle System und - Aufzeichnungen von Transaktionen, die von Benutzern in Anwendungen ausgeführt wurden, und Online-Ku ndentransaktionen		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
3.4(g)	g) Stellen Sie sicher, dass die Ereignisprotokolle gegebenenfalls Folgendes enthalten : IDs - Benutzer - Systemaktivitäten - Datum, Uhrzeit und Einzelheiten wichtiger Ereignisse, z. B. An- und Abmeldung - Geräteidentität oder Standort, falls möglich, und System-ID - Aufzeichnungen über erfolgreiche und abgelehnte Systemzugriffsversuche - Aufzeichnungen über erfolgreiche und abgelehnte Daten und andere Ressourcenzugriffsversuche - Änderungen der Systemkonfiguration - Verwendung von Rechten - Verwendung von Systemdienstprogrammen und Anwendungen - Zugriffsarten und Art des Zugriffs -	elb-logging-enabled	Die Elastic-Load-Balancing-Aktivität ist ein zentraler Kommunikationspunkt innerhalb einer Umgebung. Stellen Sie sicher, dass die ELB-Protokollierung aktiviert ist. Die gesammelten Daten enthalten detaillierte Informationen zu Anfragen, die an den ELB gesendet wurden. Jedes Protokoll enthält Informationen wie die Zeit, zu der die Anforderung einging, die Client-IP-Adresse, Latenzen, Anforderungspfade und Serverantworten.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
	Netzwerkadressen und Protokolle - Ausgelöste Alarme durch die Zugriffsk ontrolle System und - Aufzeichnungen von Transaktionen, die von Benutzern in Anwendungen ausgeführt wurden, und Online-Ku ndentransaktionen		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
3.4(g)	g) Stellen Sie sicher, dass die Ereignisprotokolle gegebenenfalls Folgendes enthalten : IDs - Benutzer - Systemaktivitäten - Datum, Uhrzeit und Einzelheiten wichtiger Ereignisse, z. B. An- und Abmeldung - Geräteidentität oder Standort, falls möglich, und System-ID - Aufzeichnungen über erfolgreiche und abgelehnte Systemzugriffsversuche - Aufzeichnungen über erfolgreiche und abgelehnte Daten und andere Ressourcenzugriffsversuche - Änderungen der Systemkonfiguration - Verwendung von Rechten - Verwendung von Systemdienstprogrammen und Anwendungen - Zugriffsarten und Art des Zugriffs -	api-gw-execution-logging-aktiviert	Die API-Gateway-Protokollierung zeigt detaillierte Ansichten der Benutzer, die auf die API zugegriffen haben, und wie diese Benutzer auf die API zugegriffen haben. Diese Insights ermöglichen die Einsicht in Benutzeraktivitäten.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
	Netzwerkadressen und Protokolle - Ausgelöste Alarme durch die Zugriffsk ontrolle System und - Aufzeichnungen von Transaktionen, die von Benutzern in Anwendungen ausgeführt wurden, und Online-Ku ndentransaktionen		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
3.4(g)	g) Stellen Sie sicher, dass die Ereignisprotokolle gegebenenfalls Folgendes enthalten : IDs - Benutzer - Systemaktivitäten - Datum, Uhrzeit und Einzelheiten wichtiger Ereignisse, z. B. An- und Abmeldung - Geräteidentität oder Standort, falls möglich, und System-ID - Aufzeichnungen über erfolgreiche und abgelehnte Systemzugriffsversuche - Aufzeichnungen über erfolgreiche und abgelehnte Daten und andere Ressourcenzugriffsversuche - Änderungen der Systemkonfiguration - Verwendung von Rechten - Verwendung von Systemdienstprogrammen und Anwendungen - Zugriffsarten und Art des Zugriffs -	cloud-trail-cloud-watch-Logs aktiviert	Verwenden Sie Amazon CloudWatch , um Protokoll ereignisaktivitäten zentral zu sammeln und zu verwalten. Die Aufnahme von AWS CloudTrail Daten liefert Einzelheiten zu den API-Aufrufaktivitäten in Ihrem AWS-Konto.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
	Netzwerkadressen und Protokolle - Ausgelöste Alarme durch die Zugriffsk ontrolle System und - Aufzeichnungen von Transaktionen, die von Benutzern in Anwendungen ausgeführt wurden, und Online-Ku ndentransaktionen		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
3.4(g)	g) Stellen Sie sicher, dass die Ereignisprotokolle gegebenenfalls Folgendes enthalten : IDs - Benutzer - Systemaktivitäten - Datum, Uhrzeit und Einzelheiten wichtiger Ereignisse, z. B. An- und Abmeldung - Geräteidentität oder Standort, falls möglich, und System-ID - Aufzeichnungen über erfolgreiche und abgelehnte Systemzugriffsversuche - Aufzeichnungen über erfolgreiche und abgelehnte Daten und andere Ressourcenzugriffsversuche - Änderungen der Systemkonfiguration - Verwendung von Rechten - Verwendung von Systemdienstprogrammen und Anwendungen - Zugriffsarten und Art des Zugriffs -	cloudtrail-enabled	AWS CloudTrail kann durch die Aufzeichnung von Aktionen und API-Aufrufen der AWS Management Console bei der Nichtabstreitbarkeit helfen. Sie können die Benutzer und die Benutzer AWS-Konten , die einen AWS Dienst aufgerufen haben, die Quell-IP-Adresse, über die die Aufrufe generiert wurden, und den Zeitpunkt der Anrufe identifizieren. Einzelheiten zu den erfassten Daten finden Sie in den AWS CloudTrail Datensatzinhalten.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
	Netzwerkadressen und Protokolle - Ausgelöste Alarme durch die Zugriffsk ontrolle System und - Aufzeichnungen von Transaktionen, die von Benutzern in Anwendungen ausgeführt wurden, und Online-Ku ndentransaktionen		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
3.4(g)	g) Stellen Sie sicher, dass die Ereignisprotokolle gegebenenfalls Folgendes enthalten : IDs - Benutzer - Systemaktivitäten - Datum, Uhrzeit und Einzelheiten wichtiger Ereignisse, z. B. An- und Abmeldung - Geräteidentität oder Standort, falls möglich, und System-ID - Aufzeichnungen über erfolgreiche und abgelehnte Systemzugriffsversuche - Aufzeichnungen über erfolgreiche und abgelehnte Daten und andere Ressourcenzugriffsversuche - Änderungen der Systemkonfiguration - Verwendung von Rechten - Verwendung von Systemdienstprogrammen und Anwendungen - Zugriffsarten und Art des Zugriffs -	vpc-flow-logs-enabled	VPC-Flow-Protokolle erfassen detaillierte Informationsdatensätze über den IP-Datenverkehr, der zu und von Netzwerkschnittstellen in Ihrer Amazon Virtual Private Cloud (Amazon VPC) fließt. Standardmäßig enthalten Flow-Protokolldatensätze Werte für die verschiedenen Komponenten des IP-Flows, einschließlich Quelle, Ziel und Protokoll.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
	Netzwerkadressen und Protokolle - Ausgelöste Alarme durch die Zugriffsk ontrolle System und - Aufzeichnungen von Transaktionen, die von Benutzern in Anwendungen ausgeführt wurden, und Online-Ku ndentransaktionen		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
3.4(g)	g) Stellen Sie sicher, dass die Ereignisprotokolle gegebenenfalls Folgendes enthalten : IDs - Benutzer - Systemaktivitäten - Datum, Uhrzeit und Einzelheiten wichtiger Ereignisse, z. B. An- und Abmeldung - Geräteidentität oder Standort, falls möglich, und System-ID - Aufzeichnungen über erfolgreiche und abgelehnte Systemzugriffsversuche - Aufzeichnungen über erfolgreiche und abgelehnte Daten und andere Ressourcenzugriffsversuche - Änderungen der Systemkonfiguration - Verwendung von Rechten - Verwendung von Systemdienstprogrammen und Anwendungen - Zugriffsarten und Art des Zugriffs -	cw-loggroup-retention-period-überprüfen	Stellen Sie sicher, dass die Ereignisprotokolldaten für Ihre Protokollgruppen über eine Mindestdauer aufbewahrt werden, um die Fehlerbehebung und forensische Untersuchungen zu unterstützen. Fehlende frühere Ereignisprotokolldaten erschweren die Rekonstruierung und Identifizierung potenziell schädlicher Ereignisse.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
	Netzwerkadressen und Protokolle - Ausgelöste Alarme durch die Zugriffsk ontrolle System und - Aufzeichnungen von Transaktionen, die von Benutzern in Anwendungen ausgeführt wurden, und Online-Ku ndentransaktionen		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
3.4(g)	g) Stellen Sie sicher, dass die Ereignisprotokolle gegebenenfalls Folgendes enthalten : IDs - Benutzer - Systemaktivitäten - Datum, Uhrzeit und Einzelheiten wichtiger Ereignisse, z. B. An- und Abmeldung - Geräteidentität oder Standort, falls möglich, und System-ID - Aufzeichnungen über erfolgreiche und abgelehnte Systemzugriffsversuche - Aufzeichnungen über erfolgreiche und abgelehnte Daten und andere Ressourcenzugriffsversuche - Änderungen der Systemkonfiguration - Verwendung von Rechten - Verwendung von Systemdienstprogrammen und Anwendungen - Zugriffsarten und Art des Zugriffs -	elasticsearch-logs-to-cloudwatch	Stellen Sie sicher, dass für Amazon OpenSearch Service-Domains Fehlerprotokolle aktiviert und zur Aufbewahrung und Beantwortung an Amazon CloudWatch Logs gestreamt werden. Domain-Fehlerprotokolle sind bei Sicherheits- und Zugriffsprüfungen sowie bei der Diagnose von Verfügbarkeitsproblemen nützlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
	Netzwerkadressen und Protokolle - Ausgelöste Alarme durch die Zugriffsk ontrolle System und - Aufzeichnungen von Transaktionen, die von Benutzern in Anwendungen ausgeführt wurden, und Online-Ku ndentransaktionen		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
3.4(g)	g) Stellen Sie sicher, dass die Ereignisprotokolle gegebenenfalls Folgendes enthalten : IDs - Benutzer - Systemaktivitäten - Datum, Uhrzeit und Einzelheiten wichtiger Ereignisse, z. B. An- und Abmeldung - Geräteidentität oder Standort, falls möglich, und System-ID - Aufzeichnungen über erfolgreiche und abgelehnte Systemzugriffsversuche - Aufzeichnungen über erfolgreiche und abgelehnte Daten und andere Ressourcenzugriffsversuche - Änderungen der Systemkonfiguration - Verwendung von Rechten - Verwendung von Systemdienstprogrammen und Anwendungen - Zugriffsarten und Art des Zugriffs -	opensearch-logs-to-cloudwatch	Stellen Sie sicher, dass für Amazon OpenSearch Service-Domains Fehlerprotokolle aktiviert und zur Aufbewahrung und Beantwortung an Amazon CloudWatch Logs gestreamt werden. OpenSearch Service-Fehlerprotokolle können bei Sicherheits- und Zugriffsprüfungen helfen und bei der Diagnose von Verfügbarkeitsproblemen helfen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
	Netzwerkadressen und Protokolle - Ausgelöste Alarme durch die Zugriffsk ontrolle System und - Aufzeichnungen von Transaktionen, die von Benutzern in Anwendungen ausgeführt wurden, und Online-Ku ndentransaktionen		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
3.6.1(a)(h)	a) BFIs müssen angemesse ne Sicherhei tsmaßnahmen für ihre Webanwend ungen sicherstellen und angemessene Maßnahmen zur Risikominderung gegen verschied ene Internet-Sicherheitsrisiken ergreifen. h) BFIs müssen angemesse ne Sicherhei tsmaßnahmen für ihre Webanwend ungen sicherstellen und angemessene Maßnahmen zur Minderung verschied ener Websicher heitsrisiken ergreifen	alb-waf-enabled	Stellen Sie sicher, dass AWS WAF auf Elastic Load Balancers (ELB) aktiviert ist, um Webanwendungen zu schützen. Eine WAF trägt zum Schutz Ihrer Webanwend ungen oder APIs vor gängigen Web-Explo its bei. Diese Web-Exploits können sich auf die Verfügbar keit auswirken, die Sicherheit gefährden oder übermäßige Ressourcen in Ihrer Umgebung verbrauch en.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
3.6.1(a)(h)	a) BFIs müssen angemesse ne Sicherhei tsmaßnahmen für ihre Webanwend ungen sicherstellen und angemessene Maßnahmen zur Risikominderung gegen verschiedene Web-Sicherheitsris iken ergreifen. h) BFIs müssen angemesse ne Sicherhei tsmaßnahmen für ihre Webanwend ungen sicherstellen und angemessene Maßnahmen zur Abwehr verschiedener Websicherheitsrisiken ergreifen	api-gw-associated-with-WAF	AWS Mit WAF können Sie eine Reihe von Regeln (als Web Access Control List (Web ACL) bezeichne t) konfigurieren, die Webanfragen auf der Grundlage von anpassbaren Websicherheitsrege ln und -bedingungen, die Sie definieren, zulassen, blockieren oder zählen. Stellen Sie sicher, dass Ihre Amazon-API-Gateway-Stufe mit einer WAF-Web-A CL verknüpft ist, um sie vor böswilligen Angriffen zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
3.6.1(b)	b) BFIs müssen die Sicherheitsanforderungen in Bezug auf ihre Internetbanking-Systeme und andere relevante Systeme bewerten und eine Verschlüsselungslösung einführen, die den erforderlichen Grad an Vertraulichkeit und Integrität berücksichtigt.	acm-certificate-expiration-check	Stellen Sie sicher, dass die Netzwerkintegrität geschützt ist, indem Sie sicherstellen, dass X509-Zertifikate von AWS ACM ausgestellt werden. Diese Zertifikate müssen gültig und dürfen nicht abgelaufen sein. Für diese Regel ist ein Wert für erforderlich daysToExpiration (Wert für bewährte AWS Grundregeln für Sicherheit: 90). Der tatsächliche Wert muss den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
3.6.1(b)	b) BFIs müssen die Sicherheitsanforde rungen in Bezug auf ihre Internetbanking-Systeme und andere relevante Systeme bewerten und eine Verschlüsselungslö sung einführen, die dem erforderlichen Grad an Vertrauli chkeit und Integrität Rechnung trägt.	alb-http-to-https-Umleitungsprüfung	Um Daten während der Übertragung zu schützen, stellen Sie sicher, dass Ihr Application Load Balancer unverschl üsselte HTTP-Anfr agen automatisch an HTTPS umleitet. Da sensible Daten vorhanden sein können, sollten Sie die Verschlüsselung bei der Übertragung aktivieren, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
3.6.1(b)	b) BFIs müssen die Sicherheitsanforderungen im Zusammenhang mit ihren Internetbanking-Systemen und anderen relevanten Systemen bewerten und eine Verschlüsselungslösung einführen, die dem erforderlichen Grad an Vertraulichkeit und Integrität Rechnung trägt.	elb-acm-certificate-required	Zum Schutz von eventuell vorhandenen sensiblen Daten sowie von Daten während der Übertragung muss die Verschlüsselung für Ihr Elastic Load Balancing aktiviert sein. Verwenden Sie AWS Certificate Manager, um öffentliche und private SSL/TLS-Zertifikate mit AWS Diensten und internen Ressourcen zu verwalten, bereitzustellen und bereitzustellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
3.6.1(b)	b) BFIs müssen die Sicherheitsanforde rungen in Bezug auf ihre Internetbanking-Systeme und andere relevante Systeme bewerten und eine Verschlüsselungslö sung einführen, die den erforderlichen Grad an Vertrauli chkeit und Integrität berücksichtigt.	redshift-require-tls-ssl	Stellen Sie sicher, dass Ihre Amazon-Redshift-Cluster eine TLS/SSL-Verschlüss elung erfordern, um eine Verbindung zu SQL-Clients herzustel len. Da sensible Daten vorhanden sein können, sollten Sie die Verschlüsselung bei der Übertragung aktivieren, um diese Daten zu schützen.
3.6.1(b)	b) BFIs müssen die Sicherheitsanforde rungen in Bezug auf ihre Internetbanking-Systeme und andere relevante Systeme bewerten und eine Verschlüsselungslö sung einführen, die dem erforderlichen Grad an Vertrauli chkeit und Integrität Rechnung trägt.	s3- bucket-ssl-request s-only	Um Daten während der Übertragung zu schützen, stellen Sie sicher, dass Ihre Amazon Simple Storage Service (Amazon S3)-Bucke ts Anfragen zur Verwendung von Secure Socket Layer (SSL)-Buckets erfordern. Da sensible Daten vorhanden sein können, sollten Sie die Verschlüsselung bei der Übertragung aktivieren, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
3.6.1(b)	b) BFIs müssen die Sicherhei tsanforderungen im Zusammenhang mit ihren Internetb anking-Systemen und anderen relevanten Systemen bewerten und eine Verschlüs selungslösung einführen, die dem erforderlichen Grad an Vertraulichkeit und Integrität Rechnung trägt.	alb-http-drop-invalid-Header-fähig	Stellen Sie sicher, dass Ihre Elastic Load Balancers (ELB) so konfiguriert sind, dass sie HTTP-Header löschen. Da sensible Daten vorhanden sein können, sollten Sie die Verschlüsselung bei der Übertragung aktivieren, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
3.6.1(b)	b) BFIs müssen die Sicherheitsanforderungen im Zusammenhang mit ihren Internetbanking-Systemen und anderen relevanten Systemen bewerten und eine Verschlüsselungslösung einführen, die dem erforderlichen Grad an Vertraulichkeit und Integrität Rechnung trägt.	elasticsearch-node-to-node-Verschlüsselungsprüfung	Stellen Sie sicher, dass die node-to-node Verschlüsselung für Amazon OpenSearch Service aktiviert ist. Node-to-nodeVerschlüsselung ermöglicht die TLS 1.2-Verschlüsselung für die gesamte Kommunikation innerhalb der Amazon Virtual Private Cloud (Amazon VPC). Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
3.6.1(b)	b) BFIs müssen die Sicherheitsanforderungen im Zusammenhang mit ihren Internetbanking-Systemen und anderen relevanten Systemen bewerten und eine Verschlüsselungslösung einführen, die den erforderlichen Grad an Vertraulichkeit und Integrität berücksichtigt.	opensearch-node-to-node-Verschlüsselungsprüfung	Stellen Sie sicher, dass die node-to-node Verschlüsselung für Amazon OpenSearch Service aktiviert ist. Node-to-nodeVerschlüsselung ermöglicht die TLS 1.2-Verschlüsselung für die gesamte Kommunikation innerhalb der Amazon Virtual Private Cloud (Amazon VPC). Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
3.6.1(b)	b) BFIs müssen die Sicherheitsanforderungen im Zusammenhang mit ihren Internetbanking-Systemen und anderen relevanten Systemen bewerten und eine Verschlüsselungslösung einführen, die den erforderlichen Grad an Vertraulichkeit und Integrität berücksichtigt.	elb-tls-https-listeners-nur	Stellen Sie sicher, dass Ihre Elastic Load Balancer (ELBs) mit SSL- oder HTTPS-Listenern konfiguriert sind. Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.
3.6.1(b)	b) BFIs müssen die Sicherheitsanforderungen in Bezug auf ihre Internetbanking-Systeme und andere relevante Systeme bewerten und eine Verschlüsselungslösung einführen, die den erforderlichen Grad an Vertraulichkeit und Integrität berücksichtigt.	api-gw-ssl-enabled	Stellen Sie sicher, dass die REST-API-Stufen von Amazon API Gateway mit SSL-Zertifikaten konfiguriert sind, damit Backend-Systeme überprüfen können, ob Anforderungen von API Gateway stammen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
3.6.1(b)	b) BFIs müssen die Sicherheitsanforderungen in Bezug auf ihre Internetbanking-Systeme und andere relevante Systeme bewerten und eine Verschlüsselungslösung einführen, die dem erforderlichen Grad an Vertraulichkeit und Integrität Rechnung trägt.	elbv2- acm-certificate-required	Zum Schutz von eventuell vorhandenen sensiblen Daten sowie von Daten während der Übertragung muss die Verschlüsselung für Ihr Elastic Load Balancing aktiviert sein. Verwenden Sie AWS Certificate Manager, um öffentliche und private SSL/TLS-Zertifikate mit AWS Diensten und internen Ressourcen zu verwalten, bereitzustellen und bereitzustellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
3.6.1(d)	d) Die BFIs Bereitstellung von Internet-Banking sollte auf ungewöhnliche Netzwerkverkehrsbedingungen und Systemleistung sowie auf einen plötzlichen Anstieg der Systemressourcenauslastung reagieren, was auf einen S-Angriff hindeuten könnte. DDo Folglich hängt der Erfolg aller präventiven und reaktiven Maßnahmen vom Einsatz geeigneter Tools ab, mit denen Anomalien in Netzwerken und Systemen wirksam erkannt, überwacht und analysiert werden können.	alb-waf-enabled	Stellen Sie sicher, dass AWS WAF auf Elastic Load Balancers (ELB) aktiviert ist, um Webanwendungen zu schützen. Eine WAF trägt zum Schutz Ihrer Webanwendungen oder APIs vor gängigen Web-Exploits bei. Diese Web-Exploits können sich auf die Verfügbarkeit auswirken, die Sicherheit gefährden oder übermäßige Ressourcen in Ihrer Umgebung verbrauchen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
3.6.1(d)	d) Die BFIs Bereitstellung von Internet-Banking sollte auf ungewöhnliche Netzwerkverkehrsbedingungen und Systemleistung und einen plötzlichen Anstieg der Systemressourcenauslastung reagieren, was auf einen S-Angriff hindeuten könnte. DDo Folglich hängt der Erfolg aller präventiven und reaktiven Maßnahmen vom Einsatz geeigneter Tools ab, mit denen Anomalien in Netzwerken und Systemen wirksam erkannt, überwacht und analysiert werden können.	guardduty-enabled-centralized	Amazon GuardDuty kann mithilfe von Threat Intelligence Feeds helfen, potenzielle Cybersicherheitsereignisse zu überwachen und zu erkennen. Dazu gehören Listen mit bösartigen IPs und maschinellen Lernmethoden zur Identifizierung unerwarteter, nicht autorisierter und bösartiger Aktivitäten in Ihrer AWS Cloud-Umgebung.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
3.6.1(d)	d) Die BFIs Bereitstellung von Internet-Banking sollte auf ungewöhnliche Netzwerkverkehrsbedingungen und Systemleistung und einen plötzlichen Anstieg der Systemressourcenauslastung reagieren, was auf einen S-Angriff hindeuten könnte. DDo Folglich hängt der Erfolg aller präventiven und reaktiven Maßnahmen vom Einsatz geeigneter Tools ab, mit denen Anomalien in Netzwerken und Systemen wirksam erkannt, überwacht und analysiert werden können.	securityhub-enabled	AWS Security Hub hilft bei der Überwachung von unbefugtem Personal, Verbindungen, Geräten und Software. AWS Security Hub aggregiert, organisiert und priorisiert die Sicherheitswarnungen oder Ergebnisse mehrerer Dienste. AWS Einige dieser Dienste sind Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer und AWS Firewall Manager sowie AWS Partnerlösungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
3.6.1(d)	d) Die BFIs Bereitstellung von Internet-Banking sollte auf ungewöhnliche Netzwerkverkehrsbedingungen und Systemleistung und einen plötzlichen Anstieg der Systemressourcenauslastung reagieren, was ein Hinweis auf einen S-Angriff sein könnte. DDo Folglich hängt der Erfolg aller präventiven und reaktiven Maßnahmen vom Einsatz geeigneter Tools ab, mit denen Anomalien in Netzwerken und Systemen wirksam erkannt, überwacht und analysiert werden können.	wafv2-logging-enabled	Um die Protokollierung und Überwachung in Ihrer Umgebung zu erleichtern, aktivieren Sie die AWS WAF (V2) -Protokollierung im regionalen und globalen Internet. ACLs AWS Die WAF-Protokollierung bietet detaillierte Informationen über den Datenverkehr, der von Ihrer Web-ACL analysiert wird. In den Protokollen werden die Uhrzeit aufgezeichnet, zu der die AWS WAF die Anfrage von Ihrer AWS Ressource erhalten hat, Informationen zu der Anfrage und eine Aktion für die Regel, der jede Anfrage entsprach.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
3.6.1(d)	d) Die BFIs Bereitstellung von Internet-Banking sollte auf ungewöhnliche Netzwerkverkehrsbedingungen und Systemleistung und einen plötzlichen Anstieg der Systemressourcenauslastung reagieren, was auf einen S-Angriff hindeuten könnte. DDo Folglich hängt der Erfolg aller präventiven und reaktiven Maßnahmen vom Einsatz geeigneter Tools ab, mit denen Anomalien in Netzwerken und Systemen wirksam erkannt, überwacht und analysiert werden können.	api-gw-associated-with-WAF	AWS Mit WAF können Sie eine Reihe von Regeln (als Web Access Control List (Web ACL) bezeichnet) konfigurieren, die Webanfragen auf der Grundlage von anpassbaren Websicherheitsregeln und -bedingungen, die Sie definieren, zulassen, blockieren oder zählen. Stellen Sie sicher, dass Ihre Amazon-API-Gateway-Stufe mit einer WAF-Web-ACL verknüpft ist, um sie vor böswilligen Angriffen zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
3.6.1(e)	e) BFIs Sie müssen regelmäßig Sicherheitslücken im Bereich Informationssicherheit bewerten und die Wirksamkeit des bestehenden Frameworks für das IT-Sicherheitsrisikomanagement bewerten und alle erforderlichen Anpassungen vornehmen, um sicherzustellen, dass neu auftretende Sicherheitslücken rechtzeitig behoben werden. Diese Bewertung sollte auch anlässlich wesentlicher Änderungen durchgeführt werden.	guardduty-non-archived-findings	Amazon GuardDuty hilft Ihnen dabei, die Auswirkungen eines Vorfalls zu verstehen, indem es die Ergebnisse nach Schweregrad klassifiziert: niedrig, mittel und hoch. Diese Klassifizierungen können Sie zur Festlegung von entsprechenden Strategien und Prioritäten zur Behebung solcher Vorfälle verwenden. Mit dieser Regel können Sie optional daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7) und daysHighSev (Config Default: 1) für nicht archivierte Ergebnisse festlegen, wie es die Richtlinien Ihrer Organisation erfordern.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
3.6.4(a)(b)	a) Beschränken Sie den Internetzugang und segmentieren Sie kritische Systeme von der allgemein en IT-Umgebung. b) Reduzieren Sie die Angriffsfläche und die Schwachstellen.	dms-replication-not-public	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass auf DMS-Replikationsin stanzen nicht öffentlic h zugegriffen werden kann. DMS-Repli kations-Instances können vertrauli che Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.
3.6.4(a)(b)	a) Beschränken Sie den Internetzugang und segmentieren Sie kritische Systeme von der allgemein en IT-Umgebung. b) Reduzieren Sie die Angriffsfläche und die Schwachstellen.	ebs-snapshot-public-restorable-überprüfen	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass EBS-Snapshots nicht öffentlich wiederher stellbar sind. EBS-Volume-Snapsho ts können vertrauli che Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
3.6.4(a)(b)	a) Beschränken Sie den Internetzugang und segmentieren Sie kritische Systeme von der allgemein en IT-Umgebung. b) Reduzieren Sie die Angriffsfläche und die Schwachstellen.	ec-2 instance-no-public-ip	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon Elastic Compute Cloud (Amazon EC2) - Instances nicht öffentlich zugänglich sind. EC2 Amazon-Instances können vertrauliche Informati onen enthalten, und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
3.6.4(a)(b)	a) Beschränken Sie den Internetzugang und segmentieren Sie kritische Systeme von der allgemein en IT-Umgebung. b) Reduzieren Sie die Angriffsfläche und die Schwachstellen.	elasticsearch-in-vpc-only	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherste llen, dass sich Amazon OpenSearc h OpenSearch Service (Service) - Domains innerhalb einer Amazon Virtual Private Cloud (Amazon VPC) befinden. Eine OpenSearch Service-Domain innerhalb einer Amazon VPC ermöglicht die sichere Kommunikation zwischen OpenSearc h Service und anderen Services innerhalb der Amazon VPC, ohne dass ein Internet-Gateway, ein NAT-Gerät oder eine VPN-Verbindung erforderlich ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
3.6.4(a)(b)	a) Beschränken Sie den Internetzugang und segmentieren Sie kritische Systeme von der allgemein en IT-Umgebung. b) Reduzieren Sie die Angriffsfläche und die Schwachstellen.	opensearch-in-vpc-only	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass sich Amazon OpenSearch Service-Domains innerhalb einer Amazon Virtual Private Cloud (Amazon VPC) befinden. Eine Amazon OpenSearc h Service-Domain innerhalb einer Amazon VPC ermöglicht die sichere Kommunikation zwischen Amazon OpenSearch Service und anderen Services innerhalb der Amazon VPC, ohne dass ein Internet-Gateway, ein NAT-Gerät oder eine VPN-Verbindung erforderlich ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
3.6.4(a)(b)	a) Beschränken Sie den Internetzugang und segmentieren Sie kritische Systeme von der allgemein en IT-Umgebung. b) Reduzieren Sie die Angriffsfläche und die Schwachstellen.	emr-master-no-public-ip	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon EMR-Clust er-Masterknoten nicht öffentlich zugänglic h sind. Amazon-EM R-Cluster-Hauptkno ten können vertrauli che Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
3.6.4(a)(b)	a) Beschränken Sie den Internetzugang und segmentieren Sie kritische Systeme von der allgemein en IT-Umgebung. b) Reduzieren Sie die Angriffsfläche und die Schwachstellen.	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) Security Groups können bei der Verwaltung des Netzwerkzugriffs helfen, indem sie eine statusbeh aftete Filterung von eingehendem und ausgehendem Netzwerkverkehr zu Ressourcen bereitste llen. AWS Wenn Sie eingehenden (oder entfernten) Datenverk ehr von 0.0.0.0/0 bis Port 22 auf Ihren Ressourcen nicht zulassen, können Sie den Remote-Zugriff einschränken.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
3.6.4(a)(b)	a) Beschränken Sie den Internetzugang und segmentieren Sie kritische Systeme von der allgemein en IT-Umgebung. b) Reduzieren Sie die Angriffsfläche und die Schwachstellen.	ec-2 instances-in-vpc	Stellen Sie Amazon Elastic Compute Cloud (Amazon EC2) -Instances innerhalb einer Amazon Virtual Private Cloud (Amazon VPC) bereit, um eine sichere Kommunika tion zwischen einer Instance und anderen Services innerhalb der Amazon VPC zu ermöglichen, ohne dass ein Internet-Gateway, ein NAT-Gerät oder eine VPN-Verbindung erforderlich ist. Der gesamte Datenverk ehr bleibt sicher in der AWS Cloud. Domains, die sich innerhalb einer VPC befinden, verfügen aufgrund ihrer logischen Isolierun g im Vergleich zu Domains mit öffentlic hen Endpunkten über eine zusätzlic he Sicherheitsebene. Weisen Sie EC2

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
			Amazon-Instances einer Amazon-VPC zu, um den Zugriff ordnungsgemäß zu verwalten.
3.6.4(a)(b)	a) Beschränken Sie den Internetzugang und segmentieren Sie kritische Systeme von der allgemeinen IT-Umgebung. b) Reduzieren Sie die Angriffsfläche und die Schwachstellen.	internet-gateway-authorized-vpc-nur	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Internet-Gateways nur mit autorisierter Amazon Virtual Private Cloud (Amazon VPC) verbunden sind. Internet-Gateways ermöglichen den bidirektionalen Internetzugang zur und von der Amazon VPC, was möglicherweise zu einem unbefugten Zugriff auf Amazon-VPC-Ressourcen führen kann.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
3.6.4(a)(b)	a) Beschränken Sie den Internetzugang und segmentieren Sie kritische Systeme von der allgemeinen IT-Umgebung. b) Reduzieren Sie die Angriffsfläche und die Schwachstellen.	lambda-function-public-access-verboten	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass AWS Lambda-Funktionen nicht öffentlich zugänglich sind. Der öffentliche Zugriff kann möglicherweise die Verfügbarkeit von Ressourcen beeinträchtigen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
3.6.4(a)(b)	a) Beschränken Sie den Internetzugang und segmentieren Sie kritische Systeme von der allgemein en IT-Umgebung. b) Reduzieren Sie die Angriffsfläche und die Schwachstellen.	lambda-inside-vpc	Stellen Sie AWS Lambda-Funktionen in einer Amazon Virtual Private Cloud (Amazon VPC) bereit, um eine sichere Kommunika tion zwischen einer Funktion und anderen Diensten innerhalb der Amazon VPC zu gewährleisten. Bei dieser Konfiguration sind kein Internet-Gateway, kein NAT-Gerät und keine VPN-Verbindung erforderlich. Der gesamte Datenverk ehr bleibt sicher in der Cloud. AWS Domains, die sich innerhalb einer VPC befinden, verfügen aufgrund ihrer logischen Isolierun g im Vergleich zu Domains mit öffentlic hen Endpunkten über eine zusätzliche Sicherheitsebene. Um den Zugriff ordnungsg emäß zu verwalten,

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
			sollten AWS Lambda-Funktionen einer VPC zugewiesen werden.
3.6.4(a)(b)	a) Beschränken Sie den Internetzugang und segmentieren Sie kritische Systeme von der allgemein en IT-Umgebung. b) Reduzieren Sie die Angriffsfläche und die Schwachstellen.	rds-instance-public-access-überprüfen	Verwalten Sie den Zugriff auf Ressource n in der AWS Cloud, indem Sie sicherste llen, dass Amazon Relational Database Service (Amazon RDS) -Instance s nicht öffentlic h sind. Amazon-RDS-Datenbank-Instances können vertrauliche Informati onen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
3.6.4(a)(b)	a) Beschränken Sie den Internetzugang und segmentieren Sie kritische Systeme von der allgemein en IT-Umgebung. b) Reduzieren Sie die Angriffsfläche und die Schwachstellen.	rds-snapshots-public-prohibited	Verwalten Sie den Zugriff auf Ressource n in der AWS Cloud, indem Sie sicherste llen, dass Amazon Relational Database Service (Amazon RDS) -Instance s nicht öffentlic h sind. Amazon-RDS-Datenbank-Instances können vertrauliche Informati onen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
3.6.4(a)(b)	a) Beschränken Sie den Internetzugang und segmentieren Sie kritische Systeme von der allgemeinen IT-Umgebung. b) Reduzieren Sie die Angriffsfläche und die Schwachstellen.	redshift-cluster-public-access-überprüfen	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Redshift Redshift-Cluster nicht öffentlich sind. Amazon-Redshift-Cluster können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
3.6.4(a)(b)	a) Beschränken Sie den Internetzugang und segmentieren Sie kritische Systeme von der allgemein en IT-Umgebung. b) Reduzieren Sie die Angriffsfläche und die Schwachstellen.	restricted-common-ports	Verwalten Sie den Zugriff auf Ressource n in der AWS Cloud, indem Sie sicherste llen, dass gemeinsam e Ports für Amazon Elastic Compute Cloud (Amazon EC2) -Sicherhe itsgruppen eingeschr ränkt sind. Wenn der Zugriff auf Ports nicht auf vertrauen swürdige Quellen beschränkt wird, kann dies zu Angriffen auf die Verfügbar keit, Integrität und Vertraulichkeit von Systemen führen. Mit dieser Regel können Sie optional die Parameter blockedPo rt1–blockedPort5 festlegen (Standard konfigurationen: 20, 21, 3389, 3306, 4333). Die tatsächli chen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
3.6.4(a)(b)	a) Beschränken Sie den Internetzugang und segmentieren Sie kritische Systeme von der allgemein en IT-Umgebung. b) Reduzieren Sie die Angriffsfläche und die Schwachstellen.	s-3 bucket-public-read -prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie nur autorisierten Benutzern, Prozessen und Geräten Zugriff auf Amazon Simple Storage Service (Amazon S3) - Buckets gewähren. Die Verwaltung des Zugriffs sollte mit der Klassifizierung der Daten übereinst immen.
3.6.4(a)(b)	a) Beschränken Sie den Internetzugang und segmentieren Sie kritische Systeme von der allgemein en IT-Umgebung. b) Reduzieren Sie die Angriffsfläche und die Schwachstellen.	s3- bucket-public-writ e-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie nur autorisierten Benutzern, Prozessen und Geräten Zugriff auf Amazon Simple Storage Service (Amazon S3) - Buckets gewähren. Die Verwaltung des Zugriffs sollte mit der Klassifizierung der Daten übereinst immen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
3.6.4(a)(b)	a) Beschränken Sie den Internetzugang und segmentieren Sie kritische Systeme von der allgemeinen IT-Umgebung. b) Reduzieren Sie die Angriffsfläche und die Schwachstellen.	sagemaker-notebook-no-direct-Internetzugang	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass SageMaker Amazon-Notebooks keinen direkten Internetzugang zulassen. Indem Sie direkten Internetzugang blockieren, vermeiden Sie, dass unbefugte Benutzer auf sensible Daten zugreifen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
3.6.4(a)(b)	a) Beschränken Sie den Internetzugang und segmentieren Sie kritische Systeme von der allgemein en IT-Umgebung. b) Reduzieren Sie die Angriffsfläche und die Schwachstellen.	vpc-default-security-group-geschlossen	Sicherheitsgruppen von Amazon Elastic Compute Cloud (Amazon EC2) können bei der Verwaltung des Netzwerkzugriffs helfen, indem sie eine statusbehaftete Filterung des ein- und ausgehenden Netzwerkverkehrs zu Ressourcen bereitstellen. AWS Die Beschränk ung des gesamten Datenverkehrs auf die Standardsicherheit sgruppe hilft dabei, den Fernzugriff auf Ihre Ressourcen einzuschränken. AWS

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
3.6.4(a)(b)	a) Beschränken Sie den Internetzugang und segmentieren Sie kritische Systeme von der allgemeinen IT-Umgebung. b) Reduzieren Sie die Angriffsfläche und die Schwachstellen.	vpc-sg-open-only-to-authorized-ports	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass gemeinsame Ports für Amazon Elastic Compute Cloud (Amazon EC2) -Sicherheitsgruppen eingeschränkt sind. Wenn der Zugriff auf Ports nicht auf vertrauenswürdige Quellen beschränkt wird, kann dies zu Angriffen auf die Verfügbarkeit, Integrität und Vertraulichkeit von Systemen führen. Durch die Beschränkung des Zugriffs auf Ressourcen innerhalb einer Sicherheitsgruppe aus dem Internet (0.0.0.0/0) kann der Fernzugriff auf interne Systeme gesteuert werden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
3.6.4(a)(b)	a) Beschränken Sie den Internetzugang und segmentieren Sie kritische Systeme von der allgemein en IT-Umgebung. b) Reduzieren Sie die Angriffsfläche und die Schwachstellen.	no-unrestricted-route-to-igw	Stellen Sie sicher, dass EC2 Amazon-Routentabellen keine uneingeschränkten Routen zu einem Internet-Gateway enthalten. Durch das Entfernen oder Beschränken des Internetzugangs für Workloads innerhalb von Amazon VPCs können unbeabsic htigte Zugriffe in Ihrer Umgebung reduziert werden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
3.6.4(a)(b)	a) Beschränken Sie den Internetzugang und segmentieren Sie kritische Systeme von der allgemein en IT-Umgebung. b) Reduzieren Sie die Angriffsfläche und die Schwachstellen.	subnet-auto-assign-public-ip-deaktiviert	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon Virtual Private Cloud (VPC) -Subnetzen nicht automatisch eine öffentliche IP-Adress e zugewiesen wird. Amazon Elastic Compute Cloud (EC2) -Instances, die in Subnetzen gestartet werden, in denen dieses Attribut aktiviert ist, haben ihrer primären Netzwerkschnittste lle eine öffentliche IP-Adresse zugewiesen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
3.6.4(a)(b)	a) Beschränken Sie den Internetzugang und segmentieren Sie kritische Systeme von der allgemein en IT-Umgebung. b) Reduzieren Sie die Angriffsfläche und die Schwachstellen.	autoscaling-launch -config-public-ip- deaktiviert	Wenn Sie Ihre Netzwerkschnittstellen mit einer öffentlichen IP-Adresse konfiguri eren, sind die diesen Netzwerkschnittste llen zugehörigen Ressourcen über das Internet erreichba r. EC2 Ressourcen sollten nicht öffentlic h zugänglich sein, da dies einen unbeabsic htigten Zugriff auf Ihre Anwendungen oder Server ermöglichen kann.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
3.6.4(a)(b)	a) Beschränken Sie den Internetzugang und segmentieren Sie kritische Systeme von der allgemein en IT-Umgebung. b) Reduzieren Sie die Angriffsfläche und die Schwachstellen.	s3- -Block-periodisch account-level-public-access	Verwalten Sie den Zugriff auf Ressource n in der AWS Cloud, indem Sie sicherste llen, dass Amazon Simple Storage Service (Amazon S3) -Buckets nicht öffentlich zugänglic h sind. Diese Regel trägt dazu bei, sensible Daten vor unbefugten Remote-Benutzern zu schützen, indem sie den öffentlichen Zugriff verhinder t. Mit dieser Regel können Sie optional die Parameter ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) und restrictPublicBuck ets Parameter (Config Default: True) festlegen. Die tatsächlichen Werte müssen den Richtlini

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen zu
			en Ihrer Organisation entsprechen.
3.6.4(a)(b)	a) Beschränken Sie den Internetzugang und segmentieren Sie kritische Systeme von der allgemein en IT-Umgebung. b) Reduzieren Sie die Angriffsfläche und die Schwachstellen.	ssm-document-not-p ublic	Stellen Sie sicher, dass AWS Systems Manager (SSM) - Dokumente nicht öffentlich sind, da dies einen unbeabsic htigten Zugriff auf Ihre SSM-Dokum ente ermöglichen kann. Ein öffentlic hes SSM-Dokum ent kann Informati onen über Ihr Konto, Ihre Ressourcen und internen Prozesse preisgeben.

Vorlage

Die Vorlage ist verfügbar unter GitHub: Operational Best Practices for NBC TRMG.

Bewährte Methoden für die Ausführung von NERC CIP BCSI

Konformitätspakete bieten ein allgemeines Compliance-Framework, das es Ihnen ermöglicht, mithilfe verwalteter oder benutzerdefinierter Regeln und Abhilfemaßnahmen Kontrollen zur Sicherheits-, Betriebs- oder Kostenoptimierung durchzuführen. AWS Config AWS Config Conformance Packs dienen als Beispielvorlagen nicht dazu, die vollständige Einhaltung eines bestimmten Governance- oder Compliance-Standards sicherzustellen. Sie sind dafür verantwortlich, selbst zu beurteilen, ob Ihre Nutzung der Services den geltenden gesetzlichen und behördlichen Anforderungen entspricht.

Im Folgenden finden Sie ein Beispiel für eine Zuordnung zwischen den Critical Infrastructure Protection Standards (NERC CIP) der North American Electric Reliability Corporation für BES Cyber

System Information (BCSI), CIP-004-7 und CIP-011-3, und verwalteten Regeln. AWS Config Jede AWS Config-Regel gilt für eine bestimmte AWS Ressource und bezieht sich auf eine oder mehrere NERC-CIP-Kontrollen, die für BCSI gelten. Eine NERC-CIP-Kontrolle kann mehreren Config-Regeln zugeordnet werden. In der folgenden Tabelle finden Sie weitere Informationen und Anleitungen zu diesen Zuordnungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen
CIP-004-7-R6 Abschnitt 6.1	Jede verantwortliche Stelle muss ein oder mehrere dokumentierte Zugriffsverwaltungsprogramme zur Autorisierung, Überprüfung und Widerrufung des bereitgestellten Zugriffs auf BCSI für die in CIP-004-7 Tabelle R6 – Zugriffsmanagement für BES Cyber System Information – genannten „anwendbaren Systemen“ implementieren, die zusammen alle zutreffenden Anforderungsabschnitte in CIP-004-7 Tabelle R6 – Zugriffsmanagement für BES Cyber System Information – enthalten. Im Rahmen dieser Anforderung	opensearch-access-control-enabled	Stellen Sie sicher, dass eine differenzierte Zugriffskontrolle für Ihre Amazon OpenSearch Service-Domains aktiviert ist. Eine differenzierte Zugriffskontrolle bietet erweiterte Autorisierungsmechanismen, um den Zugriff auf Amazon-Domains mit den geringsten Rechten zu erreichen. OpenSearch Es ermöglicht eine rollenbasierte Zugriffskontrolle auf die Domain sowie Sicherheit auf Index-, Dokument- und Feldebene, Unterstützung für OpenSearch Dashboards, Mehrmandantenfähigkeit und HTTP-Basisauthentifizierung

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen
	bezeichnet Zugang zu BCSI die Fähigkeit einer Person, BCSI zu erhalten und zu nutzen. Der bereitgestellte Zugriff ist das Ergebnis der spezifischen Maßnahmen, die ergriffen wurden, um einer oder mehreren Personen die Möglichkeit zu geben, auf BCSI zuzugreifen (kann beispielsweise physische Schlüssel oder Zugangskarten, Benutzer und damit verbundene Rechte und Privilegien, Verschlüsselungsschlüssel beinhalten). Abschnitt 6.1: Erteilen Sie Autorisierungen vor der Bereitstellung (sofern nicht bereits gemäß Abschnitt 4.1 autorisiert) nach Bedarf, wie von der verantwortlichen Stelle festgelegt, mit Ausnahme von CIP unter außergewöhnlichen Umständen: 6.1.1. Bereitgestellter		für und Kibana. OpenSearch

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen
	elektronischer Zugriff auf elektronische BCSI		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen
CIP-004-7-R6 Abschnitt 6.1	Jede verantwortliche Stelle muss ein oder mehrere dokumentierte Zugriffsverwaltungsprogramme zur Autorisierung, Überprüfung und Widerrufung des bereitgestellten Zugriffs auf BCSI für die in CIP-004-7 Tabelle R6 – Zugriffsmanagement für BES Cyber System Information – genannten „anwendbaren Systemen“ implementieren, die zusammen alle zutreffenden Anforderungsabschnitte in CIP-004-7 Tabelle R6 – Zugriffsmanagement für BES Cyber System Information – enthalten. Im Rahmen dieser Anforderung bezeichnet Zugang zu BCSI die Fähigkeit einer Person, BCSI zu erhalten und zu nutzen. Der bereitges	emr-kerberos-enabled	Die Zugriffsberechtigungen und -autorisierungen können verwaltet und nach den Prinzipien der geringsten Berechtigung und Aufgabentrennung integriert werden, indem Kerberos für Amazon-EMR-Cluster aktiviert wird. In Kerberos werden Services und Benutzer, die sich authentifizieren müssen, als Prinzipale bezeichnet. Prinzipale befinden sich in einem Kerberos-Bereich. Innerhalb dieses Bereichs wird ein Kerberos-Server als Key Distribution Center (KDC) bezeichnet. Über diesen Server können sich Prinzipale authentifizieren. Die Authentifizierung im KDC erfolgt durch die Ausstellung von Authentif

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen
	tellte Zugriff ist als Ergebnis der spezifischen Maßnahmen zu betrachten, die ergriffen wurden, um einer oder mehreren Personen die Möglichkeit zu geben, auf BCSI zuzugreifen (kann beispielsweise physische Schlüssel oder Zugangskarten, Benutzer und zugehörige Rechte und Privilegien, Verschlüsselungsschlüssel beinhalten). Abschnitt 6.1: Erteilen Sie Autorisierungen vor der Bereitstellung (sofern nicht bereits gemäß Abschnitt 4.1 autorisiert) nach Bedarf, wie von der verantwortlichen Stelle festgelegt, mit Ausnahme von CIP unter außergewöhnlichen Umständen: 6.1.1. Bereitgestellter elektronischer Zugriff auf elektronische BCSI		izierungstickets. Das KDC unterhält eine Datenbank der Prinzipale in seinem Bereich mit ihren Passwörtern und anderen administrativen Informationen zu jedem Prinzipal.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen
CIP-004-7-R6 Abschnitt 6.1	Jede verantwortliche Stelle muss ein oder mehrere dokumentierte Zugriffsverwaltungsprogramme zur Autorisierung, Überprüfung und Widerrufung des bereitgestellten Zugriffs auf BCSI für die in CIP-004-7 Tabelle R6 – Zugriffsmanagement für BES Cyber System Information – genannten „anwendbaren Systemen“ implementieren, die zusammen alle zutreffenden Anforderungsabschnitte in CIP-004-7 Tabelle R6 – Zugriffsmanagement für BES Cyber System Information – enthalten. Im Rahmen dieser Anforderung bezeichnet Zugang zu BCSI die Fähigkeit einer Person, BCSI zu erhalten und zu nutzen. Der bereitges	iam-group-has-users-überprüfen	AWS Identity and Access Management (IAM) kann Ihnen helfen, die Prinzipien der geringsten Rechte und der Aufgabentrennung mit Zugriffsberechtigungen und Autorisierungen zu integrieren, indem sichergestellt wird, dass IAM-Gruppen mindestens einen Benutzer haben. Die Einteilung von Benutzern in Gruppen auf der Grundlage der ihnen zugewiesenen Berechtigungen oder ihrer Funktion ist eine Möglichkeit, das Prinzip der geringsten Berechtigung zu implementieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen
	tellte Zugriff ist das Ergebnis der spezifischen Maßnahmen, die ergriffen wurden, um einer oder mehreren Personen die Möglichkeit zu geben, auf BCSI zuzugreifen (kann beispielsweise physische Schlüssel oder Zugangskarten, Benutzer und damit verbundene Rechte und Privilegien, Verschlüsselungsschlüssel umfassen). Abschnitt 6.1: Erteilen Sie Autorisierungen vor der Bereitstellung (sofern nicht bereits gemäß Abschnitt 4.1 autorisiert) nach Bedarf, wie von der verantwortlichen Stelle festgelegt, mit Ausnahme von CIP unter außergewöhnlichen Umständen: 6.1.1. Bereitgestellter elektronischer Zugriff auf elektronische BCSI		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen
CIP-004-7-R6 Abschnitt 6.1	Jede verantwortliche Stelle muss ein oder mehrere dokumentierte Zugriffsverwaltungsprogramme zur Autorisierung, Überprüfung und Widerrufung des bereitgestellten Zugriffs auf BCSI für die in CIP-004-7 Tabelle R6 – Zugriffsmanagement für BES Cyber System Information – genannten „anwendbaren Systemen“ implementieren, die zusammen alle zutreffenden Anforderungsabschnitte in CIP-004-7 Tabelle R6 – Zugriffsmanagement für BES Cyber System Information – enthalten. Im Rahmen dieser Anforderung bezeichnet Zugang zu BCSI die Fähigkeit einer Person, BCSI zu erhalten und zu nutzen. Der bereitges	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) kann Ihnen dabei helfen, die Prinzipien der geringsten Rechte und der Aufgabentrennung in Zugriffsberechtigungen und Autorisierungen zu integrieren und so zu verhindern, dass Richtlinien „Effect“: „Allow“ mit „Action“: „*“ anstelle von „Resource“: „*“ enthalten. Wenn Benutzern mehr Rechte eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und der Aufgabentrennung verstoßen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen
	tellte Zugriff ist das Ergebnis der spezifischen Maßnahmen, die ergriffen wurden, um einer oder mehreren Personen die Möglichkeit zu geben, auf BCSI zuzugreifen (kann beispielsweise physische Schlüssel oder Zugangskarten, Benutzer und zugehörige Rechte und Privilegien, Verschlüsselungsschlüssel beinhalten). Abschnitt 6.1: Erteilen Sie Autorisierungen vor der Bereitstellung (sofern nicht bereits gemäß Abschnitt 4.1 autorisiert) nach Bedarf, wie von der verantwortlichen Stelle festgelegt, mit Ausnahme von CIP unter außergewöhnlichen Umständen: 6.1.1. Bereitgestellter elektronischer Zugriff auf elektronische BCSI		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen
CIP-004-7-R6 Abschnitt 6.1	Jede verantwortliche Stelle muss ein oder mehrere dokumentierte Zugriffsverwaltungsprogramme zur Autorisierung, Überprüfung und Widerrufung des bereitgestellten Zugriffs auf BCSI für die in CIP-004-7 Tabelle R6 – Zugriffsmanagement für BES Cyber System Information – genannten „anwendbaren Systemen“ implementieren, die zusammen alle zutreffenden Anforderungsabschnitte in CIP-004-7 Tabelle R6 – Zugriffsmanagement für BES Cyber System Information – enthalten. Im Rahmen dieser Anforderung bezeichnet Zugang zu BCSI die Fähigkeit einer Person, BCSI zu erhalten und zu nutzen. Der bereitges	iam-root-access-key-überprüfen	Der Zugriff auf Systeme und Ressourcen kann gesteuert werden, indem überprüft wird, ob der Root-Benutzer keine Zugriffsschlüssel mit seiner AWS Identity and Access Management (IAM) -Rolle verknüpft hat. Stellen Sie sicher, dass die Root-Zugriffsschlüssel gelöscht werden. Erstellen und verwenden Sie stattdessen rollenbasierte Funktionen, AWS-Konten um das Prinzip der geringsten Funktionalität zu berücksichtigen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen
	tellte Zugriff ist das Ergebnis der spezifischen Maßnahmen, die ergriffen wurden, um einer oder mehreren Personen die Möglichkeit zu geben, auf BCSI zuzugreifen (kann beispielsweise physische Schlüssel oder Zugangskarten, Benutzer und damit verbundene Rechte und Privilegien, Verschlüsselungsschlüssel umfassen). Abschnitt 6.1: Erteilen Sie Autorisierungen vor der Bereitstellung (sofern nicht bereits gemäß Abschnitt 4.1 autorisiert) nach Bedarf, wie von der verantwortlichen Stelle festgelegt, mit Ausnahme von CIP unter außergewöhnlichen Umständen: 6.1.1. Bereitgestellter elektronischer Zugriff auf elektronische BCSI		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen
CIP-004-7-R6 Abschnitt 6.1	Jede verantwortliche Stelle muss ein oder mehrere dokumentierte Zugriffsverwaltungsprogramme zur Autorisierung, Überprüfung und Widerrufung des bereitgestellten Zugriffs auf BCSI für die in CIP-004-7 Tabelle R6 – Zugriffsmanagement für BES Cyber System Information – genannten „anwendbaren Systemen“ implementieren, die zusammen alle zutreffenden Anforderungsabschnitte in CIP-004-7 Tabelle R6 – Zugriffsmanagement für BES Cyber System Information – enthalten. Im Rahmen dieser Anforderung bezeichnet Zugang zu BCSI die Fähigkeit einer Person, BCSI zu erhalten und zu nutzen. Der bereitges	iam-user-group-membership-überprüfen	AWS Identity and Access Management (IAM) kann Ihnen helfen, Zugriffsberechtigungen und Autorisierungen einzuschränken, indem sichergestellt wird, dass Benutzer Mitglieder mindestens einer Gruppe sind. Wenn Benutzern mehr Berechtigungen eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und Aufgabentrennung verstoßen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen
	tellte Zugriff ist das Ergebnis der spezifischen Maßnahmen, die ergriffen wurden, um einer oder mehreren Personen die Möglichkeit zu geben, auf BCSI zuzugreifen (kann beispielsweise physische Schlüssel oder Zugangskarten, Benutzer und zugehörige Rechte und Privilegien, Verschlüsselungsschlüssel beinhalten). Abschnitt 6.1: Erteilen Sie Autorisierungen vor der Bereitstellung (sofern nicht bereits gemäß Abschnitt 4.1 autorisiert) nach Bedarf, wie von der verantwortlichen Stelle festgelegt, mit Ausnahme von CIP unter außergewöhnlichen Umständen: 6.1.1. Bereitgestellter elektronischer Zugriff auf elektronische BCSI		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen
CIP-004-7-R6 Abschnitt 6.1	Jede verantwortliche Stelle muss ein oder mehrere dokumentierte Zugriffsverwaltungsprogramme zur Autorisierung, Überprüfung und Widerrufung des bereitgestellten Zugriffs auf BCSI für die in CIP-004-7 Tabelle R6 – Zugriffsmanagement für BES Cyber System Information – genannten „anwendbaren Systemen“ implementieren, die zusammen alle zutreffenden Anforderungsabschnitte in CIP-004-7 Tabelle R6 – Zugriffsmanagement für BES Cyber System Information – enthalten. Im Rahmen dieser Anforderung bezeichnet Zugang zu BCSI die Fähigkeit einer Person, BCSI zu erhalten und zu nutzen. Der bereitges	iam-user-no-policies-überprüfen	Diese Regel stellt sicher, dass AWS Identity and Access Management (IAM) -Richtlinien nur Gruppen oder Rollen zugewiesen werden, um den Zugriff auf Systeme und Ressourcen zu kontrollieren. Die Zuweisung von Berechtigungen auf Gruppen- oder Rollenebene trägt dazu bei, die Wahrscheinlichkeit zu verringern, dass eine Identität übermäßige Berechtigungen erhält oder beibehält.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen
	tellte Zugriff ist das Ergebnis der spezifischen Maßnahmen, die ergriffen wurden, um einer oder mehreren Personen die Möglichkeit zu geben, auf BCSI zuzugreifen (kann beispielsweise physische Schlüssel oder Zugangskarten, Benutzer und zugehörige Rechte und Privilegien, Verschlüsselungsschlüssel beinhalten). Abschnitt 6.1: Erteilen Sie Autorisierungen vor der Bereitstellung (sofern nicht bereits gemäß Abschnitt 4.1 autorisiert) nach Bedarf, wie von der verantwortlichen Stelle festgelegt, mit Ausnahme von CIP unter außergewöhnlichen Umständen: 6.1.1. Bereitgestellter elektronischer Zugriff auf elektronische BCSI		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen
CIP-004-7-R6 Abschnitt 6.1	Jede verantwortliche Stelle muss ein oder mehrere dokumentierte Zugriffsverwaltungsprogramme zur Autorisierung, Überprüfung und Widerrufung des bereitgestellten Zugriffs auf BCSI für die in CIP-004-7 Tabelle R6 – Zugriffsmanagement für BES Cyber System Information – genannten „anwendbaren Systemen“ implementieren, die zusammen alle zutreffenden Anforderungsabschnitte in CIP-004-7 Tabelle R6 – Zugriffsmanagement für BES Cyber System Information – enthalten. Im Rahmen dieser Anforderung bezeichnet Zugang zu BCSI die Fähigkeit einer Person, BCSI zu erhalten und zu nutzen. Der bereitges	s-3 bucket-public-read-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie nur autorisierten Benutzern, Prozessen und Geräten Zugriff auf Amazon Simple Storage Service (Amazon S3) - Buckets gewähren. Die Verwaltung des Zugriffs sollte mit der Klassifizierung der Daten übereinstimmen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen
	tellte Zugriff ist das Ergebnis der spezifischen Maßnahmen, die ergriffen wurden, um einer oder mehreren Personen die Möglichkeit zu geben, auf BCSI zuzugreifen (kann beispielsweise physische Schlüssel oder Zugangskarten, Benutzer und zugehörige Rechte und Privilegien, Verschlüsselungsschlüssel beinhalten). Abschnitt 6.1: Erteilen Sie Autorisierungen vor der Bereitstellung (sofern nicht bereits gemäß Abschnitt 4.1 autorisiert) nach Bedarf, wie von der verantwortlichen Stelle festgelegt, mit Ausnahme von CIP unter außergewöhnlichen Umständen: 6.1.1. Bereitgestellter elektronischer Zugriff auf elektronische BCSI		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen
CIP-004-7-R6 Abschnitt 6.1	Jede verantwortliche Stelle muss ein oder mehrere dokumentierte Zugriffsverwaltungsprogramme zur Autorisierung, Überprüfung und Widerrufung des bereitgestellten Zugriffs auf BCSI für die in CIP-004-7 Tabelle R6 – Zugriffsmanagement für BES Cyber System Information – genannten „anwendbaren Systemen“ implementieren, die zusammen alle zutreffenden Anforderungsabschnitte in CIP-004-7 Tabelle R6 – Zugriffsmanagement für BES Cyber System Information – enthalten. Im Rahmen dieser Anforderung bezeichnet Zugang zu BCSI die Fähigkeit einer Person, BCSI zu erhalten und zu nutzen. Der bereitges	s-3 bucket-public-write-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie nur autorisierten Benutzern, Prozessen und Geräten Zugriff auf Amazon Simple Storage Service (Amazon S3) - Buckets gewähren. Die Verwaltung des Zugriffs sollte mit der Klassifizierung der Daten übereinstimmen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen
	tellte Zugriff ist als Ergebnis der spezifischen Maßnahmen zu betrachten, die ergriffen wurden, um einer oder mehreren Personen die Möglichkeit zu geben, auf BCSI zuzugreifen (kann beispielsweise physische Schlüssel oder Zugangskarten, Benutzer und zugehörige Rechte und Privilegien, Verschlüsselungsschlüssel beinhalten). Abschnitt 6.1: Erteilen Sie Autorisierungen vor der Bereitstellung (sofern nicht bereits gemäß Abschnitt 4.1 autorisiert) nach Bedarf, wie von der verantwortlichen Stelle festgelegt, mit Ausnahme von CIP unter außergewöhnlichen Umständen: 6.1.1. Bereitgestellter elektronischer Zugriff auf elektronische BCSI		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen
CIP-004-7-R6 Abschnitt 6.1	Jede verantwortliche Stelle muss ein oder mehrere dokumentierte Zugriffsverwaltungsprogramme zur Autorisierung, Überprüfung und Widerrufung des bereitgestellten Zugriffs auf BCSI für die in CIP-004-7 Tabelle R6 – Zugriffsmanagement für BES Cyber System Information – genannten „anwendbaren Systemen“ implementieren, die zusammen alle zutreffenden Anforderungsabschnitte in CIP-004-7 Tabelle R6 – Zugriffsmanagement für BES Cyber System Information – enthalten. Im Rahmen dieser Anforderung bezeichnet Zugang zu BCSI die Fähigkeit einer Person, BCSI zu erhalten und zu nutzen. Der bereitges	s-3 bucket-policy-grantee-check	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie s3_bucket_policy_grantee_check aktivieren. Diese Regel prüft, ob der vom Amazon S3 S3-Bucket gewährte Zugriff durch die von Ihnen bereitgestellten AWS Principals, Verbundbenutzer, Service Principals, IP-Adressen oder Amazon Virtual Private Cloud (Amazon VPC) IDs eingeschränkt ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen
	tellte Zugriff ist als Ergebnis der spezifischen Maßnahmen zu betrachten, die ergriffen wurden, um einer oder mehreren Personen die Möglichkeit zu geben, auf BCSI zuzugreifen (kann beispielsweise physische Schlüssel oder Zugangskarten, Benutzer und zugehörige Rechte und Privilegien, Verschlüsselungsschlüssel beinhalten). Abschnitt 6.1: Erteilen Sie Autorisierungen vor der Bereitstellung (sofern nicht bereits gemäß Abschnitt 4.1 autorisiert) nach Bedarf, wie von der verantwortlichen Stelle festgelegt, mit Ausnahme von CIP unter außergewöhnlichen Umständen: 6.1.1. Bereitgestellter elektronischer Zugriff auf elektronische BCSI		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen
CIP-011-3-R1 Abschnitt 1.2	Jede verantwortliche Stelle muss ein oder mehrere dokumentierte Informationsschutzprogramme implementieren, die zusammen alle anwendbaren Anforderungsabschnitte in CIP-011-3, Tabelle R1 – Informationsschutz – enthalten. Abschnitt 1.2: Methode(n) zum Schutz und zur sicheren Handhabung von BCSI, um das Risiko einer Gefährdung der Vertraulichkeit zu minimieren.	dms-replication-not-public	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass auf DMS-Replikationsinstanzen nicht öffentlich zugegriffen werden kann. DMS-Replikations-Instances können vertrauliche Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen
CIP-011-3-R1 Abschnitt 1.2	Jede verantwortliche Stelle muss ein oder mehrere dokumentierte Informationsschutzprogramme implementieren, die zusammen alle anwendbaren Anforderungsabschnitte in CIP-011-3, Tabelle R1 – Informationsschutz – enthalten. Abschnitt 1.2: Methode(n) zum Schutz und zur sicheren Handhabung von BCSI, um das Risiko einer Gefährdung der Vertraulichkeit zu minimieren.	ebs-snapshot-public-restorable-überprüfen	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass EBS-Snapshots nicht öffentlich wiederherstellbar sind. EBS-Volume-Snapshots können vertrauliche Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen
CIP-011-3-R1 Abschnitt 1.2	Jede verantwortliche Stelle muss ein oder mehrere dokumentierte Informationsschutzprogramme implementieren, die zusammen alle anwendbaren Anforderungsabschnitte in CIP-011-3, Tabelle R1 – Informationsschutz – enthalten. Abschnitt 1.2: Methode(n) zum Schutz und zur sicheren Handhabung von BCSI, um das Risiko einer Gefährdung der Vertraulichkeit zu minimieren.	iam-user-unused-credentials-überprüfen	AWS Identity and Access Management (IAM) kann Ihnen bei Zugriffsberechtigungen und Autorisierungen helfen, indem es nach IAM-Passwörtern und Zugriffsschlüsseln sucht, die für einen bestimmten Zeitraum nicht verwendet wurden. Wenn ungenutzte Anmeldeinformationen identifiziert werden, müssen Sie sie deaktivieren und/oder entfernen, da dies gegen das Prinzip der geringsten Berechtigung verstoßen könnte. Für diese Regel müssen Sie einen Wert für das maxCredentialUsage Alter festlegen (Standardkonfiguration: 90). Der tatsächliche Wert muss den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen
CIP-011-3-R1 Abschnitt 1.2	Jede verantwortliche Stelle muss ein oder mehrere dokumentierte Informationsschutzprogramme implementieren, die zusammen alle anwendbaren Anforderungsabschnitte in CIP-011-3, Tabelle R1 – Informationsschutz – enthalten. Abschnitt 1.2: Methode(n) zum Schutz und zur sicheren Handhabung von BCSI, um das Risiko einer Gefährdung der Vertraulichkeit zu minimieren.	lambda-function-public-access-verboten	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass AWS Lambda-Funktionen nicht öffentlich zugänglich sind. Der öffentliche Zugriff kann möglicherweise die Verfügbarkeit von Ressourcen beeinträchtigen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen
CIP-011-3-R1 Abschnitt 1.2	Jede verantwortliche Stelle muss ein oder mehrere dokumentierte Informationsschutzprogramme implementieren, die zusammen alle anwendbaren Anforderungsabschnitte in CIP-011-3, Tabelle R1 – Informationsschutz – enthalten. Abschnitt 1.2: Methode(n) zum Schutz und zur sicheren Handhabung von BCSI, um das Risiko einer Gefährdung der Vertraulichkeit zu minimieren.	rds-instance-public-access-überprüfen	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Relational Database Service (Amazon RDS) -Instances nicht öffentlich sind. Amazon-RDS-Datenbank-Instances können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen
CIP-011-3-R1 Abschnitt 1.2	Jede verantwortliche Stelle muss ein oder mehrere dokumentierte Informationsschutzprogramme implementieren, die zusammen alle anwendbaren Anforderungsabschnitte in CIP-011-3, Tabelle R1 – Informationsschutz – enthalten. Abschnitt 1.2: Methode(n) zum Schutz und zur sicheren Handhabung von BCSI, um das Risiko einer Gefährdung der Vertraulichkeit zu minimieren.	rds-snapshots-public-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Relational Database Service (Amazon RDS) -Instances nicht öffentlich sind. Amazon-RDS-Datenbank-Instances können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen
CIP-011-3-R1 Abschnitt 1.2	Jede verantwortliche Stelle muss ein oder mehrere dokumentierte Informationsschutzprogramme implementieren, die zusammen alle anwendbaren Anforderungsabschnitte in CIP-011-3, Tabelle R1 – Informationsschutz – enthalten. Abschnitt 1.2: Methode(n) zum Schutz und zur sicheren Handhabung von BCSI, um das Risiko einer Gefährdung der Vertraulichkeit zu minimieren.	redshift-cluster-public-access-überprüfen	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Redshift Redshift-Cluster nicht öffentlich sind. Amazon-Redshift-Cluster können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen
CIP-011-3-R1 Abschnitt 1.2	Jede verantwortliche Stelle muss ein oder mehrere dokumentierte Informationsschutzprogramme implementieren, die zusammen alle anwendbaren Anforderungsabschnitte in CIP-011-3, Tabelle R1 – Informationsschutz – enthalten. Abschnitt 1.2: Methode(n) zum Schutz und zur sicheren Handhabung von BCSI, um das Risiko einer Gefährdung der Vertraulichkeit zu minimieren.	s3- -Block-periodisch account-level-public-access	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Simple Storage Service (Amazon S3) -Buckets nicht öffentlich zugänglich sind. Diese Regel trägt dazu bei, sensible Daten vor unbefugten Remote-Benutzern zu schützen, indem sie den öffentlichen Zugriff verhindert. Mit dieser Regel können Sie optional die Parameter ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) und restrictPublicBuckets Parameter (Config Default: True) festlegen. Die tatsächlichen Werte müssen den Richtlini

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen
			en Ihrer Organisation entsprechen.
CIP-011-3-R1 Abschnitt 1.2	Jede verantwortliche Stelle muss ein oder mehrere dokumentierte Informationsschutzprogramme implementieren, die zusammen alle anwendbaren Anforderungsabschnitte in CIP-011-3, Tabelle R1 – Informationsschutz – enthalten. Abschnitt 1.2: Methode(n) zum Schutz und zur sicheren Handhabung von BCSI, um das Risiko einer Gefährdung der Vertraulichkeit zu minimieren.	sagemaker-notebook-no-direct-Internetzugang	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass SageMaker Amazon-Notebooks keinen direkten Internetzugang zulassen. Indem Sie direkten Internetzugang blockieren, vermeiden Sie, dass unbefugte Benutzer auf sensible Daten zugreifen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen
CIP-011-3-R1 Abschnitt 1.2	Jede verantwortliche Stelle muss ein oder mehrere dokumentierte Informationsschutzprogramme implementieren, die zusammen alle anwendbaren Anforderungsabschnitte in CIP-011-3, Tabelle R1 – Informationsschutz – enthalten. Abschnitt 1.2: Methode(n) zum Schutz und zur sicheren Handhabung von BCSI, um das Risiko einer Gefährdung der Vertraulichkeit zu minimieren.	acm-certificate-expiration-check	Stellen Sie sicher, dass die Netzwerkintegrität geschützt ist, indem Sie sicherstellen, dass X509-Zertifikate von AWS ACM ausgestellt werden. Diese Zertifikate müssen gültig und dürfen nicht abgelaufen sein. Für diese Regel ist ein Wert für erforderlich daysToExpiration (Wert für bewährte AWS Grundregeln für Sicherheit: 90). Der tatsächliche Wert muss den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen
CIP-011-3-R1 Abschnitt 1.2	Jede verantwortliche Stelle muss ein oder mehrere dokumentierte Informationsschutzprogramme implementieren, die zusammen alle anwendbaren Anforderungsabschnitte in CIP-011-3, Tabelle R1 – Informationsschutz – enthalten. Abschnitt 1.2: Methode(n) zum Schutz und zur sicheren Handhabung von BCSI, um das Risiko einer Gefährdung der Vertraulichkeit zu minimieren.	alb-http-drop-invalid-Header-aktiviert	Stellen Sie sicher, dass Ihre Elastic Load Balancers (ELB) so konfiguriert sind, dass sie HTTP-Header löschen. Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen
CIP-011-3-R1 Abschnitt 1.2	Jede verantwortliche Stelle muss ein oder mehrere dokumentierte Informationsschutzprogramme implementieren, die zusammen alle anwendbaren Anforderungsabschnitte in CIP-011-3, Tabelle R1 – Informationsschutz – enthalten. Abschnitt 1.2: Methode(n) zum Schutz und zur sicheren Handhabung von BCSI, um das Risiko einer Gefährdung der Vertraulichkeit zu minimieren.	alb-http-to-https-Umleitungsprüfung	Um Daten während der Übertragung zu schützen, stellen Sie sicher, dass Ihr Application Load Balancer unverschlüsselte HTTP-Anfragen automatisch an HTTPS umleitet. Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen
CIP-011-3-R1 Abschnitt 1.2	Jede verantwortliche Stelle muss ein oder mehrere dokumentierte Informationsschutzprogramme implementieren, die zusammen alle anwendbaren Anforderungsabschnitte in CIP-011-3, Tabelle R1 – Informationsschutz – enthalten. Abschnitt 1.2: Methode(n) zum Schutz und zur sicheren Handhabung von BCSI, um das Risiko einer Gefährdung der Vertraulichkeit zu minimieren.	api-gw-cache-enabled-und-verschlüsselt	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass die Verschlüsselung für den Cache Ihrer API-Gateway-Stufe aktiviert ist. Da für die API-Methode sensible Daten erfasst werden können, sollten Sie die Verschlüsselung von Daten im Ruhezustand aktivieren, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen
CIP-011-3-R1 Abschnitt 1.2	Jede verantwortliche Stelle muss ein oder mehrere dokumentierte Informationsschutzprogramme implementieren, die zusammen alle anwendbaren Anforderungsabschnitte in CIP-011-3, Tabelle R1 – Informationsschutz – enthalten. Abschnitt 1.2: Methode(n) zum Schutz und zur sicheren Handhabung von BCSI, um das Risiko einer Gefährdung der Vertraulichkeit zu minimieren.	cloud-trail-encryption-enabled	Zum Schutz von eventuell vorhandenen sensiblen Daten sowie Daten im Ruhezustand müssen Sie sicherstellen, dass die Verschlüsselung für Ihre AWS CloudTrail aktiviert ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen
CIP-011-3-R1 Abschnitt 1.2	Jede verantwortliche Stelle muss ein oder mehrere dokumentierte Informationsschutzprogramme implementieren, die zusammen alle anwendbaren Anforderungsabschnitte in CIP-011-3, Tabelle R1 – Informationsschutz – enthalten. Abschnitt 1.2: Methode(n) zum Schutz und zur sicheren Handhabung von BCSI, um das Risiko einer Gefährdung der Vertraulichkeit zu minimieren.	cloudwatch-log-group-encrypted	Um sensible Daten im Speicher zu schützen, stellen Sie sicher, dass die Verschlüsselung für Ihre Amazon CloudWatch Log Groups aktiviert ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen
CIP-011-3-R1 Abschnitt 1.2	Jede verantwortliche Stelle muss ein oder mehrere dokumentierte Informationsschutzprogramme implementieren, die zusammen alle anwendbaren Anforderungsabschnitte in CIP-011-3, Tabelle R1 – Informationsschutz – enthalten. Abschnitt 1.2: Methode(n) zum Schutz und zur sicheren Handhabung von BCSI, um das Risiko einer Gefährdung der Vertraulichkeit zu minimieren.	cmk-backing-key-rotation-aktiviert	Aktivieren Sie die Schlüsselrotation, um sicherzustellen, dass Schlüssel rotiert werden, sobald sie das Ende ihrer Kryptoperiode erreicht haben.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen
CIP-011-3-R1 Abschnitt 1.2	Jede verantwortliche Stelle muss ein oder mehrere dokumentierte Informationsschutzprogramme implementieren, die zusammen alle anwendbaren Anforderungsabschnitte in CIP-011-3, Tabelle R1 – Informationsschutz – enthalten. Abschnitt 1.2: Methode(n) zum Schutz und zur sicheren Handhabung von BCSI, um das Risiko einer Gefährdung der Vertraulichkeit zu minimieren.	dynamodb-table-encrypted-kms	Stellen Sie sicher, dass die Verschlüsselung für Ihre Amazon-DynamoDB-Tabellen aktiviert ist. Um eventuell vorhandene sensible Daten im Ruhezustand in diesen Tabellen zu schützen, müssen Sie die Verschlüsselung von Daten im Ruhezustand aktivieren. Standardmäßig werden DynamoDB-Tabellen mit einem AWS eigenen Kundenhauptschlüssel (CMK) verschlüselt.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen
CIP-011-3-R1 Abschnitt 1.2	Jede verantwortliche Stelle muss ein oder mehrere dokumentierte Informationsschutzprogramme implementieren, die zusammen alle anwendbaren Anforderungsabschnitte in CIP-011-3, Tabelle R1 – Informationsschutz – enthalten. Abschnitt 1.2: Methode(n) zum Schutz und zur sicheren Handhabung von BCSI, um das Risiko einer Gefährdung der Vertraulichkeit zu minimieren.	ec2- ebs-encryption-by-default	Zum Schutz von Daten im Ruhezustand müssen Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon Elastic Block Store (Amazon EBS)-Volumes aktiviert ist. Da sensible Daten auch im Ruhezustand vorhanden sein können, sollten Sie die Verschlüsselung im Ruhezustand aktivieren, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen
CIP-011-3-R1 Abschnitt 1.2	Jede verantwortliche Stelle muss ein oder mehrere dokumentierte Informationsschutzprogramme implementieren, die zusammen alle anwendbaren Anforderungsabschnitte in CIP-011-3, Tabelle R1 – Informationsschutz – enthalten. Abschnitt 1.2: Methode(n) zum Schutz und zur sicheren Handhabung von BCSI, um das Risiko einer Gefährdung der Vertraulichkeit zu minimieren.	ecr-private-image-scanning-aktiviert	Der Amazon Elastic Container Repository (ECR)-Image-Scan unterstützt die Identifizierung von Software-Schwachstellen in Ihren Container-Images. Durch die Aktivierung von Image-Scans in ECR-Repositorys werden die Integrität und Sicherheit der gespeicherten Images mit einer zusätzlichen Überprüfungsebene verbessert.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen
CIP-011-3-R1 Abschnitt 1.2	Jede verantwortliche Stelle muss ein oder mehrere dokumentierte Informationsschutzprogramme implementieren, die zusammen alle anwendbaren Anforderungsabschnitte in CIP-011-3, Tabelle R1 – Informationsschutz – enthalten. Abschnitt 1.2: Methode(n) zum Schutz und zur sicheren Handhabung von BCSI, um das Risiko einer Gefährdung der Vertraulichkeit zu minimieren.	ecr-private-tag-immutability-aktiviert	Aktivieren Sie die Unveränderlichkeit von Tags im Elastic Container Repository (ECR), um zu verhindern, dass Image-Tags in Ihren ECR-Images überschrieben werden. Bisher konnten Tags überschrieben werden, was manuelle Methoden zur eindeutigen Identifizierung eines Images erforderte.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen
CIP-011-3-R1 Abschnitt 1.2	Jede verantwortliche Stelle muss ein oder mehrere dokumentierte Informationsschutzprogramme implementieren, die zusammen alle anwendbaren Anforderungsabschnitte in CIP-011-3, Tabelle R1 – Informationsschutz – enthalten. Abschnitt 1.2: Methode(n) zum Schutz und zur sicheren Handhabung von BCSI, um das Risiko einer Gefährdung der Vertraulichkeit zu minimieren.	ecs-containers-readonly-access	Die Aktivierung des schreibgeschützten Zugriffs auf Amazon Elastic Container Service (ECS)-Container kann dazu beitragen, das Prinzip der geringsten Berechtigung einzuhalten. Diese Option kann Angriffsvektoren reduzieren, da das Dateisystem der Container-Instance nur geändert werden kann, wenn es über ausdrückliche Lese- und Schreibberechtigungen verfügt.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen
CIP-011-3-R1 Abschnitt 1.2	Jede verantwortliche Stelle muss ein oder mehrere dokumentierte Informationsschutzprogramme implementieren, die zusammen alle anwendbaren Anforderungsabschnitte in CIP-011-3, Tabelle R1 – Informationsschutz – enthalten. Abschnitt 1.2: Methode(n) zum Schutz und zur sicheren Handhabung von BCSI, um das Risiko einer Gefährdung der Vertraulichkeit zu minimieren.	efs-encrypted-check	Aktivieren Sie die Verschlüsselung für Ihr Amazon Elastic File System (EFS), um eventuell vorhandene sensible Daten sowie Daten im Ruhezustand zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen
CIP-011-3-R1 Abschnitt 1.2	Jede verantwortliche Stelle muss ein oder mehrere dokumentierte Informationsschutzprogramme implementieren, die zusammen alle anwendbaren Anforderungsabschnitte in CIP-011-3, Tabelle R1 – Informationsschutz – enthalten. Abschnitt 1.2: Methode(n) zum Schutz und zur sicheren Handhabung von BCSI, um das Risiko einer Gefährdung der Vertraulichkeit zu minimieren.	elasticsearch-encrypted-at-rest	Da sensible Daten vorhanden sein können und um Daten im Ruhezustand zu schützen, sollten Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon OpenSearch Service (OpenSearch Service) -Domains aktiviert ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen
CIP-011-3-R1 Abschnitt 1.2	Jede verantwortliche Stelle muss ein oder mehrere dokumentierte Informationsschutzprogramme implementieren, die zusammen alle anwendbaren Anforderungsabschnitte in CIP-011-3, Tabelle R1 – Informationsschutz – enthalten. Abschnitt 1.2: Methode(n) zum Schutz und zur sicheren Handhabung von BCSI, um das Risiko einer Gefährdung der Vertraulichkeit zu minimieren.	elasticsearch-node-to-node-Verschlüsselungsprüfung	Stellen Sie sicher, dass die node-to-node Verschlüsselung für Amazon OpenSearch Service aktiviert ist. Node-to-nodeVerschlüsselung ermöglicht die TLS 1.2-Verschlüsselung für die gesamte Kommunikation innerhalb der Amazon Virtual Private Cloud (Amazon VPC). Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen
CIP-011-3-R1 Abschnitt 1.2	Jede verantwortliche Stelle muss ein oder mehrere dokumentierte Informationsschutzprogramme implementieren, die zusammen alle anwendbaren Anforderungsabschnitte in CIP-011-3, Tabelle R1 – Informationsschutz – enthalten. Abschnitt 1.2: Methode(n) zum Schutz und zur sicheren Handhabung von BCSI, um das Risiko einer Gefährdung der Vertraulichkeit zu minimieren.	elb-acm-certificate-required	Zum Schutz von eventuell vorhandenen sensiblen Daten sowie von Daten während der Übertragung muss die Verschlüsselung für Ihr Elastic Load Balancing aktiviert sein. Verwenden Sie AWS Certificate Manager, um öffentliche und private SSL/TLS-Zertifikate mit AWS Diensten und internen Ressourcen zu verwalten, bereitzustellen und bereitzustellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen
CIP-011-3-R1 Abschnitt 1.2	Jede verantwortliche Stelle muss ein oder mehrere dokumentierte Informationsschutzprogramme implementieren, die zusammen alle anwendbaren Anforderungsabschnitte in CIP-011-3, Tabelle R1 – Informationsschutz – enthalten. Abschnitt 1.2: Methode(n) zum Schutz und zur sicheren Handhabung von BCSI, um das Risiko einer Gefährdung der Vertraulichkeit zu minimieren.	elb-tls-https-listeners-nur	Stellen Sie sicher, dass Ihre Elastic Load Balancer (ELBs) mit SSL- oder HTTPS-Listenern konfiguriert sind. Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen
CIP-011-3-R1 Abschnitt 1.2	Jede verantwortliche Stelle muss ein oder mehrere dokumentierte Informationsschutzprogramme implementieren, die zusammen alle anwendbaren Anforderungsabschnitte in CIP-011-3, Tabelle R1 – Informationsschutz – enthalten. Abschnitt 1.2: Methode(n) zum Schutz und zur sicheren Handhabung von BCSI, um das Risiko einer Gefährdung der Vertraulichkeit zu minimieren.	encrypted-volumes	Aktivieren Sie die Verschlüsselung für Ihre Amazon-Elastic-Block-Store (Amazon-EBS)-Volumes, um eventuell vorhandene sensible Daten sowie Daten im Ruhezustand zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen
CIP-011-3-R1 Abschnitt 1.2	Jede verantwortliche Stelle muss ein oder mehrere dokumentierte Informationsschutzprogramme implementieren, die zusammen alle anwendbaren Anforderungsabschnitte in CIP-011-3, Tabelle R1 – Informationsschutz – enthalten. Abschnitt 1.2: Methode(n) zum Schutz und zur sicheren Handhabung von BCSI, um das Risiko einer Gefährdung der Vertraulichkeit zu minimieren.	kinesis-stream-encrypted	Aktivieren Sie die Verschlüsselung für Ihre Amazon-Kinesis-Streams, um eventuell vorhandene sensible Daten sowie Daten im Ruhezustand zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen
CIP-011-3-R1 Abschnitt 1.2	Jede verantwortliche Stelle muss ein oder mehrere dokumentierte Informationsschutzprogramme implementieren, die zusammen alle anwendbaren Anforderungsabschnitte in CIP-011-3, Tabelle R1 – Informationsschutz – enthalten. Abschnitt 1.2: Methode(n) zum Schutz und zur sicheren Handhabung von BCSI, um das Risiko einer Gefährdung der Vertraulichkeit zu minimieren.	kms-cmk-not-scheduled-zum Löschen	Um Daten im Ruhezustand zu schützen, sollten Sie sicherstellen, dass die für den Kunden erforderlichen Masterschlüssel (CMKs) nicht für das Löschen im AWS Key Management Service (AWS KMS) vorgesehen sind. Da Schlüssel manchmal gelöscht werden müssen, können Sie mit dieser Regel alle zu löschenden Schlüssel überprüfen, falls ein Schlüssel versehentlich zur Löschung vorgemerkt wurde.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen
CIP-011-3-R1 Abschnitt 1.2	Jede verantwortliche Stelle muss ein oder mehrere dokumentierte Informationsschutzprogramme implementieren, die zusammen alle anwendbaren Anforderungsabschnitte in CIP-011-3, Tabelle R1 – Informationsschutz – enthalten. Abschnitt 1.2: Methode(n) zum Schutz und zur sicheren Handhabung von BCSI, um das Risiko einer Gefährdung der Vertraulichkeit zu minimieren.	opensearch-audit-logging-enabled	Stellen Sie sicher, dass die Audit-Protokollierung für Ihre Amazon OpenSearch Service-Domains aktiviert ist. Mit der Audit-Protokollierung können Sie Benutzeraktivitäten auf Ihren OpenSearch Domains verfolgen, einschließlich erfolgreicher und fehlgeschlagener Authentifizierungen OpenSearch, Anfragen an, Indexänderungen und eingehende Suchanfragen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen
CIP-011-3-R1 Abschnitt 1.2	Jede verantwortliche Stelle muss ein oder mehrere dokumentierte Informationsschutzprogramme implementieren, die zusammen alle anwendbaren Anforderungsabschnitte in CIP-011-3, Tabelle R1 – Informationsschutz – enthalten. Abschnitt 1.2: Methode(n) zum Schutz und zur sicheren Handhabung von BCSI, um das Risiko einer Gefährdung der Vertraulichkeit zu minimieren.	opensearch-encrypted-at-rest	Da sensible Daten vorhanden sein können und um Daten im Ruhezustand zu schützen, sollten Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon OpenSearch Service-Domains aktiviert ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen
CIP-011-3-R1 Abschnitt 1.2	Jede verantwortliche Stelle muss ein oder mehrere dokumentierte Informationsschutzprogramme implementieren, die zusammen alle anwendbaren Anforderungsabschnitte in CIP-011-3, Tabelle R1 – Informationsschutz – enthalten. Abschnitt 1.2: Methode(n) zum Schutz und zur sicheren Handhabung von BCSI, um das Risiko einer Gefährdung der Vertraulichkeit zu minimieren.	opensearch-https-required	Da sensible Daten existieren können und um Daten während der Übertragung zu schützen, sollten Sie sicherstellen, dass HTTPS für Verbindungen zu Ihren Amazon OpenSearch Service-Domains aktiviert ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen
CIP-011-3-R1 Abschnitt 1.2	Jede verantwortliche Stelle muss ein oder mehrere dokumentierte Informationsschutzprogramme implementieren, die zusammen alle anwendbaren Anforderungsabschnitte in CIP-011-3, Tabelle R1 – Informationsschutz – enthalten. Abschnitt 1.2: Methode(n) zum Schutz und zur sicheren Handhabung von BCSI, um das Risiko einer Gefährdung der Vertraulichkeit zu minimieren.	opensearch-in-vpc-only	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass sich Amazon OpenSearch Service-Domains innerhalb einer Amazon Virtual Private Cloud (Amazon VPC) befinden. Eine Amazon OpenSearch Service-Domain innerhalb einer Amazon VPC ermöglicht die sichere Kommunikation zwischen Amazon OpenSearch und anderen Diensten innerhalb der Amazon VPC, ohne dass ein Internet-Gateway, ein NAT-Gerät oder eine VPN-Verbindung erforderlich ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen
CIP-011-3-R1 Abschnitt 1.2	Jede verantwortliche Stelle muss ein oder mehrere dokumentierte Informationsschutzprogramme implementieren, die zusammen alle anwendbaren Anforderungsabschnitte in CIP-011-3, Tabelle R1 – Informationsschutz – enthalten. Abschnitt 1.2: Methode(n) zum Schutz und zur sicheren Handhabung von BCSI, um das Risiko einer Gefährdung der Vertraulichkeit zu minimieren.	opensearch-logs-to-cloudwatch	Stellen Sie sicher, dass für Amazon OpenSearch Service-Domains Fehlerprotokolle aktiviert und zur Aufbewahrung und Beantwortung an Amazon CloudWatch Logs gestreamt werden. Domain-Fehlerprotokolle sind bei Sicherheits- und Zugriffsprüfungen sowie bei der Diagnose von Verfügbarkeitsproblemen nützlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen
CIP-011-3-R1 Abschnitt 1.2	Jede verantwortliche Stelle muss ein oder mehrere dokumentierte Informationsschutzprogramme implementieren, die zusammen alle anwendbaren Anforderungsabschnitte in CIP-011-3, Tabelle R1 – Informationsschutz – enthalten. Abschnitt 1.2: Methode(n) zum Schutz und zur sicheren Handhabung von BCSI, um das Risiko einer Gefährdung der Vertraulichkeit zu minimieren.	opensearch-node-to-node-Verschlüsselungsprüfung	Stellen Sie sicher, dass die node-to-node Verschlüsselung für Amazon OpenSearch Service aktiviert ist. Node-to-nodeVerschlüsselung ermöglicht die TLS 1.2-Verschlüsselung für die gesamte Kommunikation innerhalb der Amazon Virtual Private Cloud (Amazon VPC). Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen
CIP-011-3-R1 Abschnitt 1.2	Jede verantwortliche Stelle muss ein oder mehrere dokumentierte Informationsschutzprogramme implementieren, die zusammen alle anwendbaren Anforderungsabschnitte in CIP-011-3, Tabelle R1 – Informationsschutz – enthalten. Abschnitt 1.2: Methode(n) zum Schutz und zur sicheren Handhabung von BCSI, um das Risiko einer Gefährdung der Vertraulichkeit zu minimieren.	rds-snapshot-encrypted	Stellen Sie sicher, dass die Verschlüsselung für Ihre Amazon Relational Database Service (Amazon RDS)-Snapshots aktiviert ist. Da sensible Daten auch im Ruhezustand vorhanden sein können, sollten Sie die Verschlüsselung im Ruhezustand aktivieren, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen
CIP-011-3-R1 Abschnitt 1.2	Jede verantwortliche Stelle muss ein oder mehrere dokumentierte Informationsschutzprogramme implementieren, die zusammen alle anwendbaren Anforderungsabschnitte in CIP-011-3, Tabelle R1 – Informationsschutz – enthalten. Abschnitt 1.2: Methode(n) zum Schutz und zur sicheren Handhabung von BCSI, um das Risiko einer Gefährdung der Vertraulichkeit zu minimieren.	rds-storage-encrypted	Zum Schutz von Daten im Ruhezustand müssen Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon Relational Database Service (Amazon RDS)-Instances aktiviert ist. Um eventuell vorhandene sensible Daten im Ruhezustand in Amazon-RDS-Instances zu schützen, muss die Verschlüsselung von Daten im Ruhezustand aktiviert sein.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen
CIP-011-3-R1 Abschnitt 1.2	Jede verantwortliche Stelle muss ein oder mehrere dokumentierte Informationsschutzprogramme implementieren, die zusammen alle anwendbaren Anforderungsabschnitte in CIP-011-3, Tabelle R1 – Informationsschutz – enthalten. Abschnitt 1.2: Methode(n) zum Schutz und zur sicheren Handhabung von BCSI, um das Risiko einer Gefährdung der Vertraulichkeit zu minimieren.	redshift-audit-logging-enabled	Aktivieren Sie die Prüfungsprotokollierung, um Informationen über Verbindungen und Benutzeraktivitäten in Ihrem Amazon-Redshift-Cluster zu erfassen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen
CIP-011-3-R1 Abschnitt 1.2	Jede verantwortliche Stelle muss ein oder mehrere dokumentierte Informationsschutzprogramme implementieren, die zusammen alle anwendbaren Anforderungsabschnitte in CIP-011-3, Tabelle R1 – Informationsschutz – enthalten. Abschnitt 1.2: Methode(n) zum Schutz und zur sicheren Handhabung von BCSI, um das Risiko einer Gefährdung der Vertraulichkeit zu minimieren.	redshift-cluster-configuration-check	Um Daten im Ruhezustand zu schützen, muss die Verschlüsselung für Ihre Amazon-Redshift-Cluster aktiviert sein. Sie müssen auch sicherstellen, dass die erforderlichen Konfigurationen auf Amazon-Redshift-Clustern bereitgestellt werden. Die Prüfungsprotokollierung muss aktiviert sein, um Informationen zu Verbindungen und Benutzeraktivitäten in der Datenbank bereitzustellen. Diese Regel erfordert, dass ein Wert für clusterDbEncrypted (Config Default: TRUE) und LoggingEnabled (Config Default: TRUE) gesetzt ist. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen
CIP-011-3-R1 Abschnitt 1.2	Jede verantwortliche Stelle muss ein oder mehrere dokumentierte Informationsschutzprogramme implementieren, die zusammen alle anwendbaren Anforderungsabschnitte in CIP-011-3, Tabelle R1 – Informationsschutz – enthalten. Abschnitt 1.2: Methode(n) zum Schutz und zur sicheren Handhabung von BCSI, um das Risiko einer Gefährdung der Vertraulichkeit zu minimieren.	redshift-require-tls-ssl	Stellen Sie sicher, dass Ihre Amazon-Redshift-Cluster eine TLS/SSL-Verschlüsselung erfordern, um eine Verbindung zu SQL-Clients herzustellen. Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen
CIP-011-3-R1 Abschnitt 1.2	Jede verantwortliche Stelle muss ein oder mehrere dokumentierte Informationsschutzprogramme implementieren, die zusammen alle anwendbaren Anforderungsabschnitte in CIP-011-3, Tabelle R1 – Informationsschutz – enthalten. Abschnitt 1.2: Methode(n) zum Schutz und zur sicheren Handhabung von BCSI, um das Risiko einer Gefährdung der Vertraulichkeit zu minimieren.	s3-aktiviert bucket-server-side-encryption	Zum Schutz von Daten im Ruhezustand müssen Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon Simple Storage Service (Amazon S3)-Buckets aktiviert ist. Um eventuell vorhandene sensible Daten im Ruhezustand in Amazon-S3-Buckets zu schützen, muss die Verschlüsselung aktiviert sein.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen
CIP-011-3-R1 Abschnitt 1.2	Jede verantwortliche Stelle muss ein oder mehrere dokumentierte Informationsschutzprogramme implementieren, die zusammen alle anwendbaren Anforderungsabschnitte in CIP-011-3, Tabelle R1 – Informationsschutz – enthalten. Abschnitt 1.2: Methode(n) zum Schutz und zur sicheren Handhabung von BCSI, um das Risiko einer Gefährdung der Vertraulichkeit zu minimieren.	s-3 bucket-ssl-requests-only	Um Daten während der Übertragung zu schützen, stellen Sie sicher, dass Ihre Amazon Simple Storage Service (Amazon S3)-Buckets Anfragen zur Verwendung von Secure Socket Layer (SSL)-Buckets erfordern. Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen
CIP-011-3-R1 Abschnitt 1.2	Jede verantwortliche Stelle muss ein oder mehrere dokumentierte Informationsschutzprogramme implementieren, die zusammen alle anwendbaren Anforderungsabschnitte in CIP-011-3, Tabelle R1 – Informationsschutz – enthalten. Abschnitt 1.2: Methode(n) zum Schutz und zur sicheren Handhabung von BCSI, um das Risiko einer Gefährdung der Vertraulichkeit zu minimieren.	s-3 default-encryption-kms	Stellen Sie sicher, dass die Verschlüsselung für Ihre Amazon Simple Storage Service (Amazon S3)-Buckets aktiviert ist. Um eventuell vorhandene sensible Daten im Ruhezustand in einem Amazon-S3-Bucket zu schützen, muss die Verschlüsselung aktiviert sein.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen
CIP-011-3-R1 Abschnitt 1.2	Jede verantwortliche Stelle muss ein oder mehrere dokumentierte Informationsschutzprogramme implementieren, die zusammen alle anwendbaren Anforderungsabschnitte in CIP-011-3, Tabelle R1 – Informationsschutz – enthalten. Abschnitt 1.2: Methode(n) zum Schutz und zur sicheren Handhabung von BCSI, um das Risiko einer Gefährdung der Vertraulichkeit zu minimieren.	s-3 event-notifications-enabled	Amazon-S3-Ereignisbenachrichtigungen können das zuständige Personal über versehentliche oder vorsätzliche Änderungen an Ihren Bucket-Objekten informieren. Zu den Warnen gehören beispielsweise: Erstellung eines neuen Objekts, Entfernung eines Objekts, Wiederherstellung eines Objekts, verloren gegangene und replizierte Objekte.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen
CIP-011-3-R1 Abschnitt 1.2	Jede verantwortliche Stelle muss ein oder mehrere dokumentierte Informationsschutzprogramme implementieren, die zusammen alle anwendbaren Anforderungsabschnitte in CIP-011-3, Tabelle R1 – Informationsschutz – enthalten. Abschnitt 1.2: Methode(n) zum Schutz und zur sicheren Handhabung von BCSI, um das Risiko einer Gefährdung der Vertraulichkeit zu minimieren.	s-3 lifecycle-policy-check	Mit Amazon-S3-Lebenszyklusregeln können Sie Aktionen definieren, die Amazon S3 während der Lebensdauer eines Objekts ausführen soll (z. B. die Überführung von Objekten in eine andere Speicherklasse, ihre Archivierung oder Löschung nach einem bestimmten Zeitraum).

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen
CIP-011-3-R1 Abschnitt 1.2	Jede verantwortliche Stelle muss ein oder mehrere dokumentierte Informationsschutzprogramme implementieren, die zusammen alle anwendbaren Anforderungsabschnitte in CIP-011-3, Tabelle R1 – Informationsschutz – enthalten. Abschnitt 1.2: Methode(n) zum Schutz und zur sicheren Handhabung von BCSI, um das Risiko einer Gefährdung der Vertraulichkeit zu minimieren.	sagemaker-endpoint-configuration-kms-key-konfiguriert	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass die Verschlüsselung mit dem AWS Key Management Service (AWS KMS) für Ihren Endpunkt aktiviert ist. SageMaker Da sensible Daten auf dem SageMaker Endgerät gespeichert werden können, sollten Sie die Verschlüsselung im Ruhezustand aktivieren, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen
CIP-011-3-R1 Abschnitt 1.2	Jede verantwortliche Stelle muss ein oder mehrere dokumentierte Informationsschutzprogramme implementieren, die zusammen alle anwendbaren Anforderungsabschnitte in CIP-011-3, Tabelle R1 – Informationsschutz – enthalten. Abschnitt 1.2: Methode(n) zum Schutz und zur sicheren Handhabung von BCSI, um das Risiko einer Gefährdung der Vertraulichkeit zu minimieren.	sagemaker-notebook-instance-kms-schlüsselkonfiguriert	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass die Verschlüsselung mit dem AWS Key Management Service (AWS KMS) für Ihr Notebook aktiviert ist. SageMaker Da vertrauliche Daten im SageMaker Notebook gespeichert werden können, sollten Sie die Verschlüsselung im Ruhezustand aktivieren, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen
CIP-011-3-R1 Abschnitt 1.2	Jede verantwortliche Stelle muss ein oder mehrere dokumentierte Informationsschutzprogramme implementieren, die zusammen alle anwendbaren Anforderungsabschnitte in CIP-011-3, Tabelle R1 – Informationsschutz – enthalten. Abschnitt 1.2: Methode(n) zum Schutz und zur sicheren Handhabung von BCSI, um das Risiko einer Gefährdung der Vertraulichkeit zu minimieren.	sns-encrypted-kms	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass Ihre Amazon Simple Notification Service (Amazon SNS) -Themen mit dem AWS Key Management Service (AWS KMS) verschlüsselt werden müssen. Um eventuell vorhandene sensible Daten im Ruhezustand in veröffentlichten Nachrichten zu schützen, muss die Verschlüsselung von Daten im Ruhezustand aktiviert sein.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen
CIP-011-3-R1 Abschnitt 1.2	Jede verantwortliche Stelle muss ein oder mehrere dokumentierte Informationsschutzprogramme implementieren, die zusammen alle anwendbaren Anforderungsabschnitte in CIP-011-3, Tabelle R1 – Informationsschutz – enthalten. Abschnitt 1.2: Methode(n) zum Schutz und zur sicheren Handhabung von BCSI, um das Risiko einer Gefährdung der Vertraulichkeit zu minimieren.	rds-cluster-default-admin-überprüfen	Da Standardbenutzernamen allgemein bekannt sind, kann eine Änderung der Standardbenutzernamen dazu beitragen, die Angriffsfläche für Ihre Datenbankcluster von Amazon Relational Database Service (Amazon RDS) zu reduzieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen
CIP-011-3-R1 Abschnitt 1.2	Jede verantwortliche Stelle muss ein oder mehrere dokumentierte Informationsschutzprogramme implementieren, die zusammen alle anwendbaren Anforderungsabschnitte in CIP-011-3, Tabelle R1 – Informationsschutz – enthalten. Abschnitt 1.2: Methode(n) zum Schutz und zur sicheren Handhabung von BCSI, um das Risiko einer Gefährdung der Vertraulichkeit zu minimieren.	rds-instance-default-admin-überprüfen	Da Standardbenutzernamen allgemein bekannt sind, kann eine Änderung der Standardbenutzernamen dazu beitragen, die Angriffsfläche für Ihre Datenbank-Instance(s) in Amazon Relational Database Service (Amazon RDS) zu reduzieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen
CIP-011-3-R1 Abschnitt 1.2	Jede verantwortliche Stelle muss ein oder mehrere dokumentierte Informationsschutzprogramme implementieren, die zusammen alle anwendbaren Anforderungsabschnitte in CIP-011-3, Tabelle R1 – Informationsschutz – enthalten. Abschnitt 1.2: Methode(n) zum Schutz und zur sicheren Handhabung von BCSI, um das Risiko einer Gefährdung der Vertraulichkeit zu minimieren.	redshift-default-admin-check	Da Standardbenutzernamen allgemein bekannt sind, kann eine Änderung der Standardbenutzernamen dazu beitragen, die Angriffsfläche für Ihre Amazon-Redshift-Cluster zu reduzieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen
CIP-011-3-R1 Abschnitt 1.2	Jede verantwortliche Stelle muss ein oder mehrere dokumentierte Informationsschutzprogramme implementieren, die zusammen alle anwendbaren Anforderungsabschnitte in CIP-011-3, Tabelle R1 – Informationsschutz – enthalten. Abschnitt 1.2: Methode(n) zum Schutz und zur sicheren Handhabung von BCSI, um das Risiko einer Gefährdung der Vertraulichkeit zu minimieren.	s3- bucket-acl-prohibited	Diese Regel prüft, ob Access Control Lists (ACLs) für die Zugriffskontrolle auf Amazon S3 S3-Buckets verwendet werden. ACLs sind veraltete Zugriffskontrollmechanismen für Amazon S3 S3-Buckets, die älter sind als AWS Identity and Access Management (IAM). Stattdessen empfiehlt es sich ACLs, IAM-Richtlinien oder S3-Bucket-Richtlinien zu verwenden, um den Zugriff auf Ihre S3-Buckets einfacher zu verwalten.

Vorlage

Die Vorlage ist verfügbar unter GitHub: Operational Best Practices for NERC CIP BCSI.

Bewährte Methoden für die Ausführung von NCSC-Cloud-Sicherheitsprinzipien

Konformitätspakete bieten ein allgemeines Compliance-Framework, das es Ihnen ermöglicht, mithilfe verwalteter oder benutzerdefinierter Regeln und Abhilfemaßnahmen Kontrollen zur Sicherheits-, Betriebs- oder Kostenoptimierung durchzuführen. AWS Config AWS Config Conformance Packs

dienen als Beispielvorlagen nicht dazu, die vollständige Einhaltung eines bestimmten Governance- oder Compliance-Standards sicherzustellen. Sie sind dafür verantwortlich, selbst zu beurteilen, ob Ihre Nutzung der Services den geltenden gesetzlichen und behördlichen Anforderungen entspricht.

Im Folgenden finden Sie ein Beispiel für eine Zuordnung zwischen den Cloud-Sicherheitsprinzipien des National Cyber Security Centre (NCSC) des Vereinigten Königreichs und den AWS verwalteten Konfigurationsregeln. Jede Config-Regel gilt für eine bestimmte AWS Ressource und bezieht sich auf eine oder mehrere Kontrollen der UK NCSC Cloud Security Principles. Eine Kontrolle gemäß den Cloud-Sicherheitsprinzipien des britischen NCSC kann mit mehreren Config-Regeln verknüpft werden. In der folgenden Tabelle finden Sie weitere Informationen und Anleitungen zu diesen Zuordnungen.

Diese beispielhafte Conformance-Pack-Vorlage enthält Zuordnungen zu Kontrollen gemäß den Cloud-Sicherheitsprinzipien des britischen NCSC (National Cyber Security Centre | Cloud-Sicherheitsprinzipien), wobei diese Informationen des öffentlichen Sektors unter der Open Government Licence v3.0 lizenziert sind. Der Zugriff auf die Open Government License ist hier möglich: Open Government Licence für Informationen des öffentlichen Sektors.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
1. Schutz von Daten während der Übertragung	Netzwerke, über die Benutzerdaten übertragen werden, sollten angemessen vor Manipulation und Eavesdropping geschützt werden.	elbv-2 acm-certificate-required	Zum Schutz von eventuell vorhandenen sensiblen Daten sowie von Daten während der Übertragung muss die Verschlüsselung für Ihr Elastic Load Balancing aktiviert sein. Verwenden Sie AWS Certificate Manager, um öffentliche und private SSL/TLS-Zertifikate mit AWS Diensten und internen Ressourcen zu verwalten,

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			bereitzustellen und bereitzustellen.
1. Schutz von Daten während der Übertragung	Netzwerke, über die Benutzerdaten übertragen werden, sollten angemessen vor Manipulation und Eavesdropping geschützt werden.	acm-certificate-expiration-check	Stellen Sie sicher, dass die Netzwerkintegrität geschützt ist, indem Sie sicherstellen, dass X509-Zertifikate von ACM ausgestellt werden. AWS Diese Zertifikate müssen gültig und dürfen nicht abgelaufen sein. Für diese Regel ist ein Wert für erforderlich daysToExpiration (Wert für bewährte AWS Grundregeln für Sicherheit: 90). Der tatsächliche Wert muss den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
1. Schutz von Daten während der Übertragung	Netzwerke, über die Benutzerdaten übertragen werden, sollten angemessen vor Manipulation und Eavesdropping geschützt werden.	alb-http-to-https-Umleitungsprüfung	Um Daten während der Übertragung zu schützen, stellen Sie sicher, dass Ihr Application Load Balancer unverschlüsselte HTTP-Anfragen automatisch an HTTPS umleitet. Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.
1. Schutz von Daten während der Übertragung	Netzwerke, über die Benutzerdaten übertragen werden, sollten angemessen vor Manipulation und Eavesdropping geschützt werden.	api-gw-ssl-enabled	Stellen Sie sicher, dass die REST-API-Stufen von Amazon API Gateway mit SSL-Zertifikaten konfiguriert sind, damit Backend-Systeme überprüfen können, ob Anforderungen von API Gateway stammen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
1. Schutz von Daten während der Übertragung	Netzwerke, über die Benutzerdaten übertragen werden, sollten angemessen vor Manipulation und Eavesdropping geschützt werden.	elasticsearch-node-to-node-Verschlüsselungsprüfung	Stellen Sie sicher, dass die node-to-node Verschlüsselung für Amazon OpenSearch Service aktiviert ist. Node-to-nodeVerschlüsselung ermöglicht die TLS 1.2-Verschlüsselung für die gesamte Kommunikation innerhalb der Amazon Virtual Private Cloud (Amazon VPC). Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
1. Schutz von Daten während der Übertragung	Netzwerke, über die Benutzerdaten übertragen werden, sollten angemessen vor Manipulation und Eavesdropping geschützt werden.	elb-acm-certificate-required	Zum Schutz von eventuell vorhandenen sensiblen Daten sowie von Daten während der Übertragung muss die Verschlüsselung für Ihr Elastic Load Balancing aktiviert sein. Verwenden Sie AWS Certificate Manager, um öffentliche und private SSL/TLS-Zertifikate mit AWS Diensten und internen Ressourcen zu verwalten, bereitzustellen und bereitzustellen.
1. Schutz von Daten während der Übertragung	Netzwerke, über die Benutzerdaten übertragen werden, sollten angemessen vor Manipulation und Eavesdropping geschützt werden.	elb-tls-https-listeners-nur	Stellen Sie sicher, dass Ihre Elastic Load Balancer (ELBs) mit SSL- oder HTTPS-Listenern konfiguriert sind. Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
1. Schutz von Daten während der Übertragung	Netzwerke, über die Benutzerdaten übertragen werden, sollten angemessen vor Manipulation und Eavesdropping geschützt werden.	opensearch-https-required	Da sensible Daten existieren können und um Daten während der Übertragung zu schützen, sollten Sie sicherstellen, dass HTTPS für Verbindungen zu Ihren Amazon OpenSearch Service-Domains aktiviert ist.
1. Schutz von Daten während der Übertragung	Netzwerke, über die Benutzerdaten übertragen werden, sollten angemessen vor Manipulation und Eavesdropping geschützt werden.	opensearch-node-to-node-Verschlüsselungsprüfung	Stellen Sie sicher, dass die node-to-node Verschlüsselung für Amazon OpenSearch Service aktiviert ist. Node-to-nodeVerschlüsselung ermöglicht die TLS 1.2-Verschlüsselung für die gesamte Kommunikation innerhalb der Amazon Virtual Private Cloud (Amazon VPC). Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
1. Schutz von Daten während der Übertragung	Netzwerke, über die Benutzerdaten übertragen werden, sollten angemessen vor Manipulation und Eavesdropping geschützt werden.	redshift-require-tls-ssl	Stellen Sie sicher, dass Ihre Amazon-Redshift-Cluster eine TLS/SSL-Verschlüsselung erfordern, um eine Verbindung zu SQL-Clients herzustellen. Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.
1. Schutz von Daten während der Übertragung	Netzwerke, über die Benutzerdaten übertragen werden, sollten angemessen vor Manipulation und Eavesdropping geschützt werden.	s-3 bucket-ssl-requests-only	Um Daten während der Übertragung zu schützen, stellen Sie sicher, dass Ihre Amazon Simple Storage Service (Amazon S3)-Buckets Anfragen zur Verwendung von Secure Socket Layer (SSL)-Buckets erfordern. Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
2. Schutz und Widerstandsfähigkeit von Ressourcen	Ihre Daten (und die Ressourcen für deren Speicherung und Verarbeitung) sollten angemessen geschützt sein.	account-part-of-organizations	Durch die zentrale Verwaltung AWS-Konten innerhalb von AWS Organizations wird sichergestellt, dass die Konten den Vorschriften entsprechen. Eine fehlende zentrale Kontoverwaltung kann zu inkonsistenten Kontokonfigurationen führen, wodurch Ressourcen und sensible Daten offengelegt werden können.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
2. Schutz und Widerstandsfähigkeit von Ressourcen	Ihre Daten (und die Ressourcen für deren Speicherung und Verarbeitung) sollten angemessen geschützt sein.	api-gw-cache-enabled-und verschlüsselt	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass die Verschlüsselung für den Cache Ihrer API-Gateway-Stufe aktiviert ist. Da für die API-Methode sensible Daten erfasst werden können, sollten Sie die Verschlüsselung von Daten im Ruhezustand aktivieren, um diese Daten zu schützen.
2. Schutz und Widerstandsfähigkeit von Ressourcen	Ihre Daten (und die Ressourcen für deren Speicherung und Verarbeitung) sollten angemessen geschützt sein.	cloudtrail-s3-dataevents-enabled	Die Erfassung von Simple Storage Service (Amazon S3)-Datenereignissen unterstützt die Erkennung von ungewöhnlichen Aktivitäten. Zu den Details gehören AWS-Konto Informationen über den Zugriff auf einen Amazon S3 S3-Bucket, die IP-Adresse und die Uhrzeit des Ereignisses.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
2. Schutz und Widerstandsfähigkeit von Ressourcen	Ihre Daten (und die Ressourcen für deren Speicherung und Verarbeitung) sollten angemessen geschützt sein.	cloudtrail-security-trail-enabled	Diese Regel trägt dazu bei, die Verwendung der AWS empfohlenen bewährten Sicherheitsmethoden für sicherzustellen AWS CloudTrail, indem geprüft wird, ob mehrere Einstellungen aktiviert sind. Dazu gehören die Verwendung von Protokollverschlüsselung, Protokollvalidierung und Aktivierung AWS CloudTrail in mehreren Regionen.
2. Schutz und Widerstandsfähigkeit von Ressourcen	Ihre Daten (und die Ressourcen für deren Speicherung und Verarbeitung) sollten angemessen geschützt sein.	codebuild-project-artifact-encryption	Um sensible Daten im Speicher zu schützen, sollten Sie sicherstellen, dass die Verschlüsselung für Ihre AWS CodeBuild Artefakte aktiviert ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
2. Schutz und Widerstandsfähigkeit von Ressourcen	Ihre Daten (und die Ressourcen für deren Speicherung und Verarbeitung) sollten angemessen geschützt sein.	db-instance-backup-enabled	Die Sicherung sfunktion von Amazon RDS erstellt Sicherung en Ihrer Datenbank en und Transakti onsprotokolle. Amazon RDS erstellt einen Snapshot für das Speichervolume Ihrer DB-Instance, sodass die gesamte DB-Instance gesichert wird. Sie können im System spezifische Aufbewahrungsfrist en festlegen, um Ihre Ausfallsicherheits anforderungen zu erfüllen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
2. Schutz und Widerstandsfähigkeit von Ressourcen	Ihre Daten (und die Ressourcen für deren Speicherung und Verarbeitung) sollten angemessen geschützt sein.	dynamodb-autoscaling-enabled	Amazon DynamoDB Auto Scaling verwendet den AWS Application Auto Scaling-Service, um die bereitgestellte Durchsatzkapazität so anzupassen, dass sie automatisch auf tatsächliche Verkehrsmuster reagiert. Auf diese Weise kann eine Tabelle oder ein globaler sekundärer Index die bereitgestellte Lese-/Schreibkapazität erhöhen, um plötzliche Erhöhungen des Datenverkehrs ohne Drosselung zu bewältigen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
2. Schutz und Widerstandsfähigkeit von Ressourcen	Ihre Daten (und die Ressourcen für deren Speicherung und Verarbeitung) sollten angemessen geschützt sein.	dynamodb-in-backup-plan	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon DynamoDB-Tabellen Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
2. Schutz und Widerstandsfähigkeit von Ressourcen	Ihre Daten (und die Ressourcen für deren Speicherung und Verarbeitung) sollten angemessen geschützt sein.	ebs-in-backup-plan	Stellen Sie zur Unterstützung der Datensicherungspro zesse sicher, dass Ihre Amazon Elastic Block Store (Amazon EBS) -Volumes Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwaltet er Backup-Service mit einer richtlini enbasierten Backup-Lösung. Diese Lösung vereinfac ht Ihr Sicherung smanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforde rungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
2. Schutz und Widerstandsfähigkeit von Ressourcen	Ihre Daten (und die Ressourcen für deren Speicherung und Verarbeitung) sollten angemessen geschützt sein.	ec2-imdsv2-check	Stellen Sie sicher, dass die Methode Instance Metadata Service Version 2 (IMDSv2) aktiviert ist, um den Zugriff auf und die Kontrolle der Amazon Elastic Compute Cloud (Amazon EC2) - Instance-Metadaten zu schützen. Die IMDSv2 Methode verwendet sitzungsbasierte Kontrollen. Mit können Kontrollen implementiert werden IMDSv2, um Änderungen an Instanzmetadaten einzuschränken.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
2. Schutz und Widerstandsfähigkeit von Ressourcen	Ihre Daten (und die Ressourcen für deren Speicherung und Verarbeitung) sollten angemessen geschützt sein.	efs-in-backup-plan	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon Elastic File System (Amazon EFS) -Dateisysteme Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
2. Schutz und Widerstandsfähigkeit von Ressourcen	Ihre Daten (und die Ressourcen für deren Speicherung und Verarbeitung) sollten angemessen geschützt sein.	elasticache-redis-cluster-automatic-Backup-Check	Wenn automatische Backups aktiviert sind, ElastiCache erstellt Amazon täglich ein Backup des Clusters. Die Sicherung kann für eine von Ihrer Organisation festgelegte Anzahl von Tagen aufbewahrt werden. Automatische Backups schützen vor Datenverlust. Bei einem Ausfall können Sie einen neuen Cluster erstellen, der Ihre Daten aus dem aktuellen Backup wiederherstellt.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
2. Schutz und Widerstandsfähigkeit von Ressourcen	Ihre Daten (und die Ressourcen für deren Speicherung und Verarbeitung) sollten angemessen geschützt sein.	elb-cross-zone-load-Balancing aktiviert	Aktivieren Sie zonenübergreifendes Load Balancing für Ihre Elastic Load Balancer (ELBs), um eine angemessene Kapazität und Verfügbarkeit aufrechtzuerhalten. Zonenübergreifendes Load Balancing reduziert die Notwendigkeit, die gleiche Anzahl von Instances in jeder aktivierten Availability Zone aufrechtzuerhalten. Es verbessert auch die Fähigkeit Ihrer Anwendung, den Verlust einer oder mehrerer Instances zu bewältigen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
2. Schutz und Widerstandsfähigkeit von Ressourcen	Ihre Daten (und die Ressourcen für deren Speicherung und Verarbeitung) sollten angemessen geschützt sein.	elb-deletion-protection-enabled	Diese Regel sorgt dafür, dass der Löschschutz für Elastic Load Balancing aktiviert ist. Verwenden Sie diese Funktion, um zu verhindern, dass Ihr Load Balancer versehentlich oder böswillig gelöscht wird, was zum Verlust der Verfügbarkeit Ihrer Anwendungen führen kann.
2. Schutz und Widerstandsfähigkeit von Ressourcen	Ihre Daten (und die Ressourcen für deren Speicherung und Verarbeitung) sollten angemessen geschützt sein.	kinesis-stream-encrypted	Aktivieren Sie die Verschlüsselung für Ihre Amazon-Kinesis-Streams, um eventuell vorhandene sensible Daten sowie Daten im Ruhezustand zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
2. Schutz und Widerstandsfähigkeit von Ressourcen	Ihre Daten (und die Ressourcen für deren Speicherung und Verarbeitung) sollten angemessen geschützt sein.	rds-in-backup-plan	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon Relational Database Service (Amazon RDS) -Instances Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
2. Schutz und Widerstandsfähigkeit von Ressourcen	Ihre Daten (und die Ressourcen für deren Speicherung und Verarbeitung) sollten angemessen geschützt sein.	rds-multi-az-support	Die Multi-AZ-Unterstützung in Amazon Relational Database Service (Amazon RDS) bietet eine verbesserte Verfügbarkeit und Beständigkeit von Datenbank-Instances. Wenn Sie eine Multi-AZ-Datenbank-Instance bereitstellen, erstellt Amazon RDS automatisch eine primäre Datenbank-Instance und repliziert die Daten synchron auf eine Standby-Instance in einer anderen Availability Zone. Jede Availability Zone läuft auf einer eigenen, physisch getrennten, unabhängigen Infrastruktur und ist auf eine hohe Verfügbarkeit ausgelegt. Im Falle eines Infrastrukturausfalls führt Amazon RDS einen automatis

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			chen Failover zum Standby-Modus durch, sodass Sie den Datenbankbetrieb wieder aufnehmen können, sobald der Failover abgeschlo ssen ist.
2. Schutz und Widerstandsfähigkeit von Ressourcen	Ihre Daten (und die Ressourcen für deren Speicherung und Verarbeitung) sollten angemessen geschützt sein.	redshift-backup-en abled	Stellen Sie zur Unterstützung der Datensicherungspro zesse sicher, dass Ihre Amazon-Re dshift-Cluster über automatisierte Snapshots verfügen. Wenn automatis ierte Snapshots für einen Cluster aktiviert sind, erstellt Redshift in regelmäßi gen Abständen Snapshots dieses Clusters. Standardm äßig erstellt Redshift alle acht Stunden oder alle 5 GB einen Snapshot für jeden Knoten mit Datenände rungen oder je nachdem, was zuerst eintritt.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
2. Schutz und Widerstandsfähigkeit von Ressourcen	Ihre Daten (und die Ressourcen für deren Speicherung und Verarbeitung) sollten angemessen geschützt sein.	s3- -blöcke-periodisch account-level-public-access	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Simple Storage Service (Amazon S3) -Buckets nicht öffentlich zugänglich sind. Diese Regel trägt dazu bei, sensible Daten vor unbefugten Remote-Benutzern zu schützen, indem sie den öffentlichen Zugriff verhindert. Mit dieser Regel können Sie optional die Parameter ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) und restrictPublicBuckets Parameter (Config Default: True) festlegen. Die tatsächlichen Werte müssen den Richtlini

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			en Ihrer Organisation entsprechen.
2. Schutz und Widerstandsfähigkeit von Ressourcen	Ihre Daten (und die Ressourcen für deren Speicherung und Verarbeitung) sollten angemessen geschützt sein.	s3- bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) unterstützt die Aufrechterhaltung einer angemesse nen Kapazität und Verfügbarkeit. CRR ermöglicht das automatische, asynchrone Kopieren von Objekten in Amazon-S3-Buckets, um die Datenverf ügbarkeit sicherzus tellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
2. Schutz und Widerstandsfähigkeit von Ressourcen	Ihre Daten (und die Ressourcen für deren Speicherung und Verarbeitung) sollten angemessen geschützt sein.	s-3 bucket-versioning-enabled	Die Versionsv erwaltung von Amazon Simple Storage Service (Amazon S3)-Bucke ts hilft dabei, mehrere Varianten eines Objekts im selben Amazon-S3-Bucket zu speichern. Verwenden Sie die Versionsv erwaltung, um sämtliche Versionen aller Objekte in Ihrem Amazon-S3-Bucket zu speichern , abzurufen oder wiederherzustellen . Mit der Versionsv erwaltung können Sie Versionen sowohl nach unbeabsic htigten Benutzera ktionen als auch nach Anwendungsfehlern problemlos wiederher stellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
2. Schutz und Widerstandsfähigkeit von Ressourcen	Ihre Daten (und die Ressourcen für deren Speicherung und Verarbeitung) sollten angemessen geschützt sein.	ssm-document-not-public	Stellen Sie sicher, dass AWS Systems Manager (SSM) - Dokumente nicht öffentlich sind, da dies einen unbeabsichtigten Zugriff auf Ihre SSM-Dokumente ermöglichen kann. Ein öffentliches SSM-Dokument kann Informationen über Ihr Konto, Ihre Ressourcen und internen Prozesse preisgeben.
2. Schutz und Widerstandsfähigkeit von Ressourcen	Ihre Daten (und die Ressourcen für deren Speicherung und Verarbeitung) sollten angemessen geschützt sein.	api-gw-cache-enabled-und verschlüsselt	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass die Verschlüsselung für den Cache Ihrer API-Gateway-Stufe aktiviert ist. Da für die API-Methode sensible Daten erfasst werden können, sollten Sie die Verschlüsselung von Daten im Ruhezustand aktivieren, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
2. Schutz und Widerstandsfähigkeit von Ressourcen	Ihre Daten (und die Ressourcen für deren Speicherung und Verarbeitung) sollten angemessen geschützt sein.	backup-recovery-point-encrypted	Stellen Sie sicher, dass die Verschlüsselung für Ihre AWS Backup-Wiederherstellungspunkte aktiviert ist. Da sensible Daten auch im Ruhezustand vorhanden sein können, sollten Sie die Verschlüsselung im Ruhezustand aktivieren, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
2. Schutz und Widerstandsfähigkeit von Ressourcen	Ihre Daten (und die Ressourcen für deren Speicherung und Verarbeitung) sollten angemessen geschützt sein.	backup-recovery-point-minimum-Aufbewahrungsprüfung	Um bei Datensicherungsprozessen zu helfen, stellen Sie sicher, dass für Ihre AWS Backup-Wiederherstellungspunkte eine Mindestaufbewahrungsdauer festgelegt ist. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen. Mit dieser Regel können Sie den Parameter requiredRetentionDays (Standardkonfiguration: 35) festlegen. Der tatsächliche Wert muss den Anforderu

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			ngen Ihrer Organisat ion entsprechen.
2. Schutz und Widerstandsfähigkeit von Ressourcen	Ihre Daten (und die Ressourcen für deren Speicherung und Verarbeitung) sollten angemessen geschützt sein.	cloud-trail-encryption-enabled	Da sensible Daten vorhanden sein können und um Daten im Ruhezustand zu schützen, sollten Sie sicherstellen, dass die Verschlüsselung für Ihre AWS CloudTrail Trails aktiviert ist.
2. Schutz und Widerstandsfähigkeit von Ressourcen	Ihre Daten (und die Ressourcen für deren Speicherung und Verarbeitung) sollten angemessen geschützt sein.	cloudwatch-log-group-encrypted	Um sensible Daten im Speicher zu schützen, stellen Sie sicher, dass die Verschlüs selung für Ihre Amazon CloudWatch Log Groups aktiviert ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
2. Schutz und Widerstandsfähigkeit von Ressourcen	Ihre Daten (und die Ressourcen für deren Speicherung und Verarbeitung) sollten angemessen geschützt sein.	dynamodb-table-encrypted-kms	Stellen Sie sicher, dass die Verschlüsselung für Ihre Amazon-DynamoDB-Tabellen aktiviert ist. Um eventuell vorhandene sensible Daten im Ruhezustand in diesen Tabellen zu schützen, müssen Sie die Verschlüsselung von Daten im Ruhezustand aktivieren. Standardmäßig werden DynamoDB-Tabellen mit einem AWS eigenen Kundenhauptschlüssel (CMK) verschlüsselt.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
2. Schutz und Widerstandsfähigkeit von Ressourcen	Ihre Daten (und die Ressourcen für deren Speicherung und Verarbeitung) sollten angemessen geschützt sein.	ebs-snapshot-public-restorable-überprüfen	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass EBS-Snapshots nicht öffentlich wiederher stellbar sind. EBS-Volume-Snapsho ts können vertrauli che Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.
2. Schutz und Widerstandsfähigkeit von Ressourcen	Ihre Daten (und die Ressourcen für deren Speicherung und Verarbeitung) sollten angemessen geschützt sein.	ec-2 ebs-encryption-by-default	Zum Schutz von Daten im Ruhezusta nd müssen Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon Elastic Block Store (Amazon EBS)-Volu mes aktiviert ist. Da sensible Daten auch im Ruhezusta nd vorhanden sein können, sollten Sie die Verschlüsselung im Ruhezustand aktivieren, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
2. Schutz und Widerstandsfähigkeit von Ressourcen	Ihre Daten (und die Ressourcen für deren Speicherung und Verarbeitung) sollten angemessen geschützt sein.	efs-encrypted-check	Aktivieren Sie die Verschlüsselung für Ihr Amazon Elastic File System (EFS), um eventuell vorhandene sensible Daten sowie Daten im Ruhezustand zu schützen.
2. Schutz und Widerstandsfähigkeit von Ressourcen	Ihre Daten (und die Ressourcen für deren Speicherung und Verarbeitung) sollten angemessen geschützt sein.	elasticsearch-encrypted-at-rest	Da sensible Daten vorhanden sein können und um Daten im Ruhezustand zu schützen, sollten Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon OpenSearch Service (OpenSearch Service) -Domains aktiviert ist.
2. Schutz und Widerstandsfähigkeit von Ressourcen	Ihre Daten (und die Ressourcen für deren Speicherung und Verarbeitung) sollten angemessen geschützt sein.	encrypted-volumes	Aktivieren Sie die Verschlüsselung für Ihre Amazon-Elastic-Block-Store (Amazon-EBS)-Volumes, um eventuell vorhandene sensible Daten sowie Daten im Ruhezustand zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
2. Schutz und Widerstandsfähigkeit von Ressourcen	Ihre Daten (und die Ressourcen für deren Speicherung und Verarbeitung) sollten angemessen geschützt sein.	kms-cmk-not-scheduled-zum Löschen	Um Daten im Ruhezustand zu schützen, sollten Sie sicherstellen, dass die für den Kunden erforderlichen Masterschlüssel (CMKs) nicht im AWS Key Management Service (AWS KMS) gelöscht werden. Da Schlüssel manchmal gelöscht werden müssen, können Sie mit dieser Regel alle zu löschenden Schlüssel überprüfen, falls ein Schlüssel versehentlich zur Löschung vorgemerkt wurde.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
2. Schutz und Widerstandsfähigkeit von Ressourcen	Ihre Daten (und die Ressourcen für deren Speicherung und Verarbeitung) sollten angemessen geschützt sein.	lambda-function-public-access-verboten	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass AWS Lambda-Funktionen nicht öffentlich zugänglich sind. Der öffentliche Zugriff kann möglicherweise die Verfügbarkeit von Ressourcen beeinträchtigen.
2. Schutz und Widerstandsfähigkeit von Ressourcen	Ihre Daten (und die Ressourcen für deren Speicherung und Verarbeitung) sollten angemessen geschützt sein.	opensearch-encrypted-at-rest	Da sensible Daten vorhanden sein können und um Daten im Ruhezustand zu schützen, sollten Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon OpenSearch Service-Domains aktiviert ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
2. Schutz und Widerstandsfähigkeit von Ressourcen	Ihre Daten (und die Ressourcen für deren Speicherung und Verarbeitung) sollten angemessen geschützt sein.	rds-snapshot-encrypted	Stellen Sie sicher, dass die Verschlüsselung für Ihre Amazon Relational Database Service (Amazon RDS)-Snapshots aktiviert ist. Da sensible Daten auch im Ruhezustand vorhanden sein können, sollten Sie die Verschlüsselung im Ruhezustand aktivieren, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
2. Schutz und Widerstandsfähigkeit von Ressourcen	Ihre Daten (und die Ressourcen für deren Speicherung und Verarbeitung) sollten angemessen geschützt sein.	rds-snapshots-public-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Relational Database Service (Amazon RDS) -Instances nicht öffentlich sind. Amazon-RDS-Datenbank-Instances können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
2. Schutz und Widerstandsfähigkeit von Ressourcen	Ihre Daten (und die Ressourcen für deren Speicherung und Verarbeitung) sollten angemessen geschützt sein.	rds-storage-encrypted	Zum Schutz von Daten im Ruhezustand müssen Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon Relational Database Service (Amazon RDS)-Instances aktiviert ist. Um eventuell vorhandene sensible Daten im Ruhezustand in Amazon-RDS-Instances zu schützen, muss die Verschlüsselung von Daten im Ruhezustand aktiviert sein.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
2. Schutz und Widerstandsfähigkeit von Ressourcen	Ihre Daten (und die Ressourcen für deren Speicherung und Verarbeitung) sollten angemessen geschützt sein.	redshift-cluster-configuration-check	Um Daten im Ruhezustand zu schützen, muss die Verschlüsselung für Ihre Amazon-Redshift-Cluster aktiviert sein. Sie müssen auch sicherstellen, dass die erforderlichen Konfigurationen auf Amazon-Redshift-Clustern bereitgestellt werden. Die Prüfungsprotokollierung muss aktiviert sein, um Informationen zu Verbindungen und Benutzeraktivitäten in der Datenbank bereitzustellen. Diese Regel erfordert, dass ein Wert für clusterDbEncrypted (Config Default: TRUE) und LoggingEnabled (Config Default: TRUE) gesetzt ist. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
2. Schutz und Widerstandsfähigkeit von Ressourcen	Ihre Daten (und die Ressourcen für deren Speicherung und Verarbeitung) sollten angemessen geschützt sein.	redshift-cluster-kms-enabled	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass die Verschlüs selung mit AWS Key Management Service (AWS KMS) für Ihren Amazon Redshift Redshift-Cluster aktiviert ist. Um eventuell vorhanden e sensible Daten im Ruhezustand in Redshift-Clustern zu schützen, muss die Verschlüsselung von Daten im Ruhezusta nd aktiviert sein.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
2. Schutz und Widerstandsfähigkeit von Ressourcen	Ihre Daten (und die Ressourcen für deren Speicherung und Verarbeitung) sollten angemessen geschützt sein.	s3- verboten bucket-level-public-access	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Simple Storage Service (Amazon S3) -Buckets nicht öffentlich zugänglich sind. Diese Regel trägt dazu bei, sensible Daten vor unbefugten Remote-Benutzern zu schützen, indem sie den öffentlichen Zugriff auf Bucket-Ebene verhindert.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
2. Schutz und Widerstandsfähigkeit von Ressourcen	Ihre Daten (und die Ressourcen für deren Speicherung und Verarbeitung) sollten angemessen geschützt sein.	s3- bucket-public-read -prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie nur autorisierten Benutzern, Prozessen und Geräten Zugriff auf Amazon Simple Storage Service (Amazon S3) - Buckets gewähren. Die Verwaltung des Zugriffs sollte mit der Klassifizierung der Daten übereinst immen.
2. Schutz und Widerstandsfähigkeit von Ressourcen	Ihre Daten (und die Ressourcen für deren Speicherung und Verarbeitung) sollten angemessen geschützt sein.	s3- bucket-public-writ e-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie nur autorisierten Benutzern, Prozessen und Geräten Zugriff auf Amazon Simple Storage Service (Amazon S3) - Buckets gewähren. Die Verwaltung des Zugriffs sollte mit der Klassifizierung der Daten übereinst immen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
2. Schutz und Widerstandsfähigkeit von Ressourcen	Ihre Daten (und die Ressourcen für deren Speicherung und Verarbeitung) sollten angemessen geschützt sein.	s3-fähig bucket-server-side-encryption	Zum Schutz von Daten im Ruhezustand müssen Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon Simple Storage Service (Amazon S3)-Buckets aktiviert ist. Um eventuell vorhandene sensible Daten im Ruhezustand in Amazon-S3-Buckets zu schützen, muss die Verschlüsselung aktiviert sein.
2. Schutz und Widerstandsfähigkeit von Ressourcen	Ihre Daten (und die Ressourcen für deren Speicherung und Verarbeitung) sollten angemessen geschützt sein.	s-3 default-encryption-kms	Stellen Sie sicher, dass die Verschlüsselung für Ihre Amazon Simple Storage Service (Amazon S3)-Buckets aktiviert ist. Um eventuell vorhandene sensible Daten im Ruhezustand in einem Amazon-S3-Bucket zu schützen, muss die Verschlüsselung aktiviert sein.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
2. Schutz und Widerstandsfähigkeit von Ressourcen	Ihre Daten (und die Ressourcen für deren Speicherung und Verarbeitung) sollten angemessen geschützt sein.	sagemaker-endpoint-configuration-kms-key-konfiguriert	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass die Verschlüsselung mit dem AWS Key Management Service (AWS KMS) für Ihren Endpunkt aktiviert ist. SageMaker Da sensible Daten auf dem SageMaker Endgerät gespeiche rt werden können, sollten Sie die Verschlüsselung im Ruhezustand aktiviere n, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
2. Schutz und Widerstandsfähigkeit von Ressourcen	Ihre Daten (und die Ressourcen für deren Speicherung und Verarbeitung) sollten angemessen geschützt sein.	sagemaker-notebook-instance-kms-schlüsselkonfiguriert	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass die Verschlüsselung mit dem AWS Key Management Service (AWS KMS) für Ihr Notebook aktiviert ist. SageMaker Da vertrauliche Daten im SageMaker Notebook gespeichert werden können, sollten Sie die Verschlüsselung im Ruhezustand aktivieren, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
2. Schutz und Widerstandsfähigkeit von Ressourcen	Ihre Daten (und die Ressourcen für deren Speicherung und Verarbeitung) sollten angemessen geschützt sein.	secretsmanager-using-cmk	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass die Verschlüsselung mit dem AWS Key Management Service (AWS KMS) für AWS Secrets Manager aktiviert ist. Aktivieren Sie die Verschlüsselung von Daten im Ruhezustand, um eventuell vorhandene sensible Daten im Ruhezustand im Secrets Manager zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
2. Schutz und Widerstandsfähigkeit von Ressourcen	Ihre Daten (und die Ressourcen für deren Speicherung und Verarbeitung) sollten angemessen geschützt sein.	sns-encrypted-kms	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass Ihre Amazon Simple Notification Service (Amazon SNS) -Themen mit dem AWS Key Management Service (AWS KMS) verschlüsselt werden müssen. Um eventuell vorhandene sensible Daten im Ruhezustand in veröffentlichten Nachrichten zu schützen, muss die Verschlüsselung von Daten im Ruhezustand aktiviert sein.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
5. Betriebssicherheit	Services müssen so betrieben und verwaltet werden, dass Angriffe erschwert, erkannt oder verhindert werden.	account-part-of-organizations	Durch die zentrale Verwaltung AWS-Konten innerhalb von AWS Organizations wird sichergestellt, dass die Konten den Vorschriften entsprechen. Eine fehlende zentrale Kontoverwaltung kann zu inkonsistenten Kontokonfigurationen führen, wodurch Ressourcen und sensible Daten offengelegt werden können.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
5. Betriebssicherheit	Services müssen so betrieben und verwaltet werden, dass Angriffe erschwert, erkannt oder verhindert werden.	cloudtrail-enabled	AWS CloudTrai l kann durch die Aufzeichnung von Aktionen und API-Aufrufen in der AWS Management Console dazu beitragen, dass die Daten nicht zurückgewiesen werden können. Sie können die Benutzer und die Benutzer AWS-Konten , die einen AWS Dienst aufgerufen haben, die Quell-IP-Adresse, über die die Aufrufe generiert wurden, und den Zeitpunkt der Anrufe identifiz ieren. Einzelheiten zu den erfassten Daten finden Sie unter Inhalt des AWS CloudTrail Datensatzes.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
5. Betriebssicherheit	Services müssen so betrieben und verwaltet werden, dass Angriffe erschwert, erkannt oder verhindert werden.	ec-2 instance-detailed-monitoring-enabled	Aktivieren Sie diese Regel, um die Amazon Elastic Compute Cloud (Amazon EC2) - Instance-Überwachung auf der EC2 Amazon-Konsole zu verbessern, in der Monitoring-Diagramme mit einem Zeitraum von 1 Minute für die Instance angezeigt werden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
5. Betriebssicherheit	Services müssen so betrieben und verwaltet werden, dass Angriffe erschwert, erkannt oder verhindert werden.	ec2-manager instance-managed-by-systems	Eine Bestandsaufnahme der Softwareplattformen und Anwendungen innerhalb des Unternehmens ist möglich, indem Amazon Elastic Compute Cloud (Amazon EC2) - Instances mit AWS Systems Manager verwaltet werden. Verwenden Sie AWS Systems Manager, um detaillierte Systemkonfigurationen, Betriebssystem-Patch-Levels, Namen und Typ der Dienste, Softwareinstallationen, Anwendungsname, Herausgeber und Version sowie andere Details zu Ihrer Umgebung bereitzustellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
5. Betriebssicherheit	Services müssen so betrieben und verwaltet werden, dass Angriffe erschwert, erkannt oder verhindert werden.	elasticsearch-logs-to-cloudwatch	Stellen Sie sicher, dass für Amazon OpenSearch Service-Domains Fehlerprotokolle aktiviert und zur Aufbewahrung und Beantwortung an Amazon CloudWatch Logs gestreamt werden. Domain-Fehlerprotokolle sind bei Sicherheits- und Zugriffsprüfungen sowie bei der Diagnose von Verfügbarkeitsproblemen nützlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
5. Betriebssicherheit	Services müssen so betrieben und verwaltet werden, dass Angriffe erschwert, erkannt oder verhindert werden.	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) Security Groups können bei der Verwaltung des Netzwerkzugriffs helfen, indem sie eine statusbeh aftete Filterung von eingehendem und ausgehendem Netzwerkverkehr zu Ressourcen bereitste llen. AWS Wenn Sie eingehenden (oder entfernten) Datenverk ehr von 0.0.0.0/0 bis Port 22 auf Ihren Ressourcen nicht zulassen, können Sie den Remote-Zugriff einschränken.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
5. Betriebssicherheit	Services müssen so betrieben und verwaltet werden, dass Angriffe erschwert, erkannt oder verhindert werden.	no-unrestricted-route-to-igw	Stellen Sie sicher, dass EC2 Amazon-Routentabellen keine uneingeschränkten Routen zu einem Internet-Gateway enthalten. Durch das Entfernen oder Beschränken des Internetzugangs für Workloads innerhalb von Amazon VPCs können unbeabsic htigte Zugriffe in Ihrer Umgebung reduziert werden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
5. Betriebssicherheit	Services müssen so betrieben und verwaltet werden, dass Angriffe erschwert, erkannt oder verhindert werden.	restricted-common-ports	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass gemeinsame Ports für Amazon Elastic Compute Cloud (Amazon EC2) -Sicherheitsgruppen eingeschränkt sind. Wenn der Zugriff auf Ports nicht auf vertrauenswürdige Quellen beschränkt wird, kann dies zu Angriffen auf die Verfügbarkeit, Integrität und Vertraulichkeit von Systemen führen. Mit dieser Regel können Sie optional die Parameter blockedPort1–blockedPort5 festlegen (Standardkonfigurationen: 20, 21, 3389, 3306, 4333). Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
5. Betriebssicherheit	Services müssen so betrieben und verwaltet werden, dass Angriffe erschwert, erkannt oder verhindert werden.	api-gw-execution-logging-aktiviert	Die API-Gateway-Protokollierung zeigt detaillierte Ansichten der Benutzer, die auf die API zugegriffen haben, und wie diese Benutzer auf die API zugegriffen haben. Diese Einblicke ermöglichen die Transparenz von Benutzeraktivitäten.
5. Betriebssicherheit	Services müssen so betrieben und verwaltet werden, dass Angriffe erschwert, erkannt oder verhindert werden.	cloud-trail-cloud-watch-logs-aktiviert	Verwenden Sie Amazon CloudWatch , um Protokoll ereignisaktivitäten zentral zu sammeln und zu verwalten. Die Aufnahme von AWS CloudTrail Daten liefert Einzelheiten zu den API-Aufrufaktivitäten in Ihrem AWS-Konto.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
5. Betriebssicherheit	Services müssen so betrieben und verwaltet werden, dass Angriffe erschwert, erkannt oder verhindert werden.	cloudtrail-s3-data events-enabled	Die Erfassung von Simple Storage Service (Amazon S3)-Datenereignissen unterstützt die Erkennung von ungewöhnlichen Aktivitäten. Zu den Details gehören AWS-Konto Informationen über den Zugriff auf einen Amazon S3 S3-Bucket, die IP-Adresse und die Uhrzeit des Ereignisses.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
5. Betriebssicherheit	Services müssen so betrieben und verwaltet werden, dass Angriffe erschwert, erkannt oder verhindert werden.	cloudwatch-alarm-action-check	Amazon CloudWatch alarmiert, wenn eine Metrik den Schwellenwert für eine bestimmte Anzahl von Bewertungszeiträumen überschreitet. Der Alarm führt eine oder mehrere Aktionen durch, die vom Wert der Metrik oder des Ausdrucks im Vergleich zu einem Schwellenwert in einer Reihe von Zeiträumen abhängt. Diese Regel erfordert einen Wert für alarmActionRequired (Config Default: True), insufficientDataAction Required (Config Default: True), okActionRequired (Config Default: False). Der tatsächliche Wert muss die Alarmaktionen für Ihre Umgebung widerspiegeln.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
5. Betriebssicherheit	Services müssen so betrieben und verwaltet werden, dass Angriffe erschwert, erkannt oder verhindert werden.	cw-loggroup-retention-period-überprüfen	Stellen Sie sicher, dass die Ereignisprotokolldaten für Ihre Protokollgruppen über eine Mindestdauer aufbewahrt werden, um die Fehlerbehebung und forensische Untersuchungen zu unterstützen. Fehlende frühere Ereignisprotokolldaten erschweren die Rekonstruierung und Identifizierung potenziell schädlicher Ereignisse.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
5. Betriebssicherheit	Services müssen so betrieben und verwaltet werden, dass Angriffe erschwert, erkannt oder verhindert werden.	ec2-imdsv2-check	Stellen Sie sicher, dass die Methode Instance Metadata Service Version 2 (IMDSv2) aktiviert ist, um den Zugriff auf und die Kontrolle der Amazon Elastic Compute Cloud (Amazon EC2) - Instance-Metadaten zu schützen. Die IMDSv2 Methode verwendet sitzungsbasierte Kontrollen. Mit können Kontrollen implementiert werden IMDSv2, um Änderungen an Instanzmetadaten einzuschränken.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
5. Betriebssicherheit	Services müssen so betrieben und verwaltet werden, dass Angriffe erschwert, erkannt oder verhindert werden.	ec2- -check managedinstance-association-compliance-status	Verwenden Sie AWS Systems Manager Associations, um bei der Inventarisierung von Softwareplattformen und Anwendungen innerhalb eines Unternehmens zu helfen. AWS Systems Manager weist Ihren verwalteten Instanzen einen Konfigurationsstatus zu und ermöglicht es Ihnen, Basiswerte für Betriebssystem-Patch-Levels, Softwareinstallationen, Anwendungskonfigurationen und andere Details zu Ihrer Umgebung festzulegen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
5. Betriebssicherheit	Services müssen so betrieben und verwaltet werden, dass Angriffe erschwert, erkannt oder verhindert werden.	ec2-check managedinstance-patch-compliance-status	Aktivieren Sie diese Regel, um bei der Identifizierung und Dokumentation von Sicherheitslücken in Amazon Elastic Compute Cloud (Amazon EC2) zu helfen. Die Regel prüft, ob die EC2 Amazon-Instance die Patch-Konformität im AWS Systems Manager gemäß den Richtlinien und Verfahren Ihrer Organisation einhält.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
5. Betriebssicherheit	Services müssen so betrieben und verwaltet werden, dass Angriffe erschwert, erkannt oder verhindert werden.	elb-logging-enabled	Die Elastic-Load-Balancing-Aktivität ist ein zentraler Kommunikationspunkt innerhalb einer Umgebung. Stellen Sie sicher, dass die ELB-Protokollierung aktiviert ist. Die gesammelten Daten enthalten detaillierte Informationen zu Anfragen, die an den ELB gesendet wurden. Jedes Protokoll enthält Informationen wie die Zeit, zu der die Anforderung einging, die Client-IP-Adresse, Latenzen, Anforderungspfade und Serverantworten.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
5. Betriebssicherheit	Services müssen so betrieben und verwaltet werden, dass Angriffe erschwert, erkannt oder verhindert werden.	guardduty-enabled-centralized	Amazon GuardDuty kann mithilfe von Threat Intellige nce Feeds helfen, potenzielle Cybersich erheitsereignisse zu überwachen und zu erkennen. Dazu gehören Listen mit bösartigen IPs und maschinel len Lernmethoden zur Identifizierung unerwarteter, nicht autorisierter und bösartiger Aktivitäten in Ihrer AWS Cloud-Umgebung.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
5. Betriebssicherheit	Services müssen so betrieben und verwaltet werden, dass Angriffe erschwert, erkannt oder verhindert werden.	guardduty-non-archived-findings	Amazon GuardDuty hilft Ihnen dabei, die Auswirkungen eines Vorfalls zu verstehen, indem es die Ergebnisse nach Schweregrad klassifiziert: niedrig, mittel und hoch. Diese Klassifizierungen können Sie zur Festlegung von entsprechenden Strategien und Prioritäten zur Behebung solcher Vorfälle verwenden. Mit dieser Regel können Sie optional daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7) und daysHighSev (Config Default: 1) für nicht archivierte Ergebnisse festlegen, wie es die Richtlinien Ihrer Organisation erfordern.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
5. Betriebssicherheit	Services müssen so betrieben und verwaltet werden, dass Angriffe erschwert, erkannt oder verhindert werden.	lambda-dlq-check	Aktivieren Sie diese Regel, um das entsprechende Personal über Amazon Simple Queue Service (Amazon SQS) oder Amazon Simple Notification Service (Amazon SNS) zu benachrichtigen, wenn eine Funktion ausgefallen ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
5. Betriebssicherheit	Services müssen so betrieben und verwaltet werden, dass Angriffe erschwert, erkannt oder verhindert werden.	multi-region-cloudtrail-enabled	AWS CloudTrail zeichnet Aktionen und API-Aufrufe der AWS Management Console auf. Sie können feststellen, welche Benutzer und Konten angerufen wurden AWS, von welcher Quell-IP-Adresse aus die Anrufe getätigt wurden und wann die Anrufe erfolgten. CloudTrail übermittelt Protokolldateien aus allen AWS Regionen an Ihren S3-Bucket , wenn MULTI_REG ION_CLOUD _TRAIL_ENABLED aktiviert ist. Außerdem wird beim AWS Start einer neuen Region derselbe Trail in der neuen Region erstellt. CloudTrail Dadurch erhalten Sie automatis ch Protokolldateien mit API-Aktivitäten für die neue Region.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
5. Betriebssicherheit	Services müssen so betrieben und verwaltet werden, dass Angriffe erschwert, erkannt oder verhindert werden.	opensearch-logs-to-cloudwatch	Stellen Sie sicher, dass für Amazon OpenSearch Service-Domains Fehlerprotokolle aktiviert und zur Aufbewahrung und Beantwortung an Amazon CloudWatch Logs gestreamt werden. OpenSearch Service-Fehlerprotokolle können bei Sicherheits- und Zugriffsprüfungen helfen und bei der Diagnose von Verfügbarkeitsproblemen helfen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
5. Betriebssicherheit	Services müssen so betrieben und verwaltet werden, dass Angriffe erschwert, erkannt oder verhindert werden.	rds-enhanced-monitoring-enabled	Aktivieren Sie Amazon Relational Database Service (Amazon RDS), um die Verfügbarkeit von Amazon RDS zu überwachen. Dies bietet einen detaillierten Einblick in den Zustand Ihrer Amazon-RDS-Datenbank-Instances. Wenn der Amazon-RDS-Speicher mehr als ein zugrunde liegendes physisches Gerät verwendet, erfasst Enhanced Monitoring die Daten für jedes Gerät. Wenn die Amazon-RDS-Datenbank-Instance in einer Multi-AZ-Bereitstellung ausgeführt wird, werden außerdem die Daten für jedes Gerät auf dem sekundären Host sowie die Metriken des sekundären Hosts erfasst.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
5. Betriebssicherheit	Services müssen so betrieben und verwaltet werden, dass Angriffe erschwert, erkannt oder verhindert werden.	rds-logging-enabled	Um die Protokollierung und Überwachung in Ihrer Umgebung zu erleichtern, stellen Sie sicher, dass die Amazon Relational Database Service (Amazon RDS)-Protokollierung aktiviert ist. Mit der Amazon-RDS-Protokollierung können Sie Ereignisse wie Verbindungen, Verbindungsabbrüche, Abfragen oder abgefragte Tabellen erfassen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
5. Betriebssicherheit	Services müssen so betrieben und verwaltet werden, dass Angriffe erschwert, erkannt oder verhindert werden.	redshift-cluster-maintenancesettings-check	Diese Regel stellt sicher, dass Amazon-Redshift-Cluster die bevorzugten Einstellungen für Ihre Organisation haben. Insbesondere sorgt sie dafür, dass Cluster bevorzugte Wartungsfenster und automatisierte Aufbewahrungsfristen für Snapshots für die Datenbank haben. Für diese Regel müssen Sie die festlegen allowVersionUpgrade. Der Standardwert ist „true“. Außerdem können Sie optional den Zeitraum preferredMaintenanceWindow (der Standardwert ist sa: 16:00 -sa: 16:30) und den automated SnapshotRetention Zeitraum (der Standardwert ist 1) festlegen. Die tatsächlichen Werte müssen den Richtlini

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			en Ihrer Organisation entsprechen.
5. Betriebssicherheit	Services müssen so betrieben und verwaltet werden, dass Angriffe erschwert, erkannt oder verhindert werden.	s3- bucket-logging-enabled	Die Amazon Simple Storage Service (Amazon S3)-Serverzugriffs protokollierung bietet eine Methode zur Überwachu ng des Netzwerks im Hinblick auf potenzielle Cybersich erheitsereignisse. Die Ereignisse werden überwacht, indem detaillierte Aufzeichn ungen über die Anfragen erfasst werden, die an einen Amazon-S3-Bucket gestellt wurden. Jeder Zugriffsprotokolle intrag enthält Details zu einer einzelnen Zugriffsanfrage. Zu den Details gehören Anforderer, Bucket-Name, Anforderu ngszeit, Anforderu ngsaktion, Antwortst atus und Fehlercode, falls relevant.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
5. Betriebssicherheit	Services müssen so betrieben und verwaltet werden, dass Angriffe erschwert, erkannt oder verhindert werden.	securityhub-enabled	AWS Security Hub hilft bei der Überwachung von unbefugtem Personal, Verbindungen, Geräten und Software. AWS Security Hub aggregiert, organisiert und priorisiert die Sicherheitswarnungen oder Ergebnisse mehrerer Dienste. AWS Einige dieser Dienste sind Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer und AWS Firewall Manager sowie AWS Partnerlösungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
5. Betriebssicherheit	Services müssen so betrieben und verwaltet werden, dass Angriffe erschwert, erkannt oder verhindert werden.	vpc-flow-logs-enabled	VPC-Flow-Protokolle erfassen detaillierte Informationsdatensätze über den IP-Datenverkehr, der zu und von Netzwerkschnittstellen in Ihrer Amazon Virtual Private Cloud (Amazon VPC) fließt. Standardmäßig enthalten Flow-Protokolldatensätze Werte für die verschiedenen Komponenten des IP-Flows, einschließlich Quelle, Ziel und Protokoll.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
5. Betriebssicherheit	Services müssen so betrieben und verwaltet werden, dass Angriffe erschwert, erkannt oder verhindert werden.	wafv2-logging-enabled	Um Ihnen bei der Protokollierung und Überwachung in Ihrer Umgebung zu helfen, aktivieren Sie die AWS WAF (V2) -Protokollierung im regionalen und globalen Web. ACLs AWS Die WAF-Protokollierung bietet detaillierte Informationen über den Datenverkehr, der von Ihrer Web-ACL analysiert wird. In den Protokollen werden die Uhrzeit aufgezeichnet, zu der die AWS WAF die Anfrage von Ihrer AWS Ressource erhalten hat, Informationen über die Anfrage und eine Aktion für die Regel, der jede Anfrage entsprach.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
7. Sichere Entwicklung	Cloud-Services sollten so konzipiert, entwickelt und bereitgestellt werden, dass sicherheitsrelevante Bedrohungen minimiert und eingedämmt werden.	codebuild-project-environment-privileged-überprüfen	Um Sie bei der Implementierung des Prinzips der geringsten Rechte zu unterstützen, stellen Sie sicher, dass in Ihrer CodeBuild Amazon-Projektumgebung der privilegierte Modus nicht aktiviert ist. Diese Einstellung sollte deaktiviert werden, um unbeabsichtigten Zugriff auf Docker APIs sowie auf die dem Container zugrunde liegende Hardware zu verhindern.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
7. Sichere Entwicklung	Cloud-Services sollten so konzipiert, entwickelt und bereitgestellt werden, dass sicherheitsrelevante Bedrohungen minimiert und eingedämmt werden.	codebuild-project-envvar-awscred-überprüfen	Stellen Sie sicher, dass die Anmeldeinformationen AWS_ACCESS_KEY_ID AWS_SECRET_ACCESS_KEY nicht in AWS Codebuild-Projektumgebungen vorhanden sind. Speichern Sie diese Variablen nicht als Klartext. Das Speichern dieser Variablen als Klartext bewirkt eine unbeabsichtigte Offenlegung von Daten sowie unberechtigte Zugriffe.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
7. Sichere Entwicklung	Cloud-Services sollten so konzipiert, entwickelt und bereitgestellt werden, dass sicherheitsrelevante Bedrohungen minimiert und eingedämmt werden.	codebuild-project-source-repo-URL-Prüfung	Stellen Sie sicher, dass die URL des Quell-Repositorys GitHub oder des Bitbucket-Quell-Repositorys keine persönlichen Zugriffstoken oder Anmeldeinformationen in Codebuild-Projektumgebungen enthält. AWS Verwende OAuth anstelle von persönlichen Zugriffstoken oder Anmeldedaten die Autorisierung für den Zugriff auf GitHub Bitbucket-Repositorys.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
9. Sicheres Benutzermanagement	Anbieter sollten Tools zur Verfügung stellen, mit denen Sie Ihre Nutzung des Services sicher verwalten können.	account-part-of-organizations	Durch die zentrale Verwaltung AWS-Konten innerhalb von AWS Organizations wird sichergestellt, dass die Konten den Vorschriften entsprechen. Eine fehlende zentrale Kontoverwaltung kann zu inkonsistenten Kontokonfigurationen führen, wodurch Ressourcen und sensible Daten offengelegt werden können.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
9. Sicheres Benutzermanagement	Anbieter sollten Tools zur Verfügung stellen, mit denen Sie Ihre Nutzung des Services sicher verwalten können.	iam-customer-policy-blocked-KMS-Aktionen	AWS Identity and Access Management (IAM) kann Ihnen helfen, die Prinzipien der geringsten Rechte und der Aufgabentrennung in Zugriffsberechtigungen und Autorisierungen zu integrieren und so zu verhindern, dass Richtlinien blockierte Aktionen für alle AWS Schlüssel des Key Management Service enthalten. Wenn Benutzer mehr Rechte haben, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und Aufgabentrennung verstoßen. Mit dieser Regel können Sie den Parameter festlegen. blockedActionsPatterns (Wert „AWS Bewährte grundlegende Sicherheitsmethoden“: kms:

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			Decrypt, kms:ReEncryptFrom). Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
9. Sicheres Benutzermanagement	Anbieter sollten Tools zur Verfügung stellen, mit denen Sie Ihre Nutzung des Services sicher verwalten können.	iam-inline-policy-blocked-kms-Aktionen	Stellen Sie sicher, dass ein Benutzer, eine IAM-Rolle oder eine IAM-Gruppe (AWS Identity and Access Management) nicht über eine Inline-Richtlinie verfügt, die blockierte Aktionen für alle AWS Schlüssel des Key Management Service zulässt. AWS empfiehlt, verwaltete Richtlinien anstelle von Inline-Richtlinien zu verwenden. Verwaltete Richtlinien ermöglichen Wiederverwendbarkeit, Versionsverwaltung, Rollback und Delegierung der Berechtigungsverwaltung. Mit dieser Regel können Sie den blockedActionsPatterns Parameter festlegen. (Wert „AWS Bewährte grundlegende Sicherheitsmethoden“: kms:Decrypt, kms:ReEncryptFrom). Die

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.
9. Sicheres Benutzermanagement	Anbieter sollten Tools zur Verfügung stellen, mit denen Sie Ihre Nutzung des Services sicher verwalten können.	iam-policy-no-statements-with-full-access	Stellen Sie sicher, dass IAM-Aktionen nur auf die benötigten Aktionen beschränkt sind. Wenn Benutzern mehr Rechte eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und der Aufgabentrennung verstoßen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
9. Sicheres Benutzermanagement	Anbieter sollten Tools zur Verfügung stellen, mit denen Sie Ihre Nutzung des Services sicher verwalten können.	mfa-enabled-for-iam-Konsolenzugriff	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass MFA für alle AWS Identity and Access Management (IAM) -Benutzer aktiviert ist, die über ein Konsolenkennwort verfügen. MFA sorgt für eine weitere Schutzebene zusätzlich zu den Anmeldeinformationen. Indem Sie MFA für Benutzer vorschreiben, können Sie Fälle kompromittierter Konten reduzieren und verhindern, dass unbefugte Benutzer auf vertrauliche Daten zugreifen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
9. Sicheres Benutzermanagement	Anbieter sollten Tools zur Verfügung stellen, mit denen Sie Ihre Nutzung des Services sicher verwalten können.	access-keys-rotated	Die Anmeldein formationen für autorisierte Geräte, Benutzer und Prozesse werden geprüft, indem sichergestellt wird, dass die IAM-Zugri ffsschlüssel gemäß den Vorgaben der Unternehmensrichtl inie rotiert werden. Das regelmäßi ge Ändern der Zugriffsschlüssel ist eine bewährte Sicherheitsmethode . Es verkürzt den Zeitraum, in dem ein Zugriffsschlüssel aktiv ist, und reduziert die Auswirkungen auf das Unternehmen, wenn die Schlüssel kompromittiert werden. Diese Regel erfordert einen Wert für die Zugriffsschlüssel-Rotation (Standard konfiguration: 90). Der tatsächliche Wert muss den Richtlini

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			en Ihrer Organisation entsprechen.
9. Sicheres Benutzermanagement	Anbieter sollten Tools zur Verfügung stellen, mit denen Sie Ihre Nutzung des Services sicher verwalten können.	iam-group-has-users-überprüfen	AWS Identity and Access Managemen t (IAM) kann Ihnen helfen, die Prinzipien der geringsten Rechte und der Aufgabent rennung mit Zugriffsb erechtigungen und Autorisierungen zu integrieren, indem sichergestellt wird, dass IAM-Gruppen mindestens einen Benutzer haben. Die Einteilung von Benutzern in Gruppen auf der Grundlage der ihnen zugewiese nen Berechtigungen oder ihrer Funktion ist eine Möglichkeit, das Prinzip der geringste n Berechtigung zu implementieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
9. Sicheres Benutzermanagement	Anbieter sollten Tools zur Verfügung stellen, mit denen Sie Ihre Nutzung des Services sicher verwalten können.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) kann Ihnen dabei helfen, die Prinzipien der geringsten Rechte und der Aufgabentrennung in Zugriffsberechtigungen und Autorisierungen zu integrieren und so zu verhindern, dass Richtlinien „Effect“: „Allow“ mit „Action“: „*“ anstelle von „Resource“: „*“ enthalten. Wenn Benutzern mehr Rechte eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und der Aufgabentrennung verstoßen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
9. Sicheres Benutzermanagement	Anbieter sollten Tools zur Verfügung stellen, mit denen Sie Ihre Nutzung des Services sicher verwalten können.	iam-root-access-key-überprüfen	Der Zugriff auf Systeme und Ressourcen kann gesteuert werden, indem überprüft wird, ob der Root-Benutzer keine Zugriffsschlüssel mit seiner AWS Identity and Access Management (IAM) -Rolle verknüpft hat. Stellen Sie sicher, dass die Root-Zugriffsschlüssel gelöscht werden. Erstellen und verwenden Sie stattdessen rollenbasierte Funktionen, AWS-Konten um das Prinzip der geringsten Funktionalität zu berücksichtigen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
9. Sicheres Benutzermanagement	Anbieter sollten Tools zur Verfügung stellen, mit denen Sie Ihre Nutzung des Services sicher verwalten können.	iam-user-group-membership-überprüfen	AWS Identity and Access Management (IAM) kann Ihnen helfen, Zugriffsberechtigungen und Autorisierungen einzuschränken, indem sichergestellt wird, dass Benutzer Mitglieder mindestens einer Gruppe sind. Wenn Benutzern mehr Berechtigungen eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und Aufgabentrennung verstoßen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
9. Sicheres Benutzermanagement	Anbieter sollten Tools zur Verfügung stellen, mit denen Sie Ihre Nutzung des Services sicher verwalten können.	iam-user-no-policies-überprüfen	Diese Regel stellt sicher, dass AWS Identity and Access Management (IAM) -Richtlinien nur Gruppen oder Rollen zugewiese n werden, um den Zugriff auf Systeme und Ressourcen zu kontrollieren. Die Zuweisung von Berechtig ungen auf Gruppen- oder Rollenebene trägt dazu bei, die Wahrscheinlichkeit zu verringern, dass eine Identität übermäßige Berechtigungen erhält oder beibehält.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
9. Sicheres Benutzermanagement	Anbieter sollten Tools zur Verfügung stellen, mit denen Sie Ihre Nutzung des Services sicher verwalten können.	iam-user-unused-credentials-überprüfen	AWS Identity and Access Management (IAM) kann Ihnen bei Zugriffsberechtigungen und Autorisierungen helfen, indem es nach IAM-Passwörtern und Zugriffsschlüsseln sucht, die für einen bestimmten Zeitraum nicht verwendet wurden. Wenn ungenutzte Anmeldeinformationen identifiziert werden, müssen Sie sie deaktivieren und/oder entfernen, da dies gegen das Prinzip der geringsten Berechtigung verstoßen könnte. Für diese Regel müssen Sie einen Wert für das maxCredentialUsage Alter festlegen (Standardkonfiguration: 90). Der tatsächliche Wert muss den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10. Identität und Authentifizierung	Der Zugang zu Serviceschnittstellen sollte authentifizierten und autorisierten Personen vorbehalten sein.	access-keys-rotated	Die Anmeldein formationen für autorisierte Geräte, Benutzer und Prozesse werden geprüft, indem sichergestellt wird, dass die IAM-Zugri ffsschlüssel entsprech end den Vorgaben der Unternehmensrichtl inie rotiert werden. Das regelmäßi ge Ändern der Zugriffsschlüssel ist eine bewährte Sicherheitsmethode . Es verkürzt den Zeitraum, in dem ein Zugriffsschlüssel aktiv ist, und reduziert die Auswirkungen auf das Unternehmen, wenn die Schlüssel kompromittiert werden. Diese Regel erfordert einen Wert für die Zugriffsschlüssel-Rotation (Standard konfiguration: 90). Der tatsächliche Wert muss den Richtlini

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			en Ihrer Organisation entsprechen.
10. Identität und Authentifizierung	Der Zugang zu Serviceschnittstellen sollte authentifizierten und autorisierten Personen vorbehalten sein.	ecs-task-definition-user-for-host-mode-check	Wenn für eine Aufgabendefinition erhöhte Berechtigungen gelten, liegt das daran, dass der Kunde diesen Konfigurationen ausdrücklich zugestimmt hat. Diese Kontrolle prüft, ob eine unerwartete Berechtigungseskalation vorliegt, wenn für eine Aufgabendefinition das Host-Netzwerk aktiviert ist, die Kunden aber keine erhöhten Berechtigungen aktiviert haben.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10. Identität und Authentifizierung	Der Zugang zu Serviceschnittstellen sollte authentifizierten und autorisierten Personen vorbehalten sein.	rds-instance-iam-authentication-aktiviert	Stellen Sie sicher, dass eine AWS Identity and Access Management (IAM) -Authentifizierung auf Amazon Relational Database Service (Amazon RDS) -Instances aktiviert ist, um den Zugriff auf Systeme und Ressourcen zu kontrollieren. Dadurch wird die Verschlüsselung von ausgehendem und eingehendem Netzwerkverkehr von und zur Datenbank anhand von Secure Sockets Layer (SSL) durchgesetzt. Da die Authentifizierung extern verwaltet wird, ist es nicht erforderlich, Benutzeranmeldeinformationen in der Datenbank zu speichern.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10. Identität und Authentifizierung	Der Zugang zu Serviceschnittstellen sollte authentifizierten und autorisierten Personen vorbehalten sein.	emr-kerberos-enabled	Die Zugriffsberechtigungen und -autorisierungen können verwaltet und nach den Prinzipien der geringsten Berechtigung und Aufgabentrennung integriert werden, indem Kerberos für Amazon-EMR-Cluster aktiviert wird. In Kerberos werden Services und Benutzer, die sich authentifizieren müssen, als Prinzipale bezeichnet. Prinzipale befinden sich in einem Kerberos-Bereich. Innerhalb dieses Bereichs wird ein Kerberos-Server als Key Distribution Center (KDC) bezeichnet. Über diesen Server können sich Prinzipale authentifizieren. Die Authentifizierung im KDC erfolgt durch die Ausstellung von Authentif

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			izierungstickets. Das KDC unterhält eine Datenbank der Prinzipale in seinem Bereich mit ihren Passwörtern und anderen administr ativen Informationen zu jedem Prinzipal.
10. Identität und Authentifizierung	Der Zugang zu Serviceschnittstellen sollte authentifizierten und autorisierten Personen vorbehalten sein.	iam-no-inline-policy-überprüfen	Stellen Sie sicher, dass ein Benutzer, eine IAM-Rolle oder eine IAM-Gruppe (AWS Identity and Access Management) nicht über eine Inline-Richtlinie zur Zugriffsk ontrolle auf Systeme und Ressource n verfügt. AWS empfiehlt, verwaltet e Richtlinien anstelle von Inline-Richtlinien zu verwenden. Verwaltete Richtlini en ermöglichen Wiederverwendbarke it, Versionsverwaltung , Rollback und Delegierung der Berechtigungsverwa ltung.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10. Identität und Authentifizierung	Der Zugang zu Serviceschnittstellen sollte authentifizierten und autorisierten Personen vorbehalten sein.	iam-password-policy	Die Identitäten und Anmeldeinformationen werden auf der Grundlage einer organisatorischen IAM-Passwortrichtlinie ausgestellt, verwaltet und verifiziert. Sie erfüllen oder übertreffen die Anforderungen von NIST SP 800-63 und dem Standard „Best Practices“ von AWS Foundational Security für die Passwortstärke. Mit dieser Regel können Sie optional RequireUppercaseCharacters (Wert für AWS grundlegende Sicherheitsbewährte Methoden: wahr), RequireLowercaseCharacters (Wert für bewährte Methoden für AWS grundlegende Sicherheit: wahr), RequireSymbols (Wert für bewährte Methoden für AWS grundlegende Sicherheit:

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			wahr), RequireNumbers (Wert für bewährte Methoden für AWS grundlegende Sicherheit: wahr), MinimumPasswordLength (Wert für bewährte Methoden für AWS grundlegende Sicherheit: 14), PasswordReusePrevention (Wert für bewährte Methoden für AWS grundlegende Sicherheit: 24) und MaxPasswordAge (Wert für bewährte Methoden für AWS grundlegende Sicherheit: 90) für Ihr IAM festlegen Kennwortrichtlinie. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10. Identität und Authentifizierung	Der Zugang zu Serviceschnittstellen sollte authentifizierten und autorisierten Personen vorbehalten sein.	iam-user-mfa-enabled	Aktivieren Sie diese Regel, um den Zugriff auf Ressourcen in der AWS Cloud einzuschränken. Diese Regel sorgt dafür, dass die Multi-Faktor-Authentifizierung (MFA) für alle Benutzer aktiviert ist. MFA sorgt für eine weitere Schutzebene zusätzlich zu den Anmeldeinformationen. Reduzieren Sie Fälle von kompromittierten Konten, indem Sie MFA für Benutzer vorschreiben.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10. Identität und Authentifizierung	Der Zugang zu Serviceschnittstellen sollte authentifizierten und autorisierten Personen vorbehalten sein.	mfa-enabled-for-iam-Konsolenzugriff	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass MFA für alle AWS Identity and Access Management (IAM) -Benutzer aktiviert ist, die über ein Konsolenkennwort verfügen. MFA sorgt für eine weitere Schutzebene zusätzlich zu den Anmeldeinformationen. Indem Sie MFA für Benutzer vorschreiben, können Sie Fälle kompromittierter Konten reduzieren und verhindern, dass unbefugte Benutzer auf vertrauliche Daten zugreifen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10. Identität und Authentifizierung	Der Zugang zu Serviceschnittstellen sollte authentifizierten und autorisierten Personen vorbehalten sein.	root-account-hardware-mfa-aktiviert	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Hardware-MFA für den Root-Benutzer aktiviert ist. Der Stammbenutzer ist der AWS-Konto-Benutzer mit den meisten Berechtigungen. MFA sorgt für eine weitere Schutzebene zusätzlich zu den Anmeldeinformationen. Indem Sie MFA für den Root-Benutzer vorschreiben, können Sie die Anzahl AWS-Konten kompromittierter Benutzer reduzieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10. Identität und Authentifizierung	Der Zugang zu Serviceschnittstellen sollte authentifizierten und autorisierten Personen vorbehalten sein.	root-account-mfa-enabled	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass MFA für den Root-Benutzer aktiviert ist. Der Stammbenutzer ist der AWS-Konto-Benutzer mit den meisten Berechtigungen. MFA sorgt für eine weitere Schutzebene zusätzlich zu den Anmeldeinformationen. Indem Sie MFA für den Root-Benutzer vorschreiben, können Sie die Anzahl AWS-Konten kompromittierter Benutzer reduzieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
11. Schutz externer Schnittstellen	Alle externen oder weniger vertrauen swürdigen Schnittst ellen zum Service sollten identifiziert und geschützt werden.	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) Security Groups können bei der Verwaltung des Netzwerkzugriffs helfen, indem sie eine statusbeh aftete Filterung von eingehendem und ausgehendem Netzwerkverkehr zu Ressourcen bereitste llen. AWS Wenn Sie eingehenden (oder entfernten) Datenverk ehr von 0.0.0.0/0 bis Port 22 auf Ihren Ressourcen nicht zulassen, können Sie den Remote-Zugriff einschränken.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
11. Schutz externer Schnittstellen	Alle externen oder weniger vertrauen swürdigen Schnittst ellen zum Service sollten identifiziert und geschützt werden.	ec-2 instances-in-vpc	Stellen Sie Amazon Elastic Compute Cloud (Amazon EC2) -Instances innerhalb einer Amazon Virtual Private Cloud (Amazon VPC) bereit, um eine sichere Kommunika tion zwischen einer Instance und anderen Services innerhalb der Amazon VPC zu ermöglichen, ohne dass ein Internet-Gateway, ein NAT-Gerät oder eine VPN-Verbindung erforderlich ist. Der gesamte Datenverk ehr bleibt sicher in der AWS Cloud. Domains, die sich innerhalb einer VPC befinden, verfügen aufgrund ihrer logischen Isolierun g im Vergleich zu Domains mit öffentlic hen Endpunkten über eine zusätzlic he Sicherheitsebene. Weisen Sie EC2

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			Amazon-Instances einer Amazon-VPC zu, um den Zugriff ordnungsgemäß zu verwalten.
11. Schutz externer Schnittstellen	Alle externen oder weniger vertrauen swürdigen Schnittst ellen zum Service sollten identifiziert und geschützt werden.	no-unrestricted-route-to-igw	Stellen Sie sicher, dass EC2 Amazon-Routentabellen keine uneingeschränkten Routen zu einem Internet-Gateway enthalten. Durch das Entfernen oder Beschränken des Internetzugangs für Workloads innerhalb von Amazon VPCs können unbeabsic htigte Zugriffe in Ihrer Umgebung reduziert werden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
11. Schutz externer Schnittstellen	Alle externen oder weniger vertrauen swürdigen Schnittst ellen zum Service sollten identifiziert und geschützt werden.	restricted-common-ports	Verwalten Sie den Zugriff auf Ressource n in der AWS Cloud, indem Sie sicherste llen, dass gemeinsam e Ports für Amazon Elastic Compute Cloud (Amazon EC2) -Sicherhe itsgruppen eingeschr ränkt sind. Wenn der Zugriff auf Ports nicht auf vertrauen swürdige Quellen beschränkt wird, kann dies zu Angriffen auf die Verfügbar keit, Integrität und Vertraulichkeit von Systemen führen. Mit dieser Regel können Sie optional die Parameter blockedPo rt1–blockedPort5 festlegen (Standard konfigurationen: 20, 21, 3389, 3306, 4333). Die tatsächli chen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
11. Schutz externer Schnittstellen	Alle externen oder weniger vertrauen swürdigen Schnittst ellen zum Service sollten identifiziert und geschützt werden.	s3- account-level-publ ic-access -Block-pe riodisch	Verwalten Sie den Zugriff auf Ressource n in der AWS Cloud, indem Sie sicherste llen, dass Amazon Simple Storage Service (Amazon S3) -Buckets nicht öffentlich zugänglic h sind. Diese Regel trägt dazu bei, sensible Daten vor unbefugten Remote-Benutzern zu schützen, indem sie den öffentlichen Zugriff verhinder t. Mit dieser Regel können Sie optional die Parameter ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) und restrictPublicBuck ets Parameter (Config Default: True) festlegen. Die tatsächlichen Werte müssen den Richtlini

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			en Ihrer Organisation entsprechen.
11. Schutz externer Schnittstellen	Alle externen oder weniger vertrauen swürdigen Schnittst ellen zum Service sollten identifiziert und geschützt werden.	ssm-document-not-p ublic	Stellen Sie sicher, dass AWS Systems Manager (SSM) - Dokumente nicht öffentlich sind, da dies einen unbeabsic htigten Zugriff auf Ihre SSM-Dokum ente ermöglichen kann. Ein öffentlic hes SSM-Dokum ent kann Informati onen über Ihr Konto, Ihre Ressourcen und internen Prozesse preisgeben.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
11. Schutz externer Schnittstellen	Alle externen oder weniger vertrauen swürdigen Schnittst ellen zum Service sollten identifiziert und geschützt werden.	alb-waf-enabled	Stellen Sie sicher, dass AWS WAF auf Elastic Load Balancers (ELB) aktiviert ist, um Webanwendungen zu schützen. Eine WAF trägt zum Schutz Ihrer Webanwend ungen oder APIs vor gängigen Web-Explo its bei. Diese Web-Exploits können sich auf die Verfügbar keit auswirken, die Sicherheit gefährden oder übermäßige Ressourcen in Ihrer Umgebung verbrauch en.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
11. Schutz externer Schnittstellen	Alle externen oder weniger vertrauen swürdigen Schnittst ellen zum Service sollten identifiziert und geschützt werden.	dms-replication-not-public	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass auf DMS-Replikationsin stanzen nicht öffentlic h zugegriffen werden kann. DMS-Repli kations-Instances können vertrauli che Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.
11. Schutz externer Schnittstellen	Alle externen oder weniger vertrauen swürdigen Schnittst ellen zum Service sollten identifiziert und geschützt werden.	ec-2 instance-no-public-ip	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon Elastic Compute Cloud (Amazon EC2) - Instances nicht öffentlich zugänglich sind. EC2 Amazon-Instances können vertrauliche Informati onen enthalten, und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
11. Schutz externer Schnittstellen	Alle externen oder weniger vertrauen swürdigen Schnittst ellen zum Service sollten identifiziert und geschützt werden.	ecs-container-insi ghts-enabled	Die Überwachu ng ist ein wichtiger Bestandteil der Aufrechterhaltung der Zuverlässigkeit, Verfügbarkeit und Leistung von Amazon Elastic Container Service (ECS) und Ihrer AWS Lösungen. Container Insights bietet auch Diagnosei nformationen, wie z. B.Fehler beim Container-Neustart, damit Sie Probleme schnell aufdecken und beheben können.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
11. Schutz externer Schnittstellen	Alle externen oder weniger vertrauen swürdigen Schnittst ellen zum Service sollten identifiziert und geschützt werden.	ecs-containers-non privileged	Um die Implement ierung des Prinzips der geringsten Berechtigung zu unterstützen, dürfen in Amazon Elastic Container Service (Amazon ECS)-Aufg abendefinitionen keine erhöhten Berechtigungen aktiviert sein. Wenn dieser Parameter den Wert „true“ aufweist, erhält der Container erhöhte Berechtig ungen auf der Host-Container-Instance (ähnlich wie der Root-Benutzer).

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
11. Schutz externer Schnittstellen	Alle externen oder weniger vertrauen swürdigen Schnittst ellen zum Service sollten identifiziert und geschützt werden.	ecs-containers-rea donly-access	Die Aktivierung des schreibgeschützten Zugriffs auf Amazon Elastic Container Service (ECS)-Container kann dazu beitragen, das Prinzip der geringste n Berechtigung einzuhalten. Diese Option kann Angriffsv ektoren reduziere n, da das Dateisyst em der Container-Instance nur geändert werden kann, wenn es über ausdrückliche Lese- und Schreibbe rechtigungen verfügt.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
11. Schutz externer Schnittstellen	Alle externen oder weniger vertrauen swürdigen Schnittst ellen zum Service sollten identifiziert und geschützt werden.	elasticsearch-in-vpc-only	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherste llen, dass sich Amazon OpenSearc h OpenSearch Service (Service) - Domains innerhalb einer Amazon Virtual Private Cloud (Amazon VPC) befinden. Eine OpenSearch Service-Domain innerhalb einer Amazon VPC ermöglicht die sichere Kommunikation zwischen OpenSearc h Service und anderen Services innerhalb der Amazon VPC, ohne dass ein Internet-Gateway, ein NAT-Gerät oder eine VPN-Verbindung erforderlich ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
11. Schutz externer Schnittstellen	Alle externen oder weniger vertrauen swürdigen Schnittst ellen zum Service sollten identifiziert und geschützt werden.	emr-master-no-public-ip	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon EMR-Clust er-Masterknoten nicht öffentlich zugänglic h sind. Amazon-EM R-Cluster-Hauptkno ten können vertrauli che Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
11. Schutz externer Schnittstellen	Alle externen oder weniger vertrauen swürdigen Schnittst ellen zum Service sollten identifiziert und geschützt werden.	ec-2 instances-in-vpc	Stellen Sie Amazon Elastic Compute Cloud (Amazon EC2) -Instances innerhalb einer Amazon Virtual Private Cloud (Amazon VPC) bereit, um eine sichere Kommunika tion zwischen einer Instance und anderen Services innerhalb der Amazon VPC zu ermöglichen, ohne dass ein Internet-Gateway, ein NAT-Gerät oder eine VPN-Verbindung erforderlich ist. Der gesamte Datenverk ehr bleibt sicher in der AWS Cloud. Domains, die sich innerhalb einer VPC befinden, verfügen aufgrund ihrer logischen Isolierun g im Vergleich zu Domains mit öffentlic hen Endpunkten über eine zusätzlic he Sicherheitsebene. Weisen Sie EC2

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			Amazon-Instances einer Amazon-VPC zu, um den Zugriff ordnungsgemäß zu verwalten.
11. Schutz externer Schnittstellen	Alle externen oder weniger vertrauen swürdigen Schnittst ellen zum Service sollten identifiziert und geschützt werden.	internet-gateway-a uthorized-vpc-nur	Verwalten Sie den Zugriff auf Ressource n in der AWS Cloud, indem Sie sicherste llen, dass Internet-Gateways nur mit autorisierter Amazon Virtual Private Cloud (Amazon VPC) verbunden sind. Internet-Gateways ermöglichen den bidirektionalen Internetzugang zur und von der Amazon VPC, was möglicher weise zu einem unbefugten Zugriff auf Amazon-VPC-Ressourcen führen kann.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
11. Schutz externer Schnittstellen	Alle externen oder weniger vertrauen swürdigen Schnittst ellen zum Service sollten identifiziert und geschützt werden.	lambda-function-pu blic-access-verboten	Verwalten Sie den Zugriff auf Ressource n in der AWS Cloud, indem Sie sicherste llen, dass AWS Lambda-Funktionen nicht öffentlich zugänglich sind. Der öffentliche Zugriff kann möglicherweise die Verfügbarkeit von Ressourcen beeinträc htigen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
11. Schutz externer Schnittstellen	Alle externen oder weniger vertrauen swürdigen Schnittst ellen zum Service sollten identifiziert und geschützt werden.	lambda-inside-vpc	Stellen Sie AWS Lambda-Funktionen in einer Amazon Virtual Private Cloud (Amazon VPC) bereit, um eine sichere Kommunika tion zwischen einer Funktion und anderen Diensten innerhalb der Amazon VPC zu gewährleisten. Bei dieser Konfiguration sind kein Internet-Gateway, kein NAT-Gerät und keine VPN-Verbindung erforderlich. Der gesamte Datenverk ehr bleibt sicher in der Cloud. AWS Domains, die sich innerhalb einer VPC befinden, verfügen aufgrund ihrer logischen Isolierun g im Vergleich zu Domains mit öffentlic hen Endpunkten über eine zusätzliche Sicherheitsebene. Um den Zugriff ordnungsg emäß zu verwalten,

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			sollten AWS Lambda-Funktionen einer VPC zugewiesen werden.
11. Schutz externer Schnittstellen	Alle externen oder weniger vertrauen swürdigen Schnittst ellen zum Service sollten identifiziert und geschützt werden.	opensearch-in-vpc-only	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass sich Amazon OpenSearch Service-Domains innerhalb einer Amazon Virtual Private Cloud (Amazon VPC) befinden. Eine Amazon OpenSearc h Service-Domain innerhalb einer Amazon VPC ermöglicht die sichere Kommunikation zwischen Amazon OpenSearch Service und anderen Services innerhalb der Amazon VPC, ohne dass ein Internet-Gateway, ein NAT-Gerät oder eine VPN-Verbindung erforderlich ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
11. Schutz externer Schnittstellen	Alle externen oder weniger vertrauen swürdigen Schnittst ellen zum Service sollten identifiziert und geschützt werden.	rds-instance-public-access-überprüfen	Verwalten Sie den Zugriff auf Ressource n in der AWS Cloud, indem Sie sicherste llen, dass Amazon Relational Database Service (Amazon RDS) -Instance s nicht öffentlic h sind. Amazon-RDS-Datenbank-Instances können vertrauliche Informati onen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
11. Schutz externer Schnittstellen	Alle externen oder weniger vertrauen swürdigen Schnittst ellen zum Service sollten identifiziert und geschützt werden.	rds-snapshots-public-prohibited	Verwalten Sie den Zugriff auf Ressource n in der AWS Cloud, indem Sie sicherste llen, dass Amazon Relational Database Service (Amazon RDS) -Instance s nicht öffentlic h sind. Amazon-RDS-Datenbank-Instances können vertrauliche Informati onen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
11. Schutz externer Schnittstellen	Alle externen oder weniger vertrauen swürdigen Schnittst ellen zum Service sollten identifiziert und geschützt werden.	redshift-cluster-public-access-überprüfen	Verwalten Sie den Zugriff auf Ressource n in der AWS Cloud, indem Sie sicherste llen, dass Amazon Redshift Redshift-Cluster nicht öffentlic h sind. Amazon-Re dshift-Cluster können vertrauliche Informati onen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
11. Schutz externer Schnittstellen	Alle externen oder weniger vertrauen swürdigen Schnittst ellen zum Service sollten identifiziert und geschützt werden.	s3- verboten bucket-le vel-public-access	Verwalten Sie den Zugriff auf Ressource n in der AWS Cloud, indem Sie sicherste llen, dass Amazon Simple Storage Service (Amazon S3) -Buckets nicht öffentlich zugänglic h sind. Diese Regel trägt dazu bei, sensible Daten vor unbefugten Remote-Benutzern zu schützen, indem sie den öffentlichen Zugriff auf Bucket-Eb ene verhindert.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
11. Schutz externer Schnittstellen	Alle externen oder weniger vertrauen swürdigen Schnittst ellen zum Service sollten identifiziert und geschützt werden.	s3- bucket-public-read -prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie nur autorisierten Benutzern, Prozessen und Geräten Zugriff auf Amazon Simple Storage Service (Amazon S3) - Buckets gewähren. Die Verwaltung des Zugriffs sollte mit der Klassifizierung der Daten übereinst immen.
11. Schutz externer Schnittstellen	Alle externen oder weniger vertrauen swürdigen Schnittst ellen zum Service sollten identifiziert und geschützt werden.	s3- bucket-public-writ e-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie nur autorisierten Benutzern, Prozessen und Geräten Zugriff auf Amazon Simple Storage Service (Amazon S3) - Buckets gewähren. Die Verwaltung des Zugriffs sollte mit der Klassifizierung der Daten übereinst immen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
11. Schutz externer Schnittstellen	Alle externen oder weniger vertrauen swürdigen Schnittst ellen zum Service sollten identifiziert und geschützt werden.	sagemaker-notebook -no-direct-Interne tzugang	Verwalten Sie den Zugriff auf Ressource n in der AWS Cloud, indem Sie sicherste llen, dass SageMaker Amazon-Notebooks keinen direkten Internetzugang zulassen. Indem Sie direkten Internetz ugang blockieren, vermeiden Sie, dass unbefugte Benutzer auf sensible Daten zugreifen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
11. Schutz externer Schnittstellen	Alle externen oder weniger vertrauen swürdigen Schnittst ellen zum Service sollten identifiziert und geschützt werden.	vpc-default-security-group-geschlossen	Sicherheitsgruppen von Amazon Elastic Compute Cloud (Amazon EC2) können bei der Verwaltung des Netzwerkzugriffs helfen, indem sie eine statusbehaftete Filterung des ein- und ausgehenden Netzwerkverkehrs zu Ressourcen bereitstellen. AWS Die Beschränk ung des gesamten Datenverkehrs auf die Standardsicherheit sgruppe hilft dabei, den Fernzugriff auf Ihre Ressourcen einzuschränken. AWS

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
11. Schutz externer Schnittstellen	Alle externen oder weniger vertrauen swürdigen Schnittst ellen zum Service sollten identifiziert und geschützt werden.	vpc-sg-open-only-to-authorized-ports	Verwalten Sie den Zugriff auf Ressource n in der AWS Cloud, indem Sie sicherste llen, dass gemeinsam e Ports für Amazon Elastic Compute Cloud (Amazon EC2) -Sicherhe itsgruppen eingeschr änkt sind. Wenn der Zugriff auf Ports nicht auf vertrauen swürdige Quellen beschränkt wird, kann dies zu Angriffen auf die Verfügbar keit, Integrität und Vertraulichkeit von Systemen führen. Durch die Beschränk ung des Zugriffs auf Ressourcen innerhalb einer Sicherhei tsgruppe aus dem Internet (0.0.0.0/0) kann der Remote-Zugriff auf interne Systeme gesteuert werden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
12. Sichere Verwaltung der Services	Cloud-Anbieter sollten den hohen Stellenwert von Verwaltungssystemen anerkennen.	iam-root-access-key-überprüfen	Der Zugriff auf Systeme und Ressourcen kann gesteuert werden, indem überprüft wird, ob der Root-Benutzer keine Zugriffsschlüssel mit seiner AWS Identity and Access Management (IAM) -Rolle verknüpft hat. Stellen Sie sicher, dass die Root-Zugriffsschlüssel gelöscht werden. Erstellen und verwenden Sie stattdessen rollenbasierte Funktionen, AWS-Konten um das Prinzip der geringsten Funktionalität zu berücksichtigen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
13. Prüfungsinformationen für Benutzer	Anbieter sollten die erforderlichen Protokolle für die Überwachung des Zugriffs auf Ihren Service und der darin enthaltenen bereitstellen.	cloudtrail-enabled	AWS CloudTrail kann durch die Aufzeichnung von Aktionen und API-Aufrufen in der AWS Management Console helfen, die Ablehnung zu verhindern. Sie können die Benutzer und die Benutzer AWS-Konten , die einen AWS Dienst aufgerufen haben, die Quell-IP-Adresse, über die die Aufrufe generiert wurden, und den Zeitpunkt der Anrufe identifizieren. Einzelheiten zu den erfassten Daten finden Sie unter Inhalt des AWS CloudTrail Datensatzes.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
13. Prüfungsinformationen für Benutzer	Anbieter sollten die erforderlichen Protokolle für die Überwachung des Zugriffs auf Ihren Service und der darin enthaltenen bereitstellen.	cloud-trail-cloud-watch-logs-aktiviert	Verwenden Sie Amazon CloudWatch , um Protokollereignisaktivitäten zentral zu sammeln und zu verwalten. Die Aufnahme von AWS CloudTrail Daten liefert Einzelheiten zu den API-Aufrufaktivitäten in Ihrem AWS-Konto.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
13. Prüfungsinformationen für Benutzer	Anbieter sollten die erforderlichen Protokolle für die Überwachung des Zugriffs auf Ihren Service und der darin enthaltenen bereitstellen.	cloud-trail-log-file-Validierung aktiviert	Verwenden Sie die AWS CloudTrail Protokolldateivalidierung, um die Integrität von Protokollen zu überprüfen. CloudTrail Mithilfe der Protokolldateivalidierung kann festgestellt werden, ob eine Protokolldatei geändert oder gelöscht wurde oder ob sie nach der Übermittlung CloudTrail unverändert geblieben ist. Dieses Feature wurde mit dem Branchenstandard entsprechenden Algorithmen entwickelt: SHA-256 für die Hashfunktion und SHA-256 mit RSA für digitale Signaturen. Das macht es rechnerisch unmöglich, CloudTrail Protokolldateien unbemerkt zu ändern, zu löschen oder zu fälschen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
13. Prüfungsinformationen für Benutzer	Anbieter sollten die erforderlichen Protokolle für die Überwachung des Zugriffs auf Ihren Service und der darin enthaltenen bereitstellen.	cloudtrail-security-trail-enabled	Diese Regel trägt dazu bei, die Verwendung der AWS empfohlenen bewährten Sicherheitsmethoden für sicherzustellen AWS CloudTrail, indem geprüft wird, ob mehrere Einstellungen aktiviert sind. Dazu gehören die Verwendung von Protokollverschlüsselung, Protokollvalidierung und Aktivierung AWS CloudTrail in mehreren Regionen.

Vorlage

Die Vorlage ist verfügbar unter GitHub: Operational Best Practices for NCSC Cloud Security Principles.

Bewährte Methoden für die Implementierung des Cyber Assessment Framework des NCSC

Konformitätspakete bieten ein allgemeines Compliance-Framework, das es Ihnen ermöglicht, mithilfe verwalteter oder benutzerdefinierter Regeln und Abhilfemaßnahmen Kontrollen zur Sicherheits-, Betriebs- oder Kostenoptimierung durchzuführen. AWS Config AWS Config Conformance Packs dienen als Beispielvorlagen nicht dazu, die vollständige Einhaltung eines bestimmten Governance-

oder Compliance-Standards sicherzustellen. Sie sind dafür verantwortlich, selbst zu beurteilen, ob Ihre Nutzung der Services den geltenden gesetzlichen und behördlichen Anforderungen entspricht.

Im Folgenden finden Sie ein Beispiel für eine Zuordnung zwischen den Steuerelementen des Cyber Assessment Framework (CAF) des UK National Cyber Security Centre (NCSC) und AWS verwalteten Konfigurationsregeln. Jede Config-Regel gilt für eine bestimmte AWS Ressource und bezieht sich auf eine oder mehrere UK NCSC CAF-Steuerungen. Eine CAF-Kontrolle des britischen NCSC kann mehreren Config-Regeln zugeordnet werden. In der folgenden Tabelle finden Sie weitere Informationen und Anleitungen zu diesen Zuordnungen.

Diese beispielhafte Conformance-Pack-Vorlage enthält Zuordnungen zu CAF-Kontrollen des britischen NCSC (National Cyber Security Centre | NCSC CAF-Richtlinien), wobei diese Informationen des öffentlichen Sektors unter der Open Government Licence v3.0 lizenziert sind. Der Zugriff auf die Open Government License ist hier möglich: Open Government Licence für Informationen des öffentlichen Sektors.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
A3.a Ressource nverwaltung	Alle für die Bereitste llung, Wartung oder Unterstützung von Netzwerken und Informationssystem en erforderlichen Ressourcen, die für den Betrieb wesentlic her Funktionen notwendig sind, müssen festgeleg t und bekannt sein. Dazu gehören Daten, Personen und Systeme sowie unterstützende Infrastruktur (wie	vpc-network-acl-un used-überprüfen	Diese Regel stellt sicher, dass Amazon Virtual Private Cloud (VPC)-Netzwerkzugr iffskontrolllisten verwendet werden. Die Überwachu ng ungenutzter Netzwerkzugriffsko ntrolllisten kann zu einer genauen Inventarisierung und Verwaltung Ihrer Umgebung beitragen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	Stromversorgung oder Kühlung).		
A3.a Ressource nverwaltung	Alle für die Bereitste llung, Wartung oder Unterstützung von Netzwerken und Informationssystem en erforderlichen Ressourcen, die für den Betrieb wesentlic her Funktionen notwendig sind, müssen festgeleg t und bekannt sein. Dazu gehören Daten, Personen und Systeme sowie unterstützende Infrastruktur (wie Stromversorgung oder Kühlung).	ec2- -Manager instance-managed-by-systems	Eine Bestandsa ufnahme der Softwareplattforme n und Anwendung en innerhalb des Unternehmens ist möglich, indem Amazon Elastic Compute Cloud (Amazon EC2) - Instances mit AWS Systems Manager verwaltet werden. Verwenden Sie AWS Systems Manager, um detaillierte Systemkonfiguratio nen, Betriebssystem-Patch-Levels, Namen und Typ der Dienste, Softwareinstallati onen, Anwendung sname, Herausgeb er und Version sowie andere Details zu Ihrer Umgebung bereitzustellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
A3.a Ressource nverwaltung	Alle für die Bereitste llung, Wartung oder Unterstützung von Netzwerken und Informationssystem en erforderlichen Ressourcen, die für den Betrieb wesentlic her Funktionen notwendig sind, müssen festgeleg t und bekannt sein. Dazu gehören Daten, Personen und Systeme sowie unterstützende Infrastruktur (wie Stromversorgung oder Kühlung).	ec2-stopped-instance	Aktivieren Sie diese Regel, um bei der Basiskonfiguration von Amazon Elastic Compute Cloud (Amazon EC2) - Instances zu helfen, indem Sie überprüfe n, ob EC2 Amazon-Instances gemäß den Standards Ihrer Organisation für mehr als die zulässige Anzahl von Tagen gestoppt wurden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
A3.a Ressource nverwaltung	Alle für die Bereitste llung, Wartung oder Unterstützung von Netzwerken und Informationssystem en erforderlichen Ressourcen, die für den Betrieb wesentlic her Funktionen notwendig sind, müssen festgeleg t und bekannt sein. Dazu gehören Daten, Personen und Systeme sowie unterstützende Infrastruktur (wie Stromversorgung oder Kühlung).	ec2- volume-inuse-check	Diese Regel stellt sicher, dass Amazon Elastic Block Store-Volumes, die an Amazon Elastic Compute Cloud (Amazon EC2) - Instances angehängt sind, zum Löschen markiert werden, wenn eine Instance beendet wird. Wenn ein Amazon-EB S-Volume nicht gelöscht wird, wenn die Instance, an die es angehängt ist, beendet wird, kann dies gegen das Konzept der geringsten Funktiona lität verstoßen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
A3.a Ressource nverwaltung	Alle für die Bereitste llung, Wartung oder Unterstützung von Netzwerken und Informationssystem en erforderlichen Ressourcen, die für den Betrieb wesentlic her Funktionen notwendig sind, müssen festgeleg t und bekannt sein. Dazu gehören Daten, Personen und Systeme sowie unterstützende Infrastruktur (wie Stromversorgung oder Kühlung).	eip-attached	Diese Regel stellt sicher, dass Elastic, die einer Amazon Virtual Private Cloud (Amazon VPC) IPs zugewiesen sind, an Amazon Elastic Compute Cloud (Amazon EC2) - Instances oder verwendete Elastic Network Interface s angehängt sind. Diese Regel hilft bei der Überwachu ng ungenutzter Inhalte EIPs in Ihrer Umgebung.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
B2.a Identitätsprüfung, Authentifizierung und Autorisierung	Sie verifizieren, authentifizieren und autorisieren zuverlässig den Zugriff auf die Netzwerke und Informationssysteme, die grundlegende Funktionen unterstützen.	iam-password-policy	Die Identitäten und Anmeldeinformationen werden auf der Grundlage einer organisatorischen IAM-Passwortrichtlinie ausgestellt, verwaltet und verifiziert. Sie erfüllen oder übertreffen die Anforderungen von NIST SP 800-63 und dem Standard „Best Practices“ von AWS Foundational Security für die Passwortstärke. Mit dieser Regel können Sie optional RequireUppercaseCharacters (Wert für AWS grundlegende Sicherheitsbewährte Methoden: wahr), RequireLowercaseCharacters (Wert für bewährte Methoden für AWS grundlegende Sicherheit: wahr), RequireSymbols (Wert für bewährte Methoden für AWS grundlegende Sicherheit:

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			wahr), RequireNumbers (Wert für bewährte Methoden für AWS grundlegende Sicherheit: wahr), MinimumPasswordLength (Wert für bewährte Methoden für AWS grundlegende Sicherheit: 14), PasswordReusePrevention (Wert für bewährte Methoden für AWS grundlegende Sicherheit: 24) und MaxPasswordAge (Wert für bewährte Methoden für AWS grundlegende Sicherheit: 90) für Ihr IAM festlegen Kennwortrichtlinie. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
B2.a Identitätsprüfung, Authentifizierung und Autorisierung	Sie verifizieren, authentifizieren und autorisieren zuverlässig den Zugriff auf die Netzwerke und Informationssysteme, die grundlegende Funktionen unterstützen.	iam-group-has-users-überprüfen	AWS Identity and Access Management (IAM) kann Ihnen helfen, die Prinzipien der geringsten Rechte und der Aufgabentrennung mit Zugriffsberechtigungen und Autorisierungen zu integrieren, indem sichergestellt wird, dass IAM-Gruppen mindestens einen Benutzer haben. Die Einteilung von Benutzern in Gruppen auf der Grundlage der ihnen zugewiesenen Berechtigungen oder ihrer Funktion ist eine Möglichkeit, das Prinzip der geringsten Berechtigung zu implementieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
B2.a Identitätsprüfung, Authentifizierung und Autorisierung	Sie verifizieren, authentifizieren und autorisieren zuverlässig den Zugriff auf die Netzwerke und Informationssysteme, die grundlegende Funktionen unterstützen.	iam-no-inline-policy-überprüfen	Stellen Sie sicher, dass ein Benutzer, eine IAM-Rolle oder eine IAM-Gruppe (AWS Identity and Access Management) nicht über eine Inline-Richtlinie zur Zugriffskontrolle auf Systeme und Ressourcen verfügt. AWS empfiehlt, verwaltete Richtlinien anstelle von Inline-Richtlinien zu verwenden. Verwaltete Richtlinien ermöglichen Wiederverwendbarkeit, Versionsverwaltung, Rollback und Delegierung der Berechtigungsverwaltung.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
B2.a Identitätsprüfung, Authentifizierung und Autorisierung	Sie verifizieren, authentifizieren und autorisieren zuverlässig den Zugriff auf die Netzwerke und Informationssysteme, die grundlegende Funktionen unterstützen.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) kann Ihnen dabei helfen, die Prinzipien der geringsten Rechte und der Aufgabentrennung in Zugriffsberechtigungen und Autorisierungen zu integrieren und so zu verhindern, dass Richtlinien „Effect“: „Allow“ mit „Action“: „*“ anstelle von „Resource“: „*“ enthalten. Wenn Benutzern mehr Rechte eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und der Aufgabentrennung verstoßen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
B2.a Identitätsprüfung, Authentifizierung und Autorisierung	Sie verifizieren, authentifizieren und autorisieren zuverlässig den Zugriff auf die Netzwerke und Informationssysteme, die grundlegende Funktionen unterstützen.	iam-user-group-membership-überprüfen	AWS Identity and Access Management (IAM) kann Ihnen helfen, Zugriffsberechtigungen und Autorisierungen einzuschränken, indem sichergestellt wird, dass Benutzer Mitglieder mindestens einer Gruppe sind. Wenn Benutzern mehr Berechtigungen eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und Aufgabentrennung verstoßen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
B2.a Identitätsprüfung, Authentifizierung und Autorisierung	Sie verifizieren, authentifizieren und autorisieren zuverlässig den Zugriff auf die Netzwerke und Informationssysteme, die grundlegende Funktionen unterstützen.	iam-user-unused-credentials-überprüfen	AWS Identity and Access Management (IAM) kann Ihnen bei Zugriffsberechtigungen und Autorisierungen helfen, indem es nach IAM-Passwörtern und Zugriffsschlüsseln sucht, die für einen bestimmten Zeitraum nicht verwendet wurden. Wenn ungenutzte Anmeldeinformationen identifiziert werden, müssen Sie sie deaktivieren und/oder entfernen, da dies gegen das Prinzip der geringsten Berechtigung verstoßen könnte. Für diese Regel müssen Sie einen Wert für das maxCredentialUsage Alter festlegen (Standardkonfiguration: 90). Der tatsächliche Wert muss den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
B2.a Identitätsprüfung, Authentifizierung und Autorisierung	Sie verifizieren, authentifizieren und autorisieren zuverlässig den Zugriff auf die Netzwerke und Informationssysteme, die grundlegende Funktionen unterstützen.	iam-user-mfa-enabled	Aktivieren Sie diese Regel, um den Zugriff auf Ressourcen in der AWS Cloud einzuschränken. Diese Regel sorgt dafür, dass die Multi-Faktor-Authentifizierung (MFA) für alle Benutzer aktiviert ist. MFA sorgt für eine weitere Schutzebene zusätzlich zu den Anmeldeinformationen. Reduzieren Sie Fälle von kompromittierten Konten, indem Sie MFA für Benutzer vorschreiben.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
B2.a Identitätsprüfung, Authentifizierung und Autorisierung	Sie verifizieren, authentifizieren und autorisieren zuverlässig den Zugriff auf die Netzwerke und Informationssysteme, die grundlegende Funktionen unterstützen.	mfa-enabled-for-iam-Konsolenzugriff	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass MFA für alle AWS Identity and Access Management (IAM) -Benutzer aktiviert ist, die über ein Konsolenkennwort verfügen. MFA sorgt für eine weitere Schutzebene zusätzlich zu den Anmeldeinformationen. Indem Sie MFA für Benutzer vorschreiben, können Sie Fälle kompromittierter Konten reduzieren und verhindern, dass unbefugte Benutzer auf vertrauliche Daten zugreifen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
B2.a Identitätsprüfung, Authentifizierung und Autorisierung	Sie verifizieren, authentifizieren und autorisieren zuverlässig den Zugriff auf die Netzwerke und Informationssysteme, die grundlegende Funktionen unterstützen.	root-account-hardware-mfa-aktiviert	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Hardware-MFA für den Root-Benutzer aktiviert ist. Der Stammbenutzer ist der AWS-Konto-Benutzer mit den meisten Berechtigungen. MFA sorgt für eine weitere Schutzebene zusätzlich zu den Anmeldeinformationen. Indem Sie MFA für den Root-Benutzer vorschreiben, können Sie die Anzahl AWS-Konten kompromittierter Benutzer reduzieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
B2.a Identitätsprüfung, Authentifizierung und Autorisierung	Sie verifizieren, authentifizieren und autorisieren zuverlässig den Zugriff auf die Netzwerke und Informationssysteme, die grundlegende Funktionen unterstützen.	root-account-mfa-enabled	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass MFA für den Root-Benutzer aktiviert ist. Der Stammbenutzer ist der AWS-Konto-Benutzer mit den meisten Berechtigungen. MFA sorgt für eine weitere Schutzebene zusätzlich zu den Anmeldeinformationen. Indem Sie MFA für den Root-Benutzer vorschreiben, können Sie die Anzahl AWS-Konten kompromittierter Benutzer reduzieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
B2.a Identitätsprüfung, Authentifizierung und Autorisierung	Sie verifizieren, authentifizieren und autorisieren zuverlässig den Zugriff auf die Netzwerke und Informationssysteme, die grundlegende Funktionen unterstützen.	iam-root-access-key-überprüfen	Der Zugriff auf Systeme und Ressourcen kann gesteuert werden, indem überprüft wird, ob der Root-Benutzer keine Zugriffsschlüssel mit seiner AWS Identity and Access Management (IAM) -Rolle verknüpft hat. Stellen Sie sicher, dass die Root-Zugriffsschlüssel gelöscht werden. Erstellen und verwenden Sie stattdessen rollenbasierte Funktionen, AWS-Konten um das Prinzip der geringsten Funktionalität zu berücksichtigen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
B2.a Identitätsprüfung, Authentifizierung und Autorisierung	Sie verifizieren, authentifizieren und autorisieren zuverlässig den Zugriff auf die Netzwerke und Informationssysteme, die grundlegende Funktionen unterstützen.	iam-user-no-policies-überprüfen	Diese Regel stellt sicher, dass AWS Identity and Access Management (IAM)-Richtlinien nur Gruppen oder Rollen zugewiesen werden, um den Zugriff auf Systeme und Ressourcen zu kontrollieren. Die Zuweisung von Berechtigungen auf Gruppen- oder Rollenebene trägt dazu bei, die Wahrscheinlichkeit zu verringern, dass eine Identität übermäßige Berechtigungen erhält oder beibehält.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
B2.a Identitätsprüfung, Authentifizierung und Autorisierung	Sie verifizieren, authentifizieren und autorisieren zuverlässig den Zugriff auf die Netzwerke und Informationssysteme, die grundlegende Funktionen unterstützen.	opensearch-access-control-enabled	Stellen Sie sicher, dass eine detaillierte Zugriffskontrolle für Ihre Amazon OpenSearch Service-Domains aktiviert ist. Eine differenzierte Zugriffskontrolle bietet erweiterte Autorisierungsmechanismen, um den Zugriff auf Amazon Service-Domains mit den geringsten Rechten zu erreichen. OpenSearch Es ermöglicht eine rollenbasierte Zugriffskontrolle auf die Domain sowie Sicherheit auf Index-, Dokument- und Feldebene, Unterstützung für OpenSearch Service-Dashboards, Mehrmandantenfähigkeit und HTTP-Basisauthentifizierung für Service und Kibana. OpenSearch

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
B2.a Identitätsprüfung, Authentifizierung und Autorisierung	Sie verifizieren, authentifizieren und autorisieren zuverlässig den Zugriff auf die Netzwerke und Informationssysteme, die grundlegende Funktionen unterstützen.	emr-kerberos-enabled	Die Zugriffsberechtigungen und -autorisierungen können verwaltet und nach den Prinzipien der geringsten Berechtigung und Aufgabentrennung integriert werden, indem Kerberos für Amazon-EMR-Cluster aktiviert wird. In Kerberos werden Services und Benutzer, die sich authentifizieren müssen, als Prinzipale bezeichnet. Prinzipale befinden sich in einem Kerberos-Bereich. Innerhalb dieses Bereichs wird ein Kerberos-Server als Key Distribution Center (KDC) bezeichnet. Über diesen Server können sich Prinzipale authentifizieren. Die Authentifizierung im KDC erfolgt durch die Ausstellung von Authentif

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			izierungstickets. Das KDC unterhält eine Datenbank der Prinzipale in seinem Bereich mit ihren Passwörtern und anderen administr ativen Informationen zu jedem Prinzipal.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
B2.b Geräteman agement	Sie kennen die Geräte, die für den Zugriff auf Ihre Netzwerke, Informati onssysteme und Daten verwendet werden, die grundlege nde Funktionen unterstützen, und vertrauen ihnen voll und ganz.	ec2-manager instance-managed-by-systems	Eine Bestandsa ufnahme der Softwareplattforme n und Anwendung en innerhalb des Unternehmens ist möglich, indem Amazon Elastic Compute Cloud (Amazon EC2) - Instances mit AWS Systems Manager verwaltet werden. Verwenden Sie AWS Systems Manager, um detaillierte Systemkonfiguratio nen, Betriebssystem-Patch-Levels, Namen und Typ der Dienste, Softwareinstallati onen, Anwendung sname, Herausgeb er und Version sowie andere Details zu Ihrer Umgebung bereitzustellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
B2.b Geräteman agement	Sie kennen die Geräte, die für den Zugriff auf Ihre Netzwerke, Informati onssysteme und Daten verwendet werden, die grundlege nde Funktionen unterstützen, und vertrauen ihnen voll und ganz.	securityhub-enabled	AWS Security Hub hilft bei der Überwachung von unbefugtem Personal, Verbindun gen, Geräten und Software. AWS Security Hub aggregiert, organisie rt und priorisie rt die Sicherhei tswarnungen oder Ergebnisse mehrerer Dienste. AWS Einige dieser Dienste sind Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer und AWS Firewall Manager sowie AWS Partnerlösungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
B2.c Verwaltung privilegierter Benutzer	Sie verwalten zuverlässig den Zugriff privilegierter Benutzer auf Netzwerke und Informationssysteme, die grundlegende Funktionen unterstützen.	iam-user-unused-credentials-überprüfen	AWS Identity and Access Management (IAM) kann Ihnen bei Zugriffsberechtigungen und Autorisierungen helfen, indem es nach IAM-Passwörtern und Zugriffsschlüsseln sucht, die für einen bestimmten Zeitraum nicht verwendet wurden. Wenn ungenutzte Anmeldeinformationen identifiziert werden, müssen Sie sie deaktivieren und/oder entfernen, da dies gegen das Prinzip der geringsten Berechtigung verstoßen könnte. Für diese Regel müssen Sie einen Wert für das maxCredentialUsage Alter festlegen (Standardkonfiguration: 90). Der tatsächliche Wert muss den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
B2.c Verwaltung privilegierter Benutzer	Sie verwalten zuverlässig den Zugriff privilegierter Benutzer auf Netzwerke und Informationssysteme, die grundlegende Funktionen unterstützen.	codebuild-project-environment-privileged-überprüfen	Um die Implementierung des Prinzips der geringsten Rechte zu unterstützen, stellen Sie sicher, dass in Ihrer CodeBuild Amazon-Projektumgebung der privilegierte Modus nicht aktiviert ist. Diese Einstellung sollte deaktiviert werden, um einen unbeabsichtigten Zugriff auf Docker APIs sowie auf die dem Container zugrundeliegende Hardware zu verhindern.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
B2.c Verwaltung privilegierter Benutzer	Sie verwalten zuverlässig den Zugriff privilegierter Benutzer auf Netzwerke und Informationssysteme, die grundlegende Funktionen unterstützen.	ec-2 instance-profile-attached	EC2 Instanzprofile übergeben eine IAM-Rolle an eine EC2 Instance. Das Anhängen eines Instance-Profils an Ihre Instances kann bei der Implementierung von geringsten Berechtigungen und der Berechtigungsverwaltung helfen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
B2.c Verwaltung privilegierter Benutzer	Sie verwalten zuverlässig den Zugriff privilegierter Benutzer auf Netzwerke und Informationssysteme, die grundlegende Funktionen unterstützen.	ecs-containers-nonprivileged	Um die Implementierung des Prinzips der geringsten Berechtigung zu unterstützen, dürfen in Amazon Elastic Container Service (Amazon ECS)-Aufgabendefinitionen keine erhöhten Berechtigungen aktiviert sein. Wenn dieser Parameter den Wert „true“ aufweist, erhält der Container erhöhte Berechtigungen auf der Host-Container-Instance (ähnlich wie der Root-Benutzer).

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
B2.c Verwaltung privilegierter Benutzer	Sie verwalten zuverlässig den Zugriff privilegierter Benutzer auf Netzwerke und Informationssysteme, die grundlegende Funktionen unterstützen.	ecs-containers-readonly-access	Die Aktivierung des schreibgeschützten Zugriffs auf Amazon Elastic Container Service (ECS)-Container kann dazu beitragen, das Prinzip der geringsten Berechtigung einzuhalten. Diese Option kann Angriffsvektoren reduzieren, da das Dateisystem der Container-Instance nur geändert werden kann, wenn es über ausdrückliche Lese- und Schreibberechtigungen verfügt.
B2.c Verwaltung privilegierter Benutzer	Sie verwalten zuverlässig den Zugriff privilegierter Benutzer auf Netzwerke und Informationssysteme, die grundlegende Funktionen unterstützen.	ecs-task-definition-nonroot-Benutzer	Sie bestimmen einen Nicht-Root-Benutzer für den Zugriff auf Ihre Aufgabendefinitionen des Amazon Elastic Container Service (Amazon ECS), um die Implementierung des Prinzips der geringsten Berechtigung zu unterstützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
B2.c Verwaltung privilegierter Benutzer	Sie verwalten zuverlässig den Zugriff privilegierter Benutzer auf Netzwerke und Informationssysteme, die grundlegende Funktionen unterstützen.	efs-access-point-enforce-Benutzeridentität	Um die Implementierung des Prinzips der geringsten Rechte zu unterstützen, stellen Sie sicher, dass die Benutzerdurchsetzung für Ihr Amazon Elastic File System (Amazon EFS) aktiviert ist. Wenn diese Option aktiviert ist, ersetzt Amazon EFS den Benutzer und die Gruppe IDs des NFS-Clients durch die Identität, die auf dem Access Point für alle Dateisystemoperationen konfiguriert ist, und gewährt nur Zugriff auf diese erzwungene Benutzeridentität.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
B2.c Verwaltung privilegierter Benutzer	Sie verwalten zuverlässig den Zugriff privilegierter Benutzer auf Netzwerke und Informationssysteme, die grundlegende Funktionen unterstützen.	emr-kerberos-enabled	Die Zugriffsberechtigungen und -autorisierungen können verwaltet und nach den Prinzipien der geringsten Berechtigung und Aufgabentrennung integriert werden, indem Kerberos für Amazon-EMR-Cluster aktiviert wird. In Kerberos werden Services und Benutzer, die sich authentifizieren müssen, als Prinzipale bezeichnet. Prinzipale befinden sich in einem Kerberos-Bereich. Innerhalb dieses Bereichs wird ein Kerberos-Server als Key Distribution Center (KDC) bezeichnet. Über diesen Server können sich Prinzipale authentifizieren. Die Authentifizierung im KDC erfolgt durch die Ausstellung von Authentif

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			izierungstickets. Das KDC unterhält eine Datenbank der Prinzipale in seinem Bereich mit ihren Passwörtern und anderen administr ativen Informationen zu jedem Prinzipal.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
B2.c Verwaltung privilegierter Benutzer	Sie verwalten zuverlässig den Zugriff privilegierter Benutzer auf Netzwerke und Informationssysteme, die grundlegende Funktionen unterstützen.	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) kann Ihnen helfen, die Prinzipien der geringsten Rechte und der Aufgabentrennung in Zugriffsberechtigungen und Autorisierungen zu integrieren und so zu verhindern, dass Richtlinien blockierte Aktionen für alle AWS Schlüssel des Key Management Service enthalten. Wenn Benutzer mehr Rechte haben, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und Aufgabentrennung verstoßen. Mit dieser Regel können Sie den Parameter festlegen. blockedActionsPatterns (Wert „AWS Bewährte grundlegende Sicherheitsmethode

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			n“: kms: Entschlüs seln, kms:ReEnc ryptFrom). Die tatsächlichen Werte müssen den Richtlini en Ihrer Organisation entsprechen.
B2.c Verwaltun g privilegierter Benutzer	Sie verwalten zuverlässig den Zugriff privilegi erter Benutzer auf Netzwerke und Informationssystem e, die grundlegende Funktionen unterstüt zen.	iam-group-has-users-überprüfen	AWS Identity and Access Managemen t (IAM) kann Ihnen helfen, die Prinzipien der geringsten Rechte und der Aufgabent rennung mit Zugriffsb erechtigungen und Autorisierungen zu integrieren, indem sichergestellt wird, dass IAM-Gruppen mindestens einen Benutzer haben. Die Einteilung von Benutzern in Gruppen auf der Grundlage der ihnen zugewiese nen Berechtigungen oder ihrer Funktion ist eine Möglichkeit, das Prinzip der geringste n Berechtigung zu implementieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
B2.c Verwaltung privilegierter Benutzer	Sie verwalten zuverlässig den Zugriff privilegierter Benutzer auf Netzwerke und Informationssysteme, die grundlegende Funktionen unterstützen.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) kann Ihnen dabei helfen, die Prinzipien der geringsten Rechte und der Aufgabentrennung in Zugriffsberechtigungen und Autorisierungen zu integrieren und so zu verhindern, dass Richtlinien „Effect“: „Allow“ mit „Action“: „*“ anstelle von „Resource“: „*“ enthalten. Wenn Benutzern mehr Rechte eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und der Aufgabentrennung verstoßen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
B2.c Verwaltung privilegierter Benutzer	Sie verwalten zuverlässig den Zugriff privilegierter Benutzer auf Netzwerke und Informationssysteme, die grundlegende Funktionen unterstützen.	iam-policy-no-statements-with-full-access	Stellen Sie sicher, dass IAM-Aktionen nur auf die benötigten Aktionen beschränkt sind. Wenn Benutzern mehr Rechte eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und der Aufgabentrennung verstoßen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
B2.c Verwaltung privilegierter Benutzer	Sie verwalten zuverlässig den Zugriff privilegierter Benutzer auf Netzwerke und Informationssysteme, die grundlegende Funktionen unterstützen.	iam-user-group-membership-überprüfen	AWS Identity and Access Management (IAM) kann Ihnen helfen, Zugriffsberechtigungen und Autorisierungen einzuschränken, indem sichergestellt wird, dass Benutzer Mitglieder mindestens einer Gruppe sind. Wenn Benutzern mehr Berechtigungen eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und Aufgabentrennung verstoßen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
B2.c Verwaltung privilegierter Benutzer	Sie verwalten zuverlässig den Zugriff privilegierter Benutzer auf Netzwerke und Informationssysteme, die grundlegende Funktionen unterstützen.	secretsmanager-secret-unused	Wenn in AWS Secrets Manager unbenutzte Anmeldeinformationen vorhanden sind, sollten Sie die Anmeldeinformationen deaktivieren und/oder entfernen, da dies gegen das Prinzip der geringsten Rechte verstoßen kann. Mit dieser Regel können Sie einen Wert auf unusedForDays (Config Default: 90) setzen. Der tatsächliche Wert muss den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
B2.c Verwaltung privilegierter Benutzer	Sie verwalten zuverlässig den Zugriff privilegierter Benutzer auf Netzwerke und Informationssysteme, die grundlegende Funktionen unterstützen.	iam-user-mfa-enabled	Aktivieren Sie diese Regel, um den Zugriff auf Ressourcen in der AWS Cloud einzuschränken. Diese Regel sorgt dafür, dass die Multi-Faktor-Authentifizierung (MFA) für alle Benutzer aktiviert ist. MFA sorgt für eine weitere Schutzebene zusätzlich zu den Anmeldeinformationen. Reduzieren Sie Fälle von kompromittierten Konten, indem Sie MFA für Benutzer vorschreiben.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
B2.c Verwaltung privilegierter Benutzer	Sie verwalten zuverlässig den Zugriff privilegierter Benutzer auf Netzwerke und Informationssysteme, die grundlegende Funktionen unterstützen.	mfa-enabled-for-iam-Konsolenzugriff	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass MFA für alle AWS Identity and Access Management (IAM) -Benutzer aktiviert ist, die über ein Konsolenkennwort verfügen. MFA sorgt für eine weitere Schutzebene zusätzlich zu den Anmeldeinformationen. Indem Sie MFA für Benutzer vorschreiben, können Sie Fälle kompromittierter Konten reduzieren und verhindern, dass unbefugte Benutzer auf vertrauliche Daten zugreifen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
B2.c Verwaltung privilegierter Benutzer	Sie verwalten zuverlässig den Zugriff privilegierter Benutzer auf Netzwerke und Informationssysteme, die grundlegende Funktionen unterstützen.	root-account-hardware-mfa-aktiviert	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Hardware-MFA für den Root-Benutzer aktiviert ist. Der Stammbenutzer ist der AWS-Konto-Benutzer mit den meisten Berechtigungen. MFA sorgt für eine weitere Schutzebene zusätzlich zu den Anmeldeinformationen. Indem Sie MFA für den Root-Benutzer vorschreiben, können Sie die Anzahl AWS-Konten kompromittierter Benutzer reduzieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
B2.c Verwaltung privilegierter Benutzer	Sie verwalten zuverlässig den Zugriff privilegierter Benutzer auf Netzwerke und Informationssysteme, die grundlegende Funktionen unterstützen.	root-account-mfa-enabled	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass MFA für den Root-Benutzer aktiviert ist. Der Stammbenutzer ist der AWS-Konto-Benutzer mit den meisten Berechtigungen. MFA sorgt für eine weitere Schutzebene zusätzlich zu den Anmeldeinformationen. Indem Sie MFA für den Root-Benutzer vorschreiben, können Sie die Anzahl AWS-Konten kompromittierter Benutzer reduzieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
B2.c Verwaltung privilegierter Benutzer	Sie verwalten zuverlässig den Zugriff privilegierter Benutzer auf Netzwerke und Informationssysteme, die grundlegende Funktionen unterstützen.	iam-root-access-key-überprüfen	Der Zugriff auf Systeme und Ressourcen kann gesteuert werden, indem überprüft wird, ob der Root-Benutzer keine Zugriffsschlüssel mit seiner AWS Identity and Access Management (IAM) -Rolle verknüpft hat. Stellen Sie sicher, dass die Root-Zugriffsschlüssel gelöscht werden. Erstellen und verwenden Sie stattdessen rollenbasierte Funktionen, AWS-Konten um das Prinzip der geringsten Funktionalität zu berücksichtigen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
B2.c Verwaltung privilegierter Benutzer	Sie verwalten zuverlässig den Zugriff privilegierter Benutzer auf Netzwerke und Informationssysteme, die grundlegende Funktionen unterstützen.	guardduty-enabled-centralized	Amazon GuardDuty kann mithilfe von Threat Intelligence Feeds helfen, potenzielle Cybersicherheitsereignisse zu überwachen und zu erkennen. Dazu gehören Listen mit bösartigen IPs und maschinellen Lernmethoden zur Identifizierung unerwarteter, nicht autorisierter und bösartiger Aktivitäten in Ihrer AWS Cloud-Umgebung.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
B2.c Verwaltung privilegierter Benutzer	Sie verwalten zuverlässig den Zugriff privilegierter Benutzer auf Netzwerke und Informationssysteme, die grundlegende Funktionen unterstützen.	guardduty-non-archived-findings	Amazon GuardDuty hilft Ihnen dabei, die Auswirkungen eines Vorfalls zu verstehen, indem es die Ergebnisse nach Schweregrad klassifiziert: niedrig, mittel und hoch. Diese Klassifizierungen können Sie zur Festlegung von entsprechenden Strategien und Prioritäten zur Behebung solcher Vorfälle verwenden. Mit dieser Regel können Sie optional daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7) und daysHighSev (Config Default: 1) für nicht archivierte Ergebnisse festlegen, wie es die Richtlinien Ihrer Organisation erfordern.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
B2.c Verwaltung privilegierter Benutzer	Sie verwalten zuverlässig den Zugriff privilegierter Benutzer auf Netzwerke und Informationssysteme, die grundlegende Funktionen unterstützen.	iam-no-inline-policy-überprüfen	Stellen Sie sicher, dass ein Benutzer, eine IAM-Rolle oder eine IAM-Gruppe (AWS Identity and Access Management) nicht über eine Inline-Richtlinie zur Zugriffskontrolle auf Systeme und Ressourcen verfügt. AWS empfiehlt, verwaltete Richtlinien anstelle von Inline-Richtlinien zu verwenden. Verwaltete Richtlinien ermöglichen Wiederverwendbarkeit, Versionsverwaltung, Rollback und Delegierung der Berechtigungsverwaltung.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
B2.d Identity and Access Management (IAM)	Sie gewährleisten eine angemessene Verwaltung und Wartung der Identitäts- und Zugriffskontrolle für Ihre Netzwerke und Informationssysteme, die wesentliche Funktionen unterstützen.	iam-group-has-users-überprüfen	AWS Identity and Access Management (IAM) kann Ihnen helfen, die Prinzipien der geringsten Rechte und der Aufgabentrennung mit Zugriffsberechtigungen und Autorisierungen zu integrieren, indem sichergestellt wird, dass IAM-Gruppen mindestens einen Benutzer haben. Die Einteilung von Benutzern in Gruppen auf der Grundlage der ihnen zugewiesenen Berechtigungen oder ihrer Funktion ist eine Möglichkeit, das Prinzip der geringsten Berechtigung zu implementieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
B2.d Identity and Access Management (IAM)	Sie gewährleisten eine angemessene Verwaltung und Wartung der Identitäts- und Zugriffskontrolle für Ihre Netzwerke und Informationssysteme, die wesentliche Funktionen unterstützen.	iam-no-inline-policy-überprüfen	Stellen Sie sicher, dass ein Benutzer, eine IAM-Rolle oder eine IAM-Gruppe (AWS Identity and Access Management) nicht über eine Inline-Richtlinie zur Zugriffskontrolle auf Systeme und Ressourcen verfügt. AWS empfiehlt, verwaltete Richtlinien anstelle von Inline-Richtlinien zu verwenden. Verwaltete Richtlinien ermöglichen Wiederverwendbarkeit, Versionsverwaltung, Rollback und Delegierung der Berechtigungsverwaltung.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
B2.d Identity and Access Management (IAM)	Sie gewährleisten eine angemessene Verwaltung und Wartung der Identitäts- und Zugriffskontrolle für Ihre Netzwerke und Informationssysteme, die wesentliche Funktionen unterstützen.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) kann Ihnen dabei helfen, die Prinzipien der geringsten Rechte und der Aufgabentrennung in Zugriffsberechtigungen und Autorisierungen zu integrieren und so zu verhindern, dass Richtlinien „Effect“: „Allow“ mit „Action“: „*“ anstelle von „Resource“: „*“ enthalten. Wenn Benutzern mehr Rechte eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und der Aufgabentrennung verstoßen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
B2.d Identity and Access Management (IAM)	Sie gewährleisten eine angemessene Verwaltung und Wartung der Identitäts- und Zugriffskontrolle für Ihre Netzwerke und Informationssysteme, die wesentliche Funktionen unterstützen.	iam-user-group-membership-überprüfen	AWS Identity and Access Management (IAM) kann Ihnen helfen, Zugriffsberechtigungen und Autorisierungen einzuschränken, indem sichergestellt wird, dass Benutzer Mitglieder mindestens einer Gruppe sind. Wenn Benutzern mehr Berechtigungen eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und Aufgabentrennung verstoßen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
B2.d Identity and Access Management (IAM)	Sie gewährleisten eine angemessene Verwaltung und Wartung der Identitäts- und Zugriffskontrolle für Ihre Netzwerke und Informationssysteme, die wesentliche Funktionen unterstützen.	iam-user-unused-credentials-überprüfen	AWS Identity and Access Management (IAM) kann Ihnen bei Zugriffsberechtigungen und Autorisierungen helfen, indem es nach IAM-Passwörtern und Zugriffsschlüsseln sucht, die für einen bestimmten Zeitraum nicht verwendet wurden. Wenn ungenutzte Anmeldeinformationen identifiziert werden, müssen Sie sie deaktivieren und/oder entfernen, da dies gegen das Prinzip der geringsten Berechtigung verstoßen könnte. Für diese Regel müssen Sie einen Wert für das maxCredentialUsage Alter festlegen (Standardkonfiguration: 90). Der tatsächliche Wert muss den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
B2.d Identity and Access Management (IAM)	Sie gewährleisten eine angemessene Verwaltung und Wartung der Identitäts- und Zugriffskontrolle für Ihre Netzwerke und Informationssysteme, die wesentliche Funktionen unterstützen.	cloudtrail-s3-dataevents-enabled	Die Erfassung von Simple Storage Service (Amazon S3)-Datenereignissen unterstützt die Erkennung von ungewöhnlichen Aktivitäten. Zu den Details gehören AWS-Konto Informationen über den Zugriff auf einen Amazon S3 S3-Bucket, die IP-Adresse und die Uhrzeit des Ereignisses.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
B2.d Identity and Access Management (IAM)	Sie gewährleisten eine angemessene Verwaltung und Wartung der Identitäts- und Zugriffskontrolle für Ihre Netzwerke und Informationssysteme, die wesentliche Funktionen unterstützen.	redshift-cluster-configuration-check	Um Daten im Ruhezustand zu schützen, muss die Verschlüsselung für Ihre Amazon-Redshift-Cluster aktiviert sein. Sie müssen auch sicherstellen, dass die erforderlichen Konfigurationen auf Amazon-Redshift-Clustern bereitgestellt werden. Die Prüfungsprotokollierung muss aktiviert sein, um Informationen zu Verbindungen und Benutzeraktivitäten in der Datenbank bereitzustellen. Diese Regel erfordert, dass ein Wert für clusterDbEncrypted (Config Default: TRUE) und LoggingEnabled (Config Default: TRUE) gesetzt ist. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
B2.d Identity and Access Management (IAM)	Sie gewährleisten eine angemessene Verwaltung und Wartung der Identitäts- und Zugriffskontrolle für Ihre Netzwerke und Informationssysteme, die wesentliche Funktionen unterstützen.	guardduty-enabled-centralized	Amazon GuardDuty kann mithilfe von Threat Intelligence Feeds helfen, potenzielle Cybersicherheitsereignisse zu überwachen und zu erkennen. Dazu gehören Listen mit bösartigen IPs und maschinellen Lernmethoden zur Identifizierung unerwarteter, nicht autorisierter und bösartiger Aktivitäten in Ihrer AWS Cloud-Umgebung.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
B2.d Identity and Access Management (IAM)	Sie gewährleisten eine angemessene Verwaltung und Wartung der Identitäts- und Zugriffskontrolle für Ihre Netzwerke und Informationssysteme, die wesentliche Funktionen unterstützen.	guardduty-non-archived-findings	Amazon GuardDuty hilft Ihnen dabei, die Auswirkungen eines Vorfalls zu verstehen, indem es die Ergebnisse nach Schweregrad klassifiziert: niedrig, mittel und hoch. Diese Klassifizierungen können Sie zur Festlegung von entsprechenden Strategien und Prioritäten zur Behebung solcher Vorfälle verwenden. Mit dieser Regel können Sie optional daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7) und daysHighSev (Config Default: 1) für nicht archivierte Ergebnisse festlegen, wie es die Richtlinien Ihrer Organisation erfordern.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
B2.d Identity and Access Management (IAM)	Sie gewährleisten eine angemessene Verwaltung und Wartung der Identitäts- und Zugriffskontrolle für Ihre Netzwerke und Informationssysteme, die wesentliche Funktionen unterstützen.	cloud-trail-cloud-watch-logs-aktiviert	Verwenden Sie Amazon CloudWatch , um Protokollereignisaktivitäten zentral zu sammeln und zu verwalten. Die Aufnahme von AWS CloudTrail Daten liefert Einzelheiten zu den API-Aufrufaktivitäten in Ihrem AWS-Konto.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
B2.d Identity and Access Management (IAM)	Sie gewährleisten eine angemessene Verwaltung und Wartung der Identitäts- und Zugriffskontrolle für Ihre Netzwerke und Informationssysteme, die wesentliche Funktionen unterstützen.	iam-password-policy	Die Identitäten und Anmeldeinformationen werden auf der Grundlage einer organisatorischen IAM-Passwortrichtlinie ausgestellt, verwaltet und verifiziert. Sie erfüllen oder übertreffen die Anforderungen von NIST SP 800-63 und dem Standard „Best Practices“ von AWS Foundational Security für die Passwortstärke. Mit dieser Regel können Sie optional RequireUppercaseCharacters (Wert für AWS grundlegende Sicherheitsbewährte Methoden: wahr), RequireLowercaseCharacters (Wert für bewährte Methoden für AWS grundlegende Sicherheit: wahr), RequireSymbols (Wert für bewährte Methoden für AWS grundlegende Sicherheit:

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			wahr), RequireNumbers (Wert für bewährte Methoden für AWS grundlegende Sicherheit: wahr), MinimumPasswordLength (Wert für bewährte Methoden für AWS grundlegende Sicherheit: 14), PasswordReusePrevention (Wert für bewährte Methoden für AWS grundlegende Sicherheit: 24) und MaxPasswordAge (Wert für bewährte Methoden für AWS grundlegende Sicherheit: 90) für Ihr IAM festlegen Kennwortrichtlinie. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
B2.d Identity and Access Management (IAM)	Sie gewährleisten eine angemessene Verwaltung und Wartung der Identitäts- und Zugriffskontrolle für Ihre Netzwerke und Informationssysteme, die wesentliche Funktionen unterstützen.	cloudwatch-alarm-action-check	Amazon CloudWatch alarmiert, wenn eine Metrik den Schwellenwert für eine bestimmte Anzahl von Bewertungszeiträumen überschreitet. Der Alarm führt eine oder mehrere Aktionen durch, die vom Wert der Metrik oder des Ausdrucks im Vergleich zu einem Schwellenwert in einer Reihe von Zeiträumen abhängt. Diese Regel erfordert einen Wert für alarmActionRequired (Config Default: True), insufficientDataAction Required (Config Default: True), okActionRequired (Config Default: False). Der tatsächliche Wert muss die Alarmaktionen für Ihre Umgebung widerspiegeln.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
B2.d Identity and Access Management (IAM)	Sie gewährleisten eine angemessene Verwaltung und Wartung der Identitäts- und Zugriffskontrolle für Ihre Netzwerke und Informationssysteme, die wesentliche Funktionen unterstützen.	securityhub-enabled	AWS Security Hub hilft bei der Überwachung von unbefugtem Personal, Verbindungen, Geräten und Software. AWS Security Hub aggregiert, organisiert und priorisiert die Sicherheitswarnungen oder Ergebnisse mehrerer Dienste. AWS Einige dieser Dienste sind Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer und AWS Firewall Manager sowie AWS Partnerlösungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
B3.a Datenkenntnis	Sie wissen, welche Daten für den Betrieb wesentlic her Funktionen wichtig sind, wo sie gespeichert sind, wohin sie übertrage n werden und wie sich deren Nichtverf ügbarkeit oder unbefugter Zugriff, Änderung oder Löschung nachteili g auf wesentliche Funktionen auswirken würden. Gleiches gilt auch für Dritte, die für den Betrieb wesentlic her Funktionen wichtige Daten speichern oder darauf zugreifen.	ec2- volume-inuse-check	Diese Regel stellt sicher, dass Amazon Elastic Block Store-Volumes, die an Amazon Elastic Compute Cloud (Amazon EC2) - Instances angehängt sind, zum Löschen markiert werden, wenn eine Instance beendet wird. Wenn ein Amazon-EB S-Volume nicht gelöscht wird, wenn die Instance, an die es angehängt ist, beendet wird, kann dies gegen das Konzept der geringsten Funktiona lität verstoßen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
B3.b Daten während der Übertragung	Sie haben die Übertragung von für wesentliche Funktionen wichtigen Daten geschützt, einschließlich der Übertragung von Daten an Dritte.	acm-certificate-expiration-check	Stellen Sie sicher, dass die Netzwerkintegrität geschützt ist, indem Sie sicherstellen, dass X509-Zertifikate von AWS ACM ausgestellt werden. Diese Zertifikate müssen gültig und dürfen nicht abgelaufen sein. Für diese Regel ist ein Wert für erforderlich daysToExpiration (Wert für bewährte AWS Grundregeln für Sicherheit: 90). Der tatsächliche Wert muss den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
B3.b Daten während der Übertragung	Sie haben die Übertragung von für wesentliche Funktionen wichtigen Daten geschützt, einschließlich der Übertragung von Daten an Dritte.	alb-http-drop-invalid-Header-aktiviert	Stellen Sie sicher, dass Ihre Elastic Load Balancers (ELB) so konfiguriert sind, dass sie HTTP-Header löschen. Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.
B3.b Daten während der Übertragung	Sie haben die Übertragung von für wesentliche Funktionen wichtigen Daten geschützt, einschließlich der Übertragung von Daten an Dritte.	alb-http-to-https-Umleitungsprüfung	Um Daten während der Übertragung zu schützen, stellen Sie sicher, dass Ihr Application Load Balancer unverschlüsselte HTTP-Anfragen automatisch an HTTPS umleitet. Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
B3.b Daten während der Übertragung	Sie haben die Übertragung von für wesentliche Funktionen wichtigen Daten geschützt, einschließlich der Übertragung von Daten an Dritte.	elasticsearch-node-to-node-Verschlüsselungsprüfung	Stellen Sie sicher, dass die node-to-node Verschlüsselung für Amazon OpenSearch Service aktiviert ist. Node-to-nodeVerschlüsselung ermöglicht die TLS 1.2-Verschlüsselung für die gesamte Kommunikation innerhalb der Amazon Virtual Private Cloud (Amazon VPC). Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
B3.b Daten während der Übertragung	Sie haben die Übertragung von für wesentliche Funktionen wichtigen Daten geschützt, einschließlich der Übertragung von Daten an Dritte.	elb-acm-certificate-required	Zum Schutz von eventuell vorhandenen sensiblen Daten sowie von Daten während der Übertragung muss die Verschlüsselung für Ihr Elastic Load Balancing aktiviert sein. Verwenden Sie AWS Certificate Manager, um öffentliche und private SSL/TLS-Zertifikate mit AWS Diensten und internen Ressourcen zu verwalten, bereitzustellen und bereitzustellen.
B3.b Daten während der Übertragung	Sie haben die Übertragung von für wesentliche Funktionen wichtigen Daten geschützt, einschließlich der Übertragung von Daten an Dritte.	elb-tls-https-listeners-nur	Stellen Sie sicher, dass Ihre Elastic Load Balancer (ELBs) mit SSL- oder HTTPS-Listenern konfiguriert sind. Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
B3.b Daten während der Übertragung	Sie haben die Übertragung von für wesentliche Funktionen wichtigen Daten geschützt, einschließlich der Übertragung von Daten an Dritte.	redshift-require-tls-ssl	Stellen Sie sicher, dass Ihre Amazon-Redshift-Cluster eine TLS/SSL-Verschlüsselung erfordern, um eine Verbindung zu SQL-Clients herzustellen. Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.
B3.b Daten während der Übertragung	Sie haben die Übertragung von für wesentliche Funktionen wichtigen Daten geschützt, einschließlich der Übertragung von Daten an Dritte.	s-3 bucket-ssl-requests-only	Um Daten während der Übertragung zu schützen, stellen Sie sicher, dass Ihre Amazon Simple Storage Service (Amazon S3)-Buckets Anfragen zur Verwendung von Secure Socket Layer (SSL)-Buckets erfordern. Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
B3.b Daten während der Übertragung	Sie haben die Übertragung von für wesentliche Funktionen wichtigen Daten geschützt, einschließlich der Übertragung von Daten an Dritte.	alb-waf-enabled	Stellen Sie sicher, dass AWS WAF auf Elastic Load Balancers (ELB) aktiviert ist, um Webanwendungen zu schützen. Eine WAF trägt zum Schutz Ihrer Webanwendungen oder APIs vor gängigen Web-Exploits bei. Diese Web-Exploits können sich auf die Verfügbarkeit auswirken, die Sicherheit gefährden oder übermäßige Ressourcen in Ihrer Umgebung verbrauchen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
B3.b Daten während der Übertragung	Sie haben die Übertragung von für wesentliche Funktionen wichtigen Daten geschützt, einschließlich der Übertragung von Daten an Dritte.	dms-replication-not-public	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass auf DMS-Replikationsinstanzen nicht öffentlich zugegriffen werden kann. DMS-Replikations-Instances können vertrauliche Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.
B3.b Daten während der Übertragung	Sie haben die Übertragung von für wesentliche Funktionen wichtigen Daten geschützt, einschließlich der Übertragung von Daten an Dritte.	ec-2 instance-no-public-ip	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon Elastic Compute Cloud (Amazon EC2) - Instances nicht öffentlich zugänglich sind. EC2 Amazon-Instances können vertrauliche Informationen enthalten, und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
B3.b Daten während der Übertragung	Sie haben die Übertragung von für wesentliche Funktionen wichtigen Daten geschützt, einschließlich der Übertragung von Daten an Dritte.	elasticsearch-in-vpc-only	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass sich Amazon OpenSearch OpenSearch Service (Service) - Domains innerhalb einer Amazon Virtual Private Cloud (Amazon VPC) befinden. Eine OpenSearch Service-Domain innerhalb einer Amazon VPC ermöglicht die sichere Kommunikation zwischen OpenSearch Service und anderen Services innerhalb der Amazon VPC, ohne dass ein Internet-Gateway, ein NAT-Gerät oder eine VPN-Verbindung erforderlich ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
B3.b Daten während der Übertragung	Sie haben die Übertragung von für wesentliche Funktionen wichtigen Daten geschützt, einschließlich der Übertragung von Daten an Dritte.	emr-master-no-public-ip	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon EMR-Cluster-Masterknoten nicht öffentlich zugänglich sind. Amazon-EMR-Cluster-Hauptknoten können vertrauliche Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
B3.b Daten während der Übertragung	Sie haben die Übertragung von für wesentliche Funktionen wichtigen Daten geschützt, einschließlich der Übertragung von Daten an Dritte.	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) Security Groups können bei der Verwaltung des Netzwerkzugriffs helfen, indem sie eine statusbehaftete Filterung von eingehendem und ausgehendem Netzwerkverkehr zu Ressourcen bereitstellen. AWS Wenn Sie eingehenden (oder entfernten) Datenverkehr von 0.0.0.0/0 bis Port 22 auf Ihren Ressourcen nicht zulassen, können Sie den Remote-Zugriff einschränken.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
B3.b Daten während der Übertragung	Sie haben die Übertragung von für wesentliche Funktionen wichtigen Daten geschützt, einschließlich der Übertragung von Daten an Dritte.	ec2- instances-in-vpc	Stellen Sie Amazon Elastic Compute Cloud (Amazon EC2) -Instances innerhalb einer Amazon Virtual Private Cloud (Amazon VPC) bereit, um eine sichere Kommunikation zwischen einer Instance und anderen Services innerhalb der Amazon VPC zu ermöglichen, ohne dass ein Internet-Gateway, ein NAT-Gerät oder eine VPN-Verbindung erforderlich ist. Der gesamte Datenverkehr bleibt sicher in der AWS Cloud. Domains, die sich innerhalb einer VPC befinden, verfügen aufgrund ihrer logischen Isolierung im Vergleich zu Domains mit öffentlichen Endpunkten über eine zusätzliche Sicherheitsebene. Weisen Sie EC2

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			Amazon-Instances einer Amazon-VPC zu, um den Zugriff ordnungsgemäß zu verwalten.
B3.b Daten während der Übertragung	Sie haben die Übertragung von für wesentliche Funktionen wichtigen Daten geschützt, einschließlich der Übertragung von Daten an Dritte.	internet-gateway-authorized-vpc-nur	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Internet-Gateways nur mit autorisierter Amazon Virtual Private Cloud (Amazon VPC) verbunden sind. Internet-Gateways ermöglichen den bidirektionalen Internetzugang zur und von der Amazon VPC, was möglicherweise zu einem unbefugten Zugriff auf Amazon-VPC-Ressourcen führen kann.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
B3.b Daten während der Übertragung	Sie haben die Übertragung von für wesentliche Funktionen wichtigen Daten geschützt, einschließlich der Übertragung von Daten an Dritte.	lambda-inside-vpc	Stellen Sie AWS Lambda-Funktionen in einer Amazon Virtual Private Cloud (Amazon VPC) bereit, um eine sichere Kommunikation zwischen einer Funktion und anderen Diensten innerhalb der Amazon VPC zu gewährleisten. Bei dieser Konfiguration sind kein Internet-Gateway, kein NAT-Gerät und keine VPN-Verbindung erforderlich. Der gesamte Datenverkehr bleibt sicher in der Cloud. AWS Domains, die sich innerhalb einer VPC befinden, verfügen aufgrund ihrer logischen Isolierung im Vergleich zu Domains mit öffentlichen Endpunkten über eine zusätzliche Sicherheitsebene. Um den Zugriff ordnungsgemäß zu verwalten,

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			sollten AWS Lambda-Funktionen einer VPC zugewiesen werden.
B3.b Daten während der Übertragung	Sie haben die Übertragung von für wesentliche Funktionen wichtigen Daten geschützt, einschließlich der Übertragung von Daten an Dritte.	rds-instance-public-access-überprüfen	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Relational Database Service (Amazon RDS) -Instances nicht öffentlich sind. Amazon-RDS-Datenbank-Instances können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
B3.b Daten während der Übertragung	Sie haben die Übertragung von für wesentliche Funktionen wichtigen Daten geschützt, einschließlich der Übertragung von Daten an Dritte.	redshift-cluster-public-access-überprüfen	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Redshift Redshift-Cluster nicht öffentlich sind. Amazon-Redshift-Cluster können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
B3.b Daten während der Übertragung	Sie haben die Übertragung von für wesentliche Funktionen wichtigen Daten geschützt, einschließlich der Übertragung von Daten an Dritte.	restricted-common-ports	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass gemeinsame Ports für Amazon Elastic Compute Cloud (Amazon EC2) -Sicherheitsgruppen eingeschränkt sind. Wenn der Zugriff auf Ports nicht auf vertrauenswürdige Quellen beschränkt wird, kann dies zu Angriffen auf die Verfügbarkeit, Integrität und Vertraulichkeit von Systemen führen. Mit dieser Regel können Sie optional die Parameter blockedPort1–blockedPort5 festlegen (Standardkonfigurationen: 20, 21, 3389, 3306, 4333). Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
B3.b Daten während der Übertragung	Sie haben die Übertragung von für wesentliche Funktionen wichtigen Daten geschützt, einschließlich der Übertragung von Daten an Dritte.	sagemaker-notebook-no-direct-Internetzugang	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass SageMaker Amazon-Notebooks keinen direkten Internetzugang zulassen. Indem Sie direkten Internetzugang blockieren, vermeiden Sie, dass unbefugte Benutzer auf sensible Daten zugreifen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
B3.b Daten während der Übertragung	Sie haben die Übertragung von für wesentliche Funktione n wichtigen Daten geschützt, einschlie ßlich der Übertragung von Daten an Dritte.	vpc-default-security-group-geschlossen	Sicherheitsgruppen von Amazon Elastic Compute Cloud (Amazon EC2) können bei der Verwaltung des Netzwerkzugriffs helfen, indem sie eine statusbehaftete Filterung des ein- und ausgehenden Netzwerkverkehrs zu Ressourcen bereitstellen. AWS Die Beschränk ung des gesamten Datenverkehrs auf die Standardsicherheit sgruppe hilft dabei, den Fernzugriff auf Ihre Ressourcen einzuschränken. AWS

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
B3.b Daten während der Übertragung	Sie haben die Übertragung von für wesentliche Funktionen wichtigen Daten geschützt, einschließlich der Übertragung von Daten an Dritte.	vpc-sg-open-only-to-authorized-ports	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass gemeinsame Ports für Amazon Elastic Compute Cloud (Amazon EC2) -Sicherheitsgruppen eingeschränkt sind. Wenn der Zugriff auf Ports nicht auf vertrauenswürdige Quellen beschränkt wird, kann dies zu Angriffen auf die Verfügbarkeit, Integrität und Vertraulichkeit von Systemen führen. Durch die Beschränkung des Zugriffs auf Ressourcen innerhalb einer Sicherheitsgruppe aus dem Internet (0.0.0.0/0) kann der Remote-Zugriff auf interne Systeme gesteuert werden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
B3.b Daten während der Übertragung	Sie haben die Übertragung von für wesentliche Funktionen wichtigen Daten geschützt, einschließlich der Übertragung von Daten an Dritte.	autoscaling-group-elb-healthcheck-erforderlich	Die Elastic Load Balancer (ELB) - Zustandsprüfungen für Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling Scaling-Gruppen unterstützen die Aufrechterhaltung einer angemessenen Kapazität und Verfügbarkeit. Der Load Balancer sendet regelmäßig Pings, versucht Verbindungen herzustellen oder sendet Anfragen, um den Zustand der EC2 Amazon-Instances in einer Gruppe mit auto-scaling zu testen. Wenn eine Instance nicht zurückmeldet, wird der Traffic an eine neue EC2 Amazon-Instance gesendet.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
B3.b Daten während der Übertragung	Sie haben die Übertragung von für wesentliche Funktionen wichtigen Daten geschützt, einschließlich der Übertragung von Daten an Dritte.	elb-cross-zone-load-Balancing aktiviert	Aktivieren Sie zonenübergreifendes Load Balancing für Ihre Elastic Load Balancer (ELBs), um eine angemessene Kapazität und Verfügbarkeit aufrechtzuerhalten. Zonenübergreifendes Load Balancing reduziert die Notwendigkeit, die gleiche Anzahl von Instances in jeder aktivierten Availability Zone aufrechtzuerhalten. Es verbessert auch die Fähigkeit Ihrer Anwendung, den Verlust einer oder mehrerer Instances zu bewältigen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
B3.b Daten während der Übertragung	Sie haben die Übertragung von für wesentliche Funktionen wichtigen Daten geschützt, einschließlich der Übertragung von Daten an Dritte.	elb-deletion-protection-enabled	Diese Regel sorgt dafür, dass der Löschschutz für Elastic Load Balancing aktiviert ist. Verwenden Sie diese Funktion, um zu verhindern, dass Ihr Load Balancer versehentlich oder böswillig gelöscht wird, was zum Verlust der Verfügbarkeit Ihrer Anwendungen führen kann.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
B3.b Daten während der Übertragung	Sie haben die Übertragung von für wesentliche Funktionen wichtigen Daten geschützt, einschließlich der Übertragung von Daten an Dritte.	vpc-vpn-2-tunnels-up	Redundante Site-to-Site VPN-Tunnel können implementiert werden, um die Anforderungen an die Ausfallsicherheit zu erfüllen. Es verwendet zwei Tunnel, um die Konnektivität sicherzustellen, falls eine der Site-to-Site VPN-Verbindungen nicht verfügbar ist. Um sich vor einem Verbindungsverlust zu schützen, können Sie für den Fall, dass Ihr Kunden-Gateway nicht verfügbar ist, eine zweite Site-to-Site VPN-Verbindung zu Ihrer Amazon Virtual Private Cloud (Amazon VPC) und Ihrem Virtual Private Gateway einrichten, indem Sie ein zweites Kunden-Gateway verwenden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
B3.b Daten während der Übertragung	Sie haben die Übertragung von für wesentliche Funktionen wichtigen Daten geschützt, einschließlich der Übertragung von Daten an Dritte.	api-gw-cache-enabled-und verschlüsselt	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass die Verschlüsselung für den Cache Ihrer API-Gateway-Stufe aktiviert ist. Da für die API-Methode sensible Daten erfasst werden können, sollten Sie die Verschlüsselung von Daten im Ruhezustand aktivieren, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
B3.b Daten während der Übertragung	Sie haben die Übertragung von für wesentliche Funktionen wichtigen Daten geschützt, einschließlich der Übertragung von Daten an Dritte.	opensearch-node-to-node-Verschlüsselungsprüfung	Stellen Sie sicher, dass die node-to-node Verschlüsselung für Amazon OpenSearch Service aktiviert ist. Node-to-nodeVerschlüsselung ermöglicht die TLS 1.2-Verschlüsselung für die gesamte Kommunikation innerhalb der Amazon Virtual Private Cloud (Amazon VPC). Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
B3.b Daten während der Übertragung	Sie haben die Übertragung von für wesentliche Funktionen wichtigen Daten geschützt, einschließlich der Übertragung von Daten an Dritte.	opensearch-in-vpc-only	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass sich Amazon OpenSearch Service-Domains innerhalb einer Amazon Virtual Private Cloud (Amazon VPC) befinden. Eine Amazon OpenSearch Service-Domain innerhalb einer Amazon VPC ermöglicht die sichere Kommunikation zwischen Amazon OpenSearch Service und anderen Services innerhalb der Amazon VPC, ohne dass ein Internet-Gateway, ein NAT-Gerät oder eine VPN-Verbindung erforderlich ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
B3.c Gespeicherte Daten	Sie haben gespeicherte Daten, die für den Betrieb wesentlicher Funktionen wichtig sind, geschützt.	cloud-trail-encryption-enabled	Da sensible Daten vorhanden sein können und um Daten im Speicher zu schützen, sollten Sie sicherstellen, dass die Verschlüsselung für Ihre AWS CloudTrail Trails aktiviert ist.
B3.c Gespeicherte Daten	Sie haben gespeicherte Daten, die für den Betrieb wesentlicher Funktionen wichtig sind, geschützt.	cloudwatch-log-group-encrypted	Um sensible Daten im Speicher zu schützen, stellen Sie sicher, dass die Verschlüsselung für Ihre Amazon CloudWatch Log Groups aktiviert ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
B3.c Gespeicherte Daten	Sie haben gespeicherte Daten, die für den Betrieb wesentlicher Funktionen wichtig sind, geschützt.	dynamodb-table-encrypted-kms	Stellen Sie sicher, dass die Verschlüsselung für Ihre Amazon-DynamoDB-Tabellen aktiviert ist. Um eventuell vorhandene sensible Daten im Ruhezustand in diesen Tabellen zu schützen, müssen Sie die Verschlüsselung von Daten im Ruhezustand aktivieren. Standardmäßig werden DynamoDB-Tabellen mit einem AWS eigenen Kundenhauptschlüssel (CMK) verschlüselt.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
B3.c Gespeicherte Daten	Sie haben gespeicherte Daten, die für den Betrieb wesentlicher Funktionen wichtig sind, geschützt.	ec2- ebs-encryption-by-default	Zum Schutz von Daten im Ruhezustand müssen Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon Elastic Block Store (Amazon EBS)-Volumes aktiviert ist. Da sensible Daten auch im Ruhezustand vorhanden sein können, sollten Sie die Verschlüsselung im Ruhezustand aktivieren, um diese Daten zu schützen.
B3.c Gespeicherte Daten	Sie haben gespeicherte Daten, die für den Betrieb wesentlicher Funktionen wichtig sind, geschützt.	efs-encrypted-check	Aktivieren Sie die Verschlüsselung für Ihr Amazon Elastic File System (EFS), um eventuell vorhandene sensible Daten sowie Daten im Ruhezustand zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
B3.c Gespeicherte Daten	Sie haben gespeicherte Daten, die für den Betrieb wesentlicher Funktionen wichtig sind, geschützt.	elasticsearch-encrypted-at-rest	Da sensible Daten vorhanden sein können und um Daten im Ruhezustand zu schützen, sollten Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon OpenSearch Service (OpenSearch Service) -Domains aktiviert ist.
B3.c Gespeicherte Daten	Sie haben gespeicherte Daten, die für den Betrieb wesentlicher Funktionen wichtig sind, geschützt.	encrypted-volumes	Aktivieren Sie die Verschlüsselung für Ihre Amazon-Elastic-Block-Store (Amazon-EBS)-Volumes, um eventuell vorhandene sensible Daten sowie Daten im Ruhezustand zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
B3.c Gespeicherte Daten	Sie haben gespeicherte Daten, die für den Betrieb wesentlicher Funktionen wichtig sind, geschützt.	rds-snapshot-encrypted	Stellen Sie sicher, dass die Verschlüsselung für Ihre Amazon Relational Database Service (Amazon RDS)-Snapshots aktiviert ist. Da sensible Daten auch im Ruhezustand vorhanden sein können, sollten Sie die Verschlüsselung im Ruhezustand aktivieren, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
B3.c Gespeicherte Daten	Sie haben gespeicherte Daten, die für den Betrieb wesentlicher Funktionen wichtig sind, geschützt.	rds-storage-encrypted	Zum Schutz von Daten im Ruhezustand müssen Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon Relational Database Service (Amazon RDS)-Instances aktiviert ist. Um eventuell vorhandene sensible Daten im Ruhezustand in Amazon-RDS-Instances zu schützen, muss die Verschlüsselung von Daten im Ruhezustand aktiviert sein.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
B3.c Gespeicherte Daten	Sie haben gespeicherte Daten, die für den Betrieb wesentlicher Funktionen wichtig sind, geschützt.	redshift-cluster-configuration-check	Um Daten im Ruhezustand zu schützen, muss die Verschlüsselung für Ihre Amazon-Redshift-Cluster aktiviert sein. Sie müssen auch sicherstellen, dass die erforderlichen Konfigurationen auf Amazon-Redshift-Clustern bereitgestellt werden. Die Prüfungsprotokollierung muss aktiviert sein, um Informationen zu Verbindungen und Benutzeraktivitäten in der Datenbank bereitzustellen. Diese Regel erfordert, dass ein Wert für clusterDbEncrypted (Config Default: TRUE) und LoggingEnabled (Config Default: TRUE) gesetzt ist. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
B3.c Gespeicherte Daten	Sie haben gespeicherte Daten, die für den Betrieb wesentlicher Funktionen wichtig sind, geschützt.	s3-aktiviert bucket-server-side-encryption	Zum Schutz von Daten im Ruhezustand müssen Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon Simple Storage Service (Amazon S3)-Buckets aktiviert ist. Um eventuell vorhandene sensible Daten im Ruhezustand in Amazon-S3-Buckets zu schützen, muss die Verschlüsselung aktiviert sein.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
B3.c Gespeicherte Daten	Sie haben gespeicherte Daten, die für den Betrieb wesentlicher Funktionen wichtig sind, geschützt.	sagemaker-endpoint-configuration-kms-key-konfiguriert	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass die Verschlüsselung mit dem AWS Key Management Service (AWS KMS) für Ihren Endpunkt aktiviert ist. SageMaker Da sensible Daten auf dem SageMaker Endgerät gespeichert werden können, sollten Sie die Verschlüsselung im Ruhezustand aktivieren, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
B3.c Gespeicherte Daten	Sie haben gespeicherte Daten, die für den Betrieb wesentlicher Funktionen wichtig sind, geschützt.	sagemaker-notebook-instance-kms-schlüsselkonfiguriert	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass die Verschlüsselung mit dem AWS Key Management Service (AWS KMS) für Ihr Notebook aktiviert ist. SageMaker Da vertrauliche Daten im SageMaker Notebook gespeichert werden können, sollten Sie die Verschlüsselung im Ruhezustand aktivieren, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
B3.c Gespeicherte Daten	Sie haben gespeicherte Daten, die für den Betrieb wesentlicher Funktionen wichtig sind, geschützt.	sns-encrypted-kms	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass Ihre Amazon Simple Notification Service (Amazon SNS) -Themen mit dem AWS Key Management Service (AWS KMS) verschlüsselt werden müssen. Um eventuell vorhandene sensible Daten im Ruhezustand in veröffentlichten Nachrichten zu schützen, muss die Verschlüsselung von Daten im Ruhezustand aktiviert sein.
B3.c Gespeicherte Daten	Sie haben gespeicherte Daten, die für den Betrieb wesentlicher Funktionen wichtig sind, geschützt.	cmk-backing-key-rotation-aktiviert	Aktivieren Sie die Schlüsselrotation, um sicherzustellen, dass Schlüssel rotiert werden, nachdem sie das Ende ihrer Krypto-Periode erreicht haben.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
B3.c Gespeicherte Daten	Sie haben gespeicherte Daten, die für den Betrieb wesentlicher Funktionen wichtig sind, geschützt.	kms-cmk-not-scheduled-zum Löschen	Um Daten im Ruhezustand zu schützen, sollten Sie sicherstellen, dass die für den Kunden erforderlichen Masterschlüssel (CMKs) nicht für das Löschen im AWS Key Management Service (AWS KMS) vorgesehen sind. Da Schlüssel manchmal gelöscht werden müssen, können Sie mit dieser Regel alle zu löschenden Schlüssel überprüfen, falls ein Schlüssel versehentlich zur Löschung vorgemerkt wurde.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
B3.c Gespeicherte Daten	Sie haben gespeicherte Daten, die für den Betrieb wesentlicher Funktionen wichtig sind, geschützt.	db-instance-backup-enabled	Die Sicherungsfunktion von Amazon RDS erstellt Sicherungen Ihrer Datenbanken und Transaktionsprotokolle. Amazon RDS erstellt einen Snapshot für das Speichervolume Ihrer DB-Instance, sodass die gesamte DB-Instance gesichert wird. Sie können im System spezifische Aufbewahrungsfristen festlegen, um Ihre Ausfallsicherheitsanforderungen zu erfüllen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
B3.c Gespeicherte Daten	Sie haben gespeicherte Daten, die für den Betrieb wesentlicher Funktionen wichtig sind, geschützt.	dynamodb-in-backup-plan	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon DynamoDB-Tabellen Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
B3.c Gespeicherte Daten	Sie haben gespeicherte Daten, die für den Betrieb wesentlicher Funktionen wichtig sind, geschützt.	dynamodb-pitr-enabled	Aktivieren Sie diese Regel, um zu überprüfen, ob die Informationen gesichert wurden. Es verwaltet auch die Backups, indem es sicherstellt, dass die point-in-time Wiederherstellung in Amazon DynamoDB aktiviert ist. Bei der Wiederherstellung werden fortlaufende Backups Ihrer Tabelle für die letzten 35 Tage gespeichert.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
B3.c Gespeicherte Daten	Sie haben gespeicherte Daten, die für den Betrieb wesentlicher Funktionen wichtig sind, geschützt.	ebs-in-backup-plan	Stellen Sie zur Unterstützung der Datensicherungsprozesse sicher, dass Ihre Amazon Elastic Block Store (Amazon EBS) -Volumes Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
B3.c Gespeicherte Daten	Sie haben gespeicherte Daten, die für den Betrieb wesentlicher Funktionen wichtig sind, geschützt.	ebs-optimized-instance	Eine optimierte Instance im Amazon Elastic Block Store (Amazon EBS) bietet zusätzliche, dedizierte Kapazität für Amazon-EBS-I/O-Vorgänge. Diese Optimierung bietet die beste Leistung für Ihr EBS-Volume, indem Konflikte zwischen Amazon-EBS-I/O und anderem Datenverkehr von Ihrer Instance minimiert werden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
B3.c Gespeicherte Daten	Sie haben gespeicherte Daten, die für den Betrieb wesentlicher Funktionen wichtig sind, geschützt.	efs-in-backup-plan	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon Elastic File System (Amazon EFS) -Dateisysteme Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
B3.c Gespeicherte Daten	Sie haben gespeicherte Daten, die für den Betrieb wesentlicher Funktionen wichtig sind, geschützt.	elasticache-redis-cluster-automatic-Backup-Check	Wenn automatische Backups aktiviert sind, ElastiCache erstellt Amazon täglich ein Backup des Clusters. Die Sicherung kann für eine von Ihrer Organisation festgelegte Anzahl von Tagen aufbewahrt werden. Automatische Backups schützen vor Datenverlust. Bei einem Ausfall können Sie einen neuen Cluster erstellen, der Ihre Daten aus dem aktuellen Backup wiederherstellt.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
B3.c Gespeicherte Daten	Sie haben gespeicherte Daten, die für den Betrieb wesentlicher Funktionen wichtig sind, geschützt.	rds-in-backup-plan	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon Relational Database Service (Amazon RDS) -Instances Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
B3.c Gespeicherte Daten	Sie haben gespeicherte Daten, die für den Betrieb wesentlicher Funktionen wichtig sind, geschützt.	s-3 bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) unterstützt die Aufrechterhaltung einer angemessenen Kapazität und Verfügbarkeit. CRR ermöglicht das automatische, asynchrone Kopieren von Objekten in Amazon-S3-Buckets, um die Datenverfügbarkeit sicherzustellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
B3.c Gespeicherte Daten	Sie haben gespeicherte Daten, die für den Betrieb wesentlicher Funktionen wichtig sind, geschützt.	s-3 bucket-versioning-enabled	Die Versionsverwaltung von Amazon Simple Storage Service (Amazon S3)-Buckets hilft dabei, mehrere Varianten eines Objekts im selben Amazon-S3-Bucket zu speichern. Verwenden Sie die Versionsverwaltung, um sämtliche Versionen aller Objekte in Ihrem Amazon-S3-Bucket zu speichern, abzurufen oder wiederherzustellen. Mit der Versionsverwaltung können Sie Versionen sowohl nach unbeabsichtigten Benutzeraktionen als auch nach Anwendungsfehlern problemlos wiederherstellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
B3.c Gespeicherte Daten	Sie haben gespeicherte Daten, die für den Betrieb wesentlicher Funktionen wichtig sind, geschützt.	rds-instance-deletion-protection-aktiviert	Stellen Sie sicher, dass Amazon Relational Database Service (Amazon RDS)-Instances den Löschschutz aktiviert haben. Verwenden Sie den Löschschutz, um zu verhindern, dass Ihre Amazon-RDS-Instances versehentlich oder böswillig gelöscht werden, was zum Verlust der Verfügbarkeit Ihrer Anwendungen führen kann.
B3.c Gespeicherte Daten	Sie haben gespeicherte Daten, die für den Betrieb wesentlicher Funktionen wichtig sind, geschützt.	s3- bucket-default-lock-enabled	Stellen Sie sicher, dass für Ihren Amazon Simple Storage Service (Amazon S3)-Bucket standardmäßig eine Sperre aktiviert ist. Zum Schutz eventuell vorhandener sensibler Daten in S3-Buckets müssen Sie Objektsperren für Daten im Ruhezustand erzwingen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
B3.c Gespeicherte Daten	Sie haben gespeicherte Daten, die für den Betrieb wesentlicher Funktionen wichtig sind, geschützt.	rds-multi-az-support	Die Multi-AZ-Unterstützung in Amazon Relational Database Service (Amazon RDS) bietet eine verbesserte Verfügbarkeit und Beständigkeit von Datenbank-Instances. Wenn Sie eine Multi-AZ-Datenbank-Instance bereitstellen, erstellt Amazon RDS automatisch eine primäre Datenbank-Instance und repliziert die Daten synchron auf eine Standby-Instance in einer anderen Availability Zone. Jede Availability Zone läuft auf einer eigenen, physisch getrennten, unabhängigen Infrastruktur und ist auf eine hohe Verfügbarkeit ausgelegt. Im Falle eines Infrastrukturausfalls führt Amazon RDS einen automatis

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			chen Failover zum Standby-Modus durch, sodass Sie den Datenbankbetrieb wieder aufnehmen können, sobald der Failover abgeschlo ssen ist.
B3.c Gespeicherte Daten	Sie haben gespeiche rte Daten, die für den Betrieb wesentlicher Funktionen wichtig sind, geschützt.	acm-certificate-ex piration-check	Stellen Sie sicher, dass die Netzwerki ntegrität geschützt ist, indem Sie sicherste llen, dass X509-Zertifikate von AWS ACM ausgestel lt werden. Diese Zertifikate müssen gültig und dürfen nicht abgelaufen sein. Für diese Regel ist ein Wert für erforderlich daysToExpiration (Wert für bewährte AWS Grundregeln für Sicherheit: 90). Der tatsächliche Wert muss den Richtlini en Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
B3.c Gespeicherte Daten	Sie haben gespeicherte Daten, die für den Betrieb wesentlicher Funktionen wichtig sind, geschützt.	opensearch-encrypted-at-rest	Da sensible Daten vorhanden sein können und um Daten im Ruhezustand zu schützen, sollten Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon OpenSearch Service-Domains aktiviert ist.
B4.a Secure by Design	Sie integrieren Sicherheit in die Netzwerk- und Informationssysteme, die den Betrieb wesentlicher Funktionen unterstützen. Sie minimieren deren Angriffsfläche und stellen sicher, dass der Betrieb wesentlicher Funktionen nicht durch die Ausnutzung einzelner Schwachstellen beeinträchtigt wird.	alb-http-drop-invalid-Header-fähig	Stellen Sie sicher, dass Ihre Elastic Load Balancers (ELB) so konfiguriert sind, dass sie HTTP-Header löschen. Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
B4.a Secure by Design	Sie integrieren Sicherheit in die Netzwerk- und Informationssysteme, die den Betrieb wesentlicher Funktionen unterstützen. Sie minimieren deren Angriffsfläche und stellen sicher, dass der Betrieb wesentlicher Funktionen nicht durch die Ausnutzung einzelner Schwachstellen beeinträchtigt wird.	alb-http-to-https-Umleitungsprüfung	Um Daten während der Übertragung zu schützen, stellen Sie sicher, dass Ihr Application Load Balancer unverschlüsselte HTTP-Anfragen automatisch an HTTPS umleitet. Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
B4.a Secure by Design	Sie integrieren Sicherheit in die Netzwerk- und Informationssysteme, die den Betrieb wesentlicher Funktionen unterstützen. Sie minimieren deren Angriffsfläche und stellen sicher, dass der Betrieb wesentlicher Funktionen nicht durch die Ausnutzung einzelner Schwachstellen beeinträchtigt wird.	alb-waf-enabled	Stellen Sie sicher, dass AWS WAF auf Elastic Load Balancers (ELB) aktiviert ist, um Webanwendungen zu schützen. Eine WAF trägt zum Schutz Ihrer Webanwendungen oder APIs vor gängigen Web-Exploits bei. Diese Web-Exploits können sich auf die Verfügbarkeit auswirken, die Sicherheit gefährden oder übermäßige Ressourcen in Ihrer Umgebung verbrauchen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
B4.a Secure by Design	Sie integrieren Sicherheit in die Netzwerk- und Informationssysteme, die den Betrieb wesentlicher Funktionen unterstützen. Sie minimieren deren Angriffsfläche und stellen sicher, dass der Betrieb wesentlicher Funktionen nicht durch die Ausnutzung einzelner Schwachstellen beeinträchtigt wird.	dms-replication-not-public	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass auf DMS-Replikationsinstanzen nicht öffentlich zugegriffen werden kann. DMS-Replikations-Instances können vertrauliche Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
B4.a Secure by Design	Sie integrieren Sicherheit in die Netzwerk- und Informationssysteme, die den Betrieb wesentlicher Funktionen unterstützen. Sie minimieren deren Angriffsfläche und stellen sicher, dass der Betrieb wesentlicher Funktionen nicht durch die Ausnutzung einzelner Schwachstellen beeinträchtigt wird.	ebs-snapshot-public-restorable-überprüfen	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass EBS-Snapshots nicht öffentlich wiederherstellbar sind. EBS-Volume-Snapshots können vertrauliche Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
B4.a Secure by Design	Sie integrieren Sicherheit in die Netzwerk- und Informationssysteme, die den Betrieb wesentlicher Funktionen unterstützen. Sie minimieren deren Angriffsfläche und stellen sicher, dass der Betrieb wesentlicher Funktionen nicht durch die Ausnutzung einzelner Schwachstellen beeinträchtigt wird.	ec-2 instance-no-public-ip	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon Elastic Compute Cloud (Amazon EC2) - Instances nicht öffentlich zugänglich sind. EC2 Amazon-Instances können vertrauliche Informationen enthalten, und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
B4.a Secure by Design	Sie integrieren Sicherheit in die Netzwerk- und Informationssysteme, die den Betrieb wesentlicher Funktionen unterstützen. Sie minimieren deren Angriffsfläche und stellen sicher, dass der Betrieb wesentlicher Funktionen nicht durch die Ausnutzung einzelner Schwachstellen beeinträchtigt wird.	elasticsearch-in-vpc-only	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass sich Amazon OpenSearch OpenSearch Service (Service) - Domains innerhalb einer Amazon Virtual Private Cloud (Amazon VPC) befinden. Eine OpenSearch Service-Domain innerhalb einer Amazon VPC ermöglicht die sichere Kommunikation zwischen OpenSearch Service und anderen Services innerhalb der Amazon VPC, ohne dass ein Internet-Gateway, ein NAT-Gerät oder eine VPN-Verbindung erforderlich ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
B4.a Secure by Design	Sie integrieren Sicherheit in die Netzwerk- und Informationssysteme, die den Betrieb wesentlicher Funktionen unterstützen. Sie minimieren deren Angriffsfläche und stellen sicher, dass der Betrieb wesentlicher Funktionen nicht durch die Ausnutzung einzelner Schwachstellen beeinträchtigt wird.	elb-acm-certificate-required	Zum Schutz von eventuell vorhandenen sensiblen Daten sowie von Daten während der Übertragung muss die Verschlüsselung für Ihr Elastic Load Balancing aktiviert sein. Verwenden Sie AWS Certificate Manager, um öffentliche und private SSL/TLS-Zertifikate mit AWS Diensten und internen Ressourcen zu verwalten, bereitzustellen und bereitzustellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
B4.a Secure by Design	Sie integrieren Sicherheit in die Netzwerk- und Informationssysteme, die den Betrieb wesentlicher Funktionen unterstützen. Sie minimieren deren Angriffsfläche und stellen sicher, dass der Betrieb wesentlicher Funktionen nicht durch die Ausnutzung einzelner Schwachstellen beeinträchtigt wird.	elb-tls-https-listeners-nur	Stellen Sie sicher, dass Ihre Elastic Load Balancer (ELBs) mit SSL- oder HTTPS-Listenern konfiguriert sind. Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
B4.a Secure by Design	Sie integrieren Sicherheit in die Netzwerk- und Informationssysteme, die den Betrieb wesentlicher Funktionen unterstützen. Sie minimieren deren Angriffsfläche und stellen sicher, dass der Betrieb wesentlicher Funktionen nicht durch die Ausnutzung einzelner Schwachstellen beeinträchtigt wird.	emr-master-no-public-ip	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon EMR-Cluster-Masterknoten nicht öffentlich zugänglich sind. Amazon-EMR-Cluster-Hauptknoten können vertrauliche Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
B4.a Secure by Design	Sie integrieren Sicherheit in die Netzwerk- und Informationssysteme, die den Betrieb wesentlicher Funktionen unterstützen. Sie minimieren deren Angriffsfläche und stellen sicher, dass der Betrieb wesentlicher Funktionen nicht durch die Ausnutzung einzelner Schwachstellen beeinträchtigt wird.	guardduty-enabled-centralized	Amazon GuardDuty kann mithilfe von Threat Intelligence Feeds helfen, potenzielle Cybersicherheitsereignisse zu überwachen und zu erkennen. Dazu gehören Listen mit bösartigen IPs und maschinellen Lernmethoden zur Identifizierung unerwarteter, nicht autorisierter und bösartiger Aktivitäten in Ihrer AWS Cloud-Umgebung.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
B4.a Secure by Design	Sie integrieren Sicherheit in die Netzwerk- und Informationssysteme, die den Betrieb wesentlicher Funktionen unterstützen. Sie minimieren deren Angriffsfläche und stellen sicher, dass der Betrieb wesentlicher Funktionen nicht durch die Ausnutzung einzelner Schwachstellen beeinträchtigt wird.	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) Security Groups können bei der Verwaltung des Netzwerkzugriffs helfen, indem sie eine statusbehaftete Filterung von eingehendem und ausgehendem Netzwerkverkehr zu Ressourcen bereitstellen. AWS Wenn Sie eingehenden (oder entfernten) Datenverkehr von 0.0.0.0/0 bis Port 22 auf Ihren Ressourcen nicht zulassen, können Sie den Remote-Zugriff einschränken.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
B4.a Secure by Design	Sie integrieren Sicherheit in die Netzwerk- und Informationssysteme, die den Betrieb wesentlicher Funktionen unterstützen. Sie minimieren deren Angriffsfläche und stellen sicher, dass der Betrieb wesentlicher Funktionen nicht durch die Ausnutzung einzelner Schwachstellen beeinträchtigt wird.	ec2- instances-in-vpc	Stellen Sie Amazon Elastic Compute Cloud (Amazon EC2) -Instances innerhalb einer Amazon Virtual Private Cloud (Amazon VPC) bereit, um eine sichere Kommunikation zwischen einer Instance und anderen Services innerhalb der Amazon VPC zu ermöglichen, ohne dass ein Internet-Gateway, ein NAT-Gerät oder eine VPN-Verbindung erforderlich ist. Der gesamte Datenverkehr bleibt sicher in der AWS Cloud. Domains, die sich innerhalb einer VPC befinden, verfügen aufgrund ihrer logischen Isolierung im Vergleich zu Domains mit öffentlichen Endpunkten über eine zusätzliche Sicherheitsebene. Weisen Sie EC2

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			Amazon-Instances einer Amazon-VPC zu, um den Zugriff ordnungsgemäß zu verwalten.
B4.a Secure by Design	Sie integrieren Sicherheit in die Netzwerk- und Informationssysteme, die den Betrieb wesentlicher Funktionen unterstützen. Sie minimieren deren Angriffsfläche und stellen sicher, dass der Betrieb wesentlicher Funktionen nicht durch die Ausnutzung einzelner Schwachstellen beeinträchtigt wird.	internet-gateway-authorized-vpc-nur	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Internet-Gateways nur mit autorisierter Amazon Virtual Private Cloud (Amazon VPC) verbunden sind. Internet-Gateways ermöglichen den bidirektionalen Internetzugang zur und von der Amazon VPC, was möglicherweise zu einem unbefugten Zugriff auf Amazon-VPC-Ressourcen führen kann.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
B4.a Secure by Design	Sie integrieren Sicherheit in die Netzwerk- und Informationssysteme, die den Betrieb wesentlicher Funktionen unterstützen. Sie minimieren deren Angriffsfläche und stellen sicher, dass der Betrieb wesentlicher Funktionen nicht durch die Ausnutzung einzelner Schwachstellen beeinträchtigt wird.	lambda-function-public-access-verboten	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass AWS Lambda-Funktionen nicht öffentlich zugänglich sind. Der öffentliche Zugriff kann möglicherweise die Verfügbarkeit von Ressourcen beeinträchtigen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
B4.a Secure by Design	Sie integrieren Sicherheit in die Netzwerk- und Informationssysteme, die den Betrieb wesentlicher Funktionen unterstützen. Sie minimieren deren Angriffsfläche und stellen sicher, dass der Betrieb wesentlicher Funktionen nicht durch die Ausnutzung einzelner Schwachstellen beeinträchtigt wird.	lambda-inside-vpc	Stellen Sie AWS Lambda-Funktionen in einer Amazon Virtual Private Cloud (Amazon VPC) bereit, um eine sichere Kommunikation zwischen einer Funktion und anderen Diensten innerhalb der Amazon VPC zu gewährleisten. Bei dieser Konfiguration sind kein Internet-Gateway, kein NAT-Gerät und keine VPN-Verbindung erforderlich. Der gesamte Datenverkehr bleibt sicher in der Cloud. AWS Domains, die sich innerhalb einer VPC befinden, verfügen aufgrund ihrer logischen Isolierung im Vergleich zu Domains mit öffentlichen Endpunkten über eine zusätzliche Sicherheitsebene. Um den Zugriff ordnungsgemäß zu verwalten,

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			sollten AWS Lambda-Funktionen einer VPC zugewiesen werden.
B4.a Secure by Design	Sie integrieren Sicherheit in die Netzwerk- und Informationssysteme, die den Betrieb wesentlicher Funktionen unterstützen. Sie minimieren deren Angriffsfläche und stellen sicher, dass der Betrieb wesentlicher Funktionen nicht durch die Ausnutzung einzelner Schwachstellen beeinträchtigt wird.	rds-instance-public-access-überprüfen	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Relational Database Service (Amazon RDS) -Instances nicht öffentlich sind. Amazon-RDS-Datenbank-Instances können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
B4.a Secure by Design	Sie integrieren Sicherheit in die Netzwerk- und Informationssysteme, die den Betrieb wesentlicher Funktionen unterstützen. Sie minimieren deren Angriffsfläche und stellen sicher, dass der Betrieb wesentlicher Funktionen nicht durch die Ausnutzung einzelner Schwachstellen beeinträchtigt wird.	rds-snapshots-public-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Relational Database Service (Amazon RDS) -Instances nicht öffentlich sind. Amazon-RDS-Datenbank-Instances können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
B4.a Secure by Design	Sie integrieren Sicherheit in die Netzwerk- und Informationssysteme, die den Betrieb wesentlicher Funktionen unterstützen. Sie minimieren deren Angriffsfläche und stellen sicher, dass der Betrieb wesentlicher Funktionen nicht durch die Ausnutzung einzelner Schwachstellen beeinträchtigt wird.	redshift-cluster-public-access-überprüfen	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Redshift Redshift-Cluster nicht öffentlich sind. Amazon-Redshift-Cluster können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
B4.a Secure by Design	Sie integrieren Sicherheit in die Netzwerk- und Informationssysteme, die den Betrieb wesentlicher Funktionen unterstützen. Sie minimieren deren Angriffsfläche und stellen sicher, dass der Betrieb wesentlicher Funktionen nicht durch die Ausnutzung einzelner Schwachstellen beeinträchtigt wird.	restricted-common-ports	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass gemeinsame Ports für Amazon Elastic Compute Cloud (Amazon EC2) -Sicherheitsgruppen eingeschränkt sind. Wenn der Zugriff auf Ports nicht auf vertrauenswürdige Quellen beschränkt wird, kann dies zu Angriffen auf die Verfügbarkeit, Integrität und Vertraulichkeit von Systemen führen. Mit dieser Regel können Sie optional die Parameter blockedPort1–blockedPort5 festlegen (Standardkonfigurationen: 20, 21, 3389, 3306, 4333). Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
B4.a Secure by Design	Sie integrieren Sicherheit in die Netzwerk- und Informationssysteme, die den Betrieb wesentlicher Funktionen unterstützen. Sie minimieren deren Angriffsfläche und stellen sicher, dass der Betrieb wesentlicher Funktionen nicht durch die Ausnutzung einzelner Schwachstellen beeinträchtigt wird.	s3- account-level-public-access -Block-periodisch	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Simple Storage Service (Amazon S3) -Buckets nicht öffentlich zugänglich sind. Diese Regel trägt dazu bei, sensible Daten vor unbefugten Remote-Benutzern zu schützen, indem sie den öffentlichen Zugriff verhindert. Mit dieser Regel können Sie optional die Parameter ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) und restrictPublicBuckets Parameter (Config Default: True) festlegen. Die tatsächlichen Werte müssen den Richtlini

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			en Ihrer Organisation entsprechen.
B4.a Secure by Design	Sie integrieren Sicherheit in die Netzwerk- und Informationssysteme, die den Betrieb wesentlicher Funktionen unterstützen. Sie minimieren deren Angriffsfläche und stellen sicher, dass der Betrieb wesentlicher Funktionen nicht durch die Ausnutzung einzelner Schwachstellen beeinträchtigt wird.	s3- bucket-public-read-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie nur autorisierten Benutzern, Prozessen und Geräten Zugriff auf Amazon Simple Storage Service (Amazon S3) - Buckets gewähren. Die Verwaltung des Zugriffs sollte mit der Klassifizierung der Daten übereinstimmen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
B4.a Secure by Design	Sie integrieren Sicherheit in die Netzwerk- und Informationssysteme, die den Betrieb wesentlicher Funktionen unterstützen. Sie minimieren deren Angriffsfläche und stellen sicher, dass der Betrieb wesentlicher Funktionen nicht durch die Ausnutzung einzelner Schwachstellen beeinträchtigt wird.	s3- bucket-public-write-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie nur autorisierten Benutzern, Prozessen und Geräten Zugriff auf Amazon Simple Storage Service (Amazon S3) - Buckets gewähren. Die Verwaltung des Zugriffs sollte mit der Klassifizierung der Daten übereinstimmen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
B4.a Secure by Design	Sie integrieren Sicherheit in die Netzwerk- und Informationssysteme, die den Betrieb wesentlicher Funktionen unterstützen. Sie minimieren deren Angriffsfläche und stellen sicher, dass der Betrieb wesentlicher Funktionen nicht durch die Ausnutzung einzelner Schwachstellen beeinträchtigt wird.	sagemaker-notebook-no-direct-Internetzugang	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass SageMaker Amazon-Notebooks keinen direkten Internetzugang zulassen. Indem Sie direkten Internetzugang blockieren, vermeiden Sie, dass unbefugte Benutzer auf sensible Daten zugreifen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
B4.a Secure by Design	Sie integrieren Sicherheit in die Netzwerk- und Informationssystem e, die den Betrieb wesentlicher Funktionen unterstüt zen. Sie minimiere n deren Angriffsf läche und stellen sicher, dass der Betrieb wesentlic her Funktionen nicht durch die Ausnutzung einzelner Schwachst ellen beeinträchtigt wird.	vpc-default-security-group-geschlossen	Sicherheitsgruppen von Amazon Elastic Compute Cloud (Amazon EC2) können bei der Verwaltung des Netzwerkzugriffs helfen, indem sie eine statusbehaftete Filterung des ein- und ausgehenden Netzwerkverkehrs zu Ressourcen bereitstellen. AWS Die Beschränk ung des gesamten Datenverkehrs auf die Standardsicherheit sgruppe hilft dabei, den Fernzugriff auf Ihre Ressourcen einzuschränken. AWS

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
B4.a Secure by Design	Sie integrieren Sicherheit in die Netzwerk- und Informationssysteme, die den Betrieb wesentlicher Funktionen unterstützen. Sie minimieren deren Angriffsfläche und stellen sicher, dass der Betrieb wesentlicher Funktionen nicht durch die Ausnutzung einzelner Schwachstellen beeinträchtigt wird.	vpc-sg-open-only-to-authorized-ports	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass gemeinsame Ports für Amazon Elastic Compute Cloud (Amazon EC2) -Sicherheitsgruppen eingeschränkt sind. Wenn der Zugriff auf Ports nicht auf vertrauenswürdige Quellen beschränkt wird, kann dies zu Angriffen auf die Verfügbarkeit, Integrität und Vertraulichkeit von Systemen führen. Durch die Beschränkung des Zugriffs auf Ressourcen innerhalb einer Sicherheitsgruppe aus dem Internet (0.0.0.0/0) kann der Remote-Zugriff auf interne Systeme gesteuert werden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
B4.a Secure by Design	Sie integrieren Sicherheit in die Netzwerk- und Informationssysteme, die den Betrieb wesentlicher Funktionen unterstützen. Sie minimieren deren Angriffsfläche und stellen sicher, dass der Betrieb wesentlicher Funktionen nicht durch die Ausnutzung einzelner Schwachstellen beeinträchtigt wird.	autoscaling-group-elb-healthcheck-erforderlich	Die Elastic Load Balancer (ELB) - Zustandsprüfungen für Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling Scaling-Gruppen unterstützen die Aufrechterhaltung einer angemessenen Kapazität und Verfügbarkeit. Der Load Balancer sendet regelmäßig Pings, versucht Verbindungen herzustellen oder sendet Anfragen, um den Zustand der EC2 Amazon-Instances in einer Gruppe mit auto-scaling zu testen. Wenn eine Instance nicht zurückmeldet, wird der Traffic an eine neue EC2 Amazon-Instance gesendet.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
B4.a Secure by Design	Sie integrieren Sicherheit in die Netzwerk- und Informationssysteme, die den Betrieb wesentlicher Funktionen unterstützen. Sie minimieren deren Angriffsfläche und stellen sicher, dass der Betrieb wesentlicher Funktionen nicht durch die Ausnutzung einzelner Schwachstellen beeinträchtigt wird.	dynamodb-autoscaling-enabled	Amazon DynamoDB Auto Scaling verwendet den AWS Application Auto Scaling-Service, um die bereitgestellte Durchsatzkapazität so anzupassen, dass sie automatisch auf tatsächliche Verkehrsmuster reagiert. Auf diese Weise kann eine Tabelle oder ein globaler sekundärer Index die bereitgestellte Lese-/Schreibkapazität erhöhen, um plötzliche Erhöhungen des Datenverkehrs ohne Drosselung zu bewältigen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
B4.a Secure by Design	Sie integrieren Sicherheit in die Netzwerk- und Informationssysteme, die den Betrieb wesentlicher Funktionen unterstützen. Sie minimieren deren Angriffsfläche und stellen sicher, dass der Betrieb wesentlicher Funktionen nicht durch die Ausnutzung einzelner Schwachstellen beeinträchtigt wird.	dynamodb-throughput-limit-check	Aktivieren Sie diese Regel, um sicherzustellen, dass die bereitgestellte Durchsatzkapazität in Ihren Amazon-DynamoDB-Tabellen überprüft wird. Dies ist der Umfang der Lese- und Schreibaktivitäten, der von den jeweiligen Tabellen unterstützt werden kann. DynamoDB verwendet diese Informationen für das Reservieren ausreichender Systemressourcen, um Ihren Durchsatz anforderungen gerecht zu werden. Diese Regel generiert eine Warnung, wenn sich der Durchsatz dem Höchstlimit für ein Kundenkonto nähert. Mit dieser Regel können Sie optional die Parameter RCUThreshold Kontoprozentsatz

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			(Konfigurationsstandard: 80) und WCUThreshold Kontoprozentsatz (Konfigurationsstandard: 80) festlegen. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
B4.a Secure by Design	Sie integrieren Sicherheit in die Netzwerk- und Informationssysteme, die den Betrieb wesentlicher Funktionen unterstützen. Sie minimieren deren Angriffsfläche und stellen sicher, dass der Betrieb wesentlicher Funktionen nicht durch die Ausnutzung einzelner Schwachstellen beeinträchtigt wird.	elb-cross-zone-load-Balancing aktiviert	Aktivieren Sie zonenübergreifendes Load Balancing für Ihre Elastic Load Balancer (ELBs), um eine angemessene Kapazität und Verfügbarkeit aufrechtzuerhalten. Zonenübergreifendes Load Balancing reduziert die Notwendigkeit, die gleiche Anzahl von Instances in jeder aktivierten Availability Zone aufrechtzuerhalten. Es verbessert auch die Fähigkeit Ihrer Anwendung, den Verlust einer oder mehrerer Instances zu bewältigen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
B4.a Secure by Design	Sie integrieren Sicherheit in die Netzwerk- und Informationssysteme, die den Betrieb wesentlicher Funktionen unterstützen. Sie minimieren deren Angriffsfläche und stellen sicher, dass der Betrieb wesentlicher Funktionen nicht durch die Ausnutzung einzelner Schwachstellen beeinträchtigt wird.	elb-deletion-protection-enabled	Diese Regel sorgt dafür, dass der Löschschutz für Elastic Load Balancing aktiviert ist. Verwenden Sie diese Funktion, um zu verhindern, dass Ihr Load Balancer versehentlich oder böswillig gelöscht wird, was zum Verlust der Verfügbarkeit Ihrer Anwendungen führen kann.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
B4.a Secure by Design	Sie integrieren Sicherheit in die Netzwerk- und Informationssysteme, die den Betrieb wesentlicher Funktionen unterstützen. Sie minimieren deren Angriffsfläche und stellen sicher, dass der Betrieb wesentlicher Funktionen nicht durch die Ausnutzung einzelner Schwachstellen beeinträchtigt wird.	lambda-concurrency-check	Diese Regel stellt sicher, dass die Höchst- und Untergrenzen für die Gleichzeitigkeit einer Lambda-Funktion festgelegt werden. Dies kann Sie beim Baselining für die Anzahl der Anforderungen unterstützen, die Ihre Funktion zu einem bestimmten Zeitpunkt verarbeitet.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
B4.a Secure by Design	Sie integrieren Sicherheit in die Netzwerk- und Informationssysteme, die den Betrieb wesentlicher Funktionen unterstützen. Sie minimieren deren Angriffsfläche und stellen sicher, dass der Betrieb wesentlicher Funktionen nicht durch die Ausnutzung einzelner Schwachstellen beeinträchtigt wird.	rds-instance-deletion-protection-aktiviert	Stellen Sie sicher, dass Amazon Relational Database Service (Amazon RDS)-Instances den Löschschutz aktiviert haben. Verwenden Sie den Löschschutz, um zu verhindern, dass Ihre Amazon-RDS-Instances versehentlich oder böswillig gelöscht werden, was zum Verlust der Verfügbarkeit Ihrer Anwendungen führen kann.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
B4.a Secure by Design	Sie integrieren Sicherheit in die Netzwerk- und Informationssysteme, die den Betrieb wesentlicher Funktionen unterstützen. Sie minimieren deren Angriffsfläche und stellen sicher, dass der Betrieb wesentlicher Funktionen nicht durch die Ausnutzung einzelner Schwachstellen beeinträchtigt wird.	rds-multi-az-support	Die Multi-AZ-Unterstützung in Amazon Relational Database Service (Amazon RDS) bietet eine verbesserte Verfügbarkeit und Beständigkeit von Datenbank-Instances. Wenn Sie eine Multi-AZ-Datenbank-Instance bereitstellen, erstellt Amazon RDS automatisch eine primäre Datenbank-Instance und repliziert die Daten synchron auf eine Standby-Instance in einer anderen Availability Zone. Jede Availability Zone läuft auf einer eigenen, physisch getrennten, unabhängigen Infrastruktur und ist auf eine hohe Verfügbarkeit ausgelegt. Im Falle eines Infrastrukturausfalls führt Amazon RDS einen automatis

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			chen Failover zum Standby-Modus durch, sodass Sie den Datenbankbetrieb wieder aufnehmen können, sobald der Failover abgeschlo ssen ist.
B4.a Secure by Design	Sie integrieren Sicherheit in die Netzwerk- und Informationssystem e, die den Betrieb wesentlicher Funktionen unterstüt zen. Sie minimiere n deren Angriffsf läche und stellen sicher, dass der Betrieb wesentlic her Funktionen nicht durch die Ausnutzung einzelner Schwachst ellen beeinträchtigt wird.	s3- bucket-default-loc k-enabled	Stellen Sie sicher, dass für Ihren Amazon Simple Storage Service (Amazon S3)-Bucke t standardmäßig eine Sperre aktiviert ist. Zum Schutz eventuell vorhanden er sensibler Daten in S3-Buckets müssen Sie Objektsperren für Daten im Ruhezusta nd erzwingen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
B4.a Secure by Design	Sie integrieren Sicherheit in die Netzwerk- und Informationssysteme, die den Betrieb wesentlicher Funktionen unterstützen. Sie minimieren deren Angriffsfläche und stellen sicher, dass der Betrieb wesentlicher Funktionen nicht durch die Ausnutzung einzelner Schwachstellen beeinträchtigt wird.	vpc-vpn-2-tunnels-up	Redundante Site-to-Site VPN-Tunnel können implementiert werden, um die Anforderungen an die Ausfallsicherheit zu erfüllen. Es verwendet zwei Tunnel, um die Konnektivität sicherzustellen, falls eine der Site-to-Site VPN-Verbindungen nicht verfügbar ist. Um sich vor einem Verbindungsverlust zu schützen, können Sie für den Fall, dass Ihr Kunden-Gateway nicht verfügbar ist, eine zweite Site-to-Site VPN-Verbindung zu Ihrer Amazon Virtual Private Cloud (Amazon VPC) und Ihrem Virtual Private Gateway einrichten, indem Sie ein zweites Kunden-Gateway verwenden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
B4.a Secure by Design	Sie integrieren Sicherheit in die Netzwerk- und Informationssysteme, die den Betrieb wesentlicher Funktionen unterstützen. Sie minimieren deren Angriffsfläche und stellen sicher, dass der Betrieb wesentlicher Funktionen nicht durch die Ausnutzung einzelner Schwachstellen beeinträchtigt wird.	ec2-manager instance-managed-by-systems	Eine Bestandsaufnahme der Softwareplattformen und Anwendungen innerhalb des Unternehmens ist möglich, indem Amazon Elastic Compute Cloud (Amazon EC2) - Instances mit AWS Systems Manager verwaltet werden. Verwenden Sie AWS Systems Manager, um detaillierte Systemkonfigurationen, Betriebssystem-Patch-Levels, Namen und Typ der Dienste, Softwareinstallationen, Anwendungsname, Herausgeber und Version sowie andere Details zu Ihrer Umgebung bereitzustellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
B4.a Secure by Design	Sie integrieren Sicherheit in die Netzwerk- und Informationssysteme, die den Betrieb wesentlicher Funktionen unterstützen. Sie minimieren deren Angriffsfläche und stellen sicher, dass der Betrieb wesentlicher Funktionen nicht durch die Ausnutzung einzelner Schwachstellen beeinträchtigt wird.	opensearch-in-vpc-only	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass sich Amazon OpenSearch Service-Domains innerhalb einer Amazon Virtual Private Cloud (Amazon VPC) befinden. Eine Amazon OpenSearch Service-Domain innerhalb einer Amazon VPC ermöglicht die sichere Kommunikation zwischen Amazon OpenSearch Service und anderen Services innerhalb der Amazon VPC, ohne dass ein Internet-Gateway, ein NAT-Gerät oder eine VPN-Verbindung erforderlich ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
B4.b Sichere Konfiguration	Sie sorgen für eine sichere Konfiguri erung der Netzwerk- und Informati onssysteme, die den Betrieb wesentlicher Funktionen unterstüt zen.	ec2-check managedin stance-association-compliance-status	Verwenden Sie AWS Systems Manager Associati ons, um bei der Inventarisierung von Softwareplattforme n und Anwendung en innerhalb eines Unternehmens zu helfen. AWS Systems Manager weist Ihren verwaltet en Instanzen einen Konfigurationsstat us zu und ermöglich t es Ihnen, Basiswert e für Betriebss ystem-Patch-Levels , Softwareinstallati onen, Anwendung skonfigurationen und andere Details zu Ihrer Umgebung festzulegen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
B4.b Sichere Konfiguration	Sie sorgen für eine sichere Konfiguri erung der Netzwerk- und Informati onssysteme, die den Betrieb wesentlicher Funktionen unterstüt zen.	ec2-check managedin stance-patch-compl iance-status	Aktivieren Sie diese Regel, um bei der Identifizierung und Dokumentation von Sicherheitslücken in Amazon Elastic Compute Cloud (Amazon EC2) zu helfen. Die Regel prüft, ob die EC2 Amazon-Instance die Patch-Konformität im AWS Systems Manager gemäß den Richtlinien und Verfahren Ihrer Organisation einhält.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
B4.b Sichere Konfiguration	Sie sorgen für eine sichere Konfiguri erung der Netzwerk- und Informati onssysteme, die den Betrieb wesentlicher Funktionen unterstüt zen.	ec2-imdsv2-check	Stellen Sie sicher, dass die Methode Instance Metadata Service Version 2 (IMDSv2) aktiviert ist, um den Zugriff auf und die Kontrolle der Amazon Elastic Compute Cloud (Amazon EC2) - Instance-Metadate n zu schützen. Die IMDSv2 Methode verwendet sitzungsb asierte Kontrollen. Mit können Kontrolle n implementiert werden IMDSv2, um Änderungen an Instanzmetadaten einzuschränken.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
B4.b Sichere Konfiguration	Sie sorgen für eine sichere Konfiguri erung der Netzwerk- und Informati onssysteme, die den Betrieb wesentlicher Funktionen unterstüt zen.	redshift-cluster-m aintenancesettings-check	Diese Regel stellt sicher, dass Amazon-Redshift-Cluster die bevorzugten Einstellungen für Ihre Organisation haben. Insbesondere sorgt sie dafür, dass Cluster bevorzugt e Wartungsfenster und automatisierte Aufbewahrungsfristen für Snapshots für die Datenbank haben. Für diese Regel müssen Sie die festlegen allowVersionUpgrad e. Der Standardwert ist „true“. Außerdem können Sie optional den Zeitraum preferredMaintenan ceWindow (der Standardwert ist sa: 16:00 -sa: 16:30) und den automated SnapshotRetention Zeitraum (der Standardwert ist 1) festlegen. Die tatsächlichen Werte müssen den Richtlini

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			en Ihrer Organisation entsprechen.
B4.c Sichere Verwaltung	Sie verwalten die Netzwerk- und Informationssysteme Ihrer Organisation, die den Betrieb wesentlic her Funktionen unterstützen, um die Sicherheit zu gewährleisten und aufrechtzuerhalten.	ec2- -check managedinstance-pa tch-compliance-status	Aktivieren Sie diese Regel, um bei der Identifizierung und Dokumentation von Sicherheitslücken in Amazon Elastic Compute Cloud (Amazon EC2) zu helfen. Die Regel prüft, ob die EC2 Amazon-Instance die Patch-Konformität im AWS Systems Manager gemäß den Richtlinien und Verfahren Ihrer Organisation einhält.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
B4.c Sichere Verwaltung	Sie verwalten die Netzwerk- und Informationssysteme Ihrer Organisation, die den Betrieb wesentlic her Funktionen unterstützen, um die Sicherheit zu gewährleisten und aufrechtzuerhalten.	ec2-imdsv2-check	Stellen Sie sicher, dass die Methode Instance Metadata Service Version 2 (IMDSv2) aktiviert ist, um den Zugriff auf und die Kontrolle der Amazon Elastic Compute Cloud (Amazon EC2) - Instance-Metadate n zu schützen. Die IMDSv2 Methode verwendet sitzungsb asierte Kontrollen. Mit können Kontrolle n implementiert werden IMDSv2, um Änderungen an Instanzmetadaten einzuschränken.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
B4.c Sichere Verwaltung	Sie verwalten die Netzwerk- und Informationssysteme Ihrer Organisation, die den Betrieb wesentlicher Funktionen unterstützen, um die Sicherheit zu gewährleisten und aufrechtzuerhalten.	ec2-manager instance-managed-by-systems	Eine Bestandsaufnahme der Softwareplattformen und Anwendungen innerhalb des Unternehmens ist möglich, indem Amazon Elastic Compute Cloud (Amazon EC2) - Instances mit AWS Systems Manager verwaltet werden. Verwenden Sie AWS Systems Manager, um detaillierte Systemkonfigurationen, Betriebssystem-Patch-Levels, Namen und Typ der Dienste, Softwareinstallationen, Anwendungsname, Herausgeber und Version sowie andere Details zu Ihrer Umgebung bereitzustellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
B4.d. Management von Schwachstellen	Sie adressieren bekannte Schwachstellen in Ihren Netzwerk- und Informationssystemen, um negative Auswirkungen auf wesentliche Funktionen zu verhindern.	ec2-check managedinstance-association-compliance-status	Verwenden Sie AWS Systems Manager Associations, um bei der Inventarisierung von Softwareplattformen und Anwendungen innerhalb eines Unternehmens zu helfen. AWS Systems Manager weist Ihren verwalteten Instanzen einen Konfigurationsstatus zu und ermöglicht es Ihnen, Basiswerte für Betriebssystem-Patch-Levels, Softwareinstallationen, Anwendungskonfigurationen und andere Details zu Ihrer Umgebung festzulegen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
B4.d. Management von Schwachstellen	Sie adressieren bekannte Schwachstellen in Ihren Netzwerk- und Informationssystemen, um negative Auswirkungen auf wesentliche Funktionen zu verhindern.	ec2-check managedinstance-patch-compliance-status	Aktivieren Sie diese Regel, um bei der Identifizierung und Dokumentation von Sicherheitslücken in Amazon Elastic Compute Cloud (Amazon EC2) zu helfen. Die Regel prüft, ob die EC2 Amazon-Instance die Patch-Konformität im AWS Systems Manager gemäß den Richtlinien und Verfahren Ihrer Organisation einhält.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
B4.d. Management von Schwachstellen	Sie adressieren bekannte Schwachstellen in Ihren Netzwerk- und Informationssystemen, um negative Auswirkungen auf wesentliche Funktionen zu verhindern.	ec2-imdsv2-check	Stellen Sie sicher, dass die Methode Instance Metadata Service Version 2 (IMDSv2) aktiviert ist, um den Zugriff auf und die Kontrolle der Amazon Elastic Compute Cloud (Amazon EC2) - Instance-Metadaten zu schützen. Die IMDSv2 Methode verwendet sitzungsbasierte Kontrollen. Mit können Kontrollen implementiert werden IMDSv2, um Änderungen an Instanzmetadaten einzuschränken.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
B4.d. Management von Schwachstellen	Sie adressieren bekannte Schwachstellen in Ihren Netzwerk- und Informationssystemen, um negative Auswirkungen auf wesentliche Funktionen zu verhindern.	redshift-cluster-maintenancesettings-check	Diese Regel stellt sicher, dass Amazon-Redshift-Cluster die bevorzugten Einstellungen für Ihre Organisation haben. Insbesondere sorgt sie dafür, dass Cluster bevorzugte Wartungsfenster und automatisierte Aufbewahrungsfristen für Snapshots für die Datenbank haben. Für diese Regel müssen Sie die festlegen allowVersionUpgrade. Der Standardwert ist „true“. Außerdem können Sie optional den Zeitraum preferredMaintenanceWindow (der Standardwert ist sa: 16:00 -sa: 16:30) und den automated SnapshotRetention Zeitraum (der Standardwert ist 1) festlegen. Die tatsächlichen Werte müssen den Richtlini

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			en Ihrer Organisation entsprechen.
B4.d. Management von Schwachstellen	Sie adressieren bekannte Schwachstellen in Ihren Netzwerk- und Informationssystemen, um negative Auswirkungen auf wesentliche Funktionen zu verhindern.	securityhub-enabled	AWS Security Hub hilft bei der Überwachung von unbefugtem Personal, Verbindungen, Geräten und Software. AWS Security Hub aggregiert, organisiert und priorisiert die Sicherheitswarnungen oder Ergebnisse mehrerer Dienste. AWS Einige dieser Dienste sind Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer und AWS Firewall Manager sowie AWS Partnerlösungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
B4.d. Management von Schwachstellen	Sie adressieren bekannte Schwachstellen in Ihren Netzwerk- und Informationssystemen, um negative Auswirkungen auf wesentliche Funktionen zu verhindern.	vpc-vpn-2-tunnels-up	Redundante Site-to-Site VPN-Tunnel können implementiert werden, um die Anforderungen an die Ausfallsicherheit zu erfüllen. Es verwendet zwei Tunnel, um die Konnektivität sicherzustellen, falls eine der Site-to-Site VPN-Verbindungen nicht verfügbar ist. Um sich vor einem Verbindungsverlust zu schützen, können Sie für den Fall, dass Ihr Kunden-Gateway nicht verfügbar ist, eine zweite Site-to-Site VPN-Verbindung zu Ihrer Amazon Virtual Private Cloud (Amazon VPC) und Ihrem Virtual Private Gateway einrichten, indem Sie ein zweites Kunden-Gateway verwenden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
B5.b Robustes Design	Sie entwerfen Netzwerk- und Informationssysteme, die wesentliche Funktionen unterstützen, im Hinblick auf deren Widerstandsfähigkeit gegenüber Cybersicherheitsvorfällen. Die Systeme werden angemessen segmentiert und Ressourcenbeschränkungen werden gemindert.	elb-cross-zone-load-Balancing aktiviert	Aktivieren Sie zonenübergreifendes Load Balancing für Ihre Elastic Load Balancer (ELBs), um eine angemessene Kapazität und Verfügbarkeit aufrechtzuerhalten. Zonenübergreifendes Load Balancing reduziert die Notwendigkeit, die gleiche Anzahl von Instances in jeder aktivierten Availability Zone aufrechtzuerhalten. Es verbessert auch die Fähigkeit Ihrer Anwendung, den Verlust einer oder mehrerer Instances zu bewältigen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
B5.b Robustes Design	Sie entwerfen Netzwerk- und Informationssysteme, die wesentliche Funktionen unterstützen, im Hinblick auf deren Widerstandsfähigkeit gegenüber Cybersicherheitsvorfällen. Die Systeme werden angemessen segmentiert und Ressourcenbeschränkungen werden gemindert.	rds-multi-az-support	Die Multi-AZ-Unterstützung in Amazon Relational Database Service (Amazon RDS) bietet eine verbesserte Verfügbarkeit und Beständigkeit von Datenbank-Instances. Wenn Sie eine Multi-AZ-Datenbank-Instance bereitstellen, erstellt Amazon RDS automatisch eine primäre Datenbank-Instance und repliziert die Daten synchron auf eine Standby-Instance in einer anderen Availability Zone. Jede Availability Zone läuft auf einer eigenen, physisch getrennten, unabhängigen Infrastruktur und ist auf eine hohe Verfügbarkeit ausgelegt. Im Falle eines Infrastrukturausfalls führt Amazon RDS einen automatis

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			chen Failover zum Standby-Modus durch, sodass Sie den Datenbankbetrieb wieder aufnehmen können, sobald der Failover abgeschlo ssen ist.
B5.b Robustes Design	Sie entwerfen Netzwerk- und Informationssystem e, die wesentliche Funktionen unterstüt zen, im Hinblick auf deren Widerstan dsfähigkeit gegenüber Cybersicherheitsvo rfällen. Die Systeme werden angemesse n segmentiert und Ressourcenbeschrän kungen werden gemindert.	db-instance-backup-enabled	Die Sicherung sfunktion von Amazon RDS erstellt Sicherung en Ihrer Datenbank en und Transakti onsprotokolle. Amazon RDS erstellt einen Snapshot für das Speichervolume Ihrer DB-Instance, sodass die gesamte DB-Instance gesichert wird. Sie können im System spezifische Aufbewahrungsfrist en festlegen, um Ihre Ausfallsicherheits anforderungen zu erfüllen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
B5.c Backups	Sie verfügen über zugängliche und gesicherte aktuelle Backups von Daten und Informati onen, die für die Wiederherstellung des Betriebs wesentlichen Funktionen erforderl ich sind.	dynamodb-in-backup-plan	Um Sie bei Datensich erungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon DynamoDB-Tabellen Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwaltet er Backup-Service mit einer richtlini enbasierten Backup-Lösung. Diese Lösung vereinfac ht Ihr Sicherung smanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforde rungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
B5.c Backups	Sie verfügen über zugängliche und gesicherte aktuelle Backups von Daten und Informati onen, die für die Wiederherstellung des Betriebs wesentlichen Funktionen erforderl ich sind.	dynamodb-pitr-enab led	Aktivieren Sie diese Regel, um zu überprüfen, ob die Informationen gesichert wurden. Es verwaltet auch die Backups, indem es sicherstellt, dass die point-in-time Wiederherstellung in Amazon DynamoDB aktiviert ist. Bei der Wiederherstellung werden fortlaufende Backups Ihrer Tabelle für die letzten 35 Tage gespeichert.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
B5.c Backups	Sie verfügen über zugängliche und gesicherte aktuelle Backups von Daten und Informati onen, die für die Wiederherstellung des Betriebs wesentlichen Funktionen erforderl ich sind.	ebs-in-backup-plan	Stellen Sie zur Unterstützung der Datensicherungspro zesse sicher, dass Ihre Amazon Elastic Block Store (Amazon EBS) -Volumes Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwaltet er Backup-Service mit einer richtlini enbasierten Backup-Lösung. Diese Lösung vereinfac ht Ihr Sicherung smanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforde rungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
B5.c Backups	Sie verfügen über zugängliche und gesicherte aktuelle Backups von Daten und Informati onen, die für die Wiederherstellung des Betriebs wesentlichen Funktionen erforderl ich sind.	ebs-optimized-inst ance	Eine optimierte Instance im Amazon Elastic Block Store (Amazon EBS) bietet zusätzliche, dedizierte Kapazität für Amazon-EBS-I/ O-Vorgänge. Diese Optimierung bietet die beste Leistung für Ihr EBS-Volume, indem Konflikte zwischen Amazon-EBS-I/O und anderem Datenverk ehr von Ihrer Instance minimiert werden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
B5.c Backups	Sie verfügen über zugängliche und gesicherte aktuelle Backups von Daten und Informati onen, die für die Wiederherstellung des Betriebs wesentlichen Funktionen erforderl ich sind.	efs-in-backup-plan	Um Sie bei Datensich erungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon Elastic File System (Amazon EFS) -Dateisysteme Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwaltet er Backup-Service mit einer richtlini enbasierten Backup-Lösung. Diese Lösung vereinfac ht Ihr Sicherung smanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforde rungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
B5.c Backups	Sie verfügen über zugängliche und gesicherte aktuelle Backups von Daten und Informati onen, die für die Wiederherstellung des Betriebs wesentlichen Funktionen erforderl ich sind.	elasticache-redis-cluster-automatic-Backup-Check	Wenn automatische Backups aktiviert sind, ElastiCache erstellt Amazon täglich ein Backup des Clusters. Die Sicherung kann für eine von Ihrer Organisation festgelegte Anzahl von Tagen aufbewahrt werden. Automatische Backups schützen vor Datenverlust. Bei einem Ausfall können Sie einen neuen Cluster erstellen, der Ihre Daten aus dem aktuellen Backup wiederherstellt.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
B5.c Backups	Sie verfügen über zugängliche und gesicherte aktuelle Backups von Daten und Informati onen, die für die Wiederherstellung des Betriebs wesentlichen Funktionen erforderl ich sind.	rds-in-backup-plan	Um Sie bei Datensich erungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon Relational Database Service (Amazon RDS) -Instance s Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwaltet er Backup-Service mit einer richtlini enbasierten Backup-Lösung. Diese Lösung vereinfac ht Ihr Sicherung smanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforde rungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
B5.c Backups	Sie verfügen über zugängliche und gesicherte aktuelle Backups von Daten und Informati onen, die für die Wiederherstellung des Betriebs wesentlichen Funktionen erforderl ich sind.	s-3 bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) unterstützt die Aufrechterhaltung einer angemesse nen Kapazität und Verfügbarkeit. CRR ermöglicht das automatische, asynchrone Kopieren von Objekten in Amazon-S3-Buckets, um die Datenverf ügbarkeit sicherzus tellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
B5.c Backups	Sie verfügen über zugängliche und gesicherte aktuelle Backups von Daten und Informati onen, die für die Wiederherstellung des Betriebs wesentlichen Funktionen erforderl ich sind.	s-3 bucket-versioning-enabled	Die Versionsv erwaltung von Amazon Simple Storage Service (Amazon S3)-Bucke ts hilft dabei, mehrere Varianten eines Objekts im selben Amazon-S3-Bucket zu speichern. Verwenden Sie die Versionsv erwaltung, um sämtliche Versionen aller Objekte in Ihrem Amazon-S3-Bucket zu speichern , abzurufen oder wiederherzustellen . Mit der Versionsv erwaltung können Sie Versionen sowohl nach unbeabsic htigten Benutzera ktionen als auch nach Anwendungsfehlern problemlos wiederher stellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
B5.c Backups	Sie verfügen über zugängliche und gesicherte aktuelle Backups von Daten und Informati onen, die für die Wiederherstellung des Betriebs wesentlichen Funktionen erforderl ich sind.	autoscaling-group-elb-healthcheck-er forderlich	Die Elastic Load Balancer (ELB) - Zustandsprüfungen für Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling Scaling-G ruppen unterstützen die Aufrechterhaltung einer angemesse nen Kapazität und Verfügbarkeit. Der Load Balancer sendet regelmäßig Pings, versucht Verbindun gen herzustellen oder sendet Anfragen, um den Zustand der EC2 Amazon-Instances in einer Gruppe mit auto-scal ing zu testen. Wenn eine Instance nicht zurückmeldet, wird der Traffic an eine neue EC2 Amazon-In stance gesendet.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
C1.a Überwachungsabdeckung	In Ihre Überwachung einbezogene Datenquellen ermöglichen die rechtzeitige Identifizierung von Sicherheitsereignissen, die den Betrieb wesentlicher Funktionen beeinträchtigen könnten.	cloud-trail-cloud-watch-logs-aktiviert	Verwenden Sie Amazon CloudWatch , um Protokollereignisaktivitäten zentral zu sammeln und zu verwalten. Die Aufnahme von AWS CloudTrail Daten liefert Einzelheiten zu den API-Aufrufaktivitäten in Ihrem AWS-Konto.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
C1.a Überwachungsabdeckung	In Ihre Überwachung einbezogene Datenquellen ermöglichen die rechtzeitige Identifizierung von Sicherheitsereignissen, die den Betrieb wesentlicher Funktionen beeinträchtigen könnten.	cloudwatch-alarm-action-check	Amazon CloudWatch alarmiert, wenn eine Metrik den Schwellenwert für eine bestimmte Anzahl von Bewertungszeiträumen überschreitet. Der Alarm führt eine oder mehrere Aktionen durch, die vom Wert der Metrik oder des Ausdrucks im Vergleich zu einem Schwellenwert in einer Reihe von Zeiträumen abhängt. Diese Regel erfordert einen Wert für alarmActionRequired (Config Default: True), insufficientDataAction Required (Config Default: True), okActionRequired (Config Default: False). Der tatsächliche Wert muss die Alarmaktionen für Ihre Umgebung widerspiegeln.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
C1.a Überwachungsabdeckung	In Ihre Überwachung einbezogene Datenquellen ermöglichen die rechtzeitige Identifizierung von Sicherheitsereignissen, die den Betrieb wesentlicher Funktionen beeinträchtigen könnten.	dynamodb-throughput-limit-check	Aktivieren Sie diese Regel, um sicherzustellen, dass die bereitgestellte Durchsatzkapazität in Ihren Amazon-DynamoDB-Tabellen überprüft wird. Dies ist der Umfang der Lese- und Schreibaktivitäten, der von den jeweiligen Tabellen unterstützt werden kann. DynamoDB verwendet diese Informationen für das Reservieren ausreichender Systemressourcen, um Ihren Durchsatzanforderungen gerecht zu werden. Diese Regel generiert eine Warnung, wenn sich der Durchsatz dem Höchstlimit für ein Kundenkonto nähert. Mit dieser Regel können Sie optional die Parameter RCUThreshold Kontoprozentsatz

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			(Konfigurationsstandard: 80) und WCUThreshold Kontoprozentsatz (Konfigurationsstandard: 80) festlegen. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.
C1.a Überwachungsabdeckung	In Ihre Überwachung einbezogene Datenquellen ermöglichen die rechtzeitige Identifizierung von Sicherheitsereignissen, die den Betrieb wesentlicher Funktionen beeinträchtigen könnten.	ec2- instance-detailed-monitoring-enabled	Aktivieren Sie diese Regel, um die Amazon Elastic Compute Cloud (Amazon EC2) - Instance-Überwachung auf der EC2 Amazon-Konsole zu verbessern, in der Monitoring-Diagramme mit einem Zeitraum von 1 Minute für die Instance angezeigt werden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
C1.a Überwachungsabdeckung	In Ihre Überwachung einbezogene Datenquellen ermöglichen die rechtzeitige Identifizierung von Sicherheitsereignissen, die den Betrieb wesentlicher Funktionen beeinträchtigen könnten.	guardduty-enabled-centralized	Amazon GuardDuty kann mithilfe von Threat Intelligence Feeds helfen, potenzielle Cybersicherheitsereignisse zu überwachen und zu erkennen. Dazu gehören Listen mit bösartigen IPs und maschinellen Lernmethoden zur Identifizierung unerwarteter, nicht autorisierter und bösartiger Aktivitäten in Ihrer AWS Cloud-Umgebung.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
C1.a Überwachungsabdeckung	In Ihre Überwachung einbezogene Datenquellen ermöglichen die rechtzeitige Identifizierung von Sicherheitsereignissen, die den Betrieb wesentlicher Funktionen beeinträchtigen könnten.	guardduty-non-archived-findings	Amazon GuardDuty hilft Ihnen dabei, die Auswirkungen eines Vorfalls zu verstehen, indem es die Ergebnisse nach Schweregrad klassifiziert: niedrig, mittel und hoch. Diese Klassifizierungen können Sie zur Festlegung von entsprechenden Strategien und Prioritäten zur Behebung solcher Vorfälle verwenden. Mit dieser Regel können Sie optional daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7) und daysHighSev (Config Default: 1) für nicht archivierte Ergebnisse festlegen, wie es die Richtlinien Ihrer Organisation erfordern.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
C1.a Überwachungsabdeckung	In Ihre Überwachung einbezogene Datenquellen ermöglichen die rechtzeitige Identifizierung von Sicherheitsereignissen, die den Betrieb wesentlicher Funktionen beeinträchtigen könnten.	lambda-concurrency-check	Diese Regel stellt sicher, dass die Höchst- und Untergrenzen für die Gleichzeitigkeit einer Lambda-Funktion festgelegt werden. Dies kann Sie beim Baselining für die Anzahl der Anforderungen unterstützen, die Ihre Funktion zu einem bestimmten Zeitpunkt verarbeitet.
C1.a Überwachungsabdeckung	In Ihre Überwachung einbezogene Datenquellen ermöglichen die rechtzeitige Identifizierung von Sicherheitsereignissen, die den Betrieb wesentlicher Funktionen beeinträchtigen könnten.	lambda-dlq-check	Aktivieren Sie diese Regel, um das entsprechende Personal über Amazon Simple Queue Service (Amazon SQS) oder Amazon Simple Notification Service (Amazon SNS) zu benachrichtigen, wenn eine Funktion ausgefallen ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
C1.a Überwachungsabdeckung	In Ihre Überwachung einbezogene Datenquellen ermöglichen die rechtzeitige Identifizierung von Sicherheitsereignissen, die den Betrieb wesentlicher Funktionen beeinträchtigen könnten.	rds-enhanced-monitoring-enabled	Aktivieren Sie Amazon Relational Database Service (Amazon RDS), um die Verfügbarkeit von Amazon RDS zu überwachen. Dies bietet einen detaillierten Einblick in den Zustand Ihrer Amazon-RDS-Datenbank-Instances. Wenn der Amazon-RDS-Speicher mehr als ein zugrunde liegendes physisches Gerät verwendet, erfasst Enhanced Monitoring die Daten für jedes Gerät. Wenn die Amazon-RDS-Datenbank-Instance in einer Multi-AZ-Bereitstellung ausgeführt wird, werden außerdem die Daten für jedes Gerät auf dem sekundären Host sowie die Metriken des sekundären Hosts erfasst.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
C1.a Überwachungsabdeckung	In Ihre Überwachung einbezogene Datenquellen ermöglichen die rechtzeitige Identifizierung von Sicherheitsereignissen, die den Betrieb wesentlicher Funktionen beeinträchtigen könnten.	securityhub-enabled	AWS Security Hub hilft bei der Überwachung von unbefugtem Personal, Verbindungen, Geräten und Software. AWS Security Hub aggregiert, organisiert und priorisiert die Sicherheitswarnungen oder Ergebnisse mehrerer Dienste. AWS Einige dieser Dienste sind Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer und AWS Firewall Manager sowie AWS Partnerlösungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
C1.a Überwachungsabdeckung	In Ihre Überwachung einbezogene Datenquellen ermöglichen die rechtzeitige Identifizierung von Sicherheitsereignissen, die den Betrieb wesentlicher Funktionen beeinträchtigen könnten.	s-3 bucket-default-lock-enabled	Stellen Sie sicher, dass für Ihren Amazon Simple Storage Service (Amazon S3)-Bucket standardmäßig eine Sperre aktiviert ist. Zum Schutz eventuell vorhandener sensibler Daten in S3-Buckets müssen Sie Objektsperren für Daten im Ruhezustand erzwingen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
C1.b Sicherung von Protokollen	Sie speichern die Protokolldaten sicher und gewähren Lesezugriff nur Konten, die diesen für geschäftliche Zwecke benötigen . Mitarbeiter sollten jemals Protokoll daten innerhalb einer vereinbarten Aufbewahrungsfrist ändern oder löschen müssen. Erst nach Ablauf dieser Frist sollten sie gelöscht werden.	s-3 bucket-logging-enabled	Die Amazon Simple Storage Service (Amazon S3)-Serverzugriffs protokollierung bietet eine Methode zur Überwachu ng des Netzwerks im Hinblick auf potenzielle Cybersich erheitsereignisse. Die Ereignisse werden überwacht, indem detaillierte Aufzeichn ungen über die Anfragen erfasst werden, die an einen Amazon-S3-Bucket gestellt wurden. Jeder Zugriffsprotokolle intrag enthält Details zu einer einzelnen Zugriffsanfrage. Zu den Details gehören Anforderer, Bucket-Name, Anforderu ngszeit, Anforderu ngsaktion, Antwortst atus und Fehlercode, falls relevant.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
C1.b Sicherung von Protokollen	Sie speichern die Protokolldaten sicher und gewähren Lesezugriff nur Konten, die diesen für geschäftliche Zwecke benötigen . Mitarbeiter sollten jemals Protokoll daten innerhalb einer vereinbarten Aufbewahrungsfrist ändern oder löschen müssen. Erst nach Ablauf dieser Frist sollten sie gelöscht werden.	s-3 bucket-policy-grantee-check	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie s3_bucket_policy_grantee_check aktivieren. Diese Regel prüft, ob der vom Amazon S3 S3-Bucket gewährte Zugriff durch die von Ihnen bereitgestellten AWS Principals, Verbundbenutzer, Service Principals, IP-Adressen oder Amazon Virtual Private Cloud (Amazon VPC) IDs eingeschränkt ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
C1.b Sicherung von Protokollen	Sie speichern die Protokolldaten sicher und gewähren Lesezugriff nur Konten, die diesen für geschäftliche Zwecke benötigen . Mitarbeiter sollten jemals Protokoll daten innerhalb einer vereinbarten Aufbewahrungsfrist ändern oder löschen müssen. Erst nach Ablauf dieser Frist sollten sie gelöscht werden.	s-3 bucket-public-read -prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie nur autorisierten Benutzern, Prozessen und Geräten Zugriff auf Amazon Simple Storage Service (Amazon S3) - Buckets gewähren. Die Verwaltung des Zugriffs sollte mit der Klassifizierung der Daten übereinst immen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
C1.b Sicherung von Protokollen	Sie speichern die Protokolldaten sicher und gewähren Lesezugriff nur Konten, die diesen für geschäftliche Zwecke benötigen . Mitarbeiter sollten jemals Protokoll daten innerhalb einer vereinbarten Aufbewahrungsfrist ändern oder löschen müssen. Erst nach Ablauf dieser Frist sollten sie gelöscht werden.	s3- bucket-public-write-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie nur autorisierten Benutzern, Prozessen und Geräten Zugriff auf Amazon Simple Storage Service (Amazon S3) - Buckets gewähren. Die Verwaltung des Zugriffs sollte mit der Klassifizierung der Daten übereinst immen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
C1.b Sicherung von Protokollen	Sie speichern die Protokolldaten sicher und gewähren Lesezugriff nur Konten, die diesen für geschäftliche Zwecke benötigen . Mitarbeiter sollten jemals Protokoll daten innerhalb einer vereinbarten Aufbewahrungsfrist ändern oder löschen müssen. Erst nach Ablauf dieser Frist sollten sie gelöscht werden.	s3- bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) unterstützt die Aufrechterhaltung einer angemesse nen Kapazität und Verfügbarkeit. CRR ermöglicht das automatische, asynchrone Kopieren von Objekten in Amazon-S3-Buckets, um die Datenverf ügbarkeit sicherzus tellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
C1.b Sicherung von Protokollen	Sie speichern die Protokolldaten sicher und gewähren Lesezugriff nur Konten, die diesen für geschäftliche Zwecke benötigen . Mitarbeiter sollten jemals Protokoll daten innerhalb einer vereinbarten Aufbewahrungsfrist ändern oder löschen müssen. Erst nach Ablauf dieser Frist sollten sie gelöscht werden.	iam-no-inline-policy-überprüfen	Stellen Sie sicher, dass ein Benutzer, eine IAM-Rolle oder eine IAM-Gruppe (AWS Identity and Access Management) nicht über eine Inline-Richtlinie zur Zugriffsk ontrolle auf Systeme und Ressource n verfügt. AWS empfiehlt, verwaltet e Richtlinien anstelle von Inline-Richtlinien zu verwenden. Verwaltete Richtlini en ermöglichen Wiederverwendbarke it, Versionsverwaltung , Rollback und Delegierung der Berechtigungsverwa ltung.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
C1.b Sicherung von Protokollen	Sie speichern die Protokolldaten sicher und gewähren Lesezugriff nur Konten, die diesen für geschäftliche Zwecke benötigen. Mitarbeiter sollten jemals Protokoll daten innerhalb einer vereinbarten Aufbewahrungsfrist ändern oder löschen müssen. Erst nach Ablauf dieser Frist sollten sie gelöscht werden.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) kann Ihnen dabei helfen, die Prinzipien der geringsten Rechte und der Aufgabentrennung in Zugriffsberechtigungen und Autorisierungen zu integrieren und so zu verhindern, dass Richtlinien „Effect“: „Allow“ mit „Action“: „*“ anstelle von „Resource“: „*“ enthalten. Wenn Benutzern mehr Rechte eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und der Aufgabentrennung verstoßen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
C1.b Sicherung von Protokollen	Sie speichern die Protokolldaten sicher und gewähren Lesezugriff nur Konten, die diesen für geschäftliche Zwecke benötigen . Mitarbeiter sollten jemals Protokoll daten innerhalb einer vereinbarten Aufbewahrungsfrist ändern oder löschen müssen. Erst nach Ablauf dieser Frist sollten sie gelöscht werden.	iam-user-group-membership-überprüfen	AWS Identity and Access Management (IAM) kann Ihnen helfen, Zugriffsberechtigungen und Autorisierungen einzuschränken, indem sichergestellt wird, dass Benutzer Mitglieder mindestens einer Gruppe sind. Wenn Benutzern mehr Berechtigungen eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und Aufgabentrennung verstoßen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
C1.b Sicherung von Protokollen	Sie speichern die Protokolldaten sicher und gewähren Lesezugriff nur Konten, die diesen für geschäftliche Zwecke benötigen . Mitarbeiter sollten jemals Protokoll daten innerhalb einer vereinbarten Aufbewahrungsfrist ändern oder löschen müssen. Erst nach Ablauf dieser Frist sollten sie gelöscht werden.	iam-user-no-policies-überprüfen	Diese Regel stellt sicher, dass AWS Identity and Access Management (IAM) -Richtlinien nur Gruppen oder Rollen zugewiese n werden, um den Zugriff auf Systeme und Ressourcen zu kontrollieren. Die Zuweisung von Berechtig ungen auf Gruppen- oder Rollenebene trägt dazu bei, die Wahrscheinlichkeit zu verringern, dass eine Identität übermäßige Berechtigungen erhält oder beibehält.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
C1.b Sicherung von Protokollen	Sie speichern die Protokolldaten sicher und gewähren Lesezugriff nur Konten, die diesen für geschäftliche Zwecke benötigen. Mitarbeiter sollten jemals Protokoll daten innerhalb einer vereinbarten Aufbewahrungsfrist ändern oder löschen müssen. Erst nach Ablauf dieser Frist sollten sie gelöscht werden.	iam-user-unused-credentials-überprüfen	AWS Identity and Access Management (IAM) kann Ihnen bei Zugriffsberechtigungen und Autorisierungen helfen, indem es nach IAM-Passwörtern und Zugriffsschlüsseln sucht, die für einen bestimmten Zeitraum nicht verwendet wurden. Wenn ungenutzte Anmeldeinformationen identifiziert werden, müssen Sie sie deaktivieren und/oder entfernen, da dies gegen das Prinzip der geringsten Berechtigung verstoßen könnte. Für diese Regel müssen Sie einen Wert für das maxCredentialUsage Alter festlegen (Standard konfiguration: 90). Der tatsächliche Wert muss den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
C1.b Sicherung von Protokollen	Sie speichern die Protokolldaten sicher und gewähren Lesezugriff nur Konten, die diesen für geschäftliche Zwecke benötigen . Mitarbeiter sollten jemals Protokoll daten innerhalb einer vereinbarten Aufbewahrungsfrist ändern oder löschen müssen. Erst nach Ablauf dieser Frist sollten sie gelöscht werden.	guardduty-enabled-centralized	Amazon GuardDuty kann mithilfe von Threat Intellige nce Feeds helfen, potenzielle Cybersich erheitsereignisse zu überwachen und zu erkennen. Dazu gehören Listen mit bösartigen IPs und maschinel len Lernmethoden zur Identifizierung unerwarteter, nicht autorisierter und bösartiger Aktivitäten in Ihrer AWS Cloud-Umgebung.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
C1.c Generierung von Warnungen	In Ihren Überwachungsdaten enthalten e Hinweise auf potenzielle Sicherheitsvorfälle werden zuverlässig identifiziert und lösen Warnen aus.	guardduty-non-archived-findings	Amazon GuardDuty hilft Ihnen dabei, die Auswirkungen eines Vorfalls zu verstehen, indem es die Ergebnisse nach Schweregrad klassifiziert: niedrig, mittel und hoch. Diese Klassifizierungen können Sie zur Festlegung von entsprechenden Strategien und Prioritäten zur Behebung solcher Vorfälle verwenden. Mit dieser Regel können Sie optional daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7) und daysHighSev (Config Default: 1) für nicht archivierte Ergebnisse festlegen, wie es die Richtlinien Ihrer Organisation erfordern.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
C1.c Generierung von Warnungen	In Ihren Überwachungsdaten enthalten e Hinweise auf potenzielle Sicherheitsvorfälle werden zuverlässig identifiziert und lösen Warnen aus.	cloudwatch-alarm-action-check	Amazon CloudWatch alarmiert, wenn eine Metrik den Schwellenwert für eine bestimmte Anzahl von Bewertungszeiträumen überschreitet. Der Alarm führt eine oder mehrere Aktionen durch, die vom Wert der Metrik oder des Ausdrucks im Vergleich zu einem Schwellenwert in einer Reihe von Zeiträumen abhängt. Diese Regel erfordert einen Wert für alarmActionRequired (Config Default: True), insufficientDataAction Required (Config Default: True), okActionRequired (Config Default: False). Der tatsächliche Wert muss die Alarmaktionen für Ihre Umgebung widerspiegeln.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
C1.c Generierung von Warnungen	In Ihren Überwachungsdaten enthalten e Hinweise auf potenzielle Sicherheitsvorfälle werden zuverlässig identifiziert und lösen Warnen aus.	s3- event-notifications-enabled	Amazon-S3-Ereignisbenachrichtigungen können das zuständige Personal über versehentliche oder vorsätzliche Änderungen an Ihren Bucket-Objekten informieren. Zu den Warnen gehören beispielsweise: Erstellung eines neuen Objekts, Entfernung eines Objekts, Wiederherstellung eines Objekts, verloren gegangene und replizierte Objekte.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
C1.c Generierung von Warnungen	In Ihren Überwachungsdaten enthalten e Hinweise auf potenzielle Sicherheitsvorfälle werden zuverlässig identifiziert und lösen Warnen aus.	securityhub-enabled	AWS Security Hub hilft bei der Überwachung von unbefugtem Personal, Verbindungen, Geräten und Software. AWS Security Hub aggregiert, organisiert und priorisiert die Sicherheitswarnungen oder Ergebnisse mehrerer Dienste. AWS Einige dieser Dienste sind Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer und AWS Firewall Manager sowie AWS Partnerlösungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
C1.c Generierung von Warnungen	In Ihren Überwachungsdaten enthalten e Hinweise auf potenzielle Sicherheitsvorfälle werden zuverlässig identifiziert und lösen Warnen aus.	api-gw-execution-logging-aktiviert	Die API-Gateway-Protokollierung zeigt detaillierte Ansichten der Benutzer, die auf die API zugegriffen haben, und wie diese Benutzer auf die API zugegriffen haben. Diese Einblicke ermöglichen die Transparenz von Benutzeraktivitäten.
C1.c Generierung von Warnungen	In Ihren Überwachungsdaten enthalten e Hinweise auf potenzielle Sicherheitsvorfälle werden zuverlässig identifiziert und lösen Warnen aus.	cloud-trail-cloud-watch-logs-aktiviert	Verwenden Sie Amazon CloudWatch , um Protokollereignisaktivitäten zentral zu sammeln und zu verwalten. Die Aufnahme von AWS CloudTrail Daten liefert Einzelheiten zu den API-Aufrufaktivitäten in Ihrem AWS-Konto.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
C1.c Generierung von Warnungen	In Ihren Überwachungsdaten enthalten e Hinweise auf potenzielle Sicherheitsvorfälle werden zuverlässig identifiziert und lösen Warnen aus.	cloudtrail-s3-dataevents-enabled	Die Erfassung von Simple Storage Service (Amazon S3)-Datenereignissen unterstützt die Erkennung von ungewöhnlichen Aktivitäten. Zu den Details gehören AWS-Konto Informationen über den Zugriff auf einen Amazon S3 S3-Bucket, die IP-Adresse und die Uhrzeit des Ereignisses.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
C1.c Generierung von Warnungen	In Ihren Überwachungsdaten enthalten Hinweise auf potenzielle Sicherheitsvorfälle werden zuverlässig identifiziert und lösen Warnen aus.	cloudtrail-security-trail-enabled	Diese Regel trägt dazu bei, die Verwendung der AWS empfohlenen bewährten Sicherheitsmethoden für sicherzustellen AWS CloudTrail, indem geprüft wird, ob mehrere Einstellungen aktiviert sind. Dazu gehören die Verwendung von Protokollverschlüsselung, Protokollvalidierung und Aktivierung AWS CloudTrail in mehreren Regionen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
C1.c Generierung von Warnungen	In Ihren Überwachungsdaten enthalten e Hinweise auf potenzielle Sicherheitsvorfälle werden zuverlässig identifiziert und lösen Warnen aus.	cw-loggroup-retention-period-überprüfen	Stellen Sie sicher, dass die Ereignisprotokolldaten für Ihre Protokollgruppen über eine Mindestdauer aufbewahrt werden, um die Fehlerbehebung und forensische Untersuchungen zu unterstützen. Fehlende frühere Ereignisprotokolldaten erschweren die Rekonstruierung und Identifizierung potenziell schädlicher Ereignisse.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
C1.c Generierung von Warnungen	In Ihren Überwachungsdaten enthalten e Hinweise auf potenzielle Sicherheitsvorfälle werden zuverlässig identifiziert und lösen Warnen aus.	elb-logging-enabled	Die Elastic-Load-Balancing-Aktivität ist ein zentraler Kommunikationspunkt innerhalb einer Umgebung. Stellen Sie sicher, dass die ELB-Protokollierung aktiviert ist. Die gesammelten Daten enthalten detaillierte Informationen zu Anfragen, die an den ELB gesendet wurden. Jedes Protokoll enthält Informationen wie die Zeit, zu der die Anforderung einging, die Client-IP-Adresse, Latenzen, Anforderungspfade und Serverantworten.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
C1.c Generierung von Warnungen	In Ihren Überwachungsdaten enthalten e Hinweise auf potenzielle Sicherheitsvorfälle werden zuverlässig identifiziert und lösen Warnen aus.	rds-logging-enabled	Um die Protokollierung und Überwachung in Ihrer Umgebung zu erleichtern, stellen Sie sicher, dass die Amazon Relational Database Service (Amazon RDS)-Protokollierung aktiviert ist. Mit der Amazon-RDS-Protokollierung können Sie Ereignisse wie Verbindungen, Verbindungsabbrüche, Abfragen oder abgefragte Tabellen erfassen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
C1.c Generierung von Warnungen	In Ihren Überwachungsdaten enthalten e Hinweise auf potenzielle Sicherheitsvorfälle werden zuverlässig identifiziert und lösen Warnen aus.	redshift-cluster-configuration-check	Um Daten im Ruhezustand zu schützen, muss die Verschlüsselung für Ihre Amazon-Redshift-Cluster aktiviert sein. Sie müssen auch sicherstellen, dass die erforderlichen Konfigurationen auf Amazon-Redshift-Clustern bereitgestellt werden. Die Prüfungsprotokollierung muss aktiviert sein, um Informationen zu Verbindungen und Benutzeraktivitäten in der Datenbank bereitzustellen. Diese Regel erfordert, dass ein Wert für clusterDbEncrypted (Config Default: TRUE) und LoggingEnabled (Config Default: TRUE) gesetzt ist. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
C1.c Generierung von Warnungen	In Ihren Überwachungsdaten enthalten e Hinweise auf potenzielle Sicherheitsvorfälle werden zuverlässig identifiziert und lösen Warnen aus.	s3- bucket-logging-enabled	Die Amazon Simple Storage Service (Amazon S3)-Serverzugriffsprotokollierung bietet eine Methode zur Überwachung des Netzwerks im Hinblick auf potenzielle Cybersicherheitsereignisse. Die Ereignisse werden überwacht, indem detaillierte Aufzeichnungen über die Anfragen erfasst werden, die an einen Amazon-S3-Bucket gestellt wurden. Jeder Zugriffsprotokolleintrag enthält Details zu einer einzelnen Zugriffsanfrage. Zu den Details gehören Anforderer, Bucket-Name, Anforderungszeit, Anforderungsaktion, Antwortstatus und Fehlercode, falls relevant.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
C1.c Generierung von Warnungen	In Ihren Überwachungsdaten enthalten e Hinweise auf potenzielle Sicherheitsvorfälle werden zuverlässig identifiziert und lösen Warnen aus.	vpc-flow-logs-enabled	VPC-Flow-Protokolle erfassen detaillierte Informationsdatensätze über den IP-Datenverkehr, der zu und von Netzwerkschnittstellen in Ihrer Amazon Virtual Private Cloud (Amazon VPC) fließt. Standardmäßig enthalten Flow-Protokolldatensätze Werte für die verschiedenen Komponenten des IP-Flows, einschließlich Quelle, Ziel und Protokoll.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
C1.c Generierung von Warnungen	In Ihren Überwachungsdaten enthalten e Hinweise auf potenzielle Sicherheitsvorfälle werden zuverlässig identifiziert und lösen Warnen aus.	wafv2-logging-enabled	Um die Protokollierung und Überwachung in Ihrer Umgebung zu erleichtern, aktivieren Sie die AWS WAF (V2) -Protokollierung im regionalen und globalen Web ACLs. AWS Die WAF-Protokollierung bietet detaillierte Informationen über den Datenverkehr, der von Ihrer Web-ACL analysiert wird. In den Protokollen werden die Uhrzeit aufgezeichnet, zu der die AWS WAF die Anfrage von Ihrer AWS Ressource erhalten hat, Informationen über die Anfrage und eine Aktion für die Regel, der jede Anfrage entsprach.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
C1.c Generierung von Warnungen	In Ihren Überwachungsdaten enthalten e Hinweise auf potenzielle Sicherheitsvorfälle werden zuverlässig identifiziert und lösen Warnen aus.	guardduty-enabled-centralized	Amazon GuardDuty kann mithilfe von Threat Intelligence Feeds helfen, potenzielle Cybersicherheitsereignisse zu überwachen und zu erkennen. Dazu gehören Listen mit bösartigen IPs und maschinellen Lernmethoden zur Identifizierung unerwarteter, nicht autorisierter und bösartiger Aktivitäten in Ihrer AWS Cloud-Umgebung.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
C1.d Identifizierung von Sicherheitsvorfällen	Sie stellen Warnungen mit Informationen über Bedrohungen und Ihre Systeme in Kontext, um die Sicherheitsvorfälle zu identifizieren, die irgendeine Form von Reaktion erfordern.	securityhub-enabled	AWS Security Hub hilft bei der Überwachung von unbefugtem Personal, Verbindungen, Geräten und Software. AWS Security Hub aggregiert, organisiert und priorisiert die Sicherheitswarnungen oder Ergebnisse mehrerer Dienste. AWS Einige dieser Dienste sind Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer und AWS Firewall Manager sowie AWS Partnerlösungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
C1.d Identifizierung von Sicherheitsvorfällen	Sie stellen Warnungen mit Informationen über Bedrohungen und Ihre Systeme in Kontext, um die Sicherheitsvorfälle zu identifizieren, die irgendeine Form von Reaktion erfordern.	guardduty-enabled-centralized	Amazon GuardDuty kann mithilfe von Threat Intelligence Feeds helfen, potenzielle Cybersicherheitsereignisse zu überwachen und zu erkennen. Dazu gehören Listen mit bösartigen IPs und maschinellen Lernmethoden zur Identifizierung unerwarteter, nicht autorisierter und bösartiger Aktivitäten in Ihrer AWS Cloud-Umgebung.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
C1.e Überwachung von Tools und Fähigkeiten	Bei der Überwachung der Fähigkeiten, Tools und Rollen der Mitarbeiter, einschließlich ausgelagerter Funktionen, sollten Governance- und Berichtsanforderungen, erwartbare Bedrohungen sowie die Komplexität der benötigten Netzwerk- oder Systemdaten berücksichtigt werden. Das Überwachungspersonal kennt die wesentlichen Funktionen, die es schützen muss.	guardduty-non-archived-findings	Amazon GuardDuty hilft Ihnen dabei, die Auswirkungen eines Vorfalls zu verstehen, indem es die Ergebnisse nach Schweregrad klassifiziert: niedrig, mittel und hoch. Diese Klassifizierungen können Sie zur Festlegung von entsprechenden Strategien und Prioritäten zur Behebung solcher Vorfälle verwenden. Mit dieser Regel können Sie optional daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7) und daysHighSev (Config Default: 1) für nicht archivierte Ergebnisse festlegen, wie es die Richtlinien Ihrer Organisation erfordern.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
C1.e Überwachung von Tools und Fähigkeiten	Bei der Überwachung der Fähigkeiten, Tools und Rollen der Mitarbeiter, einschließlich ausgelagerter Funktionen, sollten Governance- und Berichtsanforderungen, erwartbare Bedrohungen sowie die Komplexität der benötigten Netzwerk- oder Systemdaten berücksichtigt werden. Das Überwachungspersonal kennt die wesentlichen Funktionen, die es schützen muss.	securityhub-enabled	AWS Security Hub hilft bei der Überwachung von unbefugtem Personal, Verbindungen, Geräten und Software. AWS Security Hub aggregiert, organisiert und priorisiert die Sicherheitswarnungen oder Ergebnisse mehrerer Dienste. AWS Einige dieser Dienste sind Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer und AWS Firewall Manager sowie AWS Partnerlösungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
C1.e Überwachung von Tools und Fähigkeiten	Bei der Überwachung der Fähigkeiten, Tools und Rollen der Mitarbeiter, einschließlich ausgelagerter Funktionen, sollten Governance- und Berichtsanforderungen, erwartbare Bedrohungen sowie die Komplexität der benötigten Netzwerk- oder Systemdaten berücksichtigt werden. Das Überwachungspersonal kennt die wesentlichen Funktionen, die es schützen muss.	guardduty-enabled-centralized	Amazon GuardDuty kann mithilfe von Threat Intelligence Feeds helfen, potenzielle Cybersicherheitsereignisse zu überwachen und zu erkennen. Dazu gehören Listen mit bösartigen IPs und maschinellen Lernmethoden zur Identifizierung unerwarteter, nicht autorisierter und bösartiger Aktivitäten in Ihrer AWS Cloud-Umgebung.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
C2.a Systemanomalien zur Erkennung von Angriffen	Sie definieren Beispiele für ungewöhnliches Systemverhalten, die praktische Methoden zur Erkennung schädlicher Aktivitäten enthalten, die ansonsten schwer zu identifizieren sind.	securityhub-enabled	AWS Security Hub hilft bei der Überwachung von unbefugtem Personal, Verbindungen, Geräten und Software. AWS Security Hub aggregiert, organisiert und priorisiert die Sicherheitswarnungen oder Ergebnisse mehrerer Dienste. AWS Einige dieser Dienste sind Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer und AWS Firewall Manager sowie AWS Partnerlösungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
C2.a Systemano malien zur Erkennung von Angriffen	Sie definiere n Beispiele für ungewöhnliches Systemverhalten, die praktische Methoden zur Erkennung schädlicher Aktivität en enthalten, die ansonsten schwer zu identifizieren sind.	guardduty-enabled-centralized	Amazon GuardDuty kann mithilfe von Threat Intellige nce Feeds helfen, potenzielle Cybersich erheitsereignisse zu überwachen und zu erkennen. Dazu gehören Listen mit bösartigen IPs und maschinel len Lernmethoden zur Identifizierung unerwarteter, nicht autorisierter und bösartiger Aktivitäten in Ihrer AWS Cloud-Umgebung.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
D1.c Tests und Übungen	Ihre Organisation führt Übungen durch, um Reaktionspläne zu testen. Dabei werden Vorfälle aus der Vergangen heit verwendet, von denen Ihre (und andere) Organisat ionen betroffen waren, sowie Szenarien, die sich auf Bedrohung sinformationen und Ihre Risikobewertung stützen.	response-plan-exists-maintained (Prozessü berprüfung)	Stellen Sie sicher, dass Vorfallre aktionspläne erstellt, verwaltet und an das verantwortliche Personal verteilt werden. Aktualisierte und formal dokumenti erte Reaktions pläne können dazu beitragen, dass das zuständige Personal die Rollen, Verantwor tlichkeiten und Prozesse versteht, die bei einem Vorfall einzuhalten sind.
D1.c Tests und Übungen	Ihre Organisation führt Übungen durch, um Reaktionspläne zu testen. Dabei werden Vorfälle aus der Vergangen heit verwendet, von denen Ihre (und andere) Organisat ionen betroffen waren, sowie Szenarien, die sich auf Bedrohung sinformationen und Ihre Risikobewertung stützen.	response-plan-tested (Prozessüberprüfung)	Stellen Sie sicher, dass die Vorfallre aktions- und Wiederherstellungs pläne getestet wurden. Dies kann Ihnen helfen zu verstehen, ob Ihr Plan bei einem Vorfall wirksam ist und ob etwaige Lücken behoben oder Aktualisierungen vorgenommen werden müssen.

Vorlage

Die Vorlage ist verfügbar unter GitHub: Operational Best Practices for NCSC Cyber Assesment Framework.

Bewährte Methoden für die Ausführung von Services für Netzwerke und zur Bereitstellung von Inhalten

Dieses Conformance Pack enthält AWS Config Regeln, die auf Networking und Content Delivery Services basieren. Weitere Informationen finden Sie unter Netzwerke und Inhaltsbereitstellung unter AWS. Eine Liste aller verwalteten Regeln, die von unterstützt werden AWS Config, finden Sie unter Liste der AWS Config verwalteten Regeln.

Die Namen und Beschreibungen der erforderlichen Parameter finden Sie im `Parameters` Abschnitt der folgenden Vorlage.

Die Vorlage ist verfügbar unter GitHub: Operational Best Practices for Networking and Content Delivery Services.

Bewährte Methoden für die Implementierung von NIST 800-53 Rev. 4

Konformitätspakete bieten ein allgemeines Compliance-Framework, das es Ihnen ermöglicht, mithilfe verwalteter oder benutzerdefinierter Regeln und Abhilfemaßnahmen Kontrollen zur Sicherheits-, Betriebs- oder Kostenoptimierung durchzuführen. AWS Config AWS Config Conformance Packs dienen als Beispielvorlagen nicht dazu, die vollständige Einhaltung eines bestimmten Governance- oder Compliance-Standards sicherzustellen. Sie sind dafür verantwortlich, selbst zu beurteilen, ob Ihre Nutzung der Services den geltenden gesetzlichen und behördlichen Anforderungen entspricht.

Im Folgenden finden Sie ein Beispiel für eine Zuordnung zwischen den NIST 800-53- und AWS verwalteten Konfigurationsregeln. Jede Config-Regel gilt für eine bestimmte AWS Ressource und bezieht sich auf eine oder mehrere NIST 800-53-Steuerelemente. Eine Kontrolle nach NIST 800-53 kann mehreren Config-Regeln zugeordnet werden. In der folgenden Tabelle finden Sie weitere Informationen und Anleitungen zu diesen Zuordnungen.

Dieses Konformitätspaket wurde von AWS Security Assurance Services LLC (AWS SAS) validiert. Dabei handelt es sich um ein Team von qualifizierten Sicherheitsbewertern (QSAs) für die Zahlungskartenbranche (), HITRUST-zertifizierten Common Security Framework Practitionern (CCSFPs) und Compliance-Experten, die für die Beratung und Bewertung verschiedener Branchen-

Frameworks zertifiziert sind. AWS Die Experten von SAS haben dieses Conformance Pack so konzipiert, dass sich ein Kunde an einer Untergruppe von NIST 800-53 orientieren kann.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen zu
AC-2(1)	Die Organisation wendet automatisierte Mechanismen an, um die Verwaltung von Informationssystem konten zu unterstützen.	secretsmanager-scheduled-rotation-success-überprüfen	Diese Regel stellt sicher, dass AWS Secrets Manager Manager-Geheimnisse gemäß dem Rotations plan erfolgreich rotiert wurden. Die regelmäßige Rotation von Secrets kann den Zeitraum verkürzen, in dem ein Secret aktiv ist, und möglicherweise die Auswirkungen auf das Unternehmen verringern, falls es kompromittiert wird.
AC-2(1)	Die Organisation wendet automatisierte Mechanismen an, um die Verwaltung von Informationssystem konten zu unterstützen.	iam-user-group-membership-überprüfen	AWS Identity and Access Management (IAM) kann Ihnen helfen, Zugriffsberechtigungen und Autorisierungen einzuschränken, indem sichergestellt wird, dass Benutzer Mitglieder mindestens einer Gruppe sind. Wenn Benutzern

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen zu
			mehr Berechtigungen eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und Aufgabentrennung verstoßen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen zu
AC-2(1)	Die Organisation wendet automatisierte Mechanismen an, um die Verwaltung von Informationssystem konten zu unterstüt zen.	iam-password-policy	Die Identitäten und Anmeldeinformation en werden auf der Grundlage einer organisatorischen IAM-Passwortrichtlinie ausgestellt, verwaltet und verifiziert. Sie erfüllen oder übertreff en die Anforderungen von NIST SP 800-63 und dem Benchmark der Centers for Internet Security (CIS) AWS Foundatio ns in Bezug auf die Passwortstärke. Mit dieser Regel können Sie optional RequireUppercaseCh aracters (Wert für AWS grundlegende Sicherheitsbewährt e Methoden: wahr), RequireLowercaseCh aracters (Wert für bewährte Methoden für AWS grund legende Sicherhei t: wahr), RequireSy mbols (Wert für bewährte Methoden für AWS grund

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen zu
			legende Sicherhei t: wahr), RequireNu mbers (Wert für bewährte Methoden für AWS grund legende Sicherheit: wahr), MinimumPa sswordLength (Wert für bewährte Methoden für AWS grundlegende Sicherheit: 14), PasswordReusePreve ntion (Wert für bewährte Methoden für AWS grundlege nde Sicherheit: 24) und MaxPasswo rdAge (Wert für bewährte Methoden für AWS grundlege nde Sicherheit: 90) für Ihr IAM festlegen Kennwortrichtlinie. Die tatsächlichen Werte müssen den Richtlini en Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen zu
AC-2(1)	Die Organisation wendet automatisierte Mechanismen an, um die Verwaltung von Informationssystem konten zu unterstüt zen.	access-keys-rotated	Die Anmeldein formationen für autorisierte Geräte, Benutzer und Prozesse werden geprüft, indem sichergestellt wird, dass die IAM-Zugri ffsschlüssel gemäß den Vorgaben der Unternehmensrichtl inie rotiert werden. Das regelmäßi ge Ändern der Zugriffsschlüssel ist eine bewährte Sicherheitsmethode . Es verkürzt den Zeitraum, in dem ein Zugriffsschlüssel aktiv ist, und reduziert die Auswirkungen auf das Unternehmen, wenn die Schlüssel kompromittiert werden. Diese Regel erfordert einen Wert für die Zugriffsschlüssel-Rotation (Standard konfiguration: 90). Der tatsächliche Wert muss den Richtlini

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen zu
			en Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen zu
AC-2(1)	Die Organisation wendet automatisierte Mechanismen an, um die Verwaltung von Informationssystem konten zu unterstützen.	iam-user-unused-credentials-überprüfen	AWS Identity and Access Management (IAM) kann Ihnen bei Zugriffsberechtigungen und Autorisierungen helfen, indem es nach IAM-Passwörtern und Zugriffsschlüsseln sucht, die für einen bestimmten Zeitraum nicht verwendet wurden. Wenn ungenutzte Anmeldeinformationen identifiziert werden, müssen Sie sie deaktivieren und/oder entfernen, da dies gegen das Prinzip der geringsten Berechtigung verstoßen könnte. Für diese Regel müssen Sie einen Wert für das maxCredentialUsage Alter festlegen (Standardkonfiguration: 90). Der tatsächliche Wert muss den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen zu
AC-2(1)	Die Organisation wendet automatisierte Mechanismen an, um die Verwaltung von Informationssystem konten zu unterstüt zen.	securityhub-enabled	AWS Security Hub hilft bei der Überwachung von unbefugtem Personal, Verbindun gen, Geräten und Software. AWS Security Hub aggregiert, organisie rt und priorisie rt die Sicherhei tswarnungen oder Ergebnisse mehrerer Dienste. AWS Einig e dieser Dienste sind Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer und AWS Firewall Manager sowie AWS Partnerlösungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen zu
AC-2(1)	Die Organisation wendet automatisierte Mechanismen an, um die Verwaltung von Informationssystem konten zu unterstüt zen.	guardduty-enabled-centralized	Amazon GuardDuty kann mithilfe von Threat Intellige nce Feeds helfen, potenzielle Cybersich erheitsereignisse zu überwachen und zu erkennen. Dazu gehören Listen mit bösartigen IPs und maschinel len Lernmethoden zur Identifizierung unerwarteter, nicht autorisierter und bösartiger Aktivitäten in Ihrer AWS Cloud-Umgebung.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen zu
AC-2(3)	Das Informationssystem deaktiviert automatisch inaktive Konten nach [Zuordnung: organisationsdefinierter Zeitraum].	iam-user-unused-credentials-überprüfen	AWS Identity and Access Management (IAM) kann Ihnen bei Zugriffsberechtigungen und Autorisierungen helfen, indem es nach IAM-Passwörtern und Zugriffsschlüsseln sucht, die für einen bestimmten Zeitraum nicht verwendet wurden. Wenn ungenutzte Anmeldeinformationen identifiziert werden, müssen Sie sie deaktivieren und/oder entfernen, da dies gegen das Prinzip der geringsten Berechtigung verstoßen könnte. Für diese Regel müssen Sie einen Wert für das maxCredentialUsage Alter festlegen (Standardkonfiguration: 90). Der tatsächliche Wert muss den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen zu
AC-2(4)	Das Informati onssystem prüft automatisch Aktionen wie die Erstellung, Änderung, Aktivieru ng, Deaktivierung und Entfernung von Konten und benachric htigt [Zuordnung: von der Organisation designierte Mitarbeiter oder Rollen].	securityhub-enabled	AWS Security Hub hilft bei der Überwachung von unbefugtem Personal, Verbindun gen, Geräten und Software. AWS Security Hub aggregiert, organisie rt und priorisie rt die Sicherhei tswarnungen oder Ergebnisse mehrerer Dienste. AWS Einig e dieser Dienste sind Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer und AWS Firewall Manager sowie AWS Partnerlösungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen zu
AC-2(4)	Das Informati onssystem prüft automatisch Aktionen wie die Erstellung, Änderung, Aktivieru ng, Deaktivierung und Entfernung von Konten und benachric htigt [Zuordnung: von der Organisation designierte Mitarbeiter oder Rollen].	guardduty-enabled-centralized	Amazon GuardDuty kann mithilfe von Threat Intellige nce Feeds helfen, potenzielle Cybersich erheitsereignisse zu überwachen und zu erkennen. Dazu gehören Listen mit bösartigen IPs und maschinel len Lernmethoden zur Identifizierung unerwarteter, nicht autorisierter und bösartiger Aktivitäten in Ihrer AWS Cloud-Umgebung.
AC-2(4)	Das Informati onssystem prüft automatisch Aktionen wie die Erstellung, Änderung, Aktivieru ng, Deaktivierung und Entfernung von Konten und benachric htigt [Zuordnung: von der Organisation designierte Mitarbeiter oder Rollen].	cloud-trail-cloud-watch-Logs aktiviert	Verwenden Sie Amazon CloudWatc h , um Protokoll ereignisaktivitäten zentral zu sammeln und zu verwalten. Die Aufnahme von AWS CloudTrail Daten liefert Einzelheiten zu den API-Aufrufaktivitä ten in Ihrem AWS-Konto.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen zu
AC-2(4)	Das Informati onssystem prüft automatisch Aktionen wie die Erstellung, Änderung, Aktivieru ng, Deaktivierung und Entfernung von Konten und benachric htigt [Zuordnung: von der Organisation designierte Mitarbeiter oder Rollen].	cloudtrail-enabled	AWS CloudTrail kann bei der Nichtabst reitbarkeit helfen, indem Aktionen und API-Aufrufe der AWS Management Console aufgezeic hnet werden. Sie können die Benutzer und die Benutzer AWS-Konten , die einen AWS Dienst aufgerufen haben, die Quell-IP-Adresse, über die die Aufrufe generiert wurden, und den Zeitpunkt der Anrufe identifiz ieren. Einzelheiten zu den erfassten Daten finden Sie in den AWS CloudTrail Datensatzinhalten.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen zu
AC-2(4)	Das Informati onssystem prüft automatisch Aktionen wie die Erstellung, Änderung, Aktivieru ng, Deaktivierung und Entfernung von Konten und benachric htigt [Zuordnung: von der Organisation designierte Mitarbeiter oder Rollen].	multi-region-cloudtrail-enabled	AWS CloudTrail zeichnet Aktionen und API-Aufrufe der AWS Management Console auf. Sie können feststellen, welche Benutzer und Konten angerufen wurden AWS, von welcher Quell-IP-Adresse aus die Anrufe getätigt wurden und wann die Anrufe erfolgten. CloudTrai l übermittelt Protokoll dateien von allen an Ihren S3-Bucket AWS-Regionen , wenn MULTI_REG ION_CLOUD _TRAIL_ENABLED aktiviert ist. Außerdem wird beim AWS Start einer neuen Region derselbe Trail in der neuen Region erstellt. CloudTrail Dadurch erhalten Sie automatis ch Protokolldateien mit API-Aktivitäten für die neue Region.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen zu
AC-2(4)	Das Informati onssystem prüft automatisch Aktionen wie die Erstellung, Änderung, Aktivieru ng, Deaktivierung und Entfernung von Konten und benachric htigt [Zuordnung: von der Organisation designierte Mitarbeiter oder Rollen].	rds-logging-enabled	Um die Protokoll ierung und Überwachung in Ihrer Umgebung zu erleichtern, stellen Sie sicher, dass die Amazon Relationa l Database Service (Amazon RDS)-Prot okollierung aktiviert ist. Mit der Amazon-RDS-Protokollierung können Sie Ereigniss e wie Verbindungen, Verbindungsabbrüch e, Abfragen oder abgefragte Tabellen erfassen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen zu
AC-2(4)	Das Informati onssystem prüft automatisch Aktionen wie die Erstellung, Änderung, Aktivieru ng, Deaktivierung und Entfernung von Konten und benachric htigt [Zuordnung: von der Organisation designierte Mitarbeiter oder Rollen].	cloudwatch-alarm-a ction-check	Amazon CloudWatch alarmiert, wenn eine Metrik den Schwellen wert für eine bestimmte Anzahl von Bewertungszeiträum en überschreitet. Der Alarm führt eine oder mehrere Aktionen durch, die vom Wert der Metrik oder des Ausdrucks im Vergleich zu einem Schwellenwert in einer Reihe von Zeiträumen abhängt. Diese Regel erfordert einen Wert für alarmActionRequired (Config Default: True), insufficientDataAc tion Required (Config Default: True), okActionRequired (Config Default: False). Der tatsächli che Wert muss die Alarmaktionen für Ihre Umgebung widerspie geln.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen zu
AC-2(4)	Das Informationssystem prüft automatisch Aktionen wie die Erstellung, Änderung, Aktivierung, Deaktivierung und Entfernung von Konten und benachrichtigt [Zuordnung: von der Organisation designierte Mitarbeiter oder Rollen].	redshift-cluster-configuration-check	Um Daten im Ruhezustand zu schützen, muss die Verschlüsselung für Ihre Amazon-Redshift-Cluster aktiviert sein. Sie müssen auch sicherstellen, dass die erforderlichen Konfigurationen auf Amazon-Redshift-Clustern bereitgestellt werden. Die Prüfungsprotokollierung muss aktiviert sein, um Informationen zu Verbindungen und Benutzeraktivitäten in der Datenbank bereitzustellen. Diese Regel erfordert, dass ein Wert für clusterDbEncrypted (Config Default: TRUE) und LoggingEnabled (Config Default: TRUE) gesetzt ist. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen zu
AC-2(12)(a)	Die Organisation: a. Überwacht die Konten des Informationssystems im Hinblick auf [Zuordnung: von der Organisation definierte untypische Nutzung].	securityhub-enabled	AWS Security Hub hilft bei der Überwachung von unbefugtem Personal, Verbindungen, Geräten und Software. AWS Security Hub aggregiert, organisiert und priorisiert die Sicherheitswarnungen oder Ergebnisse mehrerer Dienste. AWS Einige dieser Dienste sind Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer und AWS Firewall Manager sowie AWS Partnerlösungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen zu
AC-2(12)(a)	Die Organisation: a. Überwacht die Konten des Informationssystems im Hinblick auf [Zuordnung: von der Organisation definierte untypische Nutzung].	guardduty-enabled-centralized	Amazon GuardDuty kann mithilfe von Threat Intelligence Feeds helfen, potenzielle Cybersicherheitsereignisse zu überwachen und zu erkennen. Dazu gehören Listen mit bösartigen IPs und maschinellen Lernmethoden zur Identifizierung unerwarteter, nicht autorisierter und bösartiger Aktivitäten in Ihrer AWS Cloud-Umgebung.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen zu
AC-2(f)	Die Organisation: f. Erstellt, aktiviert, ändert, deaktiviert und entfernt Konten im Informationssystem gemäß [Zuweisung: von der Organisation definierte Verfahren oder Bedingungen].	iam-user-unused-credentials-überprüfen	AWS Identity and Access Management (IAM) kann Ihnen bei Zugriffsberechtigungen und Autorisierungen helfen, indem es nach IAM-Passwörtern und Zugriffsschlüsseln sucht, die für einen bestimmten Zeitraum nicht verwendet wurden. Wenn ungenutzte Anmeldeinformationen identifiziert werden, müssen Sie sie deaktivieren und/oder entfernen, da dies gegen das Prinzip der geringsten Berechtigung verstoßen könnte. Für diese Regel müssen Sie einen Wert für das maxCredentialUsage Alter festlegen (Standardkonfiguration: 90). Der tatsächliche Wert muss den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen zu
AC-2(f)	Die Organisation: f. Erstellt, aktiviert, ändert, deaktiviert und entfernt Konten im Informationssystem gemäß [Zuweisung: von der Organisation definierte Verfahren oder Bedingungen].	iam-password-policy	Die Identitäten und Anmeldeinformationen werden auf der Grundlage einer organisatorischen IAM-Passwortrichtlinie ausgestellt, verwaltet und verifiziert. Sie erfüllen oder übertreffen die Anforderungen von NIST SP 800-63 und dem Benchmark der Centers for Internet Security (CIS) AWS Foundations in Bezug auf die Passwortstärke. Mit dieser Regel können Sie optional RequireUppercaseCharacters (Wert für AWS grundlegende Sicherheitsbewährte Methoden: wahr), RequireLowercaseCharacters (Wert für bewährte Methoden für AWS grundlegende Sicherheit: wahr), RequireSymbols (Wert für bewährte Methoden für AWS grund

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen zu
			legende Sicherhei t: wahr), RequireNu mbers (Wert für bewährte Methoden für AWS grund legende Sicherheit: wahr), MinimumPa sswordLength (Wert für bewährte Methoden für AWS grundlegende Sicherheit: 14), PasswordReusePreve ntion (Wert für bewährte Methoden für AWS grundlege nde Sicherheit: 24) und MaxPasswo rdAge (Wert für bewährte Methoden für AWS grundlege nde Sicherheit: 90) für Ihr IAM festlegen Kennwortrichtlinie. Die tatsächlichen Werte müssen den Richtlini en Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen zu
AC-2(f)	Die Organisation: f. Erstellt, aktiviert, ändert, deaktiviert und entfernt Konten im Informationssystem gemäß [Zuweisung: von der Organisation definierte Verfahren oder Bedingungen].	iam-root-access-key-überprüfen	Der Zugriff auf Systeme und Ressourcen kann gesteuert werden, indem überprüft wird, ob der Root-Benutzer keine Zugriffsschlüssel mit seiner AWS Identity and Access Management (IAM) -Rolle verknüpft hat. Stellen Sie sicher, dass die Root-Zugriffsschlüssel gelöscht werden. Erstellen und verwenden Sie stattdessen rollenbasierte Funktionen, AWS-Konten um das Prinzip der geringsten Funktionalität zu berücksichtigen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen zu
AC-2(g)	Die Organisation: g. Überwacht die Verwendung von Konten im Informationssystem.	redshift-cluster-configuration-check	Um Daten im Ruhezustand zu schützen, muss die Verschlüsselung für Ihre Amazon-Redshift-Cluster aktiviert sein. Sie müssen auch sicherstellen, dass die erforderlichen Konfigurationen auf Amazon-Redshift-Clustern bereitgestellt werden. Die Prüfungsprotokollierung muss aktiviert sein, um Informationen zu Verbindungen und Benutzeraktivitäten in der Datenbank bereitzustellen. Diese Regel erfordert, dass ein Wert für clusterDbEncrypted (Config Default: TRUE) und LoggingEnabled (Config Default: TRUE) gesetzt ist. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen zu
AC-2(g)	Die Organisation: g. Überwacht die Verwendung von Konten im Informati onssystem.	s3- bucket-logging-enabled	Die Amazon Simple Storage Service (Amazon S3)-Serverzugriffs protokollierung bietet eine Methode zur Überwachu ng des Netzwerks im Hinblick auf potenzielle Cybersich erheitsereignisse. Die Ereignisse werden überwacht, indem detaillierte Aufzeichn ungen über die Anfragen erfasst werden, die an einen Amazon-S3-Bucket gestellt wurden. Jeder Zugriffsprotokolle intrag enthält Details zu einer einzelnen Zugriffsanfrage. Zu den Details gehören Anforderer, Bucket-Name, Anforderu ngszeit, Anforderu ngsaktion, Antwortst atus und Fehlercode, falls relevant.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen zu
AC-2(g)	Die Organisation: g. Überwacht die Verwendung von Konten im Informati onssystem.	cloudtrail-enabled	AWS CloudTrail kann durch die Aufzeichn ung von Aktionen und API-Aufrufen in der AWS Manag ement Console bei der Nichtabst reitbarkeit helfen. Sie können die Benutzer und die Benutzer AWS-Konten , die einen AWS Dienst aufgerufen haben, die Quell-IP-Adresse, über die die Aufrufe generiert wurden, und den Zeitpunkt der Anrufe identifiz ieren. Einzelheiten zu den erfassten Daten finden Sie in den AWS CloudTrail Datensatzinhalten.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen zu
AC-2(g)	Die Organisation: g. Überwacht die Verwendung von Konten im Informati onssystem.	cloudtrail-s3-data events-enabled	Die Erfassung von Datenerei gnissen des Simple Storage Service (Amazon S3) hilft bei der Erkennung von ungewöhnlichen Aktivitäten. Zu den Details gehören Informationen zu dem AWS-Konto - Konto, das auf einen Amazon S3-Bucket zugegriffen hat, die IP-Adresse und die Uhrzeit des Ereigniss es.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen zu
AC-2(g)	Die Organisation: g. Überwacht die Verwendung von Konten im Informati onssystem.	securityhub-enabled	AWS Security Hub hilft bei der Überwachung von unbefugtem Personal, Verbindun gen, Geräten und Software. AWS Security Hub aggregiert, organisie rt und priorisie rt die Sicherhei tswarnungen oder Ergebnisse mehrerer Dienste. AWS Einig e dieser Dienste sind Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer und AWS Firewall Manager sowie AWS Partnerlösungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen zu
AC-2(g)	Die Organisation: g. Überwacht die Verwendung von Konten im Informati onssystem.	guardduty-enabled-centralized	Amazon GuardDuty kann mithilfe von Threat Intellige nce Feeds helfen, potenzielle Cybersich erheitsereignisse zu überwachen und zu erkennen. Dazu gehören Listen mit bösartigen IPs und maschinel len Lernmethoden zur Identifizierung unerwarteter, nicht autorisierter und bösartiger Aktivitäten in Ihrer AWS Cloud-Umgebung.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen zu
AC-2(g)	Die Organisation: g. Überwacht die Verwendung von Konten im Informati onssystem.	rds-logging-enabled	Um die Protokoll ierung und Überwachung in Ihrer Umgebung zu erleichtern, stellen Sie sicher, dass die Amazon Relationa l Database Service (Amazon RDS)-Prot okollierung aktiviert ist. Mit der Amazon-RDS-Protokollierung können Sie Ereigniss e wie Verbindungen, Verbindungsabbrüch e, Abfragen oder abgefragte Tabellen erfassen.
AC-2(g)	Die Organisation: g. Überwacht die Verwendung von Konten im Informati onssystem.	cloud-trail-cloud-watch-Logs aktiviert	Verwenden Sie Amazon CloudWatc h , um Protokoll ereignisaktivitäten zentral zu sammeln und zu verwalten. Die Aufnahme von AWS CloudTrail Daten liefert Einzelheiten zu den API-Aufrufaktivitä ten in Ihrem AWS-Konto.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen zu
AC-2(j)	Die Organisation: j. Überprüft Konten auf deren Einhaltung der Kontoverwaltungsanforderungen [Zuweisung: von der Organisation festgelegte Häufigkeit].	root-account-mfa-enabled	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass MFA für den Root-Benutzer aktiviert ist. Der Stammbenutzer ist der AWS-Konto-Benutzer mit den meisten Berechtigungen. MFA bietet eine weitere Schutzebene zusätzlich zum Benutzernamen und Passwort. Indem Sie MFA für den Root-Benutzer vorschreiben, können Sie die Anzahl AWS-Konten kompromittierter Benutzer reduzieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen zu
AC-2(j)	Die Organisation: j. Überprüft Konten auf deren Einhaltung der Kontoverwaltungsanforderungen [Zuweisung: von der Organisation festgelegte Häufigkeit].	secretsmanager-scheduled-rotation-success-überprüfen	Diese Regel stellt sicher, dass AWS Secrets Manager Manager-Geheimnisse gemäß dem Rotationsplan erfolgreich rotiert wurden. Die regelmäßige Rotation von Secrets kann den Zeitraum verkürzen, in dem ein Secret aktiv ist, und möglicherweise die Auswirkungen auf das Unternehmen verringern, falls es kompromittiert wird.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen zu
AC-2(j)	Die Organisation: j. Überprüft Konten auf deren Einhaltung der Kontoverwaltungsanforderungen [Zuweisung: von der Organisation festgelegte Häufigkeit].	iam-user-group-membership-überprüfen	AWS Identity and Access Management (IAM) kann Ihnen helfen, Zugriffsberechtigungen und Autorisierungen einzuschränken, indem sichergestellt wird, dass Benutzer Mitglieder mindestens einer Gruppe sind. Wenn Benutzern mehr Berechtigungen eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und Aufgabentrennung verstoßen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen zu
AC-2(j)	Die Organisation: j. Überprüft Konten auf deren Einhaltung der Kontoverwaltungsanforderungen [Zuweisung: von der Organisation festgelegte Häufigkeit].	iam-password-policy	Die Identitäten und Anmeldeinformationen werden auf der Grundlage einer organisatorischen IAM-Passwortrichtlinie ausgestellt, verwaltet und verifiziert. Sie erfüllen oder übertreffen die Anforderungen von NIST SP 800-63 und dem Benchmark der Centers for Internet Security (CIS) AWS Foundations in Bezug auf die Passwortstärke. Mit dieser Regel können Sie optional RequireUppercaseCharacters (Wert für AWS grundlegende Sicherheitsbewährte Methoden: wahr), RequireLowercaseCharacters (Wert für bewährte Methoden für AWS grundlegende Sicherheit: wahr), RequireSymbols (Wert für bewährte Methoden für AWS grund

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen zu
			legende Sicherhei t: wahr), RequireNu mbers (Wert für bewährte Methoden für AWS grund legende Sicherheit: wahr), MinimumPa sswordLength (Wert für bewährte Methoden für AWS grundlegende Sicherheit: 14), PasswordReusePreve ntion (Wert für bewährte Methoden für AWS grundlege nde Sicherheit: 24) und MaxPasswo rdAge (Wert für bewährte Methoden für AWS grundlege nde Sicherheit: 90) für Ihr IAM festlegen Kennwortrichtlinie. Die tatsächlichen Werte müssen den Richtlini en Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen zu
AC-2(j)	Die Organisation: j. Überprüft Konten auf deren Einhaltung der Kontoverwaltungsanforderungen [Zuweisung: von der Organisation festgelegte Häufigkeit].	access-keys-rotated	Die Anmeldeinformationen für autorisierte Geräte, Benutzer und Prozesse werden geprüft, indem sichergestellt wird, dass die IAM-Zugriffsschlüssel gemäß den Vorgaben der Unternehmensrichtlinie rotiert werden. Das regelmäßige Ändern der Zugriffsschlüssel ist eine bewährte Sicherheitsmethode. Es verkürzt den Zeitraum, in dem ein Zugriffsschlüssel aktiv ist, und reduziert die Auswirkungen auf das Unternehmen, wenn die Schlüssel kompromittiert werden. Diese Regel erfordert einen Wert für die Zugriffsschlüssel-Rotation (Standardkonfiguration: 90). Der tatsächliche Wert muss den Richtlini

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen zu
			en Ihrer Organisation entsprechen.
AC-2(j)	Die Organisation: j. Überprüft Konten auf deren Einhaltung der Kontoverwaltungsanforderungen [Zuweisung: von der Organisation festgelegte Häufigkeit].	iam-root-access-key-überprüfen	Der Zugriff auf Systeme und Ressourcen kann gesteuert werden, indem überprüft wird, ob der Root-Benutzer keine Zugriffsschlüssel mit seiner AWS Identity and Access Management (IAM) -Rolle verknüpft hat. Stellen Sie sicher, dass die Root-Zugriffsschlüssel gelöscht werden. Erstellen und verwenden Sie stattdessen rollenbasierte Funktionen, AWS-Konten um das Prinzip der geringsten Funktionalität zu berücksichtigen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen zu
AC-2(j)	Die Organisation: j. Überprüft Konten auf deren Einhaltung der Kontoverwaltungsanforderungen [Zuweisung: von der Organisation festgelegte Häufigkeit].	emr-kerberos-enabled	Die Zugriffsberechtigungen und -autorisierungen können verwaltet und nach den Prinzipien der geringsten Berechtigung und Aufgabentrennung integriert werden, indem Kerberos für Amazon-EMR-Cluster aktiviert wird. In Kerberos werden Services und Benutzer, die sich authentifizieren müssen, als Prinzipale bezeichnet. Prinzipale befinden sich in einem Kerberos-Bereich. Innerhalb dieses Bereichs wird ein Kerberos-Server als Key Distribution Center (KDC) bezeichnet. Über diesen Server können sich Prinzipale authentifizieren. Die Authentifizierung im KDC erfolgt durch die Ausstellung von Authentif

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen zu
			izierungstickets. Das KDC unterhält eine Datenbank der Prinzipale in seinem Bereich mit ihren Passwörtern und anderen administrativen Informationen zu jedem Prinzipal.
AC-2(j)	Die Organisation: j. Überprüft Konten auf deren Einhaltung der Kontoverwaltungsanforderungen [Zuweisung: von der Organisation festgelegte Häufigkeit].	iam-group-has-users-überprüfen	AWS Identity and Access Management (IAM) kann Ihnen helfen, die Prinzipien der geringsten Rechte und der Aufgabentrennung mit Zugriffsberechtigungen und Autorisierungen zu integrieren, indem sichergestellt wird, dass IAM-Gruppen mindestens einen Benutzer haben. Die Einteilung von Benutzern in Gruppen auf der Grundlage der ihnen zugewiesenen Berechtigungen oder ihrer Funktion ist eine Möglichkeit, das Prinzip der geringsten Berechtigung zu implementieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen zu
AC-2(j)	Die Organisation: j. Überprüft Konten auf deren Einhaltung der Kontoverwaltungsanforderungen [Zuweisung: von der Organisation festgelegte Häufigkeit].	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) kann Ihnen dabei helfen, die Prinzipien der geringsten Rechte und der Aufgabentrennung in Zugriffsberechtigungen und Autorisierungen zu integrieren und so zu verhindern, dass Richtlinien „Effect“: „Allow“ mit „Action“: „*“ anstelle von „Resource“: „*“ enthalten. Wenn Benutzern mehr Rechte eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und der Aufgabentrennung verstoßen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen zu
AC-2(j)	Die Organisation: j. Überprüft Konten auf deren Einhaltung der Kontoverwaltungsanforderungen [Zuweisung: von der Organisation festgelegte Häufigkeit].	iam-user-no-policies-überprüfen	Diese Regel stellt sicher, dass AWS Identity and Access Management (IAM) -Richtlinien nur Gruppen oder Rollen zugewiesen werden, um den Zugriff auf Systeme und Ressourcen zu kontrollieren. Die Zuweisung von Berechtigungen auf Gruppen- oder Rollenebene trägt dazu bei, die Wahrscheinlichkeit zu verringern, dass eine Identität übermäßige Berechtigungen erhält oder beibehält.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen zu
AC-3	Das Informati onssystem setzt genehmigte Autorisie rungen für den logischen Zugriff auf Informationen und Systemressourcen gemäß den geltenden Zugriffskontrollri chtlinien durch.	s3- bucket-public-writ e-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie nur autorisierten Benutzern, Prozessen und Geräten Zugriff auf Amazon Simple Storage Service (Amazon S3) - Buckets gewähren. Die Verwaltung des Zugriffs sollte mit der Klassifizierung der Daten übereinst immen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen zu
AC-3	Das Informati onssystem setzt genehmigte Autorisie rungen für den logischen Zugriff auf Informationen und Systemressourcen gemäß den geltenden Zugriffskontrollri chtlinien durch.	iam-user-no-policies-überprüfen	Diese Regel stellt sicher, dass AWS Identity and Access Management (IAM) -Richtlinien nur Gruppen oder Rollen zugewiese n werden, um den Zugriff auf Systeme und Ressourcen zu kontrollieren. Die Zuweisung von Berechtig ungen auf Gruppen- oder Rollenebene trägt dazu bei, die Wahrscheinlichkeit zu verringern, dass eine Identität übermäßige Berechtigungen erhält oder beibehält.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen zu
AC-3	Das Informationssystem setzt genehmigte Autorisierungen für den logischen Zugriff auf Informationen und Systemressourcen gemäß den geltenden Zugriffskontrollrichtlinien durch.	iam-user-unused-credentials-überprüfen	AWS Identity and Access Management (IAM) kann Ihnen bei Zugriffsberechtigungen und Autorisierungen helfen, indem es nach IAM-Passwörtern und Zugriffsschlüsseln sucht, die für einen bestimmten Zeitraum nicht verwendet wurden. Wenn ungenutzte Anmeldeinformationen identifiziert werden, müssen Sie sie deaktivieren und/oder entfernen, da dies gegen das Prinzip der geringsten Berechtigung verstoßen könnte. Für diese Regel müssen Sie einen Wert für das maxCredentialUsage Alter festlegen (Standardkonfiguration: 90). Der tatsächliche Wert muss den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen zu
AC-3	Das Informati onssystem setzt genehmigte Autorisie rungen für den logischen Zugriff auf Informationen und Systemressourcen gemäß den geltenden Zugriffskontrollri chtlinien durch.	lambda-function-pu blic-access-verboten	Verwalten Sie den Zugriff auf Ressource n in der AWS Cloud, indem Sie sicherste llen, dass AWS Lambda-Funktionen nicht öffentlich zugänglich sind. Der öffentliche Zugriff kann möglicherweise die Verfügbarkeit von Ressourcen beeinträc htigen.
AC-3	Das Informati onssystem setzt genehmigte Autorisie rungen für den logischen Zugriff auf Informationen und Systemressourcen gemäß den geltenden Zugriffskontrollri chtlinien durch.	rds-snapshots-public-prohibited	Verwalten Sie den Zugriff auf Ressource n in der AWS Cloud, indem Sie sicherste llen, dass Amazon Relational Database Service (Amazon RDS) -Instance s nicht öffentlic h sind. Amazon-RDS-Datenbank-Instances können vertrauliche Informati onen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen zu
AC-3	Das Informati onssystem setzt genehmigte Autorisie rungen für den logischen Zugriff auf Informationen und Systemressourcen gemäß den geltenden Zugriffskontrollri chtlinien durch.	redshift-cluster-public-access-überprüfen	Verwalten Sie den Zugriff auf Ressource n in der AWS Cloud, indem Sie sicherste llen, dass Amazon Redshift Redshift-Cluster nicht öffentlic h sind. Amazon-Re dshift-Cluster können vertrauliche Informati onen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen zu
AC-3	Das Informati onssystem setzt genehmigte Autorisie rungen für den logischen Zugriff auf Informationen und Systemressourcen gemäß den geltenden Zugriffskontrollri chtlinien durch.	s-3 bucket-policy-gran tee-check	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie s3_ bucket_policy_gran tee_check aktiviere n. Diese Regel prüft, ob der vom Amazon S3 S3-Bucket gewährte Zugriff durch die von Ihnen bereitgestellten AWS Principals, Verbundbe nutzer, Service Principals, IP-Adress en oder Amazon Virtual Private Cloud (Amazon VPC) IDs eingeschränkt ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen zu
AC-3	Das Informationssystem setzt genehmigte Autorisierungen für den logischen Zugriff auf Informationen und Systemressourcen gemäß den geltenden Zugriffskontrollrichtlinien durch.	iam-user-group-membership-überprüfen	AWS Identity and Access Management (IAM) kann Ihnen helfen, Zugriffsberechtigungen und Autorisierungen einzuschränken, indem sichergestellt wird, dass Benutzer Mitglieder mindestens einer Gruppe sind. Wenn Benutzern mehr Berechtigungen eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und Aufgabentrennung verstoßen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen zu
AC-3	Das Informati onssystem setzt genehmigte Autorisie rungen für den logischen Zugriff auf Informationen und Systemressourcen gemäß den geltenden Zugriffskontrollri chtlinien durch.	s-3 bucket-public-read -prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie nur autorisierten Benutzern, Prozessen und Geräten Zugriff auf Amazon Simple Storage Service (Amazon S3) - Buckets gewähren. Die Verwaltung des Zugriffs sollte mit der Klassifizierung der Daten übereinst immen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen zu
AC-3	Das Informati onssystem setzt genehmigte Autorisie rungen für den logischen Zugriff auf Informationen und Systemressourcen gemäß den geltenden Zugriffskontrollri chtlinien durch.	s3-Blöcke account-l evel-public-access	Verwalten Sie den Zugriff auf Ressource n in der AWS Cloud, indem Sie sicherste llen, dass Amazon Simple Storage Service (Amazon S3) -Buckets nicht öffentlich zugänglic h sind. Diese Regel trägt dazu bei, sensible Daten vor unbefugten Remote-Benutzern zu schützen, indem sie den öffentlichen Zugriff verhinder t. Mit dieser Regel können Sie optional die Parameter ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) und restrictPublicBuck ets Parameter (Config Default: True) festlegen. Die tatsächlichen Werte müssen den Richtlini

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen zu
			en Ihrer Organisation entsprechen.
AC-3	Das Informati onssystem setzt genehmigte Autorisie rungen für den logischen Zugriff auf Informationen und Systemressourcen gemäß den geltenden Zugriffskontrollri chtlinien durch.	iam-root-access-key-überprüfen	Der Zugriff auf Systeme und Ressourcen kann gesteuert werden, indem überprüft wird, ob der Root-Benu tzer keine Zugriffss chlüssel mit seiner AWS Identity and Access Management (IAM) -Rolle verknüpft hat. Stellen Sie sicher, dass die Root-Zugr iffsschlüssel gelöscht werden. Erstellen und verwenden Sie stattdessen rollenbas ierte Funktionen, AWS-Konten um das Prinzip der geringste n Funktionalität zu berücksichtigen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen zu
AC-3	Das Informati onssystem setzt genehmigte Autorisie rungen für den logischen Zugriff auf Informationen und Systemressourcen gemäß den geltenden Zugriffskontrollri chtlinien durch.	dms-replication-not-public	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass auf DMS-Replikationsin stanzen nicht öffentlic h zugegriffen werden kann. DMS-Repli kations-Instances können vertrauli che Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.
AC-3	Das Informati onssystem setzt genehmigte Autorisie rungen für den logischen Zugriff auf Informationen und Systemressourcen gemäß den geltenden Zugriffskontrollri chtlinien durch.	ebs-snapshot-public-restorable-überprüfen	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass EBS-Snapshots nicht öffentlich wiederher stellbar sind. EBS-Volume-Snapsho ts können vertrauli che Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen zu
AC-3	Das Informati onssystem setzt genehmigte Autorisie rungen für den logischen Zugriff auf Informationen und Systemressourcen gemäß den geltenden Zugriffskontrollri chtlinien durch.	emr-kerberos-enabled	Die Zugriffsberechtigu ngen und -autorisi erungen können verwaltet und nach den Prinzipien der geringsten Berechtig ung und Aufgabent rennung integrier t werden, indem Kerberos für Amazon-EMR-Cluster aktiviert wird. In Kerberos werden Services und Benutzer, die sich authentif izieren müssen, als Prinzipale bezeichnet. Prinzipal e befinden sich in einem Kerberos-Bereich. Innerhalb dieses Bereichs wird ein Kerberos-Server als Key Distribution Center (KDC) bezeichnet. Über diesen Server können sich Prinzipal e authentifizieren. Die Authentifizierung im KDC erfolgt durch die Ausstellu ng von Authentif

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen zu
			izierungstickets. Das KDC unterhält eine Datenbank der Prinzipale in seinem Bereich mit ihren Passwörtern und anderen administr ativen Informationen zu jedem Prinzipal.
AC-3	Das Informati onssystem setzt genehmigte Autorisie rungen für den logischen Zugriff auf Informationen und Systemressourcen gemäß den geltenden Zugriffskontrollri chtlinien durch.	iam-group-has-users-überprüfen	AWS Identity and Access Managemen t (IAM) kann Ihnen helfen, die Prinzipien der geringsten Rechte und der Aufgabent rennung mit Zugriffsb erechtigungen und Autorisierungen zu integrieren, indem sichergestellt wird, dass IAM-Gruppen mindestens einen Benutzer haben. Die Einteilung von Benutzern in Gruppen auf der Grundlage der ihnen zugewiese nen Berechtigungen oder ihrer Funktion ist eine Möglichkeit, das Prinzip der geringste n Berechtigung zu implementieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen zu
AC-3	Das Informationssystem setzt genehmigte Autorisierungen für den logischen Zugriff auf Informationen und Systemressourcen gemäß den geltenden Zugriffskontrollrichtlinien durch.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) kann Ihnen dabei helfen, die Prinzipien der geringsten Rechte und der Aufgabentrennung in Zugriffsberechtigungen und Autorisierungen zu integrieren und so zu verhindern, dass Richtlinien „Effect“: „Allow“ mit „Action“: „*“ anstelle von „Resource“: „*“ enthalten. Wenn Benutzern mehr Rechte eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und der Aufgabentrennung verstoßen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen zu
AC-3	Das Informationssystem setzt genehmigte Autorisierungen für den logischen Zugriff auf Informationen und Systemressourcen gemäß den geltenden Zugriffskontrollrichtlinien durch.	sagemaker-notebook-no-direct-Internetzugang	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass SageMaker Amazon-Notebooks keinen direkten Internetzugang zulassen. Indem Sie direkten Internetzugang blockieren, vermeiden Sie, dass unbefugte Benutzer auf sensible Daten zugreifen.
AC-4	Das Informationssystem setzt genehmigte Autorisierungen für die Kontrolle des Informationsflusses innerhalb des Systems und zwischen miteinander vernetzten Systemen auf der Grundlage von [Zuweisung: von der Organisation definierte Richtlinien zur Kontrolle des Informationsflusses] durch.	lambda-function-public-access-verboten	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass AWS Lambda-Funktionen nicht öffentlich zugänglich sind. Der öffentliche Zugriff kann möglicherweise die Verfügbarkeit von Ressourcen beeinträchtigen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen zu
AC-4	Das Informationssystem setzt genehmigte Autorisierungen für die Kontrolle des Informationsflusses innerhalb des Systems und zwischen miteinander vernetzten Systemen auf der Grundlage von [Zuweisung: von der Organisation definierte Richtlinien zur Kontrolle des Informationsflusses] durch.	redshift-cluster-public-access-überprüfen	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Redshift Redshift-Cluster nicht öffentlich sind. Amazon-Redshift-Cluster können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen zu
AC-4	Das Informationssystem setzt genehmigte Autorisierungen für die Kontrolle des Informationsflusses innerhalb des Systems und zwischen miteinander vernetzten Systemen auf der Grundlage von [Zuweisung: von der Organisation definierte Richtlinien zur Kontrolle des Informationsflusses] durch.	rds-snapshots-public-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Relational Database Service (Amazon RDS) -Instances nicht öffentlich sind. Amazon-RDS-Datenbank-Instances können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen zu
AC-4	Das Informationssystem setzt genehmigte Autorisierungen für die Kontrolle des Informationsflusses innerhalb des Systems und zwischen miteinander vernetzten Systemen auf der Grundlage von [Zuweisung: von der Organisation definierte Richtlinien zur Kontrolle des Informationsflusses] durch.	rds-instance-public-access-überprüfen	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Relational Database Service (Amazon RDS) -Instances nicht öffentlich sind. Amazon-RDS-Datenbank-Instances können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen zu
AC-4	Das Informationssystem setzt genehmigte Autorisierungen für die Kontrolle des Informationsflusses innerhalb des Systems und zwischen miteinander vernetzten Systemen auf der Grundlage von [Zuweisung: von der Organisation definierte Richtlinien zur Kontrolle des Informationsflusses] durch.	lambda-inside-vpc	Stellen Sie AWS Lambda-Funktionen in einer Amazon Virtual Private Cloud (Amazon VPC) bereit, um eine sichere Kommunikation zwischen einer Funktion und anderen Diensten innerhalb der Amazon VPC zu gewährleisten. Bei dieser Konfiguration sind kein Internet-Gateway, kein NAT-Gerät und keine VPN-Verbindung erforderlich. Der gesamte Datenverkehr bleibt sicher in der Cloud. AWS Domains, die sich innerhalb einer VPC befinden, verfügen aufgrund ihrer logischen Isolierung im Vergleich zu Domains mit öffentlichen Endpunkten über eine zusätzliche Sicherheitsebene. Um den Zugriff ordnungsgemäß zu verwalten,

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen zu
			sollten AWS Lambda-Funktionen einer VPC zugewiesen werden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen zu
AC-4	Das Informationssystem setzt genehmigte Autorisierungen für die Kontrolle des Informationsflusses innerhalb des Systems und zwischen miteinander vernetzten Systemen auf der Grundlage von [Zuweisung: von der Organisation definierte Richtlinien zur Kontrolle des Informationsflusses] durch.	ec-2 instances-in-vpc	Stellen Sie Amazon Elastic Compute Cloud (Amazon EC2) -Instances innerhalb einer Amazon Virtual Private Cloud (Amazon VPC) bereit, um eine sichere Kommunikation zwischen einer Instance und anderen Services innerhalb der Amazon VPC zu ermöglichen, ohne dass ein Internet-Gateway, ein NAT-Gerät oder eine VPN-Verbindung erforderlich ist. Der gesamte Datenverkehr bleibt sicher in der AWS Cloud. Domänen, die sich innerhalb einer Amazon VPC befinden, verfügen aufgrund ihrer logischen Isolierung im Vergleich zu Domänen, die öffentliche Endpunkte nutzen, über eine zusätzliche Sicherheitsebene. Weisen Sie EC2

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen zu
			Amazon-Instances einer Amazon-VPC zu, um den Zugriff ordnungsgemäß zu verwalten.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen zu
AC-4	Das Informationssystem setzt genehmigte Autorisierungen für die Kontrolle des Informationsflusses innerhalb des Systems und zwischen miteinander vernetzten Systemen auf der Grundlage von [Zuweisung: von der Organisation definierte Richtlinien zur Kontrolle des Informationsflusses] durch.	restricted-common-ports	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass gemeinsame Ports für Amazon Elastic Compute Cloud (Amazon EC2) -Sicherheitsgruppen eingeschränkt sind. Wenn der Zugriff auf Ports nicht auf vertrauenswürdige Quellen beschränkt wird, kann dies zu Angriffen auf die Verfügbarkeit, Integrität und Vertraulichkeit von Systemen führen. Mit dieser Regel können Sie optional die Parameter blockedPort1–blockedPort5 festlegen (Standardkonfigurationen: 20, 21, 3389, 3306, 4333). Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen zu
AC-4	Das Informati onssystem setzt genehmigte Autorisie rungen für die Kontrolle des Informationsflusse s innerhalb des Systems und zwischen miteinander vernetzten Systemen auf der Grundlage von [Zuweisung: von der Organisation definierte Richtlini en zur Kontrolle des Informationsflusses] durch.	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) Security Groups können bei der Verwaltung des Netzwerkzugriffs helfen, indem sie eine statusbeh aftete Filterung von eingehendem und ausgehendem Netzwerkverkehr zu Ressourcen bereitste llen. AWS Wenn Sie eingehenden (oder entfernten) Datenverk ehr von 0.0.0.0/0 bis Port 22 auf Ihren Ressourcen nicht zulassen, können Sie den Remote-Zugriff einschränken.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen zu
AC-4	Das Informationssystem setzt genehmigte Autorisierungen für die Kontrolle des Informationsflusses innerhalb des Systems und zwischen miteinander vernetzten Systemen auf der Grundlage von [Zuweisung: von der Organisation definierte Richtlinien zur Kontrolle des Informationsflusses] durch.	s3-Blöcke account-level-public-access	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Simple Storage Service (Amazon S3) -Buckets nicht öffentlich zugänglich sind. Diese Regel trägt dazu bei, sensible Daten vor unbefugten Remote-Benutzern zu schützen, indem sie den öffentlichen Zugriff verhindert. Mit dieser Regel können Sie optional die Parameter ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) und restrictPublicBuckets Parameter (Config Default: True) festlegen. Die tatsächlichen Werte müssen den Richtlini

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen zu
			en Ihrer Organisation entsprechen.
AC-4	Das Informati onssystem setzt genehmigte Autorisie rungen für die Kontrolle des Informationsflusse s innerhalb des Systems und zwischen miteinander vernetzten Systemen auf der Grundlage von [Zuweisung: von der Organisation definierte Richtlini en zur Kontrolle des Informationsflusses] durch.	s3- bucket-public-read -prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie nur autorisierten Benutzern, Prozessen und Geräten Zugriff auf Amazon Simple Storage Service (Amazon S3) - Buckets gewähren. Die Verwaltung des Zugriffs sollte mit der Klassifizierung der Daten übereinst immen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen zu
AC-4	Das Informationssystem setzt genehmigte Autorisierungen für die Kontrolle des Informationsflusses innerhalb des Systems und zwischen miteinander vernetzten Systemen auf der Grundlage von [Zuweisung: von der Organisation definierte Richtlinien zur Kontrolle des Informationsflusses] durch.	sagemaker-notebook-no-direct-Internetzugang	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass SageMaker Amazon-Notebooks keinen direkten Internetzugang zulassen. Indem Sie direkten Internetzugang blockieren, vermeiden Sie, dass unbefugte Benutzer auf sensible Daten zugreifen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen zu
AC-4	Das Informati onssystem setzt genehmigte Autorisie rungen für die Kontrolle des Informationsflusse s innerhalb des Systems und zwischen miteinander vernetzten Systemen auf der Grundlage von [Zuweisung: von der Organisation definierte Richtlini en zur Kontrolle des Informationsflusses] durch.	vpc-default-security-group-geschlossen	Sicherheitsgruppen von Amazon Elastic Compute Cloud (Amazon EC2) können bei der Verwaltung des Netzwerkzugriffs helfen, indem sie eine statusbehaftete Filterung des ein- und ausgehenden Netzwerkverkehrs zu Ressourcen bereitstellen. AWS Die Beschränk ung des gesamten Datenverkehrs auf die Standardsicherheit sgruppe hilft dabei, den Fernzugriff auf Ihre Ressourcen einzuschränken. AWS

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen zu
AC-4	Das Informationssystem setzt genehmigte Autorisierungen für die Kontrolle des Informationsflusses innerhalb des Systems und zwischen miteinander vernetzten Systemen auf der Grundlage von [Zuweisung: von der Organisation definierte Richtlinien zur Kontrolle des Informationsflusses] durch.	vpc-sg-open-only-to-authorized-ports	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass gemeinsame Ports für Amazon Elastic Compute Cloud (Amazon EC2) -Sicherheitsgruppen eingeschränkt sind. Wenn der Zugriff auf Ports nicht auf vertrauenswürdige Quellen beschränkt wird, kann dies zu Angriffen auf die Verfügbarkeit, Integrität und Vertraulichkeit von Systemen führen. Durch die Beschränkung des Zugriffs auf Ressourcen innerhalb einer Sicherheitsgruppe aus dem Internet (0.0.0.0/0) kann der Fernzugriff auf interne Systeme gesteuert werden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen zu
AC-4	Das Informationssystem setzt genehmigte Autorisierungen für die Kontrolle des Informationsflusses innerhalb des Systems und zwischen miteinander vernetzten Systemen auf der Grundlage von [Zuweisung: von der Organisation definierte Richtlinien zur Kontrolle des Informationsflusses] durch.	s-3 bucket-public-write-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie nur autorisierten Benutzern, Prozessen und Geräten Zugriff auf Amazon Simple Storage Service (Amazon S3) - Buckets gewähren. Die Verwaltung des Zugriffs sollte mit der Klassifizierung der Daten übereinstimmen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen zu
AC-4	Das Informati onssystem setzt genehmigte Autorisie rungen für die Kontrolle des Informationsflusse s innerhalb des Systems und zwischen miteinander vernetzten Systemen auf der Grundlage von [Zuweisung: von der Organisation definierte Richtlini en zur Kontrolle des Informationsflusses] durch.	acm-certificate-ex piration-check	Stellen Sie sicher, dass die Netzwerki ntegrität geschützt ist, indem Sie sicherste llen, dass X509-Zertifikate von AWS ACM ausgestel lt werden. Diese Zertifikate müssen gültig und dürfen nicht abgelaufen sein. Für diese Regel ist ein Wert für erforderlich daysToExpiration (Wert für bewährte AWS Grundregeln für Sicherheit: 90). Der tatsächliche Wert muss den Richtlini en Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen zu
AC-4	Das Informati onssystem setzt genehmigte Autorisie rungen für die Kontrolle des Informationsflusse s innerhalb des Systems und zwischen miteinander vernetzten Systemen auf der Grundlage von [Zuweisung: von der Organisation definierte Richtlini en zur Kontrolle des Informationsflusses] durch.	ec2- instance-no-public-ip	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon Elastic Compute Cloud (Amazon EC2) - Instances nicht öffentlich zugänglic h sind. EC2Amazon -Instances können vertrauliche Informati onen enthalten, und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen zu
AC-4	Das Informationssystem setzt genehmigte Autorisierungen für die Kontrolle des Informationsflusses innerhalb des Systems und zwischen miteinander vernetzten Systemen auf der Grundlage von [Zuweisung: von der Organisation definierte Richtlinien zur Kontrolle des Informationsflusses] durch.	elasticsearch-in-vpc-only	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass sich Amazon OpenSearch OpenSearch Service (Service) - Domains innerhalb einer Amazon Virtual Private Cloud (Amazon VPC) befinden. Eine OpenSearch Service-Domain innerhalb einer Amazon VPC ermöglicht die sichere Kommunikation zwischen OpenSearch Service und anderen Services innerhalb der Amazon VPC, ohne dass ein Internet-Gateway, ein NAT-Gerät oder eine VPN-Verbindung erforderlich ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen zu
AC-4	Das Informationssystem setzt genehmigte Autorisierungen für die Kontrolle des Informationsflusses innerhalb des Systems und zwischen miteinander vernetzten Systemen auf der Grundlage von [Zuweisung: von der Organisation definierte Richtlinien zur Kontrolle des Informationsflusses] durch.	dms-replication-not-public	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass auf DMS-Replikationsinstanzen nicht öffentlich zugegriffen werden kann. DMS-Replikations-Instances können vertrauliche Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen zu
AC-4	Das Informationssystem setzt genehmigte Autorisierungen für die Kontrolle des Informationsflusses innerhalb des Systems und zwischen miteinander vernetzten Systemen auf der Grundlage von [Zuweisung: von der Organisation definierte Richtlinien zur Kontrolle des Informationsflusses] durch.	ebs-snapshot-public-restorable-überprüfen	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass EBS-Snapshots nicht öffentlich wiederherstellbar sind. EBS-Volume-Snapshots können vertrauliche Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen zu
AC-4	Das Informationssystem setzt genehmigte Autorisierungen für die Kontrolle des Informationsflusses innerhalb des Systems und zwischen miteinander vernetzten Systemen auf der Grundlage von [Zuweisung: von der Organisation definierte Richtlinien zur Kontrolle des Informationsflusses] durch.	emr-master-no-public-ip	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon EMR-Cluster-Masterknoten nicht öffentlich zugänglich sind. Amazon-EMR-Cluster-Hauptknoten können vertrauliche Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen zu
AC-4	Das Informationssystem setzt genehmigte Autorisierungen für die Kontrolle des Informationsflusses innerhalb des Systems und zwischen miteinander vernetzten Systemen auf der Grundlage von [Zuweisung: von der Organisation definierte Richtlinien zur Kontrolle des Informationsflusses] durch.	internet-gateway-authorized-vpc-nur	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Internet-Gateways nur mit autorisierter Amazon Virtual Private Cloud (Amazon VPC) verbunden sind. Internet-Gateways ermöglichen den bidirektionalen Internetzugang zur und von der Amazon VPC, was möglicherweise zu einem unbefugten Zugriff auf Amazon-VPC-Ressourcen führen kann.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen zu
AC-5c	Die Organisation: c. Definiert Zugriffsberechtigungen für das Informationssystem zur Unterstützung der Aufgabentrennung.	emr-kerberos-enabled	Die Zugriffsberechtigungen und -autorisierungen können verwaltet und nach den Prinzipien der geringsten Berechtigung und Aufgabentrennung integriert werden, indem Kerberos für Amazon-EMR-Cluster aktiviert wird. In Kerberos werden Services und Benutzer, die sich authentifizieren müssen, als Prinzipale bezeichnet. Prinzipale befinden sich in einem Kerberos-Bereich. Innerhalb dieses Bereichs wird ein Kerberos-Server als Key Distribution Center (KDC) bezeichnet. Über diesen Server können sich Prinzipale authentifizieren. Die Authentifizierung im KDC erfolgt durch die Ausstellung von Authentif

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen zu
			izierungstickets. Das KDC unterhält eine Datenbank der Prinzipale in seinem Bereich mit ihren Passwörtern und anderen administrativen Informationen zu jedem Prinzipal.
AC-5c	Die Organisation: c. Definiert Zugriffsberechtigungen für das Informationssystem zur Unterstützung der Aufgabentrennung.	iam-group-has-users-überprüfen	AWS Identity and Access Management (IAM) kann Ihnen helfen, die Prinzipien der geringsten Rechte und der Aufgabentrennung mit Zugriffsberechtigungen und Autorisierungen zu integrieren, indem sichergestellt wird, dass IAM-Gruppen mindestens einen Benutzer haben. Die Einteilung von Benutzern in Gruppen auf der Grundlage der ihnen zugewiesenen Berechtigungen oder ihrer Funktion ist eine Möglichkeit, das Prinzip der geringsten Berechtigung zu implementieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen zu
AC-5c	Die Organisation: c. Definiert Zugriffsberechtigungen für das Informationssystem zur Unterstützung der Aufgabentrennung.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) kann Ihnen dabei helfen, die Prinzipien der geringsten Rechte und der Aufgabentrennung in Zugriffsberechtigungen und Autorisierungen zu integrieren und so zu verhindern, dass Richtlinien „Effect“: „Allow“ mit „Action“: „*“ anstelle von „Resource“: „*“ enthalten. Wenn Benutzern mehr Rechte eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und der Aufgabentrennung verstoßen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen zu
AC-5c	Die Organisation: c. Definiert Zugriffsb erechtigungen für das Informationssystem zur Unterstützung der Aufgabentrennung.	iam-user-no-policies-überprüfen	Diese Regel stellt sicher, dass AWS Identity and Access Management (IAM) -Richtlinien nur Gruppen oder Rollen zugewiese n werden, um den Zugriff auf Systeme und Ressourcen zu kontrollieren. Die Zuweisung von Berechtig ungen auf Gruppen- oder Rollenebene trägt dazu bei, die Wahrscheinlichkeit zu verringern, dass eine Identität übermäßige Berechtigungen erhält oder beibehält.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen zu
AC-6	Die Organisation wendet das Prinzip der geringsten Berechtigung an und erlaubt Benutzern (oder Prozessen , die im Namen von Benutzern handeln) nur dann den Zugriff, wenn dies für die Ausführun g zugewiesener Aufgaben gemäß den Unternehmenszielen und Geschäfts funktionen notwendig ist.	rds-instance-public-access-überprüfen	Verwalten Sie den Zugriff auf Ressource n in der AWS Cloud, indem Sie sicherste llen, dass Amazon Relational Database Service (Amazon RDS) -Instance s nicht öffentlic h sind. Amazon-RDS-Datenbank-Instances können vertrauliche Informati onen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen zu
AC-6	Die Organisation wendet das Prinzip der geringsten Berechtigung an und erlaubt Benutzern (oder Prozessen , die im Namen von Benutzern handeln) nur dann den Zugriff, wenn dies für die Ausführun g zugewiesener Aufgaben gemäß den Unternehmenszielen und Geschäfts funktionen notwendig ist.	rds-snapshots-public-prohibited	Verwalten Sie den Zugriff auf Ressource n in der AWS Cloud, indem Sie sicherste llen, dass Amazon Relational Database Service (Amazon RDS) -Instance s nicht öffentlic h sind. Amazon-RDS-Datenbank-Instances können vertrauliche Informati onen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen zu
AC-6	Die Organisation wendet das Prinzip der geringsten Berechtigung an und erlaubt Benutzern (oder Prozessen , die im Namen von Benutzern handeln) nur dann den Zugriff, wenn dies für die Ausführun g zugewiesener Aufgaben gemäß den Unternehmenszielen und Geschäfts funktionen notwendig ist.	redshift-cluster-public-access-überprüfen	Verwalten Sie den Zugriff auf Ressource n in der AWS Cloud, indem Sie sicherste llen, dass Amazon Redshift Redshift-Cluster nicht öffentlic h sind. Amazon-Re dshift-Cluster können vertrauliche Informati onen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen zu
AC-6	Die Organisation wendet das Prinzip der geringsten Berechtigung an und erlaubt Benutzern (oder Prozessen , die im Namen von Benutzern handeln) nur dann den Zugriff, wenn dies für die Ausführun g zugewiesener Aufgaben gemäß den Unternehmenszielen und Geschäfts funktionen notwendig ist.	s3-Blöcke account-l evel-public-access	Verwalten Sie den Zugriff auf Ressource n in der AWS Cloud, indem Sie sicherste llen, dass Amazon Simple Storage Service (Amazon S3) -Buckets nicht öffentlich zugänglic h sind. Diese Regel trägt dazu bei, sensible Daten vor unbefugten Remote-Benutzern zu schützen, indem sie den öffentlichen Zugriff verhinder t. Mit dieser Regel können Sie optional die Parameter ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) und restrictPublicBuck ets Parameter (Config Default: True) festlegen. Die tatsächlichen Werte müssen den Richtlini

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen zu
			en Ihrer Organisation entsprechen.
AC-6	Die Organisation wendet das Prinzip der geringsten Berechtigung an und erlaubt Benutzern (oder Prozessen , die im Namen von Benutzern handeln) nur dann den Zugriff, wenn dies für die Ausführun g zugewiesener Aufgaben gemäß den Unternehmenszielen und Geschäfts funktionen notwendig ist.	s3- bucket-policy-gran tee-check	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie s3_ bucket_policy_gran tee_check aktiviere n. Diese Regel prüft, ob der vom Amazon S3 S3-Bucket gewährte Zugriff durch die von Ihnen bereitgestellten AWS Principals, Verbundbe nutzer, Service Principals, IP-Adress en oder Amazon Virtual Private Cloud (Amazon VPC) IDs eingeschränkt ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen zu
AC-6	Die Organisation wendet das Prinzip der geringsten Berechtigung an und erlaubt Benutzern (oder Prozessen , die im Namen von Benutzern handeln) nur dann den Zugriff, wenn dies für die Ausführun g zugewiesener Aufgaben gemäß den Unternehmenszielen und Geschäfts funktionen notwendig ist.	s-3 bucket-public-read -prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie nur autorisierten Benutzern, Prozessen und Geräten Zugriff auf Amazon Simple Storage Service (Amazon S3) - Buckets gewähren. Die Verwaltung des Zugriffs sollte mit der Klassifizierung der Daten übereinst immen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen zu
AC-6	Die Organisation wendet das Prinzip der geringsten Berechtigung an und erlaubt Benutzern (oder Prozessen , die im Namen von Benutzern handeln) nur dann den Zugriff, wenn dies für die Ausführung zugewiesener Aufgaben gemäß den Unternehmenszielen und Geschäfts funktionen notwendig ist.	s3- bucket-public-write-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie nur autorisierten Benutzern, Prozessen und Geräten Zugriff auf Amazon Simple Storage Service (Amazon S3) - Buckets gewähren. Die Verwaltung des Zugriffs sollte mit der Klassifizierung der Daten übereinstimmen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen zu
AC-6	Die Organisation wendet das Prinzip der geringsten Berechtigung an und erlaubt Benutzern (oder Prozessen , die im Namen von Benutzern handeln) nur dann den Zugriff, wenn dies für die Ausführun g zugewiesener Aufgaben gemäß den Unternehmenszielen und Geschäfts funktionen notwendig ist.	sagemaker-notebook -no-direct-Interne tzugang	Verwalten Sie den Zugriff auf Ressource n in der AWS Cloud, indem Sie sicherste llen, dass SageMaker Amazon-Notebooks keinen direkten Internetzugang zulassen. Indem Sie direkten Internetz ugang blockieren, vermeiden Sie, dass unbefugte Benutzer auf sensible Daten zugreifen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen zu
AC-6	Die Organisation wendet das Prinzip der geringsten Berechtigung an und erlaubt Benutzern (oder Prozessen , die im Namen von Benutzern handeln) nur dann den Zugriff, wenn dies für die Ausführun g zugewiesener Aufgaben gemäß den Unternehmenszielen und Geschäfts funktionen notwendig ist.	lambda-function-pu blic-access-verboten	Verwalten Sie den Zugriff auf Ressource n in der AWS Cloud, indem Sie sicherste llen, dass AWS Lambda-Funktionen nicht öffentlich zugänglich sind. Der öffentliche Zugriff kann möglicherweise die Verfügbarkeit von Ressourcen beeinträc htigen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen zu
AC-6	Die Organisation wendet das Prinzip der geringsten Berechtigung an und erlaubt Benutzern (oder Prozessen , die im Namen von Benutzern handeln) nur dann den Zugriff, wenn dies für die Ausführung zugewiesener Aufgaben gemäß den Unternehmenszielen und Geschäfts funktionen notwendig ist.	codebuild-project-envvar-awscred-überprüfen	Stellen Sie sicher, dass die Anmeldeinformationen AWS_ACCESS_KEY_ID AWS_SECRET_ACCESS_KEY nicht in AWS Codebuild-Projektumgebungen vorhanden sind. Speichern Sie diese Variablen nicht als Klartext. Das Speichern dieser Variablen als Klartext bewirkt eine unbeabsichtigte Offenlegung von Daten sowie unberechtigte Zugriffe.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen zu
AC-6	Die Organisation wendet das Prinzip der geringsten Berechtigung an und erlaubt Benutzern (oder Prozessen , die im Namen von Benutzern handeln) nur dann den Zugriff, wenn dies für die Ausführun g zugewiesener Aufgaben gemäß den Unternehmenszielen und Geschäfts funktionen notwendig ist.	ebs-snapshot-public-restorable-überprüfen	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass EBS-Snapshots nicht öffentlich wiederher stellbar sind. EBS-Volume-Snapsho ts können vertrauli che Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen zu
AC-6	Die Organisation wendet das Prinzip der geringsten Berechtigung an und erlaubt Benutzern (oder Prozessen, die im Namen von Benutzern handeln) nur dann den Zugriff, wenn dies für die Ausführung zugewiesener Aufgaben gemäß den Unternehmenszielen und Geschäftsfunktionen notwendig ist.	iam-user-unused-credentials-überprüfen	AWS Identity and Access Management (IAM) kann Ihnen bei Zugriffsberechtigungen und Autorisierungen helfen, indem es nach IAM-Passwörtern und Zugriffsschlüsseln sucht, die für einen bestimmten Zeitraum nicht verwendet wurden. Wenn ungenutzte Anmeldeinformationen identifiziert werden, müssen Sie sie deaktivieren und/oder entfernen, da dies gegen das Prinzip der geringsten Berechtigung verstoßen könnte. Für diese Regel müssen Sie einen Wert für das maxCredentialUsage Alter festlegen (Standardkonfiguration: 90). Der tatsächliche Wert muss den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen zu
AC-6	Die Organisation wendet das Prinzip der geringsten Berechtigung an und erlaubt Benutzern (oder Prozessen , die im Namen von Benutzern handeln) nur dann den Zugriff, wenn dies für die Ausführun g zugewiesener Aufgaben gemäß den Unternehmenszielen und Geschäfts funktionen notwendig ist.	emr-kerberos-enabled	Die Zugriffsberechtigu ngen und -autorisi erungen können verwaltet und nach den Prinzipien der geringsten Berechtig ung und Aufgabent rennung integrier t werden, indem Kerberos für Amazon-EMR-Cluster aktiviert wird. In Kerberos werden Services und Benutzer, die sich authentif izieren müssen, als Prinzipale bezeichnet. Prinzipal e befinden sich in einem Kerberos-Bereich. Innerhalb dieses Bereichs wird ein Kerberos-Server als Key Distribution Center (KDC) bezeichnet. Über diesen Server können sich Prinzipal e authentifizieren. Die Authentifizierung im KDC erfolgt durch die Ausstellu ng von Authentif

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen zu
			izierungstickets. Das KDC unterhält eine Datenbank der Prinzipale in seinem Bereich mit ihren Passwörtern und anderen administrativen Informationen zu jedem Prinzipal.
AC-6	Die Organisation wendet das Prinzip der geringsten Berechtigung an und erlaubt Benutzern (oder Prozessen, die im Namen von Benutzern handeln) nur dann den Zugriff, wenn dies für die Ausführung zugewiesener Aufgaben gemäß den Unternehmenszielen und Geschäftsfunktionen notwendig ist.	iam-group-has-users-überprüfen	AWS Identity and Access Management (IAM) kann Ihnen helfen, die Prinzipien der geringsten Rechte und der Aufgabentrennung mit Zugriffsberechtigungen und Autorisierungen zu integrieren, indem sichergestellt wird, dass IAM-Gruppen mindestens einen Benutzer haben. Die Einteilung von Benutzern in Gruppen auf der Grundlage der ihnen zugewiesenen Berechtigungen oder ihrer Funktion ist eine Möglichkeit, das Prinzip der geringsten Berechtigung zu implementieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen zu
AC-6	Die Organisation wendet das Prinzip der geringsten Berechtigung an und erlaubt Benutzern (oder Prozessen , die im Namen von Benutzern handeln) nur dann den Zugriff, wenn dies für die Ausführun g zugewiesener Aufgaben gemäß den Unternehmenszielen und Geschäfts funktionen notwendig ist.	iam-policy-no-stat ements-with-admin-access	AWS Identity and Access Managemen t (IAM) kann Ihnen dabei helfen, die Prinzipien der geringsten Rechte und der Aufgabent rennung in Zugriffsb erechtigungen und Autorisierungen zu integrieren und so zu verhindern, dass Richtlinien „Effect“: „Allow“ mit „Action“: „*“ anstelle von „Resource“: „*“ enthalten. Wenn Benutzern mehr Rechte eingeräum t werden, als für die Ausführung einer Aufgabe erforderl ich sind, kann dies gegen das Prinzip der geringsten Berechtigung und der Aufgabentrennung verstoßen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen zu
AC-6	Die Organisation wendet das Prinzip der geringsten Berechtigung an und erlaubt Benutzern (oder Prozessen , die im Namen von Benutzern handeln) nur dann den Zugriff, wenn dies für die Ausführun g zugewiesener Aufgaben gemäß den Unternehmenszielen und Geschäfts funktionen notwendig ist.	iam-root-access-key-überprüfen	Der Zugriff auf Systeme und Ressourcen kann gesteuert werden, indem überprüft wird, ob der Root-Benu tzer keine Zugriffss chlüssel mit seiner AWS Identity and Access Management (IAM) -Rolle verknüpft hat. Stellen Sie sicher, dass die Root-Zugr iffsschlüssel gelöscht werden. Erstellen und verwenden Sie stattdessen rollenbas ierte Funktionen, AWS-Konten um das Prinzip der geringste n Funktionalität zu berücksichtigen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen zu
AC-6	Die Organisation wendet das Prinzip der geringsten Berechtigung an und erlaubt Benutzern (oder Prozessen , die im Namen von Benutzern handeln) nur dann den Zugriff, wenn dies für die Ausführung zugewiesener Aufgaben gemäß den Unternehmenszielen und Geschäfts funktionen notwendig ist.	iam-user-group-membership-überprüfen	AWS Identity and Access Management (IAM) kann Ihnen helfen, Zugriffsberechtigungen und Autorisierungen einzuschränken, indem sichergestellt wird, dass Benutzer Mitglieder mindestens einer Gruppe sind. Wenn Benutzern mehr Berechtigungen eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und Aufgabentrennung verstoßen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen zu
AC-6	Die Organisation wendet das Prinzip der geringsten Berechtigung an und erlaubt Benutzern (oder Prozessen , die im Namen von Benutzern handeln) nur dann den Zugriff, wenn dies für die Ausführun g zugewiesener Aufgaben gemäß den Unternehmenszielen und Geschäfts funktionen notwendig ist.	iam-user-no-policies-überprüfen	Diese Regel stellt sicher, dass AWS Identity and Access Management (IAM) -Richtlinien nur Gruppen oder Rollen zugewiese n werden, um den Zugriff auf Systeme und Ressourcen zu kontrollieren. Die Zuweisung von Berechtig ungen auf Gruppen- oder Rollenebene trägt dazu bei, die Wahrscheinlichkeit zu verringern, dass eine Identität übermäßige Berechtigungen erhält oder beibehält.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen zu
AC-6	Die Organisation wendet das Prinzip der geringsten Berechtigung an und erlaubt Benutzern (oder Prozessen , die im Namen von Benutzern handeln) nur dann den Zugriff, wenn dies für die Ausführun g zugewiesener Aufgaben gemäß den Unternehmenszielen und Geschäfts funktionen notwendig ist.	dms-replication-not-public	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass auf DMS-Replikationsin stanzen nicht öffentlic h zugegriffen werden kann. DMS-Repli kations-Instances können vertrauli che Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen zu
AC-6	Die Organisation wendet das Prinzip der geringsten Berechtigung an und erlaubt Benutzern (oder Prozessen , die im Namen von Benutzern handeln) nur dann den Zugriff, wenn dies für die Ausführun g zugewiesener Aufgaben gemäß den Unternehmenszielen und Geschäfts funktionen notwendig ist.	ec-2 instance-no-public-ip	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon Elastic Compute Cloud (Amazon EC2) - Instances nicht öffentlich zugänglic h sind. EC2Amazon -Instances können vertrauliche Informati onen enthalten, und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen zu
AC-6	Die Organisation wendet das Prinzip der geringsten Berechtigung an und erlaubt Benutzern (oder Prozessen , die im Namen von Benutzern handeln) nur dann den Zugriff, wenn dies für die Ausführun g zugewiesener Aufgaben gemäß den Unternehmenszielen und Geschäfts funktionen notwendig ist.	ec2-imdsv2-check	Stellen Sie sicher, dass die Methode Instance Metadata Service Version 2 (IMDSv2) aktiviert ist, um den Zugriff auf und die Kontrolle der Amazon Elastic Compute Cloud (Amazon EC2) - Instance-Metadate n zu schützen. Die IMDSv2 Methode verwendet sitzungsb asierte Kontrollen. Mit können Kontrolle n implementiert werden IMDSv2, um Änderungen an Instanzmetadaten einzuschränken.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen zu
AC-6	Die Organisation wendet das Prinzip der geringsten Berechtigung an und erlaubt Benutzern (oder Prozessen , die im Namen von Benutzern handeln) nur dann den Zugriff, wenn dies für die Ausführun g zugewiesener Aufgaben gemäß den Unternehmenszielen und Geschäfts funktionen notwendig ist.	iam-no-inline-policy-überprüfen	Stellen Sie sicher, dass ein Benutzer, eine IAM-Rolle oder eine IAM-Gruppe (AWS Identity and Access Management) nicht über eine Inline-Richtlinie zur Zugriffsk ontrolle auf Systeme und Ressource n verfügt. AWS empfiehlt, verwaltet e Richtlinien anstelle von Inline-Richtlinien zu verwenden. Verwaltete Richtlini en ermöglichen Wiederverwendbarke it, Versionsverwaltung , Rollback und Delegierung der Berechtigungsverwa ltung.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen zu
AC-6(10)	Das Informationssystem verhindert, dass nicht privilegierte Benutzer privilegierte Funktionen ausführen, einschließlich der Deaktivierung, Umgehung oder Änderung implementierter Sicherheitsvorkehrungen/Gegenmaßnahmen.	iam-root-access-key-überprüfen	Der Zugriff auf Systeme und Ressourcen kann gesteuert werden, indem überprüft wird, ob der Root-Benutzer keine Zugriffsschlüssel mit seiner AWS Identity and Access Management (IAM) -Rolle verknüpft hat. Stellen Sie sicher, dass die Root-Zugriffsschlüssel gelöscht werden. Erstellen und verwenden Sie stattdessen rollenbasierte Funktionen, AWS-Konten um das Prinzip der geringsten Funktionalität zu berücksichtigen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen zu
AC-17(1)	Das Informati onssystem überwacht und kontrolliert die Remote-Zugriffsmet hoden.	securityhub-enabled	AWS Security Hub hilft bei der Überwachung von unbefugtem Personal, Verbindun gen, Geräten und Software. AWS Security Hub aggregiert, organisie rt und priorisie rt die Sicherhei tswarnungen oder Ergebnisse mehrerer Dienste. AWS Einig e dieser Dienste sind Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer und AWS Firewall Manager sowie AWS Partnerlösungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen zu
AC-17(1)	Das Informati onssystem überwacht und kontrolliert die Remote-Zugriffsmet hoden.	guardduty-enabled-centralized	Amazon GuardDuty kann mithilfe von Threat Intellige nce Feeds helfen, potenzielle Cybersich erheitsereignisse zu überwachen und zu erkennen. Dazu gehören Listen mit bösartigen IPs und maschinel len Lernmethoden zur Identifizierung unerwarteter, nicht autorisierter und bösartiger Aktivitäten in Ihrer AWS Cloud-Umgebung.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen zu
AC-17(2)	Das Informati onssystem implement iert kryptografische Mechanismen, um die Vertraulichkeit und Integrität von Remote-Zugriffssitzungen zu schützen.	alb-http-to-https-Umleitungsprüfung	Um Daten während der Übertragung zu schützen, stellen Sie sicher, dass Ihr Application Load Balancer unverschl üsselte HTTP-Anfr agen automatisch an HTTPS umleitet. Um eventuell vorhanden e sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.
AC-17(2)	Das Informati onssystem implement iert kryptografische Mechanismen, um die Vertraulichkeit und Integrität von Remote-Zugriffssitzungen zu schützen.	redshift-require-tls-ssl	Stellen Sie sicher, dass Ihre Amazon-Redshift-Cluster eine TLS/SSL-Verschlüss elung erfordern, um eine Verbindun g zu SQL-Clients herzustellen. Um eventuell vorhanden e sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen zu
AC-17(2)	Das Informati onssystem implement iert kryptografische Mechanismen, um die Vertraulichkeit und Integrität von Remote-Zugriffssitzungen zu schützen.	acm-certificate-ex piration-check	Stellen Sie sicher, dass die Netzwerki ntegrität geschützt ist, indem Sie sicherste llen, dass X509-Zertifikate von ACM ausgestellt werden. AWS Diese Zertifika te müssen gültig und dürfen nicht abgelaufen sein. Für diese Regel ist ein Wert für erforderlich daysToExpiration (Wert für bewährte AWS Grundregeln für Sicherheit: 90). Der tatsächliche Wert muss den Richtlini en Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen zu
AC-17(2)	Das Informationssystem implementiert kryptografische Mechanismen, um die Vertraulichkeit und Integrität von Remote-Zugriffssitzungen zu schützen.	s-3 bucket-ssl-requests-only	Um Daten während der Übertragung zu schützen, stellen Sie sicher, dass Ihre Amazon Simple Storage Service (Amazon S3)-Buckets Anfragen zur Verwendung von Secure Socket Layer (SSL)-Buckets erfordern. Da sensible Daten vorhanden sein können, sollten Sie die Verschlüsselung bei der Übertragung aktivieren, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen zu
AC-17(2)	Das Informati onssystem implement iert kryptografische Mechanismen, um die Vertraulichkeit und Integrität von Remote-Zugriffssitzungen zu schützen.	elb-acm-certificate-required	Zum Schutz von eventuell vorhanden en sensiblen Daten sowie von Daten während der Übertragung muss die Verschlüsselung für Ihr Elastic Load Balancing aktiviert sein. Verwenden Sie AWS Certificate Manager, um öffentlic he und private SSL/ TLS-Zertifikate mit AWS Diensten und internen Ressource n zu verwalten, bereitzustellen und bereitzustellen.
AC-17(2)	Das Informati onssystem implement iert kryptografische Mechanismen, um die Vertraulichkeit und Integrität von Remote-Zugriffssitzungen zu schützen.	alb-http-drop-invalid-Header-fähig	Stellen Sie sicher, dass Ihre Elastic Load Balancers (ELB) so konfiguriert sind, dass sie HTTP-Header löschen. Da sensible Daten vorhanden sein können, sollten Sie die Verschlüsselung bei der Übertragung aktivieren, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen zu
AC-17(2)	Das Informati onssystem implement iert kryptografische Mechanismen, um die Vertraulichkeit und Integrität von Remote-Zugriffssitzungen zu schützen.	elb-tls-https-listeners-nur	Stellen Sie sicher, dass Ihre Elastic Load Balancer (ELBs) mit SSL- oder HTTPS-Listenern konfiguriert sind. Um eventuell vorhanden e sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen zu
AC-17(3)	Das Informationssystem leitet alle Fernzugriffe über [Zuweisung: von der Organisation definierte Nummer] verwaltete Netzwerkzugriffskontrollpunkte weiter.	internet-gateway-authorized-vpc-nur	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Internet-Gateways nur mit autorisierter Amazon Virtual Private Cloud (Amazon VPC) verbunden sind. Internet-Gateways ermöglichen den bidirektionalen Internetzugang zur und von der Amazon VPC, was möglicherweise zu einem unbefugten Zugriff auf Amazon-VPC-Ressourcen führen kann.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen zu
AC-21(b)	Die Organisation: b. Verwendet [Zuweisung: von der Organisation definierte automatisierte Mechanismen oder manuelle Prozesse], um Benutzer bei Entscheidungen hinsichtlich Informationsweitergabe/Zusammenarbeit zu unterstützen.	dms-replication-not-public	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass auf DMS-Replikationsinstanzen nicht öffentlich zugegriffen werden kann. DMS-Replikations-Instances können vertrauliche Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.
AC-21(b)	Die Organisation: b. Verwendet [Zuweisung: von der Organisation definierte automatisierte Mechanismen oder manuelle Prozesse], um Benutzer bei Entscheidungen hinsichtlich Informationsweitergabe/Zusammenarbeit zu unterstützen.	ebs-snapshot-public-restorable-überprüfen	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass EBS-Snapshots nicht öffentlich wiederherstellbar sind. EBS-Volume-Snapshots können vertrauliche Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen zu
AC-21(b)	Die Organisation: b. Verwendet [Zuweisung: von der Organisation definierte automatisierte Mechanismen oder manuelle Prozesse], um Benutzer bei Entscheidungen hinsichtlich Informationsweitergabe/Zusammenarbeit zu unterstützen.	ec-2 instance-no-public-ip	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon Elastic Compute Cloud (Amazon EC2) - Instances nicht öffentlich zugänglich sind. EC2Amazon-Instances können vertrauliche Informationen enthalten, und für solche Konten ist eine Zugriffskontrolle erforderlich.
AC-21(b)	Die Organisation: b. Verwendet [Zuweisung: von der Organisation definierte automatisierte Mechanismen oder manuelle Prozesse], um Benutzer bei Entscheidungen hinsichtlich Informationsweitergabe/Zusammenarbeit zu unterstützen.	emr-master-no-public-ip	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon EMR-Cluster-Masterknoten nicht öffentlich zugänglich sind. Amazon-EMR-Cluster-Hauptknoten können vertrauliche Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen zu
AC-21(b)	Die Organisation: b. Verwendet [Zuweisung: von der Organisation definierte automatisierte Mechanismen oder manuelle Prozesse], um Benutzer bei Entscheidungen hinsichtlich Informationsweitergabe/Zusammenarbeit zu unterstützen.	lambda-function-public-access-verboten	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass AWS Lambda-Funktionen nicht öffentlich zugänglich sind. Der öffentliche Zugriff kann möglicherweise die Verfügbarkeit von Ressourcen beeinträchtigen.
AC-21(b)	Die Organisation: b. Verwendet [Zuweisung: von der Organisation definierte automatisierte Mechanismen oder manuelle Prozesse], um Benutzer bei Entscheidungen hinsichtlich Informationsweitergabe/Zusammenarbeit zu unterstützen.	rds-instance-public-access-überprüfen	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Relational Database Service (Amazon RDS) -Instances nicht öffentlich sind. Amazon-RDS-Datenbank-Instances können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen zu
AC-21(b)	Die Organisation: b. Verwendet [Zuweisung: von der Organisation definierte automatisierte Mechanismen oder manuelle Prozesse], um Benutzer bei Entscheidungen hinsichtlich Informationsweitergabe/Zusammenarbeit zu unterstützen.	rds-snapshots-public-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Relational Database Service (Amazon RDS) -Instances nicht öffentlich sind. Amazon-RDS-Datenbank-Instances können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen zu
AC-21(b)	Die Organisation: b. Verwendet [Zuweisung: von der Organisation definierte automatisierte Mechanismen oder manuelle Prozesse], um Benutzer bei Entscheidungen hinsichtlich Informationsweitergabe/Zusammenarbeit zu unterstützen.	redshift-cluster-public-access-überprüfen	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Redshift Redshift-Cluster nicht öffentlich sind. Amazon-Redshift-Cluster können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen zu
AC-21(b)	Die Organisation: b. Verwendet [Zuweisung: von der Organisation definierte automatisierte Mechanismen oder manuelle Prozesse], um Benutzer bei Entscheidungen hinsichtlich Informationsweitergabe/Zusammenarbeit zu unterstützen.	s3-Blöcke account-level-public-access	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Simple Storage Service (Amazon S3) -Buckets nicht öffentlich zugänglich sind. Diese Regel trägt dazu bei, sensible Daten vor unbefugten Remote-Benutzern zu schützen, indem sie den öffentlichen Zugriff verhindert. Mit dieser Regel können Sie optional die Parameter ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) und restrictPublicBuckets Parameter (Config Default: True) festlegen. Die tatsächlichen Werte müssen den Richtlini

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen zu
			en Ihrer Organisation entsprechen.
AC-21(b)	Die Organisation: b. Verwendet [Zuweisung: von der Organisation definierte automatisierte Mechanismen oder manuelle Prozesse], um Benutzer bei Entscheidungen hinsichtlich Informationsweitergabe/Zusammenarbeit zu unterstützen.	s3- bucket-public-read-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie nur autorisierten Benutzern, Prozessen und Geräten Zugriff auf Amazon Simple Storage Service (Amazon S3) - Buckets gewähren. Die Verwaltung des Zugriffs sollte mit der Klassifizierung der Daten übereinstimmen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen zu
AC-21(b)	Die Organisation: b. Verwendet [Zuweisung: von der Organisation definierte automatisierte Mechanismen oder manuelle Prozesse], um Benutzer bei Entscheidungen hinsichtlich Informationsweitergabe/Zusammenarbeit zu unterstützen.	s3- bucket-public-write-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie nur autorisierten Benutzern, Prozessen und Geräten Zugriff auf Amazon Simple Storage Service (Amazon S3) - Buckets gewähren. Die Verwaltung des Zugriffs sollte mit der Klassifizierung der Daten übereinstimmen.
AC-21(b)	Die Organisation: b. Verwendet [Zuweisung: von der Organisation definierte automatisierte Mechanismen oder manuelle Prozesse], um Benutzer bei Entscheidungen hinsichtlich Informationsweitergabe/Zusammenarbeit zu unterstützen.	sagemaker-notebook-no-direct-Internetzugang	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass SageMaker Amazon-Notebooks keinen direkten Internetzugang zulassen. Indem Sie direkten Internetzugang blockieren, vermeiden Sie, dass unbefugte Benutzer auf sensible Daten zugreifen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen zu
AU-2(a)(d)	Die Organisation: a. Stellt fest, dass das Informationssystem in der Lage ist, die folgenden Ereignisse zu prüfen: [Aufgabe: vom Unternehmen definierte überprüfbare Ereignisse]; d. Legt fest, dass die folgenden Ereignisse innerhalb des Informationssystems geprüft werden sollen: [Zuordnung: von der Organisation definierte zu prüfende Ereignisse (die in AU-2 a. definierte Teilmenge der zu prüfenden Ereignisse) zusammen mit der Häufigkeit der Prüfung (oder der Situation, die eine Prüfung für jedes identifizierte Ereignis erfordert)].	api-gw-execution-logging-aktiviert	Die API-Gateway-Protokollierung zeigt detaillierte Ansichten der Benutzer, die auf die API zugegriffen haben, und wie diese Benutzer auf die API zugegriffen haben. Diese Einblicke ermöglichen die Transparenz von Benutzeraktivitäten.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen zu
AU-2(a)(d)	Die Organisation: a. Stellt fest, dass das Informationssystem in der Lage ist, die folgenden Ereignisse zu prüfen: [Aufgabe: vom Unternehmen definierte überprüfbare Ereignisse]; d. Legt fest, dass die folgenden Ereignisse innerhalb des Informationssystems geprüft werden sollen: [Zuordnung: von der Organisation definierte zu prüfende Ereignisse (die in AU-2 a. definierte Teilmenge der zu prüfenden Ereignisse) zusammen mit der Häufigkeit der Prüfung (oder der Situation, die eine Prüfung für jedes identifizierte Ereignis erfordert)].	cloud-trail-cloud-watch-logs-aktiviert	Verwenden Sie Amazon CloudWatch , um Protokoll ereignisaktivitäten zentral zu sammeln und zu verwalten. Die Aufnahme von AWS CloudTrail Daten liefert Einzelheiten zu den API-Aufrufaktivitäten in Ihrem AWS-Konto.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen zu
AU-2(a)(d)	Die Organisation: a. Stellt fest, dass das Informationssystem in der Lage ist, die folgenden Ereignisse zu prüfen: [Aufgabe: vom Unternehmen definierte überprüfbare Ereignisse]; d. Legt fest, dass die folgenden Ereignisse innerhalb des Informationssystems geprüft werden sollen: [Zuordnung: von der Organisation definierte zu prüfende Ereignisse (die in AU-2 a. definierte Teilmenge der zu prüfenden Ereignisse) zusammen mit der Häufigkeit der Prüfung (oder der Situation, die eine Prüfung für jedes identifizierte Ereignis erfordert)].	cloudtrail-s3-dataevents-enabled	Die Erfassung von Datenereignissen des Simple Storage Service (Amazon S3) hilft bei der Erkennung von ungewöhnlichen Aktivitäten. Zu den Details gehören Informationen zu dem AWS-Konto - Konto, das auf einen Amazon S3-Bucket zugegriffen hat, die IP-Adresse und die Uhrzeit des Ereignisses.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen zu
AU-2(a)(d)	Die Organisation: a. Stellt fest, dass das Informationssystem in der Lage ist, die folgenden Ereignisse zu prüfen: [Aufgabe: vom Unternehmen definierte überprüfbare Ereignisse]; d. Legt fest, dass die folgenden Ereignisse innerhalb des Informationssystems geprüft werden sollen: [Zuordnung: von der Organisation definierte zu prüfende Ereignisse (die in AU-2 a. definierte Teilmenge der zu prüfenden Ereignisse) zusammen mit der Häufigkeit der Prüfung (oder der Situation, die eine Prüfung für jedes identifizierte Ereignis erfordert)].	cloudtrail-enabled	AWS CloudTrail kann bei der Nichtabstreitbarkeit helfen, indem Aktionen und API-Aufrufe der AWS Management Console aufgezeichnet werden. Sie können die Benutzer und die Benutzer AWS-Konten , die einen AWS Dienst aufgerufen haben, die Quell-IP-Adresse, über die die Aufrufe generiert wurden, und den Zeitpunkt der Anrufe identifizieren. Einzelheiten zu den erfassten Daten finden Sie in den AWS CloudTrail Datensatzinhalten.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen zu
AU-2(a)(d)	Die Organisation: a. Stellt fest, dass das Informationssystem in der Lage ist, die folgenden Ereignisse zu prüfen: [Aufgabe: vom Unternehmen definierte überprüfbare Ereignisse]; d. Legt fest, dass die folgenden Ereignisse innerhalb des Informationssystems geprüft werden sollen: [Zuordnung: von der Organisation definierte zu prüfende Ereignisse (die in AU-2 a. definierte Teilmenge der zu prüfenden Ereignisse) zusammen mit der Häufigkeit der Prüfung (oder der Situation, die eine Prüfung für jedes identifizierte Ereignis erfordert)].	elb-logging-enabled	Die Elastic-Load-Balancing-Aktivität ist ein zentraler Kommunikationspunkt innerhalb einer Umgebung. Stellen Sie sicher, dass die ELB-Protokollierung aktiviert ist. Die gesammelten Daten enthalten detaillierte Informationen zu Anfragen, die an den ELB gesendet wurden. Jedes Protokoll enthält Informationen wie die Zeit, zu der die Anforderung einging, die Client-IP-Adresse, Latenzen, Anforderungspfade und Serverantworten.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen zu
AU-2(a)(d)	Die Organisation: a. Stellt fest, dass das Informationssystem in der Lage ist, die folgenden Ereignisse zu prüfen: [Aufgabe: vom Unternehmen definierte überprüfbare Ereignisse]; d. Legt fest, dass die folgenden Ereignisse innerhalb des Informationssystems geprüft werden sollen: [Zuordnung: von der Organisation definierte zu prüfende Ereignisse (die in AU-2 a. definierte Teilmenge der zu prüfenden Ereignisse) zusammen mit der Häufigkeit der Prüfung (oder der Situation, die eine Prüfung für jedes identifizierte Ereignis erfordert)].	multi-region-cloudtrail-enabled	AWS CloudTrail zeichnet Aktionen und API-Aufrufe der AWS Management Console auf. Sie können feststellen, welche Benutzer und Konten angerufen wurden AWS, von welcher Quell-IP-Adresse aus die Anrufe getätigt wurden und wann die Anrufe erfolgten. CloudTrail übermittelt Protokolldateien von allen an Ihren S3-Bucket AWS-Regionen , wenn MULTI_REGION_CLOUD_TRAIL_ENABLED aktiviert ist. Außerdem wird beim AWS Start einer neuen Region derselbe Trail in der neuen Region erstellt. CloudTrail Dadurch erhalten Sie automatisch Protokolldateien mit API-Aktivitäten für die neue Region.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen zu
AU-2(a)(d)	Die Organisation: a. Stellt fest, dass das Informationssystem in der Lage ist, die folgenden Ereignisse zu prüfen: [Aufgabe: vom Unternehmen definierte überprüfbare Ereignisse]; d. Legt fest, dass die folgenden Ereignisse innerhalb des Informationssystems geprüft werden sollen: [Zuordnung: von der Organisation definierte zu prüfende Ereignisse (die in AU-2 a. definierte Teilmenge der zu prüfenden Ereignisse) zusammen mit der Häufigkeit der Prüfung (oder der Situation, die eine Prüfung für jedes identifizierte Ereignis erfordert)].	s-3 bucket-logging-enabled	Die Amazon Simple Storage Service (Amazon S3)-Serverzugriffsprotokollierung bietet eine Methode zur Überwachung des Netzwerks im Hinblick auf potenzielle Cybersicherheitsereignisse. Die Ereignisse werden überwacht, indem detaillierte Aufzeichnungen über die Anfragen erfasst werden, die an einen Amazon-S3-Bucket gestellt wurden. Jeder Zugriffsprotokolleintrag enthält Details zu einer einzelnen Zugriffsanfrage. Zu den Details gehören Anforderer, Bucket-Name, Anforderungszeit, Anforderungsaktion, Antwortstatus und Fehlercode, falls relevant.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen zu
AU-2(a)(d)	Die Organisation: a. Stellt fest, dass das Informationssystem in der Lage ist, die folgenden Ereignisse zu prüfen: [Aufgabe: vom Unternehmen definierte überprüfbare Ereignisse]; d. Legt fest, dass die folgenden Ereignisse innerhalb des Informationssystems geprüft werden sollen: [Zuordnung: von der Organisation definierte zu prüfende Ereignisse (die in AU-2 a. definierte Teilmenge der zu prüfenden Ereignisse) zusammen mit der Häufigkeit der Prüfung (oder der Situation, die eine Prüfung für jedes identifizierte Ereignis erfordert)].	vpc-flow-logs-enabled	VPC-Flow-Protokolle erfassen detaillierte Informationsdatensätze über den IP-Datenverkehr, der zu und von Netzwerkschnittstellen in Ihrer Amazon Virtual Private Cloud (Amazon VPC) fließt. Standardmäßig enthalten Flow-Protokolldatensätze Werte für die verschiedenen Komponenten des IP-Flows, einschließlich Quelle, Ziel und Protokoll.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen zu
AU-2(a)(d)	Die Organisation: a. Stellt fest, dass das Informationssystem in der Lage ist, die folgenden Ereignisse zu prüfen: [Aufgabe: vom Unternehmen definierte überprüfbare Ereignisse]; d. Legt fest, dass die folgenden Ereignisse innerhalb des Informationssystems geprüft werden sollen: [Zuordnung: von der Organisation definierte zu prüfende Ereignisse (die in AU-2 a. definierte Teilmenge der zu prüfenden Ereignisse) zusammen mit der Häufigkeit der Prüfung (oder der Situation, die eine Prüfung für jedes identifizierte Ereignis erfordert)].	rds-logging-enabled	Um die Protokollierung und Überwachung in Ihrer Umgebung zu erleichtern, stellen Sie sicher, dass die Amazon Relational Database Service (Amazon RDS)-Protokollierung aktiviert ist. Mit der Amazon-RDS-Protokollierung können Sie Ereignisse wie Verbindungen, Verbindungsabbrüche, Abfragen oder abgefragte Tabellen erfassen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen zu
AU-2(a)(d)	Die Organisation: a. Stellt fest, dass das Informationssystem in der Lage ist, die folgenden Ereignisse zu prüfen: [Aufgabe: vom Unternehmen definierte überprüfbare Ereignisse]; d. Legt fest, dass die folgenden Ereignisse innerhalb des Informationssystems geprüft werden sollen: [Zuordnung: von der Organisation definierte zu prüfende Ereignisse (die in AU-2 a. definierte Teilmenge der zu prüfenden Ereignisse) zusammen mit der Häufigkeit der Prüfung (oder der Situation, die eine Prüfung für jedes identifizierte Ereignis erfordert)].	wafv2-logging-enabled	Um die Protokollierung und Überwachung in Ihrer Umgebung zu erleichtern, aktivieren Sie die AWS WAF (V2) -Protokollierung im regionalen und globalen Web ACLs. AWS Die WAF-Protokollierung bietet detaillierte Informationen über den Datenverkehr, der von Ihrer Web-ACL analysiert wird. In den Protokollen werden die Uhrzeit aufgezeichnet, zu der die AWS WAF die Anfrage von Ihrer AWS Ressource erhalten hat, Informationen über die Anfrage und eine Aktion für die Regel, der jede Anfrage entsprach.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen zu
AU-2(a)(d)	Die Organisation: a. Stellt fest, dass das Informationssystem in der Lage ist, die folgenden Ereignisse zu prüfen: [Aufgabe: vom Unternehmen definierte überprüfbare Ereignisse]; d. Legt fest, dass die folgenden Ereignisse innerhalb des Informationssystems geprüft werden sollen: [Zuordnung: von der Organisation definierte zu prüfende Ereignisse (die in AU-2 a. definierte Teilmenge der zu prüfenden Ereignisse) zusammen mit der Häufigkeit der Prüfung (oder der Situation, die eine Prüfung für jedes identifizierte Ereignis erfordert)].	redshift-cluster-configuration-check	Um Daten im Ruhezustand zu schützen, muss die Verschlüsselung für Ihre Amazon-Redshift-Cluster aktiviert sein. Sie müssen auch sicherstellen, dass die erforderlichen Konfigurationen auf Amazon-Redshift-Clustern bereitgestellt werden. Die Prüfungsprotokollierung muss aktiviert sein, um Informationen zu Verbindungen und Benutzeraktivitäten in der Datenbank bereitzustellen. Diese Regel erfordert, dass ein Wert für clusterDbEncrypted (Config Default: TRUE) und LoggingEnabled (Config Default: TRUE) gesetzt ist. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen zu
AU-3	Das Informationssystem generiert Prüfprotokolle mit Informationen, aus denen hervorgeht, welche Art von Ereignis eingetreten ist, wann und wo das Ereignis stattgefunden hat, welchen Ursprung das Ereignis hat, wie es ausging und mit welchen Personen oder Subjekten das Ereignis in Verbindung steht.	api-gw-execution-logging-aktiviert	Die API-Gateway-Protokollierung zeigt detaillierte Ansichten der Benutzer, die auf die API zugegriffen haben, und wie diese Benutzer auf die API zugegriffen haben. Diese Einblicke ermöglichen die Transparenz von Benutzeraktivitäten.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen zu
AU-3	Das Informati onssystem generiert Prüfprotokolle mit Informationen, aus denen hervorgeh t, welche Art von Ereignis eingetret en ist, wann und wo das Ereignis stattgefunden hat, welchen Ursprung das Ereignis hat, wie es ausging und mit welchen Personen oder Subjekten das Ereignis in Verbindun g steht.	cloud-trail-cloud-watch-logs-aktiviert	Verwenden Sie Amazon CloudWatc h , um Protokoll ereignisaktivitäten zentral zu sammeln und zu verwalten. Die Aufnahme von AWS CloudTrail Daten liefert Einzelheiten zu den API-Aufrufaktivitä ten in Ihrem AWS-Konto.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen zu
AU-3	Das Informati onssystem generiert Prüfprotokolle mit Informationen, aus denen hervorgeh t, welche Art von Ereignis eingetret en ist, wann und wo das Ereignis stattgefunden hat, welchen Ursprung das Ereignis hat, wie es ausging und mit welchen Personen oder Subjekten das Ereignis in Verbindun g steht.	cloudtrail-s3-data events-enabled	Die Erfassung von Datenerei gnissen des Simple Storage Service (Amazon S3) hilft bei der Erkennung von ungewöhnlichen Aktivitäten. Zu den Details gehören Informationen zu dem AWS-Konto - Konto, das auf einen Amazon S3-Bucket zugegriffen hat, die IP-Adresse und die Uhrzeit des Ereigniss es.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen zu
AU-3	Das Informati onssystem generiert Prüfprotokolle mit Informationen, aus denen hervorgeh t, welche Art von Ereignis eingetret en ist, wann und wo das Ereignis stattgefunden hat, welchen Ursprung das Ereignis hat, wie es ausging und mit welchen Personen oder Subjekten das Ereignis in Verbindun g steht.	rds-logging-enabled	Um die Protokoll ierung und Überwachung in Ihrer Umgebung zu erleichtern, stellen Sie sicher, dass die Amazon Relationa l Database Service (Amazon RDS)-Prot okollierung aktiviert ist. Mit der Amazon-RDS-Protokollierung können Sie Ereigniss e wie Verbindungen, Verbindungsabbrüch e, Abfragen oder abgefragte Tabellen erfassen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen zu
AU-3	Das Informati onssystem generiert Prüfprotokolle mit Informationen, aus denen hervorgeh t, welche Art von Ereignis eingetret en ist, wann und wo das Ereignis stattgefunden hat, welchen Ursprung das Ereignis hat, wie es ausging und mit welchen Personen oder Subjekten das Ereignis in Verbindun g steht.	cloudtrail-enabled	AWS CloudTrail kann bei der Nichtabst reitbarkeit helfen, indem Aktionen und API-Aufrufe der AWS Management Console aufgezeic hnet werden. Sie können die Benutzer und die Benutzer AWS-Konten , die einen AWS Dienst aufgerufen haben, die Quell-IP-Adresse, über die die Aufrufe generiert wurden, und den Zeitpunkt der Anrufe identifiz ieren. Einzelheiten zu den erfassten Daten finden Sie in den AWS CloudTrail Datensatzinhalten.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen zu
AU-3	Das Informati onssystem generiert Prüfprotokolle mit Informationen, aus denen hervorgeh t, welche Art von Ereignis eingetret en ist, wann und wo das Ereignis stattgefunden hat, welchen Ursprung das Ereignis hat, wie es ausging und mit welchen Personen oder Subjekten das Ereignis in Verbindun g steht.	elb-logging-enabled	Die Elastic-Load-Balancing-Aktivität ist ein zentraler Kommunikationspunk t innerhalb einer Umgebung. Stellen Sie sicher, dass die ELB-Protokollierun g aktiviert ist. Die gesammelten Daten enthalten detaillie rte Informationen zu Anfragen, die an den ELB gesendet wurden. Jedes Protokoll enthält Informationen wie die Zeit, zu der die Anforderung einging, die Client-IP -Adresse, Latenzen, Anforderungspfade und Serverantworten.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen zu
AU-3	Das Informati onssystem generiert Prüfprotokolle mit Informationen, aus denen hervorgeh t, welche Art von Ereignis eingetret en ist, wann und wo das Ereignis stattgefunden hat, welchen Ursprung das Ereignis hat, wie es ausging und mit welchen Personen oder Subjekten das Ereignis in Verbindun g steht.	multi-region-cloudtrail-enabled	AWS CloudTrail zeichnet Aktionen und API-Aufrufe der AWS Management Console auf. Sie können feststellen, welche Benutzer und Konten angerufen wurden AWS, von welcher Quell-IP-Adresse aus die Anrufe getätigt wurden und wann die Anrufe erfolgten. CloudTrai l übermittelt Protokoll dateien von allen an Ihren S3-Bucket AWS-Regionen , wenn MULTI_REG ION_CLOUD _TRAIL_ENABLED aktiviert ist. Außerdem wird beim AWS Start einer neuen Region derselbe Trail in der neuen Region erstellt. CloudTrail Dadurch erhalten Sie automatis ch Protokolldateien mit API-Aktivitäten für die neue Region.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen zu
AU-3	Das Informati onssystem generiert Prüfprotokolle mit Informationen, aus denen hervorgeh t, welche Art von Ereignis eingetret en ist, wann und wo das Ereignis stattgefunden hat, welchen Ursprung das Ereignis hat, wie es ausging und mit welchen Personen oder Subjekten das Ereignis in Verbindun g steht.	s-3 bucket-logging-enabled	Die Amazon Simple Storage Service (Amazon S3)-Serverzugriffs protokollierung bietet eine Methode zur Überwachu ng des Netzwerks im Hinblick auf potenzielle Cybersich erheitsereignisse. Die Ereignisse werden überwacht, indem detaillierte Aufzeichn ungen über die Anfragen erfasst werden, die an einen Amazon-S3-Bucket gestellt wurden. Jeder Zugriffsprotokolle intrag enthält Details zu einer einzelnen Zugriffsanfrage. Zu den Details gehören Anforderer, Bucket-Name, Anforderu ngszeit, Anforderu ngsaktion, Antwortst atus und Fehlercode, falls relevant.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen zu
AU-3	Das Informationssystem generiert Prüfprotokolle mit Informationen, aus denen hervorgeht, welche Art von Ereignis eingetreten ist, wann und wo das Ereignis stattgefunden hat, welchen Ursprung das Ereignis hat, wie es ausging und mit welchen Personen oder Subjekten das Ereignis in Verbindung steht.	vpc-flow-logs-enabled	VPC-Flow-Protokolle erfassen detaillierte Informationsdatensätze über den IP-Datenverkehr, der zu und von Netzwerkschnittstellen in Ihrer Amazon Virtual Private Cloud (Amazon VPC) fließt. Standardmäßig enthalten Flow-Protokolldatensätze Werte für die verschiedenen Komponenten des IP-Flows, einschließlich Quelle, Ziel und Protokoll.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen zu
AU-3	Das Informationssystem generiert Prüfprotokolle mit Informationen, aus denen hervorgeht, welche Art von Ereignis eingetreten ist, wann und wo das Ereignis stattgefunden hat, welchen Ursprung das Ereignis hat, wie es ausging und mit welchen Personen oder Subjekten das Ereignis in Verbindung steht.	redshift-cluster-configuration-check	Um Daten im Ruhezustand zu schützen, muss die Verschlüsselung für Ihre Amazon-Redshift-Cluster aktiviert sein. Sie müssen auch sicherstellen, dass die erforderlichen Konfigurationen auf Amazon-Redshift-Clustern bereitgestellt werden. Die Prüfungsprotokollierung muss aktiviert sein, um Informationen zu Verbindungen und Benutzeraktivitäten in der Datenbank bereitzustellen. Diese Regel erfordert, dass ein Wert für clusterDbEncrypted (Config Default: TRUE) und LoggingEnabled (Config Default: TRUE) gesetzt ist. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen zu
AU-3	Das Informationssystem generiert Prüfprotokolle mit Informationen, aus denen hervorgeht, welche Art von Ereignis eingetreten ist, wann und wo das Ereignis stattgefunden hat, welchen Ursprung das Ereignis hat, wie es ausging und mit welchen Personen oder Subjekten das Ereignis in Verbindung steht.	wafv2-logging-enabled	Um die Protokollierung und Überwachung in Ihrer Umgebung zu erleichtern, aktivieren Sie die AWS WAF (V2) -Protokollierung im regionalen und globalen Web. ACLs AWS Die WAF-Protokollierung bietet detaillierte Informationen über den Datenverkehr, der von Ihrer Web-ACL analysiert wird. In den Protokollen werden die Uhrzeit aufgezeichnet, zu der die AWS WAF die Anfrage von Ihrer AWS Ressource erhalten hat, Informationen über die Anfrage und eine Aktion für die Regel, der jede Anfrage entsprach.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen zu
AU-6(1)(3)	(1) Die Organisation setzt automatisierte Mechanismen zur Integration von Prüfungs-, Analyse- und Berichtsprozessen ein, um die Prozesse der Organisation zur Untersuchung und Reaktion auf verdächtige Aktivitäten zu unterstützen. (3) Die Organisation analysiert und korreliert Prüfungsunterlagen aus verschiedenen Repositorys, um sich ein Bild über die Situation in der gesamten Organisation zu verschaffen.	guardduty-enabled-centralized	Amazon GuardDuty kann mithilfe von Threat Intelligence Feeds helfen, potenzielle Cybersicherheitsereignisse zu überwachen und zu erkennen. Dazu gehören Listen mit bösartigen IPs und maschinellen Lernmethoden zur Identifizierung unerwarteter, nicht autorisierter und bösartiger Aktivitäten in Ihrer AWS Cloud-Umgebung.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen zu
AU-6(1)(3)	(1) Die Organisation setzt automatisierte Mechanismen zur Integration von Prüfungs-, Analyse- und Berichtsprozessen ein, um die Prozesse der Organisation zur Untersuchung und Reaktion auf verdächtige Aktivitäten zu unterstützen. (3) Die Organisation analysiert und korreliert Prüfungsunterlagen aus verschiedenen Repositorys, um sich ein Bild über die Situation in der gesamten Organisation zu verschaffen.	securityhub-enabled	AWS Security Hub hilft bei der Überwachung von unbefugtem Personal, Verbindungen, Geräten und Software. AWS Security Hub aggregiert, organisiert und priorisiert die Sicherheitswarnungen oder Ergebnisse mehrerer Dienste. AWS Einige dieser Dienste sind Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer und AWS Firewall Manager sowie AWS Partnerlösungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen zu
AU-6(1)(3)	(1) Die Organisation setzt automatisierte Mechanismen zur Integration von Prüfungs-, Analyse- und Berichtsprozessen ein, um die Prozesse der Organisation zur Untersuchung und Reaktion auf verdächtige Aktivitäten zu unterstützen. (3) Die Organisation analysiert und korreliert Prüfungsunterlagen aus verschiedenen Repositorys, um sich ein Bild über die Situation in der gesamten Organisation zu verschaffen.	cloudwatch-alarm-action-check	Amazon CloudWatch alarmiert, wenn eine Metrik den Schwellenwert für eine bestimmte Anzahl von Bewertungszeiträumen überschreitet. Der Alarm führt eine oder mehrere Aktionen durch, die vom Wert der Metrik oder des Ausdrucks im Vergleich zu einem Schwellenwert in einer Reihe von Zeiträumen abhängt. Diese Regel erfordert einen Wert für alarmActionRequired (Config Default: True), insufficientDataAction Required (Config Default: True), okActionRequired (Config Default: False). Der tatsächliche Wert muss die Alarmaktionen für Ihre Umgebung widerspiegeln.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen zu
AU-6(1)(3)	(1) Die Organisation setzt automatisierte Mechanismen zur Integration von Prüfungs-, Analyse- und Berichtsprozessen ein, um die Prozesse der Organisation zur Untersuchung und Reaktion auf verdächtige Aktivitäten zu unterstützen. (3) Die Organisation analysiert und korreliert Prüfungsunterlagen aus verschiedenen Repositorys, um sich ein Bild über die Situation in der gesamten Organisation zu verschaffen.	cloud-trail-cloud-watch-logs-aktiviert	Verwenden Sie Amazon CloudWatch , um Protokollereignisaktivitäten zentral zu sammeln und zu verwalten. Die Aufnahme von AWS CloudTrail Daten liefert Einzelheiten zu den API-Aufrufaktivitäten in Ihrem AWS-Konto.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen zu
AU-7(1)	Das Informationssystem bietet die Möglichkeit, Prüfungsunterlagen für Ereignisse von Interesse auf der Grundlage von [Zuweisung: von der Organisation definierte Prüfungsfelder in den Prüfungsunterlagen] zu verarbeiten.	cloudwatch-alarm-action-check	Amazon CloudWatch alarmiert, wenn eine Metrik den Schwellenwert für eine bestimmte Anzahl von Bewertungszeiträumen überschreitet. Der Alarm führt eine oder mehrere Aktionen durch, die vom Wert der Metrik oder des Ausdrucks im Vergleich zu einem Schwellenwert in einer Reihe von Zeiträumen abhängt. Diese Regel erfordert einen Wert für alarmActionRequired (Config Default: True), insufficientDataAction Required (Config Default: True), okActionRequired (Config Default: False). Der tatsächliche Wert muss die Alarmaktionen für Ihre Umgebung widerspiegeln.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen zu
AU-7(1)	Das Informationssystem bietet die Möglichkeit, Prüfungsunterlagen für Ereignisse von Interesse auf der Grundlage von [Zuweisung: von der Organisation definierte Prüfungsfelder in den Prüfungsunterlagen] zu verarbeiten.	cloud-trail-cloud-watch-logs-aktiviert	Verwenden Sie Amazon CloudWatch , um Protokollereignisaktivitäten zentral zu sammeln und zu verwalten. Die Aufnahme von AWS CloudTrail Daten liefert Einzelheiten zu den API-Aufrufaktivitäten in Ihrem AWS-Konto.
AU-9	Das Informationssystem schützt Prüfungsinformationen und -tools vor unbefugtem Zugriff, Änderung und Löschung.	cloud-trail-encryption-enabled	Da sensible Daten vorhanden sein können und um Daten im Speicher zu schützen, sollten Sie sicherstellen, dass die Verschlüsselung für Ihre AWS CloudTrail Trails aktiviert ist.
AU-9	Das Informationssystem schützt Prüfungsinformationen und -tools vor unbefugtem Zugriff, Änderung und Löschung.	cloudwatch-log-group-encrypted	Um sensible Daten im Speicher zu schützen, stellen Sie sicher, dass die Verschlüsselung für Ihre Amazon CloudWatch Log Groups aktiviert ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen zu
AU-9(2)	Das Informationssystem sichert Auditaufzeichnungen [Zuordnung: von der Organisation festgelegte Häufigkeit] auf einem physisch anderen System oder einer anderen Systemkomponente als dem zu auditierenden System oder der zu auditierenden Komponente.	s-3 bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) unterstützt die Aufrechterhaltung einer angemessenen Kapazität und Verfügbarkeit. CRR ermöglicht das automatische, asynchrone Kopieren von Objekten in Amazon S3 Buckets, um die Datenverfügbarkeit sicherzustellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen zu
AU-11	Die Organisation bewahrt Prüfaufzeichnungen für [Aufgabe: organisationsdefinierter Zeitraum im Einklang mit den Richtlinien zur Aufbewahrung von Aufzeichnungen] auf, um die after-the-fact Untersuchung von Sicherheitsvorfällen zu unterstützen und die behördlichen und organisatorischen Anforderungen zur Aufbewahrung von Informationen zu erfüllen.	cw-loggroup-retention-period-überprüfen	Stellen Sie sicher, dass die Ereignisprotokolldaten für Ihre Protokollgruppen über eine Mindestdauer aufbewahrt werden, um die Fehlerbehebung und forensische Untersuchungen zu unterstützen. Fehlende frühere Ereignisprotokolldaten erschweren die Rekonstruierung und Identifizierung potenziell schädlicher Ereignisse.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen zu
AU-12(a)(c)	Das Informationssystem: a. Bietet die Fähigkeit zur Erstellung von Audit-Aufzeichnungen für die in AU-2 a. definierten auditierbaren Ereignisse bei [Zuordnung: von der Organisation definierte Informationssystemkomponenten]; c. Generiert Prüfungsunterlagen für die in AU-2 d. definierten Ereignisse mit dem in AU-3 definierten Inhalt.	api-gw-execution-logging-aktiviert	Die API-Gateway-Protokollierung zeigt detaillierte Ansichten der Benutzer, die auf die API zugegriffen haben, und wie diese Benutzer auf die API zugegriffen haben. Diese Einblicke ermöglichen die Transparenz von Benutzeraktivitäten.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen zu
AU-12(a)(c)	Das Informationssystem: a. Bietet die Fähigkeit zur Erstellung von Audit-Aufzeichnungen für die in AU-2 a. definierten auditierbaren Ereignisse bei [Zuordnung: von der Organisation definierte Informationssystemkomponenten]; c. Generiert Prüfungsunterlagen für die in AU-2 d. definierten Ereignisse mit dem in AU-3 definierten Inhalt.	cloud-trail-cloud-watch-logs-aktiviert	Verwenden Sie Amazon CloudWatch , um Protokollereignisaktivitäten zentral zu sammeln und zu verwalten. Die Aufnahme von AWS CloudTrail Daten liefert Einzelheiten zu den API-Aufrufaktivitäten in Ihrem AWS-Konto.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen zu
AU-12(a)(c)	Das Informationssystem: a. Bietet die Fähigkeit zur Erstellung von Audit-Aufzeichnungen für die in AU-2 a. definierten auditierbaren Ereignisse bei [Zuordnung: von der Organisation definierte Informationssystemkomponenten]; c. Generiert Prüfungsunterlagen für die in AU-2 d. definierten Ereignisse mit dem in AU-3 definierten Inhalt.	cloudtrail-s3-dataevents-enabled	Die Erfassung von Datenereignissen des Simple Storage Service (Amazon S3) hilft bei der Erkennung von ungewöhnlichen Aktivitäten. Zu den Details gehören Informationen zum AWS-Konto , das auf einen Amazon S3 Bucket zugegriffen hat, die IP-Adresse und die Uhrzeit des Ereignisses.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen zu
AU-12(a)(c)	Das Informationssystem: a. Bietet die Fähigkeit zur Erstellung von Audit-Aufzeichnungen für die in AU-2 a. definierten auditierbaren Ereignisse bei [Zuordnung: von der Organisation definierte Informationssystemkomponenten]; c. Generiert Prüfungsunterlagen für die in AU-2 d. definierten Ereignisse mit dem in AU-3 definierten Inhalt.	rds-logging-enabled	Um die Protokollierung und Überwachung in Ihrer Umgebung zu erleichtern, stellen Sie sicher, dass die Amazon Relational Database Service (Amazon RDS)-Protokollierung aktiviert ist. Mit der Amazon-RDS-Protokollierung können Sie Ereignisse wie Verbindungen, Verbindungsabbrüche, Abfragen oder abgefragte Tabellen erfassen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen zu
AU-12(a)(c)	Das Informati onssystem: a. Bietet die Fähigkeit zur Erstellung von Audit-Aufzeichnungen für die in AU-2 a. definierten auditierb aren Ereignisse bei [Zuordnung: von der Organisation definiert e Informationssystem komponenten]; c. Generiert Prüfungsu nterlagen für die in AU-2 d. definierten Ereignisse mit dem in AU-3 definierten Inhalt.	cloudtrail-enabled	AWS CloudTrail kann bei der Nichtabst reitbarkeit helfen, indem Aktionen und API-Aufrufe der AWS Management Console aufgezeic hnet werden. Sie können die Benutzer und die Benutzer AWS-Konten , die einen AWS Dienst aufgerufen haben, die Quell-IP-Adresse, über die die Aufrufe generiert wurden, und den Zeitpunkt der Anrufe identifiz ieren. Einzelheiten zu den erfassten Daten finden Sie in den AWS CloudTrail Datensatzinhalten.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen zu
AU-12(a)(c)	Das Informationssystem: a. Bietet die Fähigkeit zur Erstellung von Audit-Aufzeichnungen für die in AU-2 a. definierten auditierbaren Ereignisse bei [Zuordnung: von der Organisation definierte Informationssystemkomponenten]; c. Generiert Prüfungsunterlagen für die in AU-2 d. definierten Ereignisse mit dem in AU-3 definierten Inhalt.	elb-logging-enabled	Die Elastic-Load-Balancing-Aktivität ist ein zentraler Kommunikationspunkt innerhalb einer Umgebung. Stellen Sie sicher, dass die ELB-Protokollierung aktiviert ist. Die gesammelten Daten enthalten detaillierte Informationen zu Anfragen, die an den ELB gesendet wurden. Jedes Protokoll enthält Informationen wie die Zeit, zu der die Anforderung einging, die Client-IP-Adresse, Latenzen, Anforderungspfade und Serverantworten.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen zu
AU-12(a)(c)	Das Informationssystem: a. Bietet die Fähigkeit zur Erstellung von Audit-Aufzeichnungen für die in AU-2 a. definierten auditierbaren Ereignisse bei [Zuordnung: von der Organisation definierte Informationssystemkomponenten]; c. Generiert Prüfungsunterlagen für die in AU-2 d. definierten Ereignisse mit dem in AU-3 definierten Inhalt.	multi-region-cloudtrail-enabled	AWS CloudTrail zeichnet Aktionen und API-Aufrufe der AWS Management Console auf. Sie können feststellen, welche Benutzer und Konten angerufen wurden AWS, von welcher Quell-IP-Adresse aus die Anrufe getätigt wurden und wann die Anrufe erfolgten. CloudTrail übermittelt Protokolldateien von allen an Ihren S3-Bucket AWS-Regionen , wenn MULTI_REGION_CLOUD_TRAIL_ENABLED aktiviert ist. Außerdem wird beim AWS Start einer neuen Region derselbe Trail in der neuen Region erstellt. CloudTrail Dadurch erhalten Sie automatisch Protokolldateien mit API-Aktivitäten für die neue Region.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen zu
AU-12(a)(c)	Das Informati onssystem: a. Bietet die Fähigkeit zur Erstellung von Audit-Aufzeichnungen für die in AU-2 a. definierten auditierb aren Ereignisse bei [Zuordnung: von der Organisation definiert e Informationssystem komponenten]; c. Generiert Prüfungsu nterlagen für die in AU-2 d. definierten Ereignisse mit dem in AU-3 definierten Inhalt.	s-3 bucket-logging-enabled	Die Amazon Simple Storage Service (Amazon S3)-Serverzugriffs protokollierung bietet eine Methode zur Überwachu ng des Netzwerks im Hinblick auf potenzielle Cybersich erheitsereignisse. Die Ereignisse werden überwacht, indem detaillierte Aufzeichn ungen über die Anfragen erfasst werden, die an einen Amazon-S3-Bucket gestellt wurden. Jeder Zugriffsprotokolle intrag enthält Details zu einer einzelnen Zugriffsanfrage. Zu den Details gehören Anforderer, Bucket-Name, Anforderu ngszeit, Anforderu ngsaktion, Antwortst atus und Fehlercode, falls relevant.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen zu
AU-12(a)(c)	Das Informationssystem: a. Bietet die Fähigkeit zur Erstellung von Audit-Aufzeichnungen für die in AU-2 a. definierten auditierbaren Ereignisse bei [Zuordnung: von der Organisation definierte Informationssystemkomponenten]; c. Generiert Prüfungsunterlagen für die in AU-2 d. definierten Ereignisse mit dem in AU-3 definierten Inhalt.	vpc-flow-logs-enabled	VPC-Flow-Protokolle erfassen detaillierte Informationsdatensätze über den IP-Datenverkehr, der zu und von Netzwerkschnittstellen in Ihrer Amazon Virtual Private Cloud (Amazon VPC) fließt. Standardmäßig enthalten Flow-Protokolldatensätze Werte für die verschiedenen Komponenten des IP-Flows, einschließlich Quelle, Ziel und Protokoll.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen zu
AU-12(a)(c)	Das Informationssystem: a. Bietet die Fähigkeit zur Erstellung von Audit-Aufzeichnungen für die in AU-2 a. definierten auditierbaren Ereignisse bei [Zuordnung: von der Organisation definierte Informationssystemkomponenten]; c. Generiert Prüfungsunterlagen für die in AU-2 d. definierten Ereignisse mit dem in AU-3 definierten Inhalt.	wafv2-logging-enabled	Um die Protokollierung und Überwachung in Ihrer Umgebung zu erleichtern, aktivieren Sie die AWS WAF (V2) -Protokollierung im regionalen und globalen Web ACLs. AWS Die WAF-Protokollierung bietet detaillierte Informationen über den Datenverkehr, der von Ihrer Web-ACL analysiert wird. In den Protokollen werden die Uhrzeit aufgezeichnet, zu der die AWS WAF die Anfrage von Ihrer AWS Ressource erhalten hat, Informationen über die Anfrage und eine Aktion für die Regel, der jede Anfrage entsprach.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen zu
AU-12(a)(c)	Das Informationssystem: a. Bietet die Fähigkeit zur Erstellung von Audit-Aufzeichnungen für die in AU-2 a. definierten auditierbaren Ereignisse bei [Zuordnung: von der Organisation definierte Informationssystemkomponenten]; c. Generiert Prüfungsunterlagen für die in AU-2 d. definierten Ereignisse mit dem in AU-3 definierten Inhalt.	redshift-cluster-configuration-check	Um Daten im Ruhezustand zu schützen, muss die Verschlüsselung für Ihre Amazon-Redshift-Cluster aktiviert sein. Sie müssen auch sicherstellen, dass die erforderlichen Konfigurationen auf Amazon-Redshift-Clustern bereitgestellt werden. Die Prüfungsprotokollierung muss aktiviert sein, um Informationen zu Verbindungen und Benutzeraktivitäten in der Datenbank bereitzustellen. Diese Regel erfordert, dass ein Wert für clusterDbEncrypted (Config Default: TRUE) und LoggingEnabled (Config Default: TRUE) gesetzt ist. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen zu
CA-7(a)(b)	Die Organisation entwickelt eine Strategie zur kontinuierlichen Überwachung und implementiert ein kontinuierliches Überwachungsprogramm, das Folgendes umfasst: a. Festlegung von [Zuweisung: von der Organisation definierte Kennzahlen], die überwacht werden sollen; b. Festlegung von [Zuweisung: von der Organisation festgelegte Häufigkeiten] für die Überwachung und [Zuweisung: von der Organisation festgelegte Häufigkeiten] für Bewertungen, die diese Überwachung unterstützen.	guardduty-enabled-centralized	Amazon GuardDuty kann mithilfe von Threat Intelligence Feeds helfen, potenzielle Cybersicherheitsereignisse zu überwachen und zu erkennen. Dazu gehören Listen mit bösartigen IPs und maschinellen Lernmethoden zur Identifizierung unerwarteter, nicht autorisierter und bösartiger Aktivitäten in Ihrer AWS Cloud-Umgebung.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen zu
CA-7(a)(b)	Die Organisation entwickelt eine Strategie zur kontinuierlichen Überwachung und implementiert ein kontinuierliches Überwachungsprogramm, das Folgendes umfasst: a. Festlegung von [Zuweisung: von der Organisation definierte Kennzahlen], die überwacht werden sollen; b. Festlegung von [Zuweisung: von der Organisation festgelegte Häufigkeiten] für die Überwachung und [Zuweisung: von der Organisation festgelegte Häufigkeiten] für Bewertungen, die diese Überwachung unterstützen.	securityhub-enabled	AWS Security Hub hilft bei der Überwachung von unbefugtem Personal, Verbindungen, Geräten und Software. AWS Security Hub aggregiert, organisiert und priorisiert die Sicherheitswarnungen oder Ergebnisse mehrerer Dienste. AWS Einige dieser Dienste sind Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer und AWS Firewall Manager sowie AWS Partnerlösungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen zu
CA-7(a)(b)	Die Organisation entwickelt eine Strategie zur kontinuierlichen Überwachung und implementiert ein kontinuierliches Überwachungsprogramm, das Folgendes umfasst: a. Festlegung von [Zuweisung: von der Organisation definierte Kennzahlen], die überwacht werden sollen; b. Festlegung von [Zuweisung: von der Organisation festgelegte Häufigkeiten] für die Überwachung und [Zuweisung: von der Organisation festgelegte Häufigkeiten] für Bewertungen, die diese Überwachung unterstützen.	cloud-trail-cloud-watch-logs-aktiviert	Verwenden Sie Amazon CloudWatch , um Protokoll ereignisaktivitäten zentral zu sammeln und zu verwalten. Die Aufnahme von AWS CloudTrail Daten liefert Einzelheiten zu den API-Aufrufaktivitäten in Ihrem AWS-Konto.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen zu
CA-7(a)(b)	Die Organisation entwickelt eine Strategie zur kontinuierlichen Überwachung und implementiert ein kontinuierliches Überwachungsprogramm, das Folgendes umfasst: a. Festlegung von [Zuweisung: von der Organisation definierte Kennzahlen], die überwacht werden sollen; b. Festlegung von [Zuweisung: von der Organisation festgelegte Häufigkeiten] für die Überwachung und [Zuweisung: von der Organisation festgelegte Häufigkeiten] für Bewertungen, die diese Überwachung unterstützen.	cloudwatch-alarm-action-check	Amazon CloudWatch alarmiert, wenn eine Metrik den Schwellenwert für eine bestimmte Anzahl von Bewertungszeiträumen überschreitet. Der Alarm führt eine oder mehrere Aktionen durch, die vom Wert der Metrik oder des Ausdrucks im Vergleich zu einem Schwellenwert in einer Reihe von Zeiträumen abhängt. Diese Regel erfordert einen Wert für alarmActionRequired (Config Default: True), insufficientDataAction Required (Config Default: True), okActionRequired (Config Default: False). Der tatsächliche Wert muss die Alarmaktionen für Ihre Umgebung widerspiegeln.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen zu
CA-7(a)(b)	Die Organisation entwickelt eine Strategie zur kontinuierlichen Überwachung und implementiert ein kontinuierliches Überwachungsprogramm, das Folgendes umfasst: a. Festlegung von [Zuweisung: von der Organisation definierte Kennzahlen], die überwacht werden sollen; b. Festlegung von [Zuweisung: von der Organisation festgelegte Häufigkeiten] für die Überwachung und [Zuweisung: von der Organisation festgelegte Häufigkeiten] für Bewertungen, die diese Überwachung unterstützen.	ec2- instance-detailed-monitoring-enabled	Aktivieren Sie diese Regel, um die Amazon Elastic Compute Cloud (Amazon EC2) - Instance-Überwachung auf der EC2 Amazon-Konsole zu verbessern, in der Monitoring-Diagramme mit einem Zeitraum von 1 Minute für die Instance angezeigt werden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen zu
CA-7(a)(b)	Die Organisation entwickelt eine Strategie zur kontinuierlichen Überwachung und implementiert ein kontinuierliches Überwachungsprogramm, das Folgendes umfasst: a. Festlegung von [Zuweisung: von der Organisation definierte Kennzahlen], die überwacht werden sollen; b. Festlegung von [Zuweisung: von der Organisation festgelegte Häufigkeiten] für die Überwachung und [Zuweisung: von der Organisation festgelegte Häufigkeiten] für Bewertungen, die diese Überwachung unterstützen.	rds-enhanced-monitoring-enabled	Aktivieren Sie Amazon Relational Database Service (Amazon RDS), um die Verfügbarkeit von Amazon RDS zu überwachen. Dies bietet einen detaillierten Einblick in den Zustand Ihrer Amazon-RDS-Datenbank-Instances. Wenn der Amazon-RDS-Speicher mehr als ein zugrunde liegendes physisches Gerät verwendet, erfasst Enhanced Monitoring die Daten für jedes Gerät. Wenn die Datenbank-Instance von Amazon RDS in einer Multi-AZ-Bereitstellung ausgeführt wird, werden außerdem die Daten für jedes Gerät auf dem sekundären Host sowie die Metriken des sekundären Hosts erfasst.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen zu
CM-2	Die Organisation entwickelt, dokumentiert und verwaltet unter Konfigurationskontrolle eine aktuelle Basiskonfiguration des Informationssystems.	ec2-managerinstance-managed-by-systems	Eine Bestandsaufnahme der Softwareplattformen und Anwendungen innerhalb des Unternehmens ist möglich, indem Amazon Elastic Compute Cloud (Amazon EC2) - Instances mit AWS Systems Manager verwaltet werden. Verwenden Sie AWS Systems Manager, um detaillierte Systemkonfigurationen, Betriebssystem-Patch-Levels, Namen und Typ der Dienste, Softwareinstallationen, Anwendungsname, Herausgeber und Version sowie andere Details zu Ihrer Umgebung bereitzustellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen zu
CM-2	Die Organisation entwickelt, dokumentiert und verwaltet unter Konfigurationskontrolle eine aktuelle Basiskonfiguration des Informationssystems.	ec2-check managedinstance-association-compliance-status	Verwenden Sie AWS Systems Manager Associations, um bei der Inventarisierung von Softwareplattformen und Anwendungen innerhalb eines Unternehmens zu helfen. AWS Systems Manager weist Ihren verwalteten Instances einen Konfigurationsstatus zu und ermöglicht es Ihnen, Basiswerte für Betriebssystem-Patch-Levels, Softwareinstallationen, Anwendungskonfigurationen und andere Details zu Ihrer Umgebung festzulegen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen zu
CM-2	Die Organisation entwickelt, dokumentiert und verwaltet unter Konfigurationskontrolle eine aktuelle Basiskonfiguration des Informationssystems.	ec2-stopped-instance	Aktivieren Sie diese Regel, um bei der Basiskonfiguration von Amazon Elastic Compute Cloud (Amazon EC2) - Instances zu helfen, indem Sie überprüfen, ob EC2 Amazon-Instances gemäß den Standards Ihrer Organisation für mehr als die zulässige Anzahl von Tagen gestoppt wurden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen zu
CM-2	Die Organisation entwickelt, dokumentiert und verwaltet unter Konfigurationskontrolle eine aktuelle Basiskonfiguration des Informationssystems.	ec2- volume-inuse-check	Diese Regel stellt sicher, dass Amazon Elastic Block Store-Volumes, die an Amazon Elastic Compute Cloud (Amazon EC2) - Instances angehängt sind, zum Löschen markiert werden, wenn eine Instance beendet wird. Wenn ein Amazon-EBS-Volume nicht gelöscht wird, wenn die Instance, an die es angehängt ist, beendet wird, kann dies gegen das Konzept der geringsten Funktionalität verstoßen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen zu
CM-2	Die Organisation entwickelt, dokumentiert und verwaltet unter Konfigurationskontrolle eine aktuelle Basiskonfiguration des Informationssystems.	elb-deletion-protection-enabled	Diese Regel sorgt dafür, dass der Löschschutz für Elastic Load Balancing aktiviert ist. Verwenden Sie diese Funktion, um zu verhindern, dass Ihr Load Balancer versehentlich oder böswillig gelöscht wird, was zum Verlust der Verfügbarkeit Ihrer Anwendungen führen kann.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen zu
CM-2	Die Organisation entwickelt, dokumentiert und verwaltet unter Konfigurationskontrolle eine aktuelle Basiskonfiguration des Informationssystems.	restricted-common-ports	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass gemeinsame Ports für Amazon Elastic Compute Cloud (Amazon EC2) -Sicherheitsgruppen eingeschränkt sind. Wenn der Zugriff auf Ports nicht auf vertrauenswürdige Quellen beschränkt wird, kann dies zu Angriffen auf die Verfügbarkeit, Integrität und Vertraulichkeit von Systemen führen. Mit dieser Regel können Sie optional die Parameter blockedPort1–blockedPort5 festlegen (Standardkonfigurationen: 20, 21, 3389, 3306, 4333). Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen zu
CM-2	Die Organisation entwickelt, dokumentiert und verwaltet unter Konfigurationskontrolle eine aktuelle Basiskonfiguration des Informationssystems.	cloudtrail-security-trail-enabled	Diese Regel trägt dazu bei, die Verwendung der AWS empfohlenen bewährten Sicherheitsmethoden für sicherzustellen AWS CloudTrail, indem geprüft wird, ob mehrere Einstellungen aktiviert sind. Dazu gehören die Verwendung von Protokollverschlüsselung, Protokollvalidierung und Aktivierung AWS CloudTrail in mehreren Regionen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen zu
CM-7(a)	Die Organisation: a. Konfiguriert das Informationssystem auf eine Weise, dass nur wesentliche Funktionen bereitgestellt werden.	ec2-managerinstance-managed-by-systems	Eine Bestandsaufnahme der Softwareplattformen und Anwendungen innerhalb des Unternehmens ist möglich, indem Amazon Elastic Compute Cloud (Amazon EC2) - Instances mit AWS Systems Manager verwaltet werden. Verwenden Sie AWS Systems Manager, um detaillierte Systemkonfigurationen, Betriebssystem-Patch-Levels, Namen und Typ der Dienste, Softwareinstallationen, Anwendungsname, Herausgeber und Version sowie andere Details zu Ihrer Umgebung bereitzustellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen zu
CM-7(a)	Die Organisation: a. Konfiguriert das Informationssystem auf eine Weise, dass nur wesentliche Funktionen bereitgestellt werden.	ec2-check managedinstance-association-compliance-status	Verwenden Sie AWS Systems Manager Associations, um bei der Inventarisierung von Softwareplattformen und Anwendungen innerhalb eines Unternehmens zu helfen. AWS Systems Manager weist Ihren verwalteten Instances einen Konfigurationsstatus zu und ermöglicht es Ihnen, Basiswerte für Betriebssystem-Patch-Levels, Softwareinstallationen, Anwendungskonfigurationen und andere Details zu Ihrer Umgebung festzulegen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen zu
CM-8(1)	Die Organisation aktualisiert das Inventar der Informationssystemkomponenten als integralen Bestandteil der Installation und Demontage von Komponenten sowie der Aktualisierung von Informationssystemen.	ec2-managed-instance-managed-by-systems	Eine Bestandsaufnahme der Softwareplattformen und Anwendungen innerhalb des Unternehmens ist möglich, indem Amazon Elastic Compute Cloud (Amazon EC2) - Instances mit AWS Systems Manager verwaltet werden. Verwenden Sie AWS Systems Manager, um detaillierte Systemkonfigurationen, Betriebssystem-Patch-Levels, Namen und Typ der Dienste, Softwareinstallationen, Anwendungsname, Herausgeber und Version sowie andere Details zu Ihrer Umgebung bereitzustellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen zu
CM-8(3)(a)	Die Organisation: a. Setzt automatische Mechanismen ein [Zuordnung: vom Unternehmen festgelegte Häufigkeit], um das Vorhandensein nicht autorisierter Hardware-, Software- und Firmware-Komponenten im Informationssystem zu erkennen	ec2-manager instance-managed-by-systems	Eine Bestandsaufnahme der Softwareplattformen und Anwendungen innerhalb des Unternehmens ist möglich, indem Amazon Elastic Compute Cloud (Amazon EC2) - Instances mit AWS Systems Manager verwaltet werden. Verwenden Sie AWS Systems Manager, um detaillierte Systemkonfigurationen, Betriebssystem-Patch-Levels, Namen und Typ der Dienste, Softwareinstallationen, Anwendungsname, Herausgeber und Version sowie andere Details zu Ihrer Umgebung bereitzustellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen zu
CM-8(3)(a)	Die Organisation: a. Setzt automatische Mechanismen ein [Zuordnung: vom Unternehmen festgelegte Häufigkeit], um das Vorhandensein nicht autorisierter Hardware-, Software- und Firmware-Komponenten im Informationssystem zu erkennen	ec2-check managedinstance-association-compliance-status	Verwenden Sie AWS Systems Manager Associations, um bei der Inventarisierung von Softwareplattformen und Anwendungen innerhalb eines Unternehmens zu helfen. AWS Systems Manager weist Ihren verwalteten Instances einen Konfigurationsstatus zu und ermöglicht es Ihnen, Basiswerte für Betriebssystem-Patch-Levels, Softwareinstallationen, Anwendungskonfigurationen und andere Details zu Ihrer Umgebung festzulegen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen zu
CM-8(3)(a)	Die Organisation: a. Setzt automatische Mechanismen ein [Zuordnung: vom Unternehmen festgelegte Häufigkeit], um das Vorhandensein nicht autorisierter Hardware-, Software- und Firmware-Komponenten im Informationssystem zu erkennen	ec2-prüfen managedinstance-patch-compliance-status	Aktivieren Sie diese Regel, um bei der Identifizierung und Dokumentation von Sicherheitslücken in Amazon Elastic Compute Cloud (Amazon EC2) zu helfen. Die Regel prüft, ob die EC2 Amazon-Instance die Patch-Konformität im AWS Systems Manager gemäß den Richtlinien und Verfahren Ihrer Organisation einhält.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen zu
CP-9(b)	Die Organisation: b. Führt Backups der im Informationssystem enthaltenen Informationen auf Systemebene durch [Zuordnung: von der Organisation festgelegte Häufigkeit, die mit den Zielen für die Wiederherstellungszeit und den Wiederherstellungspunkt vereinbar ist].	db-instance-backup-enabled	Die Sicherungsfunktion von Amazon RDS erstellt Sicherungen Ihrer Datenbanken und Transaktionsprotokolle. Amazon RDS erstellt einen Snapshot für das Speichervolume Ihrer DB-Instance, sodass die gesamte DB-Instance gesichert wird. Sie können im System spezifische Aufbewahrungsfristen festlegen, um Ihre Ausfallsicherheitsanforderungen zu erfüllen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen zu
CP-9(b)	Die Organisation: b. Führt Backups der im Informationssystem enthaltenen Informationen auf Systemebene durch [Zuordnung: von der Organisation festgelegte Häufigkeit, die mit den Zielen für die Wiederherstellungszeit und den Wiederherstellungspunkt vereinbar ist].	dynamodb-pitr-enabled	Aktivieren Sie diese Regel, um zu überprüfen, ob die Informationen gesichert wurden. Es verwaltet auch die Backups, indem es sicherstellt, dass die point-in-time Wiederherstellung in Amazon DynamoDB aktiviert ist. Bei der Wiederherstellung werden fortlaufende Backups Ihrer Tabelle für die letzten 35 Tage gespeichert.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen zu
CP-9(b)	Die Organisation: b. Führt Backups der im Informationssystem enthaltenen Informationen auf Systemebene durch [Zuordnung: von der Organisation festgelegte Häufigkeit, die mit den Zielen für die Wiederherstellungszeit und den Wiederherstellungspunkt vereinbar ist].	elasticache-redis-cluster-automatic-Backup-Prüfung	Wenn automatische Backups aktiviert sind, ElastiCache erstellt Amazon täglich ein Backup des Clusters. Die Sicherung kann für eine von Ihrer Organisation festgelegte Anzahl von Tagen aufbewahrt werden. Automatische Backups schützen vor Datenverlust. Bei einem Ausfall können Sie einen neuen Cluster erstellen, der Ihre Daten aus dem aktuellen Backup wiederherstellt.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen zu
CP-9(b)	Die Organisation: b. Führt Backups der im Informationssystem enthaltenen Informationen auf Systemebene durch [Zuordnung: von der Organisation festgelegte Häufigkeit, die mit den Zielen für die Wiederherstellungszeit und den Wiederherstellungspunkt vereinbar ist].	s-3 bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) unterstützt die Aufrechterhaltung einer angemessenen Kapazität und Verfügbarkeit. CRR ermöglicht das automatische, asynchrone Kopieren von Objekten in Amazon-S3-Buckets, um die Datenverfügbarkeit sicherzustellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen zu
CP-9(b)	Die Organisation: b. Führt Backups der im Informationssystem enthaltenen Informationen auf Systemebene durch [Zuordnung: von der Organisation festgelegte Häufigkeit, die mit den Zielen für die Wiederherstellungszeit und den Wiederherstellungspunkt vereinbar ist].	dynamodb-in-backup-plan	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon DynamoDB-Tabellen Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen zu
CP-9(b)	Die Organisation: b. Führt Backups der im Informationssystem enthaltenen Informationen auf Systemebene durch [Zuordnung: von der Organisation festgelegte Häufigkeit, die mit den Zielen für die Wiederherstellungszeit und den Wiederherstellungspunkt vereinbar ist].	ebs-in-backup-plan	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon Elastic Block Store (Amazon EBS) -Volumes Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihre Backup-Verwaltung und ermöglicht es Ihnen, Ihre geschäftlichen und behördlichen Anforderungen bezüglich Backups zu erfüllen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen zu
CP-9(b)	Die Organisation: b. Führt Backups der im Informationssystem enthaltenen Informationen auf Systemebene durch [Zuordnung: von der Organisation festgelegte Häufigkeit, die mit den Zielen für die Wiederherstellungszeit und den Wiederherstellungspunkt vereinbar ist].	efs-in-backup-plan	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon Elastic File System (Amazon EFS) -Dateisysteme Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen zu
CP-9(b)	Die Organisation: b. Führt Backups der im Informationssystem enthaltenen Informationen auf Systemebene durch [Zuordnung: von der Organisation festgelegte Häufigkeit, die mit den Zielen für die Wiederherstellungszeit und den Wiederherstellungspunkt vereinbar ist].	rds-in-backup-plan	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon Relational Database Service (Amazon RDS) -Instances Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen zu
CP-10	Die Organisation sorgt dafür, dass das Informationssystem nach einer Unterbrechung, einer Beeinträchtigung oder einem Ausfall wiederhergestellt und wieder in einen bekannten Zustand versetzt wird.	dynamodb-autoscaling-enabled	Amazon DynamoDB Auto Scaling verwendet den AWS Application Auto Scaling-Service, um die bereitgestellte Durchsatzkapazität so anzupassen, dass sie automatisch auf tatsächliche Verkehrsmuster reagiert. Auf diese Weise kann eine Tabelle oder ein globaler sekundärer Index die bereitgestellte Lese-/Schreibkapazität erhöhen, um plötzliche Erhöhungen des Datenverkehrs ohne Drosselung zu bewältigen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen zu
CP-10	Die Organisation sorgt dafür, dass das Informationssystem nach einer Unterbrechung, einer Beeinträchtigung oder einem Ausfall wiederhergestellt und wieder in einen bekannten Zustand versetzt wird.	elb-deletion-protection-enabled	Diese Regel sorgt dafür, dass der Löschschutz für Elastic Load Balancing aktiviert ist. Verwenden Sie diese Funktion, um zu verhindern, dass Ihr Load Balancer versehentlich oder böswillig gelöscht wird, was zum Verlust der Verfügbarkeit Ihrer Anwendungen führen kann.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen zu
CP-10	Die Organisation sorgt dafür, dass das Informationssystem nach einer Unterbrechung, einer Beeinträchtigung oder einem Ausfall wiederhergestellt und wieder in einen bekannten Zustand versetzt wird.	rds-multi-az-support	Die Multi-AZ-Unterstützung in Amazon Relational Database Service (Amazon RDS) bietet eine verbesserte Verfügbarkeit und Beständigkeit von Datenbank-Instances. Wenn Sie eine Multi-AZ-Datenbank-Instance bereitstellen, erstellt Amazon RDS automatisch eine primäre Datenbank-Instance und repliziert die Daten synchron auf eine Standby-Instance in einer anderen Availability Zone. Jede Availability Zone läuft auf einer eigenen, physisch getrennten, unabhängigen Infrastruktur und ist auf eine hohe Verfügbarkeit ausgelegt. Im Falle eines Infrastrukturausfalls führt Amazon RDS einen automatis

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen zu
			chen Failover zum Standby-Modus durch, sodass Sie den Datenbankbetrieb wieder aufnehmen können, sobald der Failover abgeschlo ssen ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen zu
CP-10	Die Organisation sorgt dafür, dass das Informationssystem nach einer Unterbrechung, einer Beeinträchtigung oder einem Ausfall wiederhergestellt und wieder in einen bekannten Zustand versetzt wird.	rds-cluster-multi-az-aktiviert	Die Multi-AZ-Unterstützung in Amazon Relational Database Service (Amazon RDS) bietet eine verbesserte Verfügbarkeit und Beständigkeit von Datenbank-Instances. Wenn Sie eine Multi-AZ-Datenbank-Instance bereitstellen, erstellt Amazon RDS automatisch eine primäre Datenbank-Instance und repliziert die Daten synchron auf eine Standby-Instance in einer anderen Availability Zone. Jede Availability Zone läuft auf einer eigenen, physisch getrennten, unabhängigen Infrastruktur und ist auf eine hohe Verfügbarkeit ausgelegt. Im Falle eines Infrastrukturausfalls führt Amazon RDS einen automatis

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen zu
			chen Failover zum Standby-Modus durch, sodass Sie den Datenbankbetrieb wieder aufnehmen können, sobald der Failover abgeschlo ssen ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen zu
CP-10	Die Organisation sorgt dafür, dass das Informationssystem nach einer Unterbrechung, einer Beeinträchtigung oder einem Ausfall wiederhergestellt und wieder in einen bekannten Zustand versetzt wird.	s3- bucket-versioning-enabled	Die Versionsverwaltung von Amazon Simple Storage Service (Amazon S3)-Buckets hilft dabei, mehrere Varianten eines Objekts im selben Amazon-S3-Bucket zu speichern. Verwenden Sie die Versionsverwaltung, um sämtliche Versionen aller Objekte in Ihrem Amazon-S3-Bucket zu speichern, abzurufen oder wiederherzustellen. Mit der Versionsverwaltung können Sie Versionen sowohl nach unbeabsichtigten Benutzeraktionen als auch nach Anwendungsfehlern problemlos wiederherstellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen zu
CP-10	Die Organisation sorgt dafür, dass das Informationssystem nach einer Unterbrechung, einer Beeinträchtigung oder einem Ausfall wiederhergestellt und wieder in einen bekannten Zustand versetzt wird.	vpc-vpn-2-tunnels-up	Redundante Site-to-Site VPN-Tunnel können implementiert werden, um die Anforderungen an die Ausfallsicherheit zu erfüllen. Es verwendet zwei Tunnel, um die Konnektivität sicherzustellen, falls eine der Site-to-Site VPN-Verbindungen nicht verfügbar ist. Um sich vor einem Verbindungsverlust zu schützen, können Sie für den Fall, dass Ihr Kunden-Gateway nicht verfügbar ist, eine zweite Site-to-Site VPN-Verbindung zu Ihrer Amazon Virtual Private Cloud (Amazon VPC) und Ihrem Virtual Private Gateway einrichten, indem Sie ein zweites Kunden-Gateway verwenden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen zu
CP-10	Die Organisation sorgt dafür, dass das Informationssystem nach einer Unterbrechung, einer Beeinträchtigung oder einem Ausfall wiederhergestellt und wieder in einen bekannten Zustand versetzt wird.	db-instance-backup-enabled	Die Sicherungsfunktion von Amazon RDS erstellt Sicherungen Ihrer Datenbanken und Transaktionsprotokolle. Amazon RDS erstellt einen Snapshot für das Speichervolume Ihrer DB-Instance, sodass die gesamte DB-Instance gesichert wird. Sie können im System spezifische Aufbewahrungsfristen festlegen, um Ihre Ausfallsicherheitsanforderungen zu erfüllen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen zu
CP-10	Die Organisation sorgt dafür, dass das Informationssystem nach einer Unterbrechung, einer Beeinträchtigung oder einem Ausfall wiederhergestellt und wieder in einen bekannten Zustand versetzt wird.	dynamodb-pitr-enabled	Aktivieren Sie diese Regel, um zu überprüfen, ob die Informationen gesichert wurden. Es verwaltet auch die Backups, indem es sicherstellt, dass die point-in-time Wiederherstellung in Amazon DynamoDB aktiviert ist. Bei der Wiederherstellung werden fortlaufende Backups Ihrer Tabelle für die letzten 35 Tage gespeichert.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen zu
CP-10	Die Organisation sorgt dafür, dass das Informationssystem nach einer Unterbrechung, einer Beeinträchtigung oder einem Ausfall wiederhergestellt und wieder in einen bekannten Zustand versetzt wird.	elasticache-redis-cluster-automatic-Backup-Prüfung	Wenn automatische Backups aktiviert sind, ElastiCache erstellt Amazon täglich ein Backup des Clusters. Die Sicherung kann für eine von Ihrer Organisation festgelegte Anzahl von Tagen aufbewahrt werden. Automatische Backups schützen vor Datenverlust. Bei einem Ausfall können Sie einen neuen Cluster erstellen, der Ihre Daten aus dem aktuellen Backup wiederherstellt.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen zu
CP-10	Die Organisation sorgt dafür, dass das Informationssystem nach einer Unterbrechung, einer Beeinträchtigung oder einem Ausfall wiederhergestellt und wieder in einen bekannten Zustand versetzt wird.	s-3 bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) unterstützt die Aufrechterhaltung einer angemessenen Kapazität und Verfügbarkeit. CRR ermöglicht das automatische, asynchrone Kopieren von Objekten in Amazon-S3-Buckets, um die Datenverfügbarkeit sicherzustellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen zu
CP-10	Die Organisation sorgt dafür, dass das Informationssystem nach einer Unterbrechung, einer Beeinträchtigung oder einem Ausfall wiederhergestellt und wieder in einen bekannten Zustand versetzt wird.	dynamodb-in-backup-plan	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon DynamoDB-Tabellen Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen zu
CP-10	Die Organisation sorgt dafür, dass das Informationssystem nach einer Unterbrechung, einer Beeinträchtigung oder einem Ausfall wiederhergestellt und wieder in einen bekannten Zustand versetzt wird.	ebs-in-backup-plan	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon Elastic Block Store (Amazon EBS) -Volumes Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihre Backup-Verwaltung und ermöglicht es Ihnen, Ihre geschäftlichen und behördlichen Anforderungen bezüglich Backups zu erfüllen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen zu
CP-10	Die Organisation sorgt dafür, dass das Informationssystem nach einer Unterbrechung, einer Beeinträchtigung oder einem Ausfall wiederhergestellt und wieder in einen bekannten Zustand versetzt wird.	efs-in-backup-plan	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon Elastic File System (Amazon EFS) -Dateisysteme Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen zu
CP-10	Die Organisation sorgt dafür, dass das Informationssystem nach einer Unterbrechung, einer Beeinträchtigung oder einem Ausfall wiederhergestellt und wieder in einen bekannten Zustand versetzt wird.	elb-cross-zone-load-Balancing aktiviert	Aktivieren Sie zonenübergreifendes Load Balancing für Ihre Elastic Load Balancer (ELBs), um eine angemessene Kapazität und Verfügbarkeit aufrechtzuerhalten. Zonenübergreifendes Load Balancing reduziert die Notwendigkeit, die gleiche Anzahl von Instances in jeder aktivierten Availability Zone aufrechtzuerhalten. Es verbessert auch die Fähigkeit Ihrer Anwendung, den Verlust einer oder mehrerer Instances zu bewältigen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen zu
CP-10	Die Organisation sorgt dafür, dass das Informationssystem nach einer Unterbrechung, einer Beeinträchtigung oder einem Ausfall wiederhergestellt und wieder in einen bekannten Zustand versetzt wird.	rds-in-backup-plan	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon Relational Database Service (Amazon RDS) -Instances Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen zu
IA-2	Das Informati onssystem nimmt eine eindeutige Identifizierung und Authentifizierung der Benutzer (oder Prozesse, die im Namen von Benutzern der Organisation handeln) vor.	iam-password-policy	Die Identitäten und Anmeldeinformation en werden auf der Grundlage einer organisatorischen IAM-Passwortrichtlinie ausgestellt, verwaltet und verifiziert. Sie erfüllen oder übertreff en die Anforderungen von NIST SP 800-63 und dem Benchmark der Centers for Internet Security (CIS) AWS Foundatio ns in Bezug auf die Passwortstärke. Mit dieser Regel können Sie optional RequireUppercaseCh aracters (Wert für AWS grundlegende Sicherheitsbewährt e Methoden: wahr), RequireLowercaseCh aracters (Wert für bewährte Methoden für AWS grund legende Sicherhei t: wahr), RequireSy mbols (Wert für bewährte Methoden für AWS grund

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen zu
			legende Sicherhei t: wahr), RequireNu mbers (Wert für bewährte Methoden für AWS grund legende Sicherheit: wahr), MinimumPa sswordLength (Wert für bewährte Methoden für AWS grundlegende Sicherheit: 14), PasswordReusePreve ntion (Wert für bewährte Methoden für AWS grundlege nde Sicherheit: 24) und MaxPasswo rdAge (Wert für bewährte Methoden für AWS grundlege nde Sicherheit: 90) für Ihr IAM festlegen Kennwortrichtlinie. Die tatsächlichen Werte müssen den Richtlini en Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen zu
IA-2(1)(11)	(1) Das Informationssystem implementiert eine Multifaktor-Authentifizierung für den Netzwerkzugriff auf privilegierte Konten. (11) Das Informationssystem implementiert eine mehrstufige Authentifizierung für den Fernzugriff auf privilegierte und nichtprivilegierte Konten, so dass einer der Faktoren von einem Gerät bereitgestellt wird, das von dem System, das den Zugriff gewährt, getrennt ist, und das Gerät erfüllt [Zuordnung: von der Organisation festgelegte Anforderungen an die Stärke des Mechanismus].	root-account-hardware-mfa-aktiviert	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Hardware-MFA für den Root-Benutzer aktiviert ist. Der Stammbenutzer ist der AWS-Konto-Benutzer mit den meisten Berechtigungen. MFA sorgt für eine weitere Schutzebene zusätzlich zu den Anmeldeinformationen. Indem Sie MFA für den Root-Benutzer vorschreiben, können Sie die Anzahl AWS-Konten kompromittierter Benutzer reduzieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen zu
IA-2(1)(11)	(1) Das Informationssystem implementiert eine Multifaktor-Authentifizierung für den Netzwerkzugriff auf privilegierte Konten. (11) Das Informationssystem implementiert eine mehrstufige Authentifizierung für den Fernzugriff auf privilegierte und nichtprivilegierte Konten, so dass einer der Faktoren von einem Gerät bereitgestellt wird, das von dem System, das den Zugriff gewährt, getrennt ist, und das Gerät erfüllt [Zuordnung: von der Organisation festgelegte Anforderungen an die Stärke des Mechanismus].	root-account-mfa-enabled	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass MFA für den Root-Benutzer aktiviert ist. Der Stammbenutzer ist der AWS-Konto-Benutzer mit den meisten Berechtigungen. MFA bietet eine weitere Schutzebene zusätzlich zum Benutzernamen und Passwort. Indem Sie MFA für den Root-Benutzer vorschreiben, können Sie die Anzahl AWS-Konten kompromittierter Benutzer reduzieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen zu
IA-2(1)(2)(11)	(1) Das Informationssystem implementiert eine Multifaktor-Authentifizierung für den Netzwerkzugriff auf privilegierte Konten. (1) Das Informationssystem implementiert eine Multifaktor-Authentifizierung für den Netzwerkzugriff auf nicht privilegierte Konten. (11) Das Informationssystem implementiert eine mehrstufige Authentifizierung für den Fernzugriff auf privilegierte und nichtprivilegierte Konten, so dass einer der Faktoren von einem Gerät bereitgestellt wird, das von dem System, das den Zugriff gewährt, getrennt ist, und das Gerät erfüllt [Zuordnung: von der Organisation festgelegte Anforderu	mfa-enabled-for-iam-Konsolenzugriff	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass MFA für alle AWS Identity and Access Management (IAM) -Benutzer aktiviert ist, die über ein Konsolenkennwort verfügen. MFA sorgt für eine weitere Schutzebene zusätzlich zu den Anmeldeinformationen. Indem Sie MFA für Benutzer vorschreiben, können Sie Fälle kompromittierter Konten reduzieren und verhindern, dass unbefugte Benutzer auf vertrauliche Daten zugreifen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen zu
	ngen an die Stärke des Mechanismus].		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen zu
IA-2(1)(2)(11)	(1) Das Informationssystem implementiert eine Multifaktor-Authentifizierung für den Netzwerkzugriff auf privilegierte Konten. (1) Das Informationssystem implementiert eine Multifaktor-Authentifizierung für den Netzwerkzugriff auf nicht privilegierte Konten. (11) Das Informationssystem implementiert eine mehrstufige Authentifizierung für den Fernzugriff auf privilegierte und nichtprivilegierte Konten, so dass einer der Faktoren von einem Gerät bereitgestellt wird, das von dem System, das den Zugriff gewährt, getrennt ist, und das Gerät erfüllt [Zuordnung: von der Organisation festgelegte Anforderu	iam-user-mfa-enabled	Aktivieren Sie diese Regel, um den Zugriff auf Ressourcen in der AWS -Cloud einzuschränken. Diese Regel stellt sicher, dass die Multi-Faktor-Authentifizierung (MFA) für alle Benutzer aktiviert ist. MFA bietet eine weitere Schutzebene zusätzlich zum Benutzernamen und Passwort. Reduzieren Sie Fälle von kompromittierten Konten, indem Sie MFA für Benutzer vorschreiben.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen zu
	ngen an die Stärke des Mechanismus].		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen zu
IA-5(1)(a)(d)(e)	Das Informati onssystem ergreift für die passwortgestützte Authentifizierung folgende Maßnahmen : a. Es erzwingt eine Mindestkomplexität von [Zuweisung: vom Unternehm en festgelegte Anforderungen an Groß- und Kleinschr eibung, Zeichenan zahl, Kombinati on aus Groß- und Kleinbuchstaben, Zahlen und Sonderzei chen, einschlie ßlich Mindestan forderungen für jeden Typ]; d. Es erzwingt die minimale und maximale Gültigkeitsdauer von Passwörtern von [Zuweisung: von der Organisat ion festgelegte Frist für die minimale und maximale Gültigkeitsdauer]; e. Verbietet die Wiederverwendung	iam-password-policy	Die Identitäten und Anmeldeinformation en werden auf der Grundlage einer organisatorischen IAM-Passwortrichtlinie ausgestellt, verwaltet und verifiziert. Sie erfüllen oder übertreff en die Anforderungen von NIST SP 800-63 und dem Benchmark der Centers for Internet Security (CIS) AWS Foundatio ns in Bezug auf die Passwortstärke. Mit dieser Regel können Sie optional RequireUppercaseCh aracters (Wert für AWS grundlegende Sicherheitsbewährt e Methoden: wahr), RequireLowercaseCh aracters (Wert für bewährte Methoden für AWS grund legende Sicherhei t: wahr), RequireSy mbols (Wert für bewährte Methoden für AWS grund

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen zu
	von Passwörtern für [Zuweisung: von der Organisation festgelegte Anzahl] Generationen.		legende Sicherhei t: wahr), RequireNu mbers (Wert für bewährte Methoden für AWS grund legende Sicherheit: wahr), MinimumPa sswordLength (Wert für bewährte Methoden für AWS grundlegende Sicherheit: 14), PasswordReusePreve ntion (Wert für bewährte Methoden für AWS grundlege nde Sicherheit: 24) und MaxPasswo rdAge (Wert für bewährte Methoden für AWS grundlege nde Sicherheit: 90) für Ihr IAM festlegen Kennwortrichtlinie. Die tatsächlichen Werte müssen den Richtlini en Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen zu
IA-5(4)	Die Organisation verwendet automatisierte Tools, um festzustellen, ob Passwortauthentifikatoren stark genug sind, um [Zuweisung: von der Organisation definierte Anforderungen] zu erfüllen.	iam-password-policy	Die Identitäten und Anmeldeinformationen werden auf der Grundlage einer organisatorischen IAM-Passwortrichtlinie ausgestellt, verwaltet und verifiziert. Sie erfüllen oder übertreffen die Anforderungen von NIST SP 800-63 und dem Benchmark der Centers for Internet Security (CIS) AWS Foundations in Bezug auf die Passwortstärke. Mit dieser Regel können Sie optional RequireUppercaseCharacters (Wert für AWS grundlegende Sicherheitsbewährte Methoden: wahr), RequireLowercaseCharacters (Wert für bewährte Methoden für AWS grundlegende Sicherheit: wahr), RequireSymbols (Wert für bewährte Methoden für AWS grund

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen zu
			legende Sicherhei t: wahr), RequireNu mbers (Wert für bewährte Methoden für AWS grund legende Sicherheit: wahr), MinimumPa sswordLength (Wert für bewährte Methoden für AWS grundlegende Sicherheit: 14), PasswordReusePreve ntion (Wert für bewährte Methoden für AWS grundlege nde Sicherheit: 24) und MaxPasswo rdAge (Wert für bewährte Methoden für AWS grundlege nde Sicherheit: 90) für Ihr IAM festlegen Kennwortrichtlinie. Die tatsächlichen Werte müssen den Richtlini en Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen zu
IA-5(7)	Die Organisation stellt sicher, dass unverschlüsselte statische Authentifikatoren nicht in Anwendungen oder Zugriffsskripts eingebettet oder in Funktionsschlüsseln gespeichert werden.	codebuild-project-envvar-awscred-überprüfen	Stellen Sie sicher, dass die Anmeldeinformationen AWS_ACCESS_KEY_ID AWS_SECRET_ACCESS_KEY nicht in AWS Codebuild-Projektumgebungen vorhanden sind. Speichern Sie diese Variablen nicht als Klartext. Das Speichern dieser Variablen als Klartext bewirkt eine unbeabsichtigte Offenlegung von Daten sowie unberechtigte Zugriffe.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen zu
IR-4(1)	Die Organisation setzt automatisierte Mechanismen ein, um die Bearbeitung von Sicherheitsvorfällen zu unterstützen.	cloudwatch-alarm-action-check	Amazon CloudWatch alarmiert, wenn eine Metrik den Schwellenwert für eine bestimmte Anzahl von Bewertungszeiträumen überschreitet. Der Alarm führt eine oder mehrere Aktionen durch, die vom Wert der Metrik oder des Ausdrucks im Vergleich zu einem Schwellenwert in einer Reihe von Zeiträumen abhängt. Diese Regel erfordert einen Wert für alarmActionRequired (Config Default: True), insufficientDataAction Required (Config Default: True), okActionRequired (Config Default: False). Der tatsächliche Wert muss die Alarmaktionen für Ihre Umgebung widerspiegeln.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen zu
IR-4(1)	Die Organisation setzt automatisierte Mechanismen ein, um die Bearbeitung von Sicherheitsvorfällen zu unterstützen.	guardduty-non-archived-findings	Amazon GuardDuty hilft Ihnen dabei, die Auswirkungen eines Vorfalls zu verstehen, indem es die Ergebnisse nach Schweregrad klassifiziert: niedrig, mittel und hoch. Diese Klassifizierungen können Sie zur Festlegung von entsprechenden Strategien und Prioritäten zur Behebung solcher Vorfälle verwenden. Mit dieser Regel können Sie optional daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7) und daysHighSev (Config Default: 1) für nicht archivierte Ergebnisse festlegen, wie es die Richtlinien Ihrer Organisation erfordern.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen zu
IR-6(1)	Die Organisation setzt automatisierte Mechanismen ein, um die Meldung von Sicherheitsvorfällen zu unterstützen.	guardduty-non-archived-findings	Amazon GuardDuty hilft Ihnen dabei, die Auswirkungen eines Vorfalls zu verstehen, indem es die Ergebnisse nach Schweregrad klassifiziert: niedrig, mittel und hoch. Diese Klassifizierungen können Sie zur Festlegung von entsprechenden Strategien und Prioritäten zur Behebung solcher Vorfälle verwenden. Mit dieser Regel können Sie optional daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7) und daysHighSev (Config Default: 1) für nicht archivierte Ergebnisse festlegen, wie es die Richtlinien Ihrer Organisation erfordern.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen zu
IR-7(1)	Die Organisation setzt automatisierte Mechanismen ein, um die Verfügbarkeit von Informationen und Unterstützung im Zusammenhang mit der Reaktion auf Vorfälle zu erhöhen.	guardduty-non-archived-findings	Amazon GuardDuty hilft Ihnen dabei, die Auswirkungen eines Vorfalls zu verstehen, indem es die Ergebnisse nach Schweregrad klassifiziert: niedrig, mittel und hoch. Diese Klassifizierungen können Sie zur Festlegung von entsprechenden Strategien und Prioritäten zur Behebung solcher Vorfälle verwenden. Mit dieser Regel können Sie optional daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7) und daysHighSev (Config Default: 1) für nicht archivierte Ergebnisse festlegen, wie es die Richtlinien Ihrer Organisation erfordern.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen zu
RA-5	Die Organisat ion: a. Sucht nach Sicherheitslücken im Informationssystem und in gehostete n Anwendungen [Zuordnung: Von der Organisation festgelegte Häufigkei t and/or randomly in accordance with organization-defin ed process] and when new vulnerabi lities potentially affecting the system/ applications der Identifizierung und Meldung; b. Wendet Tools und Techniken zum Scannen von Schwachstellen an, die die Interoper abilität zwischen den Tools erleichtern und Teile des Schwachst ellenmanagements automatisieren, indem für folgende Aktivitäten Standards angewendet werden: 1. Aufzählung von Plattformen, Softwaref	guardduty-enabled-centralized	Amazon GuardDuty kann mithilfe von Threat Intellige nce Feeds helfen, potenzielle Cybersich erheitsereignisse zu überwachen und zu erkennen. Dazu gehören Listen mit bösartigen IPs und maschinel len Lernmethoden zur Identifizierung unerwarteter, nicht autorisierter und bösartiger Aktivitäten in Ihrer AWS Cloud-Umgebung.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen zu
	ehlern und ungeeigneten Konfigurationen; 2. Formatierung von Checklisten und Testverfahren; und 3. Messung der Auswirkungen von Schwachstellen; c. Analysiert Scanberichte über Schwachstellen und Ergebnisse von Sicherheitskontrollbewertungen; d. Behebt legitime Schwachstellen [Zuweisung: von der Organisation festgelegte Reaktionszeiten] gemäß einer Risikobewertung der Organisation; und e. Leitet die Informationen aus dem Schwachstellenscan und den Sicherheitskontrollbewertungen an [Zuweisung: von der Organisation ernanntes Personal oder definierte Rollen] weiter, um ähnliche Schwachstellen in anderen Informationssystemen (d. h.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen zu
	Systemschwächen oder -mängel) zu beseitigen.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen zu
RA-5	Die Organisation: a. Sucht nach Sicherheitslücken im Informationssystem und in gehosteten Anwendungen [Zuordnung: Von der Organisation festgelegte Häufigkeit and/or randomly in accordance with organization-defined process] and when new vulnerabilities potentially affecting the system/applications der Identifizierung und Meldung; b. Wendet Tools und Techniken zum Scannen von Schwachstellen an, die die Interoperabilität zwischen den Tools erleichtern und Teile des Schwachstellenmanagements automatisieren, indem für folgende Aktivitäten Standards angewendet werden: 1. Aufzählung von Plattformen, Softwaref	guardduty-non-archived-findings	Amazon GuardDuty hilft Ihnen dabei, die Auswirkungen eines Vorfalls zu verstehen, indem es die Ergebnisse nach Schweregrad klassifiziert: niedrig, mittel und hoch. Diese Klassifizierungen können Sie zur Festlegung von entsprechenden Strategien und Prioritäten zur Behebung solcher Vorfälle verwenden. Mit dieser Regel können Sie optional daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7) und daysHighSev (Config Default: 1) für nicht archivierte Ergebnisse festlegen, wie es die Richtlinien Ihrer Organisation erfordern.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen zu
	ehlern und ungeeigneten Konfigurationen; 2. Formatierung von Checklisten und Testverfahren; und 3. Messung der Auswirkungen von Schwachstellen; c. Analysiert Scanberichte über Schwachstellen und Ergebnisse von Sicherheitskontrollbewertungen; d. Behebt legitime Schwachstellen [Zuweisung: von der Organisation festgelegte Reaktionszeiten] gemäß einer Risikobewertung der Organisation; und e. Leitet die Informationen aus dem Schwachstellenscan und den Sicherheitskontrollbewertungen an [Zuweisung: von der Organisation ernanntes Personal oder definierte Rollen] weiter, um ähnliche Schwachstellen in anderen Informationssystemen (d. h.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen zu
	Systemschwächen oder -mängel) zu beseitigen.		
SA-3(a)	Die Organisation: a. Verwaltet das Informationssystem mithilfe von [Zuweisung: von der Organisation definierter Lebenszyklus der Systementwicklung], dem Überlegungen zur Informationssicherheit zugrunde liegen.	codebuild-project-envvar-awscred-überprüfen	Stellen Sie sicher, dass die Anmeldeinformationen AWS_ACCESS_KEY_ID AWS_SECRET_ACCESS_KEY nicht in AWS Codebuild-Projektumgebungen vorhanden sind. Speichern Sie diese Variablen nicht als Klartext. Das Speichern dieser Variablen als Klartext bewirkt eine unbeabsichtigte Offenlegung von Daten sowie unberechtigte Zugriffe.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen zu
SA-3(a)	Die Organisation: a. Verwaltet das Informationssystem mithilfe von [Zuweisung: von der Organisation definierter Lebenszyklus der Systementwicklung], dem Überlegungen zur Informationssicherheit zugrunde liegen.	ec2-manager instance-managed-by-systems	Eine Bestandsaufnahme der Softwareplattformen und Anwendungen innerhalb des Unternehmens ist möglich, indem Amazon Elastic Compute Cloud (Amazon EC2) - Instances mit AWS Systems Manager verwaltet werden. Verwenden Sie AWS Systems Manager, um detaillierte Systemkonfigurationen, Betriebssystem-Patch-Levels, Namen und Typ der Dienste, Softwareinstallationen, Anwendungsname, Herausgeber und Version sowie andere Details zu Ihrer Umgebung bereitzustellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen zu
SA-3(a)	Die Organisation: a. Verwaltet das Informationssystem mithilfe von [Zuweisung: von der Organisation definierter Lebenszyklus der Systementwicklung], dem Überlegungen zur Informationssicherheit zugrunde liegen.	codebuild-project-source-repo-URL-Prüfung	Stellen Sie sicher, dass die URL des Quell-Repositorys GitHub oder des Bitbucket-Quell-Repositorys keine persönlichen Zugriffstoken oder Anmeldeinformationen in Codebuild-Projektumgebungen enthält. AWS Verwende OAuth anstelle von persönlichen Zugriffstoken oder Anmeldedaten die Autorisierung für den Zugriff auf GitHub Bitbucket-Repositorys.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen zu
SA-10	Die Organisation verlangt von den Entwicklern des Informationssystems, der Systemkomponente oder des Informationssystemservices: a. Durchführung von Konfigurationsmanagement während des Systems, der Komponente oder des Dienstes [Auswahl (eine oder mehrere): Entwurf; Entwicklung; Implementierung; Betrieb]; b. Die Dokumentation, Verwaltung und Kontrolle der Integrität von Änderungen an [Zuweisung: von der Organisation definierte Konfigurationselemente im Rahmen der Konfigurationsverwaltung]; c. Die Implementierung von ausschließlich von der Organisation genehmigten Änderungen	guardduty-enabled-centralized	Amazon GuardDuty kann mithilfe von Threat Intelligence Feeds helfen, potenzielle Cybersicherheitsereignisse zu überwachen und zu erkennen. Dazu gehören Listen mit bösartigen IPs und maschinellen Lernmethoden zur Identifizierung unerwarteter, nicht autorisierter und bösartiger Aktivitäten in Ihrer AWS Cloud-Umgebung.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen zu
	am System, der Komponente oder dem Service; d. Die Dokumentation von genehmigten Änderungen am System, der Komponente oder dem Service sowie der potenziellen Auswirkungen solcher Änderungen auf die Sicherheit; und e. Die Überwachung von Sicherheitslücken und deren Behebung innerhalb des Systems, der Komponente oder des Services und die Meldung der Ergebnisse an [Zuweisung: von der Organisation ernanntes Personal].		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen zu
SA-10	Die Organisation verlangt von den Entwicklern des Informationssystems, der Systemkomponente oder des Informationssystemservices: a. Durchführung von Konfigurationsmanagement während des Systems, der Komponente oder des Dienstes [Auswahl (eine oder mehrere): Entwurf; Entwicklung; Implementierung; Betrieb]; b. Die Dokumentation, Verwaltung und Kontrolle der Integrität von Änderungen an [Zuweisung: von der Organisation definierte Konfigurationselemente im Rahmen der Konfigurationsverwaltung]; c. Die Implementierung von ausschließlich von der Organisation genehmigten Änderungen	guardduty-non-archived-findings	Amazon GuardDuty hilft Ihnen dabei, die Auswirkungen eines Vorfalls zu verstehen, indem es die Ergebnisse nach Schweregrad klassifiziert: niedrig, mittel und hoch. Diese Klassifizierungen können Sie zur Festlegung von entsprechenden Strategien und Prioritäten zur Behebung solcher Vorfälle verwenden. Mit dieser Regel können Sie optional daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7) und daysHighSev (Config Default: 1) für nicht archivierte Ergebnisse festlegen, wie es die Richtlinien Ihrer Organisation erfordern.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen zu
	am System, der Komponente oder dem Service; d. Die Dokumentation von genehmigten Änderungen am System, der Komponente oder dem Service sowie der potenziellen Auswirkungen solcher Änderungen auf die Sicherheit; und e. Die Überwachung von Sicherheitslücken und deren Behebung innerhalb des Systems, der Komponente oder des Services und die Meldung der Ergebnisse an [Zuweisung: von der Organisation ernanntes Personal].		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen zu
SA-10	Die Organisation verlangt von den Entwicklern des Informationssystems, der Systemkomponente oder des Informationssystemservices: a. Durchführung von Konfigurationsmanagement während des Systems, der Komponente oder des Dienstes [Auswahl (eine oder mehrere): Entwurf; Entwicklung; Implementierung; Betrieb]; b. Die Dokumentation, Verwaltung und Kontrolle der Integrität von Änderungen an [Zuweisung: von der Organisation definierte Konfigurationselemente im Rahmen der Konfigurationsverwaltung]; c. Die Implementierung von ausschließlich von der Organisation genehmigten Änderungen	securityhub-enabled	AWS Security Hub hilft bei der Überwachung von unbefugtem Personal, Verbindungen, Geräten und Software. AWS Security Hub aggregiert, organisiert und priorisiert die Sicherheitswarnungen oder Ergebnisse mehrerer Dienste. AWS Einige dieser Dienste sind Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer und AWS Firewall Manager sowie AWS Partnerlösungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen zu
	am System, der Komponente oder dem Service; d. Die Dokumentation von genehmigten Änderungen am System, der Komponente oder dem Service sowie der potenziellen Auswirkungen solcher Änderungen auf die Sicherheit; und e. Die Überwachung von Sicherheitslücken und deren Behebung innerhalb des Systems, der Komponente oder des Services und die Meldung der Ergebnisse an [Zuweisung: von der Organisation ernanntes Personal].		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen zu
SA-10	Die Organisation verlangt von den Entwicklern des Informationssystems, der Systemkomponente oder des Informationssystemservices: a. Durchführung von Konfigurationsmanagement während des Systems, der Komponente oder des Dienstes [Auswahl (eine oder mehrere): Entwurf; Entwicklung; Implementierung; Betrieb]; b. Die Dokumentation, Verwaltung und Kontrolle der Integrität von Änderungen an [Zuweisung: von der Organisation definierte Konfigurationselemente im Rahmen der Konfigurationsverwaltung]; c. Die Implementierung von ausschließlich von der Organisation genehmigten Änderungen	ec2-manager instance-managed-by-systems	Eine Bestandsaufnahme der Softwareplattformen und Anwendungen innerhalb des Unternehmens ist möglich, indem Amazon Elastic Compute Cloud (Amazon EC2) - Instances mit AWS Systems Manager verwaltet werden. Verwenden Sie AWS Systems Manager, um detaillierte Systemkonfigurationen, Betriebssystem-Patch-Levels, Namen und Typ der Dienste, Softwareinstallationen, Anwendungsname, Herausgeber und Version sowie andere Details zu Ihrer Umgebung bereitzustellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen zu
	am System, der Komponente oder dem Service; d. Die Dokumentation von genehmigten Änderungen am System, der Komponente oder dem Service sowie der potenziellen Auswirkungen solcher Änderungen auf die Sicherheit; und e. Die Überwachung von Sicherheitslücken und deren Behebung innerhalb des Systems, der Komponente oder des Services und die Meldung der Ergebnisse an [Zuweisung: von der Organisation ernanntes Personal].		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen zu
SC-2	Das Informati onssystem trennt Benutzerfunktionen (einschließlich Benutzerschnittste llenservices) von den Verwaltungsfunktio nen des Informati onssystems.	iam-group-has-users-überprüfen	AWS Identity and Access Managemen t (IAM) kann Ihnen helfen, die Prinzipien der geringsten Rechte und der Aufgabent rennung mit Zugriffsb erechtigungen und Autorisierungen zu integrieren, indem sichergestellt wird, dass IAM-Gruppen mindestens einen Benutzer haben. Die Einteilung von Benutzern in Gruppen auf der Grundlage der ihnen zugewiese nen Berechtigungen oder ihrer Funktion ist eine Möglichkeit, das Prinzip der geringste n Berechtigung zu implementieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen zu
SC-2	Das Informationssystem trennt Benutzerfunktionen (einschließlich Benutzerschnittstellenservices) von den Verwaltungsfunktionen des Informationssystems.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) kann Ihnen dabei helfen, die Prinzipien der geringsten Rechte und der Aufgabentrennung in Zugriffsberechtigungen und Autorisierungen zu integrieren und so zu verhindern, dass Richtlinien „Effect“: „Allow“ mit „Action“: „*“ anstelle von „Resource“: „*“ enthalten. Wenn Benutzern mehr Rechte eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und der Aufgabentrennung verstoßen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen zu
SC-4	Das Informati onssystem verhinder t die unbefugte und unbeabsichtigte Übertragung von Informationen aus gemeinsam genutzten Systemressourcen.	ec2- volume-inuse-check	Diese Regel stellt sicher, dass Amazon Elastic Block Store-Volumes, die an Amazon Elastic Compute Cloud (Amazon EC2) - Instances angehängt sind, zum Löschen markiert werden, wenn eine Instance beendet wird. Wenn ein Amazon-EB S-Volume nicht gelöscht wird, wenn die Instance, an die es angehängt ist, beendet wird, kann dies gegen das Konzept der geringsten Funktiona lität verstoßen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen zu
SC-5	Das Informationssystem schützt vor den folgenden Arten von Denial-of-Service-Angriffen oder begrenzt deren Auswirkungen: [Zuweisung: von der Organisation definierte Arten von Denial-of-Service-Angriffen oder Verweise auf Quellen für solche Informationen] durch den Einsatz von [Zuweisung: von der Organisation definierte Sicherheitsvorkehrungen].	autoscaling-group-elb-healthcheck-erforderlich	Die Elastic Load Balancer (ELB) - Zustandsprüfungen für Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling Scaling-Gruppen unterstützen die Aufrechterhaltung einer angemessenen Kapazität und Verfügbarkeit. Der Load Balancer sendet regelmäßig Pings, versucht Verbindungen herzustellen oder sendet Anfragen, um den Zustand der EC2 Amazon-Instances in einer Gruppe mit auto-scaling zu testen. Wenn eine Instance nicht zurückmeldet, wird der Traffic an eine neue EC2 Amazon-Instance gesendet.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen zu
SC-5	Das Informationssystem schützt vor den folgenden Arten von Denial-of-Service-Angriffen oder begrenzt deren Auswirkungen: [Zuweisung: von der Organisation definierte Arten von Denial-of-Service-Angriffen oder Verweise auf Quellen für solche Informationen] durch den Einsatz von [Zuweisung: von der Organisation definierte Sicherheitsvorkehrungen].	dynamodb-autoscaling-enabled	Amazon DynamoDB Auto Scaling verwendet den AWS Application Auto Scaling-Service, um die bereitgestellte Durchsatzkapazität so anzupassen, dass sie automatisch auf tatsächliche Verkehrsmuster reagiert. Auf diese Weise kann eine Tabelle oder ein globaler sekundärer Index die bereitgestellte Lese-/Schreibkapazität erhöhen, um plötzliche Erhöhungen des Datenverkehrs ohne Drosselung zu bewältigen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen zu
SC-5	Das Informationssystem schützt vor den folgenden Arten von Denial-of-Service-Angriffen oder begrenzt deren Auswirkungen: [Zuweisung: von der Organisation definierte Arten von Denial-of-Service-Angriffen oder Verweise auf Quellen für solche Informationen] durch den Einsatz von [Zuweisung: von der Organisation definierte Sicherheitsvorkehrungen].	rds-multi-az-support	Die Multi-AZ-Unterstützung in Amazon Relational Database Service (Amazon RDS) bietet eine verbesserte Verfügbarkeit und Beständigkeit von Datenbank-Instances. Wenn Sie eine Multi-AZ-Datenbank-Instance bereitstellen, erstellt Amazon RDS automatisch eine primäre Datenbank-Instance und repliziert die Daten synchron auf eine Standby-Instance in einer anderen Availability Zone. Jede Availability Zone läuft auf einer eigenen, physisch getrennten, unabhängigen Infrastruktur und ist auf eine hohe Verfügbarkeit ausgelegt. Im Falle eines Infrastrukturausfalls führt Amazon RDS einen automatis

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen zu
			chen Failover zum Standby-Modus durch, sodass Sie den Datenbankbetrieb wieder aufnehmen können, sobald der Failover abgeschlo ssen ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen zu
SC-5	Das Informationssystem schützt vor den folgenden Arten von Denial-of-Service-Angriffen oder begrenzt deren Auswirkungen: [Zuweisung: von der Organisation definierte Arten von Denial-of-Service-Angriffen oder Verweise auf Quellen für solche Informationen] durch den Einsatz von [Zuweisung: von der Organisation definierte Sicherheitsvorkehrungen].	rds-cluster-multi-az-aktiviert	Die Multi-AZ-Unterstützung in Amazon Relational Database Service (Amazon RDS) bietet eine verbesserte Verfügbarkeit und Beständigkeit von Datenbank-Instances. Wenn Sie eine Multi-AZ-Datenbank-Instance bereitstellen, erstellt Amazon RDS automatisch eine primäre Datenbank-Instance und repliziert die Daten synchron auf eine Standby-Instance in einer anderen Availability Zone. Jede Availability Zone läuft auf einer eigenen, physisch getrennten, unabhängigen Infrastruktur und ist auf eine hohe Verfügbarkeit ausgelegt. Im Falle eines Infrastrukturausfalls führt Amazon RDS einen automatis

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen zu
			chen Failover zum Standby-Modus durch, sodass Sie den Datenbankbetrieb wieder aufnehmen können, sobald der Failover abgeschlo ssen ist.
SC-5	Das Informati onssystem schützt vor den folgenden Arten von Denial-of -Service-Angriffen oder begrenzt deren Auswirkungen: [Zuweisung: von der Organisation definiert e Arten von Denial-of-Service-Angriffen oder Verweise auf Quellen für solche Informationen] durch den Einsatz von [Zuweisung: von der Organisation definiert e Sicherheitsvorkehr ungen].	s3- bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) unterstützt die Aufrechterhaltung einer angemesse nen Kapazität und Verfügbarkeit. CRR ermöglicht das automatische, asynchrone Kopieren von Objekten in Amazon-S3-Buckets, um die Datenverf ügbarkeit sicherzus tellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen zu
SC-5	Das Informationssystem schützt vor den folgenden Arten von Denial-of-Service-Angriffen oder begrenzt deren Auswirkungen: [Zuweisung: von der Organisation definierte Arten von Denial-of-Service-Angriffen oder Verweise auf Quellen für solche Informationen] durch den Einsatz von [Zuweisung: von der Organisation definierte Sicherheitsvorkehrungen].	elb-cross-zone-load-Balancing aktiviert	Aktivieren Sie zonenübergreifendes Load Balancing für Ihre Elastic Load Balancer (ELBs), um eine angemessene Kapazität und Verfügbarkeit aufrechtzuerhalten. Zonenübergreifendes Load Balancing reduziert die Notwendigkeit, die gleiche Anzahl von Instances in jeder aktivierten Availability Zone aufrechtzuerhalten. Es verbessert auch die Fähigkeit Ihrer Anwendung, den Verlust einer oder mehrerer Instances zu bewältigen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen zu
SC-5	Das Informati onssystem schützt vor den folgenden Arten von Denial-of -Service-Angriffen oder begrenzt deren Auswirkungen: [Zuweisung: von der Organisation definiert e Arten von Denial-of-Service-Angriffen oder Verweise auf Quellen für solche Informationen] durch den Einsatz von [Zuweisung: von der Organisation definiert e Sicherheitsvorkehr ungen].	rds-instance-deletion-protection-aktiviert	Stellen Sie sicher, dass Amazon Relational Database Service (Amazon RDS)-Instances den Löschschutz aktiviert haben. Verwenden Sie den Löschschu tz, um zu verhindern, dass Ihre Amazon-RD S-Instances versehent lich oder böswillig gelöscht werden, was zum Verlust der Verfügbarkeit Ihrer Anwendungen führen kann.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen zu
SC-7	Das Informati onssystem: a. Überwacht und kontrolliert die Kommunikation an der Außengrenze des Systems und an wichtigen internen Grenzen innerhalb des Systems; b. Implementiert Subnetze für öffentlic h zugängliche Systemkomponenten, die [Auswahl: physisch; logisch] von internen Organisat ionsnetzen getrennt sind; und c. Stellt eine Verbindung zu externen Netzwerke n oder Informati onssystemen nur über verwaltete Schnittstellen her, die aus Grenzschu tzgeräten bestehen, die gemäß einer Sicherheitsarchite ktur der Organisation angeordnet sind.	ec2- instance-no-public-ip	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon Elastic Compute Cloud (Amazon EC2) - Instances nicht öffentlich zugänglic h sind. EC2Amazon -Instances können vertrauliche Informati onen enthalten, und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen zu
SC-7	Das Informationssystem: a. Überwacht und kontrolliert die Kommunikation an der Außengrenze des Systems und an wichtigen internen Grenzen innerhalb des Systems; b. Implementiert Subnetze für öffentlich zugängliche Systemkomponenten, die [Auswahl: physisch; logisch] von internen Organisationsnetzen getrennt sind; und c. Stellt eine Verbindung zu externen Netzwerken oder Informationssystemen nur über verwaltete Schnittstellen her, die aus Grenzschutzgeräten bestehen, die gemäß einer Sicherheitsarchitektur der Organisation angeordnet sind.	s-3 bucket-ssl-requests-only	Um Daten während der Übertragung zu schützen, stellen Sie sicher, dass Ihre Amazon Simple Storage Service (Amazon S3)-Buckets Anfragen zur Verwendung von Secure Socket Layer (SSL)-Buckets erfordern. Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen zu
SC-7	Das Informationssystem: a. Überwacht und kontrolliert die Kommunikation an der Außengrenze des Systems und an wichtigen internen Grenzen innerhalb des Systems; b. Implementiert Subnetze für öffentlich zugängliche Systemkomponenten, die [Auswahl: physisch; logisch] von internen Organisationsnetzen getrennt sind; und c. Stellt eine Verbindung zu externen Netzwerken oder Informationssystemen nur über verwaltete Schnittstellen her, die aus Grenzschutzgeräten bestehen, die gemäß einer Sicherheitsarchitektur der Organisation angeordnet sind.	redshift-require-tls-ssl	Stellen Sie sicher, dass Ihre Amazon-Redshift-Cluster eine TLS/SSL-Verschlüsselung erfordern, um eine Verbindung zu SQL-Clients herzustellen. Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen zu
SC-7	Das Informationssystem: a. Überwacht und kontrolliert die Kommunikation an der Außengrenze des Systems und an wichtigen internen Grenzen innerhalb des Systems; b. Implementiert Subnetze für öffentlich zugängliche Systemkomponenten, die [Auswahl: physisch; logisch] von internen Organisationsnetzen getrennt sind; und c. Stellt eine Verbindung zu externen Netzwerken oder Informationssystemen nur über verwaltete Schnittstellen her, die aus Grenzschutzgeräten bestehen, die gemäß einer Sicherheitsarchitektur der Organisation angeordnet sind.	elb-acm-certificate-required	Zum Schutz von eventuell vorhandenen sensiblen Daten sowie von Daten während der Übertragung muss die Verschlüsselung für Ihr Elastic Load Balancing aktiviert sein. Verwenden Sie AWS Certificate Manager, um öffentliche und private SSL/TLS-Zertifikate mit AWS Diensten und internen Ressourcen zu verwalten, bereitzustellen und bereitzustellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen zu
SC-7	Das Informati onssystem: a. Überwacht und kontrolliert die Kommunikation an der Außengrenze des Systems und an wichtigen internen Grenzen innerhalb des Systems; b. Implementiert Subnetze für öffentlic h zugängliche Systemkomponenten, die [Auswahl: physisch; logisch] von internen Organisat ionsnetzen getrennt sind; und c. Stellt eine Verbindung zu externen Netzwerke n oder Informati onssystemen nur über verwaltete Schnittstellen her, die aus Grenzschu tzgeräten bestehen, die gemäß einer Sicherheitsarchite ktur der Organisation angeordnet sind.	alb-http-to-https-Umleitungsprüfung	Um Daten während der Übertragung zu schützen, stellen Sie sicher, dass Ihr Application Load Balancer unverschl üsselte HTTP-Anfr agen automatisch an HTTPS umleitet. Um eventuell vorhanden e sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen zu
SC-7	Das Informationssystem: a. Überwacht und kontrolliert die Kommunikation an der Außengrenze des Systems und an wichtigen internen Grenzen innerhalb des Systems; b. Implementiert Subnetze für öffentlich zugängliche Systemkomponenten, die [Auswahl: physisch; logisch] von internen Organisationsnetzen getrennt sind; und c. Stellt eine Verbindung zu externen Netzwerken oder Informationssystemen nur über verwaltete Schnittstellen her, die aus Grenzschutzgeräten bestehen, die gemäß einer Sicherheitsarchitektur der Organisation angeordnet sind.	elb-tls-https-listeners-nur	Stellen Sie sicher, dass Ihre Elastic Load Balancer (ELBs) mit SSL- oder HTTPS-Listenern konfiguriert sind. Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen zu
SC-7	Das Informationssystem: a. Überwacht und kontrolliert die Kommunikation an der Außengrenze des Systems und an wichtigen internen Grenzen innerhalb des Systems; b. Implementiert Subnetze für öffentlich zugängliche Systemkomponenten, die [Auswahl: physisch; logisch] von internen Organisationsnetzen getrennt sind; und c. Stellt eine Verbindung zu externen Netzwerken oder Informationssystemen nur über verwaltete Schnittstellen her, die aus Grenzschutzgeräten bestehen, die gemäß einer Sicherheitsarchitektur der Organisation angeordnet sind.	wafv2-logging-enabled	Um Ihnen bei der Protokollierung und Überwachung in Ihrer Umgebung zu helfen, aktivieren Sie die AWS WAF (V2) -Protokollierung im regionalen und globalen Web. ACLs AWS Die WAF-Protokollierung bietet detaillierte Informationen über den Datenverkehr, der von Ihrer Web-ACL analysiert wird. In den Protokollen werden die Uhrzeit aufgezeichnet, zu der die AWS WAF die Anfrage von Ihrer AWS Ressource erhalten hat, Informationen über die Anfrage und eine Aktion für die Regel, der jede Anfrage entsprach.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen zu
SC-7	Das Informati onssystem: a. Überwacht und kontrolliert die Kommunikation an der Außengrenze des Systems und an wichtigen internen Grenzen innerhalb des Systems; b. Implementiert Subnetze für öffentlic h zugängliche Systemkomponenten, die [Auswahl: physisch; logisch] von internen Organisat ionsnetzen getrennt sind; und c. Stellt eine Verbindung zu externen Netzwerke n oder Informati onssystemen nur über verwaltete Schnittstellen her, die aus Grenzschu tzgeräten bestehen, die gemäß einer Sicherheitsarchite ktur der Organisation angeordnet sind.	ec2- instances-in-vpc	Stellen Sie Amazon Elastic Compute Cloud (Amazon EC2) -Instances innerhalb einer Amazon Virtual Private Cloud (Amazon VPC) bereit, um eine sichere Kommunika tion zwischen einer Instance und anderen Services innerhalb der Amazon VPC zu ermöglichen, ohne dass ein Internet-Gateway, ein NAT-Gerät oder eine VPN-Verbindung erforderl ich ist. Der gesamte Datenverkehr bleibt sicher in der AWS Cloud. Domänen, die sich innerhalb einer Amazon VPC befinden, verfügen aufgrund ihrer logischen Isolierun g im Vergleich zu Domänen, die öffentlic he Endpunkte nutzen, über eine zusätzlic he Sicherheitsebene. Weisen Sie EC2

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen zu
			Amazon-Instances einer Amazon-VPC zu, um den Zugriff ordnungsgemäß zu verwalten.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen zu
SC-7	Das Informationssystem: a. Überwacht und kontrolliert die Kommunikation an der Außengrenze des Systems und an wichtigen internen Grenzen innerhalb des Systems; b. Implementiert Subnetze für öffentlich zugängliche Systemkomponenten, die [Auswahl: physisch; logisch] von internen Organisationsnetzen getrennt sind; und c. Stellt eine Verbindung zu externen Netzwerken oder Informationssystemen nur über verwaltete Schnittstellen her, die aus Grenzschutzgeräten bestehen, die gemäß einer Sicherheitsarchitektur der Organisation angeordnet sind.	internet-gateway-authorized-vpc-nur	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Internet-Gateways nur mit autorisierter Amazon Virtual Private Cloud (Amazon VPC) verbunden sind. Internet-Gateways ermöglichen den bidirektionalen Internetzugang zur und von der Amazon VPC, was möglicherweise zu einem unbefugten Zugriff auf Amazon-VPC-Ressourcen führen kann.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen zu
SC-7	Das Informationssystem: a. Überwacht und kontrolliert die Kommunikation an der Außengrenze des Systems und an wichtigen internen Grenzen innerhalb des Systems; b. Implementiert Subnetze für öffentlich zugängliche Systemkomponenten, die [Auswahl: physisch; logisch] von internen Organisationsnetzen getrennt sind; und c. Stellt eine Verbindung zu externen Netzwerken oder Informationssystemen nur über verwaltete Schnittstellen her, die aus Grenzschutzgeräten bestehen, die gemäß einer Sicherheitsarchitektur der Organisation angeordnet sind.	dms-replication-not-public	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass auf DMS-Replikationsinstanzen nicht öffentlich zugegriffen werden kann. DMS-Replikations-Instances können vertrauliche Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen zu
SC-7	Das Informati onssystem: a. Überwacht und kontrolliert die Kommunikation an der Außengrenze des Systems und an wichtigen internen Grenzen innerhalb des Systems; b. Implementiert Subnetze für öffentlic h zugängliche Systemkomponenten, die [Auswahl: physisch; logisch] von internen Organisat ionsnetzen getrennt sind; und c. Stellt eine Verbindung zu externen Netzwerke n oder Informati onssystemen nur über verwaltete Schnittstellen her, die aus Grenzschu tzgeräten bestehen, die gemäß einer Sicherheitsarchite ktur der Organisation angeordnet sind.	ebs-snapshot-public-restorable-überprüfen	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass EBS-Snapshots nicht öffentlich wiederher stellbar sind. EBS-Volume-Snapsho ts können vertrauli che Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen zu
SC-7	Das Informationssystem: a. Überwacht und kontrolliert die Kommunikation an der Außengrenze des Systems und an wichtigen internen Grenzen innerhalb des Systems; b. Implementiert Subnetze für öffentlich zugängliche Systemkomponenten, die [Auswahl: physisch; logisch] von internen Organisationsnetzen getrennt sind; und c. Stellt eine Verbindung zu externen Netzwerken oder Informationssystemen nur über verwaltete Schnittstellen her, die aus Grenzschutzgeräten bestehen, die gemäß einer Sicherheitsarchitektur der Organisation angeordnet sind.	elasticsearch-in-vpc-only	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass sich Amazon OpenSearch OpenSearch Service (Service) - Domains innerhalb einer Amazon Virtual Private Cloud (Amazon VPC) befinden. Eine OpenSearch Service-Domain innerhalb einer Amazon VPC ermöglicht die sichere Kommunikation zwischen OpenSearch Service und anderen Services innerhalb der Amazon VPC, ohne dass ein Internet-Gateway, ein NAT-Gerät oder eine VPN-Verbindung erforderlich ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen zu
SC-7	Das Informationssystem: a. Überwacht und kontrolliert die Kommunikation an der Außengrenze des Systems und an wichtigen internen Grenzen innerhalb des Systems; b. Implementiert Subnetze für öffentlich zugängliche Systemkomponenten, die [Auswahl: physisch; logisch] von internen Organisationsnetzen getrennt sind; und c. Stellt eine Verbindung zu externen Netzwerken oder Informationssystemen nur über verwaltete Schnittstellen her, die aus Grenzschutzgeräten bestehen, die gemäß einer Sicherheitsarchitektur der Organisation angeordnet sind.	emr-master-no-public-ip	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon EMR-Cluster-Masterknoten nicht öffentlich zugänglich sind. Amazon-EMR-Cluster-Hauptknoten können vertrauliche Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen zu
SC-7	Das Informati onssystem: a. Überwacht und kontrolliert die Kommunikation an der Außengrenze des Systems und an wichtigen internen Grenzen innerhalb des Systems; b. Implementiert Subnetze für öffentlic h zugängliche Systemkomponenten, die [Auswahl: physisch; logisch] von internen Organisat ionsnetzen getrennt sind; und c. Stellt eine Verbindung zu externen Netzwerke n oder Informati onssystemen nur über verwaltete Schnittstellen her, die aus Grenzschu tzgeräten bestehen, die gemäß einer Sicherheitsarchite ktur der Organisation angeordnet sind.	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) Security Groups können bei der Verwaltung des Netzwerkzugriffs helfen, indem sie eine statusbeh aftete Filterung von eingehendem und ausgehendem Netzwerkverkehr zu Ressourcen bereitste llen. AWS Wenn Sie eingehenden (oder entfernten) Datenverk ehr von 0.0.0.0/0 bis Port 22 auf Ihren Ressourcen nicht zulassen, können Sie den Remote-Zugriff einschränken.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen zu
SC-7	Das Informati onssystem: a. Überwacht und kontrolliert die Kommunikation an der Außengrenze des Systems und an wichtigen internen Grenzen innerhalb des Systems; b. Implementiert Subnetze für öffentlic h zugängliche Systemkomponenten, die [Auswahl: physisch; logisch] von internen Organisat ionsnetzen getrennt sind; und c. Stellt eine Verbindung zu externen Netzwerke n oder Informati onssystemen nur über verwaltete Schnittstellen her, die aus Grenzschu tzgeräten bestehen, die gemäß einer Sicherheitsarchite ktur der Organisation angeordnet sind.	lambda-function-pu blic-access-verboten	Verwalten Sie den Zugriff auf Ressource n in der AWS Cloud, indem Sie sicherste llen, dass AWS Lambda-Funktionen nicht öffentlich zugänglich sind. Der öffentliche Zugriff kann möglicherweise die Verfügbarkeit von Ressourcen beeinträc htigen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen zu
SC-7	Das Informati onssystem: a. Überwacht und kontrolliert die Kommunikation an der Außengrenze des Systems und an wichtigen internen Grenzen innerhalb des Systems; b. Implementiert Subnetze für öffentlic h zugängliche Systemkomponenten, die [Auswahl: physisch; logisch] von internen Organisat ionsnetzen getrennt sind; und c. Stellt eine Verbindung zu externen Netzwerke n oder Informati onssystemen nur über verwaltete Schnittstellen her, die aus Grenzschu tzgeräten bestehen, die gemäß einer Sicherheitsarchite ktur der Organisation angeordnet sind.	lambda-inside-vpc	Stellen Sie AWS Lambda-Funktionen in einer Amazon Virtual Private Cloud (Amazon VPC) bereit, um eine sichere Kommunika tion zwischen einer Funktion und anderen Diensten innerhalb der Amazon VPC zu gewährleisten. Bei dieser Konfiguration sind kein Internet-Gateway, kein NAT-Gerät und keine VPN-Verbindung erforderlich. Der gesamte Datenverk ehr bleibt sicher in der Cloud. AWS Domains, die sich innerhalb einer VPC befinden, verfügen aufgrund ihrer logischen Isolierun g im Vergleich zu Domains mit öffentlic hen Endpunkten über eine zusätzliche Sicherheitsebene. Um den Zugriff ordnungsg emäß zu verwalten,

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen zu
			sollten AWS Lambda-Funktionen einer VPC zugewiesen werden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen zu
SC-7	Das Informationssystem: a. Überwacht und kontrolliert die Kommunikation an der Außengrenze des Systems und an wichtigen internen Grenzen innerhalb des Systems; b. Implementiert Subnetze für öffentlich zugängliche Systemkomponenten, die [Auswahl: physisch; logisch] von internen Organisationsnetzen getrennt sind; und c. Stellt eine Verbindung zu externen Netzwerken oder Informationssystemen nur über verwaltete Schnittstellen her, die aus Grenzschutzgeräten bestehen, die gemäß einer Sicherheitsarchitektur der Organisation angeordnet sind.	rds-instance-public-access-überprüfen	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Relational Database Service (Amazon RDS) -Instances nicht öffentlich sind. Amazon-RDS-Datenbank-Instances können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen zu
SC-7	Das Informationssystem: a. Überwacht und kontrolliert die Kommunikation an der Außengrenze des Systems und an wichtigen internen Grenzen innerhalb des Systems; b. Implementiert Subnetze für öffentlich zugängliche Systemkomponenten, die [Auswahl: physisch; logisch] von internen Organisationsnetzen getrennt sind; und c. Stellt eine Verbindung zu externen Netzwerken oder Informationssystemen nur über verwaltete Schnittstellen her, die aus Grenzschutzgeräten bestehen, die gemäß einer Sicherheitsarchitektur der Organisation angeordnet sind.	rds-snapshots-public-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Relational Database Service (Amazon RDS) -Instances nicht öffentlich sind. Amazon-RDS-Datenbank-Instances können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen zu
SC-7	Das Informationssystem: a. Überwacht und kontrolliert die Kommunikation an der Außengrenze des Systems und an wichtigen internen Grenzen innerhalb des Systems; b. Implementiert Subnetze für öffentlich zugängliche Systemkomponenten, die [Auswahl: physisch; logisch] von internen Organisationsnetzen getrennt sind; und c. Stellt eine Verbindung zu externen Netzwerken oder Informationssystemen nur über verwaltete Schnittstellen her, die aus Grenzschutzgeräten bestehen, die gemäß einer Sicherheitsarchitektur der Organisation angeordnet sind.	redshift-cluster-public-access-überprüfen	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Redshift Redshift-Cluster nicht öffentlich sind. Amazon-Redshift-Cluster können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen zu
SC-7	Das Informationssystem: a. Überwacht und kontrolliert die Kommunikation an der Außengrenze des Systems und an wichtigen internen Grenzen innerhalb des Systems; b. Implementiert Subnetze für öffentlich zugängliche Systemkomponenten, die [Auswahl: physisch; logisch] von internen Organisationsnetzen getrennt sind; und c. Stellt eine Verbindung zu externen Netzwerken oder Informationssystemen nur über verwaltete Schnittstellen her, die aus Grenzschutzgeräten bestehen, die gemäß einer Sicherheitsarchitektur der Organisation angeordnet sind.	restricted-common-ports	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass gemeinsame Ports für Amazon Elastic Compute Cloud (Amazon EC2) -Sicherheitsgruppen eingeschränkt sind. Wenn der Zugriff auf Ports nicht auf vertrauenswürdige Quellen beschränkt wird, kann dies zu Angriffen auf die Verfügbarkeit, Integrität und Vertraulichkeit von Systemen führen. Mit dieser Regel können Sie optional die Parameter blockedPort1–blockedPort5 festlegen (Standardkonfigurationen: 20, 21, 3389, 3306, 4333). Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen zu
SC-7	Das Informati onssystem: a. Überwacht und kontrolliert die Kommunikation an der Außengrenze des Systems und an wichtigen internen Grenzen innerhalb des Systems; b. Implementiert Subnetze für öffentlic h zugängliche Systemkomponenten, die [Auswahl: physisch; logisch] von internen Organisat ionsnetzen getrennt sind; und c. Stellt eine Verbindung zu externen Netzwerke n oder Informati onssystemen nur über verwaltete Schnittstellen her, die aus Grenzschu tzgeräten bestehen, die gemäß einer Sicherheitsarchite ktur der Organisation angeordnet sind.	s-3 bucket-public-read -prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie nur autorisierten Benutzern, Prozessen und Geräten Zugriff auf Amazon Simple Storage Service (Amazon S3) - Buckets gewähren. Die Verwaltung des Zugriffs sollte mit der Klassifizierung der Daten übereinst immen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen zu
SC-7	Das Informationssystem: a. Überwacht und kontrolliert die Kommunikation an der Außengrenze des Systems und an wichtigen internen Grenzen innerhalb des Systems; b. Implementiert Subnetze für öffentlich zugängliche Systemkomponenten, die [Auswahl: physisch; logisch] von internen Organisationsnetzen getrennt sind; und c. Stellt eine Verbindung zu externen Netzwerken oder Informationssystemen nur über verwaltete Schnittstellen her, die aus Grenzschutzgeräten bestehen, die gemäß einer Sicherheitsarchitektur der Organisation angeordnet sind.	s3- bucket-public-write-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie nur autorisierten Benutzern, Prozessen und Geräten Zugriff auf Amazon Simple Storage Service (Amazon S3) - Buckets gewähren. Die Verwaltung des Zugriffs sollte mit der Klassifizierung der Daten übereinstimmen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen zu
SC-7	Das Informationssystem: a. Überwacht und kontrolliert die Kommunikation an der Außengrenze des Systems und an wichtigen internen Grenzen innerhalb des Systems; b. Implementiert Subnetze für öffentlich zugängliche Systemkomponenten, die [Auswahl: physisch; logisch] von internen Organisationsnetzen getrennt sind; und c. Stellt eine Verbindung zu externen Netzwerken oder Informationssystemen nur über verwaltete Schnittstellen her, die aus Grenzschutzgeräten bestehen, die gemäß einer Sicherheitsarchitektur der Organisation angeordnet sind.	sagemaker-notebook-no-direct-Internetzugang	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass SageMaker Amazon-Notebooks keinen direkten Internetzugang zulassen. Indem Sie direkten Internetzugang blockieren, vermeiden Sie, dass unbefugte Benutzer auf sensible Daten zugreifen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen zu
SC-7	Das Informati onssystem: a. Überwacht und kontrolliert die Kommunikation an der Außengrenze des Systems und an wichtigen internen Grenzen innerhalb des Systems; b. Implementiert Subnetze für öffentlic h zugängliche Systemkomponenten, die [Auswahl: physisch; logisch] von internen Organisat ionsnetzen getrennt sind; und c. Stellt eine Verbindung zu externen Netzwerke n oder Informati onssystemen nur über verwaltete Schnittstellen her, die aus Grenzschu tzgeräten bestehen, die gemäß einer Sicherheitsarchite ktur der Organisation angeordnet sind.	vpc-default-security-group-geschlossen	Sicherheitsgruppen von Amazon Elastic Compute Cloud (Amazon EC2) können bei der Verwaltung des Netzwerkzugriffs helfen, indem sie eine statusbehaftete Filterung des ein- und ausgehenden Netzwerkverkehrs zu Ressourcen bereitstellen. AWS Die Beschränk ung des gesamten Datenverkehrs auf die Standardsicherheit sgruppe hilft dabei, den Fernzugriff auf Ihre Ressourcen einzuschränken. AWS

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen zu
SC-7	Das Informati onssystem: a. Überwacht und kontrolliert die Kommunikation an der Außengrenze des Systems und an wichtigen internen Grenzen innerhalb des Systems; b. Implementiert Subnetze für öffentlic h zugängliche Systemkomponenten, die [Auswahl: physisch; logisch] von internen Organisat ionsnetzen getrennt sind; und c. Stellt eine Verbindung zu externen Netzwerke n oder Informati onssystemen nur über verwaltete Schnittstellen her, die aus Grenzschu tzgeräten bestehen, die gemäß einer Sicherheitsarchite ktur der Organisation angeordnet sind.	alb-waf-enabled	Stellen Sie sicher, dass AWS WAF auf Elastic Load Balancers (ELB) aktiviert ist, um Webanwendungen zu schützen. Eine WAF trägt zum Schutz Ihrer Webanwend ungen oder APIs vor gängigen Web-Explo its bei. Diese Web-Exploits können sich auf die Verfügbar keit auswirken, die Sicherheit gefährden oder übermäßige Ressourcen in Ihrer Umgebung verbrauch en.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen zu
SC-7	Das Informationssystem: a. Überwacht und kontrolliert die Kommunikation an der Außengrenze des Systems und an wichtigen internen Grenzen innerhalb des Systems; b. Implementiert Subnetze für öffentlich zugängliche Systemkomponenten, die [Auswahl: physisch; logisch] von internen Organisationsnetzen getrennt sind; und c. Stellt eine Verbindung zu externen Netzwerken oder Informationssystemen nur über verwaltete Schnittstellen her, die aus Grenzschutzgeräten bestehen, die gemäß einer Sicherheitsarchitektur der Organisation angeordnet sind.	s-3 bucket-policy-grantee-check	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie s3_bucket_policy_grantee_check aktivieren. Diese Regel prüft, ob der vom Amazon S3 S3-Bucket gewährte Zugriff durch die von Ihnen bereitgestellten AWS Principals, Verbundbenutzer, Service Principals, IP-Adressen oder Amazon Virtual Private Cloud (Amazon VPC) IDs eingeschränkt ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen zu
SC-7	Das Informati onssystem: a. Überwacht und kontrolliert die Kommunikation an der Außengrenze des Systems und an wichtigen internen Grenzen innerhalb des Systems; b. Implementiert Subnetze für öffentlic h zugängliche Systemkomponenten, die [Auswahl: physisch; logisch] von internen Organisat ionsnetzen getrennt sind; und c. Stellt eine Verbindung zu externen Netzwerke n oder Informati onssystemen nur über verwaltete Schnittstellen her, die aus Grenzschu tzgeräten bestehen, die gemäß einer Sicherheitsarchite ktur der Organisation angeordnet sind.	s3-Blöcke account-l evel-public-access	Verwalten Sie den Zugriff auf Ressource n in der AWS Cloud, indem Sie sicherste llen, dass Amazon Simple Storage Service (Amazon S3) -Buckets nicht öffentlich zugänglic h sind. Diese Regel trägt dazu bei, sensible Daten vor unbefugten Remote-Benutzern zu schützen, indem sie den öffentlichen Zugriff verhinder t. Mit dieser Regel können Sie optional die Parameter ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) und restrictPublicBuck ets Parameter (Config Default: True) festlegen. Die tatsächlichen Werte müssen den Richtlini

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen zu
			en Ihrer Organisation entsprechen.
SC-7	Das Informati onssystem: a. Überwacht und kontrolliert die Kommunikation an der Außengrenze des Systems und an wichtigen internen Grenzen innerhalb des Systems; b. Implementiert Subnetze für öffentlic h zugängliche Systemkomponenten, die [Auswahl: physisch; logisch] von internen Organisat ionsnetzen getrennt sind; und c. Stellt eine Verbindung zu externen Netzwerke n oder Informati onssystemen nur über verwaltete Schnittstellen her, die aus Grenzschu tzgeräten bestehen, die gemäß einer Sicherheitsarchite ktur der Organisation angeordnet sind.	vpc-sg-open-only-to-authorized-ports	Verwalten Sie den Zugriff auf Ressource n in der AWS Cloud, indem Sie sicherste llen, dass gemeinsam e Ports für Amazon Elastic Compute Cloud (Amazon EC2) -Sicherhe itsgruppen eingeschr ränkt sind. Wenn der Zugriff auf Ports nicht auf vertrauen swürdige Quellen beschränkt wird, kann dies zu Angriffen auf die Verfügbar keit, Integrität und Vertraulichkeit von Systemen führen. Durch die Beschränk ung des Zugriffs auf Ressourcen innerhalb einer Sicherhei tsgruppe aus dem Internet (0.0.0.0/0) kann der Remote-Zugriff auf interne Systeme gesteuert werden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen zu
SC-7	Das Informati onssystem: a. Überwacht und kontrolliert die Kommunikation an der Außengrenze des Systems und an wichtigen internen Grenzen innerhalb des Systems; b. Implementiert Subnetze für öffentlic h zugängliche Systemkomponenten, die [Auswahl: physisch; logisch] von internen Organisat ionsnetzen getrennt sind; und c. Stellt eine Verbindung zu externen Netzwerke n oder Informati onssystemen nur über verwaltete Schnittstellen her, die aus Grenzschu tzgeräten bestehen, die gemäß einer Sicherheitsarchite ktur der Organisation angeordnet sind.	alb-http-drop-invalid-Header-fähig	Stellen Sie sicher, dass Ihre Elastic Load Balancers (ELB) so konfiguriert sind, dass sie HTTP-Header löschen. Da sensible Daten vorhanden sein können, sollten Sie die Verschlüsselung bei der Übertragung aktivieren, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen zu
SC-7	Das Informationssystem: a. Überwacht und kontrolliert die Kommunikation an der Außengrenze des Systems und an wichtigen internen Grenzen innerhalb des Systems; b. Implementiert Subnetze für öffentlich zugängliche Systemkomponenten, die [Auswahl: physisch; logisch] von internen Organisationsnetzen getrennt sind; und c. Stellt eine Verbindung zu externen Netzwerken oder Informationssystemen nur über verwaltete Schnittstellen her, die aus Grenzschutzgeräten bestehen, die gemäß einer Sicherheitsarchitektur der Organisation angeordnet sind.	elasticsearch-node-to-node-Verschlüsselungsprüfung	Stellen Sie sicher, dass die node-to-node Verschlüsselung für Amazon OpenSearch Service aktiviert ist. Node-to-nodeVerschlüsselung ermöglicht die TLS 1.2-Verschlüsselung für die gesamte Kommunikation innerhalb der Amazon Virtual Private Cloud (Amazon VPC). Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen zu
SC-7(3)	Die Organisation begrenzt die Anzahl der externen Netzwerkverbindungen zum Informationssystem.	ec2- instances-in-vpc	Stellen Sie Amazon Elastic Compute Cloud (Amazon EC2) -Instances innerhalb einer Amazon Virtual Private Cloud (Amazon VPC) bereit, um eine sichere Kommunikation zwischen einer Instance und anderen Services innerhalb der Amazon VPC zu ermöglichen, ohne dass ein Internet-Gateway, ein NAT-Gerät oder eine VPN-Verbindung erforderlich ist. Der gesamte Datenverkehr bleibt sicher in der AWS Cloud. Domänen, die sich innerhalb einer Amazon VPC befinden, verfügen aufgrund ihrer logischen Isolierung im Vergleich zu Domänen, die öffentliche Endpunkte nutzen, über eine zusätzliche Sicherheitsebene. Weisen Sie EC2

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen zu
			Amazon-Instances einer Amazon-VPC zu, um den Zugriff ordnungsgemäß zu verwalten.
SC-7(3)	Die Organisation begrenzt die Anzahl der externen Netzwerkverbindungen zum Informationssystem.	internet-gateway-authorized-vpc-nur	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Internet-Gateways nur mit autorisierter Amazon Virtual Private Cloud (Amazon VPC) verbunden sind. Internet-Gateways ermöglichen den bidirektionalen Internetzugang zur und von der Amazon VPC, was möglicherweise zu einem unbefugten Zugriff auf Amazon-VPC-Ressourcen führen kann.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen zu
SC-7(3)	Die Organisation begrenzt die Anzahl der externen Netzwerkverbindungen zum Informationssystem.	dms-replication-not-public	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass auf DMS-Replikationsinstanzen nicht öffentlich zugegriffen werden kann. DMS-Replikations-Instances können vertrauliche Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.
SC-7(3)	Die Organisation begrenzt die Anzahl der externen Netzwerkverbindungen zum Informationssystem.	ebs-snapshot-public-restorable-überprüfen	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass EBS-Snapshots nicht öffentlich wiederherstellbar sind. EBS-Volume-Snapshots können vertrauliche Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen zu
SC-7(3)	Die Organisation begrenzt die Anzahl der externen Netzwerkverbindungen zum Informationssystem.	ec-2 instance-no-public-ip	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon Elastic Compute Cloud (Amazon EC2) - Instances nicht öffentlich zugänglich sind. EC2Amazon -Instances können vertrauliche Informationen enthalten, und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen zu
SC-7(3)	Die Organisation begrenzt die Anzahl der externen Netzwerkverbindungen zum Informationssystem.	elasticsearch-in-vpc-only	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass sich Amazon OpenSearch OpenSearch Service (Service) - Domains innerhalb einer Amazon Virtual Private Cloud (Amazon VPC) befinden. Eine OpenSearch Service-Domain innerhalb einer Amazon VPC ermöglicht die sichere Kommunikation zwischen OpenSearch Service und anderen Services innerhalb der Amazon VPC, ohne dass ein Internet-Gateway, ein NAT-Gerät oder eine VPN-Verbindung erforderlich ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen zu
SC-7(3)	Die Organisation begrenzt die Anzahl der externen Netzwerkverbindungen zum Informationssystem.	emr-master-no-public-ip	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon EMR-Cluster-Masterknoten nicht öffentlich zugänglich sind. Amazon-EMR-Cluster-Hauptknoten können vertrauliche Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen zu
SC-7(3)	Die Organisation begrenzt die Anzahl der externen Netzwerkverbindungen zum Informationssystem.	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) Security Groups können bei der Verwaltung des Netzwerkzugriffs helfen, indem sie eine statusbehaftete Filterung von eingehendem und ausgehendem Netzwerkverkehr zu Ressourcen bereitstellen. AWS Wenn Sie eingehenden (oder entfernten) Datenverkehr von 0.0.0.0/0 bis Port 22 auf Ihren Ressourcen nicht zulassen, können Sie den Remote-Zugriff einschränken.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen zu
SC-7(3)	Die Organisation begrenzt die Anzahl der externen Netzwerkverbindungen zum Informationssystem.	lambda-function-public-access-verboten	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass AWS Lambda-Funktionen nicht öffentlich zugänglich sind. Der öffentliche Zugriff kann möglicherweise die Verfügbarkeit von Ressourcen beeinträchtigen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen zu
SC-7(3)	Die Organisation begrenzt die Anzahl der externen Netzwerkverbindungen zum Informationssystem.	lambda-inside-vpc	Stellen Sie AWS Lambda-Funktionen in einer Amazon Virtual Private Cloud (Amazon VPC) bereit, um eine sichere Kommunikation zwischen einer Funktion und anderen Diensten innerhalb der Amazon VPC zu gewährleisten. Bei dieser Konfiguration sind kein Internet-Gateway, kein NAT-Gerät und keine VPN-Verbindung erforderlich. Der gesamte Datenverkehr bleibt sicher in der Cloud. AWS Domains, die sich innerhalb einer VPC befinden, verfügen aufgrund ihrer logischen Isolierung im Vergleich zu Domains mit öffentlichen Endpunkten über eine zusätzliche Sicherheitsebene. Um den Zugriff ordnungsgemäß zu verwalten,

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen zu
			sollten AWS Lambda-Funktionen einer VPC zugewiesen werden.
SC-7(3)	Die Organisation begrenzt die Anzahl der externen Netzwerkverbindungen zum Informationssystem.	rds-instance-public-access-überprüfen	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Relational Database Service (Amazon RDS) -Instances nicht öffentlich sind. Amazon-RDS-Datenbank-Instances können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen zu
SC-7(3)	Die Organisation begrenzt die Anzahl der externen Netzwerkverbindungen zum Informationssystem.	rds-snapshots-public-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Relational Database Service (Amazon RDS) -Instances nicht öffentlich sind. Amazon-RDS-Datenbank-Instances können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen zu
SC-7(3)	Die Organisation begrenzt die Anzahl der externen Netzwerkverbindungen zum Informationssystem.	redshift-cluster-public-access-überprüfen	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Redshift Redshift-Cluster nicht öffentlich sind. Amazon-Redshift-Cluster können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen zu
SC-7(3)	Die Organisation begrenzt die Anzahl der externen Netzwerkverbindungen zum Informationssystem.	restricted-common-ports	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass gemeinsame Ports für Amazon Elastic Compute Cloud (Amazon EC2) -Sicherheitsgruppen eingeschränkt sind. Wenn der Zugriff auf Ports nicht auf vertrauenswürdige Quellen beschränkt wird, kann dies zu Angriffen auf die Verfügbarkeit, Integrität und Vertraulichkeit von Systemen führen. Mit dieser Regel können Sie optional die Parameter blockedPort1–blockedPort5 festlegen (Standardkonfigurationen: 20, 21, 3389, 3306, 4333). Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen zu
SC-7(3)	Die Organisation begrenzt die Anzahl der externen Netzwerkverbindungen zum Informationssystem.	account-level-public-accesss3-Blöcke	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Simple Storage Service (Amazon S3) -Buckets nicht öffentlich zugänglich sind. Diese Regel trägt dazu bei, sensible Daten vor unbefugten Remote-Benutzern zu schützen, indem sie den öffentlichen Zugriff verhindert. Mit dieser Regel können Sie optional die Parameter ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) und restrictPublicBuckets Parameter (Config Default: True) festlegen. Die tatsächlichen Werte müssen den Richtlini

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen zu
			en Ihrer Organisation entsprechen.
SC-7(3)	Die Organisation begrenzt die Anzahl der externen Netzwerkverbindungen zum Informationssystem.	s3- bucket-policy-grantee-check	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie s3_bucket_policy_grantee_check aktivieren. Diese Regel prüft, ob der vom Amazon S3 S3-Bucket gewährte Zugriff durch die von Ihnen bereitgestellten AWS Principals, Verbundbenutzer, Service Principals, IP-Adressen oder Amazon Virtual Private Cloud (Amazon VPC) IDs eingeschränkt ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen zu
SC-7(3)	Die Organisation begrenzt die Anzahl der externen Netzwerkverbindungen zum Informationssystem.	s-3 bucket-public-read-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie nur autorisierten Benutzern, Prozessen und Geräten Zugriff auf Amazon Simple Storage Service (Amazon S3) - Buckets gewähren. Die Verwaltung des Zugriffs sollte mit der Klassifizierung der Daten übereinstimmen.
SC-7(3)	Die Organisation begrenzt die Anzahl der externen Netzwerkverbindungen zum Informationssystem.	s3- bucket-public-write-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie nur autorisierten Benutzern, Prozessen und Geräten Zugriff auf Amazon Simple Storage Service (Amazon S3) - Buckets gewähren. Die Verwaltung des Zugriffs sollte mit der Klassifizierung der Daten übereinstimmen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen zu
SC-7(3)	Die Organisation begrenzt die Anzahl der externen Netzwerkverbindungen zum Informationssystem.	sagemaker-notebook-no-direct-Internetzugang	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass SageMaker Amazon-Notebooks keinen direkten Internetzugang zulassen. Indem Sie direkten Internetzugang blockieren, vermeiden Sie, dass unbefugte Benutzer auf sensible Daten zugreifen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen zu
SC-7(3)	Die Organisation begrenzt die Anzahl der externen Netzwerkverbindungen zum Informationssystem.	vpc-default-security-group-geschlossen	Sicherheitsgruppen von Amazon Elastic Compute Cloud (Amazon EC2) können bei der Verwaltung des Netzwerkzugriffs helfen, indem sie eine statusbehaftete Filterung des ein- und ausgehenden Netzwerkverkehrs zu Ressourcen bereitstellen. AWS Die Beschränkung des gesamten Datenverkehrs auf die Standardsicherheitsgruppe hilft dabei, den Fernzugriff auf Ihre Ressourcen einzuschränken. AWS

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen zu
SC-7(3)	Die Organisation begrenzt die Anzahl der externen Netzwerkverbindungen zum Informationssystem.	vpc-sg-open-only-to-authorized-ports	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass gemeinsame Ports für Amazon Elastic Compute Cloud (Amazon EC2) -Sicherheitsgruppen eingeschränkt sind. Wenn der Zugriff auf Ports nicht auf vertrauenswürdige Quellen beschränkt wird, kann dies zu Angriffen auf die Verfügbarkeit, Integrität und Vertraulichkeit von Systemen führen. Durch die Beschränkung des Zugriffs auf Ressourcen innerhalb einer Sicherheitsgruppe aus dem Internet (0.0.0.0/0) kann der Fernzugriff auf interne Systeme gesteuert werden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen zu
SC-8	Das Informationssystem schützt die [Auswahl (eine oder mehrere): Vertraulichkeit; Integrität] der übermittelten Informationen.	alb-http-to-https-Umleitungsprüfung	Um Daten während der Übertragung zu schützen, stellen Sie sicher, dass Ihr Application Load Balancer unverschlüsselte HTTP-Anfragen automatisch an HTTPS umleitet. Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.
SC-8	Das Informationssystem schützt die [Auswahl (eine oder mehrere): Vertraulichkeit; Integrität] der übermittelten Informationen.	alb-http-drop-invalid-Header-fähig	Stellen Sie sicher, dass Ihre Elastic Load Balancers (ELB) so konfiguriert sind, dass sie HTTP-Header löschen. Da sensible Daten vorhanden sein können, sollten Sie die Verschlüsselung bei der Übertragung aktivieren, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen zu
SC-8	Das Informationssystem schützt die [Auswahl (eine oder mehrere): Vertraulichkeit; Integrität] der übermittelten Informationen.	elasticsearch-node-to-node-Verschlüsselungsprüfung	Stellen Sie sicher, dass die node-to-node Verschlüsselung für Amazon OpenSearch Service aktiviert ist. Node-to-nodeVerschlüsselung ermöglicht die TLS 1.2-Verschlüsselung für die gesamte Kommunikation innerhalb der Amazon Virtual Private Cloud (Amazon VPC). Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.
SC-8	Das Informationssystem schützt die [Auswahl (eine oder mehrere): Vertraulichkeit; Integrität] der übermittelten Informationen.	elb-tls-https-listeners-nur	Stellen Sie sicher, dass Ihre Elastic Load Balancer (ELBs) mit SSL- oder HTTPS-Listenern konfiguriert sind. Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen zu
SC-8	Das Informati onssystem schützt die [Auswahl (eine oder mehrere): Vertrauli chkeit; Integrität] der übermittelten Informati onen.	redshift-require-tls-ssl	Stellen Sie sicher, dass Ihre Amazon-Redshift-Cluster eine TLS/SSL-Verschlüss elung erfordern, um eine Verbindun g zu SQL-Clients herzustellen. Um eventuell vorhanden e sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.
SC-8	Das Informati onssystem schützt die [Auswahl (eine oder mehrere): Vertrauli chkeit; Integrität] der übermittelten Informati onen.	s-3 bucket-ssl-request s-only	Um Daten während der Übertragung zu schützen, stellen Sie sicher, dass Ihre Amazon Simple Storage Service (Amazon S3)-Bucke ts Anfragen zur Verwendung von Secure Socket Layer (SSL)-Buc kets erfordern. Um eventuell vorhanden e sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen zu
SC-8	Das Informati onssystem schützt die [Auswahl (eine oder mehrere): Vertrauli chkeit; Integrität] der übermittelten Informati onen.	elb-acm-certificate-required	Zum Schutz von eventuell vorhanden en sensiblen Daten sowie von Daten während der Übertragung muss die Verschlüsselung für Ihr Elastic Load Balancing aktiviert sein. Verwenden Sie AWS Certificate Manager, um öffentlic he und private SSL/ TLS-Zertifikate mit AWS Diensten und internen Ressource n zu verwalten, bereitzustellen und bereitzustellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen zu
SC-8(1)	Das Informationssystem setzt kryptographische Mechanismen ein, um während der Übertragung [Auswahl (eine oder mehrere Optionen): eine unbefugte Offenlegung von Informationen zu verhindern; Änderungen an Informationen zu erkennen], sofern sie nicht anderweitig durch [Zuweisung: von der Organisation definierte alternative physische Schutzmaßnahmen] geschützt sind.	alb-http-to-https-Umleitungsprüfung	Um Daten während der Übertragung zu schützen, stellen Sie sicher, dass Ihr Application Load Balancer unverschlüsselte HTTP-Anfragen automatisch an HTTPS umleitet. Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen zu
SC-8(1)	Das Informati onssystem setzt kryptographische Mechanismen ein, um während der Übertragung [Auswahl (eine oder mehrere Optionen): eine unbefugte Offenlegu ng von Informati onen zu verhinder n; Änderungen an Informationen zu erkennen], sofern sie nicht anderweit ig durch [Zuweisung: von der Organisation definierte alternative physische Schutzmaß nahmen] geschützt sind.	alb-http-drop-invalid-Header-fähig	Stellen Sie sicher, dass Ihre Elastic Load Balancers (ELB) so konfiguriert sind, dass sie HTTP-Header löschen. Da sensible Daten vorhanden sein können, sollten Sie die Verschlüsselung bei der Übertragung aktivieren, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen zu
SC-8(1)	Das Informationssystem setzt kryptographische Mechanismen ein, um während der Übertragung [Auswahl (eine oder mehrere Optionen): eine unbefugte Offenlegung von Informationen zu verhindern; Änderungen an Informationen zu erkennen], sofern sie nicht anderweitig durch [Zuweisung: von der Organisation definierte alternative physische Schutzmaßnahmen] geschützt sind.	elasticsearch-node-to-node-Verschlüsselungsprüfung	Stellen Sie sicher, dass die node-to-node Verschlüsselung für Amazon OpenSearch Service aktiviert ist. Node-to-nodeVerschlüsselung ermöglicht die TLS 1.2-Verschlüsselung für die gesamte Kommunikation innerhalb der Amazon Virtual Private Cloud (Amazon VPC). Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen zu
SC-8(1)	Das Informati onssystem setzt kryptographische Mechanismen ein, um während der Übertragung [Auswahl (eine oder mehrere Optionen): eine unbefugte Offenlegu ng von Informati onen zu verhinder n; Änderungen an Informationen zu erkennen], sofern sie nicht anderweit ig durch [Zuweisung: von der Organisation definierte alternative physische Schutzmaß nahmen] geschützt sind.	elb-tls-https-listeners-nur	Stellen Sie sicher, dass Ihre Elastic Load Balancer (ELBs) mit SSL- oder HTTPS-Listenern konfiguriert sind. Um eventuell vorhanden e sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen zu
SC-8(1)	Das Informati onssystem setzt kryptographische Mechanismen ein, um während der Übertragung [Auswahl (eine oder mehrere Optionen): eine unbefugte Offenlegu ng von Informati onen zu verhinder n; Änderungen an Informationen zu erkennen], sofern sie nicht anderweit ig durch [Zuweisung: von der Organisation definierte alternative physische Schutzmaß nahmen] geschützt sind.	redshift-require-tls-ssl	Stellen Sie sicher, dass Ihre Amazon-Redshift-Cluster eine TLS/SSL-Verschlüss elung erfordern, um eine Verbindun g zu SQL-Clients herzustellen. Um eventuell vorhanden e sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen zu
SC-8(1)	Das Informationssystem setzt kryptographische Mechanismen ein, um während der Übertragung [Auswahl (eine oder mehrere Optionen): eine unbefugte Offenlegung von Informationen zu verhindern; Änderungen an Informationen zu erkennen], sofern sie nicht anderweitig durch [Zuweisung: von der Organisation definierte alternative physische Schutzmaßnahmen] geschützt sind.	s-3 bucket-ssl-requests-only	Um Daten während der Übertragung zu schützen, stellen Sie sicher, dass Ihre Amazon Simple Storage Service (Amazon S3)-Buckets Anfragen zur Verwendung von Secure Socket Layer (SSL)-Buckets erfordern. Da sensible Daten vorhanden sein können, sollten Sie die Verschlüsselung bei der Übertragung aktivieren, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen zu
SC-8(1)	Das Informationssystem setzt kryptographische Mechanismen ein, um während der Übertragung [Auswahl (eine oder mehrere Optionen): eine unbefugte Offenlegung von Informationen zu verhindern; Änderungen an Informationen zu erkennen], sofern sie nicht anderweitig durch [Zuweisung: von der Organisation definierte alternative physische Schutzmaßnahmen] geschützt sind.	elb-acm-certificate-required	Zum Schutz von eventuell vorhandenen sensiblen Daten sowie von Daten während der Übertragung muss die Verschlüsselung für Ihr Elastic Load Balancing aktiviert sein. Verwenden Sie AWS Certificate Manager, um öffentliche und private SSL/TLS-Zertifikate mit AWS Diensten und internen Ressourcen zu verwalten, bereitzustellen und bereitzustellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen zu
SC-12	Die Organisation erstellt und verwaltet kryptografische Schlüssel für die erforderliche Kryptografie, die innerhalb des Informationssystems eingesetzt wird, in Übereinstimmung mit [Zuordnung: von der Organisation festgelegte Anforderungen für die Erzeugung, Verteilung, Speicherung, den Zugriff und die Vernichtung von Schlüsseln].	cmk-backing-key-rotation-aktiviert	Aktivieren Sie die Schlüsselrotation, um sicherzustellen, dass Schlüssel rotiert werden, sobald sie das Ende ihrer Kryptoperiode erreicht haben.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen zu
SC-12	Die Organisation erstellt und verwaltet kryptografische Schlüssel für die erforderliche Kryptografie, die innerhalb des Informationssystems eingesetzt wird, in Übereinstimmung mit [Zuordnung: von der Organisation festgelegte Anforderungen für die Erzeugung, Verteilung, Speicherung, den Zugriff und die Vernichtung von Schlüsseln].	acm-certificate-expiration-check	Stellen Sie sicher, dass die Netzwerkintegrität geschützt ist, indem Sie sicherstellen, dass X509-Zertifikate von AWS ACM ausgestellt werden. Diese Zertifikate müssen gültig und dürfen nicht abgelaufen sein. Für diese Regel ist ein Wert für erforderlich daysToExpiration (Wert für bewährte AWS Grundregeln für Sicherheit: 90). Der tatsächliche Wert muss den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen zu
SC-12	Die Organisation erstellt und verwaltet kryptografische Schlüssel für die erforderliche Kryptografie, die innerhalb des Informationssystems eingesetzt wird, in Übereinstimmung mit [Zuordnung: von der Organisation festgelegte Anforderungen für die Erzeugung, Verteilung, Speicherung, den Zugriff und die Vernichtung von Schlüsseln].	kms-cmk-not-scheduled-zum Löschen	Um Daten im Ruhezustand zu schützen, sollten Sie sicherstellen, dass die für den Kunden erforderlichen Masterschlüssel (CMKs) nicht für das Löschen im AWS Key Management Service (AWS KMS) vorgesehen sind. Da Schlüssel manchmal gelöscht werden müssen, können Sie mit dieser Regel alle zu löschenden Schlüssel überprüfen, falls ein Schlüssel versehentlich zur Löschung vorgemerkt wurde.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen zu
SC-13	Das Informationssystem implementiert [Zuordnung: von der Organisation definierte kryptografische Verwendungszwecke und Art der für jeden Verwendungszweck erforderlichen Kryptografie] in Übereinstimmung mit den geltenden Bundesgesetzen, Executive Orders, Richtlinien, Grundsätzen, Vorschriften und Standards.	elb-acm-certificate-required	Zum Schutz von eventuell vorhandenen sensiblen Daten sowie von Daten während der Übertragung muss die Verschlüsselung für Ihr Elastic Load Balancing aktiviert sein. Verwenden Sie AWS Certificate Manager, um öffentliche und private SSL/TLS-Zertifikate mit AWS Diensten und internen Ressourcen zu verwalten, bereitzustellen und bereitzustellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen zu
SC-13	Das Informationssystem implementiert [Zuordnung: von der Organisation definierte kryptografische Verwendungszwecke und Art der für jeden Verwendungszweck erforderlichen Kryptografie] in Übereinstimmung mit den geltenden Bundesgesetzen, Executive Orders, Richtlinien, Grundsätzen, Vorschriften und Standards.	alb-http-to-https-Umleitungsprüfung	Um Daten während der Übertragung zu schützen, stellen Sie sicher, dass Ihr Application Load Balancer unverschlüsselte HTTP-Anfragen automatisch an HTTPS umleitet. Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen zu
SC-13	Das Informationssystem implementiert [Zuordnung: von der Organisation definierte kryptografische Verwendungszwecke und Art der für jeden Verwendungszweck erforderlichen Kryptografie] in Übereinstimmung mit den geltenden Bundesgesetzen, Executive Orders, Richtlinien, Grundsätzen, Vorschriften und Standards.	api-gw-cache-enabled-und-verschlüsselt	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass die Verschlüsselung für den Cache Ihrer API-Gateway-Stufe aktiviert ist. Da für die API-Methode sensible Daten erfasst werden können, sollten Sie die Verschlüsselung von Daten im Ruhezustand aktivieren, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen zu
SC-13	Das Informationssystem implementiert [Zuordnung: von der Organisation definierte kryptografische Verwendungszwecke und Art der für jeden Verwendungszweck erforderlichen Kryptografie] in Übereinstimmung mit den geltenden Bundesgesetzen, Executive Orders, Richtlinien, Grundsätzen, Vorschriften und Standards.	cloud-trail-encryption-enabled	Da sensible Daten vorhanden sein können und um Daten im Ruhezustand zu schützen, sollten Sie sicherstellen, dass die Verschlüsselung für Ihre AWS CloudTrail Trails aktiviert ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen zu
SC-13	Das Informati onssystem implement iert [Zuordnung: von der Organisation definierte kryptogra fische Verwendun gszwecke und Art der für jeden Verwendun gszweck erforderl ichen Kryptografie] in Übereinstimmung mit den geltenden Bundesgesetzen, Executive Orders, Richtlinien, Grundsätz en, Vorschriften und Standards.	cloudwatch-log-group-encrypted	Um sensible Daten im Speicher zu schützen, stellen Sie sicher, dass die Verschlüs selung für Ihre Amazon CloudWatch Log Groups aktiviert ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen zu
SC-13	Das Informationssystem implementiert [Zuordnung: von der Organisation definierte kryptografische Verwendungszwecke und Art der für jeden Verwendungszweck erforderlichen Kryptografie] in Übereinstimmung mit den geltenden Bundesgesetzen, Executive Orders, Richtlinien, Grundsätzen, Vorschriften und Standards.	efs-encrypted-check	Aktivieren Sie die Verschlüsselung für Ihr Amazon Elastic File System (EFS), um eventuell vorhandene sensible Daten sowie Daten im Ruhezustand zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen zu
SC-13	Das Informationssystem implementiert [Zuordnung: von der Organisation definierte kryptografische Verwendungszwecke und Art der für jeden Verwendungszweck erforderlichen Kryptografie] in Übereinstimmung mit den geltenden Bundesgesetzen, Executive Orders, Richtlinien, Grundsätzen, Vorschriften und Standards.	elasticsearch-encrypted-at-rest	Da sensible Daten vorhanden sein können und um Daten im Ruhezustand zu schützen, sollten Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon OpenSearch Service (OpenSearch Service)-Domains aktiviert ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen zu
SC-13	Das Informationssystem implementiert [Zuordnung: von der Organisation definierte kryptografische Verwendungszwecke und Art der für jeden Verwendungszweck erforderlichen Kryptografie] in Übereinstimmung mit den geltenden Bundesgesetzen, Executive Orders, Richtlinien, Grundsätzen, Vorschriften und Standards.	encrypted-volumes	Aktivieren Sie die Verschlüsselung für Ihre Amazon-Elastic-Block-Store (Amazon-EBS)-Volumes, um eventuell vorhandene sensible Daten sowie Daten im Ruhezustand zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen zu
SC-13	Das Informati onssystem implement iert [Zuordnung: von der Organisation definierte kryptogra fische Verwendun gszwecke und Art der für jeden Verwendun gszweck erforderl ichen Kryptografie] in Übereinstimmung mit den geltenden Bundesgesetzen, Executive Orders, Richtlinien, Grundsätz en, Vorschriften und Standards.	rds-storage-encrypted	Zum Schutz von Daten im Ruhezusta nd müssen Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon Relational Database Service (Amazon RDS)-Instances aktiviert ist. Um eventuell vorhanden e sensible Daten im Ruhezustand in Amazon-RDS-Instanc es zu schützen, muss die Verschlüs selung von Daten im Ruhezustand aktiviert sein.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen zu
SC-13	Das Informationssystem implementiert [Zuordnung: von der Organisation definierte kryptografische Verwendungszwecke und Art der für jeden Verwendungszweck erforderlichen Kryptografie] in Übereinstimmung mit den geltenden Bundesgesetzen, Executive Orders, Richtlinien, Grundsätzen, Vorschriften und Standards.	redshift-cluster-configuration-check	Um Daten im Ruhezustand zu schützen, muss die Verschlüsselung für Ihre Amazon-Redshift-Cluster aktiviert sein. Sie müssen auch sicherstellen, dass die erforderlichen Konfigurationen auf Amazon-Redshift-Clustern bereitgestellt werden. Die Prüfungsprotokollierung muss aktiviert sein, um Informationen zu Verbindungen und Benutzeraktivitäten in der Datenbank bereitzustellen. Diese Regel erfordert, dass ein Wert für clusterDbEncrypted (Config Default: TRUE) und LoggingEnabled (Config Default: TRUE) gesetzt ist. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen zu
SC-13	Das Informati onssystem implement iert [Zuordnung: von der Organisation definierte kryptogra fische Verwendun gszwecke und Art der für jeden Verwendun gszweck erforderl ichen Kryptografie] in Übereinstimmung mit den geltenden Bundesgesetzen, Executive Orders, Richtlinien, Grundsätz en, Vorschriften und Standards.	redshift-require-tls-ssl	Stellen Sie sicher, dass Ihre Amazon-Redshift-Cluster eine TLS/SSL-Verschlüss elung erfordern, um eine Verbindun g zu SQL-Clients herzustellen. Um eventuell vorhanden e sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen zu
SC-13	Das Informationssystem implementiert [Zuordnung: von der Organisation definierte kryptografische Verwendungszwecke und Art der für jeden Verwendungszweck erforderlichen Kryptografie] in Übereinstimmung mit den geltenden Bundesgesetzen, Executive Orders, Richtlinien, Grundsätzen, Vorschriften und Standards.	s3-aktiviert bucket-server-side-encryption	Zum Schutz von Daten im Ruhezustand müssen Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon Simple Storage Service (Amazon S3)-Buckets aktiviert ist. Um eventuell vorhandene sensible Daten im Ruhezustand in Amazon-S3-Buckets zu schützen, muss die Verschlüsselung aktiviert sein.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen zu
SC-13	Das Informationssystem implementiert [Zuordnung: von der Organisation definierte kryptografische Verwendungszwecke und Art der für jeden Verwendungszweck erforderlichen Kryptografie] in Übereinstimmung mit den geltenden Bundesgesetzen, Executive Orders, Richtlinien, Grundsätzen, Vorschriften und Standards.	s-3 bucket-ssl-requests-only	Um Daten während der Übertragung zu schützen, stellen Sie sicher, dass Ihre Amazon Simple Storage Service (Amazon S3)-Buckets Anfragen zur Verwendung von Secure Socket Layer (SSL)-Buckets erfordern. Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen zu
SC-13	Das Informationssystem implementiert [Zuordnung: von der Organisation definierte kryptografische Verwendungszwecke und Art der für jeden Verwendungszweck erforderlichen Kryptografie] in Übereinstimmung mit den geltenden Bundesgesetzen, Executive Orders, Richtlinien, Grundsätzen, Vorschriften und Standards.	sagemaker-endpoint-configuration-kms-key-konfiguriert	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass die Verschlüsselung mit dem AWS Key Management Service (AWS KMS) für Ihren Endpunkt aktiviert ist. SageMaker Da sensible Daten auf dem SageMaker Endgerät gespeichert werden können, sollten Sie die Verschlüsselung im Ruhezustand aktivieren, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen zu
SC-13	Das Informationssystem implementiert [Zuordnung: von der Organisation definierte kryptografische Verwendungszwecke und Art der für jeden Verwendungszweck erforderlichen Kryptografie] in Übereinstimmung mit den geltenden Bundesgesetzen, Executive Orders, Richtlinien, Grundsätzen, Vorschriften und Standards.	sagemaker-notebook-instance-kms-schlüsselkonfiguriert	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass die Verschlüsselung mit dem AWS Key Management Service (AWS KMS) für Ihr Notebook aktiviert ist. SageMaker Da vertrauliche Daten im SageMaker Notebook gespeichert werden können, sollten Sie die Verschlüsselung im Ruhezustand aktivieren, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen zu
SC-13	Das Informationssystem implementiert [Zuordnung: von der Organisation definierte kryptografische Verwendungszwecke und Art der für jeden Verwendungszweck erforderlichen Kryptografie] in Übereinstimmung mit den geltenden Bundesgesetzen, Executive Orders, Richtlinien, Grundsätzen, Vorschriften und Standards.	sns-encrypted-kms	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass Ihre Amazon Simple Notification Service (Amazon SNS) -Themen mit dem AWS Key Management Service (AWS KMS) verschlüsselt werden müssen. Um eventuell vorhandene sensible Daten im Ruhezustand in veröffentlichten Nachrichten zu schützen, muss die Verschlüsselung von Daten im Ruhezustand aktiviert sein.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen zu
SC-13	Das Informationssystem setzt FIPS-validierte oder NSA-zugelassene Kryptographie in Übereinstimmung mit den geltenden Bundesgesetzen, Executive Orders, Direktiven, Richtlinien, Vorschriften und Standards ein.	dynamodb-table-encrypted-kms	Stellen Sie sicher, dass die Verschlüsselung für Ihre Amazon-DynamoDB-Tabellen aktiviert ist. Um eventuell vorhandene sensible Daten im Ruhezustand in diesen Tabellen zu schützen, müssen Sie die Verschlüsselung von Daten im Ruhezustand aktivieren. Standardmäßig werden DynamoDB-Tabellen mit einem AWS eigenen Kundenhauptschlüssel (CMK) verschlüsselt.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen zu
SC-23	Das Informationssystem schützt die Authentizität der Kommunikationssitzungen.	alb-http-to-https-Umleitungsprüfung	Um Daten während der Übertragung zu schützen, stellen Sie sicher, dass Ihr Application Load Balancer unverschlüsselte HTTP-Anfragen automatisch an HTTPS umleitet. Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.
SC-23	Das Informationssystem schützt die Authentizität der Kommunikationssitzungen.	alb-http-drop-invalid-Header-fähig	Stellen Sie sicher, dass Ihre Elastic Load Balancers (ELB) so konfiguriert sind, dass sie HTTP-Header löschen. Da sensible Daten vorhanden sein können, sollten Sie die Verschlüsselung bei der Übertragung aktivieren, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen zu
SC-23	Das Informati onssystem schützt die Authentizität der Kommunikationssitz ungen.	elb-tls-https-listeners-nur	Stellen Sie sicher, dass Ihre Elastic Load Balancer (ELBs) mit SSL- oder HTTPS-Listenern konfiguriert sind. Um eventuell vorhanden e sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.
SC-28	Das Informati onssystem schützt die [Auswahl (eine oder mehrere): Vertrauli chkeit; Integrität] von [Zuweisung: von der Organisation definiert e ruhende Informati onen].	api-gw-cache-enabl ed-und verschlüsselt	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass die Verschlüsselung für den Cache Ihrer API-Gateway-Stufe aktiviert ist. Da für die API-Methode sensible Daten erfasst werden können, sollten Sie die Verschlüs selung von Daten im Ruhezustand aktiviere n, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen zu
SC-28	Das Informationssystem schützt die [Auswahl (eine oder mehrere): Vertraulichkeit; Integrität] von [Zuweisung: von der Organisation definierte ruhende Informationen].	cloud-trail-encryption-enabled	Da sensible Daten vorhanden sein können und um Daten im Ruhezustand zu schützen, sollten Sie sicherstellen, dass die Verschlüsselung für Ihre AWS CloudTrail Trails aktiviert ist.
SC-28	Das Informationssystem schützt die [Auswahl (eine oder mehrere): Vertraulichkeit; Integrität] von [Zuweisung: von der Organisation definierte ruhende Informationen].	cloudwatch-log-group-encrypted	Um sensible Daten im Speicher zu schützen, stellen Sie sicher, dass die Verschlüsselung für Ihre Amazon CloudWatch Log Groups aktiviert ist.
SC-28	Das Informationssystem schützt die [Auswahl (eine oder mehrere): Vertraulichkeit; Integrität] von [Zuweisung: von der Organisation definierte ruhende Informationen].	efs-encrypted-check	Aktivieren Sie die Verschlüsselung für Ihr Amazon Elastic File System (EFS), um eventuell vorhandene sensible Daten sowie Daten im Ruhezustand zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen zu
SC-28	Das Informationssystem schützt die [Auswahl (eine oder mehrere): Vertraulichkeit; Integrität] von [Zuweisung: von der Organisation definierte ruhende Informationen].	elasticsearch-encrypted-at-rest	Da sensible Daten vorhanden sein können und um Daten im Ruhezustand zu schützen, sollten Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon OpenSearch Service (OpenSearch Service)-Domains aktiviert ist.
SC-28	Das Informationssystem schützt die [Auswahl (eine oder mehrere): Vertraulichkeit; Integrität] von [Zuweisung: von der Organisation definierte ruhende Informationen].	encrypted-volumes	Aktivieren Sie die Verschlüsselung für Ihre Amazon-Elastic-Block-Store (Amazon-EBS)-Volumes, um eventuell vorhandene sensible Daten sowie Daten im Ruhezustand zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen zu
SC-28	Das Informationssystem schützt die [Auswahl (eine oder mehrere): Vertraulichkeit; Integrität] von [Zuweisung: von der Organisation definierte ruhende Informationen].	kms-cmk-not-scheduled-zum Löschen	Um Daten im Ruhezustand zu schützen, sollten Sie sicherstellen, dass die für den Kunden erforderlichen Masterschlüssel (CMKs) nicht für das Löschen im AWS Key Management Service (AWS KMS) vorgesehen sind. Da Schlüssel manchmal gelöscht werden müssen, können Sie mit dieser Regel alle zu löschenden Schlüssel überprüfen, falls ein Schlüssel versehentlich zur Löschung vorgemerkt wurde.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen zu
SC-28	Das Informationssystem schützt die [Auswahl (eine oder mehrere): Vertraulichkeit; Integrität] von [Zuweisung: von der Organisation definierte ruhende Informationen].	redshift-cluster-configuration-check	Um Daten im Ruhezustand zu schützen, muss die Verschlüsselung für Ihre Amazon-Redshift-Cluster aktiviert sein. Sie müssen auch sicherstellen, dass die erforderlichen Konfigurationen auf Amazon-Redshift-Clustern bereitgestellt werden. Die Prüfungsprotokollierung muss aktiviert sein, um Informationen zu Verbindungen und Benutzeraktivitäten in der Datenbank bereitzustellen. Diese Regel erfordert, dass ein Wert für clusterDbEncrypted (Config Default: TRUE) und LoggingEnabled (Config Default: TRUE) gesetzt ist. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen zu
SC-28	Das Informati onssystem schützt die [Auswahl (eine oder mehrere): Vertrauli chkeit; Integrität] von [Zuweisung: von der Organisation definiert e ruhende Informati onen].	s3- bucket-default-loc k-enabled	Stellen Sie sicher, dass für Ihren Amazon Simple Storage Service (Amazon S3)-Bucke t standardmäßig eine Sperre aktiviert ist. Zum Schutz eventuell vorhanden er sensibler Daten in S3-Buckets müssen Sie Objektsperren für Daten im Ruhezusta nd erzwingen.
SC-28	Das Informati onssystem schützt die [Auswahl (eine oder mehrere): Vertrauli chkeit; Integrität] von [Zuweisung: von der Organisation definiert e ruhende Informati onen].	s3- bucket-server-side -encryption -aktiviert	Zum Schutz von Daten im Ruhezusta nd müssen Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon Simple Storage Service (Amazon S3)-Bucke ts aktiviert ist. Um eventuell vorhanden e sensible Daten im Ruhezustand in Amazon-S3-Buckets zu schützen, muss die Verschlüsselung aktiviert sein.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen zu
SC-28	Das Informati onssystem schützt die [Auswahl (eine oder mehrere): Vertrauli chkeit; Integrität] von [Zuweisung: von der Organisation definiert e ruhende Informati onen].	sagemaker-endpoint -configuration-kms-key-konfiguriert	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass die Verschlüsselung mit dem AWS Key Management Service (AWS KMS) für Ihren Endpunkt aktiviert ist. SageMaker Da sensible Daten auf dem SageMaker Endgerät gespeiche rt werden können, sollten Sie die Verschlüsselung im Ruhezustand aktiviere n, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen zu
SC-28	Das Informati onssystem schützt die [Auswahl (eine oder mehrere): Vertrauli chkeit; Integrität] von [Zuweisung: von der Organisation definiert e ruhende Informati onen].	sagemaker-notebook -instance-kms-schl üsselkonfiguriert	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass die Verschlüsselung mit dem AWS Key Management Service (AWS KMS) für Ihr Notebook aktiviert ist. SageMaker Da vertrauliche Daten im SageMaker Notebook gespeichert werden können, sollten Sie die Verschlüsselung im Ruhezustand aktivieren, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen zu
SC-28	Das Informati onssystem schützt die [Auswahl (eine oder mehrere): Vertrauli chkeit; Integrität] von [Zuweisung: von der Organisation definiert e ruhende Informati onen].	sns-encrypted-kms	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass Ihre Amazon Simple Notification Service (Amazon SNS) -Themen mit dem AWS Key Management Service (AWS KMS) verschlüsselt werden müssen. Um eventuell vorhandene sensible Daten im Ruhezusta nd in veröffentlichten Nachrichten zu schützen, muss die Verschlüsselung von Daten im Ruhezusta nd aktiviert sein.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen zu
SC-28	Das Informati onssystem schützt die [Auswahl (eine oder mehrere): Vertrauli chkeit; Integrität] von [Zuweisung: von der Organisation definiert e ruhende Informati onen].	ec2- ebs-encryption-by-default	Zum Schutz von Daten im Ruhezusta nd müssen Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon Elastic Block Store (Amazon EBS)-Volu mes aktiviert ist. Da sensible Daten auch im Ruhezusta nd vorhanden sein können, sollten Sie die Verschlüsselung im Ruhezustand aktivieren, um diese Daten zu schützen.
SC-28	Das Informati onssystem schützt die [Auswahl (eine oder mehrere): Vertrauli chkeit; Integrität] von [Zuweisung: von der Organisation definiert e ruhende Informati onen].	rds-snapshot-encry pted	Stellen Sie sicher, dass die Verschlüs selung für Ihre Amazon Relationa l Database Service (Amazon RDS)-Snap shots aktiviert ist. Da sensible Daten auch im Ruhezusta nd vorhanden sein können, sollten Sie die Verschlüsselung im Ruhezustand aktivieren, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen zu
SC-28	Das Informati onssystem schützt die [Auswahl (eine oder mehrere): Vertrauli chkeit; Integrität] von [Zuweisung: von der Organisation definiert e ruhende Informati onen].	rds-storage-encrypted	Zum Schutz von Daten im Ruhezusta nd müssen Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon Relational Database Service (Amazon RDS)-Instances aktiviert ist. Da sensible Daten in Amazon-RDS-Instances gespeiche rt werden können, sollten Sie die Verschlüsselung von Daten im Ruhezusta nd aktivieren, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen zu
SC-36	Die Organisation verteilt [Zuweisung: organisationsdefinierte Verarbeitung und Speicherung] auf mehrere physische Standorte.	rds-multi-az-support	Die Multi-AZ-Unterstützung in Amazon Relational Database Service (Amazon RDS) bietet eine verbesserte Verfügbarkeit und Beständigkeit von Datenbank-Instances. Wenn Sie eine Multi-AZ-Datenbank-Instance bereitstellen, erstellt Amazon RDS automatisch eine primäre Datenbank-Instance und repliziert die Daten synchron auf eine Standby-Instance in einer anderen Availability Zone. Jede Availability Zone läuft auf einer eigenen, physisch getrennten, unabhängigen Infrastruktur und ist auf eine hohe Verfügbarkeit ausgelegt. Im Falle eines Infrastrukturausfalls führt Amazon RDS einen automatis

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen zu
			chen Failover zum Standby-Modus durch, sodass Sie den Datenbankbetrieb wieder aufnehmen können, sobald der Failover abgeschlo ssen ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen zu
SC-36	Die Organisation verteilt [Zuweisung: organisationsdefinierte Verarbeitung und Speicherung] auf mehrere physische Standorte.	rds-cluster-multi-az-aktiviert	Die Multi-AZ-Unterstützung in Amazon Relational Database Service (Amazon RDS) bietet eine verbesserte Verfügbarkeit und Beständigkeit von Datenbank-Instances. Wenn Sie eine Multi-AZ-Datenbank-Instance bereitstellen, erstellt Amazon RDS automatisch eine primäre Datenbank-Instance und repliziert die Daten synchron auf eine Standby-Instance in einer anderen Availability Zone. Jede Availability Zone läuft auf einer eigenen, physisch getrennten, unabhängigen Infrastruktur und ist auf eine hohe Verfügbarkeit ausgelegt. Im Falle eines Infrastrukturausfalls führt Amazon RDS einen automatis

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen zu
			chen Failover zum Standby-Modus durch, sodass Sie den Datenbankbetrieb wieder aufnehmen können, sobald der Failover abgeschlo ssen ist.
SC-36	Die Organisation verteilt [Zuweisung: organisationsdefin ierte Verarbeitung und Speicherung] auf mehrere physische Standorte.	s3- bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) unterstützt die Aufrechterhaltung einer angemesse nen Kapazität und Verfügbarkeit. CRR ermöglicht das automatische, asynchrone Kopieren von Objekten in Amazon S3 Buckets, um die Datenverf ügbarkeit sicherzus tellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen zu
SI-2(2)	Die Organisation setzt automatisierte Mechanismen [Zuordnung: von der Organisation festgelegte Häufigkeit] ein, um den Zustand der Komponenten des Informationssystems im Hinblick auf die Behebung von Fehlern zu bestimmen.	ec2-prüfen managedinstance-patch-compliance-status	Aktivieren Sie diese Regel, um bei der Identifizierung und Dokumentation von Sicherheitslücken in Amazon Elastic Compute Cloud (Amazon EC2) zu helfen. Die Regel prüft, ob die EC2 Amazon-Instance die Patch-Konformität im AWS Systems Manager gemäß den Richtlinien und Verfahren Ihrer Organisation einhält.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen zu
SI-2(2)	Die Organisation setzt automatisierte Mechanismen [Zuordnung: von der Organisation festgelegte Häufigkeit] ein, um den Zustand der Komponenten des Informationssystems im Hinblick auf die Behebung von Fehlern zu bestimmen.	ec2-managerinstance-managed-by-systems	Eine Bestandsaufnahme der Softwareplattformen und Anwendungen innerhalb des Unternehmens ist möglich, indem Amazon Elastic Compute Cloud (Amazon EC2) - Instances mit AWS Systems Manager verwaltet werden. Verwenden Sie AWS Systems Manager, um detaillierte Systemkonfigurationen, Betriebssystem-Patch-Levels, Namen und Typ der Dienste, Softwareinstallationen, Anwendungsname, Herausgeber und Version sowie andere Details zu Ihrer Umgebung bereitzustellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen zu
SI-2(2)	Die Organisation setzt automatisierte Mechanismen [Zuordnung: von der Organisation festgelegte Häufigkeit] ein, um den Zustand der Komponenten des Informationssystems im Hinblick auf die Behebung von Fehlern zu bestimmen.	ec2-check managedinstance-association-compliance-status	Verwenden Sie AWS Systems Manager Associations, um bei der Inventarisierung von Softwareplattformen und Anwendungen innerhalb eines Unternehmens zu helfen. AWS Systems Manager weist Ihren verwalteten Instances einen Konfigurationsstatus zu und ermöglicht es Ihnen, Basiswerte für Betriebssystem-Patch-Levels, Softwareinstallationen, Anwendungskonfigurationen und andere Details zu Ihrer Umgebung festzulegen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen zu
SI-4(1)	Die Organisation verbindet und konfiguriert die einzelnen Intrusion-Detection-Tools zu einem informationssystemweiten Intrusion-Detection-System.	guardduty-enabled-centralized	Amazon GuardDuty kann mithilfe von Threat Intelligence Feeds helfen, potenzielle Cybersicherheitsereignisse zu überwachen und zu erkennen. Dazu gehören Listen mit bösartigen IPs und maschinellen Lernmethoden zur Identifizierung unerwarteter, nicht autorisierter und bösartiger Aktivitäten in Ihrer AWS Cloud-Umgebung.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen zu
SI-4(2)	Die Organisation setzt automatisierte Tools ein, um die Analyse von Ereignissen nahezu in Echtzeit zu unterstützen.	guardduty-enabled-centralized	Amazon GuardDuty kann mithilfe von Threat Intelligence Feeds helfen, potenzielle Cybersicherheitsereignisse zu überwachen und zu erkennen. Dazu gehören Listen mit bösartigen IPs und maschinellen Lernmethoden zur Identifizierung unerwarteter, nicht autorisierter und bösartiger Aktivitäten in Ihrer AWS Cloud-Umgebung.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen zu
SI-4(2)	Die Organisation setzt automatisierte Tools ein, um die Analyse von Ereignissen nahezu in Echtzeit zu unterstützen.	securityhub-enabled	AWS Security Hub hilft bei der Überwachung von unbefugtem Personal, Verbindungen, Geräten und Software. AWS Security Hub aggregiert, organisiert und priorisiert die Sicherheitswarnungen oder Ergebnisse mehrerer Dienste. AWS Einige dieser Dienste sind Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer und AWS Firewall Manager sowie AWS Partnerlösungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen zu
SI-4(2)	Die Organisation setzt automatisierte Tools ein, um die Analyse von Ereignissen nahezu in Echtzeit zu unterstützen.	cloudwatch-alarm-action-check	Amazon CloudWatch alarmiert, wenn eine Metrik den Schwellenwert für eine bestimmte Anzahl von Bewertungszeiträumen überschreitet. Der Alarm führt eine oder mehrere Aktionen durch, die vom Wert der Metrik oder des Ausdrucks im Vergleich zu einem Schwellenwert in einer Reihe von Zeiträumen abhängt. Diese Regel erfordert einen Wert für alarmActionRequired (Config Default: True), insufficientDataAction Required (Config Default: True), okActionRequired (Config Default: False). Der tatsächliche Wert muss die Alarmaktionen für Ihre Umgebung widerspiegeln.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen zu
SI-4(2)	Die Organisation setzt automatisierte Tools ein, um die Analyse von Ereignissen nahezu in Echtzeit zu unterstützen.	cloud-trail-cloud-watch-logs-aktiviert	Verwenden Sie Amazon CloudWatch , um Protokoll ereignisaktivitäten zentral zu sammeln und zu verwalten. Die Aufnahme von AWS CloudTrail Daten liefert Einzelheiten zu den API-Aufrufaktivitäten in Ihrem AWS-Konto.
SI-4(2)	Die Organisation setzt automatisierte Tools ein, um die Analyse von Ereignissen nahezu in Echtzeit zu unterstützen.	ec-2 instance-detailed-monitoring-enabled	Aktivieren Sie diese Regel, um die Amazon Elastic Compute Cloud (Amazon EC2) - Instance-Überwachung auf der EC2 Amazon-Konsole zu verbessern, in der Monitoring-Diagramme mit einem Zeitraum von 1 Minute für die Instance angezeigt werden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen zu
SI-4(4)	Das Informati onssystem überwacht den ein- und ausgehenden Kommunikationsverk ehr [Zuordnung: vom Unternehmen festgelegte Häufigkei t] auf ungewöhnl iche oder unzulässi ge Aktivitäten oder Bedingungen.	guardduty-enabled-centralized	Amazon GuardDuty kann mithilfe von Threat Intellige nce Feeds helfen, potenzielle Cybersich erheitsereignisse zu überwachen und zu erkennen. Dazu gehören Listen mit bösartigen IPs und maschinel len Lernmethoden zur Identifizierung unerwarteter, nicht autorisierter und bösartiger Aktivitäten in Ihrer AWS Cloud-Umgebung.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen zu
SI-4(4)	Das Informationssystem überwacht den ein- und ausgehenden Kommunikationsverkehr [Zuordnung: vom Unternehmen festgelegte Häufigkeit] auf ungewöhnliche oder unzulässige Aktivitäten oder Bedingungen.	securityhub-enabled	AWS Security Hub hilft bei der Überwachung von unbefugtem Personal, Verbindungen, Geräten und Software. AWS Security Hub aggregiert, organisiert und priorisiert die Sicherheitswarnungen oder Ergebnisse mehrerer Dienste. AWS Einige dieser Dienste sind Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer und AWS Firewall Manager sowie AWS Partnerlösungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen zu
SI-4(4)	Das Informationssystem überwacht den ein- und ausgehenden Kommunikationsverkehr [Zuordnung: vom Unternehmen festgelegte Häufigkeit] auf ungewöhnliche oder unzulässige Aktivitäten oder Bedingungen.	cloudwatch-alarm-action-check	Amazon CloudWatch alarmiert, wenn eine Metrik den Schwellenwert für eine bestimmte Anzahl von Bewertungszeiträumen überschreitet. Der Alarm führt eine oder mehrere Aktionen durch, die vom Wert der Metrik oder des Ausdrucks im Vergleich zu einem Schwellenwert in einer Reihe von Zeiträumen abhängt. Diese Regel erfordert einen Wert für alarmActionRequired (Config Default: True), insufficientDataAction Required (Config Default: True), okActionRequired (Config Default: False). Der tatsächliche Wert muss die Alarmaktionen für Ihre Umgebung widerspiegeln.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen zu
SI-4(4)	Das Informationssystem überwacht den ein- und ausgehenden Kommunikationsverkehr [Zuordnung: vom Unternehmen festgelegte Häufigkeit] auf ungewöhnliche oder unzulässige Aktivitäten oder Bedingungen.	cloud-trail-cloud-watch-logs-aktiviert	Verwenden Sie Amazon CloudWatch , um Protokollereignisaktivitäten zentral zu sammeln und zu verwalten. Die Aufnahme von AWS CloudTrail Daten liefert Einzelheiten zu den API-Aufrufaktivitäten in Ihrem AWS-Konto.
SI-4(5)	Das Informationssystem alarmiert [Zuweisung: von der Organisation ernanntes Personal oder definierte Rollen], wenn die folgenden Anzeichen für eine bestehende oder potenzielle Gefährdung auftreten: [Zuweisung: von der Organisation definierte Gefährdungsindikatoren].	guardduty-enabled-centralized	Amazon GuardDuty kann mithilfe von Threat Intelligence Feeds helfen, potenzielle Cybersicherheitsereignisse zu überwachen und zu erkennen. Dazu gehören Listen mit bösartigen IPs und maschinellen Lernmethoden zur Identifizierung unerwarteter, nicht autorisierter und bösartiger Aktivitäten in Ihrer AWS Cloud-Umgebung.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen zu
SI-4(5)	Das Informati onssystem alarmiert [Zuweisung: von der Organisation ernanntes Personal oder definierte Rollen], wenn die folgenden Anzeichen für eine bestehend e oder potenzielle Gefährdung auftreten : [Zuweisung: von der Organisation definiert e Gefährdungsindikat oren].	securityhub-enabled	AWS Security Hub hilft bei der Überwachung von unbefugtem Personal, Verbindun gen, Geräten und Software. AWS Security Hub aggregiert, organisie rt und priorisie rt die Sicherhei tswarnungen oder Ergebnisse mehrerer Dienste. AWS Einig e dieser Dienste sind Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer und AWS Firewall Manager sowie AWS Partnerlösungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen zu
SI-4(5)	Das Informationssystem alarmiert [Zuweisung: von der Organisation ernanntes Personal oder definierte Rollen], wenn die folgenden Anzeichen für eine bestehende oder potenzielle Gefährdung auftreten: [Zuweisung: von der Organisation definierte Gefährdungsindikatoren].	cloudwatch-alarm-action-check	Amazon CloudWatch alarmiert, wenn eine Metrik den Schwellenwert für eine bestimmte Anzahl von Bewertungszeiträumen überschreitet. Der Alarm führt eine oder mehrere Aktionen durch, die vom Wert der Metrik oder des Ausdrucks im Vergleich zu einem Schwellenwert in einer Reihe von Zeiträumen abhängt. Diese Regel erfordert einen Wert für alarmActionRequired (Config Default: True), insufficientDataAction Required (Config Default: True), okActionRequired (Config Default: False). Der tatsächliche Wert muss die Alarmaktionen für Ihre Umgebung widerspiegeln.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen zu
SI-4(5)	Das Informati onssystem alarmiert [Zuweisung: von der Organisation ernanntes Personal oder definierte Rollen], wenn die folgenden Anzeichen für eine bestehend e oder potenzielle Gefährdung auftreten : [Zuweisung: von der Organisation definiert e Gefährdungsindikat oren].	cloud-trail-cloud-watch-logs-aktiviert	Verwenden Sie Amazon CloudWatc h , um Protokoll ereignisaktivitäten zentral zu sammeln und zu verwalten. Die Aufnahme von AWS CloudTrail Daten liefert Einzelheiten zu den API-Aufrufaktivitä ten in Ihrem AWS-Konto.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen zu
SI-4(16)	Die Organisation korreliert Informati onen aus Überwachu ngstools, die im gesamten Informati onssystem eingesetzt werden.	guardduty-enabled-centralized	Amazon GuardDuty kann mithilfe von Threat Intellige nce Feeds helfen, potenzielle Cybersich erheitsereignisse zu überwachen und zu erkennen. Dazu gehören Listen mit bösartigen IPs und maschinel len Lernmethoden zur Identifizierung unerwarteter, nicht autorisierter und bösartiger Aktivitäten in Ihrer AWS Cloud-Umgebung.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen zu
SI-4(16)	Die Organisation korreliert Informati onen aus Überwachu ngstools, die im gesamten Informati onssystem eingesetzt werden.	securityhub-enabled	AWS Security Hub hilft bei der Überwachung von unbefugtem Personal, Verbindun gen, Geräten und Software. AWS Security Hub aggregiert, organisie rt und priorisie rt die Sicherhei tswarnungen oder Ergebnisse mehrerer Dienste. AWS Einig e dieser Dienste sind Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer und AWS Firewall Manager sowie AWS Partnerlösungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen zu
SI-4(a)(b)(c)	Die Organisation: a. Überwacht das Informationssystem und erkennt: 1. Angriffe und Indikatoren für potenzielle Angriffe in Übereinstimmung mit [Zuweisung: von der Organisation festgelegte Überwachungsziele]; und 2. Nicht autorisierte lokale Verbindungen sowie Netzwerk- und Remoteverbindungen; b. Identifiziert die unbefugte Nutzung des Informationssystems durch [Zuweisung: von der Organisation festgelegte Techniken und Methoden]; c. Verwendet Überwachungsgeräte: i. strategisch innerhalb des Informationssystems, um von der Organisation festgelegte wesentliche Informationen zu sammeln;	guardduty-enabled-centralized	Amazon GuardDuty kann mithilfe von Threat Intelligence Feeds helfen, potenzielle Cybersicherheitsereignisse zu überwachen und zu erkennen. Dazu gehören Listen mit bösartigen IPs und maschinellen Lernmethoden zur Identifizierung unerwarteter, nicht autorisierter und bösartiger Aktivitäten in Ihrer AWS Cloud-Umgebung.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen zu
	und ii) an Ad-hoc-St andorten innerhalb des Systems, um bestimmte Arten von Vorgängen zu verfolgen, die für die Organisation von Interesse sind.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen zu
SI-4(a)(b)(c)	Die Organisation: a. Überwacht das Informationssystem und erkennt: 1. Angriffe und Indikatoren für potenzielle Angriffe in Übereinstimmung mit [Zuweisung: von der Organisation festgelegte Überwachungsziele]; und 2. Nicht autorisierte lokale Verbindungen sowie Netzwerk- und Remoteverbindungen; b. Identifiziert die unbefugte Nutzung des Informationssystems durch [Zuweisung: von der Organisation festgelegte Techniken und Methoden]; c. Verwendet Überwachungsgeräte: i. strategisch innerhalb des Informationssystems, um von der Organisation festgelegte wesentliche Informationen zu sammeln;	guardduty-non-archived-findings	Amazon GuardDuty hilft Ihnen dabei, die Auswirkungen eines Vorfalls zu verstehen, indem es die Ergebnisse nach Schweregrad klassifiziert: niedrig, mittel und hoch. Diese Klassifizierungen können Sie zur Festlegung von entsprechenden Strategien und Prioritäten zur Behebung solcher Vorfälle verwenden. Mit dieser Regel können Sie optional daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7) und daysHighSev (Config Default: 1) für nicht archivierte Ergebnisse festlegen, wie es die Richtlinien Ihrer Organisation erfordern.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen zu
	und ii) an Ad-hoc-St andorten innerhalb des Systems, um bestimmte Arten von Vorgängen zu verfolgen, die für die Organisation von Interesse sind.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen zu
SI-4(a)(b)(c)	Die Organisation: a. Überwacht das Informationssystem und erkennt: 1. Angriffe und Indikatoren für potenzielle Angriffe in Übereinstimmung mit [Zuweisung: von der Organisation festgelegte Überwachungsziele]; und 2. Nicht autorisierte lokale Verbindungen sowie Netzwerk- und Remoteverbindungen; b. Identifiziert die unbefugte Nutzung des Informationssystems durch [Zuweisung: von der Organisation festgelegte Techniken und Methoden]; c. Verwendet Überwachungsgeräte: i. strategisch innerhalb des Informationssystems, um von der Organisation festgelegte wesentliche Informationen zu sammeln;	alb-waf-enabled	Stellen Sie sicher, dass AWS WAF auf Elastic Load Balancers (ELB) aktiviert ist, um Webanwendungen zu schützen. Eine WAF trägt zum Schutz Ihrer Webanwendungen oder APIs vor gängigen Web-Exploits bei. Diese Web-Exploits können sich auf die Verfügbarkeit auswirken, die Sicherheit gefährden oder übermäßige Ressourcen in Ihrer Umgebung verbrauchen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen zu
	und ii) an Ad-hoc-St andorten innerhalb des Systems, um bestimmte Arten von Vorgängen zu verfolgen, die für die Organisation von Interesse sind.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen zu
SI-4(a)(b)(c)	Die Organisation: a. Überwacht das Informationssystem und erkennt: 1. Angriffe und Indikatoren für potenzielle Angriffe in Übereinstimmung mit [Zuweisung: von der Organisation festgelegte Überwachungsziele]; und 2. Nicht autorisierte lokale Verbindungen sowie Netzwerk- und Remoteverbindungen; b. Identifiziert die unbefugte Nutzung des Informationssystems durch [Zuweisung: von der Organisation festgelegte Techniken und Methoden]; c. Verwendet Überwachungsgeräte: i. strategisch innerhalb des Informationssystems, um von der Organisation festgelegte wesentliche Informationen zu sammeln;	wafv2-logging-enabled	Um die Protokollierung und Überwachung in Ihrer Umgebung zu erleichtern, aktivieren Sie die AWS WAF (V2) -Protokollierung im regionalen und globalen Web. ACLs AWS Die WAF-Protokollierung bietet detaillierte Informationen über den Datenverkehr, der von Ihrer Web-ACL analysiert wird. In den Protokollen werden die Uhrzeit aufgezeichnet, zu der die AWS WAF die Anfrage von Ihrer AWS Ressource erhalten hat, Informationen über die Anfrage und eine Aktion für die Regel, der jede Anfrage entsprach.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen zu
	und ii) an Ad-hoc-St andorten innerhalb des Systems, um bestimmte Arten von Vorgängen zu verfolgen, die für die Organisation von Interesse sind.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen zu
SI-4(a)(b)(c)	Die Organisation: a. Überwacht das Informationssystem und erkennt: 1. Angriffe und Indikatoren für potenzielle Angriffe in Übereinstimmung mit [Zuweisung: von der Organisation festgelegte Überwachungsziele]; und 2. Nicht autorisierte lokale Verbindungen sowie Netzwerk- und Remoteverbindungen; b. Identifiziert die unbefugte Nutzung des Informationssystems durch [Zuweisung: von der Organisation festgelegte Techniken und Methoden]; c. Verwendet Überwachungsgeräte: i. strategisch innerhalb des Informationssystems, um von der Organisation festgelegte wesentliche Informationen zu sammeln;	securityhub-enabled	AWS Security Hub hilft bei der Überwachung von unbefugtem Personal, Verbindungen, Geräten und Software. AWS Security Hub aggregiert, organisiert und priorisiert die Sicherheitswarnungen oder Ergebnisse mehrerer Dienste. AWS Einige dieser Dienste sind Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer und AWS Firewall Manager sowie AWS Partnerlösungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen zu
	und ii) an Ad-hoc-St andorten innerhalb des Systems, um bestimmte Arten von Vorgängen zu verfolgen, die für die Organisation von Interesse sind.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen zu
SI-4(a)(b)(c)	Die Organisation: a. Überwacht das Informationssystem und erkennt: 1. Angriffe und Indikatoren für potenzielle Angriffe in Übereinstimmung mit [Zuweisung: von der Organisation festgelegte Überwachungsziele]; und 2. Nicht autorisierte lokale Verbindungen sowie Netzwerk- und Remoteverbindungen; b. Identifiziert die unbefugte Nutzung des Informationssystems durch [Zuweisung: von der Organisation festgelegte Techniken und Methoden]; c. Verwendet Überwachungsgeräte: i. strategisch innerhalb des Informationssystems, um von der Organisation festgelegte wesentliche Informationen zu sammeln;	cloudwatch-alarm-action-check	Amazon CloudWatch alarmiert, wenn eine Metrik den Schwellenwert für eine bestimmte Anzahl von Bewertungszeiträumen überschreitet. Der Alarm führt eine oder mehrere Aktionen durch, die vom Wert der Metrik oder des Ausdrucks im Vergleich zu einem Schwellenwert in einer Reihe von Zeiträumen abhängt. Diese Regel erfordert einen Wert für alarmActionRequired (Config Default: True), insufficientDataAction Required (Config Default: True), okActionRequired (Config Default: False). Der tatsächliche Wert muss die Alarmaktionen für Ihre Umgebung widerspiegeln.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen zu
	und ii) an Ad-hoc-St andorten innerhalb des Systems, um bestimmte Arten von Vorgängen zu verfolgen, die für die Organisation von Interesse sind.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen zu
SI-4(a)(b)(c)	Die Organisation: a. Überwacht das Informationssystem und erkennt: 1. Angriffe und Indikatoren für potenzielle Angriffe in Übereinstimmung mit [Zuweisung: von der Organisation festgelegte Überwachungsziele]; und 2. Nicht autorisierte lokale Verbindungen sowie Netzwerk- und Remoteverbindungen; b. Identifiziert die unbefugte Nutzung des Informationssystems durch [Zuweisung: von der Organisation festgelegte Techniken und Methoden]; c. Verwendet Überwachungsgeräte: i. strategisch innerhalb des Informationssystems, um von der Organisation festgelegte wesentliche Informationen zu sammeln;	cloud-trail-cloud-watch-logs-aktiviert	Verwenden Sie Amazon CloudWatch , um Protokoll ereignisaktivitäten zentral zu sammeln und zu verwalten. Die Aufnahme von AWS CloudTrail Daten liefert Einzelheiten zu den API-Aufrufaktivitäten in Ihrem AWS-Konto.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen zu
	und ii) an Ad-hoc-St andorten innerhalb des Systems, um bestimmte Arten von Vorgängen zu verfolgen, die für die Organisation von Interesse sind.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen zu
SI-4(a)(b)(c)	Die Organisation: a. Überwacht das Informationssystem und erkennt: 1. Angriffe und Indikatoren für potenzielle Angriffe in Übereinstimmung mit [Zuweisung: von der Organisation festgelegte Überwachungsziele]; und 2. Nicht autorisierte lokale Verbindungen sowie Netzwerk- und Remoteverbindungen; b. Identifiziert die unbefugte Nutzung des Informationssystems durch [Zuweisung: von der Organisation festgelegte Techniken und Methoden]; c. Verwendet Überwachungsgeräte: i. strategisch innerhalb des Informationssystems, um von der Organisation festgelegte wesentliche Informationen zu sammeln;	ec-2 instance-detailed-monitoring-enabled	Aktivieren Sie diese Regel, um die Amazon Elastic Compute Cloud (Amazon EC2) - Instance-Überwachung auf der EC2 Amazon-Konsole zu verbessern, in der Monitoring-Diagramme mit einem Zeitraum von 1 Minute für die Instance angezeigt werden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen zu
	und ii) an Ad-hoc-St andorten innerhalb des Systems, um bestimmte Arten von Vorgängen zu verfolgen, die für die Organisation von Interesse sind.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen zu
SI-7	Die Organisation verwendet Tools zur Integritätsprüfung , um unbefugte Änderungen an [Zuweisung: von der Organisation definiert e Software, Firmware und Informationen] zu erkennen.	cloud-trail-log-file-Validierung aktiviert	Verwenden Sie die AWS CloudTrail Protokolldateivali dierung, um die Integrität von Protokoll en zu überprüfen. CloudTrail Mithilfe der Protokolldateivali dierung kann festgestellt werden, ob eine Protokoll datei geändert oder gelöscht wurde oder ob sie nach der Übermittlung CloudTrail unverände rt geblieben ist. Dieses Feature wurde mit dem Branchens tandard entsprech enden Algorithmen entwickelt: SHA-256 für die Hashfunktion und SHA-256 mit RSA für digitale Signature n. Aus diesem Grund ist es rechnerisch unmöglich, CloudTrai l Protokolldateien unbemerkt zu ändern, zu löschen oder zu fälschen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen zu
SI-7(1)	Das Informationssystem führt eine Integritätsprüfung von [Zuordnung: organisationsdefinierte Software, Firmware und Informationen] [Auswahl (eine oder mehrere): beim Start; bei [Zuordnung: organisationsdefinierte Übergangszustände oder sicherheitsrelevante Ereignisse]; [Zuordnung: organisationsdefinierte Häufigkeit]] durch.	ec2-managerinstance-managed-by-systems	Eine Bestandsaufnahme der Softwareplattformen und Anwendungen innerhalb des Unternehmens ist möglich, indem Amazon Elastic Compute Cloud (Amazon EC2) - Instances mit AWS Systems Manager verwaltet werden. Verwenden Sie AWS Systems Manager, um detaillierte Systemkonfigurationen, Betriebssystem-Patch-Levels, Namen und Typ der Dienste, Softwareinstallationen, Anwendungsname, Herausgeber und Version sowie andere Details zu Ihrer Umgebung bereitzustellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen zu
SI-7(1)	Das Informationssystem führt eine Integritätsprüfung von [Zuordnung: organisationsdefinierte Software, Firmware und Informationen] [Auswahl (eine oder mehrere): beim Start; bei [Zuordnung: organisationsdefinierte Übergangszustände oder sicherheitsrelevante Ereignisse]; [Zuordnung: organisationsdefinierte Häufigkeit]] durch.	ec2-check managedinstance-patch-compliance-status	Aktivieren Sie diese Regel, um bei der Identifizierung und Dokumentation von Sicherheitslücken in Amazon Elastic Compute Cloud (Amazon EC2) zu helfen. Die Regel prüft, ob die EC2 Amazon-Instance die Patch-Konformität im AWS Systems Manager gemäß den Richtlinien und Verfahren Ihrer Organisation einhält.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen zu
SI-7(1)	Das Informati onssystem führt eine Integritätsprüfung von [Zuordnung: organisat ionsdefinierte Software, Firmware und Informationen] [Auswahl (eine oder mehrere): beim Start; bei [Zuordnung: organisationsdefin ierte Übergangs zustände oder sicherheitsrelevan te Ereignisse]; [Zuordnung: organisat ionsdefinierte Häufigkeit]] durch.	cloud-trail-log-file-Validierung aktiviert	Verwenden Sie die AWS CloudTrail Protokolldateivali dierung, um die Integrität von Protokoll en zu überprüfen. CloudTrail Mithilfe der Protokolldateivali dierung kann festgestellt werden, ob eine Protokoll datei geändert oder gelöscht wurde oder ob sie nach der Übermittlung CloudTrail unverände rt geblieben ist. Dieses Feature wurde mit dem Branchens tandard entsprech enden Algorithmen entwickelt: SHA-256 für die Hashfunktion und SHA-256 mit RSA für digitale Signature n. Aus diesem Grund ist es rechnerisch unmöglich, CloudTrai l Protokolldateien unbemerkt zu ändern, zu löschen oder zu fälschen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen zu
SI-12	Die Organisation verarbeitet und speichert die Informationen innerhalb des Informationssystems und die aus dem System ausgegebenen Informationen gemäß den geltenden Bundesgesetzen, Verordnungen, Richtlinien, Richtlinien, Vorschriften, Standards und betrieblichen Anforderungen.	s-3 bucket-versioning-enabled	Die Versionsverwaltung von Amazon Simple Storage Service (Amazon S3)-Buckets hilft dabei, mehrere Varianten eines Objekts im selben Amazon-S3-Bucket zu speichern. Verwenden Sie die Versionsverwaltung, um sämtliche Versionen aller Objekte in Ihrem Amazon-S3-Bucket zu speichern, abzurufen oder wiederherzustellen. Mit der Versionsverwaltung können Sie Versionen sowohl nach unbeabsichtigten Benutzeraktionen als auch nach Anwendungsfehlern problemlos wiederherstellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen zu
SI-12	Die Organisation verarbeitet und speichert die Informationen innerhalb des Informationssystems und die aus dem System ausgegebenen Informationen gemäß den geltenden Bundesgesetzen, Verordnungen, Richtlinien, Richtlinien, Vorschriften, Standards und betrieblichen Anforderungen.	db-instance-backup-enabled	Die Sicherungsfunktion von Amazon RDS erstellt Sicherungen Ihrer Datenbanken und Transaktionsprotokolle. Amazon RDS erstellt einen Snapshot für das Speichervolume Ihrer DB-Instance, sodass die gesamte DB-Instance gesichert wird. Sie können im System spezifische Aufbewahrungsfristen festlegen, um Ihre Ausfallsicherheitsanforderungen zu erfüllen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen zu
SI-12	Die Organisation verarbeitet und speichert die Informationen innerhalb des Informationssystems und die aus dem System ausgegebenen Informationen gemäß den geltenden Bundesgesetzen, Verordnungen, Richtlinien, Richtlinien, Vorschriften, Standards und betrieblichen Anforderungen.	dynamodb-pitr-enabled	Aktivieren Sie diese Regel, um zu überprüfen, ob die Informationen gesichert wurden. Es verwaltet auch die Backups, indem es sicherstellt, dass die point-in-time Wiederherstellung in Amazon DynamoDB aktiviert ist. Bei der Wiederherstellung werden fortlaufende Backups Ihrer Tabelle für die letzten 35 Tage gespeichert.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen zu
SI-12	Die Organisation verarbeitet und speichert die Informationen innerhalb des Informationssysteme und die aus dem System ausgegebenen Informationen gemäß den geltenden Bundesgesetzen, Verordnungen, Richtlinien, Richtlinien, Vorschriften, Standards und betrieblichen Anforderungen.	elasticache-redis-cluster-automatic-Backup-Prüfung	Wenn automatische Backups aktiviert sind, ElastiCache erstellt Amazon täglich ein Backup des Clusters. Die Sicherung kann für eine von Ihrer Organisation festgelegte Anzahl von Tagen aufbewahrt werden. Automatische Backups schützen vor Datenverlust. Bei einem Ausfall können Sie einen neuen Cluster erstellen, der Ihre Daten aus dem aktuellen Backup wiederherstellt.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen zu
SI-12	Die Organisation verarbeitet und speichert die Informationen innerhalb des Informationssysteme und die aus dem System ausgegebenen Informationen gemäß den geltenden Bundesgesetzen, Verordnungen, Richtlinien, Richtlinien, Vorschriften, Standards und betrieblichen Anforderungen.	rds-in-backup-plan	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon Relational Database Service (Amazon RDS) -Instances Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen zu
SI-12	Die Organisation verarbeitet und speichert die Informationen innerhalb des Informationssystems und die aus dem System ausgegebenen Informationen gemäß den geltenden Bundesgesetzen, Verordnungen, Richtlinien, Richtlinien, Vorschriften, Standards und betrieblichen Anforderungen.	ebs-in-backup-plan	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon Elastic Block Store (Amazon EBS) -Volumes Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihre Backup-Verwaltung und ermöglicht es Ihnen, Ihre geschäftlichen und behördlichen Anforderungen bezüglich Backups zu erfüllen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen zu
SI-12	Die Organisation verarbeitet und speichert die Informationen innerhalb des Informationssystems und die aus dem System ausgegebenen Informationen gemäß den geltenden Bundesgesetzen, Verordnungen, Richtlinien, Richtlinien, Vorschriften, Standards und betrieblichen Anforderungen.	efs-in-backup-plan	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon Elastic File System (Amazon EFS) -Dateisysteme Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen zu
SI-12	Die Organisation verarbeitet und speichert die Informationen innerhalb des Informationssystems und die aus dem System ausgegebenen Informationen gemäß den geltenden Bundesgesetzen, Verordnungen, Richtlinien, Richtlinien, Vorschriften, Standards und betrieblichen Anforderungen.	dynamodb-in-backup-plan	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon DynamoDB-Tabellen Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config Regel	Empfehlungen zu
SI-12	Die Organisation verarbeitet und speichert die Informationen innerhalb des Informationssystems und die aus dem System ausgegebenen Informationen gemäß den geltenden Bundesgesetzen, Verordnungen, Richtlinien, Richtlinien, Vorschriften, Standards und betrieblichen Anforderungen.	cw-loggroup-retention-period-überprüfen	Stellen Sie sicher, dass die Ereignisprotokolldaten für Ihre Protokollgruppen über eine Mindestdauer aufbewahrt werden, um die Fehlerbehebung und forensische Untersuchungen zu unterstützen. Fehlende frühere Ereignisprotokolldaten erschweren die Rekonstruierung und Identifizierung potenziell schädlicher Ereignisse.

Vorlage

Die Vorlage ist verfügbar unter GitHub: Operational Best Practices for NIST 800-53 rev 4.

Bewährte Methoden für die Ausführung von NIST 800-53 Rev. 5

Konformitätspakete bieten ein allgemeines Compliance-Framework, das es Ihnen ermöglicht, mithilfe verwalteter oder benutzerdefinierter Regeln und Abhilfemaßnahmen Kontrollen zur Sicherheits-, Betriebs- oder Kostenoptimierung durchzuführen. AWS Config AWS Config Conformance Packs dienen als Beispielvorlagen nicht dazu, die vollständige Einhaltung eines bestimmten Governance- oder Compliance-Standards sicherzustellen. Sie sind dafür verantwortlich, selbst zu beurteilen, ob Ihre Nutzung der Services den geltenden gesetzlichen und behördlichen Anforderungen entspricht.

Im Folgenden finden Sie ein Beispiel für eine Zuordnung zwischen den NIST 800-53- und AWS verwalteten Konfigurationsregeln. Jede Config-Regel gilt für eine bestimmte AWS Ressource und bezieht sich auf eine oder mehrere NIST 800-53-Steuerelemente. Eine Kontrolle nach NIST 800-53

kann mehreren Config-Regeln zugeordnet werden. In der folgenden Tabelle finden Sie weitere Informationen und Anleitungen zu diesen Zuordnungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-2(4)	Kontoverwaltung | Automatisierte Prüfungsaktionen	elasticsearch-logs-to-cloudwatch	Stellen Sie sicher, dass für Amazon OpenSearch Service-Domains Fehlerprotokolle aktiviert und zur Aufbewahrung und Beantwortung an Amazon CloudWatch Logs gestreamt werden. Domain-Fehlerprotokolle sind bei Sicherheits- und Zugriffsprüfungen sowie bei der Diagnose von Verfügbarkeitsproblemen nützlich.
AC-2(4)	Kontoverwaltung | Automatisierte Prüfungsaktionen	multi-region-cloudtrail-enabled	AWS CloudTrail zeichnet Aktionen und API-Aufrufe der AWS Management Console auf. Sie können feststellen, welche Benutzer und Konten angerufen wurden AWS, von welcher Quell-IP-Adresse aus die Anrufe getätigt wurden und wann die Anrufe erfolgten.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			CloudTrail übermittelt Protokolldateien aus allen AWS Regionen an Ihren S3-Bucket , wenn MULTI_REG ION_CLOUD _TRAIL_ENABLED aktiviert ist. Außerdem wird beim AWS Start einer neuen Region derselbe Trail in der neuen Region erstellt. CloudTrail Dadurch erhalten Sie automatis ch Protokolldateien mit API-Aktivitäten für die neue Region.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-2(4)	Kontoverwaltung | Automatisierte Prüfungsaktionen	opensearch-logs-to-cloudwatch	Stellen Sie sicher, dass für Amazon OpenSearch Service-Domains Fehlerprotokolle aktiviert und zur Aufbewahrung und Beantwortung an Amazon CloudWatch Logs gestreamt werden. OpenSearch Service-Fehlerprotokolle können bei Sicherheits- und Zugriffsprüfungen helfen und bei der Diagnose von Verfügbarkeitsproblemen helfen.
AC-2(4)	Kontoverwaltung | Automatisierte Prüfungsaktionen	cloud-trail-cloud-watch-Logs aktiviert	Verwenden Sie Amazon CloudWatch , um Protokollereignisaktivitäten zentral zu sammeln und zu verwalten. Die Aufnahme von AWS CloudTrail Daten liefert Einzelheiten zu den API-Aufrufaktivitäten in Ihrem AWS-Konto.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-2(4)	Kontoverwaltung | Automatisierte Prüfungsaktionen	cloudtrail-enabled	AWS CloudTrail kann bei der Nichtabstreitbarkeit helfen, indem Aktionen und API-Aufrufe der AWS Management Console aufgezeichnet werden. Sie können die Benutzer und die Benutzer AWS-Konten , die einen AWS Dienst aufgerufen haben, die Quell-IP-Adresse, über die die Aufrufe generiert wurden, und den Zeitpunkt der Anrufe identifizieren. Einzelheiten zu den erfassten Daten finden Sie unter Inhalt des AWS CloudTrail Datensatzes.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-2(4)	Kontoverwaltung | Automatisierte Prüfungsaktionen	cloudtrail-s3-data events-enabled	Die Erfassung von Simple Storage Service (Amazon S3)-Datenereignissen unterstützt die Erkennung von ungewöhnlichen Aktivitäten. Zu den Details gehören AWS-Konto Informationen über den Zugriff auf einen Amazon S3 S3-Bucket, die IP-Adresse und die Uhrzeit des Ereignisses.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-2(4)	Kontoverwaltung | Automatisierte Prüfungsaktionen	rds-logging-enabled	Um die Protokollierung und Überwachung in Ihrer Umgebung zu erleichtern, stellen Sie sicher, dass die Amazon Relational Database Service (Amazon RDS)-Protokollierung aktiviert ist. Mit der Amazon-RDS-Protokollierung können Sie Ereignisse wie Verbindungen, Verbindungsabbrüche, Abfragen oder abgefragte Tabellen erfassen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-2(4)	Kontoverwaltung | Automatisierte Prüfungsaktionen	redshift-cluster-configuration-check	Um Daten im Ruhezustand zu schützen, muss die Verschlüsselung für Ihre Amazon-Redshift-Cluster aktiviert sein. Sie müssen auch sicherstellen, dass die erforderlichen Konfigurationen auf Amazon-Redshift-Clustern bereitgestellt werden. Die Prüfungsprotokollierung muss aktiviert sein, um Informationen zu Verbindungen und Benutzeraktivitäten in der Datenbank bereitzustellen. Diese Regel erfordert, dass ein Wert für clusterDbEncrypted (Config Default: TRUE) und LoggingEnabled (Config Default: TRUE) gesetzt ist. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-2(4)	Kontoverwaltung | Automatisierte Prüfungsaktionen	s3- bucket-logging-enabled	Die Amazon Simple Storage Service (Amazon S3)-Serverzugriffs protokollierung bietet eine Methode zur Überwachu ng des Netzwerks im Hinblick auf potenzielle Cybersich erheitsereignisse. Die Ereignisse werden überwacht, indem detaillierte Aufzeichn ungen über die Anfragen erfasst werden, die an einen Amazon-S3-Bucket gestellt wurden. Jeder Zugriffsprotokolle intrag enthält Details zu einer einzelnen Zugriffsanfrage. Zu den Details gehören Anforderer, Bucket-Name, Anforderu ngszeit, Anforderu ngsaktion, Antwortst atus und Fehlercode, falls relevant.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-2(12)	Kontoverwaltung | Kontoüberwachung bei untypischer Nutzung	guardduty-enabled-centralized	Amazon GuardDuty kann mithilfe von Threat Intellige nce Feeds helfen, potenzielle Cybersich erheitsereignisse zu überwachen und zu erkennen. Dazu gehören Listen mit bösartigen IPs und maschinel len Lernmethoden zur Identifizierung unerwarteter, nicht autorisierter und bösartiger Aktivitäten in Ihrer AWS Cloud-Umgebung.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-2	Kontenverwaltung	iam-no-inline-policy-überprüfen	Stellen Sie sicher, dass ein Benutzer, eine IAM-Rolle oder eine IAM-Gruppe (AWS Identity and Access Management) nicht über eine Inline-Richtlinie zur Zugriffskontrolle auf Systeme und Ressourcen verfügt. AWS empfiehlt, verwaltete Richtlinien anstelle von Inline-Richtlinien zu verwenden. Verwaltete Richtlinien ermöglichen Wiederverwendbarkeit, Versionsverwaltung, Rollback und Delegierung der Berechtigungsverwaltung.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-2	Kontenverwaltung	iam-policy-no-statements-with-full-access	Stellen Sie sicher, dass IAM-Aktionen nur auf die benötigten Aktionen beschränkt sind. Wenn Benutzern mehr Rechte eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und der Aufgabentrennung verstoßen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-2	Kontenverwaltung	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Managemen t (IAM) kann Ihnen helfen, die Prinzipien der geringsten Rechte und der Aufgabent rennung in Zugriffsb erechtigungen und Autorisierungen zu integrieren und so zu verhindern, dass Richtlinien blockiert e Aktionen für alle AWS Schlüssel des Key Management Service enthalten. Wenn Benutzer mehr Rechte haben, als für die Ausführung einer Aufgabe erforderl ich sind, kann dies gegen das Prinzip der geringsten Berechtig ung und Aufgabent rennung verstoßen . Mit dieser Regel können Sie den Parameter festlegen . blockedActionsPatt erns (Wert „AWS Bewährte grundlege nde Sicherhei tsmethoden“: kms:

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			Decrypt, kms:ReEncryptFrom). Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-2	Kontenverwaltung	iam-inline-policy-blocked-kms-Aktionen	Stellen Sie sicher, dass ein Benutzer, eine IAM-Rolle oder eine IAM-Gruppe (AWS Identity and Access Management) nicht über eine Inline-Richtlinie verfügt, die blockierte Aktionen für alle AWS Schlüssel des Key Management Service zulässt. AWS empfiehlt, verwaltete Richtlinien anstelle von Inline-Richtlinien zu verwenden. Verwaltete Richtlinien ermöglichen Wiederverwendbarkeit, Versionsverwaltung, Rollback und Delegierung der Berechtigungsverwaltung. Mit dieser Regel können Sie den blockedActionsPatterns Parameter festlegen. (Wert „AWS Bewährte grundlegende Sicherheitsmethoden“: kms:Decrypt, kms:ReEncryptFrom). Die

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.
AC-2	Kontenverwaltung	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) kann Ihnen dabei helfen, die Prinzipien der geringsten Rechte und der Aufgabentrennung in Zugriffsberechtigungen und Autorisierungen zu integrieren und so zu verhindern, dass Richtlinien „Effect“: „Allow“ mit „Action“: „*“ anstelle von „Resource“: „*“ enthalten. Wenn Benutzern mehr Rechte eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und der Aufgabentrennung verstoßen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-2	Kontenverwaltung	iam-user-group-membership-überprüfen	AWS Identity and Access Management (IAM) kann Ihnen helfen, Zugriffsberechtigungen und Autorisierungen einzuschränken, indem sichergestellt wird, dass Benutzer Mitglieder mindestens einer Gruppe sind. Wenn Benutzern mehr Berechtigungen eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und Aufgabentrennung verstoßen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-2	Kontenverwaltung	iam-user-unused-credentials-überprüfen	AWS Identity and Access Management (IAM) kann Ihnen bei Zugriffsberechtigungen und Autorisierungen helfen, indem es nach IAM-Passwörtern und Zugriffsschlüsseln sucht, die für einen bestimmten Zeitraum nicht verwendet wurden. Wenn ungenutzte Anmeldeinformationen identifiziert werden, müssen Sie sie deaktivieren und/oder entfernen, da dies gegen das Prinzip der geringsten Berechtigung verstoßen könnte. Für diese Regel müssen Sie einen Wert für das maxCredentialUsage Alter festlegen (Standardkonfiguration: 90). Der tatsächliche Wert muss den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-3(15)	Durchsetzung des Zugriffs | Diskretionäre und obligatorische Zugriffskontrolle	ec2-imdsv2-check	Stellen Sie sicher, dass die Methode Instance Metadata Service Version 2 (IMDSv2) aktiviert ist, um den Zugriff auf und die Kontrolle der Amazon Elastic Compute Cloud (Amazon EC2) - Instance-Metadaten zu schützen. Die IMDSv2 Methode verwendet sitzungsbasierte Kontrollen. Mit können Kontrollen implementiert werden IMDSv2, um Änderungen an Instanzmetadaten einzuschränken.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-3(15)	Durchsetzung des Zugriffs | Diskretionäre und obligatorische Zugriffskontrolle	ec-2 instance-profile-attached	EC2 Instanzprofile übergeben eine IAM-Rolle an eine EC2 Instance. Das Anhängen eines Instance-Profils an Ihre Instances kann bei der Implementierung von geringsten Berechtigungen und der Berechtigungsverwaltung helfen.
AC-3(15)	Durchsetzung des Zugriffs | Diskretionäre und obligatorische Zugriffskontrolle	ecs-containers-readonly-access	Die Aktivierung des schreibgeschützten Zugriffs auf Amazon Elastic Container Service (ECS)-Container kann dazu beitragen, das Prinzip der geringsten Berechtigung einzuhalten. Diese Option kann Angriffsvektoren reduzieren, da das Dateisystem der Container-Instance nur geändert werden kann, wenn es über ausdrückliche Lese- und Schreibberechtigungen verfügt.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-3(15)	Durchsetzung des Zugriffs | Diskretionäre und obligatorische Zugriffskontrolle	ecs-task-definition-user-for-host-mode-check	Wenn für eine Aufgabendefinition erhöhte Berechtigungen gelten, liegt das daran, dass der Kunde diesen Konfigurationen ausdrücklich zugestimmt hat. Diese Kontrolle prüft, ob eine unerwartete Berechtigungseskalation vorliegt, wenn für eine Aufgabendefinition das Host-Netzwerk aktiviert ist, die Kunden aber keine erhöhten Berechtigungen aktiviert haben.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-3(15)	Durchsetzung des Zugriffs | Diskretionäre und obligatorische Zugriffskontrolle	iam-no-inline-policy-überprüfen	Stellen Sie sicher, dass ein Benutzer, eine IAM-Rolle oder eine IAM-Gruppe (AWS Identity and Access Management) nicht über eine Inline-Richtlinie zur Zugriffskontrolle auf Systeme und Ressourcen verfügt. AWS empfiehlt, verwaltete Richtlinien anstelle von Inline-Richtlinien zu verwenden. Verwaltete Richtlinien ermöglichen Wiederverwendbarkeit, Versionsverwaltung, Rollback und Delegierung der Berechtigungsverwaltung.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-3(15)	Durchsetzung des Zugriffs | Diskretionäre und obligatorische Zugriffskontrolle	iam-policy-no-statements-with-full-access	Stellen Sie sicher, dass IAM-Aktionen nur auf die benötigten Aktionen beschränkt sind. Wenn Benutzern mehr Rechte eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und der Aufgabentrennung verstoßen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-3(15)	Durchsetzung des Zugriffs | Diskretionäre und obligatorische Zugriffskontrolle	access-keys-rotated	Die Anmeldeinformationen für autorisierte Geräte, Benutzer und Prozesse werden geprüft, indem sichergestellt wird, dass die IAM-Zugriffsschlüssel entsprechend den Vorgaben der Unternehmensrichtlinie rotiert werden. Das regelmäßige Ändern der Zugriffsschlüssel ist eine bewährte Sicherheitsmethode. Es verkürzt den Zeitraum, in dem ein Zugriffsschlüssel aktiv ist, und reduziert die Auswirkungen auf das Unternehmen, wenn die Schlüssel kompromittiert werden. Diese Regel erfordert einen Wert für die Zugriffsschlüssel-Rotation (Standardkonfiguration: 90). Der tatsächliche Wert muss den Richtlini

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			en Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-3(15)	Durchsetzung des Zugriffs | Diskretionäre und obligatorische Zugriffskontrolle	iam-customer-policy-blocked-kms-Aktionen	AWS Identity and Access Management (IAM) kann Ihnen helfen, die Prinzipien der geringsten Rechte und der Aufgabentrennung in Zugriffsberechtigungen und Autorisierungen zu integrieren und so zu verhindern, dass Richtlinien blockierte Aktionen für alle AWS Schlüssel des Key Management Service enthalten. Wenn Benutzer mehr Rechte haben, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und Aufgabentrennung verstoßen. Mit dieser Regel können Sie den Parameter festlegen. blockedActionsPatterns (Wert „AWS Bewährte grundlegende Sicherheitsmethoden“: kms:

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			Decrypt, kms:ReEncryptFrom). Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-3(15)	Durchsetzung des Zugriffs | Diskretionäre und obligatorische Zugriffskontrolle	iam-inline-policy-blocked-kms-Aktionen	Stellen Sie sicher, dass ein Benutzer, eine IAM-Rolle oder eine IAM-Gruppe (AWS Identity and Access Management) nicht über eine Inline-Richtlinie verfügt, die blockierte Aktionen für alle AWS Schlüssel des Key Management Service zulässt. AWS empfiehlt, verwaltete Richtlinien anstelle von Inline-Richtlinien zu verwenden. Verwaltete Richtlinien ermöglichen Wiederverwendbarkeit, Versionsverwaltung, Rollback und Delegierung der Berechtigungsverwaltung. Mit dieser Regel können Sie den blockedActionsPatterns Parameter festlegen. (Wert „AWS Bewährte grundlegende Sicherheitsmethoden“: kms:Decrypt, kms:ReEncryptFrom). Die

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-3(15)	Durchsetzung des Zugriffs | Diskretionäre und obligatorische Zugriffskontrolle	iam-password-policy	Die Identitäten und Anmeldeinformationen werden auf der Grundlage einer organisatorischen IAM-Passwortrichtlinie ausgestellt, verwaltet und verifiziert. Sie erfüllen oder übertreffen die Anforderungen des NIST SP 800-63 und des AWS Foundational Security Best Practices-Standards für Passwortstärke. Mit dieser Regel können Sie optional RequireUppercaseCharacters (Wert für AWS grundlegende Sicherheitsbewährte Methoden: wahr), RequireLowercaseCharacters (Wert für bewährte Methoden für AWS grundlegende Sicherheit: wahr), RequireSymbols (Wert für bewährte Methoden für AWS grundlegende Sicherheit:

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			wahr), RequireNumbers (Wert für bewährte Methoden für AWS grundlegende Sicherheit: wahr), MinimumPasswordLength (Wert für bewährte Methoden für AWS grundlegende Sicherheit: 14), PasswordReusePrevention (Wert für bewährte Methoden für AWS grundlegende Sicherheit: 24) und MaxPasswordAge (Wert für bewährte Methoden für AWS grundlegende Sicherheit: 90) für Ihr IAM festlegen Kennwortrichtlinie. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-3(15)	Durchsetzung des Zugriffs | Diskretionäre und obligatorische Zugriffskontrolle	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) kann Ihnen dabei helfen, die Prinzipien der geringsten Rechte und der Aufgabentrennung in Zugriffsberechtigungen und Autorisierungen zu integrieren und so zu verhindern, dass Richtlinien „Effect“: „Allow“ mit „Action“: „*“ anstelle von „Resource“: „*“ enthalten. Wenn Benutzern mehr Rechte eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und der Aufgabentrennung verstoßen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-3(15)	Durchsetzung des Zugriffs | Diskretionäre und obligatorische Zugriffskontrolle	iam-root-access-key-überprüfen	Der Zugriff auf Systeme und Ressourcen kann gesteuert werden, indem überprüft wird, ob der Root-Benutzer keine Zugriffsschlüssel mit seiner AWS Identity and Access Management (IAM) -Rolle verknüpft hat. Stellen Sie sicher, dass die Root-Zugriffsschlüssel gelöscht werden. Erstellen und verwenden Sie stattdessen rollenbasierte Funktionen, AWS-Konten um das Prinzip der geringsten Funktionalität zu berücksichtigen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-3(15)	Durchsetzung des Zugriffs | Diskretionäre und obligatorische Zugriffskontrolle	iam-user-group-membership-überprüfen	AWS Identity and Access Management (IAM) kann Ihnen helfen, Zugriffsberechtigungen und Autorisierungen einzuschränken, indem sichergestellt wird, dass Benutzer Mitglieder mindestens einer Gruppe sind. Wenn Benutzern mehr Berechtigungen eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und Aufgabentrennung verstoßen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-3(15)	Durchsetzung des Zugriffs | Diskretionäre und obligatorische Zugriffskontrolle	iam-user-mfa-enabled	Aktivieren Sie diese Regel, um den Zugriff auf Ressourcen in der AWS Cloud einzuschränken. Diese Regel sorgt dafür, dass die Multi-Faktor-Authentifizierung (MFA) für alle Benutzer aktiviert ist. MFA sorgt für eine weitere Schutzebene zusätzlich zu den Anmeldeinformationen. Reduzieren Sie Fälle von kompromittierten Konten, indem Sie MFA für Benutzer vorschreiben.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-3(15)	Durchsetzung des Zugriffs | Diskretionäre und obligatorische Zugriffskontrolle	iam-user-unused-credentials-überprüfen	AWS Identity and Access Management (IAM) kann Ihnen bei Zugriffsberechtigungen und Autorisierungen helfen, indem es nach IAM-Passwörtern und Zugriffsschlüsseln sucht, die für einen bestimmten Zeitraum nicht verwendet wurden. Wenn ungenutzte Anmeldeinformationen identifiziert werden, müssen Sie sie deaktivieren und/oder entfernen, da dies gegen das Prinzip der geringsten Berechtigung verstoßen könnte. Für diese Regel müssen Sie einen Wert für das maxCredentialUsage Alter festlegen (Standardkonfiguration: 90). Der tatsächliche Wert muss den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-3(15)	Durchsetzung des Zugriffs | Diskretionäre und obligatorische Zugriffskontrolle	mfa-enabled-for-iam-Konsolenzugriff	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass MFA für alle AWS Identity and Access Management (IAM) -Benutzer aktiviert ist, die über ein Konsolenkennwort verfügen. MFA sorgt für eine weitere Schutzebene zusätzlich zu den Anmeldeinformationen. Indem Sie MFA für Benutzer vorschreiben, können Sie Fälle kompromittierter Konten reduzieren und verhindern, dass unbefugte Benutzer auf vertrauliche Daten zugreifen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-3(15)	Durchsetzung des Zugriffs | Diskretionäre und obligatorische Zugriffskontrolle	root-account-hardware-mfa-aktiviert	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Hardware-MFA für den Root-Benutzer aktiviert ist. Der Stammbenutzer ist der AWS-Konto-Benutzer mit den meisten Berechtigungen. MFA sorgt für eine weitere Schutzebene zusätzlich zu den Anmeldeinformationen. Indem Sie MFA für den Root-Benutzer vorschreiben, können Sie die Anzahl AWS-Konten kompromittierter Benutzer reduzieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-3(15)	Durchsetzung des Zugriffs | Diskretionäre und obligatorische Zugriffskontrolle	root-account-mfa-enabled	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass MFA für den Root-Benutzer aktiviert ist. Der Stammbenutzer ist der AWS-Konto-Benutzer mit den meisten Berechtigungen. MFA sorgt für eine weitere Schutzebene zusätzlich zu den Anmeldeinformationen. Indem Sie MFA für den Root-Benutzer vorschreiben, können Sie die Anzahl AWS-Konten kompromittierter Benutzer reduzieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-3(15)	Durchsetzung des Zugriffs | Diskretionäre und obligatorische Zugriffskontrolle	secretsmanager-rotation-enabled-check	Diese Regel stellt sicher, dass bei AWS Secrets Manager Manager-Geheimnissen die Rotation aktiviert ist. Die regelmäßige Rotation von Secrets kann den Zeitraum verkürzen, in dem ein Secret aktiv ist, und möglicherweise die Auswirkungen auf das Unternehmen verringern, falls das Secret kompromittiert wird.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-3	Durchsetzung des Zugriffs	autoscaling-launch-config-public-ip-deaktiviert	Wenn Sie Ihre Netzwerkschnittstellen mit einer öffentlichen IP-Adresse konfigurieren, sind die diesen Netzwerkschnittstellen zugehörigen Ressourcen über das Internet erreichbar. EC2 Ressourcen sollten nicht öffentlich zugänglich sein, da dies einen unbeabsichtigten Zugriff auf Ihre Anwendungen oder Server ermöglichen kann.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-3	Durchsetzung des Zugriffs	ec2-imdsv2-check	Stellen Sie sicher, dass die Methode Instance Metadata Service Version 2 (IMDSv2) aktiviert ist, um den Zugriff auf und die Kontrolle der Amazon Elastic Compute Cloud (Amazon EC2) - Instance-Metadaten zu schützen. Die IMDSv2 Methode verwendet sitzungsbasierte Kontrollen. Mit können Kontrollen implementiert werden IMDSv2, um Änderungen an Instanzmetadaten einzuschränken.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-3	Durchsetzung des Zugriffs	ec-2 instance-profile-attached	EC2 Instanzprofile übergeben eine IAM-Rolle an eine EC2 Instance. Das Anhängen eines Instance-Profils an Ihre Instances kann bei der Implementierung von geringsten Berechtigungen und der Berechtigungsverwaltung helfen.
AC-3	Durchsetzung des Zugriffs	ecs-containers-readonly-access	Die Aktivierung des schreibgeschützten Zugriffs auf Amazon Elastic Container Service (ECS)-Container kann dazu beitragen, das Prinzip der geringsten Berechtigung einzuhalten. Diese Option kann Angriffsvektoren reduzieren, da das Dateisystem der Container-Instance nur geändert werden kann, wenn es über ausdrückliche Lese- und Schreibberechtigungen verfügt.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-3	Durchsetzung des Zugriffs	ecs-task-definition-user-for-host-mode-check	Wenn für eine Aufgabendefinition erhöhte Berechtigungen gelten, liegt das daran, dass der Kunde diesen Konfigurationen ausdrücklich zugestimmt hat. Diese Kontrolle prüft, ob eine unerwartete Berechtigungseskalation vorliegt, wenn für eine Aufgabendefinition das Host-Netzwerk aktiviert ist, die Kunden aber keine erhöhten Berechtigungen aktiviert haben.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-3	Durchsetzung des Zugriffs	iam-no-inline-policy-überprüfen	Stellen Sie sicher, dass ein Benutzer, eine IAM-Rolle oder eine IAM-Gruppe (AWS Identity and Access Management) nicht über eine Inline-Richtlinie zur Zugriffskontrolle auf Systeme und Ressourcen verfügt. AWS empfiehlt, verwaltete Richtlinien anstelle von Inline-Richtlinien zu verwenden. Verwaltete Richtlinien ermöglichen Wiederverwendbarkeit, Versionsverwaltung, Rollback und Delegierung der Berechtigungsverwaltung.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-3	Durchsetzung des Zugriffs	iam-policy-no-statements-with-full-access	Stellen Sie sicher, dass IAM-Aktionen nur auf die benötigten Aktionen beschränkt sind. Wenn Benutzern mehr Rechte eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und der Aufgabentrennung verstoßen.
AC-3	Durchsetzung des Zugriffs	ssm-document-not-public	Stellen Sie sicher, dass AWS Systems Manager (SSM) - Dokumente nicht öffentlich sind, da dies einen unbeabsichtigten Zugriff auf Ihre SSM-Dokumente ermöglichen kann. Ein öffentliches SSM-Dokument kann Informationen über Ihr Konto, Ihre Ressourcen und internen Prozesse preisgeben.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-3	Durchsetzung des Zugriffs	dms-replication-not-public	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass auf DMS-Replikationsin stanzen nicht öffentlic h zugegriffen werden kann. DMS-Repli kations-Instances können vertrauli che Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.
AC-3	Durchsetzung des Zugriffs	ebs-snapshot-public-restorable-überprüfen	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass EBS-Snapshots nicht öffentlich wiederher stellbar sind. EBS-Volume-Snapsho ts können vertrauli che Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-3	Durchsetzung des Zugriffs	ec-2 instance-no-public-ip	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon Elastic Compute Cloud (Amazon EC2) - Instances nicht öffentlich zugänglich sind. EC2 Amazon-Instances können vertrauliche Informationen enthalten, und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-3	Durchsetzung des Zugriffs	elasticsearch-in-vpc-only	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass sich Amazon OpenSearch OpenSearch Service (Service) - Domains innerhalb einer Amazon Virtual Private Cloud (Amazon VPC) befinden. Eine OpenSearch Service-Domain innerhalb einer Amazon VPC ermöglicht die sichere Kommunikation zwischen OpenSearch Service und anderen Services innerhalb der Amazon VPC, ohne dass ein Internet-Gateway, ein NAT-Gerät oder eine VPN-Verbindung erforderlich ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-3	Durchsetzung des Zugriffs	emr-master-no-public-ip	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon EMR-Cluster-Masterknoten nicht öffentlich zugänglich sind. Amazon-EMR-Cluster-Hauptknoten können vertrauliche Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-3	Durchsetzung des Zugriffs	iam-customer-policy-blocked-kms-Aktionen	AWS Identity and Access Managemen t (IAM) kann Ihnen helfen, die Prinzipien der geringsten Rechte und der Aufgabent rennung in Zugriffsb erechtigungen und Autorisierungen zu integrieren und so zu verhindern, dass Richtlinien blockiert e Aktionen für alle AWS Schlüssel des Key Management Service enthalten. Wenn Benutzer mehr Rechte haben, als für die Ausführung einer Aufgabe erforderl ich sind, kann dies gegen das Prinzip der geringsten Berechtig ung und Aufgabent rennung verstoßen . Mit dieser Regel können Sie den Parameter festlegen . blockedActionsPatt erns (Wert „AWS Bewährte grundlege nde Sicherhei tsmethoden“: kms:

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			Decrypt, kms:ReEncryptFrom). Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-3	Durchsetzung des Zugriffs	iam-inline-policy-blocked-kms-Aktionen	Stellen Sie sicher, dass ein Benutzer, eine IAM-Rolle oder eine IAM-Gruppe (AWS Identity and Access Management) nicht über eine Inline-Richtlinie verfügt, die blockierte Aktionen für alle AWS Schlüssel des Key Management Service zulässt. AWS empfiehlt, verwaltete Richtlinien anstelle von Inline-Richtlinien zu verwenden. Verwaltete Richtlinien ermöglichen Wiederverwendbarkeit, Versionsverwaltung, Rollback und Delegierung der Berechtigungsverwaltung. Mit dieser Regel können Sie den blockedActionsPatterns Parameter festlegen. (Wert „AWS Bewährte grundlegende Sicherheitsmethoden“: kms:Decrypt, kms:ReEncryptFrom). Die

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.
AC-3	Durchsetzung des Zugriffs	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) kann Ihnen dabei helfen, die Prinzipien der geringsten Rechte und der Aufgabentrennung in Zugriffsberechtigungen und Autorisierungen zu integrieren und so zu verhindern, dass Richtlinien „Effect“: „Allow“ mit „Action“: „*“ anstelle von „Resource“: „*“ enthalten. Wenn Benutzern mehr Rechte eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und der Aufgabentrennung verstoßen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-3	Durchsetzung des Zugriffs	iam-user-group-membership-überprüfen	AWS Identity and Access Management (IAM) kann Ihnen helfen, Zugriffsberechtigungen und Autorisierungen einzuschränken, indem sichergestellt wird, dass Benutzer Mitglieder mindestens einer Gruppe sind. Wenn Benutzern mehr Berechtigungen eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und Aufgabentrennung verstoßen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-3	Durchsetzung des Zugriffs	iam-user-unused-credentials-überprüfen	AWS Identity and Access Management (IAM) kann Ihnen bei Zugriffsberechtigungen und Autorisierungen helfen, indem es nach IAM-Passwörtern und Zugriffsschlüsseln sucht, die für einen bestimmten Zeitraum nicht verwendet wurden. Wenn ungenutzte Anmeldeinformationen identifiziert werden, müssen Sie sie deaktivieren und/oder entfernen, da dies gegen das Prinzip der geringsten Berechtigung verstoßen könnte. Für diese Regel müssen Sie einen Wert für das maxCredentialUsage Alter festlegen (Standardkonfiguration: 90). Der tatsächliche Wert muss den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-3	Durchsetzung des Zugriffs	lambda-function-public-access-verboten	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass AWS Lambda-Funktionen nicht öffentlich zugänglich sind. Der öffentliche Zugriff kann möglicherweise die Verfügbarkeit von Ressourcen beeinträchtigen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-3	Durchsetzung des Zugriffs	lambda-inside-vpc	Stellen Sie AWS Lambda-Funktionen in einer Amazon Virtual Private Cloud (Amazon VPC) bereit, um eine sichere Kommunika tion zwischen einer Funktion und anderen Diensten innerhalb der Amazon VPC zu gewährleisten. Bei dieser Konfiguration sind kein Internet-Gateway, kein NAT-Gerät und keine VPN-Verbindung erforderlich. Der gesamte Datenverk ehr bleibt sicher in der Cloud. AWS Domains, die sich innerhalb einer VPC befinden, verfügen aufgrund ihrer logischen Isolierun g im Vergleich zu Domains mit öffentlic hen Endpunkten über eine zusätzliche Sicherheitsebene. Um den Zugriff ordnungsg emäß zu verwalten,

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			sollten AWS Lambda-Funktionen einer VPC zugewiesen werden.
AC-3	Durchsetzung des Zugriffs	opensearch-in-vpc-only	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass sich Amazon OpenSearch Service-Domains innerhalb einer Amazon Virtual Private Cloud (Amazon VPC) befinden. Eine Amazon OpenSearch Service-Domain innerhalb einer Amazon VPC ermöglicht die sichere Kommunikation zwischen Amazon OpenSearch Service und anderen Services innerhalb der Amazon VPC, ohne dass ein Internet-Gateway, ein NAT-Gerät oder eine VPN-Verbindung erforderlich ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-3	Durchsetzung des Zugriffs	rds-instance-public-access-überprüfen	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Relational Database Service (Amazon RDS) -Instances nicht öffentlich sind. Amazon-RDS-Datenbank-Instances können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-3	Durchsetzung des Zugriffs	rds-snapshots-public-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Relational Database Service (Amazon RDS) -Instances nicht öffentlich sind. Amazon-RDS-Datenbank-Instances können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-3	Durchsetzung des Zugriffs	redshift-cluster-public-access-überprüfen	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Redshift Redshift-Cluster nicht öffentlich sind. Amazon-Redshift-Cluster können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-3	Durchsetzung des Zugriffs	s3- -Block-periodisch account-level-public-access	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Simple Storage Service (Amazon S3) -Buckets nicht öffentlich zugänglich sind. Diese Regel trägt dazu bei, sensible Daten vor unbefugten Remote-Benutzern zu schützen, indem sie den öffentlichen Zugriff verhindert. Mit dieser Regel können Sie optional die Parameter ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) und restrictPublicBuckets Parameter (Config Default: True) festlegen. Die tatsächlichen Werte müssen den Richtlini

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			en Ihrer Organisation entsprechen.
AC-3	Durchsetzung des Zugriffs	s3 bucket-level-public-access - verboten	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Simple Storage Service (Amazon S3) -Buckets nicht öffentlich zugänglich sind. Diese Regel trägt dazu bei, sensible Daten vor unbefugten Remote-Benutzern zu schützen, indem sie den öffentlichen Zugriff auf Bucket-Ebene verhindert.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-3	Durchsetzung des Zugriffs	s-3 bucket-public-read -prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie nur autorisierten Benutzern, Prozessen und Geräten Zugriff auf Amazon Simple Storage Service (Amazon S3) - Buckets gewähren. Die Verwaltung des Zugriffs sollte mit der Klassifizierung der Daten übereinst immen.
AC-3	Durchsetzung des Zugriffs	s3- bucket-public-writ e-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie nur autorisierten Benutzern, Prozessen und Geräten Zugriff auf Amazon Simple Storage Service (Amazon S3) - Buckets gewähren. Die Verwaltung des Zugriffs sollte mit der Klassifizierung der Daten übereinst immen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-3	Durchsetzung des Zugriffs	sagemaker-notebook-no-direct-Internetzugang	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass SageMaker Amazon-Notebooks keinen direkten Internetzugang zulassen. Indem Sie direkten Internetzugang blockieren, vermeiden Sie, dass unbefugte Benutzer auf sensible Daten zugreifen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-3	Durchsetzung des Zugriffs	subnet-auto-assign-public-ip-deaktiviert	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon Virtual Private Cloud (VPC) -Subnetzen nicht automatisch eine öffentliche IP-Adresse zugewiesen wird. Amazon Elastic Compute Cloud (EC2) -Instances, die in Subnetzen gestartet werden, in denen dieses Attribut aktiviert ist, haben ihrer primären Netzwerkschnittstelle eine öffentliche IP-Adresse zugewiesen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-4(26)	Durchsetzung des Informationsflusses | Prüfungsfilteraktionen	elasticsearch-logs-to-cloudwatch	Stellen Sie sicher, dass für Amazon OpenSearch Service-Domains Fehlerprotokolle aktiviert und zur Aufbewahrung und Beantwortung an Amazon CloudWatch Logs gestreamt werden. Domain-Fehlerprotokolle sind bei Sicherheits- und Zugriffsprüfungen sowie bei der Diagnose von Verfügbarkeitsproblemen nützlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-4(26)	Durchsetzung des Informationsflusses | Prüfungsfilteraktionen	multi-region-cloudtrail-enabled	AWS CloudTrail zeichnet Aktionen und API-Aufrufe der AWS Management Console auf. Sie können feststellen, welche Benutzer und Konten angerufen wurden AWS, von welcher Quell-IP-Adresse aus die Anrufe getätigt wurden und wann die Anrufe erfolgten. CloudTrail übermittelt Protokolldateien aus allen AWS Regionen an Ihren S3-Bucket , wenn MULTI_REG ION_CLOUD _TRAIL_ENABLED aktiviert ist. Außerdem wird beim AWS Start einer neuen Region derselbe Trail in der neuen Region erstellt. CloudTrail Dadurch erhalten Sie automatis ch Protokolldateien mit API-Aktivitäten für die neue Region.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-4(26)	Durchsetzung des Informationsflusses | Prüfungsfilteraktionen	opensearch-logs-to-cloudwatch	Stellen Sie sicher, dass für Amazon OpenSearch Service-Domains Fehlerprotokolle aktiviert und zur Aufbewahrung und Beantwortung an Amazon CloudWatch Logs gestreamt werden. OpenSearch Service-Fehlerprotokolle können bei Sicherheits- und Zugriffsprüfungen helfen und bei der Diagnose von Verfügbarkeitsproblemen helfen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-4(26)	Durchsetzung des Informationsflusses | Prüfungsfilteraktionen	wafv2-logging-enabled	Um die Protokollierung und Überwachung in Ihrer Umgebung zu erleichtern, aktivieren Sie die AWS WAF (V2) -Protokollierung im regionalen und globalen Internet ACLs. AWS Die WAF-Protokollierung bietet detaillierte Informationen über den Datenverkehr, der von Ihrer Web-ACL analysiert wird. In den Protokollen werden die Uhrzeit aufgezeichnet, zu der die AWS WAF die Anfrage von Ihrer AWS Ressource erhalten hat, Informationen über die Anfrage und eine Aktion für die Regel, der jede Anfrage entsprach.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-4(26)	Durchsetzung des Informationsflusses | Prüfungsfilteraktionen	api-gw-execution-logging-aktiviert	Die API-Gateway-Protokollierung zeigt detaillierte Ansichten der Benutzer, die auf die API zugegriffen haben, und wie diese Benutzer auf die API zugegriffen haben. Diese Einblicke ermöglichen die Transparenz von Benutzeraktivitäten.
AC-4(26)	Durchsetzung des Informationsflusses | Prüfungsfilteraktionen	cloud-trail-cloud-watch-logs-aktiviert	Verwenden Sie Amazon CloudWatch , um Protokoll ereignisaktivitäten zentral zu sammeln und zu verwalten. Die Aufnahme von AWS CloudTrail Daten liefert Einzelheiten zu den API-Aufrufaktivitäten in Ihrem AWS-Konto.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-4(26)	Durchsetzung des Informationsflusses | Prüfungsfilteraktionen	cloudtrail-enabled	AWS CloudTrail kann bei der Nichtabstreitbarkeit helfen, indem Aktionen und API-Aufrufe der AWS Management Console aufgezeichnet werden. Sie können die Benutzer und die Benutzer AWS-Konten , die einen AWS Dienst aufgerufen haben, die Quell-IP-Adresse, über die die Aufrufe generiert wurden, und den Zeitpunkt der Anrufe identifizieren. Einzelheiten zu den erfassten Daten finden Sie unter Inhalt des AWS CloudTrail Datensatzes.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-4(26)	Durchsetzung des Informationsflusses | Prüfungsfilteraktionen	cloudtrail-s3-data events-enabled	Die Erfassung von Simple Storage Service (Amazon S3)-Datenereignissen unterstützt die Erkennung von ungewöhnlichen Aktivitäten. Zu den Details gehören AWS-Konto Informationen über den Zugriff auf einen Amazon S3 S3-Bucket, die IP-Adresse und die Uhrzeit des Ereignisses.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-4(26)	Durchsetzung des Informationsflusses | Prüfungsfilteraktionen	elb-logging-enabled	Die Elastic-Load-Balancing-Aktivität ist ein zentraler Kommunikationspunkt innerhalb einer Umgebung. Stellen Sie sicher, dass die ELB-Protokollierung aktiviert ist. Die gesammelten Daten enthalten detaillierte Informationen zu Anfragen, die an den ELB gesendet wurden. Jedes Protokoll enthält Informationen wie die Zeit, zu der die Anforderung einging, die Client-IP-Adresse, Latenzen, Anforderungspfade und Serverantworten.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-4(26)	Durchsetzung des Informationsflusses | Prüfungsfilteraktionen	rds-logging-enabled	Um die Protokoll ierung und Überwachung in Ihrer Umgebung zu erleichtern, stellen Sie sicher, dass die Amazon Relationa l Database Service (Amazon RDS)-Prot okollierung aktiviert ist. Mit der Amazon-RDS-Protokollierung können Sie Ereigniss e wie Verbindungen, Verbindungsabbrüch e, Abfragen oder abgefragte Tabellen erfassen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-4(26)	Durchsetzung des Informationsflusses | Prüfungsfilteraktionen	redshift-cluster-configuration-check	Um Daten im Ruhezustand zu schützen, muss die Verschlüsselung für Ihre Amazon-Redshift-Cluster aktiviert sein. Sie müssen auch sicherstellen, dass die erforderlichen Konfigurationen auf Amazon-Redshift-Clustern bereitgestellt werden. Die Prüfungsprotokollierung muss aktiviert sein, um Informationen zu Verbindungen und Benutzeraktivitäten in der Datenbank bereitzustellen. Diese Regel erfordert, dass ein Wert für clusterDbEncrypted (Config Default: TRUE) und LoggingEnabled (Config Default: TRUE) gesetzt ist. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-4(26)	Durchsetzung des Informationsflusses | Prüfungsfilteraktionen	s3- bucket-logging-enabled	Die Amazon Simple Storage Service (Amazon S3)-Serverzugriffs protokollierung bietet eine Methode zur Überwachu ng des Netzwerks im Hinblick auf potenzielle Cybersich erheitsereignisse. Die Ereignisse werden überwacht, indem detaillierte Aufzeichn ungen über die Anfragen erfasst werden, die an einen Amazon-S3-Bucket gestellt wurden. Jeder Zugriffsprotokolle intrag enthält Details zu einer einzelnen Zugriffsanfrage. Zu den Details gehören Anforderer, Bucket-Name, Anforderu ngszeit, Anforderu ngsaktion, Antwortst atus und Fehlercode, falls relevant.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-4(26)	Durchsetzung des Informationsflusses | Prüfungsfilteraktionen	vpc-flow-logs-enabled	VPC-Flow-Protokolle erfassen detaillierte Informationsdatensätze über den IP-Datenverkehr, der zu und von Netzwerkschnittstellen in Ihrer Amazon Virtual Private Cloud (Amazon VPC) fließt. Standardmäßig enthalten Flow-Protokolldatensätze Werte für die verschiedenen Komponenten des IP-Flows, einschließlich Quelle, Ziel und Protokoll.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-5	Aufgabentrennung	ecs-containers-readonly-access	Die Aktivierung des schreibgeschützten Zugriffs auf Amazon Elastic Container Service (ECS)-Container kann dazu beitragen, das Prinzip der geringsten Berechtigung einzuhalten. Diese Option kann Angriffsvektoren reduzieren, da das Dateisystem der Container-Instance nur geändert werden kann, wenn es über ausdrückliche Lese- und Schreibberechtigungen verfügt.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-5	Aufgabentrennung	ecs-task-definition-user-for-host-mode-check	Wenn für eine Aufgabendefinition erhöhte Berechtigungen gelten, liegt das daran, dass der Kunde diesen Konfigurationen ausdrücklich zugestimmt hat. Diese Kontrolle prüft, ob eine unerwartete Berechtigungseskalation vorliegt, wenn für eine Aufgabendefinition das Host-Netzwerk aktiviert ist, die Kunden aber keine erhöhten Berechtigungen aktiviert haben.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-5	Aufgabentrennung	iam-policy-no-statements-with-full-access	Stellen Sie sicher, dass IAM-Aktionen nur auf die benötigten Aktionen beschränkt sind. Wenn Benutzern mehr Rechte eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und der Aufgabentrennung verstoßen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-5	Aufgabentrennung	iam-customer-policy-blocked-kms-Aktionen	AWS Identity and Access Managemen t (IAM) kann Ihnen helfen, die Prinzipien der geringsten Rechte und der Aufgabent rennung in Zugriffsb erechtigungen und Autorisierungen zu integrieren und so zu verhindern, dass Richtlinien blockiert e Aktionen für alle AWS Schlüssel des Key Management Service enthalten. Wenn Benutzer mehr Rechte haben, als für die Ausführung einer Aufgabe erforderl ich sind, kann dies gegen das Prinzip der geringsten Berechtig ung und Aufgabent rennung verstoßen . Mit dieser Regel können Sie den Parameter festlegen . blockedActionsPatt erns (Wert „AWS Bewährte grundlege nde Sicherhei tsmethoden“: kms:

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			Decrypt, kms:ReEncryptFrom). Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-5	Aufgabentrennung	iam-inline-policy-blocked-kms-Aktionen	Stellen Sie sicher, dass ein Benutzer, eine IAM-Rolle oder eine IAM-Gruppe (AWS Identity and Access Management) nicht über eine Inline-Richtlinie verfügt, die blockierte Aktionen für alle AWS Schlüssel des Key Management Service zulässt. AWS empfiehlt, verwaltete Richtlinien anstelle von Inline-Richtlinien zu verwenden. Verwaltete Richtlinien ermöglichen Wiederverwendbarkeit, Versionsverwaltung, Rollback und Delegierung der Berechtigungsverwaltung. Mit dieser Regel können Sie den blockedActionsPatterns Parameter festlegen. (Wert „AWS Bewährte grundlegende Sicherheitsmethoden“: kms:Decrypt, kms:ReEncryptFrom). Die

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.
AC-5	Aufgabentrennung	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) kann Ihnen dabei helfen, die Prinzipien der geringsten Rechte und der Aufgabentrennung in Zugriffsberechtigungen und Autorisierungen zu integrieren und so zu verhindern, dass Richtlinien „Effect“: „Allow“ mit „Action“: „*“ anstelle von „Resource“: „*“ enthalten. Wenn Benutzern mehr Rechte eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und der Aufgabentrennung verstoßen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-6(2)	Geringste Berechtigung | Nicht privilegierter Zugriff auf nicht sicherheitsrelevante Funktionen	iam-policy-no-statements-with-full-access	Stellen Sie sicher, dass IAM-Aktionen nur auf die benötigten Aktionen beschränkt sind. Wenn Benutzern mehr Rechte eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und der Aufgabentrennung verstoßen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-6(2)	Geringste Berechtigung | Nicht privilegierter Zugriff auf nicht sicherheitsrelevante Funktionen	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) kann Ihnen dabei helfen, die Prinzipien der geringsten Rechte und der Aufgabentrennung in Zugriffsberechtigungen und Autorisierungen zu integrieren und so zu verhindern, dass Richtlinien „Effect“: „Allow“ mit „Action“: „*“ anstelle von „Resource“: „*“ enthalten. Wenn Benutzern mehr Rechte eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und der Aufgabentrennung verstoßen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-6(2)	Geringste Berechtigung | Nicht privilegierter Zugriff auf nicht sicherheitsrelevante Funktionen	iam-root-access-key-überprüfen	Der Zugriff auf Systeme und Ressourcen kann gesteuert werden, indem überprüft wird, ob der Root-Benutzer keine Zugriffsschlüssel mit seiner AWS Identity and Access Management (IAM) -Rolle verknüpft hat. Stellen Sie sicher, dass die Root-Zugriffsschlüssel gelöscht werden. Erstellen und verwenden Sie stattdessen rollenbasierte Funktionen, AWS-Konten um das Prinzip der geringsten Funktionalität zu berücksichtigen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-6(3)	Geringste Berechtigung | Netzwerkzugriff auf privilegierte Befehle	iam-no-inline-policy-überprüfen	Stellen Sie sicher, dass ein Benutzer, eine IAM-Rolle oder eine IAM-Gruppe (AWS Identity and Access Management) nicht über eine Inline-Richtlinie zur Zugriffskontrolle auf Systeme und Ressourcen verfügt. AWS empfiehlt, verwaltete Richtlinien anstelle von Inline-Richtlinien zu verwenden. Verwaltete Richtlinien ermöglichen Wiederverwendbarkeit, Versionsverwaltung, Rollback und Delegierung der Berechtigungsverwaltung.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-6(3)	Geringste Berechtigung | Netzwerkzugriff auf privilegierte Befehle	iam-policy-no-statements-with-full-access	Stellen Sie sicher, dass IAM-Aktionen nur auf die benötigten Aktionen beschränkt sind. Wenn Benutzern mehr Rechte eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und der Aufgabentrennung verstoßen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-6(3)	Geringste Berechtigung | Netzwerkzugriff auf privilegierte Befehle	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) kann Ihnen helfen, die Prinzipien der geringsten Rechte und der Aufgabentrennung in Zugriffsberechtigungen und Autorisierungen zu integrieren und so zu verhindern, dass Richtlinien blockierte Aktionen für alle AWS Schlüssel des Key Management Service enthalten. Wenn Benutzer mehr Rechte haben, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und Aufgabentrennung verstoßen. Mit dieser Regel können Sie den Parameter festlegen. blockedActionsPatterns (Wert „AWS Bewährte grundlegende Sicherheitsmethoden“: kms:

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			Decrypt, kms:ReEncryptFrom). Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-6(3)	Geringste Berechtigung | Netzwerkzugriff auf privilegierte Befehle	iam-inline-policy-blocked-kms-Aktionen	Stellen Sie sicher, dass ein Benutzer, eine IAM-Rolle oder eine IAM-Gruppe (AWS Identity and Access Management) nicht über eine Inline-Richtlinie verfügt, die blockierte Aktionen für alle AWS Schlüssel des Key Management Service zulässt. AWS empfiehlt, verwaltete Richtlinien anstelle von Inline-Richtlinien zu verwenden. Verwaltete Richtlinien ermöglichen Wiederverwendbarkeit, Versionsverwaltung, Rollback und Delegierung der Berechtigungsverwaltung. Mit dieser Regel können Sie den blockedActionsPatterns Parameter festlegen. (Wert „AWS Bewährte grundlegende Sicherheitsmethoden“: kms:Decrypt, kms:ReEncryptFrom). Die

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.
AC-6(3)	Geringste Berechtigung | Netzwerkzugriff auf privilegierte Befehle	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) kann Ihnen dabei helfen, die Prinzipien der geringsten Rechte und der Aufgabentrennung in Zugriffsberechtigungen und Autorisierungen zu integrieren und so zu verhindern, dass Richtlinien „Effect“: „Allow“ mit „Action“: „*“ anstelle von „Resource“: „*“ enthalten. Wenn Benutzern mehr Rechte eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und der Aufgabentrennung verstoßen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-6(3)	Geringste Berechtigung | Netzwerkzugriff auf privilegierte Befehle	iam-user-group-membership-überprüfen	AWS Identity and Access Management (IAM) kann Ihnen helfen, Zugriffsberechtigungen und Autorisierungen einzuschränken, indem sichergestellt wird, dass Benutzer Mitglieder mindestens einer Gruppe sind. Wenn Benutzern mehr Berechtigungen eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und Aufgabentrennung verstoßen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-6(9)	Geringste Berechtigung | Protokollierung der Nutzung privilegierter Funktionen	elasticsearch-logs-to-cloudwatch	Stellen Sie sicher, dass für Amazon OpenSearch Service-Domains Fehlerprotokolle aktiviert und zur Aufbewahrung und Beantwortung an Amazon CloudWatch Logs gestreamt werden. Domain-Fehlerprotokolle sind bei Sicherheits- und Zugriffsprüfungen sowie bei der Diagnose von Verfügbarkeitsproblemen nützlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-6(9)	Geringste Berechtigung | Protokollierung der Nutzung privilegierter Funktionen	multi-region-cloudtrail-enabled	AWS CloudTrail zeichnet Aktionen und API-Aufrufe der AWS Management Console auf. Sie können feststellen, welche Benutzer und Konten angerufen wurden AWS, von welcher Quell-IP-Adresse aus die Anrufe getätigt wurden und wann die Anrufe erfolgten. CloudTrail übermittelt Protokolldateien aus allen AWS Regionen an Ihren S3-Bucket, wenn MULTI_REGION_CLOUD_TRAIL_ENABLED aktiviert ist. Außerdem wird beim AWS Start einer neuen Region derselbe Trail in der neuen Region erstellt. CloudTrail Dadurch erhalten Sie automatisch Protokolldateien mit API-Aktivitäten für die neue Region.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-6(9)	Geringste Berechtigung | Protokollierung der Nutzung privilegierter Funktionen	opensearch-logs-to-cloudwatch	Stellen Sie sicher, dass für Amazon OpenSearch Service-Domains Fehlerprotokolle aktiviert und zur Aufbewahrung und Beantwortung an Amazon CloudWatch Logs gestreamt werden. OpenSearch Service-Fehlerprotokolle können bei Sicherheits- und Zugriffsprüfungen helfen und bei der Diagnose von Verfügbarkeitsproblemen helfen.
AC-6(9)	Geringste Berechtigung | Protokollierung der Nutzung privilegierter Funktionen	cloud-trail-cloud-watch-Logs aktiviert	Verwenden Sie Amazon CloudWatch , um Protokollereignisaktivitäten zentral zu sammeln und zu verwalten. Die Aufnahme von AWS CloudTrail Daten liefert Einzelheiten zu den API-Aufrufaktivitäten in Ihrem AWS-Konto.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-6(9)	Geringste Berechtigung | Protokollierung der Nutzung privilegierter Funktionen	cloudtrail-enabled	AWS CloudTrail kann bei der Nichtabstreitbarkeit helfen, indem Aktionen und API-Aufrufe der AWS Management Console aufgezeichnet werden. Sie können die Benutzer und die Benutzer AWS-Konten , die einen AWS Dienst aufgerufen haben, die Quell-IP-Adresse, über die die Aufrufe generiert wurden, und den Zeitpunkt der Anrufe identifizieren. Einzelheiten zu den erfassten Daten finden Sie unter Inhalt des AWS CloudTrail Datensatzes.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-6(9)	Geringste Berechtigung | Protokollierung der Nutzung privilegierter Funktionen	cloudtrail-s3-dataevents-enabled	Die Erfassung von Simple Storage Service (Amazon S3)-Datenereignissen unterstützt die Erkennung von ungewöhnlichen Aktivitäten. Zu den Details gehören AWS-Konto Informationen über den Zugriff auf einen Amazon S3 S3-Bucket, die IP-Adresse und die Uhrzeit des Ereignisses.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-6(9)	Geringste Berechtigung | Protokollierung der Nutzung privilegierter Funktionen	rds-logging-enabled	Um die Protokollierung und Überwachung in Ihrer Umgebung zu erleichtern, stellen Sie sicher, dass die Amazon Relational Database Service (Amazon RDS)-Protokollierung aktiviert ist. Mit der Amazon-RDS-Protokollierung können Sie Ereignisse wie Verbindungen, Verbindungsabbrüche, Abfragen oder abgefragte Tabellen erfassen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-6(9)	Geringste Berechtigung | Protokollierung der Nutzung privilegierter Funktionen	redshift-cluster-configuration-check	Um Daten im Ruhezustand zu schützen, muss die Verschlüsselung für Ihre Amazon-Redshift-Cluster aktiviert sein. Sie müssen auch sicherstellen, dass die erforderlichen Konfigurationen auf Amazon-Redshift-Clustern bereitgestellt werden. Die Prüfungsprotokollierung muss aktiviert sein, um Informationen zu Verbindungen und Benutzeraktivitäten in der Datenbank bereitzustellen. Diese Regel erfordert, dass ein Wert für clusterDbEncrypted (Config Default: TRUE) und LoggingEnabled (Config Default: TRUE) gesetzt ist. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-6(9)	Geringste Berechtigung | Protokollierung der Nutzung privilegierter Funktionen	s3- bucket-logging-enabled	Die Amazon Simple Storage Service (Amazon S3)-Serverzugriffsprotokollierung bietet eine Methode zur Überwachung des Netzwerks im Hinblick auf potenzielle Cybersicherheitsereignisse. Die Ereignisse werden überwacht, indem detaillierte Aufzeichnungen über die Anfragen erfasst werden, die an einen Amazon-S3-Bucket gestellt wurden. Jeder Zugriffsprotokolleintrag enthält Details zu einer einzelnen Zugriffsanfrage. Zu den Details gehören Anforderer, Bucket-Name, Anforderungszeit, Anforderungsaktion, Antwortstatus und Fehlercode, falls relevant.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-6(10)	Geringste Berechtigung | Verhinderung der Ausführung privilegierter Funktionen durch nicht privilegierte Benutzer	iam-policy-no-statements-with-full-access	Stellen Sie sicher, dass IAM-Aktionen nur auf die benötigten Aktionen beschränkt sind. Wenn Benutzern mehr Rechte eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und der Aufgabentrennung verstoßen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-6(10)	Geringste Berechtigung | Verhinderung der Ausführung privilegierter Funktionen durch nicht privilegierte Benutzer	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) kann Ihnen dabei helfen, die Prinzipien der geringsten Rechte und der Aufgabentrennung in Zugriffsberechtigungen und Autorisierungen zu integrieren und so zu verhindern, dass Richtlinien „Effect“: „Allow“ mit „Action“: „*“ anstelle von „Resource“: „*“ enthalten. Wenn Benutzern mehr Rechte eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und der Aufgabentrennung verstoßen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-6(10)	Geringste Berechtigung | Verhinderung der Ausführung privilegierter Funktionen durch nicht privilegierte Benutzer	iam-root-access-key-überprüfen	Der Zugriff auf Systeme und Ressourcen kann gesteuert werden, indem überprüft wird, ob der Root-Benutzer keine Zugriffsschlüssel mit seiner AWS Identity and Access Management (IAM) -Rolle verknüpft hat. Stellen Sie sicher, dass die Root-Zugriffsschlüssel gelöscht werden. Erstellen und verwenden Sie stattdessen rollenbasierte Funktionen, AWS-Konten um das Prinzip der geringsten Funktionalität zu berücksichtigen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-17(2)	Remote-Zugriff | Schutz von Vertrauli chkeit und Integritä t durch Verschlüs selung	elbv-2 acm-certificate-required	Zum Schutz von eventuell vorhanden en sensiblen Daten sowie von Daten während der Übertragung muss die Verschlüsselung für Ihr Elastic Load Balancing aktiviert sein. Verwenden Sie AWS Certificate Manager, um öffentlic he und private SSL/ TLS-Zertifikate mit AWS Diensten und internen Ressource n zu verwalten, bereitzustellen und bereitzustellen.
AC-17(2)	Remote-Zugriff | Schutz von Vertrauli chkeit und Integritä t durch Verschlüs selung	elb-tls-https-listeners-nur	Stellen Sie sicher, dass Ihre Elastic Load Balancer (ELBs) mit SSL- oder HTTPS-Listenern konfiguriert sind. Um eventuell vorhanden e sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-17(2)	Remote-Zugriff | Schutz von Vertraulichkeit und Integrität durch Verschlüsselung	opensearch-https-required	Da sensible Daten existieren können und um Daten während der Übertragung zu schützen, sollten Sie sicherstellen, dass HTTPS für Verbindungen zu Ihren Amazon OpenSearch Service-Domains aktiviert ist.
AC-17(2)	Remote-Zugriff | Schutz von Vertraulichkeit und Integrität durch Verschlüsselung	alb-http-to-https-Umleitungsprüfung	Um Daten während der Übertragung zu schützen, stellen Sie sicher, dass Ihr Application Load Balancer unverschlüsselte HTTP-Anfragen automatisch an HTTPS umleitet. Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-17(2)	Remote-Zugriff | Schutz von Vertrauli chkeit und Integritä t durch Verschlüs selung	api-gw-ssl-enabled	Stellen Sie sicher, dass die REST-API-Stufen von Amazon API Gateway mit SSL-Zertifikaten konfiguri ert sind, damit Backend-Systeme überprüfen können, ob Anforderungen von API Gateway stammen.
AC-17(2)	Remote-Zugriff | Schutz von Vertrauli chkeit und Integritä t durch Verschlüs selung	elb-acm-certificate-required	Zum Schutz von eventuell vorhanden en sensiblen Daten sowie von Daten während der Übertragung muss die Verschlüsselung für Ihr Elastic Load Balancing aktiviert sein. Verwenden Sie AWS Certificate Manager, um öffentlic he und private SSL/ TLS-Zertifikate mit AWS Diensten und internen Ressource n zu verwalten, bereitzustellen und bereitzustellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-17(2)	Remote-Zugriff | Schutz von Vertraulichkeit und Integrität durch Verschlüsselung	s-3 bucket-ssl-requests-only	Um Daten während der Übertragung zu schützen, stellen Sie sicher, dass Ihre Amazon Simple Storage Service (Amazon S3)-Buckets Anfragen zur Verwendung von Secure Socket Layer (SSL)-Buckets erfordern. Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-21	Weitergabe von Informationen	autoscaling-launch-config-public-ip-deaktiviert	Wenn Sie Ihre Netzwerkschnittstellen mit einer öffentlichen IP-Adresse konfigurieren, sind die diesen Netzwerkschnittstellen zugehörigen Ressourcen über das Internet erreichbar. EC2 Ressourcen sollten nicht öffentlich zugänglich sein, da dies einen unbeabsichtigten Zugriff auf Ihre Anwendungen oder Server ermöglichen kann.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-21	Weitergabe von Informationen	ec2- instances-in-vpc	Stellen Sie Amazon Elastic Compute Cloud (Amazon EC2) -Instances innerhalb einer Amazon Virtual Private Cloud (Amazon VPC) bereit, um eine sichere Kommunika tion zwischen einer Instance und anderen Services innerhalb der Amazon VPC zu ermöglichen, ohne dass ein Internet-Gateway, ein NAT-Gerät oder eine VPN-Verbindung erforderlich ist. Der gesamte Datenverk ehr bleibt sicher in der AWS Cloud. Domains, die sich innerhalb einer VPC befinden, verfügen aufgrund ihrer logischen Isolierun g im Vergleich zu Domains mit öffentlic hen Endpunkten über eine zusätzlic he Sicherheitsebene. Weisen Sie EC2

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			Amazon-Instances einer Amazon-VPC zu, um den Zugriff ordnungsgemäß zu verwalten.
AC-21	Weitergabe von Informationen	ssm-document-not-public	Stellen Sie sicher, dass AWS Systems Manager (SSM) - Dokumente nicht öffentlich sind, da dies einen unbeabsichtigten Zugriff auf Ihre SSM-Dokumente ermöglichen kann. Ein öffentliches SSM-Dokument kann Informationen über Ihr Konto, Ihre Ressourcen und internen Prozesse preisgeben.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-21	Weitergabe von Informationen	dms-replication-not-public	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass auf DMS-Replikationsin stanzen nicht öffentlic h zugegriffen werden kann. DMS-Repli kations-Instances können vertrauli che Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.
AC-21	Weitergabe von Informationen	ebs-snapshot-public-restorable-überprüfen	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass EBS-Snapshots nicht öffentlich wiederher stellbar sind. EBS-Volume-Snapsho ts können vertrauli che Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-21	Weitergabe von Informationen	ec-2 instance-no-public-ip	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon Elastic Compute Cloud (Amazon EC2) - Instances nicht öffentlich zugänglich sind. EC2 Amazon-Instances können vertrauliche Informationen enthalten, und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-21	Weitergabe von Informationen	elasticsearch-in-vpc-only	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass sich Amazon OpenSearch OpenSearch Service (Service) - Domains innerhalb einer Amazon Virtual Private Cloud (Amazon VPC) befinden. Eine OpenSearch Service-Domain innerhalb einer Amazon VPC ermöglicht die sichere Kommunikation zwischen OpenSearch Service und anderen Services innerhalb der Amazon VPC, ohne dass ein Internet-Gateway, ein NAT-Gerät oder eine VPN-Verbindung erforderlich ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-21	Weitergabe von Informationen	emr-master-no-public-ip	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon EMR-Cluster-Masterknoten nicht öffentlich zugänglich sind. Amazon-EMR-Cluster-Hauptknoten können vertrauliche Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.
AC-21	Weitergabe von Informationen	lambda-function-public-access-verboten	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass AWS Lambda-Funktionen nicht öffentlich zugänglich sind. Der öffentliche Zugriff kann möglicherweise die Verfügbarkeit von Ressourcen beeinträchtigen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-21	Weitergabe von Informationen	lambda-inside-vpc	Stellen Sie AWS Lambda-Funktionen in einer Amazon Virtual Private Cloud (Amazon VPC) bereit, um eine sichere Kommunika tion zwischen einer Funktion und anderen Diensten innerhalb der Amazon VPC zu gewährleisten. Bei dieser Konfiguration sind kein Internet-Gateway, kein NAT-Gerät und keine VPN-Verbindung erforderlich. Der gesamte Datenverk ehr bleibt sicher in der Cloud. AWS Domains, die sich innerhalb einer VPC befinden, verfügen aufgrund ihrer logischen Isolierun g im Vergleich zu Domains mit öffentlic hen Endpunkten über eine zusätzliche Sicherheitsebene. Um den Zugriff ordnungsg emäß zu verwalten,

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			sollten AWS Lambda-Funktionen einer VPC zugewiesen werden.
AC-21	Weitergabe von Informationen	opensearch-in-vpc-only	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass sich Amazon OpenSearch Service-Domains innerhalb einer Amazon Virtual Private Cloud (Amazon VPC) befinden. Eine Amazon OpenSearch Service-Domain innerhalb einer Amazon VPC ermöglicht die sichere Kommunikation zwischen Amazon OpenSearch Service und anderen Services innerhalb der Amazon VPC, ohne dass ein Internet-Gateway, ein NAT-Gerät oder eine VPN-Verbindung erforderlich ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-21	Weitergabe von Informationen	rds-instance-public-access-überprüfen	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Relational Database Service (Amazon RDS) -Instances nicht öffentlich sind. Amazon-RDS-Datenbank-Instances können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-21	Weitergabe von Informationen	rds-snapshots-public-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Relational Database Service (Amazon RDS) -Instances nicht öffentlich sind. Amazon-RDS-Datenbank-Instances können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-21	Weitergabe von Informationen	redshift-cluster-public-access-überprüfen	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Redshift Redshift-Cluster nicht öffentlich sind. Amazon-Redshift-Cluster können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-21	Weitergabe von Informationen	s3- -Block-periodisch account-level-public-access	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Simple Storage Service (Amazon S3) -Buckets nicht öffentlich zugänglich sind. Diese Regel trägt dazu bei, sensible Daten vor unbefugten Remote-Benutzern zu schützen, indem sie den öffentlichen Zugriff verhindert. Mit dieser Regel können Sie optional die Parameter ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) und restrictPublicBuckets Parameter (Config Default: True) festlegen. Die tatsächlichen Werte müssen den Richtlini

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			en Ihrer Organisation entsprechen.
AC-21	Weitergabe von Informationen	s3 bucket-level-public-access - verboten	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Simple Storage Service (Amazon S3) -Buckets nicht öffentlich zugänglich sind. Diese Regel trägt dazu bei, sensible Daten vor unbefugten Remote-Benutzern zu schützen, indem sie den öffentlichen Zugriff auf Bucket-Ebene verhindert.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-21	Weitergabe von Informationen	s-3 bucket-public-read -prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie nur autorisierten Benutzern, Prozessen und Geräten Zugriff auf Amazon Simple Storage Service (Amazon S3) - Buckets gewähren. Die Verwaltung des Zugriffs sollte mit der Klassifizierung der Daten übereinst immen.
AC-21	Weitergabe von Informationen	s3- bucket-public-writ e-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie nur autorisierten Benutzern, Prozessen und Geräten Zugriff auf Amazon Simple Storage Service (Amazon S3) - Buckets gewähren. Die Verwaltung des Zugriffs sollte mit der Klassifizierung der Daten übereinst immen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-21	Weitergabe von Informationen	sagemaker-notebook-no-direct-Internetzugang	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass SageMaker Amazon-Notebooks keinen direkten Internetzugang zulassen. Indem Sie direkten Internetzugang blockieren, vermeiden Sie, dass unbefugte Benutzer auf sensible Daten zugreifen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AC-21	Weitergabe von Informationen	subnet-auto-assign-public-ip-deaktiviert	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon Virtual Private Cloud (VPC) -Subnetzen nicht automatisch eine öffentliche IP-Adresse zugewiesen wird. Amazon Elastic Compute Cloud (EC2) -Instances, die in Subnetzen gestartet werden, in denen dieses Attribut aktiviert ist, haben ihrer primären Netzwerkschnittstelle eine öffentliche IP-Adresse zugewiesen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AU-2	Ereignisprotokollierung	elasticsearch-logs-to-cloudwatch	Stellen Sie sicher, dass für Amazon OpenSearch Service-Domains Fehlerprotokolle aktiviert und zur Aufbewahrung und Beantwortung an Amazon CloudWatch Logs gestreamt werden. Domain-Fehlerprotokolle sind bei Sicherheits- und Zugriffsprüfungen sowie bei der Diagnose von Verfügbarkeitsproblemen nützlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AU-2	Ereignisprotokollierung	multi-region-cloudtrail-enabled	AWS CloudTrail zeichnet Aktionen und API-Aufrufe der AWS Management Console auf. Sie können feststellen, welche Benutzer und Konten angerufen wurden AWS, von welcher Quell-IP-Adresse aus die Anrufe getätigt wurden und wann die Anrufe erfolgten. CloudTrail übermittelt Protokolldateien aus allen AWS Regionen an Ihren S3-Bucket , wenn MULTI_REGION_CLOUD_TRAIL_ENABLED aktiviert ist. Außerdem wird beim AWS Start einer neuen Region derselbe Trail in der neuen Region erstellt. CloudTrail Dadurch erhalten Sie automatisch Protokolldateien mit API-Aktivitäten für die neue Region.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AU-2	Ereignisprotokollierung	opensearch-logs-to-cloudwatch	Stellen Sie sicher, dass für Amazon OpenSearch Service-Domains Fehlerprotokolle aktiviert und zur Aufbewahrung und Beantwortung an Amazon CloudWatch Logs gestreamt werden. OpenSearch Service-Fehlerprotokolle können bei Sicherheits- und Zugriffsprüfungen helfen und bei der Diagnose von Verfügbarkeitsproblemen helfen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AU-2	Ereignisprotokollierung	rds-logging-enabled	Um die Protokollierung und Überwachung in Ihrer Umgebung zu erleichtern, stellen Sie sicher, dass die Amazon Relational Database Service (Amazon RDS)-Protokollierung aktiviert ist. Mit der Amazon-RDS-Protokollierung können Sie Ereignisse wie Verbindungen, Verbindungsabbrüche, Abfragen oder abgefragte Tabellen erfassen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AU-2	Ereignisprotokollierung	wafv2-logging-enabled	Um die Protokollierung und Überwachung in Ihrer Umgebung zu erleichtern, aktivieren Sie die AWS WAF (V2) -Protokollierung im regionalen und globalen Internet ACLs. AWS Die WAF-Protokollierung bietet detaillierte Informationen über den Datenverkehr, der von Ihrer Web-ACL analysiert wird. In den Protokollen werden die Uhrzeit aufgezeichnet, zu der die AWS WAF die Anfrage von Ihrer AWS Ressource erhalten hat, Informationen über die Anfrage und eine Aktion für die Regel, der jede Anfrage entsprach.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AU-2	Ereignisprotokollierung	api-gw-execution-logging-aktiviert	Die API-Gateway-Protokollierung zeigt detaillierte Ansichten der Benutzer, die auf die API zugegriffen haben, und wie diese Benutzer auf die API zugegriffen haben. Diese Einblicke ermöglichen die Transparenz von Benutzeraktivitäten.
AU-2	Ereignisprotokollierung	cloud-trail-cloud-watch-logs-aktiviert	Verwenden Sie Amazon CloudWatch , um Protokollereignisaktivitäten zentral zu sammeln und zu verwalten. Die Aufnahme von AWS CloudTrail Daten liefert Einzelheiten zu den API-Aufrufaktivitäten in Ihrem AWS-Konto.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AU-2	Ereignisprotokollierung	cloudtrail-enabled	AWS CloudTrail kann bei der Nichtabstreitbarkeit helfen, indem Aktionen und API-Aufrufe der AWS Management Console aufgezeichnet werden. Sie können die Benutzer und die Benutzer AWS-Konten , die einen AWS Dienst aufgerufen haben, die Quell-IP-Adresse, über die die Aufrufe generiert wurden, und den Zeitpunkt der Anrufe identifizieren. Einzelheiten zu den erfassten Daten finden Sie in den AWS CloudTrail Datensatzinhalten.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AU-2	Ereignisprotokollierung	cloudtrail-s3-dataevents-enabled	Die Erfassung von Simple Storage Service (Amazon S3)-Datenereignissen unterstützt die Erkennung von ungewöhnlichen Aktivitäten. Zu den Details gehören AWS-Konto Informationen über den Zugriff auf einen Amazon S3 S3-Bucket, die IP-Adresse und die Uhrzeit des Ereignisses.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AU-2	Ereignisprotokollierung	elb-logging-enabled	Die Elastic-Load-Balancing-Aktivität ist ein zentraler Kommunikationspunkt innerhalb einer Umgebung. Stellen Sie sicher, dass die ELB-Protokollierung aktiviert ist. Die gesammelten Daten enthalten detaillierte Informationen zu Anfragen, die an den ELB gesendet wurden. Jedes Protokoll enthält Informationen wie die Zeit, zu der die Anforderung einging, die Client-IP-Adresse, Latenzen, Anforderungspfade und Serverantworten.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AU-2	Ereignisprotokollierung	redshift-cluster-configuration-check	Um Daten im Ruhezustand zu schützen, muss die Verschlüsselung für Ihre Amazon-Redshift-Cluster aktiviert sein. Sie müssen auch sicherstellen, dass die erforderlichen Konfigurationen auf Amazon-Redshift-Clustern bereitgestellt werden. Die Prüfungsprotokollierung muss aktiviert sein, um Informationen zu Verbindungen und Benutzeraktivitäten in der Datenbank bereitzustellen. Diese Regel erfordert, dass ein Wert für clusterDbEncrypted (Config Default: TRUE) und LoggingEnabled (Config Default: TRUE) gesetzt ist. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AU-2	Ereignisprotokollierung	s3- bucket-logging-enabled	Die Amazon Simple Storage Service (Amazon S3)-Serverzugriffsprotokollierung bietet eine Methode zur Überwachung des Netzwerks im Hinblick auf potenzielle Cybersicherheitsereignisse. Die Ereignisse werden überwacht, indem detaillierte Aufzeichnungen über die Anfragen erfasst werden, die an einen Amazon-S3-Bucket gestellt wurden. Jeder Zugriffsprotokolleintrag enthält Details zu einer einzelnen Zugriffsanfrage. Zu den Details gehören Anforderer, Bucket-Name, Anforderungszeit, Anforderungsaktion, Antwortstatus und Fehlercode, falls relevant.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AU-2	Ereignisprotokollierung	vpc-flow-logs-enabled	VPC-Flow-Protokolle erfassen detaillierte Informationsdatensätze über den IP-Datenverkehr, der zu und von Netzwerkschnittstellen in Ihrer Amazon Virtual Private Cloud (Amazon VPC) fließt. Standardmäßig enthalten Flow-Protokolldatensätze Werte für die verschiedenen Komponenten des IP-Flows, einschließlich Quelle, Ziel und Protokoll.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AU-3	Inhalt der Prüfungsunterlagen	elasticsearch-logs-to-cloudwatch	Stellen Sie sicher, dass für Amazon OpenSearch Service-Domains Fehlerprotokolle aktiviert und zur Aufbewahrung und Beantwortung an Amazon CloudWatch Logs gestreamt werden. Domain-Fehlerprotokolle sind bei Sicherheits- und Zugriffsprüfungen sowie bei der Diagnose von Verfügbarkeitsproblemen nützlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AU-3	Inhalt der Prüfungsunterlagen	multi-region-cloudtrail-enabled	AWS CloudTrail zeichnet Aktionen und API-Aufrufe der AWS Management Console auf. Sie können feststellen, welche Benutzer und Konten angerufen wurden AWS, von welcher Quell-IP-Adresse aus die Anrufe getätigt wurden und wann die Anrufe erfolgten. CloudTrail übermittelt Protokolldateien aus allen AWS Regionen an Ihren S3-Bucket , wenn MULTI_REGION_CLOUD_TRAIL_ENABLED aktiviert ist. Außerdem wird beim AWS Start einer neuen Region derselbe Trail in der neuen Region erstellt. CloudTrail Dadurch erhalten Sie automatisch Protokolldateien mit API-Aktivitäten für die neue Region.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AU-3	Inhalt der Prüfungsunterlagen	opensearch-logs-to-cloudwatch	Stellen Sie sicher, dass für Amazon OpenSearch Service-Domains Fehlerprotokolle aktiviert und zur Aufbewahrung und Beantwortung an Amazon CloudWatch Logs gestreamt werden. OpenSearch Service-Fehlerprotokolle können bei Sicherheits- und Zugriffsprüfungen helfen und bei der Diagnose von Verfügbarkeitsproblemen helfen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AU-3	Inhalt der Prüfungsunterlagen	wafv2-logging-enabled	Um die Protokollierung und Überwachung in Ihrer Umgebung zu erleichtern, aktivieren Sie die AWS WAF (V2) -Protokollierung im regionalen und globalen Internet ACLs. AWS Die WAF-Protokollierung bietet detaillierte Informationen über den Datenverkehr, der von Ihrer Web-ACL analysiert wird. In den Protokollen werden die Uhrzeit aufgezeichnet, zu der die AWS WAF die Anfrage von Ihrer AWS Ressource erhalten hat, Informationen über die Anfrage und eine Aktion für die Regel, der jede Anfrage entsprach.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AU-3	Inhalt der Prüfungsunterlagen	api-gw-execution-logging-aktiviert	Die API-Gateway-Protokollierung zeigt detaillierte Ansichten der Benutzer, die auf die API zugegriffen haben, und wie diese Benutzer auf die API zugegriffen haben. Diese Einblicke ermöglichen die Transparenz von Benutzeraktivitäten.
AU-3	Inhalt der Prüfungsunterlagen	cloud-trail-cloud-watch-logs-aktiviert	Verwenden Sie Amazon CloudWatch , um Protokollereignisaktivitäten zentral zu sammeln und zu verwalten. Die Aufnahme von AWS CloudTrail Daten liefert Einzelheiten zu den API-Aufrufaktivitäten in Ihrem AWS-Konto.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AU-3	Inhalt der Prüfungsunterlagen	cloudtrail-enabled	AWS CloudTrail kann bei der Nichtabstreitbarkeit helfen, indem Aktionen und API-Aufrufe der AWS Management Console aufgezeichnet werden. Sie können die Benutzer und die Benutzer AWS-Konten , die einen AWS Dienst aufgerufen haben, die Quell-IP-Adresse, über die die Aufrufe generiert wurden, und den Zeitpunkt der Anrufe identifizieren. Einzelheiten zu den erfassten Daten finden Sie in den AWS CloudTrail Datensatzinhalten.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AU-3	Inhalt der Prüfungsunterlagen	cloudtrail-s3-dataevents-enabled	Die Erfassung von Simple Storage Service (Amazon S3)-Datenereignissen unterstützt die Erkennung von ungewöhnlichen Aktivitäten. Zu den Details gehören AWS-Konto Informationen über den Zugriff auf einen Amazon S3 S3-Bucket, die IP-Adresse und die Uhrzeit des Ereignisses.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AU-3	Inhalt der Prüfungsunterlagen	elb-logging-enabled	Die Elastic-Load-Balancing-Aktivität ist ein zentraler Kommunikationspunkt innerhalb einer Umgebung. Stellen Sie sicher, dass die ELB-Protokollierung aktiviert ist. Die gesammelten Daten enthalten detaillierte Informationen zu Anfragen, die an den ELB gesendet wurden. Jedes Protokoll enthält Informationen wie die Zeit, zu der die Anforderung einging, die Client-IP-Adresse, Latenzen, Anforderungspfade und Serverantworten.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AU-3	Inhalt der Prüfungsunterlagen	rds-logging-enabled	Um die Protokollierung und Überwachung in Ihrer Umgebung zu erleichtern, stellen Sie sicher, dass die Amazon Relational Database Service (Amazon RDS)-Protokollierung aktiviert ist. Mit der Amazon-RDS-Protokollierung können Sie Ereignisse wie Verbindungen, Verbindungsabbrüche, Abfragen oder abgefragte Tabellen erfassen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AU-3	Inhalt der Prüfungsunterlagen	redshift-cluster-configuration-check	Um Daten im Ruhezustand zu schützen, muss die Verschlüsselung für Ihre Amazon-Redshift-Cluster aktiviert sein. Sie müssen auch sicherstellen, dass die erforderlichen Konfigurationen auf Amazon-Redshift-Clustern bereitgestellt werden. Die Prüfungsprotokollierung muss aktiviert sein, um Informationen zu Verbindungen und Benutzeraktivitäten in der Datenbank bereitzustellen. Diese Regel erfordert, dass ein Wert für clusterDbEncrypted (Config Default: TRUE) und LoggingEnabled (Config Default: TRUE) gesetzt ist. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AU-3	Inhalt der Prüfungsunterlagen	s3- bucket-logging-enabled	Die Amazon Simple Storage Service (Amazon S3)-Serverzugriffsprotokollierung bietet eine Methode zur Überwachung des Netzwerks im Hinblick auf potenzielle Cybersicherheitsereignisse. Die Ereignisse werden überwacht, indem detaillierte Aufzeichnungen über die Anfragen erfasst werden, die an einen Amazon-S3-Bucket gestellt wurden. Jeder Zugriffsprotokolleintrag enthält Details zu einer einzelnen Zugriffsanfrage. Zu den Details gehören Anforderer, Bucket-Name, Anforderungszeit, Anforderungsaktion, Antwortstatus und Fehlercode, falls relevant.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AU-3	Inhalt der Prüfungsunterlagen	vpc-flow-logs-enabled	VPC-Flow-Protokolle erfassen detaillierte Informationsdatensätze über den IP-Datenverkehr, der zu und von Netzwerkschnittstellen in Ihrer Amazon Virtual Private Cloud (Amazon VPC) fließt. Standardmäßig enthalten Flow-Protokolldatensätze Werte für die verschiedenen Komponenten des IP-Flows, einschließlich Quelle, Ziel und Protokoll.
AU-6(1)	Überprüfung, Analyse und Berichterstattung von Prüfungsunterlagen | Automatisierte Prozessintegration	cloud-trail-cloud-watch-logs-aktiviert	Verwenden Sie Amazon CloudWatch , um Protokoll ereignisaktivitäten zentral zu sammeln und zu verwalten. Die Aufnahme von AWS CloudTrail Daten liefert Einzelheiten zu den API-Aufrufaktivitäten in Ihrem AWS-Konto.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AU-6(1)	Überprüfung, Analyse und Berichterstattung von Prüfungsu nterlagen | Automatis ierte Prozessin tegration	guardduty-enabled-centralized	Amazon GuardDuty kann mithilfe von Threat Intellige nce Feeds helfen, potenzielle Cybersich erheitsereignisse zu überwachen und zu erkennen. Dazu gehören Listen mit bösartigen IPs und maschinel len Lernmethoden zur Identifizierung unerwarteter, nicht autorisierter und bösartiger Aktivitäten in Ihrer AWS Cloud-Umgebung.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AU-6(1)	Überprüfung, Analyse und Berichterstattung von Prüfungsunterlagen | Automatisierte Prozessintegration	securityhub-enabled	AWS Security Hub hilft bei der Überwachung von unbefugtem Personal, Verbindungen, Geräten und Software. AWS Security Hub aggregiert, organisiert und priorisiert die Sicherheitswarnungen oder Ergebnisse mehrerer Dienste. AWS Einige dieser Dienste sind Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer und AWS Firewall Manager sowie AWS Partnerlösungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AU-6(1)	Überprüfung, Analyse und Berichterstattung von Prüfungsunterlagen | Automatisierte Prozessintegration	cloudwatch-alarm-action-check	Amazon CloudWatch alarmiert, wenn eine Metrik den Schwellenwert für eine bestimmte Anzahl von Bewertungszeiträumen überschreitet. Der Alarm führt eine oder mehrere Aktionen durch, die vom Wert der Metrik oder des Ausdrucks im Vergleich zu einem Schwellenwert in einer Reihe von Zeiträumen abhängt. Diese Regel erfordert einen Wert für alarmActionRequired (Config Default: True), insufficientDataAction Required (Config Default: True), okActionRequired (Config Default: False). Der tatsächliche Wert muss die Alarmaktionen für Ihre Umgebung widerspiegeln.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AU-6(3)	Überprüfung, Analyse und Berichterstattung von Prüfungsunterlagen | Korrelation der Repositorys für Prüfungsunterlagen	elasticsearch-logs-to-cloudwatch	Stellen Sie sicher, dass für Amazon OpenSearch Service-Domains Fehlerprotokolle aktiviert und zur Aufbewahrung und Beantwortung an Amazon CloudWatch Logs gestreamt werden. Domain-Fehlerprotokolle sind bei Sicherheits- und Zugriffsprüfungen sowie bei der Diagnose von Verfügbarkeitsproblemen nützlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AU-6(3)	Überprüfung, Analyse und Berichterstattung von Prüfungsu nterlagen | Korrelati on der Repositorys für Prüfungsunterlagen	multi-region-cloudtrail-enabled	AWS CloudTrail zeichnet Aktionen und API-Aufrufe der AWS Management Console auf. Sie können feststellen, welche Benutzer und Konten angerufen wurden AWS, von welcher Quell-IP-Adresse aus die Anrufe getätigt wurden und wann die Anrufe erfolgten. CloudTrail übermittelt Protokolldateien aus allen AWS Regionen an Ihren S3-Bucket , wenn MULTI_REG ION_CLOUD _TRAIL_ENABLED aktiviert ist. Außerdem wird beim AWS Start einer neuen Region derselbe Trail in der neuen Region erstellt. CloudTrail Dadurch erhalten Sie automatis ch Protokolldateien mit API-Aktivitäten für die neue Region.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AU-6(3)	Überprüfung, Analyse und Berichterstattung von Prüfungsunterlagen | Korrelation der Repositorys für Prüfungsunterlagen	opensearch-logs-to-cloudwatch	Stellen Sie sicher, dass für Amazon OpenSearch Service-Domains Fehlerprotokolle aktiviert und zur Aufbewahrung und Beantwortung an Amazon CloudWatch Logs gestreamt werden. OpenSearch Service-Fehlerprotokolle können bei Sicherheits- und Zugriffsprüfungen helfen und bei der Diagnose von Verfügbarkeitsproblemen helfen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AU-6(3)	Überprüfung, Analyse und Berichterstattung von Prüfungsunterlagen | Korrelation der Repositorys für Prüfungsunterlagen	wafv2-logging-enabled	Um die Protokollierung und Überwachung in Ihrer Umgebung zu erleichtern, aktivieren Sie die AWS WAF (V2) -Protokollierung im regionalen und globalen Internet ACLs. AWS Die WAF-Protokollierung bietet detaillierte Informationen über den Datenverkehr, der von Ihrer Web-ACL analysiert wird. In den Protokollen werden die Uhrzeit aufgezeichnet, zu der die AWS WAF die Anfrage von Ihrer AWS Ressource erhalten hat, Informationen über die Anfrage und eine Aktion für die Regel, der jede Anfrage entsprach.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AU-6(3)	Überprüfung, Analyse und Berichterstattung von Prüfungsunterlagen | Korrelation der Repositorys für Prüfungsunterlagen	api-gw-execution-logging-aktiviert	Die API-Gateway-Protokollierung zeigt detaillierte Ansichten der Benutzer, die auf die API zugegriffen haben, und wie diese Benutzer auf die API zugegriffen haben. Diese Einblicke ermöglichen die Transparenz von Benutzeraktivitäten.
AU-6(3)	Überprüfung, Analyse und Berichterstattung von Prüfungsunterlagen | Korrelation der Repositorys für Prüfungsunterlagen	cloud-trail-cloud-watch-logs-aktiviert	Verwenden Sie Amazon CloudWatch , um Protokollereignisaktivitäten zentral zu sammeln und zu verwalten. Die Aufnahme von AWS CloudTrail Daten liefert Einzelheiten zu den API-Aufrufaktivitäten in Ihrem AWS-Konto.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AU-6(3)	Überprüfung, Analyse und Berichterstattung von Prüfungsu nterlagen | Korrelati on der Repositorys für Prüfungsunterlagen	cloudtrail-enabled	AWS CloudTrail kann bei der Nichtabst reitbarkeit helfen, indem Aktionen und API-Aufrufe der AWS Management Console aufgezeic hnet werden. Sie können die Benutzer und die Benutzer AWS-Konten , die einen AWS Dienst aufgerufen haben, die Quell-IP-Adresse, über die die Aufrufe generiert wurden, und den Zeitpunkt der Anrufe identifiz ieren. Einzelheiten zu den erfassten Daten finden Sie in den AWS CloudTrail Datensatzinhalten.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AU-6(3)	Überprüfung, Analyse und Berichterstattung von Prüfungsunterlagen | Korrelation der Repositorys für Prüfungsunterlagen	cloudtrail-s3-dataevents-enabled	Die Erfassung von Simple Storage Service (Amazon S3)-Datenereignissen unterstützt die Erkennung von ungewöhnlichen Aktivitäten. Zu den Details gehören AWS-Konto Informationen über den Zugriff auf einen Amazon S3 S3-Bucket, die IP-Adresse und die Uhrzeit des Ereignisses.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AU-6(3)	Überprüfung, Analyse und Berichterstattung von Prüfungsunterlagen | Korrelation der Repositorys für Prüfungsunterlagen	elb-logging-enabled	Die Elastic-Load-Balancing-Aktivität ist ein zentraler Kommunikationspunkt innerhalb einer Umgebung. Stellen Sie sicher, dass die ELB-Protokollierung aktiviert ist. Die gesammelten Daten enthalten detaillierte Informationen zu Anfragen, die an den ELB gesendet wurden. Jedes Protokoll enthält Informationen wie die Zeit, zu der die Anforderung einging, die Client-IP-Adresse, Latenzen, Anforderungspfade und Serverantworten.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AU-6(3)	Überprüfung, Analyse und Berichterstattung von Prüfungsunterlagen | Korrelation der Repositorys für Prüfungsunterlagen	rds-logging-enabled	Um die Protokollierung und Überwachung in Ihrer Umgebung zu erleichtern, stellen Sie sicher, dass die Amazon Relational Database Service (Amazon RDS)-Protokollierung aktiviert ist. Mit der Amazon-RDS-Protokollierung können Sie Ereignisse wie Verbindungen, Verbindungsabbrüche, Abfragen oder abgefragte Tabellen erfassen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AU-6(3)	Überprüfung, Analyse und Berichterstattung von Prüfungsunterlagen | Korrelation der Repositorys für Prüfungsunterlagen	redshift-cluster-configuration-check	Um Daten im Ruhezustand zu schützen, muss die Verschlüsselung für Ihre Amazon-Redshift-Cluster aktiviert sein. Sie müssen auch sicherstellen, dass die erforderlichen Konfigurationen auf Amazon-Redshift-Clustern bereitgestellt werden. Die Prüfungsprotokollierung muss aktiviert sein, um Informationen zu Verbindungen und Benutzeraktivitäten in der Datenbank bereitzustellen. Diese Regel erfordert, dass ein Wert für clusterDbEncrypted (Config Default: TRUE) und LoggingEnabled (Config Default: TRUE) gesetzt ist. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AU-6(3)	Überprüfung, Analyse und Berichterstattung von Prüfungsu nterlagen | Korrelati on der Repositorys für Prüfungsunterlagen	s3- bucket-logging-enabled	Die Amazon Simple Storage Service (Amazon S3)-Serverzugriffs protokollierung bietet eine Methode zur Überwachu ng des Netzwerks im Hinblick auf potenzielle Cybersich erheitsereignisse. Die Ereignisse werden überwacht, indem detaillierte Aufzeichn ungen über die Anfragen erfasst werden, die an einen Amazon-S3-Bucket gestellt wurden. Jeder Zugriffsprotokolle intrag enthält Details zu einer einzelnen Zugriffsanfrage. Zu den Details gehören Anforderer, Bucket-Name, Anforderu ngszeit, Anforderu ngsaktion, Antwortst atus und Fehlercode, falls relevant.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AU-6(3)	Überprüfung, Analyse und Berichterstattung von Prüfungsunterlagen | Korrelation der Repositorys für Prüfungsunterlagen	vpc-flow-logs-enabled	VPC-Flow-Protokolle erfassen detaillierte Informationsdatensätze über den IP-Datenverkehr, der zu und von Netzwerkschnittstellen in Ihrer Amazon Virtual Private Cloud (Amazon VPC) fließt. Standardmäßig enthalten Flow-Protokolldatensätze Werte für die verschiedenen Komponenten des IP-Flows, einschließlich Quelle, Ziel und Protokoll.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AU-6(4)	Prüfung, Analyse und Berichterstattung von Prüfungsunterlagen | Zentrale Überprüfung und Analyse	elasticsearch-logs-to-cloudwatch	Stellen Sie sicher, dass für Amazon OpenSearch Service-Domains Fehlerprotokolle aktiviert und zur Aufbewahrung und Beantwortung an Amazon CloudWatch Logs gestreamt werden. Domain-Fehlerprotokolle sind bei Sicherheits- und Zugriffsprüfungen sowie bei der Diagnose von Verfügbarkeitsproblemen nützlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AU-6(4)	Prüfung, Analyse und Berichterstattung von Prüfungsunterlagen | Zentrale Überprüfung und Analyse	multi-region-cloudtrail-enabled	AWS CloudTrail zeichnet Aktionen und API-Aufrufe der AWS Management Console auf. Sie können feststellen, welche Benutzer und Konten angerufen wurden AWS, von welcher Quell-IP-Adresse aus die Anrufe getätigt wurden und wann die Anrufe erfolgten. CloudTrail übermittelt Protokolldateien aus allen AWS Regionen an Ihren S3-Bucket , wenn MULTI_REG ION_CLOUD _TRAIL_ENABLED aktiviert ist. Außerdem wird beim AWS Start einer neuen Region derselbe Trail in der neuen Region erstellt. CloudTrail Dadurch erhalten Sie automatis ch Protokolldateien mit API-Aktivitäten für die neue Region.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AU-6(4)	Prüfung, Analyse und Berichterstattung von Prüfungsunterlagen | Zentrale Überprüfung und Analyse	opensearch-logs-to-cloudwatch	Stellen Sie sicher, dass für Amazon OpenSearch Service-Domains Fehlerprotokolle aktiviert und zur Aufbewahrung und Beantwortung an Amazon CloudWatch Logs gestreamt werden. OpenSearch Service-Fehlerprotokolle können bei Sicherheits- und Zugriffsprüfungen helfen und bei der Diagnose von Verfügbarkeitsproblemen helfen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AU-6(4)	Prüfung, Analyse und Berichterstattung von Prüfungsunterlagen | Zentrale Überprüfung und Analyse	wafv2-logging-enabled	Um die Protokollierung und Überwachung in Ihrer Umgebung zu erleichtern, aktivieren Sie die AWS WAF (V2) -Protokollierung im regionalen und globalen Internet ACLs. AWS Die WAF-Protokollierung bietet detaillierte Informationen über den Datenverkehr, der von Ihrer Web-ACL analysiert wird. In den Protokollen werden die Uhrzeit aufgezeichnet, zu der die AWS WAF die Anfrage von Ihrer AWS Ressource erhalten hat, Informationen über die Anfrage und eine Aktion für die Regel, der jede Anfrage entsprach.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AU-6(4)	Prüfung, Analyse und Berichterstattung von Prüfungsunterlagen | Zentrale Überprüfung und Analyse	api-gw-execution-logging-aktiviert	Die API-Gateway-Protokollierung zeigt detaillierte Ansichten der Benutzer, die auf die API zugegriff en haben, und wie diese Benutzer auf die API zugegriff en haben. Diese Einblicke ermöglichen die Transparenz von Benutzeraktivitäten.
AU-6(4)	Prüfung, Analyse und Berichterstattung von Prüfungsunterlagen | Zentrale Überprüfung und Analyse	cloud-trail-cloud-watch-logs-aktiviert	Verwenden Sie Amazon CloudWatc h , um Protokoll ereignisaktivitäten zentral zu sammeln und zu verwalten. Die Aufnahme von AWS CloudTrail Daten liefert Einzelheiten zu den API-Aufrufaktivitä ten in Ihrem AWS-Konto.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AU-6(4)	Prüfung, Analyse und Berichterstattung von Prüfungsunterlagen | Zentrale Überprüfung und Analyse	cloudtrail-enabled	AWS CloudTrail kann bei der Nichtabstreitbarkeit helfen, indem Aktionen und API-Aufrufe der AWS Management Console aufgezeichnet werden. Sie können die Benutzer und die Benutzer AWS-Konten , die einen AWS Dienst aufgerufen haben, die Quell-IP-Adresse, über die die Aufrufe generiert wurden, und den Zeitpunkt der Anrufe identifizieren. Einzelheiten zu den erfassten Daten finden Sie in den AWS CloudTrail Datensatzinhalten.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AU-6(4)	Prüfung, Analyse und Berichterstattung von Prüfungsunterlagen | Zentrale Überprüfung und Analyse	cloudtrail-s3-data events-enabled	Die Erfassung von Simple Storage Service (Amazon S3)-Datenereignissen unterstützt die Erkennung von ungewöhnlichen Aktivitäten. Zu den Details gehören AWS-Konto Informationen über den Zugriff auf einen Amazon S3 S3-Bucket, die IP-Adresse und die Uhrzeit des Ereignisses.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AU-6(4)	Prüfung, Analyse und Berichterstattung von Prüfungsunterlagen | Zentrale Überprüfung und Analyse	elb-logging-enabled	Die Elastic-Load-Balancing-Aktivität ist ein zentraler Kommunikationspunkt innerhalb einer Umgebung. Stellen Sie sicher, dass die ELB-Protokollierung aktiviert ist. Die gesammelten Daten enthalten detaillierte Informationen zu Anfragen, die an den ELB gesendet wurden. Jedes Protokoll enthält Informationen wie die Zeit, zu der die Anforderung einging, die Client-IP-Adresse, Latenzen, Anforderungspfade und Serverantworten.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AU-6(4)	Prüfung, Analyse und Berichterstattung von Prüfungsunterlagen | Zentrale Überprüfung und Analyse	rds-logging-enabled	Um die Protokollierung und Überwachung in Ihrer Umgebung zu erleichtern, stellen Sie sicher, dass die Amazon Relational Database Service (Amazon RDS)-Protokollierung aktiviert ist. Mit der Amazon-RDS-Protokollierung können Sie Ereignisse wie Verbindungen, Verbindungsabbrüche, Abfragen oder abgefragte Tabellen erfassen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AU-6(4)	Prüfung, Analyse und Berichterstattung von Prüfungsunterlagen | Zentrale Überprüfung und Analyse	redshift-cluster-configuration-check	Um Daten im Ruhezustand zu schützen, muss die Verschlüsselung für Ihre Amazon-Redshift-Cluster aktiviert sein. Sie müssen auch sicherstellen, dass die erforderlichen Konfigurationen auf Amazon-Redshift-Clustern bereitgestellt werden. Die Prüfungsprotokollierung muss aktiviert sein, um Informationen zu Verbindungen und Benutzeraktivitäten in der Datenbank bereitzustellen. Diese Regel erfordert, dass ein Wert für clusterDbEncrypted (Config Default: TRUE) und LoggingEnabled (Config Default: TRUE) gesetzt ist. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AU-6(4)	Prüfung, Analyse und Berichterstattung von Prüfungsunterlagen | Zentrale Überprüfung und Analyse	s3- bucket-logging-enabled	Die Amazon Simple Storage Service (Amazon S3)-Serverzugriffs protokollierung bietet eine Methode zur Überwachu ng des Netzwerks im Hinblick auf potenzielle Cybersich erheitsereignisse. Die Ereignisse werden überwacht, indem detaillierte Aufzeichn ungen über die Anfragen erfasst werden, die an einen Amazon-S3-Bucket gestellt wurden. Jeder Zugriffsprotokolle intrag enthält Details zu einer einzelnen Zugriffsanfrage. Zu den Details gehören Anforderer, Bucket-Name, Anforderu ngszeit, Anforderu ngsaktion, Antwortst atus und Fehlercode, falls relevant.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AU-6(4)	Prüfung, Analyse und Berichterstattung von Prüfungsunterlagen | Zentrale Überprüfung und Analyse	vpc-flow-logs-enabled	VPC-Flow-Protokolle erfassen detaillierte Informationsdatensätze über den IP-Datenverkehr, der zu und von Netzwerkschnittstellen in Ihrer Amazon Virtual Private Cloud (Amazon VPC) fließt. Standardmäßig enthalten Flow-Protokolldatensätze Werte für die verschiedenen Komponenten des IP-Flows, einschließlich Quelle, Ziel und Protokoll.
AU-6(5)	Überprüfung, Analyse und Berichterstattung von Prüfungsunterlagen | Integrierte Analyse von Prüfungsunterlagen	cloud-trail-cloud-watch-logs-aktiviert	Verwenden Sie Amazon CloudWatch , um Protokoll ereignisaktivitäten zentral zu sammeln und zu verwalten. Die Aufnahme von AWS CloudTrail Daten liefert Einzelheiten zu den API-Aufrufaktivitäten in Ihrem AWS-Konto.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AU-6(5)	Überprüfung, Analyse und Berichterstattung von Prüfungsu nterlagen | Integrier te Analyse von Prüfungsunterlagen	guardduty-enabled-centralized	Amazon GuardDuty kann mithilfe von Threat Intellige nce Feeds helfen, potenzielle Cybersich erheitsereignisse zu überwachen und zu erkennen. Dazu gehören Listen mit bösartigen IPs und maschinel len Lernmethoden zur Identifizierung unerwarteter, nicht autorisierter und bösartiger Aktivitäten in Ihrer AWS Cloud-Umgebung.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AU-6(5)	Überprüfung, Analyse und Berichterstattung von Prüfungsu nterlagen | Integrier te Analyse von Prüfungsunterlagen	securityhub-enabled	AWS Security Hub hilft bei der Überwachung von unbefugtem Personal, Verbindun gen, Geräten und Software. AWS Security Hub aggregiert, organisie rt und priorisie rt die Sicherhei tswarnungen oder Ergebnisse mehrerer Dienste. AWS Einige dieser Dienste sind Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer und AWS Firewall Manager sowie AWS Partnerlösungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AU-6(5)	Überprüfung, Analyse und Berichterstattung von Prüfungsunterlagen | Integrierte Analyse von Prüfungsunterlagen	cloudwatch-alarm-action-check	Amazon CloudWatch alarmiert, wenn eine Metrik den Schwellenwert für eine bestimmte Anzahl von Bewertungszeiträumen überschreitet. Der Alarm führt eine oder mehrere Aktionen durch, die vom Wert der Metrik oder des Ausdrucks im Vergleich zu einem Schwellenwert in einer Reihe von Zeiträumen abhängt. Diese Regel erfordert einen Wert für alarmActionRequired (Config Default: True), insufficientDataAction Required (Config Default: True), okActionRequired (Config Default: False). Der tatsächliche Wert muss die Alarmaktionen für Ihre Umgebung widerspiegeln.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AU-7(1)	Reduzierung von Prüfungsunterlagen und Berichtserstellung | Automatische Verarbeitung	cloud-trail-cloud-watch-logs-aktiviert	Verwenden Sie Amazon CloudWatch , um Protokoll ereignisaktivitäten zentral zu sammeln und zu verwalten. Die Aufnahme von AWS CloudTrail Daten liefert Einzelheiten zu den API-Aufrufaktivitäten in Ihrem AWS-Konto.
AU-9(2)	Schutz von Prüfungsinformationen | Speicherung auf separaten physischen Systemen oder Komponenten	s-3 version-lifecycle-policy-check	Mit Amazon-S3-Lebenszyklusregeln können Sie Aktionen definieren, die Amazon S3 während der Lebensdauer eines Objekts ausführen soll (z. B. die Überführung von Objekten in eine andere Speicherklasse, ihre Archivierung oder Löschung nach einem bestimmten Zeitraum).

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AU-9(2)	Schutz von Prüfungsinformationen | Speicherung auf separaten physischen Systemen oder Komponenten	s-3 bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) unterstützt die Aufrechterhaltung einer angemessenen Kapazität und Verfügbarkeit. CRR ermöglicht das automatische, asynchrone Kopieren von Objekten in Amazon-S3-Buckets, um die Datenverfügbarkeit sicherzustellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AU-9(2)	Schutz von Prüfungsinformationen | Speicherung auf separaten physischen Systemen oder Komponenten	s-3 bucket-versioning-enabled	Die Versionsverwaltung von Amazon Simple Storage Service (Amazon S3)-Buckets hilft dabei, mehrere Varianten eines Objekts im selben Amazon-S3-Bucket zu speichern. Verwenden Sie die Versionsverwaltung, um sämtliche Versionen aller Objekte in Ihrem Amazon-S3-Bucket zu speichern, abzurufen oder wiederherzustellen. Mit der Versionsverwaltung können Sie Versionen sowohl nach unbeabsichtigten Benutzeraktionen als auch nach Anwendungsfehlern problemlos wiederherstellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AU-9(7)	Schutz von Prüfungsinformationen | Speicherung auf einer Komponente mit einem anderen Betriebssystem	cloud-trail-cloud-watch-logs-aktiviert	Verwenden Sie Amazon CloudWatch , um Protokoll ereignisaktivitäten zentral zu sammeln und zu verwalten. Die Aufnahme von AWS CloudTrail Daten liefert Einzelheiten zu den API-Aufrufaktivitäten in Ihrem AWS-Konto.
AU-9	Schutz von Prüfungsinformationen	s-3 default-encryption-kms	Stellen Sie sicher, dass die Verschlüsselung für Ihre Amazon Simple Storage Service (Amazon S3)-Buckets aktiviert ist. Um eventuell vorhandene sensible Daten im Ruhezustand in einem Amazon-S3-Bucket zu schützen, muss die Verschlüsselung aktiviert sein.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AU-9	Schutz von Prüfungsinformationen	cloudtrail-enabled	AWS CloudTrail kann durch die Aufzeichnung von Aktionen und API-Aufrufen in der AWS Management Console bei der Nichtabstreitbarkeit helfen. Sie können die Benutzer und die Benutzer AWS-Konten , die einen AWS Dienst aufgerufen haben, die Quell-IP-Adresse, über die die Aufrufe generiert wurden, und den Zeitpunkt der Anrufe identifizieren. Einzelheiten zu den erfassten Daten finden Sie in den AWS CloudTrail Datensatzinhalten.
AU-9	Schutz von Prüfungsinformationen	cloud-trail-encryption-enabled	Da sensible Daten vorhanden sein können und um Daten im Speicher zu schützen, sollten Sie sicherstellen, dass die Verschlüsselung für Ihre AWS CloudTrail Spuren aktiviert ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AU-9	Schutz von Prüfungsinformationen	cloud-trail-log-file-Validierung aktiviert	Verwenden Sie die AWS CloudTrail Protokolldateivalidierung, um die Integrität von Protokollen zu überprüfen. CloudTrail Mithilfe der Protokolldateivalidierung kann festgestellt werden, ob eine Protokolldatei geändert oder gelöscht wurde oder ob sie nach der Übermittlung CloudTrail unverändert geblieben ist. Dieses Feature wurde mit dem Branchenstandard entsprechenden Algorithmen entwickelt: SHA-256 für die Hashfunktion und SHA-256 mit RSA für digitale Signaturen. Das macht es rechnerisch unmöglich, CloudTrail Protokolldateien unbemerkt zu ändern, zu löschen oder zu fälschen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AU-9	Schutz von Prüfungsinformationen	s3- aktiviert bucket-server-side-encryption	Zum Schutz von Daten im Ruhezustand müssen Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon Simple Storage Service (Amazon S3)-Buckets aktiviert ist. Um eventuell vorhandene sensible Daten im Ruhezustand in Amazon-S3-Buckets zu schützen, muss die Verschlüsselung aktiviert sein.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AU-10	Nichtabstreitbarkeit	elasticsearch-logs-to-cloudwatch	Stellen Sie sicher, dass für Amazon OpenSearch Service-Domains Fehlerprotokolle aktiviert und zur Aufbewahrung und Beantwortung an Amazon CloudWatch Logs gestreamt werden. Domain-Fehlerprotokolle sind bei Sicherheits- und Zugriffsprüfungen sowie bei der Diagnose von Verfügbarkeitsproblemen nützlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AU-10	Nichtabstreitbarkeit	multi-region-cloudtrail-enabled	AWS CloudTrail zeichnet Aktionen und API-Aufrufe der AWS Management Console auf. Sie können feststellen, welche Benutzer und Konten angerufen wurden AWS, von welcher Quell-IP-Adresse aus die Anrufe getätigt wurden und wann die Anrufe erfolgten. CloudTrail übermittelt Protokolldateien aus allen AWS Regionen an Ihren S3-Bucket , wenn MULTI_REG ION_CLOUD _TRAIL_ENABLED aktiviert ist. Außerdem wird beim AWS Start einer neuen Region derselbe Trail in der neuen Region erstellt. CloudTrail Dadurch erhalten Sie automatis ch Protokolldateien mit API-Aktivitäten für die neue Region.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AU-10	Nichtabstreitbarkeit	opensearch-logs-to-cloudwatch	Stellen Sie sicher, dass für Amazon OpenSearch Service-Domains Fehlerprotokolle aktiviert und zur Aufbewahrung und Beantwortung an Amazon CloudWatch Logs gestreamt werden. OpenSearch Service-Fehlerprotokolle können bei Sicherheits- und Zugriffsprüfungen helfen und bei der Diagnose von Verfügbarkeitsproblemen helfen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AU-10	Nichtabstreitbarkeit	rds-logging-enabled	Um die Protokollierung und Überwachung in Ihrer Umgebung zu erleichtern, stellen Sie sicher, dass die Amazon Relational Database Service (Amazon RDS)-Protokollierung aktiviert ist. Mit der Amazon-RDS-Protokollierung können Sie Ereignisse wie Verbindungen, Verbindungsabbrüche, Abfragen oder abgefragte Tabellen erfassen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AU-10	Nichtabstreitbarkeit	wafv2-logging-enabled	Um die Protokollierung und Überwachung in Ihrer Umgebung zu erleichtern, aktivieren Sie die AWS WAF (V2) -Protokollierung im regionalen und globalen Internet ACLs. AWS Die WAF-Protokollierung bietet detaillierte Informationen über den Datenverkehr, der von Ihrer Web-ACL analysiert wird. In den Protokollen werden die Uhrzeit aufgezeichnet, zu der die AWS WAF die Anfrage von Ihrer AWS Ressource erhalten hat, Informationen über die Anfrage und eine Aktion für die Regel, der jede Anfrage entsprach.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AU-10	Nichtabstreitbarkeit	api-gw-execution-logging-aktiviert	Die API-Gateway-Protokollierung zeigt detaillierte Ansichten der Benutzer, die auf die API zugegriffen haben, und wie diese Benutzer auf die API zugegriffen haben. Diese Einblicke ermöglichen die Transparenz von Benutzeraktivitäten.
AU-10	Nichtabstreitbarkeit	cloud-trail-cloud-watch-logs-aktiviert	Verwenden Sie Amazon CloudWatch , um Protokollereignisaktivitäten zentral zu sammeln und zu verwalten. Die Aufnahme von AWS CloudTrail Daten liefert Einzelheiten zu den API-Aufrufaktivitäten in Ihrem AWS-Konto.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AU-10	Nichtabstreitbarkeit	cloudtrail-enabled	AWS CloudTrail kann bei der Nichtabstreitbarkeit helfen, indem Aktionen und API-Aufrufe der AWS Management Console aufgezeichnet werden. Sie können die Benutzer und die Benutzer AWS-Konten , die einen AWS Dienst aufgerufen haben, die Quell-IP-Adresse, über die die Aufrufe generiert wurden, und den Zeitpunkt der Anrufe identifizieren. Einzelheiten zu den erfassten Daten finden Sie in den AWS CloudTrail Datensatzinhalten.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AU-10	Nichtabstreitbarkeit	cloudtrail-s3-data events-enabled	Die Erfassung von Simple Storage Service (Amazon S3)-Datenereignissen unterstützt die Erkennung von ungewöhnlichen Aktivitäten. Zu den Details gehören AWS-Konto Informationen über den Zugriff auf einen Amazon S3 S3-Bucket, die IP-Adresse und die Uhrzeit des Ereignisses.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AU-10	Nichtabstreitbarkeit	elb-logging-enabled	Die Elastic-Load-Balancing-Aktivität ist ein zentraler Kommunikationspunkt innerhalb einer Umgebung. Stellen Sie sicher, dass die ELB-Protokollierung aktiviert ist. Die gesammelten Daten enthalten detaillierte Informationen zu Anfragen, die an den ELB gesendet wurden. Jedes Protokoll enthält Informationen wie die Zeit, zu der die Anforderung einging, die Client-IP-Adresse, Latenzen, Anforderungspfade und Serverantworten.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AU-10	Nichtabstreitbarkeit	redshift-cluster-configuration-check	Um Daten im Ruhezustand zu schützen, muss die Verschlüsselung für Ihre Amazon-Redshift-Cluster aktiviert sein. Sie müssen auch sicherstellen, dass die erforderlichen Konfigurationen auf Amazon-Redshift-Clustern bereitgestellt werden. Die Prüfungsprotokollierung muss aktiviert sein, um Informationen zu Verbindungen und Benutzeraktivitäten in der Datenbank bereitzustellen. Diese Regel erfordert, dass ein Wert für clusterDbEncrypted (Config Default: TRUE) und LoggingEnabled (Config Default: TRUE) gesetzt ist. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AU-10	Nichtabstreitbarkeit	s3- bucket-logging-enabled	Die Amazon Simple Storage Service (Amazon S3)-Serverzugriffs protokollierung bietet eine Methode zur Überwachu ng des Netzwerks im Hinblick auf potenzielle Cybersich erheitsereignisse. Die Ereignisse werden überwacht, indem detaillierte Aufzeichn ungen über die Anfragen erfasst werden, die an einen Amazon-S3-Bucket gestellt wurden. Jeder Zugriffsprotokolle intrag enthält Details zu einer einzelnen Zugriffsanfrage. Zu den Details gehören Anforderer, Bucket-Name, Anforderu ngszeit, Anforderu ngsaktion, Antwortst atus und Fehlercode, falls relevant.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AU-12	Generierung von Prüfungsunterlagen	elasticsearch-logs-to-cloudwatch	Stellen Sie sicher, dass für Amazon OpenSearch Service-Domains Fehlerprotokolle aktiviert und zur Aufbewahrung und Beantwortung an Amazon CloudWatch Logs gestreamt werden. Domain-Fehlerprotokolle sind bei Sicherheits- und Zugriffsprüfungen sowie bei der Diagnose von Verfügbarkeitsproblemen nützlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AU-12	Generierung von Prüfungsunterlagen	multi-region-cloudtrail-enabled	AWS CloudTrail zeichnet Aktionen und API-Aufrufe der AWS Management Console auf. Sie können feststellen, welche Benutzer und Konten angerufen wurden AWS, von welcher Quell-IP-Adresse aus die Anrufe getätigt wurden und wann die Anrufe erfolgten. CloudTrail übermittelt Protokolldateien aus allen AWS Regionen an Ihren S3-Bucket , wenn MULTI_REG ION_CLOUD _TRAIL_ENABLED aktiviert ist. Außerdem wird beim AWS Start einer neuen Region derselbe Trail in der neuen Region erstellt. CloudTrail Dadurch erhalten Sie automatis ch Protokolldateien mit API-Aktivitäten für die neue Region.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AU-12	Generierung von Prüfungsunterlagen	opensearch-logs-to-cloudwatch	Stellen Sie sicher, dass für Amazon OpenSearch Service-Domains Fehlerprotokolle aktiviert und zur Aufbewahrung und Beantwortung an Amazon CloudWatch Logs gestreamt werden. OpenSearch Service-Fehlerprotokolle können bei Sicherheits- und Zugriffsprüfungen helfen und bei der Diagnose von Verfügbarkeitsproblemen helfen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AU-12	Generierung von Prüfungsunterlagen	wafv2-logging-enabled	Um die Protokollierung und Überwachung in Ihrer Umgebung zu erleichtern, aktivieren Sie die AWS WAF (V2) -Protokollierung im regionalen und globalen Internet ACLs. AWS Die WAF-Protokollierung bietet detaillierte Informationen über den Datenverkehr, der von Ihrer Web-ACL analysiert wird. In den Protokollen werden die Uhrzeit aufgezeichnet, zu der die AWS WAF die Anfrage von Ihrer AWS Ressource erhalten hat, Informationen über die Anfrage und eine Aktion für die Regel, der jede Anfrage entsprach.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AU-12	Generierung von Prüfungsunterlagen	api-gw-execution-logging-aktiviert	Die API-Gateway-Protokollierung zeigt detaillierte Ansichten der Benutzer, die auf die API zugegriffen haben, und wie diese Benutzer auf die API zugegriffen haben. Diese Einblicke ermöglichen die Transparenz von Benutzeraktivitäten.
AU-12	Generierung von Prüfungsunterlagen	cloud-trail-cloud-watch-logs-aktiviert	Verwenden Sie Amazon CloudWatch , um Protokoll ereignisaktivitäten zentral zu sammeln und zu verwalten. Die Aufnahme von AWS CloudTrail Daten liefert Einzelheiten zu den API-Aufrufaktivitäten in Ihrem AWS-Konto.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AU-12	Generierung von Prüfungsunterlagen	cloudtrail-enabled	AWS CloudTrail kann bei der Nichtabstreitbarkeit helfen, indem Aktionen und API-Aufrufe der AWS Management Console aufgezeichnet werden. Sie können die Benutzer und die Benutzer AWS-Konten , die einen AWS Dienst aufgerufen haben, die Quell-IP-Adresse, über die die Aufrufe generiert wurden, und den Zeitpunkt der Anrufe identifizieren. Einzelheiten zu den erfassten Daten finden Sie in den AWS CloudTrail Datensatzinhalten.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AU-12	Generierung von Prüfungsunterlagen	cloudtrail-s3-data events-enabled	Die Erfassung von Simple Storage Service (Amazon S3)-Datenereignissen unterstützt die Erkennung von ungewöhnlichen Aktivitäten. Zu den Details gehören AWS-Konto Informationen über den Zugriff auf einen Amazon S3 S3-Bucket, die IP-Adresse und die Uhrzeit des Ereignisses.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AU-12	Generierung von Prüfungsunterlagen	elb-logging-enabled	Die Elastic-Load-Balancing-Aktivität ist ein zentraler Kommunikationspunkt innerhalb einer Umgebung. Stellen Sie sicher, dass die ELB-Protokollierung aktiviert ist. Die gesammelten Daten enthalten detaillierte Informationen zu Anfragen, die an den ELB gesendet wurden. Jedes Protokoll enthält Informationen wie die Zeit, zu der die Anforderung einging, die Client-IP-Adresse, Latenzen, Anforderungspfade und Serverantworten.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AU-12	Generierung von Prüfungsunterlagen	rds-logging-enabled	Um die Protokollierung und Überwachung in Ihrer Umgebung zu erleichtern, stellen Sie sicher, dass die Amazon Relational Database Service (Amazon RDS)-Protokollierung aktiviert ist. Mit der Amazon-RDS-Protokollierung können Sie Ereignisse wie Verbindungen, Verbindungsabbrüche, Abfragen oder abgefragte Tabellen erfassen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AU-12	Generierung von Prüfungsunterlagen	redshift-cluster-configuration-check	Um Daten im Ruhezustand zu schützen, muss die Verschlüsselung für Ihre Amazon-Redshift-Cluster aktiviert sein. Sie müssen auch sicherstellen, dass die erforderlichen Konfigurationen auf Amazon-Redshift-Clustern bereitgestellt werden. Die Prüfungsprotokollierung muss aktiviert sein, um Informationen zu Verbindungen und Benutzeraktivitäten in der Datenbank bereitzustellen. Diese Regel erfordert, dass ein Wert für clusterDbEncrypted (Config Default: TRUE) und LoggingEnabled (Config Default: TRUE) gesetzt ist. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AU-12	Generierung von Prüfungsunterlagen	s3- bucket-logging-enabled	Die Amazon Simple Storage Service (Amazon S3)-Serverzugriffs protokollierung bietet eine Methode zur Überwachu ng des Netzwerks im Hinblick auf potenzielle Cybersich erheitsereignisse. Die Ereignisse werden überwacht, indem detaillierte Aufzeichn ungen über die Anfragen erfasst werden, die an einen Amazon-S3-Bucket gestellt wurden. Jeder Zugriffsprotokolle intrag enthält Details zu einer einzelnen Zugriffsanfrage. Zu den Details gehören Anforderer, Bucket-Name, Anforderu ngszeit, Anforderu ngsaktion, Antwortst atus und Fehlercode, falls relevant.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AU-12	Generierung von Prüfungsunterlagen	vpc-flow-logs-enabled	VPC-Flow-Protokolle erfassen detaillierte Informationsdatensätze über den IP-Datenverkehr, der zu und von Netzwerkschnittstellen in Ihrer Amazon Virtual Private Cloud (Amazon VPC) fließt. Standardmäßig enthalten Flow-Protokolldatensätze Werte für die verschiedenen Komponenten des IP-Flows, einschließlich Quelle, Ziel und Protokoll.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
AU-14(1)	Sitzungsprüfung | Systemstart	cloudtrail-enabled	AWS CloudTrai l kann durch die Aufzeichnung von Aktionen und API-Aufrufen in der AWS Management Console bei der Nichtabst reitbarkeit helfen. Sie können die Benutzer und die Benutzer AWS-Konten , die einen AWS Dienst aufgerufen haben, die Quell-IP-Adresse, über die die Aufrufe generiert wurden, und den Zeitpunkt der Anrufe identifiz ieren. Einzelheiten zu den erfassten Daten finden Sie in den AWS CloudTrail Datensatzinhalten.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CA-7	Kontinuierliche Überwachung	elasticsearch-logs-to-cloudwatch	Stellen Sie sicher, dass für Amazon OpenSearch Service-Domains Fehlerprotokolle aktiviert und zur Aufbewahrung und Beantwortung an Amazon CloudWatch Logs gestreamt werden. Domain-Fehlerprotokolle sind bei Sicherheits- und Zugriffsprüfungen sowie bei der Diagnose von Verfügbarkeitsproblemen nützlich.
CA-7	Kontinuierliche Überwachung	lambda-dlq-check	Aktivieren Sie diese Regel, um das entsprechende Personal über Amazon Simple Queue Service (Amazon SQS) oder Amazon Simple Notification Service (Amazon SNS) zu benachrichtigen, wenn eine Funktion ausgefallen ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CA-7	Kontinuierliche Überwachung	multi-region-cloudtrail-enabled	AWS CloudTrail zeichnet Aktionen und API-Aufrufe der AWS Management Console auf. Sie können feststellen, welche Benutzer und Konten angerufen wurden AWS, von welcher Quell-IP-Adresse aus die Anrufe getätigt wurden und wann die Anrufe erfolgten. CloudTrail übermittelt Protokolldateien aus allen AWS Regionen an Ihren S3-Bucket , wenn MULTI_REG ION_CLOUD _TRAIL_ENABLED aktiviert ist. Außerdem wird beim AWS Start einer neuen Region derselbe Trail in der neuen Region erstellt. CloudTrail Dadurch erhalten Sie automatis ch Protokolldateien mit API-Aktivitäten für die neue Region.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CA-7	Kontinuierliche Überwachung	opensearch-logs-to-cloudwatch	Stellen Sie sicher, dass für Amazon OpenSearch Service-Domains Fehlerprotokolle aktiviert und zur Aufbewahrung und Beantwortung an Amazon CloudWatch Logs gestreamt werden. OpenSearch Service-Fehlerprotokolle können bei Sicherheits- und Zugriffsprüfungen helfen und bei der Diagnose von Verfügbarkeitsproblemen helfen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CA-7	Kontinuierliche Überwachung	rds-enhanced-monitoring-enabled	Aktivieren Sie Amazon Relational Database Service (Amazon RDS), um die Verfügbarkeit von Amazon RDS zu überwachen. Dies bietet einen detaillierten Einblick in den Zustand Ihrer Amazon-RDS-Datenbank-Instances. Wenn der Amazon-RDS-Speicher mehr als ein zugrunde liegendes physisches Gerät verwendet, erfasst Enhanced Monitoring die Daten für jedes Gerät. Wenn die Amazon-RDS-Datenbank-Instance in einer Multi-AZ-Bereitstellung ausgeführt wird, werden außerdem die Daten für jedes Gerät auf dem sekundären Host sowie die Metriken des sekundären Hosts erfasst.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CA-7	Kontinuierliche Überwachung	rds-logging-enabled	Um die Protokollierung und Überwachung in Ihrer Umgebung zu erleichtern, stellen Sie sicher, dass die Amazon Relational Database Service (Amazon RDS)-Protokollierung aktiviert ist. Mit der Amazon-RDS-Protokollierung können Sie Ereignisse wie Verbindungen, Verbindungsabbrüche, Abfragen oder abgefragte Tabellen erfassen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CA-7	Kontinuierliche Überwachung	s-3 event-notification s-enabled	Amazon-S3-Ereignis benachrichtigungen können das zuständig e Personal über versehentliche oder vorsätzliche Änderungen an Ihren Bucket-Ob jekten informieren. Zu den Warnen gehören beispiels weise: Erstellung eines neuen Objekts, Entfernung eines Objekts, Wiederher stellung eines Objekts, verloren gegangene und replizierte Objekte.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CA-7	Kontinuierliche Überwachung	securityhub-enabled	AWS Security Hub hilft bei der Überwachung von unbefugtem Personal, Verbindungen, Geräten und Software. AWS Security Hub aggregiert, organisiert und priorisiert die Sicherheitswarnungen oder Ergebnisse mehrerer Dienste. AWS Einige dieser Dienste sind Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer und AWS Firewall Manager sowie AWS Partnerlösungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CA-7	Kontinuierliche Überwachung	wafv2-logging-enabled	Um Ihnen bei der Protokollierung und Überwachung in Ihrer Umgebung zu helfen, aktivieren Sie die AWS WAF (V2) -Protokollierung im regionalen und globalen Web. ACLs AWS Die WAF-Protokollierung bietet detaillierte Informationen über den Datenverkehr, der von Ihrer Web-ACL analysiert wird. In den Protokollen werden die Uhrzeit aufgezeichnet, zu der die AWS WAF die Anfrage von Ihrer AWS Ressource erhalten hat, Informationen über die Anfrage und eine Aktion für die Regel, der jede Anfrage entsprach.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CA-7	Kontinuierliche Überwachung	api-gw-execution-logging-aktiviert	Die API-Gateway-Protokollierung zeigt detaillierte Ansichten der Benutzer, die auf die API zugegriff en haben, und wie diese Benutzer auf die API zugegriff en haben. Diese Einblicke ermöglichen die Transparenz von Benutzeraktivitäten.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CA-7	Kontinuierliche Überwachung	autoscaling-group-elb-healthcheck-erforderlich	Die Elastic Load Balancer (ELB) - Zustandsprüfungen für Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling Scaling-Gruppen unterstützen die Aufrechterhaltung einer angemessenen Kapazität und Verfügbarkeit. Der Load Balancer sendet regelmäßig Pings, versucht Verbindungen herzustellen oder sendet Anfragen, um den Zustand der EC2 Amazon-Instances in einer Gruppe mit auto-scaling zu testen. Wenn eine Instance nicht zurückmeldet, wird der Traffic an eine neue EC2 Amazon-Instance gesendet.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CA-7	Kontinuierliche Überwachung	beanstalk-enhanced-health-reporting-aktiviert	AWS Die verbesserte Zustandsberichterstattung von Elastic Beanstalk ermöglicht eine schnellere Reaktion auf Veränderungen im Zustand der zugrunde liegenden Infrastruktur. Diese Änderungen könnten zu einer mangelnden Verfügbarkeit der Anwendung führen. Die erweiterten Zustandsberichte von Elastic Beanstalk bieten eine Statusbeschreibung, um den Schweregrad der identifizierten Probleme einzuschätzen und mögliche Ursachen zu identifizieren, die untersucht werden müssen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CA-7	Kontinuierliche Überwachung	cloud-trail-cloud-watch-Logs aktiviert	Verwenden Sie Amazon CloudWatch , um Protokoll ereignisaktivitäten zentral zu sammeln und zu verwalten. Die Aufnahme von AWS CloudTrail Daten liefert Einzelheiten zu den API-Aufrufaktivitäten in Ihrem AWS-Konto.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CA-7	Kontinuierliche Überwachung	cloudtrail-enabled	AWS CloudTrail kann bei der Nichtabst reitbarkeit helfen, indem Aktionen und API-Aufrufe der AWS Management Console aufgezeic hnet werden. Sie können die Benutzer und die Benutzer AWS-Konten , die einen AWS Dienst aufgerufen haben, die Quell-IP-Adresse, über die die Aufrufe generiert wurden, und den Zeitpunkt der Anrufe identifiz ieren. Einzelheiten zu den erfassten Daten finden Sie in den AWS CloudTrail Datensatzinhalten.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CA-7	Kontinuierliche Überwachung	cloudtrail-s3-data events-enabled	Die Erfassung von Simple Storage Service (Amazon S3)-Datenereignissen unterstützt die Erkennung von ungewöhnlichen Aktivitäten. Zu den Details gehören AWS-Konto Informationen über den Zugriff auf einen Amazon S3 S3-Bucket, die IP-Adresse und die Uhrzeit des Ereignisses.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CA-7	Kontinuierliche Überwachung	cloudwatch-alarm-action-check	Amazon CloudWatch alarmiert, wenn eine Metrik den Schwellenwert für eine bestimmte Anzahl von Bewertungszeiträumen überschreitet. Der Alarm führt eine oder mehrere Aktionen durch, die vom Wert der Metrik oder des Ausdrucks im Vergleich zu einem Schwellenwert in einer Reihe von Zeiträumen abhängt. Diese Regel erfordert einen Wert für alarmActionRequired (Config Default: True), insufficientDataAction Required (Config Default: True), okActionRequired (Config Default: False). Der tatsächliche Wert muss die Alarmaktionen für Ihre Umgebung widerspiegeln.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CA-7	Kontinuierliche Überwachung	dynamodb-throughput-limit-check	Aktivieren Sie diese Regel, um sicherzustellen, dass die bereitgestellte Durchsatzkapazität in Ihren Amazon-DynamoDB-Tabellen überprüft wird. Dies ist der Umfang der Lese- und Schreibaktivitäten, der von den jeweiligen Tabellen unterstützt werden kann. DynamoDB verwendet diese Informationen für das Reservieren ausreichender Systemressourcen, um Ihren Durchsatz anforderungen gerecht zu werden. Diese Regel generiert eine Warnung, wenn sich der Durchsatz dem Höchstlimit für ein Kundenkonto nähert. Mit dieser Regel können Sie optional die Parameter RCUThreshold Kontoprozentsatz

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			(Konfigurationsstandard: 80) und WCUThreshold Kontoprozentsatz (Konfigurationsstandard: 80) festlegen. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CA-7	Kontinuierliche Überwachung	elb-logging-enabled	Die Elastic-Load-Balancing-Aktivität ist ein zentraler Kommunikationspunkt innerhalb einer Umgebung. Stellen Sie sicher, dass die ELB-Protokollierung aktiviert ist. Die gesammelten Daten enthalten detaillierte Informationen zu Anfragen, die an den ELB gesendet wurden. Jedes Protokoll enthält Informationen wie die Zeit, zu der die Anforderung einging, die Client-IP-Adresse, Latenzen, Anforderungspfade und Serverantworten.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CA-7	Kontinuierliche Überwachung	guardduty-enabled-centralized	Amazon GuardDuty kann mithilfe von Threat Intellige nce Feeds helfen, potenzielle Cybersich erheitsereignisse zu überwachen und zu erkennen. Dazu gehören Listen mit bösartigen IPs und maschinel len Lernmethoden zur Identifizierung unerwarteter, nicht autorisierter und bösartiger Aktivitäten in Ihrer AWS Cloud-Umgebung.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CA-7	Kontinuierliche Überwachung	redshift-cluster-configuration-check	Um Daten im Ruhezustand zu schützen, muss die Verschlüsselung für Ihre Amazon-Redshift-Cluster aktiviert sein. Sie müssen auch sicherstellen, dass die erforderlichen Konfigurationen auf Amazon-Redshift-Clustern bereitgestellt werden. Die Prüfungsprotokollierung muss aktiviert sein, um Informationen zu Verbindungen und Benutzeraktivitäten in der Datenbank bereitzustellen. Diese Regel erfordert, dass ein Wert für clusterDbEncrypted (Config Default: TRUE) und LoggingEnabled (Config Default: TRUE) gesetzt ist. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CA-7	Kontinuierliche Überwachung	s3- bucket-logging-enabled	Die Amazon Simple Storage Service (Amazon S3)-Serverzugriffs protokollierung bietet eine Methode zur Überwachu ng des Netzwerks im Hinblick auf potenzielle Cybersich erheitsereignisse. Die Ereignisse werden überwacht, indem detaillierte Aufzeichn ungen über die Anfragen erfasst werden, die an einen Amazon-S3-Bucket gestellt wurden. Jeder Zugriffsprotokolle intrag enthält Details zu einer einzelnen Zugriffsanfrage. Zu den Details gehören Anforderer, Bucket-Name, Anforderu ngszeit, Anforderu ngsaktion, Antwortst atus und Fehlercode, falls relevant.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CA-7	Kontinuierliche Überwachung	vpc-flow-logs-enabled	VPC-Flow-Protokolle erfassen detaillierte Informationsdatensätze über den IP-Datenverkehr, der zu und von Netzwerkschnittstellen in Ihrer Amazon Virtual Private Cloud (Amazon VPC) fließt. Standardmäßig enthalten Flow-Protokolldatensätze Werte für die verschiedenen Komponenten des IP-Flows, einschließlich Quelle, Ziel und Protokoll.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CA-9(1)	Interne Systemverbindungen | Konformitätsprüfungen	account-part-of-organizations	Durch die zentrale Verwaltung AWS-Konten innerhalb von AWS Organizations wird sichergestellt, dass die Konten den Vorschriften entsprechen. Eine fehlende zentrale Kontoverwaltung kann zu inkonsistenten Kontokonfigurationen führen, wodurch Ressourcen und sensible Daten offengelegt werden können.
CA-9(1)	Interne Systemverbindungen | Konformitätsprüfungen	codebuild-project-artifact-encryption	Um sensible Daten im Speicher zu schützen, sollten Sie sicherstellen, dass die Verschlüsselung für Ihre AWS CodeBuild Artefakte aktiviert ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CA-9(1)	Interne Systemverbindungen | Konformitätsprüfungen	dynamodb-table-encrypted-kms	Stellen Sie sicher, dass die Verschlüsselung für Ihre Amazon-DynamoDB-Tabellen aktiviert ist. Um eventuell vorhandene sensible Daten im Ruhezustand in diesen Tabellen zu schützen, müssen Sie die Verschlüsselung von Daten im Ruhezustand aktivieren. Standardmäßig werden DynamoDB-Tabellen mit einem AWS eigenen Kundenhauptschlüssel (CMK) verschlüselt.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CA-9(1)	Interne Systemverbindungen | Konformitätsprüfungen	ec2- ebs-encryption-by-default	Zum Schutz von Daten im Ruhezustand müssen Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon Elastic Block Store (Amazon EBS)-Volumes aktiviert ist. Da sensible Daten auch im Ruhezustand vorhanden sein können, sollten Sie die Verschlüsselung im Ruhezustand aktivieren, um diese Daten zu schützen.
CA-9(1)	Interne Systemverbindungen | Konformitätsprüfungen	kinesis-stream-encrypted	Aktivieren Sie die Verschlüsselung für Ihre Amazon-Kinesis-Streams, um eventuell vorhandene sensible Daten sowie Daten im Ruhezustand zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CA-9(1)	Interne Systemverbindungen | Konformitätsprüfungen	rds-instance-default-admin-überprüfen	Da Standardbenutzernamen allgemein bekannt sind, kann eine Änderung der Standardbenutzernamen dazu beitragen, die Angriffsfläche für Ihre Datenbank-Instance(s) in Amazon Relational Database Service (Amazon RDS) zu reduzieren.
CA-9(1)	Interne Systemverbindungen | Konformitätsprüfungen	rds-snapshot-encrypted	Stellen Sie sicher, dass die Verschlüsselung für Ihre Amazon Relational Database Service (Amazon RDS)-Snapshots aktiviert ist. Da sensible Daten auch im Ruhezustand vorhanden sein können, sollten Sie die Verschlüsselung im Ruhezustand aktivieren, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CA-9(1)	Interne Systemverbindungen | Konformitätsprüfungen	s3- default-encryption-kms	Stellen Sie sicher, dass die Verschlüsselung für Ihre Amazon Simple Storage Service (Amazon S3)-Buckets aktiviert ist. Um eventuell vorhandene sensible Daten im Ruhezustand in einem Amazon-S3-Bucket zu schützen, muss die Verschlüsselung aktiviert sein.
CA-9(1)	Interne Systemverbindungen | Konformitätsprüfungen	sagemaker-notebook-instance-kms-key-konfiguriert	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass die Verschlüsselung mit dem AWS Key Management Service (AWS KMS) für Ihr Notebook aktiviert ist. SageMaker Da vertrauliche Daten im SageMaker Notebook gespeichert werden können, sollten Sie die Verschlüsselung im Ruhezustand aktivieren, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CA-9(1)	Interne Systemverbindungen | Konformitätsprüfungen	sns-encrypted-kms	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass Ihre Amazon Simple Notification Service (Amazon SNS) -Themen mit dem AWS Key Management Service (AWS KMS) verschlüsselt werden müssen. Um eventuell vorhandene sensible Daten im Ruhezustand in veröffentlichten Nachrichten zu schützen, muss die Verschlüsselung von Daten im Ruhezustand aktiviert sein.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CA-9(1)	Interne Systemverbindungen | Konformitätsprüfungen	api-gw-cache-enabled-und verschlüsselt	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass die Verschlüsselung für den Cache Ihrer API-Gateway-Stufe aktiviert ist. Da für die API-Methode sensible Daten erfasst werden können, sollten Sie die Verschlüsselung von Daten im Ruhezustand aktivieren, um diese Daten zu schützen.
CA-9(1)	Interne Systemverbindungen | Konformitätsprüfungen	cloud-trail-encryption-enabled	Da sensible Daten vorhanden sein können und um Daten im Ruhezustand zu schützen, sollten Sie sicherstellen, dass die Verschlüsselung für Ihre AWS CloudTrail Trails aktiviert ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CA-9(1)	Interne Systemverbindungen | Konformitätsprüfungen	ec2-managed-instance-managed-by-systems	Eine Bestandsaufnahme der Softwareplattformen und Anwendungen innerhalb des Unternehmens ist möglich, indem Amazon Elastic Compute Cloud (Amazon EC2) - Instances mit AWS Systems Manager verwaltet werden. Verwenden Sie AWS Systems Manager, um detaillierte Systemkonfigurationen, Betriebssystem-Patch-Levels, Namen und Typ der Dienste, Softwareinstallationen, Anwendungsname, Herausgeber und Version sowie andere Details zu Ihrer Umgebung bereitzustellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CA-9(1)	Interne Systemverbindungen | Konformitätsprüfungen	ec2-check managedinstance-association-compliance-status	Verwenden Sie AWS Systems Manager Associations, um bei der Inventarisierung von Softwareplattformen und Anwendungen innerhalb eines Unternehmens zu helfen. AWS Systems Manager weist Ihren verwalteten Instanzen einen Konfigurationsstatus zu und ermöglicht es Ihnen, Basiswerte für Betriebssystem-Patch-Levels, Softwareinstallationen, Anwendungskonfigurationen und andere Details zu Ihrer Umgebung festzulegen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CA-9(1)	Interne Systemverbindungen | Konformitätsprüfungen	ec2-stopped-instance	Aktivieren Sie diese Regel, um bei der Basiskonfiguration von Amazon Elastic Compute Cloud (Amazon EC2) - Instances zu helfen, indem Sie überprüfen, ob EC2 Amazon-Instances gemäß den Standards Ihrer Organisation für mehr als die zulässige Anzahl von Tagen gestoppt wurden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CA-9(1)	Interne Systemverbindungen | Konformitätsprüfungen	ec2- volume-inuse-check	Diese Regel stellt sicher, dass Amazon Elastic Block Store-Volumes, die an Amazon Elastic Compute Cloud (Amazon EC2) - Instances angehängt sind, zum Löschen markiert werden, wenn eine Instance beendet wird. Wenn ein Amazon-EBS-Volume nicht gelöscht wird, wenn die Instance, an die es angehängt ist, beendet wird, kann dies gegen das Konzept der geringsten Funktionalität verstoßen.
CA-9(1)	Interne Systemverbindungen | Konformitätsprüfungen	efs-encrypted-check	Aktivieren Sie die Verschlüsselung für Ihr Amazon Elastic File System (EFS), um eventuell vorhandene sensible Daten sowie Daten im Ruhezustand zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CA-9(1)	Interne Systemverbindungen | Konformitätsprüfungen	elasticsearch-encrypted-at-rest	Da sensible Daten vorhanden sein können und um Daten im Ruhezustand zu schützen, sollten Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon OpenSearch Service (OpenSearch Service) -Domains aktiviert ist.
CA-9(1)	Interne Systemverbindungen | Konformitätsprüfungen	elb-deletion-protection-enabled	Diese Regel sorgt dafür, dass der Löschschutz für Elastic Load Balancing aktiviert ist. Verwenden Sie diese Funktion, um zu verhindern, dass Ihr Load Balancer versehentlich oder böswillig gelöscht wird, was zum Verlust der Verfügbarkeit Ihrer Anwendungen führen kann.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CA-9(1)	Interne Systemverbindungen | Konformitätsprüfungen	encrypted-volumes	Aktivieren Sie die Verschlüsselung für Ihre Amazon-Elastic-Block-Store (Amazon-EBS)-Volumes, um eventuell vorhandene sensible Daten sowie Daten im Ruhezustand zu schützen.
CA-9(1)	Interne Systemverbindungen | Konformitätsprüfungen	opensearch-encrypted-at-rest	Da sensible Daten vorhanden sein können und um Daten im Ruhezustand zu schützen, sollten Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon OpenSearch Service-Domains aktiviert ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CA-9(1)	Interne Systemverbindungen | Konformitätsprüfungen	rds-storage-encrypted	Zum Schutz von Daten im Ruhezustand müssen Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon Relational Database Service (Amazon RDS)-Instances aktiviert ist. Um eventuell vorhandene sensible Daten im Ruhezustand in Amazon-RDS-Instances zu schützen, muss die Verschlüsselung von Daten im Ruhezustand aktiviert sein.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CA-9(1)	Interne Systemverbindungen | Konformitätsprüfungen	redshift-cluster-configuration-check	Um Daten im Ruhezustand zu schützen, muss die Verschlüsselung für Ihre Amazon-Redshift-Cluster aktiviert sein. Sie müssen auch sicherstellen, dass die erforderlichen Konfigurationen auf Amazon-Redshift-Clustern bereitgestellt werden. Die Prüfungsprotokollierung muss aktiviert sein, um Informationen zu Verbindungen und Benutzeraktivitäten in der Datenbank bereitzustellen. Diese Regel erfordert, dass ein Wert für clusterDbEncrypted (Config Default: TRUE) und LoggingEnabled (Config Default: TRUE) gesetzt ist. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CA-9(1)	Interne Systemverbindungen | Konformitätsprüfungen	redshift-cluster-kms-enabled	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass die Verschlüsselung mit AWS Key Management Service (AWS KMS) für Ihren Amazon Redshift Redshift-Cluster aktiviert ist. Um eventuell vorhandene sensible Daten im Ruhezustand in Redshift-Clustern zu schützen, muss die Verschlüsselung von Daten im Ruhezustand aktiviert sein.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CA-9(1)	Interne Systemverbindungen | Konformitätsprüfungen	redshift-cluster-maintenancesettings-check	Diese Regel stellt sicher, dass Amazon-Redshift-Cluster die bevorzugten Einstellungen für Ihre Organisation haben. Insbesondere sorgt sie dafür, dass Cluster bevorzugte Wartungsfenster und automatisierte Aufbewahrungsfristen für Snapshots für die Datenbank haben. Für diese Regel müssen Sie die allowVersionUpgrade festlegen. Der Standardwert ist „true“. Außerdem können Sie optional den Zeitraum preferredMaintenanceWindow (der Standardwert ist sa: 16:00 -sa: 16:30) und den automated SnapshotRetention Zeitraum (der Standardwert ist 1) festlegen. Die tatsächlichen Werte müssen den Richtlini

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			en Ihrer Organisation entsprechen.
CA-9(1)	Interne Systemverbindungen | Konformitätsprüfungen	redshift-default-admin-check	Da Standardbenutzernamen allgemein bekannt sind, kann eine Änderung der Standardbenutzernamen dazu beitragen, die Angriffsfläche für Ihre Amazon-Redshift-Cluster zu reduzieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CA-9(1)	Interne Systemverbindungen | Konformitätsprüfungen	restricted-common-ports	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass gemeinsame Ports für Amazon Elastic Compute Cloud (Amazon EC2) -Sicherheitsgruppen eingeschränkt sind. Wenn der Zugriff auf Ports nicht auf vertrauenswürdige Quellen beschränkt wird, kann dies zu Angriffen auf die Verfügbarkeit, Integrität und Vertraulichkeit von Systemen führen. Mit dieser Regel können Sie optional die Parameter blockedPort1–blockedPort5 festlegen (Standardkonfigurationen: 20, 21, 3389, 3306, 4333). Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CA-9(1)	Interne Systemverbindungen | Konformitätsprüfungen	bucket-server-side-encryptions3-fähig	Zum Schutz von Daten im Ruhezustand müssen Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon Simple Storage Service (Amazon S3)-Buckets aktiviert ist. Um eventuell vorhandene sensible Daten im Ruhezustand in Amazon-S3-Buckets zu schützen, muss die Verschlüsselung aktiviert sein.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CA-9(1)	Interne Systemverbindungen | Konformitätsprüfungen	sagemaker-endpoint-configuration-kms-key-konfiguriert	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass die Verschlüsselung mit dem AWS Key Management Service (AWS KMS) für Ihren Endpunkt aktiviert ist. SageMaker Da sensible Daten auf dem SageMaker Endgerät gespeichert werden können, sollten Sie die Verschlüsselung im Ruhezustand aktivieren, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CA-9(1)	Interne Systemverbindungen | Konformitätsprüfungen	secretsmanager-using-cmk	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass die Verschlüsselung mit dem AWS Key Management Service (AWS KMS) für AWS Secrets Manager aktiviert ist. Aktivieren Sie die Verschlüsselung von Daten im Ruhezustand, um eventuell vorhandene sensible Daten im Ruhezustand im Secrets Manager zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CM-2(2)	Basiskonfiguration | Automatisierungsunterstützung zur Förderung von Genauigkeit und Aktualität	ec2-manager instance-managed-by-systems	Eine Bestandsaufnahme der Softwareplattformen und Anwendungen innerhalb des Unternehmens ist möglich, indem Amazon Elastic Compute Cloud (Amazon EC2) - Instances mit AWS Systems Manager verwaltet werden. Verwenden Sie AWS Systems Manager, um detaillierte Systemkonfigurationen, Betriebssystem-Patch-Levels, Namen und Typ der Dienste, Softwareinstallationen, Anwendungsname, Herausgeber und Version sowie andere Details zu Ihrer Umgebung bereitzustellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CM-2(2)	Basiskonfiguration | Automatisierungsunterstützung zur Förderung von Genauigkeit und Aktualität	ec2-check managedinstance-association-compliance-status	Verwenden Sie AWS Systems Manager Associations, um bei der Inventarisierung von Softwareplattformen und Anwendungen innerhalb eines Unternehmens zu helfen. AWS Systems Manager weist Ihren verwalteten Instanzen einen Konfigurationsstatus zu und ermöglicht es Ihnen, Basiswerte für Betriebssystem-Patch-Levels, Softwareinstallationen, Anwendungskonfigurationen und andere Details zu Ihrer Umgebung festzulegen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CM-2(2)	Basiskonfiguration | Automatisierungsunterstützung zur Förderung von Genauigkeit und Aktualität	ec2-stopped-instance	Aktivieren Sie diese Regel, um bei der Basiskonfiguration von Amazon Elastic Compute Cloud (Amazon EC2) - Instances zu helfen, indem Sie überprüfen, ob EC2 Amazon-Instances gemäß den Standards Ihrer Organisation für mehr als die zulässige Anzahl von Tagen gestoppt wurden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CM-2(2)	Basiskonfiguration | Automatisierungsunterstützung zur Förderung von Genauigkeit und Aktualität	ec2- volume-inuse-check	Diese Regel stellt sicher, dass Amazon Elastic Block Store-Volumes, die an Amazon Elastic Compute Cloud (Amazon EC2) - Instances angehängt sind, zum Löschen markiert werden, wenn eine Instance beendet wird. Wenn ein Amazon-EBS-Volume nicht gelöscht wird, wenn die Instance, an die es angehängt ist, beendet wird, kann dies gegen das Konzept der geringsten Funktionalität verstoßen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CM-2(2)	Basiskonfiguration | Automatisierungsunterstützung zur Förderung von Genauigkeit und Aktualität	elb-deletion-protection-enabled	Diese Regel sorgt dafür, dass der Löschschutz für Elastic Load Balancing aktiviert ist. Verwenden Sie diese Funktion, um zu verhindern, dass Ihr Load Balancer versehentlich oder böswillig gelöscht wird, was zum Verlust der Verfügbarkeit Ihrer Anwendungen führen kann.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CM-2(2)	Basiskonfiguration | Automatisierungsunterstützung zur Förderung von Genauigkeit und Aktualität	restricted-common-ports	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass gemeinsame Ports für Amazon Elastic Compute Cloud (Amazon EC2) -Sicherheitsgruppen eingeschränkt sind. Wenn der Zugriff auf Ports nicht auf vertrauenswürdige Quellen beschränkt wird, kann dies zu Angriffen auf die Verfügbarkeit, Integrität und Vertraulichkeit von Systemen führen. Mit dieser Regel können Sie optional die Parameter blockedPort1–blockedPort5 festlegen (Standardkonfigurationen: 20, 21, 3389, 3306, 4333). Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CM-2	Basiskonfiguration	account-part-of-organizations	Durch die zentrale Verwaltung AWS-Konten innerhalb von AWS Organizations wird sichergestellt, dass die Konten den Vorschriften entsprechen. Eine fehlende zentrale Kontoverwaltung kann zu inkonsistenten Kontokonfigurationen führen, wodurch Ressourcen und sensible Daten offengelegt werden können.
CM-2	Basiskonfiguration	rds-instance-default-admin-überprüfen	Da Standardbenutzernamen allgemein bekannt sind, kann eine Änderung der Standardbenutzernamen dazu beitragen, die Angriffsfläche für Ihre Datenbank-Instance(s) in Amazon Relational Database Service (Amazon RDS) zu reduzieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CM-2	Basiskonfiguration	ec2- -Manager instance-managed-by-systems	Eine Bestandsaufnahme der Softwareplattformen und Anwendungen innerhalb des Unternehmens ist möglich, indem Amazon Elastic Compute Cloud (Amazon EC2) - Instances mit AWS Systems Manager verwaltet werden. Verwenden Sie AWS Systems Manager, um detaillierte Systemkonfigurationen, Betriebssystem-Patch-Levels, Namen und Typ der Dienste, Softwareinstallationen, Anwendungsname, Herausgeber und Version sowie andere Details zu Ihrer Umgebung bereitzustellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CM-2	Basiskonfiguration	ec2-check managedinstance-association-compliance-status	Verwenden Sie AWS Systems Manager Associations, um bei der Inventarisierung von Softwareplattformen und Anwendungen innerhalb eines Unternehmens zu helfen. AWS Systems Manager weist Ihren verwalteten Instanzen einen Konfigurationsstatus zu und ermöglicht es Ihnen, Basiswerte für Betriebssystem-Patch-Levels, Softwareinstallationen, Anwendungskonfigurationen und andere Details zu Ihrer Umgebung festzulegen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CM-2	Basiskonfiguration	ec2-stopped-instance	Aktivieren Sie diese Regel, um bei der Basiskonfiguration von Amazon Elastic Compute Cloud (Amazon EC2) - Instances zu helfen, indem Sie überprüfe n, ob EC2 Amazon-Instances gemäß den Standards Ihrer Organisation für mehr als die zulässige Anzahl von Tagen gestoppt wurden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CM-2	Basiskonfiguration	ec2- volume-inuse-check	Diese Regel stellt sicher, dass Amazon Elastic Block Store-Volumes, die an Amazon Elastic Compute Cloud (Amazon EC2) - Instances angehängt sind, zum Löschen markiert werden, wenn eine Instance beendet wird. Wenn ein Amazon-EB S-Volume nicht gelöscht wird, wenn die Instance, an die es angehängt ist, beendet wird, kann dies gegen das Konzept der geringsten Funktiona lität verstoßen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CM-2	Basiskonfiguration	elb-deletion-protection-enabled	Diese Regel sorgt dafür, dass der Löschschutz für Elastic Load Balancing aktiviert ist. Verwenden Sie diese Funktion, um zu verhindern, dass Ihr Load Balancer versehentlich oder böswillig gelöscht wird, was zum Verlust der Verfügbarkeit Ihrer Anwendungen führen kann.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CM-2	Basiskonfiguration	redshift-cluster-maintenancesettings-check	Diese Regel stellt sicher, dass Amazon-Redshift-Cluster die bevorzugten Einstellungen für Ihre Organisation haben. Insbesondere sorgt sie dafür, dass Cluster bevorzugte Wartungsfenster und automatisierte Aufbewahrungsfristen für Snapshots für die Datenbank haben. Für diese Regel müssen Sie die festlegen allowVersionUpgrade. Der Standardwert ist „true“. Außerdem können Sie optional den Zeitraum preferredMaintenanceWindow (der Standardwert ist sa: 16:00 -sa: 16:30) und den automated SnapshotRetention Zeitraum (der Standardwert ist 1) festlegen. Die tatsächlichen Werte müssen den Richtlini

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			en Ihrer Organisation entsprechen.
CM-2	Basiskonfiguration	redshift-default-admin-check	Da Standardbenutzernamen allgemein bekannt sind, kann eine Änderung der Standardbenutzernamen dazu beitragen, die Angriffsfläche für Ihre Amazon-Redshift-Cluster zu reduzieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CM-2	Basiskonfiguration	restricted-common-ports	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass gemeinsame Ports für Amazon Elastic Compute Cloud (Amazon EC2) -Sicherheitsgruppen eingeschränkt sind. Wenn der Zugriff auf Ports nicht auf vertrauenswürdige Quellen beschränkt wird, kann dies zu Angriffen auf die Verfügbarkeit, Integrität und Vertraulichkeit von Systemen führen. Mit dieser Regel können Sie optional die Parameter blockedPort1–blockedPort5 festlegen (Standardkonfigurationen: 20, 21, 3389, 3306, 4333). Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CM-3(6)	Kontrolle von Konfigurationsände rungen | Kryptografie-Management	codebuild-project-artifact-encryption	Um sensible Daten im Ruhezustand zu schützen, sollten Sie sicherstellen, dass die Verschlüsselung für Ihre AWS CodeBuild Artefakte aktiviert ist.
CM-3(6)	Kontrolle von Konfigurationsände rungen | Kryptografie-Management	dynamodb-table-encrypted-kms	Stellen Sie sicher, dass die Verschlüs selung für Ihre Amazon-DynamoDB-Tabellen aktiviert ist. Um eventuell vorhandene sensible Daten im Ruhezusta nd in diesen Tabellen zu schützen, müssen Sie die Verschlüs selung von Daten im Ruhezustand aktiviere n. Standardmäßig werden DynamoDB-Tabellen mit einem AWS eigenen Kundenhauptschlüss el (CMK) verschlüs selt.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CM-3(6)	Kontrolle von Konfigurationsände rungen | Kryptografie-Management	ec2- ebs-encryption-by-default	Zum Schutz von Daten im Ruhezusta nd müssen Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon Elastic Block Store (Amazon EBS)-Volu mes aktiviert ist. Da sensible Daten auch im Ruhezusta nd vorhanden sein können, sollten Sie die Verschlüsselung im Ruhezustand aktivieren, um diese Daten zu schützen.
CM-3(6)	Kontrolle von Konfigurationsände rungen | Kryptografie-Management	kinesis-stream-enc rypted	Aktivieren Sie die Verschlüsselung für Ihre Amazon-Kinesis-Streams, um eventuell vorhandene sensible Daten sowie Daten im Ruhezustand zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CM-3(6)	Kontrolle von Konfigurationsänderungen | Kryptografie-Management	rds-snapshot-encrypted	Stellen Sie sicher, dass die Verschlüsselung für Ihre Amazon Relational Database Service (Amazon RDS)-Snapshots aktiviert ist. Da sensible Daten auch im Ruhezustand vorhanden sein können, sollten Sie die Verschlüsselung im Ruhezustand aktivieren, um diese Daten zu schützen.
CM-3(6)	Kontrolle von Konfigurationsänderungen | Kryptografie-Management	s-3 default-encryption-kms	Stellen Sie sicher, dass die Verschlüsselung für Ihre Amazon Simple Storage Service (Amazon S3)-Buckets aktiviert ist. Um eventuell vorhandene sensible Daten im Ruhezustand in einem Amazon-S3-Bucket zu schützen, muss die Verschlüsselung aktiviert sein.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CM-3(6)	Kontrolle von Konfigurationsände rungen | Kryptografie-Management	sagemaker-notebook-instance-kms-key-konfiguriert	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass die Verschlüsselung mit dem AWS Key Management Service (AWS KMS) für Ihr Notebook aktiviert ist. SageMaker Da vertrauliche Daten im SageMaker Notebook gespeichert werden können, sollten Sie die Verschlüsselung im Ruhezustand aktivieren, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CM-3(6)	Kontrolle von Konfigurationsände rungen | Kryptografie-Management	sns-encrypted-kms	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass Ihre Amazon Simple Notification Service (Amazon SNS) -Themen mit dem AWS Key Management Service (AWS KMS) verschlüsselt werden müssen. Um eventuell vorhandene sensible Daten im Ruhezusta nd in veröffentlichten Nachrichten zu schützen, muss die Verschlüsselung von Daten im Ruhezusta nd aktiviert sein.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CM-3(6)	Kontrolle von Konfigurationsänderungen | Kryptografie-Management	api-gw-cache-enabled-und verschlüsselt	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass die Verschlüsselung für den Cache Ihrer API-Gateway-Stufe aktiviert ist. Da für die API-Methode sensible Daten erfasst werden können, sollten Sie die Verschlüsselung von Daten im Ruhezustand aktivieren, um diese Daten zu schützen.
CM-3(6)	Kontrolle von Konfigurationsänderungen | Kryptografie-Management	cloud-trail-encryption-enabled	Da sensible Daten vorhanden sein können und um Daten im Ruhezustand zu schützen, sollten Sie sicherstellen, dass die Verschlüsselung für Ihre AWS CloudTrail Trails aktiviert ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CM-3(6)	Kontrolle von Konfigurationsände rungen | Kryptografie-Management	efs-encrypted-check	Aktivieren Sie die Verschlüsselung für Ihr Amazon Elastic File System (EFS), um eventuell vorhandene sensible Daten sowie Daten im Ruhezustand zu schützen.
CM-3(6)	Kontrolle von Konfigurationsände rungen | Kryptografie-Management	elasticsearch-encr ypted-at-rest	Da sensible Daten vorhanden sein können und um Daten im Ruhezustand zu schützen, sollten Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon OpenSearch Service (OpenSearch Service) -Domains aktiviert ist.
CM-3(6)	Kontrolle von Konfigurationsände rungen | Kryptografie-Management	encrypted-volumes	Aktivieren Sie die Verschlüsselung für Ihre Amazon-Elastic-Block-Store (Amazon-EBS)-Volumes, um eventuell vorhandene sensible Daten sowie Daten im Ruhezusta nd zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CM-3(6)	Kontrolle von Konfigurationsänderungen | Kryptografie-Management	opensearch-encrypted-at-rest	Da sensible Daten vorhanden sein können und um Daten im Ruhezustand zu schützen, sollten Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon OpenSearch Service-Domains aktiviert ist.
CM-3(6)	Kontrolle von Konfigurationsänderungen | Kryptografie-Management	rds-storage-encrypted	Zum Schutz von Daten im Ruhezustand müssen Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon Relational Database Service (Amazon RDS)-Instances aktiviert ist. Um eventuell vorhandene sensible Daten im Ruhezustand in Amazon-RDS-Instances zu schützen, muss die Verschlüsselung von Daten im Ruhezustand aktiviert sein.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CM-3(6)	Kontrolle von Konfigurationsänderungen | Kryptografie-Management	redshift-cluster-configuration-check	Um Daten im Ruhezustand zu schützen, muss die Verschlüsselung für Ihre Amazon-Redshift-Cluster aktiviert sein. Sie müssen auch sicherstellen, dass die erforderlichen Konfigurationen auf Amazon-Redshift-Clustern bereitgestellt werden. Die Prüfungsprotokollierung muss aktiviert sein, um Informationen zu Verbindungen und Benutzeraktivitäten in der Datenbank bereitzustellen. Diese Regel erfordert, dass ein Wert für clusterDbEncrypted (Config Default: TRUE) und LoggingEnabled (Config Default: TRUE) gesetzt ist. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CM-3(6)	Kontrolle von Konfigurationsände rungen | Kryptografie-Management	redshift-cluster-kms-enabled	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass die Verschlüs selung mit AWS Key Management Service (AWS KMS) für Ihren Amazon Redshift Redshift-Cluster aktiviert ist. Um eventuell vorhanden e sensible Daten im Ruhezustand in Redshift-Clustern zu schützen, muss die Verschlüsselung von Daten im Ruhezusta nd aktiviert sein.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CM-3(6)	Kontrolle von Konfigurationsänderungen | Kryptografie-Management	s3- aktiviert bucket-server-side-encryption	Zum Schutz von Daten im Ruhezustand müssen Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon Simple Storage Service (Amazon S3)-Buckets aktiviert ist. Um eventuell vorhandene sensible Daten im Ruhezustand in Amazon-S3-Buckets zu schützen, muss die Verschlüsselung aktiviert sein.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CM-3(6)	Kontrolle von Konfigurationsänderungen | Kryptografie-Management	sagemaker-endpoint-configuration-kms-key-konfiguriert	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass die Verschlüsselung mit dem AWS Key Management Service (AWS KMS) für Ihren Endpunkt aktiviert ist. SageMaker Da sensible Daten auf dem SageMaker Endgerät gespeichert werden können, sollten Sie die Verschlüsselung im Ruhezustand aktivieren, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CM-3(6)	Kontrolle von Konfigurationsänderungen | Kryptografie-Management	secretsmanager-using-cmk	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass die Verschlüsselung mit dem AWS Key Management Service (AWS KMS) für AWS Secrets Manager aktiviert ist. Aktivieren Sie die Verschlüsselung von Daten im Ruhezustand, um eventuell vorhandene sensible Daten im Ruhezustand im Secrets Manager zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CM-3	Kontrolle von Konfigurationsänderungen	elb-deletion-protection-enabled	Diese Regel sorgt dafür, dass der Löschschutz für Elastic Load Balancing aktiviert ist. Verwenden Sie diese Funktion, um zu verhindern, dass Ihr Load Balancer versehentlich oder böswillig gelöscht wird, was zum Verlust der Verfügbarkeit Ihrer Anwendungen führen kann.
CM-3	Kontrolle von Konfigurationsänderungen	rds-instance-deletion-protection-aktiviert	Stellen Sie sicher, dass Amazon Relational Database Service (Amazon RDS)-Instances den Löschschutz aktiviert haben. Verwenden Sie den Löschschutz, um zu verhindern, dass Ihre Amazon-RDS-Instances versehentlich oder böswillig gelöscht werden, was zum Verlust der Verfügbarkeit Ihrer Anwendungen führen kann.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CM-7	Geringste Funktionalität	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) Security Groups können bei der Verwaltung des Netzwerkzugriffs helfen, indem sie eine statusbehaftete Filterung von eingehendem und ausgehendem Netzwerkverkehr zu Ressourcen bereitstellen. AWS Wenn Sie eingehenden (oder entfernten) Datenverkehr von 0.0.0.0/0 bis Port 22 auf Ihren Ressourcen nicht zulassen, können Sie den Remote-Zugriff einschränken.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CM-7	Geringste Funktionalität	no-unrestricted-route-to-igw	Stellen Sie sicher, dass EC2 Amazon-Routentabellen keine uneingeschränkten Routen zu einem Internet-Gateway enthalten. Durch das Entfernen oder Beschränken des Internetzugangs für Workloads innerhalb von Amazon VPCs können unbeabsichtigte Zugriffe in Ihrer Umgebung reduziert werden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CM-7	Geringste Funktionalität	restricted-common-ports	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass gemeinsame Ports für Amazon Elastic Compute Cloud (Amazon EC2) -Sicherheitsgruppen eingeschränkt sind. Wenn der Zugriff auf Ports nicht auf vertrauenswürdige Quellen beschränkt wird, kann dies zu Angriffen auf die Verfügbarkeit, Integrität und Vertraulichkeit von Systemen führen. Mit dieser Regel können Sie optional die Parameter blockedPort1–blockedPort5 festlegen (Standardkonfigurationen: 20, 21, 3389, 3306, 4333). Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CM-8(1)	Inventar der Systemkomponenten | Updates während der Installation und Deinstallation	ec2-manager instance-managed-by-systems	Eine Bestandsaufnahme der Softwareplattformen und Anwendungen innerhalb des Unternehmens ist möglich, indem Amazon Elastic Compute Cloud (Amazon EC2) - Instances mit AWS Systems Manager verwaltet werden. Verwenden Sie AWS Systems Manager, um detaillierte Systemkonfigurationen, Betriebssystem-Patch-Levels, Namen und Typ der Dienste, Softwareinstallationen, Anwendungsname, Herausgeber und Version sowie andere Details zu Ihrer Umgebung bereitzustellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CM-8(1)	Inventar der Systemkomponenten | Updates während der Installation und Deinstallation	ec2-check managedinstance-association-compliance-status	Verwenden Sie AWS Systems Manager Associations, um bei der Inventarisierung von Softwareplattformen und Anwendungen innerhalb eines Unternehmens zu helfen. AWS Systems Manager weist Ihren verwalteten Instanzen einen Konfigurationsstatus zu und ermöglicht es Ihnen, Basiswerte für Betriebssystem-Patch-Levels, Softwareinstallationen, Anwendungskonfigurationen und andere Details zu Ihrer Umgebung festzulegen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CM-8(2)	Inventar der Systemkomponenten | Automatisierte Wartung	ec2-manager instance-managed-by-systems	Eine Bestandsaufnahme der Softwareplattformen und Anwendungen innerhalb des Unternehmens ist möglich, indem Amazon Elastic Compute Cloud (Amazon EC2) - Instances mit AWS Systems Manager verwaltet werden. Verwenden Sie AWS Systems Manager, um detaillierte Systemkonfigurationen, Betriebssystem-Patch-Levels, Namen und Typ der Dienste, Softwareinstallationen, Anwendungsname, Herausgeber und Version sowie andere Details zu Ihrer Umgebung bereitzustellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CM-8(3)	Inventar der Systemkomponenten | Automatisierte Erkennung nicht autorisierter Komponenten	ec2-manager instance-managed-by-systems	Eine Bestandsaufnahme der Softwareplattformen und Anwendungen innerhalb des Unternehmens ist möglich, indem Amazon Elastic Compute Cloud (Amazon EC2) - Instances mit AWS Systems Manager verwaltet werden. Verwenden Sie AWS Systems Manager, um detaillierte Systemkonfigurationen, Betriebssystem-Patch-Levels, Namen und Typ der Dienste, Softwareinstallationen, Anwendungsname, Herausgeber und Version sowie andere Details zu Ihrer Umgebung bereitzustellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CM-8(3)	Inventar der Systemkomponenten | Automatisierte Erkennung nicht autorisierter Komponenten	ec2-check managedinstance-association-compliance-status	Verwenden Sie AWS Systems Manager Associations, um bei der Inventarisierung von Softwareplattformen und Anwendungen innerhalb eines Unternehmens zu helfen. AWS Systems Manager weist Ihren verwalteten Instanzen einen Konfigurationsstatus zu und ermöglicht es Ihnen, Basiswerte für Betriebssystem-Patch-Levels, Softwareinstallationen, Anwendungskonfigurationen und andere Details zu Ihrer Umgebung festzulegen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CM-8(3)	Inventar der Systemkomponenten | Automatisierte Erkennung nicht autorisierter Komponenten	ec2-check managedinstance-patch-compliance-status	Aktivieren Sie diese Regel, um bei der Identifizierung und Dokumentation von Sicherheitslücken in Amazon Elastic Compute Cloud (Amazon EC2) zu helfen. Die Regel prüft, ob die EC2 Amazon-Instance die Patch-Konformität im AWS Systems Manager gemäß den Richtlinien und Verfahren Ihrer Organisation einhält.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CM-8(3)	Inventar der Systemkomponenten | Automatisierte Erkennung nicht autorisierter Komponenten	guardduty-enabled-centralized	Amazon GuardDuty kann mithilfe von Threat Intellige nce Feeds helfen, potenzielle Cybersich erheitsereignisse zu überwachen und zu erkennen. Dazu gehören Listen mit bösartigen IPs und maschinel len Lernmethoden zur Identifizierung unerwarteter, nicht autorisierter und bösartiger Aktivitäten in Ihrer AWS Cloud-Umgebung.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CM-8	Inventar der Systemkomponenten	ec2-manager instance-managed-by-systems	Eine Bestandsaufnahme der Softwareplattformen und Anwendungen innerhalb des Unternehmens ist möglich, indem Amazon Elastic Compute Cloud (Amazon EC2) - Instances mit AWS Systems Manager verwaltet werden. Verwenden Sie AWS Systems Manager, um detaillierte Systemkonfigurationen, Betriebssystem-Patch-Levels, Namen und Typ der Dienste, Softwareinstallationen, Anwendungsname, Herausgeber und Version sowie andere Details zu Ihrer Umgebung bereitzustellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CM-8	Inventar der Systemkomponenten	ec2-check managedinstance-association-compliance-status	Verwenden Sie AWS Systems Manager Associations, um bei der Inventarisierung von Softwareplattformen und Anwendungen innerhalb eines Unternehmens zu helfen. AWS Systems Manager weist Ihren verwalteten Instanzen einen Konfigurationsstatus zu und ermöglicht es Ihnen, Basiswerte für Betriebssystem-Patch-Levels, Softwareinstallationen, Anwendungskonfigurationen und andere Details zu Ihrer Umgebung festzulegen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CP-2(2)	Notfallplan | Kapazitätsplanung	autoscaling-group-elb-healthcheck-erforderlich	Die Elastic Load Balancer (ELB) - Zustandsprüfungen für Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling Scaling-Gruppen unterstützen die Aufrechterhaltung einer angemessenen Kapazität und Verfügbarkeit. Der Load Balancer sendet regelmäßig Pings, versucht Verbindungen herzustellen oder sendet Anfragen, um den Zustand der EC2 Amazon-Instances in einer Gruppe mit auto-scaling zu testen. Wenn eine Instance nicht zurückmeldet, wird der Traffic an eine neue EC2 Amazon-Instance gesendet.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CP-2(2)	Notfallplan | Kapazitätsplanung	dynamodb-autoscaling-enabled	Amazon DynamoDB Auto Scaling verwendet den AWS Application Auto Scaling-Service, um die bereitgestellte Durchsatzkapazität so anzupassen, dass sie automatisch auf tatsächliche Verkehrsmuster reagiert. Auf diese Weise kann eine Tabelle oder ein globaler sekundärer Index die bereitgestellte Lese-/Schreibkapazität erhöhen, um plötzliche Erhöhungen des Datenverkehrs ohne Drosselung zu bewältigen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CP-6(1)	Alternativer Speicherort | Trennung vom primären Standort	dynamodb-in-backup-plan	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon DynamoDB-Tabellen Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CP-6(1)	Alternativer Speicherort | Trennung vom primären Standort	ebs-in-backup-plan	Stellen Sie zur Unterstützung der Datensicherungsprozesse sicher, dass Ihre Amazon Elastic Block Store (Amazon EBS) -Volumes Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CP-6(1)	Alternativer Speicherort | Trennung vom primären Standort	efs-in-backup-plan	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon Elastic File System (Amazon EFS) -Dateisysteme Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CP-6(1)	Alternativer Speicherort | Trennung vom primären Standort	redshift-backup-enabled	Stellen Sie zur Unterstützung der Datensicherungsprozesse sicher, dass Ihre Amazon-Redshift-Cluster über automatisierte Snapshots verfügen. Wenn automatisierte Snapshots für einen Cluster aktiviert sind, erstellt Redshift in regelmäßigen Abständen Snapshots dieses Clusters. Standardmäßig erstellt Redshift alle acht Stunden oder alle 5 GB einen Snapshot für jeden Knoten mit Datenänderungen oder je nachdem, was zuerst eintritt.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CP-6(1)	Alternativer Speicherort | Trennung vom primären Standort	db-instance-backup-enabled	Die Sicherungsfunktion von Amazon RDS erstellt Sicherungen Ihrer Datenbanken und Transaktionsprotokolle. Amazon RDS erstellt einen Snapshot für das Speichervolume Ihrer DB-Instance, sodass die gesamte DB-Instance gesichert wird. Sie können im System spezifische Aufbewahrungsfristen festlegen, um Ihre Ausfallsicherheitsanforderungen zu erfüllen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CP-6(1)	Alternativer Speicherort | Trennung vom primären Standort	elasticache-redis-cluster-automatic-Backup-Check	Wenn automatische Backups aktiviert sind, ElastiCache erstellt Amazon täglich ein Backup des Clusters. Die Sicherung kann für eine von Ihrer Organisation festgelegte Anzahl von Tagen aufbewahrt werden. Automatische Backups schützen vor Datenverlust. Bei einem Ausfall können Sie einen neuen Cluster erstellen, der Ihre Daten aus dem aktuellen Backup wiederherstellt.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CP-6(1)	Alternativer Speicherort | Trennung vom primären Standort	s-3 bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) unterstützt die Aufrechterhaltung einer angemessenen Kapazität und Verfügbarkeit. CRR ermöglicht das automatische, asynchrone Kopieren von Objekten in Amazon-S3-Buckets, um die Datenverfügbarkeit sicherzustellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CP-6(1)	Alternativer Speicherort | Trennung vom primären Standort	s-3 bucket-versioning-enabled	Die Versionsverwaltung von Amazon Simple Storage Service (Amazon S3)-Buckets hilft dabei, mehrere Varianten eines Objekts im selben Amazon-S3-Bucket zu speichern. Verwenden Sie die Versionsverwaltung, um sämtliche Versionen aller Objekte in Ihrem Amazon-S3-Bucket zu speichern, abzurufen oder wiederherzustellen. Mit der Versionsverwaltung können Sie Versionen sowohl nach unbeabsichtigten Benutzeraktionen als auch nach Anwendungsfehlern problemlos wiederherstellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CP-6(2)	Alternativer Speicherort | Recovery Time und Recovery Point Objectives	dynamodb-in-backup-plan	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon DynamoDB-Tabellen Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CP-6(2)	Alternativer Speicherort | Recovery Time und Recovery Point Objectives	ebs-in-backup-plan	Stellen Sie zur Unterstützung der Datensicherungsprozesse sicher, dass Ihre Amazon Elastic Block Store (Amazon EBS) -Volumes Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CP-6(2)	Alternativer Speicherort | Recovery Time und Recovery Point Objectives	efs-in-backup-plan	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon Elastic File System (Amazon EFS) -Dateisysteme Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CP-6(2)	Alternativer Speicherort | Recovery Time und Recovery Point Objectives	elb-cross-zone-load-Balancing aktiviert	Aktivieren Sie zonenübergreifendes Load Balancing für Ihre Elastic Load Balancer (ELBs), um eine angemessene Kapazität und Verfügbarkeit aufrechtzuerhalten. Zonenübergreifendes Load Balancing reduziert die Notwendigkeit, die gleiche Anzahl von Instances in jeder aktivierten Availability Zone aufrechtzuerhalten. Es verbessert auch die Fähigkeit Ihrer Anwendung, den Verlust einer oder mehrerer Instances zu bewältigen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CP-6(2)	Alternativer Speicherort | Recovery Time und Recovery Point Objectives	redshift-backup-enabled	Stellen Sie zur Unterstützung der Datensicherungsprozesse sicher, dass Ihre Amazon-Redshift-Cluster über automatisierte Snapshots verfügen. Wenn automatisierte Snapshots für einen Cluster aktiviert sind, erstellt Redshift in regelmäßigen Abständen Snapshots dieses Clusters. Standardmäßig erstellt Redshift alle acht Stunden oder alle 5 GB einen Snapshot für jeden Knoten mit Datenänderungen oder je nachdem, was zuerst eintritt.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CP-6(2)	Alternativer Speicherort | Recovery Time und Recovery Point Objectives	s3- version-lifecycle-policy-check	Mit Amazon-S3-Lebenszyklusregeln können Sie Aktionen definieren, die Amazon S3 während der Lebensdauer eines Objekts ausführen soll (z. B. die Überführung von Objekten in eine andere Speicherklasse, ihre Archivierung oder Löschung nach einem bestimmten Zeitraum).

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CP-6(2)	Alternativer Speicherort | Recovery Time und Recovery Point Objectives	db-instance-backup-enabled	Die Sicherungsfunktion von Amazon RDS erstellt Sicherungen Ihrer Datenbanken und Transaktionsprotokolle. Amazon RDS erstellt einen Snapshot für das Speichervolume Ihrer DB-Instance, sodass die gesamte DB-Instance gesichert wird. Sie können im System spezifische Aufbewahrungsfristen festlegen, um Ihre Ausfallsicherheitsanforderungen zu erfüllen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CP-6(2)	Alternativer Speicherort | Recovery Time und Recovery Point Objectives	dynamodb-autoscaling-enabled	Amazon DynamoDB Auto Scaling verwendet den AWS Application Auto Scaling-Service, um die bereitgestellte Durchsatzkapazität so anzupassen, dass sie automatisch auf tatsächliche Verkehrsmuster reagiert. Auf diese Weise kann eine Tabelle oder ein globaler sekundärer Index die bereitgestellte Lese-/Schreibkapazität erhöhen, um plötzliche Erhöhungen des Datenverkehrs ohne Drosselung zu bewältigen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CP-6(2)	Alternativer Speicherort | Recovery Time und Recovery Point Objectives	dynamodb-pitr-enabled	Aktivieren Sie diese Regel, um zu überprüfen, ob die Informationen gesichert wurden. Es verwaltet auch die Backups, indem es sicherstellt, dass die point-in-time Wiederherstellung in Amazon DynamoDB aktiviert ist. Bei der Wiederherstellung werden fortlaufende Backups Ihrer Tabelle für die letzten 35 Tage gespeichert.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CP-6(2)	Alternativer Speicherort | Recovery Time und Recovery Point Objectives	elasticache-redis-cluster-automatic-Backup-Prüfung	Wenn automatische Backups aktiviert sind, ElastiCache erstellt Amazon täglich ein Backup des Clusters. Die Sicherung kann für eine von Ihrer Organisation festgelegte Anzahl von Tagen aufbewahrt werden. Automatische Backups schützen vor Datenverlust. Bei einem Ausfall können Sie einen neuen Cluster erstellen, der Ihre Daten aus dem aktuellen Backup wiederherstellt.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CP-6(2)	Alternativer Speicherort | Recovery Time und Recovery Point Objectives	rds-multi-az-support	Die Multi-AZ-Unterstützung in Amazon Relational Database Service (Amazon RDS) bietet eine verbesserte Verfügbarkeit und Beständigkeit von Datenbank-Instances. Wenn Sie eine Multi-AZ-Datenbank-Instance bereitstellen, erstellt Amazon RDS automatisch eine primäre Datenbank-Instance und repliziert die Daten synchron auf eine Standby-Instance in einer anderen Availability Zone. Jede Availability Zone läuft auf einer eigenen, physisch getrennten, unabhängigen Infrastruktur und ist auf eine hohe Verfügbarkeit ausgelegt. Im Falle eines Infrastrukturausfalls führt Amazon RDS einen automatis

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			chen Failover zum Standby-Modus durch, sodass Sie den Datenbankbetrieb wieder aufnehmen können, sobald der Failover abgeschlo ssen ist.
CP-6(2)	Alternativer Speichero rt | Recovery Time und Recovery Point Objectives	s-3 bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) unterstützt die Aufrechterhaltung einer angemesse nen Kapazität und Verfügbarkeit. CRR ermöglicht das automatische, asynchrone Kopieren von Objekten in Amazon-S3-Buckets, um die Datenverf ügbarkeit sicherzus tellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CP-6(2)	Alternativer Speicherort | Recovery Time und Recovery Point Objectives	s-3 bucket-versioning-enabled	Die Versionsverwaltung von Amazon Simple Storage Service (Amazon S3)-Buckets hilft dabei, mehrere Varianten eines Objekts im selben Amazon-S3-Bucket zu speichern. Verwenden Sie die Versionsverwaltung, um sämtliche Versionen aller Objekte in Ihrem Amazon-S3-Bucket zu speichern, abzurufen oder wiederherzustellen. Mit der Versionsverwaltung können Sie Versionen sowohl nach unbeabsichtigten Benutzeraktionen als auch nach Anwendungsfehlern problemlos wiederherstellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CP-6(2)	Alternativer Speicherort | Recovery Time und Recovery Point Objectives	vpc-vpn-2-tunnels-up	Redundante Site-to-Site VPN-Tunnel können implementiert werden, um die Anforderungen an die Ausfallsicherheit zu erfüllen. Es verwendet zwei Tunnel, um die Konnektivität sicherzustellen, falls eine der Site-to-Site VPN-Verbindungen nicht verfügbar ist. Um sich vor einem Verbindungsverlust zu schützen, können Sie für den Fall, dass Ihr Kunden-Gateway nicht verfügbar ist, eine zweite Site-to-Site VPN-Verbindung zu Ihrer Amazon Virtual Private Cloud (Amazon VPC) und Ihrem Virtual Private Gateway einrichten, indem Sie ein zweites Kunden-Gateway verwenden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CP-6	Alternativer Speicherort	dynamodb-in-backup-plan	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon DynamoDB-Tabellen Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CP-6	Alternativer Speicherort	ebs-in-backup-plan	Stellen Sie zur Unterstützung der Datensicherungsprozesse sicher, dass Ihre Amazon Elastic Block Store (Amazon EBS) -Volumes Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CP-6	Alternativer Speicherort	efs-in-backup-plan	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon Elastic File System (Amazon EFS) -Dateisysteme Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CP-6	Alternativer Speicherort	redshift-backup-enabled	Stellen Sie zur Unterstützung der Datensicherungsprozesse sicher, dass Ihre Amazon-Redshift-Cluster über automatisierte Snapshots verfügen. Wenn automatisierte Snapshots für einen Cluster aktiviert sind, erstellt Redshift in regelmäßigen Abständen Snapshots dieses Clusters. Standardmäßig erstellt Redshift alle acht Stunden oder alle 5 GB einen Snapshot für jeden Knoten mit Datenänderungen oder je nachdem, was zuerst eintritt.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CP-6	Alternativer Speicherort	db-instance-backup-enabled	Die Sicherungsfunktion von Amazon RDS erstellt Sicherungen Ihrer Datenbanken und Transaktionsprotokolle. Amazon RDS erstellt einen Snapshot für das Speichervolume Ihrer DB-Instance, sodass die gesamte DB-Instance gesichert wird. Sie können im System spezifische Aufbewahrungsfristen festlegen, um Ihre Ausfallsicherheitsanforderungen zu erfüllen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CP-6	Alternativer Speicherort	elasticache-redis-cluster-automatic-Backup-Check	Wenn automatische Backups aktiviert sind, ElastiCache erstellt Amazon täglich ein Backup des Clusters. Die Sicherung kann für eine von Ihrer Organisation festgelegte Anzahl von Tagen aufbewahrt werden. Automatische Backups schützen vor Datenverlust. Bei einem Ausfall können Sie einen neuen Cluster erstellen, der Ihre Daten aus dem aktuellen Backup wiederherstellt.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CP-6	Alternativer Speicherort	s-3 bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) unterstützt die Aufrechterhaltung einer angemessenen Kapazität und Verfügbarkeit. CRR ermöglicht das automatische, asynchrone Kopieren von Objekten in Amazon-S3-Buckets, um die Datenverfügbarkeit sicherzustellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CP-6	Alternativer Speicherort	s-3 bucket-versioning-enabled	Die Versionsverwaltung von Amazon Simple Storage Service (Amazon S3)-Buckets hilft dabei, mehrere Varianten eines Objekts im selben Amazon-S3-Bucket zu speichern. Verwenden Sie die Versionsverwaltung, um sämtliche Versionen aller Objekte in Ihrem Amazon-S3-Bucket zu speichern, abzurufen oder wiederherzustellen. Mit der Versionsverwaltung können Sie Versionen sowohl nach unbeabsichtigten Benutzeraktionen als auch nach Anwendungsfehlern problemlos wiederherstellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CP-9	Systemsicherung	dynamodb-in-backup-plan	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon DynamoDB-Tabellen Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CP-9	Systemsicherung	ebs-in-backup-plan	Stellen Sie zur Unterstützung der Datensicherungspro zesse sicher, dass Ihre Amazon Elastic Block Store (Amazon EBS) -Volumes Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwaltet er Backup-Service mit einer richtlini enbasierten Backup-Lösung. Diese Lösung vereinfac ht Ihr Sicherung smanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforde rungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CP-9	Systemsicherung	efs-in-backup-plan	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon Elastic File System (Amazon EFS) -Dateisysteme Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CP-9	Systemsicherung	redshift-backup-enabled	Stellen Sie zur Unterstützung der Datensicherungsprozesse sicher, dass Ihre Amazon-Redshift-Cluster über automatisierte Snapshots verfügen. Wenn automatisierte Snapshots für einen Cluster aktiviert sind, erstellt Redshift in regelmäßigen Abständen Snapshots dieses Clusters. Standardmäßig erstellt Redshift alle acht Stunden oder alle 5 GB einen Snapshot für jeden Knoten mit Datenänderungen oder je nachdem, was zuerst eintritt.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CP-9	Systemsicherung	s3- version-lifecycle-policy-check	Mit Amazon-S3-Lebenszyklusregeln können Sie Aktionen definieren, die Amazon S3 während der Lebensdau er eines Objekts ausführen soll (z. B. die Überfüh rung von Objekten in eine andere Speicherklasse, ihre Archivierung oder Löschung nach einem bestimmten Zeitraum) .

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CP-9	Systemsicherung	db-instance-backup-enabled	Die Sicherungsfunktion von Amazon RDS erstellt Sicherungen Ihrer Datenbanken und Transaktionsprotokolle. Amazon RDS erstellt einen Snapshot für das Speichervolume Ihrer DB-Instance, sodass die gesamte DB-Instance gesichert wird. Sie können im System spezifische Aufbewahrungsfristen festlegen, um Ihre Ausfallsicherheitsanforderungen zu erfüllen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CP-9	Systemsicherung	dynamodb-pitr-enabled	Aktivieren Sie diese Regel, um zu überprüfen, ob die Informationen gesichert wurden. Es verwaltet auch die Backups, indem es sicherstellt, dass die point-in-time Wiederherstellung in Amazon DynamoDB aktiviert ist. Bei der Wiederherstellung werden fortlaufende Backups Ihrer Tabelle für die letzten 35 Tage gespeichert.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CP-9	Systemsicherung	ebs-optimized-instance	Eine optimierte Instance im Amazon Elastic Block Store (Amazon EBS) bietet zusätzliche, dedizierte Kapazität für Amazon-EBS-I/O-Vorgänge. Diese Optimierung bietet die beste Leistung für Ihr EBS-Volume, indem Konflikte zwischen Amazon-EBS-I/O und anderem Datenverkehr von Ihrer Instance minimiert werden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CP-9	Systemsicherung	elasticache-redis-cluster-automatic-Backup-Prüfung	Wenn automatische Backups aktiviert sind, ElastiCache erstellt Amazon täglich ein Backup des Clusters. Die Sicherung kann für eine von Ihrer Organisation festgelegte Anzahl von Tagen aufbewahrt werden. Automatische Backups schützen vor Datenverlust. Bei einem Ausfall können Sie einen neuen Cluster erstellen, der Ihre Daten aus dem aktuellen Backup wiederherstellt.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CP-9	Systemsicherung	redshift-cluster-maintenancesettings-check	Diese Regel stellt sicher, dass Amazon-Redshift-Cluster die bevorzugten Einstellungen für Ihre Organisation haben. Insbesondere sorgt sie dafür, dass Cluster bevorzugte Wartungsfenster und automatisierte Aufbewahrungsfristen für Snapshots für die Datenbank haben. Für diese Regel müssen Sie die festlegen allowVersionUpgrade. Der Standardwert ist „true“. Außerdem können Sie optional den Zeitraum preferredMaintenanceWindow (der Standardwert ist sa: 16:00 -sa: 16:30) und den automated SnapshotRetention Zeitraum (der Standardwert ist 1) festlegen. Die tatsächlichen Werte müssen den Richtlini

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			en Ihrer Organisation entsprechen.
CP-9	Systemsicherung	s3- bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) unterstützt die Aufrechterhaltung einer angemesse nen Kapazität und Verfügbarkeit. CRR ermöglicht das automatische, asynchrone Kopieren von Objekten in Amazon-S3-Buckets, um die Datenverf ügbarkeit sicherzus tellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CP-9	Systemsicherung	s-3 bucket-versioning-enabled	Die Versionsverwaltung von Amazon Simple Storage Service (Amazon S3)-Buckets hilft dabei, mehrere Varianten eines Objekts im selben Amazon-S3-Bucket zu speichern. Verwenden Sie die Versionsverwaltung, um sämtliche Versionen aller Objekte in Ihrem Amazon-S3-Bucket zu speichern, abzurufen oder wiederherzustellen. Mit der Versionsverwaltung können Sie Versionen sowohl nach unbeabsichtigten Benutzeraktionen als auch nach Anwendungsfehlern problemlos wiederherstellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CP-10	Systemwiederherstellung und -rekonstitution	dynamodb-in-backup-plan	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon DynamoDB-Tabellen Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CP-10	Systemwiederherstellung und -rekonstitution	ebs-in-backup-plan	Stellen Sie zur Unterstützung der Datensicherungsprozesse sicher, dass Ihre Amazon Elastic Block Store (Amazon EBS) -Volumes Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CP-10	Systemwiederherstellung und -rekonstitution	efs-in-backup-plan	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon Elastic File System (Amazon EFS) -Dateisysteme Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CP-10	Systemwiederherstellung und -rekonstitution	elb-cross-zone-load-Balancing aktiviert	Aktivieren Sie zonenübergreifendes Load Balancing für Ihre Elastic Load Balancer (ELBs), um eine angemessene Kapazität und Verfügbarkeit aufrechtzuerhalten. Zonenübergreifendes Load Balancing reduziert die Notwendigkeit, die gleiche Anzahl von Instances in jeder aktivierten Availability Zone aufrechtzuerhalten. Es verbessert auch die Fähigkeit Ihrer Anwendung, den Verlust einer oder mehrerer Instances zu bewältigen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CP-10	Systemwiederherstellung und -rekonstitution	redshift-backup-enabled	Stellen Sie zur Unterstützung der Datensicherungsprozesse sicher, dass Ihre Amazon-Redshift-Cluster über automatisierte Snapshots verfügen. Wenn automatisierte Snapshots für einen Cluster aktiviert sind, erstellt Redshift in regelmäßigen Abständen Snapshots dieses Clusters. Standardmäßig erstellt Redshift alle acht Stunden oder alle 5 GB einen Snapshot für jeden Knoten mit Datenänderungen oder je nachdem, was zuerst eintritt.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CP-10	Systemwiederherstellung und -rekonstitution	s3- version-lifecycle-policy-check	Mit Amazon-S3-Lebenszyklusregeln können Sie Aktionen definieren, die Amazon S3 während der Lebensdauer eines Objekts ausführen soll (z. B. die Überführung von Objekten in eine andere Speicherklasse, ihre Archivierung oder Löschung nach einem bestimmten Zeitraum).

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CP-10	Systemwiederherstellung und -rekonstitution	db-instance-backup-enabled	Die Sicherungsfunktion von Amazon RDS erstellt Sicherungen Ihrer Datenbanken und Transaktionsprotokolle. Amazon RDS erstellt einen Snapshot für das Speichervolume Ihrer DB-Instance, sodass die gesamte DB-Instance gesichert wird. Sie können im System spezifische Aufbewahrungsfristen festlegen, um Ihre Ausfallsicherheitsanforderungen zu erfüllen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CP-10	Systemwiederherstellung und -rekonstitution	dynamodb-autoscaling-enabled	Amazon DynamoDB Auto Scaling verwendet den AWS Application Auto Scaling-Service, um die bereitgestellte Durchsatzkapazität so anzupassen, dass sie automatisch auf tatsächliche Verkehrsmuster reagiert. Auf diese Weise kann eine Tabelle oder ein globaler sekundärer Index die bereitgestellte Lese-/Schreibkapazität erhöhen, um plötzliche Erhöhungen des Datenverkehrs ohne Drosselung zu bewältigen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CP-10	Systemwiederherstellung und -rekonstitution	dynamodb-pitr-enabled	Aktivieren Sie diese Regel, um zu überprüfen, ob die Informationen gesichert wurden. Es verwaltet auch die Backups, indem es sicherstellt, dass die point-in-time Wiederherstellung in Amazon DynamoDB aktiviert ist. Bei der Wiederherstellung werden fortlaufende Backups Ihrer Tabelle für die letzten 35 Tage gespeichert.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CP-10	Systemwiederherstellung und -rekonstitution	ebs-optimized-instance	Eine optimierte Instance im Amazon Elastic Block Store (Amazon EBS) bietet zusätzliche, dedizierte Kapazität für Amazon-EBS-I/O-Vorgänge. Diese Optimierung bietet die beste Leistung für Ihr EBS-Volume, indem Konflikte zwischen Amazon-EBS-I/O und anderem Datenverkehr von Ihrer Instance minimiert werden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CP-10	Systemwiederherstellung und -rekonstitution	elasticache-redis-cluster-automatic-Backup-Prüfung	Wenn automatische Backups aktiviert sind, ElastiCache erstellt Amazon täglich ein Backup des Clusters. Die Sicherung kann für eine von Ihrer Organisation festgelegte Anzahl von Tagen aufbewahrt werden. Automatische Backups schützen vor Datenverlust. Bei einem Ausfall können Sie einen neuen Cluster erstellen, der Ihre Daten aus dem aktuellen Backup wiederherstellt.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CP-10	Systemwiederherstellung und -rekonstitution	rds-multi-az-support	Die Multi-AZ-Unterstützung in Amazon Relational Database Service (Amazon RDS) bietet eine verbesserte Verfügbarkeit und Beständigkeit von Datenbank-Instances. Wenn Sie eine Multi-AZ-Datenbank-Instance bereitstellen, erstellt Amazon RDS automatisch eine primäre Datenbank-Instance und repliziert die Daten synchron auf eine Standby-Instance in einer anderen Availability Zone. Jede Availability Zone läuft auf einer eigenen, physisch getrennten, unabhängigen Infrastruktur und ist auf eine hohe Verfügbarkeit ausgelegt. Im Falle eines Infrastrukturausfalls führt Amazon RDS einen automatis

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			chen Failover zum Standby-Modus durch, sodass Sie den Datenbankbetrieb wieder aufnehmen können, sobald der Failover abgeschlo ssen ist.
CP-10	Systemwiederherste llung und -rekonsti tution	s-3 bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) unterstützt die Aufrechterhaltung einer angemesse nen Kapazität und Verfügbarkeit. CRR ermöglicht das automatische, asynchrone Kopieren von Objekten in Amazon-S3-Buckets, um die Datenverf ügbarkeit sicherzus tellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CP-10	Systemwiederherstellung und -rekonstitution	s-3 bucket-versioning-enabled	Die Versionsverwaltung von Amazon Simple Storage Service (Amazon S3)-Buckets hilft dabei, mehrere Varianten eines Objekts im selben Amazon-S3-Bucket zu speichern. Verwenden Sie die Versionsverwaltung, um sämtliche Versionen aller Objekte in Ihrem Amazon-S3-Bucket zu speichern, abzurufen oder wiederherzustellen. Mit der Versionsverwaltung können Sie Versionen sowohl nach unbeabsichtigten Benutzeraktionen als auch nach Anwendungsfehlern problemlos wiederherstellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CP-10	Systemwiederherstellung und -rekonstitution	vpc-vpn-2-tunnels-up	Redundante Site-to-Site VPN-Tunnel können implementiert werden, um die Anforderungen an die Ausfallsicherheit zu erfüllen. Es verwendet zwei Tunnel, um die Konnektivität sicherzustellen, falls eine der Site-to-Site VPN-Verbindungen nicht verfügbar ist. Um sich vor einem Verbindungsverlust zu schützen, können Sie für den Fall, dass Ihr Kunden-Gateway nicht verfügbar ist, eine zweite Site-to-Site VPN-Verbindung zu Ihrer Amazon Virtual Private Cloud (Amazon VPC) und Ihrem Virtual Private Gateway einrichten, indem Sie ein zweites Kunden-Gateway verwenden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
IA-2(1)	Identifizierung und Authentifizierung (Benutzer in der Organisation) | Multi-Faktor-Authentifizierung für privilegierte Konten	iam-user-mfa-enabled	Aktivieren Sie diese Regel, um den Zugriff auf Ressourcen in der AWS Cloud einzuschränken. Diese Regel sorgt dafür, dass die Multi-Faktor-Authentifizierung (MFA) für alle Benutzer aktiviert ist. MFA sorgt für eine weitere Schutzebene zusätzlich zu den Anmeldeinformationen. Reduzieren Sie Fälle von kompromittierten Konten, indem Sie MFA für Benutzer vorschreiben.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
IA-2(1)	Identifizierung und Authentifizierung (Benutzer in der Organisation) | Multi-Faktor-Authentifizierung für privilegierte Konten	mfa-enabled-for-iam-Konsolenzugriff	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass MFA für alle AWS Identity and Access Management (IAM) -Benutzer aktiviert ist, die über ein Konsolenkennwort verfügen. MFA sorgt für eine weitere Schutzebene zusätzlich zu den Anmeldeinformationen. Indem Sie MFA für Benutzer vorschreiben, können Sie Fälle kompromittierter Konten reduzieren und verhindern, dass unbefugte Benutzer auf vertrauliche Daten zugreifen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
IA-2(1)	Identifizierung und Authentifizierung (Benutzer in der Organisation) | Multi-Faktor-Authentifizierung für privilegierte Konten	root-account-hardware-mfa-aktiviert	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Hardware-MFA für den Root-Benutzer aktiviert ist. Der Stammbenutzer ist der AWS-Konto-Benutzer mit den meisten Berechtigungen. MFA sorgt für eine weitere Schutzebene zusätzlich zu den Anmeldeinformationen. Indem Sie MFA für den Root-Benutzer vorschreiben, können Sie die Anzahl AWS-Konten kompromittierter Benutzer reduzieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
IA-2(1)	Identifizierung und Authentifizierung (Benutzer in der Organisation) | Multi-Faktor-Authentifizierung für privilegierte Konten	root-account-mfa-enabled	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass MFA für den Root-Benutzer aktiviert ist. Der Stammbenutzer ist der AWS-Konto-Benutzer mit den meisten Berechtigungen. MFA sorgt für eine weitere Schutzebene zusätzlich zu den Anmeldeinformationen. Indem Sie MFA für den Root-Benutzer vorschreiben, können Sie die Anzahl AWS-Konten kompromittierter Benutzer reduzieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
IA-2(2)	Identifizierung und Authentifizierung (Benutzer in der Organisation) | Multi-Faktor-Authentifizierung für nicht privilegierte Konten	iam-user-mfa-enabled	Aktivieren Sie diese Regel, um den Zugriff auf Ressourcen in der AWS Cloud einzuschränken. Diese Regel sorgt dafür, dass die Multi-Faktor-Authentifizierung (MFA) für alle Benutzer aktiviert ist. MFA sorgt für eine weitere Schutzebene zusätzlich zu den Anmeldeinformationen. Reduzieren Sie Fälle von kompromittierten Konten, indem Sie MFA für Benutzer vorschreiben.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
IA-2(2)	Identifizierung und Authentifizierung (Benutzer in der Organisation) | Multi-Faktor-Authentifizierung für nicht privilegierte Konten	mfa-enabled-for-iam-Konsolenzugriff	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass MFA für alle AWS Identity and Access Management (IAM) -Benutzer aktiviert ist, die über ein Konsolenkennwort verfügen. MFA sorgt für eine weitere Schutzebene zusätzlich zu den Anmeldeinformationen. Indem Sie MFA für Benutzer vorschreiben, können Sie Fälle kompromittierter Konten reduzieren und verhindern, dass unbefugte Benutzer auf vertrauliche Daten zugreifen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
IA-2(2)	Identifizierung und Authentifizierung (Benutzer in der Organisation) | Multi-Faktor-Authentifizierung für nicht privilegierte Konten	root-account-hardware-mfa-aktiviert	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Hardware-MFA für den Root-Benutzer aktiviert ist. Der Stammbenutzer ist der AWS-Konto-Benutzer mit den meisten Berechtigungen. MFA sorgt für eine weitere Schutzebene zusätzlich zu den Anmeldeinformationen. Indem Sie MFA für den Root-Benutzer vorschreiben, können Sie die Anzahl AWS-Konten kompromittierter Benutzer reduzieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
IA-2(2)	Identifizierung und Authentifizierung (Benutzer in der Organisation) | Multi-Faktor-Authentifizierung für nicht privilegierte Konten	root-account-mfa-enabled	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass MFA für den Root-Benutzer aktiviert ist. Der Stammbenutzer ist der AWS-Konto-Benutzer mit den meisten Berechtigungen. MFA sorgt für eine weitere Schutzebene zusätzlich zu den Anmeldeinformationen. Indem Sie MFA für den Root-Benutzer vorschreiben, können Sie die Anzahl AWS-Konten kompromittierter Benutzer reduzieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
IA-2(6)	Identifizierung und Authentif izierung (Benutzer im Unternehmen) | Zugriff auf Konten – separates Gerät	iam-user-mfa-enabled	Aktivieren Sie diese Regel, um den Zugriff auf Ressourcen in der AWS Cloud einzuschr änken. Diese Regel sorgt dafür, dass die Multi-Faktor-Authe ntifizierung (MFA) für alle Benutzer aktiviert ist. MFA sorgt für eine weitere Schutzebe ne zusätzlich zu den Anmeldeinformation en. Reduzieren Sie Fälle von kompromit tierten Konten, indem Sie MFA für Benutzer vorschreiben.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
IA-2(6)	Identifizierung und Authentif izierung (Benutzer im Unternehmen) | Zugriff auf Konten – separates Gerät	mfa-enabled-for-iam-Konsolenzugriff	Verwalten Sie den Zugriff auf Ressource n in der AWS Cloud, indem Sie sicherste llen, dass MFA für alle AWS Identity and Access Managemen t (IAM) -Benutzer aktiviert ist, die über ein Konsolenk ennwort verfügen. MFA sorgt für eine weitere Schutzebe ne zusätzlich zu den Anmeldeinformation en. Indem Sie MFA für Benutzer vorschrei ben, können Sie Fälle kompromittierter Konten reduzieren und verhindern, dass unbefugte Benutzer auf vertrauliche Daten zugreifen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
IA-2(6)	Identifizierung und Authentifizierung (Benutzer im Unternehmen) | Zugriff auf Konten – separates Gerät	root-account-hardware-mfa-aktiviert	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Hardware-MFA für den Root-Benutzer aktiviert ist. Der Stammbenutzer ist der AWS-Konto-Benutzer mit den meisten Berechtigungen. MFA sorgt für eine weitere Schutzebene zusätzlich zu den Anmeldeinformationen. Indem Sie MFA für den Root-Benutzer vorschreiben, können Sie die Anzahl AWS-Konten kompromittierter Benutzer reduzieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
IA-2(6)	Identifizierung und Authentifizierung (Benutzer im Unternehmen) | Zugriff auf Konten – separates Gerät	root-account-mfa-enabled	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass MFA für den Root-Benutzer aktiviert ist. Der Stammbenutzer ist der AWS-Konto-Benutzer mit den meisten Berechtigungen. MFA sorgt für eine weitere Schutzebene zusätzlich zu den Anmeldeinformationen. Indem Sie MFA für den Root-Benutzer vorschreiben, können Sie die Anzahl AWS-Konten kompromittierter Benutzer reduzieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
IA-2(8)	Identifizierung und Authentif izierung (Benutzer im Unternehmen) | Zugriff auf Konten – Wiedergaberesistent	iam-user-mfa-enabled	Aktivieren Sie diese Regel, um den Zugriff auf Ressourcen in der AWS Cloud einzuschr änken. Diese Regel sorgt dafür, dass die Multi-Faktor-Authe ntifizierung (MFA) für alle Benutzer aktiviert ist. MFA sorgt für eine weitere Schutzebe ne zusätzlich zu den Anmeldeinformation en. Reduzieren Sie Fälle von kompromit tierten Konten, indem Sie MFA für Benutzer vorschreiben.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
IA-2(8)	Identifizierung und Authentif izierung (Benutzer im Unternehmen) | Zugriff auf Konten – Wiedergaberesistent	mfa-enabled-for-iam-Konsolenzugriff	Verwalten Sie den Zugriff auf Ressource n in der AWS Cloud, indem Sie sicherste llen, dass MFA für alle AWS Identity and Access Managemen t (IAM) -Benutzer aktiviert ist, die über ein Konsolenk ennwort verfügen. MFA sorgt für eine weitere Schutzebe ne zusätzlich zu den Anmeldeinformation en. Indem Sie MFA für Benutzer vorschrei ben, können Sie Fälle kompromittierter Konten reduzieren und verhindern, dass unbefugte Benutzer auf vertrauliche Daten zugreifen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
IA-2(8)	Identifizierung und Authentifizierung (Benutzer im Unternehmen) | Zugriff auf Konten – Wiedergaberesistent	root-account-hardware-mfa-aktiviert	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Hardware-MFA für den Root-Benutzer aktiviert ist. Der Stammbenutzer ist der AWS-Konto-Benutzer mit den meisten Berechtigungen. MFA sorgt für eine weitere Schutzebene zusätzlich zu den Anmeldeinformationen. Indem Sie MFA für den Root-Benutzer vorschreiben, können Sie die Anzahl AWS-Konten kompromittierter Benutzer reduzieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
IA-2(8)	Identifizierung und Authentifizierung (Benutzer im Unternehmen) | Zugriff auf Konten – Wiedergaberesistent	root-account-mfa-enabled	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass MFA für den Root-Benutzer aktiviert ist. Der Stammbenutzer ist der AWS-Konto-Benutzer mit den meisten Berechtigungen. MFA sorgt für eine weitere Schutzebene zusätzlich zu den Anmeldeinformationen. Indem Sie MFA für den Root-Benutzer vorschreiben, können Sie die Anzahl AWS-Konten kompromittierter Benutzer reduzieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
IA-5(1)	Authenticator-Management | Passwortbasierte Authentifizierung	elb-tls-https-listeners-nur	Stellen Sie sicher, dass Ihre Elastic Load Balancer (ELBs) mit SSL- oder HTTPS-Listenern konfiguriert sind. Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.
IA-5(1)	Authenticator-Management | Passwortbasierte Authentifizierung	opensearch-https-required	Da sensible Daten existieren können und um Daten während der Übertragung zu schützen, sollten Sie sicherstellen, dass HTTPS für Verbindungen zu Ihren Amazon OpenSearch Service-Domains aktiviert ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
IA-5(1)	Authenticator-Management | Passwortbasierte Authentifizierung	alb-http-to-https-Umleitungsprüfung	Um Daten während der Übertragung zu schützen, stellen Sie sicher, dass Ihr Application Load Balancer unverschlüsselte HTTP-Anfragen automatisch an HTTPS umleitet. Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.
IA-5(1)	Authenticator-Management | Passwortbasierte Authentifizierung	api-gw-ssl-enabled	Stellen Sie sicher, dass die REST-API-Stufen von Amazon API Gateway mit SSL-Zertifikaten konfiguriert sind, damit Backend-Systeme überprüfen können, ob Anforderungen von API Gateway stammen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
IA-5(1)	Authenticator-Management | Passwortbasierte Authentifizierung	elb-acm-certificate-required	Zum Schutz von eventuell vorhandenen sensiblen Daten sowie von Daten während der Übertragung muss die Verschlüsselung für Ihr Elastic Load Balancing aktiviert sein. Verwenden Sie AWS Certificate Manager, um öffentliche und private SSL/TLS-Zertifikate mit AWS Diensten und internen Ressourcen zu verwalten, bereitzustellen und bereitzustellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
IA-5(1)	Authenticator-Management | Passwortbasierte Authentifizierung	elbv2- acm-certificate-required	Zum Schutz von eventuell vorhandenen sensiblen Daten sowie von Daten während der Übertragung muss die Verschlüsselung für Ihr Elastic Load Balancing aktiviert sein. Verwenden Sie AWS Certificate Manager, um öffentliche und private SSL/TLS-Zertifikate mit AWS Diensten und internen Ressourcen zu verwalten, bereitzustellen und bereitzustellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
IA-5(1)	Authenticator-Management | Passwortbasierte Authentifizierung	iam-password-policy	Die Identitäten und Anmeldeinformationen werden auf der Grundlage einer organisatorischen IAM-Passwortrichtlinie ausgestellt, verwaltet und verifiziert. Sie erfüllen oder übertreffen die Anforderungen von NIST SP 800-63 und dem Standard „Best Practices“ von AWS Foundational Security für die Passwortstärke. Mit dieser Regel können Sie optional RequireUppercaseCharacters (Wert für AWS grundlegende Sicherheitsbewährte Methoden: wahr), RequireLowercaseCharacters (Wert für bewährte Methoden für AWS grundlegende Sicherheit: wahr), RequireSymbols (Wert für bewährte Methoden für AWS grundlegende Sicherheit:

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			wahr), RequireNumbers (Wert für bewährte Methoden für AWS grundlegende Sicherheit: wahr), MinimumPasswordLength (Wert für bewährte Methoden für AWS grundlegende Sicherheit: 14), PasswordReusePrevention (Wert für bewährte Methoden für AWS grundlegende Sicherheit: 24) und MaxPasswordAge (Wert für bewährte Methoden für AWS grundlegende Sicherheit: 90) für Ihr IAM festlegen Kennwortrichtlinie. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
IA-5(1)	Authenticator-Management | Passwortbasierte Authentifizierung	s-3 bucket-ssl-requests-only	Um Daten während der Übertragung zu schützen, stellen Sie sicher, dass Ihre Amazon Simple Storage Service (Amazon S3)-Buckets Anfragen zur Verwendung von Secure Socket Layer (SSL)-Buckets erfordern. Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
IA-5(7)	Authenticator-Management | Keine eingebetteten unverschlüsselten statischen Authentifikatoren	codebuild-project-envvar-awscred-überprüfen	Stellen Sie sicher, dass die Anmeldeinformationen AWS_ACCESS_KEY_ID AWS_SECRET_ACCESS_KEY nicht in AWS Codebuild-Projektumgebungen vorhanden sind. Speichern Sie diese Variablen nicht als Klartext. Das Speichern dieser Variablen als Klartext bewirkt eine unbeabsichtigte Offenlegung von Daten sowie unberechtigte Zugriffe.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
IR-4(1)	Bearbeitung von Vorfällen | Automatisierte Prozesse zur Bearbeitung von Vorfällen	cloudwatch-alarm-action-check	Amazon CloudWatch alarmiert, wenn eine Metrik den Schwellenwert für eine bestimmte Anzahl von Bewertungszeiträumen überschreitet. Der Alarm führt eine oder mehrere Aktionen durch, die vom Wert der Metrik oder des Ausdrucks im Vergleich zu einem Schwellenwert in einer Reihe von Zeiträumen abhängt. Diese Regel erfordert einen Wert für alarmActionRequired (Config Default: True), insufficientDataAction Required (Config Default: True), okActionRequired (Config Default: False). Der tatsächliche Wert muss die Alarmaktionen für Ihre Umgebung widerspiegeln.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
IR-4(5)	Bearbeitung von Vorfällen | Automatische Systemdeaktivierung	cloudwatch-alarm-action-check	Amazon CloudWatch alarmiert, wenn eine Metrik den Schwellenwert für eine bestimmte Anzahl von Bewertungszeiträumen überschreitet. Der Alarm führt eine oder mehrere Aktionen durch, die vom Wert der Metrik oder des Ausdrucks im Vergleich zu einem Schwellenwert in einer Reihe von Zeiträumen abhängt. Diese Regel erfordert einen Wert für alarmActionRequired (Config Default: True), insufficientDataAction Required (Config Default: True), okActionRequired (Config Default: False). Der tatsächliche Wert muss die Alarmaktionen für Ihre Umgebung widerspiegeln.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
RA-3(4)	Risikobewertung | Prädiktive Cyberanalysen	guardduty-enabled-centralized	Amazon GuardDuty kann mithilfe von Threat Intelligence Feeds helfen, potenzielle Cybersicherheitsereignisse zu überwachen und zu erkennen. Dazu gehören Listen mit bösartigen IPs und maschinellen Lernmethoden zur Identifizierung unerwarteter, nicht autorisierter und bösartiger Aktivitäten in Ihrer AWS Cloud-Umgebung.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SA-3	Lebenszyklus der Systementwicklung	codebuild-project-envvar-awscred-überprüfen	Stellen Sie sicher, dass die Anmeldeinformationen AWS_ACCESS_KEY_ID AWS_SECRET_ACCESS_KEY nicht in AWS Codebuild-Projektumgebungen vorhanden sind. Speichern Sie diese Variablen nicht als Klartext. Das Speichern dieser Variablen als Klartext bewirkt eine unbeabsichtigte Offenlegung von Daten sowie unberechtigte Zugriffe.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SA-3	Lebenszyklus der Systementwicklung	ec2-manager instance-managed-by-systems	Eine Bestandsaufnahme der Softwareplattformen und Anwendungen innerhalb des Unternehmens ist möglich, indem Amazon Elastic Compute Cloud (Amazon EC2) - Instances mit AWS Systems Manager verwaltet werden. Verwenden Sie AWS Systems Manager, um detaillierte Systemkonfigurationen, Betriebssystem-Patch-Levels, Namen und Typ der Dienste, Softwareinstallationen, Anwendungsname, Herausgeber und Version sowie andere Details zu Ihrer Umgebung bereitzustellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SA-8(19)	Prinzipien der Sicherheits- und Datenschutzentwicklung | Kontinuierlicher Schutz	guardduty-enabled-centralized	Amazon GuardDuty kann mithilfe von Threat Intelligence Feeds helfen, potenzielle Cybersicherheitsereignisse zu überwachen und zu erkennen. Dazu gehören Listen mit bösartigen IPs und maschinellen Lernmethoden zur Identifizierung unerwarteter, nicht autorisierter und bösartiger Aktivitäten in Ihrer AWS Cloud-Umgebung.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SA-8(21)	Prinzipien der Sicherheits- und Datenschutzentwicklung | Selbstanalyse	guardduty-enabled-centralized	Amazon GuardDuty kann mithilfe von Threat Intelligence Feeds helfen, potenzielle Cybersicherheitsereignisse zu überwachen und zu erkennen. Dazu gehören Listen mit bösartigen IPs und maschinellen Lernmethoden zur Identifizierung unerwarteter, nicht autorisierter und bösartiger Aktivitäten in Ihrer AWS Cloud-Umgebung.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SA-8(22)	Prinzipien der Sicherheits- und Datenschutzentwicklung | Rechenschaftspflicht und Rückverfolgbarkeit	cloudtrail-enabled	AWS CloudTrail kann durch die Aufzeichnung von Aktionen und API-Aufrufen in der AWS Management Console dazu beitragen, dass die Daten nicht zurückgewiesen werden können. Sie können die Benutzer und die Benutzer AWS-Konten , die einen AWS Dienst aufgerufen haben, die Quell-IP-Adresse, über die die Aufrufe generiert wurden, und den Zeitpunkt der Anrufe identifizieren. Einzelheiten zu den erfassten Daten finden Sie in den AWS CloudTrail Datensatzinhalten.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SA-8(25)	Prinzipien der Sicherheits- und Datenschutzentwicklung | Wirtschaftliche Sicherheit	guardduty-enabled-centralized	Amazon GuardDuty kann mithilfe von Threat Intelligence Feeds helfen, potenzielle Cybersicherheitsereignisse zu überwachen und zu erkennen. Dazu gehören Listen mit bösartigen IPs und maschinellen Lernmethoden zur Identifizierung unerwarteter, nicht autorisierter und bösartiger Aktivitäten in Ihrer AWS Cloud-Umgebung.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SA-11(1)	Tests und Bewertungen für Entwickler | Analyse statischer Codes	guardduty-enabled-centralized	Amazon GuardDuty kann mithilfe von Threat Intelligence Feeds helfen, potenzielle Cybersicherheitsereignisse zu überwachen und zu erkennen. Dazu gehören Listen mit bösartigen IPs und maschinellen Lernmethoden zur Identifizierung unerwarteter, nicht autorisierter und bösartiger Aktivitäten in Ihrer AWS Cloud-Umgebung.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SA-11(6)	Tests und Bewertungen für Entwickler | Überprüfungen der Angriffsfläche	guardduty-enabled-centralized	Amazon GuardDuty kann mithilfe von Threat Intelligence Feeds helfen, potenzielle Cybersicherheitsereignisse zu überwachen und zu erkennen. Dazu gehören Listen mit bösartigen IPs und maschinellen Lernmethoden zur Identifizierung unerwarteter, nicht autorisierter und bösartiger Aktivitäten in Ihrer AWS Cloud-Umgebung.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SA-15(2)	Entwicklungsprozess, Standards und Tools | Tools zur Überwachung von Sicherheit und Datenschutz	ec2-manager instance-managed-by-systems	Eine Bestandsaufnahme der Softwareplattformen und Anwendungen innerhalb des Unternehmens ist möglich, indem Amazon Elastic Compute Cloud (Amazon EC2) - Instances mit AWS Systems Manager verwaltet werden. Verwenden Sie AWS Systems Manager, um detaillierte Systemkonfigurationen, Betriebssystem-Patch-Levels, Namen und Typ der Dienste, Softwareinstallationen, Anwendungsname, Herausgeber und Version sowie andere Details zu Ihrer Umgebung bereitzustellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SA-15(2)	Entwicklungsprozess, Standards und Tools | Tools zur Überwachung von Sicherheit und Datenschutz	guardduty-enabled-centralized	Amazon GuardDuty kann mithilfe von Threat Intelligence Feeds helfen, potenzielle Cybersicherheitsereignisse zu überwachen und zu erkennen. Dazu gehören Listen mit bösartigen IPs und maschinellen Lernmethoden zur Identifizierung unerwarteter, nicht autorisierter und bösartiger Aktivitäten in Ihrer AWS Cloud-Umgebung.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SA-15(8)	Entwicklungsprozess, Standards und Tools | Wiederverwendung von Informationen zu Bedrohungen und Schwachstellen	ec2-manager instance-managed-by-systems	Eine Bestandsaufnahme der Softwareplattformen und Anwendungen innerhalb des Unternehmens ist möglich, indem Amazon Elastic Compute Cloud (Amazon EC2) - Instances mit AWS Systems Manager verwaltet werden. Verwenden Sie AWS Systems Manager, um detaillierte Systemkonfigurationen, Betriebssystem-Patch-Levels, Namen und Typ der Dienste, Softwareinstallationen, Anwendungsname, Herausgeber und Version sowie andere Details zu Ihrer Umgebung bereitzustellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SA-15(8)	Entwicklungsprozess, Standards und Tools | Wiederverwendung von Informationen zu Bedrohungen und Schwachstellen	guardduty-enabled-centralized	Amazon GuardDuty kann mithilfe von Threat Intellige nce Feeds helfen, potenzielle Cybersich erheitsereignisse zu überwachen und zu erkennen. Dazu gehören Listen mit bösartigen IPs und maschinel len Lernmethoden zur Identifizierung unerwarteter, nicht autorisierter und bösartiger Aktivitäten in Ihrer AWS Cloud-Umgebung.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-5(1)	Denial-of-service Schutz | Beschränken Sie die Fähigkeit, andere Systeme anzugreifen	guardduty-enabled-centralized	Amazon GuardDuty kann mithilfe von Threat Intelligence Feeds helfen, potenzielle Cybersicherheitsereignisse zu überwachen und zu erkennen. Dazu gehören Listen mit bösartigen IPs und maschinellen Lernmethoden zur Identifizierung unerwarteter, nicht autorisierter und bösartiger Aktivitäten in Ihrer AWS Cloud-Umgebung.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-5(2)	Denial-of-service Schutz | Kapazität, Bandbreite und Redundanz	dynamodb-in-backup-plan	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon DynamoDB-Tabellen Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-5(2)	Denial-of-service Schutz | Kapazität , Bandbreite und Redundanz	ebs-in-backup-plan	Stellen Sie zur Unterstützung der Datensicherungspro zesse sicher, dass Ihre Amazon Elastic Block Store (Amazon EBS) -Volumes Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwaltet er Backup-Service mit einer richtlini enbasierten Backup-Lösung. Diese Lösung vereinfac ht Ihr Sicherung smanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforde rungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-5(2)	Denial-of-service Schutz | Kapazität , Bandbreite und Redundanz	efs-in-backup-plan	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon Elastic File System (Amazon EFS) -Dateisysteme Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-5(2)	Denial-of-service Schutz | Kapazität , Bandbreite und Redundanz	elb-cross-zone-load-Balancing aktiviert	Aktivieren Sie zonenübergreifendes Load Balancing für Ihre Elastic Load Balancer (ELBs), um eine angemessene Kapazität und Verfügbarkeit aufrechtzuerhalten. Zonenübergreifendes Load Balancing reduziert die Notwendigkeit, die gleiche Anzahl von Instances in jeder aktivierten Availability Zone aufrechtzuerhalten. Es verbessert auch die Fähigkeit Ihrer Anwendung, den Verlust einer oder mehrerer Instances zu bewältigen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-5(2)	Denial-of-service Schutz | Kapazität , Bandbreite und Redundanz	rds-instance-deletion-protection-aktiviert	Stellen Sie sicher, dass Amazon Relational Database Service (Amazon RDS)-Instances den Löschschutz aktiviert haben. Verwenden Sie den Löschschu tz, um zu verhindern, dass Ihre Amazon-RD S-Instances versehent lich oder böswillig gelöscht werden, was zum Verlust der Verfügbarkeit Ihrer Anwendungen führen kann.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-5(2)	Denial-of-service Schutz | Kapazität, Bandbreite und Redundanz	redshift-backup-enabled	Stellen Sie zur Unterstützung der Datensicherungsprozesse sicher, dass Ihre Amazon-Redshift-Cluster über automatisierte Snapshots verfügen. Wenn automatisierte Snapshots für einen Cluster aktiviert sind, erstellt Redshift in regelmäßigen Abständen Snapshots dieses Clusters. Standardmäßig erstellt Redshift alle acht Stunden oder alle 5 GB einen Snapshot für jeden Knoten mit Datenänderungen oder je nachdem, was zuerst eintritt.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-5(2)	Denial-of-service Schutz | Kapazität , Bandbreite und Redundanz	s-3 version-lifecycle-policy-check	Mit Amazon-S3-Lebenszyklusregeln können Sie Aktionen definieren, die Amazon S3 während der Lebensdau er eines Objekts ausführen soll (z. B. die Überfüh rung von Objekten in eine andere Speicherklasse, ihre Archivierung oder Löschung nach einem bestimmten Zeitraum) .

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-5(2)	Denial-of-service Schutz | Kapazität , Bandbreite und Redundanz	db-instance-backup-enabled	Die Sicherung sfunktion von Amazon RDS erstellt Sicherung en Ihrer Datenbank en und Transakti onsprotokolle. Amazon RDS erstellt einen Snapshot für das Speichervolume Ihrer DB-Instance, sodass die gesamte DB-Instance gesichert wird. Sie können im System spezifische Aufbewahrungsfrist en festlegen, um Ihre Ausfallsicherheits anforderungen zu erfüllen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-5(2)	Denial-of-service Schutz | Kapazität , Bandbreite und Redundanz	dynamodb-autoscaling-enabled	Amazon DynamoDB Auto Scaling verwendet den AWS Application Auto Scaling-Service, um die bereitgestellte Durchsatzkapazität so anzupassen, dass sie automatisch auf tatsächliche Verkehrsmuster reagiert. Auf diese Weise kann eine Tabelle oder ein globaler sekundärer Index die bereitgestellte Lese-/Schreibkapazität erhöhen, um plötzliche Erhöhungen des Datenverkehrs ohne Drosselung zu bewältigen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-5(2)	Denial-of-service Schutz | Kapazität, Bandbreite und Redundanz	dynamodb-pitr-enabled	Aktivieren Sie diese Regel, um zu überprüfen, ob die Informationen gesichert wurden. Es verwaltet auch die Backups, indem es sicherstellt, dass die point-in-time Wiederherstellung in Amazon DynamoDB aktiviert ist. Bei der Wiederherstellung werden fortlaufende Backups Ihrer Tabelle für die letzten 35 Tage gespeichert.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-5(2)	Denial-of-service Schutz | Kapazität, Bandbreite und Redundanz	ebs-optimized-instance	Eine optimierte Instance im Amazon Elastic Block Store (Amazon EBS) bietet zusätzliche, dedizierte Kapazität für Amazon-EBS-I/O-Vorgänge. Diese Optimierung bietet die beste Leistung für Ihr EBS-Volume, indem Konflikte zwischen Amazon-EBS-I/O und anderem Datenverkehr von Ihrer Instance minimiert werden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-5(2)	Denial-of-service Schutz | Kapazität , Bandbreite und Redundanz	elasticache-redis-cluster-automatic-Backup-Check	Wenn automatische Backups aktiviert sind, ElastiCache erstellt Amazon täglich ein Backup des Clusters. Die Sicherung kann für eine von Ihrer Organisation festgelegte Anzahl von Tagen aufbewahrt werden. Automatische Backups schützen vor Datenverlust. Bei einem Ausfall können Sie einen neuen Cluster erstellen, der Ihre Daten aus dem aktuellen Backup wiederherstellt.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-5(2)	Denial-of-service Schutz | Kapazität, Bandbreite und Redundanz	elb-deletion-protection-enabled	Diese Regel sorgt dafür, dass der Löschschutz für Elastic Load Balancing aktiviert ist. Verwenden Sie diese Funktion, um zu verhindern, dass Ihr Load Balancer versehentlich oder böswillig gelöscht wird, was zum Verlust der Verfügbarkeit Ihrer Anwendungen führen kann.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-5(2)	Denial-of-service Schutz | Kapazität, Bandbreite und Redundanz	rds-multi-az-support	Die Multi-AZ-Unterstützung in Amazon Relational Database Service (Amazon RDS) bietet eine verbesserte Verfügbarkeit und Beständigkeit von Datenbank-Instances. Wenn Sie eine Multi-AZ-Datenbank-Instance bereitstellen, erstellt Amazon RDS automatisch eine primäre Datenbank-Instance und repliziert die Daten synchron auf eine Standby-Instance in einer anderen Availability Zone. Jede Availability Zone läuft auf einer eigenen, physisch getrennten, unabhängigen Infrastruktur und ist auf eine hohe Verfügbarkeit ausgelegt. Im Falle eines Infrastrukturausfalls führt Amazon RDS einen automatis

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			chen Failover zum Standby-Modus durch, sodass Sie den Datenbankbetrieb wieder aufnehmen können, sobald der Failover abgeschlo ssen ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-5(2)	Denial-of-service Schutz | Kapazität, Bandbreite und Redundanz	redshift-cluster-maintenancesettings-check	Diese Regel stellt sicher, dass Amazon-Redshift-Cluster die bevorzugten Einstellungen für Ihre Organisation haben. Insbesondere sorgt sie dafür, dass Cluster bevorzugte Wartungsfenster und automatisierte Aufbewahrungsfristen für Snapshots für die Datenbank haben. Für diese Regel müssen Sie die allowVersionUpgrade festlegen. Der Standardwert ist „true“. Außerdem können Sie optional den Zeitraum preferredMaintenanceWindow (der Standardwert ist sa: 16:00 -sa: 16:30) und den automated SnapshotRetention Zeitraum (der Standardwert ist 1) festlegen. Die tatsächlichen Werte müssen den Richtlini

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			en Ihrer Organisation entsprechen.
SC-5(2)	Denial-of-service Schutz | Kapazität , Bandbreite und Redundanz	s-3 bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) unterstützt die Aufrechterhaltung einer angemesse nen Kapazität und Verfügbarkeit. CRR ermöglicht das automatische, asynchrone Kopieren von Objekten in Amazon-S3-Buckets, um die Datenverf ügbarkeit sicherzus tellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-5(2)	Denial-of-service Schutz | Kapazität, Bandbreite und Redundanz	s-3 bucket-versioning-enabled	Die Versionsverwaltung von Amazon Simple Storage Service (Amazon S3)-Buckets hilft dabei, mehrere Varianten eines Objekts im selben Amazon-S3-Bucket zu speichern. Verwenden Sie die Versionsverwaltung, um sämtliche Versionen aller Objekte in Ihrem Amazon-S3-Bucket zu speichern, abzurufen oder wiederherzustellen. Mit der Versionsverwaltung können Sie Versionen sowohl nach unbeabsichtigten Benutzeraktionen als auch nach Anwendungsfehlern problemlos wiederherstellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-5(2)	Denial-of-service Schutz | Kapazität , Bandbreite und Redundanz	vpc-vpn-2-tunnels-up	Redundante Site-to-Site VPN-Tunnel können implementiert werden, um die Anforderungen an die Ausfallsicherheit zu erfüllen. Es verwendet zwei Tunnel, um die Konnektivität sicherzustellen, falls eine der Site-to-Site VPN-Verbindungen nicht verfügbar ist. Um sich vor einem Verbindungsverlust zu schützen, können Sie für den Fall, dass Ihr Kunden-Gateway nicht verfügbar ist, eine zweite Site-to-Site VPN-Verbindung zu Ihrer Amazon Virtual Private Cloud (Amazon VPC) und Ihrem Virtual Private Gateway einrichten, indem Sie ein zweites Kunden-Gateway verwenden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-5(3)	Denial-of-service Schutz | Erkennung und Überwachung	guardduty-enabled-centralized	Amazon GuardDuty kann mithilfe von Threat Intellige nce Feeds helfen, potenzielle Cybersich erheitsereignisse zu überwachen und zu erkennen. Dazu gehören Listen mit bösartigen IPs und maschinel len Lernmethoden zur Identifizierung unerwarteter, nicht autorisierter und bösartiger Aktivitäten in Ihrer AWS Cloud-Umgebung.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-5	Denial-of-service Schutz	guardduty-enabled-centralized	Amazon GuardDuty kann mithilfe von Threat Intellige nce Feeds helfen, potenzielle Cybersich erheitsereignisse zu überwachen und zu erkennen. Dazu gehören Listen mit bösartigen IPs und maschinel len Lernmethoden zur Identifizierung unerwarteter, nicht autorisierter und bösartiger Aktivitäten in Ihrer AWS Cloud-Umgebung.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-7(3)	Grenzschutz | Zugangspunkte	autoscaling-launch-config-public-ip-deaktiviert	Wenn Sie Ihre Netzwerkschnittstellen mit einer öffentlichen IP-Adresse konfigurieren, sind die diesen Netzwerkschnittstellen zugehörigen Ressourcen über das Internet erreichbar. EC2 Ressourcen sollten nicht öffentlich zugänglich sein, da dies einen unbeabsichtigten Zugriff auf Ihre Anwendungen oder Server ermöglichen kann.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-7(3)	Grenzschutz | Zugangspunkte	ec2- instances-in-vpc	Stellen Sie Amazon Elastic Compute Cloud (Amazon EC2) -Instances innerhalb einer Amazon Virtual Private Cloud (Amazon VPC) bereit, um eine sichere Kommunika tion zwischen einer Instance und anderen Services innerhalb der Amazon VPC zu ermöglichen, ohne dass ein Internet-Gateway, ein NAT-Gerät oder eine VPN-Verbindung erforderlich ist. Der gesamte Datenverk ehr bleibt sicher in der AWS Cloud. Domains, die sich innerhalb einer VPC befinden, verfügen aufgrund ihrer logischen Isolierun g im Vergleich zu Domains mit öffentlic hen Endpunkten über eine zusätzlic he Sicherheitsebene. Weisen Sie EC2

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			Amazon-Instances einer Amazon-VPC zu, um den Zugriff ordnungsgemäß zu verwalten.
SC-7(3)	Grenzschutz | Zugangspunkte	ssm-document-not-public	Stellen Sie sicher, dass AWS Systems Manager (SSM) - Dokumente nicht öffentlich sind, da dies einen unbeabsichtigten Zugriff auf Ihre SSM-Dokumente ermöglichen kann. Ein öffentliches SSM-Dokument kann Informationen über Ihr Konto, Ihre Ressourcen und internen Prozesse preisgeben.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-7(3)	Grenzschutz | Zugangspunkte	dms-replication-not-public	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass auf DMS-Replikationsin stanzen nicht öffentlic h zugegriffen werden kann. DMS-Repli kations-Instances können vertrauli che Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.
SC-7(3)	Grenzschutz | Zugangspunkte	ebs-snapshot-public-restorable-überprüfen	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass EBS-Snapshots nicht öffentlich wiederher stellbar sind. EBS-Volume-Snapsho ts können vertrauli che Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-7(3)	Grenzschutz | Zugangspunkte	ec-2 instance-no-public-ip	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon Elastic Compute Cloud (Amazon EC2) - Instances nicht öffentlich zugänglich sind. EC2 Amazon-Instances können vertrauliche Informationen enthalten, und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-7(3)	Grenzschutz | Zugangspunkte	elasticsearch-in-vpc-only	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass sich Amazon OpenSearch OpenSearch Service (Service) - Domains innerhalb einer Amazon Virtual Private Cloud (Amazon VPC) befinden. Eine OpenSearch Service-Domain innerhalb einer Amazon VPC ermöglicht die sichere Kommunikation zwischen OpenSearch Service und anderen Services innerhalb der Amazon VPC, ohne dass ein Internet-Gateway, ein NAT-Gerät oder eine VPN-Verbindung erforderlich ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-7(3)	Grenzschutz | Zugangspunkte	emr-master-no-public-ip	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon EMR-Cluster-Masterknoten nicht öffentlich zugänglich sind. Amazon-EMR-Cluster-Hauptknoten können vertrauliche Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.
SC-7(3)	Grenzschutz | Zugangspunkte	lambda-function-public-access-verboten	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass AWS Lambda-Funktionen nicht öffentlich zugänglich sind. Der öffentliche Zugriff kann möglicherweise die Verfügbarkeit von Ressourcen beeinträchtigen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-7(3)	Grenzschutz | Zugangspunkte	lambda-inside-vpc	Stellen Sie AWS Lambda-Funktionen in einer Amazon Virtual Private Cloud (Amazon VPC) bereit, um eine sichere Kommunika tion zwischen einer Funktion und anderen Diensten innerhalb der Amazon VPC zu gewährleisten. Bei dieser Konfiguration sind kein Internet-Gateway, kein NAT-Gerät und keine VPN-Verbindung erforderlich. Der gesamte Datenverk ehr bleibt sicher in der Cloud. AWS Domains, die sich innerhalb einer VPC befinden, verfügen aufgrund ihrer logischen Isolierun g im Vergleich zu Domains mit öffentlic hen Endpunkten über eine zusätzliche Sicherheitsebene. Um den Zugriff ordnungsg emäß zu verwalten,

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			sollten AWS Lambda-Funktionen einer VPC zugewiesen werden.
SC-7(3)	Grenzschutz | Zugangspunkte	opensearch-in-vpc-only	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass sich Amazon OpenSearch Service-Domains innerhalb einer Amazon Virtual Private Cloud (Amazon VPC) befinden. Eine Amazon OpenSearch Service-Domain innerhalb einer Amazon VPC ermöglicht die sichere Kommunikation zwischen Amazon OpenSearch Service und anderen Services innerhalb der Amazon VPC, ohne dass ein Internet-Gateway, ein NAT-Gerät oder eine VPN-Verbindung erforderlich ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-7(3)	Grenzschutz | Zugangspunkte	rds-instance-public-access-überprüfen	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Relational Database Service (Amazon RDS) -Instances nicht öffentlich sind. Amazon-RDS-Datenbank-Instances können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-7(3)	Grenzschutz | Zugangspunkte	rds-snapshots-public-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Relational Database Service (Amazon RDS) -Instances nicht öffentlich sind. Amazon-RDS-Datenbank-Instances können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-7(3)	Grenzschutz | Zugangspunkte	redshift-cluster-public-access-überprüfen	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Redshift Redshift-Cluster nicht öffentlich sind. Amazon-Redshift-Cluster können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-7(3)	Grenzschutz | Zugangspunkte	s3- -Block-periodisch account-level-public-access	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Simple Storage Service (Amazon S3) -Buckets nicht öffentlich zugänglich sind. Diese Regel trägt dazu bei, sensible Daten vor unbefugten Remote-Benutzern zu schützen, indem sie den öffentlichen Zugriff verhindert. Mit dieser Regel können Sie optional die Parameter ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) und restrictPublicBuckets Parameter (Config Default: True) festlegen. Die tatsächlichen Werte müssen den Richtlini

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			en Ihrer Organisation entsprechen.
SC-7(3)	Grenzschutz | Zugangspunkte	s3 bucket-level-public-access - verboten	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Simple Storage Service (Amazon S3) -Buckets nicht öffentlich zugänglich sind. Diese Regel trägt dazu bei, sensible Daten vor unbefugten Remote-Benutzern zu schützen, indem sie den öffentlichen Zugriff auf Bucket-Ebene verhindert.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-7(3)	Grenzschutz | Zugangspunkte	s-3 bucket-public-read -prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie nur autorisierten Benutzern, Prozessen und Geräten Zugriff auf Amazon Simple Storage Service (Amazon S3) - Buckets gewähren. Die Verwaltung des Zugriffs sollte mit der Klassifizierung der Daten übereinst immen.
SC-7(3)	Grenzschutz | Zugangspunkte	s3- bucket-public-writ e-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie nur autorisierten Benutzern, Prozessen und Geräten Zugriff auf Amazon Simple Storage Service (Amazon S3) - Buckets gewähren. Die Verwaltung des Zugriffs sollte mit der Klassifizierung der Daten übereinst immen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-7(3)	Grenzschutz | Zugangspunkte	sagemaker-notebook-no-direct-Internetzugang	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass SageMaker Amazon-Notebooks keinen direkten Internetzugang zulassen. Indem Sie direkten Internetzugang blockieren, vermeiden Sie, dass unbefugte Benutzer auf sensible Daten zugreifen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-7(3)	Grenzschutz | Zugangspunkte	subnet-auto-assign-public-ip-deaktiviert	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon Virtual Private Cloud (VPC) -Subnetzen nicht automatisch eine öffentliche IP-Adresse zugewiesen wird. Amazon Elastic Compute Cloud (EC2) -Instances, die in Subnetzen gestartet werden, in denen dieses Attribut aktiviert ist, haben ihrer primären Netzwerkschnittstelle eine öffentliche IP-Adresse zugewiesen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-7(4)	Grenzschutz | Externe Telekommunikations services	autoscaling-launch-config-public-ip-deaktiviert	Wenn Sie Ihre Netzwerkschnittstellen mit einer öffentlichen IP-Adresse konfigurieren, sind die diesen Netzwerkschnittstellen zugehörigen Ressourcen über das Internet erreichbar. EC2 Ressourcen sollten nicht öffentlich zugänglich sein, da dies einen unbeabsichtigten Zugriff auf Ihre Anwendungen oder Server ermöglichen kann.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-7(4)	Grenzschutz | Externe Telekommunikations services	elasticsearch-node-to-node-Verschlüsselungsprüfung	Stellen Sie sicher, dass die node-to-node Verschlüsselung für Amazon OpenSearch Service aktiviert ist. Node-to-nodeVerschlüsselung ermöglicht die TLS 1.2-Verschlüsselung für die gesamte Kommunikation innerhalb der Amazon Virtual Private Cloud (Amazon VPC). Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.
SC-7(4)	Grenzschutz | Externe Telekommunikations services	elb-tls-https-listeners-nur	Stellen Sie sicher, dass Ihre Elastic Load Balancer (ELBs) mit SSL- oder HTTPS-Listenern konfiguriert sind. Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-7(4)	Grenzschutz | Externe Telekommunikations services	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) Security Groups können bei der Verwaltung des Netzwerkzugriffs helfen, indem sie eine statusbeh aftete Filterung von eingehendem und ausgehendem Netzwerkverkehr zu Ressourcen bereitste llen. AWS Wenn Sie eingehenden (oder entfernten) Datenverk ehr von 0.0.0.0/0 bis Port 22 auf Ihren Ressourcen nicht zulassen, können Sie den Remote-Zugriff einschränken.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-7(4)	Grenzschutz | Externe Telekommunikations services	ec2- instances-in-vpc	Stellen Sie Amazon Elastic Compute Cloud (Amazon EC2) -Instances innerhalb einer Amazon Virtual Private Cloud (Amazon VPC) bereit, um eine sichere Kommunika tion zwischen einer Instance und anderen Services innerhalb der Amazon VPC zu ermöglichen, ohne dass ein Internet-Gateway, ein NAT-Gerät oder eine VPN-Verbindung erforderlich ist. Der gesamte Datenverk ehr bleibt sicher in der AWS Cloud. Domains, die sich innerhalb einer VPC befinden, verfügen aufgrund ihrer logischen Isolierun g im Vergleich zu Domains mit öffentlic hen Endpunkten über eine zusätzlic he Sicherheitsebene. Weisen Sie EC2

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			Amazon-Instances einer Amazon-VPC zu, um den Zugriff ordnungsgemäß zu verwalten.
SC-7(4)	Grenzschutz | Externe Telekommunikations services	no-unrestricted-route-to-igw	Stellen Sie sicher, dass EC2 Amazon-Routentabellen keine uneingeschränkten Routen zu einem Internet-Gateway enthalten. Durch das Entfernen oder Beschränken des Internetzugangs für Workloads innerhalb von Amazon VPCs können unbeabsic htigte Zugriffe in Ihrer Umgebung reduziert werden.
SC-7(4)	Grenzschutz | Externe Telekommunikations services	opensearch-https-required	Da sensible Daten existieren können und um Daten während der Übertragung zu schützen, sollten Sie sicherstellen, dass HTTPS für Verbindungen zu Ihren Amazon OpenSearch Service-Domains aktiviert ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-7(4)	Grenzschutz | Externe Telekommunikations services	opensearch-node-to-node-Verschlüsselungsprüfung	Stellen Sie sicher, dass die node-to-node Verschlüsselung für Amazon OpenSearch Service aktiviert ist. Node-to-nodeVerschlüsselung ermöglicht die TLS 1.2-Verschlüsselung für die gesamte Kommunikation innerhalb der Amazon Virtual Private Cloud (Amazon VPC). Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-7(4)	Grenzschutz | Externe Telekommunikations services	redshift-enhanced-vpc-routing-aktiviert	Mit Enhanced-VPC-Routing wird erzwungen, dass der gesamte COPY- und UNLOAD-Datenverkehr zwischen Ihrem Cluster und Datenrepositorys über Ihre Amazon VPC erfolgt. Anschließend können Sie VPC-Features wie Sicherheitsgruppen und Netzwerkzugriffskontrolllisten verwenden, um den Netzwerkverkehr zu schützen. Sie können auch VPC-Flow-Protokolle verwenden, um den Netzwerkverkehr zu überwachen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-7(4)	Grenzschutz | Externe Telekommunikations services	ssm-document-not-public	Stellen Sie sicher, dass AWS Systems Manager (SSM) - Dokumente nicht öffentlich sind, da dies einen unbeabsichtigten Zugriff auf Ihre SSM-Dokumente ermöglichen kann. Ein öffentliches SSM-Dokument kann Informationen über Ihr Konto, Ihre Ressourcen und internen Prozesse preisgeben.
SC-7(4)	Grenzschutz | Externe Telekommunikations services	alb-http-to-https-Umleitungsprüfung	Um Daten während der Übertragung zu schützen, stellen Sie sicher, dass Ihr Application Load Balancer unverschlüsselte HTTP-Anfragen automatisch an HTTPS umleitet. Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-7(4)	Grenzschutz | Externe Telekommunikations services	api-gw-ssl-enabled	Stellen Sie sicher, dass die REST-API-Stufen von Amazon API Gateway mit SSL-Zertifikaten konfiguriert sind, damit Backend-Systeme überprüfen können, ob Anforderungen von API Gateway stammen.
SC-7(4)	Grenzschutz | Externe Telekommunikations services	dms-replication-not-public	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass auf DMS-Replikationsinstanzen nicht öffentlich zugegriffen werden kann. DMS-Replikations-Instances können vertrauliche Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-7(4)	Grenzschutz | Externe Telekommunikations services	ebs-snapshot-public-restorable-überprüfen	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass EBS-Snapshots nicht öffentlich wiederher stellbar sind. EBS-Volume-Snapsho ts können vertrauli che Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.
SC-7(4)	Grenzschutz | Externe Telekommunikations services	ec-2 instance-no-public-ip	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon Elastic Compute Cloud (Amazon EC2) - Instances nicht öffentlich zugänglich sind. EC2 Amazon-Instances können vertrauliche Informati onen enthalten, und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-7(4)	Grenzschutz | Externe Telekommunikations services	elasticsearch-in-vpc-only	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass sich Amazon OpenSearch OpenSearch Service (Service) - Domains innerhalb einer Amazon Virtual Private Cloud (Amazon VPC) befinden. Eine OpenSearch Service-Domain innerhalb einer Amazon VPC ermöglicht die sichere Kommunikation zwischen OpenSearch Service und anderen Services innerhalb der Amazon VPC, ohne dass ein Internet-Gateway, ein NAT-Gerät oder eine VPN-Verbindung erforderlich ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-7(4)	Grenzschutz | Externe Telekommunikations services	elb-acm-certificate-required	Zum Schutz von eventuell vorhanden en sensiblen Daten sowie von Daten während der Übertragung muss die Verschlüsselung für Ihr Elastic Load Balancing aktiviert sein. Verwenden Sie AWS Certificate Manager, um öffentlic he und private SSL/ TLS-Zertifikate mit AWS Diensten und internen Ressource n zu verwalten, bereitzustellen und bereitzustellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-7(4)	Grenzschutz | Externe Telekommunikations services	elbv2- acm-certificate-required	Zum Schutz von eventuell vorhanden en sensiblen Daten sowie von Daten während der Übertragung muss die Verschlüsselung für Ihr Elastic Load Balancing aktiviert sein. Verwenden Sie AWS Certificate Manager, um öffentlic he und private SSL/ TLS-Zertifikate mit AWS Diensten und internen Ressource n zu verwalten, bereitzustellen und bereitzustellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-7(4)	Grenzschutz | Externe Telekommunikations services	emr-master-no-public-ip	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon EMR-Cluster-Masterknoten nicht öffentlich zugänglich sind. Amazon-EMR-Cluster-Hauptknoten können vertrauliche Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.
SC-7(4)	Grenzschutz | Externe Telekommunikations services	lambda-function-public-access-verboten	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass AWS Lambda-Funktionen nicht öffentlich zugänglich sind. Der öffentliche Zugriff kann möglicherweise die Verfügbarkeit von Ressourcen beeinträchtigen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-7(4)	Grenzschutz | Externe Telekommunikations services	lambda-inside-vpc	Stellen Sie AWS Lambda-Funktionen in einer Amazon Virtual Private Cloud (Amazon VPC) bereit, um eine sichere Kommunika tion zwischen einer Funktion und anderen Diensten innerhalb der Amazon VPC zu gewährleisten. Bei dieser Konfiguration sind kein Internet-Gateway, kein NAT-Gerät und keine VPN-Verbindung erforderlich. Der gesamte Datenverk ehr bleibt sicher in der Cloud. AWS Domains, die sich innerhalb einer VPC befinden, verfügen aufgrund ihrer logischen Isolierun g im Vergleich zu Domains mit öffentlic hen Endpunkten über eine zusätzliche Sicherheitsebene. Um den Zugriff ordnungsg emäß zu verwalten,

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			sollten AWS Lambda-Funktionen einer VPC zugewiesen werden.
SC-7(4)	Grenzschutz | Externe Telekommunikations services	opensearch-in-vpc-only	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass sich Amazon OpenSearch Service-Domains innerhalb einer Amazon Virtual Private Cloud (Amazon VPC) befinden. Eine Amazon OpenSearch Service-Domain innerhalb einer Amazon VPC ermöglicht die sichere Kommunikation zwischen Amazon OpenSearch Service und anderen Services innerhalb der Amazon VPC, ohne dass ein Internet-Gateway, ein NAT-Gerät oder eine VPN-Verbindung erforderlich ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-7(4)	Grenzschutz | Externe Telekommunikations services	rds-instance-public-access-überprüfen	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Relational Database Service (Amazon RDS) -Instances nicht öffentlich sind. Amazon-RDS-Datenbank-Instances können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-7(4)	Grenzschutz | Externe Telekommunikations services	rds-snapshots-public-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Relational Database Service (Amazon RDS) -Instances nicht öffentlich sind. Amazon-RDS-Datenbank-Instances können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-7(4)	Grenzschutz | Externe Telekommunikations services	redshift-cluster-public-access-überprüfen	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Redshift Redshift-Cluster nicht öffentlich sind. Amazon-Redshift-Cluster können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.
SC-7(4)	Grenzschutz | Externe Telekommunikations services	redshift-require-tls-ssl	Stellen Sie sicher, dass Ihre Amazon-Redshift-Cluster eine TLS/SSL-Verschlüsselung erfordern, um eine Verbindung zu SQL-Clients herzustellen. Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-7(4)	Grenzschutz | Externe Telekommunikations services	restricted-common-ports	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass gemeinsame Ports für Amazon Elastic Compute Cloud (Amazon EC2) -Sicherheitsgruppen eingeschränkt sind. Wenn der Zugriff auf Ports nicht auf vertrauenswürdige Quellen beschränkt wird, kann dies zu Angriffen auf die Verfügbarkeit, Integrität und Vertraulichkeit von Systemen führen. Mit dieser Regel können Sie optional die Parameter blockedPort1–blockedPort5 festlegen (Standardkonfigurationen: 20, 21, 3389, 3306, 4333). Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-7(4)	Grenzschutz | Externe Telekommunikations services	s3- account-level-public-access -Block-periodisch	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Simple Storage Service (Amazon S3) -Buckets nicht öffentlich zugänglich sind. Diese Regel trägt dazu bei, sensible Daten vor unbefugten Remote-Benutzern zu schützen, indem sie den öffentlichen Zugriff verhindert. Mit dieser Regel können Sie optional die Parameter ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) und restrictPublicBuckets Parameter (Config Default: True) festlegen. Die tatsächlichen Werte müssen den Richtlini

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			en Ihrer Organisation entsprechen.
SC-7(4)	Grenzschutz | Externe Telekommunikations services	s3 bucket-level-public-access - verboten	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Simple Storage Service (Amazon S3) -Buckets nicht öffentlich zugänglich sind. Diese Regel trägt dazu bei, sensible Daten vor unbefugten Remote-Benutzern zu schützen, indem sie den öffentlichen Zugriff auf Bucket-Ebene verhindert.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-7(4)	Grenzschutz | Externe Telekommunikations services	s-3 bucket-public-read -prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie nur autorisierten Benutzern, Prozessen und Geräten Zugriff auf Amazon Simple Storage Service (Amazon S3) - Buckets gewähren. Die Verwaltung des Zugriffs sollte mit der Klassifizierung der Daten übereinst immen.
SC-7(4)	Grenzschutz | Externe Telekommunikations services	s3- bucket-public-writ e-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie nur autorisierten Benutzern, Prozessen und Geräten Zugriff auf Amazon Simple Storage Service (Amazon S3) - Buckets gewähren. Die Verwaltung des Zugriffs sollte mit der Klassifizierung der Daten übereinst immen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-7(4)	Grenzschutz | Externe Telekommunikations services	s3- bucket-ssl-requests-only	Um Daten während der Übertragung zu schützen, stellen Sie sicher, dass Ihre Amazon Simple Storage Service (Amazon S3)-Buckets Anfragen zur Verwendung von Secure Socket Layer (SSL)-Buckets erfordern. Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-7(4)	Grenzschutz | Externe Telekommunikations services	sagemaker-notebook-no-direct-Internetzugang	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass SageMaker Amazon-Notebooks keinen direkten Internetzugang zulassen. Indem Sie direkten Internetzugang blockieren, vermeiden Sie, dass unbefugte Benutzer auf sensible Daten zugreifen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-7(4)	Grenzschutz | Externe Telekommunikations services	subnet-auto-assign-public-ip-deaktiviert	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon Virtual Private Cloud (VPC) -Subnetzen nicht automatisch eine öffentliche IP-Adresse zugewiesen wird. Amazon Elastic Compute Cloud (EC2) -Instances, die in Subnetzen gestartet werden, in denen dieses Attribut aktiviert ist, haben ihrer primären Netzwerkschnittstelle eine öffentliche IP-Adresse zugewiesen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-7(4)	Grenzschutz | Externe Telekommunikations services	vpc-default-security-group-geschlossen	Sicherheitsgruppen von Amazon Elastic Compute Cloud (Amazon EC2) können bei der Verwaltung des Netzwerkzugriffs helfen, indem sie eine statusbehaftete Filterung des ein- und ausgehenden Netzwerkverkehrs zu Ressourcen bereitstellen. AWS Die Beschränk ung des gesamten Datenverkehrs auf die Standardsicherheit sgruppe hilft dabei, den Fernzugriff auf Ihre Ressourcen einzuschränken. AWS

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-7(4)	Grenzschutz | Externe Telekommunikations services	vpc-sg-open-only-to-authorized-ports	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass gemeinsame Ports für Amazon Elastic Compute Cloud (Amazon EC2) -Sicherheitsgruppen eingeschränkt sind. Wenn der Zugriff auf Ports nicht auf vertrauenswürdige Quellen beschränkt wird, kann dies zu Angriffen auf die Verfügbarkeit, Integrität und Vertraulichkeit von Systemen führen. Durch die Beschränkung des Zugriffs auf Ressourcen innerhalb einer Sicherheitsgruppe aus dem Internet (0.0.0.0/0) kann der Remote-Zugriff auf interne Systeme gesteuert werden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-7(5)	Grenzschutz | Standardmäßige Zugriffsverweigerung – Ausnahmsweise Genehmigung	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) Security Groups können bei der Verwaltung des Netzwerkzugriffs helfen, indem sie eine statusbehaftete Filterung von eingehendem und ausgehendem Netzwerkverkehr zu Ressourcen bereitstellen. AWS Wenn Sie eingehenden (oder entfernten) Datenverkehr von 0.0.0.0/0 bis Port 22 auf Ihren Ressourcen nicht zulassen, können Sie den Remote-Zugriff einschränken.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-7(5)	Grenzschutz | Standardmäßige Zugriffsverweigerung – Ausnahmsweise Genehmigung	restricted-common-ports	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass gemeinsame Ports für Amazon Elastic Compute Cloud (Amazon EC2) -Sicherheitsgruppen eingeschränkt sind. Wenn der Zugriff auf Ports nicht auf vertrauenswürdige Quellen beschränkt wird, kann dies zu Angriffen auf die Verfügbarkeit, Integrität und Vertraulichkeit von Systemen führen. Mit dieser Regel können Sie optional die Parameter blockedPort1–blockedPort5 festlegen (Standardkonfigurationen: 20, 21, 3389, 3306, 4333). Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-7(5)	Grenzschutz | Standardmäßige Zugriffsverweigerung – Ausnahmsweise Genehmigung	vpc-default-security-group-geschlossen	Sicherheitsgruppen von Amazon Elastic Compute Cloud (Amazon EC2) können bei der Verwaltung des Netzwerkzugriffs helfen, indem sie eine statusbehaftete Filterung des ein- und ausgehenden Netzwerkverkehrs zu Ressourcen bereitstellen. AWS Die Beschränkung des gesamten Datenverkehrs auf die Standardsicherheitsgruppe hilft dabei, den Fernzugriff auf Ihre Ressourcen einzuschränken. AWS

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-7(5)	Grenzschutz | Standardmäßige Zugriffsverweigerung – Ausnahmsweise Genehmigung	vpc-sg-open-only-to-authorized-ports	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass gemeinsame Ports für Amazon Elastic Compute Cloud (Amazon EC2) -Sicherheitsgruppen eingeschränkt sind. Wenn der Zugriff auf Ports nicht auf vertrauenswürdige Quellen beschränkt wird, kann dies zu Angriffen auf die Verfügbarkeit, Integrität und Vertraulichkeit von Systemen führen. Durch die Beschränkung des Zugriffs auf Ressourcen innerhalb einer Sicherheitsgruppe aus dem Internet (0.0.0.0/0) kann der Remote-Zugriff auf interne Systeme gesteuert werden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-7(9)	Grenzschutz | Beschränkung von bedrohlichem ausgehendem Kommunikationsverkehr	autoscaling-launch-config-public-ip-deaktiviert	Wenn Sie Ihre Netzwerkschnittstellen mit einer öffentlichen IP-Adresse konfigurieren, sind die diesen Netzwerkschnittstellen zugehörigen Ressourcen über das Internet erreichbar. EC2 Ressourcen sollten nicht öffentlich zugänglich sein, da dies einen unbeabsichtigten Zugriff auf Ihre Anwendungen oder Server ermöglichen kann.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-7(9)	Grenzschutz | Beschränkung von bedrohlichem ausgehendem Kommunikationsverkehr	elasticsearch-logs-to-cloudwatch	Stellen Sie sicher, dass für Amazon OpenSearch Service-Domains Fehlerprotokolle aktiviert und zur Aufbewahrung und Beantwortung an Amazon CloudWatch Logs gestreamt werden. Domain-Fehlerprotokolle sind bei Sicherheits- und Zugriffsprüfungen sowie bei der Diagnose von Verfügbarkeitsproblemen nützlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-7(9)	Grenzschutz | Beschränkung von bedrohlichem ausgehendem Kommunikationsverkehr	ec2- instances-in-vpc	Stellen Sie Amazon Elastic Compute Cloud (Amazon EC2) -Instances innerhalb einer Amazon Virtual Private Cloud (Amazon VPC) bereit, um eine sichere Kommunikation zwischen einer Instance und anderen Services innerhalb der Amazon VPC zu ermöglichen, ohne dass ein Internet-Gateway, ein NAT-Gerät oder eine VPN-Verbindung erforderlich ist. Der gesamte Datenverkehr bleibt sicher in der AWS Cloud. Domains, die sich innerhalb einer VPC befinden, verfügen aufgrund ihrer logischen Isolierung im Vergleich zu Domains mit öffentlichen Endpunkten über eine zusätzliche Sicherheitsebene. Weisen Sie EC2

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			Amazon-Instances einer Amazon-VPC zu, um den Zugriff ordnungsgemäß zu verwalten.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-7(9)	Grenzschutz | Beschränkung von bedrohlichem ausgehendem Kommunikationsverkehr	multi-region-cloudtrail-enabled	AWS CloudTrail zeichnet Aktionen und API-Aufrufe der AWS Management Console auf. Sie können feststellen, welche Benutzer und Konten angerufen wurden AWS, von welcher Quell-IP-Adresse aus die Anrufe getätigt wurden und wann die Anrufe erfolgten. CloudTrail übermittelt Protokolldateien aus allen AWS Regionen an Ihren S3-Bucket , wenn MULTI_REGION_CLOUD_TRAIL_ENABLED aktiviert ist. Außerdem wird beim AWS Start einer neuen Region derselbe Trail in der neuen Region erstellt. CloudTrail Dadurch erhalten Sie automatisch Protokolldateien mit API-Aktivitäten für die neue Region.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-7(9)	Grenzschutz | Beschränkung von bedrohlichem ausgehendem Kommunikationsverkehr	opensearch-logs-to-cloudwatch	Stellen Sie sicher, dass für Amazon OpenSearch Service-Domains Fehlerprotokolle aktiviert und zur Aufbewahrung und Beantwortung an Amazon CloudWatch Logs gestreamt werden. OpenSearch Service-Fehlerprotokolle können bei Sicherheits- und Zugriffsprüfungen helfen und bei der Diagnose von Verfügbarkeitsproblemen helfen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-7(9)	Grenzschutz | Beschränkung von bedrohlichem ausgehendem Kommunikationsverkehr	redshift-enhanced-vpc-routing-aktiviert	Mit Enhanced-VPC-Routing wird erzwungen, dass der gesamte COPY- und UNLOAD-Datenverkehr zwischen Ihrem Cluster und Datenrepositorys über Ihre Amazon VPC erfolgt. Anschließend können Sie VPC-Features wie Sicherheitsgruppen und Netzwerkzugriffskontrolllisten verwenden, um den Netzwerkverkehr zu schützen. Sie können auch VPC-Flow-Protokolle verwenden, um den Netzwerkverkehr zu überwachen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-7(9)	Grenzschutz | Beschränkung von bedrohlichem ausgehendem Kommunikationsverkehr	ssm-document-not-public	Stellen Sie sicher, dass AWS Systems Manager (SSM) - Dokumente nicht öffentlich sind, da dies einen unbeabsichtigten Zugriff auf Ihre SSM-Dokumente ermöglichen kann. Ein öffentliches SSM-Dokument kann Informationen über Ihr Konto, Ihre Ressourcen und internen Prozesse preisgeben.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-7(9)	Grenzschutz | Beschränkung von bedrohlichem ausgehendem Kommunikationsverkehr	wafv2-logging-enabled	Um die Protokollierung und Überwachung in Ihrer Umgebung zu erleichtern, aktivieren Sie die AWS WAF (V2) -Protokollierung im regionalen und globalen Web. ACLs AWS Die WAF-Protokollierung bietet detaillierte Informationen über den Datenverkehr, der von Ihrer Web-ACL analysiert wird. In den Protokollen werden die Uhrzeit aufgezeichnet, zu der die AWS WAF die Anfrage von Ihrer AWS Ressource erhalten hat, Informationen über die Anfrage und eine Aktion für die Regel, der jede Anfrage entsprach.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-7(9)	Grenzschutz | Beschränkung von bedrohlichem ausgehendem Kommunikationsverkehr	api-gw-execution-logging-aktiviert	Die API-Gateway-Protokollierung zeigt detaillierte Ansichten der Benutzer, die auf die API zugegriffen haben, und wie diese Benutzer auf die API zugegriffen haben. Diese Einblicke ermöglichen die Transparenz von Benutzeraktivitäten.
SC-7(9)	Grenzschutz | Beschränkung von bedrohlichem ausgehendem Kommunikationsverkehr	cloud-trail-cloud-watch-logs-aktiviert	Verwenden Sie Amazon CloudWatch , um Protokoll ereignisaktivitäten zentral zu sammeln und zu verwalten. Die Aufnahme von AWS CloudTrail Daten liefert Einzelheiten zu den API-Aufrufaktivitäten in Ihrem AWS-Konto.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-7(9)	Grenzschutz | Beschränkung von bedrohlichem ausgehendem Kommunikationsverkehr	cloudtrail-enabled	AWS CloudTrail kann bei der Nichtabstreitbarkeit helfen, indem Aktionen und API-Aufrufe der AWS Management Console aufgezeichnet werden. Sie können die Benutzer und die Benutzer AWS-Konten , die einen AWS Dienst aufgerufen haben, die Quell-IP-Adresse, über die die Aufrufe generiert wurden, und den Zeitpunkt der Anrufe identifizieren. Einzelheiten zu den erfassten Daten finden Sie in den AWS CloudTrail Datensatzinhalten.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-7(9)	Grenzschutz | Beschränkung von bedrohlichem ausgehendem Kommunikationsverkehr	cloudtrail-s3-dataevents-enabled	Die Erfassung von Simple Storage Service (Amazon S3)-Datenereignissen unterstützt die Erkennung von ungewöhnlichen Aktivitäten. Zu den Details gehören AWS-Konto Informationen über den Zugriff auf einen Amazon S3 S3-Bucket, die IP-Adresse und die Uhrzeit des Ereignisses.
SC-7(9)	Grenzschutz | Beschränkung von bedrohlichem ausgehendem Kommunikationsverkehr	dms-replication-not-public	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass auf DMS-Replikationsinstanzen nicht öffentlich zugegriffen werden kann. DMS-Replikations-Instances können vertrauliche Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-7(9)	Grenzschutz | Beschränkung von bedrohlichem ausgehendem Kommunikationsverkehr	ebs-snapshot-public-restorable-überprüfen	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass EBS-Snapshots nicht öffentlich wiederherstellbar sind. EBS-Volume-Snapshots können vertrauliche Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.
SC-7(9)	Grenzschutz | Beschränkung von bedrohlichem ausgehendem Kommunikationsverkehr	ec-2 instance-no-public-ip	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon Elastic Compute Cloud (Amazon EC2) - Instances nicht öffentlich zugänglich sind. EC2 Amazon-Instances können vertrauliche Informationen enthalten, und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-7(9)	Grenzschutz | Beschränkung von bedrohlichem ausgehendem Kommunikationsverkehr	elasticsearch-in-vpc-only	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass sich Amazon OpenSearch OpenSearch Service (Service) - Domains innerhalb einer Amazon Virtual Private Cloud (Amazon VPC) befinden. Eine OpenSearch Service-Domain innerhalb einer Amazon VPC ermöglicht die sichere Kommunikation zwischen OpenSearch Service und anderen Services innerhalb der Amazon VPC, ohne dass ein Internet-Gateway, ein NAT-Gerät oder eine VPN-Verbindung erforderlich ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-7(9)	Grenzschutz | Beschränkung von bedrohlichem ausgehendem Kommunikationsverkehr	elb-logging-enabled	Die Elastic-Load-Balancing-Aktivität ist ein zentraler Kommunikationspunkt innerhalb einer Umgebung. Stellen Sie sicher, dass die ELB-Protokollierung aktiviert ist. Die gesammelten Daten enthalten detaillierte Informationen zu Anfragen, die an den ELB gesendet wurden. Jedes Protokoll enthält Informationen wie die Zeit, zu der die Anforderung einging, die Client-IP-Adresse, Latenzen, Anforderungspfade und Serverantworten.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-7(9)	Grenzschutz | Beschränkung von bedrohlichem ausgehendem Kommunikationsverkehr	emr-master-no-public-ip	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon EMR-Cluster-Masterknoten nicht öffentlich zugänglich sind. Amazon-EMR-Cluster-Hauptknoten können vertrauliche Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.
SC-7(9)	Grenzschutz | Beschränkung von bedrohlichem ausgehendem Kommunikationsverkehr	lambda-function-public-access-verboten	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass AWS Lambda-Funktionen nicht öffentlich zugänglich sind. Der öffentliche Zugriff kann möglicherweise die Verfügbarkeit von Ressourcen beeinträchtigen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-7(9)	Grenzschutz | Beschränkung von bedrohlichem ausgehendem Kommunikationsverkehr	lambda-inside-vpc	Stellen Sie AWS Lambda-Funktionen in einer Amazon Virtual Private Cloud (Amazon VPC) bereit, um eine sichere Kommunikation zwischen einer Funktion und anderen Diensten innerhalb der Amazon VPC zu gewährleisten. Bei dieser Konfiguration sind kein Internet-Gateway, kein NAT-Gerät und keine VPN-Verbindung erforderlich. Der gesamte Datenverkehr bleibt sicher in der Cloud. AWS Domains, die sich innerhalb einer VPC befinden, verfügen aufgrund ihrer logischen Isolierung im Vergleich zu Domains mit öffentlichen Endpunkten über eine zusätzliche Sicherheitsebene. Um den Zugriff ordnungsgemäß zu verwalten,

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			sollten AWS Lambda-Funktionen einer VPC zugewiesen werden.
SC-7(9)	Grenzschutz | Beschränkung von bedrohlichem ausgehendem Kommunikationsverkehr	opensearch-in-vpc-only	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass sich Amazon OpenSearch Service-Domains innerhalb einer Amazon Virtual Private Cloud (Amazon VPC) befinden. Eine Amazon OpenSearch Service-Domain innerhalb einer Amazon VPC ermöglicht die sichere Kommunikation zwischen Amazon OpenSearch Service und anderen Services innerhalb der Amazon VPC, ohne dass ein Internet-Gateway, ein NAT-Gerät oder eine VPN-Verbindung erforderlich ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-7(9)	Grenzschutz | Beschränkung von bedrohlichem ausgehendem Kommunikationsverkehr	rds-instance-public-access-überprüfen	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Relational Database Service (Amazon RDS) -Instances nicht öffentlich sind. Amazon-RDS-Datenbank-Instances können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-7(9)	Grenzschutz | Beschränkung von bedrohlichem ausgehendem Kommunikationsverkehr	rds-logging-enabled	Um die Protokollierung und Überwachung in Ihrer Umgebung zu erleichtern, stellen Sie sicher, dass die Amazon Relational Database Service (Amazon RDS)-Protokollierung aktiviert ist. Mit der Amazon-RDS-Protokollierung können Sie Ereignisse wie Verbindungen, Verbindungsabbrüche, Abfragen oder abgefragte Tabellen erfassen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-7(9)	Grenzschutz | Beschränkung von bedrohlichem ausgehendem Kommunikationsverkehr	rds-snapshots-public-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Relational Database Service (Amazon RDS) -Instances nicht öffentlich sind. Amazon-RDS-Datenbank-Instances können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-7(9)	Grenzschutz | Beschränkung von bedrohlichem ausgehendem Kommunikationsverkehr	redshift-cluster-configuration-check	Um Daten im Ruhezustand zu schützen, muss die Verschlüsselung für Ihre Amazon-Redshift-Cluster aktiviert sein. Sie müssen auch sicherstellen, dass die erforderlichen Konfigurationen auf Amazon-Redshift-Clustern bereitgestellt werden. Die Prüfungsprotokollierung muss aktiviert sein, um Informationen zu Verbindungen und Benutzeraktivitäten in der Datenbank bereitzustellen. Diese Regel erfordert, dass ein Wert für clusterDbEncrypted (Config Default: TRUE) und LoggingEnabled (Config Default: TRUE) gesetzt ist. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-7(9)	Grenzschutz | Beschränkung von bedrohlichem ausgehendem Kommunikationsverkehr	redshift-cluster-public-access-überprüfen	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Redshift Redshift-Cluster nicht öffentlich sind. Amazon-Redshift-Cluster können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-7(9)	Grenzschutz | Beschränkung von bedrohlichem ausgehendem Kommunikationsverkehr	s3- -Block-periodisch account-level-public-access	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Simple Storage Service (Amazon S3) -Buckets nicht öffentlich zugänglich sind. Diese Regel trägt dazu bei, sensible Daten vor unbefugten Remote-Benutzern zu schützen, indem sie den öffentlichen Zugriff verhindert. Mit dieser Regel können Sie optional die Parameter ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) und restrictPublicBuckets Parameter (Config Default: True) festlegen. Die tatsächlichen Werte müssen den Richtlini

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			en Ihrer Organisation entsprechen.
SC-7(9)	Grenzschutz | Beschränkung von bedrohlichem ausgehendem Kommunikationsverkehr	s3 bucket-level-public-access - verboten	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Simple Storage Service (Amazon S3) -Buckets nicht öffentlich zugänglich sind. Diese Regel trägt dazu bei, sensible Daten vor unbefugten Remote-Benutzern zu schützen, indem sie den öffentlichen Zugriff auf Bucket-Ebene verhindert.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-7(9)	Grenzschutz | Beschränkung von bedrohlichem ausgehendem Kommunikationsverkehr	s-3 bucket-logging-enabled	Die Amazon Simple Storage Service (Amazon S3)-Serverzugriffs protokollierung bietet eine Methode zur Überwachung des Netzwerks im Hinblick auf potenzielle Cybersicherheitsereignisse. Die Ereignisse werden überwacht, indem detaillierte Aufzeichnungen über die Anfragen erfasst werden, die an einen Amazon-S3-Bucket gestellt wurden. Jeder Zugriffsprotokolleintrag enthält Details zu einer einzelnen Zugriffsanfrage. Zu den Details gehören Anforderer, Bucket-Name, Anforderungszeit, Anforderungsaktion, Antwortstatus und Fehlercode, falls relevant.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-7(9)	Grenzschutz | Beschränkung von bedrohlichem ausgehendem Kommunikationsverkehr	s-3 bucket-public-read-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie nur autorisierten Benutzern, Prozessen und Geräten Zugriff auf Amazon Simple Storage Service (Amazon S3) - Buckets gewähren. Die Verwaltung des Zugriffs sollte mit der Klassifizierung der Daten übereinstimmen.
SC-7(9)	Grenzschutz | Beschränkung von bedrohlichem ausgehendem Kommunikationsverkehr	s3- bucket-public-write-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie nur autorisierten Benutzern, Prozessen und Geräten Zugriff auf Amazon Simple Storage Service (Amazon S3) - Buckets gewähren. Die Verwaltung des Zugriffs sollte mit der Klassifizierung der Daten übereinstimmen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-7(9)	Grenzschutz | Beschränkung von bedrohlichem ausgehendem Kommunikationsverkehr	sagemaker-notebook-no-direct-Internetzugang	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass SageMaker Amazon-Notebooks keinen direkten Internetzugang zulassen. Indem Sie direkten Internetzugang blockieren, vermeiden Sie, dass unbefugte Benutzer auf sensible Daten zugreifen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-7(9)	Grenzschutz | Beschränkung von bedrohlichem ausgehendem Kommunikationsverkehr	subnet-auto-assign-public-ip-deaktiviert	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon Virtual Private Cloud (VPC) -Subnetzen nicht automatisch eine öffentliche IP-Adresse zugewiesen wird. Amazon Elastic Compute Cloud (EC2) -Instances, die in Subnetzen gestartet werden, in denen dieses Attribut aktiviert ist, haben ihrer primären Netzwerkschnittstelle eine öffentliche IP-Adresse zugewiesen.
SC-7(10)	Grenzschutz | Verhinderung von Exfiltrationen	cloud-trail-encryption-enabled	Da sensible Daten vorhanden sein können und um Daten im Ruhezustand zu schützen, sollten Sie sicherstellen, dass die Verschlüsselung für Ihre AWS CloudTrail Trails aktiviert ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-7(10)	Grenzschutz | Verhinderung von Exfiltrationen	dynamodb-table-encrypted-kms	Stellen Sie sicher, dass die Verschlüsselung für Ihre Amazon-DynamoDB-Tabellen aktiviert ist. Um eventuell vorhandene sensible Daten im Ruhezustand in diesen Tabellen zu schützen, müssen Sie die Verschlüsselung von Daten im Ruhezustand aktivieren. Standardmäßig werden DynamoDB-Tabellen mit einem AWS eigenen Kundenhauptschlüssel (CMK) verschlüselt.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-7(10)	Grenzschutz | Verhinderung von Exfiltrationen	ec2- ebs-encryption-by-default	Zum Schutz von Daten im Ruhezustand müssen Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon Elastic Block Store (Amazon EBS)-Volumes aktiviert ist. Da sensible Daten auch im Ruhezustand vorhanden sein können, sollten Sie die Verschlüsselung im Ruhezustand aktivieren, um diese Daten zu schützen.
SC-7(10)	Grenzschutz | Verhinderung von Exfiltrationen	efs-encrypted-check	Aktivieren Sie die Verschlüsselung für Ihr Amazon Elastic File System (EFS), um eventuell vorhandene sensible Daten sowie Daten im Ruhezustand zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-7(10)	Grenzschutz | Verhinderung von Exfiltrationen	elasticsearch-encrypted-at-rest	Da sensible Daten vorhanden sein können und um Daten im Ruhezustand zu schützen, sollten Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon OpenSearch Service (OpenSearch Service) -Domains aktiviert ist.
SC-7(10)	Grenzschutz | Verhinderung von Exfiltrationen	encrypted-volumes	Aktivieren Sie die Verschlüsselung für Ihre Amazon-Elastic-Block-Store (Amazon-EBS)-Volumes, um eventuell vorhandene sensible Daten sowie Daten im Ruhezustand zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-7(10)	Grenzschutz | Verhinderung von Exfiltrationen	rds-logging-enabled	Um die Protokollierung und Überwachung in Ihrer Umgebung zu erleichtern, stellen Sie sicher, dass die Amazon Relational Database Service (Amazon RDS)-Protokollierung aktiviert ist. Mit der Amazon-RDS-Protokollierung können Sie Ereignisse wie Verbindungen, Verbindungsabbrüche, Abfragen oder abgefragte Tabellen erfassen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-7(10)	Grenzschutz | Verhinderung von Exfiltrationen	rds-snapshot-encrypted	Stellen Sie sicher, dass die Verschlüsselung für Ihre Amazon Relational Database Service (Amazon RDS)-Snapshots aktiviert ist. Da sensible Daten auch im Ruhezustand vorhanden sein können, sollten Sie die Verschlüsselung im Ruhezustand aktivieren, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-7(10)	Grenzschutz | Verhinderung von Exfiltrationen	rds-storage-encrypted	Zum Schutz von Daten im Ruhezustand müssen Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon Relational Database Service (Amazon RDS)-Instances aktiviert ist. Um eventuell vorhandene sensible Daten im Ruhezustand in Amazon-RDS-Instances zu schützen, muss die Verschlüsselung von Daten im Ruhezustand aktiviert sein.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-7(10)	Grenzschutz | Verhinderung von Exfiltrationen	redshift-backup-enabled	Stellen Sie zur Unterstützung der Datensicherungsprozesse sicher, dass Ihre Amazon-Redshift-Cluster über automatisierte Snapshots verfügen. Wenn automatisierte Snapshots für einen Cluster aktiviert sind, erstellt Redshift in regelmäßigen Abständen Snapshots dieses Clusters. Standardmäßig erstellt Redshift alle acht Stunden oder alle 5 GB einen Snapshot für jeden Knoten mit Datenänderungen oder je nachdem, was zuerst eintritt.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-7(10)	Grenzschutz | Verhinderung von Exfiltrationen	redshift-cluster-configuration-check	Um Daten im Ruhezustand zu schützen, muss die Verschlüsselung für Ihre Amazon-Redshift-Cluster aktiviert sein. Sie müssen auch sicherstellen, dass die erforderlichen Konfigurationen auf Amazon-Redshift-Clustern bereitgestellt werden. Die Prüfungsprotokollierung muss aktiviert sein, um Informationen zu Verbindungen und Benutzeraktivitäten in der Datenbank bereitzustellen. Diese Regel erfordert, dass ein Wert für clusterDbEncrypted (Config Default: TRUE) und LoggingEnabled (Config Default: TRUE) gesetzt ist. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-7(10)	Grenzschutz | Verhinderung von Exfiltrationen	s3-aktiviert bucket-server-side-encryption	Zum Schutz von Daten im Ruhezustand müssen Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon Simple Storage Service (Amazon S3)-Buckets aktiviert ist. Um eventuell vorhandene sensible Daten im Ruhezustand in Amazon-S3-Buckets zu schützen, muss die Verschlüsselung aktiviert sein.
SC-7(10)	Grenzschutz | Verhinderung von Exfiltrationen	s-3 default-encryption-kms	Stellen Sie sicher, dass die Verschlüsselung für Ihre Amazon Simple Storage Service (Amazon S3)-Buckets aktiviert ist. Um eventuell vorhandene sensible Daten im Ruhezustand in einem Amazon-S3-Bucket zu schützen, muss die Verschlüsselung aktiviert sein.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-7(10)	Grenzschutz | Verhinderung von Exfiltrationen	sagemaker-endpoint-configuration-kms-key-konfiguriert	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass die Verschlüsselung mit dem AWS Key Management Service (AWS KMS) für Ihren Endpunkt aktiviert ist. SageMaker Da sensible Daten auf dem SageMaker Endgerät gespeiche rt werden können, sollten Sie die Verschlüsselung im Ruhezustand aktiviere n, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-7(10)	Grenzschutz | Verhinderung von Exfiltrationen	sagemaker-notebook-instance-kms-schlüsselkonfiguriert	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass die Verschlüsselung mit dem AWS Key Management Service (AWS KMS) für Ihr Notebook aktiviert ist. SageMaker Da vertrauliche Daten im SageMaker Notebook gespeichert werden können, sollten Sie die Verschlüsselung im Ruhezustand aktivieren, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-7(10)	Grenzschutz | Verhinderung von Exfiltrationen	sns-encrypted-kms	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass Ihre Amazon Simple Notification Service (Amazon SNS) -Themen mit dem AWS Key Management Service (AWS KMS) verschlüsselt werden müssen. Um eventuell vorhandene sensible Daten im Ruhezustand in veröffentlichten Nachrichten zu schützen, muss die Verschlüsselung von Daten im Ruhezustand aktiviert sein.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-7(10)	Grenzschutz | Verhinderung von Exfiltrationen	wafv2-logging-enabled	Um Ihnen die Protokollierung und Überwachung in Ihrer Umgebung zu erleichtern, aktivieren Sie die AWS WAF (V2) -Protokollierung im regionalen und globalen Web. ACLs AWS Die WAF-Protokollierung bietet detaillierte Informationen über den Datenverkehr, der von Ihrer Web-ACL analysiert wird. In den Protokollen werden die Uhrzeit aufgezeichnet, zu der die AWS WAF die Anfrage von Ihrer AWS Ressource erhalten hat, Informationen über die Anfrage und eine Aktion für die Regel, der jede Anfrage entsprach.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-7(10)	Grenzschutz | Verhinderung von Exfiltrationen	kinesis-stream-encrypted	Aktivieren Sie die Verschlüsselung für Ihre Amazon-Kinesis-Streams, um eventuell vorhandene sensible Daten sowie Daten im Ruhezustand zu schützen.
SC-7(11)	Grenzschutz | Beschränkung von bedrohlichem eingehendem Kommunikationsverkehr	autoscaling-launch-config-public-ip-deaktiviert	Wenn Sie Ihre Netzwerkschnittstellen mit einer öffentlichen IP-Adresse konfigurieren, sind die diesen Netzwerkschnittstellen zugehörigen Ressourcen über das Internet erreichbar. EC2 Ressourcen sollten nicht öffentlich zugänglich sein, da dies einen unbeabsichtigten Zugriff auf Ihre Anwendungen oder Server ermöglichen kann.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-7(11)	Grenzschutz | Beschränkung von bedrohlichem eingehendem Kommunikationsverkehr	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) Security Groups können bei der Verwaltung des Netzwerkzugriffs helfen, indem sie eine statusbehaftete Filterung von eingehendem und ausgehendem Netzwerkverkehr zu Ressourcen bereitstellen. AWS Wenn Sie eingehenden (oder entfernten) Datenverkehr von 0.0.0.0/0 bis Port 22 auf Ihren Ressourcen nicht zulassen, können Sie den Remote-Zugriff einschränken.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-7(11)	Grenzschutz | Beschränkung von bedrohlichem eingehendem Kommunikationsverkehr	ec2- instances-in-vpc	Stellen Sie Amazon Elastic Compute Cloud (Amazon EC2) -Instances innerhalb einer Amazon Virtual Private Cloud (Amazon VPC) bereit, um eine sichere Kommunikation zwischen einer Instance und anderen Services innerhalb der Amazon VPC zu ermöglichen, ohne dass ein Internet-Gateway, ein NAT-Gerät oder eine VPN-Verbindung erforderlich ist. Der gesamte Datenverkehr bleibt sicher in der AWS Cloud. Domains, die sich innerhalb einer VPC befinden, verfügen aufgrund ihrer logischen Isolierung im Vergleich zu Domains mit öffentlichen Endpunkten über eine zusätzliche Sicherheitsebene. Weisen Sie EC2

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			Amazon-Instances einer Amazon-VPC zu, um den Zugriff ordnungsgemäß zu verwalten.
SC-7(11)	Grenzschutz | Beschränkung von bedrohlichem eingehendem Kommunikationsverkehr	no-unrestricted-route-to-igw	Stellen Sie sicher, dass EC2 Amazon-Routentabellen keine uneingeschränkten Routen zu einem Internet-Gateway enthalten. Durch das Entfernen oder Beschränken des Internetzugangs für Workloads innerhalb von Amazon VPCs können unbeabsichtigte Zugriffe in Ihrer Umgebung reduziert werden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-7(11)	Grenzschutz | Beschränkung von bedrohlichem eingehendem Kommunikationsverkehr	redshift-enhanced-vpc-routing-aktiviert	Mit Enhanced-VPC-Routing wird erzwungen, dass der gesamte COPY- und UNLOAD-Datenverkehr zwischen Ihrem Cluster und Datenrepositorys über Ihre Amazon VPC erfolgt. Anschließend können Sie VPC-Features wie Sicherheitsgruppen und Netzwerkzugriffskontrolllisten verwenden, um den Netzwerkverkehr zu schützen. Sie können auch VPC-Flow-Protokolle verwenden, um den Netzwerkverkehr zu überwachen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-7(11)	Grenzschutz | Beschränkung von bedrohlichem eingehendem Kommunikationsverkehr	ssm-document-not-public	Stellen Sie sicher, dass AWS Systems Manager (SSM) - Dokumente nicht öffentlich sind, da dies einen unbeabsichtigten Zugriff auf Ihre SSM-Dokumente ermöglichen kann. Ein öffentliches SSM-Dokument kann Informationen über Ihr Konto, Ihre Ressourcen und internen Prozesse preisgeben.
SC-7(11)	Grenzschutz | Beschränkung von bedrohlichem eingehendem Kommunikationsverkehr	dms-replication-not-public	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass auf DMS-Replikationsinstanzen nicht öffentlich zugegriffen werden kann. DMS-Replikations-Instances können vertrauliche Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-7(11)	Grenzschutz | Beschränkung von bedrohlichem eingehendem Kommunikationsverkehr	ebs-snapshot-public-restorable-überprüfen	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass EBS-Snapshots nicht öffentlich wiederherstellbar sind. EBS-Volume-Snapshots können vertrauliche Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.
SC-7(11)	Grenzschutz | Beschränkung von bedrohlichem eingehendem Kommunikationsverkehr	ec-2 instance-no-public-ip	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon Elastic Compute Cloud (Amazon EC2) - Instances nicht öffentlich zugänglich sind. EC2 Amazon-Instances können vertrauliche Informationen enthalten, und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-7(11)	Grenzschutz | Beschränkung von bedrohlichem eingehendem Kommunikationsverkehr	elasticsearch-in-vpc-only	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass sich Amazon OpenSearch OpenSearch Service (Service) - Domains innerhalb einer Amazon Virtual Private Cloud (Amazon VPC) befinden. Eine OpenSearch Service-Domain innerhalb einer Amazon VPC ermöglicht die sichere Kommunikation zwischen OpenSearch Service und anderen Services innerhalb der Amazon VPC, ohne dass ein Internet-Gateway, ein NAT-Gerät oder eine VPN-Verbindung erforderlich ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-7(11)	Grenzschutz | Beschränkung von bedrohlichem eingehendem Kommunikationsverkehr	emr-master-no-public-ip	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon EMR-Cluster-Masterknoten nicht öffentlich zugänglich sind. Amazon-EMR-Cluster-Hauptknoten können vertrauliche Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.
SC-7(11)	Grenzschutz | Beschränkung von bedrohlichem eingehendem Kommunikationsverkehr	lambda-function-public-access-verboten	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass AWS Lambda-Funktionen nicht öffentlich zugänglich sind. Der öffentliche Zugriff kann möglicherweise die Verfügbarkeit von Ressourcen beeinträchtigen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-7(11)	Grenzschutz | Beschränkung von bedrohlichem eingehendem Kommunikationsverkehr	lambda-inside-vpc	Stellen Sie AWS Lambda-Funktionen in einer Amazon Virtual Private Cloud (Amazon VPC) bereit, um eine sichere Kommunikation zwischen einer Funktion und anderen Diensten innerhalb der Amazon VPC zu gewährleisten. Bei dieser Konfiguration sind kein Internet-Gateway, kein NAT-Gerät und keine VPN-Verbindung erforderlich. Der gesamte Datenverkehr bleibt sicher in der Cloud. AWS Domains, die sich innerhalb einer VPC befinden, verfügen aufgrund ihrer logischen Isolierung im Vergleich zu Domains mit öffentlichen Endpunkten über eine zusätzliche Sicherheitsebene. Um den Zugriff ordnungsgemäß zu verwalten,

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			sollten AWS Lambda-Funktionen einer VPC zugewiesen werden.
SC-7(11)	Grenzschutz | Beschränkung von bedrohlichem eingehendem Kommunikationsverkehr	opensearch-in-vpc-only	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass sich Amazon OpenSearch Service-Domains innerhalb einer Amazon Virtual Private Cloud (Amazon VPC) befinden. Eine Amazon OpenSearch Service-Domain innerhalb einer Amazon VPC ermöglicht die sichere Kommunikation zwischen Amazon OpenSearch Service und anderen Services innerhalb der Amazon VPC, ohne dass ein Internet-Gateway, ein NAT-Gerät oder eine VPN-Verbindung erforderlich ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-7(11)	Grenzschutz | Beschränkung von bedrohlichem eingehendem Kommunikationsverkehr	rds-instance-public-access-überprüfen	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Relational Database Service (Amazon RDS) -Instances nicht öffentlich sind. Amazon-RDS-Datenbank-Instances können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-7(11)	Grenzschutz | Beschränkung von bedrohlichem eingehendem Kommunikationsverkehr	rds-snapshots-public-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Relational Database Service (Amazon RDS) -Instances nicht öffentlich sind. Amazon-RDS-Datenbank-Instances können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-7(11)	Grenzschutz | Beschränkung von bedrohlichem eingehendem Kommunikationsverkehr	redshift-cluster-public-access-überprüfen	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Redshift Redshift-Cluster nicht öffentlich sind. Amazon-Redshift-Cluster können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-7(11)	Grenzschutz | Beschränkung von bedrohlichem eingehendem Kommunikationsverkehr	restricted-common-ports	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass gemeinsame Ports für Amazon Elastic Compute Cloud (Amazon EC2) -Sicherheitsgruppen eingeschränkt sind. Wenn der Zugriff auf Ports nicht auf vertrauenswürdige Quellen beschränkt wird, kann dies zu Angriffen auf die Verfügbarkeit, Integrität und Vertraulichkeit von Systemen führen. Mit dieser Regel können Sie optional die Parameter blockedPort1–blockedPort5 festlegen (Standardkonfigurationen: 20, 21, 3389, 3306, 4333). Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-7(11)	Grenzschutz | Beschränkung von bedrohlichem eingehendem Kommunikationsverkehr	s3- account-level-public-access -Block-periodisch	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Simple Storage Service (Amazon S3) -Buckets nicht öffentlich zugänglich sind. Diese Regel trägt dazu bei, sensible Daten vor unbefugten Remote-Benutzern zu schützen, indem sie den öffentlichen Zugriff verhindert. Mit dieser Regel können Sie optional die Parameter ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) und restrictPublicBuckets Parameter (Config Default: True) festlegen. Die tatsächlichen Werte müssen den Richtlini

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			en Ihrer Organisation entsprechen.
SC-7(11)	Grenzschutz | Beschränkung von bedrohlichem eingehendem Kommunikationsverkehr	s3 bucket-level-public-access - verboten	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Simple Storage Service (Amazon S3) -Buckets nicht öffentlich zugänglich sind. Diese Regel trägt dazu bei, sensible Daten vor unbefugten Remote-Benutzern zu schützen, indem sie den öffentlichen Zugriff auf Bucket-Ebene verhindert.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-7(11)	Grenzschutz | Beschränkung von bedrohlichem eingehendem Kommunikationsverkehr	s-3 bucket-public-read-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie nur autorisierten Benutzern, Prozessen und Geräten Zugriff auf Amazon Simple Storage Service (Amazon S3) - Buckets gewähren. Die Verwaltung des Zugriffs sollte mit der Klassifizierung der Daten übereinstimmen.
SC-7(11)	Grenzschutz | Beschränkung von bedrohlichem eingehendem Kommunikationsverkehr	s3- bucket-public-write-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie nur autorisierten Benutzern, Prozessen und Geräten Zugriff auf Amazon Simple Storage Service (Amazon S3) - Buckets gewähren. Die Verwaltung des Zugriffs sollte mit der Klassifizierung der Daten übereinstimmen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-7(11)	Grenzschutz | Beschränkung von bedrohlichem eingehendem Kommunikationsverkehr	sagemaker-notebook-no-direct-Internetzugang	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass SageMaker Amazon-Notebooks keinen direkten Internetzugang zulassen. Indem Sie direkten Internetzugang blockieren, vermeiden Sie, dass unbefugte Benutzer auf sensible Daten zugreifen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-7(11)	Grenzschutz | Beschränkung von bedrohlichem eingehendem Kommunikationsverkehr	subnet-auto-assign-public-ip-deaktiviert	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon Virtual Private Cloud (VPC) -Subnetzen nicht automatisch eine öffentliche IP-Adresse zugewiesen wird. Amazon Elastic Compute Cloud (EC2) -Instances, die in Subnetzen gestartet werden, in denen dieses Attribut aktiviert ist, haben ihrer primären Netzwerkschnittstelle eine öffentliche IP-Adresse zugewiesen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-7(11)	Grenzschutz | Beschränkung von bedrohlichem eingehendem Kommunikationsverkehr	vpc-default-security-group-geschlossen	Sicherheitsgruppen von Amazon Elastic Compute Cloud (Amazon EC2) können bei der Verwaltung des Netzwerkzugriffs helfen, indem sie eine statusbehaftete Filterung des ein- und ausgehenden Netzwerkverkehrs zu Ressourcen bereitstellen. AWS Die Beschränkung des gesamten Datenverkehrs auf die Standardsicherheitsgruppe hilft dabei, den Fernzugriff auf Ihre Ressourcen einzuschränken. AWS

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-7(11)	Grenzschutz | Beschränkung von bedrohlichem eingehendem Kommunikationsverkehr	vpc-sg-open-only-to-authorized-ports	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass gemeinsame Ports für Amazon Elastic Compute Cloud (Amazon EC2) -Sicherheitsgruppen eingeschränkt sind. Wenn der Zugriff auf Ports nicht auf vertrauenswürdige Quellen beschränkt wird, kann dies zu Angriffen auf die Verfügbarkeit, Integrität und Vertraulichkeit von Systemen führen. Durch die Beschränkung des Zugriffs auf Ressourcen innerhalb einer Sicherheitsgruppe aus dem Internet (0.0.0.0/0) kann der Remote-Zugriff auf interne Systeme gesteuert werden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-7(16)	Grenzschutz | Verhinderung der Erkennung von Systemkomponenten	autoscaling-launch-config-public-ip-deaktiviert	Wenn Sie Ihre Netzwerkschnittstellen mit einer öffentlichen IP-Adresse konfigurieren, sind die diesen Netzwerkschnittstellen zugehörigen Ressourcen über das Internet erreichbar. EC2 Ressourcen sollten nicht öffentlich zugänglich sein, da dies einen unbeabsichtigten Zugriff auf Ihre Anwendungen oder Server ermöglichen kann.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-7(16)	Grenzschutz | Verhinderung der Erkennung von Systemkomponenten	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) Security Groups können bei der Verwaltung des Netzwerkzugriffs helfen, indem sie eine statusbeh aftete Filterung von eingehendem und ausgehendem Netzwerkverkehr zu Ressourcen bereitste llen. AWS Wenn Sie eingehenden (oder entfernten) Datenverk ehr von 0.0.0.0/0 bis Port 22 auf Ihren Ressourcen nicht zulassen, können Sie den Remote-Zugriff einschränken.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-7(16)	Grenzschutz | Verhinderung der Erkennung von Systemkomponenten	ec2- instances-in-vpc	Stellen Sie Amazon Elastic Compute Cloud (Amazon EC2) -Instances innerhalb einer Amazon Virtual Private Cloud (Amazon VPC) bereit, um eine sichere Kommunika tion zwischen einer Instance und anderen Services innerhalb der Amazon VPC zu ermöglichen, ohne dass ein Internet-Gateway, ein NAT-Gerät oder eine VPN-Verbindung erforderlich ist. Der gesamte Datenverk ehr bleibt sicher in der AWS Cloud. Domains, die sich innerhalb einer VPC befinden, verfügen aufgrund ihrer logischen Isolierun g im Vergleich zu Domains mit öffentlic hen Endpunkten über eine zusätzlic he Sicherheitsebene. Weisen Sie EC2

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			Amazon-Instances einer Amazon-VPC zu, um den Zugriff ordnungsgemäß zu verwalten.
SC-7(16)	Grenzschutz | Verhinderung der Erkennung von Systemkomponenten	no-unrestricted-route-to-igw	Stellen Sie sicher, dass EC2 Amazon-Routentabellen keine uneingeschränkten Routen zu einem Internet-Gateway enthalten. Durch das Entfernen oder Beschränken des Internetzugangs für Workloads innerhalb von Amazon VPCs können unbeabsic htigte Zugriffe in Ihrer Umgebung reduziert werden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-7(16)	Grenzschutz | Verhinderung der Erkennung von Systemkomponenten	ssm-document-not-public	Stellen Sie sicher, dass AWS Systems Manager (SSM) - Dokumente nicht öffentlich sind, da dies einen unbeabsichtigten Zugriff auf Ihre SSM-Dokumente ermöglichen kann. Ein öffentliches SSM-Dokument kann Informationen über Ihr Konto, Ihre Ressourcen und internen Prozesse preisgeben.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-7(16)	Grenzschutz | Verhinderung der Erkennung von Systemkomponenten	acm-certificate-expiration-check	Stellen Sie sicher, dass die Netzwerkintegrität geschützt ist, indem Sie sicherstellen, dass X509-Zertifikate von ACM ausgestellt werden. AWS Diese Zertifikate müssen gültig und dürfen nicht abgelaufen sein. Für diese Regel ist ein Wert für erforderlich daysToExpiration (Wert für bewährte AWS Grundregeln für Sicherheit: 90). Der tatsächliche Wert muss den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-7(16)	Grenzschutz | Verhinderung der Erkennung von Systemkomponenten	dms-replication-not-public	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass auf DMS-Replikationsin stanzen nicht öffentlic h zugegriffen werden kann. DMS-Repli kations-Instances können vertrauli che Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.
SC-7(16)	Grenzschutz | Verhinderung der Erkennung von Systemkomponenten	ebs-snapshot-public-restorable-überprüfen	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass EBS-Snapshots nicht öffentlich wiederher stellbar sind. EBS-Volume-Snapsho ts können vertrauli che Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-7(16)	Grenzschutz | Verhinderung der Erkennung von Systemkomponenten	ec-2 instance-no-public-ip	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon Elastic Compute Cloud (Amazon EC2) - Instances nicht öffentlich zugänglich sind. EC2 Amazon-Instances können vertrauliche Informationen enthalten, und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-7(16)	Grenzschutz | Verhinderung der Erkennung von Systemkomponenten	elasticsearch-in-vpc-only	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass sich Amazon OpenSearch OpenSearch Service (Service) - Domains innerhalb einer Amazon Virtual Private Cloud (Amazon VPC) befinden. Eine OpenSearch Service-Domain innerhalb einer Amazon VPC ermöglicht die sichere Kommunikation zwischen OpenSearch Service und anderen Services innerhalb der Amazon VPC, ohne dass ein Internet-Gateway, ein NAT-Gerät oder eine VPN-Verbindung erforderlich ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-7(16)	Grenzschutz | Verhinderung der Erkennung von Systemkomponenten	emr-master-no-public-ip	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon EMR-Cluster-Masterknoten nicht öffentlich zugänglich sind. Amazon-EMR-Cluster-Hauptknoten können vertrauliche Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.
SC-7(16)	Grenzschutz | Verhinderung der Erkennung von Systemkomponenten	lambda-function-public-access-verboten	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass AWS Lambda-Funktionen nicht öffentlich zugänglich sind. Der öffentliche Zugriff kann möglicherweise die Verfügbarkeit von Ressourcen beeinträchtigen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-7(16)	Grenzschutz | Verhinderung der Erkennung von Systemkomponenten	lambda-inside-vpc	Stellen Sie AWS Lambda-Funktionen in einer Amazon Virtual Private Cloud (Amazon VPC) bereit, um eine sichere Kommunika tion zwischen einer Funktion und anderen Diensten innerhalb der Amazon VPC zu gewährleisten. Bei dieser Konfiguration sind kein Internet-Gateway, kein NAT-Gerät und keine VPN-Verbindung erforderlich. Der gesamte Datenverk ehr bleibt sicher in der Cloud. AWS Domains, die sich innerhalb einer VPC befinden, verfügen aufgrund ihrer logischen Isolierun g im Vergleich zu Domains mit öffentlic hen Endpunkten über eine zusätzliche Sicherheitsebene. Um den Zugriff ordnungsg emäß zu verwalten,

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			sollten AWS Lambda-Funktionen einer VPC zugewiesen werden.
SC-7(16)	Grenzschutz | Verhinderung der Erkennung von Systemkomponenten	opensearch-in-vpc-only	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass sich Amazon OpenSearch Service-Domains innerhalb einer Amazon Virtual Private Cloud (Amazon VPC) befinden. Eine Amazon OpenSearch Service-Domain innerhalb einer Amazon VPC ermöglicht die sichere Kommunikation zwischen Amazon OpenSearch Service und anderen Services innerhalb der Amazon VPC, ohne dass ein Internet-Gateway, ein NAT-Gerät oder eine VPN-Verbindung erforderlich ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-7(16)	Grenzschutz | Verhinderung der Erkennung von Systemkomponenten	rds-instance-public-access-überprüfen	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Relational Database Service (Amazon RDS) -Instances nicht öffentlich sind. Amazon-RDS-Datenbank-Instances können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-7(16)	Grenzschutz | Verhinderung der Erkennung von Systemkomponenten	rds-snapshots-public-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Relational Database Service (Amazon RDS) -Instances nicht öffentlich sind. Amazon-RDS-Datenbank-Instances können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-7(16)	Grenzschutz | Verhinderung der Erkennung von Systemkomponenten	redshift-cluster-public-access-überprüfen	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Redshift Redshift-Cluster nicht öffentlich sind. Amazon-Redshift-Cluster können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-7(16)	Grenzschutz | Verhinderung der Erkennung von Systemkomponenten	restricted-common-ports	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass gemeinsame Ports für Amazon Elastic Compute Cloud (Amazon EC2) -Sicherheitsgruppen eingeschränkt sind. Wenn der Zugriff auf Ports nicht auf vertrauenswürdige Quellen beschränkt wird, kann dies zu Angriffen auf die Verfügbarkeit, Integrität und Vertraulichkeit von Systemen führen. Mit dieser Regel können Sie optional die Parameter blockedPort1–blockedPort5 festlegen (Standardkonfigurationen: 20, 21, 3389, 3306, 4333). Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-7(16)	Grenzschutz | Verhinderung der Erkennung von Systemkomponenten	s3- account-level-public-access -Block-periodisch	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Simple Storage Service (Amazon S3) -Buckets nicht öffentlich zugänglich sind. Diese Regel trägt dazu bei, sensible Daten vor unbefugten Remote-Benutzern zu schützen, indem sie den öffentlichen Zugriff verhindert. Mit dieser Regel können Sie optional die Parameter ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) und restrictPublicBuckets Parameter (Config Default: True) festlegen. Die tatsächlichen Werte müssen den Richtlini

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			en Ihrer Organisation entsprechen.
SC-7(16)	Grenzschutz | Verhinderung der Erkennung von Systemkomponenten	s3 bucket-level-public-access - verboten	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Simple Storage Service (Amazon S3) -Buckets nicht öffentlich zugänglich sind. Diese Regel trägt dazu bei, sensible Daten vor unbefugten Remote-Benutzern zu schützen, indem sie den öffentlichen Zugriff auf Bucket-Ebene verhindert.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-7(16)	Grenzschutz | Verhinderung der Erkennung von Systemkomponenten	s-3 bucket-public-read -prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie nur autorisierten Benutzern, Prozessen und Geräten Zugriff auf Amazon Simple Storage Service (Amazon S3) - Buckets gewähren. Die Verwaltung des Zugriffs sollte mit der Klassifizierung der Daten übereinst immen.
SC-7(16)	Grenzschutz | Verhinderung der Erkennung von Systemkomponenten	s3- bucket-public-writ e-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie nur autorisierten Benutzern, Prozessen und Geräten Zugriff auf Amazon Simple Storage Service (Amazon S3) - Buckets gewähren. Die Verwaltung des Zugriffs sollte mit der Klassifizierung der Daten übereinst immen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-7(16)	Grenzschutz | Verhinderung der Erkennung von Systemkomponenten	sagemaker-notebook-no-direct-Internetzugang	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass SageMaker Amazon-Notebooks keinen direkten Internetzugang zulassen. Indem Sie direkten Internetzugang blockieren, vermeiden Sie, dass unbefugte Benutzer auf sensible Daten zugreifen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-7(16)	Grenzschutz | Verhinderung der Erkennung von Systemkomponenten	subnet-auto-assign-public-ip-deaktiviert	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon Virtual Private Cloud (VPC) -Subnetzen nicht automatisch eine öffentliche IP-Adresse zugewiesen wird. Amazon Elastic Compute Cloud (EC2) -Instances, die in Subnetzen gestartet werden, in denen dieses Attribut aktiviert ist, haben ihrer primären Netzwerkschnittstelle eine öffentliche IP-Adresse zugewiesen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-7(16)	Grenzschutz | Verhinderung der Erkennung von Systemkomponenten	vpc-default-security-group-geschlossen	Sicherheitsgruppen von Amazon Elastic Compute Cloud (Amazon EC2) können bei der Verwaltung des Netzwerkzugriffs helfen, indem sie eine statusbehaftete Filterung des ein- und ausgehenden Netzwerkverkehrs zu Ressourcen bereitstellen. AWS Die Beschränk ung des gesamten Datenverkehrs auf die Standardsicherheit sgruppe hilft dabei, den Fernzugriff auf Ihre Ressourcen einzuschränken. AWS

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-7(16)	Grenzschutz | Verhinderung der Erkennung von Systemkomponenten	vpc-sg-open-only-to-authorized-ports	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass gemeinsame Ports für Amazon Elastic Compute Cloud (Amazon EC2) -Sicherheitsgruppen eingeschränkt sind. Wenn der Zugriff auf Ports nicht auf vertrauenswürdige Quellen beschränkt wird, kann dies zu Angriffen auf die Verfügbarkeit, Integrität und Vertraulichkeit von Systemen führen. Durch die Beschränkung des Zugriffs auf Ressourcen innerhalb einer Sicherheitsgruppe aus dem Internet (0.0.0.0/0) kann der Remote-Zugriff auf interne Systeme gesteuert werden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-7(21)	Grenzschutz | Isolierung von Systemkomponenten	autoscaling-launch-config-public-ip-deaktiviert	Wenn Sie Ihre Netzwerkschnittstellen mit einer öffentlichen IP-Adresse konfigurieren, sind die diesen Netzwerkschnittstellen zugehörigen Ressourcen über das Internet erreichbar. EC2 Ressourcen sollten nicht öffentlich zugänglich sein, da dies einen unbeabsichtigten Zugriff auf Ihre Anwendungen oder Server ermöglichen kann.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-7(21)	Grenzschutz | Isolierung von Systemkomponenten	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) Security Groups können bei der Verwaltung des Netzwerkzugriffs helfen, indem sie eine statusbeh aftete Filterung von eingehendem und ausgehendem Netzwerkverkehr zu Ressourcen bereitste llen. AWS Wenn Sie eingehenden (oder entfernten) Datenverk ehr von 0.0.0.0/0 bis Port 22 auf Ihren Ressourcen nicht zulassen, können Sie den Remote-Zugriff einschränken.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-7(21)	Grenzschutz | Isolierung von Systemkomponenten	ec-2 instances-in-vpc	Stellen Sie Amazon Elastic Compute Cloud (Amazon EC2) -Instances innerhalb einer Amazon Virtual Private Cloud (Amazon VPC) bereit, um eine sichere Kommunika tion zwischen einer Instance und anderen Services innerhalb der Amazon VPC zu ermöglichen, ohne dass ein Internet-Gateway, ein NAT-Gerät oder eine VPN-Verbindung erforderlich ist. Der gesamte Datenverk ehr bleibt sicher in der AWS Cloud. Domains, die sich innerhalb einer VPC befinden, verfügen aufgrund ihrer logischen Isolierun g im Vergleich zu Domains mit öffentlic hen Endpunkten über eine zusätzlic he Sicherheitsebene. Weisen Sie EC2

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			Amazon-Instances einer Amazon-VPC zu, um den Zugriff ordnungsgemäß zu verwalten.
SC-7(21)	Grenzschutz | Isolierung von Systemkomponenten	no-unrestricted-route-to-igw	Stellen Sie sicher, dass EC2 Amazon-Routentabellen keine uneingeschränkten Routen zu einem Internet-Gateway enthalten. Durch das Entfernen oder Beschränken des Internetzugangs für Workloads innerhalb von Amazon VPCs können unbeabsic htigte Zugriffe in Ihrer Umgebung reduziert werden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-7(21)	Grenzschutz | Isolierung von Systemkomponenten	redshift-enhanced-vpc-routing-aktiviert	Mit Enhanced-VPC-Routing wird erzwungen, dass der gesamte COPY- und UNLOAD-Datenverkehr zwischen Ihrem Cluster und Datenrepositorys über Ihre Amazon VPC erfolgt. Anschließend können Sie VPC-Features wie Sicherheitsgruppen und Netzwerkzugriffskontrolllisten verwenden, um den Netzwerkverkehr zu schützen. Sie können auch VPC-Flow-Protokolle verwenden, um den Netzwerkverkehr zu überwachen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-7(21)	Grenzschutz | Isolierung von Systemkomponenten	ssm-document-not-public	Stellen Sie sicher, dass AWS Systems Manager (SSM) - Dokumente nicht öffentlich sind, da dies einen unbeabsichtigten Zugriff auf Ihre SSM-Dokumente ermöglichen kann. Ein öffentliches SSM-Dokument kann Informationen über Ihr Konto, Ihre Ressourcen und internen Prozesse preisgeben.
SC-7(21)	Grenzschutz | Isolierung von Systemkomponenten	dms-replication-not-public	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass auf DMS-Replikationsinstanzen nicht öffentlich zugegriffen werden kann. DMS-Replikations-Instances können vertrauliche Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-7(21)	Grenzschutz | Isolierung von Systemkomponenten	ebs-snapshot-public-restorable-überprüfen	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass EBS-Snapshots nicht öffentlich wiederher stellbar sind. EBS-Volume-Snapsho ts können vertrauli che Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.
SC-7(21)	Grenzschutz | Isolierung von Systemkomponenten	ec-2 instance-no-public-ip	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon Elastic Compute Cloud (Amazon EC2) - Instances nicht öffentlich zugänglich sind. EC2 Amazon-Instances können vertrauliche Informati onen enthalten, und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-7(21)	Grenzschutz | Isolierung von Systemkomponenten	elasticsearch-in-vpc-only	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass sich Amazon OpenSearch OpenSearch Service (Service) - Domains innerhalb einer Amazon Virtual Private Cloud (Amazon VPC) befinden. Eine OpenSearch Service-Domain innerhalb einer Amazon VPC ermöglicht die sichere Kommunikation zwischen OpenSearch Service und anderen Services innerhalb der Amazon VPC, ohne dass ein Internet-Gateway, ein NAT-Gerät oder eine VPN-Verbindung erforderlich ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-7(21)	Grenzschutz | Isolierung von Systemkomponenten	emr-master-no-public-ip	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon EMR-Cluster-Masterknoten nicht öffentlich zugänglich sind. Amazon-EMR-Cluster-Hauptknoten können vertrauliche Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.
SC-7(21)	Grenzschutz | Isolierung von Systemkomponenten	lambda-function-public-access-verboten	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass AWS Lambda-Funktionen nicht öffentlich zugänglich sind. Der öffentliche Zugriff kann möglicherweise die Verfügbarkeit von Ressourcen beeinträchtigen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-7(21)	Grenzschutz | Isolierung von Systemkomponenten	lambda-inside-vpc	Stellen Sie AWS Lambda-Funktionen in einer Amazon Virtual Private Cloud (Amazon VPC) bereit, um eine sichere Kommunika tion zwischen einer Funktion und anderen Diensten innerhalb der Amazon VPC zu gewährleisten. Bei dieser Konfiguration sind kein Internet-Gateway, kein NAT-Gerät und keine VPN-Verbindung erforderlich. Der gesamte Datenverk ehr bleibt sicher in der Cloud. AWS Domains, die sich innerhalb einer VPC befinden, verfügen aufgrund ihrer logischen Isolierun g im Vergleich zu Domains mit öffentlic hen Endpunkten über eine zusätzliche Sicherheitsebene. Um den Zugriff ordnungsg emäß zu verwalten,

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			sollten AWS Lambda-Funktionen einer VPC zugewiesen werden.
SC-7(21)	Grenzschutz | Isolierung von Systemkomponenten	opensearch-in-vpc-only	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass sich Amazon OpenSearch Service-Domains innerhalb einer Amazon Virtual Private Cloud (Amazon VPC) befinden. Eine Amazon OpenSearch Service-Domain innerhalb einer Amazon VPC ermöglicht die sichere Kommunikation zwischen Amazon OpenSearch Service und anderen Services innerhalb der Amazon VPC, ohne dass ein Internet-Gateway, ein NAT-Gerät oder eine VPN-Verbindung erforderlich ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-7(21)	Grenzschutz | Isolierung von Systemkomponenten	rds-instance-public-access-überprüfen	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Relational Database Service (Amazon RDS) -Instances nicht öffentlich sind. Amazon-RDS-Datenbank-Instances können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-7(21)	Grenzschutz | Isolierung von Systemkomponenten	rds-snapshots-public-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Relational Database Service (Amazon RDS) -Instances nicht öffentlich sind. Amazon-RDS-Datenbank-Instances können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-7(21)	Grenzschutz | Isolierung von Systemkomponenten	redshift-cluster-public-access-überprüfen	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Redshift Redshift-Cluster nicht öffentlich sind. Amazon-Redshift-Cluster können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-7(21)	Grenzschutz | Isolierung von Systemkomponenten	restricted-common-ports	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass gemeinsame Ports für Amazon Elastic Compute Cloud (Amazon EC2) -Sicherheitsgruppen eingeschränkt sind. Wenn der Zugriff auf Ports nicht auf vertrauenswürdige Quellen beschränkt wird, kann dies zu Angriffen auf die Verfügbarkeit, Integrität und Vertraulichkeit von Systemen führen. Mit dieser Regel können Sie optional die Parameter blockedPort1–blockedPort5 festlegen (Standardkonfigurationen: 20, 21, 3389, 3306, 4333). Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-7(21)	Grenzschutz | Isolierung von Systemkomponenten	s3- account-level-public-access -Block-periodisch	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Simple Storage Service (Amazon S3) -Buckets nicht öffentlich zugänglich sind. Diese Regel trägt dazu bei, sensible Daten vor unbefugten Remote-Benutzern zu schützen, indem sie den öffentlichen Zugriff verhindert. Mit dieser Regel können Sie optional die Parameter ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) und restrictPublicBuckets Parameter (Config Default: True) festlegen. Die tatsächlichen Werte müssen den Richtlini

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			en Ihrer Organisation entsprechen.
SC-7(21)	Grenzschutz | Isolierung von Systemkomponenten	s3 bucket-level-public-access - verboten	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Simple Storage Service (Amazon S3) -Buckets nicht öffentlich zugänglich sind. Diese Regel trägt dazu bei, sensible Daten vor unbefugten Remote-Benutzern zu schützen, indem sie den öffentlichen Zugriff auf Bucket-Ebene verhindert.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-7(21)	Grenzschutz | Isolierung von Systemkomponenten	s-3 bucket-public-read -prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie nur autorisierten Benutzern, Prozessen und Geräten Zugriff auf Amazon Simple Storage Service (Amazon S3) - Buckets gewähren. Die Verwaltung des Zugriffs sollte mit der Klassifizierung der Daten übereinst immen.
SC-7(21)	Grenzschutz | Isolierung von Systemkomponenten	s3- bucket-public-writ e-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie nur autorisierten Benutzern, Prozessen und Geräten Zugriff auf Amazon Simple Storage Service (Amazon S3) - Buckets gewähren. Die Verwaltung des Zugriffs sollte mit der Klassifizierung der Daten übereinst immen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-7(21)	Grenzschutz | Isolierung von Systemkomponenten	sagemaker-notebook-no-direct-Internetzugang	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass SageMaker Amazon-Notebooks keinen direkten Internetzugang zulassen. Indem Sie direkten Internetzugang blockieren, vermeiden Sie, dass unbefugte Benutzer auf sensible Daten zugreifen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-7(21)	Grenzschutz | Isolierung von Systemkomponenten	subnet-auto-assign-public-ip-deaktiviert	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon Virtual Private Cloud (VPC) -Subnetzen nicht automatisch eine öffentliche IP-Adresse zugewiesen wird. Amazon Elastic Compute Cloud (EC2) -Instances, die in Subnetzen gestartet werden, in denen dieses Attribut aktiviert ist, haben ihrer primären Netzwerkschnittstelle eine öffentliche IP-Adresse zugewiesen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-7(21)	Grenzschutz | Isolierung von Systemkomponenten	vpc-default-security-group-geschlossen	Sicherheitsgruppen von Amazon Elastic Compute Cloud (Amazon EC2) können bei der Verwaltung des Netzwerkzugriffs helfen, indem sie eine statusbehaftete Filterung des ein- und ausgehenden Netzwerkverkehrs zu Ressourcen bereitstellen. AWS Die Beschränk ung des gesamten Datenverkehrs auf die Standardsicherheit sgruppe hilft dabei, den Fernzugriff auf Ihre Ressourcen einzuschränken. AWS

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-7(21)	Grenzschutz | Isolierung von Systemkomponenten	vpc-sg-open-only-to-authorized-ports	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass gemeinsame Ports für Amazon Elastic Compute Cloud (Amazon EC2) -Sicherheitsgruppen eingeschränkt sind. Wenn der Zugriff auf Ports nicht auf vertrauenswürdige Quellen beschränkt wird, kann dies zu Angriffen auf die Verfügbarkeit, Integrität und Vertraulichkeit von Systemen führen. Durch die Beschränkung des Zugriffs auf Ressourcen innerhalb einer Sicherheitsgruppe aus dem Internet (0.0.0.0/0) kann der Remote-Zugriff auf interne Systeme gesteuert werden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-7	Grenzschutz	autoscaling-launch-config-public-ip-deaktiviert	Wenn Sie Ihre Netzwerkschnittstellen mit einer öffentlichen IP-Adresse konfigurieren, sind die diesen Netzwerkschnittstellen zugehörigen Ressourcen über das Internet erreichbar. EC2 Ressourcen sollten nicht öffentlich zugänglich sein, da dies einen unbeabsichtigten Zugriff auf Ihre Anwendungen oder Server ermöglichen kann.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-7	Grenzschutz	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) Security Groups können bei der Verwaltung des Netzwerkzugriffs helfen, indem sie eine statusbeh aftete Filterung von eingehendem und ausgehendem Netzwerkverkehr zu Ressourcen bereitste llen. AWS Wenn Sie eingehenden (oder entfernten) Datenverk ehr von 0.0.0.0/0 bis Port 22 auf Ihren Ressourcen nicht zulassen, können Sie den Remote-Zugriff einschränken.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-7	Grenzschutz	ec-2 instances-in-vpc	Stellen Sie Amazon Elastic Compute Cloud (Amazon EC2) -Instances innerhalb einer Amazon Virtual Private Cloud (Amazon VPC) bereit, um eine sichere Kommunika tion zwischen einer Instance und anderen Services innerhalb der Amazon VPC zu ermöglichen, ohne dass ein Internet-Gateway, ein NAT-Gerät oder eine VPN-Verbindung erforderlich ist. Der gesamte Datenverk ehr bleibt sicher in der AWS Cloud. Domains, die sich innerhalb einer VPC befinden, verfügen aufgrund ihrer logischen Isolierun g im Vergleich zu Domains mit öffentlic hen Endpunkten über eine zusätzlic he Sicherheitsebene. Weisen Sie EC2

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			Amazon-Instances einer Amazon-VPC zu, um den Zugriff ordnungsgemäß zu verwalten.
SC-7	Grenzschutz	no-unrestricted-route-to-igw	Stellen Sie sicher, dass EC2 Amazon-Routentabellen keine uneingeschränkten Routen zu einem Internet-Gateway enthalten. Durch das Entfernen oder Beschränken des Internetzugangs für Workloads innerhalb von Amazon VPCs können unbeabsic htigte Zugriffe in Ihrer Umgebung reduziert werden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-7	Grenzschutz	redshift-enhanced-vpc-routing-aktiviert	Mit Enhanced-VPC-Routing wird erzwungen, dass der gesamte COPY- und UNLOAD-Datenverkehr zwischen Ihrem Cluster und Datenrepositorys über Ihre Amazon VPC erfolgt. Anschließend können Sie VPC-Features wie Sicherheitsgruppen und Netzwerkzugriffskontrolllisten verwenden, um den Netzwerkverkehr zu schützen. Sie können auch VPC-Flow-Protokolle verwenden, um den Netzwerkverkehr zu überwachen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-7	Grenzschutz	ssm-document-not-public	Stellen Sie sicher, dass AWS Systems Manager (SSM) - Dokumente nicht öffentlich sind, da dies einen unbeabsichtigten Zugriff auf Ihre SSM-Dokumente ermöglichen kann. Ein öffentliches SSM-Dokument kann Informationen über Ihr Konto, Ihre Ressourcen und internen Prozesse preisgeben.
SC-7	Grenzschutz	dms-replication-not-public	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass auf DMS-Replikationsinstanzen nicht öffentlich zugegriffen werden kann. DMS-Replikations-Instances können vertrauliche Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-7	Grenzschutz	ebs-snapshot-public-restorable-überprüfen	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass EBS-Snapshots nicht öffentlich wiederher stellbar sind. EBS-Volume-Snapsho ts können vertrauli che Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.
SC-7	Grenzschutz	ec-2 instance-no-public-ip	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon Elastic Compute Cloud (Amazon EC2) - Instances nicht öffentlich zugänglich sind. EC2 Amazon-Instances können vertrauliche Informati onen enthalten, und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-7	Grenzschutz	elasticsearch-in-vpc-only	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass sich Amazon OpenSearch OpenSearch Service (Service) - Domains innerhalb einer Amazon Virtual Private Cloud (Amazon VPC) befinden. Eine OpenSearch Service-Domain innerhalb einer Amazon VPC ermöglicht die sichere Kommunikation zwischen OpenSearch Service und anderen Services innerhalb der Amazon VPC, ohne dass ein Internet-Gateway, ein NAT-Gerät oder eine VPN-Verbindung erforderlich ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-7	Grenzschutz	emr-master-no-public-ip	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon EMR-Cluster-Masterknoten nicht öffentlich zugänglich sind. Amazon-EMR-Cluster-Hauptknoten können vertrauliche Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.
SC-7	Grenzschutz	lambda-function-public-access-verboten	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass AWS Lambda-Funktionen nicht öffentlich zugänglich sind. Der öffentliche Zugriff kann möglicherweise die Verfügbarkeit von Ressourcen beeinträchtigen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-7	Grenzschutz	lambda-inside-vpc	Stellen Sie AWS Lambda-Funktionen in einer Amazon Virtual Private Cloud (Amazon VPC) bereit, um eine sichere Kommunika tion zwischen einer Funktion und anderen Diensten innerhalb der Amazon VPC zu gewährleisten. Bei dieser Konfiguration sind kein Internet-Gateway, kein NAT-Gerät und keine VPN-Verbindung erforderlich. Der gesamte Datenverk ehr bleibt sicher in der Cloud. AWS Domains, die sich innerhalb einer VPC befinden, verfügen aufgrund ihrer logischen Isolierun g im Vergleich zu Domains mit öffentlic hen Endpunkten über eine zusätzliche Sicherheitsebene. Um den Zugriff ordnungsg emäß zu verwalten,

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			sollten AWS Lambda-Funktionen einer VPC zugewiesen werden.
SC-7	Grenzschutz	opensearch-in-vpc-only	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass sich Amazon OpenSearch Service-Domains innerhalb einer Amazon Virtual Private Cloud (Amazon VPC) befinden. Eine Amazon OpenSearch Service-Domain innerhalb einer Amazon VPC ermöglicht die sichere Kommunikation zwischen Amazon OpenSearch Service und anderen Services innerhalb der Amazon VPC, ohne dass ein Internet-Gateway, ein NAT-Gerät oder eine VPN-Verbindung erforderlich ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-7	Grenzschutz	rds-instance-public-access-überprüfen	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Relational Database Service (Amazon RDS) -Instances nicht öffentlich sind. Amazon-RDS-Datenbank-Instances können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-7	Grenzschutz	rds-snapshots-public-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Relational Database Service (Amazon RDS) -Instances nicht öffentlich sind. Amazon-RDS-Datenbank-Instances können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-7	Grenzschutz	redshift-cluster-public-access-überprüfen	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Redshift Redshift-Cluster nicht öffentlich sind. Amazon-Redshift-Cluster können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-7	Grenzschutz	restricted-common-ports	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass gemeinsame Ports für Amazon Elastic Compute Cloud (Amazon EC2) -Sicherheitsgruppen eingeschränkt sind. Wenn der Zugriff auf Ports nicht auf vertrauenswürdige Quellen beschränkt wird, kann dies zu Angriffen auf die Verfügbarkeit, Integrität und Vertraulichkeit von Systemen führen. Mit dieser Regel können Sie optional die Parameter blockedPort1–blockedPort5 festlegen (Standardkonfigurationen: 20, 21, 3389, 3306, 4333). Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-7	Grenzschutz	s3- account-level-public-access -Block-periodisch	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Simple Storage Service (Amazon S3) -Buckets nicht öffentlich zugänglich sind. Diese Regel trägt dazu bei, sensible Daten vor unbefugten Remote-Benutzern zu schützen, indem sie den öffentlichen Zugriff verhindert. Mit dieser Regel können Sie optional die Parameter ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) und restrictPublicBuckets Parameter (Config Default: True) festlegen. Die tatsächlichen Werte müssen den Richtlini

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			en Ihrer Organisation entsprechen.
SC-7	Grenzschutz	s3 bucket-level-public-access - verboten	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Simple Storage Service (Amazon S3) -Buckets nicht öffentlich zugänglich sind. Diese Regel trägt dazu bei, sensible Daten vor unbefugten Remote-Benutzern zu schützen, indem sie den öffentlichen Zugriff auf Bucket-Ebene verhindert.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-7	Grenzschutz	s-3 bucket-public-read-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie nur autorisierten Benutzern, Prozessen und Geräten Zugriff auf Amazon Simple Storage Service (Amazon S3) - Buckets gewähren. Die Verwaltung des Zugriffs sollte mit der Klassifizierung der Daten übereinst immen.
SC-7	Grenzschutz	s3- bucket-public-write-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie nur autorisierten Benutzern, Prozessen und Geräten Zugriff auf Amazon Simple Storage Service (Amazon S3) - Buckets gewähren. Die Verwaltung des Zugriffs sollte mit der Klassifizierung der Daten übereinst immen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-7	Grenzschutz	sagemaker-notebook-no-direct-Internetzugang	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass SageMaker Amazon-Notebooks keinen direkten Internetzugang zulassen. Indem Sie direkten Internetzugang blockieren, vermeiden Sie, dass unbefugte Benutzer auf sensible Daten zugreifen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-7	Grenzschutz	subnet-auto-assign-public-ip-deaktiviert	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon Virtual Private Cloud (VPC) -Subnetzen nicht automatisch eine öffentliche IP-Adresse zugewiesen wird. Amazon Elastic Compute Cloud (EC2) -Instances, die in Subnetzen gestartet werden, in denen dieses Attribut aktiviert ist, haben ihrer primären Netzwerkschnittstelle eine öffentliche IP-Adresse zugewiesen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-7	Grenzschutz	vpc-default-security-group-geschlossen	Sicherheitsgruppen von Amazon Elastic Compute Cloud (Amazon EC2) können bei der Verwaltung des Netzwerkzugriffs helfen, indem sie eine statusbehaftete Filterung des ein- und ausgehenden Netzwerkverkehrs zu Ressourcen bereitstellen. AWS Die Beschränk ung des gesamten Datenverkehrs auf die Standardsicherheit sgruppe hilft dabei, den Fernzugriff auf Ihre Ressourcen einzuschränken. AWS

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-7	Grenzschutz	vpc-sg-open-only-to-authorized-ports	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass gemeinsame Ports für Amazon Elastic Compute Cloud (Amazon EC2) -Sicherheitsgruppen eingeschränkt sind. Wenn der Zugriff auf Ports nicht auf vertrauenswürdige Quellen beschränkt wird, kann dies zu Angriffen auf die Verfügbarkeit, Integrität und Vertraulichkeit von Systemen führen. Durch die Beschränkung des Zugriffs auf Ressourcen innerhalb einer Sicherheitsgruppe aus dem Internet (0.0.0.0/0) kann der Remote-Zugriff auf interne Systeme gesteuert werden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-8(1)	Vertraulichkeit und Integrität von Übertragungen | Kryptografischer Schutz	elasticsearch-node-to-node-Verschlüsselungsprüfung	Stellen Sie sicher, dass die node-to-node Verschlüsselung für Amazon OpenSearch Service aktiviert ist. Node-to-nodeVerschlüsselung ermöglicht die TLS 1.2-Verschlüsselung für die gesamte Kommunikation innerhalb der Amazon Virtual Private Cloud (Amazon VPC). Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-8(1)	Vertraulichkeit und Integrität von Übertragungen | Kryptografischer Schutz	elbv-2 acm-certificate-required	Zum Schutz von eventuell vorhanden en sensiblen Daten sowie von Daten während der Übertragung muss die Verschlüsselung für Ihr Elastic Load Balancing aktiviert sein. Verwenden Sie AWS Certificate Manager, um öffentlic he und private SSL/ TLS-Zertifikate mit AWS Diensten und internen Ressource n zu verwalten, bereitzustellen und bereitzustellen.
SC-8(1)	Vertraulichkeit und Integrität von Übertragungen | Kryptografischer Schutz	elb-tls-https-listeners-nur	Stellen Sie sicher, dass Ihre Elastic Load Balancer (ELBs) mit SSL- oder HTTPS-Listenern konfiguriert sind. Um eventuell vorhanden e sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-8(1)	Vertraulichkeit und Integrität von Übertragungen | Kryptografischer Schutz	opensearch-https-required	Da sensible Daten existieren können und um Daten während der Übertragung zu schützen, sollten Sie sicherstellen, dass HTTPS für Verbindungen zu Ihren Amazon OpenSearch Service-Domains aktiviert ist.
SC-8(1)	Vertraulichkeit und Integrität von Übertragungen | Kryptografischer Schutz	opensearch-node-to-node-Verschlüsselungsprüfung	Stellen Sie sicher, dass die node-to-node Verschlüsselung für Amazon OpenSearch Service aktiviert ist. Node-to-nodeVerschlüsselung ermöglicht die TLS 1.2-Verschlüsselung für die gesamte Kommunikation innerhalb der Amazon Virtual Private Cloud (Amazon VPC). Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-8(1)	Vertraulichkeit und Integrität von Übertragungen | Kryptografischer Schutz	alb-http-to-https-Umleitungsprüfung	Um Daten während der Übertragung zu schützen, stellen Sie sicher, dass Ihr Application Load Balancer unverschlüsselte HTTP-Anfragen automatisch an HTTPS umleitet. Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.
SC-8(1)	Vertraulichkeit und Integrität von Übertragungen | Kryptografischer Schutz	api-gw-ssl-enabled	Stellen Sie sicher, dass die REST-API-Stufen von Amazon API Gateway mit SSL-Zertifikaten konfiguriert sind, damit Backend-Systeme überprüfen können, ob Anforderungen von API Gateway stammen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-8(1)	Vertraulichkeit und Integrität von Übertragungen | Kryptografischer Schutz	elb-acm-certificate-required	Zum Schutz von eventuell vorhanden en sensiblen Daten sowie von Daten während der Übertragung muss die Verschlüsselung für Ihr Elastic Load Balancing aktiviert sein. Verwenden Sie AWS Certificate Manager, um öffentlic he und private SSL/ TLS-Zertifikate mit AWS Diensten und internen Ressource n zu verwalten, bereitzustellen und bereitzustellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-8(1)	Vertraulichkeit und Integrität von Übertragungen | Kryptografischer Schutz	redshift-require-tls-ssl	Stellen Sie sicher, dass Ihre Amazon-Redshift-Cluster eine TLS/SSL-Verschlüsselung erfordern, um eine Verbindung zu SQL-Clients herzustellen. Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.
SC-8(1)	Vertraulichkeit und Integrität von Übertragungen | Kryptografischer Schutz	s-3 bucket-ssl-requests-only	Um Daten während der Übertragung zu schützen, stellen Sie sicher, dass Ihre Amazon Simple Storage Service (Amazon S3)-Buckets Anfragen zur Verwendung von Secure Socket Layer (SSL)-Buckets erfordern. Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-8(2)	Vertraulichkeit und Integrität von Übertragungen | Handhabung vor und nach der Übertragung	elasticsearch-node-to-node-Verschlüsselungsprüfung	Stellen Sie sicher, dass die node-to-node Verschlüsselung für Amazon OpenSearch Service aktiviert ist. Node-to-nodeVerschlüsselung ermöglicht die TLS 1.2-Verschlüsselung für die gesamte Kommunikation innerhalb der Amazon Virtual Private Cloud (Amazon VPC). Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.
SC-8(2)	Vertraulichkeit und Integrität von Übertragungen | Handhabung vor und nach der Übertragung	elb-tls-https-listeners-nur	Stellen Sie sicher, dass Ihre Elastic Load Balancer (ELBs) mit SSL- oder HTTPS-Listenern konfiguriert sind. Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-8(2)	Vertraulichkeit und Integrität von Übertragungen | Handhabung vor und nach der Übertragung	opensearch-https-required	Da sensible Daten existieren können und um Daten während der Übertragung zu schützen, sollten Sie sicherstellen, dass HTTPS für Verbindungen zu Ihren Amazon OpenSearch Service-Domains aktiviert ist.
SC-8(2)	Vertraulichkeit und Integrität von Übertragungen | Handhabung vor und nach der Übertragung	opensearch-node-to-node-Verschlüsselungsprüfung	Stellen Sie sicher, dass die node-to-node Verschlüsselung für Amazon OpenSearch Service aktiviert ist. Node-to-nodeVerschlüsselung ermöglicht die TLS 1.2-Verschlüsselung für die gesamte Kommunikation innerhalb der Amazon Virtual Private Cloud (Amazon VPC). Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-8(2)	Vertraulichkeit und Integrität von Übertragungen | Handhabung vor und nach der Übertragung	alb-http-to-https-Umleitungsprüfung	Um Daten während der Übertragung zu schützen, stellen Sie sicher, dass Ihr Application Load Balancer unverschlüsselte HTTP-Anfragen automatisch an HTTPS umleitet. Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.
SC-8(2)	Vertraulichkeit und Integrität von Übertragungen | Handhabung vor und nach der Übertragung	api-gw-ssl-enabled	Stellen Sie sicher, dass die REST-API-Stufen von Amazon API Gateway mit SSL-Zertifikaten konfiguriert sind, damit Backend-Systeme überprüfen können, ob Anforderungen von API Gateway stammen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-8(2)	Vertraulichkeit und Integrität von Übertragungen | Handhabung vor und nach der Übertragung	elb-acm-certificate-required	Zum Schutz von eventuell vorhanden en sensiblen Daten sowie von Daten während der Übertragung muss die Verschlüsselung für Ihr Elastic Load Balancing aktiviert sein. Verwenden Sie AWS Certificate Manager, um öffentlic he und private SSL/ TLS-Zertifikate mit AWS Diensten und internen Ressource n zu verwalten, bereitzustellen und bereitzustellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-8(2)	Vertraulichkeit und Integrität von Übertragungen | Handhabung vor und nach der Übertragung	elbv2- acm-certificate-required	Zum Schutz von eventuell vorhanden en sensiblen Daten sowie von Daten während der Übertragung muss die Verschlüsselung für Ihr Elastic Load Balancing aktiviert sein. Verwenden Sie AWS Certificate Manager, um öffentlic he und private SSL/ TLS-Zertifikate mit AWS Diensten und internen Ressource n zu verwalten, bereitzustellen und bereitzustellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-8(2)	Vertraulichkeit und Integrität von Übertragungen | Handhabung vor und nach der Übertragung	redshift-require-tls-ssl	Stellen Sie sicher, dass Ihre Amazon-Redshift-Cluster eine TLS/SSL-Verschlüsselung erfordern, um eine Verbindung zu SQL-Clients herzustellen. Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.
SC-8(2)	Vertraulichkeit und Integrität von Übertragungen | Handhabung vor und nach der Übertragung	s-3 bucket-ssl-requests-only	Um Daten während der Übertragung zu schützen, stellen Sie sicher, dass Ihre Amazon Simple Storage Service (Amazon S3)-Buckets Anfragen zur Verwendung von Secure Socket Layer (SSL)-Buckets erfordern. Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-8	Vertraulichkeit und Integrität von Übertragungen	elasticsearch-node-to-node-Verschlüsselungsprüfung	Stellen Sie sicher, dass die node-to-node Verschlüsselung für Amazon OpenSearch Service aktiviert ist. Node-to-nodeVerschlüsselung ermöglicht die TLS 1.2-Verschlüsselung für die gesamte Kommunikation innerhalb der Amazon Virtual Private Cloud (Amazon VPC). Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-8	Vertraulichkeit und Integrität von Übertragungen	elbv-2 acm-certificate-required	Zum Schutz von eventuell vorhanden en sensiblen Daten sowie von Daten während der Übertragung muss die Verschlüsselung für Ihr Elastic Load Balancing aktiviert sein. Verwenden Sie AWS Certificate Manager, um öffentlic he und private SSL/ TLS-Zertifikate mit AWS Diensten und internen Ressource n zu verwalten, bereitzustellen und bereitzustellen.
SC-8	Vertraulichkeit und Integrität von Übertragungen	elb-tls-https-listeners-nur	Stellen Sie sicher, dass Ihre Elastic Load Balancer (ELBs) mit SSL- oder HTTPS-Listenern konfiguriert sind. Um eventuell vorhanden e sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-8	Vertraulichkeit und Integrität von Übertragungen	opensearch-https-required	Da sensible Daten existieren können und um Daten während der Übertragung zu schützen, sollten Sie sicherstellen, dass HTTPS für Verbindungen zu Ihren Amazon OpenSearch Service-Domains aktiviert ist.
SC-8	Vertraulichkeit und Integrität von Übertragungen	opensearch-node-to-node-Verschlüsselungsprüfung	Stellen Sie sicher, dass die node-to-node Verschlüsselung für Amazon OpenSearch Service aktiviert ist. Node-to-nodeVerschlüsselung ermöglicht die TLS 1.2-Verschlüsselung für die gesamte Kommunikation innerhalb der Amazon Virtual Private Cloud (Amazon VPC). Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-8	Vertraulichkeit und Integrität von Übertragungen	alb-http-to-https-Umleitungsprüfung	Um Daten während der Übertragung zu schützen, stellen Sie sicher, dass Ihr Application Load Balancer unverschlüsselte HTTP-Anfragen automatisch an HTTPS umleitet. Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.
SC-8	Vertraulichkeit und Integrität von Übertragungen	api-gw-ssl-enabled	Stellen Sie sicher, dass die REST-API-Stufen von Amazon API Gateway mit SSL-Zertifikaten konfiguriert sind, damit Backend-Systeme überprüfen können, ob Anforderungen von API Gateway stammen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-8	Vertraulichkeit und Integrität von Übertragungen	elb-acm-certificate-required	Zum Schutz von eventuell vorhanden en sensiblen Daten sowie von Daten während der Übertragung muss die Verschlüsselung für Ihr Elastic Load Balancing aktiviert sein. Verwenden Sie AWS Certificate Manager, um öffentlic he und private SSL/ TLS-Zertifikate mit AWS Diensten und internen Ressource n zu verwalten, bereitzustellen und bereitzustellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-8	Vertraulichkeit und Integrität von Übertragungen	redshift-require-tls-ssl	Stellen Sie sicher, dass Ihre Amazon-Redshift-Cluster eine TLS/SSL-Verschlüsselung erfordern, um eine Verbindung zu SQL-Clients herzustellen. Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.
SC-8	Vertraulichkeit und Integrität von Übertragungen	s-3 bucket-ssl-requests-only	Um Daten während der Übertragung zu schützen, stellen Sie sicher, dass Ihre Amazon Simple Storage Service (Amazon S3)-Buckets Anfragen zur Verwendung von Secure Socket Layer (SSL)-Buckets erfordern. Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-12(2)	Einrichtung und Verwaltung kryptografischer Schlüssel | Symmetrische Schlüssel	cmk-backing-key-rotation-aktiviert	Aktivieren Sie die Schlüsselrotation, um sicherzustellen, dass Schlüssel rotiert werden, nachdem sie das Ende ihrer Krypto-Periode erreicht haben.
SC-12(2)	Einrichtung und Verwaltung kryptografischer Schlüssel | Symmetrische Schlüssel	kms-cmk-not-scheduled-zum Löschen	Um Daten im Ruhezustand zu schützen, sollten Sie sicherstellen, dass die für den Kunden erforderlichen Masterschlüssel (CMKs) nicht im AWS Key Management Service (AWS KMS) gelöscht werden. Da Schlüssel manchmal gelöscht werden müssen, können Sie mit dieser Regel alle zu löschenden Schlüssel überprüfen, falls ein Schlüssel versehentlich zur Löschung vorgemerkt wurde.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-12(3)	Einrichtung und Verwaltung kryptogra fischer Schlüssel | Asymmetrische Schlüssel	elbv2- acm-certificate-required	Zum Schutz von eventuell vorhanden en sensiblen Daten sowie von Daten während der Übertragung muss die Verschlüsselung für Ihr Elastic Load Balancing aktiviert sein. Verwenden Sie AWS Certificate Manager, um öffentlic he und private SSL/ TLS-Zertifikate mit AWS Diensten und internen Ressource n zu verwalten, bereitzustellen und bereitzustellen.
SC-12(3)	Einrichtung und Verwaltung kryptogra fischer Schlüssel | Asymmetrische Schlüssel	elb-tls-https-listeners-nur	Stellen Sie sicher, dass Ihre Elastic Load Balancer (ELBs) mit SSL- oder HTTPS-Listenern konfiguriert sind. Um eventuell vorhanden e sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-12(3)	Einrichtung und Verwaltung kryptografischer Schlüssel | Asymmetrische Schlüssel	opensearch-https-required	Da sensible Daten existieren können und um Daten während der Übertragung zu schützen, sollten Sie sicherstellen, dass HTTPS für Verbindungen zu Ihren Amazon OpenSearch Service-Domains aktiviert ist.
SC-12(3)	Einrichtung und Verwaltung kryptografischer Schlüssel | Asymmetrische Schlüssel	alb-http-to-https-Umleitungsprüfung	Um Daten während der Übertragung zu schützen, stellen Sie sicher, dass Ihr Application Load Balancer unverschlüsselte HTTP-Anfragen automatisch an HTTPS umleitet. Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-12(3)	Einrichtung und Verwaltung kryptogra fischer Schlüssel | Asymmetrische Schlüssel	api-gw-ssl-enabled	Stellen Sie sicher, dass die REST-API-Stufen von Amazon API Gateway mit SSL-Zertifikaten konfiguri ert sind, damit Backend-Systeme überprüfen können, ob Anforderungen von API Gateway stammen.
SC-12(3)	Einrichtung und Verwaltung kryptogra fischer Schlüssel | Asymmetrische Schlüssel	elb-acm-certificate-required	Zum Schutz von eventuell vorhanden en sensiblen Daten sowie von Daten während der Übertragung muss die Verschlüsselung für Ihr Elastic Load Balancing aktiviert sein. Verwenden Sie AWS Certificate Manager, um öffentlic he und private SSL/ TLS-Zertifikate mit AWS Diensten und internen Ressource n zu verwalten, bereitzustellen und bereitzustellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-12(3)	Einrichtung und Verwaltung kryptografischer Schlüssel | Asymmetrische Schlüssel	s-3 bucket-ssl-requests-only	Um Daten während der Übertragung zu schützen, stellen Sie sicher, dass Ihre Amazon Simple Storage Service (Amazon S3)-Buckets Anfragen zur Verwendung von Secure Socket Layer (SSL)-Buckets erfordern. Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.
SC-12	Einrichtung und Verwaltung kryptografischer Schlüssel	cmk-backing-key-rotation-aktiviert	Aktivieren Sie die Schlüsselrotation, um sicherzustellen, dass Schlüssel rotiert werden, nachdem sie das Ende ihrer Krypto-Periode erreicht haben.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-12	Einrichtung und Verwaltung kryptografischer Schlüssel	kms-cmk-not-scheduled-zum Löschen	Um Daten im Ruhezustand zu schützen, sollten Sie sicherstellen, dass die für den Kunden erforderlichen Masterschlüssel (CMKs) nicht im AWS Key Management Service (AWS KMS) gelöscht werden. Da Schlüssel manchmal gelöscht werden müssen, können Sie mit dieser Regel alle zu löschenden Schlüssel überprüfen, falls ein Schlüssel versehentlich zur Löschung vorgemerkt wurde.
SC-13	Kryptografischer Schutz	codebuild-project-artifact-encryption	Stellen Sie zum Schutz vertraulicher Daten im Speicher sicher, dass die Verschlüsselung für Ihre AWS CodeBuild Artefakte aktiviert ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-13	Kryptografischer Schutz	dynamodb-table-encrypted-kms	Stellen Sie sicher, dass die Verschlüsselung für Ihre Amazon-DynamoDB-Tabellen aktiviert ist. Um eventuell vorhandene sensible Daten im Ruhezustand in diesen Tabellen zu schützen, müssen Sie die Verschlüsselung von Daten im Ruhezustand aktivieren. Standardmäßig werden DynamoDB-Tabellen mit einem AWS eigenen Kundenhauptschlüssel (CMK) verschlüselt.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-13	Kryptografischer Schutz	ec2- ebs-encryption-by-default	Zum Schutz von Daten im Ruhezustand müssen Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon Elastic Block Store (Amazon EBS)-Volumes aktiviert ist. Da sensible Daten auch im Ruhezustand vorhanden sein können, sollten Sie die Verschlüsselung im Ruhezustand aktivieren, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-13	Kryptografischer Schutz	elasticsearch-node-to-node-Verschlüsselungsprüfung	Stellen Sie sicher, dass die node-to-node Verschlüsselung für Amazon OpenSearch Service aktiviert ist. Node-to-nodeVerschlüsselung ermöglicht die TLS 1.2-Verschlüsselung für die gesamte Kommunikation innerhalb der Amazon Virtual Private Cloud (Amazon VPC). Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.
SC-13	Kryptografischer Schutz	elb-tls-https-listeners-nur	Stellen Sie sicher, dass Ihre Elastic Load Balancer (ELBs) mit SSL- oder HTTPS-Listenern konfiguriert sind. Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-13	Kryptografischer Schutz	kinesis-stream-encrypted	Aktivieren Sie die Verschlüsselung für Ihre Amazon-Kinesis-Streams, um eventuell vorhandene sensible Daten sowie Daten im Ruhezustand zu schützen.
SC-13	Kryptografischer Schutz	opensearch-https-required	Da sensible Daten existieren können und um Daten während der Übertragung zu schützen, sollten Sie sicherstellen, dass HTTPS für Verbindungen zu Ihren Amazon OpenSearch Service-Domains aktiviert ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-13	Kryptografischer Schutz	opensearch-node-to-node-Verschlüsselungsprüfung	Stellen Sie sicher, dass die node-to-node Verschlüsselung für Amazon OpenSearch Service aktiviert ist. Node-to-nodeVerschlüsselung ermöglicht die TLS 1.2-Verschlüsselung für die gesamte Kommunikation innerhalb der Amazon Virtual Private Cloud (Amazon VPC). Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-13	Kryptografischer Schutz	rds-snapshot-encrypted	Stellen Sie sicher, dass die Verschlüsselung für Ihre Amazon Relational Database Service (Amazon RDS)-Snapshots aktiviert ist. Da sensible Daten auch im Ruhezustand vorhanden sein können, sollten Sie die Verschlüsselung im Ruhezustand aktivieren, um diese Daten zu schützen.
SC-13	Kryptografischer Schutz	s-3 default-encryption-kms	Stellen Sie sicher, dass die Verschlüsselung für Ihre Amazon Simple Storage Service (Amazon S3)-Buckets aktiviert ist. Um eventuell vorhandene sensible Daten im Ruhezustand in einem Amazon-S3-Bucket zu schützen, muss die Verschlüsselung aktiviert sein.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-13	Kryptografischer Schutz	sagemaker-notebook-instance-kms-key-konfiguriert	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass die Verschlüsselung mit dem AWS Key Management Service (AWS KMS) für Ihr Notebook aktiviert ist. SageMaker Da vertrauliche Daten im SageMaker Notebook gespeichert werden können, sollten Sie die Verschlüsselung im Ruhezustand aktivieren, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-13	Kryptografischer Schutz	sns-encrypted-kms	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass Ihre Amazon Simple Notification Service (Amazon SNS) -Themen mit dem AWS Key Management Service (AWS KMS) verschlüsselt werden müssen. Um eventuell vorhandene sensible Daten im Ruhezustand in veröffentlichten Nachrichten zu schützen, muss die Verschlüsselung von Daten im Ruhezustand aktiviert sein.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-13	Kryptografischer Schutz	alb-http-to-https-Umleitungsprüfung	Um Daten während der Übertragung zu schützen, stellen Sie sicher, dass Ihr Application Load Balancer unverschlüsselte HTTP-Anfragen automatisch an HTTPS umleitet. Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.
SC-13	Kryptografischer Schutz	api-gw-cache-enabled-und-verschlüsselt	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass die Verschlüsselung für den Cache Ihrer API-Gateway-Stufe aktiviert ist. Da für die API-Methode sensible Daten erfasst werden können, sollten Sie die Verschlüsselung von Daten im Ruhezustand aktivieren, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-13	Kryptografischer Schutz	api-gw-ssl-enabled	Stellen Sie sicher, dass die REST-API-Stufen von Amazon API Gateway mit SSL-Zertifikaten konfiguriert sind, damit Backend-Systeme überprüfen können, ob Anforderungen von API Gateway stammen.
SC-13	Kryptografischer Schutz	cloud-trail-encryption-enabled	Da sensible Daten vorhanden sein können und um Daten im Ruhezustand zu schützen, sollten Sie sicherstellen, dass die Verschlüsselung für Ihre AWS CloudTrail Trails aktiviert ist.
SC-13	Kryptografischer Schutz	efs-encrypted-check	Aktivieren Sie die Verschlüsselung für Ihr Amazon Elastic File System (EFS), um eventuell vorhandene sensible Daten sowie Daten im Ruhezustand zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-13	Kryptografischer Schutz	elasticsearch-encrypted-at-rest	Da sensible Daten vorhanden sein können und um Daten im Ruhezustand zu schützen, sollten Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon OpenSearch Service (OpenSearch Service) -Domains aktiviert ist.
SC-13	Kryptografischer Schutz	elb-acm-certificate-required	Zum Schutz von eventuell vorhanden en sensiblen Daten sowie von Daten während der Übertragung muss die Verschlüsselung für Ihr Elastic Load Balancing aktiviert sein. Verwenden Sie AWS Certificate Manager, um öffentlic he und private SSL/ TLS-Zertifikate mit AWS Diensten und internen Ressource n zu verwalten, bereitzustellen und bereitzustellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-13	Kryptografischer Schutz	elbv2- acm-certificate-required	Zum Schutz von eventuell vorhanden en sensiblen Daten sowie von Daten während der Übertragung muss die Verschlüsselung für Ihr Elastic Load Balancing aktiviert sein. Verwenden Sie AWS Certificate Manager, um öffentlic he und private SSL/ TLS-Zertifikate mit AWS Diensten und internen Ressource n zu verwalten, bereitzustellen und bereitzustellen.
SC-13	Kryptografischer Schutz	encrypted-volumes	Aktivieren Sie die Verschlüsselung für Ihre Amazon-Elastic-Block-Store (Amazon-EBS)-Volumes, um eventuell vorhandene sensible Daten sowie Daten im Ruhezusta nd zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-13	Kryptografischer Schutz	opensearch-encrypted-at-rest	Da sensible Daten vorhanden sein können und um Daten im Ruhezustand zu schützen, sollten Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon OpenSearch Service-Domains aktiviert ist.
SC-13	Kryptografischer Schutz	rds-storage-encrypted	Zum Schutz von Daten im Ruhezustand müssen Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon Relational Database Service (Amazon RDS)-Instances aktiviert ist. Um eventuell vorhandene sensible Daten im Ruhezustand in Amazon-RDS-Instances zu schützen, muss die Verschlüsselung von Daten im Ruhezustand aktiviert sein.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-13	Kryptografischer Schutz	redshift-cluster-configuration-check	Um Daten im Ruhezustand zu schützen, muss die Verschlüsselung für Ihre Amazon-Redshift-Cluster aktiviert sein. Sie müssen auch sicherstellen, dass die erforderlichen Konfigurationen auf Amazon-Redshift-Clustern bereitgestellt werden. Die Prüfungsprotokollierung muss aktiviert sein, um Informationen zu Verbindungen und Benutzeraktivitäten in der Datenbank bereitzustellen. Diese Regel erfordert, dass ein Wert für clusterDbEncrypted (Config Default: TRUE) und LoggingEnabled (Config Default: TRUE) gesetzt ist. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-13	Kryptografischer Schutz	redshift-cluster-kms-enabled	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass die Verschlüs selung mit AWS Key Management Service (AWS KMS) für Ihren Amazon Redshift Redshift-Cluster aktiviert ist. Um eventuell vorhanden e sensible Daten im Ruhezustand in Redshift-Clustern zu schützen, muss die Verschlüsselung von Daten im Ruhezusta nd aktiviert sein.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-13	Kryptografischer Schutz	redshift-require-tls-ssl	Stellen Sie sicher, dass Ihre Amazon-Redshift-Cluster eine TLS/SSL-Verschlüsselung erfordern, um eine Verbindung zu SQL-Clients herzustellen. Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.
SC-13	Kryptografischer Schutz	s3- aktiviert bucket-server-side-encryption	Zum Schutz von Daten im Ruhezustand müssen Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon Simple Storage Service (Amazon S3)-Buckets aktiviert ist. Um eventuell vorhandene sensible Daten im Ruhezustand in Amazon-S3-Buckets zu schützen, muss die Verschlüsselung aktiviert sein.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-13	Kryptografischer Schutz	s-3 bucket-ssl-requests-only	Um Daten während der Übertragung zu schützen, stellen Sie sicher, dass Ihre Amazon Simple Storage Service (Amazon S3)-Buckets Anfragen zur Verwendung von Secure Socket Layer (SSL)-Buckets erfordern. Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-13	Kryptografischer Schutz	sagemaker-endpoint-configuration-kms-key-konfiguriert	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass die Verschlüsselung mit dem AWS Key Management Service (AWS KMS) für Ihren Endpunkt aktiviert ist. SageMaker Da sensible Daten auf dem SageMaker Endgerät gespeiche rt werden können, sollten Sie die Verschlüsselung im Ruhezustand aktiviere n, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-13	Kryptografischer Schutz	secretsmanager-using-cmk	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass die Verschlüsselung mit dem AWS Key Management Service (AWS KMS) für AWS Secrets Manager aktiviert ist. Aktivieren Sie die Verschlüsselung von Daten im Ruhezustand, um eventuell vorhandene sensible Daten im Ruhezustand im Secrets Manager zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-23(3)	Sitzungsauthentizität | Eindeutige, systemseitig generierte Sitzungskennungen	elasticsearch-node-to-node-Verschlüsselungsprüfung	Stellen Sie sicher, dass die node-to-node Verschlüsselung für Amazon OpenSearch Service aktiviert ist. Node-to-nodeVerschlüsselung ermöglicht die TLS 1.2-Verschlüsselung für die gesamte Kommunikation innerhalb der Amazon Virtual Private Cloud (Amazon VPC). Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.
SC-23(3)	Sitzungsauthentizität | Eindeutige, systemseitig generierte Sitzungskennungen	elb-tls-https-listeners-nur	Stellen Sie sicher, dass Ihre Elastic Load Balancer (ELBs) mit SSL- oder HTTPS-Listenern konfiguriert sind. Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-23(3)	Sitzungsauthentizität | Eindeutige, systemseitig generierte Sitzungskennungen	opensearch-https-required	Da sensible Daten existieren können und um Daten während der Übertragung zu schützen, sollten Sie sicherstellen, dass HTTPS für Verbindungen zu Ihren Amazon OpenSearch Service-Domains aktiviert ist.
SC-23(3)	Sitzungsauthentizität | Eindeutige, systemseitig generierte Sitzungskennungen	opensearch-node-to-node-Verschlüsselungsprüfung	Stellen Sie sicher, dass die node-to-node Verschlüsselung für Amazon OpenSearch Service aktiviert ist. Node-to-nodeVerschlüsselung ermöglicht die TLS 1.2-Verschlüsselung für die gesamte Kommunikation innerhalb der Amazon Virtual Private Cloud (Amazon VPC). Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-23(3)	Sitzungsauthentizität | Eindeutige, systemseitig generierte Sitzungskennungen	alb-http-to-https-Umleitungsprüfung	Um Daten während der Übertragung zu schützen, stellen Sie sicher, dass Ihr Application Load Balancer unverschlüsselte HTTP-Anfragen automatisch an HTTPS umleitet. Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.
SC-23(3)	Sitzungsauthentizität | Eindeutige, systemseitig generierte Sitzungskennungen	api-gw-ssl-enabled	Stellen Sie sicher, dass die REST-API-Stufen von Amazon API Gateway mit SSL-Zertifikaten konfiguriert sind, damit Backend-Systeme überprüfen können, ob Anforderungen von API Gateway stammen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-23(3)	Sitzungsauthentizität | Eindeutige, systemseitig generierte Sitzungskennungen	elv 2- acm-certificate-required	Zum Schutz von eventuell vorhanden en sensiblen Daten sowie von Daten während der Übertragung muss die Verschlüsselung für Ihr Elastic Load Balancing aktiviert sein. Verwenden Sie AWS Certificate Manager, um öffentlic he und private SSL/ TLS-Zertifikate mit AWS Diensten und internen Ressource n zu verwalten, bereitzustellen und bereitzustellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-23(3)	Sitzungsauthentizität | Eindeutige, systemseitig generierte Sitzungskennungen	redshift-require-tls-ssl	Stellen Sie sicher, dass Ihre Amazon-Redshift-Cluster eine TLS/SSL-Verschlüsselung erfordern, um eine Verbindung zu SQL-Clients herzustellen. Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.
SC-23(3)	Sitzungsauthentizität | Eindeutige, systemseitig generierte Sitzungskennungen	s-3 bucket-ssl-requests-only	Um Daten während der Übertragung zu schützen, stellen Sie sicher, dass Ihre Amazon Simple Storage Service (Amazon S3)-Buckets Anfragen zur Verwendung von Secure Socket Layer (SSL)-Buckets erfordern. Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-23(5)	Sitzungsauthentizität | Zulässige Zertifizierungsstellen	Elb v 2- acm-certificate-required	Zum Schutz von eventuell vorhandenen sensiblen Daten sowie von Daten während der Übertragung muss die Verschlüsselung für Ihr Elastic Load Balancing aktiviert sein. Verwenden Sie AWS Certificate Manager, um öffentliche und private SSL/TLS-Zertifikate mit AWS Diensten und internen Ressourcen zu verwalten, bereitzustellen und bereitzustellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-23(5)	Sitzungsauthentizität | Zulässige Zertifizierungsstellen	elb-acm-certificate-required	Zum Schutz von eventuell vorhandenen sensiblen Daten sowie von Daten während der Übertragung muss die Verschlüsselung für Ihr Elastic Load Balancing aktiviert sein. Verwenden Sie AWS Certificate Manager, um öffentliche und private SSL/TLS-Zertifikate mit AWS Diensten und internen Ressourcen zu verwalten, bereitzustellen und bereitzustellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-23	Sitzungsauthentizität	elasticsearch-node-to-node-Verschlüsselungsprüfung	Stellen Sie sicher, dass die node-to-node Verschlüsselung für Amazon OpenSearch Service aktiviert ist. Node-to-nodeVerschlüsselung ermöglicht die TLS 1.2-Verschlüsselung für die gesamte Kommunikation innerhalb der Amazon Virtual Private Cloud (Amazon VPC). Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.
SC-23	Sitzungsauthentizität	elb-tls-https-listeners-nur	Stellen Sie sicher, dass Ihre Elastic Load Balancer (ELBs) mit SSL- oder HTTPS-Listenern konfiguriert sind. Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-23	Sitzungsauthentizität	opensearch-https-required	Da sensible Daten existieren können und um Daten während der Übertragung zu schützen, sollten Sie sicherstellen, dass HTTPS für Verbindungen zu Ihren Amazon OpenSearch Service-Domains aktiviert ist.
SC-23	Sitzungsauthentizität	opensearch-node-to-node-Verschlüsselungsprüfung	Stellen Sie sicher, dass die node-to-node Verschlüsselung für Amazon OpenSearch Service aktiviert ist. Node-to-nodeVerschlüsselung ermöglicht die TLS 1.2-Verschlüsselung für die gesamte Kommunikation innerhalb der Amazon Virtual Private Cloud (Amazon VPC). Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-23	Sitzungsauthentizität	alb-http-to-https-Umleitungsprüfung	Um Daten während der Übertragung zu schützen, stellen Sie sicher, dass Ihr Application Load Balancer unverschlüsselte HTTP-Anfragen automatisch an HTTPS umleitet. Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.
SC-23	Sitzungsauthentizität	api-gw-ssl-enabled	Stellen Sie sicher, dass die REST-API-Stufen von Amazon API Gateway mit SSL-Zertifikaten konfiguriert sind, damit Backend-Systeme überprüfen können, ob Anforderungen von API Gateway stammen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-23	Sitzungsauthentizität	elb-acm-certificate-required	Zum Schutz von eventuell vorhanden en sensiblen Daten sowie von Daten während der Übertragung muss die Verschlüsselung für Ihr Elastic Load Balancing aktiviert sein. Verwenden Sie AWS Certificate Manager, um öffentlic he und private SSL/ TLS-Zertifikate mit AWS Diensten und internen Ressource n zu verwalten, bereitzustellen und bereitzustellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-23	Sitzungsauthentizität	elbv2- acm-certificate-required	Zum Schutz von eventuell vorhanden en sensiblen Daten sowie von Daten während der Übertragung muss die Verschlüsselung für Ihr Elastic Load Balancing aktiviert sein. Verwenden Sie AWS Certificate Manager, um öffentlic he und private SSL/ TLS-Zertifikate mit AWS Diensten und internen Ressource n zu verwalten, bereitzustellen und bereitzustellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-23	Sitzungsauthentizität	redshift-require-tls-ssl	Stellen Sie sicher, dass Ihre Amazon-Redshift-Cluster eine TLS/SSL-Verschlüsselung erfordern, um eine Verbindung zu SQL-Clients herzustellen. Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.
SC-23	Sitzungsauthentizität	s-3 bucket-ssl-requests-only	Um Daten während der Übertragung zu schützen, stellen Sie sicher, dass Ihre Amazon Simple Storage Service (Amazon S3)-Buckets Anfragen zur Verwendung von Secure Socket Layer (SSL)-Buckets erfordern. Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-28(1)	Schutz von Informationen im Ruhezustand | Kryptografischer Schutz	codebuild-project-artifact-encryption	Um sensible Daten im Ruhezustand zu schützen, stellen Sie sicher, dass die Verschlüsselung für Ihre AWS CodeBuild Artefakte aktiviert ist.
SC-28(1)	Schutz von Informationen im Ruhezustand | Kryptografischer Schutz	dynamodb-table-encrypted-kms	Stellen Sie sicher, dass die Verschlüsselung für Ihre Amazon-DynamoDB-Tabellen aktiviert ist. Um eventuell vorhandene sensible Daten im Ruhezustand in diesen Tabellen zu schützen, müssen Sie die Verschlüsselung von Daten im Ruhezustand aktivieren. Standardmäßig werden DynamoDB-Tabellen mit einem AWS eigenen Kundenhauptschlüssel (CMK) verschlüselt.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-28(1)	Schutz von Informationen im Ruhezustand | Kryptografischer Schutz	ec2- ebs-encryption-by-default	Zum Schutz von Daten im Ruhezustand müssen Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon Elastic Block Store (Amazon EBS)-Volumes aktiviert ist. Da sensible Daten auch im Ruhezustand vorhanden sein können, sollten Sie die Verschlüsselung im Ruhezustand aktivieren, um diese Daten zu schützen.
SC-28(1)	Schutz von Informationen im Ruhezustand | Kryptografischer Schutz	kinesis-stream-encrypted	Aktivieren Sie die Verschlüsselung für Ihre Amazon-Kinesis-Streams, um eventuell vorhandene sensible Daten sowie Daten im Ruhezustand zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-28(1)	Schutz von Informationen im Ruhezustand | Kryptografischer Schutz	rds-snapshot-encrypted	Stellen Sie sicher, dass die Verschlüsselung für Ihre Amazon Relational Database Service (Amazon RDS)-Snapshots aktiviert ist. Da sensible Daten auch im Ruhezustand vorhanden sein können, sollten Sie die Verschlüsselung im Ruhezustand aktivieren, um diese Daten zu schützen.
SC-28(1)	Schutz von Informationen im Ruhezustand | Kryptografischer Schutz	s-3 default-encryption-kms	Stellen Sie sicher, dass die Verschlüsselung für Ihre Amazon Simple Storage Service (Amazon S3)-Buckets aktiviert ist. Um eventuell vorhandene sensible Daten im Ruhezustand in einem Amazon-S3-Bucket zu schützen, muss die Verschlüsselung aktiviert sein.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-28(1)	Schutz von Informationen im Ruhezustand | Kryptografischer Schutz	sagemaker-notebook-instance-kms-key-konfiguriert	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass die Verschlüsselung mit dem AWS Key Management Service (AWS KMS) für Ihr Notebook aktiviert ist. SageMaker Da vertrauliche Daten im SageMaker Notebook gespeichert werden können, sollten Sie die Verschlüsselung im Ruhezustand aktivieren, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-28(1)	Schutz von Informationen im Ruhezustand | Kryptografischer Schutz	sns-encrypted-kms	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass Ihre Amazon Simple Notification Service (Amazon SNS) -Themen mit dem AWS Key Management Service (AWS KMS) verschlüsselt werden müssen. Um eventuell vorhandene sensible Daten im Ruhezustand in veröffentlichten Nachrichten zu schützen, muss die Verschlüsselung von Daten im Ruhezustand aktiviert sein.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-28(1)	Schutz von Informationen im Ruhezustand | Kryptografischer Schutz	api-gw-cache-enabled-und verschlüsselt	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass die Verschlüsselung für den Cache Ihrer API-Gateway-Stufe aktiviert ist. Da für die API-Methode sensible Daten erfasst werden können, sollten Sie die Verschlüsselung von Daten im Ruhezustand aktivieren, um diese Daten zu schützen.
SC-28(1)	Schutz von Informationen im Ruhezustand | Kryptografischer Schutz	cloud-trail-encryption-enabled	Da sensible Daten vorhanden sein können und um Daten im Ruhezustand zu schützen, sollten Sie sicherstellen, dass die Verschlüsselung für Ihre AWS CloudTrail Trails aktiviert ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-28(1)	Schutz von Informationen im Ruhezustand | Kryptografischer Schutz	efs-encrypted-check	Aktivieren Sie die Verschlüsselung für Ihr Amazon Elastic File System (EFS), um eventuell vorhandene sensible Daten sowie Daten im Ruhezustand zu schützen.
SC-28(1)	Schutz von Informationen im Ruhezustand | Kryptografischer Schutz	elasticsearch-encrypted-at-rest	Da sensible Daten vorhanden sein können und um Daten im Ruhezustand zu schützen, sollten Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon OpenSearch Service (OpenSearch Service) -Domains aktiviert ist.
SC-28(1)	Schutz von Informationen im Ruhezustand | Kryptografischer Schutz	encrypted-volumes	Aktivieren Sie die Verschlüsselung für Ihre Amazon-Elastic-Block-Store (Amazon-EBS)-Volumes, um eventuell vorhandene sensible Daten sowie Daten im Ruhezustand zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-28(1)	Schutz von Informationen im Ruhezustand | Kryptografischer Schutz	opensearch-encrypted-at-rest	Da sensible Daten vorhanden sein können und um Daten im Ruhezustand zu schützen, sollten Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon OpenSearch Service-Domains aktiviert ist.
SC-28(1)	Schutz von Informationen im Ruhezustand | Kryptografischer Schutz	rds-storage-encrypted	Zum Schutz von Daten im Ruhezustand müssen Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon Relational Database Service (Amazon RDS)-Instances aktiviert ist. Um eventuell vorhandene sensible Daten im Ruhezustand in Amazon-RDS-Instances zu schützen, muss die Verschlüsselung von Daten im Ruhezustand aktiviert sein.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-28(1)	Schutz von Informationen im Ruhezustand | Kryptografischer Schutz	redshift-cluster-configuration-check	Um Daten im Ruhezustand zu schützen, muss die Verschlüsselung für Ihre Amazon-Redshift-Cluster aktiviert sein. Sie müssen auch sicherstellen, dass die erforderlichen Konfigurationen auf Amazon-Redshift-Clustern bereitgestellt werden. Die Prüfungsprotokollierung muss aktiviert sein, um Informationen zu Verbindungen und Benutzeraktivitäten in der Datenbank bereitzustellen. Diese Regel erfordert, dass ein Wert für clusterDbEncrypted (Config Default: TRUE) und LoggingEnabled (Config Default: TRUE) gesetzt ist. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-28(1)	Schutz von Informationen im Ruhezustand | Kryptografischer Schutz	redshift-cluster-kms-enabled	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass die Verschlüsselung mit AWS Key Management Service (AWS KMS) für Ihren Amazon Redshift Redshift-Cluster aktiviert ist. Um eventuell vorhandene sensible Daten im Ruhezustand in Redshift-Clustern zu schützen, muss die Verschlüsselung von Daten im Ruhezustand aktiviert sein.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-28(1)	Schutz von Informationen im Ruhezustand | Kryptografischer Schutz	s3- aktiviert bucket-server-side-encryption	Zum Schutz von Daten im Ruhezustand müssen Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon Simple Storage Service (Amazon S3)-Buckets aktiviert ist. Um eventuell vorhandene sensible Daten im Ruhezustand in Amazon-S3-Buckets zu schützen, muss die Verschlüsselung aktiviert sein.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-28(1)	Schutz von Informationen im Ruhezustand | Kryptografischer Schutz	sagemaker-endpoint-configuration-kms-key-konfiguriert	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass die Verschlüsselung mit dem AWS Key Management Service (AWS KMS) für Ihren Endpunkt aktiviert ist. SageMaker Da sensible Daten auf dem SageMaker Endgerät gespeichert werden können, sollten Sie die Verschlüsselung im Ruhezustand aktivieren, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-28(1)	Schutz von Informationen im Ruhezustand | Kryptografischer Schutz	secretsmanager-using-cmk	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass die Verschlüsselung mit dem AWS Key Management Service (AWS KMS) für AWS Secrets Manager aktiviert ist. Aktivieren Sie die Verschlüsselung von Daten im Ruhezustand, um eventuell vorhandene sensible Daten im Ruhezustand im Secrets Manager zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-28(3)	Schutz von Informationen im Ruhezustand | Kryptografische Schlüssel	acm-certificate-expiration-check	Stellen Sie sicher, dass die Netzwerkintegrität geschützt ist, indem Sie sicherstellen, dass X509-Zertifikate von AWS ACM ausgestellt werden. Diese Zertifikate müssen gültig und dürfen nicht abgelaufen sein. Für diese Regel ist ein Wert für erforderlich daysToExpiration (Wert für bewährte AWS Grundregeln für Sicherheit: 90). Der tatsächliche Wert muss den Richtlinien Ihrer Organisation entsprechen.
SC-28(3)	Schutz von Informationen im Ruhezustand | Kryptografische Schlüssel	cmk-backing-key-rotation-aktiviert	Aktivieren Sie die Schlüsselrotation, um sicherzustellen, dass Schlüssel rotiert werden, nachdem sie das Ende ihrer Krypto-Periode erreicht haben.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-28	Schutz von Informationen im Ruhezustand	codebuild-project-artifact-encryption	Um sensible Daten im Ruhezustand zu schützen, sollten Sie sicherstellen, dass die Verschlüsselung für Ihre AWS CodeBuild Artefakte aktiviert ist.
SC-28	Schutz von Informationen im Ruhezustand	dynamodb-table-encrypted-kms	Stellen Sie sicher, dass die Verschlüsselung für Ihre Amazon-DynamoDB-Tabellen aktiviert ist. Um eventuell vorhandene sensible Daten im Ruhezustand in diesen Tabellen zu schützen, müssen Sie die Verschlüsselung von Daten im Ruhezustand aktivieren. Standardmäßig werden DynamoDB-Tabellen mit einem AWS eigenen Kundenhauptschlüssel (CMK) verschlüselt.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-28	Schutz von Informationen im Ruhezustand	ec2- ebs-encryption-by-default	Zum Schutz von Daten im Ruhezustand müssen Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon Elastic Block Store (Amazon EBS)-Volumes aktiviert ist. Da sensible Daten auch im Ruhezustand vorhanden sein können, sollten Sie die Verschlüsselung im Ruhezustand aktivieren, um diese Daten zu schützen.
SC-28	Schutz von Informationen im Ruhezustand	kinesis-stream-encrypted	Aktivieren Sie die Verschlüsselung für Ihre Amazon-Kinesis-Streams, um eventuell vorhandene sensible Daten sowie Daten im Ruhezustand zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-28	Schutz von Informationen im Ruhezustand	rds-snapshot-encrypted	Stellen Sie sicher, dass die Verschlüsselung für Ihre Amazon Relational Database Service (Amazon RDS)-Snapshots aktiviert ist. Da sensible Daten auch im Ruhezustand vorhanden sein können, sollten Sie die Verschlüsselung im Ruhezustand aktivieren, um diese Daten zu schützen.
SC-28	Schutz von Informationen im Ruhezustand	s-3 default-encryption-kms	Stellen Sie sicher, dass die Verschlüsselung für Ihre Amazon Simple Storage Service (Amazon S3)-Buckets aktiviert ist. Um eventuell vorhandene sensible Daten im Ruhezustand in einem Amazon-S3-Bucket zu schützen, muss die Verschlüsselung aktiviert sein.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-28	Schutz von Informationen im Ruhezustand	sagemaker-notebook-instance-kms-key-konfiguriert	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass die Verschlüsselung mit dem AWS Key Management Service (AWS KMS) für Ihr Notebook aktiviert ist. SageMaker Da vertrauliche Daten im SageMaker Notebook gespeichert werden können, sollten Sie die Verschlüsselung im Ruhezustand aktivieren, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-28	Schutz von Informationen im Ruhezustand	sns-encrypted-kms	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass Ihre Amazon Simple Notification Service (Amazon SNS) -Themen mit dem AWS Key Management Service (AWS KMS) verschlüsselt werden müssen. Um eventuell vorhandene sensible Daten im Ruhezustand in veröffentlichten Nachrichten zu schützen, muss die Verschlüsselung von Daten im Ruhezustand aktiviert sein.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-28	Schutz von Informationen im Ruhezustand	api-gw-cache-enabled-und verschlüsselt	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass die Verschlüsselung für den Cache Ihrer API-Gateway-Stufe aktiviert ist. Da für die API-Methode sensible Daten erfasst werden können, sollten Sie die Verschlüsselung von Daten im Ruhezustand aktivieren, um diese Daten zu schützen.
SC-28	Schutz von Informationen im Ruhezustand	cloud-trail-encryption-enabled	Da sensible Daten vorhanden sein können und um Daten im Ruhezustand zu schützen, sollten Sie sicherstellen, dass die Verschlüsselung für Ihre AWS CloudTrail Trails aktiviert ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-28	Schutz von Informationen im Ruhezustand	efs-encrypted-check	Aktivieren Sie die Verschlüsselung für Ihr Amazon Elastic File System (EFS), um eventuell vorhandene sensible Daten sowie Daten im Ruhezustand zu schützen.
SC-28	Schutz von Informationen im Ruhezustand	elasticsearch-encrypted-at-rest	Da sensible Daten vorhanden sein können und um Daten im Ruhezustand zu schützen, sollten Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon OpenSearch Service (OpenSearch Service) -Domains aktiviert ist.
SC-28	Schutz von Informationen im Ruhezustand	encrypted-volumes	Aktivieren Sie die Verschlüsselung für Ihre Amazon-Elastic-Block-Store (Amazon-EBS)-Volumes, um eventuell vorhandene sensible Daten sowie Daten im Ruhezustand zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-28	Schutz von Informationen im Ruhezustand	opensearch-encrypted-at-rest	Da sensible Daten vorhanden sein können und um Daten im Ruhezustand zu schützen, sollten Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon OpenSearch Service-Domains aktiviert ist.
SC-28	Schutz von Informationen im Ruhezustand	rds-storage-encrypted	Zum Schutz von Daten im Ruhezustand müssen Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon Relational Database Service (Amazon RDS)-Instances aktiviert ist. Um eventuell vorhandene sensible Daten im Ruhezustand in Amazon-RDS-Instances zu schützen, muss die Verschlüsselung von Daten im Ruhezustand aktiviert sein.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-28	Schutz von Informationen im Ruhezustand	redshift-cluster-configuration-check	Um Daten im Ruhezustand zu schützen, muss die Verschlüsselung für Ihre Amazon-Redshift-Cluster aktiviert sein. Sie müssen auch sicherstellen, dass die erforderlichen Konfigurationen auf Amazon-Redshift-Clustern bereitgestellt werden. Die Prüfungsprotokollierung muss aktiviert sein, um Informationen zu Verbindungen und Benutzeraktivitäten in der Datenbank bereitzustellen. Diese Regel erfordert, dass ein Wert für clusterDbEncrypted (Config Default: TRUE) und LoggingEnabled (Config Default: TRUE) gesetzt ist. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-28	Schutz von Informationen im Ruhezustand	redshift-cluster-kms-enabled	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass die Verschlüsselung mit AWS Key Management Service (AWS KMS) für Ihren Amazon Redshift Redshift-Cluster aktiviert ist. Um eventuell vorhandene sensible Daten im Ruhezustand in Redshift-Clustern zu schützen, muss die Verschlüsselung von Daten im Ruhezustand aktiviert sein.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-28	Schutz von Informationen im Ruhezustand	s3- aktiviert bucket-server-side-encryption	Zum Schutz von Daten im Ruhezustand müssen Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon Simple Storage Service (Amazon S3)-Buckets aktiviert ist. Um eventuell vorhandene sensible Daten im Ruhezustand in Amazon-S3-Buckets zu schützen, muss die Verschlüsselung aktiviert sein.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-28	Schutz von Informationen im Ruhezustand	sagemaker-endpoint-configuration-kms-key-konfiguriert	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass die Verschlüsselung mit dem AWS Key Management Service (AWS KMS) für Ihren Endpunkt aktiviert ist. SageMaker Da sensible Daten auf dem SageMaker Endgerät gespeichert werden können, sollten Sie die Verschlüsselung im Ruhezustand aktivieren, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-28	Schutz von Informationen im Ruhezustand	secretsmanager-using-cmk	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass die Verschlüsselung mit dem AWS Key Management Service (AWS KMS) für AWS Secrets Manager aktiviert ist. Aktivieren Sie die Verschlüsselung von Daten im Ruhezustand, um eventuell vorhandene sensible Daten im Ruhezustand im Secrets Manager zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-36(2)	Verteilte Verarbeitung und Speicherung | Synchronisierung	s-3 bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) unterstützt die Aufrechterhaltung einer angemessenen Kapazität und Verfügbarkeit. CRR ermöglicht das automatische, asynchrone Kopieren von Objekten in Amazon-S3-Buckets, um die Datenverfügbarkeit sicherzustellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-36	Verteilte Verarbeitung und Speicherung	elb-cross-zone-load-Balancing aktiviert	Aktivieren Sie zonenübergreifendes Load Balancing für Ihre Elastic Load Balancer (ELBs), um eine angemessene Kapazität und Verfügbarkeit aufrechtzuerhalten. Zonenübergreifendes Load Balancing reduziert die Notwendigkeit, die gleiche Anzahl von Instances in jeder aktivierten Availability Zone aufrechtzuerhalten. Es verbessert auch die Fähigkeit Ihrer Anwendung, den Verlust einer oder mehrerer Instances zu bewältigen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-36	Verteilte Verarbeitung und Speicherung	dynamodb-autoscaling-enabled	Amazon DynamoDB Auto Scaling verwendet den AWS Application Auto Scaling-Service, um die bereitgestellte Durchsatzkapazität so anzupassen, dass sie automatisch auf tatsächliche Verkehrsmuster reagiert. Auf diese Weise kann eine Tabelle oder ein globaler sekundärer Index die bereitgestellte Lese-/Schreibkapazität erhöhen, um plötzliche Erhöhungen des Datenverkehrs ohne Drosselung zu bewältigen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-36	Verteilte Verarbeitung und Speicherung	rds-multi-az-support	Die Multi-AZ-Unterstützung in Amazon Relational Database Service (Amazon RDS) bietet eine verbesserte Verfügbarkeit und Beständigkeit von Datenbank-Instances. Wenn Sie eine Multi-AZ-Datenbank-Instance bereitstellen, erstellt Amazon RDS automatisch eine primäre Datenbank-Instance und repliziert die Daten synchron auf eine Standby-Instance in einer anderen Availability Zone. Jede Availability Zone läuft auf einer eigenen, physisch getrennten, unabhängigen Infrastruktur und ist auf eine hohe Verfügbarkeit ausgelegt. Im Falle eines Infrastrukturausfalls führt Amazon RDS einen automatis

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			chen Failover zum Standby-Modus durch, sodass Sie den Datenbankbetrieb wieder aufnehmen können, sobald der Failover abgeschlo ssen ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SC-36	Verteilte Verarbeitung und Speicherung	vpc-vpn-2-tunnels-up	Redundante Site-to-Site VPN-Tunnel können implementiert werden, um die Anforderungen an die Ausfallsicherheit zu erfüllen. Es verwendet zwei Tunnel, um die Konnektivität sicherzustellen, falls eine der Site-to-Site VPN-Verbindungen nicht verfügbar ist. Um sich vor einem Verbindungsverlust zu schützen, können Sie für den Fall, dass Ihr Kunden-Gateway nicht verfügbar ist, eine zweite Site-to-Site VPN-Verbindung zu Ihrer Amazon Virtual Private Cloud (Amazon VPC) und Ihrem Virtual Private Gateway einrichten, indem Sie ein zweites Kunden-Gateway verwenden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SI-2(2)	Fehlerkorrektur | Status der automatisierten Fehlerkorrektur	ec2-check managedinstance-patch-compliance-status	Aktivieren Sie diese Regel, um bei der Identifizierung und Dokumentation von Sicherheitslücken in Amazon Elastic Compute Cloud (Amazon EC2) zu helfen. Die Regel prüft, ob die EC2 Amazon-Instance die Patch-Konformität im AWS Systems Manager gemäß den Richtlinien und Verfahren Ihrer Organisation einhält.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SI-2(2)	Fehlerkorrektur | Status der automatisierten Fehlerkorrektur	elastic-beanstalk-managed-updates-aktiviert	Durch die Aktivierung verwalteter Plattform updates für eine Amazon-Elastic-Beanstalk-Umgebung wird sichergestellt, dass die aktuellen verfügbaren Plattform -Fixes, -Updates und -Features für die Umgebung installiert sind. Eine bewährte Methode zur Sicherung von Systemen besteht darin, stets die aktuellen Patches zu installieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SI-2(2)	Fehlerkorrektur | Status der automatisierten Fehlerkorrektur	redshift-cluster-maintenancesettings-check	Diese Regel stellt sicher, dass Amazon-Redshift-Cluster die bevorzugten Einstellungen für Ihre Organisation haben. Insbesondere sorgt sie dafür, dass Cluster bevorzugte Wartungsfenster und automatisierte Aufbewahrungsfristen für Snapshots für die Datenbank haben. Für diese Regel müssen Sie die allowVersionUpgrade festlegen. Der Standardwert ist „true“. Außerdem können Sie optional den Zeitraum preferredMaintenanceWindow (der Standardwert ist sa: 16:00 -sa: 16:30) und den automated SnapshotRetention Zeitraum (der Standardwert ist 1) festlegen. Die tatsächlichen Werte müssen den Richtlini

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			en Ihrer Organisation entsprechen.
SI-2(3)	Fehlerkorrektur | Dauer der Fehlerkorrektur und Benchmarks für Korrekturmaßnahmen	ec2- -Manager instance-managed-by-systems	Eine Bestandsaufnahme der Softwareplattformen und Anwendungen innerhalb des Unternehmens ist möglich, indem Amazon Elastic Compute Cloud (Amazon EC2) - Instances mit AWS Systems Manager verwaltet werden. Verwenden Sie AWS Systems Manager, um detaillierte Systemkonfigurationen, Betriebssystem-Patch-Levels, Namen und Typ der Dienste, Softwareinstallationen, Anwendungsname, Herausgeber und Version sowie andere Details zu Ihrer Umgebung bereitzustellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SI-2(3)	Fehlerkorrektur | Dauer der Fehlerkorrektur und Benchmarks für Korrekturmaßnahmen	ec2-check managedinstance-association-compliance-status	Verwenden Sie AWS Systems Manager Associations, um bei der Inventarisierung von Softwareplattformen und Anwendungen innerhalb eines Unternehmens zu helfen. AWS Systems Manager weist Ihren verwalteten Instanzen einen Konfigurationsstatus zu und ermöglicht es Ihnen, Basiswerte für Betriebssystem-Patch-Levels, Softwareinstallationen, Anwendungskonfigurationen und andere Details zu Ihrer Umgebung festzulegen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SI-2(3)	Fehlerkorrektur | Dauer der Fehlerkorrektur und Benchmarks für Korrekturmaßnahmen	ec2-check managedinstance-patch-compliance-status	Aktivieren Sie diese Regel, um bei der Identifizierung und Dokumentation von Sicherheitslücken in Amazon Elastic Compute Cloud (Amazon EC2) zu helfen. Die Regel prüft, ob die EC2 Amazon-Instance die Patch-Konformität im AWS Systems Manager gemäß den Richtlinien und Verfahren Ihrer Organisation einhält.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SI-2(4)	Fehlerkorrektur | Automatisierte Patch-Management-Tools	ec2-check managedinstance-patch-compliance-status	Aktivieren Sie diese Regel, um bei der Identifizierung und Dokumentation von Sicherheitslücken in Amazon Elastic Compute Cloud (Amazon EC2) zu helfen. Die Regel prüft, ob die EC2 Amazon-Instance die Patch-Konformität im AWS Systems Manager gemäß den Richtlinien und Verfahren Ihrer Organisation einhält.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SI-2(4)	Fehlerkorrektur | Automatisierte Patch-Management-Tools	elastic-beanstalk-managed-updates-aktiviert	Durch die Aktivierung verwalteter Plattform updates für eine Amazon-Elastic-Beanstalk-Umgebung wird sichergestellt, dass die aktuellen verfügbaren Plattform -Fixes, -Updates und -Features für die Umgebung installiert sind. Eine bewährte Methode zur Sicherung von Systemen besteht darin, stets die aktuellen Patches zu installieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SI-2(4)	Fehlerkorrektur | Automatisierte Patch-Management-Tools	redshift-cluster-maintenancesettings-check	Diese Regel stellt sicher, dass Amazon-Redshift-Cluster die bevorzugten Einstellungen für Ihre Organisation haben. Insbesondere sorgt sie dafür, dass Cluster bevorzugte Wartungsfenster und automatisierte Aufbewahrungsfristen für Snapshots für die Datenbank haben. Für diese Regel müssen Sie die allowVersionUpgrade festlegen. Der Standardwert ist „true“. Außerdem können Sie optional den Zeitraum preferredMaintenanceWindow (der Standardwert ist sa: 16:00 -sa: 16:30) und den automated SnapshotRetention Zeitraum (der Standardwert ist 1) festlegen. Die tatsächlichen Werte müssen den Richtlini

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			en Ihrer Organisation entsprechen.
SI-2(5)	Fehlerkorrektur | Automatische Software- und Firmware-Updates	ec2- -check managedinstance-patch-compliance-status	Aktivieren Sie diese Regel, um bei der Identifizierung und Dokumentation von Sicherheitslücken in Amazon Elastic Compute Cloud (Amazon EC2) zu helfen. Die Regel prüft, ob die EC2 Amazon-Instance die Patch-Konformität im AWS Systems Manager gemäß den Richtlinien und Verfahren Ihrer Organisation einhält.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SI-2(5)	Fehlerkorrektur | Automatische Software- und Firmware-Updates	elastic-beanstalk-managed-updates-aktiviert	Durch die Aktivierung verwalteter Plattform updates für eine Amazon-Elastic-Beanstalk-Umgebung wird sichergestellt, dass die aktuellen verfügbaren Plattform -Fixes, -Updates und -Features für die Umgebung installiert sind. Eine bewährte Methode zur Sicherung von Systemen besteht darin, stets die aktuellen Patches zu installieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SI-2(5)	Fehlerkorrektur | Automatische Software- und Firmware-Updates	redshift-cluster-maintenancesettings-check	Diese Regel stellt sicher, dass Amazon-Redshift-Cluster die bevorzugten Einstellungen für Ihre Organisation haben. Insbesondere sorgt sie dafür, dass Cluster bevorzugte Wartungsfenster und automatisierte Aufbewahrungsfristen für Snapshots für die Datenbank haben. Für diese Regel müssen Sie die allowVersionUpgrade festlegen. Der Standardwert ist „true“. Außerdem können Sie optional den Zeitraum preferredMaintenanceWindow (der Standardwert ist sa: 16:00 -sa: 16:30) und den automated SnapshotRetention Zeitraum (der Standardwert ist 1) festlegen. Die tatsächlichen Werte müssen den Richtlini

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			en Ihrer Organisation entsprechen.
SI-2	Fehlerkorrektur	lambda-dlq-check	Aktivieren Sie diese Regel, um das entsprechende Personal über Amazon Simple Queue Service (Amazon SQS) oder Amazon Simple Notification Service (Amazon SNS) zu benachrichtigen, wenn eine Funktion ausgefallen ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SI-2	Fehlerkorrektur	rds-enhanced-monitoring-enabled	Aktivieren Sie Amazon Relational Database Service (Amazon RDS), um die Verfügbarkeit von Amazon RDS zu überwachen. Dies bietet einen detaillierten Einblick in den Zustand Ihrer Amazon-RDS-Datenbank-Instances. Wenn der Amazon-RDS-Speicher mehr als ein zugrunde liegendes physisches Gerät verwendet, erfasst Enhanced Monitoring die Daten für jedes Gerät. Wenn die Amazon-RDS-Datenbank-Instance in einer Multi-AZ-Bereitstellung ausgeführt wird, werden außerdem die Daten für jedes Gerät auf dem sekundären Host sowie die Metriken des sekundären Hosts erfasst.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SI-2	Fehlerkorrektur	autoscaling-group-elb-healthcheck-erforderlich	Die Elastic Load Balancer (ELB) - Zustandsprüfungen für Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling Scaling-Gruppen unterstützen die Aufrechterhaltung einer angemessenen Kapazität und Verfügbarkeit. Der Load Balancer sendet regelmäßig Pings, versucht Verbindungen herzustellen oder sendet Anfragen, um den Zustand der EC2 Amazon-Instances in einer Gruppe mit auto-scaling zu testen. Wenn eine Instance nicht zurückmeldet, wird der Traffic an eine neue EC2 Amazon-Instance gesendet.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SI-2	Fehlerkorrektur	beanstalk-enhanced-health-reporting-aktiviert	AWS Die verbesserte Zustandsberichterstattung von Elastic Beanstalk ermöglicht eine schnellere Reaktion auf Veränderungen im Zustand der zugrunde liegenden Infrastruktur. Diese Änderungen könnten zu einer mangelnden Verfügbarkeit der Anwendung führen. Die erweiterten Zustandsberichte von Elastic Beanstalk bieten eine Statusbeschreibung, um den Schweregrad der identifizierten Probleme einzuschätzen und mögliche Ursachen zu identifizieren, die untersucht werden müssen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SI-2	Fehlerkorrektur	cloudwatch-alarm-action-check	Amazon CloudWatch alarmiert, wenn eine Metrik den Schwellenwert für eine bestimmte Anzahl von Bewertungszeiträumen überschreitet. Der Alarm führt eine oder mehrere Aktionen durch, die vom Wert der Metrik oder des Ausdrucks im Vergleich zu einem Schwellenwert in einer Reihe von Zeiträumen abhängt. Diese Regel erfordert einen Wert für alarmActionRequired (Config Default: True), insufficientDataAction Required (Config Default: True), okActionRequired (Config Default: False). Der tatsächliche Wert muss die Alarmaktionen für Ihre Umgebung widerspiegeln.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SI-2	Fehlerkorrektur	dynamodb-throughput-limit-check	Aktivieren Sie diese Regel, um sicherzustellen, dass die bereitgestellte Durchsatzkapazität in Ihren Amazon-DynamoDB-Tabellen überprüft wird. Dies ist der Umfang der Lese- und Schreibaktivitäten, der von den jeweiligen Tabellen unterstützt werden kann. DynamoDB verwendet diese Informationen für das Reservieren ausreichender Systemressourcen, um Ihren Durchsatz anforderungen gerecht zu werden. Diese Regel generiert eine Warnung, wenn sich der Durchsatz dem Höchstlimit für ein Kundenkonto nähert. Mit dieser Regel können Sie optional die Parameter RCUThreshold Kontoprozentsatz

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			(Konfigurationsstandard: 80) und WCUThreshold Kontoprozentsatz (Konfigurationsstandard: 80) festlegen. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.
SI-2	Fehlerkorrektur	ec2- -check managedinstance-patch-compliance-status	Aktivieren Sie diese Regel, um bei der Identifizierung und Dokumentation von Sicherheitslücken in Amazon Elastic Compute Cloud (Amazon EC2) zu helfen. Die Regel prüft, ob die EC2 Amazon-Instance die Patch-Konformität im AWS Systems Manager gemäß den Richtlinien und Verfahren Ihrer Organisation einhält.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SI-2	Fehlerkorrektur	elastic-beanstalk-managed-updates-aktiviert	Durch die Aktivierung verwalteter Plattform updates für eine Amazon-Elastic-Beanstalk-Umgebung wird sichergestellt, dass die aktuellen verfügbaren Plattform -Fixes, -Updates und -Features für die Umgebung installiert sind. Eine bewährte Methode zur Sicherung von Systemen besteht darin, stets die aktuellen Patches zu installieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SI-2	Fehlerkorrektur	redshift-cluster-maintenancesettings-check	Diese Regel stellt sicher, dass Amazon-Redshift-Cluster die bevorzugten Einstellungen für Ihre Organisation haben. Insbesondere sorgt sie dafür, dass Cluster bevorzugte Wartungsfenster und automatisierte Aufbewahrungsfristen für Snapshots für die Datenbank haben. Für diese Regel müssen Sie die allowVersionUpgrade festlegen. Der Standardwert ist „true“. Außerdem können Sie optional den Zeitraum preferredMaintenanceWindow (der Standardwert ist sa: 16:00 -sa: 16:30) und den automated SnapshotRetention Zeitraum (der Standardwert ist 1) festlegen. Die tatsächlichen Werte müssen den Richtlini

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			en Ihrer Organisation entsprechen.
SI-3(8)	Schutz vor schädlich em Code | Erkennung nicht autorisierter Befehle	elasticsearch-logs-to-cloudwatch	Stellen Sie sicher, dass für Amazon OpenSearch Service-Domains Fehlerpro tokolle aktiviert und zur Aufbewahrung und Beantwortung an Amazon CloudWatc h Logs gestreamt werden. Domain-Fehlerprotokolle sind bei Sicherhei ts- und Zugriffsp rüfungen sowie bei der Diagnose von Verfügbarkeitsprob lemen nützlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SI-3(8)	Schutz vor schädlich em Code | Erkennung nicht autorisierter Befehle	multi-region-cloudtrail-enabled	AWS CloudTrail zeichnet Aktionen und API-Aufrufe der AWS Management Console auf. Sie können feststellen, welche Benutzer und Konten angerufen wurden AWS, von welcher Quell-IP-Adresse aus die Anrufe getätigt wurden und wann die Anrufe erfolgten. CloudTrail übermittelt Protokolldateien aus allen AWS Regionen an Ihren S3-Bucket , wenn MULTI_REG ION_CLOUD _TRAIL_ENABLED aktiviert ist. Außerdem wird beim AWS Start einer neuen Region derselbe Trail in der neuen Region erstellt. CloudTrail Dadurch erhalten Sie automatis ch Protokolldateien mit API-Aktivitäten für die neue Region.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SI-3(8)	Schutz vor schädlich em Code | Erkennung nicht autorisierter Befehle	opensearch-logs-to-cloudwatch	Stellen Sie sicher, dass für Amazon OpenSearch Service-Domains Fehlerpro tokolle aktiviert und zur Aufbewahr ung und Beantwort ung an Amazon CloudWatch Logs gestreamt werden. OpenSearch Service-Fehlerprotokolle können bei Sicherhei ts- und Zugriffsp rüfungen helfen und bei der Diagnose von Verfügbarkeitsprob lemen helfen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SI-3(8)	Schutz vor schädlich em Code | Erkennung nicht autorisierter Befehle	s-3 event-notification s-enabled	Amazon-S3-Ereignis benachrichtigungen können das zuständig e Personal über versehentliche oder vorsätzliche Änderungen an Ihren Bucket-Ob jekten informieren. Zu den Warnen gehören beispiels weise: Erstellung eines neuen Objekts, Entfernung eines Objekts, Wiederher stellung eines Objekts, verloren gegangene und replizierte Objekte.
SI-3(8)	Schutz vor schädlich em Code | Erkennung nicht autorisierter Befehle	cloud-trail-cloud-watch-logs-aktiviert	Verwenden Sie Amazon CloudWatc h , um Protokoll ereignisaktivitäten zentral zu sammeln und zu verwalten. Die Aufnahme von AWS CloudTrail Daten liefert Einzelheiten zu den API-Aufrufaktivitä ten in Ihrem AWS-Konto.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SI-3(8)	Schutz vor schädlich em Code | Erkennung nicht autorisierter Befehle	cloudtrail-enabled	AWS CloudTrail kann bei der Nichtabst reitbarkeit helfen, indem Aktionen und API-Aufrufe der AWS Management Console aufgezeic hnet werden. Sie können die Benutzer und die Benutzer AWS-Konten , die einen AWS Dienst aufgerufen haben, die Quell-IP-Adresse, über die die Aufrufe generiert wurden, und den Zeitpunkt der Anrufe identifiz ieren. Einzelheiten zu den erfassten Daten finden Sie in den AWS CloudTrail Datensatzinhalten.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SI-3(8)	Schutz vor schädlich em Code | Erkennung nicht autorisierter Befehle	cloudtrail-s3-data events-enabled	Die Erfassung von Simple Storage Service (Amazon S3)-Datenereigniss en unterstützt die Erkennung von ungewöhnlichen Aktivitäten. Zu den Details gehören AWS-Konto Informationen über den Zugriff auf einen Amazon S3 S3-Bucket, die IP-Adress e und die Uhrzeit des Ereignisses.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SI-3(8)	Schutz vor schädlich em Code | Erkennung nicht autorisierter Befehle	guardduty-enabled-centralized	Amazon GuardDuty kann mithilfe von Threat Intellige nce Feeds helfen, potenzielle Cybersich erheitsereignisse zu überwachen und zu erkennen. Dazu gehören Listen mit bösartigen IPs und maschinel len Lernmethoden zur Identifizierung unerwarteter, nicht autorisierter und bösartiger Aktivitäten in Ihrer AWS Cloud-Umgebung.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SI-3(8)	Schutz vor schädlich em Code | Erkennung nicht autorisierter Befehle	rds-logging-enabled	Um die Protokoll ierung und Überwachung in Ihrer Umgebung zu erleichtern, stellen Sie sicher, dass die Amazon Relationa l Database Service (Amazon RDS)-Prot okollierung aktiviert ist. Mit der Amazon-RDS-Protokollierung können Sie Ereigniss e wie Verbindungen, Verbindungsabbrüch e, Abfragen oder abgefragte Tabellen erfassen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SI-3(8)	Schutz vor schädlich em Code | Erkennung nicht autorisierter Befehle	redshift-cluster-c onfiguration-check	Um Daten im Ruhezustand zu schützen, muss die Verschlüsselung für Ihre Amazon-Re dshift-Cluster aktiviert sein. Sie müssen auch sicherstellen, dass die erforderl ichen Konfigurationen auf Amazon-Redshift-Clustern bereitges tellt werden. Die Prüfungsprotokolli erung muss aktiviert sein, um Informati onen zu Verbindun gen und Benutzera ktivitäten in der Datenbank bereitzus tellen. Diese Regel erfordert, dass ein Wert für clusterDb Encrypted (Config Default: TRUE) und LoggingEnabled (Config Default: TRUE) gesetzt ist. Die tatsächlichen Werte müssen den Richtlini en Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SI-3(8)	Schutz vor schädlich em Code | Erkennung nicht autorisierter Befehle	s3- bucket-logging-enabled	Die Amazon Simple Storage Service (Amazon S3)-Serverzugriffs protokollierung bietet eine Methode zur Überwachu ng des Netzwerks im Hinblick auf potenzielle Cybersich erheitsereignisse. Die Ereignisse werden überwacht, indem detaillierte Aufzeichn ungen über die Anfragen erfasst werden, die an einen Amazon-S3-Bucket gestellt wurden. Jeder Zugriffsprotokolle intrag enthält Details zu einer einzelnen Zugriffsanfrage. Zu den Details gehören Anforderer, Bucket-Name, Anforderu ngszeit, Anforderu ngsaktion, Antwortst atus und Fehlercode, falls relevant.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SI-4(1)	Systemüberwachung | Systemweites Angriffsmeldesystem	guardduty-enabled-centralized	Amazon GuardDuty kann mithilfe von Threat Intellige nce Feeds helfen, potenzielle Cybersich erheitsereignisse zu überwachen und zu erkennen. Dazu gehören Listen mit bösartigen IPs und maschinel len Lernmethoden zur Identifizierung unerwarteter, nicht autorisierter und bösartiger Aktivitäten in Ihrer AWS Cloud-Umgebung.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SI-4(2)	Systemüberwachung | Automatisierte Tools und Mechanismen für Echtzeitanalysen	guardduty-enabled-centralized	Amazon GuardDuty kann mithilfe von Threat Intellige nce Feeds helfen, potenzielle Cybersich erheitsereignisse zu überwachen und zu erkennen. Dazu gehören Listen mit bösartigen IPs und maschinel len Lernmethoden zur Identifizierung unerwarteter, nicht autorisierter und bösartiger Aktivitäten in Ihrer AWS Cloud-Umgebung.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SI-4(4)	Systemüberwachung | Eingehender und ausgehender Kommunikationsverkehr	s-3 event-notifications-enabled	Amazon-S3-Ereignisbenachrichtigungen können das zuständige Personal über versehentliche oder vorsätzliche Änderungen an Ihren Bucket-Objekten informieren. Zu den Warnen gehören beispielsweise: Erstellung eines neuen Objekts, Entfernung eines Objekts, Wiederherstellung eines Objekts, verloren gegangene und replizierte Objekte.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SI-4(4)	Systemüberwachung | Eingehender und ausgehender Kommunikationsverkehr	guardduty-enabled-centralized	Amazon GuardDuty kann mithilfe von Threat Intelligence Feeds helfen, potenzielle Cybersicherheitsereignisse zu überwachen und zu erkennen. Dazu gehören Listen mit bösartigen IPs und maschinellen Lernmethoden zur Identifizierung unerwarteter, nicht autorisierter und bösartiger Aktivitäten in Ihrer AWS Cloud-Umgebung.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SI-4(5)	Systemüberwachung | Systemseitig generierte Warnungen	cloudwatch-alarm-action-check	Amazon CloudWatch alarmiert, wenn eine Metrik den Schwellenwert für eine bestimmte Anzahl von Bewertungszeiträumen überschreitet. Der Alarm führt eine oder mehrere Aktionen durch, die vom Wert der Metrik oder des Ausdrucks im Vergleich zu einem Schwellenwert in einer Reihe von Zeiträumen abhängt. Diese Regel erfordert einen Wert für alarmActionRequired (Config Default: True), insufficientDataAction Required (Config Default: True), okActionRequired (Config Default: False). Der tatsächliche Wert muss die Alarmaktionen für Ihre Umgebung widerspiegeln.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SI-4(5)	Systemüberwachung | Systemseitig generierte Warnungen	cloud-trail-cloud-watch-logs-aktiviert	Verwenden Sie Amazon CloudWatch , um Protokoll ereignisaktivitäten zentral zu sammeln und zu verwalten. Die Aufnahme von AWS CloudTrail Daten liefert Einzelheiten zu den API-Aufrufaktivitäten in Ihrem AWS-Konto.
SI-4(5)	Systemüberwachung | Systemseitig generierte Warnungen	guardduty-enabled-centralized	Amazon GuardDuty kann mithilfe von Threat Intelligence Feeds helfen, potenzielle Cybersicherheitsereignisse zu überwachen und zu erkennen. Dazu gehören Listen mit bösartigen IPs und maschinellen Lernmethoden zur Identifizierung unerwarteter, nicht autorisierter und bösartiger Aktivitäten in Ihrer AWS Cloud-Umgebung.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SI-4(12)	Systemüberwachung | Automatisierte, von der Organisation generierte Warnungen	cloudwatch-alarm-action-check	Amazon CloudWatch alarmiert, wenn eine Metrik den Schwellenwert für eine bestimmte Anzahl von Bewertungszeiträumen überschreitet. Der Alarm führt eine oder mehrere Aktionen durch, die vom Wert der Metrik oder des Ausdrucks im Vergleich zu einem Schwellenwert in einer Reihe von Zeiträumen abhängt. Diese Regel erfordert einen Wert für alarmActionRequired (Config Default: True), insufficientDataAction Required (Config Default: True), okActionRequired (Config Default: False). Der tatsächliche Wert muss die Alarmaktionen für Ihre Umgebung widerspiegeln.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SI-4(13)	Systemüberwachung | Analyse von Datenverkehrs- und Ereignismustern	guardduty-enabled-centralized	Amazon GuardDuty kann mithilfe von Threat Intellige nce Feeds helfen, potenzielle Cybersich erheitsereignisse zu überwachen und zu erkennen. Dazu gehören Listen mit bösartigen IPs und maschinel len Lernmethoden zur Identifizierung unerwarteter, nicht autorisierter und bösartiger Aktivitäten in Ihrer AWS Cloud-Umgebung.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SI-4(20)	Systemüberwachung | Privilegierte Benutzer	elasticsearch-logs-to-cloudwatch	Stellen Sie sicher, dass für Amazon OpenSearch Service-Domains Fehlerprotokolle aktiviert und zur Aufbewahrung und Beantwortung an Amazon CloudWatch Logs gestreamt werden. Domain-Fehlerprotokolle sind bei Sicherheits- und Zugriffsprüfungen sowie bei der Diagnose von Verfügbarkeitsproblemen nützlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SI-4(20)	Systemüberwachung | Privilegierte Benutzer	multi-region-cloudtrail-enabled	AWS CloudTrail zeichnet Aktionen und API-Aufrufe der AWS Management Console auf. Sie können feststellen, welche Benutzer und Konten angerufen wurden AWS, von welcher Quell-IP-Adresse aus die Anrufe getätigt wurden und wann die Anrufe erfolgten. CloudTrail übermittelt Protokolldateien aus allen AWS Regionen an Ihren S3-Bucket , wenn MULTI_REG ION_CLOUD _TRAIL_ENABLED aktiviert ist. Außerdem wird beim AWS Start einer neuen Region derselbe Trail in der neuen Region erstellt. CloudTrail Dadurch erhalten Sie automatis ch Protokolldateien mit API-Aktivitäten für die neue Region.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SI-4(20)	Systemüberwachung | Privilegierte Benutzer	opensearch-logs-to-cloudwatch	Stellen Sie sicher, dass für Amazon OpenSearch Service-Domains Fehlerprotokolle aktiviert und zur Aufbewahrung und Beantwortung an Amazon CloudWatch Logs gestreamt werden. OpenSearch Service-Fehlerprotokolle können bei Sicherheits- und Zugriffsprüfungen helfen und bei der Diagnose von Verfügbarkeitsproblemen helfen.
SI-4(20)	Systemüberwachung | Privilegierte Benutzer	cloud-trail-cloud-watch-Logs aktiviert	Verwenden Sie Amazon CloudWatch , um Protokollereignisaktivitäten zentral zu sammeln und zu verwalten. Die Aufnahme von AWS CloudTrail Daten liefert Einzelheiten zu den API-Aufrufaktivitäten in Ihrem AWS-Konto.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SI-4(20)	Systemüberwachung | Privilegierte Benutzer	cloudtrail-enabled	AWS CloudTrail kann bei der Nichtabstreitbarkeit helfen, indem Aktionen und API-Aufrufe der AWS Management Console aufgezeichnet werden. Sie können die Benutzer und die Benutzer AWS-Konten , die einen AWS Dienst aufgerufen haben, die Quell-IP-Adresse, über die die Aufrufe generiert wurden, und den Zeitpunkt der Anrufe identifizieren. Einzelheiten zu den erfassten Daten finden Sie in den AWS CloudTrail Datensatzinhalten.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SI-4(20)	Systemüberwachung | Privilegierte Benutzer	cloudtrail-s3-data events-enabled	Die Erfassung von Simple Storage Service (Amazon S3)-Datenereignissen unterstützt die Erkennung von ungewöhnlichen Aktivitäten. Zu den Details gehören AWS-Konto Informationen über den Zugriff auf einen Amazon S3 S3-Bucket, die IP-Adresse und die Uhrzeit des Ereignisses.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SI-4(20)	Systemüberwachung | Privilegierte Benutzer	rds-logging-enabled	Um die Protokollierung und Überwachung in Ihrer Umgebung zu erleichtern, stellen Sie sicher, dass die Amazon Relational Database Service (Amazon RDS)-Protokollierung aktiviert ist. Mit der Amazon-RDS-Protokollierung können Sie Ereignisse wie Verbindungen, Verbindungsabbrüche, Abfragen oder abgefragte Tabellen erfassen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SI-4(20)	Systemüberwachung | Privilegierte Benutzer	redshift-cluster-configuration-check	Um Daten im Ruhezustand zu schützen, muss die Verschlüsselung für Ihre Amazon-Redshift-Cluster aktiviert sein. Sie müssen auch sicherstellen, dass die erforderlichen Konfigurationen auf Amazon-Redshift-Clustern bereitgestellt werden. Die Prüfungsprotokollierung muss aktiviert sein, um Informationen zu Verbindungen und Benutzeraktivitäten in der Datenbank bereitzustellen. Diese Regel erfordert, dass ein Wert für clusterDbEncrypted (Config Default: TRUE) und LoggingEnabled (Config Default: TRUE) gesetzt ist. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SI-4(20)	Systemüberwachung | Privilegierte Benutzer	s3- bucket-logging-enabled	Die Amazon Simple Storage Service (Amazon S3)-Serverzugriffs protokollierung bietet eine Methode zur Überwachu ng des Netzwerks im Hinblick auf potenzielle Cybersich erheitsereignisse. Die Ereignisse werden überwacht, indem detaillierte Aufzeichn ungen über die Anfragen erfasst werden, die an einen Amazon-S3-Bucket gestellt wurden. Jeder Zugriffsprotokolle intrag enthält Details zu einer einzelnen Zugriffsanfrage. Zu den Details gehören Anforderer, Bucket-Name, Anforderu ngszeit, Anforderu ngsaktion, Antwortst atus und Fehlercode, falls relevant.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SI-4(22)	Systemüberwachung | Nicht autorisierte Netzwerkservices	guardduty-enabled-centralized	Amazon GuardDuty kann mithilfe von Threat Intellige nce Feeds helfen, potenzielle Cybersich erheitsereignisse zu überwachen und zu erkennen. Dazu gehören Listen mit bösartigen IPs und maschinel len Lernmethoden zur Identifizierung unerwarteter, nicht autorisierter und bösartiger Aktivitäten in Ihrer AWS Cloud-Umgebung.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SI-4(25)	Systemüberwachung | Optimierung von Netzwerkverkehrsanalysen	guardduty-enabled-centralized	Amazon GuardDuty kann mithilfe von Threat Intelligence Feeds helfen, potenzielle Cybersicherheitsereignisse zu überwachen und zu erkennen. Dazu gehören Listen mit bösartigen IPs und maschinellen Lernmethoden zur Identifizierung unerwarteter, nicht autorisierter und bösartiger Aktivitäten in Ihrer AWS Cloud-Umgebung.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SI-4	Systemüberwachung	s-3 event-notification s-enabled	Amazon-S3-Ereignis benachrichtigungen können das zuständig e Personal über versehentliche oder vorsätzliche Änderungen an Ihren Bucket-Ob jekten informieren. Zu den Warnen gehören beispiels weise: Erstellung eines neuen Objekts, Entfernung eines Objekts, Wiederher stellung eines Objekts, verloren gegangene und replizierte Objekte.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SI-4	Systemüberwachung	cloud-trail-log-file-Validierung aktiviert	Verwenden Sie die AWS CloudTrail Protokolldateivalidierung, um die Integrität von Protokollen zu überprüfen. CloudTrail Mithilfe der Protokolldateivalidierung kann festgestellt werden, ob eine Protokolldatei geändert oder gelöscht wurde oder ob sie nach der Übermittlung CloudTrail unverändert geblieben ist. Dieses Feature wurde mit dem Branchenstandard entsprechenden Algorithmen entwickelt: SHA-256 für die Hashfunktion und SHA-256 mit RSA für digitale Signaturen. Das macht es rechnerisch unmöglich, CloudTrail Protokolldateien unbemerkt zu ändern, zu löschen oder zu fälschen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SI-4	Systemüberwachung	guardduty-enabled-centralized	Amazon GuardDuty kann mithilfe von Threat Intellige nce Feeds helfen, potenzielle Cybersich erheitsereignisse zu überwachen und zu erkennen. Dazu gehören Listen mit bösartigen IPs und maschinel len Lernmethoden zur Identifizierung unerwarteter, nicht autorisierter und bösartiger Aktivitäten in Ihrer AWS Cloud-Umgebung.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SI-7(1)	Software-, Firmware- und Informationsintegrität | Zustandsprüfungen	cloud-trail-log-file-Validierung aktiviert	Verwenden Sie die AWS CloudTrail Protokolldateivalidierung, um die Integrität von Protokollen zu überprüfen. CloudTrail Mithilfe der Protokolldateivalidierung kann festgestellt werden, ob eine Protokolldatei geändert oder gelöscht wurde oder ob sie nach der Übermittlung CloudTrail unverändert geblieben ist. Dieses Feature wurde mit dem Branchenstandard entsprechenden Algorithmen entwickelt: SHA-256 für die Hashfunktion und SHA-256 mit RSA für digitale Signaturen. Das macht es rechnerisch unmöglich, CloudTrail Protokolldateien unbemerkt zu ändern, zu löschen oder zu fälschen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SI-7(3)	Software-, Firmware- und Informationsintegrität | Zentral verwaltete Integritätstools	cloud-trail-log-file-Validierung aktiviert	Verwenden Sie die AWS CloudTrail Protokolldateivalidierung, um die Integrität von Protokollen zu überprüfen. CloudTrail Mithilfe der Protokolldateivalidierung kann festgestellt werden, ob eine Protokolldatei geändert oder gelöscht wurde oder ob sie nach der Übermittlung CloudTrail unverändert geblieben ist. Dieses Feature wurde mit dem Branchenstandard entsprechenden Algorithmen entwickelt: SHA-256 für die Hashfunktion und SHA-256 mit RSA für digitale Signaturen. Das macht es rechnerisch unmöglich, CloudTrail Protokolldateien unbemerkt zu ändern, zu löschen oder zu fälschen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SI-7(6)	Software-, Firmware- und Informationsintegrität | Kryptografischer Schutz	codebuild-project-artifact-encryption	Um sensible Daten im Speicher zu schützen, sollten Sie sicherstellen, dass die Verschlüsselung für Ihre Artefakte aktiviert ist. AWS CodeBuild
SI-7(6)	Software-, Firmware- und Informationsintegrität | Kryptografischer Schutz	dynamodb-table-encrypted-kms	Stellen Sie sicher, dass die Verschlüsselung für Ihre Amazon-DynamoDB-Tabellen aktiviert ist. Um eventuell vorhandene sensible Daten im Ruhezustand in diesen Tabellen zu schützen, müssen Sie die Verschlüsselung von Daten im Ruhezustand aktivieren. Standardmäßig werden DynamoDB-Tabellen mit einem AWS eigenen Kundenhauptschlüssel (CMK) verschlüselt.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SI-7(6)	Software-, Firmware- und Informationsintegrität | Kryptografischer Schutz	ec2- ebs-encryption-by-default	Zum Schutz von Daten im Ruhezustand müssen Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon Elastic Block Store (Amazon EBS)-Volumes aktiviert ist. Da sensible Daten auch im Ruhezustand vorhanden sein können, sollten Sie die Verschlüsselung im Ruhezustand aktivieren, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SI-7(6)	Software-, Firmware- und Informationsintegrität | Kryptografischer Schutz	elv 2- acm-certificate-required	Zum Schutz von eventuell vorhanden en sensiblen Daten sowie von Daten während der Übertragung muss die Verschlüsselung für Ihr Elastic Load Balancing aktiviert sein. Verwenden Sie AWS Certificate Manager, um öffentlic he und private SSL/ TLS-Zertifikate mit AWS Diensten und internen Ressource n zu verwalten, bereitzustellen und bereitzustellen.
SI-7(6)	Software-, Firmware- und Informationsintegrität | Kryptografischer Schutz	elb-tls-https-listeners-nur	Stellen Sie sicher, dass Ihre Elastic Load Balancer (ELBs) mit SSL- oder HTTPS-Listenern konfiguriert sind. Um eventuell vorhanden e sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SI-7(6)	Software-, Firmware- und Informationsintegrität | Kryptografischer Schutz	kinesis-stream-encrypted	Aktivieren Sie die Verschlüsselung für Ihre Amazon-Kinesis-Streams, um eventuell vorhandene sensible Daten sowie Daten im Ruhezustand zu schützen.
SI-7(6)	Software-, Firmware- und Informationsintegrität | Kryptografischer Schutz	opensearch-https-required	Da sensible Daten existieren können und um Daten während der Übertragung zu schützen, sollten Sie sicherstellen, dass HTTPS für Verbindungen zu Ihren Amazon OpenSearch Service-Domains aktiviert ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SI-7(6)	Software-, Firmware- und Informationsintegrität | Kryptografischer Schutz	rds-snapshot-encrypted	Stellen Sie sicher, dass die Verschlüsselung für Ihre Amazon Relational Database Service (Amazon RDS)-Snapshots aktiviert ist. Da sensible Daten auch im Ruhezustand vorhanden sein können, sollten Sie die Verschlüsselung im Ruhezustand aktivieren, um diese Daten zu schützen.
SI-7(6)	Software-, Firmware- und Informationsintegrität | Kryptografischer Schutz	s3- default-encryption-kms	Stellen Sie sicher, dass die Verschlüsselung für Ihre Amazon Simple Storage Service (Amazon S3)-Buckets aktiviert ist. Um eventuell vorhandene sensible Daten im Ruhezustand in einem Amazon-S3-Bucket zu schützen, muss die Verschlüsselung aktiviert sein.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SI-7(6)	Software-, Firmware- und Informationsintegrität | Kryptografischer Schutz	sagemaker-notebook-instance-kms-key-konfiguriert	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass die Verschlüsselung mit dem AWS Key Management Service (AWS KMS) für Ihr Notebook aktiviert ist. SageMaker Da vertrauliche Daten im SageMaker Notebook gespeichert werden können, sollten Sie die Verschlüsselung im Ruhezustand aktivieren, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SI-7(6)	Software-, Firmware- und Informationsintegrität | Kryptografischer Schutz	sns-encrypted-kms	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass Ihre Amazon Simple Notification Service (Amazon SNS) -Themen mit dem AWS Key Management Service (AWS KMS) verschlüsselt werden müssen. Um eventuell vorhandene sensible Daten im Ruhezustand in veröffentlichten Nachrichten zu schützen, muss die Verschlüsselung von Daten im Ruhezustand aktiviert sein.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SI-7(6)	Software-, Firmware- und Informationsintegrität | Kryptografischer Schutz	alb-http-to-https-Umleitungsprüfung	Um Daten während der Übertragung zu schützen, stellen Sie sicher, dass Ihr Application Load Balancer unverschlüsselte HTTP-Anfragen automatisch an HTTPS umleitet. Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.
SI-7(6)	Software-, Firmware- und Informationsintegrität | Kryptografischer Schutz	api-gw-cache-enabled-und-verschlüsselt	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass die Verschlüsselung für den Cache Ihrer API-Gateway-Stufe aktiviert ist. Da für die API-Methode sensible Daten erfasst werden können, sollten Sie die Verschlüsselung von Daten im Ruhezustand aktivieren, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SI-7(6)	Software-, Firmware- und Informationsintegrität | Kryptografischer Schutz	api-gw-ssl-enabled	Stellen Sie sicher, dass die REST-API-Stufen von Amazon API Gateway mit SSL-Zertifikaten konfiguriert sind, damit Backend-Systeme überprüfen können, ob Anforderungen von API Gateway stammen.
SI-7(6)	Software-, Firmware- und Informationsintegrität | Kryptografischer Schutz	cloud-trail-encryption-enabled	Da sensible Daten vorhanden sein können und um Daten im Ruhezustand zu schützen, sollten Sie sicherstellen, dass die Verschlüsselung für Ihre AWS CloudTrail Trails aktiviert ist.
SI-7(6)	Software-, Firmware- und Informationsintegrität | Kryptografischer Schutz	efs-encrypted-check	Aktivieren Sie die Verschlüsselung für Ihr Amazon Elastic File System (EFS), um eventuell vorhandene sensible Daten sowie Daten im Ruhezustand zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SI-7(6)	Software-, Firmware- und Informationsintegrität | Kryptografischer Schutz	elasticsearch-encrypted-at-rest	Da sensible Daten vorhanden sein können und um Daten im Ruhezustand zu schützen, sollten Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon OpenSearch Service (OpenSearch Service) -Domains aktiviert ist.
SI-7(6)	Software-, Firmware- und Informationsintegrität | Kryptografischer Schutz	elb-acm-certificate-required	Zum Schutz von eventuell vorhandenen sensiblen Daten sowie von Daten während der Übertragung muss die Verschlüsselung für Ihr Elastic Load Balancing aktiviert sein. Verwenden Sie AWS Certificate Manager, um öffentliche und private SSL/TLS-Zertifikate mit AWS Diensten und internen Ressourcen zu verwalten, bereitzustellen und bereitzustellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SI-7(6)	Software-, Firmware- und Informationsintegrität | Kryptografischer Schutz	encrypted-volumes	Aktivieren Sie die Verschlüsselung für Ihre Amazon-Elastic-Block-Store (Amazon-EBS)-Volumes, um eventuell vorhandene sensible Daten sowie Daten im Ruhezustand zu schützen.
SI-7(6)	Software-, Firmware- und Informationsintegrität | Kryptografischer Schutz	opensearch-encrypted-at-rest	Da sensible Daten vorhanden sein können und um Daten im Ruhezustand zu schützen, sollten Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon OpenSearch Service-Domains aktiviert ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SI-7(6)	Software-, Firmware- und Informationsintegrität | Kryptografischer Schutz	rds-storage-encrypted	Zum Schutz von Daten im Ruhezustand müssen Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon Relational Database Service (Amazon RDS)-Instances aktiviert ist. Um eventuell vorhandene sensible Daten im Ruhezustand in Amazon-RDS-Instances zu schützen, muss die Verschlüsselung von Daten im Ruhezustand aktiviert sein.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SI-7(6)	Software-, Firmware- und Informationsintegrität | Kryptografischer Schutz	redshift-cluster-configuration-check	Um Daten im Ruhezustand zu schützen, muss die Verschlüsselung für Ihre Amazon-Redshift-Cluster aktiviert sein. Sie müssen auch sicherstellen, dass die erforderlichen Konfigurationen auf Amazon-Redshift-Clustern bereitgestellt werden. Die Prüfungsprotokollierung muss aktiviert sein, um Informationen zu Verbindungen und Benutzeraktivitäten in der Datenbank bereitzustellen. Diese Regel erfordert, dass ein Wert für clusterDbEncrypted (Config Default: TRUE) und LoggingEnabled (Config Default: TRUE) gesetzt ist. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SI-7(6)	Software-, Firmware- und Informationsintegrität | Kryptografischer Schutz	redshift-cluster-kms-enabled	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass die Verschlüsselung mit AWS Key Management Service (AWS KMS) für Ihren Amazon Redshift Redshift-Cluster aktiviert ist. Um eventuell vorhandene sensible Daten im Ruhezustand in Redshift-Clustern zu schützen, muss die Verschlüsselung von Daten im Ruhezustand aktiviert sein.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SI-7(6)	Software-, Firmware- und Informationsintegrität | Kryptografischer Schutz	s3- aktiviert bucket-server-side-encryption	Zum Schutz von Daten im Ruhezustand müssen Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon Simple Storage Service (Amazon S3)-Buckets aktiviert ist. Um eventuell vorhandene sensible Daten im Ruhezustand in Amazon-S3-Buckets zu schützen, muss die Verschlüsselung aktiviert sein.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SI-7(6)	Software-, Firmware- und Informationsintegrität | Kryptografischer Schutz	s-3 bucket-ssl-requests-only	Um Daten während der Übertragung zu schützen, stellen Sie sicher, dass Ihre Amazon Simple Storage Service (Amazon S3)-Buckets Anfragen zur Verwendung von Secure Socket Layer (SSL)-Buckets erfordern. Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SI-7(6)	Software-, Firmware- und Informationsintegrität | Kryptografischer Schutz	sagemaker-endpoint-configuration-kms-key-konfiguriert	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass die Verschlüsselung mit dem AWS Key Management Service (AWS KMS) für Ihren Endpunkt aktiviert ist. SageMaker Da sensible Daten auf dem SageMaker Endgerät gespeichert werden können, sollten Sie die Verschlüsselung im Ruhezustand aktivieren, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SI-7(6)	Software-, Firmware- und Informationsintegrität | Kryptografischer Schutz	secretsmanager-using-cmk	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass die Verschlüsselung mit dem AWS Key Management Service (AWS KMS) für AWS Secrets Manager aktiviert ist. Aktivieren Sie die Verschlüsselung von Daten im Ruhezustand, um eventuell vorhandene sensible Daten im Ruhezustand im Secrets Manager zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SI-7(7)	Software-, Firmware- und Informationsintegrität | Integration von Erkennung und Reaktion	cloud-trail-log-file-Validierung aktiviert	Verwenden Sie die AWS CloudTrail Protokolldateivalidierung, um die Integrität von Protokollen zu überprüfen. CloudTrail Mithilfe der Protokolldateivalidierung kann festgestellt werden, ob eine Protokolldatei geändert oder gelöscht wurde oder ob sie nach der Übermittlung CloudTrail unverändert geblieben ist. Dieses Feature wurde mit dem Branchenstandard entsprechenden Algorithmen entwickelt: SHA-256 für die Hashfunktion und SHA-256 mit RSA für digitale Signaturen. Das macht es rechnerisch unmöglich, CloudTrail Protokolldateien unbemerkt zu ändern, zu löschen oder zu fälschen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SI-7(8)	Software-, Firmware- und Informationsintegrität | Fähigkeit zur Prüfung wichtiger Ereignisse	elasticsearch-logs-to-cloudwatch	Stellen Sie sicher, dass für Amazon OpenSearch Service-Domains Fehlerprotokolle aktiviert und zur Aufbewahrung und Beantwortung an Amazon CloudWatch Logs gestreamt werden. Domain-Fehlerprotokolle sind bei Sicherheits- und Zugriffsprüfungen sowie bei der Diagnose von Verfügbarkeitsproblemen nützlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SI-7(8)	Software-, Firmware- und Informationsintegrität | Fähigkeit zur Prüfung wichtiger Ereignisse	multi-region-cloudtrail-enabled	AWS CloudTrail zeichnet Aktionen und API-Aufrufe der AWS Management Console auf. Sie können feststellen, welche Benutzer und Konten angerufen wurden AWS, von welcher Quell-IP-Adresse aus die Anrufe getätigt wurden und wann die Anrufe erfolgten. CloudTrail übermittelt Protokolldateien aus allen AWS Regionen an Ihren S3-Bucket , wenn MULTI_REGION_CLOUD_TRAIL_ENABLED aktiviert ist. Außerdem wird beim AWS Start einer neuen Region derselbe Trail in der neuen Region erstellt. CloudTrail Dadurch erhalten Sie automatisch Protokolldateien mit API-Aktivitäten für die neue Region.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SI-7(8)	Software-, Firmware- und Informationsintegrität | Fähigkeit zur Prüfung wichtiger Ereignisse	opensearch-logs-to-cloudwatch	Stellen Sie sicher, dass für Amazon OpenSearch Service-Domains Fehlerprotokolle aktiviert und zur Aufbewahrung und Beantwortung an Amazon CloudWatch Logs gestreamt werden. OpenSearch Service-Fehlerprotokolle können bei Sicherheits- und Zugriffsprüfungen helfen und bei der Diagnose von Verfügbarkeitsproblemen helfen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SI-7(8)	Software-, Firmware- und Informationsintegrität | Fähigkeit zur Prüfung wichtiger Ereignisse	wafv2-logging-enabled	Um die Protokollierung und Überwachung in Ihrer Umgebung zu erleichtern, aktivieren Sie die AWS WAF (V2) -Protokollierung im regionalen und globalen Internet ACLs. AWS Die WAF-Protokollierung bietet detaillierte Informationen über den Datenverkehr, der von Ihrer Web-ACL analysiert wird. In den Protokollen werden die Uhrzeit aufgezeichnet, zu der die AWS WAF die Anfrage von Ihrer AWS Ressource erhalten hat, Informationen über die Anfrage und eine Aktion für die Regel, der jede Anfrage entsprach.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SI-7(8)	Software-, Firmware- und Informationsintegrität | Fähigkeit zur Prüfung wichtiger Ereignisse	api-gw-execution-logging-aktiviert	Die API-Gateway-Protokollierung zeigt detaillierte Ansichten der Benutzer, die auf die API zugegriffen haben, und wie diese Benutzer auf die API zugegriffen haben. Diese Einblicke ermöglichen die Transparenz von Benutzeraktivitäten.
SI-7(8)	Software-, Firmware- und Informationsintegrität | Fähigkeit zur Prüfung wichtiger Ereignisse	cloud-trail-cloud-watch-logs-aktiviert	Verwenden Sie Amazon CloudWatch , um Protokoll ereignisaktivitäten zentral zu sammeln und zu verwalten. Die Aufnahme von AWS CloudTrail Daten liefert Einzelheiten zu den API-Aufrufaktivitäten in Ihrem AWS-Konto.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SI-7(8)	Software-, Firmware- und Informationsintegrität | Fähigkeit zur Prüfung wichtiger Ereignisse	cloudtrail-enabled	AWS CloudTrail kann bei der Nichtabstreitbarkeit helfen, indem Aktionen und API-Aufrufe der AWS Management Console aufgezeichnet werden. Sie können die Benutzer und die Benutzer AWS-Konten , die einen AWS Dienst aufgerufen haben, die Quell-IP-Adresse, über die die Aufrufe generiert wurden, und den Zeitpunkt der Anrufe identifizieren. Einzelheiten zu den erfassten Daten finden Sie in den AWS CloudTrail Datensatzinhalten.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SI-7(8)	Software-, Firmware- und Informationsintegrität | Fähigkeit zur Prüfung wichtiger Ereignisse	cloudtrail-s3-dataevents-enabled	Die Erfassung von Simple Storage Service (Amazon S3)-Datenereignissen unterstützt die Erkennung von ungewöhnlichen Aktivitäten. Zu den Details gehören AWS-Konto Informationen über den Zugriff auf einen Amazon S3 S3-Bucket, die IP-Adresse und die Uhrzeit des Ereignisses.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SI-7(8)	Software-, Firmware- und Informationsintegrität | Fähigkeit zur Prüfung wichtiger Ereignisse	elb-logging-enabled	Die Elastic-Load-Balancing-Aktivität ist ein zentraler Kommunikationspunkt innerhalb einer Umgebung. Stellen Sie sicher, dass die ELB-Protokollierung aktiviert ist. Die gesammelten Daten enthalten detaillierte Informationen zu Anfragen, die an den ELB gesendet wurden. Jedes Protokoll enthält Informationen wie die Zeit, zu der die Anforderung einging, die Client-IP-Adresse, Latenzen, Anforderungspfade und Serverantworten.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SI-7(8)	Software-, Firmware- und Informationsintegrität | Fähigkeit zur Prüfung wichtiger Ereignisse	rds-logging-enabled	Um die Protokollierung und Überwachung in Ihrer Umgebung zu erleichtern, stellen Sie sicher, dass die Amazon Relational Database Service (Amazon RDS)-Protokollierung aktiviert ist. Mit der Amazon-RDS-Protokollierung können Sie Ereignisse wie Verbindungen, Verbindungsabbrüche, Abfragen oder abgefragte Tabellen erfassen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SI-7(8)	Software-, Firmware- und Informationsintegrität | Fähigkeit zur Prüfung wichtiger Ereignisse	redshift-cluster-configuration-check	Um Daten im Ruhezustand zu schützen, muss die Verschlüsselung für Ihre Amazon-Redshift-Cluster aktiviert sein. Sie müssen auch sicherstellen, dass die erforderlichen Konfigurationen auf Amazon-Redshift-Clustern bereitgestellt werden. Die Prüfungsprotokollierung muss aktiviert sein, um Informationen zu Verbindungen und Benutzeraktivitäten in der Datenbank bereitzustellen. Diese Regel erfordert, dass ein Wert für clusterDbEncrypted (Config Default: TRUE) und LoggingEnabled (Config Default: TRUE) gesetzt ist. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SI-7(8)	Software-, Firmware- und Informationsintegrität | Fähigkeit zur Prüfung wichtiger Ereignisse	s3- bucket-logging-enabled	Die Amazon Simple Storage Service (Amazon S3)-Serverzugriffs protokollierung bietet eine Methode zur Überwachung des Netzwerks im Hinblick auf potenzielle Cybersicherheitsereignisse. Die Ereignisse werden überwacht, indem detaillierte Aufzeichnungen über die Anfragen erfasst werden, die an einen Amazon-S3-Bucket gestellt wurden. Jeder Zugriffsprotokolleintrag enthält Details zu einer einzelnen Zugriffsanfrage. Zu den Details gehören Anforderer, Bucket-Name, Anforderungszeit, Anforderungsaktion, Antwortstatus und Fehlercode, falls relevant.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SI-7(8)	Software-, Firmware- und Informationsintegrität | Fähigkeit zur Prüfung wichtiger Ereignisse	vpc-flow-logs-enabled	VPC-Flow-Protokolle erfassen detaillierte Informationsdatensätze über den IP-Datenverkehr, der zu und von Netzwerkschnittstellen in Ihrer Amazon Virtual Private Cloud (Amazon VPC) fließt. Standardmäßig enthalten Flow-Protokolldatensätze Werte für die verschiedenen Komponenten des IP-Flows, einschließlich Quelle, Ziel und Protokoll.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SI-12	Informationsmanagement und Aufbewahrung	db-instance-backup-enabled	Die Sicherungsfunktion von Amazon RDS erstellt Sicherungen Ihrer Datenbanken und Transaktionsprotokolle. Amazon RDS erstellt einen Snapshot für das Speichervolume Ihrer DB-Instance, sodass die gesamte DB-Instance gesichert wird. Sie können im System spezifische Aufbewahrungsfristen festlegen, um Ihre Ausfallsicherheitsanforderungen zu erfüllen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SI-12	Informationsmanagement und Aufbewahrung	dynamodb-in-backup-plan	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon DynamoDB-Tabellen Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SI-12	Informationsmanagement und Aufbewahrung	dynamodb-pitr-enabled	Aktivieren Sie diese Regel, um zu überprüfen, ob die Informationen gesichert wurden. Es verwaltet auch die Backups, indem es sicherstellt, dass die point-in-time Wiederherstellung in Amazon DynamoDB aktiviert ist. Bei der Wiederherstellung werden fortlaufende Backups Ihrer Tabelle für die letzten 35 Tage gespeichert.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SI-12	Informationsmanagement und Aufbewahrung	ebs-in-backup-plan	Stellen Sie zur Unterstützung der Datensicherungsprozesse sicher, dass Ihre Amazon Elastic Block Store (Amazon EBS) -Volumes Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SI-12	Informationsmanagement und Aufbewahrung	efs-in-backup-plan	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon Elastic File System (Amazon EFS) -Dateisysteme Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SI-12	Informationsmanagement und Aufbewahrung	elasticache-redis-cluster-automatic-Backup-Check	Wenn automatische Backups aktiviert sind, ElastiCache erstellt Amazon täglich ein Backup des Clusters. Die Sicherung kann für eine von Ihrer Organisation festgelegte Anzahl von Tagen aufbewahrt werden. Automatische Backups schützen vor Datenverlust. Bei einem Ausfall können Sie einen neuen Cluster erstellen, der Ihre Daten aus dem aktuellen Backup wiederherstellt.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SI-12	Informationsmanagement und Aufbewahrung	s-3 bucket-versioning-enabled	Die Versionsverwaltung von Amazon Simple Storage Service (Amazon S3)-Buckets hilft dabei, mehrere Varianten eines Objekts im selben Amazon-S3-Bucket zu speichern. Verwenden Sie die Versionsverwaltung, um sämtliche Versionen aller Objekte in Ihrem Amazon-S3-Bucket zu speichern, abzurufen oder wiederherzustellen. Mit der Versionsverwaltung können Sie Versionen sowohl nach unbeabsichtigten Benutzeraktionen als auch nach Anwendungsfehlern problemlos wiederherstellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SI-13(5)	Prädiktive Ausfallprävention | Failover-Fähigkeit	dynamodb-in-backup-plan	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon DynamoDB-Tabellen Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SI-13(5)	Prädiktive Ausfallprävention | Failover-Fähigkeit	ebs-in-backup-plan	Stellen Sie zur Unterstützung der Datensicherungsprozesse sicher, dass Ihre Amazon Elastic Block Store (Amazon EBS) -Volumes Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SI-13(5)	Prädiktive Ausfallprävention | Failover-Fähigkeit	efs-in-backup-plan	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon Elastic File System (Amazon EFS) -Dateisysteme Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SI-13(5)	Prädiktive Ausfallprävention | Failover-Fähigkeit	elb-cross-zone-load-Balancing aktiviert	Aktivieren Sie zonenübergreifendes Load Balancing für Ihre Elastic Load Balancer (ELBs), um eine angemessene Kapazität und Verfügbarkeit aufrechtzuerhalten. Zonenübergreifendes Load Balancing reduziert die Notwendigkeit, die gleiche Anzahl von Instances in jeder aktivierten Availability Zone aufrechtzuerhalten. Es verbessert auch die Fähigkeit Ihrer Anwendung, den Verlust einer oder mehrerer Instances zu bewältigen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SI-13(5)	Prädiktive Ausfallprävention | Failover-Fähigkeit	rds-instance-deletion-protection-aktiviert	Stellen Sie sicher, dass Amazon Relational Database Service (Amazon RDS)-Instances den Löschschutz aktiviert haben. Verwenden Sie den Löschschutz, um zu verhindern, dass Ihre Amazon-RDS-Instances versehentlich oder böswillig gelöscht werden, was zum Verlust der Verfügbarkeit Ihrer Anwendungen führen kann.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SI-13(5)	Prädiktive Ausfallprävention | Failover-Fähigkeit	redshift-backup-enabled	Stellen Sie zur Unterstützung der Datensicherungsprozesse sicher, dass Ihre Amazon-Redshift-Cluster über automatisierte Snapshots verfügen. Wenn automatisierte Snapshots für einen Cluster aktiviert sind, erstellt Redshift in regelmäßigen Abständen Snapshots dieses Clusters. Standardmäßig erstellt Redshift alle acht Stunden oder alle 5 GB einen Snapshot für jeden Knoten mit Datenänderungen oder je nachdem, was zuerst eintritt.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SI-13(5)	Prädiktive Ausfallprävention | Failover-Fähigkeit	s3- version-lifecycle-policy-check	Mit Amazon-S3-Lebenszyklusregeln können Sie Aktionen definieren, die Amazon S3 während der Lebensdauer eines Objekts ausführen soll (z. B. die Überführung von Objekten in eine andere Speicherklasse, ihre Archivierung oder Löschung nach einem bestimmten Zeitraum).

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SI-13(5)	Prädiktive Ausfallprävention | Failover-Fähigkeit	db-instance-backup-enabled	Die Sicherungsfunktion von Amazon RDS erstellt Sicherungen Ihrer Datenbanken und Transaktionsprotokolle. Amazon RDS erstellt einen Snapshot für das Speichervolume Ihrer DB-Instance, sodass die gesamte DB-Instance gesichert wird. Sie können im System spezifische Aufbewahrungsfristen festlegen, um Ihre Ausfallsicherheitsanforderungen zu erfüllen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SI-13(5)	Prädiktive Ausfallprävention | Failover-Fähigkeit	dynamodb-autoscaling-enabled	Amazon DynamoDB Auto Scaling verwendet den AWS Application Auto Scaling-Service, um die bereitgestellte Durchsatzkapazität so anzupassen, dass sie automatisch auf tatsächliche Verkehrsmuster reagiert. Auf diese Weise kann eine Tabelle oder ein globaler sekundärer Index die bereitgestellte Lese-/Schreibkapazität erhöhen, um plötzliche Erhöhungen des Datenverkehrs ohne Drosselung zu bewältigen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SI-13(5)	Prädiktive Ausfallprävention | Failover-Fähigkeit	dynamodb-pitr-enabled	Aktivieren Sie diese Regel, um zu überprüfen, ob die Informationen gesichert wurden. Es verwaltet auch die Backups, indem es sicherstellt, dass die point-in-time Wiederherstellung in Amazon DynamoDB aktiviert ist. Bei der Wiederherstellung werden fortlaufende Backups Ihrer Tabelle für die letzten 35 Tage gespeichert.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SI-13(5)	Prädiktive Ausfallprävention | Failover-Fähigkeit	elasticache-redis-cluster-automatic-Backup-Prüfung	Wenn automatische Backups aktiviert sind, ElastiCache erstellt Amazon täglich ein Backup des Clusters. Die Sicherung kann für eine von Ihrer Organisation festgelegte Anzahl von Tagen aufbewahrt werden. Automatische Backups schützen vor Datenverlust. Bei einem Ausfall können Sie einen neuen Cluster erstellen, der Ihre Daten aus dem aktuellen Backup wiederherstellt.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SI-13(5)	Prädiktive Ausfallprävention | Failover-Fähigkeit	rds-multi-az-support	Die Multi-AZ-Unterstützung in Amazon Relational Database Service (Amazon RDS) bietet eine verbesserte Verfügbarkeit und Beständigkeit von Datenbank-Instances. Wenn Sie eine Multi-AZ-Datenbank-Instance bereitstellen, erstellt Amazon RDS automatisch eine primäre Datenbank-Instance und repliziert die Daten synchron auf eine Standby-Instance in einer anderen Availability Zone. Jede Availability Zone läuft auf einer eigenen, physisch getrennten, unabhängigen Infrastruktur und ist auf eine hohe Verfügbarkeit ausgelegt. Im Falle eines Infrastrukturausfalls führt Amazon RDS einen automatis

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			chen Failover zum Standby-Modus durch, sodass Sie den Datenbankbetrieb wieder aufnehmen können, sobald der Failover abgeschlo ssen ist.
SI-13(5)	Prädiktive Ausfallpr ävention | Failover-Fähigkeit	s-3 bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) unterstützt die Aufrechterhaltung einer angemesse nen Kapazität und Verfügbarkeit. CRR ermöglicht das automatische, asynchrone Kopieren von Objekten in Amazon-S3-Buckets, um die Datenverf ügbarkeit sicherzus tellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SI-13(5)	Prädiktive Ausfallprävention | Failover-Fähigkeit	s-3 bucket-versioning-enabled	Die Versionsverwaltung von Amazon Simple Storage Service (Amazon S3)-Buckets hilft dabei, mehrere Varianten eines Objekts im selben Amazon-S3-Bucket zu speichern. Verwenden Sie die Versionsverwaltung, um sämtliche Versionen aller Objekte in Ihrem Amazon-S3-Bucket zu speichern, abzurufen oder wiederherzustellen. Mit der Versionsverwaltung können Sie Versionen sowohl nach unbeabsichtigten Benutzeraktionen als auch nach Anwendungsfehlern problemlos wiederherstellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SI-13(5)	Prädiktive Ausfallprävention | Failover-Fähigkeit	vpc-vpn-2-tunnels-up	Redundante Site-to-Site VPN-Tunnel können implementiert werden, um die Anforderungen an die Ausfallsicherheit zu erfüllen. Es verwendet zwei Tunnel, um die Konnektivität sicherzustellen, falls eine der Site-to-Site VPN-Verbindungen nicht verfügbar ist. Um sich vor einem Verbindungsverlust zu schützen, können Sie für den Fall, dass Ihr Kunden-Gateway nicht verfügbar ist, eine zweite Site-to-Site VPN-Verbindung zu Ihrer Amazon Virtual Private Cloud (Amazon VPC) und Ihrem Virtual Private Gateway einrichten, indem Sie ein zweites Kunden-Gateway verwenden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SI-20	Tainting	cloudwatch-alarm-action-check	Amazon CloudWatch alarmiert, wenn eine Metrik den Schwellenwert für eine bestimmte Anzahl von Bewertungszeiträumen überschreitet. Der Alarm führt eine oder mehrere Aktionen durch, die vom Wert der Metrik oder des Ausdrucks im Vergleich zu einem Schwellenwert in einer Reihe von Zeiträumen abhängt. Diese Regel erfordert einen Wert für alarmActionRequired (Config Default: True), insufficientDataAction Required (Config Default: True), okActionRequired (Config Default: False). Der tatsächliche Wert muss die Alarmaktionen für Ihre Umgebung widerspiegeln.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
SI-20	Tainting	cloud-trail-cloud-watch-logs-aktiviert	Verwenden Sie Amazon CloudWatch , um Protokoll ereignisaktivitäten zentral zu sammeln und zu verwalten. Die Aufnahme von AWS CloudTrail Daten liefert Einzelheiten zu den API-Aufrufaktivitäten in Ihrem AWS-Konto.
SI-20	Tainting	guardduty-enabled-centralized	Amazon GuardDuty kann mithilfe von Threat Intelligence Feeds helfen, potenzielle Cybersicherheitsereignisse zu überwachen und zu erkennen. Dazu gehören Listen mit bösartigen IPs und maschinellen Lernmethoden zur Identifizierung unerwarteter, nicht autorisierter und bösartiger Aktivitäten in Ihrer AWS Cloud-Umgebung.

Vorlage

Die Vorlage ist verfügbar unter GitHub: Operational Best Practices for NIST 800-53 Rev 5.

Bewährte Methoden für die Ausführung von NIST 800 171

Konformitätspakete bieten ein allgemeines Compliance-Framework, das es Ihnen ermöglicht, mithilfe verwalteter oder benutzerdefinierter AWS Config Regeln und Abhilfemaßnahmen Kontrollen zur Sicherheits-, Betriebs- oder Kostenoptimierung durchzuführen. AWS Config Conformance Packs dienen als Beispielvorlagen nicht dazu, die vollständige Einhaltung eines bestimmten Governance- oder Compliance-Standards sicherzustellen. Sie sind dafür verantwortlich, selbst zu beurteilen, ob Ihre Nutzung der Services den geltenden gesetzlichen und behördlichen Anforderungen entspricht.

Im Folgenden finden Sie ein Beispiel für eine Zuordnung zwischen den NIST 800-171- und AWS verwalteten Konfigurationsregeln. Jede Config-Regel gilt für eine bestimmte AWS Ressource und bezieht sich auf eine oder mehrere NIST 800-171-Steuerelemente. Eine Kontrolle nach NIST 800-171 kann mehreren Konfigurationsregeln zugeordnet werden. In der folgenden Tabelle finden Sie weitere Informationen und Anleitungen zu diesen Zuordnungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.1.1	Beschränken Sie den Systemzugang auf autorisierte Benutzer, Prozesse, die im Namen autorisierter Benutzer handeln, und Geräte (einschli eßlich anderer Systeme).	ec2- instance-profile-a ttached	EC2 Instanzprofile übergeben eine IAM-Rolle an eine EC2 Instance. Das Anhängen eines Instance-Profils an Ihre Instances kann bei der Implement ierung von geringste n Berechtigungen und der Berechtig ungsverwaltung helfen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.1.1	Beschränken Sie den Systemzugang auf autorisierte Benutzer, Prozesse, die im Namen autorisierter Benutzer handeln, und Geräte (einschli eßlich anderer Systeme).	ecs-task-definition-user-for-host-mode-check	Wenn für eine Aufgabendefinition erhöhte Berechtig ungen gelten, liegt das daran, dass der Kunde diesen Konfigura tionen ausdrücklich zugestimmt hat. Diese Kontrolle prüft, ob eine unerwartete Berechtigungseskal ation vorliegt, wenn für eine Aufgabend efinition das Host-Netzwerk aktiviert ist, die Kunden aber keine erhöhten Berechtigungen aktiviert haben.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.1.1	Beschränken Sie den Systemzugang auf autorisierte Benutzer, Prozesse, die im Namen autorisierter Benutzer handeln, und Geräte (einschli eßlich anderer Systeme).	iam-no-inline-policy-überprüfen	Stellen Sie sicher, dass ein Benutzer, eine IAM-Rolle oder eine IAM-Gruppe (AWS Identity and Access Management) nicht über eine Inline-Richtlinie zur Zugriffsk ontrolle auf Systeme und Ressource n verfügt. AWS empfiehlt, verwaltet e Richtlinien anstelle von Inline-Richtlinien zu verwenden. Verwaltete Richtlini en ermöglichen Wiederverwendbarke it, Versionsverwaltung , Rollback und Delegierung der Berechtigungsverwa ltung.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.1.1	Beschränken Sie den Systemzugang auf autorisierte Benutzer, Prozesse, die im Namen autorisierter Benutzer handeln, und Geräte (einschließlich anderer Systeme).	iam-policy-no-statements-with-full-access	Stellen Sie sicher, dass IAM-Aktionen nur auf die benötigten Aktionen beschränkt sind. Wenn Benutzern mehr Rechte eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Rechte und der Aufgabentrennung verstoßen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.1.1	Beschränken Sie den Systemzugang auf autorisierte Benutzer, Prozesse, die im Namen autorisierter Benutzer handeln, und Geräte (einschli eßlich anderer Systeme).	ec-2 instances-in-vpc	Stellen Sie Amazon Elastic Compute Cloud (Amazon EC2) -Instances innerhalb einer Amazon Virtual Private Cloud (Amazon VPC) bereit, um eine sichere Kommunika tion zwischen einer Instance und anderen Services innerhalb der Amazon VPC zu ermöglichen, ohne dass ein Internet-Gateway, ein NAT-Gerät oder eine VPN-Verbindung erforderlich ist. Der gesamte Datenverk ehr bleibt sicher in der AWS Cloud. Domains, die sich innerhalb einer VPC befinden, verfügen aufgrund ihrer logischen Isolierun g im Vergleich zu Domains mit öffentlic hen Endpunkten über eine zusätzlic he Sicherheitsebene. Weisen Sie EC2

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			Amazon-Instances einer Amazon-VPC zu, um den Zugriff ordnungsgemäß zu verwalten.
3.1.1	Beschränken Sie den Systemzugang auf autorisierte Benutzer, Prozesse, die im Namen autorisierter Benutzer handeln, und Geräte (einschli eßlich anderer Systeme).	redshift-enhanced-vpc-routing-aktiviert	Mit Enhanced-VPC-Routing wird erzwungen, dass der gesamte COPY- und UNLOAD-Da tenverkehr zwischen Ihrem Cluster und Datenrepositorys über Ihre Amazon VPC erfolgt. Anschließ end können Sie VPC-Features wie Sicherheitsgruppen und Netzwerkz ugriffskontrolllisten verwenden, um den Netzwerkverkehr zu schützen. Sie können auch VPC-Flow-Logs verwenden, um den Netzwerkverkehr zu überwachen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.1.1	Beschränken Sie den Systemzugang auf autorisierte Benutzer, Prozesse, die im Namen autorisierter Benutzer handeln, und Geräte (einschli eßlich anderer Systeme).	ssm-document-not-p ublic	Stellen Sie sicher, dass AWS Systems Manager (SSM) - Dokumente nicht öffentlich sind, da dies einen unbeabsic htigten Zugriff auf Ihre SSM-Dokum ente ermöglichen kann. Ein öffentlic hes SSM-Dokum ent kann Informati onen über Ihr Konto, Ihre Ressourcen und internen Prozesse preisgeben.
3.1.1	Beschränken Sie den Systemzugang auf autorisierte Benutzer, Prozesse, die im Namen autorisierter Benutzer handeln, und Geräte (einschli eßlich anderer Systeme).	dms-replication-not-public	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass auf DMS-Replikationsin stanzen nicht öffentlic h zugegriffen werden kann. DMS-Repli kations-Instances können vertrauli che Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.1.1	Beschränken Sie den Systemzugang auf autorisierte Benutzer, Prozesse, die im Namen autorisierter Benutzer handeln, und Geräte (einschli eßlich anderer Systeme).	ebs-snapshot-public-restorable-überprüfen	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass EBS-Snapshots nicht öffentlich wiederher stellbar sind. EBS-Volume-Snapsho ts können vertrauli che Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.
3.1.1	Beschränken Sie den Systemzugang auf autorisierte Benutzer, Prozesse, die im Namen autorisierter Benutzer handeln, und Geräte (einschli eßlich anderer Systeme).	ec-2 instance-no-public-ip	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon Elastic Compute Cloud (Amazon EC2) - Instances nicht öffentlich zugänglich sind. EC2 Amazon-Instances können vertrauliche Informati onen enthalten, und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.1.1	Beschränken Sie den Systemzugang auf autorisierte Benutzer, Prozesse, die im Namen autorisierter Benutzer handeln, und Geräte (einschli eßlich anderer Systeme).	elasticsearch-in-vpc-only	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherste llen, dass sich Amazon OpenSearc h OpenSearch Service (Service) - Domains innerhalb einer Amazon Virtual Private Cloud (Amazon VPC) befinden. Eine OpenSearch Service-Domain innerhalb einer Amazon VPC ermöglicht die sichere Kommunikation zwischen OpenSearc h Service und anderen Services innerhalb der Amazon VPC, ohne dass ein Internet-Gateway, ein NAT-Gerät oder eine VPN-Verbindung erforderlich ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.1.1	Beschränken Sie den Systemzugang auf autorisierte Benutzer, Prozesse, die im Namen autorisierter Benutzer handeln, und Geräte (einschli eßlich anderer Systeme).	emr-kerberos-enabled	Die Zugriffsberechtigu ngen und -autorisi erungen können verwaltet und nach den Prinzipien der geringsten Berechtig ung und Aufgabent rennung integrier t werden, indem Kerberos für Amazon-EMR-Cluster aktiviert wird. In Kerberos werden Services und Benutzer, die sich authentif izieren müssen, als Prinzipale bezeichnet. Prinzipal e befinden sich in einem Kerberos-Bereich. Innerhalb dieses Bereichs wird ein Kerberos-Server als Key Distribution Center (KDC) bezeichnet. Über diesen Server können sich Prinzipal e authentifizieren. Die Authentifizierung im KDC erfolgt durch die Ausstellu ng von Authentif

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			izierungstickets. Das KDC unterhält eine Datenbank der Prinzipale in seinem Bereich mit ihren Passwörtern und anderen administrativen Informationen zu jedem Prinzipal.
3.1.1	Beschränken Sie den Systemzugang auf autorisierte Benutzer, Prozesse, die im Namen autorisierter Benutzer handeln, und Geräte (einschließlich anderer Systeme).	emr-master-no-public-ip	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon EMR-Cluster-Masterknoten nicht öffentlich zugänglich sind. Amazon-EMR-Cluster-Hauptknoten können vertrauliche Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.1.1	Beschränken Sie den Systemzugang auf autorisierte Benutzer, Prozesse, die im Namen autorisierter Benutzer handeln, und Geräte (einschli eßlich anderer Systeme).	iam-group-has-users-überprüfen	AWS Identity and Access Managemen t (IAM) kann Ihnen helfen, die Prinzipien der geringsten Rechte und der Aufgabent rennung mit Zugriffsb erechtigungen und Autorisierungen zu integrieren, indem sichergestellt wird, dass IAM-Gruppen mindestens einen Benutzer haben. Die Einteilung von Benutzern in Gruppen auf der Grundlage der ihnen zugewiese nen Berechtigungen oder ihrer Funktion ist eine Möglichkeit, das Prinzip der geringste n Berechtigung zu implementieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.1.1	Beschränken Sie den Systemzugang auf autorisierte Benutzer, Prozesse, die im Namen autorisierter Benutzer handeln, und Geräte (einschli eßlich anderer Systeme).	iam-policy-no-stat ements-with-admin-access	AWS Identity and Access Managemen t (IAM) kann Ihnen dabei helfen, die Prinzipien der geringsten Rechte und der Aufgabent rennung in Zugriffsb erechtigungen und Autorisierungen zu integrieren und so zu verhindern, dass Richtlinien „Effect“: „Allow“ mit „Action“: „*“ anstelle von „Resource“: „*“ enthalten. Wenn Benutzern mehr Rechte eingeräum t werden, als für die Ausführung einer Aufgabe erforderl ich sind, kann dies gegen das Prinzip der geringsten Berechtigung und der Aufgabentrennung verstoßen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.1.1	Beschränken Sie den Systemzugang auf autorisierte Benutzer, Prozesse, die im Namen autorisierter Benutzer handeln, und Geräte (einschli eßlich anderer Systeme).	iam-root-access-key-überprüfen	Der Zugriff auf Systeme und Ressourcen kann gesteuert werden, indem überprüft wird, ob der Root-Benu tzer keine Zugriffss chlüssel mit seiner AWS Identity and Access Management (IAM) -Rolle verknüpft hat. Stellen Sie sicher, dass die Root-Zugr iffsschlüssel gelöscht werden. Erstellen und verwenden Sie stattdessen rollenbas ierte Funktionen, AWS-Konten um das Prinzip der geringste n Funktionalität zu berücksichtigen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.1.1	Beschränken Sie den Systemzugang auf autorisierte Benutzer, Prozesse, die im Namen autorisierter Benutzer handeln, und Geräte (einschli eßlich anderer Systeme).	iam-user-group-mem bership-überprüfen	AWS Identity and Access Managemen t (IAM) kann Ihnen helfen, Zugriffsb erechtigungen und Autorisierungen einzuschränken, indem sichergestellt wird, dass Benutzer Mitglieder mindesten s einer Gruppe sind. Wenn Benutzern mehr Berechtigungen eingeräumt werden, als für die Ausführun g einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringste n Berechtigung und Aufgabentrennung verstoßen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.1.1	Beschränken Sie den Systemzugang auf autorisierte Benutzer, Prozesse, die im Namen autorisierter Benutzer handeln, und Geräte (einschli eßlich anderer Systeme).	iam-user-mfa-enabled	Aktivieren Sie diese Regel, um den Zugriff auf Ressourcen in der AWS Cloud einzuschr änken. Diese Regel sorgt dafür, dass die Multi-Faktor-Authe ntifizierung (MFA) für alle Benutzer aktiviert ist. MFA sorgt für eine weitere Schutzebe ne zusätzlich zu den Anmeldeinformation en. Reduzieren Sie Fälle von kompromit tierten Konten, indem Sie MFA für Benutzer vorschreiben.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.1.1	Beschränken Sie den Systemzugang auf autorisierte Benutzer, Prozesse, die im Namen autorisierter Benutzer handeln, und Geräte (einschli eßlich anderer Systeme).	iam-user-no-policies-überprüfen	Diese Regel stellt sicher, dass AWS Identity and Access Management (IAM) -Richtlinien nur Gruppen oder Rollen zugewiese n werden, um den Zugriff auf Systeme und Ressourcen zu kontrollieren. Die Zuweisung von Berechtig ungen auf Gruppen- oder Rollenebene trägt dazu bei, die Wahrscheinlichkeit zu verringern, dass eine Identität übermäßige Berechtigungen erhält oder beibehält.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.1.1	Beschränken Sie den Systemzugang auf autorisierte Benutzer, Prozesse, die im Namen autorisierter Benutzer handeln, und Geräte (einschli eßlich anderer Systeme).	iam-user-unused-cr edentials-überprüfen	AWS Identity and Access Managemen t (IAM) kann Ihnen bei Zugriffsberechtigu ngen und Autorisie rungen helfen, indem es nach IAM-Passw örtern und Zugriffss chlüsseln sucht, die für einen bestimmte n Zeitraum nicht verwendet wurden. Wenn ungenutzte Anmeldeinformation en identifiziert werden, müssen Sie sie deaktivieren und/oder entfernen , da dies gegen das Prinzip der geringste n Berechtigung verstoßen könnte. Für diese Regel müssen Sie einen Wert für das maxCreden tialUsage Alter festlegen (Standard konfiguration: 90). Der tatsächliche Wert muss den Richtlini en Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.1.1	Beschränken Sie den Systemzugang auf autorisierte Benutzer, Prozesse, die im Namen autorisierter Benutzer handeln, und Geräte (einschli eßlich anderer Systeme).	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) Security Groups können bei der Verwaltung des Netzwerkzugriffs helfen, indem sie eine statusbeh aftete Filterung von eingehendem und ausgehendem Netzwerkverkehr zu Ressourcen bereitste llen. AWS Wenn Sie eingehenden (oder entfernten) Datenverk ehr von 0.0.0.0/0 bis Port 22 auf Ihren Ressourcen nicht zulassen, können Sie den Remote-Zugriff einschränken.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.1.1	Beschränken Sie den Systemzugang auf autorisierte Benutzer, Prozesse, die im Namen autorisierter Benutzer handeln, und Geräte (einschli eßlich anderer Systeme).	internet-gateway-a uthorized-vpc-nur	Verwalten Sie den Zugriff auf Ressource n in der AWS Cloud, indem Sie sicherste llen, dass Internet-Gateways nur mit autorisierter Amazon Virtual Private Cloud (Amazon VPC) verbunden sind. Internet-Gateways ermöglichen den bidirektionalen Internetzugang zur und von der Amazon VPC, was möglicher weise zu einem unbefugten Zugriff auf Amazon-VPC-Ressourcen führen kann.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.1.1	Beschränken Sie den Systemzugang auf autorisierte Benutzer, Prozesse, die im Namen autorisierter Benutzer handeln, und Geräte (einschli eßlich anderer Systeme).	lambda-function-pu blic-access-verboten	Verwalten Sie den Zugriff auf Ressource n in der AWS Cloud, indem Sie sicherste llen, dass AWS Lambda-Funktionen nicht öffentlich zugänglich sind. Der öffentliche Zugriff kann möglicherweise die Verfügbarkeit von Ressourcen beeinträc htigen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.1.1	Beschränken Sie den Systemzugang auf autorisierte Benutzer, Prozesse, die im Namen autorisierter Benutzer handeln, und Geräte (einschli eßlich anderer Systeme).	lambda-inside-vpc	Stellen Sie AWS Lambda-Funktionen in einer Amazon Virtual Private Cloud (Amazon VPC) bereit, um eine sichere Kommunika tion zwischen einer Funktion und anderen Diensten innerhalb der Amazon VPC zu gewährleisten. Bei dieser Konfiguration sind kein Internet-Gateway, kein NAT-Gerät und keine VPN-Verbindung erforderlich. Der gesamte Datenverk ehr bleibt sicher in der Cloud. AWS Domains, die sich innerhalb einer VPC befinden, verfügen aufgrund ihrer logischen Isolierun g im Vergleich zu Domains mit öffentlic hen Endpunkten über eine zusätzliche Sicherheitsebene. Um den Zugriff ordnungsg emäß zu verwalten,

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			sollten AWS Lambda-Funktionen einer VPC zugewiesen werden.
3.1.1	Beschränken Sie den Systemzugang auf autorisierte Benutzer, Prozesse, die im Namen autorisierter Benutzer handeln, und Geräte (einschli eßlich anderer Systeme).	mfa-enabled-for-iam-Konsolenzugriff	Verwalten Sie den Zugriff auf Ressource n in der AWS Cloud, indem Sie sicherste llen, dass MFA für alle AWS Identity and Access Managemen t (IAM) -Benutzer aktiviert ist, die über ein Konsolenk ennwort verfügen. MFA sorgt für eine weitere Schutzebe ne zusätzlich zu den Anmeldeinformation en. Indem Sie MFA für Benutzer vorschrei ben, können Sie Fälle kompromittierter Konten reduzieren und verhindern, dass unbefugte Benutzer auf vertrauliche Daten zugreifen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.1.1	Beschränken Sie den Systemzugang auf autorisierte Benutzer, Prozesse, die im Namen autorisierter Benutzer handeln, und Geräte (einschli eßlich anderer Systeme).	opensearch-access-control-enabled	Stellen Sie sicher, dass eine differenz ierte Zugriffskontrolle für Ihre Amazon OpenSearch Service-Domains aktiviert ist. Eine differenz ierte Zugriffskontrolle bietet erweiterte Autorisierungsmech anismen, um den Zugriff auf Amazon Service-Domains mit den geringsten Rechten zu erreichen . OpenSearch Es ermöglicht eine rollenbasierte Zugriffskontrolle auf die Domain sowie Sicherheit auf Index-, Dokument- und Feldebene, Unterstüt zung für OpenSearch Service-Dashboards, Mehrmandantenfähig keit und HTTP-Basi sauthentifizierung für Service und Kibana. OpenSearch

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.1.1	Beschränken Sie den Systemzugang auf autorisierte Benutzer, Prozesse, die im Namen autorisierter Benutzer handeln, und Geräte (einschli eßlich anderer Systeme).	opensearch-in-vpc-only	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass sich Amazon OpenSearch Service-Domains innerhalb einer Amazon Virtual Private Cloud (Amazon VPC) befinden. Eine Amazon OpenSearc h Service-Domain innerhalb einer Amazon VPC ermöglicht die sichere Kommunikation zwischen Amazon OpenSearch Service und anderen Services innerhalb der Amazon VPC, ohne dass ein Internet-Gateway, ein NAT-Gerät oder eine VPN-Verbindung erforderlich ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.1.1	Beschränken Sie den Systemzugang auf autorisierte Benutzer, Prozesse, die im Namen autorisierter Benutzer handeln, und Geräte (einschli eßlich anderer Systeme).	rds-instance-public-access-überprüfen	Verwalten Sie den Zugriff auf Ressource n in der AWS Cloud, indem Sie sicherste llen, dass Amazon Relational Database Service (Amazon RDS) -Instance s nicht öffentlic h sind. Amazon-RDS-Datenbank-Instances können vertrauliche Informati onen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.1.1	Beschränken Sie den Systemzugang auf autorisierte Benutzer, Prozesse, die im Namen autorisierter Benutzer handeln, und Geräte (einschli eßlich anderer Systeme).	rds-snapshots-public-prohibited	Verwalten Sie den Zugriff auf Ressource n in der AWS Cloud, indem Sie sicherste llen, dass Amazon Relational Database Service (Amazon RDS) -Instance s nicht öffentlic h sind. Amazon-RDS-Datenbank-Instances können vertrauliche Informati onen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.1.1	Beschränken Sie den Systemzugang auf autorisierte Benutzer, Prozesse, die im Namen autorisierter Benutzer handeln, und Geräte (einschli eßlich anderer Systeme).	redshift-cluster-public-access-überprüfen	Verwalten Sie den Zugriff auf Ressource n in der AWS Cloud, indem Sie sicherste llen, dass Amazon Redshift Redshift-Cluster nicht öffentlic h sind. Amazon-Re dshift-Cluster können vertrauliche Informati onen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.1.1	Beschränken Sie den Systemzugang auf autorisierte Benutzer, Prozesse, die im Namen autorisierter Benutzer handeln, und Geräte (einschli eßlich anderer Systeme).	restricted-common-ports	Verwalten Sie den Zugriff auf Ressource n in der AWS Cloud, indem Sie sicherste llen, dass gemeinsam e Ports für Amazon Elastic Compute Cloud (Amazon EC2) -Sicherhe itsgruppen eingeschr ränkt sind. Wenn der Zugriff auf Ports nicht auf vertrauen swürdige Quellen beschränkt wird, kann dies zu Angriffen auf die Verfügbar keit, Integrität und Vertraulichkeit von Systemen führen. Mit dieser Regel können Sie optional die Parameter blockedPo rt1–blockedPort5 festlegen (Standard konfigurationen: 20, 21, 3389, 3306, 4333). Die tatsächli chen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.1.1	Beschränken Sie den Systemzugang auf autorisierte Benutzer, Prozesse, die im Namen autorisierter Benutzer handeln, und Geräte (einschließlich anderer Systeme).	root-account-hardware-mfa-aktiviert	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Hardware-MFA für den Root-Benutzer aktiviert ist. Der Stammbenutzer ist der AWS-Konto-Benutzer mit den meisten Berechtigungen. MFA sorgt für eine weitere Schutzebene zusätzlich zu den Anmeldeinformationen. Indem Sie MFA für den Root-Benutzer vorschreiben, können Sie die Anzahl AWS-Konten kompromittierter Benutzer reduzieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.1.1	Beschränken Sie den Systemzugang auf autorisierte Benutzer, Prozesse, die im Namen autorisierter Benutzer handeln, und Geräte (einschliesslich anderer Systeme).	root-account-mfa-enabled	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass MFA für den Root-Benutzer aktiviert ist. Der Stammbenutzer ist der AWS-Konto-Benutzer mit den meisten Berechtigungen. MFA sorgt für eine weitere Schutzebene zusätzlich zu den Anmeldeinformationen. Indem Sie MFA für den Root-Benutzer vorschreiben, können Sie die Anzahl AWS-Konten kompromittierter Benutzer reduzieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.1.1	Beschränken Sie den Systemzugang auf autorisierte Benutzer, Prozesse, die im Namen autorisierter Benutzer handeln, und Geräte (einschli eßlich anderer Systeme).	s3- -blöcke-periodisch account-level-public-access	Verwalten Sie den Zugriff auf Ressource n in der AWS Cloud, indem Sie sicherste llen, dass Amazon Simple Storage Service (Amazon S3) -Buckets nicht öffentlich zugänglic h sind. Diese Regel trägt dazu bei, sensible Daten vor unbefugten Remote-Benutzern zu schützen, indem sie den öffentlichen Zugriff verhinder t. Mit dieser Regel können Sie optional die Parameter ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) und restrictPublicBuck ets Parameter (Config Default: True) festlegen. Die tatsächlichen Werte müssen den Richtlini

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			en Ihrer Organisation entsprechen.
3.1.1	Beschränken Sie den Systemzugang auf autorisierte Benutzer, Prozesse, die im Namen autorisierter Benutzer handeln, und Geräte (einschli eßlich anderer Systeme).	s3 bucket-level-public-access - verboten	Verwalten Sie den Zugriff auf Ressource n in der AWS Cloud, indem Sie sicherste llen, dass Amazon Simple Storage Service (Amazon S3) -Buckets nicht öffentlich zugänglic h sind. Diese Regel trägt dazu bei, sensible Daten vor unbefugten Remote-Benutzern zu schützen, indem sie den öffentlichen Zugriff auf Bucket-Eb ene verhindert.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.1.1	Beschränken Sie den Systemzugang auf autorisierte Benutzer, Prozesse, die im Namen autorisierter Benutzer handeln, und Geräte (einschli eßlich anderer Systeme).	s-3 bucket-policy-gran tee-check	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie s3_ bucket_policy_gran tee_check aktiviere n. Diese Regel prüft, ob der vom Amazon S3 S3-Bucket gewährte Zugriff durch die von Ihnen bereitgestellten AWS Principals, Verbundbe nutzer, Service Principals, IP-Adress en oder Amazon Virtual Private Cloud (Amazon VPC) IDs eingeschränkt ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.1.1	Beschränken Sie den Systemzugang auf autorisierte Benutzer, Prozesse, die im Namen autorisierter Benutzer handeln, und Geräte (einschli eßlich anderer Systeme).	s-3 bucket-public-read -prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie nur autorisierten Benutzern, Prozessen und Geräten Zugriff auf Amazon Simple Storage Service (Amazon S3) - Buckets gewähren. Die Verwaltung des Zugriffs sollte mit der Klassifizierung der Daten übereinst immen.
3.1.1	Beschränken Sie den Systemzugang auf autorisierte Benutzer, Prozesse, die im Namen autorisierter Benutzer handeln, und Geräte (einschli eßlich anderer Systeme).	s3- bucket-public-writ e-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie nur autorisierten Benutzern, Prozessen und Geräten Zugriff auf Amazon Simple Storage Service (Amazon S3) - Buckets gewähren. Die Verwaltung des Zugriffs sollte mit der Klassifizierung der Daten übereinst immen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.1.1	Beschränken Sie den Systemzugang auf autorisierte Benutzer, Prozesse, die im Namen autorisierter Benutzer handeln, und Geräte (einschli eßlich anderer Systeme).	sagemaker-notebook-no-direct-Internetzugang	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass SageMaker Amazon-Notebooks keinen direkten Internetzugang zulassen. Indem Sie direkten Internetzugang blockieren, vermeiden Sie, dass unbefugte Benutzer auf sensible Daten zugreifen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.1.1	Beschränken Sie den Systemzugang auf autorisierte Benutzer, Prozesse, die im Namen autorisierter Benutzer handeln, und Geräte (einschli eßlich anderer Systeme).	subnet-auto-assign-public-ip-deaktiviert	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon Virtual Private Cloud (VPC) -Subnetzen nicht automatisch eine öffentliche IP-Adress e zugewiesen wird. Amazon Elastic Compute Cloud (EC2) -Instances, die in Subnetzen gestartet werden, in denen dieses Attribut aktiviert ist, haben ihrer primären Netzwerkschnittste lle eine öffentliche IP-Adresse zugewiesen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.1.1	Beschränken Sie den Systemzugang auf autorisierte Benutzer, Prozesse, die im Namen autorisierter Benutzer handeln, und Geräte (einschli eßlich anderer Systeme).	vpc-default-security-group-geschlossen	Sicherheitsgruppen von Amazon Elastic Compute Cloud (Amazon EC2) können bei der Verwaltung des Netzwerkzugriffs helfen, indem sie eine statusbehaftete Filterung des ein- und ausgehenden Netzwerkverkehrs zu Ressourcen bereitstellen. AWS Die Beschränk ung des gesamten Datenverkehrs auf die Standardsicherheit sgruppe hilft dabei, den Fernzugriff auf Ihre Ressourcen einzuschränken. AWS

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.1.1	Beschränken Sie den Systemzugang auf autorisierte Benutzer, Prozesse, die im Namen autorisierter Benutzer handeln, und Geräte (einschli eßlich anderer Systeme).	vpc-sg-open-only-to-authorized-ports	Verwalten Sie den Zugriff auf Ressource n in der AWS Cloud, indem Sie sicherste llen, dass gemeinsam e Ports für Amazon Elastic Compute Cloud (Amazon EC2) -Sicherhe itsgruppen eingeschr ränkt sind. Wenn der Zugriff auf Ports nicht auf vertrauen swürdige Quellen beschränkt wird, kann dies zu Angriffen auf die Verfügbar keit, Integrität und Vertraulichkeit von Systemen führen. Durch die Beschränk ung des Zugriffs auf Ressourcen innerhalb einer Sicherhei tsgruppe aus dem Internet (0.0.0.0/0) kann der Fernzugriff auf interne Systeme gesteuert werden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.1.2	Beschränken Sie den Systemzugriff auf jene Transaktionen und Funktionen, die autorisierte Benutzer ausführen dürfen.	autoscaling-launch-config-public-ip-deaktiviert	Wenn Sie Ihre Netzwerkschnittstellen mit einer öffentlichen IP-Adresse konfigurieren, sind die diesen Netzwerkschnittstellen zugehörigen Ressourcen über das Internet erreichbar. EC2 Ressourcen sollten nicht öffentlich zugänglich sein, da dies einen unbeabsichtigten Zugriff auf Ihre Anwendungen oder Server ermöglichen kann.
3.1.2	Beschränken Sie den Systemzugriff auf jene Transaktionen und Funktionen, die autorisierte Benutzer ausführen dürfen.	ec2- instance-profile-attached	EC2 Instanzprofile übergeben eine IAM-Rolle an eine EC2 Instance. Das Anhängen eines Instance-Profils an Ihre Instances kann bei der Implementierung von geringsten Berechtigungen und der Berechtigungsverwaltung helfen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.1.2	Beschränken Sie den Systemzugriff auf jene Transaktionen und Funktionen, die autorisierte Benutzer ausführen dürfen.	ecs-task-definition-user-for-host-mode-check	Wenn für eine Aufgabendefinition erhöhte Berechtigungen gelten, liegt das daran, dass der Kunde diesen Konfigurationen ausdrücklich zugestimmt hat. Diese Kontrolle prüft, ob eine unerwartete Berechtigungseskalation vorliegt, wenn für eine Aufgabendefinition das Host-Netzwerk aktiviert ist, die Kunden aber keine erhöhten Berechtigungen aktiviert haben.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.1.2	Beschränken Sie den Systemzugriff auf jene Transaktionen und Funktionen, die autorisierte Benutzer ausführen dürfen.	iam-no-inline-policy-überprüfen	Stellen Sie sicher, dass ein Benutzer, eine IAM-Rolle oder eine IAM-Gruppe (AWS Identity and Access Management) nicht über eine Inline-Richtlinie zur Zugriffskontrolle auf Systeme und Ressourcen verfügt. AWS empfiehlt, verwaltete Richtlinien anstelle von Inline-Richtlinien zu verwenden. Verwaltete Richtlinien ermöglichen Wiederverwendbarkeit, Versionsverwaltung, Rollback und Delegierung der Berechtigungsverwaltung.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.1.2	Beschränken Sie den Systemzugriff auf jene Transaktionen und Funktionen, die autorisierte Benutzer ausführen dürfen.	iam-policy-no-statements-with-full-access	Stellen Sie sicher, dass IAM-Aktionen nur auf die benötigten Aktionen beschränkt sind. Wenn Benutzern mehr Rechte eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Rechte und der Aufgabentrennung verstoßen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.1.2	Beschränken Sie den Systemzugriff auf jene Transaktionen und Funktionen, die autorisierte Benutzer ausführen dürfen.	ec-2 instances-in-vpc	Stellen Sie Amazon Elastic Compute Cloud (Amazon EC2) -Instances innerhalb einer Amazon Virtual Private Cloud (Amazon VPC) bereit, um eine sichere Kommunika tion zwischen einer Instance und anderen Services innerhalb der Amazon VPC zu ermöglichen, ohne dass ein Internet-Gateway, ein NAT-Gerät oder eine VPN-Verbindung erforderlich ist. Der gesamte Datenverk ehr bleibt sicher in der AWS Cloud. Domains, die sich innerhalb einer VPC befinden, verfügen aufgrund ihrer logischen Isolierun g im Vergleich zu Domains mit öffentlic hen Endpunkten über eine zusätzlic he Sicherheitsebene. Weisen Sie EC2

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			Amazon-Instances einer Amazon-VPC zu, um den Zugriff ordnungsgemäß zu verwalten.
3.1.2	Beschränken Sie den Systemzugriff auf jene Transaktionen und Funktionen, die autorisierte Benutzer ausführen dürfen.	no-unrestricted-route-to-igw	Stellen Sie sicher, dass EC2 Amazon-Routentabellen keine uneingeschränkten Routen zu einem Internet-Gateway enthalten. Durch das Entfernen oder Beschränken des Internetzugangs für Workloads innerhalb von Amazon VPCs können unbeabsic htigte Zugriffe in Ihrer Umgebung reduziert werden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.1.2	Beschränken Sie den Systemzugriff auf jene Transaktionen und Funktionen, die autorisierte Benutzer ausführen dürfen.	ssm-document-not-public	Stellen Sie sicher, dass AWS Systems Manager (SSM) - Dokumente nicht öffentlich sind, da dies einen unbeabsichtigten Zugriff auf Ihre SSM-Dokumente ermöglichen kann. Ein öffentliches SSM-Dokument kann Informationen über Ihr Konto, Ihre Ressourcen und internen Prozesse preisgeben.
3.1.2	Beschränken Sie den Systemzugriff auf jene Transaktionen und Funktionen, die autorisierte Benutzer ausführen dürfen.	dms-replication-not-public	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass auf DMS-Replikationsinstanzen nicht öffentlich zugegriffen werden kann. DMS-Replikations-Instances können vertrauliche Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.1.2	Beschränken Sie den Systemzugriff auf jene Transaktionen und Funktionen, die autorisierte Benutzer ausführen dürfen.	ebs-snapshot-public-restorable-überprüfen	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass EBS-Snapshots nicht öffentlich wiederher stellbar sind. EBS-Volume-Snapsho ts können vertrauli che Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.
3.1.2	Beschränken Sie den Systemzugriff auf jene Transaktionen und Funktionen, die autorisierte Benutzer ausführen dürfen.	ec-2 instance-no-public-ip	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon Elastic Compute Cloud (Amazon EC2) - Instances nicht öffentlich zugänglich sind. EC2 Amazon-Instances können vertrauliche Informati onen enthalten, und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.1.2	Beschränken Sie den Systemzugriff auf jene Transaktionen und Funktionen, die autorisierte Benutzer ausführen dürfen.	elasticsearch-in-vpc-only	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass sich Amazon OpenSearch OpenSearch Service (Service) - Domains innerhalb einer Amazon Virtual Private Cloud (Amazon VPC) befinden. Eine OpenSearch Service-Domain innerhalb einer Amazon VPC ermöglicht die sichere Kommunikation zwischen OpenSearch Service und anderen Services innerhalb der Amazon VPC, ohne dass ein Internet-Gateway, ein NAT-Gerät oder eine VPN-Verbindung erforderlich ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.1.2	Beschränken Sie den Systemzugriff auf jene Transaktionen und Funktionen, die autorisierte Benutzer ausführen dürfen.	emr-kerberos-enabled	Die Zugriffsberechtigungen und -autorisierungen können verwaltet und nach den Prinzipien der geringsten Berechtigung und Aufgabentrennung integriert werden, indem Kerberos für Amazon-EMR-Cluster aktiviert wird. In Kerberos werden Services und Benutzer, die sich authentifizieren müssen, als Prinzipale bezeichnet. Prinzipale befinden sich in einem Kerberos-Bereich. Innerhalb dieses Bereichs wird ein Kerberos-Server als Key Distribution Center (KDC) bezeichnet. Über diesen Server können sich Prinzipale authentifizieren. Die Authentifizierung im KDC erfolgt durch die Ausstellung von Authentif

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			izierungstickets. Das KDC unterhält eine Datenbank der Prinzipale in seinem Bereich mit ihren Passwörtern und anderen administrativen Informationen zu jedem Prinzipal.
3.1.2	Beschränken Sie den Systemzugriff auf jene Transaktionen und Funktionen, die autorisierte Benutzer ausführen dürfen.	emr-master-no-public-ip	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon EMR-Cluster-Masterknoten nicht öffentlich zugänglich sind. Amazon-EMR-Cluster-Hauptknoten können vertrauliche Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.1.2	Beschränken Sie den Systemzugriff auf jene Transaktionen und Funktionen, die autorisierte Benutzer ausführen dürfen.	iam-group-has-users-überprüfen	AWS Identity and Access Managemen t (IAM) kann Ihnen helfen, die Prinzipien der geringsten Rechte und der Aufgabent rennung mit Zugriffsb erechtigungen und Autorisierungen zu integrieren, indem sichergestellt wird, dass IAM-Gruppen mindestens einen Benutzer haben. Die Einteilung von Benutzern in Gruppen auf der Grundlage der ihnen zugewiese nen Berechtigungen oder ihrer Funktion ist eine Möglichkeit, das Prinzip der geringste n Berechtigung zu implementieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.1.2	Beschränken Sie den Systemzugriff auf jene Transaktionen und Funktionen, die autorisierte Benutzer ausführen dürfen.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) kann Ihnen dabei helfen, die Prinzipien der geringsten Rechte und der Aufgabentrennung in Zugriffsberechtigungen und Autorisierungen zu integrieren und so zu verhindern, dass Richtlinien „Effect“: „Allow“ mit „Action“: „*“ anstelle von „Resource“: „*“ enthalten. Wenn Benutzern mehr Rechte eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und der Aufgabentrennung verstoßen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.1.2	Beschränken Sie den Systemzugriff auf jene Transaktionen und Funktionen, die autorisierte Benutzer ausführen dürfen.	iam-root-access-key-überprüfen	Der Zugriff auf Systeme und Ressourcen kann gesteuert werden, indem überprüft wird, ob der Root-Benutzer keine Zugriffsschlüssel mit seiner AWS Identity and Access Management (IAM) -Rolle verknüpft hat. Stellen Sie sicher, dass die Root-Zugriffsschlüssel gelöscht werden. Erstellen und verwenden Sie stattdessen rollenbasierte Funktionen, AWS-Konten um das Prinzip der geringsten Funktionalität zu berücksichtigen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.1.2	Beschränken Sie den Systemzugriff auf jene Transaktionen und Funktionen, die autorisierte Benutzer ausführen dürfen.	iam-user-group-membership-überprüfen	AWS Identity and Access Management (IAM) kann Ihnen helfen, Zugriffsberechtigungen und Autorisierungen einzuschränken, indem sichergestellt wird, dass Benutzer Mitglieder mindestens einer Gruppe sind. Wenn Benutzern mehr Berechtigungen eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und Aufgabentrennung verstoßen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.1.2	Beschränken Sie den Systemzugriff auf jene Transaktionen und Funktionen, die autorisierte Benutzer ausführen dürfen.	iam-user-mfa-enabled	Aktivieren Sie diese Regel, um den Zugriff auf Ressourcen in der AWS Cloud einzuschränken. Diese Regel sorgt dafür, dass die Multi-Faktor-Authentifizierung (MFA) für alle Benutzer aktiviert ist. MFA sorgt für eine weitere Schutzebene zusätzlich zu den Anmeldeinformationen. Reduzieren Sie Fälle von kompromittierten Konten, indem Sie MFA für Benutzer vorschreiben.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.1.2	Beschränken Sie den Systemzugriff auf jene Transaktionen und Funktionen, die autorisierte Benutzer ausführen dürfen.	iam-user-no-policies-überprüfen	Diese Regel stellt sicher, dass AWS Identity and Access Management (IAM) -Richtlinien nur Gruppen oder Rollen zugewiese n werden, um den Zugriff auf Systeme und Ressourcen zu kontrollieren. Die Zuweisung von Berechtig ungen auf Gruppen- oder Rollenebene trägt dazu bei, die Wahrscheinlichkeit zu verringern, dass eine Identität übermäßige Berechtigungen erhält oder beibehält.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.1.2	Beschränken Sie den Systemzugriff auf jene Transaktionen und Funktionen, die autorisierte Benutzer ausführen dürfen.	iam-user-unused-credentials-überprüfen	AWS Identity and Access Management (IAM) kann Ihnen bei Zugriffsberechtigungen und Autorisierungen helfen, indem es nach IAM-Passwörtern und Zugriffsschlüsseln sucht, die für einen bestimmten Zeitraum nicht verwendet wurden. Wenn ungenutzte Anmeldeinformationen identifiziert werden, müssen Sie sie deaktivieren und/oder entfernen, da dies gegen das Prinzip der geringsten Berechtigung verstoßen könnte. Für diese Regel müssen Sie einen Wert für das maxCredentialUsage Alter festlegen (Standardkonfiguration: 90). Der tatsächliche Wert muss den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.1.2	Beschränken Sie den Systemzugriff auf jene Transaktionen und Funktionen, die autorisierte Benutzer ausführen dürfen.	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) Security Groups können bei der Verwaltung des Netzwerkzugriffs helfen, indem sie eine statusbeh aftete Filterung von eingehendem und ausgehendem Netzwerkverkehr zu Ressourcen bereitste llen. AWS Wenn Sie eingehenden (oder entfernten) Datenverk ehr von 0.0.0.0/0 bis Port 22 auf Ihren Ressourcen nicht zulassen, können Sie den Remote-Zugriff einschränken.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.1.2	Beschränken Sie den Systemzugriff auf jene Transaktionen und Funktionen, die autorisierte Benutzer ausführen dürfen.	internet-gateway-authorized-vpc-nur	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Internet-Gateways nur mit autorisierter Amazon Virtual Private Cloud (Amazon VPC) verbunden sind. Internet-Gateways ermöglichen den bidirektionalen Internetzugang zur und von der Amazon VPC, was möglicher weise zu einem unbefugten Zugriff auf Amazon-VPC-Ressourcen führen kann.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.1.2	Beschränken Sie den Systemzugriff auf jene Transaktionen und Funktionen, die autorisierte Benutzer ausführen dürfen.	lambda-function-public-access-verboten	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass AWS Lambda-Funktionen nicht öffentlich zugänglich sind. Der öffentliche Zugriff kann möglicherweise die Verfügbarkeit von Ressourcen beeinträchtigen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.1.2	Beschränken Sie den Systemzugriff auf jene Transaktionen und Funktionen, die autorisierte Benutzer ausführen dürfen.	lambda-inside-vpc	Stellen Sie AWS Lambda-Funktionen in einer Amazon Virtual Private Cloud (Amazon VPC) bereit, um eine sichere Kommunika tion zwischen einer Funktion und anderen Diensten innerhalb der Amazon VPC zu gewährleisten. Bei dieser Konfiguration sind kein Internet-Gateway, kein NAT-Gerät und keine VPN-Verbindung erforderlich. Der gesamte Datenverk ehr bleibt sicher in der Cloud. AWS Domains, die sich innerhalb einer VPC befinden, verfügen aufgrund ihrer logischen Isolierun g im Vergleich zu Domains mit öffentlic hen Endpunkten über eine zusätzliche Sicherheitsebene. Um den Zugriff ordnungsg emäß zu verwalten,

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			sollten AWS Lambda-Funktionen einer VPC zugewiesen werden.
3.1.2	Beschränken Sie den Systemzugriff auf jene Transaktionen und Funktionen, die autorisierte Benutzer ausführen dürfen.	mfa-enabled-for-iam-Konsolenzugriff	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass MFA für alle AWS Identity and Access Management (IAM) -Benutzer aktiviert ist, die über ein Konsolenkennwort verfügen. MFA sorgt für eine weitere Schutzebene zusätzlich zu den Anmeldeinformationen. Indem Sie MFA für Benutzer vorschreiben, können Sie Fälle kompromittierter Konten reduzieren und verhindern, dass unbefugte Benutzer auf vertrauliche Daten zugreifen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.1.2	Beschränken Sie den Systemzugriff auf jene Transaktionen und Funktionen, die autorisierte Benutzer ausführen dürfen.	opensearch-access-control-enabled	Stellen Sie sicher, dass eine differenzierte Zugriffskontrolle für Ihre Amazon OpenSearch Service-Domains aktiviert ist. Eine differenzierte Zugriffskontrolle bietet erweiterte Autorisierungsmechanismen, um den Zugriff auf Amazon Service-Domains mit den geringsten Rechten zu erreichen. OpenSearch Es ermöglicht eine rollenbasierte Zugriffskontrolle auf die Domain sowie Sicherheit auf Index-, Dokument- und Feldebene, Unterstützung für OpenSearch Service-Dashboards, Mehrmandantenfähigkeit und HTTP-Basisauthentifizierung für Service und Kibana. OpenSearch

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.1.2	Beschränken Sie den Systemzugriff auf jene Transaktionen und Funktionen, die autorisierte Benutzer ausführen dürfen.	opensearch-in-vpc-only	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass sich Amazon OpenSearch Service-Domains innerhalb einer Amazon Virtual Private Cloud (Amazon VPC) befinden. Eine Amazon OpenSearch Service-Domain innerhalb einer Amazon VPC ermöglicht die sichere Kommunikation zwischen Amazon OpenSearch Service und anderen Services innerhalb der Amazon VPC, ohne dass ein Internet-Gateway, ein NAT-Gerät oder eine VPN-Verbindung erforderlich ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.1.2	Beschränken Sie den Systemzugriff auf jene Transaktionen und Funktionen, die autorisierte Benutzer ausführen dürfen.	rds-instance-public-access-überprüfen	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Relational Database Service (Amazon RDS) -Instances nicht öffentlich sind. Amazon-RDS-Datenbank-Instances können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.1.2	Beschränken Sie den Systemzugriff auf jene Transaktionen und Funktionen, die autorisierte Benutzer ausführen dürfen.	rds-snapshots-public-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Relational Database Service (Amazon RDS) -Instances nicht öffentlich sind. Amazon-RDS-Datenbank-Instances können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.1.2	Beschränken Sie den Systemzugriff auf jene Transaktionen und Funktionen, die autorisierte Benutzer ausführen dürfen.	redshift-cluster-public-access-überprüfen	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Redshift Redshift-Cluster nicht öffentlich sind. Amazon-Redshift-Cluster können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.1.2	Beschränken Sie den Systemzugriff auf jene Transaktionen und Funktionen, die autorisierte Benutzer ausführen dürfen.	restricted-common-ports	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass gemeinsame Ports für Amazon Elastic Compute Cloud (Amazon EC2) -Sicherheitsgruppen eingeschränkt sind. Wenn der Zugriff auf Ports nicht auf vertrauenswürdige Quellen beschränkt wird, kann dies zu Angriffen auf die Verfügbarkeit, Integrität und Vertraulichkeit von Systemen führen. Mit dieser Regel können Sie optional die Parameter blockedPort1–blockedPort5 festlegen (Standardkonfigurationen: 20, 21, 3389, 3306, 4333). Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.1.2	Beschränken Sie den Systemzugriff auf jene Transaktionen und Funktionen, die autorisierte Benutzer ausführen dürfen.	root-account-hardware-mfa-aktiviert	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Hardware-MFA für den Root-Benutzer aktiviert ist. Der Stammbenutzer ist der AWS-Konto-Benutzer mit den meisten Berechtigungen. MFA sorgt für eine weitere Schutzebene zusätzlich zu den Anmeldeinformationen. Indem Sie MFA für den Root-Benutzer vorschreiben, können Sie die Anzahl AWS-Konten kompromittierter Benutzer reduzieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.1.2	Beschränken Sie den Systemzugriff auf jene Transaktionen und Funktionen, die autorisierte Benutzer ausführen dürfen.	root-account-mfa-enabled	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass MFA für den Root-Benutzer aktiviert ist. Der Stammbenutzer ist der AWS-Konto-Benutzer mit den meisten Berechtigungen. MFA sorgt für eine weitere Schutzebene zusätzlich zu den Anmeldeinformationen. Indem Sie MFA für den Root-Benutzer vorschreiben, können Sie die Anzahl AWS-Konten kompromittierter Benutzer reduzieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.1.2	Beschränken Sie den Systemzugriff auf jene Transaktionen und Funktionen, die autorisierte Benutzer ausführen dürfen.	s3- -blöcke-periodisch account-level-public-access	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Simple Storage Service (Amazon S3) -Buckets nicht öffentlich zugänglich sind. Diese Regel trägt dazu bei, sensible Daten vor unbefugten Remote-Benutzern zu schützen, indem sie den öffentlichen Zugriff verhindert. Mit dieser Regel können Sie optional die Parameter ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) und restrictPublicBuckets Parameter (Config Default: True) festlegen. Die tatsächlichen Werte müssen den Richtlini

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			en Ihrer Organisation entsprechen.
3.1.2	Beschränken Sie den Systemzugriff auf jene Transaktionen und Funktionen, die autorisierte Benutzer ausführen dürfen.	s3 bucket-level-public-access - verboten	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Simple Storage Service (Amazon S3) -Buckets nicht öffentlich zugänglich sind. Diese Regel trägt dazu bei, sensible Daten vor unbefugten Remote-Benutzern zu schützen, indem sie den öffentlichen Zugriff auf Bucket-Ebene verhindert.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.1.2	Beschränken Sie den Systemzugriff auf jene Transaktionen und Funktionen, die autorisierte Benutzer ausführen dürfen.	s-3 bucket-policy-grantee-check	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie s3_bucket_policy_grantee_check aktivieren. Diese Regel prüft, ob der vom Amazon S3 S3-Bucket gewährte Zugriff durch die von Ihnen bereitgestellten AWS Principals, Verbundbenutzer, Service Principals, IP-Adressen oder Amazon Virtual Private Cloud (Amazon VPC) IDs eingeschränkt ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.1.2	Beschränken Sie den Systemzugriff auf jene Transaktionen und Funktionen, die autorisierte Benutzer ausführen dürfen.	s-3 bucket-public-read-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie nur autorisierten Benutzern, Prozessen und Geräten Zugriff auf Amazon Simple Storage Service (Amazon S3) - Buckets gewähren. Die Verwaltung des Zugriffs sollte mit der Klassifizierung der Daten übereinst immen.
3.1.2	Beschränken Sie den Systemzugriff auf jene Transaktionen und Funktionen, die autorisierte Benutzer ausführen dürfen.	s3- bucket-public-write-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie nur autorisierten Benutzern, Prozessen und Geräten Zugriff auf Amazon Simple Storage Service (Amazon S3) - Buckets gewähren. Die Verwaltung des Zugriffs sollte mit der Klassifizierung der Daten übereinst immen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.1.2	Beschränken Sie den Systemzugriff auf jene Transaktionen und Funktionen, die autorisierte Benutzer ausführen dürfen.	sagemaker-notebook-no-direct-Internetzugang	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass SageMaker Amazon-Notebooks keinen direkten Internetzugang zulassen. Indem Sie direkten Internetzugang blockieren, vermeiden Sie, dass unbefugte Benutzer auf sensible Daten zugreifen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.1.2	Beschränken Sie den Systemzugriff auf jene Transaktionen und Funktionen, die autorisierte Benutzer ausführen dürfen.	subnet-auto-assign-public-ip-deaktiviert	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon Virtual Private Cloud (VPC) -Subnetzen nicht automatisch eine öffentliche IP-Adresse zugewiesen wird. Amazon Elastic Compute Cloud (EC2) -Instances, die in Subnetzen gestartet werden, in denen dieses Attribut aktiviert ist, haben ihrer primären Netzwerkschnittstelle eine öffentliche IP-Adresse zugewiesen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.1.2	Beschränken Sie den Systemzugriff auf jene Transaktionen und Funktionen, die autorisierte Benutzer ausführen dürfen.	vpc-default-security-group-geschlossen	Sicherheitsgruppen von Amazon Elastic Compute Cloud (Amazon EC2) können bei der Verwaltung des Netzwerkzugriffs helfen, indem sie eine statusbehaftete Filterung des ein- und ausgehenden Netzwerkverkehrs zu Ressourcen bereitstellen. AWS Die Beschränk ung des gesamten Datenverkehrs auf die Standardsicherheit sgruppe hilft dabei, den Fernzugriff auf Ihre Ressourcen einzuschränken. AWS

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.1.2	Beschränken Sie den Systemzugriff auf jene Transaktionen und Funktionen, die autorisierte Benutzer ausführen dürfen.	vpc-sg-open-only-to-authorized-ports	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass gemeinsame Ports für Amazon Elastic Compute Cloud (Amazon EC2) -Sicherheitsgruppen eingeschränkt sind. Wenn der Zugriff auf Ports nicht auf vertrauenswürdige Quellen beschränkt wird, kann dies zu Angriffen auf die Verfügbarkeit, Integrität und Vertraulichkeit von Systemen führen. Durch die Beschränkung des Zugriffs auf Ressourcen innerhalb einer Sicherheitsgruppe aus dem Internet (0.0.0.0/0) kann der Fernzugriff auf interne Systeme gesteuert werden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.1.3	Steuern Sie den CUI-Ablauf gemäß den genehmigten Autorisierungen.	ec2- instances-in-vpc	Stellen Sie Amazon Elastic Compute Cloud (Amazon EC2) -Instances innerhalb einer Amazon Virtual Private Cloud (Amazon VPC) bereit, um eine sichere Kommunikation zwischen einer Instance und anderen Services innerhalb der Amazon VPC zu ermöglichen, ohne dass ein Internet-Gateway, ein NAT-Gerät oder eine VPN-Verbindung erforderlich ist. Der gesamte Datenverkehr bleibt sicher in der AWS Cloud. Domains, die sich innerhalb einer VPC befinden, verfügen aufgrund ihrer logischen Isolierung im Vergleich zu Domains mit öffentlichen Endpunkten über eine zusätzliche Sicherheitsebene. Weisen Sie EC2

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			Amazon-Instances einer Amazon-VPC zu, um den Zugriff ordnungsgemäß zu verwalten.
3.1.3	Steuern Sie den CUI-Ablauf gemäß den genehmigten Autorisie rungen.	no-unrestricted-route-to-igw	Stellen Sie sicher, dass EC2 Amazon-Routentabellen keine uneingeschränkten Routen zu einem Internet-Gateway enthalten. Durch das Entfernen oder Beschränken des Internetzugangs für Workloads innerhalb von Amazon VPCs können unbeabsic htigte Zugriffe in Ihrer Umgebung reduziert werden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.1.3	Steuern Sie den CUI-Ablauf gemäß den genehmigten Autorisierungen.	ssm-document-not-public	Stellen Sie sicher, dass AWS Systems Manager (SSM) - Dokumente nicht öffentlich sind, da dies einen unbeabsichtigten Zugriff auf Ihre SSM-Dokumente ermöglichen kann. Ein öffentliches SSM-Dokument kann Informationen über Ihr Konto, Ihre Ressourcen und internen Prozesse preisgeben.
3.1.3	Steuern Sie den CUI-Ablauf gemäß den genehmigten Autorisierungen.	dms-replication-not-public	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass auf DMS-Replikationsinstanzen nicht öffentlich zugegriffen werden kann. DMS-Replikations-Instances können vertrauliche Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.1.3	Steuern Sie den CUI-Ablauf gemäß den genehmigten Autorisierungen.	ebs-snapshot-public-restorable-überprüfen	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass EBS-Snapshots nicht öffentlich wiederherstellbar sind. EBS-Volume-Snapshots können vertrauliche Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.
3.1.3	Steuern Sie den CUI-Ablauf gemäß den genehmigten Autorisierungen.	ec-2 instance-no-public-ip	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon Elastic Compute Cloud (Amazon EC2) - Instances nicht öffentlich zugänglich sind. EC2 Amazon-Instances können vertrauliche Informationen enthalten, und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.1.3	Steuern Sie den CUI-Ablauf gemäß den genehmigten Autorisierungen.	elasticsearch-in-vpc-only	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass sich Amazon OpenSearch OpenSearch Service (Service) - Domains innerhalb einer Amazon Virtual Private Cloud (Amazon VPC) befinden. Eine OpenSearch Service-Domain innerhalb einer Amazon VPC ermöglicht die sichere Kommunikation zwischen OpenSearch Service und anderen Services innerhalb der Amazon VPC, ohne dass ein Internet-Gateway, ein NAT-Gerät oder eine VPN-Verbindung erforderlich ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.1.3	Steuern Sie den CUI-Ablauf gemäß den genehmigten Autorisierungen.	emr-master-no-public-ip	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon EMR-Cluster-Masterknoten nicht öffentlich zugänglich sind. Amazon-EMR-Cluster-Hauptknoten können vertrauliche Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.1.3	Steuern Sie den CUI-Ablauf gemäß den genehmigten Autorisierungen.	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) Security Groups können bei der Verwaltung des Netzwerkzugriffs helfen, indem sie eine statusbehaftete Filterung von eingehendem und ausgehendem Netzwerkverkehr zu Ressourcen bereitstellen. AWS Wenn Sie eingehenden (oder entfernten) Datenverkehr von 0.0.0.0/0 bis Port 22 auf Ihren Ressourcen nicht zulassen, können Sie den Remote-Zugriff einschränken.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.1.3	Steuern Sie den CUI-Ablauf gemäß den genehmigten Autorisierungen.	lambda-function-public-access-verboten	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass AWS Lambda-Funktionen nicht öffentlich zugänglich sind. Der öffentliche Zugriff kann möglicherweise die Verfügbarkeit von Ressourcen beeinträchtigen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.1.3	Steuern Sie den CUI-Ablauf gemäß den genehmigten Autorisierungen.	lambda-inside-vpc	Stellen Sie AWS Lambda-Funktionen in einer Amazon Virtual Private Cloud (Amazon VPC) bereit, um eine sichere Kommunikation zwischen einer Funktion und anderen Diensten innerhalb der Amazon VPC zu gewährleisten. Bei dieser Konfiguration sind kein Internet-Gateway, kein NAT-Gerät und keine VPN-Verbindung erforderlich. Der gesamte Datenverkehr bleibt sicher in der Cloud. AWS Domains, die sich innerhalb einer VPC befinden, verfügen aufgrund ihrer logischen Isolierung im Vergleich zu Domains mit öffentlichen Endpunkten über eine zusätzliche Sicherheitsebene. Um den Zugriff ordnungsgemäß zu verwalten,

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			sollten AWS Lambda-Funktionen einer VPC zugewiesen werden.
3.1.3	Steuern Sie den CUI-Ablauf gemäß den genehmigten Autorisierungen.	opensearch-access-control-enabled	Stellen Sie sicher, dass eine differenzierte Zugriffskontrolle für Ihre Amazon OpenSearch Service-Domains aktiviert ist. Eine differenzierte Zugriffskontrolle bietet erweiterte Autorisierungsmechanismen, um den Zugriff auf Amazon Service-Domains mit den geringsten Rechten zu erreichen. OpenSearch Es ermöglicht eine rollenbasierte Zugriffskontrolle auf die Domain sowie Sicherheit auf Index-, Dokument- und Feldebene, Unterstützung für OpenSearch Service-Dashboards, Mehrmandantenfähigkeit und HTTP-Basisauthentifizierung für Service und Kibana. OpenSearch

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.1.3	Steuern Sie den CUI-Ablauf gemäß den genehmigten Autorisierungen.	opensearch-in-vpc-only	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass sich Amazon OpenSearch Service-Domains innerhalb einer Amazon Virtual Private Cloud (Amazon VPC) befinden. Eine Amazon OpenSearch Service-Domain innerhalb einer Amazon VPC ermöglicht die sichere Kommunikation zwischen Amazon OpenSearch Service und anderen Services innerhalb der Amazon VPC, ohne dass ein Internet-Gateway, ein NAT-Gerät oder eine VPN-Verbindung erforderlich ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.1.3	Steuern Sie den CUI-Ablauf gemäß den genehmigten Autorisierungen.	rds-instance-public-access-überprüfen	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Relational Database Service (Amazon RDS) -Instances nicht öffentlich sind. Amazon-RDS-Datenbank-Instances können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.1.3	Steuern Sie den CUI-Ablauf gemäß den genehmigten Autorisierungen.	rds-snapshots-public-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Relational Database Service (Amazon RDS) -Instances nicht öffentlich sind. Amazon-RDS-Datenbank-Instances können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.1.3	Steuern Sie den CUI-Ablauf gemäß den genehmigten Autorisierungen.	redshift-cluster-public-access-überprüfen	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Redshift Redshift-Cluster nicht öffentlich sind. Amazon-Redshift-Cluster können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.1.3	Steuern Sie den CUI-Ablauf gemäß den genehmigten Autorisierungen.	restricted-common-ports	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass gemeinsame Ports für Amazon Elastic Compute Cloud (Amazon EC2) -Sicherheitsgruppen eingeschränkt sind. Wenn der Zugriff auf Ports nicht auf vertrauenswürdige Quellen beschränkt wird, kann dies zu Angriffen auf die Verfügbarkeit, Integrität und Vertraulichkeit von Systemen führen. Mit dieser Regel können Sie optional die Parameter blockedPort1–blockedPort5 festlegen (Standardkonfigurationen: 20, 21, 3389, 3306, 4333). Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.1.3	Steuern Sie den CUI-Ablauf gemäß den genehmigten Autorisierungen.	s3- account-level-public-access -Block-periodisch	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Simple Storage Service (Amazon S3) -Buckets nicht öffentlich zugänglich sind. Diese Regel trägt dazu bei, sensible Daten vor unbefugten Remote-Benutzern zu schützen, indem sie den öffentlichen Zugriff verhindert. Mit dieser Regel können Sie optional die Parameter ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) und restrictPublicBuckets Parameter (Config Default: True) festlegen. Die tatsächlichen Werte müssen den Richtlini

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			en Ihrer Organisation entsprechen.
3.1.3	Steuern Sie den CUI-Ablauf gemäß den genehmigten Autorisierungen.	s3 bucket-level-public-access - verboten	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Simple Storage Service (Amazon S3) -Buckets nicht öffentlich zugänglich sind. Diese Regel trägt dazu bei, sensible Daten vor unbefugten Remote-Benutzern zu schützen, indem sie den öffentlichen Zugriff auf Bucket-Ebene verhindert.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.1.3	Steuern Sie den CUI-Ablauf gemäß den genehmigten Autorisierungen.	s-3 bucket-public-read-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie nur autorisierten Benutzern, Prozessen und Geräten Zugriff auf Amazon Simple Storage Service (Amazon S3) - Buckets gewähren. Die Verwaltung des Zugriffs sollte mit der Klassifizierung der Daten übereinstimmen.
3.1.3	Steuern Sie den CUI-Ablauf gemäß den genehmigten Autorisierungen.	s3- bucket-public-write-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie nur autorisierten Benutzern, Prozessen und Geräten Zugriff auf Amazon Simple Storage Service (Amazon S3) - Buckets gewähren. Die Verwaltung des Zugriffs sollte mit der Klassifizierung der Daten übereinstimmen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.1.3	Steuern Sie den CUI-Ablauf gemäß den genehmigten Autorisierungen.	sagemaker-notebook-no-direct-Internetzugang	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass SageMaker Amazon-Notebooks keinen direkten Internetzugang zulassen. Indem Sie direkten Internetzugang blockieren, vermeiden Sie, dass unbefugte Benutzer auf sensible Daten zugreifen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.1.3	Steuern Sie den CUI-Ablauf gemäß den genehmigten Autorisierungen.	vpc-default-security-group-geschlossen	Sicherheitsgruppen von Amazon Elastic Compute Cloud (Amazon EC2) können bei der Verwaltung des Netzwerkzugriffs helfen, indem sie eine statusbehaftete Filterung des ein- und ausgehenden Netzwerkverkehrs zu Ressourcen bereitstellen. AWS Die Beschränkung des gesamten Datenverkehrs auf die Standardsicherheitsgruppe hilft dabei, den Fernzugriff auf Ihre Ressourcen einzuschränken. AWS

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.1.3	Steuern Sie den CUI-Ablauf gemäß den genehmigten Autorisierungen.	vpc-sg-open-only-to-authorized-ports	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass gemeinsame Ports für Amazon Elastic Compute Cloud (Amazon EC2) -Sicherheitsgruppen eingeschränkt sind. Wenn der Zugriff auf Ports nicht auf vertrauenswürdige Quellen beschränkt wird, kann dies zu Angriffen auf die Verfügbarkeit, Integrität und Vertraulichkeit von Systemen führen. Durch die Beschränkung des Zugriffs auf Ressourcen innerhalb einer Sicherheitsgruppe aus dem Internet (0.0.0.0/0) kann der Fernzugriff auf interne Systeme gesteuert werden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.1.4	Teilen Sie Aufgaben auf mehrere Personen auf, um das Risiko böswilliger Aktivitäten durch fehlende Absprache zu verringern.	ec2- instance-profile-attached	EC2 Instanzprofile übergeben eine IAM-Rolle an eine EC2 Instance. Das Anhängen eines Instance-Profils an Ihre Instances kann bei der Implementierung von geringsten Berechtigungen und der Berechtigungsverwaltung helfen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.1.4	Teilen Sie Aufgaben auf mehrere Personen auf, um das Risiko böswilliger Aktivität en durch fehlende Absprache zu verringern.	ecs-task-definition-user-for-host-mode-check	Wenn für eine Aufgabendefinition erhöhte Berechtig ungen gelten, liegt das daran, dass der Kunde diesen Konfigura tionen ausdrücklich zugestimmt hat. Diese Kontrolle prüft, ob eine unerwartete Berechtigungseskal ation vorliegt, wenn für eine Aufgabend efinition das Host-Netzwerk aktiviert ist, die Kunden aber keine erhöhten Berechtigungen aktiviert haben.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.1.4	Teilen Sie Aufgaben auf mehrere Personen auf, um das Risiko böswilliger Aktivität en durch fehlende Absprache zu verringern.	iam-no-inline-policy-überprüfen	Stellen Sie sicher, dass ein Benutzer, eine IAM-Rolle oder eine IAM-Gruppe (AWS Identity and Access Management) nicht über eine Inline-Richtlinie zur Zugriffsk ontrolle auf Systeme und Ressource n verfügt. AWS empfiehlt, verwaltet e Richtlinien anstelle von Inline-Richtlinien zu verwenden. Verwaltete Richtlini en ermöglichen Wiederverwendbarke it, Versionsverwaltung , Rollback und Delegierung der Berechtigungsverwa ltung.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.1.4	Teilen Sie Aufgaben auf mehrere Personen auf, um das Risiko böswilliger Aktivitäten durch fehlende Absprache zu verringern.	iam-policy-no-statements-with-full-access	Stellen Sie sicher, dass IAM-Aktionen nur auf die benötigten Aktionen beschränkt sind. Wenn Benutzern mehr Rechte eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Rechte und der Aufgabentrennung verstoßen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.1.4	Teilen Sie Aufgaben auf mehrere Personen auf, um das Risiko böswilliger Aktivitäten durch fehlende Absprache zu verringern.	emr-kerberos-enabled	Die Zugriffsberechtigungen und -autorisierungen können verwaltet und nach den Prinzipien der geringsten Berechtigung und Aufgabentrennung integriert werden, indem Kerberos für Amazon-EMR-Cluster aktiviert wird. In Kerberos werden Services und Benutzer, die sich authentifizieren müssen, als Prinzipale bezeichnet. Prinzipale befinden sich in einem Kerberos-Bereich. Innerhalb dieses Bereichs wird ein Kerberos-Server als Key Distribution Center (KDC) bezeichnet. Über diesen Server können sich Prinzipale authentifizieren. Die Authentifizierung im KDC erfolgt durch die Ausstellung von Authentif

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			izierungstickets. Das KDC unterhält eine Datenbank der Prinzipale in seinem Bereich mit ihren Passwörtern und anderen administr ativen Informationen zu jedem Prinzipal.
3.1.4	Teilen Sie Aufgaben auf mehrere Personen auf, um das Risiko böswilliger Aktivität en durch fehlende Absprache zu verringern.	iam-group-has-users-überprüfen	AWS Identity and Access Managemen t (IAM) kann Ihnen helfen, die Prinzipien der geringsten Rechte und der Aufgabent rennung mit Zugriffsb erechtigungen und Autorisierungen zu integrieren, indem sichergestellt wird, dass IAM-Gruppen mindestens einen Benutzer haben. Die Einteilung von Benutzern in Gruppen auf der Grundlage der ihnen zugewiese nen Berechtigungen oder ihrer Funktion ist eine Möglichkeit, das Prinzip der geringste n Berechtigung zu implementieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.1.4	Teilen Sie Aufgaben auf mehrere Personen auf, um das Risiko böswilliger Aktivitäten durch fehlende Absprache zu verringern.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) kann Ihnen dabei helfen, die Prinzipien der geringsten Rechte und der Aufgabentrennung in Zugriffsberechtigungen und Autorisierungen zu integrieren und so zu verhindern, dass Richtlinien „Effect“: „Allow“ mit „Action“: „*“ anstelle von „Resource“: „*“ enthalten. Wenn Benutzern mehr Rechte eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und der Aufgabentrennung verstoßen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.1.4	Teilen Sie Aufgaben auf mehrere Personen auf, um das Risiko böswilliger Aktivität en durch fehlende Absprache zu verringern.	iam-root-access-key-überprüfen	Der Zugriff auf Systeme und Ressourcen kann gesteuert werden, indem überprüft wird, ob der Root-Benu tzer keine Zugriffss chlüssel mit seiner AWS Identity and Access Management (IAM) -Rolle verknüpft hat. Stellen Sie sicher, dass die Root-Zugr iffsschlüssel gelöscht werden. Erstellen und verwenden Sie stattdessen rollenbas ierte Funktionen, AWS-Konten um das Prinzip der geringste n Funktionalität zu berücksichtigen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.1.4	Teilen Sie Aufgaben auf mehrere Personen auf, um das Risiko böswilliger Aktivitäten durch fehlende Absprache zu verringern.	iam-user-group-membership-überprüfen	AWS Identity and Access Management (IAM) kann Ihnen helfen, Zugriffsberechtigungen und Autorisierungen einzuschränken, indem sichergestellt wird, dass Benutzer Mitglieder mindestens einer Gruppe sind. Wenn Benutzern mehr Berechtigungen eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und Aufgabentrennung verstoßen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.1.4	Teilen Sie Aufgaben auf mehrere Personen auf, um das Risiko böswilliger Aktivität en durch fehlende Absprache zu verringern.	iam-user-no-policies-überprüfen	Diese Regel stellt sicher, dass AWS Identity and Access Management (IAM) -Richtlinien nur Gruppen oder Rollen zugewiese n werden, um den Zugriff auf Systeme und Ressourcen zu kontrollieren. Die Zuweisung von Berechtig ungen auf Gruppen- oder Rollenebene trägt dazu bei, die Wahrscheinlichkeit zu verringern, dass eine Identität übermäßige Berechtigungen erhält oder beibehält.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.1.4	Teilen Sie Aufgaben auf mehrere Personen auf, um das Risiko böswilliger Aktivitäten durch fehlende Absprache zu verringern.	iam-user-unused-credentials-überprüfen	AWS Identity and Access Management (IAM) kann Ihnen bei Zugriffsberechtigungen und Autorisierungen helfen, indem es nach IAM-Passwörtern und Zugriffsschlüsseln sucht, die für einen bestimmten Zeitraum nicht verwendet wurden. Wenn ungenutzte Anmeldeinformationen identifiziert werden, müssen Sie sie deaktivieren und/oder entfernen, da dies gegen das Prinzip der geringsten Berechtigung verstoßen könnte. Für diese Regel müssen Sie einen Wert für das maxCredentialUsage Alter festlegen (Standardkonfiguration: 90). Der tatsächliche Wert muss den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.1.4	Teilen Sie Aufgaben auf mehrere Personen auf, um das Risiko böswilliger Aktivitäten durch fehlende Absprache zu verringern.	opensearch-access-control-enabled	Stellen Sie sicher, dass eine differenzierte Zugriffskontrolle für Ihre Amazon OpenSearch Service-Domains aktiviert ist. Eine differenzierte Zugriffskontrolle bietet erweiterte Autorisierungsmechanismen, um den Zugriff auf Amazon Service-Domains mit den geringsten Rechten zu erreichen. OpenSearch Es ermöglicht eine rollenbasierte Zugriffskontrolle auf die Domain sowie Sicherheit auf Index-, Dokument- und Feldebene, Unterstützung für OpenSearch Service-Dashboards, Mehrmandantenfähigkeit und HTTP-Basisauthentifizierung für Service und Kibana. OpenSearch

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.1.4	Teilen Sie Aufgaben auf mehrere Personen auf, um das Risiko böswilliger Aktivitäten durch fehlende Absprache zu verringern.	s-3 bucket-policy-grantee-check	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie s3_bucket_policy_grantee_check aktivieren. Diese Regel prüft, ob der vom Amazon S3 S3-Bucket gewährte Zugriff durch die von Ihnen bereitgestellten AWS Principals, Verbundbenutzer, Service Principals, IP-Adressen oder Amazon Virtual Private Cloud (Amazon VPC) IDs eingeschränkt ist.
3.1.5	Wenden Sie das Prinzip der geringsten Berechtigung an, auch für spezifische Sicherheitsfunktionen und privilegierte Konten.	ec2- instance-profile-attached	EC2 Instanzprofile übergeben eine IAM-Rolle an eine EC2 Instance. Das Anhängen eines Instance-Profils an Ihre Instances kann bei der Implementierung von geringsten Berechtigungen und der Berechtigungsverwaltung helfen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.1.5	Wenden Sie das Prinzip der geringsten Berechtigung an, auch für spezifische Sicherheitsfunktionen und privilegierte Konten.	ecs-task-definition-user-for-host-mode-check	Wenn für eine Aufgabendefinition erhöhte Berechtigungen gelten, liegt das daran, dass der Kunde diesen Konfigurationen ausdrücklich zugestimmt hat. Diese Kontrolle prüft, ob eine unerwartete Berechtigungseskalation vorliegt, wenn für eine Aufgabendefinition das Host-Netzwerk aktiviert ist, die Kunden aber keine erhöhten Berechtigungen aktiviert haben.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.1.5	Wenden Sie das Prinzip der geringsten Berechtigung an, auch für spezifische Sicherheitsfunktionen und privilegierte Konten.	iam-no-inline-policy-überprüfen	Stellen Sie sicher, dass ein Benutzer, eine IAM-Rolle oder eine IAM-Gruppe (AWS Identity and Access Management) nicht über eine Inline-Richtlinie zur Zugriffskontrolle auf Systeme und Ressourcen verfügt. AWS empfiehlt, verwaltete Richtlinien anstelle von Inline-Richtlinien zu verwenden. Verwaltete Richtlinien ermöglichen Wiederverwendbarkeit, Versionsverwaltung, Rollback und Delegierung der Berechtigungsverwaltung.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.1.5	Wenden Sie das Prinzip der geringsten Berechtigung an, auch für spezifische Sicherheitsfunktionen und privilegierte Konten.	iam-policy-no-statements-with-full-access	Stellen Sie sicher, dass IAM-Aktionen nur auf die benötigten Aktionen beschränkt sind. Wenn Benutzern mehr Rechte eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Rechte und der Aufgabentrennung verstoßen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.1.5	Wenden Sie das Prinzip der geringsten Berechtigung an, auch für spezifische Sicherheitsfunktionen und privilegierte Konten.	ecs-containers-nonprivileged	Um die Implementierung des Prinzips der geringsten Berechtigung zu unterstützen, dürfen in Amazon Elastic Container Service (Amazon ECS)-Aufgabendefinitionen keine erhöhten Berechtigungen aktiviert sein. Wenn dieser Parameter den Wert „true“ aufweist, erhält der Container erhöhte Berechtigungen auf der Host-Container-Instance (ähnlich wie der Root-Benutzer).

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.1.5	Wenden Sie das Prinzip der geringsten Berechtigung an, auch für spezifische Sicherheitsfunktionen und privilegierte Konten.	ecs-containers-readonly-access	Die Aktivierung des schreibgeschützten Zugriffs auf Amazon Elastic Container Service (ECS)-Container kann dazu beitragen, das Prinzip der geringsten Berechtigung einzuhalten. Diese Option kann Angriffsvektoren reduzieren, da das Dateisystem der Container-Instance nur geändert werden kann, wenn es über ausdrückliche Lese- und Schreibberechtigungen verfügt.
3.1.5	Wenden Sie das Prinzip der geringsten Berechtigung an, auch für spezifische Sicherheitsfunktionen und privilegierte Konten.	ecs-task-definition-nonroot-Benutzer	Sie bestimmen einen Nicht-Root-Benutzer für den Zugriff auf Ihre Aufgabendefinitionen des Amazon Elastic Container Service (Amazon ECS), um die Implementierung des Prinzips der geringsten Berechtigung zu unterstützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.1.5	Wenden Sie das Prinzip der geringsten Berechtigung an, auch für spezifische Sicherheitsfunktionen und privilegierte Konten.	efs-access-point-enforce-Benutzeridentität	Um die Implementierung des Prinzips der geringsten Rechte zu unterstützen, stellen Sie sicher, dass die Benutzerdurchsetzung für Ihr Amazon Elastic File System (Amazon EFS) aktiviert ist. Wenn diese Option aktiviert ist, ersetzt Amazon EFS den Benutzer und die Gruppe IDs des NFS-Clients durch die Identität, die auf dem Access Point für alle Dateisystemoperationen konfiguriert ist, und gewährt nur Zugriff auf diese erzwungene Benutzeridentität.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.1.5	Wenden Sie das Prinzip der geringsten Berechtigung an, auch für spezifische Sicherheitsfunktionen und privilegierte Konten.	emr-kerberos-enabled	Die Zugriffsberechtigungen und -autorisierungen können verwaltet und nach den Prinzipien der geringsten Berechtigung und Aufgabentrennung integriert werden, indem Kerberos für Amazon-EMR-Cluster aktiviert wird. In Kerberos werden Services und Benutzer, die sich authentifizieren müssen, als Prinzipale bezeichnet. Prinzipale befinden sich in einem Kerberos-Bereich. Innerhalb dieses Bereichs wird ein Kerberos-Server als Key Distribution Center (KDC) bezeichnet. Über diesen Server können sich Prinzipale authentifizieren. Die Authentifizierung im KDC erfolgt durch die Ausstellung von Authentif

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			izierungstickets. Das KDC unterhält eine Datenbank der Prinzipale in seinem Bereich mit ihren Passwörtern und anderen administr ativen Informationen zu jedem Prinzipal.
3.1.5	Wenden Sie das Prinzip der geringste n Berechtigung an, auch für spezifische Sicherheitsfunktio nen und privilegierte Konten.	iam-group-has-users-überprüfen	AWS Identity and Access Managemen t (IAM) kann Ihnen helfen, die Prinzipien der geringsten Rechte und der Aufgabent rennung mit Zugriffsb erechtigungen und Autorisierungen zu integrieren, indem sichergestellt wird, dass IAM-Gruppen mindestens einen Benutzer haben. Die Einteilung von Benutzern in Gruppen auf der Grundlage der ihnen zugewiese nen Berechtigungen oder ihrer Funktion ist eine Möglichkeit, das Prinzip der geringste n Berechtigung zu implementieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.1.5	Wenden Sie das Prinzip der geringsten Berechtigung an, auch für spezifische Sicherheitsfunktionen und privilegierte Konten.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) kann Ihnen dabei helfen, die Prinzipien der geringsten Rechte und der Aufgabentrennung in Zugriffsberechtigungen und Autorisierungen zu integrieren und so zu verhindern, dass Richtlinien „Effect“: „Allow“ mit „Action“: „*“ anstelle von „Resource“: „*“ enthalten. Wenn Benutzern mehr Rechte eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und der Aufgabentrennung verstoßen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.1.5	Wenden Sie das Prinzip der geringsten Berechtigung an, auch für spezifische Sicherheitsfunktionen und privilegierte Konten.	iam-root-access-key-überprüfen	Der Zugriff auf Systeme und Ressourcen kann gesteuert werden, indem überprüft wird, ob der Root-Benutzer keine Zugriffsschlüssel mit seiner AWS Identity and Access Management (IAM) -Rolle verknüpft hat. Stellen Sie sicher, dass die Root-Zugriffsschlüssel gelöscht werden. Erstellen und verwenden Sie stattdessen rollenbasierte Funktionen, AWS-Konten um das Prinzip der geringsten Funktionalität zu berücksichtigen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.1.5	Wenden Sie das Prinzip der geringsten Berechtigung an, auch für spezifische Sicherheitsfunktionen und privilegierte Konten.	iam-user-group-membership-überprüfen	AWS Identity and Access Management (IAM) kann Ihnen helfen, Zugriffsberechtigungen und Autorisierungen einzuschränken, indem sichergestellt wird, dass Benutzer Mitglieder mindestens einer Gruppe sind. Wenn Benutzern mehr Berechtigungen eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und Aufgabentrennung verstoßen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.1.5	Wenden Sie das Prinzip der geringsten Berechtigung an, auch für spezifische Sicherheitsfunktionen und privilegierte Konten.	iam-user-no-policies-überprüfen	Diese Regel stellt sicher, dass AWS Identity and Access Management (IAM) -Richtlinien nur Gruppen oder Rollen zugewiesen werden, um den Zugriff auf Systeme und Ressourcen zu kontrollieren. Die Zuweisung von Berechtigungen auf Gruppen- oder Rollenebene trägt dazu bei, die Wahrscheinlichkeit zu verringern, dass eine Identität übermäßige Berechtigungen erhält oder beibehält.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.1.5	Wenden Sie das Prinzip der geringsten Berechtigung an, auch für spezifische Sicherheitsfunktionen und privilegierte Konten.	iam-user-unused-credentials-überprüfen	AWS Identity and Access Management (IAM) kann Ihnen bei Zugriffsberechtigungen und Autorisierungen helfen, indem es nach IAM-Passwörtern und Zugriffsschlüsseln sucht, die für einen bestimmten Zeitraum nicht verwendet wurden. Wenn ungenutzte Anmeldeinformationen identifiziert werden, müssen Sie sie deaktivieren und/oder entfernen, da dies gegen das Prinzip der geringsten Berechtigung verstoßen könnte. Für diese Regel müssen Sie einen Wert für das maxCredentialUsage Alter festlegen (Standardkonfiguration: 90). Der tatsächliche Wert muss den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.1.5	Wenden Sie das Prinzip der geringsten Berechtigung an, auch für spezifische Sicherheitsfunktionen und privilegierte Konten.	opensearch-access-control-enabled	Stellen Sie sicher, dass eine differenzierte Zugriffskontrolle für Ihre Amazon OpenSearch Service-Domains aktiviert ist. Eine differenzierte Zugriffskontrolle bietet erweiterte Autorisierungsmechanismen, um den Zugriff auf Amazon Service-Domains mit den geringsten Rechten zu erreichen. OpenSearch Es ermöglicht eine rollenbasierte Zugriffskontrolle auf die Domain sowie Sicherheit auf Index-, Dokument- und Feldebene, Unterstützung für OpenSearch Service-Dashboards, Mehrmandantenfähigkeit und HTTP-Basisauthentifizierung für Service und Kibana. OpenSearch

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.1.5	Wenden Sie das Prinzip der geringsten Berechtigung an, auch für spezifische Sicherheitsfunktionen und privilegierte Konten.	s-3 bucket-policy-grantee-check	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie s3_bucket_policy_grantee_check aktivieren. Diese Regel prüft, ob der vom Amazon S3 S3-Bucket gewährte Zugriff durch die von Ihnen bereitgestellten AWS Principals, Verbundbenutzer, Service Principals, IP-Adressen oder Amazon Virtual Private Cloud (Amazon VPC) IDs eingeschränkt ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.1.6	Verwenden Sie Konten oder Rollen ohne Berechtigungen, wenn Sie auf nicht sicherheitsrelevante Funktionen zugreifen.	iam-root-access-key-überprüfen	Der Zugriff auf Systeme und Ressourcen kann gesteuert werden, indem überprüft wird, ob der Root-Benutzer keine Zugriffsschlüssel mit seiner AWS Identity and Access Management (IAM) -Rolle verknüpft hat. Stellen Sie sicher, dass die Root-Zugriffsschlüssel gelöscht werden. Erstellen und verwenden Sie stattdessen rollenbasierte Funktionen, AWS-Konten um das Prinzip der geringsten Funktionalität zu berücksichtigen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.1.7	Verhindern Sie, dass nicht privilegierte Benutzer privilegierte Funktionen ausführen und überprüfen Sie die Ausführung solcher Funktionen.	iam-policy-no-statements-with-full-access	Stellen Sie sicher, dass IAM-Aktionen nur auf die benötigten Aktionen beschränkt sind. Wenn Benutzern mehr Rechte eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Rechte und der Aufgabentrennung verstoßen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.1.7	Verhindern Sie, dass nicht privilegierte Benutzer privilegierte Funktionen ausführen und überprüfen Sie die Ausführung solcher Funktionen.	emr-kerberos-enabled	Die Zugriffsberechtigungen und -autorisierungen können verwaltet und nach den Prinzipien der geringsten Berechtigung und Aufgabentrennung integriert werden, indem Kerberos für Amazon-EMR-Cluster aktiviert wird. In Kerberos werden Services und Benutzer, die sich authentifizieren müssen, als Prinzipale bezeichnet. Prinzipale befinden sich in einem Kerberos-Bereich. Innerhalb dieses Bereichs wird ein Kerberos-Server als Key Distribution Center (KDC) bezeichnet. Über diesen Server können sich Prinzipale authentifizieren. Die Authentifizierung im KDC erfolgt durch die Ausstellung von Authentif

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			izierungstickets. Das KDC unterhält eine Datenbank der Prinzipale in seinem Bereich mit ihren Passwörtern und anderen administr ativen Informationen zu jedem Prinzipal.
3.1.7	Verhindern Sie, dass nicht privilegierte Benutzer privilegierte Funktionen ausführen und überprüfen Sie die Ausführung solcher Funktionen.	iam-group-has-users-überprüfen	AWS Identity and Access Managemen t (IAM) kann Ihnen helfen, die Prinzipien der geringsten Rechte und der Aufgabent rennung mit Zugriffsb erechtigungen und Autorisierungen zu integrieren, indem sichergestellt wird, dass IAM-Gruppen mindestens einen Benutzer haben. Die Einteilung von Benutzern in Gruppen auf der Grundlage der ihnen zugewiese nen Berechtigungen oder ihrer Funktion ist eine Möglichkeit, das Prinzip der geringste n Berechtigung zu implementieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.1.7	Verhindern Sie, dass nicht privilegierte Benutzer privilegierte Funktionen ausführen und überprüfen Sie die Ausführung solcher Funktionen.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) kann Ihnen dabei helfen, die Prinzipien der geringsten Rechte und der Aufgabentrennung in Zugriffsberechtigungen und Autorisierungen zu integrieren und so zu verhindern, dass Richtlinien „Effect“: „Allow“ mit „Action“: „*“ anstelle von „Resource“: „*“ enthalten. Wenn Benutzern mehr Rechte eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und der Aufgabentrennung verstoßen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.1.7	Verhindern Sie, dass nicht privilegierte Benutzer privilegierte Funktionen ausführen und überprüfen Sie die Ausführung solcher Funktionen.	iam-root-access-key-überprüfen	Der Zugriff auf Systeme und Ressourcen kann gesteuert werden, indem überprüft wird, ob der Root-Benutzer keine Zugriffsschlüssel mit seiner AWS Identity and Access Management (IAM) -Rolle verknüpft hat. Stellen Sie sicher, dass die Root-Zugriffsschlüssel gelöscht werden. Erstellen und verwenden Sie stattdessen rollenbasierte Funktionen, AWS-Konten um das Prinzip der geringsten Funktionalität zu berücksichtigen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.1.7	Verhindern Sie, dass nicht privilegierte Benutzer privilegierte Funktionen ausführen und überprüfen Sie die Ausführung solcher Funktionen.	iam-user-group-membership-überprüfen	AWS Identity and Access Management (IAM) kann Ihnen helfen, Zugriffsberechtigungen und Autorisierungen einzuschränken, indem sichergestellt wird, dass Benutzer Mitglieder mindestens einer Gruppe sind. Wenn Benutzern mehr Berechtigungen eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und Aufgabentrennung verstoßen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.1.7	Verhindern Sie, dass nicht privilegierte Benutzer privilegierte Funktionen ausführen und überprüfen Sie die Ausführung solcher Funktionen.	s-3 bucket-policy-grantee-check	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie s3_bucket_policy_grantee_check aktivieren. Diese Regel prüft, ob der vom Amazon S3 S3-Bucket gewährte Zugriff durch die von Ihnen bereitgestellten AWS Principals, Verbundbenutzer, Service Principals, IP-Adressen oder Amazon Virtual Private Cloud (Amazon VPC) IDs eingeschränkt ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.1.12	Überwachen und steuern Sie Fernzugriffssitzungen.	elasticsearch-logs-to-cloudwatch	Stellen Sie sicher, dass für Amazon OpenSearch Service-Domains Fehlerprotokolle aktiviert und zur Aufbewahrung und Beantwortung an Amazon CloudWatch Logs gestreamt werden. Domain-Fehlerprotokolle sind bei Sicherheits- und Zugriffsprüfungen sowie bei der Diagnose von Verfügbarkeitsproblemen nützlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.1.12	Überwachen und steuern Sie Fernzugriffssitzungen.	multi-region-cloudtrail-enabled	AWS CloudTrail zeichnet Aktionen und API-Aufrufe der AWS Management Console auf. Sie können feststellen, welche Benutzer und Konten angerufen wurden AWS, von welcher Quell-IP-Adresse aus die Anrufe getätigt wurden und wann die Anrufe erfolgten. CloudTrail übermittelt Protokolldateien aus allen AWS Regionen an Ihren S3-Bucket, wenn MULTI_REGION_CLOUD_TRAIL_ENABLED aktiviert ist. Außerdem wird beim AWS Start einer neuen Region derselbe Trail in der neuen Region erstellt. CloudTrail Dadurch erhalten Sie automatisch Protokolldateien mit API-Aktivitäten für die neue Region.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.1.12	Überwachen und steuern Sie Fernzugriffssitzungen.	rds-logging-enabled	Um die Protokollierung und Überwachung in Ihrer Umgebung zu erleichtern, stellen Sie sicher, dass die Amazon Relational Database Service (Amazon RDS)-Protokollierung aktiviert ist. Mit der Amazon-RDS-Protokollierung können Sie Ereignisse wie Verbindungen, Verbindungsabbrüche, Abfragen oder abgefragte Tabellen erfassen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.1.12	Überwachen und steuern Sie Fernzugriffssitzungen.	securityhub-enabled	AWS Security Hub hilft bei der Überwachung von unbefugtem Personal, Verbindungen, Geräten und Software. AWS Security Hub aggregiert, organisiert und priorisiert die Sicherheitswarnungen oder Ergebnisse mehrerer Dienste. AWS Einige dieser Dienste sind Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer und AWS Firewall Manager sowie AWS Partnerlösungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.1.12	Überwachen und steuern Sie Fernzugriffssitzungen.	wafv2-logging-enabled	Um die Protokollierung und Überwachung in Ihrer Umgebung zu erleichtern, aktivieren Sie die AWS WAF (V2) -Protokollierung im regionalen und globalen Web. ACLs AWS Die WAF-Protokollierung bietet detaillierte Informationen über den Datenverkehr, der von Ihrer Web-ACL analysiert wird. In den Protokollen werden die Uhrzeit aufgezeichnet, zu der die AWS WAF die Anfrage von Ihrer AWS Ressource erhalten hat, Informationen über die Anfrage und eine Aktion für die Regel, der jede Anfrage entsprach.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.1.12	Überwachen und steuern Sie Fernzugriffssitzungen.	api-gw-execution-logging-aktiviert	Die API-Gateway-Protokollierung zeigt detaillierte Ansichten der Benutzer, die auf die API zugegriffen haben, und wie diese Benutzer auf die API zugegriffen haben. Diese Insights ermöglichen die Einsicht in Benutzeraktivitäten.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.1.12	Überwachen und steuern Sie Fernzugriffssitzungen.	cloudtrail-enabled	AWS CloudTrail kann durch die Aufzeichnung von Aktionen und API-Aufrufen in der AWS Management Console bei der Nichtabstreitbarkeit helfen. Sie können die Benutzer und die Benutzer AWS-Konten , die einen AWS Dienst aufgerufen haben, die Quell-IP-Adresse, über die die Aufrufe generiert wurden, und den Zeitpunkt der Anrufe identifizieren. Einzelheiten zu den erfassten Daten finden Sie in den AWS CloudTrail Datensatzinhalten.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.1.12	Überwachen und steuern Sie Fernzugriffssitzungen.	cloudtrail-s3-dataevents-enabled	Die Erfassung von Simple Storage Service (Amazon S3)-Datenereignissen unterstützt die Erkennung von ungewöhnlichen Aktivitäten. Zu den Details gehören AWS-Konto Informationen über den Zugriff auf einen Amazon S3 S3-Bucket, die IP-Adresse und die Uhrzeit des Ereignisses.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.1.12	Überwachen und steuern Sie Fernzugriffssitzungen.	elb-logging-enabled	Die Elastic-Load-Balancing-Aktivität ist ein zentraler Kommunikationspunkt innerhalb einer Umgebung. Stellen Sie sicher, dass die ELB-Protokollierung aktiviert ist. Die gesammelten Daten enthalten detaillierte Informationen zu Anfragen, die an den ELB gesendet wurden. Jedes Protokoll enthält Informationen wie die Zeit, zu der die Anforderung einging, die Client-IP-Adresse, Latenzen, Anforderungspfade und Serverantworten.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.1.12	Überwachen und steuern Sie Fernzugriffssitzungen.	guardduty-enabled-centralized	Amazon GuardDuty kann mithilfe von Threat Intelligence Feeds helfen, potenzielle Cybersicherheitsereignisse zu überwachen und zu erkennen. Dazu gehören Listen mit bösartigen IPs und maschinellen Lernmethoden zur Identifizierung unerwarteter, nicht autorisierter und bösartiger Aktivitäten in Ihrer AWS Cloud-Umgebung.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.1.12	Überwachen und steuern Sie Fernzugriffssitzungen.	opensearch-logs-to-cloudwatch	Stellen Sie sicher, dass für Amazon OpenSearch Service-Domains Fehlerprotokolle aktiviert und zur Aufbewahrung und Beantwortung an Amazon CloudWatch Logs gestreamt werden. OpenSearch Service-Fehlerprotokolle können bei Sicherheits- und Zugriffsprüfungen helfen und bei der Diagnose von Verfügbarkeitsproblemen helfen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.1.12	Überwachen und steuern Sie Fernzugriffssitzungen.	s-3 bucket-logging-enabled	Die Amazon Simple Storage Service (Amazon S3)-Serverzugriffsprotokollierung bietet eine Methode zur Überwachung des Netzwerks im Hinblick auf potenzielle Cybersicherheitsereignisse. Die Ereignisse werden überwacht, indem detaillierte Aufzeichnungen über die Anfragen erfasst werden, die an einen Amazon-S3-Bucket gestellt wurden. Jeder Zugriffsprotokolleintrag enthält Details zu einer einzelnen Zugriffsanfrage. Zu den Details gehören Anforderer, Bucket-Name, Anforderungszeit, Anforderungsaktion, Antwortstatus und Fehlercode, falls relevant.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.1.12	Überwachen und steuern Sie Fernzugriffssitzungen.	vpc-flow-logs-enabled	VPC-Flow-Protokolle erfassen detaillierte Informationsdatensätze über den IP-Datenverkehr, der zu und von Netzwerkschnittstellen in Ihrer Amazon Virtual Private Cloud (Amazon VPC) fließt. Standardmäßig enthalten Flow-Protokolldatensätze Werte für die verschiedenen Komponenten des IP-Flows, einschließlich Quelle, Ziel und Protokoll.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.1.13	Setzen Sie kryptografische Mechanismen ein, um die Vertraulichkeit von Fernzugriffssitzungen zu schützen.	elv v2 acm-certificate-required	Zum Schutz von eventuell vorhanden en sensiblen Daten sowie von Daten während der Übertragung muss die Verschlüsselung für Ihr Elastic Load Balancing aktiviert sein. Verwenden Sie AWS Certificate Manager, um öffentliche und private SSL/TLS-Zertifikate mit AWS Diensten und internen Ressourcen zu verwalten, bereitzustellen und bereitzustellen.
3.1.13	Setzen Sie kryptografische Mechanismen ein, um die Vertraulichkeit von Fernzugriffssitzungen zu schützen.	elb-tls-https-listeners-nur	Stellen Sie sicher, dass Ihre Elastic Load Balancer (ELBs) mit SSL- oder HTTPS-Listenern konfiguriert sind. Um eventuell vorhanden e sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.1.13	Setzen Sie kryptografische Mechanismen ein, um die Vertraulichkeit von Fernzugriffssitzungen zu schützen.	alb-http-to-https-Umleitungsprüfung	Um Daten während der Übertragung zu schützen, stellen Sie sicher, dass Ihr Application Load Balancer unverschlüsselte HTTP-Anfragen automatisch an HTTPS umleitet. Da sensible Daten vorhanden sein können, sollten Sie die Verschlüsselung bei der Übertragung aktivieren, um diese Daten zu schützen.
3.1.13	Setzen Sie kryptografische Mechanismen ein, um die Vertraulichkeit von Fernzugriffssitzungen zu schützen.	api-gw-ssl-enabled	Stellen Sie sicher, dass die REST-API-Stufen von Amazon API Gateway mit SSL-Zertifikaten konfiguriert sind, damit Backend-Systeme überprüfen können, ob Anforderungen von API Gateway stammen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.1.13	Setzen Sie kryptografische Mechanismen ein, um die Vertraulichkeit von Fernzugriffssitzungen zu schützen.	elb-acm-certificate-required	Zum Schutz von eventuell vorhanden en sensiblen Daten sowie von Daten während der Übertragung muss die Verschlüsselung für Ihr Elastic Load Balancing aktiviert sein. Verwenden Sie AWS Certificate Manager, um öffentliche und private SSL/TLS-Zertifikate mit AWS Diensten und internen Ressourcen zu verwalten, bereitzustellen und bereitzustellen.
3.1.13	Setzen Sie kryptografische Mechanismen ein, um die Vertraulichkeit von Fernzugriffssitzungen zu schützen.	opensearch-https-required	Da sensible Daten existieren können und um Daten während der Übertragung zu schützen, sollten Sie sicherstellen, dass HTTPS für Verbindungen zu Ihren Amazon OpenSearch Service-Domains aktiviert ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.1.13	Setzen Sie kryptografische Mechanismen ein, um die Vertraulichkeit von Fernzugriffssitzungen zu schützen.	redshift-require-tls-ssl	Stellen Sie sicher, dass Ihre Amazon-Redshift-Cluster eine TLS/SSL-Verschlüsselung erfordern, um eine Verbindung zu SQL-Clients herzustellen. Da sensible Daten vorhanden sein können, sollten Sie die Verschlüsselung bei der Übertragung aktivieren, um diese Daten zu schützen.
3.1.13	Setzen Sie kryptografische Mechanismen ein, um die Vertraulichkeit von Fernzugriffssitzungen zu schützen.	s-3 bucket-ssl-requests-only	Um Daten während der Übertragung zu schützen, stellen Sie sicher, dass Ihre Amazon Simple Storage Service (Amazon S3)-Buckets Anfragen zur Verwendung von Secure Socket Layer (SSL)-Buckets erfordern. Da sensible Daten vorhanden sein können, sollten Sie die Verschlüsselung bei der Übertragung aktivieren, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.1.14	Leitet den Fernzugriff von verwalteten Zugangskontrollpunkten aus weiter.	autoscaling-launch-config-public-ip-deaktiviert	Wenn Sie Ihre Netzwerkschnittstellen mit einer öffentlichen IP-Adresse konfigurieren, sind die diesen Netzwerkschnittstellen zugehörigen Ressourcen über das Internet erreichbar. EC2 Ressourcen sollten nicht öffentlich zugänglich sein, da dies einen unbeabsichtigten Zugriff auf Ihre Anwendungen oder Server ermöglichen kann.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.1.14	Leitet den Fernzugriff von verwalteten Zugangskontrollpunkten aus weiter.	ec-2 instances-in-vpc	Stellen Sie Amazon Elastic Compute Cloud (Amazon EC2) -Instances innerhalb einer Amazon Virtual Private Cloud (Amazon VPC) bereit, um eine sichere Kommunikation zwischen einer Instance und anderen Services innerhalb der Amazon VPC zu ermöglichen, ohne dass ein Internet-Gateway, ein NAT-Gerät oder eine VPN-Verbindung erforderlich ist. Der gesamte Datenverkehr bleibt sicher in der AWS Cloud. Domains, die sich innerhalb einer VPC befinden, verfügen aufgrund ihrer logischen Isolierung im Vergleich zu Domains mit öffentlichen Endpunkten über eine zusätzliche Sicherheitsebene. Weisen Sie EC2

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			Amazon-Instances einer Amazon-VPC zu, um den Zugriff ordnungsgemäß zu verwalten.
3.1.14	Leitet den Fernzugriff von verwalteten Zugangskontrollpunkten aus weiter.	no-unrestricted-route-to-igw	Stellen Sie sicher, dass EC2 Amazon-Routentabellen keine uneingeschränkten Routen zu einem Internet-Gateway enthalten. Durch das Entfernen oder Beschränken des Internetzugangs für Workloads innerhalb von Amazon VPCs können unbeabsichtigte Zugriffe in Ihrer Umgebung reduziert werden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.1.14	Leitet den Fernzugriff von verwalteten Zugangskontrollpunkten aus weiter.	ssm-document-not-public	Stellen Sie sicher, dass AWS Systems Manager (SSM) - Dokumente nicht öffentlich sind, da dies einen unbeabsichtigten Zugriff auf Ihre SSM-Dokumente ermöglichen kann. Ein öffentliches SSM-Dokument kann Informationen über Ihr Konto, Ihre Ressourcen und internen Prozesse preisgeben.
3.1.14	Leitet den Fernzugriff von verwalteten Zugangskontrollpunkten aus weiter.	dms-replication-not-public	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass auf DMS-Replikationsinstanzen nicht öffentlich zugegriffen werden kann. DMS-Replikations-Instances können vertrauliche Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.1.14	Leitet den Fernzugriff von verwalteten Zugangskontrollpunkten aus weiter.	ebs-snapshot-public-restorable-überprüfen	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass EBS-Snapshots nicht öffentlich wiederherstellbar sind. EBS-Volume-Snapshots können vertrauliche Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.
3.1.14	Leitet den Fernzugriff von verwalteten Zugangskontrollpunkten aus weiter.	ec-2 instance-no-public-ip	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon Elastic Compute Cloud (Amazon EC2) - Instances nicht öffentlich zugänglich sind. EC2 Amazon-Instances können vertrauliche Informationen enthalten, und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.1.14	Leitet den Fernzugriff von verwalteten Zugangskontrollpunkten aus weiter.	elasticsearch-in-vpc-only	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass sich Amazon OpenSearch OpenSearch Service (Service) - Domains innerhalb einer Amazon Virtual Private Cloud (Amazon VPC) befinden. Eine OpenSearch Service-Domain innerhalb einer Amazon VPC ermöglicht die sichere Kommunikation zwischen OpenSearch Service und anderen Services innerhalb der Amazon VPC, ohne dass ein Internet-Gateway, ein NAT-Gerät oder eine VPN-Verbindung erforderlich ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.1.14	Leitet den Fernzugriff von verwalteten Zugangskontrollpunkten aus weiter.	emr-master-no-public-ip	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon EMR-Cluster-Masterknoten nicht öffentlich zugänglich sind. Amazon-EMR-Cluster-Hauptknoten können vertrauliche Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.1.14	Leitet den Fernzugriff von verwalteten Zugangskontrollpunkten aus weiter.	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) Security Groups können bei der Verwaltung des Netzwerkzugriffs helfen, indem sie eine statusbehaftete Filterung von eingehendem und ausgehendem Netzwerkverkehr zu Ressourcen bereitstellen. AWS Wenn Sie eingehenden (oder entfernten) Datenverkehr von 0.0.0.0/0 bis Port 22 auf Ihren Ressourcen nicht zulassen, können Sie den Remote-Zugriff einschränken.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.1.14	Leitet den Fernzugriff von verwalteten Zugangskontrollpunkten aus weiter.	internet-gateway-authorized-vpc-nur	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Internet-Gateways nur mit autorisierter Amazon Virtual Private Cloud (Amazon VPC) verbunden sind. Internet-Gateways ermöglichen den bidirektionalen Internetzugang zur und von der Amazon VPC, was möglicherweise zu einem unbefugten Zugriff auf Amazon-VPC-Ressourcen führen kann.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.1.14	Leitet den Fernzugriff von verwalteten Zugangskontrollpunkten aus weiter.	lambda-function-public-access-verboten	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass AWS Lambda-Funktionen nicht öffentlich zugänglich sind. Der öffentliche Zugriff kann möglicherweise die Verfügbarkeit von Ressourcen beeinträchtigen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.1.14	Leitet den Fernzugriff von verwalteten Zugangskontrollpunkten aus weiter.	lambda-inside-vpc	Stellen Sie AWS Lambda-Funktionen in einer Amazon Virtual Private Cloud (Amazon VPC) bereit, um eine sichere Kommunikation zwischen einer Funktion und anderen Diensten innerhalb der Amazon VPC zu gewährleisten. Bei dieser Konfiguration sind kein Internet-Gateway, kein NAT-Gerät und keine VPN-Verbindung erforderlich. Der gesamte Datenverkehr bleibt sicher in der Cloud. AWS Domains, die sich innerhalb einer VPC befinden, verfügen aufgrund ihrer logischen Isolierung im Vergleich zu Domains mit öffentlichen Endpunkten über eine zusätzliche Sicherheitsebene. Um den Zugriff ordnungsgemäß zu verwalten,

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			sollten AWS Lambda-Funktionen einer VPC zugewiesen werden.
3.1.14	Leitet den Fernzugriff von verwalteten Zugangskontrollpunkten aus weiter.	mfa-enabled-for-iam-Konsolenzugriff	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass MFA für alle AWS Identity and Access Management (IAM) -Benutzer aktiviert ist, die über ein Konsolenkennwort verfügen. MFA sorgt für eine weitere Schutzebene zusätzlich zu den Anmeldeinformationen. Indem Sie MFA für Benutzer vorschreiben, können Sie Fälle kompromittierter Konten reduzieren und verhindern, dass unbefugte Benutzer auf vertrauliche Daten zugreifen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.1.14	Leitet den Fernzugriff von verwalteten Zugangskontrollpunkten aus weiter.	opensearch-access-control-enabled	Stellen Sie sicher, dass eine differenzierte Zugriffskontrolle für Ihre Amazon OpenSearch Service-Domains aktiviert ist. Eine differenzierte Zugriffskontrolle bietet erweiterte Autorisierungsmechanismen, um den Zugriff auf Amazon Service-Domains mit den geringsten Rechten zu erreichen. OpenSearch Es ermöglicht eine rollenbasierte Zugriffskontrolle auf die Domain sowie Sicherheit auf Index-, Dokument- und Feldebene, Unterstützung für OpenSearch Service-Dashboards, Mehrmandantenfähigkeit und HTTP-Basisauthentifizierung für Service und Kibana. OpenSearch

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.1.14	Leitet den Fernzugriff von verwalteten Zugangskontrollpunkten aus weiter.	opensearch-in-vpc-only	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass sich Amazon OpenSearch Service-Domains innerhalb einer Amazon Virtual Private Cloud (Amazon VPC) befinden. Eine Amazon OpenSearch Service-Domain innerhalb einer Amazon VPC ermöglicht die sichere Kommunikation zwischen Amazon OpenSearch Service und anderen Services innerhalb der Amazon VPC, ohne dass ein Internet-Gateway, ein NAT-Gerät oder eine VPN-Verbindung erforderlich ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.1.14	Leitet den Fernzugriff von verwalteten Zugangskontrollpunkten aus weiter.	rds-instance-public-access-überprüfen	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Relational Database Service (Amazon RDS) -Instances nicht öffentlich sind. Amazon-RDS-Datenbank-Instances können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.1.14	Leitet den Fernzugriff von verwalteten Zugangskontrollpunkten aus weiter.	rds-snapshots-public-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Relational Database Service (Amazon RDS) -Instances nicht öffentlich sind. Amazon-RDS-Datenbank-Instances können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.1.14	Leitet den Fernzugriff von verwalteten Zugangskontrollpunkten aus weiter.	redshift-cluster-public-access-überprüfen	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Redshift Redshift-Cluster nicht öffentlich sind. Amazon-Redshift-Cluster können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.1.14	Leitet den Fernzugriff von verwalteten Zugangskontrollpunkten aus weiter.	restricted-common-ports	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass gemeinsame Ports für Amazon Elastic Compute Cloud (Amazon EC2) -Sicherheitsgruppen eingeschränkt sind. Wenn der Zugriff auf Ports nicht auf vertrauenswürdige Quellen beschränkt wird, kann dies zu Angriffen auf die Verfügbarkeit, Integrität und Vertraulichkeit von Systemen führen. Mit dieser Regel können Sie optional die Parameter blockedPort1–blockedPort5 festlegen (Standardkonfigurationen: 20, 21, 3389, 3306, 4333). Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.1.14	Leitet den Fernzugriff von verwalteten Zugangskontrollpunkten aus weiter.	s3- account-level-public-access -blöcke-periodisch	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Simple Storage Service (Amazon S3) -Buckets nicht öffentlich zugänglich sind. Diese Regel trägt dazu bei, sensible Daten vor unbefugten Remote-Benutzern zu schützen, indem sie den öffentlichen Zugriff verhindert. Mit dieser Regel können Sie optional die Parameter ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) und restrictPublicBuckets Parameter (Config Default: True) festlegen. Die tatsächlichen Werte müssen den Richtlini

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			en Ihrer Organisation entsprechen.
3.1.14	Leitet den Fernzugriff von verwalteten Zugangskontrollpunkten aus weiter.	s3 bucket-level-public-access - verboten	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Simple Storage Service (Amazon S3) -Buckets nicht öffentlich zugänglich sind. Diese Regel trägt dazu bei, sensible Daten vor unbefugten Remote-Benutzern zu schützen, indem sie den öffentlichen Zugriff auf Bucket-Ebene verhindert.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.1.14	Leitet den Fernzugriff von verwalteten Zugangskontrollpunkten aus weiter.	sagemaker-notebook-no-direct-Internetzugang	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass SageMaker Amazon-Notebooks keinen direkten Internetzugang zulassen. Indem Sie direkten Internetzugang blockieren, vermeiden Sie, dass unbefugte Benutzer auf sensible Daten zugreifen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.1.14	Leitet den Fernzugriff von verwalteten Zugangskontrollpunkten aus weiter.	subnet-auto-assign-public-ip-deaktiviert	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon Virtual Private Cloud (VPC) -Subnetzen nicht automatisch eine öffentliche IP-Adresse zugewiesen wird. Amazon Elastic Compute Cloud (EC2) -Instances, die in Subnetzen gestartet werden, in denen dieses Attribut aktiviert ist, haben ihrer primären Netzwerkschnittstelle eine öffentliche IP-Adresse zugewiesen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.1.14	Leitet den Fernzugriff von verwalteten Zugangskontrollpunkten aus weiter.	vpc-default-security-group-geschlossen	Sicherheitsgruppen von Amazon Elastic Compute Cloud (Amazon EC2) können bei der Verwaltung des Netzwerkzugriffs helfen, indem sie eine statusbehaftete Filterung des ein- und ausgehenden Netzwerkverkehrs zu Ressourcen bereitstellen. AWS Die Beschränkung des gesamten Datenverkehrs auf die Standardsicherheitsgruppe hilft dabei, den Fernzugriff auf Ihre Ressourcen einzuschränken. AWS

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.1.14	Leitet den Fernzugriff von verwalteten Zugangskontrollpunkten aus weiter.	vpc-sg-open-only-to-authorized-ports	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass gemeinsame Ports für Amazon Elastic Compute Cloud (Amazon EC2) -Sicherheitsgruppen eingeschränkt sind. Wenn der Zugriff auf Ports nicht auf vertrauenswürdige Quellen beschränkt wird, kann dies zu Angriffen auf die Verfügbarkeit, Integrität und Vertraulichkeit von Systemen führen. Durch die Beschränkung des Zugriffs auf Ressourcen innerhalb einer Sicherheitsgruppe aus dem Internet (0.0.0.0/0) kann der Fernzugriff auf interne Systeme gesteuert werden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.1.20	Überprüfen und kontrollieren/beschränken Sie die Verbindungen zu externen Systemen und deren Nutzung.	no-unrestricted-route-to-igw	Stellen Sie sicher, dass EC2 Amazon-Routentabellen keine uneingeschränkten Routen zu einem Internet-Gateway enthalten. Durch das Entfernen oder Beschränken des Internetzugangs für Workloads innerhalb von Amazon VPCs können unbeabsichtigte Zugriffe in Ihrer Umgebung reduziert werden.
3.1.20	Überprüfen und kontrollieren/beschränken Sie die Verbindungen zu externen Systemen und deren Nutzung.	ssm-document-not-public	Stellen Sie sicher, dass AWS Systems Manager (SSM) - Dokumente nicht öffentlich sind, da dies einen unbeabsichtigten Zugriff auf Ihre SSM-Dokumente ermöglichen kann. Ein öffentliches SSM-Dokument kann Informationen über Ihr Konto, Ihre Ressourcen und internen Prozesse preisgeben.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.1.20	Überprüfen und kontrollieren/beschränken Sie die Verbindungen zu externen Systemen und deren Nutzung.	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) Security Groups können bei der Verwaltung des Netzwerkzugriffs helfen, indem sie eine statusbehaftete Filterung von eingehendem und ausgehendem Netzwerkverkehr zu Ressourcen bereitstellen. AWS Wenn Sie eingehenden (oder entfernten) Datenverkehr von 0.0.0.0/0 bis Port 22 auf Ihren Ressourcen nicht zulassen, können Sie den Remote-Zugriff einschränken.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.1.20	Überprüfen und kontrollieren/beschränken Sie die Verbindungen zu externen Systemen und deren Nutzung.	internet-gateway-authorized-vpc-nur	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Internet-Gateways nur mit autorisierter Amazon Virtual Private Cloud (Amazon VPC) verbunden sind. Internet-Gateways ermöglichen den bidirektionalen Internetzugang zur und von der Amazon VPC, was möglicher weise zu einem unbefugten Zugriff auf Amazon-VPC-Ressourcen führen kann.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.1.20	Überprüfen und kontrollieren/beschränken Sie die Verbindungen zu externen Systemen und deren Nutzung.	opensearch-access-control-enabled	Stellen Sie sicher, dass eine differenzierte Zugriffskontrolle für Ihre Amazon OpenSearch Service-Domains aktiviert ist. Eine differenzierte Zugriffskontrolle bietet erweiterte Autorisierungsmechanismen, um den Zugriff auf Amazon Service-Domains mit den geringsten Rechten zu erreichen. OpenSearch Es ermöglicht eine rollenbasierte Zugriffskontrolle auf die Domain sowie Sicherheit auf Index-, Dokument- und Feldebene, Unterstützung für OpenSearch Service-Dashboards, Mehrmandantenfähigkeit und HTTP-Basisauthentifizierung für Service und Kibana. OpenSearch

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.1.20	Überprüfen und kontrollieren/beschränken Sie die Verbindungen zu externen Systemen und deren Nutzung.	restricted-common-ports	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass gemeinsame Ports für Amazon Elastic Compute Cloud (Amazon EC2) -Sicherheitsgruppen eingeschränkt sind. Wenn der Zugriff auf Ports nicht auf vertrauenswürdige Quellen beschränkt wird, kann dies zu Angriffen auf die Verfügbarkeit, Integrität und Vertraulichkeit von Systemen führen. Mit dieser Regel können Sie optional die Parameter blockedPort1–blockedPort5 festlegen (Standardkonfigurationen: 20, 21, 3389, 3306, 4333). Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.1.20	Überprüfen und kontrollieren/beschränken Sie die Verbindungen zu externen Systemen und deren Nutzung.	s3-Blöcke-periodisch account-level-public-access	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Simple Storage Service (Amazon S3) -Buckets nicht öffentlich zugänglich sind. Diese Regel trägt dazu bei, sensible Daten vor unbefugten Remote-Benutzern zu schützen, indem sie den öffentlichen Zugriff verhindert. Mit dieser Regel können Sie optional die Parameter ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) und restrictPublicBuckets Parameter (Config Default: True) festlegen. Die tatsächlichen Werte müssen den Richtlini

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			en Ihrer Organisation entsprechen.
3.1.20	Überprüfen und kontrollieren/beschränken Sie die Verbindungen zu externen Systemen und deren Nutzung.	s3- verboten bucket-level-public-access	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Simple Storage Service (Amazon S3) -Buckets nicht öffentlich zugänglich sind. Diese Regel trägt dazu bei, sensible Daten vor unbefugten Remote-Benutzern zu schützen, indem sie den öffentlichen Zugriff auf Bucket-Ebene verhindert.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.1.20	Überprüfen und kontrollieren/beschränken Sie die Verbindungen zu externen Systemen und deren Nutzung.	s-3 bucket-policy-grantee-check	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie s3_bucket_policy_grantee_check aktivieren. Diese Regel prüft, ob der vom Amazon S3 S3-Bucket gewährte Zugriff durch die von Ihnen bereitgestellten AWS Principals, Verbundbenutzer, Service Principals, IP-Adressen oder Amazon Virtual Private Cloud (Amazon VPC) IDs eingeschränkt ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.1.20	Überprüfen und kontrollieren/beschränken Sie die Verbindungen zu externen Systemen und deren Nutzung.	vpc-default-security-group-geschlossen	Sicherheitsgruppen von Amazon Elastic Compute Cloud (Amazon EC2) können bei der Verwaltung des Netzwerkzugriffs helfen, indem sie eine statusbehaftete Filterung des ein- und ausgehenden Netzwerkverkehrs zu Ressourcen bereitstellen. AWS Die Beschränkung des gesamten Datenverkehrs auf die Standardsicherheitsgruppe hilft dabei, den Fernzugriff auf Ihre Ressourcen einzuschränken. AWS

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.1.20	Überprüfen und kontrollieren/beschränken Sie die Verbindungen zu externen Systemen und deren Nutzung.	vpc-sg-open-only-to-authorized-ports	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass gemeinsame Ports für Amazon Elastic Compute Cloud (Amazon EC2) -Sicherheitsgruppen eingeschränkt sind. Wenn der Zugriff auf Ports nicht auf vertrauenswürdige Quellen beschränkt wird, kann dies zu Angriffen auf die Verfügbarkeit, Integrität und Vertraulichkeit von Systemen führen. Durch die Beschränkung des Zugriffs auf Ressourcen innerhalb einer Sicherheitsgruppe aus dem Internet (0.0.0.0/0) kann der Fernzugriff auf interne Systeme gesteuert werden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.3.1	Erstellung und Aufbewahrung von Systemprüfungsprotokollen in dem Umfang, der für die Überwachung, Analyse, Untersuchung und Berichterstattung über unrechtmäßige, unbefugte oder unangemessene Systemaktivitäten erforderlich ist.	cw-loggroup-retention-period-überprüfen	Stellen Sie sicher, dass die Ereignisprotokolldaten für Ihre Protokollgruppen über eine Mindestdauer aufbewahrt werden, um die Fehlerbehebung und forensische Untersuchungen zu unterstützen. Fehlende frühere Ereignisprotokolldaten erschweren die Rekonstruierung und Identifizierung potenziell schädlicher Ereignisse.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.3.1	Erstellung und Aufbewahrung von Systemprüfungsprotokollen in dem Umfang, der für die Überwachung, Analyse, Untersuchung und Berichterstattung über unrechtmäßige, unbefugte oder unangemessene Systemaktivitäten erforderlich ist.	elasticsearch-logs-to-cloudwatch	Stellen Sie sicher, dass für Amazon OpenSearch Service-Domains Fehlerprotokolle aktiviert und zur Aufbewahrung und Beantwortung an Amazon CloudWatch Logs gestreamt werden. Domain-Fehlerprotokolle sind bei Sicherheits- und Zugriffsprüfungen sowie bei der Diagnose von Verfügbarkeitsproblemen nützlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.3.1	Erstellung und Aufbewahrung von Systemprüfungsprotokollen in dem Umfang, der für die Überwachung, Analyse, Untersuchung und Berichterstattung über unrechtmäßige, unbefugte oder unangemessene Systemaktivitäten erforderlich ist.	multi-region-cloudtrail-enabled	AWS CloudTrail zeichnet Aktionen und API-Aufrufe der AWS Management Console auf. Sie können feststellen, welche Benutzer und Konten angerufen wurden AWS, von welcher Quell-IP-Adresse aus die Anrufe getätigt wurden und wann die Anrufe erfolgten. CloudTrail übermittelt Protokolldateien aus allen AWS Regionen an Ihren S3-Bucket , wenn MULTI_REGION_CLOUD_TRAIL_ENABLED aktiviert ist. Außerdem wird beim AWS Start einer neuen Region derselbe Trail in der neuen Region erstellt. CloudTrail Dadurch erhalten Sie automatisch Protokolldateien mit API-Aktivitäten für die neue Region.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.3.1	Erstellung und Aufbewahrung von Systemprüfungsprotokollen in dem Umfang, der für die Überwachung, Analyse, Untersuchung und Berichterstattung über unrechtmäßige, unbefugte oder unangemessene Systemaktivitäten erforderlich ist.	rds-logging-enabled	Um die Protokollierung und Überwachung in Ihrer Umgebung zu erleichtern, stellen Sie sicher, dass die Amazon Relational Database Service (Amazon RDS)-Protokollierung aktiviert ist. Mit der Amazon-RDS-Protokollierung können Sie Ereignisse wie Verbindungen, Verbindungsabbrüche, Abfragen oder abgefragte Tabellen erfassen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.3.1	Erstellung und Aufbewahrung von Systemprüfungsprotokollen in dem Umfang, der für die Überwachung, Analyse, Untersuchung und Berichterstattung über unrechtmäßige, unbefugte oder unangemessene Systemaktivitäten erforderlich ist.	s-3 bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) unterstützt die Aufrechterhaltung einer angemessenen Kapazität und Verfügbarkeit. CRR ermöglicht das automatische, asynchrone Kopieren von Objekten in Amazon S3 Buckets, um die Datenverfügbarkeit sicherzustellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.3.1	Erstellung und Aufbewahrung von Systemprüfungsprotokollen in dem Umfang, der für die Überwachung, Analyse, Untersuchung und Berichterstattung über unrechtmäßige, unbefugte oder unangemessene Systemaktivitäten erforderlich ist.	securityhub-enabled	AWS Security Hub hilft bei der Überwachung von unbefugtem Personal, Verbindungen, Geräten und Software. AWS Security Hub aggregiert, organisiert und priorisiert die Sicherheitswarnungen oder Ergebnisse mehrerer Dienste. AWS Einige dieser Dienste sind Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer und AWS Firewall Manager sowie AWS Partnerlösungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.3.1	Erstellung und Aufbewahrung von Systemprüfungsprotokollen in dem Umfang, der für die Überwachung, Analyse, Untersuchung und Berichterstattung über unrechtmäßige, unbefugte oder unangemessene Systemaktivitäten erforderlich ist.	wafv2-logging-enabled	Um Ihnen bei der Protokollierung und Überwachung in Ihrer Umgebung zu helfen, aktivieren Sie die AWS WAF (V2) -Protokollierung im regionalen und globalen Web. ACLs AWS Die WAF-Protokollierung bietet detaillierte Informationen über den Datenverkehr, der von Ihrer Web-ACL analysiert wird. In den Protokollen werden die Uhrzeit aufgezeichnet, zu der die AWS WAF die Anfrage von Ihrer AWS Ressource erhalten hat, Informationen über die Anfrage und eine Aktion für die Regel, der jede Anfrage entsprach.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.3.1	Erstellung und Aufbewahrung von Systemprüfungsprotokollen in dem Umfang, der für die Überwachung, Analyse, Untersuchung und Berichterstattung über unrechtmäßige, unbefugte oder unangemessene Systemaktivitäten erforderlich ist.	api-gw-execution-logging-aktiviert	Die API-Gateway-Protokollierung zeigt detaillierte Ansichten der Benutzer, die auf die API zugegriffen haben, und wie diese Benutzer auf die API zugegriffen haben. Diese Insights ermöglichen die Einsicht in Benutzeraktivitäten.
3.3.1	Erstellung und Aufbewahrung von Systemprüfungsprotokollen in dem Umfang, der für die Überwachung, Analyse, Untersuchung und Berichterstattung über unrechtmäßige, unbefugte oder unangemessene Systemaktivitäten erforderlich ist.	cloud-trail-cloud-watch-logs-aktiviert	Verwenden Sie Amazon CloudWatch , um Protokoll ereignisaktivitäten zentral zu sammeln und zu verwalten. Die Aufnahme von AWS CloudTrail Daten liefert Einzelheiten zu den API-Aufrufaktivitäten in Ihrem AWS-Konto.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.3.1	Erstellung und Aufbewahrung von Systemprüfungsprotokollen in dem Umfang, der für die Überwachung, Analyse, Untersuchung und Berichterstattung über unrechtmäßige, unbefugte oder unangemessene Systemaktivitäten erforderlich ist.	cloudtrail-enabled	AWS CloudTrail kann bei der Nichtabstreitbarkeit helfen, indem Aktionen und API-Aufrufe der AWS Management Console aufgezeichnet werden. Sie können die Benutzer und die Benutzer AWS-Konten , die einen AWS Dienst aufgerufen haben, die Quell-IP-Adresse, über die die Aufrufe generiert wurden, und den Zeitpunkt der Anrufe identifizieren. Einzelheiten zu den erfassten Daten finden Sie in den AWS CloudTrail Datensatzinhalten.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.3.1	Erstellung und Aufbewahrung von Systemprüfungsprotokollen in dem Umfang, der für die Überwachung, Analyse, Untersuchung und Berichterstattung über unrechtmäßige, unbefugte oder unangemessene Systemaktivitäten erforderlich ist.	cloudtrail-s3-dataevents-enabled	Die Erfassung von Simple Storage Service (Amazon S3)-Datenereignissen unterstützt die Erkennung von ungewöhnlichen Aktivitäten. Zu den Details gehören AWS-Konto Informationen über den Zugriff auf einen Amazon S3 S3-Bucket, die IP-Adresse und die Uhrzeit des Ereignisses.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.3.1	Erstellung und Aufbewahrung von Systemprüfungsprotokollen in dem Umfang, der für die Überwachung, Analyse, Untersuchung und Berichterstattung über unrechtmäßige, unbefugte oder unangemessene Systemaktivitäten erforderlich ist.	elb-logging-enabled	Die Elastic-Load-Balancing-Aktivität ist ein zentraler Kommunikationspunkt innerhalb einer Umgebung. Stellen Sie sicher, dass die ELB-Protokollierung aktiviert ist. Die gesammelten Daten enthalten detaillierte Informationen zu Anfragen, die an den ELB gesendet wurden. Jedes Protokoll enthält Informationen wie die Zeit, zu der die Anforderung einging, die Client-IP-Adresse, Latenzen, Anforderungspfade und Serverantworten.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.3.1	Erstellung und Aufbewahrung von Systemprüfungsprotokollen in dem Umfang, der für die Überwachung, Analyse, Untersuchung und Berichterstattung über unrechtmäßige, unbefugte oder unangemessene Systemaktivitäten erforderlich ist.	guardduty-enabled-centralized	Amazon GuardDuty kann mithilfe von Threat Intelligence Feeds helfen, potenzielle Cybersicherheitsereignisse zu überwachen und zu erkennen. Dazu gehören Listen mit bösartigen IPs und maschinellen Lernmethoden zur Identifizierung unerwarteter, nicht autorisierter und bösartiger Aktivitäten in Ihrer AWS Cloud-Umgebung.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.3.1	Erstellung und Aufbewahrung von Systemprüfungsprotokollen in dem Umfang, der für die Überwachung, Analyse, Untersuchung und Berichterstattung über unrechtmäßige, unbefugte oder unangemessene Systemaktivitäten erforderlich ist.	opensearch-logs-to-cloudwatch	Stellen Sie sicher, dass für Amazon OpenSearch Service-Domains Fehlerprotokolle aktiviert und zur Aufbewahrung und Beantwortung an Amazon CloudWatch Logs gestreamt werden. OpenSearch Service-Fehlerprotokolle können bei Sicherheits- und Zugriffsprüfungen helfen und bei der Diagnose von Verfügbarkeitsproblemen helfen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.3.1	Erstellung und Aufbewahrung von Systemprüfungsprotokollen in dem Umfang, der für die Überwachung, Analyse, Untersuchung und Berichterstattung über unrechtmäßige, unbefugte oder unangemessene Systemaktivitäten erforderlich ist.	redshift-cluster-configuration-check	Um Daten im Ruhezustand zu schützen, muss die Verschlüsselung für Ihre Amazon-Redshift-Cluster aktiviert sein. Sie müssen auch sicherstellen, dass die erforderlichen Konfigurationen auf Amazon-Redshift-Clustern bereitgestellt werden. Die Prüfungsprotokollierung muss aktiviert sein, um Informationen zu Verbindungen und Benutzeraktivitäten in der Datenbank bereitzustellen. Diese Regel erfordert, dass ein Wert für clusterDbEncrypted (Config Default: TRUE) und LoggingEnabled (Config Default: TRUE) gesetzt ist. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.3.1	Erstellung und Aufbewahrung von Systemprüfungsprotokollen in dem Umfang, der für die Überwachung, Analyse, Untersuchung und Berichterstattung über unrechtmäßige, unbefugte oder unangemessene Systemaktivitäten erforderlich ist.	s3- bucket-logging-enabled	Die Amazon Simple Storage Service (Amazon S3)-Serverzugriffsprotokollierung bietet eine Methode zur Überwachung des Netzwerks im Hinblick auf potenzielle Cybersicherheitsereignisse. Die Ereignisse werden überwacht, indem detaillierte Aufzeichnungen über die Anfragen erfasst werden, die an einen Amazon-S3-Bucket gestellt wurden. Jeder Zugriffsprotokolleintrag enthält Details zu einer einzelnen Zugriffsanfrage. Zu den Details gehören Anforderer, Bucket-Name, Anforderungszeit, Anforderungsaktion, Antwortstatus und Fehlercode, falls relevant.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.3.1	Erstellung und Aufbewahrung von Systemprüfungsprotokollen in dem Umfang, der für die Überwachung, Analyse, Untersuchung und Berichterstattung über unrechtmäßige, unbefugte oder unangemessene Systemaktivitäten erforderlich ist.	vpc-flow-logs-enabled	VPC-Flow-Protokolle erfassen detaillierte Informationsdatensätze über den IP-Datenverkehr, der zu und von Netzwerkschnittstellen in Ihrer Amazon Virtual Private Cloud (Amazon VPC) fließt. Standardmäßig enthalten Flow-Protokolldatensätze Werte für die verschiedenen Komponenten des IP-Flows, einschließlich Quelle, Ziel und Protokoll.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.3.2	Stellen Sie sicher, dass die Aktionen einzelner Systemben utzer eindeutig auf diese Benutzer zurückgeführt werden können, sodass sie für ihre Aktionen zur Rechenschaft gezogen werden können.	multi-region-cloudtrail-enabled	AWS CloudTrail zeichnet Aktionen und API-Aufrufe der AWS Management Console auf. Sie können feststellen, welche Benutzer und Konten angerufen wurden AWS, von welcher Quell-IP-Adresse aus die Anrufe getätigt wurden und wann die Anrufe erfolgten. CloudTrail übermittelt Protokolldateien aus allen AWS Regionen an Ihren S3-Bucket , wenn MULTI_REG ION_CLOUD _TRAIL_ENABLED aktiviert ist. Außerdem wird beim AWS Start einer neuen Region derselbe Trail in der neuen Region erstellt. CloudTrail Dadurch erhalten Sie automatis ch Protokolldateien mit API-Aktivitäten für die neue Region.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.3.2	Stellen Sie sicher, dass die Aktionen einzelner Systemben utzer eindeutig auf diese Benutzer zurückgeführt werden können, sodass sie für ihre Aktionen zur Rechenschaft gezogen werden können.	rds-logging-enabled	Um die Protokoll ierung und Überwachung in Ihrer Umgebung zu erleichtern, stellen Sie sicher, dass die Amazon Relationa l Database Service (Amazon RDS)-Prot okollierung aktiviert ist. Mit der Amazon-RDS-Protokollierung können Sie Ereigniss e wie Verbindungen, Verbindungsabbrüch e, Abfragen oder abgefragte Tabellen erfassen.
3.3.2	Stellen Sie sicher, dass die Aktionen einzelner Systemben utzer eindeutig auf diese Benutzer zurückgeführt werden können, sodass sie für ihre Aktionen zur Rechenschaft gezogen werden können.	api-gw-execution-l ogging-aktiviert	Die API-Gateway-Protokollierung zeigt detaillierte Ansichten der Benutzer, die auf die API zugegriff en haben, und wie diese Benutzer auf die API zugegriffen haben. Diese Insights ermöglichen die Einsicht in Benutzera ktivitäten.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.3.2	Stellen Sie sicher, dass die Aktionen einzelner Systemben utzer eindeutig auf diese Benutzer zurückgeführt werden können, sodass sie für ihre Aktionen zur Rechenschaft gezogen werden können.	cloud-trail-cloud-watch-logs-aktiviert	Verwenden Sie Amazon CloudWatc h , um Protokoll ereignisaktivitäten zentral zu sammeln und zu verwalten. Die Aufnahme von AWS CloudTrail Daten liefert Einzelheiten zu den API-Aufrufaktivitä ten in Ihrem AWS-Konto.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.3.2	Stellen Sie sicher, dass die Aktionen einzelner Systemben utzer eindeutig auf diese Benutzer zurückgeführt werden können, sodass sie für ihre Aktionen zur Rechenschaft gezogen werden können.	cloudtrail-enabled	AWS CloudTrail kann bei der Nichtabst reitbarkeit helfen, indem Aktionen und API-Aufrufe der AWS Management Console aufgezeic hnet werden. Sie können die Benutzer und die Benutzer AWS-Konten , die einen AWS Dienst aufgerufen haben, die Quell-IP-Adresse, über die die Aufrufe generiert wurden, und den Zeitpunkt der Anrufe identifiz ieren. Einzelheiten zu den erfassten Daten finden Sie in den AWS CloudTrail Datensatzinhalten.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.3.2	Stellen Sie sicher, dass die Aktionen einzelner Systemben utzer eindeutig auf diese Benutzer zurückgeführt werden können, sodass sie für ihre Aktionen zur Rechenschaft gezogen werden können.	cloudtrail-s3-data events-enabled	Die Erfassung von Simple Storage Service (Amazon S3)-Datenereigniss en unterstützt die Erkennung von ungewöhnlichen Aktivitäten. Zu den Details gehören AWS-Konto Informationen über den Zugriff auf einen Amazon S3 S3-Bucket, die IP-Adress e und die Uhrzeit des Ereignisses.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.3.2	Stellen Sie sicher, dass die Aktionen einzelner Systemben utzer eindeutig auf diese Benutzer zurückgeführt werden können, sodass sie für ihre Aktionen zur Rechenschaft gezogen werden können.	redshift-cluster-c onfiguration-check	Um Daten im Ruhezustand zu schützen, muss die Verschlüsselung für Ihre Amazon-Re dshift-Cluster aktiviert sein. Sie müssen auch sicherstellen, dass die erforderl ichen Konfigurationen auf Amazon-Redshift-Clustern bereitges tellt werden. Die Prüfungsprotokolli erung muss aktiviert sein, um Informati onen zu Verbindun gen und Benutzera ktivitäten in der Datenbank bereitzus tellen. Diese Regel erfordert, dass ein Wert für clusterDb Encrypted (Config Default: TRUE) und LoggingEnabled (Config Default: TRUE) gesetzt ist. Die tatsächlichen Werte müssen den Richtlini en Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.3.2	Stellen Sie sicher, dass die Aktionen einzelner Systemben utzer eindeutig auf diese Benutzer zurückgeführt werden können, sodass sie für ihre Aktionen zur Rechenschaft gezogen werden können.	s3- bucket-logging-enabled	Die Amazon Simple Storage Service (Amazon S3)-Serverzugriffs protokollierung bietet eine Methode zur Überwachu ng des Netzwerks im Hinblick auf potenzielle Cybersich erheitsereignisse. Die Ereignisse werden überwacht, indem detaillierte Aufzeichn ungen über die Anfragen erfasst werden, die an einen Amazon-S3-Bucket gestellt wurden. Jeder Zugriffsprotokolle intrag enthält Details zu einer einzelnen Zugriffsanfrage. Zu den Details gehören Anforderer, Bucket-Name, Anforderu ngszeit, Anforderu ngsaktion, Antwortst atus und Fehlercode, falls relevant.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.3.4	Warnung im Falle eines fehlgesch lagenen Prüfungsp rozesses.	securityhub-enabled	AWS Security Hub hilft bei der Überwachung von unbefugtem Personal, Verbindun gen, Geräten und Software. AWS Security Hub aggregiert, organisie rt und priorisie rt die Sicherhei tswarnungen oder Ergebnisse mehrerer Dienste. AWS Einige dieser Dienste sind Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer und AWS Firewall Manager sowie AWS Partnerlösungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.3.4	Warnung im Falle eines fehlgesch lagenen Prüfungsp rozesses.	guardduty-enabled-centralized	Amazon GuardDuty kann mithilfe von Threat Intellige nce Feeds helfen, potenzielle Cybersich erheitsereignisse zu überwachen und zu erkennen. Dazu gehören Listen mit bösartigen IPs und maschinel len Lernmethoden zur Identifizierung unerwarteter, nicht autorisierter und bösartiger Aktivitäten in Ihrer AWS Cloud-Umgebung.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.3.5	Korrelieren Sie Prüfungs-, Analyse- und Berichter stattungsprozesse für die Untersuchung und Reaktion auf Hinweise auf unangemes sene, verdächtige oder ungewöhnliche Aktivitäten.	securityhub-enabled	AWS Security Hub hilft bei der Überwachung von unbefugtem Personal, Verbindun gen, Geräten und Software. AWS Security Hub aggregiert, organisie rt und priorisie rt die Sicherhei tswarnungen oder Ergebnisse mehrerer Dienste. AWS Einige dieser Dienste sind Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer und AWS Firewall Manager sowie AWS Partnerlösungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.3.5	Korrelieren Sie Prüfungs-, Analyse- und Berichter stattungsprozesse für die Untersuchung und Reaktion auf Hinweise auf unangemes sene, verdächtige oder ungewöhnliche Aktivitäten.	guardduty-enabled-centralized	Amazon GuardDuty kann mithilfe von Threat Intellige nce Feeds helfen, potenzielle Cybersich erheitsereignisse zu überwachen und zu erkennen. Dazu gehören Listen mit bösartigen IPs und maschinel len Lernmethoden zur Identifizierung unerwarteter, nicht autorisierter und bösartiger Aktivitäten in Ihrer AWS Cloud-Umgebung.
3.3.8	Schützen Sie Prüfungsinformatio nen und Tools zur Prüfung vor unbefugte m Zugriff, Änderung und Löschung.	s-3 bucket-default-loc k-enabled	Stellen Sie sicher, dass für Ihren Amazon Simple Storage Service (Amazon S3)-Bucke t standardmäßig eine Sperre aktiviert ist. Zum Schutz eventuell vorhanden er sensibler Daten in S3 Buckets müssen Sie Objektsperren für Daten im Ruhezusta nd erzwingen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.3.8	Schützen Sie Prüfungsinformationen und Tools zur Prüfung vor unbefugtem Zugriff, Änderung und Löschung.	s-3 bucket-versioning-enabled	Die Versionsverwaltung von Amazon Simple Storage Service (Amazon S3)-Buckets hilft dabei, mehrere Varianten eines Objekts im selben Amazon-S3-Bucket zu speichern. Verwenden Sie die Versionsverwaltung, um sämtliche Versionen aller Objekte in Ihrem Amazon-S3-Bucket zu speichern, abzurufen oder wiederherzustellen. Mit der Versionsverwaltung können Sie Versionen sowohl nach unbeabsichtigten Benutzeraktionen als auch nach Anwendungsfehlern problemlos wiederherstellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.3.8	Schützen Sie Prüfungsinformationen und Tools zur Prüfung vor unbefugtem Zugriff, Änderung und Löschung.	cloud-trail-log-file-Validierung aktiviert	Verwenden Sie die AWS CloudTrail Protokolldateivalidierung, um die Integrität von Protokollen zu überprüfen. CloudTrail Mithilfe der Protokolldateivalidierung kann festgestellt werden, ob eine Protokolldatei geändert oder gelöscht wurde oder ob sie nach der Übermittlung CloudTrail unverändert geblieben ist. Dieses Feature wurde mit dem Branchenstandard entsprechenden Algorithmen entwickelt: SHA-256 für die Hashfunktion und SHA-256 mit RSA für digitale Signaturen. Aus diesem Grund ist es rechnerisch unmöglich, CloudTrail Protokolldateien unbemerkt zu ändern, zu löschen oder zu fälschen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.3.8	Schützen Sie Prüfungsinformationen und Tools zur Prüfung vor unbefugtem Zugriff, Änderung und Löschung.	s3-Blöcke-periodisch account-level-public-access	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Simple Storage Service (Amazon S3) -Buckets nicht öffentlich zugänglich sind. Diese Regel trägt dazu bei, sensible Daten vor unbefugten Remote-Benutzern zu schützen, indem sie den öffentlichen Zugriff verhindert. Mit dieser Regel können Sie optional die Parameter ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) und restrictPublicBuckets Parameter (Config Default: True) festlegen. Die tatsächlichen Werte müssen den Richtlini

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			en Ihrer Organisation entsprechen.
3.3.8	Schützen Sie Prüfungsinformationen und Tools zur Prüfung vor unbefugtem Zugriff, Änderung und Löschung.	s-3 bucket-policy-grantee-check	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie s3_bucket_policy_grantee_check aktivieren. Diese Regel prüft, ob der vom Amazon S3 S3-Bucket gewährte Zugriff durch die von Ihnen bereitgestellten AWS Principals, Verbundbenutzer, Service Principals, IP-Adressen oder Amazon Virtual Private Cloud (Amazon VPC) IDs eingeschränkt ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.3.8	Schützen Sie Prüfungsinformationen und Tools zur Prüfung vor unbefugtem Zugriff, Änderung und Löschung.	s-3 bucket-public-read-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie nur autorisierten Benutzern, Prozessen und Geräten Zugriff auf Amazon Simple Storage Service (Amazon S3) - Buckets gewähren. Die Verwaltung des Zugriffs sollte mit der Klassifizierung der Daten übereinstimmen.
3.3.8	Schützen Sie Prüfungsinformationen und Tools zur Prüfung vor unbefugtem Zugriff, Änderung und Löschung.	s-3 bucket-public-write-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie nur autorisierten Benutzern, Prozessen und Geräten Zugriff auf Amazon Simple Storage Service (Amazon S3) - Buckets gewähren. Die Verwaltung des Zugriffs sollte mit der Klassifizierung der Daten übereinstimmen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.3.8	Schützen Sie Prüfungsinformationen und Tools zur Prüfung vor unbefugtem Zugriff, Änderung und Löschung.	s3-fähig bucket-server-side-encryption	Zum Schutz von Daten im Ruhezustand müssen Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon Simple Storage Service (Amazon S3)-Buckets aktiviert ist. Da sensible Daten in Amazon S3 Buckets gespeichert werden können, sollten Sie die Verschlüsselung aktivieren, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.3.8	Schützen Sie Prüfungsinformationen und Tools zur Prüfung vor unbefugtem Zugriff, Änderung und Löschung.	s-3 bucket-versioning-enabled	Die Versionsverwaltung von Amazon Simple Storage Service (Amazon S3)-Buckets hilft dabei, mehrere Varianten eines Objekts im selben Amazon-S3-Bucket zu speichern. Verwenden Sie die Versionsverwaltung, um sämtliche Versionen aller Objekte in Ihrem Amazon-S3-Bucket zu speichern, abzurufen oder wiederherzustellen. Mit der Versionsverwaltung können Sie Versionen sowohl nach unbeabsichtigten Benutzeraktionen als auch nach Anwendungsfehlern problemlos wiederherstellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.4.1	Etablieren und pflegen Sie Basiskonfigurationen und Inventare der Organisationssysteme (einschließlich Hardware, Software, Firmware und Dokumentation) während der jeweiligen Lebenszyklen der Systementwicklung.	ec2- security-group-attached-to -einperiodisch	Diese Regel stellt sicher, dass die Sicherheitsgruppen an eine Amazon Elastic Compute Cloud (Amazon EC2) -Instance oder an eine ENI angehängt sind. Diese Regel unterstützt die Überwachung ungenutzter Sicherheitsgruppen im Bestand und die Verwaltung Ihrer Umgebung.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.4.1	Etablieren und pflegen Sie Basiskonfigurationen und Inventare der Organisationssysteme (einschließlich Hardware, Software, Firmware und Dokumentation) während der jeweiligen Lebenszyklen der Systementwicklung.	ec2-manager instance-managed-by-systems	Eine Bestandsaufnahme der Softwareplattformen und Anwendungen innerhalb des Unternehmens ist möglich, indem Amazon Elastic Compute Cloud (Amazon EC2) - Instances mit AWS Systems Manager verwaltet werden. Verwenden Sie AWS Systems Manager, um detaillierte Systemkonfigurationen, Betriebssystem-Patch-Levels, Namen und Typ der Dienste, Softwareinstallationen, Anwendungsname, Herausgeber und Version sowie andere Details zu Ihrer Umgebung bereitzustellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.4.1	Etablieren und pflegen Sie Basiskonfigurationen und Inventare der Organisationssysteme (einschließlich Hardware, Software, Firmware und Dokumentation) während der jeweiligen Lebenszyklen der Systementwicklung.	ec2-check managedinstance-association-compliance-status	Verwenden Sie AWS Systems Manager Associations, um bei der Inventarisierung von Softwareplattformen und Anwendungen innerhalb eines Unternehmens zu helfen. AWS Systems Manager weist Ihren verwalteten Instanzen einen Konfigurationsstatus zu und ermöglicht es Ihnen, Basiswerte für Betriebssystem-Patch-Levels, Softwareinstallationen, Anwendungskonfigurationen und andere Details zu Ihrer Umgebung festzulegen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.4.1	Etablieren und pflegen Sie Basiskonfigurationen und Inventare der Organisationssysteme (einschließlich Hardware, Software, Firmware und Dokumentation) während der jeweiligen Lebenszyklen der Systementwicklung.	ec2-stopped-instance	Aktivieren Sie diese Regel, um bei der Basiskonfiguration von Amazon Elastic Compute Cloud (Amazon EC2) - Instances zu helfen, indem Sie überprüfen, ob EC2 Amazon-Instances gemäß den Standards Ihrer Organisation für mehr als die zulässige Anzahl von Tagen gestoppt wurden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.4.1	Etablieren und pflegen Sie Basiskonfigurationen und Inventare der Organisationssysteme (einschließlich Hardware, Software, Firmware und Dokumentation) während der jeweiligen Lebenszyklen der Systementwicklung.	ec2- volume-inuse-check	Diese Regel stellt sicher, dass Amazon Elastic Block Store-Volumes, die an Amazon Elastic Compute Cloud (Amazon EC2) - Instances angehängt sind, zum Löschen markiert werden, wenn eine Instance beendet wird. Wenn ein Amazon-EBS-Volume nicht gelöscht wird, wenn die Instance, an die es angehängt ist, beendet wird, kann dies gegen das Konzept der geringsten Funktionalität verstoßen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.4.1	Etablieren und pflegen Sie Basiskonfigurationen und Inventare der Organisationssysteme (einschließlich Hardware, Software, Firmware und Dokumentation) während der jeweiligen Lebenszyklen der Systementwicklung.	eip-attached	Diese Regel stellt sicher, dass Elastic, die einer Amazon Virtual Private Cloud (Amazon VPC) IPs zugewiesen sind, an Amazon Elastic Compute Cloud (Amazon EC2) - Instances oder verwendete Elastic Network Interfaces angehängt sind. Diese Regel hilft bei der Überwachung ungenutzter Inhalte EIPs in Ihrer Umgebung.
3.4.6	Wenden Sie das Prinzip der geringsten Funktionalität an, indem Sie Organisationssysteme so konfigurieren, dass sie nur unbedingt erforderliche Funktionen bereitstellen.	ec-2 instance-profile-attached	EC2 Instanzprofile übergeben eine IAM-Rolle an eine EC2 Instance. Das Anhängen eines Instance-Profils an Ihre Instances kann bei der Implementierung von geringsten Berechtigungen und der Berechtigungsverwaltung helfen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.4.6	Wenden Sie das Prinzip der geringsten Funktionalität an, indem Sie Organisationssysteme so konfigurieren, dass sie nur unbedingt erforderliche Funktionen bereitstellen.	ecs-task-definition-user-for-host-mode-check	Wenn für eine Aufgabendefinition erhöhte Berechtigungen gelten, liegt das daran, dass der Kunde diesen Konfigurationen ausdrücklich zugestimmt hat. Diese Kontrolle prüft, ob eine unerwartete Berechtigungseskalation vorliegt, wenn für eine Aufgabendefinition das Host-Netzwerk aktiviert ist, die Kunden aber keine erhöhten Berechtigungen aktiviert haben.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.4.6	Wenden Sie das Prinzip der geringsten Funktionalität an, indem Sie Organisationssysteme so konfigurieren, dass sie nur unbedingt erforderliche Funktionen bereitstellen.	iam-no-inline-policy-überprüfen	Stellen Sie sicher, dass ein Benutzer, eine IAM-Rolle oder eine IAM-Gruppe (AWS Identity and Access Management) nicht über eine Inline-Richtlinie zur Zugriffskontrolle auf Systeme und Ressourcen verfügt. AWS empfiehlt, verwaltete Richtlinien anstelle von Inline-Richtlinien zu verwenden. Verwaltete Richtlinien ermöglichen Wiederverwendbarkeit, Versionsverwaltung, Rollback und Delegierung der Berechtigungsverwaltung.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.4.6	Wenden Sie das Prinzip der geringsten Funktionalität an, indem Sie Organisationssysteme so konfigurieren, dass sie nur unbedingt erforderliche Funktionen bereitstellen.	iam-policy-no-statements-with-full-access	Stellen Sie sicher, dass IAM-Aktionen nur auf die benötigten Aktionen beschränkt sind. Wenn Benutzern mehr Rechte eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Rechte und der Aufgabentrennung verstoßen.
3.4.6	Wenden Sie das Prinzip der geringsten Funktionalität an, indem Sie Organisationssysteme so konfigurieren, dass sie nur unbedingt erforderliche Funktionen bereitstellen.	ssm-document-not-public	Stellen Sie sicher, dass AWS Systems Manager (SSM) - Dokumente nicht öffentlich sind, da dies einen unbeabsichtigten Zugriff auf Ihre SSM-Dokumente ermöglichen kann. Ein öffentliches SSM-Dokument kann Informationen über Ihr Konto, Ihre Ressourcen und internen Prozesse preisgeben.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.4.6	Wenden Sie das Prinzip der geringsten Funktionalität an, indem Sie Organisationssysteme so konfigurieren, dass sie nur unbedingt erforderliche Funktionen bereitstellen.	dms-replication-not-public	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass auf DMS-Replikationsinstanzen nicht öffentlich zugegriffen werden kann. DMS-Replikations-Instances können vertrauliche Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.
3.4.6	Wenden Sie das Prinzip der geringsten Funktionalität an, indem Sie Organisationssysteme so konfigurieren, dass sie nur unbedingt erforderliche Funktionen bereitstellen.	ebs-snapshot-public-restorable-überprüfen	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass EBS-Snapshots nicht öffentlich wiederherstellbar sind. EBS-Volume-Snapshots können vertrauliche Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.4.6	Wenden Sie das Prinzip der geringsten Funktionalität an, indem Sie Organisationssysteme so konfigurieren, dass sie nur unbedingt erforderliche Funktionen bereitstellen.	ec2-manager instance-managed-by-systems	Eine Bestandsaufnahme der Softwareplattformen und Anwendungen innerhalb des Unternehmens ist möglich, indem Amazon Elastic Compute Cloud (Amazon EC2) - Instances mit AWS Systems Manager verwaltet werden. Verwenden Sie AWS Systems Manager, um detaillierte Systemkonfigurationen, Betriebssystem-Patch-Levels, Namen und Typ der Dienste, Softwareinstallationen, Anwendungsname, Herausgeber und Version sowie andere Details zu Ihrer Umgebung bereitzustellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.4.6	Wenden Sie das Prinzip der geringsten Funktionalität an, indem Sie Organisationssysteme so konfigurieren, dass sie nur unbedingt erforderliche Funktionen bereitstellen.	ec2-prüfen managedinstance-association-compliance-status	Verwenden Sie AWS Systems Manager Associations, um bei der Inventarisierung von Softwareplattformen und Anwendungen innerhalb eines Unternehmens zu helfen. AWS Systems Manager weist Ihren verwalteten Instanzen einen Konfigurationsstatus zu und ermöglicht es Ihnen, Basiswerte für Betriebssystem-Patch-Levels, Softwareinstallationen, Anwendungskonfigurationen und andere Details zu Ihrer Umgebung festzulegen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.4.6	Wenden Sie das Prinzip der geringsten Funktionalität an, indem Sie Organisationssysteme so konfigurieren, dass sie nur unbedingt erforderliche Funktionen bereitstellen.	ec-2 volume-inuse-check	Diese Regel stellt sicher, dass Amazon Elastic Block Store-Volumes, die an Amazon Elastic Compute Cloud (Amazon EC2) - Instances angehängt sind, zum Löschen markiert werden, wenn eine Instance beendet wird. Wenn ein Amazon-EBS-Volume nicht gelöscht wird, wenn die Instance, an die es angehängt ist, beendet wird, kann dies gegen das Konzept der geringsten Funktionalität verstoßen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.4.6	Wenden Sie das Prinzip der geringsten Funktionalität an, indem Sie Organisationssysteme so konfigurieren, dass sie nur unbedingt erforderliche Funktionen bereitstellen.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) kann Ihnen dabei helfen, die Prinzipien der geringsten Rechte und der Aufgabentrennung in Zugriffsberechtigungen und Autorisierungen zu integrieren und so zu verhindern, dass Richtlinien „Effect“: „Allow“ mit „Action“: „*“ anstelle von „Resource“: „*“ enthalten. Wenn Benutzern mehr Rechte eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und der Aufgabentrennung verstoßen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.4.6	Wenden Sie das Prinzip der geringsten Funktionalität an, indem Sie Organisationssysteme so konfigurieren, dass sie nur unbedingt erforderliche Funktionen bereitstellen.	iam-root-access-key-überprüfen	Der Zugriff auf Systeme und Ressourcen kann gesteuert werden, indem überprüft wird, ob der Root-Benutzer keine Zugriffsschlüssel mit seiner AWS Identity and Access Management (IAM) -Rolle verknüpft hat. Stellen Sie sicher, dass die Root-Zugriffsschlüssel gelöscht werden. Erstellen und verwenden Sie stattdessen rollenbasierte Funktionen, AWS-Konten um das Prinzip der geringsten Funktionalität zu berücksichtigen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.4.6	Wenden Sie das Prinzip der geringsten Funktionalität an, indem Sie Organisationssysteme so konfigurieren, dass sie nur unbedingt erforderliche Funktionen bereitstellen.	iam-user-no-policies-überprüfen	Diese Regel stellt sicher, dass AWS Identity and Access Management (IAM)-Richtlinien nur Gruppen oder Rollen zugewiesen werden, um den Zugriff auf Systeme und Ressourcen zu kontrollieren. Die Zuweisung von Berechtigungen auf Gruppen- oder Rollenebene trägt dazu bei, die Wahrscheinlichkeit zu verringern, dass eine Identität übermäßige Berechtigungen erhält oder beibehält.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.4.6	Wenden Sie das Prinzip der geringsten Funktionalität an, indem Sie Organisationssysteme so konfigurieren, dass sie nur unbedingt erforderliche Funktionen bereitstellen.	lambda-function-public-access-verboten	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass AWS Lambda-Funktionen nicht öffentlich zugänglich sind. Der öffentliche Zugriff kann möglicherweise die Verfügbarkeit von Ressourcen beeinträchtigen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.4.6	Wenden Sie das Prinzip der geringsten Funktionalität an, indem Sie Organisationssysteme so konfigurieren, dass sie nur unbedingt erforderliche Funktionen bereitstellen.	opensearch-access-control-enabled	Stellen Sie sicher, dass eine differenzierte Zugriffskontrolle für Ihre Amazon OpenSearch Service-Domains aktiviert ist. Eine differenzierte Zugriffskontrolle bietet erweiterte Autorisierungsmechanismen, um den Zugriff auf Amazon Service-Domains mit den geringsten Rechten zu erreichen. OpenSearch Es ermöglicht eine rollenbasierte Zugriffskontrolle auf die Domain sowie Sicherheit auf Index-, Dokument- und Feldebene, Unterstützung für OpenSearch Service-Dashboards, Mehrmandantenfähigkeit und HTTP-Basisauthentifizierung für Service und Kibana. OpenSearch

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.4.6	Wenden Sie das Prinzip der geringsten Funktionalität an, indem Sie Organisationssysteme so konfigurieren, dass sie nur unbedingt erforderliche Funktionen bereitstellen.	rds-snapshots-public-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Relational Database Service (Amazon RDS) -Instances nicht öffentlich sind. Amazon-RDS-Datenbank-Instances können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.4.6	Wenden Sie das Prinzip der geringsten Funktionalität an, indem Sie Organisationssysteme so konfigurieren, dass sie nur unbedingt erforderliche Funktionen bereitstellen.	redshift-cluster-public-access-überprüfen	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Redshift Redshift-Cluster nicht öffentlich sind. Amazon-Redshift-Cluster können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.4.6	Wenden Sie das Prinzip der geringsten Funktionalität an, indem Sie Organisationssysteme so konfigurieren, dass sie nur unbedingt erforderliche Funktionen bereitstellen.	s3-Blöcke-periodisch account-level-public-access	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Simple Storage Service (Amazon S3) -Buckets nicht öffentlich zugänglich sind. Diese Regel trägt dazu bei, sensible Daten vor unbefugten Remote-Benutzern zu schützen, indem sie den öffentlichen Zugriff verhindert. Mit dieser Regel können Sie optional die Parameter ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) und restrictPublicBuckets Parameter (Config Default: True) festlegen. Die tatsächlichen Werte müssen den Richtlini

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			en Ihrer Organisation entsprechen.
3.4.6	Wenden Sie das Prinzip der geringsten Funktionalität an, indem Sie Organisationssysteme so konfigurieren, dass sie nur unbedingt erforderliche Funktionen bereitstellen.	s3- verboten bucket-level-public-access	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Simple Storage Service (Amazon S3) -Buckets nicht öffentlich zugänglich sind. Diese Regel trägt dazu bei, sensible Daten vor unbefugten Remote-Benutzern zu schützen, indem sie den öffentlichen Zugriff auf Bucket-Ebene verhindert.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.4.6	Wenden Sie das Prinzip der geringsten Funktionalität an, indem Sie Organisationssysteme so konfigurieren, dass sie nur unbedingt erforderliche Funktionen bereitstellen.	s-3 bucket-public-read-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie nur autorisierten Benutzern, Prozessen und Geräten Zugriff auf Amazon Simple Storage Service (Amazon S3) - Buckets gewähren. Die Verwaltung des Zugriffs sollte mit der Klassifizierung der Daten übereinstimmen.
3.4.6	Wenden Sie das Prinzip der geringsten Funktionalität an, indem Sie Organisationssysteme so konfigurieren, dass sie nur unbedingt erforderliche Funktionen bereitstellen.	s-3 bucket-public-write-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie nur autorisierten Benutzern, Prozessen und Geräten Zugriff auf Amazon Simple Storage Service (Amazon S3) - Buckets gewähren. Die Verwaltung des Zugriffs sollte mit der Klassifizierung der Daten übereinstimmen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.4.7	Einschränkung, Deaktivierung und Verhinderung der Verwendung von nicht unbedingt erforderl ichen Funktionen, Ports, Protokollen oder Diensten.	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) Security Groups können bei der Verwaltung des Netzwerkzugriffs helfen, indem sie eine statusbeh aftete Filterung von eingehendem und ausgehendem Netzwerkverkehr zu Ressourcen bereitste llen. AWS Wenn Sie eingehenden (oder entfernten) Datenverk ehr von 0.0.0.0/0 bis Port 22 auf Ihren Ressourcen nicht zulassen, können Sie den Remote-Zugriff einschränken.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.4.7	Einschränkung, Deaktivierung und Verhinderung der Verwendung von nicht unbedingt erforderlichen Funktionen, Ports, Protokollen oder Diensten.	restricted-common-ports	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass gemeinsame Ports für Amazon Elastic Compute Cloud (Amazon EC2) -Sicherheitsgruppen eingeschränkt sind. Wenn der Zugriff auf Ports nicht auf vertrauenswürdige Quellen beschränkt wird, kann dies zu Angriffen auf die Verfügbarkeit, Integrität und Vertraulichkeit von Systemen führen. Mit dieser Regel können Sie optional die Parameter blockedPort1–blockedPort5 festlegen (Standardkonfigurationen: 20, 21, 3389, 3306, 4333). Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.4.7	Einschränkung, Deaktivierung und Verhinderung der Verwendung von nicht unbedingt erforderl ichen Funktionen, Ports, Protokollen oder Diensten.	vpc-default-security-group-geschlossen	Sicherheitsgruppen von Amazon Elastic Compute Cloud (Amazon EC2) können bei der Verwaltung des Netzwerkzugriffs helfen, indem sie eine statusbehaftete Filterung des ein- und ausgehenden Netzwerkverkehrs zu Ressourcen bereitstellen. AWS Die Beschränk ung des gesamten Datenverkehrs auf die Standardsicherheit sgruppe hilft dabei, den Fernzugriff auf Ihre Ressourcen einzuschränken. AWS

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.4.7	Einschränkung, Deaktivierung und Verhinderung der Verwendung von nicht unbedingt erforderlichen Funktionen, Ports, Protokollen oder Diensten.	vpc-sg-open-only-to-authorized-ports	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass gemeinsame Ports für Amazon Elastic Compute Cloud (Amazon EC2) -Sicherheitsgruppen eingeschränkt sind. Wenn der Zugriff auf Ports nicht auf vertrauenswürdige Quellen beschränkt wird, kann dies zu Angriffen auf die Verfügbarkeit, Integrität und Vertraulichkeit von Systemen führen. Durch die Beschränkung des Zugriffs auf Ressourcen innerhalb einer Sicherheitsgruppe aus dem Internet (0.0.0.0/0) kann der Fernzugriff auf interne Systeme gesteuert werden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.4.9	Steuern und überwachen Sie von Benutzern installierte Software.	ec2-manager instance-managed-by-systems	Eine Bestandsaufnahme der Softwareplattformen und Anwendungen innerhalb des Unternehmens ist möglich, indem Amazon Elastic Compute Cloud (Amazon EC2) - Instances mit AWS Systems Manager verwaltet werden. Verwenden Sie AWS Systems Manager, um detaillierte Systemkonfigurationen, Betriebssystem-Patch-Levels, Namen und Typ der Dienste, Softwareinstallationen, Anwendungsname, Herausgeber und Version sowie andere Details zu Ihrer Umgebung bereitzustellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.4.9	Steuern und überwachen Sie von Benutzern installierte Software.	ec2-check managedinstance-association-compliance-status	Verwenden Sie AWS Systems Manager Associations, um bei der Inventarisierung von Softwareplattformen und Anwendungen innerhalb eines Unternehmens zu helfen. AWS Systems Manager weist Ihren verwalteten Instanzen einen Konfigurationsstatus zu und ermöglicht es Ihnen, Basiswerte für Betriebssystem-Patch-Levels, Softwareinstallationen, Anwendungskonfigurationen und andere Details zu Ihrer Umgebung festzulegen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.5.2	Authentifizieren (oder verifizieren) Sie die Identitäten dieser Benutzer, Prozesse oder Geräte als Voraussetzung für den Zugriff auf Systeme der Organisation.	efs-access-point-enforce-Benutzeridentität	Um die Implementierung des Prinzips der geringsten Rechte zu unterstützen, stellen Sie sicher, dass die Benutzerdurchsetzung für Ihr Amazon Elastic File System (Amazon EFS) aktiviert ist. Wenn diese Option aktiviert ist, ersetzt Amazon EFS den Benutzer und die Gruppe IDs des NFS-Clients durch die Identität, die auf dem Access Point für alle Dateisystemoperationen konfiguriert ist, und gewährt nur Zugriff auf diese erzwungene Benutzeridentität.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.5.2	Authentifizieren (oder verifizieren) Sie die Identitäten dieser Benutzer, Prozesse oder Geräte als Vorausset zung für den Zugriff auf Systeme der Organisation.	iam-user-mfa-enabled	Aktivieren Sie diese Regel, um den Zugriff auf Ressourcen in der Cloud einzuschr änken. AWS Diese Regel sorgt dafür, dass die Multi-Fak tor-Authentifizier ung (MFA) für alle Benutzer aktiviert ist. MFA sorgt für eine weitere Schutzebe ne zusätzlich zu den Anmeldeinformation en. Reduzieren Sie Fälle von kompromit tierten Konten, indem Sie MFA für Benutzer vorschreiben.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.5.2	Authentifizieren (oder verifizieren) Sie die Identitäten dieser Benutzer, Prozesse oder Geräte als Voraussetzung für den Zugriff auf Systeme der Organisation.	mfa-enabled-for-iam-Konsolenzugriff	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass MFA für alle AWS Identity and Access Management (IAM) -Benutzer aktiviert ist, die über ein Konsolenkennwort verfügen. MFA sorgt für eine weitere Schutzebene zusätzlich zu den Anmeldeinformationen. Indem Sie MFA für Benutzer vorschreiben, können Sie Fälle kompromittierter Konten reduzieren und verhindern, dass unbefugte Benutzer auf vertrauliche Daten zugreifen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.5.3	Verwenden Sie die Multifaktor-Authentifizierung für den lokalen und Netzwerkzugriff auf privilegierte Konten und für den Netzwerkzugriff auf nicht privilegierte Konten.	iam-user-mfa-enabled	Aktivieren Sie diese Regel, um den Zugriff auf Ressourcen in der AWS Cloud einzuschränken. Diese Regel sorgt dafür, dass die Multi-Faktor-Authentifizierung (MFA) für alle Benutzer aktiviert ist. MFA sorgt für eine weitere Schutzebene zusätzlich zu den Anmeldeinformationen. Reduzieren Sie Fälle von kompromittierten Konten, indem Sie MFA für Benutzer vorschreiben.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.5.3	Verwenden Sie die Multifaktor-Authentifizierung für den lokalen und Netzwerkzugriff auf privilegierte Konten und für den Netzwerkzugriff auf nicht privilegierte Konten.	mfa-enabled-for-iam-Konsolenzugriff	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass MFA für alle AWS Identity and Access Management (IAM) -Benutzer aktiviert ist, die über ein Konsolenkennwort verfügen. MFA sorgt für eine weitere Schutzebene zusätzlich zu den Anmeldeinformationen. Indem Sie MFA für Benutzer vorschreiben, können Sie Fälle kompromittierter Konten reduzieren und verhindern, dass unbefugte Benutzer auf vertrauliche Daten zugreifen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.5.3	Verwenden Sie die Multifaktor-Authentifizierung für den lokalen und Netzwerkzugriff auf privilegierte Konten und für den Netzwerkzugriff auf nicht privilegierte Konten.	root-account-hardware-mfa-aktiviert	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Hardware-MFA für den Root-Benutzer aktiviert ist. Der Stammbenutzer ist der AWS-Konto-Benutzer mit den meisten Berechtigungen. MFA sorgt für eine weitere Schutzebene zusätzlich zu den Anmeldeinformationen. Indem Sie MFA für den Root-Benutzer vorschreiben, können Sie die Anzahl AWS-Konten kompromittierter Benutzer reduzieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.5.3	Verwenden Sie die Multifaktor-Authentifizierung für den lokalen und Netzwerkzugriff auf privilegierte Konten und für den Netzwerkzugriff auf nicht privilegierte Konten.	root-account-mfa-enabled	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass MFA für den Root-Benutzer aktiviert ist. Der Stammbenutzer ist der AWS-Konto-Benutzer mit den meisten Berechtigungen. MFA sorgt für eine weitere Schutzebene zusätzlich zu den Anmeldeinformationen. Indem Sie MFA für den Root-Benutzer vorschreiben, können Sie die Anzahl AWS-Konten kompromittierter Benutzer reduzieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.5.5	Verhindern Sie die Wiederverwendung von Identifikatoren für einen bestimmten Zeitraum.	iam-password-policy	Die Identitäten und Anmeldeinformationen werden auf der Grundlage einer organisatorischen IAM-Passwortrichtlinie ausgestellt, verwaltet und verifiziert. Sie erfüllen oder übertreffen die Anforderungen von NIST SP 800-63 und dem Standard „Best Practices“ von AWS Foundational Security für Passwortstärke. Mit dieser Regel können Sie optional RequireUppercaseCharacters (Wert für AWS grundlegende Sicherheitsbewährte Methoden: wahr), RequireLowercaseCharacters (Wert für bewährte Methoden für AWS grundlegende Sicherheit: wahr), RequireSymbols (Wert für bewährte Methoden für AWS grundlegende Sicherheit:

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			wahr), RequireNumbers (Wert für bewährte Methoden für AWS grundlegende Sicherheit: wahr), MinimumPasswordLength (Wert für bewährte Methoden für AWS grundlegende Sicherheit: 14), PasswordReusePrevention (Wert für bewährte Methoden für AWS grundlegende Sicherheit: 24) und MaxPasswordAge (Wert für bewährte Methoden für AWS grundlegende Sicherheit: 90) für Ihr IAM festlegen. Kennwortrichtlinie. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.5.6	Deaktivieren Sie Identifikatoren nach einem bestimmten Zeitraum der Inaktivität.	iam-user-unused-credentials-überprüfen	AWS Identity and Access Management (IAM) kann Ihnen bei Zugriffsberechtigungen und Autorisierungen helfen, indem es nach IAM-Passwörtern und Zugriffsschlüsseln sucht, die für einen bestimmten Zeitraum nicht verwendet wurden. Wenn ungenutzte Anmeldeinformationen identifiziert werden, müssen Sie sie deaktivieren und/oder entfernen, da dies gegen das Prinzip der geringsten Berechtigung verstoßen könnte. Für diese Regel müssen Sie einen Wert für das maxCredentialUsage Alter festlegen (Standardkonfiguration: 90). Der tatsächliche Wert muss den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.5.7	Erzwingen Sie bei der Erstellung neuer Passwörter eine Mindestkomplexität und eine Änderung der Zeichen.	iam-password-policy	Die Identitäten und Anmeldeinformationen werden auf der Grundlage einer organisatorischen IAM-Passwortrichtlinie ausgestellt, verwaltet und verifiziert. Sie erfüllen oder übertreffen die Anforderungen, die von NIST SP 800-63 und dem Standard „Best Practices“ von AWS Foundational Security in Bezug auf die Passwortstärke festgelegt wurden. Mit dieser Regel können Sie optional RequireUppercaseCharacters (Wert für AWS grundlegende Sicherheitsbewährte Methoden: wahr), RequireLowercaseCharacters (Wert für bewährte Methoden für AWS grundlegende Sicherheit: wahr), RequireSymbols (Wert für bewährte Methoden

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			für AWS grundlegende Sicherheit: wahr), RequireNumbers (Wert für bewährte Methoden für AWS grundlegende Sicherheit: wahr), MinimumPasswordLength (Wert für bewährte Methoden für AWS grundlegende Sicherheit: 14), PasswordReusePrevention (Wert für bewährte Methoden für AWS grundlegende Sicherheit: 24) und MaxPasswordAge (Wert für bewährte Methoden für AWS grundlegende Sicherheit: 90) für Ihr IAM festlegen. Kennwortrichtlinie. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.5.8	Verbietet die Wiederverwendung von Passwörtern für eine bestimmte Anzahl neu generiert er Passwörter.	iam-password-policy	Die Identitäten und Anmeldeinformation en werden auf der Grundlage einer organisatorischen IAM-Passwortrichtlinie ausgestellt, verwaltet und verifiziert. Sie erfüllen oder übertreff en die Anforderu ngen des NIST SP 800-63 und des AWS Foundatio nal Security Best Practices-Standards für Passwortstärke. Mit dieser Regel können Sie optional RequireUppercaseCh aracters (Wert für AWS grundlegende Sicherheitsbewährt e Methoden: wahr), RequireLowercaseCh aracters (Wert für bewährte Methoden für AWS grundlege nde Sicherheit: wahr), RequireSy mbols (Wert für bewährte Methoden für AWS grundlege nde Sicherheit:

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			wahr), RequireNumbers (Wert für bewährte Methoden für AWS grundlegende Sicherheit: wahr), MinimumPasswordLength (Wert für bewährte Methoden für AWS grundlegende Sicherheit: 14), PasswordReusePrevention (Wert für bewährte Methoden für AWS grundlegende Sicherheit: 24) und MaxPasswordAge (Wert für bewährte Methoden für AWS grundlegende Sicherheit: 90) für Ihr IAM festlegen. Kennwortrichtlinie. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.5.10	Speichern und übertragen Sie nur kryptografisch geschützte Passwörter.	elasticsearch-node-to-node-Verschlüsselungsprüfung	Stellen Sie sicher, dass die node-to-node Verschlüsselung für Amazon OpenSearch Service aktiviert ist. Node-to-nodeVerschlüsselung ermöglicht die TLS 1.2-Verschlüsselung für die gesamte Kommunikation innerhalb der Amazon Virtual Private Cloud (Amazon VPC). Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.
3.5.10	Speichern und übertragen Sie nur kryptografisch geschützte Passwörter.	elb-tls-https-listeners-nur	Stellen Sie sicher, dass Ihre Elastic Load Balancer (ELBs) mit SSL- oder HTTPS-Listenern konfiguriert sind. Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.5.10	Speichern und übertragen Sie nur kryptografisch geschützte Passwörter.	alb-http-to-https-Umleitungsprüfung	Um Daten während der Übertragung zu schützen, stellen Sie sicher, dass Ihr Application Load Balancer unverschlüsselte HTTP-Anfragen automatisch an HTTPS umleitet. Da sensible Daten vorhanden sein können, sollten Sie die Verschlüsselung bei der Übertragung aktivieren, um diese Daten zu schützen.
3.5.10	Speichern und übertragen Sie nur kryptografisch geschützte Passwörter.	api-gw-ssl-enabled	Stellen Sie sicher, dass die REST-API-Stufen von Amazon API Gateway mit SSL-Zertifikaten konfiguriert sind, damit Backend-Systeme überprüfen können, ob Anforderungen von API Gateway stammen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.5.10	Speichern und übertragen Sie nur kryptografisch geschützte Passwörter.	elb-acm-certificate-required	Zum Schutz von eventuell vorhandenen sensiblen Daten sowie von Daten während der Übertragung muss die Verschlüsselung für Ihr Elastic Load Balancing aktiviert sein. Verwenden Sie AWS Certificate Manager, um öffentliche und private SSL/TLS-Zertifikate mit AWS Diensten und internen Ressourcen zu verwalten, bereitzustellen und bereitzustellen.
3.5.10	Speichern und übertragen Sie nur kryptografisch geschützte Passwörter.	encrypted-volumes	Aktivieren Sie die Verschlüsselung für Ihre Amazon-Elastic-Block-Store-(Amazon-EBS-)Volumes, um eventuell vorhandene sensible Daten sowie Daten im Ruhezustand zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.5.10	Speichern und übertragen Sie nur kryptografisch geschützte Passwörter.	opensearch-node-to-node-Verschlüsselungsprüfung	Stellen Sie sicher, dass die node-to-node Verschlüsselung für Amazon OpenSearch Service aktiviert ist. Node-to-nodeVerschlüsselung ermöglicht die TLS 1.2-Verschlüsselung für die gesamte Kommunikation innerhalb der Amazon Virtual Private Cloud (Amazon VPC). Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.5.10	Speichern und übertragen Sie nur kryptografisch geschützte Passwörter.	redshift-cluster-configuration-check	Um Daten im Ruhezustand zu schützen, muss die Verschlüsselung für Ihre Amazon-Redshift-Cluster aktiviert sein. Sie müssen auch sicherstellen, dass die erforderlichen Konfigurationen auf Amazon-Redshift-Clustern bereitgestellt werden. Die Prüfungsprotokollierung muss aktiviert sein, um Informationen zu Verbindungen und Benutzeraktivitäten in der Datenbank bereitzustellen. Diese Regel erfordert, dass ein Wert für clusterDbEncrypted (Config Default: TRUE) und LoggingEnabled (Config Default: TRUE) gesetzt ist. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.5.10	Speichern und übertragen Sie nur kryptografisch geschützte Passwörter.	redshift-require-tls-ssl	Stellen Sie sicher, dass Ihre Amazon-Redshift-Cluster eine TLS/SSL-Verschlüsselung erfordern, um eine Verbindung zu SQL-Clients herzustellen. Da sensible Daten vorhanden sein können, sollten Sie die Verschlüsselung bei der Übertragung aktivieren, um diese Daten zu schützen.
3.5.10	Speichern und übertragen Sie nur kryptografisch geschützte Passwörter.	s3-aktiviert bucket-server-side-encryption	Zum Schutz von Daten im Ruhezustand müssen Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon Simple Storage Service (Amazon S3)-Buckets aktiviert ist. Da sensible Daten in Amazon S3 Buckets gespeichert werden können, sollten Sie die Verschlüsselung aktivieren, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.5.10	Speichern und übertragen Sie nur kryptografisch geschützte Passwörter.	s-3 bucket-ssl-requests-only	Um Daten während der Übertragung zu schützen, stellen Sie sicher, dass Ihre Amazon Simple Storage Service (Amazon S3)-Buckets Anfragen zur Verwendung von Secure Socket Layer (SSL)-Buckets erfordern. Da sensible Daten vorhanden sein können, sollten Sie die Verschlüsselung bei der Übertragung aktivieren, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.6.1	Richten Sie eine Funktion zur Bearbeitung von Betriebsvorfällen für Organisationssysteme ein, die Maßnahmen zur Vorbereitung, Erkennung, Analyse, Eindämmung und Wiederherstellung sowie Benutzerr eaktionen umfasst.	guardduty-non-archived-findings	Amazon GuardDuty hilft Ihnen dabei, die Auswirkungen eines Vorfalls zu verstehen, indem es die Ergebnisse nach Schweregrad klassifiziert: niedrig, mittel und hoch. Diese Klassifizierungen können Sie zur Festlegung von entsprechenden Strategien und Prioritäten zur Behebung solcher Vorfälle verwenden. Mit dieser Regel können Sie optional daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7) und daysHighSev (Config Default: 1) für nicht archivierte Ergebnisse festlegen, wie es die Richtlinien Ihrer Organisation erfordern.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.6.1	Richten Sie eine Funktion zur Bearbeitung von Betriebsvorfällen für Organisationssysteme ein, die Maßnahmen zur Vorbereitung, Erkennung, Analyse, Eindämmung und Wiederherstellung sowie Benutzerr eaktionen umfasst.	securityhub-enabled	AWS Security Hub hilft bei der Überwachung von unbefugtem Personal, Verbindun gen, Geräten und Software. AWS Security Hub aggregiert, organisie rt und priorisie rt die Sicherhei tswarnungen oder Ergebnisse mehrerer Dienste. AWS Einige dieser Dienste sind Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer und AWS Firewall Manager sowie AWS Partnerlösungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.6.1	Richten Sie eine Funktion zur Bearbeitung von Betriebsvorfällen für Organisationssysteme ein, die Maßnahmen zur Vorbereitung, Erkennung, Analyse, Eindämmung und Wiederherstellung sowie Benutzerr eaktionen umfasst.	cloudwatch-alarm-action-check	Amazon CloudWatch alarmiert, wenn eine Metrik den Schwellen wert für eine bestimmte Anzahl von Bewertungszeiträum en überschreitet. Der Alarm führt eine oder mehrere Aktionen durch, die vom Wert der Metrik oder des Ausdrucks im Vergleich zu einem Schwellenwert in einer Reihe von Zeiträumen abhängt. Diese Regel erfordert einen Wert für alarmActionRequired (Config Default: True), insufficientDataAc tion Required (Config Default: True), okActionRequired (Config Default: False). Der tatsächli che Wert muss die Alarmaktionen für Ihre Umgebung widerspie geln.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.6.1	Richten Sie eine Funktion zur Bearbeitung von Betriebsvorfällen für Organisationssysteme ein, die Maßnahmen zur Vorbereitung, Erkennung, Analyse, Eindämmung und Wiederherstellung sowie Benutzerr eaktionen umfasst.	guardduty-enabled-centralized	Amazon GuardDuty kann mithilfe von Threat Intellige nce Feeds helfen, potenzielle Cybersich erheitsereignisse zu überwachen und zu erkennen. Dazu gehören Listen mit bösartigen IPs und maschinel len Lernmethoden zur Identifizierung unerwarteter, nicht autorisierter und bösartiger Aktivitäten in Ihrer AWS Cloud-Umgebung.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.11.2	Regelmäßiges Scannen auf Schwachstellen in den Systemen und Anwendung en der Organisat ion und wenn neue Schwachstellen, die das System betreffen, festgestellt werden.	securityhub-enabled	AWS Security Hub hilft bei der Überwachung von unbefugtem Personal, Verbindun gen, Geräten und Software. AWS Security Hub aggregiert, organisie rt und priorisie rt die Sicherhei tswarnungen oder Ergebnisse mehrerer Dienste. AWS Einige dieser Dienste sind Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer und AWS Firewall Manager sowie AWS Partnerlösungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.11.2	Regelmäßiges Scannen auf Schwachstellen in den Systemen und Anwendung en der Organisat ion und wenn neue Schwachstellen, die das System betreffen, festgestellt werden.	guardduty-enabled-centralized	Amazon GuardDuty kann mithilfe von Threat Intellige nce Feeds helfen, potenzielle Cybersich erheitsereignisse zu überwachen und zu erkennen. Dazu gehören Listen mit bösartigen IPs und maschinel len Lernmethoden zur Identifizierung unerwarteter, nicht autorisierter und bösartiger Aktivitäten in Ihrer AWS Cloud-Umgebung.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.11.3	Behebung von Sicherheitslücken gemäß Risikobeurteilungen.	guardduty-non-archived-findings	Amazon GuardDuty hilft Ihnen dabei, die Auswirkungen eines Vorfalls zu verstehen, indem es die Ergebnisse nach Schweregrad klassifiziert: niedrig, mittel und hoch. Diese Klassifizierungen können Sie zur Festlegung von entsprechenden Strategien und Prioritäten zur Behebung solcher Vorfälle verwenden. Mit dieser Regel können Sie optional daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7) und daysHighSev (Config Default: 1) für nicht archivierte Ergebnisse festlegen, wie es die Richtlinien Ihrer Organisation erfordern.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.13.1	Überwachung, Kontrolle und Schutz der Kommunika tion (d.h. der von Organisationssyste men übertragenen oder empfangenen Informationen) an den externen Grenzen und den wichtigsten internen Grenzen von Organisationssyste men.	alb-waf-enabled	Stellen Sie sicher, dass AWS WAF auf Elastic Load Balancers (ELB) aktiviert ist, um Webanwendungen zu schützen. Eine WAF trägt zum Schutz Ihrer Webanwend ungen oder APIs vor gängigen Web-Explo its bei. Diese Web-Exploits können sich auf die Verfügbar keit auswirken, die Sicherheit gefährden oder übermäßige Ressourcen in Ihrer Umgebung verbrauch en.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.13.1	Überwachung, Kontrolle und Schutz der Kommunika tion (d.h. der von Organisationssyste men übertragenen oder empfangenen Informationen) an den externen Grenzen und den wichtigsten internen Grenzen von Organisationssyste men.	elb-tls-https-listeners-nur	Stellen Sie sicher, dass Ihre Elastic Load Balancer (ELBs) mit SSL- oder HTTPS-Listenern konfiguriert sind. Um eventuell vorhanden e sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.13.1	Überwachung, Kontrolle und Schutz der Kommunika tion (d.h. der von Organisationssyste men übertragenen oder empfangenen Informationen) an den externen Grenzen und den wichtigsten internen Grenzen von Organisationssyste men.	ec-2 instances-in-vpc	Stellen Sie Amazon Elastic Compute Cloud (Amazon EC2) -Instances innerhalb einer Amazon Virtual Private Cloud (Amazon VPC) bereit, um eine sichere Kommunika tion zwischen einer Instance und anderen Services innerhalb der Amazon VPC zu ermöglichen, ohne dass ein Internet-Gateway, ein NAT-Gerät oder eine VPN-Verbindung erforderlich ist. Der gesamte Datenverk ehr bleibt sicher in der AWS Cloud. Domains, die sich innerhalb einer VPC befinden, verfügen aufgrund ihrer logischen Isolierun g im Vergleich zu Domains mit öffentlic hen Endpunkten über eine zusätzlic he Sicherheitsebene. Weisen Sie EC2

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			Amazon-Instances einer Amazon-VPC zu, um den Zugriff ordnungsgemäß zu verwalten.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.13.1	Überwachung, Kontrolle und Schutz der Kommunika tion (d.h. der von Organisationssyste men übertragenen oder empfangenen Informationen) an den externen Grenzen und den wichtigsten internen Grenzen von Organisationssyste men.	multi-region-cloudtrail-enabled	AWS CloudTrail zeichnet Aktionen und API-Aufrufe der AWS Management Console auf. Sie können feststellen, welche Benutzer und Konten angerufen wurden AWS, von welcher Quell-IP-Adresse aus die Anrufe getätigt wurden und wann die Anrufe erfolgten. CloudTrail übermittelt Protokolldateien aus allen AWS Regionen an Ihren S3-Bucket , wenn MULTI_REG ION_CLOUD _TRAIL_ENABLED aktiviert ist. Außerdem wird beim AWS Start einer neuen Region derselbe Trail in der neuen Region erstellt. CloudTrail Dadurch erhalten Sie automatis ch Protokolldateien mit API-Aktivitäten für die neue Region.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.13.1	Überwachung, Kontrolle und Schutz der Kommunika tion (d.h. der von Organisationssyste men übertragenen oder empfangenen Informationen) an den externen Grenzen und den wichtigsten internen Grenzen von Organisationssyste men.	no-unrestricted-route-to-igw	Stellen Sie sicher, dass EC2 Amazon-Routentabellen keine uneingeschränkten Routen zu einem Internet-Gateway enthalten. Durch das Entfernen oder Beschränken des Internetzugangs für Workloads innerhalb von Amazon VPCs können unbeabsic htigte Zugriffe in Ihrer Umgebung reduziert werden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.13.1	Überwachung, Kontrolle und Schutz der Kommunika tion (d.h. der von Organisationssyste men übertragenen oder empfangenen Informationen) an den externen Grenzen und den wichtigsten internen Grenzen von Organisationssyste men.	rds-logging-enabled	Um die Protokoll ierung und Überwachung in Ihrer Umgebung zu erleichtern, stellen Sie sicher, dass die Amazon Relationa l Database Service (Amazon RDS)-Prot okollierung aktiviert ist. Mit der Amazon-RDS-Protokollierung können Sie Ereigniss e wie Verbindungen, Verbindungsabbrüch e, Abfragen oder abgefragte Tabellen erfassen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.13,1	Überwachung, Kontrolle und Schutz der Kommunika tion (d.h. der von Organisationssyste men übertragenen oder empfangenen Informationen) an den externen Grenzen und den wichtigsten internen Grenzen von Organisationssyste men.	redshift-enhanced-vpc-routing-aktiviert	Mit Enhanced-VPC-Routing wird erzwungen, dass der gesamte COPY- und UNLOAD-Da tenverkehr zwischen Ihrem Cluster und Datenrepositorys über Ihre Amazon VPC erfolgt. Anschließ end können Sie VPC-Features wie Sicherheitsgruppen und Netzwerkz ugriffskontrolllisten verwenden, um den Netzwerkverkehr zu schützen. Sie können auch VPC-Flow-Logs verwenden, um den Netzwerkverkehr zu überwachen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.13.1	Überwachung, Kontrolle und Schutz der Kommunika tion (d.h. der von Organisationssyste men übertragenen oder empfangenen Informationen) an den externen Grenzen und den wichtigsten internen Grenzen von Organisationssyste men.	securityhub-enabled	AWS Security Hub hilft bei der Überwachung von unbefugtem Personal, Verbindun gen, Geräten und Software. AWS Security Hub aggregiert, organisie rt und priorisie rt die Sicherhei tswarnungen oder Ergebnisse mehrerer Dienste. AWS Einige dieser Dienste sind Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer und AWS Firewall Manager sowie AWS Partnerlösungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.13.1	Überwachung, Kontrolle und Schutz der Kommunikation (d.h. der von Organisationssystemen übertragenen oder empfangenen Informationen) an den externen Grenzen und den wichtigsten internen Grenzen von Organisationssystemen.	ssm-document-not-public	Stellen Sie sicher, dass AWS Systems Manager (SSM) - Dokumente nicht öffentlich sind, da dies einen unbeabsichtigten Zugriff auf Ihre SSM-Dokumente ermöglichen kann. Ein öffentliches SSM-Dokument kann Informationen über Ihr Konto, Ihre Ressourcen und internen Prozesse preisgeben.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.13.1	Überwachung, Kontrolle und Schutz der Kommunikation (d.h. der von Organisationssystemen übertragenen oder empfangenen Informationen) an den externen Grenzen und den wichtigsten internen Grenzen von Organisationssystemen.	wafv2-logging-enabled	Um die Protokollierung und Überwachung in Ihrer Umgebung zu erleichtern, aktivieren Sie die AWS WAF (V2) -Protokollierung im regionalen und globalen Web. ACLs AWS Die WAF-Protokollierung bietet detaillierte Informationen über den Datenverkehr, der von Ihrer Web-ACL analysiert wird. In den Protokollen werden die Uhrzeit aufgezeichnet, zu der die AWS WAF die Anfrage von Ihrer AWS Ressource erhalten hat, Informationen über die Anfrage und eine Aktion für die Regel, der jede Anfrage entsprach.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.13.1	Überwachung, Kontrolle und Schutz der Kommunikation (d.h. der von Organisationssystemen übertragenen oder empfangenen Informationen) an den externen Grenzen und den wichtigsten internen Grenzen von Organisationssystemen.	acm-certificate-expiration-check	Stellen Sie sicher, dass die Netzwerkintegrität geschützt ist, indem Sie sicherstellen, dass X509-Zertifikate von ACM ausgestellt werden. AWS Diese Zertifikate müssen gültig und dürfen nicht abgelaufen sein. Für diese Regel ist ein Wert für erforderlich daysToExpiration (Wert für bewährte AWS Grundregeln für Sicherheit: 90). Der tatsächliche Wert muss den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.13.1	Überwachung, Kontrolle und Schutz der Kommunika tion (d.h. der von Organisationssyste men übertragenen oder empfangenen Informationen) an den externen Grenzen und den wichtigsten internen Grenzen von Organisationssyste men.	alb-http-to-https-Umleitungsprüfung	Um Daten während der Übertragung zu schützen, stellen Sie sicher, dass Ihr Application Load Balancer unverschl üsselte HTTP-Anfr agen automatisch an HTTPS umleitet. Da sensible Daten vorhanden sein können, sollten Sie die Verschlüsselung bei der Übertragung aktivieren, um diese Daten zu schützen.
3.13.1	Überwachung, Kontrolle und Schutz der Kommunika tion (d.h. der von Organisationssyste men übertragenen oder empfangenen Informationen) an den externen Grenzen und den wichtigsten internen Grenzen von Organisationssyste men.	api-gw-execution-l ogging-aktiviert	Die API-Gateway-Protokollierung zeigt detaillierte Ansichten der Benutzer, die auf die API zugegriff en haben, und wie diese Benutzer auf die API zugegriffen haben. Diese Insights ermöglichen die Einsicht in Benutzera ktivitäten.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.13.1	Überwachung, Kontrolle und Schutz der Kommunika tion (d.h. der von Organisationssyste men übertragenen oder empfangenen Informationen) an den externen Grenzen und den wichtigsten internen Grenzen von Organisationssyste men.	cloudtrail-enabled	AWS CloudTrai l kann durch die Aufzeichnung von Aktionen und API-Aufrufen in der AWS Management Console bei der Nichtabst reitbarkeit helfen. Sie können die Benutzer und die Benutzer AWS-Konten , die einen AWS Dienst aufgerufen haben, die Quell-IP-Adresse, über die die Aufrufe generiert wurden, und den Zeitpunkt der Anrufe identifiz ieren. Einzelheiten zu den erfassten Daten finden Sie unter Inhalt des AWS CloudTrail Datensatzes.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.13.1	Überwachung, Kontrolle und Schutz der Kommunika tion (d.h. der von Organisationssyste men übertragenen oder empfangenen Informationen) an den externen Grenzen und den wichtigsten internen Grenzen von Organisationssyste men.	cloud-trail-log-file-Validierung aktiviert	Verwenden Sie die AWS CloudTrail Protokolldateivali dierung, um die Integrität von Protokoll en zu überprüfen. CloudTrail Mithilfe der Protokolldateivali dierung kann festgestellt werden, ob eine Protokoll datei geändert oder gelöscht wurde oder ob sie nach der Übermittlung CloudTrail unverände rt geblieben ist. Dieses Feature wurde mit dem Branchens tandard entsprech enden Algorithmen entwickelt: SHA-256 für die Hashfunktion und SHA-256 mit RSA für digitale Signature n. Aus diesem Grund ist es rechnerisch unmöglich, CloudTrai l Protokolldateien unbemerkt zu ändern, zu löschen oder zu fälschen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.13.1	Überwachung, Kontrolle und Schutz der Kommunika tion (d.h. der von Organisationssyste men übertragenen oder empfangenen Informationen) an den externen Grenzen und den wichtigsten internen Grenzen von Organisationssyste men.	cloudtrail-s3-data events-enabled	Die Erfassung von Simple Storage Service (Amazon S3)-Datenereigniss en unterstützt die Erkennung von ungewöhnlichen Aktivitäten. Zu den Details gehören AWS-Konto Informationen über den Zugriff auf einen Amazon S3 S3-Bucket, die IP-Adress e und die Uhrzeit des Ereignisses.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.13.1	Überwachung, Kontrolle und Schutz der Kommunika tion (d.h. der von Organisationssyste men übertragenen oder empfangenen Informationen) an den externen Grenzen und den wichtigsten internen Grenzen von Organisationssyste men.	elasticsearch-in-vpc-only	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherste llen, dass sich Amazon OpenSearc h OpenSearch Service (Service) - Domains innerhalb einer Amazon Virtual Private Cloud (Amazon VPC) befinden. Eine OpenSearch Service-Domain innerhalb einer Amazon VPC ermöglicht die sichere Kommunikation zwischen OpenSearc h Service und anderen Services innerhalb der Amazon VPC, ohne dass ein Internet-Gateway, ein NAT-Gerät oder eine VPN-Verbindung erforderlich ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.13.1	Überwachung, Kontrolle und Schutz der Kommunika tion (d.h. der von Organisationssyste men übertragenen oder empfangenen Informationen) an den externen Grenzen und den wichtigsten internen Grenzen von Organisationssyste men.	elb-acm-certificate-required	Zum Schutz von eventuell vorhanden en sensiblen Daten sowie von Daten während der Übertragung muss die Verschlüsselung für Ihr Elastic Load Balancing aktiviert sein. Verwenden Sie AWS Certificate Manager, um öffentlic he und private SSL/ TLS-Zertifikate mit AWS Diensten und internen Ressource n zu verwalten, bereitzustellen und bereitzustellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.13.1	Überwachung, Kontrolle und Schutz der Kommunika tion (d.h. der von Organisationssyste men übertragenen oder empfangenen Informationen) an den externen Grenzen und den wichtigsten internen Grenzen von Organisationssyste men.	elb-logging-enabled	Die Elastic-Load-Balancing-Aktivität ist ein zentraler Kommunikationspunk t innerhalb einer Umgebung. Stellen Sie sicher, dass die ELB-Protokollierun g aktiviert ist. Die gesammelten Daten enthalten detaillie rte Informationen zu Anfragen, die an den ELB gesendet wurden. Jedes Protokoll enthält Informationen wie die Zeit, zu der die Anforderung einging, die Client-IP -Adresse, Latenzen, Anforderungspfade und Serverantworten.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.13,1	Überwachung, Kontrolle und Schutz der Kommunika tion (d.h. der von Organisationssyste men übertragenen oder empfangenen Informationen) an den externen Grenzen und den wichtigsten internen Grenzen von Organisationssyste men.	guardduty-enabled-centralized	Amazon GuardDuty kann mithilfe von Threat Intellige nce Feeds helfen, potenzielle Cybersich erheitsereignisse zu überwachen und zu erkennen. Dazu gehören Listen mit bösartigen IPs und maschinel len Lernmethoden zur Identifizierung unerwarteter, nicht autorisierter und bösartiger Aktivitäten in Ihrer AWS Cloud-Umgebung.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.13.1	Überwachung, Kontrolle und Schutz der Kommunika tion (d.h. der von Organisationssyste men übertragenen oder empfangenen Informationen) an den externen Grenzen und den wichtigsten internen Grenzen von Organisationssyste men.	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) Security Groups können bei der Verwaltung des Netzwerkzugriffs helfen, indem sie eine statusbeh aftete Filterung von eingehendem und ausgehendem Netzwerkverkehr zu Ressourcen bereitste llen. AWS Wenn Sie eingehenden (oder entfernten) Datenverk ehr von 0.0.0.0/0 bis Port 22 auf Ihren Ressourcen nicht zulassen, können Sie den Remote-Zugriff einschränken.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.13.1	Überwachung, Kontrolle und Schutz der Kommunika tion (d.h. der von Organisationssyste men übertragenen oder empfangenen Informationen) an den externen Grenzen und den wichtigsten internen Grenzen von Organisationssyste men.	lambda-inside-vpc	Stellen Sie AWS Lambda-Funktionen in einer Amazon Virtual Private Cloud (Amazon VPC) bereit, um eine sichere Kommunika tion zwischen einer Funktion und anderen Diensten innerhalb der Amazon VPC zu gewährleisten. Bei dieser Konfiguration sind kein Internet-Gateway, kein NAT-Gerät und keine VPN-Verbindung erforderlich. Der gesamte Datenverk ehr bleibt sicher in der Cloud. AWS Domains, die sich innerhalb einer VPC befinden, verfügen aufgrund ihrer logischen Isolierun g im Vergleich zu Domains mit öffentlic hen Endpunkten über eine zusätzliche Sicherheitsebene. Um den Zugriff ordnungsg emäß zu verwalten,

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			sollten AWS Lambda-Funktionen einer VPC zugewiesen werden.
3.13.1	Überwachung, Kontrolle und Schutz der Kommunika tion (d.h. der von Organisationssyste men übertragenen oder empfangenen Informationen) an den externen Grenzen und den wichtigsten internen Grenzen von Organisationssyste men.	opensearch-access-control-enabled	Stellen Sie sicher, dass eine differenz ierte Zugriffskontrolle für Ihre Amazon OpenSearch Service-Domains aktiviert ist. Eine differenz ierte Zugriffskontrolle bietet erweiterte Autorisierungsmech anismen, um den Zugriff auf Amazon Service-Domains mit den geringsten Rechten zu erreichen . OpenSearch Es ermöglicht eine rollenbasierte Zugriffskontrolle auf die Domain sowie Sicherheit auf Index-, Dokument- und Feldebene, Unterstüt zung für OpenSearch Service-Dashboards, Mehrmandantenfähig keit und HTTP-Basi sauthentifizierung für Service und Kibana. OpenSearch

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.13.1	Überwachung, Kontrolle und Schutz der Kommunika tion (d.h. der von Organisationssyste men übertragenen oder empfangenen Informationen) an den externen Grenzen und den wichtigsten internen Grenzen von Organisationssyste men.	opensearch-in-vpc-only	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass sich Amazon OpenSearch Service-Domains innerhalb einer Amazon Virtual Private Cloud (Amazon VPC) befinden. Eine Amazon OpenSearc h Service-Domain innerhalb einer Amazon VPC ermöglicht die sichere Kommunikation zwischen Amazon OpenSearch Service und anderen Services innerhalb der Amazon VPC, ohne dass ein Internet-Gateway, ein NAT-Gerät oder eine VPN-Verbindung erforderlich ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.13.1	Überwachung, Kontrolle und Schutz der Kommunika tion (d.h. der von Organisationssyste men übertragenen oder empfangenen Informationen) an den externen Grenzen und den wichtigsten internen Grenzen von Organisationssyste men.	rds-instance-public-access-überprüfen	Verwalten Sie den Zugriff auf Ressource n in der AWS Cloud, indem Sie sicherste llen, dass Amazon Relational Database Service (Amazon RDS) -Instance s nicht öffentlic h sind. Amazon-RDS-Datenbank-Instances können vertrauliche Informati onen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.13.1	Überwachung, Kontrolle und Schutz der Kommunika tion (d.h. der von Organisationssyste men übertragenen oder empfangenen Informationen) an den externen Grenzen und den wichtigsten internen Grenzen von Organisationssyste men.	redshift-cluster-public-access-überprüfen	Verwalten Sie den Zugriff auf Ressource n in der AWS Cloud, indem Sie sicherste llen, dass Amazon Redshift Redshift-Cluster nicht öffentlic h sind. Amazon-Re dshift-Cluster können vertrauliche Informati onen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.
3.13.1	Überwachung, Kontrolle und Schutz der Kommunika tion (d.h. der von Organisationssyste men übertragenen oder empfangenen Informationen) an den externen Grenzen und den wichtigsten internen Grenzen von Organisationssyste men.	redshift-require-tls-ssl	Stellen Sie sicher, dass Ihre Amazon-Redshift-Cluster eine TLS/SSL-Verschlüss elung erfordern, um eine Verbindung zu SQL-Clients herzustel len. Da sensible Daten vorhanden sein können, sollten Sie die Verschlüsselung bei der Übertragung aktivieren, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.13,1	Überwachung, Kontrolle und Schutz der Kommunika tion (d.h. der von Organisationssyste men übertragenen oder empfangenen Informationen) an den externen Grenzen und den wichtigsten internen Grenzen von Organisationssyste men.	restricted-common-ports	Verwalten Sie den Zugriff auf Ressource n in der AWS Cloud, indem Sie sicherste llen, dass gemeinsam e Ports für Amazon Elastic Compute Cloud (Amazon EC2) -Sicherhe itsgruppen eingeschr ränkt sind. Wenn der Zugriff auf Ports nicht auf vertrauen swürdige Quellen beschränkt wird, kann dies zu Angriffen auf die Verfügbar keit, Integrität und Vertraulichkeit von Systemen führen. Mit dieser Regel können Sie optional die Parameter blockedPo rt1–blockedPort5 festlegen (Standard konfigurationen: 20, 21, 3389, 3306, 4333). Die tatsächli chen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.13.1	Überwachung, Kontrolle und Schutz der Kommunika tion (d.h. der von Organisationssyste men übertragenen oder empfangenen Informationen) an den externen Grenzen und den wichtigsten internen Grenzen von Organisationssyste men.	s3-Blöcke-periodisch account-level-public-access	Verwalten Sie den Zugriff auf Ressource n in der AWS Cloud, indem Sie sicherste llen, dass Amazon Simple Storage Service (Amazon S3) -Buckets nicht öffentlich zugänglic h sind. Diese Regel trägt dazu bei, sensible Daten vor unbefugten Remote-Benutzern zu schützen, indem sie den öffentlichen Zugriff verhinder t. Mit dieser Regel können Sie optional die Parameter ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) und restrictPublicBuck ets Parameter (Config Default: True) festlegen. Die tatsächlichen Werte müssen den Richtlini

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			en Ihrer Organisation entsprechen.
3.13.1	Überwachung, Kontrolle und Schutz der Kommunika tion (d.h. der von Organisationssyste men übertragenen oder empfangenen Informationen) an den externen Grenzen und den wichtigsten internen Grenzen von Organisationssyste men.	s3- verboten bucket-le vel-public-access	Verwalten Sie den Zugriff auf Ressource n in der AWS Cloud, indem Sie sicherste llen, dass Amazon Simple Storage Service (Amazon S3) -Buckets nicht öffentlich zugänglic h sind. Diese Regel trägt dazu bei, sensible Daten vor unbefugten Remote-Benutzern zu schützen, indem sie den öffentlichen Zugriff auf Bucket-Eb ene verhindert.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.13.1	Überwachung, Kontrolle und Schutz der Kommunika tion (d.h. der von Organisationssyste men übertragenen oder empfangenen Informationen) an den externen Grenzen und den wichtigsten internen Grenzen von Organisationssyste men.	s-3 bucket-logging-enabled	Die Amazon Simple Storage Service (Amazon S3)-Serverzugriffs protokollierung bietet eine Methode zur Überwachu ng des Netzwerks im Hinblick auf potenzielle Cybersich erheitsereignisse. Die Ereignisse werden überwacht, indem detaillierte Aufzeichn ungen über die Anfragen erfasst werden, die an einen Amazon-S3-Bucket gestellt wurden. Jeder Zugriffsprotokolle intrag enthält Details zu einer einzelnen Zugriffsanfrage. Zu den Details gehören Anforderer, Bucket-Name, Anforderu ngszeit, Anforderu ngsaktion, Antwortst atus und Fehlercode, falls relevant.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.13.1	Überwachung, Kontrolle und Schutz der Kommunika tion (d.h. der von Organisationssyste men übertragenen oder empfangenen Informationen) an den externen Grenzen und den wichtigsten internen Grenzen von Organisationssyste men.	s-3 bucket-ssl-request s-only	Um Daten während der Übertragung zu schützen, stellen Sie sicher, dass Ihre Amazon Simple Storage Service (Amazon S3)-Bucke ts Anfragen zur Verwendung von Secure Socket Layer (SSL)-Buckets erfordern. Da sensible Daten vorhanden sein können, sollten Sie die Verschlüsselung bei der Übertragung aktivieren, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.13.1	Überwachung, Kontrolle und Schutz der Kommunika tion (d.h. der von Organisationssyste men übertragenen oder empfangenen Informationen) an den externen Grenzen und den wichtigsten internen Grenzen von Organisationssyste men.	vpc-flow-logs-enabled	VPC-Flow-Protokoll e erfassen detaillierte Informationsdatens ätze über den IP-Datenverkehr, der zu und von Netzwerkschnittste llen in Ihrer Amazon Virtual Private Cloud (Amazon VPC) fließt. Standardmäßig enthalten Flow-Prot okolldatensätze Werte für die verschiedenen Komponenten des IP-Flows, einschlie ßlich Quelle, Ziel und Protokoll.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.13,1	Überwachung, Kontrolle und Schutz der Kommunika tion (d.h. der von Organisationssyste men übertragenen oder empfangenen Informationen) an den externen Grenzen und den wichtigsten internen Grenzen von Organisationssyste men.	vpc-sg-open-only-to-authorized-ports	Verwalten Sie den Zugriff auf Ressource n in der AWS Cloud, indem Sie sicherste llen, dass gemeinsam e Ports für Amazon Elastic Compute Cloud (Amazon EC2) -Sicherhe itsgruppen eingeschr ränkt sind. Wenn der Zugriff auf Ports nicht auf vertrauen swürdige Quellen beschränkt wird, kann dies zu Angriffen auf die Verfügbar keit, Integrität und Vertraulichkeit von Systemen führen. Durch die Beschränk ung des Zugriffs auf Ressourcen innerhalb einer Sicherhei tsgruppe aus dem Internet (0.0.0.0/0) kann der Fernzugriff auf interne Systeme gesteuert werden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.13.2	Verwenden Sie Architekturdesigns, Softwareentwicklungstechniken und Prinzipien der Systemtechnik, die eine effektive Informationssicherheit innerhalb von Organisationssystemen fördern.	autoscaling-launch-config-public-ip-deaktiviert	Wenn Sie Ihre Netzwerkschnittstellen mit einer öffentlichen IP-Adresse konfigurieren, sind die diesen Netzwerkschnittstellen zugehörigen Ressourcen über das Internet erreichbar. EC2 Ressourcen sollten nicht öffentlich zugänglich sein, da dies einen unbeabsichtigten Zugriff auf Ihre Anwendungen oder Server ermöglichen kann.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.13.2	Verwenden Sie Architekturdesigns, Softwareentwicklungstechniken und Prinzipien der Systemtechnik, die eine effektive Informationssicherheit innerhalb von Organisationssystemen fördern.	cloudtrail-security-trail-enabled	Diese Regel trägt dazu bei, die Verwendung der AWS empfohlenen bewährten Sicherheitsmethoden für sicherzustellen AWS CloudTrail, indem geprüft wird, ob mehrere Einstellungen aktiviert sind. Dazu gehören die Verwendung von Protokollverschlüsselung, Protokollvalidierung und Aktivierung AWS CloudTrail in mehreren Regionen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.13.2	Verwenden Sie Architekturdesigns, Softwareentwicklungstechniken und Prinzipien der Systemtechnik, die eine effektive Informationssicherheit innerhalb von Organisationssystemen fördern.	dynamodb-in-backup-plan	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon DynamoDB-Tabellen Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.13.2	Verwenden Sie Architekturdesigns, Softwareentwicklungstechniken und Prinzipien der Systemtechnik, die eine effektive Informationssicherheit innerhalb von Organisationssystemen fördern.	ebs-in-backup-plan	Stellen Sie zur Unterstützung der Datensicherungsprozesse sicher, dass Ihre Amazon Elastic Block Store (Amazon EBS) -Volumes Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.13.2	Verwenden Sie Architekturdesigns, Softwareentwicklungstechniken und Prinzipien der Systemtechnik, die eine effektive Informationssicherheit innerhalb von Organisationssystemen fördern.	efs-in-backup-plan	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon Elastic File System (Amazon EFS) -Dateisysteme Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.13.2	Verwenden Sie Architekturdesigns, Softwareentwicklungstechniken und Prinzipien der Systemtechnik, die eine effektive Informationssicherheit innerhalb von Organisationssystemen fördern.	elb-cross-zone-load-Balancing aktiviert	Aktivieren Sie zonenübergreifendes Load Balancing für Ihre Elastic Load Balancer (ELBs), um eine angemessene Kapazität und Verfügbarkeit aufrechtzuerhalten. Zonenübergreifendes Load Balancing reduziert die Notwendigkeit, die gleiche Anzahl von Instances in jeder aktivierten Availability Zone aufrechtzuerhalten. Es verbessert auch die Fähigkeit Ihrer Anwendung, den Verlust einer oder mehrerer Instances zu bewältigen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.13.2	Verwenden Sie Architekturdesigns, Softwareentwicklungstechniken und Prinzipien der Systemtechnik, die eine effektive Informationssicherheit innerhalb von Organisationssystemen fördern.	ec-2 instances-in-vpc	Stellen Sie Amazon Elastic Compute Cloud (Amazon EC2) -Instances innerhalb einer Amazon Virtual Private Cloud (Amazon VPC) bereit, um eine sichere Kommunikation zwischen einer Instance und anderen Services innerhalb der Amazon VPC zu ermöglichen, ohne dass ein Internet-Gateway, ein NAT-Gerät oder eine VPN-Verbindung erforderlich ist. Der gesamte Datenverkehr bleibt sicher in der AWS Cloud. Domains, die sich innerhalb einer VPC befinden, verfügen aufgrund ihrer logischen Isolierung im Vergleich zu Domains mit öffentlichen Endpunkten über eine zusätzliche Sicherheitsebene. Weisen Sie EC2

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			Amazon-Instances einer Amazon-VPC zu, um den Zugriff ordnungsgemäß zu verwalten.
3.13.2	Verwenden Sie Architekturdesigns, Softwareentwicklungstechniken und Prinzipien der Systemtechnik, die eine effektive Informationssicherheit innerhalb von Organisationssystemen fördern.	rds-instance-deletion-protection-aktiviert	Stellen Sie sicher, dass Amazon Relational Database Service (Amazon RDS)-Instances den Löschschutz aktiviert haben. Verwenden Sie den Löschschutz, um zu verhindern, dass Ihre Amazon-RDS-Instances versehentlich oder böswillig gelöscht werden, was zum Verlust der Verfügbarkeit Ihrer Anwendungen führen kann.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.13.2	Verwenden Sie Architekturdesigns, Softwareentwicklungstechniken und Prinzipien der Systemtechnik, die eine effektive Informationssicherheit innerhalb von Organisationssystemen fördern.	rds-in-backup-plan	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon Relational Database Service (Amazon RDS) -Instances Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.13.2	Verwenden Sie Architekturdesigns, Softwareentwicklungstechniken und Prinzipien der Systemtechnik, die eine effektive Informationssicherheit innerhalb von Organisationssystemen fördern.	redshift-backup-enabled	Stellen Sie zur Unterstützung der Datensicherungsprozesse sicher, dass Ihre Amazon-Redshift-Cluster über automatisierte Snapshots verfügen. Wenn automatisierte Snapshots für einen Cluster aktiviert sind, erstellt Redshift in regelmäßigen Abständen Snapshots dieses Clusters. Standardmäßig erstellt Redshift alle acht Stunden oder alle 5 GB einen Snapshot für jeden Knoten mit Datenänderungen oder je nachdem, was zuerst eintritt.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.13.2	Verwenden Sie Architekturdesigns, Softwareentwicklungstechniken und Prinzipien der Systemtechnik, die eine effektive Informationssicherheit innerhalb von Organisationssystemen fördern.	ssm-document-not-public	Stellen Sie sicher, dass AWS Systems Manager (SSM) - Dokumente nicht öffentlich sind, da dies einen unbeabsichtigten Zugriff auf Ihre SSM-Dokumente ermöglichen kann. Ein öffentliches SSM-Dokument kann Informationen über Ihr Konto, Ihre Ressourcen und internen Prozesse preisgeben.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.13.2	Verwenden Sie Architekturdesigns, Softwareentwicklungstechniken und Prinzipien der Systemtechnik, die eine effektive Informationssicherheit innerhalb von Organisationssystemen fördern.	acm-certificate-expiration-check	Stellen Sie sicher, dass die Netzwerkintegrität geschützt ist, indem Sie sicherstellen, dass X509-Zertifikate von ACM ausgestellt werden. AWS Diese Zertifikate müssen gültig und dürfen nicht abgelaufen sein. Für diese Regel ist ein Wert für erforderlich daysToExpiration (Wert für bewährte AWS Grundregeln für Sicherheit: 90). Der tatsächliche Wert muss den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.13.2	Verwenden Sie Architekturdesigns, Softwareentwicklungstechniken und Prinzipien der Systemtechnik, die eine effektive Informationssicherheit innerhalb von Organisationssystemen fördern.	autoscaling-group-elb-healthcheck-erforderlich	Die Elastic Load Balancer (ELB) - Zustandsprüfungen für Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling Scaling-Gruppen unterstützen die Aufrechterhaltung einer angemessenen Kapazität und Verfügbarkeit. Der Load Balancer sendet regelmäßig Pings, versucht Verbindungen herzustellen oder sendet Anfragen, um den Zustand der EC2 Amazon-Instances in einer Gruppe mit auto-scaling zu testen. Wenn eine Instance nicht zurückmeldet, wird der Traffic an eine neue EC2 Amazon-Instance gesendet.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.13.2	Verwenden Sie Architekturdesigns, Softwareentwicklungstechniken und Prinzipien der Systemtechnik, die eine effektive Informationssicherheit innerhalb von Organisationssystemen fördern.	codebuild-project-envvar-awscred-überprüfen	Stellen Sie sicher, dass die Anmeldeinformationen AWS_ACCESS_KEY_ID AWS_SECRET_ACCESS_KEY nicht in AWS Codebuild-Projektumgebungen vorhanden sind. Speichern Sie diese Variablen nicht als Klartext. Das Speichern dieser Variablen als Klartext bewirkt eine unbeabsichtigte Offenlegung von Daten sowie unberechtigte Zugriffe.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.13.2	Verwenden Sie Architekturdesigns, Softwareentwicklungstechniken und Prinzipien der Systemtechnik, die eine effektive Informationssicherheit innerhalb von Organisationssystemen fördern.	codebuild-project-source-repo-URL-Prüfung	Stellen Sie sicher, dass die URL des Quell-Repositorys GitHub oder des Bitbucket-Quell-Repositorys keine persönlichen Zugriffstoken oder Anmeldeinformationen in Codebuild-Projektumgebungen enthält. AWS Verwende OAuth anstelle von persönlichen Zugriffstoken oder Anmeldedaten die Autorisierung für den Zugriff auf GitHub Bitbucket-Repositorys.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.13.2	Verwenden Sie Architekturdesigns, Softwareentwicklungstechniken und Prinzipien der Systemtechnik, die eine effektive Informationssicherheit innerhalb von Organisationssystemen fördern.	db-instance-backup-enabled	Die Sicherungsfunktion von Amazon RDS erstellt Sicherungen Ihrer Datenbanken und Transaktionsprotokolle. Amazon RDS erstellt einen Snapshot für das Speichervolume Ihrer DB-Instance, sodass die gesamte DB-Instance gesichert wird. Sie können im System spezifische Aufbewahrungsfristen festlegen, um Ihre Ausfallsicherheitsanforderungen zu erfüllen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.13,2	Verwenden Sie Architekturdesigns, Softwareentwicklungstechniken und Prinzipien der Systemtechnik, die eine effektive Informationssicherheit innerhalb von Organisationssystemen fördern.	dms-replication-not-public	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass auf DMS-Replikationsinstanzen nicht öffentlich zugegriffen werden kann. DMS-Replikations-Instances können vertrauliche Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.13.2	Verwenden Sie Architekturdesigns, Softwareentwicklungstechniken und Prinzipien der Systemtechnik, die eine effektive Informationssicherheit innerhalb von Organisationssystemen fördern.	dynamodb-autoscaling-enabled	Amazon DynamoDB Auto Scaling verwendet den AWS Application Auto Scaling-Service, um die bereitgestellte Durchsatzkapazität so anzupassen, dass sie automatisch auf tatsächliche Verkehrsmuster reagiert. Auf diese Weise kann eine Tabelle oder ein globaler sekundärer Index die bereitgestellte Lese-/Schreibkapazität erhöhen, um plötzliche Erhöhungen des Datenverkehrs ohne Drosselung zu bewältigen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.13.2	Verwenden Sie Architekturdesigns, Softwareentwicklungstechniken und Prinzipien der Systemtechnik, die eine effektive Informationssicherheit innerhalb von Organisationssystemen fördern.	dynamodb-pitr-enabled	Aktivieren Sie diese Regel, um zu überprüfen, ob die Informationen gesichert wurden. Es verwaltet auch die Backups, indem es sicherstellt, dass die point-in-time Wiederherstellung in Amazon DynamoDB aktiviert ist. Bei der Wiederherstellung werden fortlaufende Backups Ihrer Tabelle für die letzten 35 Tage gespeichert.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.13.2	Verwenden Sie Architekturdesigns, Softwareentwicklungstechniken und Prinzipien der Systemtechnik, die eine effektive Informationssicherheit innerhalb von Organisationssystemen fördern.	dynamodb-throughput-limit-check	Aktivieren Sie diese Regel, um sicherzustellen, dass die bereitgestellte Durchsatzkapazität in Ihren Amazon-DynamoDB-Tabellen überprüft wird. Dies ist der Umfang der Lese- und Schreibaktivitäten, der von den jeweiligen Tabellen unterstützt werden kann. DynamoDB verwendet diese Informationen für das Reservieren ausreichender Systemressourcen, um Ihren Durchsatz anforderungen gerecht zu werden. Diese Regel generiert eine Warnung, wenn sich der Durchsatz dem Höchstlimit für ein Kundenkonto nähert. Mit dieser Regel können Sie optional die Parameter RCUThreshold Kontoprozentsatz

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			(Konfigurationsstandard: 80) und WCUThreshold Kontoprozentsatz (Konfigurationsstandard: 80) festlegen. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.
3.13.2	Verwenden Sie Architekturdesigns, Softwareentwicklungstechniken und Prinzipien der Systemtechnik, die eine effektive Informationssicherheit innerhalb von Organisationssystemen fördern.	ebs-optimized-instance	Eine optimierte Instance im Amazon Elastic Block Store (Amazon EBS) bietet zusätzliche, dedizierte Kapazität für Amazon-EBS-I/O-Vorgänge. Diese Optimierung bietet die beste Leistung für Ihr EBS-Volume, indem Konflikte zwischen Amazon-EBS-I/O und anderem Datenverkehr von Ihrer Instance minimiert werden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.13,2	Verwenden Sie Architekturdesigns, Softwareentwicklungstechniken und Prinzipien der Systemtechnik, die eine effektive Informationssicherheit innerhalb von Organisationssystemen fördern.	ebs-snapshot-public-restorable-überprüfen	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass EBS-Snapshots nicht öffentlich wiederherstellbar sind. EBS-Volume-Snapshots können vertrauliche Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.
3.13.2	Verwenden Sie Architekturdesigns, Softwareentwicklungstechniken und Prinzipien der Systemtechnik, die eine effektive Informationssicherheit innerhalb von Organisationssystemen fördern.	ec-2 instance-no-public-ip	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon Elastic Compute Cloud (Amazon EC2) - Instances nicht öffentlich zugänglich sind. EC2 Amazon-Instances können vertrauliche Informationen enthalten, und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.13.2	Verwenden Sie Architekturdesigns, Softwareentwicklungstechniken und Prinzipien der Systemtechnik, die eine effektive Informationssicherheit innerhalb von Organisationssystemen fördern.	elasticache-redis-cluster-automatic-Backup-Check	Wenn automatische Backups aktiviert sind, ElastiCache erstellt Amazon täglich ein Backup des Clusters. Die Sicherung kann für eine von Ihrer Organisation festgelegte Anzahl von Tagen aufbewahrt werden. Automatische Backups schützen vor Datenverlust. Bei einem Ausfall können Sie einen neuen Cluster erstellen, der Ihre Daten aus dem aktuellen Backup wiederherstellt.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.13.2	Verwenden Sie Architekturdesigns, Softwareentwicklungstechniken und Prinzipien der Systemtechnik, die eine effektive Informationssicherheit innerhalb von Organisationssystemen fördern.	elasticsearch-in-vpc-only	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass sich Amazon OpenSearch OpenSearch Service (Service) - Domains innerhalb einer Amazon Virtual Private Cloud (Amazon VPC) befinden. Eine OpenSearch Service-Domain innerhalb einer Amazon VPC ermöglicht die sichere Kommunikation zwischen OpenSearch Service und anderen Services innerhalb der Amazon VPC, ohne dass ein Internet-Gateway, ein NAT-Gerät oder eine VPN-Verbindung erforderlich ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.13.2	Verwenden Sie Architekturdesigns, Softwareentwicklungstechniken und Prinzipien der Systemtechnik, die eine effektive Informationssicherheit innerhalb von Organisationssystemen fördern.	elb-deletion-protection-enabled	Diese Regel sorgt dafür, dass der Löschschutz für Elastic Load Balancing aktiviert ist. Verwenden Sie diese Funktion, um zu verhindern, dass Ihr Load Balancer versehentlich oder böswillig gelöscht wird, was zum Verlust der Verfügbarkeit Ihrer Anwendungen führen kann.
3.13,2	Verwenden Sie Architekturdesigns, Softwareentwicklungstechniken und Prinzipien der Systemtechnik, die eine effektive Informationssicherheit innerhalb von Organisationssystemen fördern.	emr-master-no-public-ip	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon EMR-Cluster-Masterknoten nicht öffentlich zugänglich sind. Amazon-EMR-Cluster-Hauptknoten können vertrauliche Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.13.2	Verwenden Sie Architekturdesigns, Softwareentwicklungstechniken und Prinzipien der Systemtechnik, die eine effektive Informationssicherheit innerhalb von Organisationssystemen fördern.	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) Security Groups können bei der Verwaltung des Netzwerkzugriffs helfen, indem sie eine statusbehaftete Filterung von eingehendem und ausgehendem Netzwerkverkehr zu Ressourcen bereitstellen. AWS Wenn Sie eingehenden (oder entfernten) Datenverkehr von 0.0.0.0/0 bis Port 22 auf Ihren Ressourcen nicht zulassen, können Sie den Remote-Zugriff einschränken.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.13.2	Verwenden Sie Architekturdesigns, Softwareentwicklungstechniken und Prinzipien der Systemtechnik, die eine effektive Informationssicherheit innerhalb von Organisationssystemen fördern.	lambda-function-public-access-verboten	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass AWS Lambda-Funktionen nicht öffentlich zugänglich sind. Der öffentliche Zugriff kann möglicherweise die Verfügbarkeit von Ressourcen beeinträchtigen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.13.2	Verwenden Sie Architekturdesigns, Softwareentwicklungstechniken und Prinzipien der Systemtechnik, die eine effektive Informationssicherheit innerhalb von Organisationssystemen fördern.	lambda-inside-vpc	Stellen Sie AWS Lambda-Funktionen in einer Amazon Virtual Private Cloud (Amazon VPC) bereit, um eine sichere Kommunikation zwischen einer Funktion und anderen Diensten innerhalb der Amazon VPC zu gewährleisten. Bei dieser Konfiguration sind kein Internet-Gateway, kein NAT-Gerät und keine VPN-Verbindung erforderlich. Der gesamte Datenverkehr bleibt sicher in der Cloud. AWS Domains, die sich innerhalb einer VPC befinden, verfügen aufgrund ihrer logischen Isolierung im Vergleich zu Domains mit öffentlichen Endpunkten über eine zusätzliche Sicherheitsebene. Um den Zugriff ordnungsgemäß zu verwalten,

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			sollten AWS Lambda-Funktionen einer VPC zugewiesen werden.
3.13.2	Verwenden Sie Architekturdesigns, Softwareentwicklungstechniken und Prinzipien der Systemtechnik, die eine effektive Informationssicherheit innerhalb von Organisationssystemen fördern.	opensearch-access-control-enabled	Stellen Sie sicher, dass eine differenzierte Zugriffskontrolle für Ihre Amazon OpenSearch Service-Domains aktiviert ist. Eine differenzierte Zugriffskontrolle bietet erweiterte Autorisierungsmechanismen, um den Zugriff auf Amazon Service-Domains mit den geringsten Rechten zu erreichen. OpenSearch Es ermöglicht eine rollenbasierte Zugriffskontrolle auf die Domain sowie Sicherheit auf Index-, Dokument- und Feldebene, Unterstützung für OpenSearch Service-Dashboards, Mehrmandantenfähigkeit und HTTP-Basisauthentifizierung für Service und Kibana. OpenSearch

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.13.2	Verwenden Sie Architekturdesigns, Softwareentwicklungstechniken und Prinzipien der Systemtechnik, die eine effektive Informationssicherheit innerhalb von Organisationssystemen fördern.	opensearch-in-vpc-only	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass sich Amazon OpenSearch Service-Domains innerhalb einer Amazon Virtual Private Cloud (Amazon VPC) befinden. Eine Amazon OpenSearch Service-Domain innerhalb einer Amazon VPC ermöglicht die sichere Kommunikation zwischen Amazon OpenSearch Service und anderen Services innerhalb der Amazon VPC, ohne dass ein Internet-Gateway, ein NAT-Gerät oder eine VPN-Verbindung erforderlich ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.13.2	Verwenden Sie Architekturdesigns, Softwareentwicklungstechniken und Prinzipien der Systemtechnik, die eine effektive Informationssicherheit innerhalb von Organisationssystemen fördern.	rds-instance-public-access-überprüfen	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Relational Database Service (Amazon RDS) -Instances nicht öffentlich sind. Amazon-RDS-Datenbank-Instances können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.13.2	Verwenden Sie Architekturdesigns, Softwareentwicklungstechniken und Prinzipien der Systemtechnik, die eine effektive Informationssicherheit innerhalb von Organisationssystemen fördern.	rds-multi-az-support	Die Multi-AZ-Unterstützung in Amazon Relational Database Service (Amazon RDS) bietet eine verbesserte Verfügbarkeit und Beständigkeit von Datenbank-Instances. Wenn Sie eine Multi-AZ-Datenbank-Instance bereitstellen, erstellt Amazon RDS automatisch eine primäre Datenbank-Instance und repliziert die Daten synchron auf eine Standby-Instance in einer anderen Availability Zone. Jede Availability Zone läuft auf einer eigenen, physisch getrennten, unabhängigen Infrastruktur und ist auf eine hohe Verfügbarkeit ausgelegt. Im Falle eines Infrastrukturausfalls führt Amazon RDS einen automatis

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			chen Failover zum Standby-Modus durch, sodass Sie den Datenbankbetrieb wieder aufnehmen können, sobald der Failover abgeschlo ssen ist.
3.13,2	Verwenden Sie Architekturdesigns, Softwareentwicklun gstechniken und Prinzipien der Systemtechnik, die eine effektive Informationssicher heit innerhalb von Organisationssyste men fördern.	rds-snapshots-public-prohibited	Verwalten Sie den Zugriff auf Ressource n in der AWS Cloud, indem Sie sicherste llen, dass Amazon Relational Database Service (Amazon RDS) -Instance s nicht öffentlic h sind. Amazon-RDS-Datenbank-Instances können vertrauliche Informati onen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.13.2	Verwenden Sie Architekturdesigns, Softwareentwicklungstechniken und Prinzipien der Systemtechnik, die eine effektive Informationssicherheit innerhalb von Organisationssystemen fördern.	redshift-cluster-public-access-überprüfen	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Redshift Redshift-Cluster nicht öffentlich sind. Amazon-Redshift-Cluster können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.13.2	Verwenden Sie Architekturdesigns, Softwareentwicklungstechniken und Prinzipien der Systemtechnik, die eine effektive Informationssicherheit innerhalb von Organisationssystemen fördern.	restricted-common-ports	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass gemeinsame Ports für Amazon Elastic Compute Cloud (Amazon EC2) -Sicherheitsgruppen eingeschränkt sind. Wenn der Zugriff auf Ports nicht auf vertrauenswürdige Quellen beschränkt wird, kann dies zu Angriffen auf die Verfügbarkeit, Integrität und Vertraulichkeit von Systemen führen. Mit dieser Regel können Sie optional die Parameter blockedPort1–blockedPort5 festlegen (Standardkonfigurationen: 20, 21, 3389, 3306, 4333). Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.13.2	Verwenden Sie Architekturdesigns, Softwareentwicklungstechniken und Prinzipien der Systemtechnik, die eine effektive Informationssicherheit innerhalb von Organisationssystemen fördern.	s3-Blöcke-periodisch account-level-public-access	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Simple Storage Service (Amazon S3) -Buckets nicht öffentlich zugänglich sind. Diese Regel trägt dazu bei, sensible Daten vor unbefugten Remote-Benutzern zu schützen, indem sie den öffentlichen Zugriff verhindert. Mit dieser Regel können Sie optional die Parameter ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) und restrictPublicBuckets Parameter (Config Default: True) festlegen. Die tatsächlichen Werte müssen den Richtlini

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			en Ihrer Organisation entsprechen.
3.13.2	Verwenden Sie Architekturdesigns, Softwareentwicklungstechniken und Prinzipien der Systemtechnik, die eine effektive Informationssicherheit innerhalb von Organisationssystemen fördern.	s3- verboten bucket-level-public-access	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Simple Storage Service (Amazon S3) -Buckets nicht öffentlich zugänglich sind. Diese Regel trägt dazu bei, sensible Daten vor unbefugten Remote-Benutzern zu schützen, indem sie den öffentlichen Zugriff auf Bucket-Ebene verhindert.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.13.2	Verwenden Sie Architekturdesigns, Softwareentwicklungstechniken und Prinzipien der Systemtechnik, die eine effektive Informationssicherheit innerhalb von Organisationssystemen fördern.	s-3 bucket-public-read-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie nur autorisierten Benutzern, Prozessen und Geräten Zugriff auf Amazon Simple Storage Service (Amazon S3) - Buckets gewähren. Die Verwaltung des Zugriffs sollte mit der Klassifizierung der Daten übereinstimmen.
3.13.2	Verwenden Sie Architekturdesigns, Softwareentwicklungstechniken und Prinzipien der Systemtechnik, die eine effektive Informationssicherheit innerhalb von Organisationssystemen fördern.	s-3 bucket-public-write-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie nur autorisierten Benutzern, Prozessen und Geräten Zugriff auf Amazon Simple Storage Service (Amazon S3) - Buckets gewähren. Die Verwaltung des Zugriffs sollte mit der Klassifizierung der Daten übereinstimmen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.13.2	Verwenden Sie Architekturdesigns, Softwareentwicklungstechniken und Prinzipien der Systemtechnik, die eine effektive Informationssicherheit innerhalb von Organisationssystemen fördern.	s-3 bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) unterstützt die Aufrechterhaltung einer angemessenen Kapazität und Verfügbarkeit. CRR ermöglicht das automatische, asynchrone Kopieren von Objekten in Amazon S3 Buckets, um die Datenverfügbarkeit sicherzustellen.
3.13.2	Verwenden Sie Architekturdesigns, Softwareentwicklungstechniken und Prinzipien der Systemtechnik, die eine effektive Informationssicherheit innerhalb von Organisationssystemen fördern.	sagemaker-notebook-no-direct-Internetzugang	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass SageMaker Amazon-Notebooks keinen direkten Internetzugang zulassen. Indem Sie direkten Internetzugang blockieren, vermeiden Sie, dass unbefugte Benutzer auf sensible Daten zugreifen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.13.2	Verwenden Sie Architekturdesigns, Softwareentwicklungstechniken und Prinzipien der Systemtechnik, die eine effektive Informationssicherheit innerhalb von Organisationssystemen fördern.	subnet-auto-assign-public-ip-deaktiviert	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon Virtual Private Cloud (VPC) -Subnetzen nicht automatisch eine öffentliche IP-Adresse zugewiesen wird. Amazon Elastic Compute Cloud (EC2) -Instances, die in Subnetzen gestartet werden, in denen dieses Attribut aktiviert ist, haben ihrer primären Netzwerkschnittstelle eine öffentliche IP-Adresse zugewiesen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.13.2	Verwenden Sie Architekturdesigns, Softwareentwicklungstechniken und Prinzipien der Systemtechnik, die eine effektive Informationssicherheit innerhalb von Organisationssystemen fördern.	vpc-default-security-group-geschlossen	Sicherheitsgruppen von Amazon Elastic Compute Cloud (Amazon EC2) können bei der Verwaltung des Netzwerkzugriffs helfen, indem sie eine statusbehaftete Filterung des ein- und ausgehenden Netzwerkverkehrs zu Ressourcen bereitstellen. AWS Die Beschränkung des gesamten Datenverkehrs auf die Standardsicherheitsgruppe hilft dabei, den Fernzugriff auf Ihre Ressourcen einzuschränken. AWS

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.13.2	Verwenden Sie Architekturdesigns, Softwareentwicklungstechniken und Prinzipien der Systemtechnik, die eine effektive Informationssicherheit innerhalb von Organisationssystemen fördern.	vpc-sg-open-only-to-authorized-ports	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass gemeinsame Ports für Amazon Elastic Compute Cloud (Amazon EC2) -Sicherheitsgruppen eingeschränkt sind. Wenn der Zugriff auf Ports nicht auf vertrauenswürdige Quellen beschränkt wird, kann dies zu Angriffen auf die Verfügbarkeit, Integrität und Vertraulichkeit von Systemen führen. Durch die Beschränkung des Zugriffs auf Ressourcen innerhalb einer Sicherheitsgruppe aus dem Internet (0.0.0.0/0) kann der Fernzugriff auf interne Systeme gesteuert werden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.13.6	Netzwerkverkehr standardmäßig ablehnen und Netzwerkverkehr ausnahmsweise zulassen (d. h. allen verweigern, ausnahmsweise zulassen).	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) Security Groups können bei der Verwaltung des Netzwerkzugriffs helfen, indem sie eine statusbeh aftete Filterung von eingehendem und ausgehendem Netzwerkverkehr zu Ressourcen bereitste llen. AWS Wenn Sie eingehenden (oder entfernten) Datenverk ehr von 0.0.0.0/0 bis Port 22 auf Ihren Ressourcen nicht zulassen, können Sie den Remote-Zugriff einschränken.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.13.6	Netzwerkverkehr standardmäßig ablehnen und Netzwerkverkehr ausnahmsweise zulassen (d. h. allen verweigern, ausnahmsweise zulassen).	restricted-common-ports	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass gemeinsame Ports für Amazon Elastic Compute Cloud (Amazon EC2) -Sicherheitsgruppen eingeschränkt sind. Wenn der Zugriff auf Ports nicht auf vertrauenswürdige Quellen beschränkt wird, kann dies zu Angriffen auf die Verfügbarkeit, Integrität und Vertraulichkeit von Systemen führen. Mit dieser Regel können Sie optional die Parameter blockedPort1–blockedPort5 festlegen (Standardkonfigurationen: 20, 21, 3389, 3306, 4333). Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.13.6	Netzwerkverkehr standardmäßig ablehnen und Netzwerkverkehr ausnahmsweise zulassen (d. h. allen verweigern, ausnahmsweise zulassen).	vpc-sg-open-only-to-authorized-ports	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass gemeinsame Ports für Amazon Elastic Compute Cloud (Amazon EC2) -Sicherheitsgruppen eingeschränkt sind. Wenn der Zugriff auf Ports nicht auf vertrauenswürdige Quellen beschränkt wird, kann dies zu Angriffen auf die Verfügbarkeit, Integrität und Vertraulichkeit von Systemen führen. Durch die Beschränkung des Zugriffs auf Ressourcen innerhalb einer Sicherheitsgruppe aus dem Internet (0.0.0.0/0) kann der Fernzugriff auf interne Systeme gesteuert werden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.13.8	Implementieren Sie kryptografische Mechanismen, um die unbefugte Offenlegung von CUI während der Übertragung zu verhindern, sofern dies nicht anderweitig durch alternative physische Schutzmaßnahmen vermieden wird.	elasticsearch-node-to-node-Verschlüsselungsprüfung	Stellen Sie sicher, dass die node-to-node Verschlüsselung für Amazon OpenSearch Service aktiviert ist. Node-to-nodeVerschlüsselung ermöglicht die TLS 1.2-Verschlüsselung für die gesamte Kommunikation innerhalb der Amazon Virtual Private Cloud (Amazon VPC). Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.13.8	Implementieren Sie kryptografische Mechanismen, um die unbefugte Offenlegung von CUI während der Übertragung zu verhindern, sofern dies nicht anderweitig durch alternative physische Schutzmaßnahmen vermieden wird.	alb-http-to-https-Umleitungsprüfung	Um Daten während der Übertragung zu schützen, stellen Sie sicher, dass Ihr Application Load Balancer unverschlüsselte HTTP-Anfragen automatisch an HTTPS umleitet. Da sensible Daten vorhanden sein können, sollten Sie die Verschlüsselung bei der Übertragung aktivieren, um diese Daten zu schützen.
3.13.8	Implementieren Sie kryptografische Mechanismen, um die unbefugte Offenlegung von CUI während der Übertragung zu verhindern, sofern dies nicht anderweitig durch alternative physische Schutzmaßnahmen vermieden wird.	api-gw-ssl-enabled	Stellen Sie sicher, dass die REST-API-Stufen von Amazon API Gateway mit SSL-Zertifikaten konfiguriert sind, damit Backend-Systeme überprüfen können, ob Anforderungen von API Gateway stammen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.13,8	Implementieren Sie kryptografische Mechanismen, um die unbefugte Offenlegung von CUI während der Übertragung zu verhindern, sofern dies nicht anderweitig durch alternative physische Schutzmaßnahmen vermieden wird.	elb-acm-certificate-required	Zum Schutz von eventuell vorhandenen sensiblen Daten sowie von Daten während der Übertragung muss die Verschlüsselung für Ihr Elastic Load Balancing aktiviert sein. Verwenden Sie AWS Certificate Manager, um öffentliche und private SSL/TLS-Zertifikate mit AWS Diensten und internen Ressourcen zu verwalten, bereitzustellen und bereitzustellen.
3.13.8	Implementieren Sie kryptografische Mechanismen, um die unbefugte Offenlegung von CUI während der Übertragung zu verhindern, sofern dies nicht anderweitig durch alternative physische Schutzmaßnahmen vermieden wird.	opensearch-https-required	Da sensible Daten existieren können und um Daten während der Übertragung zu schützen, sollten Sie sicherstellen, dass HTTPS für Verbindungen zu Ihren Amazon OpenSearch Service-Domains aktiviert ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.13.8	Implementieren Sie kryptografische Mechanismen, um die unbefugte Offenlegung von CUI während der Übertragung zu verhindern, sofern dies nicht anderweitig durch alternative physische Schutzmaßnahmen vermieden wird.	opensearch-node-to-node-Verschlüsselungsprüfung	Stellen Sie sicher, dass die node-to-node Verschlüsselung für Amazon OpenSearch Service aktiviert ist. Node-to-nodeVerschlüsselung ermöglicht die TLS 1.2-Verschlüsselung für die gesamte Kommunikation innerhalb der Amazon Virtual Private Cloud (Amazon VPC). Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.13.8	Implementieren Sie kryptografische Mechanismen, um die unbefugte Offenlegung von CUI während der Übertragung zu verhindern, sofern dies nicht anderweitig durch alternative physische Schutzmaßnahmen vermieden wird.	redshift-require-tls-ssl	Stellen Sie sicher, dass Ihre Amazon-Redshift-Cluster eine TLS/SSL-Verschlüsselung erfordern, um eine Verbindung zu SQL-Clients herzustellen. Da sensible Daten vorhanden sein können, sollten Sie die Verschlüsselung bei der Übertragung aktivieren, um diese Daten zu schützen.
3.13,8	Implementieren Sie kryptografische Mechanismen, um die unbefugte Offenlegung von CUI während der Übertragung zu verhindern, sofern dies nicht anderweitig durch alternative physische Schutzmaßnahmen vermieden wird.	s-3 bucket-ssl-requests-only	Um Daten während der Übertragung zu schützen, stellen Sie sicher, dass Ihre Amazon Simple Storage Service (Amazon S3)-Buckets Anfragen zur Verwendung von Secure Socket Layer (SSL)-Buckets erfordern. Da sensible Daten vorhanden sein können, sollten Sie die Verschlüsselung bei der Übertragung aktivieren, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.13,10	Etablieren und verwalten Sie kryptografische Schlüssel für die in Organisationssysteme eingesetzte Kryptografie.	cmk-backing-key-rotation-aktiviert	Aktivieren Sie die Schlüsselrotation, um sicherzustellen, dass Schlüssel rotiert werden, nachdem sie das Ende ihrer Krypto-Periode erreicht haben.
3.13.10	Etablieren und verwalten Sie kryptografische Schlüssel für die in Organisationssysteme eingesetzte Kryptografie.	kms-cmk-not-scheduled-zum Löschen	Um Daten im Ruhezustand zu schützen, sollten Sie sicherstellen, dass die für den Kunden erforderlichen Masterschlüssel (CMKs) nicht im AWS Key Management Service (AWS KMS) gelöscht werden. Da Schlüssel manchmal gelöscht werden müssen, können Sie mit dieser Regel alle zu löschenden Schlüssel überprüfen, falls ein Schlüssel versehentlich zur Löschung vorgemerkt wurde.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.13.16	Schützen Sie die Vertraulichkeit von CUI im Ruhezustand.	dynamodb-table-encrypted-kms	Stellen Sie sicher, dass die Verschlüsselung für Ihre Amazon-DynamoDB-Tabellen aktiviert ist. Um eventuell vorhandene sensible Daten im Ruhezustand in diesen Tabellen zu schützen, müssen Sie die Verschlüsselung von Daten im Ruhezustand aktivieren. Standardmäßig werden DynamoDB-Tabellen mit einem AWS eigenen Kundenhauptschlüssel (CMK) verschlüselt.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.13.16	Schützen Sie die Vertraulichkeit von CUI im Ruhezustand.	ec-2 ebs-encryption-by-default	Zum Schutz von Daten im Ruhezustand müssen Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon Elastic Block Store (Amazon EBS)-Volumes aktiviert ist. Da sensible Daten in diesen Volumes gespeichert werden können, sollten Sie die Verschlüsselung von Daten im Ruhezustand aktivieren, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.13,16	Schützen Sie die Vertraulichkeit von CUI im Ruhezustand.	rds-snapshot-encrypted	Stellen Sie sicher, dass die Verschlüsselung für Ihre Amazon Relational Database Service (Amazon RDS)-Snapshots aktiviert ist. Da sensible Daten auch im Ruhezustand vorhanden sein können, sollten Sie die Verschlüsselung von Daten im Ruhezustand aktivieren, um diese Daten zu schützen.
3.13,16	Schützen Sie die Vertraulichkeit von CUI im Ruhezustand.	s-3 bucket-default-lock-enabled	Stellen Sie sicher, dass für Ihren Amazon Simple Storage Service (Amazon S3)-Bucket standardmäßig eine Sperre aktiviert ist. Zum Schutz eventuell vorhandener sensibler Daten in S3 Buckets müssen Sie Objektsperren für Daten im Ruhezustand erzwingen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.13,16	Schützen Sie die Vertraulichkeit von CUI im Ruhezustand.	sagemaker-notebook-instance-kms-key-konfiguriert	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass die Verschlüsselung mit dem AWS Key Management Service (AWS KMS) für Ihr Notebook aktiviert ist. SageMaker Da vertrauliche Daten im SageMaker Notebook gespeichert werden können, sollten Sie die Verschlüsselung im Ruhezustand aktivieren, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.13.16	Schützen Sie die Vertraulichkeit von CUI im Ruhezustand.	sns-encrypted-kms	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass Ihre Amazon Simple Notification Service (Amazon SNS) -Themen mit dem AWS Key Management Service (AWS KMS) verschlüsselt werden müssen. Um eventuell vorhandene sensible Daten im Ruhezustand in veröffentlichten Nachrichten zu schützen, muss die Verschlüsselung von Daten im Ruhezustand aktiviert sein.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.13.16	Schützen Sie die Vertraulichkeit von CUI im Ruhezustand.	api-gw-cache-enabled-und-verschlüsselt	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass die Verschlüsselung für den Cache Ihrer API-Gateway-Stufe aktiviert ist. Da für die API-Methode sensible Daten erfasst werden können, sollten Sie die Verschlüsselung von Daten im Ruhezustand aktivieren, um diese Daten zu schützen.
3.13.16	Schützen Sie die Vertraulichkeit von CUI im Ruhezustand.	cloud-trail-encryption-enabled	Da sensible Daten vorhanden sein können und um Daten im Ruhezustand zu schützen, sollten Sie sicherstellen, dass die Verschlüsselung für Ihre AWS CloudTrail Trails aktiviert ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.13.16	Schützen Sie die Vertraulichkeit von CUI im Ruhezustand.	cloudwatch-log-group-encrypted	Um sensible Daten im Speicher zu schützen, stellen Sie sicher, dass die Verschlüs selung für Ihre Amazon CloudWatch Log Groups aktiviert ist.
3.13.16	Schützen Sie die Vertraulichkeit von CUI im Ruhezustand.	efs-encrypted-check	Aktivieren Sie die Verschlüsselung für Ihr Amazon Elastic File System (EFS), um eventuell vorhandene sensible Daten sowie Daten im Ruhezustand zu schützen.
3.13,16	Schützen Sie die Vertraulichkeit von CUI im Ruhezustand.	elasticsearch-encrypted-at-rest	Da sensible Daten vorhanden sein können und um Daten im Ruhezustand zu schützen, sollten Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon OpenSearch Service (OpenSearch Service) -Domains aktiviert ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.13.16	Schützen Sie die Vertraulichkeit von CUI im Ruhezustand.	encrypted-volumes	Aktivieren Sie die Verschlüsselung für Ihre Amazon-Elastic-Block-Store-(Amazon-EBS-)Volumes, um eventuell vorhandene sensible Daten sowie Daten im Ruhezustand zu schützen.
3.13,16	Schützen Sie die Vertraulichkeit von CUI im Ruhezustand.	kms-cmk-not-scheduled-zum Löschen	Um Daten im Ruhezustand zu schützen, sollten Sie sicherstellen, dass die für den Kunden erforderlichen Masterschlüssel (CMKs) nicht im AWS Key Management Service (AWS KMS) gelöscht werden. Da Schlüssel manchmal gelöscht werden müssen, können Sie mit dieser Regel alle zu löschenden Schlüssel überprüfen, falls ein Schlüssel versehentlich zur Löschung vorgemerkt wurde.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.13.16	Schützen Sie die Vertraulichkeit von CUI im Ruhezustand.	opensearch-encrypted-at-rest	Da sensible Daten vorhanden sein können und um Daten im Ruhezustand zu schützen, sollten Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon OpenSearch Service-Domains aktiviert ist.
3.13.16	Schützen Sie die Vertraulichkeit von CUI im Ruhezustand.	rds-storage-encrypted	Zum Schutz von Daten im Ruhezustand müssen Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon Relational Database Service (Amazon RDS)-Instances aktiviert ist. Da sensible Daten in Amazon-RDS-Instances gespeichert werden können, sollten Sie die Verschlüsselung von Daten im Ruhezustand aktivieren, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.13,16	Schützen Sie die Vertraulichkeit von CUI im Ruhezustand.	redshift-cluster-configuration-check	Um Daten im Ruhezustand zu schützen, muss die Verschlüsselung für Ihre Amazon-Redshift-Cluster aktiviert sein. Sie müssen auch sicherstellen, dass die erforderlichen Konfigurationen auf Amazon-Redshift-Clustern bereitgestellt werden. Die Prüfungsprotokollierung muss aktiviert sein, um Informationen zu Verbindungen und Benutzeraktivitäten in der Datenbank bereitzustellen. Diese Regel erfordert, dass ein Wert für clusterDbEncrypted (Config Default: TRUE) und LoggingEnabled (Config Default: TRUE) gesetzt ist. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.13.16	Schützen Sie die Vertraulichkeit von CUI im Ruhezustand.	s3-fähig bucket-server-side-encryption	Zum Schutz von Daten im Ruhezustand müssen Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon Simple Storage Service (Amazon S3)-Buckets aktiviert ist. Da sensible Daten in Amazon S3 Buckets gespeichert werden können, sollten Sie die Verschlüsselung aktivieren, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.13.16	Schützen Sie die Vertraulichkeit von CUI im Ruhezustand.	sagemaker-endpoint-configuration-kms-key-konfiguriert	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass die Verschlüsselung mit dem AWS Key Management Service (AWS KMS) für Ihren Endpunkt aktiviert ist. SageMaker Da sensible Daten auf dem SageMaker Endgerät gespeiche rt werden können, sollten Sie die Verschlüsselung im Ruhezustand aktiviere n, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.14.1	Identifizieren, melden und korrigieren Sie Fehler in Informati onen und Systemen rechtzeitig.	securityhub-enabled	AWS Security Hub hilft bei der Überwachung von unbefugtem Personal, Verbindun gen, Geräten und Software. AWS Security Hub aggregiert, organisie rt und priorisie rt die Sicherhei tswarnungen oder Ergebnisse mehrerer Dienste. AWS Einige dieser Dienste sind Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer und AWS Firewall Manager sowie AWS Partnerlösungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.14.1	Identifizieren, melden und korrigieren Sie Fehler in Informati onen und Systemen rechtzeitig.	guardduty-enabled-centralized	Amazon GuardDuty kann mithilfe von Threat Intellige nce Feeds helfen, potenzielle Cybersich erheitsereignisse zu überwachen und zu erkennen. Dazu gehören Listen mit bösartigen IPs und maschinel len Lernmethoden zur Identifizierung unerwarteter, nicht autorisierter und bösartiger Aktivitäten in Ihrer AWS Cloud-Umgebung.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.14.2	Richten Sie Sicherheitsvorkehrungen zum Schutz vor schädlichem Code an geeigneten Stellen innerhalb der Systeme der Organisation ein.	securityhub-enabled	AWS Security Hub hilft bei der Überwachung von unbefugtem Personal, Verbindungen, Geräten und Software. AWS Security Hub aggregiert, organisiert und priorisiert die Sicherheitswarnungen oder Ergebnisse mehrerer Dienste. AWS Einige dieser Dienste sind Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer und AWS Firewall Manager sowie AWS Partnerlösungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.14.2	Richten Sie Sicherheitsvorkehrungen zum Schutz vor schädlichem Code an geeigneten Stellen innerhalb der Systeme der Organisation ein.	guardduty-enabled-centralized	Amazon GuardDuty kann mithilfe von Threat Intelligence Feeds helfen, potenzielle Cybersicherheitsereignisse zu überwachen und zu erkennen. Dazu gehören Listen mit bösartigen IPs und maschinellen Lernmethoden zur Identifizierung unerwarteter, nicht autorisierter und bösartiger Aktivitäten in Ihrer AWS Cloud-Umgebung.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.14.3	Überwachen Sie die Warnmeldungen und Hinweise zur Systemsicherheit und ergreifen Sie entsprechende Maßnahmen.	securityhub-enabled	AWS Security Hub hilft bei der Überwachung von unbefugtem Personal, Verbindungen, Geräten und Software. AWS Security Hub aggregiert, organisiert und priorisiert die Sicherheitswarnungen oder Ergebnisse mehrerer Dienste. AWS Einige dieser Dienste sind Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer und AWS Firewall Manager sowie AWS Partnerlösungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.14.3	Überwachen Sie die Warnmeldungen und Hinweise zur Systemsicherheit und ergreifen Sie entsprechende Maßnahmen.	ec2-prüfen managedinstance-patch-compliance-status	Aktivieren Sie diese Regel, um bei der Identifizierung und Dokumentation von Sicherheitslücken in Amazon Elastic Compute Cloud (Amazon EC2) zu helfen. Die Regel prüft, ob die EC2 Amazon-Instance die Patch-Konformität im AWS Systems Manager gemäß den Richtlinien und Verfahren Ihrer Organisation einhält.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.14.3	Überwachen Sie die Warnmeldungen und Hinweise zur Systemsicherheit und ergreifen Sie entsprechende Maßnahmen.	elastic-beanstalk-managed-updates-aktiviert	Durch die Aktivierung verwalteter Plattform updates für eine Amazon-Elastic-Beanstalk-Umgebung wird sichergestellt, dass die aktuellen verfügbaren Plattform -Fixes, -Updates und -Features für die Umgebung installiert sind. Eine bewährte Methode zur Sicherung von Systemen besteht darin, stets die aktuellen Patches zu installieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.14.3	Überwachen Sie die Warnmeldungen und Hinweise zur Systemsicherheit und ergreifen Sie entsprechende Maßnahmen.	guardduty-enabled-centralized	Amazon GuardDuty kann mithilfe von Threat Intellige nce Feeds helfen, potenzielle Cybersich erheitsereignisse zu überwachen und zu erkennen. Dazu gehören Listen mit bösartigen IPs und maschinel len Lernmethoden zur Identifizierung unerwarteter, nicht autorisierter und bösartiger Aktivitäten in Ihrer AWS Cloud-Umgebung.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.14.3	Überwachen Sie die Warnmeldungen und Hinweise zur Systemsicherheit und ergreifen Sie entsprechende Maßnahmen.	redshift-cluster-maintenancesettings-check	Diese Regel stellt sicher, dass Amazon-Redshift-Cluster die bevorzugten Einstellungen für Ihre Organisation haben. Insbesondere sorgt sie dafür, dass Cluster bevorzugte Wartungsfenster und automatisierte Aufbewahrungsfristen für Snapshots für die Datenbank haben. Für diese Regel müssen Sie die festlegen. allowVersionUpgrade Der Standardwert ist „true“. Außerdem können Sie optional den Zeitraum preferredMaintenanceWindow (der Standardwert ist sa: 16:00 -sa: 16:30) und den automated SnapshotRetention Zeitraum (der Standardwert ist 1) festlegen. Die tatsächlichen Werte müssen den Richtlini

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			en Ihrer Organisation entsprechen.
3.14.4	Aktualisieren Sie die Schutzmechanismen gegen bösartigen Code, wenn neue Versionen verfügbar sind.	guardduty-enabled-centralized	Amazon GuardDuty kann mithilfe von Threat Intellige nce Feeds helfen, potenzielle Cybersich erheitsereignisse zu überwachen und zu erkennen. Dazu gehören Listen mit bösartigen IPs und maschinel len Lernmethoden zur Identifizierung unerwarteter, nicht autorisierter und bösartiger Aktivitäten in Ihrer AWS Cloud-Umgebung.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.14.6	Überwachen Sie die Organisationssysteme, einschließlich eingehenden und ausgehenden Kommunikationsverkehrs, um Angriffe und Hinweise für potenzielle Angriffe zu erkennen.	alb-waf-enabled	Stellen Sie sicher, dass AWS WAF auf Elastic Load Balancers (ELB) aktiviert ist, um Webanwendungen zu schützen. Eine WAF trägt zum Schutz Ihrer Webanwendungen oder APIs vor gängigen Web-Exploits bei. Diese Web-Exploits können sich auf die Verfügbarkeit auswirken, die Sicherheit gefährden oder übermäßige Ressourcen in Ihrer Umgebung verbrauchen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.14.6	Überwachen Sie die Organisationssysteme, einschließlich eingehenden und ausgehenden Kommunikationsverkehrs, um Angriffe und Hinweise für potenzielle Angriffe zu erkennen.	api-gw-associated-with-WAF	AWS Mit WAF können Sie eine Reihe von Regeln (als Web Access Control List (Web ACL) bezeichnet) konfigurieren, die Webanfragen auf der Grundlage von anpassbaren Websicherheitsregeln und -bedingungen, die Sie definieren, zulassen, blockieren oder zählen. Stellen Sie sicher, dass Ihre Amazon-API-Gateway-Stufe mit einer WAF-Web-ACL verknüpft ist, um sie vor böswilligen Angriffen zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.14.6	Überwachen Sie die Organisationssysteme, einschließlich eingehenden und ausgehenden Kommunikationsverkehrs, um Angriffe und Hinweise für potenzielle Angriffe zu erkennen.	multi-region-cloudtrail-enabled	AWS CloudTrail zeichnet Aktionen und API-Aufrufe der AWS Management Console auf. Sie können feststellen, welche Benutzer und Konten angerufen wurden AWS, von welcher Quell-IP-Adresse aus die Anrufe getätigt wurden und wann die Anrufe erfolgten. CloudTrail übermittelt Protokolldateien aus allen AWS Regionen an Ihren S3-Bucket, wenn MULTI_REGION_CLOUD_TRAIL_ENABLED aktiviert ist. Außerdem wird beim AWS Start einer neuen Region derselbe Trail in der neuen Region erstellt. CloudTrail Dadurch erhalten Sie automatisch Protokolldateien mit API-Aktivitäten für die neue Region.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.14.6	Überwachen Sie die Organisationssysteme, einschließlich eingehenden und ausgehenden Kommunikationsverkehrs, um Angriffe und Hinweise für potenzielle Angriffe zu erkennen.	rds-logging-enabled	Um die Protokollierung und Überwachung in Ihrer Umgebung zu erleichtern, stellen Sie sicher, dass die Amazon Relational Database Service (Amazon RDS)-Protokollierung aktiviert ist. Mit der Amazon-RDS-Protokollierung können Sie Ereignisse wie Verbindungen, Verbindungsabbrüche, Abfragen oder abgefragte Tabellen erfassen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.14.6	Überwachen Sie die Organisationssysteme, einschließlich eingehenden und ausgehenden Kommunikationsverkehrs, um Angriffe und Hinweise für potenzielle Angriffe zu erkennen.	securityhub-enabled	AWS Security Hub hilft bei der Überwachung von unbefugtem Personal, Verbindungen, Geräten und Software. AWS Security Hub aggregiert, organisiert und priorisiert die Sicherheitswarnungen oder Ergebnisse mehrerer Dienste. AWS Einige dieser Dienste sind Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer und AWS Firewall Manager sowie AWS Partnerlösungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.14.6	Überwachen Sie die Organisationssysteme, einschließlich eingehenden und ausgehenden Kommunikationsverkehrs, um Angriffe und Hinweise für potenzielle Angriffe zu erkennen.	wafv2-logging-enabled	Um die Protokollierung und Überwachung in Ihrer Umgebung zu erleichtern, aktivieren Sie die AWS WAF (V2) -Protokollierung im regionalen und globalen Web. ACLs AWS Die WAF-Protokollierung bietet detaillierte Informationen über den Datenverkehr, der von Ihrer Web-ACL analysiert wird. In den Protokollen werden die Uhrzeit aufgezeichnet, zu der die AWS WAF die Anfrage von Ihrer AWS Ressource erhalten hat, Informationen über die Anfrage und eine Aktion für die Regel, der jede Anfrage entsprach.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.14.6	Überwachen Sie die Organisationssysteme, einschließlich eingehenden und ausgehenden Kommunikationsverkehrs, um Angriffe und Hinweise für potenzielle Angriffe zu erkennen.	api-gw-execution-logging-aktiviert	Die API-Gateway-Protokollierung zeigt detaillierte Ansichten der Benutzer, die auf die API zugegriffen haben, und wie diese Benutzer auf die API zugegriffen haben. Diese Insights ermöglichen die Einsicht in Benutzeraktivitäten.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.14.6	Überwachen Sie die Organisationssysteme, einschließlich eingehenden und ausgehenden Kommunikationsverkehrs, um Angriffe und Hinweise für potenzielle Angriffe zu erkennen.	cloudtrail-enabled	AWS CloudTrail kann durch die Aufzeichnung von Aktionen und API-Aufrufen in der AWS Management Console bei der Nichtabstreitbarkeit helfen. Sie können die Benutzer und die Benutzer AWS-Konten , die einen AWS Dienst aufgerufen haben, die Quell-IP-Adresse, über die die Aufrufe generiert wurden, und den Zeitpunkt der Anrufe identifizieren. Einzelheiten zu den erfassten Daten finden Sie unter Inhalt des AWS CloudTrail Datensatzes.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.14.6	Überwachen Sie die Organisationssysteme, einschließlich eingehenden und ausgehenden Kommunikationsverkehrs, um Angriffe und Hinweise für potenzielle Angriffe zu erkennen.	cloudtrail-s3-dataevents-enabled	Die Erfassung von Simple Storage Service (Amazon S3)-Datenereignissen unterstützt die Erkennung von ungewöhnlichen Aktivitäten. Zu den Details gehören AWS-Konto Informationen über den Zugriff auf einen Amazon S3 S3-Bucket, die IP-Adresse und die Uhrzeit des Ereignisses.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.14.6	Überwachen Sie die Organisationssysteme, einschließlich eingehenden und ausgehenden Kommunikationsverkehrs, um Angriffe und Hinweise für potenzielle Angriffe zu erkennen.	elb-logging-enabled	Die Elastic-Load-Balancing-Aktivität ist ein zentraler Kommunikationspunkt innerhalb einer Umgebung. Stellen Sie sicher, dass die ELB-Protokollierung aktiviert ist. Die gesammelten Daten enthalten detaillierte Informationen zu Anfragen, die an den ELB gesendet wurden. Jedes Protokoll enthält Informationen wie die Zeit, zu der die Anforderung einging, die Client-IP-Adresse, Latenzen, Anforderungspfade und Serverantworten.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.14.6	Überwachen Sie die Organisationssysteme, einschließlich eingehenden und ausgehenden Kommunikationsverkehrs, um Angriffe und Hinweise für potenzielle Angriffe zu erkennen.	guardduty-enabled-centralized	Amazon GuardDuty kann mithilfe von Threat Intelligence Feeds helfen, potenzielle Cybersicherheitsereignisse zu überwachen und zu erkennen. Dazu gehören Listen mit bösartigen IPs und maschinellen Lernmethoden zur Identifizierung unerwarteter, nicht autorisierter und bösartiger Aktivitäten in Ihrer AWS Cloud-Umgebung.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.14.6	Überwachen Sie die Organisationssysteme, einschließlich eingehenden und ausgehenden Kommunikationsverkehrs, um Angriffe und Hinweise für potenzielle Angriffe zu erkennen.	redshift-cluster-configuration-check	Um Daten im Ruhezustand zu schützen, muss die Verschlüsselung für Ihre Amazon-Redshift-Cluster aktiviert sein. Sie müssen auch sicherstellen, dass die erforderlichen Konfigurationen auf Amazon-Redshift-Clustern bereitgestellt werden. Die Prüfungsprotokollierung muss aktiviert sein, um Informationen zu Verbindungen und Benutzeraktivitäten in der Datenbank bereitzustellen. Diese Regel erfordert, dass ein Wert für clusterDbEncrypted (Config Default: TRUE) und LoggingEnabled (Config Default: TRUE) gesetzt ist. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.14.6	Überwachen Sie die Organisationssysteme, einschließlich eingehenden und ausgehenden Kommunikationsverkehrs, um Angriffe und Hinweise für potenzielle Angriffe zu erkennen.	s-3 bucket-logging-enabled	Die Amazon Simple Storage Service (Amazon S3)-Serverzugriffsprotokollierung bietet eine Methode zur Überwachung des Netzwerks im Hinblick auf potenzielle Cybersicherheitsereignisse. Die Ereignisse werden überwacht, indem detaillierte Aufzeichnungen über die Anfragen erfasst werden, die an einen Amazon-S3-Bucket gestellt wurden. Jeder Zugriffsprotokolleintrag enthält Details zu einer einzelnen Zugriffsanfrage. Zu den Details gehören Anforderer, Bucket-Name, Anforderungszeit, Anforderungsaktion, Antwortstatus und Fehlercode, falls relevant.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.14.6	Überwachen Sie die Organisationssysteme, einschließlich eingehenden und ausgehenden Kommunikationsverkehrs, um Angriffe und Hinweise für potenzielle Angriffe zu erkennen.	vpc-flow-logs-enabled	VPC-Flow-Protokolle erfassen detaillierte Informationsdatensätze über den IP-Datenverkehr, der zu und von Netzwerkschnittstellen in Ihrer Amazon Virtual Private Cloud (Amazon VPC) fließt. Standardmäßig enthalten Flow-Protokolldatensätze Werte für die verschiedenen Komponenten des IP-Flows, einschließlich Quelle, Ziel und Protokoll.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.14.7	Identifizieren Sie die unbefugte Nutzung von Organisat ionssystemen.	elasticsearch-logs-to-cloudwatch	Stellen Sie sicher, dass für Amazon OpenSearch Service-Domains Fehlerpro tokolle aktiviert und zur Aufbewahrung und Beantwortung an Amazon CloudWatc h Logs gestreamt werden. Domain-Fehlerprotokolle sind bei Sicherhei ts- und Zugriffsp rüfungen sowie bei der Diagnose von Verfügbarkeitsprob lemen nützlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.14.7	Identifizieren Sie die unbefugte Nutzung von Organisat ionssystemen.	multi-region-cloudtrail-enabled	AWS CloudTrail zeichnet Aktionen und API-Aufrufe der AWS Management Console auf. Sie können feststellen, welche Benutzer und Konten angerufen wurden AWS, von welcher Quell-IP-Adresse aus die Anrufe getätigt wurden und wann die Anrufe erfolgten. CloudTrail übermittelt Protokolldateien aus allen AWS Regionen an Ihren S3-Bucket , wenn MULTI_REG ION_CLOUD _TRAIL_ENABLED aktiviert ist. Außerdem wird beim AWS Start einer neuen Region derselbe Trail in der neuen Region erstellt. CloudTrail Dadurch erhalten Sie automatis ch Protokolldateien mit API-Aktivitäten für die neue Region.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.14.7	Identifizieren Sie die unbefugte Nutzung von Organisat ionssystemen.	rds-logging-enabled	Um die Protokoll ierung und Überwachung in Ihrer Umgebung zu erleichtern, stellen Sie sicher, dass die Amazon Relationa l Database Service (Amazon RDS)-Prot okollierung aktiviert ist. Mit der Amazon-RDS-Protokollierung können Sie Ereigniss e wie Verbindungen, Verbindungsabbrüch e, Abfragen oder abgefragte Tabellen erfassen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.14.7	Identifizieren Sie die unbefugte Nutzung von Organisat ionssystemen.	securityhub-enabled	AWS Security Hub hilft bei der Überwachung von unbefugtem Personal, Verbindun gen, Geräten und Software. AWS Security Hub aggregiert, organisie rt und priorisie rt die Sicherhei tswarnungen oder Ergebnisse mehrerer Dienste. AWS Einige dieser Dienste sind Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer und AWS Firewall Manager sowie AWS Partnerlösungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.14.7	Identifizieren Sie die unbefugte Nutzung von Organisat ionssystemen.	wafv2-logging-enab led	Um die Protokoll ierung und Überwachung in Ihrer Umgebung zu erleichtern, aktiviere n Sie die AWS WAF (V2) -Protokollierung im regionalen und globalen Web. ACLs AWS Die WAF-Protokollierung bietet detaillierte Informationen über den Datenverkehr, der von Ihrer Web-ACL analysiert wird. In den Protokollen werden die Uhrzeit aufgezeic hnet, zu der die AWS WAF die Anfrage von Ihrer AWS Ressource erhalten hat, Informati onen über die Anfrage und eine Aktion für die Regel, der jede Anfrage entsprach.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.14.7	Identifizieren Sie die unbefugte Nutzung von Organisat ionssystemen.	api-gw-execution-l ogging-aktiviert	Die API-Gateway-Protokollierung zeigt detaillierte Ansichten der Benutzer, die auf die API zugegriff en haben, und wie diese Benutzer auf die API zugegriffen haben. Diese Insights ermöglichen die Einsicht in Benutzera ktivitäten.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.14.7	Identifizieren Sie die unbefugte Nutzung von Organisat ionssystemen.	cloudtrail-enabled	AWS CloudTrai l kann durch die Aufzeichnung von Aktionen und API-Aufrufen in der AWS Management Console bei der Nichtabst reitbarkeit helfen. Sie können die Benutzer und die Benutzer AWS-Konten , die einen AWS Dienst aufgerufen haben, die Quell-IP-Adresse, über die die Aufrufe generiert wurden, und den Zeitpunkt der Anrufe identifiz ieren. Einzelheiten zu den erfassten Daten finden Sie unter Inhalt des AWS CloudTrail Datensatzes.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.14.7	Identifizieren Sie die unbefugte Nutzung von Organisat ionssystemen.	cloudtrail-s3-data events-enabled	Die Erfassung von Simple Storage Service (Amazon S3)-Datenereigniss en unterstützt die Erkennung von ungewöhnlichen Aktivitäten. Zu den Details gehören AWS-Konto Informationen über den Zugriff auf einen Amazon S3 S3-Bucket, die IP-Adress e und die Uhrzeit des Ereignisses.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.14.7	Identifizieren Sie die unbefugte Nutzung von Organisat ionssystemen.	elb-logging-enabled	Die Elastic-Load-Balancing-Aktivität ist ein zentraler Kommunikationspunk t innerhalb einer Umgebung. Stellen Sie sicher, dass die ELB-Protokollierun g aktiviert ist. Die gesammelten Daten enthalten detaillie rte Informationen zu Anfragen, die an den ELB gesendet wurden. Jedes Protokoll enthält Informationen wie die Zeit, zu der die Anforderung einging, die Client-IP -Adresse, Latenzen, Anforderungspfade und Serverantworten.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.14.7	Identifizieren Sie die unbefugte Nutzung von Organisat ionssystemen.	guardduty-enabled-centralized	Amazon GuardDuty kann mithilfe von Threat Intellige nce Feeds helfen, potenzielle Cybersich erheitsereignisse zu überwachen und zu erkennen. Dazu gehören Listen mit bösartigen IPs und maschinel len Lernmethoden zur Identifizierung unerwarteter, nicht autorisierter und bösartiger Aktivitäten in Ihrer AWS Cloud-Umgebung.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.14.7	Identifizieren Sie die unbefugte Nutzung von Organisat ionssystemen.	opensearch-logs-to-cloudwatch	Stellen Sie sicher, dass für Amazon OpenSearch Service-Domains Fehlerpro tokolle aktiviert und zur Aufbewahr ung und Beantwort ung an Amazon CloudWatch Logs gestreamt werden. OpenSearch Service-Fehlerprotokolle können bei Sicherhei ts- und Zugriffsp rüfungen helfen und bei der Diagnose von Verfügbarkeitsprob lemen helfen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.14.7	Identifizieren Sie die unbefugte Nutzung von Organisat ionssystemen.	redshift-cluster-c onfiguration-check	Um Daten im Ruhezustand zu schützen, muss die Verschlüsselung für Ihre Amazon-Re dshift-Cluster aktiviert sein. Sie müssen auch sicherstellen, dass die erforderl ichen Konfigurationen auf Amazon-Redshift-Clustern bereitges tellt werden. Die Prüfungsprotokolli erung muss aktiviert sein, um Informati onen zu Verbindun gen und Benutzera ktivitäten in der Datenbank bereitzus tellen. Diese Regel erfordert, dass ein Wert für clusterDb Encrypted (Config Default: TRUE) und LoggingEnabled (Config Default: TRUE) gesetzt ist. Die tatsächlichen Werte müssen den Richtlini en Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.14.7	Identifizieren Sie die unbefugte Nutzung von Organisat ionssystemen.	s-3 bucket-logging-enabled	Die Amazon Simple Storage Service (Amazon S3)-Serverzugriffs protokollierung bietet eine Methode zur Überwachu ng des Netzwerks im Hinblick auf potenzielle Cybersich erheitsereignisse. Die Ereignisse werden überwacht, indem detaillierte Aufzeichn ungen über die Anfragen erfasst werden, die an einen Amazon-S3-Bucket gestellt wurden. Jeder Zugriffsprotokolle intrag enthält Details zu einer einzelnen Zugriffsanfrage. Zu den Details gehören Anforderer, Bucket-Name, Anforderu ngszeit, Anforderu ngsaktion, Antwortst atus und Fehlercode, falls relevant.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.14.7	Identifizieren Sie die unbefugte Nutzung von Organisat ionssystemen.	vpc-flow-logs-enabled	VPC-Flow-Protokoll e erfassen detaillierte Informationsdatens ätze über den IP-Datenverkehr, der zu und von Netzwerkschnittste llen in Ihrer Amazon Virtual Private Cloud (Amazon VPC) fließt. Standardmäßig enthalten Flow-Prot okolldatensätze Werte für die verschiedenen Komponenten des IP-Flows, einschlie ßlich Quelle, Ziel und Protokoll.

Vorlage

Die Vorlage ist verfügbar unter GitHub: Operational Best Practices for NIST 800 171.

Bewährte Methoden für die Ausführung von NIST 800 172

Konformitätspakete bieten ein allgemeines Compliance-Framework, das es Ihnen ermöglicht, mithilfe verwalteter oder benutzerdefinierter AWS Config Regeln und Abhilfemaßnahmen Kontrollen zur Sicherheits-, Betriebs- oder Kostenoptimierung durchzuführen. AWS Config Conformance Packs dienen als Beispielvorlagen nicht dazu, die vollständige Einhaltung eines bestimmten Governance- oder Compliance-Standards sicherzustellen. Sie sind dafür verantwortlich, selbst zu beurteilen, ob Ihre Nutzung der Services den geltenden gesetzlichen und behördlichen Anforderungen entspricht.

Im Folgenden finden Sie ein Beispiel für eine Zuordnung zwischen den NIST 800-172- und AWS verwalteten Konfigurationsregeln. Jede Config-Regel gilt für eine bestimmte AWS Ressource und

bezieht sich auf eine oder mehrere NIST 800-172-Steuerelemente. Eine Kontrolle nach NIST 800-172 kann mehreren Konfigurationsregeln zugeordnet werden. In der folgenden Tabelle finden Sie weitere Informationen und Anleitungen zu diesen Zuordnungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.1.3e	Setzen Sie [Aufgabe: vom Unternehmen definierte sichere Informationsübertragungslösungen] ein, um den Informationsfluss zwischen Sicherheitsdomänen auf verbundenen Systemen zu kontrollieren.	alb-http-drop-invalid-Header-fähig	Stellen Sie sicher, dass Ihre Elastic Load Balancers (ELB) so konfiguriert sind, dass sie HTTP-Header löschen. Da sensible Daten vorhanden sein können, sollten Sie die Verschlüsselung bei der Übertragung aktivieren, um diese Daten zu schützen.
3.1.3e	Setzen Sie [Aufgabe: vom Unternehmen definierte sichere Informationsübertragungslösungen] ein, um den Informationsfluss zwischen Sicherheitsdomänen auf verbundenen Systemen zu kontrollieren.	alb-http-to-https-Umleitungsprüfung	Um Daten während der Übertragung zu schützen, stellen Sie sicher, dass Ihr Application Load Balancer unverschlüsselte HTTP-Anfragen automatisch an HTTPS umleitet. Da sensible Daten vorhanden sein können, sollten Sie die Verschlüsselung bei der Übertragung aktivieren, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.1.3e	Setzen Sie [Aufgabe: vom Unternehmen definierte sichere Informationsübertragungslösungen] ein, um den Informationsfluss zwischen Sicherheitsdomänen auf verbundenen Systemen zu kontrollieren.	api-gw-ssl-enabled	Stellen Sie sicher, dass die REST-API-Stufen von Amazon API Gateway mit SSL-Zertifikaten konfiguriert sind, damit Backend-Systeme überprüfen können, ob Anforderungen von API Gateway stammen.
3.1.3e	Setzen Sie [Aufgabe: vom Unternehmen definierte sichere Informationsübertragungslösungen] ein, um den Informationsfluss zwischen Sicherheitsdomänen auf verbundenen Systemen zu kontrollieren.	elasticsearch-node-to-node-Verschlüsselungsprüfung	Stellen Sie sicher, dass die node-to-node Verschlüsselung für Amazon OpenSearch Service aktiviert ist. Node-to-nodeVerschlüsselung ermöglicht die TLS 1.2-Verschlüsselung für die gesamte Kommunikation innerhalb der Amazon Virtual Private Cloud (Amazon VPC). Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.1.3e	Setzen Sie [Aufgabe: vom Unternehmen definierte sichere Informationsübertragungslösungen] ein, um den Informationsfluss zwischen Sicherheitsdomänen auf verbundenen Systemen zu kontrollieren.	elb-acm-certificate-required	Zum Schutz von eventuell vorhandenen sensiblen Daten sowie von Daten während der Übertragung muss die Verschlüsselung für Ihr Elastic Load Balancing aktiviert sein. Verwenden Sie AWS Certificate Manager, um öffentliche und private SSL/TLS-Zertifikate mit AWS Diensten und internen Ressourcen zu verwalten, bereitzustellen und bereitzustellen.
3.1.3e	Setzen Sie [Aufgabe: vom Unternehmen definierte sichere Informationsübertragungslösungen] ein, um den Informationsfluss zwischen Sicherheitsdomänen auf verbundenen Systemen zu kontrollieren.	elb-tls-https-listeners-nur	Stellen Sie sicher, dass Ihre Elastic Load Balancer (ELBs) mit SSL- oder HTTPS-Listenern konfiguriert sind. Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.1.3e	Setzen Sie [Aufgabe: vom Unternehmen definierte sichere Informationsübertragungslösungen] ein, um den Informationsfluss zwischen Sicherheitsdomänen auf verbundenen Systemen zu kontrollieren.	redshift-require-tls-ssl	Stellen Sie sicher, dass Ihre Amazon-Redshift-Cluster eine TLS/SSL-Verschlüsselung erfordern, um eine Verbindung zu SQL-Clients herzustellen. Da sensible Daten vorhanden sein können, sollten Sie die Verschlüsselung bei der Übertragung aktivieren, um diese Daten zu schützen.
3.1.3e	Setzen Sie [Aufgabe: vom Unternehmen definierte sichere Informationsübertragungslösungen] ein, um den Informationsfluss zwischen Sicherheitsdomänen auf verbundenen Systemen zu kontrollieren.	s-3 bucket-ssl-requests-only	Um Daten während der Übertragung zu schützen, stellen Sie sicher, dass Ihre Amazon Simple Storage Service (Amazon S3)-Buckets Anfragen zur Verwendung von Secure Socket Layer (SSL)-Buckets erfordern. Da sensible Daten vorhanden sein können, sollten Sie die Verschlüsselung bei der Übertragung aktivieren, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.1.3e	Setzen Sie [Aufgabe: vom Unternehmen definierte sichere Informationsübertragungslösungen] ein, um den Informationsfluss zwischen Sicherheitsdomänen auf verbundenen Systemen zu kontrollieren.	dms-replication-not-public	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass auf DMS-Replikationsinstanzen nicht öffentlich zugegriffen werden kann. DMS-Replikations-Instances können vertrauliche Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.
3.1.3e	Setzen Sie [Aufgabe: vom Unternehmen definierte sichere Informationsübertragungslösungen] ein, um den Informationsfluss zwischen Sicherheitsdomänen auf verbundenen Systemen zu kontrollieren.	ebs-snapshot-public-restorable-überprüfen	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass EBS-Snapshots nicht öffentlich wiederherstellbar sind. EBS-Volume-Snapshots können vertrauliche Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.1.3e	Setzen Sie [Aufgabe: vom Unternehmen definierte sichere Informationsübertragungslösungen] ein, um den Informationsfluss zwischen Sicherheitsdomänen auf verbundenen Systemen zu kontrollieren.	ec-2 instance-no-public-ip	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon Elastic Compute Cloud (Amazon EC2) - Instances nicht öffentlich zugänglich sind. EC2 Amazon-Instances können vertrauliche Informationen enthalten, und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.1.3e	Setzen Sie [Aufgabe: vom Unternehmen definierte sichere Informationsübertragungslösungen] ein, um den Informationsfluss zwischen Sicherheitsdomänen auf verbundenen Systemen zu kontrollieren.	elasticsearch-in-vpc-only	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass sich Amazon OpenSearch OpenSearch Service (Service) - Domains innerhalb einer Amazon Virtual Private Cloud (Amazon VPC) befinden. Eine OpenSearch Service-Domain innerhalb einer Amazon VPC ermöglicht die sichere Kommunikation zwischen OpenSearch Service und anderen Services innerhalb der Amazon VPC, ohne dass ein Internet-Gateway, ein NAT-Gerät oder eine VPN-Verbindung erforderlich ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.1.3e	Setzen Sie [Aufgabe: vom Unternehmen definierte sichere Informationsübertragungslösungen] ein, um den Informationsfluss zwischen Sicherheitsdomänen auf verbundenen Systemen zu kontrollieren.	emr-master-no-public-ip	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon EMR-Cluster-Masterknoten nicht öffentlich zugänglich sind. Amazon-EMR-Cluster-Hauptknoten können vertrauliche Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.1.3e	Setzen Sie [Aufgabe: vom Unternehmen definierte sichere Informationsübertragungslösungen] ein, um den Informationsfluss zwischen Sicherheitsdomänen auf verbundenen Systemen zu kontrollieren.	ec-2 instances-in-vpc	Stellen Sie Amazon Elastic Compute Cloud (Amazon EC2) -Instances innerhalb einer Amazon Virtual Private Cloud (Amazon VPC) bereit, um eine sichere Kommunikation zwischen einer Instance und anderen Services innerhalb der Amazon VPC zu ermöglichen, ohne dass ein Internet-Gateway, ein NAT-Gerät oder eine VPN-Verbindung erforderlich ist. Der gesamte Datenverkehr bleibt sicher in der AWS Cloud. Domains, die sich innerhalb einer VPC befinden, verfügen aufgrund ihrer logischen Isolierung im Vergleich zu Domains mit öffentlichen Endpunkten über eine zusätzliche Sicherheitsebene. Weisen Sie EC2

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			Amazon-Instances einer Amazon-VPC zu, um den Zugriff ordnungsgemäß zu verwalten.
3.1.3e	Setzen Sie [Aufgabe: vom Unternehmen definierte sichere Informationsübertragungslösungen] ein, um den Informationsfluss zwischen Sicherheitsdomänen auf verbundenen Systemen zu kontrollieren.	lambda-function-public-access-verboten	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass AWS Lambda-Funktionen nicht öffentlich zugänglich sind. Der öffentliche Zugriff kann möglicherweise die Verfügbarkeit von Ressourcen beeinträchtigen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.1.3e	Setzen Sie [Aufgabe: vom Unternehmen definierte sichere Informationsübertragungslösungen] ein, um den Informationsfluss zwischen Sicherheitsdomänen auf verbundenen Systemen zu kontrollieren.	lambda-inside-vpc	Stellen Sie AWS Lambda-Funktionen in einer Amazon Virtual Private Cloud (Amazon VPC) bereit, um eine sichere Kommunikation zwischen einer Funktion und anderen Diensten innerhalb der Amazon VPC zu gewährleisten. Bei dieser Konfiguration sind kein Internet-Gateway, kein NAT-Gerät und keine VPN-Verbindung erforderlich. Der gesamte Datenverkehr bleibt sicher in der Cloud. AWS Domains, die sich innerhalb einer VPC befinden, verfügen aufgrund ihrer logischen Isolierung im Vergleich zu Domains mit öffentlichen Endpunkten über eine zusätzliche Sicherheitsebene. Um den Zugriff ordnungsgemäß zu verwalten,

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			sollten AWS Lambda-Funktionen einer VPC zugewiesen werden.
3.1.3e	Setzen Sie [Aufgabe: vom Unternehmen definierte sichere Informationsübertragungslösungen] ein, um den Informationsfluss zwischen Sicherheitsdomänen auf verbundenen Systemen zu kontrollieren.	no-unrestricted-route-to-igw	Stellen Sie sicher, dass EC2 Amazon-Routentabellen keine uneingeschränkten Routen zu einem Internet-Gateway enthalten. Durch das Entfernen oder Beschränken des Internetzugangs für Workloads innerhalb von Amazon VPCs können unbeabsichtigte Zugriffe in Ihrer Umgebung reduziert werden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.1.3e	Setzen Sie [Aufgabe: vom Unternehmen definierte sichere Informationsübertragungslösungen] ein, um den Informationsfluss zwischen Sicherheitsdomänen auf verbundenen Systemen zu kontrollieren.	rds-instance-public-access-überprüfen	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Relational Database Service (Amazon RDS) -Instances nicht öffentlich sind. Amazon-RDS-Datenbank-Instances können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.1.3e	Setzen Sie [Aufgabe: vom Unternehmen definierte sichere Informationsübertragungslösungen] ein, um den Informationsfluss zwischen Sicherheitsdomänen auf verbundenen Systemen zu kontrollieren.	rds-snapshots-public-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Relational Database Service (Amazon RDS) -Instances nicht öffentlich sind. Amazon-RDS-Datenbank-Instances können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.1.3e	Setzen Sie [Aufgabe: vom Unternehmen definierte sichere Informationsübertragungslösungen] ein, um den Informationsfluss zwischen Sicherheitsdomänen auf verbundenen Systemen zu kontrollieren.	redshift-cluster-public-access-überprüfen	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Redshift Redshift-Cluster nicht öffentlich sind. Amazon-Redshift-Cluster können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.1.3e	Setzen Sie [Aufgabe: vom Unternehmen definierte sichere Informationsübertragungslösungen] ein, um den Informationsfluss zwischen Sicherheitsdomänen auf verbundenen Systemen zu kontrollieren.	restricted-common-ports	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass gemeinsame Ports für Amazon Elastic Compute Cloud (Amazon EC2) -Sicherheitsgruppen eingeschränkt sind. Wenn der Zugriff auf Ports nicht auf vertrauenswürdige Quellen beschränkt wird, kann dies zu Angriffen auf die Verfügbarkeit, Integrität und Vertraulichkeit von Systemen führen. Mit dieser Regel können Sie optional die Parameter blockedPort1–blockedPort5 festlegen (Standardkonfigurationen: 20, 21, 3389, 3306, 4333). Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.1.3e	Setzen Sie [Aufgabe: vom Unternehmen definierte sichere Informationsübertragungslösungen] ein, um den Informationsfluss zwischen Sicherheitsdomänen auf verbundenen Systemen zu kontrollieren.	s3- account-level-public-access -Block-periodisch	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Simple Storage Service (Amazon S3) -Buckets nicht öffentlich zugänglich sind. Diese Regel trägt dazu bei, sensible Daten vor unbefugten Remote-Benutzern zu schützen, indem sie den öffentlichen Zugriff verhindert. Mit dieser Regel können Sie optional die Parameter ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) und restrictPublicBuckets Parameter (Config Default: True) festlegen. Die tatsächlichen Werte müssen den Richtlini

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			en Ihrer Organisation entsprechen.
3.1.3e	Setzen Sie [Aufgabe: vom Unternehmen definierte sichere Informationsübertragungslösungen] ein, um den Informationsfluss zwischen Sicherheitsdomänen auf verbundenen Systemen zu kontrollieren.	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) Security Groups können bei der Verwaltung des Netzwerkzugriffs helfen, indem sie eine statusbehaftete Filterung von eingehendem und ausgehendem Netzwerkverkehr zu Ressourcen bereitstellen. AWS Wenn Sie eingehenden (oder entfernten) Datenverkehr von 0.0.0.0/0 bis Port 22 auf Ihren Ressourcen nicht zulassen, können Sie den Remote-Zugriff einschränken.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.1.3e	Setzen Sie [Aufgabe: vom Unternehmen definierte sichere Informationsübertragungslösungen] ein, um den Informationsfluss zwischen Sicherheitsdomänen auf verbundenen Systemen zu kontrollieren.	s3- verboten bucket-level-public-access	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Simple Storage Service (Amazon S3) -Buckets nicht öffentlich zugänglich sind. Diese Regel trägt dazu bei, sensible Daten vor unbefugten Remote-Benutzern zu schützen, indem sie den öffentlichen Zugriff auf Bucket-Ebene verhindert.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.1.3e	Setzen Sie [Aufgabe: vom Unternehmen definierte sichere Informationsübertragungslösungen] ein, um den Informationsfluss zwischen Sicherheitsdomänen auf verbundenen Systemen zu kontrollieren.	s-3 bucket-public-read-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie nur autorisierten Benutzern, Prozessen und Geräten Zugriff auf Amazon Simple Storage Service (Amazon S3) - Buckets gewähren. Die Verwaltung des Zugriffs sollte mit der Klassifizierung der Daten übereinstimmen.
3.1.3e	Setzen Sie [Aufgabe: vom Unternehmen definierte sichere Informationsübertragungslösungen] ein, um den Informationsfluss zwischen Sicherheitsdomänen auf verbundenen Systemen zu kontrollieren.	s3- bucket-public-write-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie nur autorisierten Benutzern, Prozessen und Geräten Zugriff auf Amazon Simple Storage Service (Amazon S3) - Buckets gewähren. Die Verwaltung des Zugriffs sollte mit der Klassifizierung der Daten übereinstimmen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.1.3e	Setzen Sie [Aufgabe: vom Unternehmen definierte sichere Informationsübertragungslösungen] ein, um den Informationsfluss zwischen Sicherheitsdomänen auf verbundenen Systemen zu kontrollieren.	sagemaker-notebook-no-direct-Internetzugang	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass SageMaker Amazon-Notebooks keinen direkten Internetzugang zulassen. Indem Sie direkten Internetzugang blockieren, vermeiden Sie, dass unbefugte Benutzer auf sensible Daten zugreifen.
3.1.3e	Setzen Sie [Aufgabe: vom Unternehmen definierte sichere Informationsübertragungslösungen] ein, um den Informationsfluss zwischen Sicherheitsdomänen auf verbundenen Systemen zu kontrollieren.	ssm-document-not-public	Stellen Sie sicher, dass AWS Systems Manager (SSM) - Dokumente nicht öffentlich sind, da dies einen unbeabsichtigten Zugriff auf Ihre SSM-Dokumente ermöglichen kann. Ein öffentliches SSM-Dokument kann Informationen über Ihr Konto, Ihre Ressourcen und internen Prozesse preisgeben.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.1.3e	Setzen Sie [Aufgabe: vom Unternehmen definierte sichere Informationsübertragungslösungen] ein, um den Informationsfluss zwischen Sicherheitsdomänen auf verbundenen Systemen zu kontrollieren.	subnet-auto-assign-public-ip-deaktiviert	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon Virtual Private Cloud (VPC) -Subnetzen nicht automatisch eine öffentliche IP-Adresse zugewiesen wird. Amazon Elastic Compute Cloud (EC2) -Instances, die in Subnetzen gestartet werden, in denen dieses Attribut aktiviert ist, haben ihrer primären Netzwerkschnittstelle eine öffentliche IP-Adresse zugewiesen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.1.3e	Setzen Sie [Aufgabe: vom Unternehmen definierte sichere Informationsübertragungslösungen] ein, um den Informationsfluss zwischen Sicherheitsdomänen auf verbundenen Systemen zu kontrollieren.	vpc-default-security-group-geschlossen	Sicherheitsgruppen von Amazon Elastic Compute Cloud (Amazon EC2) können bei der Verwaltung des Netzwerkzugriffs helfen, indem sie eine statusbehaftete Filterung des ein- und ausgehenden Netzwerkverkehrs zu Ressourcen bereitstellen. AWS Die Beschränkung des gesamten Datenverkehrs auf die Standardsicherheitsgruppe hilft dabei, den Fernzugriff auf Ihre Ressourcen einzuschränken. AWS

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.1.3e	Setzen Sie [Aufgabe: vom Unternehmen definierte sichere Informationsübertragungslösungen] ein, um den Informationsfluss zwischen Sicherheitsdomänen auf verbundenen Systemen zu kontrollieren.	vpc-sg-open-only-to-authorized-ports	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass gemeinsame Ports für Amazon Elastic Compute Cloud (Amazon EC2) -Sicherheitsgruppen eingeschränkt sind. Wenn der Zugriff auf Ports nicht auf vertrauenswürdige Quellen beschränkt wird, kann dies zu Angriffen auf die Verfügbarkeit, Integrität und Vertraulichkeit von Systemen führen. Durch die Beschränkung des Zugriffs auf Ressourcen innerhalb einer Sicherheitsgruppe aus dem Internet (0.0.0.0/0) kann der Fernzugriff auf interne Systeme gesteuert werden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.1.3e	Setzen Sie [Aufgabe: vom Unternehmen definierte sichere Informationsübertragungslösungen] ein, um den Informationsfluss zwischen Sicherheitsdomänen auf verbundenen Systemen zu kontrollieren.	autoscaling-launch-config-public-ip-deaktiviert	Wenn Sie Ihre Netzwerkschnittstellen mit einer öffentlichen IP-Adresse konfigurieren, sind die diesen Netzwerkschnittstellen zugehörigen Ressourcen über das Internet erreichbar. EC2 Ressourcen sollten nicht öffentlich zugänglich sein, da dies einen unbeabsichtigten Zugriff auf Ihre Anwendungen oder Server ermöglichen kann.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.1.3e	Setzen Sie [Aufgabe: vom Unternehmen definierte sichere Informationsübertragungslösungen] ein, um den Informationsfluss zwischen Sicherheitsdomänen auf verbundenen Systemen zu kontrollieren.	alb-desync-mode-check	Um Anwendungen vor HTTP-Desync-Schwachstellen zu schützen, stellen Sie sicher, dass der HTTP-Desync-Mitigationsmodus auf Ihren Anwendungs-Loadbalancern aktiviert ist. Probleme mit HTTP-Desync können zum Schmuggel von Anfragen führen und Ihre Anwendungen anfällig für Queues- oder Cache-Poisoning machen. Die desynchronen Mitigationsmodi lauten „Überwachen“, „Defensiv“ und „Am strengsten“. Defensive ist der standardmäßige Modus.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.1.3e	Setzen Sie [Aufgabe: vom Unternehmen definierte sichere Informationsübertragungslösungen] ein, um den Informationsfluss zwischen Sicherheitsdomänen auf verbundenen Systemen zu kontrollieren.	clb-desync-mode-check	Um Anwendungen vor HTTP-Desync-Schwachstellen zu schützen, stellen Sie sicher, dass der HTTP-Desync-Mitigationsmodus auf Ihren Anwendungs-Loadbalancern aktiviert ist. Probleme mit HTTP-Desync können zum Schmuggel von Anfragen führen und Ihre Anwendungen anfällig für Queues- oder Cache-Poisoning machen. Die desynchronen Mitigationsmodi lauten „Überwachen“, „Defensiv“ und „Am strengsten“. Defensive ist der standardmäßige Modus.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.1.3e	Setzen Sie [Aufgabe: vom Unternehmen definierte sichere Informationsübertragungslösungen] ein, um den Informationsfluss zwischen Sicherheitsdomänen auf verbundenen Systemen zu kontrollieren.	redshift-enhanced-vpc-routing-aktiviert	Mit Enhanced-VPC-Routing wird erzwungen, dass der gesamte COPY- und UNLOAD-Datenverkehr zwischen Ihrem Cluster und Datenrepositorys über Ihre Amazon VPC erfolgt. Anschließend können Sie VPC-Features wie Sicherheitsgruppen und Netzwerkzugriffskontrolllisten verwenden, um den Netzwerkverkehr zu schützen. Sie können auch VPC-Flow-Logs verwenden, um den Netzwerkverkehr zu überwachen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.1.3e	Setzen Sie [Aufgabe: vom Unternehmen definierte sichere Informationsübertragungslösungen] ein, um den Informationsfluss zwischen Sicherheitsdomänen auf verbundenen Systemen zu kontrollieren.	elbv2- acm-certificate-required	Zum Schutz von eventuell vorhandenen sensiblen Daten sowie von Daten während der Übertragung muss die Verschlüsselung für Ihr Elastic Load Balancing aktiviert sein. Verwenden Sie AWS Certificate Manager, um öffentliche und private SSL/TLS-Zertifikate mit AWS Diensten und internen Ressourcen zu verwalten, bereitzustellen und bereitzustellen.
3.1.3e	Setzen Sie [Aufgabe: vom Unternehmen definierte sichere Informationsübertragungslösungen] ein, um den Informationsfluss zwischen Sicherheitsdomänen auf verbundenen Systemen zu kontrollieren.	opensearch-https-required	Da sensible Daten existieren können und um Daten während der Übertragung zu schützen, sollten Sie sicherstellen, dass HTTPS für Verbindungen zu Ihren Amazon OpenSearch Service-Domains aktiviert ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.1.3e	Setzen Sie [Aufgabe: vom Unternehmen definierte sichere Informationsübertragungslösungen] ein, um den Informationsfluss zwischen Sicherheitsdomänen auf verbundenen Systemen zu kontrollieren.	opensearch-in-vpc-only	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass sich Amazon OpenSearch Service-Domains innerhalb einer Amazon Virtual Private Cloud (Amazon VPC) befinden. Eine Amazon OpenSearch Service-Domain innerhalb einer Amazon VPC ermöglicht die sichere Kommunikation zwischen Amazon OpenSearch Service und anderen Services innerhalb der Amazon VPC, ohne dass ein Internet-Gateway, ein NAT-Gerät oder eine VPN-Verbindung erforderlich ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.1.3e	Setzen Sie [Aufgabe: vom Unternehmen definierte sichere Informationsübertragungslösungen] ein, um den Informationsfluss zwischen Sicherheitsdomänen auf verbundenen Systemen zu kontrollieren.	opensearch-node-to-node-Verschlüsselungsprüfung	Stellen Sie sicher, dass die node-to-node Verschlüsselung für Amazon OpenSearch Service aktiviert ist. Node-to-nodeVerschlüsselung ermöglicht die TLS 1.2-Verschlüsselung für die gesamte Kommunikation innerhalb der Amazon Virtual Private Cloud (Amazon VPC). Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.1.3e	Setzen Sie [Aufgabe: vom Unternehmen definierte sichere Informationsübertragungslösungen] ein, um den Informationsfluss zwischen Sicherheitsdomänen auf verbundenen Systemen zu kontrollieren.	ec2- token-hop-limit-check	Stellen Sie sicher, dass die HTTP-PUT-Antwort des Instance Metadata Service (IMDS) auf die Amazon Elastic Compute Cloud (Amazon EC2) - Instance beschränkt ist. Mit kann die PUT-Antwort IMDSv2, die standardmäßig das geheime Token enthält, die Instance nicht verlassen, da das Metadaten-Antwort-Hop-Limit auf 1 gesetzt ist (Konfigurationsstandard). Wenn dieser Wert größer als 1 ist, kann das Token die EC2 Instance verlassen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.1.3e	Setzen Sie [Aufgabe: vom Unternehmen definierte sichere Informationsübertragungslösungen] ein, um den Informationsfluss zwischen Sicherheitsdomänen auf verbundenen Systemen zu kontrollieren.	nacl-no-unrestricted-ssh-rdp	Der Zugriff auf Remote-Serveradministrationsports in Ihren Network Access Control Lists (NACLs), wie Port 22 (SSH) und Port 3389 (RDP), sollte nicht öffentlich zugänglich sein, da dies einen unbeabsichtigten Zugriff auf Ressourcen innerhalb Ihrer VPC ermöglichen kann.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.2.1e	Durchführung von Sensibilisierungsschulungen [Zuweisung: von der Organisation festgelegte Häufigkeit], die sich auf das Erkennen von und die Reaktion auf Bedrohungen durch Social Engineering, Advanced Persistent Threat Actors, Sicherheitsverletzungen und verdächtiges Verhalten konzentrieren; Aktualisierung der Schulungen [Zuweisung: von der Organisation festgelegte Häufigkeit] oder bei wesentlichen Änderungen der Bedrohung.	security-awareness-program-exists (Prozessüberprüfung)	Etablieren und pflegen Sie ein Programm zur Förderung des Sicherheitsbewusstseins in Ihrer Organisation. Programme zur Förderung des Sicherheitsbewusstseins der Mitarbeiter vermitteln ihnen, wie sie die Organisation vor diversen Sicherheitsverletzungen oder Sicherheitsvorfällen schützen können.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.4.2e	Einsatz automatischer Mechanismen, um falsch konfigurierte oder nicht autorisierte Systemkomponenten zu erkennen; nach der Erkennung [Auswahl (eine oder mehrere): die Komponent en entfernen; die Komponenten in ein Quarantäne- oder Abhilfe-Netzwerk stellen], um Patches, Neukonfiguration oder andere Abhilfema ßnahmen zu erleichte rn.	ec2- prüfen managedinstance-pa tch-compliance-status	Aktivieren Sie diese Regel, um bei der Identifizierung und Dokumentation von Sicherheitslücken in Amazon Elastic Compute Cloud (Amazon EC2) zu helfen. Die Regel prüft, ob die EC2 Amazon-Instance die Patch-Konformität im AWS Systems Manager gemäß den Richtlinien und Verfahren Ihrer Organisation einhält.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.4.2e	Einsatz automatischer Mechanismen, um falsch konfigurierte oder nicht autorisierte Systemkomponenten zu erkennen; nach der Erkennung [Auswahl (eine oder mehrere): die Komponent en entfernen; die Komponenten in ein Quarantäne- oder Abhilfe-Netzwerk stellen], um Patches, Neukonfiguration oder andere Abhilfema ßnahmen zu erleichte rn.	elastic-beanstalk-managed-updates-aktiviert	Durch die Aktivierung verwalteter Plattform updates für eine Amazon-Elastic-Bea nstalk-Umgebung wird sichergestellt, dass die aktuellen verfügbaren Plattform -Fixes, -Updates und -Features für die Umgebung installiert sind. Eine bewährte Methode zur Sicherung von Systemen besteht darin, stets die aktuellen Patches zu installieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.4.2e	Einsatz automatischer Mechanismen, um falsch konfigurierte oder nicht autorisierte Systemkomponenten zu erkennen; nach der Erkennung [Auswahl (eine oder mehrere): die Komponent en entfernen; die Komponenten in ein Quarantäne- oder Abhilfe-Netzwerk stellen], um Patches, Neukonfiguration oder andere Abhilfema ßnahmen zu erleichte rn.	redshift-cluster-m aintenancesettings-check	Diese Regel stellt sicher, dass Amazon-Redshift-Cluster die bevorzugten Einstellungen für Ihre Organisation haben. Insbesondere sorgt sie dafür, dass Cluster bevorzugt e Wartungsfenster und automatisierte Aufbewahrungsfristen für Snapshots für die Datenbank haben. Für diese Regel müssen Sie die allowVers ionUpgrade festlegen . Der Standardwert ist „true“. Außerdem können Sie optional den Zeitraum preferredMaintenan ceWindow (der Standardwert ist sa: 16:00 -sa: 16:30) und den automated SnapshotRetention Zeitraum (der Standardwert ist 1) festlegen. Die tatsächlichen Werte müssen den Richtlini

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			en Ihrer Organisation entsprechen.
3.4.2e	Einsatz automatischer Mechanismen, um falsch konfigurierte oder nicht autorisierte Systemkomponenten zu erkennen; nach der Erkennung [Auswahl (eine oder mehrere): die Komponent en entfernen; die Komponenten in ein Quarantäne- oder Abhilfe-Netzwerk stellen], um Patches, Neukonfiguration oder andere Abhilfema ßnahmen zu erleichte rn.	rds-automatic-mino r-version-Upgrade aktiviert	Aktivieren Sie automatische Unterversions-Upgrades auf Ihren Amazon-Re lational-Database-Service (RDS)-Ins tances, um sicherzus tellen, dass die aktuellen Updates für Unterversionen des Relational Database Management System (RDBMS) installiert sind, die Sicherhei tspatches und Bugfixes enthalten können.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.4.3e	Nutzen Sie automatisierte Erkennungs- und Verwaltungstools, um ein vollständiges up-to-date, genaues und jederzeit verfügbares Inventar der Systemkomponenten zu führen.	ec2-manager instance-managed-by-systems	Eine Bestandsaufnahme der Softwareplattformen und Anwendungen innerhalb des Unternehmens ist möglich, indem Amazon Elastic Compute Cloud (Amazon EC2) - Instances mit AWS Systems Manager verwaltet werden. Verwenden Sie AWS Systems Manager, um detaillierte Systemkonfigurationen, Betriebssystem-Patch-Levels, Namen und Typ der Dienste, Softwareinstallationen, Anwendungsname, Herausgeber und Version sowie andere Details zu Ihrer Umgebung bereitzustellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.4.3e	Verwenden Sie automatisierte Erkennungs- und Verwaltungstools, um ein vollständiges up-to-date, genaues und jederzeit verfügbar es Inventar der Systemkomponenten zu führen.	ec2-stopped-instance	Aktivieren Sie diese Regel, um bei der Basiskonfiguration von Amazon Elastic Compute Cloud (Amazon EC2) - Instances zu helfen, indem Sie überprüfe n, ob EC2 Amazon-Instances gemäß den Standards Ihrer Organisation für mehr als die zulässige Anzahl von Tagen gestoppt wurden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.4.3e	Verwenden Sie automatisierte Erkennungs- und Verwaltungstools, um ein vollständiges up-to-date, genaues und jederzeit verfügbar es Inventar der Systemkomponenten zu führen.	ec2- volume-inuse-check	Diese Regel stellt sicher, dass Amazon Elastic Block Store-Volumes, die an Amazon Elastic Compute Cloud (Amazon EC2) - Instances angehängt sind, zum Löschen markiert werden, wenn eine Instance beendet wird. Wenn ein Amazon-EB S-Volume nicht gelöscht wird, wenn die Instance, an die es angehängt ist, beendet wird, kann dies gegen das Konzept der geringsten Funktiona lität verstoßen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.4.3e	Verwenden Sie automatisierte Erkennungs- und Verwaltungstools, um ein vollständiges up-to-date, genaues und jederzeit verfügbar es Inventar der Systemkomponenten zu führen.	eip-attached	Diese Regel stellt sicher, dass Elastic, die einer Amazon Virtual Private Cloud (Amazon VPC) IPs zugewiesen sind, an Amazon Elastic Compute Cloud (Amazon EC2) - Instances oder verwendete Elastic Network Interface s angehängt sind. Diese Regel hilft bei der Überwachu ng ungenutzter Inhalte EIPs in Ihrer Umgebung.
3.4.3e	Verwenden Sie automatisierte Erkennungs- und Verwaltungstools, um ein vollständiges up-to-date, genaues und jederzeit verfügbar es Inventar der Systemkomponenten zu führen.	vpc-network-acl-un used-überprüfen	Diese Regel stellt sicher, dass Amazon Virtual Private Cloud (VPC)-Netzwerkzugr iffskontrolllisten verwendet werden. Die Überwachu ng ungenutzter Netzwerk-Zugriffsk ontrolllisten kann zu einer genauen Inventarisierung und Verwaltung Ihrer Umgebung beitragen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.5.2e	Einsatz automatisierter Mechanismen für die Erstellung, den Schutz, die Rotation und die Verwaltung von Passwörtern für Systeme und Systemkomponenten, die keine Multifaktor-Authentifizierung oder komplexe Kontenverwaltung unterstützen.	iam-password-policy	Die Identitäten und Anmeldeinformationen werden auf der Grundlage einer organisatorischen IAM-Passwortrichtlinie ausgestellt, verwaltet und verifiziert. Sie erfüllen oder übertreffen die Anforderungen von NIST SP 800-63 und dem Standard „Best Practices“ von AWS Foundational Security für die Passwortstärke. Mit dieser Regel können Sie optional RequireUppercaseCharacters (Wert für AWS grundlegende Sicherheitsbewährte Methoden: wahr), RequireLowercaseCharacters (Wert für bewährte Methoden für AWS grundlegende Sicherheit: wahr), RequireSymbols (Wert für bewährte Methoden für AWS grundlegende Sicherheit:

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			wahr), RequireNumbers (Wert für bewährte Methoden für AWS grundlegende Sicherheit: wahr), MinimumPasswordLength (Wert für bewährte Methoden für AWS grundlegende Sicherheit: 14), PasswordReusePrevention (Wert für bewährte Methoden für AWS grundlegende Sicherheit: 24) und MaxPasswordAge (Wert für bewährte Methoden für AWS grundlegende Sicherheit: 90) für Ihr IAM festlegen Kennwortrichtlinie. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.5.2e	Einsatz automatisierter Mechanismen für die Erstellung, den Schutz, die Rotation und die Verwaltung von Passwörtern für Systeme und Systemkomponenten, die keine Multifaktor-Authentifizierung oder komplexe Kontenverwaltung unterstützen.	secretsmanager-rotation-enabled-check	Diese Regel stellt sicher, dass bei AWS Secrets Manager Manager-Geheimnissen die Rotation aktiviert ist. Die regelmäßige Rotation von Secrets kann den Zeitraum verkürzen, in dem ein Secret aktiv ist, und möglicherweise die Auswirkungen auf das Unternehmen verringern, falls das Secret kompromittiert wird.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.5.2e	Einsatz automatisierter Mechanismen für die Erstellung, den Schutz, die Rotation und die Verwaltung von Passwörtern für Systeme und Systemkomponenten, die keine Multifaktor-Authentifizierung oder komplexe Kontenverwaltung unterstützen.	secretsmanager-scheduled-rotation-success-überprüfen	Diese Regel stellt sicher, dass AWS Secrets Manager Manager-Geheimnisse gemäß dem Rotationsplan erfolgreich rotiert wurden. Die regelmäßige Rotation von Secrets kann den Zeitraum verkürzen, in dem ein Secret aktiv ist, und möglicherweise die Auswirkungen auf das Unternehmen verringern, falls es kompromittiert wird.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.5.2e	Einsatz automatisierter Mechanismen für die Erstellung, den Schutz, die Rotation und die Verwaltung von Passwörtern für Systeme und Systemkomponenten, die keine Multifaktor-Authentifizierung oder komplexe Kontenverwaltung unterstützen.	secretsmanager-scheduled-rotation-success-überprüfen	Diese Regel stellt sicher, dass AWS Secrets Manager Manager-Geheimnisse gemäß dem Rotationsplan erfolgreich rotiert wurden. Die regelmäßige Rotation von Secrets kann den Zeitraum verkürzen, in dem ein Secret aktiv ist, und möglicherweise die Auswirkungen auf das Unternehmen verringern, falls es kompromittiert wird.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.11.1e	Nutzen Sie [Aufgabe: vom Unternehmen definierte Quellen für Bedrohungsinformationen] als Teil einer Risikobeurteilung, um die Entwicklung organisatorischer Systeme, Sicherheitsarchitekturen, die Auswahl von Sicherheitslösungen, die Überwachung, die Suche nach Bedrohungen sowie die Reaktions- und Wiederherstellungsmaßnahmen zu steuern und zu unterstützen.	guardduty-enabled-centralized	Amazon GuardDuty kann mithilfe von Threat Intelligence Feeds helfen, potenzielle Cybersicherheitsereignisse zu überwachen und zu erkennen. Dazu gehören Listen mit bösartigen IPs und maschinellen Lernmethoden zur Identifizierung unerwarteter, nicht autorisierter und bösartiger Aktivitäten in Ihrer AWS Cloud-Umgebung.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.11.2e	Durchführung von Aktivitäten zur Suche nach Cyberbedrohungen [Auswahl (eine oder mehrere): [Zuordnung: organisationsdefinierte Häufigkeit]; [Zuordnung: organisationsdefiniertes Ereignis]], um in [Aufgabe: organisationsdefinierten Systemen] nach Anzeichen für eine Gefährdung zu suchen und Bedrohungen zu erkennen, zu verfolgen und zu unterbinden, die sich bestehenden Kontrollen entziehen.	guardduty-enabled-centralized	Amazon GuardDuty kann mithilfe von Threat Intelligence Feeds helfen, potenzielle Cybersicherheitsereignisse zu überwachen und zu erkennen. Dazu gehören Listen mit bösartigen IPs und maschinellen Lernmethoden zur Identifizierung unerwarteter, nicht autorisierter und bösartiger Aktivitäten in Ihrer AWS Cloud-Umgebung.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.11.5e	Beurteilen Sie auf der Grundlage aktueller und gesammelter Bedrohungsinformationen die Wirksamkeit von Sicherheitslösungen [Aufgabe: von der Organisation festgelegte Häufigkeit], um den erwarteten Risiken für die Unternehmenssysteme und das Unternehmen zu begegnen.	annual-risk-assessment-performed (Prozessüberprüfung)	Führen Sie eine jährliche Risikobewertung für Ihre Organisation durch. Risikowertungen können dabei helfen, die Wahrscheinlichkeit und Auswirkungen identifizierter Risiken und/oder Schwachstellen für eine Organisation zu ermitteln.
3.13.4e	Setzen Sie [Auswahl: (eine oder mehrere): [Aufgabe: organisationsdefinierte physische Isolationstechniken]; [Aufgabe: organisationsdefinierte logische Isolationstechniken]] in Organisationssystemen und Systemkomponenten ein.	dms-replication-not-public	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass auf DMS-Replikationsinstanzen nicht öffentlich zugegriffen werden kann. DMS-Replikations-Instances können vertrauliche Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.13.4e	Setzen Sie [Auswahl: (eine oder mehrere): [Aufgabe: organisationsdefinierte physische Isolationstechniken]; [Aufgabe: organisationsdefinierte logische Isolationstechniken]] in Organisationssystemen und Systemkomponenten ein.	ebs-snapshot-public-restorable-überprüfen	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass EBS-Snapshots nicht öffentlich wiederherstellbar sind. EBS-Volume-Snapshots können vertrauliche Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.
3.13.4e	Setzen Sie [Auswahl: (eine oder mehrere): [Aufgabe: organisationsdefinierte physische Isolationstechniken]; [Aufgabe: organisationsdefinierte logische Isolationstechniken]] in Organisationssystemen und Systemkomponenten ein.	ec-2 instance-no-public-ip	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon Elastic Compute Cloud (Amazon EC2) - Instances nicht öffentlich zugänglich sind. EC2 Amazon-Instances können vertrauliche Informationen enthalten, und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.13.4e	Setzen Sie [Auswahl: (eine oder mehrere): [Aufgabe: organisationsdefinierte physische Isolationstechniken]; [Aufgabe: organisationsdefinierte logische Isolationstechniken]] in Organisationssystemen und Systemkomponenten ein.	elasticsearch-in-vpc-only	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass sich Amazon OpenSearch OpenSearch Service (Service) - Domains innerhalb einer Amazon Virtual Private Cloud (Amazon VPC) befinden. Eine OpenSearch Service-Domain innerhalb einer Amazon VPC ermöglicht die sichere Kommunikation zwischen OpenSearch Service und anderen Services innerhalb der Amazon VPC, ohne dass ein Internet-Gateway, ein NAT-Gerät oder eine VPN-Verbindung erforderlich ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.13.4e	Setzen Sie [Auswahl: (eine oder mehrere): [Aufgabe: organisationsdefinierte physische Isolationstechniken]; [Aufgabe: organisationsdefinierte logische Isolationstechniken]] in Organisationssystemen und Systemkomponenten ein.	emr-master-no-public-ip	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon EMR-Cluster-Masterknoten nicht öffentlich zugänglich sind. Amazon-EMR-Cluster-Hauptknoten können vertrauliche Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.13.4e	Setzen Sie [Auswahl: (eine oder mehrere): [Aufgabe: organisationsdefinierte physische Isolationstechniken]; [Aufgabe: organisationsdefinierte logische Isolationstechniken]] in Organisationssystemen und Systemkomponenten ein.	ec-2 instances-in-vpc	Stellen Sie Amazon Elastic Compute Cloud (Amazon EC2) -Instances innerhalb einer Amazon Virtual Private Cloud (Amazon VPC) bereit, um eine sichere Kommunikation zwischen einer Instance und anderen Services innerhalb der Amazon VPC zu ermöglichen, ohne dass ein Internet-Gateway, ein NAT-Gerät oder eine VPN-Verbindung erforderlich ist. Der gesamte Datenverkehr bleibt sicher in der AWS Cloud. Domains, die sich innerhalb einer VPC befinden, verfügen aufgrund ihrer logischen Isolierung im Vergleich zu Domains mit öffentlichen Endpunkten über eine zusätzliche Sicherheitsebene. Weisen Sie EC2

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			Amazon-Instances einer Amazon-VPC zu, um den Zugriff ordnungsgemäß zu verwalten.
3.13.4e	Setzen Sie [Auswahl: (eine oder mehrere): [Aufgabe: organisationsdefinierte physische Isolationstechniken]; [Aufgabe: organisationsdefinierte logische Isolationstechniken]] in Organisationssystemen und Systemkomponenten ein.	lambda-function-public-access-verboten	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass AWS Lambda-Funktionen nicht öffentlich zugänglich sind. Der öffentliche Zugriff kann möglicherweise die Verfügbarkeit von Ressourcen beeinträchtigen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.13.4e	Setzen Sie [Auswahl: (eine oder mehrere): [Aufgabe: organisationsdefinierte physische Isolationstechniken]; [Aufgabe: organisationsdefinierte logische Isolationstechniken]] in Organisationssystemen und Systemkomponenten ein.	lambda-inside-vpc	Stellen Sie AWS Lambda-Funktionen in einer Amazon Virtual Private Cloud (Amazon VPC) bereit, um eine sichere Kommunikation zwischen einer Funktion und anderen Diensten innerhalb der Amazon VPC zu gewährleisten. Bei dieser Konfiguration sind kein Internet-Gateway, kein NAT-Gerät und keine VPN-Verbindung erforderlich. Der gesamte Datenverkehr bleibt sicher in der Cloud. AWS Domains, die sich innerhalb einer VPC befinden, verfügen aufgrund ihrer logischen Isolierung im Vergleich zu Domains mit öffentlichen Endpunkten über eine zusätzliche Sicherheitsebene. Um den Zugriff ordnungsgemäß zu verwalten,

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			sollten AWS Lambda-Funktionen einer VPC zugewiesen werden.
3.13.4e	Setzen Sie [Auswahl: (eine oder mehrere): [Aufgabe: organisationsdefinierte physische Isolationstechniken]; [Aufgabe: organisationsdefinierte logische Isolationstechniken]] in Organisationssystemen und Systemkomponenten ein.	rds-instance-public-access-überprüfen	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Relational Database Service (Amazon RDS) -Instances nicht öffentlich sind. Amazon-RDS-Datenbank-Instances können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.13.4e	Setzen Sie [Auswahl: (eine oder mehrere): [Aufgabe: organisationsdefinierte physische Isolationstechniken]; [Aufgabe: organisationsdefinierte logische Isolationstechniken]] in Organisationssystemen und Systemkomponenten ein.	rds-snapshots-public-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Relational Database Service (Amazon RDS) -Instances nicht öffentlich sind. Amazon-RDS-Datenbank-Instances können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.13.4e	Setzen Sie [Auswahl: (eine oder mehrere): [Aufgabe: organisationsdefinierte physische Isolationstechniken]; [Aufgabe: organisationsdefinierte logische Isolationstechniken]] in Organisationssystemen und Systemkomponenten ein.	redshift-cluster-public-access-überprüfen	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Redshift Redshift-Cluster nicht öffentlich sind. Amazon-Redshift-Cluster können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.13.4e	Setzen Sie [Auswahl: (eine oder mehrere): [Aufgabe: organisationsdefinierte physische Isolationstechniken]; [Aufgabe: organisationsdefinierte logische Isolationstechniken]] in Organisationssystemen und Systemkomponenten ein.	s3- -Block-periodisch account-level-public-access	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Simple Storage Service (Amazon S3) -Buckets nicht öffentlich zugänglich sind. Diese Regel trägt dazu bei, sensible Daten vor unbefugten Remote-Benutzern zu schützen, indem sie den öffentlichen Zugriff verhindert. Mit dieser Regel können Sie optional die Parameter ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) und restrictPublicBuckets Parameter (Config Default: True) festlegen. Die tatsächlichen Werte müssen den Richtlini

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			en Ihrer Organisation entsprechen.
3.13.4e	Setzen Sie [Auswahl: (eine oder mehrere): [Aufgabe: organisationsdefinierte physische Isolationstechniken]; [Aufgabe: organisationsdefinierte logische Isolationstechniken]] in Organisationssystemen und Systemkomponenten ein.	s3- bucket-public-read-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie nur autorisierten Benutzern, Prozessen und Geräten Zugriff auf Amazon Simple Storage Service (Amazon S3) - Buckets gewähren. Die Verwaltung des Zugriffs sollte mit der Klassifizierung der Daten übereinstimmen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.13.4e	Setzen Sie [Auswahl: (eine oder mehrere): [Aufgabe: organisationsdefinierte physische Isolationstechniken]; [Aufgabe: organisationsdefinierte logische Isolationstechniken]] in Organisationssystemen und Systemkomponenten ein.	s3- bucket-public-write-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie nur autorisierten Benutzern, Prozessen und Geräten Zugriff auf Amazon Simple Storage Service (Amazon S3) - Buckets gewähren. Die Verwaltung des Zugriffs sollte mit der Klassifizierung der Daten übereinstimmen.
3.13.4e	Setzen Sie [Auswahl: (eine oder mehrere): [Aufgabe: organisationsdefinierte physische Isolationstechniken]; [Aufgabe: organisationsdefinierte logische Isolationstechniken]] in Organisationssystemen und Systemkomponenten ein.	sagemaker-notebook-no-direct-Internetzugang	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass SageMaker Amazon-Notebooks keinen direkten Internetzugang zulassen. Indem Sie direkten Internetzugang blockieren, vermeiden Sie, dass unbefugte Benutzer auf sensible Daten zugreifen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.13.4e	Setzen Sie [Auswahl: (eine oder mehrere): [Aufgabe: organisationsdefinierte physische Isolationstechniken]; [Aufgabe: organisationsdefinierte logische Isolationstechniken]] in Organisationssystemen und Systemkomponenten ein.	subnet-auto-assign-public-ip-deaktiviert	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon Virtual Private Cloud (VPC) -Subnetzen nicht automatisch eine öffentliche IP-Adresse zugewiesen wird. Amazon Elastic Compute Cloud (EC2) -Instances, die in Subnetzen gestartet werden, in denen dieses Attribut aktiviert ist, haben ihrer primären Netzwerkschnittstelle eine öffentliche IP-Adresse zugewiesen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.13.4e	Setzen Sie [Auswahl: (eine oder mehrere): [Aufgabe: organisationsdefinierte physische Isolationstechniken]; [Aufgabe: organisationsdefinierte logische Isolationstechniken]] in Organisationssystemen und Systemkomponenten ein.	opensearch-in-vpc-only	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass sich Amazon OpenSearch Service-Domains innerhalb einer Amazon Virtual Private Cloud (Amazon VPC) befinden. Eine Amazon OpenSearch Service-Domain innerhalb einer Amazon VPC ermöglicht die sichere Kommunikation zwischen Amazon OpenSearch Service und anderen Services innerhalb der Amazon VPC, ohne dass ein Internet-Gateway, ein NAT-Gerät oder eine VPN-Verbindung erforderlich ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.13.4e	Setzen Sie [Auswahl: (eine oder mehrere): [Aufgabe: organisationsdefinierte physische Isolationstechniken]; [Aufgabe: organisationsdefinierte logische Isolationstechniken]] in Organisationssystemen und Systemkomponenten ein.	nacl-no-unrestricted-ssh-rdp	Der Zugriff auf Remote-Serveradministrationsports in Ihren Network Access Control Lists (NACLs), wie Port 22 (SSH) und Port 3389 (RDP), sollte nicht öffentlich zugänglich sein, da dies einen unbeabsichtigten Zugriff auf Ressourcen innerhalb Ihrer VPC ermöglichen kann.
3.13.4e	Setzen Sie [Auswahl: (eine oder mehrere): [Aufgabe: organisationsdefinierte physische Isolationstechniken]; [Aufgabe: organisationsdefinierte logische Isolationstechniken]] in Organisationssystemen und Systemkomponenten ein.	s3- verboten bucket-level-public-access	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Simple Storage Service (Amazon S3) -Buckets nicht öffentlich zugänglich sind. Diese Regel trägt dazu bei, sensible Daten vor unbefugten Remote-Benutzern zu schützen, indem sie den öffentlichen Zugriff auf Bucket-Ebene verhindert.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.13.4e	Setzen Sie [Auswahl: (eine oder mehrere): [Aufgabe: organisationsdefinierte physische Isolationstechniken]; [Aufgabe: organisationsdefinierte logische Isolationstechniken]] in Organisationssystemen und Systemkomponenten ein.	ssm-document-not-public	Stellen Sie sicher, dass AWS Systems Manager (SSM) - Dokumente nicht öffentlich sind, da dies einen unbeabsichtigten Zugriff auf Ihre SSM-Dokumente ermöglichen kann. Ein öffentliches SSM-Dokument kann Informationen über Ihr Konto, Ihre Ressourcen und internen Prozesse preisgeben.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.13.4e	Setzen Sie [Auswahl: (eine oder mehrere): [Aufgabe: organisationsdefinierte physische Isolationstechniken]; [Aufgabe: organisationsdefinierte logische Isolationstechniken]] in Organisationssystemen und Systemkomponenten ein.	autoscaling-launch-config-public-ip-deaktiviert	Wenn Sie Ihre Netzwerkschnittstellen mit einer öffentlichen IP-Adresse konfigurieren, sind die diesen Netzwerkschnittstellen zugehörigen Ressourcen über das Internet erreichbar. EC2 Ressourcen sollten nicht öffentlich zugänglich sein, da dies einen unbeabsichtigten Zugriff auf Ihre Anwendungen oder Server ermöglichen kann.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.13.4e	Setzen Sie [Auswahl: (eine oder mehrere): [Aufgabe: organisationsdefinierte physische Isolationstechniken]; [Aufgabe: organisationsdefinierte logische Isolationstechniken]] in Organisationssystemen und Systemkomponenten ein.	redshift-enhanced-vpc-routing-aktiviert	Mit Enhanced-VPC-Routing wird erzwungen, dass der gesamte COPY- und UNLOAD-Datenverkehr zwischen Ihrem Cluster und Datenrepositorys über Ihre Amazon VPC erfolgt. Anschließend können Sie VPC-Features wie Sicherheitsgruppen und Netzwerkzugriffskontrolllisten verwenden, um den Netzwerkverkehr zu schützen. Sie können auch VPC-Flow-Logs verwenden, um den Netzwerkverkehr zu überwachen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.13.4e	Setzen Sie [Auswahl: (eine oder mehrere): [Aufgabe: organisationsdefinierte physische Isolationstechniken]; [Aufgabe: organisationsdefinierte logische Isolationstechniken]] in Organisationssystemen und Systemkomponenten ein.	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) Security Groups können bei der Verwaltung des Netzwerkzugriffs helfen, indem sie eine statusbehaftete Filterung von eingehendem und ausgehendem Netzwerkverkehr zu Ressourcen bereitstellen. AWS Wenn Sie eingehenden (oder entfernten) Datenverkehr von 0.0.0.0/0 bis Port 22 auf Ihren Ressourcen nicht zulassen, können Sie den Remote-Zugriff einschränken.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.13.4e	Setzen Sie [Auswahl: (eine oder mehrere): [Aufgabe: organisationsdefinierte physische Isolationstechniken]; [Aufgabe: organisationsdefinierte logische Isolationstechniken]] in Organisationssystemen und Systemkomponenten ein.	restricted-common-ports	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass gemeinsame Ports für Amazon Elastic Compute Cloud (Amazon EC2) -Sicherheitsgruppen eingeschränkt sind. Wenn der Zugriff auf Ports nicht auf vertrauenswürdige Quellen beschränkt wird, kann dies zu Angriffen auf die Verfügbarkeit, Integrität und Vertraulichkeit von Systemen führen. Mit dieser Regel können Sie optional die Parameter blockedPort1–blockedPort5 festlegen (Standardkonfigurationen: 20, 21, 3389, 3306, 4333). Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.13.4e	Setzen Sie [Auswahl: (eine oder mehrere): [Aufgabe: organisationsdefinierte physische Isolationstechniken]; [Aufgabe: organisationsdefinierte logische Isolationstechniken]] in Organisationssystemen und Systemkomponenten ein.	vpc-default-security-group-geschlossen	Sicherheitsgruppen von Amazon Elastic Compute Cloud (Amazon EC2) können bei der Verwaltung des Netzwerkzugriffs helfen, indem sie eine statusbehaftete Filterung des ein- und ausgehenden Netzwerkverkehrs zu Ressourcen bereitstellen. AWS Die Beschränkung des gesamten Datenverkehrs auf die Standardsicherheitsgruppe hilft dabei, den Fernzugriff auf Ihre Ressourcen einzuschränken. AWS

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.13.4e	Setzen Sie [Auswahl: (eine oder mehrere): [Aufgabe: organisationsdefinierte physische Isolationstechniken]; [Aufgabe: organisationsdefinierte logische Isolationstechniken]] in Organisationssystemen und Systemkomponenten ein.	vpc-sg-open-only-to-authorized-ports	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass gemeinsame Ports für Amazon Elastic Compute Cloud (Amazon EC2) -Sicherheitsgruppen eingeschränkt sind. Wenn der Zugriff auf Ports nicht auf vertrauenswürdige Quellen beschränkt wird, kann dies zu Angriffen auf die Verfügbarkeit, Integrität und Vertraulichkeit von Systemen führen. Durch die Beschränkung des Zugriffs auf Ressourcen innerhalb einer Sicherheitsgruppe aus dem Internet (0.0.0.0/0) kann der Fernzugriff auf interne Systeme gesteuert werden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.13.4e	Setzen Sie [Auswahl: (eine oder mehrere): [Aufgabe: organisationsdefinierte physische Isolationstechniken]; [Aufgabe: organisationsdefinierte logische Isolationstechniken]] in Organisationssystemen und Systemkomponenten ein.	no-unrestricted-route-to-igw	Stellen Sie sicher, dass EC2 Amazon-Routentabellen keine uneingeschränkten Routen zu einem Internet-Gateway enthalten. Durch das Entfernen oder Beschränken des Internetzugangs für Workloads innerhalb von Amazon VPCs können unbeabsichtigte Zugriffe in Ihrer Umgebung reduziert werden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.14.1e	Überprüfen Sie die Integrität von [Aufgabe: vom Unternehmen definiert e sicherheitskritische oder unverzichtbare Software] mithilfe von Vertrauenswurzelme chanismen oder kryptografischen Signaturen.	cloud-trail-log-file-Validierung aktiviert	Verwenden Sie die AWS CloudTrail Protokolldateivali dierung, um die Integrität von Protokoll en zu überprüfen. CloudTrail Mithilfe der Protokolldateivali dierung kann festgestellt werden, ob eine Protokoll datei geändert oder gelöscht wurde oder ob sie nach der Übermittlung CloudTrail unverände rt geblieben ist. Dieses Feature wurde mit dem Branchens tandard entsprech enden Algorithmen entwickelt: SHA-256 für die Hashfunktion und SHA-256 mit RSA für digitale Signature n. Aus diesem Grund ist es rechnerisch unmöglich, CloudTrai l Protokolldateien unbemerkt zu ändern, zu löschen oder zu fälschen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.14.2e	Überwachen Sie organisatorische Systeme und Systemkomponenten laufend auf anormales oder verdächtiges Verhalten.	guardduty-enabled-centralized	Amazon GuardDuty kann mithilfe von Threat Intellige nce Feeds helfen, potenzielle Cybersich erheitsereignisse zu überwachen und zu erkennen. Dazu gehören Listen mit bösartigen IPs und maschinel len Lernmethoden zur Identifizierung unerwarteter, nicht autorisierter und bösartiger Aktivitäten in Ihrer AWS Cloud-Umgebung.
3.14.2e	Überwachen Sie organisatorische Systeme und Systemkomponenten laufend auf anormales oder verdächtiges Verhalten.	cloud-trail-cloud-watch-Logs aktiviert	Verwenden Sie Amazon CloudWatc h , um Protokoll ereignisaktivitäten zentral zu sammeln und zu verwalten. Die Aufnahme von AWS CloudTrail Daten liefert Einzelheiten zu den API-Aufrufaktivitä ten in Ihrem AWS-Konto.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.14.2e	Überwachen Sie organisatorische Systeme und Systemkomponenten laufend auf anormales oder verdächtiges Verhalten.	cloudwatch-alarm-action-check	Amazon CloudWatch alarmiert, wenn eine Metrik den Schwellenwert für eine bestimmte Anzahl von Bewertungszeiträumen überschreitet. Der Alarm führt eine oder mehrere Aktionen durch, die vom Wert der Metrik oder des Ausdrucks im Vergleich zu einem Schwellenwert in einer Reihe von Zeiträumen abhängt. Diese Regel erfordert einen Wert für alarmActionRequired (Config Default: True), insufficientDataAction Required (Config Default: True), okActionRequired (Config Default: False). Der tatsächliche Wert muss die Alarmaktionen für Ihre Umgebung widerspiegeln.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.14.2e	Überwachen Sie organisatorische Systeme und Systemkomponenten laufend auf anormales oder verdächtiges Verhalten.	ec2- instance-detailed-monitoring-enabled	Aktivieren Sie diese Regel, um die Amazon Elastic Compute Cloud (Amazon EC2) - Instance-Überwachung auf der EC2 Amazon-Konsole zu verbessern, in der Monitoring-Diagramme mit einem Zeitraum von 1 Minute für die Instance angezeigt werden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.14.2e	Überwachen Sie organisatorische Systeme und Systemkomponenten laufend auf anormales oder verdächtiges Verhalten.	rds-enhanced-monitoring-enabled	Aktivieren Sie Amazon Relational Database Service (Amazon RDS), um die Verfügbarkeit von Amazon RDS zu überwachen. Dies bietet einen detaillierten Einblick in den Zustand Ihrer Amazon-RDS-Datenbank-Instances. Wenn der Amazon-RDS-Speicher mehr als ein zugrunde liegendes physisches Gerät verwendet, erfasst Enhanced Monitoring die Daten für jedes Gerät. Wenn die Datenbank-Instance von Amazon RDS in einer Multi-AZ-Bereitstellung ausgeführt wird, werden außerdem die Daten für jedes Gerät auf dem sekundären Host sowie die Metriken des sekundären Hosts erfasst.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.14.2e	Überwachen Sie organisatorische Systeme und Systemkomponenten laufend auf anormales oder verdächtiges Verhalten.	vpc-flow-logs-enabled	VPC-Flow-Protokolle erfassen detaillierte Informationsdatensätze über den IP-Datenverkehr, der zu und von Netzwerkschnittstellen in Ihrer Amazon Virtual Private Cloud (Amazon VPC) fließt. Standardmäßig enthalten Flow-Protokolldatensätze Werte für die verschiedenen Komponenten des IP-Flows, einschließlich Quelle, Ziel und Protokoll.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.14.2e	Überwachen Sie organisatorische Systeme und Systemkomponenten laufend auf anormales oder verdächtiges Verhalten.	securityhub-enabled	AWS Security Hub hilft bei der Überwachung von unbefugtem Personal, Verbindungen, Geräten und Software. AWS Security Hub aggregiert, organisiert und priorisiert die Sicherheitswarnungen oder Ergebnisse mehrerer Dienste. AWS Einige dieser Dienste sind Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer und AWS Firewall Manager sowie AWS Partnerlösungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.14.6e	Verwendung von Informationen über Bedrohungsindikatoren und wirksame Abhilfemaßnahmen, die von [Zuweisung: vom Unternehmen definierte externe Organisationen] erhalten wurden, um die Erkennung von Eindringlingen und die Suche nach Bedrohungen zu steuern und zu informieren.	guardduty-enabled-centralized	Amazon GuardDuty kann mithilfe von Threat Intelligence Feeds helfen, potenzielle Cybersicherheitsereignisse zu überwachen und zu erkennen. Dazu gehören Listen mit bösartigen IPs und maschinellen Lernmethoden zur Identifizierung unerwarteter, nicht autorisierter und bösartiger Aktivitäten in Ihrer AWS Cloud-Umgebung.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.14.7e	Überprüfen Sie die Richtigkeit von [Zuordnung: organisationsdefinierte sicherheitskritische oder wesentliche Software-, Firmware- und Hardwarekomponenten] mithilfe von [Aufgabe: organisationsdefinierte Überprüfungsmethoden oder -techniken].	ec2-check managedinstance-association-compliance-status	Verwenden Sie AWS Systems Manager Associations, um bei der Inventarisierung von Softwareplattformen und Anwendungen innerhalb eines Unternehmens zu helfen. AWS Systems Manager weist Ihren verwalteten Instanzen einen Konfigurationsstatus zu und ermöglicht es Ihnen, Basiswerte für Betriebssystem-Patch-Levels, Softwareinstallationen, Anwendungskonfigurationen und andere Details zu Ihrer Umgebung festzulegen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.14.7e	Überprüfen Sie die Richtigkeit von [Zuordnung: organisationsdefinierte sicherheitskritische oder wesentliche Software-, Firmware- und Hardwarekomponenten] mithilfe von [Aufgabe: organisationsdefinierte Überprüfungsmethoden oder -techniken].	ec2-check managedinstance-patch-compliance-status	Aktivieren Sie diese Regel, um bei der Identifizierung und Dokumentation von Sicherheitslücken in Amazon Elastic Compute Cloud (Amazon EC2) zu helfen. Die Regel prüft, ob die EC2 Amazon-Instance die Patch-Konformität im AWS Systems Manager gemäß den Richtlinien und Verfahren Ihrer Organisation einhält.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.14.7e	Überprüfen Sie die Richtigkeit von [Zuordnung: organisationsdefinierte sicherheitskritische oder wesentliche Software-, Firmware- und Hardwarekomponenten] mithilfe von [Aufgabe: organisationsdefinierte Überprüfungsmethoden oder -techniken].	ec2-manager instance-managed-by-systems	Eine Bestandsaufnahme der Softwareplattformen und Anwendungen innerhalb des Unternehmens ist möglich, indem Amazon Elastic Compute Cloud (Amazon EC2) - Instances mit AWS Systems Manager verwaltet werden. Verwenden Sie AWS Systems Manager, um detaillierte Systemkonfigurationen, Betriebssystem-Patch-Levels, Namen und Typ der Dienste, Softwareinstallationen, Anwendungsname, Herausgeber und Version sowie andere Details zu Ihrer Umgebung bereitzustellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.14.7e	Überprüfen Sie die Richtigkeit von [Zuordnung: organisationsdefinierte sicherheitskritische oder wesentliche Software-, Firmware- und Hardwarekomponenten] mithilfe von [Aufgabe: organisationsdefinierte Überprüfungsmethoden oder -techniken].	ecs-fargate-latest-platform-Version	Sicherheitsupdates und Patches werden automatisch für Ihre AWS Fargate-Aufgaben bereitgestellt. Wenn ein Sicherheitsproblem gefunden wird, das eine AWS Fargate-Plattformversion betrifft, AWS wird die Plattformversion gepatcht. Um Sie bei der Patchverwaltung Ihrer Amazon Elastic Container Service (ECS) - Aufgaben zu unterstützen, auf denen AWS Fargate ausgeführt wird, aktualisieren Sie Ihre eigenständigen Service-Aufgaben, sodass sie die neueste Plattformversion verwenden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.14.7e	Überprüfen Sie die Richtigkeit von [Zuordnung: organisationsdefinierte sicherheitskritische oder wesentliche Software-, Firmware- und Hardwarekomponenten] mithilfe von [Aufgabe: organisationsdefinierte Überprüfungsmethoden oder -techniken].	ecr-private-image-scanning-aktiviert	Der Amazon Elastic Container Repository (ECR)-Image-Scan unterstützt die Identifizierung von Software-Schwachstellen in Ihren Container-Images. Durch die Aktivierung von Image-Scans in ECR-Repositorys werden die Integrität und Sicherheit der gespeicherten Images mit einer zusätzlichen Überprüfungsebene verbessert.

Vorlage

Die Vorlage ist verfügbar unter GitHub: Operational Best Practices for NIST 800 172.

Bewährte Methoden für die Ausführung von NIST 800 181

Konformitätspakete bieten ein allgemeines Compliance-Framework, das es Ihnen ermöglicht, mithilfe verwalteter oder benutzerdefinierter AWS Config Regeln und Abhilfemaßnahmen Kontrollen zur Sicherheits-, Betriebs- oder Kostenoptimierung durchzuführen. AWS Config Conformance Packs dienen als Beispielvorlagen nicht dazu, die vollständige Einhaltung eines bestimmten Governance- oder Compliance-Standards sicherzustellen. Sie sind dafür verantwortlich, selbst zu beurteilen, ob Ihre Nutzung der Services den geltenden gesetzlichen und behördlichen Anforderungen entspricht.

Im Folgenden finden Sie ein Beispiel für eine Zuordnung zwischen den NIST 800 181- und AWS verwalteten Konfigurationsregeln. Jede Config-Regel gilt für eine bestimmte AWS Ressource und

bezieht sich auf eine oder mehrere NIST 800 181-Steuerelemente. Eine Kontrolle nach NIST 800-181 kann mehreren Konfigurationsregeln zugeordnet werden. In der folgenden Tabelle finden Sie weitere Informationen und Anleitungen zu diesen Zuordnungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0008	Analysieren und planen Sie erwartete Änderungen der Datenkapazitätsanforderungen.	dynamodb-autoscaling-enabled	Amazon DynamoDB Auto Scaling verwendet den AWS Application Auto Scaling-Service, um die bereitgestellte Durchsatzkapazität so anzupassen, dass sie automatisch auf tatsächliche Verkehrsmuster reagiert. Auf diese Weise kann eine Tabelle oder ein globaler sekundärer Index die bereitgestellte Lese-/Schreibkapazität erhöhen, um plötzliche Erhöhungen des Datenverkehrs ohne Drosselung zu bewältigen.
T0008	Analysieren und planen Sie erwartete Änderungen der Datenkapazitätsanforderungen.	dynamodb-in-backup-plan	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon DynamoDB-Tabellen

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwaltet er Backup-Service mit einer richtlini enbasierten Backup-Lösung. Diese Lösung vereinfac ht Ihr Sicherung smanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforde rungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0008	Analysieren und planen Sie erwartete Änderungen der Datenkapazitätsanforderungen.	dynamodb-pitr-enabled	Aktivieren Sie diese Regel, um zu überprüfen, ob die Informationen gesichert wurden. Es verwaltet auch die Backups, indem es sicherstellt, dass die point-in-time Wiederherstellung in Amazon DynamoDB aktiviert ist. Bei der Wiederherstellung werden fortlaufende Backups Ihrer Tabelle für die letzten 35 Tage gespeichert.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0008	Analysieren und planen Sie erwartete Änderungen der Datenkapazitätsanforderungen.	dynamodb-throughput-limit-check	Aktivieren Sie diese Regel, um sicherzustellen, dass die bereitgestellte Durchsatzkapazität in Ihren Amazon-DynamoDB-Tabellen überprüft wird. Dies ist der Umfang der Lese- und Schreibaktivitäten, der von den jeweiligen Tabellen unterstützt werden kann. DynamoDB verwendet diese Informationen für das Reservieren ausreichender Systemressourcen, um Ihren Durchsatz anforderungen gerecht zu werden. Diese Regel generiert eine Warnung, wenn sich der Durchsatz dem Höchstlimit für ein Kundenkonto nähert. Mit dieser Regel können Sie optional die Parameter RCUThreshold Kontoprozentsatz

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			(Konfigurationsstandard: 80) und WCUThreshold Kontoprozentsatz (Konfigurationsstandard: 80) festlegen. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0008	Analysieren und planen Sie erwartete Änderungen der Datenkapazitätsanforderungen.	ebs-in-backup-plan	Stellen Sie zur Unterstützung der Datensicherungsprozesse sicher, dass Ihre Amazon Elastic Block Store (Amazon EBS) -Volumes Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihre Backup-Verwaltung und ermöglicht es Ihnen, Ihre geschäftlichen und behördlichen Anforderungen bezüglich Backups zu erfüllen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0008	Analysieren und planen Sie erwartete Änderungen der Datenkapazitätsanforderungen.	efs-in-backup-plan	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon Elastic File System (Amazon EFS) -Dateisysteme Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0008	Analysieren und planen Sie erwartete Änderungen der Datenkapazitätsanf orderungen.	elasticache-redis-cluster-automatic-Backup-Check	Wenn automatische Backups aktiviert sind, ElastiCache erstellt Amazon täglich ein Backup des Clusters. Die Sicherung kann für eine von Ihrer Organisation festgelegte Anzahl von Tagen aufbewahrt werden. Automatische Backups schützen vor Datenverlust. Bei einem Ausfall können Sie einen neuen Cluster erstellen, der Ihre Daten aus dem aktuellen Backup wiederherstellt.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0008	Analysieren und planen Sie erwartete Änderungen der Datenkapazitätsanforderungen.	elb-cross-zone-load-Balancing aktiviert	Aktivieren Sie zonenübergreifendes Load Balancing für Ihre Elastic Load Balancer (ELBs), um eine angemessene Kapazität und Verfügbarkeit aufrechtzuerhalten. Zonenübergreifendes Load Balancing reduziert die Notwendigkeit, die gleiche Anzahl von Instances in jeder aktivierten Availability Zone aufrechtzuerhalten. Es verbessert auch die Fähigkeit Ihrer Anwendung, den Verlust einer oder mehrerer Instances zu bewältigen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0008	Analysieren und planen Sie erwartete Änderungen der Datenkapazitätsanf orderungen.	rds-in-backup-plan	Um Sie bei Datensich erungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon Relational Database Service (Amazon RDS) -Instance s Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwaltet er Backup-Service mit einer richtlini enbasierten Backup-Lösung. Diese Lösung vereinfac ht Ihr Sicherung smanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforde rungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0008	Analysieren und planen Sie erwartete Änderungen der Datenkapazitätsanforderungen.	rds-multi-az-support	Die Multi-AZ-Unterstützung in Amazon Relational Database Service (Amazon RDS) bietet eine verbesserte Verfügbarkeit und Beständigkeit von Datenbank-Instances. Wenn Sie eine Multi-AZ-Datenbank-Instance bereitstellen, erstellt Amazon RDS automatisch eine primäre Datenbank-Instance und repliziert die Daten synchron auf eine Standby-Instance in einer anderen Availability Zone. Jede Availability Zone läuft auf einer eigenen, physisch getrennten, unabhängigen Infrastruktur und ist auf eine hohe Verfügbarkeit ausgelegt. Im Falle eines Infrastrukturausfalls führt Amazon RDS einen automatis

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			chen Failover zum Standby-Modus durch, sodass Sie den Datenbankbetrieb wieder aufnehmen können, sobald der Failover abgeschlo ssen ist.
T0008	Analysieren und planen Sie erwartete Änderungen der Datenkapazitätsanf orderungen.	redshift-backup-en abled	Stellen Sie zur Unterstützung der Datensicherungspro zesse sicher, dass Ihre Amazon-Re dshift-Cluster über automatisierte Snapshots verfügen. Wenn automatis ierte Snapshots für einen Cluster aktiviert sind, erstellt Redshift in regelmäßi gen Abständen Snapshots dieses Clusters. Standardm äßig erstellt Redshift alle acht Stunden oder alle 5 GB einen Snapshot für jeden Knoten mit Datenände rungen oder je nachdem, was zuerst eintritt.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0008	Analysieren und planen Sie erwartete Änderungen der Datenkapazitätsanf orderungen.	s3- bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) unterstützt die Aufrechterhaltung einer angemesse nen Kapazität und Verfügbarkeit. CRR ermöglicht das automatische, asynchrone Kopieren von Objekten in Amazon S3 Buckets, um die Datenverf ügbarkeit sicherzus tellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0008	Analysieren und planen Sie erwartete Änderungen der Datenkapazitätsanforderungen.	backup-plan-min-frequency-and-min-retention-check	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihr AWS Backup-Plan auf eine Mindestfrequenz und Aufbewahrung festgelegt ist. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen. Mit dieser Regel können Sie die Parameter requiredFrequencyValue (Config default: 1), requiredRetentionDays (Config default: 35) und requiredFrequencyUnit

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			(Config default: days) festlegen. Der tatsächliche Wert muss den Anforderungen Ihrer Organisation entsprechen.
T0008	Analysieren und planen Sie erwartete Änderungen der Datenkapazitätsanforderungen.	ec2-plan resources-protected-by-backup	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon Elastic Compute Cloud (Amazon EC2) -Ressourcen Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0017	Wenden Sie die Prinzipien der serviceorientierten Sicherheitsarchitektur an, um die Anforderungen des Unternehmens an Vertraulichkeit, Integrität und Verfügbarkeit zu erfüllen.	acm-certificate-expiration-check	Stellen Sie sicher, dass die Netzwerkintegrität geschützt ist, indem Sie sicherstellen, dass X509-Zertifikate von ACM ausgestellt werden. AWS Diese Zertifikate müssen gültig und dürfen nicht abgelaufen sein. Für diese Regel ist ein Wert für erforderlich daysToExpiration (Wert für bewährte AWS Grundregeln für Sicherheit: 90). Der tatsächliche Wert muss den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0017	Wenden Sie die Prinzipien der serviceorientierten Sicherheitsarchitektur an, um die Anforderungen des Unternehmens an Vertraulichkeit, Integrität und Verfügbarkeit zu erfüllen.	alb-http-to-https-Umleitungsprüfung	Um Daten während der Übertragung zu schützen, stellen Sie sicher, dass Ihr Application Load Balancer unverschlüsselte HTTP-Anfragen automatisch an HTTPS umleitet. Da sensible Daten vorhanden sein können, sollten Sie die Verschlüsselung bei der Übertragung aktivieren, um diese Daten zu schützen.
T0017	Wenden Sie die Prinzipien der serviceorientierten Sicherheitsarchitektur an, um die Anforderungen des Unternehmens an Vertraulichkeit, Integrität und Verfügbarkeit zu erfüllen.	api-gw-cache-enabled-und-verschlüsselt	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass die Verschlüsselung für den Cache Ihrer API-Gateway-Stufe aktiviert ist. Da für die API-Methode sensible Daten erfasst werden können, sollten Sie die Verschlüsselung von Daten im Ruhezustand aktivieren, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0017	Wenden Sie die Prinzipien der serviceorientierten Sicherheitsarchitektur an, um die Anforderungen des Unternehmens an Vertraulichkeit, Integrität und Verfügbarkeit zu erfüllen.	autoscaling-launch-config-public-ip-deaktiviert	Wenn Sie Ihre Netzwerkschnittstellen mit einer öffentlichen IP-Adresse konfigurieren, sind die diesen Netzwerkschnittstellen zugehörigen Ressourcen über das Internet erreichbar. EC2 Ressourcen sollten nicht öffentlich zugänglich sein, da dies einen unbeabsichtigten Zugriff auf Ihre Anwendungen oder Server ermöglichen kann.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0017	Wenden Sie die Prinzipien der serviceorientierten Sicherheitsarchitektur an, um die Anforderungen des Unternehmens an Vertraulichkeit, Integrität und Verfügbarkeit zu erfüllen.	backup-plan-min-frequency-and-min-retention-check	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihr AWS Backup-Plan auf eine Mindestfrequenz und Aufbewahrung festgelegt ist. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen. Mit dieser Regel können Sie die Parameter requiredFrequencyValue (Config default: 1), requiredRetentionDays (Config default: 35) und requiredFrequencyUnit

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			(Config default: days) festlegen. Der tatsächliche Wert muss den Anforderungen Ihrer Organisation entsprechen.
T0017	Wenden Sie die Prinzipien der serviceorientierten Sicherheitsarchitektur an, um die Anforderungen des Unternehmens an Vertraulichkeit, Integrität und Verfügbarkeit zu erfüllen.	backup-recovery-point-manual-löschen-deaktiviert	Stellen Sie sicher, dass Ihren AWS Backup-Wiederherstellungspunkten eine ressourcenbasierte Richtlinie zugeordnet ist, die das Löschen von Wiederherstellungspunkten verhindert. Die Verwendung einer ressourcenbasierten Richtlinie zur Verhinderung des Löschens von Wiederherstellungspunkten kann dazu beitragen, ein versehentliches oder absichtliches Löschen zu unterbinden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0017	Wenden Sie die Prinzipien der serviceorientierten Sicherheitsarchitektur an, um die Anforderungen des Unternehmens an Vertraulichkeit, Integrität und Verfügbarkeit zu erfüllen.	cloud-trail-encryption-enabled	Zum Schutz von eventuell vorhandenen sensiblen Daten sowie Daten im Ruhezustand müssen Sie sicherstellen, dass die Verschlüsselung für Ihre AWS CloudTrail aktiviert ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0017	Wenden Sie die Prinzipien der serviceorientierten Sicherheitsarchitektur an, um die Anforderungen des Unternehmens an Vertraulichkeit, Integrität und Verfügbarkeit zu erfüllen.	cloud-trail-log-file-Validierung aktiviert	Verwenden Sie die AWS CloudTrail Protokolldateivalidierung, um die Integrität von Protokollen zu überprüfen. CloudTrail Mithilfe der Protokolldateivalidierung kann festgestellt werden, ob eine Protokolldatei geändert oder gelöscht wurde oder ob sie nach der Übermittlung CloudTrail unverändert geblieben ist. Dieses Feature wurde mit dem Branchenstandard entsprechenden Algorithmen entwickelt: SHA-256 für die Hashfunktion und SHA-256 mit RSA für digitale Signaturen. Das macht es rechnerisch unmöglich, CloudTrail Protokolldateien unbemerkt zu ändern, zu löschen oder zu fälschen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0017	Wenden Sie die Prinzipien der serviceorientierten Sicherheitsarchitektur an, um die Anforderungen des Unternehmens an Vertraulichkeit, Integrität und Verfügbarkeit zu erfüllen.	cmk-backing-key-rotation-aktiviert	Aktivieren Sie die Schlüsselrotation, um sicherzustellen, dass Schlüssel rotiert werden, sobald sie das Ende ihrer Kryptoperiode erreicht haben.
T0017	Wenden Sie die Prinzipien der serviceorientierten Sicherheitsarchitektur an, um die Anforderungen des Unternehmens an Vertraulichkeit, Integrität und Verfügbarkeit zu erfüllen.	db-instance-backup-enabled	Die Sicherungsfunktion von Amazon RDS erstellt Sicherungen Ihrer Datenbanken und Transaktionsprotokolle. Amazon RDS erstellt einen Snapshot für das Speichervolume Ihrer DB-Instance, sodass die gesamte DB-Instance gesichert wird. Sie können im System spezifische Aufbewahrungsfristen festlegen, um Ihre Ausfallsicherheitsanforderungen zu erfüllen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0017	Wenden Sie die Prinzipien der serviceorientierten Sicherheitsarchitektur an, um die Anforderungen des Unternehmens an Vertraulichkeit, Integrität und Verfügbarkeit zu erfüllen.	dms-replication-not-public	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass auf DMS-Replikationsinstanzen nicht öffentlich zugegriffen werden kann. DMS-Replikations-Instances können vertrauliche Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0017	Wenden Sie die Prinzipien der serviceorientierten Sicherheitsarchitektur an, um die Anforderungen des Unternehmens an Vertraulichkeit, Integrität und Verfügbarkeit zu erfüllen.	dynamodb-autoscaling-enabled	Amazon DynamoDB Auto Scaling verwendet den AWS Application Auto Scaling-Service, um die bereitgestellte Durchsatzkapazität so anzupassen, dass sie automatisch auf tatsächliche Verkehrsmuster reagiert. Auf diese Weise kann eine Tabelle oder ein globaler sekundärer Index die bereitgestellte Lese-/Schreibkapazität erhöhen, um plötzliche Erhöhungen des Datenverkehrs ohne Drosselung zu bewältigen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0017	Wenden Sie die Prinzipien der serviceorientierten Sicherheitsarchitektur an, um die Anforderungen des Unternehmens an Vertraulichkeit, Integrität und Verfügbarkeit zu erfüllen.	dynamodb-pitr-enabled	Aktivieren Sie diese Regel, um zu überprüfen, ob die Informationen gesichert wurden. Es verwaltet auch die Backups, indem es sicherstellt, dass die point-in-time Wiederherstellung in Amazon DynamoDB aktiviert ist. Bei der Wiederherstellung werden fortlaufende Backups Ihrer Tabelle für die letzten 35 Tage gespeichert.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0017	Wenden Sie die Prinzipien der serviceorientierten Sicherheitsarchitektur an, um die Anforderungen des Unternehmens an Vertraulichkeit, Integrität und Verfügbarkeit zu erfüllen.	ebs-in-backup-plan	Stellen Sie zur Unterstützung der Datensicherungsprozesse sicher, dass Ihre Amazon Elastic Block Store (Amazon EBS) -Volumes Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihre Backup-Verwaltung und ermöglicht es Ihnen, Ihre geschäftlichen und behördlichen Anforderungen bezüglich Backups zu erfüllen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0017	Wenden Sie die Prinzipien der serviceorientierten Sicherheitsarchitektur an, um die Anforderungen des Unternehmens an Vertraulichkeit, Integrität und Verfügbarkeit zu erfüllen.	ebs-snapshot-public-restorable-überprüfen	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass EBS-Snapshots nicht öffentlich wiederherstellbar sind. EBS-Volume-Snapshots können vertrauliche Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.
T0017	Wenden Sie die Prinzipien der serviceorientierten Sicherheitsarchitektur an, um die Anforderungen des Unternehmens an Vertraulichkeit, Integrität und Verfügbarkeit zu erfüllen.	ec-2 ebs-encryption-by-default	Zum Schutz von Daten im Ruhezustand müssen Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon Elastic Block Store (Amazon EBS)-Volumes aktiviert ist. Da sensible Daten in diesen Volumes gespeichert werden können, sollten Sie die Verschlüsselung von Daten im Ruhezustand aktivieren, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0017	Wenden Sie die Prinzipien der serviceorientierten Sicherheitsarchitektur an, um die Anforderungen des Unternehmens an Vertraulichkeit, Integrität und Verfügbarkeit zu erfüllen.	ec2- instance-no-public-ip	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon Elastic Compute Cloud (Amazon EC2) - Instances nicht öffentlich zugänglich sind. EC2Amazon -Instances können vertrauliche Informationen enthalten, und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0017	Wenden Sie die Prinzipien der serviceorientierten Sicherheitsarchitektur an, um die Anforderungen des Unternehmens an Vertraulichkeit, Integrität und Verfügbarkeit zu erfüllen.	ec2--Plan resources-protected-by-backup	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon Elastic Compute Cloud (Amazon EC2) -Ressourcen Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0017	Wenden Sie die Prinzipien der serviceorientierten Sicherheitsarchitektur an, um die Anforderungen des Unternehmens an Vertraulichkeit, Integrität und Verfügbarkeit zu erfüllen.	efs-encrypted-check	Aktivieren Sie die Verschlüsselung für Ihr Amazon Elastic File System (EFS), um eventuell vorhandene sensible Daten sowie Daten im Ruhezustand zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0017	Wenden Sie die Prinzipien der serviceorientierten Sicherheitsarchitektur an, um die Anforderungen des Unternehmens an Vertraulichkeit, Integrität und Verfügbarkeit zu erfüllen.	efs-in-backup-plan	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon Elastic File System (Amazon EFS) -Dateisysteme Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0017	Wenden Sie die Prinzipien der serviceorientierten Sicherheitsarchitektur an, um die Anforderungen des Unternehmens an Vertraulichkeit, Integrität und Verfügbarkeit zu erfüllen.	elasticache-redis-cluster-automatic-Backup-Check	Wenn automatische Backups aktiviert sind, ElastiCache erstellt Amazon täglich ein Backup des Clusters. Die Sicherung kann für eine von Ihrer Organisation festgelegte Anzahl von Tagen aufbewahrt werden. Automatische Backups schützen vor Datenverlust. Bei einem Ausfall können Sie einen neuen Cluster erstellen, der Ihre Daten aus dem aktuellen Backup wiederherstellt.
T0017	Wenden Sie die Prinzipien der serviceorientierten Sicherheitsarchitektur an, um die Anforderungen des Unternehmens an Vertraulichkeit, Integrität und Verfügbarkeit zu erfüllen.	elasticsearch-encrypted-at-rest	Da sensible Daten vorhanden sein können und um Daten im Ruhezustand zu schützen, sollten Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon OpenSearch Service (OpenSearch Service) -Domains aktiviert ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0017	Wenden Sie die Prinzipien der serviceorientierten Sicherheitsarchitektur an, um die Anforderungen des Unternehmens an Vertraulichkeit, Integrität und Verfügbarkeit zu erfüllen.	elasticsearch-node-to-node-Verschlüsselungsprüfung	Stellen Sie sicher, dass die node-to-node Verschlüsselung für Amazon OpenSearch Service aktiviert ist. Node-to-nodeVerschlüsselung ermöglicht die TLS 1.2-Verschlüsselung für die gesamte Kommunikation innerhalb der Amazon Virtual Private Cloud (Amazon VPC). Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0017	Wenden Sie die Prinzipien der serviceorientierten Sicherheitsarchitektur an, um die Anforderungen des Unternehmens an Vertraulichkeit, Integrität und Verfügbarkeit zu erfüllen.	elbv-2 acm-certificate-required	Zum Schutz von eventuell vorhandenen sensiblen Daten sowie von Daten während der Übertragung muss die Verschlüsselung für Ihr Elastic Load Balancing aktiviert sein. Verwenden Sie AWS Certificate Manager, um öffentliche und private SSL/TLS-Zertifikate mit AWS Diensten und internen Ressourcen zu verwalten, bereitzustellen und bereitzustellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0017	Wenden Sie die Prinzipien der serviceorientierten Sicherheitsarchitektur an, um die Anforderungen des Unternehmens an Vertraulichkeit, Integrität und Verfügbarkeit zu erfüllen.	elb-acm-certificate-required	Zum Schutz von eventuell vorhandenen sensiblen Daten sowie von Daten während der Übertragung muss die Verschlüsselung für Ihr Elastic Load Balancing aktiviert sein. Verwenden Sie AWS Certificate Manager, um öffentliche und private SSL/TLS-Zertifikate mit AWS Diensten und internen Ressourcen zu verwalten, bereitzustellen und bereitzustellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0017	Wenden Sie die Prinzipien der serviceorientierten Sicherheitsarchitektur an, um die Anforderungen des Unternehmens an Vertraulichkeit, Integrität und Verfügbarkeit zu erfüllen.	elb-cross-zone-load-Balancing aktiviert	Aktivieren Sie zonenübergreifendes Load Balancing für Ihre Elastic Load Balancer (ELBs), um eine angemessene Kapazität und Verfügbarkeit aufrechtzuerhalten. Zonenübergreifendes Load Balancing reduziert die Notwendigkeit, die gleiche Anzahl von Instances in jeder aktivierten Availability Zone aufrechtzuerhalten. Es verbessert auch die Fähigkeit Ihrer Anwendung, den Verlust einer oder mehrerer Instances zu bewältigen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0017	Wenden Sie die Prinzipien der serviceorientierten Sicherheitsarchitektur an, um die Anforderungen des Unternehmens an Vertraulichkeit, Integrität und Verfügbarkeit zu erfüllen.	elb-deletion-protection-enabled	Diese Regel sorgt dafür, dass der Löschschutz für Elastic Load Balancing aktiviert ist. Verwenden Sie diese Funktion, um zu verhindern, dass Ihr Load Balancer versehentlich oder böswillig gelöscht wird, was zum Verlust der Verfügbarkeit Ihrer Anwendungen führen kann.
T0017	Wenden Sie die Prinzipien der serviceorientierten Sicherheitsarchitektur an, um die Anforderungen des Unternehmens an Vertraulichkeit, Integrität und Verfügbarkeit zu erfüllen.	elb-tls-https-listeners-nur	Stellen Sie sicher, dass Ihre Elastic Load Balancer (ELBs) mit SSL- oder HTTPS-Listenern konfiguriert sind. Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0017	Wenden Sie die Prinzipien der serviceorientierten Sicherheitsarchitektur an, um die Anforderungen des Unternehmens an Vertraulichkeit, Integrität und Verfügbarkeit zu erfüllen.	emr-master-no-public-ip	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon EMR-Cluster-Masterknoten nicht öffentlich zugänglich sind. Amazon-EMR-Cluster-Hauptknoten können vertrauliche Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.
T0017	Wenden Sie die Prinzipien der serviceorientierten Sicherheitsarchitektur an, um die Anforderungen des Unternehmens an Vertraulichkeit, Integrität und Verfügbarkeit zu erfüllen.	encrypted-volumes	Aktivieren Sie die Verschlüsselung für Ihre Amazon-Elastic-Block-Store-(Amazon-EBS-)Volumes, um eventuell vorhandene sensible Daten sowie Daten im Ruhezustand zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0017	Wenden Sie die Prinzipien der serviceorientierten Sicherheitsarchitektur an, um die Anforderungen des Unternehmens an Vertraulichkeit, Integrität und Verfügbarkeit zu erfüllen.	kms-cmk-not-scheduled-zum Löschen	Um Daten im Ruhezustand zu schützen, sollten Sie sicherstellen, dass die für den Kunden erforderlichen Masterschlüssel (CMKs) nicht für das Löschen im AWS Key Management Service (AWS KMS) vorgesehen sind. Da Schlüssel manchmal gelöscht werden müssen, können Sie mit dieser Regel alle zu löschenden Schlüssel überprüfen, falls ein Schlüssel versehentlich zur Löschung vorgemerkt wurde.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0017	Wenden Sie die Prinzipien der serviceorientierten Sicherheitsarchitektur an, um die Anforderungen des Unternehmens an Vertraulichkeit, Integrität und Verfügbarkeit zu erfüllen.	lambda-function-public-access-verboten	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass AWS Lambda-Funktionen nicht öffentlich zugänglich sind. Der öffentliche Zugriff kann möglicherweise die Verfügbarkeit von Ressourcen beeinträchtigen.
T0017	Wenden Sie die Prinzipien der serviceorientierten Sicherheitsarchitektur an, um die Anforderungen des Unternehmens an Vertraulichkeit, Integrität und Verfügbarkeit zu erfüllen.	opensearch-encrypted-at-rest	Aktivieren Sie die Verschlüsselung für Ihre Domains im Amazon Elasticsearch Service (Amazon ES), um eventuell vorhandene sensible Daten sowie Daten im Ruhezustand zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0017	Wenden Sie die Prinzipien der serviceorientierten Sicherheitsarchitektur an, um die Anforderungen des Unternehmens an Vertraulichkeit, Integrität und Verfügbarkeit zu erfüllen.	opensearch-node-to-node-Verschlüsselungsprüfung	Stellen Sie sicher, dass die node-to-node Verschlüsselung für Amazon OpenSearch Service aktiviert ist. Node-to-nodeVerschlüsselung ermöglicht die TLS 1.2-Verschlüsselung für die gesamte Kommunikation innerhalb der Amazon Virtual Private Cloud (Amazon VPC). Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0017	Wenden Sie die Prinzipien der serviceorientierten Sicherheitsarchitektur an, um die Anforderungen des Unternehmens an Vertraulichkeit, Integrität und Verfügbarkeit zu erfüllen.	rds-instance-deletion-protection-aktiviert	Stellen Sie sicher, dass Amazon Relational Database Service (Amazon RDS)-Instances den Löschschutz aktiviert haben. Verwenden Sie den Löschschutz, um zu verhindern, dass Ihre Amazon-RDS-Instances versehentlich oder böswillig gelöscht werden, was zum Verlust der Verfügbarkeit Ihrer Anwendungen führen kann.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0017	Wenden Sie die Prinzipien der serviceorientierten Sicherheitsarchitektur an, um die Anforderungen des Unternehmens an Vertraulichkeit, Integrität und Verfügbarkeit zu erfüllen.	rds-instance-public-access-überprüfen	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Relational Database Service (Amazon RDS) -Instances nicht öffentlich sind. Amazon-RDS-Datenbank-Instances können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0017	Wenden Sie die Prinzipien der serviceorientierten Sicherheitsarchitektur an, um die Anforderungen des Unternehmens an Vertraulichkeit, Integrität und Verfügbarkeit zu erfüllen.	rds-in-backup-plan	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon Relational Database Service (Amazon RDS) -Instances Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0017	Wenden Sie die Prinzipien der serviceorientierten Sicherheitsarchitektur an, um die Anforderungen des Unternehmens an Vertraulichkeit, Integrität und Verfügbarkeit zu erfüllen.	rds-multi-az-support	Die Multi-AZ-Unterstützung in Amazon Relational Database Service (Amazon RDS) bietet eine verbesserte Verfügbarkeit und Beständigkeit von Datenbank-Instances. Wenn Sie eine Multi-AZ-Datenbank-Instance bereitstellen, erstellt Amazon RDS automatisch eine primäre Datenbank-Instance und repliziert die Daten synchron auf eine Standby-Instance in einer anderen Availability Zone. Jede Availability Zone läuft auf einer eigenen, physisch getrennten, unabhängigen Infrastruktur und ist auf eine hohe Verfügbarkeit ausgelegt. Im Falle eines Infrastrukturausfalls führt Amazon RDS einen automatis

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			chen Failover zum Standby-Modus durch, sodass Sie den Datenbankbetrieb wieder aufnehmen können, sobald der Failover abgeschlo ssen ist.
T0017	Wenden Sie die Prinzipien der serviceorientierten Sicherheitsarchitektur an, um die Anforderu ngen des Unternehm ens an Vertrauli chkeit, Integrität und Verfügbarkeit zu erfüllen.	rds-snapshots-public-prohibited	Verwalten Sie den Zugriff auf Ressource n in der AWS Cloud, indem Sie sicherste llen, dass Amazon Relational Database Service (Amazon RDS) -Instance s nicht öffentlic h sind. Amazon-RDS-Datenbank-Instances können vertrauliche Informati onen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0017	Wenden Sie die Prinzipien der serviceorientierten Sicherheitsarchitektur an, um die Anforderungen des Unternehmens an Vertraulichkeit, Integrität und Verfügbarkeit zu erfüllen.	rds-snapshot-encrypted	Stellen Sie sicher, dass die Verschlüsselung für Ihre Amazon Relational Database Service (Amazon RDS)-Snapshots aktiviert ist. Da sensible Daten auch im Ruhezustand vorhanden sein können, sollten Sie die Verschlüsselung von Daten im Ruhezustand aktivieren, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0017	Wenden Sie die Prinzipien der serviceorientierten Sicherheitsarchitektur an, um die Anforderungen des Unternehmens an Vertraulichkeit, Integrität und Verfügbarkeit zu erfüllen.	rds-storage-encrypted	Zum Schutz von Daten im Ruhezustand müssen Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon Relational Database Service (Amazon RDS)-Instances aktiviert ist. Da sensible Daten in Amazon-RDS-Instances gespeichert werden können, sollten Sie die Verschlüsselung von Daten im Ruhezustand aktivieren, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0017	Wenden Sie die Prinzipien der serviceorientierten Sicherheitsarchitektur an, um die Anforderungen des Unternehmens an Vertraulichkeit, Integrität und Verfügbarkeit zu erfüllen.	redshift-backup-enabled	Stellen Sie zur Unterstützung der Datensicherungsprozesse sicher, dass Ihre Amazon-Redshift-Cluster über automatisierte Snapshots verfügen. Wenn automatisierte Snapshots für einen Cluster aktiviert sind, erstellt Redshift in regelmäßigen Abständen Snapshots dieses Clusters. Standardmäßig erstellt Redshift alle acht Stunden oder alle 5 GB einen Snapshot für jeden Knoten mit Datenänderungen oder je nachdem, was zuerst eintritt.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0017	Wenden Sie die Prinzipien der serviceorientierten Sicherheitsarchitektur an, um die Anforderungen des Unternehmens an Vertraulichkeit, Integrität und Verfügbarkeit zu erfüllen.	redshift-cluster-configuration-check	Um Daten im Ruhezustand zu schützen, muss die Verschlüsselung für Ihre Amazon-Redshift-Cluster aktiviert sein. Sie müssen auch sicherstellen, dass die erforderlichen Konfigurationen auf Amazon-Redshift-Clustern bereitgestellt werden. Die Prüfungsprotokollierung muss aktiviert sein, um Informationen zu Verbindungen und Benutzeraktivitäten in der Datenbank bereitzustellen. Diese Regel erfordert, dass ein Wert für clusterDbEncrypted (Config Default: TRUE) und LoggingEnabled (Config Default: TRUE) gesetzt ist. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0017	Wenden Sie die Prinzipien der serviceorientierten Sicherheitsarchitektur an, um die Anforderungen des Unternehmens an Vertraulichkeit, Integrität und Verfügbarkeit zu erfüllen.	redshift-cluster-public-access-überprüfen	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Redshift Redshift-Cluster nicht öffentlich sind. Amazon-Redshift-Cluster können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.
T0017	Wenden Sie die Prinzipien der serviceorientierten Sicherheitsarchitektur an, um die Anforderungen des Unternehmens an Vertraulichkeit, Integrität und Verfügbarkeit zu erfüllen.	redshift-require-tls-ssl	Stellen Sie sicher, dass Ihre Amazon-Redshift-Cluster eine TLS/SSL-Verschlüsselung erfordern, um eine Verbindung zu SQL-Clients herzustellen. Da sensible Daten vorhanden sein können, sollten Sie die Verschlüsselung bei der Übertragung aktivieren, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0017	Wenden Sie die Prinzipien der serviceorientierten Sicherheitsarchitektur an, um die Anforderungen des Unternehmens an Vertraulichkeit, Integrität und Verfügbarkeit zu erfüllen.	s3- -Block-periodisch account-level-public-access	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Simple Storage Service (Amazon S3) -Buckets nicht öffentlich zugänglich sind. Diese Regel trägt dazu bei, sensible Daten vor unbefugten Remote-Benutzern zu schützen, indem sie den öffentlichen Zugriff verhindert. Mit dieser Regel können Sie optional die Parameter ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) und restrictPublicBuckets Parameter (Config Default: True) festlegen. Die tatsächlichen Werte müssen den Richtlini

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			en Ihrer Organisation entsprechen.
T0017	Wenden Sie die Prinzipien der serviceorientierten Sicherheitsarchitektur an, um die Anforderungen des Unternehmens an Vertraulichkeit, Integrität und Verfügbarkeit zu erfüllen.	s3- bucket-public-read-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie nur autorisierten Benutzern, Prozessen und Geräten Zugriff auf Amazon Simple Storage Service (Amazon S3) - Buckets gewähren. Die Verwaltung des Zugriffs sollte mit der Klassifizierung der Daten übereinstimmen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0017	Wenden Sie die Prinzipien der serviceorientierten Sicherheitsarchitektur an, um die Anforderungen des Unternehmens an Vertraulichkeit, Integrität und Verfügbarkeit zu erfüllen.	s3- bucket-public-write-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie nur autorisierten Benutzern, Prozessen und Geräten Zugriff auf Amazon Simple Storage Service (Amazon S3) - Buckets gewähren. Die Verwaltung des Zugriffs sollte mit der Klassifizierung der Daten übereinstimmen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0017	Wenden Sie die Prinzipien der serviceorientierten Sicherheitsarchitektur an, um die Anforderungen des Unternehmens an Vertraulichkeit, Integrität und Verfügbarkeit zu erfüllen.	s3- bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) unterstützt die Aufrechterhaltung einer angemessenen Kapazität und Verfügbarkeit. CRR ermöglicht das automatische, asynchrone Kopieren von Objekten in Amazon S3 Buckets, um die Datenverfügbarkeit sicherzustellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0017	Wenden Sie die Prinzipien der serviceorientierten Sicherheitsarchitektur an, um die Anforderungen des Unternehmens an Vertraulichkeit, Integrität und Verfügbarkeit zu erfüllen.	s3- bucket-server-side -encryption -aktiviert	Zum Schutz von Daten im Ruhezustand müssen Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon Simple Storage Service (Amazon S3)-Buckets aktiviert ist. Da sensible Daten in Amazon S3 Buckets gespeichert werden können, sollten Sie die Verschlüsselung aktivieren, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0017	Wenden Sie die Prinzipien der serviceorientierten Sicherheitsarchitektur an, um die Anforderungen des Unternehmens an Vertraulichkeit, Integrität und Verfügbarkeit zu erfüllen.	s-3 bucket-ssl-requests-only	Um Daten während der Übertragung zu schützen, stellen Sie sicher, dass Ihre Amazon Simple Storage Service (Amazon S3)-Buckets Anfragen zur Verwendung von Secure Socket Layer (SSL)-Buckets erfordern. Da sensible Daten vorhanden sein können, sollten Sie die Verschlüsselung bei der Übertragung aktivieren, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0017	Wenden Sie die Prinzipien der serviceorientierten Sicherheitsarchitektur an, um die Anforderungen des Unternehmens an Vertraulichkeit, Integrität und Verfügbarkeit zu erfüllen.	s-3 bucket-versioning-enabled	Die Versionsverwaltung von Amazon Simple Storage Service (Amazon S3)-Buckets hilft dabei, mehrere Varianten eines Objekts im selben Amazon-S3-Bucket zu speichern. Verwenden Sie die Versionsverwaltung, um sämtliche Versionen aller Objekte in Ihrem Amazon-S3-Bucket zu speichern, abzurufen oder wiederherzustellen. Mit der Versionsverwaltung können Sie Versionen sowohl nach unbeabsichtigten Benutzeraktionen als auch nach Anwendungsfehlern problemlos wiederherstellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0017	Wenden Sie die Prinzipien der serviceorientierten Sicherheitsarchitektur an, um die Anforderungen des Unternehmens an Vertraulichkeit, Integrität und Verfügbarkeit zu erfüllen.	s-3 default-encryption-kms	Stellen Sie sicher, dass die Verschlüsselung für Ihre Amazon Simple Storage Service (Amazon S3)-Buckets aktiviert ist. Da sensible Daten in einem Amazon S3 Bucket gespeichert werden können, sollten Sie die Verschlüsselung im Ruhezustand aktivieren, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0017	Wenden Sie die Prinzipien der serviceorientierten Sicherheitsarchitektur an, um die Anforderungen des Unternehmens an Vertraulichkeit, Integrität und Verfügbarkeit zu erfüllen.	sagemaker-endpoint-configuration-kms-key-konfiguriert	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass die Verschlüsselung mit dem AWS Key Management Service (AWS KMS) für Ihren Endpunkt aktiviert ist. SageMaker Da sensible Daten auf dem SageMaker Endgerät gespeichert werden können, sollten Sie die Verschlüsselung im Ruhezustand aktivieren, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0017	Wenden Sie die Prinzipien der serviceorientierten Sicherheitsarchitektur an, um die Anforderungen des Unternehmens an Vertraulichkeit, Integrität und Verfügbarkeit zu erfüllen.	sagemaker-notebook-instance-kms-schlüsselkonfiguriert	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass die Verschlüsselung mit dem AWS Key Management Service (AWS KMS) für Ihr Notebook aktiviert ist. SageMaker Da vertrauliche Daten im SageMaker Notebook gespeichert werden können, sollten Sie die Verschlüsselung im Ruhezustand aktivieren, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0017	Wenden Sie die Prinzipien der serviceorientierten Sicherheitsarchitektur an, um die Anforderungen des Unternehmens an Vertraulichkeit, Integrität und Verfügbarkeit zu erfüllen.	ssm-document-not-public	Stellen Sie sicher, dass AWS Systems Manager (SSM) - Dokumente nicht öffentlich sind, da dies einen unbeabsichtigten Zugriff auf Ihre SSM-Dokumente ermöglichen kann. Ein öffentliches SSM-Dokument kann Informationen über Ihr Konto, Ihre Ressourcen und internen Prozesse preisgeben.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0017	Wenden Sie die Prinzipien der serviceorientierten Sicherheitsarchitektur an, um die Anforderungen des Unternehmens an Vertraulichkeit, Integrität und Verfügbarkeit zu erfüllen.	vpc-vpn-2-tunnels-up	Redundante Site-to-Site VPN-Tunnel können implementiert werden, um die Anforderungen an die Ausfallsicherheit zu erfüllen. Es verwendet zwei Tunnel, um die Konnektivität sicherzustellen, falls eine der Site-to-Site VPN-Verbindungen nicht verfügbar ist. Um sich vor einem Verbindungsverlust zu schützen, können Sie für den Fall, dass Ihr Kunden-Gateway nicht verfügbar ist, eine zweite Site-to-Site VPN-Verbindung zu Ihrer Amazon Virtual Private Cloud (Amazon VPC) und Ihrem Virtual Private Gateway einrichten, indem Sie ein zweites Kunden-Gateway verwenden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0017	Wenden Sie die Prinzipien der serviceorientierten Sicherheitsarchitektur an, um die Anforderungen des Unternehmens an Vertraulichkeit, Integrität und Verfügbarkeit zu erfüllen.	api-gw-ssl-enabled	Stellen Sie sicher, dass die REST-API-Stufen von Amazon API Gateway mit SSL-Zertifikaten konfiguriert sind, damit Backend-Systeme überprüfen können, ob Anforderungen von API Gateway stammen.
T0017	Wenden Sie die Prinzipien der serviceorientierten Sicherheitsarchitektur an, um die Anforderungen des Unternehmens an Vertraulichkeit, Integrität und Verfügbarkeit zu erfüllen.	backup-recovery-point-encrypted	Stellen Sie sicher, dass die Verschlüsselung für Ihre AWS Backup-Wiederherstellungspunkte aktiviert ist. Da sensible Daten auch im Ruhezustand vorhanden sein können, sollten Sie die Verschlüsselung im Ruhezustand aktivieren, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0017	Wenden Sie die Prinzipien der serviceorientierten Sicherheitsarchitektur an, um die Anforderungen des Unternehmens an Vertraulichkeit, Integrität und Verfügbarkeit zu erfüllen.	redshift-cluster-kms-enabled	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass die Verschlüsselung mit AWS Key Management Service (AWS KMS) für Ihren Amazon Redshift Redshift-Cluster aktiviert ist. Um eventuell vorhandene sensible Daten im Ruhezustand in Redshift-Clustern zu schützen, muss die Verschlüsselung von Daten im Ruhezustand aktiviert sein.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0017	Wenden Sie die Prinzipien der serviceorientierten Sicherheitsarchitektur an, um die Anforderungen des Unternehmens an Vertraulichkeit, Integrität und Verfügbarkeit zu erfüllen.	subnet-auto-assign-public-ip-deaktiviert	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon Virtual Private Cloud (VPC) -Subnetzen nicht automatisch eine öffentliche IP-Adresse zugewiesen wird. Amazon Elastic Compute Cloud (EC2) -Instances, die in Subnetzen gestartet werden, in denen dieses Attribut aktiviert ist, haben ihrer primären Netzwerkschnittstelle eine öffentliche IP-Adresse zugewiesen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0024	Sammeln und verwalten Sie Daten, die für die Berichterstattung zur Systemsicherheit erforderlich sind.	cw-loggroup-retention-period-überprüfen	Stellen Sie sicher, dass die Ereignisprotokolldaten für Ihre Protokollgruppen über eine Mindestdauer aufbewahrt werden, um die Fehlerbehebung und forensische Untersuchungen zu unterstützen. Fehlende frühere Ereignisprotokolldaten erschweren die Rekonstruierung und Identifizierung potenziell schädlicher Ereignisse.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0042	Koordinieren Sie sich mit Cyber Defense Analysts, um die Aktualisierung von Regeln und Signature n (z. B. Systeme zur Erkennung und zum Schutz vor Eindringlingen, Virenschutz und Inhaltssperrlisten) für spezielle Cyberabwe hranwendungen zu verwalten und zu verwalten.	guardduty-enabled-centralized	Amazon GuardDuty kann mithilfe von Threat Intellige nce Feeds helfen, potenzielle Cybersich erheitsereignisse zu überwachen und zu erkennen. Dazu gehören Listen mit bösartigen IPs und maschinel len Lernmethoden zur Identifizierung unerwarteter, nicht autorisierter und bösartiger Aktivitäten in Ihrer AWS Cloud-Umgebung.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0047	Korrelieren Sie Daten zu Vorfällen, um spezifische Sicherheitslücken zu identifizieren und Empfehlungen abzugeben, die eine schnelle Behebung ermöglichen.	guardduty-enabled-centralized	Amazon GuardDuty kann mithilfe von Threat Intelligence Feeds helfen, potenzielle Cybersicherheitsereignisse zu überwachen und zu erkennen. Dazu gehören Listen mit bösartigen IPs und maschinellen Lernmethoden zur Identifizierung unerwarteter, nicht autorisierter und bösartiger Aktivitäten in Ihrer AWS Cloud-Umgebung.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0051	Definieren Sie angemessene Stufen der Systemverfügbarkeit auf der Grundlage kritischer Systemfunktionen und stellen Sie sicher, dass in den Systemanforderungen angemessene Anforderungen für die Notfallwiederherstellung und die Kontinuität des Betriebs festgelegt werden, sodass auch etwaige Ausfälle berücksichtigt werdenover/alternate site requirements, backup requirements, and material supportability requirements for system recover/restoration.	backup-recovery-point-encrypted	Stellen Sie sicher, dass die Verschlüsselung für Ihre AWS Backup-Wiederherstellungspunkte aktiviert ist. Da sensible Daten auch im Ruhezustand vorhanden sein können, sollten Sie die Verschlüsselung im Ruhezustand aktivieren, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0051	Definieren Sie die geeigneten Stufen der Systemverfügbarkeit auf der Grundlage kritischer Systemfunktionen und stellen Sie sicher, dass in den Systemanforderungen die entsprechenden Anforderungen für die Notfallwiederherstellung und die Kontinuität des Betriebs festgelegt werden, sodass auch etwaige Ausfälle berücksichtigt over/alternate site requirements, backup requirements, and material supportability requirements for system recover/restoration werden.	backup-recovery-point-manual-Löschen deaktiviert	Stellen Sie sicher, dass Ihren AWS Backup-Wiederherstellungspunkten eine ressourcenbasierte Richtlinie zugeordnet ist, die das Löschen von Wiederherstellungspunkten verhindert. Die Verwendung einer ressourcenbasierten Richtlinie zur Verhinderung des Löschens von Wiederherstellungspunkten kann dazu beitragen, ein versehentliches oder absichtliches Löschen zu unterbinden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0051	Definieren Sie angemessene Stufen der Systemver fügbarkeit auf der Grundlage kritische r Systemfunktionen und stellen Sie sicher, dass in den Systemanforderunge n angemessene Anforderungen für die Notfallwi ederherstellung und die Kontinuität des Betriebs festgeleg t werden, sodass auch etwaige Ausfälle berücksichtigt werden. over/alternate site requirements, backup requirements, and material supportab ility requirements for system recover/r estoration	db-instance-backup-enabled	Die Sicherung sfunktion von Amazon RDS erstellt Sicherung en Ihrer Datenbank en und Transakti onsprotokolle. Amazon RDS erstellt einen Snapshot für das Speichervolume Ihrer DB-Instance, sodass die gesamte DB-Instance gesichert wird. Sie können im System spezifische Aufbewahrungsfrist en festlegen, um Ihre Ausfallsicherheits anforderungen zu erfüllen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0051	Definieren Sie angemessene Stufen der Systemverfügbarkeit auf der Grundlage kritischer Systemfunktionen und stellen Sie sicher, dass in den Systemanforderungen die entsprechenden Anforderungen für die Notfallwiederherstellung und die Kontinuität des Betriebs festgelegt werden, sodass auch alle entsprechenden Ausfälle berücksichtigt over/alternate site requirements, backup requirements, and material supportability requirements for system recover/restoration werden.	dynamodb-autoscaling-enabled	Amazon DynamoDB Auto Scaling verwendet den AWS Application Auto Scaling-Service, um die bereitgestellte Durchsatzkapazität so anzupassen, dass sie automatisch auf tatsächliche Verkehrsmuster reagiert. Auf diese Weise kann eine Tabelle oder ein globaler sekundärer Index die bereitgestellte Lese-/Schreibkapazität erhöhen, um plötzliche Erhöhungen des Datenverkehrs ohne Drosselung zu bewältigen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0051	Definieren Sie geeignete Stufen der Systemverfügbarkeit auf der Grundlage kritischer Systemfunktionen und stellen Sie sicher, dass in den Systemanforderungen die entsprechenden Anforderungen für die Notfallwiederherstellung und die Kontinuität des Betriebs festgelegt werden, sodass auch etwaige Ausfälle berücksichtigt werden. over/alternate site requirements, backup requirements, and material supportability requirements for system recover/restoration	dynamodb-in-backup-plan	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon DynamoDB-Tabellen Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0051	Definieren Sie angemessene Stufen der Systemverfügbarkeit auf der Grundlage kritischer Systemfunktionen und stellen Sie sicher, dass in den Systemanforderungen angemessene Anforderungen für die Notfallwiederherstellung und die Kontinuität des Betriebs festgelegt werden, sodass auch etwaige Ausfälle berücksichtigt werden. over/alternate site requirements, backup requirements, and material supportability requirements for system recover/restoration	dynamodb-pitr-enabled	Aktivieren Sie diese Regel, um zu überprüfen, ob die Informationen gesichert wurden. Es verwaltet auch die Backups, indem es sicherstellt, dass die point-in-time Wiederherstellung in Amazon DynamoDB aktiviert ist. Bei der Wiederherstellung werden fortlaufende Backups Ihrer Tabelle für die letzten 35 Tage gespeichert.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0051	Definieren Sie angemessene Stufen der Systemverfügbarkeit auf der Grundlage kritischer Systemfunktionen und stellen Sie sicher, dass in den Systemanforderungen angemessene Anforderungen für die Notfallwiederherstellung und die Kontinuität des Betriebs festgelegt werden, sodass auch etwaige Ausfälle berücksichtigt werden. over/alternate site requirements, backup requirements, and material supportability requirements for system recover/restoration	dynamodb-throughput-limit-check	Aktivieren Sie diese Regel, um sicherzustellen, dass die bereitgestellte Durchsatzkapazität in Ihren Amazon-DynamoDB-Tabellen überprüft wird. Dies ist der Umfang der Lese- und Schreibaktivitäten, der von den jeweiligen Tabellen unterstützt werden kann. DynamoDB verwendet diese Informationen für das Reservieren ausreichender Systemressourcen, um Ihren Durchsatz anforderungen gerecht zu werden. Diese Regel generiert eine Warnung, wenn sich der Durchsatz dem Höchstlimit für ein Kundenkonto nähert. Mit dieser Regel können Sie optional die Parameter RCUThreshold Kontoprozentsatz

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			(Konfigurationsstandard: 80) und WCUThreshold Kontoprozentsatz (Konfigurationsstandard: 80) festlegen. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0051	Definieren Sie angemessene Stufen der Systemverfügbarkeit auf der Grundlage kritischer Systemfunktionen und stellen Sie sicher, dass in den Systemanforderungen angemessene Anforderungen für die Notfallwiederherstellung und die Kontinuität des Betriebs festgelegt werden, sodass auch etwaige Ausfälle berücksichtigt werdenover/alternate site requirements, backup requirements, and material supportability requirements for system recover/restoration.	ebs-in-backup-plan	Stellen Sie zur Unterstützung der Datensicherungsprozesse sicher, dass Ihre Amazon Elastic Block Store (Amazon EBS) -Volumes Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihre Backup-Verwaltung und ermöglicht es Ihnen, Ihre geschäftlichen und behördlichen Anforderungen bezüglich Backups zu erfüllen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0051	Definieren Sie angemessene Stufen der Systemverfügbarkeit auf der Grundlage kritischer Systemfunktionen und stellen Sie sicher, dass in den Systemanforderungen angemessene Anforderungen für die Notfallwiederherstellung und die Kontinuität des Betriebs festgelegt werden, sodass auch etwaige Ausfälle berücksichtigt werden. over/alternate site requirements, backup requirements, and material supportability requirements for system recover/restoration	efs-in-backup-plan	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon Elastic File System (Amazon EFS) -Dateisysteme Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0051	Definieren Sie angemessene Stufen der Systemver fügbarkeit auf der Grundlage kritische r Systemfunktionen und stellen Sie sicher, dass in den Systemanforderunge n angemessene Anforderungen für die Notfallwi ederherstellung und die Kontinuität des Betriebs festgeleg t werden, sodass auch etwaige Ausfälle berücksichtigt werden. over/alternate site requirements, backup requirements, and material supportab ility requirements for system recover/r estoration	elasticache-redis-cluster-automatic-Backup-Check	Wenn automatische Backups aktiviert sind, ElastiCache erstellt Amazon täglich ein Backup des Clusters. Die Sicherung kann für eine von Ihrer Organisation festgelegte Anzahl von Tagen aufbewahrt werden. Automatische Backups schützen vor Datenverlust. Bei einem Ausfall können Sie einen neuen Cluster erstellen, der Ihre Daten aus dem aktuellen Backup wiederherstellt.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0051	Definieren Sie angemessene Stufen der Systemverfügbarkeit auf der Grundlage kritischer Systemfunktionen und stellen Sie sicher, dass in den Systemanforderungen angemessene Anforderungen für die Notfallwiederherstellung und die Kontinuität des Betriebs festgelegt werden, sodass auch etwaige Ausfälle berücksichtigt werdenover/alternate site requirements, backup requirements, and material supportability requirements for system recover/restoration.	elb-cross-zone-load-Balancing aktiviert	Aktivieren Sie zonenübergreifendes Load Balancing für Ihre Elastic Load Balancer (ELBs), um eine angemessene Kapazität und Verfügbarkeit aufrechtzuerhalten. Zonenübergreifendes Load Balancing reduziert die Notwendigkeit, die gleiche Anzahl von Instances in jeder aktivierten Availability Zone aufrechtzuerhalten. Es verbessert auch die Fähigkeit Ihrer Anwendung, den Verlust einer oder mehrerer Instances zu bewältigen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0051	Definieren Sie angemessene Stufen der Systemverfügbarkeit auf der Grundlage kritischer Systemfunktionen und stellen Sie sicher, dass in den Systemanforderungen angemessene Anforderungen für die Notfallwiederherstellung und die Kontinuität des Betriebs festgelegt werden, sodass auch etwaige Ausfälle berücksichtigt werden. over/alternate site requirements, backup requirements, and material supportability requirements for system recover/restoration	elb-deletion-protection-enabled	Diese Regel sorgt dafür, dass der Löschschutz für Elastic Load Balancing aktiviert ist. Verwenden Sie diese Funktion, um zu verhindern, dass Ihr Load Balancer versehentlich oder böswillig gelöscht wird, was zum Verlust der Verfügbarkeit Ihrer Anwendungen führen kann.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0051	Definieren Sie angemessene Stufen der Systemver fügbarkeit auf der Grundlage kritische r Systemfunktionen und stellen Sie sicher, dass in den Systemanforderunge n die entsprech enden Anforderu ngen für die Notfallwi ederherstellung und die Kontinuität des Betriebs festgelegt werden, sodass auch alle entsprechenden Ausfälle berücksichtigt over/alternate site requirements, backup requirements, and material supportab ility requirements for system recover/r estoration werden.	rds-instance-deletion-protection-aktiviert	Stellen Sie sicher, dass Amazon Relational Database Service (Amazon RDS)-Instances den Löschschutz aktiviert haben. Verwenden Sie den Löschschu tz, um zu verhindern, dass Ihre Amazon-RD S-Instances versehent lich oder böswillig gelöscht werden, was zum Verlust der Verfügbarkeit Ihrer Anwendungen führen kann.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0051	Definieren Sie angemessene Stufen der Systemver fügbarkeit auf der Grundlage kritische r Systemfunktionen und stellen Sie sicher, dass in den Systemanforderunge n die entsprech enden Anforderu ngen für die Notfallwi ederherstellung und die Kontinuität des Betriebs festgeleg t werden, sodass auch etwaige Ausfälle berücksichtigt werden. over/alternate site requirements, backup requirements, and material supportab ility requirements for system recover/r estoration	rds-in-backup-plan	Um Sie bei Datensich erungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon Relational Database Service (Amazon RDS) -Instance s Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwaltet er Backup-Service mit einer richtlini enbasierten Backup-Lösung. Diese Lösung vereinfac ht Ihr Sicherung smanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforde rungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0051	Definieren Sie angemessene Stufen der Systemverfügbarkeit auf der Grundlage kritischer Systemfunktionen und stellen Sie sicher, dass in den Systemanforderungen angemessene Anforderungen für die Notfallwiederherstellung und die Kontinuität des Betriebs festgelegt werden, sodass auch etwaige Ausfälle berücksichtigt werden. over/alternate site requirements, backup requirements, and material supportability requirements for system recover/restoration	rds-multi-az-support	Die Multi-AZ-Unterstützung in Amazon Relational Database Service (Amazon RDS) bietet eine verbesserte Verfügbarkeit und Beständigkeit von Datenbank-Instances. Wenn Sie eine Multi-AZ-Datenbank-Instance bereitstellen, erstellt Amazon RDS automatisch eine primäre Datenbank-Instance und repliziert die Daten synchron auf eine Standby-Instance in einer anderen Availability Zone. Jede Availability Zone läuft auf einer eigenen, physisch getrennten, unabhängigen Infrastruktur und ist auf eine hohe Verfügbarkeit ausgelegt. Im Falle eines Infrastrukturausfalls führt Amazon RDS einen automatis

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			chen Failover zum Standby-Modus durch, sodass Sie den Datenbankbetrieb wieder aufnehmen können, sobald der Failover abgeschlo ssen ist.
T0051	Definieren Sie angemessene Stufen der Systemver fügbarkeit auf der Grundlage kritische r Systemfunktionen und stellen Sie sicher, dass in den Systemanforderunge n die entsprech enden Anforderu ngen für die Notfallwi ederherstellung und die Kontinuität des Betriebs festgelegt werden, sodass auch alle entsprechenden Ausfälle berücksichtigt over/alternate site requirements, backup requirements, and material supportab ility requirements for system recover/r estoration werden.	redshift-backup-en abled	Stellen Sie zur Unterstützung der Datensicherungspro zesse sicher, dass Ihre Amazon-Re dshift-Cluster über automatisierte Snapshots verfügen. Wenn automatis ierte Snapshots für einen Cluster aktiviert sind, erstellt Redshift in regelmäßi gen Abständen Snapshots dieses Clusters. Standardm äßig erstellt Redshift alle acht Stunden oder alle 5 GB einen Snapshot für jeden Knoten mit Datenände rungen oder je nachdem, was zuerst eintritt.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0051	Definieren Sie angemessene Stufen der Systemver fügbarkeit auf der Grundlage kritische r Systemfunktionen und stellen Sie sicher, dass in den Systemanforderunge n die entsprech enden Anforderu ngen für die Notfallwi ederherstellung und die Kontinuität des Betriebs festgeleg t werden, sodass auch etwaige Ausfälle berücksichtigt werden. over/alternate site requirements, backup requirements, and material supportab ility requirements for system recover/r estoration	s3- bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) unterstützt die Aufrechterhaltung einer angemesse nen Kapazität und Verfügbarkeit. CRR ermöglicht das automatische, asynchrone Kopieren von Objekten in Amazon S3 Buckets, um die Datenverf ügbarkeit sicherzus tellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0051	Definieren Sie ein angemessenes Niveau der Systemverfügbarkeit auf der Grundlage kritischer Systemfunktionen und stellen Sie sicher, dass in den Systemanforderungen die entsprechenden Anforderungen für die Notfallwiederherstellung und die Kontinuität des Betriebs festgelegt werden, sodass auch etwaige Ausfälle berücksichtigt over/alternate site requirements, backup requirements, and material supportability requirements for system recover/restoration werden.	s3- bucket-versioning-enabled	Die Versionsverwaltung von Amazon Simple Storage Service (Amazon S3)-Buckets hilft dabei, mehrere Varianten eines Objekts im selben Amazon-S3-Bucket zu speichern. Verwenden Sie die Versionsverwaltung, um sämtliche Versionen aller Objekte in Ihrem Amazon-S3-Bucket zu speichern, abzurufen oder wiederherzustellen. Mit der Versionsverwaltung können Sie Versionen sowohl nach unbeabsichtigten Benutzeraktionen als auch nach Anwendungsfehlern problemlos wiederherstellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0051	Definieren Sie ein angemessenes Niveau der Systemverfügbarkeit auf der Grundlage kritischer Systemfunktionen und stellen Sie sicher, dass in den Systemanforderungen die entsprechenden Anforderungen für die Notfallwiederherstellung und die Kontinuität des Betriebs festgelegt werden, sodass auch etwaige Ausfälle berücksichtigt over/alternate site requirements, backup requirements, and material supportability requirements for system recover/restoration werden.	vpc-vpn-2-tunnels-up	Redundante Site-to-Site VPN-Tunnel können implementiert werden, um die Anforderungen an die Ausfallsicherheit zu erfüllen. Es verwendet zwei Tunnel, um die Konnektivität sicherzustellen, falls eine der Site-to-Site VPN-Verbindungen nicht verfügbar ist. Um sich vor einem Verbindungsverlust zu schützen, können Sie für den Fall, dass Ihr Kunden-Gateway nicht verfügbar ist, eine zweite Site-to-Site VPN-Verbindung zu Ihrer Amazon Virtual Private Cloud (Amazon VPC) und Ihrem Virtual Private Gateway einrichten, indem Sie ein zweites Kunden-Gateway verwenden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0051	Definieren Sie die geeigneten Stufen der Systemverfügbarkeit auf der Grundlage kritischer Systemfunktionen und stellen Sie sicher, dass in den Systemanforderungen angemessene Anforderungen für die Notfallwiederherstellung und die Kontinuität des Betriebs festgelegt werden, sodass auch etwaige Ausfälle berücksichtigt werden. over/alternate site requirements, backup requirements, and material supportability requirements for system recover/restoration	backup-plan-min-frequency-and-min-retention-check	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihr AWS Backup-Plan auf eine Mindestfrequenz und Aufbewahrung festgelegt ist. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen. Mit dieser Regel können Sie die Parameter requiredFrequencyValue (Config default: 1), requiredRetentionDays (Config default: 35) und requiredFrequencyUnit

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			(Config default: days) festlegen. Der tatsächliche Wert muss den Anforderungen Ihrer Organisation entsprechen.
T0051	Definieren Sie angemessene Stufen der Systemverfügbarkeit auf der Grundlage kritischer Systemfunktionen und stellen Sie sicher, dass in den Systemanforderungen angemessene Anforderungen für die Notfallwiederherstellung und die Kontinuität des Betriebs festgelegt werden, sodass auch alle entsprechenden Ausfälle berücksichtigt werdenover/alternate site requirements, backup requirements, and material supportability requirements for system recover/restoration.	ec2- -Plan resources-protected-by-backup	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon Elastic Compute Cloud (Amazon EC2) -Ressourcen Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0065	Entwickeln und implementieren Sie Verfahren zur Netzwerksicherung und -wiederherstellung.	backup-plan-min-frequency-and-min-retention-check	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihr AWS Backup-Plan auf eine Mindestfrequenz und Aufbewahrung festgelegt ist. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen. Mit dieser Regel können Sie die Parameter requiredFrequencyValue (Config default: 1), requiredRetentionDays (Config default: 35) und requiredFrequencyUnit

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			(Config default: days) festlegen. Der tatsächliche Wert muss den Anforderungen Ihrer Organisation entsprechen.
T0065	Entwickeln und implementieren Sie Verfahren zur Netzwerksicherung und -wiederherstellung.	backup-recovery-point-encrypted	Stellen Sie sicher, dass die Verschlüsselung für Ihre AWS Backup-Wiederherstellungspunkte aktiviert ist. Da sensible Daten auch im Ruhezustand vorhanden sein können, sollten Sie die Verschlüsselung im Ruhezustand aktivieren, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0065	Entwickeln und implementieren Sie Verfahren zur Netzwerksicherung und -wiederherstellung.	backup-recovery-point-manual-Löschen-deaktiviert	Stellen Sie sicher, dass Ihren AWS Backup-Wiederherstellungspunkten eine ressourcenbasierte Richtlinie zugeordnet ist, die das Löschen von Wiederherstellungspunkten verhindert. Die Verwendung einer ressourcenbasierten Richtlinie zur Verhinderung des Löschens von Wiederherstellungspunkten kann dazu beitragen, ein versehentliches oder absichtliches Löschen zu unterbinden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0065	Entwickeln und implementieren Sie Verfahren zur Netzwerksicherung und -wiederherstellung.	dynamodb-autoscaling-enabled	Amazon DynamoDB Auto Scaling verwendet den AWS Application Auto Scaling-Service, um die bereitgestellte Durchsatzkapazität so anzupassen, dass sie automatisch auf tatsächliche Verkehrsmuster reagiert. Auf diese Weise kann eine Tabelle oder ein globaler sekundärer Index die bereitgestellte Lese-/Schreibkapazität erhöhen, um plötzliche Erhöhungen des Datenverkehrs ohne Drosselung zu bewältigen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0065	Entwickeln und implementieren Sie Verfahren zur Netzwerksicherung und -wiederherstellung.	dynamodb-in-backup-plan	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon DynamoDB-Tabellen Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0065	Entwickeln und implementieren Sie Verfahren zur Netzwerksicherung und -wiederherstellung.	ebs-in-backup-plan	Stellen Sie zur Unterstützung der Datensicherungsprozesse sicher, dass Ihre Amazon Elastic Block Store (Amazon EBS) -Volumes Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihre Backup-Verwaltung und ermöglicht es Ihnen, Ihre geschäftlichen und behördlichen Anforderungen bezüglich Backups zu erfüllen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0065	Entwickeln und implementieren Sie Verfahren zur Netzwerksicherung und -wiederherstellung.	ec2--Plan resources-protected-by-backup	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon Elastic Compute Cloud (Amazon EC2) -Ressourcen Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0065	Entwickeln und implementieren Sie Verfahren zur Netzwerksicherung und -wiederherstellung.	efs-in-backup-plan	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon Elastic File System (Amazon EFS) -Dateisysteme Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0065	Entwickeln und implementieren Sie Verfahren zur Netzwerksicherung und -wiederherstellung.	elb-cross-zone-load-Balancing aktiviert	Aktivieren Sie zonenübergreifendes Load Balancing für Ihre Elastic Load Balancer (ELBs), um eine angemessene Kapazität und Verfügbarkeit aufrechtzuerhalten. Zonenübergreifendes Load Balancing reduziert die Notwendigkeit, die gleiche Anzahl von Instances in jeder aktivierten Availability Zone aufrechtzuerhalten. Es verbessert auch die Fähigkeit Ihrer Anwendung, den Verlust einer oder mehrerer Instances zu bewältigen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0065	Entwickeln und implementieren Sie Verfahren zur Netzwerksicherung und -wiederherstellung.	elb-deletion-protection-enabled	Diese Regel sorgt dafür, dass der Löschschutz für Elastic Load Balancing aktiviert ist. Verwenden Sie diese Funktion, um zu verhindern, dass Ihr Load Balancer versehentlich oder böswillig gelöscht wird, was zum Verlust der Verfügbarkeit Ihrer Anwendungen führen kann.
T0065	Entwickeln und implementieren Sie Verfahren zur Netzwerksicherung und -wiederherstellung.	rds-instance-deletion-protection-aktiviert	Stellen Sie sicher, dass Amazon Relational Database Service (Amazon RDS)-Instances den Löschschutz aktiviert haben. Verwenden Sie den Löschschutz, um zu verhindern, dass Ihre Amazon-RDS-Instances versehentlich oder böswillig gelöscht werden, was zum Verlust der Verfügbarkeit Ihrer Anwendungen führen kann.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0065	Entwickeln und implementieren Sie Verfahren zur Netzwerksicherung und -wiederherstellung.	rds-in-backup-plan	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon Relational Database Service (Amazon RDS) -Instances Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0065	Entwickeln und implementieren Sie Verfahren zur Netzwerksicherung und -wiederherstellung.	rds-multi-az-support	Die Multi-AZ-Unterstützung in Amazon Relational Database Service (Amazon RDS) bietet eine verbesserte Verfügbarkeit und Beständigkeit von Datenbank-Instances. Wenn Sie eine Multi-AZ-Datenbank-Instance bereitstellen, erstellt Amazon RDS automatisch eine primäre Datenbank-Instance und repliziert die Daten synchron auf eine Standby-Instance in einer anderen Availability Zone. Jede Availability Zone läuft auf einer eigenen, physisch getrennten, unabhängigen Infrastruktur und ist auf eine hohe Verfügbarkeit ausgelegt. Im Falle eines Infrastrukturausfalls führt Amazon RDS einen automatis

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			chen Failover zum Standby-Modus durch, sodass Sie den Datenbankbetrieb wieder aufnehmen können, sobald der Failover abgeschlo ssen ist.
T0065	Entwickeln und implementieren Sie Verfahren zur Netzwerksicherung und -wiederhe rstellung.	redshift-backup-en abled	Stellen Sie zur Unterstützung der Datensicherungspro zesse sicher, dass Ihre Amazon-Re dshift-Cluster über automatisierte Snapshots verfügen. Wenn automatis ierte Snapshots für einen Cluster aktiviert sind, erstellt Redshift in regelmäßi gen Abständen Snapshots dieses Clusters. Standardm äßig erstellt Redshift alle acht Stunden oder alle 5 GB einen Snapshot für jeden Knoten mit Datenände rungen oder je nachdem, was zuerst eintritt.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0065	Entwickeln und implementieren Sie Verfahren zur Netzwerksicherung und -wiederherstellung.	vpc-vpn-2-tunnels-up	Redundante Site-to-Site VPN-Tunnel können implementiert werden, um die Anforderungen an die Ausfallsicherheit zu erfüllen. Es verwendet zwei Tunnel, um die Konnektivität sicherzustellen, falls eine der Site-to-Site VPN-Verbindungen nicht verfügbar ist. Um sich vor einem Verbindungsverlust zu schützen, können Sie für den Fall, dass Ihr Kunden-Gateway nicht verfügbar ist, eine zweite Site-to-Site VPN-Verbindung zu Ihrer Amazon Virtual Private Cloud (Amazon VPC) und Ihrem Virtual Private Gateway einrichten, indem Sie ein zweites Kunden-Gateway verwenden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0065	Entwickeln und implementieren Sie Verfahren zur Netzwerksicherung und -wiederherstellung.	db-instance-backup-enabled	Die Sicherungsfunktion von Amazon RDS erstellt Sicherungen Ihrer Datenbanken und Transaktionsprotokolle. Amazon RDS erstellt einen Snapshot für das Speichervolume Ihrer DB-Instance, sodass die gesamte DB-Instance gesichert wird. Sie können im System spezifische Aufbewahrungsfristen festlegen, um Ihre Ausfallsicherheitsanforderungen zu erfüllen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0065	Entwickeln und implementieren Sie Verfahren zur Netzwerksicherung und -wiederherstellung.	dynamodb-pitr-enabled	Aktivieren Sie diese Regel, um zu überprüfen, ob die Informationen gesichert wurden. Es verwaltet auch die Backups, indem es sicherstellt, dass die point-in-time Wiederherstellung in Amazon DynamoDB aktiviert ist. Bei der Wiederherstellung werden fortlaufende Backups Ihrer Tabelle für die letzten 35 Tage gespeichert.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0065	Entwickeln und implementieren Sie Verfahren zur Netzwerksicherung und -wiederherstellung.	elasticache-redis-cluster-automatic-Backup-Prüfung	Wenn automatische Backups aktiviert sind, ElastiCache erstellt Amazon täglich ein Backup des Clusters. Die Sicherung kann für eine von Ihrer Organisation festgelegte Anzahl von Tagen aufbewahrt werden. Automatische Backups schützen vor Datenverlust. Bei einem Ausfall können Sie einen neuen Cluster erstellen, der Ihre Daten aus dem aktuellen Backup wiederherstellt.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0065	Entwickeln und implementieren Sie Verfahren zur Netzwerksicherung und -wiederherstellung.	redshift-cluster-maintenancesettings-check	Diese Regel stellt sicher, dass Amazon-Redshift-Cluster die bevorzugten Einstellungen für Ihre Organisation haben. Insbesondere sorgt sie dafür, dass Cluster bevorzugte Wartungsfenster und automatisierte Aufbewahrungsfristen für Snapshots für die Datenbank haben. Für diese Regel müssen Sie die festlegen allowVersionUpgrade. Der Standardwert ist „true“. Außerdem können Sie optional den Zeitraum preferredMaintenanceWindow (der Standardwert ist sa: 16:00 -sa: 16:30) und den automated SnapshotRetention Zeitraum (der Standardwert ist 1) festlegen. Die tatsächlichen Werte müssen den Richtlini

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			en Ihrer Organisation entsprechen.
T0065	Entwickeln und implementieren Sie Verfahren zur Netzwerksicherung und -wiederherstellung.	s3- bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) unterstützt die Aufrechterhaltung einer angemessenen Kapazität und Verfügbarkeit. CRR ermöglicht das automatische, asynchrone Kopieren von Objekten in Amazon S3 Buckets, um die Datenverfügbarkeit sicherzustellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0065	Entwickeln und implementieren Sie Verfahren zur Netzwerksicherung und -wiederherstellung.	s-3 bucket-versioning-enabled	Die Versionsverwaltung von Amazon Simple Storage Service (Amazon S3)-Buckets hilft dabei, mehrere Varianten eines Objekts im selben Amazon-S3-Bucket zu speichern. Verwenden Sie die Versionsverwaltung, um sämtliche Versionen aller Objekte in Ihrem Amazon-S3-Bucket zu speichern, abzurufen oder wiederherzustellen. Mit der Versionsverwaltung können Sie Versionen sowohl nach unbeabsichtigten Benutzeraktionen als auch nach Anwendungsfehlern problemlos wiederherstellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0070	Entwickeln Sie Pläne für die Notfallwiederherstellung und die Aufrechterhaltung des Betriebs für Systeme, die sich in der Entwicklung befinden, und stellen Sie sicher, dass die Systeme getestet werden, bevor sie in eine Produktionsumgebung übergehen.	backup-plan-min-frequency-and-min-retention-check	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihr AWS Backup-Plan auf eine Mindestfrequenz und Aufbewahrung festgelegt ist. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen. Mit dieser Regel können Sie die Parameter requiredFrequencyValue (Config default: 1), requiredRetentionDays (Config default: 35) und requiredFrequencyUnit

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			(Config default: days) festlegen. Der tatsächliche Wert muss den Anforderungen Ihrer Organisation entsprechen.
T0070	Entwickeln Sie Pläne für die Notfallwiederherstellung und die Aufrechterhaltung des Betriebs für Systeme, die sich in der Entwicklung befinden, und stellen Sie sicher, dass die Systeme getestet werden, bevor sie in eine Produktionsumgebung übergehen.	backup-recovery-point-encrypted	Stellen Sie sicher, dass die Verschlüsselung für Ihre AWS Backup-Wiederherstellungspunkte aktiviert ist. Da sensible Daten auch im Ruhezustand vorhanden sein können, sollten Sie die Verschlüsselung im Ruhezustand aktivieren, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0070	Entwickeln Sie Pläne für die Notfallwiederherstellung und die Aufrechterhaltung des Betriebs für Systeme, die sich in der Entwicklung befinden, und stellen Sie sicher, dass die Systeme getestet werden, bevor sie in eine Produktionsumgebung übergehen.	backup-recovery-point-manual-Löschen-deaktiviert	Stellen Sie sicher, dass Ihren AWS Backup-Wiederherstellungspunkten eine ressourcenbasierte Richtlinie zugeordnet ist, die das Löschen von Wiederherstellungspunkten verhindert. Die Verwendung einer ressourcenbasierten Richtlinie zur Verhinderung des Löschens von Wiederherstellungspunkten kann dazu beitragen, ein versehentliches oder absichtliches Löschen zu unterbinden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0070	Entwickeln Sie Pläne für die Notfallwiederherstellung und die Aufrechterhaltung des Betriebs für Systeme, die sich in der Entwicklung befinden, und stellen Sie sicher, dass die Systeme getestet werden, bevor sie in eine Produktionsumgebung übergehen.	dynamodb-in-backup-plan	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon DynamoDB-Tabellen Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0070	Entwickeln Sie Pläne für die Notfallwi ederherstellung und die Aufrechte rhaltung des Betriebs für Systeme, die sich in der Entwicklu ng befinden, und stellen Sie sicher, dass die Systeme getestet werden, bevor sie in eine Produktionsumgebun g übergehen.	ebs-in-backup-plan	Stellen Sie zur Unterstützung der Datensicherungspro zesse sicher, dass Ihre Amazon Elastic Block Store (Amazon EBS) -Volumes Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwaltet er Backup-Service mit einer richtlini enbasierten Backup-Lösung. Diese Lösung vereinfacht Ihre Backup-Verwaltung und ermöglicht es Ihnen, Ihre geschäftl ichen und behördlic hen Anforderungen bezüglich Backups zu erfüllen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0070	Entwickeln Sie Pläne für die Notfallwiederherstellung und die Aufrechterhaltung des Betriebs für Systeme, die sich in der Entwicklung befinden, und stellen Sie sicher, dass die Systeme getestet werden, bevor sie in eine Produktionsumgebung übergehen.	ec2--Plan resources-protected-by-backup	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon Elastic Compute Cloud (Amazon EC2) -Ressourcen Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0070	Entwickeln Sie Pläne für die Notfallwiederherstellung und die Aufrechterhaltung des Betriebs für Systeme, die sich in der Entwicklung befinden, und stellen Sie sicher, dass die Systeme getestet werden, bevor sie in eine Produktionsumgebung übergehen.	efs-in-backup-plan	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon Elastic File System (Amazon EFS) -Dateisysteme Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0070	Entwickeln Sie Pläne für die Notfallwiederherstellung und die Aufrechterhaltung des Betriebs für Systeme, die sich in der Entwicklung befinden, und stellen Sie sicher, dass die Systeme getestet werden, bevor sie in eine Produktionsumgebung übergehen.	elb-cross-zone-load-Balancing aktiviert	Aktivieren Sie zonenübergreifendes Load Balancing für Ihre Elastic Load Balancer (ELBs), um eine angemessene Kapazität und Verfügbarkeit aufrechtzuerhalten. Zonenübergreifendes Load Balancing reduziert die Notwendigkeit, die gleiche Anzahl von Instances in jeder aktivierten Availability Zone aufrechtzuerhalten. Es verbessert auch die Fähigkeit Ihrer Anwendung, den Verlust einer oder mehrerer Instances zu bewältigen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0070	Entwickeln Sie Pläne für die Notfallwi ederherstellung und die Aufrechte rhaltung des Betriebs für Systeme, die sich in der Entwicklu ng befinden, und stellen Sie sicher, dass die Systeme getestet werden, bevor sie in eine Produktionsumgebun g übergehen.	rds-instance-deletion-protection-aktiviert	Stellen Sie sicher, dass Amazon Relational Database Service (Amazon RDS)-Instances den Löschschutz aktiviert haben. Verwenden Sie den Löschschu tz, um zu verhindern, dass Ihre Amazon-RD S-Instances versehent lich oder böswillig gelöscht werden, was zum Verlust der Verfügbarkeit Ihrer Anwendungen führen kann.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0070	Entwickeln Sie Pläne für die Notfallwiederherstellung und die Aufrechterhaltung des Betriebs für Systeme, die sich in der Entwicklung befinden, und stellen Sie sicher, dass die Systeme getestet werden, bevor sie in eine Produktionsumgebung übergehen.	rds-in-backup-plan	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon Relational Database Service (Amazon RDS) -Instances Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0070	Entwickeln Sie Pläne für die Notfallwiederherstellung und die Aufrechterhaltung des Betriebs für Systeme, die sich in der Entwicklung befinden, und stellen Sie sicher, dass die Systeme getestet werden, bevor sie in eine Produktionsumgebung übergehen.	redshift-backup-enabled	Stellen Sie zur Unterstützung der Datensicherungsprozesse sicher, dass Ihre Amazon-Redshift-Cluster über automatisierte Snapshots verfügen. Wenn automatisierte Snapshots für einen Cluster aktiviert sind, erstellt Redshift in regelmäßigen Abständen Snapshots dieses Clusters. Standardmäßig erstellt Redshift alle acht Stunden oder alle 5 GB einen Snapshot für jeden Knoten mit Datenänderungen oder je nachdem, was zuerst eintritt.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0070	Entwickeln Sie Pläne für die Notfallwiederherstellung und die Aufrechterhaltung des Betriebs für Systeme, die sich in der Entwicklung befinden, und stellen Sie sicher, dass die Systeme getestet werden, bevor sie in eine Produktionsumgebung übergehen.	db-instance-backup-enabled	Die Sicherungsfunktion von Amazon RDS erstellt Sicherungen Ihrer Datenbanken und Transaktionsprotokolle. Amazon RDS erstellt einen Snapshot für das Speichervolume Ihrer DB-Instance, sodass die gesamte DB-Instance gesichert wird. Sie können im System spezifische Aufbewahrungsfristen festlegen, um Ihre Ausfallsicherheitsanforderungen zu erfüllen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0070	Entwickeln Sie Pläne für die Notfallwiederherstellung und die Aufrechterhaltung des Betriebs für Systeme, die sich in der Entwicklung befinden, und stellen Sie sicher, dass die Systeme getestet werden, bevor sie in eine Produktionsumgebung übergehen.	dynamodb-autoscaling-enabled	Amazon DynamoDB Auto Scaling verwendet den AWS Application Auto Scaling-Service, um die bereitgestellte Durchsatzkapazität so anzupassen, dass sie automatisch auf tatsächliche Verkehrsmuster reagiert. Auf diese Weise kann eine Tabelle oder ein globaler sekundärer Index die bereitgestellte Lese-/Schreibkapazität erhöhen, um plötzliche Erhöhungen des Datenverkehrs ohne Drosselung zu bewältigen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0070	Entwickeln Sie Pläne für die Notfallwiederherstellung und die Aufrechterhaltung des Betriebs für Systeme, die sich in der Entwicklung befinden, und stellen Sie sicher, dass die Systeme getestet werden, bevor sie in eine Produktionsumgebung übergehen.	dynamodb-pitr-enabled	Aktivieren Sie diese Regel, um zu überprüfen, ob die Informationen gesichert wurden. Es verwaltet auch die Backups, indem es sicherstellt, dass die point-in-time Wiederherstellung in Amazon DynamoDB aktiviert ist. Bei der Wiederherstellung werden fortlaufende Backups Ihrer Tabelle für die letzten 35 Tage gespeichert.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0070	Entwickeln Sie Pläne für die Notfallwi ederherstellung und die Aufrechte rhaltung des Betriebs für Systeme, die sich in der Entwicklu ng befinden, und stellen Sie sicher, dass die Systeme getestet werden, bevor sie in eine Produktionsumgebun g übergehen.	elasticache-redis-cluster-automatic-Backup-Prüfung	Wenn automatische Backups aktiviert sind, ElastiCache erstellt Amazon täglich ein Backup des Clusters. Die Sicherung kann für eine von Ihrer Organisation festgelegte Anzahl von Tagen aufbewahrt werden. Automatische Backups schützen vor Datenverlust. Bei einem Ausfall können Sie einen neuen Cluster erstellen, der Ihre Daten aus dem aktuellen Backup wiederherstellt.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0070	Entwickeln Sie Pläne für die Notfallwiederherstellung und die Aufrechterhaltung des Betriebs für Systeme, die sich in der Entwicklung befinden, und stellen Sie sicher, dass die Systeme getestet werden, bevor sie in eine Produktionsumgebung übergehen.	elb-deletion-protection-enabled	Diese Regel sorgt dafür, dass der Löschschutz für Elastic Load Balancing aktiviert ist. Verwenden Sie diese Funktion, um zu verhindern, dass Ihr Load Balancer versehentlich oder böswillig gelöscht wird, was zum Verlust der Verfügbarkeit Ihrer Anwendungen führen kann.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0070	Entwickeln Sie Pläne für die Notfallwiederherstellung und die Aufrechterhaltung des Betriebs für Systeme, die sich in der Entwicklung befinden, und stellen Sie sicher, dass die Systeme getestet werden, bevor sie in eine Produktionsumgebung übergehen.	rds-multi-az-support	Die Multi-AZ-Unterstützung in Amazon Relational Database Service (Amazon RDS) bietet eine verbesserte Verfügbarkeit und Beständigkeit von Datenbank-Instances. Wenn Sie eine Multi-AZ-Datenbank-Instance bereitstellen, erstellt Amazon RDS automatisch eine primäre Datenbank-Instance und repliziert die Daten synchron auf eine Standby-Instance in einer anderen Availability Zone. Jede Availability Zone läuft auf einer eigenen, physisch getrennten, unabhängigen Infrastruktur und ist auf eine hohe Verfügbarkeit ausgelegt. Im Falle eines Infrastrukturausfalls führt Amazon RDS einen automatis

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			chen Failover zum Standby-Modus durch, sodass Sie den Datenbankbetrieb wieder aufnehmen können, sobald der Failover abgeschlo ssen ist.
T0070	Entwickeln Sie Pläne für die Notfallwi ederherstellung und die Aufrechte rhaltung des Betriebs für Systeme, die sich in der Entwicklu ng befinden, und stellen Sie sicher, dass die Systeme getestet werden, bevor sie in eine Produktionsumgebun g übergehen.	s-3 bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) unterstützt die Aufrechterhaltung einer angemesse nen Kapazität und Verfügbarkeit. CRR ermöglicht das automatische, asynchrone Kopieren von Objekten in Amazon S3 Buckets, um die Datenverf ügbarkeit sicherzus tellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0070	Entwickeln Sie Pläne für die Notfallwiederherstellung und die Aufrechterhaltung des Betriebs für Systeme, die sich in der Entwicklung befinden, und stellen Sie sicher, dass die Systeme getestet werden, bevor sie in eine Produktionsumgebung übergehen.	s-3 bucket-versioning-enabled	Die Versionsverwaltung von Amazon Simple Storage Service (Amazon S3)-Buckets hilft dabei, mehrere Varianten eines Objekts im selben Amazon-S3-Bucket zu speichern. Verwenden Sie die Versionsverwaltung, um sämtliche Versionen aller Objekte in Ihrem Amazon-S3-Bucket zu speichern, abzurufen oder wiederherzustellen. Mit der Versionsverwaltung können Sie Versionen sowohl nach unbeabsichtigten Benutzeraktionen als auch nach Anwendungsfehlern problemlos wiederherstellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0070	Entwickeln Sie Pläne für die Notfallwiederherstellung und die Aufrechterhaltung des Betriebs für Systeme, die sich in der Entwicklung befinden, und stellen Sie sicher, dass die Systeme getestet werden, bevor sie in eine Produktionsumgebung übergehen.	vpc-vpn-2-tunnels-up	Redundante Site-to-Site VPN-Tunnel können implementiert werden, um die Anforderungen an die Ausfallsicherheit zu erfüllen. Es verwendet zwei Tunnel, um die Konnektivität sicherzustellen, falls eine der Site-to-Site VPN-Verbindungen nicht verfügbar ist. Um sich vor einem Verbindungsverlust zu schützen, können Sie für den Fall, dass Ihr Kunden-Gateway nicht verfügbar ist, eine zweite Site-to-Site VPN-Verbindung zu Ihrer Amazon Virtual Private Cloud (Amazon VPC) und Ihrem Virtual Private Gateway einrichten, indem Sie ein zweites Kunden-Gateway verwenden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0086	Stellen Sie sicher, dass bei der Installation von Sicherheitspatches für kommerzielle Produkte, die in das Systemdesign integriert sind, die von der Verwaltungsbehörde für die vorgesehene Betriebsumgebung festgelegten Zeitpläne eingehalten werden.	rds-automatic-minor-version-Upgrade-fähig	Aktivieren Sie automatische Unterversions-Upgrades auf Ihren Amazon-Relational-Database-Service (RDS)-Instances, um sicherzustellen, dass die aktuellen Updates für Unterversionen des Relational Database Management System (RDBMS) installiert sind, die Sicherheitspatches und Bugfixes enthalten können.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0086	Stellen Sie sicher, dass bei der Installation von Sicherheitspatches für kommerzielle Produkte, die in das Systemdesign integriert sind, die von der Verwaltungsbehörde für die vorgesehene Betriebsumgebung festgelegten Zeitpläne eingehalten werden.	ec2- prüfen managedinstance-patch-compliance-status	Aktivieren Sie diese Regel, um bei der Identifizierung und Dokumentation von Sicherheitslücken in Amazon Elastic Compute Cloud (Amazon EC2) zu helfen. Die Regel prüft, ob die EC2 Amazon-Instance die Patch-Konformität im AWS Systems Manager gemäß den Richtlinien und Verfahren Ihrer Organisation einhält.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0086	Stellen Sie sicher, dass bei der Installation von Sicherheitspatches für kommerzielle Produkte, die in das Systemdesign integriert sind, die von der Verwaltungsbehörde für die vorgesehene Betriebsumgebung festgelegten Zeitpläne eingehalten werden.	elastic-beanstalk-managed-updates-aktiviert	Durch die Aktivierung verwalteter Plattformupdates für eine Amazon-Elastic-Beanstalk-Umgebung wird sichergestellt, dass die aktuellen verfügbaren Plattform-Fixes, -Updates und -Features für die Umgebung installiert sind. Eine bewährte Methode zur Sicherung von Systemen besteht darin, stets die aktuellen Patches zu installieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0086	Stellen Sie sicher, dass bei der Installation von Sicherheitspatches für kommerzielle Produkte, die in das Systemdesign integriert sind, die von der Verwaltungsbehörde für die vorgesehene Betriebsumgebung festgelegten Zeitpläne eingehalten werden.	redshift-cluster-maintenancesettings-check	Diese Regel stellt sicher, dass Amazon-Redshift-Cluster die bevorzugten Einstellungen für Ihre Organisation haben. Insbesondere sorgt sie dafür, dass Cluster bevorzugte Wartungsfenster und automatisierte Aufbewahrungsfristen für Snapshots für die Datenbank haben. Für diese Regel müssen Sie die allowVersionUpgrade festlegen. Der Standardwert ist „true“. Außerdem können Sie optional den Zeitraum preferredMaintenanceWindow (der Standardwert ist sa: 16:00 -sa: 16:30) und den automated SnapshotRetention Zeitraum (der Standardwert ist 1) festlegen. Die tatsächlichen Werte müssen den Richtlini

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			en Ihrer Organisation entsprechen.
T0110	Identifizieren und/oder ermitteln Sie, ob ein Sicherheitsvorfall auf eine Rechtsverletzung hindeutet, die spezifische rechtliche Schritte erfordert.	securityhub-enabled	AWS Security Hub hilft bei der Überwachung von unbefugtem Personal, Verbindungen, Geräten und Software. AWS Security Hub aggregiert, organisiert und priorisiert die Sicherheitswarnungen oder Ergebnisse mehrerer Dienste. AWS Einige dieser Dienste sind Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer und AWS Firewall Manager sowie AWS Partnerlösungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0110	Identifizieren und/oder ermitteln Sie, ob ein Sicherheitsvorfall auf eine Rechtsverletzung hindeutet, die spezifische rechtliche Schritte erfordert.	cloudwatch-alarm-action-check	Amazon CloudWatch alarmiert, wenn eine Metrik den Schwellenwert für eine bestimmte Anzahl von Bewertungszeiträumen überschreitet. Der Alarm führt eine oder mehrere Aktionen durch, die vom Wert der Metrik oder des Ausdrucks im Vergleich zu einem Schwellenwert in einer Reihe von Zeiträumen abhängt. Diese Regel erfordert einen Wert für alarmActionRequired (Config Default: True), insufficientDataAction Required (Config Default: True), okActionRequired (Config Default: False). Der tatsächliche Wert muss die Alarmaktionen für Ihre Umgebung widerspiegeln.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0110	Identifizieren und/oder ermitteln Sie, ob ein Sicherheitsvorfall auf eine Rechtsverletzung hindeutet, die spezifische rechtliche Schritte erfordert.	guardduty-enabled-centralized	Amazon GuardDuty kann mithilfe von Threat Intelligence Feeds helfen, potenzielle Cybersicherheitsereignisse zu überwachen und zu erkennen. Dazu gehören Listen mit bösartigen IPs und maschinellen Lernmethoden zur Identifizierung unerwarteter, nicht autorisierter und bösartiger Aktivitäten in Ihrer AWS Cloud-Umgebung.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0128	Integrieren Sie automatisierte Funktionen für die Aktualisierung oder das Patchen von Systemsoftware, sofern dies praktikabel ist, und entwickeln Sie Prozesse und Verfahren für die manuelle Aktualisierung und das Patchen von Systemsoftware auf der Grundlage der aktuellen und geplanten Anforderungen an den Patch-Timeline für die Betriebsumgebung des Systems.	rds-automatic-minor-version-Upgrade-fähig	Aktivieren Sie automatische Unterversions-Upgrades auf Ihren Amazon-Relational-Database-Service (RDS)-Instances, um sicherzustellen, dass die aktuellen Updates für Unterversionen des Relational Database Management System (RDBMS) installiert sind, die Sicherheitspatches und Bugfixes enthalten können.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0128	Integrieren Sie automatisierte Funktionen für die Aktualisierung oder das Patchen von Systemsoftware, sofern dies praktikabel ist, und entwickeln Sie Prozesse und Verfahren für die manuelle Aktualisierung und das Patchen von Systemsoftware auf der Grundlage der aktuellen und geplanten Anforderungen an den Patch-Timeline für die Betriebsumgebung des Systems.	ec2- prüfen managedinstance-patch-compliance-status	Aktivieren Sie diese Regel, um bei der Identifizierung und Dokumentation von Sicherheitslücken in Amazon Elastic Compute Cloud (Amazon EC2) zu helfen. Die Regel prüft, ob die EC2 Amazon-Instance die Patch-Konformität im AWS Systems Manager gemäß den Richtlinien und Verfahren Ihrer Organisation einhält.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0128	Integrieren Sie automatisierte Funktionen für die Aktualisierung oder das Patchen von Systemsoftware, sofern dies praktikabel ist, und entwickeln Sie Prozesse und Verfahren für die manuelle Aktualisierung und das Patchen von Systemsoftware auf der Grundlage der aktuellen und geplanten Anforderungen an den Patch-Timeline für die Betriebsumgebung des Systems.	elastic-beanstalk-managed-updates-aktiviert	Durch die Aktivierung verwalteter Plattform updates für eine Amazon-Elastic-Beanstalk-Umgebung wird sichergestellt, dass die aktuellen verfügbaren Plattform -Fixes, -Updates und -Features für die Umgebung installiert sind. Eine bewährte Methode zur Sicherung von Systemen besteht darin, stets die aktuellen Patches zu installieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0128	Integrieren Sie automatisierte Funktionen für die Aktualisierung oder das Patchen von Systemsoftware, sofern dies praktikabel ist, und entwickeln Sie Prozesse und Verfahren für die manuelle Aktualisierung und das Patchen von Systemsoftware auf der Grundlage der aktuellen und geplanten Anforderungen an den Patch-Timeline für die Betriebsumgebung des Systems.	redshift-cluster-maintenancesettings-check	Diese Regel stellt sicher, dass Amazon-Redshift-Cluster die bevorzugten Einstellungen für Ihre Organisation haben. Insbesondere sorgt sie dafür, dass Cluster bevorzugte Wartungsfenster und automatisierte Aufbewahrungsfristen für Snapshots für die Datenbank haben. Für diese Regel müssen Sie die allowVersionUpgrade festlegen. Der Standardwert ist „true“. Außerdem können Sie optional den Zeitraum preferredMaintenanceWindow (der Standardwert ist sa: 16:00 -sa: 16:30) und den automated SnapshotRetention Zeitraum (der Standardwert ist 1) festlegen. Die tatsächlichen Werte müssen den Richtlini

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			en Ihrer Organisation entsprechen.
T0144	Verwalten von Konten, Netzwerkr echten und den Zugriff auf Systeme und Geräte.	account-part-of-or ganizations	Durch die zentrale Verwaltung AWS-Konten innerhalb von AWS Organizations wird sichergestellt, dass die Konten den Vorschriften entsprechen. Eine fehlende zentrale Kontoverwaltung kann zu inkonsist enten Kontokonf igurationen führen, wodurch Ressource n und sensible Daten offengelegt werden können.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0144	Verwalten von Konten, Netzwerkr echten und den Zugriff auf Systeme und Geräte.	alb-waf-enabled	Stellen Sie sicher, dass AWS WAF auf Elastic Load Balancers (ELB) aktiviert ist, um Webanwendungen zu schützen. Eine WAF trägt zum Schutz Ihrer Webanwend ungen oder APIs vor gängigen Web-Explo its bei. Diese Web-Exploits können sich auf die Verfügbar keit auswirken, die Sicherheit gefährden oder übermäßige Ressourcen in Ihrer Umgebung verbrauch en.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0144	Verwalten von Konten, Netzwerkr echten und den Zugriff auf Systeme und Geräte.	api-gw-associated-with-WAF	AWS Mit WAF können Sie eine Reihe von Regeln (als Web Access Control List (Web ACL) bezeichne t) konfigurieren, die Webanfragen auf der Grundlage von anpassbaren Websicherheitsrege ln und -bedingungen, die Sie definieren, zulassen, blockieren oder zählen. Stellen Sie sicher, dass Ihre Amazon-API-Gateway-Stufe mit einer WAF-Web-A CL verknüpft ist, um sie vor böswilligen Angriffen zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0144	Verwalten von Konten, Netzwerkr echten und den Zugriff auf Systeme und Geräte.	autoscaling-launch -config-public-ip- deaktiviert	Wenn Sie Ihre Netzwerkschnittstellen mit einer öffentlichen IP-Adresse konfiguri eren, sind die diesen Netzwerkschnittste llen zugehörigen Ressourcen über das Internet erreichba r. EC2 Ressourcen sollten nicht öffentlic h zugänglich sein, da dies einen unbeabsic htigten Zugriff auf Ihre Anwendungen oder Server ermöglichen kann.
T0144	Verwalten von Konten, Netzwerkr echten und den Zugriff auf Systeme und Geräte.	ec2- instance-profile-a ttached	EC2 Instanzprofile übergeben eine IAM-Rolle an eine Instanz EC2 . Das Anhängen eines Instance-Profils an Ihre Instances kann bei der Implement ierung von geringste n Berechtigungen und der Berechtig ungsverwaltung helfen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0144	Verwalten von Konten, Netzwerkr echten und den Zugriff auf Systeme und Geräte.	ecs-task-definition-user-for-host-mode-check	Wenn für eine Aufgabendefinition erhöhte Berechtig ungen gelten, liegt das daran, dass der Kunde diesen Konfigura tionen ausdrücklich zugestimmt hat. Diese Kontrolle prüft, ob eine unerwartete Berechtigungseskal ation vorliegt, wenn für eine Aufgabend efinition das Host-Netzwerk aktiviert ist, die Kunden aber keine erhöhten Berechtigungen aktiviert haben.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0144	Verwalten von Konten, Netzwerkr echten und den Zugriff auf Systeme und Geräte.	iam-no-inline-policy-überprüfen	Stellen Sie sicher, dass ein Benutzer, eine IAM-Rolle oder eine IAM-Gruppe (AWS Identity and Access Management) nicht über eine Inline-Richtlinie zur Zugriffsk ontrolle auf Systeme und Ressource n verfügt. AWS empfiehlt, verwaltet e Richtlinien anstelle von Inline-Richtlinien zu verwenden. Verwaltete Richtlini en ermöglichen Wiederverwendbarke it, Versionsverwaltung , Rollback und Delegierung der Berechtigungsverwa ltung.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0144	Verwalten von Konten, Netzwerkrechten und den Zugriff auf Systeme und Geräte.	iam-policy-no-statements-with-full-access	Stellen Sie sicher, dass IAM-Aktionen nur auf die benötigten Aktionen beschränkt sind. Wenn Benutzern mehr Rechte eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Rechte und der Aufgabentrennung verstoßen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0144	Verwalten von Konten, Netzwerkr echten und den Zugriff auf Systeme und Geräte.	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) Security Groups können bei der Verwaltung des Netzwerkzugriffs helfen, indem sie eine statusbeh aftete Filterung von eingehendem und ausgehendem Netzwerkverkehr zu Ressourcen bereitste llen. AWS Wenn Sie eingehenden (oder entfernten) Datenverk ehr von 0.0.0.0/0 bis Port 22 auf Ihren Ressourcen nicht zulassen, können Sie den Remote-Zugriff einschränken.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0144	Verwalten von Konten, Netzwerkr echten und den Zugriff auf Systeme und Geräte.	ec-2 instances-in-vpc	Stellen Sie Amazon Elastic Compute Cloud (Amazon EC2) -Instances innerhalb einer Amazon Virtual Private Cloud (Amazon VPC) bereit, um eine sichere Kommunika tion zwischen einer Instance und anderen Services innerhalb der Amazon VPC zu ermöglichen, ohne dass ein Internet-Gateway, ein NAT-Gerät oder eine VPN-Verbindung erforderlich ist. Der gesamte Datenverk ehr bleibt sicher in der AWS Cloud. Domains, die sich innerhalb einer VPC befinden, verfügen aufgrund ihrer logischen Isolierun g im Vergleich zu Domains mit öffentlic hen Endpunkten über eine zusätzlic he Sicherheitsebene. Weisen Sie EC2

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			Amazon-Instances einer Amazon-VPC zu, um den Zugriff ordnungsgemäß zu verwalten.
T0144	Verwalten von Konten, Netzwerkr echten und den Zugriff auf Systeme und Geräte.	no-unrestricted-route-to-igw	Stellen Sie sicher, dass EC2 Amazon-Routentabellen keine uneingeschränkten Routen zu einem Internet-Gateway enthalten. Durch das Entfernen oder Beschränken des Internetzugangs für Workloads innerhalb von Amazon VPCs können unbeabsic htigte Zugriffe in Ihrer Umgebung reduziert werden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0144	Verwalten von Konten, Netzwerkr echten und den Zugriff auf Systeme und Geräte.	redshift-enhanced-vpc-routing-aktiviert	Mit Enhanced-VPC-Routing wird erzwungen, dass der gesamte COPY- und UNLOAD-Da tenverkehr zwischen Ihrem Cluster und Datenrepositorys über Ihre Amazon VPC erfolgt. Anschließ end können Sie VPC-Features wie Sicherheitsgruppen und Netzwerkz ugriffskontrolllisten verwenden, um den Netzwerkverkehr zu schützen. Sie können auch VPC-Flow-Logs verwenden, um den Netzwerkverkehr zu überwachen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0144	Verwalten von Konten, Netzwerkr echten und den Zugriff auf Systeme und Geräte.	s3- -Blocke-periodisch account-level-public-access	Verwalten Sie den Zugriff auf Ressource n in der AWS Cloud, indem Sie sicherste llen, dass Amazon Simple Storage Service (Amazon S3) -Buckets nicht öffentlich zugänglic h sind. Diese Regel trägt dazu bei, sensible Daten vor unbefugten Remote-Benutzern zu schützen, indem sie den öffentlichen Zugriff verhinder t. Mit dieser Regel können Sie optional die Parameter ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) und restrictPublicBuck ets Parameter (Config Default: True) festlegen. Die tatsächlichen Werte müssen den Richtlini

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			en Ihrer Organisation entsprechen.
T0144	Verwalten von Konten, Netzwerkr echten und den Zugriff auf Systeme und Geräte.	ssm-document-not-public	Stellen Sie sicher, dass AWS Systems Manager (SSM) - Dokumente nicht öffentlich sind, da dies einen unbeabsic htigten Zugriff auf Ihre SSM-Dokum ente ermöglichen kann. Ein öffentlic hes SSM-Dokum ent kann Informati onen über Ihr Konto, Ihre Ressourcen und internen Prozesse preisgeben.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0144	Verwalten von Konten, Netzwerkr echten und den Zugriff auf Systeme und Geräte.	vpc-default-security-group-geschlossen	Sicherheitsgruppen von Amazon Elastic Compute Cloud (Amazon EC2) können bei der Verwaltung des Netzwerkzugriffs helfen, indem sie eine statusbehaftete Filterung des ein- und ausgehenden Netzwerkverkehrs zu Ressourcen bereitstellen. AWS Die Beschränk ung des gesamten Datenverkehrs auf die Standardsicherheit sgruppe hilft dabei, den Fernzugriff auf Ihre Ressourcen einzuschränken. AWS

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0144	Verwalten von Konten, Netzwerkr echten und den Zugriff auf Systeme und Geräte.	vpc-sg-open-only-to-authorized-ports	Verwalten Sie den Zugriff auf Ressource n in der AWS Cloud, indem Sie sicherste llen, dass gemeinsam e Ports für Amazon Elastic Compute Cloud (Amazon EC2) -Sicherhe itsgruppen eingeschr ränkt sind. Wenn der Zugriff auf Ports nicht auf vertrauen swürdige Quellen beschränkt wird, kann dies zu Angriffen auf die Verfügbar keit, Integrität und Vertraulichkeit von Systemen führen. Durch die Beschränk ung des Zugriffs auf Ressourcen innerhalb einer Sicherhei tsgruppe aus dem Internet (0.0.0.0/0) kann der Fernzugriff auf interne Systeme gesteuert werden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0144	Verwalten von Konten, Netzwerkr echten und den Zugriff auf Systeme und Geräte.	access-keys-rotated	Die Anmeldein formationen für autorisierte Geräte, Benutzer und Prozesse werden geprüft, indem sichergestellt wird, dass die IAM-Zugri ffsschlüssel gemäß den Vorgaben der Unternehmensrichtl inie rotiert werden. Das regelmäßi ge Ändern der Zugriffsschlüssel ist eine bewährte Sicherheitsmethode . Es verkürzt den Zeitraum, in dem ein Zugriffsschlüssel aktiv ist, und reduziert die Auswirkungen auf das Unternehmen, wenn die Schlüssel kompromittiert werden. Diese Regel erfordert einen Wert für die Zugriffsschlüssel-Rotation (Standard konfiguration: 90). Der tatsächliche Wert muss den Richtlini

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			en Ihrer Organisation entsprechen.
T0144	Verwalten von Konten, Netzwerkr echten und den Zugriff auf Systeme und Geräte.	dms-replication-not-public	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass auf DMS-Replikationsin stanzen nicht öffentlic h zugegriffen werden kann. DMS-Repli kations-Instances können vertrauli che Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.
T0144	Verwalten von Konten, Netzwerkr echten und den Zugriff auf Systeme und Geräte.	ebs-snapshot-public-restorable-überprüfen	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass EBS-Snapshots nicht öffentlich wiederher stellbar sind. EBS-Volume-Snapsho ts können vertrauli che Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0144	Verwalten von Konten, Netzwerkr echten und den Zugriff auf Systeme und Geräte.	ec-2 instance-no-public-ip	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon Elastic Compute Cloud (Amazon EC2) - Instances nicht öffentlich zugänglic h sind. EC2Amazon -Instances können vertrauliche Informati onen enthalten, und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0144	Verwalten von Konten, Netzwerkr echten und den Zugriff auf Systeme und Geräte.	elasticsearch-in-vpc-only	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherste llen, dass sich Amazon OpenSearc h OpenSearch Service (Service) - Domains innerhalb einer Amazon Virtual Private Cloud (Amazon VPC) befinden. Eine OpenSearch Service-Domain innerhalb einer Amazon VPC ermöglicht die sichere Kommunikation zwischen OpenSearc h Service und anderen Services innerhalb der Amazon VPC, ohne dass ein Internet-Gateway, ein NAT-Gerät oder eine VPN-Verbindung erforderlich ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0144	Verwalten von Konten, Netzwerkr echten und den Zugriff auf Systeme und Geräte.	emr-kerberos-enabled	Die Zugriffsberechtigu ngen und -autorisi erungen können verwaltet und nach den Prinzipien der geringsten Berechtig ung und Aufgabent rennung integrier t werden, indem Kerberos für Amazon-EMR-Cluster aktiviert wird. In Kerberos werden Services und Benutzer, die sich authentif izieren müssen, als Prinzipale bezeichnet. Prinzipal e befinden sich in einem Kerberos-Bereich. Innerhalb dieses Bereichs wird ein Kerberos-Server als Key Distribution Center (KDC) bezeichnet. Über diesen Server können sich Prinzipal e authentifizieren. Die Authentifizierung im KDC erfolgt durch die Ausstellu ng von Authentif

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			izierungstickets. Das KDC unterhält eine Datenbank der Prinzipale in seinem Bereich mit ihren Passwörtern und anderen administr ativen Informationen zu jedem Prinzipal.
T0144	Verwalten von Konten, Netzwerkr echten und den Zugriff auf Systeme und Geräte.	emr-master-no-public-ip	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon EMR-Clust er-Masterknoten nicht öffentlich zugänglic h sind. Amazon-EM R-Cluster-Hauptkno ten können vertrauli che Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0144	Verwalten von Konten, Netzwerkr echten und den Zugriff auf Systeme und Geräte.	iam-customer-policy-blocked-kms-Aktionen	AWS Identity and Access Managemen t (IAM) kann Ihnen helfen, die Prinzipien der geringsten Rechte und der Aufgabent rennung in Zugriffsb erechtigungen und Autorisierungen zu integrieren und so zu verhindern, dass Richtlinien blockiert e Aktionen für alle AWS Schlüssel des Key Management Service enthalten. Wenn Benutzer mehr Rechte haben, als für die Ausführung einer Aufgabe erforderl ich sind, kann dies gegen das Prinzip der geringsten Berechtig ung und Aufgabent rennung verstoßen . Mit dieser Regel können Sie den Parameter festlegen . blockedActionsPatt erns (Wert „AWS Bewährte grundlege nde Sicherhei tsmethoden“: kms:

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			Decrypt, kms:ReEncryptFrom). Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.
T0144	Verwalten von Konten, Netzwerkrechten und den Zugriff auf Systeme und Geräte.	iam-group-has-users-überprüfen	AWS Identity and Access Management (IAM) kann Ihnen helfen, die Prinzipien der geringsten Rechte und der Aufgabentrennung mit Zugriffsberechtigungen und Autorisierungen zu integrieren, indem sichergestellt wird, dass IAM-Gruppen mindestens einen Benutzer haben. Die Einteilung von Benutzern in Gruppen auf der Grundlage der ihnen zugewiesenen Berechtigungen oder ihrer Funktion ist eine Möglichkeit, das Prinzip der geringsten Berechtigung zu implementieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0144	Verwalten von Konten, Netzwerkr echten und den Zugriff auf Systeme und Geräte.	iam-inline-policy-blocked-kms-Aktionen	Stellen Sie sicher, dass ein Benutzer, eine IAM-Rolle oder eine IAM-Gruppe (AWS Identity and Access Management) nicht über eine Inline-Richtlinie verfügt, die blockierte Aktionen für alle AWS Schlüssel des Key Management Service zulässt. AWS empfiehlt, verwaltet e Richtlinien anstelle von Inline-Richtlinien zu verwenden. Verwaltete Richtlini en ermöglichen Wiederverwendbarke it, Versionsverwaltung , Rollback und Delegierung der Berechtigungsverwa ltung. Mit dieser Regel können Sie den blockedActionsPatt erns Parameter festlegen. (Wert „AWS Bewährte grundlege nde Sicherhei tsmethoden“: kms: Decrypt, kms:ReEnc ryptFrom). Die

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.
T0144	Verwalten von Konten, Netzwerkrechten und den Zugriff auf Systeme und Geräte.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) kann Ihnen dabei helfen, die Prinzipien der geringsten Rechte und der Aufgabentrennung in Zugriffsberechtigungen und Autorisierungen zu integrieren und so zu verhindern, dass Richtlinien „Effect“: „Allow“ mit „Action“: „*“ anstelle von „Resource“: „*“ enthalten. Wenn Benutzern mehr Rechte eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und der Aufgabentrennung verstoßen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0144	Verwalten von Konten, Netzwerkr echten und den Zugriff auf Systeme und Geräte.	iam-root-access-key-überprüfen	Der Zugriff auf Systeme und Ressourcen kann gesteuert werden, indem überprüft wird, ob der Root-Benu tzer keine Zugriffss chlüssel mit seiner AWS Identity and Access Management (IAM) -Rolle verknüpft hat. Stellen Sie sicher, dass die Root-Zugr iffsschlüssel gelöscht werden. Erstellen und verwenden Sie stattdessen rollenbas ierte Funktionen, AWS-Konten um das Prinzip der geringste n Funktionalität zu berücksichtigen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0144	Verwalten von Konten, Netzwerkrechten und den Zugriff auf Systeme und Geräte.	iam-user-group-membership-überprüfen	AWS Identity and Access Management (IAM) kann Ihnen helfen, Zugriffsberechtigungen und Autorisierungen einzuschränken, indem sichergestellt wird, dass Benutzer Mitglieder mindestens einer Gruppe sind. Wenn Benutzern mehr Berechtigungen eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und Aufgabentrennung verstoßen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0144	Verwalten von Konten, Netzwerkr echten und den Zugriff auf Systeme und Geräte.	iam-user-mfa-enabled	Aktivieren Sie diese Regel, um den Zugriff auf Ressourcen in der AWS -Cloud einzuschränken. Diese Regel stellt sicher, dass die Multi-Faktor-Authe ntifizierung (MFA) für alle Benutzer aktiviert ist. MFA bietet eine weitere Schutzebene zusätzlic h zum Benutzern amen und Passwort. Reduzieren Sie Fälle von kompromittierten Konten, indem Sie MFA für Benutzer vorschreiben.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0144	Verwalten von Konten, Netzwerkr echten und den Zugriff auf Systeme und Geräte.	iam-user-no-policies-überprüfen	Diese Regel stellt sicher, dass AWS Identity and Access Management (IAM) -Richtlinien nur Gruppen oder Rollen zugewiese n werden, um den Zugriff auf Systeme und Ressourcen zu kontrollieren. Die Zuweisung von Berechtig ungen auf Gruppen- oder Rollenebene trägt dazu bei, die Wahrscheinlichkeit zu verringern, dass eine Identität übermäßige Berechtigungen erhält oder beibehält.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0144	Verwalten von Konten, Netzwerkrechten und den Zugriff auf Systeme und Geräte.	iam-user-unused-credentials-überprüfen	AWS Identity and Access Management (IAM) kann Ihnen bei Zugriffsberechtigungen und Autorisierungen helfen, indem es nach IAM-Passwörtern und Zugriffsschlüsseln sucht, die für einen bestimmten Zeitraum nicht verwendet wurden. Wenn ungenutzte Anmeldeinformationen identifiziert werden, müssen Sie sie deaktivieren und/oder entfernen, da dies gegen das Prinzip der geringsten Berechtigung verstoßen könnte. Für diese Regel müssen Sie einen Wert für das maxCredentialUsage Alter festlegen (Standardkonfiguration: 90). Der tatsächliche Wert muss den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0144	Verwalten von Konten, Netzwerkrechten und den Zugriff auf Systeme und Geräte.	lambda-function-public-access-verboten	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass AWS Lambda-Funktionen nicht öffentlich zugänglich sind. Der öffentliche Zugriff kann möglicherweise die Verfügbarkeit von Ressourcen beeinträchtigen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0144	Verwalten von Konten, Netzwerkr echten und den Zugriff auf Systeme und Geräte.	lambda-inside-vpc	Stellen Sie AWS Lambda-Funktionen in einer Amazon Virtual Private Cloud (Amazon VPC) bereit, um eine sichere Kommunika tion zwischen einer Funktion und anderen Diensten innerhalb der Amazon VPC zu gewährleisten. Bei dieser Konfiguration sind kein Internet-Gateway, kein NAT-Gerät und keine VPN-Verbindung erforderlich. Der gesamte Datenverk ehr bleibt sicher in der Cloud. AWS Domains, die sich innerhalb einer VPC befinden, verfügen aufgrund ihrer logischen Isolierun g im Vergleich zu Domains mit öffentlic hen Endpunkten über eine zusätzliche Sicherheitsebene. Um den Zugriff ordnungsg emäß zu verwalten,

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			sollten AWS Lambda-Funktionen einer VPC zugewiesen werden.
T0144	Verwalten von Konten, Netzwerkrechten und den Zugriff auf Systeme und Geräte.	opensearch-in-vpc-only	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass sich die Domains von Amazon Elasticsearch Service (Amazon ES) innerhalb einer Amazon Virtual Private Cloud (Amazon VPC) befinden. Eine ES-Domain in einer Amazon VPC ermöglicht eine sichere Kommunikation zwischen Amazon ES und anderen Services innerhalb der Amazon VPC, ohne dass ein Internet-Gateway, ein NAT-Gerät oder eine VPN-Verbindung benötigt wird.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0144	Verwalten von Konten, Netzwerkr echten und den Zugriff auf Systeme und Geräte.	rds-instance-public-access-überprüfen	Verwalten Sie den Zugriff auf Ressource n in der AWS Cloud, indem Sie sicherste llen, dass Amazon Relational Database Service (Amazon RDS) -Instance s nicht öffentlic h sind. Amazon-RDS-Datenbank-Instances können vertrauliche Informati onen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0144	Verwalten von Konten, Netzwerkr echten und den Zugriff auf Systeme und Geräte.	rds-snapshots-public-prohibited	Verwalten Sie den Zugriff auf Ressource n in der AWS Cloud, indem Sie sicherste llen, dass Amazon Relational Database Service (Amazon RDS) -Instance s nicht öffentlic h sind. Amazon-RDS-Datenbank-Instances können vertrauliche Informati onen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0144	Verwalten von Konten, Netzwerkr echten und den Zugriff auf Systeme und Geräte.	redshift-cluster-public-access-überprüfen	Verwalten Sie den Zugriff auf Ressource n in der AWS Cloud, indem Sie sicherste llen, dass Amazon Redshift Redshift-Cluster nicht öffentlic h sind. Amazon-Re dshift-Cluster können vertrauliche Informati onen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0144	Verwalten von Konten, Netzwerkr echten und den Zugriff auf Systeme und Geräte.	restricted-common-ports	Verwalten Sie den Zugriff auf Ressource n in der AWS Cloud, indem Sie sicherste llen, dass gemeinsam e Ports für Amazon Elastic Compute Cloud (Amazon EC2) -Sicherhe itsgruppen eingeschr ränkt sind. Wenn der Zugriff auf Ports nicht auf vertrauen swürdige Quellen beschränkt wird, kann dies zu Angriffen auf die Verfügbar keit, Integrität und Vertraulichkeit von Systemen führen. Mit dieser Regel können Sie optional die Parameter blockedPo rt1–blockedPort5 festlegen (Standard konfigurationen: 20, 21, 3389, 3306, 4333). Die tatsächli chen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0144	Verwalten von Konten, Netzwerkr echten und den Zugriff auf Systeme und Geräte.	s-3 bucket-public-read -prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie nur autorisierten Benutzern, Prozessen und Geräten Zugriff auf Amazon Simple Storage Service (Amazon S3) - Buckets gewähren. Die Verwaltung des Zugriffs sollte mit der Klassifizierung der Daten übereinst immen.
T0144	Verwalten von Konten, Netzwerkr echten und den Zugriff auf Systeme und Geräte.	s3- bucket-public-writ e-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie nur autorisierten Benutzern, Prozessen und Geräten Zugriff auf Amazon Simple Storage Service (Amazon S3) - Buckets gewähren. Die Verwaltung des Zugriffs sollte mit der Klassifizierung der Daten übereinst immen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0144	Verwalten von Konten, Netzwerkr echten und den Zugriff auf Systeme und Geräte.	sagemaker-notebook-no-direct-Interne tzugang	Verwalten Sie den Zugriff auf Ressource n in der AWS Cloud, indem Sie sicherste llen, dass SageMaker Amazon-Notebooks keinen direkten Internetzugang zulassen. Indem Sie direkten Internetz ugang blockieren, vermeiden Sie, dass unbefugte Benutzer auf sensible Daten zugreifen.
T0144	Verwalten von Konten, Netzwerkr echten und den Zugriff auf Systeme und Geräte.	secretsmanager-rot ation-enabled-check	Diese Regel stellt sicher, dass bei AWS Secrets Manager Manager-Geheimnissen die Rotation aktiviert ist. Die regelmäßige Rotation von Secrets kann den Zeitraum verkürzen, in dem ein Secret aktiv ist, und möglicherweise die Auswirkungen auf das Unternehmen verringern, falls das Secret kompromittiert wird.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0144	Verwalten von Konten, Netzwerkr echten und den Zugriff auf Systeme und Geräte.	subnet-auto-assign-public-ip-deaktiviert	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon Virtual Private Cloud (VPC) -Subnetzen nicht automatisch eine öffentliche IP-Adress e zugewiesen wird. Amazon Elastic Compute Cloud (EC2) -Instances, die in Subnetzen gestartet werden, in denen dieses Attribut aktiviert ist, haben ihrer primären Netzwerkschnittste lle eine öffentliche IP-Adresse zugewiesen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0151	Überwachen und bewerten Sie die Wirksamkeit der Cybersicherheitsmaßnahmen des Unternehmens, um sicherzustellen, dass sie das beabsichtigte Schutzniveau bieten.	securityhub-enabled	AWS Security Hub hilft bei der Überwachung von unbefugtem Personal, Verbindungen, Geräten und Software. AWS Security Hub aggregiert, organisiert und priorisiert die Sicherheitswarnungen oder Ergebnisse mehrerer Dienste. AWS Einige dieser Dienste sind Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer und AWS Firewall Manager sowie AWS Partnerlösungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0151	Überwachen und bewerten Sie die Wirksamkeit der Cybersicherheitsmaßnahmen des Unternehmens, um sicherzustellen, dass sie das beabsichtigte Schutzniveau bieten.	cloudwatch-alarm-action-check	Amazon CloudWatch alarmiert, wenn eine Metrik den Schwellenwert für eine bestimmte Anzahl von Bewertungszeiträumen überschreitet. Der Alarm führt eine oder mehrere Aktionen durch, die vom Wert der Metrik oder des Ausdrucks im Vergleich zu einem Schwellenwert in einer Reihe von Zeiträumen abhängt. Diese Regel erfordert einen Wert für alarmActionRequired (Config Default: True), insufficientDataAction Required (Config Default: True), okActionRequired (Config Default: False). Der tatsächliche Wert muss die Alarmaktionen für Ihre Umgebung widerspiegeln.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0151	Überwachen und bewerten Sie die Wirksamkeit der Cybersicherheitsma ßnahmen des Unternehmens, um sicherzustellen, dass sie das beabsichtigte Schutzniveau bieten.	guardduty-enabled-centralized	Amazon GuardDuty kann mithilfe von Threat Intellige nce Feeds helfen, potenzielle Cybersich erheitsereignisse zu überwachen und zu erkennen. Dazu gehören Listen mit bösartigen IPs und maschinel len Lernmethoden zur Identifizierung unerwarteter, nicht autorisierter und bösartiger Aktivitäten in Ihrer AWS Cloud-Umgebung.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0152	Überwachen und verwalten von Datenbanken, um eine optimale Leistung sicherzus tellen.	db-instance-backup-enabled	Die Sicherung sfunktion von Amazon RDS erstellt Sicherung en Ihrer Datenbank en und Transakti onsprotokolle. Amazon RDS erstellt einen Snapshot für das Speichervolume Ihrer DB-Instance, sodass die gesamte DB-Instance gesichert wird. Sie können im System spezifische Aufbewahrungsfrist en festlegen, um Ihre Ausfallsicherheits anforderungen zu erfüllen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0152	Überwachen und verwalten von Datenbanken, um eine optimale Leistung sicherzustellen.	dynamodb-autoscaling-enabled	Amazon DynamoDB Auto Scaling verwendet den AWS Application Auto Scaling-Service, um die bereitgestellte Durchsatzkapazität so anzupassen, dass sie automatisch auf tatsächliche Verkehrsmuster reagiert. Auf diese Weise kann eine Tabelle oder ein globaler sekundärer Index die bereitgestellte Lese-/Schreibkapazität erhöhen, um plötzliche Erhöhungen des Datenverkehrs ohne Drosselung zu bewältigen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0152	Überwachen und verwalten von Datenbanken, um eine optimale Leistung sicherzustellen.	dynamodb-in-backup-plan	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon DynamoDB-Tabellen Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0152	Überwachen und verwalten von Datenbanken, um eine optimale Leistung sicherzus tellen.	dynamodb-pitr-enab led	Aktivieren Sie diese Regel, um zu überprüfen, ob die Informationen gesichert wurden. Es verwaltet auch die Backups, indem es sicherstellt, dass die point-in-time Wiederherstellung in Amazon DynamoDB aktiviert ist. Bei der Wiederherstellung werden fortlaufende Backups Ihrer Tabelle für die letzten 35 Tage gespeichert.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0152	Überwachen und verwalten von Datenbanken, um eine optimale Leistung sicherzus tellen.	dynamodb-throughpu t-limit-check	Aktivieren Sie diese Regel, um sicherzustellen, dass die bereitgestellte Durchsatzkapazität in Ihren Amazon-Dy namoDB-Tabellen überprüft wird. Dies ist der Umfang der Lese- und Schreibak tivitäten, der von den jeweiligen Tabellen unterstützt werden kann. DynamoDB verwendet diese Informationen für das Reservieren ausreichender Systemressourcen, um Ihren Durchsatz anforderungen gerecht zu werden. Diese Regel generiert eine Warnung, wenn sich der Durchsatz dem Höchstlimit für ein Kundenkonto nähert. Mit dieser Regel können Sie optional die Parameter RCUThreshold Kontoprozentsatz

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			(Konfigurationsstandard: 80) und WCUThreshold Kontoprozentsatz (Konfigurationsstandard: 80) festlegen. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.
T0152	Überwachen und verwalten von Datenbanken, um eine optimale Leistung sicherzustellen.	rds-automatic-minor-version-Upgrade aktiviert	Aktivieren Sie automatische Unterversions-Upgrades auf Ihren Amazon-Relational-Database-Service (RDS)-Instances, um sicherzustellen, dass die aktuellen Updates für Unterversionen des Relational Database Management System (RDBMS) installiert sind, die Sicherheitspatches und Bugfixes enthalten können.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0152	Überwachen und verwalten von Datenbanken, um eine optimale Leistung sicherzustellen.	rds-enhanced-monitoring-enabled	Aktivieren Sie Amazon Relational Database Service (Amazon RDS), um die Verfügbarkeit von Amazon RDS zu überwachen. Dies bietet einen detaillierten Einblick in den Zustand Ihrer Amazon-RDS-Datenbank-Instances. Wenn der Amazon-RDS-Speicher mehr als ein zugrunde liegendes physisches Gerät verwendet, erfasst Enhanced Monitoring die Daten für jedes Gerät. Wenn die Datenbank-Instance von Amazon RDS in einer Multi-AZ-Bereitstellung ausgeführt wird, werden außerdem die Daten für jedes Gerät auf dem sekundären Host sowie die Metriken des sekundären Hosts erfasst.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0152	Überwachen und verwalten von Datenbanken, um eine optimale Leistung sicherzus tellen.	rds-instance-deletion-protection-aktiviert	Stellen Sie sicher, dass Amazon Relational Database Service (Amazon RDS)-Instances den Löschschutz aktiviert haben. Verwenden Sie den Löschschu tz, um zu verhindern, dass Ihre Amazon-RD S-Instances versehent lich oder böswillig gelöscht werden, was zum Verlust der Verfügbarkeit Ihrer Anwendungen führen kann.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0152	Überwachen und verwalten von Datenbanken, um eine optimale Leistung sicherzustellen.	rds-instance-public-access-überprüfen	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Relational Database Service (Amazon RDS) -Instances nicht öffentlich sind. Amazon-RDS-Datenbank-Instances können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0152	Überwachen und verwalten von Datenbanken, um eine optimale Leistung sicherzus tellen.	rds-in-backup-plan	Um Sie bei Datensich erungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon Relational Database Service (Amazon RDS) -Instance s Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwaltet er Backup-Service mit einer richtlini enbasierten Backup-Lösung. Diese Lösung vereinfac ht Ihr Sicherung smanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforde rungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0152	Überwachen und verwalten von Datenbanken, um eine optimale Leistung sicherzustellen.	rds-logging-enabled	Um die Protokollierung und Überwachung in Ihrer Umgebung zu erleichtern, stellen Sie sicher, dass die Amazon Relational Database Service (Amazon RDS)-Protokollierung aktiviert ist. Mit der Amazon-RDS-Protokollierung können Sie Ereignisse wie Verbindungen, Verbindungsabbrüche, Abfragen oder abgefragte Tabellen erfassen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0152	Überwachen und verwalten von Datenbanken, um eine optimale Leistung sicherzustellen.	rds-multi-az-support	Die Multi-AZ-Unterstützung in Amazon Relational Database Service (Amazon RDS) bietet eine verbesserte Verfügbarkeit und Beständigkeit von Datenbank-Instances. Wenn Sie eine Multi-AZ-Datenbank-Instance bereitstellen, erstellt Amazon RDS automatisch eine primäre Datenbank-Instance und repliziert die Daten synchron auf eine Standby-Instance in einer anderen Availability Zone. Jede Availability Zone läuft auf einer eigenen, physisch getrennten, unabhängigen Infrastruktur und ist auf eine hohe Verfügbarkeit ausgelegt. Im Falle eines Infrastrukturausfalls führt Amazon RDS einen automatis

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			chen Failover zum Standby-Modus durch, sodass Sie den Datenbankbetrieb wieder aufnehmen können, sobald der Failover abgeschlo ssen ist.
T0152	Überwachen und verwalten von Datenbanken, um eine optimale Leistung sicherzus tellen.	rds-snapshots-public-prohibited	Verwalten Sie den Zugriff auf Ressource n in der AWS Cloud, indem Sie sicherste llen, dass Amazon Relational Database Service (Amazon RDS) -Instance s nicht öffentlic h sind. Amazon-RDS-Datenbank-Instances können vertrauliche Informati onen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0152	Überwachen und verwalten von Datenbanken, um eine optimale Leistung sicherzustellen.	rds-snapshot-encrypted	Stellen Sie sicher, dass die Verschlüsselung für Ihre Amazon Relational Database Service (Amazon RDS)-Snapshots aktiviert ist. Da sensible Daten auch im Ruhezustand vorhanden sein können, sollten Sie die Verschlüsselung von Daten im Ruhezustand aktivieren, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0152	Überwachen und verwalten von Datenbanken, um eine optimale Leistung sicherzustellen.	rds-storage-encrypted	Zum Schutz von Daten im Ruhezustand müssen Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon Relational Database Service (Amazon RDS)-Instances aktiviert ist. Da sensible Daten in Amazon-RDS-Instances gespeichert werden können, sollten Sie die Verschlüsselung von Daten im Ruhezustand aktivieren, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0152	Überwachen und verwalten von Datenbanken, um eine optimale Leistung sicherzustellen.	redshift-backup-enabled	Stellen Sie zur Unterstützung der Datensicherungsprozesse sicher, dass Ihre Amazon-Redshift-Cluster über automatisierte Snapshots verfügen. Wenn automatisierte Snapshots für einen Cluster aktiviert sind, erstellt Redshift in regelmäßigen Abständen Snapshots dieses Clusters. Standardmäßig erstellt Redshift alle acht Stunden oder alle 5 GB einen Snapshot für jeden Knoten mit Datenänderungen oder je nachdem, was zuerst eintritt.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0152	Überwachen und verwalten von Datenbanken, um eine optimale Leistung sicherzustellen.	redshift-cluster-configuration-check	Um Daten im Ruhezustand zu schützen, muss die Verschlüsselung für Ihre Amazon-Redshift-Cluster aktiviert sein. Sie müssen auch sicherstellen, dass die erforderlichen Konfigurationen auf Amazon-Redshift-Clustern bereitgestellt werden. Die Prüfungsprotokollierung muss aktiviert sein, um Informationen zu Verbindungen und Benutzeraktivitäten in der Datenbank bereitzustellen. Diese Regel erfordert, dass ein Wert für clusterDbEncrypted (Config Default: TRUE) und LoggingEnabled (Config Default: TRUE) gesetzt ist. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0152	Überwachen und verwalten von Datenbanken, um eine optimale Leistung sicherzus tellen.	redshift-cluster-maintenancesettings-check	Diese Regel stellt sicher, dass Amazon-Redshift-Cluster die bevorzugten Einstellungen für Ihre Organisation haben. Insbesondere sorgt sie dafür, dass Cluster bevorzugte Wartungsfenster und automatisierte Aufbewahrungsfristen für Snapshots für die Datenbank haben. Für diese Regel müssen Sie den festlegen. allowVersionUpgrade Der Standardwert ist „true“. Außerdem können Sie optional den Zeitraum preferredMaintenanceWindow (der Standardwert ist sa: 16:00 -sa: 16:30) und den automated SnapshotRetention Zeitraum (der Standardwert ist 1) festlegen. Die tatsächlichen Werte müssen den Richtlini

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			en Ihrer Organisation entsprechen.
T0152	Überwachen und verwalten von Datenbanken, um eine optimale Leistung sicherzus tellen.	redshift-cluster-public-access-überprüfen	Verwalten Sie den Zugriff auf Ressource n in der AWS Cloud, indem Sie sicherste llen, dass Amazon Redshift Redshift-Cluster nicht öffentlic h sind. Amazon-Re dshift-Cluster können vertrauliche Informati onen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0152	Überwachen und verwalten von Datenbanken, um eine optimale Leistung sicherzus tellen.	redshift-enhanced-vpc-routing-aktiviert	Mit Enhanced-VPC-Routing wird erzwungen, dass der gesamte COPY- und UNLOAD-Da tenverkehr zwischen Ihrem Cluster und Datenrepositorys über Ihre Amazon VPC erfolgt. Anschließ end können Sie VPC-Features wie Sicherheitsgruppen und Netzwerkz ugriffskontrolllisten verwenden, um den Netzwerkverkehr zu schützen. Sie können auch VPC-Flow-Logs verwenden, um den Netzwerkverkehr zu überwachen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0152	Überwachen und verwalten von Datenbanken, um eine optimale Leistung sicherzus tellen.	redshift-require-tls-ssl	Stellen Sie sicher, dass Ihre Amazon-Redshift-Cluster eine TLS/SSL-Verschlüss elung erfordern, um eine Verbindung zu SQL-Clients herzustel len. Da sensible Daten vorhanden sein können, sollten Sie die Verschlüsselung bei der Übertragung aktivieren, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0152	Überwachen und verwalten von Datenbanken, um eine optimale Leistung sicherzus tellen.	redshift-cluster-kms-enabled	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass die Verschlüs selung mit AWS Key Management Service (AWS KMS) für Ihren Amazon Redshift Redshift-Cluster aktiviert ist. Um eventuell vorhanden e sensible Daten im Ruhezustand in Redshift-Clustern zu schützen, muss die Verschlüsselung von Daten im Ruhezusta nd aktiviert sein.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0153	Überwachen der Netzwerkkapazität und -leistung.	autoscaling-group-elb-healthcheck-erforderlich	Die Elastic Load Balancer (ELB) - Zustandsprüfungen für Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling Scaling-Gruppen unterstützen die Aufrechterhaltung einer angemessenen Kapazität und Verfügbarkeit. Der Load Balancer sendet regelmäßig Pings, versucht Verbindungen herzustellen oder sendet Anfragen, um den Zustand der EC2 Amazon-Instances in einer Gruppe mit auto-scaling zu testen. Wenn eine Instance nicht zurückmeldet, wird der Traffic an eine neue EC2 Amazon-Instance gesendet.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0153	Überwachen der Netzwerkkapazität und -leistung.	dynamodb-throughput-limit-check	Aktivieren Sie diese Regel, um sicherzustellen, dass die bereitgestellte Durchsatzkapazität in Ihren Amazon-DynamoDB-Tabellen überprüft wird. Dies ist der Umfang der Lese- und Schreibaktivitäten, der von den jeweiligen Tabellen unterstützt werden kann. DynamoDB verwendet diese Informationen für das Reservieren ausreichender Systemressourcen, um Ihren Durchsatz anforderungen gerecht zu werden. Diese Regel generiert eine Warnung, wenn sich der Durchsatz dem Höchstlimit für ein Kundenkonto nähert. Mit dieser Regel können Sie optional die Parameter RCUThreshold Kontoprozentsatz

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			(Konfigurationsstandard: 80) und WCUThreshold Kontoprozentsatz (Konfigurationsstandard: 80) festlegen. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.
T0153	Überwachen der Netzwerkkapazität und -leistung.	vpc-flow-logs-enabled	VPC-Flow-Protokolle erfassen detaillierte Informationsdatensätze über den IP-Datenverkehr, der zu und von Netzwerkschnittstellen in Ihrer Amazon Virtual Private Cloud (Amazon VPC) fließt. Standardmäßig enthalten Flow-Protokolldatensätze Werte für die verschiedenen Komponenten des IP-Flows, einschließlich Quelle, Ziel und Protokoll.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0153	Überwachen der Netzwerkkapazität und -leistung.	vpc-vpn-2-tunnels-up	Redundante Site-to-Site VPN-Tunnel können implementiert werden, um die Anforderungen an die Ausfallsicherheit zu erfüllen. Es verwendet zwei Tunnel, um die Konnektivität sicherzustellen, falls eine der Site-to-Site VPN-Verbindungen nicht verfügbar ist. Um sich vor einem Verbindungsverlust zu schützen, können Sie für den Fall, dass Ihr Kunden-Gateway nicht verfügbar ist, eine zweite Site-to-Site VPN-Verbindung zu Ihrer Amazon Virtual Private Cloud (Amazon VPC) und Ihrem Virtual Private Gateway einrichten, indem Sie ein zweites Kunden-Gateway verwenden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0154	Überwachen der Nutzung von Ressourcen und Ressourcen im Wissensmanagement und Erstellen entsprechender Berichte.	cw-loggroup-retention-period-überprüfen	Stellen Sie sicher, dass die Ereignisprotokolldaten für Ihre Protokollgruppen über eine Mindestdauer aufbewahrt werden, um die Fehlerbehebung und forensische Untersuchungen zu unterstützen. Fehlende frühere Ereignisprotokolldaten erschweren die Rekonstruierung und Identifizierung potenziell schädlicher Ereignisse.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0154	Überwachen der Nutzung von Ressourcen und Ressourcen im Wissensmanagement und Erstellen entsprechender Berichte.	elasticsearch-logs-to-cloudwatch	Stellen Sie sicher, dass für Amazon OpenSearch Service-Domains Fehlerprotokolle aktiviert und zur Aufbewahrung und Beantwortung an Amazon CloudWatch Logs gestreamt werden. Domain-Fehlerprotokolle sind bei Sicherheits- und Zugriffsprüfungen sowie bei der Diagnose von Verfügbarkeitsproblemen nützlich.
T0154	Überwachen der Nutzung von Ressourcen und Ressourcen im Wissensmanagement und Erstellen entsprechender Berichte.	lambda-concurrency-check	Diese Regel stellt sicher, dass die Höchst- und Untergrenzen für die Gleichzeitigkeit einer Lambda-Funktion festgelegt werden. Dies kann Sie beim Baselining für die Anzahl der Anforderungen unterstützen, die Ihre Funktion zu einem bestimmten Zeitpunkt verarbeitet.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0154	Überwachen der Nutzung von Ressourcen und Ressourcen im Wissensmanagement und Erstellen entsprechender Berichte.	lambda-dlq-check	Aktivieren Sie diese Regel, um das entsprechende Personal über Amazon Simple Queue Service (Amazon SQS) oder Amazon Simple Notification Service (Amazon SNS) zu benachrichtigen, wenn eine Funktion ausgefallen ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0154	Überwachen der Nutzung von Ressourcen und Ressourcen im Wissensmanagement und Erstellen entsprechender Berichte.	multi-region-cloudtrail-enabled	AWS CloudTrail zeichnet Aktionen und API-Aufrufe der AWS Management Console auf. Sie können feststellen, welche Benutzer und Konten angerufen wurden AWS, von welcher Quell-IP-Adresse aus die Anrufe getätigt wurden und wann die Anrufe erfolgten. CloudTrail übermittelt Protokolldateien aus allen AWS Regionen an Ihren S3-Bucket , wenn MULTI_REG ION_CLOUD _TRAIL_ENABLED aktiviert ist. Außerdem wird beim AWS Start einer neuen Region derselbe Trail in der neuen Region erstellt. CloudTrail Dadurch erhalten Sie automatis ch Protokolldateien mit API-Aktivitäten für die neue Region.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0154	Überwachen der Nutzung von Ressourcen und Ressourcen im Wissensmanagement und Erstellen entsprechender Berichte.	rds-enhanced-monitoring-enabled	Aktivieren Sie Amazon Relational Database Service (Amazon RDS), um die Verfügbarkeit von Amazon RDS zu überwachen. Dies bietet einen detaillierten Einblick in den Zustand Ihrer Amazon-RDS-Datenbank-Instances. Wenn der Amazon-RDS-Speicher mehr als ein zugrunde liegendes physisches Gerät verwendet, erfasst Enhanced Monitoring die Daten für jedes Gerät. Wenn die Datenbank-Instance von Amazon RDS in einer Multi-AZ-Bereitstellung ausgeführt wird, werden außerdem die Daten für jedes Gerät auf dem sekundären Host sowie die Metriken des sekundären Hosts erfasst.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0154	Überwachen der Nutzung von Ressourcen und Ressourcen im Wissensmanagement und Erstellen entsprechender Berichte.	rds-logging-enabled	Um die Protokollierung und Überwachung in Ihrer Umgebung zu erleichtern, stellen Sie sicher, dass die Amazon Relational Database Service (Amazon RDS)-Protokollierung aktiviert ist. Mit der Amazon-RDS-Protokollierung können Sie Ereignisse wie Verbindungen, Verbindungsabbrüche, Abfragen oder abgefragte Tabellen erfassen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0154	Überwachen der Nutzung von Ressourcen und Ressourcen im Wissensmanagement und Erstellen entsprechender Berichte.	securityhub-enabled	AWS Security Hub hilft bei der Überwachung von unbefugtem Personal, Verbindungen, Geräten und Software. AWS Security Hub aggregiert, organisiert und priorisiert die Sicherheitswarnungen oder Ergebnisse mehrerer Dienste. AWS Einige dieser Dienste sind Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer und AWS Firewall Manager sowie AWS Partnerlösungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0154	Überwachen der Nutzung von Ressourcen und Ressourcen im Wissensmanagement und Erstellen entsprechender Berichte.	wafv2-logging-enabled	Um Ihnen bei der Protokollierung und Überwachung in Ihrer Umgebung zu helfen, aktivieren Sie die AWS WAF (V2) -Protokollierung im regionalen und globalen Web. ACLs AWS Die WAF-Protokollierung bietet detaillierte Informationen über den Datenverkehr, der von Ihrer Web-ACL analysiert wird. In den Protokollen werden die Uhrzeit aufgezeichnet, zu der die AWS WAF die Anfrage von Ihrer AWS Ressource erhalten hat, Informationen über die Anfrage und eine Aktion für die Regel, der jede Anfrage entsprach.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0154	Überwachen der Nutzung von Ressourcen und Ressourcen im Wissensmanagement und Erstellen entsprechender Berichte.	api-gw-execution-logging-aktiviert	Die API-Gateway-Protokollierung zeigt detaillierte Ansichten der Benutzer, die auf die API zugegriffen haben, und wie diese Benutzer auf die API zugegriffen haben. Diese Insights ermöglichen die Einsicht in Benutzeraktivitäten.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0154	Überwachen der Nutzung von Ressourcen und Ressourcen im Wissensmanagement und Erstellen entsprechender Berichte.	autoscaling-group-elb-healthcheck-erforderlich	Die Elastic Load Balancer (ELB) - Zustandsprüfungen für Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling Scaling-Gruppen unterstützen die Aufrechterhaltung einer angemessenen Kapazität und Verfügbarkeit. Der Load Balancer sendet regelmäßig Pings, versucht Verbindungen herzustellen oder sendet Anfragen, um den Zustand der EC2 Amazon-Instances in einer Gruppe mit auto-scaling zu testen. Wenn eine Instance nicht zurückmeldet, wird der Traffic an eine neue EC2 Amazon-Instance gesendet.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0154	Überwachen der Nutzung von Ressourcen und Ressourcen im Wissensmanagement und Erstellen entsprechender Berichte.	beanstalk-enhanced-health-reporting-aktiviert	AWS Die verbesserte Zustandsberichterstattung von Elastic Beanstalk ermöglicht eine schnellere Reaktion auf Veränderungen im Zustand der zugrunde liegenden Infrastruktur. Diese Änderungen könnten zu einer mangelnden Verfügbarkeit der Anwendung führen. Die erweiterten Zustandsberichte von Elastic Beanstalk bieten eine Statusbeschreibung, um den Schweregrad der identifizierten Probleme einzuschätzen und mögliche Ursachen zu identifizieren, die untersucht werden müssen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0154	Überwachen der Nutzung von Ressourcen und Ressourcen im Wissensmanagement und Erstellen entsprechender Berichte.	cloud-trail-cloud-watch-Logs aktiviert	Verwenden Sie Amazon CloudWatch , um Protokoll ereignisaktivitäten zentral zu sammeln und zu verwalten. Die Aufnahme von AWS CloudTrail Daten liefert Einzelheiten zu den API-Aufrufaktivitäten in Ihrem AWS-Konto.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0154	Überwachen der Nutzung von Ressourcen und Ressourcen im Wissensmanagement und Erstellen entsprechender Berichte.	cloudtrail-enabled	AWS CloudTrail kann bei der Nichtabstreitbarkeit helfen, indem Aktionen und API-Aufrufe der AWS Management Console aufgezeichnet werden. Sie können die Benutzer und die Benutzer AWS-Konten , die einen AWS Dienst aufgerufen haben, die Quell-IP-Adresse, über die die Aufrufe generiert wurden, und den Zeitpunkt der Anrufe identifizieren. Einzelheiten zu den erfassten Daten finden Sie unter Inhalt des AWS CloudTrail Datensatzes.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0154	Überwachen der Nutzung von Ressourcen und Ressourcen im Wissensmanagement und Erstellen entsprechender Berichte.	cloudtrail-s3-data events-enabled	Die Erfassung von Simple Storage Service (Amazon S3)-Datenereignissen unterstützt die Erkennung von ungewöhnlichen Aktivitäten. Zu den Details gehören Informationen zu dem AWS -Konto, das auf einen Amazon-S3-Bucket zugegriffen hat, die IP-Adresse und die Uhrzeit des Ereignisses.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0154	Überwachen der Nutzung von Ressourcen und Ressourcen im Wissensmanagement und Erstellen entsprechender Berichte.	cloudwatch-alarm-action-check	Amazon CloudWatch alarmiert, wenn eine Metrik den Schwellenwert für eine bestimmte Anzahl von Bewertungszeiträumen überschreitet. Der Alarm führt eine oder mehrere Aktionen durch, die vom Wert der Metrik oder des Ausdrucks im Vergleich zu einem Schwellenwert in einer Reihe von Zeiträumen abhängt. Diese Regel erfordert einen Wert für alarmActionRequired (Config Default: True), insufficientDataAction Required (Config Default: True), okActionRequired (Config Default: False). Der tatsächliche Wert muss die Alarmaktionen für Ihre Umgebung widerspiegeln.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0154	Überwachen der Nutzung von Ressourcen und Ressourcen im Wissensmanagement und Erstellen entsprechender Berichte.	dynamodb-throughput-limit-check	Aktivieren Sie diese Regel, um sicherzustellen, dass die bereitgestellte Durchsatzkapazität in Ihren Amazon-DynamoDB-Tabellen überprüft wird. Dies ist der Umfang der Lese- und Schreibaktivitäten, der von den jeweiligen Tabellen unterstützt werden kann. DynamoDB verwendet diese Informationen für das Reservieren ausreichender Systemressourcen, um Ihren Durchsatz anforderungen gerecht zu werden. Diese Regel generiert eine Warnung, wenn sich der Durchsatz dem Höchstlimit für ein Kundenkonto nähert. Mit dieser Regel können Sie optional die Parameter RCUThreshold Kontoprozentsatz

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			(Konfigurationsstandard: 80) und WCUThreshold Kontoprozentsatz (Konfigurationsstandard: 80) festlegen. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.
T0154	Überwachen der Nutzung von Ressourcen und Ressourcen im Wissensmanagement und Erstellen entsprechender Berichte.	ec2- instance-detailed-monitoring-enabled	Aktivieren Sie diese Regel, um die Amazon Elastic Compute Cloud (Amazon EC2) - Instance-Überwachung auf der EC2 Amazon-Konsole zu verbessern, in der Monitoring-Diagramme mit einem Zeitraum von 1 Minute für die Instance angezeigt werden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0154	Überwachen der Nutzung von Ressourcen und Ressourcen im Wissensmanagement und Erstellen entsprechender Berichte.	elb-logging-enabled	Die Elastic-Load-Balancing-Aktivität ist ein zentraler Kommunikationspunkt innerhalb einer Umgebung. Stellen Sie sicher, dass die ELB-Protokollierung aktiviert ist. Die gesammelten Daten enthalten detaillierte Informationen zu Anfragen, die an den ELB gesendet wurden. Jedes Protokoll enthält Informationen wie die Zeit, zu der die Anforderung einging, die Client-IP-Adresse, Latenzen, Anforderungspfade und Serverantworten.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0154	Überwachen der Nutzung von Ressourcen und Ressourcen im Wissensmanagement und Erstellen entsprechender Berichte.	guardduty-enabled-centralized	Amazon GuardDuty kann mithilfe von Threat Intellige nce Feeds helfen, potenzielle Cybersich erheitsereignisse zu überwachen und zu erkennen. Dazu gehören Listen mit bösartigen IPs und maschinel len Lernmethoden zur Identifizierung unerwarteter, nicht autorisierter und bösartiger Aktivitäten in Ihrer AWS Cloud-Umgebung.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0154	Überwachen der Nutzung von Ressourcen und Ressourcen im Wissensmanagement und Erstellen entsprechender Berichte.	redshift-cluster-configuration-check	Um Daten im Ruhezustand zu schützen, muss die Verschlüsselung für Ihre Amazon-Redshift-Cluster aktiviert sein. Sie müssen auch sicherstellen, dass die erforderlichen Konfigurationen auf Amazon-Redshift-Clustern bereitgestellt werden. Die Prüfungsprotokollierung muss aktiviert sein, um Informationen zu Verbindungen und Benutzeraktivitäten in der Datenbank bereitzustellen. Diese Regel erfordert, dass ein Wert für clusterDbEncrypted (Config Default: TRUE) und LoggingEnabled (Config Default: TRUE) gesetzt ist. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0154	Überwachen der Nutzung von Ressourcen und Ressourcen im Wissensmanagement und Erstellen entsprechender Berichte.	s3- bucket-logging-enabled	Die Amazon Simple Storage Service (Amazon S3)-Serverzugriffs protokollierung bietet eine Methode zur Überwachu ng des Netzwerks im Hinblick auf potenzielle Cybersich erheitsereignisse. Die Ereignisse werden überwacht, indem detaillierte Aufzeichn ungen über die Anfragen erfasst werden, die an einen Amazon-S3-Bucket gestellt wurden. Jeder Zugriffsprotokolle intrag enthält Details zu einer einzelnen Zugriffsanfrage. Zu den Details gehören Anforderer, Bucket-Name, Anforderu ngszeit, Anforderu ngsaktion, Antwortst atus und Fehlercode, falls relevant.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0154	Überwachen der Nutzung von Ressourcen und Ressourcen im Wissensmanagement und Erstellen entsprechender Berichte.	vpc-flow-logs-enabled	VPC-Flow-Protokolle erfassen detaillierte Informationsdatensätze über den IP-Datenverkehr, der zu und von Netzwerkschnittstellen in Ihrer Amazon Virtual Private Cloud (Amazon VPC) fließt. Standardmäßig enthalten Flow-Protokolldatensätze Werte für die verschiedenen Komponenten des IP-Flows, einschließlich Quelle, Ziel und Protokoll.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0156	Beaufsichtigung und Abgabe von Empfehlungen zum Konfigurationsmanagement.	account-part-of-organizations	Durch die zentrale Verwaltung AWS-Konten innerhalb von AWS Organizations wird sichergestellt, dass die Konten den Vorschriften entsprechen. Eine fehlende zentrale Kontoverwaltung kann zu inkonsistenten Kontokonfigurationen führen, wodurch Ressourcen und sensible Daten offengelegt werden können.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0156	Beaufsichtigung und Abgabe von Empfehlungen zum Konfigurationsmanagement.	ec2-manager instance-managed-by-systems	Eine Bestandsaufnahme der Softwareplattformen und Anwendungen innerhalb des Unternehmens ist möglich, indem Amazon Elastic Compute Cloud (Amazon EC2) - Instances mit AWS Systems Manager verwaltet werden. Verwenden Sie AWS Systems Manager, um detaillierte Systemkonfigurationen, Betriebssystem-Patch-Levels, Namen und Typ der Dienste, Softwareinstallationen, Anwendungsname, Herausgeber und Version sowie andere Details zu Ihrer Umgebung bereitzustellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0156	Beaufsichtigung und Abgabe von Empfehlungen zum Konfigurationsmanagement.	ec2-check managedinstance-association-compliance-status	Verwenden Sie AWS Systems Manager Associations, um bei der Inventarisierung von Softwareplattformen und Anwendungen innerhalb eines Unternehmens zu helfen. AWS Systems Manager weist Ihren verwalteten Instances einen Konfigurationsstatus zu und ermöglicht es Ihnen, Basiswerte für Betriebssystem-Patch-Levels, Softwareinstallationen, Anwendungskonfigurationen und andere Details zu Ihrer Umgebung festzulegen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0156	Beaufsichtigung und Abgabe von Empfehlungen zum Konfigurationsmanagement.	ec2-prüfen managedinstance-patch-compliance-status	Aktivieren Sie diese Regel, um bei der Identifizierung und Dokumentation von Sicherheitslücken in Amazon Elastic Compute Cloud (Amazon EC2) zu helfen. Die Regel prüft, ob die EC2 Amazon-Instance die Patch-Konformität im AWS Systems Manager gemäß den Richtlinien und Verfahren Ihrer Organisation einhält.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0156	Beaufsichtigung und Abgabe von Empfehlungen zum Konfigurationsmanagement.	redshift-cluster-maintenancesettings-check	Diese Regel stellt sicher, dass Amazon-Redshift-Cluster die bevorzugten Einstellungen für Ihre Organisation haben. Insbesondere sorgt sie dafür, dass Cluster bevorzugte Wartungsfenster und automatisierte Aufbewahrungsfristen für Snapshots für die Datenbank haben. Für diese Regel müssen Sie die festlegen allowVersionUpgrade. Der Standardwert ist „true“. Außerdem können Sie optional den Zeitraum preferredMaintenanceWindow (der Standardwert ist sa: 16:00 -sa: 16:30) und den automated SnapshotRetention Zeitraum (der Standardwert ist 1) festlegen. Die tatsächlichen Werte müssen den Richtlini

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			en Ihrer Organisation entsprechen.
T0156	Beaufsichtigung und Abgabe von Empfehlungen zum Konfigurationsmanagement.	elastic-beanstalk-managed-updates-aktiviert	Durch die Aktivierung verwalteter Plattform updates für eine Amazon-Elastic-Beanstalk-Umgebung wird sichergestellt, dass die aktuellen verfügbaren Plattform -Fixes, -Updates und -Features für die Umgebung installiert sind. Eine bewährte Methode zur Sicherung von Systemen besteht darin, stets die aktuellen Patches zu installieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0156	Beaufsichtigung und Abgabe von Empfehlungen zum Konfigurationsmanagement.	restricted-common-ports	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass gemeinsame Ports für Amazon Elastic Compute Cloud (Amazon EC2) -Sicherheitsgruppen eingeschränkt sind. Wenn der Zugriff auf Ports nicht auf vertrauenswürdige Quellen beschränkt wird, kann dies zu Angriffen auf die Verfügbarkeit, Integrität und Vertraulichkeit von Systemen führen. Mit dieser Regel können Sie optional die Parameter blockedPort1–blockedPort5 festlegen (Standardkonfigurationen: 20, 21, 3389, 3306, 4333). Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0156	Beaufsichtigung und Abgabe von Empfehlungen zum Konfigurationsmanagement.	vpc-default-security-group-geschlossen	Sicherheitsgruppen von Amazon Elastic Compute Cloud (Amazon EC2) können bei der Verwaltung des Netzwerkzugriffs helfen, indem sie eine statusbehaftete Filterung des ein- und ausgehenden Netzwerkverkehrs zu Ressourcen bereitstellen. AWS Die Beschränkung des gesamten Datenverkehrs auf die Standardsicherheitsgruppe hilft dabei, den Fernzugriff auf Ihre Ressourcen einzuschränken. AWS

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0156	Beaufsichtigung und Abgabe von Empfehlungen zum Konfigurationsmanagement.	vpc-sg-open-only-to-authorized-ports	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass gemeinsame Ports für Amazon Elastic Compute Cloud (Amazon EC2) -Sicherheitsgruppen eingeschränkt sind. Wenn der Zugriff auf Ports nicht auf vertrauenswürdige Quellen beschränkt wird, kann dies zu Angriffen auf die Verfügbarkeit, Integrität und Vertraulichkeit von Systemen führen. Durch die Beschränkung des Zugriffs auf Ressourcen innerhalb einer Sicherheitsgruppe aus dem Internet (0.0.0.0/0) kann der Fernzugriff auf interne Systeme gesteuert werden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0160	Patchen von Netzwerkschwachstellen, um sicherzustellen, dass die Informationen vor Außenstehenden geschützt sind.	rds-automatic-minor-version-Upgrade aktiviert	Aktivieren Sie automatische Unterversions-Upgrades auf Ihren Amazon-Relational-Database-Service (RDS)-Instances, um sicherzustellen, dass die aktuellen Updates für Unterversionen des Relational Database Management System (RDBMS) installiert sind, die Sicherheitspatches und Bugfixes enthalten können.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0160	Patchen von Netzwerkschwachstellen, um sicherzustellen, dass die Informationen vor Außenstehenden geschützt sind.	ec2- prüfen managedinstance-association-compliance-status	Verwenden Sie AWS Systems Manager Associations, um bei der Inventarisierung von Softwareplattformen und Anwendungen innerhalb eines Unternehmens zu helfen. AWS Systems Manager weist Ihren verwalteten Instances einen Konfigurationsstatus zu und ermöglicht es Ihnen, Basiswerte für Betriebssystem-Patch-Levels, Softwareinstallationen, Anwendungskonfigurationen und andere Details zu Ihrer Umgebung festzulegen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0160	Patchen von Netzwerkschwachstellen, um sicherzustellen, dass die Informationen vor Außenstehenden geschützt sind.	ec2-prüfen managedinstance-patch-compliance-status	Aktivieren Sie diese Regel, um bei der Identifizierung und Dokumentation von Sicherheitslücken in Amazon Elastic Compute Cloud (Amazon EC2) zu helfen. Die Regel prüft, ob die EC2 Amazon-Instance die Patch-Konformität im AWS Systems Manager gemäß den Richtlinien und Verfahren Ihrer Organisation einhält.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0162	Durchführung von Sicherungen und Wiederherstellungen von Datenbanken zur Gewährleistung der Datenintegrität.	dynamodb-in-backup-plan	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon DynamoDB-Tabellen Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0162	Durchführung von Sicherungen und Wiederherstellungen von Datenbanken zur Gewährleistung der Datenintegrität.	ebs-in-backup-plan	Stellen Sie zur Unterstützung der Datensicherungspro zesse sicher, dass Ihre Amazon Elastic Block Store (Amazon EBS) -Volumes Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwaltet er Backup-Service mit einer richtlini enbasierten Backup-Lösung. Diese Lösung vereinfacht Ihre Backup-Verwaltung und ermöglicht es Ihnen, Ihre geschäftl ichen und behördlic hen Anforderungen bezüglich Backups zu erfüllen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0162	Durchführung von Sicherungen und Wiederherstellungen von Datenbanken zur Gewährleistung der Datenintegrität.	efs-in-backup-plan	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon Elastic File System (Amazon EFS) -Dateisysteme Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0162	Durchführung von Sicherungen und Wiederherstellungen von Datenbanken zur Gewährleistung der Datenintegrität.	rds-in-backup-plan	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon Relational Database Service (Amazon RDS) -Instances Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0162	Durchführung von Sicherungen und Wiederherstellungen von Datenbanken zur Gewährleistung der Datenintegrität.	redshift-backup-enabled	Stellen Sie zur Unterstützung der Datensicherungsprozesse sicher, dass Ihre Amazon-Redshift-Cluster über automatisierte Snapshots verfügen. Wenn automatisierte Snapshots für einen Cluster aktiviert sind, erstellt Redshift in regelmäßigen Abständen Snapshots dieses Clusters. Standardmäßig erstellt Redshift alle acht Stunden oder alle 5 GB einen Snapshot für jeden Knoten mit Datenänderungen oder je nachdem, was zuerst eintritt.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0162	Durchführung von Sicherungen und Wiederherstellungen von Datenbanken zur Gewährleistung der Datenintegrität.	backup-plan-min-frequency-and-min-retention-check	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihr AWS Backup-Plan auf eine Mindestfrequenz und Aufbewahrung festgelegt ist. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen. Mit dieser Regel können Sie die Parameter requiredFrequencyValue (Config default: 1), requiredRetentionDays (Config default: 35) und requiredFrequencyUnit

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			(Config default: days) festlegen. Der tatsächliche Wert muss den Anforderungen Ihrer Organisation entsprechen.
T0162	Durchführung von Sicherungen und Wiederherstellungen von Datenbanken zur Gewährleistung der Datenintegrität.	backup-recovery-point-encrypted	Stellen Sie sicher, dass die Verschlüsselung für Ihre AWS Backup-Wiederherstellungspunkte aktiviert ist. Da sensible Daten auch im Ruhezustand vorhanden sein können, sollten Sie die Verschlüsselung im Ruhezustand aktivieren, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0162	Durchführung von Sicherungen und Wiederherstellungen von Datenbanken zur Gewährleistung der Datenintegrität.	backup-recovery-point-manual-Löschen-deaktiviert	Stellen Sie sicher, dass Ihren AWS Backup-Wiederherstellungspunkten eine ressourcenbasierte Richtlinie zugeordnet ist, die das Löschen von Wiederherstellungspunkten verhindert. Die Verwendung einer ressourcenbasierten Richtlinie zur Verhinderung des Löschens von Wiederherstellungspunkten kann dazu beitragen, ein versehentliches oder absichtliches Löschen zu unterbinden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0162	Durchführung von Sicherungen und Wiederherstellungen von Datenbanken zur Gewährleistung der Datenintegrität.	db-instance-backup-enabled	Die Sicherung sfunktion von Amazon RDS erstellt Sicherung en Ihrer Datenbank en und Transakti onsprotokolle. Amazon RDS erstellt einen Snapshot für das Speichervolume Ihrer DB-Instance, sodass die gesamte DB-Instance gesichert wird. Sie können im System spezifische Aufbewahrungsfrist en festlegen, um Ihre Ausfallsicherheits anforderungen zu erfüllen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0162	Durchführung von Sicherungen und Wiederherstellungen von Datenbanken zur Gewährleistung der Datenintegrität.	dynamodb-pitr-enabled	Aktivieren Sie diese Regel, um zu überprüfen, ob die Informationen gesichert wurden. Es verwaltet auch die Backups, indem es sicherstellt, dass die point-in-time Wiederherstellung in Amazon DynamoDB aktiviert ist. Bei der Wiederherstellung werden fortlaufende Backups Ihrer Tabelle für die letzten 35 Tage gespeichert.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0162	Durchführung von Sicherungen und Wiederherstellungen von Datenbanken zur Gewährleistung der Datenintegrität.	ec2--Plan resources-protected-by-backup	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon Elastic Compute Cloud (Amazon EC2) -Ressourcen Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0162	Durchführung von Sicherungen und Wiederherstellungen von Datenbanken zur Gewährleistung der Datenintegrität.	elasticache-redis-cluster-automatic-Backup-Check	Wenn automatische Backups aktiviert sind, ElastiCache erstellt Amazon täglich ein Backup des Clusters. Die Sicherung kann für eine von Ihrer Organisation festgelegte Anzahl von Tagen aufbewahrt werden. Automatische Backups schützen vor Datenverlust. Bei einem Ausfall können Sie einen neuen Cluster erstellen, der Ihre Daten aus dem aktuellen Backup wiederherstellt.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0162	Durchführung von Sicherungen und Wiederherstellungen von Datenbanken zur Gewährleistung der Datenintegrität.	redshift-cluster-maintenancesettings-check	Diese Regel stellt sicher, dass Amazon-Redshift-Cluster die bevorzugten Einstellungen für Ihre Organisation haben. Insbesondere sorgt sie dafür, dass Cluster bevorzugte Wartungsfenster und automatisierte Aufbewahrungsfristen für Snapshots für die Datenbank haben. Für diese Regel müssen Sie die festlegen allowVersionUpgrade. Der Standardwert ist „true“. Außerdem können Sie optional den Zeitraum preferredMaintenanceWindow (der Standardwert ist sa: 16:00 -sa: 16:30) und den automated SnapshotRetention Zeitraum (der Standardwert ist 1) festlegen. Die tatsächlichen Werte müssen den Richtlini

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			en Ihrer Organisation entsprechen.
T0162	Durchführung von Sicherungen und Wiederherstellungen von Datenbanken zur Gewährleistung der Datenintegrität.	s3- bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) unterstützt die Aufrechterhaltung einer angemesse nen Kapazität und Verfügbarkeit. CRR ermöglicht das automatische, asynchrone Kopieren von Objekten in Amazon S3 Buckets, um die Datenverf ügbarkeit sicherzus tellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0162	Durchführung von Sicherungen und Wiederherstellungen von Datenbanken zur Gewährleistung der Datenintegrität.	s-3 bucket-versioning-enabled	Die Versionsv erwaltung von Amazon Simple Storage Service (Amazon S3)-Bucke ts hilft dabei, mehrere Varianten eines Objekts im selben Amazon-S3-Bucket zu speichern. Verwenden Sie die Versionsv erwaltung, um sämtliche Versionen aller Objekte in Ihrem Amazon-S3-Bucket zu speichern , abzurufen oder wiederherzustellen . Mit der Versionsv erwaltung können Sie Versionen sowohl nach unbeabsic htigten Benutzera ktionen als auch nach Anwendungsfehlern problemlos wiederher stellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0166	Durchführung von Ereigniskorrelation unter Verwendung von Informationen, die aus einer Vielzahl von Quellen innerhalb des Unternehmens gesammelt wurden, um ein Situation sbewusstsein zu erlangen und die Wirksamkeit eines beobachteten Angriffs zu bestimmen.	cw-loggroup-retent ion-period-überprüfen	Stellen Sie sicher, dass die Ereignisp rotokolldaten für Ihre Protokollgruppen über eine Mindestdauer aufbewahrt werden, um die Fehlerbeh ebung und forensisc he Untersuchungen zu unterstützen. Fehlende frühere Ereignisprotokolld aten erschweren die Rekonstruierung und Identifizierung potenziell schädlicher Ereignisse.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0166	Durchführung von Ereigniskorrelation unter Verwendung von Informationen, die aus einer Vielzahl von Quellen innerhalb des Unternehmens gesammelt wurden, um ein Situation sbewusstsein zu erlangen und die Wirksamkeit eines beobachteten Angriffs zu bestimmen.	elasticsearch-logs-to-cloudwatch	Stellen Sie sicher, dass für Amazon OpenSearch Service-Domains Fehlerpro tokolle aktiviert und zur Aufbewahrung und Beantwortung an Amazon CloudWatc h Logs gestreamt werden. Domain-Fehlerprotokolle sind bei Sicherhei ts- und Zugriffsp rüfungen sowie bei der Diagnose von Verfügbarkeitsprob lemen nützlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0166	Durchführung von Ereigniskorrelation unter Verwendung von Informationen, die aus einer Vielzahl von Quellen innerhalb des Unternehmens gesammelt wurden, um ein Situation sbewusstsein zu erlangen und die Wirksamkeit eines beobachteten Angriffs zu bestimmen.	multi-region-cloudtrail-enabled	AWS CloudTrail zeichnet Aktionen und API-Aufrufe der AWS Management Console auf. Sie können feststellen, welche Benutzer und Konten angerufen wurden AWS, von welcher Quell-IP-Adresse aus die Anrufe getätigt wurden und wann die Anrufe erfolgten. CloudTrail übermittelt Protokolldateien aus allen AWS Regionen an Ihren S3-Bucket , wenn MULTI_REG ION_CLOUD _TRAIL_ENABLED aktiviert ist. Außerdem wird beim AWS Start einer neuen Region derselbe Trail in der neuen Region erstellt. CloudTrail Dadurch erhalten Sie automatis ch Protokolldateien mit API-Aktivitäten für die neue Region.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0166	Durchführung von Ereigniskorrelation unter Verwendung von Informationen, die aus einer Vielzahl von Quellen innerhalb des Unternehmens gesammelt wurden, um ein Situation sbewusstsein zu erlangen und die Wirksamkeit eines beobachteten Angriffs zu bestimmen.	wafv2-logging-enabled	Um die Protokollierung und Überwachung in Ihrer Umgebung zu erleichtern, aktivieren Sie die AWS WAF (V2) -Protokollierung im regionalen und globalen Web ACLs. AWS Die WAF-Protokollierung bietet detaillierte Informationen über den Datenverkehr, der von Ihrer Web-ACL analysiert wird. In den Protokollen werden die Uhrzeit aufgezeichnet, zu der die AWS WAF die Anfrage von Ihrer AWS Ressource erhalten hat, Informationen über die Anfrage und eine Aktion für die Regel, der jede Anfrage entsprach.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0166	Durchführung von Ereigniskorrelation unter Verwendung von Informationen, die aus einer Vielzahl von Quellen innerhalb des Unternehmens gesammelt wurden, um ein Situation sbewusstsein zu erlangen und die Wirksamkeit eines beobachteten Angriffs zu bestimmen.	api-gw-execution-logging-aktiviert	Die API-Gateway-Protokollierung zeigt detaillierte Ansichten der Benutzer, die auf die API zugegriff en haben, und wie diese Benutzer auf die API zugegriffen haben. Diese Insights ermöglichen die Einsicht in Benutzera ktivitäten.
T0166	Durchführung von Ereigniskorrelation unter Verwendung von Informationen, die aus einer Vielzahl von Quellen innerhalb des Unternehmens gesammelt wurden, um ein Situation sbewusstsein zu erlangen und die Wirksamkeit eines beobachteten Angriffs zu bestimmen.	cloud-trail-cloud-watch-logs-aktiviert	Verwenden Sie Amazon CloudWatc h , um Protokoll ereignisaktivitäten zentral zu sammeln und zu verwalten. Die Aufnahme von AWS CloudTrail Daten liefert Einzelheiten zu den API-Aufrufaktivitä ten in Ihrem AWS-Konto.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0166	Durchführung von Ereigniskorrelation unter Verwendung von Informationen, die aus einer Vielzahl von Quellen innerhalb des Unternehmens gesammelt wurden, um ein Situation sbewusstsein zu erlangen und die Wirksamkeit eines beobachteten Angriffs zu bestimmen.	cloudtrail-enabled	AWS CloudTrail kann bei der Nichtabst reitbarkeit helfen, indem Aktionen und API-Aufrufe der AWS Management Console aufgezeic hnet werden. Sie können die Benutzer und die Benutzer AWS-Konten , die einen AWS Dienst aufgerufen haben, die Quell-IP-Adresse, über die die Aufrufe generiert wurden, und den Zeitpunkt der Anrufe identifiz ieren. Einzelheiten zu den erfassten Daten finden Sie unter Inhalt des AWS CloudTrail Datensatzes.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0166	Durchführung von Ereigniskorrelation unter Verwendung von Informationen, die aus einer Vielzahl von Quellen innerhalb des Unternehmens gesammelt wurden, um ein Situation sbewusstsein zu erlangen und die Wirksamkeit eines beobachteten Angriffs zu bestimmen.	cloudtrail-s3-data events-enabled	Die Erfassung von Simple Storage Service (Amazon S3)-Datenereigniss en unterstützt die Erkennung von ungewöhnlichen Aktivitäten. Zu den Details gehören Informationen zu dem AWS -Konto, das auf einen Amazon-S3-Bucket zugegriffen hat, die IP-Adresse und die Uhrzeit des Ereignisses.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0166	Durchführung von Ereigniskorrelation unter Verwendung von Informationen, die aus einer Vielzahl von Quellen innerhalb des Unternehmens gesammelt wurden, um ein Situation sbewusstsein zu erlangen und die Wirksamkeit eines beobachteten Angriffs zu bestimmen.	elb-logging-enabled	Die Elastic-Load-Balancing-Aktivität ist ein zentraler Kommunikationspunk t innerhalb einer Umgebung. Stellen Sie sicher, dass die ELB-Protokollierun g aktiviert ist. Die gesammelten Daten enthalten detaillie rte Informationen zu Anfragen, die an den ELB gesendet wurden. Jedes Protokoll enthält Informationen wie die Zeit, zu der die Anforderung einging, die Client-IP -Adresse, Latenzen, Anforderungspfade und Serverantworten.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0166	Durchführung von Ereigniskorrelation unter Verwendung von Informationen, die aus einer Vielzahl von Quellen innerhalb des Unternehmens gesammelt wurden, um ein Situation sbewusstsein zu erlangen und die Wirksamkeit eines beobachteten Angriffs zu bestimmen.	rds-logging-enabled	Um die Protokoll ierung und Überwachung in Ihrer Umgebung zu erleichtern, stellen Sie sicher, dass die Amazon Relationa l Database Service (Amazon RDS)-Prot okollierung aktiviert ist. Mit der Amazon-RDS-Protokollierung können Sie Ereigniss e wie Verbindungen, Verbindungsabbrüch e, Abfragen oder abgefragte Tabellen erfassen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0166	Durchführung von Ereigniskorrelation unter Verwendung von Informationen, die aus einer Vielzahl von Quellen innerhalb des Unternehmens gesammelt wurden, um ein Situation sbewusstsein zu erlangen und die Wirksamkeit eines beobachteten Angriffs zu bestimmen.	redshift-cluster-configuration-check	Um Daten im Ruhezustand zu schützen, muss die Verschlüsselung für Ihre Amazon-Redshift-Cluster aktiviert sein. Sie müssen auch sicherstellen, dass die erforderlichen Konfigurationen auf Amazon-Redshift-Clustern bereitgestellt werden. Die Prüfungsprotokollierung muss aktiviert sein, um Informationen zu Verbindungen und Benutzeraktivitäten in der Datenbank bereitzustellen. Diese Regel erfordert, dass ein Wert für clusterDbEncrypted (Config Default: TRUE) und LoggingEnabled (Config Default: TRUE) gesetzt ist. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0166	Durchführung von Ereigniskorrelation unter Verwendung von Informationen, die aus einer Vielzahl von Quellen innerhalb des Unternehmens gesammelt wurden, um ein Situation sbewusstsein zu erlangen und die Wirksamkeit eines beobachteten Angriffs zu bestimmen.	s3- bucket-logging-enabled	Die Amazon Simple Storage Service (Amazon S3)-Serverzugriffs protokollierung bietet eine Methode zur Überwachu ng des Netzwerks im Hinblick auf potenzielle Cybersich erheitsereignisse. Die Ereignisse werden überwacht, indem detaillierte Aufzeichn ungen über die Anfragen erfasst werden, die an einen Amazon-S3-Bucket gestellt wurden. Jeder Zugriffsprotokolle intrag enthält Details zu einer einzelnen Zugriffsanfrage. Zu den Details gehören Anforderer, Bucket-Name, Anforderu ngszeit, Anforderu ngsaktion, Antwortst atus und Fehlercode, falls relevant.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0166	Durchführung von Ereigniskorrelation unter Verwendung von Informationen, die aus einer Vielzahl von Quellen innerhalb des Unternehmens gesammelt wurden, um ein Situation sbewusstsein zu erlangen und die Wirksamkeit eines beobachteten Angriffs zu bestimmen.	vpc-flow-logs-enabled	VPC-Flow-Protokolle erfassen detaillierte Informationsdatensätze über den IP-Datenverkehr, der zu und von Netzwerkschnittstellen in Ihrer Amazon Virtual Private Cloud (Amazon VPC) fließt. Standardmäßig enthalten Flow-Protokolldatensätze Werte für die verschiedenen Komponenten des IP-Flows, einschließlich Quelle, Ziel und Protokoll.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0168	Durchführung eines Hash-Vergleichs mit einer bestehenden Datenbank.	cloud-trail-log-file-Validierung aktiviert	Verwenden Sie die AWS CloudTrail Protokolldateivalidierung, um die Integrität von Protokollen zu überprüfen. CloudTrail Mithilfe der Protokolldateivalidierung kann festgestellt werden, ob eine Protokolldatei geändert oder gelöscht wurde oder ob sie nach der Übermittlung CloudTrail unverändert geblieben ist. Dieses Feature wurde mit dem Branchenstandard entsprechenden Algorithmen entwickelt: SHA-256 für die Hashfunktion und SHA-256 mit RSA für digitale Signaturen. Das macht es rechnerisch unmöglich, CloudTrail Protokolldateien unbemerkt zu ändern, zu löschen oder zu fälschen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0195	Sorgen Sie für einen gesteuerten Fluss relevanter Informationen (über webbasierte Portale oder auf andere Weise) auf der Grundlage der Missionsanforderungen.	alb-waf-enabled	Stellen Sie sicher, dass AWS WAF auf Elastic Load Balancers (ELB) aktiviert ist, um Webanwendungen zu schützen. Eine WAF trägt zum Schutz Ihrer Webanwendungen oder APIs vor gängigen Web-Exploits bei. Diese Web-Exploits können sich auf die Verfügbarkeit auswirken, die Sicherheit gefährden oder übermäßige Ressourcen in Ihrer Umgebung verbrauchen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0195	Sorgen Sie für einen gesteuerten Fluss relevanter Informationen (über webbasierte Portale oder auf andere Weise) auf der Grundlage der Missionsanforderungen.	api-gw-associated-with-WAF	AWS Mit WAF können Sie eine Reihe von Regeln (als Web Access Control List (Web ACL) bezeichnet) konfigurieren, die Webanfragen auf der Grundlage von anpassbaren Websicherheitsregeln und -bedingungen, die Sie definieren, zulassen, blockieren oder zählen. Stellen Sie sicher, dass Ihre Amazon-API-Gateway-Stufe mit einer WAF-Web-ACL verknüpft ist, um sie vor böswilligen Angriffen zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0195	Sorgen Sie für einen gesteuerten Fluss relevanter Informationen (über webbasierte Portale oder auf andere Weise) auf der Grundlage der Missionsanforderungen.	autoscaling-launch-config-public-ip-deaktiviert	Wenn Sie Ihre Netzwerkschnittstellen mit einer öffentlichen IP-Adresse konfigurieren, sind die diesen Netzwerkschnittstellen zugehörigen Ressourcen über das Internet erreichbar. EC2 Ressourcen sollten nicht öffentlich zugänglich sein, da dies einen unbeabsichtigten Zugriff auf Ihre Anwendungen oder Server ermöglichen kann.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0195	Sorgen Sie für einen gesteuerten Fluss relevanter Informationen (über webbasierte Portale oder auf andere Weise) auf der Grundlage der Missionsanforderungen.	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) Security Groups können bei der Verwaltung des Netzwerkzugriffs helfen, indem sie eine statusbehaftete Filterung von eingehendem und ausgehendem Netzwerkverkehr zu Ressourcen bereitstellen. AWS Wenn Sie eingehenden (oder entfernten) Datenverkehr von 0.0.0.0/0 bis Port 22 auf Ihren Ressourcen nicht zulassen, können Sie den Remote-Zugriff einschränken.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0195	Sorgen Sie für einen gesteuerten Fluss relevanter Informationen (über webbasierte Portale oder auf andere Weise) auf der Grundlage der Missionsanforderungen.	ec-2 instances-in-vpc	Stellen Sie Amazon Elastic Compute Cloud (Amazon EC2) -Instances innerhalb einer Amazon Virtual Private Cloud (Amazon VPC) bereit, um eine sichere Kommunikation zwischen einer Instance und anderen Services innerhalb der Amazon VPC zu ermöglichen, ohne dass ein Internet-Gateway, ein NAT-Gerät oder eine VPN-Verbindung erforderlich ist. Der gesamte Datenverkehr bleibt sicher in der AWS Cloud. Domains, die sich innerhalb einer VPC befinden, verfügen aufgrund ihrer logischen Isolierung im Vergleich zu Domains mit öffentlichen Endpunkten über eine zusätzliche Sicherheitsebene. Weisen Sie EC2

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			Amazon-Instances einer Amazon-VPC zu, um den Zugriff ordnungsgemäß zu verwalten.
T0195	Sorgen Sie für einen gesteuerten Fluss relevanter Informationen (über webbasierte Portale oder auf andere Weise) auf der Grundlage der Missionsanforderungen.	no-unrestricted-route-to-igw	Stellen Sie sicher, dass EC2 Amazon-Routentabellen keine uneingeschränkten Routen zu einem Internet-Gateway enthalten. Durch das Entfernen oder Beschränken des Internetzugangs für Workloads innerhalb von Amazon VPCs können unbeabsichtigte Zugriffe in Ihrer Umgebung reduziert werden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0195	Sorgen Sie für einen gesteuerten Fluss relevanter Informati onen (über webbasier te Portale oder auf andere Weise) auf der Grundlage der Missionsanforderun gen.	redshift-enhanced-vpc-routing-aktiviert	Mit Enhanced-VPC-Routing wird erzwungen, dass der gesamte COPY- und UNLOAD-Da tenverkehr zwischen Ihrem Cluster und Datenrepositorys über Ihre Amazon VPC erfolgt. Anschließ end können Sie VPC-Features wie Sicherheitsgruppen und Netzwerkz ugriffskontrolllisten verwenden, um den Netzwerkverkehr zu schützen. Sie können auch VPC-Flow-Logs verwenden, um den Netzwerkverkehr zu überwachen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0195	Sorgen Sie für einen gesteuerten Fluss relevanter Informationen (über webbasierte Portale oder auf andere Weise) auf der Grundlage der Missionsanforderungen.	s3- -Blocke-periodisch account-level-public-access	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Simple Storage Service (Amazon S3) -Buckets nicht öffentlich zugänglich sind. Diese Regel trägt dazu bei, sensible Daten vor unbefugten Remote-Benutzern zu schützen, indem sie den öffentlichen Zugriff verhindert. Mit dieser Regel können Sie optional die Parameter ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) und restrictPublicBuckets Parameter (Config Default: True) festlegen. Die tatsächlichen Werte müssen den Richtlini

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			en Ihrer Organisation entsprechen.
T0195	Sorgen Sie für einen gesteuerten Fluss relevanter Informationen (über webbasierte Portale oder auf andere Weise) auf der Grundlage der Missionsanforderungen.	ssm-document-not-public	Stellen Sie sicher, dass AWS Systems Manager (SSM) - Dokumente nicht öffentlich sind, da dies einen unbeabsichtigten Zugriff auf Ihre SSM-Dokumente ermöglichen kann. Ein öffentliches SSM-Dokument kann Informationen über Ihr Konto, Ihre Ressourcen und internen Prozesse preisgeben.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0195	Sorgen Sie für einen gesteuerten Fluss relevanter Informationen (über webbasierte Portale oder auf andere Weise) auf der Grundlage der Missionsanforderungen.	dms-replication-not-public	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass auf DMS-Replikationsinstanzen nicht öffentlich zugegriffen werden kann. DMS-Replikations-Instances können vertrauliche Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.
T0195	Sorgen Sie für einen gesteuerten Fluss relevanter Informationen (über webbasierte Portale oder auf andere Weise) auf der Grundlage der Missionsanforderungen.	ebs-snapshot-public-restorable-überprüfen	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass EBS-Snapshots nicht öffentlich wiederherstellbar sind. EBS-Volume-Snapshots können vertrauliche Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0195	Sorgen Sie für einen gesteuerten Fluss relevanter Informationen (über webbasierte Portale oder auf andere Weise) auf der Grundlage der Missionsanforderungen.	ec-2 instance-no-public-ip	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon Elastic Compute Cloud (Amazon EC2) - Instances nicht öffentlich zugänglich sind. EC2Amazon -Instances können vertrauliche Informationen enthalten, und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0195	Sorgen Sie für einen gesteuerten Fluss relevanter Informationen (über webbasierte Portale oder auf andere Weise) auf der Grundlage der Missionsanforderungen.	elasticsearch-in-vpc-only	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass sich Amazon OpenSearch OpenSearch Service (Service) - Domains innerhalb einer Amazon Virtual Private Cloud (Amazon VPC) befinden. Eine OpenSearch Service-Domain innerhalb einer Amazon VPC ermöglicht die sichere Kommunikation zwischen OpenSearch Service und anderen Services innerhalb der Amazon VPC, ohne dass ein Internet-Gateway, ein NAT-Gerät oder eine VPN-Verbindung erforderlich ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0195	Sorgen Sie für einen gesteuerten Fluss relevanter Informationen (über webbasierte Portale oder auf andere Weise) auf der Grundlage der Missionsanforderungen.	emr-master-no-public-ip	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon EMR-Cluster-Masterknoten nicht öffentlich zugänglich sind. Amazon-EMR-Cluster-Hauptknoten können vertrauliche Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.
T0195	Sorgen Sie für einen gesteuerten Fluss relevanter Informationen (über webbasierte Portale oder auf andere Weise) auf der Grundlage der Missionsanforderungen.	lambda-function-public-access-verboten	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass AWS Lambda-Funktionen nicht öffentlich zugänglich sind. Der öffentliche Zugriff kann möglicherweise die Verfügbarkeit von Ressourcen beeinträchtigen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0195	Sorgen Sie für einen gesteuerten Fluss relevanter Informati onen (über webbasier te Portale oder auf andere Weise) auf der Grundlage der Missionsanforderun gen.	lambda-inside-vpc	Stellen Sie AWS Lambda-Funktionen in einer Amazon Virtual Private Cloud (Amazon VPC) bereit, um eine sichere Kommunika tion zwischen einer Funktion und anderen Diensten innerhalb der Amazon VPC zu gewährleisten. Bei dieser Konfiguration sind kein Internet-Gateway, kein NAT-Gerät und keine VPN-Verbindung erforderlich. Der gesamte Datenverk ehr bleibt sicher in der Cloud. AWS Domains, die sich innerhalb einer VPC befinden, verfügen aufgrund ihrer logischen Isolierun g im Vergleich zu Domains mit öffentlic hen Endpunkten über eine zusätzliche Sicherheitsebene. Um den Zugriff ordnungsg emäß zu verwalten,

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			sollten AWS Lambda-Funktionen einer VPC zugewiesen werden.
T0195	Sorgen Sie für einen gesteuerten Fluss relevanter Informationen (über webbasierte Portale oder auf andere Weise) auf der Grundlage der Missionsanforderungen.	opensearch-in-vpc-only	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass sich die Domains von Amazon Elasticsearch Service (Amazon ES) innerhalb einer Amazon Virtual Private Cloud (Amazon VPC) befinden. Eine ES-Domain in einer Amazon VPC ermöglicht eine sichere Kommunikation zwischen Amazon ES und anderen Services innerhalb der Amazon VPC, ohne dass ein Internet-Gateway, ein NAT-Gerät oder eine VPN-Verbindung benötigt wird.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0195	Sorgen Sie für einen gesteuerten Fluss relevanter Informationen (über webbasierte Portale oder auf andere Weise) auf der Grundlage der Missionsanforderungen.	rds-instance-public-access-überprüfen	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Relational Database Service (Amazon RDS) -Instances nicht öffentlich sind. Amazon-RDS-Datenbank-Instances können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0195	Sorgen Sie für einen gesteuerten Fluss relevanter Informationen (über webbasierte Portale oder auf andere Weise) auf der Grundlage der Missionsanforderungen.	rds-snapshots-public-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Relational Database Service (Amazon RDS) -Instances nicht öffentlich sind. Amazon-RDS-Datenbank-Instances können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0195	Sorgen Sie für einen gesteuerten Fluss relevanter Informationen (über webbasierte Portale oder auf andere Weise) auf der Grundlage der Missionsanforderungen.	redshift-cluster-public-access-überprüfen	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Redshift Redshift-Cluster nicht öffentlich sind. Amazon-Redshift-Cluster können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0195	Sorgen Sie für einen gesteuerten Fluss relevanter Informationen (über webbasierte Portale oder auf andere Weise) auf der Grundlage der Missionsanforderungen.	restricted-common-ports	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass gemeinsame Ports für Amazon Elastic Compute Cloud (Amazon EC2) -Sicherheitsgruppen eingeschränkt sind. Wenn der Zugriff auf Ports nicht auf vertrauenswürdige Quellen beschränkt wird, kann dies zu Angriffen auf die Verfügbarkeit, Integrität und Vertraulichkeit von Systemen führen. Mit dieser Regel können Sie optional die Parameter blockedPort1–blockedPort5 festlegen (Standardkonfigurationen: 20, 21, 3389, 3306, 4333). Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0195	Sorgen Sie für einen gesteuerten Fluss relevanter Informationen (über webbasierte Portale oder auf andere Weise) auf der Grundlage der Missionsanforderungen.	s-3 bucket-public-read-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie nur autorisierten Benutzern, Prozessen und Geräten Zugriff auf Amazon Simple Storage Service (Amazon S3) - Buckets gewähren. Die Verwaltung des Zugriffs sollte mit der Klassifizierung der Daten übereinstimmen.
T0195	Sorgen Sie für einen gesteuerten Fluss relevanter Informationen (über webbasierte Portale oder auf andere Weise) auf der Grundlage der Missionsanforderungen.	s3- bucket-public-write-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie nur autorisierten Benutzern, Prozessen und Geräten Zugriff auf Amazon Simple Storage Service (Amazon S3) - Buckets gewähren. Die Verwaltung des Zugriffs sollte mit der Klassifizierung der Daten übereinstimmen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0195	Sorgen Sie für einen gesteuerten Fluss relevanter Informationen (über webbasierte Portale oder auf andere Weise) auf der Grundlage der Missionsanforderungen.	sagemaker-notebook-no-direct-Internetzugang	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass SageMaker Amazon-Notebooks keinen direkten Internetzugang zulassen. Indem Sie direkten Internetzugang blockieren, vermeiden Sie, dass unbefugte Benutzer auf sensible Daten zugreifen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0195	Sorgen Sie für einen gesteuerten Fluss relevanter Informationen (über webbasierte Portale oder auf andere Weise) auf der Grundlage der Missionsanforderungen.	subnet-auto-assign-public-ip-deaktiviert	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon Virtual Private Cloud (VPC) -Subnetzen nicht automatisch eine öffentliche IP-Adresse zugewiesen wird. Amazon Elastic Compute Cloud (EC2) -Instances, die in Subnetzen gestartet werden, in denen dieses Attribut aktiviert ist, haben ihrer primären Netzwerkschnittstelle eine öffentliche IP-Adresse zugewiesen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0195	Sorgen Sie für einen gesteuerten Fluss relevanter Informati onen (über webbasier te Portale oder auf andere Weise) auf der Grundlage der Missionsanforderun gen.	vpc-default-security-group-geschlossen	Sicherheitsgruppen von Amazon Elastic Compute Cloud (Amazon EC2) können bei der Verwaltung des Netzwerkzugriffs helfen, indem sie eine statusbehaftete Filterung des ein- und ausgehenden Netzwerkverkehrs zu Ressourcen bereitstellen. AWS Die Beschränk ung des gesamten Datenverkehrs auf die Standardsicherheit sgruppe hilft dabei, den Fernzugriff auf Ihre Ressourcen einzuschränken. AWS

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0195	Sorgen Sie für einen gesteuerten Fluss relevanter Informationen (über webbasierte Portale oder auf andere Weise) auf der Grundlage der Missionsanforderungen.	vpc-sg-open-only-to-authorized-ports	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass gemeinsame Ports für Amazon Elastic Compute Cloud (Amazon EC2) -Sicherheitsgruppen eingeschränkt sind. Wenn der Zugriff auf Ports nicht auf vertrauenswürdige Quellen beschränkt wird, kann dies zu Angriffen auf die Verfügbarkeit, Integrität und Vertraulichkeit von Systemen führen. Durch die Beschränkung des Zugriffs auf Ressourcen innerhalb einer Sicherheitsgruppe aus dem Internet (0.0.0.0/0) kann der Fernzugriff auf interne Systeme gesteuert werden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0215	Erkennen eines möglichen Sicherheitsverstoßes und Ergreifen geeigneter Maßnahmen zur Meldung des Vorfalls, soweit erforderlich.	guardduty-enabled-centralized	Amazon GuardDuty kann mithilfe von Threat Intelligence Feeds helfen, potenzielle Cybersicherheitsereignisse zu überwachen und zu erkennen. Dazu gehören Listen mit bösartigen IPs und maschinellen Lernmethoden zur Identifizierung unerwarteter, nicht autorisierter und bösartiger Aktivitäten in Ihrer AWS Cloud-Umgebung.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0244	Stellen Sie sicher, dass die software/network/system Sicherheitsvorkehrungen für Anwendungen wie angegeben umgesetzt werden, dokumentieren Sie Abweichungen und empfehlen Sie die erforderlichen Maßnahmen, um diese Abweichungen zu korrigieren.	cloud-trail-log-file-Validierung aktiviert	Verwenden Sie die AWS CloudTrail Protokolldateivalidierung, um die Integrität von Protokollen zu überprüfen. CloudTrail Mithilfe der Protokolldateivalidierung kann festgestellt werden, ob eine Protokolldatei geändert oder gelöscht wurde oder ob sie nach der Übermittlung CloudTrail unverändert geblieben ist. Dieses Feature wurde mit dem Branchenstandard entsprechenden Algorithmen entwickelt: SHA-256 für die Hashfunktion und SHA-256 mit RSA für digitale Signaturen. Das macht es rechnerisch unmöglich, CloudTrail Protokolldateien unbemerkt zu ändern, zu löschen oder zu fälschen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0244	Stellen Sie sicher, dass die software/network/system Sicherheitsvorkehrungen der Anwendungen wie angegeben umgesetzt werden, dokumentieren Sie Abweichungen und empfehlen Sie die erforderlichen Maßnahmen, um diese Abweichungen zu korrigieren.	ec2-manager instance-managed-by-systems	Eine Bestandsaufnahme der Softwareplattformen und Anwendungen innerhalb des Unternehmens ist möglich, indem Amazon Elastic Compute Cloud (Amazon EC2) - Instances mit AWS Systems Manager verwaltet werden. Verwenden Sie AWS Systems Manager, um detaillierte Systemkonfigurationen, Betriebssystem-Patch-Levels, Namen und Typ der Dienste, Softwareinstallationen, Anwendungsname, Herausgeber und Version sowie andere Details zu Ihrer Umgebung bereitzustellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0244	Stellen Sie sicher, dass die software/network/system Sicherheitsvorkehrungen der Anwendungen wie angegeben umgesetzt werden, dokumentieren Sie Abweichungen und empfehlen Sie die erforderlichen Maßnahmen, um diese Abweichungen zu korrigieren.	ec2- -check managedinstance-association-compliance-status	Verwenden Sie AWS Systems Manager Associations, um bei der Inventarisierung von Softwareplattformen und Anwendungen innerhalb eines Unternehmens zu helfen. AWS Systems Manager weist Ihren verwalteten Instances einen Konfigurationsstatus zu und ermöglicht es Ihnen, Basiswerte für Betriebssystem-Patch-Levels, Softwareinstallationen, Anwendungskonfigurationen und andere Details zu Ihrer Umgebung festzulegen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0258	Sorgen Sie für die rechtzeitige Erkennung und Identifizierung möglicher Angriffe/ Eingriffe, anomaler Aktivitäten und missbräuchlicher Aktivitäten und unterscheiden Sie diese Vorfälle und Ereignisse von harmlosen Aktivitäten.	guardduty-enabled-centralized	Amazon GuardDuty kann mithilfe von Threat Intellige nce Feeds helfen, potenzielle Cybersich erheitsereignisse zu überwachen und zu erkennen. Dazu gehören Listen mit bösartigen IPs und maschinel len Lernmethoden zur Identifizierung unerwarteter, nicht autorisierter und bösartiger Aktivitäten in Ihrer AWS Cloud-Umgebung.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0259	Verwenden Sie Tools zur Cyberabwehr zur kontinuierlichen Überwachung und Analyse der Systemaktivitäten, um böswillige Aktivitäten zu identifizieren.	guardduty-enabled-centralized	Amazon GuardDuty kann mithilfe von Threat Intelligence Feeds helfen, potenzielle Cybersicherheitsereignisse zu überwachen und zu erkennen. Dazu gehören Listen mit bösartigen IPs und maschinellen Lernmethoden zur Identifizierung unerwarteter, nicht autorisierter und bösartiger Aktivitäten in Ihrer AWS Cloud-Umgebung.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0262	Wenden Sie anerkannte defense-in-depth Prinzipien und Praktiken an (z. B. defense-in-multiple Orte, mehrschichtige Schutzmaßnahmen, Robustheit der Sicherheit).	alb-waf-enabled	Stellen Sie sicher, dass AWS WAF auf Elastic Load Balancers (ELB) aktiviert ist, um Webanwendungen zu schützen. Eine WAF trägt zum Schutz Ihrer Webanwendungen oder APIs vor gängigen Web-Exploits bei. Diese Web-Exploits können sich auf die Verfügbarkeit auswirken, die Sicherheit gefährden oder übermäßige Ressourcen in Ihrer Umgebung verbrauchen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0262	Wenden Sie anerkannte defense-in-depth Prinzipien und Praktiken an (z. B. defense-in-multiple Orte, mehrschichtige Schutzmaßnahmen, Robustheit der Sicherheit).	api-gw-associated-with-WAF	AWS Mit WAF können Sie eine Reihe von Regeln (als Web Access Control List (Web ACL) bezeichnet) konfigurieren, die Webanfragen auf der Grundlage von anpassbaren Websicherheitsregeln und -bedingungen, die Sie definieren, zulassen, blockieren oder zählen. Stellen Sie sicher, dass Ihre Amazon-API-Gateway-Stufe mit einer WAF-Web-ACL verknüpft ist, um sie vor böswilligen Angriffen zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0262	Wenden Sie anerkannte defense-in-depth Prinzipien und Praktiken an (z. B. defense-in-multiple Orte, mehrschichtige Schutzmaßnahmen, Robustheit der Sicherheit).	autoscaling-launch-config-public-ip-deaktiviert	Wenn Sie Ihre Netzwerkschnittstellen mit einer öffentlichen IP-Adresse konfigurieren, sind die diesen Netzwerkschnittstellen zugehörigen Ressourcen über das Internet erreichbar. EC2 Ressourcen sollten nicht öffentlich zugänglich sein, da dies einen unbeabsichtigten Zugriff auf Ihre Anwendungen oder Server ermöglichen kann.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0262	Wenden Sie anerkannte defense-in-depth Prinzipien und Verfahren an (z. B. defense-in-multiple Orte, mehrschichtige Schutzmaßnahmen, robuste Sicherheit).	ec-2 instances-in-vpc	Stellen Sie Amazon Elastic Compute Cloud (Amazon EC2) -Instances innerhalb einer Amazon Virtual Private Cloud (Amazon VPC) bereit, um eine sichere Kommunika tion zwischen einer Instance und anderen Services innerhalb der Amazon VPC zu ermöglichen, ohne dass ein Internet-Gateway, ein NAT-Gerät oder eine VPN-Verbindung erforderlich ist. Der gesamte Datenverk ehr bleibt sicher in der AWS Cloud. Domains, die sich innerhalb einer VPC befinden, verfügen aufgrund ihrer logischen Isolierun g im Vergleich zu Domains mit öffentlic hen Endpunkten über eine zusätzlic he Sicherheitsebene. Weisen Sie EC2

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			Amazon-Instances einer Amazon-VPC zu, um den Zugriff ordnungsgemäß zu verwalten.
T0262	Wenden Sie anerkannte defense-in-depth Prinzipien und Praktiken an (z. B. defense-in-multiple Orte, mehrschichtige Schutzmaßnahmen, Robustheit der Sicherheit).	no-unrestricted-route-to-igw	Stellen Sie sicher, dass EC2 Amazon-Routentabellen keine uneingeschränkten Routen zu einem Internet-Gateway enthalten. Durch das Entfernen oder Beschränken des Internetzugangs für Workloads innerhalb von Amazon VPCs können unbeabsichtigte Zugriffe in Ihrer Umgebung reduziert werden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0262	Wenden Sie anerkannte defense-in-depth Prinzipien und Verfahren an (z. B. defense-in-multiple Orte, mehrschichtige Schutzmaßnahmen, robuste Sicherheit).	redshift-enhanced-vpc-routing-aktiviert	Mit Enhanced-VPC-Routing wird erzwungen, dass der gesamte COPY- und UNLOAD-Datenverkehr zwischen Ihrem Cluster und Datenrepositorys über Ihre Amazon VPC erfolgt. Anschließend können Sie VPC-Features wie Sicherheitsgruppen und Netzwerkzugriffskontrolllisten verwenden, um den Netzwerkverkehr zu schützen. Sie können auch VPC-Flow-Logs verwenden, um den Netzwerkverkehr zu überwachen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0262	Wenden Sie anerkannte defense-in-depth Prinzipien und Verfahren an (z. B. defense-in-multiple Orte, mehrschichtige Schutzmaßnahmen, Robustheit der Sicherheit).	s3- -Block-periodisch account-level-public-access	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Simple Storage Service (Amazon S3) -Buckets nicht öffentlich zugänglich sind. Diese Regel trägt dazu bei, sensible Daten vor unbefugten Remote-Benutzern zu schützen, indem sie den öffentlichen Zugriff verhindert. Mit dieser Regel können Sie optional die Parameter ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) und restrictPublicBuckets Parameter (Config Default: True) festlegen. Die tatsächlichen Werte müssen den Richtlini

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			en Ihrer Organisation entsprechen.
T0262	Wenden Sie anerkannte defense-in-depth Prinzipien und Verfahren an (z. B. defense-in-multiple Orte, mehrschichtige Schutzmaßnahmen, Robustheit der Sicherheit).	ssm-document-not-public	Stellen Sie sicher, dass AWS Systems Manager (SSM) - Dokumente nicht öffentlich sind, da dies einen unbeabsichtigten Zugriff auf Ihre SSM-Dokumente ermöglichen kann. Ein öffentliches SSM-Dokument kann Informationen über Ihr Konto, Ihre Ressourcen und internen Prozesse preisgeben.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0262	Wenden Sie anerkannte defense-in-depth Prinzipien und Verfahren an (z. B. defense-in-multiple Orte, mehrschichtige Schutzmaßnahmen, Robustheit der Sicherheit).	dms-replication-not-public	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass auf DMS-Replikationsinstanzen nicht öffentlich zugegriffen werden kann. DMS-Replikations-Instances können vertrauliche Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.
T0262	Wenden Sie anerkannte defense-in-depth Prinzipien und Praktiken an (z. B. defense-in-multiple Orte, mehrschichtige Schutzmaßnahmen, Robustheit der Sicherheit).	ebs-snapshot-public-restorable-überprüfen	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass EBS-Snapshots nicht öffentlich wiederherstellbar sind. EBS-Volume-Snapshots können vertrauliche Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0262	Wenden Sie anerkannte defense-in-depth Prinzipien und Praktiken an (z. B. defense-in-multiple Orte, mehrschichtige Schutzmaßnahmen, Robustheit der Sicherheit).	ec-2 instance-no-public-ip	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon Elastic Compute Cloud (Amazon EC2) - Instances nicht öffentlich zugänglich sind. EC2Amazon -Instances können vertrauliche Informationen enthalten, und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0262	Wenden Sie anerkannte defense-in-depth Prinzipien und Praktiken an (z. B. defense-in-multiple Orte, mehrschichtige Schutzmaßnahmen, Robustheit der Sicherheit).	elasticsearch-in-vpc-only	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass sich Amazon OpenSearch OpenSearch Service (Service) - Domains innerhalb einer Amazon Virtual Private Cloud (Amazon VPC) befinden. Eine OpenSearch Service-Domain innerhalb einer Amazon VPC ermöglicht die sichere Kommunikation zwischen OpenSearch Service und anderen Services innerhalb der Amazon VPC, ohne dass ein Internet-Gateway, ein NAT-Gerät oder eine VPN-Verbindung erforderlich ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0262	Wenden Sie anerkannte defense-in-depth Prinzipien und Praktiken an (z. B. defense-in-multiple Orte, mehrschichtige Schutzmaßnahmen, Robustheit der Sicherheit).	emr-master-no-public-ip	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon EMR-Cluster-Masterknoten nicht öffentlich zugänglich sind. Amazon-EMR-Cluster-Hauptknoten können vertrauliche Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.
T0262	Wenden Sie anerkannte defense-in-depth Prinzipien und Praktiken an (z. B. defense-in-multiple Orte, mehrschichtige Schutzmaßnahmen, Robustheit der Sicherheit).	lambda-function-public-access-verboten	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass AWS Lambda-Funktionen nicht öffentlich zugänglich sind. Der öffentliche Zugriff kann möglicherweise die Verfügbarkeit von Ressourcen beeinträchtigen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0262	Wenden Sie anerkannte defense-in-depth Prinzipien und Praktiken an (z. B. defense-in-multiple Orte, mehrschichtige Schutzmaßnahmen, Robustheit der Sicherheit).	lambda-inside-vpc	Stellen Sie AWS Lambda-Funktionen in einer Amazon Virtual Private Cloud (Amazon VPC) bereit, um eine sichere Kommunikation zwischen einer Funktion und anderen Diensten innerhalb der Amazon VPC zu gewährleisten. Bei dieser Konfiguration sind kein Internet-Gateway, kein NAT-Gerät und keine VPN-Verbindung erforderlich. Der gesamte Datenverkehr bleibt sicher in der Cloud. AWS Domains, die sich innerhalb einer VPC befinden, verfügen aufgrund ihrer logischen Isolierung im Vergleich zu Domains mit öffentlichen Endpunkten über eine zusätzliche Sicherheitsebene. Um den Zugriff ordnungsgemäß zu verwalten,

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			sollten AWS Lambda-Funktionen einer VPC zugewiesen werden.
T0262	Wenden Sie anerkannte defense-in-depth Prinzipien und Praktiken an (z. B. defense-in-multiple Orte, mehrschichtige Schutzmaßnahmen, Robustheit der Sicherheit).	opensearch-in-vpc-only	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass sich die Domains von Amazon Elasticsearch Service (Amazon ES) innerhalb einer Amazon Virtual Private Cloud (Amazon VPC) befinden. Eine ES-Domain in einer Amazon VPC ermöglicht eine sichere Kommunikation zwischen Amazon ES und anderen Services innerhalb der Amazon VPC, ohne dass ein Internet-Gateway, ein NAT-Gerät oder eine VPN-Verbindung benötigt wird.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0262	Wenden Sie anerkannte defense-in-depth Prinzipien und Praktiken an (z. B. defense-in-multiple Orte, mehrschichtige Schutzmaßnahmen, Robustheit der Sicherheit).	rds-instance-public-access-überprüfen	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Relational Database Service (Amazon RDS) -Instances nicht öffentlich sind. Amazon-RDS-Datenbank-Instances können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0262	Wenden Sie anerkannte defense-in-depth Prinzipien und Praktiken an (z. B. defense-in-multiple Orte, mehrschichtige Schutzmaßnahmen, Robustheit der Sicherheit).	rds-snapshots-public-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Relational Database Service (Amazon RDS) -Instances nicht öffentlich sind. Amazon-RDS-Datenbank-Instances können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0262	Wenden Sie anerkannte defense-in-depth Prinzipien und Praktiken an (z. B. defense-in-multiple Orte, mehrschichtige Schutzmaßnahmen, Robustheit der Sicherheit).	redshift-cluster-public-access-überprüfen	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Redshift Redshift-Cluster nicht öffentlich sind. Amazon-Redshift-Cluster können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0262	Wenden Sie anerkannte defense-in-depth Prinzipien und Praktiken an (z. B. defense-in-multiple Orte, mehrschichtige Schutzmaßnahmen, Robustheit der Sicherheit).	restricted-common-ports	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass gemeinsame Ports für Amazon Elastic Compute Cloud (Amazon EC2) -Sicherheitsgruppen eingeschränkt sind. Wenn der Zugriff auf Ports nicht auf vertrauenswürdige Quellen beschränkt wird, kann dies zu Angriffen auf die Verfügbarkeit, Integrität und Vertraulichkeit von Systemen führen. Mit dieser Regel können Sie optional die Parameter blockedPort1–blockedPort5 festlegen (Standardkonfigurationen: 20, 21, 3389, 3306, 4333). Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0262	Wenden Sie anerkannte defense-in-depth Prinzipien und Praktiken an (z. B. defense-in-multiple Orte, mehrschichtige Schutzmaßnahmen, Robustheit der Sicherheit).	s-3 bucket-public-read-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie nur autorisierten Benutzern, Prozessen und Geräten Zugriff auf Amazon Simple Storage Service (Amazon S3) - Buckets gewähren. Die Verwaltung des Zugriffs sollte mit der Klassifizierung der Daten übereinstimmen.
T0262	Wenden Sie anerkannte defense-in-depth Prinzipien und Praktiken an (z. B. defense-in-multiple Orte, mehrschichtige Schutzmaßnahmen, Robustheit der Sicherheit).	s-3 bucket-public-write-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie nur autorisierten Benutzern, Prozessen und Geräten Zugriff auf Amazon Simple Storage Service (Amazon S3) - Buckets gewähren. Die Verwaltung des Zugriffs sollte mit der Klassifizierung der Daten übereinstimmen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0262	Wenden Sie anerkannte defense-in-depth Prinzipien und Praktiken an (z. B. defense-in-multiple Orte, mehrschichtige Schutzmaßnahmen, Robustheit der Sicherheit).	sagemaker-notebook-no-direct-Internetzugang	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass SageMaker Amazon-Notebooks keinen direkten Internetzugang zulassen. Indem Sie direkten Internetzugang blockieren, vermeiden Sie, dass unbefugte Benutzer auf sensible Daten zugreifen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0262	Wenden Sie anerkannte defense-in-depth Prinzipien und Praktiken an (z. B. defense-in-multiple Orte, mehrschichtige Schutzmaßnahmen, robuste Sicherheit).	subnet-auto-assign-public-ip-deaktiviert	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon Virtual Private Cloud (VPC) -Subnetzen nicht automatisch eine öffentliche IP-Adresse zugewiesen wird. Amazon Elastic Compute Cloud (EC2) -Instances, die in Subnetzen gestartet werden, in denen dieses Attribut aktiviert ist, haben ihrer primären Netzwerkschnittstelle eine öffentliche IP-Adresse zugewiesen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0262	Wenden Sie anerkannte defense-in-depth Prinzipien und Praktiken an (z. B. defense-in-multiple Orte, mehrschichtige Schutzmaßnahmen, Robustheit der Sicherheit).	vpc-default-security-group-geschlossen	Sicherheitsgruppen von Amazon Elastic Compute Cloud (Amazon EC2) können bei der Verwaltung des Netzwerkzugriffs helfen, indem sie eine statusbehaftete Filterung des ein- und ausgehenden Netzwerkverkehrs zu Ressourcen bereitstellen. AWS Die Beschränkung des gesamten Datenverkehrs auf die Standardsicherheitsgruppe hilft dabei, den Fernzugriff auf Ihre Ressourcen einzuschränken. AWS

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0262	Wenden Sie bewährte defense-in-depth Prinzipien und Verfahren an (z. B. defense-in-multiple Orte, mehrschichtige Schutzmaßnahmen, robuste Sicherheit).	vpc-sg-open-only-to-authorized-ports	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass gemeinsame Ports für Amazon Elastic Compute Cloud (Amazon EC2) -Sicherheitsgruppen eingeschränkt sind. Wenn der Zugriff auf Ports nicht auf vertrauenswürdige Quellen beschränkt wird, kann dies zu Angriffen auf die Verfügbarkeit, Integrität und Vertraulichkeit von Systemen führen. Durch die Beschränkung des Zugriffs auf Ressourcen innerhalb einer Sicherheitsgruppe aus dem Internet (0.0.0.0/0) kann der Fernzugriff auf interne Systeme gesteuert werden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0284	Entwerfen Entwickeln neuer Tools/ Technologien im Zusammenhang mit Cybersicherheit.	account-part-of-organizations	Durch die zentrale Verwaltung AWS-Konten innerhalb von AWS Organizations wird sichergestellt, dass die Konten den Vorschriften entsprechen. Eine fehlende zentrale Kontoverwaltung kann zu inkonsistenten Kontokonfigurationen führen, wodurch Ressourcen und sensible Daten offengelegt werden können.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0284	Entwerfen Entwickeln neuer Tools/ Technologien im Zusammenhang mit Cybersicherheit.	alb-waf-enabled	Stellen Sie sicher, dass AWS WAF auf Elastic Load Balancers (ELB) aktiviert ist, um Webanwendungen zu schützen. Eine WAF trägt zum Schutz Ihrer Webanwendungen oder APIs vor gängigen Web-Exploits bei. Diese Web-Exploits können sich auf die Verfügbarkeit auswirken, die Sicherheit gefährden oder übermäßige Ressourcen in Ihrer Umgebung verbrauchen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0284	Entwerfen Entwickeln neuer Tools/ Technologien im Zusammenhang mit Cybersicherheit.	api-gw-associated-with-WAF	AWS Mit WAF können Sie eine Reihe von Regeln (als Web Access Control List (Web ACL) bezeichnet) konfigurieren, die Webanfragen auf der Grundlage von anpassbaren Websicherheitsregeln und -bedingungen, die Sie definieren, zulassen, blockieren oder zählen. Stellen Sie sicher, dass Ihre Amazon-API-Gateway-Stufe mit einer WAF-Web-ACL verknüpft ist, um sie vor böswilligen Angriffen zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0284	Entwerfen Entwickeln neuer Tools/ Technologien im Zusammenhang mit Cybersicherheit.	autoscaling-launch-config-public-ip-deaktiviert	Wenn Sie Ihre Netzwerkschnittstellen mit einer öffentlichen IP-Adresse konfigurieren, sind die diesen Netzwerkschnittstellen zugehörigen Ressourcen über das Internet erreichbar. EC2 Ressourcen sollten nicht öffentlich zugänglich sein, da dies einen unbeabsichtigten Zugriff auf Ihre Anwendungen oder Server ermöglichen kann.
T0284	Entwerfen Entwickeln neuer Tools/ Technologien im Zusammenhang mit Cybersicherheit.	ec2- instance-profile-attached	EC2 Instanzprofile übergeben eine IAM-Rolle an eine Instanz EC2 . Das Anhängen eines Instance-Profils an Ihre Instances kann bei der Implementierung von geringsten Berechtigungen und der Berechtigungsverwaltung helfen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0284	Entwerfen Entwickeln neuer Tools/ Technologien im Zusammenhang mit Cybersicherheit.	ecs-task-definition-user-for-host-mode-check	Wenn für eine Aufgabendefinition erhöhte Berechtigungen gelten, liegt das daran, dass der Kunde diesen Konfigurationen ausdrücklich zugestimmt hat. Diese Kontrolle prüft, ob eine unerwartete Berechtigungseskalation vorliegt, wenn für eine Aufgabendefinition das Host-Netzwerk aktiviert ist, die Kunden aber keine erhöhten Berechtigungen aktiviert haben.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0284	Entwerfen Entwickeln neuer Tools/ Technologien im Zusammenhang mit Cybersicherheit.	iam-no-inline-policy-überprüfen	Stellen Sie sicher, dass ein Benutzer, eine IAM-Rolle oder eine IAM-Gruppe (AWS Identity and Access Management) nicht über eine Inline-Richtlinie zur Zugriffskontrolle auf Systeme und Ressourcen verfügt. AWS empfiehlt, verwaltete Richtlinien anstelle von Inline-Richtlinien zu verwenden. Verwaltete Richtlinien ermöglichen Wiederverwendbarkeit, Versionsverwaltung, Rollback und Delegierung der Berechtigungsverwaltung.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0284	Entwerfen Entwickeln neuer Tools/ Technologien im Zusammenhang mit Cybersicherheit.	iam-policy-no-statements-with-full-access	Stellen Sie sicher, dass IAM-Aktionen nur auf die benötigten Aktionen beschränkt sind. Wenn Benutzern mehr Rechte eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Rechte und der Aufgabentrennung verstoßen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0284	Entwerfen Entwickeln neuer Tools/ Technologien im Zusammenhang mit Cybersicherheit.	ec-2 instances-in-vpc	Stellen Sie Amazon Elastic Compute Cloud (Amazon EC2) -Instances innerhalb einer Amazon Virtual Private Cloud (Amazon VPC) bereit, um eine sichere Kommunikation zwischen einer Instance und anderen Services innerhalb der Amazon VPC zu ermöglichen, ohne dass ein Internet-Gateway, ein NAT-Gerät oder eine VPN-Verbindung erforderlich ist. Der gesamte Datenverkehr bleibt sicher in der AWS Cloud. Domains, die sich innerhalb einer VPC befinden, verfügen aufgrund ihrer logischen Isolierung im Vergleich zu Domains mit öffentlichen Endpunkten über eine zusätzliche Sicherheitsebene. Weisen Sie EC2

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			Amazon-Instances einer Amazon-VPC zu, um den Zugriff ordnungsgemäß zu verwalten.
T0284	Entwerfen Entwickeln neuer Tools/ Technologien im Zusammenhang mit Cybersicherheit.	no-unrestricted-route-to-igw	Stellen Sie sicher, dass EC2 Amazon-Routentabellen keine uneingeschränkten Routen zu einem Internet-Gateway enthalten. Durch das Entfernen oder Beschränken des Internetzugangs für Workloads innerhalb von Amazon VPCs können unbeabsichtigte Zugriffe in Ihrer Umgebung reduziert werden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0284	Entwerfen Entwickeln neuer Tools/ Technologien im Zusammenhang mit Cybersicherheit.	rds-automatic-minor-version-Upgrade aktiviert	Aktivieren Sie automatische Unterversions-Upgrades auf Ihren Amazon-Relational-Database-Service (RDS)-Instances, um sicherzustellen, dass die aktuellen Updates für Unterversionen des Relational Database Management System (RDBMS) installiert sind, die Sicherheitspatches und Bugfixes enthalten können.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0284	Entwerfen Entwickeln neuer Tools/ Technologien im Zusammenhang mit Cybersicherheit.	redshift-enhanced-vpc-routing-aktiviert	Mit Enhanced-VPC-Routing wird erzwungen, dass der gesamte COPY- und UNLOAD-Datenverkehr zwischen Ihrem Cluster und Datenrepositorys über Ihre Amazon VPC erfolgt. Anschließend können Sie VPC-Features wie Sicherheitsgruppen und Netzwerkzugriffskontrolllisten verwenden, um den Netzwerkverkehr zu schützen. Sie können auch VPC-Flow-Logs verwenden, um den Netzwerkverkehr zu überwachen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0284	Entwerfen Entwickeln neuer Tools/ Technologien im Zusammenhang mit Cybersicherheit.	s3- -Blocke-periodisch account-level-public-access	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Simple Storage Service (Amazon S3) -Buckets nicht öffentlich zugänglich sind. Diese Regel trägt dazu bei, sensible Daten vor unbefugten Remote-Benutzern zu schützen, indem sie den öffentlichen Zugriff verhindert. Mit dieser Regel können Sie optional die Parameter ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) und restrictPublicBuckets Parameter (Config Default: True) festlegen. Die tatsächlichen Werte müssen den Richtlini

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			en Ihrer Organisation entsprechen.
T0284	Entwerfen Entwickeln neuer Tools/ Technologien im Zusammenhang mit Cybersicherheit.	ssm-document-not-public	Stellen Sie sicher, dass AWS Systems Manager (SSM) - Dokumente nicht öffentlich sind, da dies einen unbeabsichtigten Zugriff auf Ihre SSM-Dokumente ermöglichen kann. Ein öffentliches SSM-Dokument kann Informationen über Ihr Konto, Ihre Ressourcen und internen Prozesse preisgeben.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0284	Entwerfen Entwickeln neuer Tools/ Technologien im Zusammenhang mit Cybersicherheit.	backup-recovery-point-manual-Löschen-deaktiviert	Stellen Sie sicher, dass Ihren AWS Backup-Wiederherstellungspunkten eine ressourcenbasierte Richtlinie zugeordnet ist, die das Löschen von Wiederherstellungspunkten verhindert. Die Verwendung einer ressourcenbasierten Richtlinie zur Verhinderung des Löschens von Wiederherstellungspunkten kann dazu beitragen, ein versehentliches oder absichtliches Löschen zu unterbinden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0284	Entwerfen Entwickeln neuer Tools/ Technologien im Zusammenhang mit Cybersicherheit.	cloud-trail-log-file-Validierung aktiviert	Verwenden Sie die AWS CloudTrail Protokolldateivalidierung, um die Integrität von Protokollen zu überprüfen. CloudTrail Mithilfe der Protokolldateivalidierung kann festgestellt werden, ob eine Protokolldatei geändert oder gelöscht wurde oder ob sie nach der Übermittlung CloudTrail unverändert geblieben ist. Dieses Feature wurde mit dem Branchenstandard entsprechenden Algorithmen entwickelt: SHA-256 für die Hashfunktion und SHA-256 mit RSA für digitale Signaturen. Das macht es rechnerisch unmöglich, CloudTrail Protokolldateien unbemerkt zu ändern, zu löschen oder zu fälschen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0284	Entwerfen Entwickeln neuer Tools/ Technologien im Zusammenhang mit Cybersicherheit.	codebuild-project-envvar-awscred-überprüfen	Stellen Sie sicher, dass die Anmeldeinformationen AWS_ACCESS_KEY_ID AWS_SECRET_ACCESS_KEY nicht in AWS Codebuild-Projektumgebungen vorhanden sind. Speichern Sie diese Variablen nicht als Klartext. Das Speichern dieser Variablen als Klartext bewirkt eine unbeabsichtigte Offenlegung von Daten sowie unberechtigte Zugriffe.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0284	Entwerfen Entwickeln neuer Tools/ Technologien im Zusammenhang mit Cybersicherheit.	codebuild-project-source-repo-URL-Prüfung	Stellen Sie sicher, dass die URL des Quell-Repositorys GitHub oder des Bitbucket-Quell-Repositorys keine persönlichen Zugriffstoken oder Anmeldeinformationen in Codebuild-Projektumgebungen enthält. AWS Verwende OAuth anstelle von persönlichen Zugriffstoken oder Anmeldedaten die Autorisierung für den Zugriff auf GitHub Bitbucket-Repositorys.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0284	Entwerfen Entwickeln neuer Tools/ Technologien im Zusammenhang mit Cybersicherheit.	dms-replication-not-public	Verwalte den Zugriff auf die AWS Cloud, indem du sicherstellst, dass auf DMS-Replikationsinstanzen nicht öffentlich zugegriffen werden kann. DMS-Replikations-Instances können vertrauliche Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.
T0284	Entwerfen Entwickeln neuer Tools/ Technologien im Zusammenhang mit Cybersicherheit.	ebs-snapshot-public-restorable-überprüfen	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass EBS-Snapshots nicht öffentlich wiederherstellbar sind. EBS-Volume-Snapshots können vertrauliche Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0284	Entwerfen Entwickeln neuer Tools/ Technologien im Zusammenhang mit Cybersicherheit.	ec-2 instance-no-public-ip	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon Elastic Compute Cloud (Amazon EC2) - Instances nicht öffentlich zugänglich sind. EC2Amazon -Instances können vertrauliche Informationen enthalten, und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0284	Entwerfen Entwickeln neuer Tools/ Technologien im Zusammenhang mit Cybersicherheit.	elasticsearch-in-vpc-only	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass sich Amazon OpenSearch OpenSearch Service (Service) - Domains innerhalb einer Amazon Virtual Private Cloud (Amazon VPC) befinden. Eine OpenSearch Service-Domain innerhalb einer Amazon VPC ermöglicht die sichere Kommunikation zwischen OpenSearch Service und anderen Services innerhalb der Amazon VPC, ohne dass ein Internet-Gateway, ein NAT-Gerät oder eine VPN-Verbindung erforderlich ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0284	Entwerfen Entwickeln neuer Tools/ Technologien im Zusammenhang mit Cybersicherheit.	emr-kerberos-enabled	Die Zugriffsberechtigungen und -autorisierungen können verwaltet und nach den Prinzipien der geringsten Berechtigung und Aufgabentrennung integriert werden, indem Kerberos für Amazon-EMR-Cluster aktiviert wird. In Kerberos werden Services und Benutzer, die sich authentifizieren müssen, als Prinzipale bezeichnet. Prinzipale befinden sich in einem Kerberos-Bereich. Innerhalb dieses Bereichs wird ein Kerberos-Server als Key Distribution Center (KDC) bezeichnet. Über diesen Server können sich Prinzipale authentifizieren. Die Authentifizierung im KDC erfolgt durch die Ausstellung von Authentif

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			izierungstickets. Das KDC unterhält eine Datenbank der Prinzipale in seinem Bereich mit ihren Passwörtern und anderen administrativen Informationen zu jedem Prinzipal.
T0284	Entwerfen Entwickeln neuer Tools/ Technologien im Zusammenhang mit Cybersicherheit.	emr-master-no-public-ip	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon EMR-Cluster-Masterknoten nicht öffentlich zugänglich sind. Amazon-EMR-Cluster-Hauptknoten können vertrauliche Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0284	Entwerfen Entwickeln neuer Tools/ Technologien im Zusammenhang mit Cybersicherheit.	iam-customer-policy-blocked-kms-Aktionen	AWS Identity and Access Management (IAM) kann Ihnen helfen, die Prinzipien der geringsten Rechte und der Aufgabentrennung in Zugriffsberechtigungen und Autorisierungen zu integrieren und so zu verhindern, dass Richtlinien blockierte Aktionen für alle AWS Schlüssel des Key Management Service enthalten. Wenn Benutzer mehr Rechte haben, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und Aufgabentrennung verstoßen. Mit dieser Regel können Sie den Parameter festlegen. blockedActionsPatterns (Wert „AWS Bewährte grundlegende Sicherheitsmethoden“: kms:

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			Decrypt, kms:ReEncryptFrom). Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.
T0284	Entwerfen Entwickeln neuer Tools/ Technologien im Zusammenhang mit Cybersicherheit.	iam-group-has-users-überprüfen	AWS Identity and Access Management (IAM) kann Ihnen helfen, die Prinzipien der geringsten Rechte und der Aufgabentrennung mit Zugriffsberechtigungen und Autorisierungen zu integrieren, indem sichergestellt wird, dass IAM-Gruppen mindestens einen Benutzer haben. Die Einteilung von Benutzern in Gruppen auf der Grundlage der ihnen zugewiesenen Berechtigungen oder ihrer Funktion ist eine Möglichkeit, das Prinzip der geringsten Berechtigung zu implementieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0284	Entwerfen Entwickeln neuer Tools/ Technologien im Zusammenhang mit Cybersicherheit.	iam-inline-policy-blocked-kms-Aktionen	Stellen Sie sicher, dass ein Benutzer, eine IAM-Rolle oder eine IAM-Gruppe (AWS Identity and Access Management) nicht über eine Inline-Richtlinie verfügt, die blockierte Aktionen für alle AWS Schlüssel des Key Management Service zulässt. AWS empfiehlt, verwaltete Richtlinien anstelle von Inline-Richtlinien zu verwenden. Verwaltete Richtlinien ermöglichen Wiederverwendbarkeit, Versionsverwaltung, Rollback und Delegierung der Berechtigungsverwaltung. Mit dieser Regel können Sie den blockedActionsPatterns Parameter festlegen. (Wert „AWS Bewährte grundlegende Sicherheitsmethoden“: kms:Decrypt, kms:ReEncryptFrom). Die

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0284	Entwerfen Entwickeln neuer Tools/ Technologien im Zusammenhang mit Cybersicherheit.	iam-password-policy	Die Identitäten und Anmeldeinformationen werden auf der Grundlage einer organisatorischen IAM-Passwortrichtlinie ausgestellt, verwaltet und verifiziert. Sie erfüllen oder übertreffen die Anforderungen des NIST SP 800-63 und des AWS Foundational Security Best Practices-Standards für Passwortstärke. Mit dieser Regel können Sie optional RequireUppercaseCharacters (Wert für AWS grundlegende Sicherheitsbewährte Methoden: wahr), RequireLowercaseCharacters (Wert für bewährte Methoden für AWS grundlegende Sicherheit: wahr), RequireSymbols (Wert für bewährte Methoden für AWS grundlegende Sicherheit:

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			wahr), RequireNumbers (Wert für bewährte Methoden für AWS grundlegende Sicherheit: wahr), MinimumPasswordLength (Wert für bewährte Methoden für AWS grundlegende Sicherheit: 14), PasswordReusePrevention (Wert für bewährte Methoden für AWS grundlegende Sicherheit: 24) und MaxPasswordAge (Wert für bewährte Methoden für AWS grundlegende Sicherheit: 90) für Ihr IAM festlegen Kennwortrichtlinie. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0284	Entwerfen Entwickeln neuer Tools/ Technologien im Zusammenhang mit Cybersicherheit.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) kann Ihnen dabei helfen, die Prinzipien der geringsten Rechte und der Aufgabentrennung in Zugriffsberechtigungen und Autorisierungen zu integrieren und so zu verhindern, dass Richtlinien „Effect“: „Allow“ mit „Action“: „*“ anstelle von „Resource“: „*“ enthalten. Wenn Benutzern mehr Rechte eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und der Aufgabentrennung verstoßen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0284	Entwerfen Entwickeln neuer Tools/ Technologien im Zusammenhang mit Cybersicherheit.	iam-root-access-key-überprüfen	Der Zugriff auf Systeme und Ressourcen kann gesteuert werden, indem überprüft wird, ob der Root-Benutzer keine Zugriffsschlüssel mit seiner AWS Identity and Access Management (IAM) -Rolle verknüpft hat. Stellen Sie sicher, dass die Root-Zugriffsschlüssel gelöscht werden. Erstellen und verwenden Sie stattdessen rollenbasierte Funktionen, AWS-Konten um das Prinzip der geringsten Funktionalität zu berücksichtigen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0284	Entwerfen Entwickeln neuer Tools/ Technologien im Zusammenhang mit Cybersicherheit.	iam-user-group-membership-überprüfen	AWS Identity and Access Management (IAM) kann Ihnen helfen, Zugriffsberechtigungen und Autorisierungen einzuschränken, indem sichergestellt wird, dass Benutzer Mitglieder mindestens einer Gruppe sind. Wenn Benutzern mehr Berechtigungen eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und Aufgabentrennung verstoßen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0284	Entwerfen Entwickeln neuer Tools/ Technologien im Zusammenhang mit Cybersicherheit.	iam-user-mfa-enabled	Aktivieren Sie diese Regel, um den Zugriff auf Ressourcen in der AWS -Cloud einzuschränken. Diese Regel stellt sicher, dass die Multi-Faktor-Authentifizierung (MFA) für alle Benutzer aktiviert ist. MFA bietet eine weitere Schutzebene zusätzlich zum Benutzernamen und Passwort. Reduzieren Sie Fälle von kompromittierten Konten, indem Sie MFA für Benutzer vorschreiben.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0284	Entwerfen Entwickeln neuer Tools/ Technologien im Zusammenhang mit Cybersicherheit.	iam-user-no-policies-überprüfen	Diese Regel stellt sicher, dass AWS Identity and Access Management (IAM) -Richtlinien nur Gruppen oder Rollen zugewiesen werden, um den Zugriff auf Systeme und Ressourcen zu kontrollieren. Die Zuweisung von Berechtigungen auf Gruppen- oder Rollenebene trägt dazu bei, die Wahrscheinlichkeit zu verringern, dass eine Identität übermäßige Berechtigungen erhält oder beibehält.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0284	Entwerfen Entwickeln neuer Tools/ Technologien im Zusammenhang mit Cybersicherheit.	iam-user-unused-credentials-überprüfen	AWS Identity and Access Management (IAM) kann Ihnen bei Zugriffsberechtigungen und Autorisierungen helfen, indem es nach IAM-Passwörtern und Zugriffsschlüsseln sucht, die für einen bestimmten Zeitraum nicht verwendet wurden. Wenn ungenutzte Anmeldeinformationen identifiziert werden, müssen Sie sie deaktivieren und/oder entfernen, da dies gegen das Prinzip der geringsten Berechtigung verstoßen könnte. Für diese Regel müssen Sie einen Wert für das maxCredentialUsage Alter festlegen (Standardkonfiguration: 90). Der tatsächliche Wert muss den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0284	Entwerfen Entwickeln neuer Tools/ Technologien im Zusammenhang mit Cybersicherheit.	lambda-function-public-access-verboten	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass AWS Lambda-Funktionen nicht öffentlich zugänglich sind. Der öffentliche Zugriff kann möglicherweise die Verfügbarkeit von Ressourcen beeinträchtigen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0284	Entwerfen Entwickeln neuer Tools/ Technologien im Zusammenhang mit Cybersicherheit.	lambda-inside-vpc	Stellen Sie AWS Lambda-Funktionen in einer Amazon Virtual Private Cloud (Amazon VPC) bereit, um eine sichere Kommunikation zwischen einer Funktion und anderen Diensten innerhalb der Amazon VPC zu gewährleisten. Bei dieser Konfiguration sind kein Internet-Gateway, kein NAT-Gerät und keine VPN-Verbindung erforderlich. Der gesamte Datenverkehr bleibt sicher in der Cloud. AWS Domains, die sich innerhalb einer VPC befinden, verfügen aufgrund ihrer logischen Isolierung im Vergleich zu Domains mit öffentlichen Endpunkten über eine zusätzliche Sicherheitsebene. Um den Zugriff ordnungsgemäß zu verwalten,

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			sollten AWS Lambda-Funktionen einer VPC zugewiesen werden.
T0284	Entwerfen Entwickeln neuer Tools/ Technologien im Zusammenhang mit Cybersicherheit.	mfa-enabled-for-iam-Konsolenzugriff	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass MFA für alle AWS Identity and Access Management (IAM) -Benutzer aktiviert ist, die über ein Konsolenkennwort verfügen. MFA sorgt für eine weitere Schutzebene zusätzlich zu den Anmeldeinformationen. Indem Sie MFA für Benutzer vorschreiben, können Sie Fälle kompromittierter Konten reduzieren und verhindern, dass unbefugte Benutzer auf vertrauliche Daten zugreifen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0284	Entwerfen Entwickeln neuer Tools/ Technologien im Zusammenhang mit Cybersicherheit.	opensearch-in-vpc-only	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass sich die Domains von Amazon Elasticsearch Service (Amazon ES) innerhalb einer Amazon Virtual Private Cloud (Amazon VPC) befinden. Eine ES-Domain in einer Amazon VPC ermöglicht eine sichere Kommunikation zwischen Amazon ES und anderen Services innerhalb der Amazon VPC, ohne dass ein Internet-Gateway, ein NAT-Gerät oder eine VPN-Verbindung benötigt wird.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0284	Entwerfen Entwickeln neuer Tools/ Technologien im Zusammenhang mit Cybersicherheit.	rds-instance-public-access-überprüfen	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Relational Database Service (Amazon RDS) -Instances nicht öffentlich sind. Amazon-RDS-Datenbank-Instances können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0284	Entwerfen Entwickeln neuer Tools/ Technologien im Zusammenhang mit Cybersicherheit.	rds-snapshots-public-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Relational Database Service (Amazon RDS) -Instances nicht öffentlich sind. Amazon-RDS-Datenbank-Instances können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0284	Entwerfen Entwickeln neuer Tools/ Technologien im Zusammenhang mit Cybersicherheit.	redshift-cluster-maintenancesettings-check	Diese Regel stellt sicher, dass Amazon-Redshift-Cluster die bevorzugten Einstellungen für Ihre Organisation haben. Insbesondere sorgt sie dafür, dass Cluster bevorzugte Wartungsfenster und automatisierte Aufbewahrungsfristen für Snapshots für die Datenbank haben. Für diese Regel müssen Sie die allowVersionUpgrade festlegen. Der Standardwert ist „true“. Außerdem können Sie optional den Zeitraum preferredMaintenanceWindow (der Standardwert ist sa: 16:00 -sa: 16:30) und den automated SnapshotRetention Zeitraum (der Standardwert ist 1) festlegen. Die tatsächlichen Werte müssen den Richtlini

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			en Ihrer Organisation entsprechen.
T0284	Entwerfen Entwickeln neuer Tools/ Technologien im Zusammenhang mit Cybersicherheit.	redshift-cluster-public-access-überprüfen	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Redshift Redshift-Cluster nicht öffentlich sind. Amazon-Redshift-Cluster können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0284	Entwerfen Entwickeln neuer Tools/ Technologien im Zusammenhang mit Cybersicherheit.	restricted-common-ports	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass gemeinsame Ports für Amazon Elastic Compute Cloud (Amazon EC2) -Sicherheitsgruppen eingeschränkt sind. Wenn der Zugriff auf Ports nicht auf vertrauenswürdige Quellen beschränkt wird, kann dies zu Angriffen auf die Verfügbarkeit, Integrität und Vertraulichkeit von Systemen führen. Mit dieser Regel können Sie optional die Parameter blockedPort1–blockedPort5 festlegen (Standardkonfigurationen: 20, 21, 3389, 3306, 4333). Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0284	Entwerfen Entwickeln neuer Tools/ Technologien im Zusammenhang mit Cybersicherheit.	root-account-hardware-mfa-aktiviert	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Hardware-MFA für den Root-Benutzer aktiviert ist. Der Stammbenutzer ist der AWS-Konto-Benutzer mit den meisten Berechtigungen. MFA sorgt für eine weitere Schutzebene zusätzlich zu den Anmeldeinformationen. Indem Sie MFA für den Root-Benutzer vorschreiben, können Sie die Anzahl AWS-Konten kompromittierter Benutzer reduzieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0284	Entwerfen Entwickeln neuer Tools/ Technologien im Zusammenhang mit Cybersicherheit.	root-account-mfa-enabled	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass MFA für den Root-Benutzer aktiviert ist. Der Stammbenutzer ist der AWS-Konto-Benutzer mit den meisten Berechtigungen. MFA bietet eine weitere Schutzebene zusätzlich zum Benutzernamen und Passwort. Indem Sie MFA für den Root-Benutzer vorschreiben, können Sie die Anzahl AWS-Konten kompromittierter Benutzer reduzieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0284	Entwerfen Entwickeln neuer Tools/ Technologien im Zusammenhang mit Cybersicherheit.	s-3 bucket-public-read-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie nur autorisierten Benutzern, Prozessen und Geräten Zugriff auf Amazon Simple Storage Service (Amazon S3) - Buckets gewähren. Die Verwaltung des Zugriffs sollte mit der Klassifizierung der Daten übereinstimmen.
T0284	Entwerfen Entwickeln neuer Tools/ Technologien im Zusammenhang mit Cybersicherheit.	s3- bucket-public-write-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie nur autorisierten Benutzern, Prozessen und Geräten Zugriff auf Amazon Simple Storage Service (Amazon S3) - Buckets gewähren. Die Verwaltung des Zugriffs sollte mit der Klassifizierung der Daten übereinstimmen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0284	Entwerfen Entwickeln neuer Tools/ Technologien im Zusammenhang mit Cybersicherheit.	sagemaker-notebook-no-direct-Internetzugang	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass SageMaker Amazon-Notebooks keinen direkten Internetzugang zulassen. Indem Sie direkten Internetzugang blockieren, vermeiden Sie, dass unbefugte Benutzer auf sensible Daten zugreifen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0284	Entwerfen Entwickeln neuer Tools/ Technologien im Zusammenhang mit Cybersicherheit.	subnet-auto-assign-public-ip-deaktiviert	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon Virtual Private Cloud (VPC) -Subnetzen nicht automatisch eine öffentliche IP-Adresse zugewiesen wird. Amazon Elastic Compute Cloud (EC2) -Instances, die in Subnetzen gestartet werden, in denen dieses Attribut aktiviert ist, haben ihrer primären Netzwerkschnittstelle eine öffentliche IP-Adresse zugewiesen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0284	Entwerfen Entwickeln neuer Tools/ Technologien im Zusammenhang mit Cybersicherheit.	vpc-default-security-group-geschlossen	Sicherheitsgruppen von Amazon Elastic Compute Cloud (Amazon EC2) können bei der Verwaltung des Netzwerkzugriffs helfen, indem sie eine statusbehaftete Filterung des ein- und ausgehenden Netzwerkverkehrs zu Ressourcen bereitstellen. AWS Die Beschränkung des gesamten Datenverkehrs auf die Standardsicherheitsgruppe hilft dabei, den Fernzugriff auf Ihre Ressourcen einzuschränken. AWS

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0284	Entwerfen Entwickeln neuer Tools/ Technologien im Zusammenhang mit Cybersicherheit.	vpc-sg-open-only-to-authorized-ports	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass gemeinsame Ports für Amazon Elastic Compute Cloud (Amazon EC2) -Sicherheitsgruppen eingeschränkt sind. Wenn der Zugriff auf Ports nicht auf vertrauenswürdige Quellen beschränkt wird, kann dies zu Angriffen auf die Verfügbarkeit, Integrität und Vertraulichkeit von Systemen führen. Durch die Beschränkung des Zugriffs auf Ressourcen innerhalb einer Sicherheitsgruppe aus dem Internet (0.0.0.0/0) kann der Fernzugriff auf interne Systeme gesteuert werden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0306	Unterstützt Incident Management, Service Level Management, Change Management, Release Management, Continuity Management und Verfügbarkeitsmanagement für Datenbanken und Datenmanagementsysteme.	securityhub-enabled	AWS Security Hub hilft bei der Überwachung von unbefugtem Personal, Verbindungen, Geräten und Software. AWS Security Hub aggregiert, organisiert und priorisiert die Sicherheitswarnungen oder Ergebnisse mehrerer Dienste. AWS Einige dieser Dienste sind Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer und AWS Firewall Manager sowie AWS Partnerlösungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0306	Unterstützt Incident Management, Service Level Management, Change Management, Release Management, Continuity Management und Verfügbarkeitsmanagement für Datenbanken und Datenmanagementsysteme.	cloudwatch-alarm-action-check	Amazon CloudWatch alarmiert, wenn eine Metrik den Schwellenwert für eine bestimmte Anzahl von Bewertungszeiträumen überschreitet. Der Alarm führt eine oder mehrere Aktionen durch, die vom Wert der Metrik oder des Ausdrucks im Vergleich zu einem Schwellenwert in einer Reihe von Zeiträumen abhängt. Diese Regel erfordert einen Wert für alarmActionRequired (Config Default: True), insufficientDataAction Required (Config Default: True), okActionRequired (Config Default: False). Der tatsächliche Wert muss die Alarmaktionen für Ihre Umgebung widerspiegeln.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0306	Unterstützt Incident Management, Service Level Management, Change Management, Release Management, Continuity Management und Verfügbarkeitsmanagement für Datenbanken und Datenmanagementsysteme.	guardduty-enabled-centralized	Amazon GuardDuty kann mithilfe von Threat Intelligence Feeds helfen, potenzielle Cybersicherheitsereignisse zu überwachen und zu erkennen. Dazu gehören Listen mit bösartigen IPs und maschinellen Lernmethoden zur Identifizierung unerwarteter, nicht autorisierter und bösartiger Aktivitäten in Ihrer AWS Cloud-Umgebung.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0314	Entwickeln Sie einen Systemsicherheitskontext, ein vorläufiges Betriebskonzept für die Systemsicherheit (CONOPS) und definieren Sie grundlegende Anforderungen an die Systemsicherheit gemäß den geltenden Cybersicherheitsanforderungen.	ec2-manager instance-managed-by-systems	Eine Bestandsaufnahme der Softwareplattformen und Anwendungen innerhalb des Unternehmens ist möglich, indem Amazon Elastic Compute Cloud (Amazon EC2) - Instances mit AWS Systems Manager verwaltet werden. Verwenden Sie AWS Systems Manager, um detaillierte Systemkonfigurationen, Betriebssystem-Patch-Levels, Namen und Typ der Dienste, Softwareinstallationen, Anwendungsname, Herausgeber und Version sowie andere Details zu Ihrer Umgebung bereitzustellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0314	Entwickeln Sie einen Systemsicherheitskontext, ein vorläufiges Betriebskonzept für die Systemsicherheit (CONOPS) und definieren Sie grundlegende Anforderungen an die Systemsicherheit gemäß den geltenden Cybersicherheitsanforderungen.	ec2-check managedinstance-association-compliance-status	Verwenden Sie AWS Systems Manager Associations, um bei der Inventarisierung von Softwareplattformen und Anwendungen innerhalb eines Unternehmens zu helfen. AWS Systems Manager weist Ihren verwalteten Instances einen Konfigurationsstatus zu und ermöglicht es Ihnen, Basiswerte für Betriebssystem-Patch-Levels, Softwareinstallationen, Anwendungskonfigurationen und andere Details zu Ihrer Umgebung festzulegen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0314	Entwickeln Sie einen Systemsicherheitskontext, ein vorläufiges Betriebskonzept für die Systemsicherheit (CONOPS) und definieren Sie grundlegende Anforderungen an die Systemsicherheit gemäß den geltenden Cybersicherheitsanforderungen.	ec2-stopped-instance	Aktivieren Sie diese Regel, um bei der Basiskonfiguration von Amazon Elastic Compute Cloud (Amazon EC2) - Instances zu helfen, indem Sie überprüfen, ob EC2 Amazon-Instances gemäß den Standards Ihrer Organisation für mehr als die zulässige Anzahl von Tagen gestoppt wurden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0314	Entwickeln Sie einen Systemsicherheitskontext, ein vorläufiges Betriebskonzept für die Systemsicherheit (CONOPS) und definieren Sie grundlegende Anforderungen an die Systemsicherheit gemäß den geltenden Cybersicherheitsanforderungen.	ec2- volume-inuse-check	Diese Regel stellt sicher, dass Amazon Elastic Block Store-Volumes, die an Amazon Elastic Compute Cloud (Amazon EC2) - Instances angehängt sind, zum Löschen markiert werden, wenn eine Instance beendet wird. Wenn ein Amazon-EBS-Volume nicht gelöscht wird, wenn die Instance, an die es angehängt ist, beendet wird, kann dies gegen das Konzept der geringsten Funktionalität verstoßen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0314	Entwickeln Sie einen Systemsicherheitskontext, ein vorläufiges Betriebskonzept für die Systemsicherheit (CONOPS) und definieren Sie grundlegende Anforderungen an die Systemsicherheit gemäß den geltenden Cybersicherheitsanforderungen.	elb-deletion-protection-enabled	Diese Regel sorgt dafür, dass der Löschschutz für Elastic Load Balancing aktiviert ist. Verwenden Sie diese Funktion, um zu verhindern, dass Ihr Load Balancer versehentlich oder böswillig gelöscht wird, was zum Verlust der Verfügbarkeit Ihrer Anwendungen führen kann.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0314	Entwickeln Sie einen Systemsicherheitskontext, ein vorläufiges Betriebskonzept für die Systemsicherheit (CONOPS) und definieren Sie grundlegende Anforderungen an die Systemsicherheit gemäß den geltenden Cybersicherheitsanforderungen.	restricted-common-ports	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass gemeinsame Ports für Amazon Elastic Compute Cloud (Amazon EC2) -Sicherheitsgruppen eingeschränkt sind. Wenn der Zugriff auf Ports nicht auf vertrauenswürdige Quellen beschränkt wird, kann dies zu Angriffen auf die Verfügbarkeit, Integrität und Vertraulichkeit von Systemen führen. Mit dieser Regel können Sie optional die Parameter blockedPort1–blockedPort5 festlegen (Standardkonfigurationen: 20, 21, 3389, 3306, 4333). Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0333	Durchführung von Trendanalysen und -berichten zum Thema Cyberverteidigung.	securityhub-enabled	AWS Security Hub hilft bei der Überwachung von unbefugtem Personal, Verbindungen, Geräten und Software. AWS Security Hub aggregiert, organisiert und priorisiert die Sicherheitswarnungen oder Ergebnisse mehrerer Dienste. AWS Einige dieser Dienste sind Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer und AWS Firewall Manager sowie AWS Partnerlösungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0333	Durchführung von Trendanalysen und -berichten zum Thema Cyberverteidigung.	guardduty-enabled-centralized	Amazon GuardDuty kann mithilfe von Threat Intellige nce Feeds helfen, potenzielle Cybersich erheitsereignisse zu überwachen und zu erkennen. Dazu gehören Listen mit bösartigen IPs und maschinel len Lernmethoden zur Identifizierung unerwarteter, nicht autorisierter und bösartiger Aktivitäten in Ihrer AWS Cloud-Umgebung.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0347	Beurteilen Sie die Gültigkeit der Quelldaten und der nachfolgenden Ergebnisse.	guardduty-enabled-centralized	Amazon GuardDuty kann mithilfe von Threat Intellige nce Feeds helfen, potenzielle Cybersich erheitsereignisse zu überwachen und zu erkennen. Dazu gehören Listen mit bösartigen IPs und maschinel len Lernmethoden zur Identifizierung unerwarteter, nicht autorisierter und bösartiger Aktivitäten in Ihrer AWS Cloud-Umgebung.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0358	Entwerfen und entwickeln Sie Funktionen zur Systemadministration und -verwaltung für Benutzer mit privilegi ertem Zugriff.	iam-no-inline-policy-überprüfen	Stellen Sie sicher, dass ein Benutzer, eine IAM-Rolle oder eine IAM-Gruppe (AWS Identity and Access Management) nicht über eine Inline-Richtlinie zur Zugriffsk ontrolle auf Systeme und Ressource n verfügt. AWS empfiehlt, verwaltet e Richtlinien anstelle von Inline-Richtlinien zu verwenden. Verwaltete Richtlini en ermöglichen Wiederverwendbarke it, Versionsverwaltung , Rollback und Delegierung der Berechtigungsverwa ltung.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0358	Entwerfen und entwickeln Sie Funktionen zur Systemadministration und -verwaltung für Benutzer mit privilegiertem Zugriff.	iam-policy-no-statements-with-full-access	Stellen Sie sicher, dass IAM-Aktionen nur auf die benötigten Aktionen beschränkt sind. Wenn Benutzern mehr Rechte eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Rechte und der Aufgabentrennung verstoßen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0358	Entwerfen und entwickeln Sie Funktionen zur Systemadministration und -verwaltung für Benutzer mit privilegi ertem Zugriff.	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Managemen t (IAM) kann Ihnen helfen, die Prinzipien der geringsten Rechte und der Aufgabent rennung in Zugriffsb erechtigungen und Autorisierungen zu integrieren und so zu verhindern, dass Richtlinien blockiert e Aktionen für alle AWS Schlüssel des Key Management Service enthalten. Wenn Benutzer mehr Rechte haben, als für die Ausführung einer Aufgabe erforderl ich sind, kann dies gegen das Prinzip der geringsten Berechtig ung und Aufgabent rennung verstoßen . Mit dieser Regel können Sie den Parameter festlegen . blockedActionsPatt erns (Wert „AWS Bewährte grundlege nde Sicherhei tsmethoden“: kms:

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			Decrypt, kms:ReEncryptFrom). Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.
T0358	Entwerfen und entwickeln Sie Funktionen zur Systemadministration und -verwaltung für Benutzer mit privilegiertem Zugriff.	iam-group-has-users-überprüfen	AWS Identity and Access Management (IAM) kann Ihnen helfen, die Prinzipien der geringsten Rechte und der Aufgabentrennung mit Zugriffsberechtigungen und Autorisierungen zu integrieren, indem sichergestellt wird, dass IAM-Gruppen mindestens einen Benutzer haben. Die Einteilung von Benutzern in Gruppen auf der Grundlage der ihnen zugewiesenen Berechtigungen oder ihrer Funktion ist eine Möglichkeit, das Prinzip der geringsten Berechtigung zu implementieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0358	Entwerfen und entwickeln Sie Funktionen zur Systemadministration und -verwaltung für Benutzer mit privilegi ertem Zugriff.	iam-inline-policy-blocked-kms-Aktionen	Stellen Sie sicher, dass ein Benutzer, eine IAM-Rolle oder eine IAM-Gruppe (AWS Identity and Access Management) nicht über eine Inline-Richtlinie verfügt, die blockierte Aktionen für alle AWS Schlüssel des Key Management Service zulässt. AWS empfiehlt, verwaltet e Richtlinien anstelle von Inline-Richtlinien zu verwenden. Verwaltete Richtlini en ermöglichen Wiederverwendbarke it, Versionsverwaltung , Rollback und Delegierung der Berechtigungsverwa ltung. Mit dieser Regel können Sie den blockedActionsPatt erns Parameter festlegen. (Wert „AWS Bewährte grundlege nde Sicherhei tsmethoden“: kms: Decrypt, kms:ReEnc ryptFrom). Die

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.
T0358	Entwerfen und entwickeln Sie Funktionen zur Systemadministration und -verwaltung für Benutzer mit privilegiertem Zugriff.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) kann Ihnen dabei helfen, die Prinzipien der geringsten Rechte und der Aufgabentrennung in Zugriffsberechtigungen und Autorisierungen zu integrieren und so zu verhindern, dass Richtlinien „Effect“: „Allow“ mit „Action“: „*“ anstelle von „Resource“: „*“ enthalten. Wenn Benutzern mehr Rechte eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und der Aufgabentrennung verstoßen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0358	Entwerfen und entwickeln Sie Funktionen zur Systemadministration und -verwaltung für Benutzer mit privilegiertem Zugriff.	iam-user-group-membership-überprüfen	AWS Identity and Access Management (IAM) kann Ihnen helfen, Zugriffsberechtigungen und Autorisierungen einzuschränken, indem sichergestellt wird, dass Benutzer Mitglieder mindestens einer Gruppe sind. Wenn Benutzern mehr Berechtigungen eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und Aufgabentrennung verstoßen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0358	Entwerfen und entwickeln Sie Funktionen zur Systemadministration und -verwaltung für Benutzer mit privilegi ertem Zugriff.	iam-user-no-policies-überprüfen	Diese Regel stellt sicher, dass AWS Identity and Access Management (IAM) -Richtlinien nur Gruppen oder Rollen zugewiese n werden, um den Zugriff auf Systeme und Ressourcen zu kontrollieren. Die Zuweisung von Berechtig ungen auf Gruppen- oder Rollenebene trägt dazu bei, die Wahrscheinlichkeit zu verringern, dass eine Identität übermäßige Berechtigungen erhält oder beibehält.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0376	Einrichtung, Bereitstellung, Implementierung und Bewertung von Cyber-Workforce-Management-Programmen gemäß den organisatorischen Anforderungen.	ec2- instance-profile-attached	EC2 Instanzprofile übergeben eine IAM-Rolle an eine Instanz EC2 . Das Anhängen eines Instance-Profils an Ihre Instances kann bei der Implementierung von geringsten Berechtigungen und der Berechtigungsverwaltung helfen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0376	Einrichtung, Bereitstellung, Implementierung und Bewertung von Cyber-Workforce-Management-Programmen gemäß den organisatorischen Anforderungen.	ecs-task-definition-user-for-host-mode-check	Wenn für eine Aufgabendefinition erhöhte Berechtigungen gelten, liegt das daran, dass der Kunde diesen Konfigurationen ausdrücklich zugestimmt hat. Diese Kontrolle prüft, ob eine unerwartete Berechtigungseskalation vorliegt, wenn für eine Aufgabendefinition das Host-Netzwerk aktiviert ist, die Kunden aber keine erhöhten Berechtigungen aktiviert haben.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0376	Einrichtung, Bereitstellung, Implementierung und Bewertung von Cyber-Workforce-Management-Programmen gemäß den organisatorischen Anforderungen.	elasticsearch-logs-to-cloudwatch	Stellen Sie sicher, dass für Amazon OpenSearch Service-Domains Fehlerprotokolle aktiviert und zur Aufbewahrung und Beantwortung an Amazon CloudWatch Logs gestreamt werden. Domain-Fehlerprotokolle sind bei Sicherheits- und Zugriffsprüfungen sowie bei der Diagnose von Verfügbarkeitsproblemen nützlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0376	Einrichtung, Bereitstellung, Implementierung und Bewertung von Cyber-Workforce-Management-Programmen gemäß den organisatorischen Anforderungen.	iam-no-inline-policy-überprüfen	Stellen Sie sicher, dass ein Benutzer, eine IAM-Rolle oder eine IAM-Gruppe (AWS Identity and Access Management) nicht über eine Inline-Richtlinie zur Zugriffskontrolle auf Systeme und Ressourcen verfügt. AWS empfiehlt, verwaltete Richtlinien anstelle von Inline-Richtlinien zu verwenden. Verwaltete Richtlinien ermöglichen Wiederverwendbarkeit, Versionsverwaltung, Rollback und Delegierung der Berechtigungsverwaltung.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0376	Einrichtung, Bereitstellung, Implementierung und Bewertung von Cyber-Workforce-Management-Programmen gemäß den organisatorischen Anforderungen.	iam-policy-no-statements-with-full-access	Stellen Sie sicher, dass IAM-Aktionen nur auf die benötigten Aktionen beschränkt sind. Wenn Benutzern mehr Rechte eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Rechte und der Aufgabentrennung verstoßen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0376	Einrichtung, Bereitstellung, Implementierung und Bewertung von Cyber-Workforce-Management-Programmen gemäß den organisatorischen Anforderungen.	multi-region-cloudtrail-enabled	AWS CloudTrail zeichnet Aktionen und API-Aufrufe der AWS Management Console auf. Sie können feststellen, welche Benutzer und Konten angerufen wurden AWS, von welcher Quell-IP-Adresse aus die Anrufe getätigt wurden und wann die Anrufe erfolgten. CloudTrail übermittelt Protokolldateien aus allen AWS Regionen an Ihren S3-Bucket, wenn MULTI_REGION_CLOUD_TRAIL_ENABLED aktiviert ist. Außerdem wird beim AWS Start einer neuen Region derselbe Trail in der neuen Region erstellt. CloudTrail Dadurch erhalten Sie automatisch Protokolldateien mit API-Aktivitäten für die neue Region.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0376	Einrichtung, Bereitstellung, Implementierung und Bewertung von Cyber-Workforce-Management-Programmen gemäß den organisatorischen Anforderungen.	rds-logging-enabled	Um die Protokollierung und Überwachung in Ihrer Umgebung zu erleichtern, stellen Sie sicher, dass die Amazon Relational Database Service (Amazon RDS)-Protokollierung aktiviert ist. Mit der Amazon-RDS-Protokollierung können Sie Ereignisse wie Verbindungen, Verbindungsabbrüche, Abfragen oder abgefragte Tabellen erfassen.
T0376	Einrichtung, Bereitstellung, Implementierung und Bewertung von Cyber-Workforce-Management-Programmen gemäß den organisatorischen Anforderungen.	cloud-trail-cloud-watch-logs-aktiviert	Verwenden Sie Amazon CloudWatch , um Protokollereignisaktivitäten zentral zu sammeln und zu verwalten. Die Aufnahme von AWS CloudTrail Daten liefert Einzelheiten zu den API-Aufrufaktivitäten in Ihrem AWS-Konto.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0376	Einrichtung, Bereitstellung, Implementierung und Bewertung von Cyber-Workforce-Management-Programmen gemäß den organisatorischen Anforderungen.	cloudtrail-enabled	AWS CloudTrail kann bei der Nichtabstreitbarkeit helfen, indem Aktionen und API-Aufrufe der AWS Management Console aufgezeichnet werden. Sie können die Benutzer und die Benutzer AWS-Konten , die einen AWS Dienst aufgerufen haben, die Quell-IP-Adresse, über die die Aufrufe generiert wurden, und den Zeitpunkt der Anrufe identifizieren. Einzelheiten zu den erfassten Daten finden Sie unter Inhalt des AWS CloudTrail Datensatzes.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0376	Einrichtung, Bereitstellung, Implementierung und Bewertung von Cyber-Workforce-Management-Programmen gemäß den organisatorischen Anforderungen.	cloudtrail-s3-dataevents-enabled	Die Erfassung von Simple Storage Service (Amazon S3)-Datenereignissen unterstützt die Erkennung von ungewöhnlichen Aktivitäten. Zu den Details gehören Informationen zu dem AWS -Konto, das auf einen Amazon-S3-Bucket zugegriffen hat, die IP-Adresse und die Uhrzeit des Ereignisses.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0376	Einrichtung, Bereitstellung, Implementierung und Bewertung von Cyber-Workforce-Management-Programmen gemäß den organisatorischen Anforderungen.	emr-kerberos-enabled	Die Zugriffsberechtigungen und -autorisierungen können verwaltet und nach den Prinzipien der geringsten Berechtigung und Aufgabentrennung integriert werden, indem Kerberos für Amazon-EMR-Cluster aktiviert wird. In Kerberos werden Services und Benutzer, die sich authentifizieren müssen, als Prinzipale bezeichnet. Prinzipale befinden sich in einem Kerberos-Bereich. Innerhalb dieses Bereichs wird ein Kerberos-Server als Key Distribution Center (KDC) bezeichnet. Über diesen Server können sich Prinzipale authentifizieren. Die Authentifizierung im KDC erfolgt durch die Ausstellung von Authentif

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			izierungstickets. Das KDC unterhält eine Datenbank der Prinzipale in seinem Bereich mit ihren Passwörtern und anderen administr ativen Informationen zu jedem Prinzipal.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0376	Einrichtung, Bereitstellung, Implementierung und Bewertung von Cyber-Workforce-Management-Programmen gemäß den organisatorischen Anforderungen.	iam-customer-policy-blocked-kms-Aktionen	AWS Identity and Access Management (IAM) kann Ihnen helfen, die Prinzipien der geringsten Rechte und der Aufgabentrennung in Zugriffsberechtigungen und Autorisierungen zu integrieren und so zu verhindern, dass Richtlinien blockierte Aktionen für alle AWS Schlüssel des Key Management Service enthalten. Wenn Benutzer mehr Rechte haben, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und Aufgabentrennung verstoßen. Mit dieser Regel können Sie den Parameter festlegen. blockedActionsPatterns (Wert „AWS Bewährte grundlegende Sicherheitsmethoden“: kms:

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			Decrypt, kms:ReEncryptFrom). Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.
T0376	Einrichtung, Bereitstellung, Implementierung und Bewertung von Cyber-Workforce-Management-Programmen gemäß den organisatorischen Anforderungen.	iam-group-has-users-überprüfen	AWS Identity and Access Management (IAM) kann Ihnen helfen, die Prinzipien der geringsten Rechte und der Aufgabentrennung mit Zugriffsberechtigungen und Autorisierungen zu integrieren, indem sichergestellt wird, dass IAM-Gruppen mindestens einen Benutzer haben. Die Einteilung von Benutzern in Gruppen auf der Grundlage der ihnen zugewiesenen Berechtigungen oder ihrer Funktion ist eine Möglichkeit, das Prinzip der geringsten Berechtigung zu implementieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0376	Einrichtung, Bereitstellung, Implementierung und Bewertung von Cyber-Workforce-Management-Programmen gemäß den organisatorischen Anforderungen.	iam-inline-policy-blocked-kms-Aktionen	Stellen Sie sicher, dass ein Benutzer, eine IAM-Rolle oder eine IAM-Gruppe (AWS Identity and Access Management) nicht über eine Inline-Richtlinie verfügt, die blockierte Aktionen für alle AWS Schlüssel des Key Management Service zulässt. AWS empfiehlt, verwaltete Richtlinien anstelle von Inline-Richtlinien zu verwenden. Verwaltete Richtlinien ermöglichen Wiederverwendbarkeit, Versionsverwaltung, Rollback und Delegierung der Berechtigungsverwaltung. Mit dieser Regel können Sie den blockedActionsPatterns Parameter festlegen. (Wert „AWS Bewährte grundlegende Sicherheitsmethoden“: kms:Decrypt, kms:ReEncryptFrom). Die

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.
T0376	Einrichtung, Bereitstellung, Implementierung und Bewertung von Cyber-Workforce-Management-Programmen gemäß den organisatorischen Anforderungen.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) kann Ihnen dabei helfen, die Prinzipien der geringsten Rechte und der Aufgabentrennung in Zugriffsberechtigungen und Autorisierungen zu integrieren und so zu verhindern, dass Richtlinien „Effect“: „Allow“ mit „Action“: „*“ anstelle von „Resource“: „*“ enthalten. Wenn Benutzern mehr Rechte eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und der Aufgabentrennung verstoßen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0376	Einrichtung, Bereitstellung, Implementierung und Bewertung von Cyber-Workforce-Management-Programmen gemäß den organisatorischen Anforderungen.	iam-user-group-membership-überprüfen	AWS Identity and Access Management (IAM) kann Ihnen helfen, Zugriffsberechtigungen und Autorisierungen einzuschränken, indem sichergestellt wird, dass Benutzer Mitglieder mindestens einer Gruppe sind. Wenn Benutzern mehr Berechtigungen eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und Aufgabentrennung verstoßen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0376	Einrichtung, Bereitstellung, Implementierung und Bewertung von Cyber-Workforce-Management-Programmen gemäß den organisatorischen Anforderungen.	iam-user-no-policies-überprüfen	Diese Regel stellt sicher, dass AWS Identity and Access Management (IAM) -Richtlinien nur Gruppen oder Rollen zugewiesen werden, um den Zugriff auf Systeme und Ressourcen zu kontrollieren. Die Zuweisung von Berechtigungen auf Gruppen- oder Rollenebene trägt dazu bei, die Wahrscheinlichkeit zu verringern, dass eine Identität übermäßige Berechtigungen erhält oder beibehält.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0376	Einrichtung, Bereitstellung, Implementierung und Bewertung von Cyber-Workforce-Management-Programmen gemäß den organisatorischen Anforderungen.	s3- bucket-logging-enabled	Die Amazon Simple Storage Service (Amazon S3)-Serverzugriffsprotokollierung bietet eine Methode zur Überwachung des Netzwerks im Hinblick auf potenzielle Cybersicherheitsereignisse. Die Ereignisse werden überwacht, indem detaillierte Aufzeichnungen über die Anfragen erfasst werden, die an einen Amazon-S3-Bucket gestellt wurden. Jeder Zugriffsprotokolleintrag enthält Details zu einer einzelnen Zugriffsanfrage. Zu den Details gehören Anforderer, Bucket-Name, Anforderungszeit, Anforderungsaktion, Antwortstatus und Fehlercode, falls relevant.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0376	Einrichtung, Bereitstellung, Implementierung und Bewertung von Cyber-Workforce-Management-Programmen gemäß den organisatorischen Anforderungen.	vpc-flow-logs-enabled	VPC-Flow-Protokolle erfassen detaillierte Informationsdatensätze über den IP-Datenverkehr, der zu und von Netzwerkschnittstellen in Ihrer Amazon Virtual Private Cloud (Amazon VPC) fließt. Standardmäßig enthalten Flow-Protokolldatensätze Werte für die verschiedenen Komponenten des IP-Flows, einschließlich Quelle, Ziel und Protokoll.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0416	Ermöglichen Sie Anwendungen mit Public Keying, indem Sie vorhandene PKI-Bibliotheken (Public Key Infrastructure) nutzen und gegebenenfalls Zertifikatsmanagement- und Verschlüsselungsfunktionen einbinden.	acm-certificate-expiration-check	Stellen Sie sicher, dass die Netzwerkintegrität geschützt ist, indem Sie sicherstellen, dass X509-Zertifikate von AWS ACM ausgestellt werden. Diese Zertifikate müssen gültig und dürfen nicht abgelaufen sein. Für diese Regel ist ein Wert für erforderlich daysToExpiration (Wert für bewährte AWS Grundregeln für Sicherheit: 90). Der tatsächliche Wert muss den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0416	Ermöglichen Sie Anwendungen mit Public Keying, indem Sie vorhandene PKI-Bibliotheken (Public Key Infrastructure) nutzen und gegebenenfalls Zertifikatsmanagement- und Verschlüsselungsfunktionen einbinden.	alb-http-to-https-Umleitungsprüfung	Um Daten während der Übertragung zu schützen, stellen Sie sicher, dass Ihr Application Load Balancer unverschlüsselte HTTP-Anfragen automatisch an HTTPS umleitet. Da sensible Daten vorhanden sein können, sollten Sie die Verschlüsselung bei der Übertragung aktivieren, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0416	Ermöglichen Sie Anwendungen mit Public Keying, indem Sie vorhandene PKI-Bibliotheken (Public Key Infrastructure) nutzen und gegebenenfalls Zertifikatsmanagement- und Verschlüsselungsfunktionen einbinden.	elasticsearch-node-to-node-Verschlüsselungsprüfung	Stellen Sie sicher, dass die node-to-node Verschlüsselung für Amazon OpenSearch Service aktiviert ist. Node-to-nodeVerschlüsselung ermöglicht die TLS 1.2-Verschlüsselung für die gesamte Kommunikation innerhalb der Amazon Virtual Private Cloud (Amazon VPC). Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0416	Ermöglichen Sie Anwendungen mit Public Keying, indem Sie vorhandene PKI-Bibliotheken (Public Key Infrastructure) nutzen und gegebenenfalls Zertifikatsmanagement- und Verschlüsselungsfunktionen einbinden.	elbv-2 acm-certificate-required	Zum Schutz von eventuell vorhandenen sensiblen Daten sowie von Daten während der Übertragung muss die Verschlüsselung für Ihr Elastic Load Balancing aktiviert sein. Verwenden Sie AWS Certificate Manager, um öffentliche und private SSL/TLS-Zertifikate mit AWS Diensten und internen Ressourcen zu verwalten, bereitzustellen und bereitzustellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0416	Ermöglichen Sie Anwendungen mit Public Keying, indem Sie vorhandene PKI-Bibliotheken (Public Key Infrastructure) nutzen und gegebenenfalls Zertifikatsmanagement- und Verschlüsselungsfunktionen einbinden.	elb-acm-certificate-required	Zum Schutz von eventuell vorhanden en sensiblen Daten sowie von Daten während der Übertragung muss die Verschlüsselung für Ihr Elastic Load Balancing aktiviert sein. Verwenden Sie AWS Certificate Manager, um öffentliche und private SSL/TLS-Zertifikate mit AWS Diensten und internen Ressourcen zu verwalten, bereitzustellen und bereitzustellen.
T0416	Ermöglichen Sie Anwendungen mit Public Keying, indem Sie vorhandene PKI-Bibliotheken (Public Key Infrastructure) nutzen und gegebenenfalls Zertifikatsmanagement- und Verschlüsselungsfunktionen einbinden.	elb-tls-https-listeners-nur	Stellen Sie sicher, dass Ihre Elastic Load Balancer (ELBs) mit SSL- oder HTTPS-Listenern konfiguriert sind. Um eventuell vorhanden e sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0416	Ermöglichen Sie Anwendungen mit Public Keying, indem Sie vorhandene PKI-Bibliotheken (Public Key Infrastructure) nutzen und gegebenenfalls Zertifikatsmanagement- und Verschlüsselungsfunktionen einbinden.	opensearch-node-to-node-Verschlüsselungsprüfung	Stellen Sie sicher, dass die node-to-node Verschlüsselung für Amazon OpenSearch Service aktiviert ist. Node-to-nodeVerschlüsselung ermöglicht die TLS 1.2-Verschlüsselung für die gesamte Kommunikation innerhalb der Amazon Virtual Private Cloud (Amazon VPC). Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0416	Ermöglichen Sie Anwendungen mit Public Keying, indem Sie vorhandene PKI-Bibliotheken (Public Key Infrastructure) nutzen und gegebenenfalls Zertifikatsmanagement- und Verschlüsselungsfunktionen einbinden.	redshift-require-tls-ssl	Stellen Sie sicher, dass Ihre Amazon-Redshift-Cluster eine TLS/SSL-Verschlüsselung erfordern, um eine Verbindung zu SQL-Clients herzustellen. Da sensible Daten vorhanden sein können, sollten Sie die Verschlüsselung bei der Übertragung aktivieren, um diese Daten zu schützen.
T0416	Ermöglichen Sie Anwendungen mit Public Keying, indem Sie vorhandene PKI-Bibliotheken (Public Key Infrastructure) nutzen und gegebenenfalls Zertifikatsmanagement- und Verschlüsselungsfunktionen einbinden.	s-3 bucket-ssl-requests-only	Um Daten während der Übertragung zu schützen, stellen Sie sicher, dass Ihre Amazon Simple Storage Service (Amazon S3)-Buckets Anfragen zur Verwendung von Secure Socket Layer (SSL)-Buckets erfordern. Da sensible Daten vorhanden sein können, sollten Sie die Verschlüsselung bei der Übertragung aktivieren, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0416	Ermöglichen Sie Anwendungen mit Public Keying, indem Sie vorhandene PKI-Bibliotheken (Public Key Infrastructure) nutzen und gegebenenfalls Zertifikatsmanagement- und Verschlüsselungsfunktionen einbinden.	api-gw-ssl-enabled	Stellen Sie sicher, dass die REST-API-Stufen von Amazon API Gateway mit SSL-Zertifikaten konfiguriert sind, damit Backend-Systeme überprüfen können, ob Anforderungen von API Gateway stammen.
T0421	Verwalten Sie die Indexierung/Katalogisierung, Speicherung und den Zugriff auf explizites Unternehmenswissen (z. B. gedruckte Dokumente, digitale Dateien).	autoscaling-launch-config-public-ip-deaktiviert	Wenn Sie Ihre Netzwerkschnittstellen mit einer öffentlichen IP-Adresse konfigurieren, sind die diesen Netzwerkschnittstellen zugehörigen Ressourcen über das Internet erreichbar. EC2 Ressourcen sollten nicht öffentlich zugänglich sein, da dies einen unbeabsichtigten Zugriff auf Ihre Anwendungen oder Server ermöglichen kann.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0421	Verwalten Sie die Indexierung/Katalogisierung, Speicherung und den Zugriff auf explizites Unternehmenswissen (z. B. gedruckte Dokumente, digitale Dateien).	dms-replication-not-public	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass auf DMS-Replikationsinstanzen nicht öffentlich zugegriffen werden kann. DMS-Replikations-Instances können vertrauliche Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.
T0421	Verwalten Sie die Indexierung/Katalogisierung, Speicherung und den Zugriff auf explizites Unternehmenswissen (z. B. gedruckte Dokumente, digitale Dateien).	ebs-snapshot-public-restorable-überprüfen	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass EBS-Snapshots nicht öffentlich wiederherstellbar sind. EBS-Volume-Snapshots können vertrauliche Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0421	Verwalten Sie die Indexierung/Katalogisierung, Speicherung und den Zugriff auf explizites Unternehmenswissen (z. B. gedruckte Dokumente, digitale Dateien).	ec2- instance-no-public-ip	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon Elastic Compute Cloud (Amazon EC2) - Instances nicht öffentlich zugänglich sind. EC2Amazon-Instances können vertrauliche Informationen enthalten, und für solche Konten ist eine Zugriffskontrolle erforderlich.
T0421	Verwalten Sie die Indexierung/Katalogisierung, Speicherung und den Zugriff auf explizites Unternehmenswissen (z. B. gedruckte Dokumente, digitale Dateien).	emr-master-no-public-ip	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon EMR-Cluster-Masterknoten nicht öffentlich zugänglich sind. Amazon-EMR-Cluster-Hauptknoten können vertrauliche Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0421	Verwalten Sie die Indexierung/Katalogisierung, Speicherung und den Zugriff auf explizites Unternehmenswissen (z. B. gedruckte Dokumente, digitale Dateien).	lambda-function-public-access-verboten	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass AWS Lambda-Funktionen nicht öffentlich zugänglich sind. Der öffentliche Zugriff kann möglicherweise die Verfügbarkeit von Ressourcen beeinträchtigen.
T0421	Verwalten Sie die Indexierung/Katalogisierung, Speicherung und den Zugriff auf explizites Unternehmenswissen (z. B. gedruckte Dokumente, digitale Dateien).	rds-instance-public-access-überprüfen	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Relational Database Service (Amazon RDS) -Instances nicht öffentlich sind. Amazon-RDS-Datenbank-Instances können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0421	Verwalten Sie die Indexierung/Katalogisierung, Speicherung und den Zugriff auf explizites Unternehmenswissen (z. B. gedruckte Dokumente, digitale Dateien).	rds-snapshots-public-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Relational Database Service (Amazon RDS) -Instances nicht öffentlich sind. Amazon-RDS-Datenbank-Instances können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0421	Verwalten Sie die Indexierung/Katalogisierung, Speicherung und den Zugriff auf explizites Unternehmenswissen (z. B. gedruckte Dokumente, digitale Dateien).	redshift-cluster-public-access-überprüfen	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Redshift Redshift-Cluster nicht öffentlich sind. Amazon-Redshift-Cluster können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0421	Verwalten Sie die Indexierung/Katalogisierung, Speicherung und den Zugriff auf explizites Unternehmenswissen (z. B. gedruckte Dokumente, digitale Dateien).	account-level-public-accesss3-Blöcke-periodisch	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Simple Storage Service (Amazon S3) -Buckets nicht öffentlich zugänglich sind. Diese Regel trägt dazu bei, sensible Daten vor unbefugten Remote-Benutzern zu schützen, indem sie den öffentlichen Zugriff verhindert. Mit dieser Regel können Sie optional die Parameter ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) und restrictPublicBuckets Parameter (Config Default: True) festlegen. Die tatsächlichen Werte müssen den Richtlini

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			en Ihrer Organisation entsprechen.
T0421	Verwalten Sie die Indexierung/Katalogisierung, Speicherung und den Zugriff auf explizites Unternehmenswissen (z. B. gedruckte Dokumente, digitale Dateien).	s-3 bucket-public-read-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie nur autorisierten Benutzern, Prozessen und Geräten Zugriff auf Amazon Simple Storage Service (Amazon S3) - Buckets gewähren. Die Verwaltung des Zugriffs sollte mit der Klassifizierung der Daten übereinstimmen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0421	Verwalten Sie die Indexierung/Katalogisierung, Speicherung und den Zugriff auf explizites Unternehmenswissen (z. B. gedruckte Dokumente, digitale Dateien).	s-3 bucket-public-write-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie nur autorisierten Benutzern, Prozessen und Geräten Zugriff auf Amazon Simple Storage Service (Amazon S3) - Buckets gewähren. Die Verwaltung des Zugriffs sollte mit der Klassifizierung der Daten übereinstimmen.
T0421	Verwalten Sie die Indexierung/Katalogisierung, Speicherung und den Zugriff auf explizites Unternehmenswissen (z. B. gedruckte Dokumente, digitale Dateien).	ssm-document-not-public	Stellen Sie sicher, dass AWS Systems Manager (SSM) - Dokumente nicht öffentlich sind, da dies einen unbeabsichtigten Zugriff auf Ihre SSM-Dokumente ermöglichen kann. Ein öffentliches SSM-Dokument kann Informationen über Ihr Konto, Ihre Ressourcen und internen Prozesse preisgeben.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0421	Verwalten Sie die Indexierung/Katalogisierung, Speicherung und den Zugriff auf explizites Unternehmenswissen (z. B. gedruckte Dokumente, digitale Dateien).	emr-kerberos-enabled	Die Zugriffsberechtigungen und -autorisierungen können verwaltet und nach den Prinzipien der geringsten Berechtigung und Aufgabentrennung integriert werden, indem Kerberos für Amazon-EMR-Cluster aktiviert wird. In Kerberos werden Services und Benutzer, die sich authentifizieren müssen, als Prinzipale bezeichnet. Prinzipale befinden sich in einem Kerberos-Bereich. Innerhalb dieses Bereichs wird ein Kerberos-Server als Key Distribution Center (KDC) bezeichnet. Über diesen Server können sich Prinzipale authentifizieren. Die Authentifizierung im KDC erfolgt durch die Ausstellung von Authentif

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			izierungstickets. Das KDC unterhält eine Datenbank der Prinzipale in seinem Bereich mit ihren Passwörtern und anderen administr ativen Informationen zu jedem Prinzipal.
T0421	Verwalten Sie die Indexierung/Katalo gisierung, Speicheru ng und den Zugriff auf explizites Unternehm enswissen (z. B. gedruckte Dokumente , digitale Dateien).	subnet-auto-assign-public-ip-deaktiviert	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon Virtual Private Cloud (VPC) -Subnetzen nicht automatisch eine öffentliche IP-Adress e zugewiesen wird. Amazon Elastic Compute Cloud (EC2) -Instances, die in Subnetzen gestartet werden, in denen dieses Attribut aktiviert ist, haben ihrer primären Netzwerkschnittste lle eine öffentliche IP-Adresse zugewiesen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0475	Beurteilen Sie angemessene Zugriffskontrollen auf der Grundlage der Prinzipien der geringsten Rechte und need-to-know.	autoscaling-launch-config-public-ip-deaktiviert	Wenn Sie Ihre Netzwerkschnittstellen mit einer öffentlichen IP-Adresse konfigurieren, sind die diesen Netzwerkschnittstellen zugehörigen Ressourcen über das Internet erreichbar. EC2 Ressourcen sollten nicht öffentlich zugänglich sein, da dies einen unbeabsichtigten Zugriff auf Ihre Anwendungen oder Server ermöglichen kann.
T0475	Beurteilen Sie angemessene Zugriffskontrollen auf der Grundlage der Grundsätze der geringsten Rechte und need-to-know.	ec-2 instance-profile-attached	EC2 Instanzprofile übergeben eine IAM-Rolle an eine Instanz EC2 . Das Anhängen eines Instance-Profils an Ihre Instances kann bei der Implementierung von geringsten Berechtigungen und der Berechtigungsverwaltung helfen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0475	Beurteilen Sie angemessene Zugriffskontrollen auf der Grundlage der Prinzipien der geringsten Rechte und need-to-know.	ecs-task-definition-user-for-host-mode-check	Wenn für eine Aufgabendefinition erhöhte Berechtigungen gelten, liegt das daran, dass der Kunde diesen Konfigurationen ausdrücklich zugestimmt hat. Diese Kontrolle prüft, ob eine unerwartete Berechtigungseskalation vorliegt, wenn für eine Aufgabendefinition das Host-Netzwerk aktiviert ist, die Kunden aber keine erhöhten Berechtigungen aktiviert haben.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0475	Bewertung angemessener Zugriffskontrollen auf der Grundlage der Grundsätze der geringsten Rechte und need-to-know	iam-no-inline-policy-überprüfen	Stellen Sie sicher, dass ein Benutzer, eine IAM-Rolle oder eine IAM-Gruppe (AWS Identity and Access Management) nicht über eine Inline-Richtlinie zur Zugriffskontrolle auf Systeme und Ressourcen verfügt. AWS empfiehlt, verwaltete Richtlinien anstelle von Inline-Richtlinien zu verwenden. Verwaltete Richtlinien ermöglichen Wiederverwendbarkeit, Versionsverwaltung, Rollback und Delegierung der Berechtigungsverwaltung.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0475	Beurteilen Sie angemessene Zugriffskontrollen auf der Grundlage der Grundsätze der geringsten Rechte und need-to-know.	iam-policy-no-statements-with-full-access	Stellen Sie sicher, dass IAM-Aktionen nur auf die benötigten Aktionen beschränkt sind. Wenn Benutzern mehr Rechte eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Rechte und der Aufgabentrennung verstoßen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0475	Bewertung angemessener Zugriffskontrollen auf der Grundlage der Grundsätze der geringsten Rechte und need-to-know	ec-2 instances-in-vpc	Stellen Sie Amazon Elastic Compute Cloud (Amazon EC2) -Instances innerhalb einer Amazon Virtual Private Cloud (Amazon VPC) bereit, um eine sichere Kommunika tion zwischen einer Instance und anderen Services innerhalb der Amazon VPC zu ermöglichen, ohne dass ein Internet-Gateway, ein NAT-Gerät oder eine VPN-Verbindung erforderlich ist. Der gesamte Datenverk ehr bleibt sicher in der AWS Cloud. Domains, die sich innerhalb einer VPC befinden, verfügen aufgrund ihrer logischen Isolierun g im Vergleich zu Domains mit öffentlic hen Endpunkten über eine zusätzlic he Sicherheitsebene. Weisen Sie EC2

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			Amazon-Instances einer Amazon-VPC zu, um den Zugriff ordnungsgemäß zu verwalten.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0475	Beurteilen Sie angemessene Zugriffskontrollen auf der Grundlage der Prinzipien der geringsten Rechte und need-to-know.	s3- account-level-public-access -blöcke-periodisch	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Simple Storage Service (Amazon S3) -Buckets nicht öffentlich zugänglich sind. Diese Regel trägt dazu bei, sensible Daten vor unbefugten Remote-Benutzern zu schützen, indem sie den öffentlichen Zugriff verhindert. Mit dieser Regel können Sie optional die Parameter ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) und restrictPublicBuckets Parameter (Config Default: True) festlegen. Die tatsächlichen Werte müssen den Richtlini

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			en Ihrer Organisation entsprechen.
T0475	Beurteilen Sie angemessene Zugriffskontrollen auf der Grundlage der Prinzipien der geringsten Rechte und need-to-know.	ssm-document-not-public	Stellen Sie sicher, dass AWS Systems Manager (SSM) - Dokumente nicht öffentlich sind, da dies einen unbeabsichtigten Zugriff auf Ihre SSM-Dokumente ermöglichen kann. Ein öffentliches SSM-Dokument kann Informationen über Ihr Konto, Ihre Ressourcen und internen Prozesse preisgeben.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0475	Beurteilen Sie angemessene Zugriffskontrollen auf der Grundlage der Grundsätze der geringsten Rechte und. need-to-know	dms-replication-not-public	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass auf DMS-Replikationsin stanzen nicht öffentlic h zugegriffen werden kann. DMS-Repli kations-Instances können vertrauli che Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.
T0475	Beurteilen Sie angemessene Zugriffskontrollen auf der Grundlage der Grundsätze der geringsten Rechte und need-to-know.	ebs-snapshot-public-restorable-überprüfen	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass EBS-Snapshots nicht öffentlich wiederher stellbar sind. EBS-Volume-Snapsho ts können vertrauli che Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0475	Beurteilen Sie angemessene Zugriffskontrollen auf der Grundlage der Prinzipien der geringsten Rechte und. need-to-know	ec-2 instance-no-public-ip	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon Elastic Compute Cloud (Amazon EC2) - Instances nicht öffentlich zugänglic h sind. EC2Amazon -Instances können vertrauliche Informati onen enthalten, und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0475	Beurteilen Sie angemessene Zugriffskontrollen auf der Grundlage der Grundsätze der geringsten Rechte und need-to-know.	elasticsearch-in-vpc-only	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass sich Amazon OpenSearch OpenSearch Service (Service) - Domains innerhalb einer Amazon Virtual Private Cloud (Amazon VPC) befinden. Eine OpenSearch Service-Domain innerhalb einer Amazon VPC ermöglicht die sichere Kommunikation zwischen OpenSearch Service und anderen Services innerhalb der Amazon VPC, ohne dass ein Internet-Gateway, ein NAT-Gerät oder eine VPN-Verbindung erforderlich ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0475	Beurteilen Sie angemessene Zugriffskontrollen auf der Grundlage der Grundsätze der geringsten Rechte und. need-to-know	emr-kerberos-enabled	Die Zugriffsberechtigungen und -autorisierungen können verwaltet und nach den Prinzipien der geringsten Berechtigung und Aufgabentrennung integriert werden, indem Kerberos für Amazon-EMR-Cluster aktiviert wird. In Kerberos werden Services und Benutzer, die sich authentifizieren müssen, als Prinzipale bezeichnet. Prinzipale befinden sich in einem Kerberos-Bereich. Innerhalb dieses Bereichs wird ein Kerberos-Server als Key Distribution Center (KDC) bezeichnet. Über diesen Server können sich Prinzipale authentifizieren. Die Authentifizierung im KDC erfolgt durch die Ausstellung von Authentif

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			izierungstickets. Das KDC unterhält eine Datenbank der Prinzipale in seinem Bereich mit ihren Passwörtern und anderen administr ativen Informationen zu jedem Prinzipal.
T0475	Bewertung angemessener Zugriffskontrollen auf der Grundlage der Grundsätze der geringsten Rechte und need-to-know	emr-master-no-public-ip	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon EMR-Clust er-Masterknoten nicht öffentlich zugänglic h sind. Amazon-EM R-Cluster-Hauptkno ten können vertrauli che Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0475	Beurteilen Sie angemessene Zugriffskontrollen auf der Grundlage der Grundsätze der geringsten Rechte und need-to-know.	iam-customer-policy-blocked-KMS-Aktionen	AWS Identity and Access Management (IAM) kann Ihnen helfen, die Prinzipien der geringsten Rechte und der Aufgabentrennung in Zugriffsberechtigungen und Autorisierungen zu integrieren und so zu verhindern, dass Richtlinien blockierte Aktionen für alle AWS Schlüssel des Key Management Service enthalten. Wenn Benutzer mehr Rechte haben, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und Aufgabentrennung verstoßen. Mit dieser Regel können Sie den Parameter festlegen. blockedActionsPatterns (Wert „AWS Bewährte grundlegende Sicherheitsmethoden“: kms:

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			Decrypt, kms:ReEncryptFrom). Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.
T0475	Beurteilen Sie angemessene Zugriffskontrollen auf der Grundlage der Prinzipien der geringsten Rechte und. need-to-know	iam-group-has-users-überprüfen	AWS Identity and Access Management (IAM) kann Ihnen helfen, die Prinzipien der geringsten Rechte und der Aufgabentrennung mit Zugriffsberechtigungen und Autorisierungen zu integrieren, indem sichergestellt wird, dass IAM-Gruppen mindestens einen Benutzer haben. Die Einteilung von Benutzern in Gruppen auf der Grundlage der ihnen zugewiesenen Berechtigungen oder ihrer Funktion ist eine Möglichkeit, das Prinzip der geringsten Berechtigung zu implementieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0475	Beurteilen Sie angemessene Zugriffskontrollen auf der Grundlage der Prinzipien der geringsten Rechte und. need-to-know	iam-inline-policy-blocked-KMS-Aktionen	Stellen Sie sicher, dass ein Benutzer, eine IAM-Rolle oder eine IAM-Gruppe (AWS Identity and Access Management) nicht über eine Inline-Richtlinie verfügt, die blockierte Aktionen für alle AWS Schlüssel des Key Management Service zulässt. AWS empfiehlt, verwaltete Richtlinien anstelle von Inline-Richtlinien zu verwenden. Verwaltete Richtlinien ermöglichen Wiederverwendbarkeit, Versionsverwaltung, Rollback und Delegierung der Berechtigungsverwaltung. Mit dieser Regel können Sie den blockedActionsPatterns Parameter festlegen. (Wert „AWS Bewährte grundlegende Sicherheitsmethoden“: kms:Decrypt, kms:ReEncryptFrom). Die

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.
T0475	Beurteilen Sie angemessene Zugriffskontrollen auf der Grundlage der Prinzipien der geringsten Rechte und. need-to-know	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) kann Ihnen dabei helfen, die Prinzipien der geringsten Rechte und der Aufgabentrennung in Zugriffsberechtigungen und Autorisierungen zu integrieren und so zu verhindern, dass Richtlinien „Effect“: „Allow“ mit „Action“: „*“ anstelle von „Resource“: „*“ enthalten. Wenn Benutzern mehr Rechte eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und der Aufgabentrennung verstoßen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0475	Beurteilen Sie angemessene Zugriffskontrollen auf der Grundlage der Prinzipien der geringsten Rechte und. need-to-know	iam-root-access-key-überprüfen	Der Zugriff auf Systeme und Ressourcen kann gesteuert werden, indem überprüft wird, ob der Root-Benutzer keine Zugriffsschlüssel mit seiner AWS Identity and Access Management (IAM) -Rolle verknüpft hat. Stellen Sie sicher, dass die Root-Zugriffsschlüssel gelöscht werden. Erstellen und verwenden Sie stattdessen rollenbasierte Funktionen, AWS-Konten um das Prinzip der geringsten Funktionalität zu berücksichtigen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0475	Beurteilen Sie angemessene Zugriffskontrollen auf der Grundlage der Prinzipien der geringsten Rechte und. need-to-know	iam-user-group-membership-überprüfen	AWS Identity and Access Management (IAM) kann Ihnen helfen, Zugriffsberechtigungen und Autorisierungen einzuschränken, indem sichergestellt wird, dass Benutzer Mitglieder mindestens einer Gruppe sind. Wenn Benutzern mehr Berechtigungen eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und Aufgabentrennung verstoßen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0475	Beurteilen Sie angemessene Zugriffskontrollen auf der Grundlage der Prinzipien der geringsten Rechte und. need-to-know	iam-user-no-policies-überprüfen	Diese Regel stellt sicher, dass AWS Identity and Access Management (IAM) -Richtlinien nur Gruppen oder Rollen zugewiese n werden, um den Zugriff auf Systeme und Ressourcen zu kontrollieren. Die Zuweisung von Berechtig ungen auf Gruppen- oder Rollenebene trägt dazu bei, die Wahrscheinlichkeit zu verringern, dass eine Identität übermäßige Berechtigungen erhält oder beibehält.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0475	Beurteilen Sie angemessene Zugriffskontrollen auf der Grundlage der Grundsätze der geringsten Rechte und need-to-know.	iam-user-unused-credentials-überprüfen	AWS Identity and Access Management (IAM) kann Ihnen bei Zugriffsberechtigungen und Autorisierungen helfen, indem es nach IAM-Passwörtern und Zugriffsschlüsseln sucht, die für einen bestimmten Zeitraum nicht verwendet wurden. Wenn ungenutzte Anmeldeinformationen identifiziert werden, müssen Sie sie deaktivieren und/oder entfernen, da dies gegen das Prinzip der geringsten Berechtigung verstoßen könnte. Für diese Regel müssen Sie einen Wert für das maxCredentialUsage Alter festlegen (Standardkonfiguration: 90). Der tatsächliche Wert muss den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0475	Beurteilen Sie angemessene Zugriffskontrollen auf der Grundlage der Prinzipien der geringsten Rechte und need-to-know.	lambda-function-public-access-verboten	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass AWS Lambda-Funktionen nicht öffentlich zugänglich sind. Der öffentliche Zugriff kann möglicherweise die Verfügbarkeit von Ressourcen beeinträchtigen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0475	Beurteilen Sie angemessene Zugriffskontrollen auf der Grundlage der Grundsätze der geringsten Rechte und need-to-know.	lambda-inside-vpc	Stellen Sie AWS Lambda-Funktionen in einer Amazon Virtual Private Cloud (Amazon VPC) bereit, um eine sichere Kommunika tion zwischen einer Funktion und anderen Diensten innerhalb der Amazon VPC zu gewährleisten. Bei dieser Konfiguration sind kein Internet-Gateway, kein NAT-Gerät und keine VPN-Verbindung erforderlich. Der gesamte Datenverk ehr bleibt sicher in der Cloud. AWS Domains, die sich innerhalb einer VPC befinden, verfügen aufgrund ihrer logischen Isolierun g im Vergleich zu Domains mit öffentlic hen Endpunkten über eine zusätzliche Sicherheitsebene. Um den Zugriff ordnungsg emäß zu verwalten,

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			sollten AWS Lambda-Funktionen einer VPC zugewiesen werden.
T0475	Beurteilen Sie angemessene Zugriffskontrollen auf der Grundlage der Prinzipien der geringsten Rechte und. need-to-know	opensearch-in-vpc-only	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass sich die Domains von Amazon Elasticsearch Service (Amazon ES) innerhalb einer Amazon Virtual Private Cloud (Amazon VPC) befinden. Eine ES-Domain in einer Amazon VPC ermöglicht eine sichere Kommunikation zwischen Amazon ES und anderen Services innerhalb der Amazon VPC, ohne dass ein Internet-Gateway, ein NAT-Gerät oder eine VPN-Verbindung benötigt wird.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0475	Beurteilen Sie angemessene Zugriffskontrollen auf der Grundlage der Prinzipien der geringsten Rechte und. need-to-know	rds-instance-public-access-überprüfen	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Relational Database Service (Amazon RDS) -Instances nicht öffentlich sind. Amazon-RDS-Datenbank-Instances können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0475	Beurteilen Sie angemessene Zugriffskontrollen auf der Grundlage der Grundsätze der geringsten Rechte und need-to-know.	rds-snapshots-public-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Relational Database Service (Amazon RDS) -Instances nicht öffentlich sind. Amazon-RDS-Datenbank-Instances können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0475	Beurteilen Sie angemessene Zugriffskontrollen auf der Grundlage der Grundsätze der geringsten Rechte und need-to-know.	redshift-cluster-public-access-überprüfen	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Redshift Redshift-Cluster nicht öffentlich sind. Amazon-Redshift-Cluster können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.
T0475	Beurteilen Sie angemessene Zugriffskontrollen auf der Grundlage der Prinzipien der geringsten Rechte und need-to-know.	s-3 bucket-public-read-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie nur autorisierten Benutzern, Prozessen und Geräten Zugriff auf Amazon Simple Storage Service (Amazon S3) - Buckets gewähren. Die Verwaltung des Zugriffs sollte mit der Klassifizierung der Daten übereinstimmen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0475	Beurteilen Sie angemessene Zugriffskontrollen auf der Grundlage der Prinzipien der geringsten Rechte und need-to-know.	s-3 bucket-public-write-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie nur autorisierten Benutzern, Prozessen und Geräten Zugriff auf Amazon Simple Storage Service (Amazon S3) - Buckets gewähren. Die Verwaltung des Zugriffs sollte mit der Klassifizierung der Daten übereinstimmen.
T0475	Beurteilen Sie angemessene Zugriffskontrollen auf der Grundlage der Prinzipien der geringsten Rechte und need-to-know.	sagemaker-notebook-no-direct-Internetzugang	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass SageMaker Amazon-Notebooks keinen direkten Internetzugang zulassen. Indem Sie direkten Internetzugang blockieren, vermeiden Sie, dass unbefugte Benutzer auf sensible Daten zugreifen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0475	Beurteilen Sie angemessene Zugriffskontrollen auf der Grundlage der Grundsätze der geringsten Rechte und need-to-know.	subnet-auto-assign-public-ip-deaktiviert	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon Virtual Private Cloud (VPC) -Subnetzen nicht automatisch eine öffentliche IP-Adresse zugewiesen wird. Amazon Elastic Compute Cloud (EC2) -Instances, die in Subnetzen gestartet werden, in denen dieses Attribut aktiviert ist, haben ihrer primären Netzwerkschnittstelle eine öffentliche IP-Adresse zugewiesen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0489	Umsetzung von Systemsicherheitsmaßnahmen in Übereinstimmung mit festgelegten Verfahren zur Gewährleistung von Vertraulichkeit, Integrität, Verfügbarkeit, Authentifizierung und Nichtabstreitbarkeit.	elasticsearch-logs-to-cloudwatch	Stellen Sie sicher, dass für Amazon OpenSearch Service-Domains Fehlerprotokolle aktiviert und zur Aufbewahrung und Beantwortung an Amazon CloudWatch Logs gestreamt werden. Domain-Fehlerprotokolle sind bei Sicherheits- und Zugriffsprüfungen sowie bei der Diagnose von Verfügbarkeitsproblemen nützlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0489	Umsetzung von Systemsicherheitsmaßnahmen in Übereinstimmung mit festgelegten Verfahren zur Gewährleistung von Vertraulichkeit, Integrität, Verfügbarkeit, Authentifizierung und Nichtabstreitbarkeit.	multi-region-cloudtrail-enabled	AWS CloudTrail zeichnet Aktionen und API-Aufrufe der AWS Management Console auf. Sie können feststellen, welche Benutzer und Konten angerufen wurden AWS, von welcher Quell-IP-Adresse aus die Anrufe getätigt wurden und wann die Anrufe erfolgten. CloudTrail übermittelt Protokolldateien aus allen AWS Regionen an Ihren S3-Bucket, wenn MULTI_REGION_CLOUD_TRAIL_ENABLED aktiviert ist. Außerdem wird beim AWS Start einer neuen Region derselbe Trail in der neuen Region erstellt. CloudTrail Dadurch erhalten Sie automatisch Protokolldateien mit API-Aktivitäten für die neue Region.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0489	Umsetzung von Systemsicherheitsmaßnahmen in Übereinstimmung mit festgelegten Verfahren zur Gewährleistung von Vertraulichkeit, Integrität, Verfügbarkeit, Authentifizierung und Nichtabstreitbarkeit.	wafv2-logging-enabled	Um die Protokollierung und Überwachung in Ihrer Umgebung zu erleichtern, aktivieren Sie die AWS WAF (V2) -Protokollierung im regionalen und globalen Web ACLs. AWS Die WAF-Protokollierung bietet detaillierte Informationen über den Datenverkehr, der von Ihrer Web-ACL analysiert wird. In den Protokollen werden die Uhrzeit aufgezeichnet, zu der die AWS WAF die Anfrage von Ihrer AWS Ressource erhalten hat, Informationen über die Anfrage und eine Aktion für die Regel, der jede Anfrage entsprach.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0489	Umsetzung von Systemsicherheitsmaßnahmen in Übereinstimmung mit festgelegten Verfahren zur Gewährleistung von Vertraulichkeit, Integrität, Verfügbarkeit, Authentifizierung und Nichtabstreitbarkeit.	api-gw-execution-logging-aktiviert	Die API-Gateway-Protokollierung zeigt detaillierte Ansichten der Benutzer, die auf die API zugegriffen haben, und wie diese Benutzer auf die API zugegriffen haben. Diese Insights ermöglichen die Einsicht in Benutzeraktivitäten.
T0489	Umsetzung von Systemsicherheitsmaßnahmen in Übereinstimmung mit festgelegten Verfahren zur Gewährleistung von Vertraulichkeit, Integrität, Verfügbarkeit, Authentifizierung und Nichtabstreitbarkeit.	cloud-trail-cloud-watch-logs-aktiviert	Verwenden Sie Amazon CloudWatch , um Protokollereignisaktivitäten zentral zu sammeln und zu verwalten. Die Aufnahme von AWS CloudTrail Daten liefert Einzelheiten zu den API-Aufrufaktivitäten in Ihrem AWS-Konto.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0489	Umsetzung von Systemsicherheitsmaßnahmen in Übereinstimmung mit festgelegten Verfahren zur Gewährleistung von Vertraulichkeit, Integrität, Verfügbarkeit, Authentifizierung und Nichtabstreitbarkeit.	cloudtrail-enabled	AWS CloudTrail kann bei der Nichtabstreitbarkeit helfen, indem Aktionen und API-Aufrufe der AWS Management Console aufgezeichnet werden. Sie können die Benutzer und die Benutzer AWS-Konten , die einen AWS Dienst aufgerufen haben, die Quell-IP-Adresse, über die die Aufrufe generiert wurden, und den Zeitpunkt der Anrufe identifizieren. Einzelheiten zu den erfassten Daten finden Sie unter Inhalt des AWS CloudTrail Datensatzes.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0489	Umsetzung von Systemsicherheitsmaßnahmen in Übereinstimmung mit festgelegten Verfahren zur Gewährleistung von Vertraulichkeit, Integrität, Verfügbarkeit, Authentifizierung und Nichtabstreitbarkeit.	cloudtrail-s3-dataevents-enabled	Die Erfassung von Simple Storage Service (Amazon S3)-Datenereignissen unterstützt die Erkennung von ungewöhnlichen Aktivitäten. Zu den Details gehören Informationen zu dem AWS -Konto, das auf einen Amazon-S3-Bucket zugegriffen hat, die IP-Adresse und die Uhrzeit des Ereignisses.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0489	Umsetzung von Systemsicherheitsmaßnahmen in Übereinstimmung mit festgelegten Verfahren zur Gewährleistung von Vertraulichkeit, Integrität, Verfügbarkeit, Authentifizierung und Nichtabstreitbarkeit.	elb-logging-enabled	Die Elastic-Load-Balancing-Aktivität ist ein zentraler Kommunikationspunkt innerhalb einer Umgebung. Stellen Sie sicher, dass die ELB-Protokollierung aktiviert ist. Die gesammelten Daten enthalten detaillierte Informationen zu Anfragen, die an den ELB gesendet wurden. Jedes Protokoll enthält Informationen wie die Zeit, zu der die Anforderung einging, die Client-IP-Adresse, Latenzen, Anforderungspfade und Serverantworten.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0489	Umsetzung von Systemsicherheitsmaßnahmen in Übereinstimmung mit festgelegten Verfahren zur Gewährleistung von Vertraulichkeit, Integrität, Verfügbarkeit, Authentifizierung und Nichtabstreitbarkeit.	rds-logging-enabled	Um die Protokollierung und Überwachung in Ihrer Umgebung zu erleichtern, stellen Sie sicher, dass die Amazon Relational Database Service (Amazon RDS)-Protokollierung aktiviert ist. Mit der Amazon-RDS-Protokollierung können Sie Ereignisse wie Verbindungen, Verbindungsabbrüche, Abfragen oder abgefragte Tabellen erfassen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0489	Umsetzung von Systemsicherheitsmaßnahmen in Übereinstimmung mit festgelegten Verfahren zur Gewährleistung von Vertraulichkeit, Integrität, Verfügbarkeit, Authentifizierung und Nichtabstreitbarkeit.	redshift-cluster-configuration-check	Um Daten im Ruhezustand zu schützen, muss die Verschlüsselung für Ihre Amazon-Redshift-Cluster aktiviert sein. Sie müssen auch sicherstellen, dass die erforderlichen Konfigurationen auf Amazon-Redshift-Clustern bereitgestellt werden. Die Prüfungsprotokollierung muss aktiviert sein, um Informationen zu Verbindungen und Benutzeraktivitäten in der Datenbank bereitzustellen. Diese Regel erfordert, dass ein Wert für clusterDbEncrypted (Config Default: TRUE) und LoggingEnabled (Config Default: TRUE) gesetzt ist. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0489	Umsetzung von Systemsicherheitsmaßnahmen in Übereinstimmung mit festgelegten Verfahren zur Gewährleistung von Vertraulichkeit, Integrität, Verfügbarkeit, Authentifizierung und Nichtabstreitbarkeit.	s3- bucket-logging-enabled	Die Amazon Simple Storage Service (Amazon S3)-Serverzugriffsprotokollierung bietet eine Methode zur Überwachung des Netzwerks im Hinblick auf potenzielle Cybersicherheitsereignisse. Die Ereignisse werden überwacht, indem detaillierte Aufzeichnungen über die Anfragen erfasst werden, die an einen Amazon-S3-Bucket gestellt wurden. Jeder Zugriffsprotokolleintrag enthält Details zu einer einzelnen Zugriffsanfrage. Zu den Details gehören Anforderer, Bucket-Name, Anforderungszeit, Anforderungsaktion, Antwortstatus und Fehlercode, falls relevant.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0489	Umsetzung von Systemsicherheitsmaßnahmen in Übereinstimmung mit festgelegten Verfahren zur Gewährleistung von Vertraulichkeit, Integrität, Verfügbarkeit, Authentifizierung und Nichtabstreitbarkeit.	vpc-flow-logs-enabled	VPC-Flow-Protokolle erfassen detaillierte Informationsdatensätze über den IP-Datenverkehr, der zu und von Netzwerkschnittstellen in Ihrer Amazon Virtual Private Cloud (Amazon VPC) fließt. Standardmäßig enthalten Flow-Protokolldatensätze Werte für die verschiedenen Komponenten des IP-Flows, einschließlich Quelle, Ziel und Protokoll.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0491	Installation und Konfiguration von Hardware, Software und Peripheriegeräten für Systembenutzer in Übereinstimmung mit den Unternehm ensstandards.	ec2-manager instance-managed-by-systems	Eine Bestandsa ufnahme der Softwareplattforme n und Anwendung en innerhalb des Unternehmens ist möglich, indem Amazon Elastic Compute Cloud (Amazon EC2) - Instances mit AWS Systems Manager verwaltet werden. Verwenden Sie AWS Systems Manager, um detaillierte Systemkonfiguratio nen, Betriebssystem-Patch-Levels, Namen und Typ der Dienste, Softwareinstallati onen, Anwendung sname, Herausgeb er und Version sowie andere Details zu Ihrer Umgebung bereitzustellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0491	Installation und Konfiguration von Hardware, Software und Peripheriegeräten für Systembenutzer in Übereinstimmung mit den Unternehm ensstandards.	ec2-check managedin stance-association-compliance-status	Verwenden Sie AWS Systems Manager Associati ons, um bei der Inventarisierung von Softwareplattforme n und Anwendung en innerhalb eines Unternehmens zu helfen. AWS Syste ms Manager weist Ihren verwalteten Instances einen Konfigurationsstat us zu und ermöglich t es Ihnen, Basiswert e für Betriebss ystem-Patch-Levels , Softwareinstallati onen, Anwendung skonfigurationen und andere Details zu Ihrer Umgebung festzulegen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0491	Installation und Konfiguration von Hardware, Software und Peripheriegeräten für Systembenutzer in Übereinstimmung mit den Unternehm ensstandards.	ec2-prüfen managedinstance-patch-compliance-status	Aktivieren Sie diese Regel, um bei der Identifizierung und Dokumentation von Sicherheitslücken in Amazon Elastic Compute Cloud (Amazon EC2) zu helfen. Die Regel prüft, ob die EC2 Amazon-Instance die Patch-Konformität im AWS Systems Manager gemäß den Richtlinien und Verfahren Ihrer Organisation einhält.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0503	Überwachen Sie externe Datenquellen (z. B. Websites von Anbietern von Cyberabwehr, Computer-Notfallteams, Security Focus), um stets auf dem neuesten Stand der Cyberabwehr zu sein und festzustellen, welche Sicherheitsprobleme sich auf das Unternehmen auswirken könnten.	guardduty-enabled-centralized	Amazon GuardDuty kann mithilfe von Threat Intelligence Feeds helfen, potenzielle Cybersicherheitsereignisse zu überwachen und zu erkennen. Dazu gehören Listen mit bösartigen IPs und maschinellen Lernmethoden zur Identifizierung unerwarteter, nicht autorisierter und bösartiger Aktivitäten in Ihrer AWS Cloud-Umgebung.
T0509	Durchführung einer Risikobewertung der Informationssicherheit.	annual-risk-assessment-performed (Prozessprüfung)	Führen Sie eine jährliche Risikobewertung für Ihre Organisation durch. Risikowertungen können dabei helfen, die Wahrscheinlichkeit und Auswirkungen identifizierter Risiken und/oder Schwachstellen für eine Organisation zu ermitteln.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0553	Wenden Sie Cybersicherheitsfunktionen (z. B. Verschlüsselung, Zugriffskontrolle und Identitätsmanagement) an, um Ausnutzungsmöglichkeiten zu verringern.	ec2- ebs-encryption-by-default	Zum Schutz von Daten im Ruhezustand müssen Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon Elastic Block Store (Amazon EBS)-Volumes aktiviert ist. Da sensible Daten in diesen Volumes gespeichert werden können, sollten Sie die Verschlüsselung von Daten im Ruhezustand aktivieren, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0553	Wenden Sie Cybersicherheitsfunktionen (z. B. Verschlüsselung, Zugriffskontrolle und Identitätsmanagement) an, um Ausnutzungsmöglichkeiten zu verringern.	elasticsearch-node-to-node-Verschlüsselungsprüfung	Stellen Sie sicher, dass die node-to-node Verschlüsselung für Amazon Elasticsearch Service aktiviert ist. Node-to-nodeVerschlüsselung ermöglicht die TLS 1.2-Verschlüsselung für die gesamte Kommunikation innerhalb der Amazon Virtual Private Cloud (Amazon VPC). Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.
T0553	Wenden Sie Cybersicherheitsfunktionen (z. B. Verschlüsselung, Zugriffskontrolle und Identitätsmanagement) an, um Ausnutzungsmöglichkeiten zu reduzieren.	elb-tls-https-listeners-nur	Stellen Sie sicher, dass Ihre Elastic Load Balancer (ELBs) mit SSL- oder HTTPS-Listenern konfiguriert sind. Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0553	Wenden Sie Cybersicherheitsfunktionen (z. B. Verschlüsselung, Zugriffskontrolle und Identitätsmanagement) an, um Ausnutzungsmöglichkeiten zu reduzieren.	iam-customer-policy-blocked-kms-Aktionen	AWS Identity and Access Management (IAM) kann Ihnen helfen, die Prinzipien der geringsten Rechte und der Aufgabentrennung in Zugriffsberechtigungen und Autorisierungen zu integrieren und so zu verhindern, dass Richtlinien blockierte Aktionen für alle AWS Schlüssel des Key Management Service enthalten. Wenn Benutzer mehr Rechte haben, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und Aufgabentrennung verstoßen. Mit dieser Regel können Sie den Parameter festlegen. blockedActionsPatterns (Wert „AWS Bewährte grundlegende Sicherheitsmethoden“: kms:

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			Decrypt, kms:ReEncryptFrom). Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.
T0553	Wenden Sie Cybersicherheitsfunktionen (z. B. Verschlüsselung, Zugriffskontrolle und Identitätsmanagement) an, um Ausnutzungsmöglichkeiten zu verringern.	iam-group-has-users-überprüfen	AWS Identity and Access Management (IAM) kann Ihnen helfen, die Prinzipien der geringsten Rechte und der Aufgabentrennung mit Zugriffsberechtigungen und Autorisierungen zu integrieren, indem sichergestellt wird, dass IAM-Gruppen mindestens einen Benutzer haben. Die Einteilung von Benutzern in Gruppen auf der Grundlage der ihnen zugewiesenen Berechtigungen oder ihrer Funktion ist eine Möglichkeit, das Prinzip der geringsten Berechtigung zu implementieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0553	Wenden Sie Cybersicherheitsfunktionen (z. B. Verschlüsselung, Zugriffskontrolle und Identitätsmanagement) an, um Ausnutzungsmöglichkeiten zu reduzieren.	iam-inline-policy-blocked-kms-Aktionen	Stellen Sie sicher, dass ein Benutzer, eine IAM-Rolle oder eine IAM-Gruppe (AWS Identity and Access Management) nicht über eine Inline-Richtlinie verfügt, die blockierte Aktionen für alle AWS Schlüssel des Key Management Service zulässt. AWS empfiehlt, verwaltete Richtlinien anstelle von Inline-Richtlinien zu verwenden. Verwaltete Richtlinien ermöglichen Wiederverwendbarkeit, Versionsverwaltung, Rollback und Delegierung der Berechtigungsverwaltung. Mit dieser Regel können Sie den blockedActionsPatterns Parameter festlegen. (Wert „AWS Bewährte grundlegende Sicherheitsmethoden“: kms:Decrypt, kms:ReEncryptFrom). Die

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.
T0553	Wenden Sie Cybersicherheitsfunktionen (z. B. Verschlüsselung, Zugriffskontrolle und Identitätsmanagement) an, um Ausnutzungsmöglichkeiten zu verringern.	iam-no-inline-policy-überprüfen	Stellen Sie sicher, dass ein Benutzer, eine IAM-Rolle oder eine IAM-Gruppe (AWS Identity and Access Management) nicht über eine Inline-Richtlinie zur Zugriffskontrolle auf Systeme und Ressourcen verfügt. AWS empfiehlt, verwaltete Richtlinien anstelle von Inline-Richtlinien zu verwenden. Verwaltete Richtlinien ermöglichen Wiederverwendbarkeit, Versionsverwaltung, Rollback und Delegierung der Berechtigungsverwaltung.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0553	Wenden Sie Cybersicherheitsfunktionen an (z. B. Verschlüsselung, Zugriffskontrolle und Identitätsmanagement), um Ausnutzungsmöglichkeiten zu verringern.	iam-password-policy	Die Identitäten und Anmeldeinformationen werden auf der Grundlage einer organisatorischen IAM-Passwortrichtlinie ausgestellt, verwaltet und verifiziert. Sie erfüllen oder übertreffen die Anforderungen von NIST SP 800-63 und dem Standard „Best Practices“ von AWS Foundational Security für die Passwortstärke. Mit dieser Regel können Sie optional RequireUppercaseCharacters (Wert für AWS grundlegende Sicherheitsbewährte Methoden: wahr), RequireLowercaseCharacters (Wert für bewährte Methoden für AWS grundlegende Sicherheit: wahr), RequireSymbols (Wert für bewährte Methoden für AWS grundlegende Sicherheit:

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			wahr), RequireNumbers (Wert für bewährte Methoden für AWS grundlegende Sicherheit: wahr), MinimumPasswordLength (Wert für bewährte Methoden für AWS grundlegende Sicherheit: 14), PasswordReusePrevention (Wert für bewährte Methoden für AWS grundlegende Sicherheit: 24) und MaxPasswordAge (Wert für bewährte Methoden für AWS grundlegende Sicherheit: 90) für Ihr IAM festlegen Kennwortrichtlinie. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0553	Wenden Sie Cybersicherheitsfunktionen (z. B. Verschlüsselung, Zugriffskontrolle und Identitätsmanagement) an, um Ausnutzungsmöglichkeiten zu verringern.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) kann Ihnen dabei helfen, die Prinzipien der geringsten Rechte und der Aufgabentrennung in Zugriffsberechtigungen und Autorisierungen zu integrieren und so zu verhindern, dass Richtlinien „Effect“: „Allow“ mit „Action“: „*“ anstelle von „Resource“: „*“ enthalten. Wenn Benutzern mehr Rechte eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und der Aufgabentrennung verstoßen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0553	Wenden Sie Cybersicherheitsfunktionen (z. B. Verschlüsselung, Zugriffskontrolle und Identitätsmanagement) an, um Ausnutzungsmöglichkeiten zu reduzieren.	iam-policy-no-statements-with-full-access	Stellen Sie sicher, dass IAM-Aktionen nur auf die benötigten Aktionen beschränkt sind. Wenn Benutzern mehr Rechte eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Rechte und der Aufgabentrennung verstoßen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0553	Wenden Sie Cybersicherheitsfunktionen (z. B. Verschlüsselung, Zugriffskontrolle und Identitätsmanagement) an, um Ausnutzungsmöglichkeiten zu verringern.	iam-root-access-key-überprüfen	Der Zugriff auf Systeme und Ressourcen kann gesteuert werden, indem überprüft wird, ob der Root-Benutzer keine Zugriffsschlüssel mit seiner AWS Identity and Access Management (IAM) -Rolle verknüpft hat. Stellen Sie sicher, dass die Root-Zugriffsschlüssel gelöscht werden. Erstellen und verwenden Sie stattdessen rollenbasierte Funktionen, AWS-Konten um das Prinzip der geringsten Funktionalität zu berücksichtigen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0553	Wenden Sie Cybersicherheitsfunktionen (z. B. Verschlüsselung, Zugriffskontrolle und Identitätsmanagement) an, um Ausnutzungsmöglichkeiten zu verringern.	iam-user-group-membership-überprüfen	AWS Identity and Access Management (IAM) kann Ihnen helfen, Zugriffsberechtigungen und Autorisierungen einzuschränken, indem sichergestellt wird, dass Benutzer Mitglieder mindestens einer Gruppe sind. Wenn Benutzern mehr Berechtigungen eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und Aufgabentrennung verstoßen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0553	Wenden Sie Cybersicherheitsfunktionen (z. B. Verschlüsselung, Zugriffskontrolle und Identitätsmanagement) an, um Ausnutzungsmöglichkeiten zu reduzieren.	iam-user-mfa-enabled	Aktivieren Sie diese Regel, um den Zugriff auf Ressourcen in der AWS -Cloud einzuschränken. Diese Regel stellt sicher, dass die Multi-Faktor-Authentifizierung (MFA) für alle Benutzer aktiviert ist. MFA bietet eine weitere Schutzebene zusätzlich zum Benutzernamen und Passwort. Reduzieren Sie Fälle von kompromittierten Konten, indem Sie MFA für Benutzer vorschreiben.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0553	Wenden Sie Cybersicherheitsfunktionen (z. B. Verschlüsselung, Zugriffskontrolle und Identitätsmanagement) an, um Ausnutzungsmöglichkeiten zu verringern.	iam-user-no-policies-überprüfen	Diese Regel stellt sicher, dass AWS Identity and Access Management (IAM) -Richtlinien nur Gruppen oder Rollen zugewiesen werden, um den Zugriff auf Systeme und Ressourcen zu kontrollieren. Die Zuweisung von Berechtigungen auf Gruppen- oder Rollenebene trägt dazu bei, die Wahrscheinlichkeit zu verringern, dass eine Identität übermäßige Berechtigungen erhält oder beibehält.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0553	Wenden Sie Cybersicherheitsfunktionen (z. B. Verschlüsselung, Zugriffskontrolle und Identitätsmanagement) an, um Ausnutzungsmöglichkeiten zu verringern.	iam-user-unused-credentials-überprüfen	AWS Identity and Access Management (IAM) kann Ihnen bei Zugriffsberechtigungen und Autorisierungen helfen, indem es nach IAM-Passwörtern und Zugriffsschlüsseln sucht, die für einen bestimmten Zeitraum nicht verwendet wurden. Wenn ungenutzte Anmeldeinformationen identifiziert werden, müssen Sie sie deaktivieren und/oder entfernen, da dies gegen das Prinzip der geringsten Berechtigung verstoßen könnte. Für diese Regel müssen Sie einen Wert für das maxCredentialUsage Alter festlegen (Standardkonfiguration: 90). Der tatsächliche Wert muss den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0553	Wenden Sie Cybersicherheitsfunktionen (z. B. Verschlüsselung, Zugriffskontrolle und Identitätsmanagement) an, um Ausnutzungsmöglichkeiten zu reduzieren.	mfa-enabled-for-iam-Konsolenzugriff	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass MFA für alle AWS Identity and Access Management (IAM) -Benutzer aktiviert ist, die über ein Konsolenkennwort verfügen. MFA sorgt für eine weitere Schutzebene zusätzlich zu den Anmeldeinformationen. Indem Sie MFA für Benutzer vorschreiben, können Sie Fälle kompromittierter Konten reduzieren und verhindern, dass unbefugte Benutzer auf vertrauliche Daten zugreifen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0553	Wenden Sie Cybersicherheitsfunktionen (z. B. Verschlüsselung, Zugriffskontrolle und Identitätsmanagement) an, um Ausnutzungsmöglichkeiten zu reduzieren.	opensearch-encrypted-at-rest	Da sensible Daten existieren können und um Daten im Ruhezustand zu schützen, sollten Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon Elasticsearch Service (Amazon ES) -Domains aktiviert ist.
T0553	Wenden Sie Cybersicherheitsfunktionen (z. B. Verschlüsselung, Zugriffskontrolle und Identitätsmanagement) an, um Ausnutzungsmöglichkeiten zu verringern.	opensearch-node-to-node-Verschlüsselungsprüfung	Stellen Sie sicher, dass die node-to-node Verschlüsselung für Amazon Elasticsearch Service aktiviert ist. Node-to-nodeVerschlüsselung ermöglicht die TLS 1.2-Verschlüsselung für die gesamte Kommunikation innerhalb der Amazon Virtual Private Cloud (Amazon VPC). Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0553	Wenden Sie Cybersicherheitsfunktionen (z. B. Verschlüsselung, Zugriffskontrolle und Identitätsmanagement) an, um Ausnutzungsmöglichkeiten zu reduzieren.	rds-snapshot-encrypted	Stellen Sie sicher, dass die Verschlüsselung für Ihre Amazon Relational Database Service (Amazon RDS)-Snapshots aktiviert ist. Da sensible Daten auch im Ruhezustand vorhanden sein können, sollten Sie die Verschlüsselung von Daten im Ruhezustand aktivieren, um diese Daten zu schützen.
T0553	Wenden Sie Cybersicherheitsfunktionen (z. B. Verschlüsselung, Zugriffskontrolle und Identitätsmanagement) an, um Ausnutzungsmöglichkeiten zu verringern.	s-3 default-encryption-kms	Stellen Sie sicher, dass die Verschlüsselung für Ihre Amazon Simple Storage Service (Amazon S3)-Buckets aktiviert ist. Da sensible Daten in einem Amazon S3 Bucket gespeichert werden können, sollten Sie die Verschlüsselung im Ruhezustand aktivieren, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0553	Wenden Sie Cybersicherheitsfunktionen (z. B. Verschlüsselung, Zugriffskontrolle und Identitätsmanagement) an, um die Ausnutzungsmöglichkeiten zu verringern.	sagemaker-notebook-instance-kms-schlüsselkonfiguriert	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass die Verschlüsselung mit dem AWS Key Management Service (AWS KMS) für Ihr Notebook aktiviert ist. SageMaker Da vertrauliche Daten im SageMaker Notebook gespeichert werden können, sollten Sie die Verschlüsselung im Ruhezustand aktivieren, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0553	Wenden Sie Cybersicherheitsfunktionen (z. B. Verschlüsselung, Zugriffskontrolle und Identitätsmanagement) an, um Ausnutzungsmöglichkeiten zu verringern.	alb-http-to-https-Umleitungsprüfung	Um Daten während der Übertragung zu schützen, stellen Sie sicher, dass Ihr Application Load Balancer unverschlüsselte HTTP-Anfragen automatisch an HTTPS umleitet. Da sensible Daten vorhanden sein können, sollten Sie die Verschlüsselung bei der Übertragung aktivieren, um diese Daten zu schützen.
T0553	Wenden Sie Cybersicherheitsfunktionen (z. B. Verschlüsselung, Zugriffskontrolle und Identitätsmanagement) an, um Ausnutzungsmöglichkeiten zu verringern.	api-gw-cache-enabled-und verschlüsselt	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass die Verschlüsselung für den Cache Ihrer API-Gateway-Stufe aktiviert ist. Da für die API-Methode sensible Daten erfasst werden können, sollten Sie die Verschlüsselung von Daten im Ruhezustand aktivieren, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0553	Wenden Sie Cybersicherheitsfunktionen (z. B. Verschlüsselung, Zugriffskontrolle und Identitätsmanagement) an, um Ausnutzungsmöglichkeiten zu reduzieren.	api-gw-ssl-enabled	Stellen Sie sicher, dass die REST-API-Stufen von Amazon API Gateway mit SSL-Zertifikaten konfiguriert sind, damit Backend-Systeme überprüfen können, ob Anforderungen von API Gateway stammen.
T0553	Wenden Sie Cybersicherheitsfunktionen (z. B. Verschlüsselung, Zugriffskontrolle und Identitätsmanagement) an, um Ausnutzungsmöglichkeiten zu verringern.	cloud-trail-encryption-enabled	Zum Schutz von eventuell vorhandenen sensiblen Daten sowie Daten im Ruhezustand müssen Sie sicherstellen, dass die Verschlüsselung für Ihre AWS CloudTrail aktiviert ist.
T0553	Wenden Sie Cybersicherheitsfunktionen (z. B. Verschlüsselung, Zugriffskontrolle und Identitätsmanagement) an, um Ausnutzungsmöglichkeiten zu verringern.	efs-encrypted-check	Aktivieren Sie die Verschlüsselung für Ihr Amazon Elastic File System (EFS), um eventuell vorhandene sensible Daten sowie Daten im Ruhezustand zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0553	Wenden Sie Cybersicherheitsfunktionen (z. B. Verschlüsselung, Zugriffskontrolle und Identitätsmanagement) an, um Ausnutzungsmöglichkeiten zu verringern.	elasticsearch-encrypted-at-rest	Da sensible Daten existieren können und um Daten im Ruhezustand zu schützen, sollten Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon Elasticsearch Service (Amazon ES) -Domains aktiviert ist.
T0553	Wenden Sie Cybersicherheitsfunktionen (z. B. Verschlüsselung, Zugriffskontrolle und Identitätsmanagement) an, um Ausnutzungsmöglichkeiten zu verringern.	elb-acm-certificate-required	Zum Schutz von eventuell vorhanden en sensiblen Daten sowie von Daten während der Übertragung muss die Verschlüsselung für Ihr Elastic Load Balancing aktiviert sein. Verwenden Sie AWS Certificate Manager, um öffentliche und private SSL/TLS-Zertifikate mit AWS Diensten und internen Ressourcen zu verwalten, bereitzustellen und bereitzustellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0553	Wenden Sie Cybersicherheitsfunktionen (z. B. Verschlüsselung, Zugriffskontrolle und Identitätsmanagement) an, um Ausnutzungsmöglichkeiten zu reduzieren.	encrypted-volumes	Aktivieren Sie die Verschlüsselung für Ihre Amazon-Elastic-Block-Store-(Amazon-EBS-)Volumes, um eventuell vorhandene sensible Daten sowie Daten im Ruhezustand zu schützen.
T0553	Wenden Sie Cybersicherheitsfunktionen (z. B. Verschlüsselung, Zugriffskontrolle und Identitätsmanagement) an, um Ausnutzungsmöglichkeiten zu verringern.	rds-storage-encrypted	Zum Schutz von Daten im Ruhezustand müssen Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon Relational Database Service (Amazon RDS)-Instances aktiviert ist. Da sensible Daten in Amazon-RDS-Instances gespeichert werden können, sollten Sie die Verschlüsselung von Daten im Ruhezustand aktivieren, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0553	Wenden Sie Cybersicherheitsfunktionen (z. B. Verschlüsselung, Zugriffskontrolle und Identitätsmanagement) an, um Ausnutzungsmöglichkeiten zu verringern.	redshift-cluster-configuration-check	Um Daten im Ruhezustand zu schützen, muss die Verschlüsselung für Ihre Amazon-Redshift-Cluster aktiviert sein. Sie müssen auch sicherstellen, dass die erforderlichen Konfigurationen auf Amazon-Redshift-Clustern bereitgestellt werden. Die Prüfungsprotokollierung muss aktiviert sein, um Informationen zu Verbindungen und Benutzeraktivitäten in der Datenbank bereitzustellen. Diese Regel erfordert, dass ein Wert für clusterDbEncrypted (Config Default: TRUE) und LoggingEnabled (Config Default: TRUE) gesetzt ist. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0553	Wenden Sie Cybersicherheitsfunktionen (z. B. Verschlüsselung, Zugriffskontrolle und Identitätsmanagement) an, um Ausnutzungsmöglichkeiten zu reduzieren.	redshift-cluster-kms-enabled	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass die Verschlüsselung mit AWS Key Management Service (AWS KMS) für Ihren Amazon Redshift Redshift-Cluster aktiviert ist. Um eventuell vorhandene sensible Daten im Ruhezustand in Redshift-Clustern zu schützen, muss die Verschlüsselung von Daten im Ruhezustand aktiviert sein.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0553	Wenden Sie Cybersicherheitsfunktionen (z. B. Verschlüsselung, Zugriffskontrolle und Identitätsmanagement) an, um Ausnutzungsmöglichkeiten zu reduzieren.	redshift-require-tls-ssl	Stellen Sie sicher, dass Ihre Amazon-Redshift-Cluster eine TLS/SSL-Verschlüsselung erfordern, um eine Verbindung zu SQL-Clients herzustellen. Da sensible Daten vorhanden sein können, sollten Sie die Verschlüsselung bei der Übertragung aktivieren, um diese Daten zu schützen.
T0553	Wenden Sie Cybersicherheitsfunktionen (z. B. Verschlüsselung, Zugriffskontrolle und Identitätsmanagement) an, um Ausnutzungsmöglichkeiten zu verringern.	bucket-server-side-encryptions3-fähig	Zum Schutz von Daten im Ruhezustand müssen Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon Simple Storage Service (Amazon S3)-Buckets aktiviert ist. Da sensible Daten in Amazon S3 Buckets gespeichert werden können, sollten Sie die Verschlüsselung aktivieren, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0553	Wenden Sie Cybersicherheitsfunktionen (z. B. Verschlüsselung, Zugriffskontrolle und Identitätsmanagement) an, um Ausnutzungsmöglichkeiten zu reduzieren.	s-3 bucket-ssl-requests-only	Um Daten während der Übertragung zu schützen, stellen Sie sicher, dass Ihre Amazon Simple Storage Service (Amazon S3)-Buckets Anfragen zur Verwendung von Secure Socket Layer (SSL)-Buckets erfordern. Da sensible Daten vorhanden sein können, sollten Sie die Verschlüsselung bei der Übertragung aktivieren, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0553	Wenden Sie Cybersicherheitsfunktionen (z. B. Verschlüsselung, Zugriffskontrolle und Identitätsmanagement) an, um die Ausnutzungsmöglichkeiten zu verringern.	sagemaker-endpoint-configuration-kms-schlüsselkonfiguriert	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass die Verschlüsselung mit dem AWS Key Management Service (AWS KMS) für Ihren Endpunkt aktiviert ist. SageMaker Da sensible Daten auf dem SageMaker Endgerät gespeichert werden können, sollten Sie die Verschlüsselung im Ruhezustand aktivieren, um diese Daten zu schützen.
T0557	Integration von Schlüsselverwaltungsfunktionen im Zusammenhang mit dem Cyberspace.	cmk-backing-key-rotation-aktiviert	Aktivieren Sie die Schlüsselrotation, um sicherzustellen, dass Schlüssel rotiert werden, sobald sie das Ende ihrer Kryptoperiode erreicht haben.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0557	Integration von Schlüsselverwaltungsfunktionen im Zusammenhang mit dem Cyberspace.	kms-cmk-not-scheduled-zum Löschen	Um Daten im Ruhezustand zu schützen, sollten Sie sicherstellen, dass die für den Kunden erforderlichen Masterschlüssel (CMKs) nicht für das Löschen im AWS Key Management Service (AWS KMS) vorgesehen sind. Da Schlüssel manchmal gelöscht werden müssen, können Sie mit dieser Regel alle zu löschenden Schlüssel überprüfen, falls ein Schlüssel versehentlich zur Löschung vorgemerkt wurde.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0576	Bewertung von Informationen aus allen Quellen und Empfehlung von Zielen zur Unterstüt zung der Ziele von Cyberoperationen.	guardduty-enabled-centralized	Amazon GuardDuty kann mithilfe von Threat Intellige nce Feeds helfen, potenzielle Cybersich erheitsereignisse zu überwachen und zu erkennen. Dazu gehören Listen mit bösartigen IPs und maschinel len Lernmethoden zur Identifizierung unerwarteter, nicht autorisierter und bösartiger Aktivitäten in Ihrer AWS Cloud-Umgebung.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0609	Durchführung der Zugriffsfreigabe auf drahtlose Computer- und Digitalnetze.	alb-waf-enabled	Stellen Sie sicher, dass AWS WAF auf Elastic Load Balancers (ELB) aktiviert ist, um Webanwendungen zu schützen. Eine WAF trägt zum Schutz Ihrer Webanwend ungen oder APIs vor gängigen Web-Explo its bei. Diese Web-Exploits können sich auf die Verfügbar keit auswirken, die Sicherheit gefährden oder übermäßige Ressourcen in Ihrer Umgebung verbrauch en.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0609	Durchführung der Zugriffsfreigabe auf drahtlose Computer- und Digitalnetze.	api-gw-associated-with-WAF	AWS Mit WAF können Sie eine Reihe von Regeln (als Web Access Control List (Web ACL) bezeichnet) konfigurieren, die Webanfragen auf der Grundlage von anpassbaren Websicherheitsregeln und -bedingungen, die Sie definieren, zulassen, blockieren oder zählen. Stellen Sie sicher, dass Ihre Amazon-API-Gateway-Stufe mit einer WAF-Web-ACL verknüpft ist, um sie vor böswilligen Angriffen zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0609	Durchführung der Zugriffsfreigabe auf drahtlose Computer- und Digitalnetze.	autoscaling-launch-config-public-ip-deaktiviert	Wenn Sie Ihre Netzwerkschnittstellen mit einer öffentlichen IP-Adresse konfigurieren, sind die diesen Netzwerkschnittstellen zugehörigen Ressourcen über das Internet erreichbar. EC2 Ressourcen sollten nicht öffentlich zugänglich sein, da dies einen unbeabsichtigten Zugriff auf Ihre Anwendungen oder Server ermöglichen kann.
T0609	Durchführung der Zugriffsfreigabe auf drahtlose Computer- und Digitalnetze.	dms-replication-not-public	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass auf DMS-Replikationsinstanzen nicht öffentlich zugegriffen werden kann. DMS-Replikations-Instances können vertrauliche Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0609	Durchführung der Zugriffsfreigabe auf drahtlose Computer- und Digitalnetze.	ebs-snapshot-public-restorable-überprüfen	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass EBS-Snapshots nicht öffentlich wiederher stellbar sind. EBS-Volume-Snapsho ts können vertrauli che Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.
T0609	Durchführung der Zugriffsfreigabe auf drahtlose Computer- und Digitalnetze.	ec-2 instance-no-public-ip	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon Elastic Compute Cloud (Amazon EC2) - Instances nicht öffentlich zugänglic h sind. EC2Amazon -Instances können vertrauliche Informati onen enthalten, und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0609	Durchführung der Zugriffsfreigabe auf drahtlose Computer- und Digitalnetze.	elasticsearch-in-vpc-only	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass sich die Domains von Amazon Elasticsearch Service (Amazon ES) innerhalb einer Amazon Virtual Private Cloud (Amazon VPC) befinden. Eine ES-Domain in einer Amazon VPC ermöglicht eine sichere Kommunikation zwischen Amazon ES und anderen Services innerhalb der Amazon VPC, ohne dass ein Internet-Gateway, ein NAT-Gerät oder eine VPN-Verbindung benötigt wird.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0609	Durchführung der Zugriffsfreigabe auf drahtlose Computer- und Digitalnetze.	emr-master-no-public-ip	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon EMR-Cluster-Masterknoten nicht öffentlich zugänglich sind. Amazon-EMR-Cluster-Hauptknoten können vertrauliche Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0609	Durchführung der Zugriffsfreigabe auf drahtlose Computer- und Digitalnetze.	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) Security Groups können bei der Verwaltung des Netzwerkzugriffs helfen, indem sie eine statusbeh aftete Filterung von eingehendem und ausgehendem Netzwerkverkehr zu Ressourcen bereitste llen. AWS Wenn Sie eingehenden (oder entfernten) Datenverk ehr von 0.0.0.0/0 bis Port 22 auf Ihren Ressourcen nicht zulassen, können Sie den Remote-Zugriff einschränken.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0609	Durchführung der Zugriffsfreigabe auf drahtlose Computer- und Digitalnetze.	ec-2 instances-in-vpc	Stellen Sie Amazon Elastic Compute Cloud (Amazon EC2) -Instances innerhalb einer Amazon Virtual Private Cloud (Amazon VPC) bereit, um eine sichere Kommunika tion zwischen einer Instance und anderen Services innerhalb der Amazon VPC zu ermöglichen, ohne dass ein Internet-Gateway, ein NAT-Gerät oder eine VPN-Verbindung erforderlich ist. Der gesamte Datenverk ehr bleibt sicher in der AWS Cloud. Domains, die sich innerhalb einer VPC befinden, verfügen aufgrund ihrer logischen Isolierun g im Vergleich zu Domains mit öffentlic hen Endpunkten über eine zusätzlic he Sicherheitsebene. Weisen Sie EC2

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			Amazon-Instances einer Amazon-VPC zu, um den Zugriff ordnungsgemäß zu verwalten.
T0609	Durchführung der Zugriffsfreigabe auf drahtlose Computer- und Digitalnetze.	lambda-function-public-access-verboten	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass AWS Lambda-Funktionen nicht öffentlich zugänglich sind. Der öffentliche Zugriff kann möglicherweise die Verfügbarkeit von Ressourcen beeinträchtigen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0609	Durchführung der Zugriffsfreigabe auf drahtlose Computer- und Digitalnetze.	lambda-inside-vpc	Stellen Sie AWS Lambda-Funktionen in einer Amazon Virtual Private Cloud (Amazon VPC) bereit, um eine sichere Kommunika tion zwischen einer Funktion und anderen Diensten innerhalb der Amazon VPC zu gewährleisten. Bei dieser Konfiguration sind kein Internet-Gateway, kein NAT-Gerät und keine VPN-Verbindung erforderlich. Der gesamte Datenverk ehr bleibt sicher in der Cloud. AWS Domains, die sich innerhalb einer VPC befinden, verfügen aufgrund ihrer logischen Isolierun g im Vergleich zu Domains mit öffentlic hen Endpunkten über eine zusätzliche Sicherheitsebene. Um den Zugriff ordnungsg emäß zu verwalten,

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			sollten AWS Lambda-Funktionen einer VPC zugewiesen werden.
T0609	Durchführung der Zugriffsfreigabe auf drahtlose Computer- und Digitalnetze.	no-unrestricted-route-to-igw	Stellen Sie sicher, dass EC2 Amazon-Routentabellen keine uneingeschränkten Routen zu einem Internet-Gateway enthalten. Durch das Entfernen oder Beschränken des Internetzugangs für Workloads innerhalb von Amazon VPCs können unbeabsic htigte Zugriffe in Ihrer Umgebung reduziert werden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0609	Durchführung der Zugriffsfreigabe auf drahtlose Computer- und Digitalnetze.	rds-instance-public-access-überprüfen	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Relational Database Service (Amazon RDS) -Instances nicht öffentlich sind. Amazon-RDS-Datenbank-Instances können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0609	Durchführung der Zugriffsfreigabe auf drahtlose Computer- und Digitalnetze.	rds-snapshots-public-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Relational Database Service (Amazon RDS) -Instances nicht öffentlich sind. Amazon-RDS-Datenbank-Instances können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0609	Durchführung der Zugriffsfreigabe auf drahtlose Computer- und Digitalnetze.	redshift-cluster-public-access-überprüfen	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Redshift Redshift-Cluster nicht öffentlich sind. Amazon-Redshift-Cluster können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0609	Durchführung der Zugriffsfreigabe auf drahtlose Computer- und Digitalnetze.	redshift-enhanced-vpc-routing-aktiviert	Mit Enhanced-VPC-Routing wird erzwungen, dass der gesamte COPY- und UNLOAD-Datenverkehr zwischen Ihrem Cluster und Datenrepositorys über Ihre Amazon VPC erfolgt. Anschließend können Sie VPC-Features wie Sicherheitsgruppen und Netzwerkzugriffskontrolllisten verwenden, um den Netzwerkverkehr zu schützen. Sie können auch VPC-Flow-Logs verwenden, um den Netzwerkverkehr zu überwachen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0609	Durchführung der Zugriffsfreigabe auf drahtlose Computer- und Digitalnetze.	restricted-common-ports	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass gemeinsame Ports für Amazon Elastic Compute Cloud (Amazon EC2) -Sicherheitsgruppen eingeschränkt sind. Wenn der Zugriff auf Ports nicht auf vertrauenswürdige Quellen beschränkt wird, kann dies zu Angriffen auf die Verfügbarkeit, Integrität und Vertraulichkeit von Systemen führen. Mit dieser Regel können Sie optional die Parameter blockedPort1–blockedPort5 festlegen (Standardkonfigurationen: 20, 21, 3389, 3306, 4333). Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0609	Durchführung der Zugriffsfreigabe auf drahtlose Computer- und Digitalnetze.	s3- account-level-public-access -Block-periodisch	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Simple Storage Service (Amazon S3) -Buckets nicht öffentlich zugänglich sind. Diese Regel trägt dazu bei, sensible Daten vor unbefugten Remote-Benutzern zu schützen, indem sie den öffentlichen Zugriff verhindert. Mit dieser Regel können Sie optional die Parameter ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) und restrictPublicBuckets Parameter (Config Default: True) festlegen. Die tatsächlichen Werte müssen den Richtlini

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			en Ihrer Organisation entsprechen.
T0609	Durchführung der Zugriffsfreigabe auf drahtlose Computer- und Digitalnetze.	s3- bucket-public-read -prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie nur autorisierten Benutzern, Prozessen und Geräten Zugriff auf Amazon Simple Storage Service (Amazon S3) - Buckets gewähren. Die Verwaltung des Zugriffs sollte mit der Klassifizierung der Daten übereinst immen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0609	Durchführung der Zugriffsfreigabe auf drahtlose Computer- und Digitalnetze.	s3- bucket-public-write-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie nur autorisierten Benutzern, Prozessen und Geräten Zugriff auf Amazon Simple Storage Service (Amazon S3) - Buckets gewähren. Die Verwaltung des Zugriffs sollte mit der Klassifizierung der Daten übereinstimmen.
T0609	Durchführung der Zugriffsfreigabe auf drahtlose Computer- und Digitalnetze.	sagemaker-notebook-no-direct-Internetzugang	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass SageMaker Amazon-Notebooks keinen direkten Internetzugang zulassen. Indem Sie direkten Internetzugang blockieren, vermeiden Sie, dass unbefugte Benutzer auf sensible Daten zugreifen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0609	Durchführung der Zugriffsfreigabe auf drahtlose Computer- und Digitalnetze.	vpc-default-security-group-geschlossen	Sicherheitsgruppen von Amazon Elastic Compute Cloud (Amazon EC2) können bei der Verwaltung des Netzwerkzugriffs helfen, indem sie eine statusbehaftete Filterung des ein- und ausgehenden Netzwerkverkehrs zu Ressourcen bereitstellen. AWS Die Beschränk ung des gesamten Datenverkehrs auf die Standardsicherheit sgruppe hilft dabei, den Fernzugriff auf Ihre Ressourcen einzuschränken. AWS

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0609	Durchführung der Zugriffsfreigabe auf drahtlose Computer- und Digitalnetze.	vpc-sg-open-only-to-authorized-ports	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass gemeinsame Ports für Amazon Elastic Compute Cloud (Amazon EC2) -Sicherheitsgruppen eingeschränkt sind. Wenn der Zugriff auf Ports nicht auf vertrauenswürdige Quellen beschränkt wird, kann dies zu Angriffen auf die Verfügbarkeit, Integrität und Vertraulichkeit von Systemen führen. Durch die Beschränkung des Zugriffs auf Ressourcen innerhalb einer Sicherheitsgruppe aus dem Internet (0.0.0.0/0) kann der Fernzugriff auf interne Systeme gesteuert werden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0609	Durchführung der Zugriffsfreigabe auf drahtlose Computer- und Digitalnetze.	opensearch-in-vpc-only	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass sich die Domains von Amazon Elasticsearch Service (Amazon ES) innerhalb einer Amazon Virtual Private Cloud (Amazon VPC) befinden. Eine ES-Domain in einer Amazon VPC ermöglicht eine sichere Kommunikation zwischen Amazon ES und anderen Services innerhalb der Amazon VPC, ohne dass ein Internet-Gateway, ein NAT-Gerät oder eine VPN-Verbindung benötigt wird.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0609	Durchführung der Zugriffsfreigabe auf drahtlose Computer- und Digitalnetze.	subnet-auto-assign-public-ip-deaktiviert	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon Virtual Private Cloud (VPC) -Subnetzen nicht automatisch eine öffentliche IP-Adresse zugewiesen wird. Amazon Elastic Compute Cloud (EC2) -Instances, die in Subnetzen gestartet werden, in denen dieses Attribut aktiviert ist, haben ihrer primären Netzwerkschnittstelle eine öffentliche IP-Adresse zugewiesen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0616	Durchführung von Netzwerk-Scouting und Schwachst ellenanalysen von Systemen innerhalb eines Netzwerks.	guardduty-enabled-centralized	Amazon GuardDuty kann mithilfe von Threat Intellige nce Feeds helfen, potenzielle Cybersich erheitsereignisse zu überwachen und zu erkennen. Dazu gehören Listen mit bösartigen IPs und maschinel len Lernmethoden zur Identifizierung unerwarteter, nicht autorisierter und bösartiger Aktivitäten in Ihrer AWS Cloud-Umgebung.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0686	Identifizieren von Bedrohungs-Schwachstellen.	ec2-check managedinstance-patch-compliance-status	Aktivieren Sie diese Regel, um bei der Identifizierung und Dokumentation von Sicherheitslücken in Amazon Elastic Compute Cloud (Amazon EC2) zu helfen. Die Regel prüft, ob die EC2 Amazon-Instance die Patch-Konformität im AWS Systems Manager gemäß den Richtlinien und Verfahren Ihrer Organisation einhält.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0686	Identifizieren von Bedrohungs-Schwach stellen.	guardduty-enabled-centralized	Amazon GuardDuty kann mithilfe von Threat Intellige nce Feeds helfen, potenzielle Cybersich erheitsereignisse zu überwachen und zu erkennen. Dazu gehören Listen mit bösartigen IPs und maschinel len Lernmethoden zur Identifizierung unerwarteter, nicht autorisierter und bösartiger Aktivitäten in Ihrer AWS Cloud-Umgebung.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0706	Sammeln Sie Informationen über Netzwerke mithilfe herkömmlicher und alternativer Techniken (z. B. Analyse sozialer Netzwerke, Anrufverkettung, Verkehrsanalyse).	cw-loggroup-retention-period-überprüfen	Stellen Sie sicher, dass die Ereignisprotokolldaten für Ihre Protokollgruppen über eine Mindestdauer aufbewahrt werden, um die Fehlerbehebung und forensische Untersuchungen zu unterstützen. Fehlende frühere Ereignisprotokolldaten erschweren die Rekonstruierung und Identifizierung potenziell schädlicher Ereignisse.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0706	Sammeln Sie Informationen über Netzwerke mithilfe herkömmlicher und alternativer Techniken (z. B. Analyse sozialer Netzwerke, Anrufverkettung, Verkehrsanalyse).	elasticsearch-logs-to-cloudwatch	Stellen Sie sicher, dass für Amazon Elasticsearch Service-Domains Fehlerprotokolle aktiviert und zur Aufbewahrung und Beantwortung an Amazon CloudWatch Logs gestreamt werden. Domain-Fehlerprotokolle sind bei Sicherheits- und Zugriffsprüfungen sowie bei der Diagnose von Verfügbarkeitsproblemen nützlich.
T0706	Sammeln Sie Informationen über Netzwerke mithilfe herkömmlicher und alternativer Techniken (z. B. Analyse sozialer Netzwerke, Anrufverkettung, Verkehrsanalyse).	lambda-concurrency-check	Diese Regel stellt sicher, dass die Höchst- und Untergrenzen für die Gleichzeitigkeit einer Lambda-Funktion festgelegt werden. Dies kann Sie beim Baselining für die Anzahl der Anforderungen unterstützen, die Ihre Funktion zu einem bestimmten Zeitpunkt verarbeitet.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0706	Sammeln Sie Informationen über Netzwerke mithilfe herkömmlicher und alternativer Techniken (z. B. Analyse sozialer Netzwerke, Anrufverkettung, Verkehrsanalyse).	lambda-dlq-check	Aktivieren Sie diese Regel, um das entsprechende Personal über Amazon Simple Queue Service (Amazon SQS) oder Amazon Simple Notification Service (Amazon SNS) zu benachrichtigen, wenn eine Funktion ausgefallen ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0706	Sammeln Sie Informationen über Netzwerke mithilfe herkömmlicher und alternativer Techniken (z. B. Analyse sozialer Netzwerke, Anrufverkettung, Verkehrsanalyse).	multi-region-cloudtrail-enabled	AWS CloudTrail zeichnet Aktionen und API-Aufrufe der AWS Management Console auf. Sie können feststellen, welche Benutzer und Konten angerufen wurden AWS, von welcher Quell-IP-Adresse aus die Anrufe getätigt wurden und wann die Anrufe erfolgten. CloudTrail übermittelt Protokolldateien aus allen AWS Regionen an Ihren S3-Bucket , wenn MULTI_REGION_CLOUD_TRAIL_ENABLED aktiviert ist. Außerdem wird beim AWS Start einer neuen Region derselbe Trail in der neuen Region erstellt. CloudTrail Dadurch erhalten Sie automatisch Protokolldateien mit API-Aktivitäten für die neue Region.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0706	Sammeln Sie Informationen über Netzwerke mithilfe herkömmlicher und alternativer Techniken (z. B. Analyse sozialer Netzwerke, Anrufverkettung, Verkehrsanalyse).	rds-enhanced-monitoring-enabled	Aktivieren Sie Amazon Relational Database Service (Amazon RDS), um die Verfügbarkeit von Amazon RDS zu überwachen. Dies bietet einen detaillierten Einblick in den Zustand Ihrer Amazon-RDS-Datenbank-Instances. Wenn der Amazon-RDS-Speicher mehr als ein zugrunde liegendes physisches Gerät verwendet, erfasst Enhanced Monitoring die Daten für jedes Gerät. Wenn die Datenbank-Instance von Amazon RDS in einer Multi-AZ-Bereitstellung ausgeführt wird, werden außerdem die Daten für jedes Gerät auf dem sekundären Host sowie die Metriken des sekundären Hosts erfasst.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0706	Sammeln Sie Informationen über Netzwerke mithilfe herkömmlicher und alternativer Techniken (z. B. Analyse sozialer Netzwerke, Anrufverkettung, Verkehrsanalyse).	rds-logging-enabled	Um die Protokollierung und Überwachung in Ihrer Umgebung zu erleichtern, stellen Sie sicher, dass die Amazon Relational Database Service (Amazon RDS)-Protokollierung aktiviert ist. Mit der Amazon-RDS-Protokollierung können Sie Ereignisse wie Verbindungen, Verbindungsabbrüche, Abfragen oder abgefragte Tabellen erfassen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0706	Sammeln Sie Informationen über Netzwerke mithilfe herkömmlicher und alternativer Techniken (z. B. Analyse sozialer Netzwerke, Anrufverkettung, Verkehrsanalyse).	securityhub-enabled	AWS Security Hub hilft bei der Überwachung von unbefugtem Personal, Verbindungen, Geräten und Software. AWS Security Hub aggregiert, organisiert und priorisiert die Sicherheitswarnungen oder Ergebnisse mehrerer Dienste. AWS Einige dieser Dienste sind Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer und AWS Firewall Manager sowie AWS Partnerlösungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0706	Sammeln Sie Informationen über Netzwerke mithilfe herkömmlicher und alternativer Techniken (z. B. Analyse sozialer Netzwerke, Anrufverkettung, Verkehrsanalyse).	wafv2-logging-enabled	Um die Protokollierung und Überwachung in Ihrer Umgebung zu erleichtern, aktivieren Sie die AWS WAF (V2) -Protokollierung im regionalen und globalen Web. ACLs AWS Die WAF-Protokollierung bietet detaillierte Informationen über den Datenverkehr, der von Ihrer Web-ACL analysiert wird. In den Protokollen werden die Uhrzeit aufgezeichnet, zu der die AWS WAF die Anfrage von Ihrer AWS Ressource erhalten hat, Informationen über die Anfrage und eine Aktion für die Regel, der jede Anfrage entsprach.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0706	Sammeln Sie Informationen über Netzwerke mithilfe herkömmlicher und alternativer Techniken (z. B. Analyse sozialer Netzwerke, Anrufverkettung, Verkehrsanalyse).	api-gw-execution-logging-aktiviert	Die API-Gateway-Protokollierung zeigt detaillierte Ansichten der Benutzer, die auf die API zugegriffen haben, und wie diese Benutzer auf die API zugegriffen haben. Diese Insights ermöglichen die Einsicht in Benutzeraktivitäten.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0706	Sammeln Sie Informationen über Netzwerke mithilfe herkömmlicher und alternativer Techniken (z. B. Analyse sozialer Netzwerke, Anrufverkettung, Verkehrsanalyse).	autoscaling-group-elb-healthcheck-erforderlich	Die Elastic Load Balancer (ELB) - Zustandsprüfungen für Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling Scaling-Gruppen unterstützen die Aufrechterhaltung einer angemessenen Kapazität und Verfügbarkeit. Der Load Balancer sendet regelmäßig Pings, versucht Verbindungen herzustellen oder sendet Anfragen, um den Zustand der EC2 Amazon-Instances in einer Gruppe mit auto-scaling zu testen. Wenn eine Instance nicht zurückmeldet, wird der Traffic an eine neue EC2 Amazon-Instance gesendet.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0706	Sammeln Sie Informationen über Netzwerke mithilfe herkömmlicher und alternativer Techniken (z. B. Analyse sozialer Netzwerke, Anrufverkettung, Verkehrsanalyse).	beanstalk-enhanced-health-reporting-aktiviert	AWS Die verbesserte Zustandsberichterstattung von Elastic Beanstalk ermöglicht eine schnellere Reaktion auf Veränderungen im Zustand der zugrunde liegenden Infrastruktur. Diese Änderungen könnten zu einer mangelnden Verfügbarkeit der Anwendung führen. Die erweiterten Zustandsberichte von Elastic Beanstalk bieten eine Statusbeschreibung, um den Schweregrad der identifizierten Probleme einzuschätzen und mögliche Ursachen zu identifizieren, die untersucht werden müssen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0706	Sammeln Sie Informationen über Netzwerke mithilfe herkömmlicher und alternativer Techniken (z. B. Analyse sozialer Netzwerke, Anrufverkettung, Verkehrsanalyse).	cloud-trail-cloud-watch-Logs aktiviert	Verwenden Sie Amazon CloudWatch , um Protokoll ereignisaktivitäten zentral zu sammeln und zu verwalten. Die Aufnahme von AWS CloudTrail Daten liefert Einzelheiten zu den API-Aufrufaktivitäten in Ihrem AWS-Konto.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0706	Sammeln Sie Informationen über Netzwerke mithilfe herkömmlicher und alternativer Techniken (z. B. Analyse sozialer Netzwerke, Anrufverkettung, Verkehrsanalyse).	cloudtrail-enabled	AWS CloudTrail kann durch die Aufzeichnung AWS von Aktionen und API-Aufrufen in der Management Console helfen, die Ablehnung zu verhindern. Sie können die Benutzer und die Benutzer AWS-Konten , die einen AWS Dienst aufgerufen haben, die Quell-IP-Adresse, über die die Aufrufe generiert wurden, und den Zeitpunkt der Anrufe identifizieren. Einzelheiten zu den erfassten Daten finden Sie unter Inhalt des AWS CloudTrail Datensatzes.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0706	Sammeln Sie Informationen über Netzwerke mithilfe herkömmlicher und alternativer Techniken (z. B. Analyse sozialer Netzwerke, Anrufverkettung, Verkehrsanalyse).	cloudtrail-s3-dataevents-enabled	Die Erfassung von Simple Storage Service (Amazon S3)-Datenereignissen unterstützt die Erkennung von ungewöhnlichen Aktivitäten. Zu den Details gehören Informationen zu dem AWS -Konto, das auf einen Amazon-S3-Bucket zugegriffen hat, die IP-Adresse und die Uhrzeit des Ereignisses.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0706	Sammeln Sie Informationen über Netzwerke mithilfe herkömmlicher und alternativer Techniken (z. B. Analyse sozialer Netzwerke, Anrufverkettung, Verkehrsanalyse).	cloudwatch-alarm-action-check	Amazon CloudWatch alarmiert, wenn eine Metrik den Schwellenwert für eine bestimmte Anzahl von Bewertungszeiträumen überschreitet. Der Alarm führt eine oder mehrere Aktionen durch, die vom Wert der Metrik oder des Ausdrucks im Vergleich zu einem Schwellenwert in einer Reihe von Zeiträumen abhängt. Diese Regel erfordert einen Wert für alarmActionRequired (Config Default: True), insufficientDataAction Required (Config Default: True), okActionRequired (Config Default: False). Der tatsächliche Wert muss die Alarmaktionen für Ihre Umgebung widerspiegeln.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0706	Sammeln Sie Informationen über Netzwerke mithilfe herkömmlicher und alternativer Techniken (z. B. Analyse sozialer Netzwerke, Anrufverkettung, Verkehrsanalyse).	dynamodb-throughput-limit-check	Aktivieren Sie diese Regel, um sicherzustellen, dass die bereitgestellte Durchsatzkapazität in Ihren Amazon-DynamoDB-Tabellen überprüft wird. Dies ist der Umfang der Lese- und Schreibaktivitäten, der von den jeweiligen Tabellen unterstützt werden kann. DynamoDB verwendet diese Informationen für das Reservieren ausreichender Systemressourcen, um Ihren Durchsatz anforderungen gerecht zu werden. Diese Regel generiert eine Warnung, wenn sich der Durchsatz dem Höchstlimit für ein Kundenkonto nähert. Mit dieser Regel können Sie optional die Parameter RCUThreshold Kontoprozentsatz

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			(Konfigurationsstandard: 80) und WCUThreshold Kontoprozentsatz (Konfigurationsstandard: 80) festlegen. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.
T0706	Sammeln Sie Informationen über Netzwerke mithilfe herkömmlicher und alternativer Techniken (z. B. Analyse sozialer Netzwerke, Anrufverkettung, Verkehrsanalyse).	ec2- instance-detailed-monitoring-enabled	Aktivieren Sie diese Regel, um die Amazon Elastic Compute Cloud (Amazon EC2) - Instance-Überwachung auf der EC2 Amazon-Konsole zu verbessern, in der Monitoring-Diagramme mit einem Zeitraum von 1 Minute für die Instance angezeigt werden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0706	Sammeln Sie Informationen über Netzwerke mithilfe herkömmlicher und alternativer Techniken (z. B. Analyse sozialer Netzwerke, Anrufverkettung, Verkehrsanalyse).	elb-logging-enabled	Die Elastic-Load-Balancing-Aktivität ist ein zentraler Kommunikationspunkt innerhalb einer Umgebung. Stellen Sie sicher, dass die ELB-Protokollierung aktiviert ist. Die gesammelten Daten enthalten detaillierte Informationen zu Anfragen, die an den ELB gesendet wurden. Jedes Protokoll enthält Informationen wie die Zeit, zu der die Anforderung einging, die Client-IP-Adresse, Latenzen, Anforderungspfade und Serverantworten.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0706	Sammeln Sie Informationen über Netzwerke mithilfe herkömmlicher und alternativer Techniken (z. B. Analyse sozialer Netzwerke, Anrufverkettung, Verkehrsanalyse).	guardduty-enabled-centralized	Amazon GuardDuty kann mithilfe von Threat Intelligence Feeds helfen, potenzielle Cybersicherheitsereignisse zu überwachen und zu erkennen. Dazu gehören Listen mit bösartigen IPs und maschinellen Lernmethoden zur Identifizierung unerwarteter, nicht autorisierter und bösartiger Aktivitäten in Ihrer AWS Cloud-Umgebung.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0706	Sammeln Sie Informationen über Netzwerke mithilfe herkömmlicher und alternativer Techniken (z. B. Analyse sozialer Netzwerke, Anrufverkettung, Verkehrsanalyse).	redshift-cluster-configuration-check	Um Daten im Ruhezustand zu schützen, muss die Verschlüsselung für Ihre Amazon-Redshift-Cluster aktiviert sein. Sie müssen auch sicherstellen, dass die erforderlichen Konfigurationen auf Amazon-Redshift-Clustern bereitgestellt werden. Die Prüfungsprotokollierung muss aktiviert sein, um Informationen zu Verbindungen und Benutzeraktivitäten in der Datenbank bereitzustellen. Diese Regel erfordert, dass ein Wert für clusterDbEncrypted (Config Default: TRUE) und LoggingEnabled (Config Default: TRUE) gesetzt ist. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0706	Sammeln Sie Informationen über Netzwerke mithilfe herkömmlicher und alternativer Techniken (z. B. Analyse sozialer Netzwerke, Anrufverkettung, Verkehrsanalyse).	s3- bucket-logging-enabled	Die Amazon Simple Storage Service (Amazon S3)-Serverzugriffsprotokollierung bietet eine Methode zur Überwachung des Netzwerks im Hinblick auf potenzielle Cybersicherheitsereignisse. Die Ereignisse werden überwacht, indem detaillierte Aufzeichnungen über die Anfragen erfasst werden, die an einen Amazon-S3-Bucket gestellt wurden. Jeder Zugriffsprotokolleintrag enthält Details zu einer einzelnen Zugriffsanfrage. Zu den Details gehören Anforderer, Bucket-Name, Anforderungszeit, Anforderungsaktion, Antwortstatus und Fehlercode, falls relevant.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0706	Sammeln Sie Informationen über Netzwerke mithilfe herkömmlicher und alternativer Techniken (z. B. Analyse sozialer Netzwerke, Anrufverkettung, Verkehrsanalyse).	vpc-flow-logs-enabled	VPC-Flow-Protokolle erfassen detaillierte Informationsdatensätze über den IP-Datenverkehr, der zu und von Netzwerkschnittstellen in Ihrer Amazon Virtual Private Cloud (Amazon VPC) fließt. Standardmäßig enthalten Flow-Protokolldatensätze Werte für die verschiedenen Komponenten des IP-Flows, einschließlich Quelle, Ziel und Protokoll.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0777	Profile von Netzwerk- oder Systemadm inistratoren und deren Tätigkeiten.	guardduty-enabled-centralized	Amazon GuardDuty kann mithilfe von Threat Intellige nce Feeds helfen, potenzielle Cybersich erheitsereignisse zu überwachen und zu erkennen. Dazu gehören Listen mit bösartigen IPs und maschinel len Lernmethoden zur Identifizierung unerwarteter, nicht autorisierter und bösartiger Aktivitäten in Ihrer AWS Cloud-Umgebung.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0805	Meldung nachricht endienstlich ermittelt er signifikanter Netzwerkereignisse und Eindringlinge.	guardduty-enabled-centralized	Amazon GuardDuty kann mithilfe von Threat Intellige nce Feeds helfen, potenzielle Cybersich erheitsereignisse zu überwachen und zu erkennen. Dazu gehören Listen mit bösartigen IPs und maschinel len Lernmethoden zur Identifizierung unerwarteter, nicht autorisierter und bösartiger Aktivitäten in Ihrer AWS Cloud-Umgebung.
T0877	Zusammenarbeit mit den zuständig en Organisat ionseinheiten bei der Überwachung der Zugangsrechte zu Verbraucherinforma tionen	ec2- instance-profile-a ttached	EC2 Instanzprofile übergeben eine IAM-Rolle an eine Instanz EC2 . Das Anhängen eines Instance-Profils an Ihre Instances kann bei der Implement ierung von geringste n Berechtigungen und der Berechtig ungsverwaltung helfen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0877	Zusammenarbeit mit den zuständigen Organisationseinheiten bei der Überwachung der Zugangsrechte zu Verbraucherinformationen	ecs-task-definition-user-for-host-mode-check	Wenn für eine Aufgabendefinition erhöhte Berechtigungen gelten, liegt das daran, dass der Kunde diesen Konfigurationen ausdrücklich zugestimmt hat. Diese Kontrolle prüft, ob eine unerwartete Berechtigungseskalation vorliegt, wenn für eine Aufgabendefinition das Host-Netzwerk aktiviert ist, die Kunden aber keine erhöhten Berechtigungen aktiviert haben.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0877	Zusammenarbeit mit den zuständigen Organisationseinheiten bei der Überwachung der Zugangsrechte zu Verbraucherinformationen	iam-no-inline-policy-überprüfen	Stellen Sie sicher, dass ein Benutzer, eine IAM-Rolle oder eine IAM-Gruppe (AWS Identity and Access Management) nicht über eine Inline-Richtlinie zur Zugriffskontrolle auf Systeme und Ressourcen verfügt. AWS empfiehlt, verwaltete Richtlinien anstelle von Inline-Richtlinien zu verwenden. Verwaltete Richtlinien ermöglichen Wiederverwendbarkeit, Versionsverwaltung, Rollback und Delegierung der Berechtigungsverwaltung.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0877	Zusammenarbeit mit den zuständigen Organisationseinheiten bei der Überwachung der Zugangsrechte zu Verbraucherinformationen	iam-policy-no-statements-with-full-access	Stellen Sie sicher, dass IAM-Aktionen nur auf die benötigten Aktionen beschränkt sind. Wenn Benutzern mehr Rechte eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Rechte und der Aufgabentrennung verstoßen.
T0877	Zusammenarbeit mit den zuständigen Organisationseinheiten bei der Überwachung der Zugangsrechte zu Verbraucherinformationen	ssm-document-not-public	Stellen Sie sicher, dass AWS Systems Manager (SSM) - Dokumente nicht öffentlich sind, da dies einen unbeabsichtigten Zugriff auf Ihre SSM-Dokumente ermöglichen kann. Ein öffentliches SSM-Dokument kann Informationen über Ihr Konto, Ihre Ressourcen und internen Prozesse preisgeben.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0877	Zusammenarbeit mit den zuständigen Organisationseinheiten bei der Überwachung der Zugangsrechte zu Verbraucherinformationen	emr-kerberos-enabled	Die Zugriffsberechtigungen und -autorisierungen können verwaltet und nach den Prinzipien der geringsten Berechtigung und Aufgabentrennung integriert werden, indem Kerberos für Amazon-EMR-Cluster aktiviert wird. In Kerberos werden Services und Benutzer, die sich authentifizieren müssen, als Prinzipale bezeichnet. Prinzipale befinden sich in einem Kerberos-Bereich. Innerhalb dieses Bereichs wird ein Kerberos-Server als Key Distribution Center (KDC) bezeichnet. Über diesen Server können sich Prinzipale authentifizieren. Die Authentifizierung im KDC erfolgt durch die Ausstellung von Authentif

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			izierungstickets. Das KDC unterhält eine Datenbank der Prinzipale in seinem Bereich mit ihren Passwörtern und anderen administr ativen Informationen zu jedem Prinzipal.
T0877	Zusammenarbeit mit den zuständig en Organisat ionseinheiten bei der Überwachung der Zugangsrechte zu Verbraucherinforma tionen	iam-group-has-users-überprüfen	AWS Identity and Access Managemen t (IAM) kann Ihnen helfen, die Prinzipien der geringsten Rechte und der Aufgabent rennung mit Zugriffsb erechtigungen und Autorisierungen zu integrieren, indem sichergestellt wird, dass IAM-Gruppen mindestens einen Benutzer haben. Die Einteilung von Benutzern in Gruppen auf der Grundlage der ihnen zugewiese nen Berechtigungen oder ihrer Funktion ist eine Möglichkeit, das Prinzip der geringste n Berechtigung zu implementieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0877	Zusammenarbeit mit den zuständigen Organisationseinheiten bei der Überwachung der Zugangsrechte zu Verbraucherinformationen	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) kann Ihnen dabei helfen, die Prinzipien der geringsten Rechte und der Aufgabentrennung in Zugriffsberechtigungen und Autorisierungen zu integrieren und so zu verhindern, dass Richtlinien „Effect“: „Allow“ mit „Action“: „*“ anstelle von „Resource“: „*“ enthalten. Wenn Benutzern mehr Rechte eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und der Aufgabentrennung verstoßen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0877	Zusammenarbeit mit den zuständigen Organisationseinheiten bei der Überwachung der Zugangsrechte zu Verbraucherinformationen	iam-user-group-membership-überprüfen	AWS Identity and Access Management (IAM) kann Ihnen helfen, Zugriffsberechtigungen und Autorisierungen einzuschränken, indem sichergestellt wird, dass Benutzer Mitglieder mindestens einer Gruppe sind. Wenn Benutzern mehr Berechtigungen eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und Aufgabentrennung verstoßen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0877	Zusammenarbeit mit den zuständigen Organisationseinheiten bei der Überwachung der Zugangsrechte zu Verbraucherinformationen	iam-user-no-policies-überprüfen	Diese Regel stellt sicher, dass AWS Identity and Access Management (IAM)-Richtlinien nur Gruppen oder Rollen zugewiesen werden, um den Zugriff auf Systeme und Ressourcen zu kontrollieren. Die Zuweisung von Berechtigungen auf Gruppen- oder Rollenebene trägt dazu bei, die Wahrscheinlichkeit zu verringern, dass eine Identität übermäßige Berechtigungen erhält oder beibehält.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0877	Zusammenarbeit mit den zuständigen Organisationseinheiten bei der Überwachung der Zugangsrechte zu Verbraucherinformationen	restricted-common-ports	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass gemeinsame Ports für Amazon Elastic Compute Cloud (Amazon EC2) -Sicherheitsgruppen eingeschränkt sind. Wenn der Zugriff auf Ports nicht auf vertrauenswürdige Quellen beschränkt wird, kann dies zu Angriffen auf die Verfügbarkeit, Integrität und Vertraulichkeit von Systemen führen. Mit dieser Regel können Sie optional die Parameter blockedPort1–blockedPort5 festlegen (Standardkonfigurationen: 20, 21, 3389, 3306, 4333). Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0935	Durchführung einer Risikobewertung der Informationssicherheit.	annual-risk-assessment-performed (Prozessprüfung)	Führen Sie eine jährliche Risikobewertung für Ihre Organisation durch. Risikowertungen können dabei helfen, die Wahrscheinlichkeit und Auswirkungen identifizierter Risiken und/oder Schwachstellen für eine Organisation zu ermitteln.
T0960	Überwachung von Änderungen an einem System und seiner Betriebsumgebung.	lambda-concurrency-check	Diese Regel stellt sicher, dass die Höchst- und Untergrenzen für die Gleichzeitigkeit einer Lambda-Funktion festgelegt werden. Dies kann Sie beim Baselining für die Anzahl der Anforderungen unterstützen, die Ihre Funktion zu einem bestimmten Zeitpunkt verarbeitet.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0960	Überwachung von Änderungen an einem System und seiner Betriebsumgebung.	lambda-dlq-check	Aktivieren Sie diese Regel, um das entsprechende Personal über Amazon Simple Queue Service (Amazon SQS) oder Amazon Simple Notification Service (Amazon SNS) zu benachrichtigen, wenn eine Funktion ausgefallen ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0960	Überwachung von Änderungen an einem System und seiner Betriebsumgebung.	rds-enhanced-monitoring-enabled	Aktivieren Sie Amazon Relational Database Service (Amazon RDS), um die Verfügbarkeit von Amazon RDS zu überwachen. Dies bietet einen detaillierten Einblick in den Zustand Ihrer Amazon-RDS-Datenbank-Instances. Wenn der Amazon-RDS-Speicher mehr als ein zugrunde liegendes physisches Gerät verwendet, erfasst Enhanced Monitoring die Daten für jedes Gerät. Wenn die Datenbank-Instance von Amazon RDS in einer Multi-AZ-Bereitstellung ausgeführt wird, werden außerdem die Daten für jedes Gerät auf dem sekundären Host sowie die Metriken des sekundären Hosts erfasst.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0960	Überwachung von Änderungen an einem System und seiner Betriebsumgebung.	autoscaling-group-elb-healthcheck-erforderlich	Die Elastic Load Balancer (ELB) - Zustandsprüfungen für Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling Scaling-Gruppen unterstützen die Aufrechterhaltung einer angemessenen Kapazität und Verfügbarkeit. Der Load Balancer sendet regelmäßig Pings, versucht Verbindungen herzustellen oder sendet Anfragen, um den Zustand der EC2 Amazon-Instances in einer Gruppe mit auto-scaling zu testen. Wenn eine Instance nicht zurückmeldet, wird der Traffic an eine neue EC2 Amazon-Instance gesendet.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0960	Überwachung von Änderungen an einem System und seiner Betriebsumgebung.	beanstalk-enhanced-health-reporting-aktiviert	AWS Die verbesserte Zustandsberichterstattung von Elastic Beanstalk ermöglicht eine schnellere Reaktion auf Veränderungen im Zustand der zugrunde liegenden Infrastruktur. Diese Änderungen könnten zu einer mangelnden Verfügbarkeit der Anwendung führen. Die erweiterten Zustandsberichte von Elastic Beanstalk bieten eine Statusbeschreibung, um den Schweregrad der identifizierten Probleme einzuschätzen und mögliche Ursachen zu identifizieren, die untersucht werden müssen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0960	Überwachung von Änderungen an einem System und seiner Betriebsumgebung.	cloudwatch-alarm-action-check	Amazon CloudWatch alarmiert, wenn eine Metrik den Schwellenwert für eine bestimmte Anzahl von Bewertungszeiträumen überschreitet. Der Alarm führt eine oder mehrere Aktionen durch, die vom Wert der Metrik oder des Ausdrucks im Vergleich zu einem Schwellenwert in einer Reihe von Zeiträumen abhängt. Diese Regel erfordert einen Wert für alarmActionRequired (Config Default: True), insufficientDataAction Required (Config Default: True), okActionRequired (Config Default: False). Der tatsächliche Wert muss die Alarmaktionen für Ihre Umgebung widerspiegeln.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0960	Überwachung von Änderungen an einem System und seiner Betriebsumgebung.	dynamodb-throughput-limit-check	Aktivieren Sie diese Regel, um sicherzustellen, dass die bereitgestellte Durchsatzkapazität in Ihren Amazon-DynamoDB-Tabellen überprüft wird. Dies ist der Umfang der Lese- und Schreibaktivitäten, der von den jeweiligen Tabellen unterstützt werden kann. DynamoDB verwendet diese Informationen für das Reservieren ausreichender Systemressourcen, um Ihren Durchsatz anforderungen gerecht zu werden. Diese Regel generiert eine Warnung, wenn sich der Durchsatz dem Höchstlimit für ein Kundenkonto nähert. Mit dieser Regel können Sie optional die Parameter RCUThreshold Kontoprozentsatz

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			(Konfigurationsstandard: 80) und WCUThreshold Kontoprozentsatz (Konfigurationsstandard: 80) festlegen. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.
T0960	Überwachung von Änderungen an einem System und seiner Betriebsumgebung.	ec2- instance-detailed-monitoring-enabled	Aktivieren Sie diese Regel, um die Amazon Elastic Compute Cloud (Amazon EC2) - Instance-Überwachung auf der EC2 Amazon-Konsole zu verbessern, in der Monitoring-Diagramme mit einem Zeitraum von 1 Minute für die Instance angezeigt werden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0992	Legen Sie fest, wie die Ergebnisse der kontinuierlichen Überwachung bei der laufenden Genehmigung verwendet werden sollen.	ec-2 instance-profile-attached	EC2 Instanzprofile übergeben eine IAM-Rolle an eine Instanz EC2 . Das Anhängen eines Instance-Profils an Ihre Instances kann bei der Implementierung von geringsten Berechtigungen und der Berechtigungsverwaltung helfen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0992	Legen Sie fest, wie die Ergebnisse der kontinuierlichen Überwachung bei der laufenden Genehmigung verwendet werden sollen.	ecs-task-definition-user-for-host-mode-check	Wenn für eine Aufgabendefinition erhöhte Berechtigungen gelten, liegt das daran, dass der Kunde diesen Konfigurationen ausdrücklich zugestimmt hat. Diese Kontrolle prüft, ob eine unerwartete Berechtigungseskalation vorliegt, wenn für eine Aufgabendefinition das Host-Netzwerk aktiviert ist, die Kunden aber keine erhöhten Berechtigungen aktiviert haben.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0992	Legen Sie fest, wie die Ergebnisse der kontinuierlichen Überwachung bei der laufenden Genehmigung verwendet werden sollen.	iam-no-inline-policy-überprüfen	Stellen Sie sicher, dass ein Benutzer, eine IAM-Rolle oder eine IAM-Gruppe (AWS Identity and Access Management) nicht über eine Inline-Richtlinie zur Zugriffskontrolle auf Systeme und Ressourcen verfügt. AWS empfiehlt, verwaltete Richtlinien anstelle von Inline-Richtlinien zu verwenden. Verwaltete Richtlinien ermöglichen Wiederverwendbarkeit, Versionsverwaltung, Rollback und Delegierung der Berechtigungsverwaltung.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0992	Legen Sie fest, wie die Ergebnisse der kontinuierlichen Überwachung bei der laufenden Genehmigung verwendet werden sollen.	iam-policy-no-statements-with-full-access	Stellen Sie sicher, dass IAM-Aktionen nur auf die benötigten Aktionen beschränkt sind. Wenn Benutzern mehr Rechte eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Rechte und der Aufgabentrennung verstoßen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0992	Legen Sie fest, wie die Ergebnisse der kontinuierlichen Überwachung bei der laufenden Genehmigung verwendet werden sollen.	access-keys-rotated	Die Anmeldeinformationen für autorisierte Geräte, Benutzer und Prozesse werden geprüft, indem sichergestellt wird, dass die IAM-Zugriffsschlüssel entsprechend den Vorgaben der Unternehmensrichtlinie rotiert werden. Das regelmäßige Ändern der Zugriffsschlüssel ist eine bewährte Sicherheitsmethode. Es verkürzt den Zeitraum, in dem ein Zugriffsschlüssel aktiv ist, und reduziert die Auswirkungen auf das Unternehmen, wenn die Schlüssel kompromittiert werden. Diese Regel erfordert einen Wert für die Zugriffsschlüssel-Rotation (Standardkonfiguration: 90). Der tatsächliche Wert muss den Richtlini

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			en Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0992	Legen Sie fest, wie die Ergebnisse der kontinuierlichen Überwachung bei der laufenden Genehmigung verwendet werden sollen.	emr-kerberos-enabled	Die Zugriffsberechtigungen und -autorisierungen können verwaltet und nach den Prinzipien der geringsten Berechtigung und Aufgabentrennung integriert werden, indem Kerberos für Amazon-EMR-Cluster aktiviert wird. In Kerberos werden Services und Benutzer, die sich authentifizieren müssen, als Prinzipale bezeichnet. Prinzipale befinden sich in einem Kerberos-Bereich. Innerhalb dieses Bereichs wird ein Kerberos-Server als Key Distribution Center (KDC) bezeichnet. Über diesen Server können sich Prinzipale authentifizieren. Die Authentifizierung im KDC erfolgt durch die Ausstellung von Authentif

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			izierungstickets. Das KDC unterhält eine Datenbank der Prinzipale in seinem Bereich mit ihren Passwörtern und anderen administr ativen Informationen zu jedem Prinzipal.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0992	Legen Sie fest, wie die Ergebnisse der kontinuierlichen Überwachung bei der laufenden Genehmigung verwendet werden sollen.	iam-customer-policy-blocked-kms-Aktionen	AWS Identity and Access Management (IAM) kann Ihnen helfen, die Prinzipien der geringsten Rechte und der Aufgabentrennung in Zugriffsberechtigungen und Autorisierungen zu integrieren und so zu verhindern, dass Richtlinien blockierte Aktionen für alle AWS Schlüssel des Key Management Service enthalten. Wenn Benutzer mehr Rechte haben, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und Aufgabentrennung verstoßen. Mit dieser Regel können Sie den Parameter festlegen. blockedActionsPatterns (Wert „AWS Bewährte grundlegende Sicherheitsmethoden“: kms:

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			Decrypt, kms:ReEncryptFrom). Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.
T0992	Legen Sie fest, wie die Ergebnisse der kontinuierlichen Überwachung bei der laufenden Genehmigung verwendet werden sollen.	iam-group-has-users-überprüfen	AWS Identity and Access Management (IAM) kann Ihnen helfen, die Prinzipien der geringsten Rechte und der Aufgabentrennung mit Zugriffsberechtigungen und Autorisierungen zu integrieren, indem sichergestellt wird, dass IAM-Gruppen mindestens einen Benutzer haben. Die Einteilung von Benutzern in Gruppen auf der Grundlage der ihnen zugewiesenen Berechtigungen oder ihrer Funktion ist eine Möglichkeit, das Prinzip der geringsten Berechtigung zu implementieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0992	Legen Sie fest, wie die Ergebnisse der kontinuierlichen Überwachung bei der laufenden Genehmigung verwendet werden sollen.	iam-inline-policy-blocked-kms-Aktionen	Stellen Sie sicher, dass ein Benutzer, eine IAM-Rolle oder eine IAM-Gruppe (AWS Identity and Access Management) nicht über eine Inline-Richtlinie verfügt, die blockierte Aktionen für alle AWS Schlüssel des Key Management Service zulässt. AWS empfiehlt, verwaltete Richtlinien anstelle von Inline-Richtlinien zu verwenden. Verwaltete Richtlinien ermöglichen Wiederverwendbarkeit, Versionsverwaltung, Rollback und Delegierung der Berechtigungsverwaltung. Mit dieser Regel können Sie den blockedActionsPatterns Parameter festlegen. (Wert „AWS Bewährte grundlegende Sicherheitsmethoden“: kms:Decrypt, kms:ReEncryptFrom). Die

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0992	Legen Sie fest, wie die Ergebnisse der kontinuierlichen Überwachung bei der laufenden Genehmigung verwendet werden sollen.	iam-password-policy	Die Identitäten und Anmeldeinformationen werden auf der Grundlage einer organisatorischen IAM-Passwortrichtlinie ausgestellt, verwaltet und verifiziert. Sie erfüllen oder übertreffen die Anforderungen des NIST SP 800-63 und des AWS Foundational Security Best Practices-Standards für Passwortstärke. Mit dieser Regel können Sie optional RequireUppercaseCharacters (Wert für AWS grundlegende Sicherheitsbewährte Methoden: wahr), RequireLowercaseCharacters (Wert für bewährte Methoden für AWS grundlegende Sicherheit: wahr), RequireSymbols (Wert für bewährte Methoden für AWS grundlegende Sicherheit:

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			wahr), RequireNumbers (Wert für bewährte Methoden für AWS grundlegende Sicherheit: wahr), MinimumPasswordLength (Wert für bewährte Methoden für AWS grundlegende Sicherheit: 14), PasswordReusePrevention (Wert für bewährte Methoden für AWS grundlegende Sicherheit: 24) und MaxPasswordAge (Wert für bewährte Methoden für AWS grundlegende Sicherheit: 90) für Ihr IAM festlegen Kennwortrichtlinie. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0992	Legen Sie fest, wie die Ergebnisse der kontinuierlichen Überwachung bei der laufenden Genehmigung verwendet werden sollen.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) kann Ihnen dabei helfen, die Prinzipien der geringsten Rechte und der Aufgabentrennung in Zugriffsberechtigungen und Autorisierungen zu integrieren und so zu verhindern, dass Richtlinien „Effect“: „Allow“ mit „Action“: „*“ anstelle von „Resource“: „*“ enthalten. Wenn Benutzern mehr Rechte eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und der Aufgabentrennung verstoßen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0992	Legen Sie fest, wie die Ergebnisse der kontinuierlichen Überwachung bei der laufenden Genehmigung verwendet werden sollen.	iam-root-access-key-überprüfen	Der Zugriff auf Systeme und Ressourcen kann gesteuert werden, indem überprüft wird, ob der Root-Benutzer keine Zugriffsschlüssel mit seiner AWS Identity and Access Management (IAM) -Rolle verknüpft hat. Stellen Sie sicher, dass die Root-Zugriffsschlüssel gelöscht werden. Erstellen und verwenden Sie stattdessen rollenbasierte Funktionen, AWS-Konten um das Prinzip der geringsten Funktionalität zu berücksichtigen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0992	Legen Sie fest, wie die Ergebnisse der kontinuierlichen Überwachung bei der laufenden Genehmigung verwendet werden sollen.	iam-user-group-membership-überprüfen	AWS Identity and Access Management (IAM) kann Ihnen helfen, Zugriffsberechtigungen und Autorisierungen einzuschränken, indem sichergestellt wird, dass Benutzer Mitglieder mindestens einer Gruppe sind. Wenn Benutzern mehr Berechtigungen eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und Aufgabentrennung verstoßen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0992	Legen Sie fest, wie die Ergebnisse der kontinuierlichen Überwachung bei der laufenden Genehmigung verwendet werden sollen.	iam-user-mfa-enabled	Aktivieren Sie diese Regel, um den Zugriff auf Ressourcen in der AWS -Cloud einzuschränken. Diese Regel stellt sicher, dass die Multi-Faktor-Authentifizierung (MFA) für alle Benutzer aktiviert ist. MFA bietet eine weitere Schutzebene zusätzlich zum Benutzernamen und Passwort. Reduzieren Sie Fälle von kompromittierten Konten, indem Sie MFA für Benutzer vorschreiben.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0992	Legen Sie fest, wie die Ergebnisse der kontinuierlichen Überwachung bei der laufenden Genehmigung verwendet werden sollen.	iam-user-no-policies-überprüfen	Diese Regel stellt sicher, dass AWS Identity and Access Management (IAM) -Richtlinien nur Gruppen oder Rollen zugewiesen werden, um den Zugriff auf Systeme und Ressourcen zu kontrollieren. Die Zuweisung von Berechtigungen auf Gruppen- oder Rollenebene trägt dazu bei, die Wahrscheinlichkeit zu verringern, dass eine Identität übermäßige Berechtigungen erhält oder beibehält.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0992	Legen Sie fest, wie die Ergebnisse der kontinuierlichen Überwachung bei der laufenden Genehmigung verwendet werden sollen.	iam-user-unused-credentials-überprüfen	AWS Identity and Access Management (IAM) kann Ihnen bei Zugriffsberechtigungen und Autorisierungen helfen, indem es nach IAM-Passwörtern und Zugriffsschlüsseln sucht, die für einen bestimmten Zeitraum nicht verwendet wurden. Wenn ungenutzte Anmeldeinformationen identifiziert werden, müssen Sie sie deaktivieren und/oder entfernen, da dies gegen das Prinzip der geringsten Berechtigung verstoßen könnte. Für diese Regel müssen Sie einen Wert für das maxCredentialUsage Alter festlegen (Standardkonfiguration: 90). Der tatsächliche Wert muss den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0992	Legen Sie fest, wie die Ergebnisse der kontinuierlichen Überwachung bei der laufenden Genehmigung verwendet werden sollen.	mfa-enabled-for-iam-Konsolenzugriff	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass MFA für alle AWS Identity and Access Management (IAM) -Benutzer aktiviert ist, die über ein Konsolenkennwort verfügen. MFA sorgt für eine weitere Schutzebene zusätzlich zu den Anmeldeinformationen. Indem Sie MFA für Benutzer vorschreiben, können Sie Fälle kompromittierter Konten reduzieren und verhindern, dass unbefugte Benutzer auf vertrauliche Daten zugreifen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0992	Legen Sie fest, wie die Ergebnisse der kontinuierlichen Überwachung bei der laufenden Genehmigung verwendet werden sollen.	root-account-hardware-mfa-aktiviert	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Hardware-MFA für den Root-Benutzer aktiviert ist. Der Stammbenutzer ist der AWS-Konto-Benutzer mit den meisten Berechtigungen. MFA sorgt für eine weitere Schutzebene zusätzlich zu den Anmeldeinformationen. Indem Sie MFA für den Root-Benutzer vorschreiben, können Sie die Anzahl AWS-Konten kompromittierter Benutzer reduzieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0992	Legen Sie fest, wie die Ergebnisse der kontinuierlichen Überwachung bei der laufenden Genehmigung verwendet werden sollen.	root-account-mfa-enabled	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass MFA für den Root-Benutzer aktiviert ist. Der Stammbenutzer ist der AWS-Konto-Benutzer mit den meisten Berechtigungen. MFA bietet eine weitere Schutzebene zusätzlich zum Benutzernamen und Passwort. Indem Sie MFA für den Root-Benutzer vorschreiben, können Sie die Anzahl AWS-Konten kompromittierter Benutzer reduzieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0992	Legen Sie fest, wie die Ergebnisse der kontinuierlichen Überwachung bei der laufenden Genehmigung verwendet werden sollen.	secretsmanager-rotation-enabled-check	Diese Regel stellt sicher, dass bei AWS Secrets Manager Manager-Geheimnissen die Rotation aktiviert ist. Die regelmäßige Rotation von Secrets kann den Zeitraum verkürzen, in dem ein Secret aktiv ist, und möglicherweise die Auswirkungen auf das Unternehmen verringern, falls das Secret kompromittiert wird.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0993	Einrichtung von Verfahren und Verfahren zur kontinuierlichen Überwachung von Tools und Technologien für die Zugangskontrolle	iam-customer-policy-blocked-kms-Aktionen	AWS Identity and Access Management (IAM) kann Ihnen helfen, die Prinzipien der geringsten Rechte und der Aufgabentrennung in Zugriffsberechtigungen und Autorisierungen zu integrieren und so zu verhindern, dass Richtlinien blockierte Aktionen für alle AWS Schlüssel des Key Management Service enthalten. Wenn Benutzer mehr Rechte haben, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und Aufgabentrennung verstoßen. Mit dieser Regel können Sie den Parameter festlegen. blockedActionsPatterns (Wert „AWS Bewährte grundlegende Sicherheitsmethoden“: kms:

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			Decrypt, kms:ReEncryptFrom). Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.
T0993	Einrichtung von Verfahren und Verfahren zur kontinuierlichen Überwachung von Tools und Technologien für die Zugangskontrolle	iam-group-has-users-überprüfen	AWS Identity and Access Management (IAM) kann Ihnen helfen, die Prinzipien der geringsten Rechte und der Aufgabentrennung mit Zugriffsberechtigungen und Autorisierungen zu integrieren, indem sichergestellt wird, dass IAM-Gruppen mindestens einen Benutzer haben. Die Einteilung von Benutzern in Gruppen auf der Grundlage der ihnen zugewiesenen Berechtigungen oder ihrer Funktion ist eine Möglichkeit, das Prinzip der geringsten Berechtigung zu implementieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0993	Einrichtung von Verfahren und Verfahren zur kontinuierlichen Überwachung von Tools und Technologien für die Zugangskontrolle	iam-inline-policy-blocked-kms-Aktionen	Stellen Sie sicher, dass ein Benutzer, eine IAM-Rolle oder eine IAM-Gruppe (AWS Identity and Access Management) nicht über eine Inline-Richtlinie verfügt, die blockierte Aktionen für alle AWS Schlüssel des Key Management Service zulässt. AWS empfiehlt, verwaltete Richtlinien anstelle von Inline-Richtlinien zu verwenden. Verwaltete Richtlinien ermöglichen Wiederverwendbarkeit, Versionsverwaltung, Rollback und Delegierung der Berechtigungsverwaltung. Mit dieser Regel können Sie den blockedActionsPatterns Parameter festlegen. (Wert „AWS Bewährte grundlegende Sicherheitsmethoden“: kms:Decrypt, kms:ReEncryptFrom). Die

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.
T0993	Einrichtung von Verfahren und Verfahren zur kontinuierlichen Überwachung von Tools und Technologien für die Zugangskontrolle	iam-no-inline-policy-überprüfen	Stellen Sie sicher, dass ein Benutzer, eine IAM-Rolle oder eine IAM-Gruppe (AWS Identity and Access Management) nicht über eine Inline-Richtlinie zur Zugriffskontrolle auf Systeme und Ressourcen verfügt. AWS empfiehlt, verwaltete Richtlinien anstelle von Inline-Richtlinien zu verwenden. Verwaltete Richtlinien ermöglichen Wiederverwendbarkeit, Versionsverwaltung, Rollback und Delegierung der Berechtigungsverwaltung.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0993	Einrichtung von Verfahren und Verfahren zur kontinuierlichen Überwachung von Tools und Technologien für die Zugangskontrolle	iam-password-policy	Die Identitäten und Anmeldeinformationen werden auf der Grundlage einer organisatorischen IAM-Passwortrichtlinie ausgestellt, verwaltet und verifiziert. Sie erfüllen oder übertreffen die Anforderungen von NIST SP 800-63 und dem Standard „Best Practices“ von AWS Foundational Security für die Passwortstärke. Mit dieser Regel können Sie optional RequireUppercaseCharacters (Wert für AWS grundlegende Sicherheitsbewährte Methoden: wahr), RequireLowercaseCharacters (Wert für bewährte Methoden für AWS grundlegende Sicherheit: wahr), RequireSymbols (Wert für bewährte Methoden für AWS grundlegende Sicherheit:

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			wahr), RequireNumbers (Wert für bewährte Methoden für AWS grundlegende Sicherheit: wahr), MinimumPasswordLength (Wert für bewährte Methoden für AWS grundlegende Sicherheit: 14), PasswordReusePrevention (Wert für bewährte Methoden für AWS grundlegende Sicherheit: 24) und MaxPasswordAge (Wert für bewährte Methoden für AWS grundlegende Sicherheit: 90) für Ihr IAM festlegen Kennwortrichtlinie. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0993	Einrichtung von Verfahren und Verfahren zur kontinuierlichen Überwachung von Tools und Technologien für die Zugangskontrolle	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) kann Ihnen dabei helfen, die Prinzipien der geringsten Rechte und der Aufgabentrennung in Zugriffsberechtigungen und Autorisierungen zu integrieren und so zu verhindern, dass Richtlinien „Effect“: „Allow“ mit „Action“: „*“ anstelle von „Resource“: „*“ enthalten. Wenn Benutzern mehr Rechte eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und der Aufgabentrennung verstoßen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0993	Einrichtung von Verfahren und Verfahren zur kontinuierlichen Überwachung von Tools und Technologien für die Zugangskontrolle	iam-policy-no-statements-with-full-access	Stellen Sie sicher, dass IAM-Aktionen nur auf die benötigten Aktionen beschränkt sind. Wenn Benutzern mehr Rechte eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Rechte und der Aufgabentrennung verstoßen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0993	Einrichtung von Verfahren und Verfahren zur kontinuierlichen Überwachung von Tools und Technologien für die Zugangskontrolle	iam-root-access-key-überprüfen	Der Zugriff auf Systeme und Ressourcen kann gesteuert werden, indem überprüft wird, ob der Root-Benutzer keine Zugriffsschlüssel mit seiner AWS Identity and Access Management (IAM) -Rolle verknüpft hat. Stellen Sie sicher, dass die Root-Zugriffsschlüssel gelöscht werden. Erstellen und verwenden Sie stattdessen rollenbasierte Funktionen, AWS-Konten um das Prinzip der geringsten Funktionalität zu berücksichtigen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0993	Einrichtung von Verfahren und Verfahren zur kontinuierlichen Überwachung von Tools und Technologien für die Zugangskontrolle	iam-user-group-membership-überprüfen	AWS Identity and Access Management (IAM) kann Ihnen helfen, Zugriffsberechtigungen und Autorisierungen einzuschränken, indem sichergestellt wird, dass Benutzer Mitglieder mindestens einer Gruppe sind. Wenn Benutzern mehr Berechtigungen eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und Aufgabentrennung verstoßen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0993	Einrichtung von Verfahren und Verfahren zur kontinuierlichen Überwachung von Tools und Technologien für die Zugangskontrolle	iam-user-no-policies-überprüfen	Diese Regel stellt sicher, dass AWS Identity and Access Management (IAM) -Richtlinien nur Gruppen oder Rollen zugewiesen werden, um den Zugriff auf Systeme und Ressourcen zu kontrollieren. Die Zuweisung von Berechtigungen auf Gruppen- oder Rollenebene trägt dazu bei, die Wahrscheinlichkeit zu verringern, dass eine Identität übermäßige Berechtigungen erhält oder beibehält.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0993	Einrichtung von Verfahren und Verfahren zur kontinuierlichen Überwachung von Tools und Technologien für die Zugangskontrolle	iam-user-unused-credentials-überprüfen	AWS Identity and Access Management (IAM) kann Ihnen bei Zugriffsberechtigungen und Autorisierungen helfen, indem es nach IAM-Passwörtern und Zugriffsschlüsseln sucht, die für einen bestimmten Zeitraum nicht verwendet wurden. Wenn ungenutzte Anmeldeinformationen identifiziert werden, müssen Sie sie deaktivieren und/oder entfernen, da dies gegen das Prinzip der geringsten Berechtigung verstoßen könnte. Für diese Regel müssen Sie einen Wert für das maxCredentialUsage Alter festlegen (Standardkonfiguration: 90). Der tatsächliche Wert muss den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0993	Einrichtung von Verfahren und Verfahren zur kontinuierlichen Überwachung von Tools und Technologien für die Zugangskontrolle	mfa-enabled-for-iam-Konsolenzugriff	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass MFA für alle AWS Identity and Access Management (IAM) -Benutzer aktiviert ist, die über ein Konsolenkennwort verfügen. MFA sorgt für eine weitere Schutzebene zusätzlich zu den Anmeldeinformationen. Indem Sie MFA für Benutzer vorschreiben, können Sie Fälle kompromittierter Konten reduzieren und verhindern, dass unbefugte Benutzer auf vertrauliche Daten zugreifen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0993	Einrichtung von Verfahren und Verfahren zur kontinuierlichen Überwachung von Tools und Technologien für die Zugangskontrolle	iam-user-mfa-enabled	Aktivieren Sie diese Regel, um den Zugriff auf Ressourcen in der AWS -Cloud einzuschränken. Diese Regel stellt sicher, dass die Multi-Faktor-Authentifizierung (MFA) für alle Benutzer aktiviert ist. MFA bietet eine weitere Schutzebene zusätzlich zum Benutzernamen und Passwort. Reduzieren Sie Fälle von kompromittierten Konten, indem Sie MFA für Benutzer vorschreiben.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0993	Einrichtung von Verfahren und Verfahren zur kontinuierlichen Überwachung von Tools und Technologien für die Zugangskontrolle	root-account-hardware-mfa-aktiviert	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Hardware-MFA für den Root-Benutzer aktiviert ist. Der Stammbenutzer ist der AWS-Konto-Benutzer mit den meisten Berechtigungen. MFA sorgt für eine weitere Schutzebene zusätzlich zu den Anmeldeinformationen. Indem Sie MFA für den Root-Benutzer vorschreiben, können Sie die Anzahl AWS-Konten kompromittierter Benutzer reduzieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
T0993	Einrichtung von Verfahren und Verfahren zur kontinuierlichen Überwachung von Tools und Technologien für die Zugangskontrolle	root-account-mfa-enabled	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass MFA für den Root-Benutzer aktiviert ist. Der Stammbenutzer ist der AWS-Konto-Benutzer mit den meisten Berechtigungen. MFA bietet eine weitere Schutzebene zusätzlich zum Benutzernamen und Passwort. Indem Sie MFA für den Root-Benutzer vorschreiben, können Sie die Anzahl AWS-Konten kompromittierter Benutzer reduzieren.

Vorlage

Die Vorlage ist verfügbar unter GitHub: Operational Best Practices for NIST 800 181.

Bewährte Methoden für die Ausführung von NIST 1800 25

Konformitätspakete bieten ein allgemeines Compliance-Framework, das es Ihnen ermöglicht, mithilfe verwalteter oder benutzerdefinierter AWS Config Regeln und Abhilfemaßnahmen Kontrollen zur Sicherheits-, Betriebs- oder Kostenoptimierung durchzuführen. AWS Config Conformance Packs dienen als Beispielvorlagen nicht dazu, die vollständige Einhaltung eines bestimmten Governance-

oder Compliance-Standards sicherzustellen. Sie sind dafür verantwortlich, selbst zu beurteilen, ob Ihre Nutzung der Services den geltenden gesetzlichen und behördlichen Anforderungen entspricht.

Im Folgenden finden Sie ein Beispiel für eine Zuordnung zwischen NIST 1800-25 und AWS verwalteten Konfigurationsregeln. Jede AWS Config bezieht sich auf eine bestimmte AWS Ressource und bezieht sich auf eine oder mehrere NIST 1800-25-Steuerelemente. Ein NIST 1800-25-Steuerelement kann sich auf mehrere Regeln beziehen. AWS Config In der folgenden Tabelle finden Sie weitere Informationen und Anleitungen zu diesen Zuordnungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
ID.AM-2	Softwareplattformen und Anwendungen innerhalb der Organisation werden inventarisiert	ec2-managerinstance-managed-by-systems	Eine Bestandsaufnahme der Softwareplattformen und Anwendungen innerhalb des Unternehmens ist möglich, indem Amazon Elastic Compute Cloud (Amazon EC2) - Instances mit AWS Systems Manager verwaltet werden. Verwenden Sie AWS Systems Manager, um detaillierte Systemkonfigurationen, Betriebssystem-Patch-Levels, Namen und Typ der Dienste, Softwareinstallationen, Anwendungsname, Herausgeber und Version sowie andere Details zu

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			Ihrer Umgebung bereitzustellen.
ID.AM-2	Softwareplattformen und Anwendungen innerhalb der Organisation werden inventarisiert	ec2-check managedinstance-association-compliance-status	Verwenden Sie AWS Systems Manager Associations, um bei der Inventarisierung von Softwareplattformen und Anwendungen innerhalb eines Unternehmens zu helfen. AWS Systems Manager weist Ihren verwalteten Instances einen Konfigurationsstatus zu und ermöglicht es Ihnen, Basiswerte für Betriebssystem-Patch-Levels, Softwareinstallationen, Anwendungskonfigurationen und andere Details zu Ihrer Umgebung festzulegen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
ID.AM-2	Softwareplattformen und Anwendungen innerhalb der Organisation werden inventarisiert	ec2-stopped-instance	Aktivieren Sie diese Regel, um bei der Basiskonfiguration von Amazon Elastic Compute Cloud (Amazon EC2) - Instances zu helfen, indem Sie überprüfen, ob EC2 Amazon-Instances gemäß den Standards Ihrer Organisation für mehr als die zulässige Anzahl von Tagen gestoppt wurden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
ID.AM-2	Softwareplattformen und Anwendungen innerhalb der Organisation werden inventarisiert	eip-attached	Diese Regel stellt sicher, dass Elastic, die einer Amazon Virtual Private Cloud (Amazon VPC) IPs zugewiesen sind, an Amazon Elastic Compute Cloud (Amazon EC2) - Instances oder verwendete Elastic Network Interfaces angehängt sind. Diese Regel hilft bei der Überwachung ungenutzter Inhalte EIPs in Ihrer Umgebung.
ID.AM-2	Softwareplattformen und Anwendungen innerhalb der Organisation werden inventarisiert	vpc-network-acl-unused-überprüfen	Diese Regel stellt sicher, dass Amazon Virtual Private Cloud (VPC)-Netzwerkzugriffskontrolllisten verwendet werden. Die Überwachung ungenutzter Netzwerk-Zugriffskontrolllisten kann zu einer genauen Inventarisierung und Verwaltung Ihrer Umgebung beitragen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
ID.RA-1	Sicherheitslücken in Vermögenswerten werden identifiziert und dokumentiert	rds-automatic-minor-version-Upgrade aktiviert	Aktivieren Sie automatische Unterversions-Upgrades auf Ihren Amazon-Relational-Database-Service-(RDS-)-Instances, um sicherzustellen, dass die aktuellen Updates für Unterversionen des Relational Database Management System (RDBMS) installiert sind, die Sicherheitspatches und Bugfixes enthalten können.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
ID.RA-1	Sicherheitslücken in Vermögenswerten werden identifiziert und dokumentiert	ec2- prüfen managedinstance-patch-compliance-status	Aktivieren Sie diese Regel, um bei der Identifizierung und Dokumentation von Sicherheitslücken in Amazon Elastic Compute Cloud (Amazon EC2) zu helfen. Die Regel prüft, ob die EC2 Amazon-Instance die Patch-Konformität im AWS Systems Manager gemäß den Richtlinien und Verfahren Ihrer Organisation einhält.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
ID.RA-1	Sicherheitslücken in Vermögenswerten werden identifiziert und dokumentiert	elastic-beanstalk-managed-updates-aktiviert	Durch die Aktivierung verwalteter Plattform updates für eine Amazon-Elastic-Beanstalk-Umgebung wird sichergestellt, dass die aktuellen verfügbaren Plattform -Fixes, -Updates und -Features für die Umgebung installiert sind. Eine bewährte Methode zur Sicherung von Systemen besteht darin, stets die aktuellen Patches zu installieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
ID.RA-1	Sicherheitslücken in Vermögenswerten werden identifiziert und dokumentiert	guardduty-enabled-centralized	Amazon GuardDuty kann mithilfe von Threat Intellige nce Feeds helfen, potenzielle Cybersich erheitsereignisse zu überwachen und zu erkennen. Dazu gehören Listen mit bösartigen IPs und maschinel len Lernmethoden zur Identifizierung unerwarteter, nicht autorisierter und bösartiger Aktivitäten in Ihrer AWS Cloud-Umgebung.
PR.AC-1	Identitäten und Anmeldeinformation en werden für autorisierte Geräte, Benutzer und Prozesse ausgestellt, verwaltet, verifiziert, gesperrt und geprüft	ec2- instance-profile-a ttached	EC2 Instanzprofile übergeben eine IAM-Rolle an eine EC2 Instance. Das Anhängen eines Instance-Profils an Ihre Instances kann bei der Implement ierung von geringste n Berechtigungen und der Berechtig ungsverwaltung helfen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.AC-1	Identitäten und Anmeldeinformationen werden für autorisierte Geräte, Benutzer und Prozesse ausgestellt, verwaltet, verifiziert, gesperrt und geprüft	ecs-task-definition-user-for-host-mode-check	Wenn für eine Aufgabendefinition erhöhte Berechtigungen gelten, liegt das daran, dass der Kunde diesen Konfigurationen ausdrücklich zugestimmt hat. Diese Kontrolle prüft, ob eine unerwartete Berechtigungseskalation vorliegt, wenn für eine Aufgabendefinition das Host-Netzwerk aktiviert ist, die Kunden aber keine erhöhten Berechtigungen aktiviert haben.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.AC-1	Identitäten und Anmeldeinformationen werden für autorisierte Geräte, Benutzer und Prozesse ausgestellt, verwaltet, verifiziert, gesperrt und geprüft	iam-no-inline-policy-überprüfen	Stellen Sie sicher, dass ein Benutzer, eine IAM-Rolle oder eine IAM-Gruppe (AWS Identity and Access Management) nicht über eine Inline-Richtlinie zur Zugriffskontrolle auf Systeme und Ressourcen verfügt. AWS empfiehlt, verwaltete Richtlinien anstelle von Inline-Richtlinien zu verwenden. Verwaltete Richtlinien ermöglichen Wiederverwendbarkeit, Versionsverwaltung, Rollback und Delegierung der Berechtigungsverwaltung.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.AC-1	Identitäten und Anmeldeinformationen werden für autorisierte Geräte, Benutzer und Prozesse ausgestellt, verwaltet, verifiziert, gesperrt und geprüft	iam-policy-no-statements-with-full-access	Stellen Sie sicher, dass IAM-Aktionen nur auf die benötigten Aktionen beschränkt sind. Wenn Benutzern mehr Rechte eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Rechte und der Aufgabentrennung verstoßen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.AC-1	Identitäten und Anmeldeinformationen werden für autorisierte Geräte, Benutzer und Prozesse ausgestellt, verwaltet, verifiziert, gesperrt und geprüft	access-keys-rotated	Die Anmeldeinformationen für autorisierte Geräte, Benutzer und Prozesse werden geprüft, indem sichergestellt wird, dass die IAM-Zugriffsschlüssel entsprechend den Vorgaben der Unternehmensrichtlinie rotiert werden. Das regelmäßige Ändern der Zugriffsschlüssel ist eine bewährte Sicherheitsmethode. Es verkürzt den Zeitraum, in dem ein Zugriffsschlüssel aktiv ist, und reduziert die Auswirkungen auf das Unternehmen, wenn die Schlüssel kompromittiert werden. Diese Regel erfordert einen Wert für die Zugriffsschlüssel-Rotation (Standardkonfiguration: 90). Der tatsächliche Wert muss den Richtlini

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			en Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.AC-1	Identitäten und Anmeldeinformationen werden für autorisierte Geräte, Benutzer und Prozesse ausgestellt, verwaltet, verifiziert, gesperrt und geprüft	emr-kerberos-enabled	Die Zugriffsberechtigungen und -autorisierungen können verwaltet und nach den Prinzipien der geringsten Berechtigung und Aufgabentrennung integriert werden, indem Kerberos für Amazon-EMR-Cluster aktiviert wird. In Kerberos werden Services und Benutzer, die sich authentifizieren müssen, als Prinzipale bezeichnet. Prinzipale befinden sich in einem Kerberos-Bereich. Innerhalb dieses Bereichs wird ein Kerberos-Server als Key Distribution Center (KDC) bezeichnet. Über diesen Server können sich Prinzipale authentifizieren. Die Authentifizierung im KDC erfolgt durch die Ausstellung von Authentif

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			izierungstickets. Das KDC unterhält eine Datenbank der Prinzipale in seinem Bereich mit ihren Passwörtern und anderen administr ativen Informationen zu jedem Prinzipal.
PR.AC-1	Identitäten und Anmeldeinformation en werden für autorisierte Geräte, Benutzer und Prozesse ausgestellt, verwaltet, verifiziert, gesperrt und geprüft	iam-group-has-users-überprüfen	AWS Identity and Access Managemen t (IAM) kann Ihnen helfen, die Prinzipien der geringsten Rechte und der Aufgabent rennung mit Zugriffsb erechtigungen und Autorisierungen zu integrieren, indem sichergestellt wird, dass IAM-Gruppen mindestens einen Benutzer haben. Die Einteilung von Benutzern in Gruppen auf der Grundlage der ihnen zugewiese nen Berechtigungen oder ihrer Funktion ist eine Möglichkeit, das Prinzip der geringste n Berechtigung zu implementieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.AC-1	Identitäten und Anmeldeinformationen werden für autorisierte Geräte, Benutzer und Prozesse ausgestellt, verwaltet, verifiziert, gesperrt und geprüft	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) kann Ihnen dabei helfen, die Prinzipien der geringsten Rechte und der Aufgabentrennung in Zugriffsberechtigungen und Autorisierungen zu integrieren und so zu verhindern, dass Richtlinien „Effect“: „Allow“ mit „Action“: „*“ anstelle von „Resource“: „*“ enthalten. Wenn Benutzern mehr Rechte eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und der Aufgabentrennung verstoßen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.AC-1	Identitäten und Anmeldeinformationen werden für autorisierte Geräte, Benutzer und Prozesse ausgestellt, verwaltet, verifiziert, gesperrt und geprüft	iam-root-access-key-überprüfen	Der Zugriff auf Systeme und Ressourcen kann gesteuert werden, indem überprüft wird, ob der Root-Benutzer keine Zugriffsschlüssel mit seiner AWS Identity and Access Management (IAM) -Rolle verknüpft hat. Stellen Sie sicher, dass die Root-Zugriffsschlüssel gelöscht werden. Erstellen und verwenden Sie stattdessen rollenbasierte Funktionen, AWS-Konten um das Prinzip der geringsten Funktionalität zu berücksichtigen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.AC-1	Identitäten und Anmeldeinformationen werden für autorisierte Geräte, Benutzer und Prozesse ausgestellt, verwaltet, verifiziert, gesperrt und geprüft	iam-user-mfa-enabled	Aktivieren Sie diese Regel, um den Zugriff auf Ressourcen in der AWS -Cloud einzuschränken. Diese Regel stellt sicher, dass die Multi-Faktor-Authentifizierung (MFA) für alle Benutzer aktiviert ist. MFA bietet eine weitere Schutzebene zusätzlich zum Benutzernamen und Passwort. Reduzieren Sie Fälle von kompromittierten Konten, indem Sie MFA für Benutzer vorschreiben.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.AC-1	Identitäten und Anmeldeinformationen werden für autorisierte Geräte, Benutzer und Prozesse ausgestellt, verwaltet, verifiziert, gesperrt und geprüft	iam-user-no-policies-überprüfen	Diese Regel stellt sicher, dass AWS Identity and Access Management (IAM) -Richtlinien nur Gruppen oder Rollen zugewiesen werden, um den Zugriff auf Systeme und Ressourcen zu kontrollieren. Die Zuweisung von Berechtigungen auf Gruppen- oder Rollenebene trägt dazu bei, die Wahrscheinlichkeit zu verringern, dass eine Identität übermäßige Berechtigungen erhält oder beibehält.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.AC-1	Identitäten und Anmeldeinformationen werden für autorisierte Geräte, Benutzer und Prozesse ausgestellt, verwaltet, verifiziert, gesperrt und geprüft	iam-user-unused-credentials-überprüfen	AWS Identity and Access Management (IAM) kann Ihnen bei Zugriffsberechtigungen und Autorisierungen helfen, indem es nach IAM-Passwörtern und Zugriffsschlüsseln sucht, die für einen bestimmten Zeitraum nicht verwendet wurden. Wenn ungenutzte Anmeldeinformationen identifiziert werden, müssen Sie sie deaktivieren und/oder entfernen, da dies gegen das Prinzip der geringsten Berechtigung verstoßen könnte. Für diese Regel müssen Sie einen Wert für das maxCredentialUsage Alter festlegen (Standardkonfiguration: 90). Der tatsächliche Wert muss den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.AC-1	Identitäten und Anmeldeinformationen werden für autorisierte Geräte, Benutzer und Prozesse ausgestellt, verwaltet, verifiziert, gesperrt und geprüft	secretsmanager-rotation-enabled-check	Diese Regel stellt sicher, dass bei AWS Secrets Manager Manager-Geheimnissen die Rotation aktiviert ist. Die regelmäßige Rotation von Secrets kann den Zeitraum verkürzen, in dem ein Secret aktiv ist, und möglicherweise die Auswirkungen auf das Unternehmen verringern, falls das Secret kompromittiert wird.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.AC-3	Der Fernzugriff wird verwaltet.	autoscaling-launch-config-public-ip-deaktiviert	Wenn Sie Ihre Netzwerkschnittstellen mit einer öffentlichen IP-Adresse konfigurieren, sind die diesen Netzwerkschnittstellen zugehörigen Ressourcen über das Internet erreichbar. EC2 Ressourcen sollten nicht öffentlich zugänglich sein, da dies einen unbeabsichtigten Zugriff auf Ihre Anwendungen oder Server ermöglichen kann.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.AC-3	Der Fernzugriff wird verwaltet.	ec2- instances-in-vpc	Stellen Sie Amazon Elastic Compute Cloud (Amazon EC2) -Instances innerhalb einer Amazon Virtual Private Cloud (Amazon VPC) bereit, um eine sichere Kommunika tion zwischen einer Instance und anderen Services innerhalb der Amazon VPC zu ermöglichen, ohne dass ein Internet-Gateway, ein NAT-Gerät oder eine VPN-Verbindung erforderlich ist. Der gesamte Datenverk ehr bleibt sicher in der AWS Cloud. Domains, die sich innerhalb einer VPC befinden, verfügen aufgrund ihrer logischen Isolierun g im Vergleich zu Domains mit öffentlic hen Endpunkten über eine zusätzlic he Sicherheitsebene. Weisen Sie EC2

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			Amazon-Instances einer Amazon-VPC zu, um den Zugriff ordnungsgemäß zu verwalten.
PR.AC-3	Der Fernzugriff wird verwaltet.	no-unrestricted-route-to-igw	Stellen Sie sicher, dass EC2 Amazon-Routentabellen keine uneingeschränkten Routen zu einem Internet-Gateway enthalten. Durch das Entfernen oder Beschränken des Internetzugangs für Workloads innerhalb von Amazon VPCs können unbeabsic htigte Zugriffe in Ihrer Umgebung reduziert werden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.AC-3	Der Fernzugriff wird verwaltet.	redshift-enhanced-vpc-routing-aktiviert	Mit Enhanced-VPC-Routing wird erzwungen, dass der gesamte COPY- und UNLOAD-Datenverkehr zwischen Ihrem Cluster und Datenrepositorys über Ihre Amazon VPC erfolgt. Anschließend können Sie VPC-Features wie Sicherheitsgruppen und Netzwerkzugriffskontrolllisten verwenden, um den Netzwerkverkehr zu schützen. Sie können auch VPC-Flow-Logs verwenden, um den Netzwerkverkehr zu überwachen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.AC-3	Der Fernzugriff wird verwaltet.	ssm-document-not-public	Stellen Sie sicher, dass AWS Systems Manager (SSM) - Dokumente nicht öffentlich sind, da dies einen unbeabsichtigten Zugriff auf Ihre SSM-Dokumente ermöglichen kann. Ein öffentliches SSM-Dokument kann Informationen über Ihr Konto, Ihre Ressourcen und internen Prozesse preisgeben.
PR.AC-3	Der Fernzugriff wird verwaltet.	dms-replication-not-public	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass auf DMS-Replikationsinstanzen nicht öffentlich zugegriffen werden kann. DMS-Replikations-Instances können vertrauliche Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.AC-3	Der Fernzugriff wird verwaltet.	ebs-snapshot-public-restorable-überprüfen	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass EBS-Snapshots nicht öffentlich wiederher stellbar sind. EBS-Volume-Snapsho ts können vertrauli che Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.
PR.AC-3	Der Fernzugriff wird verwaltet.	ec-2 instance-no-public-ip	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon Elastic Compute Cloud (Amazon EC2) - Instances nicht öffentlich zugänglic h sind. EC2Amazon -Instances können vertrauliche Informati onen enthalten, und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.AC-3	Der Fernzugriff wird verwaltet.	elasticsearch-in-vpc-only	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass sich Amazon OpenSearch OpenSearch Service (Service) - Domains innerhalb einer Amazon Virtual Private Cloud (Amazon VPC) befinden. Eine OpenSearch Service-Domain innerhalb einer Amazon VPC ermöglicht die sichere Kommunikation zwischen OpenSearch Service und anderen Services innerhalb der Amazon VPC, ohne dass ein Internet-Gateway, ein NAT-Gerät oder eine VPN-Verbindung erforderlich ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.AC-3	Der Fernzugriff wird verwaltet.	emr-master-no-public-ip	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon EMR-Cluster-Masterknoten nicht öffentlich zugänglich sind. Amazon-EMR-Cluster-Hauptknoten können vertrauliche Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.AC-3	Der Fernzugriff wird verwaltet.	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) Security Groups können bei der Verwaltung des Netzwerkzugriffs helfen, indem sie eine statusbeh aftete Filterung von eingehendem und ausgehendem Netzwerkverkehr zu Ressourcen bereitste llen. AWS Wenn Sie eingehenden (oder entfernten) Datenverk ehr von 0.0.0.0/0 bis Port 22 auf Ihren Ressourcen nicht zulassen, können Sie den Remote-Zugriff einschränken.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.AC-3	Der Fernzugriff wird verwaltet.	lambda-function-public-access-verboten	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass AWS Lambda-Funktionen nicht öffentlich zugänglich sind. Der öffentliche Zugriff kann möglicherweise die Verfügbarkeit von Ressourcen beeinträchtigen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.AC-3	Der Fernzugriff wird verwaltet.	lambda-inside-vpc	Stellen Sie AWS Lambda-Funktionen in einer Amazon Virtual Private Cloud (Amazon VPC) bereit, um eine sichere Kommunika tion zwischen einer Funktion und anderen Diensten innerhalb der Amazon VPC zu gewährleisten. Bei dieser Konfiguration sind kein Internet-Gateway, kein NAT-Gerät und keine VPN-Verbindung erforderlich. Der gesamte Datenverk ehr bleibt sicher in der Cloud. AWS Domains, die sich innerhalb einer VPC befinden, verfügen aufgrund ihrer logischen Isolierun g im Vergleich zu Domains mit öffentlic hen Endpunkten über eine zusätzliche Sicherheitsebene. Um den Zugriff ordnungsg emäß zu verwalten,

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			sollten AWS Lambda-Funktionen einer VPC zugewiesen werden.
PR.AC-3	Der Fernzugriff wird verwaltet.	opensearch-in-vpc-only	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass sich Amazon OpenSearch Service-Domains innerhalb einer Amazon Virtual Private Cloud (Amazon VPC) befinden. Eine Amazon OpenSearch Service-Domain innerhalb einer Amazon VPC ermöglicht die sichere Kommunikation zwischen Amazon OpenSearch Service und anderen Services innerhalb der Amazon VPC, ohne dass ein Internet-Gateway, ein NAT-Gerät oder eine VPN-Verbindung erforderlich ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.AC-3	Der Fernzugriff wird verwaltet.	rds-instance-public-access-überprüfen	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Relational Database Service (Amazon RDS) -Instances nicht öffentlich sind. Amazon-RDS-Datenbank-Instances können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.AC-3	Der Fernzugriff wird verwaltet.	rds-snapshots-public-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Relational Database Service (Amazon RDS) -Instances nicht öffentlich sind. Amazon-RDS-Datenbank-Instances können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.AC-3	Der Fernzugriff wird verwaltet.	redshift-cluster-public-access-überprüfen	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Redshift Redshift-Cluster nicht öffentlich sind. Amazon-Redshift-Cluster können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.AC-3	Der Fernzugriff wird verwaltet.	restricted-common-ports	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass gemeinsame Ports für Amazon Elastic Compute Cloud (Amazon EC2) -Sicherheitsgruppen eingeschränkt sind. Wenn der Zugriff auf Ports nicht auf vertrauenswürdige Quellen beschränkt wird, kann dies zu Angriffen auf die Verfügbarkeit, Integrität und Vertraulichkeit von Systemen führen. Mit dieser Regel können Sie optional die Parameter blockedPort1–blockedPort5 festlegen (Standardkonfigurationen: 20, 21, 3389, 3306, 4333). Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.AC-3	Der Fernzugriff wird verwaltet.	s3- account-level-public-access -Block-periodisch	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Simple Storage Service (Amazon S3) -Buckets nicht öffentlich zugänglich sind. Diese Regel trägt dazu bei, sensible Daten vor unbefugten Remote-Benutzern zu schützen, indem sie den öffentlichen Zugriff verhindert. Mit dieser Regel können Sie optional die Parameter ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) und restrictPublicBuckets Parameter (Config Default: True) festlegen. Die tatsächlichen Werte müssen den Richtlini

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			en Ihrer Organisation entsprechen.
PR.AC-3	Der Fernzugriff wird verwaltet.	s3 bucket-level-public-access - verboten	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Simple Storage Service (Amazon S3) -Buckets nicht öffentlich zugänglich sind. Diese Regel trägt dazu bei, sensible Daten vor unbefugten Remote-Benutzern zu schützen, indem sie den öffentlichen Zugriff auf Bucket-Ebene verhindert.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.AC-3	Der Fernzugriff wird verwaltet.	s-3 bucket-public-read -prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie nur autorisierten Benutzern, Prozessen und Geräten Zugriff auf Amazon Simple Storage Service (Amazon S3) - Buckets gewähren. Die Verwaltung des Zugriffs sollte mit der Klassifizierung der Daten übereinst immen.
PR.AC-3	Der Fernzugriff wird verwaltet.	s3- bucket-public-writ e-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie nur autorisierten Benutzern, Prozessen und Geräten Zugriff auf Amazon Simple Storage Service (Amazon S3) - Buckets gewähren. Die Verwaltung des Zugriffs sollte mit der Klassifizierung der Daten übereinst immen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.AC-3	Der Fernzugriff wird verwaltet.	sagemaker-notebook-no-direct-Internetzugang	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass SageMaker Amazon-Notebooks keinen direkten Internetzugang zulassen. Indem Sie direkten Internetzugang blockieren, vermeiden Sie, dass unbefugte Benutzer auf sensible Daten zugreifen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.AC-3	Der Fernzugriff wird verwaltet.	subnet-auto-assign-public-ip-deaktiviert	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon Virtual Private Cloud (VPC) -Subnetzen nicht automatisch eine öffentliche IP-Adresse zugewiesen wird. Amazon Elastic Compute Cloud (EC2) -Instances, die in Subnetzen gestartet werden, in denen dieses Attribut aktiviert ist, haben ihrer primären Netzwerkschnittstelle eine öffentliche IP-Adresse zugewiesen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.AC-3	Der Fernzugriff wird verwaltet.	vpc-default-security-group-geschlossen	Sicherheitsgruppen von Amazon Elastic Compute Cloud (Amazon EC2) können bei der Verwaltung des Netzwerkzugriffs helfen, indem sie eine statusbehaftete Filterung des ein- und ausgehenden Netzwerkverkehrs zu Ressourcen bereitstellen. AWS Die Beschränk ung des gesamten Datenverkehrs auf die Standardsicherheit sgruppe hilft dabei, den Fernzugriff auf Ihre Ressourcen einzuschränken. AWS

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.AC-3	Der Fernzugriff wird verwaltet.	vpc-sg-open-only-to-authorized-ports	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass gemeinsame Ports für Amazon Elastic Compute Cloud (Amazon EC2) -Sicherheitsgruppen eingeschränkt sind. Wenn der Zugriff auf Ports nicht auf vertrauenswürdige Quellen beschränkt wird, kann dies zu Angriffen auf die Verfügbarkeit, Integrität und Vertraulichkeit von Systemen führen. Durch die Beschränkung des Zugriffs auf Ressourcen innerhalb einer Sicherheitsgruppe aus dem Internet (0.0.0.0/0) kann der Fernzugriff auf interne Systeme gesteuert werden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.AC-4	Zugriffsberechtigungen und Autorisierungen werden nach den Grundsätzen der geringsten Rechte und der Aufgabentrennung verwaltet	autoscaling-launch-config-public-ip-deaktiviert	Wenn Sie Ihre Netzwerkschnittstellen mit einer öffentlichen IP-Adresse konfigurieren, sind die diesen Netzwerkschnittstellen zugehörigen Ressourcen über das Internet erreichbar. EC2 Ressourcen sollten nicht öffentlich zugänglich sein, da dies einen unbeabsichtigten Zugriff auf Ihre Anwendungen oder Server ermöglichen kann.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.AC-4	Zugriffsberechtigungen und Autorisierungen werden nach den Grundsätzen der geringsten Rechte und der Aufgabentrennung verwaltet	ec2-imdsv2-check	Stellen Sie sicher, dass die Methode Instance Metadata Service Version 2 (IMDSv2) aktiviert ist, um den Zugriff auf und die Kontrolle der Amazon Elastic Compute Cloud (Amazon EC2) - Instance-Metadaten zu schützen. Die IMDSv2 Methode verwendet sitzungsbasierte Kontrollen. Mit können Kontrollen implementiert werden IMDSv2, um Änderungen an Instanzmetadaten einzuschränken.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.AC-4	Zugriffsberechtigungen und Autorisierungen werden nach den Grundsätzen der geringsten Rechte und der Aufgabentrennung verwaltet	ec-2 instance-profile-attached	EC2 Instanzprofile übergeben eine IAM-Rolle an eine EC2 Instance. Das Anhängen eines Instance-Profils an Ihre Instances kann bei der Implementierung von geringsten Berechtigungen und der Berechtigungsverwaltung helfen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.AC-4	Zugriffsberechtigungen und Autorisierungen werden nach den Grundsätzen der geringsten Rechte und der Aufgabentrennung verwaltet	ecs-task-definition-user-for-host-mode-check	Wenn für eine Aufgabendefinition erhöhte Berechtigungen gelten, liegt das daran, dass der Kunde diesen Konfigurationen ausdrücklich zugestimmt hat. Diese Kontrolle prüft, ob eine unerwartete Berechtigungseskalation vorliegt, wenn für eine Aufgabendefinition das Host-Netzwerk aktiviert ist, die Kunden aber keine erhöhten Berechtigungen aktiviert haben.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.AC-4	Zugriffsberechtigungen und Autorisierungen werden nach den Grundsätzen der geringsten Rechte und der Aufgabentrennung verwaltet	iam-no-inline-policy-überprüfen	Stellen Sie sicher, dass ein Benutzer, eine IAM-Rolle oder eine IAM-Gruppe (AWS Identity and Access Management) nicht über eine Inline-Richtlinie zur Zugriffskontrolle auf Systeme und Ressourcen verfügt. AWS empfiehlt, verwaltete Richtlinien anstelle von Inline-Richtlinien zu verwenden. Verwaltete Richtlinien ermöglichen Wiederverwendbarkeit, Versionsverwaltung, Rollback und Delegierung der Berechtigungsverwaltung.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.AC-4	Zugriffsberechtigungen und Autorisierungen werden nach den Grundsätzen der geringsten Rechte und der Aufgabentrennung verwaltet	iam-policy-no-statements-with-full-access	Stellen Sie sicher, dass IAM-Aktionen nur auf die benötigten Aktionen beschränkt sind. Wenn Benutzern mehr Rechte eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Rechte und der Aufgabentrennung verstoßen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.AC-4	Zugriffsberechtigungen und Autorisierungen werden nach den Grundsätzen der geringsten Rechte und der Aufgabentrennung verwaltet	ec-2 instances-in-vpc	Stellen Sie Amazon Elastic Compute Cloud (Amazon EC2) -Instances innerhalb einer Amazon Virtual Private Cloud (Amazon VPC) bereit, um eine sichere Kommunikation zwischen einer Instance und anderen Services innerhalb der Amazon VPC zu ermöglichen, ohne dass ein Internet-Gateway, ein NAT-Gerät oder eine VPN-Verbindung erforderlich ist. Der gesamte Datenverkehr bleibt sicher in der AWS Cloud. Domains, die sich innerhalb einer VPC befinden, verfügen aufgrund ihrer logischen Isolierung im Vergleich zu Domains mit öffentlichen Endpunkten über eine zusätzliche Sicherheitsebene. Weisen Sie EC2

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			Amazon-Instances einer Amazon-VPC zu, um den Zugriff ordnungsgemäß zu verwalten.
PR.AC-4	Zugriffsberechtigungen und Autorisierungen werden nach den Grundsätzen der geringsten Rechte und der Aufgabentrennung verwaltet	ssm-document-not-public	Stellen Sie sicher, dass AWS Systems Manager (SSM) - Dokumente nicht öffentlich sind, da dies einen unbeabsichtigten Zugriff auf Ihre SSM-Dokumente ermöglichen kann. Ein öffentliches SSM-Dokument kann Informationen über Ihr Konto, Ihre Ressourcen und internen Prozesse preisgeben.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.AC-4	Zugriffsberechtigungen und Autorisierungen werden nach den Grundsätzen der geringsten Rechte und der Aufgabentrennung verwaltet	dms-replication-not-public	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass auf DMS-Replikationsinstanzen nicht öffentlich zugegriffen werden kann. DMS-Replikations-Instances können vertrauliche Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.
PR.AC-4	Zugriffsberechtigungen und Autorisierungen werden nach den Grundsätzen der geringsten Rechte und der Aufgabentrennung verwaltet	ebs-snapshot-public-restorable-überprüfen	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass EBS-Snapshots nicht öffentlich wiederherstellbar sind. EBS-Volume-Snapshots können vertrauliche Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.AC-4	Zugriffsberechtigungen und Autorisierungen werden nach den Grundsätzen der geringsten Rechte und der Aufgabentrennung verwaltet	ec-2 instance-no-public-ip	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon Elastic Compute Cloud (Amazon EC2) - Instances nicht öffentlich zugänglich sind. EC2Amazon -Instances können vertrauliche Informationen enthalten, und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.AC-4	Zugriffsberechtigungen und Autorisierungen werden nach den Grundsätzen der geringsten Rechte und der Aufgabentrennung verwaltet	elasticsearch-in-vpc-only	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass sich Amazon OpenSearch OpenSearch Service (Service) - Domains innerhalb einer Amazon Virtual Private Cloud (Amazon VPC) befinden. Eine OpenSearch Service-Domain innerhalb einer Amazon VPC ermöglicht die sichere Kommunikation zwischen OpenSearch Service und anderen Services innerhalb der Amazon VPC, ohne dass ein Internet-Gateway, ein NAT-Gerät oder eine VPN-Verbindung erforderlich ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.AC-4	Zugriffsberechtigungen und Autorisierungen werden nach den Grundsätzen der geringsten Rechte und der Aufgabentrennung verwaltet	emr-kerberos-enabled	Die Zugriffsberechtigungen und -autorisierungen können verwaltet und nach den Prinzipien der geringsten Berechtigung und Aufgabentrennung integriert werden, indem Kerberos für Amazon-EMR-Cluster aktiviert wird. In Kerberos werden Services und Benutzer, die sich authentifizieren müssen, als Prinzipale bezeichnet. Prinzipale befinden sich in einem Kerberos-Bereich. Innerhalb dieses Bereichs wird ein Kerberos-Server als Key Distribution Center (KDC) bezeichnet. Über diesen Server können sich Prinzipale authentifizieren. Die Authentifizierung im KDC erfolgt durch die Ausstellung von Authentif

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			izierungstickets. Das KDC unterhält eine Datenbank der Prinzipale in seinem Bereich mit ihren Passwörtern und anderen administrativen Informationen zu jedem Prinzipal.
PR.AC-4	Zugriffsberechtigungen und Autorisierungen werden nach den Grundsätzen der geringsten Rechte und der Aufgabentrennung verwaltet	emr-master-no-public-ip	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon EMR-Cluster-Masterknoten nicht öffentlich zugänglich sind. Amazon-EMR-Cluster-Hauptknoten können vertrauliche Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.AC-4	Zugriffsberechtigungen und Autorisierungen werden nach den Grundsätzen der geringsten Rechte und der Aufgabentrennung verwaltet	iam-group-has-users-überprüfen	AWS Identity and Access Management (IAM) kann Ihnen helfen, die Prinzipien der geringsten Rechte und der Aufgabentrennung mit Zugriffsberechtigungen und Autorisierungen zu integrieren, indem sichergestellt wird, dass IAM-Gruppen mindestens einen Benutzer haben. Die Einteilung von Benutzern in Gruppen auf der Grundlage der ihnen zugewiesenen Berechtigungen oder ihrer Funktion ist eine Möglichkeit, das Prinzip der geringsten Berechtigung zu implementieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.AC-4	Zugriffsberechtigungen und Autorisierungen werden nach den Grundsätzen der geringsten Rechte und der Aufgabentrennung verwaltet	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) kann Ihnen dabei helfen, die Prinzipien der geringsten Rechte und der Aufgabentrennung in Zugriffsberechtigungen und Autorisierungen zu integrieren und so zu verhindern, dass Richtlinien „Effect“: „Allow“ mit „Action“: „*“ anstelle von „Resource“: „*“ enthalten. Wenn Benutzern mehr Rechte eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und der Aufgabentrennung verstoßen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.AC-4	Zugriffsberechtigungen und Autorisierungen werden nach den Grundsätzen der geringsten Rechte und der Aufgabentrennung verwaltet	iam-root-access-key-überprüfen	Der Zugriff auf Systeme und Ressourcen kann gesteuert werden, indem überprüft wird, ob der Root-Benutzer keine Zugriffsschlüssel mit seiner AWS Identity and Access Management (IAM) -Rolle verknüpft hat. Stellen Sie sicher, dass die Root-Zugriffsschlüssel gelöscht werden. Erstellen und verwenden Sie stattdessen rollenbasierte Funktionen, AWS-Konten um das Prinzip der geringsten Funktionalität zu berücksichtigen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.AC-4	Zugriffsberechtigungen und Autorisierungen werden nach den Grundsätzen der geringsten Rechte und der Aufgabentrennung verwaltet	iam-user-no-policies-überprüfen	Diese Regel stellt sicher, dass AWS Identity and Access Management (IAM) -Richtlinien nur Gruppen oder Rollen zugewiesen werden, um den Zugriff auf Systeme und Ressourcen zu kontrollieren. Die Zuweisung von Berechtigungen auf Gruppen- oder Rollenebene trägt dazu bei, die Wahrscheinlichkeit zu verringern, dass eine Identität übermäßige Berechtigungen erhält oder beibehält.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.AC-4	Zugriffsberechtigungen und Autorisierungen werden nach den Grundsätzen der geringsten Rechte und der Aufgabentrennung verwaltet	iam-user-unused-credentials-überprüfen	AWS Identity and Access Management (IAM) kann Ihnen bei Zugriffsberechtigungen und Autorisierungen helfen, indem es nach IAM-Passwörtern und Zugriffsschlüsseln sucht, die für einen bestimmten Zeitraum nicht verwendet wurden. Wenn ungenutzte Anmeldeinformationen identifiziert werden, müssen Sie sie deaktivieren und/oder entfernen, da dies gegen das Prinzip der geringsten Berechtigung verstoßen könnte. Für diese Regel müssen Sie einen Wert für das maxCredentialUsage Alter festlegen (Standardkonfiguration: 90). Der tatsächliche Wert muss den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.AC-4	Zugriffsberechtigungen und Autorisierungen werden nach den Grundsätzen der geringsten Rechte und der Aufgabentrennung verwaltet	lambda-function-public-access-verboten	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass AWS Lambda-Funktionen nicht öffentlich zugänglich sind. Der öffentliche Zugriff kann möglicherweise die Verfügbarkeit von Ressourcen beeinträchtigen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.AC-4	Zugriffsberechtigungen und Autorisierungen werden nach den Grundsätzen der geringsten Rechte und der Aufgabentrennung verwaltet	lambda-inside-vpc	Stellen Sie AWS Lambda-Funktionen in einer Amazon Virtual Private Cloud (Amazon VPC) bereit, um eine sichere Kommunikation zwischen einer Funktion und anderen Diensten innerhalb der Amazon VPC zu gewährleisten. Bei dieser Konfiguration sind kein Internet-Gateway, kein NAT-Gerät und keine VPN-Verbindung erforderlich. Der gesamte Datenverkehr bleibt sicher in der Cloud. AWS Domains, die sich innerhalb einer VPC befinden, verfügen aufgrund ihrer logischen Isolierung im Vergleich zu Domains mit öffentlichen Endpunkten über eine zusätzliche Sicherheitsebene. Um den Zugriff ordnungsgemäß zu verwalten,

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			sollten AWS Lambda-Funktionen einer VPC zugewiesen werden.
PR.AC-4	Zugriffsberechtigungen und Autorisierungen werden nach den Grundsätzen der geringsten Rechte und der Aufgabentrennung verwaltet	opensearch-in-vpc-only	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass sich Amazon OpenSearch Service-Domains innerhalb einer Amazon Virtual Private Cloud (Amazon VPC) befinden. Eine Amazon OpenSearch Service-Domain innerhalb einer Amazon VPC ermöglicht die sichere Kommunikation zwischen Amazon OpenSearch Service und anderen Services innerhalb der Amazon VPC, ohne dass ein Internet-Gateway, ein NAT-Gerät oder eine VPN-Verbindung erforderlich ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.AC-4	Zugriffsberechtigungen und Autorisierungen werden nach den Grundsätzen der geringsten Rechte und der Aufgabentrennung verwaltet	rds-instance-public-access-überprüfen	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Relational Database Service (Amazon RDS) -Instances nicht öffentlich sind. Amazon-RDS-Datenbank-Instances können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.AC-4	Zugriffsberechtigungen und Autorisierungen werden nach den Grundsätzen der geringsten Rechte und der Aufgabentrennung verwaltet	rds-snapshots-public-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Relational Database Service (Amazon RDS) -Instances nicht öffentlich sind. Amazon-RDS-Datenbank-Instances können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.AC-4	Zugriffsberechtigungen und Autorisierungen werden nach den Grundsätzen der geringsten Rechte und der Aufgabentrennung verwaltet	redshift-cluster-public-access-überprüfen	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Redshift Redshift-Cluster nicht öffentlich sind. Amazon-Redshift-Cluster können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.AC-4	Zugriffsberechtigungen und Autorisierungen werden nach den Grundsätzen der geringsten Rechte und der Aufgabentrennung verwaltet	s3- -Block-periodisch account-level-public-access	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Simple Storage Service (Amazon S3) -Buckets nicht öffentlich zugänglich sind. Diese Regel trägt dazu bei, sensible Daten vor unbefugten Remote-Benutzern zu schützen, indem sie den öffentlichen Zugriff verhindert. Mit dieser Regel können Sie optional die Parameter ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) und restrictPublicBuckets Parameter (Config Default: True) festlegen. Die tatsächlichen Werte müssen den Richtlini

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			en Ihrer Organisation entsprechen.
PR.AC-4	Zugriffsberechtigungen und Autorisierungen werden nach den Grundsätzen der geringsten Rechte und der Aufgabentrennung verwaltet	s3 bucket-level-public-access - verboten	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Simple Storage Service (Amazon S3) -Buckets nicht öffentlich zugänglich sind. Diese Regel trägt dazu bei, sensible Daten vor unbefugten Remote-Benutzern zu schützen, indem sie den öffentlichen Zugriff auf Bucket-Ebene verhindert.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.AC-4	Zugriffsberechtigungen und Autorisierungen werden nach den Grundsätzen der geringsten Rechte und der Aufgabentrennung verwaltet	s-3 bucket-public-read-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie nur autorisierten Benutzern, Prozessen und Geräten Zugriff auf Amazon Simple Storage Service (Amazon S3) - Buckets gewähren. Die Verwaltung des Zugriffs sollte mit der Klassifizierung der Daten übereinstimmen.
PR.AC-4	Zugriffsberechtigungen und Autorisierungen werden nach den Grundsätzen der geringsten Rechte und der Aufgabentrennung verwaltet	s3- bucket-public-write-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie nur autorisierten Benutzern, Prozessen und Geräten Zugriff auf Amazon Simple Storage Service (Amazon S3) - Buckets gewähren. Die Verwaltung des Zugriffs sollte mit der Klassifizierung der Daten übereinstimmen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.AC-4	Zugriffsberechtigungen und Autorisierungen werden nach den Grundsätzen der geringsten Rechte und der Aufgabentrennung verwaltet	sagemaker-notebook-no-direct-Internetzugang	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass SageMaker Amazon-Notebooks keinen direkten Internetzugang zulassen. Indem Sie direkten Internetzugang blockieren, vermeiden Sie, dass unbefugte Benutzer auf sensible Daten zugreifen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.AC-4	Zugriffsberechtigungen und Autorisierungen werden nach den Grundsätzen der geringsten Rechte und der Aufgabentrennung verwaltet	subnet-auto-assign-public-ip-deaktiviert	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon Virtual Private Cloud (VPC) -Subnetzen nicht automatisch eine öffentliche IP-Adresse zugewiesen wird. Amazon Elastic Compute Cloud (EC2) -Instances, die in Subnetzen gestartet werden, in denen dieses Attribut aktiviert ist, haben ihrer primären Netzwerkschnittstelle eine öffentliche IP-Adresse zugewiesen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.AC-5	Die Netzwerkintegrität ist geschützt (z. B. Netzwerktrennung, Netzwerksegmentierung)	autoscaling-launch-config-public-ip-deaktiviert	Wenn Sie Ihre Netzwerkschnittstellen mit einer öffentlichen IP-Adresse konfigurieren, sind die diesen Netzwerkschnittstellen zugehörigen Ressourcen über das Internet erreichbar. EC2 Ressourcen sollten nicht öffentlich zugänglich sein, da dies einen unbeabsichtigten Zugriff auf Ihre Anwendungen oder Server ermöglichen kann.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.AC-5	Die Netzwerkintegrität ist geschützt (z. B. Netzwerktrennung, Netzwerksegmentierung)	ec2- instances-in-vpc	Stellen Sie Amazon Elastic Compute Cloud (Amazon EC2) -Instances innerhalb einer Amazon Virtual Private Cloud (Amazon VPC) bereit, um eine sichere Kommunikation zwischen einer Instance und anderen Services innerhalb der Amazon VPC zu ermöglichen, ohne dass ein Internet-Gateway, ein NAT-Gerät oder eine VPN-Verbindung erforderlich ist. Der gesamte Datenverkehr bleibt sicher in der AWS Cloud. Domains, die sich innerhalb einer VPC befinden, verfügen aufgrund ihrer logischen Isolierung im Vergleich zu Domains mit öffentlichen Endpunkten über eine zusätzliche Sicherheitsebene. Weisen Sie EC2

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			Amazon-Instances einer Amazon-VPC zu, um den Zugriff ordnungsgemäß zu verwalten.
PR.AC-5	Die Netzwerkintegrität ist geschützt (z. B. Netzwerktrennung, Netzwerksegmentierung)	no-unrestricted-route-to-igw	Stellen Sie sicher, dass EC2 Amazon-Routentabellen keine uneingeschränkten Routen zu einem Internet-Gateway enthalten. Durch das Entfernen oder Beschränken des Internetzugangs für Workloads innerhalb von Amazon VPCs können unbeabsichtigte Zugriffe in Ihrer Umgebung reduziert werden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.AC-5	Die Netzwerkintegrität ist geschützt (z. B. Netzwerktrennung, Netzwerksegmentierung)	redshift-enhanced-vpc-routing-aktiviert	Mit Enhanced-VPC-Routing wird erzwungen, dass der gesamte COPY- und UNLOAD-Datenverkehr zwischen Ihrem Cluster und Datenrepositorys über Ihre Amazon VPC erfolgt. Anschließend können Sie VPC-Features wie Sicherheitsgruppen und Netzwerkzugriffskontrolllisten verwenden, um den Netzwerkverkehr zu schützen. Sie können auch VPC-Flow-Logs verwenden, um den Netzwerkverkehr zu überwachen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.AC-5	Die Netzwerkintegrität ist geschützt (z. B. Netzwerktrennung, Netzwerksegmentierung)	ssm-document-not-public	Stellen Sie sicher, dass AWS Systems Manager (SSM) - Dokumente nicht öffentlich sind, da dies einen unbeabsichtigten Zugriff auf Ihre SSM-Dokumente ermöglichen kann. Ein öffentliches SSM-Dokument kann Informationen über Ihr Konto, Ihre Ressourcen und internen Prozesse preisgeben.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.AC-5	Die Netzwerkintegrität ist geschützt (z. B. Netzwerktrennung, Netzwerksegmentierung)	acm-certificate-expiration-check	Stellen Sie sicher, dass die Netzwerkintegrität geschützt ist, indem Sie sicherstellen, dass X509-Zertifikate von ACM ausgestellt werden. AWS Diese Zertifikate müssen gültig und dürfen nicht abgelaufen sein. Für diese Regel ist ein Wert für erforderlich daysToExpiration (Wert für bewährte AWS Grundregeln für Sicherheit: 90). Der tatsächliche Wert muss den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.AC-5	Die Netzwerkintegrität ist geschützt (z. B. Netzwerktrennung, Netzwerksegmentierung)	dms-replication-not-public	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass auf DMS-Replikationsinstanzen nicht öffentlich zugegriffen werden kann. DMS-Replikations-Instances können vertrauliche Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.
PR.AC-5	Die Netzwerkintegrität ist geschützt (z. B. Netzwerktrennung, Netzwerksegmentierung)	ebs-snapshot-public-restorable-überprüfen	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass EBS-Snapshots nicht öffentlich wiederherstellbar sind. EBS-Volume-Snapshots können vertrauliche Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.AC-5	Die Netzwerkintegrität ist geschützt (z. B. Netzwerktrennung, Netzwerksegmentierung)	ec2- instance-no-public-ip	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon Elastic Compute Cloud (Amazon EC2) - Instances nicht öffentlich zugänglich sind. EC2Amazon -Instances können vertrauliche Informationen enthalten, und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.AC-5	Die Netzwerkintegrität ist geschützt (z. B. Netzwerktrennung, Netzwerksegmentierung)	elasticsearch-in-vpc-only	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass sich Amazon OpenSearch OpenSearch Service (Service) - Domains innerhalb einer Amazon Virtual Private Cloud (Amazon VPC) befinden. Eine OpenSearch Service-Domain innerhalb einer Amazon VPC ermöglicht die sichere Kommunikation zwischen OpenSearch Service und anderen Services innerhalb der Amazon VPC, ohne dass ein Internet-Gateway, ein NAT-Gerät oder eine VPN-Verbindung erforderlich ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.AC-5	Die Netzwerkintegrität ist geschützt (z. B. Netzwerktrennung, Netzwerksegmentierung)	emr-master-no-public-ip	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon EMR-Cluster-Masterknoten nicht öffentlich zugänglich sind. Amazon-EMR-Cluster-Hauptknoten können vertrauliche Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.AC-5	Die Netzwerkintegrität ist geschützt (z. B. Netzwerktrennung, Netzwerksegmentierung)	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) Security Groups können bei der Verwaltung des Netzwerkzugriffs helfen, indem sie eine statusbehaftete Filterung von eingehendem und ausgehendem Netzwerkverkehr zu Ressourcen bereitstellen. AWS Wenn Sie eingehenden (oder entfernten) Datenverkehr von 0.0.0.0/0 bis Port 22 auf Ihren Ressourcen nicht zulassen, können Sie den Remote-Zugriff einschränken.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.AC-5	Die Netzwerkintegrität ist geschützt (z. B. Netzwerktrennung, Netzwerksegmentierung)	lambda-function-public-access-verboten	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass AWS Lambda-Funktionen nicht öffentlich zugänglich sind. Der öffentliche Zugriff kann möglicherweise die Verfügbarkeit von Ressourcen beeinträchtigen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.AC-5	Die Netzwerkintegrität ist geschützt (z. B. Netzwerktrennung, Netzwerksegmentierung)	lambda-inside-vpc	Stellen Sie AWS Lambda-Funktionen in einer Amazon Virtual Private Cloud (Amazon VPC) bereit, um eine sichere Kommunikation zwischen einer Funktion und anderen Diensten innerhalb der Amazon VPC zu gewährleisten. Bei dieser Konfiguration sind kein Internet-Gateway, kein NAT-Gerät und keine VPN-Verbindung erforderlich. Der gesamte Datenverkehr bleibt sicher in der Cloud. AWS Domains, die sich innerhalb einer VPC befinden, verfügen aufgrund ihrer logischen Isolierung im Vergleich zu Domains mit öffentlichen Endpunkten über eine zusätzliche Sicherheitsebene. Um den Zugriff ordnungsgemäß zu verwalten,

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			sollten AWS Lambda-Funktionen einer VPC zugewiesen werden.
PR.AC-5	Die Netzwerkintegrität ist geschützt (z. B. Netzwerktrennung, Netzwerksegmentierung)	opensearch-in-vpc-only	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass sich Amazon OpenSearch Service-Domains innerhalb einer Amazon Virtual Private Cloud (Amazon VPC) befinden. Eine Amazon OpenSearch Service-Domain innerhalb einer Amazon VPC ermöglicht die sichere Kommunikation zwischen Amazon OpenSearch Service und anderen Services innerhalb der Amazon VPC, ohne dass ein Internet-Gateway, ein NAT-Gerät oder eine VPN-Verbindung erforderlich ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.AC-5	Die Netzwerkintegrität ist geschützt (z. B. Netzwerktrennung, Netzwerksegmentierung)	rds-instance-public-access-überprüfen	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Relational Database Service (Amazon RDS) -Instances nicht öffentlich sind. Amazon-RDS-Datenbank-Instances können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.AC-5	Die Netzwerkintegrität ist geschützt (z. B. Netzwerktrennung, Netzwerksegmentierung)	rds-snapshots-public-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Relational Database Service (Amazon RDS) -Instances nicht öffentlich sind. Amazon-RDS-Datenbank-Instances können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.AC-5	Die Netzwerkintegrität ist geschützt (z. B. Netzwerktrennung, Netzwerksegmentierung)	redshift-cluster-public-access-überprüfen	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Redshift Redshift-Cluster nicht öffentlich sind. Amazon-Redshift-Cluster können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.AC-5	Die Netzwerkintegrität ist geschützt (z. B. Netzwerktrennung, Netzwerksegmentierung)	restricted-common-ports	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass gemeinsame Ports für Amazon Elastic Compute Cloud (Amazon EC2) -Sicherheitsgruppen eingeschränkt sind. Wenn der Zugriff auf Ports nicht auf vertrauenswürdige Quellen beschränkt wird, kann dies zu Angriffen auf die Verfügbarkeit, Integrität und Vertraulichkeit von Systemen führen. Mit dieser Regel können Sie optional die Parameter blockedPort1–blockedPort5 festlegen (Standardkonfigurationen: 20, 21, 3389, 3306, 4333). Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.AC-5	Die Netzwerkintegrität ist geschützt (z. B. Netzwerktrennung, Netzwerksegmentierung)	s3- -Blocke-periodisch account-level-public-access	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Simple Storage Service (Amazon S3) -Buckets nicht öffentlich zugänglich sind. Diese Regel trägt dazu bei, sensible Daten vor unbefugten Remote-Benutzern zu schützen, indem sie den öffentlichen Zugriff verhindert. Mit dieser Regel können Sie optional die Parameter ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) und restrictPublicBuckets Parameter (Config Default: True) festlegen. Die tatsächlichen Werte müssen den Richtlini

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			en Ihrer Organisation entsprechen.
PR.AC-5	Die Netzwerkintegrität ist geschützt (z. B. Netzwerktrennung, Netzwerksegmentierung)	s-3 bucket-public-read-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie nur autorisierten Benutzern, Prozessen und Geräten Zugriff auf Amazon Simple Storage Service (Amazon S3) - Buckets gewähren. Die Verwaltung des Zugriffs sollte mit der Klassifizierung der Daten übereinstimmen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.AC-5	Die Netzwerkintegrität ist geschützt (z. B. Netzwerktrennung, Netzwerksegmentierung)	s-3 bucket-public-write-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie nur autorisierten Benutzern, Prozessen und Geräten Zugriff auf Amazon Simple Storage Service (Amazon S3) - Buckets gewähren. Die Verwaltung des Zugriffs sollte mit der Klassifizierung der Daten übereinstimmen.
PR.AC-5	Die Netzwerkintegrität ist geschützt (z. B. Netzwerktrennung, Netzwerksegmentierung)	sagemaker-notebook-no-direct-Internetzugang	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass SageMaker Amazon-Notebooks keinen direkten Internetzugang zulassen. Indem Sie direkten Internetzugang blockieren, vermeiden Sie, dass unbefugte Benutzer auf sensible Daten zugreifen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.AC-5	Die Netzwerkintegrität ist geschützt (z. B. Netzwerktrennung, Netzwerksegmentierung)	subnet-auto-assign-public-ip-deaktiviert	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon Virtual Private Cloud (VPC) -Subnetzen nicht automatisch eine öffentliche IP-Adresse zugewiesen wird. Amazon Elastic Compute Cloud (EC2) -Instances, die in Subnetzen gestartet werden, in denen dieses Attribut aktiviert ist, haben ihrer primären Netzwerkschnittstelle eine öffentliche IP-Adresse zugewiesen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.AC-5	Die Netzwerkintegrität ist geschützt (z. B. Netzwerktrennung, Netzwerksegmentierung)	vpc-default-security-group-geschlossen	Sicherheitsgruppen von Amazon Elastic Compute Cloud (Amazon EC2) können bei der Verwaltung des Netzwerkzugriffs helfen, indem sie eine statusbehaftete Filterung des ein- und ausgehenden Netzwerkverkehrs zu Ressourcen bereitstellen. AWS Die Beschränkung des gesamten Datenverkehrs auf die Standardsicherheitsgruppe hilft dabei, den Fernzugriff auf Ihre Ressourcen einzuschränken. AWS

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.AC-5	Die Netzwerkintegrität ist geschützt (z. B. Netzwerktrennung, Netzwerksegmentierung)	vpc-sg-open-only-to-authorized-ports	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass gemeinsame Ports für Amazon Elastic Compute Cloud (Amazon EC2) -Sicherheitsgruppen eingeschränkt sind. Wenn der Zugriff auf Ports nicht auf vertrauenswürdige Quellen beschränkt wird, kann dies zu Angriffen auf die Verfügbarkeit, Integrität und Vertraulichkeit von Systemen führen. Durch die Beschränkung des Zugriffs auf Ressourcen innerhalb einer Sicherheitsgruppe aus dem Internet (0.0.0.0/0) kann der Fernzugriff auf interne Systeme gesteuert werden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.DS-1	Data-at-rest ist geschützt	ec-2 ebs-encryption-by-default	Zum Schutz von Daten im Ruhezustand müssen Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon Elastic Block Store (Amazon EBS)-Volumes aktiviert ist. Da sensible Daten in diesen Volumes gespeichert werden können, sollten Sie die Verschlüsselung von Daten im Ruhezustand aktivieren, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.DS-1	Data-at-rest ist geschützt	rds-snapshot-encrypted	Stellen Sie sicher, dass die Verschlüsselung für Ihre Amazon Relational Database Service (Amazon RDS)-Snapshots aktiviert ist. Da sensible Daten auch im Ruhezustand vorhanden sein können, sollten Sie die Verschlüsselung von Daten im Ruhezustand aktivieren, um diese Daten zu schützen.
PR.DS-1	Data-at-rest ist geschützt	s-3 default-encryption-kms	Stellen Sie sicher, dass die Verschlüsselung für Ihre Amazon Simple Storage Service (Amazon S3)-Buckets aktiviert ist. Da sensible Daten in einem Amazon S3 Bucket gespeichert werden können, sollten Sie die Verschlüsselung im Ruhezustand aktivieren, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.DS-1	Data-at-rest ist geschützt	sagemaker-notebook-instance-kms-key-konfiguriert	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass die Verschlüsselung mit dem AWS Key Management Service (AWS KMS) für Ihr Notebook aktiviert ist. SageMaker Da vertrauliche Daten im SageMaker Notebook gespeichert werden können, sollten Sie die Verschlüsselung im Ruhezustand aktivieren, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.DS-1	Data-at-rest ist geschützt	sns-encrypted-kms	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass Ihre Amazon Simple Notification Service (Amazon SNS) -Themen mit dem AWS Key Management Service (AWS KMS) verschlüsselt werden müssen. Um eventuell vorhandene sensible Daten im Ruhezustand in veröffentlichten Nachrichten zu schützen, muss die Verschlüsselung von Daten im Ruhezustand aktiviert sein.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.DS-1	Data-at-rest ist geschützt	api-gw-cache-enabled-und verschlüsselt	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass die Verschlüsselung für den Cache Ihrer API-Gateway-Stufe aktiviert ist. Da für die API-Methode sensible Daten erfasst werden können, sollten Sie die Verschlüsselung von Daten im Ruhezustand aktivieren, um diese Daten zu schützen.
PR.DS-1	Data-at-rest ist geschützt	cloud-trail-encryption-enabled	Zum Schutz von eventuell vorhandenen sensiblen Daten sowie Daten im Ruhezustand müssen Sie sicherstellen, dass die Verschlüsselung für Ihre AWS CloudTrail aktiviert ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.DS-1	Data-at-rest ist geschützt	efs-encrypted-check	Aktivieren Sie die Verschlüsselung für Ihr Amazon Elastic File System (EFS), um eventuell vorhandene sensible Daten sowie Daten im Ruhezustand zu schützen.
PR.DS-1	Data-at-rest ist geschützt	elasticsearch-encrypted-at-rest	Da sensible Daten vorhanden sein können und um Daten im Ruhezustand zu schützen, sollten Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon OpenSearch Service (OpenSearch Service) -Domains aktiviert ist.
PR.DS-1	Data-at-rest ist geschützt	encrypted-volumes	Aktivieren Sie die Verschlüsselung für Ihre Amazon-Elastic-Block-Store-(Amazon-EBS-)Volumes, um eventuell vorhandene sensible Daten sowie Daten im Ruhezustand zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.DS-1	Data-at-rest ist geschützt	kms-cmk-not-scheduled-zum Löschen	Um Daten im Ruhezustand zu schützen, sollten Sie sicherstellen, dass die für den Kunden erforderlichen Masterschlüssel (CMKs) nicht im AWS Key Management Service (AWS KMS) gelöscht werden. Da Schlüssel manchmal gelöscht werden müssen, können Sie mit dieser Regel alle zu löschenden Schlüssel überprüfen, falls ein Schlüssel versehentlich zur Löschung vorgemerkt wurde.
PR.DS-1	Data-at-rest ist geschützt	opensearch-encrypted-at-rest	Da sensible Daten vorhanden sein können und um Daten im Ruhezustand zu schützen, sollten Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon OpenSearch Service-Domains aktiviert ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.DS-1	Data-at-rest ist geschützt	rds-storage-encrypted	Zum Schutz von Daten im Ruhezustand müssen Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon Relational Database Service (Amazon RDS)-Instances aktiviert ist. Da sensible Daten in Amazon-RDS-Instances gespeichert werden können, sollten Sie die Verschlüsselung von Daten im Ruhezustand aktivieren, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.DS-1	Data-at-rest ist geschützt	redshift-cluster-configuration-check	Um Daten im Ruhezustand zu schützen, muss die Verschlüsselung für Ihre Amazon-Redshift-Cluster aktiviert sein. Sie müssen auch sicherstellen, dass die erforderlichen Konfigurationen auf Amazon-Redshift-Clustern bereitgestellt werden. Die Prüfungsprotokollierung muss aktiviert sein, um Informationen zu Verbindungen und Benutzeraktivitäten in der Datenbank bereitzustellen. Diese Regel erfordert, dass ein Wert für clusterDbEncrypted (Config Default: TRUE) und LoggingEnabled (Config Default: TRUE) gesetzt ist. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.DS-1	Data-at-rest ist geschützt	redshift-cluster-kms-enabled	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass die Verschlüs selung mit AWS Key Management Service (AWS KMS) für Ihren Amazon Redshift Redshift-Cluster aktiviert ist. Da sensible Daten in Redshift-Clustern gespeichert werden können, sollten Sie Verschlüsselung von Daten im Ruhezusta nd aktivieren, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.DS-1	Data-at-rest ist geschützt	bucket-server-side-encryptions3-fähig	Zum Schutz von Daten im Ruhezustand müssen Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon Simple Storage Service (Amazon S3)-Buckets aktiviert ist. Da sensible Daten in Amazon S3 Buckets gespeichert werden können, sollten Sie die Verschlüsselung aktivieren, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.DS-1	Data-at-rest ist geschützt	sagemaker-endpoint-configuration-kms-key-konfiguriert	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass die Verschlüsselung mit dem AWS Key Management Service (AWS KMS) für Ihren Endpunkt aktiviert ist. SageMaker Da sensible Daten auf dem SageMaker Endgerät gespeiche rt werden können, sollten Sie die Verschlüsselung im Ruhezustand aktiviere n, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.DS-1	Data-at-rest ist geschützt	secretsmanager-using-cmk	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass die Verschlüsselung mit dem AWS Key Management Service (AWS KMS) für AWS Secrets Manager aktiviert ist. Aktivieren Sie die Verschlüsselung von Daten im Ruhezustand, um eventuell vorhandene sensible Daten im Ruhezustand im Secrets Manager zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.DS-2	Data-in-transit ist geschützt	elasticsearch-node-to-node-Verschlüsselungsprüfung	Stellen Sie sicher, dass die node-to-node Verschlüsselung für Amazon OpenSearch Service aktiviert ist. Node-to-nodeVerschlüsselung ermöglicht die TLS 1.2-Verschlüsselung für die gesamte Kommunikation innerhalb der Amazon Virtual Private Cloud (Amazon VPC). Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.DS-2	Data-in-transit ist geschützt	elbv-2 acm-certificate-required	Zum Schutz von eventuell vorhanden en sensiblen Daten sowie von Daten während der Übertragung muss die Verschlüsselung für Ihr Elastic Load Balancing aktiviert sein. Verwenden Sie AWS Certificate Manager, um öffentlic he und private SSL/ TLS-Zertifikate mit AWS Diensten und internen Ressource n zu verwalten, bereitzustellen und bereitzustellen.
PR.DS-2	Data-in-transit ist geschützt	elb-tls-https-listeners-nur	Stellen Sie sicher, dass Ihre Elastic Load Balancer (ELBs) mit SSL- oder HTTPS-Listenern konfiguriert sind. Um eventuell vorhanden e sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.DS-2	Data-in-transit ist geschützt	opensearch-node-to-node-Verschlüsselungsprüfung	Stellen Sie sicher, dass die node-to-node Verschlüsselung für Amazon OpenSearch Service aktiviert ist. Node-to-nodeVerschlüsselung ermöglicht die TLS 1.2-Verschlüsselung für die gesamte Kommunikation innerhalb der Amazon Virtual Private Cloud (Amazon VPC). Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.DS-2	Data-in-transit ist geschützt	alb-http-to-https-Umleitungsprüfung	Um Daten während der Übertragung zu schützen, stellen Sie sicher, dass Ihr Application Load Balancer unverschlüsselte HTTP-Anfragen automatisch an HTTPS umleitet. Da sensible Daten vorhanden sein können, sollten Sie die Verschlüsselung bei der Übertragung aktivieren, um diese Daten zu schützen.
PR.DS-2	Data-in-transit ist geschützt	api-gw-ssl-enabled	Stellen Sie sicher, dass die REST-API-Stufen von Amazon API Gateway mit SSL-Zertifikaten konfiguriert sind, damit Backend-Systeme überprüfen können, ob Anforderungen von API Gateway stammen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.DS-2	Data-in-transit ist geschützt	elb-acm-certificate-required	Zum Schutz von eventuell vorhanden en sensiblen Daten sowie von Daten während der Übertragung muss die Verschlüsselung für Ihr Elastic Load Balancing aktiviert sein. Verwenden Sie AWS Certificate Manager, um öffentlic he und private SSL/ TLS-Zertifikate mit AWS Diensten und internen Ressource n zu verwalten, bereitzustellen und bereitzustellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.DS-2	Data-in-transit ist geschützt	redshift-require-tls-ssl	Stellen Sie sicher, dass Ihre Amazon-Redshift-Cluster eine TLS/SSL-Verschlüsselung erfordern, um eine Verbindung zu SQL-Clients herzustellen. Da sensible Daten vorhanden sein können, sollten Sie die Verschlüsselung bei der Übertragung aktivieren, um diese Daten zu schützen.
PR.DS-2	Data-in-transit ist geschützt	s-3 bucket-ssl-requests-only	Um Daten während der Übertragung zu schützen, stellen Sie sicher, dass Ihre Amazon Simple Storage Service (Amazon S3)-Buckets Anfragen zur Verwendung von Secure Socket Layer (SSL)-Buckets erfordern. Da sensible Daten vorhanden sein können, sollten Sie die Verschlüsselung bei der Übertragung aktivieren, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.DS-6	Mechanismen zur Integritätsprüfung werden verwendet, um die Integrität von Software, Firmware und Informationen zu überprüfen	cloud-trail-log-file-Validierung aktiviert	Verwenden Sie die AWS CloudTrail Protokolldateivalidierung, um die Integrität von Protokollen zu überprüfen. CloudTrail Mithilfe der Protokolldateivalidierung kann festgestellt werden, ob eine Protokolldatei geändert oder gelöscht wurde oder ob sie nach der Übermittlung CloudTrail unverändert geblieben ist. Dieses Feature wurde mit dem Branchenstandard entsprechenden Algorithmen entwickelt: SHA-256 für die Hashfunktion und SHA-256 mit RSA für digitale Signaturen. Aus diesem Grund ist es rechnerisch unmöglich, CloudTrail Protokolldateien unbemerkt zu ändern, zu löschen oder zu fälschen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.DS-6	Mechanismen zur Integritätsprüfung werden verwendet, um die Integrität von Software, Firmware und Informationen zu überprüfen	s-3 bucket-versioning-enabled	Die Versionsv erwaltung von Amazon Simple Storage Service (Amazon S3)-Bucke ts hilft dabei, mehrere Varianten eines Objekts im selben Amazon-S3-Bucket zu speichern. Verwenden Sie die Versionsv erwaltung, um sämtliche Versionen aller Objekte in Ihrem Amazon-S3-Bucket zu speichern , abzurufen oder wiederherzustellen . Mit der Versionsv erwaltung können Sie Versionen sowohl nach unbeabsic htigten Benutzera ktionen als auch nach Anwendungsfehlern problemlos wiederher stellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.IP-1	Es wird eine Basiskonfiguration für Informationstechnologie/industrielle Steuerungssysteme erstellt und beibehalten, die Sicherheitsprinzipien (z. B. das Konzept der geringsten Funktionalität) berücksichtigt	account-part-of-organizations	Durch die zentrale Verwaltung AWS-Konten innerhalb von AWS Organizations wird sichergestellt, dass die Konten den Vorschriften entsprechen. Eine fehlende zentrale Kontoverwaltung kann zu inkonsistenten Kontokonfigurationen führen, wodurch Ressourcen und sensible Daten offengelegt werden können.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.IP-1	Es wird eine Basiskonfiguration von Informati onstechnologie-/in dustriellen Steuerung ssystemen erstellt und verwaltet, die Sicherheitsprinzipien (z. B. das Konzept der geringsten Funktiona lität) berücksichtigt	ec2-manager instance-managed-by-systems	Eine Bestandsa ufnahme der Softwareplattforme n und Anwendung en innerhalb des Unternehmens ist möglich, indem Amazon Elastic Compute Cloud (Amazon EC2) - Instances mit AWS Systems Manager verwaltet werden. Verwenden Sie AWS Systems Manager, um detaillierte Systemkonfiguratio nen, Betriebssystem-Patch-Levels, Namen und Typ der Dienste, Softwareinstallati onen, Anwendung sname, Herausgeb er und Version sowie andere Details zu Ihrer Umgebung bereitzustellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.IP-1	Es wird eine Basiskonfiguration für Informationstechnologie/industrielle Steuerungssysteme erstellt und verwaltet, die Sicherheitsprinzipien (z. B. das Konzept der geringsten Funktionalität) berücksichtigt	ec2-check managedinstance-association-compliance-status	Verwenden Sie AWS Systems Manager Associations, um bei der Inventarisierung von Softwareplattformen und Anwendungen innerhalb eines Unternehmens zu helfen. AWS Systems Manager weist Ihren verwalteten Instances einen Konfigurationsstatus zu und ermöglicht es Ihnen, Basiswerte für Betriebssystem-Patch-Levels, Softwareinstallationen, Anwendungskonfigurationen und andere Details zu Ihrer Umgebung festzulegen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.IP-1	Es wird eine Basiskonfiguration von Informati onstechnologie-/in dustriellen Steuerung ssystemen erstellt und verwaltet, die Sicherheitsprinzip ien berücksichtigt (z. B. das Konzept der geringsten Funktiona lität)	ec2-stopped-instance	Aktivieren Sie diese Regel, um bei der Basiskonfiguration von Amazon Elastic Compute Cloud (Amazon EC2) - Instances zu helfen, indem Sie überprüfe n, ob EC2 Amazon-Instances gemäß den Standards Ihrer Organisation für mehr als die zulässige Anzahl von Tagen gestoppt wurden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.IP-1	Es wird eine Basiskonfiguration von Informati onstechnologie-/in dustriellen Kontrolls ystemen erstellt und verwaltet, die Sicherheitsprinzipien (z. B. das Konzept der geringsten Funktiona lität) berücksichtigt	ec2- volume-inuse-check	Diese Regel stellt sicher, dass Amazon Elastic Block Store-Volumes, die an Amazon Elastic Compute Cloud (Amazon EC2) - Instances angehängt sind, zum Löschen markiert werden, wenn eine Instance beendet wird. Wenn ein Amazon-EB S-Volume nicht gelöscht wird, wenn die Instance, an die es angehängt ist, beendet wird, kann dies gegen das Konzept der geringsten Funktiona lität verstoßen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.IP-1	Es wird eine Basiskonfiguration von Informati onstechnologie-/in dustriellen Kontrolls ystemen erstellt und verwaltet, die Sicherheitsprinzipien (z. B. das Konzept der geringsten Funktiona lität) berücksichtigt	redshift-cluster-m aintenancesettings-check	Diese Regel stellt sicher, dass Amazon-Redshift-Cluster die bevorzugten Einstellungen für Ihre Organisation haben. Insbesondere sorgt sie dafür, dass Cluster bevorzugt e Wartungsfenster und automatisierte Aufbewahrungsfristen für Snapshots für die Datenbank haben. Für diese Regel müssen Sie die festlegen. allowVersionUpgrad e Der Standardwert ist „true“. Außerdem können Sie optional den Zeitraum preferredMaintenan ceWindow (der Standardwert ist sa: 16:00 -sa: 16:30) und den automated SnapshotRetention Zeitraum (der Standardwert ist 1) festlegen. Die tatsächlichen Werte müssen den Richtlini

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			en Ihrer Organisation entsprechen.
PR.IP-3	Prozesse zur Steuerung von Konfigurationsänderungen sind vorhanden	elb-deletion-protection-enabled	Diese Regel sorgt dafür, dass der Löschschutz für Elastic Load Balancing aktiviert ist. Verwenden Sie diese Funktion, um zu verhindern, dass Ihr Load Balancer versehentlich oder böswillig gelöscht wird, was zum Verlust der Verfügbarkeit Ihrer Anwendungen führen kann.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.IP-3	Prozesse zur Steuerung von Konfigurationsände rungen sind vorhanden	rds-instance-deletion-protection-aktiviert	Stellen Sie sicher, dass Amazon Relational Database Service (Amazon RDS)-Instances den Löschschutz aktiviert haben. Verwenden Sie den Löschschu tz, um zu verhindern, dass Ihre Amazon-RD S-Instances versehent lich oder böswillig gelöscht werden, was zum Verlust der Verfügbarkeit Ihrer Anwendungen führen kann.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.IP-4	Datensicherungen werden durchgeführt, verwaltet und getestet	dynamodb-in-backup-plan	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon DynamoDB-Tabellen Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.IP-4	Datensicherungen werden durchgeführt, verwaltet und getestet	ebs-in-backup-plan	Stellen Sie zur Unterstützung der Datensicherungspro zesse sicher, dass Ihre Amazon Elastic Block Store (Amazon EBS) -Volumes Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwaltet er Backup-Service mit einer richtlini enbasierten Backup-Lösung. Diese Lösung vereinfacht Ihre Backup-Verwaltung und ermöglicht es Ihnen, Ihre geschäftl ichen und behördlic hen Anforderungen bezüglich Backups zu erfüllen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.IP-4	Datensicherungen werden durchgeführt, verwaltet und getestet	efs-in-backup-plan	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon Elastic File System (Amazon EFS) -Dateisysteme Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.IP-4	Datensicherungen werden durchgeführt, verwaltet und getestet	rds-in-backup-plan	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon Relational Database Service (Amazon RDS) -Instances Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.IP-4	Datensicherungen werden durchgeführt, verwaltet und getestet	redshift-backup-enabled	Stellen Sie zur Unterstützung der Datensicherungsprozesse sicher, dass Ihre Amazon-Redshift-Cluster über automatisierte Snapshots verfügen. Wenn automatisierte Snapshots für einen Cluster aktiviert sind, erstellt Redshift in regelmäßigen Abständen Snapshots dieses Clusters. Standardmäßig erstellt Redshift alle acht Stunden oder alle 5 GB einen Snapshot für jeden Knoten mit Datenänderungen oder je nachdem, was zuerst eintritt.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.IP-4	Datensicherungen werden durchgeführt, verwaltet und getestet	db-instance-backup-enabled	Die Sicherungsfunktion von Amazon RDS erstellt Sicherungen Ihrer Datenbanken und Transaktionsprotokolle. Amazon RDS erstellt einen Snapshot für das Speichervolume Ihrer DB-Instance, sodass die gesamte DB-Instance gesichert wird. Sie können im System spezifische Aufbewahrungsfristen festlegen, um Ihre Ausfallsicherheitsanforderungen zu erfüllen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.IP-4	Datensicherungen werden durchgeführt, verwaltet und getestet	dynamodb-pitr-enabled	Aktivieren Sie diese Regel, um zu überprüfen, ob die Informationen gesichert wurden. Es verwaltet auch die Backups, indem es sicherstellt, dass die point-in-time Wiederherstellung in Amazon DynamoDB aktiviert ist. Bei der Wiederherstellung werden fortlaufende Backups Ihrer Tabelle für die letzten 35 Tage gespeichert.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.IP-4	Datensicherungen werden durchgeführt, verwaltet und getestet	elasticache-redis-cluster-automatic-Backup-Prüfung	Wenn automatische Backups aktiviert sind, ElastiCache erstellt Amazon täglich ein Backup des Clusters. Die Sicherung kann für eine von Ihrer Organisation festgelegte Anzahl von Tagen aufbewahrt werden. Automatische Backups schützen vor Datenverlust. Bei einem Ausfall können Sie einen neuen Cluster erstellen, der Ihre Daten aus dem aktuellen Backup wiederherstellt.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.IP-4	Datensicherungen werden durchgeführt, verwaltet und getestet	redshift-cluster-maintenancesettings-check	Diese Regel stellt sicher, dass Amazon-Redshift-Cluster die bevorzugten Einstellungen für Ihre Organisation haben. Insbesondere sorgt sie dafür, dass Cluster bevorzugte Wartungsfenster und automatisierte Aufbewahrungsfristen für Snapshots für die Datenbank haben. Für diese Regel müssen Sie die festlegen allowVersionUpgrade. Der Standardwert ist „true“. Außerdem können Sie optional den Zeitraum preferredMaintenanceWindow (der Standardwert ist sa: 16:00 -sa: 16:30) und den automated SnapshotRetention Zeitraum (der Standardwert ist 1) festlegen. Die tatsächlichen Werte müssen den Richtlini

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			en Ihrer Organisation entsprechen.
PR.IP-4	Datensicherungen werden durchgeführt, verwaltet und getestet	s3- bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) unterstützt die Aufrechterhaltung einer angemesse nen Kapazität und Verfügbarkeit. CRR ermöglicht das automatische, asynchrone Kopieren von Objekten in Amazon S3 Buckets, um die Datenverf ügbarkeit sicherzus tellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.IP-4	Datensicherungen werden durchgeführt, verwaltet und getestet	s-3 bucket-versioning-enabled	Die Versionsv erwaltung von Amazon Simple Storage Service (Amazon S3)-Bucke ts hilft dabei, mehrere Varianten eines Objekts im selben Amazon-S3-Bucket zu speichern. Verwenden Sie die Versionsv erwaltung, um sämtliche Versionen aller Objekte in Ihrem Amazon-S3-Bucket zu speichern , abzurufen oder wiederherzustellen . Mit der Versionsv erwaltung können Sie Versionen sowohl nach unbeabsic htigten Benutzera ktionen als auch nach Anwendungsfehlern problemlos wiederher stellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.IP-9	Reaktionspläne (Incident Response und Business Continuity) und Wiederherstellungspläne (Incident Recovery und Disaster Recovery) sind vorhanden und werden verwaltet.	response-plan-exists-maintained (Prozessüberprüfung)	Stellen Sie sicher, dass Vorfallreaktionspläne erstellt, verwaltet und an das verantwortliche Personal verteilt werden. Aktualisierte und formal dokumentierte Reaktionspläne können dazu beitragen, dass das zuständige Personal die Rollen, Verantwortlichkeiten und Prozesse versteht, die bei einem Vorfall einzuhalten sind.
PR.IP-10	Reaktions- und Wiederherstellungspläne werden getestet.	response-plan-tested (Prozessüberprüfung)	Stellen Sie sicher, dass die Vorfallreaktions- und Wiederherstellungspläne getestet wurden. Dies kann Ihnen helfen zu verstehen, ob Ihr Plan bei einem Vorfall wirksam ist und ob etwaige Lücken behoben oder Aktualisierungen vorgenommen werden müssen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.IP-12	Ein Plan für das Management von Schwachstellen wird entwickelt und umgesetzt.	vuln-management-plan-exists (Prozessüberprüfung)	Stellen Sie sicher, dass ein Plan für das Schwachstellenmanagement entwickelt und implementiert wird, damit Sie über formell definierte Prozesse zur Behebung von Schwachstellen in Ihrer Umgebung verfügen. Dazu zählen Tools für das Schwachstellenmanagement, regelmäßige Umgebungsscans sowie entsprechende Rollen und Verantwortlichkeiten.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.IP-12	Ein Plan für das Schwachstellenmanagement wird entwickelt und umgesetzt	ec2-manager instance-managed-by-systems	Eine Bestandsaufnahme der Softwareplattformen und Anwendungen innerhalb des Unternehmens ist möglich, indem Amazon Elastic Compute Cloud (Amazon EC2) - Instances mit AWS Systems Manager verwaltet werden. Verwenden Sie AWS Systems Manager, um detaillierte Systemkonfigurationen, Betriebssystem-Patch-Levels, Namen und Typ der Dienste, Softwareinstallationen, Anwendungsname, Herausgeber und Version sowie andere Details zu Ihrer Umgebung bereitzustellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.IP-12	Ein Plan für das Schwachstellenmanagement wird entwickelt und umgesetzt	ec2-check managedinstance-association-compliance-status	Verwenden Sie AWS Systems Manager Associations, um bei der Inventarisierung von Softwareplattformen und Anwendungen innerhalb eines Unternehmens zu helfen. AWS Systems Manager weist Ihren verwalteten Instances einen Konfigurationsstatus zu und ermöglicht es Ihnen, Basiswerte für Betriebssystem-Patch-Levels, Softwareinstallationen, Anwendungskonfigurationen und andere Details zu Ihrer Umgebung festzulegen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.IP-12	Ein Plan für das Schwachstellenmanagement wird entwickelt und umgesetzt	ec2-prüfen managedinstance-patch-compliance-status	Aktivieren Sie diese Regel, um bei der Identifizierung und Dokumentation von Sicherheitslücken in Amazon Elastic Compute Cloud (Amazon EC2) zu helfen. Die Regel prüft, ob die EC2 Amazon-Instance die Patch-Konformität im AWS Systems Manager gemäß den Richtlinien und Verfahren Ihrer Organisation einhält.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.MA-2	Die Fernwartung von Unternehm ensressourcen wird genehmigt, protokoll iert und in einer Weise durchgeführt, die unbefugten Zugriff verhindert.	multi-region-cloudtrail-enabled	AWS CloudTrail zeichnet Aktionen und API-Aufrufe der AWS Management Console auf. Sie können feststellen, welche Benutzer und Konten angerufen wurden AWS, von welcher Quell-IP-Adresse aus die Anrufe getätigt wurden und wann die Anrufe erfolgten. CloudTrail übermittelt Protokolldateien aus allen AWS Regionen an Ihren S3-Bucket , wenn MULTI_REG ION_CLOUD _TRAIL_ENABLED aktiviert ist. Außerdem wird beim AWS Start einer neuen Region derselbe Trail in der neuen Region erstellt. CloudTrail Dadurch erhalten Sie automatis ch Protokolldateien mit API-Aktivitäten für die neue Region.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.MA-2	Die Fernwartung von Unternehm ensressourcen wird genehmigt, protokoll iert und in einer Weise durchgeführt, die unbefugten Zugriff verhindert.	cloudtrail-enabled	AWS CloudTrai l kann durch die Aufzeichnung von Aktionen und API-Aufrufen in der AWS Management Console bei der Nichtabst reitbarkeit helfen. Sie können die Benutzer und die Benutzer AWS-Konten , die einen AWS Dienst aufgerufen haben, die Quell-IP-Adresse, über die die Aufrufe generiert wurden, und den Zeitpunkt der Anrufe identifiz ieren. Einzelheiten zu den erfassten Daten finden Sie in den AWS CloudTrail Datensatzinhalten.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.PT-1	Audit-/Protokollaufzeichnungen werden in Übereinstimmung mit den Richtlinien festgelegt, dokumentiert, umgesetzt und überprüft.	elasticsearch-logs-to-cloudwatch	Stellen Sie sicher, dass für Amazon OpenSearch Service-Domains Fehlerprotokolle aktiviert und zur Aufbewahrung und Beantwortung an Amazon CloudWatch Logs gestreamt werden. Domain-Fehlerprotokolle sind bei Sicherheits- und Zugriffsprüfungen sowie bei der Diagnose von Verfügbarkeitsproblemen nützlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.PT-1	Audit-/Protokollaufzeichnungen werden in Übereinstimmung mit den Richtlinien festgelegt, dokumentiert, umgesetzt und überprüft.	guardduty-non-archived-findings	Amazon GuardDuty hilft Ihnen dabei, die Auswirkungen eines Vorfalls zu verstehen, indem es die Ergebnisse nach Schweregrad klassifiziert: niedrig, mittel und hoch. Diese Klassifizierungen können Sie zur Festlegung von entsprechenden Strategien und Prioritäten zur Behebung solcher Vorfälle verwenden. Mit dieser Regel können Sie optional daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7) und daysHighSev (Config Default: 1) für nicht archivierte Ergebnisse festlegen, wie es die Richtlinien Ihrer Organisation erfordern.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.PT-1	Audit-/Protokollaufzeichnungen werden in Übereinstimmung mit den Richtlinien festgelegt, dokumentiert, umgesetzt und überprüft.	multi-region-cloudtrail-enabled	AWS CloudTrail zeichnet Aktionen und API-Aufrufe der AWS Management Console auf. Sie können feststellen, welche Benutzer und Konten angerufen wurden AWS, von welcher Quell-IP-Adresse aus die Anrufe getätigt wurden und wann die Anrufe erfolgten. CloudTrail übermittelt Protokolldateien aus allen AWS Regionen an Ihren S3-Bucket , wenn MULTI_REGION_CLOUD_TRAIL_ENABLED aktiviert ist. Außerdem wird beim AWS Start einer neuen Region derselbe Trail in der neuen Region erstellt. CloudTrail Dadurch erhalten Sie automatisch Protokolldateien mit API-Aktivitäten für die neue Region.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.PT-1	Kommunikations- und Kontrollnetzwerke sind geschützt	opensearch-logs-to-cloudwatch	Stellen Sie sicher, dass für Amazon OpenSearch Service-Domains Fehlerprotokolle aktiviert und zur Aufbewahrung und Beantwortung an Amazon CloudWatch Logs gestreamt werden. OpenSearch Service-Fehlerprotokolle können bei Sicherheits- und Zugriffsprüfungen helfen und bei der Diagnose von Verfügbarkeitsproblemen helfen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.PT-1	Audit-/Protokollaufzeichnungen werden in Übereinstimmung mit den Richtlinien festgelegt, dokumentiert, umgesetzt und überprüft.	rds-enhanced-monitoring-enabled	Aktivieren Sie Amazon Relational Database Service (Amazon RDS), um die Verfügbarkeit von Amazon RDS zu überwachen. Dies bietet einen detaillierten Einblick in den Zustand Ihrer Amazon-RDS-Datenbank-Instances. Wenn der Amazon-RDS-Speicher mehr als ein zugrunde liegendes physisches Gerät verwendet, erfasst Enhanced Monitoring die Daten für jedes Gerät. Wenn die Datenbank-Instance von Amazon RDS in einer Multi-AZ-Bereitstellung ausgeführt wird, werden außerdem die Daten für jedes Gerät auf dem sekundären Host sowie die Metriken des sekundären Hosts erfasst.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.PT-1	Audit-/Protokollaufzeichnungen werden in Übereinstimmung mit den Richtlinien festgelegt, dokumentiert, umgesetzt und überprüft.	rds-logging-enabled	Um die Protokollierung und Überwachung in Ihrer Umgebung zu erleichtern, stellen Sie sicher, dass die Amazon Relational Database Service (Amazon RDS)-Protokollierung aktiviert ist. Mit der Amazon-RDS-Protokollierung können Sie Ereignisse wie Verbindungen, Verbindungsabbrüche, Abfragen oder abgefragte Tabellen erfassen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.PT-1	Audit-/Protokollaufzeichnungen werden in Übereinstimmung mit den Richtlinien festgelegt, dokumentiert, umgesetzt und überprüft.	wafv2-logging-enabled	Um die Protokollierung und Überwachung in Ihrer Umgebung zu erleichtern, aktivieren Sie die AWS WAF (V2) -Protokollierung im regionalen und globalen Internet ACLs. AWS Die WAF-Protokollierung bietet detaillierte Informationen über den Datenverkehr, der von Ihrer Web-ACL analysiert wird. In den Protokollen werden die Uhrzeit aufgezeichnet, zu der die AWS WAF die Anfrage von Ihrer AWS Ressource erhalten hat, Informationen über die Anfrage und eine Aktion für die Regel, der jede Anfrage entsprach.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.PT-1	Audit-/Protokollaufzeichnungen werden in Übereinstimmung mit den Richtlinien festgelegt, dokumentiert, umgesetzt und überprüft.	api-gw-execution-logging-aktiviert	Die API-Gateway-Protokollierung zeigt detaillierte Ansichten der Benutzer, die auf die API zugegriffen haben, und wie diese Benutzer auf die API zugegriffen haben. Diese Insights ermöglichen die Einsicht in Benutzeraktivitäten.
PR.PT-1	Audit-/Protokollaufzeichnungen werden in Übereinstimmung mit den Richtlinien festgelegt, dokumentiert, umgesetzt und überprüft.	cloud-trail-cloud-watch-logs-aktiviert	Verwenden Sie Amazon CloudWatch , um Protokollereignisaktivitäten zentral zu sammeln und zu verwalten. Die Aufnahme von AWS CloudTrail Daten liefert Einzelheiten zu den API-Aufrufaktivitäten in Ihrem AWS-Konto.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.PT-1	Audit-/Protokollaufzeichnungen werden in Übereinstimmung mit den Richtlinien festgelegt, dokumentiert, umgesetzt und überprüft.	cloudtrail-enabled	AWS CloudTrail kann bei der Nichtabstreitbarkeit helfen, indem Aktionen und API-Aufrufe der AWS Management Console aufgezeichnet werden. Sie können die Benutzer und die Benutzer AWS-Konten , die einen AWS Dienst aufgerufen haben, die Quell-IP-Adresse, über die die Aufrufe generiert wurden, und den Zeitpunkt der Anrufe identifizieren. Einzelheiten zu den erfassten Daten finden Sie in den AWS CloudTrail Datensatzinhalten.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.PT-1	Audit-/Protokollaufzeichnungen werden in Übereinstimmung mit den Richtlinien festgelegt, dokumentiert, umgesetzt und überprüft.	cloudtrail-s3-dataevents-enabled	Die Erfassung von Simple Storage Service (Amazon S3)-Datenereignissen unterstützt die Erkennung von ungewöhnlichen Aktivitäten. Zu den Details gehören Informationen zum AWS -Konto, das auf einen Amazon S3 Bucket zugegriffen hat, die IP-Adresse und die Uhrzeit des Ereignisses.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.PT-1	Audit-/Protokollaufzeichnungen werden in Übereinstimmung mit den Richtlinien festgelegt, dokumentiert, umgesetzt und überprüft.	elb-logging-enabled	Die Elastic-Load-Balancing-Aktivität ist ein zentraler Kommunikationspunkt innerhalb einer Umgebung. Stellen Sie sicher, dass die ELB-Protokollierung aktiviert ist. Die gesammelten Daten enthalten detaillierte Informationen zu Anfragen, die an den ELB gesendet wurden. Jedes Protokoll enthält Informationen wie die Zeit, zu der die Anforderung einging, die Client-IP-Adresse, Latenzen, Anforderungspfade und Serverantworten.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.PT-1	Audit-/Protokollaufzeichnungen werden in Übereinstimmung mit den Richtlinien festgelegt, dokumentiert, umgesetzt und überprüft.	guardduty-enabled-centralized	Amazon GuardDuty kann mithilfe von Threat Intelligence Feeds helfen, potenzielle Cybersicherheitsereignisse zu überwachen und zu erkennen. Dazu gehören Listen mit bösartigen IPs und maschinellen Lernmethoden zur Identifizierung unerwarteter, nicht autorisierter und bösartiger Aktivitäten in Ihrer AWS Cloud-Umgebung.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.PT-1	Audit-/Protokollaufzeichnungen werden in Übereinstimmung mit den Richtlinien festgelegt, dokumentiert, umgesetzt und überprüft.	redshift-cluster-configuration-check	Um Daten im Ruhezustand zu schützen, muss die Verschlüsselung für Ihre Amazon-Redshift-Cluster aktiviert sein. Sie müssen auch sicherstellen, dass die erforderlichen Konfigurationen auf Amazon-Redshift-Clustern bereitgestellt werden. Die Prüfungsprotokollierung muss aktiviert sein, um Informationen zu Verbindungen und Benutzeraktivitäten in der Datenbank bereitzustellen. Diese Regel erfordert, dass ein Wert für clusterDbEncrypted (Config Default: TRUE) und LoggingEnabled (Config Default: TRUE) gesetzt ist. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.PT-1	Audit-/Protokollaufzeichnungen werden in Übereinstimmung mit den Richtlinien festgelegt, dokumentiert, umgesetzt und überprüft.	s3- bucket-logging-enabled	Die Amazon Simple Storage Service (Amazon S3)-Serverzugriffsprotokollierung bietet eine Methode zur Überwachung des Netzwerks im Hinblick auf potenzielle Cybersicherheitsereignisse. Die Ereignisse werden überwacht, indem detaillierte Aufzeichnungen über die Anfragen erfasst werden, die an einen Amazon-S3-Bucket gestellt wurden. Jeder Zugriffsprotokolleintrag enthält Details zu einer einzelnen Zugriffsanfrage. Zu den Details gehören Anforderer, Bucket-Name, Anforderungszeit, Anforderungsaktion, Antwortstatus und Fehlercode, falls relevant.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.PT-1	Audit-/Protokollaufzeichnungen werden in Übereinstimmung mit den Richtlinien festgelegt, dokumentiert, umgesetzt und überprüft.	vpc-flow-logs-enabled	VPC-Flow-Protokolle erfassen detaillierte Informationsdatensätze über den IP-Datenverkehr, der zu und von Netzwerkschnittstellen in Ihrer Amazon Virtual Private Cloud (Amazon VPC) fließt. Standardmäßig enthalten Flow-Protokolldatensätze Werte für die verschiedenen Komponenten des IP-Flows, einschließlich Quelle, Ziel und Protokoll.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.PT-3	Das Prinzip der geringsten Funktionalität wird durch die Konfiguration von Systemen umgesetzt, die nur die wesentlichen Funktionen bereitstellen.	autoscaling-launch-config-public-ip-deaktiviert	Wenn Sie Ihre Netzwerkschnittstellen mit einer öffentlichen IP-Adresse konfigurieren, sind die diesen Netzwerkschnittstellen zugehörigen Ressourcen über das Internet erreichbar. EC2 Ressourcen sollten nicht öffentlich zugänglich sein, da dies einen unbeabsichtigten Zugriff auf Ihre Anwendungen oder Server ermöglichen kann.
PR.PT-3	Das Prinzip der geringsten Funktionalität wird durch die Konfiguration von Systemen umgesetzt, die nur die wesentlichen Funktionen bereitstellen.	ec2- instance-profile-attached	EC2 Instanzprofile übergeben eine IAM-Rolle an eine EC2 Instance. Das Anhängen eines Instance-Profils an Ihre Instances kann bei der Implementierung von geringsten Berechtigungen und der Berechtigungsverwaltung helfen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.PT-3	Das Prinzip der geringsten Funktionalität wird durch die Konfiguration von Systemen umgesetzt, die nur die wesentlichen Funktionen bereitstellen.	ec2- instances-in-vpc	Stellen Sie Amazon Elastic Compute Cloud (Amazon EC2) -Instances innerhalb einer Amazon Virtual Private Cloud (Amazon VPC) bereit, um eine sichere Kommunikation zwischen einer Instance und anderen Services innerhalb der Amazon VPC zu ermöglichen, ohne dass ein Internet-Gateway, ein NAT-Gerät oder eine VPN-Verbindung erforderlich ist. Der gesamte Datenverkehr bleibt sicher in der AWS Cloud. Domains, die sich innerhalb einer VPC befinden, verfügen aufgrund ihrer logischen Isolierung im Vergleich zu Domains mit öffentlichen Endpunkten über eine zusätzliche Sicherheitsebene. Weisen Sie EC2

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			Amazon-Instances einer Amazon-VPC zu, um den Zugriff ordnungsgemäß zu verwalten.
PR.PT-3	Das Prinzip der geringsten Funktionalität wird durch die Konfiguration von Systemen umgesetzt, die nur die wesentlichen Funktionen bereitstellen.	redshift-enhanced-vpc-routing-aktiviert	Mit Enhanced-VPC-Routing wird erzwungen, dass der gesamte COPY- und UNLOAD-Datenverkehr zwischen Ihrem Cluster und Datenrepositorys über Ihre Amazon VPC erfolgt. Anschließend können Sie VPC-Features wie Sicherheitsgruppen und Netzwerkzugriffskontrolllisten verwenden, um den Netzwerkverkehr zu schützen. Sie können auch VPC-Flow-Logs verwenden, um den Netzwerkverkehr zu überwachen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.PT-3	Das Prinzip der geringsten Funktionalität wird durch die Konfiguration von Systemen umgesetzt, die nur die wesentlichen Funktionen bereitstellen.	ssm-document-not-public	Stellen Sie sicher, dass AWS Systems Manager (SSM) - Dokumente nicht öffentlich sind, da dies einen unbeabsichtigten Zugriff auf Ihre SSM-Dokumente ermöglichen kann. Ein öffentliches SSM-Dokument kann Informationen über Ihr Konto, Ihre Ressourcen und internen Prozesse preisgeben.
PR.PT-3	Das Prinzip der geringsten Funktionalität wird durch die Konfiguration von Systemen umgesetzt, die nur die wesentlichen Funktionen bereitstellen.	dms-replication-not-public	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass auf DMS-Replikationsinstanzen nicht öffentlich zugegriffen werden kann. DMS-Replikations-Instances können vertrauliche Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.PT-3	Das Prinzip der geringsten Funktionalität wird durch die Konfiguration von Systemen umgesetzt, die nur die wesentlichen Funktionen bereitstellen.	ebs-snapshot-public-restorable-überprüfen	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass EBS-Snapshots nicht öffentlich wiederherstellbar sind. EBS-Volume-Snapshots können vertrauliche Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.
PR.PT-3	Das Prinzip der geringsten Funktionalität wird durch die Konfiguration von Systemen umgesetzt, die nur die wesentlichen Funktionen bereitstellen.	ec-2 instance-no-public-ip	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon Elastic Compute Cloud (Amazon EC2) - Instances nicht öffentlich zugänglich sind. EC2Amazon -Instances können vertrauliche Informationen enthalten, und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.PT-3	Das Prinzip der geringsten Funktionalität wird durch die Konfiguration von Systemen umgesetzt, die nur die wesentlichen Funktionen bereitstellen.	elasticsearch-in-vpc-only	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass sich Amazon OpenSearch OpenSearch Service (Service) - Domains innerhalb einer Amazon Virtual Private Cloud (Amazon VPC) befinden. Eine OpenSearch Service-Domain innerhalb einer Amazon VPC ermöglicht die sichere Kommunikation zwischen OpenSearch Service und anderen Services innerhalb der Amazon VPC, ohne dass ein Internet-Gateway, ein NAT-Gerät oder eine VPN-Verbindung erforderlich ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.PT-3	Das Prinzip der geringsten Funktionalität wird durch die Konfiguration von Systemen umgesetzt, die nur die wesentlichen Funktionen bereitstellen.	emr-master-no-public-ip	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon EMR-Cluster-Masterknoten nicht öffentlich zugänglich sind. Amazon-EMR-Cluster-Hauptknoten können vertrauliche Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.PT-3	Das Prinzip der geringsten Funktionalität wird durch die Konfiguration von Systemen umgesetzt, die nur die wesentlichen Funktionen bereitstellen.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) kann Ihnen dabei helfen, die Prinzipien der geringsten Rechte und der Aufgabentrennung in Zugriffsberechtigungen und Autorisierungen zu integrieren und so zu verhindern, dass Richtlinien „Effect“: „Allow“ mit „Action“: „*“ anstelle von „Resource“: „*“ enthalten. Wenn Benutzern mehr Rechte eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Rechte und der Aufgabentrennung verstoßen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.PT-3	Das Prinzip der geringsten Funktionalität wird durch die Konfiguration von Systemen umgesetzt, die nur die wesentlichen Funktionen bereitstellen.	iam-root-access-key-überprüfen	Der Zugriff auf Systeme und Ressourcen kann gesteuert werden, indem überprüft wird, ob der Root-Benutzer keine Zugriffsschlüssel mit seiner AWS Identity and Access Management (IAM) -Rolle verknüpft hat. Stellen Sie sicher, dass die Root-Zugriffsschlüssel gelöscht werden. Erstellen und verwenden Sie stattdessen rollenbasierte Funktionen, AWS-Konten um das Prinzip der geringsten Funktionalität zu berücksichtigen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.PT-3	Das Prinzip der geringsten Funktionalität wird durch die Konfiguration von Systemen umgesetzt, die nur die wesentlichen Funktionen bereitstellen.	iam-user-no-policies-überprüfen	Diese Regel stellt sicher, dass AWS Identity and Access Management (IAM)-Richtlinien nur Gruppen oder Rollen zugewiesen werden, um den Zugriff auf Systeme und Ressourcen zu kontrollieren. Die Zuweisung von Berechtigungen auf Gruppen- oder Rollenebene trägt dazu bei, die Wahrscheinlichkeit zu verringern, dass eine Identität übermäßige Berechtigungen erhält oder beibehält.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.PT-3	Das Prinzip der geringsten Funktionalität wird durch die Konfiguration von Systemen umgesetzt, die nur die wesentlichen Funktionen bereitstellen.	lambda-function-public-access-verboten	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass AWS Lambda-Funktionen nicht öffentlich zugänglich sind. Der öffentliche Zugriff kann möglicherweise die Verfügbarkeit von Ressourcen beeinträchtigen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.PT-3	Das Prinzip der geringsten Funktionalität wird durch die Konfiguration von Systemen umgesetzt, die nur die wesentlichen Funktionen bereitstellen.	lambda-inside-vpc	Stellen Sie AWS Lambda-Funktionen in einer Amazon Virtual Private Cloud (Amazon VPC) bereit, um eine sichere Kommunikation zwischen einer Funktion und anderen Diensten innerhalb der Amazon VPC zu gewährleisten. Bei dieser Konfiguration sind kein Internet-Gateway, kein NAT-Gerät und keine VPN-Verbindung erforderlich. Der gesamte Datenverkehr bleibt sicher in der Cloud. AWS Domains, die sich innerhalb einer VPC befinden, verfügen aufgrund ihrer logischen Isolierung im Vergleich zu Domains mit öffentlichen Endpunkten über eine zusätzliche Sicherheitsebene. Um den Zugriff ordnungsgemäß zu verwalten,

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			sollten AWS Lambda-Funktionen einer VPC zugewiesen werden.
PR.PT-3	Das Prinzip der geringsten Funktionalität wird durch die Konfiguration von Systemen umgesetzt, die nur die wesentlichen Funktionen bereitstellen.	opensearch-in-vpc-only	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass sich Amazon OpenSearch Service-Domains innerhalb einer Amazon Virtual Private Cloud (Amazon VPC) befinden. Eine Amazon OpenSearch Service-Domain innerhalb einer Amazon VPC ermöglicht die sichere Kommunikation zwischen Amazon OpenSearch Service und anderen Services innerhalb der Amazon VPC, ohne dass ein Internet-Gateway, ein NAT-Gerät oder eine VPN-Verbindung erforderlich ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.PT-3	Das Prinzip der geringsten Funktionalität wird durch die Konfiguration von Systemen umgesetzt, die nur die wesentlichen Funktionen bereitstellen.	rds-instance-public-access-überprüfen	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Relational Database Service (Amazon RDS) -Instances nicht öffentlich sind. Amazon-RDS-Datenbank-Instances können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.PT-3	Das Prinzip der geringsten Funktionalität wird durch die Konfiguration von Systemen umgesetzt, die nur die wesentlichen Funktionen bereitstellen.	rds-snapshots-public-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Relational Database Service (Amazon RDS) -Instances nicht öffentlich sind. Amazon-RDS-Datenbank-Instances können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.PT-3	Das Prinzip der geringsten Funktionalität wird durch die Konfiguration von Systemen umgesetzt, die nur die wesentlichen Funktionen bereitstellen.	redshift-cluster-public-access-überprüfen	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Redshift Redshift-Cluster nicht öffentlich sind. Amazon-Redshift-Cluster können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.PT-3	Das Prinzip der geringsten Funktionalität wird durch die Konfiguration von Systemen umgesetzt, die nur die wesentlichen Funktionen bereitstellen.	s3- -Block-periodisch account-level-public-access	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Simple Storage Service (Amazon S3) -Buckets nicht öffentlich zugänglich sind. Diese Regel trägt dazu bei, sensible Daten vor unbefugten Remote-Benutzern zu schützen, indem sie den öffentlichen Zugriff verhindert. Mit dieser Regel können Sie optional die Parameter ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) und restrictPublicBuckets Parameter (Config Default: True) festlegen. Die tatsächlichen Werte müssen den Richtlini

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			en Ihrer Organisation entsprechen.
PR.PT-3	Das Prinzip der geringsten Funktionalität wird durch die Konfiguration von Systemen umgesetzt, die nur die wesentlichen Funktionen bereitstellen.	s3 bucket-level-public-access - verboten	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Simple Storage Service (Amazon S3) -Buckets nicht öffentlich zugänglich sind. Diese Regel trägt dazu bei, sensible Daten vor unbefugten Remote-Benutzern zu schützen, indem sie den öffentlichen Zugriff auf Bucket-Ebene verhindert.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.PT-3	Das Prinzip der geringsten Funktionalität wird durch die Konfiguration von Systemen umgesetzt, die nur die wesentlichen Funktionen bereitstellen.	s-3 bucket-public-read-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie nur autorisierten Benutzern, Prozessen und Geräten Zugriff auf Amazon Simple Storage Service (Amazon S3) - Buckets gewähren. Die Verwaltung des Zugriffs sollte mit der Klassifizierung der Daten übereinstimmen.
PR.PT-3	Das Prinzip der geringsten Funktionalität wird durch die Konfiguration von Systemen umgesetzt, die nur die wesentlichen Funktionen bereitstellen.	s3- bucket-public-write-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie nur autorisierten Benutzern, Prozessen und Geräten Zugriff auf Amazon Simple Storage Service (Amazon S3) - Buckets gewähren. Die Verwaltung des Zugriffs sollte mit der Klassifizierung der Daten übereinstimmen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.PT-3	Das Prinzip der geringsten Funktionalität wird durch die Konfiguration von Systemen umgesetzt, die nur die wesentlichen Funktionen bereitstellen.	sagemaker-notebook-no-direct-Internetzugang	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass SageMaker Amazon-Notebooks keinen direkten Internetzugang zulassen. Indem Sie direkten Internetzugang blockieren, vermeiden Sie, dass unbefugte Benutzer auf sensible Daten zugreifen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.PT-3	Das Prinzip der geringsten Funktionalität wird durch die Konfiguration von Systemen umgesetzt, die nur die wesentlichen Funktionen bereitstellen.	subnet-auto-assign-public-ip-deaktiviert	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon Virtual Private Cloud (VPC) -Subnetzen nicht automatisch eine öffentliche IP-Adresse zugewiesen wird. Amazon Elastic Compute Cloud (EC2) -Instances, die in Subnetzen gestartet werden, in denen dieses Attribut aktiviert ist, haben ihrer primären Netzwerkschnittstelle eine öffentliche IP-Adresse zugewiesen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.PT-4	Kommunikations- und Kontrollnetzwerke sind geschützt	autoscaling-launch-config-public-ip-deaktiviert	Wenn Sie Ihre Netzwerkschnittstellen mit einer öffentlichen IP-Adresse konfigurieren, sind die diesen Netzwerkschnittstellen zugehörigen Ressourcen über das Internet erreichbar. EC2 Ressourcen sollten nicht öffentlich zugänglich sein, da dies einen unbeabsichtigten Zugriff auf Ihre Anwendungen oder Server ermöglichen kann.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.PT-4	Kommunikations- und Kontrollnetzwerke sind geschützt	ec2- instances-in-vpc	Stellen Sie Amazon Elastic Compute Cloud (Amazon EC2) -Instances innerhalb einer Amazon Virtual Private Cloud (Amazon VPC) bereit, um eine sichere Kommunika tion zwischen einer Instance und anderen Services innerhalb der Amazon VPC zu ermöglichen, ohne dass ein Internet-Gateway, ein NAT-Gerät oder eine VPN-Verbindung erforderlich ist. Der gesamte Datenverk ehr bleibt sicher in der AWS Cloud. Domains, die sich innerhalb einer VPC befinden, verfügen aufgrund ihrer logischen Isolierun g im Vergleich zu Domains mit öffentlic hen Endpunkten über eine zusätzlic he Sicherheitsebene. Weisen Sie EC2

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			Amazon-Instances einer Amazon-VPC zu, um den Zugriff ordnungsgemäß zu verwalten.
PR.PT-4	Kommunikations- und Kontrollnetzwerke sind geschützt	no-unrestricted-route-to-igw	Stellen Sie sicher, dass EC2 Amazon-Routentabellen keine uneingeschränkten Routen zu einem Internet-Gateway enthalten. Durch das Entfernen oder Beschränken des Internetzugangs für Workloads innerhalb von Amazon VPCs können unbeabsic htigte Zugriffe in Ihrer Umgebung reduziert werden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.PT-4	Kommunikations- und Kontrollnetzwerke sind geschützt	ssm-document-not-public	Stellen Sie sicher, dass AWS Systems Manager (SSM) - Dokumente nicht öffentlich sind, da dies einen unbeabsichtigten Zugriff auf Ihre SSM-Dokumente ermöglichen kann. Ein öffentliches SSM-Dokument kann Informationen über Ihr Konto, Ihre Ressourcen und internen Prozesse preisgeben.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.PT-4	Kommunikations- und Kontrollnetzwerke sind geschützt	acm-certificate-expiration-check	Stellen Sie sicher, dass die Netzwerkintegrität geschützt ist, indem Sie sicherstellen, dass X509-Zertifikate von ACM ausgestellt werden. AWS Diese Zertifikate müssen gültig und dürfen nicht abgelaufen sein. Für diese Regel ist ein Wert für erforderlich daysToExpiration (Wert für bewährte AWS Grundregeln für Sicherheit: 90). Der tatsächliche Wert muss den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.PT-4	Kommunikations- und Kontrollnetzwerke sind geschützt	dms-replication-not-public	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass auf DMS-Replikationsin stanzen nicht öffentlic h zugegriffen werden kann. DMS-Repli kations-Instances können vertrauli che Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.
PR.PT-4	Kommunikations- und Kontrollnetzwerke sind geschützt	ebs-snapshot-public-restorable-überprüfen	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass EBS-Snapshots nicht öffentlich wiederher stellbar sind. EBS-Volume-Snapsho ts können vertrauli che Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.PT-4	Kommunikations- und Kontrollnetzwerke sind geschützt	ec-2 instance-no-public-ip	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon Elastic Compute Cloud (Amazon EC2) - Instances nicht öffentlich zugänglic h sind. EC2Amazon -Instances können vertrauliche Informati onen enthalten, und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.PT-4	Kommunikations- und Kontrollnetzwerke sind geschützt	elasticsearch-in-vpc-only	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass sich Amazon OpenSearch OpenSearch Service (Service) - Domains innerhalb einer Amazon Virtual Private Cloud (Amazon VPC) befinden. Eine OpenSearch Service-Domain innerhalb einer Amazon VPC ermöglicht die sichere Kommunikation zwischen OpenSearch Service und anderen Services innerhalb der Amazon VPC, ohne dass ein Internet-Gateway, ein NAT-Gerät oder eine VPN-Verbindung erforderlich ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.PT-4	Kommunikations- und Kontrollnetzwerke sind geschützt	emr-master-no-public-ip	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon EMR-Cluster-Masterknoten nicht öffentlich zugänglich sind. Amazon-EMR-Cluster-Hauptknoten können vertrauliche Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.PT-4	Kommunikations- und Kontrollnetzwerke sind geschützt	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) Security Groups können bei der Verwaltung des Netzwerkzugriffs helfen, indem sie eine statusbeh aftete Filterung von eingehendem und ausgehendem Netzwerkverkehr zu Ressourcen bereitste llen. AWS Wenn Sie eingehenden (oder entfernten) Datenverk ehr von 0.0.0.0/0 bis Port 22 auf Ihren Ressourcen nicht zulassen, können Sie den Fernzugriff einschränken.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.PT-4	Kommunikations- und Kontrollnetzwerke sind geschützt	lambda-function-public-access-verboten	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass AWS Lambda-Funktionen nicht öffentlich zugänglich sind. Der öffentliche Zugriff kann möglicherweise die Verfügbarkeit von Ressourcen beeinträchtigen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.PT-4	Kommunikations- und Kontrollnetzwerke sind geschützt	lambda-inside-vpc	Stellen Sie AWS Lambda-Funktionen in einer Amazon Virtual Private Cloud (Amazon VPC) bereit, um eine sichere Kommunika tion zwischen einer Funktion und anderen Diensten innerhalb der Amazon VPC zu gewährleisten. Bei dieser Konfiguration sind kein Internet-Gateway, kein NAT-Gerät und keine VPN-Verbindung erforderlich. Der gesamte Datenverk ehr bleibt sicher in der Cloud. AWS Domains, die sich innerhalb einer VPC befinden, verfügen aufgrund ihrer logischen Isolierun g im Vergleich zu Domains mit öffentlic hen Endpunkten über eine zusätzliche Sicherheitsebene. Um den Zugriff ordnungsg emäß zu verwalten,

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			sollten AWS Lambda-Funktionen einer VPC zugewiesen werden.
PR.PT-4	Kommunikations- und Kontrollnetzwerke sind geschützt	opensearch-in-vpc-only	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass sich Amazon OpenSearch Service-Domains innerhalb einer Amazon Virtual Private Cloud (Amazon VPC) befinden. Eine Amazon OpenSearch Service-Domain innerhalb einer Amazon VPC ermöglicht die sichere Kommunikation zwischen Amazon OpenSearch Service und anderen Services innerhalb der Amazon VPC, ohne dass ein Internet-Gateway, ein NAT-Gerät oder eine VPN-Verbindung erforderlich ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.PT-4	Kommunikations- und Kontrollnetzwerke sind geschützt	rds-instance-public-access-überprüfen	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Relational Database Service (Amazon RDS) -Instances nicht öffentlich sind. Amazon-RDS-Datenbank-Instances können vertrauliche Informationen enthalten und für solche Konten sind Grundsätze und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.PT-4	Kommunikations- und Kontrollnetzwerke sind geschützt	rds-snapshots-public-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Relational Database Service (Amazon RDS) -Instances nicht öffentlich sind. Amazon-RDS-Datenbank-Instances können vertrauliche Informationen enthalten, und für solche Konten sind Prinzipien und eine Zugriffskontrolle erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.PT-4	Kommunikations- und Kontrollnetzwerke sind geschützt	redshift-cluster-public-access-überprüfen	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Redshift Redshift-Cluster nicht öffentlich sind. Amazon-Redshift-Cluster können vertrauliche Informationen enthalten und für solche Konten sind Prinzipale und eine Zugriffskontrolle erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.PT-4	Kommunikations- und Kontrollnetzwerke sind geschützt	restricted-common-ports	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass gemeinsame Ports für Amazon Elastic Compute Cloud (Amazon EC2) -Sicherheitsgruppen eingeschränkt sind. Wenn der Zugriff auf Ports nicht auf vertrauenswürdige Quellen beschränkt wird, kann dies zu Angriffen auf die Verfügbarkeit, Integrität und Vertraulichkeit von Systemen führen. Mit dieser Regel können Sie optional die Parameter blockedPort1–blockedPort5 festlegen (Standardkonfigurationen: 20, 21, 3389, 3306, 4333). Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.PT-4	Kommunikations- und Kontrollnetzwerke sind geschützt	s3- account-level-public-access -Block-periodisch	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Simple Storage Service (Amazon S3) -Buckets nicht öffentlich zugänglich sind. Diese Regel trägt dazu bei, sensible Daten vor unbefugten Remote-Benutzern zu schützen, indem sie den öffentlichen Zugriff verhindert. Mit dieser Regel können Sie optional die Parameter ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) und restrictPublicBuckets Parameter (Config Default: True) festlegen. Die tatsächlichen Werte müssen den Richtlini

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			en Ihrer Organisation entsprechen.
PR.PT-4	Kommunikations- und Kontrollnetzwerke sind geschützt	s3- bucket-public-read -prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie nur autorisierten Benutzern, Prozessen und Geräten Zugriff auf Amazon Simple Storage Service (Amazon S3) - Buckets gewähren. Die Verwaltung des Zugriffs sollte mit der Klassifizierung der Daten übereinst immen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.PT-4	Kommunikations- und Kontrollnetzwerke sind geschützt	s3- bucket-public-write-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie nur autorisierten Benutzern, Prozessen und Geräten Zugriff auf Amazon Simple Storage Service (Amazon S3) - Buckets gewähren. Die Verwaltung des Zugriffs sollte mit der Klassifizierung der Daten übereinstimmen.
PR.PT-4	Kommunikations- und Kontrollnetzwerke sind geschützt	sagemaker-notebook-no-direct-Internetzugang	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass SageMaker Amazon-Notebooks keinen direkten Internetzugang zulassen. Indem Sie direkten Internetzugang blockieren, vermeiden Sie, dass unbefugte Benutzer auf sensible Daten zugreifen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.PT-4	Kommunikations- und Kontrollnetzwerke sind geschützt	subnet-auto-assign-public-ip-deaktiviert	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon Virtual Private Cloud (VPC) -Subnetzen nicht automatisch eine öffentliche IP-Adresse zugewiesen wird. Amazon Elastic Compute Cloud (EC2) -Instances, die in Subnetzen gestartet werden, in denen dieses Attribut aktiviert ist, haben ihrer primären Netzwerkschnittstelle eine öffentliche IP-Adresse zugewiesen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.PT-4	Kommunikations- und Kontrollnetzwerke sind geschützt	vpc-default-security-group-geschlossen	Sicherheitsgruppen von Amazon Elastic Compute Cloud (Amazon EC2) können bei der Verwaltung des Netzwerkzugriffs helfen, indem sie eine statusbehaftete Filterung des ein- und ausgehenden Netzwerkverkehrs zu Ressourcen bereitstellen. AWS Die Beschränk ung des gesamten Datenverkehrs auf die Standardsicherheit sgruppe hilft dabei, den Fernzugriff auf Ihre Ressourcen einzuschränken. AWS

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.PT-4	Kommunikations- und Kontrollnetzwerke sind geschützt	vpc-sg-open-only-to-authorized-ports	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass gemeinsame Ports für Amazon Elastic Compute Cloud (Amazon EC2) -Sicherheitsgruppen eingeschränkt sind. Wenn der Zugriff auf Ports nicht auf vertrauenswürdige Quellen beschränkt wird, kann dies zu Angriffen auf die Verfügbarkeit, Integrität und Vertraulichkeit von Systemen führen. Durch die Beschränkung des Zugriffs auf Ressourcen innerhalb einer Sicherheitsgruppe aus dem Internet (0.0.0.0/0) kann der Fernzugriff auf interne Systeme gesteuert werden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
DE.CM-8	Sicherheitslückenscans werden durchgeführt.	vuln-scans-performed (Prozessüberprüfung)	Stellen Sie sicher, dass Schwachstellenscans gemäß Ihren Compliance-Anforderungen durchgeführt werden. Die Häufigkeit der Scans, die verwendeten Tools und die Verwendung der Ergebnisse sollten von Ihrer Organisation festgelegt werden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
RS.MI-3	Neu erkannte Schwachstellen werden gemildert oder als akzeptierte Risiken dokumentiert.	vuln-mitigated-accepted (Prozessüberprüfung)	Stellen Sie sicher, dass neu identifizierte Schwachstellen behoben oder als akzeptierte Risiken dokumentiert werden. Dienste wie AWS Security Hub, Amazon Guard Duty, Amazon Inspector und AWS Config können Sie bei der Identifizierung von Sicherheitslücken in Ihrer Umgebung unterstützen. Schwachstellen sollten entsprechend den Compliance-Anforderungen Ihrer Organisation behoben oder als Risiken akzeptiert werden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
RS.MI-3	Neu erkannte Schwachstellen werden gemildert oder als akzeptierte Risiken dokumentiert	guardduty-non-archived-findings	Amazon GuardDuty hilft Ihnen dabei, die Auswirkungen eines Vorfalls zu verstehen, indem es die Ergebnisse nach Schweregrad klassifiziert: niedrig, mittel und hoch. Diese Klassifizierungen können Sie zur Festlegung von entsprechenden Strategien und Prioritäten zur Behebung solcher Vorfälle verwenden. Mit dieser Regel können Sie optional daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7) und daysHighSev (Config Default: 1) für nicht archivierte Ergebnisse festlegen, wie es die Richtlinien Ihrer Organisation erfordern.

Vorlage

Die Vorlage ist verfügbar unter GitHub: Operational Best Practices for NIST 1800 25.

Bewährte Methoden für die Ausführung von NIST CSF

Konformitätspakete bieten ein allgemeines Compliance-Framework, das es Ihnen ermöglicht, mithilfe verwalteter oder benutzerdefinierter Regeln und Abhilfemaßnahmen Kontrollen zur Sicherheits-, Betriebs- oder Kostenoptimierung durchzuführen. AWS Config AWS Config Conformance Packs dienen als Beispielvorlagen nicht dazu, die vollständige Einhaltung eines bestimmten Governance- oder Compliance-Standards sicherzustellen. Sie sind dafür verantwortlich, selbst zu beurteilen, ob Ihre Nutzung der Services den geltenden gesetzlichen und behördlichen Anforderungen entspricht.

Im Folgenden finden Sie ein Beispiel für eine Zuordnung zwischen dem NIST Cyber Security Framework (CSF) und den AWS verwalteten Konfigurationsregeln. Jede AWS Config Regel gilt für eine bestimmte AWS Ressource und bezieht sich auf eine oder mehrere NIST-CSF-Steuerelemente. Eine Kontrolle nach NIST CSF kann mehreren Konfigurationsregeln zugeordnet werden. In der folgenden Tabelle finden Sie weitere Informationen und Anleitungen zu diesen Zuordnungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
DE.AE-1	Es wird eine Grundlage für den Netzwerkbetrieb und die zu erwartend en Datenflüsse für Benutzer und Systeme erstellt und verwaltet	elasticsearch-logs-to-cloudwatch	Stellen Sie sicher, dass für Amazon OpenSearch Service-Domains Fehlerpro tokolle aktiviert und zur Aufbewahrung und Beantwortung an Amazon CloudWatc h Logs gestreamt werden. Domain-Fehlerprotokolle sind bei Sicherhei ts- und Zugriffsp rüfungen sowie bei der Diagnose von Verfügbarkeitsprob lemen nützlich.
DE.AE-1	Es wird eine Grundlage für den	multi-region-cloudtrail-enabled	AWS CloudTrail zeichnet Aktionen und

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	Netzwerkbetrieb und die zu erwartend en Datenflüsse für Benutzer und Systeme erstellt und verwaltet		API-Aufrufe der AWS Management Console auf. Sie können feststellen, welche Benutzer und Konten angerufen wurden AWS, von welcher Quell-IP-Adresse aus die Anrufe getätigt wurden und wann die Anrufe erfolgten. CloudTrail übermittelt Protokolldateien aus allen AWS Regionen an Ihren S3-Bucket , wenn MULTI_REG ION_CLOUD _TRAIL_ENABLED aktiviert ist. Außerdem wird beim AWS Start einer neuen Region derselbe Trail in der neuen Region erstellt. CloudTrail Dadurch erhalten Sie automatis ch Protokolldateien mit API-Aktivitäten für die neue Region.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
DE.AE-1	Es wird eine Grundlage für den Netzwerkbetrieb und die zu erwartend en Datenflüsse für Benutzer und Systeme erstellt und verwaltet	no-unrestricted-route-to-igw	Stellen Sie sicher, dass EC2 Amazon-Routentabellen keine uneingeschränkten Routen zu einem Internet-Gateway enthalten. Durch das Entfernen oder Beschränken des Internetzugangs für Workloads innerhalb von Amazon VPCs können unbeabsic htigte Zugriffe in Ihrer Umgebung reduziert werden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
DE.AE-1	Es wird eine Grundlage für den Netzwerkbetrieb und die zu erwartend en Datenflüsse für Benutzer und Systeme erstellt und verwaltet	opensearch-logs-to-cloudwatch	Stellen Sie sicher, dass für Amazon OpenSearch Service-Domains Fehlerpro tokolle aktiviert und zur Aufbewahr ung und Beantwort ung an Amazon CloudWatch Logs gestreamt werden. OpenSearch Service-Fehlerprotokolle können bei Sicherhei ts- und Zugriffsp rüfungen helfen und bei der Diagnose von Verfügbarkeitsprob lemen helfen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
DE.AE-1	Es wird eine Grundlage für den Netzwerkbetrieb und die zu erwartenden Datenflüsse für Benutzer und Systeme erstellt und verwaltet	wafv2-logging-enabled	Um die Protokollierung und Überwachung in Ihrer Umgebung zu erleichtern, aktivieren Sie die AWS WAF (V2) -Protokollierung im regionalen und globalen Internet ACLs. AWS Die WAF-Protokollierung bietet detaillierte Informationen über den Datenverkehr, der von Ihrer Web-ACL analysiert wird. In den Protokollen werden die Uhrzeit aufgezeichnet, zu der die AWS WAF die Anfrage von Ihrer AWS Ressource erhalten hat, Informationen zu der Anfrage und eine Aktion für die Regel, der jede Anfrage entsprach.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
DE.AE-1	Es wird eine Grundlage für den Netzwerkbetrieb und die zu erwartend en Datenflüsse für Benutzer und Systeme erstellt und verwaltet	api-gw-execution-l ogging-aktiviert	Die API-Gateway-Protokollierung zeigt detaillierte Ansichten der Benutzer, die auf die API zugegriff en haben, und wie diese Benutzer auf die API zugegriffen haben. Diese Insights ermöglichen die Einsicht in Benutzera ktivitäten.
DE.AE-1	Es wird eine Grundlage für den Netzwerkbetrieb und die zu erwartend en Datenflüsse für Benutzer und Systeme erstellt und verwaltet	cloud-trail-cloud-watch-logs-aktiviert	Verwenden Sie Amazon CloudWatc h , um Protokoll ereignisaktivitäten zentral zu sammeln und zu verwalten. Die Aufnahme von AWS CloudTrail Daten liefert Einzelheiten zu den API-Aufrufaktivitä ten in Ihrem AWS-Konto.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
DE.AE-1	Es wird eine Grundlage für den Netzwerkbetrieb und die zu erwartend en Datenflüsse für Benutzer und Systeme erstellt und verwaltet	cloudtrail-enabled	AWS CloudTrail kann bei der Nichtabst reitbarkeit helfen, indem Aktionen und API-Aufrufe der AWS Management Console aufgezeic hnet werden. Sie können die Benutzer und die Benutzer AWS-Konten , die einen AWS Dienst aufgerufen haben, die Quell-IP-Adresse, über die die Aufrufe generiert wurden, und den Zeitpunkt der Anrufe identifiz ieren. Einzelheiten zu den erfassten Daten finden Sie in den AWS CloudTrail Datensatzinhalten.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
DE.AE-1	Es wird eine Grundlage für den Netzwerkbetrieb und die zu erwartend en Datenflüsse für Benutzer und Systeme erstellt und verwaltet	cloudtrail-s3-data events-enabled	Die Erfassung von Simple Storage Service (Amazon S3)-Datenereigniss en unterstützt die Erkennung von ungewöhnlichen Aktivitäten. Zu den Details gehören Informationen zu dem AWS -Konto, das auf einen Amazon-S3-Bucket zugegriffen hat, die IP-Adresse und die Uhrzeit des Ereignisses.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
DE.AE-1	Es wird eine Grundlage für den Netzwerkbetrieb und die zu erwartend en Datenflüsse für Benutzer und Systeme erstellt und verwaltet	elb-logging-enabled	Die Elastic-Load-Balancing-Aktivität ist ein zentraler Kommunikationspunk t innerhalb einer Umgebung. Stellen Sie sicher, dass die ELB-Protokollierun g aktiviert ist. Die gesammelten Daten enthalten detaillie rte Informationen zu Anfragen, die an den ELB gesendet wurden. Jedes Protokoll enthält Informationen wie die Zeit, zu der die Anforderung einging, die Client-IP -Adresse, Latenzen, Anforderungspfade und Serverantworten.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
DE.AE-1	Es wird eine Grundlage für den Netzwerkbetrieb und die zu erwartend en Datenflüsse für Benutzer und Systeme erstellt und verwaltet	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) Security Groups können bei der Verwaltung des Netzwerkzugriffs helfen, indem sie eine statusbeh aftete Filterung von eingehendem und ausgehendem Netzwerkverkehr zu Ressourcen bereitste llen. AWS Wenn Sie eingehenden (oder entfernten) Datenverk ehr von 0.0.0.0/0 bis Port 22 auf Ihren Ressourcen nicht zulassen, können Sie den Remote-Zugriff einschränken.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
DE.AE-1	Es wird eine Grundlage für den Netzwerkbetrieb und die zu erwartend en Datenflüsse für Benutzer und Systeme erstellt und verwaltet	rds-logging-enabled	Um die Protokoll ierung und Überwachung in Ihrer Umgebung zu erleichtern, stellen Sie sicher, dass die Amazon Relationa l Database Service (Amazon RDS)-Prot okollierung aktiviert ist. Mit der Amazon-RDS-Protokollierung können Sie Ereigniss e wie Verbindungen, Verbindungsabbrüch e, Abfragen oder abgefragte Tabellen erfassen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
DE.AE-1	Es wird eine Grundlage für den Netzwerkbetrieb und die zu erwartend en Datenflüsse für Benutzer und Systeme erstellt und verwaltet	redshift-cluster-c onfiguration-check	Um Daten im Ruhezustand zu schützen, muss die Verschlüsselung für Ihre Amazon-Re dshift-Cluster aktiviert sein. Sie müssen auch sicherstellen, dass die erforderl ichen Konfigurationen auf Amazon-Redshift-Clustern bereitges tellt werden. Die Prüfungsprotokolli erung muss aktiviert sein, um Informati onen zu Verbindun gen und Benutzera ktivitäten in der Datenbank bereitzus tellen. Diese Regel erfordert, dass ein Wert für clusterDb Encrypted (Config Default: TRUE) und LoggingEnabled (Config Default: TRUE) gesetzt ist. Die tatsächlichen Werte müssen den Richtlini en Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
DE.AE-1	Es wird eine Grundlage für den Netzwerkbetrieb und die zu erwartend en Datenflüsse für Benutzer und Systeme erstellt und verwaltet	restricted-common-ports	Verwalten Sie den Zugriff auf Ressource n in der AWS Cloud, indem Sie sicherste llen, dass gemeinsam e Ports für Amazon Elastic Compute Cloud (Amazon EC2) -Sicherhe itsgruppen eingeschr ränkt sind. Wenn der Zugriff auf Ports nicht auf vertrauen swürdige Quellen beschränkt wird, kann dies zu Angriffen auf die Verfügbar keit, Integrität und Vertraulichkeit von Systemen führen. Mit dieser Regel können Sie optional die Parameter blockedPo rt1–blockedPort5 festlegen (Standard konfigurationen: 20, 21, 3389, 3306, 4333). Die tatsächli chen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
DE.AE-1	Es wird eine Grundlage für den Netzwerkbetrieb und die zu erwartend en Datenflüsse für Benutzer und Systeme erstellt und verwaltet	s-3 bucket-logging-enabled	Die Amazon Simple Storage Service (Amazon S3)-Serverzugriffs protokollierung bietet eine Methode zur Überwachu ng des Netzwerks im Hinblick auf potenzielle Cybersich erheitsereignisse. Die Ereignisse werden überwacht, indem detaillierte Aufzeichn ungen über die Anfragen erfasst werden, die an einen Amazon-S3-Bucket gestellt wurden. Jeder Zugriffsprotokolle intrag enthält Details zu einer einzelnen Zugriffsanfrage. Zu den Details gehören Anforderer, Bucket-Name, Anforderu ngszeit, Anforderu ngsaktion, Antwortst atus und Fehlercode, falls relevant.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
DE.AE-1	Es wird eine Grundlage für den Netzwerkbetrieb und die zu erwartend en Datenflüsse für Benutzer und Systeme erstellt und verwaltet	vpc-default-security-group-geschlossen	Sicherheitsgruppen von Amazon Elastic Compute Cloud (Amazon EC2) können bei der Verwaltung des Netzwerkzugriffs helfen, indem sie eine statusbehaftete Filterung des ein- und ausgehenden Netzwerkverkehrs zu Ressourcen bereitstellen. AWS Die Beschränk ung des gesamten Datenverkehrs auf die Standardsicherheit sgruppe hilft dabei, den Fernzugriff auf Ihre Ressourcen einzuschränken. AWS

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
DE.AE-1	Es wird eine Grundlage für den Netzwerkbetrieb und die zu erwartenden Datenflüsse für Benutzer und Systeme erstellt und verwaltet	vpc-flow-logs-enabled	VPC-Flow-Protokolle erfassen detaillierte Informationsdatensätze über den IP-Datenverkehr, der zu und von Netzwerkschnittstellen in Ihrer Amazon Virtual Private Cloud (Amazon VPC) fließt. Standardmäßig enthalten Flow-Protokolldatensätze Werte für die verschiedenen Komponenten des IP-Flows, einschließlich Quelle, Ziel und Protokoll.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
DE.AE-1	Es wird eine Grundlage für den Netzwerkbetrieb und die zu erwartend en Datenflüsse für Benutzer und Systeme erstellt und verwaltet	vpc-sg-open-only-to-authorized-ports	Verwalten Sie den Zugriff auf Ressource n in der AWS Cloud, indem Sie sicherste llen, dass gemeinsam e Ports für Amazon Elastic Compute Cloud (Amazon EC2) -Sicherhe itsgruppen eingeschr ränkt sind. Wenn der Zugriff auf Ports nicht auf vertrauen swürdige Quellen beschränkt wird, kann dies zu Angriffen auf die Verfügbar keit, Integrität und Vertraulichkeit von Systemen führen. Durch die Beschränk ung des Zugriffs auf Ressourcen innerhalb einer Sicherhei tsgruppe aus dem Internet (0.0.0.0/0) kann der Fernzugriff auf interne Systeme gesteuert werden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
DE.AE-2	Die erkannten Ereignisse werden analysiert, um die Ziele und Methoden der Angriffe besser zu verstehen	guardduty-non-archived-findings	Amazon GuardDuty hilft Ihnen dabei, die Auswirkungen eines Vorfalls zu verstehen, indem es die Ergebnisse nach Schweregrad klassifiziert: niedrig, mittel und hoch. Diese Klassifizierungen können Sie zur Festlegung von entsprechenden Strategien und Prioritäten zur Behebung solcher Vorfälle verwenden. Mit dieser Regel können Sie optional daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7) und daysHighSev (Config Default: 1) für nicht archivierte Ergebnisse festlegen, wie es die Richtlinien Ihrer Organisation erfordern.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
DE.AE-2	Die erkannten Ereignisse werden analysiert, um die Ziele und Methoden der Angriffe besser zu verstehen	guardduty-enabled-centralized	Amazon GuardDuty kann mithilfe von Threat Intellige nce Feeds helfen, potenzielle Cybersich erheitsereignisse zu überwachen und zu erkennen. Dazu gehören Listen mit bösartigen IPs und maschinel len Lernmethoden zur Identifizierung unerwarteter, nicht autorisierter und bösartiger Aktivitäten in Ihrer AWS Cloud-Umgebung.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
DE.AE-3	Ereignisdaten werden aus verschiedenen Quellen und Sensoren gesammelt und korreliert	elasticsearch-logs-to-cloudwatch	Stellen Sie sicher, dass für Amazon OpenSearch Service-Domains Fehlerprotokolle aktiviert und zur Aufbewahrung und Beantwortung an Amazon CloudWatch Logs gestreamt werden. Domain-Fehlerprotokolle sind bei Sicherheits- und Zugriffsprüfungen sowie bei der Diagnose von Verfügbarkeitsproblemen nützlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
DE.AE-3	Ereignisdaten werden aus verschiedenen Quellen und Sensoren gesammelt und korreliert	multi-region-cloudtrail-enabled	AWS CloudTrail zeichnet Aktionen und API-Aufrufe der AWS Management Console auf. Sie können feststellen, welche Benutzer und Konten angerufen wurden AWS, von welcher Quell-IP-Adresse aus die Anrufe getätigt wurden und wann die Anrufe erfolgten. CloudTrail übermittelt Protokolldateien aus allen AWS Regionen an Ihren S3-Bucket , wenn MULTI_REG ION_CLOUD _TRAIL_ENABLED aktiviert ist. Außerdem wird beim AWS Start einer neuen Region derselbe Trail in der neuen Region erstellt. CloudTrail Dadurch erhalten Sie automatis ch Protokolldateien mit API-Aktivitäten für die neue Region.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
DE.AE-3	Ereignisdaten werden aus verschiedenen Quellen und Sensoren gesammelt und korreliert	opensearch-logs-to-cloudwatch	Stellen Sie sicher, dass für Amazon OpenSearch Service-Domains Fehlerprotokolle aktiviert und zur Aufbewahrung und Beantwortung an Amazon CloudWatch Logs gestreamt werden. OpenSearch Service-Fehlerprotokolle können bei Sicherheits- und Zugriffsprüfungen helfen und bei der Diagnose von Verfügbarkeitsproblemen helfen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
DE.AE-3	Ereignisdaten werden aus verschiedenen Quellen und Sensoren gesammelt und korreliert	wafv2-logging-enabled	Um die Protokollierung und Überwachung in Ihrer Umgebung zu erleichtern, aktivieren Sie die AWS WAF (V2) -Protokollierung im regionalen und globalen Internet ACLs. AWS Die WAF-Protokollierung bietet detaillierte Informationen über den Datenverkehr, der von Ihrer Web-ACL analysiert wird. In den Protokollen werden die Uhrzeit aufgezeichnet, zu der die AWS WAF die Anfrage von Ihrer AWS Ressource erhalten hat, Informationen zu der Anfrage und eine Aktion für die Regel, der jede Anfrage entsprach.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
DE.AE-3	Ereignisdaten werden aus verschiedenen Quellen und Sensoren gesammelt und korreliert	api-gw-execution-logging-aktiviert	Die API-Gateway-Protokollierung zeigt detaillierte Ansichten der Benutzer, die auf die API zugegriffen haben, und wie diese Benutzer auf die API zugegriffen haben. Diese Insights ermöglichen die Einsicht in Benutzeraktivitäten.
DE.AE-3	Ereignisdaten werden aus verschiedenen Quellen und Sensoren gesammelt und korreliert	cloud-trail-cloud-watch-logs-aktiviert	Verwenden Sie Amazon CloudWatch , um Protokoll ereignisaktivitäten zentral zu sammeln und zu verwalten. Die Aufnahme von AWS CloudTrail Daten liefert Einzelheiten zu den API-Aufrufaktivitäten in Ihrem AWS-Konto.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
DE.AE-3	Ereignisdaten werden aus verschiedenen Quellen und Sensoren gesammelt und korreliert	cloudtrail-enabled	AWS CloudTrail kann bei der Nichtabst reitbarkeit helfen, indem Aktionen und API-Aufrufe der AWS Management Console aufgezeic hnet werden. Sie können die Benutzer und die Benutzer AWS-Konten , die einen AWS Dienst aufgerufen haben, die Quell-IP-Adresse, über die die Aufrufe generiert wurden, und den Zeitpunkt der Anrufe identifiz ieren. Einzelheiten zu den erfassten Daten finden Sie in den AWS CloudTrail Datensatzinhalten.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
DE.AE-3	Ereignisdaten werden aus verschiedenen Quellen und Sensoren gesammelt und korreliert	cloudtrail-s3-data events-enabled	Die Erfassung von Simple Storage Service (Amazon S3)-Datenereignissen unterstützt die Erkennung von ungewöhnlichen Aktivitäten. Zu den Details gehören Informationen zu dem AWS -Konto, das auf einen Amazon-S3-Bucket zugegriffen hat, die IP-Adresse und die Uhrzeit des Ereignisses.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
DE.AE-3	Ereignisdaten werden aus verschiedenen Quellen und Sensoren gesammelt und korreliert	elb-logging-enabled	Die Elastic-Load-Balancing-Aktivität ist ein zentraler Kommunikationspunkt innerhalb einer Umgebung. Stellen Sie sicher, dass die ELB-Protokollierung aktiviert ist. Die gesammelten Daten enthalten detaillierte Informationen zu Anfragen, die an den ELB gesendet wurden. Jedes Protokoll enthält Informationen wie die Zeit, zu der die Anforderung einging, die Client-IP-Adresse, Latenzen, Anforderungspfade und Serverantworten.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
DE.AE-3	Ereignisdaten werden aus verschiedenen Quellen und Sensoren gesammelt und korreliert	guardduty-enabled-centralized	Amazon GuardDuty kann mithilfe von Threat Intellige nce Feeds helfen, potenzielle Cybersich erheitsereignisse zu überwachen und zu erkennen. Dazu gehören Listen mit bösartigen IPs und maschinel len Lernmethoden zur Identifizierung unerwarteter, nicht autorisierter und bösartiger Aktivitäten in Ihrer AWS Cloud-Umgebung.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
DE.AE-3	Ereignisdaten werden aus verschiedenen Quellen und Sensoren gesammelt und korreliert	rds-logging-enabled	Um die Protokollierung und Überwachung in Ihrer Umgebung zu erleichtern, stellen Sie sicher, dass die Amazon Relational Database Service (Amazon RDS)-Protokollierung aktiviert ist. Mit der Amazon-RDS-Protokollierung können Sie Ereignisse wie Verbindungen, Verbindungsabbrüche, Abfragen oder abgefragte Tabellen erfassen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
DE.AE-3	Ereignisdaten werden aus verschiedenen Quellen und Sensoren gesammelt und korreliert	redshift-cluster-configuration-check	Um Daten im Ruhezustand zu schützen, muss die Verschlüsselung für Ihre Amazon-Redshift-Cluster aktiviert sein. Sie müssen auch sicherstellen, dass die erforderlichen Konfigurationen auf Amazon-Redshift-Clustern bereitgestellt werden. Die Prüfungsprotokollierung muss aktiviert sein, um Informationen zu Verbindungen und Benutzeraktivitäten in der Datenbank bereitzustellen. Diese Regel erfordert, dass ein Wert für clusterDbEncrypted (Config Default: TRUE) und LoggingEnabled (Config Default: TRUE) gesetzt ist. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
DE.AE-3	Ereignisdaten werden aus verschiedenen Quellen und Sensoren gesammelt und korreliert	s3- bucket-logging-enabled	Die Amazon Simple Storage Service (Amazon S3)-Serverzugriffs protokollierung bietet eine Methode zur Überwachu ng des Netzwerks im Hinblick auf potenzielle Cybersich erheitsereignisse. Die Ereignisse werden überwacht, indem detaillierte Aufzeichn ungen über die Anfragen erfasst werden, die an einen Amazon-S3-Bucket gestellt wurden. Jeder Zugriffsprotokolle intrag enthält Details zu einer einzelnen Zugriffsanfrage. Zu den Details gehören Anforderer, Bucket-Name, Anforderu ngszeit, Anforderu ngsaktion, Antwortst atus und Fehlercode, falls relevant.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
DE.AE-3	Ereignisdaten werden aus verschiedenen Quellen und Sensoren gesammelt und korreliert	vpc-flow-logs-enabled	VPC-Flow-Protokolle erfassen detaillierte Informationsdatensätze über den IP-Datenverkehr, der zu und von Netzwerkschnittstellen in Ihrer Amazon Virtual Private Cloud (Amazon VPC) fließt. Standardmäßig enthalten Flow-Protokolldatensätze Werte für die verschiedenen Komponenten des IP-Flows, einschließlich Quelle, Ziel und Protokoll.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
DE.AE-4	Die Auswirkungen der Ereignisse werden bestimmt	cloudtrail-s3-data events-enabled	Die Erfassung von Simple Storage Service (Amazon S3)-Datenereignissen unterstützt die Erkennung von ungewöhnlichen Aktivitäten. Zu den Details gehören Informationen zu dem AWS -Konto, das auf einen Amazon-S3-Bucket zugegriffen hat, die IP-Adresse und die Uhrzeit des Ereignisses.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
DE.AE-4	Die Auswirkungen der Ereignisse werden bestimmt	cloudtrail-enabled	AWS CloudTrai l kann durch die Aufzeichnung von Aktionen und API-Aufrufen in der AWS Management Console bei der Nichtabst reitbarkeit helfen. Sie können die Benutzer und die Benutzer AWS-Konten , die einen AWS Dienst aufgerufen haben, die Quell-IP-Adresse, über die die Aufrufe generiert wurden, und den Zeitpunkt der Anrufe identifiz ieren. Einzelheiten zu den erfassten Daten finden Sie in den AWS CloudTrail Datensatzinhalten.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
DE.AE-4	Die Auswirkungen der Ereignisse werden bestimmt	elb-logging-enabled	Die Elastic-Load-Balancing-Aktivität ist ein zentraler Kommunikationspunkt innerhalb einer Umgebung. Stellen Sie sicher, dass die ELB-Protokollierung aktiviert ist. Die gesammelten Daten enthalten detaillierte Informationen zu Anfragen, die an den ELB gesendet wurden. Jedes Protokoll enthält Informationen wie die Zeit, zu der die Anforderung einging, die Client-IP-Adresse, Latenzen, Anforderungspfade und Serverantworten.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
DE.AE-4	Die Auswirkungen der Ereignisse werden bestimmt	guardduty-enabled-centralized	Amazon GuardDuty kann mithilfe von Threat Intellige nce Feeds helfen, potenzielle Cybersich erheitsereignisse zu überwachen und zu erkennen. Dazu gehören Listen mit bösartigen IPs und maschinel len Lernmethoden zur Identifizierung unerwarteter, nicht autorisierter und bösartiger Aktivitäten in Ihrer AWS Cloud-Umgebung.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
DE.AE-4	Die Auswirkungen der Ereignisse werden bestimmt	guardduty-non-archived-findings	Amazon GuardDuty hilft Ihnen dabei, die Auswirkungen eines Vorfalls zu verstehen, indem es die Ergebnisse nach Schweregrad klassifiziert: niedrig, mittel und hoch. Diese Klassifizierungen können Sie zur Festlegung von entsprechenden Strategien und Prioritäten zur Behebung solcher Vorfälle verwenden. Mit dieser Regel können Sie optional daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7) und daysHighSev (Config Default: 1) für nicht archivierte Ergebnisse festlegen, wie es die Richtlinien Ihrer Organisation erfordern.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
DE.AE-4	Die Auswirkungen der Ereignisse werden bestimmt	multi-region-cloudtrail-enabled	AWS CloudTrail zeichnet Aktionen und API-Aufrufe der AWS Management Console auf. Sie können feststellen, welche Benutzer und Konten angerufen wurden AWS, von welcher Quell-IP-Adresse aus die Anrufe getätigt wurden und wann die Anrufe erfolgten. CloudTrail übermittelt Protokolldateien aus allen AWS Regionen an Ihren S3-Bucket , wenn MULTI_REG ION_CLOUD _TRAIL_ENABLED aktiviert ist. Außerdem wird beim AWS Start einer neuen Region derselbe Trail in der neuen Region erstellt. CloudTrail Dadurch erhalten Sie automatis ch Protokolldateien mit API-Aktivitäten für die neue Region.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
DE.AE-4	Die Auswirkungen der Ereignisse werden bestimmt	s-3 bucket-logging-enabled	Die Amazon Simple Storage Service (Amazon S3)-Serverzugriffs protokollierung bietet eine Methode zur Überwachu ng des Netzwerks im Hinblick auf potenzielle Cybersich erheitsereignisse. Die Ereignisse werden überwacht, indem detaillierte Aufzeichn ungen über die Anfragen erfasst werden, die an einen Amazon-S3-Bucket gestellt wurden. Jeder Zugriffsprotokolle intrag enthält Details zu einer einzelnen Zugriffsanfrage. Zu den Details gehören Anforderer, Bucket-Name, Anforderu ngszeit, Anforderu ngsaktion, Antwortst atus und Fehlercode, falls relevant.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
DE.AE-4	Die Auswirkungen der Ereignisse werden bestimmt	securityhub-enabled	AWS Security Hub hilft bei der Überwachung von unbefugtem Personal, Verbindungen, Geräten und Software. AWS Security Hub aggregiert, organisiert und priorisiert die Sicherheitswarnungen oder Ergebnisse mehrerer Dienste. AWS Einige dieser Dienste sind Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer und AWS Firewall Manager sowie AWS Partnerlösungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
DE.CM-1	Das Netzwerk wird überwacht, um potenzielle Cybersicherheitsereignisse zu erkennen	api-gw-execution-logging-aktiviert	Die API-Gateway-Protokollierung zeigt detaillierte Ansichten der Benutzer, die auf die API zugegriffen haben, und wie diese Benutzer auf die API zugegriffen haben. Diese Insights ermöglichen die Einsicht in Benutzeraktivitäten.
DE.CM-1	Das Netzwerk wird überwacht, um potenzielle Cybersicherheitsereignisse zu erkennen	cloudtrail-s3-dataevents-enabled	Die Erfassung von Simple Storage Service (Amazon S3)-Datenereignissen unterstützt die Erkennung von ungewöhnlichen Aktivitäten. Zu den Details gehören Informationen zu dem AWS -Konto, das auf einen Amazon-S3-Bucket zugegriffen hat, die IP-Adresse und die Uhrzeit des Ereignisses.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
DE.CM-1	Das Netzwerk wird überwacht, um potenzielle Cybersicherheitsereignisse zu erkennen	cloudtrail-enabled	AWS CloudTrail kann durch die Aufzeichnung von Aktionen und API-Aufrufen in der AWS Management Console bei der Nichtabstreitbarkeit helfen. Sie können die Benutzer und die Benutzer AWS-Konten , die einen AWS Dienst aufgerufen haben, die Quell-IP-Adresse, über die die Aufrufe generiert wurden, und den Zeitpunkt der Anrufe identifizieren. Einzelheiten zu den erfassten Daten finden Sie in den AWS CloudTrail Datensatzinhalten.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
DE.CM-1	Das Netzwerk wird überwacht, um potenzielle Cybersicherheitsereignisse zu erkennen	elb-logging-enabled	Die Elastic-Load-Balancing-Aktivität ist ein zentraler Kommunikationspunkt innerhalb einer Umgebung. Stellen Sie sicher, dass die ELB-Protokollierung aktiviert ist. Die gesammelten Daten enthalten detaillierte Informationen zu Anfragen, die an den ELB gesendet wurden. Jedes Protokoll enthält Informationen wie die Zeit, zu der die Anforderung einging, die Client-IP-Adresse, Latenzen, Anforderungspfade und Serverantworten.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
DE.CM-1	Das Netzwerk wird überwacht, um potenzielle Cybersich erheitsereignisse zu erkennen	guardduty-enabled-centralized	Amazon GuardDuty kann mithilfe von Threat Intellige nce Feeds helfen, potenzielle Cybersich erheitsereignisse zu überwachen und zu erkennen. Dazu gehören Listen mit bösartigen IPs und maschinel len Lernmethoden zur Identifizierung unerwarteter, nicht autorisierter und bösartiger Aktivitäten in Ihrer AWS Cloud-Umgebung.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
DE.CM-1	Das Netzwerk wird überwacht, um potenzielle Cybersich erheitsereignisse zu erkennen	multi-region-cloudtrail-enabled	AWS CloudTrail zeichnet Aktionen und API-Aufrufe der AWS Management Console auf. Sie können feststellen, welche Benutzer und Konten angerufen wurden AWS, von welcher Quell-IP-Adresse aus die Anrufe getätigt wurden und wann die Anrufe erfolgten. CloudTrail übermittelt Protokolldateien aus allen AWS Regionen an Ihren S3-Bucket , wenn MULTI_REG ION_CLOUD _TRAIL_ENABLED aktiviert ist. Außerdem wird beim AWS Start einer neuen Region derselbe Trail in der neuen Region erstellt. CloudTrail Dadurch erhalten Sie automatis ch Protokolldateien mit API-Aktivitäten für die neue Region.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
DE.CM-1	Das Netzwerk wird überwacht, um potenzielle Cybersicherheitsereignisse zu erkennen	s-3 bucket-logging-enabled	Die Amazon Simple Storage Service (Amazon S3)-Serverzugriffsprotokollierung bietet eine Methode zur Überwachung des Netzwerks im Hinblick auf potenzielle Cybersicherheitsereignisse. Die Ereignisse werden überwacht, indem detaillierte Aufzeichnungen über die Anfragen erfasst werden, die an einen Amazon-S3-Bucket gestellt wurden. Jeder Zugriffsprotokolleintrag enthält Details zu einer einzelnen Zugriffsanfrage. Zu den Details gehören Anforderer, Bucket-Name, Anforderungszeit, Anforderungsaktion, Antwortstatus und Fehlercode, falls relevant.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
DE.CM-1	Das Netzwerk wird überwacht, um potenzielle Cybersicherheitsereignisse zu erkennen	s-3 event-notifications-enabled	Amazon-S3-Ereignisbenachrichtigungen können das zuständige Personal über versehentliche oder vorsätzliche Änderungen an Ihren Bucket-Objekten informieren. Zu den Warnen gehören beispielsweise: Erstellung eines neuen Objekts, Entfernung eines Objekts, Wiederherstellung eines Objekts, verloren gegangene und replizierte Objekte.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
DE.CM-1	Das Netzwerk wird überwacht, um potenzielle Cybersicherheitsereignisse zu erkennen	securityhub-enabled	AWS Security Hub hilft bei der Überwachung von unbefugtem Personal, Verbindungen, Geräten und Software. AWS Security Hub aggregiert, organisiert und priorisiert die Sicherheitswarnungen oder Ergebnisse mehrerer Dienste. AWS Einige dieser Dienste sind Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer und AWS Firewall Manager sowie AWS Partnerlösungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
DE.CM-1	Das Netzwerk wird überwacht, um potenzielle Cybersicherheitsereignisse zu erkennen	vpc-flow-logs-enabled	VPC-Flow-Protokolle erfassen detaillierte Informationsdatensätze über den IP-Datenverkehr, der zu und von Netzwerkschnittstellen in Ihrer Amazon Virtual Private Cloud (Amazon VPC) fließt. Standardmäßig enthalten Flow-Protokolldatensätze Werte für die verschiedenen Komponenten des IP-Flows, einschließlich Quelle, Ziel und Protokoll.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
DE.CM-3	Die Aktivitäten der Mitarbeiter werden überwacht, um potenzielle Cybersicherheitsvorfälle zu erkennen.	cloudtrail-s3-dataevents-enabled	Die Erfassung von Simple Storage Service (Amazon S3)-Datenereignissen unterstützt die Erkennung von ungewöhnlichen Aktivitäten. Zu den Details gehören Informationen zu dem AWS -Konto, das auf einen Amazon-S3-Bucket zugegriffen hat, die IP-Adresse und die Uhrzeit des Ereignisses.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
DE.CM-3	Die Aktivitäten der Mitarbeiter werden überwacht, um potenzielle Cybersich erheitsvorfälle zu erkennen.	cloudtrail-enabled	AWS CloudTrai l kann durch die Aufzeichnung von Aktionen und API-Aufrufen in der AWS Management Console bei der Nichtabst reitbarkeit helfen. Sie können die Benutzer und die Benutzer AWS-Konten , die einen AWS Dienst aufgerufen haben, die Quell-IP-Adresse, über die die Aufrufe generiert wurden, und den Zeitpunkt der Anrufe identifiz ieren. Einzelheiten zu den erfassten Daten finden Sie in den AWS CloudTrail Datensatzinhalten.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
DE.CM-3	Die Aktivitäten der Mitarbeiter werden überwacht, um potenzielle Cybersich erheitsvorfälle zu erkennen.	guardduty-enabled-centralized	Amazon GuardDuty kann mithilfe von Threat Intellige nce Feeds helfen, potenzielle Cybersich erheitsereignisse zu überwachen und zu erkennen. Dazu gehören Listen mit bösartigen IPs und maschinel len Lernmethoden zur Identifizierung unerwarteter, nicht autorisierter und bösartiger Aktivitäten in Ihrer AWS Cloud-Umgebung.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
DE.CM-3	Die Aktivitäten der Mitarbeiter werden überwacht, um potenzielle Cybersich erheitsvorfälle zu erkennen.	multi-region-cloudtrail-enabled	AWS CloudTrail zeichnet Aktionen und API-Aufrufe der AWS Management Console auf. Sie können feststellen, welche Benutzer und Konten angerufen wurden AWS, von welcher Quell-IP-Adresse aus die Anrufe getätigt wurden und wann die Anrufe erfolgten. CloudTrail übermittelt Protokolldateien aus allen AWS Regionen an Ihren S3-Bucket , wenn MULTI_REG ION_CLOUD _TRAIL_ENABLED aktiviert ist. Außerdem wird beim AWS Start einer neuen Region derselbe Trail in der neuen Region erstellt. CloudTrail Dadurch erhalten Sie automatis ch Protokolldateien mit API-Aktivitäten für die neue Region.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
DE.CM-3	Die Aktivitäten der Mitarbeiter werden überwacht, um potenzielle Cybersich erheitsvorfälle zu erkennen.	s-3 bucket-logging-enabled	Die Amazon Simple Storage Service (Amazon S3)-Serverzugriffs protokollierung bietet eine Methode zur Überwachu ng des Netzwerks im Hinblick auf potenzielle Cybersich erheitsereignisse. Die Ereignisse werden überwacht, indem detaillierte Aufzeichn ungen über die Anfragen erfasst werden, die an einen Amazon-S3-Bucket gestellt wurden. Jeder Zugriffsprotokolle intrag enthält Details zu einer einzelnen Zugriffsanfrage. Zu den Details gehören Anforderer, Bucket-Name, Anforderu ngszeit, Anforderu ngsaktion, Antwortst atus und Fehlercode, falls relevant.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
DE.CM-3	Die Aktivitäten der Mitarbeiter werden überwacht, um potenzielle Cybersich erheitsvorfälle zu erkennen.	securityhub-enabled	AWS Security Hub hilft bei der Überwachung von unbefugtem Personal, Verbindun gen, Geräten und Software. AWS Security Hub aggregiert, organisie rt und priorisie rt die Sicherhei tswarnungen oder Ergebnisse mehrerer Dienste. AWS Einig e dieser Dienste sind Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer und AWS Firewall Manager sowie AWS Partnerlösungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
DE.CM-4	Bösartiger Code wird erkannt	guardduty-non-archived-findings	Amazon GuardDuty hilft Ihnen dabei, die Auswirkungen eines Vorfalls zu verstehen, indem es die Ergebnisse nach Schweregrad klassifiziert: niedrig, mittel und hoch. Diese Klassifizierungen können Sie zur Festlegung von entsprechenden Strategien und Prioritäten zur Behebung solcher Vorfälle verwenden. Mit dieser Regel können Sie optional daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7) und daysHighSev (Config Default: 1) für nicht archivierte Ergebnisse festlegen, wie es die Richtlinien Ihrer Organisation erfordern.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
DE.CM-4	Bösartiger Code wird erkannt	guardduty-enabled-centralized	Amazon GuardDuty kann mithilfe von Threat Intellige nce Feeds helfen, potenzielle Cybersich erheitsereignisse zu überwachen und zu erkennen. Dazu gehören Listen mit bösartigen IPs und maschinel len Lernmethoden zur Identifizierung unerwarteter, nicht autorisierter und bösartiger Aktivitäten in Ihrer AWS Cloud-Umgebung.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
DE.CM-5	Unerlaubter Mobilcode wird erkannt	alb-waf-enabled	Stellen Sie sicher, dass AWS WAF auf Elastic Load Balancers (ELB) aktiviert ist, um Webanwendungen zu schützen. Eine WAF trägt zum Schutz Ihrer Webanwend ungen oder APIs vor gängigen Web-Explo its bei. Diese Web-Exploits können sich auf die Verfügbar keit auswirken, die Sicherheit gefährden oder übermäßige Ressourcen in Ihrer Umgebung verbrauch en.
DE.CM-5	Unerlaubter Mobilcode wird erkannt	cloud-trail-cloud-watch-logs-aktiviert	Verwenden Sie Amazon CloudWatc h , um Protokoll ereignisaktivitäten zentral zu sammeln und zu verwalten. Die Aufnahme von AWS CloudTrail Daten liefert Einzelheiten zu den API-Aufrufaktivitä ten in Ihrem AWS-Konto.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
DE.CM-5	Unerlaubter Mobilcode wird erkannt	guardduty-enabled-centralized	Amazon GuardDuty kann mithilfe von Threat Intellige nce Feeds helfen, potenzielle Cybersich erheitsereignisse zu überwachen und zu erkennen. Dazu gehören Listen mit bösartigen IPs und maschinel len Lernmethoden zur Identifizierung unerwarteter, nicht autorisierter und bösartiger Aktivitäten in Ihrer AWS Cloud-Umgebung.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
DE.CM-5	Unerlaubter Mobilcode wird erkannt	guardduty-non-archived-findings	Amazon GuardDuty hilft Ihnen dabei, die Auswirkungen eines Vorfalls zu verstehen, indem es die Ergebnisse nach Schweregrad klassifiziert: niedrig, mittel und hoch. Diese Klassifizierungen können Sie zur Festlegung von entsprechenden Strategien und Prioritäten zur Behebung solcher Vorfälle verwenden. Mit dieser Regel können Sie optional daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7) und daysHighSev (Config Default: 1) für nicht archivierte Ergebnisse festlegen, wie es die Richtlinien Ihrer Organisation erfordern.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
DE.CM-5	Unerlaubter Mobilcode wird erkannt	securityhub-enabled	AWS Security Hub hilft bei der Überwachung von unbefugtem Personal, Verbindungen, Geräten und Software. AWS Security Hub aggregiert, organisiert und priorisiert die Sicherheitswarnungen oder Ergebnisse mehrerer Dienste. AWS Einige dieser Dienste sind Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer und AWS Firewall Manager sowie AWS Partnerlösungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
DE.CM-5	Unerlaubter Mobilcode wird erkannt	wafv2-logging-enabled	Um Ihnen bei der Protokollierung und Überwachung in Ihrer Umgebung zu helfen, aktivieren Sie die AWS WAF (V2) -Protokollierung im regionalen und globalen Web. ACLs AWS Die WAF-Protokollierung bietet detaillierte Informationen über den Datenverkehr, der von Ihrer Web-ACL analysiert wird. In den Protokollen werden die Uhrzeit aufgezeichnet, zu der die AWS WAF die Anfrage von Ihrer AWS Ressource erhalten hat, Informationen zu der Anfrage und eine Aktion für die Regel, der jede Anfrage entsprach.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
DE.CM-6	Die Aktivitäten von externen Dienstlei stern werden überwacht, um potenzielle Cybersich erheitsvorfälle zu erkennen.	cloudtrail-s3-data events-enabled	Die Erfassung von Simple Storage Service (Amazon S3)-Datenereigniss en unterstützt die Erkennung von ungewöhnlichen Aktivitäten. Zu den Details gehören Informationen zu dem AWS -Konto, das auf einen Amazon-S3-Bucket zugegriffen hat, die IP-Adresse und die Uhrzeit des Ereignisses.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
DE.CM-6	Die Aktivitäten von externen Dienstlei stern werden überwacht, um potenzielle Cybersich erheitsvorfälle zu erkennen.	cloudtrail-enabled	AWS CloudTrail kann dabei helfen, die Ablehnung zu verhindern, indem Aktionen und API-Aufrufe der AWS Management Console aufgezeichnet werden. Sie können die Benutzer und die Benutzer AWS-Konten , die einen AWS Dienst aufgerufe n haben, die Quell-IP-Adresse, über die die Aufrufe generiert wurden, und den Zeitpunkt der Anrufe identifiz ieren. Einzelheiten zu den erfassten Daten finden Sie in den AWS CloudTrail Datensatzinhalten.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
DE.CM-6	Die Aktivitäten von externen Dienstlei stern werden überwacht, um potenzielle Cybersich erheitsvorfälle zu erkennen.	guardduty-enabled-centralized	Amazon GuardDuty kann mithilfe von Threat Intellige nce Feeds helfen, potenzielle Cybersich erheitsereignisse zu überwachen und zu erkennen. Dazu gehören Listen mit bösartigen IPs und maschinel len Lernmethoden zur Identifizierung unerwarteter, nicht autorisierter und bösartiger Aktivitäten in Ihrer AWS Cloud-Umgebung.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
DE.CM-6	Die Aktivitäten von externen Dienstlei stern werden überwacht, um potenzielle Cybersich erheitsvorfälle zu erkennen.	multi-region-cloudtrail-enabled	AWS CloudTrail zeichnet Aktionen und API-Aufrufe der AWS Management Console auf. Sie können feststellen, welche Benutzer und Konten angerufen wurden AWS, von welcher Quell-IP-Adresse aus die Anrufe getätigt wurden und wann die Anrufe erfolgten. CloudTrail übermittelt Protokolldateien aus allen AWS Regionen an Ihren S3-Bucket , wenn MULTI_REG ION_CLOUD _TRAIL_ENABLED aktiviert ist. Außerdem wird beim AWS Start einer neuen Region derselbe Trail in der neuen Region erstellt. CloudTrail Dadurch erhalten Sie automatis ch Protokolldateien mit API-Aktivitäten für die neue Region.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
DE.CM-6	Die Aktivitäten von externen Dienstlei stern werden überwacht, um potenzielle Cybersich erheitsvorfälle zu erkennen.	s-3 bucket-logging-enabled	Die Amazon Simple Storage Service (Amazon S3)-Serverzugriffs protokollierung bietet eine Methode zur Überwachu ng des Netzwerks im Hinblick auf potenzielle Cybersich erheitsereignisse. Die Ereignisse werden überwacht, indem detaillierte Aufzeichn ungen über die Anfragen erfasst werden, die an einen Amazon-S3-Bucket gestellt wurden. Jeder Zugriffsprotokolle intrag enthält Details zu einer einzelnen Zugriffsanfrage. Zu den Details gehören Anforderer, Bucket-Name, Anforderu ngszeit, Anforderu ngsaktion, Antwortst atus und Fehlercode, falls relevant.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
DE.CM-6	Die Aktivitäten von externen Dienstlei stern werden überwacht, um potenzielle Cybersich erheitsvorfälle zu erkennen.	securityhub-enabled	AWS Security Hub hilft bei der Überwachung von unbefugtem Personal, Verbindun gen, Geräten und Software. AWS Security Hub aggregiert, organisie rt und priorisie rt die Sicherhei tswarnungen oder Ergebnisse mehrerer Dienste. AWS Einig e dieser Dienste sind Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer und AWS Firewall Manager sowie AWS Partnerlösungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
DE.CM-7	Es wird eine Überwachung auf unbefugtes Personal, Verbindungen, Geräte und Software durchgeführt	api-gw-execution-logging-aktiviert	Die API-Gateway-Protokollierung zeigt detaillierte Ansichten der Benutzer, die auf die API zugegriffen haben, und wie diese Benutzer auf die API zugegriffen haben. Diese Insights ermöglichen die Einsicht in Benutzeraktivitäten.
DE.CM-7	Es wird eine Überwachung auf unbefugtes Personal, Verbindungen, Geräte und Software durchgeführt	cloudtrail-s3-dataevents-enabled	Die Erfassung von Simple Storage Service (Amazon S3)-Datenereignissen unterstützt die Erkennung von ungewöhnlichen Aktivitäten. Zu den Details gehören Informationen zu dem AWS -Konto, das auf einen Amazon-S3-Bucket zugegriffen hat, die IP-Adresse und die Uhrzeit des Ereignisses.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
DE.CM-7	Es wird eine Überwachung auf unbefugtes Personal, Verbindungen, Geräte und Software durchgeführt	cloudtrail-enabled	AWS CloudTrai l kann durch die Aufzeichnung von Aktionen und API-Aufrufen in der AWS Management Console bei der Nichtabst reitbarkeit helfen. Sie können die Benutzer und die Benutzer AWS-Konten , die einen AWS Dienst aufgerufen haben, die Quell-IP-Adresse, über die die Aufrufe generiert wurden, und den Zeitpunkt der Anrufe identifiz ieren. Einzelheiten zu den erfassten Daten finden Sie in den AWS CloudTrail Datensatzinhalten.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
DE.CM-7	Es wird eine Überwachung auf unbefugtes Personal, Verbindungen, Geräte und Software durchgeführt	elb-logging-enabled	Die Elastic-Load-Balancing-Aktivität ist ein zentraler Kommunikationspunkt innerhalb einer Umgebung. Stellen Sie sicher, dass die ELB-Protokollierung aktiviert ist. Die gesammelten Daten enthalten detaillierte Informationen zu Anfragen, die an den ELB gesendet wurden. Jedes Protokoll enthält Informationen wie die Zeit, zu der die Anforderung einging, die Client-IP-Adresse, Latenzen, Anforderungspfade und Serverantworten.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
DE.CM-7	Es wird eine Überwachung auf unbefugtes Personal, Verbindungen, Geräte und Software durchgeführt	guardduty-enabled-centralized	Amazon GuardDuty kann mithilfe von Threat Intellige nce Feeds helfen, potenzielle Cybersich erheitsereignisse zu überwachen und zu erkennen. Dazu gehören Listen mit bösartigen IPs und maschinel len Lernmethoden zur Identifizierung unerwarteter, nicht autorisierter und bösartiger Aktivitäten in Ihrer AWS Cloud-Umgebung.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
DE.CM-7	Es wird eine Überwachung auf unbefugtes Personal, Verbindungen, Geräte und Software durchgeführt	multi-region-cloudtrail-enabled	AWS CloudTrail zeichnet Aktionen und API-Aufrufe der AWS Management Console auf. Sie können feststellen, welche Benutzer und Konten angerufen wurden AWS, von welcher Quell-IP-Adresse aus die Anrufe getätigt wurden und wann die Anrufe erfolgten. CloudTrail übermittelt Protokolldateien aus allen AWS Regionen an Ihren S3-Bucket , wenn MULTI_REG ION_CLOUD _TRAIL_ENABLED aktiviert ist. Außerdem wird beim AWS Start einer neuen Region derselbe Trail in der neuen Region erstellt. CloudTrail Dadurch erhalten Sie automatis ch Protokolldateien mit API-Aktivitäten für die neue Region.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
DE.CM-7	Es wird eine Überwachung auf unbefugtes Personal, Verbindungen, Geräte und Software durchgeführt	s-3 bucket-logging-enabled	Die Amazon Simple Storage Service (Amazon S3)-Serverzugriffs protokollierung bietet eine Methode zur Überwachu ng des Netzwerks im Hinblick auf potenzielle Cybersich erheitsereignisse. Die Ereignisse werden überwacht, indem detaillierte Aufzeichn ungen über die Anfragen erfasst werden, die an einen Amazon-S3-Bucket gestellt wurden. Jeder Zugriffsprotokolle intrag enthält Details zu einer einzelnen Zugriffsanfrage. Zu den Details gehören Anforderer, Bucket-Name, Anforderu ngszeit, Anforderu ngsaktion, Antwortst atus und Fehlercode, falls relevant.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
DE.CM-7	Es wird eine Überwachung auf unbefugtes Personal, Verbindungen, Geräte und Software durchgeführt	securityhub-enabled	AWS Security Hub hilft bei der Überwachung von unbefugtem Personal, Verbindungen, Geräten und Software. AWS Security Hub aggregiert, organisiert und priorisiert die Sicherheitswarnungen oder Ergebnisse mehrerer Dienste. AWS Einige dieser Dienste sind Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer und AWS Firewall Manager sowie AWS Partnerlösungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
DE.CM-7	Es wird eine Überwachung auf unbefugtes Personal, Verbindungen, Geräte und Software durchgeführt	vpc-flow-logs-enabled	VPC-Flow-Protokolle erfassen detaillierte Informationsdatensätze über den IP-Datenverkehr, der zu und von Netzwerkschnittstellen in Ihrer Amazon Virtual Private Cloud (Amazon VPC) fließt. Standardmäßig enthalten Flow-Protokolldatensätze Werte für die verschiedenen Komponenten des IP-Flows, einschließlich Quelle, Ziel und Protokoll.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
DE.DP-4	Informationen zur Erkennung von Ereignissen werden übermittelt	alb-waf-enabled	Stellen Sie sicher, dass AWS WAF auf Elastic Load Balancers (ELB) aktiviert ist, um Webanwendungen zu schützen. Eine WAF trägt zum Schutz Ihrer Webanwend ungen oder APIs vor gängigen Web-Explo its bei. Diese Web-Exploits können sich auf die Verfügbar keit auswirken, die Sicherheit gefährden oder übermäßige Ressourcen in Ihrer Umgebung verbrauch en.
DE.DP-4	Informationen zur Erkennung von Ereignissen werden übermittelt	cloud-trail-cloud-watch-logs-aktiviert	Verwenden Sie Amazon CloudWatc h , um Protokoll ereignisaktivitäten zentral zu sammeln und zu verwalten. Die Aufnahme von AWS CloudTrail Daten liefert Einzelheiten zu den API-Aufrufaktivitä ten in Ihrem AWS-Konto.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
DE.DP-4	Informationen zur Erkennung von Ereignissen werden übermittelt	guardduty-enabled-centralized	Amazon GuardDuty kann mithilfe von Threat Intellige nce Feeds helfen, potenzielle Cybersich erheitsereignisse zu überwachen und zu erkennen. Dazu gehören Listen mit bösartigen IPs und maschinel len Lernmethoden zur Identifizierung unerwarteter, nicht autorisierter und bösartiger Aktivitäten in Ihrer AWS Cloud-Umgebung.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
DE.DP-4	Informationen zur Erkennung von Ereignissen werden übermittelt	guardduty-non-archived-findings	Amazon GuardDuty hilft Ihnen dabei, die Auswirkungen eines Vorfalls zu verstehen, indem es die Ergebnisse nach Schweregrad klassifiziert: niedrig, mittel und hoch. Diese Klassifizierungen können Sie zur Festlegung von entsprechenden Strategien und Prioritäten zur Behebung solcher Vorfälle verwenden. Mit dieser Regel können Sie optional daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7) und daysHighSev (Config Default: 1) für nicht archivierte Ergebnisse festlegen, wie es die Richtlinien Ihrer Organisation erfordern.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
DE.DP-4	Informationen zur Erkennung von Ereignissen werden übermittelt	s-3 event-notification s-enabled	Amazon-S3-Ereignis benachrichtigungen können das zuständig e Personal über versehentliche oder vorsätzliche Änderungen an Ihren Bucket-Ob jekten informieren. Zu den Warnen gehören beispiels weise: Erstellung eines neuen Objekts, Entfernung eines Objekts, Wiederher stellung eines Objekts, verloren gegangene und replizierte Objekte.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
DE.DP-4	Informationen zur Erkennung von Ereignissen werden übermittelt	securityhub-enabled	AWS Security Hub hilft bei der Überwachung von unbefugtem Personal, Verbindungen, Geräten und Software. AWS Security Hub aggregiert, organisiert und priorisiert die Sicherheitswarnungen oder Ergebnisse mehrerer Dienste. AWS Einige dieser Dienste sind Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer und AWS Firewall Manager sowie AWS Partnerlösungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
DE.DP-4	Informationen zur Erkennung von Ereignissen werden übermittelt	wafv2-logging-enabled	Um Ihnen bei der Protokollierung und Überwachung in Ihrer Umgebung zu helfen, aktivieren Sie die AWS WAF (V2) -Protokollierung im regionalen und globalen Web. ACLs AWS Die WAF-Protokollierung bietet detaillierte Informationen über den Datenverkehr, der von Ihrer Web-ACL analysiert wird. In den Protokollen werden die Uhrzeit aufgezeichnet, zu der die AWS WAF die Anfrage von Ihrer AWS Ressource erhalten hat, Informationen zu der Anfrage und eine Aktion für die Regel, der jede Anfrage entsprach.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
DE.DP-5	Die Erkennung sprozesse werden kontinuierlich verbessert	guardduty-enabled-centralized	Amazon GuardDuty kann mithilfe von Threat Intellige nce Feeds helfen, potenzielle Cybersich erheitsereignisse zu überwachen und zu erkennen. Dazu gehören Listen mit bösartigen IPs und maschinel len Lernmethoden zur Identifizierung unerwarteter, nicht autorisierter und bösartiger Aktivitäten in Ihrer AWS Cloud-Umgebung.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
ID.AM-2	Softwareplattformen und Anwendungen innerhalb der Organisation werden inventarisiert	ec2-manager instance-managed-by-systems	Eine Bestandsaufnahme der Softwareplattformen und Anwendungen innerhalb des Unternehmens ist möglich, indem Amazon Elastic Compute Cloud (Amazon EC2) - Instances mit AWS Systems Manager verwaltet werden. Verwenden Sie AWS Systems Manager, um detaillierte Systemkonfigurationen, Betriebssystem-Patch-Levels, Namen und Typ der Dienste, Softwareinstallationen, Anwendungsname, Herausgeber und Version sowie andere Details zu Ihrer Umgebung bereitzustellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
ID.AM-2	Softwareplattformen und Anwendungen innerhalb der Organisation werden inventarisiert	ec2-check managedinstance-association-compliance-status	Verwenden Sie AWS Systems Manager Associations, um bei der Inventarisierung von Softwareplattformen und Anwendungen innerhalb eines Unternehmens zu helfen. AWS Systems Manager weist Ihren verwalteten Instances einen Konfigurationsstatus zu und ermöglicht es Ihnen, Basiswerte für Betriebssystem-Patch-Levels, Softwareinstallationen, Anwendungskonfigurationen und andere Details zu Ihrer Umgebung festzulegen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
ID.AM-2	Softwareplattformen und Anwendungen innerhalb der Organisation werden inventarisiert	ec2-stopped-instance	Aktivieren Sie diese Regel, um bei der Basiskonfiguration von Amazon Elastic Compute Cloud (Amazon EC2) - Instances zu helfen, indem Sie überprüfen, ob EC2 Amazon-Instances gemäß den Standards Ihrer Organisation für mehr als die zulässige Anzahl von Tagen gestoppt wurden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
ID.AM-2	Softwareplattformen und Anwendungen innerhalb der Organisation werden inventarisiert	eip-attached	Diese Regel stellt sicher, dass Elastic, die einer Amazon Virtual Private Cloud (Amazon VPC) IPs zugewiesen sind, an Amazon Elastic Compute Cloud (Amazon EC2) - Instances oder verwendete Elastic Network Interfaces angehängt sind. Diese Regel hilft bei der Überwachung ungenutzter Inhalte EIPs in Ihrer Umgebung.
ID.AM-2	Softwareplattformen und Anwendungen innerhalb der Organisation werden inventarisiert	vpc-network-acl-unused-überprüfen	Diese Regel stellt sicher, dass Amazon Virtual Private Cloud (VPC)-Netzwerkzugriffskontrolllisten verwendet werden. Die Überwachung ungenutzter Netzwerk-Zugriffskontrolllisten kann zu einer genauen Inventarisierung und Verwaltung Ihrer Umgebung beitragen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
ID.AM-3	Organisatorische Kommunikation und Datenflüsse werden abgebildet	api-gw-execution-logging-aktiviert	Die API-Gateway-Protokollierung zeigt detaillierte Ansichten der Benutzer, die auf die API zugegriffen haben, und wie diese Benutzer auf die API zugegriffen haben. Diese Insights ermöglichen die Einsicht in Benutzeraktivitäten.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
ID.AM-3	Organisatorische Kommunikation und Datenflüsse werden abgebildet	cloudtrail-enabled	AWS CloudTrai l kann durch die Aufzeichnung von Aktionen und API-Aufrufen in der AWS Management Console bei der Nichtabst reitbarkeit helfen. Sie können die Benutzer und die Benutzer AWS-Konten , die einen AWS Dienst aufgerufen haben, die Quell-IP-Adresse, über die die Aufrufe generiert wurden, und den Zeitpunkt der Anrufe identifiz ieren. Einzelheiten zu den erfassten Daten finden Sie in den AWS CloudTrail Datensatzinhalten.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
ID.AM-3	Organisatorische Kommunikation und Datenflüsse werden abgebildet	elb-logging-enabled	Die Elastic-Load-Balancing-Aktivität ist ein zentraler Kommunikationspunkt innerhalb einer Umgebung. Stellen Sie sicher, dass die ELB-Protokollierung aktiviert ist. Die gesammelten Daten enthalten detaillierte Informationen zu Anfragen, die an den ELB gesendet wurden. Jedes Protokoll enthält Informationen wie die Zeit, zu der die Anforderung einging, die Client-IP-Adresse, Latenzen, Anforderungspfade und Serverantworten.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
ID.AM-3	Organisatorische Kommunikation und Datenflüsse werden abgebildet	multi-region-cloudtrail-enabled	AWS CloudTrail zeichnet Aktionen und API-Aufrufe der AWS Management Console auf. Sie können feststellen, welche Benutzer und Konten angerufen wurden AWS, von welcher Quell-IP-Adresse aus die Anrufe getätigt wurden und wann die Anrufe erfolgten. CloudTrail übermittelt Protokolldateien aus allen AWS Regionen an Ihren S3-Bucket , wenn MULTI_REG ION_CLOUD _TRAIL_ENABLED aktiviert ist. Außerdem wird beim AWS Start einer neuen Region derselbe Trail in der neuen Region erstellt. CloudTrail Dadurch erhalten Sie automatis ch Protokolldateien mit API-Aktivitäten für die neue Region.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
ID.AM-3	Organisatorische Kommunikation und Datenflüsse werden abgebildet	redshift-cluster-configuration-check	Um Daten im Ruhezustand zu schützen, muss die Verschlüsselung für Ihre Amazon-Redshift-Cluster aktiviert sein. Sie müssen auch sicherstellen, dass die erforderlichen Konfigurationen auf Amazon-Redshift-Clustern bereitgestellt werden. Die Prüfungsprotokollierung muss aktiviert sein, um Informationen zu Verbindungen und Benutzeraktivitäten in der Datenbank bereitzustellen. Diese Regel erfordert, dass ein Wert für clusterDbEncrypted (Config Default: TRUE) und LoggingEnabled (Config Default: TRUE) gesetzt ist. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
ID.AM-3	Organisatorische Kommunikation und Datenflüsse werden abgebildet	s3- bucket-logging-enabled	Die Amazon Simple Storage Service (Amazon S3)-Serverzugriffs protokollierung bietet eine Methode zur Überwachu ng des Netzwerks im Hinblick auf potenzielle Cybersich erheitsereignisse. Die Ereignisse werden überwacht, indem detaillierte Aufzeichn ungen über die Anfragen erfasst werden, die an einen Amazon-S3-Bucket gestellt wurden. Jeder Zugriffsprotokolle intrag enthält Details zu einer einzelnen Zugriffsanfrage. Zu den Details gehören Anforderer, Bucket-Name, Anforderu ngszeit, Anforderu ngsaktion, Antwortst atus und Fehlercode, falls relevant.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
ID.AM-3	Organisatorische Kommunikation und Datenflüsse werden abgebildet	vpc-flow-logs-enabled	VPC-Flow-Protokolle erfassen detaillierte Informationsdatensätze über den IP-Datenverkehr, der zu und von Netzwerkschnittstellen in Ihrer Amazon Virtual Private Cloud (Amazon VPC) fließt. Standardmäßig enthalten Flow-Protokolldatensätze Werte für die verschiedenen Komponenten des IP-Flows, einschließlich Quelle, Ziel und Protokoll.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
ID.BE-5	Resilienzanforderungen zur Unterstützung der Bereitstellung kritischer Dienste werden für alle Betriebszustände festgelegt (z. B. unter Not/Angriff, während der Wiederherstellung, normaler Betrieb)	dynamodb-in-backup-plan	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon DynamoDB-Tabellen Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
ID.BE-5	Stabilitätsanforderungen zur Unterstützung der Bereitstellung kritischer Dienste werden für alle Betriebszustände festgelegt (z. B. unter Not/Angriff, während der Wiederherstellung, normaler Betrieb)	ebs-in-backup-plan	Stellen Sie zur Unterstützung der Datensicherungsprozesse sicher, dass Ihre Amazon Elastic Block Store (Amazon EBS) -Volumes Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihre Backup-Verwaltung und ermöglicht es Ihnen, Ihre geschäftlichen und behördlichen Anforderungen bezüglich Backups zu erfüllen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
ID.BE-5	Stabilitätsanforderungen zur Unterstützung der Bereitstellung kritischer Dienste werden für alle Betriebszustände festgelegt (z. B. unter Not/Angriff, während der Wiederherstellung, normaler Betrieb)	efs-in-backup-plan	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon Elastic File System (Amazon EFS) -Dateisysteme Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
ID.BE-5	Stabilitätsanforderungen zur Unterstützung der Bereitstellung kritischer Dienste werden für alle Betriebszustände festgelegt (z. B. unter Not/Angriff, während der Wiederherstellung, normaler Betrieb)	elb-cross-zone-load-Balancing aktiviert	Aktivieren Sie zonenübergreifendes Load Balancing für Ihre Elastic Load Balancer (ELBs), um eine angemessene Kapazität und Verfügbarkeit aufrechtzuerhalten. Zonenübergreifendes Load Balancing reduziert die Notwendigkeit, die gleiche Anzahl von Instances in jeder aktivierten Availability Zone aufrechtzuerhalten. Es verbessert auch die Fähigkeit Ihrer Anwendung, den Verlust einer oder mehrerer Instances zu bewältigen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
ID.BE-5	Resilienzanforderungen zur Unterstützung der Bereitstellung kritischer Dienste werden für alle Betriebszustände festgelegt (z. B. unter Not/Angriff, während der Wiederherstellung, normaler Betrieb)	rds-instance-deletion-protection-aktiviert	Stellen Sie sicher, dass Amazon Relational Database Service (Amazon RDS)-Instances den Löschschutz aktiviert haben. Verwenden Sie den Löschschutz, um zu verhindern, dass Ihre Amazon-RDS-Instances versehentlich oder böswillig gelöscht werden, was zum Verlust der Verfügbarkeit Ihrer Anwendungen führen kann.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
ID.BE-5	Stabilitätsanforderungen zur Unterstützung der Bereitstellung kritischer Dienste werden für alle Betriebszustände festgelegt (z. B. unter Not/Angriff, während der Wiederherstellung, normaler Betrieb)	rds-in-backup-plan	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon Relational Database Service (Amazon RDS) -Instances Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
ID.BE-5	Stabilitätsanforderungen zur Unterstützung der Bereitstellung kritischer Dienste werden für alle Betriebszustände festgelegt (z. B. unter Not/Angriff, während der Wiederherstellung, normaler Betrieb)	redshift-backup-enabled	Stellen Sie zur Unterstützung der Datensicherungsprozesse sicher, dass Ihre Amazon-Redshift-Cluster über automatisierte Snapshots verfügen. Wenn automatisierte Snapshots für einen Cluster aktiviert sind, erstellt Redshift in regelmäßigen Abständen Snapshots dieses Clusters. Standardmäßig erstellt Redshift alle acht Stunden oder alle 5 GB einen Snapshot für jeden Knoten mit Datenänderungen oder je nachdem, was zuerst eintritt.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
ID.BE-5	Stabilitätsanforderungen zur Unterstützung der Bereitstellung kritischer Dienste werden für alle Betriebszustände festgelegt (z. B. unter Zwang oder Angriff, während der Wiederherstellung, normaler Betrieb)	db-instance-backup-enabled	Die Sicherungsfunktion von Amazon RDS erstellt Sicherungen Ihrer Datenbanken und Transaktionsprotokolle. Amazon RDS erstellt einen Snapshot für das Speichervolume Ihrer DB-Instance, sodass die gesamte DB-Instance gesichert wird. Sie können im System spezifische Aufbewahrungsfristen festlegen, um Ihre Ausfallsicherheitsanforderungen zu erfüllen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
ID.BE-5	Resilienzanforderungen zur Unterstützung der Bereitstellung kritischer Dienste werden für alle Betriebszustände festgelegt (z. B. unter Zwang oder Angriff, während der Wiederherstellung, normaler Betrieb)	dynamodb-autoscaling-enabled	Amazon DynamoDB Auto Scaling verwendet den AWS Application Auto Scaling-Service, um die bereitgestellte Durchsatzkapazität so anzupassen, dass sie automatisch auf tatsächliche Verkehrsmuster reagiert. Auf diese Weise kann eine Tabelle oder ein globaler sekundärer Index die bereitgestellte Lese-/Schreibkapazität erhöhen, um plötzliche Erhöhungen des Datenverkehrs ohne Drosselung zu bewältigen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
ID.BE-5	Resilienzanforderungen zur Unterstützung der Bereitstellung kritischer Services werden für alle Betriebszustände festgelegt (z. B. unter Zwang oder Angriff, während der Wiederherstellung, normaler Betrieb)	dynamodb-pitr-enabled	Aktivieren Sie diese Regel, um zu überprüfen, ob die Informationen gesichert wurden. Es verwaltet auch die Backups, indem es sicherstellt, dass die point-in-time Wiederherstellung in Amazon DynamoDB aktiviert ist. Bei der Wiederherstellung werden fortlaufende Backups Ihrer Tabelle für die letzten 35 Tage gespeichert.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
ID.BE-5	Stabilitätsanforderungen zur Unterstützung der Bereitstellung kritischer Services werden für alle Betriebszustände festgelegt (z. B. unter Not/Angriff, während der Wiederherstellung, normaler Betrieb)	elasticache-redis-cluster-automatic-Backup-Check	Wenn automatische Backups aktiviert sind, ElastiCache erstellt Amazon täglich ein Backup des Clusters. Die Sicherung kann für eine von Ihrer Organisation festgelegte Anzahl von Tagen aufbewahrt werden. Automatische Backups schützen vor Datenverlust. Bei einem Ausfall können Sie einen neuen Cluster erstellen, der Ihre Daten aus dem aktuellen Backup wiederherstellt.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
ID.BE-5	Stabilitätsanforderungen zur Unterstützung der Bereitstellung kritischer Services werden für alle Betriebszustände festgelegt (z. B. unter Not/Angriff, während der Wiederherstellung, normaler Betrieb)	elb-deletion-protection-enabled	Diese Regel sorgt dafür, dass der Löschschutz für Elastic Load Balancing aktiviert ist. Verwenden Sie diese Funktion, um zu verhindern, dass Ihr Load Balancer versehentlich oder böswillig gelöscht wird, was zum Verlust der Verfügbarkeit Ihrer Anwendungen führen kann.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
ID.BE-5	Resilienzanforderungen zur Unterstützung der Bereitstellung kritischer Dienste werden für alle Betriebszustände festgelegt (z. B. unter Zwang oder Angriff, während der Wiederherstellung, normaler Betrieb)	rds-multi-az-support	Die Multi-AZ-Unterstützung in Amazon Relational Database Service (Amazon RDS) bietet eine verbesserte Verfügbarkeit und Beständigkeit von Datenbank-Instances. Wenn Sie eine Multi-AZ-Datenbank-Instance bereitstellen, erstellt Amazon RDS automatisch eine primäre Datenbank-Instance und repliziert die Daten synchron auf eine Standby-Instance in einer anderen Availability Zone. Jede Availability Zone läuft auf einer eigenen, physisch getrennten, unabhängigen Infrastruktur und ist auf eine hohe Verfügbarkeit ausgelegt. Im Falle eines Infrastrukturausfalls führt Amazon RDS einen automatis

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			chen Failover zum Standby-Modus durch, sodass Sie den Datenbankbetrieb wieder aufnehmen können, sobald der Failover abgeschlo ssen ist.
ID.BE-5	Resilienzanforderu ngen zur Unterstüt zung der Bereitste llung kritischer Dienste werden für alle Betriebszustände festgelegt (z. B. unter Zwang oder Angriff, während der Wiederherstellung, normaler Betrieb)	s3- bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) unterstützt die Aufrechterhaltung einer angemesse nen Kapazität und Verfügbarkeit. CRR ermöglicht das automatische, asynchrone Kopieren von Objekten in Amazon S3 Buckets, um die Datenverf ügbarkeit sicherzus tellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
ID.BE-5	Resilienzanforderungen zur Unterstützung der Bereitstellung kritischer Dienste werden für alle Betriebszustände festgelegt (z. B. unter Not/Angriff, während der Wiederherstellung, normaler Betrieb)	s3- bucket-versioning-enabled	Die Versionsverwaltung von Amazon Simple Storage Service (Amazon S3)-Buckets hilft dabei, mehrere Varianten eines Objekts im selben Amazon-S3-Bucket zu speichern. Verwenden Sie die Versionsverwaltung, um sämtliche Versionen aller Objekte in Ihrem Amazon-S3-Bucket zu speichern, abzurufen oder wiederherzustellen. Mit der Versionsverwaltung können Sie Versionen sowohl nach unbeabsichtigten Benutzeraktionen als auch nach Anwendungsfehlern problemlos wiederherstellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
ID.BE-5	Resilienzanforderungen zur Unterstützung der Bereitstellung kritischer Dienste werden für alle Betriebszustände festgelegt (z. B. unter Not/Angriff, während der Wiederherstellung, normaler Betrieb)	vpc-vpn-2-tunnels-up	Redundante Site-to-Site VPN-Tunnel können implementiert werden, um die Anforderungen an die Ausfallsicherheit zu erfüllen. Es verwendet zwei Tunnel, um die Konnektivität sicherzustellen, falls eine der Site-to-Site VPN-Verbindungen nicht verfügbar ist. Um sich vor einem Verbindungsverlust zu schützen, können Sie für den Fall, dass Ihr Kunden-Gateway nicht verfügbar ist, eine zweite Site-to-Site VPN-Verbindung zu Ihrer Amazon Virtual Private Cloud (Amazon VPC) und Ihrem Virtual Private Gateway einrichten, indem Sie ein zweites Kunden-Gateway verwenden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
ID.RA-1	Sicherheitslücken in Vermögenswerten werden identifiziert und dokumentiert	rds-automatic-minor-version-Upgrade-fähig	Aktivieren Sie automatische Unterversions-Upgrades auf Ihren Amazon-Relational-Database-Service-(RDS-)-Instances, um sicherzustellen, dass die aktuellen Updates für Unterversionen des Relational Database Management System (RDBMS) installiert sind, die Sicherheitspatches und Bugfixes enthalten können.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
ID.RA-1	Sicherheitslücken in Vermögenswerten werden identifiziert und dokumentiert	ec2- prüfen managedinstance-patch-compliance-status	Aktivieren Sie diese Regel, um bei der Identifizierung und Dokumentation von Sicherheitslücken in Amazon Elastic Compute Cloud (Amazon EC2) zu helfen. Die Regel prüft, ob die EC2 Amazon-Instance die Patch-Konformität im AWS Systems Manager gemäß den Richtlinien und Verfahren Ihrer Organisation einhält.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
ID.RA-1	Sicherheitslücken in Vermögenswerten werden identifiziert und dokumentiert	elastic-beanstalk-managed-updates-aktiviert	Durch die Aktivierung verwalteter Plattform updates für eine Amazon-Elastic-Beanstalk-Umgebung wird sichergestellt, dass die aktuellen verfügbaren Plattform -Fixes, -Updates und -Features für die Umgebung installiert sind. Eine bewährte Methode zur Sicherung von Systemen besteht darin, stets die aktuellen Patches zu installieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
ID.RA-1	Sicherheitslücken in Vermögenswerten werden identifiziert und dokumentiert	guardduty-enabled-centralized	Amazon GuardDuty kann mithilfe von Threat Intellige nce Feeds helfen, potenzielle Cybersich erheitsereignisse zu überwachen und zu erkennen. Dazu gehören Listen mit bösartigen IPs und maschinel len Lernmethoden zur Identifizierung unerwarteter, nicht autorisierter und bösartiger Aktivitäten in Ihrer AWS Cloud-Umgebung.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
ID.RA-2	Informationen zu Cyberbedrohungen stammen aus Foren und Quellen zum Informationsaustau sch	guardduty-enabled-centralized	Amazon GuardDuty kann mithilfe von Threat Intellige nce Feeds helfen, potenzielle Cybersich erheitsereignisse zu überwachen und zu erkennen. Dazu gehören Listen mit bösartigen IPs und maschinel len Lernmethoden zur Identifizierung unerwarteter, nicht autorisierter und bösartiger Aktivitäten in Ihrer AWS Cloud-Umgebung.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
ID.RA-3	Interne und externe Bedrohungen werden identifiziert und dokumentiert	ec2-check managedinstance-patch-compliance-status	Aktivieren Sie diese Regel, um bei der Identifizierung und Dokumentation von Sicherheitslücken in Amazon Elastic Compute Cloud (Amazon EC2) zu helfen. Die Regel prüft, ob die EC2 Amazon-Instance die Patch-Konformität im AWS Systems Manager gemäß den Richtlinien und Verfahren Ihrer Organisation einhält.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
ID.RA-3	Interne und externe Bedrohungen werden identifiziert und dokumentiert	guardduty-enabled-centralized	Amazon GuardDuty kann mithilfe von Threat Intellige nce Feeds helfen, potenzielle Cybersich erheitsereignisse zu überwachen und zu erkennen. Dazu gehören Listen mit bösartigen IPs und maschinel len Lernmethoden zur Identifizierung unerwarteter, nicht autorisierter und bösartiger Aktivitäten in Ihrer AWS Cloud-Umgebung.
ID.RA-5	Bedrohungen, Sicherheitslücken, Wahrscheinlichkeit en und Auswirkungen werden verwendet , um Risiken zu bestimmen	cloud-trail-cloud-watch-Logs aktiviert	Verwenden Sie Amazon CloudWatc h , um Protokoll ereignisaktivitäten zentral zu sammeln und zu verwalten. Die Aufnahme von AWS CloudTrail Daten liefert Einzelheiten zu den API-Aufrufaktivitä ten in Ihrem AWS-Konto.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
ID.RA-5	Bedrohungen, Sicherheitslücken, Wahrscheinlichkeiten und Auswirkungen werden verwendet, um Risiken zu bestimmen	guardduty-enabled-centralized	Amazon GuardDuty kann mithilfe von Threat Intelligence Feeds helfen, potenzielle Cybersicherheitsereignisse zu überwachen und zu erkennen. Dazu gehören Listen mit bösartigen IPs und maschinellen Lernmethoden zur Identifizierung unerwarteter, nicht autorisierter und bösartiger Aktivitäten in Ihrer AWS Cloud-Umgebung.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
ID.RA-5	Bedrohungen, Sicherheitslücken, Wahrscheinlichkeiten und Auswirkungen werden verwendet, um Risiken zu bestimmen	rds-enhanced-monitoring-enabled	Aktivieren Sie Amazon Relational Database Service (Amazon RDS), um die Verfügbarkeit von Amazon RDS zu überwachen. Dies bietet einen detaillierten Einblick in den Zustand Ihrer Amazon-RDS-Datenbank-Instances. Wenn der Amazon-RDS-Speicher mehr als ein zugrunde liegendes physisches Gerät verwendet, erfasst Enhanced Monitoring die Daten für jedes Gerät. Wenn die Datenbank-Instance von Amazon RDS in einer Multi-AZ-Bereitstellung ausgeführt wird, werden außerdem die Daten für jedes Gerät auf dem sekundären Host sowie die Metriken des sekundären Hosts erfasst.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
ID.RA-5	Bedrohungen, Sicherheitslücken, Wahrscheinlichkeiten und Auswirkungen werden verwendet, um Risiken zu bestimmen	securityhub-enabled	AWS Security Hub hilft bei der Überwachung von unbefugtem Personal, Verbindungen, Geräten und Software. AWS Security Hub aggregiert, organisiert und priorisiert die Sicherheitswarnungen oder Ergebnisse mehrerer Dienste. AWS Einige dieser Dienste sind Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer und AWS Firewall Manager sowie AWS Partnerlösungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
ID.SC-4	Lieferanten und Drittanbieter werden routinemäßig anhand von Audits, Testergebnissen oder anderen Formen von Bewertungen bewertet, um zu bestätigen, dass sie ihren vertragli chen Verpflichtungen nachkommen.	cloud-trail-cloud-watch-logs-aktiviert	Verwenden Sie Amazon CloudWatc h , um Protokoll ereignisaktivitäten zentral zu sammeln und zu verwalten. Die Aufnahme von AWS CloudTrail Daten liefert Einzelheiten zu den API-Aufrufaktivitä ten in Ihrem AWS-Konto.
ID.SC-4	Lieferanten und Drittanbieter werden routinemäßig anhand von Audits, Testergebnissen oder anderen Formen von Bewertungen bewertet, um zu bestätigen, dass sie ihren vertragli chen Verpflichtungen nachkommen.	guardduty-enabled-centralized	Amazon GuardDuty kann mithilfe von Threat Intellige nce Feeds helfen, potenzielle Cybersich erheitsereignisse zu überwachen und zu erkennen. Dazu gehören Listen mit bösartigen IPs und maschinel len Lernmethoden zur Identifizierung unerwarteter, nicht autorisierter und bösartiger Aktivitäten in Ihrer AWS Cloud-Umgebung.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
ID.SC-4	Lieferanten und Drittanbieter werden routinemäßig anhand von Audits, Testergebnissen oder anderen Formen von Bewertungen bewertet, um zu bestätigen, dass sie ihren vertragli chen Verpflichtungen nachkommen.	rds-enhanced-monit oring-enabled	Aktivieren Sie Amazon Relationa l Database Service (Amazon RDS), um die Verfügbarkeit von Amazon RDS zu überwachen. Dies bietet einen detaillierten Einblick in den Zustand Ihrer Amazon-RDS-Datenbank-Instances. Wenn der Amazon-RDS-Speicher mehr als ein zugrunde liegendes physische s Gerät verwendet , erfasst Enhanced Monitoring die Daten für jedes Gerät. Wenn die Datenbank-Instance von Amazon RDS in einer Multi-AZ-Bereitstellung ausgeführt wird, werden außerdem die Daten für jedes Gerät auf dem sekundären Host sowie die Metriken des sekundären Hosts erfasst.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
ID.SC-4	Lieferanten und Drittanbieter werden routinemäßig anhand von Audits, Testergebnissen oder anderen Formen von Bewertungen bewertet, um zu bestätigen, dass sie ihren vertragli chen Verpflichtungen nachkommen.	securityhub-enabled	AWS Security Hub hilft bei der Überwachung von unbefugtem Personal, Verbindun gen, Geräten und Software. AWS Security Hub aggregiert, organisie rt und priorisie rt die Sicherhei tswarnungen oder Ergebnisse mehrerer Dienste. AWS Einig e dieser Dienste sind Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer und AWS Firewall Manager sowie AWS Partnerlösungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.AC-1	Identitäten und Anmeldeinformationen werden für autorisierte Geräte, Benutzer und Prozesse ausgestellt, verwaltet, verifiziert, gesperrt und geprüft	ec2- instance-profile-attached	EC2 Instanzprofile übergeben eine IAM-Rolle an eine EC2 Instance. Das Anhängen eines Instance-Profils an Ihre Instances kann bei der Implementierung von geringsten Berechtigungen und der Berechtigungsverwaltung helfen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.AC-1	Identitäten und Anmeldeinformationen werden für autorisierte Geräte, Benutzer und Prozesse ausgestellt, verwaltet, verifiziert, gesperrt und geprüft	ecs-task-definition-user-for-host-mode-check	Wenn für eine Aufgabendefinition erhöhte Berechtigungen gelten, liegt das daran, dass der Kunde diesen Konfigurationen ausdrücklich zugestimmt hat. Diese Kontrolle prüft, ob eine unerwartete Berechtigungseskalation vorliegt, wenn für eine Aufgabendefinition das Host-Netzwerk aktiviert ist, die Kunden aber keine erhöhten Berechtigungen aktiviert haben.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.AC-1	Identitäten und Anmeldeinformationen werden für autorisierte Geräte, Benutzer und Prozesse ausgestellt, verwaltet, verifiziert, gesperrt und geprüft	iam-no-inline-policy-überprüfen	Stellen Sie sicher, dass ein Benutzer, eine IAM-Rolle oder eine IAM-Gruppe (AWS Identity and Access Management) nicht über eine Inline-Richtlinie zur Zugriffskontrolle auf Systeme und Ressourcen verfügt. AWS empfiehlt, verwaltete Richtlinien anstelle von Inline-Richtlinien zu verwenden. Verwaltete Richtlinien ermöglichen Wiederverwendbarkeit, Versionsverwaltung, Rollback und Delegierung der Berechtigungsverwaltung.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.AC-1	Identitäten und Anmeldeinformationen werden für autorisierte Geräte, Benutzer und Prozesse ausgestellt, verwaltet, verifiziert, gesperrt und geprüft	iam-policy-no-statements-with-full-access	Stellen Sie sicher, dass IAM-Aktionen nur auf die benötigten Aktionen beschränkt sind. Wenn Benutzern mehr Rechte eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Rechte und der Aufgabentrennung verstoßen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.AC-1	Identitäten und Anmeldeinformationen werden für autorisierte Geräte, Benutzer und Prozesse ausgestellt, verwaltet, verifiziert, gesperrt und geprüft	access-keys-rotated	Die Anmeldeinformationen für autorisierte Geräte, Benutzer und Prozesse werden geprüft, indem sichergestellt wird, dass die IAM-Zugriffsschlüssel entsprechend den Vorgaben der Unternehmensrichtlinie rotiert werden. Das regelmäßige Ändern der Zugriffsschlüssel ist eine bewährte Sicherheitsmethode. Es verkürzt den Zeitraum, in dem ein Zugriffsschlüssel aktiv ist, und reduziert die Auswirkungen auf das Unternehmen, wenn die Schlüssel kompromittiert werden. Diese Regel erfordert einen Wert für die Zugriffsschlüssel-Rotation (Standard konfiguration: 90). Der tatsächliche Wert muss den Richtlini

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			en Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.AC-1	Identitäten und Anmeldeinformationen werden für autorisierte Geräte, Benutzer und Prozesse ausgestellt, verwaltet, verifiziert, gesperrt und geprüft	emr-kerberos-enabled	Die Zugriffsberechtigungen und -autorisierungen können verwaltet und nach den Prinzipien der geringsten Berechtigung und Aufgabentrennung integriert werden, indem Kerberos für Amazon-EMR-Cluster aktiviert wird. In Kerberos werden Services und Benutzer, die sich authentifizieren müssen, als Prinzipale bezeichnet. Prinzipale befinden sich in einem Kerberos-Bereich. Innerhalb dieses Bereichs wird ein Kerberos-Server als Key Distribution Center (KDC) bezeichnet. Über diesen Server können sich Prinzipale authentifizieren. Die Authentifizierung im KDC erfolgt durch die Ausstellung von Authentif

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			izierungstickets. Das KDC unterhält eine Datenbank der Prinzipale in seinem Bereich mit ihren Passwörtern und anderen administr ativen Informationen zu jedem Prinzipal.
PR.AC-1	Identitäten und Anmeldeinformation en werden für autorisierte Geräte, Benutzer und Prozesse ausgestellt, verwaltet, verifiziert, gesperrt und geprüft	iam-group-has-users-überprüfen	AWS Identity and Access Managemen t (IAM) kann Ihnen helfen, die Prinzipien der geringsten Rechte und der Aufgabent rennung mit Zugriffsb erechtigungen und Autorisierungen zu integrieren, indem sichergestellt wird, dass IAM-Gruppen mindestens einen Benutzer haben. Die Einteilung von Benutzern in Gruppen auf der Grundlage der ihnen zugewiese nen Berechtigungen oder ihrer Funktion ist eine Möglichkeit, das Prinzip der geringste n Berechtigung zu implementieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.AC-1	Identitäten und Anmeldeinformationen werden für autorisierte Geräte, Benutzer und Prozesse ausgestellt, verwaltet, verifiziert, gesperrt und geprüft	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) kann Ihnen dabei helfen, die Prinzipien der geringsten Rechte und der Aufgabentrennung in Zugriffsberechtigungen und Autorisierungen zu integrieren und so zu verhindern, dass Richtlinien „Effect“: „Allow“ mit „Action“: „*“ anstelle von „Resource“: „*“ enthalten. Wenn Benutzern mehr Rechte eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und der Aufgabentrennung verstoßen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.AC-1	Identitäten und Anmeldeinformationen werden für autorisierte Geräte, Benutzer und Prozesse ausgestellt, verwaltet, verifiziert, gesperrt und geprüft	iam-root-access-key-überprüfen	Der Zugriff auf Systeme und Ressourcen kann gesteuert werden, indem überprüft wird, ob der Root-Benutzer keine Zugriffsschlüssel mit seiner AWS Identity and Access Management (IAM) -Rolle verknüpft hat. Stellen Sie sicher, dass die Root-Zugriffsschlüssel gelöscht werden. Erstellen und verwenden Sie stattdessen rollenbasierte Funktionen, AWS-Konten um das Prinzip der geringsten Funktionalität zu berücksichtigen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.AC-1	Identitäten und Anmeldeinformationen werden für autorisierte Geräte, Benutzer und Prozesse ausgestellt, verwaltet, verifiziert, gesperrt und geprüft	iam-user-mfa-enabled	Aktivieren Sie diese Regel, um den Zugriff auf Ressourcen in der AWS -Cloud einzuschränken. Diese Regel stellt sicher, dass die Multi-Faktor-Authentifizierung (MFA) für alle Benutzer aktiviert ist. MFA bietet eine weitere Schutzebene zusätzlich zum Benutzernamen und Passwort. Reduzieren Sie Fälle von kompromittierten Konten, indem Sie MFA für Benutzer vorschreiben.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.AC-1	Identitäten und Anmeldeinformationen werden für autorisierte Geräte, Benutzer und Prozesse ausgestellt, verwaltet, verifiziert, gesperrt und geprüft	iam-user-no-policies-überprüfen	Diese Regel stellt sicher, dass AWS Identity and Access Management (IAM) -Richtlinien nur Gruppen oder Rollen zugewiesen werden, um den Zugriff auf Systeme und Ressourcen zu kontrollieren. Die Zuweisung von Berechtigungen auf Gruppen- oder Rollenebene trägt dazu bei, die Wahrscheinlichkeit zu verringern, dass eine Identität übermäßige Berechtigungen erhält oder beibehält.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.AC-1	Identitäten und Anmeldeinformationen werden für autorisierte Geräte, Benutzer und Prozesse ausgestellt, verwaltet, verifiziert, gesperrt und geprüft	iam-user-unused-credentials-überprüfen	AWS Identity and Access Management (IAM) kann Ihnen bei Zugriffsberechtigungen und Autorisierungen helfen, indem es nach IAM-Passwörtern und Zugriffsschlüsseln sucht, die für einen bestimmten Zeitraum nicht verwendet wurden. Wenn ungenutzte Anmeldeinformationen identifiziert werden, müssen Sie sie deaktivieren und/oder entfernen, da dies gegen das Prinzip der geringsten Berechtigung verstoßen könnte. Für diese Regel müssen Sie einen Wert für das maxCredentialUsage Alter festlegen (Standardkonfiguration: 90). Der tatsächliche Wert muss den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.AC-1	Identitäten und Anmeldeinformationen werden für autorisierte Geräte, Benutzer und Prozesse ausgestellt, verwaltet, verifiziert, gesperrt und geprüft	secretsmanager-rotation-enabled-check	Diese Regel stellt sicher, dass bei AWS Secrets Manager Manager-Geheimnissen die Rotation aktiviert ist. Die regelmäßige Rotation von Secrets kann den Zeitraum verkürzen, in dem ein Secret aktiv ist, und möglicherweise die Auswirkungen auf das Unternehmen verringern, falls das Secret kompromittiert wird.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.AC-1	Identitäten und Anmeldeinformationen werden für autorisierte Geräte, Benutzer und Prozesse ausgestellt, verwaltet, verifiziert, gesperrt und geprüft	iam-password-policy	Die Identitäten und Anmeldeinformationen werden auf der Grundlage einer organisatorischen IAM-Passwortrichtlinie ausgestellt, verwaltet und verifiziert. Sie erfüllen oder übertreffen die Anforderungen, die von NIST SP 800-63 und dem Standard AWS Foundational Security Best Practices für die Passwortstärke festgelegt sind. Mit dieser Regel können Sie optional RequireUppercaseCharacters (Wert für AWS grundlegende Sicherheitsbewährte Methoden: wahr), RequireLowercaseCharacters (Wert für bewährte Methoden für AWS grundlegende Sicherheit: wahr), RequireSymbols (Wert für bewährte Methoden für AWS grundlege

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			nde Sicherheit: wahr), RequireNumbers (Wert für bewährte Methoden für AWS grundlegende Sicherheit: wahr), MinimumPasswordLength (Wert für bewährte Methoden für AWS grundlegende Sicherheit: 14), PasswordReusePrevention (Wert für bewährte Methoden für AWS grundlegende Sicherheit: 24) und MaxPasswordAge (Wert für bewährte Methoden für AWS grundlegende Sicherheit: 90) für Ihr IAM festlegen Kennwortrichtlinie. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.AC-3	Der Fernzugriff wird verwaltet.	autoscaling-launch-config-public-ip-deaktiviert	Wenn Sie Ihre Netzwerkschnittstellen mit einer öffentlichen IP-Adresse konfigurieren, sind die diesen Netzwerkschnittstellen zugehörigen Ressourcen über das Internet erreichbar. EC2 Ressourcen sollten nicht öffentlich zugänglich sein, da dies einen unbeabsichtigten Zugriff auf Ihre Anwendungen oder Server ermöglichen kann.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.AC-3	Der Fernzugriff wird verwaltet.	ec2- instances-in-vpc	Stellen Sie Amazon Elastic Compute Cloud (Amazon EC2) -Instances innerhalb einer Amazon Virtual Private Cloud (Amazon VPC) bereit, um eine sichere Kommunika tion zwischen einer Instance und anderen Services innerhalb der Amazon VPC zu ermöglichen, ohne dass ein Internet-Gateway, ein NAT-Gerät oder eine VPN-Verbindung erforderlich ist. Der gesamte Datenverk ehr bleibt sicher in der AWS Cloud. Domains, die sich innerhalb einer VPC befinden, verfügen aufgrund ihrer logischen Isolierun g im Vergleich zu Domains mit öffentlic hen Endpunkten über eine zusätzlic he Sicherheitsebene. Weisen Sie EC2

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			Amazon-Instances einer Amazon-VPC zu, um den Zugriff ordnungsgemäß zu verwalten.
PR.AC-3	Der Fernzugriff wird verwaltet.	no-unrestricted-route-to-igw	Stellen Sie sicher, dass EC2 Amazon-Routentabellen keine uneingeschränkten Routen zu einem Internet-Gateway enthalten. Durch das Entfernen oder Beschränken des Internetzugangs für Workloads innerhalb von Amazon VPCs können unbeabsic htigte Zugriffe in Ihrer Umgebung reduziert werden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.AC-3	Der Fernzugriff wird verwaltet.	redshift-enhanced-vpc-routing-aktiviert	Mit Enhanced-VPC-Routing wird erzwungen, dass der gesamte COPY- und UNLOAD-Datenverkehr zwischen Ihrem Cluster und Datenrepositorys über Ihre Amazon VPC erfolgt. Anschließend können Sie VPC-Features wie Sicherheitsgruppen und Netzwerkzugriffskontrolllisten verwenden, um den Netzwerkverkehr zu schützen. Sie können auch VPC-Flow-Logs verwenden, um den Netzwerkverkehr zu überwachen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.AC-3	Der Fernzugriff wird verwaltet.	ssm-document-not-public	Stellen Sie sicher, dass AWS Systems Manager (SSM) - Dokumente nicht öffentlich sind, da dies einen unbeabsichtigten Zugriff auf Ihre SSM-Dokumente ermöglichen kann. Ein öffentliches SSM-Dokument kann Informationen über Ihr Konto, Ihre Ressourcen und internen Prozesse preisgeben.
PR.AC-3	Der Fernzugriff wird verwaltet.	dms-replication-not-public	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass auf DMS-Replikationsinstanzen nicht öffentlich zugegriffen werden kann. DMS-Replikations-Instances können vertrauliche Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.AC-3	Der Fernzugriff wird verwaltet.	ebs-snapshot-public-restorable-überprüfen	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass EBS-Snapshots nicht öffentlich wiederher stellbar sind. EBS-Volume-Snapsho ts können vertrauli che Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.
PR.AC-3	Der Fernzugriff wird verwaltet.	ec-2 instance-no-public-ip	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon Elastic Compute Cloud (Amazon EC2) - Instances nicht öffentlich zugänglic h sind. EC2Amazon -Instances können vertrauliche Informati onen enthalten, und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.AC-3	Der Fernzugriff wird verwaltet.	elasticsearch-in-vpc-only	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass sich Amazon OpenSearch OpenSearch Service (Service) - Domains innerhalb einer Amazon Virtual Private Cloud (Amazon VPC) befinden. Eine OpenSearch Service-Domain innerhalb einer Amazon VPC ermöglicht die sichere Kommunikation zwischen OpenSearch Service und anderen Services innerhalb der Amazon VPC, ohne dass ein Internet-Gateway, ein NAT-Gerät oder eine VPN-Verbindung erforderlich ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.AC-3	Der Fernzugriff wird verwaltet.	emr-master-no-public-ip	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon EMR-Cluster-Masterknoten nicht öffentlich zugänglich sind. Amazon-EMR-Cluster-Hauptknoten können vertrauliche Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.AC-3	Der Fernzugriff wird verwaltet.	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) Security Groups können bei der Verwaltung des Netzwerkzugriffs helfen, indem sie eine statusbeh aftete Filterung von eingehendem und ausgehendem Netzwerkverkehr zu Ressourcen bereitste llen. AWS Wenn Sie eingehenden (oder entfernten) Datenverk ehr von 0.0.0.0/0 bis Port 22 auf Ihren Ressourcen nicht zulassen, können Sie den Remote-Zugriff einschränken.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.AC-3	Der Fernzugriff wird verwaltet.	lambda-function-public-access-verboten	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass AWS Lambda-Funktionen nicht öffentlich zugänglich sind. Der öffentliche Zugriff kann möglicherweise die Verfügbarkeit von Ressourcen beeinträchtigen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.AC-3	Der Fernzugriff wird verwaltet.	lambda-inside-vpc	Stellen Sie AWS Lambda-Funktionen in einer Amazon Virtual Private Cloud (Amazon VPC) bereit, um eine sichere Kommunika tion zwischen einer Funktion und anderen Diensten innerhalb der Amazon VPC zu gewährleisten. Bei dieser Konfiguration sind kein Internet-Gateway, kein NAT-Gerät und keine VPN-Verbindung erforderlich. Der gesamte Datenverk ehr bleibt sicher in der Cloud. AWS Domains, die sich innerhalb einer VPC befinden, verfügen aufgrund ihrer logischen Isolierun g im Vergleich zu Domains mit öffentlic hen Endpunkten über eine zusätzliche Sicherheitsebene. Um den Zugriff ordnungsg emäß zu verwalten,

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			sollten AWS Lambda-Funktionen einer VPC zugewiesen werden.
PR.AC-3	Der Fernzugriff wird verwaltet.	opensearch-in-vpc-only	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass sich Amazon OpenSearch Service-Domains innerhalb einer Amazon Virtual Private Cloud (Amazon VPC) befinden. Eine Amazon OpenSearch Service-Domain innerhalb einer Amazon VPC ermöglicht die sichere Kommunikation zwischen Amazon OpenSearch Service und anderen Services innerhalb der Amazon VPC, ohne dass ein Internet-Gateway, ein NAT-Gerät oder eine VPN-Verbindung erforderlich ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.AC-3	Der Fernzugriff wird verwaltet.	rds-instance-public-access-überprüfen	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Relational Database Service (Amazon RDS) -Instances nicht öffentlich sind. Amazon-RDS-Datenbank-Instances können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.AC-3	Der Fernzugriff wird verwaltet.	rds-snapshots-public-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Relational Database Service (Amazon RDS) -Instances nicht öffentlich sind. Amazon-RDS-Datenbank-Instances können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.AC-3	Der Fernzugriff wird verwaltet.	redshift-cluster-public-access-überprüfen	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Redshift Redshift-Cluster nicht öffentlich sind. Amazon-Redshift-Cluster können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.AC-3	Der Fernzugriff wird verwaltet.	restricted-common-ports	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass gemeinsame Ports für Amazon Elastic Compute Cloud (Amazon EC2) -Sicherheitsgruppen eingeschränkt sind. Wenn der Zugriff auf Ports nicht auf vertrauenswürdige Quellen beschränkt wird, kann dies zu Angriffen auf die Verfügbarkeit, Integrität und Vertraulichkeit von Systemen führen. Mit dieser Regel können Sie optional die Parameter blockedPort1–blockedPort5 festlegen (Standardkonfigurationen: 20, 21, 3389, 3306, 4333). Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.AC-3	Der Fernzugriff wird verwaltet.	s3- account-level-public-access -Block-periodisch	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Simple Storage Service (Amazon S3) -Buckets nicht öffentlich zugänglich sind. Diese Regel trägt dazu bei, sensible Daten vor unbefugten Remote-Benutzern zu schützen, indem sie den öffentlichen Zugriff verhindert. Mit dieser Regel können Sie optional die Parameter ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) und restrictPublicBuckets Parameter (Config Default: True) festlegen. Die tatsächlichen Werte müssen den Richtlini

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			en Ihrer Organisation entsprechen.
PR.AC-3	Der Fernzugriff wird verwaltet.	s3- bucket-public-read -prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie nur autorisierten Benutzern, Prozessen und Geräten Zugriff auf Amazon Simple Storage Service (Amazon S3) - Buckets gewähren. Die Verwaltung des Zugriffs sollte mit der Klassifizierung der Daten übereinst immen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.AC-3	Der Fernzugriff wird verwaltet.	s3- bucket-public-write-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie nur autorisierten Benutzern, Prozessen und Geräten Zugriff auf Amazon Simple Storage Service (Amazon S3) - Buckets gewähren. Die Verwaltung des Zugriffs sollte mit der Klassifizierung der Daten übereinstimmen.
PR.AC-3	Der Fernzugriff wird verwaltet.	sagemaker-notebook-no-direct-Internetzugang	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass SageMaker Amazon-Notebooks keinen direkten Internetzugang zulassen. Indem Sie direkten Internetzugang blockieren, vermeiden Sie, dass unbefugte Benutzer auf sensible Daten zugreifen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.AC-3	Der Fernzugriff wird verwaltet.	subnet-auto-assign-public-ip-deaktiviert	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon Virtual Private Cloud (VPC) -Subnetzen nicht automatisch eine öffentliche IP-Adresse zugewiesen wird. Amazon Elastic Compute Cloud (EC2) -Instances, die in Subnetzen gestartet werden, in denen dieses Attribut aktiviert ist, haben ihrer primären Netzwerkschnittstelle eine öffentliche IP-Adresse zugewiesen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.AC-3	Der Fernzugriff wird verwaltet.	vpc-default-security-group-geschlossen	Sicherheitsgruppen von Amazon Elastic Compute Cloud (Amazon EC2) können bei der Verwaltung des Netzwerkzugriffs helfen, indem sie eine statusbehaftete Filterung des ein- und ausgehenden Netzwerkverkehrs zu Ressourcen bereitstellen. AWS Die Beschränk ung des gesamten Datenverkehrs auf die Standardsicherheit sgruppe hilft dabei, den Fernzugriff auf Ihre Ressourcen einzuschränken. AWS

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.AC-3	Der Fernzugriff wird verwaltet.	vpc-sg-open-only-to-authorized-ports	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass gemeinsame Ports für Amazon Elastic Compute Cloud (Amazon EC2) -Sicherheitsgruppen eingeschränkt sind. Wenn der Zugriff auf Ports nicht auf vertrauenswürdige Quellen beschränkt wird, kann dies zu Angriffen auf die Verfügbarkeit, Integrität und Vertraulichkeit von Systemen führen. Durch die Beschränkung des Zugriffs auf Ressourcen innerhalb einer Sicherheitsgruppe aus dem Internet (0.0.0.0/0) kann der Fernzugriff auf interne Systeme gesteuert werden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.AC-4	Zugriffsberechtigungen und Autorisierungen werden nach den Grundsätzen der geringsten Rechte und der Aufgabentrennung verwaltet	autoscaling-launch-config-public-ip-deaktiviert	Wenn Sie Ihre Netzwerkschnittstellen mit einer öffentlichen IP-Adresse konfigurieren, sind die diesen Netzwerkschnittstellen zugehörigen Ressourcen über das Internet erreichbar. EC2 Ressourcen sollten nicht öffentlich zugänglich sein, da dies einen unbeabsichtigten Zugriff auf Ihre Anwendungen oder Server ermöglichen kann.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.AC-4	Zugriffsberechtigungen und Autorisierungen werden nach den Grundsätzen der geringsten Rechte und der Aufgabentrennung verwaltet	ec2-imdsv2-check	Stellen Sie sicher, dass die Methode Instance Metadata Service Version 2 (IMDSv2) aktiviert ist, um den Zugriff auf und die Kontrolle der Amazon Elastic Compute Cloud (Amazon EC2) - Instance-Metadaten zu schützen. Die IMDSv2 Methode verwendet sitzungsbasierte Kontrollen. Mit können Kontrollen implementiert werden IMDSv2, um Änderungen an Instanzmetadaten einzuschränken.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.AC-4	Zugriffsberechtigungen und Autorisierungen werden nach den Grundsätzen der geringsten Rechte und der Aufgabentrennung verwaltet	ec-2 instance-profile-attached	EC2 Instanzprofile übergeben eine IAM-Rolle an eine EC2 Instance. Das Anhängen eines Instance-Profils an Ihre Instances kann bei der Implementierung von geringsten Berechtigungen und der Berechtigungsverwaltung helfen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.AC-4	Zugriffsberechtigungen und Autorisierungen werden nach den Grundsätzen der geringsten Rechte und der Aufgabentrennung verwaltet	ecs-task-definition-user-for-host-mode-check	Wenn für eine Aufgabendefinition erhöhte Berechtigungen gelten, liegt das daran, dass der Kunde diesen Konfigurationen ausdrücklich zugestimmt hat. Diese Kontrolle prüft, ob eine unerwartete Berechtigungseskalation vorliegt, wenn für eine Aufgabendefinition das Host-Netzwerk aktiviert ist, die Kunden aber keine erhöhten Berechtigungen aktiviert haben.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.AC-4	Zugriffsberechtigungen und Autorisierungen werden nach den Grundsätzen der geringsten Rechte und der Aufgabentrennung verwaltet	iam-no-inline-policy-überprüfen	Stellen Sie sicher, dass ein Benutzer, eine IAM-Rolle oder eine IAM-Gruppe (AWS Identity and Access Management) nicht über eine Inline-Richtlinie zur Zugriffskontrolle auf Systeme und Ressourcen verfügt. AWS empfiehlt, verwaltete Richtlinien anstelle von Inline-Richtlinien zu verwenden. Verwaltete Richtlinien ermöglichen Wiederverwendbarkeit, Versionsverwaltung, Rollback und Delegierung der Berechtigungsverwaltung.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.AC-4	Zugriffsberechtigungen und Autorisierungen werden nach den Grundsätzen der geringsten Rechte und der Aufgabentrennung verwaltet	iam-policy-no-statements-with-full-access	Stellen Sie sicher, dass IAM-Aktionen nur auf die benötigten Aktionen beschränkt sind. Wenn Benutzern mehr Rechte eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Rechte und der Aufgabentrennung verstoßen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.AC-4	Zugriffsberechtigungen und Autorisierungen werden nach den Grundsätzen der geringsten Rechte und der Aufgabentrennung verwaltet	ec-2 instances-in-vpc	Stellen Sie Amazon Elastic Compute Cloud (Amazon EC2) -Instances innerhalb einer Amazon Virtual Private Cloud (Amazon VPC) bereit, um eine sichere Kommunikation zwischen einer Instance und anderen Services innerhalb der Amazon VPC zu ermöglichen, ohne dass ein Internet-Gateway, ein NAT-Gerät oder eine VPN-Verbindung erforderlich ist. Der gesamte Datenverkehr bleibt sicher in der AWS Cloud. Domains, die sich innerhalb einer VPC befinden, verfügen aufgrund ihrer logischen Isolierung im Vergleich zu Domains mit öffentlichen Endpunkten über eine zusätzliche Sicherheitsebene. Weisen Sie EC2

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			Amazon-Instances einer Amazon-VPC zu, um den Zugriff ordnungsgemäß zu verwalten.
PR.AC-4	Zugriffsberechtigungen und Autorisierungen werden nach den Grundsätzen der geringsten Rechte und der Aufgabentrennung verwaltet	ssm-document-not-public	Stellen Sie sicher, dass AWS Systems Manager (SSM) - Dokumente nicht öffentlich sind, da dies einen unbeabsichtigten Zugriff auf Ihre SSM-Dokumente ermöglichen kann. Ein öffentliches SSM-Dokument kann Informationen über Ihr Konto, Ihre Ressourcen und internen Prozesse preisgeben.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.AC-4	Zugriffsberechtigungen und Autorisierungen werden nach den Grundsätzen der geringsten Rechte und der Aufgabentrennung verwaltet	dms-replication-not-public	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass auf DMS-Replikationsinstanzen nicht öffentlich zugegriffen werden kann. DMS-Replikations-Instances können vertrauliche Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.
PR.AC-4	Zugriffsberechtigungen und Autorisierungen werden nach den Grundsätzen der geringsten Rechte und der Aufgabentrennung verwaltet	ebs-snapshot-public-restorable-überprüfen	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass EBS-Snapshots nicht öffentlich wiederherstellbar sind. EBS-Volume-Snapshots können vertrauliche Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.AC-4	Zugriffsberechtigungen und Autorisierungen werden nach den Grundsätzen der geringsten Rechte und der Aufgabentrennung verwaltet	ec-2 instance-no-public-ip	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon Elastic Compute Cloud (Amazon EC2) - Instances nicht öffentlich zugänglich sind. EC2Amazon -Instances können vertrauliche Informationen enthalten, und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.AC-4	Zugriffsberechtigungen und Autorisierungen werden nach den Grundsätzen der geringsten Rechte und der Aufgabentrennung verwaltet	elasticsearch-in-vpc-only	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass sich Amazon OpenSearch OpenSearch Service (Service) - Domains innerhalb einer Amazon Virtual Private Cloud (Amazon VPC) befinden. Eine OpenSearch Service-Domain innerhalb einer Amazon VPC ermöglicht die sichere Kommunikation zwischen OpenSearch Service und anderen Services innerhalb der Amazon VPC, ohne dass ein Internet-Gateway, ein NAT-Gerät oder eine VPN-Verbindung erforderlich ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.AC-4	Zugriffsberechtigungen und Autorisierungen werden nach den Grundsätzen der geringsten Rechte und der Aufgabentrennung verwaltet	emr-kerberos-enabled	Die Zugriffsberechtigungen und -autorisierungen können verwaltet und nach den Prinzipien der geringsten Berechtigung und Aufgabentrennung integriert werden, indem Kerberos für Amazon-EMR-Cluster aktiviert wird. In Kerberos werden Services und Benutzer, die sich authentifizieren müssen, als Prinzipale bezeichnet. Prinzipale befinden sich in einem Kerberos-Bereich. Innerhalb dieses Bereichs wird ein Kerberos-Server als Key Distribution Center (KDC) bezeichnet. Über diesen Server können sich Prinzipale authentifizieren. Die Authentifizierung im KDC erfolgt durch die Ausstellung von Authentif

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			izierungstickets. Das KDC unterhält eine Datenbank der Prinzipale in seinem Bereich mit ihren Passwörtern und anderen administrativen Informationen zu jedem Prinzipal.
PR.AC-4	Zugriffsberechtigungen und Autorisierungen werden nach den Grundsätzen der geringsten Rechte und der Aufgabentrennung verwaltet	emr-master-no-public-ip	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon EMR-Cluster-Masterknoten nicht öffentlich zugänglich sind. Amazon-EMR-Cluster-Hauptknoten können vertrauliche Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.AC-4	Zugriffsberechtigungen und Autorisierungen werden nach den Grundsätzen der geringsten Rechte und der Aufgabentrennung verwaltet	iam-group-has-users-überprüfen	AWS Identity and Access Management (IAM) kann Ihnen helfen, die Prinzipien der geringsten Rechte und der Aufgabentrennung mit Zugriffsberechtigungen und Autorisierungen zu integrieren, indem sichergestellt wird, dass IAM-Gruppen mindestens einen Benutzer haben. Die Einteilung von Benutzern in Gruppen auf der Grundlage der ihnen zugewiesenen Berechtigungen oder ihrer Funktion ist eine Möglichkeit, das Prinzip der geringsten Berechtigung zu implementieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.AC-4	Zugriffsberechtigungen und Autorisierungen werden nach den Grundsätzen der geringsten Rechte und der Aufgabentrennung verwaltet	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) kann Ihnen dabei helfen, die Prinzipien der geringsten Rechte und der Aufgabentrennung in Zugriffsberechtigungen und Autorisierungen zu integrieren und so zu verhindern, dass Richtlinien „Effect“: „Allow“ mit „Action“: „*“ anstelle von „Resource“: „*“ enthalten. Wenn Benutzern mehr Rechte eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und der Aufgabentrennung verstoßen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.AC-4	Zugriffsberechtigungen und Autorisierungen werden nach den Grundsätzen der geringsten Rechte und der Aufgabentrennung verwaltet	iam-root-access-key-überprüfen	Der Zugriff auf Systeme und Ressourcen kann gesteuert werden, indem überprüft wird, ob der Root-Benutzer keine Zugriffsschlüssel mit seiner AWS Identity and Access Management (IAM) -Rolle verknüpft hat. Stellen Sie sicher, dass die Root-Zugriffsschlüssel gelöscht werden. Erstellen und verwenden Sie stattdessen rollenbasierte Funktionen, AWS-Konten um das Prinzip der geringsten Funktionalität zu berücksichtigen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.AC-4	Zugriffsberechtigungen und Autorisierungen werden nach den Grundsätzen der geringsten Rechte und der Aufgabentrennung verwaltet	iam-user-no-policies-überprüfen	Diese Regel stellt sicher, dass AWS Identity and Access Management (IAM) -Richtlinien nur Gruppen oder Rollen zugewiesen werden, um den Zugriff auf Systeme und Ressourcen zu kontrollieren. Die Zuweisung von Berechtigungen auf Gruppen- oder Rollenebene trägt dazu bei, die Wahrscheinlichkeit zu verringern, dass eine Identität übermäßige Berechtigungen erhält oder beibehält.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.AC-4	Zugriffsberechtigungen und Autorisierungen werden nach den Grundsätzen der geringsten Rechte und der Aufgabentrennung verwaltet	iam-user-unused-credentials-überprüfen	AWS Identity and Access Management (IAM) kann Ihnen bei Zugriffsberechtigungen und Autorisierungen helfen, indem es nach IAM-Passwörtern und Zugriffsschlüsseln sucht, die für einen bestimmten Zeitraum nicht verwendet wurden. Wenn ungenutzte Anmeldeinformationen identifiziert werden, müssen Sie sie deaktivieren und/oder entfernen, da dies gegen das Prinzip der geringsten Berechtigung verstoßen könnte. Für diese Regel müssen Sie einen Wert für das maxCredentialUsage Alter festlegen (Standardkonfiguration: 90). Der tatsächliche Wert muss den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.AC-4	Zugriffsberechtigungen und Autorisierungen werden nach den Grundsätzen der geringsten Rechte und der Aufgabentrennung verwaltet	lambda-function-public-access-verboten	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass AWS Lambda-Funktionen nicht öffentlich zugänglich sind. Der öffentliche Zugriff kann möglicherweise die Verfügbarkeit von Ressourcen beeinträchtigen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.AC-4	Zugriffsberechtigungen und Autorisierungen werden nach den Grundsätzen der geringsten Rechte und der Aufgabentrennung verwaltet	lambda-inside-vpc	Stellen Sie AWS Lambda-Funktionen in einer Amazon Virtual Private Cloud (Amazon VPC) bereit, um eine sichere Kommunikation zwischen einer Funktion und anderen Diensten innerhalb der Amazon VPC zu gewährleisten. Bei dieser Konfiguration sind kein Internet-Gateway, kein NAT-Gerät und keine VPN-Verbindung erforderlich. Der gesamte Datenverkehr bleibt sicher in der Cloud. AWS Domains, die sich innerhalb einer VPC befinden, verfügen aufgrund ihrer logischen Isolierung im Vergleich zu Domains mit öffentlichen Endpunkten über eine zusätzliche Sicherheitsebene. Um den Zugriff ordnungsgemäß zu verwalten,

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			sollten AWS Lambda-Funktionen einer VPC zugewiesen werden.
PR.AC-4	Zugriffsberechtigungen und Autorisierungen werden nach den Grundsätzen der geringsten Rechte und der Aufgabentrennung verwaltet	opensearch-in-vpc-only	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass sich Amazon OpenSearch Service-Domains innerhalb einer Amazon Virtual Private Cloud (Amazon VPC) befinden. Eine Amazon OpenSearch Service-Domain innerhalb einer Amazon VPC ermöglicht die sichere Kommunikation zwischen Amazon OpenSearch Service und anderen Services innerhalb der Amazon VPC, ohne dass ein Internet-Gateway, ein NAT-Gerät oder eine VPN-Verbindung erforderlich ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.AC-4	Zugriffsberechtigungen und Autorisierungen werden nach den Grundsätzen der geringsten Rechte und der Aufgabentrennung verwaltet	rds-instance-public-access-überprüfen	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Relational Database Service (Amazon RDS) -Instances nicht öffentlich sind. Amazon-RDS-Datenbank-Instances können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.AC-4	Zugriffsberechtigungen und Autorisierungen werden nach den Grundsätzen der geringsten Rechte und der Aufgabentrennung verwaltet	rds-snapshots-public-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Relational Database Service (Amazon RDS) -Instances nicht öffentlich sind. Amazon-RDS-Datenbank-Instances können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.AC-4	Zugriffsberechtigungen und Autorisierungen werden nach den Grundsätzen der geringsten Rechte und der Aufgabentrennung verwaltet	redshift-cluster-public-access-überprüfen	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Redshift Redshift-Cluster nicht öffentlich sind. Amazon-Redshift-Cluster können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.AC-4	Zugriffsberechtigungen und Autorisierungen werden nach den Grundsätzen der geringsten Rechte und der Aufgabentrennung verwaltet	s3- -Block-periodisch account-level-public-access	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Simple Storage Service (Amazon S3) -Buckets nicht öffentlich zugänglich sind. Diese Regel trägt dazu bei, sensible Daten vor unbefugten Remote-Benutzern zu schützen, indem sie den öffentlichen Zugriff verhindert. Mit dieser Regel können Sie optional die Parameter ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) und restrictPublicBuckets Parameter (Config Default: True) festlegen. Die tatsächlichen Werte müssen den Richtlini

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			en Ihrer Organisation entsprechen.
PR.AC-4	Zugriffsberechtigungen und Autorisierungen werden nach den Grundsätzen der geringsten Rechte und der Aufgabentrennung verwaltet	s3- bucket-public-read-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie nur autorisierten Benutzern, Prozessen und Geräten Zugriff auf Amazon Simple Storage Service (Amazon S3) - Buckets gewähren. Die Verwaltung des Zugriffs sollte mit der Klassifizierung der Daten übereinstimmen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.AC-4	Zugriffsberechtigungen und Autorisierungen werden nach den Grundsätzen der geringsten Rechte und der Aufgabentrennung verwaltet	s3- bucket-public-write-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie nur autorisierten Benutzern, Prozessen und Geräten Zugriff auf Amazon Simple Storage Service (Amazon S3) - Buckets gewähren. Die Verwaltung des Zugriffs sollte mit der Klassifizierung der Daten übereinstimmen.
PR.AC-4	Zugriffsberechtigungen und Autorisierungen werden nach den Grundsätzen der geringsten Rechte und der Aufgabentrennung verwaltet	sagemaker-notebook-no-direct-Internetzugang	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass SageMaker Amazon-Notebooks keinen direkten Internetzugang zulassen. Indem Sie direkten Internetzugang blockieren, vermeiden Sie, dass unbefugte Benutzer auf sensible Daten zugreifen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.AC-4	Zugriffsberechtigungen und Autorisierungen werden nach den Grundsätzen der geringsten Rechte und der Aufgabentrennung verwaltet	subnet-auto-assign-public-ip-deaktiviert	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon Virtual Private Cloud (VPC) -Subnetzen nicht automatisch eine öffentliche IP-Adresse zugewiesen wird. Amazon Elastic Compute Cloud (EC2) -Instances, die in Subnetzen gestartet werden, in denen dieses Attribut aktiviert ist, haben ihrer primären Netzwerkschnittstelle eine öffentliche IP-Adresse zugewiesen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.AC-5	Die Netzwerkintegrität ist geschützt (z. B. Netzwerktrennung, Netzwerksegmentierung)	autoscaling-launch-config-public-ip-deaktiviert	Wenn Sie Ihre Netzwerkschnittstellen mit einer öffentlichen IP-Adresse konfigurieren, sind die diesen Netzwerkschnittstellen zugehörigen Ressourcen über das Internet erreichbar. EC2 Ressourcen sollten nicht öffentlich zugänglich sein, da dies einen unbeabsichtigten Zugriff auf Ihre Anwendungen oder Server ermöglichen kann.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.AC-5	Die Netzwerkintegrität ist geschützt (z. B. Netzwerktrennung, Netzwerksegmentierung)	ec2- instances-in-vpc	Stellen Sie Amazon Elastic Compute Cloud (Amazon EC2) -Instances innerhalb einer Amazon Virtual Private Cloud (Amazon VPC) bereit, um eine sichere Kommunikation zwischen einer Instance und anderen Services innerhalb der Amazon VPC zu ermöglichen, ohne dass ein Internet-Gateway, ein NAT-Gerät oder eine VPN-Verbindung erforderlich ist. Der gesamte Datenverkehr bleibt sicher in der AWS Cloud. Domains, die sich innerhalb einer VPC befinden, verfügen aufgrund ihrer logischen Isolierung im Vergleich zu Domains mit öffentlichen Endpunkten über eine zusätzliche Sicherheitsebene. Weisen Sie EC2

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			Amazon-Instances einer Amazon-VPC zu, um den Zugriff ordnungsgemäß zu verwalten.
PR.AC-5	Die Netzwerkintegrität ist geschützt (z. B. Netzwerktrennung, Netzwerksegmentierung)	no-unrestricted-route-to-igw	Stellen Sie sicher, dass EC2 Amazon-Routentabellen keine uneingeschränkten Routen zu einem Internet-Gateway enthalten. Durch das Entfernen oder Beschränken des Internetzugangs für Workloads innerhalb von Amazon VPCs können unbeabsichtigte Zugriffe in Ihrer Umgebung reduziert werden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.AC-5	Die Netzwerkintegrität ist geschützt (z. B. Netzwerktrennung, Netzwerksegmentierung)	redshift-enhanced-vpc-routing-aktiviert	Mit Enhanced-VPC-Routing wird erzwungen, dass der gesamte COPY- und UNLOAD-Datenverkehr zwischen Ihrem Cluster und Datenrepositorys über Ihre Amazon VPC erfolgt. Anschließend können Sie VPC-Features wie Sicherheitsgruppen und Netzwerkzugriffskontrolllisten verwenden, um den Netzwerkverkehr zu schützen. Sie können auch VPC-Flow-Logs verwenden, um den Netzwerkverkehr zu überwachen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.AC-5	Die Netzwerkintegrität ist geschützt (z. B. Netzwerktrennung, Netzwerksegmentierung)	ssm-document-not-public	Stellen Sie sicher, dass AWS Systems Manager (SSM) - Dokumente nicht öffentlich sind, da dies einen unbeabsichtigten Zugriff auf Ihre SSM-Dokumente ermöglichen kann. Ein öffentliches SSM-Dokument kann Informationen über Ihr Konto, Ihre Ressourcen und internen Prozesse preisgeben.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.AC-5	Die Netzwerkintegrität ist geschützt (z. B. Netzwerktrennung, Netzwerksegmentierung)	acm-certificate-expiration-check	Stellen Sie sicher, dass die Netzwerkintegrität geschützt ist, indem Sie sicherstellen, dass X509-Zertifikate von ACM ausgestellt werden. AWS Diese Zertifikate müssen gültig und dürfen nicht abgelaufen sein. Für diese Regel ist ein Wert für erforderlich daysToExpiration (Wert für bewährte AWS Grundregeln für Sicherheit: 90). Der tatsächliche Wert muss den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.AC-5	Die Netzwerkintegrität ist geschützt (z. B. Netzwerktrennung, Netzwerksegmentierung)	dms-replication-not-public	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass auf DMS-Replikationsinstanzen nicht öffentlich zugegriffen werden kann. DMS-Replikations-Instances können vertrauliche Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.
PR.AC-5	Die Netzwerkintegrität ist geschützt (z. B. Netzwerktrennung, Netzwerksegmentierung)	ebs-snapshot-public-restorable-überprüfen	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass EBS-Snapshots nicht öffentlich wiederherstellbar sind. EBS-Volume-Snapshots können vertrauliche Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.AC-5	Die Netzwerkintegrität ist geschützt (z. B. Netzwerktrennung, Netzwerksegmentierung)	ec2- instance-no-public-ip	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon Elastic Compute Cloud (Amazon EC2) - Instances nicht öffentlich zugänglich sind. EC2Amazon -Instances können vertrauliche Informationen enthalten, und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.AC-5	Die Netzwerkintegrität ist geschützt (z. B. Netzwerktrennung, Netzwerksegmentierung)	elasticsearch-in-vpc-only	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass sich Amazon OpenSearch OpenSearch Service (Service) - Domains innerhalb einer Amazon Virtual Private Cloud (Amazon VPC) befinden. Eine OpenSearch Service-Domain innerhalb einer Amazon VPC ermöglicht die sichere Kommunikation zwischen OpenSearch Service und anderen Services innerhalb der Amazon VPC, ohne dass ein Internet-Gateway, ein NAT-Gerät oder eine VPN-Verbindung erforderlich ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.AC-5	Die Netzwerkintegrität ist geschützt (z. B. Netzwerktrennung, Netzwerksegmentierung)	emr-master-no-public-ip	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon EMR-Cluster-Masterknoten nicht öffentlich zugänglich sind. Amazon-EMR-Cluster-Hauptknoten können vertrauliche Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.AC-5	Die Netzwerkintegrität ist geschützt (z. B. Netzwerktrennung, Netzwerksegmentierung)	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) Security Groups können bei der Verwaltung des Netzwerkzugriffs helfen, indem sie eine statusbehaftete Filterung von eingehendem und ausgehendem Netzwerkverkehr zu Ressourcen bereitstellen. AWS Wenn Sie eingehenden (oder entfernten) Datenverkehr von 0.0.0.0/0 bis Port 22 auf Ihren Ressourcen nicht zulassen, können Sie den Remote-Zugriff einschränken.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.AC-5	Die Netzwerkintegrität ist geschützt (z. B. Netzwerktrennung, Netzwerksegmentierung)	lambda-function-public-access-verboten	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass AWS Lambda-Funktionen nicht öffentlich zugänglich sind. Der öffentliche Zugriff kann möglicherweise die Verfügbarkeit von Ressourcen beeinträchtigen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.AC-5	Die Netzwerkintegrität ist geschützt (z. B. Netzwerktrennung, Netzwerksegmentierung)	lambda-inside-vpc	Stellen Sie AWS Lambda-Funktionen in einer Amazon Virtual Private Cloud (Amazon VPC) bereit, um eine sichere Kommunikation zwischen einer Funktion und anderen Diensten innerhalb der Amazon VPC zu gewährleisten. Bei dieser Konfiguration sind kein Internet-Gateway, kein NAT-Gerät und keine VPN-Verbindung erforderlich. Der gesamte Datenverkehr bleibt sicher in der Cloud. AWS Domains, die sich innerhalb einer VPC befinden, verfügen aufgrund ihrer logischen Isolierung im Vergleich zu Domains mit öffentlichen Endpunkten über eine zusätzliche Sicherheitsebene. Um den Zugriff ordnungsgemäß zu verwalten,

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			sollten AWS Lambda-Funktionen einer VPC zugewiesen werden.
PR.AC-5	Die Netzwerkintegrität ist geschützt (z. B. Netzwerktrennung, Netzwerksegmentierung)	opensearch-in-vpc-only	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass sich Amazon OpenSearch Service-Domains innerhalb einer Amazon Virtual Private Cloud (Amazon VPC) befinden. Eine Amazon OpenSearch Service-Domain innerhalb einer Amazon VPC ermöglicht die sichere Kommunikation zwischen Amazon OpenSearch Service und anderen Services innerhalb der Amazon VPC, ohne dass ein Internet-Gateway, ein NAT-Gerät oder eine VPN-Verbindung erforderlich ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.AC-5	Die Netzwerkintegrität ist geschützt (z. B. Netzwerktrennung, Netzwerksegmentierung)	rds-instance-public-access-überprüfen	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Relational Database Service (Amazon RDS) -Instances nicht öffentlich sind. Amazon-RDS-Datenbank-Instances können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.AC-5	Die Netzwerkintegrität ist geschützt (z. B. Netzwerktrennung, Netzwerksegmentierung)	rds-snapshots-public-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Relational Database Service (Amazon RDS) -Instances nicht öffentlich sind. Amazon-RDS-Datenbank-Instances können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.AC-5	Die Netzwerkintegrität ist geschützt (z. B. Netzwerktrennung, Netzwerksegmentierung)	redshift-cluster-public-access-überprüfen	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Redshift Redshift-Cluster nicht öffentlich sind. Amazon-Redshift-Cluster können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.AC-5	Die Netzwerkintegrität ist geschützt (z. B. Netzwerktrennung, Netzwerksegmentierung)	restricted-common-ports	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass gemeinsame Ports für Amazon Elastic Compute Cloud (Amazon EC2) -Sicherheitsgruppen eingeschränkt sind. Wenn der Zugriff auf Ports nicht auf vertrauenswürdige Quellen beschränkt wird, kann dies zu Angriffen auf die Verfügbarkeit, Integrität und Vertraulichkeit von Systemen führen. Mit dieser Regel können Sie optional die Parameter blockedPort1–blockedPort5 festlegen (Standardkonfigurationen: 20, 21, 3389, 3306, 4333). Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.AC-5	Die Netzwerkintegrität ist geschützt (z. B. Netzwerktrennung, Netzwerksegmentierung)	s3- -Blocke-periodisch account-level-public-access	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Simple Storage Service (Amazon S3) -Buckets nicht öffentlich zugänglich sind. Diese Regel trägt dazu bei, sensible Daten vor unbefugten Remote-Benutzern zu schützen, indem sie den öffentlichen Zugriff verhindert. Mit dieser Regel können Sie optional die Parameter ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) und restrictPublicBuckets Parameter (Config Default: True) festlegen. Die tatsächlichen Werte müssen den Richtlini

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			en Ihrer Organisation entsprechen.
PR.AC-5	Die Netzwerkintegrität ist geschützt (z. B. Netzwerktrennung, Netzwerksegmentierung)	s-3 bucket-public-read-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie nur autorisierten Benutzern, Prozessen und Geräten Zugriff auf Amazon Simple Storage Service (Amazon S3) - Buckets gewähren. Die Verwaltung des Zugriffs sollte mit der Klassifizierung der Daten übereinstimmen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.AC-5	Die Netzwerkintegrität ist geschützt (z. B. Netzwerktrennung, Netzwerksegmentierung)	s-3 bucket-public-write-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie nur autorisierten Benutzern, Prozessen und Geräten Zugriff auf Amazon Simple Storage Service (Amazon S3) - Buckets gewähren. Die Verwaltung des Zugriffs sollte mit der Klassifizierung der Daten übereinstimmen.
PR.AC-5	Die Netzwerkintegrität ist geschützt (z. B. Netzwerktrennung, Netzwerksegmentierung)	sagemaker-notebook-no-direct-Internetzugang	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass SageMaker Amazon-Notebooks keinen direkten Internetzugang zulassen. Indem Sie direkten Internetzugang blockieren, vermeiden Sie, dass unbefugte Benutzer auf sensible Daten zugreifen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.AC-5	Die Netzwerkintegrität ist geschützt (z. B. Netzwerktrennung, Netzwerksegmentierung)	subnet-auto-assign-public-ip-deaktiviert	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon Virtual Private Cloud (VPC) -Subnetzen nicht automatisch eine öffentliche IP-Adresse zugewiesen wird. Amazon Elastic Compute Cloud (EC2) -Instances, die in Subnetzen gestartet werden, in denen dieses Attribut aktiviert ist, haben ihrer primären Netzwerkschnittstelle eine öffentliche IP-Adresse zugewiesen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.AC-5	Die Netzwerkintegrität ist geschützt (z. B. Netzwerktrennung, Netzwerksegmentierung)	vpc-default-security-group-geschlossen	Sicherheitsgruppen von Amazon Elastic Compute Cloud (Amazon EC2) können bei der Verwaltung des Netzwerkzugriffs helfen, indem sie eine statusbehaftete Filterung des ein- und ausgehenden Netzwerkverkehrs zu Ressourcen bereitstellen. AWS Die Beschränkung des gesamten Datenverkehrs auf die Standardsicherheitsgruppe hilft dabei, den Fernzugriff auf Ihre Ressourcen einzuschränken. AWS

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.AC-5	Die Netzwerkintegrität ist geschützt (z. B. Netzwerktrennung, Netzwerksegmentierung)	vpc-sg-open-only-to-authorized-ports	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass gemeinsame Ports für Amazon Elastic Compute Cloud (Amazon EC2) -Sicherheitsgruppen eingeschränkt sind. Wenn der Zugriff auf Ports nicht auf vertrauenswürdige Quellen beschränkt wird, kann dies zu Angriffen auf die Verfügbarkeit, Integrität und Vertraulichkeit von Systemen führen. Durch die Beschränkung des Zugriffs auf Ressourcen innerhalb einer Sicherheitsgruppe aus dem Internet (0.0.0.0/0) kann der Fernzugriff auf interne Systeme gesteuert werden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.AC-6	Identitäten werden geprüft und an Zugangsdaten gebunden und im Rahmen von Interaktionen bestätigt	emr-kerberos-enabled	Die Zugriffsberechtigungen und -autorisierungen können verwaltet und nach den Prinzipien der geringsten Berechtigung und Aufgabentrennung integriert werden, indem Kerberos für Amazon-EMR-Cluster aktiviert wird. In Kerberos werden Services und Benutzer, die sich authentifizieren müssen, als Prinzipale bezeichnet. Prinzipale befinden sich in einem Kerberos-Bereich. Innerhalb dieses Bereichs wird ein Kerberos-Server als Key Distribution Center (KDC) bezeichnet. Über diesen Server können sich Prinzipale authentifizieren. Die Authentifizierung im KDC erfolgt durch die Ausstellung von Authentif

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			izierungstickets. Das KDC unterhält eine Datenbank der Prinzipale in seinem Bereich mit ihren Passwörtern und anderen administr ativen Informationen zu jedem Prinzipal.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.AC-6	Identitäten werden geprüft und an Zugangsdaten gebunden und im Rahmen von Interaktionen bestätigt	iam-password-policy	Die Identitäten und Anmeldeinformationen werden auf der Grundlage einer organisatorischen IAM-Passwortrichtlinie ausgestellt, verwaltet und verifiziert. Sie erfüllen oder übertreffen die Anforderungen von NIST SP 800-63 und dem Standard „Best Practices“ von AWS Foundational Security für die Passwortstärke. Mit dieser Regel können Sie optional RequireUppercaseCharacters (Wert für AWS grundlegende Sicherheitsbewährte Methoden: wahr), RequireLowercaseCharacters (Wert für bewährte Methoden für AWS grundlegende Sicherheit: wahr), RequireSymbols (Wert für bewährte Methoden für AWS grundlegende Sicherheit:

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			wahr), RequireNumbers (Wert für bewährte Methoden für AWS grundlegende Sicherheit: wahr), MinimumPasswordLength (Wert für bewährte Methoden für AWS grundlegende Sicherheit: 14), PasswordReusePrevention (Wert für bewährte Methoden für AWS grundlegende Sicherheit: 24) und MaxPasswordAge (Wert für bewährte Methoden für AWS grundlegende Sicherheit: 90) für Ihr IAM festlegen Kennwortrichtlinie. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.AC-7	Benutzer, Geräte und andere Ressourcen werden entsprechend dem Transaktionsrisiko authentifiziert (z. B. Einzelfaktor- oder Multifaktorrisiko) (z. B. Sicherheits- und Datenschutzrisiken von Einzelpersonen und andere organisatorische Risiken)	iam-password-policy	Die Identitäten und Anmeldeinformationen werden auf der Grundlage einer organisatorischen IAM-Passwortrichtlinie ausgestellt, verwaltet und verifiziert. Sie erfüllen oder übertreffen die Anforderungen von NIST SP 800-63 und dem Standard „Best Practices“ von Foundational Security für die AWS Passwortstärke. Mit dieser Regel können Sie optional RequireUppercaseCharacters (Wert für AWS grundlegende Sicherheitsbewährte Methoden: wahr), RequireLowercaseCharacters (Wert für bewährte Methoden für AWS grundlegende Sicherheit: wahr), RequireSymbols (Wert für bewährte Methoden für AWS grundlegende Sicherheit:

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			wahr), RequireNumbers (Wert für bewährte Methoden für AWS grundlegende Sicherheit: wahr), MinimumPasswordLength (Wert für bewährte Methoden für AWS grundlegende Sicherheit: 14), PasswordReusePrevention (Wert für bewährte Methoden für AWS grundlegende Sicherheit: 24) und MaxPasswordAge (Wert für bewährte Methoden für AWS grundlegende Sicherheit: 90) für Ihr IAM festlegen Kennwortrichtlinie. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.AC-7	Benutzer, Geräte und andere Ressourcen werden entsprechend dem Transaktionsrisiko authentifiziert (z. B. Einzelfaktor- oder Multifaktorrisiko) (z. B. Sicherheits- und Datenschutzrisiken von Einzelpersonen und andere organisatorische Risiken)	iam-user-mfa-enabled	Aktivieren Sie diese Regel, um den Zugriff auf Ressourcen in der AWS -Cloud einzuschränken. Diese Regel stellt sicher, dass die Multi-Faktor-Authentifizierung (MFA) für alle Benutzer aktiviert ist. MFA bietet eine weitere Schutzebene zusätzlich zum Benutzernamen und Passwort. Reduzieren Sie Fälle von kompromittierten Konten, indem Sie MFA für Benutzer vorschreiben.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.AC-7	Benutzer, Geräte und andere Ressourcen werden entsprechend dem Transaktionsrisiko authentifiziert (z. B. Einzelfaktor-, Multifaktorauthentifizierung) (z. B. Sicherheits- und Datenschutzrisiken von Einzelpersonen und andere Unternehmensrisiken)	mfa-enabled-for-iam-Konsolenzugriff	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass MFA für alle AWS Identity and Access Management (IAM) -Benutzer aktiviert ist, die über ein Konsolenkennwort verfügen. MFA sorgt für eine weitere Schutzebene zusätzlich zu den Anmeldeinformationen. Indem Sie MFA für Benutzer vorschreiben, können Sie Fälle kompromittierter Konten reduzieren und verhindern, dass unbefugte Benutzer auf vertrauliche Daten zugreifen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.AC-7	Benutzer, Geräte und andere Ressourcen werden entsprechend dem Transaktionsrisiko authentifiziert (z. B. Einzelfaktor- oder Multifaktorrisiko) (z. B. Sicherheits- und Datenschutzrisiken von Einzelpersonen und andere organisatorische Risiken)	root-account-hardware-mfa-aktiviert	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Hardware-MFA für den Root-Benutzer aktiviert ist. Der Stammbenutzer ist der AWS-Konto-Benutzer mit den meisten Berechtigungen. MFA sorgt für eine weitere Schutzebene zusätzlich zu den Anmeldeinformationen. Indem Sie MFA für den Root-Benutzer vorschreiben, können Sie die Anzahl AWS-Konten kompromittierter Benutzer reduzieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.AC-7	Benutzer, Geräte und andere Ressourcen werden entsprechend dem Transaktionsrisiko authentifiziert (z. B. Einzelfaktor-, Multifaktorauthentifizierung) (z. B. Sicherheits- und Datenschutzrisiken von Einzelpersonen und andere Unternehmensrisiken)	root-account-mfa-enabled	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass MFA für den Root-Benutzer aktiviert ist. Der Stammbenutzer ist der AWS-Konto-Benutzer mit den meisten Berechtigungen. MFA bietet eine weitere Schutzebene zusätzlich zum Benutzernamen und Passwort. Indem Sie MFA für den Root-Benutzer vorschreiben, können Sie die Anzahl AWS-Konten kompromittierter Benutzer reduzieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.AT-1	Alle Nutzer werden informiert und geschult	security-awareness -program-exists (Prozessüberprüfung)	Etablieren und pflegen Sie ein Programm zur Förderung des Sicherheitsbewusst seins in Ihrer Organisation. Programme zur Förderung des Sicherheitsbewusst seins der Mitarbeiter vermitteln ihnen, wie sie die Organisation vor diversen Sicherhei tsverletzungen oder Sicherheitsvorfällen schützen können.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.DS-1	Data-at-rest ist geschützt	ec-2 ebs-encryption-by-default	Zum Schutz von Daten im Ruhezustand müssen Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon Elastic Block Store (Amazon EBS)-Volumes aktiviert ist. Da sensible Daten in diesen Volumes gespeichert werden können, sollten Sie die Verschlüsselung von Daten im Ruhezustand aktivieren, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.DS-1	Data-at-rest ist geschützt	rds-snapshot-encrypted	Stellen Sie sicher, dass die Verschlüsselung für Ihre Amazon Relational Database Service (Amazon RDS)-Snapshots aktiviert ist. Da sensible Daten auch im Ruhezustand vorhanden sein können, sollten Sie die Verschlüsselung von Daten im Ruhezustand aktivieren, um diese Daten zu schützen.
PR.DS-1	Data-at-rest ist geschützt	s-3 default-encryption-kms	Stellen Sie sicher, dass die Verschlüsselung für Ihre Amazon Simple Storage Service (Amazon S3)-Buckets aktiviert ist. Da sensible Daten in einem Amazon S3 Bucket gespeichert werden können, sollten Sie die Verschlüsselung im Ruhezustand aktivieren, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.DS-1	Data-at-rest ist geschützt	sagemaker-notebook-instance-kms-key-konfiguriert	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass die Verschlüsselung mit dem AWS Key Management Service (AWS KMS) für Ihr Notebook aktiviert ist. SageMaker Da vertrauliche Daten im SageMaker Notebook gespeichert werden können, sollten Sie die Verschlüsselung im Ruhezustand aktivieren, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.DS-1	Data-at-rest ist geschützt	sns-encrypted-kms	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass Ihre Amazon Simple Notification Service (Amazon SNS) -Themen mit dem AWS Key Management Service (AWS KMS) verschlüsselt werden müssen. Um eventuell vorhandene sensible Daten im Ruhezustand in veröffentlichten Nachrichten zu schützen, muss die Verschlüsselung von Daten im Ruhezustand aktiviert sein.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.DS-1	Data-at-rest ist geschützt	api-gw-cache-enabled-und-verschlüsselt	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass die Verschlüsselung für den Cache Ihrer API-Gateway-Stufe aktiviert ist. Da für die API-Methode sensible Daten erfasst werden können, sollten Sie die Verschlüsselung von Daten im Ruhezustand aktivieren, um diese Daten zu schützen.
PR.DS-1	Data-at-rest ist geschützt	cloud-trail-encryption-enabled	Zum Schutz von eventuell vorhandenen sensiblen Daten sowie Daten im Ruhezustand müssen Sie sicherstellen, dass die Verschlüsselung für Ihre AWS CloudTrail aktiviert ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.DS-1	Data-at-rest ist geschützt	efs-encrypted-check	Aktivieren Sie die Verschlüsselung für Ihr Amazon Elastic File System (EFS), um eventuell vorhandene sensible Daten sowie Daten im Ruhezustand zu schützen.
PR.DS-1	Data-at-rest ist geschützt	elasticsearch-encrypted-at-rest	Da sensible Daten vorhanden sein können und um Daten im Ruhezustand zu schützen, sollten Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon OpenSearch Service (OpenSearch Service) -Domains aktiviert ist.
PR.DS-1	Data-at-rest ist geschützt	encrypted-volumes	Aktivieren Sie die Verschlüsselung für Ihre Amazon-Elastic-Block-Store-(Amazon-EBS-)Volumes, um eventuell vorhandene sensible Daten sowie Daten im Ruhezustand zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.DS-1	Data-at-rest ist geschützt	kms-cmk-not-scheduled-zum Löschen	Um Daten im Ruhezustand zu schützen, sollten Sie sicherstellen, dass die für den Kunden erforderlichen Masterschlüssel (CMKs) nicht im AWS Key Management Service (AWS KMS) gelöscht werden. Da Schlüssel manchmal gelöscht werden müssen, können Sie mit dieser Regel alle zu löschenden Schlüssel überprüfen, falls ein Schlüssel versehentlich zur Löschung vorgemerkt wurde.
PR.DS-1	Data-at-rest ist geschützt	opensearch-encrypted-at-rest	Da sensible Daten vorhanden sein können und um Daten im Ruhezustand zu schützen, sollten Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon OpenSearch Service-Domains aktiviert ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.DS-1	Data-at-rest ist geschützt	rds-storage-encrypted	Zum Schutz von Daten im Ruhezustand müssen Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon Relational Database Service (Amazon RDS)-Instances aktiviert ist. Da sensible Daten in Amazon-RDS-Instances gespeichert werden können, sollten Sie die Verschlüsselung von Daten im Ruhezustand aktivieren, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.DS-1	Data-at-rest ist geschützt	redshift-cluster-configuration-check	Um Daten im Ruhezustand zu schützen, muss die Verschlüsselung für Ihre Amazon-Redshift-Cluster aktiviert sein. Sie müssen auch sicherstellen, dass die erforderlichen Konfigurationen auf Amazon-Redshift-Clustern bereitgestellt werden. Die Prüfungsprotokollierung muss aktiviert sein, um Informationen zu Verbindungen und Benutzeraktivitäten in der Datenbank bereitzustellen. Diese Regel erfordert, dass ein Wert für clusterDbEncrypted (Config Default: TRUE) und LoggingEnabled (Config Default: TRUE) gesetzt ist. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.DS-1	Data-at-rest ist geschützt	redshift-cluster-kms-enabled	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass die Verschlüs selung mit AWS Key Management Service (AWS KMS) für Ihren Amazon Redshift Redshift-Cluster aktiviert ist. Da sensible Daten in Redshift-Clustern gespeichert werden können, sollten Sie Verschlüsselung von Daten im Ruhezusta nd aktivieren, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.DS-1	Data-at-rest ist geschützt	bucket-server-side-encryptions3-fähig	Zum Schutz von Daten im Ruhezustand müssen Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon Simple Storage Service (Amazon S3)-Buckets aktiviert ist. Da sensible Daten in Amazon S3 Buckets gespeichert werden können, sollten Sie die Verschlüsselung aktivieren, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.DS-1	Data-at-rest ist geschützt	sagemaker-endpoint-configuration-kms-key-konfiguriert	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass die Verschlüsselung mit dem AWS Key Management Service (AWS KMS) für Ihren Endpunkt aktiviert ist. SageMaker Da sensible Daten auf dem SageMaker Endgerät gespeiche rt werden können, sollten Sie die Verschlüsselung im Ruhezustand aktiviere n, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.DS-1	Data-at-rest ist geschützt	secretsmanager-using-cmk	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass die Verschlüsselung mit dem AWS Key Management Service (AWS KMS) für AWS Secrets Manager aktiviert ist. Aktivieren Sie die Verschlüsselung von Daten im Ruhezustand, um eventuell vorhandene sensible Daten im Ruhezustand im Secrets Manager zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.DS-2	Data-in-transit ist geschützt	elasticsearch-node-to-node-Verschlüsselungsprüfung	Stellen Sie sicher, dass die node-to-node Verschlüsselung für Amazon OpenSearch Service aktiviert ist. Node-to-nodeVerschlüsselung ermöglicht die TLS 1.2-Verschlüsselung für die gesamte Kommunikation innerhalb der Amazon Virtual Private Cloud (Amazon VPC). Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.DS-2	Data-in-transit ist geschützt	elbv2- acm-certificate-required	Zum Schutz von eventuell vorhanden en sensiblen Daten sowie von Daten während der Übertragung muss die Verschlüsselung für Ihr Elastic Load Balancing aktiviert sein. Verwenden Sie AWS Certificate Manager, um öffentlic he und private SSL/ TLS-Zertifikate mit AWS Diensten und internen Ressource n zu verwalten, bereitzustellen und bereitzustellen.
PR.DS-2	Data-in-transit ist geschützt	elb-tls-https-listeners-nur	Stellen Sie sicher, dass Ihre Elastic Load Balancer (ELBs) mit SSL- oder HTTPS-Listenern konfiguriert sind. Um eventuell vorhanden e sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.DS-2	Data-in-transit ist geschützt	opensearch-node-to-node-Verschlüsselungsprüfung	Stellen Sie sicher, dass die node-to-node Verschlüsselung für Amazon OpenSearch Service aktiviert ist. Node-to-nodeVerschlüsselung ermöglicht die TLS 1.2-Verschlüsselung für die gesamte Kommunikation innerhalb der Amazon Virtual Private Cloud (Amazon VPC). Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.DS-2	Data-in-transit ist geschützt	alb-http-to-https-Umleitungsprüfung	Um Daten während der Übertragung zu schützen, stellen Sie sicher, dass Ihr Application Load Balancer unverschlüsselte HTTP-Anfragen automatisch an HTTPS umleitet. Da sensible Daten vorhanden sein können, sollten Sie die Verschlüsselung bei der Übertragung aktivieren, um diese Daten zu schützen.
PR.DS-2	Data-in-transit ist geschützt	api-gw-ssl-enabled	Stellen Sie sicher, dass die REST-API-Stufen von Amazon API Gateway mit SSL-Zertifikaten konfiguriert sind, damit Backend-Systeme überprüfen können, ob Anforderungen von API Gateway stammen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.DS-2	Data-in-transit ist geschützt	elb-acm-certificate-required	Zum Schutz von eventuell vorhanden en sensiblen Daten sowie von Daten während der Übertragung muss die Verschlüsselung für Ihr Elastic Load Balancing aktiviert sein. Verwenden Sie AWS Certificate Manager, um öffentlic he und private SSL/ TLS-Zertifikate mit AWS Diensten und internen Ressource n zu verwalten, bereitzustellen und bereitzustellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.DS-2	Data-in-transit ist geschützt	redshift-require-tls-ssl	Stellen Sie sicher, dass Ihre Amazon-Redshift-Cluster eine TLS/SSL-Verschlüsselung erfordern, um eine Verbindung zu SQL-Clients herzustellen. Da sensible Daten vorhanden sein können, sollten Sie die Verschlüsselung bei der Übertragung aktivieren, um diese Daten zu schützen.
PR.DS-2	Data-in-transit ist geschützt	s-3 bucket-ssl-requests-only	Um Daten während der Übertragung zu schützen, stellen Sie sicher, dass Ihre Amazon Simple Storage Service (Amazon S3)-Buckets Anfragen zur Verwendung von Secure Socket Layer (SSL)-Buckets erfordern. Da sensible Daten vorhanden sein können, sollten Sie die Verschlüsselung bei der Übertragung aktivieren, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.DS-3	Vermögenswerte werden während des Umzugs, der Übertragung und der Veräußerung formal verwaltet	ec2-manager instance-managed-by-systems	Eine Bestandsaufnahme der Softwareplattformen und Anwendungen innerhalb des Unternehmens ist möglich, indem Amazon Elastic Compute Cloud (Amazon EC2) - Instances mit AWS Systems Manager verwaltet werden. Verwenden Sie AWS Systems Manager, um detaillierte Systemkonfigurationen, Betriebssystem-Patch-Levels, Namen und Typ der Dienste, Softwareinstallationen, Anwendungsname, Herausgeber und Version sowie andere Details zu Ihrer Umgebung bereitzustellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.DS-3	Vermögenswerte werden während des Umzugs, der Übertragung und der Veräußerung formal verwaltet	ec2-check managedinstance-association-compliance-status	Verwenden Sie AWS Systems Manager Associations, um bei der Inventarisierung von Softwareplattformen und Anwendungen innerhalb eines Unternehmens zu helfen. AWS Systems Manager weist Ihren verwalteten Instances einen Konfigurationsstatus zu und ermöglicht es Ihnen, Basiswerte für Betriebssystem-Patch-Levels, Softwareinstallationen, Anwendungskonfigurationen und andere Details zu Ihrer Umgebung festzulegen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.DS-3	Vermögenswerte werden während des Umzugs, der Übertragung und der Veräußerung formal verwaltet	eip-attached	Diese Regel stellt sicher, dass Elastic, die einer Amazon Virtual Private Cloud (Amazon VPC) IPs zugewiesen sind, an Amazon Elastic Compute Cloud (Amazon EC2) - Instances oder verwendete Elastic Network Interface s angehängt sind. Diese Regel hilft bei der Überwachu ng ungenutzter Inhalte EIPs in Ihrer Umgebung.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.DS-4	Ausreichende Kapazität zur Sicherstellung der Verfügbarkeit	dynamodb-in-backup-plan	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon DynamoDB-Tabellen Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.DS-4	Ausreichende Kapazität zur Sicherstellung der Verfügbarkeit	ebs-in-backup-plan	Stellen Sie zur Unterstützung der Datensicherungspro zesse sicher, dass Ihre Amazon Elastic Block Store (Amazon EBS) -Volumes Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwaltet er Backup-Service mit einer richtlini enbasierten Backup-Lösung. Diese Lösung vereinfacht Ihre Backup-Verwaltung und ermöglicht es Ihnen, Ihre geschäftl ichen und behördlic hen Anforderungen bezüglich Backups zu erfüllen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.DS-4	Ausreichende Kapazität zur Sicherstellung der Verfügbarkeit	efs-in-backup-plan	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon Elastic File System (Amazon EFS) -Dateisysteme Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.DS-4	Ausreichende Kapazität zur Sicherstellung der Verfügbarkeit	elb-cross-zone-load-Balancing aktiviert	Aktivieren Sie zonenübergreifendes Load Balancing für Ihre Elastic Load Balancer (ELBs), um eine angemessene Kapazität und Verfügbarkeit aufrechtzuerhalten. Zonenübergreifendes Load Balancing reduziert die Notwendigkeit, die gleiche Anzahl von Instances in jeder aktivierten Availability Zone aufrechtzuerhalten. Es verbessert auch die Fähigkeit Ihrer Anwendung, den Verlust einer oder mehrerer Instances zu bewältigen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.DS-4	Ausreichende Kapazität zur Sicherstellung der Verfügbarkeit	rds-instance-deletion-protection-aktiviert	Stellen Sie sicher, dass Amazon Relational Database Service (Amazon RDS)-Instances den Löschschutz aktiviert haben. Verwenden Sie den Löschschutz, um zu verhindern, dass Ihre Amazon-RDS-Instances versehentlich oder böswillig gelöscht werden, was zum Verlust der Verfügbarkeit Ihrer Anwendungen führen kann.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.DS-4	Ausreichende Kapazität zur Sicherstellung der Verfügbarkeit	rds-in-backup-plan	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon Relational Database Service (Amazon RDS) -Instances Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.DS-4	Ausreichende Kapazität zur Sicherstellung der Verfügbarkeit	redshift-backup-enabled	Stellen Sie zur Unterstützung der Datensicherungsprozesse sicher, dass Ihre Amazon-Redshift-Cluster über automatisierte Snapshots verfügen. Wenn automatisierte Snapshots für einen Cluster aktiviert sind, erstellt Redshift in regelmäßigen Abständen Snapshots dieses Clusters. Standardmäßig erstellt Redshift alle acht Stunden oder alle 5 GB einen Snapshot für jeden Knoten mit Datenänderungen oder je nachdem, was zuerst eintritt.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.DS-4	Ausreichende Kapazität zur Sicherstellung der Verfügbarkeit	db-instance-backup-enabled	Die Sicherung sfunktion von Amazon RDS erstellt Sicherung en Ihrer Datenbank en und Transakti onsprotokolle. Amazon RDS erstellt einen Snapshot für das Speichervolume Ihrer DB-Instance, sodass die gesamte DB-Instance gesichert wird. Sie können im System spezifische Aufbewahrungsfrist en festlegen, um Ihre Ausfallsicherheits anforderungen zu erfüllen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.DS-4	Ausreichende Kapazität zur Sicherstellung der Verfügbarkeit	dynamodb-autoscaling-enabled	Amazon DynamoDB Auto Scaling verwendet den AWS Application Auto Scaling-Service, um die bereitgestellte Durchsatzkapazität so anzupassen, dass sie automatisch auf tatsächliche Verkehrsmuster reagiert. Auf diese Weise kann eine Tabelle oder ein globaler sekundärer Index die bereitgestellte Lese-/Schreibkapazität erhöhen, um plötzliche Erhöhungen des Datenverkehrs ohne Drosselung zu bewältigen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.DS-4	Ausreichende Kapazität zur Sicherstellung der Verfügbarkeit	dynamodb-pitr-enabled	Aktivieren Sie diese Regel, um zu überprüfen, ob die Informationen gesichert wurden. Es verwaltet auch die Backups, indem es sicherstellt, dass die point-in-time Wiederherstellung in Amazon DynamoDB aktiviert ist. Bei der Wiederherstellung werden fortlaufende Backups Ihrer Tabelle für die letzten 35 Tage gespeichert.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.DS-4	Ausreichende Kapazität zur Sicherstellung der Verfügbarkeit	elasticache-redis-cluster-automatic-Backup-Prüfung	Wenn automatische Backups aktiviert sind, ElastiCache erstellt Amazon täglich ein Backup des Clusters. Die Sicherung kann für eine von Ihrer Organisation festgelegte Anzahl von Tagen aufbewahrt werden. Automatische Backups schützen vor Datenverlust. Bei einem Ausfall können Sie einen neuen Cluster erstellen, der Ihre Daten aus dem aktuellen Backup wiederherstellt.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.DS-4	Ausreichende Kapazität zur Sicherstellung der Verfügbarkeit	elb-deletion-protection-enabled	Diese Regel sorgt dafür, dass der Löschschutz für Elastic Load Balancing aktiviert ist. Verwenden Sie diese Funktion, um zu verhindern, dass Ihr Load Balancer versehentlich oder böswillig gelöscht wird, was zum Verlust der Verfügbarkeit Ihrer Anwendungen führen kann.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.DS-4	Ausreichende Kapazität zur Sicherstellung der Verfügbarkeit	rds-multi-az-support	Die Multi-AZ-Unterstützung in Amazon Relational Database Service (Amazon RDS) bietet eine verbesserte Verfügbarkeit und Beständigkeit von Datenbank-Instances. Wenn Sie eine Multi-AZ-Datenbank-Instance bereitstellen, erstellt Amazon RDS automatisch eine primäre Datenbank-Instance und repliziert die Daten synchron auf eine Standby-Instance in einer anderen Availability Zone. Jede Availability Zone läuft auf einer eigenen, physisch getrennten, unabhängigen Infrastruktur und ist auf eine hohe Verfügbarkeit ausgelegt. Im Falle eines Infrastrukturausfalls führt Amazon RDS einen automatis

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			chen Failover zum Standby-Modus durch, sodass Sie den Datenbankbetrieb wieder aufnehmen können, sobald der Failover abgeschlo ssen ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.DS-4	Ausreichende Kapazität zur Sicherstellung der Verfügbarkeit	redshift-cluster-maintenancesettings-check	Diese Regel stellt sicher, dass Amazon-Redshift-Cluster die bevorzugten Einstellungen für Ihre Organisation haben. Insbesondere sorgt sie dafür, dass Cluster bevorzugte Wartungsfenster und automatisierte Aufbewahrungsfristen für Snapshots für die Datenbank haben. Für diese Regel müssen Sie die festlegen allowVersionUpgrade. Der Standardwert ist „true“. Außerdem können Sie optional den Zeitraum preferredMaintenanceWindow (der Standardwert ist sa: 16:00 -sa: 16:30) und den automated SnapshotRetention Zeitraum (der Standardwert ist 1) festlegen. Die tatsächlichen Werte müssen den Richtlini

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			en Ihrer Organisation entsprechen.
PR.DS-4	Ausreichende Kapazität zur Sicherstellung der Verfügbarkeit	s3- bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) unterstützt die Aufrechterhaltung einer angemesse nen Kapazität und Verfügbarkeit. CRR ermöglicht das automatische, asynchrone Kopieren von Objekten in Amazon S3 Buckets, um die Datenverf ügbarkeit sicherzus tellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.DS-4	Ausreichende Kapazität zur Sicherstellung der Verfügbarkeit	s-3 bucket-versioning-enabled	Die Versionsv erwaltung von Amazon Simple Storage Service (Amazon S3)-Bucke ts hilft dabei, mehrere Varianten eines Objekts im selben Amazon-S3-Bucket zu speichern. Verwenden Sie die Versionsv erwaltung, um sämtliche Versionen aller Objekte in Ihrem Amazon-S3-Bucket zu speichern , abzurufen oder wiederherzustellen . Mit der Versionsv erwaltung können Sie Versionen sowohl nach unbeabsic htigten Benutzera ktionen als auch nach Anwendungsfehlern problemlos wiederher stellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.DS-4	Ausreichende Kapazität zur Sicherstellung der Verfügbarkeit	vpc-vpn-2-tunnels-up	Redundante Site-to-Site VPN-Tunnel können implementiert werden, um die Anforderungen an die Ausfallsicherheit zu erfüllen. Es verwendet zwei Tunnel, um die Konnektivität sicherzustellen, falls eine der Site-to-Site VPN-Verbindungen nicht verfügbar ist. Um sich vor einem Verbindungsverlust zu schützen, können Sie für den Fall, dass Ihr Kunden-Gateway nicht verfügbar ist, eine zweite Site-to-Site VPN-Verbindung zu Ihrer Amazon Virtual Private Cloud (Amazon VPC) und Ihrem Virtual Private Gateway einrichten, indem Sie ein zweites Kunden-Gateway verwenden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.DS-5	Schutzmaßnahmen gegen Datenlecks sind implementiert	autoscaling-launch-config-public-ip-deaktiviert	Wenn Sie Ihre Netzwerkschnittstellen mit einer öffentlichen IP-Adresse konfigurieren, sind die diesen Netzwerkschnittstellen zugehörigen Ressourcen über das Internet erreichbar. EC2 Ressourcen sollten nicht öffentlich zugänglich sein, da dies einen unbeabsichtigten Zugriff auf Ihre Anwendungen oder Server ermöglichen kann.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.DS-5	Schutzmaßnahmen gegen Datenlecks sind implementiert	multi-region-cloudtrail-enabled	AWS CloudTrail zeichnet Aktionen und API-Aufrufe der AWS Management Console auf. Sie können feststellen, welche Benutzer und Konten angerufen wurden AWS, von welcher Quell-IP-Adresse aus die Anrufe getätigt wurden und wann die Anrufe erfolgten. CloudTrail übermittelt Protokolldateien aus allen AWS Regionen an Ihren S3-Bucket , wenn MULTI_REG ION_CLOUD _TRAIL_ENABLED aktiviert ist. Außerdem wird beim AWS Start einer neuen Region derselbe Trail in der neuen Region erstellt. CloudTrail Dadurch erhalten Sie automatis ch Protokolldateien mit API-Aktivitäten für die neue Region.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.DS-5	Schutzmaßnahmen gegen Datenlecks sind implementiert	securityhub-enabled	AWS Security Hub hilft bei der Überwachung von unbefugtem Personal, Verbindungen, Geräten und Software. AWS Security Hub aggregiert, organisiert und priorisiert die Sicherheitswarnungen oder Ergebnisse mehrerer Dienste. AWS Einige dieser Dienste sind Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer und AWS Firewall Manager sowie AWS Partnerlösungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.DS-5	Schutzmaßnahmen gegen Datenlecks sind implementiert	ssm-document-not-public	Stellen Sie sicher, dass AWS Systems Manager (SSM) - Dokumente nicht öffentlich sind, da dies einen unbeabsichtigten Zugriff auf Ihre SSM-Dokumente ermöglichen kann. Ein öffentliches SSM-Dokument kann Informationen über Ihr Konto, Ihre Ressourcen und internen Prozesse preisgeben.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.DS-5	Schutzmaßnahmen gegen Datenlecks sind implementiert	cloudtrail-enabled	AWS CloudTrai l kann durch die Aufzeichnung AWS von Aktionen und API-Aufrufen in der Management Console helfen, die Ablehnung zu verhindern. Sie können die Benutzer und die Benutzer AWS-Konten , die einen AWS Dienst aufgerufen haben, die Quell-IP-Adresse, über die die Aufrufe generiert wurden, und den Zeitpunkt der Anrufe identifiz ieren. Einzelheiten zu den erfassten Daten finden Sie in den AWS CloudTrail Datensatzinhalten.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.DS-5	Schutzmaßnahmen gegen Datenlecks sind implementiert	cloudtrail-s3-data events-enabled	Die Erfassung von Simple Storage Service (Amazon S3)-Datenereignissen unterstützt die Erkennung von ungewöhnlichen Aktivitäten. Zu den Details gehören Informationen zu dem AWS -Konto, das auf einen Amazon-S3-Bucket zugegriffen hat, die IP-Adresse und die Uhrzeit des Ereignisses.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.DS-5	Schutzmaßnahmen gegen Datenlecks sind implementiert	codebuild-project-envvar-awscred-überprüfen	Stellen Sie sicher, dass die Anmeldeinformationen AWS_ACCESS_KEY_ID AWS_SECRET_ACCESS_KEY nicht in AWS Codebuild-Projektumgebungen vorhanden sind. Speichern Sie diese Variablen nicht als Klartext. Das Speichern dieser Variablen als Klartext bewirkt eine unbeabsichtigte Offenlegung von Daten sowie unberechtigte Zugriffe.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.DS-5	Schutzmaßnahmen gegen Datenlecks sind implementiert	codebuild-project-source-repo-URL-Prüfung	Stellen Sie sicher, dass die URL des Quell-Repositorys GitHub oder des Bitbucket-Quell-Repositorys keine persönlichen Zugriffstoken oder Anmeldeinformationen in Codebuild-Projektumgebungen enthält. AWS Verwende OAuth anstelle von persönlichen Zugriffstoken oder Anmeldedaten die Autorisierung für den Zugriff auf GitHub Bitbucket-Repositorys.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.DS-5	Schutzmaßnahmen gegen Datenlecks sind implementiert	dms-replication-not-public	Verwalte den Zugriff auf die AWS Cloud, indem du sicherstellst, dass auf DMS-Replikationsinstanzen nicht öffentlich zugegriffen werden kann. DMS-Replikations-Instances können vertrauliche Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.
PR.DS-5	Schutzmaßnahmen gegen Datenlecks sind implementiert	ebs-snapshot-public-restorable-überprüfen	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass EBS-Snapshots nicht öffentlich wiederherstellbar sind. EBS-Volume-Snapshots können vertrauliche Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.DS-5	Schutzmaßnahmen gegen Datenlecks sind implementiert	elasticsearch-in-vpc-only	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass sich Amazon OpenSearch OpenSearch Service (Service) - Domains innerhalb einer Amazon Virtual Private Cloud (Amazon VPC) befinden. Eine OpenSearch Service-Domain innerhalb einer Amazon VPC ermöglicht die sichere Kommunikation zwischen OpenSearch Service und anderen Services innerhalb der Amazon VPC, ohne dass ein Internet-Gateway, ein NAT-Gerät oder eine VPN-Verbindung erforderlich ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.DS-5	Schutzmaßnahmen gegen Datenlecks sind implementiert	guardduty-enabled-centralized	Amazon GuardDuty kann mithilfe von Threat Intellige nce Feeds helfen, potenzielle Cybersich erheitsereignisse zu überwachen und zu erkennen. Dazu gehören Listen mit bösartigen IPs und maschinel len Lernmethoden zur Identifizierung unerwarteter, nicht autorisierter und bösartiger Aktivitäten in Ihrer AWS Cloud-Umgebung.
PR.DS-5	Schutzmaßnahmen gegen Datenlecks sind implementiert	lambda-function-public-access-verboten	Verwalten Sie den Zugriff auf Ressource n in der AWS Cloud, indem Sie sicherste llen, dass AWS Lambda-Funktionen nicht öffentlich zugänglich sind. Der öffentliche Zugriff kann möglicherweise die Verfügbarkeit von Ressourcen beeinträc htigen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.DS-5	Schutzmaßnahmen gegen Datenlecks sind implementiert	opensearch-in-vpc-only	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass sich Amazon OpenSearch Service-Domains innerhalb einer Amazon Virtual Private Cloud (Amazon VPC) befinden. Eine Amazon OpenSearch Service-Domain innerhalb einer Amazon VPC ermöglicht die sichere Kommunikation zwischen Amazon OpenSearch Service und anderen Services innerhalb der Amazon VPC, ohne dass ein Internet-Gateway, ein NAT-Gerät oder eine VPN-Verbindung erforderlich ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.DS-5	Schutzmaßnahmen gegen Datenlecks sind implementiert	rds-instance-public-access-überprüfen	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Relational Database Service (Amazon RDS) -Instances nicht öffentlich sind. Amazon-RDS-Datenbank-Instances können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.DS-5	Schutzmaßnahmen gegen Datenlecks sind implementiert	rds-snapshots-public-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Relational Database Service (Amazon RDS) -Instances nicht öffentlich sind. Amazon-RDS-Datenbank-Instances können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.DS-5	Schutzmaßnahmen gegen Datenlecks sind implementiert	redshift-cluster-public-access-überprüfen	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Redshift Redshift-Cluster nicht öffentlich sind. Amazon-Redshift-Cluster können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.DS-5	Schutzmaßnahmen gegen Datenlecks sind implementiert	s3- -Block-periodisch account-level-public-access	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Simple Storage Service (Amazon S3) -Buckets nicht öffentlich zugänglich sind. Diese Regel trägt dazu bei, sensible Daten vor unbefugten Remote-Benutzern zu schützen, indem sie den öffentlichen Zugriff verhindert. Mit dieser Regel können Sie optional die Parameter ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) und restrictPublicBuckets Parameter (Config Default: True) festlegen. Die tatsächlichen Werte müssen den Richtlini

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			en Ihrer Organisation entsprechen.
PR.DS-5	Schutzmaßnahmen gegen Datenlecks sind implementiert	s3- bucket-logging-enabled	Die Amazon Simple Storage Service (Amazon S3)-Serverzugriffs protokollierung bietet eine Methode zur Überwachu ng des Netzwerks im Hinblick auf potenzielle Cybersich erheitsereignisse. Die Ereignisse werden überwacht, indem detaillierte Aufzeichn ungen über die Anfragen erfasst werden, die an einen Amazon-S3-Bucket gestellt wurden. Jeder Zugriffsprotokolle intrag enthält Details zu einer einzelnen Zugriffsanfrage. Zu den Details gehören Anforderer, Bucket-Name, Anforderu ngszeit, Anforderu ngsaktion, Antwortst atus und Fehlercode, falls relevant.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.DS-5	Schutzmaßnahmen gegen Datenlecks sind implementiert	s-3 bucket-public-read -prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie nur autorisierten Benutzern, Prozessen und Geräten Zugriff auf Amazon Simple Storage Service (Amazon S3) - Buckets gewähren. Die Verwaltung des Zugriffs sollte mit der Klassifizierung der Daten übereinst immen.
PR.DS-5	Schutzmaßnahmen gegen Datenlecks sind implementiert	s3- bucket-public-writ e-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie nur autorisierten Benutzern, Prozessen und Geräten Zugriff auf Amazon Simple Storage Service (Amazon S3) - Buckets gewähren. Die Verwaltung des Zugriffs sollte mit der Klassifizierung der Daten übereinst immen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.DS-5	Schutzmaßnahmen gegen Datenlecks sind implementiert	sagemaker-notebook-no-direct-Internetzugang	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass SageMaker Amazon-Notebooks keinen direkten Internetzugang zulassen. Indem Sie direkten Internetzugang blockieren, vermeiden Sie, dass unbefugte Benutzer auf sensible Daten zugreifen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.DS-5	Schutzmaßnahmen gegen Datenlecks sind implementiert	vpc-flow-logs-enabled	VPC-Flow-Protokolle erfassen detaillierte Informationsdatensätze über den IP-Datenverkehr, der zu und von Netzwerkschnittstellen in Ihrer Amazon Virtual Private Cloud (Amazon VPC) fließt. Standardmäßig enthalten Flow-Protokolldatensätze Werte für die verschiedenen Komponenten des IP-Flows, einschließlich Quelle, Ziel und Protokoll.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.DS-6	Mechanismen zur Integritätsprüfung werden verwendet, um die Integrität von Software, Firmware und Informationen zu überprüfen	cloud-trail-log-file-Validierung aktiviert	Verwenden Sie die AWS CloudTrail Protokolldateivalidierung, um die Integrität von Protokollen zu überprüfen. CloudTrail Mithilfe der Protokolldateivalidierung kann festgestellt werden, ob eine Protokolldatei geändert oder gelöscht wurde oder ob sie nach der Übermittlung CloudTrail unverändert geblieben ist. Dieses Feature wurde mit dem Branchenstandard entsprechenden Algorithmen entwickelt: SHA-256 für die Hashfunktion und SHA-256 mit RSA für digitale Signaturen. Das macht es rechnerisch unmöglich, CloudTrail Protokolldateien unbemerkt zu ändern, zu löschen oder zu fälschen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.DS-6	Mechanismen zur Integritätsprüfung werden verwendet, um die Integrität von Software, Firmware und Informationen zu überprüfen	s-3 bucket-versioning-enabled	Die Versionsv erwaltung von Amazon Simple Storage Service (Amazon S3)-Bucke ts hilft dabei, mehrere Varianten eines Objekts im selben Amazon-S3-Bucket zu speichern. Verwenden Sie die Versionsv erwaltung, um sämtliche Versionen aller Objekte in Ihrem Amazon-S3-Bucket zu speichern , abzurufen oder wiederherzustellen . Mit der Versionsv erwaltung können Sie Versionen sowohl nach unbeabsic htigten Benutzera ktionen als auch nach Anwendungsfehlern problemlos wiederher stellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.DS-7	Die Entwicklungs- und Testumgebung(en) sind von der Produktionsumgebung getrennt	ec2-manager instance-managed-by-systems	Eine Bestandsaufnahme der Softwareplattformen und Anwendungen innerhalb des Unternehmens ist möglich, indem Amazon Elastic Compute Cloud (Amazon EC2) - Instances mit AWS Systems Manager verwaltet werden. Verwenden Sie AWS Systems Manager, um detaillierte Systemkonfigurationen, Betriebssystem-Patch-Levels, Namen und Typ der Dienste, Softwareinstallationen, Anwendungsname, Herausgeber und Version sowie andere Details zu Ihrer Umgebung bereitzustellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.DS-7	Die Entwicklungs- und Testumgebung(en) sind von der Produktionsumgebung getrennt	ec2-check managedinstance-association-compliance-status	Verwenden Sie AWS Systems Manager Associations, um bei der Inventarisierung von Softwareplattformen und Anwendungen innerhalb eines Unternehmens zu helfen. AWS Systems Manager weist Ihren verwalteten Instances einen Konfigurationsstatus zu und ermöglicht es Ihnen, Basiswerte für Betriebssystem-Patch-Levels, Softwareinstallationen, Anwendungskonfigurationen und andere Details zu Ihrer Umgebung festzulegen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.DS-7	Die Entwicklungs- und Testumgebung(en) sind von der Produktionsumgebung getrennt	ec2-stopped-instance	Aktivieren Sie diese Regel, um bei der Basiskonfiguration von Amazon Elastic Compute Cloud (Amazon EC2) - Instances zu helfen, indem Sie überprüfen, ob EC2 Amazon-Instances gemäß den Standards Ihrer Organisation für mehr als die zulässige Anzahl von Tagen gestoppt wurden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.DS-7	Die Entwicklungs- und Testumgebung(en) sind von der Produktionsumgebung getrennt	ec2- volume-inuse-check	Diese Regel stellt sicher, dass Amazon Elastic Block Store-Volumes, die an Amazon Elastic Compute Cloud (Amazon EC2) - Instances angehängt sind, zum Löschen markiert werden, wenn eine Instance beendet wird. Wenn ein Amazon-EBS-Volume nicht gelöscht wird, wenn die Instance, an die es angehängt ist, beendet wird, kann dies gegen das Konzept der geringsten Funktionalität verstoßen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.DS-7	Die Entwicklungs- und Testumgebung(en) sind von der Produktionsumgebung getrennt	elb-deletion-protection-enabled	Diese Regel sorgt dafür, dass der Löschschutz für Elastic Load Balancing aktiviert ist. Verwenden Sie diese Funktion, um zu verhindern, dass Ihr Load Balancer versehentlich oder böswillig gelöscht wird, was zum Verlust der Verfügbarkeit Ihrer Anwendungen führen kann.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.DS-7	Die Entwicklungs- und Testumgebung(en) sind von der Produktionsumgebung getrennt	restricted-common-ports	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass gemeinsame Ports für Amazon Elastic Compute Cloud (Amazon EC2) -Sicherheitsgruppen eingeschränkt sind. Wenn der Zugriff auf Ports nicht auf vertrauenswürdige Quellen beschränkt wird, kann dies zu Angriffen auf die Verfügbarkeit, Integrität und Vertraulichkeit von Systemen führen. Mit dieser Regel können Sie optional die Parameter blockedPort1–blockedPort5 festlegen (Standardkonfigurationen: 20, 21, 3389, 3306, 4333). Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.IP-1	Es wird eine Basiskonfiguration von Informationstechnologie-/industriellen Steuerungssystemen erstellt und verwaltet, die Sicherheitsprinzipien (z. B. das Konzept der geringsten Funktionalität) berücksichtigt	account-part-of-organizations	Durch die zentrale Verwaltung AWS-Konten innerhalb von AWS Organizations wird sichergestellt, dass die Konten den Vorschriften entsprechen. Eine fehlende zentrale Kontoverwaltung kann zu inkonsistenten Kontokonfigurationen führen, wodurch Ressourcen und sensible Daten offengelegt werden können.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.IP-1	Es wird eine Basiskonfiguration von Informati onstechnologie-/in dustriellen Steuerung ssystemen erstellt und verwaltet, die Sicherheitsprinzipien (z. B. das Konzept der geringsten Funktiona lität) berücksichtigt	ec2-manager instance-managed-by-systems	Eine Bestandsa ufnahme der Softwareplattforme n und Anwendung en innerhalb des Unternehmens ist möglich, indem Amazon Elastic Compute Cloud (Amazon EC2) - Instances mit AWS Systems Manager verwaltet werden. Verwenden Sie AWS Systems Manager, um detaillierte Systemkonfiguratio nen, Betriebssystem-Patch-Levels, Namen und Typ der Dienste, Softwareinstallati onen, Anwendung sname, Herausgeb er und Version sowie andere Details zu Ihrer Umgebung bereitzustellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.IP-1	Es wird eine Basiskonfiguration für Informationstechnologie/industrielle Steuerungssysteme erstellt und verwaltet, die Sicherheitsprinzipien (z. B. das Konzept der geringsten Funktionalität) berücksichtigt	ec2-check managedinstance-association-compliance-status	Verwenden Sie AWS Systems Manager Associations, um bei der Inventarisierung von Softwareplattformen und Anwendungen innerhalb eines Unternehmens zu helfen. AWS Systems Manager weist Ihren verwalteten Instances einen Konfigurationsstatus zu und ermöglicht es Ihnen, Basiswerte für Betriebssystem-Patch-Levels, Softwareinstallationen, Anwendungskonfigurationen und andere Details zu Ihrer Umgebung festzulegen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.IP-1	Es wird eine Basiskonfiguration von Informati onstechnologie-/in dustriellen Steuerung ssystemen erstellt und verwaltet, die Sicherheitsprinzip ien berücksichtigt (z. B. das Konzept der geringsten Funktiona lität)	ec2-stopped-instance	Aktivieren Sie diese Regel, um bei der Basiskonfiguration von Amazon Elastic Compute Cloud (Amazon EC2) - Instances zu helfen, indem Sie überprüfe n, ob EC2 Amazon-Instances gemäß den Standards Ihrer Organisation für mehr als die zulässige Anzahl von Tagen gestoppt wurden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.IP-1	Es wird eine Basiskonfiguration von Informati onstechnologie-/in dustriellen Kontrolls ystemen erstellt und verwaltet, die Sicherheitsprinzipien (z. B. das Konzept der geringsten Funktiona lität) berücksichtigt	ec2- volume-inuse-check	Diese Regel stellt sicher, dass Amazon Elastic Block Store-Volumes, die an Amazon Elastic Compute Cloud (Amazon EC2) - Instances angehängt sind, zum Löschen markiert werden, wenn eine Instance beendet wird. Wenn ein Amazon-EB S-Volume nicht gelöscht wird, wenn die Instance, an die es angehängt ist, beendet wird, kann dies gegen das Konzept der geringsten Funktiona lität verstoßen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.IP-1	Es wird eine Basiskonfiguration von Informati onstechnologie-/in dustriellen Kontrolls ystemen erstellt und verwaltet, die Sicherheitsprinzipien (z. B. das Konzept der geringsten Funktiona lität) berücksichtigt	redshift-cluster-m aintenancesettings-check	Diese Regel stellt sicher, dass Amazon-Redshift-Cluster die bevorzugten Einstellungen für Ihre Organisation haben. Insbesondere sorgt sie dafür, dass Cluster bevorzugt e Wartungsfenster und automatisierte Aufbewahrungsfristen für Snapshots für die Datenbank haben. Für diese Regel müssen Sie die festlegen. allowVersionUpgrad e Der Standardwert ist „true“. Außerdem können Sie optional den Zeitraum preferredMaintenan ceWindow (der Standardwert ist sa: 16:00 -sa: 16:30) und den automated SnapshotRetention Zeitraum (der Standardwert ist 1) festlegen. Die tatsächlichen Werte müssen den Richtlini

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			en Ihrer Organisation entsprechen.
PR.IP-2	Ein Systement wicklungszyklus zur Verwaltung von Systemen ist implementiert	codebuild-project-envvar-awscred-überprüfen	Stellen Sie sicher, dass die Anmeldeinformationen AWS_ACCESS_KEY_ID AWS_SECRET_ACCESS_KEY nicht in AWS Codebuild-Projektumgebungen vorhanden sind. Speichern Sie diese Variablen nicht als Klartext. Das Speichern dieser Variablen als Klartext bewirkt eine unbeabsichtigte Offenlegung von Daten sowie unberechtigte Zugriffe.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.IP-2	Ein Systement wicklungszyklus zur Verwaltung von Systemen ist implementiert	codebuild-project-source-repo-URL-Prüfung	Stellen Sie sicher, dass die URL des Quell-Repositorys GitHub oder des Bitbucket-Quell-Repositorys keine persönlichen Zugriffstoken oder Anmeldeinformationen in Codebuild-Projektumgebungen enthält. AWS Verwende OAuth anstelle von persönlichen Zugriffstoken oder Anmeldedaten die Autorisierung für den Zugriff auf GitHub Bitbucket-Repositorys.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.IP-2	Ein Systement wicklungszyklus zur Verwaltung von Systemen ist implementiert	ec2-manager instance-managed-by-systems	Eine Bestandsa ufnahme der Softwareplattforme n und Anwendung en innerhalb des Unternehmens ist möglich, indem Amazon Elastic Compute Cloud (Amazon EC2) - Instances mit AWS Systems Manager verwaltet werden. Verwenden Sie AWS Systems Manager, um detaillierte Systemkonfiguratio nen, Betriebssystem-Patch-Levels, Namen und Typ der Dienste, Softwareinstallati onen, Anwendung sname, Herausgeb er und Version sowie andere Details zu Ihrer Umgebung bereitzustellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.IP-3	Prozesse zur Steuerung von Konfigurationsänderungen sind vorhanden	elb-deletion-protection-enabled	Diese Regel sorgt dafür, dass der Löschschutz für Elastic Load Balancing aktiviert ist. Verwenden Sie diese Funktion, um zu verhindern, dass Ihr Load Balancer versehentlich oder böswillig gelöscht wird, was zum Verlust der Verfügbarkeit Ihrer Anwendungen führen kann.
PR.IP-3	Prozesse zur Steuerung von Konfigurationsänderungen sind vorhanden	rds-instance-deletion-protection-aktiviert	Stellen Sie sicher, dass Amazon Relational Database Service (Amazon RDS)-Instances den Löschschutz aktiviert haben. Verwenden Sie den Löschschutz, um zu verhindern, dass Ihre Amazon-RDS-Instances versehentlich oder böswillig gelöscht werden, was zum Verlust der Verfügbarkeit Ihrer Anwendungen führen kann.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.IP-4	Datensicherungen werden durchgeführt, verwaltet und getestet	dynamodb-in-backup-plan	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon DynamoDB-Tabellen Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.IP-4	Datensicherungen werden durchgeführt, verwaltet und getestet	ebs-in-backup-plan	Stellen Sie zur Unterstützung der Datensicherungspro zesse sicher, dass Ihre Amazon Elastic Block Store (Amazon EBS) -Volumes Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwaltet er Backup-Service mit einer richtlini enbasierten Backup-Lösung. Diese Lösung vereinfacht Ihre Backup-Verwaltung und ermöglicht es Ihnen, Ihre geschäftl ichen und behördlic hen Anforderungen bezüglich Backups zu erfüllen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.IP-4	Datensicherungen werden durchgeführt, verwaltet und getestet	efs-in-backup-plan	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon Elastic File System (Amazon EFS) -Dateisysteme Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.IP-4	Datensicherungen werden durchgeführt, verwaltet und getestet	rds-in-backup-plan	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon Relational Database Service (Amazon RDS) -Instances Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.IP-4	Datensicherungen werden durchgeführt, verwaltet und getestet	redshift-backup-enabled	Stellen Sie zur Unterstützung der Datensicherungsprozesse sicher, dass Ihre Amazon-Redshift-Cluster über automatisierte Snapshots verfügen. Wenn automatisierte Snapshots für einen Cluster aktiviert sind, erstellt Redshift in regelmäßigen Abständen Snapshots dieses Clusters. Standardmäßig erstellt Redshift alle acht Stunden oder alle 5 GB einen Snapshot für jeden Knoten mit Datenänderungen oder je nachdem, was zuerst eintritt.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.IP-4	Datensicherungen werden durchgeführt, verwaltet und getestet	db-instance-backup-enabled	Die Sicherungsfunktion von Amazon RDS erstellt Sicherungen Ihrer Datenbanken und Transaktionsprotokolle. Amazon RDS erstellt einen Snapshot für das Speichervolume Ihrer DB-Instance, sodass die gesamte DB-Instance gesichert wird. Sie können im System spezifische Aufbewahrungsfristen festlegen, um Ihre Ausfallsicherheitsanforderungen zu erfüllen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.IP-4	Datensicherungen werden durchgeführt, verwaltet und getestet	dynamodb-pitr-enabled	Aktivieren Sie diese Regel, um zu überprüfen, ob die Informationen gesichert wurden. Es verwaltet auch die Backups, indem es sicherstellt, dass die point-in-time Wiederherstellung in Amazon DynamoDB aktiviert ist. Bei der Wiederherstellung werden fortlaufende Backups Ihrer Tabelle für die letzten 35 Tage gespeichert.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.IP-4	Datensicherungen werden durchgeführt, verwaltet und getestet	elasticache-redis-cluster-automatic-Backup-Prüfung	Wenn automatische Backups aktiviert sind, ElastiCache erstellt Amazon täglich ein Backup des Clusters. Die Sicherung kann für eine von Ihrer Organisation festgelegte Anzahl von Tagen aufbewahrt werden. Automatische Backups schützen vor Datenverlust. Bei einem Ausfall können Sie einen neuen Cluster erstellen, der Ihre Daten aus dem aktuellen Backup wiederherstellt.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.IP-4	Datensicherungen werden durchgeführt, verwaltet und getestet	redshift-cluster-maintenancesettings-check	Diese Regel stellt sicher, dass Amazon-Redshift-Cluster die bevorzugten Einstellungen für Ihre Organisation haben. Insbesondere sorgt sie dafür, dass Cluster bevorzugte Wartungsfenster und automatisierte Aufbewahrungsfristen für Snapshots für die Datenbank haben. Für diese Regel müssen Sie die festlegen allowVersionUpgrade. Der Standardwert ist „true“. Außerdem können Sie optional den Zeitraum preferredMaintenanceWindow (der Standardwert ist sa: 16:00 -sa: 16:30) und den automated SnapshotRetention Zeitraum (der Standardwert ist 1) festlegen. Die tatsächlichen Werte müssen den Richtlini

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			en Ihrer Organisation entsprechen.
PR.IP-4	Datensicherungen werden durchgeführt, verwaltet und getestet	s3- bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) unterstützt die Aufrechterhaltung einer angemesse nen Kapazität und Verfügbarkeit. CRR ermöglicht das automatische, asynchrone Kopieren von Objekten in Amazon S3 Buckets, um die Datenverf ügbarkeit sicherzus tellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.IP-4	Datensicherungen werden durchgeführt, verwaltet und getestet	s-3 bucket-versioning-enabled	Die Versionsv erwaltung von Amazon Simple Storage Service (Amazon S3)-Bucke ts hilft dabei, mehrere Varianten eines Objekts im selben Amazon-S3-Bucket zu speichern. Verwenden Sie die Versionsv erwaltung, um sämtliche Versionen aller Objekte in Ihrem Amazon-S3-Bucket zu speichern , abzurufen oder wiederherzustellen . Mit der Versionsv erwaltung können Sie Versionen sowohl nach unbeabsic htigten Benutzera ktionen als auch nach Anwendungsfehlern problemlos wiederher stellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.IP-7	Die Schutzprozesse werden verbessert	ebs-optimized-instance	Eine optimierte Instance im Amazon Elastic Block Store (Amazon EBS) bietet zusätzliche, dedizierte Kapazität für Amazon-EBS-I/O-Vorgänge. Diese Optimierung bietet die beste Leistung für Ihr EBS-Volume, indem Konflikte zwischen Amazon-EBS-I/O und anderem Datenverkehr von Ihrer Instance minimiert werden.
PR.IP-8	Die Wirksamkeit der Schutztechnologien wird geteilt	dms-replication-not-public	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass auf DMS-Replikationsinstanzen nicht öffentlich zugegriffen werden kann. DMS-Replikations-Instances können vertrauliche Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.IP-8	Die Wirksamkeit der Schutztechnologien wird geteilt	ebs-snapshot-public-restorable-überprüfen	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass EBS-Snapshots nicht öffentlich wiederher stellbar sind. EBS-Volume-Snapsho ts können vertrauli che Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.
PR.IP-8	Die Wirksamkeit der Schutztechnologien wird geteilt	ec-2 instance-no-public-ip	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon Elastic Compute Cloud (Amazon EC2) - Instances nicht öffentlich zugänglic h sind. EC2Amazon -Instances können vertrauliche Informati onen enthalten, und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.IP-8	Die Wirksamkeit der Schutztechnologien wird geteilt	emr-master-no-public-ip	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon EMR-Cluster-Masterknoten nicht öffentlich zugänglich sind. Amazon-EMR-Cluster-Hauptknoten können vertrauliche Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.
PR.IP-8	Die Wirksamkeit der Schutztechnologien wird geteilt	lambda-function-public-access-verboten	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass AWS Lambda-Funktionen nicht öffentlich zugänglich sind. Der öffentliche Zugriff kann möglicherweise die Verfügbarkeit von Ressourcen beeinträchtigen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.IP-8	Die Wirksamkeit der Schutztechnologien wird geteilt	rds-instance-public-access-überprüfen	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Relational Database Service (Amazon RDS) -Instances nicht öffentlich sind. Amazon-RDS-Datenbank-Instances können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.IP-8	Die Wirksamkeit der Schutztechnologien wird geteilt	rds-snapshots-public-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Relational Database Service (Amazon RDS) -Instances nicht öffentlich sind. Amazon-RDS-Datenbank-Instances können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.IP-8	Die Wirksamkeit der Schutztechnologien wird geteilt	redshift-cluster-public-access-überprüfen	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Redshift Redshift-Cluster nicht öffentlich sind. Amazon-Redshift-Cluster können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.
PR.IP-8	Die Wirksamkeit der Schutztechnologien wird geteilt	s-3 bucket-public-read-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie nur autorisierten Benutzern, Prozessen und Geräten Zugriff auf Amazon Simple Storage Service (Amazon S3) - Buckets gewähren. Die Verwaltung des Zugriffs sollte mit der Klassifizierung der Daten übereinstimmen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.IP-8	Die Wirksamkeit der Schutztechnologien wird geteilt	s3- bucket-public-write-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie nur autorisierten Benutzern, Prozessen und Geräten Zugriff auf Amazon Simple Storage Service (Amazon S3) - Buckets gewähren. Die Verwaltung des Zugriffs sollte mit der Klassifizierung der Daten übereinstimmen.
PR.IP-8	Die Wirksamkeit der Schutztechnologien wird geteilt	sagemaker-notebook-no-direct-Internetzugang	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass SageMaker Amazon-Notebooks keinen direkten Internetzugang zulassen. Indem Sie direkten Internetzugang blockieren, vermeiden Sie, dass unbefugte Benutzer auf sensible Daten zugreifen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.IP-8	Die Wirksamkeit der Schutztechnologien wird geteilt	subnet-auto-assign-public-ip-deaktiviert	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon Virtual Private Cloud (VPC) -Subnetzen nicht automatisch eine öffentliche IP-Adresse zugewiesen wird. Amazon Elastic Compute Cloud (EC2) -Instances, die in Subnetzen gestartet werden, in denen dieses Attribut aktiviert ist, haben ihrer primären Netzwerkschnittstelle eine öffentliche IP-Adresse zugewiesen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.IP-12	Ein Plan für das Schwachstellenmanagement wird entwickelt und umgesetzt	ec2-manager instance-managed-by-systems	Eine Bestandsaufnahme der Softwareplattformen und Anwendungen innerhalb des Unternehmens ist möglich, indem Amazon Elastic Compute Cloud (Amazon EC2) - Instances mit AWS Systems Manager verwaltet werden. Verwenden Sie AWS Systems Manager, um detaillierte Systemkonfigurationen, Betriebssystem-Patch-Levels, Namen und Typ der Dienste, Softwareinstallationen, Anwendungsname, Herausgeber und Version sowie andere Details zu Ihrer Umgebung bereitzustellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.IP-12	Ein Plan für das Schwachstellenmanagement wird entwickelt und umgesetzt	ec2-check managedinstance-association-compliance-status	Verwenden Sie AWS Systems Manager Associations, um bei der Inventarisierung von Softwareplattformen und Anwendungen innerhalb eines Unternehmens zu helfen. AWS Systems Manager weist Ihren verwalteten Instances einen Konfigurationsstatus zu und ermöglicht es Ihnen, Basiswerte für Betriebssystem-Patch-Levels, Softwareinstallationen, Anwendungskonfigurationen und andere Details zu Ihrer Umgebung festzulegen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.IP-12	Ein Plan für das Schwachstellenmanagement wird entwickelt und umgesetzt	ec2-prüfen managedinstance-patch-compliance-status	Aktivieren Sie diese Regel, um bei der Identifizierung und Dokumentation von Sicherheitslücken in Amazon Elastic Compute Cloud (Amazon EC2) zu helfen. Die Regel prüft, ob die EC2 Amazon-Instance die Patch-Konformität im AWS Systems Manager gemäß den Richtlinien und Verfahren Ihrer Organisation einhält.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.MA-2	Die Fernwartung von Unternehm ensressourcen wird genehmigt, protokoll iert und in einer Weise durchgeführt, die unbefugten Zugriff verhindert.	multi-region-cloudtrail-enabled	AWS CloudTrail zeichnet Aktionen und API-Aufrufe der AWS Management Console auf. Sie können feststellen, welche Benutzer und Konten angerufen wurden AWS, von welcher Quell-IP-Adresse aus die Anrufe getätigt wurden und wann die Anrufe erfolgten. CloudTrail übermittelt Protokolldateien aus allen AWS Regionen an Ihren S3-Bucket , wenn MULTI_REG ION_CLOUD _TRAIL_ENABLED aktiviert ist. Außerdem wird beim AWS Start einer neuen Region derselbe Trail in der neuen Region erstellt. CloudTrail Dadurch erhalten Sie automatis ch Protokolldateien mit API-Aktivitäten für die neue Region.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.MA-2	Die Fernwartung von Unternehm ensressourcen wird genehmigt, protokoll iert und in einer Weise durchgeführt, die unbefugten Zugriff verhindert.	cloudtrail-enabled	AWS CloudTrai l kann durch die Aufzeichnung von Aktionen und API-Aufrufen in der AWS Management Console bei der Nichtabst reitbarkeit helfen. Sie können die Benutzer und die Benutzer AWS-Konten , die einen AWS Dienst aufgerufen haben, die Quell-IP-Adresse, über die die Aufrufe generiert wurden, und den Zeitpunkt der Anrufe identifiz ieren. Einzelheiten zu den erfassten Daten finden Sie in den AWS CloudTrail Datensatzinhalten.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.PT-1	Audit-/Protokollaufzeichnungen werden in Übereinstimmung mit den Richtlinien festgelegt, dokumentiert, umgesetzt und überprüft.	elasticsearch-logs-to-cloudwatch	Stellen Sie sicher, dass für Amazon OpenSearch Service-Domains Fehlerprotokolle aktiviert und zur Aufbewahrung und Beantwortung an Amazon CloudWatch Logs gestreamt werden. Domain-Fehlerprotokolle sind bei Sicherheits- und Zugriffsprüfungen sowie bei der Diagnose von Verfügbarkeitsproblemen nützlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.PT-1	Audit-/Protokollaufzeichnungen werden in Übereinstimmung mit den Richtlinien festgelegt, dokumentiert, umgesetzt und überprüft.	guardduty-non-archived-findings	Amazon GuardDuty hilft Ihnen dabei, die Auswirkungen eines Vorfalls zu verstehen, indem es die Ergebnisse nach Schweregrad klassifiziert: niedrig, mittel und hoch. Diese Klassifizierungen können Sie zur Festlegung von entsprechenden Strategien und Prioritäten zur Behebung solcher Vorfälle verwenden. Mit dieser Regel können Sie optional daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7) und daysHighSev (Config Default: 1) für nicht archivierte Ergebnisse festlegen, wie es die Richtlinien Ihrer Organisation erfordern.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.PT-1	Audit-/Protokollaufzeichnungen werden in Übereinstimmung mit den Richtlinien festgelegt, dokumentiert, umgesetzt und überprüft.	multi-region-cloudtrail-enabled	AWS CloudTrail zeichnet Aktionen und API-Aufrufe der AWS Management Console auf. Sie können feststellen, welche Benutzer und Konten angerufen wurden AWS, von welcher Quell-IP-Adresse aus die Anrufe getätigt wurden und wann die Anrufe erfolgten. CloudTrail übermittelt Protokolldateien aus allen AWS Regionen an Ihren S3-Bucket , wenn MULTI_REGION_CLOUD_TRAIL_ENABLED aktiviert ist. Außerdem wird beim AWS Start einer neuen Region derselbe Trail in der neuen Region erstellt. CloudTrail Dadurch erhalten Sie automatisch Protokolldateien mit API-Aktivitäten für die neue Region.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.PT-1	Kommunikations- und Kontrollnetzwerke sind geschützt	opensearch-logs-to-cloudwatch	Stellen Sie sicher, dass für Amazon OpenSearch Service-Domains Fehlerprotokolle aktiviert und zur Aufbewahrung und Beantwortung an Amazon CloudWatch Logs gestreamt werden. OpenSearch Service-Fehlerprotokolle können bei Sicherheits- und Zugriffsprüfungen helfen und bei der Diagnose von Verfügbarkeitsproblemen helfen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.PT-1	Audit-/Protokollaufzeichnungen werden in Übereinstimmung mit den Richtlinien festgelegt, dokumentiert, umgesetzt und überprüft.	rds-enhanced-monitoring-enabled	Aktivieren Sie Amazon Relational Database Service (Amazon RDS), um die Verfügbarkeit von Amazon RDS zu überwachen. Dies bietet einen detaillierten Einblick in den Zustand Ihrer Amazon-RDS-Datenbank-Instances. Wenn der Amazon-RDS-Speicher mehr als ein zugrunde liegendes physisches Gerät verwendet, erfasst Enhanced Monitoring die Daten für jedes Gerät. Wenn die Datenbank-Instance von Amazon RDS in einer Multi-AZ-Bereitstellung ausgeführt wird, werden außerdem die Daten für jedes Gerät auf dem sekundären Host sowie die Metriken des sekundären Hosts erfasst.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.PT-1	Audit-/Protokollaufzeichnungen werden in Übereinstimmung mit den Richtlinien festgelegt, dokumentiert, umgesetzt und überprüft.	rds-logging-enabled	Um die Protokollierung und Überwachung in Ihrer Umgebung zu erleichtern, stellen Sie sicher, dass die Amazon Relational Database Service (Amazon RDS)-Protokollierung aktiviert ist. Mit der Amazon-RDS-Protokollierung können Sie Ereignisse wie Verbindungen, Verbindungsabbrüche, Abfragen oder abgefragte Tabellen erfassen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.PT-1	Audit-/Protokollaufzeichnungen werden in Übereinstimmung mit den Richtlinien festgelegt, dokumentiert, umgesetzt und überprüft.	wafv2-logging-enabled	Um die Protokollierung und Überwachung in Ihrer Umgebung zu erleichtern, aktivieren Sie die AWS WAF (V2) -Protokollierung im regionalen und globalen Internet ACLs. AWS Die WAF-Protokollierung bietet detaillierte Informationen über den Datenverkehr, der von Ihrer Web-ACL analysiert wird. In den Protokollen werden die Uhrzeit aufgezeichnet, zu der die AWS WAF die Anfrage von Ihrer AWS Ressource erhalten hat, Informationen zu der Anfrage und eine Aktion für die Regel, der jede Anfrage entsprach.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.PT-1	Audit-/Protokollaufzeichnungen werden in Übereinstimmung mit den Richtlinien festgelegt, dokumentiert, umgesetzt und überprüft.	api-gw-execution-logging-aktiviert	Die API-Gateway-Protokollierung zeigt detaillierte Ansichten der Benutzer, die auf die API zugegriffen haben, und wie diese Benutzer auf die API zugegriffen haben. Diese Insights ermöglichen die Einsicht in Benutzeraktivitäten.
PR.PT-1	Audit-/Protokollaufzeichnungen werden in Übereinstimmung mit den Richtlinien festgelegt, dokumentiert, umgesetzt und überprüft.	cloud-trail-cloud-watch-logs-aktiviert	Verwenden Sie Amazon CloudWatch , um Protokollereignisaktivitäten zentral zu sammeln und zu verwalten. Die Aufnahme von AWS CloudTrail Daten liefert Einzelheiten zu den API-Aufrufaktivitäten in Ihrem AWS-Konto.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.PT-1	Audit-/Protokollaufzeichnungen werden in Übereinstimmung mit den Richtlinien festgelegt, dokumentiert, umgesetzt und überprüft.	cloudtrail-enabled	AWS CloudTrail kann bei der Nichtabstreitbarkeit helfen, indem Aktionen und API-Aufrufe der AWS Management Console aufgezeichnet werden. Sie können die Benutzer und die Benutzer AWS-Konten , die einen AWS Dienst aufgerufen haben, die Quell-IP-Adresse, über die die Aufrufe generiert wurden, und den Zeitpunkt der Anrufe identifizieren. Einzelheiten zu den erfassten Daten finden Sie in den AWS CloudTrail Datensatzinhalten.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.PT-1	Audit-/Protokollaufzeichnungen werden in Übereinstimmung mit den Richtlinien festgelegt, dokumentiert, umgesetzt und überprüft.	cloudtrail-s3-dataevents-enabled	Die Erfassung von Simple Storage Service (Amazon S3)-Datenereignissen unterstützt die Erkennung von ungewöhnlichen Aktivitäten. Zu den Details gehören Informationen zum AWS -Konto, das auf einen Amazon S3 Bucket zugegriffen hat, die IP-Adresse und die Uhrzeit des Ereignisses.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.PT-1	Audit-/Protokollaufzeichnungen werden in Übereinstimmung mit den Richtlinien festgelegt, dokumentiert, umgesetzt und überprüft.	elb-logging-enabled	Die Elastic-Load-Balancing-Aktivität ist ein zentraler Kommunikationspunkt innerhalb einer Umgebung. Stellen Sie sicher, dass die ELB-Protokollierung aktiviert ist. Die gesammelten Daten enthalten detaillierte Informationen zu Anfragen, die an den ELB gesendet wurden. Jedes Protokoll enthält Informationen wie die Zeit, zu der die Anforderung einging, die Client-IP-Adresse, Latenzen, Anforderungspfade und Serverantworten.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.PT-1	Audit-/Protokollaufzeichnungen werden in Übereinstimmung mit den Richtlinien festgelegt, dokumentiert, umgesetzt und überprüft.	guardduty-enabled-centralized	Amazon GuardDuty kann mithilfe von Threat Intelligence Feeds helfen, potenzielle Cybersicherheitsereignisse zu überwachen und zu erkennen. Dazu gehören Listen mit bösartigen IPs und maschinellen Lernmethoden zur Identifizierung unerwarteter, nicht autorisierter und bösartiger Aktivitäten in Ihrer AWS Cloud-Umgebung.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.PT-1	Audit-/Protokollaufzeichnungen werden in Übereinstimmung mit den Richtlinien festgelegt, dokumentiert, umgesetzt und überprüft.	redshift-cluster-configuration-check	Um Daten im Ruhezustand zu schützen, muss die Verschlüsselung für Ihre Amazon-Redshift-Cluster aktiviert sein. Sie müssen auch sicherstellen, dass die erforderlichen Konfigurationen auf Amazon-Redshift-Clustern bereitgestellt werden. Die Prüfungsprotokollierung muss aktiviert sein, um Informationen zu Verbindungen und Benutzeraktivitäten in der Datenbank bereitzustellen. Diese Regel erfordert, dass ein Wert für clusterDbEncrypted (Config Default: TRUE) und LoggingEnabled (Config Default: TRUE) gesetzt ist. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.PT-1	Audit-/Protokollaufzeichnungen werden in Übereinstimmung mit den Richtlinien festgelegt, dokumentiert, umgesetzt und überprüft.	s3- bucket-logging-enabled	Die Amazon Simple Storage Service (Amazon S3)-Serverzugriffsprotokollierung bietet eine Methode zur Überwachung des Netzwerks im Hinblick auf potenzielle Cybersicherheitsereignisse. Die Ereignisse werden überwacht, indem detaillierte Aufzeichnungen über die Anfragen erfasst werden, die an einen Amazon-S3-Bucket gestellt wurden. Jeder Zugriffsprotokolleintrag enthält Details zu einer einzelnen Zugriffsanfrage. Zu den Details gehören Anforderer, Bucket-Name, Anforderungszeit, Anforderungsaktion, Antwortstatus und Fehlercode, falls relevant.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.PT-1	Audit-/Protokollaufzeichnungen werden in Übereinstimmung mit den Richtlinien festgelegt, dokumentiert, umgesetzt und überprüft.	vpc-flow-logs-enabled	VPC-Flow-Protokolle erfassen detaillierte Informationsdatensätze über den IP-Datenverkehr, der zu und von Netzwerkschnittstellen in Ihrer Amazon Virtual Private Cloud (Amazon VPC) fließt. Standardmäßig enthalten Flow-Protokolldatensätze Werte für die verschiedenen Komponenten des IP-Flows, einschließlich Quelle, Ziel und Protokoll.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.PT-3	Das Prinzip der geringsten Funktionalität wird durch die Konfiguration von Systemen umgesetzt, die nur die wesentlichen Funktionen bereitstellen.	autoscaling-launch-config-public-ip-deaktiviert	Wenn Sie Ihre Netzwerkschnittstellen mit einer öffentlichen IP-Adresse konfigurieren, sind die diesen Netzwerkschnittstellen zugehörigen Ressourcen über das Internet erreichbar. EC2 Ressourcen sollten nicht öffentlich zugänglich sein, da dies einen unbeabsichtigten Zugriff auf Ihre Anwendungen oder Server ermöglichen kann.
PR.PT-3	Das Prinzip der geringsten Funktionalität wird durch die Konfiguration von Systemen umgesetzt, die nur die wesentlichen Funktionen bereitstellen.	ec2- instance-profile-attached	EC2 Instanzprofile übergeben eine IAM-Rolle an eine EC2 Instance. Das Anhängen eines Instance-Profils an Ihre Instances kann bei der Implementierung von geringsten Berechtigungen und der Berechtigungsverwaltung helfen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.PT-3	Das Prinzip der geringsten Funktionalität wird durch die Konfiguration von Systemen umgesetzt, die nur die wesentlichen Funktionen bereitstellen.	ec2- instances-in-vpc	Stellen Sie Amazon Elastic Compute Cloud (Amazon EC2) -Instances innerhalb einer Amazon Virtual Private Cloud (Amazon VPC) bereit, um eine sichere Kommunikation zwischen einer Instance und anderen Services innerhalb der Amazon VPC zu ermöglichen, ohne dass ein Internet-Gateway, ein NAT-Gerät oder eine VPN-Verbindung erforderlich ist. Der gesamte Datenverkehr bleibt sicher in der AWS Cloud. Domains, die sich innerhalb einer VPC befinden, verfügen aufgrund ihrer logischen Isolierung im Vergleich zu Domains mit öffentlichen Endpunkten über eine zusätzliche Sicherheitsebene. Weisen Sie EC2

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			Amazon-Instances einer Amazon-VPC zu, um den Zugriff ordnungsgemäß zu verwalten.
PR.PT-3	Das Prinzip der geringsten Funktionalität wird durch die Konfiguration von Systemen umgesetzt, die nur die wesentlichen Funktionen bereitstellen.	redshift-enhanced-vpc-routing-aktiviert	Mit Enhanced-VPC-Routing wird erzwungen, dass der gesamte COPY- und UNLOAD-Datenverkehr zwischen Ihrem Cluster und Datenrepositorys über Ihre Amazon VPC erfolgt. Anschließend können Sie VPC-Features wie Sicherheitsgruppen und Netzwerkzugriffskontrolllisten verwenden, um den Netzwerkverkehr zu schützen. Sie können auch VPC-Flow-Logs verwenden, um den Netzwerkverkehr zu überwachen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.PT-3	Das Prinzip der geringsten Funktionalität wird durch die Konfiguration von Systemen umgesetzt, die nur die wesentlichen Funktionen bereitstellen.	ssm-document-not-public	Stellen Sie sicher, dass AWS Systems Manager (SSM) - Dokumente nicht öffentlich sind, da dies einen unbeabsichtigten Zugriff auf Ihre SSM-Dokumente ermöglichen kann. Ein öffentliches SSM-Dokument kann Informationen über Ihr Konto, Ihre Ressourcen und internen Prozesse preisgeben.
PR.PT-3	Das Prinzip der geringsten Funktionalität wird durch die Konfiguration von Systemen umgesetzt, die nur die wesentlichen Funktionen bereitstellen.	dms-replication-not-public	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass auf DMS-Replikationsinstanzen nicht öffentlich zugegriffen werden kann. DMS-Replikations-Instances können vertrauliche Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.PT-3	Das Prinzip der geringsten Funktionalität wird durch die Konfiguration von Systemen umgesetzt, die nur die wesentlichen Funktionen bereitstellen.	ebs-snapshot-public-restorable-überprüfen	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass EBS-Snapshots nicht öffentlich wiederherstellbar sind. EBS-Volume-Snapshots können vertrauliche Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.
PR.PT-3	Das Prinzip der geringsten Funktionalität wird durch die Konfiguration von Systemen umgesetzt, die nur die wesentlichen Funktionen bereitstellen.	ec-2 instance-no-public-ip	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon Elastic Compute Cloud (Amazon EC2) - Instances nicht öffentlich zugänglich sind. EC2Amazon-Instances können vertrauliche Informationen enthalten, und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.PT-3	Das Prinzip der geringsten Funktionalität wird durch die Konfiguration von Systemen umgesetzt, die nur die wesentlichen Funktionen bereitstellen.	elasticsearch-in-vpc-only	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass sich Amazon OpenSearch OpenSearch Service (Service) - Domains innerhalb einer Amazon Virtual Private Cloud (Amazon VPC) befinden. Eine OpenSearch Service-Domain innerhalb einer Amazon VPC ermöglicht die sichere Kommunikation zwischen OpenSearch Service und anderen Services innerhalb der Amazon VPC, ohne dass ein Internet-Gateway, ein NAT-Gerät oder eine VPN-Verbindung erforderlich ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.PT-3	Das Prinzip der geringsten Funktionalität wird durch die Konfiguration von Systemen umgesetzt, die nur die wesentlichen Funktionen bereitstellen.	emr-master-no-public-ip	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon EMR-Cluster-Masterknoten nicht öffentlich zugänglich sind. Amazon-EMR-Cluster-Hauptknoten können vertrauliche Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.PT-3	Das Prinzip der geringsten Funktionalität wird durch die Konfiguration von Systemen umgesetzt, die nur die wesentlichen Funktionen bereitstellen.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) kann Ihnen dabei helfen, die Prinzipien der geringsten Rechte und der Aufgabentrennung in Zugriffsberechtigungen und Autorisierungen zu integrieren und so zu verhindern, dass Richtlinien „Effect“: „Allow“ mit „Action“: „*“ anstelle von „Resource“: „*“ enthalten. Wenn Benutzern mehr Rechte eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Rechte und der Aufgabentrennung verstoßen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.PT-3	Das Prinzip der geringsten Funktionalität wird durch die Konfiguration von Systemen umgesetzt, die nur die wesentlichen Funktionen bereitstellen.	iam-root-access-key-überprüfen	Der Zugriff auf Systeme und Ressourcen kann gesteuert werden, indem überprüft wird, ob der Root-Benutzer keine Zugriffsschlüssel mit seiner AWS Identity and Access Management (IAM) -Rolle verknüpft hat. Stellen Sie sicher, dass die Root-Zugriffsschlüssel gelöscht werden. Erstellen und verwenden Sie stattdessen rollenbasierte Funktionen, AWS-Konten um das Prinzip der geringsten Funktionalität zu berücksichtigen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.PT-3	Das Prinzip der geringsten Funktionalität wird durch die Konfiguration von Systemen umgesetzt, die nur die wesentlichen Funktionen bereitstellen.	iam-user-no-policies-überprüfen	Diese Regel stellt sicher, dass AWS Identity and Access Management (IAM)-Richtlinien nur Gruppen oder Rollen zugewiesen werden, um den Zugriff auf Systeme und Ressourcen zu kontrollieren. Die Zuweisung von Berechtigungen auf Gruppen- oder Rollenebene trägt dazu bei, die Wahrscheinlichkeit zu verringern, dass eine Identität übermäßige Berechtigungen erhält oder beibehält.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.PT-3	Das Prinzip der geringsten Funktionalität wird durch die Konfiguration von Systemen umgesetzt, die nur die wesentlichen Funktionen bereitstellen.	lambda-function-public-access-verboten	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass AWS Lambda-Funktionen nicht öffentlich zugänglich sind. Der öffentliche Zugriff kann möglicherweise die Verfügbarkeit von Ressourcen beeinträchtigen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.PT-3	Das Prinzip der geringsten Funktionalität wird durch die Konfiguration von Systemen umgesetzt, die nur die wesentlichen Funktionen bereitstellen.	lambda-inside-vpc	Stellen Sie AWS Lambda-Funktionen in einer Amazon Virtual Private Cloud (Amazon VPC) bereit, um eine sichere Kommunikation zwischen einer Funktion und anderen Diensten innerhalb der Amazon VPC zu gewährleisten. Bei dieser Konfiguration sind kein Internet-Gateway, kein NAT-Gerät und keine VPN-Verbindung erforderlich. Der gesamte Datenverkehr bleibt sicher in der Cloud. AWS Domains, die sich innerhalb einer VPC befinden, verfügen aufgrund ihrer logischen Isolierung im Vergleich zu Domains mit öffentlichen Endpunkten über eine zusätzliche Sicherheitsebene. Um den Zugriff ordnungsgemäß zu verwalten,

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			sollten AWS Lambda-Funktionen einer VPC zugewiesen werden.
PR.PT-3	Das Prinzip der geringsten Funktionalität wird durch die Konfiguration von Systemen umgesetzt, die nur die wesentlichen Funktionen bereitstellen.	opensearch-in-vpc-only	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass sich Amazon OpenSearch Service-Domains innerhalb einer Amazon Virtual Private Cloud (Amazon VPC) befinden. Eine Amazon OpenSearch Service-Domain innerhalb einer Amazon VPC ermöglicht die sichere Kommunikation zwischen Amazon OpenSearch Service und anderen Services innerhalb der Amazon VPC, ohne dass ein Internet-Gateway, ein NAT-Gerät oder eine VPN-Verbindung erforderlich ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.PT-3	Das Prinzip der geringsten Funktionalität wird durch die Konfiguration von Systemen umgesetzt, die nur die wesentlichen Funktionen bereitstellen.	rds-instance-public-access-überprüfen	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Relational Database Service (Amazon RDS) -Instances nicht öffentlich sind. Amazon-RDS-Datenbank-Instances können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.PT-3	Das Prinzip der geringsten Funktionalität wird durch die Konfiguration von Systemen umgesetzt, die nur die wesentlichen Funktionen bereitstellen.	rds-snapshots-public-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Relational Database Service (Amazon RDS) -Instances nicht öffentlich sind. Amazon-RDS-Datenbank-Instances können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.PT-3	Das Prinzip der geringsten Funktionalität wird durch die Konfiguration von Systemen umgesetzt, die nur die wesentlichen Funktionen bereitstellen.	redshift-cluster-public-access-überprüfen	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Redshift Redshift-Cluster nicht öffentlich sind. Amazon-Redshift-Cluster können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.PT-3	Das Prinzip der geringsten Funktionalität wird durch die Konfiguration von Systemen umgesetzt, die nur die wesentlichen Funktionen bereitstellen.	s3- -Block-periodisch account-level-public-access	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Simple Storage Service (Amazon S3) -Buckets nicht öffentlich zugänglich sind. Diese Regel trägt dazu bei, sensible Daten vor unbefugten Remote-Benutzern zu schützen, indem sie den öffentlichen Zugriff verhindert. Mit dieser Regel können Sie optional die Parameter ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) und restrictPublicBuckets Parameter (Config Default: True) festlegen. Die tatsächlichen Werte müssen den Richtlini

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			en Ihrer Organisation entsprechen.
PR.PT-3	Das Prinzip der geringsten Funktionalität wird durch die Konfiguration von Systemen umgesetzt, die nur die wesentlichen Funktionen bereitstellen.	s3- bucket-public-read-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie nur autorisierten Benutzern, Prozessen und Geräten Zugriff auf Amazon Simple Storage Service (Amazon S3) - Buckets gewähren. Die Verwaltung des Zugriffs sollte mit der Klassifizierung der Daten übereinstimmen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.PT-3	Das Prinzip der geringsten Funktionalität wird durch die Konfiguration von Systemen umgesetzt, die nur die wesentlichen Funktionen bereitstellen.	s3- bucket-public-write-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie nur autorisierten Benutzern, Prozessen und Geräten Zugriff auf Amazon Simple Storage Service (Amazon S3) - Buckets gewähren. Die Verwaltung des Zugriffs sollte mit der Klassifizierung der Daten übereinstimmen.
PR.PT-3	Das Prinzip der geringsten Funktionalität wird durch die Konfiguration von Systemen umgesetzt, die nur die wesentlichen Funktionen bereitstellen.	sagemaker-notebook-no-direct-Internetzugang	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass SageMaker Amazon-Notebooks keinen direkten Internetzugang zulassen. Indem Sie direkten Internetzugang blockieren, vermeiden Sie, dass unbefugte Benutzer auf sensible Daten zugreifen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.PT-3	Das Prinzip der geringsten Funktionalität wird durch die Konfiguration von Systemen umgesetzt, die nur die wesentlichen Funktionen bereitstellen.	subnet-auto-assign-public-ip-deaktiviert	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon Virtual Private Cloud (VPC) -Subnetzen nicht automatisch eine öffentliche IP-Adresse zugewiesen wird. Amazon Elastic Compute Cloud (EC2) -Instances, die in Subnetzen gestartet werden, in denen dieses Attribut aktiviert ist, haben ihrer primären Netzwerkschnittstelle eine öffentliche IP-Adresse zugewiesen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.PT-4	Kommunikations- und Kontrollnetzwerke sind geschützt	autoscaling-launch-config-public-ip-deaktiviert	Wenn Sie Ihre Netzwerkschnittstellen mit einer öffentlichen IP-Adresse konfigurieren, sind die diesen Netzwerkschnittstellen zugehörigen Ressourcen über das Internet erreichbar. EC2 Ressourcen sollten nicht öffentlich zugänglich sein, da dies einen unbeabsichtigten Zugriff auf Ihre Anwendungen oder Server ermöglichen kann.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.PT-4	Kommunikations- und Kontrollnetzwerke sind geschützt	ec2- instances-in-vpc	Stellen Sie Amazon Elastic Compute Cloud (Amazon EC2) -Instances innerhalb einer Amazon Virtual Private Cloud (Amazon VPC) bereit, um eine sichere Kommunika tion zwischen einer Instance und anderen Services innerhalb der Amazon VPC zu ermöglichen, ohne dass ein Internet-Gateway, ein NAT-Gerät oder eine VPN-Verbindung erforderlich ist. Der gesamte Datenverk ehr bleibt sicher in der AWS Cloud. Domains, die sich innerhalb einer VPC befinden, verfügen aufgrund ihrer logischen Isolierun g im Vergleich zu Domains mit öffentlic hen Endpunkten über eine zusätzlic he Sicherheitsebene. Weisen Sie EC2

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			Amazon-Instances einer Amazon-VPC zu, um den Zugriff ordnungsgemäß zu verwalten.
PR.PT-4	Kommunikations- und Kontrollnetzwerke sind geschützt	no-unrestricted-route-to-igw	Stellen Sie sicher, dass EC2 Amazon-Routentabellen keine uneingeschränkten Routen zu einem Internet-Gateway enthalten. Durch das Entfernen oder Beschränken des Internetzugangs für Workloads innerhalb von Amazon VPCs können unbeabsic htigte Zugriffe in Ihrer Umgebung reduziert werden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.PT-4	Kommunikations- und Kontrollnetzwerke sind geschützt	ssm-document-not-public	Stellen Sie sicher, dass AWS Systems Manager (SSM) - Dokumente nicht öffentlich sind, da dies einen unbeabsichtigten Zugriff auf Ihre SSM-Dokumente ermöglichen kann. Ein öffentliches SSM-Dokument kann Informationen über Ihr Konto, Ihre Ressourcen und internen Prozesse preisgeben.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.PT-4	Kommunikations- und Kontrollnetzwerke sind geschützt	acm-certificate-expiration-check	Stellen Sie sicher, dass die Netzwerkintegrität geschützt ist, indem Sie sicherstellen, dass X509-Zertifikate von ACM ausgestellt werden. AWS Diese Zertifikate müssen gültig und dürfen nicht abgelaufen sein. Für diese Regel ist ein Wert für erforderlich daysToExpiration (Wert für bewährte AWS Grundregeln für Sicherheit: 90). Der tatsächliche Wert muss den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.PT-4	Kommunikations- und Kontrollnetzwerke sind geschützt	dms-replication-not-public	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass auf DMS-Replikationsin stanzen nicht öffentlic h zugegriffen werden kann. DMS-Repli kations-Instances können vertrauli che Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.
PR.PT-4	Kommunikations- und Kontrollnetzwerke sind geschützt	ebs-snapshot-public-restorable-überprüfen	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass EBS-Snapshots nicht öffentlich wiederher stellbar sind. EBS-Volume-Snapsho ts können vertrauli che Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.PT-4	Kommunikations- und Kontrollnetzwerke sind geschützt	ec-2 instance-no-public-ip	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon Elastic Compute Cloud (Amazon EC2) - Instances nicht öffentlich zugänglic h sind. EC2Amazon -Instances können vertrauliche Informati onen enthalten, und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.PT-4	Kommunikations- und Kontrollnetzwerke sind geschützt	elasticsearch-in-vpc-only	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass sich Amazon OpenSearch OpenSearch Service (Service) - Domains innerhalb einer Amazon Virtual Private Cloud (Amazon VPC) befinden. Eine OpenSearch Service-Domain innerhalb einer Amazon VPC ermöglicht die sichere Kommunikation zwischen OpenSearch Service und anderen Services innerhalb der Amazon VPC, ohne dass ein Internet-Gateway, ein NAT-Gerät oder eine VPN-Verbindung erforderlich ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.PT-4	Kommunikations- und Kontrollnetzwerke sind geschützt	emr-master-no-public-ip	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon EMR-Cluster-Masterknoten nicht öffentlich zugänglich sind. Amazon-EMR-Cluster-Hauptknoten können vertrauliche Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.PT-4	Kommunikations- und Kontrollnetzwerke sind geschützt	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) Security Groups können bei der Verwaltung des Netzwerkzugriffs helfen, indem sie eine statusbeh aftete Filterung von eingehendem und ausgehendem Netzwerkverkehr zu Ressourcen bereitste llen. AWS Wenn Sie eingehenden (oder entfernten) Datenverk ehr von 0.0.0.0/0 bis Port 22 auf Ihren Ressourcen nicht zulassen, können Sie den Fernzugriff einschränken.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.PT-4	Kommunikations- und Kontrollnetzwerke sind geschützt	lambda-function-public-access-verboten	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass AWS Lambda-Funktionen nicht öffentlich zugänglich sind. Der öffentliche Zugriff kann möglicherweise die Verfügbarkeit von Ressourcen beeinträchtigen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.PT-4	Kommunikations- und Kontrollnetzwerke sind geschützt	lambda-inside-vpc	Stellen Sie AWS Lambda-Funktionen in einer Amazon Virtual Private Cloud (Amazon VPC) bereit, um eine sichere Kommunika tion zwischen einer Funktion und anderen Diensten innerhalb der Amazon VPC zu gewährleisten. Bei dieser Konfiguration sind kein Internet-Gateway, kein NAT-Gerät und keine VPN-Verbindung erforderlich. Der gesamte Datenverk ehr bleibt sicher in der Cloud. AWS Domains, die sich innerhalb einer VPC befinden, verfügen aufgrund ihrer logischen Isolierun g im Vergleich zu Domains mit öffentlic hen Endpunkten über eine zusätzliche Sicherheitsebene. Um den Zugriff ordnungsg emäß zu verwalten,

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			sollten AWS Lambda-Funktionen einer VPC zugewiesen werden.
PR.PT-4	Kommunikations- und Kontrollnetzwerke sind geschützt	opensearch-in-vpc-only	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass sich Amazon OpenSearch Service-Domains innerhalb einer Amazon Virtual Private Cloud (Amazon VPC) befinden. Eine Amazon OpenSearch Service-Domain innerhalb einer Amazon VPC ermöglicht die sichere Kommunikation zwischen Amazon OpenSearch Service und anderen Services innerhalb der Amazon VPC, ohne dass ein Internet-Gateway, ein NAT-Gerät oder eine VPN-Verbindung erforderlich ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.PT-4	Kommunikations- und Kontrollnetzwerke sind geschützt	rds-instance-public-access-überprüfen	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Relational Database Service (Amazon RDS) -Instances nicht öffentlich sind. Amazon-RDS-Datenbank-Instances können vertrauliche Informationen enthalten und für solche Konten sind Grundsätze und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.PT-4	Kommunikations- und Kontrollnetzwerke sind geschützt	rds-snapshots-public-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Relational Database Service (Amazon RDS) -Instances nicht öffentlich sind. Amazon-RDS-Datenbank-Instances können vertrauliche Informationen enthalten, und für solche Konten sind Prinzipien und eine Zugriffskontrolle erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.PT-4	Kommunikations- und Kontrollnetzwerke sind geschützt	redshift-cluster-public-access-überprüfen	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Redshift Redshift-Cluster nicht öffentlich sind. Amazon-Redshift-Cluster können vertrauliche Informationen enthalten und für solche Konten sind Prinzipale und eine Zugriffskontrolle erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.PT-4	Kommunikations- und Kontrollnetzwerke sind geschützt	restricted-common-ports	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass gemeinsame Ports für Amazon Elastic Compute Cloud (Amazon EC2) -Sicherheitsgruppen eingeschränkt sind. Wenn der Zugriff auf Ports nicht auf vertrauenswürdige Quellen beschränkt wird, kann dies zu Angriffen auf die Verfügbarkeit, Integrität und Vertraulichkeit von Systemen führen. Mit dieser Regel können Sie optional die Parameter blockedPort1–blockedPort5 festlegen (Standardkonfigurationen: 20, 21, 3389, 3306, 4333). Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.PT-4	Kommunikations- und Kontrollnetzwerke sind geschützt	s3- account-level-public-access -Block-periodisch	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Simple Storage Service (Amazon S3) -Buckets nicht öffentlich zugänglich sind. Diese Regel trägt dazu bei, sensible Daten vor unbefugten Remote-Benutzern zu schützen, indem sie den öffentlichen Zugriff verhindert. Mit dieser Regel können Sie optional die Parameter ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) und restrictPublicBuckets Parameter (Config Default: True) festlegen. Die tatsächlichen Werte müssen den Richtlini

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			en Ihrer Organisation entsprechen.
PR.PT-4	Kommunikations- und Kontrollnetzwerke sind geschützt	s3- bucket-public-read -prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie nur autorisierten Benutzern, Prozessen und Geräten Zugriff auf Amazon Simple Storage Service (Amazon S3) - Buckets gewähren. Die Verwaltung des Zugriffs sollte mit der Klassifizierung der Daten übereinst immen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.PT-4	Kommunikations- und Kontrollnetzwerke sind geschützt	s3- bucket-public-write-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie nur autorisierten Benutzern, Prozessen und Geräten Zugriff auf Amazon Simple Storage Service (Amazon S3) - Buckets gewähren. Die Verwaltung des Zugriffs sollte mit der Klassifizierung der Daten übereinstimmen.
PR.PT-4	Kommunikations- und Kontrollnetzwerke sind geschützt	sagemaker-notebook-no-direct-Internetzugang	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass SageMaker Amazon-Notebooks keinen direkten Internetzugang zulassen. Indem Sie direkten Internetzugang blockieren, vermeiden Sie, dass unbefugte Benutzer auf sensible Daten zugreifen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.PT-4	Kommunikations- und Kontrollnetzwerke sind geschützt	subnet-auto-assign-public-ip-deaktiviert	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon Virtual Private Cloud (VPC) -Subnetzen nicht automatisch eine öffentliche IP-Adresse zugewiesen wird. Amazon Elastic Compute Cloud (EC2) -Instances, die in Subnetzen gestartet werden, in denen dieses Attribut aktiviert ist, haben ihrer primären Netzwerkschnittstelle eine öffentliche IP-Adresse zugewiesen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.PT-4	Kommunikations- und Kontrollnetzwerke sind geschützt	vpc-default-security-group-geschlossen	Sicherheitsgruppen von Amazon Elastic Compute Cloud (Amazon EC2) können bei der Verwaltung des Netzwerkzugriffs helfen, indem sie eine statusbehaftete Filterung des ein- und ausgehenden Netzwerkverkehrs zu Ressourcen bereitstellen. AWS Die Beschränk ung des gesamten Datenverkehrs auf die Standardsicherheit sgruppe hilft dabei, den Fernzugriff auf Ihre Ressourcen einzuschränken. AWS

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.PT-4	Kommunikations- und Kontrollnetzwerke sind geschützt	vpc-sg-open-only-to-authorized-ports	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass gemeinsame Ports für Amazon Elastic Compute Cloud (Amazon EC2) -Sicherheitsgruppen eingeschränkt sind. Wenn der Zugriff auf Ports nicht auf vertrauenswürdige Quellen beschränkt wird, kann dies zu Angriffen auf die Verfügbarkeit, Integrität und Vertraulichkeit von Systemen führen. Durch die Beschränkung des Zugriffs auf Ressourcen innerhalb einer Sicherheitsgruppe aus dem Internet (0.0.0.0/0) kann der Fernzugriff auf interne Systeme gesteuert werden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.PT-5	Mechanismen (z. B. Failsafe, Load Balancing, Hot-Swap) werden implement iert, um die Anforderu ngen an die Ausfallsi cherheit in normalen und widrigen Situation en zu erfüllen	dynamodb-in-backup-plan	Um Sie bei Datensich erungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon DynamoDB-Tabellen Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwaltet er Backup-Service mit einer richtlini enbasierten Backup-Lösung. Diese Lösung vereinfac ht Ihr Sicherung smanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforde rungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.PT-5	Mechanismen (z. B. Failsafe, Load Balancing, Hot-Swap) werden implement iert, um die Anforderu ngen an die Ausfallsi cherheit in normalen und widrigen Situation en zu erfüllen	ebs-in-backup-plan	Stellen Sie zur Unterstützung der Datensicherungspro zesse sicher, dass Ihre Amazon Elastic Block Store (Amazon EBS) -Volumes Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwaltet er Backup-Service mit einer richtlini enbasierten Backup-Lösung. Diese Lösung vereinfacht Ihre Backup-Verwaltung und ermöglicht es Ihnen, Ihre geschäftl ichen und behördlic hen Anforderungen bezüglich Backups zu erfüllen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.PT-5	Mechanismen (z. B. Failsafe, Load Balancing, Hot-Swap) werden implement iert, um die Anforderu ngen an die Ausfallsi cherheit in normalen und widrigen Situation en zu erfüllen	efs-in-backup-plan	Um Sie bei Datensich erungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon Elastic File System (Amazon EFS) -Dateisysteme Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwaltet er Backup-Service mit einer richtlini enbasierten Backup-Lösung. Diese Lösung vereinfac ht Ihr Sicherung smanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforde rungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.PT-5	Mechanismen (z. B. Failsafe, Load Balancing, Hot-Swap) werden implementiert, um die Anforderungen an die Ausfallsicherheit in normalen und widrigen Situationen zu erfüllen	elb-cross-zone-load-Balancing aktiviert	Aktivieren Sie zonenübergreifendes Load Balancing für Ihre Elastic Load Balancer (ELBs), um eine angemessene Kapazität und Verfügbarkeit aufrechtzuerhalten. Zonenübergreifendes Load Balancing reduziert die Notwendigkeit, die gleiche Anzahl von Instances in jeder aktivierten Availability Zone aufrechtzuerhalten. Es verbessert auch die Fähigkeit Ihrer Anwendung, den Verlust einer oder mehrerer Instances zu bewältigen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.PT-5	Mechanismen (z. B. Failsafe, Load Balancing, Hot-Swap) werden implement iert, um die Anforderu ngen an die Ausfallsi cherheit in normalen und widrigen Situation en zu erfüllen	rds-instance-deletion-protection-aktiviert	Stellen Sie sicher, dass Amazon Relational Database Service (Amazon RDS)-Instances den Löschschutz aktiviert haben. Verwenden Sie den Löschschu tz, um zu verhindern, dass Ihre Amazon-RD S-Instances versehent lich oder böswillig gelöscht werden, was zum Verlust der Verfügbarkeit Ihrer Anwendungen führen kann.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.PT-5	Mechanismen (z. B. Failsafe, Load Balancing, Hot-Swap) werden implement iert, um die Anforderu ngen an die Ausfallsi cherheit in normalen und widrigen Situation en zu erfüllen	rds-in-backup-plan	Um Sie bei Datensich erungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon Relational Database Service (Amazon RDS) -Instance s Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwaltet er Backup-Service mit einer richtlini enbasierten Backup-Lösung. Diese Lösung vereinfac ht Ihr Sicherung smanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforde rungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.PT-5	Mechanismen (z. B. Failsafe, Load Balancing, Hot-Swap) werden implementiert, um die Anforderungen an die Ausfallsicherheit in normalen und widrigen Situationen zu erfüllen	redshift-backup-enabled	Stellen Sie zur Unterstützung der Datensicherungsprozesse sicher, dass Ihre Amazon-Redshift-Cluster über automatisierte Snapshots verfügen. Wenn automatisierte Snapshots für einen Cluster aktiviert sind, erstellt Redshift in regelmäßigen Abständen Snapshots dieses Clusters. Standardmäßig erstellt Redshift alle acht Stunden oder alle 5 GB einen Snapshot für jeden Knoten mit Datenänderungen oder je nachdem, was zuerst eintritt.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.PT-5	Mechanismen (z. B. Failsafe, Load Balancing, Hot-Swap) werden implement iert, um die Anforderu ngen an die Ausfallsi cherheit in normalen und widrigen Situation en zu erfüllen	autoscaling-group-elb-healthcheck-er forderlich	Die Elastic Load Balancer (ELB) - Zustandsprüfungen für Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling Scaling-G ruppen unterstützen die Aufrechterhaltung einer angemesse nen Kapazität und Verfügbarkeit. Der Load Balancer sendet regelmäßig Pings, versucht Verbindun gen herzustellen oder sendet Anfragen, um den Zustand der EC2 Amazon-Instances in einer Gruppe mit auto-scal ing zu testen. Wenn eine Instance nicht zurückmeldet, wird der Traffic an eine neue EC2 Amazon-In stance gesendet.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.PT-5	Mechanismen (z. B. Failsafe, Load Balancing, Hot-Swap) werden implement iert, um die Anforderu ngen an die Ausfallsi cherheit in normalen und widrigen Situation en zu erfüllen	db-instance-backup-enabled	Die Sicherung sfunktion von Amazon RDS erstellt Sicherung en Ihrer Datenbank en und Transakti onsprotokolle. Amazon RDS erstellt einen Snapshot für das Speichervolume Ihrer DB-Instance, sodass die gesamte DB-Instance gesichert wird. Sie können im System spezifische Aufbewahrungsfrist en festlegen, um Ihre Ausfallsicherheits anforderungen zu erfüllen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.PT-5	Mechanismen (z. B. Failsafe, Load Balancing, Hot-Swap) werden implementiert, um die Anforderungen an die Widerstandsfähigkeit in normalen und widrigen Situationen zu erfüllen	dynamodb-autoscaling-enabled	Amazon DynamoDB Auto Scaling verwendet den AWS Application Auto Scaling-Service, um die bereitgestellte Durchsatzkapazität so anzupassen, dass sie automatisch auf tatsächliche Verkehrsmuster reagiert. Auf diese Weise kann eine Tabelle oder ein globaler sekundärer Index die bereitgestellte Lese-/Schreibkapazität erhöhen, um plötzliche Erhöhungen des Datenverkehrs ohne Drosselung zu bewältigen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.PT-5	Mechanismen (z. B. Failsafe, Load Balancing, Hot-Swap) werden implement iert, um die Anforderu ngen an die Ausfallsi cherheit in normalen und ungünstigen Situationen zu erfüllen	dynamodb-pitr-enab led	Aktivieren Sie diese Regel, um zu überprüfen, ob die Informationen gesichert wurden. Es verwaltet auch die Backups, indem es sicherstellt, dass die point-in-time Wiederherstellung in Amazon DynamoDB aktiviert ist. Bei der Wiederherstellung werden fortlaufende Backups Ihrer Tabelle für die letzten 35 Tage gespeichert.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.PT-5	Mechanismen (z. B. Failsafe, Load Balancing, Hot-Swap) werden implement iert, um die Anforderu ngen an die Ausfallsi cherheit in normalen und widrigen Situation en zu erfüllen	elasticache-redis-cluster-automatic-Backup-Check	Wenn automatische Backups aktiviert sind, ElastiCache erstellt Amazon täglich ein Backup des Clusters. Die Sicherung kann für eine von Ihrer Organisation festgelegte Anzahl von Tagen aufbewahrt werden. Automatische Backups schützen vor Datenverlust. Bei einem Ausfall können Sie einen neuen Cluster erstellen, der Ihre Daten aus dem aktuellen Backup wiederherstellt.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.PT-5	Mechanismen (z. B. Failsafe, Load Balancing, Hot-Swap) werden implementiert, um die Anforderungen an die Ausfallsicherheit in normalen und widrigen Situationen zu erfüllen	elb-deletion-protection-enabled	Diese Regel sorgt dafür, dass der Löschschutz für Elastic Load Balancing aktiviert ist. Verwenden Sie diese Funktion, um zu verhindern, dass Ihr Load Balancer versehentlich oder böswillig gelöscht wird, was zum Verlust der Verfügbarkeit Ihrer Anwendungen führen kann.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.PT-5	Mechanismen (z. B. Failsafe, Load Balancing, Hot-Swap) werden implementiert, um die Anforderungen an die Widerstandsfähigkeit in normalen und widrigen Situationen zu erfüllen	rds-multi-az-support	Die Multi-AZ-Unterstützung in Amazon Relational Database Service (Amazon RDS) bietet eine verbesserte Verfügbarkeit und Beständigkeit von Datenbank-Instances. Wenn Sie eine Multi-AZ-Datenbank-Instance bereitstellen, erstellt Amazon RDS automatisch eine primäre Datenbank-Instance und repliziert die Daten synchron auf eine Standby-Instance in einer anderen Availability Zone. Jede Availability Zone läuft auf einer eigenen, physisch getrennten, unabhängigen Infrastruktur und ist auf eine hohe Verfügbarkeit ausgelegt. Im Falle eines Infrastrukturausfalls führt Amazon RDS einen automatis

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			chen Failover zum Standby-Modus durch, sodass Sie den Datenbankbetrieb wieder aufnehmen können, sobald der Failover abgeschlo ssen ist.
PR.PT-5	Mechanismen (z. B. Failsafe, Load Balancing, Hot-Swap) werden implementiert, um die Anforderungen an die Widerstandsfähigke it in normalen und widrigen Situationen zu erfüllen	s3- bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) unterstützt die Aufrechterhaltung einer angemesse nen Kapazität und Verfügbarkeit. CRR ermöglicht das automatische, asynchrone Kopieren von Objekten in Amazon S3 Buckets, um die Datenverf ügbarkeit sicherzus tellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.PT-5	Mechanismen (z. B. Failsafe, Load Balancing, Hot-Swap) werden implement iert, um die Anforderu ngen an die Ausfallsi cherheit in normalen und widrigen Situation en zu erfüllen	s3- bucket-versioning-enabled	Die Versionsv erwaltung von Amazon Simple Storage Service (Amazon S3)-Bucke ts hilft dabei, mehrere Varianten eines Objekts im selben Amazon-S3-Bucket zu speichern. Verwenden Sie die Versionsv erwaltung, um sämtliche Versionen aller Objekte in Ihrem Amazon-S3-Bucket zu speichern , abzurufen oder wiederherzustellen . Mit der Versionsv erwaltung können Sie Versionen sowohl nach unbeabsic htigten Benutzera ktionen als auch nach Anwendungsfehlern problemlos wiederher stellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.PT-5	Mechanismen (z. B. Failsafe, Load Balancing, Hot-Swap) werden implement iert, um die Anforderu ngen an die Ausfallsi cherheit in normalen und widrigen Situation en zu erfüllen	vpc-vpn-2-tunnels-up	Redundante Site-to-Site VPN-Tunne l können implement iert werden, um die Anforderungen an die Ausfallsicherheit zu erfüllen. Es verwendet zwei Tunnel, um die Konnektivität sicherzustellen, falls eine der Site-to-Site VPN-Verbindungen nicht verfügbar ist. Um sich vor einem Verbindungsverlust zu schützen, können Sie für den Fall, dass Ihr Kunden-Gateway nicht verfügbar ist, eine zweite Site-to-S ite VPN-Verbindung zu Ihrer Amazon Virtual Private Cloud (Amazon VPC) und Ihrem Virtual Private Gateway einrichten, indem Sie ein zweites Kunden-Gateway verwenden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
RC.RP-1	Der Wiederherstellungsplan wird während oder nach einem Cybersicherheitsvorfall ausgeführt	dynamodb-in-backup-plan	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon DynamoDB-Tabellen Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
RC.RP-1	Der Wiederherstellungsplan wird während oder nach einem Cybersicherheitsvorfall ausgeführt	ebs-in-backup-plan	Stellen Sie zur Unterstützung der Datensicherungsprozesse sicher, dass Ihre Amazon Elastic Block Store (Amazon EBS) -Volumes Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihre Backup-Verwaltung und ermöglicht es Ihnen, Ihre geschäftlichen und behördlichen Anforderungen bezüglich Backups zu erfüllen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
RC.RP-1	Der Wiederherstellungsplan wird während oder nach einem Cybersicherheitsvorfall ausgeführt	efs-in-backup-plan	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon Elastic File System (Amazon EFS) -Dateisysteme Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
RC.RP-1	Der Wiederherstellungsplan wird während oder nach einem Cybersicherheitsvorfall ausgeführt	elb-cross-zone-load-Balancing aktiviert	Aktivieren Sie zonenübergreifendes Load Balancing für Ihre Elastic Load Balancer (ELBs), um eine angemessene Kapazität und Verfügbarkeit aufrechtzuerhalten. Zonenübergreifendes Load Balancing reduziert die Notwendigkeit, die gleiche Anzahl von Instances in jeder aktivierten Availability Zone aufrechtzuerhalten. Es verbessert auch die Fähigkeit Ihrer Anwendung, den Verlust einer oder mehrerer Instances zu bewältigen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
RC.RP-1	Der Wiederherstellungsplan wird während oder nach einem Cybersicherheitsvorfall ausgeführt	rds-instance-deletion-protection-aktiviert	Stellen Sie sicher, dass Amazon Relational Database Service (Amazon RDS)-Instances den Löschschutz aktiviert haben. Verwenden Sie den Löschschutz, um zu verhindern, dass Ihre Amazon-RDS-Instances versehentlich oder böswillig gelöscht werden, was zum Verlust der Verfügbarkeit Ihrer Anwendungen führen kann.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
RC.RP-1	Der Wiederherstellungsplan wird während oder nach einem Cybersicherheitsvorfall ausgeführt	rds-in-backup-plan	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon Relational Database Service (Amazon RDS) -Instances Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
RC.RP-1	Der Wiederherstellungsplan wird während oder nach einem Cybersicherheitsvorfall ausgeführt	redshift-backup-enabled	Stellen Sie zur Unterstützung der Datensicherungsprozesse sicher, dass Ihre Amazon-Redshift-Cluster über automatisierte Snapshots verfügen. Wenn automatisierte Snapshots für einen Cluster aktiviert sind, erstellt Redshift in regelmäßigen Abständen Snapshots dieses Clusters. Standardmäßig erstellt Redshift alle acht Stunden oder alle 5 GB einen Snapshot für jeden Knoten mit Datenänderungen oder je nachdem, was zuerst eintritt.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
RC.RP-1	Der Wiederherstellungsplan wird während oder nach einem Cybersicherheitsvorfall ausgeführt	db-instance-backup-enabled	Die Sicherungsfunktion von Amazon RDS erstellt Sicherungen Ihrer Datenbanken und Transaktionsprotokolle. Amazon RDS erstellt einen Snapshot für das Speichervolume Ihrer DB-Instance, sodass die gesamte DB-Instance gesichert wird. Sie können im System spezifische Aufbewahrungsfristen festlegen, um Ihre Ausfallsicherheitsanforderungen zu erfüllen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
RC.RP-1	Der Wiederherstellungsplan wird während oder nach einem Cybersicherheitsvorfall ausgeführt	dynamodb-autoscaling-enabled	Amazon DynamoDB Auto Scaling verwendet den AWS Application Auto Scaling-Service, um die bereitgestellte Durchsatzkapazität so anzupassen, dass sie automatisch auf tatsächliche Verkehrsmuster reagiert. Auf diese Weise kann eine Tabelle oder ein globaler sekundärer Index die bereitgestellte Lese-/Schreibkapazität erhöhen, um plötzliche Erhöhungen des Datenverkehrs ohne Drosselung zu bewältigen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
RC.RP-1	Der Wiederherstellungsplan wird während oder nach einem Cybersicherheitsvorfall ausgeführt	dynamodb-pitr-enabled	Aktivieren Sie diese Regel, um zu überprüfen, ob die Informationen gesichert wurden. Es verwaltet auch die Backups, indem es sicherstellt, dass die point-in-time Wiederherstellung in Amazon DynamoDB aktiviert ist. Bei der Wiederherstellung werden fortlaufende Backups Ihrer Tabelle für die letzten 35 Tage gespeichert.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
RC.RP-1	Der Wiederherstellungsplan wird während oder nach einem Cybersicherheitsvorfall ausgeführt	elasticache-redis-cluster-automatic-Backup-Prüfung	Wenn automatische Backups aktiviert sind, ElastiCache erstellt Amazon täglich ein Backup des Clusters. Die Sicherung kann für eine von Ihrer Organisation festgelegte Anzahl von Tagen aufbewahrt werden. Automatische Backups schützen vor Datenverlust. Bei einem Ausfall können Sie einen neuen Cluster erstellen, der Ihre Daten aus dem aktuellen Backup wiederherstellt.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
RC.RP-1	Der Wiederherstellungsplan wird während oder nach einem Cybersicherheitsvorfall ausgeführt	elb-deletion-protection-enabled	Diese Regel sorgt dafür, dass der Löschschutz für Elastic Load Balancing aktiviert ist. Verwenden Sie diese Funktion, um zu verhindern, dass Ihr Load Balancer versehentlich oder böswillig gelöscht wird, was zum Verlust der Verfügbarkeit Ihrer Anwendungen führen kann.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
RC.RP-1	Der Wiederherstellungsplan wird während oder nach einem Cybersicherheitsvorfall ausgeführt	rds-multi-az-support	Die Multi-AZ-Unterstützung in Amazon Relational Database Service (Amazon RDS) bietet eine verbesserte Verfügbarkeit und Beständigkeit von Datenbank-Instances. Wenn Sie eine Multi-AZ-Datenbank-Instance bereitstellen, erstellt Amazon RDS automatisch eine primäre Datenbank-Instance und repliziert die Daten synchron auf eine Standby-Instance in einer anderen Availability Zone. Jede Availability Zone läuft auf einer eigenen, physisch getrennten, unabhängigen Infrastruktur und ist auf eine hohe Verfügbarkeit ausgelegt. Im Falle eines Infrastrukturausfalls führt Amazon RDS einen automatis

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			chen Failover zum Standby-Modus durch, sodass Sie den Datenbankbetrieb wieder aufnehmen können, sobald der Failover abgeschlo ssen ist.
RC.RP-1	Der Wiederher stellungsplan wird während oder nach einem Cybersicherheitsvo rfall ausgeführt	s-3 bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) unterstützt die Aufrechterhaltung einer angemesse nen Kapazität und Verfügbarkeit. CRR ermöglicht das automatische, asynchrone Kopieren von Objekten in Amazon S3 Buckets, um die Datenverf ügbarkeit sicherzus tellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
RC.RP-1	Der Wiederherstellungsplan wird während oder nach einem Cybersicherheitsvorfall ausgeführt	s-3 bucket-versioning-enabled	Die Versionsverwaltung von Amazon Simple Storage Service (Amazon S3)-Buckets hilft dabei, mehrere Varianten eines Objekts im selben Amazon-S3-Bucket zu speichern. Verwenden Sie die Versionsverwaltung, um sämtliche Versionen aller Objekte in Ihrem Amazon-S3-Bucket zu speichern, abzurufen oder wiederherzustellen. Mit der Versionsverwaltung können Sie Versionen sowohl nach unbeabsichtigten Benutzeraktionen als auch nach Anwendungsfehlern problemlos wiederherstellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
RC.RP-1	Der Wiederherstellungsplan wird während oder nach einem Cybersicherheitsvorfall ausgeführt	vpc-vpn-2-tunnels-up	Redundante Site-to-Site VPN-Tunnel können implementiert werden, um die Anforderungen an die Ausfallsicherheit zu erfüllen. Es verwendet zwei Tunnel, um die Konnektivität sicherzustellen, falls eine der Site-to-Site VPN-Verbindungen nicht verfügbar ist. Um sich vor einem Verbindungsverlust zu schützen, können Sie für den Fall, dass Ihr Kunden-Gateway nicht verfügbar ist, eine zweite Site-to-Site VPN-Verbindung zu Ihrer Amazon Virtual Private Cloud (Amazon VPC) und Ihrem Virtual Private Gateway einrichten, indem Sie ein zweites Kunden-Gateway verwenden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
RS.AN-2	Die Auswirkungen des Vorfalls sind bekannt	guardduty-non-archived-findings	Amazon GuardDuty hilft Ihnen dabei, die Auswirkungen eines Vorfalls zu verstehen, indem es die Ergebnisse nach Schweregrad klassifiziert: niedrig, mittel und hoch. Diese Klassifizierungen können Sie zur Festlegung von entsprechenden Strategien und Prioritäten zur Behebung solcher Vorfälle verwenden. Mit dieser Regel können Sie optional daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7) und daysHighSev (Config Default: 1) für nicht archivierte Ergebnisse festlegen, wie es die Richtlinien Ihrer Organisation erfordern.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
RS.MI-3	Neu erkannte Schwachstellen werden gemildert oder als akzeptierte Risiken dokumentiert	guardduty-non-archived-findings	Amazon GuardDuty hilft Ihnen dabei, die Auswirkungen eines Vorfalls zu verstehen, indem es die Ergebnisse nach Schweregrad klassifiziert: niedrig, mittel und hoch. Diese Klassifizierungen können Sie zur Festlegung von entsprechenden Strategien und Prioritäten zur Behebung solcher Vorfälle verwenden. Mit dieser Regel können Sie optional daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7) und daysHighSev (Config Default: 1) für nicht archivierte Ergebnisse festlegen, wie es die Richtlinien Ihrer Organisation erfordern.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
RS.RP-1	Reaktionsplan wird während oder nach einem Vorfall ausgeführt	aurora-resources-protected-by-Backup-Plan	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon Aurora Aurora-Ressourcen Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
RS.RP-1	Reaktionsplan wird während oder nach einem Vorfall ausgeführt	backup-plan-min-frequency-and-min-retention-check	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihr AWS Backup-Plan auf eine Mindestfrequenz und Aufbewahrung festgelegt ist. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen. Mit dieser Regel können Sie die Parameter requiredFrequencyValue (Config default: 1), requiredRetentionDays (Config default: 35) und requiredFrequencyUnit

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			(Config default: days) festlegen. Der tatsächliche Wert muss den Anforderungen Ihrer Organisation entsprechen.
RS.RP-1	Reaktionsplan wird während oder nach einem Vorfall ausgeführt	backup-recovery-point-encrypted	Stellen Sie sicher, dass die Verschlüsselung für Ihre AWS Backup-Wiederherstellungspunkte aktiviert ist. Da sensible Daten auch im Ruhezustand vorhanden sein können, sollten Sie die Verschlüsselung im Ruhezustand aktivieren, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
RS.RP-1	Reaktionsplan wird während oder nach einem Vorfall ausgeführt	backup-recovery-point-manual-Löschen-deaktiviert	Stellen Sie sicher, dass Ihren AWS Backup-Wiederherstellungspunkten eine ressourcenbasierte Richtlinie zugeordnet ist, die das Löschen von Wiederherstellungspunkten verhindert. Die Verwendung einer ressourcenbasierten Richtlinie zur Verhinderung des Löschens von Wiederherstellungspunkten kann dazu beitragen, ein versehentliches oder absichtliches Löschen zu unterbinden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
RS.RP-1	Reaktionsplan wird während oder nach einem Vorfall ausgeführt	db-instance-backup-enabled	Die Sicherungsfunktion von Amazon RDS erstellt Sicherungen Ihrer Datenbanken und Transaktionsprotokolle. Amazon RDS erstellt einen Snapshot für das Speichervolume Ihrer DB-Instance, sodass die gesamte DB-Instance gesichert wird. Sie können im System spezifische Aufbewahrungsfristen festlegen, um Ihre Ausfallsicherheitsanforderungen zu erfüllen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
RS.RP-1	Reaktionsplan wird während oder nach einem Vorfall ausgeführt	dynamodb-autoscaling-enabled	Amazon DynamoDB Auto Scaling verwendet den AWS Application Auto Scaling-Service, um die bereitgestellte Durchsatzkapazität so anzupassen, dass sie automatisch auf tatsächliche Verkehrsmuster reagiert. Auf diese Weise kann eine Tabelle oder ein globaler sekundärer Index die bereitgestellte Lese-/Schreibkapazität erhöhen, um plötzliche Erhöhungen des Datenverkehrs ohne Drosselung zu bewältigen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
RS.RP-1	Reaktionsplan wird während oder nach einem Vorfall ausgeführt	dynamodb-in-backup-plan	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon DynamoDB-Tabellen Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
RS.RP-1	Reaktionsplan wird während oder nach einem Vorfall ausgeführt	dynamodb-pitr-enabled	Aktivieren Sie diese Regel, um zu überprüfen, ob die Informationen gesichert wurden. Es verwaltet auch die Backups, indem es sicherstellt, dass die point-in-time Wiederherstellung in Amazon DynamoDB aktiviert ist. Bei der Wiederherstellung werden fortlaufende Backups Ihrer Tabelle für die letzten 35 Tage gespeichert.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
RS.RP-1	Reaktionsplan wird während oder nach einem Vorfall ausgeführt	ebs-in-backup-plan	Stellen Sie zur Unterstützung der Datensicherungspro zesse sicher, dass Ihre Amazon Elastic Block Store (Amazon EBS) -Volumes Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwaltet er Backup-Service mit einer richtlini enbasierten Backup-Lösung. Diese Lösung vereinfacht Ihre Backup-Verwaltung und ermöglicht es Ihnen, Ihre geschäftl ichen und behördlic hen Anforderungen bezüglich Backups zu erfüllen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
RS.RP-1	Reaktionsplan wird während oder nach einem Vorfall ausgeführt	ec2--Plan resources-protected-by-backup	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon Elastic Compute Cloud (Amazon EC2) -Ressourcen Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
RS.RP-1	Reaktionsplan wird während oder nach einem Vorfall ausgeführt	efs-in-backup-plan	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon Elastic File System (Amazon EFS) -Dateisysteme Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
RS.RP-1	Reaktionsplan wird während oder nach einem Vorfall ausgeführt	elasticache-redis-cluster-automatic-Backup-Check	Wenn automatische Backups aktiviert sind, ElastiCache erstellt Amazon täglich ein Backup des Clusters. Die Sicherung kann für eine von Ihrer Organisation festgelegte Anzahl von Tagen aufbewahrt werden. Automatische Backups schützen vor Datenverlust. Bei einem Ausfall können Sie einen neuen Cluster erstellen, der Ihre Daten aus dem aktuellen Backup wiederherstellt.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
RS.RP-1	Reaktionsplan wird während oder nach einem Vorfall ausgeführt	elb-cross-zone-load-Balancing aktiviert	Aktivieren Sie zonenübergreifendes Load Balancing für Ihre Elastic Load Balancer (ELBs), um eine angemessene Kapazität und Verfügbarkeit aufrechtzuerhalten. Zonenübergreifendes Load Balancing reduziert die Notwendigkeit, die gleiche Anzahl von Instances in jeder aktivierten Availability Zone aufrechtzuerhalten. Es verbessert auch die Fähigkeit Ihrer Anwendung, den Verlust einer oder mehrerer Instances zu bewältigen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
RS.RP-1	Reaktionsplan wird während oder nach einem Vorfall ausgeführt	elb-deletion-protection-enabled	Diese Regel sorgt dafür, dass der Löschschutz für Elastic Load Balancing aktiviert ist. Verwenden Sie diese Funktion, um zu verhindern, dass Ihr Load Balancer versehentlich oder böswillig gelöscht wird, was zum Verlust der Verfügbarkeit Ihrer Anwendungen führen kann.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
RS.RP-1	Reaktionsplan wird während oder nach einem Vorfall ausgeführt	rds-in-backup-plan	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon Relational Database Service (Amazon RDS) -Instances Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
RS.RP-1	Reaktionsplan wird während oder nach einem Vorfall ausgeführt	rds-multi-az-support	Die Multi-AZ-Unterstützung in Amazon Relational Database Service (Amazon RDS) bietet eine verbesserte Verfügbarkeit und Beständigkeit von Datenbank-Instances. Wenn Sie eine Multi-AZ-Datenbank-Instance bereitstellen, erstellt Amazon RDS automatisch eine primäre Datenbank-Instance und repliziert die Daten synchron auf eine Standby-Instance in einer anderen Availability Zone. Jede Availability Zone läuft auf einer eigenen, physisch getrennten, unabhängigen Infrastruktur und ist auf eine hohe Verfügbarkeit ausgelegt. Im Falle eines Infrastrukturausfalls führt Amazon RDS einen automatis

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			chen Failover zum Standby-Modus durch, sodass Sie den Datenbankbetrieb wieder aufnehmen können, sobald der Failover abgeschlo ssen ist.
RS.RP-1	Reaktionsplan wird während oder nach einem Vorfall ausgeführt	redshift-backup-en abled	Stellen Sie zur Unterstützung der Datensicherungspro zesse sicher, dass Ihre Amazon-Re dshift-Cluster über automatisierte Snapshots verfügen. Wenn automatis ierte Snapshots für einen Cluster aktiviert sind, erstellt Redshift in regelmäßi gen Abständen Snapshots dieses Clusters. Standardm äßig erstellt Redshift alle acht Stunden oder alle 5 GB einen Snapshot für jeden Knoten mit Datenände rungen oder je nachdem, was zuerst eintritt.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
RS.RP-1	Reaktionsplan wird während oder nach einem Vorfall ausgeführt	s3- bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) unterstützt die Aufrechterhaltung einer angemessenen Kapazität und Verfügbarkeit. CRR ermöglicht das automatische, asynchrone Kopieren von Objekten in Amazon S3 Buckets, um die Datenverfügbarkeit sicherzustellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
RS.RP-1	Reaktionsplan wird während oder nach einem Vorfall ausgeführt	s-3 bucket-versioning-enabled	Die Versionsv erwaltung von Amazon Simple Storage Service (Amazon S3)-Bucke ts hilft dabei, mehrere Varianten eines Objekts im selben Amazon-S3-Bucket zu speichern. Verwenden Sie die Versionsv erwaltung, um sämtliche Versionen aller Objekte in Ihrem Amazon-S3-Bucket zu speichern , abzurufen oder wiederherzustellen . Mit der Versionsv erwaltung können Sie Versionen sowohl nach unbeabsic htigten Benutzera ktionen als auch nach Anwendungsfehlern problemlos wiederher stellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
RS.RP-1	Reaktionsplan wird während oder nach einem Vorfall ausgeführt	vpc-vpn-2-tunnels-up	Redundante Site-to-Site VPN-Tunnel können implementiert werden, um die Anforderungen an die Ausfallsicherheit zu erfüllen. Es verwendet zwei Tunnel, um die Konnektivität sicherzustellen, falls eine der Site-to-Site VPN-Verbindungen nicht verfügbar ist. Um sich vor einem Verbindungsverlust zu schützen, können Sie für den Fall, dass Ihr Kunden-Gateway nicht verfügbar ist, eine zweite Site-to-Site VPN-Verbindung zu Ihrer Amazon Virtual Private Cloud (Amazon VPC) und Ihrem Virtual Private Gateway einrichten, indem Sie ein zweites Kunden-Gateway verwenden.

Vorlage

Die Vorlage ist verfügbar unter GitHub: Operational Best Practices for NIST CSF.

Bewährte Betriebspraktiken für NIST Privacy Framework v1.0

Konformitätspakete bieten ein allgemeines Compliance-Framework, das es Ihnen ermöglicht, mithilfe verwalteter oder benutzerdefinierter AWS Config Regeln und Abhilfemaßnahmen Kontrollen zur Sicherheits-, Betriebs- oder Kostenoptimierung durchzuführen. AWS Config Conformance Packs dienen als Beispielvorlagen nicht dazu, die vollständige Einhaltung eines bestimmten Governance- oder Compliance-Standards sicherzustellen. Sie sind dafür verantwortlich, selbst zu beurteilen, ob Ihre Nutzung der Services den geltenden gesetzlichen und behördlichen Anforderungen entspricht.

Im Folgenden finden Sie ein Beispiel für eine Zuordnung zwischen NIST Privacy Framework und von AWS verwalteten Konfigurationsregeln. Jede AWS Config Regel gilt für eine bestimmte AWS Ressource und bezieht sich auf eine oder mehrere NIST Privacy Framework-Kontrollen. Ein NIST Privacy Framework-Steuerelement kann sich auf mehrere AWS Config Regeln beziehen. In der folgenden Tabelle finden Sie weitere Informationen und Anleitungen zu diesen Zuordnungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CT.DM-P7	Mechanismen für die Übermittlung von Verarbeitungserlaubnissen und zugehörigen Datenwerten mit Datenelementen sind eingerichtet und in Kraft.	alb-http-to-https-Umleitungsprüfung	Um Daten während der Übertragung zu schützen, stellen Sie sicher, dass Ihr Application Load Balancer unverschlüsselte HTTP-Anfragen automatisch an HTTPS umleitet. Da sensible Daten vorhanden sein können, sollten Sie die Verschlüsselung bei der Übertragung aktivieren, um diese Daten zu schützen.
CT.DM-P7	Mechanismen für die Übermittlung von Verarbeit	api-gw-ssl-enabled	Stellen Sie sicher, dass die REST-API-Stufen von Amazon

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	ungserlaubnissen und zugehörigen Datenwerten mit Datenelementen sind eingerichtet und in Kraft.		API Gateway mit SSL-Zertifikaten konfiguriert sind, damit Backend-Systeme überprüfen können, ob Anforderungen von API Gateway stammen.
CT.DM-P7	Mechanismen für die Übermittlung von Verarbeitungserlaubnissen und zugehörigen Datenwerten mit Datenelementen sind eingerichtet und in Kraft.	elasticsearch-node-to-node-Verschlüsselungsprüfung	Stellen Sie sicher, dass die node-to-node Verschlüsselung für Amazon OpenSearch Service aktiviert ist. Node-to-nodeVerschlüsselung ermöglicht die TLS 1.2-Verschlüsselung für die gesamte Kommunikation innerhalb der Amazon Virtual Private Cloud (Amazon VPC). Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CT.DM-P7	Mechanismen für die Übermittlung von Verarbeitungserlaubnissen und zugehörigen Datenwerten mit Datenelementen sind eingerichtet und in Kraft.	opensearch-node-to-node-Verschlüsselungsprüfung	Stellen Sie sicher, dass die node-to-node Verschlüsselung für Amazon OpenSearch Service aktiviert ist. Node-to-nodeVerschlüsselung ermöglicht die TLS 1.2-Verschlüsselung für die gesamte Kommunikation innerhalb der Amazon Virtual Private Cloud (Amazon VPC). Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CT.DM-P7	Mechanismen für die Übermittlung von Verarbeitungserlaubnissen und zugehörigen Datenwerten mit Datenelementen sind eingerichtet und in Kraft.	elb-acm-certificate-required	Zum Schutz von eventuell vorhandenen sensiblen Daten sowie von Daten während der Übertragung muss die Verschlüsselung für Ihr Elastic Load Balancing aktiviert sein. Verwenden Sie AWS Certificate Manager, um öffentliche und private SSL/TLS-Zertifikate mit AWS Diensten und internen Ressourcen zu verwalten, bereitzustellen und bereitzustellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CT.DM-P7	Mechanismen für die Übermittlung von Verarbeitungserlaubnissen und zugehörigen Datenwerten mit Datenelementen sind eingerichtet und in Kraft.	elbv2- acm-certificate-required	Zum Schutz von eventuell vorhandenen sensiblen Daten sowie von Daten während der Übertragung muss die Verschlüsselung für Ihr Elastic Load Balancing aktiviert sein. Verwenden Sie AWS Certificate Manager, um öffentliche und private SSL/TLS-Zertifikate mit AWS Diensten und internen Ressourcen zu verwalten, bereitzustellen und bereitzustellen.
CT.DM-P7	Mechanismen für die Übermittlung von Verarbeitungserlaubnissen und zugehörigen Datenwerten mit Datenelementen sind eingerichtet und in Kraft.	elb-tls-https-listeners-nur	Stellen Sie sicher, dass Ihre Elastic Load Balancer (ELBs) mit SSL- oder HTTPS-Listenern konfiguriert sind. Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CT.DM-P7	Mechanismen für die Übermittlung von Verarbeitungserlaubnissen und zugehörigen Datenwerten mit Datenelementen sind eingerichtet und in Kraft.	redshift-require-tls-ssl	Stellen Sie sicher, dass Ihre Amazon-Redshift-Cluster eine TLS/SSL-Verschlüsselung erfordern, um eine Verbindung zu SQL-Clients herzustellen. Da sensible Daten vorhanden sein können, sollten Sie die Verschlüsselung bei der Übertragung aktivieren, um diese Daten zu schützen.
CT.DM-P7	Mechanismen für die Übermittlung von Verarbeitungserlaubnissen und zugehörigen Datenwerten mit Datenelementen sind eingerichtet und in Kraft.	s-3 bucket-ssl-requests-only	Um Daten während der Übertragung zu schützen, stellen Sie sicher, dass Ihre Amazon Simple Storage Service (Amazon S3)-Buckets Anfragen zur Verwendung von Secure Socket Layer (SSL)-Buckets erfordern. Da sensible Daten vorhanden sein können, sollten Sie die Verschlüsselung bei der Übertragung aktivieren, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CT.DM-P8	Audit-/Protokollaufzeichnungen werden in Übereinstimmung mit den Richtlinien und unter Berücksichtigung des Grundsatzes der Datenminimierung festgelegt, dokumentiert, umgesetzt und überprüft.	audit-log-policy-exists(Prozessüberprüfung)	Richten Sie eine Richtlinie zur Verwaltung von Prüfprotokollen ein, in der die Protokollierungsanforderungen Ihres Unternehmens definiert sind, und pflegen Sie diese Richtlinie. Dies beinhaltet, ist aber nicht beschränkt auf die Überprüfung und Aufbewahrung von Auditprotokollen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CT.DM-P8	Audit-/Protokollaufzeichnungen werden in Übereinstimmung mit den Richtlinien und unter Berücksichtigung des Grundsatzes der Datenminimierung festgelegt, dokumentiert, umgesetzt und überprüft.	autoscaling-group-elb-healthcheck-erforderlich	Die Elastic Load Balancer (ELB) - Zustandsprüfungen für Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling Scaling-Gruppen unterstützen die Aufrechterhaltung einer angemessenen Kapazität und Verfügbarkeit. Der Load Balancer sendet regelmäßig Pings, versucht Verbindungen herzustellen oder sendet Anfragen, um den Zustand der EC2 Amazon-Instances in einer Gruppe mit auto-scaling zu testen. Wenn eine Instance nicht zurückmeldet, wird der Traffic an eine neue EC2 Amazon-Instance gesendet.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CT.DM-P8	Audit-/Protokollaufzeichnungen werden in Übereinstimmung mit den Richtlinien und unter Berücksichtigung des Grundsatzes der Datenminimierung festgelegt, dokumentiert, umgesetzt und überprüft.	api-gw-execution-logging-aktiviert	Die API-Gateway-Protokollierung zeigt detaillierte Ansichten der Benutzer, die auf die API zugegriffen haben, und wie diese Benutzer auf die API zugegriffen haben. Diese Insights ermöglichen die Einsicht in Benutzeraktivitäten.
CT.DM-P8	Audit-/Protokollaufzeichnungen werden in Übereinstimmung mit den Richtlinien und unter Berücksichtigung des Grundsatzes der Datenminimierung festgelegt, dokumentiert, umgesetzt und überprüft.	cloud-trail-cloud-watch-logs-aktiviert	Verwenden Sie Amazon CloudWatch , um Protokollereignisaktivitäten zentral zu sammeln und zu verwalten. Die Aufnahme von AWS CloudTrail Daten liefert Einzelheiten zu den API-Aufrufaktivitäten in Ihrem AWS-Konto.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CT.DM-P8	Audit-/Protokollaufzeichnungen werden in Übereinstimmung mit den Richtlinien und unter Berücksichtigung des Grundsatzes der Datenminimierung festgelegt, dokumentiert, umgesetzt und überprüft.	cloudtrail-enabled	AWS CloudTrail kann bei der Nichtabstreitbarkeit helfen, indem Aktionen und API-Aufrufe der AWS Management Console aufgezeichnet werden. Sie können die Benutzer und die Benutzer AWS-Konten , die einen AWS Dienst aufgerufen haben, die Quell-IP-Adresse, über die die Aufrufe generiert wurden, und den Zeitpunkt der Anrufe identifizieren. Einzelheiten zu den erfassten Daten finden Sie unter Inhalt des AWS CloudTrail Datensatzes.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CT.DM-P8	Audit-/Protokollaufzeichnungen werden in Übereinstimmung mit den Richtlinien und unter Berücksichtigung des Grundsatzes der Datenminimierung festgelegt, dokumentiert, umgesetzt und überprüft.	cloudtrail-s3-dataevents-enabled	Die Erfassung von Simple Storage Service (Amazon S3)-Datenereignissen unterstützt die Erkennung von ungewöhnlichen Aktivitäten. Zu den Details gehören AWS-Konto Informationen über den Zugriff auf einen Amazon S3 S3-Bucket, die IP-Adresse und die Uhrzeit des Ereignisses.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CT.DM-P8	Audit-/Protokollaufzeichnungen werden in Übereinstimmung mit den Richtlinien und unter Berücksichtigung des Grundsatzes der Datenminimierung festgelegt, dokumentiert, umgesetzt und überprüft.	cloudwatch-alarm-action-check	Amazon CloudWatch alarmiert, wenn eine Metrik den Schwellenwert für eine bestimmte Anzahl von Bewertungszeiträumen überschreitet. Der Alarm führt eine oder mehrere Aktionen durch, die vom Wert der Metrik oder des Ausdrucks im Vergleich zu einem Schwellenwert in einer Reihe von Zeiträumen abhängt. Diese Regel erfordert einen Wert für alarmActionRequired (Config Default: True), insufficientDataAction Required (Config Default: True), okActionRequired (Config Default: False). Der tatsächliche Wert muss die Alarmaktionen für Ihre Umgebung widerspiegeln.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CT.DM-P8	Audit-/Protokollaufzeichnungen werden in Übereinstimmung mit den Richtlinien und unter Berücksichtigung des Grundsatzes der Datenminimierung festgelegt, dokumentiert, umgesetzt und überprüft.	cw-loggroup-retention-period-überprüfen	Stellen Sie sicher, dass die Ereignisprotokolldaten für Ihre Protokollgruppen über eine Mindestdauer aufbewahrt werden, um die Fehlerbehebung und forensische Untersuchungen zu unterstützen. Fehlende frühere Ereignisprotokolldaten erschweren die Rekonstruierung und Identifizierung potenziell schädlicher Ereignisse.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CT.DM-P8	Audit-/Protokollaufzeichnungen werden in Übereinstimmung mit den Richtlinien und unter Berücksichtigung des Grundsatzes der Datenminimierung festgelegt, dokumentiert, umgesetzt und überprüft.	dynamodb-throughput-limit-check	Aktivieren Sie diese Regel, um sicherzustellen, dass die bereitgestellte Durchsatzkapazität in Ihren Amazon-DynamoDB-Tabellen überprüft wird. Dies ist der Umfang der Lese- und Schreibaktivitäten, der von den jeweiligen Tabellen unterstützt werden kann. DynamoDB verwendet diese Informationen für das Reservieren ausreichender Systemressourcen, um Ihren Durchsatz anforderungen gerecht zu werden. Diese Regel generiert eine Warnung, wenn sich der Durchsatz dem Höchstlimit für ein Kundenkonto nähert. Mit dieser Regel können Sie optional die Parameter RCUThreshold Kontoprozentsatz

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			(Konfigurationsstandard: 80) und WCUThreshold Kontoprozentsatz (Konfigurationsstandard: 80) festlegen. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.
CT.DM-P8	Audit-/Protokollaufzeichnungen werden in Übereinstimmung mit den Richtlinien und unter Berücksichtigung des Grundsatzes der Datenminimierung festgelegt, dokumentiert, umgesetzt und überprüft.	ec2- instance-detailed-monitoring-enabled	Aktivieren Sie diese Regel, um die Amazon Elastic Compute Cloud (Amazon EC2) - Instance-Überwachung auf der EC2 Amazon-Konsole zu verbessern, in der Monitoring-Diagramme mit einem Zeitraum von 1 Minute für die Instance angezeigt werden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CT.DM-P8	Audit-/Protokollaufzeichnungen werden in Übereinstimmung mit den Richtlinien und unter Berücksichtigung des Grundsatzes der Datenminimierung festgelegt, dokumentiert, umgesetzt und überprüft.	elb-logging-enabled	Die Elastic-Load-Balancing-Aktivität ist ein zentraler Kommunikationspunkt innerhalb einer Umgebung. Stellen Sie sicher, dass die ELB-Protokollierung aktiviert ist. Die gesammelten Daten enthalten detaillierte Informationen zu Anfragen, die an den ELB gesendet wurden. Jedes Protokoll enthält Informationen wie die Zeit, zu der die Anforderung einging, die Client-IP-Adresse, Latenzen, Anforderungspfade und Serverantworten.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CT.DM-P8	Audit-/Protokollaufzeichnungen werden in Übereinstimmung mit den Richtlinien und unter Berücksichtigung des Grundsatzes der Datenminimierung festgelegt, dokumentiert, umgesetzt und überprüft.	cloudtrail-security-trail-enabled	Diese Regel trägt dazu bei, die Verwendung der AWS empfohlenen bewährten Sicherheitsmethoden für sicherzustellen AWS CloudTrail, indem geprüft wird, ob mehrere Einstellungen aktiviert sind. Dazu gehören die Verwendung von Protokollverschlüsselung, Protokollvalidierung und Aktivierung AWS CloudTrail in mehreren Regionen.
CT.DM-P8	Audit-/Protokollaufzeichnungen werden in Übereinstimmung mit den Richtlinien und unter Berücksichtigung des Grundsatzes der Datenminimierung festgelegt, dokumentiert, umgesetzt und überprüft.	redshift-audit-logging-enabled	Aktivieren Sie die Prüfungsprotokollierung, um Informationen über Verbindungen und Benutzeraktivitäten in Ihrem Amazon-Redshift-Cluster zu erfassen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CT.DM-P8	Audit-/Protokollaufzeichnungen werden in Übereinstimmung mit den Richtlinien und unter Berücksichtigung des Grundsatzes der Datenminimierung festgelegt, dokumentiert, umgesetzt und überprüft.	rds-logging-enabled	Um die Protokollierung und Überwachung in Ihrer Umgebung zu erleichtern, stellen Sie sicher, dass die Amazon Relational Database Service (Amazon RDS)-Protokollierung aktiviert ist. Mit der Amazon-RDS-Protokollierung können Sie Ereignisse wie Verbindungen, Verbindungsabbrüche, Abfragen oder abgefragte Tabellen erfassen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CT.DM-P8	Audit-/Protokollaufzeichnungen werden in Übereinstimmung mit den Richtlinien und unter Berücksichtigung des Grundsatzes der Datenminimierung festgelegt, dokumentiert, umgesetzt und überprüft.	rds-enhanced-monitoring-enabled	Aktivieren Sie Amazon Relational Database Service (Amazon RDS), um die Verfügbarkeit von Amazon RDS zu überwachen. Dies bietet einen detaillierten Einblick in den Zustand Ihrer Amazon-RDS-Datenbank-Instances. Wenn der Amazon-RDS-Speicher mehr als ein zugrunde liegendes physisches Gerät verwendet, erfasst Enhanced Monitoring die Daten für jedes Gerät. Wenn die Datenbank-Instance von Amazon RDS in einer Multi-AZ-Bereitstellung ausgeführt wird, werden außerdem die Daten für jedes Gerät auf dem sekundären Host sowie die Metriken des sekundären Hosts erfasst.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CT.DM-P8	Audit-/Protokollaufzeichnungen werden in Übereinstimmung mit den Richtlinien und unter Berücksichtigung des Grundsatzes der Datenminimierung festgelegt, dokumentiert, umgesetzt und überprüft.	s-3 bucket-logging-enabled	Die Amazon Simple Storage Service (Amazon S3)-Serverzugriffsprotokollierung bietet eine Methode zur Überwachung des Netzwerks im Hinblick auf potenzielle Cybersicherheitsereignisse. Die Ereignisse werden überwacht, indem detaillierte Aufzeichnungen über die Anfragen erfasst werden, die an einen Amazon-S3-Bucket gestellt wurden. Jeder Zugriffsprotokolleintrag enthält Details zu einer einzelnen Zugriffsanfrage. Zu den Details gehören Anforderer, Bucket-Name, Anforderungszeit, Anforderungsaktion, Antwortstatus und Fehlercode, falls relevant.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CT.DM-P8	Audit-/Protokollaufzeichnungen werden in Übereinstimmung mit den Richtlinien und unter Berücksichtigung des Grundsatzes der Datenminimierung festgelegt, dokumentiert, umgesetzt und überprüft.	securityhub-enabled	AWS Security Hub hilft bei der Überwachung von unbefugtem Personal, Verbindungen, Geräten und Software. AWS Security Hub aggregiert, organisiert und priorisiert die Sicherheitswarnungen oder Ergebnisse mehrerer Dienste. AWS Einige dieser Dienste sind Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer und AWS Firewall Manager sowie AWS Partnerlösungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CT.DM-P8	Audit-/Protokollaufzeichnungen werden in Übereinstimmung mit den Richtlinien und unter Berücksichtigung des Grundsatzes der Datenminimierung festgelegt, dokumentiert, umgesetzt und überprüft.	vpc-flow-logs-enabled	VPC-Flow-Protokolle erfassen detaillierte Informationsdatensätze über den IP-Datenverkehr, der zu und von Netzwerkschnittstellen in Ihrer Amazon Virtual Private Cloud (Amazon VPC) fließt. Standardmäßig enthalten Flow-Protokolldatensätze Werte für die verschiedenen Komponenten des IP-Flows, einschließlich Quelle, Ziel und Protokoll.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CT.DM-P8	Audit-/Protokollaufzeichnungen werden in Übereinstimmung mit den Richtlinien und unter Berücksichtigung des Grundsatzes der Datenminimierung festgelegt, dokumentiert, umgesetzt und überprüft.	wafv2-logging-enabled	Um Ihnen bei der Protokollierung und Überwachung in Ihrer Umgebung zu helfen, aktivieren Sie die AWS WAF (V2) -Protokollierung im regionalen und globalen Web. ACLs AWS Die WAF-Protokollierung bietet detaillierte Informationen über den Datenverkehr, der von Ihrer Web-ACL analysiert wird. In den Protokollen werden die Uhrzeit aufgezeichnet, zu der die AWS WAF die Anfrage von Ihrer AWS Ressource erhalten hat, Informationen über die Anfrage und eine Aktion für die Regel, der jede Anfrage entsprach.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CT.DM-P8	Audit-/Protokollaufzeichnungen werden in Übereinstimmung mit den Richtlinien und unter Berücksichtigung des Grundsatzes der Datenminimierung festgelegt, dokumentiert, umgesetzt und überprüft.	elasticsearch-logs-to-cloudwatch	Stellen Sie sicher, dass für Amazon OpenSearch Service-Domains Fehlerprotokolle aktiviert und zur Aufbewahrung und Beantwortung an Amazon CloudWatch Logs gestreamt werden. Domain-Fehlerprotokolle sind bei Sicherheits- und Zugriffsprüfungen sowie bei der Diagnose von Verfügbarkeitsproblemen nützlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CT.DM-P8	Audit-/Protokollaufzeichnungen werden in Übereinstimmung mit den Richtlinien und unter Berücksichtigung des Grundsatzes der Datenminimierung festgelegt, dokumentiert, umgesetzt und überprüft.	opensearch-logs-to-cloudwatch	Stellen Sie sicher, dass für Amazon OpenSearch Service-Domains Fehlerprotokolle aktiviert und zur Aufbewahrung und Beantwortung an Amazon CloudWatch Logs gestreamt werden. OpenSearch Service-Fehlerprotokolle können bei Sicherheits- und Zugriffsprüfungen helfen und bei der Diagnose von Verfügbarkeitsproblemen helfen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CT.DM-P8	Audit-/Protokollaufzeichnungen werden in Übereinstimmung mit den Richtlinien und unter Berücksichtigung des Grundsatzes der Datenminimierung festgelegt, dokumentiert, umgesetzt und überprüft.	guardduty-non-archived-findings	Amazon GuardDuty hilft Ihnen dabei, die Auswirkungen eines Vorfalls zu verstehen, indem es die Ergebnisse nach Schweregrad klassifiziert: niedrig, mittel und hoch. Diese Klassifizierungen können Sie zur Festlegung von entsprechenden Strategien und Prioritäten zur Behebung solcher Vorfälle verwenden. Mit dieser Regel können Sie optional daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7) und daysHighSev (Config Default: 1) für nicht archivierte Ergebnisse festlegen, wie es die Richtlinien Ihrer Organisation erfordern.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
CT.DM-P8	Audit-/Protokollaufzeichnungen werden in Übereinstimmung mit den Richtlinien und unter Berücksichtigung des Grundsatzes der Datenminimierung festgelegt, dokumentiert, umgesetzt und überprüft.	redshift-cluster-configuration-check	Um Daten im Ruhezustand zu schützen, muss die Verschlüsselung für Ihre Amazon-Redshift-Cluster aktiviert sein. Sie müssen auch sicherstellen, dass die erforderlichen Konfigurationen auf Amazon-Redshift-Clustern bereitgestellt werden. Die Prüfungsprotokollierung muss aktiviert sein, um Informationen zu Verbindungen und Benutzeraktivitäten in der Datenbank bereitzustellen. Diese Regel erfordert, dass ein Wert für clusterDbEncrypted (Config Default: TRUE) und LoggingEnabled (Config Default: TRUE) gesetzt ist. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
ID.DE-P2	Die am Datenverarbeitungs-Ökosystem beteiligten Parteien (z. B. Dienstleister, Kunden, Partner, Produkthersteller, Anwendungsentwickler) werden anhand eines Verfahrens zur Bewertung von Datenschutzrisiken identifiziert, priorisiert und bewertet.	annual-risk-assessment-performed(Prozessüberprüfung)	Führen Sie eine jährliche Risikobewertung für Ihre Organisation durch. Risikowertungen können dabei helfen, die Wahrscheinlichkeit und Auswirkungen identifizierter Risiken und/oder Schwachstellen für eine Organisation zu ermitteln.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.AC-P1	Identitäten und Berechtigungsnachweise werden für autorisierte Personen, Prozesse und Geräte ausgestellt, verwaltet, verifiziert, widerrufen und geprüft.	iam-user-group-membership-überprüfen	AWS Identity and Access Management (IAM) kann Ihnen helfen, Zugriffsberechtigungen und Autorisierungen einzuschränken, indem sichergestellt wird, dass Benutzer Mitglieder mindestens einer Gruppe sind. Wenn Benutzern mehr Berechtigungen eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und Aufgabentrennung verstoßen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.AC-P1	Identitäten und Berechtigungsnachweise werden für autorisierte Personen, Prozesse und Geräte ausgestellt, verwaltet, verifiziert, widerrufen und geprüft.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) kann Ihnen dabei helfen, die Prinzipien der geringsten Rechte und der Aufgabentrennung in Zugriffsberechtigungen und Autorisierungen zu integrieren und so zu verhindern, dass Richtlinien „Effect“: „Allow“ mit „Action“: „*“ anstelle von „Resource“: „*“ enthalten. Wenn Benutzern mehr Rechte eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und der Aufgabentrennung verstoßen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.AC-P1	Identitäten und Berechtigungsnachweise werden für autorisierte Personen, Prozesse und Geräte ausgestellt, verwaltet, verifiziert, widerrufen und geprüft.	access-keys-rotated	Die Anmeldeinformationen für autorisierte Geräte, Benutzer und Prozesse werden geprüft, indem sichergestellt wird, dass die IAM-Zugriffsschlüssel entsprechend den Vorgaben der Unternehmensrichtlinie rotiert werden. Das regelmäßige Ändern der Zugriffsschlüssel ist eine bewährte Sicherheitsmethode. Es verkürzt den Zeitraum, in dem ein Zugriffsschlüssel aktiv ist, und reduziert die Auswirkungen auf das Unternehmen, wenn die Schlüssel kompromittiert werden. Diese Regel erfordert einen Wert für die Zugriffsschlüssel-Rotation (Standard konfiguration: 90). Der tatsächliche Wert muss den Richtlini

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			en Ihrer Organisation entsprechen.
PR.AC-P1	Identitäten und Berechtigungsnachweise werden für autorisierte Personen, Prozesse und Geräte ausgestellt, verwaltet, verifiziert, widerrufen und geprüft.	iam-root-access-key-überprüfen	Der Zugriff auf Systeme und Ressourcen kann gesteuert werden, indem überprüft wird, ob der Root-Benutzer keine Zugriffsschlüssel mit seiner AWS Identity and Access Management (IAM) -Rolle verknüpft hat. Stellen Sie sicher, dass die Root-Zugriffsschlüssel gelöscht werden. Erstellen und verwenden Sie stattdessen rollenbasierte Funktionen, AWS-Konten um das Prinzip der geringsten Funktionalität zu berücksichtigen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.AC-P1	Identitäten und Berechtigungsnachweise werden für autorisierte Personen, Prozesse und Geräte ausgestellt, verwaltet, verifiziert, widerrufen und geprüft.	iam-password-policy	Die Identitäten und Anmeldeinformationen werden auf der Grundlage einer organisatorischen IAM-Passwortrichtlinie ausgestellt, verwaltet und verifiziert. Sie erfüllen oder übertreffen die Anforderungen von NIST SP 800-63 und dem Standard „Best Practices“ von AWS Foundational Security für die Passwortstärke. Mit dieser Regel können Sie optional RequireUppercaseCharacters (Wert für AWS grundlegende Sicherheitsbewährte Methoden: wahr), RequireLowercaseCharacters (Wert für bewährte Methoden für AWS grundlegende Sicherheit: wahr), RequireSymbols (Wert für bewährte Methoden für AWS grundlegende Sicherheit:

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			wahr), RequireNumbers (Wert für bewährte Methoden für AWS grundlegende Sicherheit: wahr), MinimumPasswordLength (Wert für bewährte Methoden für AWS grundlegende Sicherheit: 14), PasswordReusePrevention (Wert für bewährte Methoden für AWS grundlegende Sicherheit: 24) und MaxPasswordAge (Wert für bewährte Methoden für AWS grundlegende Sicherheit: 90) für Ihr IAM festlegen Kennwortrichtlinie. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.AC-P1	Identitäten und Berechtigungsnachweise werden für autorisierte Personen, Prozesse und Geräte ausgestellt, verwaltet, verifiziert, widerrufen und geprüft.	iam-user-unused-credentials-überprüfen	AWS Identity and Access Management (IAM) kann Ihnen bei Zugriffsberechtigungen und Autorisierungen helfen, indem es nach IAM-Passwörtern und Zugriffsschlüsseln sucht, die für einen bestimmten Zeitraum nicht verwendet wurden. Wenn ungenutzte Anmeldeinformationen identifiziert werden, müssen Sie sie deaktivieren und/oder entfernen, da dies gegen das Prinzip der geringsten Berechtigung verstoßen könnte. Für diese Regel müssen Sie einen Wert für das maxCredentialUsage Alter festlegen (Standardkonfiguration: 90). Der tatsächliche Wert muss den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.AC-P1	Identitäten und Berechtigungsnachweise werden für autorisierte Personen, Prozesse und Geräte ausgestellt, verwaltet, verifiziert, widerrufen und geprüft.	secretsmanager-rotation-enabled-check	Diese Regel stellt sicher, dass bei AWS Secrets Manager Manager-Geheimnissen die Rotation aktiviert ist. Die regelmäßige Rotation von Secrets kann den Zeitraum verkürzen, in dem ein Secret aktiv ist, und möglicherweise die Auswirkungen auf das Unternehmen verringern, falls das Secret kompromittiert wird.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.AC-P1	Identitäten und Berechtigungsnachweise werden für autorisierte Personen, Prozesse und Geräte ausgestellt, verwaltet, verifiziert, widerrufen und geprüft.	emr-kerberos-enabled	Die Zugriffsberechtigungen und -autorisierungen können verwaltet und nach den Prinzipien der geringsten Berechtigung und Aufgabentrennung integriert werden, indem Kerberos für Amazon-EMR-Cluster aktiviert wird. In Kerberos werden Services und Benutzer, die sich authentifizieren müssen, als Prinzipale bezeichnet. Prinzipale befinden sich in einem Kerberos-Bereich. Innerhalb dieses Bereichs wird ein Kerberos-Server als Key Distribution Center (KDC) bezeichnet. Über diesen Server können sich Prinzipale authentifizieren. Die Authentifizierung im KDC erfolgt durch die Ausstellung von Authentif

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			izierungstickets. Das KDC unterhält eine Datenbank der Prinzipale in seinem Bereich mit ihren Passwörtern und anderen administr ativen Informationen zu jedem Prinzipal.
PR.AC-P1	Identitäten und Berechtigungsnachw eise werden für autorisierte Personen, Prozesse und Geräte ausgestellt, verwaltet , verifiziert, widerrufen und geprüft.	iam-user-mfa-enabled	Aktivieren Sie diese Regel, um den Zugriff auf Ressourcen in der AWS Cloud einzuschr änken. Diese Regel sorgt dafür, dass die Multi-Faktor-Authe ntifizierung (MFA) für alle Benutzer aktiviert ist. MFA sorgt für eine weitere Schutzebe ne zusätzlich zu den Anmeldeinformation en. Reduzieren Sie Fälle von kompromit tierten Konten, indem Sie MFA für Benutzer vorschreiben.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.AC-P1	Identitäten und Berechtigungsnachweise werden für autorisierte Personen, Prozesse und Geräte ausgestellt, verwaltet, verifiziert, widerrufen und geprüft.	s-3 bucket-policy-grantee-check	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie s3_bucket_policy_grantee_check aktivieren. Diese Regel prüft, ob der vom Amazon S3 S3-Bucket gewährte Zugriff durch die von Ihnen bereitgestellten AWS Principals, Verbundbenutzer, Service Principals, IP-Adressen oder Amazon Virtual Private Cloud (Amazon VPC) IDs eingeschränkt ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.AC-P1	Identitäten und Berechtigungsnachweise werden für autorisierte Personen, Prozesse und Geräte ausgestellt, verwaltet, verifiziert, widerrufen und geprüft.	iam-policy-no-statements-with-full-access	Stellen Sie sicher, dass IAM-Aktionen nur auf die benötigten Aktionen beschränkt sind. Wenn Benutzern mehr Rechte eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Rechte und der Aufgabentrennung verstoßen.
PR.AC-P1	Identitäten und Berechtigungsnachweise werden für autorisierte Personen, Prozesse und Geräte ausgestellt, verwaltet, verifiziert, widerrufen und geprüft.	ec2- instance-profile-attached	EC2 Instanzprofile übergeben eine IAM-Rolle an eine EC2 Instance. Das Anhängen eines Instance-Profils an Ihre Instances kann bei der Implementierung von geringsten Berechtigungen und der Berechtigungsverwaltung helfen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.AC-P1	Identitäten und Berechtigungsnachweise werden für autorisierte Personen, Prozesse und Geräte ausgestellt, verwaltet, verifiziert, widerrufen und geprüft.	ecs-task-definition-user-for-host-mode-check	Wenn für eine Aufgabendefinition erhöhte Berechtigungen gelten, liegt das daran, dass der Kunde diesen Konfigurationen ausdrücklich zugestimmt hat. Diese Kontrolle prüft, ob eine unerwartete Berechtigungseskalation vorliegt, wenn für eine Aufgabendefinition das Host-Netzwerk aktiviert ist, die Kunden aber keine erhöhten Berechtigungen aktiviert haben.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.AC-P1	Identitäten und Berechtigungsnachweise werden für autorisierte Personen, Prozesse und Geräte ausgestellt, verwaltet, verifiziert, widerrufen und geprüft.	restricted-common-ports	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass gemeinsame Ports für Amazon Elastic Compute Cloud (Amazon EC2) -Sicherheitsgruppen eingeschränkt sind. Wenn der Zugriff auf Ports nicht auf vertrauenswürdige Quellen beschränkt wird, kann dies zu Angriffen auf die Verfügbarkeit, Integrität und Vertraulichkeit von Systemen führen. Mit dieser Regel können Sie optional die Parameter blockedPort1–blockedPort5 festlegen (Standardkonfigurationen: 20, 21, 3389, 3306, 4333). Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.AC-P1	Identitäten und Berechtigungsnachweise werden für autorisierte Personen, Prozesse und Geräte ausgestellt, verwaltet, verifiziert, widerrufen und geprüft.	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) Security Groups können bei der Verwaltung des Netzwerkzugriffs helfen, indem sie eine statusbehaftete Filterung von eingehendem und ausgehendem Netzwerkverkehr zu Ressourcen bereitstellen. AWS Wenn Sie eingehenden (oder entfernten) Datenverkehr von 0.0.0.0/0 bis Port 22 auf Ihren Ressourcen nicht zulassen, können Sie den Remote-Zugriff einschränken.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.AC-P1	Identitäten und Berechtigungsnachweise werden für autorisierte Personen, Prozesse und Geräte ausgestellt, verwaltet, verifiziert, widerrufen und geprüft.	ssm-document-not-public	Stellen Sie sicher, dass AWS Systems Manager (SSM) - Dokumente nicht öffentlich sind, da dies einen unbeabsichtigten Zugriff auf Ihre SSM-Dokumente ermöglichen kann. Ein öffentliches SSM-Dokument kann Informationen über Ihr Konto, Ihre Ressourcen und internen Prozesse preisgeben.
PR.AC-P3	Der Fernzugriff wird verwaltet.	dms-replication-not-public	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass auf DMS-Replikationsinstanzen nicht öffentlich zugegriffen werden kann. DMS-Replikations-Instances können vertrauliche Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.AC-P3	Der Fernzugriff wird verwaltet.	ebs-snapshot-public-restorable-überprüfen	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass EBS-Snapshots nicht öffentlich wiederher stellbar sind. EBS-Volume-Snapsho ts können vertrauli che Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.
PR.AC-P3	Der Fernzugriff wird verwaltet.	ec-2 instance-no-public-ip	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon Elastic Compute Cloud (Amazon EC2) - Instances nicht öffentlich zugänglich sind. EC2 Amazon-Instances können vertrauliche Informati onen enthalten, und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.AC-P3	Der Fernzugriff wird verwaltet.	elasticsearch-in-vpc-only	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass sich Amazon OpenSearch OpenSearch Service (Service) - Domains innerhalb einer Amazon Virtual Private Cloud (Amazon VPC) befinden. Eine OpenSearch Service-Domain innerhalb einer Amazon VPC ermöglicht die sichere Kommunikation zwischen OpenSearch Service und anderen Services innerhalb der Amazon VPC, ohne dass ein Internet-Gateway, ein NAT-Gerät oder eine VPN-Verbindung erforderlich ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.AC-P3	Der Fernzugriff wird verwaltet.	opensearch-in-vpc-only	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass sich Amazon OpenSearch Service-Domains innerhalb einer Amazon Virtual Private Cloud (Amazon VPC) befinden. Eine Amazon OpenSearch Service-Domain innerhalb einer Amazon VPC ermöglicht die sichere Kommunikation zwischen Amazon OpenSearch Service und anderen Services innerhalb der Amazon VPC, ohne dass ein Internet-Gateway, ein NAT-Gerät oder eine VPN-Verbindung erforderlich ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.AC-P3	Der Fernzugriff wird verwaltet.	emr-master-no-public-ip	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon EMR-Cluster-Masterknoten nicht öffentlich zugänglich sind. Amazon-EMR-Cluster-Hauptknoten können vertrauliche Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.AC-P3	Der Fernzugriff wird verwaltet.	ec-2 instances-in-vpc	Stellen Sie Amazon Elastic Compute Cloud (Amazon EC2) -Instances innerhalb einer Amazon Virtual Private Cloud (Amazon VPC) bereit, um eine sichere Kommunika tion zwischen einer Instance und anderen Services innerhalb der Amazon VPC zu ermöglichen, ohne dass ein Internet-Gateway, ein NAT-Gerät oder eine VPN-Verbindung erforderlich ist. Der gesamte Datenverk ehr bleibt sicher in der AWS Cloud. Domains, die sich innerhalb einer VPC befinden, verfügen aufgrund ihrer logischen Isolierun g im Vergleich zu Domains mit öffentlic hen Endpunkten über eine zusätzlic he Sicherheitsebene. Weisen Sie EC2

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			Amazon-Instances einer Amazon-VPC zu, um den Zugriff ordnungsgemäß zu verwalten.
PR.AC-P3	Der Fernzugriff wird verwaltet.	lambda-function-public-access-verboten	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass AWS Lambda-Funktionen nicht öffentlich zugänglich sind. Der öffentliche Zugriff kann möglicherweise die Verfügbarkeit von Ressourcen beeinträchtigen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.AC-P3	Der Fernzugriff wird verwaltet.	lambda-inside-vpc	Stellen Sie AWS Lambda-Funktionen in einer Amazon Virtual Private Cloud (Amazon VPC) bereit, um eine sichere Kommunika tion zwischen einer Funktion und anderen Diensten innerhalb der Amazon VPC zu gewährleisten. Bei dieser Konfiguration sind kein Internet-Gateway, kein NAT-Gerät und keine VPN-Verbindung erforderlich. Der gesamte Datenverk ehr bleibt sicher in der Cloud. AWS Domains, die sich innerhalb einer VPC befinden, verfügen aufgrund ihrer logischen Isolierun g im Vergleich zu Domains mit öffentlic hen Endpunkten über eine zusätzliche Sicherheitsebene. Um den Zugriff ordnungsg emäß zu verwalten,

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			sollten AWS Lambda-Funktionen einer VPC zugewiesen werden.
PR.AC-P3	Der Fernzugriff wird verwaltet.	no-unrestricted-route-to-igw	Stellen Sie sicher, dass EC2 Amazon-Routentabellen keine uneingeschränkten Routen zu einem Internet-Gateway enthalten. Durch das Entfernen oder Beschränken des Internetzugangs für Workloads innerhalb von Amazon VPCs können unbeabsic htigte Zugriffe in Ihrer Umgebung reduziert werden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.AC-P3	Der Fernzugriff wird verwaltet.	rds-instance-public-access-überprüfen	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Relational Database Service (Amazon RDS) -Instances nicht öffentlich sind. Amazon-RDS-Datenbank-Instances können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.AC-P3	Der Fernzugriff wird verwaltet.	rds-snapshots-public-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Relational Database Service (Amazon RDS) -Instances nicht öffentlich sind. Amazon-RDS-Datenbank-Instances können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.AC-P3	Der Fernzugriff wird verwaltet.	redshift-cluster-public-access-überprüfen	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Redshift Redshift-Cluster nicht öffentlich sind. Amazon-Redshift-Cluster können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.AC-P3	Der Fernzugriff wird verwaltet.	restricted-common-ports	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass gemeinsame Ports für Amazon Elastic Compute Cloud (Amazon EC2) -Sicherheitsgruppen eingeschränkt sind. Wenn der Zugriff auf Ports nicht auf vertrauenswürdige Quellen beschränkt wird, kann dies zu Angriffen auf die Verfügbarkeit, Integrität und Vertraulichkeit von Systemen führen. Mit dieser Regel können Sie optional die Parameter blockedPort1–blockedPort5 festlegen (Standardkonfigurationen: 20, 21, 3389, 3306, 4333). Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.AC-P3	Der Fernzugriff wird verwaltet.	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) Security Groups können bei der Verwaltung des Netzwerkzugriffs helfen, indem sie eine statusbeh aftete Filterung von eingehendem und ausgehendem Netzwerkverkehr zu Ressourcen bereitste llen. AWS Wenn Sie eingehenden (oder entfernten) Datenverk ehr von 0.0.0.0/0 bis Port 22 auf Ihren Ressourcen nicht zulassen, können Sie den Remote-Zugriff einschränken.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.AC-P3	Der Fernzugriff wird verwaltet.	s3-Blöcke, periodisch account-level-public-access	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Simple Storage Service (Amazon S3) -Buckets nicht öffentlich zugänglich sind. Diese Regel trägt dazu bei, sensible Daten vor unbefugten Remote-Benutzern zu schützen, indem sie den öffentlichen Zugriff verhindert. Mit dieser Regel können Sie optional die Parameter ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) und restrictPublicBuckets Parameter (Config Default: True) festlegen. Die tatsächlichen Werte müssen den Richtlini

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			en Ihrer Organisation entsprechen.
PR.AC-P3	Der Fernzugriff wird verwaltet.	s3- bucket-public-read -prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie nur autorisierten Benutzern, Prozessen und Geräten Zugriff auf Amazon Simple Storage Service (Amazon S3) - Buckets gewähren. Die Verwaltung des Zugriffs sollte mit der Klassifizierung der Daten übereinst immen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.AC-P3	Der Fernzugriff wird verwaltet.	s3- bucket-public-write-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie nur autorisierten Benutzern, Prozessen und Geräten Zugriff auf Amazon Simple Storage Service (Amazon S3) - Buckets gewähren. Die Verwaltung des Zugriffs sollte mit der Klassifizierung der Daten übereinstimmen.
PR.AC-P3	Der Fernzugriff wird verwaltet.	sagemaker-notebook-no-direct-Internetzugang	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass SageMaker Amazon-Notebooks keinen direkten Internetzugang zulassen. Indem Sie direkten Internetzugang blockieren, vermeiden Sie, dass unbefugte Benutzer auf sensible Daten zugreifen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.AC-P3	Der Fernzugriff wird verwaltet.	ssm-document-not-public	Stellen Sie sicher, dass AWS Systems Manager (SSM) - Dokumente nicht öffentlich sind, da dies einen unbeabsichtigten Zugriff auf Ihre SSM-Dokumente ermöglichen kann. Ein öffentliches SSM-Dokument kann Informationen über Ihr Konto, Ihre Ressourcen und internen Prozesse preisgeben.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.AC-P3	Der Fernzugriff wird verwaltet.	subnet-auto-assign-public-ip-deaktiviert	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon Virtual Private Cloud (VPC) -Subnetzen nicht automatisch eine öffentliche IP-Adresse zugewiesen wird. Amazon Elastic Compute Cloud (EC2) -Instances, die in Subnetzen gestartet werden, in denen dieses Attribut aktiviert ist, haben ihrer primären Netzwerkschnittstelle eine öffentliche IP-Adresse zugewiesen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.AC-P3	Der Fernzugriff wird verwaltet.	vpc-default-security-group-geschlossen	Sicherheitsgruppen von Amazon Elastic Compute Cloud (Amazon EC2) können bei der Verwaltung des Netzwerkzugriffs helfen, indem sie eine statusbehaftete Filterung des ein- und ausgehenden Netzwerkverkehrs zu Ressourcen bereitstellen. AWS Die Beschränk ung des gesamten Datenverkehrs auf die Standardsicherheit sgruppe hilft dabei, den Fernzugriff auf Ihre Ressourcen einzuschränken. AWS

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.AC-P3	Der Fernzugriff wird verwaltet.	vpc-sg-open-only-to-authorized-ports	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass gemeinsame Ports für Amazon Elastic Compute Cloud (Amazon EC2) -Sicherheitsgruppen eingeschränkt sind. Wenn der Zugriff auf Ports nicht auf vertrauenswürdige Quellen beschränkt wird, kann dies zu Angriffen auf die Verfügbarkeit, Integrität und Vertraulichkeit von Systemen führen. Durch die Beschränkung des Zugriffs auf Ressourcen innerhalb einer Sicherheitsgruppe aus dem Internet (0.0.0.0/0) kann der Fernzugriff auf interne Systeme gesteuert werden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.AC-P3	Der Fernzugriff wird verwaltet.	autoscaling-launch-config-public-ip-deaktiviert	Wenn Sie Ihre Netzwerkschnittstellen mit einer öffentlichen IP-Adresse konfigurieren, sind die diesen Netzwerkschnittstellen zugehörigen Ressourcen über das Internet erreichbar. EC2 Ressourcen sollten nicht öffentlich zugänglich sein, da dies einen unbeabsichtigten Zugriff auf Ihre Anwendungen oder Server ermöglichen kann.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.AC-P3	Der Fernzugriff wird verwaltet.	redshift-enhanced-vpc-routing-aktiviert	Mit Enhanced-VPC-Routing wird erzwungen, dass der gesamte COPY- und UNLOAD-Datenverkehr zwischen Ihrem Cluster und Datenrepositorys über Ihre Amazon VPC erfolgt. Anschließend können Sie VPC-Features wie Sicherheitsgruppen und Netzwerkzugriffskontrolllisten verwenden, um den Netzwerkverkehr zu schützen. Sie können auch VPC-Flow-Logs verwenden, um den Netzwerkverkehr zu überwachen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.AC-P4	Zugriffsberechtigungen und Autorisierungen werden nach den Grundsätzen der geringsten Rechte und der Aufgabentrennung verwaltet	ec2-imdsv2-check	Stellen Sie sicher, dass die Methode Instance Metadata Service Version 2 (IMDSv2) aktiviert ist, um den Zugriff auf und die Kontrolle der Amazon Elastic Compute Cloud (Amazon EC2) - Instance-Metadaten zu schützen. Die IMDSv2 Methode verwendet sitzungsbasierte Kontrollen. Mit können Kontrollen implementiert werden IMDSv2, um Änderungen an Instanzmetadaten einzuschränken.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.AC-P4	Zugriffsberechtigungen und Autorisierungen werden nach den Grundsätzen der geringsten Rechte und der Aufgabentrennung verwaltet	emr-kerberos-enabled	Die Zugriffsberechtigungen und -autorisierungen können verwaltet und nach den Prinzipien der geringsten Berechtigung und Aufgabentrennung integriert werden, indem Kerberos für Amazon-EMR-Cluster aktiviert wird. In Kerberos werden Services und Benutzer, die sich authentifizieren müssen, als Prinzipale bezeichnet. Prinzipale befinden sich in einem Kerberos-Bereich. Innerhalb dieses Bereichs wird ein Kerberos-Server als Key Distribution Center (KDC) bezeichnet. Über diesen Server können sich Prinzipale authentifizieren. Die Authentifizierung im KDC erfolgt durch die Ausstellung von Authentif

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			izierungstickets. Das KDC unterhält eine Datenbank der Prinzipale in seinem Bereich mit ihren Passwörtern und anderen administr ativen Informationen zu jedem Prinzipal.
PR.AC-P4	Zugriffsberechtigu ngen und Autorisie rungen werden nach den Grundsätzen der geringsten Rechte und der Aufgabent rennung verwaltet	iam-group-has-users-überprüfen	AWS Identity and Access Managemen t (IAM) kann Ihnen helfen, die Prinzipien der geringsten Rechte und der Aufgabent rennung mit Zugriffsb erechtigungen und Autorisierungen zu integrieren, indem sichergestellt wird, dass IAM-Gruppen mindestens einen Benutzer haben. Die Einteilung von Benutzern in Gruppen auf der Grundlage der ihnen zugewiese nen Berechtigungen oder ihrer Funktion ist eine Möglichkeit, das Prinzip der geringste n Berechtigung zu implementieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.AC-P4	Zugriffsberechtigungen und Autorisierungen werden nach den Grundsätzen der geringsten Rechte und der Aufgabentrennung verwaltet	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) kann Ihnen dabei helfen, die Prinzipien der geringsten Rechte und der Aufgabentrennung in Zugriffsberechtigungen und Autorisierungen zu integrieren und so zu verhindern, dass Richtlinien „Effect“: „Allow“ mit „Action“: „*“ anstelle von „Resource“: „*“ enthalten. Wenn Benutzern mehr Rechte eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und der Aufgabentrennung verstoßen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.AC-P4	Zugriffsberechtigungen und Autorisierungen werden nach den Grundsätzen der geringsten Rechte und der Aufgabentrennung verwaltet	iam-root-access-key-überprüfen	Der Zugriff auf Systeme und Ressourcen kann gesteuert werden, indem überprüft wird, ob der Root-Benutzer keine Zugriffsschlüssel mit seiner AWS Identity and Access Management (IAM) -Rolle verknüpft hat. Stellen Sie sicher, dass die Root-Zugriffsschlüssel gelöscht werden. Erstellen und verwenden Sie stattdessen rollenbasierte Funktionen, AWS-Konten um das Prinzip der geringsten Funktionalität zu berücksichtigen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.AC-P4	Zugriffsberechtigungen und Autorisierungen werden nach den Grundsätzen der geringsten Rechte und der Aufgabentrennung verwaltet	iam-user-group-membership-überprüfen	AWS Identity and Access Management (IAM) kann Ihnen helfen, Zugriffsberechtigungen und Autorisierungen einzuschränken, indem sichergestellt wird, dass Benutzer Mitglieder mindestens einer Gruppe sind. Wenn Benutzern mehr Berechtigungen eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und Aufgabentrennung verstoßen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.AC-P4	Zugriffsberechtigungen und Autorisierungen werden nach den Grundsätzen der geringsten Rechte und der Aufgabentrennung verwaltet	iam-user-unused-credentials-überprüfen	AWS Identity and Access Management (IAM) kann Ihnen bei Zugriffsberechtigungen und Autorisierungen helfen, indem es nach IAM-Passwörtern und Zugriffsschlüsseln sucht, die für einen bestimmten Zeitraum nicht verwendet wurden. Wenn ungenutzte Anmeldeinformationen identifiziert werden, müssen Sie sie deaktivieren und/oder entfernen, da dies gegen das Prinzip der geringsten Berechtigung verstoßen könnte. Für diese Regel müssen Sie einen Wert für das maxCredentialUsage Alter festlegen (Standardkonfiguration: 90). Der tatsächliche Wert muss den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.AC-P4	Zugriffsberechtigungen und Autorisierungen werden nach den Grundsätzen der geringsten Rechte und der Aufgabentrennung verwaltet	s-3 bucket-policy-grantee-check	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie s3_bucket_policy_grantee_check aktivieren. Diese Regel prüft, ob der vom Amazon S3 S3-Bucket gewährte Zugriff durch die von Ihnen bereitgestellten AWS Principals, Verbundbenutzer, Service Principals, IP-Adressen oder Amazon Virtual Private Cloud (Amazon VPC) IDs eingeschränkt ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.AC-P4	Zugriffsberechtigungen und Autorisierungen werden nach den Grundsätzen der geringsten Rechte und der Aufgabentrennung verwaltet	iam-policy-no-statements-with-full-access	Stellen Sie sicher, dass IAM-Aktionen nur auf die benötigten Aktionen beschränkt sind. Wenn Benutzern mehr Rechte eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Rechte und der Aufgabentrennung verstoßen.
PR.AC-P4	Zugriffsberechtigungen und Autorisierungen werden nach den Grundsätzen der geringsten Rechte und der Aufgabentrennung verwaltet	ec2- instance-profile-attached	EC2 Instanzprofile übergeben eine IAM-Rolle an eine EC2 Instance. Das Anhängen eines Instance-Profils an Ihre Instances kann bei der Implementierung von geringsten Berechtigungen und der Berechtigungsverwaltung helfen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.AC-P4	Zugriffsberechtigungen und Autorisierungen werden nach den Grundsätzen der geringsten Rechte und der Aufgabentrennung verwaltet	dms-replication-not-public	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass auf DMS-Replikationsinstanzen nicht öffentlich zugegriffen werden kann. DMS-Replikations-Instances können vertrauliche Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.
PR.AC-P4	Zugriffsberechtigungen und Autorisierungen werden nach den Grundsätzen der geringsten Rechte und der Aufgabentrennung verwaltet	ebs-snapshot-public-restorable-überprüfen	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass EBS-Snapshots nicht öffentlich wiederherstellbar sind. EBS-Volume-Snapshots können vertrauliche Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.AC-P4	Zugriffsberechtigungen und Autorisierungen werden nach den Grundsätzen der geringsten Rechte und der Aufgabentrennung verwaltet	ec-2 instance-no-public-ip	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon Elastic Compute Cloud (Amazon EC2) - Instances nicht öffentlich zugänglich sind. EC2 Amazon-Instances können vertrauliche Informationen enthalten, und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.AC-P4	Zugriffsberechtigungen und Autorisierungen werden nach den Grundsätzen der geringsten Rechte und der Aufgabentrennung verwaltet	elasticsearch-in-vpc-only	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass sich Amazon OpenSearch OpenSearch Service (Service) - Domains innerhalb einer Amazon Virtual Private Cloud (Amazon VPC) befinden. Eine OpenSearch Service-Domain innerhalb einer Amazon VPC ermöglicht die sichere Kommunikation zwischen OpenSearch Service und anderen Services innerhalb der Amazon VPC, ohne dass ein Internet-Gateway, ein NAT-Gerät oder eine VPN-Verbindung erforderlich ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.AC-P4	Zugriffsberechtigungen und Autorisierungen werden nach den Grundsätzen der geringsten Rechte und der Aufgabentrennung verwaltet	opensearch-in-vpc-only	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass sich Amazon OpenSearch Service-Domains innerhalb einer Amazon Virtual Private Cloud (Amazon VPC) befinden. Eine Amazon OpenSearch Service-Domain innerhalb einer Amazon VPC ermöglicht die sichere Kommunikation zwischen Amazon OpenSearch Service und anderen Services innerhalb der Amazon VPC, ohne dass ein Internet-Gateway, ein NAT-Gerät oder eine VPN-Verbindung erforderlich ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.AC-P4	Zugriffsberechtigungen und Autorisierungen werden nach den Grundsätzen der geringsten Rechte und der Aufgabentrennung verwaltet	emr-master-no-public-ip	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon EMR-Cluster-Masterknoten nicht öffentlich zugänglich sind. Amazon-EMR-Cluster-Hauptknoten können vertrauliche Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.AC-P4	Zugriffsberechtigungen und Autorisierungen werden nach den Grundsätzen der geringsten Rechte und der Aufgabentrennung verwaltet	ec-2 instances-in-vpc	Stellen Sie Amazon Elastic Compute Cloud (Amazon EC2) -Instances innerhalb einer Amazon Virtual Private Cloud (Amazon VPC) bereit, um eine sichere Kommunikation zwischen einer Instance und anderen Services innerhalb der Amazon VPC zu ermöglichen, ohne dass ein Internet-Gateway, ein NAT-Gerät oder eine VPN-Verbindung erforderlich ist. Der gesamte Datenverkehr bleibt sicher in der AWS Cloud. Domains, die sich innerhalb einer VPC befinden, verfügen aufgrund ihrer logischen Isolierung im Vergleich zu Domains mit öffentlichen Endpunkten über eine zusätzliche Sicherheitsebene. Weisen Sie EC2

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			Amazon-Instances einer Amazon-VPC zu, um den Zugriff ordnungsgemäß zu verwalten.
PR.AC-P4	Zugriffsberechtigungen und Autorisierungen werden nach den Grundsätzen der geringsten Rechte und der Aufgabentrennung verwaltet	lambda-function-public-access-verboten	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass AWS Lambda-Funktionen nicht öffentlich zugänglich sind. Der öffentliche Zugriff kann möglicherweise die Verfügbarkeit von Ressourcen beeinträchtigen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.AC-P4	Zugriffsberechtigungen und Autorisierungen werden nach den Grundsätzen der geringsten Rechte und der Aufgabentrennung verwaltet	lambda-inside-vpc	Stellen Sie AWS Lambda-Funktionen in einer Amazon Virtual Private Cloud (Amazon VPC) bereit, um eine sichere Kommunikation zwischen einer Funktion und anderen Diensten innerhalb der Amazon VPC zu gewährleisten. Bei dieser Konfiguration sind kein Internet-Gateway, kein NAT-Gerät und keine VPN-Verbindung erforderlich. Der gesamte Datenverkehr bleibt sicher in der Cloud. AWS Domains, die sich innerhalb einer VPC befinden, verfügen aufgrund ihrer logischen Isolierung im Vergleich zu Domains mit öffentlichen Endpunkten über eine zusätzliche Sicherheitsebene. Um den Zugriff ordnungsgemäß zu verwalten,

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			sollten AWS Lambda-Funktionen einer VPC zugewiesen werden.
PR.AC-P4	Zugriffsberechtigungen und Autorisierungen werden nach den Grundsätzen der geringsten Rechte und der Aufgabentrennung verwaltet	rds-instance-public-access-überprüfen	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Relational Database Service (Amazon RDS) -Instances nicht öffentlich sind. Amazon-RDS-Datenbank-Instances können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.AC-P4	Zugriffsberechtigungen und Autorisierungen werden nach den Grundsätzen der geringsten Rechte und der Aufgabentrennung verwaltet	rds-snapshots-public-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Relational Database Service (Amazon RDS) -Instances nicht öffentlich sind. Amazon-RDS-Datenbank-Instances können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.AC-P4	Zugriffsberechtigungen und Autorisierungen werden nach den Grundsätzen der geringsten Rechte und der Aufgabentrennung verwaltet	redshift-cluster-public-access-überprüfen	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Redshift Redshift-Cluster nicht öffentlich sind. Amazon-Redshift-Cluster können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.AC-P4	Zugriffsberechtigungen und Autorisierungen werden nach den Grundsätzen der geringsten Rechte und der Aufgabentrennung verwaltet	s3- -Block-periodisch account-level-public-access	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Simple Storage Service (Amazon S3) -Buckets nicht öffentlich zugänglich sind. Diese Regel trägt dazu bei, sensible Daten vor unbefugten Remote-Benutzern zu schützen, indem sie den öffentlichen Zugriff verhindert. Mit dieser Regel können Sie optional die Parameter ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) und restrictPublicBuckets Parameter (Config Default: True) festlegen. Die tatsächlichen Werte müssen den Richtlini

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			en Ihrer Organisation entsprechen.
PR.AC-P4	Zugriffsberechtigungen und Autorisierungen werden nach den Grundsätzen der geringsten Rechte und der Aufgabentrennung verwaltet	s3- bucket-public-read-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie nur autorisierten Benutzern, Prozessen und Geräten Zugriff auf Amazon Simple Storage Service (Amazon S3) - Buckets gewähren. Die Verwaltung des Zugriffs sollte mit der Klassifizierung der Daten übereinstimmen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.AC-P4	Zugriffsberechtigungen und Autorisierungen werden nach den Grundsätzen der geringsten Rechte und der Aufgabentrennung verwaltet	s3- bucket-public-write-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie nur autorisierten Benutzern, Prozessen und Geräten Zugriff auf Amazon Simple Storage Service (Amazon S3) - Buckets gewähren. Die Verwaltung des Zugriffs sollte mit der Klassifizierung der Daten übereinstimmen.
PR.AC-P4	Zugriffsberechtigungen und Autorisierungen werden nach den Grundsätzen der geringsten Rechte und der Aufgabentrennung verwaltet	sagemaker-notebook-no-direct-Internetzugang	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass SageMaker Amazon-Notebooks keinen direkten Internetzugang zulassen. Indem Sie direkten Internetzugang blockieren, vermeiden Sie, dass unbefugte Benutzer auf sensible Daten zugreifen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.AC-P4	Zugriffsberechtigungen und Autorisierungen werden nach den Grundsätzen der geringsten Rechte und der Aufgabentrennung verwaltet	subnet-auto-assign-public-ip-deaktiviert	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon Virtual Private Cloud (VPC) -Subnetzen nicht automatisch eine öffentliche IP-Adresse zugewiesen wird. Amazon Elastic Compute Cloud (EC2) -Instances, die in Subnetzen gestartet werden, in denen dieses Attribut aktiviert ist, haben ihrer primären Netzwerkschnittstelle eine öffentliche IP-Adresse zugewiesen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.AC-P4	Zugriffsberechtigungen und Autorisierungen werden nach den Grundsätzen der geringsten Rechte und der Aufgabentrennung verwaltet	ecs-task-definition-user-for-host-mode-check	Wenn für eine Aufgabendefinition erhöhte Berechtigungen gelten, liegt das daran, dass der Kunde diesen Konfigurationen ausdrücklich zugestimmt hat. Diese Kontrolle prüft, ob eine unerwartete Berechtigungseskalation vorliegt, wenn für eine Aufgabendefinition das Host-Netzwerk aktiviert ist, die Kunden aber keine erhöhten Berechtigungen aktiviert haben.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.AC-P4	Zugriffsberechtigungen und Autorisierungen werden nach den Grundsätzen der geringsten Rechte und der Aufgabentrennung verwaltet	ssm-document-not-public	Stellen Sie sicher, dass AWS Systems Manager (SSM) - Dokumente nicht öffentlich sind, da dies einen unbeabsichtigten Zugriff auf Ihre SSM-Dokumente ermöglichen kann. Ein öffentliches SSM-Dokument kann Informationen über Ihr Konto, Ihre Ressourcen und internen Prozesse preisgeben.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.AC-P4	Zugriffsberechtigungen und Autorisierungen werden nach den Grundsätzen der geringsten Rechte und der Aufgabentrennung verwaltet	autoscaling-launch-config-public-ip-deaktiviert	Wenn Sie Ihre Netzwerkschnittstellen mit einer öffentlichen IP-Adresse konfigurieren, sind die diesen Netzwerkschnittstellen zugehörigen Ressourcen über das Internet erreichbar. EC2 Ressourcen sollten nicht öffentlich zugänglich sein, da dies einen unbeabsichtigten Zugriff auf Ihre Anwendungen oder Server ermöglichen kann.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.AC-P5	Die Netzwerkintegrität ist geschützt (z. B. Netzwerktrennung, Netzwerksegmentierung).	acm-certificate-expiration-check	Stellen Sie sicher, dass die Netzwerkintegrität geschützt ist, indem Sie sicherstellen, dass X509-Zertifikate von ACM ausgestellt werden. AWS Diese Zertifikate müssen gültig und dürfen nicht abgelaufen sein. Für diese Regel ist ein Wert für erforderlich daysToExpiration (Wert für bewährte AWS Grundregeln für Sicherheit: 90). Der tatsächliche Wert muss den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.AC-P5	Die Netzwerkintegrität ist geschützt (z. B. Netzwerktrennung, Netzwerksegmentierung).	dms-replication-not-public	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass auf DMS-Replikationsinstanzen nicht öffentlich zugegriffen werden kann. DMS-Replikations-Instances können vertrauliche Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.
PR.AC-P5	Die Netzwerkintegrität ist geschützt (z. B. Netzwerktrennung, Netzwerksegmentierung).	ebs-snapshot-public-restorable-überprüfen	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass EBS-Snapshots nicht öffentlich wiederherstellbar sind. EBS-Volume-Snapshots können vertrauliche Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.AC-P5	Die Netzwerkintegrität ist geschützt (z. B. Netzwerktrennung, Netzwerksegmentierung).	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) Security Groups können bei der Verwaltung des Netzwerkzugriffs helfen, indem sie eine statusbehaftete Filterung von eingehendem und ausgehendem Netzwerkverkehr zu Ressourcen bereitstellen. AWS Wenn Sie eingehenden (oder entfernten) Datenverkehr von 0.0.0.0/0 bis Port 22 auf Ihren Ressourcen nicht zulassen, können Sie den Remote-Zugriff einschränken.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.AC-P5	Die Netzwerkintegrität ist geschützt (z. B. Netzwerktrennung, Netzwerksegmentier ung).	vpc-default-security-group-geschlossen	Sicherheitsgruppen von Amazon Elastic Compute Cloud (Amazon EC2) können bei der Verwaltung des Netzwerkzugriffs helfen, indem sie eine statusbehaftete Filterung des ein- und ausgehenden Netzwerkverkehrs zu Ressourcen bereitstellen. AWS Die Beschränk ung des gesamten Datenverkehrs auf die Standardsicherheit sgruppe hilft dabei, den Fernzugriff auf Ihre Ressourcen einzuschränken. AWS

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.AC-P5	Die Netzwerkintegrität ist geschützt (z. B. Netzwerktrennung, Netzwerksegmentierung).	ec2- instance-no-public-ip	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon Elastic Compute Cloud (Amazon EC2) - Instances nicht öffentlich zugänglich sind. EC2 Amazon-Instances können vertrauliche Informationen enthalten, und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.AC-P5	Die Netzwerkintegrität ist geschützt (z. B. Netzwerktrennung, Netzwerksegmentierung).	elasticsearch-in-vpc-only	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass sich Amazon OpenSearch OpenSearch Service (Service) - Domains innerhalb einer Amazon Virtual Private Cloud (Amazon VPC) befinden. Eine OpenSearch Service-Domain innerhalb einer Amazon VPC ermöglicht die sichere Kommunikation zwischen OpenSearch Service und anderen Services innerhalb der Amazon VPC, ohne dass ein Internet-Gateway, ein NAT-Gerät oder eine VPN-Verbindung erforderlich ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.AC-P5	Die Netzwerkintegrität ist geschützt (z. B. Netzwerktrennung, Netzwerksegmentierung).	opensearch-in-vpc-only	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass sich Amazon OpenSearch Service-Domains innerhalb einer Amazon Virtual Private Cloud (Amazon VPC) befinden. Eine Amazon OpenSearch Service-Domain innerhalb einer Amazon VPC ermöglicht die sichere Kommunikation zwischen Amazon OpenSearch Service und anderen Services innerhalb der Amazon VPC, ohne dass ein Internet-Gateway, ein NAT-Gerät oder eine VPN-Verbindung erforderlich ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.AC-P5	Die Netzwerkintegrität ist geschützt (z. B. Netzwerktrennung, Netzwerksegmentierung).	ec2- instances-in-vpc	Stellen Sie Amazon Elastic Compute Cloud (Amazon EC2) -Instances innerhalb einer Amazon Virtual Private Cloud (Amazon VPC) bereit, um eine sichere Kommunikation zwischen einer Instance und anderen Services innerhalb der Amazon VPC zu ermöglichen, ohne dass ein Internet-Gateway, ein NAT-Gerät oder eine VPN-Verbindung erforderlich ist. Der gesamte Datenverkehr bleibt sicher in der AWS Cloud. Domains, die sich innerhalb einer VPC befinden, verfügen aufgrund ihrer logischen Isolierung im Vergleich zu Domains mit öffentlichen Endpunkten über eine zusätzliche Sicherheitsebene. Weisen Sie EC2

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			Amazon-Instances einer Amazon-VPC zu, um den Zugriff ordnungsgemäß zu verwalten.
PR.AC-P5	Die Netzwerkintegrität ist geschützt (z. B. Netzwerktrennung, Netzwerksegmentierung).	emr-master-no-public-ip	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon EMR-Cluster-Masterknoten nicht öffentlich zugänglich sind. Amazon-EMR-Cluster-Hauptknoten können vertrauliche Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.AC-P5	Die Netzwerkintegrität ist geschützt (z. B. Netzwerktrennung, Netzwerksegmentierung).	no-unrestricted-route-to-igw	Stellen Sie sicher, dass EC2 Amazon-Routentabellen keine uneingeschränkten Routen zu einem Internet-Gateway enthalten. Durch das Entfernen oder Beschränken des Internetzugangs für Workloads innerhalb von Amazon VPCs können unbeabsichtigte Zugriffe in Ihrer Umgebung reduziert werden.
PR.AC-P5	Die Netzwerkintegrität ist geschützt (z. B. Netzwerktrennung, Netzwerksegmentierung).	lambda-function-public-access-verboten	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass AWS Lambda-Funktionen nicht öffentlich zugänglich sind. Der öffentliche Zugriff kann möglicherweise die Verfügbarkeit von Ressourcen beeinträchtigen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.AC-P5	Die Netzwerkintegrität ist geschützt (z. B. Netzwerktrennung, Netzwerksegmentierung).	lambda-inside-vpc	Stellen Sie AWS Lambda-Funktionen in einer Amazon Virtual Private Cloud (Amazon VPC) bereit, um eine sichere Kommunikation zwischen einer Funktion und anderen Diensten innerhalb der Amazon VPC zu gewährleisten. Bei dieser Konfiguration sind kein Internet-Gateway, kein NAT-Gerät und keine VPN-Verbindung erforderlich. Der gesamte Datenverkehr bleibt sicher in der Cloud. AWS Domains, die sich innerhalb einer VPC befinden, verfügen aufgrund ihrer logischen Isolierung im Vergleich zu Domains mit öffentlichen Endpunkten über eine zusätzliche Sicherheitsebene. Um den Zugriff ordnungsgemäß zu verwalten,

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			sollten AWS Lambda-Funktionen einer VPC zugewiesen werden.
PR.AC-P5	Die Netzwerkintegrität ist geschützt (z. B. Netzwerktrennung, Netzwerksegmentierung).	rds-snapshots-public-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Relational Database Service (Amazon RDS) -Instances nicht öffentlich sind. Amazon-RDS-Datenbank-Instances können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.AC-P5	Die Netzwerkintegrität ist geschützt (z. B. Netzwerktrennung, Netzwerksegmentierung).	rds-instance-public-access-überprüfen	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Relational Database Service (Amazon RDS) -Instances nicht öffentlich sind. Amazon-RDS-Datenbank-Instances können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.AC-P5	Die Netzwerkintegrität ist geschützt (z. B. Netzwerktrennung, Netzwerksegmentierung).	restricted-common-ports	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass gemeinsame Ports für Amazon Elastic Compute Cloud (Amazon EC2) -Sicherheitsgruppen eingeschränkt sind. Wenn der Zugriff auf Ports nicht auf vertrauenswürdige Quellen beschränkt wird, kann dies zu Angriffen auf die Verfügbarkeit, Integrität und Vertraulichkeit von Systemen führen. Mit dieser Regel können Sie optional die Parameter blockedPort1–blockedPort5 festlegen (Standardkonfigurationen: 20, 21, 3389, 3306, 4333). Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.AC-P5	Die Netzwerkintegrität ist geschützt (z. B. Netzwerktrennung, Netzwerksegmentierung).	redshift-cluster-public-access-überprüfen	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Redshift Redshift-Cluster nicht öffentlich sind. Amazon-Redshift-Cluster können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.AC-P5	Die Netzwerkintegrität ist geschützt (z. B. Netzwerktrennung, Netzwerksegmentierung).	s3- -Block-periodisch account-level-public-access	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Simple Storage Service (Amazon S3) -Buckets nicht öffentlich zugänglich sind. Diese Regel trägt dazu bei, sensible Daten vor unbefugten Remote-Benutzern zu schützen, indem sie den öffentlichen Zugriff verhindert. Mit dieser Regel können Sie optional die Parameter ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) und restrictPublicBuckets Parameter (Config Default: True) festlegen. Die tatsächlichen Werte müssen den Richtlini

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			en Ihrer Organisation entsprechen.
PR.AC-P5	Die Netzwerkintegrität ist geschützt (z. B. Netzwerktrennung, Netzwerksegmentierung).	s-3 bucket-public-read-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie nur autorisierten Benutzern, Prozessen und Geräten Zugriff auf Amazon Simple Storage Service (Amazon S3) - Buckets gewähren. Die Verwaltung des Zugriffs sollte mit der Klassifizierung der Daten übereinstimmen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.AC-P5	Die Netzwerkintegrität ist geschützt (z. B. Netzwerktrennung, Netzwerksegmentierung).	s-3 bucket-public-write-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie nur autorisierten Benutzern, Prozessen und Geräten Zugriff auf Amazon Simple Storage Service (Amazon S3) - Buckets gewähren. Die Verwaltung des Zugriffs sollte mit der Klassifizierung der Daten übereinstimmen.
PR.AC-P5	Die Netzwerkintegrität ist geschützt (z. B. Netzwerktrennung, Netzwerksegmentierung).	sagemaker-notebook-no-direct-Internetzugang	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass SageMaker Amazon-Notebooks keinen direkten Internetzugang zulassen. Indem Sie direkten Internetzugang blockieren, vermeiden Sie, dass unbefugte Benutzer auf sensible Daten zugreifen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.AC-P5	Die Netzwerkintegrität ist geschützt (z. B. Netzwerktrennung, Netzwerksegmentierung).	subnet-auto-assign-public-ip-deaktiviert	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon Virtual Private Cloud (VPC) -Subnetzen nicht automatisch eine öffentliche IP-Adresse zugewiesen wird. Amazon Elastic Compute Cloud (EC2) -Instances, die in Subnetzen gestartet werden, in denen dieses Attribut aktiviert ist, haben ihrer primären Netzwerkschnittstelle eine öffentliche IP-Adresse zugewiesen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.AC-P5	Die Netzwerkintegrität ist geschützt (z. B. Netzwerktrennung, Netzwerksegmentierung).	vpc-sg-open-only-to-authorized-ports	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass gemeinsame Ports für Amazon Elastic Compute Cloud (Amazon EC2) -Sicherheitsgruppen eingeschränkt sind. Wenn der Zugriff auf Ports nicht auf vertrauenswürdige Quellen beschränkt wird, kann dies zu Angriffen auf die Verfügbarkeit, Integrität und Vertraulichkeit von Systemen führen. Durch die Beschränkung des Zugriffs auf Ressourcen innerhalb einer Sicherheitsgruppe aus dem Internet (0.0.0.0/0) kann der Fernzugriff auf interne Systeme gesteuert werden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.AC-P5	Die Netzwerkintegrität ist geschützt (z. B. Netzwerktrennung, Netzwerksegmentierung).	ssm-document-not-public	Stellen Sie sicher, dass AWS Systems Manager (SSM) - Dokumente nicht öffentlich sind, da dies einen unbeabsichtigten Zugriff auf Ihre SSM-Dokumente ermöglichen kann. Ein öffentliches SSM-Dokument kann Informationen über Ihr Konto, Ihre Ressourcen und internen Prozesse preisgeben.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.AC-P5	Die Netzwerkintegrität ist geschützt (z. B. Netzwerktrennung, Netzwerksegmentierung).	autoscaling-launch-config-public-ip-deaktiviert	Wenn Sie Ihre Netzwerkschnittstellen mit einer öffentlichen IP-Adresse konfigurieren, sind die diesen Netzwerkschnittstellen zugehörigen Ressourcen über das Internet erreichbar. EC2 Ressourcen sollten nicht öffentlich zugänglich sein, da dies einen unbeabsichtigten Zugriff auf Ihre Anwendungen oder Server ermöglichen kann.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.AC-P5	Die Netzwerkintegrität ist geschützt (z. B. Netzwerktrennung, Netzwerksegmentierung).	redshift-enhanced-vpc-routing-aktiviert	Mit Enhanced-VPC-Routing wird erzwungen, dass der gesamte COPY- und UNLOAD-Datenverkehr zwischen Ihrem Cluster und Datenrepositorys über Ihre Amazon VPC erfolgt. Anschließend können Sie VPC-Features wie Sicherheitsgruppen und Netzwerkzugriffskontrolllisten verwenden, um den Netzwerkverkehr zu schützen. Sie können auch VPC-Flow-Protokolle verwenden, um den Netzwerkverkehr zu überwachen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.AC-P6	Personen und Geräte werden entsprechend dem Transaktionsrisiko geprüft und an Anmeldeinformationen gebunden und authentifiziert (z. B. Sicherheits- und Datenschutzrisiken von Einzelpersonen und andere organisatorische Risiken).	iam-password-policy	Die Identitäten und Anmeldeinformationen werden auf der Grundlage einer organisatorischen IAM-Passwortrichtlinie ausgestellt, verwaltet und verifiziert. Sie erfüllen oder übertreffen die Anforderungen von NIST SP 800-63 und dem Standard „Best Practices“ von AWS Foundational Security für die Passwortstärke. Mit dieser Regel können Sie optional RequireUppercaseCharacters (Wert für AWS grundlegende Sicherheitsbewährte Methoden: wahr), RequireLowercaseCharacters (Wert für bewährte Methoden für AWS grundlegende Sicherheit: wahr), RequireSymbols (Wert für bewährte Methoden für AWS grundlegende Sicherheit:

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			wahr), RequireNumbers (Wert für bewährte Methoden für AWS grundlegende Sicherheit: wahr), MinimumPasswordLength (Wert für bewährte Methoden für AWS grundlegende Sicherheit: 14), PasswordReusePrevention (Wert für bewährte Methoden für AWS grundlegende Sicherheit: 24) und MaxPasswordAge (Wert für bewährte Methoden für AWS grundlegende Sicherheit: 90) für Ihr IAM festlegen Kennwortrichtlinie. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.AC-P6	Personen und Geräte werden entsprechend dem Transaktionsrisiko geprüft und an Anmeldeinformationen gebunden und authentifiziert (z. B. Sicherheits- und Datenschutzrisiken von Einzelpersonen und andere organisatorische Risiken).	iam-user-mfa-enabled	Aktivieren Sie diese Regel, um den Zugriff auf Ressourcen in der Cloud einzuschränken. AWS Diese Regel sorgt dafür, dass die Multi-Faktor-Authentifizierung (MFA) für alle Benutzer aktiviert ist. MFA sorgt für eine weitere Schutzebene zusätzlich zu den Anmeldeinformationen. Reduzieren Sie Fälle von kompromittierten Konten, indem Sie MFA für Benutzer vorschreiben.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.AC-P6	Einzelpersonen und Geräte werden entsprechend dem Risiko der Transaktion geprüft und an Anmeldeinformationen gebunden und authentifiziert (z. B. Sicherheits- und Datenschutzrisiken von Einzelpersonen und andere organisatorische Risiken).	mfa-enabled-for-iam-Konsolenzugriff	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass MFA für alle AWS Identity and Access Management (IAM) -Benutzer aktiviert ist, die über ein Konsolenkennwort verfügen. MFA sorgt für eine weitere Schutzebene zusätzlich zu den Anmeldeinformationen. Indem Sie MFA für Benutzer vorschreiben, können Sie Fälle kompromittierter Konten reduzieren und verhindern, dass unbefugte Benutzer auf vertrauliche Daten zugreifen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.AC-P6	Einzelpersonen und Geräte werden entsprechend dem Risiko der Transaktion geprüft und an Anmeldeinformationen gebunden (z. B. Sicherheits- und Datenschutzrisiken von Einzelpersonen und andere organisatorische Risiken).	root-account-hardware-mfa-aktiviert	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Hardware-MFA für den Root-Benutzer aktiviert ist. Der Stammbenutzer ist der AWS-Konto-Benutzer mit den meisten Berechtigungen. MFA sorgt für eine weitere Schutzebene zusätzlich zu den Anmeldeinformationen. Indem Sie MFA für den Root-Benutzer vorschreiben, können Sie die Anzahl AWS-Konten kompromittierter Benutzer reduzieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.AC-P6	Einzelpersonen und Geräte werden entsprechend dem Risiko der Transaktion geprüft und an Anmeldeinformationen gebunden und authentifiziert (z. B. Sicherheits- und Datenschutzrisiken für Einzelpersonen und andere organisatorische Risiken).	root-account-mfa-enabled	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass MFA für den Root-Benutzer aktiviert ist. Der Stammbenutzer ist der AWS-Konto-Benutzer mit den meisten Berechtigungen. MFA sorgt für eine weitere Schutzebene zusätzlich zu den Anmeldeinformationen. Indem Sie MFA für den Root-Benutzer vorschreiben, können Sie die Anzahl AWS-Konten kompromittierter Benutzer reduzieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.DS-P1	Data-at-rest sind geschützt.	api-gw-cache-enabled-und-verschlüsselt	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass die Verschlüsselung für den Cache Ihrer API-Gateway-Stufe aktiviert ist. Da für die API-Methode sensible Daten erfasst werden können, sollten Sie die Verschlüsselung von Daten im Ruhezustand aktivieren, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.DS-P1	Data-at-rest sind geschützt.	cloudtrail-security-trail-enabled	Diese Regel trägt dazu bei, die Verwendung der AWS empfohlenen bewährten Sicherheitsmethoden für sicherzustellen AWS CloudTrail, indem geprüft wird, ob mehrere Einstellungen aktiviert sind. Dazu gehören die Verwendung von Protokollverschlüsselung, Protokollvalidierung und Aktivierung AWS CloudTrail in mehreren Regionen.
PR.DS-P1	Data-at-rest sind geschützt.	encrypted-volumes	Aktivieren Sie die Verschlüsselung für Ihre Amazon-Elastic-Block-Store-(Amazon-EBS-)Volumes, um eventuell vorhandene sensible Daten sowie Daten im Ruhezustand zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.DS-P1	Data-at-rest sind geschützt.	ec-2 ebs-encryption-by-default	Zum Schutz von Daten im Ruhezustand müssen Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon Elastic Block Store (Amazon EBS)-Volumes aktiviert ist. Da sensible Daten in diesen Volumes gespeichert werden können, sollten Sie die Verschlüsselung von Daten im Ruhezustand aktivieren, um diese Daten zu schützen.
PR.DS-P1	Data-at-rest sind geschützt.	efs-encrypted-check	Aktivieren Sie die Verschlüsselung für Ihr Amazon Elastic File System (EFS), um eventuell vorhandene sensible Daten sowie Daten im Ruhezustand zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.DS-P1	Data-at-rest sind geschützt.	elasticsearch-encrypted-at-rest	Da sensible Daten vorhanden sein können und um Daten im Ruhezustand zu schützen, sollten Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon OpenSearch Service (OpenSearch Service) -Domains aktiviert ist.
PR.DS-P1	Data-at-rest sind geschützt.	opensearch-encrypted-at-rest	Da sensible Daten vorhanden sein können und um Daten im Ruhezustand zu schützen, sollten Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon OpenSearch Service-Domains aktiviert ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.DS-P1	Data-at-rest sind geschützt.	redshift-cluster-kms-enabled	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass die Verschlüs selung mit AWS Key Management Service (AWS KMS) für Ihren Amazon Redshift Redshift-Cluster aktiviert ist. Um eventuell vorhanden e sensible Daten im Ruhezustand in Redshift-Clustern zu schützen, muss die Verschlüsselung von Daten im Ruhezusta nd aktiviert sein.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.DS-P1	Data-at-rest sind geschützt.	rds-storage-encrypted	Zum Schutz von Daten im Ruhezustand müssen Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon Relational Database Service (Amazon RDS)-Instances aktiviert ist. Da sensible Daten in Amazon-RDS-Instances gespeichert werden können, sollten Sie die Verschlüsselung von Daten im Ruhezustand aktivieren, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.DS-P1	Data-at-rest sind geschützt.	rds-snapshot-encrypted	Stellen Sie sicher, dass die Verschlüsselung für Ihre Amazon Relational Database Service (Amazon RDS)-Snapshots aktiviert ist. Da sensible Daten auch im Ruhezustand vorhanden sein können, sollten Sie die Verschlüsselung von Daten im Ruhezustand aktivieren, um diese Daten zu schützen.
PR.DS-P1	Data-at-rest sind geschützt.	s-3 default-encryption-kms	Stellen Sie sicher, dass die Verschlüsselung für Ihre Amazon Simple Storage Service (Amazon S3)-Buckets aktiviert ist. Da sensible Daten in einem Amazon S3 Bucket gespeichert werden können, sollten Sie die Verschlüsselung im Ruhezustand aktivieren, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.DS-P1	Data-at-rest sind geschützt.	redshift-cluster-configuration-check	Um Daten im Ruhezustand zu schützen, muss die Verschlüsselung für Ihre Amazon-Redshift-Cluster aktiviert sein. Sie müssen auch sicherstellen, dass die erforderlichen Konfigurationen auf Amazon-Redshift-Clustern bereitgestellt werden. Die Prüfungsprotokollierung muss aktiviert sein, um Informationen zu Verbindungen und Benutzeraktivitäten in der Datenbank bereitzustellen. Diese Regel erfordert, dass ein Wert für clusterDbEncrypted (Config Default: TRUE) und LoggingEnabled (Config Default: TRUE) gesetzt ist. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.DS-P1	Data-at-rest sind geschützt.	sagemaker-endpoint-configuration-kms-key-konfiguriert	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass die Verschlüsselung mit dem AWS Key Management Service (AWS KMS) für Ihren Endpunkt aktiviert ist. SageMaker Da sensible Daten auf dem SageMaker Endgerät gespeiche rt werden können, sollten Sie die Verschlüsselung im Ruhezustand aktiviere n, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.DS-P1	Data-at-rest sind geschützt.	sagemaker-notebook-instance-kms-key-konfiguriert	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass die Verschlüsselung mit dem AWS Key Management Service (AWS KMS) für Ihr Notebook aktiviert ist. SageMaker Da vertrauliche Daten im SageMaker Notebook gespeichert werden können, sollten Sie die Verschlüsselung im Ruhezustand aktivieren, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.DS-P1	Data-at-rest sind geschützt.	secretsmanager-using-cmk	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass die Verschlüsselung mit dem AWS Key Management Service (AWS KMS) für AWS Secrets Manager aktiviert ist. Aktivieren Sie die Verschlüsselung von Daten im Ruhezustand, um eventuell vorhandene sensible Daten im Ruhezustand im Secrets Manager zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.DS-P1	Data-at-rest sind geschützt.	bucket-server-side-encryptions3-fähig	Zum Schutz von Daten im Ruhezustand müssen Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon Simple Storage Service (Amazon S3)-Buckets aktiviert ist. Da sensible Daten in Amazon S3 Buckets gespeichert werden können, sollten Sie die Verschlüsselung aktivieren, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.DS-P1	Data-at-rest sind geschützt.	sns-encrypted-kms	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass Ihre Amazon Simple Notification Service (Amazon SNS) -Themen mit dem AWS Key Management Service (AWS KMS) verschlüsselt werden müssen. Um eventuell vorhandene sensible Daten im Ruhezustand in veröffentlichten Nachrichten zu schützen, muss die Verschlüsselung von Daten im Ruhezustand aktiviert sein.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.DS-P1	Data-at-rest sind geschützt.	kms-cmk-not-scheduled-zum Löschen	Um Daten im Ruhezustand zu schützen, sollten Sie sicherstellen, dass die für den Kunden erforderlichen Masterschlüssel (CMKs) nicht im AWS Key Management Service (AWS KMS) gelöscht werden. Da Schlüssel manchmal gelöscht werden müssen, können Sie mit dieser Regel alle zu löschenden Schlüssel überprüfen, falls ein Schlüssel versehentlich zur Löschung vorgemerkt wurde.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.DS-P1	Data-at-rest sind geschützt.	dynamodb-table-encrypted-kms	Stellen Sie sicher, dass die Verschlüsselung für Ihre Amazon-DynamoDB-Tabellen aktiviert ist. Um eventuell vorhandene sensible Daten im Ruhezustand in diesen Tabellen zu schützen, müssen Sie die Verschlüsselung von Daten im Ruhezustand aktivieren. Standardmäßig werden DynamoDB-Tabellen mit einem AWS eigenen Kundenhauptschlüssel (CMK) verschlüselt.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.DS-P2	Data-in-transit sind geschützt.	alb-http-to-https-Umleitungsprüfung	Um Daten während der Übertragung zu schützen, stellen Sie sicher, dass Ihr Application Load Balancer unverschlüsselte HTTP-Anfragen automatisch an HTTPS umleitet. Da sensible Daten vorhanden sein können, sollten Sie die Verschlüsselung bei der Übertragung aktivieren, um diese Daten zu schützen.
PR.DS-P2	Data-in-transit sind geschützt.	api-gw-ssl-enabled	Stellen Sie sicher, dass die REST-API-Stufen von Amazon API Gateway mit SSL-Zertifikaten konfiguriert sind, damit Backend-Systeme überprüfen können, ob Anforderungen von API Gateway stammen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.DS-P2	Data-in-transit sind geschützt.	elb-acm-certificate-required	Zum Schutz von eventuell vorhanden en sensiblen Daten sowie von Daten während der Übertragung muss die Verschlüsselung für Ihr Elastic Load Balancing aktiviert sein. Verwenden Sie AWS Certificate Manager, um öffentlic he und private SSL/ TLS-Zertifikate mit AWS Diensten und internen Ressource n zu verwalten, bereitzustellen und bereitzustellen.
PR.DS-P2	Data-in-transit sind geschützt.	elb-tls-https-listeners-nur	Stellen Sie sicher, dass Ihre Elastic Load Balancer (ELBs) mit SSL- oder HTTPS-Listenern konfiguriert sind. Um eventuell vorhanden e sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.DS-P2	Data-in-transit sind geschützt.	s-3 bucket-ssl-requests-only	Um Daten während der Übertragung zu schützen, stellen Sie sicher, dass Ihre Amazon Simple Storage Service (Amazon S3)-Buckets Anfragen zur Verwendung von Secure Socket Layer (SSL)-Buckets erfordern. Da sensible Daten vorhanden sein können, sollten Sie die Verschlüsselung bei der Übertragung aktivieren, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.DS-P4	Angemessene Kapazitäten zur Sicherstellung der Verfügbarkeit werden aufrechterhalten.	dynamodb-autoscaling-enabled	Amazon DynamoDB Auto Scaling verwendet den AWS Application Auto Scaling-Service, um die bereitgestellte Durchsatzkapazität so anzupassen, dass sie automatisch auf tatsächliche Verkehrsmuster reagiert. Auf diese Weise kann eine Tabelle oder ein globaler sekundärer Index die bereitgestellte Lese-/Schreibkapazität erhöhen, um plötzliche Erhöhungen des Datenverkehrs ohne Drosselung zu bewältigen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.DS-P4	Angemessene Kapazitäten zur Sicherstellung der Verfügbarkeit werden aufrechterhalten.	elb-cross-zone-load-Balancing aktiviert	Aktivieren Sie zonenübergreifendes Load Balancing für Ihre Elastic Load Balancer (ELBs), um eine angemessene Kapazität und Verfügbarkeit aufrechtzuerhalten. Zonenübergreifendes Load Balancing reduziert die Notwendigkeit, die gleiche Anzahl von Instances in jeder aktivierten Availability Zone aufrechtzuerhalten. Es verbessert auch die Fähigkeit Ihrer Anwendung, den Verlust einer oder mehrerer Instances zu bewältigen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.DS-P4	Angemessene Kapazitäten zur Sicherstellung der Verfügbarkeit werden aufrechterhalten.	elb-deletion-protection-enabled	Diese Regel sorgt dafür, dass der Löschschutz für Elastic Load Balancing aktiviert ist. Verwenden Sie diese Funktion, um zu verhindern, dass Ihr Load Balancer versehentlich oder böswillig gelöscht wird, was zum Verlust der Verfügbarkeit Ihrer Anwendungen führen kann.
PR.DS-P4	Angemessene Kapazitäten zur Sicherstellung der Verfügbarkeit werden aufrechterhalten.	rds-instance-deletion-protection-aktiviert	Stellen Sie sicher, dass Amazon Relational Database Service (Amazon RDS)-Instances den Löschschutz aktiviert haben. Verwenden Sie den Löschschutz, um zu verhindern, dass Ihre Amazon-RDS-Instances versehentlich oder böswillig gelöscht werden, was zum Verlust der Verfügbarkeit Ihrer Anwendungen führen kann.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.DS-P4	Angemessene Kapazitäten zur Sicherstellung der Verfügbarkeit werden aufrechterhalten.	rds-multi-az-support	Die Multi-AZ-Unterstützung in Amazon Relational Database Service (Amazon RDS) bietet eine verbesserte Verfügbarkeit und Beständigkeit von Datenbank-Instances. Wenn Sie eine Multi-AZ-Datenbank-Instance bereitstellen, erstellt Amazon RDS automatisch eine primäre Datenbank-Instance und repliziert die Daten synchron auf eine Standby-Instance in einer anderen Availability Zone. Jede Availability Zone läuft auf einer eigenen, physisch getrennten, unabhängigen Infrastruktur und ist auf eine hohe Verfügbarkeit ausgelegt. Im Falle eines Infrastrukturausfalls führt Amazon RDS einen automatis

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			chen Failover zum Standby-Modus durch, sodass Sie den Datenbankbetrieb wieder aufnehmen können, sobald der Failover abgeschlo ssen ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.DS-P4	Angemessene Kapazitäten zur Sicherstellung der Verfügbarkeit werden aufrechterhalten.	vpc-vpn-2-tunnels-up	Redundante Site-to-Site VPN-Tunnel können implementiert werden, um die Anforderungen an die Ausfallsicherheit zu erfüllen. Es verwendet zwei Tunnel, um die Konnektivität sicherzustellen, falls eine der Site-to-Site VPN-Verbindungen nicht verfügbar ist. Um sich vor einem Verbindungsverlust zu schützen, können Sie für den Fall, dass Ihr Kunden-Gateway nicht verfügbar ist, eine zweite Site-to-Site VPN-Verbindung zu Ihrer Amazon Virtual Private Cloud (Amazon VPC) und Ihrem Virtual Private Gateway einrichten, indem Sie ein zweites Kunden-Gateway verwenden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.DS-P4	Angemessene Kapazitäten zur Sicherstellung der Verfügbarkeit werden aufrechterhalten.	db-instance-backup-enabled	Die Sicherung sfunktion von Amazon RDS erstellt Sicherung en Ihrer Datenbank en und Transakti onsprotokolle. Amazon RDS erstellt einen Snapshot für das Speichervolume Ihrer DB-Instance, sodass die gesamte DB-Instance gesichert wird. Sie können im System spezifische Aufbewahrungsfrist en festlegen, um Ihre Ausfallsicherheits anforderungen zu erfüllen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.DS-P4	Angemessene Kapazitäten zur Sicherstellung der Verfügbarkeit werden aufrechterhalten.	dynamodb-in-backup-plan	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon DynamoDB-Tabellen Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.DS-P4	Angemessene Kapazitäten zur Sicherstellung der Verfügbarkeit werden aufrechterhalten.	dynamodb-pitr-enabled	Aktivieren Sie diese Regel, um zu überprüfen, ob die Informationen gesichert wurden. Es verwaltet auch die Backups, indem es sicherstellt, dass die point-in-time Wiederherstellung in Amazon DynamoDB aktiviert ist. Bei der Wiederherstellung werden fortlaufende Backups Ihrer Tabelle für die letzten 35 Tage gespeichert.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.DS-P4	Angemessene Kapazitäten zur Sicherstellung der Verfügbarkeit werden aufrechterhalten.	ebs-in-backup-plan	Stellen Sie zur Unterstützung der Datensicherungspro zesse sicher, dass Ihre Amazon Elastic Block Store (Amazon EBS) -Volumes Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwaltet er Backup-Service mit einer richtlini enbasierten Backup-Lösung. Diese Lösung vereinfac ht Ihr Sicherung smanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforde rungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.DS-P4	Angemessene Kapazitäten zur Sicherstellung der Verfügbarkeit werden aufrechterhalten.	ebs-optimized-instance	Eine optimierte Instance im Amazon Elastic Block Store (Amazon EBS) bietet zusätzliche, dedizierte Kapazität für Amazon-EBS-I/O-Vorgänge. Diese Optimierung bietet die beste Leistung für Ihr EBS-Volume, indem Konflikte zwischen Amazon-EBS-I/O und anderem Datenverkehr von Ihrer Instance minimiert werden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.DS-P4	Angemessene Kapazitäten zur Sicherstellung der Verfügbarkeit werden aufrechterhalten.	efs-in-backup-plan	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon Elastic File System (Amazon EFS) -Dateisysteme Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.DS-P4	Angemessene Kapazitäten zur Sicherstellung der Verfügbarkeit werden aufrechterhalten.	elasticache-redis-cluster-automatic-Backup-Check	Wenn automatische Backups aktiviert sind, ElastiCache erstellt Amazon täglich ein Backup des Clusters. Die Sicherung kann für eine von Ihrer Organisation festgelegte Anzahl von Tagen aufbewahrt werden. Automatische Backups schützen vor Datenverlust. Bei einem Ausfall können Sie einen neuen Cluster erstellen, der Ihre Daten aus dem aktuellen Backup wiederherstellt.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.DS-P4	Angemessene Kapazitäten zur Sicherstellung der Verfügbarkeit werden aufrechterhalten.	rds-in-backup-plan	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon Relational Database Service (Amazon RDS) -Instances Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.DS-P4	Angemessene Kapazitäten zur Sicherstellung der Verfügbarkeit werden aufrechterhalten.	redshift-backup-enabled	Stellen Sie zur Unterstützung der Datensicherungsprozesse sicher, dass Ihre Amazon-Redshift-Cluster über automatisierte Snapshots verfügen. Wenn automatisierte Snapshots für einen Cluster aktiviert sind, erstellt Redshift in regelmäßigen Abständen Snapshots dieses Clusters. Standardmäßig erstellt Redshift alle acht Stunden oder alle 5 GB einen Snapshot für jeden Knoten mit Datenänderungen oder je nachdem, was zuerst eintritt.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.DS-P4	Angemessene Kapazitäten zur Sicherstellung der Verfügbarkeit werden aufrechterhalten.	s3- bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) unterstützt die Aufrechterhaltung einer angemesse nen Kapazität und Verfügbarkeit. CRR ermöglicht das automatische, asynchrone Kopieren von Objekten in Amazon S3 Buckets, um die Datenverf ügbarkeit sicherzus tellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.DS-P4	Angemessene Kapazitäten zur Sicherstellung der Verfügbarkeit werden aufrechterhalten.	s-3 bucket-versioning-enabled	Die Versionsv erwaltung von Amazon Simple Storage Service (Amazon S3)-Bucke ts hilft dabei, mehrere Varianten eines Objekts im selben Amazon-S3-Bucket zu speichern. Verwenden Sie die Versionsv erwaltung, um sämtliche Versionen aller Objekte in Ihrem Amazon-S3-Bucket zu speichern , abzurufen oder wiederherzustellen . Mit der Versionsv erwaltung können Sie Versionen sowohl nach unbeabsic htigten Benutzera ktionen als auch nach Anwendungsfehlern problemlos wiederher stellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.DS-P4	Angemessene Kapazitäten zur Sicherstellung der Verfügbarkeit werden aufrechterhalten.	redshift-cluster-maintenancesettings-check	Diese Regel stellt sicher, dass Amazon-Redshift-Cluster die bevorzugten Einstellungen für Ihre Organisation haben. Insbesondere sorgt sie dafür, dass Cluster bevorzugte Wartungsfenster und automatisierte Aufbewahrungsfristen für Snapshots für die Datenbank haben. Für diese Regel müssen Sie die festlegen allowVersionUpgrade. Der Standardwert ist „true“. Außerdem können Sie optional den Zeitraum preferredMaintenanceWindow (der Standardwert ist sa: 16:00 -sa: 16:30) und den automated SnapshotRetention Zeitraum (der Standardwert ist 1) festlegen. Die tatsächlichen Werte müssen den Richtlini

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			en Ihrer Organisation entsprechen.
PR.DS-P4	Angemessene Kapazitäten zur Sicherstellung der Verfügbarkeit werden aufrechterhalten.	aurora-resources-protected-by-Backup-Plan	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon Aurora Aurora-Ressourcen Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.DS-P4	Angemessene Kapazitäten zur Sicherstellung der Verfügbarkeit werden aufrechterhalten.	backup-plan-min-frequency-and-min-retention-check	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihr AWS Backup-Plan auf eine Mindestfrequenz und Aufbewahrung festgelegt ist. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen. Mit dieser Regel können Sie die Parameter requiredFrequencyValue (Config default: 1), requiredRetentionDays (Config default: 35) und requiredFrequencyUnit

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			(Config default: days) festlegen. Der tatsächliche Wert muss den Anforderungen Ihrer Organisation entsprechen.
PR.DS-P4	Angemessene Kapazitäten zur Sicherstellung der Verfügbarkeit werden aufrechterhalten.	backup-recovery-point-encrypted	Stellen Sie sicher, dass die Verschlüsselung für Ihre AWS Backup-Wiederherstellungspunkte aktiviert ist. Da sensible Daten auch im Ruhezustand vorhanden sein können, sollten Sie die Verschlüsselung im Ruhezustand aktivieren, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.DS-P4	Angemessene Kapazitäten zur Sicherstellung der Verfügbarkeit werden aufrechterhalten.	backup-recovery-point-manual-Löschen-deaktiviert	Stellen Sie sicher, dass Ihren AWS Backup-Wiederherstellungspunkten eine ressourcenbasierte Richtlinie zugeordnet ist, die das Löschen von Wiederherstellungspunkten verhindert. Die Verwendung einer ressourcenbasierten Richtlinie zur Verhinderung des Löschens von Wiederherstellungspunkten kann dazu beitragen, ein versehentliches oder absichtliches Löschen zu unterbinden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.DS-P4	Angemessene Kapazitäten zur Sicherstellung der Verfügbarkeit werden aufrechterhalten.	backup-recovery-point-minimum-Aufbewahrungsprüfung	Um bei Datensicherungsprozessen zu helfen, stellen Sie sicher, dass für Ihre AWS Backup-Wiederherstellungspunkte eine Mindestaufbewahrungsdauer festgelegt ist. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen. Mit dieser Regel können Sie den Parameter requiredRetentionDays (Config Default: 35) festlegen. Der tatsächliche Wert muss den Anforderu

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			ngen Ihrer Organisat ion entsprechen.
PR.DS-P4	Angemessene Kapazitäten zur Sicherstellung der Verfügbarkeit werden aufrechterhalten.	ec2--Plan resources-protected-by-backup	Um Sie bei Datensich erungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon Elastic Compute Cloud (Amazon EC2) -Ressourc en Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwaltet er Backup-Service mit einer richtlini enbasierten Backup-Lösung. Diese Lösung vereinfac ht Ihr Sicherung smanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforde rungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.DS-P4	Angemessene Kapazitäten zur Sicherstellung der Verfügbarkeit werden aufrechterhalten.	fsx-resources-protected-by-Backup-Plan	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre FSx Amazon-Dateisysteme Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.DS-P5	Schutzmaßnahmen gegen Datenlecks sind implementiert	cloudtrail-s3-data events-enabled	Die Erfassung von Simple Storage Service (Amazon S3)-Datenereignissen unterstützt die Erkennung von ungewöhnlichen Aktivitäten. Zu den Details gehören AWS-Konto Informationen über den Zugriff auf einen Amazon S3 S3-Bucket, die IP-Adresse und die Uhrzeit des Ereignisses.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.DS-P5	Schutzmaßnahmen gegen Datenlecks sind implementiert	cloudtrail-security-trail-enabled	Diese Regel trägt dazu bei, die Verwendung der AWS empfohlenen bewährten Sicherheitsmethoden für sicherzustellen AWS CloudTrail, indem geprüft wird, ob mehrere Einstellungen aktiviert sind. Dazu gehören die Verwendung von Protokollverschlüsselung, Protokollvalidierung und Aktivierung AWS CloudTrail in mehreren Regionen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.DS-P5	Schutzmaßnahmen gegen Datenlecks sind implementiert	cloudtrail-enabled	AWS CloudTrai l kann durch die Aufzeichnung von Aktionen und API-Aufrufen der AWS Management Console bei der Nichtabst reitbarkeit helfen. Sie können die Benutzer und die Benutzer AWS-Konten , die einen AWS Dienst aufgerufen haben, die Quell-IP-Adresse, über die die Aufrufe generiert wurden, und den Zeitpunkt der Anrufe identifiz ieren. Einzelheiten zu den erfassten Daten finden Sie unter Inhalt des AWS CloudTrail Datensatzes.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.DS-P5	Schutzmaßnahmen gegen Datenlecks sind implementiert	codebuild-project-envvar-awscred-überprüfen	Stellen Sie sicher, dass die Anmeldeinformationen AWS_ACCESS_KEY_ID AWS_SECRET_ACCESS_KEY nicht in AWS Codebuild-Projektumgebungen vorhanden sind. Speichern Sie diese Variablen nicht als Klartext. Das Speichern dieser Variablen als Klartext bewirkt eine unbeabsichtigte Offenlegung von Daten sowie unberechtigte Zugriffe.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.DS-P5	Schutzmaßnahmen gegen Datenlecks sind implementiert	dms-replication-not-public	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass auf DMS-Replikationsin stanzen nicht öffentlic h zugegriffen werden kann. DMS-Repli kations-Instances können vertrauli che Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.
PR.DS-P5	Schutzmaßnahmen gegen Datenlecks sind implementiert	ebs-snapshot-public-restorable-überprüfen	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass EBS-Snapshots nicht öffentlich wiederher stellbar sind. EBS-Volume-Snapsho ts können vertrauli che Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.DS-P5	Schutzmaßnahmen gegen Datenlecks sind implementiert	vpc-flow-logs-enabled	VPC-Flow-Protokolle erfassen detaillierte Informationsdatensätze über den IP-Datenverkehr, der zu und von Netzwerkschnittstellen in Ihrer Amazon Virtual Private Cloud (Amazon VPC) fließt. Standardmäßig enthalten Flow-Protokolldatensätze Werte für die verschiedenen Komponenten des IP-Flows, einschließlich Quelle, Ziel und Protokoll.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.DS-P5	Schutzmaßnahmen gegen Datenlecks sind implementiert	elasticsearch-in-vpc-only	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass sich Amazon OpenSearch OpenSearch Service (Service) - Domains innerhalb einer Amazon Virtual Private Cloud (Amazon VPC) befinden. Eine OpenSearch Service-Domain innerhalb einer Amazon VPC ermöglicht die sichere Kommunikation zwischen OpenSearch Service und anderen Services innerhalb der Amazon VPC, ohne dass ein Internet-Gateway, ein NAT-Gerät oder eine VPN-Verbindung erforderlich ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.DS-P5	Schutzmaßnahmen gegen Datenlecks sind implementiert	opensearch-in-vpc-only	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass sich Amazon OpenSearch Service-Domains innerhalb einer Amazon Virtual Private Cloud (Amazon VPC) befinden. Eine Amazon OpenSearch Service-Domain innerhalb einer Amazon VPC ermöglicht die sichere Kommunikation zwischen Amazon OpenSearch Service und anderen Services innerhalb der Amazon VPC, ohne dass ein Internet-Gateway, ein NAT-Gerät oder eine VPN-Verbindung erforderlich ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.DS-P5	Schutzmaßnahmen gegen Datenlecks sind implementiert	guardduty-enabled-centralized	Amazon GuardDuty kann mithilfe von Threat Intellige nce Feeds helfen, potenzielle Cybersich erheitsereignisse zu überwachen und zu erkennen. Dazu gehören Listen mit bösartigen IPs und maschinel len Lernmethoden zur Identifizierung unerwarteter, nicht autorisierter und bösartiger Aktivitäten in Ihrer AWS Cloud-Umgebung.
PR.DS-P5	Schutzmaßnahmen gegen Datenlecks sind implementiert	lambda-function-public-access-verboten	Verwalten Sie den Zugriff auf Ressource n in der AWS Cloud, indem Sie sicherste llen, dass AWS Lambda-Funktionen nicht öffentlich zugänglich sind. Der öffentliche Zugriff kann möglicherweise die Verfügbarkeit von Ressourcen beeinträc htigen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.DS-P5	Schutzmaßnahmen gegen Datenlecks sind implementiert	rds-snapshots-public-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Relational Database Service (Amazon RDS) -Instances nicht öffentlich sind. Amazon-RDS-Datenbank-Instances können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.DS-P5	Schutzmaßnahmen gegen Datenlecks sind implementiert	rds-instance-public-access-überprüfen	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Relational Database Service (Amazon RDS) -Instances nicht öffentlich sind. Amazon-RDS-Datenbank-Instances können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.DS-P5	Schutzmaßnahmen gegen Datenlecks sind implementiert	s-3 bucket-logging-enabled	Die Amazon Simple Storage Service (Amazon S3)-Serverzugriffs protokollierung bietet eine Methode zur Überwachu ng des Netzwerks im Hinblick auf potenzielle Cybersich erheitsereignisse. Die Ereignisse werden überwacht, indem detaillierte Aufzeichn ungen über die Anfragen erfasst werden, die an einen Amazon-S3-Bucket gestellt wurden. Jeder Zugriffsprotokolle intrag enthält Details zu einer einzelnen Zugriffsanfrage. Zu den Details gehören Anforderer, Bucket-Name, Anforderu ngszeit, Anforderu ngsaktion, Antwortst atus und Fehlercode, falls relevant.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.DS-P5	Schutzmaßnahmen gegen Datenlecks sind implementiert	redshift-cluster-public-access-überprüfen	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Redshift Redshift-Cluster nicht öffentlich sind. Amazon-Redshift-Cluster können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.DS-P5	Schutzmaßnahmen gegen Datenlecks sind implementiert	s3- -Block-periodisch account-level-public-access	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Simple Storage Service (Amazon S3) -Buckets nicht öffentlich zugänglich sind. Diese Regel trägt dazu bei, sensible Daten vor unbefugten Remote-Benutzern zu schützen, indem sie den öffentlichen Zugriff verhindert. Mit dieser Regel können Sie optional die Parameter ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) und restrictPublicBuckets Parameter (Config Default: True) festlegen. Die tatsächlichen Werte müssen den Richtlini

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			en Ihrer Organisation entsprechen.
PR.DS-P5	Schutzmaßnahmen gegen Datenlecks sind implementiert	securityhub-enabled	AWS Security Hub hilft bei der Überwachung von unbefugtem Personal, Verbindungen, Geräten und Software. AWS Security Hub aggregiert, organisiert und priorisiert die Sicherheitswarnungen oder Ergebnisse mehrerer Dienste. AWS Einige dieser Dienste sind Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer und AWS Firewall Manager sowie AWS Partnerlösungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.DS-P5	Schutzmaßnahmen gegen Datenlecks sind implementiert	s-3 bucket-public-read -prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie nur autorisierten Benutzern, Prozessen und Geräten Zugriff auf Amazon Simple Storage Service (Amazon S3) - Buckets gewähren. Die Verwaltung des Zugriffs sollte mit der Klassifizierung der Daten übereinst immen.
PR.DS-P5	Schutzmaßnahmen gegen Datenlecks sind implementiert	s3- bucket-public-writ e-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie nur autorisierten Benutzern, Prozessen und Geräten Zugriff auf Amazon Simple Storage Service (Amazon S3) - Buckets gewähren. Die Verwaltung des Zugriffs sollte mit der Klassifizierung der Daten übereinst immen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.DS-P5	Schutzmaßnahmen gegen Datenlecks sind implementiert	sagemaker-notebook-no-direct-Internetzugang	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass SageMaker Amazon-Notebooks keinen direkten Internetzugang zulassen. Indem Sie direkten Internetzugang blockieren, vermeiden Sie, dass unbefugte Benutzer auf sensible Daten zugreifen.
PR.DS-P5	Schutzmaßnahmen gegen Datenlecks sind implementiert	ssm-document-not-public	Stellen Sie sicher, dass AWS Systems Manager (SSM) - Dokumente nicht öffentlich sind, da dies einen unbeabsichtigten Zugriff auf Ihre SSM-Dokumente ermöglichen kann. Ein öffentliches SSM-Dokument kann Informationen über Ihr Konto, Ihre Ressourcen und internen Prozesse preisgeben.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.DS-P5	Schutzmaßnahmen gegen Datenlecks sind implementiert	autoscaling-launch-config-public-ip-deaktiviert	Wenn Sie Ihre Netzwerkschnittstellen mit einer öffentlichen IP-Adresse konfigurieren, sind die diesen Netzwerkschnittstellen zugehörigen Ressourcen über das Internet erreichbar. EC2 Ressourcen sollten nicht öffentlich zugänglich sein, da dies einen unbeabsichtigten Zugriff auf Ihre Anwendungen oder Server ermöglichen kann.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.DS-P6	Mechanismen zur Integritätsprüfung werden verwendet, um die Integrität von Software, Firmware und Informationen zu überprüfen	cloudtrail-security-trail-enabled	Diese Regel trägt dazu bei, die Verwendung der AWS empfohlenen bewährten Sicherheitsmethoden für sicherzustellen AWS CloudTrail, indem geprüft wird, ob mehrere Einstellungen aktiviert sind. Dazu gehören die Verwendung von Protokollverschlüsselung, Protokollvalidierung und Aktivierung AWS CloudTrail in mehreren Regionen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.MA-P2	Die Fernwartung von Unternehm ensressourcen wird genehmigt, protokoll iert und in einer Weise durchgeführt, die unbefugten Zugriff verhindert.	cloudtrail-security-trail-enabled	Diese Regel trägt dazu bei, die Verwendung der AWS empfohlenen bewährten Sicherhei tsmethoden für sicherzustellen AWS CloudTrai l, indem geprüft wird, ob mehrere Einstellungen aktiviert sind. Dazu gehören die Verwendun g von Protokoll verschlüsselung, Protokollvalidieru ng und Aktivierung AWS CloudTrail in mehreren Regionen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.MA-P2	Die Fernwartung von Unternehm ensressourcen wird genehmigt, protokoll iert und in einer Weise durchgeführt, die unbefugten Zugriff verhindert.	cloudtrail-enabled	AWS CloudTrai l kann durch die Aufzeichnung von Aktionen und API-Aufrufen der AWS Management Console bei der Nichtabst reitbarkeit helfen. Sie können die Benutzer und die Benutzer AWS-Konten , die einen AWS Dienst aufgerufen haben, die Quell-IP-Adresse, über die die Aufrufe generiert wurden, und den Zeitpunkt der Anrufe identifiz ieren. Einzelheiten zu den erfassten Daten finden Sie unter Inhalt des AWS CloudTrail Datensatzes.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.PO-P1	Eine grundlegende Konfiguration der Informationstechnologie wird erstellt und beibehalten, wobei Sicherheitsprinzipien (z. B. das Konzept der geringsten Funktionalität) berücksichtigt werden.	cloudtrail-security-trail-enabled	Diese Regel trägt dazu bei, die Verwendung der AWS empfohlenen bewährten Sicherheitsmethoden für sicherzustellen AWS CloudTrail, indem geprüft wird, ob mehrere Einstellungen aktiviert sind. Dazu gehören die Verwendung von Protokollverschlüsselung, Protokollvalidierung und Aktivierung AWS CloudTrail in mehreren Regionen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.PO-P1	Es wird eine Basiskonfiguration der Informationstechnologie erstellt und verwaltet, die Sicherheitsprinzipien berücksichtigt (z. B. das Konzept der geringsten Funktionalität).	ec2-manager instance-managed-by-systems	Eine Bestandsaufnahme der Softwareplattformen und Anwendungen innerhalb des Unternehmens ist möglich, indem Amazon Elastic Compute Cloud (Amazon EC2) - Instances mit AWS Systems Manager verwaltet werden. Verwenden Sie AWS Systems Manager, um detaillierte Systemkonfigurationen, Betriebssystem-Patch-Levels, Namen und Typ der Dienste, Softwareinstallationen, Anwendungsname, Herausgeber und Version sowie andere Details zu Ihrer Umgebung bereitzustellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.PO-P1	Es wird eine Basiskonfiguration der Informationstechnologie erstellt und verwaltet, die Sicherheitsprinzipien berücksichtigt (z. B. das Konzept der geringsten Funktionalität).	ec2-check managedinstance-association-compliance-status	Verwenden Sie AWS Systems Manager Associations, um bei der Inventarisierung von Softwareplattformen und Anwendungen innerhalb eines Unternehmens zu helfen. AWS Systems Manager weist Ihren verwalteten Instanzen einen Konfigurationsstatus zu und ermöglicht es Ihnen, Basiswerte für Betriebssystem-Patch-Levels, Softwareinstallationen, Anwendungskonfigurationen und andere Details zu Ihrer Umgebung festzulegen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.PO-P1	Es wird eine Basiskonfiguration der Informationstechnologie erstellt und verwaltet, die Sicherheitsprinzipien berücksichtigt (z. B. das Konzept der geringsten Funktionalität).	ec2-stopped-instance	Aktivieren Sie diese Regel, um bei der Basiskonfiguration von Amazon Elastic Compute Cloud (Amazon EC2) - Instances zu helfen, indem Sie überprüfen, ob EC2 Amazon-Instances gemäß den Standards Ihrer Organisation für mehr als die zulässige Anzahl von Tagen gestoppt wurden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.PO-P1	Es wird eine Basiskonfiguration der Informationstechnologie erstellt und verwaltet, die Sicherheitsprinzipien berücksichtigt (z. B. das Konzept der geringsten Funktionalität).	ec2- volume-inuse-check	Diese Regel stellt sicher, dass Amazon Elastic Block Store-Volumes, die an Amazon Elastic Compute Cloud (Amazon EC2) - Instances angehängt sind, zum Löschen markiert werden, wenn eine Instance beendet wird. Wenn ein Amazon-EBS-Volume nicht gelöscht wird, wenn die Instance, an die es angehängt ist, beendet wird, kann dies gegen das Konzept der geringsten Funktionalität verstoßen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.PO-P1	Es wird eine grundlegende Konfiguration der Informationstechnologie erstellt und verwaltet, die Sicherheitsprinzipien berücksichtigt (z. B. das Konzept der geringsten Funktionalität).	elb-deletion-protection-enabled	Diese Regel sorgt dafür, dass der Löschschutz für Elastic Load Balancing aktiviert ist. Verwenden Sie diese Funktion, um zu verhindern, dass Ihr Load Balancer versehentlich oder böswillig gelöscht wird, was zum Verlust der Verfügbarkeit Ihrer Anwendungen führen kann.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.PO-P1	Es wird eine Basiskonfiguration der Informationstechnologie geschaffen und beibehalten, die Sicherheitsprinzipien (z. B. das Konzept der geringsten Funktionalität) einbezieht.	restricted-common-ports	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass gemeinsame Ports für Amazon Elastic Compute Cloud (Amazon EC2) -Sicherheitsgruppen eingeschränkt sind. Wenn der Zugriff auf Ports nicht auf vertrauenswürdige Quellen beschränkt wird, kann dies zu Angriffen auf die Verfügbarkeit, Integrität und Vertraulichkeit von Systemen führen. Mit dieser Regel können Sie optional die Parameter blockedPort1–blockedPort5 festlegen (Standardkonfigurationen: 20, 21, 3389, 3306, 4333). Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.PO-P1	Es wird eine Basiskonfiguration der Informationstechnologie erstellt und verwaltet, die Sicherheitsprinzipien berücksichtigt (z. B. das Konzept der geringsten Funktionalität).	account-part-of-organizations	Durch die zentrale Verwaltung AWS-Konten innerhalb von AWS Organizations wird sichergestellt, dass die Konten den Vorschriften entsprechen. Eine fehlende zentrale Kontoverwaltung kann zu inkonsistenten Kontokonfigurationen führen, wodurch Ressourcen und sensible Daten offengelegt werden können.
AT-1: PR.PO-P10	Ein Plan für das Management von Schwachstellen wird entwickelt und umgesetzt.	vuln-management-plan-exists(Prozessüberprüfung)	Stellen Sie sicher, dass ein Plan für das Schwachstellenmanagement entwickelt und implementiert wird, damit Sie über formell definierte Prozesse zur Behebung von Schwachstellen in Ihrer Umgebung verfügen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.PO-P2	Verfahren zur Kontrolle von Konfigurationsände rungen sind eingerich tet und in Kraft.	elb-deletion-prote ction-enabled	Diese Regel sorgt dafür, dass der Löschschutz für Elastic Load Balancing aktiviert ist. Verwenden Sie diese Funktion, um zu verhindern, dass Ihr Load Balancer versehentlich oder böswillig gelöscht wird, was zum Verlust der Verfügbarkeit Ihrer Anwendungen führen kann.
PR.PO-P2	Verfahren zur Kontrolle von Konfigurationsände rungen sind eingerich tet und in Kraft.	rds-instance-deletion-protection-aktiviert	Stellen Sie sicher, dass Amazon Relational Database Service (Amazon RDS)-Instances den Löschschutz aktiviert haben. Verwenden Sie den Löschschu tz, um zu verhindern, dass Ihre Amazon-RD S-Instances versehent lich oder böswillig gelöscht werden, was zum Verlust der Verfügbarkeit Ihrer Anwendungen führen kann.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.PO-P3	Datensicherungen werden durchgeführt, verwaltet und getestet	db-instance-backup-enabled	Die Sicherungsfunktion von Amazon RDS erstellt Sicherungen Ihrer Datenbanken und Transaktionsprotokolle. Amazon RDS erstellt einen Snapshot für das Speichervolume Ihrer DB-Instance, sodass die gesamte DB-Instance gesichert wird. Sie können im System spezifische Aufbewahrungsfristen festlegen, um Ihre Ausfallsicherheitsanforderungen zu erfüllen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.PO-P3	Datensicherungen werden durchgeführt, verwaltet und getestet	dynamodb-in-backup-plan	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon DynamoDB-Tabellen Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.PO-P3	Datensicherungen werden durchgeführt, verwaltet und getestet	dynamodb-pitr-enabled	Aktivieren Sie diese Regel, um zu überprüfen, ob die Informationen gesichert wurden. Es verwaltet auch die Backups, indem es sicherstellt, dass die point-in-time Wiederherstellung in Amazon DynamoDB aktiviert ist. Bei der Wiederherstellung werden fortlaufende Backups Ihrer Tabelle für die letzten 35 Tage gespeichert.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.PO-P3	Datensicherungen werden durchgeführt, verwaltet und getestet	ebs-in-backup-plan	Stellen Sie zur Unterstützung der Datensicherungspro zesse sicher, dass Ihre Amazon Elastic Block Store (Amazon EBS) -Volumes Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwaltet er Backup-Service mit einer richtlini enbasierten Backup-Lösung. Diese Lösung vereinfac ht Ihr Sicherung smanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforde rungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.PO-P3	Datensicherungen werden durchgeführt, verwaltet und getestet	ebs-optimized-instance	Eine optimierte Instance im Amazon Elastic Block Store (Amazon EBS) bietet zusätzliche, dedizierte Kapazität für Amazon-EBS-I/O-Vorgänge. Diese Optimierung bietet die beste Leistung für Ihr EBS-Volume, indem Konflikte zwischen Amazon-EBS-I/O und anderem Datenverkehr von Ihrer Instance minimiert werden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.PO-P3	Datensicherungen werden durchgeführt, verwaltet und getestet	efs-in-backup-plan	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon Elastic File System (Amazon EFS) -Dateisysteme Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.PO-P3	Datensicherungen werden durchgeführt, verwaltet und getestet	elasticache-redis-cluster-automatic-Backup-Check	Wenn automatische Backups aktiviert sind, ElastiCache erstellt Amazon täglich ein Backup des Clusters. Die Sicherung kann für eine von Ihrer Organisation festgelegte Anzahl von Tagen aufbewahrt werden. Automatische Backups schützen vor Datenverlust. Bei einem Ausfall können Sie einen neuen Cluster erstellen, der Ihre Daten aus dem aktuellen Backup wiederherstellt.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.PO-P3	Datensicherungen werden durchgeführt, verwaltet und getestet	rds-in-backup-plan	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon Relational Database Service (Amazon RDS) -Instances Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.PO-P3	Datensicherungen werden durchgeführt, verwaltet und getestet	redshift-backup-enabled	Stellen Sie zur Unterstützung der Datensicherungsprozesse sicher, dass Ihre Amazon-Redshift-Cluster über automatisierte Snapshots verfügen. Wenn automatisierte Snapshots für einen Cluster aktiviert sind, erstellt Redshift in regelmäßigen Abständen Snapshots dieses Clusters. Standardmäßig erstellt Redshift alle acht Stunden oder alle 5 GB einen Snapshot für jeden Knoten mit Datenänderungen oder je nachdem, was zuerst eintritt.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.PO-P3	Datensicherungen werden durchgeführt, verwaltet und getestet	s3- bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) unterstützt die Aufrechterhaltung einer angemesse nen Kapazität und Verfügbarkeit. CRR ermöglicht das automatische, asynchrone Kopieren von Objekten in Amazon S3 Buckets, um die Datenverf ügbarkeit sicherzus tellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.PO-P3	Datensicherungen werden durchgeführt, verwaltet und getestet	s-3 bucket-versioning-enabled	Die Versionsv erwaltung von Amazon Simple Storage Service (Amazon S3)-Bucke ts hilft dabei, mehrere Varianten eines Objekts im selben Amazon-S3-Bucket zu speichern. Verwenden Sie die Versionsv erwaltung, um sämtliche Versionen aller Objekte in Ihrem Amazon-S3-Bucket zu speichern , abzurufen oder wiederherzustellen . Mit der Versionsv erwaltung können Sie Versionen sowohl nach unbeabsic htigten Benutzera ktionen als auch nach Anwendungsfehlern problemlos wiederher stellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.PO-P3	Datensicherungen werden durchgeführt, verwaltet und getestet	redshift-cluster-maintenancesettings-check	Diese Regel stellt sicher, dass Amazon-Redshift-Cluster die bevorzugten Einstellungen für Ihre Organisation haben. Insbesondere sorgt sie dafür, dass Cluster bevorzugte Wartungsfenster und automatisierte Aufbewahrungsfristen für Snapshots für die Datenbank haben. Für diese Regel müssen Sie die festlegen allowVersionUpgrade. Der Standardwert ist „true“. Außerdem können Sie optional den Zeitraum preferredMaintenanceWindow (der Standardwert ist sa: 16:00 -sa: 16:30) und den automated SnapshotRetention Zeitraum (der Standardwert ist 1) festlegen. Die tatsächlichen Werte müssen den Richtlini

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			en Ihrer Organisation entsprechen.
PR.PO-P3	Datensicherungen werden durchgeführt, verwaltet und getestet	aurora-resources-protected-by-Backup-Plan	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon Aurora Aurora-Ressourcen Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.PO-P3	Datensicherungen werden durchgeführt, verwaltet und getestet	backup-plan-min-frequency-and-min-retention-check	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihr AWS Backup-Plan auf eine Mindestfrequenz und Aufbewahrung festgelegt ist. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen. Mit dieser Regel können Sie die Parameter requiredFrequencyValue (Config default: 1), requiredRetentionDays (Config default: 35) und requiredFrequencyUnit

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			(Config default: days) festlegen. Der tatsächliche Wert muss den Anforderungen Ihrer Organisation entsprechen.
PR.PO-P3	Datensicherungen werden durchgeführt, verwaltet und getestet	backup-recovery-point-encrypted	Stellen Sie sicher, dass die Verschlüsselung für Ihre AWS Backup-Wiederherstellungspunkte aktiviert ist. Da sensible Daten auch im Ruhezustand vorhanden sein können, sollten Sie die Verschlüsselung im Ruhezustand aktivieren, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.PO-P3	Datensicherungen werden durchgeführt, verwaltet und getestet	backup-recovery-point-manual-Löschen-deaktiviert	Stellen Sie sicher, dass Ihren AWS Backup-Wiederherstellungspunkten eine ressourcenbasierte Richtlinie zugeordnet ist, die das Löschen von Wiederherstellungspunkten verhindert. Die Verwendung einer ressourcenbasierten Richtlinie zur Verhinderung des Löschens von Wiederherstellungspunkten kann dazu beitragen, ein versehentliches oder absichtliches Löschen zu unterbinden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.PO-P3	Datensicherungen werden durchgeführt, verwaltet und getestet	backup-recovery-point-minimum-Aufbewahrungsprüfung	Um bei Datensicherungsprozessen zu helfen, stellen Sie sicher, dass für Ihre AWS Backup-Wiederherstellungspunkte eine Mindestaufbewahrungsdauer festgelegt ist. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen. Mit dieser Regel können Sie den Parameter requiredRetentionDays (Config Default: 35) festlegen. Der tatsächliche Wert muss den Anforderu

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			ngen Ihrer Organisat ion entsprechen.
PR.PO-P3	Datensicherungen werden durchgeführt, verwaltet und getestet	ec2--Plan resources-protected-by-backup	Um Sie bei Datensich erungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon Elastic Compute Cloud (Amazon EC2) -Ressourc en Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwaltet er Backup-Service mit einer richtlini enbasierten Backup-Lösung. Diese Lösung vereinfac ht Ihr Sicherung smanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforde rungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.PO-P3	Datensicherungen werden durchgeführt, verwaltet und getestet	fsx-resources-protected-by-Backup-Plan	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre FSx Amazon-Dateisysteme Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.PO-P7	Reaktionspläne (Incident Response und Business Continuity) und Wiederherstellungspläne (Incident Recovery und Disaster Recovery) sind erstellt, vorhanden und werden verwaltet.	db-instance-backup-enabled	Die Sicherungsfunktion von Amazon RDS erstellt Sicherungen Ihrer Datenbanken und Transaktionsprotokolle. Amazon RDS erstellt einen Snapshot für das Speichervolume Ihrer DB-Instance, sodass die gesamte DB-Instance gesichert wird. Sie können im System spezifische Aufbewahrungsfristen festlegen, um Ihre Ausfallsicherheitsanforderungen zu erfüllen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.PO-P7	Reaktionspläne (Incident Response und Business Continuity) und Wiederherstellungspläne (Incident Recovery und Disaster Recovery) sind erstellt, vorhanden und werden verwaltet.	dynamodb-in-backup-plan	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon DynamoDB-Tabellen Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.PO-P7	Reaktionspläne (Incident Response und Business Continuity) und Wiederherstellungspläne (Incident Recovery und Disaster Recovery) sind erstellt, vorhanden und werden verwaltet.	dynamodb-pitr-enabled	Aktivieren Sie diese Regel, um zu überprüfen, ob die Informationen gesichert wurden. Es verwaltet auch die Backups, indem es sicherstellt, dass die point-in-time Wiederherstellung in Amazon DynamoDB aktiviert ist. Bei der Wiederherstellung werden fortlaufende Backups Ihrer Tabelle für die letzten 35 Tage gespeichert.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.PO-P7	Reaktionspläne (Incident Response und Business Continuity) und Wiederherstellungspläne (Incident Recovery und Disaster Recovery) sind erstellt, vorhanden und werden verwaltet.	ebs-in-backup-plan	Stellen Sie zur Unterstützung der Datensicherungsprozesse sicher, dass Ihre Amazon Elastic Block Store (Amazon EBS) -Volumes Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.PO-P7	Reaktionspläne (Incident Response und Business Continuity) und Wiederherstellungspläne (Incident Recovery und Disaster Recovery) sind erstellt, vorhanden und werden verwaltet.	efs-in-backup-plan	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon Elastic File System (Amazon EFS) -Dateisysteme Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.PO-P7	Reaktionspläne (Incident Response und Business Continuity) und Wiederherstellungspläne (Incident Recovery und Disaster Recovery) sind erstellt, vorhanden und werden verwaltet.	elasticache-redis-cluster-automatic-Backup-Check	Wenn automatische Backups aktiviert sind, ElastiCache erstellt Amazon täglich ein Backup des Clusters. Die Sicherung kann für eine von Ihrer Organisation festgelegte Anzahl von Tagen aufbewahrt werden. Automatische Backups schützen vor Datenverlust. Bei einem Ausfall können Sie einen neuen Cluster erstellen, der Ihre Daten aus dem aktuellen Backup wiederherstellt.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.PO-P7	Reaktionspläne (Incident Response und Business Continuity) und Wiederherstellungspläne (Incident Recovery und Disaster Recovery) sind erstellt, vorhanden und werden verwaltet.	rds-in-backup-plan	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon Relational Database Service (Amazon RDS) -Instances Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.PO-P7	Reaktionspläne (Incident Response und Business Continuity) und Wiederherstellungspläne (Incident Recovery und Disaster Recovery) sind erstellt, vorhanden und werden verwaltet.	redshift-backup-enabled	Stellen Sie zur Unterstützung der Datensicherungsprozesse sicher, dass Ihre Amazon-Redshift-Cluster über automatisierte Snapshots verfügen. Wenn automatisierte Snapshots für einen Cluster aktiviert sind, erstellt Redshift in regelmäßigen Abständen Snapshots dieses Clusters. Standardmäßig erstellt Redshift alle acht Stunden oder alle 5 GB einen Snapshot für jeden Knoten mit Datenänderungen oder je nachdem, was zuerst eintritt.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.PO-P7	Reaktionspläne (Incident Response und Business Continuity) und Wiederherstellungs pläne (Incident Recovery und Disaster Recovery) sind erstellt, vorhanden und werden verwaltet.	s3- bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) unterstützt die Aufrechterhaltung einer angemesse nen Kapazität und Verfügbarkeit. CRR ermöglicht das automatische, asynchrone Kopieren von Objekten in Amazon S3 Buckets, um die Datenverf ügbarkeit sicherzus tellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.PO-P7	Reaktionspläne (Incident Response und Business Continuity) und Wiederherstellungspläne (Incident Recovery und Disaster Recovery) sind erstellt, vorhanden und werden verwaltet.	s-3 bucket-versioning-enabled	Die Versionsverwaltung von Amazon Simple Storage Service (Amazon S3)-Buckets hilft dabei, mehrere Varianten eines Objekts im selben Amazon-S3-Bucket zu speichern. Verwenden Sie die Versionsverwaltung, um sämtliche Versionen aller Objekte in Ihrem Amazon-S3-Bucket zu speichern, abzurufen oder wiederherzustellen. Mit der Versionsverwaltung können Sie Versionen sowohl nach unbeabsichtigten Benutzeraktionen als auch nach Anwendungsfehlern problemlos wiederherstellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.PO-P7	Reaktionspläne (Incident Response und Business Continuity) und Wiederherstellungspläne (Incident Recovery und Disaster Recovery) sind erstellt, vorhanden und werden verwaltet.	aurora-resources-protected-by-Backup-Plan	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon Aurora Aurora-Ressourcen Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.PO-P7	Reaktionspläne (Incident Response und Business Continuity) und Wiederherstellungspläne (Incident Recovery und Disaster Recovery) sind erstellt, vorhanden und werden verwaltet.	backup-plan-min-frequency-and-min-retention-check	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihr AWS Backup-Plan auf eine Mindestfrequenz und Aufbewahrung festgelegt ist. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen. Mit dieser Regel können Sie die Parameter requiredFrequencyValue (Config default: 1), requiredRetentionDays (Config default: 35) und requiredFrequencyUnit

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			(Config default: days) festlegen. Der tatsächliche Wert muss den Anforderungen Ihrer Organisation entsprechen.
PR.PO-P7	Reaktionspläne (Incident Response und Business Continuity) und Wiederherstellungspläne (Incident Recovery und Disaster Recovery) sind erstellt, vorhanden und werden verwaltet.	backup-recovery-point-encrypted	Stellen Sie sicher, dass die Verschlüsselung für Ihre AWS Backup-Wiederherstellungspunkte aktiviert ist. Da sensible Daten auch im Ruhezustand vorhanden sein können, sollten Sie die Verschlüsselung im Ruhezustand aktivieren, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.PO-P7	Reaktionspläne (Incident Response und Business Continuity) und Wiederherstellungspläne (Incident Recovery und Disaster Recovery) sind erstellt, vorhanden und werden verwaltet.	backup-recovery-point-manual-Löschen-deaktiviert	Stellen Sie sicher, dass Ihren AWS Backup-Wiederherstellungspunkten eine ressourcenbasierte Richtlinie zugeordnet ist, die das Löschen von Wiederherstellungspunkten verhindert. Die Verwendung einer ressourcenbasierten Richtlinie zur Verhinderung des Löschens von Wiederherstellungspunkten kann dazu beitragen, ein versehentliches oder absichtliches Löschen zu unterbinden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.PO-P7	Reaktionspläne (Incident Response und Business Continuity) und Wiederherstellungspläne (Incident Recovery und Disaster Recovery) sind erstellt, vorhanden und werden verwaltet.	backup-recovery-point-minimum-Aufbewahrungsprüfung	Um bei Datensicherungsprozessen zu helfen, stellen Sie sicher, dass für Ihre AWS Backup-Wiederherstellungspunkte eine Mindestaufbewahrungsdauer festgelegt ist. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen. Mit dieser Regel können Sie den Parameter requiredRetentionDays (Config Default: 35) festlegen. Der tatsächliche Wert muss den Anforderu

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			ngen Ihrer Organisat ion entsprechen.
PR.PO-P7	Reaktionspläne (Incident Response und Business Continuity) und Wiederherstellungs pläne (Incident Recovery und Disaster Recovery) sind erstellt, vorhanden und werden verwaltet.	ec2--Plan resources-protected-by-backup	Um Sie bei Datensich erungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon Elastic Compute Cloud (Amazon EC2) -Ressourc en Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwaltet er Backup-Service mit einer richtlini enbasierten Backup-Lösung. Diese Lösung vereinfac ht Ihr Sicherung smanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforde rungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.PO-P7	Reaktionspläne (Incident Response und Business Continuity) und Wiederherstellungspläne (Incident Recovery und Disaster Recovery) sind erstellt, vorhanden und werden verwaltet.	fsx-resources-protected-by-Backup-Plan	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre FSx Amazon-Dateisysteme Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.PO-P8	Reaktions- und Wiederherstellungs pläne werden getestet.	response-plan-test ed(Prozessüberprüf ung)	Stellen Sie sicher, dass die Vorfallre aktions- und Wiederherstellungs pläne getestet wurden. Dies kann Ihnen helfen zu verstehen, ob Ihr Plan bei einem Vorfall wirksam ist und ob etwaige Lücken behoben oder Aktualisierungen vorgenommen werden müssen.
PR.PT-P2	Das Prinzip der geringsten Funktiona lität wird durch die Konfiguration von Systemen umgesetzt , die nur die wesentlic hen Funktionen bereitstellen.	dms-replication-not-public	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass auf DMS-Replikationsin stanzen nicht öffentlic h zugegriffen werden kann. DMS-Repli kations-Instances können vertrauli che Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.PT-P2	Das Prinzip der geringsten Funktionalität wird durch die Konfiguration von Systemen umgesetzt, die nur die wesentlichen Funktionen bereitstellen.	ebs-snapshot-public-restorable-überprüfen	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass EBS-Snapshots nicht öffentlich wiederherstellbar sind. EBS-Volume-Snapshots können vertrauliche Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.PT-P2	Das Prinzip der geringsten Funktionalität wird durch die Konfiguration von Systemen umgesetzt, die nur die wesentlichen Funktionen bereitstellen.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) kann Ihnen dabei helfen, die Prinzipien der geringsten Rechte und der Aufgabentrennung in Zugriffsberechtigungen und Autorisierungen zu integrieren und so zu verhindern, dass Richtlinien „Effect“: „Allow“ mit „Action“: „*“ anstelle von „Resource“: „*“ enthalten. Wenn Benutzern mehr Rechte eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und der Aufgabentrennung verstoßen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.PT-P2	Das Prinzip der geringsten Funktionalität wird durch die Konfiguration von Systemen umgesetzt, die nur die wesentlichen Funktionen bereitstellen.	iam-root-access-key-überprüfen	Der Zugriff auf Systeme und Ressourcen kann gesteuert werden, indem überprüft wird, ob der Root-Benutzer keine Zugriffsschlüssel mit seiner AWS Identity and Access Management (IAM) -Rolle verknüpft hat. Stellen Sie sicher, dass die Root-Zugriffsschlüssel gelöscht werden. Erstellen und verwenden Sie stattdessen rollenbasierte Funktionen, AWS-Konten um das Prinzip der geringsten Funktionalität zu berücksichtigen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.PT-P2	Das Prinzip der geringsten Funktionalität wird durch die Konfiguration von Systemen umgesetzt, die nur die wesentlichen Funktionen bereitstellen.	lambda-function-public-access-verboten	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass AWS Lambda-Funktionen nicht öffentlich zugänglich sind. Der öffentliche Zugriff kann möglicherweise die Verfügbarkeit von Ressourcen beeinträchtigen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.PT-P2	Das Prinzip der geringsten Funktionalität wird durch die Konfiguration von Systemen umgesetzt, die nur die wesentlichen Funktionen bereitstellen.	elasticsearch-in-vpc-only	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass sich Amazon OpenSearch OpenSearch Service (Service) - Domains innerhalb einer Amazon Virtual Private Cloud (Amazon VPC) befinden. Eine OpenSearch Service-Domain innerhalb einer Amazon VPC ermöglicht die sichere Kommunikation zwischen OpenSearch Service und anderen Services innerhalb der Amazon VPC, ohne dass ein Internet-Gateway, ein NAT-Gerät oder eine VPN-Verbindung erforderlich ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.PT-P3	Das Prinzip der geringsten Funktionalität wird durch die Konfiguration von Systemen umgesetzt, die nur die wesentlichen Funktionen bereitstellen.	opensearch-in-vpc-only	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass sich Amazon OpenSearch Service-Domains innerhalb einer Amazon Virtual Private Cloud (Amazon VPC) befinden. Eine Amazon OpenSearch Service-Domain innerhalb einer Amazon VPC ermöglicht die sichere Kommunikation zwischen Amazon OpenSearch Service und anderen Services innerhalb der Amazon VPC, ohne dass ein Internet-Gateway, ein NAT-Gerät oder eine VPN-Verbindung erforderlich ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.PT-P2	Das Prinzip der geringsten Funktionalität wird durch die Konfiguration von Systemen umgesetzt, die nur die wesentlichen Funktionen bereitstellen.	rds-snapshots-public-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Relational Database Service (Amazon RDS) -Instances nicht öffentlich sind. Amazon-RDS-Datenbank-Instances können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.PT-P2	Das Prinzip der geringsten Funktionalität wird durch die Konfiguration von Systemen umgesetzt, die nur die wesentlichen Funktionen bereitstellen.	redshift-cluster-public-access-überprüfen	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Redshift Redshift-Cluster nicht öffentlich sind. Amazon-Redshift-Cluster können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.PT-P2	Das Prinzip der geringsten Funktionalität wird durch die Konfiguration von Systemen umgesetzt, die nur die wesentlichen Funktionen bereitstellen.	s3- -Block-periodisch account-level-public-access	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Simple Storage Service (Amazon S3) -Buckets nicht öffentlich zugänglich sind. Diese Regel trägt dazu bei, sensible Daten vor unbefugten Remote-Benutzern zu schützen, indem sie den öffentlichen Zugriff verhindert. Mit dieser Regel können Sie optional die Parameter ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) und restrictPublicBuckets Parameter (Config Default: True) festlegen. Die tatsächlichen Werte müssen den Richtlini

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			en Ihrer Organisation entsprechen.
PR.PT-P2	Das Prinzip der geringsten Funktionalität wird durch die Konfiguration von Systemen umgesetzt, die nur die wesentlichen Funktionen bereitstellen.	s3- bucket-public-read-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie nur autorisierten Benutzern, Prozessen und Geräten Zugriff auf Amazon Simple Storage Service (Amazon S3) - Buckets gewähren. Die Verwaltung des Zugriffs sollte mit der Klassifizierung der Daten übereinstimmen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.PT-P2	Das Prinzip der geringsten Funktionalität wird durch die Konfiguration von Systemen umgesetzt, die nur die wesentlichen Funktionen bereitstellen.	s3- bucket-public-write-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie nur autorisierten Benutzern, Prozessen und Geräten Zugriff auf Amazon Simple Storage Service (Amazon S3) - Buckets gewähren. Die Verwaltung des Zugriffs sollte mit der Klassifizierung der Daten übereinstimmen.
PR.PT-P2	Das Prinzip der geringsten Funktionalität wird durch die Konfiguration von Systemen umgesetzt, die nur die wesentlichen Funktionen bereitstellen.	ec2- instance-no-public-ip	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon Elastic Compute Cloud (Amazon EC2) - Instances nicht öffentlich zugänglich sind. EC2 Amazon-Instances können vertrauliche Informationen enthalten, und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.PT-P2	Das Prinzip der geringsten Funktionalität wird durch die Konfiguration von Systemen umgesetzt, die nur die wesentlichen Funktionen bereitstellen.	emr-master-no-public-ip	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon EMR-Cluster-Masterknoten nicht öffentlich zugänglich sind. Amazon-EMR-Cluster-Hauptknoten können vertrauliche Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.PT-P2	Das Prinzip der geringsten Funktionalität wird durch die Konfiguration von Systemen umgesetzt, die nur die wesentlichen Funktionen bereitstellen.	ec-2 instances-in-vpc	Stellen Sie Amazon Elastic Compute Cloud (Amazon EC2) -Instances innerhalb einer Amazon Virtual Private Cloud (Amazon VPC) bereit, um eine sichere Kommunikation zwischen einer Instance und anderen Services innerhalb der Amazon VPC zu ermöglichen, ohne dass ein Internet-Gateway, ein NAT-Gerät oder eine VPN-Verbindung erforderlich ist. Der gesamte Datenverkehr bleibt sicher in der AWS Cloud. Domains, die sich innerhalb einer VPC befinden, verfügen aufgrund ihrer logischen Isolierung im Vergleich zu Domains mit öffentlichen Endpunkten über eine zusätzliche Sicherheitsebene. Weisen Sie EC2

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			Amazon-Instances einer Amazon-VPC zu, um den Zugriff ordnungsgemäß zu verwalten.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.PT-P2	Das Prinzip der geringsten Funktionalität wird durch die Konfiguration von Systemen umgesetzt, die nur die wesentlichen Funktionen bereitstellen.	lambda-inside-vpc	Stellen Sie AWS Lambda-Funktionen in einer Amazon Virtual Private Cloud (Amazon VPC) bereit, um eine sichere Kommunikation zwischen einer Funktion und anderen Diensten innerhalb der Amazon VPC zu gewährleisten. Bei dieser Konfiguration sind kein Internet-Gateway, kein NAT-Gerät und keine VPN-Verbindung erforderlich. Der gesamte Datenverkehr bleibt sicher in der Cloud. AWS Domains, die sich innerhalb einer VPC befinden, verfügen aufgrund ihrer logischen Isolierung im Vergleich zu Domains mit öffentlichen Endpunkten über eine zusätzliche Sicherheitsebene. Um den Zugriff ordnungsgemäß zu verwalten,

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			sollten AWS Lambda-Funktionen einer VPC zugewiesen werden.
PR.PT-P2	Das Prinzip der geringsten Funktionalität wird durch die Konfiguration von Systemen umgesetzt, die nur die wesentlichen Funktionen bereitstellen.	rds-instance-public-access-überprüfen	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Relational Database Service (Amazon RDS) -Instances nicht öffentlich sind. Amazon-RDS-Datenbank-Instances können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.PT-P2	Das Prinzip der geringsten Funktionalität wird durch die Konfiguration von Systemen umgesetzt, die nur die wesentlichen Funktionen bereitstellen.	sagemaker-notebook-no-direct-Internetzugang	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass SageMaker Amazon-Notebooks keinen direkten Internetzugang zulassen. Indem Sie direkten Internetzugang blockieren, vermeiden Sie, dass unbefugte Benutzer auf sensible Daten zugreifen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.PT-P2	Das Prinzip der geringsten Funktionalität wird durch die Konfiguration von Systemen umgesetzt, die nur die wesentlichen Funktionen bereitstellen.	subnet-auto-assign-public-ip-deaktiviert	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon Virtual Private Cloud (VPC) -Subnetzen nicht automatisch eine öffentliche IP-Adresse zugewiesen wird. Amazon Elastic Compute Cloud (EC2) -Instances, die in Subnetzen gestartet werden, in denen dieses Attribut aktiviert ist, haben ihrer primären Netzwerkschnittstelle eine öffentliche IP-Adresse zugewiesen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.PT-P2	Das Prinzip der geringsten Funktionalität wird durch die Konfiguration von Systemen umgesetzt, die nur die wesentlichen Funktionen bereitstellen.	s3- bucket-policy-grantee-check	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie s3_bucket_policy_grantee_check aktivieren. Diese Regel prüft, ob der vom Amazon S3 S3-Bucket gewährte Zugriff durch die von Ihnen bereitgestellten AWS Principals, Verbundbenutzer, Service Principals, IP-Adressen oder Amazon Virtual Private Cloud (Amazon VPC) IDs eingeschränkt ist.
PR.PT-P2	Das Prinzip der geringsten Funktionalität wird durch die Konfiguration von Systemen umgesetzt, die nur die wesentlichen Funktionen bereitstellen.	ec2- instance-profile-attached	EC2 Instanzprofile übergeben eine IAM-Rolle an eine EC2 Instance. Das Anhängen eines Instance-Profils an Ihre Instances kann bei der Implementierung von geringsten Berechtigungen und der Berechtigungsverwaltung helfen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.PT-P2	Das Prinzip der geringsten Funktionalität wird durch die Konfiguration von Systemen umgesetzt, die nur die wesentlichen Funktionen bereitstellen.	ssm-document-not-public	Stellen Sie sicher, dass AWS Systems Manager (SSM) - Dokumente nicht öffentlich sind, da dies einen unbeabsichtigten Zugriff auf Ihre SSM-Dokumente ermöglichen kann. Ein öffentliches SSM-Dokument kann Informationen über Ihr Konto, Ihre Ressourcen und internen Prozesse preisgeben.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.PT-P2	Das Prinzip der geringsten Funktionalität wird durch die Konfiguration von Systemen umgesetzt, die nur die wesentlichen Funktionen bereitstellen.	autoscaling-launch-config-public-ip-deaktiviert	Wenn Sie Ihre Netzwerkschnittstellen mit einer öffentlichen IP-Adresse konfigurieren, sind die diesen Netzwerkschnittstellen zugehörigen Ressourcen über das Internet erreichbar. EC2 Ressourcen sollten nicht öffentlich zugänglich sein, da dies einen unbeabsichtigten Zugriff auf Ihre Anwendungen oder Server ermöglichen kann.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.PT-P2	Das Prinzip der geringsten Funktionalität wird durch die Konfiguration von Systemen umgesetzt, die nur die wesentlichen Funktionen bereitstellen.	redshift-enhanced-vpc-routing-aktiviert	Mit Enhanced-VPC-Routing wird erzwungen, dass der gesamte COPY- und UNLOAD-Datenverkehr zwischen Ihrem Cluster und Datenrepositorys über Ihre Amazon VPC erfolgt. Anschließend können Sie VPC-Features wie Sicherheitsgruppen und Netzwerkzugriffskontrolllisten verwenden, um den Netzwerkverkehr zu schützen. Sie können auch VPC-Flow-Logs verwenden, um den Netzwerkverkehr zu überwachen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.PT-P3	Kommunikations- und Kontrollnetzwerke sind geschützt.	ec2- instances-in-vpc	Stellen Sie Amazon Elastic Compute Cloud (Amazon EC2) -Instances innerhalb einer Amazon Virtual Private Cloud (Amazon VPC) bereit, um eine sichere Kommunika tion zwischen einer Instance und anderen Services innerhalb der Amazon VPC zu ermöglichen, ohne dass ein Internet-Gateway, ein NAT-Gerät oder eine VPN-Verbindung erforderlich ist. Der gesamte Datenverk ehr bleibt sicher in der AWS Cloud. Domains, die sich innerhalb einer VPC befinden, verfügen aufgrund ihrer logischen Isolierun g im Vergleich zu Domains mit öffentlic hen Endpunkten über eine zusätzlic he Sicherheitsebene. Weisen Sie EC2

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			Amazon-Instances einer Amazon-VPC zu, um den Zugriff ordnungsgemäß zu verwalten.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.PT-P3	Kommunikations- und Kontrollnetzwerke sind geschützt.	restricted-common-ports	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass gemeinsame Ports für Amazon Elastic Compute Cloud (Amazon EC2) -Sicherheitsgruppen eingeschränkt sind. Wenn der Zugriff auf Ports nicht auf vertrauenswürdige Quellen beschränkt wird, kann dies zu Angriffen auf die Verfügbarkeit, Integrität und Vertraulichkeit von Systemen führen. Mit dieser Regel können Sie optional die Parameter blockedPort1–blockedPort5 festlegen (Standardkonfigurationen: 20, 21, 3389, 3306, 4333). Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.PT-P3	Kommunikations- und Kontrollnetzwerke sind geschützt.	acm-certificate-expiration-check	Stellen Sie sicher, dass die Netzwerkintegrität geschützt ist, indem Sie sicherstellen, dass X509-Zertifikate von AWS ACM ausgestellt werden. Diese Zertifikate müssen gültig und dürfen nicht abgelaufen sein. Für diese Regel ist ein Wert für erforderlich daysToExpiration (Wert für bewährte AWS Grundregeln für Sicherheit: 90). Der tatsächliche Wert muss den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.PT-P3	Kommunikations- und Kontrollnetzwerke sind geschützt.	dms-replication-not-public	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass auf DMS-Replikationsin stanzen nicht öffentlic h zugegriffen werden kann. DMS-Repli kations-Instances können vertrauli che Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.
PR.PT-P3	Kommunikations- und Kontrollnetzwerke sind geschützt.	ebs-snapshot-public-restorable-überprüfen	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass EBS-Snapshots nicht öffentlich wiederher stellbar sind. EBS-Volume-Snapsho ts können vertrauli che Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.PT-P3	Kommunikations- und Kontrollnetzwerke sind geschützt.	vpc-default-security-group-geschlossen	Sicherheitsgruppen von Amazon Elastic Compute Cloud (Amazon EC2) können bei der Verwaltung des Netzwerkzugriffs helfen, indem sie eine statusbehaftete Filterung des ein- und ausgehenden Netzwerkverkehrs zu Ressourcen bereitstellen. AWS Die Beschränk ung des gesamten Datenverkehrs auf die Standardsicherheit sgruppe hilft dabei, den Fernzugriff auf Ihre Ressourcen einzuschränken. AWS

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.PT-P3	Kommunikations- und Kontrollnetzwerke sind geschützt.	ec2- instance-no-public-ip	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon Elastic Compute Cloud (Amazon EC2) - Instances nicht öffentlich zugänglich sind. EC2 Amazon-Instances können vertrauliche Informationen enthalten, und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.PT-P3	Kommunikations- und Kontrollnetzwerke sind geschützt.	elasticsearch-in-vpc-only	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass sich Amazon OpenSearch OpenSearch Service (Service) - Domains innerhalb einer Amazon Virtual Private Cloud (Amazon VPC) befinden. Eine OpenSearch Service-Domain innerhalb einer Amazon VPC ermöglicht die sichere Kommunikation zwischen OpenSearch Service und anderen Services innerhalb der Amazon VPC, ohne dass ein Internet-Gateway, ein NAT-Gerät oder eine VPN-Verbindung erforderlich ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.PT-P3	Kommunikations- und Kontrollnetzwerke sind geschützt.	opensearch-in-vpc-only	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass sich Amazon OpenSearch Service-Domains innerhalb einer Amazon Virtual Private Cloud (Amazon VPC) befinden. Eine Amazon OpenSearch Service-Domain innerhalb einer Amazon VPC ermöglicht die sichere Kommunikation zwischen Amazon OpenSearch Service und anderen Services innerhalb der Amazon VPC, ohne dass ein Internet-Gateway, ein NAT-Gerät oder eine VPN-Verbindung erforderlich ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.PT-P3	Kommunikations- und Kontrollnetzwerke sind geschützt.	emr-master-no-public-ip	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon EMR-Cluster-Masterknoten nicht öffentlich zugänglich sind. Amazon-EMR-Cluster-Hauptknoten können vertrauliche Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.
PR.PT-P3	Kommunikations- und Kontrollnetzwerke sind geschützt.	lambda-function-public-access-verboten	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass AWS Lambda-Funktionen nicht öffentlich zugänglich sind. Der öffentliche Zugriff kann möglicherweise die Verfügbarkeit von Ressourcen beeinträchtigen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.PT-P3	Kommunikations- und Kontrollnetzwerke sind geschützt.	lambda-inside-vpc	Stellen Sie AWS Lambda-Funktionen in einer Amazon Virtual Private Cloud (Amazon VPC) bereit, um eine sichere Kommunika tion zwischen einer Funktion und anderen Diensten innerhalb der Amazon VPC zu gewährleisten. Bei dieser Konfiguration sind kein Internet-Gateway, kein NAT-Gerät und keine VPN-Verbindung erforderlich. Der gesamte Datenverk ehr bleibt sicher in der Cloud. AWS Domains, die sich innerhalb einer VPC befinden, verfügen aufgrund ihrer logischen Isolierun g im Vergleich zu Domains mit öffentlic hen Endpunkten über eine zusätzliche Sicherheitsebene. Um den Zugriff ordnungsg emäß zu verwalten,

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			sollten AWS Lambda-Funktionen einer VPC zugewiesen werden.
PR.PT-P3	Kommunikations- und Kontrollnetzwerke sind geschützt.	rds-snapshots-public-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Relational Database Service (Amazon RDS) -Instances nicht öffentlich sind. Amazon-RDS-Datenbank-Instances können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.PT-P3	Kommunikations- und Kontrollnetzwerke sind geschützt.	rds-instance-public-access-überprüfen	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Relational Database Service (Amazon RDS) -Instances nicht öffentlich sind. Amazon-RDS-Datenbank-Instances können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.PT-P3	Kommunikations- und Kontrollnetzwerke sind geschützt.	redshift-cluster-public-access-überprüfen	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Redshift Redshift-Cluster nicht öffentlich sind. Amazon-Redshift-Cluster können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.PT-P3	Kommunikations- und Kontrollnetzwerke sind geschützt.	s3- -Block-periodisch account-level-public-access	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Simple Storage Service (Amazon S3) -Buckets nicht öffentlich zugänglich sind. Diese Regel trägt dazu bei, sensible Daten vor unbefugten Remote-Benutzern zu schützen, indem sie den öffentlichen Zugriff verhindert. Mit dieser Regel können Sie optional die Parameter ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) und restrictPublicBuckets Parameter (Config Default: True) festlegen. Die tatsächlichen Werte müssen den Richtlini

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			en Ihrer Organisation entsprechen.
PR.PT-P3	Kommunikations- und Kontrollnetzwerke sind geschützt.	s3- bucket-public-read -prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie nur autorisierten Benutzern, Prozessen und Geräten Zugriff auf Amazon Simple Storage Service (Amazon S3) - Buckets gewähren. Die Verwaltung des Zugriffs sollte mit der Klassifizierung der Daten übereinst immen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.PT-P3	Kommunikations- und Kontrollnetzwerke sind geschützt.	s3- bucket-public-write-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie nur autorisierten Benutzern, Prozessen und Geräten Zugriff auf Amazon Simple Storage Service (Amazon S3) - Buckets gewähren. Die Verwaltung des Zugriffs sollte mit der Klassifizierung der Daten übereinstimmen.
PR.PT-P3	Kommunikations- und Kontrollnetzwerke sind geschützt.	sagemaker-notebook-no-direct-Internetzugang	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass SageMaker Amazon-Notebooks keinen direkten Internetzugang zulassen. Indem Sie direkten Internetzugang blockieren, vermeiden Sie, dass unbefugte Benutzer auf sensible Daten zugreifen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.PT-P3	Kommunikations- und Kontrollnetzwerke sind geschützt.	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) Security Groups können bei der Verwaltung des Netzwerkzugriffs helfen, indem sie eine statusbeh aftete Filterung von eingehendem und ausgehendem Netzwerkverkehr zu Ressourcen bereitste llen. AWS Wenn Sie eingehenden (oder entfernten) Datenverk ehr von 0.0.0.0/0 bis Port 22 auf Ihren Ressourcen nicht zulassen, können Sie den Remote-Zugriff einschränken.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.PT-P3	Kommunikations- und Kontrollnetzwerke sind geschützt.	vpc-sg-open-only-to-authorized-ports	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass gemeinsame Ports für Amazon Elastic Compute Cloud (Amazon EC2) -Sicherheitsgruppen eingeschränkt sind. Wenn der Zugriff auf Ports nicht auf vertrauenswürdige Quellen beschränkt wird, kann dies zu Angriffen auf die Verfügbarkeit, Integrität und Vertraulichkeit von Systemen führen. Durch die Beschränkung des Zugriffs auf Ressourcen innerhalb einer Sicherheitsgruppe aus dem Internet (0.0.0.0/0) kann der Fernzugriff auf interne Systeme gesteuert werden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.PT-P3	Kommunikations- und Kontrollnetzwerke sind geschützt.	subnet-auto-assign-public-ip-deaktiviert	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon Virtual Private Cloud (VPC) -Subnetzen nicht automatisch eine öffentliche IP-Adresse zugewiesen wird. Amazon Elastic Compute Cloud (EC2) -Instances, die in Subnetzen gestartet werden, in denen dieses Attribut aktiviert ist, haben ihrer primären Netzwerkschnittstelle eine öffentliche IP-Adresse zugewiesen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.PT-P3	Kommunikations- und Kontrollnetzwerke sind geschützt.	no-unrestricted-route-to-igw	Stellen Sie sicher, dass EC2 Amazon-Routentabellen keine uneingeschränkten Routen zu einem Internet-Gateway enthalten. Durch das Entfernen oder Beschränken des Internetzugangs für Workloads innerhalb von Amazon VPCs können unbeabsichtigte Zugriffe in Ihrer Umgebung reduziert werden.
PR.PT-P3	Kommunikations- und Kontrollnetzwerke sind geschützt.	ssm-document-not-public	Stellen Sie sicher, dass AWS Systems Manager (SSM) - Dokumente nicht öffentlich sind, da dies einen unbeabsichtigten Zugriff auf Ihre SSM-Dokumente ermöglichen kann. Ein öffentliches SSM-Dokument kann Informationen über Ihr Konto, Ihre Ressourcen und internen Prozesse preisgeben.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.PT-P3	Kommunikations- und Kontrollnetzwerke sind geschützt.	autoscaling-launch-config-public-ip-deaktiviert	Wenn Sie Ihre Netzwerkschnittstellen mit einer öffentlichen IP-Adresse konfigurieren, sind die diesen Netzwerkschnittstellen zugehörigen Ressourcen über das Internet erreichbar. EC2 Ressourcen sollten nicht öffentlich zugänglich sein, da dies einen unbeabsichtigten Zugriff auf Ihre Anwendungen oder Server ermöglichen kann.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.PT-P4	Mechanismen (z. B. Failsafe, Load Balancing, Hot-Swap) werden implement iert, um die Anforderu ngen an die Ausfallsi cherheit in normalen und widrigen Situation en zu erfüllen.	autoscaling-group-elb-healthcheck-er forderlich	Die Elastic Load Balancer (ELB) - Zustandsprüfungen für Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling Scaling-G ruppen unterstützen die Aufrechterhaltung einer angemesse nen Kapazität und Verfügbarkeit. Der Load Balancer sendet regelmäßig Pings, versucht Verbindun gen herzustellen oder sendet Anfragen, um den Zustand der EC2 Amazon-Instances in einer Gruppe mit auto-scal ing zu testen. Wenn eine Instance nicht zurückmeldet, wird der Traffic an eine neue EC2 Amazon-In stance gesendet.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.PT-P4	Mechanismen (z. B. Failsafe, Load Balancing, Hot-Swap) werden implement iert, um die Anforderu ngen an die Ausfallsi cherheit in normalen und widrigen Situation en zu erfüllen.	dynamodb-in-backup-plan	Um Sie bei Datensich erungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon DynamoDB-Tabellen Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwaltet er Backup-Service mit einer richtlini enbasierten Backup-Lösung. Diese Lösung vereinfac ht Ihr Sicherung smanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforde rungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.PT-P4	Mechanismen (z. B. Failsafe, Load Balancing, Hot-Swap) werden implement iert, um die Anforderu ngen an die Ausfallsi cherheit in normalen und widrigen Situation en zu erfüllen.	ebs-in-backup-plan	Stellen Sie zur Unterstützung der Datensicherungspro zesse sicher, dass Ihre Amazon Elastic Block Store (Amazon EBS) -Volumes Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwaltet er Backup-Service mit einer richtlini enbasierten Backup-Lösung. Diese Lösung vereinfac ht Ihr Sicherung smanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforde rungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.PT-P4	Mechanismen (z. B. Failsafe, Load Balancing, Hot-Swap) werden implementiert, um die Anforderungen an die Ausfallsicherheit in normalen und widrigen Situationen zu erfüllen.	dynamodb-autoscaling-enabled	Amazon DynamoDB Auto Scaling verwendet den AWS Application Auto Scaling-Service, um die bereitgestellte Durchsatzkapazität so anzupassen, dass sie automatisch auf tatsächliche Verkehrsmuster reagiert. Auf diese Weise kann eine Tabelle oder ein globaler sekundärer Index die bereitgestellte Lese-/Schreibkapazität erhöhen, um plötzliche Erhöhungen des Datenverkehrs ohne Drosselung zu bewältigen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.PT-P4	Mechanismen (z. B. Failsafe, Load Balancing, Hot-Swap) werden implementiert, um die Anforderungen an die Ausfallsicherheit in normalen und ungünstigen Situationen zu erfüllen.	dynamodb-pitr-enabled	Aktivieren Sie diese Regel, um zu überprüfen, ob die Informationen gesichert wurden. Es verwaltet auch die Backups, indem es sicherstellt, dass die point-in-time Wiederherstellung in Amazon DynamoDB aktiviert ist. Bei der Wiederherstellung werden fortlaufende Backups Ihrer Tabelle für die letzten 35 Tage gespeichert.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.PT-P4	Mechanismen (z. B. Failsafe, Load Balancing, Hot-Swap) werden implement iert, um die Anforderu ngen an die Ausfallsi cherheit in normalen und widrigen Situation en zu erfüllen.	elasticache-redis-cluster-automatic-Backup-Check	Wenn automatische Backups aktiviert sind, ElastiCache erstellt Amazon täglich ein Backup des Clusters. Die Sicherung kann für eine von Ihrer Organisation festgelegte Anzahl von Tagen aufbewahrt werden. Automatische Backups schützen vor Datenverlust. Bei einem Ausfall können Sie einen neuen Cluster erstellen, der Ihre Daten aus dem aktuellen Backup wiederherstellt.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.PT-P4	Mechanismen (z. B. Failsafe, Load Balancing, Hot-Swap) werden implementiert, um die Anforderungen an die Ausfallsicherheit in normalen und widrigen Situationen zu erfüllen.	elb-cross-zone-load-Balancing aktiviert	Aktivieren Sie zonenübergreifendes Load Balancing für Ihre Elastic Load Balancer (ELBs), um eine angemessene Kapazität und Verfügbarkeit aufrechtzuerhalten. Zonenübergreifendes Load Balancing reduziert die Notwendigkeit, die gleiche Anzahl von Instances in jeder aktivierten Availability Zone aufrechtzuerhalten. Es verbessert auch die Fähigkeit Ihrer Anwendung, den Verlust einer oder mehrerer Instances zu bewältigen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.PT-P4	Mechanismen (z. B. Failsafe, Load Balancing, Hot-Swap) werden implementiert, um die Anforderungen an die Ausfallsicherheit in normalen und widrigen Situationen zu erfüllen.	efs-in-backup-plan	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon Elastic File System (Amazon EFS) -Dateisysteme Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.PT-P4	Mechanismen (z. B. Failsafe, Load Balancing, Hot-Swap) werden implementiert, um die Anforderungen an die Ausfallsicherheit in normalen und widrigen Situationen zu erfüllen.	elb-deletion-protection-enabled	Diese Regel sorgt dafür, dass der Löschschutz für Elastic Load Balancing aktiviert ist. Verwenden Sie diese Funktion, um zu verhindern, dass Ihr Load Balancer versehentlich oder böswillig gelöscht wird, was zum Verlust der Verfügbarkeit Ihrer Anwendungen führen kann.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.PT-P4	Mechanismen (z. B. Failsafe, Load Balancing, Hot-Swap) werden implementiert, um die Anforderungen an die Widerstandsfähigkeit in normalen und widrigen Situationen zu erfüllen.	rds-in-backup-plan	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon Relational Database Service (Amazon RDS) -Instances Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.PT-P4	Mechanismen (z. B. Failsafe, Load Balancing, Hot-Swap) werden implement iert, um die Anforderu ngen an die Ausfallsi cherheit in normalen und widrigen Situation en zu erfüllen.	db-instance-backup-enabled	Die Sicherung sfunktion von Amazon RDS erstellt Sicherung en Ihrer Datenbank en und Transakti onsprotokolle. Amazon RDS erstellt einen Snapshot für das Speichervolume Ihrer DB-Instance, sodass die gesamte DB-Instance gesichert wird. Sie können im System spezifische Aufbewahrungsfrist en festlegen, um Ihre Ausfallsicherheits anforderungen zu erfüllen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.PT-P4	Mechanismen (z. B. Failsafe, Load Balancing, Hot-Swap) werden implementiert, um die Anforderungen an die Widerstandsfähigkeit in normalen und widrigen Situationen zu erfüllen.	rds-multi-az-support	Die Multi-AZ-Unterstützung in Amazon Relational Database Service (Amazon RDS) bietet eine verbesserte Verfügbarkeit und Beständigkeit von Datenbank-Instances. Wenn Sie eine Multi-AZ-Datenbank-Instance bereitstellen, erstellt Amazon RDS automatisch eine primäre Datenbank-Instance und repliziert die Daten synchron auf eine Standby-Instance in einer anderen Availability Zone. Jede Availability Zone läuft auf einer eigenen, physisch getrennten, unabhängigen Infrastruktur und ist auf eine hohe Verfügbarkeit ausgelegt. Im Falle eines Infrastrukturausfalls führt Amazon RDS einen automatis

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			chen Failover zum Standby-Modus durch, sodass Sie den Datenbankbetrieb wieder aufnehmen können, sobald der Failover abgeschlo ssen ist.
PR.PT-P4	Mechanismen (z. B. Failsafe, Load Balancing, Hot-Swap) werden implementiert, um die Anforderungen an die Widerstandsfähigke it in normalen und widrigen Situationen zu erfüllen.	rds-instance-deletion-protection-aktiviert	Stellen Sie sicher, dass Amazon Relational Database Service (Amazon RDS)-Instances den Löschschutz aktiviert haben. Verwenden Sie den Löschschu tz, um zu verhindern, dass Ihre Amazon-RD S-Instances versehent lich oder böswillig gelöscht werden, was zum Verlust der Verfügbarkeit Ihrer Anwendungen führen kann.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.PT-P4	Mechanismen (z. B. Failsafe, Load Balancing, Hot-Swap) werden implement iert, um die Anforderu ngen an die Ausfallsi cherheit in normalen und ungünstigen Situationen zu erfüllen.	s-3 bucket-versioning-enabled	Die Versionsv erwaltung von Amazon Simple Storage Service (Amazon S3)-Bucke ts hilft dabei, mehrere Varianten eines Objekts im selben Amazon-S3-Bucket zu speichern. Verwenden Sie die Versionsv erwaltung, um sämtliche Versionen aller Objekte in Ihrem Amazon-S3-Bucket zu speichern , abzurufen oder wiederherzustellen . Mit der Versionsv erwaltung können Sie Versionen sowohl nach unbeabsic htigten Benutzera ktionen als auch nach Anwendungsfehlern problemlos wiederher stellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.PT-P4	Mechanismen (z. B. Failsafe, Load Balancing, Hot-Swap) werden implementiert, um die Anforderungen an die Ausfallsicherheit in normalen und widrigen Situationen zu erfüllen.	redshift-backup-enabled	Stellen Sie zur Unterstützung der Datensicherungsprozesse sicher, dass Ihre Amazon-Redshift-Cluster über automatisierte Snapshots verfügen. Wenn automatisierte Snapshots für einen Cluster aktiviert sind, erstellt Redshift in regelmäßigen Abständen Snapshots dieses Clusters. Standardmäßig erstellt Redshift alle acht Stunden oder alle 5 GB einen Snapshot für jeden Knoten mit Datenänderungen oder je nachdem, was zuerst eintritt.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.PT-P4	Mechanismen (z. B. Failsafe, Load Balancing, Hot-Swap) werden implement iert, um die Anforderu ngen an die Ausfallsi cherheit in normalen und widrigen Situation en zu erfüllen.	s-3 bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) unterstützt die Aufrechterhaltung einer angemesse nen Kapazität und Verfügbarkeit. CRR ermöglicht das automatische, asynchrone Kopieren von Objekten in Amazon S3 Buckets, um die Datenverf ügbarkeit sicherzus tellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.PT-P4	Mechanismen (z. B. Failsafe, Load Balancing, Hot-Swap) werden implement iert, um die Anforderu ngen an die Ausfallsi cherheit in normalen und widrigen Situation en zu erfüllen.	vpc-vpn-2-tunnels-up	Redundante Site-to-Site VPN-Tunne l können implement iert werden, um die Anforderungen an die Ausfallsicherheit zu erfüllen. Es verwendet zwei Tunnel, um die Konnektivität sicherzustellen, falls eine der Site-to-Site VPN-Verbindungen nicht verfügbar ist. Um sich vor einem Verbindungsverlust zu schützen, können Sie für den Fall, dass Ihr Kunden-Gateway nicht verfügbar ist, eine zweite Site-to-S ite VPN-Verbindung zu Ihrer Amazon Virtual Private Cloud (Amazon VPC) und Ihrem Virtual Private Gateway einrichten, indem Sie ein zweites Kunden-Gateway verwenden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.PT-P4	Mechanismen (z. B. Failsafe, Load Balancing, Hot-Swap) werden implementiert, um die Anforderungen an die Ausfallsicherheit in normalen und widrigen Situationen zu erfüllen.	aurora-resources-protected-by-Backup-Plan	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon Aurora Aurora-Ressourcen Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.PT-P4	Mechanismen (z. B. Failsafe, Load Balancing, Hot-Swap) werden implementiert, um die Anforderungen an die Ausfallsicherheit in normalen und widrigen Situationen zu erfüllen.	backup-plan-min-frequency-and-min-retention-check	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihr AWS Backup-Plan auf eine Mindestfrequenz und Aufbewahrung festgelegt ist. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen. Mit dieser Regel können Sie die Parameter requiredFrequencyValue (Config default: 1), requiredRetentionDays (Config default: 35) und requiredFrequencyUnit

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			(Config default: days) festlegen. Der tatsächliche Wert muss den Anforderungen Ihrer Organisation entsprechen.
PR.PT-P4	Mechanismen (z. B. Failsafe, Load Balancing, Hot-Swap) werden implementiert, um die Anforderungen an die Ausfallsicherheit in normalen und widrigen Situationen zu erfüllen.	backup-recovery-point-encrypted	Stellen Sie sicher, dass die Verschlüsselung für Ihre AWS Backup-Wiederherstellungspunkte aktiviert ist. Da sensible Daten auch im Ruhezustand vorhanden sein können, sollten Sie die Verschlüsselung im Ruhezustand aktivieren, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.PT-P4	Mechanismen (z. B. Failsafe, Load Balancing, Hot-Swap) werden implementiert, um die Anforderungen an die Ausfallsicherheit in normalen und widrigen Situationen zu erfüllen.	backup-recovery-point-manual-Löschen-deaktiviert	Stellen Sie sicher, dass Ihren AWS Backup-Wiederherstellungspunkten eine ressourcenbasierte Richtlinie zugeordnet ist, die das Löschen von Wiederherstellungspunkten verhindert. Die Verwendung einer ressourcenbasierten Richtlinie zur Verhinderung des Löschens von Wiederherstellungspunkten kann dazu beitragen, ein versehentliches oder absichtliches Löschen zu unterbinden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.PT-P4	Mechanismen (z. B. Failsafe, Load Balancing, Hot-Swap) werden implementiert, um die Anforderungen an die Ausfallsicherheit in normalen und widrigen Situationen zu erfüllen.	backup-recovery-point-minimum-Aufbewahrungsprüfung	Um bei Datensicherungsprozessen zu helfen, stellen Sie sicher, dass für Ihre AWS Backup-Wiederherstellungspunkte eine Mindestaufbewahrungsdauer festgelegt ist. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen. Mit dieser Regel können Sie den Parameter requiredRetentionDays (Config Default: 35) festlegen. Der tatsächliche Wert muss den Anforderu

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			ngen Ihrer Organisat ion entsprechen.
PR.PT-P4	Mechanismen (z. B. Failsafe, Load Balancing, Hot-Swap) werden implement iert, um die Anforderu ngen an die Ausfallsi cherheit in normalen und widrigen Situation en zu erfüllen.	ec2-Plan resources-protected-by-backup	Um Sie bei Datensich erungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon Elastic Compute Cloud (Amazon EC2) -Ressourc en Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwaltet er Backup-Service mit einer richtlini enbasierten Backup-Lösung. Diese Lösung vereinfac ht Ihr Sicherung smanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforde rungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
PR.PT-P4	Mechanismen (z. B. Failsafe, Load Balancing, Hot-Swap) werden implementiert, um die Anforderungen an die Ausfallsicherheit in normalen und widrigen Situationen zu erfüllen.	fsx-resources-protected-by-Backup-Plan	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre FSx Amazon-Dateisysteme Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Vorlage

Die Vorlage ist verfügbar unter GitHub: Operational Best Practices for NIST Privacy Framework v1.0.

Bewährte Methoden für die Ausführung von NYDFS 23

Konformitätspakete bieten ein allgemeines Compliance-Framework, das es Ihnen ermöglicht, mithilfe verwalteter oder benutzerdefinierter Regeln und Abhilfemaßnahmen Kontrollen zur Sicherheits-, Betriebs- oder Kostenoptimierung durchzuführen. AWS Config AWS Config Conformance Packs

dienen als Beispielvorlagen nicht dazu, die vollständige Einhaltung eines bestimmten Governance- oder Compliance-Standards sicherzustellen. Sie sind dafür verantwortlich, selbst zu beurteilen, ob Ihre Nutzung der Services den geltenden gesetzlichen und behördlichen Anforderungen entspricht.

Im Folgenden finden Sie ein Beispiel für eine Zuordnung zwischen den Cybersicherheitsanforderungen des New York State Department of Financial Services (NYDFS) für Finanzdienstleistungsunternehmen (23 NYCRR 500) und AWS verwalteten Konfigurationsregeln. Jede AWS Config Regel gilt für eine bestimmte AWS Ressource und bezieht sich auf eine oder mehrere US-amerikanische NYDFS-Steuerelemente. Eine 23-NYCRR-500-Kontrolle des US NYDFS kann mehreren Konfigurationsregeln zugeordnet werden. In der folgenden Tabelle finden Sie weitere Informationen und Anleitungen zu diesen Zuordnungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
500.02(a)	(a) Cybersicherheitsprogramm. Jedes abgedeckte Unternehmen unterhält ein Cybersicherheitsprogramm, das darauf abzielt, die Vertraulichkeit, Integrität und Verfügbarkeit seiner Informationssysteme zu schützen.	acm-certificate-expiration-check	Stellen Sie sicher, dass die Netzwerkintegrität geschützt ist, indem Sie sicherstellen, dass X509-Zertifikate von AWS ACM ausgestellt werden. Diese Zertifikate müssen gültig und dürfen nicht abgelaufen sein. Für diese Regel ist ein Wert für erforderlich daysToExpiration (Wert für bewährte AWS Grundregeln für Sicherheit: 90). Der tatsächliche Wert muss den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
500.02(a)	(a) Cybersicherheitsprogramm. Jedes abgedeckte Unternehmen unterhält ein Cybersicherheitsprogramm, das darauf abzielt, die Vertraulichkeit, Integrität und Verfügbarkeit seiner Informationssysteme zu schützen.	alb-http-to-https-Umleitungsprüfung	Um Daten während der Übertragung zu schützen, stellen Sie sicher, dass Ihr Application Load Balancer unverschlüsselte HTTP-Anfragen automatisch an HTTPS umleitet. Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.
500.02(a)	(a) Cybersicherheitsprogramm. Jedes abgedeckte Unternehmen unterhält ein Cybersicherheitsprogramm, das darauf abzielt, die Vertraulichkeit, Integrität und Verfügbarkeit seiner Informationssysteme zu schützen.	api-gw-cache-enabled-und-verschlüsselt	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass die Verschlüsselung für den Cache Ihrer API-Gateway-Stufe aktiviert ist. Zum Schutz von für die API-Methode erfassten sensiblen Daten müssen Sie die Verschlüsselung von Daten im Ruhezustand aktivieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
500.02(a)	(a) Cybersicherheitsprogramm. Jedes abgedeckte Unternehmen unterhält ein Cybersicherheitsprogramm, das darauf abzielt, die Vertraulichkeit, Integrität und Verfügbarkeit seiner Informationssysteme zu schützen.	cloud-trail-encryption-enabled	Da sensible Daten vorhanden sein können und um Daten im Ruhezustand zu schützen, sollten Sie sicherstellen, dass die Verschlüsselung für Ihre AWS CloudTrail Trails aktiviert ist.
500.02(a)	(a) Cybersicherheitsprogramm. Jedes abgedeckte Unternehmen unterhält ein Cybersicherheitsprogramm, das darauf abzielt, die Vertraulichkeit, Integrität und Verfügbarkeit seiner Informationssysteme zu schützen.	cloudwatch-log-group-encrypted	Um sensible Daten im Speicher zu schützen, stellen Sie sicher, dass die Verschlüsselung für Ihre Amazon CloudWatch Log Groups aktiviert ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
500.02(a)	(a) Cybersicherheitsprogramm. Jedes abgedeckte Unternehmen unterhält ein Cybersicherheitsprogramm, das darauf abzielt, die Vertraulichkeit, Integrität und Verfügbarkeit seiner Informationssysteme zu schützen.	efs-encrypted-check	Aktivieren Sie die Verschlüsselung für Ihr Amazon Elastic File System (EFS), um eventuell vorhandene sensible Daten sowie Daten im Ruhezustand zu schützen.
500.02(a)	(a) Cybersicherheitsprogramm. Jedes abgedeckte Unternehmen unterhält ein Cybersicherheitsprogramm, das darauf abzielt, die Vertraulichkeit, Integrität und Verfügbarkeit seiner Informationssysteme zu schützen.	elasticsearch-encrypted-at-rest	Da sensible Daten vorhanden sein können und um Daten im Ruhezustand zu schützen, sollten Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon OpenSearch Service (OpenSearch Service)-Domains aktiviert ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
500.02(a)	(a) Cybersicherheitsprogramm. Jedes abgedeckte Unternehmen unterhält ein Cybersicherheitsprogramm, das darauf abzielt, die Vertraulichkeit, Integrität und Verfügbarkeit seiner Informationssysteme zu schützen.	elb-acm-certificate-required	Zum Schutz von eventuell vorhandenen sensiblen Daten sowie von Daten während der Übertragung muss die Verschlüsselung für Ihr Elastic Load Balancing aktiviert sein. Verwenden Sie AWS Certificate Manager, um öffentliche und private SSL/TLS-Zertifikate mit AWS Diensten und internen Ressourcen zu verwalten, bereitzustellen und bereitzustellen.
500.02(a)	(a) Cybersicherheitsprogramm. Jedes abgedeckte Unternehmen unterhält ein Cybersicherheitsprogramm, das darauf abzielt, die Vertraulichkeit, Integrität und Verfügbarkeit seiner Informationssysteme zu schützen.	encrypted-volumes	Um eventuell vorhandene sensible Daten sowie Daten im Ruhezustand zu schützen, muss die Verschlüsselung für Ihre Amazon Elastic Block Store (Amazon EBS)-Volumes aktiviert sein.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
500.02(a)	(a) Cybersicherheitsprogramm. Jedes abgedeckte Unternehmen unterhält ein Cybersicherheitsprogramm, das darauf abzielt, die Vertraulichkeit, Integrität und Verfügbarkeit seiner Informationssysteme zu schützen.	rds-storage-encrypted	Zum Schutz von Daten im Ruhezustand müssen Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon Relational Database Service (Amazon RDS)-Instances aktiviert ist. Um eventuell vorhandene sensible Daten im Ruhezustand in Amazon-RDS-Instances zu schützen, muss die Verschlüsselung von Daten im Ruhezustand aktiviert sein.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
500.02(a)	(a) Cybersicherheitsprogramm. Jedes abgedeckte Unternehmen unterhält ein Cybersicherheitsprogramm, das darauf abzielt, die Vertraulichkeit, Integrität und Verfügbarkeit seiner Informationssysteme zu schützen.	redshift-cluster-configuration-check	Um Daten im Ruhezustand zu schützen, muss die Verschlüsselung für Ihre Amazon-Redshift-Cluster aktiviert sein. Sie müssen auch sicherstellen, dass die erforderlichen Konfigurationen auf Amazon-Redshift-Clustern bereitgestellt werden. Die Prüfungsprotokollierung muss aktiviert sein, um Informationen zu Verbindungen und Benutzeraktivitäten in der Datenbank bereitzustellen. Diese Regel erfordert, dass ein Wert für clusterDbEncrypted (Config Default: TRUE) und LoggingEnabled (Config Default: TRUE) gesetzt ist. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
500.02(a)	(a) Cybersicherheitsprogramm. Jedes abgedeckte Unternehmen unterhält ein Cybersicherheitsprogramm, das darauf abzielt, die Vertraulichkeit, Integrität und Verfügbarkeit seiner Informationssysteme zu schützen.	redshift-require-tls-ssl	Stellen Sie sicher, dass Ihre Amazon-Redshift-Cluster eine TLS/SSL-Verschlüsselung erfordern, um eine Verbindung zu SQL-Clients herzustellen. Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.
500.02(a)	(a) Cybersicherheitsprogramm. Jedes abgedeckte Unternehmen unterhält ein Cybersicherheitsprogramm, das darauf abzielt, die Vertraulichkeit, Integrität und Verfügbarkeit seiner Informationssysteme zu schützen.	s3-aktiviert bucket-server-side-encryption	Zum Schutz von Daten im Ruhezustand müssen Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon Simple Storage Service (Amazon S3)-Buckets aktiviert ist. Um eventuell vorhandene sensible Daten im Ruhezustand in Amazon-S3-Buckets zu schützen, muss die Verschlüsselung aktiviert sein.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
500.02(a)	(a) Cybersicherheitsprogramm. Jedes abgedeckte Unternehmen unterhält ein Cybersicherheitsprogramm, das darauf abzielt, die Vertraulichkeit, Integrität und Verfügbarkeit seiner Informationssysteme zu schützen.	s-3 bucket-ssl-requests-only	Um Daten während der Übertragung zu schützen, stellen Sie sicher, dass Ihre Amazon Simple Storage Service (Amazon S3)-Buckets Anfragen zur Verwendung von Secure Socket Layer (SSL)-Buckets erfordern. Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
500.02(a)	(a) Cybersicherheitsprogramm. Jedes abgedeckte Unternehmen unterhält ein Cybersicherheitsprogramm, das darauf abzielt, die Vertraulichkeit, Integrität und Verfügbarkeit seiner Informationssysteme zu schützen.	sagemaker-endpoint-configuration-kms-key-konfiguriert	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass die Verschlüsselung mit dem AWS Key Management Service (AWS KMS) für Ihren Endpunkt aktiviert ist. SageMaker Da sensible Daten auf dem SageMaker Endgerät gespeichert werden können, sollten Sie die Verschlüsselung im Ruhezustand aktivieren, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
500.02(a)	(a) Cybersicherheitsprogramm. Jedes abgedeckte Unternehmen unterhält ein Cybersicherheitsprogramm, das darauf abzielt, die Vertraulichkeit, Integrität und Verfügbarkeit seiner Informationssysteme zu schützen.	sagemaker-notebook-instance-kms-schlüsselkonfiguriert	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass die Verschlüsselung mit dem AWS Key Management Service (AWS KMS) für Ihr Notebook aktiviert ist. SageMaker Da vertrauliche Daten im SageMaker Notebook gespeichert werden können, sollten Sie die Verschlüsselung im Ruhezustand aktivieren, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
500.02(a)	(a) Cybersicherheitsprogramm. Jedes abgedeckte Unternehmen unterhält ein Cybersicherheitsprogramm, das darauf abzielt, die Vertraulichkeit, Integrität und Verfügbarkeit seiner Informationssysteme zu schützen.	sns-encrypted-kms	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass Ihre Amazon Simple Notification Service (Amazon SNS) -Themen mit dem AWS Key Management Service (AWS KMS) verschlüsselt werden müssen. Um eventuell vorhandene sensible Daten im Ruhezustand in veröffentlichten Nachrichten zu schützen, muss die Verschlüsselung von Daten im Ruhezustand aktiviert sein.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
500.02(a)	(a) Cybersicherheitsprogramm. Jedes abgedeckte Unternehmen unterhält ein Cybersicherheitsprogramm, das darauf abzielt, die Vertraulichkeit, Integrität und Verfügbarkeit seiner Informationssysteme zu schützen.	ec2- ebs-encryption-by-default	Zum Schutz von Daten im Ruhezustand müssen Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon Elastic Block Store (Amazon EBS)-Volumes aktiviert ist. Um eventuell vorhandene sensible Daten im Ruhezustand zu schützen, müssen Sie die Verschlüsselung von Daten im Ruhezustand aktivieren.
500.02(a)	(a) Cybersicherheitsprogramm. Jedes abgedeckte Unternehmen unterhält ein Cybersicherheitsprogramm, das darauf abzielt, die Vertraulichkeit, Integrität und Verfügbarkeit seiner Informationssysteme zu schützen.	rds-snapshot-encrypted	Stellen Sie sicher, dass die Verschlüsselung für Ihre Amazon Relational Database Service (Amazon RDS)-Snapshots aktiviert ist. Um eventuell vorhandene sensible Daten im Ruhezustand zu schützen, muss die Verschlüsselung von Daten im Ruhezustand aktiviert sein.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
500.02(a)	(a) Cybersicherheitsprogramm. Jedes abgedeckte Unternehmen unterhält ein Cybersicherheitsprogramm, das darauf abzielt, die Vertraulichkeit, Integrität und Verfügbarkeit seiner Informationssysteme zu schützen.	alb-http-drop-invalid-Header-fähig	Stellen Sie sicher, dass Ihre Elastic Load Balancers (ELB) so konfiguriert sind, dass sie HTTP-Header löschen. Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.
500.02(a)	(a) Cybersicherheitsprogramm. Jedes abgedeckte Unternehmen unterhält ein Cybersicherheitsprogramm, das darauf abzielt, die Vertraulichkeit, Integrität und Verfügbarkeit seiner Informationssysteme zu schützen.	kinesis-stream-encrypted	Aktivieren Sie die Verschlüsselung für Ihre Amazon-Kinesis-Streams, um eventuell vorhandene sensible Daten sowie Daten im Ruhezustand zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
500.02(a)	(a) Cybersicherheitsprogramm. Jedes abgedeckte Unternehmen unterhält ein Cybersicherheitsprogramm, das darauf abzielt, die Vertraulichkeit, Integrität und Verfügbarkeit seiner Informationssysteme zu schützen.	elasticsearch-node-to-node-Verschlüsselungsprüfung	Stellen Sie sicher, dass die node-to-node Verschlüsselung für Amazon OpenSearch Service aktiviert ist. Node-to-nodeVerschlüsselung ermöglicht die TLS 1.2-Verschlüsselung für die gesamte Kommunikation innerhalb der Amazon Virtual Private Cloud (Amazon VPC). Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.
500.02(a)	(a) Cybersicherheitsprogramm. Jedes abgedeckte Unternehmen unterhält ein Cybersicherheitsprogramm, das darauf abzielt, die Vertraulichkeit, Integrität und Verfügbarkeit seiner Informationssysteme zu schützen.	elb-tls-https-listeners-nur	Stellen Sie sicher, dass Ihre Elastic Load Balancer (ELBs) mit SSL- oder HTTPS-Listenern konfiguriert sind. Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
500.02(a)	(a) Cybersicherheitsprogramm. Jedes abgedeckte Unternehmen unterhält ein Cybersicherheitsprogramm, das darauf abzielt, die Vertraulichkeit, Integrität und Verfügbarkeit seiner Informationssysteme zu schützen.	cloud-trail-log-file-Validierung aktiviert	Verwenden Sie die AWS CloudTrail Protokolldateivalidierung, um die Integrität von Protokollen zu überprüfen. CloudTrail Mithilfe der Protokolldateivalidierung kann festgestellt werden, ob eine Protokolldatei geändert oder gelöscht wurde oder ob sie nach der Übermittlung CloudTrail unverändert geblieben ist. Dieses Feature wurde mit dem Branchenstandard entsprechenden Algorithmen entwickelt: SHA-256 für die Hashfunktion und SHA-256 mit RSA für digitale Signaturen. Aus diesem Grund ist es rechnerisch unmöglich, CloudTrail Protokolldateien unbemerkt zu ändern, zu löschen oder zu fälschen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
500.02(a)	(a) Cybersicherheitsprogramm. Jedes abgedeckte Unternehmen unterhält ein Cybersicherheitsprogramm, das darauf abzielt, die Vertraulichkeit, Integrität und Verfügbarkeit seiner Informationssysteme zu schützen.	dynamodb-autoscaling-enabled	Amazon DynamoDB Auto Scaling verwendet den AWS Application Auto Scaling-Service, um die bereitgestellte Durchsatzkapazität so anzupassen, dass sie automatisch auf tatsächliche Verkehrsmuster reagiert. Auf diese Weise kann eine Tabelle oder ein globaler sekundärer Index die bereitgestellte Lese-/Schreibkapazität erhöhen, um plötzliche Erhöhungen des Datenverkehrs ohne Drosselung zu bewältigen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
500.02(a)	(a) Cybersicherheitsprogramm. Jedes abgedeckte Unternehmen unterhält ein Cybersicherheitsprogramm, das darauf abzielt, die Vertraulichkeit, Integrität und Verfügbarkeit seiner Informationssysteme zu schützen.	elb-deletion-protection-enabled	Diese Regel sorgt dafür, dass der Löschschutz für Elastic Load Balancing aktiviert ist. Verwenden Sie diese Funktion, um zu verhindern, dass Ihr Load Balancer versehentlich oder böswillig gelöscht wird, was zum Verlust der Verfügbarkeit Ihrer Anwendungen führen kann.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
500.02(a)	(a) Cybersicherheitsprogramm. Jedes abgedeckte Unternehmen unterhält ein Cybersicherheitsprogramm, das darauf abzielt, die Vertraulichkeit, Integrität und Verfügbarkeit seiner Informationssysteme zu schützen.	rds-multi-az-support	Die Multi-AZ-Unterstützung in Amazon Relational Database Service (Amazon RDS) bietet eine verbesserte Verfügbarkeit und Beständigkeit von Datenbank-Instances. Wenn Sie eine Multi-AZ-Datenbank-Instance bereitstellen, erstellt Amazon RDS automatisch eine primäre Datenbank-Instance und repliziert die Daten synchron auf eine Standby-Instance in einer anderen Availability Zone. Jede Availability Zone läuft auf einer eigenen, physisch getrennten, unabhängigen Infrastruktur und ist auf eine hohe Verfügbarkeit ausgelegt. Im Falle eines Infrastrukturausfalls führt Amazon RDS einen automatis

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			chen Failover zum Standby-Modus durch, sodass Sie den Datenbankbetrieb wieder aufnehmen können, sobald der Failover abgeschlo ssen ist.
500.02(a)	(a) Cybersich erheitsprogramm. Jedes abgedeckt e Unternehm en unterhält ein Cybersicherheitspr ogramm, das darauf abzielt, die Vertrauli chkeit, Integrität und Verfügbarkeit seiner Informationssysteme zu schützen.	s3- bucket-default-loc k-enabled	Stellen Sie sicher, dass für Ihren Amazon Simple Storage Service (Amazon S3)-Bucke t standardmäßig eine Sperre aktiviert ist. Zum Schutz eventuell vorhanden er sensibler Daten in S3-Buckets müssen Sie Objektsperren für Daten im Ruhezusta nd erzwingen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
500.02(a)	(a) Cybersicherheitsprogramm. Jedes abgedeckte Unternehmen unterhält ein Cybersicherheitsprogramm, das darauf abzielt, die Vertraulichkeit, Integrität und Verfügbarkeit seiner Informationssysteme zu schützen.	vpc-vpn-2-tunnels-up	Redundante Site-to-Site VPN-Tunnel können implementiert werden, um die Anforderungen an die Ausfallsicherheit zu erfüllen. Es verwendet zwei Tunnel, um die Konnektivität sicherzustellen, falls eine der Site-to-Site VPN-Verbindungen nicht verfügbar ist. Um sich vor einem Verbindungsverlust zu schützen, können Sie für den Fall, dass Ihr Kunden-Gateway nicht verfügbar ist, eine zweite Site-to-Site VPN-Verbindung zu Ihrer Amazon Virtual Private Cloud (Amazon VPC) und Ihrem Virtual Private Gateway einrichten, indem Sie ein zweites Kunden-Gateway verwenden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
500.02(a)	(a) Cybersicherheitsprogramm. Jedes abgedeckte Unternehmen unterhält ein Cybersicherheitsprogramm, das darauf abzielt, die Vertraulichkeit, Integrität und Verfügbarkeit seiner Informationssysteme zu schützen.	elb-cross-zone-load-Balancing aktiviert	Aktivieren Sie zonenübergreifendes Load Balancing für Ihre Elastic Load Balancer (ELBs), um eine angemessene Kapazität und Verfügbarkeit aufrechtzuerhalten. Zonenübergreifendes Load Balancing reduziert die Notwendigkeit, die gleiche Anzahl von Instances in jeder aktivierten Availability Zone aufrechtzuerhalten. Es verbessert auch die Fähigkeit Ihrer Anwendung, den Verlust einer oder mehrerer Instances zu bewältigen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
500.02(a)	(a) Cybersicherheitsprogramm. Jedes abgedeckte Unternehmen unterhält ein Cybersicherheitsprogramm, das darauf abzielt, die Vertraulichkeit, Integrität und Verfügbarkeit seiner Informationssysteme zu schützen.	rds-instance-deletion-protection-aktiviert	Stellen Sie sicher, dass Amazon Relational Database Service (Amazon RDS)-Instances den Löschschutz aktiviert haben. Verwenden Sie den Löschschutz, um zu verhindern, dass Ihre Amazon-RDS-Instances versehentlich oder böswillig gelöscht werden, was zum Verlust der Verfügbarkeit Ihrer Anwendungen führen kann.
500.02(a)	(a) Cybersicherheitsprogramm. Jedes abgedeckte Unternehmen unterhält ein Cybersicherheitsprogramm, das darauf abzielt, die Vertraulichkeit, Integrität und Verfügbarkeit seiner Informationssysteme zu schützen.	api-gw-ssl-enabled	Stellen Sie sicher, dass die REST-API-Stufen von Amazon API Gateway mit SSL-Zertifikaten konfiguriert sind, damit Backend-Systeme überprüfen können, ob Anforderungen von API Gateway stammen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
500.02(a)	(a) Cybersicherheitsprogramm. Jedes abgedeckte Unternehmen unterhält ein Cybersicherheitsprogramm, das darauf abzielt, die Vertraulichkeit, Integrität und Verfügbarkeit seiner Informationssysteme zu schützen.	autoscaling-group-elb-healthcheck-erforderlich	Die Elastic Load Balancer (ELB) - Zustandsprüfungen für Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling Scaling-Gruppen unterstützen die Aufrechterhaltung einer angemessenen Kapazität und Verfügbarkeit. Der Load Balancer sendet regelmäßig Pings, versucht Verbindungen herzustellen oder sendet Anfragen, um den Zustand der EC2 Amazon-Instances in einer Gruppe mit auto-scaling zu testen. Wenn eine Instance nicht zurückmeldet, wird der Traffic an eine neue EC2 Amazon-Instance gesendet.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
500.02(a)	(a) Cybersicherheitsprogramm. Jedes abgedeckte Unternehmen unterhält ein Cybersicherheitsprogramm, das darauf abzielt, die Vertraulichkeit, Integrität und Verfügbarkeit seiner Informationssysteme zu schützen.	autoscaling-launch-config-public-ip-deaktiviert	Wenn Sie Ihre Netzwerkschnittstellen mit einer öffentlichen IP-Adresse konfigurieren, sind die diesen Netzwerkschnittstellen zugehörigen Ressourcen über das Internet erreichbar. EC2 Ressourcen sollten nicht öffentlich zugänglich sein, da dies einen unbeabsichtigten Zugriff auf Ihre Anwendungen oder Server ermöglichen kann.
500.02(a)	(a) Cybersicherheitsprogramm. Jedes abgedeckte Unternehmen unterhält ein Cybersicherheitsprogramm, das darauf abzielt, die Vertraulichkeit, Integrität und Verfügbarkeit seiner Informationssysteme zu schützen.	backup-recovery-point-encrypted	Stellen Sie sicher, dass die Verschlüsselung für Ihre AWS Backup-Wiederherstellungspunkte aktiviert ist. Da sensible Daten auch im Ruhezustand vorhanden sein können, sollten Sie die Verschlüsselung im Ruhezustand aktivieren, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
500.02(a)	(a) Cybersicherheitsprogramm. Jedes abgedeckte Unternehmen unterhält ein Cybersicherheitsprogramm, das darauf abzielt, die Vertraulichkeit, Integrität und Verfügbarkeit seiner Informationssysteme zu schützen.	beanstalk-enhanced-health-reporting-aktiviert	AWS Die verbesserte Zustandsberichterstattung von Elastic Beanstalk ermöglicht eine schnellere Reaktion auf Veränderungen im Zustand der zugrunde liegenden Infrastruktur. Diese Änderungen könnten zu einer mangelnden Verfügbarkeit der Anwendung führen. Die erweiterten Zustandsberichte von Elastic Beanstalk bieten eine Statusbeschreibung, um den Schweregrad der identifizierten Probleme einzuschätzen und mögliche Ursachen zu identifizieren, die untersucht werden müssen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
500.02(a)	(a) Cybersicherheitsprogramm. Jedes abgedeckte Unternehmen unterhält ein Cybersicherheitsprogramm, das darauf abzielt, die Vertraulichkeit, Integrität und Verfügbarkeit seiner Informationssysteme zu schützen.	dynamodb-table-encrypted-kms	Stellen Sie sicher, dass die Verschlüsselung für Ihre Amazon-DynamoDB-Tabellen aktiviert ist. Um eventuell vorhandene sensible Daten im Ruhezustand in diesen Tabellen zu schützen, müssen Sie die Verschlüsselung von Daten im Ruhezustand aktivieren. Standardmäßig werden DynamoDB-Tabellen mit einem AWS eigenen Kundenhauptschlüssel (CMK) verschlüsselt.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
500.02(a)	(a) Cybersicherheitsprogramm. Jedes abgedeckte Unternehmen unterhält ein Cybersicherheitsprogramm, das darauf abzielt, die Vertraulichkeit, Integrität und Verfügbarkeit seiner Informationssysteme zu schützen.	ec2- instance-detailed-monitoring-enabled	Aktivieren Sie diese Regel, um die Amazon Elastic Compute Cloud (Amazon EC2) - Instance-Überwachung auf der EC2 Amazon-Konsole zu verbessern, in der Monitoring-Diagramme mit einem Zeitraum von 1 Minute für die Instance angezeigt werden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
500.02(a)	(a) Cybersicherheitsprogramm. Jedes abgedeckte Unternehmen unterhält ein Cybersicherheitsprogramm, das darauf abzielt, die Vertraulichkeit, Integrität und Verfügbarkeit seiner Informationssysteme zu schützen.	elbv-2 acm-certificate-required	Zum Schutz von eventuell vorhandenen sensiblen Daten sowie von Daten während der Übertragung muss die Verschlüsselung für Ihr Elastic Load Balancing aktiviert sein. Verwenden Sie AWS Certificate Manager, um öffentliche und private SSL/TLS-Zertifikate mit AWS Diensten und internen Ressourcen zu verwalten, bereitzustellen und bereitzustellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
500.02(a)	(a) Cybersicherheitsprogramm. Jedes abgedeckte Unternehmen unterhält ein Cybersicherheitsprogramm, das darauf abzielt, die Vertraulichkeit, Integrität und Verfügbarkeit seiner Informationssysteme zu schützen.	s3- -Blocks-periodisch account-level-public-access	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Simple Storage Service (Amazon S3) -Buckets nicht öffentlich zugänglich sind. Diese Regel trägt dazu bei, sensible Daten vor unbefugten Remote-Benutzern zu schützen, indem sie den öffentlichen Zugriff verhindert. Mit dieser Regel können Sie optional die Parameter ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) und restrictPublicBuckets Parameter (Config Default: True) festlegen. Die tatsächlichen Werte müssen den Richtlini

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			en Ihrer Organisation entsprechen.
500.02(a)	(a) Cybersicherheitsprogramm. Jedes abgedeckte Unternehmen unterhält ein Cybersicherheitsprogramm, das darauf abzielt, die Vertraulichkeit, Integrität und Verfügbarkeit seiner Informationssysteme zu schützen.	s3- default-encryption-kms	Stellen Sie sicher, dass die Verschlüsselung für Ihre Amazon Simple Storage Service (Amazon S3)-Buckets aktiviert ist. Um eventuell vorhandene sensible Daten im Ruhezustand in einem Amazon-S3-Bucket zu schützen, muss die Verschlüsselung aktiviert sein.
500.02(a)	(a) Cybersicherheitsprogramm. Jedes abgedeckte Unternehmen unterhält ein Cybersicherheitsprogramm, das darauf abzielt, die Vertraulichkeit, Integrität und Verfügbarkeit seiner Informationssysteme zu schützen.	ssm-document-not-public	Stellen Sie sicher, dass AWS Systems Manager (SSM) - Dokumente nicht öffentlich sind, da dies einen unbeabsichtigten Zugriff auf Ihre SSM-Dokumente ermöglichen kann. Ein öffentliches SSM-Dokument kann Informationen über Ihr Konto, Ihre Ressourcen und internen Prozesse preisgeben.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
500.02(a)	(a) Cybersicherheitsprogramm. Jedes abgedeckte Unternehmen unterhält ein Cybersicherheitsprogramm, das darauf abzielt, die Vertraulichkeit, Integrität und Verfügbarkeit seiner Informationssysteme zu schützen.	opensearch-encrypted-at-rest	Da sensible Daten vorhanden sein können und um Daten im Ruhezustand zu schützen, sollten Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon OpenSearch Service-Domains aktiviert ist.
500.02(a)	(a) Cybersicherheitsprogramm. Jedes abgedeckte Unternehmen unterhält ein Cybersicherheitsprogramm, das darauf abzielt, die Vertraulichkeit, Integrität und Verfügbarkeit seiner Informationssysteme zu schützen.	opensearch-node-to-node-Verschlüsselungsprüfung	Stellen Sie sicher, dass die node-to-node Verschlüsselung für Amazon OpenSearch Service aktiviert ist. Node-to-nodeVerschlüsselung ermöglicht die TLS 1.2-Verschlüsselung für die gesamte Kommunikation innerhalb der Amazon Virtual Private Cloud (Amazon VPC). Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
500.02(a)	(a) Cybersicherheitsprogramm. Jedes abgedeckte Unternehmen unterhält ein Cybersicherheitsprogramm, das darauf abzielt, die Vertraulichkeit, Integrität und Verfügbarkeit seiner Informationssysteme zu schützen.	codebuild-project-artifact-encryption	Um sensible Daten im Speicher zu schützen, stellen Sie sicher, dass die Verschlüsselung für Ihre AWS CodeBuild Artefakte aktiviert ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
500.02(b)(2)	(b) Das Cybersicherheitsprogramm basiert auf der Risikobeurteilung des abgedeckten Unternehmens und ist darauf ausgelegt, die folgenden zentralen Cybersicherheitsfunktionen zu erfüllen: (2) Nutzung einer defensiven Infrastruktur und Umsetzung von Richtlinien und Verfahren zum Schutz der Informationssysteme des abgedeckten Unternehmens und der in diesen Informationssystemen gespeicherten nicht öffentlichen Informationen vor unbefugtem Zugriff, unbefugter Nutzung oder anderen böswilligen Handlungen.	emr-kerberos-enabled	Die Zugriffsberechtigungen und -autorisierungen können verwaltet und nach den Prinzipien der geringsten Berechtigung und Aufgabentrennung integriert werden, indem Kerberos für Amazon-EMR-Cluster aktiviert wird. In Kerberos werden Services und Benutzer, die sich authentifizieren müssen, als Prinzipale bezeichnet. Prinzipale befinden sich in einem Kerberos-Bereich. Innerhalb dieses Bereichs wird ein Kerberos-Server als Key Distribution Center (KDC) bezeichnet. Über diesen Server können sich Prinzipale authentifizieren. Die Authentifizierung im KDC erfolgt durch die Ausstellung von Authentif

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			izierungstickets. Das KDC unterhält eine Datenbank der Prinzipale in seinem Bereich mit ihren Passwörtern und anderen administr ativen Informationen zu jedem Prinzipal.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
500.02(b)(2)	(b) Das Cybersicherheitsprogramm basiert auf der Risikobeurteilung des abgedeckten Unternehmens und ist darauf ausgelegt, die folgenden zentralen Cybersicherheitsfunktionen zu erfüllen: (2) Nutzung einer defensiven Infrastruktur und Umsetzung von Richtlinien und Verfahren zum Schutz der Informationssysteme des abgedeckten Unternehmens und der in diesen Informationssystemen gespeicherten nicht öffentlichen Informationen vor unbefugtem Zugriff, unbefugter Nutzung oder anderen böswilligen Handlungen.	iam-group-has-users-überprüfen	AWS Identity and Access Management (IAM) kann Ihnen helfen, die Prinzipien der geringsten Rechte und der Aufgabentrennung mit Zugriffsberechtigungen und Autorisierungen zu integrieren, indem sichergestellt wird, dass IAM-Gruppen mindestens einen Benutzer haben. Die Einteilung von Benutzern in Gruppen auf der Grundlage der ihnen zugewiesenen Berechtigungen oder ihrer Funktion ist eine Möglichkeit, das Prinzip der geringsten Berechtigung zu implementieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
500.02(b)(2)	(b) Das Cybersicherheitsprogramm basiert auf der Risikobeurteilung des abgedeckten Unternehmens und ist darauf ausgelegt, die folgenden zentralen Cybersicherheitsfunktionen zu erfüllen: (2) Nutzung einer defensiven Infrastruktur und Umsetzung von Richtlinien und Verfahren zum Schutz der Informationssysteme des abgedeckten Unternehmens und der in diesen Informationssystemen gespeicherten nicht öffentlichen Informationen vor unbefugtem Zugriff, unbefugter Nutzung oder anderen böswilligen Handlungen.	iam-password-policy	Die Identitäten und Anmeldeinformationen werden auf der Grundlage einer organisatorischen IAM-Passwortrichtlinie ausgestellt, verwaltet und verifiziert. Sie erfüllen oder übertreffen die Anforderungen von NIST SP 800-63 und dem Standard „Best Practices“ von AWS Foundational Security für die Passwortstärke. Mit dieser Regel können Sie optional RequireUppercaseCharacters (Wert für AWS grundlegende Sicherheitsbewährte Methoden: wahr), RequireLowercaseCharacters (Wert für bewährte Methoden für AWS grundlegende Sicherheit: wahr), RequireSymbols (Wert für bewährte Methoden für AWS grundlegende Sicherheit:

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			wahr), RequireNumbers (Wert für bewährte Methoden für AWS grundlegende Sicherheit: wahr), MinimumPasswordLength (Wert für bewährte Methoden für AWS grundlegende Sicherheit: 14), PasswordReusePrevention (Wert für bewährte Methoden für AWS grundlegende Sicherheit: 24) und MaxPasswordAge (Wert für bewährte Methoden für AWS grundlegende Sicherheit: 90) für Ihr IAM festlegen Kennwortrichtlinie. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
500.02(b)(2)	(b) Das Cybersicherheitsprogramm basiert auf der Risikobeurteilung des abgedeckten Unternehmens und ist darauf ausgelegt, die folgenden zentralen Cybersicherheitsfunktionen zu erfüllen: (2) Nutzung einer defensiven Infrastruktur und Umsetzung von Richtlinien und Verfahren zum Schutz der Informationssysteme des abgedeckten Unternehmens und der in diesen Informationssystemen gespeicherten nicht öffentlichen Informationen vor unbefugtem Zugriff, unbefugter Nutzung oder anderen böswilligen Handlungen.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) kann Ihnen dabei helfen, die Prinzipien der geringsten Rechte und der Aufgabentrennung in Zugriffsberechtigungen und Autorisierungen zu integrieren und so zu verhindern, dass Richtlinien „Effect“: „Allow“ mit „Action“: „*“ anstelle von „Resource“: „*“ enthalten. Wenn Benutzern mehr Rechte eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und der Aufgabentrennung verstoßen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
500.02(b)(2)	(b) Das Cybersicherheitsprogramm basiert auf der Risikobeurteilung des abgedeckten Unternehmens und ist darauf ausgelegt, die folgenden zentralen Cybersicherheitsfunktionen zu erfüllen: (2) Nutzung einer defensiven Infrastruktur und Umsetzung von Richtlinien und Verfahren zum Schutz der Informationssysteme des abgedeckten Unternehmens und der in diesen Informationssystemen gespeicherten nicht öffentlichen Informationen vor unbefugtem Zugriff, unbefugter Nutzung oder anderen böswilligen Handlungen.	iam-root-access-key-überprüfen	Der Zugriff auf Systeme und Ressourcen kann gesteuert werden, indem überprüft wird, ob der Root-Benutzer keine Zugriffsschlüssel mit seiner AWS Identity and Access Management (IAM) -Rolle verknüpft hat. Stellen Sie sicher, dass die Root-Zugriffsschlüssel gelöscht werden. Erstellen und verwenden Sie stattdessen rollenbasierte Funktionen, AWS-Konten um das Prinzip der geringsten Funktionalität zu berücksichtigen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
500.02(b)(2)	(b) Das Cybersicherheitsprogramm basiert auf der Risikobeurteilung des abgedeckten Unternehmens und ist darauf ausgelegt, die folgenden zentralen Cybersicherheitsfunktionen zu erfüllen: (2) Nutzung einer defensiven Infrastruktur und Umsetzung von Richtlinien und Verfahren zum Schutz der Informationssysteme des abgedeckten Unternehmens und der in diesen Informationssystemen gespeicherten nicht öffentlichen Informationen vor unbefugtem Zugriff, unbefugter Nutzung oder anderen böswilligen Handlungen.	iam-user-group-membership-überprüfen	AWS Identity and Access Management (IAM) kann Ihnen helfen, Zugriffsberechtigungen und Autorisierungen einzuschränken, indem sichergestellt wird, dass Benutzer Mitglieder mindestens einer Gruppe sind. Wenn Benutzern mehr Berechtigungen eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und Aufgabentrennung verstoßen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
500.02(b)(2)	(b) Das Cybersicherheitsprogramm basiert auf der Risikobeurteilung des abgedeckten Unternehmens und ist darauf ausgelegt, die folgenden zentralen Cybersicherheitsfunktionen zu erfüllen: (2) Nutzung einer defensiven Infrastruktur und Umsetzung von Richtlinien und Verfahren zum Schutz der Informationssysteme des abgedeckten Unternehmens und der in diesen Informationssystemen gespeicherten nicht öffentlichen Informationen vor unbefugtem Zugriff, unbefugter Nutzung oder anderen böswilligen Handlungen.	iam-user-mfa-enabled	Aktivieren Sie diese Regel, um den Zugriff auf Ressourcen in der AWS Cloud einzuschränken. Diese Regel sorgt dafür, dass die Multi-Faktor-Authentifizierung (MFA) für alle Benutzer aktiviert ist. MFA sorgt für eine weitere Schutzebene zusätzlich zu den Anmeldeinformationen. Reduzieren Sie Fälle von kompromittierten Konten, indem Sie MFA für Benutzer vorschreiben.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
500.02(b)(2)	(b) Das Cybersicherheitsprogramm basiert auf der Risikobeurteilung des abgedeckten Unternehmens und ist darauf ausgelegt, die folgenden zentralen Cybersicherheitsfunktionen zu erfüllen: (2) Nutzung einer defensiven Infrastruktur und Umsetzung von Richtlinien und Verfahren zum Schutz der Informationssysteme des abgedeckten Unternehmens und der in diesen Informationssystemen gespeicherten nicht öffentlichen Informationen vor unbefugtem Zugriff, unbefugter Nutzung oder anderen böswilligen Handlungen.	iam-user-no-policies-überprüfen	Diese Regel stellt sicher, dass AWS Identity and Access Management (IAM) -Richtlinien nur Gruppen oder Rollen zugewiesen werden, um den Zugriff auf Systeme und Ressourcen zu kontrollieren. Die Zuweisung von Berechtigungen auf Gruppen- oder Rollenebene trägt dazu bei, die Wahrscheinlichkeit zu verringern, dass eine Identität übermäßige Berechtigungen erhält oder beibehält.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
500.02(b)(2)	(b) Das Cybersicherheitsprogramm basiert auf der Risikobeurteilung des abgedeckten Unternehmens und ist darauf ausgelegt, die folgenden zentralen Cybersicherheitsfunktionen zu erfüllen: (2) Nutzung einer defensiven Infrastruktur und Umsetzung von Richtlinien und Verfahren zum Schutz der Informationssysteme des abgedeckten Unternehmens und der in diesen Informationssystemen gespeicherten nicht öffentlichen Informationen vor unbefugtem Zugriff, unbefugter Nutzung oder anderen böswilligen Handlungen.	mfa-enabled-for-iam-Konsolenzugriff	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass MFA für alle AWS Identity and Access Management (IAM) -Benutzer aktiviert ist, die über ein Konsolenkennwort verfügen. MFA sorgt für eine weitere Schutzebene zusätzlich zu den Anmeldeinformationen. Indem Sie MFA für Benutzer vorschreiben, können Sie Fälle kompromittierter Konten reduzieren und verhindern, dass unbefugte Benutzer auf vertrauliche Daten zugreifen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
500.02(b)(2)	(b) Das Cybersicherheitsprogramm basiert auf der Risikobeurteilung des abgedeckten Unternehmens und ist darauf ausgelegt, die folgenden zentralen Cybersicherheitsfunktionen zu erfüllen: (2) Nutzung einer defensiven Infrastruktur und Umsetzung von Richtlinien und Verfahren zum Schutz der Informationssysteme des abgedeckten Unternehmens und der in diesen Informationssystemen gespeicherten nicht öffentlichen Informationen vor unbefugtem Zugriff, unbefugter Nutzung oder anderen böswilligen Handlungen.	root-account-hardware-mfa-aktiviert	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Hardware-MFA für den Root-Benutzer aktiviert ist. Der Stammbenutzer ist der AWS-Konto-Benutzer mit den meisten Berechtigungen. MFA sorgt für eine weitere Schutzebene zusätzlich zu den Anmeldeinformationen. Indem Sie MFA für den Root-Benutzer vorschreiben, können Sie die Anzahl AWS-Konten kompromittierter Benutzer reduzieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
500.02(b)(2)	(b) Das Cybersicherheitsprogramm basiert auf der Risikobeurteilung des abgedeckten Unternehmens und ist darauf ausgelegt, die folgenden zentralen Cybersicherheitsfunktionen zu erfüllen: (2) Nutzung einer defensiven Infrastruktur und Umsetzung von Richtlinien und Verfahren zum Schutz der Informationssysteme des abgedeckten Unternehmens und der in diesen Informationssystemen gespeicherten nicht öffentlichen Informationen vor unbefugtem Zugriff, unbefugter Nutzung oder anderen böswilligen Handlungen.	root-account-mfa-enabled	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass MFA für den Root-Benutzer aktiviert ist. Der Stammbenutzer ist der AWS-Konto-Benutzer mit den meisten Berechtigungen. MFA sorgt für eine weitere Schutzebene zusätzlich zu den Anmeldeinformationen. Indem Sie MFA für den Root-Benutzer vorschreiben, können Sie die Anzahl AWS-Konten kompromittierter Benutzer reduzieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
500.02(b)(2)	(b) Das Cybersicherheitsprogramm basiert auf der Risikobeurteilung des abgedeckten Unternehmens und ist darauf ausgelegt, die folgenden zentralen Cybersicherheitsfunktionen zu erfüllen: (2) Nutzung einer defensiven Infrastruktur und Umsetzung von Richtlinien und Verfahren zum Schutz der Informationssysteme des abgedeckten Unternehmens und der in diesen Informationssystemen gespeicherten nicht öffentlichen Informationen vor unbefugtem Zugriff, unbefugter Nutzung oder anderen böswilligen Handlungen.	s-3 bucket-policy-grantee-check	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie s3_bucket_policy_grantee_check aktivieren. Diese Regel prüft, ob der vom Amazon S3 S3-Bucket gewährte Zugriff durch die von Ihnen bereitgestellten AWS Principals, Verbundbenutzer, Service Principals, IP-Adressen oder Amazon Virtual Private Cloud (Amazon VPC) IDs eingeschränkt ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
500.02(b)(2)	(b) Das Cybersicherheitsprogramm basiert auf der Risikobeurteilung des abgedeckten Unternehmens und ist darauf ausgelegt, die folgenden zentralen Cybersicherheitsfunktionen zu erfüllen: (2) Nutzung einer defensiven Infrastruktur und Umsetzung von Richtlinien und Verfahren zum Schutz der Informationssysteme des abgedeckten Unternehmens und der in diesen Informationssystemen gespeicherten nicht öffentlichen Informationen vor unbefugtem Zugriff, unbefugter Nutzung oder anderen böswilligen Handlungen.	ec2-imdsv2-check	Stellen Sie sicher, dass die Methode Instance Metadata Service Version 2 (IMDSv2) aktiviert ist, um den Zugriff auf und die Kontrolle der Amazon Elastic Compute Cloud (Amazon EC2) - Instance-Metadaten zu schützen. Die IMDSv2 Methode verwendet sitzungsbasierte Kontrollen. Mit können Kontrollen implementiert werden IMDSv2, um Änderungen an Instanzmetadaten einzuschränken.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
500.02(b)(2)	(b) Das Cybersicherheitsprogramm basiert auf der Risikobeurteilung des abgedeckten Unternehmens und ist darauf ausgelegt, die folgenden zentralen Cybersicherheitsfunktionen zu erfüllen: (2) Nutzung einer defensiven Infrastruktur und Umsetzung von Richtlinien und Verfahren zum Schutz der Informationssysteme des abgedeckten Unternehmens und der in diesen Informationssystemen gespeicherten nicht öffentlichen Informationen vor unbefugtem Zugriff, unbefugter Nutzung oder anderen böswilligen Handlungen.	iam-no-inline-policy-überprüfen	Stellen Sie sicher, dass ein Benutzer, eine IAM-Rolle oder eine IAM-Gruppe (AWS Identity and Access Management) nicht über eine Inline-Richtlinie zur Zugriffskontrolle auf Systeme und Ressourcen verfügt. AWS empfiehlt, verwaltete Richtlinien anstelle von Inline-Richtlinien zu verwenden. Verwaltete Richtlinien ermöglichen Wiederverwendbarkeit, Versionsverwaltung, Rollback und Delegierung der Berechtigungsverwaltung.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
500.02(b)(2)	(b) Das Cybersicherheitsprogramm basiert auf der Risikobeurteilung des abgedeckten Unternehmens und ist darauf ausgelegt, die folgenden zentralen Cybersicherheitsfunktionen zu erfüllen: (2) Nutzung einer defensiven Infrastruktur und Umsetzung von Richtlinien und Verfahren zum Schutz der Informationssysteme des abgedeckten Unternehmens und der in diesen Informationssystemen gespeicherten nicht öffentlichen Informationen vor unbefugtem Zugriff, unbefugter Nutzung oder anderen böswilligen Handlungen.	dms-replication-not-public	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass auf DMS-Replikationsinstanzen nicht öffentlich zugegriffen werden kann. DMS-Replikations-Instances können vertrauliche Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
500.02(b)(2)	(b) Das Cybersicherheitsprogramm basiert auf der Risikobeurteilung des abgedeckten Unternehmens und ist darauf ausgelegt, die folgenden zentralen Cybersicherheitsfunktionen zu erfüllen: (2) Nutzung einer defensiven Infrastruktur und Umsetzung von Richtlinien und Verfahren zum Schutz der Informationssysteme des abgedeckten Unternehmens und der in diesen Informationssystemen gespeicherten nicht öffentlichen Informationen vor unbefugtem Zugriff, unbefugter Nutzung oder anderen böswilligen Handlungen.	ebs-snapshot-public-restorable-überprüfen	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass EBS-Snapshots nicht öffentlich wiederherstellbar sind. EBS-Volume-Snapshots können vertrauliche Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
500.02(b)(2)	(b) Das Cybersicherheitsprogramm basiert auf der Risikobeurteilung des abgedeckten Unternehmens und ist darauf ausgelegt, die folgenden zentralen Cybersicherheitsfunktionen zu erfüllen: (2) Nutzung einer defensiven Infrastruktur und Umsetzung von Richtlinien und Verfahren zum Schutz der Informationssysteme des abgedeckten Unternehmens und der in diesen Informationssystemen gespeicherten nicht öffentlichen Informationen vor unbefugtem Zugriff, unbefugter Nutzung oder anderen böswilligen Handlungen.	ec-2 instance-no-public-ip	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon Elastic Compute Cloud (Amazon EC2) - Instances nicht öffentlich zugänglich sind. EC2 Amazon-Instances können vertrauliche Informationen enthalten, und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
500.02(b)(2)	(b) Das Cybersicherheitsprogramm basiert auf der Risikobeurteilung des abgedeckten Unternehmens und ist darauf ausgelegt, die folgenden zentralen Cybersicherheitsfunktionen zu erfüllen: (2) Nutzung einer defensiven Infrastruktur und Umsetzung von Richtlinien und Verfahren zum Schutz der Informationssysteme des abgedeckten Unternehmens und der in diesen Informationssystemen gespeicherten nicht öffentlichen Informationen vor unbefugtem Zugriff, unbefugter Nutzung oder anderen böswilligen Handlungen.	elasticsearch-in-vpc-only	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass sich Amazon OpenSearch OpenSearch Service (Service) - Domains innerhalb einer Amazon Virtual Private Cloud (Amazon VPC) befinden. Eine OpenSearch Service-Domain innerhalb einer Amazon VPC ermöglicht die sichere Kommunikation zwischen OpenSearch Service und anderen Services innerhalb der Amazon VPC, ohne dass ein Internet-Gateway, ein NAT-Gerät oder eine VPN-Verbindung erforderlich ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
500.02(b)(2)	(b) Das Cybersicherheitsprogramm basiert auf der Risikobeurteilung des abgedeckten Unternehmens und ist darauf ausgelegt, die folgenden zentralen Cybersicherheitsfunktionen zu erfüllen: (2) Nutzung einer defensiven Infrastruktur und Umsetzung von Richtlinien und Verfahren zum Schutz der Informationssysteme des abgedeckten Unternehmens und der in diesen Informationssystemen gespeicherten nicht öffentlichen Informationen vor unbefugtem Zugriff, unbefugter Nutzung oder anderen böswilligen Handlungen.	emr-master-no-public-ip	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon EMR-Cluster-Masterknoten nicht öffentlich zugänglich sind. Amazon-EMR-Cluster-Hauptknoten können vertrauliche Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
500.02(b)(2)	(b) Das Cybersicherheitsprogramm basiert auf der Risikobeurteilung des abgedeckten Unternehmens und ist darauf ausgelegt, die folgenden zentralen Cybersicherheitsfunktionen zu erfüllen: (2) Nutzung einer defensiven Infrastruktur und Umsetzung von Richtlinien und Verfahren zum Schutz der Informationssysteme des abgedeckten Unternehmens und der in diesen Informationssystemen gespeicherten nicht öffentlichen Informationen vor unbefugtem Zugriff, unbefugter Nutzung oder anderen böswilligen Handlungen.	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) Security Groups können bei der Verwaltung des Netzwerkzugriffs helfen, indem sie eine statusbehaftete Filterung von eingehendem und ausgehendem Netzwerkverkehr zu Ressourcen bereitstellen. AWS Wenn Sie eingehenden (oder entfernten) Datenverkehr von 0.0.0.0/0 bis Port 22 auf Ihren Ressourcen nicht zulassen, können Sie den Remote-Zugriff einschränken.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
500.02(b)(2)	(b) Das Cybersicherheitsprogramm basiert auf der Risikobeurteilung des abgedeckten Unternehmens und ist darauf ausgelegt, die folgenden zentralen Cybersicherheitsfunktionen zu erfüllen: (2) Nutzung einer defensiven Infrastruktur und Umsetzung von Richtlinien und Verfahren zum Schutz der Informationssysteme des abgedeckten Unternehmens und der in diesen Informationssystemen gespeicherten nicht öffentlichen Informationen vor unbefugtem Zugriff, unbefugter Nutzung oder anderen böswilligen Handlungen.	ec-2 instances-in-vpc	Stellen Sie Amazon Elastic Compute Cloud (Amazon EC2) -Instances innerhalb einer Amazon Virtual Private Cloud (Amazon VPC) bereit, um eine sichere Kommunikation zwischen einer Instance und anderen Services innerhalb der Amazon VPC zu ermöglichen, ohne dass ein Internet-Gateway, ein NAT-Gerät oder eine VPN-Verbindung erforderlich ist. Der gesamte Datenverkehr bleibt sicher in der AWS Cloud. Domains, die sich innerhalb einer VPC befinden, verfügen aufgrund ihrer logischen Isolierung im Vergleich zu Domains mit öffentlichen Endpunkten über eine zusätzliche Sicherheitsebene. Weisen Sie EC2

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			Amazon-Instances einer Amazon-VPC zu, um den Zugriff ordnungsgemäß zu verwalten.
500.02(b)(2)	(b) Das Cybersicherheitsprogramm basiert auf der Risikobeurteilung des abgedeckten Unternehmens und ist darauf ausgelegt, die folgenden zentralen Cybersicherheitsfunktionen zu erfüllen: (2) Nutzung einer defensiven Infrastruktur und Umsetzung von Richtlinien und Verfahren zum Schutz der Informationssysteme des abgedeckten Unternehmens und der in diesen Informationssystemen gespeicherten nicht öffentlichen Informationen vor unbefugtem Zugriff, unbefugter Nutzung oder anderen böswilligen Handlungen.	internet-gateway-authorized-vpc-nur	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Internet-Gateways nur mit autorisierter Amazon Virtual Private Cloud (Amazon VPC) verbunden sind. Internet-Gateways ermöglichen den bidirektionalen Internetzugang zur und von der Amazon VPC, was möglicherweise zu einem unbefugten Zugriff auf Amazon-VPC-Ressourcen führen kann.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
500.02(b)(2)	(b) Das Cybersicherheitsprogramm basiert auf der Risikobeurteilung des abgedeckten Unternehmens und ist darauf ausgelegt, die folgenden zentralen Cybersicherheitsfunktionen zu erfüllen: (2) Nutzung einer defensiven Infrastruktur und Umsetzung von Richtlinien und Verfahren zum Schutz der Informationssysteme des abgedeckten Unternehmens und der in diesen Informationssystemen gespeicherten nicht öffentlichen Informationen vor unbefugtem Zugriff, unbefugter Nutzung oder anderen böswilligen Handlungen.	lambda-function-public-access-verboten	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass AWS Lambda-Funktionen nicht öffentlich zugänglich sind. Der öffentliche Zugriff kann möglicherweise die Verfügbarkeit von Ressourcen beeinträchtigen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
500.02(b)(2)	(b) Das Cybersicherheitsprogramm basiert auf der Risikobeurteilung des abgedeckten Unternehmens und ist darauf ausgelegt, die folgenden zentralen Cybersicherheitsfunktionen zu erfüllen: (2) Nutzung einer defensiven Infrastruktur und Umsetzung von Richtlinien und Verfahren zum Schutz der Informationssysteme des abgedeckten Unternehmens und der in diesen Informationssystemen gespeicherten nicht öffentlichen Informationen vor unbefugtem Zugriff, unbefugter Nutzung oder anderen böswilligen Handlungen.	lambda-inside-vpc	Stellen Sie AWS Lambda-Funktionen in einer Amazon Virtual Private Cloud (Amazon VPC) bereit, um eine sichere Kommunikation zwischen einer Funktion und anderen Diensten innerhalb der Amazon VPC zu gewährleisten. Bei dieser Konfiguration sind kein Internet-Gateway, kein NAT-Gerät und keine VPN-Verbindung erforderlich. Der gesamte Datenverkehr bleibt sicher in der Cloud. AWS Domains, die sich innerhalb einer VPC befinden, verfügen aufgrund ihrer logischen Isolierung im Vergleich zu Domains mit öffentlichen Endpunkten über eine zusätzliche Sicherheitsebene. Um den Zugriff ordnungsgemäß zu verwalten,

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			sollten AWS Lambda-Funktionen einer VPC zugewiesen werden.
500.02(b)(2)	(b) Das Cybersicherheitsprogramm basiert auf der Risikobeurteilung des abgedeckten Unternehmens und ist darauf ausgelegt, die folgenden zentralen Cybersicherheitsfunktionen zu erfüllen: (2) Nutzung einer defensiven Infrastruktur und Umsetzung von Richtlinien und Verfahren zum Schutz der Informationssysteme des abgedeckten Unternehmens und der in diesen Informationssystemen gespeicherten nicht öffentlichen Informationen vor unbefugtem Zugriff, unbefugter Nutzung oder anderen böswilligen Handlungen.	rds-instance-public-access-überprüfen	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Relational Database Service (Amazon RDS) -Instances nicht öffentlich sind. Amazon-RDS-Datenbank-Instances können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
500.02(b)(2)	(b) Das Cybersicherheitsprogramm basiert auf der Risikobeurteilung des abgedeckten Unternehmens und ist darauf ausgelegt, die folgenden zentralen Cybersicherheitsfunktionen zu erfüllen: (2) Nutzung einer defensiven Infrastruktur und Umsetzung von Richtlinien und Verfahren zum Schutz der Informationssysteme des abgedeckten Unternehmens und der in diesen Informationssystemen gespeicherten nicht öffentlichen Informationen vor unbefugtem Zugriff, unbefugter Nutzung oder anderen böswilligen Handlungen.	rds-snapshots-public-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Relational Database Service (Amazon RDS) -Instances nicht öffentlich sind. Amazon-RDS-Datenbank-Instances können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
500.02(b)(2)	(b) Das Cybersicherheitsprogramm basiert auf der Risikobeurteilung des abgedeckten Unternehmens und ist darauf ausgelegt, die folgenden zentralen Cybersicherheitsfunktionen zu erfüllen: (2) Nutzung einer defensiven Infrastruktur und Umsetzung von Richtlinien und Verfahren zum Schutz der Informationssysteme des abgedeckten Unternehmens und der in diesen Informationssystemen gespeicherten nicht öffentlichen Informationen vor unbefugtem Zugriff, unbefugter Nutzung oder anderen böswilligen Handlungen.	redshift-cluster-public-access-überprüfen	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Redshift Redshift-Cluster nicht öffentlich sind. Amazon-Redshift-Cluster können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
500.02(b)(2)	(b) Das Cybersicherheitsprogramm basiert auf der Risikobeurteilung des abgedeckten Unternehmens und ist darauf ausgelegt, die folgenden zentralen Cybersicherheitsfunktionen zu erfüllen: (2) Nutzung einer defensiven Infrastruktur und Umsetzung von Richtlinien und Verfahren zum Schutz der Informationssysteme des abgedeckten Unternehmens und der in diesen Informationssystemen gespeicherten nicht öffentlichen Informationen vor unbefugtem Zugriff, unbefugter Nutzung oder anderen böswilligen Handlungen.	restricted-common-ports	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass gemeinsame Ports für Amazon Elastic Compute Cloud (Amazon EC2) -Sicherheitsgruppen eingeschränkt sind. Wenn der Zugriff auf Ports nicht auf vertrauenswürdige Quellen beschränkt wird, kann dies zu Angriffen auf die Verfügbarkeit, Integrität und Vertraulichkeit von Systemen führen. Mit dieser Regel können Sie optional die Parameter blockedPort1–blockedPort5 festlegen (Standardkonfigurationen: 20, 21, 3389, 3306, 4333). Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
500.02(b)(2)	(b) Das Cybersicherheitsprogramm basiert auf der Risikobeurteilung des abgedeckten Unternehmens und ist darauf ausgelegt, die folgenden zentralen Cybersicherheitsfunktionen zu erfüllen: (2) Nutzung einer defensiven Infrastruktur und Umsetzung von Richtlinien und Verfahren zum Schutz der Informationssysteme des abgedeckten Unternehmens und der in diesen Informationssystemen gespeicherten nicht öffentlichen Informationen vor unbefugtem Zugriff, unbefugter Nutzung oder anderen böswilligen Handlungen.	s-3 bucket-public-read-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie nur autorisierten Benutzern, Prozessen und Geräten Zugriff auf Amazon Simple Storage Service (Amazon S3) - Buckets gewähren. Die Verwaltung des Zugriffs sollte mit der Klassifizierung der Daten übereinstimmen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
500.02(b)(2)	(b) Das Cybersicherheitsprogramm basiert auf der Risikobeurteilung des abgedeckten Unternehmens und ist darauf ausgelegt, die folgenden zentralen Cybersicherheitsfunktionen zu erfüllen: (2) Nutzung einer defensiven Infrastruktur und Umsetzung von Richtlinien und Verfahren zum Schutz der Informationssysteme des abgedeckten Unternehmens und der in diesen Informationssystemen gespeicherten nicht öffentlichen Informationen vor unbefugtem Zugriff, unbefugter Nutzung oder anderen böswilligen Handlungen.	s3- bucket-public-write-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie nur autorisierten Benutzern, Prozessen und Geräten Zugriff auf Amazon Simple Storage Service (Amazon S3) - Buckets gewähren. Die Verwaltung des Zugriffs sollte mit der Klassifizierung der Daten übereinstimmen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
500.02(b)(2)	(b) Das Cybersicherheitsprogramm basiert auf der Risikobeurteilung des abgedeckten Unternehmens und ist darauf ausgelegt, die folgenden zentralen Cybersicherheitsfunktionen zu erfüllen: (2) Nutzung einer defensiven Infrastruktur und Umsetzung von Richtlinien und Verfahren zum Schutz der Informationssysteme des abgedeckten Unternehmens und der in diesen Informationssystemen gespeicherten nicht öffentlichen Informationen vor unbefugtem Zugriff, unbefugter Nutzung oder anderen böswilligen Handlungen.	sagemaker-notebook-no-direct-Internetzugang	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass SageMaker Amazon-Notebooks keinen direkten Internetzugang zulassen. Indem Sie direkten Internetzugang blockieren, vermeiden Sie, dass unbefugte Benutzer auf sensible Daten zugreifen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
500.02(b)(2)	(b) Das Cybersicherheitsprogramm basiert auf der Risikobeurteilung des abgedeckten Unternehmens und ist darauf ausgelegt, die folgenden zentralen Cybersicherheitsfunktionen zu erfüllen: (2) Nutzung einer defensiven Infrastruktur und Umsetzung von Richtlinien und Verfahren zum Schutz der Informationssysteme des abgedeckten Unternehmens und der in diesen Informationssystemen gespeicherten nicht öffentlichen Informationen vor unbefugtem Zugriff, unbefugter Nutzung oder anderen böswilligen Handlungen.	vpc-default-security-group-geschlossen	Sicherheitsgruppen von Amazon Elastic Compute Cloud (Amazon EC2) können bei der Verwaltung des Netzwerkzugriffs helfen, indem sie eine statusbehaftete Filterung des ein- und ausgehenden Netzwerkverkehrs zu Ressourcen bereitstellen. AWS Die Beschränkung des gesamten Datenverkehrs auf die Standardsicherheitsgruppe hilft dabei, den Fernzugriff auf Ihre Ressourcen einzuschränken. AWS

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
500.02(b)(2)	(b) Das Cybersicherheitsprogramm basiert auf der Risikobeurteilung des abgedeckten Unternehmens und ist darauf ausgelegt, die folgenden zentralen Cybersicherheitsfunktionen zu erfüllen: (2) Nutzung einer defensiven Infrastruktur und Umsetzung von Richtlinien und Verfahren zum Schutz der Informationssysteme des abgedeckten Unternehmens und der in diesen Informationssystemen gespeicherten nicht öffentlichen Informationen vor unbefugtem Zugriff, unbefugter Nutzung oder anderen böswilligen Handlungen.	vpc-sg-open-only-to-authorized-ports	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass gemeinsame Ports für Amazon Elastic Compute Cloud (Amazon EC2) -Sicherheitsgruppen eingeschränkt sind. Wenn der Zugriff auf Ports nicht auf vertrauenswürdige Quellen beschränkt wird, kann dies zu Angriffen auf die Verfügbarkeit, Integrität und Vertraulichkeit von Systemen führen. Durch die Beschränkung des Zugriffs auf Ressourcen innerhalb einer Sicherheitsgruppe aus dem Internet (0.0.0.0/0) kann der Fernzugriff auf interne Systeme gesteuert werden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
500.02(b)(2)	(b) Das Cybersicherheitsprogramm basiert auf der Risikobeurteilung des abgedeckten Unternehmens und ist darauf ausgelegt, die folgenden zentralen Cybersicherheitsfunktionen zu erfüllen: (2) Nutzung einer defensiven Infrastruktur und Umsetzung von Richtlinien und Verfahren zum Schutz der Informationssysteme des abgedeckten Unternehmens und der in diesen Informationssystemen gespeicherten nicht öffentlichen Informationen vor unbefugtem Zugriff, unbefugter Nutzung oder anderen böswilligen Handlungen.	alb-waf-enabled	Stellen Sie sicher, dass AWS WAF auf Elastic Load Balancers (ELB) aktiviert ist, um Webanwendungen zu schützen. Eine WAF trägt zum Schutz Ihrer Webanwendungen oder APIs vor gängigen Web-Exploits bei. Diese Web-Exploits können sich auf die Verfügbarkeit auswirken, die Sicherheit gefährden oder übermäßige Ressourcen in Ihrer Umgebung verbrauchen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
500.02(b)(2)	(b) Das Cybersicherheitsprogramm basiert auf der Risikobeurteilung des abgedeckten Unternehmens und ist darauf ausgelegt, die folgenden zentralen Cybersicherheitsfunktionen zu erfüllen: (2) Nutzung einer defensiven Infrastruktur und Umsetzung von Richtlinien und Verfahren zum Schutz der Informationssysteme des abgedeckten Unternehmens und der in diesen Informationssystemen gespeicherten nicht öffentlichen Informationen vor unbefugtem Zugriff, unbefugter Nutzung oder anderen böswilligen Handlungen.	api-gw-associated-with-WAF	AWS Mit WAF können Sie eine Reihe von Regeln (als Web Access Control List (Web ACL) bezeichnet) konfigurieren, die Webanfragen auf der Grundlage von anpassbaren Websicherheitsregeln und -bedingungen, die Sie definieren, zulassen, blockieren oder zählen. Stellen Sie sicher, dass Ihre Amazon-API-Gateway-Stufe mit einer WAF-Web-ACL verknüpft ist, um sie vor böswilligen Angriffen zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
500.02(b)(2)	(b) Das Cybersicherheitsprogramm basiert auf der Risikobeurteilung des abgedeckten Unternehmens und ist darauf ausgelegt, die folgenden zentralen Cybersicherheitsfunktionen zu erfüllen: (2) Nutzung einer defensiven Infrastruktur und Umsetzung von Richtlinien und Verfahren zum Schutz der Informationssysteme des abgedeckten Unternehmens und der in diesen Informationssystemen gespeicherten nicht öffentlichen Informationen vor unbefugtem Zugriff, unbefugter Nutzung oder anderen böswilligen Handlungen.	no-unrestricted-route-to-igw	Stellen Sie sicher, dass EC2 Amazon-Routentabellen keine uneingeschränkten Routen zu einem Internet-Gateway enthalten. Durch das Entfernen oder Beschränken des Internetzugangs für Workloads innerhalb von Amazon VPCs können unbeabsichtigte Zugriffe in Ihrer Umgebung reduziert werden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
500.02(b)(2)	(b) Das Cybersicherheitsprogramm basiert auf der Risikobeurteilung des abgedeckten Unternehmens und ist darauf ausgelegt, die folgenden zentralen Cybersicherheitsfunktionen zu erfüllen: (2) Nutzung einer defensiven Infrastruktur und Umsetzung von Richtlinien und Verfahren zum Schutz der Informationssysteme des abgedeckten Unternehmens und der in diesen Informationssystemen gespeicherten nicht öffentlichen Informationen vor unbefugtem Zugriff, unbefugter Nutzung oder anderen böswilligen Handlungen.	s3- -blöcke-periodisch account-level-public-access	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Simple Storage Service (Amazon S3) -Buckets nicht öffentlich zugänglich sind. Diese Regel trägt dazu bei, sensible Daten vor unbefugten Remote-Benutzern zu schützen, indem sie den öffentlichen Zugriff verhindert. Mit dieser Regel können Sie optional die Parameter ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) und restrictPublicBuckets Parameter (Config Default: True) festlegen. Die tatsächlichen Werte müssen den Richtlini

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			en Ihrer Organisation entsprechen.
500.02(b)(2)	(b) Das Cybersicherheitsprogramm basiert auf der Risikobeurteilung des abgedeckten Unternehmens und ist darauf ausgelegt, die folgenden zentralen Cybersicherheitsfunktionen zu erfüllen: (2) Nutzung einer defensiven Infrastruktur und Umsetzung von Richtlinien und Verfahren zum Schutz der Informationssysteme des abgedeckten Unternehmens und der in diesen Informationssystemen gespeicherten nicht öffentlichen Informationen vor unbefugtem Zugriff, unbefugter Nutzung oder anderen böswilligen Handlungen.	ssm-document-not-public	Stellen Sie sicher, dass AWS Systems Manager (SSM) - Dokumente nicht öffentlich sind, da dies einen unbeabsichtigten Zugriff auf Ihre SSM-Dokumente ermöglichen kann. Ein öffentliches SSM-Dokument kann Informationen über Ihr Konto, Ihre Ressourcen und internen Prozesse preisgeben.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
500.02(b)(2)	(b) Das Cybersicherheitsprogramm basiert auf der Risikobeurteilung des abgedeckten Unternehmens und ist darauf ausgelegt, die folgenden zentralen Cybersicherheitsfunktionen zu erfüllen: (2) Nutzung einer defensiven Infrastruktur und Umsetzung von Richtlinien und Verfahren zum Schutz der Informationssysteme des abgedeckten Unternehmens und der in diesen Informationssystemen gespeicherten nicht öffentlichen Informationen vor unbefugtem Zugriff, unbefugter Nutzung oder anderen böswilligen Handlungen.	opensearch-in-vpc-only	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass sich Amazon OpenSearch Service-Domains innerhalb einer Amazon Virtual Private Cloud (Amazon VPC) befinden. Eine Amazon OpenSearch Service-Domain innerhalb einer Amazon VPC ermöglicht die sichere Kommunikation zwischen Amazon OpenSearch Service und anderen Services innerhalb der Amazon VPC, ohne dass ein Internet-Gateway, ein NAT-Gerät oder eine VPN-Verbindung erforderlich ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
500.02(b)(3)	(b) Das Cybersicherheitsprogramm basiert auf der Risikobeurteilung des abgedeckten Unternehmens und ist darauf ausgelegt, die folgenden zentralen Cybersicherheitsfunktionen zu erfüllen: (3) Erkennung von Cybersicherheitsereignissen.	opensearch-logs-to-cloudwatch	Stellen Sie sicher, dass für Amazon OpenSearch Service-Domains Fehlerprotokolle aktiviert und zur Aufbewahrung und Beantwortung an Amazon CloudWatch Logs gestreamt werden. OpenSearch Service-Fehlerprotokolle können bei Sicherheits- und Zugriffsprüfungen helfen und bei der Diagnose von Verfügbarkeitsproblemen helfen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
500.02(b)(3)	(b) Das Cybersicherheitsprogramm basiert auf der Risikobeurteilung des abgedeckten Unternehmens und ist darauf ausgelegt, die folgenden zentralen Cybersicherheitsfunktionen zu erfüllen: (3) Erkennung von Cybersicherheitsereignissen.	guardduty-enabled-centralized	Amazon GuardDuty kann mithilfe von Threat Intelligence Feeds helfen, potenzielle Cybersicherheitsereignisse zu überwachen und zu erkennen. Dazu gehören Listen mit bösartigen IPs und maschinellen Lernmethoden zur Identifizierung unerwarteter, nicht autorisierter und bösartiger Aktivitäten in Ihrer AWS Cloud-Umgebung.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
500.02(b)(3)	(b) Das Cybersicherheitsprogramm basiert auf der Risikobeurteilung des abgedeckten Unternehmens und ist darauf ausgelegt, die folgenden zentralen Cybersicherheitsfunktionen zu erfüllen: (3) Erkennung von Cybersicherheitsereignissen.	securityhub-enabled	AWS Security Hub hilft bei der Überwachung von unbefugtem Personal, Verbindungen, Geräten und Software. AWS Security Hub aggregiert, organisiert und priorisiert die Sicherheitswarnungen oder Ergebnisse mehrerer Dienste. AWS Einige dieser Dienste sind Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer und AWS Firewall Manager sowie AWS Partnerlösungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
500.02(b)(3)	(b) Das Cybersicherheitsprogramm basiert auf der Risikobeurteilung des abgedeckten Unternehmens und ist darauf ausgelegt, die folgenden zentralen Cybersicherheitsfunktionen zu erfüllen: (3) Erkennung von Cybersicherheitsereignissen.	api-gw-execution-logging-aktiviert	Die API-Gateway-Protokollierung zeigt detaillierte Ansichten der Benutzer, die auf die API zugegriffen haben, und wie diese Benutzer auf die API zugegriffen haben. Diese Einblicke ermöglichen die Transparenz von Benutzeraktivitäten.
500.02(b)(3)	(b) Das Cybersicherheitsprogramm basiert auf der Risikobeurteilung des abgedeckten Unternehmens und ist darauf ausgelegt, die folgenden zentralen Cybersicherheitsfunktionen zu erfüllen: (3) Erkennung von Cybersicherheitsereignissen.	cloud-trail-cloud-watch-logs-aktiviert	Verwenden Sie Amazon CloudWatch , um Protokollereignisaktivitäten zentral zu sammeln und zu verwalten. Die Aufnahme von AWS CloudTrail Daten liefert Einzelheiten zu den API-Aufrufaktivitäten in Ihrem AWS-Konto.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
500.02(b)(3)	(b) Das Cybersicherheitsprogramm basiert auf der Risikobeurteilung des abgedeckten Unternehmens und ist darauf ausgelegt, die folgenden zentralen Cybersicherheitsfunktionen zu erfüllen: (3) Erkennung von Cybersicherheitsereignissen.	cloudtrail-enabled	AWS CloudTrail kann bei der Nichtabstreitbarkeit helfen, indem Aktionen und API-Aufrufe der AWS Management Console aufgezeichnet werden. Sie können die Benutzer und die Benutzer AWS-Konten , die einen AWS Dienst aufgerufen haben, die Quell-IP-Adresse, über die die Aufrufe generiert wurden, und den Zeitpunkt der Anrufe identifizieren. Einzelheiten zu den erfassten Daten finden Sie in den AWS CloudTrail Datensatzinhalten.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
500.02(b)(3)	(b) Das Cybersicherheitsprogramm basiert auf der Risikobeurteilung des abgedeckten Unternehmens und ist darauf ausgelegt, die folgenden zentralen Cybersicherheitsfunktionen zu erfüllen: (3) Erkennung von Cybersicherheitsereignissen.	redshift-audit-logging-enabled	Aktivieren Sie die Prüfungsprotokollierung, um Informationen über Verbindungen und Benutzeraktivitäten in Ihrem Amazon-Redshift-Cluster zu erfassen.
500.02(b)(3)	(b) Das Cybersicherheitsprogramm basiert auf der Risikobeurteilung des abgedeckten Unternehmens und ist darauf ausgelegt, die folgenden zentralen Cybersicherheitsfunktionen zu erfüllen: (3) Erkennung von Cybersicherheitsereignissen.	ec-2 instance-detailed-monitoring-enabled	Aktivieren Sie diese Regel, um die Amazon Elastic Compute Cloud (Amazon EC2) - Instance-Überwachung auf der EC2 Amazon-Konsole zu verbessern, in der Monitoring-Diagramme mit einem Zeitraum von 1 Minute für die Instance angezeigt werden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
500.02(b)(3)	(b) Das Cybersicherheitsprogramm basiert auf der Risikobeurteilung des abgedeckten Unternehmens und ist darauf ausgelegt, die folgenden zentralen Cybersicherheitsfunktionen zu erfüllen: (3) Erkennung von Cybersicherheitsereignissen.	ec2-check managedinstance-association-compliance-status	Verwenden Sie AWS Systems Manager Associations, um bei der Inventarisierung von Softwareplattformen und Anwendungen innerhalb eines Unternehmens zu helfen. AWS Systems Manager weist Ihren verwalteten Instanzen einen Konfigurationsstatus zu und ermöglicht es Ihnen, Basiswerte für Betriebssystem-Patch-Levels, Softwareinstallationen, Anwendungskonfigurationen und andere Details zu Ihrer Umgebung festzulegen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
500.02(b)(3)	(b) Das Cybersicherheitsprogramm basiert auf der Risikobeurteilung des abgedeckten Unternehmens und ist darauf ausgelegt, die folgenden zentralen Cybersicherheitsfunktionen zu erfüllen: (3) Erkennung von Cybersicherheitsereignissen.	elasticsearch-logs-to-cloudwatch	Stellen Sie sicher, dass für Amazon OpenSearch Service-Domains Fehlerprotokolle aktiviert und zur Aufbewahrung und Beantwortung an Amazon CloudWatch Logs gestreamt werden. Domain-Fehlerprotokolle sind bei Sicherheits- und Zugriffsprüfungen sowie bei der Diagnose von Verfügbarkeitsproblemen nützlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
500.02(b)(3)	(b) Das Cybersicherheitsprogramm basiert auf der Risikobeurteilung des abgedeckten Unternehmens und ist darauf ausgelegt, die folgenden zentralen Cybersicherheitsfunktionen zu erfüllen: (3) Erkennung von Cybersicherheitsereignissen.	rds-enhanced-monitoring-enabled	Aktivieren Sie Amazon Relational Database Service (Amazon RDS), um die Verfügbarkeit von Amazon RDS zu überwachen. Dies bietet einen detaillierten Einblick in den Zustand Ihrer Amazon-RDS-Datenbank-Instances. Wenn der Amazon-RDS-Speicher mehr als ein zugrunde liegendes physisches Gerät verwendet, erfasst Enhanced Monitoring die Daten für jedes Gerät. Wenn die Amazon-RDS-Datenbank-Instance in einer Multi-AZ-Bereitstellung ausgeführt wird, werden außerdem die Daten für jedes Gerät auf dem sekundären Host sowie die Metriken des sekundären Hosts erfasst.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
500.02(b)(3)	(b) Das Cybersicherheitsprogramm basiert auf der Risikobeurteilung des abgedeckten Unternehmens und ist darauf ausgelegt, die folgenden zentralen Cybersicherheitsfunktionen zu erfüllen: (3) Erkennung von Cybersicherheitsereignissen.	cloudtrail-s3-dataevents-enabled	Die Erfassung von Simple Storage Service (Amazon S3)-Datenereignissen unterstützt die Erkennung von ungewöhnlichen Aktivitäten. Zu den Details gehören AWS-Konto Informationen über den Zugriff auf einen Amazon S3 S3-Bucket, die IP-Adresse und die Uhrzeit des Ereignisses.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
500.02(b)(3)	(b) Das Cybersicherheitsprogramm basiert auf der Risikobeurteilung des abgedeckten Unternehmens und ist darauf ausgelegt, die folgenden zentralen Cybersicherheitsfunktionen zu erfüllen: (3) Erkennung von Cybersicherheitsereignissen.	elb-logging-enabled	Die Elastic-Load-Balancing-Aktivität ist ein zentraler Kommunikationspunkt innerhalb einer Umgebung. Stellen Sie sicher, dass die ELB-Protokollierung aktiviert ist. Die gesammelten Daten enthalten detaillierte Informationen zu Anfragen, die an den ELB gesendet wurden. Jedes Protokoll enthält Informationen wie die Zeit, zu der die Anforderung einging, die Client-IP-Adresse, Latenzen, Anforderungspfade und Serverantworten.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
500.02(b)(3)	(b) Das Cybersicherheitsprogramm basiert auf der Risikobeurteilung des abgedeckten Unternehmens und ist darauf ausgelegt, die folgenden zentralen Cybersicherheitsfunktionen zu erfüllen: (3) Erkennung von Cybersicherheitsereignissen.	multi-region-cloudtrail-enabled	AWS CloudTrail zeichnet Aktionen und API-Aufrufe der AWS Management Console auf. Sie können feststellen, welche Benutzer und Konten angerufen wurden AWS, von welcher Quell-IP-Adresse aus die Anrufe getätigt wurden und wann die Anrufe erfolgten. CloudTrail übermittelt Protokolldateien aus allen AWS Regionen an Ihren S3-Bucket, wenn MULTI_REGION_CLOUD_TRAIL_ENABLED aktiviert ist. Außerdem wird beim AWS Start einer neuen Region derselbe Trail in der neuen Region erstellt. CloudTrail Dadurch erhalten Sie automatisch Protokolldateien mit API-Aktivitäten für die neue Region.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
500.02(b)(3)	(b) Das Cybersicherheitsprogramm basiert auf der Risikobeurteilung des abgedeckten Unternehmens und ist darauf ausgelegt, die folgenden zentralen Cybersicherheitsfunktionen zu erfüllen: (3) Erkennung von Cybersicherheitsereignissen.	s-3 bucket-logging-enabled	Die Amazon Simple Storage Service (Amazon S3)-Serverzugriffsprotokollierung bietet eine Methode zur Überwachung des Netzwerks im Hinblick auf potenzielle Cybersicherheitsereignisse. Die Ereignisse werden überwacht, indem detaillierte Aufzeichnungen über die Anfragen erfasst werden, die an einen Amazon-S3-Bucket gestellt wurden. Jeder Zugriffsprotokolleintrag enthält Details zu einer einzelnen Zugriffsanfrage. Zu den Details gehören Auftraggeber, Bucket-Name, Anforderungszeit, Anforderungsaktion, Antwortstatus und Fehlercode, falls relevant.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
500.02(b)(3)	(b) Das Cybersicherheitsprogramm basiert auf der Risikobeurteilung des abgedeckten Unternehmens und ist darauf ausgelegt, die folgenden zentralen Cybersicherheitsfunktionen zu erfüllen: (3) Erkennung von Cybersicherheitsereignissen.	opensearch-audit-logging-enabled	Stellen Sie sicher, dass die Audit-Protokollierung für Ihre Amazon OpenSearch Service-Domains aktiviert ist. Mit der Audit-Protokollierung können Sie Benutzeraktivitäten auf Ihren OpenSearch Domains verfolgen, einschließlich erfolgreicher und fehlgeschlagener Authentifizierungen OpenSearch, Anfragen an, Indexänderungen und eingehende Suchanfragen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
500.02(b)(3)	(b) Das Cybersicherheitsprogramm basiert auf der Risikobeurteilung des abgedeckten Unternehmens und ist darauf ausgelegt, die folgenden zentralen Cybersicherheitsfunktionen zu erfüllen: (3) Erkennung von Cybersicherheitsereignissen.	vpc-flow-logs-enabled	VPC-Flow-Protokolle erfassen detaillierte Informationsdatensätze über den IP-Datenverkehr, der zu und von Netzwerkschnittstellen in Ihrer Amazon Virtual Private Cloud (Amazon VPC) fließt. Standardmäßig enthalten Flow-Protokolldatensätze Werte für die verschiedenen Komponenten des IP-Flows, einschließlich Quelle, Ziel und Protokoll.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
500.02(b)(3)	(b) Das Cybersicherheitsprogramm basiert auf der Risikobeurteilung des abgedeckten Unternehmens und ist darauf ausgelegt, die folgenden zentralen Cybersicherheitsfunktionen zu erfüllen: (3) Erkennung von Cybersicherheitsereignissen.	codebuild-project-logging-enabled	Stellen Sie sicher, dass die AWS CodeBuild Projektprotokollierung aktiviert ist, damit Ihre Build-Ausgabeprotokolle entweder an Amazon CloudWatch oder Amazon Simple Storage Service (Amazon S3) gesendet werden. Build-Ausgabeprotokolle enthalten detaillierte Informationen zu Ihrem Build-Projekt.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
500.02(b)(3)	(b) Das Cybersicherheitsprogramm basiert auf der Risikobeurteilung des abgedeckten Unternehmens und ist darauf ausgelegt, die folgenden zentralen Cybersicherheitsfunktionen zu erfüllen: (3) Erkennung von Cybersicherheitsereignissen.	rds-logging-enabled	Um die Protokollierung und Überwachung in Ihrer Umgebung zu erleichtern, stellen Sie sicher, dass die Amazon Relational Database Service (Amazon RDS)-Protokollierung aktiviert ist. Mit der Amazon-RDS-Protokollierung können Sie Ereignisse wie Verbindungen, Verbindungsabbrüche, Abfragen oder abgefragte Tabellen erfassen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
500.02(b)(3)	(b) Das Cybersicherheitsprogramm basiert auf der Risikobeurteilung des abgedeckten Unternehmens und ist darauf ausgelegt, die folgenden zentralen Cybersicherheitsfunktionen zu erfüllen: (3) Erkennung von Cybersicherheitsereignissen.	wafv2-logging-enabled	Um die Protokollierung und Überwachung in Ihrer Umgebung zu erleichtern, aktivieren Sie die AWS WAF (V2) -Protokollierung im regionalen und globalen Web ACLs. AWS Die WAF-Protokollierung bietet detaillierte Informationen über den Datenverkehr, der von Ihrer Web-ACL analysiert wird. In den Protokollen werden die Uhrzeit aufgezeichnet, zu der die AWS WAF die Anfrage von Ihrer AWS Ressource erhalten hat, Informationen über die Anfrage und eine Aktion für die Regel, der jede Anfrage entsprach.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
500.02(b)(3)	(b) Das Cybersicherheitsprogramm basiert auf der Risikobeurteilung des abgedeckten Unternehmens und ist darauf ausgelegt, die folgenden zentralen Cybersicherheitsfunktionen zu erfüllen: (3) Erkennung von Cybersicherheitsereignissen.	redshift-cluster-configuration-check	Um Daten im Ruhezustand zu schützen, muss die Verschlüsselung für Ihre Amazon-Redshift-Cluster aktiviert sein. Sie müssen auch sicherstellen, dass die erforderlichen Konfigurationen auf Amazon-Redshift-Clustern bereitgestellt werden. Die Prüfungsprotokollierung muss aktiviert sein, um Informationen zu Verbindungen und Benutzeraktivitäten in der Datenbank bereitzustellen. Diese Regel erfordert, dass ein Wert für clusterDbEncrypted (Config Default: TRUE) und LoggingEnabled (Config Default: TRUE) gesetzt ist. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
500.02(b)(5)	(b) Das Cybersicherheitsprogramm basiert auf der Risikobeurteilung des abgedeckten Unternehmens und ist darauf ausgelegt, die folgenden zentralen Cybersicherheitsfunktionen zu erfüllen: (5) Wiederherstellung nach Cybersicherheitsereignissen und Wiederherstellung des normalen Betriebs und der Services.	db-instance-backup-enabled	Die Sicherungsfunktion von Amazon RDS erstellt Sicherungen Ihrer Datenbanken und Transaktionsprotokolle. Amazon RDS erstellt einen Snapshot für das Speichervolume Ihrer DB-Instance, sodass die gesamte DB-Instance gesichert wird. Sie können im System spezifische Aufbewahrungsfristen festlegen, um Ihre Ausfallsicherheitsanforderungen zu erfüllen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
500.02(b)(5)	(b) Das Cybersicherheitsprogramm basiert auf der Risikobeurteilung des abgedeckten Unternehmens und ist darauf ausgelegt, die folgenden zentralen Cybersicherheitsfunktionen zu erfüllen: (5) Wiederherstellung nach Cybersicherheitsereignissen und Wiederherstellung des normalen Betriebs und der Services.	redshift-backup-enabled	Stellen Sie zur Unterstützung der Datensicherungsprozesse sicher, dass Ihre Amazon-Redshift-Cluster über automatisierte Snapshots verfügen. Wenn automatisierte Snapshots für einen Cluster aktiviert sind, erstellt Redshift in regelmäßigen Abständen Snapshots dieses Clusters. Standardmäßig erstellt Redshift alle acht Stunden oder alle 5 GB einen Snapshot für jeden Knoten mit Datenänderungen oder je nachdem, was zuerst eintritt.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
500.02(b)(5)	(b) Das Cybersicherheitsprogramm basiert auf der Risikobeurteilung des abgedeckten Unternehmens und ist darauf ausgelegt, die folgenden zentralen Cybersicherheitsfunktionen zu erfüllen: (5) Wiederherstellung nach Cybersicherheitsereignissen und Wiederherstellung des normalen Betriebs und der Services.	dynamodb-pitr-enabled	Aktivieren Sie diese Regel, um zu überprüfen, ob die Informationen gesichert wurden. Es verwaltet auch die Backups, indem es sicherstellt, dass die point-in-time Wiederherstellung in Amazon DynamoDB aktiviert ist. Bei der Wiederherstellung werden fortlaufende Sicherungen Ihrer Tabelle für die letzten 35 Tage gespeichert.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
500.02(b)(5)	(b) Das Cybersicherheitsprogramm basiert auf der Risikobeurteilung des abgedeckten Unternehmens und ist darauf ausgelegt, die folgenden zentralen Cybersicherheitsfunktionen zu erfüllen: (5) Wiederherstellung nach Cybersicherheitsereignissen und Wiederherstellung des normalen Betriebs und der Services.	ebs-optimized-instance	Eine optimierte Instance im Amazon Elastic Block Store (Amazon EBS) bietet zusätzliche, dedizierte Kapazität für Amazon-EBS-I/O-Vorgänge. Diese Optimierung garantiert eine optimale Leistung für Ihr EBS-Volume, indem die Konflikte zwischen Amazon Amazon-EBS-I/O und anderem Datenverkehr von Ihrer Instance minimiert werden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
500.02(b)(5)	(b) Das Cybersicherheitsprogramm basiert auf der Risikobeurteilung des abgedeckten Unternehmens und ist darauf ausgelegt, die folgenden zentralen Cybersicherheitsfunktionen zu erfüllen: (5) Wiederherstellung nach Cybersicherheitsereignissen und Wiederherstellung des normalen Betriebs und der Services.	elasticache-redis-cluster-automatic-Backup-Prüfung	Wenn automatische Backups aktiviert sind, ElastiCache erstellt Amazon täglich ein Backup des Clusters. Die Sicherung kann für eine von Ihrer Organisation festgelegte Anzahl von Tagen aufbewahrt werden. Automatische Backups schützen vor Datenverlust. Bei einem Ausfall können Sie einen neuen Cluster erstellen, der Ihre Daten aus der aktuellen Sicherung wiederherstellt.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
500.02(b)(5)	(b) Das Cybersicherheitsprogramm basiert auf der Risikobeurteilung des abgedeckten Unternehmens und ist darauf ausgelegt, die folgenden zentralen Cybersicherheitsfunktionen zu erfüllen: (5) Wiederherstellung nach Cybersicherheitsereignissen und Wiederherstellung des normalen Betriebs und der Services.	s-3 bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) unterstützt die Aufrechterhaltung einer angemessenen Kapazität und Verfügbarkeit. CRR ermöglicht das automatische, asynchrone Kopieren von Objekten in Amazon-S3-Buckets, um die Datenverfügbarkeit sicherzustellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
500.02(b)(5)	(b) Das Cybersicherheitsprogramm basiert auf der Risikobeurteilung des abgedeckten Unternehmens und ist darauf ausgelegt, die folgenden zentralen Cybersicherheitsfunktionen zu erfüllen: (5) Wiederherstellung nach Cybersicherheitsereignissen und Wiederherstellung des normalen Betriebs und der Services.	s-3 bucket-versioning-enabled	Die Versionsverwaltung von Amazon Simple Storage Service (Amazon S3)-Buckets hilft dabei, mehrere Varianten eines Objekts im selben Amazon-S3-Bucket zu speichern. Verwenden Sie die Versionsverwaltung, um sämtliche Versionen aller Objekte in Ihrem Amazon-S3-Bucket zu speichern, abzurufen oder wiederherzustellen. Mit der Versionsverwaltung können Sie Versionen sowohl nach unbeabsichtigten Benutzeraktionen als auch nach Anwendungsfehlern problemlos wiederherstellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
500.02(b)(5)	(b) Das Cybersicherheitsprogramm basiert auf der Risikobeurteilung des abgedeckten Unternehmens und ist darauf ausgelegt, die folgenden zentralen Cybersicherheitsfunktionen zu erfüllen: (5) Wiederherstellung nach Cybersicherheitsereignissen und Wiederherstellung des normalen Betriebs und der Services.	dynamodb-in-backup-plan	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon DynamoDB-Tabellen Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
500.02(b)(5)	(b) Das Cybersicherheitsprogramm basiert auf der Risikobeurteilung des abgedeckten Unternehmens und ist darauf ausgelegt, die folgenden zentralen Cybersicherheitsfunktionen zu erfüllen: (5) Wiederherstellung nach Cybersicherheitsereignissen und Wiederherstellung des normalen Betriebs und der Services.	ebs-in-backup-plan	Stellen Sie zur Unterstützung der Datensicherungsprozesse sicher, dass Ihre Amazon Elastic Block Store (Amazon EBS) -Volumes Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
500.02(b)(5)	(b) Das Cybersicherheitsprogramm basiert auf der Risikobeurteilung des abgedeckten Unternehmens und ist darauf ausgelegt, die folgenden zentralen Cybersicherheitsfunktionen zu erfüllen: (5) Wiederherstellung nach Cybersicherheitsereignissen und Wiederherstellung des normalen Betriebs und der Services.	efs-in-backup-plan	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon Elastic File System (Amazon EFS) -Dateisysteme Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
500.02(b)(5)	(b) Das Cybersicherheitsprogramm basiert auf der Risikobeurteilung des abgedeckten Unternehmens und ist darauf ausgelegt, die folgenden zentralen Cybersicherheitsfunktionen zu erfüllen: (5) Wiederherstellung nach Cybersicherheitsereignissen und Wiederherstellung des normalen Betriebs und der Services.	rds-in-backup-plan	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon Relational Database Service (Amazon RDS) -Instances Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
500.02(b)(5)	(b) Das Cybersicherheitsprogramm basiert auf der Risikobeurteilung des abgedeckten Unternehmens und ist darauf ausgelegt, die folgenden zentralen Cybersicherheitsfunktionen zu erfüllen: (5) Wiederherstellung nach Cybersicherheitsereignissen und Wiederherstellung des normalen Betriebs und der Services.	backup-plan-min-frequency-and-min-retention-check	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihr AWS Backup-Plan auf eine Mindestfrequenz und Aufbewahrung festgelegt ist. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen. Mit dieser Regel können Sie die Parameter requiredFrequencyValue (Config default: 1), requiredRetentionDays (Config default: 35) und requiredFrequencyUnit

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			(Config default: days) festlegen. Der tatsächliche Wert muss den Anforderungen Ihrer Organisation entsprechen.
500.02(b)(5)	(b) Das Cybersicherheitsprogramm basiert auf der Risikobeurteilung des abgedeckten Unternehmens und ist darauf ausgelegt, die folgenden zentralen Cybersicherheitsfunktionen zu erfüllen: (5) Wiederherstellung nach Cybersicherheitsereignissen und Wiederherstellung des normalen Betriebs und der Services.	backup-recovery-point-manual-löschen-deaktiviert	Stellen Sie sicher, dass Ihren AWS Backup-Wiederherstellungspunkten eine ressourcenbasierte Richtlinie zugeordnet ist, die das Löschen von Wiederherstellungspunkten verhindert. Die Verwendung einer ressourcenbasierten Richtlinie zur Verhinderung des Löschens von Wiederherstellungspunkten kann dazu beitragen, ein versehentliches oder absichtliches Löschen zu verhindern.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
500,05	Das Cybersicherheitsprogramm für jedes abgedeckte Unternehmen umfasst Überwachungs- und Testverfahren, die im Einklang mit der Risikobewertung des abgedeckten Unternehmens entwickelt wurden und dazu dienen, die Wirksamkeit des Cybersicherheitsprogramms des abgedeckten Unternehmens zu bewerten. Die Überwachung und Prüfung umfasst eine kontinuierliche Überwachung oder regelmäßige Penetrationstests und Schwachstellenbewertungen. In Ermangelung einer wirksamen kontinuierlichen Überwachung oder anderer Systeme zur laufenden Erkennung von Veränderungen an Informati	vuln-management-plan-exists (Prozessüberprüfung)	Stellen Sie sicher, dass ein Plan für das Schwachstellenmanagement entwickelt und implementiert wird, damit Sie über formell definierte Prozesse zur Behebung von Schwachstellen in Ihrer Umgebung verfügen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	onssystemen, die zu Schwachstellen führen oder darauf hinweisen könnten, führen die abgedeckten Unternehmen Folgendes durch: a) jährliche Penetrationstests der Informationssysteme des abgedeckten Unternehmens, die jedes Jahr auf der Grundlage relevanter identifizierter Risiken gemäß der Risikobewertung ermittelt werden, und (b) halbjährliche Schwachstellenbewertungen, einschließlich systematischer Scans oder Überprüfungen von Informationssystemen, die dazu geeignet sind, öffentlich bekannte Cybersicherheitsschwachstellen in den Informationssystemen des abgedeckten Unternehmens basierend auf der		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	Risikobewertung zu identifizieren.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
500.06(a)	(a) Jedes abgedeckte Unternehmen muss sicher Systeme betreiben, die, soweit zutreffend und auf der Grundlage der Risikobeurteilung, folgende Merkmale aufweisen: (1) Sie sind darauf ausgelegt, wesentliche Finanztransaktionen ausreichend zu rekonstruieren, um den normalen Betrieb und die Verpflichtungen des abgedeckten Unternehmens zu erfüllen, und (2) sie enthalten Audit Trails, die dazu dienen, Cybersicherheitsereignisse aufzudecken und darauf zu reagieren, bei denen eine begründete Wahrscheinlichkeit besteht, dass sie einen wesentlichen Teil des normalen Geschäftsbetriebs des abgedeckten Unternehmens	api-gw-execution-logging-aktiviert	Die API-Gateway-Protokollierung zeigt detaillierte Ansichten der Benutzer, die auf die API zugegriffen haben, und wie diese Benutzer auf die API zugegriffen haben. Diese Einblicke ermöglichen die Transparenz von Benutzeraktivitäten.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	erheblich beeinträchtigen.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
500.06(a)	(a) Jedes abgedeckte Unternehmen muss sicher Systeme betreiben, die, soweit zutreffend und auf der Grundlage der Risikobeurteilung, folgende Merkmale aufweisen: (1) Sie sind darauf ausgelegt, wesentliche Finanztransaktionen ausreichend zu rekonstruieren, um den normalen Betrieb und die Verpflichtungen des abgedeckten Unternehmens zu erfüllen, und (2) sie enthalten Audit Trails, die dazu dienen, Cybersicherheitsereignisse aufzudecken und darauf zu reagieren, bei denen eine begründete Wahrscheinlichkeit besteht, dass sie einen wesentlichen Teil des normalen Geschäftsbetriebs des abgedeckten Unternehmens	cloud-trail-cloud-watch-logs-aktiviert	Verwenden Sie Amazon CloudWatch , um Protokoll ereignisaktivitäten zentral zu sammeln und zu verwalten. Die Aufnahme von AWS CloudTrail Daten liefert Einzelheiten zu den API-Aufrufaktivitäten in Ihrem AWS-Konto.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	erheblich beeinträchtigen.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
500.06(a)	(a) Jedes abgedeckte Unternehmen muss sicher Systeme betreiben, die, soweit zutreffend und auf der Grundlage der Risikobeurteilung, folgende Merkmale aufweisen: (1) Sie sind darauf ausgelegt, wesentliche Finanztransaktionen ausreichend zu rekonstruieren, um den normalen Betrieb und die Verpflichtungen des abgedeckten Unternehmens zu erfüllen, und (2) sie enthalten Audit Trails, die dazu dienen, Cybersicherheitsereignisse aufzudecken und darauf zu reagieren, bei denen eine begründete Wahrscheinlichkeit besteht, dass sie einen wesentlichen Teil des normalen Geschäftsbetriebs des abgedeckten Unternehmens	cloudtrail-enabled	AWS CloudTrail kann bei der Nichtabstreitbarkeit helfen, indem Aktionen und API-Aufrufe der AWS Management Console aufgezeichnet werden. Sie können die Benutzer und die Benutzer AWS-Konten , die einen AWS Dienst aufgerufen haben, die Quell-IP-Adresse, über die die Aufrufe generiert wurden, und den Zeitpunkt der Anrufe identifizieren. Einzelheiten zu den erfassten Daten finden Sie in den AWS CloudTrail Datensatzinhalten.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	erheblich beeinträchtigen.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
500.06(a)	(a) Jedes abgedeckte Unternehmen muss sicher Systeme betreiben, die, soweit zutreffend und auf der Grundlage der Risikobeurteilung, folgende Merkmale aufweisen: (1) Sie sind darauf ausgelegt, wesentliche Finanztransaktionen ausreichend zu rekonstruieren, um den normalen Betrieb und die Verpflichtungen des abgedeckten Unternehmens zu erfüllen, und (2) sie enthalten Audit Trails, die dazu dienen, Cybersicherheitsereignisse aufzudecken und darauf zu reagieren, bei denen eine begründete Wahrscheinlichkeit besteht, dass sie einen wesentlichen Teil des normalen Geschäftsbetriebs des abgedeckten Unternehmens	cloudtrail-s3-dataevents-enabled	Die Erfassung von Simple Storage Service (Amazon S3)-Datenereignissen unterstützt die Erkennung von ungewöhnlichen Aktivitäten. Zu den Details gehören AWS-Konto Informationen über den Zugriff auf einen Amazon S3 S3-Bucket, die IP-Adresse und die Uhrzeit des Ereignisses.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	erheblich beeinträchtigen.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
500.06(a)	(a) Jedes abgedeckte Unternehmen muss sicher Systeme betreiben, die, soweit zutreffend und auf der Grundlage der Risikobeurteilung, folgende Merkmale aufweisen: (1) Sie sind darauf ausgelegt, wesentliche Finanztransaktionen ausreichend zu rekonstruieren, um den normalen Betrieb und die Verpflichtungen des abgedeckten Unternehmens zu erfüllen, und (2) sie enthalten Audit Trails, die dazu dienen, Cybersicherheitsereignisse aufzudecken und darauf zu reagieren, bei denen eine begründete Wahrscheinlichkeit besteht, dass sie einen wesentlichen Teil des normalen Geschäftsbetriebs des abgedeckten Unternehmens	elb-logging-enabled	Die Elastic-Load-Balancing-Aktivität ist ein zentraler Kommunikationspunkt innerhalb einer Umgebung. Stellen Sie sicher, dass die ELB-Protokollierung aktiviert ist. Die gesammelten Daten enthalten detaillierte Informationen zu Anfragen, die an den ELB gesendet wurden. Jedes Protokoll enthält Informationen wie die Zeit, zu der die Anforderung einging, die Client-IP-Adresse, Latenzen, Anforderungspfade und Serverantworten.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	erheblich beeinträchtigen.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
500.06(a)	(a) Jedes abgedeckte Unternehmen muss sicher Systeme betreiben, die, soweit zutreffend und auf der Grundlage der Risikobeurteilung, folgende Merkmale aufweisen: (1) Sie sind darauf ausgelegt, wesentliche Finanztransaktionen ausreichend zu rekonstruieren, um den normalen Betrieb und die Verpflichtungen des abgedeckten Unternehmens zu erfüllen, und (2) sie enthalten Audit Trails, die dazu dienen, Cybersicherheitsereignisse aufzudecken und darauf zu reagieren, bei denen eine begründete Wahrscheinlichkeit besteht, dass sie einen wesentlichen Teil des normalen Geschäftsbetriebs des abgedeckten Unternehmens	multi-region-cloudtrail-enabled	AWS CloudTrail zeichnet Aktionen und API-Aufrufe der AWS Management Console auf. Sie können feststellen, welche Benutzer und Konten angerufen wurden AWS, von welcher Quell-IP-Adresse aus die Anrufe getätigt wurden und wann die Anrufe erfolgten. CloudTrail übermittelt Protokolldateien aus allen AWS Regionen an Ihren S3-Bucket, wenn MULTI_REGION_CLOUD_TRAIL_ENABLED aktiviert ist. Außerdem wird beim AWS Start einer neuen Region derselbe Trail in der neuen Region erstellt. CloudTrail Dadurch erhalten Sie automatisch Protokolldateien mit API-Aktivitäten für die neue Region.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	erheblich beeinträchtigen.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
500.06(a)	(a) Jedes abgedeckte Unternehmen muss sicher Systeme betreiben, die, soweit zutreffend und auf der Grundlage der Risikobeurteilung, folgende Merkmale aufweisen: (1) Sie sind darauf ausgelegt, wesentliche Finanztransaktionen ausreichend zu rekonstruieren, um den normalen Betrieb und die Verpflichtungen des abgedeckten Unternehmens zu erfüllen, und (2) sie enthalten Audit Trails, die dazu dienen, Cybersicherheitsereignisse aufzudecken und darauf zu reagieren, bei denen eine begründete Wahrscheinlichkeit besteht, dass sie einen wesentlichen Teil des normalen Geschäftsbetriebs des abgedeckten Unternehmens	s-3 bucket-logging-enabled	Die Amazon Simple Storage Service (Amazon S3)-Serverzugriffsprotokollierung bietet eine Methode zur Überwachung des Netzwerks im Hinblick auf potenzielle Cybersicherheitsereignisse. Die Ereignisse werden überwacht, indem detaillierte Aufzeichnungen über die Anfragen erfasst werden, die an einen Amazon-S3-Bucket gestellt wurden. Jeder Zugriffsprotokolleintrag enthält Details zu einer einzelnen Zugriffsanfrage. Zu den Details gehören Auftraggeber, Bucket-Name, Anforderungszeit, Anforderungsaktion, Antwortstatus und Fehlercode, falls relevant.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	erheblich beeinträchtigen.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
500.06(a)	(a) Jedes abgedeckte Unternehmen muss sicher Systeme betreiben, die, soweit zutreffend und auf der Grundlage der Risikobeurteilung, folgende Merkmale aufweisen: (1) Sie sind darauf ausgelegt, wesentliche Finanztransaktionen ausreichend zu rekonstruieren, um den normalen Betrieb und die Verpflichtungen des abgedeckten Unternehmens zu erfüllen, und (2) sie enthalten Audit Trails, die dazu dienen, Cybersicherheitsereignisse aufzudecken und darauf zu reagieren, bei denen eine begründete Wahrscheinlichkeit besteht, dass sie einen wesentlichen Teil des normalen Geschäftsbetriebs des abgedeckten Unternehmens	vpc-flow-logs-enabled	VPC-Flow-Protokolle erfassen detaillierte Informationsdatensätze über den IP-Datenverkehr, der zu und von Netzwerkschnittstellen in Ihrer Amazon Virtual Private Cloud (Amazon VPC) fließt. Standardmäßig enthalten Flow-Protokolldatensätze Werte für die verschiedenen Komponenten des IP-Flows, einschließlich Quelle, Ziel und Protokoll.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	erheblich beeinträchtigen.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
500.06(a)	(a) Jedes abgedeckte Unternehmen muss sicher Systeme betreiben, die, soweit zutreffend und auf der Grundlage der Risikobeurteilung, folgende Merkmale aufweisen: (1) Sie sind darauf ausgelegt, wesentliche Finanztransaktionen ausreichend zu rekonstruieren, um den normalen Betrieb und die Verpflichtungen des abgedeckten Unternehmens zu erfüllen, und (2) sie enthalten Audit Trails, die dazu dienen, Cybersicherheitsereignisse aufzudecken und darauf zu reagieren, bei denen eine begründete Wahrscheinlichkeit besteht, dass sie einen wesentlichen Teil des normalen Geschäftsbetriebs des abgedeckten Unternehmens	rds-logging-enabled	Um die Protokollierung und Überwachung in Ihrer Umgebung zu erleichtern, stellen Sie sicher, dass die Amazon Relational Database Service (Amazon RDS)-Protokollierung aktiviert ist. Mit der Amazon-RDS-Protokollierung können Sie Ereignisse wie Verbindungen, Verbindungsabbrüche, Abfragen oder abgefragte Tabellen erfassen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	erheblich beeinträchtigen.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
500.06(a)	(a) Jedes abgedeckte Unternehmen muss sicher Systeme betreiben, die, soweit zutreffend und auf der Grundlage der Risikobeurteilung, folgende Merkmale aufweisen: (1) Sie sind darauf ausgelegt, wesentliche Finanztransaktionen ausreichend zu rekonstruieren, um den normalen Betrieb und die Verpflichtungen des abgedeckten Unternehmens zu erfüllen, und (2) sie enthalten Audit Trails, die dazu dienen, Cybersicherheitsereignisse aufzudecken und darauf zu reagieren, bei denen eine begründete Wahrscheinlichkeit besteht, dass sie einen wesentlichen Teil des normalen Geschäftsbetriebs des abgedeckten Unternehmens	codebuild-project-logging-enabled	Stellen Sie sicher, dass die AWS CodeBuild Projektprotokollierung aktiviert ist, damit Ihre Build-Ausgabeprotokolle entweder an Amazon CloudWatch oder Amazon Simple Storage Service (Amazon S3) gesendet werden. Build-Ausgabeprotokolle enthalten detaillierte Informationen zu Ihrem Build-Projekt.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	erheblich beeinträchtigen.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
500.06(a)	(a) Jedes abgedeckte Unternehmen muss sicher Systeme betreiben, die, soweit zutreffend und auf der Grundlage der Risikobeurteilung, folgende Merkmale aufweisen: (1) Sie sind darauf ausgelegt, wesentliche Finanztransaktionen ausreichend zu rekonstruieren, um den normalen Betrieb und die Verpflichtungen des abgedeckten Unternehmens zu erfüllen, und (2) sie enthalten Audit Trails, die dazu dienen, Cybersicherheitsereignisse aufzudecken und darauf zu reagieren, bei denen eine begründete Wahrscheinlichkeit besteht, dass sie einen wesentlichen Teil des normalen Geschäftsbetriebs des abgedeckten Unternehmens	redshift-audit-logging-enabled	Aktivieren Sie die Prüfungsprotokollierung, um Informationen über Verbindungen und Benutzeraktivitäten in Ihrem Amazon-Redshift-Cluster zu erfassen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	erheblich beeinträchtigen.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
500.06(a)	(a) Jedes abgedeckte Unternehmen muss sicher Systeme betreiben, die, soweit zutreffend und auf der Grundlage der Risikobeurteilung, folgende Merkmale aufweisen: (1) Sie sind darauf ausgelegt, wesentliche Finanztransaktionen ausreichend zu rekonstruieren, um den normalen Betrieb und die Verpflichtungen des abgedeckten Unternehmens zu erfüllen, und (2) sie enthalten Audit Trails, die dazu dienen, Cybersicherheitsereignisse aufzudecken und darauf zu reagieren, bei denen eine begründete Wahrscheinlichkeit besteht, dass sie einen wesentlichen Teil des normalen Geschäftsbetriebs des abgedeckten Unternehmens	wafv2-logging-enabled	Um die Protokollierung und Überwachung in Ihrer Umgebung zu erleichtern, aktivieren Sie die AWS WAF (V2) -Protokollierung im regionalen und globalen Web ACLs. AWS Die WAF-Protokollierung bietet detaillierte Informationen über den Datenverkehr, der von Ihrer Web-ACL analysiert wird. In den Protokollen werden die Uhrzeit aufgezeichnet, zu der die AWS WAF die Anfrage von Ihrer AWS Ressource erhalten hat, Informationen über die Anfrage und eine Aktion für die Regel, der jede Anfrage entsprach.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	erheblich beeinträchtigen.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
500.06(a)	(a) Jedes abgedeckte Unternehmen muss sicher Systeme betreiben, die, soweit zutreffend und auf der Grundlage der Risikobeurteilung, folgende Merkmale aufweisen: (1) Sie sind darauf ausgelegt, wesentliche Finanztransaktionen ausreichend zu rekonstruieren, um den normalen Betrieb und die Verpflichtungen des abgedeckten Unternehmens zu erfüllen, und (2) sie enthalten Audit Trails, die dazu dienen, Cybersicherheitsereignisse aufzudecken und darauf zu reagieren, bei denen eine begründete Wahrscheinlichkeit besteht, dass sie einen wesentlichen Teil des normalen Geschäftsbetriebs des abgedeckten Unternehmens	opensearch-audit-logging-enabled	Stellen Sie sicher, dass die Audit-Protokollierung für Ihre Amazon OpenSearch Service-Domains aktiviert ist. Mit der Audit-Protokollierung können Sie Benutzeraktivitäten auf Ihren OpenSearch Domains verfolgen, einschließlich erfolgreicher und fehlgeschlagener Authentifizierungen OpenSearch, Anfragen an, Indexänderungen und eingehende Suchanfragen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	erheblich beeinträchtigen.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
500.06(a)	(a) Jedes abgedeckte Unternehmen muss sicher Systeme betreiben, die, soweit zutreffend und auf der Grundlage der Risikobeurteilung, folgende Merkmale aufweisen: (1) Sie sind darauf ausgelegt, wesentliche Finanztransaktionen ausreichend zu rekonstruieren, um den normalen Betrieb und die Verpflichtungen des abgedeckten Unternehmens zu erfüllen, und (2) sie enthalten Audit Trails, die dazu dienen, Cybersicherheitsereignisse aufzudecken und darauf zu reagieren, bei denen eine begründete Wahrscheinlichkeit besteht, dass sie einen wesentlichen Teil des normalen Geschäftsbetriebs des abgedeckten Unternehmens	redshift-cluster-configuration-check	Um Daten im Ruhezustand zu schützen, muss die Verschlüsselung für Ihre Amazon-Redshift-Cluster aktiviert sein. Sie müssen auch sicherstellen, dass die erforderlichen Konfigurationen auf Amazon-Redshift-Clustern bereitgestellt werden. Die Prüfungsprotokollierung muss aktiviert sein, um Informationen zu Verbindungen und Benutzeraktivitäten in der Datenbank bereitzustellen. Diese Regel erfordert, dass ein Wert für clusterDbEncrypted (Config Default: TRUE) und LoggingEnabled (Config Default: TRUE) gesetzt ist. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	erheblich beeinträchtigen.		
500.06(b)	(b) Jedes abgedeckte Unternehmen muss die in Abschnitt 500.06(a)(1) dieses Teils vorgeschriebenen Aufzeichnungen mindestens fünf Jahre lang und die gemäß Abschnitt 500.06(a)(2) dieses Teils erforderlichen Aufzeichnungen mindestens drei Jahre lang aufbewahren.	cw-loggroup-retention-period-überprüfen	Stellen Sie sicher, dass die Ereignisprotokolldaten für Ihre Protokollgruppen über eine Mindestdauer aufbewahrt werden, um die Fehlerbehebung und forensische Untersuchungen zu unterstützen. Fehlende frühere Ereignisprotokolldaten erschweren die Rekonstruierung und Identifizierung potenziell schädlicher Ereignisse.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
500.06(a)	(a) Jedes abgedeckte Unternehmen muss sicher Systeme betreiben, die, soweit zutreffend und auf der Grundlage der Risikobeurteilung, folgende Merkmale aufweisen: (1) Sie sind darauf ausgelegt, wesentliche Finanztransaktionen ausreichend zu rekonstruieren, um den normalen Betrieb und die Verpflichtungen des abgedeckten Unternehmens zu erfüllen, und (2) sie enthalten Audit Trails, die dazu dienen, Cybersicherheitsereignisse aufzudecken und darauf zu reagieren, bei denen eine begründete Wahrscheinlichkeit besteht, dass sie einen wesentlichen Teil des normalen Geschäftsbetriebs des abgedeckten Unternehmens	elasticsearch-logs-to-cloudwatch	Stellen Sie sicher, dass für Amazon OpenSearch Service-Domains Fehlerprotokolle aktiviert und zur Aufbewahrung und Beantwortung an Amazon CloudWatch Logs gestreamt werden. Domain-Fehlerprotokolle sind bei Sicherheits- und Zugriffsprüfungen sowie bei der Diagnose von Verfügbarkeitsproblemen nützlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	erheblich beeinträchtigen.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
500.06(a)	(a) Jedes abgedeckte Unternehmen muss sicher Systeme betreiben, die, soweit zutreffend und auf der Grundlage der Risikobeurteilung, folgende Merkmale aufweisen: (1) Sie sind darauf ausgelegt, wesentliche Finanztransaktionen ausreichend zu rekonstruieren, um den normalen Betrieb und die Verpflichtungen des abgedeckten Unternehmens zu erfüllen, und (2) sie enthalten Audit Trails, die dazu dienen, Cybersicherheitsereignisse aufzudecken und darauf zu reagieren, bei denen eine begründete Wahrscheinlichkeit besteht, dass sie einen wesentlichen Teil des normalen Geschäftsbetriebs des abgedeckten Unternehmens	opensearch-logs-to-cloudwatch	Stellen Sie sicher, dass für Amazon OpenSearch Service-Domains Fehlerprotokolle aktiviert und zur Aufbewahrung und Beantwortung an Amazon CloudWatch Logs gestreamt werden. OpenSearch Service-Fehlerprotokolle können bei Sicherheits- und Zugriffsprüfungen helfen und bei der Diagnose von Verfügbarkeitsproblemen helfen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	erheblich beeinträchtigen.		
500.07	Im Rahmen ihres Cybersicherheitsprogramms beschränkt jedes abgedeckte Unternehmen auf der Grundlage der Risikobeurteilung des Unternehmens die Benutzerzugriffsberechtigungen auf Informationssysteme, die Zugang zu nicht öffentlichen Informationen bieten, und überprüft diese Zugriffsberechtigungen regelmäßig.	opensearch-in-vpc-only	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass sich Amazon OpenSearch Service-Domains innerhalb einer Amazon Virtual Private Cloud (Amazon VPC) befinden. Eine Amazon OpenSearch Service-Domain innerhalb einer Amazon VPC ermöglicht die sichere Kommunikation zwischen Amazon OpenSearch Service und anderen Services innerhalb der Amazon VPC, ohne dass ein Internet-Gateway, ein NAT-Gerät oder eine VPN-Verbindung erforderlich ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
500.07	Im Rahmen ihres Cybersicherheitsprogramms beschränkt jedes abgedeckte Unternehmen auf der Grundlage der Risikobeurteilung des Unternehmens die Benutzerzugriffsberechtigungen auf Informationssysteme, die Zugang zu nicht öffentlichen Informationen bieten, und überprüft diese Zugriffsberechtigungen regelmäßig.	access-keys-rotated	Die Anmeldeinformationen für autorisierte Geräte, Benutzer und Prozesse werden geprüft, indem sichergestellt wird, dass die IAM-Zugriffsschlüssel entsprechend den Vorgaben der Unternehmensrichtlinie rotiert werden. Das regelmäßige Ändern der Zugriffsschlüssel ist eine bewährte Sicherheitsmethode. Es verkürzt den Zeitraum, in dem ein Zugriffsschlüssel aktiv ist, und reduziert die Auswirkungen auf das Unternehmen, wenn die Schlüssel kompromittiert werden. Diese Regel erfordert einen Wert für die Zugriffsschlüssel-Rotation (Standardkonfiguration: 90). Der tatsächliche Wert muss den Richtlini

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			en Ihrer Organisation entsprechen.
500.07	Im Rahmen ihres Cybersicherheitsprogramms beschränkt jedes abgedeckte Unternehmen auf der Grundlage der Risikobeurteilung des Unternehmens die Benutzerzugriffsberechtigungen auf Informationssysteme, die Zugang zu nicht öffentlichen Informationen bieten, und überprüft diese Zugriffsberechtigungen regelmäßig.	ecs-task-definition-user-for-host-mode-check	Wenn für eine Aufgabendefinition erhöhte Berechtigungen gelten, liegt das daran, dass der Kunde diesen Konfigurationen ausdrücklich zugestimmt hat. Diese Kontrolle prüft, ob eine unerwartete Berechtigungseskalation vorliegt, wenn für eine Aufgabendefinition das Host-Netzwerk aktiviert ist, der Kunde aber keine erhöhten Berechtigungen aktiviert hat.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
500,07	Im Rahmen ihres Cybersicherheitsprogramms beschränkt jedes abgedeckte Unternehmen auf der Grundlage der Risikobeurteilung des Unternehmens die Benutzerzugriffsberechtigungen auf Informationssysteme, die Zugang zu nicht öffentlichen Informationen bieten, und überprüft diese Zugriffsberechtigungen regelmäßig.	no-unrestricted-route-to-igw	Stellen Sie sicher, dass EC2 Amazon-Routentabellen keine uneingeschränkten Routen zu einem Internet-Gateway enthalten. Durch das Entfernen oder Beschränken des Internetzugangs für Workloads innerhalb von Amazon VPCs können unbeabsichtigte Zugriffe in Ihrer Umgebung reduziert werden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
500.07	Im Rahmen ihres Cybersicherheitsprogramms beschränkt jedes abgedeckte Unternehmen auf der Grundlage der Risikobeurteilung des Unternehmens die Benutzerzugriffsberechtigungen auf Informationssysteme, die Zugang zu nicht öffentlichen Informationen bieten, und überprüft diese Zugriffsberechtigungen regelmäßig.	s3-Blöcke-periodisch account-level-public-access	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Simple Storage Service (Amazon S3) -Buckets nicht öffentlich zugänglich sind. Diese Regel trägt dazu bei, sensible Daten vor unbefugten Remote-Benutzern zu schützen, indem sie den öffentlichen Zugriff verhindert. Mit dieser Regel können Sie optional die Parameter ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) und restrictPublicBuckets Parameter (Config Default: True) festlegen. Die tatsächlichen Werte müssen den Richtlini

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			en Ihrer Organisation entsprechen.
500,07	Im Rahmen ihres Cybersicherheitsprogramms beschränkt jedes abgedeckte Unternehmen auf der Grundlage der Risikobeurteilung des Unternehmens die Benutzerzugriffsberechtigungen auf Informationssysteme, die Zugang zu nicht öffentlichen Informationen bieten, und überprüft diese Zugriffsberechtigungen regelmäßig.	ssm-document-not-public	Stellen Sie sicher, dass AWS Systems Manager (SSM) - Dokumente nicht öffentlich sind, da dies einen unbeabsichtigten Zugriff auf Ihre SSM-Dokumente ermöglichen kann. Ein öffentliches SSM-Dokument kann Informationen über Ihr Konto, Ihre Ressourcen und internen Prozesse preisgeben.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
500.07	Im Rahmen ihres Cybersicherheitsprogramms beschränkt jedes abgedeckte Unternehmen auf der Grundlage der Risikobeurteilung des Unternehmens die Benutzerzugriffsberechtigungen auf Informationssysteme, die Zugang zu nicht öffentlichen Informationen bieten, und überprüft diese Zugriffsberechtigungen regelmäßig.	subnet-auto-assign-public-ip-deaktiviert	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon Virtual Private Cloud (VPC) -Subnetzen nicht automatisch eine öffentliche IP-Adresse zugewiesen wird. Amazon Elastic Compute Cloud (EC2) -Instances, die in Subnetzen gestartet werden, in denen dieses Attribut aktiviert ist, haben ihrer primären Netzwerkschnittstelle eine öffentliche IP-Adresse zugewiesen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
500.07	Im Rahmen ihres Cybersicherheitsprogramms beschränkt jedes abgedeckte Unternehmen auf der Grundlage der Risikobeurteilung des Unternehmens die Benutzerzugriffsberechtigungen auf Informationssysteme, die Zugang zu nicht öffentlichen Informationen bieten, und überprüft diese Zugriffsberechtigungen regelmäßig.	iam-user-unused-credentials-überprüfen	AWS Identity and Access Management (IAM) kann Ihnen bei Zugriffsberechtigungen und Autorisierungen helfen, indem es nach IAM-Passwörtern und Zugriffsschlüsseln sucht, die für einen bestimmten Zeitraum nicht verwendet wurden. Wenn ungenutzte Anmeldeinformationen identifiziert werden, müssen Sie sie deaktivieren und/oder entfernen, da dies gegen das Prinzip der geringsten Berechtigung verstoßen könnte. Für diese Regel müssen Sie einen Wert für das maxCredentialUsage Alter festlegen (Standardkonfiguration: 90). Der tatsächliche Wert muss den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
500,07	Im Rahmen ihres Cybersicherheitsprogramms beschränkt jedes abgedeckte Unternehmen auf der Grundlage der Risikobeurteilung des Unternehmens die Benutzerzugriffsberechtigungen auf Informationssysteme, die Zugang zu nicht öffentlichen Informationen bieten, und überprüft diese Zugriffsberechtigungen regelmäßig.	secretsmanager-rotation-enabled-check	Diese Regel stellt sicher, dass bei AWS Secrets Manager Manager-Geheimnissen die Rotation aktiviert ist. Die regelmäßige Rotation von Secrets kann den Zeitraum verkürzen, in dem ein Secret aktiv ist, und möglicherweise die Auswirkungen auf das Unternehmen verringern, falls das Secret kompromittiert wird.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
500.07	Im Rahmen ihres Cybersicherheitsprogramms beschränkt jedes abgedeckte Unternehmen auf der Grundlage der Risikobeurteilung des Unternehmens die Benutzerzugriffsberechtigungen auf Informationssysteme, die Zugang zu nicht öffentlichen Informationen bieten, und überprüft diese Zugriffsberechtigungen regelmäßig.	secretsmanager-scheduled-rotation-success-überprüfen	Diese Regel stellt sicher, dass AWS Secrets Manager Manager-Geheimnisse gemäß dem Rotationsplan erfolgreich rotiert wurden. Die regelmäßige Rotation von Secrets kann den Zeitraum verkürzen, in dem ein Secret aktiv ist, und möglicherweise die Auswirkungen auf das Unternehmen verringern, falls es kompromittiert wird.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
500.07	Im Rahmen ihres Cybersicherheitsprogramms beschränkt jedes abgedeckte Unternehmen auf der Grundlage der Risikobeurteilung des Unternehmens die Benutzerzugriffsberechtigungen auf Informationssysteme, die Zugang zu nicht öffentlichen Informationen bieten, und überprüft diese Zugriffsberechtigungen regelmäßig.	emr-kerberos-enabled	Die Zugriffsberechtigungen und -autorisierungen können verwaltet und nach den Prinzipien der geringsten Berechtigung und Aufgabentrennung integriert werden, indem Kerberos für Amazon-EMR-Cluster aktiviert wird. In Kerberos werden Services und Benutzer, die sich authentifizieren müssen, als Prinzipale bezeichnet. Prinzipale befinden sich in einem Kerberos-Bereich. Innerhalb dieses Bereichs wird ein Kerberos-Server als Key Distribution Center (KDC) bezeichnet. Über diesen Server können sich Prinzipale authentifizieren. Die Authentifizierung im KDC erfolgt durch die Ausstellung von Authentif

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			izierungstickets. Das KDC unterhält eine Datenbank der Prinzipale in seinem Bereich mit ihren Passwörtern und anderen administrativen Informationen zu jedem Prinzipal.
500,07	Im Rahmen ihres Cybersicherheitsprogramms beschränkt jedes abgedeckte Unternehmen auf der Grundlage der Risikobeurteilung des Unternehmens die Benutzerzugriffsberechtigungen auf Informationssysteme, die Zugang zu nicht öffentlichen Informationen bieten, und überprüft diese Zugriffsberechtigungen regelmäßig.	iam-group-has-users-überprüfen	AWS Identity and Access Management (IAM) kann Ihnen helfen, die Prinzipien der geringsten Rechte und der Aufgabentrennung mit Zugriffsberechtigungen und Autorisierungen zu integrieren, indem sichergestellt wird, dass IAM-Gruppen mindestens einen Benutzer haben. Die Einteilung von Benutzern in Gruppen auf der Grundlage der ihnen zugewiesenen Berechtigungen oder ihrer Funktion ist eine Möglichkeit, das Prinzip der geringsten Berechtigung zu implementieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
500.07	Im Rahmen ihres Cybersicherheitsprogramms beschränkt jedes abgedeckte Unternehmen auf der Grundlage der Risikobeurteilung des Unternehmens die Benutzerzugriffsberechtigungen auf Informationssysteme, die Zugang zu nicht öffentlichen Informationen bieten, und überprüft diese Zugriffsberechtigungen regelmäßig.	iam-password-policy	Die Identitäten und Anmeldeinformationen werden auf der Grundlage einer organisatorischen IAM-Passwortrichtlinie ausgestellt, verwaltet und verifiziert. Sie erfüllen oder übertreffen die Anforderungen von NIST SP 800-63 und dem Standard „Best Practices“ von AWS Foundational Security für Passwortstärke. Mit dieser Regel können Sie optional RequireUppercaseCharacters (Wert für AWS grundlegende Sicherheitsbewährte Methoden: wahr), RequireLowercaseCharacters (Wert für bewährte Methoden für AWS grundlegende Sicherheit: wahr), RequireSymbols (Wert für bewährte Methoden für AWS grundlegende Sicherheit:

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			wahr), RequireNumbers (Wert für bewährte Methoden für AWS grundlegende Sicherheit: wahr), MinimumPasswordLength (Wert für bewährte Methoden für AWS grundlegende Sicherheit: 14), PasswordReusePrevention (Wert für bewährte Methoden für AWS grundlegende Sicherheit: 24) und MaxPasswordAge (Wert für bewährte Methoden für AWS grundlegende Sicherheit: 90) für Ihr IAM festlegen Kennwortrichtlinie. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
500.07	Im Rahmen ihres Cybersicherheitsprogramms beschränkt jedes abgedeckte Unternehmen auf der Grundlage der Risikobeurteilung des Unternehmens die Benutzerzugriffsberechtigungen auf Informationssysteme, die Zugang zu nicht öffentlichen Informationen bieten, und überprüft diese Zugriffsberechtigungen regelmäßig.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) kann Ihnen dabei helfen, die Prinzipien der geringsten Rechte und der Aufgabentrennung in Zugriffsberechtigungen und Autorisierungen zu integrieren und so zu verhindern, dass Richtlinien „Effect“: „Allow“ mit „Action“: „*“ anstelle von „Resource“: „*“ enthalten. Wenn Benutzern mehr Berechtigungen eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und Aufgabentrennung verstoßen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
500,07	Im Rahmen ihres Cybersicherheitsprogramms beschränkt jedes abgedeckte Unternehmen auf der Grundlage der Risikobeurteilung des Unternehmens die Benutzerzugriffsberechtigungen auf Informationssysteme, die Zugang zu nicht öffentlichen Informationen bieten, und überprüft diese Zugriffsberechtigungen regelmäßig.	iam-root-access-key-überprüfen	Der Zugriff auf Systeme und Ressourcen kann gesteuert werden, indem überprüft wird, ob der Root-Benutzer keine Zugriffsschlüssel mit seiner AWS Identity and Access Management (IAM) -Rolle verknüpft hat. Stellen Sie sicher, dass die Root-Zugriffsschlüssel gelöscht werden. Erstellen und verwenden Sie stattdessen rollenbasierte Funktionen, AWS-Konten um das Prinzip der geringsten Funktionalität zu berücksichtigen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
500.07	Im Rahmen ihres Cybersicherheitsprogramms beschränkt jedes abgedeckte Unternehmen auf der Grundlage der Risikobeurteilung des Unternehmens die Benutzerzugriffsberechtigungen auf Informationssysteme, die Zugang zu nicht öffentlichen Informationen bieten, und überprüft diese Zugriffsberechtigungen regelmäßig.	iam-user-group-membership-überprüfen	AWS Identity and Access Management (IAM) kann Ihnen helfen, Zugriffsberechtigungen und Autorisierungen einzuschränken, indem sichergestellt wird, dass Benutzer Mitglieder mindestens einer Gruppe sind. Wenn Benutzern mehr Berechtigungen eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und Aufgabentrennung verstoßen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
500.07	Im Rahmen ihres Cybersicherheitsprogramms beschränkt jedes abgedeckte Unternehmen auf der Grundlage der Risikobeurteilung des Unternehmens die Benutzerzugriffsberechtigungen auf Informationssysteme, die Zugang zu nicht öffentlichen Informationen bieten, und überprüft diese Zugriffsberechtigungen regelmäßig.	iam-user-no-policies-überprüfen	Diese Regel stellt sicher, dass AWS Identity and Access Management (IAM)-Richtlinien nur Gruppen oder Rollen zugewiesen werden, um den Zugriff auf Systeme und Ressourcen zu kontrollieren. Die Zuweisung von Berechtigungen auf Gruppen- oder Rollenebene trägt dazu bei, die Wahrscheinlichkeit zu verringern, dass eine Identität übermäßige Berechtigungen erhält oder beibehält.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
500.07	Im Rahmen ihres Cybersicherheitsprogramms beschränkt jedes abgedeckte Unternehmen auf der Grundlage der Risikobeurteilung des Unternehmens die Benutzerzugriffsberechtigungen auf Informationssysteme, die Zugang zu nicht öffentlichen Informationen bieten, und überprüft diese Zugriffsberechtigungen regelmäßig.	s-3 bucket-policy-grantee-check	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie s3_bucket_policy_grantee_check aktivieren. Diese Regel prüft, ob der vom Amazon S3 S3-Bucket gewährte Zugriff durch die von Ihnen bereitgestellten AWS Principals, Verbundbenutzer, Service Principals, IP-Adressen oder Amazon Virtual Private Cloud (Amazon VPC) IDs eingeschränkt ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
500.07	Im Rahmen ihres Cybersicherheitsprogramms beschränkt jedes abgedeckte Unternehmen auf der Grundlage der Risikobeurteilung des Unternehmens die Benutzerzugriffsberechtigungen auf Informationssysteme, die Zugang zu nicht öffentlichen Informationen bieten, und überprüft diese Zugriffsberechtigungen regelmäßig.	iam-no-inline-policy-überprüfen	Stellen Sie sicher, dass ein Benutzer, eine IAM-Rolle oder eine IAM-Gruppe (AWS Identity and Access Management) nicht über eine Inline-Richtlinie zur Zugriffskontrolle auf Systeme und Ressourcen verfügt. AWS empfiehlt, verwaltete Richtlinien anstelle von Inline-Richtlinien zu verwenden. Verwaltete Richtlinien ermöglichen Wiederverwendbarkeit, Versionsverwaltung, Rollback und Delegierung der Berechtigungsverwaltung.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
500.07	Im Rahmen ihres Cybersicherheitsprogramms beschränkt jedes abgedeckte Unternehmen auf der Grundlage der Risikobeurteilung des Unternehmens die Benutzerzugriffsberechtigungen auf Informationssysteme, die Zugang zu nicht öffentlichen Informationen bieten, und überprüft diese Zugriffsberechtigungen regelmäßig.	dms-replication-not-public	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass auf DMS-Replikationsinstanzen nicht öffentlich zugegriffen werden kann. DMS-Replikations-Instances können vertrauliche Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
500.07	Im Rahmen ihres Cybersicherheitsprogramms beschränkt jedes abgedeckte Unternehmen auf der Grundlage der Risikobeurteilung des Unternehmens die Benutzerzugriffsberechtigungen auf Informationssysteme, die Zugang zu nicht öffentlichen Informationen bieten, und überprüft diese Zugriffsberechtigungen regelmäßig.	ebs-snapshot-public-restorable-überprüfen	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass EBS-Snapshots nicht öffentlich wiederherstellbar sind. EBS-Volume–Snapshots können vertrauliche Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
500.07	Im Rahmen ihres Cybersicherheitsprogramms beschränkt jedes abgedeckte Unternehmen auf der Grundlage der Risikobeurteilung des Unternehmens die Benutzerzugriffsberechtigungen auf Informationssysteme, die Zugang zu nicht öffentlichen Informationen bieten, und überprüft diese Zugriffsberechtigungen regelmäßig.	ec-2 instance-no-public-ip	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon Elastic Compute Cloud (Amazon EC2) - Instances nicht öffentlich zugänglich sind. EC2 Amazon-Instances können vertrauliche Informationen enthalten, und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
500,07	Im Rahmen ihres Cybersicherheitsprogramms beschränkt jedes abgedeckte Unternehmen auf der Grundlage der Risikobeurteilung des Unternehmens die Benutzerzugriffsberechtigungen auf Informationssysteme, die Zugang zu nicht öffentlichen Informationen bieten, und überprüft diese Zugriffsberechtigungen regelmäßig.	elasticsearch-in-vpc-only	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass sich Amazon OpenSearch OpenSearch Service (Service) - Domains innerhalb einer Amazon Virtual Private Cloud (Amazon VPC) befinden. Eine OpenSearch Service-Domain innerhalb einer Amazon VPC ermöglicht die sichere Kommunikation zwischen OpenSearch Service und anderen Services innerhalb der Amazon VPC, ohne dass ein Internet-Gateway, ein NAT-Gerät oder eine VPN-Verbindung erforderlich ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
500.07	Im Rahmen ihres Cybersicherheitsprogramms beschränkt jedes abgedeckte Unternehmen auf der Grundlage der Risikobeurteilung des Unternehmens die Benutzerzugriffsberechtigungen auf Informationssysteme, die Zugang zu nicht öffentlichen Informationen bieten, und überprüft diese Zugriffsberechtigungen regelmäßig.	emr-master-no-public-ip	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon EMR-Cluster-Masterknoten nicht öffentlich zugänglich sind. Amazon-EMR-Cluster-Hauptknoten können vertrauliche Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
500.07	Im Rahmen ihres Cybersicherheitsprogramms beschränkt jedes abgedeckte Unternehmen auf der Grundlage der Risikobeurteilung des Unternehmens die Benutzerzugriffsberechtigungen auf Informationssysteme, die Zugang zu nicht öffentlichen Informationen bieten, und überprüft diese Zugriffsberechtigungen regelmäßig.	ec-2 instances-in-vpc	Stellen Sie Amazon Elastic Compute Cloud (Amazon EC2) -Instances innerhalb einer Amazon Virtual Private Cloud (Amazon VPC) bereit, um eine sichere Kommunikation zwischen einer Instance und anderen Services innerhalb der Amazon VPC zu ermöglichen, ohne dass ein Internet-Gateway, ein NAT-Gerät oder eine VPN-Verbindung erforderlich ist. Der gesamte Datenverkehr bleibt sicher in der AWS Cloud. Domains, die sich innerhalb einer VPC befinden, verfügen aufgrund ihrer logischen Isolierung im Vergleich zu Domains mit öffentlichen Endpunkten über eine zusätzliche Sicherheitsebene. Weisen Sie EC2

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			Amazon-Instances einer Amazon-VPC zu, um den Zugriff ordnungsgemäß zu verwalten.
500,07	Im Rahmen ihres Cybersicherheitsprogramms beschränkt jedes abgedeckte Unternehmen auf der Grundlage der Risikobeurteilung des Unternehmens die Benutzerzugriffsberechtigungen auf Informationssysteme, die Zugang zu nicht öffentlichen Informationen bieten, und überprüft diese Zugriffsberechtigungen regelmäßig.	internet-gateway-authorized-vpc-nur	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Internet-Gateways nur mit autorisierter Amazon Virtual Private Cloud (Amazon VPC) verbunden sind. Internet-Gateways ermöglichen den bidirektionalen Internetzugang zu und von Amazon VPC, was möglicherweise zu einem unbefugten Zugriff auf Amazon-VPC-Ressourcen führen kann.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
500,07	Im Rahmen ihres Cybersicherheitsprogramms beschränkt jedes abgedeckte Unternehmen auf der Grundlage der Risikobeurteilung des Unternehmens die Benutzerzugriffsberechtigungen auf Informationssysteme, die Zugang zu nicht öffentlichen Informationen bieten, und überprüft diese Zugriffsberechtigungen regelmäßig.	lambda-function-public-access-verboten	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass AWS Lambda-Funktionen nicht öffentlich zugänglich sind. Der öffentliche Zugriff kann möglicherweise zu einer Verschlechterung der Verfügbarkeit von Ressourcen führen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
500.07	Im Rahmen ihres Cybersicherheitsprogramms beschränkt jedes abgedeckte Unternehmen auf der Grundlage der Risikobeurteilung des Unternehmens die Benutzerzugriffsberechtigungen auf Informationssysteme, die Zugang zu nicht öffentlichen Informationen bieten, und überprüft diese Zugriffsberechtigungen regelmäßig.	lambda-inside-vpc	Stellen Sie AWS Lambda-Funktionen in einer Amazon Virtual Private Cloud (Amazon VPC) bereit, um eine sichere Kommunikation zwischen einer Funktion und anderen Diensten innerhalb der Amazon VPC zu gewährleisten. Bei dieser Konfiguration sind kein Internet-Gateway, kein NAT-Gerät und keine VPN-Verbindung erforderlich. Der gesamte Datenverkehr bleibt sicher in der Cloud. AWS Domains, die sich innerhalb einer VPC befinden, verfügen aufgrund ihrer logischen Isolierung im Vergleich zu Domains mit öffentlichen Endpunkten über eine zusätzliche Sicherheitsebene. Um den Zugriff ordnungsgemäß zu verwalten,

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			sollten AWS Lambda-Funktionen einer VPC zugewiesen werden.
500.07	Im Rahmen ihres Cybersicherheitsprogramms beschränkt jedes abgedeckte Unternehmen auf der Grundlage der Risikobeurteilung des Unternehmens die Benutzerzugriffsberechtigungen auf Informationssysteme, die Zugang zu nicht öffentlichen Informationen bieten, und überprüft diese Zugriffsberechtigungen regelmäßig.	rds-instance-public-access-überprüfen	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Relational Database Service (Amazon RDS) -Instances nicht öffentlich sind. Amazon-RDS-Datenbank-Instances können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und eine Zugriffskontrolle erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
500,07	Im Rahmen ihres Cybersicherheitsprogramms beschränkt jedes abgedeckte Unternehmen auf der Grundlage der Risikobeurteilung des Unternehmens die Benutzerzugriffsberechtigungen auf Informationssysteme, die Zugang zu nicht öffentlichen Informationen bieten, und überprüft diese Zugriffsberechtigungen regelmäßig.	rds-snapshots-public-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Relational Database Service (Amazon RDS) -Instances nicht öffentlich sind. Amazon-RDS-Datenbank-Instances können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und eine Zugriffskontrolle erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
500,07	Im Rahmen ihres Cybersicherheitsprogramms beschränkt jedes abgedeckte Unternehmen auf der Grundlage der Risikobeurteilung des Unternehmens die Benutzerzugriffsberechtigungen auf Informationssysteme, die Zugang zu nicht öffentlichen Informationen bieten, und überprüft diese Zugriffsberechtigungen regelmäßig.	redshift-cluster-public-access-überprüfen	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Redshift Redshift-Cluster nicht öffentlich sind. Amazon-Redshift-Cluster können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
500,07	Im Rahmen ihres Cybersicherheitsprogramms beschränkt jedes abgedeckte Unternehmen auf der Grundlage der Risikobeurteilung des Unternehmens die Benutzerzugriffsberechtigungen auf Informationssysteme, die Zugang zu nicht öffentlichen Informationen bieten, und überprüft diese Zugriffsberechtigungen regelmäßig.	s-3 bucket-public-read-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie nur autorisierten Benutzern, Prozessen und Geräten Zugriff auf Amazon Simple Storage Service (Amazon S3) - Buckets gewähren. Die Verwaltung des Zugriffs sollte mit der Klassifizierung der Daten übereinstimmen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
500.07	Im Rahmen ihres Cybersicherheitsprogramms beschränkt jedes abgedeckte Unternehmen auf der Grundlage der Risikobeurteilung des Unternehmens die Benutzerzugriffsberechtigungen auf Informationssysteme, die Zugang zu nicht öffentlichen Informationen bieten, und überprüft diese Zugriffsberechtigungen regelmäßig.	s-3 bucket-public-write-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie nur autorisierten Benutzern, Prozessen und Geräten Zugriff auf Amazon Simple Storage Service (Amazon S3) - Buckets gewähren. Die Verwaltung des Zugriffs sollte mit der Klassifizierung der Daten übereinstimmen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
500.07	Im Rahmen ihres Cybersicherheitsprogramms beschränkt jedes abgedeckte Unternehmen auf der Grundlage der Risikobeurteilung des Unternehmens die Benutzerzugriffsberechtigungen auf Informationssysteme, die Zugang zu nicht öffentlichen Informationen bieten, und überprüft diese Zugriffsberechtigungen regelmäßig.	sagemaker-notebook-no-direct-Internetzugang	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass SageMaker Amazon-Notebooks keinen direkten Internetzugang zulassen. Indem Sie direkten Internetzugang blockieren, vermeiden Sie, dass unbefugte Benutzer auf sensible Daten zugreifen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
500.8(a)	(a) Das Cybersicherheitsprogramm jedes abgedeckten Unternehmens muss schriftliche Verfahren, Richtlinien und Standards umfassen, mit denen gewährleistet werden soll, dass sichere Entwicklungspraktiken für intern entwickelte Anwendungen angewendet werden, die vom abgedeckten Unternehmen genutzt werden, sowie Verfahren zur Evaluierung, Bewertung oder Prüfung der Sicherheit von extern entwickelten Anwendungen, die vom abgedeckten Unternehmen im Kontext der Technologieumgebung des Unternehmens verwendet werden.	codebuild-project-envvar-awscred-überprüfen	Stellen Sie sicher, dass die Anmeldeinformationen AWS_ACCESS_KEY_ID AWS_SECRET_ACCESS_KEY nicht in AWS Codebuild-Projektumgebungen vorhanden sind. Speichern Sie diese Variablen nicht als Klartext. Das Speichern dieser Variablen als Klartext bewirkt eine unbeabsichtigte Offenlegung von Daten sowie unberechtigte Zugriffe.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
500.8(a)	(a) Das Cybersicherheitsprogramm jedes abgedeckten Unternehmens muss schriftliche Verfahren, Richtlinien und Standards umfassen, mit denen gewährleistet werden soll, dass sichere Entwicklungspraktiken für intern entwickelte Anwendungen angewendet werden, die vom abgedeckten Unternehmen genutzt werden, sowie Verfahren zur Evaluierung, Bewertung oder Prüfung der Sicherheit von extern entwickelten Anwendungen, die vom abgedeckten Unternehmen im Kontext der Technologieumgebung des Unternehmens verwendet werden.	codebuild-project-source-repo-URL-Prüfung	Stellen Sie sicher, dass die URL des Quell-Repositorys GitHub oder des Bitbucket-Quell-Repositorys keine persönlichen Zugriffstoken oder Anmeldeinformationen in Codebuild-Projektumgebungen enthält. AWS Verwende OAuth anstelle von persönlichen Zugriffstoken oder Anmeldedaten die Autorisierung für den Zugriff auf GitHub Bitbucket-Repositorys.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
500.09	(a) Jedes abgedeckte Unternehmen führt regelmäßig eine Risikobewertung der Informationssysteme des Unternehmens durch, die als Grundlage für die Definition des Cybersicherheitsprogramms gemäß diesem Teil ausreicht. Diese Risikobewertung wird aktualisiert, soweit dies erforderlich ist, um Änderungen an den Informationssystemen, den nicht öffentlichen Informationen oder den Geschäftsabläufen des abgedeckten Unternehmens Rechnung zu tragen. Die Risikobewertung des abgedeckten Unternehmens muss eine Überarbeitung der Kontrollen ermöglichen, um auf technologische Entwicklungen	annual-risk-assessment-performed (Prozessüberprüfung) >	Führen Sie eine jährliche Risikobewertung für Ihre Organisation durch. Risikobeurteilungen können dabei helfen, die Wahrscheinlichkeit und Auswirkungen identifizierter Risiken und/oder Schwachstellen für ein Unternehmen zu ermitteln.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	und sich entwickel nde Bedrohungen reagieren zu können, und berücksichtigt die besonderen Risiken der Geschäftstätigkeit des abgedeckten Unternehmens in Bezug auf Cybersich erheit, erfasste oder gespeicherte nicht öffentliche Informati onen, verwendete Informationssysteme sowie die Verfügbar keit und Wirksamke it von Kontrollen zum Schutz nicht öffentlic her Informationen und Informationssysteme.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
500.12	(a) Multi-Factor Authentication Auf der Grundlage seiner Risikobeurteilung muss jedes abgedeckte Unternehmen wirksame Kontrollen anwenden, u. a. Multi-Faktor-Authentifizierung oder risikobasierte Authentifizierung, um sich vor unbefugtem Zugriff auf nicht öffentliche Informationen oder Informationssysteme zu schützen. (b) Die Multi-Faktor-Authentifizierung wird für jede Person verwendet, die über ein externes Netzwerk auf die internen Netzwerke des abgedeckten Unternehmens zugreift, es sei denn, der CISO des abgedeckten Unternehmens hat schriftlich die Verwendung gleichwertiger oder	iam-user-mfa-enabled	Aktivieren Sie diese Regel, um den Zugriff auf Ressourcen in der AWS Cloud einzuschränken. Diese Regel sorgt dafür, dass die Multi-Faktor-Authentifizierung (MFA) für alle Benutzer aktiviert ist. MFA sorgt für eine weitere Schutzebene zusätzlich zu den Anmeldeinformationen. Reduzieren Sie Fälle von kompromittierten Konten, indem Sie MFA für Benutzer vorschreiben.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	sichererer Zugriffsk ontrollen genehmigt.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
500,12	(a) Multi-Factor Authentication Auf der Grundlage seiner Risikobeurteilung muss jedes abgedeckte Unternehmen wirksame Kontrollen anwenden, u. a. Multi-Faktor-Authentifizierung oder risikobasierte Authentifizierung, um sich vor unbefugtem Zugriff auf nicht öffentliche Informationen oder Informationssysteme zu schützen. (b) Die Multi-Faktor-Authentifizierung wird für jede Person verwendet, die über ein externes Netzwerk auf die internen Netzwerke des abgedeckten Unternehmens zugreift, es sei denn, der CISO des abgedeckten Unternehmens hat schriftlich die Verwendung gleichwertiger oder	mfa-enabled-for-iam-Konsolenzugriff	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass MFA für alle AWS Identity and Access Management (IAM) -Benutzer aktiviert ist, die über ein Konsolenkennwort verfügen. MFA sorgt für eine weitere Schutzebene zusätzlich zu den Anmeldeinformationen. Indem Sie MFA für Benutzer vorschreiben, können Sie Fälle kompromittierter Konten reduzieren und verhindern, dass unbefugte Benutzer auf vertrauliche Daten zugreifen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	sichererer Zugriffsk ontrollen genehmigt.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
500.12	(a) Multi-Factor Authentication Auf der Grundlage seiner Risikobeurteilung muss jedes abgedeckte Unternehmen wirksame Kontrollen anwenden, u. a. Multi-Faktor-Authentifizierung oder risikobasierte Authentifizierung, um sich vor unbefugtem Zugriff auf nicht öffentliche Informationen oder Informationssysteme zu schützen. (b) Die Multi-Faktor-Authentifizierung wird für jede Person verwendet, die über ein externes Netzwerk auf die internen Netzwerke des abgedeckten Unternehmens zugreift, es sei denn, der CISO des abgedeckten Unternehmens hat schriftlich die Verwendung gleichwertiger oder	iam-root-access-key-überprüfen	Der Zugriff auf Systeme und Ressourcen kann gesteuert werden, indem überprüft wird, ob der Root-Benutzer keine Zugriffsschlüssel mit seiner AWS Identity and Access Management (IAM) -Rolle verknüpft hat. Stellen Sie sicher, dass die Root-Zugriffsschlüssel gelöscht werden. Erstellen und verwenden Sie stattdessen rollenbasierte Funktionen, AWS-Konten um das Prinzip der geringsten Funktionalität zu berücksichtigen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	sichererer Zugriffsk ontrollen genehmigt.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
500.12	(a) Multi-Factor Authentication Auf der Grundlage seiner Risikobeurteilung muss jedes abgedeckte Unternehmen wirksame Kontrollen anwenden, u. a. Multi-Faktor-Authentifizierung oder risikobasierte Authentifizierung, um sich vor unbefugtem Zugriff auf nicht öffentliche Informationen oder Informationssysteme zu schützen. (b) Die Multi-Faktor-Authentifizierung wird für jede Person verwendet, die über ein externes Netzwerk auf die internen Netzwerke des abgedeckten Unternehmens zugreift, es sei denn, der CISO des abgedeckten Unternehmens hat schriftlich die Verwendung gleichwertiger oder	root-account-hardware-mfa-aktiviert	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Hardware-MFA für den Root-Benutzer aktiviert ist. Der Stammbenutzer ist der AWS-Konto-Benutzer mit den meisten Berechtigungen. MFA sorgt für eine weitere Schutzebene zusätzlich zu den Anmeldeinformationen. Indem Sie MFA für den Root-Benutzer vorschreiben, können Sie die Anzahl AWS-Konten kompromittierter Benutzer reduzieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	sichererer Zugriffsk ontrollen genehmigt.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
500,12	(a) Multi-Factor Authentication Auf der Grundlage seiner Risikobeurteilung muss jedes abgedeckte Unternehmen wirksame Kontrollen anwenden, u. a. Multi-Faktor-Authentifizierung oder risikobasierte Authentifizierung, um sich vor unbefugtem Zugriff auf nicht öffentliche Informationen oder Informationssysteme zu schützen. (b) Die Multi-Faktor-Authentifizierung wird für jede Person verwendet, die über ein externes Netzwerk auf die internen Netzwerke des abgedeckten Unternehmens zugreift, es sei denn, der CISO des abgedeckten Unternehmens hat schriftlich die Verwendung gleichwertiger oder	root-account-mfa-enabled	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass MFA für den Root-Benutzer aktiviert ist. Der Stammbenutzer ist der AWS-Konto-Benutzer mit den meisten Berechtigungen. MFA sorgt für eine weitere Schutzebene zusätzlich zu den Anmeldeinformationen. Indem Sie MFA für den Root-Benutzer vorschreiben, können Sie die Anzahl AWS-Konten kompromittierter Benutzer reduzieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	sichererer Zugriffsk ontrollen genehmigt.		
500.14(a)	(a) Implementierung risikobasierter Richtlinien, Verfahren und Kontrollen zur Überwachung der Aktivitäten autorisie rter Benutzer und zur Erkennung des unbefugten Zugriffs oder der unbefugte n Verwendung oder Manipulation von nicht öffentlichen Informationen durch diese autorisierten Benutzer.	cloudwatch-alarm-a ction-check	Amazon CloudWatch alarmiert, wenn eine Metrik den Schwellen wert für eine bestimmte Anzahl von Bewertungszeiträum en überschreitet. Der Alarm führt eine oder mehrere Aktionen durch, die vom Wert der Metrik oder des Ausdrucks im Vergleich zu einem Schwellenwert in einer Reihe von Zeiträumen abhängt. Diese Regel erfordert einen Wert für alarmActionRequired (Config Default: True), insufficientDataAc tion Required (Config Default: True), okActionRequired (Config Default: False). Der tatsächli che Wert muss die Alarmaktionen für Ihre Umgebung widerspie geln.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
500.14(a)	(a) Implementierung risikobasierter Richtlinien, Verfahren und Kontrollen zur Überwachung der Aktivitäten autorisierter Benutzer und zur Erkennung des unbefugten Zugriffs oder der unbefugten Verwendung oder Manipulation von nicht öffentlichen Informationen durch diese autorisierten Benutzer.	api-gw-execution-logging-aktiviert	Die API-Gateway-Protokollierung zeigt detaillierte Ansichten der Benutzer, die auf die API zugegriffen haben, und wie diese Benutzer auf die API zugegriffen haben. Diese Einblicke ermöglichen die Transparenz von Benutzeraktivitäten.
500.14(a)	(a) Implementierung risikobasierter Richtlinien, Verfahren und Kontrollen zur Überwachung der Aktivitäten autorisierter Benutzer und zur Erkennung des unbefugten Zugriffs oder der unbefugten Verwendung oder Manipulation von nicht öffentlichen Informationen durch diese autorisierten Benutzer.	cloud-trail-cloud-watch-logs-aktiviert	Verwenden Sie Amazon CloudWatch , um Protokollereignisaktivitäten zentral zu sammeln und zu verwalten. Die Aufnahme von AWS CloudTrail Daten liefert Einzelheiten zu den API-Aufrufaktivitäten in Ihrem AWS-Konto.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
500.14(a)	(a) Implementierung risikobasierter Richtlinien, Verfahren und Kontrollen zur Überwachung der Aktivitäten autorisierter Benutzer und zur Erkennung des unbefugten Zugriffs oder der unbefugten Verwendung oder Manipulation von nicht öffentlichen Informationen durch diese autorisierten Benutzer.	cloudtrail-enabled	AWS CloudTrail kann bei der Nichtabstreitbarkeit helfen, indem Aktionen und API-Aufrufe der AWS Management Console aufgezeichnet werden. Sie können die Benutzer und die Benutzer AWS-Konten , die einen AWS Dienst aufgerufen haben, die Quell-IP-Adresse, über die die Aufrufe generiert wurden, und den Zeitpunkt der Anrufe identifizieren. Einzelheiten zu den erfassten Daten finden Sie in den AWS CloudTrail Datensatzinhalten.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
500.14(a)	(a) Implementierung risikobasierter Richtlinien, Verfahren und Kontrollen zur Überwachung der Aktivitäten autorisierter Benutzer und zur Erkennung des unbefugten Zugriffs oder der unbefugten Verwendung oder Manipulation von nicht öffentlichen Informationen durch diese autorisierten Benutzer.	cloudtrail-s3-dataevents-enabled	Die Erfassung von Simple Storage Service (Amazon S3)-Datenereignissen unterstützt die Erkennung von ungewöhnlichen Aktivitäten. Zu den Details gehören AWS-Konto Informationen über den Zugriff auf einen Amazon S3 S3-Bucket, die IP-Adresse und die Uhrzeit des Ereignisses.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
500.14(a)	(a) Implementierung risikobasierter Richtlinien, Verfahren und Kontrollen zur Überwachung der Aktivitäten autorisierter Benutzer und zur Erkennung des unbefugten Zugriffs oder der unbefugten Verwendung oder Manipulation von nicht öffentlichen Informationen durch diese autorisierten Benutzer.	elb-logging-enabled	Die Elastic-Load-Balancing-Aktivität ist ein zentraler Kommunikationspunkt innerhalb einer Umgebung. Stellen Sie sicher, dass die ELB-Protokollierung aktiviert ist. Die gesammelten Daten enthalten detaillierte Informationen zu Anfragen, die an den ELB gesendet wurden. Jedes Protokoll enthält Informationen wie die Zeit, zu der die Anforderung einging, die Client-IP-Adresse, Latenzen, Anforderungspfade und Serverantworten.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
500.14(a)	(a) Implementierung risikobasierter Richtlinien, Verfahren und Kontrollen zur Überwachung der Aktivitäten autorisierter Benutzer und zur Erkennung des unbefugten Zugriffs oder der unbefugten Verwendung oder Manipulation von nicht öffentlichen Informationen durch diese autorisierten Benutzer.	multi-region-cloudtrail-enabled	AWS CloudTrail zeichnet Aktionen und API-Aufrufe der AWS Management Console auf. Sie können feststellen, welche Benutzer und Konten angerufen wurden AWS, von welcher Quell-IP-Adresse aus die Anrufe getätigt wurden und wann die Anrufe erfolgten. CloudTrail übermittelt Protokolldateien aus allen AWS Regionen an Ihren S3-Bucket, wenn MULTI_REGION_CLOUD_TRAIL_ENABLED aktiviert ist. Außerdem wird beim AWS Start einer neuen Region derselbe Trail in der neuen Region erstellt. CloudTrail Infolgedessen erhalten Sie Protokolldateien mit API-Aktivitäten für die neue Region, ohne Maßnahmen ergreifen zu müssen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
500.14(a)	(a) Implementierung risikobasierter Richtlinien, Verfahren und Kontrollen zur Überwachung der Aktivitäten autorisierter Benutzer und zur Erkennung des unbefugten Zugriffs oder der unbefugten Verwendung oder Manipulation von nicht öffentlichen Informationen durch diese autorisierten Benutzer.	s-3 bucket-logging-enabled	Die Amazon Simple Storage Service (Amazon S3)-Serverzugriffsprotokollierung bietet eine Methode zur Überwachung des Netzwerks im Hinblick auf potenzielle Cybersicherheitsereignisse. Die Ereignisse werden überwacht, indem detaillierte Aufzeichnungen über die Anfragen erfasst werden, die an einen Amazon-S3-Bucket gestellt wurden. Jeder Zugriffsprotokolleintrag enthält Details zu einer einzelnen Zugriffsanfrage. Zu den Details gehören Auftraggeber, Bucket-Name, Anforderungszeit, Anforderungsaktion, Antwortstatus und Fehlercode, falls relevant.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
500.14(a)	(a) Implementierung risikobasierter Richtlinien, Verfahren und Kontrollen zur Überwachung der Aktivitäten autorisierter Benutzer und zur Erkennung des unbefugten Zugriffs oder der unbefugten Verwendung oder Manipulation von nicht öffentlichen Informationen durch diese autorisierten Benutzer.	vpc-flow-logs-enabled	VPC-Flow-Protokolle erfassen detaillierte Informationsdatensätze über den IP-Datenverkehr, der zu und von Netzwerkschnittstellen in Ihrer Amazon Virtual Private Cloud (Amazon VPC) fließt. Standardmäßig enthalten Flow-Protokolldatensätze Werte für die verschiedenen Komponenten des IP-Flows, einschließlich Quelle, Ziel und Protokoll.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
500.14(a)	(a) Implementierung risikobasierter Richtlinien, Verfahren und Kontrollen zur Überwachung der Aktivitäten autorisierter Benutzer und zur Erkennung des unbefugten Zugriffs oder der unbefugten Verwendung oder Manipulation von nicht öffentlichen Informationen durch diese autorisierten Benutzer.	cw-loggroup-retention-period-überprüfen	Stellen Sie sicher, dass die Ereignisprotokolldaten für Ihre Protokollgruppen über eine Mindestdauer aufbewahrt werden, um die Fehlerbehebung und forensische Untersuchungen zu unterstützen. Fehlende frühere Ereignisprotokolldaten erschweren die Rekonstruierung und Identifizierung potenziell schädlicher Ereignisse.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
500.14(a)	(a) Implementierung risikobasierter Richtlinien, Verfahren und Kontrollen zur Überwachung der Aktivitäten autorisierter Benutzer und zur Erkennung des unbefugten Zugriffs oder der unbefugten Verwendung oder Manipulation von nicht öffentlichen Informationen durch diese autorisierten Benutzer.	rds-logging-enabled	Um die Protokollierung und Überwachung in Ihrer Umgebung zu erleichtern, stellen Sie sicher, dass die Amazon Relational Database Service (Amazon RDS)-Protokollierung aktiviert ist. Mit der Amazon-RDS-Protokollierung können Sie Ereignisse wie Verbindungen, Verbindungsabbrüche, Abfragen oder abgefragte Tabellen erfassen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
500.14(a)	(a) Implementierung risikobasierter Richtlinien, Verfahren und Kontrollen zur Überwachung der Aktivitäten autorisierter Benutzer und zur Erkennung des unbefugten Zugriffs oder der unbefugten Verwendung oder Manipulation von nicht öffentlichen Informationen durch diese autorisierten Benutzer.	codebuild-project-logging-enabled	Stellen Sie sicher, dass die AWS CodeBuild Projektprotokollierung aktiviert ist, damit Ihre Build-Ausgabeprotokolle entweder an Amazon CloudWatch oder Amazon Simple Storage Service (Amazon S3) gesendet werden. Build-Ausgabeprotokolle enthalten detaillierte Informationen zu Ihrem Build-Projekt.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
500.14(a)	(a) Implementierung risikobasierter Richtlinien, Verfahren und Kontrollen zur Überwachung der Aktivitäten autorisierter Benutzer und zur Erkennung des unbefugten Zugriffs oder der unbefugten Verwendung oder Manipulation von nicht öffentlichen Informationen durch diese autorisierten Benutzer.	wafv2-logging-enabled	Um die Protokollierung und Überwachung in Ihrer Umgebung zu erleichtern, aktivieren Sie die AWS WAF (V2) -Protokollierung im regionalen und globalen Web ACLs. AWS Die WAF-Protokollierung bietet detaillierte Informationen über den Datenverkehr, der von Ihrer Web-ACL analysiert wird. In den Protokollen werden die Uhrzeit aufgezeichnet, zu der die AWS WAF die Anfrage von Ihrer AWS Ressource erhalten hat, Informationen über die Anfrage und eine Aktion für die Regel, der jede Anfrage entsprach.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
500.14(a)	(a) Implementierung risikobasierter Richtlinien, Verfahren und Kontrollen zur Überwachung der Aktivitäten autorisierter Benutzer und zur Erkennung des unbefugten Zugriffs oder der unbefugten Verwendung oder Manipulation von nicht öffentlichen Informationen durch diese autorisierten Benutzer.	guardduty-enabled-centralized	Amazon GuardDuty kann mithilfe von Threat Intelligence Feeds helfen, potenzielle Cybersicherheitsereignisse zu überwachen und zu erkennen. Dazu gehören Listen mit bösartigen IPs und maschinellen Lernmethoden zur Identifizierung unerwarteter, nicht autorisierter und bösartiger Aktivitäten in Ihrer AWS Cloud-Umgebung.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
500.14(a)	(a) Implementierung risikobasierter Richtlinien, Verfahren und Kontrollen zur Überwachung der Aktivitäten autorisierter Benutzer und zur Erkennung des unbefugten Zugriffs oder der unbefugten Verwendung oder Manipulation von nicht öffentlichen Informationen durch diese autorisierten Benutzer.	securityhub-enabled	AWS Security Hub hilft bei der Überwachung von unbefugtem Personal, Verbindungen, Geräten und Software. AWS Security Hub aggregiert, organisiert und priorisiert die Sicherheitswarnungen oder Ergebnisse mehrerer Dienste. AWS Einige dieser Dienste sind Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer und AWS Firewall Manager sowie AWS Partnerlösungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
500.14(a)	(a) Implementierung risikobasierter Richtlinien, Verfahren und Kontrollen zur Überwachung der Aktivitäten autorisierter Benutzer und zur Erkennung des unbefugten Zugriffs oder der unbefugten Verwendung oder Manipulation von nicht öffentlichen Informationen durch diese autorisierten Benutzer.	redshift-cluster-configuration-check	Um Daten im Ruhezustand zu schützen, muss die Verschlüsselung für Ihre Amazon-Redshift-Cluster aktiviert sein. Sie müssen auch sicherstellen, dass die erforderlichen Konfigurationen auf Amazon-Redshift-Clustern bereitgestellt werden. Die Prüfungsprotokollierung muss aktiviert sein, um Informationen zu Verbindungen und Benutzeraktivitäten in der Datenbank bereitzustellen. Diese Regel erfordert, dass ein Wert für clusterDbEncrypted (Config Default: TRUE) und LoggingEnabled (Config Default: TRUE) gesetzt ist. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
500.14(a)	(a) Implementierung risikobasierter Richtlinien, Verfahren und Kontrollen zur Überwachung der Aktivitäten autorisierter Benutzer und zur Erkennung des unbefugten Zugriffs oder der unbefugten Verwendung oder Manipulation von nicht öffentlichen Informationen durch diese autorisierten Benutzer.	opensearch-audit-logging-enabled	Stellen Sie sicher, dass die Audit-Protokollierung für Ihre Amazon OpenSearch Service-Domains aktiviert ist. Mit der Audit-Protokollierung können Sie Benutzeraktivitäten auf Ihren OpenSearch Domains verfolgen, einschließlich erfolgreicher und fehlgeschlagener Authentifizierungen OpenSearch, Anfragen an, Indexänderungen und eingehende Suchanfragen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
500.14(a)	(a) Implementierung risikobasierter Richtlinien, Verfahren und Kontrollen zur Überwachung der Aktivitäten autorisierter Benutzer und zur Erkennung des unbefugten Zugriffs oder der unbefugten Verwendung oder Manipulation von nicht öffentlichen Informationen durch diese autorisierten Benutzer.	elasticsearch-logs-to-cloudwatch	Stellen Sie sicher, dass für Amazon OpenSearch Service-Domains Fehlerprotokolle aktiviert und zur Aufbewahrung und Beantwortung an Amazon CloudWatch Logs gestreamt werden. Domain-Fehlerprotokolle können bei Sicherheits- und Zugriffsprüfungen sowie bei der Diagnose von Verfügbarkeitsproblemen helfen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
500.14(a)	(a) Implementierung risikobasierter Richtlinien, Verfahren und Kontrollen zur Überwachung der Aktivitäten autorisierter Benutzer und zur Erkennung des unbefugten Zugriffs oder der unbefugten Verwendung oder Manipulation von nicht öffentlichen Informationen durch diese autorisierten Benutzer.	redshift-audit-logging-enabled	Um Informationen über Verbindungen und Benutzeraktivitäten in Ihrem Amazon-Redshift-Cluster zu erfassen, stellen Sie sicher, dass die Prüfungsprotokollierung aktiviert ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
500.14(a)	(a) Implementierung risikobasierter Richtlinien, Verfahren und Kontrollen zur Überwachung der Aktivitäten autorisierter Benutzer und zur Erkennung des unbefugten Zugriffs oder der unbefugten Verwendung oder Manipulation von nicht öffentlichen Informationen durch diese autorisierten Benutzer.	opensearch-logs-to-cloudwatch	Stellen Sie sicher, dass für Amazon OpenSearch Service-Domains Fehlerprotokolle aktiviert und zur Aufbewahrung und Beantwortung an Amazon CloudWatch Logs gestreamt werden. OpenSearch Service-Fehlerprotokolle können bei Sicherheits- und Zugriffsprüfungen helfen und bei der Diagnose von Verfügbarkeitsproblemen helfen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
500.14(b)	Im Rahmen ihres Cybersicherheitsprogramms muss jedes abgedeckte Unternehmen: (b) regelmäßige Sensibilisierungsschulungen des gesamten Personals im Bereich Cybersicherheit anbieten, die auf dem neuesten Stand gehalten werden, um den Risiken Rechnung zu tragen, die das abgedeckte Unternehmen in seiner Risikobewertung identifiziert hat.	security-awareness-program-exists (Prozessüberprüfung)	Etablieren und pflegen Sie ein Programm zur Förderung des Sicherheitsbewusstseins in Ihrer Organisation. Programme zur Förderung des Sicherheitsbewusstseins der Mitarbeiter vermitteln ihnen, wie sie die Organisation vor diversen Sicherheitsverletzungen oder Sicherheitsvorfällen schützen können.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
500.15(a)	(a) Im Rahmen seines Cybersicherheitsprogramms führt jedes abgedeckte Unternehmen auf der Grundlage seiner Risikobewertung Kontrollen durch, einschließlich Verschlüsselung, um nicht öffentliche Informationen, die von dem abgedeckten Unternehmen gespeichert oder übertragen werden, sowohl bei der Übertragung über externe Netzwerke als auch im Ruhezustand zu schützen.	opensearch-encrypted-at-rest	Da sensible Daten vorhanden sein können und um Daten im Ruhezustand zu schützen, sollten Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon OpenSearch Service-Domains aktiviert ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
500.15(a)	(a) Im Rahmen seines Cybersicherheitsprogramms führt jedes abgedeckte Unternehmen auf der Grundlage seiner Risikobewertung Kontrollen durch, einschließlich Verschlüsselung, um nicht öffentliche Informationen, die von dem abgedeckten Unternehmen gespeichert oder übertragen werden, sowohl bei der Übertragung über externe Netzwerke als auch im Ruhezustand zu schützen.	opensearch-node-to-node-Verschlüsselungsprüfung	Stellen Sie sicher, dass die node-to-node Verschlüsselung für Amazon OpenSearch Service aktiviert ist. Node-to-nodeVerschlüsselung ermöglicht die TLS 1.2-Verschlüsselung für die gesamte Kommunikation innerhalb der Amazon Virtual Private Cloud (Amazon VPC). Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
500.15(a)	(a) Im Rahmen seines Cybersicherheitsprogramms führt jedes abgedeckte Unternehmen auf der Grundlage seiner Risikobewertung Kontrollen durch, einschließlich Verschlüsselung, um nicht öffentliche Informationen, die von dem abgedeckten Unternehmen gespeichert oder übertragen werden, sowohl bei der Übertragung über externe Netzwerke als auch im Ruhezustand zu schützen.	acm-certificate-expiration-check	Stellen Sie sicher, dass die Netzwerkintegrität geschützt ist, indem Sie sicherstellen, dass X509-Zertifikate von AWS ACM ausgestellt werden. Diese Zertifikate müssen gültig und dürfen nicht abgelaufen sein. Für diese Regel ist ein Wert für erforderlich daysToExpiration (Wert für bewährte AWS Grundregeln für Sicherheit: 90). Der tatsächliche Wert muss den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
500.15(a)	(a) Im Rahmen seines Cybersicherheitsprogramms führt jedes abgedeckte Unternehmen auf der Grundlage seiner Risikobewertung Kontrollen durch, einschließlich Verschlüsselung, um nicht öffentliche Informationen, die von dem abgedeckten Unternehmen gespeichert oder übertragen werden, sowohl bei der Übertragung über externe Netzwerke als auch im Ruhezustand zu schützen.	alb-http-to-https-Umleitungsprüfung	Um Daten während der Übertragung zu schützen, stellen Sie sicher, dass Ihr Application Load Balancer unverschlüsselte HTTP-Anfragen automatisch an HTTPS umleitet. Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
500.15(a)	(a) Im Rahmen seines Cybersicherheitsprogramms führt jedes abgedeckte Unternehmen auf der Grundlage seiner Risikobewertung Kontrollen durch, einschließlich Verschlüsselung, um nicht öffentliche Informationen, die von dem abgedeckten Unternehmen gespeichert oder übertragen werden, sowohl bei der Übertragung über externe Netzwerke als auch im Ruhezustand zu schützen.	api-gw-cache-enabled-und-verschlüsselt	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass die Verschlüsselung für den Cache Ihrer API-Gateway-Stufe aktiviert ist. Zum Schutz von für die API-Methode erfassten sensiblen Daten müssen Sie die Verschlüsselung von Daten im Ruhezustand aktivieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
500.15(a)	(a) Im Rahmen seines Cybersicherheitsprogramms führt jedes abgedeckte Unternehmen auf der Grundlage seiner Risikobewertung Kontrollen durch, einschließlich Verschlüsselung, um nicht öffentliche Informationen, die von dem abgedeckten Unternehmen gespeichert oder übertragen werden, sowohl bei der Übertragung über externe Netzwerke als auch im Ruhezustand zu schützen.	cloud-trail-encryption-enabled	Da sensible Daten vorhanden sein können und um Daten im Ruhezustand zu schützen, sollten Sie sicherstellen, dass die Verschlüsselung für Ihre AWS CloudTrail Trails aktiviert ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
500.15(a)	(a) Im Rahmen seines Cybersicherheitsprogramms führt jedes abgedeckte Unternehmen auf der Grundlage seiner Risikobewertung Kontrollen durch, einschließlich Verschlüsselung, um nicht öffentliche Informationen, die von dem abgedeckten Unternehmen gespeichert oder übertragen werden, sowohl bei der Übertragung über externe Netzwerke als auch im Ruhezustand zu schützen.	cloudwatch-log-group-encrypted	Um sensible Daten im Speicher zu schützen, stellen Sie sicher, dass die Verschlüsselung für Ihre Amazon CloudWatch Log Groups aktiviert ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
500.15(a)	(a) Im Rahmen seines Cybersicherheitsprogramms führt jedes abgedeckte Unternehmen auf der Grundlage seiner Risikobewertung Kontrollen durch, einschließlich Verschlüsselung, um nicht öffentliche Informationen, die von dem abgedeckten Unternehmen gespeichert oder übertragen werden, sowohl bei der Übertragung über externe Netzwerke als auch im Ruhezustand zu schützen.	efs-encrypted-check	Um eventuell vorhandene sensible Daten sowie Daten im Ruhezustand zu schützen, muss die Verschlüsselung für Ihr Amazon Elastic File System (EFS) aktiviert sein.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
500.15(a)	(a) Im Rahmen seines Cybersicherheitsprogramms führt jedes abgedeckte Unternehmen auf der Grundlage seiner Risikobewertung Kontrollen durch, einschließlich Verschlüsselung, um nicht öffentliche Informationen, die von dem abgedeckten Unternehmen gespeichert oder übertragen werden, sowohl bei der Übertragung über externe Netzwerke als auch im Ruhezustand zu schützen.	elasticsearch-encrypted-at-rest	Da sensible Daten vorhanden sein können und um Daten im Ruhezustand zu schützen, sollten Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon OpenSearch Service (OpenSearch Service) -Domains aktiviert ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
500.15(a)	(a) Im Rahmen seines Cybersicherheitsprogramms führt jedes abgedeckte Unternehmen auf der Grundlage seiner Risikobewertung Kontrollen durch, einschließlich Verschlüsselung, um nicht öffentliche Informationen, die von dem abgedeckten Unternehmen gespeichert oder übertragen werden, sowohl bei der Übertragung über externe Netzwerke als auch im Ruhezustand zu schützen.	elb-acm-certificate-required	Zum Schutz von eventuell vorhandenen sensiblen Daten sowie von Daten während der Übertragung muss die Verschlüsselung für Ihr Elastic Load Balancing aktiviert sein. Verwenden Sie AWS Certificate Manager, um öffentliche und private SSL/TLS-Zertifikate mit AWS Diensten und internen Ressourcen zu verwalten, bereitzustellen und bereitzustellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
500.15(a)	(a) Im Rahmen seines Cybersicherheitsprogramms führt jedes abgedeckte Unternehmen auf der Grundlage seiner Risikobewertung Kontrollen durch, einschließlich Verschlüsselung, um nicht öffentliche Informationen, die von dem abgedeckten Unternehmen gespeichert oder übertragen werden, sowohl bei der Übertragung über externe Netzwerke als auch im Ruhezustand zu schützen.	encrypted-volumes	Um eventuell vorhandene sensible Daten sowie Daten im Ruhezustand zu schützen, muss die Verschlüsselung für Ihre Amazon Elastic Block Store (Amazon EBS)-Volumes aktiviert sein.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
500.15(a)	(a) Im Rahmen seines Cybersicherheitsprogramms führt jedes abgedeckte Unternehmen auf der Grundlage seiner Risikobewertung Kontrollen durch, einschließlich Verschlüsselung, um nicht öffentliche Informationen, die von dem abgedeckten Unternehmen gespeichert oder übertragen werden, sowohl bei der Übertragung über externe Netzwerke als auch im Ruhezustand zu schützen.	rds-storage-encrypted	Zum Schutz von Daten im Ruhezustand müssen Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon Relational Database Service (Amazon RDS)-Instances aktiviert ist. Um eventuell vorhandene sensible Daten im Ruhezustand in Amazon-RDS-Instances zu schützen, muss die Verschlüsselung von Daten im Ruhezustand aktiviert sein.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
500.15(a)	(a) Im Rahmen seines Cybersicherheitsprogramms führt jedes abgedeckte Unternehmen auf der Grundlage seiner Risikobewertung Kontrollen durch, einschließlich Verschlüsselung, um nicht öffentliche Informationen, die von dem abgedeckten Unternehmen gespeichert oder übertragen werden, sowohl bei der Übertragung über externe Netzwerke als auch im Ruhezustand zu schützen.	redshift-cluster-configuration-check	Um Daten im Ruhezustand zu schützen, muss die Verschlüsselung für Ihre Amazon-Redshift-Cluster aktiviert sein. Sie müssen auch sicherstellen, dass die erforderlichen Konfigurationen auf Amazon-Redshift-Clustern bereitgestellt werden. Die Prüfungsprotokollierung muss aktiviert sein, um Informationen zu Verbindungen und Benutzeraktivitäten in der Datenbank bereitzustellen. Diese Regel erfordert, dass ein Wert für clusterDbEncrypted (Config Default: TRUE) und LoggingEnabled (Config Default: TRUE) gesetzt ist. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
500.15(a)	(a) Im Rahmen seines Cybersicherheitsprogramms führt jedes abgedeckte Unternehmen auf der Grundlage seiner Risikobewertung Kontrollen durch, einschließlich Verschlüsselung, um nicht öffentliche Informationen, die von dem abgedeckten Unternehmen gespeichert oder übertragen werden, sowohl bei der Übertragung über externe Netzwerke als auch im Ruhezustand zu schützen.	redshift-require-tls-ssl	Stellen Sie sicher, dass Ihre Amazon-Redshift-Cluster eine TLS/SSL-Verschlüsselung erfordern, um eine Verbindung zu SQL-Clients herzustellen. Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
500.15(a)	(a) Im Rahmen seines Cybersicherheitsprogramms führt jedes abgedeckte Unternehmen auf der Grundlage seiner Risikobewertung Kontrollen durch, einschließlich Verschlüsselung, um nicht öffentliche Informationen, die von dem abgedeckten Unternehmen gespeichert oder übertragen werden, sowohl bei der Übertragung über externe Netzwerke als auch im Ruhezustand zu schützen.	s3-aktiviert bucket-server-side-encryption	Zum Schutz von Daten im Ruhezustand müssen Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon Simple Storage Service (Amazon S3)-Buckets aktiviert ist. Um eventuell vorhandene sensible Daten im Ruhezustand in Amazon-S3-Buckets zu schützen, muss die Verschlüsselung aktiviert sein.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
500.15(a)	(a) Im Rahmen seines Cybersicherheitsprogramms führt jedes abgedeckte Unternehmen auf der Grundlage seiner Risikobewertung Kontrollen durch, einschließlich Verschlüsselung, um nicht öffentliche Informationen, die von dem abgedeckten Unternehmen gespeichert oder übertragen werden, sowohl bei der Übertragung über externe Netzwerke als auch im Ruhezustand zu schützen.	s-3 bucket-ssl-requests-only	Um Daten während der Übertragung zu schützen, stellen Sie sicher, dass Ihre Amazon Simple Storage Service (Amazon S3)-Buckets Anfragen zur Verwendung von Secure Socket Layer (SSL)-Buckets erfordern. Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
500.15(a)	(a) Im Rahmen seines Cybersicherheitsprogramms führt jedes abgedeckte Unternehmen auf der Grundlage seiner Risikobewertung Kontrollen durch, einschließlich Verschlüsselung, um nicht öffentliche Informationen, die von dem abgedeckten Unternehmen gespeichert oder übertragen werden, sowohl bei der Übertragung über externe Netzwerke als auch im Ruhezustand zu schützen.	sagemaker-endpoint-configuration-kms-key-konfiguriert	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass die Verschlüsselung mit dem AWS Key Management Service (AWS KMS) für Ihren Endpunkt aktiviert ist. SageMaker Da sensible Daten auf dem SageMaker Endgerät gespeichert werden können, sollten Sie die Verschlüsselung im Ruhezustand aktivieren, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
500.15(a)	(a) Im Rahmen seines Cybersicherheitsprogramms führt jedes abgedeckte Unternehmen auf der Grundlage seiner Risikobewertung Kontrollen durch, einschließlich Verschlüsselung, um nicht öffentliche Informationen, die von dem abgedeckten Unternehmen gespeichert oder übertragen werden, sowohl bei der Übertragung über externe Netzwerke als auch im Ruhezustand zu schützen.	sagemaker-notebook-instance-kms-schlüsselkonfiguriert	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass die Verschlüsselung mit dem AWS Key Management Service (AWS KMS) für Ihr Notebook aktiviert ist. SageMaker Da vertrauliche Daten im SageMaker Notebook gespeichert werden können, sollten Sie die Verschlüsselung im Ruhezustand aktivieren, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
500.15(a)	(a) Im Rahmen seines Cybersicherheitsprogramms führt jedes abgedeckte Unternehmen auf der Grundlage seiner Risikobewertung Kontrollen durch, einschließlich Verschlüsselung, um nicht öffentliche Informationen, die von dem abgedeckten Unternehmen gespeichert oder übertragen werden, sowohl bei der Übertragung über externe Netzwerke als auch im Ruhezustand zu schützen.	sns-encrypted-kms	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass Ihre Amazon Simple Notification Service (Amazon SNS) -Themen mit dem AWS Key Management Service (AWS KMS) verschlüsselt werden müssen. Um eventuell vorhandene sensible Daten im Ruhezustand in veröffentlichten Nachrichten zu schützen, muss die Verschlüsselung von Daten im Ruhezustand aktiviert sein.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
500.15(a)	(a) Im Rahmen seines Cybersicherheitsprogramms führt jedes abgedeckte Unternehmen auf der Grundlage seiner Risikobewertung Kontrollen durch, einschließlich Verschlüsselung, um nicht öffentliche Informationen, die von dem abgedeckten Unternehmen gespeichert oder übertragen werden, sowohl bei der Übertragung über externe Netzwerke als auch im Ruhezustand zu schützen.	ec2- ebs-encryption-by-default	Zum Schutz von Daten im Ruhezustand müssen Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon Elastic Block Store (Amazon EBS)-Volumes aktiviert ist. Um eventuell vorhandene sensible Daten im Ruhezustand zu schützen, müssen Sie die Verschlüsselung von Daten im Ruhezustand aktivieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
500.15(a)	(a) Im Rahmen seines Cybersicherheitsprogramms führt jedes abgedeckte Unternehmen auf der Grundlage seiner Risikobewertung Kontrollen durch, einschließlich Verschlüsselung, um nicht öffentliche Informationen, die von dem abgedeckten Unternehmen gespeichert oder übertragen werden, sowohl bei der Übertragung über externe Netzwerke als auch im Ruhezustand zu schützen.	rds-snapshot-encrypted	Stellen Sie sicher, dass die Verschlüsselung für Ihre Amazon Relational Database Service (Amazon RDS)-Snapshots aktiviert ist. Um eventuell vorhandene sensible Daten im Ruhezustand zu schützen, muss die Verschlüsselung von Daten im Ruhezustand aktiviert sein.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
500.15(a)	(a) Im Rahmen seines Cybersicherheitsprogramms führt jedes abgedeckte Unternehmen auf der Grundlage seiner Risikobewertung Kontrollen durch, einschließlich Verschlüsselung, um nicht öffentliche Informationen, die von dem abgedeckten Unternehmen gespeichert oder übertragen werden, sowohl bei der Übertragung über externe Netzwerke als auch im Ruhezustand zu schützen.	alb-http-drop-invalid-Header-fähig	Stellen Sie sicher, dass Ihre Elastic Load Balancers (ELB) so konfiguriert sind, dass sie HTTP-Header löschen. Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
500.15(a)	(a) Im Rahmen seines Cybersicherheitsprogramms führt jedes abgedeckte Unternehmen auf der Grundlage seiner Risikobewertung Kontrollen durch, einschließlich Verschlüsselung, um nicht öffentliche Informationen, die von dem abgedeckten Unternehmen gespeichert oder übertragen werden, sowohl bei der Übertragung über externe Netzwerke als auch im Ruhezustand zu schützen.	elasticsearch-node-to-node-Verschlüsselungsprüfung	Stellen Sie sicher, dass die node-to-node Verschlüsselung für Amazon OpenSearch Service aktiviert ist. Node-to-nodeVerschlüsselung ermöglicht die TLS 1.2-Verschlüsselung für die gesamte Kommunikation innerhalb der Amazon Virtual Private Cloud (Amazon VPC). Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
500.15(a)	(a) Im Rahmen seines Cybersicherheitsprogramms führt jedes abgedeckte Unternehmen auf der Grundlage seiner Risikobewertung Kontrollen durch, einschließlich Verschlüsselung, um nicht öffentliche Informationen, die von dem abgedeckten Unternehmen gespeichert oder übertragen werden, sowohl bei der Übertragung über externe Netzwerke als auch im Ruhezustand zu schützen.	elb-tls-https-listeners-nur	Stellen Sie sicher, dass Ihre Elastic Load Balancer (ELBs) mit SSL- oder HTTPS-Listenern konfiguriert sind. Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
500.15(a)	(a) Im Rahmen seines Cybersicherheitsprogramms führt jedes abgedeckte Unternehmen auf der Grundlage seiner Risikobewertung Kontrollen durch, einschließlich Verschlüsselung, um nicht öffentliche Informationen, die von dem abgedeckten Unternehmen gespeichert oder übertragen werden, sowohl bei der Übertragung über externe Netzwerke als auch im Ruhezustand zu schützen.	api-gw-ssl-enabled	Stellen Sie sicher, dass die REST-API-Stufen von Amazon API Gateway mit SSL-Zertifikaten konfiguriert sind, damit Backend-Systeme überprüfen können, ob Anforderungen von API Gateway stammen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
500.15(a)	(a) Im Rahmen seines Cybersicherheitsprogramms führt jedes abgedeckte Unternehmen auf der Grundlage seiner Risikobewertung Kontrollen durch, einschließlich Verschlüsselung, um nicht öffentliche Informationen, die von dem abgedeckten Unternehmen gespeichert oder übertragen werden, sowohl bei der Übertragung über externe Netzwerke als auch im Ruhezustand zu schützen.	dynamodb-table-encrypted-kms	Stellen Sie sicher, dass die Verschlüsselung für Ihre Amazon-DynamoDB-Tabellen aktiviert ist. Um eventuell vorhandene sensible Daten im Ruhezustand in diesen Tabellen zu schützen, müssen Sie die Verschlüsselung von Daten im Ruhezustand aktivieren. Standardmäßig werden DynamoDB-Tabellen mit einem AWS eigenen Kundenhauptschlüssel (CMK) verschlüsselt.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
500.15(a)	(a) Im Rahmen seines Cybersicherheitsprogramms führt jedes abgedeckte Unternehmen auf der Grundlage seiner Risikobewertung Kontrollen durch, einschließlich Verschlüsselung, um nicht öffentliche Informationen, die von dem abgedeckten Unternehmen gespeichert oder übertragen werden, sowohl bei der Übertragung über externe Netzwerke als auch im Ruhezustand zu schützen.	elbv2- acm-certificate-required	Zum Schutz von eventuell vorhandenen sensiblen Daten sowie von Daten während der Übertragung muss die Verschlüsselung für Ihr Elastic Load Balancing aktiviert sein. Verwenden Sie AWS Certificate Manager, um öffentliche und private SSL/TLS-Zertifikate mit AWS Diensten und internen Ressourcen zu verwalten, bereitzustellen und bereitzustellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
500.15(a)	(a) Im Rahmen seines Cybersicherheitsprogramms führt jedes abgedeckte Unternehmen auf der Grundlage seiner Risikobewertung Kontrollen durch, einschließlich Verschlüsselung, um nicht öffentliche Informationen, die von dem abgedeckten Unternehmen gespeichert oder übertragen werden, sowohl bei der Übertragung über externe Netzwerke als auch im Ruhezustand zu schützen.	redshift-cluster-kms-enabled	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass die Verschlüsselung mit AWS Key Management Service (AWS KMS) für Ihren Amazon Redshift Redshift-Cluster aktiviert ist. Um eventuell vorhandene sensible Daten im Ruhezustand in Redshift-Clustern zu schützen, muss die Verschlüsselung von Daten im Ruhezustand aktiviert sein.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
500.15(a)	(a) Im Rahmen seines Cybersicherheitsprogramms führt jedes abgedeckte Unternehmen auf der Grundlage seiner Risikobewertung Kontrollen durch, einschließlich Verschlüsselung, um nicht öffentliche Informationen, die von dem abgedeckten Unternehmen gespeichert oder übertragen werden, sowohl bei der Übertragung über externe Netzwerke als auch im Ruhezustand zu schützen.	s-3 default-encryption-kms	Stellen Sie sicher, dass die Verschlüsselung für Ihre Amazon Simple Storage Service (Amazon S3)-Buckets aktiviert ist. Um eventuell vorhandene sensible Daten im Ruhezustand in einem Amazon-S3-Bucket zu schützen, muss die Verschlüsselung aktiviert sein.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
500.15(a)	(a) Im Rahmen seines Cybersicherheitsprogramms führt jedes abgedeckte Unternehmen auf der Grundlage seiner Risikobewertung Kontrollen durch, einschließlich Verschlüsselung, um nicht öffentliche Informationen, die von dem abgedeckten Unternehmen gespeichert oder übertragen werden, sowohl bei der Übertragung über externe Netzwerke als auch im Ruhezustand zu schützen.	secretsmanager-using-cmk	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass die Verschlüsselung mit dem AWS Key Management Service (AWS KMS) für AWS Secrets Manager aktiviert ist. Um eventuell vorhandene sensible Daten im Ruhezustand im Secrets Manager zu schützen, muss die Verschlüsselung von Daten im Ruhezustand aktiviert sein.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
500.15(a)	(a) Im Rahmen seines Cybersicherheitsprogramms führt jedes abgedeckte Unternehmen auf der Grundlage seiner Risikobewertung Kontrollen durch, einschließlich Verschlüsselung, um nicht öffentliche Informationen, die von dem abgedeckten Unternehmen gespeichert oder übertragen werden, sowohl bei der Übertragung über externe Netzwerke als auch im Ruhezustand zu schützen.	backup-recovery-point-encrypted	Stellen Sie sicher, dass die Verschlüsselung für Ihre AWS Backup-Wiederherstellungspunkte aktiviert ist. Um eventuell vorhandene sensible Daten im Ruhezustand zu schützen, muss die Verschlüsselung von Daten im Ruhezustand aktiviert sein.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
500.15(a)	(a) Im Rahmen seines Cybersicherheitsprogramms führt jedes abgedeckte Unternehmen auf der Grundlage seiner Risikobewertung Kontrollen durch, einschließlich Verschlüsselung, um nicht öffentliche Informationen, die von dem abgedeckten Unternehmen gespeichert oder übertragen werden, sowohl bei der Übertragung über externe Netzwerke als auch im Ruhezustand zu schützen.	codebuild-project-artifact-encryption	Um sensible Daten im Ruhezustand zu schützen, stellen Sie sicher, dass die Verschlüsselung für Ihre AWS CodeBuild Artefakte aktiviert ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
500.15(a)	(a) Im Rahmen seines Cybersicherheitsprogramms führt jedes abgedeckte Unternehmen auf der Grundlage seiner Risikobewertung Kontrollen durch, einschließlich Verschlüsselung, um nicht öffentliche Informationen, die von dem abgedeckten Unternehmen gespeichert oder übertragen werden, sowohl bei der Übertragung über externe Netzwerke als auch im Ruhezustand zu schützen.	kinesis-stream-encrypted	Um eventuell vorhandene sensible Daten sowie Daten im Ruhezustand zu schützen, muss die Verschlüsselung für Ihre Amazon-Kinesis-Streams aktiviert sein.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
500,16	(a) Im Rahmen seines Cybersicherheitsprogramms erstellt jedes abgedeckte Unternehmen einen schriftlichen Plan zur Reaktion auf Vorfälle, der die Reaktion auf Cybersicherheitsereignissen und Wiederherstellung nach solchen Ereignissen ermöglicht, die die Vertraulichkeit, Integrität oder Verfügbarkeit der Informationssysteme des abgedeckten Unternehmens oder die kontinuierliche Funktionsfähigkeit aller Aspekte der Geschäftstätigkeit oder des Betriebs des abgedeckten Unternehmens erheblich beeinträchtigen.	response-plan-exists-maintained (Prozessüberprüfung)	Stellen Sie sicher, dass Vorfallreaktionspläne erstellt, verwaltet und an die verantwortlichen Mitarbeiter verteilt werden.

Vorlage

Die Vorlage ist verfügbar unter GitHub: Operational Best Practices for NYDFS 23.

Bewährte Betriebspraktiken für NZISM 3.8

Konformitätspakete bieten ein allgemeines Compliance-Framework, das es Ihnen ermöglicht, mithilfe verwalteter oder benutzerdefinierter AWS Config Regeln und Abhilfemaßnahmen Kontrollen zur Sicherheits-, Betriebs- oder Kostenoptimierung durchzuführen. AWS Config Conformance Packs dienen als Beispielvorlagen nicht dazu, die vollständige Einhaltung eines bestimmten Governance- oder Compliance-Standards sicherzustellen. Sie sind dafür verantwortlich, selbst zu beurteilen, ob Ihre Nutzung der Services den geltenden gesetzlichen und behördlichen Anforderungen entspricht.

Im Folgenden finden Sie ein Beispiel für eine Zuordnung zwischen dem Information Security Manual (NZISM) 2021-09 Version 3.8 des Neuseeland Government Communications Security Bureau (GCSB) und AWS den Managed Config-Regeln. Jede Config-Regel gilt für einen bestimmten AWS Ressourcentyp und bezieht sich auf ein oder mehrere NZISM-Steuerelemente. Eine NZISM-Kontrolle kann mehreren Konfigurationsregeln zugeordnet werden. In der folgenden Tabelle finden Sie weitere Informationen und Anleitungen zu diesen Zuordnungen. In den Zuordnungen sind nur Kontrollen enthalten, die eine empfohlene oder grundlegende Vorgehensweise für Informationen darstellen, die als EINGESCHRÄNKT und weiter unten eingestuft sind.

Diese Vorlage für ein Konformitätspaket enthält Zuordnungen zu Kontrollen innerhalb des NZISM-Frameworks, das ein integraler Bestandteil des PSR-Frameworks (Protective Security Requirements) ist, das die Erwartungen der neuseeländischen Regierung an das Personal-, Informations- und physische Sicherheitsmanagement festlegt.

Das NZISM ist unter der Creative Commons Attribution 4.0 Neuseeland Zealand-Lizenz lizenziert, erhältlich bei https://creativecom mons. org/licenses/by/4.0/. Informationen zum Urheberrecht finden Sie unter NZISM New Zealand Information Security Manual | Legal, Privacy, and Copyright.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
1149	Softwaresicherheit, Standardbetriebsumgebungen, Entwicklung gehärteter Systeme SOEs (14.1.8.C.01.)	ec2-manager instance-managed-by-systems	Eine Bestandsaufnahme der Softwareplattformen und Anwendungen innerhalb des Unternehmens ist möglich, indem Amazon Elastic

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			Compute Cloud (Amazon EC2) - Instances mit AWS Systems Manager verwaltet werden. Verwenden Sie AWS Systems Manager, um detaillierte Systemkonfigurationen, Betriebssystem-Patch-Levels, Namen und Typ der Dienste, Softwareinstallationen, Anwendungsname, Herausgeber und Version sowie andere Details zu Ihrer Umgebung bereitzustellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
1149	Softwaresicherheit, Standardbetriebsumgebungen, Entwicklung gehärteter Systeme SOEs (14.1.8.C.01.)	ec2-prüfen managedinstance-association-compliance-status	Verwenden Sie AWS Systems Manager Associations, um bei der Inventarisierung von Softwareplattformen und Anwendungen innerhalb eines Unternehmens zu helfen. AWS Systems Manager weist Ihren verwalteten Instanzen einen Konfigurationsstatus zu und ermöglicht es Ihnen, Basiswerte für Betriebssystem-Patch-Levels, Softwareinstallationen, Anwendungskonfigurationen und andere Details zu Ihrer Umgebung festzulegen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
1149	Softwaresicherheit, Standardbetriebsumgebungen, Entwicklung gehärteter Systeme SOEs (14.1.8.C.01.)	ecs-containers-nonprivileged	Dieses Steuerelement prüft, ob der privilegierte Parameter in der Container-Definition von Amazon ECS-Aufgabendefinitionen auf true gesetzt ist. Die Steuerung schlägt fehl, wenn dieser Parameter den Wert true hat. Dieses Steuerelement bewertet nur die letzte aktive Revision einer Amazon ECS-Aufgabendefinition. Wir empfehlen, dass Sie erhöhte Rechte aus Ihren ECS-Aufgabendefinitionen entfernen. Wenn der Berechtigungsparameter true ist, erhält der Container erhöhte Rechte auf der Host-Container-Instance (ähnlich wie dem Root-Benutzer).

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
1149	Softwaresicherheit, Standardbetriebsumgebungen, Entwicklung gehärteter Systeme SOEs (14.1.8.C.01.)	ecs-containers-readonly-access	Diese Kontrolle prüft, ob Amazon ECS-Container auf den schreibgeschützten Zugriff auf bereitgestellte Root-Dateisysteme beschränkt sind. Diese Steuerung schlägt fehl, wenn der ReadonlyRootFilesystem Parameter in der Container-Definition der Amazon ECS-Aufgabendefinitionen auf False gesetzt ist. Dieses Steuerelement bewertet nur die letzte aktive Revision einer Amazon ECS-Aufgabendefinition. Durch die Aktivierung dieser Option werden Sicherheitsangriffsvektoren reduziert, da das Dateisystem der Container-Instance nur manipuliert oder beschrieben werden kann, wenn sie über explizite Lese- und Schreibberechtigungen für

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			ihren Dateisyst emordner und ihre Verzeichnisse verfügt. Diese Steuerung folgt außerdem dem Prinzip der geringsten Rechte.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
1661	Softwaresicherheit, Entwicklung von Webanwendungen, Inhalt der Behördenwebsite (14.5.6.C.01.)	cloudfront-default-root-object-konfiguriert	Dieses Steuerelement prüft, ob eine CloudFront Amazon-Distribution so konfiguriert ist, dass sie ein bestimmtes Objekt zurückgibt, das das Standard-Root-Objekt ist. Die Steuerung schlägt fehl, wenn für die CloudFront Verteilung kein Standard-Stammobjekt konfiguriert ist. Ein Benutzer kann manchmal die Stamm-URL der Distribution anstelle eines Objekts in der Distribution anfordern. In diesem Fall können Sie durch die Festlegung eines Standardstammobjekt verhindern, dass die Inhalte Ihrer Web-Verteilung preisgegeben werden. Diese Regel muss in der Region us-east-1 angewendet werden. Mit dem Vorlagenparameter

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			DeployEdgeRules = true bereitstellen
1667	Softwaresicherheit, Entwicklung von Webanwendungen, Webanwendungen (14.5.8.C.01.)	acm-certificate-expiration-check	Stellen Sie sicher, dass die Netzwerkintegrität geschützt ist, indem Sie sicherstellen, dass X509-Zertifikate von ACM ausgestellt werden. AWS Diese Zertifikate müssen gültig und dürfen nicht abgelaufen sein. Diese Regel erfordert einen Wert für. daysToExpiration Der Wert ist 90 Tage.
1667	Softwaresicherheit, Entwicklung von Webanwendungen, Webanwendungen (14.5.8.C.01.)	elb-tls-https-listeners-nur	Stellen Sie sicher, dass Ihre Elastic Load Balancer (ELBs) mit SSL- oder HTTPS-Listenern konfiguriert sind. Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
1841	Zugriffskontrolle und Passwörte r, Identifikation, Authentifizierung und Passwörte r, Methoden zur Identifizierung und Authentifizierung von Systembenutzern (16.1.35.C.02.)	iam-user-mfa-enabled	Aktivieren Sie diese Regel, um den Zugriff auf Ressourcen in der Cloud einzuschr änken. AWS Diese Regel stellt sicher, dass die Multi-Fak tor-Authentifizierung (MFA) für alle IAM-Benutzer aktiviert ist. MFA bietet eine weitere Schutzebe ne zusätzlich zum Benutzernamen und Passwort. Reduziere n Sie Fälle von kompromittierten Konten, indem Sie MFA für IAM-Benutzer vorschreiben.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
1841	Zugriffskontrolle und Passwörte r, Identifikation, Authentifizierung und Passwörte r, Methoden zur Identifizierung und Authentifizierung von Systembenutzern (16.1.35.C.02.)	mfa-enabled-for-iam-Konsolenzugriff	Verwalten Sie den Zugriff auf Ressource n in der AWS Cloud, indem Sie sicherste llen, dass MFA für alle AWS Identity and Access Managemen t (IAM) -Benutzer aktiviert ist, die über ein Konsolenk ennwort verfügen. MFA bietet eine weitere Schutzebe ne zusätzlich zum Benutzernamen und Passwort. Indem Sie MFA für IAM-Benut zer vorschreiben, können Sie Vorfälle kompromittierter Konten reduzieren und verhindern, dass unbefugte Benutzer auf vertrauliche Daten zugreifen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
1841	Zugriffskontrolle und Passwörte r, Identifikation, Authentifizierung und Passwörte r, Methoden zur Identifizierung und Authentifizierung von Systembenutzern (16.1.35.C.02.)	root-account-hardw are-mfa-aktiviert	Verwalten Sie den Zugriff auf Ressource n in der AWS Cloud, indem Sie sicherste llen, dass Hardware-MFA für den Root-Benutzer aktiviert ist. Der Root-Benutzer ist der Benutzer mit den meisten Rechten in einem AWS Konto. MFA bietet eine weitere Schutzebe ne zusätzlich zum Benutzernamen und Passwort. Indem Sie MFA für den Root-Benutzer vorschrei ben, können Sie die Anzahl kompromit tierter Konten AWS reduzieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
1841	Zugriffskontrolle und Passwörte r, Identifikation, Authentifizierung und Passwörte r, Methoden zur Identifizierung und Authentifizierung von Systembenutzern (16.1.35.C.02.)	root-account-mfa-e nabled	Verwalten Sie den Zugriff auf Ressource n in der AWS Cloud, indem Sie sicherste llen, dass MFA für den Root-Benutzer aktiviert ist. Der Root-Benutzer ist der privilegierteste Benutzer in einem AWS Konto. MFA bietet eine weitere Schutzebene zusätzlic h zum Benutzern amen und Passwort. Indem Sie MFA für den Root-Benu tzer vorschreiben, können Sie die Anzahl kompromit tierter Konten AWS reduzieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
1847	Zugriffskontrolle und Passwörte r, Identifikation, Authentifizierung und Passwörter, Schutz von Authentif izierungsdaten bei der Übertragung (16.1.37. C.01.)	alb-http-to-https-Weiterleitungsprüfung	Um Daten während der Übertragung zu schützen, stellen Sie sicher, dass Ihr Application Load Balancer unverschl üsselte HTTP-Anfr agen automatisch an HTTPS umleitet. Da sensible Daten vorhanden sein können, sollten Sie die Verschlüsselung bei der Übertragung aktivieren, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
1847	Zugriffskontrolle und Passwörte r, Identifikation, Authentifizierung und Passwörter, Schutz von Authentif izierungsdaten bei der Übertragung (16.1.37. C.01.)	cloudfront-viewer-policy-https	Diese Kontrolle prüft, ob eine CloudFront Amazon-Distributio n verlangt, dass Zuschauer HTTPS direkt verwenden , oder ob sie eine Umleitung verwendet . Das Steuerelement schlägt fehl, wenn ViewerProtocolPoli cy es für defaultCa cheBehavior oder für CacheBehaviors auf allow-all gesetzt ist. HTTPS (TLS) kann verwendet werden, um zu verhinder n, dass potenzielle Angreifer person-in-the-middle oder ähnliche Angriffe verwenden, um den Netzwerkverkehr zu belauschen oder zu manipulieren. Nur verschlüsselte Verbindungen über HTTPS (TLS) sollten zugelassen werden. Diese Regel muss in der Region us-east-1 angewende

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			t werden. Mit dem Vorlagenparameter = true bereitstellen DeployEdgeRules

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
1847	Zugriffskontrolle und Passwörte r, Identifikation, Authentifizierung und Passwörter, Schutz von Authentif izierungsdaten bei der Übertragung (16.1.37. C.01.)	elasticsearch-node -to-node-Verschlüs selungsprüfung	Dieses Steuerelement prüft, ob für Elasticse arch-Domains die Verschlüsselung aktiviert ist. node-to-node Diese Kontrolle schlägt fehl, wenn die node-to-node Verschlüsselung auf der Domain deaktivie rt ist. HTTPS (TLS) kann verwendet werden, um zu verhindern, dass potenzielle Angreifer den Netzwerkverkehr mit person-in-the-middle oder ähnlichen Angriffen abhören oder manipulieren. Nur verschlüsselte Verbindungen über HTTPS (TLS) sollten zugelassen werden. Durch die Aktivieru ng der node-to-node Verschlüsselung für Elasticsearch-Doma ins wird sichergestellt, dass die Kommunika tion innerhalb des Clusters während

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			der Übertragung verschlüsselt wird.
1847	Zugriffskontrolle und Passwörte r, Identifikation, Authentifizierung und Passwörter, Schutz von Authentif izierungsdaten bei der Übertragung (16.1.37. C.01.)	elb-tls-https-listeners-nur	Stellen Sie sicher, dass Ihre Elastic Load Balancer (ELBs) mit SSL- oder HTTPS-Listenern konfiguriert sind. Um eventuell vorhanden e sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
1847	Zugriffskontrolle und Passwörte r, Identifikation, Authentifizierung und Passwörter, Schutz von Authentif izierungsdaten bei der Übertragung (16.1.37. C.01.)	opensearch-node-to -node-Verschlüssel ungsprüfung	Dieses Steuerelement prüft, ob OpenSearc h für Domänen die Verschlüsselung aktiviert ist. node-to-node Diese Kontrolle schlägt fehl, wenn die node-to-node Verschlüsselung in der Domain deaktivie rt ist. HTTPS (TLS) kann verwendet werden, um zu verhindern, dass potenzielle Angreifer den Netzwerkverkehr mit person-in-the-middle oder ähnlichen Angriffen abhören oder manipulie ren. Nur verschlüs selte Verbindungen über HTTPS (TLS) sollten zugelassen werden. Durch die Aktivierung der node-to-node Verschlüs selung für OpenSearc h Domänen wird sichergestellt, dass die Kommunika tion innerhalb des Clusters während

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			der Übertragung verschlüsselt wird.
1858	Zugriffskontrolle und Passwörte r, Identifikation, Authentifizierung und Passwörter, Richtlinie zur Passwortauswahl (16.1.40.C.02.)	iam-password-policy	HTTPS (TLS) kann verwendet werden, um zu verhinder n, dass potenzielle Angreifer person-in-the-middle oder ähnliche Angriffe verwenden, um den Netzwerkverkehr zu belauschen oder zu manipulieren. Nur verschlüsselte Verbindungen über HTTPS (TLS) sollten zugelassen werden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
1893	Zugriffskontrolle und Passwörte r, Identifizierung, Authentifizierung und Passwörte r, Sperrung des Zugangs (16.1.46. C.02.)	iam-user-unused-cr edentials-überprüfen	AWS Identity and Access Managemen t (IAM) kann Ihnen bei Zugriffsberechtigu ngen und Autorisie rungen helfen, indem es nach IAM-Passw örtern und Zugriffss chlüsseln sucht, die für einen bestimmte n Zeitraum nicht verwendet wurden. Wenn ungenutzte Anmeldeinformation en identifiziert werden, müssen Sie sie deaktivieren und/oder entfernen , da dies gegen das Prinzip der geringste n Berechtigung verstoßen könnte. Diese Regel legt das maxCredentialUsage Alter auf 30 Tage fest.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
1946	Zugriffskontrolle und Passwörter, Zugriff für privilegierte Benutzer, Verwendung privilegierter Konten (16.3.5.C.02.)	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) kann Ihnen dabei helfen, die Prinzipien der geringsten Rechte und der Aufgabentrennung in Zugriffsberechtigungen und Autorisierungen zu integrieren und so zu verhindern, dass Richtlinien „Effect“: „Allow“ mit „Action“: „*“ anstelle von „Resource“: „*“ enthalten. Wenn Benutzern mehr Rechte eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und der Aufgabentrennung verstoßen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
1946	Zugriffskontrolle und Passwörter, Zugriff für privilegierte Benutzer, Verwendung privilegierter Konten (16.3.5.C.02.)	iam-root-access-key-überprüfen	Der Zugriff auf Systeme und Ressourcen kann gesteuert werden, indem überprüft wird, ob der Root-Benutzer keine Zugriffsschlüssel mit seiner AWS Identity and Access Management (IAM) -Rolle verknüpft hat. Stellen Sie sicher, dass die Root-Zugriffsschlüssel gelöscht werden. Erstellen und verwenden Sie stattdessen rollenbasierte AWS Konten, um dem Prinzip der geringsten Funktionalität Rechnung zu tragen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
1998	Zugriffskontrolle und Passwörter, Ereignisprotokollierung und -überwachung, Pflege von Systemverwaltungsprotokollen (16.6.6.C.02.)	cloud-trail-cloud-watch-logs-aktiviert	Sie sollten CloudTrail mit CloudWatch Logs konfigurieren, um Ihre Trail-Logs zu überwachen und bei bestimmten Aktivitäten benachrichtigt zu werden. Diese Regel prüft, ob AWS CloudTrail Trails so konfiguriert sind, dass sie Logs an CloudWatch Amazon-Logs senden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
1998	Zugriffskontrolle und Passwörter, Ereignisprotokollierung und -überwachung, Pflege von Systemverwaltungsprotokollen (16.6.6.C.02.)	cloudtrail-enabled	AWS CloudTrail kann durch die Aufzeichnung von Aktionen und API-Aufrufen in der Management Console bei der Nichtabstreitbarkeit helfen. AWS Sie können die Benutzer und AWS Konten, die einen AWS Dienst aufgerufen haben, die Quell-IP-Adresse, über die die Anrufe generiert wurden, und die Zeitpunkte der Anrufe identifizieren. Einzelheiten zu den erfassten Daten finden Sie in den AWS CloudTrail Datensatzinhalten.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
1998	Zugriffskontrolle und Passwörter, Ereignisprotokollierung und -überwachung, Pflege von Systemverwaltungsprotokollen (16.6.6.C.02.)	cw-loggroup-retention-period-überprüfen	Stellen Sie sicher, dass die Ereignisprotokolldaten für Ihre Protokollgruppen über eine Mindestdauer aufbewahrt werden, um die Fehlerbehebung und forensische Untersuchungen zu unterstützen. Fehlende frühere Ereignisprotokolldaten erschweren die Rekonstruierung und Identifizierung potenziell schädlicher Ereignisse. Die Mindestaufbewahrungsdauer beträgt 18 Monate.
2013	Zugriffskontrolle und Passwörter, Ereignisprotokollierung und Überwachung, Zusätzliche zu protokollierende Ereignisse (16.6.10.C.02.)	api-gw-execution-logging-aktiviert	Die API-Gateway-Protokollierung zeigt detaillierte Ansichten der Benutzer, die auf die API zugegriffen haben, und wie diese Benutzer auf die API zugegriffen haben. Diese Insights ermöglichen die Einsicht in Benutzeraktivitäten.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
2013	Zugriffskontrolle und Passwörter, Ereignisprotokollierung und Überwachung, Zusätzliche zu protokollierende Ereignisse (16.6.10.C.02.)	cloudfront-accesslogs-enabled	Dieses Steuerelement prüft, ob die Serverzugriffsprotokollierung auf Distributionen aktiviert ist. CloudFront Die Steuerung schlägt fehl, wenn die Zugriffsprotokollierung für eine Verteilung nicht aktiviert ist. CloudFront Zugriffsprotokolle enthalten detaillierte Informationen zu jeder eingehenden CloudFront Benutzeranfrage. Jedes Protokoll enthält Informationen wie Datum und Uhrzeit des Eingangs der Anfrage, die IP-Adresse des Betrachters, der die Anfrage gestellt hat, die Quelle der Anfrage und die Portnummer der Anfrage vom Betrachter. Diese Protokolle sind für Anwendungen wie

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			Sicherheits- und Zugriffsprüfungen sowie forensische Untersuchungen nützlich. Diese Regel muss in der Region us-east-1 angewendet werden. Stellen Sie das Gerät mit dem Vorlagenparameter DeployEdgeRules = true bereit

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
2013	Zugriffskontrolle und Passwörter, Ereignisprotokollierung und Überwachung, Zusätzliche zu protokollierende Ereignisse (16.6.10.C.02.)	cloudtrail-enabled	AWS CloudTrail kann durch die Aufzeichnung von Aktionen und API-Aufrufen in der Management Console bei der Nichtabstreitbarkeit helfen. AWS Sie können die Benutzer und AWS Konten, die einen AWS Dienst aufgerufen haben, die Quell-IP-Adresse, über die die Anrufe generiert wurden, und die Zeitpunkte der Anrufe identifizieren. Einzelheiten zu den erfassten Daten finden Sie in den AWS CloudTrail Datensatzinhalten.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
2013	Zugriffskontrolle und Passwörter, Ereignisprotokollierung und Überwachung, Zusätzliche zu protokollierende Ereignisse (16.6.10.C.02.)	elb-logging-enabled	Die Elastic-Load-Balancing-Aktivität ist ein zentraler Kommunikationspunkt innerhalb einer Umgebung. Stellen Sie sicher, dass die ELB-Protokollierung aktiviert ist. Die gesammelten Daten enthalten detaillierte Informationen zu Anfragen, die an den ELB gesendet wurden. Jedes Protokoll enthält Informationen wie die Zeit, zu der die Anforderung einging, die Client-IP-Adresse, Latenzen, Anforderungspfade und Serverantworten.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
2013	Zugriffskontrolle und Passwörter, Ereignisprotokollierung und Überwachung, Zusätzliche zu protokollierende Ereignisse (16.6.10.C.02.)	rds-logging-enabled	Um die Protokollierung und Überwachung in Ihrer Umgebung zu erleichtern, stellen Sie sicher, dass die Amazon Relational Database Service (Amazon RDS)-Protokollierung aktiviert ist. Mit der Amazon-RDS-Protokollierung können Sie Ereignisse wie Verbindungen, Verbindungsabbrüche, Abfragen oder abgefragte Tabellen erfassen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
2013	Zugriffskontrolle und Passwörter, Ereignisprotokollierung und Überwachung, Zusätzliche zu protokollierende Ereignisse (16.6.10.C.02.)	wafv2-logging-enabled	Um die Protokollierung und Überwachung in Ihrer Umgebung zu erleichtern, aktivieren Sie die AWS WAF (V2) -Protokollierung im regionalen und globalen Web. ACLs AWS Die WAF-Protokollierung bietet detaillierte Informationen über den Datenverkehr, der von Ihrer Web-ACL analysiert wird. In den Protokollen werden die Uhrzeit aufgezeichnet, zu der die AWS WAF die Anfrage von Ihrer AWS Ressource erhalten hat, Informationen über die Anfrage und eine Aktion für die Regel, der jede Anfrage entsprach.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
2022	Zugriffskontrolle und Passwörter, Ereignisprotokollierung und -überwachung, Schutz von Ereignisprotokollen (16.6.12.C.01.)	cloud-trail-log-file-validierung aktiviert	Verwenden Sie die Überprüfung von AWS CloudTrail Protokolldateien, um die Integrität von Protokollen zu überprüfen. CloudTrail Mithilfe der Protokolldateivalidierung kann festgestellt werden, ob eine Protokolldatei geändert oder gelöscht wurde oder ob sie nach der Übermittlung CloudTrail unverändert geblieben ist. Dieses Feature wurde mit dem Branchenstandard entsprechenden Algorithmen entwickelt: SHA-256 für die Hashfunktion und SHA-256 mit RSA für digitale Signaturen. Aus diesem Grund ist es rechnerisch unmöglich, CloudTrail Protokolldateien unbemerkt zu ändern, zu löschen oder zu fälschen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
2022	Zugriffskontrolle und Passwörter, Ereignisprotokollierung und -überwachung, Schutz von Ereignisprotokollen (16.6.12.C.01.)	cloudwatch-log-group-encrypted	Um sensible Daten im Speicher zu schützen, stellen Sie sicher, dass die Verschlüsselung für Ihre Amazon CloudWatch Log Groups aktiviert ist.
2028	Zugriffskontrolle und Passwörter, Ereignisprotokollierung und -überwachung, Ereignisprotokollarchive (16.6.13.C.01.)	cw-loggroup-retention-period-überprüfen	Stellen Sie sicher, dass die Ereignisprotokolldaten für Ihre Protokollgruppen über eine Mindestdauer aufbewahrt werden, um die Fehlerbehebung und forensische Untersuchungen zu unterstützen. Fehlende frühere Ereignisprotokolldaten erschweren die Rekonstruierung und Identifizierung potenziell schädlicher Ereignisse. Die Mindestaufbewahrungsdauer beträgt 18 Monate.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
2082	Kryptografie, kryptografische Grundlagen, Reduzierung der Speicher- und physischen Übertragungsanforderungen (17.1.53.C.04.)	api-gw-cache-enabled-und-verschlüsselt	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass die Verschlüsselung für den Cache Ihrer API-Gateway-Stufe aktiviert ist. Da für die API-Methode sensible Daten erfasst werden können, sollten Sie die Verschlüsselung von Daten im Ruhezustand aktivieren, um diese Daten zu schützen. Eine Ausnahme ist für Vorproduktionsumgebungen verfügbar.
2082	Kryptografie, kryptografische Grundlagen, Reduzierung der Speicher- und physischen Übertragungsanforderungen (17.1.53.C.04.)	cloud-trail-encryption-enabled	Da sensible Daten vorhanden sein können und um Daten im Ruhezustand zu schützen, sollten Sie sicherstellen, dass die Verschlüsselung für Ihre Spuren aktiviert ist. AWS CloudTrail

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
2082	Kryptografie, kryptografische Grundlagen, Reduzierung der Speicher- und physischen Übertragungsanforderungen (17.1.53.C.04.)	ec2- ebs-encryption-by-default	Zum Schutz von Daten im Ruhezustand müssen Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon Elastic Block Store (Amazon EBS)-Volumes aktiviert ist. Da sensible Daten in diesen Volumes gespeichert werden können, sollten Sie die Verschlüsselung von Daten im Ruhezustand aktivieren, um diese Daten zu schützen.
2082	Kryptografie, kryptografische Grundlagen, Reduzierung der Speicher- und physischen Übertragungsanforderungen (17.1.53.C.04.)	efs-encrypted-check	Aktivieren Sie die Verschlüsselung für Ihr Amazon Elastic File System (EFS), um eventuell vorhandene sensible Daten sowie Daten im Ruhezustand zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
2082	Kryptografie, kryptografische Grundlagen, Reduzierung der Speicher- und physischen Übertragungsanforderungen (17.1.53.C.04.)	elasticsearch-encrypted-at-rest	Dieses Steuerelement prüft, ob für Elasticsearch-Domains die Konfiguration aktiviert ist. encryption-at-rest Die Prüfung schlägt fehl, wenn die Verschlüsselung im Ruhezustand nicht aktiviert ist. Für eine zusätzliche Sicherheitsebene für sensible Daten sollten Sie Ihre Elasticsearch Service-Domain so konfigurieren, dass sie im Ruhezustand verschlüsselt wird. Wenn Sie die Verschlüsselung von Daten im Ruhezustand konfigurieren, speichert und verwaltet AWS KMS Ihre Verschlüsselungsschlüssel. Für die Verschlüsselung verwendet AWS KMS den Advanced Encryption Standard-Algorithmus mit 256-Bit-Schlüsseln (AES-256).

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
2082	Kryptografie, kryptografische Grundlagen, Reduzierung der Speicher- und physischen Übertragungsanforderungen (17.1.53.C.04.)	encrypted-volumes	Aktivieren Sie die Verschlüsselung für Ihre Amazon-Elastic-Block-Store (Amazon-EBS)-Volumes, um eventuell vorhandene sensible Daten sowie Daten im Ruhezustand zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
2082	Kryptografie, kryptografische Grundlagen, Reduzierung der Speicher- und physischen Übertragungsanforderungen (17.1.53.C.04.)	opensearch-encrypted-at-rest	Dieses Steuerelement prüft, ob für Domänen die Konfiguration aktiviert ist. OpenSearch encryption-at-rest Die Prüfung schlägt fehl, wenn die Verschlüsselung im Ruhezustand nicht aktiviert ist. Für eine zusätzliche Sicherheitsebene für vertrauliche Daten sollten Sie Ihre OpenSearch Service-Domain so konfigurieren, dass sie im Ruhezustand verschlüsselt wird. Wenn Sie die Verschlüsselung von Daten im Ruhezustand konfigurieren, speichert und verwaltet AWS KMS Ihre Verschlüsselungsschlüssel. Für die Verschlüsselung verwendet AWS KMS den Advanced Encryption Standard-Algorithmus mit 256-Bit-Schlüsseln (AES-256).

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
2082	Kryptografie, kryptografische Grundlagen, Reduzierung der Speicher- und physischen Übertragungsanforderungen (17.1.53.C.04.)	rds-snapshot-encrypted	Stellen Sie sicher, dass die Verschlüsselung für Ihre Amazon Relational Database Service (Amazon RDS)-Snapshots aktiviert ist. Da sensible Daten auch im Ruhezustand vorhanden sein können, sollten Sie die Verschlüsselung von Daten im Ruhezustand aktivieren, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
2082	Kryptografie, kryptografische Grundlagen, Reduzierung der Speicher- und physischen Übertragungsanforderungen (17.1.53.C.04.)	rds-storage-encrypted	Zum Schutz von Daten im Ruhezustand müssen Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon Relational Database Service (Amazon RDS)-Instances aktiviert ist. Da sensible Daten in Amazon-RDS-Instances gespeichert werden können, sollten Sie die Verschlüsselung von Daten im Ruhezustand aktivieren, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
2082	Kryptografie, kryptografische Grundlagen, Reduzierung der Speicher- und physischen Übertragungsanforderungen (17.1.53.C.04.)	bucket-server-side-encryptions3-fähig	Zum Schutz von Daten im Ruhezustand müssen Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon Simple Storage Service (Amazon S3)-Buckets aktiviert ist. Da sensible Daten in Amazon S3 Buckets gespeichert werden können, sollten Sie die Verschlüsselung aktivieren, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
2082	Kryptografie, kryptografische Grundlagen, Reduzierung der Speicher- und physischen Übertragungsanforderungen (17.1.53.C.04.)	s-3 default-encryption-kms	Um Daten im Ruhezustand zu schützen, sollten Sie sicherstellen, dass die Verschlüsselung für Ihre S3-Buckets aktiviert ist. Um eventuell vorhandene sensible Daten im Ruhezustand in einem Amazon-S3-Bucket zu schützen, muss die Verschlüsselung aktiviert sein. Weitere Informationen zum Verschlüsselungsprozess und zur Verwaltung erhalten Sie über den vom Kunden AWS verwalteten Key Management Service (AWS KMS). CMKs Eine Ausnahme ist für Buckets mit nicht sensiblen Daten verfügbar, sofern SSE aktiviert ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
2090	Kryptographie, kryptografische Grundlagen, Informations- und Systemschutz (17.1.55.C.02.)	alb-http-to-https-Weiterleitungsprüfung	Um Daten während der Übertragung zu schützen, stellen Sie sicher, dass Ihr Application Load Balancer unverschlüsselte HTTP-Anfragen automatisch an HTTPS umleitet. Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.
2090	Kryptographie, kryptografische Grundlagen, Informations- und Systemschutz (17.1.55.C.02.)	elb-tls-https-listeners-nur	Stellen Sie sicher, dass Ihre Elastic Load Balancer () ELBs mit SSL- oder HTTPS-Listenern konfiguriert sind. Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
2090	Kryptographie, kryptografische Grundlagen, Informations- und Systemschutz (17.1.55.C.02.)	redshift-require-tls-ssl	Stellen Sie sicher, dass Ihre Amazon-Redshift-Cluster eine TLS/SSL-Verschlüsselung erfordern, um eine Verbindung zu SQL-Clients herzustellen. Da sensible Daten vorhanden sein können, sollten Sie die Verschlüsselung bei der Übertragung aktivieren, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
2598	Kryptografie, Transport Layer Security, Verwendung von TLS (17.4.16. C.01.)	elb-custom-security-policy-ssl-Prüfung	Stellen Sie zum Schutz von Daten während der Übertragung sicher, dass Ihre Classic ElasticLoadBalancer SSL-Listener eine benutzerdefinierte Sicherheitsrichtlinie verwenden. Diese Richtlinien können verschiedene hochsichere kryptografische Algorithmen bereitstellen, um eine verschlüsselte Netzwerkkommunikation zwischen Systemen sicherzustellen. Diese Regel erfordert, dass Sie eine benutzerdefinierte Sicherheitsrichtlinie für Ihre SSL-Listener festlegen. Die Sicherheitsrichtlinie lautet: Protocol-TLSv1 .2, ECDHE-ECDSA- -GCM-. AES128 SHA256

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
2600	Kryptografie, Transport Layer Security, Verwendung von TLS (17.4.16. C.02.)	elb-custom-security-policy-ssl-Prüfung	Stellen Sie zum Schutz von Daten während der Übertragung sicher, dass Ihre Classic ElasticLoadBalancer SSL-Listener eine benutzerdefinierte Sicherheitsrichtlinie verwenden. Diese Richtlinien können verschiedene hochsichere kryptografische Algorithmen bereitstellen, um eine verschlüsselte Netzwerkkommunikation zwischen Systemen sicherzustellen. Diese Regel erfordert, dass Sie eine benutzerdefinierte Sicherheitsrichtlinie für Ihre SSL-Listener festlegen. Die Standard-Sicherheitsrichtlinie lautet: Protocol- TLSv1 .2, ECDHE-ECDSA--GCM-. AES128 SHA256

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
2726	Kryptografie, Secure Shell, automatisierter Fernzugriff (17.5.8.C .02.)	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) Security Groups können bei der Verwaltung des Netzwerkzugriffs helfen, indem sie eine statusbeh aftete Filterung von eingehendem und ausgehendem Netzwerkverkehr zu Ressourcen bereitste llen. AWS Wenn Sie eingehenden (oder entfernten) Datenverk ehr von 0.0.0.0/0 bis Port 22 auf Ihren Ressourcen nicht zulassen, können Sie den Remote-Zugriff einschränken.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3021	Kryptografie, Schlüsselverwaltung, Inhalt von KMPs (17.9.25.C.01.)	cmk-backing-key-rotation-aktiviert	AWS Mit KMS können Kunden den Backing-Schlüssel rotieren. Dabei handelt es sich um Schlüsselmaterial, das in AWS KMS gespeichert und mit der Schlüssel-ID des CMK verknüpft ist. Der Unterstützungsschlüssel wird zum Durchführen kryptografischer Vorgänge wie z. B. Ver- und Entschlüsselungen verwendet. Die automatische Schlüsselrotation speichert derzeit alle vorherigen Unterstützungsschlüssel, sodass eine transparente Entschlüsselung verschlüsselter Daten erfolgen kann. Das Rotieren der Verschlüsselungsschlüssel trägt zur Verringerung der potenziellen Auswirkungen eines kompromittierten Schlüssels

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			bei, da der Zugriff auf mit einem neuen Schlüssel verschlüs selte Daten mit einem vorherigen Schlüssel , der möglicherweise kompromittiert wurde, nicht möglich ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3205	Netzwerksicherheit, Netzwerkmanagement, Beschränkung des Netzwerkzugriffs (18.1.13.C.02.)	vpc-sg-open-only-to-authorized-ports	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass gemeinsame Ports für Amazon Elastic Compute Cloud (Amazon EC2) -Sicherheitsgruppen eingeschränkt sind. Wenn der Zugriff auf Ports nicht auf vertrauenswürdige Quellen beschränkt wird, kann dies zu Angriffen auf die Verfügbarkeit, Integrität und Vertraulichkeit von Systemen führen. Durch die Beschränkung des Zugriffs auf Ressourcen innerhalb einer Sicherheitsgruppe aus dem Internet (0.0.0.0/0) kann der Remote-Zugriff auf interne Systeme gesteuert werden. Die Liste der autorisierten Internet-Ports lautet: nur 443

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3449	Produktsicherheit, Patchen und Updates von Produkten , Patchen von Sicherheitslücken in Produkten (12.4.4.C .02.)	ec2-prüfen managedinstance-patch-compliance-status	Aktivieren Sie die Regel, um bei der Identifizierung und Dokumentation von Sicherheitslücken in Amazon Elastic Compute Cloud (Amazon EC2) zu helfen. Die Regel prüft, ob die EC2 Amazon-Instance die Patch-Konformität im AWS Systems Manager gemäß den Richtlinien und Verfahren Ihrer Organisation einhält.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3449	Produktsicherheit, Patchen und Aktualisieren von Produkten, Patchen von Sicherheitslücken in Produkten (12.4.4.C.02.)	ecr-private-image-scanning-aktiviert	Dieses Steuerelement prüft, ob in einem privaten ECR-Repository das Scannen von Bildern konfiguriert ist. Diese Steuerung schlägt fehl, wenn für ein privates ECR-Repository kein Bildscan konfiguriert ist. Beachten Sie, dass Sie auch Scan on Push für jedes Repository konfigurieren müssen, um diese Kontrolle zu bestehen. Das Scannen von ECR-Images hilft bei der Identifizierung von Softwareschwachstellen in Ihren Container-Images. ECR verwendet die Datenbank Common Vulnerabilities and Exposures (CVEs) aus dem Open-Source-Projekt Clair und bietet eine Liste der Scanergebnisse. Durch die Aktivierung von Image-Scans

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			in ECR-Repositorys werden die Integritä t und Sicherheit der gespeicherten Images mit einer zusätzlichen Überprüfungsebene verbessert.
3449	Produktsicherheit, Patches und Updates von Produkten , Patchen von Sicherheitslücken in Produkten (12.4.4.C .02.)	redshift-cluster-m aintenancesettings-check	Diese Regel stellt sicher, dass Amazon-Redshift-Cluster die bevorzugten Einstellungen für Ihre Organisation haben. Insbesondere sorgt sie dafür, dass Cluster bevorzugt e Wartungsfenster und automatisierte Aufbewahrungsfrist en für Snapshots für die Datenbank haben. allowVersionUpgrad e Diese Regel ist auf TRUE gesetzt.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3451	Produktsicherheit, Patchen und Updates von Produkten , Patchen von Sicherheitslücken in Produkten (12.4.4.C .04.)	ec2-prüfen managedinstance-patch-compliance-status	Aktivieren Sie die Regel, um bei der Identifizierung und Dokumentation von Sicherheitslücken in Amazon Elastic Compute Cloud (Amazon EC2) zu helfen. Die Regel prüft, ob die EC2 Amazon-Instance die Patch-Konformität im AWS Systems Manager gemäß den Richtlinien und Verfahren Ihrer Organisation einhält.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3452	Produktsicherheit, Patchen und Aktualisieren von Produkten, Patchen von Sicherheitslücken in Produkten (12.4.4.C.05.)	ec2-prüfen managedinstance-patch-compliance-status	Aktivieren Sie die Regel, um bei der Identifizierung und Dokumentation von Sicherheitslücken in Amazon Elastic Compute Cloud (Amazon EC2) zu helfen. Die Regel prüft, ob die EC2 Amazon-Instance die Patch-Konformität im AWS Systems Manager gemäß den Richtlinien und Verfahren Ihrer Organisation einhält.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3452	Produktsicherheit, Patchen und Aktualisieren von Produkten, Patchen von Sicherheitslücken in Produkten (12.4.4.C.05.)	elastic-beanstalk-managed-updates-aktiviert	Dieses Steuerelement prüft, ob verwaltete Plattformupdates für die Elastic Beanstalk Beanstalk-Umgebung aktiviert sind. Durch die Aktivierung verwalteter Plattformupdates wird sichergestellt, dass die neuesten verfügbaren Plattformkorrekturen, Updates und Funktionen für die Umgebung installiert werden. Ein wichtiger Schritt zur Sicherung der Systeme ist es, bei der Patch-Installation auf dem Laufenden zu bleiben.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3452	Produktsicherheit, Patchen und Updates von Produkten , Patchen von Sicherheitslücken in Produkten (12.4.4.C .05.)	rds-automatic-minor-version-upgrade-fähig	Dieses Steuerelement prüft, ob automatische Upgrades kleinerer Versionen für die RDS-Datenbank-Instance aktiviert sind. Durch die Aktivierung automatis cher Nebenvers ions-Upgrades wird sichergestellt, dass die neuesten Updates für die Nebenvers ionen des relationa len Datenbank managementsystems (RDBMS) installie rt werden. Diese Upgrades können Sicherheitspatches und Bugfixes beinhalten. Es ist ein wichtiger Schritt zur Sicherung von Systemen, über die Installation von Patches auf dem Laufenden zu bleiben.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3453	Produktsicherheit, Patchen und Updates von Produkten , Patchen von Sicherheitslücken in Produkten (12.4.4.C .06.)	ec2-prüfen managedinstance-patch-compliance-status	Aktivieren Sie die Regel, um bei der Identifizierung und Dokumentation von Sicherheitslücken in Amazon Elastic Compute Cloud (Amazon EC2) zu helfen. Die Regel prüft, ob die EC2 Amazon-Instance die Patch-Konformität im AWS Systems Manager gemäß den Richtlinien und Verfahren Ihrer Organisation einhält.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3453	Produktsicherheit, Patchen und Aktualisieren von Produkten, Patchen von Sicherheitslücken in Produkten (12.4.4.C.06.)	redshift-cluster-maintenancesettings-check	Diese Regel stellt sicher, dass Amazon-Redshift-Cluster die bevorzugten Einstellungen für Ihre Organisation haben. Insbesondere sorgt sie dafür, dass Cluster bevorzugte Wartungsfenster und automatisierte Aufbewahrungsfristen für Snapshots für die Datenbank haben. allowVersionUpgrade Diese Regel ist auf TRUE gesetzt.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3562	Gateway-Sicherheit, Gateways, Konfiguration von Gateways (19.1.12.C.01.)	alb-waf-enabled	Stellen Sie sicher, dass AWS WAF auf Elastic Load Balancers (ELB) aktiviert ist, um Webanwendungen zu schützen. Eine WAF trägt zum Schutz Ihrer Webanwendungen oder APIs vor gängigen Web-Exploits bei. Diese Web-Exploits können sich auf die Verfügbarkeit auswirken, die Sicherheit gefährden oder übermäßige Ressourcen in Ihrer Umgebung verbrauchen. Eine Ausnahme ist verfügbar, wenn der Load Balancer der Ursprung einer CloudFront Distribution mit aktivierter WAF ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3562	Gateway-Sicherheit, Gateways, Konfiguration von Gateways (19.1.12.C.01.)	api-gw-associated-with-WAF	Dieses Steuerelement prüft, ob ein API-Gateway-Schritt eine AWS WAF-Webzugriffskontrolllliste (ACL) verwendet. Dieses Steuerelement schlägt fehl, wenn keine regionale AWS WAF-Web-ACL an eine REST-API-Gateway-Stufe angehängt ist. AWS WAF ist eine Firewall für Webanwendungen, die zum Schutz APIs von Webanwendungen und vor Angriffen beiträgt. Damit können Sie eine ACL konfigurieren. Dabei handelt es sich um eine Reihe von Regeln, die Webanfragen auf der Grundlage von anpassbaren Websicherheitsregeln und -bedingungen, die Sie definieren, zulassen, blockieren oder zählen. Stellen

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			Sie sicher, dass Ihre API-Gatew ay-Stufe mit einer AWS WAF-Web-A CL verknüpft ist, um sie vor böswilligen Angriffen zu schützen. Eine Ausnahme ist verfügbar, wenn das API Gateway der Ursprung für eine CloudFront Distribut ion mit aktivierter WAF ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3562	Gateway-Sicherheit, Gateways, Konfiguration von Gateways (19.1.12.C.01.)	cloudfront-associated-with-waf	Dieses Steuerelement prüft, ob CloudFront Distributionen entweder der WAF oder dem Web zugeordnet sind. AWS AWS WAFv2 ACLs Die Steuerung schlägt fehl, wenn die Verteilung keiner Web-ACL zugeordnet ist. AWS WAF ist eine Firewall für Webanwendungen, die zum Schutz von Webanwendungen und vor APIs Angriffen beiträgt. Sie ermöglicht es ihnen, eine Gruppe von Regeln (eine sogenannte Web-Zugriffskontrollliste oder Web-ACL) zum Zulassen, Blockieren oder Zählen von Webanforderungen basierend auf von Ihnen definierten anpassbaren Web-Sicherheitsregeln und Bedingungen zu konfigurieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			Stellen Sie sicher, dass Ihre CloudFront Distribution mit einer AWS WAF-Web-ACL verknüpft ist, um sie vor böswilligen Angriffen zu schützen. Diese Regel muss in der Region us-east-1 angewendet werden. Bereitstellen mit dem Vorlagenparameter DeployEdgeRules = true
3562	Gateway-Sicherheit, Gateways, Konfiguration von Gateways (19.1.12.C.01.)	dms-replication-not-public	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass auf DMS-Replikationsinstanzen nicht öffentlich zugegriffen werden kann. DMS-Replikations-Instances können vertrauliche Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3562	Gateway-Sicherheit, Gateways, Konfiguration von Gateways (19.1.12.C.01.)	ec2-imdsv2-check	Stellen Sie sicher, dass die Methode Instance Metadata Service Version 2 (IMDSv2) aktiviert ist, um den Zugriff auf und die Kontrolle der Amazon Elastic Compute Cloud (Amazon EC2) - Instance-Metadaten zu schützen. Die IMDSv2 Methode verwendet sitzungsbasierte Kontrollen. Mit können Kontrollen implementiert werden IMDSv2, um Änderungen an Instanzmetadaten einzuschränken.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3562	Gateway-Sicherheit, Gateways, Konfiguration von Gateways (19.1.12.C.01.)	ec2- instance-no-public-ip	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon Elastic Compute Cloud (Amazon EC2) - Instances nicht öffentlich zugänglich sind. EC2 Amazon-Instances können vertrauliche Informationen enthalten, und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3562	Gateway-Sicherheit, Gateways, Konfiguration von Gateways (19.1.12.C.01.)	ec2- instances-in-vpc	Stellen Sie Amazon Elastic Compute Cloud (Amazon EC2) -Instances innerhalb einer Amazon Virtual Private Cloud (Amazon VPC) bereit, um eine sichere Kommunikation zwischen einer Instance und anderen Services innerhalb der Amazon VPC zu ermöglichen, ohne dass ein Internet-Gateway, ein NAT-Gerät oder eine VPN-Verbindung erforderlich ist. Der gesamte Datenverkehr bleibt sicher in der AWS Cloud. Domänen, die sich innerhalb einer Amazon VPC befinden, verfügen aufgrund ihrer logischen Isolierung im Vergleich zu Domänen, die öffentliche Endpunkte nutzen, über eine zusätzliche Sicherheitsebene. Weisen Sie EC2

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			Amazon-Instances einer Amazon VPC zu, um den Zugriff ordnungsgemäß zu verwalten.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3562	Gateway-Sicherheit, Gateways, Konfiguration von Gateways (19.1.12.C.01.)	elasticsearch-in-vpc-only	Dieses Steuerelement prüft, ob sich Elasticsearch-Domains in einer VPC befinden. Es bewertet nicht die Konfiguration des VPC-Subnetz-Routings, um den öffentlichen Zugriff zu bestimmen. Sie sollten sicherstellen, dass Elasticsearch-Domains nicht an öffentliche Subnetze angehängt sind. Elasticsearch-Domains, die in einer VPC bereitgestellt werden, können über das private AWS Netzwerk mit VPC-Ressourcen kommunizieren, ohne das öffentliche Internet durchqueren zu müssen. Diese Konfiguration erhöht die Sicherheitslage, indem der Zugriff auf die Daten während der Übertragung eingeschränkt wird. VPCs bieten eine

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			Reihe von Netzwerkk ontrollen, um den Zugriff auf Elasticse arch-Domains zu sichern, einschließlich Netzwerk-ACL und Sicherheitsgruppen
3562	Gateway-Sicherheit, Gateways, Konfigura tion von Gateways (19.1.12.C.01.)	emr-master-no-public-ip	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon EMR-Clust er-Masterknoten nicht öffentlich zugänglic h sind. Amazon-EM R-Cluster-Hauptkno ten können vertrauli che Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3562	Gateway-Sicherheit, Gateways, Konfiguration von Gateways (19.1.12.C.01.)	guardduty-enabled-centralized	Amazon GuardDuty kann mithilfe von Threat Intelligence Feeds helfen, potenzielle Cybersicherheitsereignisse zu überwachen und zu erkennen. Dazu gehören Listen mit bösartigen IPs und maschinellen Lernmethoden zur Identifizierung unerwarteter, nicht autorisierter und bösartiger Aktivitäten in Ihrer AWS Cloud-Umgebung.
3562	Gateway-Sicherheit, Gateways, Konfiguration von Gateways (19.1.12.C.01.)	lambda-function-public-access-verboten	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass AWS Lambda-Funktionen nicht öffentlich zugänglich sind. Der öffentliche Zugriff kann möglicherweise die Verfügbarkeit von Ressourcen beeinträchtigen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3562	Gateway-Sicherheit, Gateways, Konfiguration von Gateways (19.1.12.C.01.)	opensearch-in-vpc-only	Dieses Steuerelement prüft, ob sich OpenSearch Domänen in einer VPC befinden. Es bewertet nicht die Konfiguration des VPC-Subnetz-Routings, um den öffentlichen Zugriff zu bestimmen. Sie sollten sicherstellen, dass OpenSearch Domänen nicht an öffentliche Subnetze angehängt sind. OpenSearch Domänen, die in einer VPC bereitgestellt werden, können über das private AWS Netzwerk mit VPC-Ressourcen kommunizieren, ohne das öffentliche Internet durchqueren zu müssen. Diese Konfiguration erhöht das Sicherheitsniveau, indem der Zugriff auf die Daten während der Übertragung

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			eingeschränkt wird. VPCs bieten eine Reihe von Netzwerkk ontrollen, um den Zugriff auf OpenSearc h Domänen zu sichern, einschließlich Netzwerk-ACL und Sicherheitsgruppen.
3562	Gateway-Sicherheit, Gateways, Konfigura tion von Gateways (19.1.12.C.01.)	rds-instance-public-access-überprüfen	Verwalten Sie den Zugriff auf Ressource n in der AWS Cloud, indem Sie sicherste llen, dass Amazon Relational Database Service (Amazon RDS) -Instance s nicht öffentlic h sind. Amazon-RDS-Datenbank-Instances können vertrauliche Informati onen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3562	Gateway-Sicherheit, Gateways, Konfiguration von Gateways (19.1.12.C.01.)	redshift-cluster-public-access-überprüfen	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Redshift Redshift-Cluster nicht öffentlich sind. Amazon-Redshift-Cluster können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3562	Gateway-Sicherheit, Gateways, Konfiguration von Gateways (19.1.12.C.01.)	account-level-public-accesss3-Blöcke-periodisch	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Simple Storage Service (Amazon S3) -Buckets nicht öffentlich zugänglich sind. Diese Regel trägt dazu bei, sensible Daten vor unbefugten Remote-Benutzern zu schützen, indem sie den öffentlichen Zugriff verhindert. Diese Regel wird ignorePublicAcls auf TRUE blockPublicPolicy , TRUE, blockPublicAcls TRUE und TRUE restrictPublicBuckets gesetzt.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3562	Gateway-Sicherheit, Gateways, Konfiguration von Gateways (19.1.12.C.01.)	sagemaker-notebook-no-direct-Internetzugang	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass SageMaker Amazon-Notebooks keinen direkten Internetzugang zulassen. Indem Sie direkten Internetzugang blockieren, vermeiden Sie, dass unbefugte Benutzer auf sensible Daten zugreifen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3562	Gateway-Sicherheit, Gateways, Konfigura tion von Gateways (19.1.12.C.01.)	vpc-default-security-group-geschlossen	Sicherheitsgruppen von Amazon Elastic Compute Cloud (Amazon EC2) können bei der Verwaltung des Netzwerkzugriffs helfen, indem sie eine statusbehaftete Filterung des ein- und ausgehenden Netzwerkverkehrs zu Ressourcen bereitstellen. AWS Die Beschränk ung des gesamten Datenverkehrs auf die Standardsicherheit sgruppe hilft dabei, den Fernzugriff auf Ihre Ressourcen einzuschränken. AWS

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3562	Gateway-Sicherheit, Gateways, Konfiguration von Gateways (19.1.12.C.01.)	vpc-flow-logs-enabled	VPC-Flow-Protokolle erfassen detaillierte Informationsdatensätze über den IP-Datenverkehr, der zu und von Netzwerkschnittstellen in Ihrer Amazon Virtual Private Cloud (Amazon VPC) fließt. Standardmäßig enthalten Flow-Protokolldatensätze Werte für die verschiedenen Komponenten des IP-Flows, einschließlich Quelle, Ziel und Protokoll.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3623	Gateway-Sicherheit , Gateways, entmilitarisierte Zonen (19.1.14.C.02.)	elasticsearch-in-vpc-only	Dieses Steuerelement prüft, ob sich Elasticsearch-Domains in einer VPC befinden. Es bewertet nicht die Konfiguration des VPC-Subnetz-Routings, um den öffentlichen Zugriff zu bestimmen. Sie sollten sicherstellen, dass Elasticsearch-Domains nicht an öffentliche Subnetze angehängt sind. Elasticsearch-Domains, die in einer VPC bereitgestellt werden, können über das private AWS Netzwerk mit VPC-Ressourcen kommunizieren, ohne das öffentliche Internet durchqueren zu müssen. Diese Konfiguration erhöht die Sicherheitslage, indem der Zugriff auf die Daten während der Übertragung eingeschränkt wird. VPCs bieten eine

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			Reihe von Netzwerkk ontrollen, um den Zugriff auf Elasticse arch-Domains zu sichern, einschließlich Netzwerk-ACL und Sicherheitsgruppen

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3623	Gateway-Sicherheit, Gateways, entmilitarisierte Zonen (19.1.14.C.02.)	opensearch-in-vpc-only	Dieses Steuerelement prüft, ob sich OpenSearch Domänen in einer VPC befinden. Es bewertet nicht die Konfiguration des VPC-Subnetz-Routings, um den öffentlichen Zugriff zu bestimmen. Sie sollten sicherstellen, dass OpenSearch Domänen nicht an öffentliche Subnetze angehängt sind. OpenSearch Domänen, die in einer VPC bereitgestellt werden, können über das private AWS Netzwerk mit VPC-Ressourcen kommunizieren, ohne das öffentliche Internet durchqueren zu müssen. Diese Konfiguration erhöht das Sicherheitsniveau, indem der Zugriff auf die Daten während der Übertragung

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			eingeschränkt wird. VPCs bieten eine Reihe von Netzwerkkontrollen, um den Zugriff auf OpenSearch Domänen zu sichern, einschließlich Netzwerk-ACL und Sicherheitsgruppen.
3623	Gateway-Sicherheit, Gateways, entmilitarisierte Zonen (19.1.14.C.02.)	rds-instance-public-access-überprüfen	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Relational Database Service (Amazon RDS) -Instances nicht öffentlich sind. Amazon-RDS-Datenbank-Instances können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3623	Gateway-Sicherheit , Gateways, entmilitarisierte Zonen (19.1.14.C.02.)	redshift-cluster-public-access-überprüfen	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Redshift Redshift-Cluster nicht öffentlich sind. Amazon-Redshift-Cluster können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3815	Netzwerksicherheit, Erkennung und Verhinderung von Eindringlingen, IDS/IPS-Wartung (18.4.9.C.01.)	guardduty-enabled-centralized	Amazon GuardDuty kann mithilfe von Threat Intelligence Feeds helfen, potenzielle Cybersicherheitsereignisse zu überwachen und zu erkennen. Dazu gehören Listen mit bösartigen IPs und maschinellen Lernmethoden zur Identifizierung unerwarteter, nicht autorisierter und bösartiger Aktivitäten in Ihrer AWS Cloud-Umgebung.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3857	Netzwerksicherheit, Erkennung und Verhinderung von Eindringlingen, Konfiguration von IDS/IPS (18.4.11.C.01.)	guardduty-eks-protection-audit-aktiviert	Dieses Steuerelement prüft, ob EKS Audit Log Monitoring aktiviert ist. GuardDuty GuardDuty EKS Audit Log Monitoring hilft Ihnen dabei, potenziell verdächtige Aktivitäten in Ihren Amazon Elastic Kubernetes Service (Amazon EKS) -Clustern zu erkennen. EKS Audit Log Monitoring verwendet Kubernetes-Prüfungsprotokolle, um chronologische Aktivitäten von Benutzern, Anwendungen, die die Kubernetes-API verwenden und der Steuerebene zu erfassen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3857	Netzwerksicherheit, Erkennung und Verhinderung von Eindringlingen, Konfiguration von IDS/IPS (18.4.11.C.01.)	guardduty-eks-protection-runtime-aktiviert	Dieses Steuerelement prüft, ob GuardDuty EKS Runtime Monitoring mit automatisierter Agentenverwaltung aktiviert ist. EKS Protection in Amazon GuardDuty bietet Schutz vor Bedrohungserkennung, um Sie beim Schutz von Amazon EKS-Clustern in Ihrer AWS Umgebung zu unterstützen. EKS Runtime Monitoring verwendet Ereignisse auf Betriebssystemebene, um Ihnen zu helfen, potenzielle Bedrohungen in EKS-Knoten und Containern in Ihren EKS-Clustern zu erkennen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3857	Netzwerksicherheit, Erkennung und Verhinderung von Eindringlingen, Konfiguration von IDS/IPS (18.4.11.C.01.)	guardduty-lambda-protection-enabled	Dieses Steuerelement prüft, ob GuardDuty Lambda Protection aktiviert ist. GuardDuty Lambda Protection hilft Ihnen dabei, potenzielle Sicherheitsbedrohungen zu identifizieren, wenn eine AWS Lambda-Funktion aufgerufen wird. Nachdem Sie Lambda Protection aktiviert haben, GuardDuty beginnt die Überwachung der Lambda-Netzwerkaktivitätsprotokolle, die mit den Lambda-Funktionen in Ihrem Konto verknüpft sind. AWS Wenn eine Lambda-Funktion aufgerufen wird und verdächtigen Netzwerkverkehr GuardDuty identifiziert, der auf das Vorhandensein eines potenziell bösartigen Codes in Ihrer Lambda-Funktion

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			hinweist, GuardDuty wird ein Befund generiert.
3857	Netzwerksicherheit, Erkennung und Verhinderung von Eindringlingen, Konfiguration von IDS/IPS (18.4.11.C.01.)	GuardDuty-S3-Schutz aktiviert	Dieses Steuerelement prüft, ob S3 Protection aktiviert ist. GuardDuty S3 Protection ermöglicht GuardDuty die Überwachung von API-Vorgängen auf Objektebene, um potenzielle Sicherheitsrisiken für Daten in Ihren Amazon S3 S3-Buckets zu identifizieren. GuardDuty überwacht Bedrohungen für Ihre S3-Ressourcen, indem AWS CloudTrail Verwaltungsereignisse und CloudTrail S3-Datenereignisse analysiert werden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3875	Netzwerksicherheit , Erkennung und Verhinderung von Eindringlingen, Ereignismanagement und Korrelation (18.4.12.C.01.)	guardduty-enabled-centralized	Amazon GuardDuty kann mithilfe von Threat Intellige nce Feeds helfen, potenzielle Cybersich erheitsereignisse zu überwachen und zu erkennen. Dazu gehören Listen mit bösartigen IPs und maschinel len Lernmethoden zur Identifizierung unerwarteter, nicht autorisierter und bösartiger Aktivitäten in Ihrer AWS Cloud-Umgebung.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3875	Netzwerksicherheit , Erkennung und Verhinderung von Eindringlingen, Ereignismanagement und Korrelation (18.4.12.C.01.)	securityhub-enabled	AWS Security Hub hilft bei der Überwachung von unbefugtem Personal, Verbindungen, Geräten und Software. AWS Security Hub aggregiert, organisiert und priorisiert die Sicherheitswarnungen oder Ergebnisse mehrerer Dienste. AWS Einige dieser Dienste sind Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer und AWS Firewall Manager sowie AWS Partnerlösungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
4333	Datenmanagement, Inhaltsfilterung, Inhaltsvalidierung (20.3.7.C.02.)	alb-waf-enabled	Stellen Sie sicher, dass AWS WAF auf Elastic Load Balancers (ELB) aktiviert ist, um Webanwendungen zu schützen. Eine WAF trägt zum Schutz Ihrer Webanwend ungen oder APIs vor gängigen Web-Explo its bei. Diese Web-Exploits können sich auf die Verfügbar keit auswirken, die Sicherheit gefährden oder übermäßige Ressourcen in Ihrer Umgebung verbrauch en.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
4333	Datenmanagement, Inhaltsfilterung, Inhaltsvalidierung (20.3.7.C.02.)	api-gw-associated-with-WAF	Dieses Steuerelement prüft, ob ein API-Gateway-Schritt eine AWS WAF-Webzugriffskontrolllliste (ACL) verwendet. Dieses Steuerelement schlägt fehl, wenn keine regionale AWS WAF-Web-ACL an eine REST-API-Gateway-Stufe angehängt ist. AWS WAF ist eine Firewall für Webanwendungen, die zum Schutz APIs von Webanwendungen und vor Angriffen beiträgt. Damit können Sie eine ACL konfigurieren. Dabei handelt es sich um eine Reihe von Regeln, die Webanfragen auf der Grundlage von anpassbaren Websicherheitsregeln und -bedingungen, die Sie definieren, zulassen, blockieren oder zählen. Stellen

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			Sie sicher, dass Ihre API-Gatew ay-Stufe mit einer AWS WAF-Web-A CL verknüpft ist, um sie vor böswilligen Angriffen zu schützen. Eine Ausnahme ist verfügbar, wenn das API Gateway der Ursprung für eine CloudFront Distribut ion mit aktivierter WAF ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
4441	Datenverwaltung, Datenbanken, Datenbankdateien (20.4.4.C.02.)	elasticsearch-encrypted-at-rest	Dieses Steuerelement prüft, ob für Elasticsearch-Domains die Konfiguration aktiviert ist. encryption-at-rest Die Prüfung schlägt fehl, wenn die Verschlüsselung im Ruhezustand nicht aktiviert ist. Für eine zusätzliche Sicherheitsebene für sensible Daten sollten Sie Ihre Elasticsearch Service-Domain so konfigurieren, dass sie im Ruhezustand verschlüsselt wird. Wenn Sie die Verschlüsselung von Daten im Ruhezustand konfigurieren, speichert und verwaltet AWS KMS Ihre Verschlüsselungsschlüssel. Für die Verschlüsselung verwendet AWS KMS den Advanced Encryption Standard-Algorithmus mit 256-Bit-Schlüsseln (AES-256).

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
4441	Datenverwaltung, Datenbanken, Datenbankdateien (20.4.4.C.02.)	opensearch-encrypted-at-rest	Dieses Steuerelement prüft, ob OpenSearch für Domänen die Konfiguration aktiviert ist. encryption-at-rest Die Prüfung schlägt fehl, wenn die Verschlüsselung im Ruhezustand nicht aktiviert ist. Für eine zusätzliche Sicherheitsebene für vertrauliche Daten sollten Sie Ihre OpenSearch Service-Domain so konfigurieren, dass sie im Ruhezustand verschlüsselt wird. Wenn Sie die Verschlüsselung von Daten im Ruhezustand konfigurieren, speichert und verwaltet AWS KMS Ihre Verschlüsselungsschlüssel. Für die Verschlüsselung verwendet AWS KMS den Advanced Encryption Standard-Algorithmus mit 256-Bit-Schlüsseln (AES-256).

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
4441	Datenverwaltung, Datenbanken, Datenbankdateien (20.4.4.C.02.)	rds-logging-enabled	Um die Protokollierung und Überwachung in Ihrer Umgebung zu erleichtern, stellen Sie sicher, dass die Amazon Relational Database Service (Amazon RDS)-Protokollierung aktiviert ist. Mit der Amazon-RDS-Protokollierung können Sie Ereignisse wie Verbindungen, Verbindungsabbrüche, Abfragen oder abgefragte Tabellen erfassen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
4441	Datenverwaltung, Datenbanken, Datenbankdateien (20.4.4.C.02.)	rds-snapshot-encrypted	Stellen Sie sicher, dass die Verschlüsselung für Ihre Amazon Relational Database Service (Amazon RDS)-Snapshots aktiviert ist. Da sensible Daten auch im Ruhezustand vorhanden sein können, sollten Sie die Verschlüsselung von Daten im Ruhezustand aktivieren, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
4441	Datenverwaltung, Datenbanken, Datenbankdateien (20.4.4.C.02.)	rds-snapshots-public-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Relational Database Service (Amazon RDS) -Instances nicht öffentlich sind. Amazon-RDS-Datenbank-Instances können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
4441	Datenverwaltung, Datenbanken, Datenbankdateien (20.4.4.C.02.)	rds-storage-encrypted	Zum Schutz von Daten im Ruhezustand müssen Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon Relational Database Service (Amazon RDS)-Instances aktiviert ist. Da sensible Daten in Amazon-RDS-Instances gespeichert werden können, sollten Sie die Verschlüsselung von Daten im Ruhezustand aktivieren, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
4441	Datenverwaltung, Datenbanken, Datenbankdateien (20.4.4.C.02.)	redshift-cluster-configuration-check	Um Daten im Ruhezustand zu schützen, muss die Verschlüsselung für Ihre Amazon-Redshift-Cluster aktiviert sein. Sie müssen auch sicherstellen, dass die erforderlichen Konfigurationen auf Amazon-Redshift-Clustern bereitgestellt werden. Die Prüfungsprotokollierung muss aktiviert sein, um Informationen zu Verbindungen und Benutzeraktivitäten in der Datenbank bereitzustellen. Diese Regel ist clusterDbEncrypted auf TRUE und LoggingEnabled auf TRUE gesetzt.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
4445	Datenmanagement, Datenbanken, Rechenschaftspflicht (20.4.5.C.02.)	rds-logging-enabled	Um die Protokollierung und Überwachung in Ihrer Umgebung zu erleichtern, stellen Sie sicher, dass die Amazon Relational Database Service (Amazon RDS)-Protokollierung aktiviert ist. Mit der Amazon-RDS-Protokollierung können Sie Ereignisse wie Verbindungen, Verbindungsabbrüche, Abfragen oder abgefragte Tabellen erfassen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
4445	Datenmanagement, Datenbanken, Rechenschaftspflicht (20.4.5.C.02.)	redshift-cluster-configuration-check	Um Daten im Ruhezustand zu schützen, muss die Verschlüsselung für Ihre Amazon-Redshift-Cluster aktiviert sein. Sie müssen auch sicherstellen, dass die erforderlichen Konfigurationen auf Amazon-Redshift-Clustern bereitgestellt werden. Die Prüfungsprotokollierung muss aktiviert sein, um Informationen zu Verbindungen und Benutzeraktivitäten in der Datenbank bereitzustellen. Diese Regel ist clusterDbEncrypted auf TRUE und LoggingEnabled auf TRUE gesetzt.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
4829	Sicherheit von Unternehmenssystemen, Cloud Computing, Systemverfügbarkeit (22.1.23.C.01.)	dynamodb-autoscaling-enabled	Amazon DynamoDB Auto Scaling verwendet den AWS Application Auto Scaling-Service, um die bereitgestellte Durchsatzkapazität so anzupassen, dass sie automatisch auf tatsächliche Verkehrsmuster reagiert. Auf diese Weise kann eine Tabelle oder ein globaler sekundärer Index die bereitgestellte Lese-/Schreibkapazität erhöhen, um plötzliche Erhöhungen des Datenverkehrs ohne Drosselung zu bewältigen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
4829	Sicherheit von Unternehmenssystemen, Cloud Computing, Systemverfügbarkeit (22.1.23.C.01.)	elb-cross-zone-load-Balancing aktiviert	Aktivieren Sie zonenübergreifendes Load Balancing für Ihre Elastic Load Balancer (ELBs), um eine angemessene Kapazität und Verfügbarkeit aufrechtzuerhalten. Zonenübergreifendes Load Balancing reduziert die Notwendigkeit, die gleiche Anzahl von Instances in jeder aktivierten Availability Zone aufrechtzuerhalten. Es verbessert auch die Fähigkeit Ihrer Anwendung, den Verlust einer oder mehrerer Instances zu bewältigen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
4829	Sicherheit von Unternehmenssystemen, Cloud Computing, Systemverfügbarkeit (22.1.23.C.01.)	rds-cluster-multi-az-aktiviert	Amazon Aurora speichert Kopien der Daten in einem DB-Cluster über mehrere Availability Zones in einer einzigen AWS Region. Dieser Speichervorgang von Aurora erfolgt unabhängig davon, ob die DB-Instances im DB-Cluster mehrere Availability Zones umfassen. Wenn Daten in die primäre DB-Instance geschrieben werden, repliziert Aurora die Daten synchron über die Availability Zones auf sechs Speicherknoten, die Ihrem Cluster-Volume zugeordnet sind. Auf diese Weise werden eine Datenredundanz erreicht, das Blockieren von I/Os verhindert und Latenzspitzen bei System-Backups minimiert. Wenn Sie eine DB-Instance mit hoher Verfügbarkeit

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			ausführen, kann dies die Verfügbarkeit bei geplanten Systemwartungen verbessern. Außerdem kann dies Ihre Datenbanken bei Ausfällen und bei Nichtverfügbarkeit von Availability Zones schützen. Diese Regel prüft, ob die Multi-AZ-Replikation auf Amazon Aurora Aurora-Clustern aktiviert ist, die von Amazon RDS verwaltet werden. Eine Ausnahme ist für Vorproduktionsumgebungen verfügbar.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
4829	Sicherheit von Unternehmenssystemen, Cloud Computing, Systemverfügbarkeit (22.1.23.C.01.)	rds-multi-az-support	Die Multi-AZ-Unterstützung in Amazon Relational Database Service (Amazon RDS) bietet eine verbesserte Verfügbarkeit und Beständigkeit von Datenbank-Instances. Wenn Sie eine Multi-AZ-Datenbank-Instance bereitstellen, erstellt Amazon RDS automatisch eine primäre Datenbank-Instance und repliziert die Daten synchron auf eine Standby-Instance in einer anderen Availability Zone. Jede Availability Zone läuft auf einer eigenen, physisch getrennten, unabhängigen Infrastruktur und ist auf eine hohe Verfügbarkeit ausgelegt. Im Falle eines Infrastrukturausfalls führt Amazon RDS einen automatis

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			chen Failover zum Standby-Modus durch, sodass Sie den Datenbank betrieb wieder aufnehmen können, sobald der Failover abgeschlossen ist. Eine Ausnahme ist für Vorproduktionsumge bungen verfügbar.
4838	Sicherheit von Unternehmenssystem en, Cloud Computing , unbefugter Zugriff (22.1.24.C.03.)	cloudtrail-s3-data events-enabled	Die Erfassung von Simple Storage Service (Amazon S3)-Datenereigniss en unterstützt die Erkennung von ungewöhnlichen Aktivitäten. Zu den Details gehören AWS Kontoinformationen , über die auf einen Amazon S3 S3-Bucket zugegriffen wurde, die IP-Adress e und die Uhrzeit des Ereignisses.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
4838	Sicherheit von Unternehmenssystemen, Cloud Computing, unbefugter Zugriff (22.1.24.C.03.)	ebs-snapshot-public-restorable-überprüfen	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass EBS-Snapshots nicht öffentlich wiederherstellbar sind. EBS-Volume-Snapshots können vertrauliche Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
4838	Sicherheit von Unternehmenssystemen, Cloud Computing, unbefugter Zugriff (22.1.24.C.03.)	account-level-public-accesss3-Blöcke-periodisch	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Simple Storage Service (Amazon S3) -Buckets nicht öffentlich zugänglich sind. Diese Regel trägt dazu bei, sensible Daten vor unbefugten Remote-Benutzern zu schützen, indem sie den öffentlichen Zugriff verhindert. Diese Regel wird ignorePublicAcls auf TRUE blockPublicPolicy , TRUE, blockPublicAcls TRUE und TRUE restrictPublicBuckets gesetzt.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
4838	Sicherheit von Unternehmenssystemen, Cloud Computing, unbefugter Zugriff (22.1.24.C.03.)	s-3 bucket-public-read-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie nur autorisierten Benutzern, Prozessen und Geräten Zugriff auf Amazon Simple Storage Service (Amazon S3) - Buckets gewähren. Die Verwaltung des Zugriffs sollte mit der Klassifizierung der Daten übereinstimmen.
4838	Sicherheit von Unternehmenssystemen, Cloud Computing, unbefugter Zugriff (22.1.24.C.03.)	s-3 bucket-public-write-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie nur autorisierten Benutzern, Prozessen und Geräten Zugriff auf Amazon Simple Storage Service (Amazon S3) - Buckets gewähren. Die Verwaltung des Zugriffs sollte mit der Klassifizierung der Daten übereinstimmen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
4839	Sicherheit von Unternehmenssystemen, Cloud Computing, unbefugter Zugriff (22.1.24.C.04.)	dynamodb-table-encrypted-kms	Stellen Sie sicher, dass die Verschlüsselung für Ihre Amazon-DynamoDB-Tabellen aktiviert ist. Um eventuell vorhandene sensible Daten im Ruhezustand in diesen Tabellen zu schützen, müssen Sie die Verschlüsselung von Daten im Ruhezustand aktivieren. Standardmäßig werden DynamoDB-Tabellen mit einem AWS eigenen Kundenhauptschlüssel (CMK) verschlüsselt.
4839	Sicherheit von Unternehmenssystemen, Cloud Computing, unbefugter Zugriff (22.1.24.C.04.)	efs-encrypted-check	Aktivieren Sie die Verschlüsselung für Ihr Amazon Elastic File System (EFS), um eventuell vorhandene sensible Daten sowie Daten im Ruhezustand zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
4839	Sicherheit von Unternehmenssystemen, Cloud Computing, unbefugter Zugriff (22.1.24.C.04.)	elasticsearch-encrypted-at-rest	Dieses Steuerelement prüft, ob für Elasticsearch-Domains die Konfiguration aktiviert ist. encryption-at-rest Die Prüfung schlägt fehl, wenn die Verschlüsselung im Ruhezustand nicht aktiviert ist. Für eine zusätzliche Sicherheitsebene für sensible Daten sollten Sie Ihre Elasticsearch Service-Domain so konfigurieren, dass sie im Ruhezustand verschlüsselt wird. Wenn Sie die Verschlüsselung von Daten im Ruhezustand konfigurieren, speichert und verwaltet AWS KMS Ihre Verschlüsselungsschlüssel. Für die Verschlüsselung verwendet AWS KMS den Advanced Encryption Standard-Algorithmus mit 256-Bit-Schlüsseln (AES-256).

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
4839	Sicherheit von Unternehmenssystemen, Cloud Computing, unbefugter Zugriff (22.1.24.C.04.)	elasticsearch-node-to-node-Verschlüsselungsprüfung	Dieses Steuerelement prüft, ob für Elasticsearch-Domains die Verschlüsselung aktiviert ist. node-to-node Diese Kontrolle schlägt fehl, wenn die node-to-node Verschlüsselung auf der Domain deaktiviert ist. HTTPS (TLS) kann verwendet werden, um zu verhindern, dass potenzielle Angreifer den Netzwerkverkehr mit person-in-the-middle oder ähnlichen Angriffen abhören oder manipulieren. Nur verschlüsselte Verbindungen über HTTPS (TLS) sollten zugelassen werden. Durch die Aktivierung der node-to-node Verschlüsselung für Elasticsearch-Domains wird sichergestellt, dass die Kommunikation innerhalb des Clusters während

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			der Übertragung verschlüsselt wird.
4839	Sicherheit von Unternehmenssystemen, Cloud Computing, unbefugter Zugriff (22.1.24.C.04.)	elb-tls-https-listeners-nur	Stellen Sie sicher, dass Ihre Elastic Load Balancer (ELBs) mit SSL- oder HTTPS-Listenern konfiguriert sind. Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.
4839	Sicherheit von Unternehmenssystemen, Cloud Computing, unbefugter Zugriff (22.1.24.C.04.)	encrypted-volumes	Aktivieren Sie die Verschlüsselung für Ihre Amazon-Elastic-Block-Store (Amazon-EBS)-Volumes, um eventuell vorhandene sensible Daten sowie Daten im Ruhezustand zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
4839	Sicherheit von Unternehmenssystemen, Cloud Computing, unbefugter Zugriff (22.1.24.C.04.)	opensearch-encrypted-at-rest	Dieses Steuerelement prüft, ob die Konfiguration für Domänen aktiviert ist. OpenSearch encryption-at-rest Die Prüfung schlägt fehl, wenn die Verschlüsselung im Ruhezustand nicht aktiviert ist. Für eine zusätzliche Sicherheitsebene für vertrauliche Daten sollten Sie Ihre OpenSearch Service-Domain so konfigurieren, dass sie im Ruhezustand verschlüsselt wird. Wenn Sie die Verschlüsselung von Daten im Ruhezustand konfigurieren, speichert und verwaltet AWS KMS Ihre Verschlüsselungsschlüssel. Für die Verschlüsselung verwendet AWS KMS den Advanced Encryption Standard-Algorithmus mit 256-Bit-Schlüsseln (AES-256).

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
4839	Sicherheit von Unternehmenssystemen, Cloud Computing, unbefugter Zugriff (22.1.24.C.04.)	opensearch-node-to-node-Verschlüsselungsprüfung	Dieses Steuerelement prüft, ob für Domänen die Verschlüsselung aktiviert ist. OpenSearch node-to-node Diese Kontrolle schlägt fehl, wenn die node-to-node Verschlüsselung in der Domain deaktiviert ist. HTTPS (TLS) kann verwendet werden, um zu verhindern, dass potenzielle Angreifer den Netzwerkverkehr mit person-in-the-middle oder ähnlichen Angriffen abhören oder manipulieren. Nur verschlüsselte Verbindungen über HTTPS (TLS) sollten zugelassen werden. Durch die Aktivierung der node-to-node Verschlüsselung für OpenSearch Domänen wird sichergestellt, dass die Kommunikation innerhalb des Clusters während

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			der Übertragung verschlüsselt wird.
4839	Sicherheit von Unternehmenssystemen, Cloud Computing, unbefugter Zugriff (22.1.24.C.04.)	rds-snapshot-encrypted	Stellen Sie sicher, dass die Verschlüsselung für Ihre Amazon Relational Database Service (Amazon RDS)-Snapshots aktiviert ist. Da sensible Daten auch im Ruhezustand vorhanden sein können, sollten Sie die Verschlüsselung von Daten im Ruhezustand aktivieren, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
4839	Sicherheit von Unternehmenssystemen, Cloud Computing, unbefugter Zugriff (22.1.24.C.04.)	rds-storage-encrypted	Zum Schutz von Daten im Ruhezustand müssen Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon Relational Database Service (Amazon RDS)-Instances aktiviert ist. Da sensible Daten in Amazon-RDS-Instances gespeichert werden können, sollten Sie die Verschlüsselung von Daten im Ruhezustand aktivieren, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
4839	Sicherheit von Unternehmenssystemen, Cloud Computing, unbefugter Zugriff (22.1.24.C.04.)	redshift-cluster-configuration-check	Um Daten im Ruhezustand zu schützen, muss die Verschlüsselung für Ihre Amazon-Redshift-Cluster aktiviert sein. Sie müssen auch sicherstellen, dass die erforderlichen Konfigurationen auf Amazon-Redshift-Clustern bereitgestellt werden. Die Prüfungsprotokollierung muss aktiviert sein, um Informationen zu Verbindungen und Benutzeraktivitäten in der Datenbank bereitzustellen. Diese Regel ist clusterDbEncrypted auf TRUE und LoggingEnabled auf TRUE gesetzt.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
4839	Sicherheit von Unternehmenssystemen, Cloud Computing, unbefugter Zugriff (22.1.24.C.04.)	redshift-require-tls-ssl	Stellen Sie sicher, dass Ihre Amazon-Redshift-Cluster eine TLS/SSL-Verschlüsselung erfordern, um eine Verbindung zu SQL-Clients herzustellen. Da sensible Daten vorhanden sein können, sollten Sie die Verschlüsselung bei der Übertragung aktivieren, um diese Daten zu schützen.
4839	Sicherheit von Unternehmenssystemen, Cloud Computing, unbefugter Zugriff (22.1.24.C.04.)	s-3 bucket-ssl-requests-only	Um Daten während der Übertragung zu schützen, stellen Sie sicher, dass Ihre Amazon Simple Storage Service (Amazon S3)-Buckets Anfragen zur Verwendung von Secure Socket Layer (SSL)-Buckets erfordern. Da sensible Daten vorhanden sein können, sollten Sie die Verschlüsselung bei der Übertragung aktivieren, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
4839	Sicherheit von Unternehmenssystemen, Cloud Computing, unbefugter Zugriff (22.1.24.C.04.)	sagemaker-endpoint-configuration-kms-schlüsselkonfiguriert	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass die Verschlüsselung mit dem AWS Key Management Service (AWS KMS) für Ihren Endpunkt aktiviert ist. SageMaker Da sensible Daten auf dem SageMaker Endgerät gespeichert werden können, sollten Sie die Verschlüsselung im Ruhezustand aktivieren, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
4839	Sicherheit von Unternehmenssystemen, Cloud Computing, unbefugter Zugriff (22.1.24.C.04.)	sagemaker-notebook-instance-kms-schlüsselkonfiguriert	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass die Verschlüsselung mit dem AWS Key Management Service (AWS KMS) für Ihr Notebook aktiviert ist. SageMaker Da vertrauliche Daten im SageMaker Notebook gespeichert werden können, sollten Sie die Verschlüsselung im Ruhezustand aktivieren, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
4839	Sicherheit von Unternehmenssystemen, Cloud Computing, unbefugter Zugriff (22.1.24.C.04.)	secretsmanager-using-cmk	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass die Verschlüsselung mit dem AWS Key Management Service (AWS KMS) für AWS Secrets Manager aktiviert ist. Aktivieren Sie die Verschlüsselung von Daten im Ruhezustand, um eventuell vorhandene sensible Daten im Ruhezustand im Secrets Manager zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
4839	Sicherheit von Unternehmenssystemen, Cloud Computing, unbefugter Zugriff (22.1.24.C.04.)	sns-encrypted-kms	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass Ihre Amazon Simple Notification Service (Amazon SNS) -Themen mit dem AWS Key Management Service (AWS KMS) verschlüsselt werden müssen. Um eventuell vorhandene sensible Daten im Ruhezustand in veröffentlichten Nachrichten zu schützen, muss die Verschlüsselung von Daten im Ruhezustand aktiviert sein. Eine Ausnahme ist verfügbar, wenn Nachrichten, die zu diesem Thema veröffentlicht wurden, keine sensiblen Daten enthalten.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
4849	Sicherheit von Unternehmenssystemen, Cloud Computing, Backup, Recovery, Archivierung und Datenremanenz (22.1.26.C.01.)	db-instance-backup-enabled	Die Sicherungsfunktion von Amazon RDS erstellt Sicherungen Ihrer Datenbanken und Transaktionsprotokolle. Amazon RDS erstellt einen Snapshot für das Speichervolume Ihrer DB-Instance, sodass die gesamte DB-Instance gesichert wird. Sie können im System spezifische Aufbewahrungsfristen festlegen, um Ihre Ausfallsicherheitsanforderungen zu erfüllen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
4849	Sicherheit von Unternehmenssystemen, Cloud Computing, Backup, Recovery, Archivierung und Datenremanenz (22.1.26.C.01.)	dynamodb-in-backup-plan	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon DynamoDB-Tabellen Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen. Eine Ausnahme ist verfügbar, wenn eine kompensierende Wiederherstellungslösung konfiguriert wurde.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
4849	Sicherheit von Unternehmenssystemen, Cloud Computing, Backup, Recovery, Archivierung und Datenremanenz (22.1.26.C.01.)	dynamodb-pitr-enabled	Aktivieren Sie diese Regel, um zu überprüfen, ob die Informationen gesichert wurden. Es verwaltet auch die Backups, indem es sicherstellt, dass die point-in-time Wiederherstellung in Amazon DynamoDB aktiviert ist. Bei der Wiederherstellung werden fortlaufende Backups Ihrer Tabelle für die letzten 35 Tage gespeichert.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
4849	Sicherheit von Unternehmenssystemen, Cloud Computing, Backup, Recovery, Archivierung und Datenremanenz (22.1.26.C.01.)	ebs-in-backup-plan	Stellen Sie zur Unterstützung der Datensicherungsprozesse sicher, dass Ihre Amazon Elastic Block Store (Amazon EBS) -Volumes Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen. Eine Ausnahme ist verfügbar, wenn eine kompensierende Wiederherstellungslösung konfiguriert wurde.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
4849	Sicherheit von Unternehmenssystemen, Cloud Computing, Backup, Recovery, Archivierung und Datenremanenz (22.1.26.C.01.)	efs-in-backup-plan	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon Elastic File System (Amazon EFS) -Dateisysteme Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen. Eine Ausnahme ist verfügbar, wenn eine kompensierende Wiederherstellungslösung konfiguriert wurde.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
4849	Sicherheit von Unternehmenssystemen, Cloud Computing, Backup, Recovery, Archivierung und Datenremanenz (22.1.26.C.01.)	elasticache-redis-cluster-automatic-Backup-Check	Wenn automatische Backups aktiviert sind, ElastiCache erstellt Amazon täglich ein Backup des Clusters. Die Sicherung kann für eine von Ihrer Organisation festgelegte Anzahl von Tagen aufbewahrt werden. Automatische Backups schützen vor Datenverlust. Bei einem Ausfall können Sie einen neuen Cluster erstellen, der Ihre Daten aus dem aktuellen Backup wiederherstellt.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
4849	Sicherheit von Unternehmenssystemen, Cloud Computing, Backup, Recovery, Archivierung und Datenremanenz (22.1.26.C.01.)	rds-cluster-deletion-protection-aktiviert	Stellen Sie sicher, dass für Amazon RDS-Instances der Löschschutz aktiviert ist. Verwenden Sie den Löschschutz, um zu verhindern, dass Ihre RDS-Instances versehentlich oder böswillig gelöscht werden, was zum Verlust der Verfügbarkeit Ihrer Anwendungen führen kann.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
4849	Sicherheit von Unternehmenssystemen, Cloud Computing, Backup, Recovery, Archivierung und Datenremanenz (22.1.26.C.01.)	rds-in-backup-plan	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon Relational Database Service (Amazon RDS) -Instances Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen. Eine Ausnahme ist verfügbar, wenn eine kompensierende Wiederherstellungslösung konfiguriert wurde.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
4849	Sicherheit von Unternehmenssystemen, Cloud Computing, Backup, Recovery, Archivierung und Datenremanenz (22.1.26.C.01.)	rds-instance-deletion-protection-aktiviert	Stellen Sie sicher, dass Amazon Relational Database Service (Amazon RDS)-Instances den Löschschutz aktiviert haben. Verwenden Sie den Löschschutz, um zu verhindern, dass Ihre Amazon-RDS-Instances versehentlich oder böswillig gelöscht werden, was zum Verlust der Verfügbarkeit Ihrer Anwendungen führen kann.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
4849	Sicherheit von Unternehmenssystemen, Cloud Computing, Backup, Recovery, Archivierung und Datenremanenz (22.1.26.C.01.)	redshift-backup-enabled	Stellen Sie zur Unterstützung der Datensicherungsprozesse sicher, dass Ihre Amazon-Redshift-Cluster über automatisierte Snapshots verfügen. Wenn automatisierte Snapshots für einen Cluster aktiviert sind, erstellt Redshift in regelmäßigen Abständen Snapshots dieses Clusters. Standardmäßig erzeugt Redshift ungefähr alle acht Stunden oder nach 5 GB geänderten Daten pro Knoten einen Snapshot, je nachdem, was zuerst auftritt.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
4849	Sicherheit von Unternehmenssystemen, Cloud Computing, Backup, Recovery, Archivierung und Datenremanenz (22.1.26.C.01.)	s-3 bucket-versioning-enabled	Die Versionsverwaltung von Amazon Simple Storage Service (Amazon S3)-Buckets hilft dabei, mehrere Varianten eines Objekts im selben Amazon-S3-Bucket zu speichern. Verwenden Sie die Versionsverwaltung, um sämtliche Versionen aller Objekte in Ihrem Amazon-S3-Bucket zu speichern, abzurufen oder wiederherzustellen. Mit der Versionsverwaltung können Sie Versionen sowohl nach unbeabsichtigten Benutzeraktionen als auch nach Anwendungsfehlern problemlos wiederherstellen. Eine Ausnahme ist verfügbar, wenn nur eine einzige Variante eines Objekts erstellt wird oder wenn eine kompensierende

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			Wiederherstellungslösung konfiguriert wurde.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
6843	Zugriffskontrolle und Passwörter, Privileged Access Management, das Prinzip der geringsten Rechte (16.4.31.C.02.)	mfa-enabled-for-iam-Konsolenzugriff	MFA bietet zusätzliche Sicherheit, da Benutzer beim Zugriff auf Websites oder Dienste zusätzlich zu ihren regulären Anmeldeinformationen eine eindeutige Authentifizierung über einen von AWS unterstützten MFA-Mechanismus vornehmen müssen. AWS Zu den unterstützten Mechanismen gehören U2F-Sicherheitsschlüssel, virtuelle oder Hardware-MFA-Geräte und SMS-basierte Codes. Diese Regel prüft, ob AWS Multi-Factor Authentication (MFA) für alle AWS Identity and Access Management (IAM)-Benutzer aktiviert ist, die ein Konsolenkennwort verwenden. Die Regel ist konform, wenn MFA aktiviert ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
6843	Zugriffskontrolle und Passwörter, Privileged Access Management, das Prinzip der geringsten Rechte (16.4.31.C.02.)	root-account-hardware-mfa-aktiviert	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Hardware-MFA für den Root-Benutzer aktiviert ist. Der Root-Benutzer ist der Benutzer mit den meisten Rechten in einem AWS Konto. MFA bietet eine weitere Schutzebene zusätzlich zum Benutzernamen und Passwort. Indem Sie MFA für den Root-Benutzer vorschreiben, können Sie die Anzahl kompromittierter Konten AWS reduzieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
6852	Zugriffskontrolle und Passwörte r, Verwaltun g privilegierter Zugriffe, Sperrung und Widerruf von Zugangsdaten (16.4.33.C.01.)	iam-user-unused-cr edentials-überprüfen	AWS Identity and Access Managemen t (IAM) kann Ihnen bei Zugriffsberechtigu ngen und Autorisie rungen helfen, indem es nach IAM-Passw örtern und Zugriffss chlüsseln sucht, die für einen bestimmte n Zeitraum nicht verwendet wurden. Wenn ungenutzte Anmeldeinformation en identifiziert werden, müssen Sie sie deaktivieren und/oder entfernen , da dies gegen das Prinzip der geringste n Berechtigung verstoßen könnte. Diese Regel legt das maxCredentialUsage Alter auf 30 Tage fest.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
6860	Zugriffskontrolle und Passwörte r, Verwaltung, Überwachung und Überprüfung privilegi erter Zugriffe (16.4.35. C.02.)	cloud-trail-cloud-watch-logs-aktiviert	Sie sollten CloudTrai l mit CloudWatch Logs konfigurieren, um Ihre Trail-Logs zu überwachen und bei bestimmten Aktivität en benachrichtigt zu werden. Diese Regel prüft, ob AWS CloudTrail Trails so konfiguriert sind, dass sie Logs an CloudWatch Amazon-Logs senden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
6860	Zugriffskontrolle und Passwörte r, Verwaltung, Überwachung und Überprüfung privilegi erter Zugriffe (16.4.35. C.02.)	cloudtrail-enabled	AWS CloudTrail kann durch die Aufzeichn ung von Aktionen und API-Aufrufen in der Managemen t Console bei der Nichtabstreitbarke it helfen. AWS Sie können die Benutzer und AWS Konten, die einen AWS Dienst aufgerufen haben, die Quell-IP-Adresse, über die die Anrufe generiert wurden, und die Zeitpunkte der Anrufe identifiz ieren. Einzelheiten zu den erfassten Daten finden Sie in den AWS CloudTrail Datensatzinhalten.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
6861	Zugriffskontrolle und Passwörte r, Verwaltung, Überwachung und Überprüfung privilegi erter Zugriffe (16.4.35. C.03.)	cloudtrail-security-trail-enabled	Diese Regel trägt dazu bei, die Verwendung der AWS empfohlenen bewährten Sicherhei tsmethoden für sicherzustellen AWS CloudTrai l, indem geprüft wird, ob mehrere Einstellungen aktiviert sind. Dazu gehören die Verwendun g von Protokoll verschlüsselung, Protokollvalidieru ng und Aktivierung AWS CloudTrail in mehreren Regionen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
6953	Zugriffskontrolle und Passwörter, Multi-Faktor-Authentifizierung, Systemarchitektur und Sicherheitskontrollen (16.7.34.C.02.)	mfa-enabled-for-iam-Konsolenzugriff	MFA bietet zusätzliche Sicherheit, da Benutzer beim Zugriff auf Websites oder Dienste zusätzlich zu ihren regulären Anmeldeinformationen eine eindeutige Authentifizierung über einen von AWS unterstützten MFA-Mechanismus vornehmen müssen. AWS Zu den unterstützten Mechanismen gehören U2F-Sicherheitsschlüssel, virtuelle oder Hardware-MFA-Geräte und SMS-basierte Codes. Diese Regel prüft, ob AWS Multi-Factor Authentication (MFA) für alle AWS Identity and Access Management (IAM)-Benutzer aktiviert ist, die ein Konsolenkennwort verwenden. Die Regel ist konform, wenn MFA aktiviert ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
6953	Zugriffskontrolle und Passwörter, Multi-Faktor-Authentifizierung, Systemarchitektur und Sicherheitskontrollen (16.7.34.C.02.)	root-account-hardware-mfa-aktiviert	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Hardware-MFA für den Root-Benutzer aktiviert ist. Der Root-Benutzer ist der Benutzer mit den meisten Rechten in einem AWS Konto. MFA bietet eine weitere Schutzebene zusätzlich zum Benutzernamen und Passwort. Indem Sie MFA für den Root-Benutzer vorschreiben, können Sie die Anzahl kompromittierter Konten AWS reduzieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
7436	Sicherheit in öffentlichen Clouds, Identitätsmanagement und Zugriffskontrolle, Benutzername und Passwörter (23.3.19.C.01.)	iam-user-mfa-enabled	Aktivieren Sie diese Regel, um den Zugriff auf Ressourcen in der Cloud einzuschränken. AWS Diese Regel stellt sicher, dass die Multi-Faktor-Authentifizierung (MFA) für alle IAM-Benutzer aktiviert ist. MFA bietet eine weitere Schutzebene zusätzlich zum Benutzernamen und Passwort. Reduzieren Sie Fälle von kompromittierten Konten, indem Sie MFA für IAM-Benutzer vorschreiben.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
7436	Sicherheit in öffentlichen Clouds, Identitätsmanagement und Zugriffskontrolle, Benutzername und Passwörter (23.3.19.C.01.)	mfa-enabled-for-iam-Konsolenzugriff	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass MFA für alle AWS Identity and Access Management (IAM) -Benutzer aktiviert ist, die über ein Konsolenkennwort verfügen. MFA bietet eine weitere Schutzebene zusätzlich zum Benutzernamen und Passwort. Indem Sie MFA für IAM-Benutzer vorschreiben, können Sie Vorfälle kompromittierter Konten reduzieren und verhindern, dass unbefugte Benutzer auf vertrauliche Daten zugreifen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
7436	Sicherheit in öffentlichen Clouds, Identitätsmanagement und Zugriffskontrolle, Benutzername und Passwörter (23.3.19.C.01.)	root-account-hardware-mfa-aktiviert	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Hardware-MFA für den Root-Benutzer aktiviert ist. Der Root-Benutzer ist der Benutzer mit den meisten Rechten in einem AWS Konto. MFA bietet eine weitere Schutzebene zusätzlich zum Benutzernamen und Passwort. Indem Sie MFA für den Root-Benutzer vorschreiben, können Sie die Anzahl kompromittierter Konten AWS reduzieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
7436	Sicherheit in öffentlichen Clouds, Identitätsmanagement und Zugriffskontrolle, Benutzername und Passwörter (23.3.19.C.01.)	root-account-mfa-enabled	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass MFA für den Root-Benutzer aktiviert ist. Der Root-Benutzer ist der privilegierteste Benutzer in einem AWS Konto. MFA bietet eine weitere Schutzebene zusätzlich zum Benutzernamen und Passwort. Indem Sie MFA für den Root-Benutzer vorschreiben, können Sie die Anzahl kompromittierter Konten AWS reduzieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
7437	Sicherheit in öffentlichen Clouds, Identitätsmanagement und Zugriffskontrolle, Benutzername und Passwörter (23.3.19.C.01.)	iam-user-mfa-enabled	Aktivieren Sie diese Regel, um den Zugriff auf Ressourcen in der Cloud einzuschränken. AWS Diese Regel stellt sicher, dass die Multi-Faktor-Authentifizierung (MFA) für alle IAM-Benutzer aktiviert ist. MFA bietet eine weitere Schutzebene zusätzlich zum Benutzernamen und Passwort. Reduzieren Sie Fälle von kompromittierten Konten, indem Sie MFA für IAM-Benutzer vorschreiben.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
7437	Sicherheit in öffentlichen Clouds, Identitätsmanagement und Zugriffskontrolle, Benutzername und Passwörter (23.3.19.C.01.)	mfa-enabled-for-iam-Konsolenzugriff	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass MFA für alle AWS Identity and Access Management (IAM) -Benutzer aktiviert ist, die über ein Konsolenkennwort verfügen. MFA bietet eine weitere Schutzebene zusätzlich zum Benutzernamen und Passwort. Indem Sie MFA für IAM-Benutzer vorschreiben, können Sie Vorfälle kompromittierter Konten reduzieren und verhindern, dass unbefugte Benutzer auf vertrauliche Daten zugreifen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
7437	Sicherheit in öffentlichen Clouds, Identitätsmanagement und Zugriffskontrolle, Benutzername und Passwörter (23.3.19.C.01.)	root-account-hardware-mfa-aktiviert	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Hardware-MFA für den Root-Benutzer aktiviert ist. Der Root-Benutzer ist der Benutzer mit den meisten Rechten in einem AWS Konto. MFA bietet eine weitere Schutzebene zusätzlich zum Benutzernamen und Passwort. Indem Sie MFA für den Root-Benutzer vorschreiben, können Sie die Anzahl kompromittierter Konten AWS reduzieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
7437	Sicherheit in öffentlichen Clouds, Identitätsmanagement und Zugriffskontrolle, Benutzername und Passwörter (23.3.19.C.01.)	root-account-mfa-enabled	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass MFA für den Root-Benutzer aktiviert ist. Der Root-Benutzer ist der privilegierteste Benutzer in einem AWS Konto. MFA bietet eine weitere Schutzebene zusätzlich zum Benutzernamen und Passwort. Indem Sie MFA für den Root-Benutzer vorschreiben, können Sie die Anzahl kompromittierter Konten AWS reduzieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
7466	Sicherheit in öffentlichen Clouds, Datenschutz in der öffentlichen Cloud, Datenzugänglichkeit (23.4.10.C.01.)	alb-waf-enabled	Stellen Sie sicher, dass AWS WAF auf Elastic Load Balancers (ELB) aktiviert ist, um Webanwendungen zu schützen. Eine WAF trägt zum Schutz Ihrer Webanwend ungen oder APIs vor gängigen Web-Explo its bei. Diese Web-Exploits können sich auf die Verfügbar keit auswirken, die Sicherheit gefährden oder übermäßige Ressourcen in Ihrer Umgebung verbrauch en.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
7466	Sicherheit in öffentlichen Clouds, Datenschutz in der öffentlichen Cloud, Datenzugänglichkeit (23.4.10.C.01.)	api-gw-associated-with-WAF	Dieses Steuerelement prüft, ob ein API-Gateway-Schritt eine AWS WAF-Webzugriffskontrolllliste (ACL) verwendet. Dieses Steuerelement schlägt fehl, wenn keine regionale AWS WAF-Web-ACL an eine REST-API-Gateway-Stufe angehängt ist. AWS WAF ist eine Firewall für Webanwendungen, die zum Schutz APIs von Webanwendungen und vor Angriffen beiträgt. Damit können Sie eine ACL konfigurieren. Dabei handelt es sich um eine Reihe von Regeln, die Webanfragen auf der Grundlage von anpassbaren Websicherheitsregeln und -bedingungen, die Sie definieren, zulassen, blockieren oder zählen. Stellen

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			Sie sicher, dass Ihre API-Gatew ay-Stufe mit einer AWS WAF-Web-A CL verknüpft ist, um sie vor böswilligen Angriffen zu schützen. Eine Ausnahme ist verfügbar, wenn das API Gateway der Ursprung für eine CloudFront Distribut ion mit aktivierter WAF ist.
7466	Sicherheit in öffentlichen Clouds, Datenschutz in der öffentlichen Cloud, Datenzugänglichkeit (23.4.10.C.01.)	dms-replication-not-public	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass auf DMS-Replikationsin stanzen nicht öffentlic h zugegriffen werden kann. DMS-Repli kations-Instances können vertrauli che Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
7466	Sicherheit in öffentlichen Clouds, Datenschutz in der öffentlichen Cloud, Datenzugänglichkeit (23.4.10.C.01.)	ec2-imdsv2-check	Stellen Sie sicher, dass die Methode Instance Metadata Service Version 2 (IMDSv2) aktiviert ist, um den Zugriff auf und die Kontrolle der Amazon Elastic Compute Cloud (Amazon EC2) - Instance-Metadate n zu schützen. Die IMDSv2 Methode verwendet sitzungsb asierte Kontrollen. Mit können Kontrolle n implementiert werden IMDSv2, um Änderungen an Instanzmetadaten einzuschränken.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
7466	Sicherheit in öffentlichen Clouds, Datenschutz in der öffentlichen Cloud, Datenzugänglichkeit (23.4.10.C.01.)	ec2- instance-no-public-ip	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon Elastic Compute Cloud (Amazon EC2) - Instances nicht öffentlich zugänglich sind. EC2 Amazon-Instances können vertrauliche Informationen enthalten, und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
7466	Sicherheit in öffentlichen Clouds, Datenschutz in der öffentlichen Cloud, Datenzugänglichkeit (23.4.10.C.01.)	ec2- instances-in-vpc	Stellen Sie Amazon Elastic Compute Cloud (Amazon EC2) -Instances innerhalb einer Amazon Virtual Private Cloud (Amazon VPC) bereit, um eine sichere Kommunika tion zwischen einer Instance und anderen Services innerhalb der Amazon VPC zu ermöglichen, ohne dass ein Internet-Gateway, ein NAT-Gerät oder eine VPN-Verbindung erforderl ich ist. Der gesamte Datenverkehr bleibt sicher in der AWS Cloud. Domänen, die sich innerhalb einer Amazon VPC befinden, verfügen aufgrund ihrer logischen Isolierun g im Vergleich zu Domänen, die öffentlic he Endpunkte nutzen, über eine zusätzlic he Sicherheitsebene. Weisen Sie EC2

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			Amazon-Instances einer Amazon VPC zu, um den Zugriff ordnungsgemäß zu verwalten.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
7466	Sicherheit in öffentlichen Clouds, Datenschutz in der öffentlichen Cloud, Datenzugänglichkeit (23.4.10.C.01.)	elasticsearch-in-vpc-only	Dieses Steuerelement prüft, ob sich Elasticsearch-Domains in einer VPC befinden. Es bewertet nicht die Konfiguration des VPC-Subnetz-Routings, um den öffentlichen Zugriff zu bestimmen. Sie sollten sicherstellen, dass Elasticsearch-Domains nicht an öffentliche Subnetze angehängt sind. Elasticsearch-Domains, die in einer VPC bereitgestellt werden, können über das private AWS Netzwerk mit VPC-Ressourcen kommunizieren, ohne das öffentliche Internet durchqueren zu müssen. Diese Konfiguration erhöht die Sicherheitslage, indem der Zugriff auf die Daten während der Übertragung eingeschränkt wird. VPCs bieten eine

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			Reihe von Netzwerkk ontrollen, um den Zugriff auf Elasticse arch-Domains zu sichern, einschließlich Netzwerk-ACL und Sicherheitsgruppen
7466	Sicherheit in öffentlichen Clouds, Datenschutz in der öffentlichen Cloud, Datenzugänglichkeit (23.4.10.C.01.)	emr-master-no-public-ip	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon EMR-Clust er-Masterknoten nicht öffentlich zugänglic h sind. Amazon-EM R-Cluster-Hauptkno ten können vertrauli che Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
7466	Sicherheit in öffentlichen Clouds, Datenschutz in der öffentlichen Cloud, Datenzugänglichkeit (23.4.10.C.01.)	guardduty-enabled-centralized	Amazon GuardDuty kann mithilfe von Threat Intellige nce Feeds helfen, potenzielle Cybersich erheitsereignisse zu überwachen und zu erkennen. Dazu gehören Listen mit bösartigen IPs und maschinel len Lernmethoden zur Identifizierung unerwarteter, nicht autorisierter und bösartiger Aktivitäten in Ihrer AWS Cloud-Umgebung.
7466	Sicherheit in öffentlichen Clouds, Datenschutz in der öffentlichen Cloud, Datenzugänglichkeit (23.4.10.C.01.)	lambda-function-public-access-verboten	Verwalten Sie den Zugriff auf Ressource n in der AWS Cloud, indem Sie sicherste llen, dass AWS Lambda-Funktionen nicht öffentlich zugänglich sind. Der öffentliche Zugriff kann möglicherweise die Verfügbarkeit von Ressourcen beeinträc htigen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
7466	Sicherheit in öffentlichen Clouds, Datenschutz in der öffentlichen Cloud, Datenzugänglichkeit (23.4.10.C.01.)	opensearch-in-vpc-only	Dieses Steuerelement prüft, ob sich OpenSearch Domänen in einer VPC befinden. Es bewertet nicht die Konfiguration des VPC-Subnetz-Routings, um den öffentlichen Zugriff zu bestimmen. Sie sollten sicherstellen, dass OpenSearch Domänen nicht an öffentliche Subnetze angehängt sind. OpenSearch Domänen, die in einer VPC bereitgestellt werden, können über das private AWS Netzwerk mit VPC-Ressourcen kommunizieren, ohne das öffentliche Internet durchqueren zu müssen. Diese Konfiguration erhöht das Sicherheitsniveau, indem der Zugriff auf die Daten während der Übertragung

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			eingeschränkt wird. VPCs bieten eine Reihe von Netzwerkkontrollen, um den Zugriff auf OpenSearch Domänen zu sichern, einschließlich Netzwerk-ACL und Sicherheitsgruppen.
7466	Sicherheit in öffentlichen Clouds, Datenschutz in der öffentlichen Cloud, Datenzugänglichkeit (23.4.10.C.01.)	rds-instance-public-access-überprüfen	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Relational Database Service (Amazon RDS) -Instances nicht öffentlich sind. Amazon-RDS-Datenbank-Instances können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
7466	Sicherheit in öffentlichen Clouds, Datenschutz in der öffentlichen Cloud, Datenzugänglichkeit (23.4.10.C.01.)	redshift-cluster-public-access-überprüfen	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Redshift Redshift-Cluster nicht öffentlich sind. Amazon-Redshift-Cluster können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
7466	Sicherheit in öffentlichen Clouds, Datenschutz in der öffentlichen Cloud, Datenzugänglichkeit (23.4.10.C.01.)	account-level-public-accesss3-Blöcke-periodisch	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Simple Storage Service (Amazon S3) -Buckets nicht öffentlich zugänglich sind. Diese Regel trägt dazu bei, sensible Daten vor unbefugten Remote-Benutzern zu schützen, indem sie den öffentlichen Zugriff verhindert. Diese Regel wird ignorePublicAcls auf TRUE blockPublicPolicy , TRUE, blockPublicAcls TRUE und TRUE restrictPublicBuckets gesetzt.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
7466	Sicherheit in öffentlichen Clouds, Datenschutz in der öffentlichen Cloud, Datenzugänglichkeit (23.4.10.C.01.)	sagemaker-notebook-no-direct-Internetzugang	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass SageMaker Amazon-Notebooks keinen direkten Internetzugang zulassen. Indem Sie direkten Internetzugang blockieren, vermeiden Sie, dass unbefugte Benutzer auf sensible Daten zugreifen.
7466	Sicherheit in öffentlichen Clouds, Datenschutz in der öffentlichen Cloud, Datenzugänglichkeit (23.4.10.C.01.)	ssm-document-not-public	Stellen Sie sicher, dass AWS Systems Manager (SSM) - Dokumente nicht öffentlich sind, da dies einen unbeabsichtigten Zugriff auf Ihre SSM-Dokumente ermöglichen kann. Ein öffentliches SSM-Dokument kann Informationen über Ihr Konto, Ihre Ressourcen und internen Prozesse preisgeben.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
7466	Sicherheit in öffentlichen Clouds, Datenschutz in der öffentlichen Cloud, Datenzugänglichkeit (23.4.10.C.01.)	vpc-default-security-group-geschlossen	Sicherheitsgruppen von Amazon Elastic Compute Cloud (Amazon EC2) können bei der Verwaltung des Netzwerkzugriffs helfen, indem sie eine statusbehaftete Filterung des ein- und ausgehenden Netzwerkverkehrs zu Ressourcen bereitstellen. AWS Die Beschränk ung des gesamten Datenverkehrs auf die Standardsicherheit sgruppe hilft dabei, den Fernzugriff auf Ihre Ressourcen einzuschränken. AWS

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
7466	Sicherheit in öffentlichen Clouds, Datenschutz in der öffentlichen Cloud, Datenzugänglichkeit (23.4.10.C.01.)	vpc-flow-logs-enabled	VPC-Flow-Protokolle erfassen detaillierte Informationsdatensätze über den IP-Datenverkehr, der zu und von Netzwerkschnittstellen in Ihrer Amazon Virtual Private Cloud (Amazon VPC) fließt. Standardmäßig enthalten Flow-Protokolldatensätze Werte für die verschiedenen Komponenten des IP-Flows, einschließlich Quelle, Ziel und Protokoll.
7496	Öffentliche Cloud-Sicherheit, Protokollierung und Warnmeldungen in der Public Cloud, Protokollierungsanforderungen (23.5.11.C.01.)	api-gw-execution-logging-aktiviert	Die API-Gateway-Protokollierung zeigt detaillierte Ansichten der Benutzer, die auf die API zugegriffen haben, und wie diese Benutzer auf die API zugegriffen haben. Diese Insights ermöglichen die Einsicht in Benutzeraktivitäten.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
7496	Öffentliche Cloud-Sicherheit, Protokollierung und Warnmeldungen in der Public Cloud, Protokollierungsan forderungen (23.5.11. C.01.)	cloud-trail-log-file-validierung aktiviert	Verwenden Sie die Validierung von AWS CloudTrail Protokolldateien, um die Integrität von Protokollen zu überprüfen. CloudTrai l Mithilfe der Protokoll dateivalidierung kann festgestellt werden, ob eine Protokoll datei geändert oder gelöscht wurde oder ob sie nach der Übermittlung CloudTrail unverände rt geblieben ist. Dieses Feature wurde mit dem Branchens tandard entsprech enden Algorithmen entwickelt: SHA-256 für die Hashfunktion und SHA-256 mit RSA für digitale Signature n. Aus diesem Grund ist es rechnerisch unmöglich, CloudTrai l Protokolldateien unbemerkt zu ändern, zu löschen oder zu fälschen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
7496	Öffentliche Cloud-Sicherheit, Protokollierung und Warnmeldungen in der Public Cloud, Protokollierungsanforderungen (23.5.11.C.01.)	cloudfront-accesslogs-enabled	Dieses Steuerelement prüft, ob die Serverzugriffsprotokollierung für Distributionen aktiviert ist. CloudFront Die Steuerung schlägt fehl, wenn die Zugriffsprotokollierung für eine Verteilung nicht aktiviert ist. CloudFront Zugriffsprotokolle enthalten detaillierte Informationen zu jeder eingehenden CloudFront Benutzeranfrage. Jedes Protokoll enthält Informationen wie Datum und Uhrzeit des Eingangs der Anfrage, die IP-Adresse des Betrachters, der die Anfrage gestellt hat, die Quelle der Anfrage und die Portnummer der Anfrage vom Betrachter. Diese Protokolle sind für Anwendungen wie

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			Sicherheits- und Zugriffsprüfungen sowie forensische Untersuchungen nützlich. Diese Regel muss in der Region us-east-1 angewende t werden.
7496	Öffentliche Cloud-Sicherheit, Protokollierung und Warnmeldungen in der Public Cloud, Protokollierungsan forderungen (23.5.11. C.01.)	cloudtrail-enabled	AWS CloudTrail kann durch die Aufzeichn ung von Aktionen und API-Aufrufen in der Managemen t Console bei der Nichtabstreitbarke it helfen. AWS Sie können die Benutzer und AWS Konten, die einen AWS Dienst aufgerufen haben, die Quell-IP-Adresse, über die die Anrufe generiert wurden, und die Zeitpunkte der Anrufe identifiz ieren. Einzelheiten zu den erfassten Daten finden Sie in den AWS CloudTrail Datensatzinhalten.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
7496	Öffentliche Cloud-Sicherheit, Protokollierung und Warnmeldungen in der Public Cloud, Protokollierungsanforderungen (23.5.11.C.01.)	cloudwatch-log-group-encrypted	Um sensible Daten im Speicher zu schützen, stellen Sie sicher, dass die Verschlüsselung für Ihre Amazon CloudWatch Log Groups aktiviert ist.
7496	Öffentliche Cloud-Sicherheit, Protokollierung und Warnmeldungen in der Public Cloud, Protokollierungsanforderungen (23.5.11.C.01.)	elb-logging-enabled	Die Elastic-Load-Balancing-Aktivität ist ein zentraler Kommunikationspunkt innerhalb einer Umgebung. Stellen Sie sicher, dass die ELB-Protokollierung aktiviert ist. Die gesammelten Daten enthalten detaillierte Informationen zu Anfragen, die an den ELB gesendet wurden. Jedes Protokoll enthält Informationen wie die Zeit, zu der die Anforderung einging, die Client-IP-Adresse, Latenzen, Anforderungspfade und Serverantworten.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
7496	Öffentliche Cloud-Sicherheit, Protokollierung und Warnmeldungen in der Public Cloud, Protokollierungsanforderungen (23.5.11.C.01.)	rds-logging-enabled	Um die Protokollierung und Überwachung in Ihrer Umgebung zu erleichtern, stellen Sie sicher, dass die Amazon Relational Database Service (Amazon RDS)-Protokollierung aktiviert ist. Mit der Amazon-RDS-Protokollierung können Sie Ereignisse wie Verbindungen, Verbindungsabbrüche, Abfragen oder abgefragte Tabellen erfassen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
7496	Öffentliche Cloud-Sicherheit, Protokollierung und Warnmeldungen in der Public Cloud, Protokollierungsanforderungen (23.5.11.C.01.)	wafv2-logging-enabled	Um die Protokollierung und Überwachung in Ihrer Umgebung zu erleichtern, aktivieren Sie die AWS WAF (V2) -Protokollierung im regionalen und globalen Web. ACLs AWS Die WAF-Protokollierung bietet detaillierte Informationen über den Datenverkehr, der von Ihrer Web-ACL analysiert wird. In den Protokollen werden die Uhrzeit aufgezeichnet, zu der die AWS WAF die Anfrage von Ihrer AWS Ressource erhalten hat, Informationen über die Anfrage und eine Aktion für die Regel, der jede Anfrage entsprach.

Vorlage

Die Vorlage ist verfügbar unter GitHub: Operational Best Practices for NZISM.

Bewährte Methoden für die Ausführung von PCI DSS 3.2.1

Konformitätspakete bieten ein allgemeines Compliance-Framework, das es Ihnen ermöglicht, mithilfe verwalteter oder benutzerdefinierter Regeln und Abhilfemaßnahmen Kontrollen zur Sicherheits-, Betriebs- oder Kostenoptimierung durchzuführen. AWS Config AWS Config Conformance Packs dienen als Beispielvorlagen nicht dazu, die vollständige Einhaltung eines bestimmten Governance- oder Compliance-Standards sicherzustellen. Sie sind dafür verantwortlich, selbst zu beurteilen, ob Ihre Nutzung der Services den geltenden gesetzlichen und behördlichen Anforderungen entspricht.

Im Folgenden finden Sie ein Beispiel für eine Zuordnung zwischen dem Payment Card Industry Data Security Standard (PCI DSS) 3.2.1 und AWS verwalteten Konfigurationsregeln. Jede AWS Config Regel gilt für eine bestimmte AWS Ressource und bezieht sich auf eine oder mehrere PCI-DSS-Steuerelemente. Eine PCI-DSS-Kontrolle kann mehreren Konfigurationsregeln zugeordnet werden. In der folgenden Tabelle finden Sie weitere Informationen und Anleitungen zu diesen Zuordnungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
1.3	Verbieten Sie den direkten öffentlichen Zugriff zwischen dem Internet und allen Systemkomponenten in der Karteninh aberdatenumgebung.	alb-desync-mode-check	Um Anwendungen vor HTTP-Desync-Schwachstellen zu schützen, stellen Sie sicher, dass der HTTP-Desync-Mitigationsmodus auf Ihren Anwendungs-Loadbalancern aktiviert ist. Probleme mit HTTP-Desync können zum Schmuggel von Anfragen führen und Ihre Anwendungen anfällig für Queues- oder Cache-Poisoning machen. Die desynchronen Mitigationsmodi

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			lauten „Überwachen“, „Defensiv“ und „Am strengsten“. Defensive ist der standardmäßige Modus.
1.3	Verbieten Sie den direkten öffentlichen Zugriff zwischen dem Internet und allen Systemkomponenten in der Karteninhaberdatenumgebung.	alb-http-drop-invalid-Header-fähig	Stellen Sie sicher, dass Ihre Elastic Load Balancers (ELB) so konfiguriert sind, dass sie HTTP-Header löschen. Da sensible Daten vorhanden sein können, sollten Sie die Verschlüsselung bei der Übertragung aktivieren, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
1.3	Verbieten Sie den direkten öffentlichen Zugriff zwischen dem Internet und allen Systemkomponenten in der Karteninh aberdatenumgebung.	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) Security Groups können bei der Verwaltung des Netzwerkzugriffs helfen, indem sie eine statusbeh aftete Filterung von eingehendem und ausgehendem Netzwerkverkehr zu Ressourcen bereitste llen. AWS Wenn Sie eingehenden (oder entfernten) Datenverk ehr von 0.0.0.0/0 bis Port 22 auf Ihren Ressourcen nicht zulassen, können Sie den Remote-Zugriff einschränken.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
1.3	Verbieten Sie den direkten öffentlichen Zugriff zwischen dem Internet und allen Systemkomponenten in der Karteninh aberdatenumgebung.	autoscaling-launch-config-public-ip-deaktiviert	Wenn Sie Ihre Netzwerkschnittstellen mit einer öffentlichen IP-Adresse konfiguri eren, sind die diesen Netzwerkschnittste llen zugehörigen Ressourcen über das Internet erreichba r. EC2 Ressourcen sollten nicht öffentlic h zugänglich sein, da dies einen unbeabsic htigten Zugriff auf Ihre Anwendungen oder Server ermöglichen kann.
1.3	Verbieten Sie den direkten öffentlichen Zugriff zwischen dem Internet und allen Systemkomponenten in der Karteninh aberdatenumgebung.	dms-replication-not-public	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass auf DMS-Replikationsin stanzen nicht öffentlic h zugegriffen werden kann. DMS-Repli kations-Instances können vertrauli che Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
1.3	Verbieten Sie den direkten öffentlichen Zugriff zwischen dem Internet und allen Systemkomponenten in der Karteninh aberdatenumgebung.	ebs-snapshot-public-restorable-überprüfen	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass EBS-Snapshots nicht öffentlich wiederher stellbar sind. EBS-Volume-Snapsho ts können vertrauli che Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.
1.3	Verbieten Sie den direkten öffentlichen Zugriff zwischen dem Internet und allen Systemkomponenten in der Karteninh aberdatenumgebung.	ec-2 instance-no-public-ip	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon Elastic Compute Cloud (Amazon EC2) - Instances nicht öffentlich zugänglich sind. EC2 Amazon-Instances können vertrauliche Informati onen enthalten, und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
1.3	Verbieten Sie den direkten öffentlichen Zugriff zwischen dem Internet und allen Systemkomponenten in der Karteninh aberdatenumgebung.	elasticsearch-in-vpc-only	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherste llen, dass sich Amazon OpenSearc h OpenSearch Service (Service) - Domains innerhalb einer Amazon Virtual Private Cloud (Amazon VPC) befinden. Eine OpenSearch Service-Domain innerhalb einer Amazon VPC ermöglicht die sichere Kommunikation zwischen OpenSearc h Service und anderen Services innerhalb der Amazon VPC, ohne dass ein Internet-Gateway, ein NAT-Gerät oder eine VPN-Verbindung erforderlich ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
1.3	Verbieten Sie den direkten öffentlichen Zugriff zwischen dem Internet und allen Systemkomponenten in der Karteninh aberdatenumgebung.	emr-master-no-public-ip	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon EMR-Clust er-Masterknoten nicht öffentlich zugänglic h sind. Amazon-EM R-Cluster-Hauptkno ten können vertrauli che Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
1.3	Verbieten Sie den direkten öffentlichen Zugriff zwischen dem Internet und allen Systemkomponenten in der Karteninh aberdatenumgebung.	ec-2 instances-in-vpc	Stellen Sie Amazon Elastic Compute Cloud (Amazon EC2) -Instances innerhalb einer Amazon Virtual Private Cloud (Amazon VPC) bereit, um eine sichere Kommunika tion zwischen einer Instance und anderen Services innerhalb der Amazon VPC zu ermöglichen, ohne dass ein Internet-Gateway, ein NAT-Gerät oder eine VPN-Verbindung erforderlich ist. Der gesamte Datenverk ehr bleibt sicher in der AWS Cloud. Domains, die sich innerhalb einer VPC befinden, verfügen aufgrund ihrer logischen Isolierun g im Vergleich zu Domains mit öffentlic hen Endpunkten über eine zusätzlic he Sicherheitsebene. Weisen Sie EC2

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			Amazon-Instances einer Amazon-VPC zu, um den Zugriff ordnungsgemäß zu verwalten.
1.3	Verbieten Sie den direkten öffentlichen Zugriff zwischen dem Internet und allen Systemkomponenten in der Karteninh aberdatenumgebung.	lambda-function-public-access-verboten	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass AWS Lambda-Funktionen nicht öffentlich zugänglich sind. Der öffentliche Zugriff kann möglicherweise die Verfügbarkeit von Ressourcen beeinträchtigen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
1.3	Verbieten Sie den direkten öffentlichen Zugriff zwischen dem Internet und allen Systemkomponenten in der Karteninh aberdatenumgebung.	lambda-inside-vpc	Stellen Sie AWS Lambda-Funktionen in einer Amazon Virtual Private Cloud (Amazon VPC) bereit, um eine sichere Kommunika tion zwischen einer Funktion und anderen Diensten innerhalb der Amazon VPC zu gewährleisten. Bei dieser Konfiguration sind kein Internet-Gateway, kein NAT-Gerät und keine VPN-Verbindung erforderlich. Der gesamte Datenverk ehr bleibt sicher in der Cloud. AWS Domains, die sich innerhalb einer VPC befinden, verfügen aufgrund ihrer logischen Isolierun g im Vergleich zu Domains mit öffentlic hen Endpunkten über eine zusätzliche Sicherheitsebene. Um den Zugriff ordnungsg emäß zu verwalten,

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			sollten AWS Lambda-Funktionen einer VPC zugewiesen werden.
1.3	Verbieten Sie den direkten öffentlichen Zugriff zwischen dem Internet und allen Systemkomponenten in der Karteninh aberdatenumgebung.	netfw-stateless-rule-group-nicht leer	Eine AWS Netzwerkf irewall-Regelgrupp e enthält Regeln, die definieren, wie Ihre Firewall den Verkehr in Ihrer VPC verarbeit et. Wenn eine leere statuslose Regelgrup pe in einer Firewall-Richtlinie vorhanden ist, verarbeitet sie keinen Datenverkehr.
1.3	Verbieten Sie den direkten öffentlichen Zugriff zwischen dem Internet und allen Systemkomponenten in der Karteninh aberdatenumgebung.	no-unrestricted-route-to-igw	Stellen Sie sicher, dass EC2 Amazon-Routentabellen keine uneingeschränkten Routen zu einem Internet-Gateway enthalten. Durch das Entfernen oder Beschränken des Internetzugangs für Workloads innerhalb von Amazon VPCs können unbeabsic htigte Zugriffe in Ihrer Umgebung reduziert werden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
1.3	Verbieten Sie den direkten öffentlichen Zugriff zwischen dem Internet und allen Systemkomponenten in der Karteninh aberdatenumgebung.	opensearch-in-vpc-only	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass sich Amazon OpenSearch Service-Domains innerhalb einer Amazon Virtual Private Cloud (Amazon VPC) befinden. Eine Amazon OpenSearc h Service-Domain innerhalb einer Amazon VPC ermöglicht die sichere Kommunikation zwischen Amazon OpenSearch Service und anderen Services innerhalb der Amazon VPC, ohne dass ein Internet-Gateway, ein NAT-Gerät oder eine VPN-Verbindung erforderlich ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
1.3	Verbieten Sie den direkten öffentlichen Zugriff zwischen dem Internet und allen Systemkomponenten in der Karteninh aberdatenumgebung.	rds-instance-public-access-überprüfen	Verwalten Sie den Zugriff auf Ressource n in der AWS Cloud, indem Sie sicherste llen, dass Amazon Relational Database Service (Amazon RDS) -Instance s nicht öffentlic h sind. Amazon-RDS-Datenbank-Instances können vertrauliche Informati onen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
1.3	Verbieten Sie den direkten öffentlichen Zugriff zwischen dem Internet und allen Systemkomponenten in der Karteninh aberdatenumgebung.	rds-snapshots-public-prohibited	Verwalten Sie den Zugriff auf Ressource n in der AWS Cloud, indem Sie sicherste llen, dass Amazon Relational Database Service (Amazon RDS) -Instance s nicht öffentlic h sind. Amazon-RDS-Datenbank-Instances können vertrauliche Informati onen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
1.3	Verbieten Sie den direkten öffentlichen Zugriff zwischen dem Internet und allen Systemkomponenten in der Karteninh aberdatenumgebung.	redshift-cluster-public-access-überprüfen	Verwalten Sie den Zugriff auf Ressource n in der AWS Cloud, indem Sie sicherste llen, dass Amazon Redshift Redshift-Cluster nicht öffentlic h sind. Amazon-Re dshift-Cluster können vertrauliche Informati onen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
1.3	Verbieten Sie den direkten öffentlichen Zugriff zwischen dem Internet und allen Systemkomponenten in der Karteninh aberdatenumgebung.	restricted-common-ports	Verwalten Sie den Zugriff auf Ressource n in der AWS Cloud, indem Sie sicherste llen, dass gemeinsam e Ports für Amazon Elastic Compute Cloud (Amazon EC2) -Sicherhe itsgruppen eingeschr änkt sind. Wenn der Zugriff auf Ports nicht auf vertrauen swürdige Quellen beschränkt wird, kann dies zu Angriffen auf die Verfügbar keit, Integrität und Vertraulichkeit von Systemen führen. Mit dieser Regel können Sie optional die Parameter blockedPo rt1–blockedPort5 festlegen (Standard konfigurationen: 20, 21, 3389, 3306, 4333). Die tatsächli chen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
1.3	Verbieten Sie den direkten öffentlichen Zugriff zwischen dem Internet und allen Systemkomponenten in der Karteninh aberdatenumgebung.	s3- account-level-publ ic-access -Block-pe riodisch	Verwalten Sie den Zugriff auf Ressource n in der AWS Cloud, indem Sie sicherste llen, dass Amazon Simple Storage Service (Amazon S3) -Buckets nicht öffentlich zugänglic h sind. Diese Regel trägt dazu bei, sensible Daten vor unbefugten Remote-Benutzern zu schützen, indem sie den öffentlichen Zugriff verhinder t. Mit dieser Regel können Sie optional die Parameter ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) und restrictPublicBuck ets Parameter (Config Default: True) festlegen. Die tatsächlichen Werte müssen den Richtlini

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			en Ihrer Organisation entsprechen.
1.3	Verbieten Sie den direkten öffentlichen Zugriff zwischen dem Internet und allen Systemkomponenten in der Karteninh aberdatenumgebung.	s3 bucket-level-public-access - verboten	Verwalten Sie den Zugriff auf Ressource n in der AWS Cloud, indem Sie sicherste llen, dass Amazon Simple Storage Service (Amazon S3) -Buckets nicht öffentlich zugänglic h sind. Diese Regel trägt dazu bei, sensible Daten vor unbefugten Remote-Benutzern zu schützen, indem sie den öffentlichen Zugriff auf Bucket-Eb ene verhindert.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
1.3	Verbieten Sie den direkten öffentlichen Zugriff zwischen dem Internet und allen Systemkomponenten in der Karteninh aberdatenumgebung.	s-3 bucket-public-read -prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie nur autorisierten Benutzern, Prozessen und Geräten Zugriff auf Amazon Simple Storage Service (Amazon S3) - Buckets gewähren. Die Verwaltung des Zugriffs sollte mit der Klassifizierung der Daten übereinst immen.
1.3	Verbieten Sie den direkten öffentlichen Zugriff zwischen dem Internet und allen Systemkomponenten in der Karteninh aberdatenumgebung.	s3- bucket-public-writ e-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie nur autorisierten Benutzern, Prozessen und Geräten Zugriff auf Amazon Simple Storage Service (Amazon S3) - Buckets gewähren. Die Verwaltung des Zugriffs sollte mit der Klassifizierung der Daten übereinst immen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
1.3	Verbieten Sie den direkten öffentlichen Zugriff zwischen dem Internet und allen Systemkomponenten in der Karteninh aberdatenumgebung.	sagemaker-notebook-no-direct-Internetzugang	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass SageMaker Amazon-Notebooks keinen direkten Internetzugang zulassen. Indem Sie direkten Internetzugang blockieren, vermeiden Sie, dass unbefugte Benutzer auf sensible Daten zugreifen.
1.3	Verbieten Sie den direkten öffentlichen Zugriff zwischen dem Internet und allen Systemkomponenten in der Karteninh aberdatenumgebung.	ssm-document-not-public	Stellen Sie sicher, dass AWS Systems Manager (SSM) - Dokumente nicht öffentlich sind, da dies einen unbeabsichtigten Zugriff auf Ihre SSM-Dokumente ermöglichen kann. Ein öffentliches SSM-Dokument kann Informationen über Ihr Konto, Ihre Ressourcen und internen Prozesse preisgeben.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
1.3	Verbieten Sie den direkten öffentlichen Zugriff zwischen dem Internet und allen Systemkomponenten in der Karteninh aberdatenumgebung.	subnet-auto-assign-public-ip-deaktiviert	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon Virtual Private Cloud (VPC) -Subnetzen nicht automatisch eine öffentliche IP-Adress e zugewiesen wird. Amazon Elastic Compute Cloud (EC2) -Instances, die in Subnetzen gestartet werden, in denen dieses Attribut aktiviert ist, haben ihrer primären Netzwerkschnittste lle eine öffentliche IP-Adresse zugewiesen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
1.3	Verbieten Sie den direkten öffentlichen Zugriff zwischen dem Internet und allen Systemkomponenten in der Karteninh aberdatenumgebung.	vpc-default-security-group-geschlossen	Sicherheitsgruppen von Amazon Elastic Compute Cloud (Amazon EC2) können bei der Verwaltung des Netzwerkzugriffs helfen, indem sie eine statusbehaftete Filterung des ein- und ausgehenden Netzwerkverkehrs zu Ressourcen bereitstellen. AWS Die Beschränk ung des gesamten Datenverkehrs auf die Standardsicherheit sgruppe hilft dabei, den Fernzugriff auf Ihre Ressourcen einzuschränken. AWS

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
1.3	Verbieten Sie den direkten öffentlichen Zugriff zwischen dem Internet und allen Systemkomponenten in der Karteninh aberdatenumgebung.	vpc-sg-open-only-to-authorized-ports	Verwalten Sie den Zugriff auf Ressource n in der AWS Cloud, indem Sie sicherste llen, dass gemeinsam e Ports für Amazon Elastic Compute Cloud (Amazon EC2) -Sicherhe itsgruppen eingeschr ränkt sind. Wenn der Zugriff auf Ports nicht auf vertrauen swürdige Quellen beschränkt wird, kann dies zu Angriffen auf die Verfügbar keit, Integrität und Vertraulichkeit von Systemen führen. Durch die Beschränk ung des Zugriffs auf Ressourcen innerhalb einer Sicherhei tsgruppe aus dem Internet (0.0.0.0/0) kann der Fernzugriff auf interne Systeme gesteuert werden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
1.3.6	Speichern von Systemkomponenten, die Karteninh aberdaten beinhalten (z. B. eine Datenbank), in einer internen Netzwerkzone, die sowohl von der DMZ als auch von anderen nicht vertrauen swürdigen Netzwerke n getrennt ist.	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) Security Groups können bei der Verwaltung des Netzwerkzugriffs helfen, indem sie eine statusbeh aftete Filterung von eingehendem und ausgehendem Netzwerkverkehr zu Ressourcen bereitste llen. AWS Wenn Sie eingehenden (oder entfernten) Datenverk ehr von 0.0.0.0/0 bis Port 22 auf Ihren Ressourcen nicht zulassen, können Sie den Remote-Zugriff einschränken.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
1.3.6	Speichern von Systemkomponenten, die Karteninh aberdaten beinhalten (z. B. eine Datenbank), in einer internen Netzwerkzone, die sowohl von der DMZ als auch von anderen nicht vertrauen swürdigen Netzwerke n getrennt ist.	autoscaling-launch -config-public-ip- deaktiviert	Wenn Sie Ihre Netzwerkschnittstellen mit einer öffentlichen IP-Adresse konfiguri eren, sind die diesen Netzwerkschnittste llen zugehörigen Ressourcen über das Internet erreichba r. EC2 Ressourcen sollten nicht öffentlic h zugänglich sein, da dies einen unbeabsic htigten Zugriff auf Ihre Anwendungen oder Server ermöglichen kann.
1.3.6	Speichern von Systemkomponenten, die Karteninh aberdaten beinhalten (z. B. eine Datenbank), in einer internen Netzwerkzone, die sowohl von der DMZ als auch von anderen nicht vertrauen swürdigen Netzwerke n getrennt ist.	dms-replication-not- public	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass auf DMS-Replikationsin stanzen nicht öffentlic h zugegriffen werden kann. DMS-Repli kations-Instances können vertrauli che Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
1.3.6	Speichern von Systemkomponenten, die Karteninh aberdaten beinhalten (z. B. eine Datenbank), in einer internen Netzwerkzone, die sowohl von der DMZ als auch von anderen nicht vertrauen swürdigen Netzwerke n getrennt ist.	ebs-snapshot-public-restorable-überprüfen	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass EBS-Snapshots nicht öffentlich wiederher stellbar sind. EBS-Volume-Snapsho ts können vertrauli che Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.
1.3.6	Speichern von Systemkomponenten, die Karteninh aberdaten beinhalten (z. B. eine Datenbank), in einer internen Netzwerkzone, die sowohl von der DMZ als auch von anderen nicht vertrauen swürdigen Netzwerke n getrennt ist.	ec-2 instance-no-public-ip	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon Elastic Compute Cloud (Amazon EC2) - Instances nicht öffentlich zugänglich sind. EC2 Amazon-Instances können vertrauliche Informati onen enthalten, und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
1.3.6	Speichern von Systemkomponenten, die Karteninh aberdaten beinhalten (z. B. eine Datenbank), in einer internen Netzwerkzone, die sowohl von der DMZ als auch von anderen nicht vertrauen swürdigen Netzwerke n getrennt ist.	elasticsearch-in-vpc-only	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherste llen, dass sich Amazon OpenSearc h OpenSearch Service (Service) - Domains innerhalb einer Amazon Virtual Private Cloud (Amazon VPC) befinden. Eine OpenSearch Service-Domain innerhalb einer Amazon VPC ermöglicht die sichere Kommunikation zwischen OpenSearc h Service und anderen Services innerhalb der Amazon VPC, ohne dass ein Internet-Gateway, ein NAT-Gerät oder eine VPN-Verbindung erforderlich ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
1.3.6	Speichern von Systemkomponenten, die Karteninh aberdaten beinhalten (z. B. eine Datenbank), in einer internen Netzwerkzone, die sowohl von der DMZ als auch von anderen nicht vertrauen swürdigen Netzwerke n getrennt ist.	ec2- instances-in-vpc	Stellen Sie Amazon Elastic Compute Cloud (Amazon EC2) -Instances innerhalb einer Amazon Virtual Private Cloud (Amazon VPC) bereit, um eine sichere Kommunika tion zwischen einer Instance und anderen Services innerhalb der Amazon VPC zu ermöglichen, ohne dass ein Internet-Gateway, ein NAT-Gerät oder eine VPN-Verbindung erforderlich ist. Der gesamte Datenverk ehr bleibt sicher in der AWS Cloud. Domains, die sich innerhalb einer VPC befinden, verfügen aufgrund ihrer logischen Isolierun g im Vergleich zu Domains mit öffentlic hen Endpunkten über eine zusätzlic he Sicherheitsebene. Weisen Sie EC2

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			Amazon-Instances einer Amazon-VPC zu, um den Zugriff ordnungsgemäß zu verwalten.
1.3.6	Speichern von Systemkomponenten, die Karteninh aberdaten beinhalten (z. B. eine Datenbank), in einer internen Netzwerkzone, die sowohl von der DMZ als auch von anderen nicht vertrauen swürdigen Netzwerke n getrennt ist.	netfw-policy-rule-group-verknüpft	Eine AWS Netzwerk-Firewall-Richtlinie definiert, wie Ihre Firewall den Verkehr in einer Amazon VPC überwacht und verarbeitet. Sie konfigurieren statusfre ie und statusbehaftete Regelgruppen, um Pakete und Datenverk ehrsströme zu filtern, und Sie definiere n den standardm äßigen Umgang mit Datenverkehr.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
1.3.6	Speichern von Systemkomponenten, die Karteninh aberdaten beinhalten (z. B. eine Datenbank), in einer internen Netzwerkzone, die sowohl von der DMZ als auch von anderen nicht vertrauen swürdigen Netzwerke n getrennt ist.	netfw-stateless-rule-group-nicht leer	Eine AWS Netzwerkf irewall-Regelgrupp e enthält Regeln, die definieren, wie Ihre Firewall den Verkehr in Ihrer VPC verarbeit et. Wenn eine leere statuslose Regelgrup pe in einer Firewall-Richtlinie vorhanden ist, verarbeitet sie keinen Datenverkehr.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
1.3.6	Speichern von Systemkomponenten, die Karteninh aberdaten beinhalten (z. B. eine Datenbank), in einer internen Netzwerkzone, die sowohl von der DMZ als auch von anderen nicht vertrauen swürdigen Netzwerke n getrennt ist.	opensearch-in-vpc-only	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass sich Amazon OpenSearch Service-Domains innerhalb einer Amazon Virtual Private Cloud (Amazon VPC) befinden. Eine Amazon OpenSearc h Service-Domain innerhalb einer Amazon VPC ermöglicht die sichere Kommunikation zwischen Amazon OpenSearch Service und anderen Services innerhalb der Amazon VPC, ohne dass ein Internet-Gateway, ein NAT-Gerät oder eine VPN-Verbindung erforderlich ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
1.3.6	Speichern von Systemkomponenten, die Karteninh aberdaten beinhalten (z. B. eine Datenbank), in einer internen Netzwerkzone, die sowohl von der DMZ als auch von anderen nicht vertrauen swürdigen Netzwerke n getrennt ist.	rds-instance-public-access-überprüfen	Verwalten Sie den Zugriff auf Ressource n in der AWS Cloud, indem Sie sicherste llen, dass Amazon Relational Database Service (Amazon RDS) -Instance s nicht öffentlic h sind. Amazon-RDS-Datenbank-Instances können vertrauliche Informati onen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
1.3.6	Speichern von Systemkomponenten, die Karteninh aberdaten beinhalten (z. B. eine Datenbank), in einer internen Netzwerkzone, die sowohl von der DMZ als auch von anderen nicht vertrauen swürdigen Netzwerke n getrennt ist.	rds-snapshots-public-prohibited	Verwalten Sie den Zugriff auf Ressource n in der AWS Cloud, indem Sie sicherste llen, dass Amazon Relational Database Service (Amazon RDS) -Instance s nicht öffentlic h sind. Amazon-RDS-Datenbank-Instances können vertrauliche Informati onen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
1.3.6	Speichern von Systemkomponenten, die Karteninh aberdaten beinhalten (z. B. eine Datenbank), in einer internen Netzwerkzone, die sowohl von der DMZ als auch von anderen nicht vertrauen swürdigen Netzwerke n getrennt ist.	redshift-cluster-public-access-überprüfen	Verwalten Sie den Zugriff auf Ressource n in der AWS Cloud, indem Sie sicherste llen, dass Amazon Redshift Redshift-Cluster nicht öffentlic h sind. Amazon-Re dshift-Cluster können vertrauliche Informati onen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
1.3.6	Speichern von Systemkomponenten, die Karteninh aberdaten beinhalten (z. B. eine Datenbank), in einer internen Netzwerkzone, die sowohl von der DMZ als auch von anderen nicht vertrauen swürdigen Netzwerke n getrennt ist.	restricted-common-ports	Verwalten Sie den Zugriff auf Ressource n in der AWS Cloud, indem Sie sicherste llen, dass gemeinsam e Ports für Amazon Elastic Compute Cloud (Amazon EC2) -Sicherhe itsgruppen eingeschr ränkt sind. Wenn der Zugriff auf Ports nicht auf vertrauen swürdige Quellen beschränkt wird, kann dies zu Angriffen auf die Verfügbar keit, Integrität und Vertraulichkeit von Systemen führen. Mit dieser Regel können Sie optional die Parameter blockedPo rt1–blockedPort5 festlegen (Standard konfigurationen: 20, 21, 3389, 3306, 4333). Die tatsächli chen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
1.3.6	Speichern von Systemkomponenten, die Karteninh aberdaten beinhalten (z. B. eine Datenbank), in einer internen Netzwerkzone, die sowohl von der DMZ als auch von anderen nicht vertrauen swürdigen Netzwerke n getrennt ist.	s3- account-level-publ ic-access -Block-pe riodisch	Verwalten Sie den Zugriff auf Ressource n in der AWS Cloud, indem Sie sicherste llen, dass Amazon Simple Storage Service (Amazon S3) -Buckets nicht öffentlich zugänglic h sind. Diese Regel trägt dazu bei, sensible Daten vor unbefugten Remote-Benutzern zu schützen, indem sie den öffentlichen Zugriff verhinder t. Mit dieser Regel können Sie optional die Parameter ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) und restrictPublicBuck ets Parameter (Config Default: True) festlegen. Die tatsächlichen Werte müssen den Richtlini

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			en Ihrer Organisation entsprechen.
1.3.6	Speichern von Systemkomponenten, die Karteninh aberdaten beinhalten (z. B. eine Datenbank), in einer internen Netzwerkzone, die sowohl von der DMZ als auch von anderen nicht vertrauen swürdigen Netzwerke n getrennt ist.	s3 bucket-level-public-access - verboten	Verwalten Sie den Zugriff auf Ressource n in der AWS Cloud, indem Sie sicherste llen, dass Amazon Simple Storage Service (Amazon S3) -Buckets nicht öffentlich zugänglic h sind. Diese Regel trägt dazu bei, sensible Daten vor unbefugten Remote-Benutzern zu schützen, indem sie den öffentlichen Zugriff auf Bucket-Eb ene verhindert.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
1.3.6	Speichern von Systemkomponenten, die Karteninh aberdaten beinhalten (z. B. eine Datenbank), in einer internen Netzwerkzone, die sowohl von der DMZ als auch von anderen nicht vertrauen swürdigen Netzwerke n getrennt ist.	s-3 bucket-public-read -prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie nur autorisierten Benutzern, Prozessen und Geräten Zugriff auf Amazon Simple Storage Service (Amazon S3) - Buckets gewähren. Die Verwaltung des Zugriffs sollte mit der Klassifizierung der Daten übereinst immen.
1.3.6	Speichern von Systemkomponenten, die Karteninh aberdaten beinhalten (z. B. eine Datenbank), in einer internen Netzwerkzone, die sowohl von der DMZ als auch von anderen nicht vertrauen swürdigen Netzwerke n getrennt ist.	s3- bucket-public-writ e-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie nur autorisierten Benutzern, Prozessen und Geräten Zugriff auf Amazon Simple Storage Service (Amazon S3) - Buckets gewähren. Die Verwaltung des Zugriffs sollte mit der Klassifizierung der Daten übereinst immen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
1.3.6	Speichern von Systemkomponenten, die Karteninh aberdaten beinhalten (z. B. eine Datenbank), in einer internen Netzwerkzone, die sowohl von der DMZ als auch von anderen nicht vertrauen swürdigen Netzwerke n getrennt ist.	sagemaker-notebook -no-direct-Interne tzugang	Verwalten Sie den Zugriff auf Ressource n in der AWS Cloud, indem Sie sicherste llen, dass SageMaker Amazon-Notebooks keinen direkten Internetzugang zulassen. Indem Sie direkten Internetz ugang blockieren, vermeiden Sie, dass unbefugte Benutzer auf sensible Daten zugreifen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
1.3.6	Speichern von Systemkomponenten, die Karteninh aberdaten beinhalten (z. B. eine Datenbank), in einer internen Netzwerkzone, die sowohl von der DMZ als auch von anderen nicht vertrauen swürdigen Netzwerke n getrennt ist.	subnet-auto-assign-public-ip-deaktiviert	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon Virtual Private Cloud (VPC) -Subnetzen nicht automatisch eine öffentliche IP-Adress e zugewiesen wird. Amazon Elastic Compute Cloud (EC2) -Instances, die in Subnetzen gestartet werden, in denen dieses Attribut aktiviert ist, haben ihrer primären Netzwerkschnittste lle eine öffentliche IP-Adresse zugewiesen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
1.3.6	Speichern von Systemkomponenten, die Karteninh aberdaten beinhalten (z. B. eine Datenbank), in einer internen Netzwerkzone, die sowohl von der DMZ als auch von anderen nicht vertrauen swürdigen Netzwerke n getrennt ist.	vpc-default-security-group-geschlossen	Sicherheitsgruppen von Amazon Elastic Compute Cloud (Amazon EC2) können bei der Verwaltung des Netzwerkzugriffs helfen, indem sie eine statusbehaftete Filterung des ein- und ausgehenden Netzwerkverkehrs zu Ressourcen bereitstellen. AWS Die Beschränk ung des gesamten Datenverkehrs auf die Standardsicherheit sgruppe hilft dabei, den Fernzugriff auf Ihre Ressourcen einzuschränken. AWS

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
1.3.6	Speichern von Systemkomponenten, die Karteninh aberdaten beinhalten (z. B. eine Datenbank), in einer internen Netzwerkzone, die sowohl von der DMZ als auch von anderen nicht vertrauen swürdigen Netzwerke n getrennt ist.	vpc-sg-open-only-to-authorized-ports	Verwalten Sie den Zugriff auf Ressource n in der AWS Cloud, indem Sie sicherste llen, dass gemeinsam e Ports für Amazon Elastic Compute Cloud (Amazon EC2) -Sicherhe itsgruppen eingeschr ränkt sind. Wenn der Zugriff auf Ports nicht auf vertrauen swürdige Quellen beschränkt wird, kann dies zu Angriffen auf die Verfügbar keit, Integrität und Vertraulichkeit von Systemen führen. Durch die Beschränk ung des Zugriffs auf Ressourcen innerhalb einer Sicherhei tsgruppe aus dem Internet (0.0.0.0/0) kann der Fernzugriff auf interne Systeme gesteuert werden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
2.1	Ändern Sie immer die vom Herstelle r bereitgestellten Standardeinstellun gen und entfernen oder deaktivieren Sie unnötige Standardk onten, bevor Sie ein System im Netzwerk installie ren. Dies gilt für ALLE Standardkennwörter , einschließlich, aber nicht beschränk t auf solche, die von Betriebss ystemen, Software, die Sicherhei tsdienste bereitste llt, Anwendungs- und Systemkon ten, point-of-sale (POS-) Terminals, Zahlungsanwendunge n, Community-Strings des Simple Network Managemen t Protocol (SNMP) usw.) verwendet werden.	rds-cluster-default-admin-überprüfen	Da Standardb enutzernamen allgemein bekannt sind, kann eine Änderung der Standardbenutzerna men dazu beitragen , die Angriffsfläche für Ihre Datenbank-Cluster(s) in Amazon Relational Database Service (Amazon RDS) zu reduzieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
2.1	Ändern Sie immer die vom Herstelle r bereitgestellten Standardeinstellun gen und entfernen oder deaktivieren Sie unnötige Standardk onten, bevor Sie ein System im Netzwerk installie ren. Dies gilt für ALLE Standardkennwörter , einschließlich, aber nicht beschränk t auf Passwörter, die von Betriebss ystemen, Software zur Bereitstellung von Sicherheitsdienste n, Anwendungs- und Systemkon ten, point-of-sale (POS-) Terminals, Zahlungsanwendunge n, Community-Strings für Simple Network Management Protocol (SNMP) usw. verwendet werden.	rds-instance-default-admin-überprüfen	Da Standardb enutzernamen allgemein bekannt sind, kann eine Änderung der Standardbenutzerna men dazu beitragen , die Angriffsfläche für Ihre Datenbank-Instance(s) in Amazon Relational Database Service (Amazon RDS) zu reduzieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
2.1	Ändern Sie immer die vom Herstelle r bereitgestellten Standardeinstellun gen und entfernen oder deaktivieren Sie unnötige Standardk onten, bevor Sie ein System im Netzwerk installie ren. Dies gilt für ALLE Standardkennwörter , einschließlich, aber nicht beschränk t auf Passwörter, die von Betriebss ystemen, Software zur Bereitstellung von Sicherheitsdienste n, Anwendungs- und Systemkon ten, point-of-sale (POS-) Terminals, Zahlungsanwendunge n, Community-Strings für Simple Network Management Protocol (SNMP) usw. verwendet werden.	redshift-default-a dmin-check	Da Standardb enutzernamen allgemein bekannt sind, kann eine Änderung der Standardbenutzerna men dazu beitragen , die Angriffsfläche für Ihre Amazon-Redshift-Cluster zu reduzieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
2.1	Ändern Sie immer die vom Herstelle r bereitgestellten Standardeinstellun gen und entfernen oder deaktivieren Sie unnötige Standardk onten, bevor Sie ein System im Netzwerk installie ren. Dies gilt für ALLE Standardkennwörter , einschließlich, aber nicht beschränk t auf solche, die von Betriebss ystemen, Software, die Sicherhei tsdienste bereitste llt, Anwendungs- und Systemkonten, point-of-sale (POS-) Terminals, Zahlungsa nwendungen, Simple Network Managemen t Protocol (SNMP) - Community-Strings usw.) verwendet werden.	redshift-default-db-name-überprüfen	Standardnamen sind allgemein bekannt und sollten bei der Konfiguration geändert werden. Das Ändern des Standard-Datenbank namens Ihres Amazon Redshift Redshift-Clusters kann dazu beitragen, die Angriffsfläche für Ihren Redshift-Cluster zu reduzieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
2.1	Ändern Sie immer die vom Herstelle r bereitgestellten Standardeinstellun gen und entfernen oder deaktivieren Sie unnötige Standardk onten, bevor Sie ein System im Netzwerk installie ren. Dies gilt für ALLE Standardkennwörter , einschließlich, aber nicht beschränk t auf Passwörter, die von Betriebss ystemen, Software zur Bereitstellung von Sicherheitsdienste n, Anwendungs- und Systemkon ten, point-of-sale (POS-) Terminals, Zahlungsanwendunge n, Community-Strings für Simple Network Management Protocol (SNMP) usw. verwendet werden.	root-account-mfa-e nabled	Verwalten Sie den Zugriff auf Ressource n in der AWS Cloud, indem Sie sicherste llen, dass MFA für den Root-Benu tzer aktiviert ist. Der Stammbenu tzer ist der AWS-Konto-Benutzer mit den meisten Berechtigungen. MFA bietet eine weitere Schutzebene zusätzlic h zum Benutzern amen und Passwort. Indem Sie MFA für den Root-Benutzer vorschreiben, können Sie die Anzahl AWS-Konten kompromit tierter Benutzer reduzieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
2.1	Ändern Sie immer die vom Herstelle r bereitgestellten Standardeinstellun gen und entfernen oder deaktivieren Sie unnötige Standardk onten, bevor Sie ein System im Netzwerk installie ren. Dies gilt für ALLE Standardkennwörter , einschließlich, aber nicht beschränk t auf solche, die von Betriebss ystemen, Software zur Bereitstellung von Sicherheitsdienste n, Anwendungs- und Systemkon ten, point-of-sale (POS-) Terminals, Zahlungsanwendunge n, Community-Strings des Simple Network Management Protocol (SNMP) usw. verwendet werden.	vpc-default-security-group-geschlossen	Sicherheitsgruppen von Amazon Elastic Compute Cloud (Amazon EC2) können bei der Verwaltung des Netzwerkzugriffs helfen, indem sie eine statusbehaftete Filterung des ein- und ausgehenden Netzwerkverkehrs zu Ressourcen bereitstellen. AWS Die Beschränk ung des gesamten Datenverkehrs auf die Standardsicherheit sgruppe hilft dabei, den Fernzugriff auf Ihre Ressourcen einzuschränken. AWS

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
2.2	Entwickeln von Konfigurationsstandards für alle Systemkomponenten. Gewährleisten, dass diese Standards alle bekannten Sicherheitslücken adressieren und branchenweit akzeptierten Standards zur Systemstabilisierung entsprechen. Zu den Quellen branchenweit anerkannter Standards für die Systemhärtung können gehören, ohne darauf beschränkt zu sein: • Center for Internet Security (CIS) • International Organization for Standardization (ISO) • SysAdmin Audit Network Security (SANS) Institute • National Institute of Standards Technology (NIST).	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) Security Groups können bei der Verwaltung des Netzwerkzugriffs helfen, indem sie eine statusbehaftete Filterung von eingehendem und ausgehendem Netzwerkverkehr zu Ressourcen bereitstellen. AWS Wenn Sie eingehenden (oder entfernten) Datenverkehr von 0.0.0.0/0 bis Port 22 auf Ihren Ressourcen nicht zulassen, können Sie den Remote-Zugriff einschränken.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
2.2	Entwickeln von Konfigurationsstandards für alle Systemkomponenten. Gewährleisten, dass diese Standards alle bekannten Sicherheitslücken adressieren und branchenweit akzeptierten Standards zur Systemstabilisierung entsprechen. Zu den Quellen branchenweit anerkannter Standards für die Systemhärtung können gehören, ohne darauf beschränkt zu sein: • Center for Internet Security (CIS) • International Organization for Standardization (ISO) • SysAdmin Audit Network Security (SANS) Institute • National Institute of Standards Technology (NIST).	multi-region-cloudtrail-enabled	AWS CloudTrail zeichnet Aktionen und API-Aufrufe der AWS Management Console auf. Sie können feststellen, welche Benutzer und Konten angerufen wurden AWS, von welcher Quell-IP-Adresse aus die Anrufe getätigt wurden und wann die Anrufe erfolgten. CloudTrail übermittelt Protokolldateien aus allen AWS Regionen an Ihren S3-Bucket, wenn MULTI_REGION_CLOUD_TRAIL_ENABLED aktiviert ist. Außerdem wird beim AWS Start einer neuen Region derselbe Trail in der neuen Region erstellt. CloudTrail Dadurch erhalten Sie automatisch Protokolldateien mit API-Aktivitäten für die neue Region.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
2.2	Entwickeln von Konfigurationsstandards für alle Systemkomponenten. Gewährleisten, dass diese Standards alle bekannten Sicherheitslücken adressieren und branchenweit akzeptierten Standards zur Systemstabilisierung entsprechen. Zu den Quellen branchenweit anerkannter Standards für die Systemhärtung können gehören, ohne darauf beschränkt zu sein: • Center for Internet Security (CIS) • International Organization for Standardization (ISO) • SysAdmin Audit Network Security (SANS) Institute • National Institute of Standards Technology (NIST).	access-keys-rotated	Die Anmeldeinformationen für autorisierte Geräte, Benutzer und Prozesse werden geprüft, indem sichergestellt wird, dass die IAM-Zugriffsschlüssel entsprechend den Vorgaben der Unternehmensrichtlinie rotiert werden. Das regelmäßige Ändern der Zugriffsschlüssel ist eine bewährte Sicherheitsmethode. Es verkürzt den Zeitraum, in dem ein Zugriffsschlüssel aktiv ist, und reduziert die Auswirkungen auf das Unternehmen, wenn die Schlüssel kompromittiert werden. Diese Regel erfordert einen Wert für die Zugriffsschlüssel-Rotation (Standardkonfiguration: 90). Der tatsächliche Wert muss den Richtlini

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			en Ihrer Organisation entsprechen.
2.2	Entwickeln von Konfigurationsstandards für alle Systemkomponenten. Gewährleisten, dass diese Standards alle bekannten Sicherheitslücken adressieren und branchenweit akzeptierten Standards zur Systemstabilisierung entsprechen. Zu den Quellen branchenweit anerkannter Standards für die Systemhärtung können gehören, ohne darauf beschränkt zu sein: • Center for Internet Security (CIS) • International Organization for Standardization (ISO) • SysAdmin Audit Network Security (SANS) Institute • National Institute of Standards Technology (NIST).	account-part-of-organizations	Durch die zentrale Verwaltung AWS-Konten innerhalb von AWS Organizations wird sichergestellt, dass die Konten den Vorschriften entsprechen. Eine fehlende zentrale Kontoverwaltung kann zu inkonsistenten Kontokonfigurationen führen, wodurch Ressourcen und sensible Daten offengelegt werden können.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
2.2	Entwickeln von Konfigurationsstandards für alle Systemkomponenten. Gewährleisten, dass diese Standards alle bekannten Sicherheitslücken adressieren und branchenweit akzeptierten Standards zur Systemstabilisierung entsprechen. Zu den Quellen branchenweit anerkannter Standards für die Systemhärtung können gehören, ohne darauf beschränkt zu sein: • Center for Internet Security (CIS) • International Organization for Standardization (ISO) • SysAdmin Audit Network Security (SANS) Institute • National Institute of Standards Technology (NIST).	autoscaling-launch-config-public-ip ist deaktiviert	Wenn Sie Ihre Netzwerkschnittstellen mit einer öffentlichen IP-Adresse konfigurieren, sind die diesen Netzwerkschnittstellen zugehörigen Ressourcen über das Internet erreichbar. EC2 Ressourcen sollten nicht öffentlich zugänglich sein, da dies einen unbeabsichtigten Zugriff auf Ihre Anwendungen oder Server ermöglichen kann.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
2.2	Entwickeln von Konfigurationsstandards für alle Systemkomponenten. Gewährleisten, dass diese Standards alle bekannten Sicherheitslücken adressieren und branchenweit akzeptierten Standards zur Systemstabilisierung entsprechen. Zu den Quellen branchenweit anerkannter Standards für die Systemhärtung können gehören, ohne darauf beschränkt zu sein: • Center for Internet Security (CIS) • International Organization for Standardization (ISO) • SysAdmin Audit Network Security (SANS) Institute • National Institute of Standards Technology (NIST).	cloud-trail-cloud-watch-Logs aktiviert	Verwenden Sie Amazon CloudWatch , um Protokoll ereignisaktivitäten zentral zu sammeln und zu verwalten. Die Aufnahme von AWS CloudTrail Daten liefert Einzelheiten zu den API-Aufrufaktivitäten in Ihrem AWS-Konto.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
2.2	Entwickeln von Konfigurationsstandards für alle Systemkomponenten. Gewährleisten, dass diese Standards alle bekannten Sicherheitslücken adressieren und branchenweit akzeptierten Standards zur Systemstabilisierung entsprechen. Zu den Quellen branchenweit anerkannter Standards für die Systemhärtung können gehören, ohne darauf beschränkt zu sein: • Center for Internet Security (CIS) • International Organization for Standardization (ISO) • SysAdmin Audit Network Security (SANS) Institute • National Institute of Standards Technology (NIST).	cloud-trail-encryption-enabled	Da sensible Daten vorhanden sein können und um Daten im Ruhezustand zu schützen, sollten Sie sicherstellen, dass die Verschlüsselung für Ihre Trails aktiviert ist. AWS CloudTrail

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
2.2	Entwickeln von Konfigurationsstandards für alle Systemkomponenten. Gewährleisten, dass diese Standards alle bekannten Sicherheitslücken adressieren und branchenweit akzeptierten Standards zur Systemstabilisierung entsprechen. Zu den Quellen branchenweit anerkannter Standards für die Systemhärtung können gehören, ohne darauf beschränkt zu sein: • Center for Internet Security (CIS) • International Organization for Standardization (ISO) • SysAdmin Audit Network Security (SANS) Institute • National Institute of Standards Technology (NIST).	cloud-trail-log-file-Validierung aktiviert	Verwenden Sie die AWS CloudTrail Protokolldateivalidierung, um die Integrität von Protokollen zu überprüfen. CloudTrail Mithilfe der Protokolldateivalidierung kann festgestellt werden, ob eine Protokolldatei geändert oder gelöscht wurde oder ob sie nach der Übermittlung CloudTrail unverändert geblieben ist. Dieses Feature wurde mit dem Branchenstandard entsprechenden Algorithmen entwickelt: SHA-256 für die Hashfunktion und SHA-256 mit RSA für digitale Signaturen. Aus diesem Grund ist es rechnerisch unmöglich, CloudTrail Protokolldateien unbemerkt zu ändern, zu löschen oder zu fälschen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
2.2	Entwickeln von Konfigurationsstandards für alle Systemkomponenten. Gewährleisten, dass diese Standards alle bekannten Sicherheitslücken adressieren und branchenweit akzeptierten Standards zur Systemstabilisierung entsprechen. Zu den Quellen branchenweit anerkannter Standards für die Systemhärtung können gehören, ohne darauf beschränkt zu sein: • Center for Internet Security (CIS) • International Organization for Standardization (ISO) • SysAdmin Audit Network Security (SANS) Institute • National Institute of Standards Technology (NIST).	cloudtrail-s3-dataevents-enabled	Die Erfassung von Simple Storage Service (Amazon S3)-Datenereignissen unterstützt die Erkennung von ungewöhnlichen Aktivitäten. Zu den Details gehören AWS-Konto Informationen über den Zugriff auf einen Amazon S3 S3-Bucket, die IP-Adresse und die Uhrzeit des Ereignisses.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
2.2	Entwickeln von Konfigurationsstandards für alle Systemkomponenten. Gewährleisten, dass diese Standards alle bekannten Sicherheitslücken adressieren und branchenweit akzeptierten Standards zur Systemstabilisierung entsprechen. Zu den Quellen branchenweit anerkannter Standards für die Systemhärtung können gehören, ohne darauf beschränkt zu sein: • Center for Internet Security (CIS) • International Organization for Standardization (ISO) • SysAdmin Audit Network Security (SANS) Institute • National Institute of Standards Technology (NIST).	cmk-backing-key-rotation-aktiviert	Aktivieren Sie die Schlüsselrotation, um sicherzustellen, dass Schlüssel rotiert werden, nachdem sie das Ende ihrer Krypto-Periode erreicht haben.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
2.2	Entwickeln von Konfigurationsstandards für alle Systemkomponenten. Gewährleisten, dass diese Standards alle bekannten Sicherheitslücken adressieren und branchenweit akzeptierten Standards zur Systemstabilisierung entsprechen. Zu den Quellen branchenweit anerkannter Standards für die Systemhärtung können gehören, ohne darauf beschränkt zu sein: • Center for Internet Security (CIS) • International Organization for Standardization (ISO) • SysAdmin Audit Network Security (SANS) Institute • National Institute of Standards Technology (NIST).	ec-2 ebs-encryption-by-default	Zum Schutz von Daten im Ruhezustand müssen Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon Elastic Block Store (Amazon EBS)-Volumes aktiviert ist. Da sensible Daten in diesen Volumes gespeichert werden können, sollten Sie die Verschlüsselung von Daten im Ruhezustand aktivieren, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
2.2	Entwickeln von Konfigurationsstandards für alle Systemkomponenten. Gewährleisten, dass diese Standards alle bekannten Sicherheitslücken adressieren und branchenweit akzeptierten Standards zur Systemstabilisierung entsprechen. Zu den Quellen branchenweit anerkannter Standards für die Systemhärtung können gehören, ohne darauf beschränkt zu sein: • Center for Internet Security (CIS) • International Organization for Standardization (ISO) • SysAdmin Audit Network Security (SANS) Institute • National Institute of Standards Technology (NIST).	ec-2 instance-multiple-eni-check	Diese Regel prüft, ob Ihre Amazon Elastic Compute Cloud (Amazon EC2)-Instances mehrere haben ENIs. Wenn mehrere vorhanden sind, ENIs kann dies zu doppelt vernetzten Instanzen führen, d. h. zu Instanzen mit mehreren Subnetzen. Dies kann die Komplexität der Netzwerksicherheit erhöhen und unbeabsichtigte Netzwerkpfade und Zugriffe zur Folge haben.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
2.2	Entwickeln von Konfigurationsstandards für alle Systemkomponenten. Gewährleisten, dass diese Standards alle bekannten Sicherheitslücken adressieren und branchenweit akzeptierten Standards zur Systemstabilisierung entsprechen. Zu den Quellen branchenweit anerkannter Standards für die Systemhärtung gehören unter anderem: ‚Ä¢ Center for Internet Security (CIS) ‚International Organization for Standardization (ISO) ‚Ä¢ SysAdmin Audit Network Security (SANS) Institute ‚Ä¢ National Institute of Standards Technology (NIST).	ec2- -check managedinstance-association-compliance-status	Verwenden Sie AWS Systems Manager Associations, um bei der Inventarisierung von Softwareplattformen und Anwendungen innerhalb eines Unternehmens zu helfen. AWS Systems Manager weist Ihren verwalteten Instanzen einen Konfigurationsstatus zu und ermöglicht es Ihnen, Basiswerte für Betriebssystem-Patch-Levels, Softwareinstallationen, Anwendungskonfigurationen und andere Details zu Ihrer Umgebung festzulegen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
2.2	Entwickeln von Konfigurationsstandards für alle Systemkomponenten. Gewährleisten, dass diese Standards alle bekannten Sicherheitslücken adressieren und branchenweit akzeptierten Standards zur Systemstabilisierung entsprechen. Zu den Quellen branchenweit anerkannter Standards für die Systemhärtung können gehören, ohne darauf beschränkt zu sein: • Center for Internet Security (CIS) • International Organization for Standardization (ISO) • SysAdmin Audit Network Security (SANS) Institute • National Institute of Standards Technology (NIST).	ec2-check managedinstance-patch-compliance-status	Aktivieren Sie diese Regel, um bei der Identifizierung und Dokumentation von Sicherheitslücken in Amazon Elastic Compute Cloud (Amazon EC2) zu helfen. Die Regel prüft, ob die EC2 Amazon-Instance die Patch-Konformität im AWS Systems Manager gemäß den Richtlinien und Verfahren Ihrer Organisation einhält.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
2.2	Entwickeln von Konfigurationsstandards für alle Systemkomponenten. Gewährleisten, dass diese Standards alle bekannten Sicherheitslücken adressieren und branchenweit akzeptierten Standards zur Systemstabilisierung entsprechen. Zu den Quellen branchenweit anerkannter Standards für die Systemhärtung können gehören, ohne darauf beschränkt zu sein: • Center for Internet Security (CIS) • International Organization for Standardization (ISO) • SysAdmin Audit Network Security (SANS) Institute • National Institute of Standards Technology (NIST).	ec2- -einperiodisch security-group-attached-to	Diese Regel stellt sicher, dass die Sicherheitsgruppen an eine Amazon Elastic Compute Cloud (Amazon EC2) -Instance oder an eine ENI angehängt sind. Diese Regel unterstützt die Überwachung ungenutzter Sicherheitsgruppen im Bestand und die Verwaltung Ihrer Umgebung.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
2.2	Entwickeln von Konfigurationsstandards für alle Systemkomponenten. Gewährleisten, dass diese Standards alle bekannten Sicherheitslücken adressieren und branchenweit akzeptierten Standards zur Systemstabilisierung entsprechen. Zu den Quellen branchenweit anerkannter Standards für die Systemhärtung können gehören, ohne darauf beschränkt zu sein: • Center for Internet Security (CIS) • International Organization for Standardization (ISO) • SysAdmin Audit Network Security (SANS) Institute • National Institute of Standards Technology (NIST).	encrypted-volumes	Aktivieren Sie die Verschlüsselung für Ihre Amazon-Elastic-Block-Store-(Amazon-EBS-)Volumes, um eventuell vorhandene sensible Daten sowie Daten im Ruhezustand zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
2.2	Entwickeln von Konfigurationsstandards für alle Systemkomponenten. Gewährleisten, dass diese Standards alle bekannten Sicherheitslücken adressieren und branchenweit akzeptierten Standards zur Systemstabilisierung entsprechen. Zu den Quellen branchenweit anerkannter Standards für die Systemhärtung können gehören, ohne darauf beschränkt zu sein: • Center for Internet Security (CIS) • International Organization for Standardization (ISO) • SysAdmin Audit Network Security (SANS) Institute • National Institute of Standards Technology (NIST).	iam-no-inline-policy-überprüfen	Stellen Sie sicher, dass ein Benutzer, eine IAM-Rolle oder eine IAM-Gruppe (AWS Identity and Access Management) nicht über eine Inline-Richtlinie zur Zugriffskontrolle auf Systeme und Ressourcen verfügt. AWS empfiehlt, verwaltete Richtlinien anstelle von Inline-Richtlinien zu verwenden. Verwaltete Richtlinien ermöglichen Wiederverwendbarkeit, Versionsverwaltung, Rollback und Delegierung der Berechtigungsverwaltung.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
2.2	Entwickeln von Konfigurationsstandards für alle Systemkomponenten. Gewährleisten, dass diese Standards alle bekannten Sicherheitslücken adressieren und branchenweit akzeptierten Standards zur Systemstabilisierung entsprechen. Zu den Quellen branchenweit anerkannter Standards für die Systemhärtung können gehören, ohne darauf beschränkt zu sein: • Center for Internet Security (CIS) • International Organization for Standardization (ISO) • SysAdmin Audit Network Security (SANS) Institute • National Institute of Standards Technology (NIST).	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) kann Ihnen dabei helfen, die Prinzipien der geringsten Rechte und der Aufgabentrennung in Zugriffsberechtigungen und Autorisierungen zu integrieren und so zu verhindern, dass Richtlinien „Effect“: „Allow“ mit „Action“: „*“ anstelle von „Resource“: „*“ enthalten. Wenn Benutzern mehr Rechte eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und der Aufgabentrennung verstoßen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
2.2	Entwickeln von Konfigurationsstandards für alle Systemkomponenten. Gewährleisten, dass diese Standards alle bekannten Sicherheitslücken adressieren und branchenweit akzeptierten Standards zur Systemstabilisierung entsprechen. Zu den Quellen branchenweit anerkannter Standards für die Systemhärtung können gehören, ohne darauf beschränkt zu sein: • Center for Internet Security (CIS) • International Organization for Standardization (ISO) • SysAdmin Audit Network Security (SANS) Institute • National Institute of Standards Technology (NIST).	iam-root-access-key-überprüfen	Der Zugriff auf Systeme und Ressourcen kann gesteuert werden, indem überprüft wird, ob der Root-Benutzer keine Zugriffsschlüssel mit seiner AWS Identity and Access Management (IAM) -Rolle verknüpft hat. Stellen Sie sicher, dass die Root-Zugriffsschlüssel gelöscht werden. Erstellen und verwenden Sie stattdessen rollenbasierte Funktionen, AWS-Konten um das Prinzip der geringsten Funktionalität zu berücksichtigen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
2.2	Entwickeln von Konfigurationsstandards für alle Systemkomponenten. Gewährleisten, dass diese Standards alle bekannten Sicherheitslücken adressieren und branchenweit akzeptierten Standards zur Systemstabilisierung entsprechen. Zu den Quellen branchenweit anerkannter Standards für die Systemhärtung können gehören, ohne darauf beschränkt zu sein: • Center for Internet Security (CIS) • International Organization for Standardization (ISO) • SysAdmin Audit Network Security (SANS) Institute • National Institute of Standards Technology (NIST).	iam-user-group-membership-überprüfen	AWS Identity and Access Management (IAM) kann Ihnen helfen, Zugriffsberechtigungen und Autorisierungen einzuschränken, indem sichergestellt wird, dass Benutzer Mitglieder mindestens einer Gruppe sind. Wenn Benutzern mehr Berechtigungen eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und Aufgabentrennung verstoßen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
2.2	Entwickeln von Konfigurationsstandards für alle Systemkomponenten. Gewährleisten, dass diese Standards alle bekannten Sicherheitslücken adressieren und branchenweit akzeptierten Standards zur Systemstabilisierung entsprechen. Zu den Quellen branchenweit anerkannter Standards für die Systemhärtung können gehören, ohne darauf beschränkt zu sein: • Center for Internet Security (CIS) • International Organization for Standardization (ISO) • SysAdmin Audit Network Security (SANS) Institute • National Institute of Standards Technology (NIST).	iam-user-no-policies-überprüfen	Diese Regel stellt sicher, dass AWS Identity and Access Management (IAM) -Richtlinien nur Gruppen oder Rollen zugewiesen werden, um den Zugriff auf Systeme und Ressourcen zu kontrollieren. Die Zuweisung von Berechtigungen auf Gruppen- oder Rollenebene trägt dazu bei, die Wahrscheinlichkeit zu verringern, dass eine Identität übermäßige Berechtigungen erhält oder beibehält.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
2.2	Entwickeln von Konfigurationsstandards für alle Systemkomponenten. Gewährleisten, dass diese Standards alle bekannten Sicherheitslücken adressieren und branchenweit akzeptierten Standards zur Systemstabilisierung entsprechen. Zu den Quellen branchenweit anerkannter Standards für die Systemhärtung können gehören, ohne darauf beschränkt zu sein: • Center for Internet Security (CIS) • International Organization for Standardization (ISO) • SysAdmin Audit Network Security (SANS) Institute • National Institute of Standards Technology (NIST).	iam-user-unused-credentials-überprüfen	AWS Identity and Access Management (IAM) kann Ihnen bei Zugriffsberechtigungen und Autorisierungen helfen, indem es nach IAM-Passwörtern und Zugriffsschlüsseln sucht, die für einen bestimmten Zeitraum nicht verwendet wurden. Wenn ungenutzte Anmeldeinformationen identifiziert werden, müssen Sie sie deaktivieren und/oder entfernen, da dies gegen das Prinzip der geringsten Berechtigung verstoßen könnte. Für diese Regel müssen Sie einen Wert für das maxCredentialUsage Alter festlegen (Standardkonfiguration: 90). Der tatsächliche Wert muss den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
2.2	Entwickeln von Konfigurationsstandards für alle Systemkomponenten. Gewährleisten, dass diese Standards alle bekannten Sicherheitslücken adressieren und branchenweit akzeptierten Standards zur Systemstabilisierung entsprechen. Zu den Quellen branchenweit anerkannter Standards für die Systemhärtung können gehören, ohne darauf beschränkt zu sein: • Center for Internet Security (CIS) • International Organization for Standardization (ISO) • SysAdmin Audit Network Security (SANS) Institute • National Institute of Standards Technology (NIST).	mfa-enabled-for-iam-Konsolenzugriff	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass MFA für alle AWS Identity and Access Management (IAM) -Benutzer aktiviert ist, die über ein Konsolenkennwort verfügen. MFA bietet eine weitere Schutzebene zusätzlich zum Benutzernamen und Passwort. Indem Sie MFA für Benutzer vorschreiben, können Sie Fälle kompromittierter Konten reduzieren und verhindern, dass unbefugte Benutzer auf vertrauliche Daten zugreifen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
2.2	Entwickeln von Konfigurationsstandards für alle Systemkomponenten. Gewährleisten, dass diese Standards alle bekannten Sicherheitslücken adressieren und branchenweit akzeptierten Standards zur Systemstabilisierung entsprechen. Zu den Quellen branchenweit anerkannter Standards für die Systemhärtung können gehören, ohne darauf beschränkt zu sein: • Center for Internet Security (CIS) • International Organization for Standardization (ISO) • SysAdmin Audit Network Security (SANS) Institute • National Institute of Standards Technology (NIST).	restricted-common-ports	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass gemeinsame Ports für Amazon Elastic Compute Cloud (Amazon EC2) -Sicherheitsgruppen eingeschränkt sind. Wenn der Zugriff auf Ports nicht auf vertrauenswürdige Quellen beschränkt wird, kann dies zu Angriffen auf die Verfügbarkeit, Integrität und Vertraulichkeit von Systemen führen. Mit dieser Regel können Sie optional die Parameter blockedPort1–blockedPort5 festlegen (Standardkonfigurationen: 20, 21, 3389, 3306, 4333). Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
2.2	Entwickeln von Konfigurationsstandards für alle Systemkomponenten. Gewährleisten, dass diese Standards alle bekannten Sicherheitslücken adressieren und branchenweit akzeptierten Standards zur Systemstabilisierung entsprechen. Zu den Quellen branchenweit anerkannter Standards für die Systemhärtung können gehören, ohne darauf beschränkt zu sein: • Center for Internet Security (CIS) • International Organization for Standardization (ISO) • SysAdmin Audit Network Security (SANS) Institute • National Institute of Standards Technology (NIST).	root-account-hardware-mfa-aktiviert	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Hardware-MFA für den Root-Benutzer aktiviert ist. Der Stammbenutzer ist der AWS-Konto-Benutzer mit den meisten Berechtigungen. MFA bietet eine weitere Schutzebene zusätzlich zum Benutzernamen und Passwort. Indem Sie MFA für den Root-Benutzer vorschreiben, können Sie die Anzahl AWS-Konten kompromittierter Benutzer reduzieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
2.2	Entwickeln von Konfigurationsstandards für alle Systemkomponenten. Gewährleisten, dass diese Standards alle bekannten Sicherheitslücken adressieren und branchenweit akzeptierten Standards zur Systemstabilisierung entsprechen. Zu den Quellen branchenweit anerkannter Standards für die Systemhärtung können gehören, ohne darauf beschränkt zu sein: • Center for Internet Security (CIS) • International Organization for Standardization (ISO) • SysAdmin Audit Network Security (SANS) Institute • National Institute of Standards Technology (NIST).	root-account-mfa-enabled	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass MFA für den Root-Benutzer aktiviert ist. Der Stammbenutzer ist der AWS-Konto-Benutzer mit den meisten Berechtigungen. MFA bietet eine weitere Schutzebene zusätzlich zum Benutzernamen und Passwort. Indem Sie MFA für den Root-Benutzer vorschreiben, können Sie die Anzahl AWS-Konten kompromittierter Benutzer reduzieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
2.2	Entwickeln von Konfigurationsstandards für alle Systemkomponenten. Gewährleisten, dass diese Standards alle bekannten Sicherheitslücken adressieren und branchenweit akzeptierten Standards zur Systemstabilisierung entsprechen. Zu den Quellen branchenweit anerkannter Standards für die Systemhärtung können gehören, ohne darauf beschränkt zu sein: • Center for Internet Security (CIS) • International Organization for Standardization (ISO) • SysAdmin Audit Network Security (SANS) Institute • National Institute of Standards Technology (NIST).	s3- -Block-periodisch account-level-public-access	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Simple Storage Service (Amazon S3) -Buckets nicht öffentlich zugänglich sind. Diese Regel trägt dazu bei, sensible Daten vor unbefugten Remote-Benutzern zu schützen, indem sie den öffentlichen Zugriff verhindert. Mit dieser Regel können Sie optional die Parameter ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) und restrictPublicBuckets Parameter (Config Default: True) festlegen. Die tatsächlichen Werte müssen den Richtlini

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			en Ihrer Organisation entsprechen.
2.2	Entwickeln von Konfigurationsstandards für alle Systemkomponenten. Gewährleisten, dass diese Standards alle bekannten Sicherheitslücken adressieren und branchenweit akzeptierten Standards zur Systemstabilisierung entsprechen. Zu den Quellen branchenweit anerkannter Standards für die Systemhärtung können gehören, ohne darauf beschränkt zu sein: • Center for Internet Security (CIS) • International Organization for Standardization (ISO) • SysAdmin Audit Network Security (SANS) Institute • National Institute of Standards Technology (NIST).	s3- bucket-logging-enabled	Die Amazon Simple Storage Service (Amazon S3)-Serverzugriffsprotokollierung bietet eine Methode zur Überwachung des Netzwerks im Hinblick auf potenzielle Cybersicherheitsereignisse. Die Ereignisse werden überwacht, indem detaillierte Aufzeichnungen über die Anfragen erfasst werden, die an einen Amazon-S3-Bucket gestellt wurden. Jeder Zugriffsprotokolleintrag enthält Details zu einer einzelnen Zugriffsanfrage. Zu den Details gehören Anforderer, Bucket-Name, Anforderungszeit, Anforderungsaktion, Antwortstatus und Fehlercode, falls relevant.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
2.2	Entwickeln von Konfigurationsstandards für alle Systemkomponenten. Gewährleisten, dass diese Standards alle bekannten Sicherheitslücken adressieren und branchenweit akzeptierten Standards zur Systemstabilisierung entsprechen. Zu den Quellen branchenweit anerkannter Standards für die Systemhärtung können gehören, ohne darauf beschränkt zu sein: • Center for Internet Security (CIS) • International Organization for Standardization (ISO) • SysAdmin Audit Network Security (SANS) Institute • National Institute of Standards Technology (NIST).	s3- bucket-public-read-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie nur autorisierten Benutzern, Prozessen und Geräten Zugriff auf Amazon Simple Storage Service (Amazon S3) - Buckets gewähren. Die Verwaltung des Zugriffs sollte mit der Klassifizierung der Daten übereinstimmen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
2.2	Entwickeln von Konfigurationsstandards für alle Systemkomponenten. Gewährleisten, dass diese Standards alle bekannten Sicherheitslücken adressieren und branchenweit akzeptierten Standards zur Systemstabilisierung entsprechen. Zu den Quellen branchenweit anerkannter Standards für die Systemhärtung können gehören, ohne darauf beschränkt zu sein: • Center for Internet Security (CIS) • International Organization for Standardization (ISO) • SysAdmin Audit Network Security (SANS) Institute • National Institute of Standards Technology (NIST).	s3- bucket-public-write-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie nur autorisierten Benutzern, Prozessen und Geräten Zugriff auf Amazon Simple Storage Service (Amazon S3) - Buckets gewähren. Die Verwaltung des Zugriffs sollte mit der Klassifizierung der Daten übereinstimmen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
2.2	Entwickeln von Konfigurationsstandards für alle Systemkomponenten. Gewährleisten, dass diese Standards alle bekannten Sicherheitslücken adressieren und branchenweit akzeptierten Standards zur Systemstabilisierung entsprechen. Zu den Quellen branchenweit anerkannter Standards für die Systemhärtung können gehören, ohne darauf beschränkt zu sein: „Center for Internet Security (CIS)“, „International Organization for Standardization (ISO)“, „ SysAdmin Audit Network Security (SANS) Institute“, „National Institute of Standards Technology (NIST)“.	s3- bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) unterstützt die Aufrechterhaltung einer angemessenen Kapazität und Verfügbarkeit. CRR ermöglicht das automatische, asynchrone Kopieren von Objekten in Amazon S3 Buckets, um die Datenverfügbarkeit sicherzustellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
2.2	Entwickeln von Konfigurationsstandards für alle Systemkomponenten. Gewährleisten, dass diese Standards alle bekannten Sicherheitslücken adressieren und branchenweit akzeptierten Standards zur Systemstabilisierung entsprechen. Zu den Quellen branchenweit anerkannter Standards für die Systemhärtung können gehören, ohne darauf beschränkt zu sein: • Center for Internet Security (CIS) • International Organization for Standardization (ISO) • SysAdmin Audit Network Security (SANS) Institute • National Institute of Standards Technology (NIST).	s3-fähig bucket-server-side-encryption	Zum Schutz von Daten im Ruhezustand müssen Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon Simple Storage Service (Amazon S3)-Buckets aktiviert ist. Da sensible Daten in Amazon S3 Buckets gespeichert werden können, sollten Sie die Verschlüsselung aktivieren, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
2.2	Entwickeln von Konfigurationsstandards für alle Systemkomponenten. Gewährleisten, dass diese Standards alle bekannten Sicherheitslücken adressieren und branchenweit akzeptierten Standards zur Systemstabilisierung entsprechen. Zu den Quellen branchenweit anerkannter Standards für die Systemhärtung können gehören, ohne darauf beschränkt zu sein: • Center for Internet Security (CIS) • International Organization for Standardization (ISO) • SysAdmin Audit Network Security (SANS) Institute • National Institute of Standards Technology (NIST).	s3- bucket-ssl-requests-only	Um Daten während der Übertragung zu schützen, stellen Sie sicher, dass Ihre Amazon Simple Storage Service (Amazon S3)-Buckets Anfragen zur Verwendung von Secure Socket Layer (SSL)-Buckets erfordern. Da sensible Daten vorhanden sein können, sollten Sie die Verschlüsselung bei der Übertragung aktivieren, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
2.2	Entwickeln von Konfigurationsstandards für alle Systemkomponenten. Gewährleisten, dass diese Standards alle bekannten Sicherheitslücken adressieren und branchenweit akzeptierten Standards zur Systemstabilisierung entsprechen. Zu den Quellen branchenweit anerkannter Standards für die Systemhärtung können gehören, ohne darauf beschränkt zu sein: • Center for Internet Security (CIS) • International Organization for Standardization (ISO) • SysAdmin Audit Network Security (SANS) Institute • National Institute of Standards Technology (NIST).	vpc-default-security-group-geschlossen	Sicherheitsgruppen von Amazon Elastic Compute Cloud (Amazon EC2) können bei der Verwaltung des Netzwerkzugriffs helfen, indem sie eine statusbehaftete Filterung des ein- und ausgehenden Netzwerkverkehrs zu Ressourcen bereitstellen. AWS Die Beschränkung des gesamten Datenverkehrs auf die Standardsicherheitsgruppe hilft dabei, den Fernzugriff auf Ihre Ressourcen einzuschränken. AWS

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
2.2	Entwickeln von Konfigurationsstandards für alle Systemkomponenten. Gewährleisten, dass diese Standards alle bekannten Sicherheitslücken adressieren und branchenweit akzeptierten Standards zur Systemstabilisierung entsprechen. Zu den Quellen branchenweit anerkannter Standards für die Systemhärtung können gehören, ohne darauf beschränkt zu sein: • Center for Internet Security (CIS) • International Organization for Standardization (ISO) • SysAdmin Audit Network Security (SANS) Institute • National Institute of Standards Technology (NIST).	vpc-flow-logs-enabled	VPC-Flow-Protokolle erfassen detaillierte Informationsdatensätze über den IP-Datenverkehr, der zu und von Netzwerkschnittstellen in Ihrer Amazon Virtual Private Cloud (Amazon VPC) fließt. Standardmäßig enthalten Flow-Protokolldatensätze Werte für die verschiedenen Komponenten des IP-Flows, einschließlich Quelle, Ziel und Protokoll.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
2.2.2	Aktivieren Sie nur die Dienste, Protokolle, Daemons usw., die für die Funktion des Systems erforderlich sind.	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) Security Groups können bei der Verwaltung des Netzwerkzugriffs helfen, indem sie eine statusbeh aftete Filterung von eingehendem und ausgehendem Netzwerkverkehr zu Ressourcen bereitste llen. AWS Wenn Sie eingehenden (oder entfernten) Datenverk ehr von 0.0.0.0/0 bis Port 22 auf Ihren Ressourcen nicht zulassen, können Sie den Remote-Zugriff einschränken.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
2.2.2	Aktivieren Sie nur die Dienste, Protokolle, Daemons usw., die für die Funktion des Systems erforderlich sind.	autoscaling-launch-config-public-ip-deaktiviert	Wenn Sie Ihre Netzwerkschnittstellen mit einer öffentlichen IP-Adresse konfigurieren, sind die diesen Netzwerkschnittstellen zugehörigen Ressourcen über das Internet erreichbar. EC2 Ressourcen sollten nicht öffentlich zugänglich sein, da dies einen unbeabsichtigten Zugriff auf Ihre Anwendungen oder Server ermöglichen kann.
2.2.2	Aktivieren Sie nur die Dienste, Protokolle, Daemons usw., die für die Funktion des Systems erforderlich sind.	dms-replication-not-public	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass auf DMS-Replikationsinstanzen nicht öffentlich zugegriffen werden kann. DMS-Replikations-Instances können vertrauliche Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
2.2.2	Aktivieren Sie nur die Dienste, Protokolle, Daemons usw., die für die Funktion des Systems erforderlich sind.	ebs-snapshot-public-restorable-überprüfen	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass EBS-Snapshots nicht öffentlich wiederher stellbar sind. EBS-Volume-Snapsho ts können vertrauli che Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.
2.2.2	Aktivieren Sie nur die Dienste, Protokolle, Daemons usw., die für die Funktion des Systems erforderlich sind.	ec-2 instance-no-public-ip	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon Elastic Compute Cloud (Amazon EC2) - Instances nicht öffentlich zugänglich sind. EC2 Amazon-Instances können vertrauliche Informati onen enthalten, und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
2.2.2	Aktivieren Sie nur die Dienste, Protokolle, Daemons usw., die für die Funktion des Systems erforderlich sind.	emr-master-no-public-ip	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon EMR-Cluster-Masterknoten nicht öffentlich zugänglich sind. Amazon-EMR-Cluster-Hauptknoten können vertrauliche Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
2.2.2	Aktivieren Sie nur die Dienste, Protokolle, Daemons usw., die für die Funktion des Systems erforderlich sind.	ec-2 instances-in-vpc	Stellen Sie Amazon Elastic Compute Cloud (Amazon EC2) -Instances innerhalb einer Amazon Virtual Private Cloud (Amazon VPC) bereit, um eine sichere Kommunika tion zwischen einer Instance und anderen Services innerhalb der Amazon VPC zu ermöglichen, ohne dass ein Internet-Gateway, ein NAT-Gerät oder eine VPN-Verbindung erforderlich ist. Der gesamte Datenverk ehr bleibt sicher in der AWS Cloud. Domains, die sich innerhalb einer VPC befinden, verfügen aufgrund ihrer logischen Isolierun g im Vergleich zu Domains mit öffentlic hen Endpunkten über eine zusätzlic he Sicherheitsebene. Weisen Sie EC2

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			Amazon-Instances einer Amazon-VPC zu, um den Zugriff ordnungsgemäß zu verwalten.
2.2.2	Aktivieren Sie nur die Dienste, Protokolle, Daemons usw., die für die Funktion des Systems erforderlich sind.	lambda-function-public-access-verboten	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass AWS Lambda-Funktionen nicht öffentlich zugänglich sind. Der öffentliche Zugriff kann möglicherweise die Verfügbarkeit von Ressourcen beeinträchtigen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
2.2.2	Aktivieren Sie nur die Dienste, Protokolle, Daemons usw., die für die Funktion des Systems erforderlich sind.	lambda-inside-vpc	Stellen Sie AWS Lambda-Funktionen in einer Amazon Virtual Private Cloud (Amazon VPC) bereit, um eine sichere Kommunika tion zwischen einer Funktion und anderen Diensten innerhalb der Amazon VPC zu gewährleisten. Bei dieser Konfiguration sind kein Internet-Gateway, kein NAT-Gerät und keine VPN-Verbindung erforderlich. Der gesamte Datenverk ehr bleibt sicher in der Cloud. AWS Domains, die sich innerhalb einer VPC befinden, verfügen aufgrund ihrer logischen Isolierun g im Vergleich zu Domains mit öffentlic hen Endpunkten über eine zusätzliche Sicherheitsebene. Um den Zugriff ordnungsg emäß zu verwalten,

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			sollten AWS Lambda-Funktionen einer VPC zugewiesen werden.
2.2.2	Aktivieren Sie nur die Dienste, Protokolle, Daemons usw., die für die Funktion des Systems erforderlich sind.	no-unrestricted-route-to-igw	Stellen Sie sicher, dass EC2 Amazon-Routentabellen keine uneingeschränkten Routen zu einem Internet-Gateway enthalten. Durch das Entfernen oder Beschränken des Internetzugangs für Workloads innerhalb von Amazon VPCs können unbeabsichtigte Zugriffe in Ihrer Umgebung reduziert werden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
2.2.2	Aktivieren Sie nur die Dienste, Protokolle, Daemons usw., die für die Funktion des Systems erforderlich sind.	rds-instance-public-access-überprüfen	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Relational Database Service (Amazon RDS) -Instances nicht öffentlich sind. Amazon-RDS-Datenbank-Instances können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
2.2.2	Aktivieren Sie nur die Dienste, Protokolle, Daemons usw., die für die Funktion des Systems erforderlich sind.	rds-snapshots-public-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Relational Database Service (Amazon RDS) -Instances nicht öffentlich sind. Amazon-RDS-Datenbank-Instances können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
2.2.2	Aktivieren Sie nur die Dienste, Protokolle, Daemons usw., die für die Funktion des Systems erforderlich sind.	redshift-cluster-public-access-überprüfen	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Redshift Redshift-Cluster nicht öffentlich sind. Amazon-Redshift-Cluster können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
2.2.2	Aktivieren Sie nur die Dienste, Protokolle, Daemons usw., die für die Funktion des Systems erforderlich sind.	restricted-common-ports	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass gemeinsame Ports für Amazon Elastic Compute Cloud (Amazon EC2) -Sicherheitsgruppen eingeschränkt sind. Wenn der Zugriff auf Ports nicht auf vertrauenswürdige Quellen beschränkt wird, kann dies zu Angriffen auf die Verfügbarkeit, Integrität und Vertraulichkeit von Systemen führen. Mit dieser Regel können Sie optional die Parameter blockedPort1–blockedPort5 festlegen (Standardkonfigurationen: 20, 21, 3389, 3306, 4333). Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
2.2.2	Aktivieren Sie nur die Dienste, Protokolle, Daemons usw., die für die Funktion des Systems erforderlich sind.	s3- account-level-public-access -Block-periodisch	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Simple Storage Service (Amazon S3) -Buckets nicht öffentlich zugänglich sind. Diese Regel trägt dazu bei, sensible Daten vor unbefugten Remote-Benutzern zu schützen, indem sie den öffentlichen Zugriff verhindert. Mit dieser Regel können Sie optional die Parameter ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) und restrictPublicBuckets Parameter (Config Default: True) festlegen. Die tatsächlichen Werte müssen den Richtlini

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			en Ihrer Organisation entsprechen.
2.2.2	Aktivieren Sie nur die Dienste, Protokolle, Daemons usw., die für die Funktion des Systems erforderlich sind.	s3 bucket-level-public-access - verboten	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Simple Storage Service (Amazon S3) -Buckets nicht öffentlich zugänglich sind. Diese Regel trägt dazu bei, sensible Daten vor unbefugten Remote-Benutzern zu schützen, indem sie den öffentlichen Zugriff auf Bucket-Ebene verhindert.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
2.2.2	Aktivieren Sie nur die Dienste, Protokolle, Daemons usw., die für die Funktion des Systems erforderlich sind.	s-3 bucket-public-read-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie nur autorisierten Benutzern, Prozessen und Geräten Zugriff auf Amazon Simple Storage Service (Amazon S3) - Buckets gewähren. Die Verwaltung des Zugriffs sollte mit der Klassifizierung der Daten übereinst immen.
2.2.2	Aktivieren Sie nur die Dienste, Protokolle, Daemons usw., die für die Funktion des Systems erforderlich sind.	s3- bucket-public-write-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie nur autorisierten Benutzern, Prozessen und Geräten Zugriff auf Amazon Simple Storage Service (Amazon S3) - Buckets gewähren. Die Verwaltung des Zugriffs sollte mit der Klassifizierung der Daten übereinst immen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
2.2.2	Aktivieren Sie nur die Dienste, Protokolle, Daemons usw., die für die Funktion des Systems erforderlich sind.	sagemaker-notebook-no-direct-Internetzugang	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass SageMaker Amazon-Notebooks keinen direkten Internetzugang zulassen. Indem Sie direkten Internetzugang blockieren, vermeiden Sie, dass unbefugte Benutzer auf sensible Daten zugreifen.
2.2.2	Aktivieren Sie nur die Dienste, Protokolle, Daemons usw., die für die Funktion des Systems erforderlich sind.	ssm-document-not-public	Stellen Sie sicher, dass AWS Systems Manager (SSM) - Dokumente nicht öffentlich sind, da dies einen unbeabsichtigten Zugriff auf Ihre SSM-Dokumente ermöglichen kann. Ein öffentliches SSM-Dokument kann Informationen über Ihr Konto, Ihre Ressourcen und internen Prozesse preisgeben.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
2.2.2	Aktivieren Sie nur die Dienste, Protokolle, Daemons usw., die für die Funktion des Systems erforderlich sind.	subnet-auto-assign-public-ip-deaktiviert	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon Virtual Private Cloud (VPC) -Subnetzen nicht automatisch eine öffentliche IP-Adresse zugewiesen wird. Amazon Elastic Compute Cloud (EC2) -Instances, die in Subnetzen gestartet werden, in denen dieses Attribut aktiviert ist, haben ihrer primären Netzwerkschnittstelle eine öffentliche IP-Adresse zugewiesen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
2.2.2	Aktivieren Sie nur die Dienste, Protokolle, Daemons usw., die für die Funktion des Systems erforderlich sind.	vpc-default-security-group-geschlossen	Sicherheitsgruppen von Amazon Elastic Compute Cloud (Amazon EC2) können bei der Verwaltung des Netzwerkzugriffs helfen, indem sie eine statusbehaftete Filterung des ein- und ausgehenden Netzwerkverkehrs zu Ressourcen bereitstellen. AWS Die Beschränk ung des gesamten Datenverkehrs auf die Standardsicherheit sgruppe hilft dabei, den Fernzugriff auf Ihre Ressourcen einzuschränken. AWS

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
2.2.2	Aktivieren Sie nur die Dienste, Protokolle, Daemons usw., die für die Funktion des Systems erforderlich sind.	vpc-sg-open-only-to-authorized-ports	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass gemeinsame Ports für Amazon Elastic Compute Cloud (Amazon EC2) -Sicherheitsgruppen eingeschränkt sind. Wenn der Zugriff auf Ports nicht auf vertrauenswürdige Quellen beschränkt wird, kann dies zu Angriffen auf die Verfügbarkeit, Integrität und Vertraulichkeit von Systemen führen. Durch die Beschränkung des Zugriffs auf Ressourcen innerhalb einer Sicherheitsgruppe aus dem Internet (0.0.0.0/0) kann der Fernzugriff auf interne Systeme gesteuert werden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
2.2.3	Implementieren Sie zusätzliche Sicherheitsfunktionen für alle erforderlichen Dienste, Protokolle oder Daemons, die als unsicher gelten.	alb-desync-mode-check	Um Anwendungen vor HTTP-Desync-Schwachstellen zu schützen, stellen Sie sicher, dass der HTTP-Desync-Mitigationsmodus auf Ihren Anwendungs-Loadbalancern aktiviert ist. Probleme mit HTTP-Desync können zum Schmuggel von Anfragen führen und Ihre Anwendungen anfällig für Queues- oder Cache-Poisoning machen. Die desynchronen Mitigationsmodi lauten „Überwachen“, „Defensiv“ und „Am strengsten“. Defensive ist der standardmäßige Modus.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
2.3	Verschlüsseln Sie alle administrativen Zugriffe außerhalb der Konsole mithilfe starker Kryptografie.	alb-http-to-https-Umleitungsprüfung	Um Daten während der Übertragung zu schützen, stellen Sie sicher, dass Ihr Application Load Balancer unverschlüsselte HTTP-Anfragen automatisch an HTTPS umleitet. Da sensible Daten vorhanden sein können, sollten Sie die Verschlüsselung bei der Übertragung aktivieren, um diese Daten zu schützen.
2.3	Verschlüsseln Sie alle administrativen Zugriffe außerhalb der Konsole mithilfe starker Kryptografie.	api-gw-ssl-enabled	Stellen Sie sicher, dass die REST-API-Stufen von Amazon API Gateway mit SSL-Zertifikaten konfiguriert sind, damit Backend-Systeme überprüfen können, ob Anforderungen von API Gateway stammen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
2.3	Verschlüsseln Sie alle administrativen Zugriffe außerhalb der Konsole mithilfe starker Kryptografie.	elb-tls-https-listeners-nur	Stellen Sie sicher, dass Ihre Elastic Load Balancer (ELBs) mit SSL- oder HTTPS-Listenern konfiguriert sind. Um eventuell vorhanden e sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.
2.3	Verschlüsseln Sie alle administrativen Zugriffe außerhalb der Konsole mithilfe starker Kryptografie.	opensearch-https-required	Da sensible Daten existieren können und um Daten während der Übertragung zu schützen, sollten Sie sicherstellen, dass HTTPS für Verbindungen zu Ihren Amazon OpenSearch Service-Domains aktiviert ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
2.3	Verschlüsseln Sie alle administrativen Zugriffe außerhalb der Konsole mithilfe starker Kryptografie.	redshift-require-tls-ssl	Stellen Sie sicher, dass Ihre Amazon-Redshift-Cluster eine TLS/SSL-Verschlüsselung erfordern, um eine Verbindung zu SQL-Clients herzustellen. Da sensible Daten vorhanden sein können, sollten Sie die Verschlüsselung bei der Übertragung aktivieren, um diese Daten zu schützen.
2.4	Verwalten einer Bestandsaufnahme der Systemkomponenten, die im Bereich von PCI DSS liegen.	ec2- security-group-attached-to -eni-periodisch	Diese Regel stellt sicher, dass die Sicherheitsgruppen an eine Amazon Elastic Compute Cloud (Amazon EC2) -Instance oder an eine ENI angehängt sind. Diese Regel unterstützt die Überwachung ungenutzter Sicherheitsgruppen im Bestand und die Verwaltung Ihrer Umgebung.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
2.4	Verwalten einer Bestandsaufnahme der Systemkom ponenten, die im Bereich von PCI DSS liegen.	eip-attached	Diese Regel stellt sicher, dass Elastic, die einer Amazon Virtual Private Cloud (Amazon VPC) IPs zugewiesen sind, an Amazon Elastic Compute Cloud (Amazon EC2) - Instances oder verwendete Elastic Network Interface s angehängt sind. Diese Regel hilft bei der Überwachu ng ungenutzter Inhalte EIPs in Ihrer Umgebung.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
2.4	Verwalten einer Bestandsaufnahme der Systemkom ponenten, die im Bereich von PCI DSS liegen.	ec2-manager instance-managed-by-systems	Eine Bestandsa ufnahme der Softwareplattforme n und Anwendung en innerhalb des Unternehmens ist möglich, indem Amazon Elastic Compute Cloud (Amazon EC2) - Instances mit AWS Systems Manager verwaltet werden. Verwenden Sie AWS Systems Manager, um detaillierte Systemkonfiguratio nen, Betriebssystem-Patch-Levels, Namen und Typ der Dienste, Softwareinstallati onen, Anwendung sname, Herausgeb er und Version sowie andere Details zu Ihrer Umgebung bereitzustellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
2.4	Verwalten einer Bestandsaufnahme der Systemkom ponenten, die im Bereich von PCI DSS liegen.	vpc-network-acl-un used-überprüfen	Diese Regel stellt sicher, dass Amazon Virtual Private Cloud (VPC)-Netzwerkzugr iffskontrolllisten verwendet werden. Die Überwachu ng ungenutzter Netzwerk-Zugriffsk ontrolllisten kann zu einer genauen Inventarisierung und Verwaltung Ihrer Umgebung beitragen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.1	Beschränken Sie die Speicherung von Karteninh aberdaten auf ein Minimum, indem Sie Richtlinien, Verfahren und Prozesse für die Datenaufb ewahrung und - vernichtung einführen , die mindestens Folgendes für die gesamte Speicheru ng von Karteninh aberdaten umfassen: - Begrenzung des Umfangs und der Dauer der Datenspei cherung auf das Maß, das für gesetzlic he, behördliche und/oder geschäftl iche Anforderu ngen erforderlich ist - Spezifische Aufbewahrungsanfor derungen für Karteninhaberdaten - Verfahren zur sicheren Löschung von Daten, wenn diese nicht mehr benötigt werden -	s3- lifecycle-policy-c heck	Mit Amazon-S3-Lebenszyklusregeln können Sie Aktionen definieren, die Amazon S3 während der Lebensdau er eines Objekts ausführen soll (z. B. die Überführu ng von Objekten in eine andere Speicherklasse, ihre Archivierung oder Löschung nach einem bestimmten Zeitraum) .

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	Ein vierteljährliches Verfahren zur Ermittlung und sicheren Löschung gespeicherter Karteninhaberdaten , die die festgelegte Aufbewahrungsdauer überschreiten.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.1	Beschränken Sie die Speicherung von Karteninhaberdaten auf ein Minimum, indem Sie Richtlinien, Verfahren und Prozesse für die Datenaufbewahrung und -vernichtung einführen, die mindestens Folgendes für die gesamte Speicherung von Karteninhaberdaten umfassen: - Begrenzung des Umfangs und der Dauer der Datenspeicherung auf das Maß, das für gesetzliche, behördliche und/oder geschäftliche Anforderungen erforderlich ist - Spezifische Aufbewahrungsanforderungen für Karteninhaberdaten - Verfahren zur sicheren Löschung von Daten, wenn diese nicht mehr benötigt werden -	backup-plan-min-frequency-and-min-retention-check	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihr AWS Backup-Plan auf eine Mindestfrequenz und Aufbewahrung festgelegt ist. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen. Mit dieser Regel können Sie die Parameter requiredFrequencyValue (Config default: 1), requiredRetentionDays (Config default: 35) und requiredFrequencyUnit

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	Ein vierteljährliches Verfahren zur Ermittlung und sicheren Löschung gespeicherter Karteninhaberdaten, die die festgelegte Aufbewahrungsdauer überschreiten.		(Config default: days) festlegen. Der tatsächliche Wert muss den Anforderungen Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.1	Beschränken Sie die Speicherung von Karteninhaberdaten auf ein Minimum, indem Sie Richtlinien, Verfahren und Prozesse für die Datenaufbewahrung und -vernichtung einführen, die mindestens Folgendes für die gesamte Speicherung von Karteninhaberdaten umfassen: - Begrenzung des Umfangs und der Dauer der Datenspeicherung auf das Maß, das für gesetzliche, behördliche und/oder geschäftliche Anforderungen erforderlich ist - Spezifische Aufbewahrungsanforderungen für Karteninhaberdaten - Verfahren zur sicheren Löschung von Daten, wenn diese nicht mehr benötigt werden -	backup-recovery-point-minimum-Aufbewahrungsprüfung	Um bei Datensicherungsprozessen zu helfen, stellen Sie sicher, dass für Ihre AWS Backup-Wiederherstellungspunkte eine Mindestaufbewahrungsdauer festgelegt ist. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen. Mit dieser Regel können Sie den Parameter requiredRetentionDays (Standardkonfiguration: 35) festlegen. Der tatsächliche Wert muss den Anforderu

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	Ein vierteljährliches Verfahren zur Ermittlung und sicheren Löschung gespeicherter Karteninhaberdaten , die die festgelegte Aufbewahrungsdauer überschreiten.		ngen Ihrer Organisat ion entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.1	Beschränken Sie die Speicherung von Karteninh aberdaten auf ein Minimum, indem Sie Richtlinien, Verfahren und Prozesse für die Datenaufb ewahrung und - vernichtung einführen , die mindestens Folgendes für die gesamte Speicheru ng von Karteninh aberdaten umfassen: - Begrenzung des Umfangs und der Dauer der Datenspei cherung auf das Maß, das für gesetzlic he, behördliche und/oder geschäftl iche Anforderu ngen erforderlich ist - Spezifische Aufbewahrungsanfor derungen für Karteninhaberdaten - Verfahren zur sicheren Löschung von Daten, wenn diese nicht mehr benötigt werden -	elasticache-redis-cluster-automatic-backup-check	Wenn automatische Backups aktiviert sind, ElastiCache erstellt Amazon täglich ein Backup des Clusters. Die Sicherung kann für eine von Ihrer Organisation festgelegte Anzahl von Tagen aufbewahrt werden. Automatische Backups schützen vor Datenverlust. Bei einem Ausfall können Sie einen neuen Cluster erstellen, der Ihre Daten aus dem aktuellen Backup wiederherstellt.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	Ein vierteljährliches Verfahren zur Ermittlung und sicheren Löschung gespeicherter Karteninhaberdaten , die die festgelegte Aufbewahrungsdauer überschreiten.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.4	Machen Sie PAN überall dort unlesbar, wo es gespeichert ist (einschließlich auf tragbaren digitalen Medien, Backup-Medien und in Protokollen), indem Sie einen der folgenden Ansätze verwenden: • Einseitige Hashes, die auf starker Kryptografie basieren (der Hash muss aus der gesamten PAN stammen) • Kürzung (Hashing kann nicht verwendet werden, um das gekürzte PAN-Segment zu ersetzen) • Index-Tokens und -Pads (Pads müssen sicher gespeichert werden) • Starke Kryptografie mit zugehörigen Schlüsselverwaltungsprozessen und -verfahren. Hinweis: Es ist ein relativ einfacher Versuch für eine böswillige Person, ursprüngl	backup-recovery-point-encrypted	Stellen Sie sicher, dass die Verschlüsselung für Ihre AWS Backup-Wiederherstellungspunkte aktiviert ist. Da sensible Daten auch im Ruhezustand vorhanden sein können, sollten Sie die Verschlüsselung im Ruhezustand aktivieren, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	iche PAN-Daten zu rekonstruieren, wenn sie Zugriff sowohl auf die gekürzte als auch auf die Hash-Version einer PAN hat. Wenn Hash-Versionen und gekürzte Versionen derselben PAN in der Umgebung einer Entität vorhanden sind, müssen zusätzliche Kontrolle n eingerichtet werden, um sicherzustellen, dass die gehashten und gekürzten Versionen nicht korreliert werden können, um die ursprüngliche PAN zu rekonstruieren.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.4	Machen Sie PAN überall dort unlesbar, wo es gespeichert ist (einschließlich auf tragbaren digitalen Medien, Backup-Me dien und in Protokoll en), indem Sie einen der folgenden Ansätze verwenden: • Einseitige Hashes, die auf starker Kryptogra fie basieren (der Hash muss aus der gesamten PAN stammen) • Kürzung (Hashing kann nicht verwendet werden, um das gekürzte PAN-Segment zu ersetzen) • Index-Tokens und -Pads (Pads müssen sicher gespeichert werden) • Starke Kryptogra fie mit zugehörigen Schlüsselverwaltun gsprozessen und -verfahren. Hinweis: Es ist ein relativ einfacher Versuch für eine böswillige Person, ursprüngl	cloud-trail-encryption-enabled	Da sensible Daten vorhanden sein können und um Daten im Ruhezustand zu schützen, sollten Sie sicherstellen, dass die Verschlüsselung für Ihre AWS CloudTrail Trails aktiviert ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	iche PAN-Daten zu rekonstruieren, wenn sie Zugriff sowohl auf die gekürzte als auch auf die Hash-Version einer PAN hat. Wenn Hash-Versionen und gekürzte Versionen derselben PAN in der Umgebung einer Entität vorhanden sind, müssen zusätzliche Kontrolle n eingerichtet werden, um sicherzustellen, dass die gehashten und gekürzten Versionen nicht korreliert werden können, um die ursprüngliche PAN zu rekonstruieren.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.4	Machen Sie PAN überall dort unlesbar, wo es gespeichert ist (einschließlich auf tragbaren digitalen Medien, Backup-Me dien und in Protokoll en), indem Sie einen der folgenden Ansätze verwenden: • Einseitige Hashes, die auf starker Kryptogra fie basieren (der Hash muss aus der gesamten PAN stammen) • Kürzung (Hashing kann nicht verwendet werden, um das gekürzte PAN-Segment zu ersetzen) • Index-Tokens und -Pads (Pads müssen sicher gespeichert werden) • Starke Kryptogra fie mit zugehörigen Schlüsselverwaltun gsprozessen und -verfahren. Hinweis: Es ist ein relativ einfacher Versuch für eine böswillige Person, ursprüngl	cloudwatch-log-group-encrypted	Um sensible Daten im Speicher zu schützen, stellen Sie sicher, dass die Verschlüs selung für Ihre Amazon CloudWatch Log Groups aktiviert ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	iche PAN-Daten zu rekonstruieren, wenn sie Zugriff sowohl auf die gekürzte als auch auf die Hash-Version einer PAN hat. Wenn Hash-Versionen und gekürzte Versionen derselben PAN in der Umgebung einer Entität vorhanden sind, müssen zusätzliche Kontrolle n eingerichtet werden, um sicherzustellen, dass die gehashten und gekürzten Versionen nicht korreliert werden können, um die ursprüngliche PAN zu rekonstruieren.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.4	Machen Sie PAN überall dort unlesbar, wo es gespeichert ist (einschließlich auf tragbaren digitalen Medien, Backup-Medien und in Protokollen), indem Sie einen der folgenden Ansätze verwenden: • Einseitige Hashes, die auf starker Kryptografie basieren (der Hash muss aus der gesamten PAN stammen) • Kürzung (Hashing kann nicht verwendet werden, um das gekürzte PAN-Segment zu ersetzen) • Index-Tokens und -Pads (Pads müssen sicher gespeichert werden) • Starke Kryptografie mit zugehörigen Schlüsselverwaltungsprozessen und -verfahren. Hinweis: Es ist ein relativ einfacher Versuch für eine böswillige Person, ursprüngl	ec2- ebs-encryption-by-default	Zum Schutz von Daten im Ruhezustand müssen Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon Elastic Block Store (Amazon EBS)-Volumes aktiviert ist. Da sensible Daten in diesen Volumes gespeichert werden können, sollten Sie die Verschlüsselung von Daten im Ruhezustand aktivieren, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	iche PAN-Daten zu rekonstruieren, wenn sie Zugriff sowohl auf die gekürzte als auch auf die Hash-Version einer PAN hat. Wenn Hash-Versionen und gekürzte Versionen derselben PAN in der Umgebung einer Entität vorhanden sind, müssen zusätzliche Kontrolle n eingerichtet werden, um sicherzustellen, dass die gehashten und gekürzten Versionen nicht korreliert werden können, um die ursprüngliche PAN zu rekonstruieren.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.4	Machen Sie PAN überall dort unlesbar, wo es gespeichert ist (einschließlich auf tragbaren digitalen Medien, Backup-Me dien und in Protokoll en), indem Sie einen der folgenden Ansätze verwenden: • Einseitige Hashes, die auf starker Kryptogra fie basieren (der Hash muss aus der gesamten PAN stammen) • Kürzung (Hashing kann nicht verwendet werden, um das gekürzte PAN-Segment zu ersetzen) • Index-Tokens und -Pads (Pads müssen sicher gespeichert werden) • Starke Kryptogra fie mit zugehörigen Schlüsselverwaltun gsprozessen und -verfahren. Hinweis: Es ist ein relativ einfacher Versuch für eine böswillige Person, ursprüngl	efs-encrypted-check	Aktivieren Sie die Verschlüsselung für Ihr Amazon Elastic File System (EFS), um eventuell vorhandene sensible Daten sowie Daten im Ruhezustand zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	iche PAN-Daten zu rekonstruieren, wenn sie Zugriff sowohl auf die gekürzte als auch auf die Hash-Version einer PAN hat. Wenn Hash-Versionen und gekürzte Versionen derselben PAN in der Umgebung einer Entität vorhanden sind, müssen zusätzliche Kontrolle n eingerichtet werden, um sicherzustellen, dass die gehashten und gekürzten Versionen nicht korreliert werden können, um die ursprüngliche PAN zu rekonstruieren.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.4	Machen Sie PAN überall dort unlesbar, wo es gespeichert ist (einschließlich auf tragbaren digitalen Medien, Backup-Me dien und in Protokoll en), indem Sie einen der folgenden Ansätze verwenden: • Einseitige Hashes, die auf starker Kryptogra fie basieren (der Hash muss aus der gesamten PAN stammen) • Kürzung (Hashing kann nicht verwendet werden, um das gekürzte PAN-Segment zu ersetzen) • Index-Tokens und -Pads (Pads müssen sicher gespeichert werden) • Starke Kryptogra fie mit zugehörigen Schlüsselverwaltun gsprozessen und -verfahren. Hinweis: Es ist ein relativ einfacher Versuch für eine böswillige Person, ursprüngl	encrypted-volumes	Aktivieren Sie die Verschlüsselung für Ihre Amazon-Elastic-Block-Store-(Amazon-EBS-)Volumes, um eventuell vorhandene sensible Daten sowie Daten im Ruhezusta nd zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	iche PAN-Daten zu rekonstruieren, wenn sie Zugriff sowohl auf die gekürzte als auch auf die Hash-Version einer PAN hat. Wenn Hash-Versionen und gekürzte Versionen derselben PAN in der Umgebung einer Entität vorhanden sind, müssen zusätzliche Kontrolle n eingerichtet werden, um sicherzustellen, dass die gehashten und gekürzten Versionen nicht korreliert werden können, um die ursprüngliche PAN zu rekonstruieren.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.4	Machen Sie PAN überall dort unlesbar, wo es gespeichert ist (einschließlich auf tragbaren digitalen Medien, Backup-Medien und in Protokollen), indem Sie einen der folgenden Ansätze verwenden: • Einseitige Hashes, die auf starker Kryptografie basieren (der Hash muss aus der gesamten PAN stammen) • Kürzung (Hashing kann nicht verwendet werden, um das gekürzte PAN-Segment zu ersetzen) • Index-Tokens und -Pads (Pads müssen sicher gespeichert werden) • Starke Kryptografie mit zugehörigen Schlüsselverwaltungsprozessen und -verfahren. Hinweis: Es ist ein relativ einfacher Versuch für eine böswillige Person, ursprüngl	rds-snapshot-encrypted	Stellen Sie sicher, dass die Verschlüsselung für Ihre Amazon Relational Database Service (Amazon RDS)-Snapshots aktiviert ist. Da sensible Daten auch im Ruhezustand vorhanden sein können, sollten Sie die Verschlüsselung von Daten im Ruhezustand aktivieren, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	iche PAN-Daten zu rekonstruieren, wenn sie Zugriff sowohl auf die gekürzte als auch auf die Hash-Version einer PAN hat. Wenn Hash-Versionen und gekürzte Versionen derselben PAN in der Umgebung einer Entität vorhanden sind, müssen zusätzliche Kontrolle n eingerichtet werden, um sicherzustellen, dass die gehashten und gekürzten Versionen nicht korreliert werden können, um die ursprüngliche PAN zu rekonstruieren.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.4	Machen Sie PAN überall dort unlesbar, wo es gespeichert ist (einschließlich auf tragbaren digitalen Medien, Backup-Medien und in Protokollen), indem Sie einen der folgenden Ansätze verwenden: • Einseitige Hashes, die auf starker Kryptografie basieren (der Hash muss aus der gesamten PAN stammen) • Kürzung (Hashing kann nicht verwendet werden, um das gekürzte PAN-Segment zu ersetzen) • Index-Tokens und -Pads (Pads müssen sicher gespeichert werden) • Starke Kryptografie mit zugehörigen Schlüsselverwaltungsprozessen und -verfahren. Hinweis: Es ist ein relativ einfacher Versuch für eine böswillige Person, ursprüngl	rds-storage-encrypted	Zum Schutz von Daten im Ruhezustand müssen Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon Relational Database Service (Amazon RDS)-Instances aktiviert ist. Da sensible Daten in Amazon-RDS-Instances gespeichert werden können, sollten Sie die Verschlüsselung von Daten im Ruhezustand aktivieren, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	iche PAN-Daten zu rekonstruieren, wenn sie Zugriff sowohl auf die gekürzte als auch auf die Hash-Version einer PAN hat. Wenn Hash-Versionen und gekürzte Versionen derselben PAN in der Umgebung einer Entität vorhanden sind, müssen zusätzliche Kontrolle n eingerichtet werden, um sicherzustellen, dass die gehashten und gekürzten Versionen nicht korreliert werden können, um die ursprüngliche PAN zu rekonstruieren.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.4	Machen Sie PAN überall dort unlesbar, wo es gespeichert ist (einschließlich auf tragbaren digitalen Medien, Backup-Medien und in Protokollen), indem Sie einen der folgenden Ansätze verwenden: • Einseitige Hashes, die auf starker Kryptografie basieren (der Hash muss aus der gesamten PAN stammen) • Kürzung (Hashing kann nicht verwendet werden, um das gekürzte PAN-Segment zu ersetzen) • Index-Tokens und -Pads (Pads müssen sicher gespeichert werden) • Starke Kryptografie mit zugehörigen Schlüsselverwaltungsprozessen und -verfahren. Hinweis: Es ist ein relativ einfacher Versuch für eine böswillige Person, ursprüngl	redshift-cluster-configuration-check	Um Daten im Ruhezustand zu schützen, muss die Verschlüsselung für Ihre Amazon-Redshift-Cluster aktiviert sein. Sie müssen auch sicherstellen, dass die erforderlichen Konfigurationen auf Amazon-Redshift-Clustern bereitgestellt werden. Die Prüfungsprotokollierung muss aktiviert sein, um Informationen zu Verbindungen und Benutzeraktivitäten in der Datenbank bereitzustellen. Diese Regel erfordert, dass ein Wert für clusterDbEncrypted (Config Default: TRUE) und LoggingEnabled (Config Default: TRUE) gesetzt ist. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	iche PAN-Daten zu rekonstruieren, wenn sie Zugriff sowohl auf die gekürzte als auch auf die Hash-Version einer PAN hat. Wenn Hash-Versionen und gekürzte Versionen derselben PAN in der Umgebung einer Entität vorhanden sind, müssen zusätzliche Kontrolle n eingerichtet werden, um sicherzustellen, dass die gehashten und gekürzten Versionen nicht korreliert werden können, um die ursprüngliche PAN zu rekonstruieren.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.4	Machen Sie PAN überall dort unlesbar, wo es gespeichert ist (einschließlich auf tragbaren digitalen Medien, Backup-Medien und in Protokollen), indem Sie einen der folgenden Ansätze verwenden: • Einseitige Hashes, die auf starker Kryptografie basieren (der Hash muss aus der gesamten PAN stammen) • Kürzung (Hashing kann nicht verwendet werden, um das gekürzte PAN-Segment zu ersetzen) • Index-Tokens und -Pads (Pads müssen sicher gespeichert werden) • Starke Kryptografie mit zugehörigen Schlüsselverwaltungsprozessen und -verfahren. Hinweis: Es ist ein relativ einfacher Versuch für eine böswillige Person, ursprüngl	s3-aktiviert bucket-server-side-encryption	Zum Schutz von Daten im Ruhezustand müssen Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon Simple Storage Service (Amazon S3)-Buckets aktiviert ist. Da sensible Daten in Amazon S3 Buckets gespeichert werden können, sollten Sie die Verschlüsselung aktivieren, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	iche PAN-Daten zu rekonstruieren, wenn sie Zugriff sowohl auf die gekürzte als auch auf die Hash-Version einer PAN hat. Wenn Hash-Versionen und gekürzte Versionen derselben PAN in der Umgebung einer Entität vorhanden sind, müssen zusätzliche Kontrolle n eingerichtet werden, um sicherzustellen, dass die gehashten und gekürzten Versionen nicht korreliert werden können, um die ursprüngliche PAN zu rekonstruieren.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.4	Machen Sie PAN überall dort unlesbar, wo es gespeichert ist (einschließlich auf tragbaren digitalen Medien, Backup-Medien und in Protokollen), indem Sie einen der folgenden Ansätze verwenden: • Einseitige Hashes, die auf starker Kryptografie basieren (der Hash muss aus der gesamten PAN stammen) • Kürzung (Hashing kann nicht verwendet werden, um das gekürzte PAN-Segment zu ersetzen) • Index-Tokens und -Pads (Pads müssen sicher gespeichert werden) • Starke Kryptografie mit zugehörigen Schlüsselverwaltungsprozessen und -verfahren. Hinweis: Es ist ein relativ einfacher Versuch für eine böswillige Person, ursprüngl	s-3 default-encryption-kms	Stellen Sie sicher, dass die Verschlüsselung für Ihre Amazon Simple Storage Service (Amazon S3)-Buckets aktiviert ist. Da sensible Daten in einem Amazon S3 Bucket gespeichert werden können, sollten Sie die Verschlüsselung im Ruhezustand aktivieren, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	iche PAN-Daten zu rekonstruieren, wenn sie Zugriff sowohl auf die gekürzte als auch auf die Hash-Version einer PAN hat. Wenn Hash-Versionen und gekürzte Versionen derselben PAN in der Umgebung einer Entität vorhanden sind, müssen zusätzliche Kontrolle n eingerichtet werden, um sicherzustellen, dass die gehashten und gekürzten Versionen nicht korreliert werden können, um die ursprüngliche PAN zu rekonstruieren.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.4	Machen Sie PAN überall dort unlesbar, wo es gespeichert ist (einschließlich auf tragbaren digitalen Medien, Backup-Me dien und in Protokoll en), indem Sie einen der folgenden Ansätze verwenden: • Einseitige Hashes, die auf starker Kryptogra fie basieren (der Hash muss aus der gesamten PAN stammen) • Kürzung (Hashing kann nicht verwendet werden, um das gekürzte PAN-Segment zu ersetzen) • Index-Tokens und -Pads (Pads müssen sicher gespeichert werden) • Starke Kryptogra fie mit zugehörigen Schlüsselverwaltun gsprozessen und -verfahren. Hinweis: Es ist ein relativ einfacher Versuch für eine böswillige Person, ursprüngl	sagemaker-endpoint -configuration-kms-key-konfiguriert	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass die Verschlüsselung mit dem AWS Key Management Service (AWS KMS) für Ihren Endpunkt aktiviert ist. SageMaker Da sensible Daten auf dem SageMaker Endgerät gespeiche rt werden können, sollten Sie die Verschlüsselung im Ruhezustand aktiviere n, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	iche PAN-Daten zu rekonstruieren, wenn sie Zugriff sowohl auf die gekürzte als auch auf die Hash-Version einer PAN hat. Wenn Hash-Versionen und gekürzte Versionen derselben PAN in der Umgebung einer Entität vorhanden sind, müssen zusätzliche Kontrolle n eingerichtet werden, um sicherzustellen, dass die gehashten und gekürzten Versionen nicht korreliert werden können, um die ursprüngliche PAN zu rekonstruieren.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.4	Machen Sie PAN überall dort unlesbar, wo es gespeichert ist (einschließlich auf tragbaren digitalen Medien, Backup-Medien und in Protokollen), indem Sie einen der folgenden Ansätze verwenden: • Einseitige Hashes, die auf starker Kryptografie basieren (der Hash muss aus der gesamten PAN stammen) • Kürzung (Hashing kann nicht verwendet werden, um das gekürzte PAN-Segment zu ersetzen) • Index-Tokens und -Pads (Pads müssen sicher gespeichert werden) • Starke Kryptografie mit zugehörigen Schlüsselverwaltungsprozessen und -verfahren. Hinweis: Es ist ein relativ einfacher Versuch für eine böswillige Person, ursprüngl	sagemaker-notebook-instance-kms-schlüsselkonfiguriert	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass die Verschlüsselung mit dem AWS Key Management Service (AWS KMS) für Ihr Notebook aktiviert ist. SageMaker Da vertrauliche Daten im SageMaker Notebook gespeichert werden können, sollten Sie die Verschlüsselung im Ruhezustand aktivieren, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	iche PAN-Daten zu rekonstruieren, wenn sie Zugriff sowohl auf die gekürzte als auch auf die Hash-Version einer PAN hat. Wenn Hash-Versionen und gekürzte Versionen derselben PAN in der Umgebung einer Entität vorhanden sind, müssen zusätzliche Kontrolle n eingerichtet werden, um sicherzustellen, dass die gehashten und gekürzten Versionen nicht korreliert werden können, um die ursprüngliche PAN zu rekonstruieren.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.4	Machen Sie PAN überall dort unlesbar, wo es gespeichert ist (einschließlich auf tragbaren digitalen Medien, Backup-Me dien und in Protokoll en), indem Sie einen der folgenden Ansätze verwenden: • Einseitige Hashes, die auf starker Kryptogra fie basieren (der Hash muss aus der gesamten PAN stammen) • Kürzung (Hashing kann nicht verwendet werden, um das gekürzte PAN-Segment zu ersetzen) • Index-Tokens und -Pads (Pads müssen sicher gespeichert werden) • Starke Kryptogra fie mit zugehörigen Schlüsselverwaltun gsprozessen und -verfahren. Hinweis: Es ist ein relativ einfacher Versuch für eine böswillige Person, ursprüngl	sns-encrypted-kms	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass Ihre Amazon Simple Notification Service (Amazon SNS) -Themen mit dem AWS Key Management Service (AWS KMS) verschlüsselt werden müssen. Um eventuell vorhandene sensible Daten im Ruhezusta nd in veröffentlichten Nachrichten zu schützen, muss die Verschlüsselung von Daten im Ruhezusta nd aktiviert sein.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	iche PAN-Daten zu rekonstruieren, wenn sie Zugriff sowohl auf die gekürzte als auch auf die Hash-Version einer PAN hat. Wenn Hash-Versionen und gekürzte Versionen derselben PAN in der Umgebung einer Entität vorhanden sind, müssen zusätzliche Kontrolle n eingerichtet werden, um sicherzustellen, dass die gehashten und gekürzten Versionen nicht korreliert werden können, um die ursprüngliche PAN zu rekonstruieren.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.5.2	Beschränken Sie den Zugriff auf kryptogra fische Schlüssel auf die geringstmögliche Anzahl von Verwalter n.	iam-customer-policy-blocked-kms-Aktionen	AWS Identity and Access Managemen t (IAM) kann Ihnen helfen, die Prinzipien der geringsten Rechte und der Aufgabent rennung in Zugriffsb erechtigungen und Autorisierungen zu integrieren und so zu verhindern, dass Richtlinien blockiert e Aktionen für alle AWS Schlüssel des Key Management Service enthalten. Wenn Benutzer mehr Rechte haben, als für die Ausführun g einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringste n Berechtigung und Aufgabentrennung verstoßen. Mit dieser Regel können Sie den Parameter festlegen. blockedAc tionsPatterns (Wert „AWS Bewährte grundlegende Sicherheitsmethode

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			n“: kms: Entschlüs seln, kms:ReEnc ryptFrom). Die tatsächlichen Werte müssen den Richtlini en Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.5.2	Beschränken Sie den Zugriff auf kryptogra fische Schlüssel auf die geringstmögliche Anzahl von Verwalter n.	iam-inline-policy-blocked-kms-Aktionen	Stellen Sie sicher, dass ein Benutzer, eine IAM-Rolle oder eine IAM-Gruppe (AWS Identity and Access Management) nicht über eine Inline-Richtlinie verfügt, die blockierte Aktionen für alle AWS Schlüssel des Key Management Service zulässt. AWS empfiehlt, verwaltet e Richtlinien anstelle von Inline-Richtlinien zu verwenden. Verwaltete Richtlini en ermöglichen Wiederverwendbarke it, Versionsverwaltung , Rollback und Delegierung der Berechtigungsverwa ltung. Mit dieser Regel können Sie den blockedActionsPatt erns Parameter festlegen. (Wert „AWS Bewährte grundlegende Sicherheitsmethode n“: kms: Entschlüs seln, kms:ReEnc

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			ryptFrom). Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.5.3	Speichern Sie geheime und private Schlüssel, die zum Ver-/Entschlüsseln von Karteninh aberdaten verwendet werden, jederzeit in einer (oder mehreren) der folgenden Formen: • Verschlüs selt mit einem Schlüsselverschlüs selungsschlüssel, der mindestens so stark ist wie der Datenvers chlüsselungsschlüs sel und der getrennt vom Datenvers chlüsselungsschlüs sel gespeichert wird • In einem sicheren kryptogra fischen Gerät (z. B. einem Hardware-(Host-) Sicherhei tsmodul (HSM) oder einem PTS-zugel assenen point-of-interaction Gerät) • Als mindesten s zwei vollständ ige Länge von Schlüsselkomponent	s-3 default-encryption -kms	Stellen Sie sicher, dass die Verschlüs selung für Ihre Amazon Simple Storage Service (Amazon S3)-Bucke ts aktiviert ist. Da sensible Daten in einem Amazon S3 Bucket gespeiche rt werden können, sollten Sie die Verschlüsselung im Ruhezustand aktiviere n, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	en oder Schlüssel freigaben gemäß einer branchenü blichen Methode Hinweis: Es ist nicht erforderlich, dass öffentliche Schlüssel in einem von diese Formen.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.5.3	Speichern Sie geheime und private Schlüssel, die zum Ver-/Entschlüsseln von Karteninh aberdaten verwendet werden, jederzeit in einer (oder mehreren) der folgenden Formen: • Verschlüs selt mit einem Schlüsselverschlüs selungsschlüssel, der mindestens so stark ist wie der Datenvers chlüsselungsschlüs sel und der getrennt vom Datenvers chlüsselungsschlüs sel gespeichert wird • In einem sicheren kryptogra fischen Gerät (z. B. einem Hardware-(Host-) Sicherhei tsmodul (HSM) oder einem PTS-zugel assenen point-of-interaction Gerät) • Als mindesten s zwei vollständ ige Länge von Schlüsselkomponent	sagemaker-endpoint -configuration-kms-key-konfiguriert	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass die Verschlüsselung mit dem AWS Key Management Service (AWS KMS) für Ihren Endpunkt aktiviert ist. SageMaker Da sensible Daten auf dem SageMaker Endgerät gespeiche rt werden können, sollten Sie die Verschlüsselung im Ruhezustand aktiviere n, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	en oder Schlüssel freigaben gemäß einer branchenü blichen Methode Hinweis: Es ist nicht erforderlich, dass öffentliche Schlüssel in einem von diese Formen.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.5.3	Speichern Sie geheime und private Schlüssel, die zum Ver-/Entschlüsseln von Karteninh aberdaten verwendet werden, jederzeit in einer (oder mehreren) der folgenden Formen: • Verschlüs selt mit einem Schlüsselverschlüs selungsschlüssel, der mindestens so stark ist wie der Datenvers chlüsselungsschlüs sel und der getrennt vom Datenvers chlüsselungsschlüs sel gespeichert wird • In einem sicheren kryptogra fischen Gerät (z. B. einem Hardware-(Host-) Sicherhei tsmodul (HSM) oder einem PTS-zugel assenen point-of-interaction Gerät) • Als mindesten s zwei vollständ ige Länge von Schlüsselkomponent	sagemaker-notebook-instance-kms-key-konfiguriert	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass die Verschlüsselung mit dem AWS Key Management Service (AWS KMS) für Ihr Notebook aktiviert ist. SageMaker Da vertrauliche Daten im SageMaker Notebook gespeichert werden können, sollten Sie die Verschlüsselung im Ruhezustand aktivieren, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	en oder Schlüssel freigaben gemäß einer branchenü blichen Methode Hinweis: Es ist nicht erforderlich, dass öffentliche Schlüssel in einem von diese Formen.		
3.6.4	Änderungen an kryptografischen Schlüsseln für Schlüssel, die das Ende ihrer Kryptoper iode erreicht haben (z. B. nach Ablauf eines bestimmte n Zeitraums und/ oder nachdem durch einen bestimmte n Schlüssel eine bestimmte Menge an Chiffretext erzeugt wurde), wie vom jeweiligen Anwendung sanbieter oder Schlüsseleigentüme r festgelegt und auf bewährten Verfahren und Richtlinien der Branche (z. B. NIST-Sonderpublikation 800-57) basieren.	cmk-backing-key-ro tation-aktiviert	Aktivieren Sie die Schlüsselrotation, um sicherzustellen, dass Schlüssel rotiert werden, nachdem sie das Ende ihrer Krypto-Periode erreicht haben.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.6.5	Außerbetriebnahme oder Ersatz (z. B. Archivierung, Vernichtung, and/or revocation) of keys as deemed necessary when the integrity of the key has been weakened (for example, departure of an employee with knowledge of a clear-text key component), or keys are suspected of being compromised. Note: If retired or replaced cryptographic keys need to be retained, these keys must be securely archived (for example, by using a key-encryption key). Archived cryptographic keys should only be used for decryption/verification Verwendungszwecke).	kms-cmk-not-scheduled-zum Löschen	Um Daten im Ruhezustand zu schützen, sollten Sie sicherstellen, dass die für den Kunden erforderlichen Masterschlüssel (CMKs) nicht im AWS Key Management Service (AWS KMS) gelöscht werden. Da Schlüssel manchmal gelöscht werden müssen, können Sie mit dieser Regel alle zu löschenden Schlüssel überprüfen, falls ein Schlüssel versehentlich zur Löschung vorgemerkt wurde.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.6.7	Verhinderung der unbefugten Ersetzung kryptografischer Schlüssel.	kms-cmk-not-scheduled-zum Löschen	Um Daten im Ruhezustand zu schützen, sollten Sie sicherstellen, dass die für den Kunden erforderlichen Masterschlüssel (CMKs) nicht im AWS Key Management Service (AWS KMS) gelöscht werden. Da Schlüssel manchmal gelöscht werden müssen, können Sie mit dieser Regel alle zu löschenden Schlüssel überprüfen, falls ein Schlüssel versehentlich zur Löschung vorgemerkt wurde.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
4.1	Verwenden Sie starke Kryptografie- und Sicherheitsprotokolle, um sensible Karteninhaberdaten bei der Übertragung über offene, öffentliche Netzwerke zu schützen, einschließlich der folgenden: • Nur vertrauenswürdige Schlüssel und Zertifikate werden akzeptiert. • Das verwendete Protokoll unterstützt nur sichere Versionen oder Konfigurationen. • Die Verschlüsselungsstärke ist der verwendeten Verschlüsselungsmethode angemessen. Beispiele für offene, öffentliche Netzwerke sind unter anderem: • Das Internet • Drahtlostechnologien, einschließlich 802.11 und Bluetooth • Mobilfunktechnologien, z. B. Global System for Mobile	acm-certificate-expiration-check	Stellen Sie sicher, dass die Netzwerkintegrität geschützt ist, indem Sie sicherstellen, dass X509-Zertifikate von AWS ACM ausgestellt werden. Diese Zertifikate müssen gültig und dürfen nicht abgelaufen sein. Für diese Regel ist ein Wert für erforderlich daysToExpiration (Wert für bewährte AWS Grundregeln für Sicherheit: 90). Der tatsächliche Wert muss den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	Communications (GSM), Code Division Multiple Access (CDMA) • General Packet Radio Service (GPRS) • Satellite nkommunikation		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
4.1	Verwenden Sie starke Kryptografie- und Sicherheitsprotokolle, um sensible Karteninhaberdaten bei der Übertragung über offene, öffentliche Netzwerke zu schützen, einschließlich der folgenden: • Nur vertrauenswürdige Schlüssel und Zertifikate werden akzeptiert. • Das verwendete Protokoll unterstützt nur sichere Versionen oder Konfigurationen. • Die Verschlüsselungsstärke ist der verwendeten Verschlüsselungsmethode angemessen. Beispiele für offene, öffentliche Netzwerke sind unter anderem: • Das Internet • Drahtlostechnologien, einschließlich 802.11 und Bluetooth • Mobilfunktechnologien, z. B. Global System for Mobile	alb-http-to-https-Umleitungsprüfung	Um Daten während der Übertragung zu schützen, stellen Sie sicher, dass Ihr Application Load Balancer unverschlüsselte HTTP-Anfragen automatisch an HTTPS umleitet. Da sensible Daten vorhanden sein können, sollten Sie die Verschlüsselung bei der Übertragung aktivieren, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	Communications (GSM), Code Division Multiple Access (CDMA) • General Packet Radio Service (GPRS) • Satellite nkommunikation		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
4.1	Verwenden Sie starke Kryptografie- und Sicherheitsprotokolle, um sensible Karteninhaberdaten bei der Übertragung über offene, öffentliche Netzwerke zu schützen, einschließlich der folgenden: • Nur vertrauenswürdige Schlüssel und Zertifikate werden akzeptiert. • Das verwendete Protokoll unterstützt nur sichere Versionen oder Konfigurationen. • Die Verschlüsselungsstärke ist der verwendeten Verschlüsselungsmethode angemessen. Beispiele für offene, öffentliche Netzwerke sind unter anderem: • Das Internet • Drahtlostechnologien, einschließlich 802.11 und Bluetooth • Mobilfunktechnologien, z. B. Global System for Mobile	api-gw-ssl-enabled	Stellen Sie sicher, dass die REST-API-Stufen von Amazon API Gateway mit SSL-Zertifikaten konfiguriert sind, damit Backend-Systeme überprüfen können, ob Anforderungen von API Gateway stammen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	Communications (GSM), Code Division Multiple Access (CDMA) • General Packet Radio Service (GPRS) • Satellite nkommunikation		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
4.1	Verwenden Sie starke Kryptografie- und Sicherheitsprotokolle, um sensible Karteninhaberdaten bei der Übertragung über offene, öffentliche Netzwerke zu schützen, einschließlich der folgenden: • Nur vertrauenswürdige Schlüssel und Zertifikate werden akzeptiert. • Das verwendete Protokoll unterstützt nur sichere Versionen oder Konfigurationen. • Die Verschlüsselungsstärke ist der verwendeten Verschlüsselungsmethode angemessen. Beispiele für offene, öffentliche Netzwerke sind unter anderem: • Das Internet • Drahtlostechnologien, einschließlich 802.11 und Bluetooth • Mobilfunktechnologien, z. B. Global System for Mobile	elasticsearch-node-to-node-Verschlüsselungsprüfung	Stellen Sie sicher, dass die node-to-node Verschlüsselung für Amazon OpenSearch Service aktiviert ist. Node-to-nodeVerschlüsselung ermöglicht die TLS 1.2-Verschlüsselung für die gesamte Kommunikation innerhalb der Amazon Virtual Private Cloud (Amazon VPC). Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	Communications (GSM), Code Division Multiple Access (CDMA) • General Packet Radio Service (GPRS) • Satellite nkommunikation		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
4.1	Verwenden Sie starke Kryptografie- und Sicherheitsprotokolle, um sensible Karteninhaberdaten bei der Übertragung über offene, öffentliche Netzwerke zu schützen, einschließlich der folgenden: • Nur vertrauenswürdige Schlüssel und Zertifikate werden akzeptiert. • Das verwendete Protokoll unterstützt nur sichere Versionen oder Konfigurationen. • Die Verschlüsselungsstärke ist der verwendeten Verschlüsselungsmethode angemessen. Beispiele für offene, öffentliche Netzwerke sind unter anderem: • Das Internet • Drahtlostechnologien, einschließlich 802.11 und Bluetooth • Mobilfunktechnologien, z. B. Global System for Mobile	elb-tls-https-listeners-nur	Stellen Sie sicher, dass Ihre Elastic Load Balancer (ELBs) mit SSL- oder HTTPS-Listenern konfiguriert sind. Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	Communications (GSM), Code Division Multiple Access (CDMA) • General Packet Radio Service (GPRS) • Satellite nkommunikation		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
4.1	Verwenden Sie starke Kryptografie- und Sicherheitsprotokolle, um sensible Karteninhaberdaten bei der Übertragung über offene, öffentliche Netzwerke zu schützen, einschließlich der folgenden: • Nur vertrauenswürdige Schlüssel und Zertifikate werden akzeptiert. • Das verwendete Protokoll unterstützt nur sichere Versionen oder Konfigurationen. • Die Verschlüsselungsstärke ist der verwendeten Verschlüsselungsmethode angemessen. Beispiele für offene, öffentliche Netzwerke sind unter anderem: • Das Internet • Drahtlostechnologien, einschließlich 802.11 und Bluetooth • Mobilfunktechnologien, z. B. Global System for Mobile	elbv-2 acm-certificate-required	Zum Schutz von eventuell vorhandenen sensiblen Daten sowie von Daten während der Übertragung muss die Verschlüsselung für Ihr Elastic Load Balancing aktiviert sein. Verwenden Sie AWS Certificate Manager, um öffentliche und private SSL/TLS-Zertifikate mit AWS Diensten und internen Ressourcen zu verwalten, bereitzustellen und bereitzustellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	Communications (GSM), Code Division Multiple Access (CDMA) • General Packet Radio Service (GPRS) • Satellite nkommunikation		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
4.1	Verwenden Sie starke Kryptografie- und Sicherheitsprotokolle, um sensible Karteninhaberdaten bei der Übertragung über offene, öffentliche Netzwerke zu schützen, einschließlich der folgenden: • Nur vertrauenswürdige Schlüssel und Zertifikate werden akzeptiert. • Das verwendete Protokoll unterstützt nur sichere Versionen oder Konfigurationen. • Die Verschlüsselungsstärke ist der verwendeten Verschlüsselungsmethode angemessen. Beispiele für offene, öffentliche Netzwerke sind unter anderem: • Das Internet • Drahtlostechnologien, einschließlich 802.11 und Bluetooth • Mobilfunktechnologien, z. B. Global System for Mobile	opensearch-https-required	Da sensible Daten existieren können und um Daten während der Übertragung zu schützen, sollten Sie sicherstellen, dass HTTPS für Verbindungen zu Ihren Amazon OpenSearch Service-Domains aktiviert ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	Communications (GSM), Code Division Multiple Access (CDMA) • General Packet Radio Service (GPRS) • Satellite nkommunikation		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
4.1	Verwenden Sie starke Kryptografie- und Sicherheitsprotokolle, um sensible Karteninhaberdaten bei der Übertragung über offene, öffentliche Netzwerke zu schützen, einschließlich der folgenden: • Nur vertrauenswürdige Schlüssel und Zertifikate werden akzeptiert. • Das verwendete Protokoll unterstützt nur sichere Versionen oder Konfigurationen. • Die Verschlüsselungsstärke ist der verwendeten Verschlüsselungsmethode angemessen. Beispiele für offene, öffentliche Netzwerke sind unter anderem: • Das Internet • Drahtlostechnologien, einschließlich 802.11 und Bluetooth • Mobilfunktechnologien, z. B. Global System for Mobile	opensearch-node-to-node-Verschlüsselungsprüfung	Stellen Sie sicher, dass die node-to-node Verschlüsselung für Amazon OpenSearch Service aktiviert ist. Node-to-nodeVerschlüsselung ermöglicht die TLS 1.2-Verschlüsselung für die gesamte Kommunikation innerhalb der Amazon Virtual Private Cloud (Amazon VPC). Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	Communications (GSM), Code Division Multiple Access (CDMA) • General Packet Radio Service (GPRS) • Satellite nkommunikation		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
4.1	Verwenden Sie starke Kryptografie- und Sicherheitsprotokolle, um sensible Karteninhaberdaten bei der Übertragung über offene, öffentliche Netzwerke zu schützen, einschließlich der folgenden: • Nur vertrauenswürdige Schlüssel und Zertifikate werden akzeptiert. • Das verwendete Protokoll unterstützt nur sichere Versionen oder Konfigurationen. • Die Verschlüsselungsstärke ist der verwendeten Verschlüsselungsmethode angemessen. Beispiele für offene, öffentliche Netzwerke sind unter anderem: • Das Internet • Drahtlostechnologien, einschließlich 802.11 und Bluetooth • Mobilfunktechnologien, z. B. Global System for Mobile	redshift-require-tls-ssl	Stellen Sie sicher, dass Ihre Amazon-Redshift-Cluster eine TLS/SSL-Verschlüsselung erfordern, um eine Verbindung zu SQL-Clients herzustellen. Da sensible Daten vorhanden sein können, sollten Sie die Verschlüsselung bei der Übertragung aktivieren, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	Communications (GSM), Code Division Multiple Access (CDMA) • General Packet Radio Service (GPRS) • Satellite nkommunikation		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
4.1	Verwenden Sie starke Kryptografie- und Sicherheitsprotokolle, um sensible Karteninhaberdaten bei der Übertragung über offene, öffentliche Netzwerke zu schützen, einschließlich der folgenden: • Nur vertrauenswürdige Schlüssel und Zertifikate werden akzeptiert. • Das verwendete Protokoll unterstützt nur sichere Versionen oder Konfigurationen. • Die Verschlüsselungsstärke ist der verwendeten Verschlüsselungsmethode angemessen. Beispiele für offene, öffentliche Netzwerke sind unter anderem: • Das Internet • Drahtlostechnologien, einschließlich 802.11 und Bluetooth • Mobilfunktechnologien, z. B. Global System for Mobile	s-3 bucket-ssl-requests-only	Um Daten während der Übertragung zu schützen, stellen Sie sicher, dass Ihre Amazon Simple Storage Service (Amazon S3)-Buckets Anfragen zur Verwendung von Secure Socket Layer (SSL)-Buckets erfordern. Da sensible Daten vorhanden sein können, sollten Sie die Verschlüsselung bei der Übertragung aktivieren, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	Communications (GSM), Code Division Multiple Access (CDMA) • General Packet Radio Service (GPRS) • Satellite nkommunikation		
6.2	Sicherstellen, dass alle Systemkom ponenten und Software vor bekannten Sicherhei tslücken geschützt sind, indem Sie entsprechende Sicherheitspatches installieren. Kritische Sicherheitspatches müssen innerhalb eines Monats nach ihrer Veröffentlichung installiert werden. Hinweis: Kritische Sicherheitspatches sollten gemäß dem in Anforderung 6.1 definierten Verfahren zur Risikoeinstufung identifiziert werden.	elastic-beanstalk-managed-updates-aktiviert	Durch die Aktivierung verwalteter Plattform updates für eine Amazon-Elastic-Bea nstalk-Umgebung wird sichergestellt, dass die aktuellen verfügbaren Plattform -Fixes, -Updates und -Features für die Umgebung installiert sind. Eine bewährte Methode zur Sicherung von Systemen besteht darin, stets die aktuellen Patches zu installieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
6.2	Sicherstellen, dass alle Systemkomponenten und Software vor bekannten Sicherheitslücken geschützt sind, indem Sie entsprechende Sicherheitspatches installieren. Kritische Sicherheitspatches müssen innerhalb eines Monats nach ihrer Veröffentlichung installiert werden. Hinweis: Kritische Sicherheitspatches sollten gemäß dem in Anforderung 6.1 definierten Verfahren zur Risikoeinstufung identifiziert werden.	ec2- prüfen managedinstance-association-compliance-status	Verwenden Sie AWS Systems Manager Associations, um bei der Inventarisierung von Softwareplattformen und Anwendungen innerhalb eines Unternehmens zu helfen. AWS Systems Manager weist Ihren verwalteten Instanzen einen Konfigurationsstatus zu und ermöglicht es Ihnen, Basiswerte für Betriebssystem-Patch-Levels, Softwareinstallationen, Anwendungskonfigurationen und andere Details zu Ihrer Umgebung festzulegen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
6.2	Sicherstellen, dass alle Systemkomponenten und Software vor bekannten Sicherheitslücken geschützt sind, indem Sie entsprechende Sicherheitspatches installieren. Kritische Sicherheitspatches müssen innerhalb eines Monats nach ihrer Veröffentlichung installiert werden. Hinweis: Kritische Sicherheitspatches sollten gemäß dem in Anforderung 6.1 definierten Verfahren zur Risikoeinstufung identifiziert werden.	ec2-check managedinstance-patch-compliance-status	Aktivieren Sie diese Regel, um bei der Identifizierung und Dokumentation von Sicherheitslücken in Amazon Elastic Compute Cloud (Amazon EC2) zu helfen. Die Regel prüft, ob die EC2 Amazon-Instance die Patch-Konformität im AWS Systems Manager gemäß den Richtlinien und Verfahren Ihrer Organisation einhält.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
6.2	Sicherstellen, dass alle Systemkomponenten und Software vor bekannten Sicherheitslücken geschützt sind, indem Sie entsprechende Sicherheitspatches installieren. Kritische Sicherheitspatches müssen innerhalb eines Monats nach ihrer Veröffentlichung installiert werden. Hinweis: Kritische Sicherheitspatches sollten gemäß dem in Anforderung 6.1 definierten Verfahren zur Risikoeinstufung identifiziert werden.	ecs-fargate-latest-platform-Version	Sicherheitsupdates und Patches werden automatisch für Ihre AWS Fargate-Aufgaben bereitgestellt. Wenn ein Sicherheitsproblem gefunden wird, das eine AWS Fargate-Plattformversion betrifft, AWS wird die Plattformversion gepatcht. Um Sie bei der Patchverwaltung Ihrer Amazon Elastic Container Service (ECS) - Aufgaben zu unterstützen, auf denen AWS Fargate ausgeführt wird, aktualisieren Sie Ihre eigenständigen Service-Aufgaben, sodass sie die neueste Plattformversion verwenden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
6.2	Sicherstellen, dass alle Systemkom ponenten und Software vor bekannten Sicherhei tslücken geschützt sind, indem Sie entsprechende Sicherheitspatches installieren. Kritische Sicherheitspatches müssen innerhalb eines Monats nach ihrer Veröffentlichung installiert werden. Hinweis: Kritische Sicherheitspatches sollten gemäß dem in Anforderung 6.1 definierten Verfahren zur Risikoeinstufung identifiziert werden.	rds-automatic-minor-version-Upgrade-fähig	Aktivieren Sie automatische Unterversions-Upgrades auf Ihren Amazon-Re lational-Database-Service (RDS)-Ins tances, um sicherzus tellen, dass die aktuellen Updates für Unterversionen des Relational Database Management System (RDBMS) installiert sind, die Sicherhei tspatches und Bugfixes enthalten können.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
6.2	Sicherstellen, dass alle Systemkomponenten und Software vor bekannten Sicherheitslücken geschützt sind, indem Sie entsprechende Sicherheitspatches installieren. Kritische Sicherheitspatches müssen innerhalb eines Monats nach ihrer Veröffentlichung installiert werden. Hinweis: Kritische Sicherheitspatches sollten gemäß dem in Anforderung 6.1 definierten Verfahren zur Risikoeinstufung identifiziert werden.	redshift-cluster-maintenancesettings-check	Diese Regel stellt sicher, dass Amazon-Redshift-Cluster die bevorzugten Einstellungen für Ihre Organisation haben. Insbesondere sorgt sie dafür, dass Cluster bevorzugte Wartungsfenster und automatisierte Aufbewahrungsfristen für Snapshots für die Datenbank haben. Für diese Regel müssen Sie die festlegen. allowVersionUpgrade Der Standardwert ist „true“. Außerdem können Sie optional den Zeitraum preferredMaintenanceWindow (der Standardwert ist sa: 16:00 -sa: 16:30) und den automated SnapshotRetention Zeitraum (der Standardwert ist 1) festlegen. Die tatsächlichen Werte müssen den Richtlini

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			en Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
6.3.2	Überprüfen Sie benutzerdefinierte n Code vor der Freigabe für die Produktion oder für Kunden, um potenziel le Sicherheitslücken bei der Programmi erung zu identifiz ieren (entweder mithilfe manueller oder automatis ierter Verfahren), und schließen Sie mindestens Folgendes ein: • Codeänderungen werden von anderen Personen als dem ursprünglichen Code-Autor sowie von Personen geprüft, die sich mit Code-Revi ew-Techniken und sicheren Codierung spraktiken auskennen . • Codeprüfungen stellen sicher, dass der Code gemäß den Richtlinien für sicheres Codieren entwickelt wird • Entsprechende	ecr-private-image-scanning-aktiviert	Der Amazon Elastic Container Repositor y (ECR)-Image-Scan unterstützt die Identifizierung von Software-Schwachstellen in Ihren Container-Images. Durch die Aktivierung von Image-Scans in ECR-Repositorys werden die Integritä t und Sicherheit der gespeicherten Images mit einer zusätzlichen Überprüfungsebene verbessert.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	Korrekturen werden vor der Veröffent lichung vorgenomm en. • Die Ergebniss e der Code-Revi ews werden vor der Veröffentlichung vom Managemen t überprüft und genehmigt. (Fortsetz ung auf der nächsten Seite)		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
6.6	Gehen Sie bei öffentlich zugänglichen Webanwendungen kontinuierlich auf neue Bedrohungen und Sicherheitslücken ein und stellen Sie sicher, dass diese Anwendungen mit einer der folgenden Methoden vor bekannten Angriffen geschützt sind: • Überprüfung öffentlich zugänglicher Webanwendungen anhand manueller oder automatisierter Tools oder Methoden zur Bewertung von Anwendungsschwachstellen, mindestens einmal jährlich und nach Änderungen Hinweis: Diese Bewertung ist nicht identisch mit den Schwachstellenscans, die für Anforderung 11.2 durchgeführt wurden. • Installation einer automatisierten	alb-desync-mode-check	Um Anwendungen vor HTTP-Desync-Schwachstellen zu schützen, stellen Sie sicher, dass der HTTP-Desync-Mitigationsmodus auf Ihren Anwendungs-Loadbalancern aktiviert ist. Probleme mit HTTP-Desync können zum Schmuggel von Anfragen führen und Ihre Anwendungen anfällig für Queues- oder Cache-Poisoning machen. Die desynchronen Mitigationsmodi lauten „Überwachen“, „Defensiv“ und „Am strengsten“. Defensive ist der standardmäßige Modus.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	technischen Lösung, die webbasier te Angriffe (z. B. eine Webanwend ungs-Firewall) vor öffentlich zugänglic hen Webanwend ungen erkennt und verhindert, um den gesamten Datenverk ehr kontinuierlich zu überprüfen.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
6.6	Gehen Sie bei öffentlich zugänglichen Webanwendungen kontinuierlich auf neue Bedrohungen und Sicherheitslücken ein und stellen Sie sicher, dass diese Anwendungen mit einer der folgenden Methoden vor bekannten Angriffen geschützt sind: • Überprüfung öffentlich zugänglicher Webanwendungen anhand manueller oder automatisierter Tools oder Methoden zur Bewertung von Anwendungsschwachstellen, mindestens einmal jährlich und nach Änderungen Hinweis: Diese Bewertung ist nicht identisch mit den Schwachstellenscans, die für Anforderung 11.2 durchgeführt wurden. • Installation einer automatisierten	alb-waf-enabled	Stellen Sie sicher, dass AWS WAF auf Elastic Load Balancers (ELB) aktiviert ist, um Webanwendungen zu schützen. Eine WAF trägt zum Schutz Ihrer Webanwendungen oder APIs vor gängigen Web-Exploits bei. Diese Web-Exploits können sich auf die Verfügbarkeit auswirken, die Sicherheit gefährden oder übermäßige Ressourcen in Ihrer Umgebung verbrauchen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	technischen Lösung, die webbasier te Angriffe (z. B. eine Webanwend ungs-Firewall) vor öffentlich zugänglic hen Webanwend ungen erkennt und verhindert, um den gesamten Datenverk ehr kontinuierlich zu überprüfen.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
6.6	Gehen Sie bei öffentlich zugänglichen Webanwendungen kontinuierlich auf neue Bedrohungen und Sicherheitslücken ein und stellen Sie sicher, dass diese Anwendungen mit einer der folgenden Methoden vor bekannten Angriffen geschützt sind: • Überprüfung öffentlich zugänglicher Webanwendungen anhand manueller oder automatisierter Tools oder Methoden zur Bewertung von Anwendungsschwachstellen, mindestens einmal jährlich und nach Änderungen Hinweis: Diese Bewertung ist nicht identisch mit den Schwachstellenscans, die für Anforderung 11.2 durchgeführt wurden. • Installation einer automatisierten	api-gw-associated-with-WAF	AWS Mit WAF können Sie eine Reihe von Regeln (als Web Access Control List (Web ACL) bezeichnet) konfigurieren, die Webanfragen auf der Grundlage von anpassbaren Websicherheitsregeln und -bedingungen, die Sie definieren, zulassen, blockieren oder zählen. Stellen Sie sicher, dass Ihre Amazon-API-Gateway-Stufe mit einer WAF-Web-ACL verknüpft ist, um sie vor böswilligen Angriffen zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	technischen Lösung, die webbasier te Angriffe (z. B. eine Webanwend ungs-Firewall) vor öffentlich zugänglic hen Webanwend ungen erkennt und verhindert, um den gesamten Datenverk ehr kontinuierlich zu überprüfen.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
6.6	Gehen Sie bei öffentlich zugänglichen Webanwendungen kontinuierlich auf neue Bedrohungen und Sicherheitslücken ein und stellen Sie sicher, dass diese Anwendungen mit einer der folgenden Methoden vor bekannten Angriffen geschützt sind: • Überprüfung öffentlich zugänglicher Webanwendungen anhand manueller oder automatisierter Tools oder Methoden zur Bewertung von Anwendungsschwachstellen, mindestens einmal jährlich und nach Änderungen Hinweis: Diese Bewertung ist nicht identisch mit den Schwachstellenscans, die für Anforderung 11.2 durchgeführt wurden. • Installation einer automatisierten	waf-regional-rule-not-leer	Stellen Sie sicher, dass Ihre AWS WAF eine Regel hat, die nicht leer ist. Eine Regel ohne Bedingungen kann zu unbeabsichtigtem Verhalten führen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	technischen Lösung, die webbasier te Angriffe (z. B. eine Webanwend ungs-Firewall) vor öffentlich zugänglic hen Webanwend ungen erkennt und verhindert, um den gesamten Datenverk ehr kontinuierlich zu überprüfen.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
6.6	Gehen Sie bei öffentlich zugänglichen Webanwendungen kontinuierlich auf neue Bedrohungen und Sicherheitslücken ein und stellen Sie sicher, dass diese Anwendungen mit einer der folgenden Methoden vor bekannten Angriffen geschützt sind: • Überprüfung öffentlich zugänglicher Webanwendungen anhand manueller oder automatisierter Tools oder Methoden zur Bewertung von Anwendungsschwachstellen, mindestens einmal jährlich und nach Änderungen Hinweis: Diese Bewertung ist nicht identisch mit den Schwachstellenscans, die für Anforderung 11.2 durchgeführt wurden. • Installation einer automatisierten	waf-regional-rulegroup-not-leer	Stellen Sie sicher, dass Ihre AWS WAF eine Regelgruppe hat, die nicht leer ist. Eine leere Regelgruppe kann zu unbeabsichtigtem Verhalten führen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	technischen Lösung, die webbasier te Angriffe (z. B. eine Webanwend ungs-Firewall) vor öffentlich zugänglic hen Webanwend ungen erkennt und verhindert, um den gesamten Datenverk ehr kontinuierlich zu überprüfen.		

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
6.6	Gehen Sie bei öffentlich zugänglichen Webanwendungen kontinuierlich auf neue Bedrohungen und Sicherheitslücken ein und stellen Sie sicher, dass diese Anwendungen mit einer der folgenden Methoden vor bekannten Angriffen geschützt sind: • Überprüfung öffentlich zugänglicher Webanwendungen anhand manueller oder automatisierter Tools oder Methoden zur Bewertung von Anwendungsschwachstellen, mindestens einmal jährlich und nach Änderungen Hinweis: Diese Bewertung ist nicht identisch mit den Schwachstellenscans, die für Anforderung 11.2 durchgeführt wurden. • Installation einer automatisierten	waf-regional-webacl-not-leer	Eine an eine AWS WAF angehängte Web-ACL kann eine Sammlung von Regeln und Regelgruppen zur Überprüfung und Steuerung von Webanfragen enthalten. Wenn eine Web-ACL leer ist, wird der Webdatenverkehr weitergeleitet, ohne von der WAF erkannt oder bearbeitet zu werden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
	technischen Lösung, die webbasier te Angriffe (z. B. eine Webanwend ungs-Firewall) vor öffentlich zugänglic hen Webanwend ungen erkennt und verhindert, um den gesamten Datenverk ehr kontinuierlich zu überprüfen.		
7.1.1	Definieren Sie die Zugriffsanforderun gen für jede Rolle, einschließlich: • Systemkomponenten und Datenressourcen, auf die jede Rolle für ihre jeweilige Funktion zugreifen muss • die erforderl ichen Rechte (z. B. Benutzer, Administr ator usw.) für den Zugriff auf Ressource n.	ecs-task-definition-nonroot-Benutzer	Sie bestimmen einen Nicht-Root-Benutzer für den Zugriff auf Ihre Aufgabendefinitionen des Amazon Elastic Container Service (Amazon ECS), um die Implementierung des Prinzips der geringsten Berechtig ung zu unterstützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
7.1.1	Definieren Sie die Zugriffsanforderungen für jede Rolle, einschließlich: • Systemkomponenten und Datenressourcen, auf die jede Rolle für ihre jeweilige Funktion zugreifen muss • die erforderlichen Rechte (z. B. Benutzer, Administrator usw.) für den Zugriff auf Ressourcen.	s-3 bucket-acl-prohibited	Diese Regel prüft, ob Access Control Lists (ACLs) für die Zugriffskontrolle auf Amazon S3 S3-Buckets verwendet werden. ACLs sind veraltete Zugriffskontrollmechanismen für Amazon S3 S3-Buckets, die älter sind als AWS Identity and Access Management (IAM). Stattdessen empfiehlt es sich ACLs, IAM-Richtlinien oder S3-Bucket-Richtlinien zu verwenden, um den Zugriff auf Ihre S3-Buckets einfacher zu verwalten.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
7.1.1	Definieren Sie die Zugriffsanforderungen für jede Rolle, einschließlich: • Systemkomponenten und Datenressourcen, auf die jede Rolle für ihre jeweilige Funktion zugreifen muss • die erforderlichen Rechte (z. B. Benutzer, Administrator usw.) für den Zugriff auf Ressourcen.	ecs-containers-nonprivileged	Um die Implementierung des Prinzips der geringsten Berechtigung zu unterstützen, dürfen in Amazon Elastic Container Service (Amazon ECS)-Aufgabendefinitionen keine erhöhten Berechtigungen aktiviert sein. Wenn dieser Parameter den Wert „true“ aufweist, erhält der Container erhöhte Berechtigungen auf der Host-Container-Instance (ähnlich wie der Root-Benutzer).

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
7.1.1	Definieren Sie die Zugriffsanforderungen für jede Rolle, einschließlich: • Systemkomponenten und Datenressourcen, auf die jede Rolle für ihre jeweilige Funktion zugreifen muss • die erforderlichen Rechte (z. B. Benutzer, Administrator usw.) für den Zugriff auf Ressourcen.	ecs-containers-readonly-access	Die Aktivierung des schreibgeschützten Zugriffs auf Amazon Elastic Container Service (ECS)-Container kann dazu beitragen, das Prinzip der geringsten Berechtigung einzuhalten. Diese Option kann Angriffsvektoren reduzieren, da das Dateisystem der Container-Instance nur geändert werden kann, wenn es über ausdrückliche Lese- und Schreibberechtigungen verfügt.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
7.1.1	Definieren Sie die Zugriffsanforderungen für jede Rolle, einschließlich: • Systemkomponenten und Datenressourcen, auf die jede Rolle für ihre jeweilige Funktion zugreifen muss • die erforderlichen Rechte (z. B. Benutzer, Administrator usw.) für den Zugriff auf Ressourcen.	efs-access-point-enforce-root-Verzeichnis	Die Durchsetzung eines Stammverzeichnisses für einen Amazon-Elastic-File-System (Amazon-EFS)-Zugangspunkt trägt dazu bei, den Datenzugriff einzuschränken, indem sichergestellt wird, dass Benutzer des Zugangspunkts nur auf Dateien des angegebenen Unterverzeichnisses zugreifen können.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
7.1.1	Definieren Sie die Zugriffsanforderungen für jede Rolle, einschließlich: • Systemkomponenten und Datenressourcen, auf die jede Rolle für ihre jeweilige Funktion zugreifen muss • die erforderlichen Rechte (z. B. Benutzer, Administrator usw.) für den Zugriff auf Ressourcen.	efs-access-point-enforce-Benutzeridentität	Um die Implementierung des Prinzips der geringsten Rechte zu unterstützen, stellen Sie sicher, dass die Benutzerdurchsetzung für Ihr Amazon Elastic File System (Amazon EFS) aktiviert ist. Wenn diese Option aktiviert ist, ersetzt Amazon EFS den Benutzer und die Gruppe IDs des NFS-Clients durch die Identität, die auf dem Access Point für alle Dateisystemoperationen konfiguriert ist, und gewährt nur Zugriff auf diese erzwungene Benutzeridentität.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
7.1.1	Definieren Sie die Zugriffsanforderungen für jede Rolle, einschließlich: • Systemkomponenten und Datenressourcen, auf die jede Rolle für ihre jeweilige Funktion zugreifen muss • die erforderlichen Rechte (z. B. Benutzer, Administrator usw.) für den Zugriff auf Ressourcen.	emr-kerberos-enabled	Die Zugriffsberechtigungen und -autorisierungen können verwaltet und nach den Prinzipien der geringsten Berechtigung und Aufgabentrennung integriert werden, indem Kerberos für Amazon-EMR-Cluster aktiviert wird. In Kerberos werden Services und Benutzer, die sich authentifizieren müssen, als Prinzipale bezeichnet. Prinzipale befinden sich in einem Kerberos-Bereich. Innerhalb dieses Bereichs wird ein Kerberos-Server als Key Distribution Center (KDC) bezeichnet. Über diesen Server können sich Prinzipale authentifizieren. Die Authentifizierung im KDC erfolgt durch die Ausstellung von Authentif

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			izierungstickets. Das KDC unterhält eine Datenbank der Prinzipale in seinem Bereich mit ihren Passwörtern und anderen administr ativen Informationen zu jedem Prinzipal.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
7.1.1	Definieren Sie die Zugriffsanforderungen für jede Rolle, einschließlich: • Systemkomponenten und Datenressourcen, auf die jede Rolle für ihre jeweilige Funktion zugreifen muss • die erforderlichen Rechte (z. B. Benutzer, Administrator usw.) für den Zugriff auf Ressourcen.	iam-customer-policy-blocked-kms-Aktionen	AWS Identity and Access Management (IAM) kann Ihnen helfen, die Prinzipien der geringsten Rechte und der Aufgabentrennung in Zugriffsberechtigungen und Autorisierungen zu integrieren und so zu verhindern, dass Richtlinien blockierte Aktionen für alle AWS Schlüssel des Key Management Service enthalten. Wenn Benutzer mehr Rechte haben, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und Aufgabentrennung verstoßen. Mit dieser Regel können Sie den Parameter festlegen. blockedActionsPatterns (Wert „AWS Bewährte grundlegende Sicherheitsmethode

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			n“: kms: Entschlüs seln, kms:ReEnc ryptFrom). Die tatsächlichen Werte müssen den Richtlini en Ihrer Organisation entsprechen.
7.1.1	Definieren Sie die Zugriffsanforderun gen für jede Rolle, einschließlich: • Systemkomponenten und Datenressourcen, auf die jede Rolle für ihre jeweilige Funktion zugreifen muss • die erforderl ichen Rechte (z. B. Benutzer, Administr ator usw.) für den Zugriff auf Ressource n.	iam-group-has-users-überprüfen	AWS Identity and Access Managemen t (IAM) kann Ihnen helfen, die Prinzipien der geringsten Rechte und der Aufgabent rennung mit Zugriffsb erechtigungen und Autorisierungen zu integrieren, indem sichergestellt wird, dass IAM-Gruppen mindestens einen Benutzer haben. Die Einteilung von Benutzern in Gruppen auf der Grundlage der ihnen zugewiese nen Berechtigungen oder ihrer Funktion ist eine Möglichkeit, das Prinzip der geringste n Berechtigung zu implementieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
7.1.1	Definieren Sie die Zugriffsanforderungen für jede Rolle, einschließlich: • Systemkomponenten und Datenressourcen, auf die jede Rolle für ihre jeweilige Funktion zugreifen muss • die erforderlichen Rechte (z. B. Benutzer, Administrator usw.) für den Zugriff auf Ressourcen.	iam-inline-policy-blocked-kms-Aktionen	Stellen Sie sicher, dass ein Benutzer, eine IAM-Rolle oder eine IAM-Gruppe (AWS Identity and Access Management) nicht über eine Inline-Richtlinie verfügt, die blockierte Aktionen für alle AWS Schlüssel des Key Management Service zulässt. AWS empfiehlt, verwaltete Richtlinien anstelle von Inline-Richtlinien zu verwenden. Verwaltete Richtlinien ermöglichen Wiederverwendbarkeit, Versionsverwaltung, Rollback und Delegierung der Berechtigungsverwaltung. Mit dieser Regel können Sie den blockedActionsPatterns Parameter festlegen. (Wert „AWS Bewährte grundlegende Sicherheitsmethoden“: kms: Entschlüsseln, kms:ReEnc

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			ryptFrom). Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.
7.1.1	Definieren Sie die Zugriffsanforderungen für jede Rolle, einschließlich: • Systemkomponenten und Datenressourcen, auf die jede Rolle für ihre jeweilige Funktion zugreifen muss • die erforderlichen Rechte (z. B. Benutzer, Administrator usw.) für den Zugriff auf Ressourcen.	iam-no-inline-policy-überprüfen	Stellen Sie sicher, dass ein Benutzer, eine IAM-Rolle oder eine IAM-Gruppe (AWS Identity and Access Management) nicht über eine Inline-Richtlinie zur Zugriffskontrolle auf Systeme und Ressourcen verfügt. AWS empfiehlt, verwaltete Richtlinien anstelle von Inline-Richtlinien zu verwenden. Verwaltete Richtlinien ermöglichen Wiederverwendbarkeit, Versionsverwaltung, Rollback und Delegierung der Berechtigungsverwaltung.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
7.1.1	Definieren Sie die Zugriffsanforderungen für jede Rolle, einschließlich: • Systemkomponenten und Datenressourcen, auf die jede Rolle für ihre jeweilige Funktion zugreifen muss • die erforderlichen Rechte (z. B. Benutzer, Administrator usw.) für den Zugriff auf Ressourcen.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) kann Ihnen dabei helfen, die Prinzipien der geringsten Rechte und der Aufgabentrennung in Zugriffsberechtigungen und Autorisierungen zu integrieren und so zu verhindern, dass Richtlinien „Effect“: „Allow“ mit „Action“: „*“ anstelle von „Resource“: „*“ enthalten. Wenn Benutzern mehr Rechte eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und der Aufgabentrennung verstoßen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
7.1.1	Definieren Sie die Zugriffsanforderungen für jede Rolle, einschließlich: • Systemkomponenten und Datenressourcen, auf die jede Rolle für ihre jeweilige Funktion zugreifen muss • die erforderlichen Rechte (z. B. Benutzer, Administrator usw.) für den Zugriff auf Ressourcen.	iam-policy-no-statements-with-full-access	Stellen Sie sicher, dass IAM-Aktionen nur auf die benötigten Aktionen beschränkt sind. Wenn Benutzern mehr Rechte eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Rechte und der Aufgabentrennung verstoßen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
7.1.1	Definieren Sie die Zugriffsanforderungen für jede Rolle, einschließlich: • Systemkomponenten und Datenressourcen, auf die jede Rolle für ihre jeweilige Funktion zugreifen muss • die erforderlichen Rechte (z. B. Benutzer, Administrator usw.) für den Zugriff auf Ressourcen.	iam-root-access-key-überprüfen	Der Zugriff auf Systeme und Ressourcen kann gesteuert werden, indem überprüft wird, ob der Root-Benutzer keine Zugriffsschlüssel mit seiner AWS Identity and Access Management (IAM) -Rolle verknüpft hat. Stellen Sie sicher, dass die Root-Zugriffsschlüssel gelöscht werden. Erstellen und verwenden Sie stattdessen rollenbasierte Funktionen, AWS-Konten um das Prinzip der geringsten Funktionalität zu berücksichtigen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
7.1.1	Definieren Sie die Zugriffsanforderungen für jede Rolle, einschließlich: • Systemkomponenten und Datenressourcen, auf die jede Rolle für ihre jeweilige Funktion zugreifen muss • die erforderlichen Rechte (z. B. Benutzer, Administrator usw.) für den Zugriff auf Ressourcen.	iam-user-group-membership-überprüfen	AWS Identity and Access Management (IAM) kann Ihnen helfen, Zugriffsberechtigungen und Autorisierungen einzuschränken, indem sichergestellt wird, dass Benutzer Mitglieder mindestens einer Gruppe sind. Wenn Benutzern mehr Berechtigungen eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und Aufgabentrennung verstoßen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
7.1.1	Definieren Sie die Zugriffsanforderungen für jede Rolle, einschließlich: • Systemkomponenten und Datenressourcen, auf die jede Rolle für ihre jeweilige Funktion zugreifen muss • die erforderlichen Rechte (z. B. Benutzer, Administrator usw.) für den Zugriff auf Ressourcen.	iam-user-no-policies-überprüfen	Diese Regel stellt sicher, dass AWS Identity and Access Management (IAM) -Richtlinien nur Gruppen oder Rollen zugewiesen werden, um den Zugriff auf Systeme und Ressourcen zu kontrollieren. Die Zuweisung von Berechtigungen auf Gruppen- oder Rollenebene trägt dazu bei, die Wahrscheinlichkeit zu verringern, dass eine Identität übermäßige Berechtigungen erhält oder beibehält.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
7.1.1	Definieren Sie die Zugriffsanforderungen für jede Rolle, einschließlich: • Systemkomponenten und Datenressourcen, auf die jede Rolle für ihre jeweilige Funktion zugreifen muss • die erforderlichen Rechte (z. B. Benutzer, Administrator usw.) für den Zugriff auf Ressourcen.	opensearch-access-control-enabled	Stellen Sie sicher, dass eine detaillierte Zugriffskontrolle für Ihre Amazon OpenSearch Service-Domains aktiviert ist. Eine differenzierte Zugriffskontrolle bietet erweiterte Autorisierungsmechanismen, um den Zugriff auf Amazon Service-Domains mit den geringsten Rechten zu erreichen. OpenSearch Es ermöglicht eine rollenbasierte Zugriffskontrolle auf die Domain sowie Sicherheit auf Index-, Dokument- und Feldebene, Unterstützung für OpenSearch Service-Dashboards, Mehrmandantenfähigkeit und HTTP-Basisauthentifizierung für Service und Kibana. OpenSearch

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
7.1.2	Beschränken Sie den Zugriff auf privilegierte Benutzer IDs auf die geringsten Rechte, die zur Erfüllung ihrer Aufgaben erforderlich sind.	iam-customer-policy-blocked-kms-Aktionen	AWS Identity and Access Managemen t (IAM) kann Ihnen helfen, die Prinzipien der geringsten Rechte und der Aufgabent rennung in Zugriffsb erechtigungen und Autorisierungen zu integrieren und so zu verhindern, dass Richtlinien blockiert e Aktionen für alle AWS Schlüssel des Key Management Service enthalten. Wenn Benutzer mehr Rechte haben, als für die Ausführun g einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringste n Berechtigung und Aufgabentrennung verstoßen. Mit dieser Regel können Sie den Parameter festlegen. blockedAc tionsPatterns (Wert „AWS Bewährte grundlegende Sicherheitsmethode

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			n“: kms: Entschlüs seln, kms:ReEnc ryptFrom). Die tatsächlichen Werte müssen den Richtlini en Ihrer Organisation entsprechen.
7.1.2	Beschränken Sie den Zugriff auf privilegierte Benutzer IDs auf die geringsten Rechte, die zur Erfüllung ihrer Aufgaben erforderlich sind.	iam-group-has-users-überprüfen	AWS Identity and Access Managemen t (IAM) kann Ihnen helfen, die Prinzipien der geringsten Rechte und der Aufgabent rennung mit Zugriffsb erechtigungen und Autorisierungen zu integrieren, indem sichergestellt wird, dass IAM-Gruppen mindestens einen Benutzer haben. Die Einteilung von Benutzern in Gruppen auf der Grundlage der ihnen zugewiese nen Berechtigungen oder ihrer Funktion ist eine Möglichkeit, das Prinzip der geringste n Berechtigung zu implementieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
7.1.2	Beschränken Sie den Zugriff auf privilegierte Benutzer IDs auf die geringsten Rechte, die zur Erfüllung ihrer Aufgaben erforderlich sind.	iam-inline-policy-blocked-kms-Aktionen	Stellen Sie sicher, dass ein Benutzer, eine IAM-Rolle oder eine IAM-Gruppe (AWS Identity and Access Management) nicht über eine Inline-Richtlinie verfügt, die blockierte Aktionen für alle AWS Schlüssel des Key Management Service zulässt. AWS empfiehlt, verwaltete Richtlinien anstelle von Inline-Richtlinien zu verwenden. Verwaltete Richtlinien ermöglichen Wiederverwendbarkeit, Versionsverwaltung, Rollback und Delegierung der Berechtigungsverwaltung. Mit dieser Regel können Sie den blockedActionsPatterns Parameter festlegen. (Wert „AWS Bewährte grundlegende Sicherheitsmethoden“: kms: Entschlüsseln, kms:ReEnc

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			ryptFrom). Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.
7.1.2	Beschränken Sie den Zugriff auf privilegierte Benutzer IDs auf die geringsten Rechte, die zur Erfüllung ihrer Aufgaben erforderlich sind.	iam-no-inline-policy-überprüfen	Stellen Sie sicher, dass ein Benutzer, eine IAM-Rolle oder eine IAM-Gruppe (AWS Identity and Access Management) nicht über eine Inline-Richtlinie zur Zugriffskontrolle auf Systeme und Ressourcen verfügt. AWS empfiehlt, verwaltete Richtlinien anstelle von Inline-Richtlinien zu verwenden. Verwaltete Richtlinien ermöglichen Wiederverwendbarkeit, Versionsverwaltung, Rollback und Delegierung der Berechtigungsverwaltung.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
7.1.2	Beschränken Sie den Zugriff auf privilegierte Benutzer IDs auf die geringsten Rechte, die zur Erfüllung ihrer Aufgaben erforderlich sind.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) kann Ihnen dabei helfen, die Prinzipien der geringsten Rechte und der Aufgabentrennung in Zugriffsberechtigungen und Autorisierungen zu integrieren und so zu verhindern, dass Richtlinien „Effect“: „Allow“ mit „Action“: „*“ anstelle von „Resource“: „*“ enthalten. Wenn Benutzern mehr Rechte eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und der Aufgabentrennung verstoßen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
7.1.2	Beschränken Sie den Zugriff auf privilegierte Benutzer IDs auf die geringsten Rechte, die zur Erfüllung ihrer Aufgaben erforderlich sind.	iam-policy-no-statements-with-full-access	Stellen Sie sicher, dass IAM-Aktionen nur auf die benötigten Aktionen beschränkt sind. Wenn Benutzern mehr Rechte eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Rechte und der Aufgabentrennung verstoßen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
7.1.2	Beschränken Sie den Zugriff auf privilegierte Benutzer IDs auf die geringsten Rechte, die zur Erfüllung ihrer Aufgaben erforderlich sind.	iam-root-access-key-überprüfen	Der Zugriff auf Systeme und Ressourcen kann gesteuert werden, indem überprüft wird, ob der Root-Benutzer keine Zugriffsschlüssel mit seiner AWS Identity and Access Management (IAM) -Rolle verknüpft hat. Stellen Sie sicher, dass die Root-Zugriffsschlüssel gelöscht werden. Erstellen und verwenden Sie stattdessen rollenbasierte Funktionen, AWS-Konten um das Prinzip der geringsten Funktionalität zu berücksichtigen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
7.1.2	Beschränken Sie den Zugriff auf privilegierte Benutzer IDs auf die geringsten Rechte, die zur Erfüllung ihrer Aufgaben erforderlich sind.	iam-user-group-membership-überprüfen	AWS Identity and Access Management (IAM) kann Ihnen helfen, Zugriffsberechtigungen und Autorisierungen einzuschränken, indem sichergestellt wird, dass Benutzer Mitglieder mindestens einer Gruppe sind. Wenn Benutzern mehr Berechtigungen eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und Aufgabentrennung verstoßen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
7.1.2	Beschränken Sie den Zugriff auf privilegierte Benutzer IDs auf die geringsten Rechte, die zur Erfüllung ihrer Aufgaben erforderlich sind.	iam-user-no-policies-überprüfen	Diese Regel stellt sicher, dass AWS Identity and Access Management (IAM) -Richtlinien nur Gruppen oder Rollen zugewiese n werden, um den Zugriff auf Systeme und Ressourcen zu kontrollieren. Die Zuweisung von Berechtig ungen auf Gruppen- oder Rollenebene trägt dazu bei, die Wahrscheinlichkeit zu verringern, dass eine Identität übermäßige Berechtigungen erhält oder beibehält.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
7.2.1	Festlegen von Zugriffskontrollsystemen für Systemkomponenten, die den Zugriff anhand des Informationsbedarfs eines Benutzers einschränkt und auf „Alle ablehnen“ gesetzt ist, sofern der Zugriff nicht ausdrücklich zugelassen wird. Diese Zugriffskontrollsysteme müssen Folgendes enthalten: Abdeckung aller Systemkomponenten.	ecs-containers-nonprivileged	Um die Implementierung des Prinzips der geringsten Berechtigung zu unterstützen, dürfen in Amazon Elastic Container Service (Amazon ECS)-Aufgabendefinitionen keine erhöhten Berechtigungen aktiviert sein. Wenn dieser Parameter den Wert „true“ aufweist, erhält der Container erhöhte Berechtigungen auf der Host-Container-Instance (ähnlich wie der Root-Benutzer).

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
7.2.1	Festlegen von Zugriffskontrollsystemen für Systemkomponenten, die den Zugriff anhand des Informationsbedarfs eines Benutzers einschränkt und auf „Alle ablehnen“ gesetzt ist, sofern der Zugriff nicht ausdrücklich zugelassen wird. Diese Zugriffskontrollsysteme müssen Folgendes enthalten: Abdeckung aller Systemkomponenten.	ecs-containers-readonly-access	Die Aktivierung des schreibgeschützten Zugriffs auf Amazon Elastic Container Service (ECS)-Container kann dazu beitragen, das Prinzip der geringsten Berechtigung einzuhalten. Diese Option kann Angriffsvektoren reduzieren, da das Dateisystem der Container-Instance nur geändert werden kann, wenn es über ausdrückliche Lese- und Schreibberechtigungen verfügt.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
7.2.1	Festlegen von Zugriffskontrollsystemen für Systemkomponenten, die den Zugriff anhand des Informationsbedarfs eines Benutzers einschränkt und auf „Alle ablehnen“ gesetzt ist, sofern der Zugriff nicht ausdrücklich zugelassen wird. Diese Zugriffskontrollsysteme müssen Folgendes enthalten: Abdeckung aller Systemkomponenten.	efs-access-point-enforce-Stammverzeichnis	Die Durchsetzung eines Stammverzeichnisses für einen Amazon-Elastic-File-System (Amazon-EFS)-Zugangspunkt trägt dazu bei, den Datenzugriff einzuschränken, indem sichergestellt wird, dass Benutzer des Zugangspunkts nur auf Dateien des angegebenen Unterverzeichnisses zugreifen können.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
7.2.1	Festlegen von Zugriffskontrollsystemen für Systemkomponenten, die den Zugriff anhand des Informationsbedarfs eines Benutzers einschränkt und auf „Alle ablehnen“ gesetzt ist, sofern der Zugriff nicht ausdrücklich zugelassen wird. Diese Zugriffskontrollsysteme müssen Folgendes enthalten: Abdeckung aller Systemkomponenten.	efs-access-point-enforce-Benutzeridentität	Um die Implementierung des Prinzips der geringsten Rechte zu unterstützen, stellen Sie sicher, dass die Benutzerdurchsetzung für Ihr Amazon Elastic File System (Amazon EFS) aktiviert ist. Wenn diese Option aktiviert ist, ersetzt Amazon EFS den Benutzer und die Gruppe IDs des NFS-Clients durch die Identität, die auf dem Access Point für alle Dateisystemoperationen konfiguriert ist, und gewährt nur Zugriff auf diese erzwungene Benutzeridentität.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
7.2.1	Festlegen von Zugriffskontrollsystemen für Systemkomponenten, die den Zugriff anhand des Informationsbedarfs eines Benutzers einschränkt und auf „Alle ablehnen“ gesetzt ist, sofern der Zugriff nicht ausdrücklich zugelassen wird. Diese Zugriffskontrollsysteme müssen Folgendes enthalten: Abdeckung aller Systemkomponenten.	emr-kerberos-enabled	Die Zugriffsberechtigungen und -autorisierungen können verwaltet und nach den Prinzipien der geringsten Berechtigung und Aufgabentrennung integriert werden, indem Kerberos für Amazon-EMR-Cluster aktiviert wird. In Kerberos werden Services und Benutzer, die sich authentifizieren müssen, als Prinzipale bezeichnet. Prinzipale befinden sich in einem Kerberos-Bereich. Innerhalb dieses Bereichs wird ein Kerberos-Server als Key Distribution Center (KDC) bezeichnet. Über diesen Server können sich Prinzipale authentifizieren. Die Authentifizierung im KDC erfolgt durch die Ausstellung von Authentif

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			izierungstickets. Das KDC unterhält eine Datenbank der Prinzipale in seinem Bereich mit ihren Passwörtern und anderen administr ativen Informationen zu jedem Prinzipal.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
7.2.1	Festlegen von Zugriffskontrollsystemen für Systemkomponenten, die den Zugriff anhand des Informationsbedarfs eines Benutzers einschränkt und auf „Alle ablehnen“ gesetzt ist, sofern der Zugriff nicht ausdrücklich zugelassen wird. Diese Zugriffskontrollsysteme müssen Folgendes enthalten: Abdeckung aller Systemkomponenten.	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) kann Ihnen helfen, die Prinzipien der geringsten Rechte und der Aufgabentrennung in Zugriffsberechtigungen und Autorisierungen zu integrieren und so zu verhindern, dass Richtlinien blockierte Aktionen für alle AWS Schlüssel des Key Management Service enthalten. Wenn Benutzer mehr Rechte haben, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und Aufgabentrennung verstoßen. Mit dieser Regel können Sie den Parameter festlegen. blockedActionsPatterns (Wert „AWS Bewährte grundlegende Sicherheitsmethode

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			n“: kms: Entschlüs seln, kms:ReEnc ryptFrom). Die tatsächlichen Werte müssen den Richtlini en Ihrer Organisation entsprechen.
7.2.1	Festlegen von Zugriffskontrollsy stemen für Systemkomponenten, die den Zugriff anhand des Informati onsbedarfs eines Benutzers einschrän kt und auf „Alle ablehnen“ gesetzt ist, sofern der Zugriff nicht ausdrücklich zugelassen wird. Diese Zugriffsk ontrollsysteme müssen Folgendes enthalten: Abdeckung aller Systemkom ponenten.	iam-group-has-users-überprüfen	AWS Identity and Access Managemen t (IAM) kann Ihnen helfen, die Prinzipien der geringsten Rechte und der Aufgabent rennung mit Zugriffsb erechtigungen und Autorisierungen zu integrieren, indem sichergestellt wird, dass IAM-Gruppen mindestens einen Benutzer haben. Die Einteilung von Benutzern in Gruppen auf der Grundlage der ihnen zugewiese nen Berechtigungen oder ihrer Funktion ist eine Möglichkeit, das Prinzip der geringste n Berechtigung zu implementieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
7.2.1	Festlegen von Zugriffskontrollsystemen für Systemkomponenten, die den Zugriff anhand des Informationsbedarfs eines Benutzers einschränkt und auf „Alle ablehnen“ gesetzt ist, sofern der Zugriff nicht ausdrücklich zugelassen wird. Diese Zugriffskontrollsysteme müssen Folgendes enthalten: Abdeckung aller Systemkomponenten.	iam-inline-policy-blocked-kms-Aktionen	Stellen Sie sicher, dass ein Benutzer, eine IAM-Rolle oder eine IAM-Gruppe (AWS Identity and Access Management) nicht über eine Inline-Richtlinie verfügt, die blockierte Aktionen für alle AWS Schlüssel des Key Management Service zulässt. AWS empfiehlt, verwaltete Richtlinien anstelle von Inline-Richtlinien zu verwenden. Verwaltete Richtlinien ermöglichen Wiederverwendbarkeit, Versionsverwaltung, Rollback und Delegierung der Berechtigungsverwaltung. Mit dieser Regel können Sie den blockedActionsPatterns Parameter festlegen. (Wert „AWS Bewährte grundlegende Sicherheitsmethoden“: kms: Entschlüsseln, kms:ReEnc

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			ryptFrom). Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.
7.2.1	Festlegen von Zugriffskontrollsystemen für Systemkomponenten, die den Zugriff anhand des Informationsbedarfs eines Benutzers einschränkt und auf „Alle ablehnen“ gesetzt ist, sofern der Zugriff nicht ausdrücklich zugelassen wird. Diese Zugriffskontrollsysteme müssen Folgendes enthalten: Abdeckung aller Systemkomponenten.	iam-no-inline-policy-überprüfen	Stellen Sie sicher, dass ein Benutzer, eine IAM-Rolle oder eine IAM-Gruppe (AWS Identity and Access Management) nicht über eine Inline-Richtlinie zur Zugriffskontrolle auf Systeme und Ressourcen verfügt. AWS empfiehlt, verwaltete Richtlinien anstelle von Inline-Richtlinien zu verwenden. Verwaltete Richtlinien ermöglichen Wiederverwendbarkeit, Versionsverwaltung, Rollback und Delegierung der Berechtigungsverwaltung.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
7.2.1	Festlegen von Zugriffskontrollsystemen für Systemkomponenten, die den Zugriff anhand des Informationsbedarfs eines Benutzers einschränkt und auf „Alle ablehnen“ gesetzt ist, sofern der Zugriff nicht ausdrücklich zugelassen wird. Diese Zugriffskontrollsysteme müssen Folgendes enthalten: Abdeckung aller Systemkomponenten.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) kann Ihnen dabei helfen, die Prinzipien der geringsten Rechte und der Aufgabentrennung in Zugriffsberechtigungen und Autorisierungen zu integrieren und so zu verhindern, dass Richtlinien „Effect“: „Allow“ mit „Action“: „*“ anstelle von „Resource“: „*“ enthalten. Wenn Benutzern mehr Rechte eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und der Aufgabentrennung verstoßen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
7.2.1	Festlegen von Zugriffskontrollsystemen für Systemkomponenten, die den Zugriff anhand des Informationsbedarfs eines Benutzers einschränkt und auf „Alle ablehnen“ gesetzt ist, sofern der Zugriff nicht ausdrücklich zugelassen wird. Diese Zugriffskontrollsysteme müssen Folgendes enthalten: Abdeckung aller Systemkomponenten.	iam-policy-no-statements-with-full-access	Stellen Sie sicher, dass IAM-Aktionen nur auf die benötigten Aktionen beschränkt sind. Wenn Benutzern mehr Rechte eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Rechte und der Aufgabentrennung verstoßen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
7.2.1	Festlegen von Zugriffskontrollsystemen für Systemkomponenten, die den Zugriff anhand des Informationsbedarfs eines Benutzers einschränkt und auf „Alle ablehnen“ gesetzt ist, sofern der Zugriff nicht ausdrücklich zugelassen wird. Diese Zugriffskontrollsysteme müssen Folgendes enthalten: Abdeckung aller Systemkomponenten.	iam-root-access-key-überprüfen	Der Zugriff auf Systeme und Ressourcen kann gesteuert werden, indem überprüft wird, ob der Root-Benutzer keine Zugriffsschlüssel mit seiner AWS Identity and Access Management (IAM) -Rolle verknüpft hat. Stellen Sie sicher, dass die Root-Zugriffsschlüssel gelöscht werden. Erstellen und verwenden Sie stattdessen rollenbasierte Funktionen, AWS-Konten um das Prinzip der geringsten Funktionalität zu berücksichtigen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
7.2.1	Festlegen von Zugriffskontrollsystemen für Systemkomponenten, die den Zugriff anhand des Informationsbedarfs eines Benutzers einschränkt und auf „Alle ablehnen“ gesetzt ist, sofern der Zugriff nicht ausdrücklich zugelassen wird. Diese Zugriffskontrollsysteme müssen Folgendes enthalten: Abdeckung aller Systemkomponenten.	iam-user-group-membership-überprüfen	AWS Identity and Access Management (IAM) kann Ihnen helfen, Zugriffsberechtigungen und Autorisierungen einzuschränken, indem sichergestellt wird, dass Benutzer Mitglieder mindestens einer Gruppe sind. Wenn Benutzern mehr Berechtigungen eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und Aufgabentrennung verstoßen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
7.2.1	Festlegen von Zugriffskontrollsystemen für Systemkomponenten, die den Zugriff anhand des Informationsbedarfs eines Benutzers einschränkt und auf „Alle ablehnen“ gesetzt ist, sofern der Zugriff nicht ausdrücklich zugelassen wird. Diese Zugriffskontrollsysteme müssen Folgendes enthalten: Abdeckung aller Systemkomponenten.	iam-user-no-policies-überprüfen	Diese Regel stellt sicher, dass AWS Identity and Access Management (IAM) -Richtlinien nur Gruppen oder Rollen zugewiesen werden, um den Zugriff auf Systeme und Ressourcen zu kontrollieren. Die Zuweisung von Berechtigungen auf Gruppen- oder Rollenebene trägt dazu bei, die Wahrscheinlichkeit zu verringern, dass eine Identität übermäßige Berechtigungen erhält oder beibehält.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
7.2.1	Festlegen von Zugriffskontrollsystemen für Systemkomponenten, die den Zugriff anhand des Informationsbedarfs eines Benutzers einschränkt und auf „Alle ablehnen“ gesetzt ist, sofern der Zugriff nicht ausdrücklich zugelassen wird. Diese Zugriffskontrollsysteme müssen Folgendes enthalten: Abdeckung aller Systemkomponenten.	opensearch-access-control-enabled	Stellen Sie sicher, dass eine detaillierte Zugriffskontrolle für Ihre Amazon OpenSearch Service-Domains aktiviert ist. Eine differenzierte Zugriffskontrolle bietet erweiterte Autorisierungsmechanismen, um den Zugriff auf Amazon Service-Domains mit den geringsten Rechten zu erreichen. OpenSearch Es ermöglicht eine rollenbasierte Zugriffskontrolle auf die Domain sowie Sicherheit auf Index-, Dokument- und Feldebene, Unterstützung für OpenSearch Service-Dashboards, Mehrmandantenfähigkeit und HTTP-Basisauthentifizierung für Service und Kibana. OpenSearch

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
7.2.2	Festlegen von Zugriffskontrollsystemen für Systemkomponenten, die den Zugriff anhand des Informationsbedarfs eines Benutzers einschränkt und auf „Alle ablehnen“ gesetzt ist, sofern der Zugriff nicht ausdrücklich zugelassen wird. Dieses Zugriffskontrollsystem/diese Zugriffskontrollsysteme muss/müssen Folgendes beinhalten: Zuweisung von Rechten an Personen auf der Grundlage der Berufsklassifizierung und Funktion.	ecs-containers-nonprivileged	Um die Implementierung des Prinzips der geringsten Berechtigung zu unterstützen, dürfen in Amazon Elastic Container Service (Amazon ECS)-Aufgabendefinitionen keine erhöhten Berechtigungen aktiviert sein. Wenn dieser Parameter den Wert „true“ aufweist, erhält der Container erhöhte Berechtigungen auf der Host-Container-Instance (ähnlich wie der Root-Benutzer).

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
7.2.2	Festlegen von Zugriffskontrollsystemen für Systemkomponenten, die den Zugriff anhand des Informationsbedarfs eines Benutzers einschränkt und auf „Alle ablehnen“ gesetzt ist, sofern der Zugriff nicht ausdrücklich zugelassen wird. Dieses Zugriffskontrollsystem/diese Zugriffskontrollsysteme muss/müssen Folgendes beinhalten: Zuweisung von Rechten an Personen auf der Grundlage der Berufsklassifizierung und Funktion.	ecs-containers-readonly-access	Die Aktivierung des schreibgeschützten Zugriffs auf Amazon Elastic Container Service (ECS)-Container kann dazu beitragen, das Prinzip der geringsten Berechtigung einzuhalten. Diese Option kann Angriffsvektoren reduzieren, da das Dateisystem der Container-Instance nur geändert werden kann, wenn es über ausdrückliche Lese- und Schreibberechtigungen verfügt.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
7.2.2	Festlegen von Zugriffskontrollsystemen für Systemkomponenten, die den Zugriff anhand des Informationsbedarfs eines Benutzers einschränkt und auf „Alle ablehnen“ gesetzt ist, sofern der Zugriff nicht ausdrücklich zugelassen wird. Dieses Zugriffskontrollsystem/diese Zugriffskontrollsysteme muss/müssen Folgendes beinhalten: Zuweisung von Rechten an Personen auf der Grundlage der Berufsklassifizierung und Funktion.	efs-access-point-enforce-Stammverzeichnis	Die Durchsetzung eines Stammverzeichnisses für einen Amazon-Elastic-File-System (Amazon-EFS)-Zugangspunkt trägt dazu bei, den Datenzugriff einzuschränken, indem sichergestellt wird, dass Benutzer des Zugangspunkts nur auf Dateien des angegebenen Unterverzeichnisses zugreifen können.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
7.2.2	Festlegen von Zugriffskontrollsystemen für Systemkomponenten, die den Zugriff anhand des Informationsbedarfs eines Benutzers einschränkt und auf „Alle ablehnen“ gesetzt ist, sofern der Zugriff nicht ausdrücklich zugelassen wird. Dieses Zugriffskontrollsystem/diese Zugriffskontrollsysteme muss/müssen Folgendes beinhalten: Zuweisung von Rechten an Personen auf der Grundlage der Berufsklassifizierung und Funktion.	efs-access-point-enforce-Benutzeridentität	Um die Implementierung des Prinzips der geringsten Rechte zu unterstützen, stellen Sie sicher, dass die Benutzerdurchsetzung für Ihr Amazon Elastic File System (Amazon EFS) aktiviert ist. Wenn diese Option aktiviert ist, ersetzt Amazon EFS den Benutzer und die Gruppe IDs des NFS-Clients durch die Identität, die auf dem Access Point für alle Dateisystemoperationen konfiguriert ist, und gewährt nur Zugriff auf diese erzwungene Benutzeridentität.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
7.2.2	Festlegen von Zugriffskontrollsystemen für Systemkomponenten, die den Zugriff anhand des Informationsbedarfs eines Benutzers einschränkt und auf „Alle ablehnen“ gesetzt ist, sofern der Zugriff nicht ausdrücklich zugelassen wird. Dieses Zugriffskontrollsystem/diese Zugriffskontrollsysteme muss/müssen Folgendes beinhalten: Zuweisung von Rechten an Personen auf der Grundlage der Berufsklassifizierung und Funktion.	emr-kerberos-enabled	Die Zugriffsberechtigungen und -autorisierungen können verwaltet und nach den Prinzipien der geringsten Berechtigung und Aufgabentrennung integriert werden, indem Kerberos für Amazon-EMR-Cluster aktiviert wird. In Kerberos werden Services und Benutzer, die sich authentifizieren müssen, als Prinzipale bezeichnet. Prinzipale befinden sich in einem Kerberos-Bereich. Innerhalb dieses Bereichs wird ein Kerberos-Server als Key Distribution Center (KDC) bezeichnet. Über diesen Server können sich Prinzipale authentifizieren. Die Authentifizierung im KDC erfolgt durch die Ausstellung von Authentif

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			izierungstickets. Das KDC unterhält eine Datenbank der Prinzipale in seinem Bereich mit ihren Passwörtern und anderen administr ativen Informationen zu jedem Prinzipal.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
7.2.2	Festlegen von Zugriffskontrollsystemen für Systemkomponenten, die den Zugriff anhand des Informationsbedarfs eines Benutzers einschränkt und auf „Alle ablehnen“ gesetzt ist, sofern der Zugriff nicht ausdrücklich zugelassen wird. Dieses Zugriffskontrollsystem/diese Zugriffskontrollsysteme muss/müssen Folgendes beinhalten: Zuweisung von Rechten an Personen auf der Grundlage der Berufsklassifizierung und Funktion.	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) kann Ihnen helfen, die Prinzipien der geringsten Rechte und der Aufgabentrennung in Zugriffsberechtigungen und Autorisierungen zu integrieren und so zu verhindern, dass Richtlinien blockierte Aktionen für alle AWS Schlüssel des Key Management Service enthalten. Wenn Benutzer mehr Rechte haben, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und Aufgabentrennung verstoßen. Mit dieser Regel können Sie den Parameter festlegen. blockedActionsPatterns (Wert „AWS Bewährte grundlegende Sicherheitsmethode

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			n“: kms: Entschlüs seln, kms:ReEnc ryptFrom). Die tatsächlichen Werte müssen den Richtlini en Ihrer Organisation entsprechen.
7.2.2	Festlegen von Zugriffskontrollsy stemen für Systemkomponenten, die den Zugriff anhand des Informati onsbedarfs eines Benutzers einschrän kt und auf „Alle ablehnen“ gesetzt ist, sofern der Zugriff nicht ausdrücklich zugelassen wird. Dieses Zugriffsk ontrollsystem/dies e Zugriffskontrollsy steme muss/müssen Folgendes beinhalte n: Zuweisung von Rechten an Personen auf der Grundlage der Berufsklassifizierung und Funktion.	iam-group-has-users-überprüfen	AWS Identity and Access Managemen t (IAM) kann Ihnen helfen, die Prinzipien der geringsten Rechte und der Aufgabent rennung mit Zugriffsb erechtigungen und Autorisierungen zu integrieren, indem sichergestellt wird, dass IAM-Gruppen mindestens einen Benutzer haben. Die Einteilung von Benutzern in Gruppen auf der Grundlage der ihnen zugewiese nen Berechtigungen oder ihrer Funktion ist eine Möglichkeit, das Prinzip der geringste n Berechtigung zu implementieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
7.2.2	Festlegen von Zugriffskontrollsystemen für Systemkomponenten, die den Zugriff anhand des Informationsbedarfs eines Benutzers einschränkt und auf „Alle ablehnen“ gesetzt ist, sofern der Zugriff nicht ausdrücklich zugelassen wird. Dieses Zugriffskontrollsystem/diese Zugriffskontrollsysteme muss/müssen Folgendes beinhalten: Zuweisung von Rechten an Personen auf der Grundlage der Berufsklassifizierung und Funktion.	iam-inline-policy-blocked-kms-Aktionen	Stellen Sie sicher, dass ein Benutzer, eine IAM-Rolle oder eine IAM-Gruppe (AWS Identity and Access Management) nicht über eine Inline-Richtlinie verfügt, die blockierte Aktionen für alle AWS Schlüssel des Key Management Service zulässt. AWS empfiehlt, verwaltete Richtlinien anstelle von Inline-Richtlinien zu verwenden. Verwaltete Richtlinien ermöglichen Wiederverwendbarkeit, Versionsverwaltung, Rollback und Delegierung der Berechtigungsverwaltung. Mit dieser Regel können Sie den blockedActionsPatterns Parameter festlegen. (Wert „AWS Bewährte grundlegende Sicherheitsmethoden“: kms: Entschlüsseln, kms:ReEnc

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			ryptFrom). Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.
7.2.2	Festlegen von Zugriffskontrollsystemen für Systemkomponenten, die den Zugriff anhand des Informationsbedarfs eines Benutzers einschränkt und auf „Alle ablehnen“ gesetzt ist, sofern der Zugriff nicht ausdrücklich zugelassen wird. Dieses Zugriffskontrollsystem/diese Zugriffskontrollsysteme muss/müssen Folgendes beinhalten: Zuweisung von Rechten an Personen auf der Grundlage der Berufsklassifizierung und Funktion.	iam-no-inline-policy-überprüfen	Stellen Sie sicher, dass ein Benutzer, eine IAM-Rolle oder eine IAM-Gruppe (AWS Identity and Access Management) nicht über eine Inline-Richtlinie zur Zugriffskontrolle auf Systeme und Ressourcen verfügt. AWS empfiehlt, verwaltete Richtlinien anstelle von Inline-Richtlinien zu verwenden. Verwaltete Richtlinien ermöglichen Wiederverwendbarkeit, Versionsverwaltung, Rollback und Delegierung der Berechtigungsverwaltung.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
7.2.2	Festlegen von Zugriffskontrollsystemen für Systemkomponenten, die den Zugriff anhand des Informationsbedarfs eines Benutzers einschränkt und auf „Alle ablehnen“ gesetzt ist, sofern der Zugriff nicht ausdrücklich zugelassen wird. Dieses Zugriffskontrollsystem/diese Zugriffskontrollsysteme muss/müssen Folgendes beinhalten: Zuweisung von Rechten an Personen auf der Grundlage der Berufsklassifizierung und Funktion.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) kann Ihnen dabei helfen, die Prinzipien der geringsten Rechte und der Aufgabentrennung in Zugriffsberechtigungen und Autorisierungen zu integrieren und so zu verhindern, dass Richtlinien „Effect“: „Allow“ mit „Action“: „*“ anstelle von „Resource“: „*“ enthalten. Wenn Benutzern mehr Rechte eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und der Aufgabentrennung verstoßen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
7.2.2	Festlegen von Zugriffskontrollsystemen für Systemkomponenten, die den Zugriff anhand des Informationsbedarfs eines Benutzers einschränkt und auf „Alle ablehnen“ gesetzt ist, sofern der Zugriff nicht ausdrücklich zugelassen wird. Dieses Zugriffskontrollsystem/diese Zugriffskontrollsysteme muss/müssen Folgendes beinhalten: Zuweisung von Rechten an Personen auf der Grundlage der Berufsklassifizierung und Funktion.	iam-policy-no-statements-with-full-access	Stellen Sie sicher, dass IAM-Aktionen nur auf die benötigten Aktionen beschränkt sind. Wenn Benutzern mehr Rechte eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Rechte und der Aufgabentrennung verstoßen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
7.2.2	Festlegen von Zugriffskontrollsystemen für Systemkomponenten, die den Zugriff anhand des Informationsbedarfs eines Benutzers einschränkt und auf „Alle ablehnen“ gesetzt ist, sofern der Zugriff nicht ausdrücklich zugelassen wird. Dieses Zugriffskontrollsystem/diese Zugriffskontrollsysteme muss/müssen Folgendes beinhalten: Zuweisung von Rechten an Personen auf der Grundlage der Berufsklassifizierung und Funktion.	iam-root-access-key-überprüfen	Der Zugriff auf Systeme und Ressourcen kann gesteuert werden, indem überprüft wird, ob der Root-Benutzer keine Zugriffsschlüssel mit seiner AWS Identity and Access Management (IAM) -Rolle verknüpft hat. Stellen Sie sicher, dass die Root-Zugriffsschlüssel gelöscht werden. Erstellen und verwenden Sie stattdessen rollenbasierte Funktionen, AWS-Konten um das Prinzip der geringsten Funktionalität zu berücksichtigen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
7.2.2	Festlegen von Zugriffskontrollsystemen für Systemkomponenten, die den Zugriff anhand des Informationsbedarfs eines Benutzers einschränkt und auf „Alle ablehnen“ gesetzt ist, sofern der Zugriff nicht ausdrücklich zugelassen wird. Dieses Zugriffskontrollsystem/diese Zugriffskontrollsysteme muss/müssen Folgendes beinhalten: Zuweisung von Rechten an Personen auf der Grundlage der Berufsklassifizierung und Funktion.	iam-user-group-membership-überprüfen	AWS Identity and Access Management (IAM) kann Ihnen helfen, Zugriffsberechtigungen und Autorisierungen einzuschränken, indem sichergestellt wird, dass Benutzer Mitglieder mindestens einer Gruppe sind. Wenn Benutzern mehr Berechtigungen eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und Aufgabentrennung verstoßen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
7.2.2	Festlegen von Zugriffskontrollsystemen für Systemkomponenten, die den Zugriff anhand des Informationsbedarfs eines Benutzers einschränkt und auf „Alle ablehnen“ gesetzt ist, sofern der Zugriff nicht ausdrücklich zugelassen wird. Dieses Zugriffskontrollsystem/diese Zugriffskontrollsysteme muss/müssen Folgendes beinhalten: Zuweisung von Rechten an Personen auf der Grundlage der Berufsklassifizierung und Funktion.	iam-user-no-policies-überprüfen	Diese Regel stellt sicher, dass AWS Identity and Access Management (IAM)-Richtlinien nur Gruppen oder Rollen zugewiesen werden, um den Zugriff auf Systeme und Ressourcen zu kontrollieren. Die Zuweisung von Berechtigungen auf Gruppen- oder Rollenebene trägt dazu bei, die Wahrscheinlichkeit zu verringern, dass eine Identität übermäßige Berechtigungen erhält oder beibehält.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
7.2.2	Festlegen von Zugriffskontrollsystemen für Systemkomponenten, die den Zugriff anhand des Informationsbedarfs eines Benutzers einschränkt und auf „Alle ablehnen“ gesetzt ist, sofern der Zugriff nicht ausdrücklich zugelassen wird. Dieses Zugriffskontrollsystem/diese Zugriffskontrollsysteme muss/müssen Folgendes beinhalten: Zuweisung von Rechten an Personen auf der Grundlage der Berufsklassifizierung und Funktion.	opensearch-access-control-enabled	Stellen Sie sicher, dass eine detaillierte Zugriffskontrolle für Ihre Amazon OpenSearch Service-Domains aktiviert ist. Eine differenzierte Zugriffskontrolle bietet erweiterte Autorisierungsmechanismen, um den Zugriff auf Amazon Service-Domains mit den geringsten Rechten zu erreichen. OpenSearch Es ermöglicht eine rollenbasierte Zugriffskontrolle auf die Domain sowie Sicherheit auf Index-, Dokument- und Feldebene, Unterstützung für OpenSearch Service-Dashboards, Mehrmandantenfähigkeit und HTTP-Basisauthentifizierung für Service und Kibana. OpenSearch

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
7.2.3	Standardeinstellung „Deny-All“.	s-3 bucket-acl-prohibited	Diese Regel prüft, ob Access Control Lists (ACLs) für die Zugriffskontrolle auf Amazon S3 S3-Buckets verwendet werden. ACLs sind veraltete Zugriffskontrollmechanismen für Amazon S3 S3-Buckets, die älter sind als AWS Identity and Access Management (IAM). Stattdessen empfiehlt es sich ACLs, IAM-Richtlinien oder S3-Bucket-Richtlinien zu verwenden, um den Zugriff auf Ihre S3-Buckets einfacher zu verwalten.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
8.1.1	Weisen Sie allen Benutzern eine eindeutige ID zu, bevor Sie ihnen Zugriff auf Systemkomponenten oder Karteninh aberdaten gewähren.	iam-root-access-key-überprüfen	Der Zugriff auf Systeme und Ressourcen kann gesteuert werden, indem überprüft wird, ob der Root-Benu tzer keine Zugriffss chlüssel mit seiner AWS Identity and Access Management (IAM) -Rolle verknüpft hat. Stellen Sie sicher, dass die Root-Zugr iffsschlüssel gelöscht werden. Erstellen und verwenden Sie stattdessen rollenbas ierte Funktionen, AWS-Konten um das Prinzip der geringste n Funktionalität zu berücksichtigen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
8.1.4	Entfernen/deaktivieren Sie inaktive Benutzerkonten innerhalb von 90 Tagen.	iam-user-unused-credentials-überprüfen	AWS Identity and Access Management (IAM) kann Ihnen bei Zugriffsberechtigungen und Autorisierungen helfen, indem es nach IAM-Passwörtern und Zugriffsschlüsseln sucht, die für einen bestimmten Zeitraum nicht verwendet wurden. Wenn ungenutzte Anmeldeinformationen identifiziert werden, müssen Sie sie deaktivieren und/oder entfernen, da dies gegen das Prinzip der geringsten Berechtigung verstoßen könnte. Für diese Regel müssen Sie einen Wert für das maxCredentialUsage Alter festlegen (Standardkonfiguration: 90). Der tatsächliche Wert muss den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
8.2.1	Unter Verwendung einer starken Kryptographie werden alle Authentifizierungsdaten (wie Passwörter/Phrasen) während der Übertragung und Speicherung auf allen Systemkomponenten unlesbar gemacht.	codebuild-project-environment-privileged-überprüfen	Um Sie bei der Implementierung des Prinzips der geringsten Rechte zu unterstützen, stellen Sie sicher, dass in Ihrer CodeBuild Amazon-Projektumgebung der privilegierte Modus nicht aktiviert ist. Diese Einstellung sollte deaktiviert werden, um unbeabsichtigten Zugriff auf Docker APIs sowie auf die dem Container zugrunde liegende Hardware zu verhindern.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
8.2.1	Unter Verwendung einer starken Kryptographie werden alle Authentifizierungsdaten (wie Passwörter/Phrasen) während der Übertragung und Speicherung auf allen Systemkomponenten unlesbar gemacht.	ecs-no-environment-secrets	Als bewährte Methode für Sicherheit übergibt sensible Informationen als Umgebungsvariablen an Container. Sie können Daten sicher in Ihre Amazon Elastic Container Service (ECS) -Container einfügen, indem Sie auf Werte verweisen, die in AWS Systems Manager Parameter Store oder AWS Secrets Manager in der Container-Definition einer Amazon ECS-Aufgabendefinition gespeichert sind. Anschließend können Sie Ihre vertraulichen Informationen als Umgebungsvariablen oder in der Protokollkonfiguration eines Containers verfügbar machen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
8.2.1	Unter Verwendung einer starken Kryptographie werden alle Authentifizierungsdaten (wie Passwörter/Phrasen) während der Übertragung und Speicherung auf allen Systemkomponenten unlesbar gemacht.	alb-http-to-https-Umleitungsprüfung	Um Daten während der Übertragung zu schützen, stellen Sie sicher, dass Ihr Application Load Balancer unverschlüsselte HTTP-Anfragen automatisch an HTTPS umleitet. Da sensible Daten vorhanden sein können, sollten Sie die Verschlüsselung bei der Übertragung aktivieren, um diese Daten zu schützen.
8.2.1	Unter Verwendung einer starken Kryptographie werden alle Authentifizierungsdaten (wie Passwörter/Phrasen) während der Übertragung und Speicherung auf allen Systemkomponenten unlesbar gemacht.	api-gw-ssl-enabled	Stellen Sie sicher, dass die REST-API-Stufen von Amazon API Gateway mit SSL-Zertifikaten konfiguriert sind, damit Backend-Systeme überprüfen können, ob Anforderungen von API Gateway stammen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
8.2.1	Unter Verwendung einer starken Kryptographie werden alle Authentifizierungsdaten (wie Passwörter/Phrasen) während der Übertragung und Speicherung auf allen Systemkomponenten unlesbar gemacht.	ec2- ebs-encryption-by-default	Zum Schutz von Daten im Ruhezustand müssen Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon Elastic Block Store (Amazon EBS)-Volumes aktiviert ist. Da sensible Daten in diesen Volumes gespeichert werden können, sollten Sie die Verschlüsselung von Daten im Ruhezustand aktivieren, um diese Daten zu schützen.
8.2.1	Unter Verwendung einer starken Kryptographie werden alle Authentifizierungsdaten (wie Passwörter/Phrasen) während der Übertragung und Speicherung auf allen Systemkomponenten unlesbar gemacht.	efs-encrypted-check	Aktivieren Sie die Verschlüsselung für Ihr Amazon Elastic File System (EFS), um eventuell vorhandene sensible Daten sowie Daten im Ruhezustand zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
8.2.1	Unter Verwendung einer starken Kryptographie werden alle Authentifizierungsdaten (wie Passwörter/Phrasen) während der Übertragung und Speicherung auf allen Systemkomponenten unlesbar gemacht.	elasticsearch-encrypted-at-rest	Da sensible Daten vorhanden sein können und um Daten im Ruhezustand zu schützen, sollten Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon OpenSearch Service (OpenSearch Service)-Domains aktiviert ist.
8.2.1	Unter Verwendung einer starken Kryptographie werden alle Authentifizierungsdaten (wie Passwörter/Phrasen) während der Übertragung und Speicherung auf allen Systemkomponenten unlesbar gemacht.	elb-tls-https-listeners-nur	Stellen Sie sicher, dass Ihre Elastic Load Balancer (ELBs) mit SSL- oder HTTPS-Listenern konfiguriert sind. Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
8.2.1	Unter Verwendung einer starken Kryptographie werden alle Authentifizierungsdaten (wie Passwörter/Phrasen) während der Übertragung und Speicherung auf allen Systemkomponenten unlesbar gemacht.	encrypted-volumes	Aktivieren Sie die Verschlüsselung für Ihre Amazon-Elastic-Block-Store-(Amazon-EBS-)Volumes, um eventuell vorhandene sensible Daten sowie Daten im Ruhezustand zu schützen.
8.2.1	Unter Verwendung einer starken Kryptographie werden alle Authentifizierungsdaten (wie Passwörter/Phrasen) während der Übertragung und Speicherung auf allen Systemkomponenten unlesbar gemacht.	opensearch-encrypted-at-rest	Da sensible Daten vorhanden sein können und um Daten im Ruhezustand zu schützen, sollten Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon OpenSearch Service-Domains aktiviert ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
8.2.1	Unter Verwendung einer starken Kryptographie werden alle Authentifizierungsdaten (wie Passwörter/Phrasen) während der Übertragung und Speicherung auf allen Systemkomponenten unlesbar gemacht.	rds-snapshot-encrypted	Stellen Sie sicher, dass die Verschlüsselung für Ihre Amazon Relational Database Service (Amazon RDS)-Snapshots aktiviert ist. Da sensible Daten auch im Ruhezustand vorhanden sein können, sollten Sie die Verschlüsselung von Daten im Ruhezustand aktivieren, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
8.2.1	Unter Verwendung einer starken Kryptographie werden alle Authentifizierungsdaten (wie Passwörter/Phrasen) während der Übertragung und Speicherung auf allen Systemkomponenten unlesbar gemacht.	rds-storage-encrypted	Zum Schutz von Daten im Ruhezustand müssen Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon Relational Database Service (Amazon RDS)-Instances aktiviert ist. Da sensible Daten in Amazon-RDS-Instances gespeichert werden können, sollten Sie die Verschlüsselung von Daten im Ruhezustand aktivieren, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
8.2.1	Unter Verwendung einer starken Kryptographie werden alle Authentifizierungsdaten (wie Passwörter/Phrasen) während der Übertragung und Speicherung auf allen Systemkomponenten unlesbar gemacht.	redshift-cluster-configuration-check	Um Daten im Ruhezustand zu schützen, muss die Verschlüsselung für Ihre Amazon-Redshift-Cluster aktiviert sein. Sie müssen auch sicherstellen, dass die erforderlichen Konfigurationen auf Amazon-Redshift-Clustern bereitgestellt werden. Die Prüfungsprotokollierung muss aktiviert sein, um Informationen zu Verbindungen und Benutzeraktivitäten in der Datenbank bereitzustellen. Diese Regel erfordert, dass ein Wert für clusterDbEncrypted (Config Default: TRUE) und LoggingEnabled (Config Default: TRUE) gesetzt ist. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
8.2.1	Unter Verwendung einer starken Kryptographie werden alle Authentifizierungsdaten (wie Passwörter/Phrasen) während der Übertragung und Speicherung auf allen Systemkomponenten unlesbar gemacht.	s3-aktiviert bucket-server-side-encryption	Zum Schutz von Daten im Ruhezustand müssen Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon Simple Storage Service (Amazon S3)-Buckets aktiviert ist. Da sensible Daten in Amazon S3 Buckets gespeichert werden können, sollten Sie die Verschlüsselung aktivieren, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
8.2.1	Unter Verwendung einer starken Kryptographie werden alle Authentifizierungsdaten (wie Passwörter/Phrasen) während der Übertragung und Speicherung auf allen Systemkomponenten unlesbar gemacht.	s-3 bucket-ssl-requests-only	Um Daten während der Übertragung zu schützen, stellen Sie sicher, dass Ihre Amazon Simple Storage Service (Amazon S3)-Buckets Anfragen zur Verwendung von Secure Socket Layer (SSL)-Buckets erfordern. Da sensible Daten vorhanden sein können, sollten Sie die Verschlüsselung bei der Übertragung aktivieren, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
8.2.1	Unter Verwendung einer starken Kryptographie werden alle Authentifizierungsdaten (wie Passwörter/Phrasen) während der Übertragung und Speicherung auf allen Systemkomponenten unlesbar gemacht.	s-3 default-encryption-kms	Stellen Sie sicher, dass die Verschlüsselung für Ihre Amazon Simple Storage Service (Amazon S3)-Buckets aktiviert ist. Da sensible Daten in einem Amazon S3 Bucket gespeichert werden können, sollten Sie die Verschlüsselung im Ruhezustand aktivieren, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
8.2.1	Unter Verwendung einer starken Kryptographie werden alle Authentifizierungsdaten (wie Passwörter/Phrasen) während der Übertragung und Speicherung auf allen Systemkomponenten unlesbar gemacht.	sagemaker-endpoint-configuration-kms-key-konfiguriert	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass die Verschlüsselung mit dem AWS Key Management Service (AWS KMS) für Ihren Endpunkt aktiviert ist. SageMaker Da sensible Daten auf dem SageMaker Endgerät gespeichert werden können, sollten Sie die Verschlüsselung im Ruhezustand aktivieren, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
8.2.1	Unter Verwendung einer starken Kryptographie werden alle Authentifizierungsdaten (wie Passwörter/Phrasen) während der Übertragung und Speicherung auf allen Systemkomponenten unlesbar gemacht.	sagemaker-notebook-instance-kms-schlüsselkonfiguriert	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass die Verschlüsselung mit dem AWS Key Management Service (AWS KMS) für Ihr Notebook aktiviert ist. SageMaker Da vertrauliche Daten im SageMaker Notebook gespeichert werden können, sollten Sie die Verschlüsselung im Ruhezustand aktivieren, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
8.2.1	Unter Verwendung einer starken Kryptographie werden alle Authentifizierungsdaten (wie Passwörter/Phrasen) während der Übertragung und Speicherung auf allen Systemkomponenten unlesbar gemacht.	secretsmanager-using-cmk	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass die Verschlüsselung mit dem AWS Key Management Service (AWS KMS) für AWS Secrets Manager aktiviert ist. Aktivieren Sie die Verschlüsselung von Daten im Ruhezustand, um eventuell vorhandene sensible Daten im Ruhezustand im Secrets Manager zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
8.2.1	Unter Verwendung einer starken Kryptographie werden alle Authentifizierungsdaten (wie Passwörter/Phrasen) während der Übertragung und Speicherung auf allen Systemkomponenten unlesbar gemacht.	sns-encrypted-kms	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass Ihre Amazon Simple Notification Service (Amazon SNS) -Themen mit dem AWS Key Management Service (AWS KMS) verschlüsselt werden müssen. Um eventuell vorhandene sensible Daten im Ruhezustand in veröffentlichten Nachrichten zu schützen, muss die Verschlüsselung von Daten im Ruhezustand aktiviert sein.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
8.2.3	Kennwörter/Passphrasen müssen folgende Bedingungen erfüllen: • Sie müssen mindestens sieben Zeichen lang sein. • Enthalten sowohl numerische als auch alphabetische Zeichen. Alternativ müssen die Kennwörter/Passphrasen eine Komplexität und Stärke aufweisen, die mindestens den oben angegebenen Parametern entsprechen.	iam-password-policy	Die Identitäten und Anmeldeinformationen werden auf der Grundlage einer organisatorischen IAM-Passwortrichtlinie ausgestellt, verwaltet und verifiziert. Sie erfüllen oder übertreffen die Anforderungen von NIST SP 800-63 und dem Standard „Best Practices“ von AWS Foundational Security für die Passwortstärke. Mit dieser Regel können Sie optional RequireUppercaseCharacters (PCI DSS-Standard: falsch), RequireLowercaseCharacters (PCI DSS-Standard: true), RequireSymbols (PCI DSS-Standard: falsch), RequireNumbers (PCI DSS-Standard: true), MinimumPasswordLength (PCI DSS-Standard: 7), PasswordReusePreve

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			ntion (PCI DSS-Standard: 4) und MaxPasswordAge (PCI DSS-Standard: 90) für Ihre IAM-Passwortrichtlinie festlegen. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
8.2.4	Ändern Sie Benutzerpasswörter/Passphrasen mindestens alle 90 Tage.	access-keys-rotated	Die Anmeldeinformationen für autorisierte Geräte, Benutzer und Prozesse werden geprüft, indem sichergestellt wird, dass die IAM-Zugriffsschlüssel gemäß den Vorgaben der Unternehmensrichtlinie rotiert werden. Das regelmäßige Ändern der Zugriffsschlüssel ist eine bewährte Sicherheitsmethode. Es verkürzt den Zeitraum, in dem ein Zugriffsschlüssel aktiv ist, und reduziert die Auswirkungen auf das Unternehmen, wenn die Schlüssel kompromittiert werden. Diese Regel erfordert einen Wert für die Zugriffsschlüssel-Rotation (Standardkonfiguration: 90). Der tatsächliche Wert muss den Richtlini

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			en Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
8.2.4	Ändern Sie Benutzerpasswörter/Passphrasen mindestens alle 90 Tage.	iam-password-policy	Die Identitäten und Anmeldeinformationen werden auf der Grundlage einer organisatorischen IAM-Passwortrichtlinie ausgestellt, verwaltet und verifiziert. Sie erfüllen oder übertreffen die Anforderungen von NIST SP 800-63 und dem Standard „Best Practices“ von AWS Foundational Security für die Passwortstärke. Mit dieser Regel können Sie optional RequireUppercaseCharacters (PCI DSS-Standard: falsch), RequireLowercaseCharacters (PCI DSS-Standard: true), RequireSymbols (PCI DSS-Standard: falsch), RequireNumbers (PCI DSS-Standard: true), MinimumPasswordLength (PCI DSS-Standard: 7), PasswordReusePreve

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			ntion (PCI DSS-Standard: 4) und MaxPasswordAge (PCI DSS-Standard: 90) für Ihre IAM-Passwortrichtlinie festlegen. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.
8.2.4	Ändern Sie Benutzerpasswörter/Passphrasen mindestens alle 90 Tage.	secretsmanager-rotation-enabled-check	Diese Regel stellt sicher, dass bei AWS Secrets Manager Manager-Geheimnissen die Rotation aktiviert ist. Die regelmäßige Rotation von Secrets kann den Zeitraum verkürzen, in dem ein Secret aktiv ist, und möglicherweise die Auswirkungen auf das Unternehmen verringern, falls das Secret kompromittiert wird.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
8.2.5	Erlauben Sie einer Person nicht, ein neues, password/passphrase that is the same as any of the last four passwords /passphrases von ihr verwendetes Dokument einzureichen.	iam-password-policy	Die Identitäten und Anmeldeinformationen werden auf der Grundlage einer organisatorischen IAM-Passwortrichtlinie ausgestellt, verwaltet und verifiziert. Sie erfüllen oder übertreffen die Anforderungen von NIST SP 800-63 und dem Standard „Best Practices“ von AWS Foundational Security für die Passwortstärke. Mit dieser Regel können Sie optional RequireUppercaseCharacters (PCI DSS-Standard: falsch), RequireLowercaseCharacters (PCI DSS-Standard: true), RequireSymbols (PCI DSS-Standard: falsch), RequireNumbers (PCI DSS-Standard: true), MinimumPasswordLength (PCI DSS-Standard: 7), PasswordReusePreve

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			ntion (PCI DSS-Standard: 4) und MaxPasswordAge (PCI DSS-Standard: 90) für Ihre IAM-Passwortrichtlinie festlegen. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.
8.3.1	Integrieren Sie Multi-Factor Authentication für alle Nicht-Konsolenzugriffe in die Karteninhaberdaten-Umgebung (CDE) für Personal mit Administratorzugriff.	iam-user-mfa-enabled	Aktivieren Sie diese Regel, um den Zugriff auf Ressourcen in der Cloud einzuschränken. AWS Diese Regel stellt sicher, dass die Multi-Faktor-Authentifizierung (MFA) für alle Benutzer aktiviert ist. MFA bietet eine weitere Schutzebene zusätzlich zum Benutzernamen und Passwort. Reduzieren Sie Fälle von kompromittierten Konten, indem Sie MFA für Benutzer vorschreiben.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
8.3.1	Integrieren Sie Multi-Factor Authentication für alle Nicht-Konsolenzugriffe in die Karteninhaberdaten-Umgebung (CDE) für Personal mit Administratorzugriff.	mfa-enabled-for-iam-Konsolenzugriff	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass MFA für alle AWS Identity and Access Management (IAM) -Benutzer aktiviert ist, die über ein Konsolenkennwort verfügen. MFA bietet eine weitere Schutzebene zusätzlich zum Benutzernamen und Passwort. Indem Sie MFA für Benutzer vorschreiben, können Sie Fälle kompromittierter Konten reduzieren und verhindern, dass unbefugte Benutzer auf vertrauliche Daten zugreifen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
8.3.1	Integrieren Sie Multi-Factor Authentication für alle Nicht-Konsolenzugriffe in die Karteninhaberdaten-Umgebung (CDE) für Personal mit Administratorzugriff.	root-account-hardware-mfa-aktiviert	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Hardware-MFA für den Root-Benutzer aktiviert ist. Der Stammbenutzer ist der AWS-Konto-Benutzer mit den meisten Berechtigungen. MFA bietet eine weitere Schutzebene zusätzlich zum Benutzernamen und Passwort. Indem Sie MFA für den Root-Benutzer vorschreiben, können Sie die Anzahl AWS-Konten kompromittierter Benutzer reduzieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
8.3.1	Integrieren Sie Multi-Factor Authentication für alle Nicht-Konsolenzugriffe in die Karteninhaberdaten-Umgebung (CDE) für Personal mit Administratorzugriff.	root-account-mfa-enabled	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass MFA für den Root-Benutzer aktiviert ist. Der Stammbenutzer ist der AWS-Konto-Benutzer mit den meisten Berechtigungen. MFA bietet eine weitere Schutzebene zusätzlich zum Benutzernamen und Passwort. Indem Sie MFA für den Root-Benutzer vorschreiben, können Sie die Anzahl AWS-Konten kompromittierter Benutzer reduzieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
8.3.2	Integrieren Sie eine Multi-Faktor-Authentifizierung für alle Remote-Netzwerkzugriffe (sowohl Benutzer als auch Administrator, einschließlich Zugriff durch Dritte zu Support- oder Wartungszwecken), die von außerhalb des Unternehmensnetzwerks erfolgen.	iam-user-mfa-enabled	Aktivieren Sie diese Regel, um den Zugriff auf Ressourcen in der AWS Cloud einzuschränken. Diese Regel stellt sicher, dass die Multi-Faktor-Authentifizierung (MFA) für alle Benutzer aktiviert ist. MFA bietet eine weitere Schutzebene zusätzlich zum Benutzernamen und Passwort. Reduzieren Sie Fälle von kompromittierten Konten, indem Sie MFA für Benutzer vorschreiben.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
8.3.2	Integrieren Sie eine Multi-Faktor-Authentifizierung für alle Remote-Netzwerkzugriffe (sowohl Benutzer als auch Administrator, einschließlich Zugriff durch Dritte zu Support- oder Wartungszwecken), die von außerhalb des Unternehmensnetzwerks erfolgen.	mfa-enabled-for-iam-Konsolenzugriff	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass MFA für alle AWS Identity and Access Management (IAM) -Benutzer aktiviert ist, die über ein Konsolenkennwort verfügen. MFA bietet eine weitere Schutzebene zusätzlich zum Benutzernamen und Passwort. Indem Sie MFA für Benutzer vorschreiben, können Sie Fälle kompromittierter Konten reduzieren und verhindern, dass unbefugte Benutzer auf vertrauliche Daten zugreifen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
8.3.2	Integrieren Sie eine Multi-Faktor-Authentifizierung für alle Remote-Netzwerkzugriffe (sowohl Benutzer als auch Administrator, einschließlich Zugriff durch Dritte zu Support- oder Wartungszwecken), die von außerhalb des Unternehmensnetzwerks erfolgen.	root-account-hardware-mfa-aktiviert	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Hardware-MFA für den Root-Benutzer aktiviert ist. Der Stammbenutzer ist der AWS-Konto-Benutzer mit den meisten Berechtigungen. MFA bietet eine weitere Schutzebene zusätzlich zum Benutzernamen und Passwort. Indem Sie MFA für den Root-Benutzer vorschreiben, können Sie die Anzahl AWS-Konten kompromittierter Benutzer reduzieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
8.3.2	Integrieren Sie eine Multi-Faktor-Authentifizierung für alle Remote-Netzwerkzugriffe (sowohl Benutzer als auch Administrator, einschließlich Zugriff durch Dritte zu Support- oder Wartungszwecken), die von außerhalb des Unternehmensnetzwerks erfolgen.	root-account-mfa-enabled	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass MFA für den Root-Benutzer aktiviert ist. Der Stammbenutzer ist der AWS-Konto-Benutzer mit den meisten Berechtigungen. MFA bietet eine weitere Schutzebene zusätzlich zum Benutzernamen und Passwort. Indem Sie MFA für den Root-Benutzer vorschreiben, können Sie die Anzahl AWS-Konten kompromittierter Benutzer reduzieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.1	Implementieren Sie Audit-Trails, um den gesamten Zugriff auf Systemkom ponenten mit jedem einzelnen Benutzer zu verknüpfen.	api-gw-execution-l ogging-aktiviert	Die API-Gateway-Protokollierung zeigt detaillierte Ansichten der Benutzer, die auf die API zugegriff en haben, und wie diese Benutzer auf die API zugegriffen haben. Diese Insights ermöglichen die Einsicht in Benutzera ktivitäten.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.1	Implementieren Sie Audit-Trails, um den gesamten Zugriff auf Systemkom ponenten mit jedem einzelnen Benutzer zu verknüpfen.	elb-logging-enabled	Die Elastic-Load-Balancing-Aktivität ist ein zentraler Kommunikationspunk t innerhalb einer Umgebung. Stellen Sie sicher, dass die ELB-Protokollierun g aktiviert ist. Die gesammelten Daten enthalten detaillie rte Informationen zu Anfragen, die an den ELB gesendet wurden. Jedes Protokoll enthält Informationen wie die Zeit, zu der die Anforderung einging, die Client-IP -Adresse, Latenzen, Anforderungspfade und Serverantworten.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.1	Implementieren Sie Audit-Trails, um den gesamten Zugriff auf Systemkom ponenten mit jedem einzelnen Benutzer zu verknüpfen.	multi-region-cloudtrail-enabled	AWS CloudTrail zeichnet Aktionen und API-Aufrufe der AWS Management Console auf. Sie können feststellen, welche Benutzer und Konten angerufen wurden AWS, von welcher Quell-IP-Adresse aus die Anrufe getätigt wurden und wann die Anrufe erfolgten. CloudTrail übermittelt Protokolldateien aus allen AWS Regionen an Ihren S3-Bucket , wenn MULTI_REG ION_CLOUD _TRAIL_ENABLED aktiviert ist. Außerdem wird beim AWS Start einer neuen Region derselbe Trail in der neuen Region erstellt. CloudTrail Dadurch erhalten Sie automatis ch Protokolldateien mit API-Aktivitäten für die neue Region.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.1	Implementieren Sie Audit-Trails, um den gesamten Zugriff auf Systemkom ponenten mit jedem einzelnen Benutzer zu verknüpfen.	s-3 bucket-logging-enabled	Die Amazon Simple Storage Service (Amazon S3)-Serverzugriffs protokollierung bietet eine Methode zur Überwachu ng des Netzwerks im Hinblick auf potenzielle Cybersich erheitsereignisse. Die Ereignisse werden überwacht, indem detaillierte Aufzeichn ungen über die Anfragen erfasst werden, die an einen Amazon-S3-Bucket gestellt wurden. Jeder Zugriffsprotokolle intrag enthält Details zu einer einzelnen Zugriffsanfrage. Zu den Details gehören Anforderer, Bucket-Name, Anforderu ngszeit, Anforderu ngsaktion, Antwortst atus und Fehlercode, falls relevant.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.1	Implementieren Sie Audit-Trails, um den gesamten Zugriff auf Systemkom ponenten mit jedem einzelnen Benutzer zu verknüpfen.	vpc-flow-logs-enabled	VPC-Flow-Protokoll e erfassen detaillierte Informationsdatens ätze über den IP-Datenverkehr, der zu und von Netzwerkschnittste llen in Ihrer Amazon Virtual Private Cloud (Amazon VPC) fließt. Standardmäßig enthalten Flow-Prot okolldatensätze Werte für die verschiedenen Komponenten des IP-Flows, einschlie ßlich Quelle, Ziel und Protokoll.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.1	Implementieren Sie Audit-Trails, um den gesamten Zugriff auf Systemkom ponenten mit jedem einzelnen Benutzer zu verknüpfen.	wafv2-logging-enab led	Um die Protokoll ierung und Überwachung in Ihrer Umgebung zu erleichtern, aktiviere n Sie die AWS WAF (V2) -Protokol lierung im regionale n und globalen Web ACLs. AWS Die WAF-Protokollierun g bietet detaillierte Informationen über den Datenverkehr, der von Ihrer Web-ACL analysiert wird. In den Protokollen werden die Uhrzeit aufgezeic hnet, zu der die AWS WAF die Anfrage von Ihrer AWS Ressource erhalten hat, Informati onen über die Anfrage und eine Aktion für die Regel, der jede Anfrage entsprach.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.1	Implementieren Sie Audit-Trails, um den gesamten Zugriff auf Systemkom ponenten mit jedem einzelnen Benutzer zu verknüpfen.	cloudtrail-enabled	AWS CloudTrail kann dabei helfen, die Ablehnung zu verhindern, indem Aktionen und API-Aufrufe der AWS Management Console aufgezeichnet werden. Sie können die Benutzer und die Benutzer AWS-Konten , die einen AWS Dienst aufgerufe n haben, die Quell-IP-Adresse, über die die Aufrufe generiert wurden, und den Zeitpunkt der Anrufe identifiz ieren. Einzelheiten zu den erfassten Daten finden Sie in den AWS CloudTrail Datensatzinhalten.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.1	Implementieren Sie Audit-Trails, um den gesamten Zugriff auf Systemkom ponenten mit jedem einzelnen Benutzer zu verknüpfen.	cloudtrail-s3-data events-enabled	Die Erfassung von Simple Storage Service (Amazon S3)-Datenereigniss en unterstützt die Erkennung von ungewöhnlichen Aktivitäten. Zu den Details gehören AWS-Konto Informationen über den Zugriff auf einen Amazon S3 S3-Bucket, die IP-Adress e und die Uhrzeit des Ereignisses.
10.1	Implementieren Sie Audit-Trails, um den gesamten Zugriff auf Systemkom ponenten mit jedem einzelnen Benutzer zu verknüpfen.	codebuild-project-logging-enabled	Stellen Sie sicher, dass die AWS CodeBuild Projektpr otokollierung aktiviert ist, damit Ihre Build-Ausgabeproto kolle entweder an Amazon CloudWatc h oder Amazon Simple Storage Service (Amazon S3) gesendet werden. Build-Ausgabeproto kolle enthalten detaillierte Informati onen zu Ihrem Build-Projekt.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.1	Implementieren Sie Audit-Trails, um den gesamten Zugriff auf Systemkom ponenten mit jedem einzelnen Benutzer zu verknüpfen.	elasticsearch-logs-to-cloudwatch	Stellen Sie sicher, dass für Amazon OpenSearch Service-Domains Fehlerpro tokolle aktiviert und zur Aufbewahrung und Beantwortung an Amazon CloudWatc h Logs gestreamt werden. Domain-Fehlerprotokolle sind bei Sicherhei ts- und Zugriffsp rüfungen sowie bei der Diagnose von Verfügbarkeitsprob lemen nützlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.1	Implementieren Sie Audit-Trails, um den gesamten Zugriff auf Systemkomponenten mit jedem einzelnen Benutzer zu verknüpfen.	opensearch-audit-logging-enabled	Stellen Sie sicher, dass die Audit-Protokollierung für Ihre Amazon OpenSearch Service-Domains aktiviert ist. Mit der Audit-Protokollierung können Sie Benutzeraktivitäten auf Ihren OpenSearch Domains verfolgen, einschließlich erfolgreicher und fehlgeschlagener Authentifizierungen OpenSearch, Anfragen an, Indexänderungen und eingehende Suchanfragen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.1	Implementieren Sie Audit-Trails, um den gesamten Zugriff auf Systemkom ponenten mit jedem einzelnen Benutzer zu verknüpfen.	opensearch-logs-to-cloudwatch	Stellen Sie sicher, dass für Amazon OpenSearch Service-Domains Fehlerpro tokolle aktiviert und zur Aufbewahr ung und Beantwort ung an Amazon CloudWatch Logs gestreamt werden. OpenSearch Service-Fehlerprotokolle können bei Sicherhei ts- und Zugriffsp rüfungen helfen und bei der Diagnose von Verfügbarkeitsprob lemen helfen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.1	Implementieren Sie Audit-Trails, um den gesamten Zugriff auf Systemkom ponenten mit jedem einzelnen Benutzer zu verknüpfen.	rds-logging-enabled	Um die Protokoll ierung und Überwachung in Ihrer Umgebung zu erleichtern, stellen Sie sicher, dass die Amazon Relationa l Database Service (Amazon RDS)-Prot okollierung aktiviert ist. Mit der Amazon-RDS-Protokollierung können Sie Ereigniss e wie Verbindungen, Verbindungsabbrüch e, Abfragen oder abgefragte Tabellen erfassen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.1	Implementieren Sie Audit-Trails, um den gesamten Zugriff auf Systemkom ponenten mit jedem einzelnen Benutzer zu verknüpfen.	redshift-cluster-c onfiguration-check	Um Daten im Ruhezustand zu schützen, muss die Verschlüsselung für Ihre Amazon-Re dshift-Cluster aktiviert sein. Sie müssen auch sicherstellen, dass die erforderl ichen Konfigurationen auf Amazon-Redshift-Clustern bereitges tellt werden. Die Prüfungsprotokolli erung muss aktiviert sein, um Informati onen zu Verbindun gen und Benutzera ktivitäten in der Datenbank bereitzus tellen. Diese Regel erfordert, dass ein Wert für clusterDb Encrypted (Config Default: TRUE) und LoggingEnabled (Config Default: TRUE) gesetzt ist. Die tatsächlichen Werte müssen den Richtlini en Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.2.1	Implementieren Sie automatisierte Audit-Trails für alle Systemkom ponenten, um die folgenden Ereignisse zu rekonstruieren: Alle einzelnen Benutzerz ugriffe auf Karteninh aberdaten.	api-gw-execution-l ogging-aktiviert	Die API-Gateway-Protokollierung zeigt detaillierte Ansichten der Benutzer, die auf die API zugegriff en haben, und wie diese Benutzer auf die API zugegriffen haben. Diese Insights ermöglichen die Einsicht in Benutzera ktivitäten.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.2.1	Implementieren Sie automatisierte Audit-Trails für alle Systemkom ponenten, um die folgenden Ereignisse zu rekonstruieren: Alle einzelnen Benutzerz ugriffe auf Karteninh aberdaten.	multi-region-cloudtrail-enabled	AWS CloudTrail zeichnet Aktionen und API-Aufrufe der AWS Management Console auf. Sie können feststellen, welche Benutzer und Konten angerufen wurden AWS, von welcher Quell-IP-Adresse aus die Anrufe getätigt wurden und wann die Anrufe erfolgten. CloudTrail übermittelt Protokolldateien aus allen AWS Regionen an Ihren S3-Bucket , wenn MULTI_REG ION_CLOUD _TRAIL_ENABLED aktiviert ist. Außerdem wird beim AWS Start einer neuen Region derselbe Trail in der neuen Region erstellt. CloudTrail Dadurch erhalten Sie automatis ch Protokolldateien mit API-Aktivitäten für die neue Region.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.2.1	Implementieren Sie automatisierte Audit-Trails für alle Systemkom ponenten, um die folgenden Ereignisse zu rekonstruieren: Alle einzelnen Benutzerz ugriffe auf Karteninh aberdaten.	s-3 bucket-logging-enabled	Die Amazon Simple Storage Service (Amazon S3)-Serverzugriffs protokollierung bietet eine Methode zur Überwachu ng des Netzwerks im Hinblick auf potenzielle Cybersich erheitsereignisse. Die Ereignisse werden überwacht, indem detaillierte Aufzeichn ungen über die Anfragen erfasst werden, die an einen Amazon-S3-Bucket gestellt wurden. Jeder Zugriffsprotokolle intrag enthält Details zu einer einzelnen Zugriffsanfrage. Zu den Details gehören Anforderer, Bucket-Name, Anforderu ngszeit, Anforderu ngsaktion, Antwortst atus und Fehlercode, falls relevant.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.2.1	Implementieren Sie automatisierte Audit-Trails für alle Systemkom ponenten, um die folgenden Ereignisse zu rekonstruieren: Alle einzelnen Benutzerz ugriffe auf Karteninh aberdaten.	cloudtrail-enabled	AWS CloudTrai l kann durch die Aufzeichnung von Aktionen und API-Aufrufen in der AWS Management Console bei der Nichtabst reitbarkeit helfen. Sie können die Benutzer und die Benutzer AWS-Konten , die einen AWS Dienst aufgerufen haben, die Quell-IP-Adresse, über die die Aufrufe generiert wurden, und den Zeitpunkt der Anrufe identifiz ieren. Einzelheiten zu den erfassten Daten finden Sie in den AWS CloudTrail Datensatzinhalten.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.2.1	Implementieren Sie automatisierte Audit-Trails für alle Systemkom ponenten, um die folgenden Ereignisse zu rekonstruieren: Alle einzelnen Benutzerz ugriffe auf Karteninh aberdaten.	cloudtrail-s3-data events-enabled	Die Erfassung von Simple Storage Service (Amazon S3)-Datenereigniss en unterstützt die Erkennung von ungewöhnlichen Aktivitäten. Zu den Details gehören AWS-Konto Informationen über den Zugriff auf einen Amazon S3 S3-Bucket, die IP-Adress e und die Uhrzeit des Ereignisses.
10.2.1	Implementieren Sie automatisierte Audit-Trails für alle Systemkom ponenten, um die folgenden Ereignisse zu rekonstruieren: Alle einzelnen Benutzerz ugriffe auf Karteninh aberdaten.	codebuild-project-logging-enabled	Stellen Sie sicher, dass die AWS CodeBuild Projektpr otokollierung aktiviert ist, damit Ihre Build-Ausgabeproto kolle entweder an Amazon CloudWatc h oder Amazon Simple Storage Service (Amazon S3) gesendet werden. Build-Ausgabeproto kolle enthalten detaillierte Informati onen zu Ihrem Build-Projekt.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.2.1	Implementieren Sie automatisierte Audit-Trails für alle Systemkom ponenten, um die folgenden Ereignisse zu rekonstruieren: Alle einzelnen Benutzerz ugriffe auf Karteninh aberdaten.	elasticsearch-logs-to-cloudwatch	Stellen Sie sicher, dass für Amazon OpenSearch Service-Domains Fehlerpro tokolle aktiviert und zur Aufbewahrung und Beantwortung an Amazon CloudWatc h Logs gestreamt werden. Domain-Fehlerprotokolle sind bei Sicherhei ts- und Zugriffsp rüfungen sowie bei der Diagnose von Verfügbarkeitsprob lemen nützlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.2.1	Implementieren Sie automatisierte Audit-Trails für alle Systemkomponenten, um die folgenden Ereignisse zu rekonstruieren: Alle einzelnen Benutzerzugriffe auf Karteninhaberdaten.	opensearch-audit-logging-enabled	Stellen Sie sicher, dass die Audit-Protokollierung für Ihre Amazon OpenSearch Service-Domains aktiviert ist. Mit der Audit-Protokollierung können Sie Benutzeraktivitäten auf Ihren OpenSearch Domains verfolgen, einschließlich erfolgreicher und fehlgeschlagener Authentifizierungen OpenSearch, Anfragen an, Indexänderungen und eingehende Suchanfragen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.2.1	Implementieren Sie automatisierte Audit-Trails für alle Systemkom ponenten, um die folgenden Ereignisse zu rekonstruieren: Alle einzelnen Benutzerz ugriffe auf Karteninh aberdaten.	opensearch-logs-to-cloudwatch	Stellen Sie sicher, dass für Amazon OpenSearch Service-Domains Fehlerpro tokolle aktiviert und zur Aufbewahr ung und Beantwort ung an Amazon CloudWatch Logs gestreamt werden. OpenSearch Service-Fehlerprotokolle können bei Sicherhei ts- und Zugriffsp rüfungen helfen und bei der Diagnose von Verfügbarkeitsprob lemen helfen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.2.1	Implementieren Sie automatisierte Audit-Trails für alle Systemkom ponenten, um die folgenden Ereignisse zu rekonstruieren: Alle einzelnen Benutzerz ugriffe auf Karteninh aberdaten.	rds-logging-enabled	Um die Protokoll ierung und Überwachung in Ihrer Umgebung zu erleichtern, stellen Sie sicher, dass die Amazon Relationa l Database Service (Amazon RDS)-Prot okollierung aktiviert ist. Mit der Amazon-RDS-Protokollierung können Sie Ereigniss e wie Verbindungen, Verbindungsabbrüch e, Abfragen oder abgefragte Tabellen erfassen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.2.1	Implementieren Sie automatisierte Audit-Trails für alle Systemkomponenten, um die folgenden Ereignisse zu rekonstruieren: Alle einzelnen Benutzerzugriffe auf Karteninhaberdaten.	redshift-cluster-configuration-check	Um Daten im Ruhezustand zu schützen, muss die Verschlüsselung für Ihre Amazon-Redshift-Cluster aktiviert sein. Sie müssen auch sicherstellen, dass die erforderlichen Konfigurationen auf Amazon-Redshift-Clustern bereitgestellt werden. Die Prüfungsprotokollierung muss aktiviert sein, um Informationen zu Verbindungen und Benutzeraktivitäten in der Datenbank bereitzustellen. Diese Regel erfordert, dass ein Wert für clusterDbEncrypted (Config Default: TRUE) und LoggingEnabled (Config Default: TRUE) gesetzt ist. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.2.2	Implementieren Sie automatisierte Audit-Trails für alle Systemkom ponenten, um die folgenden Ereigniss e zu rekonstruieren: Alle Aktionen, die von jedem Benutzer mit Stamm- oder Administratorrechten ausgeführt werden.	multi-region-cloudtrail-enabled	AWS CloudTrail zeichnet Aktionen und API-Aufrufe der AWS Management Console auf. Sie können feststellen, welche Benutzer und Konten angerufen wurden AWS, von welcher Quell-IP-Adresse aus die Anrufe getätigt wurden und wann die Anrufe erfolgten. CloudTrail übermittelt Protokolldateien aus allen AWS Regionen an Ihren S3-Bucket , wenn MULTI_REG ION_CLOUD _TRAIL_ENABLED aktiviert ist. Außerdem wird beim AWS Start einer neuen Region derselbe Trail in der neuen Region erstellt. CloudTrail Dadurch erhalten Sie automatis ch Protokolldateien mit API-Aktivitäten für die neue Region.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.2.2	Implementieren Sie automatisierte Audit-Trails für alle Systemkom ponenten, um die folgenden Ereigniss e zu rekonstruieren: Alle Aktionen, die von jedem Benutzer mit Stamm- oder Administratorrechten ausgeführt werden.	cloudtrail-enabled	AWS CloudTrail kann bei der Nichtabst reitbarkeit helfen, indem Aktionen und API-Aufrufe der AWS Management Console aufgezeic hnet werden. Sie können die Benutzer und die Benutzer AWS-Konten , die einen AWS Dienst aufgerufen haben, die Quell-IP-Adresse, über die die Aufrufe generiert wurden, und den Zeitpunkt der Anrufe identifiz ieren. Einzelheiten zu den erfassten Daten finden Sie in den AWS CloudTrail Datensatzinhalten.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.2.2	Implementieren Sie automatisierte Audit-Trails für alle Systemkomponenten, um die folgenden Ereignisse zu rekonstruieren: Alle Aktionen, die von jedem Benutzer mit Stamm- oder Administratorrechten ausgeführt werden.	codebuild-project-logging-enabled	Stellen Sie sicher, dass die AWS CodeBuild Projektprotokollierung aktiviert ist, damit Ihre Build-Ausgabeprotokolle entweder an Amazon CloudWatch oder Amazon Simple Storage Service (Amazon S3) gesendet werden. Build-Ausgabeprotokolle enthalten detaillierte Informationen zu Ihrem Build-Projekt.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.2.2	Implementieren Sie automatisierte Audit-Trails für alle Systemkomponenten, um die folgenden Ereignisse zu rekonstruieren: Alle Aktionen, die von jedem Benutzer mit Stamm- oder Administratorrechten ausgeführt werden.	elasticsearch-logs-to-cloudwatch	Stellen Sie sicher, dass für Amazon OpenSearch Service-Domains Fehlerprotokolle aktiviert und zur Aufbewahrung und Beantwortung an Amazon CloudWatch Logs gestreamt werden. Domain-Fehlerprotokolle sind bei Sicherheits- und Zugriffsprüfungen sowie bei der Diagnose von Verfügbarkeitsproblemen nützlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.2.2	Implementieren Sie automatisierte Audit-Trails für alle Systemkomponenten, um die folgenden Ereignisse zu rekonstruieren: Alle Aktionen, die von jedem Benutzer mit Stamm- oder Administratorrechten ausgeführt werden.	opensearch-audit-logging-enabled	Stellen Sie sicher, dass die Audit-Protokollierung für Ihre Amazon OpenSearch Service-Domains aktiviert ist. Mit der Audit-Protokollierung können Sie Benutzeraktivitäten auf Ihren OpenSearch Domains verfolgen, einschließlich erfolgreicher und fehlgeschlagener Authentifizierungen OpenSearch, Anfragen an, Indexänderungen und eingehende Suchanfragen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.2.2	Implementieren Sie automatisierte Audit-Trails für alle Systemkom ponenten, um die folgenden Ereigniss e zu rekonstruieren: Alle Aktionen, die von jedem Benutzer mit Stamm- oder Administratorrechten ausgeführt werden.	opensearch-logs-to-cloudwatch	Stellen Sie sicher, dass für Amazon OpenSearch Service-Domains Fehlerpro tokolle aktiviert und zur Aufbewahr ung und Beantwort ung an Amazon CloudWatch Logs gestreamt werden. OpenSearch Service-Fehlerprotokolle können bei Sicherhei ts- und Zugriffsp rüfungen helfen und bei der Diagnose von Verfügbarkeitsprob lemen helfen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.2.2	Implementieren Sie automatisierte Audit-Trails für alle Systemkom ponenten, um die folgenden Ereigniss e zu rekonstruieren: Alle Aktionen, die von jedem Benutzer mit Stamm- oder Administratorrechten ausgeführt werden.	rds-logging-enabled	Um die Protokoll ierung und Überwachung in Ihrer Umgebung zu erleichtern, stellen Sie sicher, dass die Amazon Relationa l Database Service (Amazon RDS)-Prot okollierung aktiviert ist. Mit der Amazon-RDS-Protokollierung können Sie Ereigniss e wie Verbindungen, Verbindungsabbrüch e, Abfragen oder abgefragte Tabellen erfassen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.2.2	Implementieren Sie automatisierte Audit-Trails für alle Systemkomponenten, um die folgenden Ereignisse zu rekonstruieren: Alle Aktionen, die von jedem Benutzer mit Stamm- oder Administratorrechten ausgeführt werden.	redshift-cluster-configuration-check	Um Daten im Ruhezustand zu schützen, muss die Verschlüsselung für Ihre Amazon-Redshift-Cluster aktiviert sein. Sie müssen auch sicherstellen, dass die erforderlichen Konfigurationen auf Amazon-Redshift-Clustern bereitgestellt werden. Die Prüfungsprotokollierung muss aktiviert sein, um Informationen zu Verbindungen und Benutzeraktivitäten in der Datenbank bereitzustellen. Diese Regel erfordert, dass ein Wert für clusterDbEncrypted (Config Default: TRUE) und LoggingEnabled (Config Default: TRUE) gesetzt ist. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.2.3	Implementieren Sie automatisierte Audit-Trails für alle Systemkom ponenten, um die folgenden Ereigniss e zu rekonstruieren: Zugriff auf alle Audit-Trails	multi-region-cloudtrail-enabled	AWS CloudTrail zeichnet Aktionen und API-Aufrufe der AWS Management Console auf. Sie können feststellen, welche Benutzer und Konten angerufen wurden AWS, von welcher Quell-IP-Adresse aus die Anrufe getätigt wurden und wann die Anrufe erfolgten. CloudTrail übermittelt Protokolldateien aus allen AWS Regionen an Ihren S3-Bucket , wenn MULTI_REG ION_CLOUD _TRAIL_ENABLED aktiviert ist. Außerdem wird beim AWS Start einer neuen Region derselbe Trail in der neuen Region erstellt. CloudTrail Dadurch erhalten Sie automatis ch Protokolldateien mit API-Aktivitäten für die neue Region.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.2.3	Implementieren Sie automatisierte Audit-Trails für alle Systemkom ponenten, um die folgenden Ereigniss e zu rekonstruieren: Zugriff auf alle Audit-Trails	cloudtrail-enabled	AWS CloudTrail kann bei der Nichtabst reitbarkeit helfen, indem Aktionen und API-Aufrufe der AWS Management Console aufgezeic hnet werden. Sie können die Benutzer und die Benutzer AWS-Konten , die einen AWS Dienst aufgerufen haben, die Quell-IP-Adresse, über die die Aufrufe generiert wurden, und den Zeitpunkt der Anrufe identifiz ieren. Einzelheiten zu den erfassten Daten finden Sie in den AWS CloudTrail Datensatzinhalten.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.2.3	Implementieren Sie automatisierte Audit-Trails für alle Systemkomponenten, um die folgenden Ereignisse zu rekonstruieren: Zugriff auf alle Audit-Trails	cloudtrail-s3-dataevents-enabled	Die Erfassung von Simple Storage Service (Amazon S3)-Datenereignissen unterstützt die Erkennung von ungewöhnlichen Aktivitäten. Zu den Details gehören AWS-Konto Informationen über den Zugriff auf einen Amazon S3 S3-Bucket, die IP-Adresse und die Uhrzeit des Ereignisses.
10.2.3	Implementieren Sie automatisierte Audit-Trails für alle Systemkomponenten, um die folgenden Ereignisse zu rekonstruieren: Zugriff auf alle Audit-Trails	codebuild-project-logging-enabled	Stellen Sie sicher, dass die AWS CodeBuild Projektprotokollierung aktiviert ist, damit Ihre Build-Ausgabeprotokolle entweder an Amazon CloudWatch oder Amazon Simple Storage Service (Amazon S3) gesendet werden. Build-Ausgabeprotokolle enthalten detaillierte Informationen zu Ihrem Build-Projekt.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.2.3	Implementieren Sie automatisierte Audit-Trails für alle Systemkomponenten, um die folgenden Ereignisse zu rekonstruieren: Zugriff auf alle Audit-Trails	elasticsearch-logs-to-cloudwatch	Stellen Sie sicher, dass für Amazon OpenSearch Service-Domains Fehlerprotokolle aktiviert und zur Aufbewahrung und Beantwortung an Amazon CloudWatch Logs gestreamt werden. Domain-Fehlerprotokolle sind bei Sicherheits- und Zugriffsprüfungen sowie bei der Diagnose von Verfügbarkeitsproblemen nützlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.2.3	Implementieren Sie automatisierte Audit-Trails für alle Systemkomponenten, um die folgenden Ereignisse zu rekonstruieren: Zugriff auf alle Audit-Trails	opensearch-audit-logging-enabled	Stellen Sie sicher, dass die Audit-Protokollierung für Ihre Amazon OpenSearch Service-Domains aktiviert ist. Mit der Audit-Protokollierung können Sie Benutzeraktivitäten auf Ihren OpenSearch Domains verfolgen, einschließlich erfolgreicher und fehlgeschlagener Authentifizierungen OpenSearch, Anfragen an, Indexänderungen und eingehende Suchanfragen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.2.3	Implementieren Sie automatisierte Audit-Trails für alle Systemkom ponenten, um die folgenden Ereigniss e zu rekonstruieren: Zugriff auf alle Audit-Trails	opensearch-logs-to-cloudwatch	Stellen Sie sicher, dass für Amazon OpenSearch Service-Domains Fehlerpro tokolle aktiviert und zur Aufbewahr ung und Beantwort ung an Amazon CloudWatch Logs gestreamt werden. OpenSearch Service-Fehlerprotokolle können bei Sicherhei ts- und Zugriffsp rüfungen helfen und bei der Diagnose von Verfügbarkeitsprob lemen helfen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.2.3	Implementieren Sie automatisierte Audit-Trails für alle Systemkomponenten, um die folgenden Ereignisse zu rekonstruieren: Zugriff auf alle Audit-Trails	rds-logging-enabled	Um die Protokollierung und Überwachung in Ihrer Umgebung zu erleichtern, stellen Sie sicher, dass die Amazon Relational Database Service (Amazon RDS)-Protokollierung aktiviert ist. Mit der Amazon-RDS-Protokollierung können Sie Ereignisse wie Verbindungen, Verbindungsabbrüche, Abfragen oder abgefragte Tabellen erfassen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.2.3	Implementieren Sie automatisierte Audit-Trails für alle Systemkomponenten, um die folgenden Ereignisse zu rekonstruieren: Zugriff auf alle Audit-Trails	redshift-cluster-configuration-check	Um Daten im Ruhezustand zu schützen, muss die Verschlüsselung für Ihre Amazon-Redshift-Cluster aktiviert sein. Sie müssen auch sicherstellen, dass die erforderlichen Konfigurationen auf Amazon-Redshift-Clustern bereitgestellt werden. Die Prüfungsprotokollierung muss aktiviert sein, um Informationen zu Verbindungen und Benutzeraktivitäten in der Datenbank bereitzustellen. Diese Regel erfordert, dass ein Wert für clusterDbEncrypted (Config Default: TRUE) und LoggingEnabled (Config Default: TRUE) gesetzt ist. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.2.3	Implementieren Sie automatisierte Audit-Trails für alle Systemkom ponenten, um die folgenden Ereigniss e zu rekonstruieren: Zugriff auf alle Audit-Trails	s-3 bucket-logging-enabled	Die Amazon Simple Storage Service (Amazon S3)-Serverzugriffs protokollierung bietet eine Methode zur Überwachu ng des Netzwerks im Hinblick auf potenzielle Cybersich erheitsereignisse. Die Ereignisse werden überwacht, indem detaillierte Aufzeichn ungen über die Anfragen erfasst werden, die an einen Amazon-S3-Bucket gestellt wurden. Jeder Zugriffsprotokolle intrag enthält Details zu einer einzelnen Zugriffsanfrage. Zu den Details gehören Anforderer, Bucket-Name, Anforderu ngszeit, Anforderu ngsaktion, Antwortst atus und Fehlercode, falls relevant.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.2.4	Implementieren Sie automatisierte Audit-Trails für alle Systemkom ponenten, um die folgenden Ereigniss e zu rekonstruieren: Ungültige logische Zugriffsversuche	api-gw-execution-l ogging-aktiviert	Die API-Gateway-Protokollierung zeigt detaillierte Ansichten der Benutzer, die auf die API zugegriff en haben, und wie diese Benutzer auf die API zugegriffen haben. Diese Insights ermöglichen die Einsicht in Benutzera ktivitäten.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.2.4	Implementieren Sie automatisierte Audit-Trails für alle Systemkom ponenten, um die folgenden Ereigniss e zu rekonstruieren: Ungültige logische Zugriffsversuche	multi-region-cloudtrail-enabled	AWS CloudTrail zeichnet Aktionen und API-Aufrufe der AWS Management Console auf. Sie können feststellen, welche Benutzer und Konten angerufen wurden AWS, von welcher Quell-IP-Adresse aus die Anrufe getätigt wurden und wann die Anrufe erfolgten. CloudTrail übermittelt Protokolldateien aus allen AWS Regionen an Ihren S3-Bucket , wenn MULTI_REG ION_CLOUD _TRAIL_ENABLED aktiviert ist. Außerdem wird beim AWS Start einer neuen Region derselbe Trail in der neuen Region erstellt. CloudTrail Dadurch erhalten Sie automatis ch Protokolldateien mit API-Aktivitäten für die neue Region.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.2.4	Implementieren Sie automatisierte Audit-Trails für alle Systemkom ponenten, um die folgenden Ereigniss e zu rekonstruieren: Ungültige logische Zugriffsversuche	s-3 bucket-logging-enabled	Die Amazon Simple Storage Service (Amazon S3)-Serverzugriffs protokollierung bietet eine Methode zur Überwachu ng des Netzwerks im Hinblick auf potenzielle Cybersich erheitsereignisse. Die Ereignisse werden überwacht, indem detaillierte Aufzeichn ungen über die Anfragen erfasst werden, die an einen Amazon-S3-Bucket gestellt wurden. Jeder Zugriffsprotokolle intrag enthält Details zu einer einzelnen Zugriffsanfrage. Zu den Details gehören Anforderer, Bucket-Name, Anforderu ngszeit, Anforderu ngsaktion, Antwortst atus und Fehlercode, falls relevant.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.2.4	Implementieren Sie automatisierte Audit-Trails für alle Systemkom ponenten, um die folgenden Ereigniss e zu rekonstruieren: Ungültige logische Zugriffsversuche	cloudtrail-enabled	AWS CloudTrail kann bei der Nichtabst reitbarkeit helfen, indem Aktionen und API-Aufrufe der AWS Management Console aufgezeic hnet werden. Sie können die Benutzer und die Benutzer AWS-Konten , die einen AWS Dienst aufgerufen haben, die Quell-IP-Adresse, über die die Aufrufe generiert wurden, und den Zeitpunkt der Anrufe identifiz ieren. Einzelheiten zu den erfassten Daten finden Sie in den AWS CloudTrail Datensatzinhalten.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.2.4	Implementieren Sie automatisierte Audit-Trails für alle Systemkomponenten, um die folgenden Ereignisse zu rekonstruieren: Ungültige logische Zugriffsversuche	cloudtrail-s3-dataevents-enabled	Die Erfassung von Simple Storage Service (Amazon S3)-Datenereignissen unterstützt die Erkennung von ungewöhnlichen Aktivitäten. Zu den Details gehören AWS-Konto Informationen über den Zugriff auf einen Amazon S3 S3-Bucket, die IP-Adresse und die Uhrzeit des Ereignisses.
10.2.4	Implementieren Sie automatisierte Audit-Trails für alle Systemkomponenten, um die folgenden Ereignisse zu rekonstruieren: Ungültige logische Zugriffsversuche	codebuild-project-logging-enabled	Stellen Sie sicher, dass die AWS CodeBuild Projektprotokollierung aktiviert ist, damit Ihre Build-Ausgabeprotokolle entweder an Amazon CloudWatch oder Amazon Simple Storage Service (Amazon S3) gesendet werden. Build-Ausgabeprotokolle enthalten detaillierte Informationen zu Ihrem Build-Projekt.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.2.4	Implementieren Sie automatisierte Audit-Trails für alle Systemkom ponenten, um die folgenden Ereigniss e zu rekonstruieren: Ungültige logische Zugriffsversuche	elasticsearch-logs-to-cloudwatch	Stellen Sie sicher, dass für Amazon OpenSearch Service-Domains Fehlerpro tokolle aktiviert und zur Aufbewahrung und Beantwortung an Amazon CloudWatc h Logs gestreamt werden. Domain-Fehlerprotokolle sind bei Sicherhei ts- und Zugriffsp rüfungen sowie bei der Diagnose von Verfügbarkeitsprob lemen nützlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.2.4	Implementieren Sie automatisierte Audit-Trails für alle Systemkomponenten, um die folgenden Ereignisse zu rekonstruieren: Ungültige logische Zugriffsversuche	opensearch-audit-logging-enabled	Stellen Sie sicher, dass die Audit-Protokollierung für Ihre Amazon OpenSearch Service-Domains aktiviert ist. Mit der Audit-Protokollierung können Sie Benutzeraktivitäten auf Ihren OpenSearch Domains verfolgen, einschließlich erfolgreicher und fehlgeschlagener Authentifizierungen OpenSearch, Anfragen an, Indexänderungen und eingehende Suchanfragen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.2.4	Implementieren Sie automatisierte Audit-Trails für alle Systemkom ponenten, um die folgenden Ereigniss e zu rekonstruieren: Ungültige logische Zugriffsversuche	opensearch-logs-to-cloudwatch	Stellen Sie sicher, dass für Amazon OpenSearch Service-Domains Fehlerpro tokolle aktiviert und zur Aufbewahr ung und Beantwort ung an Amazon CloudWatch Logs gestreamt werden. OpenSearch Service-Fehlerprotokolle können bei Sicherhei ts- und Zugriffsp rüfungen helfen und bei der Diagnose von Verfügbarkeitsprob lemen helfen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.2.4	Implementieren Sie automatisierte Audit-Trails für alle Systemkomponenten, um die folgenden Ereignisse zu rekonstruieren: Ungültige logische Zugriffsversuche	rds-logging-enabled	Um die Protokollierung und Überwachung in Ihrer Umgebung zu erleichtern, stellen Sie sicher, dass die Amazon Relational Database Service (Amazon RDS)-Protokollierung aktiviert ist. Mit der Amazon-RDS-Protokollierung können Sie Ereignisse wie Verbindungen, Verbindungsabbrüche, Abfragen oder abgefragte Tabellen erfassen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.2.4	Implementieren Sie automatisierte Audit-Trails für alle Systemkomponenten, um die folgenden Ereignisse zu rekonstruieren: Ungültige logische Zugriffsversuche	redshift-cluster-configuration-check	Um Daten im Ruhezustand zu schützen, muss die Verschlüsselung für Ihre Amazon-Redshift-Cluster aktiviert sein. Sie müssen auch sicherstellen, dass die erforderlichen Konfigurationen auf Amazon-Redshift-Clustern bereitgestellt werden. Die Prüfungsprotokollierung muss aktiviert sein, um Informationen zu Verbindungen und Benutzeraktivitäten in der Datenbank bereitzustellen. Diese Regel erfordert, dass ein Wert für clusterDbEncrypted (Config Default: TRUE) und LoggingEnabled (Config Default: TRUE) gesetzt ist. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.2.5	Implementieren Sie automatisierte Audit-Trails für alle Systemkomponenten, um die folgenden Ereignisse zu rekonstruieren: Verwendung und Änderung von Identifikations- und Authentifizierungsmechanismen – einschließlich, aber nicht beschränkt auf die Erstellung neuer Konten und die Erhöhung von Berechtigungen – sowie alle Änderungen, Ergänzungen oder Löschungen für Konten mit Stamm- oder Administratorrechten	multi-region-cloudtrail-enabled	AWS CloudTrail zeichnet Aktionen und API-Aufrufe der AWS Management Console auf. Sie können feststellen, welche Benutzer und Konten angerufen wurden AWS, von welcher Quell-IP-Adresse aus die Anrufe getätigt wurden und wann die Anrufe erfolgten. CloudTrail übermittelt Protokolldateien aus allen AWS Regionen an Ihren S3-Bucket, wenn MULTI_REGION_CLOUD_TRAIL_ENABLED aktiviert ist. Außerdem wird beim AWS Start einer neuen Region derselbe Trail in der neuen Region erstellt. CloudTrail Dadurch erhalten Sie automatisch Protokolldateien mit API-Aktivitäten für die neue Region.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.2.5	Implementieren Sie automatisierte Audit-Trails für alle Systemkomponenten, um die folgenden Ereignisse zu rekonstruieren: Verwendung und Änderung von Identifikations- und Authentifizierungsmechanismen – einschließlich, aber nicht beschränkt auf die Erstellung neuer Konten und die Erhöhung von Berechtigungen – sowie alle Änderungen, Ergänzungen oder Löschungen für Konten mit Stamm- oder Administratorrechten	cloudtrail-enabled	AWS CloudTrail kann bei der Nichtabstreitbarkeit helfen, indem Aktionen und API-Aufrufe der AWS Management Console aufgezeichnet werden. Sie können die Benutzer und die Benutzer AWS-Konten , die einen AWS Dienst aufgerufen haben, die Quell-IP-Adresse, über die die Aufrufe generiert wurden, und den Zeitpunkt der Anrufe identifizieren. Einzelheiten zu den erfassten Daten finden Sie in den AWS CloudTrail Datensatzinhalten.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.2.5	Implementieren Sie automatisierte Audit-Trails für alle Systemkomponenten, um die folgenden Ereignisse zu rekonstruieren: Verwendung und Änderung von Identifikations- und Authentifizierungsmechanismen – einschließlich, aber nicht beschränkt auf die Erstellung neuer Konten und die Erhöhung von Berechtigungen – sowie alle Änderungen, Ergänzungen oder Löschungen für Konten mit Stamm- oder Administratorrechten	codebuild-project-logging-enabled	Stellen Sie sicher, dass die AWS CodeBuild Projektprotokollierung aktiviert ist, damit Ihre Build-Ausgabeprotokolle entweder an Amazon CloudWatch oder Amazon Simple Storage Service (Amazon S3) gesendet werden. Build-Ausgabeprotokolle enthalten detaillierte Informationen zu Ihrem Build-Projekt.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.2.5	Implementieren Sie automatisierte Audit-Trails für alle Systemkomponenten, um die folgenden Ereignisse zu rekonstruieren: Verwendung und Änderung von Identifikations- und Authentifizierungsmechanismen – einschließlich, aber nicht beschränkt auf die Erstellung neuer Konten und die Erhöhung von Berechtigungen – sowie alle Änderungen, Ergänzungen oder Löschungen für Konten mit Stamm- oder Administratorrechten	elasticsearch-logs-to-cloudwatch	Stellen Sie sicher, dass für Amazon OpenSearch Service-Domains Fehlerprotokolle aktiviert und zur Aufbewahrung und Beantwortung an Amazon CloudWatch Logs gestreamt werden. Domain-Fehlerprotokolle sind bei Sicherheits- und Zugriffsprüfungen sowie bei der Diagnose von Verfügbarkeitsproblemen nützlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.2.5	Implementieren Sie automatisierte Audit-Trails für alle Systemkomponenten, um die folgenden Ereignisse zu rekonstruieren: Verwendung und Änderung von Identifikations- und Authentifizierungsmechanismen – einschließlich, aber nicht beschränkt auf die Erstellung neuer Konten und die Erhöhung von Berechtigungen – sowie alle Änderungen, Ergänzungen oder Löschungen für Konten mit Stamm- oder Administratorrechten	opensearch-audit-logging-enabled	Stellen Sie sicher, dass die Audit-Protokollierung für Ihre Amazon OpenSearch Service-Domains aktiviert ist. Mit der Audit-Protokollierung können Sie Benutzeraktivitäten auf Ihren OpenSearch Domains verfolgen, einschließlich erfolgreicher und fehlgeschlagener Authentifizierungen OpenSearch, Anfragen an, Indexänderungen und eingehende Suchanfragen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.2.5	Implementieren Sie automatisierte Audit-Trails für alle Systemkomponenten, um die folgenden Ereignisse zu rekonstruieren: Verwendung und Änderung von Identifikations- und Authentifizierungsmechanismen – einschließlich, aber nicht beschränkt auf die Erstellung neuer Konten und die Erhöhung von Berechtigungen – sowie alle Änderungen, Ergänzungen oder Löschungen für Konten mit Stamm- oder Administratorrechten	opensearch-logs-to-cloudwatch	Stellen Sie sicher, dass für Amazon OpenSearch Service-Domains Fehlerprotokolle aktiviert und zur Aufbewahrung und Beantwortung an Amazon CloudWatch Logs gestreamt werden. OpenSearch Service-Fehlerprotokolle können bei Sicherheits- und Zugriffsprüfungen helfen und bei der Diagnose von Verfügbarkeitsproblemen helfen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.2.5	Implementieren Sie automatisierte Audit-Trails für alle Systemkomponenten, um die folgenden Ereignisse zu rekonstruieren: Verwendung und Änderung von Identifikations- und Authentifizierungsmechanismen – einschließlich, aber nicht beschränkt auf die Erstellung neuer Konten und die Erhöhung von Berechtigungen – sowie alle Änderungen, Ergänzungen oder Löschungen für Konten mit Stamm- oder Administratorrechten	rds-logging-enabled	Um die Protokollierung und Überwachung in Ihrer Umgebung zu erleichtern, stellen Sie sicher, dass die Amazon Relational Database Service (Amazon RDS)-Protokollierung aktiviert ist. Mit der Amazon-RDS-Protokollierung können Sie Ereignisse wie Verbindungen, Verbindungsabbrüche, Abfragen oder abgefragte Tabellen erfassen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.2.5	Implementieren Sie automatisierte Audit-Trails für alle Systemkomponenten, um die folgenden Ereignisse zu rekonstruieren: Verwendung und Änderung von Identifikations- und Authentifizierungsmechanismen – einschließlich, aber nicht beschränkt auf die Erstellung neuer Konten und die Erhöhung von Berechtigungen – sowie alle Änderungen, Ergänzungen oder Löschungen für Konten mit Stamm- oder Administratorrechten	redshift-cluster-configuration-check	Um Daten im Ruhezustand zu schützen, muss die Verschlüsselung für Ihre Amazon-Redshift-Cluster aktiviert sein. Sie müssen auch sicherstellen, dass die erforderlichen Konfigurationen auf Amazon-Redshift-Clustern bereitgestellt werden. Die Prüfungsprotokollierung muss aktiviert sein, um Informationen zu Verbindungen und Benutzeraktivitäten in der Datenbank bereitzustellen. Diese Regel erfordert, dass ein Wert für clusterDbEncrypted (Config Default: TRUE) und LoggingEnabled (Config Default: TRUE) gesetzt ist. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.2.6	Implementieren Sie automatisierte Audit-Trails für alle Systemkom ponenten, um die folgenden Ereigniss e zu rekonstru ieren: Initialisierung, Beenden oder Anhalten der Audit-Protokolle	multi-region-cloudtrail-enabled	AWS CloudTrail zeichnet Aktionen und API-Aufrufe der AWS Management Console auf. Sie können feststellen, welche Benutzer und Konten angerufen wurden AWS, von welcher Quell-IP-Adresse aus die Anrufe getätigt wurden und wann die Anrufe erfolgten. CloudTrail übermittelt Protokolldateien aus allen AWS Regionen an Ihren S3-Bucket , wenn MULTI_REG ION_CLOUD _TRAIL_ENABLED aktiviert ist. Außerdem wird beim AWS Start einer neuen Region derselbe Trail in der neuen Region erstellt. CloudTrail Dadurch erhalten Sie automatis ch Protokolldateien mit API-Aktivitäten für die neue Region.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.2.6	Implementieren Sie automatisierte Audit-Trails für alle Systemkom ponenten, um die folgenden Ereigniss e zu rekonstru ieren: Initialisierung, Beenden oder Anhalten der Audit-Protokolle	cloudtrail-enabled	AWS CloudTrail kann bei der Nichtabst reitbarkeit helfen, indem Aktionen und API-Aufrufe der AWS Management Console aufgezeic hnet werden. Sie können die Benutzer und die Benutzer AWS-Konten , die einen AWS Dienst aufgerufen haben, die Quell-IP-Adresse, über die die Aufrufe generiert wurden, und den Zeitpunkt der Anrufe identifiz ieren. Einzelheiten zu den erfassten Daten finden Sie in den AWS CloudTrail Datensatzinhalten.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.2.6	Implementieren Sie automatisierte Audit-Trails für alle Systemkom ponenten, um die folgenden Ereigniss e zu rekonstru ieren: Initialisierung, Beenden oder Anhalten der Audit-Protokolle	rds-logging-enabled	Um die Protokoll ierung und Überwachung in Ihrer Umgebung zu erleichtern, stellen Sie sicher, dass die Amazon Relationa l Database Service (Amazon RDS)-Prot okollierung aktiviert ist. Mit der Amazon-RDS-Protokollierung können Sie Ereigniss e wie Verbindungen, Verbindungsabbrüch e, Abfragen oder abgefragte Tabellen erfassen.
10.2.7	Implementieren Sie automatisierte Audit-Trails für alle Systemkomponenten, um folgende Ereigniss e zu rekonstruieren: Erstellen und Löschen von Objekten auf Systemebene	api-gw-execution-l ogging-aktiviert	Die API-Gateway-Protokollierung zeigt detaillierte Ansichten der Benutzer, die auf die API zugegriff en haben, und wie diese Benutzer auf die API zugegriffen haben. Diese Insights ermöglichen die Einsicht in Benutzera ktivitäten.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.2.7	Implementieren Sie automatisierte Audit-Trails für alle Systemkomponenten, um folgende Ereignisse zu rekonstruieren: Erstellen und Löschen von Objekten auf Systemebene	multi-region-cloudtrail-enabled	AWS CloudTrail zeichnet Aktionen und API-Aufrufe der AWS Management Console auf. Sie können feststellen, welche Benutzer und Konten angerufen wurden AWS, von welcher Quell-IP-Adresse aus die Anrufe getätigt wurden und wann die Anrufe erfolgten. CloudTrail übermittelt Protokolldateien aus allen AWS Regionen an Ihren S3-Bucket, wenn MULTI_REGION_CLOUD_TRAIL_ENABLED aktiviert ist. Außerdem wird beim AWS Start einer neuen Region derselbe Trail in der neuen Region erstellt. CloudTrail Dadurch erhalten Sie automatisch Protokolldateien mit API-Aktivitäten für die neue Region.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.2.7	Implementieren Sie automatisierte Audit-Trails für alle Systemkomponenten, um folgende Ereignisse zu rekonstruieren: Erstellen und Löschen von Objekten auf Systemebene	cloudtrail-enabled	AWS CloudTrail kann durch die Aufzeichnung von Aktionen und API-Aufrufen in der AWS Management Console bei der Nichtabstreitbarkeit helfen. Sie können die Benutzer und die Benutzer AWS-Konten , die einen AWS Dienst aufgerufen haben, die Quell-IP-Adresse, über die die Aufrufe generiert wurden, und den Zeitpunkt der Anrufe identifizieren. Einzelheiten zu den erfassten Daten finden Sie in den AWS CloudTrail Datensatzinhalten.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.2.7	Implementieren Sie automatisierte Audit-Trails für alle Systemkomponenten, um folgende Ereignisse zu rekonstruieren: Erstellen und Löschen von Objekten auf Systemebene	elasticsearch-logs-to-cloudwatch	Stellen Sie sicher, dass für Amazon OpenSearch Service-Domains Fehlerprotokolle aktiviert und zur Aufbewahrung und Beantwortung an Amazon CloudWatch Logs gestreamt werden. Domain-Fehlerprotokolle sind bei Sicherheits- und Zugriffsprüfungen sowie bei der Diagnose von Verfügbarkeitsproblemen nützlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.2.7	Implementieren Sie automatisierte Audit-Trails für alle Systemkomponenten, um folgende Ereignisse zu rekonstruieren: Erstellen und Löschen von Objekten auf Systemebene	opensearch-audit-logging-enabled	Stellen Sie sicher, dass die Audit-Protokollierung für Ihre Amazon OpenSearch Service-Domains aktiviert ist. Mit der Audit-Protokollierung können Sie Benutzeraktivitäten auf Ihren OpenSearch Domains verfolgen, einschließlich erfolgreicher und fehlgeschlagener Authentifizierungen OpenSearch, Anfragen an, Indexänderungen und eingehende Suchanfragen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.2.7	Implementieren Sie automatisierte Audit-Trails für alle Systemkomponenten, um folgende Ereignisse zu rekonstruieren: Erstellen und Löschen von Objekten auf Systemebene	opensearch-logs-to-cloudwatch	Stellen Sie sicher, dass für Amazon OpenSearch Service-Domains Fehlerprotokolle aktiviert und zur Aufbewahrung und Beantwortung an Amazon CloudWatch Logs gestreamt werden. OpenSearch Service-Fehlerprotokolle können bei Sicherheits- und Zugriffsprüfungen helfen und bei der Diagnose von Verfügbarkeitsproblemen helfen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.2.7	Implementieren Sie automatisierte Audit-Trails für alle Systemkomponenten, um folgende Ereignisse zu rekonstruieren: Erstellen und Löschen von Objekten auf Systemebene	rds-logging-enabled	Um die Protokollierung und Überwachung in Ihrer Umgebung zu erleichtern, stellen Sie sicher, dass die Amazon Relational Database Service (Amazon RDS)-Protokollierung aktiviert ist. Mit der Amazon-RDS-Protokollierung können Sie Ereignisse wie Verbindungen, Verbindungsabbrüche, Abfragen oder abgefragte Tabellen erfassen.
10.3.1	Zeichnen Sie mindestens die folgenden Audit-Trail-Einträge für alle Systemkomponenten zu jedem Ereignis auf: Benutzeridentifikation	api-gw-execution-logging-aktiviert	Die API-Gateway-Protokollierung zeigt detaillierte Ansichten der Benutzer, die auf die API zugegriffen haben, und wie diese Benutzer auf die API zugegriffen haben. Diese Insights ermöglichen die Einsicht in Benutzeraktivitäten.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.3.1	Zeichnen Sie mindestens die folgenden Audit-Tra il-Einträge für alle Systemkomponenten zu jedem Ereignis auf: Benutzeridentifikation	elb-logging-enabled	Die Elastic-Load-Balancing-Aktivität ist ein zentraler Kommunikationspunk t innerhalb einer Umgebung. Stellen Sie sicher, dass die ELB-Protokollierun g aktiviert ist. Die gesammelten Daten enthalten detaillie rte Informationen zu Anfragen, die an den ELB gesendet wurden. Jedes Protokoll enthält Informationen wie die Zeit, zu der die Anforderung einging, die Client-IP -Adresse, Latenzen, Anforderungspfade und Serverantworten.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.3.1	Zeichnen Sie mindestens die folgenden Audit-Tra il-Einträge für alle Systemkomponenten zu jedem Ereignis auf: Benutzeridentifikation	multi-region-cloudtrail-enabled	AWS CloudTrail zeichnet Aktionen und API-Aufrufe der AWS Management Console auf. Sie können feststellen, welche Benutzer und Konten angerufen wurden AWS, von welcher Quell-IP-Adresse aus die Anrufe getätigt wurden und wann die Anrufe erfolgten. CloudTrail übermittelt Protokolldateien aus allen AWS Regionen an Ihren S3-Bucket , wenn MULTI_REG ION_CLOUD _TRAIL_ENABLED aktiviert ist. Außerdem wird beim AWS Start einer neuen Region derselbe Trail in der neuen Region erstellt. CloudTrail Dadurch erhalten Sie automatis ch Protokolldateien mit API-Aktivitäten für die neue Region.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.3.1	Zeichnen Sie mindestens die folgenden Audit-Tra il-Einträge für alle Systemkomponenten zu jedem Ereignis auf: Benutzeridentifikation	s-3 bucket-logging-enabled	Die Amazon Simple Storage Service (Amazon S3)-Serverzugriffs protokollierung bietet eine Methode zur Überwachu ng des Netzwerks im Hinblick auf potenzielle Cybersich erheitsereignisse. Die Ereignisse werden überwacht, indem detaillierte Aufzeichn ungen über die Anfragen erfasst werden, die an einen Amazon-S3-Bucket gestellt wurden. Jeder Zugriffsprotokolle intrag enthält Details zu einer einzelnen Zugriffsanfrage. Zu den Details gehören Anforderer, Bucket-Name, Anforderu ngszeit, Anforderu ngsaktion, Antwortst atus und Fehlercode, falls relevant.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.3.1	Zeichnen Sie mindestens die folgenden Audit-Trail-Einträge für alle Systemkomponenten zu jedem Ereignis auf: Benutzeridentifikation	vpc-flow-logs-enabled	VPC-Flow-Protokolle erfassen detaillierte Informationsdatensätze über den IP-Datenverkehr, der zu und von Netzwerkschnittstellen in Ihrer Amazon Virtual Private Cloud (Amazon VPC) fließt. Standardmäßig enthalten Flow-Protokolldatensätze Werte für die verschiedenen Komponenten des IP-Flows, einschließlich Quelle, Ziel und Protokoll.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.3.1	Zeichnen Sie mindestens die folgenden Audit-Trail-Einträge für alle Systemkomponenten zu jedem Ereignis auf: Benutzeridentifikation	wafv2-logging-enabled	Um die Protokollierung und Überwachung in Ihrer Umgebung zu erleichtern, aktivieren Sie die AWS WAF (V2) -Protokollierung im regionalen und globalen Web. ACLs AWS Die WAF-Protokollierung bietet detaillierte Informationen über den Datenverkehr, der von Ihrer Web-ACL analysiert wird. In den Protokollen werden die Uhrzeit aufgezeichnet, zu der die AWS WAF die Anfrage von Ihrer AWS Ressource erhalten hat, Informationen über die Anfrage und eine Aktion für die Regel, der jede Anfrage entsprach.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.3.1	Zeichnen Sie mindestens die folgenden Audit-Tra il-Einträge für alle Systemkomponenten zu jedem Ereignis auf: Benutzeridentifikation	cloudtrail-enabled	AWS CloudTrai l kann durch die Aufzeichnung von Aktionen und API-Aufrufen in der AWS Management Console bei der Nichtabst reitbarkeit helfen. Sie können die Benutzer und die Benutzer AWS-Konten , die einen AWS Dienst aufgerufen haben, die Quell-IP-Adresse, über die die Aufrufe generiert wurden, und den Zeitpunkt der Anrufe identifiz ieren. Einzelheiten zu den erfassten Daten finden Sie in den AWS CloudTrail Datensatzinhalten.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.3.1	Zeichnen Sie mindestens die folgenden Audit-Trail-Einträge für alle Systemkomponenten zu jedem Ereignis auf: Benutzeridentifikation	cloudtrail-s3-dataevents-enabled	Die Erfassung von Simple Storage Service (Amazon S3)-Datenereignissen unterstützt die Erkennung von ungewöhnlichen Aktivitäten. Zu den Details gehören AWS-Konto Informationen über den Zugriff auf einen Amazon S3 S3-Bucket, die IP-Adresse und die Uhrzeit des Ereignisses.
10.3.1	Zeichnen Sie mindestens die folgenden Audit-Trail-Einträge für alle Systemkomponenten zu jedem Ereignis auf: Benutzeridentifikation	codebuild-project-logging-enabled	Stellen Sie sicher, dass die AWS CodeBuild Projektprotokollierung aktiviert ist, damit Ihre Build-Ausgabeprotokolle entweder an Amazon CloudWatch oder Amazon Simple Storage Service (Amazon S3) gesendet werden. Build-Ausgabeprotokolle enthalten detaillierte Informationen zu Ihrem Build-Projekt.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.3.1	Zeichnen Sie mindestens die folgenden Audit-Trail-Einträge für alle Systemkomponenten zu jedem Ereignis auf: Benutzeridentifikation	elasticsearch-logs-to-cloudwatch	Stellen Sie sicher, dass für Amazon OpenSearch Service-Domains Fehlerprotokolle aktiviert und zur Aufbewahrung und Beantwortung an Amazon CloudWatch Logs gestreamt werden. Domain-Fehlerprotokolle sind bei Sicherheits- und Zugriffsprüfungen sowie bei der Diagnose von Verfügbarkeitsproblemen nützlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.3.1	Zeichnen Sie mindestens die folgenden Audit-Trail-Einträge für alle Systemkomponenten zu jedem Ereignis auf: Benutzeridentifikation	opensearch-audit-logging-enabled	Stellen Sie sicher, dass die Audit-Protokollierung für Ihre Amazon OpenSearch Service-Domains aktiviert ist. Mit der Audit-Protokollierung können Sie Benutzeraktivitäten auf Ihren OpenSearch Domains verfolgen, einschließlich erfolgreicher und fehlgeschlagener Authentifizierungen OpenSearch, Anfragen an, Indexänderungen und eingehende Suchanfragen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.3.1	Zeichnen Sie mindestens die folgenden Audit-Tra il-Einträge für alle Systemkomponenten zu jedem Ereignis auf: Benutzeridentifikation	opensearch-logs-to-cloudwatch	Stellen Sie sicher, dass für Amazon OpenSearch Service-Domains Fehlerpro tokolle aktiviert und zur Aufbewahr ung und Beantwort ung an Amazon CloudWatch Logs gestreamt werden. OpenSearch Service-Fehlerprotokolle können bei Sicherhei ts- und Zugriffsp rüfungen helfen und bei der Diagnose von Verfügbarkeitsprob lemen helfen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.3.1	Zeichnen Sie mindestens die folgenden Audit-Trail-Einträge für alle Systemkomponenten zu jedem Ereignis auf: Benutzeridentifikation	rds-logging-enabled	Um die Protokollierung und Überwachung in Ihrer Umgebung zu erleichtern, stellen Sie sicher, dass die Amazon Relational Database Service (Amazon RDS)-Protokollierung aktiviert ist. Mit der Amazon-RDS-Protokollierung können Sie Ereignisse wie Verbindungen, Verbindungsabbrüche, Abfragen oder abgefragte Tabellen erfassen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.3.1	Zeichnen Sie mindestens die folgenden Audit-Trail-Einträge für alle Systemkomponenten zu jedem Ereignis auf: Benutzeridentifikation	redshift-cluster-configuration-check	Um Daten im Ruhezustand zu schützen, muss die Verschlüsselung für Ihre Amazon-Redshift-Cluster aktiviert sein. Sie müssen auch sicherstellen, dass die erforderlichen Konfigurationen auf Amazon-Redshift-Clustern bereitgestellt werden. Die Prüfungsprotokollierung muss aktiviert sein, um Informationen zu Verbindungen und Benutzeraktivitäten in der Datenbank bereitzustellen. Diese Regel erfordert, dass ein Wert für clusterDbEncrypted (Config Default: TRUE) und LoggingEnabled (Config Default: TRUE) gesetzt ist. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.5	Sichere Prüfproto kolle, damit sie nicht verändert werden können.	cloud-trail-encryption-enabled	Da sensible Daten vorhanden sein können und um Daten im Ruhezustand zu schützen, sollten Sie sicherstellen, dass die Verschlüsselung für Ihre Trails aktiviert ist. AWS CloudTrail
10.5	Sichere Prüfproto kolle, damit sie nicht verändert werden können.	s3 bucket-server-side-encryption - aktiviert	Zum Schutz von Daten im Ruhezusta nd müssen Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon Simple Storage Service (Amazon S3)-Bucke ts aktiviert ist. Da sensible Daten in Amazon S3 Buckets gespeichert werden können, sollten Sie die Verschlüsselung aktivieren, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.5	Sichere Prüfprotokolle, damit sie nicht verändert werden können.	s-3 default-encryption-kms	Stellen Sie sicher, dass die Verschlüsselung für Ihre Amazon Simple Storage Service (Amazon S3)-Buckets aktiviert ist. Da sensible Daten in einem Amazon S3 Bucket gespeichert werden können, sollten Sie die Verschlüsselung im Ruhezustand aktivieren, um diese Daten zu schützen.
10.5.2	Schützen Sie Audit-Trail-Dateien vor nicht autorisierten Änderungen.	cloud-trail-encryption-enabled	Da sensible Daten vorhanden sein können und um Daten im Ruhezustand zu schützen, sollten Sie sicherstellen, dass die Verschlüsselung für Ihre AWS CloudTrail Trails aktiviert ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.5.2	Schützen Sie Audit-Trail-Dateien vor nicht autorisierten Änderungen.	s3-fähig bucket-server-side-encryption	Zum Schutz von Daten im Ruhezustand müssen Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon Simple Storage Service (Amazon S3)-Buckets aktiviert ist. Da sensible Daten in Amazon S3 Buckets gespeichert werden können, sollten Sie die Verschlüsselung aktivieren, um diese Daten zu schützen.
10.5.2	Schützen Sie Audit-Trail-Dateien vor nicht autorisierten Änderungen.	s-3 default-encryption-kms	Stellen Sie sicher, dass die Verschlüsselung für Ihre Amazon Simple Storage Service (Amazon S3)-Buckets aktiviert ist. Da sensible Daten in einem Amazon S3 Bucket gespeichert werden können, sollten Sie die Verschlüsselung im Ruhezustand aktivieren, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.5.3	Sofortige Sicherung von Audit-Trail-Dateien auf einem zentralen Protokollserver oder auf Medien, die sich nur schwer ändern lassen.	s-3 lifecycle-policy-check	Mit Amazon-S3-Lebenszyklusregeln können Sie Aktionen definieren, die Amazon S3 während der Lebensdauer eines Objekts ausführen soll (z. B. die Überführung von Objekten in eine andere Speicherklasse, ihre Archivierung oder Löschung nach einem bestimmten Zeitraum).

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.5.3	Sofortige Sicherung von Audit-Trail-Dateien auf einem zentralen Protokollserver oder auf Medien, die sich nur schwer ändern lassen.	backup-plan-min-frequency-and-min-retention-check	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihr AWS Backup-Plan auf eine Mindestfrequenz und Aufbewahrung festgelegt ist. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen. Mit dieser Regel können Sie die Parameter requiredFrequencyValue (Config default: 1), requiredRetentionDays (Config default: 35) und requiredFrequencyUnit

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			(Config default: days) festlegen. Der tatsächliche Wert muss den Anforderungen Ihrer Organisation entsprechen.
10.5.3	Sofortige Sicherung von Audit-Trail-Dateien auf einem zentralen Protokollserver oder auf Medien, die sich nur schwer ändern lassen.	cloud-trail-cloud-watch-logs-aktiviert	Verwenden Sie Amazon CloudWatch , um Protokoll ereignisaktivitäten zentral zu sammeln und zu verwalten. Die Aufnahme von AWS CloudTrail Daten liefert Einzelheiten zu den API-Aufrufaktivitäten in Ihrem AWS-Konto.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.5.3	Sofortige Sicherung von Audit-Trail-Dateien auf einem zentralen Protokollserver oder auf Medien, die sich nur schwer ändern lassen.	s-3 bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) unterstützt die Aufrechterhaltung einer angemessenen Kapazität und Verfügbarkeit. CRR ermöglicht das automatische, asynchrone Kopieren von Objekten in Amazon S3 Buckets, um die Datenverfügbarkeit sicherzustellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.5.5	Verwenden Sie Dateiintegritätsüberwachungs- oder Änderungserkennungssoftware für Protokolle, um sicherzustellen, dass vorhandene Protokolldaten nicht ohne Generierung von Warnungen geändert werden können (obwohl neu hinzukommende Daten keinen Alarm auslösen sollten).	cloud-trail-log-file-Validierung aktiviert	Verwenden Sie die AWS CloudTrail Protokolldateivalidierung, um die Integrität von Protokollen zu überprüfen. CloudTrail Mithilfe der Protokolldateivalidierung kann festgestellt werden, ob eine Protokolldatei geändert oder gelöscht wurde oder ob sie nach der Übermittlung CloudTrail unverändert geblieben ist. Dieses Feature wurde mit dem Branchenstandard entsprechenden Algorithmen entwickelt: SHA-256 für die Hashfunktion und SHA-256 mit RSA für digitale Signaturen. Aus diesem Grund ist es rechnerisch unmöglich, CloudTrail Protokolldateien unbemerkt zu ändern, zu löschen oder zu fälschen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.5.5	Verwenden Sie Dateiintegritätsüb erwachungs- oder Änderungserkennung ssoftware für Protokoll e, um sicherzustellen, dass vorhandene Protokolldaten nicht ohne Generierung von Warnungen geändert werden können (obwohl neu hinzukommende Daten keinen Alarm auslösen sollten).	s-3 bucket-versioning-enabled	Die Versionsv erwaltung von Amazon Simple Storage Service (Amazon S3)-Bucke ts hilft dabei, mehrere Varianten eines Objekts im selben Amazon-S3-Bucket zu speichern. Verwenden Sie die Versionsv erwaltung, um sämtliche Versionen aller Objekte in Ihrem Amazon-S3-Bucket zu speichern , abzurufen oder wiederherzustellen . Mit der Versionsv erwaltung können Sie Versionen sowohl nach unbeabsic htigten Benutzera ktionen als auch nach Anwendungsfehlern problemlos wiederher stellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.7	Bewahren Sie den Audit-Trail-Verlauf für mindestens ein Jahr auf, wobei mindestens drei Monate sofort für Analysen zur Verfügung stehen (z. B. online, archiviert oder aus einem Backup wiederherstellbar).	s-3 lifecycle-policy-check	Stellen Sie sicher, dass Amazon S3-Lebenszyklusrichtlinien konfiguriert sind, um Aktionen zu definieren, die Amazon S3 während der Lebensdauer eines Objekts durchführen soll (z. B. Übergabe von Objekten an eine andere Speicherklasse, Archivierung oder Löschen nach einem bestimmten Zeitraum).

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.7	Bewahren Sie den Audit-Trail-Verlauf für mindestens ein Jahr auf, wobei mindestens drei Monate sofort für Analysen zur Verfügung stehen (z. B. online, archiviert oder aus einem Backup wiederherstellbar).	backup-plan-min-frequency-and-min-retention-check	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihr AWS Backup-Plan auf eine Mindestfrequenz und Aufbewahrung festgelegt ist. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen. Mit dieser Regel können Sie die Parameter requiredFrequencyValue (Config default: 1), requiredRetentionDays (Config default: 35) und requiredFrequencyUnit

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			(Config default: days) festlegen. Der tatsächliche Wert muss den Anforderungen Ihrer Organisation entsprechen.
11.2.3	Führen Sie interne und externe Scans durch und führen Sie bei Bedarf nach jeder wesentlichen Änderung weitere Scans durch. Die Scans müssen von qualifiziertem Personal durchgeführt werden.	ecr-private-image-scanning-aktiviert	Der Amazon Elastic Container Repository (ECR)-Image-Scan unterstützt die Identifizierung von Software-Schwachstellen in Ihren Container-Images. Durch die Aktivierung von Image-Scans in ECR-Repositorys werden die Integrität und Sicherheit der gespeicherten Images mit einer zusätzlichen Überprüfungsebene verbessert.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
11.4	Verwenden Sie die Einbruchserkennung, um Eindringversuche in and/or intrusion-prevention techniques to detect and/or das Netzwerk zu verhindern. Überwachen Sie den gesamten Datenverkehr am Perimeter der Karteninhaberdatenumgebung sowie an kritischen Punkten in der Karteninhaberdatenumgebung und warnen Sie das Personal vor mutmaßlichen Sicherheitsbedrohungen. Halten Sie alle Engines, Baselines und Signaturen zur Erkennung und Abwehr von Eindringlingen auf dem neuesten Stand.	guardduty-enabled-centralized	Amazon GuardDuty kann mithilfe von Threat Intelligence Feeds helfen, potenzielle Cybersicherheitsereignisse zu überwachen und zu erkennen. Dazu gehören Listen mit bösartigen IPs und maschinellen Lernmethoden zur Identifizierung unerwarteter, nicht autorisierter und bösartiger Aktivitäten in Ihrer AWS Cloud-Umgebung.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
11.4	Verwenden Sie die Eindringlingserkennung, and/or intrusion-prevention techniques to detect and/or um Eindringversuche in das Netzwerk zu verhindern. Überwachen Sie den gesamten Datenverkehr am Perimeter der Karteninhaberdatenumgebung sowie an kritischen Punkten in der Karteninhaberdatenumgebung und warnen Sie das Personal vor mutmaßlichen Sicherheitsbedrohungen. Halten Sie alle Engines, Baselines und Signaturen zur Erkennung und Abwehr von Eindringlingen auf dem neuesten Stand.	netfw-policy-rule-group-assoziiert	Eine AWS Netzwerk-Firewall-Richtlinie definiert, wie Ihre Firewall den Verkehr in einer Amazon VPC überwacht und verarbeitet. Sie konfigurieren statusfreie und statusbehaftete Regelgruppen, um Pakete und Datenverkehrsströme zu filtern, und Sie definieren den standardmäßigen Umgang mit Datenverkehr.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
11.5	Stellen Sie einen Mechanismus zur Erkennung von Änderungen bereit (z. B. Tools zur Überwachung der Dateiintegrität), um das Personal vor unbefugten Änderungen (einschließlich Änderungen, Hinzufügungen und Löschungen) kritischer Systemdateien, Konfigurationsdateien oder Inhaltsdateien zu warnen, und konfigurieren Sie die Software so, dass kritische Dateivergleiche mindestens wöchentlich durchgeführt werden.	cloud-trail-log-file-Validierung aktiviert	Verwenden Sie die AWS CloudTrail Protokolldateivalidierung, um die Integrität von Protokollen zu überprüfen. CloudTrail Mithilfe der Protokolldateivalidierung kann festgestellt werden, ob eine Protokolldatei geändert oder gelöscht wurde oder ob sie nach der Übermittlung CloudTrail unverändert geblieben ist. Dieses Feature wurde mit dem Branchenstandard entsprechenden Algorithmen entwickelt: SHA-256 für die Hashfunktion und SHA-256 mit RSA für digitale Signaturen. Aus diesem Grund ist es rechnerisch unmöglich, CloudTrail Protokolldateien unbemerkt zu ändern, zu löschen oder zu fälschen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
11.5	Stellen Sie einen Mechanismus zur Erkennung von Änderungen bereit (z. B. Tools zur Überwachung der Dateiintegrität), um das Personal vor unbefugten Änderungen (einschließlich Änderungen, Hinzufügungen und Löschungen) kritischer Systemdateien, Konfigurationsdateien oder Inhaltsdateien zu warnen, und konfigurieren Sie die Software so, dass kritische Dateivergleiche mindestens wöchentlich durchgeführt werden.	securityhub-enabled	AWS Security Hub hilft bei der Überwachung von unbefugtem Personal, Verbindungen, Geräten und Software. AWS Security Hub aggregiert, organisiert und priorisiert die Sicherheitswarnungen oder Ergebnisse mehrerer Dienste. AWS Einige dieser Dienste sind Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer und AWS Firewall Manager sowie AWS Partnerlösungen.

Vorlage

Die Vorlage ist verfügbar unter GitHub: Operational Best Practices for PCI DSS 3.2.1.

Operative Best Practices für PCI DSS 4.0 (ohne globale Ressourcentypen)

Konformitätspakete bieten ein allgemeines Compliance-Framework, das es Ihnen ermöglicht, mithilfe verwalteter oder benutzerdefinierter AWS Config Regeln und Abhilfemaßnahmen Kontrollen zur Sicherheits-, Betriebs- oder Kostenoptimierung durchzuführen. AWS Config Conformance Packs

dienen als Beispielvorlagen nicht dazu, die vollständige Einhaltung eines bestimmten Governance- oder Compliance-Standards sicherzustellen. Sie sind dafür verantwortlich, selbst zu beurteilen, ob Ihre Nutzung der Services den geltenden gesetzlichen und behördlichen Anforderungen entspricht.

Im Folgenden finden Sie ein Beispiel für eine Zuordnung zwischen dem Payment Card Industry Data Security Standard (PCI DSS) 4.0 (ohne globale Ressourcentypen) und AWS verwalteten Konfigurationsregeln. Jede AWS Config Regel gilt für eine bestimmte AWS Ressource und bezieht sich auf eine oder mehrere PCI-DSS-Kontrollen. Eine PCI-DSS-Kontrolle kann mehreren Konfigurationsregeln zugeordnet werden. In der folgenden Tabelle finden Sie weitere Informationen und Anleitungen zu diesen Zuordnungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
1.2.5	Die Netzwerks icherheitskontroll en (NSCs) werden konfiguriert und verwaltet. (PCI-DSS-v4.0)	transfer-family-server-no-ftp	Stellen Sie sicher, dass ein mit AWS Transfer Family erstellter Server kein FTP für die Endpunktverbindung verwendet. Die Regel lautet NON_COMPL IANT, wenn das Serverprotokoll für die Endpunktverbindung FTP-fähig ist.
1.2.8	Die Netzwerks icherheitskontroll en (NSCs) werden konfiguriert und verwaltet. (PCI-DSS-v4.0)	api-gw-endpoint-type-überprüfen	Stellen Sie sicher, dass Amazon API Gateway APIs dem Typ entspricht, der im Regelparameter 'endpointConfigura tionType' angegeben ist. Die Regel gibt NON_COMPLIANT zurück, wenn die

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			REST-API nicht mit dem Endpunkttyp übereinstimmt, der im Regelparameter konfiguriert ist.
1.2.8	Die Netzwerks icherheitskontroll en (NSCs) werden konfiguriert und verwaltet. (PCI-DSS-v4.0)	netfw-policy-defau lt-action-fragment-Pakete	Stellen Sie sicher, dass eine AWS Netzwerk-Firewall-Richtlinie mit einer benutzerdefinierte n statusfreien Standardaktion für fragmentierte Pakete konfiguriert ist. Die Regel ist NON_COMPLIANT, wenn die zustandsl ose Standardaktion für fragmentierte Pakete nicht mit der benutzerdefinierte n Standardaktion übereinstimmt.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
1.2.8	Die Netzwerks icherheitskontroll en (NSCs) werden konfiguriert und verwaltet. (PCI-DSS-v4.0)	eks-endpoint-no-pu blic-Zugang	Stellen Sie sicher, dass der Amazon Elastic Kubernete s Service (Amazon EKS) -Endpunkt nicht öffentlich zugänglic h ist. Die Regel ist NON_COMPLIANT, wenn der Endpunkt öffentlich zugänglich ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
1.2.8	Die Netzwerks icherheitskontroll en (NSCs) werden konfiguriert und verwaltet. (PCI-DSS-v4.0)	restricted-ssh	Hinweis: Bei dieser Regel untersche iden sich die Regel-ID (INCOMING _SSH_DISABLED) und der Regelname (restricted-ssh). Stellen Sie sicher, dass auf den eingehenden SSH-Verkehr für die Sicherheitsgruppen zugegriffen werden kann. Die Regel ist COMPLIANT, wenn die IP-Adressen des eingehenden SSH-Datenverkehrs in den Sicherheitsgruppen eingeschränkt sind (CIDR ungleich 0.0.0.0/0 oder ::/0). Andernfalls ist sie NON_COMPLIANT.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
1.2.8	Die Netzwerks icherheitskontroll en (NSCs) werden konfiguriert und verwaltet. (PCI-DSS-v4.0)	appsync-associated-with-waf	Stellen Sie sicher, dass AWS AppSync APIs sie den AWS WAFv2 Web-Zugri ffskontrolllisten () zugeordnet sind. ACLs Die Regel ist NON_COMPL IANT für eine AWS AppSync API, wenn sie keiner Web-ACL zugeordnet ist.
1.2.8	Die Netzwerks icherheitskontroll en (NSCs) werden konfiguriert und verwaltet. (PCI-DSS-v4.0)	codebuild-project-source-repo-URL-Prüfung	Stellen Sie sicher, dass die URL des Bitbucket-Quell-Re positorys KEINE Anmeldeinformation en enthält oder nicht. Die Regel ist NON_COMPL IANT, wenn die URL Anmeldeinformation en enthält, und COMPLIANT, falls dies nicht der Fall ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
1.2.8	Die Netzwerks icherheitskontroll en (NSCs) werden konfiguriert und verwaltet. (PCI-DSS-v4.0)	elb-acm-certificate-required	Stellen Sie sicher, dass die Classic Load Balancers SSL-Zerti fikate verwenden, die vom AWS Certificate Manager bereitgestellt werden. Verwenden Sie zur Nutzung dieser Regel mit Ihrem Classic Load Balancer einen SSL- oder HTTPS-Listener. Hinweis: Diese Regel gilt nur für Classic Load Balancers. Mit dieser Regel werden keine Applicati on Load Balancer oder Network Load Balancer geprüft.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
1.2.8	Die Netzwerks icherheitskontroll en (NSCs) werden konfiguriert und verwaltet. (PCI-DSS-v4.0)	emr-block-public-a ccess	Stellen Sie sicher, dass für ein Konto bei Amazon EMR die Einstellungen zum Sperren des öffentlic hen Zugriffs aktiviert sind. Die Regel ist NON_COMPLIANT, wenn sie falsch BlockPublicSecurit yGroupRules ist, oder wenn sie wahr ist, sind andere Ports als Port 22 unter aufgeführt. Permitted PublicSecurityGrou pRuleRanges
1.2.8	Die Netzwerks icherheitskontroll en (NSCs) werden konfiguriert und verwaltet. (PCI-DSS-v4.0)	nacl-no-unrestricted-ssh-rdp	Stellen Sie sicher, dass die Standardp orts für eingehenden SSH/RDP-Datenverke hr für Netzwerkz ugriffskontrolllisten () eingeschränkt sind. NACLs Die Regel ist NON_COMPLIANT, wenn ein eingehender NACL-Eintrag für die Ports 22 oder 3389 einen CIDR-Block des Typs Quell-TCP oder -UDP zulässt.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
1.2.8	Die Netzwerks icherheitskontroll en (NSCs) werden konfiguriert und verwaltet. (PCI-DSS-v4.0)	ec2- -alle client-vpn-not-authorize	Stellen Sie sicher, dass die AWS Client-VPN-Autorisierungsre geln nicht den Verbindungszugriff für alle Clients autorisie ren. Die Regel ist NON_COMPLIANT, wenn 'AccessAll' vorhanden und auf true gesetzt ist.
1.2.8	Die Netzwerks icherheitskontroll en (NSCs) werden konfiguriert und verwaltet. (PCI-DSS-v4.0)	internet-gateway-a uthorized-vpc-nur	Stellen Sie sicher, dass Internet-Gateways an eine autorisierte virtuelle private Cloud (Amazon VPC) angeschlo ssen sind. Die Regel ist NON_COMPL IANT, wenn Internet-Gateways an eine nicht autorisierte VPC angehängt sind.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
1.2.8	Die Netzwerks icherheitskontroll en (NSCs) werden konfiguriert und verwaltet. (PCI-DSS-v4.0)	access-point-public-accesss3-Blöcke	Stellen Sie sicher, dass Amazon S3 S3-Zugriffspunkten die Einstellungen zum Blockieren des öffentlichen Zugriffs aktiviert sind. Die Regel ist NON_COMPLIANT, wenn die Einstellung zum Blockieren des öffentlichen Zugriffs für S3-Zugangspunkte nicht aktiviert ist.
1.2.8	Die Netzwerks icherheitskontroll en (NSCs) werden konfiguriert und verwaltet. (PCI-DSS-v4.0)	account-level-public-accesss3-Blöcke	Stellen Sie sicher, dass die erforderl ichen Einstellungen für die Sperrung des öffentlichen Zugriffs auf Kontoebene konfiguriert sind. Die Regel ist nur NON_COMPL IANT, wenn die unten festgeleg ten Felder nicht mit den entsprech enden Feldern im Konfigurationselement übereinstimmen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
1.3.1	Der Netzwerkzugriff zur und von der Karteninhaberdaten umgebung ist eingeschränkt. (PCI-DSS-v4.0)	api-gw-endpoint-type-überprüfen	Stellen Sie sicher, dass Amazon API Gateway APIs dem Typ entspricht, der im Regelparameter 'endpointConfigurationType' angegeben ist. Die Regel gibt NON_COMPLIANT zurück, wenn die REST-API nicht mit dem Endpunkttyp übereinstimmt, der im Regelparameter konfiguriert ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
1.3.1	Der Netzwerkzugriff zur und von der Karteninhaberdaten umgebung ist eingeschränkt. (PCI-DSS-v4.0)	netfw-policy-default-action-fragment-Pakete	Stellen Sie sicher, dass eine AWS Netzwerk-Firewall-Richtlinie mit einer benutzerdefinierten statusfreien Standardaktion für fragmentierte Pakete konfiguriert ist. Die Regel ist NON_COMPLIANT, wenn die zustandslose Standardaktion für fragmentierte Pakete nicht mit der benutzerdefinierten Standardaktion übereinstimmt.
1.3.1	Der Netzwerkzugriff zur und von der Karteninhaberdaten umgebung ist eingeschränkt. (PCI-DSS-v4.0)	redshift-enhanced-vpc-routing-aktiviert	Stellen Sie sicher, dass Amazon Redshift Redshift-Cluster 'enhanced VpcRouting' aktiviert sind. Die Regel ist NON_COMPLIANT, wenn 'enhanced VpcRouting' nicht aktiviert ist oder wenn die Konfiguration nicht aktiviert ist. enhancedVpcRouting Feld ist 'falsch'.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
1.3.1	Der Netzwerkzugriff zur und von der Karteninhaberdaten umgebung ist eingeschränkt. (PCI-DSS-v4.0)	eks-endpoint-no-public-Zugang	Stellen Sie sicher, dass der Amazon Elastic Kubernetes Service (Amazon EKS) -Endpunkt nicht öffentlich zugänglich ist. Die Regel ist NON_COMPLIANT, wenn der Endpunkt öffentlich zugänglich ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
1.3.1	Der Netzwerkzugriff zur und von der Karteninhaberdaten umgebung ist eingeschränkt. (PCI-DSS-v4.0)	restricted-ssh	Hinweis: Bei dieser Regel untersche iden sich die Regel-ID (INCOMING _SSH_DISABLED) und der Regelname (restricted-ssh). Stellen Sie sicher, dass auf den eingehenden SSH-Verkehr für die Sicherheitsgruppen zugegriffen werden kann. Die Regel ist COMPLIANT, wenn die IP-Adressen des eingehenden SSH-Datenverkehrs in den Sicherheitsgruppen eingeschränkt sind (CIDR ungleich 0.0.0.0/0 oder ::/0). Andernfalls ist sie NON_COMPLIANT.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
1.3.1	Der Netzwerkzugriff zur und von der Karteninhaberdaten umgebung ist eingeschränkt. (PCI-DSS-v4.0)	appsync-associated-with-waf	Stellen Sie sicher, dass AWS AppSync APIs sie den AWS WAFv2 Web-Zugriffskontrolllisten () zugeordnet sind. ACLs Die Regel ist NON_COMPLIANT für eine AWS AppSync API, wenn sie keiner Web-ACL zugeordnet ist.
1.3.1	Der Netzwerkzugriff zur und von der Karteninhaberdaten umgebung ist eingeschränkt. (PCI-DSS-v4.0)	codebuild-project-source-repo-URL-Prüfung	Stellen Sie sicher, dass die URL des Bitbucket-Quell-Repositorys KEINE Anmeldeinformationen enthält oder nicht. Die Regel ist NON_COMPLIANT, wenn die URL Anmeldeinformationen enthält, und COMPLIANT, falls dies nicht der Fall ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
1.3.1	Der Netzwerkzugriff zur und von der Karteninhaberdaten umgebung ist eingeschränkt. (PCI-DSS-v4.0)	elb-acm-certificate-required	Stellen Sie sicher, dass die Classic Load Balancers SSL-Zerti fikate verwenden, die vom AWS Certificate Manager bereitgestellt werden. Verwenden Sie zur Nutzung dieser Regel mit Ihrem Classic Load Balancer einen SSL- oder HTTPS-Listener. Hinweis: Diese Regel gilt nur für Classic Load Balancers. Mit dieser Regel werden keine Applicati on Load Balancer oder Network Load Balancer geprüft.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
1.3.1	Der Netzwerkzugriff zur und von der Karteninhaberdaten umgebung ist eingeschränkt. (PCI-DSS-v4.0)	emr-block-public-access	Stellen Sie sicher, dass für ein Konto bei Amazon EMR die Einstellungen zum Sperren des öffentlichen Zugriffs aktiviert sind. Die Regel ist NON_COMPLIANT, wenn sie falsch BlockPublicSecurityGroupRules ist, oder wenn sie wahr ist, sind andere Ports als Port 22 unter aufgeführt. Permitted PublicSecurityGroupRuleRanges
1.3.1	Der Netzwerkzugriff zur und von der Karteninhaberdaten umgebung ist eingeschränkt. (PCI-DSS-v4.0)	nacl-no-unrestricted-ssh-rdp	Stellen Sie sicher, dass die Standardports für eingehenden SSH/RDP-Datenverkehr für Netzwerkzugriffskontrolllisten () eingeschränkt sind. NACLs Die Regel ist NON_COMPLIANT, wenn ein eingehender NACL-Eintrag für die Ports 22 oder 3389 einen CIDR-Block des Typs Quell-TCP oder -UDP zulässt.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
1.3.1	Der Netzwerkzugriff zur und von der Karteninhaberdaten umgebung ist eingeschränkt. (PCI-DSS-v4.0)	ec2- -alle client-vpn-not-authorize	Stellen Sie sicher, dass die AWS Client-VPN-Autorisierungsregeln nicht den Verbindungszugriff für alle Clients autorisieren. Die Regel ist NON_COMPLIANT, wenn 'AccessAll' vorhanden und auf true gesetzt ist.
1.3.1	Der Netzwerkzugriff zur und von der Karteninhaberdaten umgebung ist eingeschränkt. (PCI-DSS-v4.0)	internet-gateway-authorized-vpc-nur	Stellen Sie sicher, dass Internet-Gateways an eine autorisierte virtuelle private Cloud (Amazon VPC) angeschlossen sind. Die Regel ist NON_COMPLIANT, wenn Internet-Gateways an eine nicht autorisierte VPC angehängt sind.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
1.3.1	Der Netzwerkzugriff zur und von der Karteninhaberdaten umgebung ist eingeschränkt. (PCI-DSS-v4.0)	access-point-public-accesss3-Blöcke	Stellen Sie sicher, dass Amazon S3 S3-Zugriffspunkten die Einstellungen zum Blockieren des öffentlichen Zugriffs aktiviert sind. Die Regel ist NON_COMPLIANT, wenn die Einstellung zum Blockieren des öffentlichen Zugriffs für S3-Zugangspunkte nicht aktiviert ist.
1.3.1	Der Netzwerkzugriff zur und von der Karteninhaberdaten umgebung ist eingeschränkt. (PCI-DSS-v4.0)	account-level-public-accesss3-Blöcke	Stellen Sie sicher, dass die erforderl ichen Einstellungen für die Sperrung des öffentlichen Zugriffs auf Kontoebene konfiguriert sind. Die Regel ist nur NON_COMPL IANT, wenn die unten festgeleg ten Felder nicht mit den entsprech enden Feldern im Konfigurationselement übereinstimmen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
1.3.2	Der Netzwerkzugriff zur und von der Karteninhaberdaten umgebung ist eingeschränkt. (PCI-DSS-v4.0)	api-gw-endpoint-type-überprüfen	Stellen Sie sicher, dass Amazon API Gateway APIs dem Typ entspricht, der im Regelparameter 'endpointConfigurationType' angegeben ist. Die Regel gibt NON_COMPLIANT zurück, wenn die REST-API nicht mit dem Endpunkttyp übereinstimmt, der im Regelparameter konfiguriert ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
1.3.2	Der Netzwerkzugriff zur und von der Karteninhaberdaten umgebung ist eingeschränkt. (PCI-DSS-v4.0)	netfw-policy-default-action-fragment-Pakete	Stellen Sie sicher, dass eine AWS Netzwerk-Firewall-Richtlinie mit einer benutzerdefinierten statusfreien Standardaktion für fragmentierte Pakete konfiguriert ist. Die Regel ist NON_COMPLIANT, wenn die zustandslose Standardaktion für fragmentierte Pakete nicht mit der benutzerdefinierten Standardaktion übereinstimmt.
1.3.2	Der Netzwerkzugriff zur und von der Karteninhaberdaten umgebung ist eingeschränkt. (PCI-DSS-v4.0)	redshift-enhanced-vpc-routing-aktiviert	Stellen Sie sicher, dass Amazon Redshift Redshift-Cluster 'enhanced VpcRouting' aktiviert sind. Die Regel ist NON_COMPLIANT, wenn 'enhanced VpcRouting' nicht aktiviert ist oder wenn die Konfiguration nicht aktiviert ist. enhancedVpcRouting Feld ist 'falsch'.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
1.3.2	Der Netzwerkzugriff zur und von der Karteninhaberdaten umgebung ist eingeschränkt. (PCI-DSS-v4.0)	eks-endpoint-no-public-Zugang	Stellen Sie sicher, dass der Amazon Elastic Kubernetes Service (Amazon EKS) -Endpunkt nicht öffentlich zugänglich ist. Die Regel ist NON_COMPLIANT, wenn der Endpunkt öffentlich zugänglich ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
1.3.2	Der Netzwerkzugriff zur und von der Karteninhaberdaten umgebung ist eingeschränkt. (PCI-DSS-v4.0)	restricted-ssh	Hinweis: Bei dieser Regel untersche iden sich die Regel-ID (INCOMING _SSH_DISABLED) und der Regelname (restricted-ssh). Stellen Sie sicher, dass auf den eingehenden SSH-Verkehr für die Sicherheitsgruppen zugegriffen werden kann. Die Regel ist COMPLIANT, wenn die IP-Adressen des eingehenden SSH-Datenverkehrs in den Sicherheitsgruppen eingeschränkt sind (CIDR ungleich 0.0.0.0/0 oder ::/0). Andernfalls ist sie NON_COMPLIANT.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
1.3.2	Der Netzwerkzugriff zur und von der Karteninhaberdaten umgebung ist eingeschränkt. (PCI-DSS-v4.0)	appsync-associated-with-waf	Stellen Sie sicher, dass AWS AppSync APIs sie den AWS WAFv2 Web-Zugriffskontrolllisten () zugeordnet sind. ACLs Die Regel ist NON_COMPLIANT für eine AWS AppSync API, wenn sie keiner Web-ACL zugeordnet ist.
1.3.2	Der Netzwerkzugriff zur und von der Karteninhaberdaten umgebung ist eingeschränkt. (PCI-DSS-v4.0)	codebuild-project-source-repo-URL-Prüfung	Stellen Sie sicher, dass die URL des Bitbucket-Quell-Repositorys KEINE Anmeldeinformationen enthält oder nicht. Die Regel ist NON_COMPLIANT, wenn die URL Anmeldeinformationen enthält, und COMPLIANT, falls dies nicht der Fall ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
1.3.2	Der Netzwerkzugriff zur und von der Karteninhaberdaten umgebung ist eingeschränkt. (PCI-DSS-v4.0)	elb-acm-certificate-required	Stellen Sie sicher, dass die Classic Load Balancers SSL-Zerti fikate verwenden, die vom AWS Certificate Manager bereitgestellt werden. Verwenden Sie zur Nutzung dieser Regel mit Ihrem Classic Load Balancer einen SSL- oder HTTPS-Listener. Hinweis: Diese Regel gilt nur für Classic Load Balancers. Mit dieser Regel werden keine Applicati on Load Balancer oder Network Load Balancer geprüft.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
1.3.2	Der Netzwerkzugriff zur und von der Karteninhaberdaten umgebung ist eingeschränkt. (PCI-DSS-v4.0)	emr-block-public-access	Stellen Sie sicher, dass für ein Konto bei Amazon EMR die Einstellungen zum Sperren des öffentlichen Zugriffs aktiviert sind. Die Regel ist NON_COMPLIANT, wenn sie falsch BlockPublicSecurityGroupRules ist, oder wenn sie wahr ist, sind andere Ports als Port 22 unter aufgeführt. Permitted PublicSecurityGroupRuleRanges
1.3.2	Der Netzwerkzugriff zur und von der Karteninhaberdaten umgebung ist eingeschränkt. (PCI-DSS-v4.0)	nacl-no-unrestricted-ssh-rdp	Stellen Sie sicher, dass die Standardports für eingehenden SSH/RDP-Datenverkehr für Netzwerkzugriffskontrolllisten () eingeschränkt sind. NACLs Die Regel ist NON_COMPLIANT, wenn ein eingehender NACL-Eintrag für die Ports 22 oder 3389 einen CIDR-Block des Typs Quell-TCP oder -UDP zulässt.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
1.3.2	Der Netzwerkzugriff zur und von der Karteninhaberdaten umgebung ist eingeschränkt. (PCI-DSS-v4.0)	ec2- -alle client-vpn-not-authorize	Stellen Sie sicher, dass die AWS Client-VPN-Autorisierungsregeln nicht den Verbindungszugriff für alle Clients autorisieren. Die Regel ist NON_COMPLIANT, wenn 'AccessAll' vorhanden und auf true gesetzt ist.
1.3.2	Der Netzwerkzugriff zur und von der Karteninhaberdaten umgebung ist eingeschränkt. (PCI-DSS-v4.0)	internet-gateway-authorized-vpc-nur	Stellen Sie sicher, dass Internet-Gateways an eine autorisierte virtuelle private Cloud (Amazon VPC) angeschlossen sind. Die Regel ist NON_COMPLIANT, wenn Internet-Gateways an eine nicht autorisierte VPC angehängt sind.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
1.3.2	Der Netzwerkzugriff zur und von der Karteninhaberdaten umgebung ist eingeschränkt. (PCI-DSS-v4.0)	access-point-public-accesss3-Blöcke	Stellen Sie sicher, dass Amazon S3 S3-Zugriffspunkten die Einstellungen zum Blockieren des öffentlichen Zugriffs aktiviert sind. Die Regel ist NON_COMPLIANT, wenn die Einstellung zum Blockieren des öffentlichen Zugriffs für S3-Zugangspunkte nicht aktiviert ist.
1.3.2	Der Netzwerkzugriff zur und von der Karteninhaberdaten umgebung ist eingeschränkt. (PCI-DSS-v4.0)	account-level-public-accesss3-Blöcke	Stellen Sie sicher, dass die erforderl ichen Einstellungen für die Sperrung des öffentlichen Zugriffs auf Kontoebene konfiguriert sind. Die Regel ist nur NON_COMPL IANT, wenn die unten festgeleg ten Felder nicht mit den entsprech enden Feldern im Konfigurationselement übereinstimmen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
1.4.1	Netzwerkverbindungen zwischen vertrauenswürdigen und nicht vertrauenswürdigen Netzwerken werden kontrolliert. (PCI-DSS-v4.0)	api-gw-endpoint-type-überprüfen	Stellen Sie sicher, dass Amazon API Gateway APIs dem Typ entspricht, der im Regelparameter 'endpointConfigurationType' angegeben ist. Die Regel gibt NON_COMPLIANT zurück, wenn die REST-API nicht mit dem Endpunkttyp übereinstimmt, der im Regelparameter konfiguriert ist.
1.4.1	Netzwerkverbindungen zwischen vertrauenswürdigen und nicht vertrauenswürdigen Netzwerken werden kontrolliert. (PCI-DSS-v4.0)	redshift-enhanced-vpc-routing-aktiviert	Stellen Sie sicher, dass Amazon Redshift Redshift-Cluster 'enhancedVpcRouting' aktiviert sind. Die Regel ist NON_COMPLIANT, wenn 'enhancedVpcRouting' nicht aktiviert ist oder wenn die Konfiguration nicht aktiviert ist. enhancedVpcRouting Feld ist 'falsch'.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
1.4.1	Netzwerkverbindungen zwischen vertrauenswürdigen und nicht vertrauenswürdigen Netzwerken werden kontrolliert. (PCI-DSS-v4.0)	internet-gateway-authorized-vpc-nur	Stellen Sie sicher, dass Internet-Gateways an eine autorisierte virtuelle private Cloud (Amazon VPC) angeschlossen sind. Die Regel ist NON_COMPLIANT, wenn Internet-Gateways an eine nicht autorisierte VPC angehängt sind.
1.4.2	Netzwerkverbindungen zwischen vertrauenswürdigen und nicht vertrauenswürdigen Netzwerken werden kontrolliert. (PCI-DSS-v4.0)	api-gw-endpoint-type-überprüfen	Stellen Sie sicher, dass Amazon API Gateway APIs dem Typ entspricht, der im Regelparameter 'endpointConfigurationType' angegeben ist. Die Regel gibt NON_COMPLIANT zurück, wenn die REST-API nicht mit dem Endpunkttyp übereinstimmt, der im Regelparameter konfiguriert ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
1.4.2	Netzwerkverbindungen zwischen vertrauenswürdigen und nicht vertrauenswürdigen Netzwerken werden kontrolliert. (PCI-DSS-v4.0)	cloudfront-custom-ssl-certificate	Stellen Sie sicher, dass das mit einer CloudFront Amazon-Distribution verknüpfte Zertifikat nicht das Standard-SSL-Zertifikat ist. Die Regel lautet NON_COMPLIANT, wenn eine CloudFront Distribution das Standard-SSL-Zertifikat verwendet.
1.4.2	Netzwerkverbindungen zwischen vertrauenswürdigen und nicht vertrauenswürdigen Netzwerken werden kontrolliert. (PCI-DSS-v4.0)	netfw-policy-default-action-fragment-Pakete	Stellen Sie sicher, dass eine AWS Netzwerk-Firewall-Richtlinie mit einer benutzerdefinierten statusfreien Standardaktion für fragmentierte Pakete konfiguriert ist. Die Regel ist NON_COMPLIANT, wenn die zustandslose Standardaktion für fragmentierte Pakete nicht mit der benutzerdefinierten Standardaktion übereinstimmt.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
1.4.2	Netzwerkverbindungen zwischen vertrauenswürdigen und nicht vertrauenswürdigen Netzwerken werden kontrolliert. (PCI-DSS-v4.0)	redshift-enhanced-vpc-routing-aktiviert	Stellen Sie sicher, dass Amazon Redshift Redshift-Cluster 'enhanced VpcRouting' aktiviert sind. Die Regel ist NON_COMPLIANT, wenn 'enhanced VpcRouting' nicht aktiviert ist oder wenn die Konfiguration nicht aktiviert ist. enhancedVpcRouting Feld ist 'falsch'.
1.4.2	Netzwerkverbindungen zwischen vertrauenswürdigen und nicht vertrauenswürdigen Netzwerken werden kontrolliert. (PCI-DSS-v4.0)	eks-endpoint-no-public-Zugang	Stellen Sie sicher, dass der Amazon Elastic Kubernetes Service (Amazon EKS) -Endpunkt nicht öffentlich zugänglich ist. Die Regel ist NON_COMPLIANT, wenn der Endpunkt öffentlich zugänglich ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
1.4.2	Netzwerkverbindungen zwischen vertrauenswürdigen und nicht vertrauenswürdigen Netzwerken werden kontrolliert. (PCI-DSS-v4.0)	restricted-ssh	Hinweis: Bei dieser Regel unterscheiden sich die Regel-ID (INCOMING_SSH_DISABLED) und der Regelname (restricted-ssh). Stellen Sie sicher, dass auf den eingehenden SSH-Verkehr für die Sicherheitsgruppen zugegriffen werden kann. Die Regel ist COMPLIANT, wenn die IP-Adressen des eingehenden SSH-Datenverkehrs in den Sicherheitsgruppen eingeschränkt sind (CIDR ungleich 0.0.0.0/0 oder ::/0). Andernfalls ist sie NON_COMPLIANT.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
1.4.2	Netzwerkverbindungen zwischen vertrauenswürdigen und nicht vertrauenswürdigen Netzwerken werden kontrolliert. (PCI-DSS-v4.0)	appsync-associated-with-waf	Stellen Sie sicher, dass AWS AppSync APIs sie den AWS WAFv2 Web-Zugriffskontrolllisten () zugeordnet sind. ACLs Die Regel ist NON_COMPLIANT für eine AWS AppSync API, wenn sie keiner Web-ACL zugeordnet ist.
1.4.2	Netzwerkverbindungen zwischen vertrauenswürdigen und nicht vertrauenswürdigen Netzwerken werden kontrolliert. (PCI-DSS-v4.0)	codebuild-project-source-repo-URL-Prüfung	Stellen Sie sicher, dass die URL des Bitbucket-Quell-Repositorys KEINE Anmeldeinformationen enthält oder nicht. Die Regel ist NON_COMPLIANT, wenn die URL Anmeldeinformationen enthält, und COMPLIANT, falls dies nicht der Fall ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
1.4.2	Netzwerkverbindungen zwischen vertrauenswürdigen und nicht vertrauenswürdigen Netzwerken werden kontrolliert. (PCI-DSS-v4.0)	elb-acm-certificate-required	Stellen Sie sicher, dass die Classic Load Balancers SSL-Zertifikate verwenden, die vom AWS Certificate Manager bereitgestellt werden. Verwenden Sie zur Nutzung dieser Regel mit Ihrem Classic Load Balancer einen SSL- oder HTTPS-Listener. Hinweis: Diese Regel gilt nur für Classic Load Balancers. Mit dieser Regel werden keine Application Load Balancer oder Network Load Balancer geprüft.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
1.4.2	Netzwerkverbindungen zwischen vertrauenswürdigen und nicht vertrauenswürdigen Netzwerken werden kontrolliert. (PCI-DSS-v4.0)	emr-block-public-access	Stellen Sie sicher, dass für ein Konto bei Amazon EMR die Einstellungen zum Sperren des öffentlichen Zugriffs aktiviert sind. Die Regel ist NON_COMPLIANT, wenn sie falsch BlockPublicSecurityGroupRules ist, oder wenn sie wahr ist, sind andere Ports als Port 22 unter aufgeführt. Permitted PublicSecurityGroupRuleRanges
1.4.2	Netzwerkverbindungen zwischen vertrauenswürdigen und nicht vertrauenswürdigen Netzwerken werden kontrolliert. (PCI-DSS-v4.0)	nacl-no-unrestricted-ssh-rdp	Stellen Sie sicher, dass die Standardports für eingehenden SSH/RDP-Datenverkehr für Netzwerkzugriffskontrolllisten () eingeschränkt sind. NACLs Die Regel ist NON_COMPLIANT, wenn ein eingehender NACL-Eintrag für die Ports 22 oder 3389 einen CIDR-Block des Typs Quell-TCP oder -UDP zulässt.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
1.4.2	Netzwerkverbindungen zwischen vertrauenswürdigen und nicht vertrauenswürdigen Netzwerken werden kontrolliert. (PCI-DSS-v4.0)	ec2- -alle client-vpn-not-authorize	Stellen Sie sicher, dass die AWS Client-VPN-Autorisierungsregeln nicht den Verbindungszugriff für alle Clients autorisieren. Die Regel ist NON_COMPLIANT, wenn 'AccessAll' vorhanden und auf true gesetzt ist.
1.4.2	Netzwerkverbindungen zwischen vertrauenswürdigen und nicht vertrauenswürdigen Netzwerken werden kontrolliert. (PCI-DSS-v4.0)	internet-gateway-authorized-vpc-nur	Stellen Sie sicher, dass Internet-Gateways an eine autorisierte virtuelle private Cloud (Amazon VPC) angeschlossen sind. Die Regel ist NON_COMPLIANT, wenn Internet-Gateways an eine nicht autorisierte VPC angehängt sind.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
1.4.2	Netzwerkverbindungen zwischen vertrauenswürdigen und nicht vertrauenswürdigen Netzwerken werden kontrolliert. (PCI-DSS-v4.0)	access-point-public-accesss3-Blöcke	Stellen Sie sicher, dass Amazon S3 S3-Zugriffspunkten die Einstellungen zum Blockieren des öffentlichen Zugriffs aktiviert sind. Die Regel ist NON_COMPLIANT, wenn die Einstellung zum Blockieren des öffentlichen Zugriffs für S3-Zugangspunkte nicht aktiviert ist.
1.4.2	Netzwerkverbindungen zwischen vertrauenswürdigen und nicht vertrauenswürdigen Netzwerken werden kontrolliert. (PCI-DSS-v4.0)	account-level-public-accesss3-Blöcke	Stellen Sie sicher, dass die erforderlichen Einstellungen für die Sperrung des öffentlichen Zugriffs auf Kontoebene konfiguriert sind. Die Regel ist nur NON_COMPLIANT, wenn die unten festgelegten Felder nicht mit den entsprechenden Feldern im Konfigurationselement übereinstimmen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
1.4.3	Netzwerkverbindungen zwischen vertrauenswürdigen und nicht vertrauenswürdigen Netzwerken werden kontrolliert. (PCI-DSS-v4.0)	netfw-policy-default-action-fragment-Pakete	Stellen Sie sicher, dass eine AWS Netzwerk-Firewall-Richtlinie mit einer benutzerdefinierten statusfreien Standardaktion für fragmentierte Pakete konfiguriert ist. Die Regel ist NON_COMPLIANT, wenn die zustandslose Standardaktion für fragmentierte Pakete nicht mit der benutzerdefinierten Standardaktion übereinstimmt.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
1.4.3	Netzwerkverbindungen zwischen vertrauenswürdigen und nicht vertrauenswürdigen Netzwerken werden kontrolliert. (PCI-DSS-v4.0)	netfw-policy-default-action-fragment-Pakete	Stellen Sie sicher, dass eine AWS Netzwerk-Firewall-Richtlinie mit einer benutzerdefinierten statusfreien Standardaktion für fragmentierte Pakete konfiguriert ist. Die Regel ist NON_COMPLIANT, wenn die zustandslose Standardaktion für fragmentierte Pakete nicht mit der benutzerdefinierten Standardaktion übereinstimmt.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
1.4.3	Netzwerkverbindungen zwischen vertrauenswürdigen und nicht vertrauenswürdigen Netzwerken werden kontrolliert. (PCI-DSS-v4.0)	netfw-policy-default-action-vollständige Pakete	Stellen Sie sicher, dass eine AWS Netzwerk-Firewall-Richtlinie mit einer benutzerdefinierten statusfreien Standardaktion für vollständige Pakete konfiguriert ist. Diese Regel ist NON_COMPLIANT, wenn die zustandslose Standardaktion für vollständige Pakete nicht mit der benutzerdefinierten statuslosen Standardaktion übereinstimmt.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
1.4.4	Netzwerkverbindungen zwischen vertrauenswürdigen und nicht vertrauenswürdigen Netzwerken werden kontrolliert. (PCI-DSS-v4.0)	api-gw-endpoint-type-überprüfen	Stellen Sie sicher, dass Amazon API Gateway APIs dem Typ entspricht, der im Regelparameter 'endpointConfigurationType' angegeben ist. Die Regel gibt NON_COMPLIANT zurück, wenn die REST-API nicht mit dem Endpunkttyp übereinstimmt, der im Regelparameter konfiguriert ist.
1.4.4	Netzwerkverbindungen zwischen vertrauenswürdigen und nicht vertrauenswürdigen Netzwerken werden kontrolliert. (PCI-DSS-v4.0)	redshift-enhanced-vpc-routing-aktiviert	Stellen Sie sicher, dass Amazon Redshift Redshift-Cluster 'enhancedVpcRouting' aktiviert sind. Die Regel ist NON_COMPLIANT, wenn 'enhancedVpcRouting' nicht aktiviert ist oder wenn die Konfiguration nicht aktiviert ist. enhancedVpcRouting Feld ist 'falsch'.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
1.4.4	Netzwerkverbindungen zwischen vertrauenswürdigen und nicht vertrauenswürdigen Netzwerken werden kontrolliert. (PCI-DSS-v4.0)	internet-gateway-authorized-vpc-nur	Stellen Sie sicher, dass Internet-Gateways an eine autorisierte virtuelle private Cloud (Amazon VPC) angeschlossen sind. Die Regel ist NON_COMPLIANT, wenn Internet-Gateways an eine nicht autorisierte VPC angehängt sind.
1.4.5	Netzwerkverbindungen zwischen vertrauenswürdigen und nicht vertrauenswürdigen Netzwerken werden kontrolliert. (PCI-DSS-v4.0)	ecs-task-definition-pid-Modusprüfung	Stellen Sie sicher, dass ECSTask Definitionen so konfiguriert sind, dass sie den Prozess-Namespace eines Hosts mit seinen Amazon Elastic Container Service (Amazon ECS) -Containern gemeinsam nutzen. Die Regel lautet NON_COMPLIANT, wenn der PidMode-Parameter auf „host“ gesetzt ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
1.4.5	Netzwerkverbindungen zwischen vertrauenswürdigen und nicht vertrauenswürdigen Netzwerken werden kontrolliert. (PCI-DSS-v4.0)	ec2- deaktiviert launch-template-public-ip	Stellen Sie sicher, dass Amazon EC2 Launch Templates nicht so eingerichtet sind, dass Netzwerkschnittstellen öffentliche IP-Adressen zugewiesen werden. Die Regel lautet NON_COMPLIANT, wenn die Standardversion einer EC2 Startvorlage mindestens eine Netzwerkschnittstelle hat, bei der '' auf 'trueAssociatePublicIpAddress' gesetzt ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
1.5.1	Risiken für das CDE, die von Computergeräten ausgehen, die eine Verbindung sowohl mit nicht vertrauenswürdigen Netzwerken als auch mit dem CDE herstellen können, werden gemindert. (PCI-DSS-v4.0)	api-gw-endpoint-type-überprüfen	Stellen Sie sicher, dass Amazon API Gateway APIs dem Typ entspricht, der im Regelparameter 'endpointConfigurationType' angegeben ist. Die Regel gibt NON_COMPLIANT zurück, wenn die REST-API nicht mit dem Endpunkttyp übereinstimmt, der im Regelparameter konfiguriert ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
1.5.1	Risiken für das CDE, die von Computergeräten ausgehen, die sowohl mit nicht vertrauenswürdigen Netzwerken als auch mit dem CDE verbunden werden können, werden gemindert. (PCI-DSS-v4.0)	netfw-policy-default-action-fragment-Pakete	Stellen Sie sicher, dass eine AWS Netzwerk-Firewall-Richtlinie mit einer benutzerdefinierten statusfreien Standardaktion für fragmentierte Pakete konfiguriert ist. Die Regel ist NON_COMPLIANT, wenn die zustandslose Standardaktion für fragmentierte Pakete nicht mit der benutzerdefinierten Standardaktion übereinstimmt.
1.5.1	Risiken für das CDE, die von Computergeräten ausgehen, die eine Verbindung sowohl mit nicht vertrauenswürdigen Netzwerken als auch mit dem CDE herstellen können, werden gemindert. (PCI-DSS-v4.0)	eks-endpoint-no-public-Zugang	Stellen Sie sicher, dass der Amazon Elastic Kubernetes Service (Amazon EKS) -Endpunkt nicht öffentlich zugänglich ist. Die Regel ist NON_COMPLIANT, wenn der Endpunkt öffentlich zugänglich ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
1.5.1	Risiken für das CDE, die von Computergeräten ausgehen, die eine Verbindung sowohl mit nicht vertrauenswürdigen Netzwerken als auch mit dem CDE herstellen können, werden gemindert. (PCI-DSS-v4.0)	restricted-ssh	Hinweis: Bei dieser Regel unterscheiden sich die Regel-ID (INCOMING_SSH_DISABLED) und der Regelname (restricted-ssh). Stellen Sie sicher, dass auf den eingehenden SSH-Verkehr für die Sicherheitsgruppen zugegriffen werden kann. Die Regel ist COMPLIANT, wenn die IP-Adressen des eingehenden SSH-Datenverkehrs in den Sicherheitsgruppen eingeschränkt sind (CIDR ungleich 0.0.0.0/0 oder ::/0). Andernfalls ist sie NON_COMPLIANT.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
1.5.1	Risiken für das CDE, die von Computergeräten ausgehen, die eine Verbindung sowohl mit nicht vertrauenswürdigen Netzwerken als auch mit dem CDE herstellen können, werden gemindert. (PCI-DSS-v4.0)	appsync-associated-with-waf	Stellen Sie sicher, dass AWS AppSync APIs sie den AWS WAFv2 Web-Zugriffskontrolllisten () zugeordnet sind. ACLs Die Regel ist NON_COMPLIANT für eine AWS AppSync API, wenn sie keiner Web-ACL zugeordnet ist.
1.5.1	Die Risiken für das CDE, die von Computergeräten ausgehen, die eine Verbindung sowohl mit nicht vertrauenswürdigen Netzwerken als auch mit dem CDE herstellen können, werden gemindert. (PCI-DSS-v4.0)	codebuild-project-source-repo-URL-Prüfung	Stellen Sie sicher, dass die URL des Bitbucket-Quell-Repositorys KEINE Anmeldeinformationen enthält oder nicht. Die Regel ist NON_COMPLIANT, wenn die URL Anmeldeinformationen enthält, und COMPLIANT, falls dies nicht der Fall ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
1.5.1	Die Risiken für das CDE, die von Computergeräten ausgehen, die sich sowohl mit nicht vertrauenswürdigen Netzwerken als auch mit dem CDE verbinden können, werden gemindert. (PCI-DSS-v4.0)	elb-acm-certificate-required	Stellen Sie sicher, dass die Classic Load Balancers SSL-Zerti fikate verwenden, die vom AWS Certificate Manager bereitgestellt werden. Verwenden Sie zur Nutzung dieser Regel mit Ihrem Classic Load Balancer einen SSL- oder HTTPS-Listener. Hinweis: Diese Regel gilt nur für Classic Load Balancers. Mit dieser Regel werden keine Applicati on Load Balancer oder Network Load Balancer geprüft.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
1.5.1	Die Risiken für das CDE, die von Computergeräten ausgehen, die sowohl mit nicht vertrauen swürdigen Netzwerke n als auch mit dem CDE verbunden werden können, werden gemindert. (PCI-DSS-v4.0)	emr-block-public-a ccess	Stellen Sie sicher, dass für ein Konto bei Amazon EMR die Einstellungen zum Sperren des öffentlic hen Zugriffs aktiviert sind. Die Regel ist NON_COMPLIANT, wenn sie falsch BlockPublicSecurit yGroupRules ist, oder wenn sie wahr ist, sind andere Ports als Port 22 unter aufgeführt. Permitted PublicSecurityGrou pRuleRanges
1.5.1	Risiken für das CDE, die von Computerg eräten ausgehen, die eine Verbindun g sowohl mit nicht vertrauenswürdigen Netzwerken als auch mit dem CDE herstellen können, werden gemindert. (PCI-DSS-v4.0)	nacl-no-unrestricted-ssh-rdp	Stellen Sie sicher, dass die Standardp orts für eingehenden SSH/RDP-Datenverke hr für Netzwerkz ugriffskontrolllisten () eingeschränkt sind. NACLs Die Regel ist NON_COMPLIANT, wenn ein eingehender NACL-Eintrag für die Ports 22 oder 3389 einen CIDR-Block des Typs Quell-TCP oder -UDP zulässt.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
1.5.1	Die Risiken für das CDE, die von Computergeräten ausgehen, die sowohl mit nicht vertrauen swürdigen Netzwerke n als auch mit dem CDE verbunden werden können, werden gemindert. (PCI-DSS-v4.0)	ec2- -alle client-vpn-not-authorize	Stellen Sie sicher, dass die AWS Client-VPN-Autorisierungsre geln nicht den Verbindungszugriff für alle Clients autorisie ren. Die Regel ist NON_COMPLIANT, wenn 'AccessAll' vorhanden und auf true gesetzt ist.
1.5.1	Die Risiken für das CDE, die von Computergeräten ausgehen, die sowohl mit nicht vertrauen swürdigen Netzwerke n als auch mit dem CDE verbunden werden können, werden gemindert. (PCI-DSS-v4.0)	internet-gateway-a uthorized-vpc-nur	Stellen Sie sicher, dass Internet-Gateways an eine autorisierte virtuelle private Cloud (Amazon VPC) angeschlo ssen sind. Die Regel ist NON_COMPL IANT, wenn Internet-Gateways an eine nicht autorisierte VPC angehängt sind.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
1.5.1	Risiken für das CDE, die von Computergeräten ausgehen, die eine Verbindung sowohl mit nicht vertrauenswürdigen Netzwerken als auch mit dem CDE herstellen können, werden gemindert. (PCI-DSS-v4.0)	access-point-public-accesss3-Blöcke	Stellen Sie sicher, dass Amazon S3 S3-Zugriffspunkten die Einstellungen zum Blockieren des öffentlichen Zugriffs aktiviert sind. Die Regel ist NON_COMPLIANT, wenn die Einstellung zum Blockieren des öffentlichen Zugriffs für S3-Zugangspunkte nicht aktiviert ist.
1.5.1	Die Risiken für das CDE, die von Computergeräten ausgehen, die sowohl mit nicht vertrauenswürdigen Netzwerken als auch mit dem CDE verbunden werden können, werden gemindert. (PCI-DSS-v4.0)	account-level-public-accesss3-Blöcke	Stellen Sie sicher, dass die erforderlichen Einstellungen für die Sperrung des öffentlichen Zugriffs auf Kontoebene konfiguriert sind. Die Regel ist nur NON_COMPLIANT, wenn die unten festgelegten Felder nicht mit den entsprechenden Feldern im Konfigurationselement übereinstimmen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.2.1	Auditprotokolle werden implementiert, um die Erkennung von Anomalien und verdächtigen Aktivitäten sowie die forensische Analyse von Ereignissen zu unterstützen. (PCI-DSS-v4.0)	api-gwv2- access-logs-enabled	Stellen Sie sicher, dass die Amazon API Gateway V2-Stufen die Zugriffsprotokollierung aktiviert haben. Die Regel ist NON_COMPLIANT, wenn 'accessLogSettings' in der Stage-Konfiguration nicht vorhanden ist.
10.2.1	Auditprotokolle werden implementiert, um die Erkennung von Anomalien und verdächtigen Aktivitäten sowie die forensische Analyse von Ereignissen zu unterstützen. (PCI-DSS-v4.0)	api-gw-xray-enabled	Stellen Sie sicher, dass AWS X-Ray Tracing auf Amazon API Gateway REST APIs aktiviert ist. Die Regel ist COMPLIANT, wenn die X-Ray-Ablaufverfolgung aktiviert ist, andernfalls ist sie NON_COMPLIANT.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.2.1	Auditprotokolle werden implementiert, um die Erkennung von Anomalien und verdächtigen Aktivitäten sowie die forensische Analyse von Ereignissen zu unterstützen. (PCI-DSS-v4.0)	neptune-cluster-cloudwatch-log-exportfähig	Stellen Sie sicher, dass in einem Amazon Neptune Neptune-Cluster der Protokollexport für CloudWatch Audit-Logs aktiviert ist. Die Regel lautet NON_COMPLIANT, wenn für einen Neptune-Cluster der Protokollexport für CloudWatch Audit-Logs nicht aktiviert ist.
10.2.1	Auditprotokolle werden implementiert, um die Erkennung von Anomalien und verdächtigen Aktivitäten sowie die forensische Analyse von Ereignissen zu unterstützen. (PCI-DSS-v4.0)	ecs-task-definition-log-Konfiguration	Stellen Sie sicher, dass LogConfiguration für aktive ECS-Aufgabendefinitionen festgelegt ist. Diese Regel ist NON_COMPLIANT, wenn für eine aktive ECSTask Definition die LogConfiguration-Ressource nicht definiert ist oder der Wert für LogConfiguration in mindestens einer Containerdefinition Null ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.2.1	Auditprotokolle werden implementiert, um die Erkennung von Anomalien und verdächtigen Aktivitäten sowie die forensische Analyse von Ereignissen zu unterstützen. (PCI-DSS-v4.0)	cloudtrail-enabled	Hinweis: Bei dieser Regel untersche iden sich die Regel-ID (CLOUD_TR AIL_ENABLED) und der Regelname (cloudtrail-enabled). Stellen Sie sicher, dass in Ihrem Konto ein Trail aktiviert ist AWS CloudTrail . AWS Die Regel ist NON_COMPLIANT, wenn ein Trail nicht aktiviert ist. Optional überprüft die Regel einen bestimmten S3-Bucket, ein Amazon Simple Notification Service (Amazon SNS) -Thema und eine CloudWatch Protokollgruppe.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.2.1	Auditprotokolle werden implementiert, um die Erkennung von Anomalien und verdächtigen Aktivitäten sowie die forensische Analyse von Ereignissen zu unterstützen. (PCI-DSS-v4.0)	multi-region-cloudtrail-enabled	Hinweis: Bei dieser Regel untersche iden sich die Regel-ID (MULTI_RE GION_CLOU D_TRAIL_ENABLED) und der Regelname (). multi-region-cloudtrail-enabled Stellen Sie sicher, dass mindesten s eine Region mit mehreren Regionen vorhanden ist. AWS CloudTrail Die Regel ist NON_COMPL IANT, wenn die Trails nicht mit den Eingabeparametern übereinstimmen. Die Regel lautet NON_COMPLIANT, wenn das ExcludeMa nagementEventSourc es Feld nicht leer ist oder wenn sie so konfiguriert AWS CloudTrail ist, dass Verwaltungsereigni sse wie AWS KMS-Ereignisse oder Amazon RDS-Daten -API-Ereignisse

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			ausgeschlossen werden.
10.2.1	Auditprotokolle werden implementiert, um die Erkennung von Anomalien und verdächtigen Aktivitäten sowie die forensische Analyse von Ereignissen zu unterstützen. (PCI-DSS-v4.0)	appsync-logging-enabled	Stellen Sie sicher, dass für eine API die Protokollierung aktiviert ist. AWS AppSync Die Regel lautet NON_COMPLIANT, wenn die Protokollierung nicht aktiviert ist, oder 'fieldLogLevel' ist weder ERROR noch ALL.
10.2.1	Auditprotokolle werden implementiert, um die Erkennung von Anomalien und verdächtigen Aktivitäten sowie die forensische Analyse von Ereignissen zu unterstützen. (PCI-DSS-v4.0)	mq-cloudwatch-audit-logging-aktiviert	Stellen Sie sicher, dass Amazon MQ-Broker die CloudWatch Amazon-Auditprotokollierung aktiviert haben. Die Regel ist NON_COMPLIANT, wenn für einen Broker die Audit-Protokollierung nicht aktiviert ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.2.1	Auditprotokolle werden implementiert, um die Erkennung von Anomalien und verdächtigen Aktivitäten sowie die forensische Analyse von Ereignissen zu unterstützen. (PCI-DSS-v4.0)	mq-cloudwatch-audit-log-aktiviert	Stellen Sie sicher, dass bei einem Amazon MQ-Broker die CloudWatch Auditprotokollierung aktiviert ist. Die Regel lautet NON_COMPLIANT, wenn für den Broker die Audit-Protokollierung nicht aktiviert ist.
10.2.1	Auditprotokolle werden implementiert, um die Erkennung von Anomalien und verdächtigen Aktivitäten sowie die forensische Analyse von Ereignissen zu unterstützen. (PCI-DSS-v4.0)	eks-cluster-logging-enabled	Stellen Sie sicher, dass ein Amazon Elastic Kubernetes Service (Amazon EKS) -Cluster mit aktivierter Protokollierung konfiguriert ist. Die Regel ist NON_COMPLIANT, wenn die Protokollierung für Amazon-EKS-Cluster nicht für alle Protokolltypen aktiviert ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.2.1	Auditprotokolle werden implementiert, um die Erkennung von Anomalien und verdächtigen Aktivitäten sowie die forensische Analyse von Ereignissen zu unterstützen. (PCI-DSS-v4.0)	elastic-beanstalk-logs-to-Wolkenbeobachtung	Stellen Sie sicher, dass AWS Elastic Beanstalk Beanstalk -Umgebungen so konfiguriert sind, dass sie Protokolle an Amazon CloudWatch Logs senden. Die Regel lautet NON_COMPLIANT, wenn der Wert von `` StreamLogs falsch ist.
10.2.1	Auditprotokolle werden implementiert, um die Erkennung von Anomalien und verdächtigen Aktivitäten sowie die forensische Analyse von Ereignissen zu unterstützen. (PCI-DSS-v4.0)	step-functions-state-machine-Protokollierung aktiviert	Stellen Sie sicher, dass auf der AWS Step Functions Functions-Maschine die Protokollierung aktiviert ist Die Regel ist NON_COMPLIANT, wenn für eine Zustandsmaschine die Protokollierung nicht aktiviert ist oder die Protokollierungskonfiguration nicht auf dem angegebenen Mindestniveau liegt.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.2.1	Auditprotokolle werden implementiert, um die Erkennung von Anomalien und verdächtigen Aktivitäten sowie die forensische Analyse von Ereignissen zu unterstützen. (PCI-DSS-v4.0)	netfw-logging-enabled	Stellen Sie sicher, dass die AWS Netzwerk-Firewall-Firewalls die Protokollierung aktiviert haben. Die Regel ist NON_COMPLIANT, wenn kein Protokollierungstyp konfiguriert ist. Sie können angeben, welchen Protokollierungstyp die Regel prüfen soll.
10.2.1.1	Auditprotokolle werden implementiert, um die Erkennung von Anomalien und verdächtigen Aktivitäten sowie die forensische Analyse von Ereignissen zu unterstützen. (PCI-DSS-v4.0)	api-gwv2- access-logs-enabled	Stellen Sie sicher, dass die Amazon API Gateway V2-Stufen die Zugriffsprotokollierung aktiviert haben. Die Regel ist NON_COMPLIANT, wenn 'accessLogSettings' in der Stage-Konfiguration nicht vorhanden ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.2.1.1	Auditprotokolle werden implementiert, um die Erkennung von Anomalien und verdächtigen Aktivitäten sowie die forensische Analyse von Ereignissen zu unterstützen. (PCI-DSS-v4.0)	api-gw-xray-enabled	Stellen Sie sicher, dass AWS X-Ray Tracing auf Amazon API Gateway REST APIs aktiviert ist. Die Regel ist COMPLIANT, wenn die X-Ray-Abl aufverfolgung aktiviert ist, andernfalls ist sie NON_COMPLIANT.
10.2.1.1	Auditprotokolle werden implementiert, um die Erkennung von Anomalien und verdächtigen Aktivitäten sowie die forensische Analyse von Ereignissen zu unterstützen. (PCI-DSS-v4.0)	neptune-cluster-cloudwatch-log-exportfähig	Stellen Sie sicher, dass in einem Amazon Neptune Neptune-Cluster der Protokollexport für CloudWatch Audit-Logs aktiviert ist. Die Regel lautet NON_COMPLIANT, wenn für einen Neptune-Cluster der Protokollexport für CloudWatch Audit-Logs nicht aktiviert ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.2.1.1	Auditprotokolle werden implementiert, um die Erkennung von Anomalien und verdächtigen Aktivitäten sowie die forensische Analyse von Ereignissen zu unterstützen. (PCI-DSS-v4.0)	ec2- instance-detailed-monitoring-enabled	Stellen Sie sicher, dass die detaillierte Überwachung für Instanzen aktiviert ist. EC2 Die Regel ist NON_COMPLIANT, wenn keine detaillierte Überwachung aktiviert ist.
10.2.1.1	Auditprotokolle werden implementiert, um die Erkennung von Anomalien und verdächtigen Aktivitäten sowie die forensische Analyse von Ereignissen zu unterstützen. (PCI-DSS-v4.0)	ecs-task-definition-log-Konfiguration	Stellen Sie sicher, dass LogConfig uration für aktive ECS-Aufgabendefini tionen festgelegt ist. Diese Regel ist NON_COMPLIANT, wenn für eine aktive ECSTask Definition die LogConfiguration-Ressource nicht definiert ist oder der Wert für LogConfig uration in mindesten s einer Container definition Null ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.2.1.1	Auditprotokolle werden implementiert, um die Erkennung von Anomalien und verdächtigen Aktivitäten sowie die forensische Analyse von Ereignissen zu unterstützen. (PCI-DSS-v4.0)	cloudwatch-alarm-action-check	Stellen Sie sicher, dass bei CloudWatch Alarmen eine Aktion für den Status ALARM, INSUFFICIENT_DATA oder OK konfiguriert ist. Stellen Sie optional sicher, dass alle Aktionen mit einem benannten ARN übereinstimmen. Die Regel ist NON_COMPLIANT, wenn für den Alarm oder den optionalen Parameter keine Aktion festgelegt ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.2.1.1	Auditprotokolle werden implementiert, um die Erkennung von Anomalien und verdächtigen Aktivitäten sowie die forensische Analyse von Ereignissen zu unterstützen. (PCI-DSS-v4.0)	cloudwatch-alarm-action-check	Stellen Sie sicher, dass bei CloudWatch Alarmen eine Aktion für den Status ALARM, INSUFFICIENT_DATA oder OK konfiguriert ist. Stellen Sie optional sicher, dass alle Aktionen mit einem benannten ARN übereinstimmen. Die Regel ist NON_COMPLIANT, wenn für den Alarm oder den optionalen Parameter keine Aktion festgelegt ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.2.1.1	Auditprotokolle werden implementiert, um die Erkennung von Anomalien und verdächtigen Aktivitäten sowie die forensische Analyse von Ereignissen zu unterstützen. (PCI-DSS-v4.0)	cloudwatch-alarm-action-check	Stellen Sie sicher, dass bei CloudWatch Alarmen eine Aktion für den Status ALARM, INSUFFICIENT_DATA oder OK konfiguriert ist. Stellen Sie optional sicher, dass alle Aktionen mit einem benannten ARN übereinstimmen. Die Regel ist NON_COMPLIANT, wenn für den Alarm oder den optionalen Parameter keine Aktion festgelegt ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.2.1.1	Auditprotokolle werden implementiert, um die Erkennung von Anomalien und verdächtigen Aktivitäten sowie die forensische Analyse von Ereignissen zu unterstützen. (PCI-DSS-v4.0)	cloudwatch-alarm-resource-check	Stellen Sie sicher, dass ein Ressourcentyp einen CloudWatch Alarm für die angegebene Metrik hat. Als Ressourcentyp können Sie EBS-Volumes, EC2 Instances, Amazon RDS-Cluster oder S3-Buckets angeben. Die Regel ist KONFORM, wenn die benannte Metrik eine Ressourcen-ID und CloudWatch einen Alarm hat.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.2.1.1	Auditprotokolle werden implementiert, um die Erkennung von Anomalien und verdächtigen Aktivitäten sowie die forensische Analyse von Ereignissen zu unterstützen. (PCI-DSS-v4.0)	cloudtrail-enabled	Hinweis: Bei dieser Regel untersche iden sich die Regel-ID (CLOUD_TR AIL_ENABLED) und der Regelname (cloudtrail-enabled). Stellen Sie sicher, dass in Ihrem Konto ein Trail aktiviert ist AWS CloudTrail . AWS Die Regel ist NON_COMPLIANT, wenn ein Trail nicht aktiviert ist. Optional überprüft die Regel einen bestimmten S3-Bucket, ein Amazon Simple Notification Service (Amazon SNS) -Thema und eine CloudWatch Protokollgruppe.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.2.1.1	Auditprotokolle werden implementiert, um die Erkennung von Anomalien und verdächtigen Aktivitäten sowie die forensische Analyse von Ereignissen zu unterstützen. (PCI-DSS-v4.0)	multi-region-cloudtrail-enabled	Hinweis: Bei dieser Regel untersche iden sich die Regel-ID (MULTI_RE GION_CLOU D_TRAIL_ENABLED) und der Regelname (). multi-region-cloudtrail-enabled Stellen Sie sicher, dass mindesten s eine Region mit mehreren Regionen vorhanden ist. AWS CloudTrail Die Regel ist NON_COMPL IANT, wenn die Trails nicht mit den Eingabeparametern übereinstimmen. Die Regel lautet NON_COMPLIANT, wenn das ExcludeMa nagementEventSourc es Feld nicht leer ist oder wenn sie so konfiguriert AWS CloudTrail ist, dass Verwaltungsereigni sse wie AWS KMS-Ereignisse oder Amazon RDS-Daten -API-Ereignisse

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			ausgeschlossen werden.
10.2.1.1	Auditprotokolle werden implementiert, um die Erkennung von Anomalien und verdächtigen Aktivitäten sowie die forensische Analyse von Ereignissen zu unterstützen. (PCI-DSS-v4.0)	appsync-logging-enabled	Stellen Sie sicher, dass für eine API die Protokollierung aktiviert ist. AWS AppSync Die Regel lautet NON_COMPLIANT, wenn die Protokollierung nicht aktiviert ist, oder 'fieldLogLevel' ist weder ERROR noch ALL.
10.2.1.1	Auditprotokolle werden implementiert, um die Erkennung von Anomalien und verdächtigen Aktivitäten sowie die forensische Analyse von Ereignissen zu unterstützen. (PCI-DSS-v4.0)	mq-cloudwatch-audit-logging-aktiviert	Stellen Sie sicher, dass Amazon MQ-Broker die CloudWatch Amazon-Auditprotokollierung aktiviert haben. Die Regel ist NON_COMPLIANT, wenn für einen Broker die Audit-Protokollierung nicht aktiviert ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.2.1.1	Auditprotokolle werden implementiert, um die Erkennung von Anomalien und verdächtigen Aktivitäten sowie die forensische Analyse von Ereignissen zu unterstützen. (PCI-DSS-v4.0)	mq-cloudwatch-audit-log-aktiviert	Stellen Sie sicher, dass bei einem Amazon MQ-Broker die CloudWatch Auditprotokollierung aktiviert ist. Die Regel lautet NON_COMPLIANT, wenn für den Broker die Audit-Protokollierung nicht aktiviert ist.
10.2.1.1	Auditprotokolle werden implementiert, um die Erkennung von Anomalien und verdächtigen Aktivitäten sowie die forensische Analyse von Ereignissen zu unterstützen. (PCI-DSS-v4.0)	eks-cluster-logging-enabled	Stellen Sie sicher, dass ein Amazon Elastic Kubernetes Service (Amazon EKS) -Cluster mit aktivierter Protokollierung konfiguriert ist. Die Regel ist NON_COMPLIANT, wenn die Protokollierung für Amazon-EKS-Cluster nicht für alle Protokolltypen aktiviert ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.2.1.1	Auditprotokolle werden implementiert, um die Erkennung von Anomalien und verdächtigen Aktivitäten sowie die forensische Analyse von Ereignissen zu unterstützen. (PCI-DSS-v4.0)	elastic-beanstalk-logs-to-Wolkenbeobachtung	Stellen Sie sicher, dass AWS Elastic Beanstalk Beanstalk -Umgebungen so konfiguriert sind, dass sie Protokolle an Amazon CloudWatch Logs senden. Die Regel lautet NON_COMPLIANT, wenn der Wert von `` StreamLogs falsch ist.
10.2.1.1	Auditprotokolle werden implementiert, um die Erkennung von Anomalien und verdächtigen Aktivitäten sowie die forensische Analyse von Ereignissen zu unterstützen. (PCI-DSS-v4.0)	WAF 2- rulegroup-logging-enabled	Stellen Sie sicher, dass die Erfassung von CloudWatch Amazon-Sicherheitsmetriken für AWS WAFv2 Regelgruppen aktiviert ist. Die Regel ist NON_COMPLIANT, wenn '. VisibilityConfig CloudWatchMetricsEnabledDas Feld 'ist auf falsch gesetzt.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.2.1.1	Auditprotokolle werden implementiert, um die Erkennung von Anomalien und verdächtigen Aktivitäten sowie die forensische Analyse von Ereignissen zu unterstützen. (PCI-DSS-v4.0)	sns-topic-message-delivery-Benachrichtigung aktiviert	Stellen Sie sicher, dass die Amazon Simple Notification Service (SNS) - Protokollierung für den Zustellungsstatus von Benachrichtigungen aktiviert ist, die an ein Thema für die Endgeräte gesendet werden. Die Regel ist NON_COMPLIANT, wenn die Benachrichtigung über den Status der Zustellung von Nachrichten nicht aktiviert ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.2.1.1	Auditprotokolle werden implementiert, um die Erkennung von Anomalien und verdächtigen Aktivitäten sowie die forensische Analyse von Ereignissen zu unterstützen. (PCI-DSS-v4.0)	step-functions-state-machine-Protokollierung aktiviert	Stellen Sie sicher, dass auf der AWS Step Functions Functions-Maschine die Protokollierung aktiviert ist Die Regel ist NON_COMPLIANT, wenn für eine Zustandsmaschine die Protokollierung nicht aktiviert ist oder die Protokollierungskonfiguration nicht auf dem angegebenen Mindestniveau liegt.
10.2.1.1	Auditprotokolle werden implementiert, um die Erkennung von Anomalien und verdächtigen Aktivitäten sowie die forensische Analyse von Ereignissen zu unterstützen. (PCI-DSS-v4.0)	netfw-logging-enabled	Stellen Sie sicher, dass die AWS Netzwerk-Firewall-Firewalls die Protokollierung aktiviert haben. Die Regel ist NON_COMPLIANT, wenn kein Protokollierungstyp konfiguriert ist. Sie können angeben, welchen Protokollierungstyp die Regel prüfen soll.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.2.1.2	Auditprotokolle werden implementiert, um die Erkennung von Anomalien und verdächtigen Aktivitäten sowie die forensische Analyse von Ereignissen zu unterstützen. (PCI-DSS-v4.0)	api-gwv2- access-logs-enabled	Stellen Sie sicher, dass die Amazon API Gateway V2-Stufen die Zugriffsprotokollierung aktiviert haben. Die Regel ist NON_COMPLIANT, wenn 'accessLogSettings' in der Stage-Konfiguration nicht vorhanden ist.
10.2.1.2	Auditprotokolle werden implementiert, um die Erkennung von Anomalien und verdächtigen Aktivitäten sowie die forensische Analyse von Ereignissen zu unterstützen. (PCI-DSS-v4.0)	api-gw-xray-enabled	Stellen Sie sicher, dass AWS X-Ray Tracing auf Amazon API Gateway REST APIs aktiviert ist. Die Regel ist COMPLIANT, wenn die X-Ray-Abl aufverfolgung aktiviert ist, andernfalls ist sie NON_COMPLIANT.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.2.1.2	Auditprotokolle werden implementiert, um die Erkennung von Anomalien und verdächtigen Aktivitäten sowie die forensische Analyse von Ereignissen zu unterstützen. (PCI-DSS-v4.0)	neptune-cluster-cloudwatch-log-exportfähig	Stellen Sie sicher, dass in einem Amazon Neptune Neptune-Cluster der Protokollexport für CloudWatch Audit-Logs aktiviert ist. Die Regel lautet NON_COMPLIANT, wenn für einen Neptune-Cluster der Protokollexport für CloudWatch Audit-Logs nicht aktiviert ist.
10.2.1.2	Auditprotokolle werden implementiert, um die Erkennung von Anomalien und verdächtigen Aktivitäten sowie die forensische Analyse von Ereignissen zu unterstützen. (PCI-DSS-v4.0)	ecs-task-definition-log-Konfiguration	Stellen Sie sicher, dass LogConfiguration für aktive ECS-Aufgabendefinitionen festgelegt ist. Diese Regel ist NON_COMPLIANT, wenn für eine aktive ECSTask Definition die LogConfiguration-Ressource nicht definiert ist oder der Wert für LogConfiguration in mindestens einer Containerdefinition Null ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.2.1.2	Auditprotokolle werden implementiert, um die Erkennung von Anomalien und verdächtigen Aktivitäten sowie die forensische Analyse von Ereignissen zu unterstützen. (PCI-DSS-v4.0)	cloudtrail-enabled	Hinweis: Bei dieser Regel untersche iden sich die Regel-ID (CLOUD_TR AIL_ENABLED) und der Regelname (cloudtrail-enabled). Stellen Sie sicher, dass in Ihrem Konto ein Trail aktiviert ist AWS CloudTrail . AWS Die Regel ist NON_COMPLIANT, wenn ein Trail nicht aktiviert ist. Optional überprüft die Regel einen bestimmten S3-Bucket, ein Amazon Simple Notification Service (Amazon SNS) -Thema und eine CloudWatch Protokollgruppe.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.2.1.2	Auditprotokolle werden implementiert, um die Erkennung von Anomalien und verdächtigen Aktivitäten sowie die forensische Analyse von Ereignissen zu unterstützen. (PCI-DSS-v4.0)	multi-region-cloudtrail-enabled	Hinweis: Bei dieser Regel untersche iden sich die Regel-ID (MULTI_RE GION_CLOU D_TRAIL_ENABLED) und der Regelname (). multi-region-cloudtrail-enabled Stellen Sie sicher, dass mindesten s eine Region mit mehreren Regionen vorhanden ist. AWS CloudTrail Die Regel ist NON_COMPL IANT, wenn die Trails nicht mit den Eingabeparametern übereinstimmen. Die Regel lautet NON_COMPLIANT, wenn das ExcludeMa nagementEventSourc es Feld nicht leer ist oder wenn sie so konfiguriert AWS CloudTrail ist, dass Verwaltungsereigni sse wie AWS KMS-Ereignisse oder Amazon RDS-Daten -API-Ereignisse

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			ausgeschlossen werden.
10.2.1.2	Auditprotokolle werden implementiert, um die Erkennung von Anomalien und verdächtigen Aktivitäten sowie die forensische Analyse von Ereignissen zu unterstützen. (PCI-DSS-v4.0)	appsync-logging-enabled	Stellen Sie sicher, dass für eine API die Protokollierung aktiviert ist. AWS AppSync Die Regel lautet NON_COMPLIANT, wenn die Protokollierung nicht aktiviert ist, oder 'fieldLogLevel' ist weder ERROR noch ALL.
10.2.1.2	Auditprotokolle werden implementiert, um die Erkennung von Anomalien und verdächtigen Aktivitäten sowie die forensische Analyse von Ereignissen zu unterstützen. (PCI-DSS-v4.0)	mq-cloudwatch-audit-logging-aktiviert	Stellen Sie sicher, dass Amazon MQ-Broker die CloudWatch Amazon-Auditprotokollierung aktiviert haben. Die Regel ist NON_COMPLIANT, wenn für einen Broker die Audit-Protokollierung nicht aktiviert ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.2.1.2	Auditprotokolle werden implementiert, um die Erkennung von Anomalien und verdächtigen Aktivitäten sowie die forensische Analyse von Ereignissen zu unterstützen. (PCI-DSS-v4.0)	mq-cloudwatch-audit-log-aktiviert	Stellen Sie sicher, dass bei einem Amazon MQ-Broker die CloudWatch Auditprotokollierung aktiviert ist. Die Regel lautet NON_COMPLIANT, wenn für den Broker die Audit-Protokollierung nicht aktiviert ist.
10.2.1.2	Auditprotokolle werden implementiert, um die Erkennung von Anomalien und verdächtigen Aktivitäten sowie die forensische Analyse von Ereignissen zu unterstützen. (PCI-DSS-v4.0)	eks-cluster-logging-enabled	Stellen Sie sicher, dass ein Amazon Elastic Kubernetes Service (Amazon EKS) -Cluster mit aktivierter Protokollierung konfiguriert ist. Die Regel ist NON_COMPLIANT, wenn die Protokollierung für Amazon-EKS-Cluster nicht für alle Protokolltypen aktiviert ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.2.1.2	Auditprotokolle werden implementiert, um die Erkennung von Anomalien und verdächtigen Aktivitäten sowie die forensische Analyse von Ereignissen zu unterstützen. (PCI-DSS-v4.0)	elastic-beanstalk-logs-to-Wolkenbeobachtung	Stellen Sie sicher, dass AWS Elastic Beanstalk Beanstalk -Umgebungen so konfiguriert sind, dass sie Protokolle an Amazon CloudWatch Logs senden. Die Regel lautet NON_COMPLIANT, wenn der Wert von `` StreamLogs falsch ist.
10.2.1.2	Auditprotokolle werden implementiert, um die Erkennung von Anomalien und verdächtigen Aktivitäten sowie die forensische Analyse von Ereignissen zu unterstützen. (PCI-DSS-v4.0)	step-functions-state-machine-Protokollierung aktiviert	Stellen Sie sicher, dass auf der AWS Step Functions Functions-Maschine die Protokollierung aktiviert ist Die Regel ist NON_COMPLIANT, wenn für eine Zustandsmaschine die Protokollierung nicht aktiviert ist oder die Protokollierungskonfiguration nicht auf dem angegebenen Mindestniveau liegt.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.2.1.2	Auditprotokolle werden implementiert, um die Erkennung von Anomalien und verdächtigen Aktivitäten sowie die forensische Analyse von Ereignissen zu unterstützen. (PCI-DSS-v4.0)	netfw-logging-enabled	Stellen Sie sicher, dass die AWS Netzwerk-Firewall-Firewalls die Protokollierung aktiviert haben. Die Regel ist NON_COMPLIANT, wenn kein Protokollierungstyp konfiguriert ist. Sie können angeben, welchen Protokollierungstyp die Regel prüfen soll.
10.2.1.3	Auditprotokolle werden implementiert, um die Erkennung von Anomalien und verdächtigen Aktivitäten sowie die forensische Analyse von Ereignissen zu unterstützen. (PCI-DSS-v4.0)	api-gwv2- access-logs-enabled	Stellen Sie sicher, dass die Amazon API Gateway V2-Stufen die Zugriffsprotokollierung aktiviert haben. Die Regel ist NON_COMPLIANT, wenn 'accessLogSettings' in der Stage-Konfiguration nicht vorhanden ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.2.1.3	Auditprotokolle werden implementiert, um die Erkennung von Anomalien und verdächtigen Aktivitäten sowie die forensische Analyse von Ereignissen zu unterstützen. (PCI-DSS-v4.0)	api-gw-xray-enabled	Stellen Sie sicher, dass AWS X-Ray Tracing auf Amazon API Gateway REST APIs aktiviert ist. Die Regel ist COMPLIANT, wenn die X-Ray-Abl aufverfolgung aktiviert ist, andernfalls ist sie NON_COMPLIANT.
10.2.1.3	Auditprotokolle werden implementiert, um die Erkennung von Anomalien und verdächtigen Aktivitäten sowie die forensische Analyse von Ereignissen zu unterstützen. (PCI-DSS-v4.0)	neptune-cluster-cloudwatch-log-exportfähig	Stellen Sie sicher, dass in einem Amazon Neptune Neptune-Cluster der Protokollexport für CloudWatch Audit-Logs aktiviert ist. Die Regel lautet NON_COMPLIANT, wenn für einen Neptune-Cluster der Protokollexport für CloudWatch Audit-Logs nicht aktiviert ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.2.1.3	Auditprotokolle werden implementiert, um die Erkennung von Anomalien und verdächtigen Aktivitäten sowie die forensische Analyse von Ereignissen zu unterstützen. (PCI-DSS-v4.0)	ecs-task-definition-log-Konfiguration	Stellen Sie sicher, dass LogConfiguration für aktive ECS-Aufgabendefinitionen festgelegt ist. Diese Regel ist NON_COMPLIANT, wenn für eine aktive ECSTask Definition die LogConfiguration-Ressource nicht definiert ist oder der Wert für LogConfiguration in mindestens einer Containerdefinition Null ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.2.1.3	Auditprotokolle werden implementiert, um die Erkennung von Anomalien und verdächtigen Aktivitäten sowie die forensische Analyse von Ereignissen zu unterstützen. (PCI-DSS-v4.0)	cloudtrail-enabled	Hinweis: Bei dieser Regel untersche iden sich die Regel-ID (CLOUD_TR AIL_ENABLED) und der Regelname (cloudtrail-enabled). Stellen Sie sicher, dass in Ihrem Konto ein Trail aktiviert ist AWS CloudTrail . AWS Die Regel ist NON_COMPLIANT, wenn ein Trail nicht aktiviert ist. Optional überprüft die Regel einen bestimmten S3-Bucket, ein Amazon Simple Notification Service (Amazon SNS) -Thema und eine CloudWatch Protokollgruppe.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.2.1.3	Auditprotokolle werden implementiert, um die Erkennung von Anomalien und verdächtigen Aktivitäten sowie die forensische Analyse von Ereignissen zu unterstützen. (PCI-DSS-v4.0)	multi-region-cloudtrail-enabled	Hinweis: Bei dieser Regel untersche iden sich die Regel-ID (MULTI_RE GION_CLOU D_TRAIL_ENABLED) und der Regelname (). multi-region-cloudtrail-enabled Stellen Sie sicher, dass mindesten s eine Region mit mehreren Regionen vorhanden ist. AWS CloudTrail Die Regel ist NON_COMPL IANT, wenn die Trails nicht mit den Eingabeparametern übereinstimmen. Die Regel lautet NON_COMPLIANT, wenn das ExcludeMa nagementEventSourc es Feld nicht leer ist oder wenn sie so konfiguriert AWS CloudTrail ist, dass Verwaltungsereigni sse wie AWS KMS-Ereignisse oder Amazon RDS-Daten -API-Ereignisse

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			ausgeschlossen werden.
10.2.1.3	Auditprotokolle werden implementiert, um die Erkennung von Anomalien und verdächtigen Aktivitäten sowie die forensische Analyse von Ereignissen zu unterstützen. (PCI-DSS-v4.0)	appsync-logging-enabled	Stellen Sie sicher, dass für eine API die Protokollierung aktiviert ist. AWS AppSync Die Regel lautet NON_COMPLIANT, wenn die Protokollierung nicht aktiviert ist, oder 'fieldLogLevel' ist weder ERROR noch ALL.
10.2.1.3	Auditprotokolle werden implementiert, um die Erkennung von Anomalien und verdächtigen Aktivitäten sowie die forensische Analyse von Ereignissen zu unterstützen. (PCI-DSS-v4.0)	mq-cloudwatch-audit-logging-aktiviert	Stellen Sie sicher, dass Amazon MQ-Broker die CloudWatch Amazon-Auditprotokollierung aktiviert haben. Die Regel ist NON_COMPLIANT, wenn für einen Broker die Audit-Protokollierung nicht aktiviert ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.2.1.3	Auditprotokolle werden implementiert, um die Erkennung von Anomalien und verdächtigen Aktivitäten sowie die forensische Analyse von Ereignissen zu unterstützen. (PCI-DSS-v4.0)	mq-cloudwatch-audit-log-aktiviert	Stellen Sie sicher, dass bei einem Amazon MQ-Broker die CloudWatch Auditprotokollierung aktiviert ist. Die Regel lautet NON_COMPLIANT, wenn für den Broker die Audit-Protokollierung nicht aktiviert ist.
10.2.1.3	Auditprotokolle werden implementiert, um die Erkennung von Anomalien und verdächtigen Aktivitäten sowie die forensische Analyse von Ereignissen zu unterstützen. (PCI-DSS-v4.0)	eks-cluster-logging-enabled	Stellen Sie sicher, dass ein Amazon Elastic Kubernetes Service (Amazon EKS) -Cluster mit aktivierter Protokollierung konfiguriert ist. Die Regel ist NON_COMPLIANT, wenn die Protokollierung für Amazon-EKS-Cluster nicht für alle Protokolltypen aktiviert ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.2.1.3	Auditprotokolle werden implementiert, um die Erkennung von Anomalien und verdächtigen Aktivitäten sowie die forensische Analyse von Ereignissen zu unterstützen. (PCI-DSS-v4.0)	elastic-beanstalk-logs-to-Wolkenbeobachtung	Stellen Sie sicher, dass AWS Elastic Beanstalk Beanstalk -Umgebungen so konfiguriert sind, dass sie Protokolle an Amazon CloudWatch Logs senden. Die Regel lautet NON_COMPLIANT, wenn der Wert von `` StreamLogs falsch ist.
10.2.1.3	Auditprotokolle werden implementiert, um die Erkennung von Anomalien und verdächtigen Aktivitäten sowie die forensische Analyse von Ereignissen zu unterstützen. (PCI-DSS-v4.0)	step-functions-state-machine-Protokollierung aktiviert	Stellen Sie sicher, dass auf der AWS Step Functions Functions-Maschine die Protokollierung aktiviert ist Die Regel ist NON_COMPLIANT, wenn für eine Zustandsmaschine die Protokollierung nicht aktiviert ist oder die Protokollierungskonfiguration nicht auf dem angegebenen Mindestniveau liegt.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.2.1.3	Auditprotokolle werden implementiert, um die Erkennung von Anomalien und verdächtigen Aktivitäten sowie die forensische Analyse von Ereignissen zu unterstützen. (PCI-DSS-v4.0)	netfw-logging-enabled	Stellen Sie sicher, dass die AWS Netzwerk-Firewall-Firewalls die Protokollierung aktiviert haben. Die Regel ist NON_COMPLIANT, wenn kein Protokollierungstyp konfiguriert ist. Sie können angeben, welchen Protokollierungstyp die Regel prüfen soll.
10.2.1.4	Auditprotokolle werden implementiert, um die Erkennung von Anomalien und verdächtigen Aktivitäten sowie die forensische Analyse von Ereignissen zu unterstützen. (PCI-DSS-v4.0)	api-gwv2- access-logs-enabled	Stellen Sie sicher, dass die Amazon API Gateway V2-Stufen die Zugriffsprotokollierung aktiviert haben. Die Regel ist NON_COMPLIANT, wenn 'accessLogSettings' in der Stage-Konfiguration nicht vorhanden ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.2.1.4	Auditprotokolle werden implementiert, um die Erkennung von Anomalien und verdächtigen Aktivitäten sowie die forensische Analyse von Ereignissen zu unterstützen. (PCI-DSS-v4.0)	api-gw-xray-enabled	Stellen Sie sicher, dass AWS X-Ray Tracing auf Amazon API Gateway REST APIs aktiviert ist. Die Regel ist COMPLIANT, wenn die X-Ray-Abl aufverfolgung aktiviert ist, andernfalls ist sie NON_COMPLIANT.
10.2.1.4	Auditprotokolle werden implementiert, um die Erkennung von Anomalien und verdächtigen Aktivitäten sowie die forensische Analyse von Ereignissen zu unterstützen. (PCI-DSS-v4.0)	neptune-cluster-cloudwatch-log-exportfähig	Stellen Sie sicher, dass in einem Amazon Neptune Neptune-Cluster der Protokollexport für CloudWatch Audit-Logs aktiviert ist. Die Regel lautet NON_COMPLIANT, wenn für einen Neptune-Cluster der Protokollexport für CloudWatch Audit-Logs nicht aktiviert ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.2.1.4	Auditprotokolle werden implementiert, um die Erkennung von Anomalien und verdächtigen Aktivitäten sowie die forensische Analyse von Ereignissen zu unterstützen. (PCI-DSS-v4.0)	ecs-task-definition-log-Konfiguration	Stellen Sie sicher, dass LogConfiguration für aktive ECS-Aufgabendefinitionen festgelegt ist. Diese Regel ist NON_COMPLIANT, wenn für eine aktive ECSTask Definition die LogConfiguration-Ressource nicht definiert ist oder der Wert für LogConfiguration in mindestens einer Containerdefinition Null ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.2.1.4	Auditprotokolle werden implementiert, um die Erkennung von Anomalien und verdächtigen Aktivitäten sowie die forensische Analyse von Ereignissen zu unterstützen. (PCI-DSS-v4.0)	cloudtrail-enabled	Hinweis: Bei dieser Regel untersche iden sich die Regel-ID (CLOUD_TR AIL_ENABLED) und der Regelname (cloudtrail-enabled). Stellen Sie sicher, dass in Ihrem Konto ein Trail aktiviert ist AWS CloudTrail . AWS Die Regel ist NON_COMPLIANT, wenn ein Trail nicht aktiviert ist. Optional überprüft die Regel einen bestimmten S3-Bucket, ein Amazon Simple Notification Service (Amazon SNS) -Thema und eine CloudWatch Protokollgruppe.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.2.1.4	Auditprotokolle werden implementiert, um die Erkennung von Anomalien und verdächtigen Aktivitäten sowie die forensische Analyse von Ereignissen zu unterstützen. (PCI-DSS-v4.0)	multi-region-cloudtrail-enabled	Hinweis: Bei dieser Regel untersche iden sich die Regel-ID (MULTI_RE GION_CLOU D_TRAIL_ENABLED) und der Regelname (). multi-region-cloudtrail-enabled Stellen Sie sicher, dass mindesten s eine Region mit mehreren Regionen vorhanden ist. AWS CloudTrail Die Regel ist NON_COMPL IANT, wenn die Trails nicht mit den Eingabeparametern übereinstimmen. Die Regel lautet NON_COMPLIANT, wenn das ExcludeMa nagementEventSourc es Feld nicht leer ist oder wenn sie so konfiguriert AWS CloudTrail ist, dass Verwaltungsereigni sse wie AWS KMS-Ereignisse oder Amazon RDS-Daten -API-Ereignisse

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			ausgeschlossen werden.
10.2.1.4	Auditprotokolle werden implementiert, um die Erkennung von Anomalien und verdächtigen Aktivitäten sowie die forensische Analyse von Ereignissen zu unterstützen. (PCI-DSS-v4.0)	appsync-logging-enabled	Stellen Sie sicher, dass für eine API die Protokollierung aktiviert ist. AWS AppSync Die Regel lautet NON_COMPLIANT, wenn die Protokollierung nicht aktiviert ist, oder 'fieldLogLevel' ist weder ERROR noch ALL.
10.2.1.4	Auditprotokolle werden implementiert, um die Erkennung von Anomalien und verdächtigen Aktivitäten sowie die forensische Analyse von Ereignissen zu unterstützen. (PCI-DSS-v4.0)	mq-cloudwatch-audit-logging-aktiviert	Stellen Sie sicher, dass Amazon MQ-Broker die CloudWatch Amazon-Auditprotokollierung aktiviert haben. Die Regel ist NON_COMPLIANT, wenn für einen Broker die Audit-Protokollierung nicht aktiviert ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.2.1.4	Auditprotokolle werden implementiert, um die Erkennung von Anomalien und verdächtigen Aktivitäten sowie die forensische Analyse von Ereignissen zu unterstützen. (PCI-DSS-v4.0)	mq-cloudwatch-audit-log-aktiviert	Stellen Sie sicher, dass bei einem Amazon MQ-Broker die CloudWatch Auditprotokollierung aktiviert ist. Die Regel lautet NON_COMPLIANT, wenn für den Broker die Audit-Protokollierung nicht aktiviert ist.
10.2.1.4	Auditprotokolle werden implementiert, um die Erkennung von Anomalien und verdächtigen Aktivitäten sowie die forensische Analyse von Ereignissen zu unterstützen. (PCI-DSS-v4.0)	eks-cluster-logging-enabled	Stellen Sie sicher, dass ein Amazon Elastic Kubernetes Service (Amazon EKS) -Cluster mit aktivierter Protokollierung konfiguriert ist. Die Regel ist NON_COMPLIANT, wenn die Protokollierung für Amazon-EKS-Cluster nicht für alle Protokolltypen aktiviert ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.2.1.4	Auditprotokolle werden implementiert, um die Erkennung von Anomalien und verdächtigen Aktivitäten sowie die forensische Analyse von Ereignissen zu unterstützen. (PCI-DSS-v4.0)	elastic-beanstalk-logs-to-Wolkenbeobachtung	Stellen Sie sicher, dass AWS Elastic Beanstalk Beanstalk -Umgebungen so konfiguriert sind, dass sie Protokolle an Amazon CloudWatch Logs senden. Die Regel lautet NON_COMPLIANT, wenn der Wert von `` StreamLogs falsch ist.
10.2.1.4	Auditprotokolle werden implementiert, um die Erkennung von Anomalien und verdächtigen Aktivitäten sowie die forensische Analyse von Ereignissen zu unterstützen. (PCI-DSS-v4.0)	step-functions-state-machine-Protokollierung aktiviert	Stellen Sie sicher, dass auf der AWS Step Functions Functions-Maschine die Protokollierung aktiviert ist Die Regel ist NON_COMPLIANT, wenn für eine Zustandsmaschine die Protokollierung nicht aktiviert ist oder die Protokollierungskonfiguration nicht auf dem angegebenen Mindestniveau liegt.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.2.1.4	Auditprotokolle werden implementiert, um die Erkennung von Anomalien und verdächtigen Aktivitäten sowie die forensische Analyse von Ereignissen zu unterstützen. (PCI-DSS-v4.0)	netfw-logging-enabled	Stellen Sie sicher, dass die AWS Netzwerk-Firewall-Firewalls die Protokollierung aktiviert haben. Die Regel ist NON_COMPLIANT, wenn kein Protokollierungstyp konfiguriert ist. Sie können angeben, welchen Protokollierungstyp die Regel prüfen soll.
10.2.1.5	Auditprotokolle werden implementiert, um die Erkennung von Anomalien und verdächtigen Aktivitäten sowie die forensische Analyse von Ereignissen zu unterstützen. (PCI-DSS-v4.0)	api-gwv2- access-logs-enabled	Stellen Sie sicher, dass die Amazon API Gateway V2-Stufen die Zugriffsprotokollierung aktiviert haben. Die Regel ist NON_COMPLIANT, wenn 'accessLogSettings' in der Stage-Konfiguration nicht vorhanden ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.2.1.5	Auditprotokolle werden implementiert, um die Erkennung von Anomalien und verdächtigen Aktivitäten sowie die forensische Analyse von Ereignissen zu unterstützen. (PCI-DSS-v4.0)	api-gw-xray-enabled	Stellen Sie sicher, dass AWS X-Ray Tracing auf Amazon API Gateway REST APIs aktiviert ist. Die Regel ist COMPLIANT, wenn die X-Ray-Abl aufverfolgung aktiviert ist, andernfalls ist sie NON_COMPLIANT.
10.2.1.5	Auditprotokolle werden implementiert, um die Erkennung von Anomalien und verdächtigen Aktivitäten sowie die forensische Analyse von Ereignissen zu unterstützen. (PCI-DSS-v4.0)	neptune-cluster-cloudwatch-log-exportfähig	Stellen Sie sicher, dass in einem Amazon Neptune Neptune-Cluster der Protokollexport für CloudWatch Audit-Logs aktiviert ist. Die Regel lautet NON_COMPLIANT, wenn für einen Neptune-Cluster der Protokollexport für CloudWatch Audit-Logs nicht aktiviert ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.2.1.5	Auditprotokolle werden implementiert, um die Erkennung von Anomalien und verdächtigen Aktivitäten sowie die forensische Analyse von Ereignissen zu unterstützen. (PCI-DSS-v4.0)	ecs-task-definition-log-Konfiguration	Stellen Sie sicher, dass LogConfiguration für aktive ECS-Aufgabendefinitionen festgelegt ist. Diese Regel ist NON_COMPLIANT, wenn für eine aktive ECSTask Definition die LogConfiguration-Ressource nicht definiert ist oder der Wert für LogConfiguration in mindestens einer Containerdefinition Null ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.2.1.5	Auditprotokolle werden implementiert, um die Erkennung von Anomalien und verdächtigen Aktivitäten sowie die forensische Analyse von Ereignissen zu unterstützen. (PCI-DSS-v4.0)	cloudtrail-enabled	Hinweis: Bei dieser Regel untersche iden sich die Regel-ID (CLOUD_TR AIL_ENABLED) und der Regelname (cloudtrail-enabled). Stellen Sie sicher, dass in Ihrem Konto ein Trail aktiviert ist AWS CloudTrail . AWS Die Regel ist NON_COMPLIANT, wenn ein Trail nicht aktiviert ist. Optional überprüft die Regel einen bestimmten S3-Bucket, ein Amazon Simple Notification Service (Amazon SNS) -Thema und eine CloudWatch Protokollgruppe.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.2.1.5	Auditprotokolle werden implementiert, um die Erkennung von Anomalien und verdächtigen Aktivitäten sowie die forensische Analyse von Ereignissen zu unterstützen. (PCI-DSS-v4.0)	multi-region-cloudtrail-enabled	Hinweis: Bei dieser Regel untersche iden sich die Regel-ID (MULTI_RE GION_CLOU D_TRAIL_ENABLED) und der Regelname (). multi-region-cloudtrail-enabled Stellen Sie sicher, dass mindesten s eine Region mit mehreren Regionen vorhanden ist. AWS CloudTrail Die Regel ist NON_COMPL IANT, wenn die Trails nicht mit den Eingabeparametern übereinstimmen. Die Regel lautet NON_COMPLIANT, wenn das ExcludeMa nagementEventSourc es Feld nicht leer ist oder wenn sie so konfiguriert AWS CloudTrail ist, dass Verwaltungsereigni sse wie AWS KMS-Ereignisse oder Amazon RDS-Daten -API-Ereignisse

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			ausgeschlossen werden.
10.2.1.5	Auditprotokolle werden implementiert, um die Erkennung von Anomalien und verdächtigen Aktivitäten sowie die forensische Analyse von Ereignissen zu unterstützen. (PCI-DSS-v4.0)	appsync-logging-enabled	Stellen Sie sicher, dass für eine API die Protokollierung aktiviert ist. AWS AppSync Die Regel lautet NON_COMPLIANT, wenn die Protokollierung nicht aktiviert ist, oder 'fieldLogLevel' ist weder ERROR noch ALL.
10.2.1.5	Auditprotokolle werden implementiert, um die Erkennung von Anomalien und verdächtigen Aktivitäten sowie die forensische Analyse von Ereignissen zu unterstützen. (PCI-DSS-v4.0)	mq-cloudwatch-audit-logging-aktiviert	Stellen Sie sicher, dass Amazon MQ-Broker die CloudWatch Amazon-Auditprotokollierung aktiviert haben. Die Regel ist NON_COMPLIANT, wenn für einen Broker die Audit-Protokollierung nicht aktiviert ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.2.1.5	Auditprotokolle werden implementiert, um die Erkennung von Anomalien und verdächtigen Aktivitäten sowie die forensische Analyse von Ereignissen zu unterstützen. (PCI-DSS-v4.0)	mq-cloudwatch-audit-log-aktiviert	Stellen Sie sicher, dass bei einem Amazon MQ-Broker die CloudWatch Auditprotokollierung aktiviert ist. Die Regel lautet NON_COMPLIANT, wenn für den Broker die Audit-Protokollierung nicht aktiviert ist.
10.2.1.5	Auditprotokolle werden implementiert, um die Erkennung von Anomalien und verdächtigen Aktivitäten sowie die forensische Analyse von Ereignissen zu unterstützen. (PCI-DSS-v4.0)	eks-cluster-logging-enabled	Stellen Sie sicher, dass ein Amazon Elastic Kubernetes Service (Amazon EKS) -Cluster mit aktivierter Protokollierung konfiguriert ist. Die Regel ist NON_COMPLIANT, wenn die Protokollierung für Amazon-EKS-Cluster nicht für alle Protokolltypen aktiviert ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.2.1.5	Auditprotokolle werden implementiert, um die Erkennung von Anomalien und verdächtigen Aktivitäten sowie die forensische Analyse von Ereignissen zu unterstützen. (PCI-DSS-v4.0)	elastic-beanstalk-logs-to-Wolkenbeobachtung	Stellen Sie sicher, dass AWS Elastic Beanstalk Beanstalk -Umgebungen so konfiguriert sind, dass sie Protokolle an Amazon CloudWatch Logs senden. Die Regel lautet NON_COMPLIANT, wenn der Wert von `` StreamLogs falsch ist.
10.2.1.5	Auditprotokolle werden implementiert, um die Erkennung von Anomalien und verdächtigen Aktivitäten sowie die forensische Analyse von Ereignissen zu unterstützen. (PCI-DSS-v4.0)	step-functions-state-machine-Protokollierung aktiviert	Stellen Sie sicher, dass auf der AWS Step Functions Functions-Maschine die Protokollierung aktiviert ist Die Regel ist NON_COMPLIANT, wenn für eine Zustandsmaschine die Protokollierung nicht aktiviert ist oder die Protokollierungskonfiguration nicht auf dem angegebenen Mindestniveau liegt.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.2.1.5	Auditprotokolle werden implementiert, um die Erkennung von Anomalien und verdächtigen Aktivitäten sowie die forensische Analyse von Ereignissen zu unterstützen. (PCI-DSS-v4.0)	netfw-logging-enabled	Stellen Sie sicher, dass die AWS Netzwerk-Firewall-Firewalls die Protokollierung aktiviert haben. Die Regel ist NON_COMPLIANT, wenn kein Protokollierungstyp konfiguriert ist. Sie können angeben, welchen Protokollierungstyp die Regel prüfen soll.
10.2.1.6	Auditprotokolle werden implementiert, um die Erkennung von Anomalien und verdächtigen Aktivitäten sowie die forensische Analyse von Ereignissen zu unterstützen. (PCI-DSS-v4.0)	api-gwv2- access-logs-enabled	Stellen Sie sicher, dass die Amazon API Gateway V2-Stufen die Zugriffsprotokollierung aktiviert haben. Die Regel ist NON_COMPLIANT, wenn 'accessLogSettings' in der Stage-Konfiguration nicht vorhanden ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.2.1.6	Auditprotokolle werden implementiert, um die Erkennung von Anomalien und verdächtigen Aktivitäten sowie die forensische Analyse von Ereignissen zu unterstützen. (PCI-DSS-v4.0)	api-gw-xray-enabled	Stellen Sie sicher, dass AWS X-Ray Tracing auf Amazon API Gateway REST APIs aktiviert ist. Die Regel ist COMPLIANT, wenn die X-Ray-Abl aufverfolgung aktiviert ist, andernfalls ist sie NON_COMPLIANT.
10.2.1.6	Auditprotokolle werden implementiert, um die Erkennung von Anomalien und verdächtigen Aktivitäten sowie die forensische Analyse von Ereignissen zu unterstützen. (PCI-DSS-v4.0)	neptune-cluster-cloudwatch-log-exportfähig	Stellen Sie sicher, dass in einem Amazon Neptune Neptune-Cluster der Protokollexport für CloudWatch Audit-Logs aktiviert ist. Die Regel lautet NON_COMPLIANT, wenn für einen Neptune-Cluster der Protokollexport für CloudWatch Audit-Logs nicht aktiviert ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.2.1.6	Auditprotokolle werden implementiert, um die Erkennung von Anomalien und verdächtigen Aktivitäten sowie die forensische Analyse von Ereignissen zu unterstützen. (PCI-DSS-v4.0)	ecs-task-definition-log-Konfiguration	Stellen Sie sicher, dass LogConfiguration für aktive ECS-Aufgabendefinitionen festgelegt ist. Diese Regel ist NON_COMPLIANT, wenn für eine aktive ECSTask Definition die LogConfiguration-Ressource nicht definiert ist oder der Wert für LogConfiguration in mindestens einer Containerdefinition Null ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.2.1.6	Auditprotokolle werden implementiert, um die Erkennung von Anomalien und verdächtigen Aktivitäten sowie die forensische Analyse von Ereignissen zu unterstützen. (PCI-DSS-v4.0)	cloudtrail-enabled	Hinweis: Bei dieser Regel untersche iden sich die Regel-ID (CLOUD_TR AIL_ENABLED) und der Regelname (cloudtrail-enabled). Stellen Sie sicher, dass in Ihrem Konto ein Trail aktiviert ist AWS CloudTrail . AWS Die Regel ist NON_COMPLIANT, wenn ein Trail nicht aktiviert ist. Optional überprüft die Regel einen bestimmten S3-Bucket, ein Amazon Simple Notification Service (Amazon SNS) -Thema und eine CloudWatch Protokollgruppe.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.2.1.6	Auditprotokolle werden implementiert, um die Erkennung von Anomalien und verdächtigen Aktivitäten sowie die forensische Analyse von Ereignissen zu unterstützen. (PCI-DSS-v4.0)	multi-region-cloudtrail-enabled	Hinweis: Bei dieser Regel untersche iden sich die Regel-ID (MULTI_RE GION_CLOU D_TRAIL_ENABLED) und der Regelname (). multi-region-cloudtrail-enabled Stellen Sie sicher, dass mindesten s eine Region mit mehreren Regionen vorhanden ist. AWS CloudTrail Die Regel ist NON_COMPL IANT, wenn die Trails nicht mit den Eingabeparametern übereinstimmen. Die Regel lautet NON_COMPLIANT, wenn das ExcludeMa nagementEventSourc es Feld nicht leer ist oder wenn sie so konfiguriert AWS CloudTrail ist, dass Verwaltungsereigni sse wie AWS KMS-Ereignisse oder Amazon RDS-Daten -API-Ereignisse

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			ausgeschlossen werden.
10.2.1.6	Auditprotokolle werden implementiert, um die Erkennung von Anomalien und verdächtigen Aktivitäten sowie die forensische Analyse von Ereignissen zu unterstützen. (PCI-DSS-v4.0)	appsync-logging-enabled	Stellen Sie sicher, dass für eine API die Protokollierung aktiviert ist. AWS AppSync Die Regel lautet NON_COMPLIANT, wenn die Protokollierung nicht aktiviert ist, oder 'fieldLogLevel' ist weder ERROR noch ALL.
10.2.1.6	Auditprotokolle werden implementiert, um die Erkennung von Anomalien und verdächtigen Aktivitäten sowie die forensische Analyse von Ereignissen zu unterstützen. (PCI-DSS-v4.0)	mq-cloudwatch-audit-logging-aktiviert	Stellen Sie sicher, dass Amazon MQ-Broker die CloudWatch Amazon-Auditprotokollierung aktiviert haben. Die Regel ist NON_COMPLIANT, wenn für einen Broker die Audit-Protokollierung nicht aktiviert ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.2.1.6	Auditprotokolle werden implementiert, um die Erkennung von Anomalien und verdächtigen Aktivitäten sowie die forensische Analyse von Ereignissen zu unterstützen. (PCI-DSS-v4.0)	mq-cloudwatch-audit-log-aktiviert	Stellen Sie sicher, dass bei einem Amazon MQ-Broker die CloudWatch Auditprotokollierung aktiviert ist. Die Regel lautet NON_COMPLIANT, wenn für den Broker die Audit-Protokollierung nicht aktiviert ist.
10.2.1.6	Auditprotokolle werden implementiert, um die Erkennung von Anomalien und verdächtigen Aktivitäten sowie die forensische Analyse von Ereignissen zu unterstützen. (PCI-DSS-v4.0)	eks-cluster-logging-enabled	Stellen Sie sicher, dass ein Amazon Elastic Kubernetes Service (Amazon EKS) -Cluster mit aktivierter Protokollierung konfiguriert ist. Die Regel ist NON_COMPLIANT, wenn die Protokollierung für Amazon-EKS-Cluster nicht für alle Protokolltypen aktiviert ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.2.1.6	Auditprotokolle werden implementiert, um die Erkennung von Anomalien und verdächtigen Aktivitäten sowie die forensische Analyse von Ereignissen zu unterstützen. (PCI-DSS-v4.0)	elastic-beanstalk-logs-to-Wolkenbeobachtung	Stellen Sie sicher, dass AWS Elastic Beanstalk Beanstalk -Umgebungen so konfiguriert sind, dass sie Protokolle an Amazon CloudWatch Logs senden. Die Regel lautet NON_COMPLIANT, wenn der Wert von `` StreamLogs falsch ist.
10.2.1.6	Auditprotokolle werden implementiert, um die Erkennung von Anomalien und verdächtigen Aktivitäten sowie die forensische Analyse von Ereignissen zu unterstützen. (PCI-DSS-v4.0)	step-functions-state-machine-Protokollierung aktiviert	Stellen Sie sicher, dass auf der AWS Step Functions Functions-Maschine die Protokollierung aktiviert ist Die Regel ist NON_COMPLIANT, wenn für eine Zustandsmaschine die Protokollierung nicht aktiviert ist oder die Protokollierungskonfiguration nicht auf dem angegebenen Mindestniveau liegt.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.2.1.6	Auditprotokolle werden implementiert, um die Erkennung von Anomalien und verdächtigen Aktivitäten sowie die forensische Analyse von Ereignissen zu unterstützen. (PCI-DSS-v4.0)	netfw-logging-enabled	Stellen Sie sicher, dass die AWS Netzwerk-Firewall-Firewalls die Protokollierung aktiviert haben. Die Regel ist NON_COMPLIANT, wenn kein Protokollierungstyp konfiguriert ist. Sie können angeben, welchen Protokollierungstyp die Regel prüfen soll.
10.2.1.7	Auditprotokolle werden implementiert, um die Erkennung von Anomalien und verdächtigen Aktivitäten sowie die forensische Analyse von Ereignissen zu unterstützen. (PCI-DSS-v4.0)	api-gwv2- access-logs-enabled	Stellen Sie sicher, dass die Amazon API Gateway V2-Stufen die Zugriffsprotokollierung aktiviert haben. Die Regel ist NON_COMPLIANT, wenn 'accessLogSettings' in der Stage-Konfiguration nicht vorhanden ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.2.1.7	Auditprotokolle werden implementiert, um die Erkennung von Anomalien und verdächtigen Aktivitäten sowie die forensische Analyse von Ereignissen zu unterstützen. (PCI-DSS-v4.0)	api-gw-xray-enabled	Stellen Sie sicher, dass AWS X-Ray Tracing auf Amazon API Gateway REST APIs aktiviert ist. Die Regel ist COMPLIANT, wenn die X-Ray-Abl aufverfolgung aktiviert ist, andernfalls ist sie NON_COMPLIANT.
10.2.1.7	Auditprotokolle werden implementiert, um die Erkennung von Anomalien und verdächtigen Aktivitäten sowie die forensische Analyse von Ereignissen zu unterstützen. (PCI-DSS-v4.0)	neptune-cluster-cloudwatch-log-exportfähig	Stellen Sie sicher, dass in einem Amazon Neptune Neptune-Cluster der Protokollexport für CloudWatch Audit-Logs aktiviert ist. Die Regel lautet NON_COMPLIANT, wenn für einen Neptune-Cluster der Protokollexport für CloudWatch Audit-Logs nicht aktiviert ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.2.1.7	Auditprotokolle werden implementiert, um die Erkennung von Anomalien und verdächtigen Aktivitäten sowie die forensische Analyse von Ereignissen zu unterstützen. (PCI-DSS-v4.0)	ecs-task-definition-log-Konfiguration	Stellen Sie sicher, dass LogConfiguration für aktive ECS-Aufgabendefinitionen festgelegt ist. Diese Regel ist NON_COMPLIANT, wenn für eine aktive ECSTask Definition die LogConfiguration-Ressource nicht definiert ist oder der Wert für LogConfiguration in mindestens einer Containerdefinition Null ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.2.1.7	Auditprotokolle werden implementiert, um die Erkennung von Anomalien und verdächtigen Aktivitäten sowie die forensische Analyse von Ereignissen zu unterstützen. (PCI-DSS-v4.0)	cloudtrail-enabled	Hinweis: Bei dieser Regel untersche iden sich die Regel-ID (CLOUD_TR AIL_ENABLED) und der Regelname (cloudtrail-enabled). Stellen Sie sicher, dass in Ihrem Konto ein Trail aktiviert ist AWS CloudTrail . AWS Die Regel ist NON_COMPLIANT, wenn ein Trail nicht aktiviert ist. Optional überprüft die Regel einen bestimmten S3-Bucket, ein Amazon Simple Notification Service (Amazon SNS) -Thema und eine CloudWatch Protokollgruppe.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.2.1.7	Auditprotokolle werden implementiert, um die Erkennung von Anomalien und verdächtigen Aktivitäten sowie die forensische Analyse von Ereignissen zu unterstützen. (PCI-DSS-v4.0)	multi-region-cloudtrail-enabled	Hinweis: Bei dieser Regel untersche iden sich die Regel-ID (MULTI_RE GION_CLOU D_TRAIL_ENABLED) und der Regelname (). multi-region-cloudtrail-enabled Stellen Sie sicher, dass mindesten s eine Region mit mehreren Regionen vorhanden ist. AWS CloudTrail Die Regel ist NON_COMPL IANT, wenn die Trails nicht mit den Eingabeparametern übereinstimmen. Die Regel lautet NON_COMPLIANT, wenn das ExcludeMa nagementEventSourc es Feld nicht leer ist oder wenn sie so konfiguriert AWS CloudTrail ist, dass Verwaltungsereigni sse wie AWS KMS-Ereignisse oder Amazon RDS-Daten -API-Ereignisse

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			ausgeschlossen werden.
10.2.1.7	Auditprotokolle werden implementiert, um die Erkennung von Anomalien und verdächtigen Aktivitäten sowie die forensische Analyse von Ereignissen zu unterstützen. (PCI-DSS-v4.0)	appsync-logging-enabled	Stellen Sie sicher, dass für eine API die Protokollierung aktiviert ist. AWS AppSync Die Regel lautet NON_COMPLIANT, wenn die Protokollierung nicht aktiviert ist, oder 'fieldLogLevel' ist weder ERROR noch ALL.
10.2.1.7	Auditprotokolle werden implementiert, um die Erkennung von Anomalien und verdächtigen Aktivitäten sowie die forensische Analyse von Ereignissen zu unterstützen. (PCI-DSS-v4.0)	mq-cloudwatch-audit-logging-aktiviert	Stellen Sie sicher, dass Amazon MQ-Broker die CloudWatch Amazon-Auditprotokollierung aktiviert haben. Die Regel ist NON_COMPLIANT, wenn für einen Broker die Audit-Protokollierung nicht aktiviert ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.2.1.7	Auditprotokolle werden implementiert, um die Erkennung von Anomalien und verdächtigen Aktivitäten sowie die forensische Analyse von Ereignissen zu unterstützen. (PCI-DSS-v4.0)	mq-cloudwatch-audit-log-aktiviert	Stellen Sie sicher, dass bei einem Amazon MQ-Broker die CloudWatch Auditprotokollierung aktiviert ist. Die Regel lautet NON_COMPLIANT, wenn für den Broker die Audit-Protokollierung nicht aktiviert ist.
10.2.1.7	Auditprotokolle werden implementiert, um die Erkennung von Anomalien und verdächtigen Aktivitäten sowie die forensische Analyse von Ereignissen zu unterstützen. (PCI-DSS-v4.0)	eks-cluster-logging-enabled	Stellen Sie sicher, dass ein Amazon Elastic Kubernetes Service (Amazon EKS) -Cluster mit aktivierter Protokollierung konfiguriert ist. Die Regel ist NON_COMPLIANT, wenn die Protokollierung für Amazon-EKS-Cluster nicht für alle Protokolltypen aktiviert ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.2.1.7	Auditprotokolle werden implementiert, um die Erkennung von Anomalien und verdächtigen Aktivitäten sowie die forensische Analyse von Ereignissen zu unterstützen. (PCI-DSS-v4.0)	elastic-beanstalk-logs-to-Wolkenbeobachtung	Stellen Sie sicher, dass AWS Elastic Beanstalk Beanstalk -Umgebungen so konfiguriert sind, dass sie Protokolle an Amazon CloudWatch Logs senden. Die Regel lautet NON_COMPLIANT, wenn der Wert von `` StreamLogs falsch ist.
10.2.1.7	Auditprotokolle werden implementiert, um die Erkennung von Anomalien und verdächtigen Aktivitäten sowie die forensische Analyse von Ereignissen zu unterstützen. (PCI-DSS-v4.0)	step-functions-state-machine-Protokollierung aktiviert	Stellen Sie sicher, dass auf der AWS Step Functions Functions-Maschine die Protokollierung aktiviert ist Die Regel ist NON_COMPLIANT, wenn für eine Zustandsmaschine die Protokollierung nicht aktiviert ist oder die Protokollierungskonfiguration nicht auf dem angegebenen Mindestniveau liegt.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.2.1.7	Auditprotokolle werden implementiert, um die Erkennung von Anomalien und verdächtigen Aktivitäten sowie die forensische Analyse von Ereignissen zu unterstützen. (PCI-DSS-v4.0)	netfw-logging-enabled	Stellen Sie sicher, dass die AWS Netzwerk-Firewall-Firewalls die Protokollierung aktiviert haben. Die Regel ist NON_COMPLIANT, wenn kein Protokollierungstyp konfiguriert ist. Sie können angeben, welchen Protokollierungstyp die Regel prüfen soll.
10.2.2	Auditprotokolle werden implementiert, um die Erkennung von Anomalien und verdächtigen Aktivitäten sowie die forensische Analyse von Ereignissen zu unterstützen. (PCI-DSS-v4.0)	api-gwv2- access-logs-enabled	Stellen Sie sicher, dass die Amazon API Gateway V2-Stufen die Zugriffsprotokollierung aktiviert haben. Die Regel ist NON_COMPLIANT, wenn 'accessLogSettings' in der Stage-Konfiguration nicht vorhanden ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.2.2	Auditprotokolle werden implementiert, um die Erkennung von Anomalien und verdächtigen Aktivitäten sowie die forensische Analyse von Ereignissen zu unterstützen. (PCI-DSS-v4.0)	api-gw-xray-enabled	Stellen Sie sicher, dass AWS X-Ray Tracing auf Amazon API Gateway REST APIs aktiviert ist. Die Regel ist COMPLIANT, wenn die X-Ray-Abl aufverfolgung aktiviert ist, andernfalls ist sie NON_COMPLIANT.
10.2.2	Auditprotokolle werden implementiert, um die Erkennung von Anomalien und verdächtigen Aktivitäten sowie die forensische Analyse von Ereignissen zu unterstützen. (PCI-DSS-v4.0)	neptune-cluster-cloudwatch-log-exportfähig	Stellen Sie sicher, dass in einem Amazon Neptune Neptune-Cluster der Protokollexport für CloudWatch Audit-Logs aktiviert ist. Die Regel lautet NON_COMPLIANT, wenn für einen Neptune-Cluster der Protokollexport für CloudWatch Audit-Logs nicht aktiviert ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.2.2	Auditprotokolle werden implementiert, um die Erkennung von Anomalien und verdächtigen Aktivitäten sowie die forensische Analyse von Ereignissen zu unterstützen. (PCI-DSS-v4.0)	ecs-task-definition-log-Konfiguration	Stellen Sie sicher, dass LogConfiguration für aktive ECS-Aufgabendefinitionen festgelegt ist. Diese Regel ist NON_COMPLIANT, wenn für eine aktive ECSTask Definition die LogConfiguration-Ressource nicht definiert ist oder der Wert für LogConfiguration in mindestens einer Containerdefinition Null ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.2.2	Auditprotokolle werden implementiert, um die Erkennung von Anomalien und verdächtigen Aktivitäten sowie die forensische Analyse von Ereignissen zu unterstützen. (PCI-DSS-v4.0)	cloudtrail-enabled	Hinweis: Bei dieser Regel untersche iden sich die Regel-ID (CLOUD_TR AIL_ENABLED) und der Regelname (cloudtrail-enabled). Stellen Sie sicher, dass in Ihrem Konto ein Trail aktiviert ist AWS CloudTrail . AWS Die Regel ist NON_COMPLIANT, wenn ein Trail nicht aktiviert ist. Optional überprüft die Regel einen bestimmten S3-Bucket, ein Amazon Simple Notification Service (Amazon SNS) -Thema und eine CloudWatch Protokollgruppe.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.2.2	Auditprotokolle werden implementiert, um die Erkennung von Anomalien und verdächtigen Aktivitäten sowie die forensische Analyse von Ereignissen zu unterstützen. (PCI-DSS-v4.0)	multi-region-cloudtrail-enabled	Hinweis: Bei dieser Regel untersche iden sich die Regel-ID (MULTI_RE GION_CLOU D_TRAIL_ENABLED) und der Regelname (). multi-region-cloudtrail-enabled Stellen Sie sicher, dass mindesten s eine Region mit mehreren Regionen vorhanden ist. AWS CloudTrail Die Regel ist NON_COMPL IANT, wenn die Trails nicht mit den Eingabeparametern übereinstimmen. Die Regel lautet NON_COMPLIANT, wenn das ExcludeMa nagementEventSourc es Feld nicht leer ist oder wenn sie so konfiguriert AWS CloudTrail ist, dass Verwaltungsereigni sse wie AWS KMS-Ereignisse oder Amazon RDS-Daten -API-Ereignisse

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			ausgeschlossen werden.
10.2.2	Auditprotokolle werden implementiert, um die Erkennung von Anomalien und verdächtigen Aktivitäten sowie die forensische Analyse von Ereignissen zu unterstützen. (PCI-DSS-v4.0)	appsync-logging-enabled	Stellen Sie sicher, dass für eine API die Protokollierung aktiviert ist. AWS AppSync Die Regel lautet NON_COMPLIANT, wenn die Protokollierung nicht aktiviert ist, oder 'fieldLogLevel' ist weder ERROR noch ALL.
10.2.2	Auditprotokolle werden implementiert, um die Erkennung von Anomalien und verdächtigen Aktivitäten sowie die forensische Analyse von Ereignissen zu unterstützen. (PCI-DSS-v4.0)	mq-cloudwatch-audit-logging-aktiviert	Stellen Sie sicher, dass Amazon MQ-Broker die CloudWatch Amazon-Auditprotokollierung aktiviert haben. Die Regel ist NON_COMPLIANT, wenn für einen Broker die Audit-Protokollierung nicht aktiviert ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.2.2	Auditprotokolle werden implementiert, um die Erkennung von Anomalien und verdächtigen Aktivitäten sowie die forensische Analyse von Ereignissen zu unterstützen. (PCI-DSS-v4.0)	mq-cloudwatch-audit-log-aktiviert	Stellen Sie sicher, dass bei einem Amazon MQ-Broker die CloudWatch Auditprotokollierung aktiviert ist. Die Regel lautet NON_COMPLIANT, wenn für den Broker die Audit-Protokollierung nicht aktiviert ist.
10.2.2	Auditprotokolle werden implementiert, um die Erkennung von Anomalien und verdächtigen Aktivitäten sowie die forensische Analyse von Ereignissen zu unterstützen. (PCI-DSS-v4.0)	eks-cluster-logging-enabled	Stellen Sie sicher, dass ein Amazon Elastic Kubernetes Service (Amazon EKS) -Cluster mit aktivierter Protokollierung konfiguriert ist. Die Regel ist NON_COMPLIANT, wenn die Protokollierung für Amazon-EKS-Cluster nicht für alle Protokolltypen aktiviert ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.2.2	Auditprotokolle werden implementiert, um die Erkennung von Anomalien und verdächtigen Aktivitäten sowie die forensische Analyse von Ereignissen zu unterstützen. (PCI-DSS-v4.0)	elastic-beanstalk-logs-to-Wolkenbeobachtung	Stellen Sie sicher, dass AWS Elastic Beanstalk Beanstalk -Umgebungen so konfiguriert sind, dass sie Protokolle an Amazon CloudWatch Logs senden. Die Regel lautet NON_COMPLIANT, wenn der Wert von `` StreamLogs falsch ist.
10.2.2	Auditprotokolle werden implementiert, um die Erkennung von Anomalien und verdächtigen Aktivitäten sowie die forensische Analyse von Ereignissen zu unterstützen. (PCI-DSS-v4.0)	step-functions-state-machine-Protokollierung aktiviert	Stellen Sie sicher, dass auf der AWS Step Functions Functions-Maschine die Protokollierung aktiviert ist Die Regel ist NON_COMPLIANT, wenn für eine Zustandsmaschine die Protokollierung nicht aktiviert ist oder die Protokollierungskonfiguration nicht auf dem angegebenen Mindestniveau liegt.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.2.2	Auditprotokolle werden implementiert, um die Erkennung von Anomalien und verdächtigen Aktivitäten sowie die forensische Analyse von Ereignissen zu unterstützen. (PCI-DSS-v4.0)	netfw-logging-enabled	Stellen Sie sicher, dass die AWS Netzwerk-Firewall-Firewalls die Protokollierung aktiviert haben. Die Regel ist NON_COMPLIANT, wenn kein Protokollierungstyp konfiguriert ist. Sie können angeben, welchen Protokollierungstyp die Regel prüfen soll.
10.3.1	Auditprotokolle sind vor Zerstörung und unbefugten Änderungen geschützt. (PCI-DSS-v4.0)	api-gwv2- access-logs-enabled	Stellen Sie sicher, dass die Amazon API Gateway V2-Stufen die Zugriffsprotokollierung aktiviert haben. Die Regel ist NON_COMPLIANT, wenn 'accessLogSettings' in der Stage-Konfiguration nicht vorhanden ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.3.1	Auditprotokolle sind vor Zerstörun g und unbefugte n Änderungen geschützt. (PCI-DSS-v4.0)	api-gw-xray-enabled	Stellen Sie sicher, dass AWS X-Ray Tracing auf Amazon API Gateway REST APIs aktiviert ist. Die Regel ist COMPLIANT, wenn die X-Ray-Abl aufverfolgung aktiviert ist, andernfalls ist sie NON_COMPLIANT.
10.3.1	Auditprotokolle sind vor Zerstörun g und unbefugte n Änderungen geschützt. (PCI-DSS-v4.0)	neptune-cluster-cl oudwatch-log-expor tfähig	Stellen Sie sicher, dass in einem Amazon Neptune Neptune-Cluster der Protokollexport für CloudWatch Audit-Logs aktiviert ist. Die Regel lautet NON_COMPLIANT, wenn für einen Neptune-Cluster der Protokollexport für CloudWatch Audit-Logs nicht aktiviert ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.3.1	Auditprotokolle sind vor Zerstörun g und unbefugte n Änderungen geschützt. (PCI-DSS-v4.0)	ecs-task-definition-log-Konfiguration	Stellen Sie sicher, dass LogConfig uration für aktive ECS-Aufgabendefini tionen festgelegt ist. Diese Regel ist NON_COMPLIANT, wenn für eine aktive ECSTask Definition die LogConfiguration-Ressource nicht definiert ist oder der Wert für LogConfig uration in mindesten s einer Container definition Null ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.3.1	Auditprotokolle sind vor Zerstörun g und unbefugte n Änderungen geschützt. (PCI-DSS-v4.0)	cloudtrail-enabled	Hinweis: Bei dieser Regel untersche iden sich die Regel-ID (CLOUD_TR AIL_ENABLED) und der Regelname (cloudtrail-enabled). Stellen Sie sicher, dass in Ihrem Konto ein Trail aktiviert ist AWS CloudTrail . AWS Die Regel ist NON_COMPLIANT, wenn ein Trail nicht aktiviert ist. Optional überprüft die Regel einen bestimmten S3-Bucket, ein Amazon Simple Notification Service (Amazon SNS) -Thema und eine CloudWatch Protokollgruppe.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.3.1	Auditprotokolle sind vor Zerstörun g und unbefugte n Änderungen geschützt. (PCI-DSS-v4.0)	multi-region-cloudtrail-enabled	Hinweis: Bei dieser Regel untersche iden sich die Regel-ID (MULTI_RE GION_CLOU D_TRAIL_ENABLED) und der Regelname (). multi-region-cloudtrail-enabled Stellen Sie sicher, dass mindesten s eine Region mit mehreren Regionen vorhanden ist. AWS CloudTrail Die Regel ist NON_COMPL IANT, wenn die Trails nicht mit den Eingabeparametern übereinstimmen. Die Regel lautet NON_COMPLIANT, wenn das ExcludeMa nagementEventSourc es Feld nicht leer ist oder wenn sie so konfiguriert AWS CloudTrail ist, dass Verwaltungsereigni sse wie AWS KMS-Ereignisse oder Amazon RDS-Daten -API-Ereignisse

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			ausgeschlossen werden.
10.3.1	Auditprotokolle sind vor Zerstörung und unbefugten Änderungen geschützt. (PCI-DSS-v4.0)	appsync-logging-enabled	Stellen Sie sicher, dass für eine API die Protokollierung aktiviert ist. AWS AppSync Die Regel lautet NON_COMPLIANT, wenn die Protokollierung nicht aktiviert ist, oder 'fieldLogLevel' ist weder ERROR noch ALL.
10.3.1	Auditprotokolle sind vor Zerstörung und unbefugten Änderungen geschützt. (PCI-DSS-v4.0)	mq-cloudwatch-audit-logging-aktiviert	Stellen Sie sicher, dass Amazon MQ-Broker die CloudWatch Amazon-Auditprotokollierung aktiviert haben. Die Regel ist NON_COMPLIANT, wenn für einen Broker die Audit-Protokollierung nicht aktiviert ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.3.1	Auditprotokolle sind vor Zerstörung und unbefugten Änderungen geschützt. (PCI-DSS-v4.0)	mq-cloudwatch-audit-log-aktiviert	Stellen Sie sicher, dass bei einem Amazon MQ-Broker die CloudWatch Auditprotokollierung aktiviert ist. Die Regel lautet NON_COMPLIANT, wenn für den Broker die Audit-Protokollierung nicht aktiviert ist.
10.3.1	Auditprotokolle sind vor Zerstörung und unbefugten Änderungen geschützt. (PCI-DSS-v4.0)	eks-cluster-logging-enabled	Stellen Sie sicher, dass ein Amazon Elastic Kubernetes Service (Amazon EKS) -Cluster mit aktivierter Protokollierung konfiguriert ist. Die Regel ist NON_COMPLIANT, wenn die Protokollierung für Amazon-EKS-Cluster nicht für alle Protokolltypen aktiviert ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.3.1	Auditprotokolle sind vor Zerstörung und unbefugten Änderungen geschützt. (PCI-DSS-v4.0)	elastic-beanstalk-logs-to-Wolkenbeobachtung	Stellen Sie sicher, dass AWS Elastic Beanstalk Beanstalk-Umgebungen so konfiguriert sind, dass sie Protokolle an Amazon CloudWatch Logs senden. Die Regel lautet NON_COMPLIANT, wenn der Wert von `` StreamLogs falsch ist.
10.3.1	Auditprotokolle sind vor Zerstörung und unbefugten Änderungen geschützt. (PCI-DSS-v4.0)	step-functions-state-machine-Protokollierung aktiviert	Stellen Sie sicher, dass auf der AWS Step Functions Functions-Maschine die Protokollierung aktiviert ist Die Regel ist NON_COMPLIANT, wenn für eine Zustandsmaschine die Protokollierung nicht aktiviert ist oder die Protokollierungskonfiguration nicht auf dem angegebenen Mindestniveau liegt.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.3.1	Auditprotokolle sind vor Zerstörung und unbefugten Änderungen geschützt. (PCI-DSS-v4.0)	netfw-logging-enabled	Stellen Sie sicher, dass die AWS Netzwerk-Firewall-Firewalls die Protokollierung aktiviert haben. Die Regel ist NON_COMPLIANT, wenn kein Protokollierungstyp konfiguriert ist. Sie können angeben, welchen Protokollierungstyp die Regel prüfen soll.
10.3.2	Auditprotokolle sind vor Zerstörung und unbefugten Änderungen geschützt. (PCI-DSS-v4.0)	cloudtrail-security-trail-enabled	Stellen Sie sicher, dass mindestens ein AWS CloudTrail Pfad mit bewährten Sicherheitsmethoden definiert ist. Diese Regel ist COMPLIANT, wenn es mindestens einen Trail gibt, der alle der folgenden Bedingungen erfüllt:

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.3.2	Auditprotokolle sind vor Zerstörung und unbefugten Änderungen geschützt. (PCI-DSS-v4.0)	neptune-cluster-snapshot-public-verboten	Stellen Sie sicher, dass ein manueller Amazon Neptune Neptune-DB-Cluster-Snapshot nicht öffentlich ist. Die Regel ist NON_COMPLIANT, wenn es vorhandene und neue Neptune-Cluster-Snapshots gibt, die öffentlich zugänglich sind.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.3.2	Auditprotokolle sind vor Zerstörung und unbefugten Änderungen geschützt. (PCI-DSS-v4.0)	backup-recovery-point-manual-Löschen-deaktiviert	Stellen Sie sicher, dass an einen Backup-Tresor eine ressourcenbasierte Richtlinie angehängt ist, die das Löschen von Wiederherstellungspunkten verhindert. Die Regel lautet NON_COMPLIANT, wenn der Backup-Tresor keine ressourcenbasierten Richtlinien oder Richtlinien ohne eine geeignete „Deny“ -Anweisung (Anweisung mit den Berechtigungen backup:DeleteRecoveryPoint, backup: und backup:UpdateRecoveryPointLifecycle) hat. PutBackupVaultAccessPolicy

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.3.2	Auditprotokolle sind vor Zerstörung und unbefugten Änderungen geschützt. (PCI-DSS-v4.0)	emr-block-public-access	Stellen Sie sicher, dass für ein Konto bei Amazon EMR die Einstellungen zum Sperren des öffentlichen Zugriffs aktiviert sind. Die Regel ist NON_COMPLIANT, wenn sie falsch BlockPublicSecurityGroupRules ist, oder wenn sie wahr ist, sind andere Ports als Port 22 unter aufgeführt. PermittedPublicSecurityGroupRuleRanges
10.3.2	Auditprotokolle sind vor Zerstörung und unbefugten Änderungen geschützt. (PCI-DSS-v4.0)	access-point-public-accesss3-Blöcke	Stellen Sie sicher, dass Amazon S3 S3-Zugriffspunkten die Einstellungen zum Blockieren des öffentlichen Zugriffs aktiviert sind. Die Regel ist NON_COMPLIANT, wenn die Einstellung zum Blockieren des öffentlichen Zugriffs für S3-Zugangspunkte nicht aktiviert ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.3.2	Auditprotokolle sind vor Zerstörun g und unbefugte n Änderungen geschützt. (PCI-DSS-v4.0)	account-level-public-accesss3-Blöcke	Stellen Sie sicher, dass die erforderl ichen Einstellungen für die Sperrung des öffentlichen Zugriffs auf Kontoebene konfiguriert sind. Die Regel ist nur NON_COMPL IANT, wenn die unten festgeleg ten Felder nicht mit den entsprech enden Feldern im Konfigurationselement übereinstimmen.
10.3.2	Auditprotokolle sind vor Zerstörun g und unbefugte n Änderungen geschützt. (PCI-DSS-v4.0)	s-3 bucket-mfa-delete-enabled	Stellen Sie sicher, dass MFA Delete in der Bucket-Ve rsionierungskonfig uration von Amazon Simple Storage Service (Amazon S3) aktiviert ist. Die Regel ist NON_COMPL IANT, wenn MFA Delete nicht aktiviert ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.3.3	Auditprotokolle sind vor Zerstörung und unbefugten Änderungen geschützt. (PCI-DSS-v4.0)	aurora-resources-protected-by-Backup-Plan	Stellen Sie sicher, dass Amazon Aurora Aurora-DB-Cluster durch einen Backup-Plan geschützt sind. Die Regel ist NON_COMPLIANT, wenn der Datenbank-Cluster von Amazon Relational Database Service (Amazon RDS) nicht durch einen Backup-Plan geschützt ist.
10.3.3	Auditprotokolle sind vor Zerstörung und unbefugten Änderungen geschützt. (PCI-DSS-v4.0)	db-instance-backup-enabled	Stellen Sie sicher, dass für RDS-DB-Instances Backups aktiviert sind. Optional wird von der Regel auch der Aufbewahrungszeitraum für Backups und das Sicherungsfenster überprüft.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.3.3	Auditprotokolle sind vor Zerstörun g und unbefugte n Änderungen geschützt. (PCI-DSS-v4.0)	dynamodb-in-backup-plan	Stellen Sie sicher, dass Amazon DynamoDB-Tabellen in AWS Backup-Plänen vorhanden sind. Die Regel lautet NON_COMPL IANT, wenn Amazon DynamoDB-Tabellen in keinem Backup-Plan enthalten sind. AWS
10.3.3	Auditprotokolle sind vor Zerstörun g und unbefugte n Änderungen geschützt. (PCI-DSS-v4.0)	dynamodb-resources-protected-by-Backup-Plan	Stellen Sie sicher, dass Amazon DynamoDB-Tabellen durch einen Backup-Plan geschützt sind. Die Regel ist NON_COMPLIANT, wenn die DynamoDB-Tabelle nicht durch einen Backup-Plan gedeckt ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.3.3	Auditprotokolle sind vor Zerstörun g und unbefugte n Änderungen geschützt. (PCI-DSS-v4.0)	ebs-in-backup-plan	Stellen Sie sicher, dass Amazon Elastic Block Store (Amazon EBS) -Volumes zu den Backup-Plänen von AWS Backup hinzugefügt werden. Die Regel ist NON_COMPLIANT, wenn Amazon-EB S-Volumes nicht in den Backup-Plänen enthalten sind.
10.3.3	Auditprotokolle sind vor Zerstörun g und unbefugte n Änderungen geschützt. (PCI-DSS-v4.0)	ebs-resources-prot ected-by-Backup-Plan	Stellen Sie sicher, dass Amazon Elastic Block Store (Amazon EBS) -Volumes durch einen Backup-Plan geschützt sind. Die Regel ist NON_COMPLIANT, wenn das Amazon-EB S-Volume nicht durch einen Backup-Plan gedeckt ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.3.3	Auditprotokolle sind vor Zerstörun g und unbefugte n Änderungen geschützt. (PCI-DSS-v4.0)	ec2--Plan resources-protected-by-backup	Stellen Sie sicher, dass Amazon Elastic Compute Cloud (Amazon EC2) - Instances durch einen Backup-Pl an geschützt sind. Die Regel lautet NON_COMPL IANT, wenn die EC2 Amazon-In stance nicht durch einen Backup-Plan abgedeckt ist.
10.3.3	Auditprotokolle sind vor Zerstörun g und unbefugte n Änderungen geschützt. (PCI-DSS-v4.0)	efs-resources-prot ected-by-Backup-Plan	Stellen Sie sicher, dass die Dateisyst eme von Amazon Elastic File System (Amazon EFS) durch einen Backup-Plan geschützt sind. Die Regel ist NON_COMPLIANT, wenn das EFS-Datei system nicht durch einen Backup-Plan gedeckt ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.3.3	Auditprotokolle sind vor Zerstörung und unbefugten Änderungen geschützt. (PCI-DSS-v4.0)	elasticache-redis-cluster-automatic-Backup-Check	Prüfen Sie, ob die Amazon ElastiCache Redis-Cluster die automatische Sicherung aktiviert haben. Die Regel lautet NON_COMPLIANT, wenn der SnapshotRetentionLimit For-Redis-Cluster kleiner als der Parameter ist. SnapshotRetentionPeriod Beispiel: Wenn der Parameter 15 ist, ist die Regel nicht konform, wenn der snapshotRetentionPeriod zwischen 0 und 15 liegt.
10.3.3	Auditprotokolle sind vor Zerstörung und unbefugten Änderungen geschützt. (PCI-DSS-v4.0)	fsx-resources-protected-by-Backup-Plan	Stellen Sie sicher, dass Amazon FSx File Systems durch einen Backup-Plan geschützt sind. Die Regel lautet NON_COMPLIANT, wenn das FSx Amazon-Dateisystem nicht durch einen Backup-Plan abgedeckt ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.3.3	Auditprotokolle sind vor Zerstörung und unbefugten Änderungen geschützt. (PCI-DSS-v4.0)	neptune-cluster-backup-retention-überprüfen	Stellen Sie sicher, dass die Aufbewahrungsfrist für Amazon Neptune DB-Cluster auf eine bestimmte Anzahl von Tagen festgelegt ist. Die Regel ist NON_COMPLIANT, wenn der Aufbewahrungszeitraum kürzer ist als durch den Parameter angegeben.
10.3.3	Auditprotokolle sind vor Zerstörung und unbefugten Änderungen geschützt. (PCI-DSS-v4.0)	rds-in-backup-plan	Stellen Sie sicher, dass Amazon Relational Database Service (Amazon RDS) -Datenbanken in den AWS Backup-Plänen enthalten sind. Die Regel lautet NON_COMPLIANT, wenn Amazon RDS-Datenbanken in keinem AWS Backup-Plan enthalten sind.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.3.3	Auditprotokolle sind vor Zerstörung und unbefugten Änderungen geschützt. (PCI-DSS-v4.0)	redshift-backup-enabled	Stellen Sie sicher, dass automatisierte Amazon Redshift Redshift-Snapshots für Cluster aktiviert sind. Die Regel lautet NON_COMPLIANT, wenn der Wert für automatedSnapshotRetention Period größer MaxRetentionPeriod oder kleiner MinRetentionPeriod oder der Wert 0 ist.
10.3.3	Auditprotokolle sind vor Zerstörung und unbefugten Änderungen geschützt. (PCI-DSS-v4.0)	s-3-Plan resources-protected-by-backup	Stellen Sie sicher, dass Amazon Simple Storage Service (Amazon S3) -Buckets durch einen Backup-Plan geschützt sind. Die Regel ist NON_COMPLIANT, wenn der Amazon-S3 -Bucket nicht durch einen Backup-Plan gedeckt ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.3.3	Auditprotokolle sind vor Zerstörung und unbefugten Änderungen geschützt. (PCI-DSS-v4.0)	cloudtrail-security-trail-enabled	Stellen Sie sicher, dass mindestens ein AWS CloudTrail Pfad mit bewährten Sicherheitsmethoden definiert ist. Diese Regel ist COMPLIANT, wenn es mindestens einen Trail gibt, der alle der folgenden Bedingungen erfüllt:
10.3.3	Auditprotokolle sind vor Zerstörung und unbefugten Änderungen geschützt. (PCI-DSS-v4.0)	db-instance-backup-enabled	Stellen Sie sicher, dass für RDS-DB-Instances Backups aktiviert sind. Optional wird von der Regel auch der Aufbewahrungszeitraum für Backups und das Sicherungsfenster überprüft.
10.3.3	Auditprotokolle sind vor Zerstörung und unbefugten Änderungen geschützt. (PCI-DSS-v4.0)	dynamodb-pitr-enabled	Stellen Sie sicher, dass point-in-time Recovery (PITR) für Amazon DynamoDB-Tabellen aktiviert ist. Die Regel ist NON_COMPLIANT, wenn PITR für DynamoDB-Tabellen nicht aktiviert ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.3.4	Auditprotokolle sind vor Zerstörung und unbefugten Änderungen geschützt. (PCI-DSS-v4.0)	s-3 bucket-default-lock-enabled	Stellen Sie sicher, dass für den S3-Bucket die Sperre standardmäßig aktiviert ist. Die Regel ist NON_COMPLIANT, wenn die Sperre nicht aktiviert ist.
10.3.4	Auditprotokolle sind vor Zerstörung und unbefugten Änderungen geschützt. (PCI-DSS-v4.0)	s-3 bucket-versioning-enabled	Stellen Sie sicher, dass die Versionierung für Ihre S3-Buckets aktiviert ist. Optional wird von der Regel überprüft, ob die MFA-Löschung für Ihre S3-Buckets aktiviert ist.
10.3.4	Auditprotokolle sind vor Zerstörung und unbefugten Änderungen geschützt. (PCI-DSS-v4.0)	cloudtrail-security-trail-enabled	Stellen Sie sicher, dass mindestens ein AWS CloudTrail Pfad mit bewährten Sicherheitsmethoden definiert ist. Diese Regel ist COMPLIANT, wenn es mindestens einen Trail gibt, der alle der folgenden Bedingungen erfüllt:

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.4.1	Auditprotokolle werden überprüft, um Anomalien oder verdächtige Aktivitäten zu identifizieren. (PCI-DSS-v4.0)	api-gw-xray-enabled	Stellen Sie sicher, dass AWS X-Ray Tracing auf Amazon API Gateway REST APIs aktiviert ist. Die Regel ist COMPLIANT, wenn die X-Ray-Abl aufverfolgung aktiviert ist, andernfalls ist sie NON_COMPLIANT.
10.4.1	Auditprotokolle werden überprüft, um Anomalien oder verdächtige Aktivitäten zu identifizieren. (PCI-DSS-v4.0)	ec2- instance-detailed-monitoring-enabled	Stellen Sie sicher, dass die detaillierte Überwachung für Instanzen aktiviert ist. EC2 Die Regel ist NON_COMPLIANT, wenn keine detaillierte Überwachung aktiviert ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.4.1	Auditprotokolle werden überprüft, um Anomalien oder verdächtige Aktivitäten zu identifizieren. (PCI-DSS-v4.0)	cloudwatch-alarm-action-check	Stellen Sie sicher, dass bei CloudWatch Alarmen eine Aktion für den Status ALARM, INSUFFICIENT_DATA oder OK konfiguriert ist. Stellen Sie optional sicher, dass alle Aktionen mit einem benannten ARN übereinstimmen. Die Regel ist NON_COMPLIANT, wenn für den Alarm oder den optionalen Parameter keine Aktion festgelegt ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.4.1	Auditprotokolle werden überprüft, um Anomalien oder verdächtige Aktivitäten zu identifizieren. (PCI-DSS-v4.0)	cloudwatch-alarm-action-check	Stellen Sie sicher, dass bei CloudWatch Alarmen eine Aktion für den Status ALARM, INSUFFICIENT_DATA oder OK konfiguriert ist. Stellen Sie optional sicher, dass alle Aktionen mit einem benannten ARN übereinstimmen. Die Regel ist NON_COMPLIANT, wenn für den Alarm oder den optionalen Parameter keine Aktion festgelegt ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.4.1	Auditprotokolle werden überprüft, um Anomalien oder verdächtige Aktivitäten zu identifizieren. (PCI-DSS-v4.0)	cloudwatch-alarm-action-check	Stellen Sie sicher, dass bei CloudWatch Alarmen eine Aktion für den Status ALARM, INSUFFICIENT_DATA oder OK konfiguriert ist. Stellen Sie optional sicher, dass alle Aktionen mit einem benannten ARN übereinstimmen. Die Regel ist NON_COMPLIANT, wenn für den Alarm oder den optionalen Parameter keine Aktion festgelegt ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.4.1	Auditprotokolle werden überprüft, um Anomalien oder verdächtige Aktivitäten zu identifizieren. (PCI-DSS-v4.0)	cloudwatch-alarm-resource-check	Stellen Sie sicher, dass ein Ressourcentyp einen CloudWatch Alarm für die angegebene Metrik hat. Als Ressourcentyp können Sie EBS-Volumes, EC2 Instances, Amazon RDS-Cluster oder S3-Buckets angeben. Die Regel ist KONFORM, wenn die benannte Metrik eine Ressourcen-ID und CloudWatch einen Alarm hat.
10.4.1	Auditprotokolle werden überprüft, um Anomalien oder verdächtige Aktivitäten zu identifizieren. (PCI-DSS-v4.0)	WAF 2- rulegroup-logging-enabled	Stellen Sie sicher, dass die Erfassung von CloudWatch Amazon-Sicherheitsmetriken für AWS WAFv2 Regelgruppen aktiviert ist. Die Regel ist NON_COMPLIANT, wenn '. VisibilityConfig CloudWatchMetricsEnabledDas Feld 'ist auf falsch gesetzt.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.4.1	Auditprotokolle werden überprüft, um Anomalien oder verdächtige Aktivitäten zu identifizieren. (PCI-DSS-v4.0)	sns-topic-message-delivery-Benachrichtigung aktiviert	Stellen Sie sicher, dass die Amazon Simple Notification Service (SNS) - Protokollierung für den Zustellungsstatus von Benachrichtigungen aktiviert ist, die an ein Thema für die Endgeräte gesendet werden. Die Regel ist NON_COMPLIANT, wenn die Benachrichtigung über den Status der Zustellung von Nachrichten nicht aktiviert ist.
10.4.1.1	Auditprotokolle werden überprüft, um Anomalien oder verdächtige Aktivitäten zu identifizieren. (PCI-DSS-v4.0)	api-gw-xray-enabled	Stellen Sie sicher, dass AWS X-Ray Tracing auf Amazon API Gateway REST APIs aktiviert ist. Die Regel ist COMPLIANT, wenn die X-Ray-Ablaufverfolgung aktiviert ist, andernfalls ist sie NON_COMPLIANT.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.4.1.1	Auditprotokolle werden überprüft, um Anomalien oder verdächtige Aktivitäten zu identifizieren. (PCI-DSS-v4.0)	ec2- instance-detailed-monitoring-enabled	Stellen Sie sicher, dass die detaillierte Überwachung für Instanzen aktiviert ist. EC2 Die Regel ist NON_COMPLIANT, wenn keine detaillierte Überwachung aktiviert ist.
10.4.1.1	Auditprotokolle werden überprüft, um Anomalien oder verdächtige Aktivitäten zu identifizieren. (PCI-DSS-v4.0)	cloudwatch-alarm-action-check	Stellen Sie sicher, dass bei CloudWatch Alarmen eine Aktion für den Status ALARM, INSUFFICIENT_DATA oder OK konfiguriert ist. Stellen Sie optional sicher, dass alle Aktionen mit einem benannten ARN übereinstimmen. Die Regel ist NON_COMPLIANT, wenn für den Alarm oder den optionalen Parameter keine Aktion festgelegt ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.4.1.1	Auditprotokolle werden überprüft, um Anomalien oder verdächtige Aktivitäten zu identifizieren. (PCI-DSS-v4.0)	cloudwatch-alarm-action-check	Stellen Sie sicher, dass bei CloudWatch Alarmen eine Aktion für den Status ALARM, INSUFFICIENT_DATA oder OK konfiguriert ist. Stellen Sie optional sicher, dass alle Aktionen mit einem benannten ARN übereinstimmen. Die Regel ist NON_COMPLIANT, wenn für den Alarm oder den optionalen Parameter keine Aktion festgelegt ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.4.1.1	Auditprotokolle werden überprüft, um Anomalien oder verdächtige Aktivitäten zu identifizieren. (PCI-DSS-v4.0)	cloudwatch-alarm-action-check	Stellen Sie sicher, dass bei CloudWatch Alarmen eine Aktion für den Status ALARM, INSUFFICIENT_DATA oder OK konfiguriert ist. Stellen Sie optional sicher, dass alle Aktionen mit einem benannten ARN übereinstimmen. Die Regel ist NON_COMPLIANT, wenn für den Alarm oder den optionalen Parameter keine Aktion festgelegt ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.4.1.1	Auditprotokolle werden überprüft, um Anomalien oder verdächtige Aktivitäten zu identifizieren. (PCI-DSS-v4.0)	cloudwatch-alarm-resource-check	Stellen Sie sicher, dass ein Ressourcentyp einen CloudWatch Alarm für die angegebene Metrik hat. Als Ressourcentyp können Sie EBS-Volumes, EC2 Instances, Amazon RDS-Cluster oder S3-Buckets angeben. Die Regel ist KONFORM, wenn die benannte Metrik eine Ressourcen-ID und CloudWatch einen Alarm hat.
10.4.1.1	Auditprotokolle werden überprüft, um Anomalien oder verdächtige Aktivitäten zu identifizieren. (PCI-DSS-v4.0)	WAF 2- rulegroup-logging-enabled	Stellen Sie sicher, dass die Erfassung von CloudWatch Amazon-Sicherheitsmetriken für AWS WAFv2 Regelgruppen aktiviert ist. Die Regel ist NON_COMPLIANT, wenn '. VisibilityConfig CloudWatchMetricsEnabledDas Feld 'ist auf falsch gesetzt.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.4.1.1	Auditprotokolle werden überprüft, um Anomalien oder verdächtige Aktivitäten zu identifizieren. (PCI-DSS-v4.0)	sns-topic-message-delivery-Benachrichtigung aktiviert	Stellen Sie sicher, dass die Amazon Simple Notification Service (SNS) - Protokollierung für den Zustellungsstatus von Benachrichtigungen aktiviert ist, die an ein Thema für die Endgeräte gesendet werden. Die Regel ist NON_COMPLIANT, wenn die Benachrichtigung über den Status der Zustellung von Nachrichten nicht aktiviert ist.
10.4.2	Auditprotokolle werden überprüft, um Anomalien oder verdächtige Aktivitäten zu identifizieren. (PCI-DSS-v4.0)	api-gw-xray-enabled	Stellen Sie sicher, dass AWS X-Ray Tracing auf Amazon API Gateway REST APIs aktiviert ist. Die Regel ist COMPLIANT, wenn die X-Ray-Ablaufverfolgung aktiviert ist, andernfalls ist sie NON_COMPLIANT.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.4.2	Auditprotokolle werden überprüft, um Anomalien oder verdächtige Aktivitäten zu identifizieren. (PCI-DSS-v4.0)	ec2- instance-detailed-monitoring-enabled	Stellen Sie sicher, dass die detaillierte Überwachung für Instanzen aktiviert ist. EC2 Die Regel ist NON_COMPLIANT, wenn keine detaillierte Überwachung aktiviert ist.
10.4.2	Auditprotokolle werden überprüft, um Anomalien oder verdächtige Aktivitäten zu identifizieren. (PCI-DSS-v4.0)	cloudwatch-alarm-action-check	Stellen Sie sicher, dass bei CloudWatch Alarmen eine Aktion für den Status ALARM, INSUFFICIENT_DATA oder OK konfiguriert ist. Stellen Sie optional sicher, dass alle Aktionen mit einem benannten ARN übereinstimmen. Die Regel ist NON_COMPLIANT, wenn für den Alarm oder den optionalen Parameter keine Aktion festgelegt ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.4.2	Auditprotokolle werden überprüft, um Anomalien oder verdächtige Aktivitäten zu identifizieren. (PCI-DSS-v4.0)	cloudwatch-alarm-action-check	Stellen Sie sicher, dass bei CloudWatch Alarmen eine Aktion für den Status ALARM, INSUFFICIENT_DATA oder OK konfiguriert ist. Stellen Sie optional sicher, dass alle Aktionen mit einem benannten ARN übereinstimmen. Die Regel ist NON_COMPLIANT, wenn für den Alarm oder den optionalen Parameter keine Aktion festgelegt ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.4.2	Auditprotokolle werden überprüft, um Anomalien oder verdächtige Aktivitäten zu identifizieren. (PCI-DSS-v4.0)	cloudwatch-alarm-action-check	Stellen Sie sicher, dass bei CloudWatch Alarmen eine Aktion für den Status ALARM, INSUFFICIENT_DATA oder OK konfiguriert ist. Stellen Sie optional sicher, dass alle Aktionen mit einem benannten ARN übereinstimmen. Die Regel ist NON_COMPLIANT, wenn für den Alarm oder den optionalen Parameter keine Aktion festgelegt ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.4.2	Auditprotokolle werden überprüft, um Anomalien oder verdächtige Aktivitäten zu identifizieren. (PCI-DSS-v4.0)	cloudwatch-alarm-resource-check	Stellen Sie sicher, dass ein Ressourcentyp einen CloudWatch Alarm für die angegebene Metrik hat. Als Ressourcentyp können Sie EBS-Volumes, EC2 Instances, Amazon RDS-Cluster oder S3-Buckets angeben. Die Regel ist KONFORM, wenn die benannte Metrik eine Ressourcen-ID und CloudWatch einen Alarm hat.
10.4.2	Auditprotokolle werden überprüft, um Anomalien oder verdächtige Aktivitäten zu identifizieren. (PCI-DSS-v4.0)	WAF 2- rulegroup-logging-enabled	Stellen Sie sicher, dass die Erfassung von CloudWatch Amazon-Sicherheitsmetriken für AWS WAFv2 Regelgruppen aktiviert ist. Die Regel ist NON_COMPLIANT, wenn '. VisibilityConfig CloudWatchMetricsEnabledDas Feld 'ist auf falsch gesetzt.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.4.2	Auditprotokolle werden überprüft, um Anomalien oder verdächtige Aktivitäten zu identifizieren. (PCI-DSS-v4.0)	sns-topic-message-delivery-Benachrichtigung aktiviert	Stellen Sie sicher, dass die Amazon Simple Notification Service (SNS) - Protokollierung für den Zustellungsstatus von Benachrichtigungen aktiviert ist, die an ein Thema für die Endgeräte gesendet werden. Die Regel ist NON_COMPLIANT, wenn die Benachrichtigung über den Status der Zustellung von Nachrichten nicht aktiviert ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.4.3	Auditprotokolle werden überprüft, um Anomalien oder verdächtige Aktivitäten zu identifizieren. (PCI-DSS-v4.0)	cloudwatch-alarm-action-check	Stellen Sie sicher, dass bei CloudWatch Alarmen eine Aktion für den Status ALARM, INSUFFICIENT_DATA oder OK konfiguriert ist. Stellen Sie optional sicher, dass alle Aktionen mit einem benannten ARN übereinstimmen. Die Regel ist NON_COMPLIANT, wenn für den Alarm oder den optionalen Parameter keine Aktion festgelegt ist.
10.5.1	Der Verlauf des Auditprotokolls wird beibehalten und steht zur Analyse zur Verfügung. (PCI-DSS-v4.0)	cloudtrail-security-trail-enabled	Stellen Sie sicher, dass mindestens ein AWS CloudTrail Pfad mit bewährten Sicherheitsmethoden definiert ist. Diese Regel ist COMPLIANT, wenn es mindestens einen Trail gibt, der alle der folgenden Bedingungen erfüllt:

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.5.1	Der Verlauf des Auditprotokolls wird beibehalten und steht zur Analyse zur Verfügung. (PCI-DSS-v4.0)	ec2- volume-inuse-check	Stellen Sie sicher, dass EBS-Volumes an Instances angehängt sind. EC2 Stellen Sie optional sicher, dass EBS-Volumes zum Löschen markiert sind, wenn eine Instance beendet wird.
10.5.1	Der Verlauf des Auditprotokolls wird beibehalten und steht zur Analyse zur Verfügung. (PCI-DSS-v4.0)	ecr-private-lifecycle-policy-konfiguriert	Stellen Sie sicher, dass für ein privates Amazon Elastic Container Registry (ECR) -Repository mindestens eine Lebenszyklusrichtlinie konfiguriert ist. Die Regel ist NON_COMPLIANT, wenn keine Lebenszyklus-Richtlinie für das private ECR-Repository konfiguriert ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.5.1	Der Verlauf des Auditprotokolls wird beibehalten und steht zur Analyse zur Verfügung. (PCI-DSS-v4.0)	dynamodb-pitr-enabled	Stellen Sie sicher, dass point-in-time Recovery (PITR) für Amazon DynamoDB-Tabellen aktiviert ist. Die Regel ist NON_COMPLIANT, wenn PITR für DynamoDB-Tabellen nicht aktiviert ist.
10.5.1	Der Verlauf des Auditprotokolls wird beibehalten und steht zur Analyse zur Verfügung. (PCI-DSS-v4.0)	cw-loggroup-retention-period-überprüfen	Stellen Sie sicher, dass ein CloudWatch LogGroup Amazon-Aufbewahrungszeitraum auf mehr als 365 Tage oder einen bestimmten Aufbewahrungszeitraum festgelegt ist. Die Regel lautet NON_COMPLIANT, wenn die Aufbewahrungsfrist weniger als MinRetentionTime, falls angegeben, oder andernfalls 365 Tage beträgt.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.6.3	Mechanismen zur Zeitsynchronisierung unterstützen konsistente Zeiteinstellungen auf allen Systemen. (PCI-DSS-v4.0)	api-gwv2- access-logs-enabled	Stellen Sie sicher, dass die Amazon API Gateway V2-Stufen die Zugriffsprotokollierung aktiviert haben. Die Regel ist NON_COMPLIANT, wenn 'accessLogSettings' in der Stage-Konfiguration nicht vorhanden ist.
10.6.3	Mechanismen zur Zeitsynchronisierung unterstützen konsistente Zeiteinstellungen auf allen Systemen. (PCI-DSS-v4.0)	api-gw-xray-enabled	Stellen Sie sicher, dass AWS X-Ray Tracing auf Amazon API Gateway REST APIs aktiviert ist. Die Regel ist COMPLIANT, wenn die X-Ray-Ablaufverfolgung aktiviert ist, andernfalls ist sie NON_COMPLIANT.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.6.3	Mechanismen zur Zeitsynchronisierung unterstützen konsistente Zeiteinstellungen auf allen Systemen. (PCI-DSS-v4.0)	s-3 bucket-blacklisted-actions-prohibited	Stellen Sie sicher, dass eine Bucket-Richtlinie von Amazon Simple Storage Service (Amazon S3) keine Aktionen auf Bucket- und Objektebene auf Blocklisten für Ressourcen im Bucket für Prinzipale anderer Konten zulässt. AWS Die Regel überprüft beispielsweise, ob die Amazon S3 S3-Bucket-Richtlinie einem anderen AWS Konto nicht erlaubt, s3: GetBucket *-Aktionen und s3: DeleteObject für ein Objekt im Bucket auszuführen. Die Regel ist NON_COMPLIANT, wenn gesperrte Aktionen gemäß der Bucket-Richtlinie von Amazon S3 zulässig sind.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.6.3	Mechanismen zur Zeitsynchronisierung unterstützen konsistente Zeiteinstellungen auf allen Systemen. (PCI-DSS-v4.0)	bucket-policy-not-mores3-permissiv	Stellen Sie sicher, dass Ihre Amazon Simple Storage Service (S3) -Bucket-Richtlinien keine anderen Kontoberechtigungen zulassen als die von Ihnen Amazon S3 S3-Bucket-Kontrollrichtlinie.
10.6.3	Mechanismen zur Zeitsynchronisierung unterstützen konsistente Zeiteinstellungen auf allen Systemen. (PCI-DSS-v4.0)	neptune-cluster-cloudwatch-log-exportfähig	Stellen Sie sicher, dass in einem Amazon Neptune Neptune-Cluster der Protokollexport für CloudWatch Audit-Logs aktiviert ist. Die Regel lautet NON_COMPLIANT, wenn für einen Neptune-Cluster der Protokollexport für CloudWatch Audit-Logs nicht aktiviert ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.6.3	Mechanismen zur Zeitsynchronisierung unterstützen konsistente Zeiteinstellungen auf allen Systemen. (PCI-DSS-v4.0)	ec2- instance-detailed-monitoring-enabled	Stellen Sie sicher, dass die detaillierte Überwachung für Instanzen aktiviert ist. EC2 Die Regel ist NON_COMPLIANT, wenn keine detaillierte Überwachung aktiviert ist.
10.6.3	Mechanismen zur Zeitsynchronisierung unterstützen konsistente Zeiteinstellungen auf allen Systemen. (PCI-DSS-v4.0)	ecs-task-definition-log-Konfiguration	Stellen Sie sicher, dass LogConfiguration für aktive ECS-Aufgabendefinitionen festgelegt ist. Diese Regel ist NON_COMPLIANT, wenn für eine aktive ECSTask Definition die LogConfiguration-Ressource nicht definiert ist oder der Wert für LogConfiguration in mindestens einer Containerdefinition Null ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.6.3	Mechanismen zur Zeitsynchronisierung unterstützen konsistente Zeiteinstellungen auf allen Systemen. (PCI-DSS-v4.0)	cloudwatch-alarm-action-check	Stellen Sie sicher, dass bei CloudWatch Alarmen eine Aktion für den Status ALARM, INSUFFICIENT_DATA oder OK konfiguriert ist. Stellen Sie optional sicher, dass alle Aktionen mit einem benannten ARN übereinstimmen. Die Regel ist NON_COMPLIANT, wenn für den Alarm oder den optionalen Parameter keine Aktion festgelegt ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.6.3	Mechanismen zur Zeitsynchronisierung unterstützen konsistente Zeiteinstellungen auf allen Systemen. (PCI-DSS-v4.0)	cloudwatch-alarm-action-check	Stellen Sie sicher, dass bei CloudWatch Alarmen eine Aktion für den Status ALARM, INSUFFICIENT_DATA oder OK konfiguriert ist. Stellen Sie optional sicher, dass alle Aktionen mit einem benannten ARN übereinstimmen. Die Regel ist NON_COMPLIANT, wenn für den Alarm oder den optionalen Parameter keine Aktion festgelegt ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.6.3	Mechanismen zur Zeitsynchronisierung unterstützen konsistente Zeiteinstellungen auf allen Systemen. (PCI-DSS-v4.0)	cloudwatch-alarm-action-check	Stellen Sie sicher, dass bei CloudWatch Alarmen eine Aktion für den Status ALARM, INSUFFICIENT_DATA oder OK konfiguriert ist. Stellen Sie optional sicher, dass alle Aktionen mit einem benannten ARN übereinstimmen. Die Regel ist NON_COMPLIANT, wenn für den Alarm oder den optionalen Parameter keine Aktion festgelegt ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.6.3	Mechanismen zur Zeitsynchronisierung unterstützen konsistente Zeiteinstellungen auf allen Systemen. (PCI-DSS-v4.0)	cloudwatch-alarm-resource-check	Stellen Sie sicher, dass ein Ressourcentyp einen CloudWatch Alarm für die angegebene Metrik hat. Als Ressourcentyp können Sie EBS-Volumes, EC2 Instances, Amazon RDS-Cluster oder S3-Buckets angeben. Die Regel ist KONFORM, wenn die benannte Metrik eine Ressourcen-ID und CloudWatch einen Alarm hat.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.6.3	Mechanismen zur Zeitsynchronisierung unterstützen konsistente Zeiteinstellungen auf allen Systemen. (PCI-DSS-v4.0)	cloudtrail-enabled	Hinweis: Bei dieser Regel unterscheiden sich die Regel-ID (CLOUD_TRAIL_ENABLED) und der Regelname (cloudtrail-enabled). Stellen Sie sicher, dass in Ihrem Konto ein Trail aktiviert ist AWS CloudTrail . AWS Die Regel ist NON_COMPLIANT, wenn ein Trail nicht aktiviert ist. Optional überprüft die Regel einen bestimmten S3-Bucket, ein Amazon Simple Notification Service (Amazon SNS) -Thema und eine CloudWatch Protokollgruppe.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.6.3	Mechanismen zur Zeitsynchronisierung unterstützen konsistente Zeiteinstellungen auf allen Systemen. (PCI-DSS-v4.0)	multi-region-cloudtrail-enabled	Hinweis: Bei dieser Regel unterscheiden sich die Regel-ID (MULTI_REGION_CLOUD_TRAIL_ENABLED) und der Regelname (). multi-region-cloudtrail-enabled Stellen Sie sicher, dass mindestens eine Region mit mehreren Regionen vorhanden ist. AWS CloudTrail Die Regel ist NON_COMPLIANT, wenn die Trails nicht mit den Eingabeparametern übereinstimmen. Die Regel lautet NON_COMPLIANT, wenn das ExcludeManagementEventSources Feld nicht leer ist oder wenn sie so konfiguriert AWS CloudTrail ist, dass Verwaltungsereignisse wie AWS KMS-Ereignisse oder Amazon RDS-Daten-API-Ereignisse

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			ausgeschlossen werden.
10.6.3	Mechanismen zur Zeitsynchronisierung unterstützen konsistente Zeiteinstellungen auf allen Systemen. (PCI-DSS-v4.0)	appsync-logging-enabled	Stellen Sie sicher, dass für eine API die Protokollierung aktiviert ist. AWS AppSync Die Regel lautet NON_COMPLIANT, wenn die Protokollierung nicht aktiviert ist, oder 'fieldLogLevel' ist weder ERROR noch ALL.
10.6.3	Mechanismen zur Zeitsynchronisierung unterstützen konsistente Zeiteinstellungen auf allen Systemen. (PCI-DSS-v4.0)	mq-cloudwatch-audit-logging-aktiviert	Stellen Sie sicher, dass Amazon MQ-Broker die CloudWatch Amazon-Auditprotokollierung aktiviert haben. Die Regel ist NON_COMPLIANT, wenn für einen Broker die Audit-Protokollierung nicht aktiviert ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.6.3	Mechanismen zur Zeitsynchronisierung unterstützen konsistente Zeiteinstellungen auf allen Systemen. (PCI-DSS-v4.0)	mq-cloudwatch-audit-log-aktiviert	Stellen Sie sicher, dass bei einem Amazon MQ-Broker die CloudWatch Auditprotokollierung aktiviert ist. Die Regel lautet NON_COMPLIANT, wenn für den Broker die Audit-Protokollierung nicht aktiviert ist.
10.6.3	Mechanismen zur Zeitsynchronisierung unterstützen konsistente Zeiteinstellungen auf allen Systemen. (PCI-DSS-v4.0)	eks-cluster-logging-enabled	Stellen Sie sicher, dass ein Amazon Elastic Kubernetes Service (Amazon EKS) -Cluster mit aktivierter Protokollierung konfiguriert ist. Die Regel ist NON_COMPLIANT, wenn die Protokollierung für Amazon-EKS-Cluster nicht für alle Protokolltypen aktiviert ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.6.3	Mechanismen zur Zeitsynchronisierung unterstützen konsistente Zeiteinstellungen auf allen Systemen. (PCI-DSS-v4.0)	elastic-beanstalk-logs-to-Wolkenbeobachtung	Stellen Sie sicher, dass AWS Elastic Beanstalk Beanstalk -Umgebungen so konfiguriert sind, dass sie Protokolle an Amazon CloudWatch Logs senden. Die Regel lautet NON_COMPLIANT, wenn der Wert von `` StreamLogs falsch ist.
10.6.3	Mechanismen zur Zeitsynchronisierung unterstützen konsistente Zeiteinstellungen auf allen Systemen. (PCI-DSS-v4.0)	WAF 2- rulegroup-logging-enabled	Stellen Sie sicher, dass die Erfassung von CloudWatch Amazon-Sicherheitsmetriken für AWS WAFv2 Regelgruppen aktiviert ist. Die Regel ist NON_COMPLIANT, wenn '. VisibilityConfig CloudWatchMetricsEnabledDas Feld 'ist auf falsch gesetzt.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.6.3	Mechanismen zur Zeitsynchronisierung unterstützen konsistente Zeiteinstellungen auf allen Systemen. (PCI-DSS-v4.0)	sns-topic-message-delivery-Benachrichtigung aktiviert	Stellen Sie sicher, dass die Amazon Simple Notification Service (SNS) - Protokollierung für den Zustellungsstatus von Benachrichtigungen aktiviert ist, die an ein Thema für die Endgeräte gesendet werden. Die Regel ist NON_COMPLIANT, wenn die Benachrichtigung über den Status der Zustellung von Nachrichten nicht aktiviert ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.6.3	Mechanismen zur Zeitsynchronisierung unterstützen konsistente Zeiteinstellungen auf allen Systemen. (PCI-DSS-v4.0)	step-functions-state-machine-Protokollierung aktiviert	Stellen Sie sicher, dass auf der AWS Step Functions Functions-Maschine die Protokollierung aktiviert ist Die Regel ist NON_COMPLIANT, wenn für eine Zustandsmaschine die Protokollierung nicht aktiviert ist oder die Protokollierungskonfiguration nicht auf dem angegebenen Mindestniveau liegt.
10.6.3	Mechanismen zur Zeitsynchronisierung unterstützen konsistente Zeiteinstellungen auf allen Systemen. (PCI-DSS-v4.0)	netfw-logging-enabled	Stellen Sie sicher, dass die AWS Netzwerk-Firewall-Firewalls die Protokollierung aktiviert haben. Die Regel ist NON_COMPLIANT, wenn kein Protokollierungstyp konfiguriert ist. Sie können angeben, welchen Protokollierungstyp die Regel prüfen soll.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.7.1	Ausfälle kritischer Sicherheitskontrol lsysteme werden erkannt, gemeldet und umgehend behoben. (PCI-DSS-v4.0)	api-gw-xray-enabled	Stellen Sie sicher, dass AWS X-Ray Tracing auf Amazon API Gateway REST APIs aktiviert ist. Die Regel ist COMPLIANT, wenn die X-Ray-Abl aufverfolgung aktiviert ist, andernfalls ist sie NON_COMPLIANT.
10.7.1	Ausfälle kritischer Sicherheitskontrol lsysteme werden erkannt, gemeldet und umgehend behoben. (PCI-DSS-v4.0)	ec2- instance-detailed-monitoring-enabled	Stellen Sie sicher, dass die detaillierte Überwachung für Instanzen aktiviert ist. EC2 Die Regel ist NON_COMPLIANT, wenn keine detaillierte Überwachung aktiviert ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.7.1	Ausfälle kritischer Sicherheitskontrollsysteme werden erkannt, gemeldet und umgehend behoben. (PCI-DSS-v4.0)	cloudwatch-alarm-action-check	Stellen Sie sicher, dass bei CloudWatch Alarmen eine Aktion für den Status ALARM, INSUFFICIENT_DATA oder OK konfiguriert ist. Stellen Sie optional sicher, dass alle Aktionen mit einem benannten ARN übereinstimmen. Die Regel ist NON_COMPLIANT, wenn für den Alarm oder den optionalen Parameter keine Aktion festgelegt ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.7.1	Ausfälle kritischer Sicherheitskontrollsysteme werden erkannt, gemeldet und umgehend behoben. (PCI-DSS-v4.0)	cloudwatch-alarm-action-check	Stellen Sie sicher, dass bei CloudWatch Alarmen eine Aktion für den Status ALARM, INSUFFICIENT_DATA oder OK konfiguriert ist. Stellen Sie optional sicher, dass alle Aktionen mit einem benannten ARN übereinstimmen. Die Regel ist NON_COMPLIANT, wenn für den Alarm oder den optionalen Parameter keine Aktion festgelegt ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.7.1	Ausfälle kritischer Sicherheitskontrollsysteme werden erkannt, gemeldet und umgehend behoben. (PCI-DSS-v4.0)	cloudwatch-alarm-action-check	Stellen Sie sicher, dass bei CloudWatch Alarmen eine Aktion für den Status ALARM, INSUFFICIENT_DATA oder OK konfiguriert ist. Stellen Sie optional sicher, dass alle Aktionen mit einem benannten ARN übereinstimmen. Die Regel ist NON_COMPLIANT, wenn für den Alarm oder den optionalen Parameter keine Aktion festgelegt ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.7.1	Ausfälle kritischer Sicherheitskontrollsysteme werden erkannt, gemeldet und umgehend behoben. (PCI-DSS-v4.0)	cloudwatch-alarm-resource-check	Stellen Sie sicher, dass ein Ressourcentyp einen CloudWatch Alarm für die angegebene Metrik hat. Als Ressourcentyp können Sie EBS-Volumes, EC2 Instances, Amazon RDS-Cluster oder S3-Buckets angeben. Die Regel ist KONFORM, wenn die benannte Metrik eine Ressourcen-ID und CloudWatch einen Alarm hat.
10.7.1	Ausfälle kritischer Sicherheitskontrollsysteme werden erkannt, gemeldet und umgehend behoben. (PCI-DSS-v4.0)	WAF 2- rulegroup-logging-enabled	Stellen Sie sicher, dass die Erfassung von CloudWatch Amazon-Sicherheitsmetriken für AWS WAFv2 Regelgruppen aktiviert ist. Die Regel ist NON_COMPLIANT, wenn '. VisibilityConfig CloudWatchMetricsEnabledDas Feld 'ist auf falsch gesetzt.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.7.1	Ausfälle kritischer Sicherheitskontrollsysteme werden erkannt, gemeldet und umgehend behoben. (PCI-DSS-v4.0)	sns-topic-message-delivery-Benachrichtigung aktiviert	Stellen Sie sicher, dass die Amazon Simple Notification Service (SNS) - Protokollierung für den Zustellungsstatus von Benachrichtigungen aktiviert ist, die an ein Thema für die Endgeräte gesendet werden. Die Regel ist NON_COMPLIANT, wenn die Benachrichtigung über den Status der Zustellung von Nachrichten nicht aktiviert ist.
10.7.2	Ausfälle kritischer Sicherheitskontrollsysteme werden erkannt, gemeldet und umgehend behoben. (PCI-DSS-v4.0)	api-gw-xray-enabled	Stellen Sie sicher, dass AWS X-Ray Tracing auf Amazon API Gateway REST APIs aktiviert ist. Die Regel ist COMPLIANT, wenn die X-Ray-Ablaufverfolgung aktiviert ist, andernfalls ist sie NON_COMPLIANT.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.7.2	Ausfälle kritischer Sicherheitskontrollsysteme werden erkannt, gemeldet und umgehend behoben. (PCI-DSS-v4.0)	ec2- instance-detailed-monitoring-enabled	Stellen Sie sicher, dass die detaillierte Überwachung für Instanzen aktiviert ist. EC2 Die Regel ist NON_COMPLIANT, wenn keine detaillierte Überwachung aktiviert ist.
10.7.2	Ausfälle kritischer Sicherheitskontrollsysteme werden erkannt, gemeldet und umgehend behoben. (PCI-DSS-v4.0)	cloudwatch-alarm-action-check	Stellen Sie sicher, dass bei CloudWatch Alarmen eine Aktion für den Status ALARM, INSUFFICIENT_DATA oder OK konfiguriert ist. Stellen Sie optional sicher, dass alle Aktionen mit einem benannten ARN übereinstimmen. Die Regel ist NON_COMPLIANT, wenn für den Alarm oder den optionalen Parameter keine Aktion festgelegt ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.7.2	Ausfälle kritischer Sicherheitskontrollsysteme werden erkannt, gemeldet und umgehend behoben. (PCI-DSS-v4.0)	cloudwatch-alarm-action-check	Stellen Sie sicher, dass bei CloudWatch Alarmen eine Aktion für den Status ALARM, INSUFFICIENT_DATA oder OK konfiguriert ist. Stellen Sie optional sicher, dass alle Aktionen mit einem benannten ARN übereinstimmen. Die Regel ist NON_COMPLIANT, wenn für den Alarm oder den optionalen Parameter keine Aktion festgelegt ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.7.2	Ausfälle kritischer Sicherheitskontrollsysteme werden erkannt, gemeldet und umgehend behoben. (PCI-DSS-v4.0)	cloudwatch-alarm-action-check	Stellen Sie sicher, dass bei CloudWatch Alarmen eine Aktion für den Status ALARM, INSUFFICIENT_DATA oder OK konfiguriert ist. Stellen Sie optional sicher, dass alle Aktionen mit einem benannten ARN übereinstimmen. Die Regel ist NON_COMPLIANT, wenn für den Alarm oder den optionalen Parameter keine Aktion festgelegt ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.7.2	Ausfälle kritischer Sicherheitskontrollsysteme werden erkannt, gemeldet und umgehend behoben. (PCI-DSS-v4.0)	cloudwatch-alarm-resource-check	Stellen Sie sicher, dass ein Ressourcentyp einen CloudWatch Alarm für die angegebene Metrik hat. Als Ressourcentyp können Sie EBS-Volumes, EC2 Instances, Amazon RDS-Cluster oder S3-Buckets angeben. Die Regel ist KONFORM, wenn die benannte Metrik eine Ressourcen-ID und CloudWatch einen Alarm hat.
10.7.2	Ausfälle kritischer Sicherheitskontrollsysteme werden erkannt, gemeldet und umgehend behoben. (PCI-DSS-v4.0)	WAF 2- rulegroup-logging-enabled	Stellen Sie sicher, dass die Erfassung von CloudWatch Amazon-Sicherheitsmetriken für AWS WAFv2 Regelgruppen aktiviert ist. Die Regel ist NON_COMPLIANT, wenn '. VisibilityConfig CloudWatchMetricsEnabledDas Feld 'ist auf falsch gesetzt.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.7.2	Ausfälle kritischer Sicherheitskontrollsysteme werden erkannt, gemeldet und umgehend behoben. (PCI-DSS-v4.0)	sns-topic-message-delivery-Benachrichtigung aktiviert	Stellen Sie sicher, dass die Amazon Simple Notification Service (SNS) - Protokollierung für den Zustellungsstatus von Benachrichtigungen aktiviert ist, die an ein Thema für die Endgeräte gesendet werden. Die Regel ist NON_COMPLIANT, wenn die Benachrichtigung über den Status der Zustellung von Nachrichten nicht aktiviert ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
11.5.2	Netzwerkeinbrüche und unerwartete Dateiänderungen werden erkannt und darauf reagiert. (PCI-DSS-v4.0)	cloudwatch-alarm-action-check	Stellen Sie sicher, dass bei CloudWatch Alarmen eine Aktion für den Status ALARM, INSUFFICIENT_DATA oder OK konfiguriert ist. Stellen Sie optional sicher, dass alle Aktionen mit einem benannten ARN übereinstimmen. Die Regel ist NON_COMPLIANT, wenn für den Alarm oder den optionalen Parameter keine Aktion festgelegt ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
11.5.2	Netzwerkeinbrüche und unerwartete Dateiänderungen werden erkannt und darauf reagiert. (PCI-DSS-v4.0)	cloudwatch-alarm-action-check	Stellen Sie sicher, dass bei CloudWatch Alarmen eine Aktion für den Status ALARM, INSUFFICIENT_DATA oder OK konfiguriert ist. Stellen Sie optional sicher, dass alle Aktionen mit einem benannten ARN übereinstimmen. Die Regel ist NON_COMPLIANT, wenn für den Alarm oder den optionalen Parameter keine Aktion festgelegt ist.
11.5.2	Netzwerkeinbrüche und unerwartete Dateiänderungen werden erkannt und darauf reagiert. (PCI-DSS-v4.0)	cloudwatch-alarm-settings-check	Stellen Sie sicher, dass CloudWatch Alarme mit dem angegebenen Metriknamen die angegebenen Einstellungen haben.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
11.5.2	Netzwerkeinbrüche und unerwartete Dateiänderungen werden erkannt und darauf reagiert. (PCI-DSS-v4.0)	sns-topic-message-delivery-Benachrichtigung aktiviert	Stellen Sie sicher, dass die Amazon Simple Notification Service (SNS) - Protokollierung für den Zustellungsstatus von Benachrichtigungen aktiviert ist, die an ein Thema für die Endgeräte gesendet werden. Die Regel ist NON_COMPLIANT, wenn die Benachrichtigung über den Status der Zustellung von Nachrichten nicht aktiviert ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
11.6.1	Unbefugte Änderungen auf Zahlungsseiten werden erkannt und darauf reagiert. (PCI-DSS-v4.0)	cloudwatch-alarm-action-check	Stellen Sie sicher, dass bei CloudWatch Alarmen eine Aktion für den Status ALARM, INSUFFICIENT_DATA oder OK konfiguriert ist. Stellen Sie optional sicher, dass alle Aktionen mit einem benannten ARN übereinstimmen. Die Regel ist NON_COMPLIANT, wenn für den Alarm oder den optionalen Parameter keine Aktion festgelegt ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
11.6.1	Unbefugte Änderungen auf Zahlungsseiten werden erkannt und darauf reagiert. (PCI-DSS-v4.0)	cloudwatch-alarm-action-check	Stellen Sie sicher, dass bei CloudWatch Alarmen eine Aktion für den Status ALARM, INSUFFICIENT_DATA oder OK konfiguriert ist. Stellen Sie optional sicher, dass alle Aktionen mit einem benannten ARN übereinstimmen. Die Regel ist NON_COMPLIANT, wenn für den Alarm oder den optionalen Parameter keine Aktion festgelegt ist.
11.6.1	Unbefugte Änderungen auf Zahlungsseiten werden erkannt und darauf reagiert. (PCI-DSS-v4.0)	cloudwatch-alarm-settings-check	Stellen Sie sicher, dass CloudWatch Alarme mit dem angegebenen Metriknamen die angegebenen Einstellungen haben.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
11.6.1	Unbefugte Änderungen auf Zahlungsseiten werden erkannt und darauf reagiert. (PCI-DSS-v4.0)	sns-topic-message-delivery-Benachrichtigung aktiviert	Stellen Sie sicher, dass die Amazon Simple Notification Service (SNS) - Protokollierung für den Zustellungsstatus von Benachrichtigungen aktiviert ist, die an ein Thema für die Endgeräte gesendet werden. Die Regel ist NON_COMPLIANT, wenn die Benachrichtigung über den Status der Zustellung von Nachrichten nicht aktiviert ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
12.10.5	Auf vermutete und bestätigte Sicherheitsvorfälle, die sich auf das CDE auswirken könnten, wird sofort reagiert. (PCI-DSS-v4.0)	cloudwatch-alarm-action-check	Stellen Sie sicher, dass bei CloudWatch Alarmen eine Aktion für den Status ALARM, INSUFFICIENT_DATA oder OK konfiguriert ist. Stellen Sie optional sicher, dass alle Aktionen mit einem benannten ARN übereinstimmen. Die Regel ist NON_COMPLIANT, wenn für den Alarm oder den optionalen Parameter keine Aktion festgelegt ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
12.10.5	Auf vermutete und bestätigte Sicherheitsvorfälle, die sich auf das CDE auswirken könnten, wird sofort reagiert. (PCI-DSS-v4.0)	cloudwatch-alarm-action-check	Stellen Sie sicher, dass bei CloudWatch Alarmen eine Aktion für den Status ALARM, INSUFFICIENT_DATA oder OK konfiguriert ist. Stellen Sie optional sicher, dass alle Aktionen mit einem benannten ARN übereinstimmen. Die Regel ist NON_COMPLIANT, wenn für den Alarm oder den optionalen Parameter keine Aktion festgelegt ist.
12.10.5	Auf vermutete und bestätigte Sicherheitsvorfälle, die sich auf das CDE auswirken könnten, wird sofort reagiert. (PCI-DSS-v4.0)	cloudwatch-alarm-settings-check	Stellen Sie sicher, dass CloudWatch Alarme mit dem angegebenen Metriknamen die angegebenen Einstellungen haben.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
12.10.5	Auf vermutete und bestätigte Sicherheitsvorfälle, die sich auf das CDE auswirken könnten, wird sofort reagiert. (PCI-DSS-v4.0)	sns-topic-message-delivery-Benachrichtigung aktiviert	Stellen Sie sicher, dass die Amazon Simple Notification Service (SNS) - Protokollierung für den Zustellungsstatus von Benachrichtigungen aktiviert ist, die an ein Thema für die Endgeräte gesendet werden. Die Regel ist NON_COMPLIANT, wenn die Benachrichtigung über den Status der Zustellung von Nachrichten nicht aktiviert ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
12.4.2.1	Die PCI-DSS-Konformität wird verwaltet. (PCI-DSS-v4.0)	service-catalog-shared-within-Organisation	Stellen Sie sicher, dass AWS Service Catalog Portfolios an eine Organisation weitergibt (eine Sammlung von AWS Konten, die als eine Einheit behandelt werden), wenn die Integration mit AWS Organizations aktiviert ist. Die Regel lautet NON_COMPLIANT, wenn der Wert `Type` einer Aktie `ACCOUNT` ist.
2.2.5	Systemkomponenten werden sicher konfiguriert und verwaltet. (PCI-DSS-v4.0)	transfer-family-server-no-ftp	Stellen Sie sicher, dass ein mit AWS Transfer Family erstellter Server kein FTP für die Endpunktverbindung verwendet. Die Regel lautet NON_COMPLIANT, wenn das Serverprotokoll für die Endpunktverbindung FTP-fähig ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
2.2.7	Systemkomponenten werden sicher konfiguriert und verwaltet. (PCI-DSS-v4.0)	dms-redis-tls-enabled	Stellen Sie sicher, dass die Endpunkte des AWS Database Migration Service (AWS DMS) für Redis-Datenspeicher aktiviert sind, sodass die TLS/SSL encryption of data communicated with other endpoints. The rule is NON_COMPLIANT if TLS/SSL Verschlüsselung nicht aktiviert ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
2.2.7	Systemkomponenten werden sicher konfiguriert und verwaltet. (PCI-DSS-v4.0)	elb-acm-certificate-required	Stellen Sie sicher, dass die Classic Load Balancers SSL-Zerti fikate verwenden, die vom AWS Certificate Manager bereitgestellt werden. Verwenden Sie zur Nutzung dieser Regel mit Ihrem Classic Load Balancer einen SSL- oder HTTPS-Listener. Hinweis: Diese Regel gilt nur für Classic Load Balancers. Mit dieser Regel werden keine Applicati on Load Balancer oder Network Load Balancer geprüft.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
2.2.7	Systemkomponenten werden sicher konfiguriert und verwaltet. (PCI-DSS-v4.0)	msk-in-cluster-node-TLS erforderlich	Stellen Sie sicher, dass ein Amazon MSK-Cluster die Verschlüsselung während der Übertragung mithilfe von HTTPS (TLS) mit den Broker-Kn oten des Clusters erzwingt. Die Regel ist NON_COMPL IANT, wenn Klartextk ommunikation für Broker-Knotenverbi ndungen in Clustern aktiviert ist.
2.2.7	Systemkomponenten werden sicher konfiguriert und verwaltet. (PCI-DSS-v4.0)	dms-endpoint-ssl-c onfigured	Stellen Sie sicher, dass die Endpoints des AWS Database Migration Service (AWS DMS) mit einer SSL-Verbindung konfiguriert sind. Die Regel lautet NON_COMPLIANT, wenn für AWS DMS keine SSL-Verbi ndung konfiguriert ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.2.1	Die Speicherung von Kontodaten wird auf ein Minimum beschränkt. (PCI-DSS-v4.0)	ec2- volume-inuse-check	Stellen Sie sicher, dass EBS-Volumes an Instances angehängt sind. EC2 Stellen Sie optional sicher, dass EBS-Volumes zum Löschen markiert sind, wenn eine Instance beendet wird.
3.2.1	Die Speicherung von Kontodaten wird auf ein Minimum beschränkt. (PCI-DSS-v4.0)	ecr-private-lifecycle-policy-konfiguriert	Stellen Sie sicher, dass für ein privates Amazon Elastic Container Registry (ECR) -Repository mindestens eine Lebenszyklusrichtlinie konfiguriert ist. Die Regel ist NON_COMPLIANT, wenn keine Lebenszyklus-Richtlinie für das private ECR-Repository konfiguriert ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.2.1	Die Speicherung von Kontodaten wird auf ein Minimum beschränkt. (PCI-DSS-v4.0)	dynamodb-pitr-enabled	Stellen Sie sicher, dass point-in-time Recovery (PITR) für Amazon DynamoDB-Tabellen aktiviert ist. Die Regel ist NON_COMPLIANT, wenn PITR für DynamoDB-Tabellen nicht aktiviert ist.
3.2.1	Die Speicherung von Kontodaten wird auf ein Minimum beschränkt. (PCI-DSS-v4.0)	cw-loggroup-retention-period-überprüfen	Stellen Sie sicher, dass ein CloudWatch LogGroup Amazon-Aufbewahrungszeitraum auf mehr als 365 Tage oder einen bestimmten Aufbewahrungszeitraum festgelegt ist. Die Regel lautet NON_COMPLIANT, wenn die Aufbewahrungsfrist weniger als MinRetentionTime, falls angegeben, oder andernfalls 365 Tage beträgt.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.3.1.1	Sensible Authentif izierungsdaten (SAD) werden nach der Autorisierung nicht gespeichert. (PCI-DSS-v4.0)	ec2- volume-inuse-check	Stellen Sie sicher, dass EBS-Volum es an Instances angehängt sind. EC2 Stellen Sie optional sicher, dass EBS-Volumes zum Löschen markiert sind, wenn eine Instance beendet wird.
3.3.1.1	Sensible Authentif izierungsdaten (SAD) werden nach der Autorisierung nicht gespeichert. (PCI-DSS-v4.0)	ecr-private-lifecycle-policy-konfiguriert	Stellen Sie sicher, dass für ein privates Amazon Elastic Container Registry (ECR) -Reposito ry mindestens eine Lebenszyk lusrichtlinie konfiguri ert ist. Die Regel ist NON_COMPL IANT, wenn keine Lebenszyklus-Richt linie für das private ECR-Repository konfiguriert ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.3.1.1	Sensible Authentifizierungsdaten (SAD) werden nach der Autorisierung nicht gespeichert. (PCI-DSS-v4.0)	dynamodb-pitr-enabled	Stellen Sie sicher, dass point-in-time Recovery (PITR) für Amazon DynamoDB-Tabellen aktiviert ist. Die Regel ist NON_COMPLIANT, wenn PITR für DynamoDB-Tabellen nicht aktiviert ist.
3.3.1.1	Sensible Authentifizierungsdaten (SAD) werden nach der Autorisierung nicht gespeichert. (PCI-DSS-v4.0)	cw-loggroup-retention-period-überprüfen	Stellen Sie sicher, dass ein CloudWatch LogGroup Amazon-Aufbewahrungszeitraum auf mehr als 365 Tage oder einen bestimmten Aufbewahrungszeitraum festgelegt ist. Die Regel lautet NON_COMPLIANT, wenn die Aufbewahrungsfrist weniger als MinRetentionTime, falls angegeben, oder andernfalls 365 Tage beträgt.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.3.1.3	Sensible Authentif izierungsdaten (SAD) werden nach der Autorisierung nicht gespeichert. (PCI-DSS-v4.0)	ec2- volume-inuse-check	Stellen Sie sicher, dass EBS-Volum es an Instances angehängt sind. EC2 Stellen Sie optional sicher, dass EBS-Volumes zum Löschen markiert sind, wenn eine Instance beendet wird.
3.3.1.3	Sensible Authentif izierungsdaten (SAD) werden nach der Autorisierung nicht gespeichert. (PCI-DSS-v4.0)	ecr-private-lifecycle-policy-konfiguriert	Stellen Sie sicher, dass für ein privates Amazon Elastic Container Registry (ECR) -Reposito ry mindestens eine Lebenszyk lusrichtlinie konfiguri ert ist. Die Regel ist NON_COMPL IANT, wenn keine Lebenszyklus-Richt linie für das private ECR-Repository konfiguriert ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.3.1.3	Sensible Authentifizierungsdaten (SAD) werden nach der Autorisierung nicht gespeichert. (PCI-DSS-v4.0)	dynamodb-pitr-enabled	Stellen Sie sicher, dass point-in-time Recovery (PITR) für Amazon DynamoDB-Tabellen aktiviert ist. Die Regel ist NON_COMPLIANT, wenn PITR für DynamoDB-Tabellen nicht aktiviert ist.
3.3.1.3	Sensible Authentifizierungsdaten (SAD) werden nach der Autorisierung nicht gespeichert. (PCI-DSS-v4.0)	cw-loggroup-retention-period-überprüfen	Stellen Sie sicher, dass ein CloudWatch LogGroup Amazon-Aufbewahrungszeitraum auf mehr als 365 Tage oder einen bestimmten Aufbewahrungszeitraum festgelegt ist. Die Regel lautet NON_COMPLIANT, wenn die Aufbewahrungsfrist weniger als MinRetentionTime, falls angegeben, oder andernfalls 365 Tage beträgt.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.3.2	Sensible Authentif izierungsdaten (SAD) werden nach der Autorisierung nicht gespeichert. (PCI-DSS-v4.0)	ec2- volume-inuse-check	Stellen Sie sicher, dass EBS-Volum es an Instances angehängt sind. EC2 Stellen Sie optional sicher, dass EBS-Volumes zum Löschen markiert sind, wenn eine Instance beendet wird.
3.3.2	Sensible Authentif izierungsdaten (SAD) werden nach der Autorisierung nicht gespeichert. (PCI-DSS-v4.0)	ecr-private-lifecycle-policy-konfiguriert	Stellen Sie sicher, dass für ein privates Amazon Elastic Container Registry (ECR) -Reposito ry mindestens eine Lebenszyk lusrichtlinie konfiguri ert ist. Die Regel ist NON_COMPL IANT, wenn keine Lebenszyklus-Richt linie für das private ECR-Repository konfiguriert ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.3.2	Sensible Authentifizierungsdaten (SAD) werden nach der Autorisierung nicht gespeichert. (PCI-DSS-v4.0)	dynamodb-pitr-enabled	Stellen Sie sicher, dass point-in-time Recovery (PITR) für Amazon DynamoDB-Tabellen aktiviert ist. Die Regel ist NON_COMPLIANT, wenn PITR für DynamoDB-Tabellen nicht aktiviert ist.
3.3.2	Sensible Authentifizierungsdaten (SAD) werden nach der Autorisierung nicht gespeichert. (PCI-DSS-v4.0)	cw-loggroup-retention-period-überprüfen	Stellen Sie sicher, dass ein CloudWatch LogGroup Amazon-Aufbewahrungszeitraum auf mehr als 365 Tage oder einen bestimmten Aufbewahrungszeitraum festgelegt ist. Die Regel lautet NON_COMPLIANT, wenn die Aufbewahrungsfrist weniger als MinRetentionTime, falls angegeben, oder andernfalls 365 Tage beträgt.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.3.3	Sensible Authentif izierungsdaten (SAD) werden nach der Autorisierung nicht gespeichert. (PCI-DSS-v4.0)	ec2- volume-inuse-check	Stellen Sie sicher, dass EBS-Volum es an Instances angehängt sind. EC2 Stellen Sie optional sicher, dass EBS-Volumes zum Löschen markiert sind, wenn eine Instance beendet wird.
3.3.3	Sensible Authentif izierungsdaten (SAD) werden nach der Autorisierung nicht gespeichert. (PCI-DSS-v4.0)	ecr-private-lifecycle-policy-konfiguriert	Stellen Sie sicher, dass für ein privates Amazon Elastic Container Registry (ECR) -Reposito ry mindestens eine Lebenszyk lusrichtlinie konfiguri ert ist. Die Regel ist NON_COMPL IANT, wenn keine Lebenszyklus-Richt linie für das private ECR-Repository konfiguriert ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.3.3	Sensible Authentifizierungsdaten (SAD) werden nach der Autorisierung nicht gespeichert. (PCI-DSS-v4.0)	dynamodb-pitr-enabled	Stellen Sie sicher, dass point-in-time Recovery (PITR) für Amazon DynamoDB-Tabellen aktiviert ist. Die Regel ist NON_COMPLIANT, wenn PITR für DynamoDB-Tabellen nicht aktiviert ist.
3.3.3	Sensible Authentifizierungsdaten (SAD) werden nach der Autorisierung nicht gespeichert. (PCI-DSS-v4.0)	cw-loggroup-retention-period-überprüfen	Stellen Sie sicher, dass ein CloudWatch LogGroup Amazon-Aufbewahrungszeitraum auf mehr als 365 Tage oder einen bestimmten Aufbewahrungszeitraum festgelegt ist. Die Regel lautet NON_COMPLIANT, wenn die Aufbewahrungsfrist weniger als MinRetentionTime, falls angegeben, oder andernfalls 365 Tage beträgt.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.5.1	Die primäre Kontonummer (PAN) ist überall dort gesichert, wo sie gespeichert ist. (PCI-DSS-v4.0)	athena-workgroup-encrypted-at-ausruhen	Stellen Sie sicher, dass eine Amazon Athena Athena-Arbeitsgruppe im Ruhezustand verschlüsselt ist. Die Regel ist NON_COMPLIANT, wenn die Verschlüsselung von Daten im Ruhezustand für eine Athena-Arbeitsgruppe nicht aktiviert ist.
3.5.1	Die primäre Kontonummer (PAN) ist überall dort gesichert, wo sie gespeichert ist. (PCI-DSS-v4.0)	neptune-cluster-snapshot-encrypted	Stellen Sie sicher, dass ein Amazon Neptune Neptune-DB-Cluster über verschlüsselte Snapshots verfügt. Die Regel ist NON_COMPLIANT, wenn ein Neptune-Cluster keine verschlüsselten Snapshots enthält.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.5.1	Die primäre Kontonummer (PAN) ist überall dort gesichert, wo sie gespeichert ist. (PCI-DSS-v4.0)	redshift-cluster-kms-enabled	Stellen Sie sicher, dass Amazon Redshift Redshift-Cluster einen bestimmten AWS Key Management Service (AWS KMS) -Schlüssel für die Verschlüsselung verwenden. Die Regel ist KONFORM, wenn die Verschlüs selung aktiviert ist und der Cluster mit dem im kmsKeyArn Parameter angegeben en Schlüssel verschlüsselt ist. Die Regel ist NON_COMPLIANT, wenn der Cluster nicht oder mit einem anderen Schlüssel verschlüsselt ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.5.1	Die primäre Kontonummer (PAN) ist überall dort gesichert, wo sie gespeichert ist. (PCI-DSS-v4.0)	codebuild-project-s3-log-verschlüsselt	Stellen Sie sicher, dass bei einem mit Amazon S3 Logs konfigurierten AWS CodeBuild Projekt die Verschlüsselung für die Protokolle aktiviert ist. Die Regel lautet NON_COMPLIANT, wenn 'EncryptionDisabled' in einem LogsConfig S3-Projekt auf 'true' gesetzt ist. CodeBuild
3.5.1	Die primäre Kontonummer (PAN) ist überall dort gesichert, wo sie gespeichert ist. (PCI-DSS-v4.0)	eks-secrets-encrypted	Stellen Sie sicher, dass Amazon Elastic Kubernetes Service Service-Cluster so konfiguriert sind, dass Kubernetes-Geheimnisse mithilfe von AWS Key Management Service (KMS) - Schlüsseln verschlüsselt werden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.5.1	Die primäre Kontonummer (PAN) ist überall dort gesichert, wo sie gespeichert ist. (PCI-DSS-v4.0)	api-gw-cache-enabled-und-verschlüsselt	Stellen Sie sicher, dass für alle Methoden in den Amazon API Gateway Gateway-Stufen der Cache aktiviert und der Cache verschlüsselt ist. Die Regel ist NON_COMPLIANT, wenn für eine Methode in einer Amazon-API-Gateway-Stufe der Cache nicht konfiguriert oder nicht verschlüsselt ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.5.1	Die primäre Kontonummer (PAN) ist überall dort gesichert, wo sie gespeichert ist. (PCI-DSS-v4.0)	dynamodb-table-encrypted-kms	Stellen Sie sicher, dass die Amazon DynamoDB-Tabelle mit dem AWS Key Management Service (KMS) verschlüsselt ist. Die Regel lautet NON_COMPLIANT, wenn die Amazon DynamoDB-Tabelle nicht mit KMS verschlüsselt ist. AWS Die Regel ist auch NON_COMPLIANT, wenn der verschlüsselte AWS KMS-Schlüssel nicht im Eingabeparameter vorhanden ist. kmsKeyArns

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.5.1	Die primäre Kontonummer (PAN) ist überall dort gesichert, wo sie gespeichert ist. (PCI-DSS-v4.0)	codebuild-project-envvar-awscred-überprüfen	Stellen Sie sicher, dass das Projekt KEINE Umgebungs variablen und _ACCESS_KEY enthält. AWS_ACCES S_KEY_ID AWS_SECRE T Die Regel ist NON_COMPLIANT, wenn die Projekt-U mgebungsvariablen Klartext-Anmeldein formationen enthalten.
3.5.1	Die primäre Kontonummer (PAN) ist überall dort gesichert, wo sie gespeichert ist. (PCI-DSS-v4.0)	eks-cluster-secrets-encrypted	Stellen Sie sicher, dass Amazon EKS-Cluster nicht so konfiguriert sind, dass Kubernetes-Geheimnisse mit KMS verschlüsselt AWS werden. Die Regel lautet NON_COMPL IANT, wenn ein EKS-Cluster keine EncryptionConfig-R essource hat oder wenn Encryptio nConfig Geheimnisse nicht als Ressource benennt.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.5.1	Die primäre Kontonummer (PAN) ist überall dort gesichert, wo sie gespeichert ist. (PCI-DSS-v4.0)	kinesis-stream-encrypted	Stellen Sie sicher, dass Amazon Kinesis Kinesis-Streams im Ruhezustand mit serverseitiger Verschlüsselung verschlüsselt werden. Die Regel lautet NON_COMPLIANT für einen Kinesis-Stream, wenn 'StreamEncryption' nicht vorhanden ist.
3.5.1	Die primäre Kontonummer (PAN) ist überall dort gesichert, wo sie gespeichert ist. (PCI-DSS-v4.0)	neptune-cluster-encrypted	Stellen Sie sicher, dass die Speicherverschlüsselung für Ihre Amazon Neptune Neptune-DB-Cluster aktiviert ist. Die Regel ist NON_COMPLIANT, wenn die Speicherverschlüsselung nicht aktiviert ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.5.1.1	Die primäre Kontonummer (PAN) ist überall dort gesichert, wo sie gespeichert ist. (PCI-DSS-v4.0)	acm-pca-root-ca-deaktiviert	Stellen Sie sicher, dass die AWS Private Certificate Authority (AWS Private CA) über eine deaktivierte Stammzertifizierungsstelle verfügt. Die Regel ist NON_COMPLIANT für Root-Benutzer CAs mit einem Status, der nicht DEAKTIVIERT ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.5.1.1	Die primäre Kontonummer (PAN) ist überall dort gesichert, wo sie gespeichert ist. (PCI-DSS-v4.0)	elb-acm-certificate-required	Stellen Sie sicher, dass die Classic Load Balancers SSL-Zerti fikate verwenden, die vom AWS Certificate Manager bereitgestellt werden. Verwenden Sie zur Nutzung dieser Regel mit Ihrem Classic Load Balancer einen SSL- oder HTTPS-Listener. Hinweis: Diese Regel gilt nur für Classic Load Balancers. Mit dieser Regel werden keine Applicati on Load Balancer oder Network Load Balancer geprüft.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.5.1.3	Die primäre Kontonummer (PAN) ist überall dort gesichert, wo sie gespeichert ist. (PCI-DSS-v4.0)	acm-pca-root-ca-deaktiviert	Stellen Sie sicher, dass die AWS Private Certificate Authority (AWS Private CA) über eine deaktivierte Stammzertifizierungsstelle verfügt. Die Regel ist NON_COMPLIANT für Root-Benutzer CAs mit einem Status, der nicht DEAKTIVIERT ist.
3.5.1.3	Die primäre Kontonummer (PAN) ist überall dort gesichert, wo sie gespeichert ist. (PCI-DSS-v4.0)	neptune-cluster-snapshot-public-verboten	Stellen Sie sicher, dass ein manueller Amazon Neptune Neptune-DB-Cluster-Snapshot nicht öffentlich ist. Die Regel ist NON_COMPLIANT, wenn es vorhandene und neue Neptune-Cluster-Snapshots gibt, die öffentlich zugänglich sind.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.5.1.3	Die primäre Kontonummer (PAN) ist überall dort gesichert, wo sie gespeichert ist. (PCI-DSS-v4.0)	backup-recovery-point-manual-Löschen-deaktiviert	Stellen Sie sicher, dass an einen Backup-Tresor eine ressourcenbasierte Richtlinie angehängt ist, die das Löschen von Wiederherstellungspunkten verhindert. Die Regel lautet NON_COMPLIANT, wenn der Backup-Tresor keine ressourcenbasierten Richtlinien oder Richtlinien ohne eine geeignete „Deny“ -Anweisung (Anweisung mit den Berechtigungen backup:DeleteRecoveryPoint, backup: und backup:UpdateRecoveryPointLifecycle) hat. PutBackupVaultAccessPolicy

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.5.1.3	Die primäre Kontonummer (PAN) ist überall dort gesichert, wo sie gespeichert ist. (PCI-DSS-v4.0)	elb-acm-certificate-required	Stellen Sie sicher, dass die Classic Load Balancers SSL-Zerti fikate verwenden, die vom AWS Certificate Manager bereitgestellt werden. Verwenden Sie zur Nutzung dieser Regel mit Ihrem Classic Load Balancer einen SSL- oder HTTPS-Listener. Hinweis: Diese Regel gilt nur für Classic Load Balancers. Mit dieser Regel werden keine Applicati on Load Balancer oder Network Load Balancer geprüft.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.5.1.3	Die primäre Kontonummer (PAN) ist überall dort gesichert, wo sie gespeichert ist. (PCI-DSS-v4.0)	emr-block-public-access	Stellen Sie sicher, dass für ein Konto bei Amazon EMR die Einstellungen zum Sperren des öffentlichen Zugriffs aktiviert sind. Die Regel ist NON_COMPLIANT, wenn sie falsch BlockPublicSecurityGroupRules ist, oder wenn sie wahr ist, sind andere Ports als Port 22 unter aufgeführt. Permitted PublicSecurityGroupRuleRanges
3.5.1.3	Die primäre Kontonummer (PAN) ist überall dort gesichert, wo sie gespeichert ist. (PCI-DSS-v4.0)	access-point-public-accesss3-Blöcke	Stellen Sie sicher, dass Amazon S3 S3-Zugriffspunkten die Einstellungen zum Blockieren des öffentlichen Zugriffs aktiviert sind. Die Regel ist NON_COMPLIANT, wenn die Einstellung zum Blockieren des öffentlichen Zugriffs für S3-Zugangspunkte nicht aktiviert ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.5.1.3	Die primäre Kontonummer (PAN) ist überall dort gesichert, wo sie gespeichert ist. (PCI-DSS-v4.0)	account-level-public-accesss3-Blöcke	Stellen Sie sicher, dass die erforderl ichen Einstellungen für die Sperrung des öffentlichen Zugriffs auf Kontoebene konfiguriert sind. Die Regel ist nur NON_COMPL IANT, wenn die unten festgeleg ten Felder nicht mit den entsprech enden Feldern im Konfigurationselement übereinstimmen.
3.5.1.3	Die primäre Kontonummer (PAN) ist überall dort gesichert, wo sie gespeichert ist. (PCI-DSS-v4.0)	s-3 bucket-mfa-delete-enabled	Stellen Sie sicher, dass MFA Delete in der Bucket-Ve rsionierungskonfig uration von Amazon Simple Storage Service (Amazon S3) aktiviert ist. Die Regel ist NON_COMPL IANT, wenn MFA Delete nicht aktiviert ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.6.1	Kryptografische Schlüssel, die zum Schutz der gespeicherten Kontodaten verwendet werden, sind gesichert. (PCI-DSS-v4.0)	acm-pca-root-ca-deaktiviert	Stellen Sie sicher, dass die AWS Private Certificate Authority (AWS Private CA) über eine deaktivierte Stammzertifizierungsstelle verfügt. Die Regel ist NON_COMPLIANT für Root-Benutzer CAs mit einem Status, der nicht DEAKTIVIERT ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.6.1	Kryptografische Schlüssel, die zum Schutz der gespeiche rten Kontodaten verwendet werden, sind gesichert. (PCI-DSS-v4.0)	elb-acm-certificate-required	Stellen Sie sicher, dass die Classic Load Balancers SSL-Zerti fikate verwenden, die vom AWS Certificate Manager bereitgestellt werden. Verwenden Sie zur Nutzung dieser Regel mit Ihrem Classic Load Balancer einen SSL- oder HTTPS-Listener. Hinweis: Diese Regel gilt nur für Classic Load Balancers. Mit dieser Regel werden keine Applicati on Load Balancer oder Network Load Balancer geprüft.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.6.1.2	Kryptografische Schlüssel, die zum Schutz der gespeicherten Kontodaten verwendet werden, sind gesichert. (PCI-DSS-v4.0)	acm-pca-root-ca-deaktiviert	Stellen Sie sicher, dass die AWS Private Certificate Authority (AWS Private CA) über eine deaktivierte Stammzertifizierungsstelle verfügt. Die Regel ist NON_COMPLIANT für Root-Benutzer CAs mit einem Status, der nicht DEAKTIVIERT ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.6.1.2	Kryptografische Schlüssel, die zum Schutz der gespeiche rten Kontodaten verwendet werden, sind gesichert. (PCI-DSS-v4.0)	elb-acm-certificate-required	Stellen Sie sicher, dass die Classic Load Balancers SSL-Zerti fikate verwenden, die vom AWS Certificate Manager bereitgestellt werden. Verwenden Sie zur Nutzung dieser Regel mit Ihrem Classic Load Balancer einen SSL- oder HTTPS-Listener. Hinweis: Diese Regel gilt nur für Classic Load Balancers. Mit dieser Regel werden keine Applicati on Load Balancer oder Network Load Balancer geprüft.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.6.1.3	Kryptografische Schlüssel, die zum Schutz der gespeicherten Kontodaten verwendet werden, sind gesichert. (PCI-DSS-v4.0)	acm-pca-root-ca-deaktiviert	Stellen Sie sicher, dass die AWS Private Certificate Authority (AWS Private CA) über eine deaktivierte Stammzertifizierungsstelle verfügt. Die Regel ist NON_COMPLIANT für Root-Benutzer CAs mit einem Status, der nicht DEAKTIVIERT ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.6.1.3	Kryptografische Schlüssel, die zum Schutz der gespeiche rten Kontodaten verwendet werden, sind gesichert. (PCI-DSS-v4.0)	elb-acm-certificate-required	Stellen Sie sicher, dass die Classic Load Balancers SSL-Zerti fikate verwenden, die vom AWS Certificate Manager bereitgestellt werden. Verwenden Sie zur Nutzung dieser Regel mit Ihrem Classic Load Balancer einen SSL- oder HTTPS-Listener. Hinweis: Diese Regel gilt nur für Classic Load Balancers. Mit dieser Regel werden keine Applicati on Load Balancer oder Network Load Balancer geprüft.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.6.1.4	Kryptografische Schlüssel, die zum Schutz der gespeicherten Kontodaten verwendet werden, sind gesichert. (PCI-DSS-v4.0)	acm-pca-root-ca-deaktiviert	Stellen Sie sicher, dass die AWS Private Certificate Authority (AWS Private CA) über eine deaktivierte Stammzertifizierungsstelle verfügt. Die Regel ist NON_COMPLIANT für Root-Benutzer CAs mit einem Status, der nicht DEAKTIVIERT ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.6.1.4	Kryptografische Schlüssel, die zum Schutz der gespeiche rten Kontodaten verwendet werden, sind gesichert. (PCI-DSS-v4.0)	elb-acm-certificate-required	Stellen Sie sicher, dass die Classic Load Balancers SSL-Zerti fikate verwenden, die vom AWS Certificate Manager bereitgestellt werden. Verwenden Sie zur Nutzung dieser Regel mit Ihrem Classic Load Balancer einen SSL- oder HTTPS-Listener. Hinweis: Diese Regel gilt nur für Classic Load Balancers. Mit dieser Regel werden keine Applicati on Load Balancer oder Network Load Balancer geprüft.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.7.1	Wo Kryptografie zum Schutz gespeicherter Kontodaten eingesetzt wird, werden Schlüsselverwaltungsprozesse und -verfahren, die alle Aspekte des Schlüssellebenszyklus abdecken, definiert und implementiert. (PCI-DSS-v4.0)	acm-certificate-rsa-check	Stellen Sie sicher, dass von AWS Certificate Manager (ACM) verwaltete RSA-Zertifikate eine Schlüssellänge von mindestens '2048' Bit haben. Die Regel lautet NON_COMPLIANT, wenn die Mindestschlüssellänge weniger als 2048 Bit beträgt.
3.7.1	Wo Kryptografie zum Schutz gespeicherter Kontodaten verwendet wird, werden Schlüsselverwaltungsprozesse und -verfahren, die alle Aspekte des Schlüssellebenszyklus abdecken, definiert und implementiert. (PCI-DSS-v4.0)	acm-pca-root-ca-deaktiviert	Stellen Sie sicher, dass die AWS Private Certificate Authority (AWS Private CA) über eine deaktivierte Stammzertifizierungsstelle verfügt. Die Regel ist NON_COMPLIANT für Root-Benutzer CAs mit einem Status, der nicht DEAKTIVIERT ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.7.1	Wo Kryptografie zum Schutz gespeicherter Kontodaten eingesetzt wird, werden Schlüsselverwaltungsprozesse und -verfahren, die alle Aspekte des Schlüssellebenszyklus abdecken, definiert und implementiert. (PCI-DSS-v4.0)	elb-acm-certificate-required	Stellen Sie sicher, dass die Classic Load Balancers SSL-Zertifikate verwenden, die vom AWS Certificate Manager bereitgestellt werden. Verwenden Sie zur Nutzung dieser Regel mit Ihrem Classic Load Balancer einen SSL- oder HTTPS-Listener. Hinweis: Diese Regel gilt nur für Classic Load Balancers. Mit dieser Regel werden keine Application Load Balancer oder Network Load Balancer geprüft.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.7.2	Wo Kryptografie zum Schutz gespeicherter Kontodaten eingesetzt wird, werden Schlüsselverwaltungsprozesse und -verfahren, die alle Aspekte des Schlüssellebenszyklus abdecken, definiert und implementiert. (PCI-DSS-v4.0)	acm-pca-root-ca-deaktiviert	Stellen Sie sicher, dass die AWS Private Certificate Authority (AWS Private CA) über eine deaktivierte Stammzertifizierungsstelle verfügt. Die Regel ist NON_COMPLIANT für Root-Benutzer CAs mit einem Status, der nicht DEAKTIVIERT ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.7.2	Wo Kryptografie zum Schutz gespeicherter Kontodaten eingesetzt wird, werden Schlüsselverwaltungsprozesse und -verfahren, die alle Aspekte des Schlüssellebenszyklus abdecken, definiert und implementiert. (PCI-DSS-v4.0)	elb-acm-certificate-required	Stellen Sie sicher, dass die Classic Load Balancers SSL-Zertifikate verwenden, die vom AWS Certificate Manager bereitgestellt werden. Verwenden Sie zur Nutzung dieser Regel mit Ihrem Classic Load Balancer einen SSL- oder HTTPS-Listener. Hinweis: Diese Regel gilt nur für Classic Load Balancers. Mit dieser Regel werden keine Application Load Balancer oder Network Load Balancer geprüft.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.7.4	Wo Kryptografie zum Schutz gespeicherter Kontodaten eingesetzt wird, werden Schlüsselverwaltungsprozesse und -verfahren, die alle Aspekte des Schlüssellebenszyklus abdecken, definiert und implementiert. (PCI-DSS-v4.0)	acm-pca-root-ca-deaktiviert	Stellen Sie sicher, dass die AWS Private Certificate Authority (AWS Private CA) über eine deaktivierte Stammzertifizierungsstelle verfügt. Die Regel ist NON_COMPLIANT für Root-Benutzer CAs mit einem Status, der nicht DEAKTIVIERT ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.7.4	Wo Kryptografie zum Schutz gespeicherter Kontodaten eingesetzt wird, werden Schlüsselverwaltungsprozesse und -verfahren, die alle Aspekte des Schlüssellebenszyklus abdecken, definiert und implementiert. (PCI-DSS-v4.0)	elb-acm-certificate-required	Stellen Sie sicher, dass die Classic Load Balancers SSL-Zertifikate verwenden, die vom AWS Certificate Manager bereitgestellt werden. Verwenden Sie zur Nutzung dieser Regel mit Ihrem Classic Load Balancer einen SSL- oder HTTPS-Listener. Hinweis: Diese Regel gilt nur für Classic Load Balancers. Mit dieser Regel werden keine Application Load Balancer oder Network Load Balancer geprüft.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.7.6	Wo Kryptografie zum Schutz gespeicherter Kontodaten eingesetzt wird, werden Schlüsselverwaltungsprozesse und -verfahren, die alle Aspekte des Schlüssellebenszyklus abdecken, definiert und implementiert. (PCI-DSS-v4.0)	acm-pca-root-ca-deaktiviert	Stellen Sie sicher, dass die AWS Private Certificate Authority (AWS Private CA) über eine deaktivierte Stammzertifizierungsstelle verfügt. Die Regel ist NON_COMPLIANT für Root-Benutzer CAs mit einem Status, der nicht DEAKTIVIERT ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.7.6	Wo Kryptografie zum Schutz gespeicherter Kontodaten eingesetzt wird, werden Schlüsselverwaltungsprozesse und -verfahren, die alle Aspekte des Schlüssellebenszyklus abdecken, definiert und implementiert. (PCI-DSS-v4.0)	elb-acm-certificate-required	Stellen Sie sicher, dass die Classic Load Balancers SSL-Zertifikate verwenden, die vom AWS Certificate Manager bereitgestellt werden. Verwenden Sie zur Nutzung dieser Regel mit Ihrem Classic Load Balancer einen SSL- oder HTTPS-Listener. Hinweis: Diese Regel gilt nur für Classic Load Balancers. Mit dieser Regel werden keine Application Load Balancer oder Network Load Balancer geprüft.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.7.7	Wo Kryptografie zum Schutz gespeicherter Kontodaten eingesetzt wird, werden wichtige Verwaltungsprozesse und -verfahren, die alle Aspekte des Schlüssel lebenszyklus abdecken, definiert und implementiert. (PCI-DSS-v4.0)	acm-pca-root-ca-deaktiviert	Stellen Sie sicher, dass die AWS Private Certificate Authority (AWS Private CA) über eine deaktivierte Stammzertifizierungsstelle verfügt. Die Regel ist NON_COMPLIANT für Root-Benutzer CAs mit einem Status, der nicht DEAKTIVIERT ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.7.7	Wo Kryptografie zum Schutz gespeicherter Kontodaten eingesetzt wird, werden wichtige Verwaltungsprozess e und -verfahren, die alle Aspekte des Schlüssel lebenszyklus abdecken, definiert und implementiert. (PCI-DSS-v4.0)	elb-acm-certificate-required	Stellen Sie sicher, dass die Classic Load Balancers SSL-Zerti fikate verwenden, die vom AWS Certificate Manager bereitgestellt werden. Verwenden Sie zur Nutzung dieser Regel mit Ihrem Classic Load Balancer einen SSL- oder HTTPS-Listener. Hinweis: Diese Regel gilt nur für Classic Load Balancers. Mit dieser Regel werden keine Applicati on Load Balancer oder Network Load Balancer geprüft.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
4.2.1	PAN ist während der Übertragung mit starker Kryptografie geschützt. (PCI-DSS-v4.0)	dms-redis-tls-enabled	Stellen Sie sicher, dass die Endpunkte des AWS Database Migration Service (AWS DMS) für Redis-Datenspeicher aktiviert sind, sodass die TLS/SSL encryption of data communicated with other endpoints. The rule is NON_COMPLIANT if TLS/SSL Verschlüsselung nicht aktiviert ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
4.2.1	PAN ist während der Übertragung mit starker Kryptografie geschützt. (PCI-DSS-v4.0)	elb-acm-certificate-required	Stellen Sie sicher, dass die Classic Load Balancers SSL-Zerti fikate verwenden, die vom AWS Certificate Manager bereitgestellt werden. Verwenden Sie zur Nutzung dieser Regel mit Ihrem Classic Load Balancer einen SSL- oder HTTPS-Listener. Hinweis: Diese Regel gilt nur für Classic Load Balancers. Mit dieser Regel werden keine Applicati on Load Balancer oder Network Load Balancer geprüft.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
4.2.1	PAN ist während der Übertragung mit starker Kryptografie geschützt. (PCI-DSS-v4.0)	msk-in-cluster-node-TLS erforderlich	Stellen Sie sicher, dass ein Amazon MSK-Cluster die Verschlüsselung während der Übertragung mithilfe von HTTPS (TLS) mit den Broker-Kn oten des Clusters erzwingt. Die Regel ist NON_COMPL IANT, wenn Klartextk ommunikation für Broker-Knotenverbi ndungen in Clustern aktiviert ist.
4.2.1	PAN ist während der Übertragung mit starker Kryptografie geschützt. (PCI-DSS-v4.0)	dms-endpoint-ssl-c onfigured	Stellen Sie sicher, dass die Endpoints des AWS Database Migration Service (AWS DMS) mit einer SSL-Verbindung konfiguriert sind. Die Regel lautet NON_COMPLIANT, wenn für AWS DMS keine SSL-Verbi ndung konfiguriert ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
4.2.1.1	PAN ist während der Übertragung durch starke Kryptografie geschützt. (PCI-DSS-v4.0)	acm-pca-root-ca-deaktiviert	Stellen Sie sicher, dass die AWS Private Certificate Authority (AWS Private CA) über eine deaktivierte Stammzertifizierungsstelle verfügt. Die Regel ist NON_COMPLIANT für Root-Benutzer CAs mit einem Status, der nicht DEAKTIVIERT ist.
4.2.1.1	PAN ist während der Übertragung durch starke Kryptografie geschützt. (PCI-DSS-v4.0)	cloudfront-custom-ssl-certificate	Stellen Sie sicher, dass das mit einer CloudFront Amazon-Distribution verknüpfte Zertifikat nicht das Standard-SSL-Zertifikat ist. Die Regel lautet NON_COMPLIANT, wenn eine CloudFront Distribution das Standard-SSL-Zertifikat verwendet.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
4.2.1.1	PAN ist während der Übertragung durch starke Kryptografie geschützt. (PCI-DSS-v4.0)	dms-redis-tls-enabled	Stellen Sie sicher, dass die Endpunkte des AWS Database Migration Service (AWS DMS) für Redis-Datenspeicher aktiviert sind, sodass die TLS/SSL encryption of data communicated with other endpoints. The rule is NON_COMPLIANT if TLS/SSL Verschlüsselung nicht aktiviert ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
4.2.1.1	PAN ist während der Übertragung durch starke Kryptografie geschützt. (PCI-DSS-v4.0)	elb-acm-certificate-required	Stellen Sie sicher, dass die Classic Load Balancers SSL-Zerti fikate verwenden, die vom AWS Certificate Manager bereitgestellt werden. Verwenden Sie zur Nutzung dieser Regel mit Ihrem Classic Load Balancer einen SSL- oder HTTPS-Listener. Hinweis: Diese Regel gilt nur für Classic Load Balancers. Mit dieser Regel werden keine Applicati on Load Balancer oder Network Load Balancer geprüft.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
4.2.1.1	PAN ist während der Übertragung durch starke Kryptografie geschützt. (PCI-DSS-v4.0)	msk-in-cluster-node-TLS erforderlich	Stellen Sie sicher, dass ein Amazon MSK-Cluster die Verschlüsselung während der Übertragung mithilfe von HTTPS (TLS) mit den Broker-Kn oten des Clusters erzwingt. Die Regel ist NON_COMPL IANT, wenn Klartextk ommunikation für Broker-Knotenverbi ndungen in Clustern aktiviert ist.
4.2.1.1	PAN ist während der Übertragung durch starke Kryptografie geschützt. (PCI-DSS-v4.0)	dms-endpoint-ssl-c onfigured	Stellen Sie sicher, dass die Endpoints des AWS Database Migration Service (AWS DMS) mit einer SSL-Verbindung konfiguriert sind. Die Regel lautet NON_COMPLIANT, wenn für AWS DMS keine SSL-Verbi ndung konfiguriert ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
5.3.4	Anti-Malware-Mechanismen und -Prozesse sind aktiv, werden gewartet und überwacht. (PCI-DSS-v4.0)	api-gwv2- access-logs-enabled	Stellen Sie sicher, dass die Amazon API Gateway V2-Stufen die Zugriffsprotokollierung aktiviert haben. Die Regel ist NON_COMPLIANT, wenn 'accessLogSettings' in der Stage-Konfiguration nicht vorhanden ist.
5.3.4	Anti-Malware-Mechanismen und -Prozesse sind aktiv, werden gewartet und überwacht. (PCI-DSS-v4.0)	api-gw-xray-enabled	Stellen Sie sicher, dass AWS X-Ray Tracing auf Amazon API Gateway REST APIs aktiviert ist. Die Regel ist COMPLIANT, wenn die X-Ray-Abl aufverfolgung aktiviert ist, andernfalls ist sie NON_COMPLIANT.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
5.3.4	Anti-Malware-Mechanismen und -Prozesse sind aktiv, werden gewartet und überwacht. (PCI-DSS-v4.0)	cloudtrail-security-trail-enabled	Stellen Sie sicher, dass mindestens ein AWS CloudTrail Pfad mit bewährten Sicherheitsmethoden definiert ist. Diese Regel ist COMPLIANT, wenn es mindestens einen Trail gibt, der alle der folgenden Bedingungen erfüllt:
5.3.4	Anti-Malware-Mechanismen und -Prozesse sind aktiv, werden gewartet und überwacht. (PCI-DSS-v4.0)	neptune-cluster-cloudwatch-log-exportfähig	Stellen Sie sicher, dass in einem Amazon Neptune Neptune-Cluster der Protokollexport für CloudWatch Audit-Logs aktiviert ist. Die Regel lautet NON_COMPLIANT, wenn für einen Neptune-Cluster der Protokollexport für CloudWatch Audit-Logs nicht aktiviert ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
5.3.4	Anti-Malware-Mechanismen und -Prozesse sind aktiv, werden gewartet und überwacht. (PCI-DSS-v4.0)	ecs-task-definition-log-Konfiguration	Stellen Sie sicher, dass LogConfiguration für aktive ECS-Aufgabendefinitionen festgelegt ist. Diese Regel ist NON_COMPLIANT, wenn für eine aktive ECSTask Definition die LogConfiguration-Ressource nicht definiert ist oder der Wert für LogConfiguration in mindestens einer Containerdefinition Null ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
5.3.4	Anti-Malware-Mechanismen und -Prozesse sind aktiv, werden gewartet und überwacht. (PCI-DSS-v4.0)	cloudtrail-enabled	Hinweis: Bei dieser Regel untersche iden sich die Regel-ID (CLOUD_TR AIL_ENABLED) und der Regelname (cloudtrail-enabled). Stellen Sie sicher, dass in Ihrem Konto ein Trail aktiviert ist AWS CloudTrail . AWS Die Regel ist NON_COMPLIANT, wenn ein Trail nicht aktiviert ist. Optional überprüft die Regel einen bestimmten S3-Bucket, ein Amazon Simple Notification Service (Amazon SNS) -Thema und eine CloudWatch Protokollgruppe.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
5.3.4	Anti-Malware-Mechanismen und -Prozesse sind aktiv, werden gewartet und überwacht. (PCI-DSS-v4.0)	multi-region-cloudtrail-enabled	Hinweis: Bei dieser Regel untersche iden sich die Regel-ID (MULTI_RE GION_CLOU D_TRAIL_ENABLED) und der Regelname (). multi-region-cloudtrail-enabled Stellen Sie sicher, dass mindesten s eine Region mit mehreren Regionen vorhanden ist. AWS CloudTrail Die Regel ist NON_COMPL IANT, wenn die Trails nicht mit den Eingabeparametern übereinstimmen. Die Regel lautet NON_COMPLIANT, wenn das ExcludeMa nagementEventSourc es Feld nicht leer ist oder wenn sie so konfiguriert AWS CloudTrail ist, dass Verwaltungsereigni sse wie AWS KMS-Ereignisse oder Amazon RDS-Daten -API-Ereignisse

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			ausgeschlossen werden.
5.3.4	Anti-Malware-Mechanismen und -Prozesse sind aktiv, werden gewartet und überwacht. (PCI-DSS-v4.0)	appsync-logging-enabled	Stellen Sie sicher, dass für eine API die Protokollierung aktiviert ist. AWS AppSync Die Regel lautet NON_COMPLIANT, wenn die Protokollierung nicht aktiviert ist, oder 'fieldLogLevel' ist weder ERROR noch ALL.
5.3.4	Anti-Malware-Mechanismen und -Prozesse sind aktiv, werden gewartet und überwacht. (PCI-DSS-v4.0)	mq-cloudwatch-audit-logging-aktiviert	Stellen Sie sicher, dass Amazon MQ-Broker die CloudWatch Amazon-Auditprotokollierung aktiviert haben. Die Regel ist NON_COMPLIANT, wenn für einen Broker die Audit-Protokollierung nicht aktiviert ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
5.3.4	Anti-Malware-Mechanismen und -Prozesse sind aktiv, werden gewartet und überwacht. (PCI-DSS-v4.0)	mq-cloudwatch-audit-log-aktiviert	Stellen Sie sicher, dass bei einem Amazon MQ-Broker die CloudWatch Auditprotokollierung aktiviert ist. Die Regel lautet NON_COMPLIANT, wenn für den Broker die Audit-Protokollierung nicht aktiviert ist.
5.3.4	Anti-Malware-Mechanismen und -Prozesse sind aktiv, werden gewartet und überwacht. (PCI-DSS-v4.0)	eks-cluster-logging-enabled	Stellen Sie sicher, dass ein Amazon Elastic Kubernetes Service (Amazon EKS) -Cluster mit aktivierter Protokollierung konfiguriert ist. Die Regel ist NON_COMPLIANT, wenn die Protokollierung für Amazon-EKS-Cluster nicht für alle Protokolltypen aktiviert ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
5.3.4	Anti-Malware-Mechanismen und -Prozesse sind aktiv, werden gewartet und überwacht. (PCI-DSS-v4.0)	elastic-beanstalk-logs-to-Wolkenbeobachtung	Stellen Sie sicher, dass AWS Elastic Beanstalk Beanstalk -Umgebungen so konfiguriert sind, dass sie Protokolle an Amazon CloudWatch Logs senden. Die Regel lautet NON_COMPLIANT, wenn der Wert von `` StreamLogs falsch ist.
5.3.4	Anti-Malware-Mechanismen und -Prozesse sind aktiv, werden gewartet und überwacht. (PCI-DSS-v4.0)	step-functions-state-machine-Protokollierung aktiviert	Stellen Sie sicher, dass auf der AWS Step Functions Functions-Maschine die Protokollierung aktiviert ist Die Regel ist NON_COMPLIANT, wenn für eine Zustandsmaschine die Protokollierung nicht aktiviert ist oder die Protokollierungskonfiguration nicht auf dem angegebenen Mindestniveau liegt.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
5.3.4	Anti-Malware-Mechanismen und -Prozesse sind aktiv, werden gewartet und überwacht. (PCI-DSS-v4.0)	netfw-logging-enabled	Stellen Sie sicher, dass die AWS Netzwerk-Firewall-Firewalls die Protokollierung aktiviert haben. Die Regel ist NON_COMPLIANT, wenn kein Protokollierungstyp konfiguriert ist. Sie können angeben, welchen Protokollierungstyp die Regel prüfen soll.
5.3.4	Anti-Malware-Mechanismen und -Prozesse sind aktiv, werden gewartet und überwacht. (PCI-DSS-v4.0)	cw-loggroup-retention-period-überprüfen	Stellen Sie sicher, dass ein CloudWatch LogGroup Amazon-Aufbewahrungszeitraum auf mehr als 365 Tage oder einen bestimmten Aufbewahrungszeitraum festgelegt ist. Die Regel lautet NON_COMPLIANT, wenn die Aufbewahrungsfrist weniger als MinRetentionTime, falls angegeben, oder andernfalls 365 Tage beträgt.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
6.3.3	Sicherheitslücken werden identifiziert und behoben. (PCI-DSS-v4.0)	lambda-function-settings-check	Stellen Sie sicher, dass die AWS Lambda-Funktionseinstellungen für Laufzeit, Rolle, Timeout und Speichergröße den erwarteten Werten entsprechen. Die Regel ignoriert Funktionen mit dem Pakettyp „Image“ und Funktionen, deren Laufzeit auf „Nur Betriebssystem-Laufzeit“ gesetzt ist. Die Regel ist NON_COMPLIANT, wenn die Einstellungen der Lambda-Funktion nicht den erwarteten Werten entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
6.3.3	Sicherheitslücken werden identifiziert und behoben. (PCI-DSS-v4.0)	eks-cluster-oldest-supported-Ausführung	Stellen Sie sicher, dass auf einem Amazon Elastic Kubernetes Service (EKS) -Cluster nicht die älteste unterstützte Version ausgeführt wird. Die Regel ist NON_COMPLIANT, wenn auf einem EKS-Cluster die älteste unterstützte Version (gleich dem Parameter oldestVersionSupported) ausgeführt wird.
6.4.1	Öffentliche Webanwendungen sind vor Angriffen geschützt. (PCI-DSS-v4.0)	appsync-associated-with-waf	Stellen Sie sicher, dass AWS AppSync APIs sie den AWS WAFv2 Web-Zugriffskontrolllisten () zugeordnet sind. ACLs Die Regel ist NON_COMPLIANT für eine AWS AppSync API, wenn sie keiner Web-ACL zugeordnet ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
6.4.1	Öffentliche Webanwendungen sind vor Angriffen geschützt. (PCI-DSS-v4.0)	WAF 2- webacl-not-empty	Stellen Sie sicher, dass eine WAFv2 Web-ACL alle WAF-Regeln oder WAF-Regelgruppen enthält. Diese Regel ist NON_COMPLIANT, wenn eine Web-ACL keine WAF-Regel n oder WAF-Regel gruppen enthält.
6.4.1	Öffentliche Webanwendungen sind vor Angriffen geschützt. (PCI-DSS-v4.0)	WAF 2- rulegroup-not-empty	Stellen Sie sicher, dass Regelgruppen Regeln enthalten. WAFv2 Die Regel ist NON_COMPLIANT, wenn eine WAFv2 Regelgruppe keine Regeln enthält.
6.4.2	Öffentliche Webanwendungen sind vor Angriffen geschützt. (PCI-DSS-v4.0)	appsync-associated-with-waf	Stellen Sie sicher, dass AWS AppSync APIs sie den AWS WAFv2 Web-Zugri ffskontrolllisten () zugeordnet sind. ACLs Die Regel ist NON_COMPL IANT für eine AWS AppSync API, wenn sie keiner Web-ACL zugeordnet ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
6.4.2	Öffentliche Webanwendungen sind vor Angriffen geschützt. (PCI-DSS-v4.0)	WAF 2- webacl-not-empty	Stellen Sie sicher, dass eine WAFv2 Web-ACL alle WAF-Regeln oder WAF-Regelgruppen enthält. Diese Regel ist NON_COMPLIANT, wenn eine Web-ACL keine WAF-Regel n oder WAF-Regel gruppen enthält.
6.4.2	Öffentliche Webanwendungen sind vor Angriffen geschützt. (PCI-DSS-v4.0)	WAF 2- rulegroup-not-empty	Stellen Sie sicher, dass Regelgruppen Regeln enthalten. WAFv2 Die Regel ist NON_COMPLIANT, wenn eine WAFv2 Regelgruppe keine Regeln enthält.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
6.5.5	Änderungen an allen Systemkom ponenten werden sicher verwaltet. (PCI-DSS-v4.0)	codedeploy-lambda-allatonce-traffic-shift-deaktiviert	Stellen Sie sicher, dass die Bereitste llungsgruppe für Lambda Compute Platform nicht die Standardbereitstel lungskonfiguration verwendet. Die Regel lautet NON_COMPL IANT, wenn die Bereitstellungsgruppe die Bereitstellungskon figuration 'verwende t. CodeDeployDefault LambdaAllAtOnce'.
6.5.6	Änderungen an allen Systemkom ponenten werden sicher verwaltet. (PCI-DSS-v4.0)	codedeploy-lambda-allatonce-traffic-shift-deaktiviert	Stellen Sie sicher, dass die Bereitste llungsgruppe für Lambda Compute Platform nicht die Standardbereitstel lungskonfiguration verwendet. Die Regel lautet NON_COMPL IANT, wenn die Bereitstellungsgruppe die Bereitstellungskon figuration 'verwende t. CodeDeployDefault LambdaAllAtOnce'.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
7.2.1	Der Zugriff auf Systemkomponenten und Daten ist angemessen definiert und zugewiesen. (PCI-DSS-v4.0)	s-3 bucket-blacklisted-actions-prohibited	Stellen Sie sicher, dass eine Bucket-Richtlinie von Amazon Simple Storage Service (Amazon S3) keine Aktionen auf Bucket- und Objektebene auf Blocklisten für Ressourcen im Bucket für Prinzipale anderer Konten zulässt. AWS Die Regel überprüft beispielsweise, ob die Amazon S3 S3-Bucket-Richtlinie einem anderen AWS Konto nicht erlaubt, s3: GetBucket *-Aktionen und s3: DeleteObject für ein Objekt im Bucket auszuführen. Die Regel ist NON_COMPLIANT, wenn gesperrte Aktionen gemäß der Bucket-Richtlinie von Amazon S3 zulässig sind.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
7.2.1	Der Zugriff auf Systemkomponenten und Daten ist entsprechend definiert und zugewiesen. (PCI-DSS-v4.0)	bucket-policy-not-mores3-permissiv	Stellen Sie sicher, dass Ihre Amazon Simple Storage Service (S3) -Bucket-Richtlinien keine anderen Kontobere chtigungen zulassen als die von Ihnen Amazon S3 S3-Bucket-Kontrollrichtlini e.
7.2.1	Der Zugriff auf Systemkomponenten und Daten ist entsprechend definiert und zugewiesen. (PCI-DSS-v4.0)	iam-policy-in-use	Stellen Sie sicher, dass ein IAM-Richt linien-ARN einem IAM-Benutzer oder einer Gruppe mit einem oder mehreren IAM-Benutzern oder einer IAM-Rolle mit einer oder mehreren vertrauenswürdigen Entitäten zugewiesen ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
7.2.1	Der Zugriff auf Systemkomponenten und Daten ist angemessen definiert und zugewiesen. (PCI-DSS-v4.0)	neptune-cluster-iam-database-Authentifizierung	Stellen Sie sicher, dass für einen Amazon Neptune Neptune-Cluster die AWS Identity and Access Management (IAM) -Datenbankauthentifizierung aktiviert ist. Die Regel ist NON_COMPLIANT, wenn für einen Amazon-Neptune-Cluster die IAM-Datenbankauthentifizierung nicht aktiviert ist.
7.2.1	Der Zugriff auf Systemkomponenten und Daten ist entsprechend definiert und zugewiesen. (PCI-DSS-v4.0)	ec2- instance-profile-attached	Stellen Sie sicher, dass an eine EC2 Instanz ein AWS Identity and Access Management (IAM) -Profil angehängt ist. Die Regel lautet NON_COMPLIANT, wenn der Instanz kein IAM-Profil angehängt ist. EC2

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
7.2.1	Der Zugriff auf Systemkomponenten und Daten ist entsprechend definiert und zugewiesen. (PCI-DSS-v4.0)	backup-recovery-point-manual-Löschen-deaktiviert	Stellen Sie sicher, dass an einen Backup-Tresor eine ressourcenbasierte Richtlinie angehängt ist, die das Löschen von Wiederherstellungspunkten verhindert. Die Regel lautet NON_COMPLIANT, wenn der Backup-Tresor keine ressourcenbasierten Richtlinien oder Richtlinien ohne eine geeignete „Deny“ -Anweisung (Anweisung mit den Berechtigungen backup:DeleteRecoveryPoint, backup: und backup:UpdateRecoveryPointLifecycle) hat. PutBackupVaultAccessPolicy

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
7.2.2	Der Zugriff auf Systemkomponenten und Daten ist entsprechend definiert und zugewiesen. (PCI-DSS-v4.0)	s-3 bucket-blacklisted-actions-prohibited	Stellen Sie sicher, dass eine Bucket-Richtlinie von Amazon Simple Storage Service (Amazon S3) keine Aktionen auf Bucket- und Objektebene auf Blocklisten für Ressourcen im Bucket für Prinzipale anderer Konten zulässt. AWS Die Regel überprüft beispielsweise, ob die Amazon S3 S3-Bucket-Richtlinie einem anderen AWS Konto nicht erlaubt, s3: GetBucket *-Aktionen und s3: DeleteObject für ein Objekt im Bucket auszuführen. Die Regel ist NON_COMPLIANT, wenn gesperrte Aktionen gemäß der Bucket-Richtlinie von Amazon S3 zulässig sind.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
7.2.2	Der Zugriff auf Systemkomponenten und Daten ist entsprechend definiert und zugewiesen. (PCI-DSS-v4.0)	bucket-policy-not-mores3-permissiv	Stellen Sie sicher, dass Ihre Amazon Simple Storage Service (S3) -Bucket-Richtlinien keine anderen Kontobere chtigungen zulassen als die von Ihnen Amazon S3 S3-Bucket-Kontrollrichtlini e.
7.2.2	Der Zugriff auf Systemkomponenten und Daten ist entsprechend definiert und zugewiesen. (PCI-DSS-v4.0)	iam-policy-in-use	Stellen Sie sicher, dass ein IAM-Richt linien-ARN einem IAM-Benutzer oder einer Gruppe mit einem oder mehreren IAM-Benutzern oder einer IAM-Rolle mit einer oder mehreren vertrauenswürdigen Entitäten zugewiesen ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
7.2.2	Der Zugriff auf Systemkomponenten und Daten ist angemessen definiert und zugewiesen. (PCI-DSS-v4.0)	neptune-cluster-iam-database-Authentifizierung	Stellen Sie sicher, dass für einen Amazon Neptune Neptune-Cluster die AWS Identity and Access Management (IAM) -Datenbankauthentifizierung aktiviert ist. Die Regel ist NON_COMPLIANT, wenn für einen Amazon-Neptune-Cluster die IAM-Datenbankauthentifizierung nicht aktiviert ist.
7.2.2	Der Zugriff auf Systemkomponenten und Daten ist entsprechend definiert und zugewiesen. (PCI-DSS-v4.0)	ec2- instance-profile-attached	Stellen Sie sicher, dass an eine EC2 Instanz ein AWS Identity and Access Management (IAM) -Profil angehängt ist. Die Regel lautet NON_COMPLIANT, wenn der Instanz kein IAM-Profil angehängt ist. EC2

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
7.2.2	Der Zugriff auf Systemkomponenten und Daten ist entsprechend definiert und zugewiesen. (PCI-DSS-v4.0)	backup-recovery-point-manual-Löschen-deaktiviert	Stellen Sie sicher, dass an einen Backup-Tresor eine ressourcenbasierte Richtlinie angehängt ist, die das Löschen von Wiederherstellungspunkten verhindert. Die Regel lautet NON_COMPLIANT, wenn der Backup-Tresor keine ressourcenbasierten Richtlinien oder Richtlinien ohne eine geeignete „Deny“ -Anweisung (Anweisung mit den Berechtigungen backup:DeleteRecoveryPoint, backup: und backup:UpdateRecoveryPointLifecycle) hat. PutBackupVaultAccessPolicy

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
7.2.4	Der Zugriff auf Systemkomponenten und Daten ist entsprechend definiert und zugewiesen. (PCI-DSS-v4.0)	secretsmanager-secret-unused	Stellen Sie sicher, dass auf AWS Secrets Manager-Geheimnisse innerhalb einer bestimmten Anzahl von Tagen zugegriffen wurde. Die Regel lautet NON_COMPLIANT, wenn innerhalb von 'unusedForDays' Tagen nicht auf ein Geheimnis zugegriffen wurde. Der Standardwert lautet 90 Tage.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
7.2.5	Der Zugriff auf Systemkomponenten und Daten ist entsprechend definiert und zugewiesen. (PCI-DSS-v4.0)	s-3 bucket-blacklisted-actions-prohibited	Stellen Sie sicher, dass eine Bucket-Richtlinie von Amazon Simple Storage Service (Amazon S3) keine Aktionen auf Bucket- und Objektebene auf Blocklisten für Ressourcen im Bucket für Prinzipale anderer Konten zulässt. AWS Die Regel überprüft beispielsweise, ob die Amazon S3 S3-Bucket-Richtlinie einem anderen AWS Konto nicht erlaubt, s3: GetBucket *-Aktionen und s3: DeleteObject für ein Objekt im Bucket auszuführen. Die Regel ist NON_COMPLIANT, wenn gesperrte Aktionen gemäß der Bucket-Richtlinie von Amazon S3 zulässig sind.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
7.2.5	Der Zugriff auf Systemkomponenten und Daten ist entsprechend definiert und zugewiesen. (PCI-DSS-v4.0)	bucket-policy-not-mores3-permissiv	Stellen Sie sicher, dass Ihre Amazon Simple Storage Service (S3) -Bucket-Richtlinien keine anderen Kontobere chtigungen zulassen als die von Ihnen Amazon S3 S3-Bucket-Kontrollrichtlini e.
7.2.5	Der Zugriff auf Systemkomponenten und Daten ist entsprechend definiert und zugewiesen. (PCI-DSS-v4.0)	iam-policy-in-use	Stellen Sie sicher, dass ein IAM-Richt linien-ARN einem IAM-Benutzer oder einer Gruppe mit einem oder mehreren IAM-Benutzern oder einer IAM-Rolle mit einer oder mehreren vertrauenswürdigen Entitäten zugewiesen ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
7.2.5	Der Zugriff auf Systemkomponenten und Daten ist angemessen definiert und zugewiesen. (PCI-DSS-v4.0)	neptune-cluster-iam-database-Authentifizierung	Stellen Sie sicher, dass für einen Amazon Neptune Neptune-Cluster die AWS Identity and Access Management (IAM) -Datenbankauthentifizierung aktiviert ist. Die Regel ist NON_COMPLIANT, wenn für einen Amazon-Neptune-Cluster die IAM-Datenbankauthentifizierung nicht aktiviert ist.
7.2.5	Der Zugriff auf Systemkomponenten und Daten ist entsprechend definiert und zugewiesen. (PCI-DSS-v4.0)	ec2- instance-profile-attached	Stellen Sie sicher, dass an eine EC2 Instanz ein AWS Identity and Access Management (IAM) -Profil angehängt ist. Die Regel lautet NON_COMPLIANT, wenn der Instanz kein IAM-Profil angehängt ist. EC2

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
7.2.5	Der Zugriff auf Systemkomponenten und Daten ist entsprechend definiert und zugewiesen. (PCI-DSS-v4.0)	backup-recovery-point-manual-Löschen-deaktiviert	Stellen Sie sicher, dass an einen Backup-Tresor eine ressourcenbasierte Richtlinie angehängt ist, die das Löschen von Wiederherstellungspunkten verhindert. Die Regel lautet NON_COMPLIANT, wenn der Backup-Tresor keine ressourcenbasierten Richtlinien oder Richtlinien ohne eine geeignete „Deny“ -Anweisung (Anweisung mit den Berechtigungen backup:DeleteRecoveryPoint, backup: und backup:UpdateRecoveryPointLifecycle) hat. PutBackupVaultAccessPolicy

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
7.2.5.1	Der Zugriff auf Systemkomponenten und Daten ist entsprechend definiert und zugewiesen. (PCI-DSS-v4.0)	secretsmanager-secret-unused	Stellen Sie sicher, dass auf AWS Secrets Manager-Geheimnisse innerhalb einer bestimmten Anzahl von Tagen zugegriffen wurde. Die Regel lautet NON_COMPLIANT, wenn innerhalb von 'unusedForDays' Tagen nicht auf ein Geheimnis zugegriffen wurde. Der Standardwert lautet 90 Tage.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
7.2.6	Der Zugriff auf Systemkomponenten und Daten ist angemessen definiert und zugewiesen. (PCI-DSS-v4.0)	s-3 bucket-blacklisted-actions-prohibited	Stellen Sie sicher, dass eine Bucket-Richtlinie von Amazon Simple Storage Service (Amazon S3) keine Aktionen auf Bucket- und Objektebene auf Blocklisten für Ressourcen im Bucket für Prinzipale anderer Konten zulässt. AWS Die Regel überprüft beispielsweise, ob die Amazon S3 S3-Bucket-Richtlinie einem anderen AWS Konto nicht erlaubt, s3: GetBucket *-Aktionen und s3: DeleteObject für ein Objekt im Bucket auszuführen. Die Regel ist NON_COMPLIANT, wenn gesperrte Aktionen gemäß der Bucket-Richtlinie von Amazon S3 zulässig sind.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
7.2.6	Der Zugriff auf Systemkomponenten und Daten ist angemessen definiert und zugewiesen. (PCI-DSS-v4.0)	bucket-policy-not-mores3-permissiv	Stellen Sie sicher, dass Ihre Amazon Simple Storage Service (S3) -Bucket-Richtlinien keine anderen Kontobere chtigungen zulassen als die von Ihnen Amazon S3 S3-Bucket-Kontrollrichtlini e.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
7.3.1	Der Zugriff auf Systemkomponenten und Daten wird über ein oder mehrere Zugriffskontrollsysteme verwaltet. (PCI-DSS-v4.0)	s-3 bucket-blacklisted-actions-prohibited	Stellen Sie sicher, dass eine Bucket-Richtlinie von Amazon Simple Storage Service (Amazon S3) keine Aktionen auf Bucket- und Objektebene auf Blocklisten für Ressourcen im Bucket für Prinzipale anderer Konten zulässt. AWS Die Regel überprüft beispielsweise, ob die Amazon S3 S3-Bucket-Richtlinie einem anderen AWS Konto nicht erlaubt, s3: GetBucket *-Aktionen und s3: DeleteObject für ein Objekt im Bucket auszuführen. Die Regel ist NON_COMPLIANT, wenn gesperrte Aktionen gemäß der Bucket-Richtlinie von Amazon S3 zulässig sind.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
7.3.1	Der Zugriff auf Systemkomponenten und Daten wird über ein oder mehrere Zugriffskontrollsy steme verwaltet. (PCI-DSS-v4.0)	bucket-policy-not-mores3-permissiv	Stellen Sie sicher, dass Ihre Amazon Simple Storage Service (S3) -Bucket-Richtlinien keine anderen Kontobere chtigungen zulassen als die von Ihnen Amazon S3 S3-Bucket-Kontrollrichtlini e.
7.3.1	Der Zugriff auf Systemkomponenten und Daten wird über ein oder mehrere Zugriffskontrollsy steme verwaltet. (PCI-DSS-v4.0)	iam-policy-in-use	Stellen Sie sicher, dass ein IAM-Richt linien-ARN einem IAM-Benutzer oder einer Gruppe mit einem oder mehreren IAM-Benutzern oder einer IAM-Rolle mit einer oder mehreren vertrauenswürdigen Entitäten zugewiesen ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
7.3.1	Der Zugriff auf Systemkomponenten und Daten wird über ein oder mehrere Zugriffskontrollsysteme verwaltet. (PCI-DSS-v4.0)	neptune-cluster-iam-database-Authentifizierung	Stellen Sie sicher, dass für einen Amazon Neptune Neptune-Cluster die AWS Identity and Access Management (IAM) -Datenbankauthentifizierung aktiviert ist. Die Regel ist NON_COMPLIANT, wenn für einen Amazon-Neptune-Cluster die IAM-Datenbankauthentifizierung nicht aktiviert ist.
7.3.1	Der Zugriff auf Systemkomponenten und Daten wird über ein oder mehrere Zugriffskontrollsysteme verwaltet. (PCI-DSS-v4.0)	ec2- instance-profile-attached	Stellen Sie sicher, dass an eine EC2 Instanz ein AWS Identity and Access Management (IAM) -Profil angehängt ist. Die Regel lautet NON_COMPLIANT, wenn der Instanz kein IAM-Profil angehängt ist. EC2

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
7.3.1	Der Zugriff auf Systemkomponenten und Daten wird über ein oder mehrere Zugriffskontrollsysteme verwaltet. (PCI-DSS-v4.0)	backup-recovery-point-manual-Löschen-deaktiviert	Stellen Sie sicher, dass an einen Backup-Tresor eine ressourcenbasierte Richtlinie angehängt ist, die das Löschen von Wiederherstellungspunkten verhindert. Die Regel lautet NON_COMPLIANT, wenn der Backup-Tresor keine ressourcenbasierten Richtlinien oder Richtlinien ohne eine geeignete „Deny“ -Anweisung (Anweisung mit den Berechtigungen backup:DeleteRecoveryPoint, backup: und backup:UpdateRecoveryPointLifecycle) hat. PutBackupVaultAccessPolicy

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
7.3.2	Der Zugriff auf Systemkomponenten und Daten wird über ein oder mehrere Zugriffskontrollsysteme verwaltet. (PCI-DSS-v4.0)	s-3 bucket-blacklisted-actions-prohibited	Stellen Sie sicher, dass eine Bucket-Richtlinie von Amazon Simple Storage Service (Amazon S3) keine Aktionen auf Bucket- und Objektebene auf Blocklisten für Ressourcen im Bucket für Prinzipale anderer Konten zulässt. AWS Die Regel überprüft beispielsweise, ob die Amazon S3 S3-Bucket-Richtlinie einem anderen AWS Konto nicht erlaubt, s3: GetBucket *-Aktionen und s3: DeleteObject für ein Objekt im Bucket auszuführen. Die Regel ist NON_COMPLIANT, wenn gesperrte Aktionen gemäß der Bucket-Richtlinie von Amazon S3 zulässig sind.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
7.3.2	Der Zugriff auf Systemkomponenten und Daten wird über ein oder mehrere Zugriffskontrollsy steme verwaltet. (PCI-DSS-v4.0)	bucket-policy-not-mores3-permissiv	Stellen Sie sicher, dass Ihre Amazon Simple Storage Service (S3) -Bucket-Richtlinien keine anderen Kontobere chtigungen zulassen als die von Ihnen Amazon S3 S3-Bucket-Kontrollrichtlini e.
7.3.2	Der Zugriff auf Systemkomponenten und Daten wird über ein oder mehrere Zugriffskontrollsy steme verwaltet. (PCI-DSS-v4.0)	iam-policy-in-use	Stellen Sie sicher, dass ein IAM-Richt linien-ARN einem IAM-Benutzer oder einer Gruppe mit einem oder mehreren IAM-Benutzern oder einer IAM-Rolle mit einer oder mehreren vertrauenswürdigen Entitäten zugewiesen ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
7.3.2	Der Zugriff auf Systemkomponenten und Daten wird über ein oder mehrere Zugriffskontrollsysteme verwaltet. (PCI-DSS-v4.0)	neptune-cluster-iam-database-Authentifizierung	Stellen Sie sicher, dass für einen Amazon Neptune Neptune-Cluster die AWS Identity and Access Management (IAM) -Datenbankauthentifizierung aktiviert ist. Die Regel ist NON_COMPLIANT, wenn für einen Amazon-Neptune-Cluster die IAM-Datenbankauthentifizierung nicht aktiviert ist.
7.3.2	Der Zugriff auf Systemkomponenten und Daten wird über ein oder mehrere Zugriffskontrollsysteme verwaltet. (PCI-DSS-v4.0)	ec2- instance-profile-attached	Stellen Sie sicher, dass an eine EC2 Instanz ein AWS Identity and Access Management (IAM) -Profil angehängt ist. Die Regel lautet NON_COMPLIANT, wenn der Instanz kein IAM-Profil angehängt ist. EC2

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
7.3.2	Der Zugriff auf Systemkomponenten und Daten wird über ein oder mehrere Zugriffskontrollsysteme verwaltet. (PCI-DSS-v4.0)	backup-recovery-point-manual-Löschen-deaktiviert	Stellen Sie sicher, dass an einen Backup-Tresor eine ressourcenbasierte Richtlinie angehängt ist, die das Löschen von Wiederherstellungspunkten verhindert. Die Regel lautet NON_COMPLIANT, wenn der Backup-Tresor keine ressourcenbasierten Richtlinien oder Richtlinien ohne eine geeignete „Deny“ -Anweisung (Anweisung mit den Berechtigungen backup:DeleteRecoveryPoint, backup: und backup:UpdateRecoveryPointLifecycle) hat. PutBackupVaultAccessPolicy

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
7.3.3	Der Zugriff auf Systemkomponenten und Daten wird über ein oder mehrere Zugangskontrollsys teme verwaltet. (PCI-DSS-v4.0)	s-3 bucket-blacklisted-actions-prohibited	Stellen Sie sicher, dass eine Bucket-Richtlinie von Amazon Simple Storage Service (Amazon S3) keine Aktionen auf Bucket- und Objektebene auf Blocklisten für Ressourcen im Bucket für Prinzipale anderer Konten zulässt. AWS Die Regel überprüft beispielsweise, ob die Amazon S3 S3-Bucket-Richtlinie einem anderen AWS Konto nicht erlaubt, s3: GetBucket *-Aktionen und s3: DeleteObject für ein Objekt im Bucket auszuführen. Die Regel ist NON_COMPLIANT, wenn gesperrte Aktionen gemäß der Bucket-Richtlinie von Amazon S3 zulässig sind.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
7.3.3	Der Zugriff auf Systemkomponenten und Daten wird über ein oder mehrere Zugangskontrollsys teme verwaltet. (PCI-DSS-v4.0)	bucket-policy-not-mores3-permissiv	Stellen Sie sicher, dass Ihre Amazon Simple Storage Service (S3) -Bucket-Richtlinien keine anderen Kontobere chtigungen zulassen als die von Ihnen Amazon S3 S3-Bucket-Kontrollrichtlini e.
7.3.3	Der Zugriff auf Systemkomponenten und Daten wird über ein oder mehrere Zugangskontrollsys teme verwaltet. (PCI-DSS-v4.0)	iam-policy-in-use	Stellen Sie sicher, dass ein IAM-Richt linien-ARN einem IAM-Benutzer oder einer Gruppe mit einem oder mehreren IAM-Benutzern oder einer IAM-Rolle mit einer oder mehreren vertrauenswürdigen Entitäten zugewiesen ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
7.3.3	Der Zugriff auf Systemkomponenten und Daten wird über ein oder mehrere Zugangskontrollsysteme verwaltet. (PCI-DSS-v4.0)	neptune-cluster-iam-database-Authentifizierung	Stellen Sie sicher, dass für einen Amazon Neptune Neptune-Cluster die AWS Identity and Access Management (IAM) -Datenbankauthentifizierung aktiviert ist. Die Regel ist NON_COMPLIANT, wenn für einen Amazon-Neptune-Cluster die IAM-Datenbankauthentifizierung nicht aktiviert ist.
7.3.3	Der Zugriff auf Systemkomponenten und Daten wird über ein oder mehrere Zugangskontrollsysteme verwaltet. (PCI-DSS-v4.0)	ec2- instance-profile-attached	Stellen Sie sicher, dass an eine EC2 Instanz ein AWS Identity and Access Management (IAM) -Profil angehängt ist. Die Regel lautet NON_COMPLIANT, wenn der Instanz kein IAM-Profil angehängt ist. EC2

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
7.3.3	Der Zugriff auf Systemkomponenten und Daten wird über ein oder mehrere Zugangskontrollsysteme verwaltet. (PCI-DSS-v4.0)	backup-recovery-point-manual-Löschen-deaktiviert	Stellen Sie sicher, dass an einen Backup-Tresor eine ressourcenbasierte Richtlinie angehängt ist, die das Löschen von Wiederherstellungspunkten verhindert. Die Regel lautet NON_COMPLIANT, wenn der Backup-Tresor keine ressourcenbasierten Richtlinien oder Richtlinien ohne eine geeignete „Deny“ -Anweisung (Anweisung mit den Berechtigungen backup:DeleteRecoveryPoint, backup: und backup:UpdateRecoveryPointLifecycle) hat. PutBackupVaultAccessPolicy

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
8.2.1	Die Benutzeri dentifikation und die zugehörigen Konten für Benutzer und Administratoren werden während des gesamten Lebenszyk lus eines Kontos streng verwaltet. (PCI-DSS-v4.0)	iam-policy-in-use	Stellen Sie sicher, dass ein IAM-Richt linien-ARN einem IAM-Benutzer oder einer Gruppe mit einem oder mehreren IAM-Benutzern oder einer IAM-Rolle mit einer oder mehreren vertrauenswürdigen Entitäten zugewiesen ist.
8.2.1	Die Benutzeri dentifikation und die zugehörigen Konten für Benutzer und Administratoren werden während des gesamten Kontolebe nszyklus streng verwaltet. (PCI-DSS-v4.0)	ec2- no-amazon-key-pair	Stellen Sie sicher, dass laufende Amazon Elastic Compute Cloud (EC2) -Instances nicht mit Amazon-Schlüsselpaaren gestartet werden. Die Regel lautet NON_COMPLIANT, wenn eine laufende EC2 Instance mit einem key pair gestartet wird.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
8.2.2	Die Benutzeri dentifikation und die zugehörigen Konten für Benutzer und Administratoren werden während des gesamten Lebenszyk lus eines Kontos streng verwaltet. (PCI-DSS-v4.0)	iam-policy-in-use	Stellen Sie sicher, dass ein IAM-Richt linien-ARN einem IAM-Benutzer oder einer Gruppe mit einem oder mehreren IAM-Benutzern oder einer IAM-Rolle mit einer oder mehreren vertrauenswürdigen Entitäten zugewiesen ist.
8.2.2	Die Benutzeri dentifikation und die zugehörigen Konten für Benutzer und Administratoren werden während des gesamten Lebenszyk lus eines Kontos streng verwaltet. (PCI-DSS-v4.0)	ec2- no-amazon-key-pair	Stellen Sie sicher, dass laufende Amazon Elastic Compute Cloud (EC2) -Instances nicht mit Amazon-Schlüsselpaaren gestartet werden. Die Regel lautet NON_COMPLIANT, wenn eine laufende EC2 Instance mit einem key pair gestartet wird.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
8.2.2	Die Benutzeri dentifikation und die zugehörigen Konten für Benutzer und Administratoren werden während des gesamten Lebenszyk lus eines Kontos streng verwaltet. (PCI-DSS-v4.0)	codebuild-project-envvar-awscred-überprüfen	Stellen Sie sicher, dass das Projekt KEINE Umgebungs variablen und _ACCESS_KEY enthält. AWS_ACCES S_KEY_ID AWS_SECRE T Die Regel ist NON_COMPLIANT, wenn die Projekt-U mgebungsvariablen Klartext-Anmeldein formationen enthalten.
8.2.2	Die Benutzeri dentifikation und die zugehörigen Konten für Benutzer und Administratoren werden während des gesamten Lebenszyk lus eines Kontos streng verwaltet. (PCI-DSS-v4.0)	secretsmanager-scheduled-rotation-success-überprüfen	Stellen Sie sicher, dass AWS Secrets Manager-Geheimniss e gemäß dem Rotationsplan erfolgreich rotiert wurden. Secrets Manager berechnet das Datum, an dem die Rotation stattfind en soll. Die Regel ist NON_COMPLIANT, wenn das Datum verstrichen ist und das Secret nicht rotiert wurde.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
8.2.2	Die Benutzeri dentifikation und die zugehörigen Konten für Benutzer und Administratoren werden während des gesamten Lebenszyk lus eines Kontos streng verwaltet. (PCI-DSS-v4.0)	secretsmanager-sec ret-periodic-rotation	Stellen Sie sicher, dass AWS Secrets Manager-Geheimniss e in der letzten angegebenen Anzahl von Tagen rotiert wurden. Die Regel lautet NON_COMPL IANT, wenn ein Secret länger als die Anzahl der maxDaysSince Rotationstage nicht gewechselt wurde. Der Standardwert lautet 90 Tage.
8.2.2	Die Benutzeri dentifikation und die zugehörigen Konten für Benutzer und Administratoren werden während des gesamten Lebenszyk lus eines Kontos streng verwaltet. (PCI-DSS-v4.0)	secretsmanager-sec ret-unused	Stellen Sie sicher, dass auf AWS Secrets Manager-G eheimnisse innerhalb einer bestimmten Anzahl von Tagen zugegriffen wurde. Die Regel lautet NON_COMPLIANT, wenn innerhalb von 'unusedForDays' Tagen nicht auf ein Geheimnis zugegriff en wurde. Der Standardwert lautet 90 Tage.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
8.2.4	Die Benutzeri dentifikation und die zugehörigen Konten für Benutzer und Administratoren werden während des gesamten Lebenszyk lus eines Kontos streng verwaltet. (PCI-DSS-v4.0)	iam-policy-in-use	Stellen Sie sicher, dass ein IAM-Richt linien-ARN einem IAM-Benutzer oder einer Gruppe mit einem oder mehreren IAM-Benutzern oder einer IAM-Rolle mit einer oder mehreren vertrauenswürdigen Entitäten zugewiesen ist.
8.2.4	Die Benutzeri dentifikation und die zugehörigen Konten für Benutzer und Administratoren werden während des gesamten Kontolebe nszyklus streng verwaltet. (PCI-DSS-v4.0)	ec2- no-amazon-key-pair	Stellen Sie sicher, dass laufende Amazon Elastic Compute Cloud (EC2) -Instances nicht mit Amazon-Schlüsselpaaren gestartet werden. Die Regel lautet NON_COMPLIANT, wenn eine laufende EC2 Instance mit einem key pair gestartet wird.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
8.2.5	Die Benutzeri dentifikation und die zugehörigen Konten für Benutzer und Administratoren werden während des gesamten Lebenszyk lus eines Kontos streng verwaltet. (PCI-DSS-v4.0)	iam-policy-in-use	Stellen Sie sicher, dass ein IAM-Richt linien-ARN einem IAM-Benutzer oder einer Gruppe mit einem oder mehreren IAM-Benutzern oder einer IAM-Rolle mit einer oder mehreren vertrauenswürdigen Entitäten zugewiesen ist.
8.2.5	Die Benutzeri dentifikation und die zugehörigen Konten für Benutzer und Administratoren werden während des gesamten Kontolebe nszyklus streng verwaltet. (PCI-DSS-v4.0)	ec2- no-amazon-key-pair	Stellen Sie sicher, dass laufende Amazon Elastic Compute Cloud (EC2) -Instances nicht mit Amazon-Schlüsselpaaren gestartet werden. Die Regel lautet NON_COMPLIANT, wenn eine laufende EC2 Instance mit einem key pair gestartet wird.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
8.2.6	Die Benutzeri dentifikation und die zugehörigen Konten für Benutzer und Administratoren werden während des gesamten Lebenszyk lus eines Kontos streng verwaltet. (PCI-DSS-v4.0)	secretsmanager-sec ret-unused	Stellen Sie sicher, dass auf AWS Secrets Manager-G eheimnisse innerhalb einer bestimmten Anzahl von Tagen zugegriffen wurde. Die Regel lautet NON_COMPLIANT, wenn innerhalb von 'unusedForDays' Tagen nicht auf ein Geheimnis zugegriff en wurde. Der Standardwert lautet 90 Tage.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
8.2.7	Die Benutzeri dentifikation und die zugehörigen Konten für Benutzer und Administratoren werden während des gesamten Lebenszyk lus eines Kontos streng verwaltet. (PCI-DSS-v4.0)	s-3 bucket-blacklisted-actions-prohibited	Stellen Sie sicher, dass eine Bucket-Ri chtlinie von Amazon Simple Storage Service (Amazon S3) keine Aktionen auf Bucket- und Objektebene auf Blocklisten für Ressourcen im Bucket für Prinzipal e anderer Konten zulässt. AWS Die Regel überprüft beispielsweise, ob die Amazon S3 S3-Bucket-Richtlin ie einem anderen AWS Konto nicht erlaubt, s3: GetBucket *-Aktionen und s3: DeleteObject für ein Objekt im Bucket auszuführ en. Die Regel ist NON_COMPLIANT, wenn gesperrte Aktionen gemäß der Bucket-Richtlinie von Amazon S3 zulässig sind.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
8.2.7	Die Benutzeri dentifikation und die zugehörigen Konten für Benutzer und Administratoren werden während des gesamten Lebenszyk lus eines Kontos streng verwaltet. (PCI-DSS-v4.0)	bucket-policy-not-mores3-permissiv	Stellen Sie sicher, dass Ihre Amazon Simple Storage Service (S3) -Bucket-Richtlinien keine anderen Kontobere chtigungen zulassen als die von Ihnen Amazon S3 S3-Bucket-Kontrollrichtlini e.
8.2.7	Die Benutzeri dentifikation und die zugehörigen Konten für Benutzer und Administratoren werden während des gesamten Kontolebe nszyklus strikt verwaltet. (PCI-DSS-v4.0)	iam-policy-in-use	Stellen Sie sicher, dass ein IAM-Richt linien-ARN einem IAM-Benutzer oder einer Gruppe mit einem oder mehreren IAM-Benutzern oder einer IAM-Rolle mit einer oder mehreren vertrauenswürdigen Entitäten zugewiesen ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
8.2.7	Die Benutzeri dentifikation und die zugehörigen Konten für Benutzer und Administratoren werden während des gesamten Kontolebe nszyklus streng verwaltet. (PCI-DSS-v4.0)	neptune-cluster-ia m-database-Authent ifizierung	Stellen Sie sicher, dass für einen Amazon Neptune Neptune-Cluster die AWS Identity and Access Managemen t (IAM) -Datenban kauthentifizierung aktiviert ist. Die Regel ist NON_COMPL IANT, wenn für einen Amazon-Neptune-Clu ster die IAM-Daten bankauthentifizierung nicht aktiviert ist.
8.2.7	Die Benutzeri dentifikation und die zugehörigen Konten für Benutzer und Administratoren werden während des gesamten Kontolebe nszyklus streng verwaltet. (PCI-DSS-v4.0)	ec2- instance-profile-a ttached	Stellen Sie sicher, dass an eine EC2 Instanz ein AWS Identity and Access Management (IAM) -Profil angehängt ist. Die Regel lautet NON_COMPLIANT, wenn der Instanz kein IAM-Profil angehängt ist. EC2

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
8.2.7	Die Benutzeridentifikation und die zugehörigen Konten für Benutzer und Administratoren werden während des gesamten Kontolebenszyklus strikt verwaltet. (PCI-DSS-v4.0)	backup-recovery-point-manual-Löschen-deaktiviert	Stellen Sie sicher, dass an einen Backup-Tresor eine ressourcenbasierte Richtlinie angehängt ist, die das Löschen von Wiederherstellungspunkten verhindert. Die Regel lautet NON_COMPLIANT, wenn der Backup-Tresor keine ressourcenbasierten Richtlinien oder Richtlinien ohne eine geeignete „Deny“ -Anweisung (Anweisung mit den Berechtigungen backup:DeleteRecoveryPoint, backup: und backup:UpdateRecoveryPointLifecycle) hat. PutBackupVaultAccessPolicy

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
8.2.8	Die Benutzeri dentifikation und die zugehörigen Konten für Benutzer und Administratoren werden während des gesamten Lebenszyk lus eines Kontos streng verwaltet. (PCI-DSS-v4.0)	s-3 bucket-blacklisted-actions-prohibited	Stellen Sie sicher, dass eine Bucket-Ri chtlinie von Amazon Simple Storage Service (Amazon S3) keine Aktionen auf Bucket- und Objektebene auf Blocklisten für Ressourcen im Bucket für Prinzipal e anderer Konten zulässt. AWS Die Regel überprüft beispielsweise, ob die Amazon S3 S3-Bucket-Richtlin ie einem anderen AWS Konto nicht erlaubt, s3: GetBucket *-Aktionen und s3: DeleteObject für ein Objekt im Bucket auszuführ en. Die Regel ist NON_COMPLIANT, wenn gesperrte Aktionen gemäß der Bucket-Richtlinie von Amazon S3 zulässig sind.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
8.2.8	Die Benutzeri dentifikation und die zugehörigen Konten für Benutzer und Administratoren werden während des gesamten Lebenszyk lus eines Kontos streng verwaltet. (PCI-DSS-v4.0)	bucket-policy-not-mores3-permissiv	Stellen Sie sicher, dass Ihre Amazon Simple Storage Service (S3) -Bucket-Richtlinien keine anderen Kontobere chtigungen zulassen als die von Ihnen Amazon S3 S3-Bucket-Kontrollrichtlini e.
8.2.8	Die Benutzeri dentifikation und die zugehörigen Konten für Benutzer und Administratoren werden während des gesamten Lebenszyk lus eines Kontos streng verwaltet. (PCI-DSS-v4.0)	iam-policy-in-use	Stellen Sie sicher, dass ein IAM-Richt linien-ARN einem IAM-Benutzer oder einer Gruppe mit einem oder mehreren IAM-Benutzern oder einer IAM-Rolle mit einer oder mehreren vertrauenswürdigen Entitäten zugewiesen ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
8.2.8	Die Benutzeri dentifikation und die zugehörigen Konten für Benutzer und Administratoren werden während des gesamten Lebenszyk lus eines Kontos streng verwaltet. (PCI-DSS-v4.0)	neptune-cluster-ia m-database-Authent ifizierung	Stellen Sie sicher, dass für einen Amazon Neptune Neptune-Cluster die AWS Identity and Access Managemen t (IAM) -Datenban kauthentifizierung aktiviert ist. Die Regel ist NON_COMPL IANT, wenn für einen Amazon-Neptune-Clu ster die IAM-Daten bankauthentifizierung nicht aktiviert ist.
8.2.8	Die Benutzeri dentifikation und die zugehörigen Konten für Benutzer und Administratoren werden während des gesamten Lebenszyk lus eines Kontos streng verwaltet. (PCI-DSS-v4.0)	ec2-imdsv2-check	Stellen Sie sicher, dass die Metadaten version Ihrer Amazon Elastic Compute Cloud (Amazon EC2) -Instance mit Instance Metadata Service Version 2 (IMDSv2) konfiguri ert ist. Die Regel lautet NON_COMPL IANT, wenn sie auf HttpTokens optional gesetzt ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
8.2.8	Die Benutzeri dentifikation und die zugehörigen Konten für Benutzer und Administratoren werden während des gesamten Lebenszyk lus eines Kontos streng verwaltet. (PCI-DSS-v4.0)	ec2- instance-profile-a ttached	Stellen Sie sicher, dass an eine EC2 Instanz ein AWS Identity and Access Management (IAM) -Profil angehängt ist. Die Regel lautet NON_COMPLIANT, wenn der Instanz kein IAM-Profil angehängt ist. EC2
8.2.8	Die Benutzeri dentifikation und die zugehörigen Konten für Benutzer und Administratoren werden während des gesamten Lebenszyk lus eines Kontos streng verwaltet. (PCI-DSS-v4.0)	autoscaling-launch config-requires-im dsv2	Stellen Sie sicher, dass nur aktiviert ist. IMDSv2 Diese Regel ist NON_COMPL IANT, wenn die Metadaten-Version nicht in der Startkonf iguration enthalten ist oder sowohl Metadaten V1 als auch V2 aktiviert sind.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
8.2.8	Die Benutzeridentifikation und die zugehörigen Konten für Benutzer und Administratoren werden während des gesamten Lebenszyklus eines Kontos streng verwaltet. (PCI-DSS-v4.0)	backup-recovery-point-manual-Löschen-deaktiviert	Stellen Sie sicher, dass an einen Backup-Tresor eine ressourcenbasierte Richtlinie angehängt ist, die das Löschen von Wiederherstellungspunkten verhindert. Die Regel lautet NON_COMPLIANT, wenn der Backup-Tresor keine ressourcenbasierten Richtlinien oder Richtlinien ohne eine geeignete „Deny“ -Anweisung (Anweisung mit den Berechtigungen backup:DeleteRecoveryPoint, backup: und backup:UpdateRecoveryPointLifecycle) hat. PutBackupVaultAccessPolicy

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
8.3.10.1	Eine starke Authentifizierung für Benutzer und Administratoren wird eingerichtet und verwaltet. (PCI-DSS-v4.0)	access-keys-rotated	Stellen Sie sicher, dass aktive IAM-Zugriffsschlüssel innerhalb der unter Alter angegebenen Anzahl von Tagen rotiert (geändert) werden. maxAccessKey Die Regel ist NON_COMPLIANT, wenn die Zugriffsschlüssel nicht innerhalb des angegebenen Zeitraums rotiert werden. Der Standardwert lautet 90 Tage.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
8.3.10.1	Eine starke Authentifizierung für Benutzer und Administratoren wird eingerichtet und verwaltet. (PCI-DSS-v4.0)	secretsmanager-scheduled-rotation-success-überprüfen	Stellen Sie sicher, dass AWS Secrets Manager-Geheimnisse gemäß dem Rotationsplan erfolgreich rotiert wurden. Secrets Manager berechnet das Datum, an dem die Rotation stattfinden soll. Die Regel ist NON_COMPLIANT, wenn das Datum verstrichen ist und das Secret nicht rotiert wurde.
8.3.10.1	Eine starke Authentifizierung für Benutzer und Administratoren wird eingerichtet und verwaltet. (PCI-DSS-v4.0)	secretsmanager-secret-periodic-rotation	Stellen Sie sicher, dass AWS Secrets Manager-Geheimnisse in der letzten angegebenen Anzahl von Tagen rotiert wurden. Die Regel lautet NON_COMPLIANT, wenn ein Secret länger als die Anzahl der maxDaysSince Rotationstage nicht gewechselt wurde. Der Standardwert lautet 90 Tage.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
8.3.11	Eine starke Authentifizierung für Benutzer und Administratoren wird eingerichtet und verwaltet. (PCI-DSS-v4.0)	iam-policy-in-use	Stellen Sie sicher, dass ein IAM-Richtlinien-ARN einem IAM-Benutzer oder einer Gruppe mit einem oder mehreren IAM-Benutzern oder einer IAM-Rolle mit einer oder mehreren vertrauenswürdigen Entitäten zugewiesen ist.
8.3.11	Eine starke Authentifizierung für Benutzer und Administratoren wird eingerichtet und verwaltet. (PCI-DSS-v4.0)	ec2- no-amazon-key-pair	Stellen Sie sicher, dass laufende Amazon Elastic Compute Cloud (EC2) -Instances nicht mit Amazon-Schlüsselpaaren gestartet werden. Die Regel lautet NON_COMPLIANT, wenn eine laufende EC2 Instance mit einem key pair gestartet wird.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
8.3.2	Eine starke Authentifizierung für Benutzer und Administratoren wird eingerichtet und verwaltet. (PCI-DSS-v4.0)	athena-workgroup-encrypted-at-ausruhen	Stellen Sie sicher, dass eine Amazon Athena Athena-Arbeitsgruppe im Ruhezustand verschlüsselt ist. Die Regel ist NON_COMPLIANT, wenn die Verschlüsselung von Daten im Ruhezustand für eine Athena-Arbeitsgruppe nicht aktiviert ist.
8.3.2	Eine starke Authentifizierung für Benutzer und Administratoren wird eingerichtet und verwaltet. (PCI-DSS-v4.0)	neptune-cluster-snapshot-encrypted	Stellen Sie sicher, dass ein Amazon Neptune Neptune-DB-Cluster über verschlüsselte Snapshots verfügt. Die Regel ist NON_COMPLIANT, wenn ein Neptune-Cluster keine verschlüsselten Snapshots enthält.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
8.3.2	Eine starke Authentifizierung für Benutzer und Administratoren wird eingerichtet und verwaltet. (PCI-DSS-v4.0)	redshift-cluster-kms-enabled	Stellen Sie sicher, dass Amazon Redshift Redshift-Cluster einen bestimmten AWS Key Management Service (AWS KMS) -Schlüssel für die Verschlüsselung verwenden. Die Regel ist KONFORM, wenn die Verschlüsselung aktiviert ist und der Cluster mit dem im kmsKeyArn Parameter angegebenen Schlüssel verschlüsselt ist. Die Regel ist NON_COMPLIANT, wenn der Cluster nicht oder mit einem anderen Schlüssel verschlüsselt ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
8.3.2	Eine starke Authentifizierung für Benutzer und Administratoren wird eingerichtet und verwaltet. (PCI-DSS-v4.0)	codebuild-project-s3-log-verschlüsselt	Stellen Sie sicher, dass bei einem mit Amazon S3 Logs konfigurierten AWS CodeBuild Projekt die Verschlüsselung für die Protokolle aktiviert ist. Die Regel lautet NON_COMPLIANT, wenn 'EncryptionDisabled' in einem LogsConfig S3-Projekt auf 'true' gesetzt ist. CodeBuild
8.3.2	Eine starke Authentifizierung für Benutzer und Administratoren wird eingerichtet und verwaltet. (PCI-DSS-v4.0)	dms-redis-tls-enabled	Stellen Sie sicher, dass die Endpunkte des AWS Database Migration Service (AWS DMS) für Redis-Datenspeicher aktiviert sind, sodass die TLS/SSL encryption of data communicated with other endpoints. The rule is NON_COMPLIANT if TLS/SSL Verschlüsselung nicht aktiviert ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
8.3.2	Eine starke Authentifizierung für Benutzer und Administratoren wird eingerichtet und verwaltet. (PCI-DSS-v4.0)	eks-secrets-encrypted	Stellen Sie sicher, dass Amazon Elastic Kubernetes Service Service-Cluster so konfiguriert sind, dass Kubernetes-Geheimnisse mithilfe von AWS Key Management Service (KMS) - Schlüsseln verschlüsselt werden.
8.3.2	Eine starke Authentifizierung für Benutzer und Administratoren wird eingerichtet und verwaltet. (PCI-DSS-v4.0)	api-gw-cache-enabled-und-verschlüsselt	Stellen Sie sicher, dass für alle Methoden in den Amazon API Gateway Gateway-Stufen der Cache aktiviert und der Cache verschlüsselt ist. Die Regel ist NON_COMPLIANT, wenn für eine Methode in einer Amazon-API-Gateway-Stufe der Cache nicht konfiguriert oder nicht verschlüsselt ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
8.3.2	Eine starke Authentifizierung für Benutzer und Administratoren wird eingerichtet und verwaltet. (PCI-DSS-v4.0)	dynamodb-table-encrypted-kms	Stellen Sie sicher, dass die Amazon DynamoDB-Tabelle mit dem AWS Key Management Service (KMS) verschlüsselt ist. Die Regel lautet NON_COMPLIANT, wenn die Amazon DynamoDB-Tabelle nicht mit KMS verschlüsselt ist. AWS Die Regel ist auch NON_COMPLIANT, wenn der verschlüsselte AWS KMS-Schlüssel nicht im Eingabeparameter vorhanden ist. kmsKeyArns

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
8.3.2	Eine starke Authentifizierung für Benutzer und Administratoren wird eingerichtet und verwaltet. (PCI-DSS-v4.0)	codebuild-project-envvar-awscred-überprüfen	Stellen Sie sicher, dass das Projekt KEINE Umgebungsvariablen und _ACCESS_KEY enthält. AWS_ACCESS_KEY_ID AWS_SECRET Die Regel ist NON_COMPLIANT, wenn die Projekt-Umgebungsvariablen Klartext-Anmeldeinformationen enthalten.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
8.3.2	Eine starke Authentif izierung für Benutzer und Administratoren wird eingerichtet und verwaltet. (PCI-DSS-v4.0)	elb-acm-certificate-required	Stellen Sie sicher, dass die Classic Load Balancers SSL-Zerti fikate verwenden, die vom AWS Certificate Manager bereitgestellt werden. Verwenden Sie zur Nutzung dieser Regel mit Ihrem Classic Load Balancer einen SSL- oder HTTPS-Listener. Hinweis: Diese Regel gilt nur für Classic Load Balancers. Mit dieser Regel werden keine Applicati on Load Balancer oder Network Load Balancer geprüft.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
8.3.2	Eine starke Authentifizierung für Benutzer und Administratoren wird eingerichtet und verwaltet. (PCI-DSS-v4.0)	eks-cluster-secrets-encrypted	Stellen Sie sicher, dass Amazon EKS-Cluster nicht so konfiguriert sind, dass Kubernetes-Geheimnisse mit KMS verschlüsselt AWS werden. Die Regel lautet NON_COMPLIANT, wenn ein EKS-Cluster keine EncryptionConfig-Ressource hat oder wenn EncryptionConfig Geheimnisse nicht als Ressource benennt.
8.3.2	Eine starke Authentifizierung für Benutzer und Administratoren wird eingerichtet und verwaltet. (PCI-DSS-v4.0)	kinesis-stream-encrypted	Stellen Sie sicher, dass Amazon Kinesis Kinesis-Streams im Ruhezustand mit serverseitiger Verschlüsselung verschlüsselt werden. Die Regel lautet NON_COMPLIANT für einen Kinesis-Stream, wenn 'StreamEncryption' nicht vorhanden ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
8.3.2	Eine starke Authentif izierung für Benutzer und Administratoren ist eingerichtet und wird verwaltet. (PCI-DSS-v4.0)	msk-in-cluster-node-TLS erforderlich	Stellen Sie sicher, dass ein Amazon MSK-Cluster die Verschlüsselung während der Übertragung mithilfe von HTTPS (TLS) mit den Broker-Kn oten des Clusters erzwingt. Die Regel ist NON_COMPL IANT, wenn Klartextk ommunikation für Broker-Knotenverbi ndungen in Clustern aktiviert ist.
8.3.2	Eine starke Authentif izierung für Benutzer und Administratoren wird eingerichtet und verwaltet. (PCI-DSS-v4.0)	neptune-cluster-en crypted	Stellen Sie sicher, dass die Speicherv erschlüsselung für Ihre Amazon Neptune Neptune-DB-Cluster aktiviert ist. Die Regel ist NON_COMPL IANT, wenn die Speicherverschlüss elung nicht aktiviert ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
8.3.2	Eine starke Authentifizierung für Benutzer und Administratoren wird eingerichtet und verwaltet. (PCI-DSS-v4.0)	dms-endpoint-ssl-configured	Stellen Sie sicher, dass die Endpoints des AWS Database Migration Service (AWS DMS) mit einer SSL-Verbindung konfiguriert sind. Die Regel lautet NON_COMPLIANT, wenn für AWS DMS keine SSL-Verbindung konfiguriert ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
8.3.4	Eine starke Authentifizierung für Benutzer und Administratoren wird eingerichtet und verwaltet. (PCI-DSS-v4.0)	s-3 bucket-blacklisted-actions-prohibited	Stellen Sie sicher, dass eine Bucket-Richtlinie von Amazon Simple Storage Service (Amazon S3) keine Aktionen auf Bucket- und Objektebene auf Blocklisten für Ressourcen im Bucket für Prinzipale anderer Konten zulässt. AWS Die Regel überprüft beispielsweise, ob die Amazon S3 S3-Bucket-Richtlinie einem anderen AWS Konto nicht erlaubt, s3: GetBucket *-Aktionen und s3: DeleteObject für ein Objekt im Bucket auszuführen. Die Regel ist NON_COMPLIANT, wenn gesperrte Aktionen gemäß der Bucket-Richtlinie von Amazon S3 zulässig sind.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
8.3.4	Eine starke Authentifizierung für Benutzer und Administratoren wird eingerichtet und verwaltet. (PCI-DSS-v4.0)	bucket-policy-not-mores3-permissiv	Stellen Sie sicher, dass Ihre Amazon Simple Storage Service (S3) -Bucket-Richtlinien keine anderen Kontobere chtigungen zulassen als die von Ihnen Amazon S3 S3-Bucket-Kontrollrichtlinie.
8.3.4	Eine starke Authentifizierung für Benutzer und Administratoren wird eingerichtet und verwaltet. (PCI-DSS-v4.0)	iam-policy-in-use	Stellen Sie sicher, dass ein IAM-Richtlinien-ARN einem IAM-Benutzer oder einer Gruppe mit einem oder mehreren IAM-Benutzern oder einer IAM-Rolle mit einer oder mehreren vertrauenswürdigen Entitäten zugewiesen ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
8.3.4	Eine starke Authentifizierung für Benutzer und Administratoren wird eingerichtet und verwaltet. (PCI-DSS-v4.0)	neptune-cluster-iam-database-Authentifizierung	Stellen Sie sicher, dass für einen Amazon Neptune Neptune-Cluster die AWS Identity and Access Management (IAM) -Datenbankauthentifizierung aktiviert ist. Die Regel ist NON_COMPLIANT, wenn für einen Amazon-Neptune-Cluster die IAM-Datenbankauthentifizierung nicht aktiviert ist.
8.3.4	Eine starke Authentifizierung für Benutzer und Administratoren wird eingerichtet und verwaltet. (PCI-DSS-v4.0)	ec2- instance-profile-attached	Stellen Sie sicher, dass an eine EC2 Instanz ein AWS Identity and Access Management (IAM) -Profil angehängt ist. Die Regel lautet NON_COMPLIANT, wenn der Instanz kein IAM-Profil angehängt ist. EC2

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
8.3.4	Eine starke Authentifizierung für Benutzer und Administratoren wird eingerichtet und verwaltet. (PCI-DSS-v4.0)	backup-recovery-point-manual-Löschen-deaktiviert	Stellen Sie sicher, dass an einen Backup-Tresor eine ressourcenbasierte Richtlinie angehängt ist, die das Löschen von Wiederherstellungspunkten verhindert. Die Regel lautet NON_COMPLIANT, wenn der Backup-Tresor keine ressourcenbasierten Richtlinien oder Richtlinien ohne eine geeignete „Deny“ -Anweisung (Anweisung mit den Berechtigungen backup:DeleteRecoveryPoint, backup: und backup:UpdateRecoveryPointLifecycle) hat. PutBackupVaultAccessPolicy

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
8.3.5	Eine starke Authentifizierung für Benutzer und Administratoren wird eingerichtet und verwaltet. (PCI-DSS-v4.0)	access-keys-rotated	Stellen Sie sicher, dass aktive IAM-Zugriffsschlüssel innerhalb der unter Alter angegebenen Anzahl von Tagen rotiert (geändert) werden. maxAccessKey Die Regel ist NON_COMPLIANT, wenn die Zugriffsschlüssel nicht innerhalb des angegebenen Zeitraums rotiert werden. Der Standardwert lautet 90 Tage.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
8.3.5	Eine starke Authentifizierung für Benutzer und Administratoren wird eingerichtet und verwaltet. (PCI-DSS-v4.0)	secretsmanager-scheduled-rotation-success-überprüfen	Stellen Sie sicher, dass AWS Secrets Manager-Geheimnisse gemäß dem Rotationsplan erfolgreich rotiert wurden. Secrets Manager berechnet das Datum, an dem die Rotation stattfinden soll. Die Regel ist NON_COMPLIANT, wenn das Datum verstrichen ist und das Secret nicht rotiert wurde.
8.3.5	Eine starke Authentifizierung für Benutzer und Administratoren wird eingerichtet und verwaltet. (PCI-DSS-v4.0)	secretsmanager-secret-periodic-rotation	Stellen Sie sicher, dass AWS Secrets Manager-Geheimnisse in der letzten angegebenen Anzahl von Tagen rotiert wurden. Die Regel lautet NON_COMPLIANT, wenn ein Secret länger als die Anzahl der maxDaysSince Rotationstage nicht gewechselt wurde. Der Standardwert lautet 90 Tage.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
8.3.7	Eine starke Authentif izierung für Benutzer und Administratoren wird eingerichtet und verwaltet. (PCI-DSS-v4.0)	access-keys-rotated	Stellen Sie sicher, dass aktive IAM-Zugriffsschlüssel innerhalb der unter Alter angegebenen Anzahl von Tagen rotiert (geändert) werden. maxAccess Key Die Regel ist NON_COMPL IANT, wenn die Zugriffsschlüssel nicht innerhalb des angegeben en Zeitraums rotiert werden. Der Standardwert lautet 90 Tage.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
8.3.7	Eine starke Authentifizierung für Benutzer und Administratoren wird eingerichtet und verwaltet. (PCI-DSS-v4.0)	secretsmanager-scheduled-rotation-success-überprüfen	Stellen Sie sicher, dass AWS Secrets Manager-Geheimnisse gemäß dem Rotationsplan erfolgreich rotiert wurden. Secrets Manager berechnet das Datum, an dem die Rotation stattfinden soll. Die Regel ist NON_COMPLIANT, wenn das Datum verstrichen ist und das Secret nicht rotiert wurde.
8.3.7	Eine starke Authentifizierung für Benutzer und Administratoren wird eingerichtet und verwaltet. (PCI-DSS-v4.0)	secretsmanager-secret-periodic-rotation	Stellen Sie sicher, dass AWS Secrets Manager-Geheimnisse in der letzten angegebenen Anzahl von Tagen rotiert wurden. Die Regel lautet NON_COMPLIANT, wenn ein Secret länger als die Anzahl der maxDaysSince Rotationstage nicht gewechselt wurde. Der Standardwert lautet 90 Tage.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
8.3.9	Eine starke Authentifizierung für Benutzer und Administratoren wird eingerichtet und verwaltet. (PCI-DSS-v4.0)	access-keys-rotated	Stellen Sie sicher, dass aktive IAM-Zugriffsschlüssel innerhalb der unter Alter angegebenen Anzahl von Tagen rotiert (geändert) werden. maxAccessKey Die Regel ist NON_COMPLIANT, wenn die Zugriffsschlüssel nicht innerhalb des angegebenen Zeitraums rotiert werden. Der Standardwert lautet 90 Tage.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
8.3.9	Eine starke Authentifizierung für Benutzer und Administratoren wird eingerichtet und verwaltet. (PCI-DSS-v4.0)	secretsmanager-scheduled-rotation-success-überprüfen	Stellen Sie sicher, dass AWS Secrets Manager-Geheimnisse gemäß dem Rotationsplan erfolgreich rotiert wurden. Secrets Manager berechnet das Datum, an dem die Rotation stattfinden soll. Die Regel ist NON_COMPLIANT, wenn das Datum verstrichen ist und das Secret nicht rotiert wurde.
8.3.9	Eine starke Authentifizierung für Benutzer und Administratoren wird eingerichtet und verwaltet. (PCI-DSS-v4.0)	secretsmanager-secret-periodic-rotation	Stellen Sie sicher, dass AWS Secrets Manager-Geheimnisse in der letzten angegebenen Anzahl von Tagen rotiert wurden. Die Regel lautet NON_COMPLIANT, wenn ein Secret länger als die Anzahl der maxDaysSince Rotationstage nicht gewechselt wurde. Der Standardwert lautet 90 Tage.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
8.4.1	Die Multi-Faktor-Authentifizierung (MFA) wird implementiert, um den Zugriff auf die CDE zu sichern. (PCI-DSS-v4.0)	s-3 bucket-mfa-delete-enabled	Stellen Sie sicher, dass MFA Delete in der Bucket-Versionierungskonfiguration von Amazon Simple Storage Service (Amazon S3) aktiviert ist. Die Regel ist NON_COMPLIANT, wenn MFA Delete nicht aktiviert ist.
8.4.2	Die Multi-Faktor-Authentifizierung (MFA) wird implementiert, um den Zugriff auf die CDE zu sichern. (PCI-DSS-v4.0)	s-3 bucket-mfa-delete-enabled	Stellen Sie sicher, dass MFA Delete in der Bucket-Versionierungskonfiguration von Amazon Simple Storage Service (Amazon S3) aktiviert ist. Die Regel ist NON_COMPLIANT, wenn MFA Delete nicht aktiviert ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
8.4.3	Die Multi-Faktor-Authentifizierung (MFA) wird implementiert, um den Zugriff auf die CDE zu sichern. (PCI-DSS-v4.0)	s-3 bucket-mfa-delete-enabled	Stellen Sie sicher, dass MFA Delete in der Bucket-Versionierungskonfiguration von Amazon Simple Storage Service (Amazon S3) aktiviert ist. Die Regel ist NON_COMPLIANT, wenn MFA Delete nicht aktiviert ist.
8.6.3	Die Verwendung von Anwendungs- und Systemkonten und den damit verbundenen Authentifizierungsfaktoren wird strikt verwaltet. (PCI-DSS-v4.0)	access-keys-rotated	Stellen Sie sicher, dass aktive IAM-Zugriffsschlüssel innerhalb der unter Alter angegebenen Anzahl von Tagen rotiert (geändert) werden. maxAccessKey Die Regel ist NON_COMPLIANT, wenn die Zugriffsschlüssel nicht innerhalb des angegebenen Zeitraums rotiert werden. Der Standardwert lautet 90 Tage.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
8.6.3	Die Verwendung von Anwendungs- und Systemkonten und den damit verbunden en Authentifizierungs faktoren wird strikt verwaltet. (PCI-DSS-v4.0)	secretsmanager-sch eduled-rotation-su ccess-überprüfen	Stellen Sie sicher, dass AWS Secrets Manager-Geheimniss e gemäß dem Rotationsplan erfolgreich rotiert wurden. Secrets Manager berechnet das Datum, an dem die Rotation stattfind en soll. Die Regel ist NON_COMPLIANT, wenn das Datum verstrichen ist und das Secret nicht rotiert wurde.
8.6.3	Die Verwendung von Anwendungs- und Systemkonten und den damit verbunden en Authentifizierungs faktoren wird strikt verwaltet. (PCI-DSS-v4.0)	secretsmanager-sec ret-periodic-rotation	Stellen Sie sicher, dass AWS Secrets Manager-Geheimniss e in der letzten angegebenen Anzahl von Tagen rotiert wurden. Die Regel lautet NON_COMPL IANT, wenn ein Secret länger als die Anzahl der maxDaysSince Rotationstage nicht gewechselt wurde. Der Standardwert lautet 90 Tage.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
A1.1.2	Multi-Tenant-Servi ceprovider schützen und trennen alle Kundenumgebungen und Daten voneinand er. (PCI-DSS-v4.0)	neptune-cluster-sn apshot-public-verb oten	Stellen Sie sicher, dass ein manueller Amazon Neptune Neptune-DB-Cluster-Snapshot nicht öffentlich ist. Die Regel ist NON_COMPLIANT, wenn es vorhanden e und neue Neptune-Cluster-Snapshots gibt, die öffentlich zugänglich sind.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
A1.1.2	Multi-Tenant-Servi ceprovider schützen und trennen alle Kundenumgebungen und Daten voneinand er. (PCI-DSS-v4.0)	backup-recovery-po int-manual-Löschen-deaktiviert	Stellen Sie sicher, dass an einen Backup-Tresor eine ressource nbasierte Richtlini e angehängt ist, die das Löschen von Wiederherstellungs punkten verhinder t. Die Regel lautet NON_COMPLIANT, wenn der Backup-Tr esor keine ressource nbasierten Richtlini en oder Richtlinien ohne eine geeignete „Deny“ -Anweisun g (Anweisung mit den Berechtigungen backup:DeleteRecov eryPoint, backup: und backup:UpdateRecov eryPointLifecycle) hat. PutBackupVaultAcce ssPolicy

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
A1.1.2	Multi-Tenant-Servi ceprovider schützen und trennen alle Kundenumgebungen und Daten voneinand er. (PCI-DSS-v4.0)	emr-block-public-a ccess	Stellen Sie sicher, dass für ein Konto bei Amazon EMR die Einstellungen zum Sperren des öffentlic hen Zugriffs aktiviert sind. Die Regel ist NON_COMPLIANT, wenn sie falsch BlockPublicSecurit yGroupRules ist, oder wenn sie wahr ist, sind andere Ports als Port 22 unter aufgeführt. Permitted PublicSecurityGrou pRuleRanges
A1.1.2	Multi-Tenant-Servi ceprovider schützen und trennen alle Kundenumgebungen und Daten voneinand er. (PCI-DSS-v4.0)	access-point-public-accesss3-Blöcke	Stellen Sie sicher, dass Amazon S3 S3-Zugriffspunkten die Einstellungen zum Blockieren des öffentlichen Zugriffs aktiviert sind. Die Regel ist NON_COMPLIANT, wenn die Einstellung zum Blockieren des öffentlichen Zugriffs für S3-Zugangspunkte nicht aktiviert ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
A1.1.2	Multi-Tenant-Servi ceprovider schützen und trennen alle Kundenumgebungen und Daten voneinand er. (PCI-DSS-v4.0)	account-level-public-accesss3-Blöcke	Stellen Sie sicher, dass die erforderl ichen Einstellungen für die Sperrung des öffentlichen Zugriffs auf Kontoebene konfiguriert sind. Die Regel ist nur NON_COMPL IANT, wenn die unten festgeleg ten Felder nicht mit den entsprech enden Feldern im Konfigurationselement übereinstimmen.
A1.1.2	Dienstanbieter mit mehreren Mandanten schützen und trennen alle Kundenumg ebungen und Daten voneinander. (PCI-DSS-v4.0)	s-3 bucket-mfa-delete-enabled	Stellen Sie sicher, dass MFA Delete in der Bucket-Ve rsionierungskonfig uration von Amazon Simple Storage Service (Amazon S3) aktiviert ist. Die Regel ist NON_COMPL IANT, wenn MFA Delete nicht aktiviert ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
A1.1.3	Dienstanbieter mit mehreren Mandanten schützen und trennen alle Kundenumg ebungen und Daten voneinander. (PCI-DSS-v4.0)	api-gw-endpoint-type-überprüfen	Stellen Sie sicher, dass Amazon API Gateway APIs dem Typ entspricht, der im Regelparameter 'endpointConfigurationType' angegeben ist. Die Regel gibt NON_COMPLIANT zurück, wenn die REST-API nicht mit dem Endpunkttyp übereinstimmt, der im Regelparameter konfiguriert ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
A1.1.3	Dienstanbieter mit mehreren Mandanten schützen und trennen alle Kundenumg ebungen und Daten voneinander. (PCI-DSS-v4.0)	netfw-policy-defau lt-action-fragment-Pakete	Stellen Sie sicher, dass eine AWS Netzwerk-Firewall-Richtlinie mit einer benutzerdefinierte n statusfreien Standardaktion für fragmentierte Pakete konfiguriert ist. Die Regel ist NON_COMPLIANT, wenn die zustandsl ose Standardaktion für fragmentierte Pakete nicht mit der benutzerdefinierte n Standardaktion übereinstimmt.
A1.1.3	Dienstanbieter mit mehreren Mandanten schützen und trennen alle Kundenumg ebungen und Daten voneinander. (PCI-DSS-v4.0)	eks-endpoint-no-pu blic-Zugang	Stellen Sie sicher, dass der Amazon Elastic Kubernete s Service (Amazon EKS) -Endpunkt nicht öffentlich zugänglic h ist. Die Regel ist NON_COMPLIANT, wenn der Endpunkt öffentlich zugänglich ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
A1.1.3	Dienstanbieter mit mehreren Mandanten schützen und trennen alle Kundenumg ebungen und Daten voneinander. (PCI-DSS-v4.0)	restricted-ssh	Hinweis: Bei dieser Regel untersche iden sich die Regel-ID (INCOMING _SSH_DISABLED) und der Regelname (restricted-ssh). Stellen Sie sicher, dass auf den eingehenden SSH-Verkehr für die Sicherheitsgruppen zugegriffen werden kann. Die Regel ist COMPLIANT, wenn die IP-Adressen des eingehenden SSH-Datenverkehrs in den Sicherheitsgruppen eingeschränkt sind (CIDR ungleich 0.0.0.0/0 oder ::/0). Andernfalls ist sie NON_COMPLIANT.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
A1.1.3	Dienstanbieter mit mehreren Mandanten schützen und trennen alle Kundenumg ebungen und Daten voneinander. (PCI-DSS-v4.0)	appsync-associated-with-waf	Stellen Sie sicher, dass AWS AppSync APIs sie den AWS WAFv2 Web-Zugri ffskontrolllisten () zugeordnet sind. ACLs Die Regel ist NON_COMPL IANT für eine AWS AppSync API, wenn sie keiner Web-ACL zugeordnet ist.
A1.1.3	Dienstanbieter mit mehreren Mandanten schützen und trennen alle Kundenumg ebungen und Daten voneinander. (PCI-DSS-v4.0)	codebuild-project-source-repo-URL-Prüfung	Stellen Sie sicher, dass die URL des Bitbucket-Quell-Repositorys KEINE Anmeldeinformationen enthält oder nicht. Die Regel ist NON_COMPL IANT, wenn die URL Anmeldeinformationen enthält, und COMPLIANT, falls dies nicht der Fall ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
A1.1.3	Dienstanbieter mit mehreren Mandanten schützen und trennen alle Kundenumg ebungen und Daten voneinander. (PCI-DSS-v4.0)	elb-acm-certificate-required	Stellen Sie sicher, dass die Classic Load Balancers SSL-Zerti fikate verwenden, die vom AWS Certificate Manager bereitgestellt werden. Verwenden Sie zur Nutzung dieser Regel mit Ihrem Classic Load Balancer einen SSL- oder HTTPS-Listener. Hinweis: Diese Regel gilt nur für Classic Load Balancers. Mit dieser Regel werden keine Applicati on Load Balancer oder Network Load Balancer geprüft.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
A1.1.3	Dienstanbieter mit mehreren Mandanten schützen und trennen alle Kundenumg ebungen und Daten voneinander. (PCI-DSS-v4.0)	emr-block-public-access	Stellen Sie sicher, dass für ein Konto bei Amazon EMR die Einstellungen zum Sperren des öffentlichen Zugriffs aktiviert sind. Die Regel ist NON_COMPLIANT, wenn sie falsch BlockPublicSecurityGroupRules ist, oder wenn sie wahr ist, sind andere Ports als Port 22 unter aufgeführt. Permitted PublicSecurityGroupRuleRanges
A1.1.3	Dienstanbieter mit mehreren Mandanten schützen und trennen alle Kundenumg ebungen und Daten voneinander. (PCI-DSS-v4.0)	nacl-no-unrestricted-ssh-rdp	Stellen Sie sicher, dass die Standardports für eingehenden SSH/RDP-Datenverkehr für Netzwerkzugriffskontrolllisten () eingeschränkt sind. NACLs Die Regel ist NON_COMPLIANT, wenn ein eingehender NACL-Eintrag für die Ports 22 oder 3389 einen CIDR-Block des Typs Quell-TCP oder -UDP zulässt.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
A1.1.3	Dienstanbieter mit mehreren Mandanten schützen und trennen alle Kundenumg ebungen und Daten voneinander. (PCI-DSS-v4.0)	ec2- -alle client-vpn-not-authorize	Stellen Sie sicher, dass die AWS Client-VPN-Autorisierungsre geln nicht den Verbindungszugriff für alle Clients autorisie ren. Die Regel ist NON_COMPLIANT, wenn 'AccessAll' vorhanden und auf true gesetzt ist.
A1.1.3	Dienstanbieter mit mehreren Mandanten schützen und trennen alle Kundenumg ebungen und Daten voneinander. (PCI-DSS-v4.0)	internet-gateway-a uthorized-vpc-nur	Stellen Sie sicher, dass Internet-Gateways an eine autorisierte virtuelle private Cloud (Amazon VPC) angeschlo ssen sind. Die Regel ist NON_COMPL IANT, wenn Internet-Gateways an eine nicht autorisierte VPC angehängt sind.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
A1.1.3	Dienstanbieter mit mehreren Mandanten schützen und trennen alle Kundenumg ebungen und Daten voneinander. (PCI-DSS-v4.0)	access-point-public-accesss3-Blöcke	Stellen Sie sicher, dass Amazon S3 S3-Zugriffspunkten die Einstellungen zum Blockieren des öffentlichen Zugriffs aktiviert sind. Die Regel ist NON_COMPLIANT, wenn die Einstellung zum Blockieren des öffentlichen Zugriffs für S3-Zugangspunkte nicht aktiviert ist.
A1.1.3	Dienstanbieter mit mehreren Mandanten schützen und trennen alle Kundenumg ebungen und Daten voneinander. (PCI-DSS-v4.0)	account-level-public-accesss3-Blöcke	Stellen Sie sicher, dass die erforderl ichen Einstellungen für die Sperrung des öffentlichen Zugriffs auf Kontoebene konfiguriert sind. Die Regel ist nur NON_COMPL IANT, wenn die unten festgeleg ten Felder nicht mit den entsprech enden Feldern im Konfigurationselement übereinstimmen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
A1.2.1	Multi-Tenant-Dienstanbieter erleichtern allen Kunden die Protokollierung und Reaktion auf Vorfälle. (PCI-DSS-v4.0)	api-gwv2- access-logs-enabled	Stellen Sie sicher, dass die Amazon API Gateway V2-Stufen die Zugriffsprotokollierung aktiviert haben. Die Regel ist NON_COMPLIANT, wenn 'accessLogSettings' in der Stage-Konfiguration nicht vorhanden ist.
A1.2.1	Multi-Tenant-Dienstanbieter erleichtern allen Kunden die Protokollierung und Reaktion auf Vorfälle. (PCI-DSS-v4.0)	api-gw-xray-enabled	Stellen Sie sicher, dass AWS X-Ray Tracing auf Amazon API Gateway REST APIs aktiviert ist. Die Regel ist COMPLIANT, wenn die X-Ray-Ablaufverfolgung aktiviert ist, andernfalls ist sie NON_COMPLIANT.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
A1.2.1	Multi-Tenant-Dienstanbieter erleichtern allen Kunden die Protokollierung und Reaktion auf Vorfälle. (PCI-DSS-v4.0)	cloudtrail-security-trail-enabled	Stellen Sie sicher, dass mindestens ein AWS CloudTrail Pfad mit bewährten Sicherheitsmethoden definiert ist. Diese Regel ist COMPLIANT, wenn es mindestens einen Trail gibt, der alle der folgenden Bedingungen erfüllt:
A1.2.1	Multi-Tenant-Dienstanbieter erleichtern allen Kunden die Protokollierung und Reaktion auf Vorfälle. (PCI-DSS-v4.0)	neptune-cluster-cloudwatch-log-exportfähig	Stellen Sie sicher, dass in einem Amazon Neptune Neptune-Cluster der Protokollexport für CloudWatch Audit-Logs aktiviert ist. Die Regel lautet NON_COMPLIANT, wenn für einen Neptune-Cluster der Protokollexport für CloudWatch Audit-Logs nicht aktiviert ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
A1.2.1	Multi-Tenant-Dienstanbieter erleichtern allen Kunden die Protokollierung und Reaktion auf Vorfälle. (PCI-DSS-v4.0)	ecs-task-definition-log-Konfiguration	Stellen Sie sicher, dass LogConfiguration für aktive ECS-Aufgabendefinitionen festgelegt ist. Diese Regel ist NON_COMPLIANT, wenn für eine aktive ECSTask Definition die LogConfiguration-Ressource nicht definiert ist oder der Wert für LogConfiguration in mindestens einer Containerdefinition Null ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
A1.2.1	Multi-Tenant-Dienstanbieter erleichtern allen Kunden die Protokollierung und Reaktion auf Vorfälle. (PCI-DSS-v4.0)	cloudtrail-enabled	Hinweis: Bei dieser Regel unterscheiden sich die Regel-ID (CLOUD_TRAIL_ENABLED) und der Regelname (cloudtrail-enabled). Stellen Sie sicher, dass in Ihrem Konto ein Trail aktiviert ist AWS CloudTrail . AWS Die Regel ist NON_COMPLIANT, wenn ein Trail nicht aktiviert ist. Optional überprüft die Regel einen bestimmten S3-Bucket, ein Amazon Simple Notification Service (Amazon SNS) -Thema und eine CloudWatch Protokollgruppe.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
A1.2.1	Multi-Tenant-Dienstanbieter erleichtern allen Kunden die Protokollierung und Reaktion auf Vorfälle. (PCI-DSS-v4.0)	multi-region-cloudtrail-enabled	Hinweis: Bei dieser Regel unterscheiden sich die Regel-ID (MULTI_REGION_CLOUD_TRAIL_ENABLED) und der Regelname (). multi-region-cloudtrail-enabled Stellen Sie sicher, dass mindestens eine Region mit mehreren Regionen vorhanden ist. AWS CloudTrail Die Regel ist NON_COMPLIANT, wenn die Trails nicht mit den Eingabeparametern übereinstimmen. Die Regel lautet NON_COMPLIANT, wenn das ExcludeManagementEventSources Feld nicht leer ist oder wenn sie so konfiguriert AWS CloudTrail ist, dass Verwaltungsereignisse wie AWS KMS-Ereignisse oder Amazon RDS-Daten-API-Ereignisse

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			ausgeschlossen werden.
A1.2.1	Multi-Tenant-Dienstanbieter erleichtern allen Kunden die Protokollierung und Reaktion auf Vorfälle. (PCI-DSS-v4.0)	appsync-logging-enabled	Stellen Sie sicher, dass für eine API die Protokollierung aktiviert ist. AWS AppSync Die Regel lautet NON_COMPLIANT, wenn die Protokollierung nicht aktiviert ist, oder 'fieldLogLevel' ist weder ERROR noch ALL.
A1.2.1	Multi-Tenant-Dienstanbieter erleichtern allen Kunden die Protokollierung und Reaktion auf Vorfälle. (PCI-DSS-v4.0)	mq-cloudwatch-audit-logging-aktiviert	Stellen Sie sicher, dass Amazon MQ-Broker die CloudWatch Amazon-Auditprotokollierung aktiviert haben. Die Regel ist NON_COMPLIANT, wenn für einen Broker die Audit-Protokollierung nicht aktiviert ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
A1.2.1	Multi-Tenant-Dienstanbieter erleichtern allen Kunden die Protokollierung und Reaktion auf Vorfälle. (PCI-DSS-v4.0)	mq-cloudwatch-audit-log-aktiviert	Stellen Sie sicher, dass bei einem Amazon MQ-Broker die CloudWatch Auditprotokollierung aktiviert ist. Die Regel lautet NON_COMPLIANT, wenn für den Broker die Audit-Protokollierung nicht aktiviert ist.
A1.2.1	Multi-Tenant-Dienstanbieter erleichtern allen Kunden die Protokollierung und Reaktion auf Vorfälle. (PCI-DSS-v4.0)	eks-cluster-logging-enabled	Stellen Sie sicher, dass ein Amazon Elastic Kubernetes Service (Amazon EKS) -Cluster mit aktivierter Protokollierung konfiguriert ist. Die Regel ist NON_COMPLIANT, wenn die Protokollierung für Amazon-EKS-Cluster nicht für alle Protokolltypen aktiviert ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
A1.2.1	Multi-Tenant-Dienstanbieter erleichtern allen Kunden die Protokollierung und Reaktion auf Vorfälle. (PCI-DSS-v4.0)	elastic-beanstalk-logs-to-Wolkenbeobachtung	Stellen Sie sicher, dass AWS Elastic Beanstalk Beanstalk -Umgebungen so konfiguriert sind, dass sie Protokolle an Amazon CloudWatch Logs senden. Die Regel lautet NON_COMPLIANT, wenn der Wert von `` StreamLogs falsch ist.
A1.2.1	Multi-Tenant-Dienstanbieter erleichtern allen Kunden die Protokollierung und Reaktion auf Vorfälle. (PCI-DSS-v4.0)	step-functions-state-machine-Protokollierung aktiviert	Stellen Sie sicher, dass auf der AWS Step Functions Functions-Maschine die Protokollierung aktiviert ist Die Regel ist NON_COMPLIANT, wenn für eine Zustandsmaschine die Protokollierung nicht aktiviert ist oder die Protokollierungskonfiguration nicht auf dem angegebenen Mindestniveau liegt.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
A1.2.1	Multi-Tenant-Dienstanbieter erleichtern allen Kunden die Protokollierung und Reaktion auf Vorfälle. (PCI-DSS-v4.0)	netfw-logging-enabled	Stellen Sie sicher, dass die AWS Netzwerk-Firewall-Firewalls die Protokollierung aktiviert haben. Die Regel ist NON_COMPLIANT, wenn kein Protokollierungstyp konfiguriert ist. Sie können angeben, welchen Protokollierungstyp die Regel prüfen soll.
A1.2.3	Multi-Tenant-Dienstanbieter erleichtern allen Kunden die Protokollierung und Reaktion auf Vorfälle. (PCI-DSS-v4.0)	security-account-information-provided	Stellen Sie sicher, dass Sie die Sicherheitskontaktinformationen für Ihre Kontokontakte angegeben haben. AWS Die Regel ist NON_COMPLIANT, wenn keine Sicherheitskontaktinformationen innerhalb des Kontos angegeben wurden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
A3.2.5.1	Der PCI-DSS-Umfang ist dokumentiert und validiert. (PCI-DSS-v4.0)	macie-auto-sensitive-data-Discovery-Check	Stellen Sie sicher, dass die automatische Erkennung sensibler Daten für Amazon Macie aktiviert ist. Die Regel lautet NON_COMPLIANT, wenn die automatis che Erkennung sensibler Daten deaktiviert ist. Die Regel gilt für Administratorkonte n und NICHT FÜR Mitgliedskonten.
A3.2.5.1	Der PCI-DSS-Umfang ist dokumentiert und validiert. (PCI-DSS-v4.0)	macie-status-check	Stellen Sie sicher, dass Amazon Macie in Ihrem Konto pro Region aktiviert ist. Die Regel ist NON_COMPLIANT, wenn das Attribut „status“ nicht auf „ENABLED“ festgeleg t ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
A3.2.5.2	Der PCI-DSS-Umfang ist dokumentiert und validiert. (PCI-DSS-v4.0)	macie-auto-sensitive-data-Discovery-Check	Stellen Sie sicher, dass die automatische Erkennung sensibler Daten für Amazon Macie aktiviert ist. Die Regel lautet NON_COMPLIANT, wenn die automatis che Erkennung sensibler Daten deaktiviert ist. Die Regel gilt für Administratorkonte n und NICHT FÜR Mitgliedskonten.
A3.2.5.2	Der PCI-DSS-Umfang ist dokumentiert und validiert. (PCI-DSS-v4.0)	macie-status-check	Stellen Sie sicher, dass Amazon Macie in Ihrem Konto pro Region aktiviert ist. Die Regel ist NON_COMPLIANT, wenn das Attribut „status“ nicht auf „ENABLED“ festgeleg t ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
A3.3.1	PCI DSS ist Teil der Aktivitäten von business-as-usual (BAU). (PCI-DSS-v4.0)	api-gw-xray-enabled	Stellen Sie sicher, dass AWS X-Ray Tracing auf Amazon API Gateway REST APIs aktiviert ist. Die Regel ist COMPLIANT, wenn die X-Ray-Abl aufverfolgung aktiviert ist, andernfalls ist sie NON_COMPLIANT.
A 3.3.1	PCI DSS ist Teil der Aktivitäten von business-as-usual (BAU). (PCI-DSS-v4.0)	ec2- instance-detailed-monitoring-enabled	Stellen Sie sicher, dass die detaillierte Überwachung für Instanzen aktiviert ist. EC2 Die Regel ist NON_COMPLIANT, wenn keine detaillierte Überwachung aktiviert ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
A3.3.1	PCI DSS ist Teil der Aktivitäten von business-as-usual (BAU). (PCI-DSS-v4.0)	cloudwatch-alarm-action-check	Stellen Sie sicher, dass bei CloudWatch Alarmen eine Aktion für den Status ALARM, INSUFFICIENT_DATA oder OK konfiguriert ist. Stellen Sie optional sicher, dass alle Aktionen mit einem benannten ARN übereinstimmen. Die Regel ist NON_COMPLIANT, wenn für den Alarm oder den optionalen Parameter keine Aktion festgelegt ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
A3.3.1	PCI DSS ist Teil der Aktivitäten von business-as-usual (BAU). (PCI-DSS-v4.0)	cloudwatch-alarm-action-check	Stellen Sie sicher, dass bei CloudWatch Alarmen eine Aktion für den Status ALARM, INSUFFICIENT_DATA oder OK konfiguriert ist. Stellen Sie optional sicher, dass alle Aktionen mit einem benannten ARN übereinstimmen. Die Regel ist NON_COMPLIANT, wenn für den Alarm oder den optionalen Parameter keine Aktion festgelegt ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
A3.3.1	PCI DSS ist Teil der Aktivitäten von business-as-usual (BAU). (PCI-DSS-v4.0)	cloudwatch-alarm-action-check	Stellen Sie sicher, dass bei CloudWatch Alarmen eine Aktion für den Status ALARM, INSUFFICIENT_DATA oder OK konfiguriert ist. Stellen Sie optional sicher, dass alle Aktionen mit einem benannten ARN übereinstimmen. Die Regel ist NON_COMPLIANT, wenn für den Alarm oder den optionalen Parameter keine Aktion festgelegt ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
A3.3.1	PCI DSS ist Teil der Aktivitäten von business-as-usual (BAU). (PCI-DSS-v4.0)	cloudwatch-alarm-action-check	Stellen Sie sicher, dass bei CloudWatch Alarmen eine Aktion für den Status ALARM, INSUFFICIENT_DATA oder OK konfiguriert ist. Stellen Sie optional sicher, dass alle Aktionen mit einem benannten ARN übereinstimmen. Die Regel ist NON_COMPLIANT, wenn für den Alarm oder den optionalen Parameter keine Aktion festgelegt ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
A3.3.1	PCI DSS ist Teil der Aktivitäten von business-as-usual (BAU). (PCI-DSS-v4.0)	cloudwatch-alarm-resource-check	Stellen Sie sicher, dass ein Ressourcentyp einen CloudWatch Alarm für die angegebene Metrik hat. Als Ressourcentyp können Sie EBS-Volumes, EC2 Instances, Amazon RDS-Cluster oder S3-Buckets angeben. Die Regel ist KONFORM, wenn die benannte Metrik eine Ressourcen-ID und CloudWatch einen Alarm hat.
A3.3.1	PCI DSS ist Teil der Aktivitäten von business-as-usual (BAU). (PCI-DSS-v4.0)	cloudwatch-alarm-settings-check	Stellen Sie sicher, dass CloudWatch Alarme mit dem angegebenen Metriknamen die angegebenen Einstellungen haben.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
A3.3.1	PCI DSS ist Teil der Aktivitäten von business-as-usual (BAU). (PCI-DSS-v4.0)	WAF 2- rulegroup-logging-enabled	Stellen Sie sicher, dass die Erfassung von CloudWatch Amazon-Sicherheits metriken für AWS WAFv2 Regelgruppen aktiviert ist. Die Regel ist NON_COMPL IANT, wenn '. Visibilit yConfig CloudWatc hMetricsEnabledDas Feld 'ist auf falsch gesetzt.
A3.3.1	PCI DSS ist Teil der Aktivitäten von business-as-usual (BAU). (PCI-DSS-v4.0)	sns-topic-message-delivery-Benachric htigung aktiviert	Stellen Sie sicher, dass die Amazon Simple Notificat ion Service (SNS) - Protokollierung für den Zustellungsstatus von Benachric htigungen aktiviert ist, die an ein Thema für die Endgeräte gesendet werden. Die Regel ist NON_COMPLIANT, wenn die Benachric htigung über den Status der Zustellung von Nachrichten nicht aktiviert ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
A3.4.1	Der logische Zugriff auf die Karteninhaberdatenumgebung wird kontrolliert und verwaltet. (PCI-DSS-v4.0)	neptune-cluster-snapshot-public-verboten	Stellen Sie sicher, dass ein manueller Amazon Neptune Neptune-DB-Cluster-Snapshot nicht öffentlich ist. Die Regel ist NON_COMPLIANT, wenn es vorhandene und neue Neptune-Cluster-Snapshots gibt, die öffentlich zugänglich sind.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
A3.4.1	Der logische Zugriff auf die Karteninhaberdatenumgebung wird kontrolliert und verwaltet. (PCI-DSS-v4.0)	backup-recovery-point-manual-Löschen-deaktiviert	Stellen Sie sicher, dass an einen Backup-Tresor eine ressourcenbasierte Richtlinie angehängt ist, die das Löschen von Wiederherstellungspunkten verhindert. Die Regel lautet NON_COMPLIANT, wenn der Backup-Tresor keine ressourcenbasierten Richtlinien oder Richtlinien ohne eine geeignete „Deny“ -Anweisung (Anweisung mit den Berechtigungen backup:DeleteRecoveryPoint, backup: und backup:UpdateRecoveryPointLifecycle) hat. PutBackupVaultAccessPolicy

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
A3.4.1	Der logische Zugriff auf die Karteninh aberdatenumgebung wird kontrolliert und verwaltet. (PCI-DSS-v4.0)	emr-block-public-access	Stellen Sie sicher, dass für ein Konto bei Amazon EMR die Einstellungen zum Sperren des öffentlichen Zugriffs aktiviert sind. Die Regel ist NON_COMPLIANT, wenn sie falsch BlockPublicSecurityGroupRules ist, oder wenn sie wahr ist, sind andere Ports als Port 22 unter aufgeführt. PermittedPublicSecurityGroupRuleRanges

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
A3.4.1	Der logische Zugriff auf die Karteninh aberdatenumgebung wird kontrolliert und verwaltet. (PCI-DSS-v4.0)	secretsmanager-secret-unused	Stellen Sie sicher, dass auf AWS Secrets Manager-Geheimnisse innerhalb einer bestimmten Anzahl von Tagen zugegriffen wurde. Die Regel lautet NON_COMPLIANT, wenn innerhalb von 'unusedForDays' Tagen nicht auf ein Geheimnis zugegriffen wurde. Der Standardwert lautet 90 Tage.
A3.4.1	Der logische Zugriff auf die Karteninh aberdatenumgebung wird kontrolliert und verwaltet. (PCI-DSS-v4.0)	access-point-public-accesss3-Blöcke	Stellen Sie sicher, dass Amazon S3 S3-Zugriffspunkten die Einstellungen zum Blockieren des öffentlichen Zugriffs aktiviert sind. Die Regel ist NON_COMPLIANT, wenn die Einstellung zum Blockieren des öffentlichen Zugriffs für S3-Zugangspunkte nicht aktiviert ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
A3.4.1	Der logische Zugriff auf die Karteninh aberdatenumgebung wird kontrolliert und verwaltet. (PCI-DSS-v4.0)	account-level-public-accesss3-Blöcke	Stellen Sie sicher, dass die erforderl ichen Einstellungen für die Sperrung des öffentlichen Zugriffs auf Kontoebene konfiguriert sind. Die Regel ist nur NON_COMPL IANT, wenn die unten festgeleg ten Felder nicht mit den entsprech enden Feldern im Konfigurationselement übereinstimmen.
A3.4.1	Der logische Zugriff auf die Karteninh aberdatenumgebung wird kontrolliert und verwaltet. (PCI-DSS-v4.0)	s-3 bucket-mfa-delete-enabled	Stellen Sie sicher, dass MFA Delete in der Bucket-Ve rsionierungskonfig uration von Amazon Simple Storage Service (Amazon S3) aktiviert ist. Die Regel ist NON_COMPL IANT, wenn MFA Delete nicht aktiviert ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
A 3.5.1	Verdächtige Ereignisse werden identifiziert und darauf reagiert. (PCI-DSS-v4.0)	api-gw-xray-enabled	Stellen Sie sicher, dass AWS X-Ray Tracing auf Amazon API Gateway REST APIs aktiviert ist. Die Regel ist COMPLIANT, wenn die X-Ray-Abl aufverfolgung aktiviert ist, andernfalls ist sie NON_COMPLIANT.
A 3.5.1	Verdächtige Ereignisse werden identifiziert und darauf reagiert. (PCI-DSS-v4.0)	ec2- instance-detailed-monitoring-enabled	Stellen Sie sicher, dass die detaillierte Überwachung für Instanzen aktiviert ist. EC2 Die Regel ist NON_COMPLIANT, wenn keine detaillierte Überwachung aktiviert ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
A3.5.1	Verdächtige Ereignisse werden identifiziert und darauf reagiert. (PCI-DSS-v4.0)	cloudwatch-alarm-action-check	Stellen Sie sicher, dass bei CloudWatch Alarmen eine Aktion für den Status ALARM, INSUFFICIENT_DATA oder OK konfiguriert ist. Stellen Sie optional sicher, dass alle Aktionen mit einem benannten ARN übereinstimmen. Die Regel ist NON_COMPLIANT, wenn für den Alarm oder den optionalen Parameter keine Aktion festgelegt ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
A3.5.1	Verdächtige Ereignisse werden identifiziert und darauf reagiert. (PCI-DSS-v4.0)	cloudwatch-alarm-action-check	Stellen Sie sicher, dass bei CloudWatch Alarmen eine Aktion für den Status ALARM, INSUFFICIENT_DATA oder OK konfiguriert ist. Stellen Sie optional sicher, dass alle Aktionen mit einem benannten ARN übereinstimmen. Die Regel ist NON_COMPLIANT, wenn für den Alarm oder den optionalen Parameter keine Aktion festgelegt ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
A3.5.1	Verdächtige Ereignisse werden identifiziert und darauf reagiert. (PCI-DSS-v4.0)	cloudwatch-alarm-action-check	Stellen Sie sicher, dass bei CloudWatch Alarmen eine Aktion für den Status ALARM, INSUFFICIENT_DATA oder OK konfiguriert ist. Stellen Sie optional sicher, dass alle Aktionen mit einem benannten ARN übereinstimmen. Die Regel ist NON_COMPLIANT, wenn für den Alarm oder den optionalen Parameter keine Aktion festgelegt ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
A3.5.1	Verdächtige Ereignisse werden identifiziert und darauf reagiert. (PCI-DSS-v4.0)	cloudwatch-alarm-action-check	Stellen Sie sicher, dass bei CloudWatch Alarmen eine Aktion für den Status ALARM, INSUFFICIENT_DATA oder OK konfiguriert ist. Stellen Sie optional sicher, dass alle Aktionen mit einem benannten ARN übereinstimmen. Die Regel ist NON_COMPLIANT, wenn für den Alarm oder den optionalen Parameter keine Aktion festgelegt ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
A3.5.1	Verdächtige Ereignisse werden identifiziert und darauf reagiert. (PCI-DSS-v4.0)	cloudwatch-alarm-resource-check	Stellen Sie sicher, dass ein Ressourcentyp einen CloudWatch Alarm für die angegebene Metrik hat. Als Ressourcentyp können Sie EBS-Volumes, EC2 Instances, Amazon RDS-Cluster oder S3-Buckets angeben. Die Regel ist KONFORM, wenn die benannte Metrik eine Ressourcen-ID und CloudWatch einen Alarm hat.
A3.5.1	Verdächtige Ereignisse werden identifiziert und darauf reagiert. (PCI-DSS-v4.0)	cloudwatch-alarm-settings-check	Stellen Sie sicher, dass CloudWatch Alarme mit dem angegebenen Metriknamen die angegebenen Einstellungen haben.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
A3.5.1	Verdächtige Ereignisse werden identifiziert und darauf reagiert. (PCI-DSS-v4.0)	WAF 2- rulegroup-logging-enabled	Stellen Sie sicher, dass die Erfassung von CloudWatch Amazon-Sicherheitsmetriken für AWS WAFv2 Regelgruppen aktiviert ist. Die Regel ist NON_COMPLIANT, wenn '. VisibilityConfig CloudWatchMetricsEnabledDas Feld 'ist auf falsch gesetzt.
A3.5.1	Verdächtige Ereignisse werden identifiziert und darauf reagiert. (PCI-DSS-v4.0)	sns-topic-message-delivery-Benachrichtigung aktiviert	Stellen Sie sicher, dass die Amazon Simple Notification Service (SNS) - Protokollierung für den Zustellungsstatus von Benachrichtigungen aktiviert ist, die an ein Thema für die Endgeräte gesendet werden. Die Regel ist NON_COMPLIANT, wenn die Benachrichtigung über den Status der Zustellung von Nachrichten nicht aktiviert ist.

Vorlage

Die Vorlage ist verfügbar unter GitHub: Operational Best Practices for PCI DSS 4.0 (ausgenommen globale Ressourcentypen).

Operative Best Practices für PCI DSS 4.0 (einschließlich globaler Ressourcentypen)

Konformitätspakete bieten ein allgemeines Compliance-Framework, das es Ihnen ermöglicht, mithilfe verwalteter oder benutzerdefinierter AWS Config Regeln und Abhilfemaßnahmen Kontrollen zur Sicherheits-, Betriebs- oder Kostenoptimierung durchzuführen. AWS Config Conformance Packs dienen als Beispielvorlagen nicht dazu, die vollständige Einhaltung eines bestimmten Governance- oder Compliance-Standards sicherzustellen. Sie sind dafür verantwortlich, selbst zu beurteilen, ob Ihre Nutzung der Services den geltenden gesetzlichen und behördlichen Anforderungen entspricht.

Im Folgenden finden Sie ein Beispiel für eine Zuordnung zwischen dem Payment Card Industry Data Security Standard (PCI DSS) 4.0 (ohne globale Ressourcentypen) und AWS verwalteten Konfigurationsregeln. Jede AWS Config Regel gilt für eine bestimmte AWS Ressource und bezieht sich auf eine oder mehrere PCI-DSS-Kontrollen. Eine PCI-DSS-Kontrolle kann mehreren Konfigurationsregeln zugeordnet werden. In der folgenden Tabelle finden Sie weitere Informationen und Anleitungen zu diesen Zuordnungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
1.2.5	Die Netzwerks icherheitskontroll en (NSCs) werden konfiguriert und verwaltet. (PCI-DSS-v4.0)	cloudfront-security-policy-check	Stellen Sie sicher, dass CloudFron t Amazon-Di stributionen eine Mindestsicherheits richtlinie und eine Verschlüsselungssu ite von TLSv1 .2 oder höher für Zuschauerverbindun gen verwenden . Diese Regel ist

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			NON_COMPLIANT für eine CloudFron t Distribution, deren Wert unter .2_2018 liegt. minimumPr otocolVersion TLSv1
1.2.5	Die Netzwerks icherheitskontroll en (NSCs) werden konfiguriert und verwaltet. (PCI-DSS-v4.0)	cloudfront-sni-enabled	Stellen Sie sicher, dass CloudFront Amazon-Distributio nen ein benutzerd efiniertes SSL-Zerti fikat verwenden und so konfiguri ert sind, dass SNI zur Bearbeitung von HTTPS-Anf ragen verwendet wird. Die Regel ist NON_COMPLIANT, wenn ein benutzerd efiniertes SSL-Zerti fikat zugeordnet ist, die SSL-Unter stützungsmethode jedoch eine dedizierte IP-Adresse ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
1.2.5	Die Netzwerks icherheitskontroll en (NSCs) werden konfiguriert und verwaltet. (PCI-DSS-v4.0)	transfer-family-server-no-ftp	Stellen Sie sicher, dass ein mit AWS Transfer Family erstellter Server kein FTP für die Endpunktverbindung verwendet. Die Regel lautet NON_COMPL IANT, wenn das Serverprotokoll für die Endpunktverbindung FTP-fähig ist.
1.2.5	Die Netzwerks icherheitskontroll en (NSCs) werden konfiguriert und verwaltet. (PCI-DSS-v4.0)	cloudfront-no-depr ecated-ssl-protokolle	Stellen Sie sicher, dass CloudFront Distributionen keine veralteten SSL-Proto kolle für die HTTPS-Kommunikation zwischen Edge-Stan dorten und benutzerd efinierten Ursprünge n verwenden . CloudFront Diese Regel ist NON_COMPLIANT für eine CloudFron t Verteilung, falls eine Verteilung 'einschließt'. OriginSsl Protocols SSLv3

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
1.2.5	Die Netzwerks icherheitskontroll en (NSCs) werden konfiguriert und verwaltet. (PCI-DSS-v4.0)	cloudfront-traffic-to-origin-verschlüsselt	Stellen Sie sicher, dass CloudFront Amazon-Distributio nen den Datenverkehr zu benutzerdefinierten Ursprüngen verschlüs seln. Die Regel lautet NON_COMPLIANT, falls " " " " " " " " für 'nur' HTTP 'ist oder wennOriginProtocol Policy' 'für' Match-Viewer 'steht und' 'für 'Allow-All' steht. OriginProtocolPolicy ViewerProtocolPolicy
1.2.5	Die NSCs Netzwerks icherheitskontrollen () werden konfiguriert und verwaltet. (PCI-DSS-v4.0)	cloudfront-viewer-policy-https	Stellen Sie sicher, dass Ihre CloudFron t Amazon-Di stributionen HTTPS verwenden (direkt oder über eine Umleitung). Die Regel lautet NON_COMPL IANT, wenn der Wert von auf 'allow-all' für oder für gesetzt ViewerPro tocolPolicy ist. DefaultCacheBehavi or CacheBehaviors

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
1.2.8	Die Netzwerks icherheitskontroll en (NSCs) werden konfiguriert und verwaltet. (PCI-DSS-v4.0)	api-gw-endpoint-type-überprüfen	Stellen Sie sicher, dass Amazon API Gateway APIs dem Typ entspricht, der im Regelparameter 'endpointConfigura tionType' angegeben ist. Die Regel gibt NON_COMPLIANT zurück, wenn die REST-API nicht mit dem Endpunkttyp übereinstimmt, der im Regelparameter konfiguriert ist.
1.2.8	Die Netzwerks icherheitskontroll en (NSCs) werden konfiguriert und verwaltet. (PCI-DSS-v4.0)	cloudfront-associated-with-waf	Stellen Sie sicher, dass CloudFront Amazon-Distributio nen entweder mit Web Application Firewall (WAF) oder WAFv2 Web Access Control Lists (ACLs) verknüpft sind. Die Regel lautet NON_COMPLIANT, wenn eine CloudFron t Distribution keiner WAF-Web-ACL zugeordnet ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
1.2.8	Die Netzwerks icherheitskontroll en (NSCs) werden konfiguriert und verwaltet. (PCI-DSS-v4.0)	cloudfront-custom-ssl-certificate	Stellen Sie sicher, dass das mit einer CloudFront Amazon-Distribution verknüpft e Zertifikat nicht das Standard-SSL-Zerti fikat ist. Die Regel lautet NON_COMPL IANT, wenn eine CloudFront Distribut ion das Standard-SSL-Zertifikat verwendet.
1.2.8	Die Netzwerks icherheitskontroll en (NSCs) werden konfiguriert und verwaltet. (PCI-DSS-v4.0)	netfw-policy-defau lt-action-fragment-Pakete	Stellen Sie sicher, dass eine AWS Netzwerk-Firewall-Richtlinie mit einer benutzerdefinierte n statusfreien Standardaktion für fragmentierte Pakete konfiguriert ist. Die Regel ist NON_COMPLIANT, wenn die zustandsl ose Standardaktion für fragmentierte Pakete nicht mit der benutzerdefinierte n Standardaktion übereinstimmt.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
1.2.8	Die Netzwerks icherheitskontroll en (NSCs) werden konfiguriert und verwaltet. (PCI-DSS-v4.0)	rds-db-security-group-nicht erlaubt	Stellen Sie sicher, dass es sich bei den DB-Sicher heitsgruppen von Amazon Relationa l Database Service (Amazon RDS) um die Standards icherheitsgruppe handelt. Die Regel ist NON_COMPLIANT, wenn es DB-Sicher heitsgruppen gibt, die nicht die standardm äßige DB-Sicher heitsgruppe sind.
1.2.8	Die Netzwerks icherheitskontroll en (NSCs) werden konfiguriert und verwaltet. (PCI-DSS-v4.0)	ec2- transit-gateway-auto-vpc -attach-d eaktiviert	Stellen Sie sicher, dass bei Amazon Elastic Compute Cloud (Amazon EC2) Transit Gateways 'AutoAcceptSharedA ttachments' nicht aktiviert ist. Die Regel ist NON_COMPL IANT für ein Transit Gateway, wenn '' auf AutoAcceptSharedAt tachments 'aktiviert' gesetzt ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
1.2.8	Die Netzwerks icherheitskontroll en (NSCs) werden konfiguriert und verwaltet. (PCI-DSS-v4.0)	eks-endpoint-no-pu blic-Zugang	Stellen Sie sicher, dass der Amazon Elastic Kubernete s Service (Amazon EKS) -Endpunkt nicht öffentlich zugänglic h ist. Die Regel ist NON_COMPLIANT, wenn der Endpunkt öffentlich zugänglich ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
1.2.8	Die Netzwerks icherheitskontroll en (NSCs) werden konfiguriert und verwaltet. (PCI-DSS-v4.0)	restricted-ssh	Hinweis: Bei dieser Regel untersche iden sich die Regel-ID (INCOMING _SSH_DISABLED) und der Regelname (restricted-ssh). Stellen Sie sicher, dass auf den eingehenden SSH-Verkehr für die Sicherheitsgruppen zugegriffen werden kann. Die Regel ist COMPLIANT, wenn die IP-Adressen des eingehenden SSH-Datenverkehrs in den Sicherheitsgruppen eingeschränkt sind (CIDR ungleich 0.0.0.0/0 oder ::/0). Andernfalls ist sie NON_COMPLIANT.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
1.2.8	Die Netzwerks icherheitskontroll en (NSCs) werden konfiguriert und verwaltet. (PCI-DSS-v4.0)	appsync-associated-with-waf	Stellen Sie sicher, dass AWS AppSync APIs sie den AWS WAFv2 Web-Zugri ffskontrolllisten () zugeordnet sind. ACLs Die Regel ist NON_COMPL IANT für eine AWS AppSync API, wenn sie keiner Web-ACL zugeordnet ist.
1.2.8	Die Netzwerks icherheitskontroll en (NSCs) werden konfiguriert und verwaltet. (PCI-DSS-v4.0)	docdb-cluster-snap shot-public-verboten	Stellen Sie sicher, dass manuelle Cluster-Snapshots von Amazon DocumentDB nicht öffentlich sind. Die Regel ist NON_COMPLIANT, wenn manuelle Cluster-Snapshots von Amazon DocumentDB öffentlic h sind.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
1.2.8	Die Netzwerks icherheitskontroll en (NSCs) werden konfiguriert und verwaltet. (PCI-DSS-v4.0)	codebuild-project-source-repo-URL-Prüfung	Stellen Sie sicher, dass die URL des Bitbucket-Quell-Repositorys KEINE Anmeldeinformationen enthält oder nicht. Die Regel ist NON_COMPLIANT, wenn die URL Anmeldeinformationen enthält, und COMPLIANT, falls dies nicht der Fall ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
1.2.8	Die Netzwerks icherheitskontroll en (NSCs) werden konfiguriert und verwaltet. (PCI-DSS-v4.0)	elb-acm-certificate-required	Stellen Sie sicher, dass die Classic Load Balancers SSL-Zerti fikate verwenden, die vom AWS Certificate Manager bereitgestellt werden. Verwenden Sie zur Nutzung dieser Regel mit Ihrem Classic Load Balancer einen SSL- oder HTTPS-Listener. Hinweis: Diese Regel gilt nur für Classic Load Balancers. Mit dieser Regel werden keine Applicati on Load Balancer oder Network Load Balancer geprüft.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
1.2.8	Die Netzwerks icherheitskontroll en (NSCs) werden konfiguriert und verwaltet. (PCI-DSS-v4.0)	emr-block-public-a ccess	Stellen Sie sicher, dass für ein Konto bei Amazon EMR die Einstellungen zum Sperren des öffentlic hen Zugriffs aktiviert sind. Die Regel ist NON_COMPLIANT, wenn sie falsch BlockPublicSecurit yGroupRules ist, oder wenn sie wahr ist, sind andere Ports als Port 22 unter aufgeführt. Permitted PublicSecurityGrou pRuleRanges
1.2.8	Die Netzwerks icherheitskontroll en (NSCs) werden konfiguriert und verwaltet. (PCI-DSS-v4.0)	nacl-no-unrestricted-ssh-rdp	Stellen Sie sicher, dass die Standardp orts für eingehenden SSH/RDP-Datenverke hr für Netzwerkz ugriffskontrolllisten () eingeschränkt sind. NACLs Die Regel ist NON_COMPLIANT, wenn ein eingehender NACL-Eintrag für die Ports 22 oder 3389 einen CIDR-Block des Typs Quell-TCP oder -UDP zulässt.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
1.2.8	Die Netzwerks icherheitskontroll en (NSCs) werden konfiguriert und verwaltet. (PCI-DSS-v4.0)	waf-global-webacl-not-leer	Stellen Sie sicher, dass eine WAF Global Web ACL einige WAF-Regeln oder Regelgruppen enthält. Diese Regel ist NON_COMPLIANT, wenn eine globale Web-ACL keine WAF-Regel oder -Regelgru ppe enthält.
1.2.8	Die Netzwerks icherheitskontroll en (NSCs) werden konfiguriert und verwaltet. (PCI-DSS-v4.0)	waf-global-rulegroup-not-leer	Stellen Sie sicher, dass eine AWS WAF Classic-Regelgrupp e einige Regeln enthält. Die Regel ist NON_COMPLIANT, wenn innerhalb einer Regelgruppe keine Regeln vorhanden sind.
1.2.8	Die Netzwerks icherheitskontroll en (NSCs) werden konfiguriert und verwaltet. (PCI-DSS-v4.0)	waf-global-rule-not-leer	Stellen Sie sicher, dass eine globale AWS WAF-Regel einige Bedingungen enthält. Die Regel ist NON_COMPL IANT, wenn in der globalen WAF-Regel keine Bedingungen vorhanden sind.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
1.2.8	Die Netzwerks icherheitskontroll en (NSCs) werden konfiguriert und verwaltet. (PCI-DSS-v4.0)	ec2- -alle client-vpn-not-authorize	Stellen Sie sicher, dass die AWS Client-VPN-Autorisierungsre geln nicht den Verbindungszugriff für alle Clients autorisie ren. Die Regel ist NON_COMPLIANT, wenn 'AccessAll' vorhanden und auf true gesetzt ist.
1.2.8	Die Netzwerks icherheitskontroll en (NSCs) werden konfiguriert und verwaltet. (PCI-DSS-v4.0)	internet-gateway-a uthorized-vpc-nur	Stellen Sie sicher, dass Internet-Gateways an eine autorisierte virtuelle private Cloud (Amazon VPC) angeschlo ssen sind. Die Regel ist NON_COMPL IANT, wenn Internet-Gateways an eine nicht autorisierte VPC angehängt sind.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
1.2.8	Die Netzwerks icherheitskontroll en (NSCs) werden konfiguriert und verwaltet. (PCI-DSS-v4.0)	access-point-public-accesss3-Blöcke	Stellen Sie sicher, dass Amazon S3 S3-Zugriffspunkten die Einstellungen zum Blockieren des öffentlichen Zugriffs aktiviert sind. Die Regel ist NON_COMPLIANT, wenn die Einstellung zum Blockieren des öffentlichen Zugriffs für S3-Zugangspunkte nicht aktiviert ist.
1.2.8	Die Netzwerks icherheitskontroll en (NSCs) werden konfiguriert und verwaltet. (PCI-DSS-v4.0)	account-level-public-accesss3-Blöcke	Stellen Sie sicher, dass die erforderl ichen Einstellungen für die Sperrung des öffentlichen Zugriffs auf Kontoebene konfiguriert sind. Die Regel ist nur NON_COMPL IANT, wenn die unten festgeleg ten Felder nicht mit den entsprech enden Feldern im Konfigurationselement übereinstimmen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
1.3.1	Der Netzwerkzugriff zur und von der Karteninhaberdaten umgebung ist eingeschränkt. (PCI-DSS-v4.0)	api-gw-endpoint-type-überprüfen	Stellen Sie sicher, dass Amazon API Gateway APIs dem Typ entspricht, der im Regelparameter 'endpointConfigurationType' angegeben ist. Die Regel gibt NON_COMPLIANT zurück, wenn die REST-API nicht mit dem Endpunkttyp übereinstimmt, der im Regelparameter konfiguriert ist.
1.3.1	Der Netzwerkzugriff zur und von der Karteninhaberdaten umgebung ist eingeschränkt. (PCI-DSS-v4.0)	cloudfront-associated-with-waf	Stellen Sie sicher, dass CloudFront Amazon-Distributionen entweder mit Web Application Firewall (WAF) oder WAFv2 Web Access Control Lists (ACLs) verknüpft sind. Die Regel lautet NON_COMPLIANT, wenn eine CloudFront Distribution keiner WAF-Web-ACL zugeordnet ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
1.3.1	Der Netzwerkzugriff zur und von der Karteninhaberdaten umgebung ist eingeschränkt. (PCI-DSS-v4.0)	cloudfront-custom-ssl-certificate	Stellen Sie sicher, dass das mit einer CloudFront Amazon-Distribution verknüpfte Zertifikat nicht das Standard-SSL-Zertifikat ist. Die Regel lautet NON_COMPLIANT, wenn eine CloudFront Distribution das Standard-SSL-Zertifikat verwendet.
1.3.1	Der Netzwerkzugriff zur und von der Karteninhaberdaten umgebung ist eingeschränkt. (PCI-DSS-v4.0)	netfw-policy-default-action-fragment-Pakete	Stellen Sie sicher, dass eine AWS Netzwerk-Firewall-Richtlinie mit einer benutzerdefinierten statusfreien Standardaktion für fragmentierte Pakete konfiguriert ist. Die Regel ist NON_COMPLIANT, wenn die zustandslose Standardaktion für fragmentierte Pakete nicht mit der benutzerdefinierten Standardaktion übereinstimmt.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
1.3.1	Der Netzwerkzugriff zur und von der Karteninhaberdaten umgebung ist eingeschränkt. (PCI-DSS-v4.0)	rds-db-security-group-nicht erlaubt	Stellen Sie sicher, dass es sich bei den DB-Sicher heitsgruppen von Amazon Relationa l Database Service (Amazon RDS) um die Standards icherheitsgruppe handelt. Die Regel ist NON_COMPLIANT, wenn es DB-Sicher heitsgruppen gibt, die nicht die standardm äßige DB-Sicher heitsgruppe sind.
1.3.1	Der Netzwerkzugriff zur und von der Karteninhaberdaten umgebung ist eingeschränkt. (PCI-DSS-v4.0)	redshift-enhanced-vpc-routing-aktiviert	Stellen Sie sicher, dass Amazon Redshift Redshift-Cluster 'enhanced VpcRouting' aktiviert sind. Die Regel ist NON_COMPLIANT, wenn 'enhanced VpcRouting' nicht aktiviert ist oder wenn die Konfiguration nicht aktiviert ist. enhancedVpcRouting Feld ist 'falsch'.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
1.3.1	Der Netzwerkzugriff zur und von der Karteninhaberdaten umgebung ist eingeschränkt. (PCI-DSS-v4.0)	ec2- transit-gateway-auto-vpc -attach-deaktiviert	Stellen Sie sicher, dass bei Amazon Elastic Compute Cloud (Amazon EC2) Transit Gateways 'AutoAcceptSharedAttachments' nicht aktiviert ist. Die Regel ist NON_COMPLIANT für ein Transit Gateway, wenn '' auf AutoAcceptSharedAttachments 'aktiviert' gesetzt ist.
1.3.1	Der Netzwerkzugriff zur und von der Karteninhaberdaten umgebung ist eingeschränkt. (PCI-DSS-v4.0)	eks-endpoint-no-public-Zugang	Stellen Sie sicher, dass der Amazon Elastic Kubernetes Service (Amazon EKS) -Endpunkt nicht öffentlich zugänglich ist. Die Regel ist NON_COMPLIANT, wenn der Endpunkt öffentlich zugänglich ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
1.3.1	Der Netzwerkzugriff zur und von der Karteninhaberdaten umgebung ist eingeschränkt. (PCI-DSS-v4.0)	restricted-ssh	Hinweis: Bei dieser Regel untersche iden sich die Regel-ID (INCOMING _SSH_DISABLED) und der Regelname (restricted-ssh). Stellen Sie sicher, dass auf den eingehenden SSH-Verkehr für die Sicherheitsgruppen zugegriffen werden kann. Die Regel ist COMPLIANT, wenn die IP-Adressen des eingehenden SSH-Datenverkehrs in den Sicherheitsgruppen eingeschränkt sind (CIDR ungleich 0.0.0.0/0 oder ::/0). Andernfalls ist sie NON_COMPLIANT.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
1.3.1	Der Netzwerkzugriff zur und von der Karteninhaberdaten umgebung ist eingeschränkt. (PCI-DSS-v4.0)	appsync-associated-with-waf	Stellen Sie sicher, dass AWS AppSync APIs sie den AWS WAFv2 Web-Zugriffskontrolllisten () zugeordnet sind. ACLs Die Regel ist NON_COMPLIANT für eine AWS AppSync API, wenn sie keiner Web-ACL zugeordnet ist.
1.3.1	Der Netzwerkzugriff zur und von der Karteninhaberdaten umgebung ist eingeschränkt. (PCI-DSS-v4.0)	docdb-cluster-snapshot-public-verboten	Stellen Sie sicher, dass manuelle Cluster-Snapshots von Amazon DocumentDB nicht öffentlich sind. Die Regel ist NON_COMPLIANT, wenn manuelle Cluster-Snapshots von Amazon DocumentDB öffentlich sind.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
1.3.1	Der Netzwerkzugriff zur und von der Karteninhaberdaten umgebung ist eingeschränkt. (PCI-DSS-v4.0)	codebuild-project-source-repo-URL-Prüfung	Stellen Sie sicher, dass die URL des Bitbucket-Quell-Repositorys KEINE Anmeldeinformationen enthält oder nicht. Die Regel ist NON_COMPLIANT, wenn die URL Anmeldeinformationen enthält, und COMPLIANT, falls dies nicht der Fall ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
1.3.1	Der Netzwerkzugriff zur und von der Karteninhaberdaten umgebung ist eingeschränkt. (PCI-DSS-v4.0)	elb-acm-certificate-required	Stellen Sie sicher, dass die Classic Load Balancers SSL-Zerti fikate verwenden, die vom AWS Certificate Manager bereitgestellt werden. Verwenden Sie zur Nutzung dieser Regel mit Ihrem Classic Load Balancer einen SSL- oder HTTPS-Listener. Hinweis: Diese Regel gilt nur für Classic Load Balancers. Mit dieser Regel werden keine Applicati on Load Balancer oder Network Load Balancer geprüft.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
1.3.1	Der Netzwerkzugriff zur und von der Karteninhaberdaten umgebung ist eingeschränkt. (PCI-DSS-v4.0)	emr-block-public-access	Stellen Sie sicher, dass für ein Konto bei Amazon EMR die Einstellungen zum Sperren des öffentlichen Zugriffs aktiviert sind. Die Regel ist NON_COMPLIANT, wenn sie falsch BlockPublicSecurityGroupRules ist, oder wenn sie wahr ist, sind andere Ports als Port 22 unter aufgeführt. Permitted PublicSecurityGroupRuleRanges
1.3.1	Der Netzwerkzugriff zur und von der Karteninhaberdaten umgebung ist eingeschränkt. (PCI-DSS-v4.0)	nacl-no-unrestricted-ssh-rdp	Stellen Sie sicher, dass die Standardports für eingehenden SSH/RDP-Datenverkehr für Netzwerkzugriffskontrolllisten () eingeschränkt sind. NACLs Die Regel ist NON_COMPLIANT, wenn ein eingehender NACL-Eintrag für die Ports 22 oder 3389 einen CIDR-Block des Typs Quell-TCP oder -UDP zulässt.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
1.3.1	Der Netzwerkzugriff zur und von der Karteninhaberdaten umgebung ist eingeschränkt. (PCI-DSS-v4.0)	waf-global-webacl-not-leer	Stellen Sie sicher, dass eine WAF Global Web ACL einige WAF-Regeln oder Regelgruppen enthält. Diese Regel ist NON_COMPLIANT, wenn eine globale Web-ACL keine WAF-Regel oder -Regelgruppe enthält.
1.3.1	Der Netzwerkzugriff zur und von der Karteninhaberdaten umgebung ist eingeschränkt. (PCI-DSS-v4.0)	waf-global-rulegroup-not-leer	Stellen Sie sicher, dass eine AWS WAF Classic-Regelgruppe einige Regeln enthält. Die Regel ist NON_COMPLIANT, wenn innerhalb einer Regelgruppe keine Regeln vorhanden sind.
1.3.1	Der Netzwerkzugriff zur und von der Karteninhaberdaten umgebung ist eingeschränkt. (PCI-DSS-v4.0)	waf-global-rule-not-leer	Stellen Sie sicher, dass eine globale AWS WAF-Regel einige Bedingungen enthält. Die Regel ist NON_COMPLIANT, wenn in der globalen WAF-Regel keine Bedingungen vorhanden sind.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
1.3.1	Der Netzwerkzugriff zur und von der Karteninhaberdaten umgebung ist eingeschränkt. (PCI-DSS-v4.0)	ec2- -alle client-vpn-not-authorize	Stellen Sie sicher, dass die AWS Client-VPN-Autorisierungsregeln nicht den Verbindungszugriff für alle Clients autorisieren. Die Regel ist NON_COMPLIANT, wenn 'AccessAll' vorhanden und auf true gesetzt ist.
1.3.1	Der Netzwerkzugriff zur und von der Karteninhaberdaten umgebung ist eingeschränkt. (PCI-DSS-v4.0)	internet-gateway-authorized-vpc-nur	Stellen Sie sicher, dass Internet-Gateways an eine autorisierte virtuelle private Cloud (Amazon VPC) angeschlossen sind. Die Regel ist NON_COMPLIANT, wenn Internet-Gateways an eine nicht autorisierte VPC angehängt sind.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
1.3.1	Der Netzwerkzugriff zur und von der Karteninhaberdaten umgebung ist eingeschränkt. (PCI-DSS-v4.0)	access-point-public-accesss3-Blöcke	Stellen Sie sicher, dass Amazon S3 S3-Zugriffspunkten die Einstellungen zum Blockieren des öffentlichen Zugriffs aktiviert sind. Die Regel ist NON_COMPLIANT, wenn die Einstellung zum Blockieren des öffentlichen Zugriffs für S3-Zugangspunkte nicht aktiviert ist.
1.3.1	Der Netzwerkzugriff zur und von der Karteninhaberdaten umgebung ist eingeschränkt. (PCI-DSS-v4.0)	account-level-public-accesss3-Blöcke	Stellen Sie sicher, dass die erforderl ichen Einstellungen für die Sperrung des öffentlichen Zugriffs auf Kontoebene konfiguriert sind. Die Regel ist nur NON_COMPL IANT, wenn die unten festgeleg ten Felder nicht mit den entsprech enden Feldern im Konfigurationselement übereinstimmen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
1.3.2	Der Netzwerkzugriff zur und von der Karteninhaberdaten umgebung ist eingeschränkt. (PCI-DSS-v4.0)	api-gw-endpoint-type-überprüfen	Stellen Sie sicher, dass Amazon API Gateway APIs dem Typ entspricht, der im Regelparameter 'endpointConfigurationType' angegeben ist. Die Regel gibt NON_COMPLIANT zurück, wenn die REST-API nicht mit dem Endpunkttyp übereinstimmt, der im Regelparameter konfiguriert ist.
1.3.2	Der Netzwerkzugriff zur und von der Karteninhaberdaten umgebung ist eingeschränkt. (PCI-DSS-v4.0)	cloudfront-associated-with-waf	Stellen Sie sicher, dass CloudFront Amazon-Distributionen entweder mit Web Application Firewall (WAF) oder WAFv2 Web Access Control Lists (ACLs) verknüpft sind. Die Regel lautet NON_COMPLIANT, wenn eine CloudFront Distribution keiner WAF-Web-ACL zugeordnet ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
1.3.2	Der Netzwerkzugriff zur und von der Karteninhaberdaten umgebung ist eingeschränkt. (PCI-DSS-v4.0)	cloudfront-custom-ssl-certificate	Stellen Sie sicher, dass das mit einer CloudFront Amazon-Distribution verknüpfte Zertifikat nicht das Standard-SSL-Zertifikat ist. Die Regel lautet NON_COMPLIANT, wenn eine CloudFront Distribution das Standard-SSL-Zertifikat verwendet.
1.3.2	Der Netzwerkzugriff zur und von der Karteninhaberdaten umgebung ist eingeschränkt. (PCI-DSS-v4.0)	netfw-policy-default-action-fragment-Pakete	Stellen Sie sicher, dass eine AWS Netzwerk-Firewall-Richtlinie mit einer benutzerdefinierten statusfreien Standardaktion für fragmentierte Pakete konfiguriert ist. Die Regel ist NON_COMPLIANT, wenn die zustandslose Standardaktion für fragmentierte Pakete nicht mit der benutzerdefinierten Standardaktion übereinstimmt.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
1.3.2	Der Netzwerkzugriff zur und von der Karteninhaberdaten umgebung ist eingeschränkt. (PCI-DSS-v4.0)	rds-db-security-group-nicht erlaubt	Stellen Sie sicher, dass es sich bei den DB-Sicher heitsgruppen von Amazon Relationa l Database Service (Amazon RDS) um die Standards icherheitsgruppe handelt. Die Regel ist NON_COMPLIANT, wenn es DB-Sicher heitsgruppen gibt, die nicht die standardm äßige DB-Sicher heitsgruppe sind.
1.3.2	Der Netzwerkzugriff zur und von der Karteninhaberdaten umgebung ist eingeschränkt. (PCI-DSS-v4.0)	redshift-enhanced-vpc-routing-aktiviert	Stellen Sie sicher, dass Amazon Redshift Redshift-Cluster 'enhanced VpcRouting' aktiviert sind. Die Regel ist NON_COMPLIANT, wenn 'enhanced VpcRouting' nicht aktiviert ist oder wenn die Konfiguration nicht aktiviert ist. enhancedVpcRouting Feld ist 'falsch'.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
1.3.2	Der Netzwerkzugriff zur und von der Karteninhaberdaten umgebung ist eingeschränkt. (PCI-DSS-v4.0)	ec2- transit-gateway-auto-vpc -attach-deaktiviert	Stellen Sie sicher, dass bei Amazon Elastic Compute Cloud (Amazon EC2) Transit Gateways 'AutoAcceptSharedAttachments' nicht aktiviert ist. Die Regel ist NON_COMPLIANT für ein Transit Gateway, wenn '' auf AutoAcceptSharedAttachments 'aktiviert' gesetzt ist.
1.3.2	Der Netzwerkzugriff zur und von der Karteninhaberdaten umgebung ist eingeschränkt. (PCI-DSS-v4.0)	eks-endpoint-no-public-Zugang	Stellen Sie sicher, dass der Amazon Elastic Kubernetes Service (Amazon EKS) -Endpunkt nicht öffentlich zugänglich ist. Die Regel ist NON_COMPLIANT, wenn der Endpunkt öffentlich zugänglich ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
1.3.2	Der Netzwerkzugriff zur und von der Karteninhaberdaten umgebung ist eingeschränkt. (PCI-DSS-v4.0)	restricted-ssh	Hinweis: Bei dieser Regel untersche iden sich die Regel-ID (INCOMING _SSH_DISABLED) und der Regelname (restricted-ssh). Stellen Sie sicher, dass auf den eingehenden SSH-Verkehr für die Sicherheitsgruppen zugegriffen werden kann. Die Regel ist COMPLIANT, wenn die IP-Adressen des eingehenden SSH-Datenverkehrs in den Sicherheitsgruppen eingeschränkt sind (CIDR ungleich 0.0.0.0/0 oder ::/0). Andernfalls ist sie NON_COMPLIANT.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
1.3.2	Der Netzwerkzugriff zur und von der Karteninhaberdaten umgebung ist eingeschränkt. (PCI-DSS-v4.0)	appsync-associated-with-waf	Stellen Sie sicher, dass AWS AppSync APIs sie den AWS WAFv2 Web-Zugriffskontrolllisten () zugeordnet sind. ACLs Die Regel ist NON_COMPLIANT für eine AWS AppSync API, wenn sie keiner Web-ACL zugeordnet ist.
1.3.2	Der Netzwerkzugriff zur und von der Karteninhaberdaten umgebung ist eingeschränkt. (PCI-DSS-v4.0)	docdb-cluster-snapshot-public-verboten	Stellen Sie sicher, dass manuelle Cluster-Snapshots von Amazon DocumentDB nicht öffentlich sind. Die Regel ist NON_COMPLIANT, wenn manuelle Cluster-Snapshots von Amazon DocumentDB öffentlich sind.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
1.3.2	Der Netzwerkzugriff zur und von der Karteninhaberdaten umgebung ist eingeschränkt. (PCI-DSS-v4.0)	codebuild-project-source-repo-URL-Prüfung	Stellen Sie sicher, dass die URL des Bitbucket-Quell-Repositorys KEINE Anmeldeinformationen enthält oder nicht. Die Regel ist NON_COMPLIANT, wenn die URL Anmeldeinformationen enthält, und COMPLIANT, falls dies nicht der Fall ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
1.3.2	Der Netzwerkzugriff zur und von der Karteninhaberdaten umgebung ist eingeschränkt. (PCI-DSS-v4.0)	elb-acm-certificate-required	Stellen Sie sicher, dass die Classic Load Balancers SSL-Zerti fikate verwenden, die vom AWS Certificate Manager bereitgestellt werden. Verwenden Sie zur Nutzung dieser Regel mit Ihrem Classic Load Balancer einen SSL- oder HTTPS-Listener. Hinweis: Diese Regel gilt nur für Classic Load Balancers. Mit dieser Regel werden keine Applicati on Load Balancer oder Network Load Balancer geprüft.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
1.3.2	Der Netzwerkzugriff zur und von der Karteninhaberdaten umgebung ist eingeschränkt. (PCI-DSS-v4.0)	emr-block-public-access	Stellen Sie sicher, dass für ein Konto bei Amazon EMR die Einstellungen zum Sperren des öffentlichen Zugriffs aktiviert sind. Die Regel ist NON_COMPLIANT, wenn sie falsch BlockPublicSecurityGroupRules ist, oder wenn sie wahr ist, sind andere Ports als Port 22 unter aufgeführt. Permitted PublicSecurityGroupRuleRanges
1.3.2	Der Netzwerkzugriff zur und von der Karteninhaberdaten umgebung ist eingeschränkt. (PCI-DSS-v4.0)	nacl-no-unrestricted-ssh-rdp	Stellen Sie sicher, dass die Standardports für eingehenden SSH/RDP-Datenverkehr für Netzwerkzugriffskontrolllisten () eingeschränkt sind. NACLs Die Regel ist NON_COMPLIANT, wenn ein eingehender NACL-Eintrag für die Ports 22 oder 3389 einen CIDR-Block des Typs Quell-TCP oder -UDP zulässt.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
1.3.2	Der Netzwerkzugriff zur und von der Karteninhaberdaten umgebung ist eingeschränkt. (PCI-DSS-v4.0)	waf-global-webacl-not-leer	Stellen Sie sicher, dass eine WAF Global Web ACL einige WAF-Regeln oder Regelgruppen enthält. Diese Regel ist NON_COMPLIANT, wenn eine globale Web-ACL keine WAF-Regel oder -Regelgruppe enthält.
1.3.2	Der Netzwerkzugriff zur und von der Karteninhaberdaten umgebung ist eingeschränkt. (PCI-DSS-v4.0)	waf-global-rulegroup-not-leer	Stellen Sie sicher, dass eine AWS WAF Classic-Regelgruppe einige Regeln enthält. Die Regel ist NON_COMPLIANT, wenn innerhalb einer Regelgruppe keine Regeln vorhanden sind.
1.3.2	Der Netzwerkzugriff zur und von der Karteninhaberdaten umgebung ist eingeschränkt. (PCI-DSS-v4.0)	waf-global-rule-not-leer	Stellen Sie sicher, dass eine globale AWS WAF-Regel einige Bedingungen enthält. Die Regel ist NON_COMPLIANT, wenn in der globalen WAF-Regel keine Bedingungen vorhanden sind.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
1.3.2	Der Netzwerkzugriff zur und von der Karteninhaberdaten umgebung ist eingeschränkt. (PCI-DSS-v4.0)	ec2- -alle client-vpn-not-authorize	Stellen Sie sicher, dass die AWS Client-VPN-Autorisierungsregeln nicht den Verbindungszugriff für alle Clients autorisieren. Die Regel ist NON_COMPLIANT, wenn 'AccessAll' vorhanden und auf true gesetzt ist.
1.3.2	Der Netzwerkzugriff zur und von der Karteninhaberdaten umgebung ist eingeschränkt. (PCI-DSS-v4.0)	internet-gateway-authorized-vpc-nur	Stellen Sie sicher, dass Internet-Gateways an eine autorisierte virtuelle private Cloud (Amazon VPC) angeschlossen sind. Die Regel ist NON_COMPLIANT, wenn Internet-Gateways an eine nicht autorisierte VPC angehängt sind.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
1.3.2	Der Netzwerkzugriff zur und von der Karteninhaberdaten umgebung ist eingeschränkt. (PCI-DSS-v4.0)	access-point-public-accesss3-Blöcke	Stellen Sie sicher, dass Amazon S3 S3-Zugriffspunkten die Einstellungen zum Blockieren des öffentlichen Zugriffs aktiviert sind. Die Regel ist NON_COMPLIANT, wenn die Einstellung zum Blockieren des öffentlichen Zugriffs für S3-Zugangspunkte nicht aktiviert ist.
1.3.2	Der Netzwerkzugriff zur und von der Karteninhaberdaten umgebung ist eingeschränkt. (PCI-DSS-v4.0)	account-level-public-accesss3-Blöcke	Stellen Sie sicher, dass die erforderl ichen Einstellungen für die Sperrung des öffentlichen Zugriffs auf Kontoebene konfiguriert sind. Die Regel ist nur NON_COMPL IANT, wenn die unten festgeleg ten Felder nicht mit den entsprech enden Feldern im Konfigurationselement übereinstimmen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
1.4.1	Netzwerkverbindungen zwischen vertrauenswürdigen und nicht vertrauenswürdigen Netzwerken werden kontrolliert. (PCI-DSS-v4.0)	api-gw-endpoint-type-überprüfen	Stellen Sie sicher, dass Amazon API Gateway APIs dem Typ entspricht, der im Regelparameter 'endpointConfigurationType' angegeben ist. Die Regel gibt NON_COMPLIANT zurück, wenn die REST-API nicht mit dem Endpunkttyp übereinstimmt, der im Regelparameter konfiguriert ist.
1.4.1	Netzwerkverbindungen zwischen vertrauenswürdigen und nicht vertrauenswürdigen Netzwerken werden kontrolliert. (PCI-DSS-v4.0)	redshift-enhanced-vpc-routing-aktiviert	Stellen Sie sicher, dass Amazon Redshift Redshift-Cluster 'enhancedVpcRouting' aktiviert sind. Die Regel ist NON_COMPLIANT, wenn 'enhancedVpcRouting' nicht aktiviert ist oder wenn die Konfiguration nicht aktiviert ist. enhancedVpcRouting Feld ist 'falsch'.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
1.4.1	Netzwerkverbindungen zwischen vertrauenswürdigen und nicht vertrauenswürdigen Netzwerken werden kontrolliert. (PCI-DSS-v4.0)	internet-gateway-authorized-vpc-nur	Stellen Sie sicher, dass Internet-Gateways an eine autorisierte virtuelle private Cloud (Amazon VPC) angeschlossen sind. Die Regel ist NON_COMPLIANT, wenn Internet-Gateways an eine nicht autorisierte VPC angehängt sind.
1.4.2	Netzwerkverbindungen zwischen vertrauenswürdigen und nicht vertrauenswürdigen Netzwerken werden kontrolliert. (PCI-DSS-v4.0)	api-gw-endpoint-type-überprüfen	Stellen Sie sicher, dass Amazon API Gateway APIs dem Typ entspricht, der im Regelparameter 'endpointConfigurationType' angegeben ist. Die Regel gibt NON_COMPLIANT zurück, wenn die REST-API nicht mit dem Endpunkttyp übereinstimmt, der im Regelparameter konfiguriert ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
1.4.2	Netzwerkverbindungen zwischen vertrauenswürdigen und nicht vertrauenswürdigen Netzwerken werden kontrolliert. (PCI-DSS-v4.0)	cloudfront-associated-with-waf	Stellen Sie sicher, dass CloudFront Amazon-Distributionen entweder mit Web Application Firewall (WAF) oder WAFv2 Web Access Control Lists (ACLs) verknüpft sind. Die Regel lautet NON_COMPLIANT, wenn eine CloudFront Distribution keiner WAF-Web-ACL zugeordnet ist.
1.4.2	Netzwerkverbindungen zwischen vertrauenswürdigen und nicht vertrauenswürdigen Netzwerken werden kontrolliert. (PCI-DSS-v4.0)	cloudfront-custom-ssl-certificate	Stellen Sie sicher, dass das mit einer CloudFront Amazon-Distribution verknüpfte Zertifikat nicht das Standard-SSL-Zertifikat ist. Die Regel lautet NON_COMPLIANT, wenn eine CloudFront Distribution das Standard-SSL-Zertifikat verwendet.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
1.4.2	Netzwerkverbindungen zwischen vertrauenswürdigen und nicht vertrauenswürdigen Netzwerken werden kontrolliert. (PCI-DSS-v4.0)	netfw-policy-default-action-fragment-Pakete	Stellen Sie sicher, dass eine AWS Netzwerk-Firewall-Richtlinie mit einer benutzerdefinierten statusfreien Standardaktion für fragmentierte Pakete konfiguriert ist. Die Regel ist NON_COMPLIANT, wenn die zustandslose Standardaktion für fragmentierte Pakete nicht mit der benutzerdefinierten Standardaktion übereinstimmt.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
1.4.2	Netzwerkverbindungen zwischen vertrauenswürdigen und nicht vertrauenswürdigen Netzwerken werden kontrolliert. (PCI-DSS-v4.0)	rds-db-security-group-nicht erlaubt	Stellen Sie sicher, dass es sich bei den DB-Sicherheitsgruppen von Amazon Relational Database Service (Amazon RDS) um die Standardsicherheitsgruppe handelt. Die Regel ist NON_COMPLIANT, wenn es DB-Sicherheitsgruppen gibt, die nicht die standardmäßige DB-Sicherheitsgruppe sind.
1.4.2	Netzwerkverbindungen zwischen vertrauenswürdigen und nicht vertrauenswürdigen Netzwerken werden kontrolliert. (PCI-DSS-v4.0)	redshift-enhanced-vpc-routing-aktiviert	Stellen Sie sicher, dass Amazon Redshift Redshift-Cluster 'enhancedVpcRouting' aktiviert sind. Die Regel ist NON_COMPLIANT, wenn 'enhancedVpcRouting' nicht aktiviert ist oder wenn die Konfiguration nicht aktiviert ist. enhancedVpcRouting Feld ist 'falsch'.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
1.4.2	Netzwerkverbindungen zwischen vertrauenswürdigen und nicht vertrauenswürdigen Netzwerken werden kontrolliert. (PCI-DSS-v4.0)	ec2- transit-gateway-auto-vpc -attach-deaktiviert	Stellen Sie sicher, dass bei Amazon Elastic Compute Cloud (Amazon EC2) Transit Gateways 'AutoAcceptSharedAttachments' nicht aktiviert ist. Die Regel ist NON_COMPLIANT für ein Transit Gateway, wenn '' auf AutoAcceptSharedAttachments 'aktiviert' gesetzt ist.
1.4.2	Netzwerkverbindungen zwischen vertrauenswürdigen und nicht vertrauenswürdigen Netzwerken werden kontrolliert. (PCI-DSS-v4.0)	eks-endpoint-no-public-Zugang	Stellen Sie sicher, dass der Amazon Elastic Kubernetes Service (Amazon EKS) -Endpunkt nicht öffentlich zugänglich ist. Die Regel ist NON_COMPLIANT, wenn der Endpunkt öffentlich zugänglich ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
1.4.2	Netzwerkverbindungen zwischen vertrauenswürdigen und nicht vertrauenswürdigen Netzwerken werden kontrolliert. (PCI-DSS-v4.0)	restricted-ssh	Hinweis: Bei dieser Regel unterscheiden sich die Regel-ID (INCOMING_SSH_DISABLED) und der Regelname (restricted-ssh). Stellen Sie sicher, dass auf den eingehenden SSH-Verkehr für die Sicherheitsgruppen zugegriffen werden kann. Die Regel ist COMPLIANT, wenn die IP-Adressen des eingehenden SSH-Datenverkehrs in den Sicherheitsgruppen eingeschränkt sind (CIDR ungleich 0.0.0.0/0 oder ::/0). Andernfalls ist sie NON_COMPLIANT.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
1.4.2	Netzwerkverbindungen zwischen vertrauenswürdigen und nicht vertrauenswürdigen Netzwerken werden kontrolliert. (PCI-DSS-v4.0)	appsync-associated-with-waf	Stellen Sie sicher, dass AWS AppSync APIs sie den AWS WAFv2 Web-Zugriffskontrolllisten () zugeordnet sind. ACLs Die Regel ist NON_COMPLIANT für eine AWS AppSync API, wenn sie keiner Web-ACL zugeordnet ist.
1.4.2	Netzwerkverbindungen zwischen vertrauenswürdigen und nicht vertrauenswürdigen Netzwerken werden kontrolliert. (PCI-DSS-v4.0)	docdb-cluster-snapshot-public-verboten	Stellen Sie sicher, dass manuelle Cluster-Snapshots von Amazon DocumentDB nicht öffentlich sind. Die Regel ist NON_COMPLIANT, wenn manuelle Cluster-Snapshots von Amazon DocumentDB öffentlich sind.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
1.4.2	Netzwerkverbindungen zwischen vertrauenswürdigen und nicht vertrauenswürdigen Netzwerken werden kontrolliert. (PCI-DSS-v4.0)	codebuild-project-source-repo-URL-Prüfung	Stellen Sie sicher, dass die URL des Bitbucket-Quell-Repositorys KEINE Anmeldeinformationen enthält oder nicht. Die Regel ist NON_COMPLIANT, wenn die URL Anmeldeinformationen enthält, und COMPLIANT, falls dies nicht der Fall ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
1.4.2	Netzwerkverbindungen zwischen vertrauenswürdigen und nicht vertrauenswürdigen Netzwerken werden kontrolliert. (PCI-DSS-v4.0)	elb-acm-certificate-required	Stellen Sie sicher, dass die Classic Load Balancers SSL-Zertifikate verwenden, die vom AWS Certificate Manager bereitgestellt werden. Verwenden Sie zur Nutzung dieser Regel mit Ihrem Classic Load Balancer einen SSL- oder HTTPS-Listener. Hinweis: Diese Regel gilt nur für Classic Load Balancers. Mit dieser Regel werden keine Application Load Balancer oder Network Load Balancer geprüft.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
1.4.2	Netzwerkverbindungen zwischen vertrauenswürdigen und nicht vertrauenswürdigen Netzwerken werden kontrolliert. (PCI-DSS-v4.0)	emr-block-public-access	Stellen Sie sicher, dass für ein Konto bei Amazon EMR die Einstellungen zum Sperren des öffentlichen Zugriffs aktiviert sind. Die Regel ist NON_COMPLIANT, wenn sie falsch BlockPublicSecurityGroupRules ist, oder wenn sie wahr ist, sind andere Ports als Port 22 unter aufgeführt. Permitted PublicSecurityGroupRuleRanges
1.4.2	Netzwerkverbindungen zwischen vertrauenswürdigen und nicht vertrauenswürdigen Netzwerken werden kontrolliert. (PCI-DSS-v4.0)	nacl-no-unrestricted-ssh-rdp	Stellen Sie sicher, dass die Standardports für eingehenden SSH/RDP-Datenverkehr für Netzwerkzugriffskontrolllisten () eingeschränkt sind. NACLs Die Regel ist NON_COMPLIANT, wenn ein eingehender NACL-Eintrag für die Ports 22 oder 3389 einen CIDR-Block des Typs Quell-TCP oder -UDP zulässt.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
1.4.2	Netzwerkverbindungen zwischen vertrauenswürdigen und nicht vertrauenswürdigen Netzwerken werden kontrolliert. (PCI-DSS-v4.0)	waf-global-webacl-not-leer	Stellen Sie sicher, dass eine WAF Global Web ACL einige WAF-Regeln oder Regelgruppen enthält. Diese Regel ist NON_COMPLIANT, wenn eine globale Web-ACL keine WAF-Regel oder -Regelgruppe enthält.
1.4.2	Netzwerkverbindungen zwischen vertrauenswürdigen und nicht vertrauenswürdigen Netzwerken werden kontrolliert. (PCI-DSS-v4.0)	waf-global-rulegroup-not-leer	Stellen Sie sicher, dass eine AWS WAF Classic-Regelgruppe einige Regeln enthält. Die Regel ist NON_COMPLIANT, wenn innerhalb einer Regelgruppe keine Regeln vorhanden sind.
1.4.2	Netzwerkverbindungen zwischen vertrauenswürdigen und nicht vertrauenswürdigen Netzwerken werden kontrolliert. (PCI-DSS-v4.0)	waf-global-rule-not-leer	Stellen Sie sicher, dass eine globale AWS WAF-Regel einige Bedingungen enthält. Die Regel ist NON_COMPLIANT, wenn in der globalen WAF-Regel keine Bedingungen vorhanden sind.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
1.4.2	Netzwerkverbindungen zwischen vertrauenswürdigen und nicht vertrauenswürdigen Netzwerken werden kontrolliert. (PCI-DSS-v4.0)	ec2- -alle client-vpn-not-authorize	Stellen Sie sicher, dass die AWS Client-VPN-Autorisierungsregeln nicht den Verbindungszugriff für alle Clients autorisieren. Die Regel ist NON_COMPLIANT, wenn 'AccessAll' vorhanden und auf true gesetzt ist.
1.4.2	Netzwerkverbindungen zwischen vertrauenswürdigen und nicht vertrauenswürdigen Netzwerken werden kontrolliert. (PCI-DSS-v4.0)	internet-gateway-authorized-vpc-nur	Stellen Sie sicher, dass Internet-Gateways an eine autorisierte virtuelle private Cloud (Amazon VPC) angeschlossen sind. Die Regel ist NON_COMPLIANT, wenn Internet-Gateways an eine nicht autorisierte VPC angehängt sind.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
1.4.2	Netzwerkverbindungen zwischen vertrauenswürdigen und nicht vertrauenswürdigen Netzwerken werden kontrolliert. (PCI-DSS-v4.0)	access-point-public-accesss3-Blöcke	Stellen Sie sicher, dass Amazon S3 S3-Zugriffspunkten die Einstellungen zum Blockieren des öffentlichen Zugriffs aktiviert sind. Die Regel ist NON_COMPLIANT, wenn die Einstellung zum Blockieren des öffentlichen Zugriffs für S3-Zugangspunkte nicht aktiviert ist.
1.4.2	Netzwerkverbindungen zwischen vertrauenswürdigen und nicht vertrauenswürdigen Netzwerken werden kontrolliert. (PCI-DSS-v4.0)	account-level-public-accesss3-Blöcke	Stellen Sie sicher, dass die erforderlichen Einstellungen für die Sperrung des öffentlichen Zugriffs auf Kontoebene konfiguriert sind. Die Regel ist nur NON_COMPLIANT, wenn die unten festgelegten Felder nicht mit den entsprechenden Feldern im Konfigurationselement übereinstimmen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
1.4.3	Netzwerkverbindungen zwischen vertrauenswürdigen und nicht vertrauenswürdigen Netzwerken werden kontrolliert. (PCI-DSS-v4.0)	netfw-policy-default-action-fragment-Pakete	Stellen Sie sicher, dass eine AWS Netzwerk-Firewall-Richtlinie mit einer benutzerdefinierten statusfreien Standardaktion für fragmentierte Pakete konfiguriert ist. Die Regel ist NON_COMPLIANT, wenn die zustandslose Standardaktion für fragmentierte Pakete nicht mit der benutzerdefinierten Standardaktion übereinstimmt.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
1.4.3	Netzwerkverbindungen zwischen vertrauenswürdigen und nicht vertrauenswürdigen Netzwerken werden kontrolliert. (PCI-DSS-v4.0)	netfw-policy-default-action-fragment-Pakete	Stellen Sie sicher, dass eine AWS Netzwerk-Firewall-Richtlinie mit einer benutzerdefinierten statusfreien Standardaktion für fragmentierte Pakete konfiguriert ist. Die Regel ist NON_COMPLIANT, wenn die zustandslose Standardaktion für fragmentierte Pakete nicht mit der benutzerdefinierten Standardaktion übereinstimmt.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
1.4.3	Netzwerkverbindungen zwischen vertrauenswürdigen und nicht vertrauenswürdigen Netzwerken werden kontrolliert. (PCI-DSS-v4.0)	netfw-policy-default-action-vollständige Pakete	Stellen Sie sicher, dass eine AWS Netzwerk-Firewall-Richtlinie mit einer benutzerdefinierten statusfreien Standardaktion für vollständige Pakete konfiguriert ist. Diese Regel ist NON_COMPLIANT, wenn die zustandslose Standardaktion für vollständige Pakete nicht mit der benutzerdefinierten statuslosen Standardaktion übereinstimmt.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
1.4.4	Netzwerkverbindungen zwischen vertrauenswürdigen und nicht vertrauenswürdigen Netzwerken werden kontrolliert. (PCI-DSS-v4.0)	api-gw-endpoint-type-überprüfen	Stellen Sie sicher, dass Amazon API Gateway APIs dem Typ entspricht, der im Regelparameter 'endpointConfigurationType' angegeben ist. Die Regel gibt NON_COMPLIANT zurück, wenn die REST-API nicht mit dem Endpunkttyp übereinstimmt, der im Regelparameter konfiguriert ist.
1.4.4	Netzwerkverbindungen zwischen vertrauenswürdigen und nicht vertrauenswürdigen Netzwerken werden kontrolliert. (PCI-DSS-v4.0)	redshift-enhanced-vpc-routing-aktiviert	Stellen Sie sicher, dass Amazon Redshift Redshift-Cluster 'enhancedVpcRouting' aktiviert sind. Die Regel ist NON_COMPLIANT, wenn 'enhancedVpcRouting' nicht aktiviert ist oder wenn die Konfiguration nicht aktiviert ist. enhancedVpcRouting Feld ist 'falsch'.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
1.4.4	Netzwerkverbindungen zwischen vertrauenswürdigen und nicht vertrauenswürdigen Netzwerken werden kontrolliert. (PCI-DSS-v4.0)	internet-gateway-authorized-vpc-nur	Stellen Sie sicher, dass Internet-Gateways an eine autorisierte virtuelle private Cloud (Amazon VPC) angeschlossen sind. Die Regel ist NON_COMPLIANT, wenn Internet-Gateways an eine nicht autorisierte VPC angehängt sind.
1.4.5	Netzwerkverbindungen zwischen vertrauenswürdigen und nicht vertrauenswürdigen Netzwerken werden kontrolliert. (PCI-DSS-v4.0)	ecs-task-definition-pid-Modusprüfung	Stellen Sie sicher, dass ECSTask Definitionen so konfiguriert sind, dass sie den Prozess-Namespace eines Hosts mit seinen Amazon Elastic Container Service (Amazon ECS) -Containern gemeinsam nutzen. Die Regel lautet NON_COMPLIANT, wenn der PidMode-Parameter auf „host“ gesetzt ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
1.4.5	Netzwerkverbindungen zwischen vertrauenswürdigen und nicht vertrauenswürdigen Netzwerken werden kontrolliert. (PCI-DSS-v4.0)	ec2- deaktiviert launch-template-public-ip	Stellen Sie sicher, dass Amazon EC2 Launch Templates nicht so eingerichtet sind, dass Netzwerkschnittstellen öffentliche IP-Adressen zugewiesen werden. Die Regel lautet NON_COMPLIANT, wenn die Standardversion einer EC2 Startvorlage mindestens eine Netzwerkschnittstelle hat, bei der '' auf 'trueAssociatePublicIpAddress' gesetzt ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
1.5.1	Risiken für das CDE, die von Computergeräten ausgehen, die eine Verbindung sowohl mit nicht vertrauenswürdigen Netzwerken als auch mit dem CDE herstellen können, werden gemindert. (PCI-DSS-v4.0)	api-gw-endpoint-type-überprüfen	Stellen Sie sicher, dass Amazon API Gateway APIs dem Typ entspricht, der im Regelparameter 'endpointConfigurationType' angegeben ist. Die Regel gibt NON_COMPLIANT zurück, wenn die REST-API nicht mit dem Endpunkttyp übereinstimmt, der im Regelparameter konfiguriert ist.
1.5.1	Risiken für das CDE, die von Computergeräten ausgehen, die sowohl mit nicht vertrauenswürdigen Netzwerken als auch mit dem CDE verbunden werden können, werden gemindert. (PCI-DSS-v4.0)	cloudfront-associated-with-waf	Stellen Sie sicher, dass CloudFront Amazon-Distributionen entweder mit Web Application Firewall (WAF) oder WAFv2 Web Access Control Lists (ACLs) verknüpft sind. Die Regel lautet NON_COMPLIANT, wenn eine CloudFront Distribution keiner WAF-Web-ACL zugeordnet ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
1.5.1	Risiken für das CDE, die von Computergeräten ausgehen, die eine Verbindung sowohl mit nicht vertrauenswürdigen Netzwerken als auch mit dem CDE herstellen können, werden gemindert. (PCI-DSS-v4.0)	cloudfront-custom-ssl-certificate	Stellen Sie sicher, dass das mit einer CloudFront Amazon-Distribution verknüpfte Zertifikat nicht das Standard-SSL-Zertifikat ist. Die Regel lautet NON_COMPLIANT, wenn eine CloudFront Distribution das Standard-SSL-Zertifikat verwendet.
1.5.1	Die Risiken für das CDE, die von Computergeräten ausgehen, die sowohl mit nicht vertrauenswürdigen Netzwerken als auch mit dem CDE verbunden werden können, werden gemindert. (PCI-DSS-v4.0)	netfw-policy-default-action-fragment-Pakete	Stellen Sie sicher, dass eine AWS Netzwerk-Firewall-Richtlinie mit einer benutzerdefinierten statusfreien Standardaktion für fragmentierte Pakete konfiguriert ist. Die Regel ist NON_COMPLIANT, wenn die zustandslose Standardaktion für fragmentierte Pakete nicht mit der benutzerdefinierten Standardaktion übereinstimmt.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
1.5.1	Risiken für das CDE, die von Computerg eräten ausgehen, die eine Verbindun g sowohl mit nicht vertrauenswürdigen Netzwerken als auch mit dem CDE herstellen können, werden gemindert. (PCI-DSS-v4.0)	rds-db-security-group-nicht erlaubt	Stellen Sie sicher, dass es sich bei den DB-Sicher heitsgruppen von Amazon Relationa l Database Service (Amazon RDS) um die Standards icherheitsgruppe handelt. Die Regel ist NON_COMPLIANT, wenn es DB-Sicher heitsgruppen gibt, die nicht die standardm äßige DB-Sicher heitsgruppe sind.
1.5.1	Risiken für das CDE, die von Computerg eräten ausgehen, die eine Verbindun g sowohl mit nicht vertrauenswürdigen Netzwerken als auch mit dem CDE herstellen können, werden gemindert. (PCI-DSS-v4.0)	ec2- transit-gateway-auto-vpc -attach-d eaktiviert	Stellen Sie sicher, dass bei Amazon Elastic Compute Cloud (Amazon EC2) Transit Gateways 'AutoAcceptSharedA ttachments' nicht aktiviert ist. Die Regel ist NON_COMPL IANT für ein Transit Gateway, wenn '' auf AutoAcceptSharedAt tachments 'aktiviert' gesetzt ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
1.5.1	Risiken für das CDE, die von Computergeräten ausgehen, die eine Verbindung sowohl mit nicht vertrauenswürdigen Netzwerken als auch mit dem CDE herstellen können, werden gemindert. (PCI-DSS-v4.0)	eks-endpoint-no-public-Zugang	Stellen Sie sicher, dass der Amazon Elastic Kubernetes Service (Amazon EKS) -Endpunkt nicht öffentlich zugänglich ist. Die Regel ist NON_COMPLIANT, wenn der Endpunkt öffentlich zugänglich ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
1.5.1	Risiken für das CDE, die von Computergeräten ausgehen, die eine Verbindung sowohl mit nicht vertrauenswürdigen Netzwerken als auch mit dem CDE herstellen können, werden gemindert. (PCI-DSS-v4.0)	restricted-ssh	Hinweis: Bei dieser Regel unterscheiden sich die Regel-ID (INCOMING_SSH_DISABLED) und der Regelname (restricted-ssh). Stellen Sie sicher, dass auf den eingehenden SSH-Verkehr für die Sicherheitsgruppen zugegriffen werden kann. Die Regel ist COMPLIANT, wenn die IP-Adressen des eingehenden SSH-Datenverkehrs in den Sicherheitsgruppen eingeschränkt sind (CIDR ungleich 0.0.0.0/0 oder ::/0). Andernfalls ist sie NON_COMPLIANT.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
1.5.1	Risiken für das CDE, die von Computerg eräten ausgehen, die eine Verbindun g sowohl mit nicht vertrauenswürdigen Netzwerken als auch mit dem CDE herstellen können, werden gemindert. (PCI-DSS-v4.0)	appsync-associated-with-waf	Stellen Sie sicher, dass AWS AppSync APIs sie den AWS WAFv2 Web-Zugri ffskontrolllisten () zugeordnet sind. ACLs Die Regel ist NON_COMPL IANT für eine AWS AppSync API, wenn sie keiner Web-ACL zugeordnet ist.
1.5.1	Risiken für das CDE, die von Computerg eräten ausgehen, die eine Verbindun g sowohl mit nicht vertrauenswürdigen Netzwerken als auch mit dem CDE herstellen können, werden gemindert. (PCI-DSS-v4.0)	docdb-cluster-snap shot-public-verboten	Stellen Sie sicher, dass manuelle Cluster-Snapshots von Amazon DocumentDB nicht öffentlich sind. Die Regel ist NON_COMPLIANT, wenn manuelle Cluster-Snapshots von Amazon DocumentDB öffentlic h sind.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
1.5.1	Die Risiken für das CDE, die von Computergeräten ausgehen, die sowohl mit nicht vertrauen swürdigen Netzwerke n als auch mit dem CDE verbunden werden können, werden gemindert. (PCI-DSS-v4.0)	codebuild-project-source-repo-URL-Prüfung	Stellen Sie sicher, dass die URL des Bitbucket-Quell-Repositorys KEINE Anmeldeinformationen enthält oder nicht. Die Regel ist NON_COMPLIANT, wenn die URL Anmeldeinformationen enthält, und COMPLIANT, falls dies nicht der Fall ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
1.5.1	Die Risiken für das CDE, die von Computergeräten ausgehen, die sich sowohl mit nicht vertrauenswürdigen Netzwerken als auch mit dem CDE verbinden können, werden gemindert. (PCI-DSS-v4.0)	elb-acm-certificate-required	Stellen Sie sicher, dass die Classic Load Balancers SSL-Zerti fikate verwenden, die vom AWS Certificate Manager bereitgestellt werden. Verwenden Sie zur Nutzung dieser Regel mit Ihrem Classic Load Balancer einen SSL- oder HTTPS-Listener. Hinweis: Diese Regel gilt nur für Classic Load Balancers. Mit dieser Regel werden keine Applicati on Load Balancer oder Network Load Balancer geprüft.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
1.5.1	Die Risiken für das CDE, die von Computergeräten ausgehen, die sowohl mit nicht vertrauen swürdigen Netzwerke n als auch mit dem CDE verbunden werden können, werden gemindert. (PCI-DSS-v4.0)	emr-block-public-a ccess	Stellen Sie sicher, dass für ein Konto bei Amazon EMR die Einstellungen zum Sperren des öffentlic hen Zugriffs aktiviert sind. Die Regel ist NON_COMPLIANT, wenn sie falsch BlockPublicSecurit yGroupRules ist, oder wenn sie wahr ist, sind andere Ports als Port 22 unter aufgeführt. Permitted PublicSecurityGrou pRuleRanges
1.5.1	Risiken für das CDE, die von Computerg eräten ausgehen, die eine Verbindun g sowohl mit nicht vertrauenswürdigen Netzwerken als auch mit dem CDE herstellen können, werden gemindert. (PCI-DSS-v4.0)	nacl-no-unrestricted-ssh-rdp	Stellen Sie sicher, dass die Standardp orts für eingehenden SSH/RDP-Datenverke hr für Netzwerkz ugriffskontrolllisten () eingeschränkt sind. NACLs Die Regel ist NON_COMPLIANT, wenn ein eingehender NACL-Eintrag für die Ports 22 oder 3389 einen CIDR-Block des Typs Quell-TCP oder -UDP zulässt.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
1.5.1	Die Risiken für das CDE, die von Computergeräten ausgehen, die sowohl mit nicht vertrauen swürdigen Netzwerke n als auch mit dem CDE verbunden werden können, werden gemindert. (PCI-DSS-v4.0)	waf-global-webacl-not-leer	Stellen Sie sicher, dass eine WAF Global Web ACL einige WAF-Regeln oder Regelgruppen enthält. Diese Regel ist NON_COMPLIANT, wenn eine globale Web-ACL keine WAF-Regel oder -Regelgru ppe enthält.
1.5.1	Die Risiken für das CDE, die von Computergeräten ausgehen, die sowohl mit nicht vertrauen swürdigen Netzwerke n als auch mit dem CDE verbunden werden können, werden gemindert. (PCI-DSS-v4.0)	waf-global-rulegroup-not-leer	Stellen Sie sicher, dass eine AWS WAF Classic-Regelgrupp e einige Regeln enthält. Die Regel ist NON_COMPLIANT, wenn innerhalb einer Regelgruppe keine Regeln vorhanden sind.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
1.5.1	Die Risiken für das CDE, die von Computergeräten ausgehen, die sowohl mit nicht vertrauen swürdigen Netzwerke n als auch mit dem CDE verbunden werden können, werden gemindert. (PCI-DSS-v4.0)	waf-global-rule-not-leer	Stellen Sie sicher, dass eine globale AWS WAF-Regel einige Bedingungen enthält. Die Regel ist NON_COMPL IANT, wenn in der globalen WAF-Regel keine Bedingungen vorhanden sind.
1.5.1	Die Risiken für das CDE, die von Computergeräten ausgehen, die sowohl mit nicht vertrauen swürdigen Netzwerke n als auch mit dem CDE verbunden werden können, werden gemindert. (PCI-DSS-v4.0)	ec2- -alle client-vpn-not-authorize	Stellen Sie sicher, dass die AWS Client-VPN-Autorisierungsre geln nicht den Verbindungszugriff für alle Clients autorisie ren. Die Regel ist NON_COMPLIANT, wenn 'AccessAll' vorhanden und auf true gesetzt ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
1.5.1	Die Risiken für das CDE, die von Computergeräten ausgehen, die sowohl mit nicht vertrauen swürdigen Netzwerke n als auch mit dem CDE verbunden werden können, werden gemindert. (PCI-DSS-v4.0)	internet-gateway-a uthorized-vpc-nur	Stellen Sie sicher, dass Internet-Gateways an eine autorisierte virtuelle private Cloud (Amazon VPC) angeschlo ssen sind. Die Regel ist NON_COMPL IANT, wenn Internet-Gateways an eine nicht autorisierte VPC angehängt sind.
1.5.1	Risiken für das CDE, die von Computerg eräten ausgehen, die eine Verbindun g sowohl mit nicht vertrauenswürdigen Netzwerken als auch mit dem CDE herstellen können, werden gemindert. (PCI-DSS-v4.0)	access-point-public-accesss3-Blöcke	Stellen Sie sicher, dass Amazon S3 S3-Zugriffspunkten die Einstellungen zum Blockieren des öffentlichen Zugriffs aktiviert sind. Die Regel ist NON_COMPLIANT, wenn die Einstellung zum Blockieren des öffentlichen Zugriffs für S3-Zugangspunkte nicht aktiviert ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
1.5.1	Die Risiken für das CDE, die von Computergeräten ausgehen, die sowohl mit nicht vertrauen swürdigen Netzwerke n als auch mit dem CDE verbunden werden können, werden gemindert. (PCI-DSS-v4.0)	account-level-public-accesss3-Blöcke	Stellen Sie sicher, dass die erforderl ichen Einstellungen für die Sperrung des öffentlichen Zugriffs auf Kontoebene konfiguriert sind. Die Regel ist nur NON_COMPL IANT, wenn die unten festgeleg ten Felder nicht mit den entsprech enden Feldern im Konfigurationselement übereinstimmen.
10.2.1	Auditprotokolle werden implementiert, um die Erkennung von Anomalien und verdächtigen Aktivitäten sowie die forensische Analyse von Ereignissen zu unterstützen. (PCI-DSS-v4.0)	api-gwv2- access-lo gs-enabled	Stellen Sie sicher, dass die Amazon API Gateway V2-Stufen die Zugriffsp rotokollierung aktiviert haben. Die Regel ist NON_COMPL IANT, wenn 'accessLo gSettings' in der Stage-Konfiguration nicht vorhanden ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.2.1	Auditprotokolle werden implementiert, um die Erkennung von Anomalien und verdächtigen Aktivitäten sowie die forensische Analyse von Ereignissen zu unterstützen. (PCI-DSS-v4.0)	api-gw-xray-enabled	Stellen Sie sicher, dass AWS X-Ray Tracing auf Amazon API Gateway REST APIs aktiviert ist. Die Regel ist COMPLIANT, wenn die X-Ray-Abl aufverfolgung aktiviert ist, andernfalls ist sie NON_COMPLIANT.
10.2.1	Auditprotokolle werden implementiert, um die Erkennung von Anomalien und verdächtigen Aktivitäten sowie die forensische Analyse von Ereignissen zu unterstützen. (PCI-DSS-v4.0)	cloudfront-accesslogs-enabled	Stellen Sie sicher, dass CloudFront Amazon-Distributionen so konfiguriert sind, dass sie Zugriffsprotokolle an einen Amazon S3-Bucket senden. Die Regel lautet NON_COMPLIANT, wenn für eine CloudFront Distribution keine Protokollierung konfiguriert ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.2.1	Auditprotokolle werden implementiert, um die Erkennung von Anomalien und verdächtigen Aktivitäten sowie die forensische Analyse von Ereignissen zu unterstützen. (PCI-DSS-v4.0)	neptune-cluster-cloudwatch-log-exportfähig	Stellen Sie sicher, dass in einem Amazon Neptune Neptune-Cluster der Protokollexport für CloudWatch Audit-Logs aktiviert ist. Die Regel lautet NON_COMPLIANT, wenn für einen Neptune-Cluster der Protokollexport für CloudWatch Audit-Logs nicht aktiviert ist.
10.2.1	Auditprotokolle werden implementiert, um die Erkennung von Anomalien und verdächtigen Aktivitäten sowie die forensische Analyse von Ereignissen zu unterstützen. (PCI-DSS-v4.0)	ecs-task-definition-log-Konfiguration	Stellen Sie sicher, dass LogConfiguration für aktive ECS-Aufgabendefinitionen festgelegt ist. Diese Regel ist NON_COMPLIANT, wenn für eine aktive ECSTask Definition die LogConfiguration-Ressource nicht definiert ist oder der Wert für LogConfiguration in mindestens einer Containerdefinition Null ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.2.1	Auditprotokolle werden implementiert, um die Erkennung von Anomalien und verdächtigen Aktivitäten sowie die forensische Analyse von Ereignissen zu unterstützen. (PCI-DSS-v4.0)	cloudtrail-enabled	Hinweis: Bei dieser Regel untersche iden sich die Regel-ID (CLOUD_TR AIL_ENABLED) und der Regelname (cloudtrail-enabled). Stellen Sie sicher, dass in Ihrem Konto ein Trail aktiviert ist AWS CloudTrail . AWS Die Regel ist NON_COMPLIANT, wenn ein Trail nicht aktiviert ist. Optional überprüft die Regel einen bestimmten S3-Bucket, ein Amazon Simple Notification Service (Amazon SNS) -Thema und eine CloudWatch Protokollgruppe.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.2.1	Auditprotokolle werden implementiert, um die Erkennung von Anomalien und verdächtigen Aktivitäten sowie die forensische Analyse von Ereignissen zu unterstützen. (PCI-DSS-v4.0)	multi-region-cloudtrail-enabled	Hinweis: Bei dieser Regel untersche iden sich die Regel-ID (MULTI_RE GION_CLOU D_TRAIL_ENABLED) und der Regelname (). multi-region-cloudtrail-enabled Stellen Sie sicher, dass mindesten s eine Region mit mehreren Regionen vorhanden ist. AWS CloudTrail Die Regel ist NON_COMPL IANT, wenn die Trails nicht mit den Eingabeparametern übereinstimmen. Die Regel lautet NON_COMPLIANT, wenn das ExcludeMa nagementEventSourc es Feld nicht leer ist oder wenn sie so konfiguriert AWS CloudTrail ist, dass Verwaltungsereigni sse wie AWS KMS-Ereignisse oder Amazon RDS-Daten -API-Ereignisse

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			ausgeschlossen werden.
10.2.1	Auditprotokolle werden implementiert, um die Erkennung von Anomalien und verdächtigen Aktivitäten sowie die forensische Analyse von Ereignissen zu unterstützen. (PCI-DSS-v4.0)	appsync-logging-enabled	Stellen Sie sicher, dass für eine API die Protokollierung aktiviert ist. AWS AppSync Die Regel lautet NON_COMPLIANT, wenn die Protokollierung nicht aktiviert ist, oder 'fieldLogLevel' ist weder ERROR noch ALL.
10.2.1	Auditprotokolle werden implementiert, um die Erkennung von Anomalien und verdächtigen Aktivitäten sowie die forensische Analyse von Ereignissen zu unterstützen. (PCI-DSS-v4.0)	waf-classic-logging-enabled	Stellen Sie sicher, dass die Protokollierung auf den AWS WAF Classic Global Web Access Control Lists (Web) aktiviert ist. ACLs Die Regel ist NON_COMPLIANT für eine globale Web-ACL, wenn die Protokollierung nicht aktiviert ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.2.1	Auditprotokolle werden implementiert, um die Erkennung von Anomalien und verdächtigen Aktivitäten sowie die forensische Analyse von Ereignissen zu unterstützen. (PCI-DSS-v4.0)	mq-cloudwatch-audit-logging-aktiviert	Stellen Sie sicher, dass Amazon MQ-Broker die CloudWatch Amazon-Auditprotokollierung aktiviert haben. Die Regel ist NON_COMPLIANT, wenn für einen Broker die Audit-Protokollierung nicht aktiviert ist.
10.2.1	Auditprotokolle werden implementiert, um die Erkennung von Anomalien und verdächtigen Aktivitäten sowie die forensische Analyse von Ereignissen zu unterstützen. (PCI-DSS-v4.0)	mq-cloudwatch-audit-log-aktiviert	Stellen Sie sicher, dass bei einem Amazon MQ-Broker die CloudWatch Auditprotokollierung aktiviert ist. Die Regel lautet NON_COMPLIANT, wenn für den Broker die Audit-Protokollierung nicht aktiviert ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.2.1	Auditprotokolle werden implementiert, um die Erkennung von Anomalien und verdächtigen Aktivitäten sowie die forensische Analyse von Ereignissen zu unterstützen. (PCI-DSS-v4.0)	eks-cluster-logging-enabled	Stellen Sie sicher, dass ein Amazon Elastic Kubernete s Service (Amazon EKS) -Cluster mit aktivierter Protokoll ierung konfiguriert ist. Die Regel ist NON_COMPLIANT, wenn die Protokoll ierung für Amazon-EKS-Cluster nicht für alle Protokolltypen aktiviert ist.
10.2.1	Auditprotokolle werden implementiert, um die Erkennung von Anomalien und verdächtigen Aktivitäten sowie die forensische Analyse von Ereignissen zu unterstützen. (PCI-DSS-v4.0)	elastic-beanstalk-logs-to-Wolkenbeob achtung	Stellen Sie sicher, dass AWS Elastic Beanstalk Beanstalk -Umgebungen so konfiguriert sind, dass sie Protokolle an Amazon CloudWatc h Logs senden. Die Regel lautet NON_COMPLIANT, wenn der Wert von `` StreamLogs falsch ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.2.1	Auditprotokolle werden implementiert, um die Erkennung von Anomalien und verdächtigen Aktivitäten sowie die forensische Analyse von Ereignissen zu unterstützen. (PCI-DSS-v4.0)	step-functions-state-machine-Protokollierung aktiviert	Stellen Sie sicher, dass auf der AWS Step Functions Functions-Maschine die Protokollierung aktiviert ist Die Regel ist NON_COMPLIANT, wenn für eine Zustandsmaschine die Protokollierung nicht aktiviert ist oder die Protokollierungskonfiguration nicht auf dem angegebenen Mindestniveau liegt.
10.2.1	Auditprotokolle werden implementiert, um die Erkennung von Anomalien und verdächtigen Aktivitäten sowie die forensische Analyse von Ereignissen zu unterstützen. (PCI-DSS-v4.0)	netfw-logging-enabled	Stellen Sie sicher, dass die AWS Netzwerk-Firewall-Firewalls die Protokollierung aktiviert haben. Die Regel ist NON_COMPLIANT, wenn kein Protokollierungstyp konfiguriert ist. Sie können angeben, welchen Protokollierungstyp die Regel prüfen soll.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.2.1.1	Auditprotokolle werden implementiert, um die Erkennung von Anomalien und verdächtigen Aktivitäten sowie die forensische Analyse von Ereignissen zu unterstützen. (PCI-DSS-v4.0)	api-gwv2- access-logs-enabled	Stellen Sie sicher, dass die Amazon API Gateway V2-Stufen die Zugriffsprotokollierung aktiviert haben. Die Regel ist NON_COMPLIANT, wenn 'accessLogSettings' in der Stage-Konfiguration nicht vorhanden ist.
10.2.1.1	Auditprotokolle werden implementiert, um die Erkennung von Anomalien und verdächtigen Aktivitäten sowie die forensische Analyse von Ereignissen zu unterstützen. (PCI-DSS-v4.0)	api-gw-xray-enabled	Stellen Sie sicher, dass AWS X-Ray Tracing auf Amazon API Gateway REST APIs aktiviert ist. Die Regel ist COMPLIANT, wenn die X-Ray-Abl aufverfolgung aktiviert ist, andernfalls ist sie NON_COMPLIANT.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.2.1.1	Auditprotokolle werden implementiert, um die Erkennung von Anomalien und verdächtigen Aktivitäten sowie die forensische Analyse von Ereignissen zu unterstützen. (PCI-DSS-v4.0)	cloudfront-accesslogs-enabled	Stellen Sie sicher, dass CloudFront Amazon-Distributionen so konfiguriert sind, dass sie Zugriffsprotokolle an einen Amazon S3-Bucket senden. Die Regel lautet NON_COMPLIANT, wenn für eine CloudFront Distribution keine Protokollierung konfiguriert ist.
10.2.1.1	Auditprotokolle werden implementiert, um die Erkennung von Anomalien und verdächtigen Aktivitäten sowie die forensische Analyse von Ereignissen zu unterstützen. (PCI-DSS-v4.0)	neptune-cluster-cloudwatch-log-exportfähig	Stellen Sie sicher, dass in einem Amazon Neptune Neptune-Cluster der Protokollexport für CloudWatch Audit-Logs aktiviert ist. Die Regel lautet NON_COMPLIANT, wenn für einen Neptune-Cluster der Protokollexport für CloudWatch Audit-Logs nicht aktiviert ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.2.1.1	Auditprotokolle werden implementiert, um die Erkennung von Anomalien und verdächtigen Aktivitäten sowie die forensische Analyse von Ereignissen zu unterstützen. (PCI-DSS-v4.0)	ec2- instance-detailed-monitoring-enabled	Stellen Sie sicher, dass die detaillierte Überwachung für Instanzen aktiviert ist. EC2 Die Regel ist NON_COMPLIANT, wenn keine detaillierte Überwachung aktiviert ist.
10.2.1.1	Auditprotokolle werden implementiert, um die Erkennung von Anomalien und verdächtigen Aktivitäten sowie die forensische Analyse von Ereignissen zu unterstützen. (PCI-DSS-v4.0)	ecs-task-definition-log-Konfiguration	Stellen Sie sicher, dass LogConfig uration für aktive ECS-Aufgabendefini tionen festgelegt ist. Diese Regel ist NON_COMPLIANT, wenn für eine aktive ECSTask Definition die LogConfiguration-Ressource nicht definiert ist oder der Wert für LogConfig uration in mindesten s einer Container definition Null ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.2.1.1	Auditprotokolle werden implementiert, um die Erkennung von Anomalien und verdächtigen Aktivitäten sowie die forensische Analyse von Ereignissen zu unterstützen. (PCI-DSS-v4.0)	cloudwatch-alarm-action-check	Stellen Sie sicher, dass bei CloudWatch Alarmen eine Aktion für den Status ALARM, INSUFFICIENT_DATA oder OK konfiguriert ist. Stellen Sie optional sicher, dass alle Aktionen mit einem benannten ARN übereinstimmen. Die Regel ist NON_COMPLIANT, wenn für den Alarm oder den optionalen Parameter keine Aktion festgelegt ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.2.1.1	Auditprotokolle werden implementiert, um die Erkennung von Anomalien und verdächtigen Aktivitäten sowie die forensische Analyse von Ereignissen zu unterstützen. (PCI-DSS-v4.0)	cloudwatch-alarm-action-check	Stellen Sie sicher, dass bei CloudWatch Alarmen eine Aktion für den Status ALARM, INSUFFICIENT_DATA oder OK konfiguriert ist. Stellen Sie optional sicher, dass alle Aktionen mit einem benannten ARN übereinstimmen. Die Regel ist NON_COMPLIANT, wenn für den Alarm oder den optionalen Parameter keine Aktion festgelegt ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.2.1.1	Auditprotokolle werden implementiert, um die Erkennung von Anomalien und verdächtigen Aktivitäten sowie die forensische Analyse von Ereignissen zu unterstützen. (PCI-DSS-v4.0)	cloudwatch-alarm-action-check	Stellen Sie sicher, dass bei CloudWatch Alarmen eine Aktion für den Status ALARM, INSUFFICIENT_DATA oder OK konfiguriert ist. Stellen Sie optional sicher, dass alle Aktionen mit einem benannten ARN übereinstimmen. Die Regel ist NON_COMPLIANT, wenn für den Alarm oder den optionalen Parameter keine Aktion festgelegt ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.2.1.1	Auditprotokolle werden implementiert, um die Erkennung von Anomalien und verdächtigen Aktivitäten sowie die forensische Analyse von Ereignissen zu unterstützen. (PCI-DSS-v4.0)	cloudwatch-alarm-resource-check	Stellen Sie sicher, dass ein Ressourcentyp einen CloudWatch Alarm für die angegebene Metrik hat. Als Ressourcentyp können Sie EBS-Volumes, EC2 Instances, Amazon RDS-Cluster oder S3-Buckets angeben. Die Regel ist KONFORM, wenn die benannte Metrik eine Ressourcen-ID und CloudWatch einen Alarm hat.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.2.1.1	Auditprotokolle werden implementiert, um die Erkennung von Anomalien und verdächtigen Aktivitäten sowie die forensische Analyse von Ereignissen zu unterstützen. (PCI-DSS-v4.0)	cloudtrail-enabled	Hinweis: Bei dieser Regel untersche iden sich die Regel-ID (CLOUD_TR AIL_ENABLED) und der Regelname (cloudtrail-enabled). Stellen Sie sicher, dass in Ihrem Konto ein Trail aktiviert ist AWS CloudTrail . AWS Die Regel ist NON_COMPLIANT, wenn ein Trail nicht aktiviert ist. Optional überprüft die Regel einen bestimmten S3-Bucket, ein Amazon Simple Notification Service (Amazon SNS) -Thema und eine CloudWatch Protokollgruppe.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.2.1.1	Auditprotokolle werden implementiert, um die Erkennung von Anomalien und verdächtigen Aktivitäten sowie die forensische Analyse von Ereignissen zu unterstützen. (PCI-DSS-v4.0)	multi-region-cloudtrail-enabled	Hinweis: Bei dieser Regel untersche iden sich die Regel-ID (MULTI_RE GION_CLOU D_TRAIL_ENABLED) und der Regelname (). multi-region-cloudtrail-enabled Stellen Sie sicher, dass mindesten s eine Region mit mehreren Regionen vorhanden ist. AWS CloudTrail Die Regel ist NON_COMPL IANT, wenn die Trails nicht mit den Eingabeparametern übereinstimmen. Die Regel lautet NON_COMPLIANT, wenn das ExcludeMa nagementEventSourc es Feld nicht leer ist oder wenn sie so konfiguriert AWS CloudTrail ist, dass Verwaltungsereigni sse wie AWS KMS-Ereignisse oder Amazon RDS-Daten -API-Ereignisse

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			ausgeschlossen werden.
10.2.1.1	Auditprotokolle werden implementiert, um die Erkennung von Anomalien und verdächtigen Aktivitäten sowie die forensische Analyse von Ereignissen zu unterstützen. (PCI-DSS-v4.0)	appsync-logging-enabled	Stellen Sie sicher, dass für eine API die Protokollierung aktiviert ist. AWS AppSync Die Regel lautet NON_COMPLIANT, wenn die Protokollierung nicht aktiviert ist, oder 'fieldLogLevel' ist weder ERROR noch ALL.
10.2.1.1	Auditprotokolle werden implementiert, um die Erkennung von Anomalien und verdächtigen Aktivitäten sowie die forensische Analyse von Ereignissen zu unterstützen. (PCI-DSS-v4.0)	waf-classic-logging-enabled	Stellen Sie sicher, dass die Protokollierung auf den AWS WAF Classic Global Web Access Control Lists (Web) aktiviert ist. ACLs Die Regel ist NON_COMPLIANT für eine globale Web-ACL, wenn die Protokollierung nicht aktiviert ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.2.1.1	Auditprotokolle werden implementiert, um die Erkennung von Anomalien und verdächtigen Aktivitäten sowie die forensische Analyse von Ereignissen zu unterstützen. (PCI-DSS-v4.0)	mq-cloudwatch-audit-logging-aktiviert	Stellen Sie sicher, dass Amazon MQ-Broker die CloudWatch Amazon-Auditprotokollierung aktiviert haben. Die Regel ist NON_COMPLIANT, wenn für einen Broker die Audit-Protokollierung nicht aktiviert ist.
10.2.1.1	Auditprotokolle werden implementiert, um die Erkennung von Anomalien und verdächtigen Aktivitäten sowie die forensische Analyse von Ereignissen zu unterstützen. (PCI-DSS-v4.0)	mq-cloudwatch-audit-log-aktiviert	Stellen Sie sicher, dass bei einem Amazon MQ-Broker die CloudWatch Auditprotokollierung aktiviert ist. Die Regel lautet NON_COMPLIANT, wenn für den Broker die Audit-Protokollierung nicht aktiviert ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.2.1.1	Auditprotokolle werden implementiert, um die Erkennung von Anomalien und verdächtigen Aktivitäten sowie die forensische Analyse von Ereignissen zu unterstützen. (PCI-DSS-v4.0)	eks-cluster-logging-enabled	Stellen Sie sicher, dass ein Amazon Elastic Kubernete s Service (Amazon EKS) -Cluster mit aktivierter Protokoll ierung konfiguriert ist. Die Regel ist NON_COMPLIANT, wenn die Protokoll ierung für Amazon-EKS-Cluster nicht für alle Protokolltypen aktiviert ist.
10.2.1.1	Auditprotokolle werden implementiert, um die Erkennung von Anomalien und verdächtigen Aktivitäten sowie die forensische Analyse von Ereignissen zu unterstützen. (PCI-DSS-v4.0)	elastic-beanstalk-logs-to-Wolkenbeob achtung	Stellen Sie sicher, dass AWS Elastic Beanstalk Beanstalk -Umgebungen so konfiguriert sind, dass sie Protokolle an Amazon CloudWatc h Logs senden. Die Regel lautet NON_COMPLIANT, wenn der Wert von `` StreamLogs falsch ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.2.1.1	Auditprotokolle werden implementiert, um die Erkennung von Anomalien und verdächtigen Aktivitäten sowie die forensische Analyse von Ereignissen zu unterstützen. (PCI-DSS-v4.0)	WAF 2- rulegroup-logging-enabled	Stellen Sie sicher, dass die Erfassung von CloudWatch Amazon-Sicherheits metriken für AWS WAFv2 Regelgruppen aktiviert ist. Die Regel ist NON_COMPL IANT, wenn '. Visibilit yConfig CloudWatc hMetricsEnabledDas Feld 'ist auf falsch gesetzt.
10.2.1.1	Auditprotokolle werden implementiert, um die Erkennung von Anomalien und verdächtigen Aktivitäten sowie die forensische Analyse von Ereignissen zu unterstützen. (PCI-DSS-v4.0)	sns-topic-message-delivery-Benachric htigung aktiviert	Stellen Sie sicher, dass die Amazon Simple Notificat ion Service (SNS) - Protokollierung für den Zustellungsstatus von Benachric htigungen aktiviert ist, die an ein Thema für die Endgeräte gesendet werden. Die Regel ist NON_COMPLIANT, wenn die Benachric htigung über den Status der Zustellung von Nachrichten nicht aktiviert ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.2.1.1	Auditprotokolle werden implementiert, um die Erkennung von Anomalien und verdächtigen Aktivitäten sowie die forensische Analyse von Ereignissen zu unterstützen. (PCI-DSS-v4.0)	step-functions-state-machine-Protokollierung aktiviert	Stellen Sie sicher, dass auf der AWS Step Functions Functions-Maschine die Protokollierung aktiviert ist Die Regel ist NON_COMPLIANT, wenn für eine Zustandsmaschine die Protokollierung nicht aktiviert ist oder die Protokollierungskonfiguration nicht auf dem angegebenen Mindestniveau liegt.
10.2.1.1	Auditprotokolle werden implementiert, um die Erkennung von Anomalien und verdächtigen Aktivitäten sowie die forensische Analyse von Ereignissen zu unterstützen. (PCI-DSS-v4.0)	netfw-logging-enabled	Stellen Sie sicher, dass die AWS Netzwerk-Firewall-Firewalls die Protokollierung aktiviert haben. Die Regel ist NON_COMPLIANT, wenn kein Protokollierungstyp konfiguriert ist. Sie können angeben, welchen Protokollierungstyp die Regel prüfen soll.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.2.1.2	Auditprotokolle werden implementiert, um die Erkennung von Anomalien und verdächtigen Aktivitäten sowie die forensische Analyse von Ereignissen zu unterstützen. (PCI-DSS-v4.0)	api-gwv2- access-logs-enabled	Stellen Sie sicher, dass die Amazon API Gateway V2-Stufen die Zugriffsprotokollierung aktiviert haben. Die Regel ist NON_COMPLIANT, wenn 'accessLogSettings' in der Stage-Konfiguration nicht vorhanden ist.
10.2.1.2	Auditprotokolle werden implementiert, um die Erkennung von Anomalien und verdächtigen Aktivitäten sowie die forensische Analyse von Ereignissen zu unterstützen. (PCI-DSS-v4.0)	api-gw-xray-enabled	Stellen Sie sicher, dass AWS X-Ray Tracing auf Amazon API Gateway REST APIs aktiviert ist. Die Regel ist COMPLIANT, wenn die X-Ray-Abl aufverfolgung aktiviert ist, andernfalls ist sie NON_COMPLIANT.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.2.1.2	Auditprotokolle werden implementiert, um die Erkennung von Anomalien und verdächtigen Aktivitäten sowie die forensische Analyse von Ereignissen zu unterstützen. (PCI-DSS-v4.0)	cloudfront-accesslogs-enabled	Stellen Sie sicher, dass CloudFront Amazon-Distributionen so konfiguriert sind, dass sie Zugriffsprotokolle an einen Amazon S3-Bucket senden. Die Regel lautet NON_COMPLIANT, wenn für eine CloudFront Distribution keine Protokollierung konfiguriert ist.
10.2.1.2	Auditprotokolle werden implementiert, um die Erkennung von Anomalien und verdächtigen Aktivitäten sowie die forensische Analyse von Ereignissen zu unterstützen. (PCI-DSS-v4.0)	neptune-cluster-cloudwatch-log-exportfähig	Stellen Sie sicher, dass in einem Amazon Neptune Neptune-Cluster der Protokollexport für CloudWatch Audit-Logs aktiviert ist. Die Regel lautet NON_COMPLIANT, wenn für einen Neptune-Cluster der Protokollexport für CloudWatch Audit-Logs nicht aktiviert ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.2.1.2	Auditprotokolle werden implementiert, um die Erkennung von Anomalien und verdächtigen Aktivitäten sowie die forensische Analyse von Ereignissen zu unterstützen. (PCI-DSS-v4.0)	ecs-task-definition-log-Konfiguration	Stellen Sie sicher, dass LogConfiguration für aktive ECS-Aufgabendefinitionen festgelegt ist. Diese Regel ist NON_COMPLIANT, wenn für eine aktive ECSTask Definition die LogConfiguration-Ressource nicht definiert ist oder der Wert für LogConfiguration in mindestens einer Containerdefinition Null ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.2.1.2	Auditprotokolle werden implementiert, um die Erkennung von Anomalien und verdächtigen Aktivitäten sowie die forensische Analyse von Ereignissen zu unterstützen. (PCI-DSS-v4.0)	cloudtrail-enabled	Hinweis: Bei dieser Regel untersche iden sich die Regel-ID (CLOUD_TR AIL_ENABLED) und der Regelname (cloudtrail-enabled). Stellen Sie sicher, dass in Ihrem Konto ein Trail aktiviert ist AWS CloudTrail . AWS Die Regel ist NON_COMPLIANT, wenn ein Trail nicht aktiviert ist. Optional überprüft die Regel einen bestimmten S3-Bucket, ein Amazon Simple Notification Service (Amazon SNS) -Thema und eine CloudWatch Protokollgruppe.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.2.1.2	Auditprotokolle werden implementiert, um die Erkennung von Anomalien und verdächtigen Aktivitäten sowie die forensische Analyse von Ereignissen zu unterstützen. (PCI-DSS-v4.0)	multi-region-cloudtrail-enabled	Hinweis: Bei dieser Regel untersche iden sich die Regel-ID (MULTI_RE GION_CLOU D_TRAIL_ENABLED) und der Regelname (). multi-region-cloudtrail-enabled Stellen Sie sicher, dass mindesten s eine Region mit mehreren Regionen vorhanden ist. AWS CloudTrail Die Regel ist NON_COMPL IANT, wenn die Trails nicht mit den Eingabeparametern übereinstimmen. Die Regel lautet NON_COMPLIANT, wenn das ExcludeMa nagementEventSourc es Feld nicht leer ist oder wenn sie so konfiguriert AWS CloudTrail ist, dass Verwaltungsereigni sse wie AWS KMS-Ereignisse oder Amazon RDS-Daten -API-Ereignisse

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			ausgeschlossen werden.
10.2.1.2	Auditprotokolle werden implementiert, um die Erkennung von Anomalien und verdächtigen Aktivitäten sowie die forensische Analyse von Ereignissen zu unterstützen. (PCI-DSS-v4.0)	appsync-logging-enabled	Stellen Sie sicher, dass für eine API die Protokollierung aktiviert ist. AWS AppSync Die Regel lautet NON_COMPLIANT, wenn die Protokollierung nicht aktiviert ist, oder 'fieldLogLevel' ist weder ERROR noch ALL.
10.2.1.2	Auditprotokolle werden implementiert, um die Erkennung von Anomalien und verdächtigen Aktivitäten sowie die forensische Analyse von Ereignissen zu unterstützen. (PCI-DSS-v4.0)	waf-classic-logging-enabled	Stellen Sie sicher, dass die Protokollierung auf den AWS WAF Classic Global Web Access Control Lists (Web) aktiviert ist. ACLs Die Regel ist NON_COMPLIANT für eine globale Web-ACL, wenn die Protokollierung nicht aktiviert ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.2.1.2	Auditprotokolle werden implementiert, um die Erkennung von Anomalien und verdächtigen Aktivitäten sowie die forensische Analyse von Ereignissen zu unterstützen. (PCI-DSS-v4.0)	mq-cloudwatch-audit-logging-aktiviert	Stellen Sie sicher, dass Amazon MQ-Broker die CloudWatch Amazon-Auditprotokollierung aktiviert haben. Die Regel ist NON_COMPLIANT, wenn für einen Broker die Audit-Protokollierung nicht aktiviert ist.
10.2.1.2	Auditprotokolle werden implementiert, um die Erkennung von Anomalien und verdächtigen Aktivitäten sowie die forensische Analyse von Ereignissen zu unterstützen. (PCI-DSS-v4.0)	mq-cloudwatch-audit-log-aktiviert	Stellen Sie sicher, dass bei einem Amazon MQ-Broker die CloudWatch Auditprotokollierung aktiviert ist. Die Regel lautet NON_COMPLIANT, wenn für den Broker die Audit-Protokollierung nicht aktiviert ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.2.1.2	Auditprotokolle werden implementiert, um die Erkennung von Anomalien und verdächtigen Aktivitäten sowie die forensische Analyse von Ereignissen zu unterstützen. (PCI-DSS-v4.0)	eks-cluster-logging-enabled	Stellen Sie sicher, dass ein Amazon Elastic Kubernete s Service (Amazon EKS) -Cluster mit aktivierter Protokoll ierung konfiguriert ist. Die Regel ist NON_COMPLIANT, wenn die Protokoll ierung für Amazon-EKS-Cluster nicht für alle Protokolltypen aktiviert ist.
10.2.1.2	Auditprotokolle werden implementiert, um die Erkennung von Anomalien und verdächtigen Aktivitäten sowie die forensische Analyse von Ereignissen zu unterstützen. (PCI-DSS-v4.0)	elastic-beanstalk-logs-to-Wolkenbeob achtung	Stellen Sie sicher, dass AWS Elastic Beanstalk Beanstalk -Umgebungen so konfiguriert sind, dass sie Protokolle an Amazon CloudWatc h Logs senden. Die Regel lautet NON_COMPLIANT, wenn der Wert von `` StreamLogs falsch ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.2.1.2	Auditprotokolle werden implementiert, um die Erkennung von Anomalien und verdächtigen Aktivitäten sowie die forensische Analyse von Ereignissen zu unterstützen. (PCI-DSS-v4.0)	step-functions-state-machine-Protokollierung aktiviert	Stellen Sie sicher, dass auf der AWS Step Functions Functions-Maschine die Protokollierung aktiviert ist Die Regel ist NON_COMPLIANT, wenn für eine Zustandsmaschine die Protokollierung nicht aktiviert ist oder die Protokollierungskonfiguration nicht auf dem angegebenen Mindestniveau liegt.
10.2.1.2	Auditprotokolle werden implementiert, um die Erkennung von Anomalien und verdächtigen Aktivitäten sowie die forensische Analyse von Ereignissen zu unterstützen. (PCI-DSS-v4.0)	netfw-logging-enabled	Stellen Sie sicher, dass die AWS Netzwerk-Firewall-Firewalls die Protokollierung aktiviert haben. Die Regel ist NON_COMPLIANT, wenn kein Protokollierungstyp konfiguriert ist. Sie können angeben, welchen Protokollierungstyp die Regel prüfen soll.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.2.1.3	Auditprotokolle werden implementiert, um die Erkennung von Anomalien und verdächtigen Aktivitäten sowie die forensische Analyse von Ereignissen zu unterstützen. (PCI-DSS-v4.0)	api-gwv2- access-logs-enabled	Stellen Sie sicher, dass die Amazon API Gateway V2-Stufen die Zugriffsprotokollierung aktiviert haben. Die Regel ist NON_COMPLIANT, wenn 'accessLogSettings' in der Stage-Konfiguration nicht vorhanden ist.
10.2.1.3	Auditprotokolle werden implementiert, um die Erkennung von Anomalien und verdächtigen Aktivitäten sowie die forensische Analyse von Ereignissen zu unterstützen. (PCI-DSS-v4.0)	api-gw-xray-enabled	Stellen Sie sicher, dass AWS X-Ray Tracing auf Amazon API Gateway REST APIs aktiviert ist. Die Regel ist COMPLIANT, wenn die X-Ray-Ablaufverfolgung aktiviert ist, andernfalls ist sie NON_COMPLIANT.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.2.1.3	Auditprotokolle werden implementiert, um die Erkennung von Anomalien und verdächtigen Aktivitäten sowie die forensische Analyse von Ereignissen zu unterstützen. (PCI-DSS-v4.0)	cloudfront-accesslogs-enabled	Stellen Sie sicher, dass CloudFront Amazon-Distributionen so konfiguriert sind, dass sie Zugriffsprotokolle an einen Amazon S3-Bucket senden. Die Regel lautet NON_COMPLIANT, wenn für eine CloudFront Distribution keine Protokollierung konfiguriert ist.
10.2.1.3	Auditprotokolle werden implementiert, um die Erkennung von Anomalien und verdächtigen Aktivitäten sowie die forensische Analyse von Ereignissen zu unterstützen. (PCI-DSS-v4.0)	neptune-cluster-cloudwatch-log-exportfähig	Stellen Sie sicher, dass in einem Amazon Neptune Neptune-Cluster der Protokollexport für CloudWatch Audit-Logs aktiviert ist. Die Regel lautet NON_COMPLIANT, wenn für einen Neptune-Cluster der Protokollexport für CloudWatch Audit-Logs nicht aktiviert ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.2.1.3	Auditprotokolle werden implementiert, um die Erkennung von Anomalien und verdächtigen Aktivitäten sowie die forensische Analyse von Ereignissen zu unterstützen. (PCI-DSS-v4.0)	ecs-task-definition-log-Konfiguration	Stellen Sie sicher, dass LogConfiguration für aktive ECS-Aufgabendefinitionen festgelegt ist. Diese Regel ist NON_COMPLIANT, wenn für eine aktive ECSTask Definition die LogConfiguration-Ressource nicht definiert ist oder der Wert für LogConfiguration in mindestens einer Containerdefinition Null ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.2.1.3	Auditprotokolle werden implementiert, um die Erkennung von Anomalien und verdächtigen Aktivitäten sowie die forensische Analyse von Ereignissen zu unterstützen. (PCI-DSS-v4.0)	cloudtrail-enabled	Hinweis: Bei dieser Regel untersche iden sich die Regel-ID (CLOUD_TR AIL_ENABLED) und der Regelname (cloudtrail-enabled). Stellen Sie sicher, dass in Ihrem Konto ein Trail aktiviert ist AWS CloudTrail . AWS Die Regel ist NON_COMPLIANT, wenn ein Trail nicht aktiviert ist. Optional überprüft die Regel einen bestimmten S3-Bucket, ein Amazon Simple Notification Service (Amazon SNS) -Thema und eine CloudWatch Protokollgruppe.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.2.1.3	Auditprotokolle werden implementiert, um die Erkennung von Anomalien und verdächtigen Aktivitäten sowie die forensische Analyse von Ereignissen zu unterstützen. (PCI-DSS-v4.0)	multi-region-cloudtrail-enabled	Hinweis: Bei dieser Regel untersche iden sich die Regel-ID (MULTI_RE GION_CLOU D_TRAIL_ENABLED) und der Regelname (). multi-region-cloudtrail-enabled Stellen Sie sicher, dass mindesten s eine Region mit mehreren Regionen vorhanden ist. AWS CloudTrail Die Regel ist NON_COMPL IANT, wenn die Trails nicht mit den Eingabeparametern übereinstimmen. Die Regel lautet NON_COMPLIANT, wenn das ExcludeMa nagementEventSourc es Feld nicht leer ist oder wenn sie so konfiguriert AWS CloudTrail ist, dass Verwaltungsereigni sse wie AWS KMS-Ereignisse oder Amazon RDS-Daten -API-Ereignisse

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			ausgeschlossen werden.
10.2.1.3	Auditprotokolle werden implementiert, um die Erkennung von Anomalien und verdächtigen Aktivitäten sowie die forensische Analyse von Ereignissen zu unterstützen. (PCI-DSS-v4.0)	appsync-logging-enabled	Stellen Sie sicher, dass für eine API die Protokollierung aktiviert ist. AWS AppSync Die Regel lautet NON_COMPLIANT, wenn die Protokollierung nicht aktiviert ist, oder 'fieldLogLevel' ist weder ERROR noch ALL.
10.2.1.3	Auditprotokolle werden implementiert, um die Erkennung von Anomalien und verdächtigen Aktivitäten sowie die forensische Analyse von Ereignissen zu unterstützen. (PCI-DSS-v4.0)	waf-classic-logging-enabled	Stellen Sie sicher, dass die Protokollierung auf den AWS WAF Classic Global Web Access Control Lists (Web) aktiviert ist. ACLs Die Regel ist NON_COMPLIANT für eine globale Web-ACL, wenn die Protokollierung nicht aktiviert ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.2.1.3	Auditprotokolle werden implementiert, um die Erkennung von Anomalien und verdächtigen Aktivitäten sowie die forensische Analyse von Ereignissen zu unterstützen. (PCI-DSS-v4.0)	mq-cloudwatch-audit-logging-aktiviert	Stellen Sie sicher, dass Amazon MQ-Broker die CloudWatch Amazon-Auditprotokollierung aktiviert haben. Die Regel ist NON_COMPLIANT, wenn für einen Broker die Audit-Protokollierung nicht aktiviert ist.
10.2.1.3	Auditprotokolle werden implementiert, um die Erkennung von Anomalien und verdächtigen Aktivitäten sowie die forensische Analyse von Ereignissen zu unterstützen. (PCI-DSS-v4.0)	mq-cloudwatch-audit-log-aktiviert	Stellen Sie sicher, dass bei einem Amazon MQ-Broker die CloudWatch Auditprotokollierung aktiviert ist. Die Regel lautet NON_COMPLIANT, wenn für den Broker die Audit-Protokollierung nicht aktiviert ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.2.1.3	Auditprotokolle werden implementiert, um die Erkennung von Anomalien und verdächtigen Aktivitäten sowie die forensische Analyse von Ereignissen zu unterstützen. (PCI-DSS-v4.0)	eks-cluster-logging-enabled	Stellen Sie sicher, dass ein Amazon Elastic Kubernete s Service (Amazon EKS) -Cluster mit aktivierter Protokoll ierung konfiguriert ist. Die Regel ist NON_COMPLIANT, wenn die Protokoll ierung für Amazon-EKS-Cluster nicht für alle Protokolltypen aktiviert ist.
10.2.1.3	Auditprotokolle werden implementiert, um die Erkennung von Anomalien und verdächtigen Aktivitäten sowie die forensische Analyse von Ereignissen zu unterstützen. (PCI-DSS-v4.0)	elastic-beanstalk-logs-to-Wolkenbeob achtung	Stellen Sie sicher, dass AWS Elastic Beanstalk Beanstalk -Umgebungen so konfiguriert sind, dass sie Protokolle an Amazon CloudWatc h Logs senden. Die Regel lautet NON_COMPLIANT, wenn der Wert von `` StreamLogs falsch ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.2.1.3	Auditprotokolle werden implementiert, um die Erkennung von Anomalien und verdächtigen Aktivitäten sowie die forensische Analyse von Ereignissen zu unterstützen. (PCI-DSS-v4.0)	step-functions-state-machine-Protokollierung aktiviert	Stellen Sie sicher, dass auf der AWS Step Functions Functions-Maschine die Protokollierung aktiviert ist Die Regel ist NON_COMPLIANT, wenn für eine Zustandsmaschine die Protokollierung nicht aktiviert ist oder die Protokollierungskonfiguration nicht auf dem angegebenen Mindestniveau liegt.
10.2.1.3	Auditprotokolle werden implementiert, um die Erkennung von Anomalien und verdächtigen Aktivitäten sowie die forensische Analyse von Ereignissen zu unterstützen. (PCI-DSS-v4.0)	netfw-logging-enabled	Stellen Sie sicher, dass die AWS Netzwerk-Firewall-Firewalls die Protokollierung aktiviert haben. Die Regel ist NON_COMPLIANT, wenn kein Protokollierungstyp konfiguriert ist. Sie können angeben, welchen Protokollierungstyp die Regel prüfen soll.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.2.1.4	Auditprotokolle werden implementiert, um die Erkennung von Anomalien und verdächtigen Aktivitäten sowie die forensische Analyse von Ereignissen zu unterstützen. (PCI-DSS-v4.0)	api-gwv2- access-logs-enabled	Stellen Sie sicher, dass die Amazon API Gateway V2-Stufen die Zugriffsprotokollierung aktiviert haben. Die Regel ist NON_COMPLIANT, wenn 'accessLogSettings' in der Stage-Konfiguration nicht vorhanden ist.
10.2.1.4	Auditprotokolle werden implementiert, um die Erkennung von Anomalien und verdächtigen Aktivitäten sowie die forensische Analyse von Ereignissen zu unterstützen. (PCI-DSS-v4.0)	api-gw-xray-enabled	Stellen Sie sicher, dass AWS X-Ray Tracing auf Amazon API Gateway REST APIs aktiviert ist. Die Regel ist COMPLIANT, wenn die X-Ray-Abl aufverfolgung aktiviert ist, andernfalls ist sie NON_COMPLIANT.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.2.1.4	Auditprotokolle werden implementiert, um die Erkennung von Anomalien und verdächtigen Aktivitäten sowie die forensische Analyse von Ereignissen zu unterstützen. (PCI-DSS-v4.0)	cloudfront-accesslogs-enabled	Stellen Sie sicher, dass CloudFront Amazon-Distributionen so konfiguriert sind, dass sie Zugriffsprotokolle an einen Amazon S3-Bucket senden. Die Regel lautet NON_COMPLIANT, wenn für eine CloudFront Distribution keine Protokollierung konfiguriert ist.
10.2.1.4	Auditprotokolle werden implementiert, um die Erkennung von Anomalien und verdächtigen Aktivitäten sowie die forensische Analyse von Ereignissen zu unterstützen. (PCI-DSS-v4.0)	neptune-cluster-cloudwatch-log-exportfähig	Stellen Sie sicher, dass in einem Amazon Neptune Neptune-Cluster der Protokollexport für CloudWatch Audit-Logs aktiviert ist. Die Regel lautet NON_COMPLIANT, wenn für einen Neptune-Cluster der Protokollexport für CloudWatch Audit-Logs nicht aktiviert ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.2.1.4	Auditprotokolle werden implementiert, um die Erkennung von Anomalien und verdächtigen Aktivitäten sowie die forensische Analyse von Ereignissen zu unterstützen. (PCI-DSS-v4.0)	ecs-task-definition-log-Konfiguration	Stellen Sie sicher, dass LogConfiguration für aktive ECS-Aufgabendefinitionen festgelegt ist. Diese Regel ist NON_COMPLIANT, wenn für eine aktive ECSTask Definition die LogConfiguration-Ressource nicht definiert ist oder der Wert für LogConfiguration in mindestens einer Containerdefinition Null ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.2.1.4	Auditprotokolle werden implementiert, um die Erkennung von Anomalien und verdächtigen Aktivitäten sowie die forensische Analyse von Ereignissen zu unterstützen. (PCI-DSS-v4.0)	cloudtrail-enabled	Hinweis: Bei dieser Regel untersche iden sich die Regel-ID (CLOUD_TR AIL_ENABLED) und der Regelname (cloudtrail-enabled). Stellen Sie sicher, dass in Ihrem Konto ein Trail aktiviert ist AWS CloudTrail . AWS Die Regel ist NON_COMPLIANT, wenn ein Trail nicht aktiviert ist. Optional überprüft die Regel einen bestimmten S3-Bucket, ein Amazon Simple Notification Service (Amazon SNS) -Thema und eine CloudWatch Protokollgruppe.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.2.1.4	Auditprotokolle werden implementiert, um die Erkennung von Anomalien und verdächtigen Aktivitäten sowie die forensische Analyse von Ereignissen zu unterstützen. (PCI-DSS-v4.0)	multi-region-cloudtrail-enabled	Hinweis: Bei dieser Regel untersche iden sich die Regel-ID (MULTI_RE GION_CLOU D_TRAIL_ENABLED) und der Regelname (). multi-region-cloudtrail-enabled Stellen Sie sicher, dass mindesten s eine Region mit mehreren Regionen vorhanden ist. AWS CloudTrail Die Regel ist NON_COMPL IANT, wenn die Trails nicht mit den Eingabeparametern übereinstimmen. Die Regel lautet NON_COMPLIANT, wenn das ExcludeMa nagementEventSourc es Feld nicht leer ist oder wenn sie so konfiguriert AWS CloudTrail ist, dass Verwaltungsereigni sse wie AWS KMS-Ereignisse oder Amazon RDS-Daten -API-Ereignisse

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			ausgeschlossen werden.
10.2.1.4	Auditprotokolle werden implementiert, um die Erkennung von Anomalien und verdächtigen Aktivitäten sowie die forensische Analyse von Ereignissen zu unterstützen. (PCI-DSS-v4.0)	appsync-logging-enabled	Stellen Sie sicher, dass für eine API die Protokollierung aktiviert ist. AWS AppSync Die Regel lautet NON_COMPLIANT, wenn die Protokollierung nicht aktiviert ist, oder 'fieldLogLevel' ist weder ERROR noch ALL.
10.2.1.4	Auditprotokolle werden implementiert, um die Erkennung von Anomalien und verdächtigen Aktivitäten sowie die forensische Analyse von Ereignissen zu unterstützen. (PCI-DSS-v4.0)	waf-classic-logging-enabled	Stellen Sie sicher, dass die Protokollierung auf den AWS WAF Classic Global Web Access Control Lists (Web) aktiviert ist. ACLs Die Regel ist NON_COMPLIANT für eine globale Web-ACL, wenn die Protokollierung nicht aktiviert ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.2.1.4	Auditprotokolle werden implementiert, um die Erkennung von Anomalien und verdächtigen Aktivitäten sowie die forensische Analyse von Ereignissen zu unterstützen. (PCI-DSS-v4.0)	mq-cloudwatch-audit-logging-aktiviert	Stellen Sie sicher, dass Amazon MQ-Broker die CloudWatch Amazon-Auditprotokollierung aktiviert haben. Die Regel ist NON_COMPLIANT, wenn für einen Broker die Audit-Protokollierung nicht aktiviert ist.
10.2.1.4	Auditprotokolle werden implementiert, um die Erkennung von Anomalien und verdächtigen Aktivitäten sowie die forensische Analyse von Ereignissen zu unterstützen. (PCI-DSS-v4.0)	mq-cloudwatch-audit-log-aktiviert	Stellen Sie sicher, dass bei einem Amazon MQ-Broker die CloudWatch Auditprotokollierung aktiviert ist. Die Regel lautet NON_COMPLIANT, wenn für den Broker die Audit-Protokollierung nicht aktiviert ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.2.1.4	Auditprotokolle werden implementiert, um die Erkennung von Anomalien und verdächtigen Aktivitäten sowie die forensische Analyse von Ereignissen zu unterstützen. (PCI-DSS-v4.0)	eks-cluster-logging-enabled	Stellen Sie sicher, dass ein Amazon Elastic Kubernete s Service (Amazon EKS) -Cluster mit aktivierter Protokoll ierung konfiguriert ist. Die Regel ist NON_COMPLIANT, wenn die Protokoll ierung für Amazon-EKS-Cluster nicht für alle Protokolltypen aktiviert ist.
10.2.1.4	Auditprotokolle werden implementiert, um die Erkennung von Anomalien und verdächtigen Aktivitäten sowie die forensische Analyse von Ereignissen zu unterstützen. (PCI-DSS-v4.0)	elastic-beanstalk-logs-to-Wolkenbeob achtung	Stellen Sie sicher, dass AWS Elastic Beanstalk Beanstalk -Umgebungen so konfiguriert sind, dass sie Protokolle an Amazon CloudWatc h Logs senden. Die Regel lautet NON_COMPLIANT, wenn der Wert von `` StreamLogs falsch ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.2.1.4	Auditprotokolle werden implementiert, um die Erkennung von Anomalien und verdächtigen Aktivitäten sowie die forensische Analyse von Ereignissen zu unterstützen. (PCI-DSS-v4.0)	step-functions-state-machine-Protokollierung aktiviert	Stellen Sie sicher, dass auf der AWS Step Functions Functions-Maschine die Protokollierung aktiviert ist Die Regel ist NON_COMPLIANT, wenn für eine Zustandsmaschine die Protokollierung nicht aktiviert ist oder die Protokollierungskonfiguration nicht auf dem angegebenen Mindestniveau liegt.
10.2.1.4	Auditprotokolle werden implementiert, um die Erkennung von Anomalien und verdächtigen Aktivitäten sowie die forensische Analyse von Ereignissen zu unterstützen. (PCI-DSS-v4.0)	netfw-logging-enabled	Stellen Sie sicher, dass die AWS Netzwerk-Firewall-Firewalls die Protokollierung aktiviert haben. Die Regel ist NON_COMPLIANT, wenn kein Protokollierungstyp konfiguriert ist. Sie können angeben, welchen Protokollierungstyp die Regel prüfen soll.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.2.1.5	Auditprotokolle werden implementiert, um die Erkennung von Anomalien und verdächtigen Aktivitäten sowie die forensische Analyse von Ereignissen zu unterstützen. (PCI-DSS-v4.0)	api-gwv2- access-logs-enabled	Stellen Sie sicher, dass die Amazon API Gateway V2-Stufen die Zugriffsprotokollierung aktiviert haben. Die Regel ist NON_COMPLIANT, wenn 'accessLogSettings' in der Stage-Konfiguration nicht vorhanden ist.
10.2.1.5	Auditprotokolle werden implementiert, um die Erkennung von Anomalien und verdächtigen Aktivitäten sowie die forensische Analyse von Ereignissen zu unterstützen. (PCI-DSS-v4.0)	api-gw-xray-enabled	Stellen Sie sicher, dass AWS X-Ray Tracing auf Amazon API Gateway REST APIs aktiviert ist. Die Regel ist COMPLIANT, wenn die X-Ray-Ablaufverfolgung aktiviert ist, andernfalls ist sie NON_COMPLIANT.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.2.1.5	Auditprotokolle werden implementiert, um die Erkennung von Anomalien und verdächtigen Aktivitäten sowie die forensische Analyse von Ereignissen zu unterstützen. (PCI-DSS-v4.0)	cloudfront-accesslogs-enabled	Stellen Sie sicher, dass CloudFront Amazon-Distributionen so konfiguriert sind, dass sie Zugriffsprotokolle an einen Amazon S3-Bucket senden. Die Regel lautet NON_COMPLIANT, wenn für eine CloudFront Distribution keine Protokollierung konfiguriert ist.
10.2.1.5	Auditprotokolle werden implementiert, um die Erkennung von Anomalien und verdächtigen Aktivitäten sowie die forensische Analyse von Ereignissen zu unterstützen. (PCI-DSS-v4.0)	neptune-cluster-cloudwatch-log-exportfähig	Stellen Sie sicher, dass in einem Amazon Neptune Neptune-Cluster der Protokollexport für CloudWatch Audit-Logs aktiviert ist. Die Regel lautet NON_COMPLIANT, wenn für einen Neptune-Cluster der Protokollexport für CloudWatch Audit-Logs nicht aktiviert ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.2.1.5	Auditprotokolle werden implementiert, um die Erkennung von Anomalien und verdächtigen Aktivitäten sowie die forensische Analyse von Ereignissen zu unterstützen. (PCI-DSS-v4.0)	ecs-task-definition-log-Konfiguration	Stellen Sie sicher, dass LogConfiguration für aktive ECS-Aufgabendefinitionen festgelegt ist. Diese Regel ist NON_COMPLIANT, wenn für eine aktive ECSTask Definition die LogConfiguration-Ressource nicht definiert ist oder der Wert für LogConfiguration in mindestens einer Containerdefinition Null ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.2.1.5	Auditprotokolle werden implementiert, um die Erkennung von Anomalien und verdächtigen Aktivitäten sowie die forensische Analyse von Ereignissen zu unterstützen. (PCI-DSS-v4.0)	cloudtrail-enabled	Hinweis: Bei dieser Regel untersche iden sich die Regel-ID (CLOUD_TR AIL_ENABLED) und der Regelname (cloudtrail-enabled). Stellen Sie sicher, dass in Ihrem Konto ein Trail aktiviert ist AWS CloudTrail . AWS Die Regel ist NON_COMPLIANT, wenn ein Trail nicht aktiviert ist. Optional überprüft die Regel einen bestimmten S3-Bucket, ein Amazon Simple Notification Service (Amazon SNS) -Thema und eine CloudWatch Protokollgruppe.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.2.1.5	Auditprotokolle werden implementiert, um die Erkennung von Anomalien und verdächtigen Aktivitäten sowie die forensische Analyse von Ereignissen zu unterstützen. (PCI-DSS-v4.0)	multi-region-cloudtrail-enabled	Hinweis: Bei dieser Regel untersche iden sich die Regel-ID (MULTI_RE GION_CLOU D_TRAIL_ENABLED) und der Regelname (). multi-region-cloudtrail-enabled Stellen Sie sicher, dass mindesten s eine Region mit mehreren Regionen vorhanden ist. AWS CloudTrail Die Regel ist NON_COMPL IANT, wenn die Trails nicht mit den Eingabeparametern übereinstimmen. Die Regel lautet NON_COMPLIANT, wenn das ExcludeMa nagementEventSourc es Feld nicht leer ist oder wenn sie so konfiguriert AWS CloudTrail ist, dass Verwaltungsereigni sse wie AWS KMS-Ereignisse oder Amazon RDS-Daten -API-Ereignisse

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			ausgeschlossen werden.
10.2.1.5	Auditprotokolle werden implementiert, um die Erkennung von Anomalien und verdächtigen Aktivitäten sowie die forensische Analyse von Ereignissen zu unterstützen. (PCI-DSS-v4.0)	appsync-logging-enabled	Stellen Sie sicher, dass für eine API die Protokollierung aktiviert ist. AWS AppSync Die Regel lautet NON_COMPLIANT, wenn die Protokollierung nicht aktiviert ist, oder 'fieldLogLevel' ist weder ERROR noch ALL.
10.2.1.5	Auditprotokolle werden implementiert, um die Erkennung von Anomalien und verdächtigen Aktivitäten sowie die forensische Analyse von Ereignissen zu unterstützen. (PCI-DSS-v4.0)	waf-classic-logging-enabled	Stellen Sie sicher, dass die Protokollierung auf den AWS WAF Classic Global Web Access Control Lists (Web) aktiviert ist. ACLs Die Regel ist NON_COMPLIANT für eine globale Web-ACL, wenn die Protokollierung nicht aktiviert ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.2.1.5	Auditprotokolle werden implementiert, um die Erkennung von Anomalien und verdächtigen Aktivitäten sowie die forensische Analyse von Ereignissen zu unterstützen. (PCI-DSS-v4.0)	mq-cloudwatch-audit-logging-aktiviert	Stellen Sie sicher, dass Amazon MQ-Broker die CloudWatch Amazon-Auditprotokollierung aktiviert haben. Die Regel ist NON_COMPLIANT, wenn für einen Broker die Audit-Protokollierung nicht aktiviert ist.
10.2.1.5	Auditprotokolle werden implementiert, um die Erkennung von Anomalien und verdächtigen Aktivitäten sowie die forensische Analyse von Ereignissen zu unterstützen. (PCI-DSS-v4.0)	mq-cloudwatch-audit-log-aktiviert	Stellen Sie sicher, dass bei einem Amazon MQ-Broker die CloudWatch Auditprotokollierung aktiviert ist. Die Regel lautet NON_COMPLIANT, wenn für den Broker die Audit-Protokollierung nicht aktiviert ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.2.1.5	Auditprotokolle werden implementiert, um die Erkennung von Anomalien und verdächtigen Aktivitäten sowie die forensische Analyse von Ereignissen zu unterstützen. (PCI-DSS-v4.0)	eks-cluster-logging-enabled	Stellen Sie sicher, dass ein Amazon Elastic Kubernete s Service (Amazon EKS) -Cluster mit aktivierter Protokoll ierung konfiguriert ist. Die Regel ist NON_COMPLIANT, wenn die Protokoll ierung für Amazon-EKS-Cluster nicht für alle Protokolltypen aktiviert ist.
10.2.1.5	Auditprotokolle werden implementiert, um die Erkennung von Anomalien und verdächtigen Aktivitäten sowie die forensische Analyse von Ereignissen zu unterstützen. (PCI-DSS-v4.0)	elastic-beanstalk-logs-to-Wolkenbeob achtung	Stellen Sie sicher, dass AWS Elastic Beanstalk Beanstalk -Umgebungen so konfiguriert sind, dass sie Protokolle an Amazon CloudWatc h Logs senden. Die Regel lautet NON_COMPLIANT, wenn der Wert von `` StreamLogs falsch ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.2.1.5	Auditprotokolle werden implementiert, um die Erkennung von Anomalien und verdächtigen Aktivitäten sowie die forensische Analyse von Ereignissen zu unterstützen. (PCI-DSS-v4.0)	step-functions-state-machine-Protokollierung aktiviert	Stellen Sie sicher, dass auf der AWS Step Functions Functions-Maschine die Protokollierung aktiviert ist Die Regel ist NON_COMPLIANT, wenn für eine Zustandsmaschine die Protokollierung nicht aktiviert ist oder die Protokollierungskonfiguration nicht auf dem angegebenen Mindestniveau liegt.
10.2.1.5	Auditprotokolle werden implementiert, um die Erkennung von Anomalien und verdächtigen Aktivitäten sowie die forensische Analyse von Ereignissen zu unterstützen. (PCI-DSS-v4.0)	netfw-logging-enabled	Stellen Sie sicher, dass die AWS Netzwerk-Firewall-Firewalls die Protokollierung aktiviert haben. Die Regel ist NON_COMPLIANT, wenn kein Protokollierungstyp konfiguriert ist. Sie können angeben, welchen Protokollierungstyp die Regel prüfen soll.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.2.1.6	Auditprotokolle werden implementiert, um die Erkennung von Anomalien und verdächtigen Aktivitäten sowie die forensische Analyse von Ereignissen zu unterstützen. (PCI-DSS-v4.0)	api-gwv2- access-logs-enabled	Stellen Sie sicher, dass die Amazon API Gateway V2-Stufen die Zugriffsprotokollierung aktiviert haben. Die Regel ist NON_COMPLIANT, wenn 'accessLogSettings' in der Stage-Konfiguration nicht vorhanden ist.
10.2.1.6	Auditprotokolle werden implementiert, um die Erkennung von Anomalien und verdächtigen Aktivitäten sowie die forensische Analyse von Ereignissen zu unterstützen. (PCI-DSS-v4.0)	api-gw-xray-enabled	Stellen Sie sicher, dass AWS X-Ray Tracing auf Amazon API Gateway REST APIs aktiviert ist. Die Regel ist COMPLIANT, wenn die X-Ray-Abl aufverfolgung aktiviert ist, andernfalls ist sie NON_COMPLIANT.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.2.1.6	Auditprotokolle werden implementiert, um die Erkennung von Anomalien und verdächtigen Aktivitäten sowie die forensische Analyse von Ereignissen zu unterstützen. (PCI-DSS-v4.0)	cloudfront-accesslogs-enabled	Stellen Sie sicher, dass CloudFront Amazon-Distributionen so konfiguriert sind, dass sie Zugriffsprotokolle an einen Amazon S3-Bucket senden. Die Regel lautet NON_COMPLIANT, wenn für eine CloudFront Distribution keine Protokollierung konfiguriert ist.
10.2.1.6	Auditprotokolle werden implementiert, um die Erkennung von Anomalien und verdächtigen Aktivitäten sowie die forensische Analyse von Ereignissen zu unterstützen. (PCI-DSS-v4.0)	neptune-cluster-cloudwatch-log-exportfähig	Stellen Sie sicher, dass in einem Amazon Neptune Neptune-Cluster der Protokollexport für CloudWatch Audit-Logs aktiviert ist. Die Regel lautet NON_COMPLIANT, wenn für einen Neptune-Cluster der Protokollexport für CloudWatch Audit-Logs nicht aktiviert ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.2.1.6	Auditprotokolle werden implementiert, um die Erkennung von Anomalien und verdächtigen Aktivitäten sowie die forensische Analyse von Ereignissen zu unterstützen. (PCI-DSS-v4.0)	ecs-task-definition-log-Konfiguration	Stellen Sie sicher, dass LogConfiguration für aktive ECS-Aufgabendefinitionen festgelegt ist. Diese Regel ist NON_COMPLIANT, wenn für eine aktive ECSTask Definition die LogConfiguration-Ressource nicht definiert ist oder der Wert für LogConfiguration in mindestens einer Containerdefinition Null ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.2.1.6	Auditprotokolle werden implementiert, um die Erkennung von Anomalien und verdächtigen Aktivitäten sowie die forensische Analyse von Ereignissen zu unterstützen. (PCI-DSS-v4.0)	cloudtrail-enabled	Hinweis: Bei dieser Regel untersche iden sich die Regel-ID (CLOUD_TR AIL_ENABLED) und der Regelname (cloudtrail-enabled). Stellen Sie sicher, dass in Ihrem Konto ein Trail aktiviert ist AWS CloudTrail . AWS Die Regel ist NON_COMPLIANT, wenn ein Trail nicht aktiviert ist. Optional überprüft die Regel einen bestimmten S3-Bucket, ein Amazon Simple Notification Service (Amazon SNS) -Thema und eine CloudWatch Protokollgruppe.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.2.1.6	Auditprotokolle werden implementiert, um die Erkennung von Anomalien und verdächtigen Aktivitäten sowie die forensische Analyse von Ereignissen zu unterstützen. (PCI-DSS-v4.0)	multi-region-cloudtrail-enabled	Hinweis: Bei dieser Regel untersche iden sich die Regel-ID (MULTI_RE GION_CLOU D_TRAIL_ENABLED) und der Regelname (). multi-region-cloudtrail-enabled Stellen Sie sicher, dass mindesten s eine Region mit mehreren Regionen vorhanden ist. AWS CloudTrail Die Regel ist NON_COMPL IANT, wenn die Trails nicht mit den Eingabeparametern übereinstimmen. Die Regel lautet NON_COMPLIANT, wenn das ExcludeMa nagementEventSourc es Feld nicht leer ist oder wenn sie so konfiguriert AWS CloudTrail ist, dass Verwaltungsereigni sse wie AWS KMS-Ereignisse oder Amazon RDS-Daten -API-Ereignisse

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			ausgeschlossen werden.
10.2.1.6	Auditprotokolle werden implementiert, um die Erkennung von Anomalien und verdächtigen Aktivitäten sowie die forensische Analyse von Ereignissen zu unterstützen. (PCI-DSS-v4.0)	appsync-logging-enabled	Stellen Sie sicher, dass für eine API die Protokollierung aktiviert ist. AWS AppSync Die Regel lautet NON_COMPLIANT, wenn die Protokollierung nicht aktiviert ist, oder 'fieldLogLevel' ist weder ERROR noch ALL.
10.2.1.6	Auditprotokolle werden implementiert, um die Erkennung von Anomalien und verdächtigen Aktivitäten sowie die forensische Analyse von Ereignissen zu unterstützen. (PCI-DSS-v4.0)	waf-classic-logging-enabled	Stellen Sie sicher, dass die Protokollierung auf den AWS WAF Classic Global Web Access Control Lists (Web) aktiviert ist. ACLs Die Regel ist NON_COMPLIANT für eine globale Web-ACL, wenn die Protokollierung nicht aktiviert ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.2.1.6	Auditprotokolle werden implementiert, um die Erkennung von Anomalien und verdächtigen Aktivitäten sowie die forensische Analyse von Ereignissen zu unterstützen. (PCI-DSS-v4.0)	mq-cloudwatch-audit-logging-aktiviert	Stellen Sie sicher, dass Amazon MQ-Broker die CloudWatch Amazon-Auditprotokollierung aktiviert haben. Die Regel ist NON_COMPLIANT, wenn für einen Broker die Audit-Protokollierung nicht aktiviert ist.
10.2.1.6	Auditprotokolle werden implementiert, um die Erkennung von Anomalien und verdächtigen Aktivitäten sowie die forensische Analyse von Ereignissen zu unterstützen. (PCI-DSS-v4.0)	mq-cloudwatch-audit-log-aktiviert	Stellen Sie sicher, dass bei einem Amazon MQ-Broker die CloudWatch Auditprotokollierung aktiviert ist. Die Regel lautet NON_COMPLIANT, wenn für den Broker die Audit-Protokollierung nicht aktiviert ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.2.1.6	Auditprotokolle werden implementiert, um die Erkennung von Anomalien und verdächtigen Aktivitäten sowie die forensische Analyse von Ereignissen zu unterstützen. (PCI-DSS-v4.0)	eks-cluster-logging-enabled	Stellen Sie sicher, dass ein Amazon Elastic Kubernete s Service (Amazon EKS) -Cluster mit aktivierter Protokoll ierung konfiguriert ist. Die Regel ist NON_COMPLIANT, wenn die Protokoll ierung für Amazon-EKS-Cluster nicht für alle Protokolltypen aktiviert ist.
10.2.1.6	Auditprotokolle werden implementiert, um die Erkennung von Anomalien und verdächtigen Aktivitäten sowie die forensische Analyse von Ereignissen zu unterstützen. (PCI-DSS-v4.0)	elastic-beanstalk-logs-to-Wolkenbeob achtung	Stellen Sie sicher, dass AWS Elastic Beanstalk Beanstalk -Umgebungen so konfiguriert sind, dass sie Protokolle an Amazon CloudWatc h Logs senden. Die Regel lautet NON_COMPLIANT, wenn der Wert von `` StreamLogs falsch ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.2.1.6	Auditprotokolle werden implementiert, um die Erkennung von Anomalien und verdächtigen Aktivitäten sowie die forensische Analyse von Ereignissen zu unterstützen. (PCI-DSS-v4.0)	step-functions-state-machine-Protokollierung aktiviert	Stellen Sie sicher, dass auf der AWS Step Functions Functions-Maschine die Protokollierung aktiviert ist Die Regel ist NON_COMPLIANT, wenn für eine Zustandsmaschine die Protokollierung nicht aktiviert ist oder die Protokollierungskonfiguration nicht auf dem angegebenen Mindestniveau liegt.
10.2.1.6	Auditprotokolle werden implementiert, um die Erkennung von Anomalien und verdächtigen Aktivitäten sowie die forensische Analyse von Ereignissen zu unterstützen. (PCI-DSS-v4.0)	netfw-logging-enabled	Stellen Sie sicher, dass die AWS Netzwerk-Firewall-Firewalls die Protokollierung aktiviert haben. Die Regel ist NON_COMPLIANT, wenn kein Protokollierungstyp konfiguriert ist. Sie können angeben, welchen Protokollierungstyp die Regel prüfen soll.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.2.1.7	Auditprotokolle werden implementiert, um die Erkennung von Anomalien und verdächtigen Aktivitäten sowie die forensische Analyse von Ereignissen zu unterstützen. (PCI-DSS-v4.0)	api-gwv2- access-logs-enabled	Stellen Sie sicher, dass die Amazon API Gateway V2-Stufen die Zugriffsprotokollierung aktiviert haben. Die Regel ist NON_COMPLIANT, wenn 'accessLogSettings' in der Stage-Konfiguration nicht vorhanden ist.
10.2.1.7	Auditprotokolle werden implementiert, um die Erkennung von Anomalien und verdächtigen Aktivitäten sowie die forensische Analyse von Ereignissen zu unterstützen. (PCI-DSS-v4.0)	api-gw-xray-enabled	Stellen Sie sicher, dass AWS X-Ray Tracing auf Amazon API Gateway REST APIs aktiviert ist. Die Regel ist COMPLIANT, wenn die X-Ray-Abl aufverfolgung aktiviert ist, andernfalls ist sie NON_COMPLIANT.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.2.1.7	Auditprotokolle werden implementiert, um die Erkennung von Anomalien und verdächtigen Aktivitäten sowie die forensische Analyse von Ereignissen zu unterstützen. (PCI-DSS-v4.0)	cloudfront-accesslogs-enabled	Stellen Sie sicher, dass CloudFront Amazon-Distributionen so konfiguriert sind, dass sie Zugriffsprotokolle an einen Amazon S3-Bucket senden. Die Regel lautet NON_COMPLIANT, wenn für eine CloudFront Distribution keine Protokollierung konfiguriert ist.
10.2.1.7	Auditprotokolle werden implementiert, um die Erkennung von Anomalien und verdächtigen Aktivitäten sowie die forensische Analyse von Ereignissen zu unterstützen. (PCI-DSS-v4.0)	neptune-cluster-cloudwatch-log-exportfähig	Stellen Sie sicher, dass in einem Amazon Neptune Neptune-Cluster der Protokollexport für CloudWatch Audit-Logs aktiviert ist. Die Regel lautet NON_COMPLIANT, wenn für einen Neptune-Cluster der Protokollexport für CloudWatch Audit-Logs nicht aktiviert ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.2.1.7	Auditprotokolle werden implementiert, um die Erkennung von Anomalien und verdächtigen Aktivitäten sowie die forensische Analyse von Ereignissen zu unterstützen. (PCI-DSS-v4.0)	ecs-task-definition-log-Konfiguration	Stellen Sie sicher, dass LogConfiguration für aktive ECS-Aufgabendefinitionen festgelegt ist. Diese Regel ist NON_COMPLIANT, wenn für eine aktive ECSTask Definition die LogConfiguration-Ressource nicht definiert ist oder der Wert für LogConfiguration in mindestens einer Containerdefinition Null ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.2.1.7	Auditprotokolle werden implementiert, um die Erkennung von Anomalien und verdächtigen Aktivitäten sowie die forensische Analyse von Ereignissen zu unterstützen. (PCI-DSS-v4.0)	cloudtrail-enabled	Hinweis: Bei dieser Regel untersche iden sich die Regel-ID (CLOUD_TR AIL_ENABLED) und der Regelname (cloudtrail-enabled). Stellen Sie sicher, dass in Ihrem Konto ein Trail aktiviert ist AWS CloudTrail . AWS Die Regel ist NON_COMPLIANT, wenn ein Trail nicht aktiviert ist. Optional überprüft die Regel einen bestimmten S3-Bucket, ein Amazon Simple Notification Service (Amazon SNS) -Thema und eine CloudWatch Protokollgruppe.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.2.1.7	Auditprotokolle werden implementiert, um die Erkennung von Anomalien und verdächtigen Aktivitäten sowie die forensische Analyse von Ereignissen zu unterstützen. (PCI-DSS-v4.0)	multi-region-cloudtrail-enabled	Hinweis: Bei dieser Regel untersche iden sich die Regel-ID (MULTI_RE GION_CLOU D_TRAIL_ENABLED) und der Regelname (). multi-region-cloudtrail-enabled Stellen Sie sicher, dass mindesten s eine Region mit mehreren Regionen vorhanden ist. AWS CloudTrail Die Regel ist NON_COMPL IANT, wenn die Trails nicht mit den Eingabeparametern übereinstimmen. Die Regel lautet NON_COMPLIANT, wenn das ExcludeMa nagementEventSourc es Feld nicht leer ist oder wenn sie so konfiguriert AWS CloudTrail ist, dass Verwaltungsereigni sse wie AWS KMS-Ereignisse oder Amazon RDS-Daten -API-Ereignisse

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			ausgeschlossen werden.
10.2.1.7	Auditprotokolle werden implementiert, um die Erkennung von Anomalien und verdächtigen Aktivitäten sowie die forensische Analyse von Ereignissen zu unterstützen. (PCI-DSS-v4.0)	appsync-logging-enabled	Stellen Sie sicher, dass für eine API die Protokollierung aktiviert ist. AWS AppSync Die Regel lautet NON_COMPLIANT, wenn die Protokollierung nicht aktiviert ist, oder 'fieldLogLevel' ist weder ERROR noch ALL.
10.2.1.7	Auditprotokolle werden implementiert, um die Erkennung von Anomalien und verdächtigen Aktivitäten sowie die forensische Analyse von Ereignissen zu unterstützen. (PCI-DSS-v4.0)	waf-classic-logging-enabled	Stellen Sie sicher, dass die Protokollierung auf den AWS WAF Classic Global Web Access Control Lists (Web) aktiviert ist. ACLs Die Regel ist NON_COMPLIANT für eine globale Web-ACL, wenn die Protokollierung nicht aktiviert ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.2.1.7	Auditprotokolle werden implementiert, um die Erkennung von Anomalien und verdächtigen Aktivitäten sowie die forensische Analyse von Ereignissen zu unterstützen. (PCI-DSS-v4.0)	mq-cloudwatch-audit-logging-aktiviert	Stellen Sie sicher, dass Amazon MQ-Broker die CloudWatch Amazon-Auditprotokollierung aktiviert haben. Die Regel ist NON_COMPLIANT, wenn für einen Broker die Audit-Protokollierung nicht aktiviert ist.
10.2.1.7	Auditprotokolle werden implementiert, um die Erkennung von Anomalien und verdächtigen Aktivitäten sowie die forensische Analyse von Ereignissen zu unterstützen. (PCI-DSS-v4.0)	mq-cloudwatch-audit-log-aktiviert	Stellen Sie sicher, dass bei einem Amazon MQ-Broker die CloudWatch Auditprotokollierung aktiviert ist. Die Regel lautet NON_COMPLIANT, wenn für den Broker die Audit-Protokollierung nicht aktiviert ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.2.1.7	Auditprotokolle werden implementiert, um die Erkennung von Anomalien und verdächtigen Aktivitäten sowie die forensische Analyse von Ereignissen zu unterstützen. (PCI-DSS-v4.0)	eks-cluster-logging-enabled	Stellen Sie sicher, dass ein Amazon Elastic Kubernete s Service (Amazon EKS) -Cluster mit aktivierter Protokoll ierung konfiguriert ist. Die Regel ist NON_COMPLIANT, wenn die Protokoll ierung für Amazon-EKS-Cluster nicht für alle Protokolltypen aktiviert ist.
10.2.1.7	Auditprotokolle werden implementiert, um die Erkennung von Anomalien und verdächtigen Aktivitäten sowie die forensische Analyse von Ereignissen zu unterstützen. (PCI-DSS-v4.0)	elastic-beanstalk-logs-to-Wolkenbeob achtung	Stellen Sie sicher, dass AWS Elastic Beanstalk Beanstalk -Umgebungen so konfiguriert sind, dass sie Protokolle an Amazon CloudWatc h Logs senden. Die Regel lautet NON_COMPLIANT, wenn der Wert von `` StreamLogs falsch ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.2.1.7	Auditprotokolle werden implementiert, um die Erkennung von Anomalien und verdächtigen Aktivitäten sowie die forensische Analyse von Ereignissen zu unterstützen. (PCI-DSS-v4.0)	step-functions-state-machine-Protokollierung aktiviert	Stellen Sie sicher, dass auf der AWS Step Functions Functions-Maschine die Protokollierung aktiviert ist Die Regel ist NON_COMPLIANT, wenn für eine Zustandsmaschine die Protokollierung nicht aktiviert ist oder die Protokollierungskonfiguration nicht auf dem angegebenen Mindestniveau liegt.
10.2.1.7	Auditprotokolle werden implementiert, um die Erkennung von Anomalien und verdächtigen Aktivitäten sowie die forensische Analyse von Ereignissen zu unterstützen. (PCI-DSS-v4.0)	netfw-logging-enabled	Stellen Sie sicher, dass die AWS Netzwerk-Firewall-Firewalls die Protokollierung aktiviert haben. Die Regel ist NON_COMPLIANT, wenn kein Protokollierungstyp konfiguriert ist. Sie können angeben, welchen Protokollierungstyp die Regel prüfen soll.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.2.2	Auditprotokolle werden implementiert, um die Erkennung von Anomalien und verdächtigen Aktivitäten sowie die forensische Analyse von Ereignissen zu unterstützen. (PCI-DSS-v4.0)	api-gwv2- access-logs-enabled	Stellen Sie sicher, dass die Amazon API Gateway V2-Stufen die Zugriffsprotokollierung aktiviert haben. Die Regel ist NON_COMPLIANT, wenn 'accessLogSettings' in der Stage-Konfiguration nicht vorhanden ist.
10.2.2	Auditprotokolle werden implementiert, um die Erkennung von Anomalien und verdächtigen Aktivitäten sowie die forensische Analyse von Ereignissen zu unterstützen. (PCI-DSS-v4.0)	api-gw-xray-enabled	Stellen Sie sicher, dass AWS X-Ray Tracing auf Amazon API Gateway REST APIs aktiviert ist. Die Regel ist COMPLIANT, wenn die X-Ray-Abl aufverfolgung aktiviert ist, andernfalls ist sie NON_COMPLIANT.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.2.2	Auditprotokolle werden implementiert, um die Erkennung von Anomalien und verdächtigen Aktivitäten sowie die forensische Analyse von Ereignissen zu unterstützen. (PCI-DSS-v4.0)	cloudfront-accesslogs-enabled	Stellen Sie sicher, dass CloudFront Amazon-Distributionen so konfiguriert sind, dass sie Zugriffsprotokolle an einen Amazon S3-Bucket senden. Die Regel lautet NON_COMPLIANT, wenn für eine CloudFront Distribution keine Protokollierung konfiguriert ist.
10.2.2	Auditprotokolle werden implementiert, um die Erkennung von Anomalien und verdächtigen Aktivitäten sowie die forensische Analyse von Ereignissen zu unterstützen. (PCI-DSS-v4.0)	neptune-cluster-cloudwatch-log-exportfähig	Stellen Sie sicher, dass in einem Amazon Neptune Neptune-Cluster der Protokollexport für CloudWatch Audit-Logs aktiviert ist. Die Regel lautet NON_COMPLIANT, wenn für einen Neptune-Cluster der Protokollexport für CloudWatch Audit-Logs nicht aktiviert ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.2.2	Auditprotokolle werden implementiert, um die Erkennung von Anomalien und verdächtigen Aktivitäten sowie die forensische Analyse von Ereignissen zu unterstützen. (PCI-DSS-v4.0)	ecs-task-definition-log-Konfiguration	Stellen Sie sicher, dass LogConfiguration für aktive ECS-Aufgabendefinitionen festgelegt ist. Diese Regel ist NON_COMPLIANT, wenn für eine aktive ECSTask Definition die LogConfiguration-Ressource nicht definiert ist oder der Wert für LogConfiguration in mindestens einer Containerdefinition Null ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.2.2	Auditprotokolle werden implementiert, um die Erkennung von Anomalien und verdächtigen Aktivitäten sowie die forensische Analyse von Ereignissen zu unterstützen. (PCI-DSS-v4.0)	cloudtrail-enabled	Hinweis: Bei dieser Regel untersche iden sich die Regel-ID (CLOUD_TR AIL_ENABLED) und der Regelname (cloudtrail-enabled). Stellen Sie sicher, dass in Ihrem Konto ein Trail aktiviert ist AWS CloudTrail . AWS Die Regel ist NON_COMPLIANT, wenn ein Trail nicht aktiviert ist. Optional überprüft die Regel einen bestimmten S3-Bucket, ein Amazon Simple Notification Service (Amazon SNS) -Thema und eine CloudWatch Protokollgruppe.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.2.2	Auditprotokolle werden implementiert, um die Erkennung von Anomalien und verdächtigen Aktivitäten sowie die forensische Analyse von Ereignissen zu unterstützen. (PCI-DSS-v4.0)	multi-region-cloudtrail-enabled	Hinweis: Bei dieser Regel untersche iden sich die Regel-ID (MULTI_RE GION_CLOU D_TRAIL_ENABLED) und der Regelname (). multi-region-cloudtrail-enabled Stellen Sie sicher, dass mindesten s eine Region mit mehreren Regionen vorhanden ist. AWS CloudTrail Die Regel ist NON_COMPL IANT, wenn die Trails nicht mit den Eingabeparametern übereinstimmen. Die Regel lautet NON_COMPLIANT, wenn das ExcludeMa nagementEventSourc es Feld nicht leer ist oder wenn sie so konfiguriert AWS CloudTrail ist, dass Verwaltungsereigni sse wie AWS KMS-Ereignisse oder Amazon RDS-Daten -API-Ereignisse

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			ausgeschlossen werden.
10.2.2	Auditprotokolle werden implementiert, um die Erkennung von Anomalien und verdächtigen Aktivitäten sowie die forensische Analyse von Ereignissen zu unterstützen. (PCI-DSS-v4.0)	appsync-logging-enabled	Stellen Sie sicher, dass für eine API die Protokollierung aktiviert ist. AWS AppSync Die Regel lautet NON_COMPLIANT, wenn die Protokollierung nicht aktiviert ist, oder 'fieldLogLevel' ist weder ERROR noch ALL.
10.2.2	Auditprotokolle werden implementiert, um die Erkennung von Anomalien und verdächtigen Aktivitäten sowie die forensische Analyse von Ereignissen zu unterstützen. (PCI-DSS-v4.0)	waf-classic-logging-enabled	Stellen Sie sicher, dass die Protokollierung auf den AWS WAF Classic Global Web Access Control Lists (Web) aktiviert ist. ACLs Die Regel ist NON_COMPLIANT für eine globale Web-ACL, wenn die Protokollierung nicht aktiviert ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.2.2	Auditprotokolle werden implementiert, um die Erkennung von Anomalien und verdächtigen Aktivitäten sowie die forensische Analyse von Ereignissen zu unterstützen. (PCI-DSS-v4.0)	mq-cloudwatch-audit-logging-aktiviert	Stellen Sie sicher, dass Amazon MQ-Broker die CloudWatch Amazon-Auditprotokollierung aktiviert haben. Die Regel ist NON_COMPLIANT, wenn für einen Broker die Audit-Protokollierung nicht aktiviert ist.
10.2.2	Auditprotokolle werden implementiert, um die Erkennung von Anomalien und verdächtigen Aktivitäten sowie die forensische Analyse von Ereignissen zu unterstützen. (PCI-DSS-v4.0)	mq-cloudwatch-audit-log-aktiviert	Stellen Sie sicher, dass bei einem Amazon MQ-Broker die CloudWatch Auditprotokollierung aktiviert ist. Die Regel lautet NON_COMPLIANT, wenn für den Broker die Audit-Protokollierung nicht aktiviert ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.2.2	Auditprotokolle werden implementiert, um die Erkennung von Anomalien und verdächtigen Aktivitäten sowie die forensische Analyse von Ereignissen zu unterstützen. (PCI-DSS-v4.0)	eks-cluster-logging-enabled	Stellen Sie sicher, dass ein Amazon Elastic Kubernete s Service (Amazon EKS) -Cluster mit aktivierter Protokoll ierung konfiguriert ist. Die Regel ist NON_COMPLIANT, wenn die Protokoll ierung für Amazon-EKS-Cluster nicht für alle Protokolltypen aktiviert ist.
10.2.2	Auditprotokolle werden implementiert, um die Erkennung von Anomalien und verdächtigen Aktivitäten sowie die forensische Analyse von Ereignissen zu unterstützen. (PCI-DSS-v4.0)	elastic-beanstalk-logs-to-Wolkenbeob achtung	Stellen Sie sicher, dass AWS Elastic Beanstalk Beanstalk -Umgebungen so konfiguriert sind, dass sie Protokolle an Amazon CloudWatc h Logs senden. Die Regel lautet NON_COMPLIANT, wenn der Wert von `` StreamLogs falsch ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.2.2	Auditprotokolle werden implementiert, um die Erkennung von Anomalien und verdächtigen Aktivitäten sowie die forensische Analyse von Ereignissen zu unterstützen. (PCI-DSS-v4.0)	step-functions-state-machine-Protokollierung aktiviert	Stellen Sie sicher, dass auf der AWS Step Functions Functions-Maschine die Protokollierung aktiviert ist Die Regel ist NON_COMPLIANT, wenn für eine Zustandsmaschine die Protokollierung nicht aktiviert ist oder die Protokollierungskonfiguration nicht auf dem angegebenen Mindestniveau liegt.
10.2.2	Auditprotokolle werden implementiert, um die Erkennung von Anomalien und verdächtigen Aktivitäten sowie die forensische Analyse von Ereignissen zu unterstützen. (PCI-DSS-v4.0)	netfw-logging-enabled	Stellen Sie sicher, dass die AWS Netzwerk-Firewall-Firewalls die Protokollierung aktiviert haben. Die Regel ist NON_COMPLIANT, wenn kein Protokollierungstyp konfiguriert ist. Sie können angeben, welchen Protokollierungstyp die Regel prüfen soll.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.3.1	Auditprotokolle sind vor Zerstörung und unbefugten Änderungen geschützt. (PCI-DSS-v4.0)	api-gwv2- access-logs-enabled	Stellen Sie sicher, dass die Amazon API Gateway V2-Stufen die Zugriffsprotokollierung aktiviert haben. Die Regel ist NON_COMPLIANT, wenn 'accessLogSettings' in der Stage-Konfiguration nicht vorhanden ist.
10.3.1	Auditprotokolle sind vor Zerstörung und unbefugten Änderungen geschützt. (PCI-DSS-v4.0)	api-gw-xray-enabled	Stellen Sie sicher, dass AWS X-Ray Tracing auf Amazon API Gateway REST APIs aktiviert ist. Die Regel ist COMPLIANT, wenn die X-Ray-Ablaufverfolgung aktiviert ist, andernfalls ist sie NON_COMPLIANT.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.3.1	Auditprotokolle sind vor Zerstörung und unbefugten Änderungen geschützt. (PCI-DSS-v4.0)	cloudfront-accesslogs-enabled	Stellen Sie sicher, dass CloudFront Amazon-Distributionen so konfiguriert sind, dass sie Zugriffsprotokolle an einen Amazon S3-Bucket senden. Die Regel lautet NON_COMPLIANT, wenn für eine CloudFront Distribution keine Protokollierung konfiguriert ist.
10.3.1	Auditprotokolle sind vor Zerstörung und unbefugten Änderungen geschützt. (PCI-DSS-v4.0)	neptune-cluster-cloudwatch-log-exportfähig	Stellen Sie sicher, dass in einem Amazon Neptune Neptune-Cluster der Protokollexport für CloudWatch Audit-Logs aktiviert ist. Die Regel lautet NON_COMPLIANT, wenn für einen Neptune-Cluster der Protokollexport für CloudWatch Audit-Logs nicht aktiviert ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.3.1	Auditprotokolle sind vor Zerstörun g und unbefugte n Änderungen geschützt. (PCI-DSS-v4.0)	ecs-task-definition-log-Konfiguration	Stellen Sie sicher, dass LogConfig uration für aktive ECS-Aufgabendefini tionen festgelegt ist. Diese Regel ist NON_COMPLIANT, wenn für eine aktive ECSTask Definition die LogConfiguration-Ressource nicht definiert ist oder der Wert für LogConfig uration in mindesten s einer Container definition Null ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.3.1	Auditprotokolle sind vor Zerstörun g und unbefugte n Änderungen geschützt. (PCI-DSS-v4.0)	cloudtrail-enabled	Hinweis: Bei dieser Regel untersche iden sich die Regel-ID (CLOUD_TR AIL_ENABLED) und der Regelname (cloudtrail-enabled). Stellen Sie sicher, dass in Ihrem Konto ein Trail aktiviert ist AWS CloudTrail . AWS Die Regel ist NON_COMPLIANT, wenn ein Trail nicht aktiviert ist. Optional überprüft die Regel einen bestimmten S3-Bucket, ein Amazon Simple Notification Service (Amazon SNS) -Thema und eine CloudWatch Protokollgruppe.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.3.1	Auditprotokolle sind vor Zerstörun g und unbefugte n Änderungen geschützt. (PCI-DSS-v4.0)	multi-region-cloudtrail-enabled	Hinweis: Bei dieser Regel untersche iden sich die Regel-ID (MULTI_RE GION_CLOU D_TRAIL_ENABLED) und der Regelname (). multi-region-cloudtrail-enabled Stellen Sie sicher, dass mindesten s eine Region mit mehreren Regionen vorhanden ist. AWS CloudTrail Die Regel ist NON_COMPL IANT, wenn die Trails nicht mit den Eingabeparametern übereinstimmen. Die Regel lautet NON_COMPLIANT, wenn das ExcludeMa nagementEventSourc es Feld nicht leer ist oder wenn sie so konfiguriert AWS CloudTrail ist, dass Verwaltungsereigni sse wie AWS KMS-Ereignisse oder Amazon RDS-Daten -API-Ereignisse

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			ausgeschlossen werden.
10.3.1	Auditprotokolle sind vor Zerstörung und unbefugten Änderungen geschützt. (PCI-DSS-v4.0)	appsync-logging-enabled	Stellen Sie sicher, dass für eine API die Protokollierung aktiviert ist. AWS AppSync Die Regel lautet NON_COMPLIANT, wenn die Protokollierung nicht aktiviert ist, oder 'fieldLogLevel' ist weder ERROR noch ALL.
10.3.1	Auditprotokolle sind vor Zerstörung und unbefugten Änderungen geschützt. (PCI-DSS-v4.0)	waf-classic-logging-enabled	Stellen Sie sicher, dass die Protokollierung auf den AWS WAF Classic Global Web Access Control Lists (Web) aktiviert ist. ACLs Die Regel ist NON_COMPLIANT für eine globale Web-ACL, wenn die Protokollierung nicht aktiviert ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.3.1	Auditprotokolle sind vor Zerstörung und unbefugten Änderungen geschützt. (PCI-DSS-v4.0)	mq-cloudwatch-audit-logging-aktiviert	Stellen Sie sicher, dass Amazon MQ-Broker die CloudWatch Amazon-Auditprotokollierung aktiviert haben. Die Regel ist NON_COMPLIANT, wenn für einen Broker die Audit-Protokollierung nicht aktiviert ist.
10.3.1	Auditprotokolle sind vor Zerstörung und unbefugten Änderungen geschützt. (PCI-DSS-v4.0)	mq-cloudwatch-audit-log-aktiviert	Stellen Sie sicher, dass bei einem Amazon MQ-Broker die CloudWatch Auditprotokollierung aktiviert ist. Die Regel lautet NON_COMPLIANT, wenn für den Broker die Audit-Protokollierung nicht aktiviert ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.3.1	Auditprotokolle sind vor Zerstörun g und unbefugte n Änderungen geschützt. (PCI-DSS-v4.0)	eks-cluster-logging-enabled	Stellen Sie sicher, dass ein Amazon Elastic Kubernete s Service (Amazon EKS) -Cluster mit aktivierter Protokoll ierung konfiguriert ist. Die Regel ist NON_COMPLIANT, wenn die Protokoll ierung für Amazon-EKS-Cluster nicht für alle Protokolltypen aktiviert ist.
10.3.1	Auditprotokolle sind vor Zerstörun g und unbefugte n Änderungen geschützt. (PCI-DSS-v4.0)	elastic-beanstalk-logs-to-Wolkenbeob achtung	Stellen Sie sicher, dass AWS Elastic Beanstalk Beanstalk -Umgebungen so konfiguriert sind, dass sie Protokolle an Amazon CloudWatc h Logs senden. Die Regel lautet NON_COMPLIANT, wenn der Wert von `` StreamLogs falsch ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.3.1	Auditprotokolle sind vor Zerstörung und unbefugten Änderungen geschützt. (PCI-DSS-v4.0)	step-functions-state-machine-Protokollierung aktiviert	Stellen Sie sicher, dass auf der AWS Step Functions Functions-Maschine die Protokollierung aktiviert ist Die Regel ist NON_COMPLIANT, wenn für eine Zustandsmaschine die Protokollierung nicht aktiviert ist oder die Protokollierungskonfiguration nicht auf dem angegebenen Mindestniveau liegt.
10.3.1	Auditprotokolle sind vor Zerstörung und unbefugten Änderungen geschützt. (PCI-DSS-v4.0)	netfw-logging-enabled	Stellen Sie sicher, dass die AWS Netzwerk-Firewall-Firewalls die Protokollierung aktiviert haben. Die Regel ist NON_COMPLIANT, wenn kein Protokollierungstyp konfiguriert ist. Sie können angeben, welchen Protokollierungstyp die Regel prüfen soll.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.3.2	Auditprotokolle sind vor Zerstörung und unbefugten Änderungen geschützt. (PCI-DSS-v4.0)	cloudtrail-security-trail-enabled	Stellen Sie sicher, dass mindestens ein AWS CloudTrail Pfad mit bewährten Sicherheitsmethoden definiert ist. Diese Regel ist COMPLIANT, wenn es mindestens einen Trail gibt, der alle der folgenden Bedingungen erfüllt:
10.3.2	Auditprotokolle sind vor Zerstörung und unbefugten Änderungen geschützt. (PCI-DSS-v4.0)	neptune-cluster-snapshot-public-verboten	Stellen Sie sicher, dass ein manueller Amazon Neptune Neptune-DB-Cluster-Snapshot nicht öffentlich ist. Die Regel ist NON_COMPLIANT, wenn es vorhandene und neue Neptune-Cluster-Snapshots gibt, die öffentlich zugänglich sind.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.3.2	Auditprotokolle sind vor Zerstörung und unbefugten Änderungen geschützt. (PCI-DSS-v4.0)	docdb-cluster-snapshot-public-verboten	Stellen Sie sicher, dass manuelle Cluster-Snapshots von Amazon DocumentDB nicht öffentlich sind. Die Regel ist NON_COMPLIANT, wenn manuelle Cluster-Snapshots von Amazon DocumentDB öffentlich sind.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.3.2	Auditprotokolle sind vor Zerstörung und unbefugten Änderungen geschützt. (PCI-DSS-v4.0)	backup-recovery-point-manual-Löschen-deaktiviert	Stellen Sie sicher, dass einem Backup-Tresor eine ressourcenbasierte Richtlinie zugeordnet ist, die das Löschen von Wiederherstellungspunkten verhindert. Die Regel lautet NON_COMPLIANT, wenn der Backup-Tresor keine ressourcenbasierten Richtlinien oder Richtlinien ohne eine geeignete „Deny“ -Anweisung (Anweisung mit den Berechtigungen backup:DeleteRecoveryPoint, backup: und backup:UpdateRecoveryPointLifecycle) hat. PutBackupVaultAccessPolicy

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.3.2	Auditprotokolle sind vor Zerstörung und unbefugten Änderungen geschützt. (PCI-DSS-v4.0)	emr-block-public-access	Stellen Sie sicher, dass für ein Konto bei Amazon EMR die Einstellungen zum Sperren des öffentlichen Zugriffs aktiviert sind. Die Regel ist NON_COMPLIANT, wenn sie falsch BlockPublicSecurityGroupRules ist, oder wenn sie wahr ist, sind andere Ports als Port 22 unter aufgeführt. Permitted PublicSecurityGroupRuleRanges
10.3.2	Auditprotokolle sind vor Zerstörung und unbefugten Änderungen geschützt. (PCI-DSS-v4.0)	access-point-public-accesss3-Blöcke	Stellen Sie sicher, dass Amazon S3 S3-Zugriffspunkten die Einstellungen zum Blockieren des öffentlichen Zugriffs aktiviert sind. Die Regel ist NON_COMPLIANT, wenn die Einstellung zum Blockieren des öffentlichen Zugriffs für S3-Zugangspunkte nicht aktiviert ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.3.2	Auditprotokolle sind vor Zerstörun g und unbefugte n Änderungen geschützt. (PCI-DSS-v4.0)	account-level-public-accesss3-Blöcke	Stellen Sie sicher, dass die erforderl ichen Einstellungen für die Sperrung des öffentlichen Zugriffs auf Kontoebene konfiguriert sind. Die Regel ist nur NON_COMPL IANT, wenn die unten festgeleg ten Felder nicht mit den entsprech enden Feldern im Konfigurationselement übereinstimmen.
10.3.2	Auditprotokolle sind vor Zerstörun g und unbefugte n Änderungen geschützt. (PCI-DSS-v4.0)	s-3 bucket-mfa-delete-enabled	Stellen Sie sicher, dass MFA Delete in der Bucket-Ve rsionierungskonfig uration von Amazon Simple Storage Service (Amazon S3) aktiviert ist. Die Regel ist NON_COMPL IANT, wenn MFA Delete nicht aktiviert ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.3.3	Auditprotokolle sind vor Zerstörung und unbefugten Änderungen geschützt. (PCI-DSS-v4.0)	aurora-resources-protected-by-Backup-Plan	Stellen Sie sicher, dass Amazon Aurora Aurora-DB-Cluster durch einen Backup-Plan geschützt sind. Die Regel ist NON_COMPLIANT, wenn der Datenbank-Cluster von Amazon Relational Database Service (Amazon RDS) nicht durch einen Backup-Plan geschützt ist.
10.3.3	Auditprotokolle sind vor Zerstörung und unbefugten Änderungen geschützt. (PCI-DSS-v4.0)	db-instance-backup-enabled	Stellen Sie sicher, dass für RDS-DB-Instances Backups aktiviert sind. Optional wird von der Regel auch der Aufbewahrungszeitraum für Backups und das Sicherungsfenster überprüft.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.3.3	Auditprotokolle sind vor Zerstörun g und unbefugte n Änderungen geschützt. (PCI-DSS-v4.0)	dynamodb-in-backup-plan	Stellen Sie sicher, dass Amazon DynamoDB-Tabellen in den AWS Backup-Plänen vorhanden sind. Die Regel lautet NON_COMPL IANT, wenn Amazon DynamoDB-Tabellen in keinem Backup-Plan enthalten sind. AWS
10.3.3	Auditprotokolle sind vor Zerstörun g und unbefugte n Änderungen geschützt. (PCI-DSS-v4.0)	dynamodb-resources-protected-by-Backup-Plan	Stellen Sie sicher, dass Amazon DynamoDB-Tabellen durch einen Backup-Plan geschützt sind. Die Regel ist NON_COMPLIANT, wenn die DynamoDB-Tabelle nicht durch einen Backup-Plan gedeckt ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.3.3	Auditprotokolle sind vor Zerstörun g und unbefugte n Änderungen geschützt. (PCI-DSS-v4.0)	ebs-in-backup-plan	Stellen Sie sicher, dass Amazon Elastic Block Store (Amazon EBS) -Volumes zu den Backup-Plänen von AWS Backup hinzugefügt werden. Die Regel ist NON_COMPLIANT, wenn Amazon-EB S-Volumes nicht in den Backup-Plänen enthalten sind.
10.3.3	Auditprotokolle sind vor Zerstörun g und unbefugte n Änderungen geschützt. (PCI-DSS-v4.0)	ebs-resources-prot ected-by-Backup-Plan	Stellen Sie sicher, dass Amazon Elastic Block Store (Amazon EBS) -Volumes durch einen Backup-Plan geschützt sind. Die Regel ist NON_COMPLIANT, wenn das Amazon-EB S-Volume nicht durch einen Backup-Plan gedeckt ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.3.3	Auditprotokolle sind vor Zerstörun g und unbefugte n Änderungen geschützt. (PCI-DSS-v4.0)	ec2--Plan resources-protected-by-backup	Stellen Sie sicher, dass Amazon Elastic Compute Cloud (Amazon EC2) - Instances durch einen Backup-Pl an geschützt sind. Die Regel lautet NON_COMPL IANT, wenn die EC2 Amazon-In stance nicht durch einen Backup-Plan abgedeckt ist.
10.3.3	Auditprotokolle sind vor Zerstörun g und unbefugte n Änderungen geschützt. (PCI-DSS-v4.0)	efs-in-backup-plan	Stellen Sie sicher, dass die Dateisyst eme von Amazon Elastic File System (Amazon EFS) zu den Backup-Plänen von AWS Backup hinzugefügt werden. Die Regel ist NON_COMPL IANT, wenn EFS-Dateisysteme nicht in den Backup-Plänen enthalten sind.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.3.3	Auditprotokolle sind vor Zerstörung und unbefugten Änderungen geschützt. (PCI-DSS-v4.0)	efs-resources-protected-by-Backup-Plan	Stellen Sie sicher, dass die Dateisysteme von Amazon Elastic File System (Amazon EFS) durch einen Backup-Plan geschützt sind. Die Regel ist NON_COMPLIANT, wenn das EFS-Dateisystem nicht durch einen Backup-Plan gedeckt ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.3.3	Auditprotokolle sind vor Zerstörung und unbefugten Änderungen geschützt. (PCI-DSS-v4.0)	elasticache-redis-cluster-automatic-Backup-Check	Prüfen Sie, ob die Amazon ElastiCache Redis-Cluster die automatische Sicherung aktiviert haben. Die Regel lautet NON_COMPLIANT, wenn der SnapshotRetentionLimit For-Redis-Cluster kleiner als der Parameter ist. SnapshotRetentionPeriod Beispiel: Wenn der Parameter 15 ist, ist die Regel nicht konform, wenn der snapshotRetentionPeriod zwischen 0 und 15 liegt.
10.3.3	Auditprotokolle sind vor Zerstörung und unbefugten Änderungen geschützt. (PCI-DSS-v4.0)	fsx-resources-protected-by-Backup-Plan	Stellen Sie sicher, dass Amazon FSx File Systems durch einen Backup-Plan geschützt sind. Die Regel lautet NON_COMPLIANT, wenn das FSx Amazon-Dateisystem nicht durch einen Backup-Plan abgedeckt ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.3.3	Auditprotokolle sind vor Zerstörung und unbefugten Änderungen geschützt. (PCI-DSS-v4.0)	neptune-cluster-backup-retention-überprüfen	Stellen Sie sicher, dass die Aufbewahrungsfrist für Amazon Neptune DB-Cluster auf eine bestimmte Anzahl von Tagen festgelegt ist. Die Regel ist NON_COMPLIANT, wenn der Aufbewahrungszeitraum kürzer ist als durch den Parameter angegeben.
10.3.3	Auditprotokolle sind vor Zerstörung und unbefugten Änderungen geschützt. (PCI-DSS-v4.0)	rds-in-backup-plan	Stellen Sie sicher, dass Amazon Relational Database Service (Amazon RDS) -Datenbanken in den AWS Backup-Plänen enthalten sind. Die Regel lautet NON_COMPLIANT, wenn Amazon RDS-Datenbanken in keinem AWS Backup-Plan enthalten sind.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.3.3	Auditprotokolle sind vor Zerstörung und unbefugten Änderungen geschützt. (PCI-DSS-v4.0)	rds-resources-protected-by-Backup-Plan	Stellen Sie sicher, dass Amazon Relational Database Service (Amazon RDS) -Instances durch einen Backup-Plan geschützt sind. Die Regel ist NON_COMPLIANT, wenn die Instance der Amazon-RDS-Datenbank nicht durch einen Backup-Plan gedeckt ist.
10.3.3	Auditprotokolle sind vor Zerstörung und unbefugten Änderungen geschützt. (PCI-DSS-v4.0)	redshift-backup-enabled	Stellen Sie sicher, dass automatisierte Amazon Redshift Redshift-Snapshots für Cluster aktiviert sind. Die Regel lautet NON_COMPLIANT, wenn der Wert für automatedSnapshotRetention Period größer MaxRetentionPeriod oder kleiner MinRetentionPeriod oder der Wert 0 ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.3.3	Auditprotokolle sind vor Zerstörung und unbefugten Änderungen geschützt. (PCI-DSS-v4.0)	s-3-Plan resources-protected-by-backup	Stellen Sie sicher, dass Amazon Simple Storage Service (Amazon S3) -Buckets durch einen Backup-Plan geschützt sind. Die Regel ist NON_COMPLIANT, wenn der Amazon-S3 -Bucket nicht durch einen Backup-Plan gedeckt ist.
10.3.3	Auditprotokolle sind vor Zerstörung und unbefugten Änderungen geschützt. (PCI-DSS-v4.0)	cloudtrail-security-trail-enabled	Stellen Sie sicher, dass mindestens ein AWS CloudTrail Pfad mit bewährten Sicherheitsmethoden definiert ist. Diese Regel ist COMPLIANT, wenn es mindestens einen Trail gibt, der alle der folgenden Bedingungen erfüllt:

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.3.3	Auditprotokolle sind vor Zerstörung und unbefugten Änderungen geschützt. (PCI-DSS-v4.0)	db-instance-backup-enabled	Stellen Sie sicher, dass für RDS-DB-Instances Backups aktiviert sind. Optional wird von der Regel auch der Aufbewahrungszeitraum für Backups und das Sicherungsfenster überprüft.
10.3.3	Auditprotokolle sind vor Zerstörung und unbefugten Änderungen geschützt. (PCI-DSS-v4.0)	dynamodb-pitr-enabled	Stellen Sie sicher, dass point-in-time Recovery (PITR) für Amazon DynamoDB-Tabellen aktiviert ist. Die Regel ist NON_COMPLIANT, wenn PITR für DynamoDB-Tabellen nicht aktiviert ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.3.4	Auditprotokolle sind vor Zerstörung und unbefugten Änderungen geschützt. (PCI-DSS-v4.0)	cloudfront-origin-access-identity-aktiviert	Stellen Sie sicher, dass für die CloudFront Verteilung mit dem Amazon S3 S3-Origin-Typ die Origin Access Identity (OAI) konfiguriert ist. Die Regel lautet NON_COMPLIANT, wenn die CloudFront Verteilung von S3 unterstützt wird und ein Quelltyp nicht OAI-konfiguriert ist oder der Ursprung kein S3-Bucket ist.
10.3.4	Auditprotokolle sind vor Zerstörung und unbefugten Änderungen geschützt. (PCI-DSS-v4.0)	Wolkenfront - 3 origin-access-control-enabled	Stellen Sie sicher, dass bei einer CloudFront Amazon-Distribution mit einem Amazon Simple Storage Service (Amazon S3) Origin Access Control (OAC) aktiviert ist. Die Regel lautet NON_COMPLIANT für CloudFront Distributionen mit Amazon S3 S3-Ursprung, für die OAC nicht aktiviert ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.3.4	Auditprotokolle sind vor Zerstörung und unbefugten Änderungen geschützt. (PCI-DSS-v4.0)	s-3 bucket-default-lock-enabled	Stellen Sie sicher, dass für den S3-Bucket die Sperre standardmäßig aktiviert ist. Die Regel ist NON_COMPLIANT, wenn die Sperre nicht aktiviert ist.
10.3.4	Auditprotokolle sind vor Zerstörung und unbefugten Änderungen geschützt. (PCI-DSS-v4.0)	s-3 bucket-versioning-enabled	Stellen Sie sicher, dass die Versionierung für Ihre S3-Buckets aktiviert ist. Optional wird von der Regel überprüft, ob die MFA-Löschung für Ihre S3-Buckets aktiviert ist.
10.3.4	Auditprotokolle sind vor Zerstörung und unbefugten Änderungen geschützt. (PCI-DSS-v4.0)	cloudtrail-security-trail-enabled	Stellen Sie sicher, dass mindestens ein AWS CloudTrail Pfad mit bewährten Sicherheitsmethoden definiert ist. Diese Regel ist COMPLIANT, wenn es mindestens einen Trail gibt, der alle der folgenden Bedingungen erfüllt:

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.4.1	Auditprotokolle werden überprüft, um Anomalien oder verdächtige Aktivitäten zu identifizieren. (PCI-DSS-v4.0)	api-gw-xray-enabled	Stellen Sie sicher, dass AWS X-Ray Tracing auf Amazon API Gateway REST APIs aktiviert ist. Die Regel ist COMPLIANT, wenn die X-Ray-Abl aufverfolgung aktiviert ist, andernfalls ist sie NON_COMPLIANT.
10.4.1	Auditprotokolle werden überprüft, um Anomalien oder verdächtige Aktivitäten zu identifizieren. (PCI-DSS-v4.0)	ec2- instance-detailed-monitoring-enabled	Stellen Sie sicher, dass die detaillierte Überwachung für Instanzen aktiviert ist. EC2 Die Regel ist NON_COMPLIANT, wenn keine detaillierte Überwachung aktiviert ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.4.1	Auditprotokolle werden überprüft, um Anomalien oder verdächtige Aktivitäten zu identifizieren. (PCI-DSS-v4.0)	cloudwatch-alarm-action-check	Stellen Sie sicher, dass bei CloudWatch Alarmen eine Aktion für den Status ALARM, INSUFFICIENT_DATA oder OK konfiguriert ist. Stellen Sie optional sicher, dass alle Aktionen mit einem benannten ARN übereinstimmen. Die Regel ist NON_COMPLIANT, wenn für den Alarm oder den optionalen Parameter keine Aktion festgelegt ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.4.1	Auditprotokolle werden überprüft, um Anomalien oder verdächtige Aktivitäten zu identifizieren. (PCI-DSS-v4.0)	cloudwatch-alarm-action-check	Stellen Sie sicher, dass bei CloudWatch Alarmen eine Aktion für den Status ALARM, INSUFFICIENT_DATA oder OK konfiguriert ist. Stellen Sie optional sicher, dass alle Aktionen mit einem benannten ARN übereinstimmen. Die Regel ist NON_COMPLIANT, wenn für den Alarm oder den optionalen Parameter keine Aktion festgelegt ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.4.1	Auditprotokolle werden überprüft, um Anomalien oder verdächtige Aktivitäten zu identifizieren. (PCI-DSS-v4.0)	cloudwatch-alarm-action-check	Stellen Sie sicher, dass bei CloudWatch Alarmen eine Aktion für den Status ALARM, INSUFFICIENT_DATA oder OK konfiguriert ist. Stellen Sie optional sicher, dass alle Aktionen mit einem benannten ARN übereinstimmen. Die Regel ist NON_COMPLIANT, wenn für den Alarm oder den optionalen Parameter keine Aktion festgelegt ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.4.1	Auditprotokolle werden überprüft, um Anomalien oder verdächtige Aktivitäten zu identifizieren. (PCI-DSS-v4.0)	cloudwatch-alarm-resource-check	Stellen Sie sicher, dass ein Ressourcentyp einen CloudWatch Alarm für die angegebene Metrik hat. Als Ressourcentyp können Sie EBS-Volumes, EC2 Instances, Amazon RDS-Cluster oder S3-Buckets angeben. Die Regel ist KONFORM, wenn die benannte Metrik eine Ressourcen-ID und CloudWatch einen Alarm hat.
10.4.1	Auditprotokolle werden überprüft, um Anomalien oder verdächtige Aktivitäten zu identifizieren. (PCI-DSS-v4.0)	WAF 2- rulegroup-logging-enabled	Stellen Sie sicher, dass die Erfassung von CloudWatch Amazon-Sicherheitsmetriken für AWS WAFv2 Regelgruppen aktiviert ist. Die Regel ist NON_COMPLIANT, wenn '. VisibilityConfig CloudWatchMetricsEnabledDas Feld 'ist auf falsch gesetzt.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.4.1	Auditprotokolle werden überprüft, um Anomalien oder verdächtige Aktivitäten zu identifizieren. (PCI-DSS-v4.0)	sns-topic-message-delivery-Benachrichtigung aktiviert	Stellen Sie sicher, dass die Amazon Simple Notification Service (SNS) - Protokollierung für den Zustellungsstatus von Benachrichtigungen aktiviert ist, die an ein Thema für die Endgeräte gesendet werden. Die Regel ist NON_COMPLIANT, wenn die Benachrichtigung über den Status der Zustellung von Nachrichten nicht aktiviert ist.
10.4.1.1	Auditprotokolle werden überprüft, um Anomalien oder verdächtige Aktivitäten zu identifizieren. (PCI-DSS-v4.0)	api-gw-xray-enabled	Stellen Sie sicher, dass AWS X-Ray Tracing auf Amazon API Gateway REST APIs aktiviert ist. Die Regel ist COMPLIANT, wenn die X-Ray-Ablaufverfolgung aktiviert ist, andernfalls ist sie NON_COMPLIANT.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.4.1.1	Auditprotokolle werden überprüft, um Anomalien oder verdächtige Aktivitäten zu identifizieren. (PCI-DSS-v4.0)	ec2- instance-detailed-monitoring-enabled	Stellen Sie sicher, dass die detaillierte Überwachung für Instanzen aktiviert ist. EC2 Die Regel ist NON_COMPLIANT, wenn keine detaillierte Überwachung aktiviert ist.
10.4.1.1	Auditprotokolle werden überprüft, um Anomalien oder verdächtige Aktivitäten zu identifizieren. (PCI-DSS-v4.0)	cloudwatch-alarm-action-check	Stellen Sie sicher, dass bei CloudWatch Alarmen eine Aktion für den Status ALARM, INSUFFICIENT_DATA oder OK konfiguriert ist. Stellen Sie optional sicher, dass alle Aktionen mit einem benannten ARN übereinstimmen. Die Regel ist NON_COMPLIANT, wenn für den Alarm oder den optionalen Parameter keine Aktion festgelegt ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.4.1.1	Auditprotokolle werden überprüft, um Anomalien oder verdächtige Aktivitäten zu identifizieren. (PCI-DSS-v4.0)	cloudwatch-alarm-action-check	Stellen Sie sicher, dass bei CloudWatch Alarmen eine Aktion für den Status ALARM, INSUFFICIENT_DATA oder OK konfiguriert ist. Stellen Sie optional sicher, dass alle Aktionen mit einem benannten ARN übereinstimmen. Die Regel ist NON_COMPLIANT, wenn für den Alarm oder den optionalen Parameter keine Aktion festgelegt ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.4.1.1	Auditprotokolle werden überprüft, um Anomalien oder verdächtige Aktivitäten zu identifizieren. (PCI-DSS-v4.0)	cloudwatch-alarm-action-check	Stellen Sie sicher, dass bei CloudWatch Alarmen eine Aktion für den Status ALARM, INSUFFICIENT_DATA oder OK konfiguriert ist. Stellen Sie optional sicher, dass alle Aktionen mit einem benannten ARN übereinstimmen. Die Regel ist NON_COMPLIANT, wenn für den Alarm oder den optionalen Parameter keine Aktion festgelegt ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.4.1.1	Auditprotokolle werden überprüft, um Anomalien oder verdächtige Aktivitäten zu identifizieren. (PCI-DSS-v4.0)	cloudwatch-alarm-resource-check	Stellen Sie sicher, dass ein Ressourcentyp einen CloudWatch Alarm für die angegebene Metrik hat. Als Ressourcentyp können Sie EBS-Volumes, EC2 Instances, Amazon RDS-Cluster oder S3-Buckets angeben. Die Regel ist KONFORM, wenn die benannte Metrik eine Ressourcen-ID und CloudWatch einen Alarm hat.
10.4.1.1	Auditprotokolle werden überprüft, um Anomalien oder verdächtige Aktivitäten zu identifizieren. (PCI-DSS-v4.0)	WAF 2- rulegroup-logging-enabled	Stellen Sie sicher, dass die Erfassung von CloudWatch Amazon-Sicherheitsmetriken für AWS WAFv2 Regelgruppen aktiviert ist. Die Regel ist NON_COMPLIANT, wenn '. VisibilityConfig CloudWatchMetricsEnabledDas Feld 'ist auf falsch gesetzt.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.4.1.1	Auditprotokolle werden überprüft, um Anomalien oder verdächtige Aktivitäten zu identifizieren. (PCI-DSS-v4.0)	sns-topic-message-delivery-Benachrichtigung aktiviert	Stellen Sie sicher, dass die Amazon Simple Notification Service (SNS) - Protokollierung für den Zustellungsstatus von Benachrichtigungen aktiviert ist, die an ein Thema für die Endgeräte gesendet werden. Die Regel ist NON_COMPLIANT, wenn die Benachrichtigung über den Status der Zustellung von Nachrichten nicht aktiviert ist.
10.4.2	Auditprotokolle werden überprüft, um Anomalien oder verdächtige Aktivitäten zu identifizieren. (PCI-DSS-v4.0)	api-gw-xray-enabled	Stellen Sie sicher, dass AWS X-Ray Tracing auf Amazon API Gateway REST APIs aktiviert ist. Die Regel ist COMPLIANT, wenn die X-Ray-Ablaufverfolgung aktiviert ist, andernfalls ist sie NON_COMPLIANT.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.4.2	Auditprotokolle werden überprüft, um Anomalien oder verdächtige Aktivitäten zu identifizieren. (PCI-DSS-v4.0)	ec2- instance-detailed-monitoring-enabled	Stellen Sie sicher, dass die detaillierte Überwachung für Instanzen aktiviert ist. EC2 Die Regel ist NON_COMPLIANT, wenn keine detaillierte Überwachung aktiviert ist.
10.4.2	Auditprotokolle werden überprüft, um Anomalien oder verdächtige Aktivitäten zu identifizieren. (PCI-DSS-v4.0)	cloudwatch-alarm-action-check	Stellen Sie sicher, dass bei CloudWatch Alarmen eine Aktion für den Status ALARM, INSUFFICIENT_DATA oder OK konfiguriert ist. Stellen Sie optional sicher, dass alle Aktionen mit einem benannten ARN übereinstimmen. Die Regel ist NON_COMPLIANT, wenn für den Alarm oder den optionalen Parameter keine Aktion festgelegt ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.4.2	Auditprotokolle werden überprüft, um Anomalien oder verdächtige Aktivitäten zu identifizieren. (PCI-DSS-v4.0)	cloudwatch-alarm-action-check	Stellen Sie sicher, dass bei CloudWatch Alarmen eine Aktion für den Status ALARM, INSUFFICIENT_DATA oder OK konfiguriert ist. Stellen Sie optional sicher, dass alle Aktionen mit einem benannten ARN übereinstimmen. Die Regel ist NON_COMPLIANT, wenn für den Alarm oder den optionalen Parameter keine Aktion festgelegt ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.4.2	Auditprotokolle werden überprüft, um Anomalien oder verdächtige Aktivitäten zu identifizieren. (PCI-DSS-v4.0)	cloudwatch-alarm-action-check	Stellen Sie sicher, dass bei CloudWatch Alarmen eine Aktion für den Status ALARM, INSUFFICIENT_DATA oder OK konfiguriert ist. Stellen Sie optional sicher, dass alle Aktionen mit einem benannten ARN übereinstimmen. Die Regel ist NON_COMPLIANT, wenn für den Alarm oder den optionalen Parameter keine Aktion festgelegt ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.4.2	Auditprotokolle werden überprüft, um Anomalien oder verdächtige Aktivitäten zu identifizieren. (PCI-DSS-v4.0)	cloudwatch-alarm-resource-check	Stellen Sie sicher, dass ein Ressourcentyp einen CloudWatch Alarm für die angegebene Metrik hat. Als Ressourcentyp können Sie EBS-Volumes, EC2 Instances, Amazon RDS-Cluster oder S3-Buckets angeben. Die Regel ist KONFORM, wenn die benannte Metrik eine Ressourcen-ID und CloudWatch einen Alarm hat.
10.4.2	Auditprotokolle werden überprüft, um Anomalien oder verdächtige Aktivitäten zu identifizieren. (PCI-DSS-v4.0)	WAF 2- rulegroup-logging-enabled	Stellen Sie sicher, dass die Erfassung von CloudWatch Amazon-Sicherheitsmetriken für AWS WAFv2 Regelgruppen aktiviert ist. Die Regel ist NON_COMPLIANT, wenn '. VisibilityConfig CloudWatchMetricsEnabledDas Feld 'ist auf falsch gesetzt.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.4.2	Auditprotokolle werden überprüft, um Anomalien oder verdächtige Aktivitäten zu identifizieren. (PCI-DSS-v4.0)	sns-topic-message-delivery-Benachrichtigung aktiviert	Stellen Sie sicher, dass die Amazon Simple Notification Service (SNS) - Protokollierung für den Zustellungsstatus von Benachrichtigungen aktiviert ist, die an ein Thema für die Endgeräte gesendet werden. Die Regel ist NON_COMPLIANT, wenn die Benachrichtigung über den Status der Zustellung von Nachrichten nicht aktiviert ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.4.3	Auditprotokolle werden überprüft, um Anomalien oder verdächtige Aktivitäten zu identifizieren. (PCI-DSS-v4.0)	cloudwatch-alarm-action-check	Stellen Sie sicher, dass bei CloudWatch Alarmen eine Aktion für den Status ALARM, INSUFFICIENT_DATA oder OK konfiguriert ist. Stellen Sie optional sicher, dass alle Aktionen mit einem benannten ARN übereinstimmen. Die Regel ist NON_COMPLIANT, wenn für den Alarm oder den optionalen Parameter keine Aktion festgelegt ist.
10.5.1	Der Verlauf des Auditprotokolls wird beibehalten und steht zur Analyse zur Verfügung. (PCI-DSS-v4.0)	cloudtrail-security-trail-enabled	Stellen Sie sicher, dass mindestens ein AWS CloudTrail Pfad mit bewährten Sicherheitsmethoden definiert ist. Diese Regel ist COMPLIANT, wenn es mindestens einen Trail gibt, der alle der folgenden Bedingungen erfüllt:

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.5.1	Der Verlauf des Auditprotokolls wird beibehalten und steht zur Analyse zur Verfügung. (PCI-DSS-v4.0)	ec2- volume-inuse-check	Stellen Sie sicher, dass EBS-Volumes an Instances angehängt sind. EC2 Stellen Sie optional sicher, dass EBS-Volumes zum Löschen markiert sind, wenn eine Instance beendet wird.
10.5.1	Der Verlauf des Auditprotokolls wird beibehalten und steht zur Analyse zur Verfügung. (PCI-DSS-v4.0)	ecr-private-lifecycle-policy-konfiguriert	Stellen Sie sicher, dass für ein privates Amazon Elastic Container Registry (ECR) -Repository mindestens eine Lebenszyklusrichtlinie konfiguriert ist. Die Regel ist NON_COMPLIANT, wenn keine Lebenszyklus-Richtlinie für das private ECR-Repository konfiguriert ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.5.1	Der Verlauf des Auditprotokolls wird beibehalten und steht zur Analyse zur Verfügung. (PCI-DSS-v4.0)	dynamodb-pitr-enabled	Stellen Sie sicher, dass point-in-time Recovery (PITR) für Amazon DynamoDB-Tabellen aktiviert ist. Die Regel ist NON_COMPLIANT, wenn PITR für DynamoDB-Tabellen nicht aktiviert ist.
10.5.1	Der Verlauf des Auditprotokolls wird beibehalten und steht zur Analyse zur Verfügung. (PCI-DSS-v4.0)	cw-loggroup-retention-period-überprüfen	Stellen Sie sicher, dass ein CloudWatch LogGroup Amazon-Aufbewahrungszeitraum auf mehr als 365 Tage oder einen bestimmten Aufbewahrungszeitraum festgelegt ist. Die Regel lautet NON_COMPLIANT, wenn die Aufbewahrungsfrist weniger als MinRetentionTime, falls angegeben, oder andernfalls 365 Tage beträgt.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.6.3	Mechanismen zur Zeitsynchronisierung unterstützen konsistente Zeiteinstellungen auf allen Systemen. (PCI-DSS-v4.0)	api-gwv2- access-logs-enabled	Stellen Sie sicher, dass die Amazon API Gateway V2-Stufen die Zugriffsprotokollierung aktiviert haben. Die Regel ist NON_COMPLIANT, wenn 'accessLogSettings' in der Stage-Konfiguration nicht vorhanden ist.
10.6.3	Mechanismen zur Zeitsynchronisierung unterstützen konsistente Zeiteinstellungen auf allen Systemen. (PCI-DSS-v4.0)	api-gw-xray-enabled	Stellen Sie sicher, dass AWS X-Ray Tracing auf Amazon API Gateway REST APIs aktiviert ist. Die Regel ist COMPLIANT, wenn die X-Ray-Ablaufverfolgung aktiviert ist, andernfalls ist sie NON_COMPLIANT.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.6.3	Mechanismen zur Zeitsynchronisierung unterstützen konsistente Zeiteinstellungen auf allen Systemen. (PCI-DSS-v4.0)	cloudfront-accesslogs-enabled	Stellen Sie sicher, dass CloudFront Amazon-Distributionen so konfiguriert sind, dass sie Zugriffsprotokolle an einen Amazon S3-Bucket senden. Die Regel lautet NON_COMPLIANT, wenn für eine CloudFront Distribution keine Protokollierung konfiguriert ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.6.3	Mechanismen zur Zeitsynchronisierung unterstützen konsistente Zeiteinstellungen auf allen Systemen. (PCI-DSS-v4.0)	s-3 bucket-blacklisted-actions-prohibited	Stellen Sie sicher, dass eine Bucket-Richtlinie von Amazon Simple Storage Service (Amazon S3) keine Aktionen auf Bucket- und Objektebene auf Blocklisten für Ressourcen im Bucket für Prinzipale anderer Konten zulässt. AWS Die Regel überprüft beispielsweise, ob die Amazon S3 S3-Bucket-Richtlinie einem anderen AWS Konto nicht erlaubt, s3: GetBucket *-Aktionen und s3: DeleteObject für ein Objekt im Bucket auszuführen. Die Regel ist NON_COMPLIANT, wenn gesperrte Aktionen gemäß der Bucket-Richtlinie von Amazon S3 zulässig sind.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.6.3	Mechanismen zur Zeitsynchronisierung unterstützen konsistente Zeiteinstellungen auf allen Systemen. (PCI-DSS-v4.0)	bucket-policy-not-mores3-permissiv	Stellen Sie sicher, dass Ihre Amazon Simple Storage Service (S3) -Bucket-Richtlinien keine anderen Kontoberechtigungen zulassen als die von Ihnen Amazon S3 S3-Bucket-Kontrollrichtlinie.
10.6.3	Mechanismen zur Zeitsynchronisierung unterstützen konsistente Zeiteinstellungen auf allen Systemen. (PCI-DSS-v4.0)	neptune-cluster-cloudwatch-log-exportfähig	Stellen Sie sicher, dass in einem Amazon Neptune Neptune-Cluster der Protokollexport für CloudWatch Audit-Logs aktiviert ist. Die Regel lautet NON_COMPLIANT, wenn für einen Neptune-Cluster der Protokollexport für CloudWatch Audit-Logs nicht aktiviert ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.6.3	Mechanismen zur Zeitsynchronisierung unterstützen konsistente Zeiteinstellungen auf allen Systemen. (PCI-DSS-v4.0)	ec2- instance-detailed-monitoring-enabled	Stellen Sie sicher, dass die detaillierte Überwachung für Instanzen aktiviert ist. EC2 Die Regel ist NON_COMPLIANT, wenn keine detaillierte Überwachung aktiviert ist.
10.6.3	Mechanismen zur Zeitsynchronisierung unterstützen konsistente Zeiteinstellungen auf allen Systemen. (PCI-DSS-v4.0)	ecs-task-definition-log-Konfiguration	Stellen Sie sicher, dass LogConfiguration für aktive ECS-Aufgabendefinitionen festgelegt ist. Diese Regel ist NON_COMPLIANT, wenn für eine aktive ECSTask Definition die LogConfiguration-Ressource nicht definiert ist oder der Wert für LogConfiguration in mindestens einer Containerdefinition Null ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.6.3	Mechanismen zur Zeitsynchronisierung unterstützen konsistente Zeiteinstellungen auf allen Systemen. (PCI-DSS-v4.0)	cloudwatch-alarm-action-check	Stellen Sie sicher, dass bei CloudWatch Alarmen eine Aktion für den Status ALARM, INSUFFICIENT_DATA oder OK konfiguriert ist. Stellen Sie optional sicher, dass alle Aktionen mit einem benannten ARN übereinstimmen. Die Regel ist NON_COMPLIANT, wenn für den Alarm oder den optionalen Parameter keine Aktion festgelegt ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.6.3	Mechanismen zur Zeitsynchronisierung unterstützen konsistente Zeiteinstellungen auf allen Systemen. (PCI-DSS-v4.0)	cloudwatch-alarm-action-check	Stellen Sie sicher, dass bei CloudWatch Alarmen eine Aktion für den Status ALARM, INSUFFICIENT_DATA oder OK konfiguriert ist. Stellen Sie optional sicher, dass alle Aktionen mit einem benannten ARN übereinstimmen. Die Regel ist NON_COMPLIANT, wenn für den Alarm oder den optionalen Parameter keine Aktion festgelegt ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.6.3	Mechanismen zur Zeitsynchronisierung unterstützen konsistente Zeiteinstellungen auf allen Systemen. (PCI-DSS-v4.0)	cloudwatch-alarm-action-check	Stellen Sie sicher, dass bei CloudWatch Alarmen eine Aktion für den Status ALARM, INSUFFICIENT_DATA oder OK konfiguriert ist. Stellen Sie optional sicher, dass alle Aktionen mit einem benannten ARN übereinstimmen. Die Regel ist NON_COMPLIANT, wenn für den Alarm oder den optionalen Parameter keine Aktion festgelegt ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.6.3	Mechanismen zur Zeitsynchronisierung unterstützen konsistente Zeiteinstellungen auf allen Systemen. (PCI-DSS-v4.0)	cloudwatch-alarm-resource-check	Stellen Sie sicher, dass ein Ressourcentyp einen CloudWatch Alarm für die angegebene Metrik hat. Als Ressourcentyp können Sie EBS-Volumes, EC2 Instances, Amazon RDS-Cluster oder S3-Buckets angeben. Die Regel ist KONFORM, wenn die benannte Metrik eine Ressourcen-ID und CloudWatch einen Alarm hat.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.6.3	Mechanismen zur Zeitsynchronisierung unterstützen konsistente Zeiteinstellungen auf allen Systemen. (PCI-DSS-v4.0)	cloudtrail-enabled	Hinweis: Bei dieser Regel unterscheiden sich die Regel-ID (CLOUD_TRAIL_ENABLED) und der Regelname (cloudtrail-enabled). Stellen Sie sicher, dass in Ihrem Konto ein Trail aktiviert ist AWS CloudTrail . AWS Die Regel ist NON_COMPLIANT, wenn ein Trail nicht aktiviert ist. Optional überprüft die Regel einen bestimmten S3-Bucket, ein Amazon Simple Notification Service (Amazon SNS) -Thema und eine CloudWatch Protokollgruppe.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.6.3	Mechanismen zur Zeitsynchronisierung unterstützen konsistente Zeiteinstellungen auf allen Systemen. (PCI-DSS-v4.0)	multi-region-cloudtrail-enabled	Hinweis: Bei dieser Regel unterscheiden sich die Regel-ID (MULTI_REGION_CLOUD_TRAIL_ENABLED) und der Regelname (). multi-region-cloudtrail-enabled Stellen Sie sicher, dass mindestens eine Region mit mehreren Regionen vorhanden ist. AWS CloudTrail Die Regel ist NON_COMPLIANT, wenn die Trails nicht mit den Eingabeparametern übereinstimmen. Die Regel lautet NON_COMPLIANT, wenn das ExcludeManagementEventSources Feld nicht leer ist oder wenn sie so konfiguriert AWS CloudTrail ist, dass Verwaltungsereignisse wie AWS KMS-Ereignisse oder Amazon RDS-Daten-API-Ereignisse

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			ausgeschlossen werden.
10.6.3	Mechanismen zur Zeitsynchronisierung unterstützen konsistente Zeiteinstellungen auf allen Systemen. (PCI-DSS-v4.0)	appsync-logging-enabled	Stellen Sie sicher, dass für eine API die Protokollierung aktiviert ist. AWS AppSync Die Regel lautet NON_COMPLIANT, wenn die Protokollierung nicht aktiviert ist, oder 'fieldLogLevel' ist weder ERROR noch ALL.
10.6.3	Mechanismen zur Zeitsynchronisierung unterstützen konsistente Zeiteinstellungen auf allen Systemen. (PCI-DSS-v4.0)	waf-classic-logging-enabled	Stellen Sie sicher, dass die Protokollierung auf den AWS WAF Classic Global Web Access Control Lists (Web) aktiviert ist. ACLs Die Regel ist NON_COMPLIANT für eine globale Web-ACL, wenn die Protokollierung nicht aktiviert ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.6.3	Mechanismen zur Zeitsynchronisierung unterstützen konsistente Zeiteinstellungen auf allen Systemen. (PCI-DSS-v4.0)	mq-cloudwatch-audit-logging-aktiviert	Stellen Sie sicher, dass Amazon MQ-Broker die CloudWatch Amazon-Auditprotokollierung aktiviert haben. Die Regel ist NON_COMPLIANT, wenn für einen Broker die Audit-Protokollierung nicht aktiviert ist.
10.6.3	Mechanismen zur Zeitsynchronisierung unterstützen konsistente Zeiteinstellungen auf allen Systemen. (PCI-DSS-v4.0)	mq-cloudwatch-audit-log-aktiviert	Stellen Sie sicher, dass bei einem Amazon MQ-Broker die CloudWatch Auditprotokollierung aktiviert ist. Die Regel lautet NON_COMPLIANT, wenn für den Broker die Audit-Protokollierung nicht aktiviert ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.6.3	Mechanismen zur Zeitsynchronisierung unterstützen konsistente Zeiteinstellungen auf allen Systemen. (PCI-DSS-v4.0)	eks-cluster-logging-enabled	Stellen Sie sicher, dass ein Amazon Elastic Kubernetes Service (Amazon EKS) -Cluster mit aktivierter Protokollierung konfiguriert ist. Die Regel ist NON_COMPLIANT, wenn die Protokollierung für Amazon-EKS-Cluster nicht für alle Protokolltypen aktiviert ist.
10.6.3	Mechanismen zur Zeitsynchronisierung unterstützen konsistente Zeiteinstellungen auf allen Systemen. (PCI-DSS-v4.0)	elastic-beanstalk-logs-to-Wolkenbeobachtung	Stellen Sie sicher, dass AWS Elastic Beanstalk Beanstalk -Umgebungen so konfiguriert sind, dass sie Protokolle an Amazon CloudWatch Logs senden. Die Regel lautet NON_COMPLIANT, wenn der Wert von `` StreamLogs falsch ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.6.3	Mechanismen zur Zeitsynchronisierung unterstützen konsistente Zeiteinstellungen auf allen Systemen. (PCI-DSS-v4.0)	WAF 2- rulegroup-logging-enabled	Stellen Sie sicher, dass die Erfassung von CloudWatch Amazon-Sicherheitsmetriken für AWS WAFv2 Regelgruppen aktiviert ist. Die Regel ist NON_COMPLIANT, wenn '. VisibilityConfig CloudWatchMetricsEnabledDas Feld 'ist auf falsch gesetzt.
10.6.3	Mechanismen zur Zeitsynchronisierung unterstützen konsistente Zeiteinstellungen auf allen Systemen. (PCI-DSS-v4.0)	sns-topic-message-delivery-Benachrichtigung aktiviert	Stellen Sie sicher, dass die Amazon Simple Notification Service (SNS) - Protokollierung für den Zustellungsstatus von Benachrichtigungen aktiviert ist, die an ein Thema für die Endgeräte gesendet werden. Die Regel ist NON_COMPLIANT, wenn die Benachrichtigung über den Status der Zustellung von Nachrichten nicht aktiviert ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.6.3	Mechanismen zur Zeitsynchronisierung unterstützen konsistente Zeiteinstellungen auf allen Systemen. (PCI-DSS-v4.0)	step-functions-state-machine-Protokollierung aktiviert	Stellen Sie sicher, dass auf der AWS Step Functions Functions-Maschine die Protokollierung aktiviert ist Die Regel ist NON_COMPLIANT, wenn für eine Zustandsmaschine die Protokollierung nicht aktiviert ist oder die Protokollierungskonfiguration nicht auf dem angegebenen Mindestniveau liegt.
10.6.3	Mechanismen zur Zeitsynchronisierung unterstützen konsistente Zeiteinstellungen auf allen Systemen. (PCI-DSS-v4.0)	netfw-logging-enabled	Stellen Sie sicher, dass die AWS Netzwerk-Firewall-Firewalls die Protokollierung aktiviert haben. Die Regel ist NON_COMPLIANT, wenn kein Protokollierungstyp konfiguriert ist. Sie können angeben, welchen Protokollierungstyp die Regel prüfen soll.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.7.1	Ausfälle kritischer Sicherheitskontrollsysteme werden erkannt, gemeldet und umgehend behoben. (PCI-DSS-v4.0)	api-gw-xray-enabled	Stellen Sie sicher, dass AWS X-Ray Tracing auf Amazon API Gateway REST APIs aktiviert ist. Die Regel ist COMPLIANT, wenn die X-Ray-Abl aufverfolgung aktiviert ist, andernfalls ist sie NON_COMPLIANT.
10.7.1	Ausfälle kritischer Sicherheitskontrollsysteme werden erkannt, gemeldet und umgehend behoben. (PCI-DSS-v4.0)	cloudformation-stack-notification-check	Stellen Sie sicher, dass Ihre CloudFormation Stacks Ereignisbenachrichtigungen an ein Amazon SNS SNS-Thema senden. Stellen Sie optional sicher, dass die angegebenen Amazon SNS SNS-Themen verwendet werden. Die Regel lautet NON_COMPLIANT, wenn CloudFormation Stacks keine Benachrichtigungen senden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.7.1	Ausfälle kritischer Sicherheitskontrollsysteme werden erkannt, gemeldet und umgehend behoben. (PCI-DSS-v4.0)	ec2- instance-detailed-monitoring-enabled	Stellen Sie sicher, dass die detaillierte Überwachung für Instanzen aktiviert ist. EC2 Die Regel ist NON_COMPLIANT, wenn keine detaillierte Überwachung aktiviert ist.
10.7.1	Ausfälle kritischer Sicherheitskontrollsysteme werden erkannt, gemeldet und umgehend behoben. (PCI-DSS-v4.0)	cloudwatch-alarm-action-check	Stellen Sie sicher, dass bei CloudWatch Alarmen eine Aktion für den Status ALARM, INSUFFICIENT_DATA oder OK konfiguriert ist. Stellen Sie optional sicher, dass alle Aktionen mit einem benannten ARN übereinstimmen. Die Regel ist NON_COMPLIANT, wenn für den Alarm oder den optionalen Parameter keine Aktion festgelegt ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.7.1	Ausfälle kritischer Sicherheitskontrollsysteme werden erkannt, gemeldet und umgehend behoben. (PCI-DSS-v4.0)	cloudwatch-alarm-action-check	Stellen Sie sicher, dass bei CloudWatch Alarmen eine Aktion für den Status ALARM, INSUFFICIENT_DATA oder OK konfiguriert ist. Stellen Sie optional sicher, dass alle Aktionen mit einem benannten ARN übereinstimmen. Die Regel ist NON_COMPLIANT, wenn für den Alarm oder den optionalen Parameter keine Aktion festgelegt ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.7.1	Ausfälle kritischer Sicherheitskontrollsysteme werden erkannt, gemeldet und umgehend behoben. (PCI-DSS-v4.0)	cloudwatch-alarm-action-check	Stellen Sie sicher, dass bei CloudWatch Alarmen eine Aktion für den Status ALARM, INSUFFICIENT_DATA oder OK konfiguriert ist. Stellen Sie optional sicher, dass alle Aktionen mit einem benannten ARN übereinstimmen. Die Regel ist NON_COMPLIANT, wenn für den Alarm oder den optionalen Parameter keine Aktion festgelegt ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.7.1	Ausfälle kritischer Sicherheitskontrollsysteme werden erkannt, gemeldet und umgehend behoben. (PCI-DSS-v4.0)	cloudwatch-alarm-resource-check	Stellen Sie sicher, dass ein Ressourcentyp einen CloudWatch Alarm für die angegebene Metrik hat. Als Ressourcentyp können Sie EBS-Volumes, EC2 Instances, Amazon RDS-Cluster oder S3-Buckets angeben. Die Regel ist KONFORM, wenn die benannte Metrik eine Ressourcen-ID und CloudWatch einen Alarm hat.
10.7.1	Ausfälle kritischer Sicherheitskontrollsysteme werden erkannt, gemeldet und umgehend behoben. (PCI-DSS-v4.0)	WAF 2- rulegroup-logging-enabled	Stellen Sie sicher, dass die Erfassung von CloudWatch Amazon-Sicherheitsmetriken für AWS WAFv2 Regelgruppen aktiviert ist. Die Regel ist NON_COMPLIANT, wenn '. VisibilityConfig CloudWatchMetricsEnabledDas Feld 'ist auf falsch gesetzt.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.7.1	Ausfälle kritischer Sicherheitskontrollsysteme werden erkannt, gemeldet und umgehend behoben. (PCI-DSS-v4.0)	sns-topic-message-delivery-Benachrichtigung aktiviert	Stellen Sie sicher, dass die Amazon Simple Notification Service (SNS) - Protokollierung für den Zustellungsstatus von Benachrichtigungen aktiviert ist, die an ein Thema für die Endgeräte gesendet werden. Die Regel ist NON_COMPLIANT, wenn die Benachrichtigung über den Status der Zustellung von Nachrichten nicht aktiviert ist.
10.7.2	Ausfälle kritischer Sicherheitskontrollsysteme werden erkannt, gemeldet und umgehend behoben. (PCI-DSS-v4.0)	api-gw-xray-enabled	Stellen Sie sicher, dass AWS X-Ray Tracing auf Amazon API Gateway REST APIs aktiviert ist. Die Regel ist COMPLIANT, wenn die X-Ray-Ablaufverfolgung aktiviert ist, andernfalls ist sie NON_COMPLIANT.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.7.2	Ausfälle kritischer Sicherheitskontrollsysteme werden erkannt, gemeldet und umgehend behoben. (PCI-DSS-v4.0)	cloudformation-stack-notification-check	Stellen Sie sicher, dass Ihre CloudFormation Stacks Ereignisbenachrichtigungen an ein Amazon SNS SNS-Thema senden. Stellen Sie optional sicher, dass die angegebenen Amazon SNS SNS-Themen verwendet werden. Die Regel lautet NON_COMPLIANT, wenn CloudFormation Stacks keine Benachrichtigungen senden.
10.7.2	Ausfälle kritischer Sicherheitskontrollsysteme werden erkannt, gemeldet und umgehend behoben. (PCI-DSS-v4.0)	ec2- instance-detailed-monitoring-enabled	Stellen Sie sicher, dass die detaillierte Überwachung für Instanzen aktiviert ist. EC2 Die Regel ist NON_COMPLIANT, wenn keine detaillierte Überwachung aktiviert ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.7.2	Ausfälle kritischer Sicherheitskontrollsysteme werden erkannt, gemeldet und umgehend behoben. (PCI-DSS-v4.0)	cloudwatch-alarm-action-check	Stellen Sie sicher, dass bei CloudWatch Alarmen eine Aktion für den Status ALARM, INSUFFICIENT_DATA oder OK konfiguriert ist. Stellen Sie optional sicher, dass alle Aktionen mit einem benannten ARN übereinstimmen. Die Regel ist NON_COMPLIANT, wenn für den Alarm oder den optionalen Parameter keine Aktion festgelegt ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.7.2	Ausfälle kritischer Sicherheitskontrollsysteme werden erkannt, gemeldet und umgehend behoben. (PCI-DSS-v4.0)	cloudwatch-alarm-action-check	Stellen Sie sicher, dass bei CloudWatch Alarmen eine Aktion für den Status ALARM, INSUFFICIENT_DATA oder OK konfiguriert ist. Stellen Sie optional sicher, dass alle Aktionen mit einem benannten ARN übereinstimmen. Die Regel ist NON_COMPLIANT, wenn für den Alarm oder den optionalen Parameter keine Aktion festgelegt ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.7.2	Ausfälle kritischer Sicherheitskontrollsysteme werden erkannt, gemeldet und umgehend behoben. (PCI-DSS-v4.0)	cloudwatch-alarm-action-check	Stellen Sie sicher, dass bei CloudWatch Alarmen eine Aktion für den Status ALARM, INSUFFICIENT_DATA oder OK konfiguriert ist. Stellen Sie optional sicher, dass alle Aktionen mit einem benannten ARN übereinstimmen. Die Regel ist NON_COMPLIANT, wenn für den Alarm oder den optionalen Parameter keine Aktion festgelegt ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.7.2	Ausfälle kritischer Sicherheitskontrollsysteme werden erkannt, gemeldet und umgehend behoben. (PCI-DSS-v4.0)	cloudwatch-alarm-resource-check	Stellen Sie sicher, dass ein Ressourcentyp einen CloudWatch Alarm für die angegebene Metrik hat. Als Ressourcentyp können Sie EBS-Volumes, EC2 Instances, Amazon RDS-Cluster oder S3-Buckets angeben. Die Regel ist KONFORM, wenn die benannte Metrik eine Ressourcen-ID und CloudWatch einen Alarm hat.
10.7.2	Ausfälle kritischer Sicherheitskontrollsysteme werden erkannt, gemeldet und umgehend behoben. (PCI-DSS-v4.0)	WAF 2- rulegroup-logging-enabled	Stellen Sie sicher, dass die Erfassung von CloudWatch Amazon-Sicherheitsmetriken für AWS WAFv2 Regelgruppen aktiviert ist. Die Regel ist NON_COMPLIANT, wenn '. VisibilityConfig CloudWatchMetricsEnabledDas Feld 'ist auf falsch gesetzt.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
10.7.2	Ausfälle kritischer Sicherheitskontrollsysteme werden erkannt, gemeldet und umgehend behoben. (PCI-DSS-v4.0)	sns-topic-message-delivery-Benachrichtigung aktiviert	Stellen Sie sicher, dass die Amazon Simple Notification Service (SNS) - Protokollierung für den Zustellungsstatus von Benachrichtigungen aktiviert ist, die an ein Thema für die Endgeräte gesendet werden. Die Regel ist NON_COMPLIANT, wenn die Benachrichtigung über den Status der Zustellung von Nachrichten nicht aktiviert ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
11.5.2	Netzwerkeinbrüche und unerwartete Dateiänderungen werden erkannt und darauf reagiert. (PCI-DSS-v4.0)	cloudformation-stack-notification-check	Stellen Sie sicher, dass Ihre CloudFormation Stacks Ereignisbenachrichtigungen an ein Amazon SNS SNS-Thema senden. Stellen Sie optional sicher, dass die angegebenen Amazon SNS SNS-Themen verwendet werden. Die Regel lautet NON_COMPLIANT, wenn CloudFormation Stacks keine Benachrichtigungen senden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
11.5.2	Netzwerkeinbrüche und unerwartete Dateiänderungen werden erkannt und darauf reagiert. (PCI-DSS-v4.0)	cloudwatch-alarm-action-check	Stellen Sie sicher, dass bei CloudWatch Alarmen eine Aktion für den Status ALARM, INSUFFICIENT_DATA oder OK konfiguriert ist. Stellen Sie optional sicher, dass alle Aktionen mit einem benannten ARN übereinstimmen. Die Regel ist NON_COMPLIANT, wenn für den Alarm oder den optionalen Parameter keine Aktion festgelegt ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
11.5.2	Netzwerkeinbrüche und unerwartete Dateiänderungen werden erkannt und darauf reagiert. (PCI-DSS-v4.0)	cloudwatch-alarm-action-check	Stellen Sie sicher, dass bei CloudWatch Alarmen eine Aktion für den Status ALARM, INSUFFICIENT_DATA oder OK konfiguriert ist. Stellen Sie optional sicher, dass alle Aktionen mit einem benannten ARN übereinstimmen. Die Regel ist NON_COMPLIANT, wenn für den Alarm oder den optionalen Parameter keine Aktion festgelegt ist.
11.5.2	Netzwerkeinbrüche und unerwartete Dateiänderungen werden erkannt und darauf reagiert. (PCI-DSS-v4.0)	cloudwatch-alarm-settings-check	Stellen Sie sicher, dass CloudWatch Alarme mit dem angegebenen Metriknamen die angegebenen Einstellungen haben.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
11.5.2	Netzwerkeinbrüche und unerwartete Dateiänderungen werden erkannt und darauf reagiert. (PCI-DSS-v4.0)	sns-topic-message-delivery-Benachrichtigung aktiviert	Stellen Sie sicher, dass die Amazon Simple Notification Service (SNS) - Protokollierung für den Zustellungsstatus von Benachrichtigungen aktiviert ist, die an ein Thema für die Endgeräte gesendet werden. Die Regel ist NON_COMPLIANT, wenn die Benachrichtigung über den Status der Zustellung von Nachrichten nicht aktiviert ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
11.6.1	Unbefugte Änderungen auf Zahlungsseiten werden erkannt und darauf reagiert. (PCI-DSS-v4.0)	cloudformation-stack-notification-check	Stellen Sie sicher, dass Ihre CloudFormation Stacks Ereignisbenachrichtigungen an ein Amazon SNS SNS-Thema senden. Stellen Sie optional sicher, dass die angegebenen Amazon SNS SNS-Themen verwendet werden. Die Regel lautet NON_COMPLIANT, wenn CloudFormation Stacks keine Benachrichtigungen senden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
11.6.1	Unbefugte Änderungen auf Zahlungsseiten werden erkannt und darauf reagiert. (PCI-DSS-v4.0)	cloudwatch-alarm-action-check	Stellen Sie sicher, dass bei CloudWatch Alarmen eine Aktion für den Status ALARM, INSUFFICIENT_DATA oder OK konfiguriert ist. Stellen Sie optional sicher, dass alle Aktionen mit einem benannten ARN übereinstimmen. Die Regel ist NON_COMPLIANT, wenn für den Alarm oder den optionalen Parameter keine Aktion festgelegt ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
11.6.1	Unbefugte Änderungen auf Zahlungsseiten werden erkannt und darauf reagiert. (PCI-DSS-v4.0)	cloudwatch-alarm-action-check	Stellen Sie sicher, dass bei CloudWatch Alarmen eine Aktion für den Status ALARM, INSUFFICIENT_DATA oder OK konfiguriert ist. Stellen Sie optional sicher, dass alle Aktionen mit einem benannten ARN übereinstimmen. Die Regel ist NON_COMPLIANT, wenn für den Alarm oder den optionalen Parameter keine Aktion festgelegt ist.
11.6.1	Unbefugte Änderungen auf Zahlungsseiten werden erkannt und darauf reagiert. (PCI-DSS-v4.0)	cloudwatch-alarm-settings-check	Stellen Sie sicher, dass CloudWatch Alarme mit dem angegebenen Metriknamen die angegebenen Einstellungen haben.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
11.6.1	Unbefugte Änderungen auf Zahlungsseiten werden erkannt und darauf reagiert. (PCI-DSS-v4.0)	sns-topic-message-delivery-Benachrichtigung aktiviert	Stellen Sie sicher, dass die Amazon Simple Notification Service (SNS) - Protokollierung für den Zustellungsstatus von Benachrichtigungen aktiviert ist, die an ein Thema für die Endgeräte gesendet werden. Die Regel ist NON_COMPLIANT, wenn die Benachrichtigung über den Status der Zustellung von Nachrichten nicht aktiviert ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
12.10.5	Auf vermutete und bestätigte Sicherheitsvorfälle, die sich auf das CDE auswirken könnten, wird sofort reagiert. (PCI-DSS-v4.0)	cloudformation-stack-notification-check	Stellen Sie sicher, dass Ihre CloudFormation Stacks Ereignisbenachrichtigungen an ein Amazon SNS SNS-Thema senden. Stellen Sie optional sicher, dass die angegebenen Amazon SNS SNS-Themen verwendet werden. Die Regel lautet NON_COMPLIANT, wenn CloudFormation Stacks keine Benachrichtigungen senden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
12.10.5	Auf vermutete und bestätigte Sicherheitsvorfälle, die sich auf das CDE auswirken könnten, wird sofort reagiert. (PCI-DSS-v4.0)	cloudwatch-alarm-action-check	Stellen Sie sicher, dass bei CloudWatch Alarmen eine Aktion für den Status ALARM, INSUFFICIENT_DATA oder OK konfiguriert ist. Stellen Sie optional sicher, dass alle Aktionen mit einem benannten ARN übereinstimmen. Die Regel ist NON_COMPLIANT, wenn für den Alarm oder den optionalen Parameter keine Aktion festgelegt ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
12.10.5	Auf vermutete und bestätigte Sicherheitsvorfälle, die sich auf das CDE auswirken könnten, wird sofort reagiert. (PCI-DSS-v4.0)	cloudwatch-alarm-action-check	Stellen Sie sicher, dass bei CloudWatch Alarmen eine Aktion für den Status ALARM, INSUFFICIENT_DATA oder OK konfiguriert ist. Stellen Sie optional sicher, dass alle Aktionen mit einem benannten ARN übereinstimmen. Die Regel ist NON_COMPLIANT, wenn für den Alarm oder den optionalen Parameter keine Aktion festgelegt ist.
12.10.5	Auf vermutete und bestätigte Sicherheitsvorfälle, die sich auf das CDE auswirken könnten, wird sofort reagiert. (PCI-DSS-v4.0)	cloudwatch-alarm-settings-check	Stellen Sie sicher, dass CloudWatch Alarme mit dem angegebenen Metriknamen die angegebenen Einstellungen haben.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
12.10.5	Auf vermutete und bestätigte Sicherheitsvorfälle, die sich auf das CDE auswirken könnten, wird sofort reagiert. (PCI-DSS-v4.0)	sns-topic-message-delivery-Benachrichtigung aktiviert	Stellen Sie sicher, dass die Amazon Simple Notification Service (SNS) - Protokollierung für den Zustellungsstatus von Benachrichtigungen aktiviert ist, die an ein Thema für die Endgeräte gesendet werden. Die Regel ist NON_COMPLIANT, wenn die Benachrichtigung über den Status der Zustellung von Nachrichten nicht aktiviert ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
12.4.2.1	Die PCI-DSS-Konformität wird verwaltet. (PCI-DSS-v4.0)	service-catalog-shared-within-Organisation	Stellen Sie sicher, dass AWS Service Catalog Portfolios an eine Organisation weitergibt (eine Sammlung von AWS Konten, die als eine Einheit behandelt werden), wenn die Integration mit AWS Organizations aktiviert ist. Die Regel lautet NON_COMPLIANT, wenn der Wert `Type` einer Aktie `ACCOUNT` ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
2.2.5	Systemkomponenten werden sicher konfiguriert und verwaltet. (PCI-DSS-v4.0)	cloudfront-security-policy-check	Stellen Sie sicher, dass CloudFron t Amazon-Di stributionen eine Mindestsicherheits richtlinie und eine Verschlüsselungssu ite von TLSv1 .2 oder höher für Zuschauerverbindun gen verwenden . Diese Regel ist NON_COMPLIANT für eine CloudFron t Distribution, deren Wert unter .2_2018 liegt. minimumPr otocolVersion TLSv1

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
2.2.5	Systemkomponenten werden sicher konfiguriert und verwaltet. (PCI-DSS-v4.0)	cloudfront-sni-enabled	Stellen Sie sicher, dass CloudFront Amazon-Distributionen ein benutzerdefiniertes SSL-Zertifikat verwenden und so konfiguriert sind, dass SNI zur Bearbeitung von HTTPS-Anfragen verwendet wird. Die Regel ist NON_COMPLIANT, wenn ein benutzerdefiniertes SSL-Zertifikat zugeordnet ist, die SSL-Unterstützungsmethode jedoch eine dedizierte IP-Adresse ist.
2.2.5	Die Systemkomponenten werden sicher konfiguriert und verwaltet. (PCI-DSS-v4.0)	transfer-family-server-no-ftp	Stellen Sie sicher, dass ein mit AWS Transfer Family erstellter Server kein FTP für die Endpunktverbindung verwendet. Die Regel lautet NON_COMPLIANT, wenn das Serverprotokoll für die Endpunktverbindung FTP-fähig ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
2.2.5	Systemkomponenten werden sicher konfiguriert und verwaltet. (PCI-DSS-v4.0)	cloudfront-no-deprecated-ssl-protokolle	Stellen Sie sicher, dass CloudFront Distributionen keine veralteten SSL-Protokolle für die HTTPS-Kommunikation zwischen Edge-Standorten und benutzerdefinierten Ursprüngen verwenden . CloudFront Diese Regel ist NON_COMPLIANT für eine CloudFront Verteilung, falls eine Verteilung 'einschließt'. OriginSslProtocols SSLv3

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
2.2.5	Systemkomponenten werden sicher konfiguriert und verwaltet. (PCI-DSS-v4.0)	cloudfront-traffic-to-origin-verschlüsselt	Stellen Sie sicher, dass CloudFront Amazon-Distributionen den Datenverkehr zu benutzerdefinierten Ursprüngen verschlüsseln. Die Regel lautet NON_COMPLIANT, falls " " " " " " " " für 'nur' HTTP 'ist oder wennOriginProtocolPolicy' 'für' Match-Viewer 'steht und' 'für 'Allow-All' steht. OriginProtocolPolicy ViewerProtocolPolicy
2.2.5	Systemkomponenten werden sicher konfiguriert und verwaltet. (PCI-DSS-v4.0)	cloudfront-viewer-policy-https	Stellen Sie sicher, dass Ihre CloudFront Amazon-Distributionen HTTPS verwenden (direkt oder über eine Umleitung). Die Regel lautet NON_COMPLIANT, wenn der Wert von auf 'allow-all' für oder für gesetzt ViewerProtocolPolicy ist. DefaultCacheBehavior CacheBehaviors

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
2.2.7	Systemkomponenten werden sicher konfiguriert und verwaltet. (PCI-DSS-v4.0)	dms-redis-tls-enabled	Stellen Sie sicher, dass die Endpunkte des AWS Database Migration Service (AWS DMS) für Redis-Datenspeicher aktiviert sind, sodass die TLS/SSL encryption of data communicated with other endpoints. The rule is NON_COMPLIANT if TLS/SSL Verschlüsselung nicht aktiviert ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
2.2.7	Systemkomponenten werden sicher konfiguriert und verwaltet. (PCI-DSS-v4.0)	cloudfront-no-deprecated-ssl-protokolle	Stellen Sie sicher, dass CloudFront Distributionen keine veralteten SSL-Protokolle für die HTTPS-Kommunikation zwischen Edge-Standorten und benutzerdefinierten Ursprüngen verwenden . CloudFront Diese Regel ist NON_COMPLIANT für eine CloudFront Verteilung, falls eine Verteilung 'einschließt'. OriginSslProtocols SSLv3

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
2.2.7	Systemkomponenten werden sicher konfiguriert und verwaltet. (PCI-DSS-v4.0)	cloudfront-traffic-to-origin-verschlüsselt	Stellen Sie sicher, dass CloudFront Amazon-Distributionen den Datenverkehr zu benutzerdefinierten Ursprüngen verschlüsseln. Die Regel lautet NON_COMPLIANT, falls " " " " " " " " für 'nur' HTTP 'ist oder wennOriginProtocolPolicy' 'für' Match-Viewer 'steht und' 'für 'Allow-All' steht. OriginProtocolPolicy ViewerProtocolPolicy
2.2.7	Systemkomponenten werden sicher konfiguriert und verwaltet. (PCI-DSS-v4.0)	cloudfront-viewer-policy-https	Stellen Sie sicher, dass Ihre CloudFront Amazon-Distributionen HTTPS verwenden (direkt oder über eine Umleitung). Die Regel lautet NON_COMPLIANT, wenn der Wert von auf 'allow-all' für oder für gesetzt ViewerProtocolPolicy ist. DefaultCacheBehavior CacheBehaviors

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
2.2.7	Systemkomponenten werden sicher konfiguriert und verwaltet. (PCI-DSS-v4.0)	elb-acm-certificate-required	Stellen Sie sicher, dass die Classic Load Balancers SSL-Zerti fikate verwenden, die vom AWS Certificate Manager bereitgestellt werden. Verwenden Sie zur Nutzung dieser Regel mit Ihrem Classic Load Balancer einen SSL- oder HTTPS-Listener. Hinweis: Diese Regel gilt nur für Classic Load Balancers. Mit dieser Regel werden keine Applicati on Load Balancer oder Network Load Balancer geprüft.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
2.2.7	Systemkomponenten werden sicher konfiguriert und verwaltet. (PCI-DSS-v4.0)	dax-tls-endpoint-encryption	Stellen Sie sicher, dass Ihr Amazon DynamoDB Accelerator (DAX) -Cluster auf TLS ClusterEndpointEncryptionType eingestellt ist. Die Regel lautet NON_COMPLIANT, wenn ein DAX-Cluster nicht mit Transport Layer Security (TLS) verschlüsselt ist.
2.2.7	Systemkomponenten werden sicher konfiguriert und verwaltet. (PCI-DSS-v4.0)	msk-in-cluster-node-TLS erforderlich	Stellen Sie sicher, dass ein Amazon MSK-Cluster die Verschlüsselung während der Übertragung mithilfe von HTTPS (TLS) mit den Broker-Knoten des Clusters erzwingt. Die Regel ist NON_COMPLIANT, wenn Klartextkommunikation für Broker-Knotenverbindungen in Clustern aktiviert ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
2.2.7	Systemkomponenten werden sicher konfiguriert und verwaltet. (PCI-DSS-v4.0)	dms-endpoint-ssl-configured	Stellen Sie sicher, dass die Endpunkte des AWS Database Migration Service (AWS DMS) mit einer SSL-Verbindung konfiguriert sind. Die Regel lautet NON_COMPLIANT, wenn für AWS DMS keine SSL-Verbindung konfiguriert ist.
3.2.1	Die Speicherung von Kontodaten wird auf ein Minimum beschränkt. (PCI-DSS-v4.0)	ec2- volume-inuse-check	Stellen Sie sicher, dass EBS-Volumes an Instances angehängt sind. EC2 Stellen Sie optional sicher, dass EBS-Volumes zum Löschen markiert sind, wenn eine Instance beendet wird.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.2.1	Die Speicherung von Kontodaten wird auf ein Minimum beschränkt. (PCI-DSS-v4.0)	ecr-private-lifecycle-policy-konfiguriert	Stellen Sie sicher, dass für ein privates Amazon Elastic Container Registry (ECR) -Repository mindestens eine Lebenszyklusrichtlinie konfiguriert ist. Die Regel ist NON_COMPLIANT, wenn keine Lebenszyklus-Richtlinie für das private ECR-Repository konfiguriert ist.
3.2.1	Die Speicherung von Kontodaten wird auf ein Minimum beschränkt. (PCI-DSS-v4.0)	dynamodb-pitr-enabled	Stellen Sie sicher, dass point-in-time Recovery (PITR) für Amazon DynamoDB-Tabellen aktiviert ist. Die Regel ist NON_COMPLIANT, wenn PITR für DynamoDB-Tabellen nicht aktiviert ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.2.1	Die Speicherung von Kontodaten wird auf ein Minimum beschränkt. (PCI-DSS-v4.0)	cw-loggroup-retention-period-überprüfen	Stellen Sie sicher, dass ein CloudWatch LogGroup Amazon-Aufbewahrungszeitraum auf mehr als 365 Tage oder einen bestimmten Aufbewahrungszeitraum festgelegt ist. Die Regel lautet NON_COMPLIANT, wenn die Aufbewahrungsfrist weniger als MinRetentionTime, falls angegeben, oder andernfalls 365 Tage beträgt.
3.3.1.1	Sensible Authentifizierungsdaten (SAD) werden nach der Autorisierung nicht gespeichert. (PCI-DSS-v4.0)	ec2- volume-inuse-check	Stellen Sie sicher, dass EBS-Volumes an Instances angehängt sind. EC2 Stellen Sie optional sicher, dass EBS-Volumes zum Löschen markiert sind, wenn eine Instance beendet wird.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.3.1.1	Sensible Authentif izierungsdaten (SAD) werden nach der Autorisierung nicht gespeichert. (PCI-DSS-v4.0)	ecr-private-lifecycle-policy-konfiguriert	Stellen Sie sicher, dass für ein privates Amazon Elastic Container Registry (ECR) -Reposito ry mindestens eine Lebenszyk lusrichtlinie konfiguri ert ist. Die Regel ist NON_COMPL IANT, wenn keine Lebenszyklus-Richt linie für das private ECR-Repository konfiguriert ist.
3.3.1.1	Sensible Authentif izierungsdaten (SAD) werden nach der Autorisierung nicht gespeichert. (PCI-DSS-v4.0)	dynamodb-pitr-enab led	Stellen Sie sicher, dass point-in-time Recovery (PITR) für Amazon DynamoDB-Tabellen aktiviert ist. Die Regel ist NON_COMPLIANT, wenn PITR für DynamoDB-Tabellen nicht aktiviert ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.3.1.1	Sensible Authentif izierungsdaten (SAD) werden nach der Autorisierung nicht gespeichert. (PCI-DSS-v4.0)	cw-loggroup-retent ion-period-überprüfen	Stellen Sie sicher, dass ein CloudWatc h LogGroup Amazon-Aufbewahrungszeitrau m auf mehr als 365 Tage oder einen bestimmten Aufbewahrungszeitr aum festgelegt ist. Die Regel lautet NON_COMPLIANT, wenn die Aufbewahr ungsfrist weniger als MinRetentionTime, falls angegeben, oder andernfalls 365 Tage beträgt.
3.3.1.3	Sensible Authentif izierungsdaten (SAD) werden nach der Autorisierung nicht gespeichert. (PCI-DSS-v4.0)	ec2- volume-inuse-check	Stellen Sie sicher, dass EBS-Volum es an Instances angehängt sind. EC2 Stellen Sie optional sicher, dass EBS-Volumes zum Löschen markiert sind, wenn eine Instance beendet wird.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.3.1.3	Sensible Authentif izierungsdaten (SAD) werden nach der Autorisierung nicht gespeichert. (PCI-DSS-v4.0)	ecr-private-lifecycle-policy-konfiguriert	Stellen Sie sicher, dass für ein privates Amazon Elastic Container Registry (ECR) -Reposito ry mindestens eine Lebenszyk lusrichtlinie konfiguri ert ist. Die Regel ist NON_COMPL IANT, wenn keine Lebenszyklus-Richt linie für das private ECR-Repository konfiguriert ist.
3.3.1.3	Sensible Authentif izierungsdaten (SAD) werden nach der Autorisierung nicht gespeichert. (PCI-DSS-v4.0)	dynamodb-pitr-enab led	Stellen Sie sicher, dass point-in-time Recovery (PITR) für Amazon DynamoDB-Tabellen aktiviert ist. Die Regel ist NON_COMPLIANT, wenn PITR für DynamoDB-Tabellen nicht aktiviert ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.3.1.3	Sensible Authentif izierungsdaten (SAD) werden nach der Autorisierung nicht gespeichert. (PCI-DSS-v4.0)	cw-loggroup-retent ion-period-überprüfen	Stellen Sie sicher, dass ein CloudWatc h LogGroup Amazon-Aufbewahrungszeitrau m auf mehr als 365 Tage oder einen bestimmten Aufbewahrungszeitr aum festgelegt ist. Die Regel lautet NON_COMPLIANT, wenn die Aufbewahr ungsfrist weniger als MinRetentionTime, falls angegeben, oder andernfalls 365 Tage beträgt.
3.3.2	Sensible Authentif izierungsdaten (SAD) werden nach der Autorisierung nicht gespeichert. (PCI-DSS-v4.0)	ec2- volume-inuse-check	Stellen Sie sicher, dass EBS-Volum es an Instances angehängt sind. EC2 Stellen Sie optional sicher, dass EBS-Volumes zum Löschen markiert sind, wenn eine Instance beendet wird.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.3.2	Sensible Authentif izierungsdaten (SAD) werden nach der Autorisierung nicht gespeichert. (PCI-DSS-v4.0)	ecr-private-lifecycle-policy-konfiguriert	Stellen Sie sicher, dass für ein privates Amazon Elastic Container Registry (ECR) -Reposito ry mindestens eine Lebenszyk lusrichtlinie konfiguri ert ist. Die Regel ist NON_COMPL IANT, wenn keine Lebenszyklus-Richt linie für das private ECR-Repository konfiguriert ist.
3.3.2	Sensible Authentif izierungsdaten (SAD) werden nach der Autorisierung nicht gespeichert. (PCI-DSS-v4.0)	dynamodb-pitr-enab led	Stellen Sie sicher, dass point-in-time Recovery (PITR) für Amazon DynamoDB-Tabellen aktiviert ist. Die Regel ist NON_COMPLIANT, wenn PITR für DynamoDB-Tabellen nicht aktiviert ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.3.2	Sensible Authentif izierungsdaten (SAD) werden nach der Autorisierung nicht gespeichert. (PCI-DSS-v4.0)	cw-loggroup-retent ion-period-überprüfen	Stellen Sie sicher, dass ein CloudWatc h LogGroup Amazon-Aufbewahrungszeitrau m auf mehr als 365 Tage oder einen bestimmten Aufbewahrungszeitr aum festgelegt ist. Die Regel lautet NON_COMPLIANT, wenn die Aufbewahr ungsfrist weniger als MinRetentionTime, falls angegeben, oder andernfalls 365 Tage beträgt.
3.3.3	Sensible Authentif izierungsdaten (SAD) werden nach der Autorisierung nicht gespeichert. (PCI-DSS-v4.0)	ec2- volume-inuse-check	Stellen Sie sicher, dass EBS-Volum es an Instances angehängt sind. EC2 Stellen Sie optional sicher, dass EBS-Volumes zum Löschen markiert sind, wenn eine Instance beendet wird.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.3.3	Sensible Authentif izierungsdaten (SAD) werden nach der Autorisierung nicht gespeichert. (PCI-DSS-v4.0)	ecr-private-lifecycle-policy-konfiguriert	Stellen Sie sicher, dass für ein privates Amazon Elastic Container Registry (ECR) -Reposito ry mindestens eine Lebenszyk lusrichtlinie konfiguri ert ist. Die Regel ist NON_COMPL IANT, wenn keine Lebenszyklus-Richt linie für das private ECR-Repository konfiguriert ist.
3.3.3	Sensible Authentif izierungsdaten (SAD) werden nach der Autorisierung nicht gespeichert. (PCI-DSS-v4.0)	dynamodb-pitr-enab led	Stellen Sie sicher, dass point-in-time Recovery (PITR) für Amazon DynamoDB-Tabellen aktiviert ist. Die Regel ist NON_COMPLIANT, wenn PITR für DynamoDB-Tabellen nicht aktiviert ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.3.3	Sensible Authentifizierungsdaten (SAD) werden nach der Autorisierung nicht gespeichert. (PCI-DSS-v4.0)	cw-loggroup-retention-period-überprüfen	Stellen Sie sicher, dass ein CloudWatch LogGroup Amazon-Aufbewahrungszeitraum auf mehr als 365 Tage oder einen bestimmten Aufbewahrungszeitraum festgelegt ist. Die Regel lautet NON_COMPLIANT, wenn die Aufbewahrungsfrist weniger als MinRetentionTime, falls angegeben, oder andernfalls 365 Tage beträgt.
3.5.1	Die primäre Kontonummer (PAN) ist überall dort gesichert, wo sie gespeichert ist. (PCI-DSS-v4.0)	athena-workgroup-encrypted-at-ausruhen	Stellen Sie sicher, dass eine Amazon Athena Athena-Arbeitsgruppe im Ruhezustand verschlüsselt ist. Die Regel ist NON_COMPLIANT, wenn die Verschlüsselung von Daten im Ruhezustand für eine Athena-Arbeitsgruppe nicht aktiviert ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.5.1	Die primäre Kontonummer (PAN) ist überall dort gesichert, wo sie gespeichert ist. (PCI-DSS-v4.0)	neptune-cluster-snapshot-encrypted	Stellen Sie sicher, dass ein Amazon Neptune Neptune-DB-Cluster über verschlüsselte Snapshots verfügt. Die Regel ist NON_COMPLIANT, wenn ein Neptune-Cluster keine verschlüsselten Snapshots enthält.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.5.1	Die primäre Kontonummer (PAN) ist überall dort gesichert, wo sie gespeichert ist. (PCI-DSS-v4.0)	redshift-cluster-kms-enabled	Stellen Sie sicher, dass Amazon Redshift Redshift-Cluster einen bestimmten AWS Key Management Service (AWS KMS) -Schlüssel für die Verschlüsselung verwenden. Die Regel ist KONFORM, wenn die Verschlüs selung aktiviert ist und der Cluster mit dem im kmsKeyArn Parameter angegeben en Schlüssel verschlüsselt ist. Die Regel ist NON_COMPLIANT, wenn der Cluster nicht oder mit einem anderen Schlüssel verschlüsselt ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.5.1	Die primäre Kontonummer (PAN) ist überall dort gesichert, wo sie gespeichert ist. (PCI-DSS-v4.0)	codebuild-project-artifact-encryption	Stellen Sie sicher, dass in einem AWS CodeBuild Projekt die Verschlüsselung für alle Artefakte aktiviert ist. Die Regel ist NON_COMPLIANT, wenn „encryptionDisabled“ für alle primären oder sekundären (falls vorhanden) Artefaktkonfigurationen auf „True“ festgelegt ist.
3.5.1	Die primäre Kontonummer (PAN) ist überall dort gesichert, wo sie gespeichert ist. (PCI-DSS-v4.0)	codebuild-project-s3-log-verschlüsselt	Stellen Sie sicher, dass bei einem mit Amazon S3 Logs konfigurierten AWS CodeBuild Projekt die Verschlüsselung für die Protokolle aktiviert ist. Die Regel lautet NON_COMPLIANT, wenn „EncryptionDisabled“ in einem S3-Projekt auf „true“ gesetzt ist. LogsConfig CodeBuild

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.5.1	Die primäre Kontonummer (PAN) ist überall dort gesichert, wo sie gespeichert ist. (PCI-DSS-v4.0)	dax-encryption-enabled	Stellen Sie sicher, dass Amazon DynamoDB Accelerator (DAX) -Cluster verschlüsselt sind. Die Regel ist NON_COMPLIANT, wenn ein DAX-Cluster nicht verschlüsselt ist.
3.5.1	Die primäre Kontonummer (PAN) ist überall dort gesichert, wo sie gespeichert ist. (PCI-DSS-v4.0)	eks-secrets-encrypted	Stellen Sie sicher, dass Amazon Elastic Kubernetes Service Service-Cluster so konfiguriert sind, dass Kubernetes-Geheimnisse mithilfe von AWS Key Management Service (KMS) -Schlüsseln verschlüsselt werden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.5.1	Die primäre Kontonummer (PAN) ist überall dort gesichert, wo sie gespeichert ist. (PCI-DSS-v4.0)	api-gw-cache-enabled-und-verschlüsselt	Stellen Sie sicher, dass für alle Methoden in den Amazon API Gateway Gateway-Stufen der Cache aktiviert und der Cache verschlüsselt ist. Die Regel ist NON_COMPLIANT, wenn für eine Methode in einer Amazon-API-Gateway-Stufe der Cache nicht konfiguriert oder nicht verschlüsselt ist.
3.5.1	Die primäre Kontonummer (PAN) ist überall dort gesichert, wo sie gespeichert ist. (PCI-DSS-v4.0)	docdb-cluster-encrypted	Stellen Sie sicher, dass die Speicherverschlüsselung für Ihre Amazon DocumentDB-Cluster (mit MongoDB-Kompatibilität) aktiviert ist. Die Regel ist NON_COMPLIANT, wenn die Speicherverschlüsselung nicht aktiviert ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.5.1	Die primäre Kontonummer (PAN) ist überall dort gesichert, wo sie gespeichert ist. (PCI-DSS-v4.0)	dynamodb-table-encrypted-kms	Stellen Sie sicher, dass die Amazon DynamoDB-Tabelle mit dem AWS Key Management Service (KMS) verschlüsselt ist. Die Regel lautet NON_COMPLIANT, wenn die Amazon DynamoDB-Tabelle nicht mit KMS verschlüsselt ist. AWS Die Regel ist auch NON_COMPLIANT, wenn der verschlüsselte AWS KMS-Schlüssel nicht im Eingabeparameter vorhanden ist. kmsKeyArns
3.5.1	Die primäre Kontonummer (PAN) ist überall dort gesichert, wo sie gespeichert ist. (PCI-DSS-v4.0)	dynamodb-table-encryption-enabled	Stellen Sie sicher, dass die Amazon DynamoDB-Tabellen verschlüsselt sind, und überprüfen Sie ihren Status. Die Regel ist COMPLIANT, wenn der Status "Aktiviert" oder "Wird aktiviert" lautet.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.5.1	Die primäre Kontonummer (PAN) ist überall dort gesichert, wo sie gespeichert ist. (PCI-DSS-v4.0)	codebuild-project-envvar-awscred-überprüfen	Stellen Sie sicher, dass das Projekt KEINE Umgebungs variablen und _ACCESS_KEY enthält. AWS_ACCES S_KEY_ID AWS_SECRE T Die Regel ist NON_COMPLIANT, wenn die Projekt-U mgebungsvariablen Klartext-Anmeldein formationen enthalten.
3.5.1	Die primäre Kontonummer (PAN) ist überall dort gesichert, wo sie gespeichert ist. (PCI-DSS-v4.0)	eks-cluster-secrets-encrypted	Stellen Sie sicher, dass Amazon EKS-Cluster nicht so konfiguriert sind, dass Kubernetes-Geheimnisse mit KMS verschlüsselt AWS werden. Die Regel lautet NON_COMPL IANT, wenn ein EKS-Cluster keine EncryptionConfig-R essource hat oder wenn Encryptio nConfig Geheimnisse nicht als Ressource benennt.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.5.1	Die primäre Kontonummer (PAN) ist überall dort gesichert, wo sie gespeichert ist. (PCI-DSS-v4.0)	kinesis-stream-encrypted	Stellen Sie sicher, dass Amazon Kinesis Kinesis-Streams im Ruhezustand mit serverseitiger Verschlüsselung verschlüsselt werden. Die Regel lautet NON_COMPLIANT für einen Kinesis-Stream, wenn 'StreamEncryption' nicht vorhanden ist.
3.5.1	Die primäre Kontonummer (PAN) ist überall dort gesichert, wo sie gespeichert ist. (PCI-DSS-v4.0)	neptune-cluster-encrypted	Stellen Sie sicher, dass die Speicherverschlüsselung für Ihre Amazon Neptune Neptune-DB-Cluster aktiviert ist. Die Regel ist NON_COMPLIANT, wenn die Speicherverschlüsselung nicht aktiviert ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.5.1.1	Die primäre Kontonummer (PAN) ist überall dort gesichert, wo sie gespeichert ist. (PCI-DSS-v4.0)	acm-pca-root-ca-deaktiviert	Stellen Sie sicher, dass die AWS Private Certificate Authority (AWS Private CA) über eine deaktivierte Stammzertifizierungsstelle verfügt. Die Regel ist NON_COMPLIANT für Root-Benutzer CAs mit einem Status, der nicht DEAKTIVIERT ist.
3.5.1.1	Die primäre Kontonummer (PAN) ist überall dort gesichert, wo sie gespeichert ist. (PCI-DSS-v4.0)	cloudfront-custom-ssl-certificate	Stellen Sie sicher, dass das mit einer CloudFront Amazon-Distribution verknüpfte Zertifikat nicht das Standard-SSL-Zertifikat ist. Die Regel lautet NON_COMPLIANT, wenn eine CloudFront Distribution das Standard-SSL-Zertifikat verwendet.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.5.1.1	Die primäre Kontonummer (PAN) ist überall dort gesichert, wo sie gespeichert ist. (PCI-DSS-v4.0)	elb-acm-certificate-required	Stellen Sie sicher, dass die Classic Load Balancers SSL-Zerti fikate verwenden, die vom AWS Certificate Manager bereitgestellt werden. Verwenden Sie zur Nutzung dieser Regel mit Ihrem Classic Load Balancer einen SSL- oder HTTPS-Listener. Hinweis: Diese Regel gilt nur für Classic Load Balancers. Mit dieser Regel werden keine Applicati on Load Balancer oder Network Load Balancer geprüft.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.5.1.3	Die primäre Kontonummer (PAN) ist überall dort gesichert, wo sie gespeichert ist. (PCI-DSS-v4.0)	acm-pca-root-ca-deaktiviert	Stellen Sie sicher, dass die AWS Private Certificate Authority (AWS Private CA) über eine deaktivierte Stammzertifizierungsstelle verfügt. Die Regel ist NON_COMPLIANT für Root-Benutzer CAs mit einem Status, der nicht DEAKTIVIERT ist.
3.5.1.3	Die primäre Kontonummer (PAN) ist überall dort gesichert, wo sie gespeichert ist. (PCI-DSS-v4.0)	cloudfront-custom-ssl-certificate	Stellen Sie sicher, dass das mit einer CloudFront Amazon-Distribution verknüpfte Zertifikat nicht das Standard-SSL-Zertifikat ist. Die Regel lautet NON_COMPLIANT, wenn eine CloudFront Distribution das Standard-SSL-Zertifikat verwendet.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.5.1.3	Die primäre Kontonummer (PAN) ist überall dort gesichert, wo sie gespeichert ist. (PCI-DSS-v4.0)	neptune-cluster-snapshot-public-verboten	Stellen Sie sicher, dass ein manueller Amazon Neptune Neptune-DB-Cluster-Snapshot nicht öffentlich ist. Die Regel ist NON_COMPLIANT, wenn es vorhandene und neue Neptune-Cluster-Snapshots gibt, die öffentlich zugänglich sind.
3.5.1.3	Die primäre Kontonummer (PAN) ist überall dort gesichert, wo sie gespeichert ist. (PCI-DSS-v4.0)	docdb-cluster-snapshot-public-verboten	Stellen Sie sicher, dass manuelle Cluster-Snapshots von Amazon DocumentDB nicht öffentlich sind. Die Regel ist NON_COMPLIANT, wenn manuelle Cluster-Snapshots von Amazon DocumentDB öffentlich sind.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.5.1.3	Die primäre Kontonummer (PAN) ist überall dort gesichert, wo sie gespeichert ist. (PCI-DSS-v4.0)	backup-recovery-point-manual-Löschen-deaktiviert	Stellen Sie sicher, dass einem Backup-Tresor eine ressourcenbasierte Richtlinie zugeordnet ist, die das Löschen von Wiederherstellungspunkten verhindert. Die Regel lautet NON_COMPLIANT, wenn der Backup-Tresor keine ressourcenbasierten Richtlinien oder Richtlinien ohne eine geeignete „Deny“ -Anweisung (Anweisung mit den Berechtigungen backup:DeleteRecoveryPoint, backup: und backup:UpdateRecoveryPointLifecycle) hat. PutBackupVaultAccessPolicy

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.5.1.3	Die primäre Kontonummer (PAN) ist überall dort gesichert, wo sie gespeichert ist. (PCI-DSS-v4.0)	elb-acm-certificate-required	Stellen Sie sicher, dass die Classic Load Balancers SSL-Zerti fikate verwenden, die vom AWS Certificate Manager bereitgestellt werden. Verwenden Sie zur Nutzung dieser Regel mit Ihrem Classic Load Balancer einen SSL- oder HTTPS-Listener. Hinweis: Diese Regel gilt nur für Classic Load Balancers. Mit dieser Regel werden keine Applicati on Load Balancer oder Network Load Balancer geprüft.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.5.1.3	Die primäre Kontonummer (PAN) ist überall dort gesichert, wo sie gespeichert ist. (PCI-DSS-v4.0)	emr-block-public-access	Stellen Sie sicher, dass für ein Konto bei Amazon EMR die Einstellungen zum Sperren des öffentlichen Zugriffs aktiviert sind. Die Regel ist NON_COMPLIANT, wenn sie falsch BlockPublicSecurityGroupRules ist, oder wenn sie wahr ist, sind andere Ports als Port 22 unter aufgeführt. Permitted PublicSecurityGroupRuleRanges
3.5.1.3	Die primäre Kontonummer (PAN) ist überall dort gesichert, wo sie gespeichert ist. (PCI-DSS-v4.0)	access-point-public-accesss3-Blöcke	Stellen Sie sicher, dass Amazon S3 S3-Zugriffspunkten die Einstellungen zum Blockieren des öffentlichen Zugriffs aktiviert sind. Die Regel ist NON_COMPLIANT, wenn die Einstellung zum Blockieren des öffentlichen Zugriffs für S3-Zugangspunkte nicht aktiviert ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.5.1.3	Die primäre Kontonummer (PAN) ist überall dort gesichert, wo sie gespeichert ist. (PCI-DSS-v4.0)	account-level-public-accesss3-Blöcke	Stellen Sie sicher, dass die erforderl ichen Einstellungen für die Sperrung des öffentlichen Zugriffs auf Kontoebene konfiguriert sind. Die Regel ist nur NON_COMPL IANT, wenn die unten festgeleg ten Felder nicht mit den entsprech enden Feldern im Konfigurationselement übereinstimmen.
3.5.1.3	Die primäre Kontonummer (PAN) ist überall dort gesichert, wo sie gespeichert ist. (PCI-DSS-v4.0)	s-3 bucket-mfa-delete-enabled	Stellen Sie sicher, dass MFA Delete in der Bucket-Ve rsionierungskonfig uration von Amazon Simple Storage Service (Amazon S3) aktiviert ist. Die Regel ist NON_COMPL IANT, wenn MFA Delete nicht aktiviert ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.6.1	Kryptografische Schlüssel, die zum Schutz der gespeicherten Kontodaten verwendet werden, sind gesichert. (PCI-DSS-v4.0)	acm-pca-root-ca-deaktiviert	Stellen Sie sicher, dass die AWS Private Certificate Authority (AWS Private CA) über eine deaktivierte Stammzertifizierungsstelle verfügt. Die Regel ist NON_COMPLIANT für Root-Benutzer CAs mit einem Status, der nicht DEAKTIVIERT ist.
3.6.1	Kryptografische Schlüssel, die zum Schutz der gespeicherten Kontodaten verwendet werden, sind gesichert. (PCI-DSS-v4.0)	cloudfront-custom-ssl-certificate	Stellen Sie sicher, dass das mit einer CloudFront Amazon-Distribution verknüpfte Zertifikat nicht das Standard-SSL-Zertifikat ist. Die Regel lautet NON_COMPLIANT, wenn eine CloudFront Distribution das Standard-SSL-Zertifikat verwendet.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.6.1	Kryptografische Schlüssel, die zum Schutz der gespeiche rten Kontodaten verwendet werden, sind gesichert. (PCI-DSS-v4.0)	elb-acm-certificate-required	Stellen Sie sicher, dass die Classic Load Balancers SSL-Zerti fikate verwenden, die vom AWS Certificate Manager bereitgestellt werden. Verwenden Sie zur Nutzung dieser Regel mit Ihrem Classic Load Balancer einen SSL- oder HTTPS-Listener. Hinweis: Diese Regel gilt nur für Classic Load Balancers. Mit dieser Regel werden keine Applicati on Load Balancer oder Network Load Balancer geprüft.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.6.1.2	Kryptografische Schlüssel, die zum Schutz der gespeicherten Kontodaten verwendet werden, sind gesichert. (PCI-DSS-v4.0)	acm-pca-root-ca-deaktiviert	Stellen Sie sicher, dass die AWS Private Certificate Authority (AWS Private CA) über eine deaktivierte Stammzertifizierungsstelle verfügt. Die Regel ist NON_COMPLIANT für Root-Benutzer CAs mit einem Status, der nicht DEAKTIVIERT ist.
3.6.1.2	Kryptografische Schlüssel, die zum Schutz der gespeicherten Kontodaten verwendet werden, sind gesichert. (PCI-DSS-v4.0)	cloudfront-custom-ssl-certificate	Stellen Sie sicher, dass das mit einer CloudFront Amazon-Distribution verknüpfte Zertifikat nicht das Standard-SSL-Zertifikat ist. Die Regel lautet NON_COMPLIANT, wenn eine CloudFront Distribution das Standard-SSL-Zertifikat verwendet.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.6.1.2	Kryptografische Schlüssel, die zum Schutz der gespeiche rten Kontodaten verwendet werden, sind gesichert. (PCI-DSS-v4.0)	elb-acm-certificate-required	Stellen Sie sicher, dass die Classic Load Balancers SSL-Zerti fikate verwenden, die vom AWS Certificate Manager bereitgestellt werden. Verwenden Sie zur Nutzung dieser Regel mit Ihrem Classic Load Balancer einen SSL- oder HTTPS-Listener. Hinweis: Diese Regel gilt nur für Classic Load Balancers. Mit dieser Regel werden keine Applicati on Load Balancer oder Network Load Balancer geprüft.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.6.1.3	Kryptografische Schlüssel, die zum Schutz der gespeicherten Kontodaten verwendet werden, sind gesichert. (PCI-DSS-v4.0)	acm-pca-root-ca-deaktiviert	Stellen Sie sicher, dass die AWS Private Certificate Authority (AWS Private CA) über eine deaktivierte Stammzertifizierungsstelle verfügt. Die Regel ist NON_COMPLIANT für Root-Benutzer CAs mit einem Status, der nicht DEAKTIVIERT ist.
3.6.1.3	Kryptografische Schlüssel, die zum Schutz der gespeicherten Kontodaten verwendet werden, sind gesichert. (PCI-DSS-v4.0)	cloudfront-custom-ssl-certificate	Stellen Sie sicher, dass das mit einer CloudFront Amazon-Distribution verknüpfte Zertifikat nicht das Standard-SSL-Zertifikat ist. Die Regel lautet NON_COMPLIANT, wenn eine CloudFront Distribution das Standard-SSL-Zertifikat verwendet.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.6.1.3	Kryptografische Schlüssel, die zum Schutz der gespeiche rten Kontodaten verwendet werden, sind gesichert. (PCI-DSS-v4.0)	elb-acm-certificate-required	Stellen Sie sicher, dass die Classic Load Balancers SSL-Zerti fikate verwenden, die vom AWS Certificate Manager bereitgestellt werden. Verwenden Sie zur Nutzung dieser Regel mit Ihrem Classic Load Balancer einen SSL- oder HTTPS-Listener. Hinweis: Diese Regel gilt nur für Classic Load Balancers. Mit dieser Regel werden keine Applicati on Load Balancer oder Network Load Balancer geprüft.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.6.1.4	Kryptografische Schlüssel, die zum Schutz der gespeicherten Kontodaten verwendet werden, sind gesichert. (PCI-DSS-v4.0)	acm-pca-root-ca-deaktiviert	Stellen Sie sicher, dass die AWS Private Certificate Authority (AWS Private CA) über eine deaktivierte Stammzertifizierungsstelle verfügt. Die Regel ist NON_COMPLIANT für Root-Benutzer CAs mit einem Status, der nicht DEAKTIVIERT ist.
3.6.1.4	Kryptografische Schlüssel, die zum Schutz der gespeicherten Kontodaten verwendet werden, sind gesichert. (PCI-DSS-v4.0)	cloudfront-custom-ssl-certificate	Stellen Sie sicher, dass das mit einer CloudFront Amazon-Distribution verknüpfte Zertifikat nicht das Standard-SSL-Zertifikat ist. Die Regel lautet NON_COMPLIANT, wenn eine CloudFront Distribution das Standard-SSL-Zertifikat verwendet.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.6.1.4	Kryptografische Schlüssel, die zum Schutz der gespeiche rten Kontodaten verwendet werden, sind gesichert. (PCI-DSS-v4.0)	elb-acm-certificate-required	Stellen Sie sicher, dass die Classic Load Balancers SSL-Zerti fikate verwenden, die vom AWS Certificate Manager bereitgestellt werden. Verwenden Sie zur Nutzung dieser Regel mit Ihrem Classic Load Balancer einen SSL- oder HTTPS-Listener. Hinweis: Diese Regel gilt nur für Classic Load Balancers. Mit dieser Regel werden keine Applicati on Load Balancer oder Network Load Balancer geprüft.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.7.1	Wo Kryptografie zum Schutz gespeicherter Kontodaten eingesetzt wird, werden Schlüsselverwaltungsprozesse und -verfahren, die alle Aspekte des Schlüssellebenszyklus abdecken, definiert und implementiert. (PCI-DSS-v4.0)	acm-certificate-rsa-check	Stellen Sie sicher, dass von AWS Certificate Manager (ACM) verwaltete RSA-Zertifikate eine Schlüssellänge von mindestens '2048' Bit haben. Die Regel lautet NON_COMPLIANT, wenn die Mindestschlüssellänge weniger als 2048 Bit beträgt.
3.7.1	Wo Kryptografie zum Schutz gespeicherter Kontodaten verwendet wird, werden Schlüsselverwaltungsprozesse und -verfahren, die alle Aspekte des Schlüssellebenszyklus abdecken, definiert und implementiert. (PCI-DSS-v4.0)	acm-pca-root-ca-deaktiviert	Stellen Sie sicher, dass die AWS Private Certificate Authority (AWS Private CA) über eine deaktivierte Stammzertifizierungsstelle verfügt. Die Regel ist NON_COMPLIANT für Root-Benutzer CAs mit einem Status, der nicht DEAKTIVIERT ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.7.1	Wo Kryptografie zum Schutz gespeicherter Kontodaten eingesetzt wird, werden Schlüsselverwaltungsprozesse und -verfahren, die alle Aspekte des Schlüssellebenszyklus abdecken, definiert und implementiert. (PCI-DSS-v4.0)	cloudfront-custom-ssl-certificate	Stellen Sie sicher, dass das mit einer CloudFront Amazon-Distribution verknüpfte Zertifikat nicht das Standard-SSL-Zertifikat ist. Die Regel lautet NON_COMPLIANT, wenn eine CloudFront Distribution das Standard-SSL-Zertifikat verwendet.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.7.1	Wenn Kryptogra fie zum Schutz gespeicherter Kontodaten verwendet wird, werden Schlüssel verwaltungsprozess e und -verfahren, die alle Aspekte des Schlüssel lebenszyklus abdecken, definiert und implementiert. (PCI-DSS-v4.0)	elb-acm-certificate-required	Stellen Sie sicher, dass die Classic Load Balancers SSL-Zerti fikate verwenden, die vom AWS Certificate Manager bereitgestellt werden. Verwenden Sie zur Nutzung dieser Regel mit Ihrem Classic Load Balancer einen SSL- oder HTTPS-Listener. Hinweis: Diese Regel gilt nur für Classic Load Balancers. Mit dieser Regel werden keine Applicati on Load Balancer oder Network Load Balancer geprüft.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.7.2	Wo Kryptografie zum Schutz gespeicherter Kontodaten eingesetzt wird, werden Schlüsselverwaltungsprozesse und -verfahren, die alle Aspekte des Schlüssellebenszyklus abdecken, definiert und implementiert. (PCI-DSS-v4.0)	acm-pca-root-ca-deaktiviert	Stellen Sie sicher, dass die AWS Private Certificate Authority (AWS Private CA) über eine deaktivierte Stammzertifizierungsstelle verfügt. Die Regel ist NON_COMPLIANT für Root-Benutzer CAs mit einem Status, der nicht DEAKTIVIERT ist.
3.7.2	Wo Kryptografie zum Schutz gespeicherter Kontodaten eingesetzt wird, werden Schlüsselverwaltungsprozesse und -verfahren, die alle Aspekte des Schlüssellebenszyklus abdecken, definiert und implementiert. (PCI-DSS-v4.0)	cloudfront-custom-ssl-certificate	Stellen Sie sicher, dass das mit einer CloudFront Amazon-Distribution verknüpfte Zertifikat nicht das Standard-SSL-Zertifikat ist. Die Regel lautet NON_COMPLIANT, wenn eine CloudFront Distribution das Standard-SSL-Zertifikat verwendet.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.7.2	Wenn Kryptogra fie zum Schutz gespeicherter Kontodaten verwendet wird, werden Schlüssel verwaltungsprozess e und -verfahren, die alle Aspekte des Schlüssel lebenszyklus abdecken, definiert und implementiert. (PCI-DSS-v4.0)	elb-acm-certificate-required	Stellen Sie sicher, dass die Classic Load Balancers SSL-Zerti fikate verwenden, die vom AWS Certificate Manager bereitgestellt werden. Verwenden Sie zur Nutzung dieser Regel mit Ihrem Classic Load Balancer einen SSL- oder HTTPS-Listener. Hinweis: Diese Regel gilt nur für Classic Load Balancers. Mit dieser Regel werden keine Applicati on Load Balancer oder Network Load Balancer geprüft.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.7.4	Wo Kryptografie zum Schutz gespeicherter Kontodaten eingesetzt wird, werden Schlüsselverwaltungsprozesse und -verfahren, die alle Aspekte des Schlüssellebenszyklus abdecken, definiert und implementiert. (PCI-DSS-v4.0)	acm-pca-root-ca-deaktiviert	Stellen Sie sicher, dass die AWS Private Certificate Authority (AWS Private CA) über eine deaktivierte Stammzertifizierungsstelle verfügt. Die Regel ist NON_COMPLIANT für Root-Benutzer CAs mit einem Status, der nicht DEAKTIVIERT ist.
3.7.4	Wo Kryptografie zum Schutz gespeicherter Kontodaten eingesetzt wird, werden Schlüsselverwaltungsprozesse und -verfahren, die alle Aspekte des Schlüssellebenszyklus abdecken, definiert und implementiert. (PCI-DSS-v4.0)	cloudfront-custom-ssl-certificate	Stellen Sie sicher, dass das mit einer CloudFront Amazon-Distribution verknüpfte Zertifikat nicht das Standard-SSL-Zertifikat ist. Die Regel lautet NON_COMPLIANT, wenn eine CloudFront Distribution das Standard-SSL-Zertifikat verwendet.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.7.4	Wo Kryptografie zum Schutz gespeicherter Kontodaten eingesetzt wird, werden Schlüsselverwaltungsprozesse und -verfahren, die alle Aspekte des Schlüssellebenszyklus abdecken, definiert und implementiert. (PCI-DSS-v4.0)	elb-acm-certificate-required	Stellen Sie sicher, dass die Classic Load Balancers SSL-Zertifikate verwenden, die vom AWS Certificate Manager bereitgestellt werden. Verwenden Sie zur Nutzung dieser Regel mit Ihrem Classic Load Balancer einen SSL- oder HTTPS-Listener. Hinweis: Diese Regel gilt nur für Classic Load Balancers. Mit dieser Regel werden keine Application Load Balancer oder Network Load Balancer geprüft.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.7.6	Wo Kryptografie zum Schutz gespeicherter Kontodaten eingesetzt wird, werden Schlüsselverwaltungsprozesse und -verfahren, die alle Aspekte des Schlüssellebenszyklus abdecken, definiert und implementiert. (PCI-DSS-v4.0)	acm-pca-root-ca-deaktiviert	Stellen Sie sicher, dass die AWS Private Certificate Authority (AWS Private CA) über eine deaktivierte Stammzertifizierungsstelle verfügt. Die Regel ist NON_COMPLIANT für Root-Benutzer CAs mit einem Status, der nicht DEAKTIVIERT ist.
3.7.6	Wo Kryptografie zum Schutz gespeicherter Kontodaten eingesetzt wird, werden Schlüsselverwaltungsprozesse und -verfahren, die alle Aspekte des Schlüssellebenszyklus abdecken, definiert und implementiert. (PCI-DSS-v4.0)	cloudfront-custom-ssl-certificate	Stellen Sie sicher, dass das mit einer CloudFront Amazon-Distribution verknüpfte Zertifikat nicht das Standard-SSL-Zertifikat ist. Die Regel lautet NON_COMPLIANT, wenn eine CloudFront Distribution das Standard-SSL-Zertifikat verwendet.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.7.6	Wo Kryptografie zum Schutz gespeicherter Kontodaten eingesetzt wird, werden Schlüsselverwaltungsprozesse und -verfahren, die alle Aspekte des Schlüssellebenszyklus abdecken, definiert und implementiert. (PCI-DSS-v4.0)	elb-acm-certificate-required	Stellen Sie sicher, dass die Classic Load Balancers SSL-Zertifikate verwenden, die vom AWS Certificate Manager bereitgestellt werden. Verwenden Sie zur Nutzung dieser Regel mit Ihrem Classic Load Balancer einen SSL- oder HTTPS-Listener. Hinweis: Diese Regel gilt nur für Classic Load Balancers. Mit dieser Regel werden keine Application Load Balancer oder Network Load Balancer geprüft.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.7.7	Wo Kryptografie zum Schutz gespeicherter Kontodaten eingesetzt wird, werden wichtige Verwaltungsprozesse und -verfahren, die alle Aspekte des Schlüssel lebenszyklus abdecken, definiert und implementiert. (PCI-DSS-v4.0)	acm-pca-root-ca-deaktiviert	Stellen Sie sicher, dass die AWS Private Certificate Authority (AWS Private CA) über eine deaktivierte Stammzertifizierungsstelle verfügt. Die Regel ist NON_COMPLIANT für Root-Benutzer CAs mit einem Status, der nicht DEAKTIVIERT ist.
3.7.7	Wo Kryptografie zum Schutz gespeicherter Kontodaten eingesetzt wird, werden wichtige Verwaltungsprozesse und -verfahren, die alle Aspekte des Schlüssel lebenszyklus abdecken, definiert und implementiert. (PCI-DSS-v4.0)	cloudfront-custom-ssl-certificate	Stellen Sie sicher, dass das mit einer CloudFront Amazon-Distribution verknüpfte Zertifikat nicht das Standard-SSL-Zertifikat ist. Die Regel lautet NON_COMPLIANT, wenn eine CloudFront Distribution das Standard-SSL-Zertifikat verwendet.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.7.7	Wo Kryptografie zum Schutz gespeicherter Kontodaten eingesetzt wird, werden wichtige Verwaltungsprozess e und -verfahren, die alle Aspekte des Schlüssel lebenszyklus abdecken, definiert und implementiert. (PCI-DSS-v4.0)	elb-acm-certificate-required	Stellen Sie sicher, dass die Classic Load Balancers SSL-Zerti fikate verwenden, die vom AWS Certificate Manager bereitgestellt werden. Verwenden Sie zur Nutzung dieser Regel mit Ihrem Classic Load Balancer einen SSL- oder HTTPS-Listener. Hinweis: Diese Regel gilt nur für Classic Load Balancers. Mit dieser Regel werden keine Applicati on Load Balancer oder Network Load Balancer geprüft.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
4.2.1	PAN ist während der Übertragung mit starker Kryptografie geschützt. (PCI-DSS-v4.0)	dms-redis-tls-enabled	Stellen Sie sicher, dass die Endpunkte des AWS Database Migration Service (AWS DMS) für Redis-Datenspeicher aktiviert sind, sodass die TLS/SSL encryption of data communicated with other endpoints. The rule is NON_COMPLIANT if TLS/SSL Verschlüsselung nicht aktiviert ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
4.2.1	PAN ist während der Übertragung mit starker Kryptografie geschützt. (PCI-DSS-v4.0)	cloudfront-no-deprecated-ssl-protokolle	Stellen Sie sicher, dass CloudFront Distributionen keine veralteten SSL-Protokolle für die HTTPS-Kommunikation zwischen Edge-Standorten und benutzerdefinierten Ursprüngen verwenden . CloudFront Diese Regel ist NON_COMPLIANT für eine CloudFront Verteilung, falls eine Verteilung 'einschließt'. OriginSslProtocols SSLv3

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
4.2.1	PAN ist während der Übertragung mit starker Kryptografie geschützt. (PCI-DSS-v4.0)	cloudfront-traffic-to-origin-verschlüsselt	Stellen Sie sicher, dass CloudFront Amazon-Distributionen den Datenverkehr zu benutzerdefinierten Ursprüngen verschlüsseln. Die Regel lautet NON_COMPLIANT, falls " " " " " " " " für 'nur' HTTP 'ist oder wennOriginProtocolPolicy' 'für' Match-Viewer 'steht und' 'für 'Allow-All' steht. OriginProtocolPolicy ViewerProtocolPolicy
4.2.1	PAN ist während der Übertragung mit starker Kryptografie geschützt. (PCI-DSS-v4.0)	cloudfront-viewer-policy-https	Stellen Sie sicher, dass Ihre CloudFront Amazon-Distributionen HTTPS verwenden (direkt oder über eine Umleitung). Die Regel lautet NON_COMPLIANT, wenn der Wert von auf 'allow-all' für oder für gesetzt ViewerProtocolPolicy ist. DefaultCacheBehavior CacheBehaviors

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
4.2.1	PAN ist während der Übertragung mit starker Kryptografie geschützt. (PCI-DSS-v4.0)	elb-acm-certificate-required	Stellen Sie sicher, dass die Classic Load Balancers SSL-Zerti fikate verwenden, die vom AWS Certificate Manager bereitgestellt werden. Verwenden Sie zur Nutzung dieser Regel mit Ihrem Classic Load Balancer einen SSL- oder HTTPS-Listener. Hinweis: Diese Regel gilt nur für Classic Load Balancers. Mit dieser Regel werden keine Applicati on Load Balancer oder Network Load Balancer geprüft.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
4.2.1	PAN ist während der Übertragung mit starker Kryptografie geschützt. (PCI-DSS-v4.0)	dax-tls-endpoint-encryption	Stellen Sie sicher, dass Ihr Amazon DynamoDB Accelerator (DAX) -Cluster auf TLS ClusterEndpointEncryptionType eingestellt ist. Die Regel lautet NON_COMPLIANT, wenn ein DAX-Cluster nicht mit Transport Layer Security (TLS) verschlüsselt ist.
4.2.1	PAN ist während der Übertragung mit starker Kryptografie geschützt. (PCI-DSS-v4.0)	msk-in-cluster-node-TLS erforderlich	Stellen Sie sicher, dass ein Amazon MSK-Cluster die Verschlüsselung während der Übertragung mithilfe von HTTPS (TLS) mit den Broker-Knoten des Clusters erzwingt. Die Regel ist NON_COMPLIANT, wenn Klartextkommunikation für Broker-Knotenverbindungen in Clustern aktiviert ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
4.2.1	PAN ist während der Übertragung mit starker Kryptografie geschützt. (PCI-DSS-v4.0)	dms-endpoint-ssl-configured	Stellen Sie sicher, dass die Endpunkte des AWS Database Migration Service (AWS DMS) mit einer SSL-Verbindung konfiguriert sind. Die Regel lautet NON_COMPLIANT, wenn für AWS DMS keine SSL-Verbindung konfiguriert ist.
4.2.1.1	PAN ist während der Übertragung durch starke Kryptografie geschützt. (PCI-DSS-v4.0)	acm-pca-root-ca-deaktiviert	Stellen Sie sicher, dass die AWS Private Certificate Authority (AWS Private CA) über eine deaktivierte Stammzertifizierungsstelle verfügt. Die Regel ist NON_COMPLIANT für Root-Benutzer CAs mit einem Status, der nicht DEAKTIVIERT ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
4.2.1.1	PAN ist während der Übertragung durch starke Kryptografie geschützt. (PCI-DSS-v4.0)	cloudfront-custom-ssl-certificate	Stellen Sie sicher, dass das mit einer CloudFront Amazon-Distribution verknüpfte Zertifikat nicht das Standard-SSL-Zertifikat ist. Die Regel lautet NON_COMPLIANT, wenn eine CloudFront Distribution das Standard-SSL-Zertifikat verwendet.
4.2.1.1	PAN ist während der Übertragung durch starke Kryptografie geschützt. (PCI-DSS-v4.0)	dms-redis-tls-enabled	Stellen Sie sicher, dass die Endpunkte des AWS Database Migration Service (AWS DMS) für Redis-Datenspeicher aktiviert sind, sodass die TLS/SSL encryption of data communicated with other endpoints. The rule is NON_COMPLIANT if TLS/SSL Verschlüsselung nicht aktiviert ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
4.2.1.1	PAN ist während der Übertragung durch starke Kryptografie geschützt. (PCI-DSS-v4.0)	cloudfront-no-deprecated-ssl-protokolle	Stellen Sie sicher, dass CloudFront Distributionen keine veralteten SSL-Protokolle für die HTTPS-Kommunikation zwischen Edge-Standorten und benutzerdefinierten Ursprüngen verwenden . CloudFront Diese Regel ist NON_COMPLIANT für eine CloudFront Verteilung, falls eine Verteilung 'einschließt'. OriginSslProtocols SSLv3

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
4.2.1.1	PAN ist während der Übertragung durch starke Kryptografie geschützt. (PCI-DSS-v4.0)	cloudfront-traffic-to-origin-verschlüsselt	Stellen Sie sicher, dass CloudFront Amazon-Distributionen den Datenverkehr zu benutzerdefinierten Ursprüngen verschlüsseln. Die Regel lautet NON_COMPLIANT, falls " " " " " " " " für 'nur' HTTP 'ist oder wennOriginProtocolPolicy' 'für' Match-Viewer 'steht und' 'für 'Allow-All' steht. OriginProtocolPolicy ViewerProtocolPolicy
4.2.1.1	PAN ist während der Übertragung durch starke Kryptografie geschützt. (PCI-DSS-v4.0)	cloudfront-viewer-policy-https	Stellen Sie sicher, dass Ihre CloudFront Amazon-Distributionen HTTPS verwenden (direkt oder über eine Umleitung). Die Regel lautet NON_COMPLIANT, wenn der Wert von auf 'allow-all' für oder für gesetzt ViewerProtocolPolicy ist. DefaultCacheBehavior CacheBehaviors

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
4.2.1.1	PAN ist während der Übertragung durch starke Kryptografie geschützt. (PCI-DSS-v4.0)	elb-acm-certificate-required	Stellen Sie sicher, dass die Classic Load Balancers SSL-Zerti fikate verwenden, die vom AWS Certificate Manager bereitgestellt werden. Verwenden Sie zur Nutzung dieser Regel mit Ihrem Classic Load Balancer einen SSL- oder HTTPS-Listener. Hinweis: Diese Regel gilt nur für Classic Load Balancers. Mit dieser Regel werden keine Applicati on Load Balancer oder Network Load Balancer geprüft.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
4.2.1.1	PAN ist während der Übertragung durch starke Kryptografie geschützt. (PCI-DSS-v4.0)	dax-tls-endpoint-encryption	Stellen Sie sicher, dass Ihr Amazon DynamoDB Accelerator (DAX) -Cluster auf TLS ClusterEndpointEncryptionType eingestellt ist. Die Regel lautet NON_COMPLIANT, wenn ein DAX-Cluster nicht mit Transport Layer Security (TLS) verschlüsselt ist.
4.2.1.1	PAN ist während der Übertragung durch starke Kryptografie geschützt. (PCI-DSS-v4.0)	msk-in-cluster-node-TLS erforderlich	Stellen Sie sicher, dass ein Amazon MSK-Cluster die Verschlüsselung während der Übertragung mithilfe von HTTPS (TLS) mit den Broker-Knoten des Clusters erzwingt. Die Regel ist NON_COMPLIANT, wenn Klartextkommunikation für Broker-Knotenverbindungen in Clustern aktiviert ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
4.2.1.1	PAN ist während der Übertragung durch starke Kryptografie geschützt. (PCI-DSS-v4.0)	dms-endpoint-ssl-configured	Stellen Sie sicher, dass die Endpoints des AWS Database Migration Service (AWS DMS) mit einer SSL-Verbindung konfiguriert sind. Die Regel lautet NON_COMPLIANT, wenn für AWS DMS keine SSL-Verbindung konfiguriert ist.
5.3.4	Anti-Malware-Mechanismen und -Prozesse sind aktiv, werden gewartet und überwacht. (PCI-DSS-v4.0)	api-gwv2- access-logs-enabled	Stellen Sie sicher, dass die Amazon API Gateway V2-Stufen die Zugriffsprotokollierung aktiviert haben. Die Regel ist NON_COMPLIANT, wenn 'accessLogSettings' in der Stage-Konfiguration nicht vorhanden ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
5.3.4	Anti-Malware-Mechanismen und -Prozesse sind aktiv, werden gewartet und überwacht. (PCI-DSS-v4.0)	api-gw-xray-enabled	Stellen Sie sicher, dass AWS X-Ray Tracing auf Amazon API Gateway REST APIs aktiviert ist. Die Regel ist COMPLIANT, wenn die X-Ray-Abl aufverfolgung aktiviert ist, andernfalls ist sie NON_COMPLIANT.
5.3.4	Anti-Malware-Mechanismen und -Prozesse sind aktiv, werden gewartet und überwacht. (PCI-DSS-v4.0)	cloudfront-accesslogs-enabled	Stellen Sie sicher, dass CloudFront Amazon-Distributionen so konfiguriert sind, dass sie Zugriffsprotokolle an einen Amazon S3-Bucket senden. Die Regel lautet NON_COMPLIANT, wenn für eine CloudFront Distribution keine Protokollierung konfiguriert ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
5.3.4	Anti-Malware-Mechanismen und -Prozesse sind aktiv, werden gewartet und überwacht. (PCI-DSS-v4.0)	cloudtrail-security-trail-enabled	Stellen Sie sicher, dass mindestens ein AWS CloudTrail Pfad mit bewährten Sicherheitsmethoden definiert ist. Diese Regel ist COMPLIANT, wenn es mindestens einen Trail gibt, der alle der folgenden Bedingungen erfüllt:
5.3.4	Anti-Malware-Mechanismen und -Prozesse sind aktiv, werden gewartet und überwacht. (PCI-DSS-v4.0)	neptune-cluster-cloudwatch-log-exportfähig	Stellen Sie sicher, dass in einem Amazon Neptune Neptune-Cluster der Protokollexport für CloudWatch Audit-Logs aktiviert ist. Die Regel lautet NON_COMPLIANT, wenn für einen Neptune-Cluster der Protokollexport für CloudWatch Audit-Logs nicht aktiviert ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
5.3.4	Anti-Malware-Mechanismen und -Prozesse sind aktiv, werden gewartet und überwacht. (PCI-DSS-v4.0)	ecs-task-definition-log-Konfiguration	Stellen Sie sicher, dass LogConfiguration für aktive ECS-Aufgabendefinitionen festgelegt ist. Diese Regel ist NON_COMPLIANT, wenn für eine aktive ECSTask Definition die LogConfiguration-Ressource nicht definiert ist oder der Wert für LogConfiguration in mindestens einer Containerdefinition Null ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
5.3.4	Anti-Malware-Mechanismen und -Prozesse sind aktiv, werden gewartet und überwacht. (PCI-DSS-v4.0)	cloudtrail-enabled	Hinweis: Bei dieser Regel untersche iden sich die Regel-ID (CLOUD_TR AIL_ENABLED) und der Regelname (cloudtrail-enabled). Stellen Sie sicher, dass in Ihrem Konto ein Trail aktiviert ist AWS CloudTrail . AWS Die Regel ist NON_COMPLIANT, wenn ein Trail nicht aktiviert ist. Optional überprüft die Regel einen bestimmten S3-Bucket, ein Amazon Simple Notification Service (Amazon SNS) -Thema und eine CloudWatch Protokollgruppe.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
5.3.4	Anti-Malware-Mechanismen und -Prozesse sind aktiv, werden gewartet und überwacht. (PCI-DSS-v4.0)	multi-region-cloudtrail-enabled	Hinweis: Bei dieser Regel untersche iden sich die Regel-ID (MULTI_RE GION_CLOU D_TRAIL_ENABLED) und der Regelname (). multi-region-cloudtrail-enabled Stellen Sie sicher, dass mindesten s eine Region mit mehreren Regionen vorhanden ist. AWS CloudTrail Die Regel ist NON_COMPL IANT, wenn die Trails nicht mit den Eingabeparametern übereinstimmen. Die Regel lautet NON_COMPLIANT, wenn das ExcludeMa nagementEventSourc es Feld nicht leer ist oder wenn sie so konfiguriert AWS CloudTrail ist, dass Verwaltungsereigni sse wie AWS KMS-Ereignisse oder Amazon RDS-Daten -API-Ereignisse

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			ausgeschlossen werden.
5.3.4	Anti-Malware-Mechanismen und -Prozesse sind aktiv, werden gewartet und überwacht. (PCI-DSS-v4.0)	appsync-logging-enabled	Stellen Sie sicher, dass für eine API die Protokollierung aktiviert ist. AWS AppSync Die Regel lautet NON_COMPLIANT, wenn die Protokollierung nicht aktiviert ist, oder 'fieldLogLevel' ist weder ERROR noch ALL.
5.3.4	Anti-Malware-Mechanismen und -Prozesse sind aktiv, werden gewartet und überwacht. (PCI-DSS-v4.0)	waf-classic-logging-enabled	Stellen Sie sicher, dass die Protokollierung auf den AWS WAF Classic Global Web Access Control Lists (Web) aktiviert ist. ACLs Die Regel ist NON_COMPLIANT für eine globale Web-ACL, wenn die Protokollierung nicht aktiviert ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
5.3.4	Anti-Malware-Mechanismen und -Prozesse sind aktiv, werden gewartet und überwacht. (PCI-DSS-v4.0)	mq-cloudwatch-audit-logging-aktiviert	Stellen Sie sicher, dass Amazon MQ-Broker die CloudWatch Amazon-Auditprotokollierung aktiviert haben. Die Regel ist NON_COMPLIANT, wenn für einen Broker die Audit-Protokollierung nicht aktiviert ist.
5.3.4	Anti-Malware-Mechanismen und -Prozesse sind aktiv, werden gewartet und überwacht. (PCI-DSS-v4.0)	mq-cloudwatch-audit-log-aktiviert	Stellen Sie sicher, dass bei einem Amazon MQ-Broker die CloudWatch Auditprotokollierung aktiviert ist. Die Regel lautet NON_COMPLIANT, wenn für den Broker die Audit-Protokollierung nicht aktiviert ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
5.3.4	Anti-Malware-Mechanismen und -Prozesse sind aktiv, werden gewartet und überwacht. (PCI-DSS-v4.0)	eks-cluster-logging-enabled	Stellen Sie sicher, dass ein Amazon Elastic Kubernete s Service (Amazon EKS) -Cluster mit aktivierter Protokoll ierung konfiguriert ist. Die Regel ist NON_COMPLIANT, wenn die Protokoll ierung für Amazon-EKS-Cluster nicht für alle Protokolltypen aktiviert ist.
5.3.4	Anti-Malware-Mechanismen und -Prozesse sind aktiv, werden gewartet und überwacht. (PCI-DSS-v4.0)	elastic-beanstalk-logs-to-Wolkenbeob achtung	Stellen Sie sicher, dass AWS Elastic Beanstalk Beanstalk -Umgebungen so konfiguriert sind, dass sie Protokolle an Amazon CloudWatc h Logs senden. Die Regel lautet NON_COMPLIANT, wenn der Wert von `` StreamLogs falsch ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
5.3.4	Anti-Malware-Mechanismen und -Prozesse sind aktiv, werden gewartet und überwacht. (PCI-DSS-v4.0)	step-functions-state-machine-Protokollierung aktiviert	Stellen Sie sicher, dass auf der AWS Step Functions Functions-Maschine die Protokollierung aktiviert ist Die Regel ist NON_COMPLIANT, wenn für eine Zustandsmaschine die Protokollierung nicht aktiviert ist oder die Protokollierungskonfiguration nicht auf dem angegebenen Mindestniveau liegt.
5.3.4	Anti-Malware-Mechanismen und -Prozesse sind aktiv, werden gewartet und überwacht. (PCI-DSS-v4.0)	netfw-logging-enabled	Stellen Sie sicher, dass die AWS Netzwerk-Firewall-Firewalls die Protokollierung aktiviert haben. Die Regel ist NON_COMPLIANT, wenn kein Protokollierungstyp konfiguriert ist. Sie können angeben, welchen Protokollierungstyp die Regel prüfen soll.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
5.3.4	Anti-Malware-Mechanismen und -Prozesse sind aktiv, werden gewartet und überwacht. (PCI-DSS-v4.0)	cw-loggroup-retention-period-überprüfen	Stellen Sie sicher, dass ein CloudWatch LogGroup Amazon-Aufbewahrungszeitraum auf mehr als 365 Tage oder einen bestimmten Aufbewahrungszeitraum festgelegt ist. Die Regel lautet NON_COMPLIANT, wenn die Aufbewahrungsfrist weniger als MinRetentionTime, falls angegeben, oder andernfalls 365 Tage beträgt.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
6.3.3	Sicherheitslücken werden identifiziert und behoben. (PCI-DSS-v4.0)	lambda-function-settings-check	Stellen Sie sicher, dass die AWS Lambda-Funktionseinstellungen für Laufzeit, Rolle, Timeout und Speichergröße den erwarteten Werten entsprechen. Die Regel ignoriert Funktionen mit dem Pakettyp „Image“ und Funktionen, deren Laufzeit auf „Nur Betriebssystem-Laufzeit“ gesetzt ist. Die Regel ist NON_COMPLIANT, wenn die Einstellungen der Lambda-Funktion nicht den erwarteten Werten entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
6.3.3	Sicherheitslücken werden identifiziert und behoben. (PCI-DSS-v4.0)	eks-cluster-oldest-supported-Ausführung	Stellen Sie sicher, dass auf einem Amazon Elastic Kubernetes Service (EKS) -Cluster nicht die älteste unterstützte Version ausgeführt wird. Die Regel ist NON_COMPLIANT, wenn auf einem EKS-Cluster die älteste unterstützte Version (gleich dem Parameter oldestVersionSupported) ausgeführt wird.
6.4.1	Öffentliche Webanwendungen sind vor Angriffen geschützt. (PCI-DSS-v4.0)	cloudfront-associated-with-waf	Stellen Sie sicher, dass CloudFront Amazon-Distributionen entweder mit Web Application Firewall (WAF) oder WAFv2 Web Access Control Lists (ACLs) verknüpft sind. Die Regel lautet NON_COMPLIANT, wenn eine CloudFront Distribution keiner WAF-Web-ACL zugeordnet ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
6.4.1	Öffentliche Webanwendungen sind vor Angriffen geschützt. (PCI-DSS-v4.0)	appsync-associated-with-waf	Stellen Sie sicher, dass AWS AppSync APIs sie den AWS WAFv2 Web-Zugriffskontrolllisten () zugeordnet sind. ACLs Die Regel ist NON_COMPLIANT für eine AWS AppSync API, wenn sie keiner Web-ACL zugeordnet ist.
6.4.1	Öffentliche Webanwendungen sind vor Angriffen geschützt. (PCI-DSS-v4.0)	WAF 2- webacl-not-empty	Stellen Sie sicher, dass eine WAFv2 Web-ACL alle WAF-Regeln oder WAF-Regelgruppen enthält. Diese Regel ist NON_COMPLIANT, wenn eine Web-ACL keine WAF-Regeln oder WAF-Regelgruppen enthält.
6.4.1	Öffentliche Webanwendungen sind vor Angriffen geschützt. (PCI-DSS-v4.0)	WAF 2- rulegroup-not-empty	Stellen Sie sicher, dass Regelgruppen Regeln enthalten. WAFv2 Die Regel ist NON_COMPLIANT, wenn eine WAFv2 Regelgruppe keine Regeln enthält.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
6.4.1	Öffentliche Webanwendungen sind vor Angriffen geschützt. (PCI-DSS-v4.0)	waf-global-webacl-not-leer	Stellen Sie sicher, dass eine WAF Global Web ACL einige WAF-Regeln oder Regelgruppen enthält. Diese Regel ist NON_COMPLIANT, wenn eine globale Web-ACL keine WAF-Regel oder -Regelgruppe enthält.
6.4.1	Öffentlich zugängliche Webanwendungen sind vor Angriffen geschützt. (PCI-DSS-v4.0)	waf-global-rulegroup-not-leer	Stellen Sie sicher, dass eine AWS WAF Classic-Regelgruppe einige Regeln enthält. Die Regel ist NON_COMPLIANT, wenn innerhalb einer Regelgruppe keine Regeln vorhanden sind.
6.4.1	Öffentlich zugängliche Webanwendungen sind vor Angriffen geschützt. (PCI-DSS-v4.0)	waf-global-rulegroup-not-leer	Stellen Sie sicher, dass eine AWS WAF Classic-Regelgruppe einige Regeln enthält. Die Regel ist NON_COMPLIANT, wenn innerhalb einer Regelgruppe keine Regeln vorhanden sind.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
6.4.1	Öffentlich zugänglic he Webanwendungen sind vor Angriffen geschützt. (PCI-DSS-v4.0)	waf-global-rule-not-leer	Stellen Sie sicher, dass eine globale AWS WAF-Regel einige Bedingungen enthält. Die Regel ist NON_COMPL IANT, wenn in der globalen WAF-Regel keine Bedingungen vorhanden sind.
6.4.2	Öffentlich zugänglic he Webanwendungen sind vor Angriffen geschützt. (PCI-DSS-v4.0)	cloudfront-associated-with-waf	Stellen Sie sicher, dass CloudFront Amazon-Distributio nen entweder mit Web Application Firewall (WAF) oder WAFv2 Web Access Control Lists (ACLs) verknüpft sind. Die Regel lautet NON_COMPLIANT, wenn eine CloudFron t Distribution keiner WAF-Web-ACL zugeordnet ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
6.4.2	Öffentlich zugänglic he Webanwendungen sind vor Angriffen geschützt. (PCI-DSS-v4.0)	appsync-associated-with-waf	Stellen Sie sicher, dass AWS AppSync APIs sie den AWS WAFv2 Web-Zugri ffskontrolllisten () zugeordnet sind. ACLs Die Regel ist NON_COMPL IANT für eine AWS AppSync API, wenn sie keiner Web-ACL zugeordnet ist.
6.4.2	Öffentlich zugänglic he Webanwendungen sind vor Angriffen geschützt. (PCI-DSS-v4.0)	WAF 2- webacl-not-empty	Stellen Sie sicher, dass eine WAFv2 Web-ACL alle WAF-Regeln oder WAF-Regelgruppen enthält. Diese Regel ist NON_COMPLIANT, wenn eine Web-ACL keine WAF-Regel n oder WAF-Regel gruppen enthält.
6.4.2	Öffentlich zugänglic he Webanwendungen sind vor Angriffen geschützt. (PCI-DSS-v4.0)	WAF 2- rulegroup-not-empty	Stellen Sie sicher, dass Regelgruppen Regeln enthalten. WAFv2 Die Regel ist NON_COMPLIANT, wenn eine WAFv2 Regelgruppe keine Regeln enthält.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
6.4.2	Öffentlich zugänglic he Webanwendungen sind vor Angriffen geschützt. (PCI-DSS-v4.0)	waf-global-webacl-not-leer	Stellen Sie sicher, dass eine WAF Global Web ACL einige WAF-Regeln oder Regelgruppen enthält. Diese Regel ist NON_COMPLIANT, wenn eine globale Web-ACL keine WAF-Regel oder -Regelgru ppe enthält.
6.4.2	Öffentlich zugänglic he Webanwendungen sind vor Angriffen geschützt. (PCI-DSS-v4.0)	waf-global-rulegroup-not-leer	Stellen Sie sicher, dass eine AWS WAF Classic-Regelgrupp e einige Regeln enthält. Die Regel ist NON_COMPLIANT, wenn innerhalb einer Regelgruppe keine Regeln vorhanden sind.
6.4.2	Öffentlich zugänglic he Webanwendungen sind vor Angriffen geschützt. (PCI-DSS-v4.0)	waf-global-rulegroup-not-leer	Stellen Sie sicher, dass eine AWS WAF Classic-Regelgrupp e einige Regeln enthält. Die Regel ist NON_COMPLIANT, wenn innerhalb einer Regelgruppe keine Regeln vorhanden sind.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
6.4.2	Öffentlich zugänglic he Webanwendungen sind vor Angriffen geschützt. (PCI-DSS-v4.0)	waf-global-rule-not-leer	Stellen Sie sicher, dass eine globale AWS WAF-Regel einige Bedingungen enthält. Die Regel ist NON_COMPL IANT, wenn in der globalen WAF-Regel keine Bedingungen vorhanden sind.
6.5.5	Änderungen an allen Systemkom ponenten werden sicher verwaltet. (PCI-DSS-v4.0)	codedeploy-lambda-allatonce-traffic-shift-deaktiviert	Stellen Sie sicher, dass die Bereitste llungsgruppe für Lambda Compute Platform nicht die Standardbereitstel lungskonfiguration verwendet. Die Regel lautet NON_COMPL IANT, wenn die Bereitstellungsgruppe die Bereitstellungskon figuration 'verwende t. CodeDeployDefault LambdaAllAtOnce'.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
6.5.5	Änderungen an allen Systemkom ponenten werden sicher verwaltet. (PCI-DSS-v4.0)	codepipeline-deplo yment-count-check	Stellen Sie sicher, dass in der ersten Bereitstellungspha se von mindestens eine Bereitstellung durchgeführt wird. AWS CodePipel ine Dies dient der Überwachung der kontinuierlichen Bereitstellungsakt ivitäten, der Sicherste llung regelmäßi ger Updates und der Identifizierung inaktiver oder nicht ausgelast eter Pipelines, die auf Probleme im Entwicklungs- oder Bereitstellungspro zess hinweisen können. Stellen Sie optional sicher, dass jede der nachfolge nden verbleibenden Phasen für mehr als die angegebene Anzahl von Bereitste llungen (Deployme ntLimit) bereitgestellt wird.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
6.5.6	Änderungen an allen Systemkom ponenten werden sicher verwaltet. (PCI-DSS-v4.0)	codedeploy-lambda-allatonce-traffic-shift-deaktiviert	Stellen Sie sicher, dass die Bereitste llungsgruppe für Lambda Compute Platform nicht die Standardbereitstel lungskonfiguration verwendet. Die Regel lautet NON_COMPL IANT, wenn die Bereitstellungsgruppe die Bereitstellungskon figuration 'verwende t. CodeDeployDefault LambdaAllAtOnce'.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
6.5.6	Änderungen an allen Systemkom ponenten werden sicher verwaltet. (PCI-DSS-v4.0)	codepipeline-deplo yment-count-check	Stellen Sie sicher, dass in der ersten Bereitstellungspha se von mindestens eine Bereitstellung durchgeführt wird. AWS CodePipel ine Dies dient der Überwachung der kontinuierlichen Bereitstellungsakt ivitäten, der Sicherste llung regelmäßi ger Updates und der Identifizierung inaktiver oder nicht ausgelast eter Pipelines, die auf Probleme im Entwicklungs- oder Bereitstellungspro zess hinweisen können. Stellen Sie optional sicher, dass jede der nachfolge nden verbleibenden Phasen für mehr als die angegebene Anzahl von Bereitste llungen (Deployme ntLimit) bereitgestellt wird.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
7.2.1	Der Zugriff auf Systemkomponenten und Daten ist entsprechend definiert und zugewiesen. (PCI-DSS-v4.0)	s-3 bucket-blacklisted-actions-prohibited	Stellen Sie sicher, dass eine Bucket-Richtlinie von Amazon Simple Storage Service (Amazon S3) keine Aktionen auf Bucket- und Objektebene auf Blocklisten für Ressourcen im Bucket für Prinzipale anderer Konten zulässt. AWS Die Regel überprüft beispielsweise, ob die Amazon S3 S3-Bucket-Richtlinie einem anderen AWS Konto nicht erlaubt, s3: GetBucket *-Aktionen und s3: DeleteObject für ein Objekt im Bucket auszuführen. Die Regel ist NON_COMPLIANT, wenn gesperrte Aktionen gemäß der Bucket-Richtlinie von Amazon S3 zulässig sind.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
7.2.1	Der Zugriff auf Systemkomponenten und Daten ist entsprechend definiert und zugewiesen. (PCI-DSS-v4.0)	bucket-policy-not-mores3-permissiv	Stellen Sie sicher, dass Ihre Amazon Simple Storage Service (S3) -Bucket-Richtlinien keine anderen Kontobere chtigungen zulassen als die von Ihnen Amazon S3 S3-Bucket-Kontrollrichtlini e.
7.2.1	Der Zugriff auf Systemkomponenten und Daten ist entsprechend definiert und zugewiesen. (PCI-DSS-v4.0)	shield-drt-access	Stellen Sie sicher, dass das Shield Response Team (SRT) auf Ihr AWS Konto zugreifen kann. Die Regel lautet NON_COMPLIANT, wenn AWS Shield Advanced aktiviert ist, die Rolle für den SRT-Zugriff jedoch nicht konfiguriert ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
7.2.1	Der Zugriff auf Systemkomponenten und Daten ist entsprechend definiert und zugewiesen. (PCI-DSS-v4.0)	iam-policy-in-use	Stellen Sie sicher, dass ein IAM-Richt linien-ARN einem IAM-Benutzer oder einer Gruppe mit einem oder mehreren IAM-Benutzern oder einer IAM-Rolle mit einer oder mehreren vertrauenswürdigen Entitäten zugewiesen ist.
7.2.1	Der Zugriff auf Systemkomponenten und Daten ist angemessen definiert und zugewiesen. (PCI-DSS-v4.0)	neptune-cluster-ia m-database-Authent ifizierung	Stellen Sie sicher, dass für einen Amazon Neptune Neptune-Cluster die AWS Identity and Access Managemen t (IAM) -Datenban kauthentifizierung aktiviert ist. Die Regel ist NON_COMPL IANT, wenn für einen Amazon-Neptune-Clu ster die IAM-Daten bankauthentifizierung nicht aktiviert ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
7.2.1	Der Zugriff auf Systemkomponenten und Daten ist entsprechend definiert und zugewiesen. (PCI-DSS-v4.0)	rds-cluster-iam-authentication-aktiviert	Stellen Sie sicher, dass für einen Amazon Relational Database Service (Amazon RDS) - Cluster die AWS Identity and Access Management (IAM) -Authentifizierung aktiviert ist. Die Regel ist NON_COMPLIANT, wenn für einen Amazon-RDS-Cluster die IAM-Authentifizierung nicht aktiviert ist.
7.2.1	Der Zugriff auf Systemkomponenten und Daten ist entsprechend definiert und zugewiesen. (PCI-DSS-v4.0)	ec2- instance-profile-attached	Stellen Sie sicher, dass an eine EC2 Instanz ein AWS Identity and Access Management (IAM) -Profil angehängt ist. Die Regel lautet NON_COMPLIANT, wenn der Instanz kein IAM-Profil angehängt ist. EC2

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
7.2.1	Der Zugriff auf Systemkomponenten und Daten ist entsprechend definiert und zugewiesen. (PCI-DSS-v4.0)	backup-recovery-point-manual-Löschen-deaktiviert	Stellen Sie sicher, dass einem Backup-Tresor eine ressourcenbasierte Richtlinie zugeordnet ist, die das Löschen von Wiederherstellungspunkten verhindert. Die Regel lautet NON_COMPLIANT, wenn der Backup-Tresor keine ressourcenbasierten Richtlinien oder Richtlinien ohne eine geeignete „Deny“ -Anweisung (Anweisung mit den Berechtigungen backup:DeleteRecoveryPoint, backup: und backup:UpdateRecoveryPointLifecycle) hat. PutBackupVaultAccessPolicy

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
7.2.1	Der Zugriff auf Systemkomponenten und Daten ist entsprechend definiert und zugewiesen. (PCI-DSS-v4.0)	rds-instance-iam-authentication-aktiviert	Stellen Sie sicher, dass für eine Amazon Relational Database Service (Amazon RDS) -Instance die AWS Identity and Access Management (IAM) -Authentifizierung aktiviert ist. Die Regel ist NON_COMPLIANT, wenn für eine Amazon-RDS-Instance die IAM-Authentifizierung nicht aktiviert ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
7.2.2	Der Zugriff auf Systemkomponenten und Daten ist entsprechend definiert und zugewiesen. (PCI-DSS-v4.0)	s-3 bucket-blacklisted-actions-prohibited	Stellen Sie sicher, dass eine Bucket-Richtlinie von Amazon Simple Storage Service (Amazon S3) keine Aktionen auf Bucket- und Objektebene auf Blocklisten für Ressourcen im Bucket für Prinzipale anderer Konten zulässt. AWS Die Regel überprüft beispielsweise, ob die Amazon S3 S3-Bucket-Richtlinie einem anderen AWS Konto nicht erlaubt, s3: GetBucket *-Aktionen und s3: DeleteObject für ein Objekt im Bucket auszuführen. Die Regel ist NON_COMPLIANT, wenn gesperrte Aktionen gemäß der Bucket-Richtlinie von Amazon S3 zulässig sind.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
7.2.2	Der Zugriff auf Systemkomponenten und Daten ist entsprechend definiert und zugewiesen. (PCI-DSS-v4.0)	bucket-policy-not-mores3-permissiv	Stellen Sie sicher, dass Ihre Amazon Simple Storage Service (S3) -Bucket-Richtlinien keine anderen Kontobere chtigungen zulassen als die von Ihnen Amazon S3 S3-Bucket-Kontrollrichtlini e.
7.2.2	Der Zugriff auf Systemkomponenten und Daten ist entsprechend definiert und zugewiesen. (PCI-DSS-v4.0)	shield-drt-access	Stellen Sie sicher, dass das Shield Response Team (SRT) auf Ihr AWS Konto zugreifen kann. Die Regel lautet NON_COMPLIANT, wenn AWS Shield Advanced aktiviert ist, die Rolle für den SRT-Zugriff jedoch nicht konfiguriert ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
7.2.2	Der Zugriff auf Systemkomponenten und Daten ist entsprechend definiert und zugewiesen. (PCI-DSS-v4.0)	iam-policy-in-use	Stellen Sie sicher, dass ein IAM-Richtlinien-ARN einem IAM-Benutzer oder einer Gruppe mit einem oder mehreren IAM-Benutzern oder einer IAM-Rolle mit einer oder mehreren vertrauenswürdigen Entitäten zugewiesen ist.
7.2.2	Der Zugriff auf Systemkomponenten und Daten ist angemessen definiert und zugewiesen. (PCI-DSS-v4.0)	neptune-cluster-iam-database-Authentifizierung	Stellen Sie sicher, dass für einen Amazon Neptune Neptune-Cluster die AWS Identity and Access Management (IAM) -Datenbankauthentifizierung aktiviert ist. Die Regel ist NON_COMPLIANT, wenn für einen Amazon-Neptune-Cluster die IAM-Datenbankauthentifizierung nicht aktiviert ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
7.2.2	Der Zugriff auf Systemkomponenten und Daten ist entsprechend definiert und zugewiesen. (PCI-DSS-v4.0)	rds-cluster-iam-authentication-aktiviert	Stellen Sie sicher, dass für einen Amazon Relational Database Service (Amazon RDS) -Cluster die AWS Identity and Access Management (IAM) -Authentifizierung aktiviert ist. Die Regel ist NON_COMPLIANT, wenn für einen Amazon-RDS-Cluster die IAM-Authentifizierung nicht aktiviert ist.
7.2.2	Der Zugriff auf Systemkomponenten und Daten ist entsprechend definiert und zugewiesen. (PCI-DSS-v4.0)	ec2- instance-profile-attached	Stellen Sie sicher, dass an eine EC2 Instanz ein AWS Identity and Access Management (IAM) -Profil angehängt ist. Die Regel lautet NON_COMPLIANT, wenn der Instanz kein IAM-Profil angehängt ist. EC2

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
7.2.2	Der Zugriff auf Systemkomponenten und Daten ist entsprechend definiert und zugewiesen. (PCI-DSS-v4.0)	backup-recovery-point-manual-Löschen-deaktiviert	Stellen Sie sicher, dass einem Backup-Tresor eine ressourcenbasierte Richtlinie zugeordnet ist, die das Löschen von Wiederherstellungspunkten verhindert. Die Regel lautet NON_COMPLIANT, wenn der Backup-Tresor keine ressourcenbasierten Richtlinien oder Richtlinien ohne eine geeignete „Deny“ -Anweisung (Anweisung mit den Berechtigungen backup:DeleteRecoveryPoint, backup: und backup:UpdateRecoveryPointLifecycle) hat. PutBackupVaultAccessPolicy

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
7.2.2	Der Zugriff auf Systemkomponenten und Daten ist entsprechend definiert und zugewiesen. (PCI-DSS-v4.0)	rds-instance-iam-authentication-aktiviert	Stellen Sie sicher, dass für eine Amazon Relational Database Service (Amazon RDS) -Instance die AWS Identity and Access Management (IAM) -Authentifizierung aktiviert ist. Die Regel ist NON_COMPLIANT, wenn für eine Amazon-RDS-Instance die IAM-Authentifizierung nicht aktiviert ist.
7.2.4	Der Zugriff auf Systemkomponenten und Daten ist entsprechend definiert und zugewiesen. (PCI-DSS-v4.0)	secretsmanager-secret-unused	Stellen Sie sicher, dass auf AWS Secrets Manager-Geheimnisse innerhalb einer bestimmten Anzahl von Tagen zugegriffen wurde. Die Regel lautet NON_COMPLIANT, wenn innerhalb von 'unusedForDays' Tagen nicht auf ein Geheimnis zugegriffen wurde. Der Standardwert lautet 90 Tage.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
7.2.5	Der Zugriff auf Systemkomponenten und Daten ist entsprechend definiert und zugewiesen. (PCI-DSS-v4.0)	s-3 bucket-blacklisted-actions-prohibited	Stellen Sie sicher, dass eine Bucket-Richtlinie von Amazon Simple Storage Service (Amazon S3) keine Aktionen auf Bucket- und Objektebene auf Blocklisten für Ressourcen im Bucket für Prinzipale anderer Konten zulässt. AWS Die Regel überprüft beispielsweise, ob die Amazon S3 S3-Bucket-Richtlinie einem anderen AWS Konto nicht erlaubt, s3: GetBucket *-Aktionen und s3: DeleteObject für ein Objekt im Bucket auszuführen. Die Regel ist NON_COMPLIANT, wenn gesperrte Aktionen gemäß der Bucket-Richtlinie von Amazon S3 zulässig sind.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
7.2.5	Der Zugriff auf Systemkomponenten und Daten ist entsprechend definiert und zugewiesen. (PCI-DSS-v4.0)	bucket-policy-not-mores3-permissiv	Stellen Sie sicher, dass Ihre Amazon Simple Storage Service (S3) -Bucket-Richtlinien keine anderen Kontobere chtigungen zulassen als die von Ihnen Amazon S3 S3-Bucket-Kontrollrichtlini e.
7.2.5	Der Zugriff auf Systemkomponenten und Daten ist entsprechend definiert und zugewiesen. (PCI-DSS-v4.0)	shield-drt-access	Stellen Sie sicher, dass das Shield Response Team (SRT) auf Ihr AWS Konto zugreifen kann. Die Regel lautet NON_COMPLIANT, wenn AWS Shield Advanced aktiviert ist, die Rolle für den SRT-Zugriff jedoch nicht konfiguriert ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
7.2.5	Der Zugriff auf Systemkomponenten und Daten ist entsprechend definiert und zugewiesen. (PCI-DSS-v4.0)	iam-policy-in-use	Stellen Sie sicher, dass ein IAM-Richt linien-ARN einem IAM-Benutzer oder einer Gruppe mit einem oder mehreren IAM-Benutzern oder einer IAM-Rolle mit einer oder mehreren vertrauenswürdigen Entitäten zugewiesen ist.
7.2.5	Der Zugriff auf Systemkomponenten und Daten ist angemessen definiert und zugewiesen. (PCI-DSS-v4.0)	neptune-cluster-ia m-database-Authent ifizierung	Stellen Sie sicher, dass für einen Amazon Neptune Neptune-Cluster die AWS Identity and Access Managemen t (IAM) -Datenban kauthentifizierung aktiviert ist. Die Regel ist NON_COMPL IANT, wenn für einen Amazon-Neptune-Clu ster die IAM-Daten bankauthentifizierung nicht aktiviert ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
7.2.5	Der Zugriff auf Systemkomponenten und Daten ist entsprechend definiert und zugewiesen. (PCI-DSS-v4.0)	rds-cluster-iam-authentication-aktiviert	Stellen Sie sicher, dass für einen Amazon Relational Database Service (Amazon RDS) -Cluster die AWS Identity and Access Management (IAM) -Authentifizierung aktiviert ist. Die Regel ist NON_COMPLIANT, wenn für einen Amazon-RDS-Cluster die IAM-Authentifizierung nicht aktiviert ist.
7.2.5	Der Zugriff auf Systemkomponenten und Daten ist entsprechend definiert und zugewiesen. (PCI-DSS-v4.0)	ec2- instance-profile-attached	Stellen Sie sicher, dass an eine EC2 Instanz ein AWS Identity and Access Management (IAM) -Profil angehängt ist. Die Regel lautet NON_COMPLIANT, wenn der Instanz kein IAM-Profil angehängt ist. EC2

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
7.2.5	Der Zugriff auf Systemkomponenten und Daten ist entsprechend definiert und zugewiesen. (PCI-DSS-v4.0)	backup-recovery-point-manual-Löschen-deaktiviert	Stellen Sie sicher, dass einem Backup-Tresor eine ressourcenbasierte Richtlinie zugeordnet ist, die das Löschen von Wiederherstellungspunkten verhindert. Die Regel lautet NON_COMPLIANT, wenn der Backup-Tresor keine ressourcenbasierten Richtlinien oder Richtlinien ohne eine geeignete „Deny“ -Anweisung (Anweisung mit den Berechtigungen backup:DeleteRecoveryPoint, backup: und backup:UpdateRecoveryPointLifecycle) hat. PutBackupVaultAccessPolicy

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
7.2.5	Der Zugriff auf Systemkomponenten und Daten ist entsprechend definiert und zugewiesen. (PCI-DSS-v4.0)	rds-instance-iam-authentication-aktiviert	Stellen Sie sicher, dass für eine Amazon Relational Database Service (Amazon RDS) -Instance die AWS Identity and Access Management (IAM) -Authentifizierung aktiviert ist. Die Regel ist NON_COMPLIANT, wenn für eine Amazon-RDS-Instance die IAM-Authentifizierung nicht aktiviert ist.
7.2.5.1	Der Zugriff auf Systemkomponenten und Daten ist entsprechend definiert und zugewiesen. (PCI-DSS-v4.0)	secretsmanager-secret-unused	Stellen Sie sicher, dass auf AWS Secrets Manager-Geheimnisse innerhalb einer bestimmten Anzahl von Tagen zugegriffen wurde. Die Regel lautet NON_COMPLIANT, wenn innerhalb von 'unusedForDays' Tagen nicht auf ein Geheimnis zugegriffen wurde. Der Standardwert lautet 90 Tage.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
7.2.6	Der Zugriff auf Systemkomponenten und Daten ist angemessen definiert und zugewiesen. (PCI-DSS-v4.0)	s-3 bucket-blacklisted-actions-prohibited	Stellen Sie sicher, dass eine Bucket-Richtlinie von Amazon Simple Storage Service (Amazon S3) keine Aktionen auf Bucket- und Objektebene auf Blocklisten für Ressourcen im Bucket für Prinzipale anderer Konten zulässt. AWS Die Regel überprüft beispielsweise, ob die Amazon S3 S3-Bucket-Richtlinie einem anderen AWS Konto nicht erlaubt, s3: GetBucket *-Aktionen und s3: DeleteObject für ein Objekt im Bucket auszuführen. Die Regel ist NON_COMPLIANT, wenn gesperrte Aktionen gemäß der Bucket-Richtlinie von Amazon S3 zulässig sind.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
7.2.6	Der Zugriff auf Systemkomponenten und Daten ist angemessen definiert und zugewiesen. (PCI-DSS-v4.0)	bucket-policy-not-mores3-permissiv	Stellen Sie sicher, dass Ihre Amazon Simple Storage Service (S3) -Bucket-Richtlinien keine anderen Kontobere chtigungen zulassen als die von Ihnen Amazon S3 S3-Bucket-Kontrollrichtlini e.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
7.3.1	Der Zugriff auf Systemkomponenten und Daten wird über ein oder mehrere Zugriffskontrollsysteme verwaltet. (PCI-DSS-v4.0)	s-3 bucket-blacklisted-actions-prohibited	Stellen Sie sicher, dass eine Bucket-Richtlinie von Amazon Simple Storage Service (Amazon S3) keine Aktionen auf Bucket- und Objektebene auf Blocklisten für Ressourcen im Bucket für Prinzipale anderer Konten zulässt. AWS Die Regel überprüft beispielsweise, ob die Amazon S3 S3-Bucket-Richtlinie einem anderen AWS Konto nicht erlaubt, s3: GetBucket *-Aktionen und s3: DeleteObject für ein Objekt im Bucket auszuführen. Die Regel ist NON_COMPLIANT, wenn gesperrte Aktionen gemäß der Bucket-Richtlinie von Amazon S3 zulässig sind.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
7.3.1	Der Zugriff auf Systemkomponenten und Daten wird über ein oder mehrere Zugriffskontrollsy steme verwaltet. (PCI-DSS-v4.0)	bucket-policy-not-mores3-permissiv	Stellen Sie sicher, dass Ihre Amazon Simple Storage Service (S3) -Bucket-Richtlinien keine anderen Kontobere chtigungen zulassen als die von Ihnen Amazon S3 S3-Bucket-Kontrollrichtlini e.
7.3.1	Der Zugriff auf Systemkomponenten und Daten wird über ein oder mehrere Zugriffskontrollsy steme verwaltet. (PCI-DSS-v4.0)	shield-drt-access	Stellen Sie sicher, dass das Shield Response Team (SRT) auf Ihr AWS Konto zugreifen kann. Die Regel lautet NON_COMPLIANT, wenn AWS Shield Advanced aktiviert ist, die Rolle für den SRT-Zugriff jedoch nicht konfiguriert ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
7.3.1	Der Zugriff auf Systemkomponenten und Daten wird über ein oder mehrere Zugriffskontrollsysteme verwaltet. (PCI-DSS-v4.0)	iam-policy-in-use	Stellen Sie sicher, dass ein IAM-Richtlinien-ARN einem IAM-Benutzer oder einer Gruppe mit einem oder mehreren IAM-Benutzern oder einer IAM-Rolle mit einer oder mehreren vertrauenswürdigen Entitäten zugewiesen ist.
7.3.1	Der Zugriff auf Systemkomponenten und Daten wird über ein oder mehrere Zugriffskontrollsysteme verwaltet. (PCI-DSS-v4.0)	neptune-cluster-iam-database-Authentifizierung	Stellen Sie sicher, dass für einen Amazon Neptune Neptune-Cluster die AWS Identity and Access Management (IAM) -Datenbankauthentifizierung aktiviert ist. Die Regel ist NON_COMPLIANT, wenn für einen Amazon-Neptune-Cluster die IAM-Datenbankauthentifizierung nicht aktiviert ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
7.3.1	Der Zugriff auf Systemkomponenten und Daten wird über ein oder mehrere Zugriffskontrollsysteme verwaltet. (PCI-DSS-v4.0)	rds-cluster-iam-authentication-aktiviert	Stellen Sie sicher, dass für einen Amazon Relational Database Service (Amazon RDS) -Cluster die AWS Identity and Access Management (IAM) -Authentifizierung aktiviert ist. Die Regel ist NON_COMPLIANT, wenn für einen Amazon-RDS-Cluster die IAM-Authentifizierung nicht aktiviert ist.
7.3.1	Der Zugriff auf Systemkomponenten und Daten wird über ein oder mehrere Zugriffskontrollsysteme verwaltet. (PCI-DSS-v4.0)	ec2- instance-profile-attached	Stellen Sie sicher, dass an eine EC2 Instanz ein AWS Identity and Access Management (IAM) -Profil angehängt ist. Die Regel lautet NON_COMPLIANT, wenn der Instanz kein IAM-Profil angehängt ist. EC2

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
7.3.1	Der Zugriff auf Systemkomponenten und Daten wird über ein oder mehrere Zugriffskontrollsysteme verwaltet. (PCI-DSS-v4.0)	backup-recovery-point-manual-Löschen-deaktiviert	Stellen Sie sicher, dass einem Backup-Tresor eine ressourcenbasierte Richtlinie zugeordnet ist, die das Löschen von Wiederherstellungspunkten verhindert. Die Regel lautet NON_COMPLIANT, wenn der Backup-Tresor keine ressourcenbasierten Richtlinien oder Richtlinien ohne eine geeignete „Deny“ -Anweisung (Anweisung mit den Berechtigungen backup:DeleteRecoveryPoint, backup: und backup:UpdateRecoveryPointLifecycle) hat. PutBackupVaultAccessPolicy

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
7.3.1	Der Zugriff auf Systemkomponenten und Daten wird über ein oder mehrere Zugriffskontrollsysteme verwaltet. (PCI-DSS-v4.0)	rds-instance-iam-authentication-aktiviert	Stellen Sie sicher, dass für eine Amazon Relational Database Service (Amazon RDS) -Instance die AWS Identity and Access Management (IAM) -Authentifizierung aktiviert ist. Die Regel ist NON_COMPLIANT, wenn für eine Amazon-RDS-Instance die IAM-Authentifizierung nicht aktiviert ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
7.3.2	Der Zugriff auf Systemkomponenten und Daten wird über ein oder mehrere Zugriffskontrollsysteme verwaltet. (PCI-DSS-v4.0)	s-3 bucket-blacklisted-actions-prohibited	Stellen Sie sicher, dass eine Bucket-Richtlinie von Amazon Simple Storage Service (Amazon S3) keine Aktionen auf Bucket- und Objektebene auf Blocklisten für Ressourcen im Bucket für Prinzipale anderer Konten zulässt. AWS Die Regel überprüft beispielsweise, ob die Amazon S3 S3-Bucket-Richtlinie einem anderen AWS Konto nicht erlaubt, s3: GetBucket *-Aktionen und s3: DeleteObject für ein Objekt im Bucket auszuführen. Die Regel ist NON_COMPLIANT, wenn gesperrte Aktionen gemäß der Bucket-Richtlinie von Amazon S3 zulässig sind.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
7.3.2	Der Zugriff auf Systemkomponenten und Daten wird über ein oder mehrere Zugriffskontrollsy steme verwaltet. (PCI-DSS-v4.0)	bucket-policy-not-mores3-permissiv	Stellen Sie sicher, dass Ihre Amazon Simple Storage Service (S3) -Bucket-Richtlinien keine anderen Kontobere chtigungen zulassen als die von Ihnen Amazon S3 S3-Bucket-Kontrollrichtlini e.
7.3.2	Der Zugriff auf Systemkomponenten und Daten wird über ein oder mehrere Zugriffskontrollsy steme verwaltet. (PCI-DSS-v4.0)	shield-drt-access	Stellen Sie sicher, dass das Shield Response Team (SRT) auf Ihr AWS Konto zugreifen kann. Die Regel lautet NON_COMPLIANT, wenn AWS Shield Advanced aktiviert ist, die Rolle für den SRT-Zugriff jedoch nicht konfiguriert ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
7.3.2	Der Zugriff auf Systemkomponenten und Daten wird über ein oder mehrere Zugriffskontrollsysteme verwaltet. (PCI-DSS-v4.0)	iam-policy-in-use	Stellen Sie sicher, dass ein IAM-Richtlinien-ARN einem IAM-Benutzer oder einer Gruppe mit einem oder mehreren IAM-Benutzern oder einer IAM-Rolle mit einer oder mehreren vertrauenswürdigen Entitäten zugewiesen ist.
7.3.2	Der Zugriff auf Systemkomponenten und Daten wird über ein oder mehrere Zugriffskontrollsysteme verwaltet. (PCI-DSS-v4.0)	neptune-cluster-iam-database-Authentifizierung	Stellen Sie sicher, dass für einen Amazon Neptune Neptune-Cluster die AWS Identity and Access Management (IAM) -Datenbankauthentifizierung aktiviert ist. Die Regel ist NON_COMPLIANT, wenn für einen Amazon-Neptune-Cluster die IAM-Datenbankauthentifizierung nicht aktiviert ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
7.3.2	Der Zugriff auf Systemkomponenten und Daten wird über ein oder mehrere Zugriffskontrollsysteme verwaltet. (PCI-DSS-v4.0)	rds-cluster-iam-authentication-aktiviert	Stellen Sie sicher, dass für einen Amazon Relational Database Service (Amazon RDS) -Cluster die AWS Identity and Access Management (IAM) -Authentifizierung aktiviert ist. Die Regel ist NON_COMPLIANT, wenn für einen Amazon-RDS-Cluster die IAM-Authentifizierung nicht aktiviert ist.
7.3.2	Der Zugriff auf Systemkomponenten und Daten wird über ein oder mehrere Zugriffskontrollsysteme verwaltet. (PCI-DSS-v4.0)	ec2- instance-profile-attached	Stellen Sie sicher, dass an eine EC2 Instanz ein AWS Identity and Access Management (IAM) -Profil angehängt ist. Die Regel lautet NON_COMPLIANT, wenn der Instanz kein IAM-Profil angehängt ist. EC2

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
7.3.2	Der Zugriff auf Systemkomponenten und Daten wird über ein oder mehrere Zugriffskontrollsysteme verwaltet. (PCI-DSS-v4.0)	backup-recovery-point-manual-Löschen-deaktiviert	Stellen Sie sicher, dass einem Backup-Tresor eine ressourcenbasierte Richtlinie zugeordnet ist, die das Löschen von Wiederherstellungspunkten verhindert. Die Regel lautet NON_COMPLIANT, wenn der Backup-Tresor keine ressourcenbasierten Richtlinien oder Richtlinien ohne eine geeignete „Deny“ -Anweisung (Anweisung mit den Berechtigungen backup:DeleteRecoveryPoint, backup: und backup:UpdateRecoveryPointLifecycle) hat. PutBackupVaultAccessPolicy

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
7.3.2	Der Zugriff auf Systemkomponenten und Daten wird über ein oder mehrere Zugriffskontrollsysteme verwaltet. (PCI-DSS-v4.0)	rds-instance-iam-authentication-aktiviert	Stellen Sie sicher, dass für eine Amazon Relational Database Service (Amazon RDS) -Instance die AWS Identity and Access Management (IAM) -Authentifizierung aktiviert ist. Die Regel ist NON_COMPLIANT, wenn für eine Amazon-RDS-Instance die IAM-Authentifizierung nicht aktiviert ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
7.3.3	Der Zugriff auf Systemkomponenten und Daten wird über ein oder mehrere Zugangskontrollsys teme verwaltet. (PCI-DSS-v4.0)	s-3 bucket-blacklisted-actions-prohibited	Stellen Sie sicher, dass eine Bucket-Richtlinie von Amazon Simple Storage Service (Amazon S3) keine Aktionen auf Bucket- und Objektebene auf Blocklisten für Ressourcen im Bucket für Prinzipale anderer Konten zulässt. AWS Die Regel überprüft beispielsweise, ob die Amazon S3 S3-Bucket-Richtlinie einem anderen AWS Konto nicht erlaubt, s3: GetBucket *-Aktionen und s3: DeleteObject für ein Objekt im Bucket auszuführen. Die Regel ist NON_COMPLIANT, wenn gesperrte Aktionen gemäß der Bucket-Richtlinie von Amazon S3 zulässig sind.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
7.3.3	Der Zugriff auf Systemkomponenten und Daten wird über ein oder mehrere Zugangskontrollsys teme verwaltet. (PCI-DSS-v4.0)	bucket-policy-not-mores3-permissiv	Stellen Sie sicher, dass Ihre Amazon Simple Storage Service (S3) -Bucket-Richtlinien keine anderen Kontobere chtigungen zulassen als die von Ihnen Amazon S3 S3-Bucket-Kontrollrichtlini e.
7.3.3	Der Zugriff auf Systemkomponenten und Daten wird über ein oder mehrere Zugangskontrollsys teme verwaltet. (PCI-DSS-v4.0)	shield-drt-access	Stellen Sie sicher, dass das Shield Response Team (SRT) auf Ihr AWS Konto zugreifen kann. Die Regel lautet NON_COMPLIANT, wenn AWS Shield Advanced aktiviert ist, die Rolle für den SRT-Zugriff jedoch nicht konfiguriert ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
7.3.3	Der Zugriff auf Systemkomponenten und Daten wird über ein oder mehrere Zugangskontrollsys teme verwaltet. (PCI-DSS-v4.0)	iam-policy-in-use	Stellen Sie sicher, dass ein IAM-Richt linien-ARN einem IAM-Benutzer oder einer Gruppe mit einem oder mehreren IAM-Benutzern oder einer IAM-Rolle mit einer oder mehreren vertrauenswürdigen Entitäten zugewiesen ist.
7.3.3	Der Zugriff auf Systemkomponenten und Daten wird über ein oder mehrere Zugangskontrollsys teme verwaltet. (PCI-DSS-v4.0)	neptune-cluster-ia m-database-Authent ifizierung	Stellen Sie sicher, dass für einen Amazon Neptune Neptune-Cluster die AWS Identity and Access Managemen t (IAM) -Datenban kauthentifizierung aktiviert ist. Die Regel ist NON_COMPL IANT, wenn für einen Amazon-Neptune-Clu ster die IAM-Daten bankauthentifizierung nicht aktiviert ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
7.3.3	Der Zugriff auf Systemkomponenten und Daten wird über ein oder mehrere Zugangskontrollsysteme verwaltet. (PCI-DSS-v4.0)	rds-cluster-iam-authentication-aktiviert	Stellen Sie sicher, dass für einen Amazon Relational Database Service (Amazon RDS) -Cluster die AWS Identity and Access Management (IAM) -Authentifizierung aktiviert ist. Die Regel ist NON_COMPLIANT, wenn für einen Amazon-RDS-Cluster die IAM-Authentifizierung nicht aktiviert ist.
7.3.3	Der Zugriff auf Systemkomponenten und Daten wird über ein oder mehrere Zugangskontrollsysteme verwaltet. (PCI-DSS-v4.0)	ec2- instance-profile-attached	Stellen Sie sicher, dass an eine EC2 Instanz ein AWS Identity and Access Management (IAM) -Profil angehängt ist. Die Regel lautet NON_COMPLIANT, wenn der Instanz kein IAM-Profil angehängt ist. EC2

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
7.3.3	Der Zugriff auf Systemkomponenten und Daten wird über ein oder mehrere Zugangskontrollsys teme verwaltet. (PCI-DSS-v4.0)	backup-recovery-point-manual-Löschen-deaktiviert	Stellen Sie sicher, dass einem Backup-Tresor eine ressource nbasierte Richtlinie zugeordnet ist, die das Löschen von Wiederherstellungs punkten verhinder t. Die Regel lautet NON_COMPLIANT, wenn der Backup-Tr esor keine ressource nbasierten Richtlini en oder Richtlinien ohne eine geeignete „Deny“ -Anweisun g (Anweisung mit den Berechtigungen backup:DeleteRecov eryPoint, backup: und backup:UpdateRecov eryPointLifecycle) hat. PutBackupVaultAcce ssPolicy

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
7.3.3	Der Zugriff auf Systemkomponenten und Daten wird über ein oder mehrere Zugangskontrollsysteme verwaltet. (PCI-DSS-v4.0)	rds-instance-iam-authentication-aktiviert	Stellen Sie sicher, dass für eine Amazon Relational Database Service (Amazon RDS) -Instance die AWS Identity and Access Management (IAM) -Authentifizierung aktiviert ist. Die Regel ist NON_COMPLIANT, wenn für eine Amazon-RDS-Instance die IAM-Authentifizierung nicht aktiviert ist.
8.2.1	Die Benutzeridentifikation und die zugehörigen Konten für Benutzer und Administratoren werden während des gesamten Kontolebenszyklus streng verwaltet. (PCI-DSS-v4.0)	iam-policy-in-use	Stellen Sie sicher, dass ein IAM-Richtlinien-ARN einem IAM-Benutzer oder einer Gruppe mit einem oder mehreren IAM-Benutzern oder einer IAM-Rolle mit einer oder mehreren vertrauenswürdigen Entitäten zugewiesen ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
8.2.1	Die Benutzeri dentifikation und die zugehörigen Konten für Benutzer und Administratoren werden während des gesamten Kontolebe nszyklus strikt verwaltet. (PCI-DSS-v4.0)	ec2- no-amazon-key-pair	Stellen Sie sicher, dass laufende Amazon Elastic Compute Cloud (EC2) -Instances nicht mit Amazon-Schlüsselpaaren gestartet werden. Die Regel lautet NON_COMPLIANT, wenn eine laufende EC2 Instance mit einem key pair gestartet wird.
8.2.2	Die Benutzeri dentifikation und die zugehörigen Konten für Benutzer und Administratoren werden während des gesamten Lebenszyk lus eines Kontos streng verwaltet. (PCI-DSS-v4.0)	iam-policy-in-use	Stellen Sie sicher, dass ein IAM-Richt linien-ARN einem IAM-Benutzer oder einer Gruppe mit einem oder mehreren IAM-Benutzern oder einer IAM-Rolle mit einer oder mehreren vertrauenswürdigen Entitäten zugewiesen ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
8.2.2	Die Benutzeri dentifikation und die zugehörigen Konten für Benutzer und Administratoren werden während des gesamten Lebenszyk lus eines Kontos streng verwaltet. (PCI-DSS-v4.0)	ec2- no-amazon-key-pair	Stellen Sie sicher, dass laufende Amazon Elastic Compute Cloud (EC2) -Instances nicht mit Amazon-Schlüsselpaaren gestartet werden. Die Regel lautet NON_COMPLIANT, wenn eine laufende EC2 Instance mit einem key pair gestartet wird.
8.2.2	Die Benutzeri dentifikation und die zugehörigen Konten für Benutzer und Administratoren werden während des gesamten Lebenszyk lus eines Kontos streng verwaltet. (PCI-DSS-v4.0)	codebuild-project-envvar-awscred-überprüfen	Stellen Sie sicher, dass das Projekt KEINE Umgebungs variablen und _ACCESS_KEY enthält. AWS_ACCES S_KEY_ID AWS_SECRE T Die Regel ist NON_COMPLIANT, wenn die Projekt-U mgebungsvariablen Klartext-Anmeldein formationen enthalten.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
8.2.2	Die Benutzeri dentifikation und die zugehörigen Konten für Benutzer und Administratoren werden während des gesamten Lebenszyk lus eines Kontos streng verwaltet. (PCI-DSS-v4.0)	secretsmanager-sch eduled-rotation-su ccess-überprüfen	Stellen Sie sicher, dass AWS Secrets Manager-Geheimniss e gemäß dem Rotationsplan erfolgreich rotiert wurden. Secrets Manager berechnet das Datum, an dem die Rotation stattfind en soll. Die Regel ist NON_COMPLIANT, wenn das Datum verstrichen ist und das Secret nicht rotiert wurde.
8.2.2	Die Benutzeri dentifikation und die zugehörigen Konten für Benutzer und Administratoren werden während des gesamten Lebenszyk lus eines Kontos streng verwaltet. (PCI-DSS-v4.0)	secretsmanager-sec ret-periodic-rotation	Stellen Sie sicher, dass AWS Secrets Manager-Geheimniss e in der letzten angegebenen Anzahl von Tagen rotiert wurden. Die Regel lautet NON_COMPL IANT, wenn ein Secret länger als die Anzahl der maxDaysSince Rotationstage nicht gewechselt wurde. Der Standardwert lautet 90 Tage.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
8.2.2	Die Benutzeri dentifikation und die zugehörigen Konten für Benutzer und Administratoren werden während des gesamten Lebenszyk lus eines Kontos streng verwaltet. (PCI-DSS-v4.0)	secretsmanager-sec ret-unused	Stellen Sie sicher, dass auf AWS Secrets Manager-G eheimnisse innerhalb einer bestimmten Anzahl von Tagen zugegriffen wurde. Die Regel lautet NON_COMPLIANT, wenn innerhalb von 'unusedForDays' Tagen nicht auf ein Geheimnis zugegriff en wurde. Der Standardwert lautet 90 Tage.
8.2.4	Die Benutzeri dentifikation und die zugehörigen Konten für Benutzer und Administratoren werden während des gesamten Lebenszyk lus eines Kontos streng verwaltet. (PCI-DSS-v4.0)	iam-policy-in-use	Stellen Sie sicher, dass ein IAM-Richt linien-ARN einem IAM-Benutzer oder einer Gruppe mit einem oder mehreren IAM-Benutzern oder einer IAM-Rolle mit einer oder mehreren vertrauenswürdigen Entitäten zugewiesen ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
8.2.4	Die Benutzeri dentifikation und die zugehörigen Konten für Benutzer und Administratoren werden während des gesamten Kontolebe nszyklus strikt verwaltet. (PCI-DSS-v4.0)	ec2- no-amazon-key-pair	Stellen Sie sicher, dass laufende Amazon Elastic Compute Cloud (EC2) -Instances nicht mit Amazon-Schlüsselpaaren gestartet werden. Die Regel lautet NON_COMPLIANT, wenn eine laufende EC2 Instance mit einem key pair gestartet wird.
8.2.5	Die Benutzeri dentifikation und die zugehörigen Konten für Benutzer und Administratoren werden während des gesamten Lebenszyk lus eines Kontos streng verwaltet. (PCI-DSS-v4.0)	iam-policy-in-use	Stellen Sie sicher, dass ein IAM-Richt linien-ARN einem IAM-Benutzer oder einer Gruppe mit einem oder mehreren IAM-Benutzern oder einer IAM-Rolle mit einer oder mehreren vertrauenswürdigen Entitäten zugewiesen ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
8.2.5	Die Benutzeri dentifikation und die zugehörigen Konten für Benutzer und Administratoren werden während des gesamten Kontolebe nszyklus strikt verwaltet. (PCI-DSS-v4.0)	ec2- no-amazon-key-pair	Stellen Sie sicher, dass laufende Amazon Elastic Compute Cloud (EC2) -Instances nicht mit Amazon-Schlüsselpaaren gestartet werden. Die Regel lautet NON_COMPLIANT, wenn eine laufende EC2 Instance mit einem key pair gestartet wird.
8.2.6	Die Benutzeri dentifikation und die zugehörigen Konten für Benutzer und Administratoren werden während des gesamten Lebenszyk lus eines Kontos streng verwaltet. (PCI-DSS-v4.0)	secretsmanager-sec ret-unused	Stellen Sie sicher, dass auf AWS Secrets Manager-G eheimnisse innerhalb einer bestimmten Anzahl von Tagen zugegriffen wurde. Die Regel lautet NON_COMPLIANT, wenn innerhalb von 'unusedForDays' Tagen nicht auf ein Geheimnis zugegriff en wurde. Der Standardwert lautet 90 Tage.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
8.2.7	Die Benutzeri dentifikation und die zugehörigen Konten für Benutzer und Administratoren werden während des gesamten Lebenszyk lus eines Kontos streng verwaltet. (PCI-DSS-v4.0)	s-3 bucket-blacklisted-actions-prohibited	Stellen Sie sicher, dass eine Bucket-Ri chtlinie von Amazon Simple Storage Service (Amazon S3) keine Aktionen auf Bucket- und Objektebene auf Blocklisten für Ressourcen im Bucket für Prinzipal e anderer Konten zulässt. AWS Die Regel überprüft beispielsweise, ob die Amazon S3 S3-Bucket-Richtlin ie einem anderen AWS Konto nicht erlaubt, s3: GetBucket *-Aktionen und s3: DeleteObject für ein Objekt im Bucket auszuführ en. Die Regel ist NON_COMPLIANT, wenn gesperrte Aktionen gemäß der Bucket-Richtlinie von Amazon S3 zulässig sind.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
8.2.7	Die Benutzeri dentifikation und die zugehörigen Konten für Benutzer und Administratoren werden während des gesamten Lebenszyk lus eines Kontos streng verwaltet. (PCI-DSS-v4.0)	bucket-policy-not-mores3-permissiv	Stellen Sie sicher, dass Ihre Amazon Simple Storage Service (S3) -Bucket-Richtlinien keine anderen Kontobere chtigungen zulassen als die von Ihnen Amazon S3 S3-Bucket-Kontrollrichtlini e.
8.2.7	Die Benutzeri dentifikation und die zugehörigen Konten für Benutzer und Administratoren werden während des gesamten Kontolebe nszyklus strikt verwaltet. (PCI-DSS-v4.0)	shield-drt-access	Stellen Sie sicher, dass das Shield Response Team (SRT) auf Ihr AWS Konto zugreifen kann. Die Regel lautet NON_COMPLIANT, wenn AWS Shield Advanced aktiviert ist, die Rolle für den SRT-Zugriff jedoch nicht konfiguriert ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
8.2.7	Die Benutzeri dentifikation und die zugehörigen Konten für Benutzer und Administratoren werden während des gesamten Lebenszyk lus eines Kontos streng verwaltet. (PCI-DSS-v4.0)	iam-policy-in-use	Stellen Sie sicher, dass ein IAM-Richt linien-ARN einem IAM-Benutzer oder einer Gruppe mit einem oder mehreren IAM-Benutzern oder einer IAM-Rolle mit einer oder mehreren vertrauenswürdigen Entitäten zugewiesen ist.
8.2.7	Die Benutzeri dentifikation und die zugehörigen Konten für Benutzer und Administratoren werden während des gesamten Kontolebe nszyklus strikt verwaltet. (PCI-DSS-v4.0)	neptune-cluster-ia m-database-Authent ifizierung	Stellen Sie sicher, dass für einen Amazon Neptune Neptune-Cluster die AWS Identity and Access Managemen t (IAM) -Datenban kauthentifizierung aktiviert ist. Die Regel ist NON_COMPL IANT, wenn für einen Amazon-Neptune-Clu ster die IAM-Daten bankauthentifizierung nicht aktiviert ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
8.2.7	Die Benutzeri dentifikation und die zugehörigen Konten für Benutzer und Administratoren werden während des gesamten Kontolebe nszyklus streng verwaltet. (PCI-DSS-v4.0)	rds-cluster-iam-au thentication-aktiviert	Stellen Sie sicher, dass für einen Amazon Relationa l Database Service (Amazon RDS) - Cluster die AWS Identity and Access Management (IAM) -Authentifizierung aktiviert ist. Die Regel ist NON_COMPL IANT, wenn für einen Amazon-RDS-Cluster die IAM-Authentifizier ung nicht aktiviert ist.
8.2.7	Die Benutzeri dentifikation und die zugehörigen Konten für Benutzer und Administratoren werden während des gesamten Kontolebe nszyklus streng verwaltet. (PCI-DSS-v4.0)	ec2- instance-profile-a ttached	Stellen Sie sicher, dass an eine EC2 Instanz ein AWS Identity and Access Management (IAM) -Profil angehängt ist. Die Regel lautet NON_COMPLIANT, wenn der Instanz kein IAM-Profil angehängt ist. EC2

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
8.2.7	Die Benutzeri dentifikation und die zugehörigen Konten für Benutzer und Administratoren werden während des gesamten Kontolebe nszyklus strikt verwaltet. (PCI-DSS-v4.0)	backup-recovery-po int-manual-Löschen-deaktiviert	Stellen Sie sicher, dass einem Backup-Tresor eine ressource nbasierte Richtlinie zugeordnet ist, die das Löschen von Wiederherstellungs punkten verhinder t. Die Regel lautet NON_COMPLIANT, wenn der Backup-Tr esor keine ressource nbasierten Richtlini en oder Richtlinien ohne eine geeignete „Deny“ -Anweisun g (Anweisung mit den Berechtigungen backup:DeleteRecov eryPoint, backup: und backup:UpdateRecov eryPointLifecycle) hat. PutBackupVaultAcce ssPolicy

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
8.2.7	Die Benutzeri dentifikation und die zugehörigen Konten für Benutzer und Administratoren werden während des gesamten Lebenszyk lus eines Kontos streng verwaltet. (PCI-DSS-v4.0)	rds-instance-iam-a uthentication-aktiviert	Stellen Sie sicher, dass für eine Amazon Relational Database Service (Amazon RDS) -Instance die AWS Identity and Access Managemen t (IAM) -Authenti fizierung aktiviert ist. Die Regel ist NON_COMPL IANT, wenn für eine Amazon-RDS-Instanc e die IAM-Authe ntifizierung nicht aktiviert ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
8.2.8	Die Benutzeri dentifikation und die zugehörigen Konten für Benutzer und Administratoren werden während des gesamten Lebenszyk lus eines Kontos streng verwaltet. (PCI-DSS-v4.0)	s-3 bucket-blacklisted-actions-prohibited	Stellen Sie sicher, dass eine Bucket-Ri chtlinie von Amazon Simple Storage Service (Amazon S3) keine Aktionen auf Bucket- und Objektebene auf Blocklisten für Ressourcen im Bucket für Prinzipal e anderer Konten zulässt. AWS Die Regel überprüft beispielsweise, ob die Amazon S3 S3-Bucket-Richtlin ie einem anderen AWS Konto nicht erlaubt, s3: GetBucket *-Aktionen und s3: DeleteObject für ein Objekt im Bucket auszuführ en. Die Regel ist NON_COMPLIANT, wenn gesperrte Aktionen gemäß der Bucket-Richtlinie von Amazon S3 zulässig sind.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
8.2.8	Die Benutzeri dentifikation und die zugehörigen Konten für Benutzer und Administratoren werden während des gesamten Lebenszyk lus eines Kontos streng verwaltet. (PCI-DSS-v4.0)	bucket-policy-not-mores3-permissiv	Stellen Sie sicher, dass Ihre Amazon Simple Storage Service (S3) -Bucket-Richtlinien keine anderen Kontobere chtigungen zulassen als die von Ihnen Amazon S3 S3-Bucket-Kontrollrichtlini e.
8.2.8	Die Benutzeri dentifikation und die zugehörigen Konten für Benutzer und Administratoren werden während des gesamten Lebenszyk lus eines Kontos streng verwaltet. (PCI-DSS-v4.0)	shield-drt-access	Stellen Sie sicher, dass das Shield Response Team (SRT) auf Ihr AWS Konto zugreifen kann. Die Regel lautet NON_COMPLIANT, wenn AWS Shield Advanced aktiviert ist, die Rolle für den SRT-Zugriff jedoch nicht konfiguriert ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
8.2.8	Die Benutzeri dentifikation und die zugehörigen Konten für Benutzer und Administratoren werden während des gesamten Lebenszyk lus eines Kontos streng verwaltet. (PCI-DSS-v4.0)	iam-policy-in-use	Stellen Sie sicher, dass ein IAM-Richt linien-ARN einem IAM-Benutzer oder einer Gruppe mit einem oder mehreren IAM-Benutzern oder einer IAM-Rolle mit einer oder mehreren vertrauenswürdigen Entitäten zugewiesen ist.
8.2.8	Die Benutzeri dentifikation und die zugehörigen Konten für Benutzer und Administratoren werden während des gesamten Lebenszyk lus eines Kontos streng verwaltet. (PCI-DSS-v4.0)	neptune-cluster-ia m-database-Authent ifizierung	Stellen Sie sicher, dass für einen Amazon Neptune Neptune-Cluster die AWS Identity and Access Managemen t (IAM) -Datenban kauthentifizierung aktiviert ist. Die Regel ist NON_COMPL IANT, wenn für einen Amazon-Neptune-Clu ster die IAM-Daten bankauthentifizierung nicht aktiviert ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
8.2.8	Die Benutzeri dentifikation und die zugehörigen Konten für Benutzer und Administratoren werden während des gesamten Lebenszyk lus eines Kontos streng verwaltet. (PCI-DSS-v4.0)	rds-cluster-iam-au thentication-aktiviert	Stellen Sie sicher, dass für einen Amazon Relationa l Database Service (Amazon RDS) - Cluster die AWS Identity and Access Management (IAM) -Authentifizierung aktiviert ist. Die Regel ist NON_COMPL IANT, wenn für einen Amazon-RDS-Cluster die IAM-Authentifizier ung nicht aktiviert ist.
8.2.8	Die Benutzeri dentifikation und die zugehörigen Konten für Benutzer und Administratoren werden während des gesamten Lebenszyk lus eines Kontos streng verwaltet. (PCI-DSS-v4.0)	ec2-imdsv2-check	Stellen Sie sicher, dass die Metadaten version Ihrer Amazon Elastic Compute Cloud (Amazon EC2) -Instance mit Instance Metadata Service Version 2 (IMDSv2) konfiguri ert ist. Die Regel lautet NON_COMPL IANT, wenn sie auf HttpTokens optional gesetzt ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
8.2.8	Die Benutzeri dentifikation und die zugehörigen Konten für Benutzer und Administratoren werden während des gesamten Lebenszyk lus eines Kontos streng verwaltet. (PCI-DSS-v4.0)	ec2- instance-profile-a ttached	Stellen Sie sicher, dass an eine EC2 Instanz ein AWS Identity and Access Management (IAM) -Profil angehängt ist. Die Regel lautet NON_COMPLIANT, wenn der Instanz kein IAM-Profil angehängt ist. EC2
8.2.8	Die Benutzeri dentifikation und die zugehörigen Konten für Benutzer und Administratoren werden während des gesamten Lebenszyk lus eines Kontos streng verwaltet. (PCI-DSS-v4.0)	autoscaling-launch config-requires-im dsv2	Stellen Sie sicher, dass nur aktiviert ist. IMDSv2 Diese Regel ist NON_COMPL IANT, wenn die Metadaten-Version nicht in der Startkonf iguration enthalten ist oder sowohl Metadaten V1 als auch V2 aktiviert sind.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
8.2.8	Die Benutzeridentifikation und die zugehörigen Konten für Benutzer und Administratoren werden während des gesamten Lebenszyklus eines Kontos streng verwaltet. (PCI-DSS-v4.0)	backup-recovery-point-manual-Löschen-deaktiviert	Stellen Sie sicher, dass einem Backup-Tresor eine ressourcenbasierte Richtlinie zugeordnet ist, die das Löschen von Wiederherstellungspunkten verhindert. Die Regel lautet NON_COMPLIANT, wenn der Backup-Tresor keine ressourcenbasierten Richtlinien oder Richtlinien ohne eine geeignete „Deny“ -Anweisung (Anweisung mit den Berechtigungen backup:DeleteRecoveryPoint, backup: und backup:UpdateRecoveryPointLifecycle) hat. PutBackupVaultAccessPolicy

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
8.2.8	Die Benutzeri dentifikation und die zugehörigen Konten für Benutzer und Administratoren werden während des gesamten Lebenszyk lus eines Kontos streng verwaltet. (PCI-DSS-v4.0)	rds-instance-iam-a uthentication-aktiviert	Stellen Sie sicher, dass für eine Amazon Relational Database Service (Amazon RDS) -Instance die AWS Identity and Access Managemen t (IAM) -Authenti fizierung aktiviert ist. Die Regel ist NON_COMPL IANT, wenn für eine Amazon-RDS-Instanc e die IAM-Authe ntifizierung nicht aktiviert ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
8.3.10.1	Eine starke Authentifizierung für Benutzer und Administratoren wird eingerichtet und verwaltet. (PCI-DSS-v4.0)	access-keys-rotated	Stellen Sie sicher, dass aktive IAM-Zugriffsschlüssel innerhalb der unter Alter angegebenen Anzahl von Tagen rotiert (geändert) werden. maxAccessKey Die Regel ist NON_COMPLIANT, wenn die Zugriffsschlüssel nicht innerhalb des angegebenen Zeitraums rotiert werden. Der Standardwert lautet 90 Tage.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
8.3.10.1	Eine starke Authentifizierung für Benutzer und Administratoren wird eingerichtet und verwaltet. (PCI-DSS-v4.0)	secretsmanager-scheduled-rotation-success-überprüfen	Stellen Sie sicher, dass AWS Secrets Manager-Geheimnisse gemäß dem Rotationsplan erfolgreich rotiert wurden. Secrets Manager berechnet das Datum, an dem die Rotation stattfinden soll. Die Regel ist NON_COMPLIANT, wenn das Datum verstrichen ist und das Secret nicht rotiert wurde.
8.3.10.1	Eine starke Authentifizierung für Benutzer und Administratoren wird eingerichtet und verwaltet. (PCI-DSS-v4.0)	secretsmanager-secret-periodic-rotation	Stellen Sie sicher, dass AWS Secrets Manager-Geheimnisse in der letzten angegebenen Anzahl von Tagen rotiert wurden. Die Regel lautet NON_COMPLIANT, wenn ein Secret länger als die Anzahl der maxDaysSince Rotationstage nicht gewechselt wurde. Der Standardwert lautet 90 Tage.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
8.3.11	Eine starke Authentifizierung für Benutzer und Administratoren wird eingerichtet und verwaltet. (PCI-DSS-v4.0)	iam-policy-in-use	Stellen Sie sicher, dass ein IAM-Richtlinien-ARN einem IAM-Benutzer oder einer Gruppe mit einem oder mehreren IAM-Benutzern oder einer IAM-Rolle mit einer oder mehreren vertrauenswürdigen Entitäten zugewiesen ist.
8.3.11	Eine starke Authentifizierung für Benutzer und Administratoren wird eingerichtet und verwaltet. (PCI-DSS-v4.0)	ec2- no-amazon-key-pair	Stellen Sie sicher, dass laufende Amazon Elastic Compute Cloud (EC2) -Instances nicht mit Amazon-Schlüsselpaaren gestartet werden. Die Regel lautet NON_COMPLIANT, wenn eine laufende EC2 Instance mit einem key pair gestartet wird.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
8.3.2	Eine starke Authentifizierung für Benutzer und Administratoren wird eingerichtet und verwaltet. (PCI-DSS-v4.0)	athena-workgroup-encrypted-at-ausruhen	Stellen Sie sicher, dass eine Amazon Athena Athena-Arbeitsgruppe im Ruhezustand verschlüsselt ist. Die Regel ist NON_COMPLIANT, wenn die Verschlüsselung von Daten im Ruhezustand für eine Athena-Arbeitsgruppe nicht aktiviert ist.
8.3.2	Eine starke Authentifizierung für Benutzer und Administratoren wird eingerichtet und verwaltet. (PCI-DSS-v4.0)	neptune-cluster-snapshot-encrypted	Stellen Sie sicher, dass ein Amazon Neptune Neptune-DB-Cluster über verschlüsselte Snapshots verfügt. Die Regel ist NON_COMPLIANT, wenn ein Neptune-Cluster keine verschlüsselten Snapshots enthält.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
8.3.2	Eine starke Authentifizierung für Benutzer und Administratoren wird eingerichtet und verwaltet. (PCI-DSS-v4.0)	redshift-cluster-kms-enabled	Stellen Sie sicher, dass Amazon Redshift Redshift-Cluster einen bestimmten AWS Key Management Service (AWS KMS) -Schlüssel für die Verschlüsselung verwenden. Die Regel ist KONFORM, wenn die Verschlüsselung aktiviert ist und der Cluster mit dem im kmsKeyArn Parameter angegebenen Schlüssel verschlüsselt ist. Die Regel ist NON_COMPLIANT, wenn der Cluster nicht oder mit einem anderen Schlüssel verschlüsselt ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
8.3.2	Eine starke Authentifizierung für Benutzer und Administratoren wird eingerichtet und verwaltet. (PCI-DSS-v4.0)	codebuild-project-artifact-encryption	Stellen Sie sicher, dass in einem AWS CodeBuild Projekt die Verschlüsselung für alle Artefakte aktiviert ist. Die Regel ist NON_COMPLIANT, wenn „encryptionDisabled“ für alle primären oder sekundären (falls vorhanden) Artefaktkonfigurationen auf „True“ festgelegt ist.
8.3.2	Eine starke Authentifizierung für Benutzer und Administratoren wird eingerichtet und verwaltet. (PCI-DSS-v4.0)	codebuild-project-s3-log-verschlüsselt	Stellen Sie sicher, dass bei einem mit Amazon S3 Logs konfigurierten AWS CodeBuild Projekt die Verschlüsselung für die Protokolle aktiviert ist. Die Regel lautet NON_COMPLIANT, wenn „EncryptionDisabled“ in einem S3-Projekt auf „true“ gesetzt ist. LogsConfig CodeBuild

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
8.3.2	Eine starke Authentifizierung für Benutzer und Administratoren wird eingerichtet und verwaltet. (PCI-DSS-v4.0)	dax-encryption-enabled	Stellen Sie sicher, dass Amazon DynamoDB Accelerator (DAX) -Cluster verschlüsselt sind. Die Regel ist NON_COMPLIANT, wenn ein DAX-Cluster nicht verschlüsselt ist.
8.3.2	Eine starke Authentifizierung für Benutzer und Administratoren wird eingerichtet und verwaltet. (PCI-DSS-v4.0)	dms-redis-tls-enabled	Stellen Sie sicher, dass die Endpunkte des AWS Database Migration Service (AWS DMS) für Redis-Datenspeicher aktiviert sind, sodass die TLS/SSL encryption of data communicated with other endpoints. The rule is NON_COMPLIANT if TLS/SSL Verschlüsselung nicht aktiviert ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
8.3.2	Eine starke Authentifizierung für Benutzer und Administratoren wird eingerichtet und verwaltet. (PCI-DSS-v4.0)	eks-secrets-encrypted	Stellen Sie sicher, dass Amazon Elastic Kubernetes Service Service-Cluster so konfiguriert sind, dass Kubernetes-Geheimnisse mithilfe von AWS Key Management Service (KMS) - Schlüsseln verschlüsselt werden.
8.3.2	Eine starke Authentifizierung für Benutzer und Administratoren wird eingerichtet und verwaltet. (PCI-DSS-v4.0)	api-gw-cache-enabled-und-verschlüsselt	Stellen Sie sicher, dass für alle Methoden in den Amazon API Gateway Gateway-Stufen der Cache aktiviert und der Cache verschlüsselt ist. Die Regel ist NON_COMPLIANT, wenn für eine Methode in einer Amazon-API-Gateway-Stufe der Cache nicht konfiguriert oder nicht verschlüsselt ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
8.3.2	Eine starke Authentifizierung für Benutzer und Administratoren wird eingerichtet und verwaltet. (PCI-DSS-v4.0)	docdb-cluster-encrypted	Stellen Sie sicher, dass die Speicherverschlüsselung für Ihre Amazon DocumentDB-Cluster (mit MongoDB-Kompatibilität) aktiviert ist. Die Regel ist NON_COMPLIANT, wenn die Speicherverschlüsselung nicht aktiviert ist.
8.3.2	Eine starke Authentifizierung für Benutzer und Administratoren wird eingerichtet und verwaltet. (PCI-DSS-v4.0)	dynamodb-table-encrypted-kms	Stellen Sie sicher, dass die Amazon DynamoDB-Tabelle mit dem AWS Key Management Service (KMS) verschlüsselt ist. Die Regel lautet NON_COMPLIANT, wenn die Amazon DynamoDB-Tabelle nicht mit KMS verschlüsselt ist. AWS Die Regel ist auch NON_COMPLIANT, wenn der verschlüsselte AWS KMS-Schlüssel nicht im Eingabeparameter vorhanden ist. kmsKeyArns

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
8.3.2	Eine starke Authentifizierung für Benutzer und Administratoren wird eingerichtet und verwaltet. (PCI-DSS-v4.0)	dynamodb-table-encryption-enabled	Stellen Sie sicher, dass die Amazon DynamoDB-Tabellen verschlüsselt sind, und überprüfen Sie ihren Status. Die Regel ist COMPLIANT, wenn der Status "Aktiviert" oder "Wird aktiviert" lautet.
8.3.2	Eine starke Authentifizierung für Benutzer und Administratoren wird eingerichtet und verwaltet. (PCI-DSS-v4.0)	cloudfront-no-deprecated-ssl-protokolle	Stellen Sie sicher, dass CloudFront Distributionen keine veralteten SSL-Protokolle für die HTTPS-Kommunikation zwischen Edge-Standorten und benutzerdefinierten Ursprüngen verwenden . CloudFront Diese Regel ist NON_COMPLIANT für eine CloudFront Verteilung, falls eine Verteilung 'einschließt'. OriginSslProtocols SSLv3

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
8.3.2	Eine starke Authentifizierung für Benutzer und Administratoren wird eingerichtet und verwaltet. (PCI-DSS-v4.0)	cloudfront-traffic-to-origin-verschlüsselt	Stellen Sie sicher, dass CloudFront Amazon-Distributionen den Datenverkehr zu benutzerdefinierten Ursprüngen verschlüsseln. Die Regel lautet NON_COMPLIANT, falls " " " " " " " " für 'nur' HTTP 'ist oder wennOriginProtocolPolicy' 'für' Match-Viewer 'steht und' 'für 'Allow-All' steht. OriginProtocolPolicy ViewerProtocolPolicy
8.3.2	Eine starke Authentifizierung für Benutzer und Administratoren wird eingerichtet und verwaltet. (PCI-DSS-v4.0)	cloudfront-viewer-policy-https	Stellen Sie sicher, dass Ihre CloudFront Amazon-Distributionen HTTPS verwenden (direkt oder über eine Umleitung). Die Regel lautet NON_COMPLIANT, wenn der Wert von auf 'allow-all' für oder für gesetzt ViewerProtocolPolicy ist. DefaultCacheBehavior CacheBehaviors

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
8.3.2	Eine starke Authentifizierung für Benutzer und Administratoren wird eingerichtet und verwaltet. (PCI-DSS-v4.0)	codebuild-project-envvar-awscred-überprüfen	Stellen Sie sicher, dass das Projekt KEINE Umgebungsvariablen und _ACCESS_KEY enthält. AWS_ACCESS_KEY_ID AWS_SECRET Die Regel ist NON_COMPLIANT, wenn die Projekt-Umgebungsvariablen Klartext-Anmeldeinformationen enthalten.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
8.3.2	Eine starke Authentif izierung für Benutzer und Administratoren wird eingerichtet und verwaltet. (PCI-DSS-v4.0)	elb-acm-certificate-required	Stellen Sie sicher, dass die Classic Load Balancers SSL-Zerti fikate verwenden, die vom AWS Certificate Manager bereitgestellt werden. Verwenden Sie zur Nutzung dieser Regel mit Ihrem Classic Load Balancer einen SSL- oder HTTPS-Listener. Hinweis: Diese Regel gilt nur für Classic Load Balancers. Mit dieser Regel werden keine Applicati on Load Balancer oder Network Load Balancer geprüft.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
8.3.2	Eine starke Authentifizierung für Benutzer und Administratoren wird eingerichtet und verwaltet. (PCI-DSS-v4.0)	dax-tls-endpoint-encryption	Stellen Sie sicher, dass Ihr Amazon DynamoDB Accelerator (DAX) -Cluster auf TLS ClusterEndpointEncryptionType eingestellt ist. Die Regel lautet NON_COMPLIANT, wenn ein DAX-Cluster nicht mit Transport Layer Security (TLS) verschlüsselt ist.
8.3.2	Eine starke Authentifizierung für Benutzer und Administratoren wird eingerichtet und verwaltet. (PCI-DSS-v4.0)	eks-cluster-secrets-encrypted	Stellen Sie sicher, dass Amazon EKS-Cluster nicht so konfiguriert sind, dass Kubernetes-Geheimnisse mit KMS verschlüsselt AWS werden. Die Regel lautet NON_COMPLIANT, wenn ein EKS-Cluster keine EncryptionConfig-Ressource hat oder wenn EncryptionConfig Geheimnisse nicht als Ressource benennt.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
8.3.2	Eine starke Authentifizierung für Benutzer und Administratoren wird eingerichtet und verwaltet. (PCI-DSS-v4.0)	kinesis-stream-encrypted	Stellen Sie sicher, dass Amazon Kinesis Kinesis-Streams im Ruhezustand mit serverseitiger Verschlüsselung verschlüsselt werden. Die Regel lautet NON_COMPLIANT für einen Kinesis-Stream, wenn 'StreamEncryption' nicht vorhanden ist.
8.3.2	Eine starke Authentifizierung für Benutzer und Administratoren wird eingerichtet und verwaltet. (PCI-DSS-v4.0)	msk-in-cluster-node-TLS erforderlich	Stellen Sie sicher, dass ein Amazon MSK-Cluster die Verschlüsselung während der Übertragung mithilfe von HTTPS (TLS) mit den Broker-Knoten des Clusters erzwingt. Die Regel ist NON_COMPLIANT, wenn Klartextkommunikation für Broker-Knotenverbindungen in Clustern aktiviert ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
8.3.2	Eine starke Authentifizierung für Benutzer und Administratoren wird eingerichtet und verwaltet. (PCI-DSS-v4.0)	neptune-cluster-encrypted	Stellen Sie sicher, dass die Speicherverschlüsselung für Ihre Amazon Neptune Neptune-DB-Cluster aktiviert ist. Die Regel ist NON_COMPLIANT, wenn die Speicherverschlüsselung nicht aktiviert ist.
8.3.2	Eine starke Authentifizierung für Benutzer und Administratoren wird eingerichtet und verwaltet. (PCI-DSS-v4.0)	dms-endpoint-ssl-configured	Stellen Sie sicher, dass die Endpoints des AWS Database Migration Service (AWS DMS) mit einer SSL-Verbindung konfiguriert sind. Die Regel lautet NON_COMPLIANT, wenn für AWS DMS keine SSL-Verbindung konfiguriert ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
8.3.4	Eine starke Authentifizierung für Benutzer und Administratoren wird eingerichtet und verwaltet. (PCI-DSS-v4.0)	s-3 bucket-blacklisted-actions-prohibited	Stellen Sie sicher, dass eine Bucket-Richtlinie von Amazon Simple Storage Service (Amazon S3) keine Aktionen auf Bucket- und Objektebene auf Blocklisten für Ressourcen im Bucket für Prinzipale anderer Konten zulässt. AWS Die Regel überprüft beispielsweise, ob die Amazon S3 S3-Bucket-Richtlinie einem anderen AWS Konto nicht erlaubt, s3: GetBucket *-Aktionen und s3: DeleteObject für ein Objekt im Bucket auszuführen. Die Regel ist NON_COMPLIANT, wenn gesperrte Aktionen gemäß der Bucket-Richtlinie von Amazon S3 zulässig sind.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
8.3.4	Eine starke Authentifizierung für Benutzer und Administratoren wird eingerichtet und verwaltet. (PCI-DSS-v4.0)	bucket-policy-not-mores3-permissiv	Stellen Sie sicher, dass Ihre Amazon Simple Storage Service (S3) -Bucket-Richtlinien keine anderen Kontobere chtigungen zulassen als die von Ihnen Amazon S3 S3-Bucket-Kontrollrichtlinie.
8.3.4	Eine starke Authentifizierung für Benutzer und Administratoren wird eingerichtet und verwaltet. (PCI-DSS-v4.0)	shield-drt-access	Stellen Sie sicher, dass das Shield Response Team (SRT) auf Ihr AWS Konto zugreifen kann. Die Regel lautet NON_COMPLIANT, wenn AWS Shield Advanced aktiviert ist, die Rolle für den SRT-Zugriff jedoch nicht konfiguriert ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
8.3.4	Eine starke Authentifizierung für Benutzer und Administratoren wird eingerichtet und verwaltet. (PCI-DSS-v4.0)	iam-policy-in-use	Stellen Sie sicher, dass ein IAM-Richtlinien-ARN einem IAM-Benutzer oder einer Gruppe mit einem oder mehreren IAM-Benutzern oder einer IAM-Rolle mit einer oder mehreren vertrauenswürdigen Entitäten zugewiesen ist.
8.3.4	Eine starke Authentifizierung für Benutzer und Administratoren wird eingerichtet und verwaltet. (PCI-DSS-v4.0)	neptune-cluster-iam-database-Authentifizierung	Stellen Sie sicher, dass für einen Amazon Neptune Neptune-Cluster die AWS Identity and Access Management (IAM) -Datenbankauthentifizierung aktiviert ist. Die Regel ist NON_COMPLIANT, wenn für einen Amazon-Neptune-Cluster die IAM-Datenbankauthentifizierung nicht aktiviert ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
8.3.4	Eine starke Authentifizierung für Benutzer und Administratoren wird eingerichtet und verwaltet. (PCI-DSS-v4.0)	rds-cluster-iam-authentication-aktiviert	Stellen Sie sicher, dass für einen Amazon Relational Database Service (Amazon RDS) -Cluster die AWS Identity and Access Management (IAM) -Authentifizierung aktiviert ist. Die Regel ist NON_COMPLIANT, wenn für einen Amazon-RDS-Cluster die IAM-Authentifizierung nicht aktiviert ist.
8.3.4	Eine starke Authentifizierung für Benutzer und Administratoren wird eingerichtet und verwaltet. (PCI-DSS-v4.0)	ec2- instance-profile-attached	Stellen Sie sicher, dass an eine EC2 Instanz ein AWS Identity and Access Management (IAM) -Profil angehängt ist. Die Regel lautet NON_COMPLIANT, wenn der Instanz kein IAM-Profil angehängt ist. EC2

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
8.3.4	Eine starke Authentifizierung für Benutzer und Administratoren wird eingerichtet und verwaltet. (PCI-DSS-v4.0)	backup-recovery-point-manual-Löschen-deaktiviert	Stellen Sie sicher, dass einem Backup-Tresor eine ressourcenbasierte Richtlinie zugeordnet ist, die das Löschen von Wiederherstellungspunkten verhindert. Die Regel lautet NON_COMPLIANT, wenn der Backup-Tresor keine ressourcenbasierten Richtlinien oder Richtlinien ohne eine geeignete „Deny“ -Anweisung (Anweisung mit den Berechtigungen backup:DeleteRecoveryPoint, backup: und backup:UpdateRecoveryPointLifecycle) hat. PutBackupVaultAccessPolicy

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
8.3.4	Eine starke Authentifizierung für Benutzer und Administratoren ist eingerichtet und wird verwaltet. (PCI-DSS-v4.0)	rds-instance-iam-authentication-aktiviert	Stellen Sie sicher, dass für eine Amazon Relational Database Service (Amazon RDS) -Instance die AWS Identity and Access Management (IAM) -Authentifizierung aktiviert ist. Die Regel ist NON_COMPLIANT, wenn für eine Amazon-RDS-Instance die IAM-Authentifizierung nicht aktiviert ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
8.3.5	Eine starke Authentifizierung für Benutzer und Administratoren wird eingerichtet und verwaltet. (PCI-DSS-v4.0)	access-keys-rotated	Stellen Sie sicher, dass aktive IAM-Zugriffsschlüssel innerhalb der unter Alter angegebenen Anzahl von Tagen rotiert (geändert) werden. maxAccessKey Die Regel ist NON_COMPLIANT, wenn die Zugriffsschlüssel nicht innerhalb des angegebenen Zeitraums rotiert werden. Der Standardwert lautet 90 Tage.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
8.3.5	Eine starke Authentifizierung für Benutzer und Administratoren wird eingerichtet und verwaltet. (PCI-DSS-v4.0)	secretsmanager-scheduled-rotation-success-überprüfen	Stellen Sie sicher, dass AWS Secrets Manager-Geheimnisse gemäß dem Rotationsplan erfolgreich rotiert wurden. Secrets Manager berechnet das Datum, an dem die Rotation stattfinden soll. Die Regel ist NON_COMPLIANT, wenn das Datum verstrichen ist und das Secret nicht rotiert wurde.
8.3.5	Eine starke Authentifizierung für Benutzer und Administratoren wird eingerichtet und verwaltet. (PCI-DSS-v4.0)	secretsmanager-secret-periodic-rotation	Stellen Sie sicher, dass AWS Secrets Manager-Geheimnisse in der letzten angegebenen Anzahl von Tagen rotiert wurden. Die Regel lautet NON_COMPLIANT, wenn ein Secret länger als die Anzahl der maxDaysSince Rotationstage nicht gewechselt wurde. Der Standardwert lautet 90 Tage.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
8.3.7	Eine starke Authentif izierung für Benutzer und Administratoren wird eingerichtet und verwaltet. (PCI-DSS-v4.0)	access-keys-rotated	Stellen Sie sicher, dass aktive IAM-Zugriffsschlüssel innerhalb der unter Alter angegebenen Anzahl von Tagen rotiert (geändert) werden. maxAccess Key Die Regel ist NON_COMPL IANT, wenn die Zugriffsschlüssel nicht innerhalb des angegeben en Zeitraums rotiert werden. Der Standardwert lautet 90 Tage.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
8.3.7	Eine starke Authentifizierung für Benutzer und Administratoren wird eingerichtet und verwaltet. (PCI-DSS-v4.0)	secretsmanager-scheduled-rotation-success-überprüfen	Stellen Sie sicher, dass AWS Secrets Manager-Geheimnisse gemäß dem Rotationsplan erfolgreich rotiert wurden. Secrets Manager berechnet das Datum, an dem die Rotation stattfinden soll. Die Regel ist NON_COMPLIANT, wenn das Datum verstrichen ist und das Secret nicht rotiert wurde.
8.3.7	Eine starke Authentifizierung für Benutzer und Administratoren wird eingerichtet und verwaltet. (PCI-DSS-v4.0)	secretsmanager-secret-periodic-rotation	Stellen Sie sicher, dass AWS Secrets Manager-Geheimnisse in der letzten angegebenen Anzahl von Tagen rotiert wurden. Die Regel lautet NON_COMPLIANT, wenn ein Secret länger als die Anzahl der maxDaysSince Rotationstage nicht gewechselt wurde. Der Standardwert lautet 90 Tage.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
8.3.9	Eine starke Authentif izierung für Benutzer und Administratoren wird eingerichtet und verwaltet. (PCI-DSS-v4.0)	access-keys-rotated	Stellen Sie sicher, dass aktive IAM-Zugriffsschlüssel innerhalb der unter Alter angegebenen Anzahl von Tagen rotiert (geändert) werden. maxAccess Key Die Regel ist NON_COMPL IANT, wenn die Zugriffsschlüssel nicht innerhalb des angegeben en Zeitraums rotiert werden. Der Standardwert lautet 90 Tage.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
8.3.9	Eine starke Authentifizierung für Benutzer und Administratoren wird eingerichtet und verwaltet. (PCI-DSS-v4.0)	secretsmanager-scheduled-rotation-success-überprüfen	Stellen Sie sicher, dass AWS Secrets Manager-Geheimnisse gemäß dem Rotationsplan erfolgreich rotiert wurden. Secrets Manager berechnet das Datum, an dem die Rotation stattfinden soll. Die Regel ist NON_COMPLIANT, wenn das Datum verstrichen ist und das Secret nicht rotiert wurde.
8.3.9	Eine starke Authentifizierung für Benutzer und Administratoren wird eingerichtet und verwaltet. (PCI-DSS-v4.0)	secretsmanager-secret-periodic-rotation	Stellen Sie sicher, dass AWS Secrets Manager-Geheimnisse in der letzten angegebenen Anzahl von Tagen rotiert wurden. Die Regel lautet NON_COMPLIANT, wenn ein Secret länger als die Anzahl der maxDaysSince Rotationstage nicht gewechselt wurde. Der Standardwert lautet 90 Tage.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
8.4.1	Die Multi-Faktor-Authentifizierung (MFA) wird implementiert, um den Zugriff auf die CDE zu sichern. (PCI-DSS-v4.0)	s-3 bucket-mfa-delete-enabled	Stellen Sie sicher, dass MFA Delete in der Bucket-Versionierungskonfiguration von Amazon Simple Storage Service (Amazon S3) aktiviert ist. Die Regel ist NON_COMPLIANT, wenn MFA Delete nicht aktiviert ist.
8.4.2	Die Multi-Faktor-Authentifizierung (MFA) wird implementiert, um den Zugriff auf die CDE zu sichern. (PCI-DSS-v4.0)	s-3 bucket-mfa-delete-enabled	Stellen Sie sicher, dass MFA Delete in der Bucket-Versionierungskonfiguration von Amazon Simple Storage Service (Amazon S3) aktiviert ist. Die Regel ist NON_COMPLIANT, wenn MFA Delete nicht aktiviert ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
8.4.3	Die Multi-Faktor-Authentifizierung (MFA) wird implementiert, um den Zugriff auf die CDE zu sichern. (PCI-DSS-v4.0)	s-3 bucket-mfa-delete-enabled	Stellen Sie sicher, dass MFA Delete in der Bucket-Versionierungskonfiguration von Amazon Simple Storage Service (Amazon S3) aktiviert ist. Die Regel ist NON_COMPLIANT, wenn MFA Delete nicht aktiviert ist.
8.6.3	Die Verwendung von Anwendungs- und Systemkonten und den damit verbundenen Authentifizierungsfaktoren wird strikt verwaltet. (PCI-DSS-v4.0)	access-keys-rotated	Stellen Sie sicher, dass aktive IAM-Zugriffsschlüssel innerhalb der unter Alter angegebenen Anzahl von Tagen rotiert (geändert) werden. maxAccessKey Die Regel ist NON_COMPLIANT, wenn die Zugriffsschlüssel nicht innerhalb des angegebenen Zeitraums rotiert werden. Der Standardwert lautet 90 Tage.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
8.6.3	Die Verwendung von Anwendungs- und Systemkonten und den damit verbunden en Authentifizierungs faktoren wird strikt verwaltet. (PCI-DSS-v4.0)	secretsmanager-sch eduled-rotation-su ccess-überprüfen	Stellen Sie sicher, dass AWS Secrets Manager-Geheimniss e gemäß dem Rotationsplan erfolgreich rotiert wurden. Secrets Manager berechnet das Datum, an dem die Rotation stattfind en soll. Die Regel ist NON_COMPLIANT, wenn das Datum verstrichen ist und das Secret nicht rotiert wurde.
8.6.3	Die Verwendung von Anwendungs- und Systemkonten und den damit verbunden en Authentifizierungs faktoren wird strikt verwaltet. (PCI-DSS-v4.0)	secretsmanager-sec ret-periodic-rotation	Stellen Sie sicher, dass AWS Secrets Manager-Geheimniss e in der letzten angegebenen Anzahl von Tagen rotiert wurden. Die Regel lautet NON_COMPL IANT, wenn ein Secret länger als die Anzahl der maxDaysSince Rotationstage nicht gewechselt wurde. Der Standardwert lautet 90 Tage.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
A1.1.2	Multi-Tenant-Servi ceprovider schützen und trennen alle Kundenumgebungen und -daten voneinand er. (PCI-DSS-v4.0)	neptune-cluster-sn apshot-public-verb oten	Stellen Sie sicher, dass ein manueller Amazon Neptune Neptune-DB-Cluster-Snapshot nicht öffentlich ist. Die Regel ist NON_COMPLIANT, wenn es vorhanden e und neue Neptune-Cluster-Snapshots gibt, die öffentlich zugänglich sind.
A1.1.2	Multi-Tenant-Servi ceprovider schützen und trennen alle Kundenumgebungen und -daten voneinand er. (PCI-DSS-v4.0)	docdb-cluster-snap shot-public-verboten	Stellen Sie sicher, dass manuelle Cluster-Snapshots von Amazon DocumentDB nicht öffentlich sind. Die Regel ist NON_COMPLIANT, wenn manuelle Cluster-Snapshots von Amazon DocumentDB öffentlic h sind.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
A1.1.2	Multi-Tenant-Servi ceprovider schützen und trennen alle Kundenumgebungen und -daten voneinand er. (PCI-DSS-v4.0)	backup-recovery-po int-manual-Löschen-deaktiviert	Stellen Sie sicher, dass einem Backup-Tresor eine ressource nbasierte Richtlinie zugeordnet ist, die das Löschen von Wiederherstellungs punkten verhinder t. Die Regel lautet NON_COMPLIANT, wenn der Backup-Tr esor keine ressource nbasierten Richtlini en oder Richtlinien ohne eine geeignete „Deny“ -Anweisun g (Anweisung mit den Berechtigungen backup:DeleteRecov eryPoint, backup: und backup:UpdateRecov eryPointLifecycle) hat. PutBackupVaultAcce ssPolicy

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
A1.1.2	Multi-Tenant-Servi ceprovider schützen und trennen alle Kundenumgebungen und -daten voneinand er. (PCI-DSS-v4.0)	emr-block-public-a ccess	Stellen Sie sicher, dass für ein Konto bei Amazon EMR die Einstellungen zum Sperren des öffentlic hen Zugriffs aktiviert sind. Die Regel ist NON_COMPLIANT, wenn sie falsch BlockPublicSecurit yGroupRules ist, oder wenn sie wahr ist, sind andere Ports als Port 22 unter aufgeführt. Permitted PublicSecurityGrou pRuleRanges
A1.1.2	Multi-Tenant-Servi ceprovider schützen und trennen alle Kundenumgebungen und -daten voneinand er. (PCI-DSS-v4.0)	access-point-public-accesss3-Blöcke	Stellen Sie sicher, dass Amazon S3 S3-Zugriffspunkten die Einstellungen zum Blockieren des öffentlichen Zugriffs aktiviert sind. Die Regel ist NON_COMPLIANT, wenn die Einstellung zum Blockieren des öffentlichen Zugriffs für S3-Zugangspunkte nicht aktiviert ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
A1.1.2	Multi-Tenant-Servi ceprovider schützen und trennen alle Kundenumgebungen und -daten voneinand er. (PCI-DSS-v4.0)	account-level-public-accesss3-Blöcke	Stellen Sie sicher, dass die erforderl ichen Einstellungen für die Sperrung des öffentlichen Zugriffs auf Kontoebene konfiguriert sind. Die Regel ist nur NON_COMPL IANT, wenn die unten festgeleg ten Felder nicht mit den entsprech enden Feldern im Konfigurationselement übereinstimmen.
A1.1.2	Multi-Tenant-Servi ceprovider schützen und trennen alle Kundenumgebungen und -daten voneinand er. (PCI-DSS-v4.0)	s-3 bucket-mfa-delete-enabled	Stellen Sie sicher, dass MFA Delete in der Bucket-Ve rsionierungskonfig uration von Amazon Simple Storage Service (Amazon S3) aktiviert ist. Die Regel ist NON_COMPL IANT, wenn MFA Delete nicht aktiviert ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
A1.1.3	Multi-Tenant-Servi ceprovider schützen und trennen alle Kundenumgebungen und -daten voneinand er. (PCI-DSS-v4.0)	api-gw-endpoint-type-überprüfen	Stellen Sie sicher, dass Amazon API Gateway APIs dem Typ entspricht, der im Regelparameter 'endpointConfigura tionType' angegeben ist. Die Regel gibt NON_COMPLIANT zurück, wenn die REST-API nicht mit dem Endpunkttyp übereinstimmt, der im Regelparameter konfiguriert ist.
A1.1.3	Multi-Tenant-Servi ceprovider schützen und trennen alle Kundenumgebungen und -daten voneinand er. (PCI-DSS-v4.0)	cloudfront-associated-with-waf	Stellen Sie sicher, dass CloudFront Amazon-Distributio nen entweder mit Web Application Firewall (WAF) oder WAFv2 Web Access Control Lists (ACLs) verknüpft sind. Die Regel lautet NON_COMPLIANT, wenn eine CloudFron t Distribution keiner WAF-Web-ACL zugeordnet ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
A1.1.3	Multi-Tenant-Servi ceprovider schützen und trennen alle Kundenumgebungen und -daten voneinand er. (PCI-DSS-v4.0)	cloudfront-custom-ssl-certificate	Stellen Sie sicher, dass das mit einer CloudFront Amazon-Distribution verknüpft e Zertifikat nicht das Standard-SSL-Zerti fikat ist. Die Regel lautet NON_COMPL IANT, wenn eine CloudFront Distribut ion das Standard-SSL-Zertifikat verwendet.
A1.1.3	Multi-Tenant-Servi ceprovider schützen und trennen alle Kundenumgebungen und -daten voneinand er. (PCI-DSS-v4.0)	netfw-policy-defau lt-action-fragment-Pakete	Stellen Sie sicher, dass eine AWS Netzwerk-Firewall-Richtlinie mit einer benutzerdefinierte n statusfreien Standardaktion für fragmentierte Pakete konfiguriert ist. Die Regel ist NON_COMPLIANT, wenn die zustandsl ose Standardaktion für fragmentierte Pakete nicht mit der benutzerdefinierte n Standardaktion übereinstimmt.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
A1.1.3	Multi-Tenant-Servi ceprovider schützen und trennen alle Kundenumgebungen und -daten voneinand er. (PCI-DSS-v4.0)	rds-db-security-group-nicht erlaubt	Stellen Sie sicher, dass es sich bei den DB-Sicher heitsgruppen von Amazon Relationa l Database Service (Amazon RDS) um die Standards icherheitsgruppe handelt. Die Regel ist NON_COMPLIANT, wenn es DB-Sicher heitsgruppen gibt, die nicht die standardm äßige DB-Sicher heitsgruppe sind.
A1.1.3	Multi-Tenant-Servi ceprovider schützen und trennen alle Kundenumgebungen und -daten voneinand er. (PCI-DSS-v4.0)	ec2- transit-gateway-auto-vpc -attach-d eaktiviert	Stellen Sie sicher, dass bei Amazon Elastic Compute Cloud (Amazon EC2) Transit Gateways 'AutoAcceptSharedA ttachments' nicht aktiviert ist. Die Regel ist NON_COMPL IANT für ein Transit Gateway, wenn '' auf AutoAcceptSharedAt tachments 'aktiviert' gesetzt ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
A1.1.3	Multi-Tenant-Servi ceprovider schützen und trennen alle Kundenumgebungen und -daten voneinand er. (PCI-DSS-v4.0)	eks-endpoint-no-pu blic-Zugang	Stellen Sie sicher, dass der Amazon Elastic Kubernete s Service (Amazon EKS) -Endpunkt nicht öffentlich zugänglic h ist. Die Regel ist NON_COMPLIANT, wenn der Endpunkt öffentlich zugänglich ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
A1.1.3	Multi-Tenant-Servi ceprovider schützen und trennen alle Kundenumgebungen und -daten voneinand er. (PCI-DSS-v4.0)	restricted-ssh	Hinweis: Bei dieser Regel untersche iden sich die Regel-ID (INCOMING _SSH_DISABLED) und der Regelname (restricted-ssh). Stellen Sie sicher, dass auf den eingehenden SSH-Verkehr für die Sicherheitsgruppen zugegriffen werden kann. Die Regel ist COMPLIANT, wenn die IP-Adressen des eingehenden SSH-Datenverkehrs in den Sicherheitsgruppen eingeschränkt sind (CIDR ungleich 0.0.0.0/0 oder ::/0). Andernfalls ist sie NON_COMPLIANT.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
A1.1.3	Multi-Tenant-Servi ceprovider schützen und trennen alle Kundenumgebungen und -daten voneinand er. (PCI-DSS-v4.0)	appsync-associated-with-waf	Stellen Sie sicher, dass AWS AppSync APIs sie den AWS WAFv2 Web-Zugri ffskontrolllisten () zugeordnet sind. ACLs Die Regel ist NON_COMPL IANT für eine AWS AppSync API, wenn sie keiner Web-ACL zugeordnet ist.
A1.1.3	Multi-Tenant-Servi ceprovider schützen und trennen alle Kundenumgebungen und -daten voneinand er. (PCI-DSS-v4.0)	docdb-cluster-snap shot-public-verboten	Stellen Sie sicher, dass manuelle Cluster-Snapshots von Amazon DocumentDB nicht öffentlich sind. Die Regel ist NON_COMPLIANT, wenn manuelle Cluster-Snapshots von Amazon DocumentDB öffentlic h sind.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
A1.1.3	Multi-Tenant-Servi ceprovider schützen und trennen alle Kundenumgebungen und -daten voneinand er. (PCI-DSS-v4.0)	codebuild-project-source-repo-URL-Prüfung	Stellen Sie sicher, dass die URL des Bitbucket-Quell-Re positorys KEINE Anmeldeinformation en enthält oder nicht. Die Regel ist NON_COMPL IANT, wenn die URL Anmeldeinformation en enthält, und COMPLIANT, falls dies nicht der Fall ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
A1.1.3	Multi-Tenant-Servi ceprovider schützen und trennen alle Kundenumgebungen und -daten voneinand er. (PCI-DSS-v4.0)	elb-acm-certificate-required	Stellen Sie sicher, dass die Classic Load Balancers SSL-Zerti fikate verwenden, die vom AWS Certificate Manager bereitgestellt werden. Verwenden Sie zur Nutzung dieser Regel mit Ihrem Classic Load Balancer einen SSL- oder HTTPS-Listener. Hinweis: Diese Regel gilt nur für Classic Load Balancers. Mit dieser Regel werden keine Applicati on Load Balancer oder Network Load Balancer geprüft.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
A1.1.3	Multi-Tenant-Servi ceprovider schützen und trennen alle Kundenumgebungen und -daten voneinand er. (PCI-DSS-v4.0)	emr-block-public-a ccess	Stellen Sie sicher, dass für ein Konto bei Amazon EMR die Einstellungen zum Sperren des öffentlic hen Zugriffs aktiviert sind. Die Regel ist NON_COMPLIANT, wenn sie falsch BlockPublicSecurit yGroupRules ist, oder wenn sie wahr ist, sind andere Ports als Port 22 unter aufgeführt. Permitted PublicSecurityGrou pRuleRanges
A1.1.3	Multi-Tenant-Servi ceprovider schützen und trennen alle Kundenumgebungen und -daten voneinand er. (PCI-DSS-v4.0)	nacl-no-unrestricted-ssh-rdp	Stellen Sie sicher, dass die Standardp orts für eingehenden SSH/RDP-Datenverke hr für Netzwerkz ugriffskontrolllisten () eingeschränkt sind. NACLs Die Regel ist NON_COMPLIANT, wenn ein eingehender NACL-Eintrag für die Ports 22 oder 3389 einen CIDR-Block des Typs Quell-TCP oder -UDP zulässt.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
A1.1.3	Multi-Tenant-Servi ceprovider schützen und trennen alle Kundenumgebungen und -daten voneinand er. (PCI-DSS-v4.0)	waf-global-webacl-not-leer	Stellen Sie sicher, dass eine WAF Global Web ACL einige WAF-Regeln oder Regelgruppen enthält. Diese Regel ist NON_COMPLIANT, wenn eine globale Web-ACL keine WAF-Regel oder -Regelgru ppe enthält.
A1.1.3	Multi-Tenant-Servi ceprovider schützen und trennen alle Kundenumgebungen und -daten voneinand er. (PCI-DSS-v4.0)	waf-global-rulegroup-not-leer	Stellen Sie sicher, dass eine AWS WAF Classic-Regelgrupp e einige Regeln enthält. Die Regel ist NON_COMPLIANT, wenn innerhalb einer Regelgruppe keine Regeln vorhanden sind.
A1.1.3	Multi-Tenant-Servi ceprovider schützen und trennen alle Kundenumgebungen und Daten voneinand er. (PCI-DSS-v4.0)	waf-global-rule-not-leer	Stellen Sie sicher, dass eine globale AWS WAF-Regel einige Bedingungen enthält. Die Regel ist NON_COMPL IANT, wenn in der globalen WAF-Regel keine Bedingungen vorhanden sind.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
A1.1.3	Multi-Tenant-Servi ceprovider schützen und trennen alle Kundenumgebungen und Daten voneinand er. (PCI-DSS-v4.0)	ec2- -alle client-vpn-not-authorize	Stellen Sie sicher, dass die AWS Client-VPN-Autorisierungsre geln nicht den Verbindungszugriff für alle Clients autorisie ren. Die Regel ist NON_COMPLIANT, wenn 'AccessAll' vorhanden und auf true gesetzt ist.
A1.1.3	Multi-Tenant-Servi ceprovider schützen und trennen alle Kundenumgebungen und Daten voneinand er. (PCI-DSS-v4.0)	internet-gateway-a uthorized-vpc-nur	Stellen Sie sicher, dass Internet-Gateways an eine autorisierte virtuelle private Cloud (Amazon VPC) angeschlo ssen sind. Die Regel ist NON_COMPL IANT, wenn Internet-Gateways an eine nicht autorisierte VPC angehängt sind.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
A1.1.3	Multi-Tenant-Servi ceprovider schützen und trennen alle Kundenumgebungen und Daten voneinand er. (PCI-DSS-v4.0)	access-point-public-accesss3-Blöcke	Stellen Sie sicher, dass Amazon S3 S3-Zugriffspunkten die Einstellungen zum Blockieren des öffentlichen Zugriffs aktiviert sind. Die Regel ist NON_COMPLIANT, wenn die Einstellung zum Blockieren des öffentlichen Zugriffs für S3-Zugangspunkte nicht aktiviert ist.
A1.1.3	Multi-Tenant-Servi ceprovider schützen und trennen alle Kundenumgebungen und Daten voneinand er. (PCI-DSS-v4.0)	account-level-public-accesss3-Blöcke	Stellen Sie sicher, dass die erforderl ichen Einstellungen für die Sperrung des öffentlichen Zugriffs auf Kontoebene konfiguriert sind. Die Regel ist nur NON_COMPL IANT, wenn die unten festgeleg ten Felder nicht mit den entsprech enden Feldern im Konfigurationselement übereinstimmen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
A1.2.1	Multi-Tenant-Dienstanbieter erleichtern allen Kunden die Protokollierung und Reaktion auf Vorfälle. (PCI-DSS-v4.0)	api-gwv2- access-logs-enabled	Stellen Sie sicher, dass die Amazon API Gateway V2-Stufen die Zugriffsprotokollierung aktiviert haben. Die Regel ist NON_COMPLIANT, wenn 'accessLogSettings' in der Stage-Konfiguration nicht vorhanden ist.
A1.2.1	Multi-Tenant-Dienstanbieter erleichtern allen Kunden die Protokollierung und Reaktion auf Vorfälle. (PCI-DSS-v4.0)	api-gw-xray-enabled	Stellen Sie sicher, dass AWS X-Ray Tracing auf Amazon API Gateway REST APIs aktiviert ist. Die Regel ist COMPLIANT, wenn die X-Ray-Ablaufverfolgung aktiviert ist, andernfalls ist sie NON_COMPLIANT.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
A1.2.1	Multi-Tenant-Dienstanbieter erleichtern allen Kunden die Protokollierung und Reaktion auf Vorfälle. (PCI-DSS-v4.0)	cloudfront-accesslogs-enabled	Stellen Sie sicher, dass CloudFront Amazon-Distributionen so konfiguriert sind, dass sie Zugriffsprotokolle an einen Amazon S3-Bucket senden. Die Regel lautet NON_COMPLIANT, wenn für eine CloudFront Distribution keine Protokollierung konfiguriert ist.
A1.2.1	Multi-Tenant-Dienstanbieter erleichtern allen Kunden die Protokollierung und Reaktion auf Vorfälle. (PCI-DSS-v4.0)	cloudtrail-security-trail-enabled	Stellen Sie sicher, dass mindestens ein AWS CloudTrail Pfad mit bewährten Sicherheitsmethoden definiert ist. Diese Regel ist COMPLIANT, wenn es mindestens einen Trail gibt, der alle der folgenden Bedingungen erfüllt:

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
A1.2.1	Multi-Tenant-Dienstanbieter erleichtern allen Kunden die Protokollierung und Reaktion auf Vorfälle. (PCI-DSS-v4.0)	neptune-cluster-cloudwatch-log-exportfähig	Stellen Sie sicher, dass in einem Amazon Neptune Neptune-Cluster der Protokollexport für CloudWatch Audit-Logs aktiviert ist. Die Regel lautet NON_COMPLIANT, wenn für einen Neptune-Cluster der Protokollexport für CloudWatch Audit-Logs nicht aktiviert ist.
A1.2.1	Multi-Tenant-Dienstanbieter erleichtern allen Kunden die Protokollierung und Reaktion auf Vorfälle. (PCI-DSS-v4.0)	ecs-task-definition-log-Konfiguration	Stellen Sie sicher, dass LogConfiguration für aktive ECS-Aufgabendefinitionen festgelegt ist. Diese Regel ist NON_COMPLIANT, wenn für eine aktive ECSTask Definition die LogConfiguration-Ressource nicht definiert ist oder der Wert für LogConfiguration in mindestens einer Containerdefinition Null ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
A1.2.1	Multi-Tenant-Dienstanbieter erleichtern allen Kunden die Protokollierung und Reaktion auf Vorfälle. (PCI-DSS-v4.0)	cloudtrail-enabled	Hinweis: Bei dieser Regel unterscheiden sich die Regel-ID (CLOUD_TRAIL_ENABLED) und der Regelname (cloudtrail-enabled). Stellen Sie sicher, dass in Ihrem Konto ein Trail aktiviert ist AWS CloudTrail . AWS Die Regel ist NON_COMPLIANT, wenn ein Trail nicht aktiviert ist. Optional überprüft die Regel einen bestimmten S3-Bucket, ein Amazon Simple Notification Service (Amazon SNS) -Thema und eine CloudWatch Protokollgruppe.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
A1.2.1	Multi-Tenant-Dienstanbieter erleichtern allen Kunden die Protokollierung und Reaktion auf Vorfälle. (PCI-DSS-v4.0)	multi-region-cloudtrail-enabled	Hinweis: Bei dieser Regel unterscheiden sich die Regel-ID (MULTI_REGION_CLOUD_TRAIL_ENABLED) und der Regelname (). multi-region-cloudtrail-enabled Stellen Sie sicher, dass mindestens eine Region mit mehreren Regionen vorhanden ist. AWS CloudTrail Die Regel ist NON_COMPLIANT, wenn die Trails nicht mit den Eingabeparametern übereinstimmen. Die Regel lautet NON_COMPLIANT, wenn das ExcludeManagementEventSources Feld nicht leer ist oder wenn sie so konfiguriert AWS CloudTrail ist, dass Verwaltungsereignisse wie AWS KMS-Ereignisse oder Amazon RDS-Daten-API-Ereignisse

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			ausgeschlossen werden.
A1.2.1	Multi-Tenant-Dienstanbieter erleichtern allen Kunden die Protokollierung und Reaktion auf Vorfälle. (PCI-DSS-v4.0)	appsync-logging-enabled	Stellen Sie sicher, dass für eine API die Protokollierung aktiviert ist. AWS AppSync Die Regel lautet NON_COMPLIANT, wenn die Protokollierung nicht aktiviert ist, oder 'fieldLogLevel' ist weder ERROR noch ALL.
A1.2.1	Multi-Tenant-Dienstanbieter erleichtern allen Kunden die Protokollierung und Reaktion auf Vorfälle. (PCI-DSS-v4.0)	waf-classic-logging-enabled	Stellen Sie sicher, dass die Protokollierung auf den AWS WAF Classic Global Web Access Control Lists (Web) aktiviert ist. ACLs Die Regel ist NON_COMPLIANT für eine globale Web-ACL, wenn die Protokollierung nicht aktiviert ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
A1.2.1	Multi-Tenant-Dienstanbieter erleichtern allen Kunden die Protokollierung und Reaktion auf Vorfälle. (PCI-DSS-v4.0)	mq-cloudwatch-audit-logging-aktiviert	Stellen Sie sicher, dass Amazon MQ-Broker die CloudWatch Amazon-Auditprotokollierung aktiviert haben. Die Regel ist NON_COMPLIANT, wenn für einen Broker die Audit-Protokollierung nicht aktiviert ist.
A1.2.1	Multi-Tenant-Dienstanbieter erleichtern allen Kunden die Protokollierung und Reaktion auf Vorfälle. (PCI-DSS-v4.0)	mq-cloudwatch-audit-log-aktiviert	Stellen Sie sicher, dass bei einem Amazon MQ-Broker die CloudWatch Auditprotokollierung aktiviert ist. Die Regel lautet NON_COMPLIANT, wenn für den Broker die Audit-Protokollierung nicht aktiviert ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
A1.2.1	Multi-Tenant-Dienstanbieter erleichtern allen Kunden die Protokollierung und Reaktion auf Vorfälle. (PCI-DSS-v4.0)	eks-cluster-logging-enabled	Stellen Sie sicher, dass ein Amazon Elastic Kubernetes Service (Amazon EKS) -Cluster mit aktivierter Protokollierung konfiguriert ist. Die Regel ist NON_COMPLIANT, wenn die Protokollierung für Amazon-EKS-Cluster nicht für alle Protokolltypen aktiviert ist.
A1.2.1	Multi-Tenant-Dienstanbieter erleichtern allen Kunden die Protokollierung und Reaktion auf Vorfälle. (PCI-DSS-v4.0)	elastic-beanstalk-logs-to-Wolkenbeobachtung	Stellen Sie sicher, dass AWS Elastic Beanstalk Beanstalk -Umgebungen so konfiguriert sind, dass sie Protokolle an Amazon CloudWatch Logs senden. Die Regel lautet NON_COMPLIANT, wenn der Wert von `` StreamLogs falsch ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
A1.2.1	Multi-Tenant-Dienstanbieter erleichtern allen Kunden die Protokollierung und Reaktion auf Vorfälle. (PCI-DSS-v4.0)	step-functions-state-machine-Protokollierung aktiviert	Stellen Sie sicher, dass auf der AWS Step Functions Functions-Maschine die Protokollierung aktiviert ist Die Regel ist NON_COMPLIANT, wenn für eine Zustandsmaschine die Protokollierung nicht aktiviert ist oder die Protokollierungskonfiguration nicht auf dem angegebenen Mindestniveau liegt.
A1.2.1	Multi-Tenant-Dienstanbieter erleichtern allen Kunden die Protokollierung und Reaktion auf Vorfälle. (PCI-DSS-v4.0)	netfw-logging-enabled	Stellen Sie sicher, dass die AWS Netzwerk-Firewall-Firewalls die Protokollierung aktiviert haben. Die Regel ist NON_COMPLIANT, wenn kein Protokollierungstyp konfiguriert ist. Sie können angeben, welchen Protokollierungstyp die Regel prüfen soll.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
A1.2.3	Multi-Tenant-Dienstanbieter erleichtern allen Kunden die Protokollierung und Reaktion auf Vorfälle. (PCI-DSS-v4.0)	security-account-information-provided	Stellen Sie sicher, dass Sie die Sicherheitskontaktinformationen für Ihre Kontokontakte angegeben haben. AWS Die Regel ist NON_COMPLIANT, wenn keine Sicherheitskontaktinformationen innerhalb des Kontos angegeben wurden.
A3.2.5.1	Der PCI-DSS-Umfang ist dokumentiert und validiert. (PCI-DSS-v4.0)	macie-auto-sensitive-data-Discovery-Check	Stellen Sie sicher, dass die automatische Erkennung sensibler Daten für Amazon Macie aktiviert ist. Die Regel lautet NON_COMPLIANT, wenn die automatische Erkennung sensibler Daten deaktiviert ist. Die Regel gilt für Administratorkonten und NICHT FÜR Mitgliedskonten.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
A3.2.5.1	Der PCI-DSS-Umfang ist dokumentiert und validiert. (PCI-DSS-v4.0)	macie-status-check	Stellen Sie sicher, dass Amazon Macie in Ihrem Konto pro Region aktiviert ist. Die Regel ist NON_COMPLIANT, wenn das Attribut „status“ nicht auf „ENABLED“ festgeleg t ist.
A3.2.5.2	Der Umfang des PCI DSS ist dokumentiert und validiert. (PCI-DSS-v4.0)	macie-auto-sensitive-data-Discovery-Check	Stellen Sie sicher, dass die automatische Erkennung sensibler Daten für Amazon Macie aktiviert ist. Die Regel lautet NON_COMPLIANT, wenn die automatis che Erkennung sensibler Daten deaktiviert ist. Die Regel gilt für Administratorkonte n und NICHT FÜR Mitgliedskonten.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
A3.2.5.2	Der Umfang des PCI DSS ist dokumentiert und validiert. (PCI-DSS-v4.0)	macie-status-check	Stellen Sie sicher, dass Amazon Macie in Ihrem Konto pro Region aktiviert ist. Die Regel ist NON_COMPLIANT, wenn das Attribut „status“ nicht auf „ENABLED“ festgeleg t ist.
A3.3.1	PCI DSS ist Teil der Aktivitäten von business-as-usual (BAU). (PCI-DSS-v4.0)	api-gw-xray-enabled	Stellen Sie sicher, dass AWS X-Ray Tracing auf Amazon API Gateway REST APIs aktiviert ist. Die Regel ist COMPLIANT, wenn die X-Ray-Abl aufverfolgung aktiviert ist, andernfalls ist sie NON_COMPLIANT.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
A 3.3.1	PCI DSS ist Teil der Aktivitäten von business-as-usual (BAU). (PCI-DSS-v4.0)	cloudformation-stack-notification-check	Stellen Sie sicher, dass Ihre CloudFormation Stacks Ereignisbenachrichtigungen an ein Amazon SNS SNS-Thema senden. Stellen Sie optional sicher, dass die angegebenen Amazon SNS SNS-Themen verwendet werden. Die Regel lautet NON_COMPLIANT, wenn CloudFormation Stacks keine Benachrichtigungen senden.
A3.3.1	PCI DSS ist Teil der Aktivitäten von business-as-usual (BAU). (PCI-DSS-v4.0)	ec2- instance-detailed-monitoring-enabled	Stellen Sie sicher, dass die detaillierte Überwachung für Instanzen aktiviert ist. EC2 Die Regel ist NON_COMPLIANT, wenn keine detaillierte Überwachung aktiviert ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
A3.3.1	PCI DSS ist Teil der Aktivitäten von business-as-usual (BAU). (PCI-DSS-v4.0)	cloudwatch-alarm-action-check	Stellen Sie sicher, dass bei CloudWatch Alarmen eine Aktion für den Status ALARM, INSUFFICIENT_DATA oder OK konfiguriert ist. Stellen Sie optional sicher, dass alle Aktionen mit einem benannten ARN übereinstimmen. Die Regel ist NON_COMPLIANT, wenn für den Alarm oder den optionalen Parameter keine Aktion festgelegt ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
A3.3.1	PCI DSS ist Teil der Aktivitäten von business-as-usual (BAU). (PCI-DSS-v4.0)	cloudwatch-alarm-action-check	Stellen Sie sicher, dass bei CloudWatch Alarmen eine Aktion für den Status ALARM, INSUFFICIENT_DATA oder OK konfiguriert ist. Stellen Sie optional sicher, dass alle Aktionen mit einem benannten ARN übereinstimmen. Die Regel ist NON_COMPLIANT, wenn für den Alarm oder den optionalen Parameter keine Aktion festgelegt ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
A3.3.1	PCI DSS ist Teil der Aktivitäten von business-as-usual (BAU). (PCI-DSS-v4.0)	cloudwatch-alarm-action-check	Stellen Sie sicher, dass bei CloudWatch Alarmen eine Aktion für den Status ALARM, INSUFFICIENT_DATA oder OK konfiguriert ist. Stellen Sie optional sicher, dass alle Aktionen mit einem benannten ARN übereinstimmen. Die Regel ist NON_COMPLIANT, wenn für den Alarm oder den optionalen Parameter keine Aktion festgelegt ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
A3.3.1	PCI DSS ist Teil der Aktivitäten von business-as-usual (BAU). (PCI-DSS-v4.0)	cloudwatch-alarm-action-check	Stellen Sie sicher, dass bei CloudWatch Alarmen eine Aktion für den Status ALARM, INSUFFICIENT_DATA oder OK konfiguriert ist. Stellen Sie optional sicher, dass alle Aktionen mit einem benannten ARN übereinstimmen. Die Regel ist NON_COMPLIANT, wenn für den Alarm oder den optionalen Parameter keine Aktion festgelegt ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
A3.3.1	PCI DSS ist Teil der Aktivitäten von business-as-usual (BAU). (PCI-DSS-v4.0)	cloudwatch-alarm-resource-check	Stellen Sie sicher, dass ein Ressourcentyp einen CloudWatch Alarm für die angegebene Metrik hat. Als Ressourcentyp können Sie EBS-Volumes, EC2 Instances, Amazon RDS-Cluster oder S3-Buckets angeben. Die Regel ist KONFORM, wenn die benannte Metrik eine Ressourcen-ID und CloudWatch einen Alarm hat.
A3.3.1	PCI DSS ist Teil der Aktivitäten von business-as-usual (BAU). (PCI-DSS-v4.0)	cloudwatch-alarm-settings-check	Stellen Sie sicher, dass CloudWatch Alarme mit dem angegebenen Metriknamen die angegebenen Einstellungen haben.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
A3.3.1	PCI DSS ist Teil der Aktivitäten von business-as-usual (BAU). (PCI-DSS-v4.0)	WAF 2- rulegroup-logging-enabled	Stellen Sie sicher, dass die Erfassung von CloudWatch Amazon-Sicherheits metriken für AWS WAFv2 Regelgruppen aktiviert ist. Die Regel ist NON_COMPL IANT, wenn '. Visibilit yConfig CloudWatc hMetricsEnabledDas Feld 'ist auf falsch gesetzt.
A3.3.1	PCI DSS ist Teil der Aktivitäten von business-as-usual (BAU). (PCI-DSS-v4.0)	sns-topic-message-delivery-Benachric htigung aktiviert	Stellen Sie sicher, dass die Amazon Simple Notificat ion Service (SNS) - Protokollierung für den Zustellungsstatus von Benachric htigungen aktiviert ist, die an ein Thema für die Endgeräte gesendet werden. Die Regel ist NON_COMPLIANT, wenn die Benachric htigung über den Status der Zustellung von Nachrichten nicht aktiviert ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
A3.4.1	Der logische Zugriff auf die Karteninhaberdatenumgebung wird kontrolliert und verwaltet. (PCI-DSS-v4.0)	neptune-cluster-snapshot-public-verboten	Stellen Sie sicher, dass ein manueller Amazon Neptune Neptune-DB-Cluster-Snapshot nicht öffentlich ist. Die Regel ist NON_COMPLIANT, wenn es vorhandene und neue Neptune-Cluster-Snapshots gibt, die öffentlich zugänglich sind.
A3.4.1	Der logische Zugriff auf die Karteninhaberdatenumgebung wird kontrolliert und verwaltet. (PCI-DSS-v4.0)	docdb-cluster-snapshot-public-verboten	Stellen Sie sicher, dass manuelle Cluster-Snapshots von Amazon DocumentDB nicht öffentlich sind. Die Regel ist NON_COMPLIANT, wenn manuelle Cluster-Snapshots von Amazon DocumentDB öffentlich sind.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
A3.4.1	Der logische Zugriff auf die Karteninh aberdatenumgebung wird kontrolliert und verwaltet. (PCI-DSS-v4.0)	backup-recovery-point-manual-Löschen-deaktiviert	Stellen Sie sicher, dass einem Backup-Tresor eine ressourcenbasierte Richtlinie zugeordnet ist, die das Löschen von Wiederherstellungspunkten verhindert. Die Regel lautet NON_COMPLIANT, wenn der Backup-Tresor keine ressourcenbasierten Richtlinien oder Richtlinien ohne eine geeignete „Deny“ -Anweisung (Anweisung mit den Berechtigungen backup:DeleteRecoveryPoint, backup: und backup:UpdateRecoveryPointLifecycle) hat. PutBackupVaultAccessPolicy

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
A3.4.1	Der logische Zugriff auf die Karteninh aberdatenumgebung wird kontrolliert und verwaltet. (PCI-DSS-v4.0)	emr-block-public-access	Stellen Sie sicher, dass für ein Konto bei Amazon EMR die Einstellungen zum Sperren des öffentlichen Zugriffs aktiviert sind. Die Regel ist NON_COMPLIANT, wenn sie falsch BlockPublicSecurityGroupRules ist, oder wenn sie wahr ist, sind andere Ports als Port 22 unter aufgeführt. PermittedPublicSecurityGroupRuleRanges

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
A3.4.1	Der logische Zugriff auf die Karteninh aberdatenumgebung wird kontrolliert und verwaltet. (PCI-DSS-v4.0)	secretsmanager-secret-unused	Stellen Sie sicher, dass auf AWS Secrets Manager-Geheimnisse innerhalb einer bestimmten Anzahl von Tagen zugegriffen wurde. Die Regel lautet NON_COMPLIANT, wenn innerhalb von 'unusedForDays' Tagen nicht auf ein Geheimnis zugegriffen wurde. Der Standardwert lautet 90 Tage.
A3.4.1	Der logische Zugriff auf die Karteninh aberdatenumgebung wird kontrolliert und verwaltet. (PCI-DSS-v4.0)	access-point-public-accesss3-Blöcke	Stellen Sie sicher, dass Amazon S3 S3-Zugriffspunkten die Einstellungen zum Blockieren des öffentlichen Zugriffs aktiviert sind. Die Regel ist NON_COMPLIANT, wenn die Einstellung zum Blockieren des öffentlichen Zugriffs für S3-Zugangspunkte nicht aktiviert ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
A3.4.1	Der logische Zugriff auf die Karteninh aberdatenumgebung wird kontrolliert und verwaltet. (PCI-DSS-v4.0)	account-level-public-accesss3-Blöcke	Stellen Sie sicher, dass die erforderl ichen Einstellungen für die Sperrung des öffentlichen Zugriffs auf Kontoebene konfiguriert sind. Die Regel ist nur NON_COMPL IANT, wenn die unten festgeleg ten Felder nicht mit den entsprech enden Feldern im Konfigurationselement übereinstimmen.
A3.4.1	Der logische Zugriff auf die Karteninh aberdatenumgebung wird kontrolliert und verwaltet. (PCI-DSS-v4.0)	s-3 bucket-mfa-delete-enabled	Stellen Sie sicher, dass MFA Delete in der Bucket-Ve rsionierungskonfig uration von Amazon Simple Storage Service (Amazon S3) aktiviert ist. Die Regel ist NON_COMPL IANT, wenn MFA Delete nicht aktiviert ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
A 3.5.1	Verdächtige Ereignisse werden identifiziert und darauf reagiert. (PCI-DSS-v4.0)	api-gw-xray-enabled	Stellen Sie sicher, dass AWS X-Ray Tracing auf Amazon API Gateway REST APIs aktiviert ist. Die Regel ist COMPLIANT, wenn die X-Ray-Abl aufverfolgung aktiviert ist, andernfalls ist sie NON_COMPLIANT.
A 3.5.1	Verdächtige Ereignisse werden identifiziert und darauf reagiert. (PCI-DSS-v4.0)	cloudformation-stack-notification-check	Stellen Sie sicher, dass Ihre CloudFormation Stacks Ereignisbenachrichtigungen an ein Amazon SNS SNS-Thema senden. Stellen Sie optional sicher, dass die angegebenen Amazon SNS SNS-Themen verwendet werden. Die Regel lautet NON_COMPLIANT, wenn CloudFormation Stacks keine Benachrichtigungen senden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
A3.5.1	Verdächtige Ereignisse werden identifiziert und darauf reagiert. (PCI-DSS-v4.0)	ec2- instance-detailed-monitoring-enabled	Stellen Sie sicher, dass die detaillierte Überwachung für Instanzen aktiviert ist. EC2 Die Regel ist NON_COMPLIANT, wenn keine detaillierte Überwachung aktiviert ist.
A3.5.1	Verdächtige Ereignisse werden identifiziert und darauf reagiert. (PCI-DSS-v4.0)	cloudwatch-alarm-action-check	Stellen Sie sicher, dass bei CloudWatch Alarmen eine Aktion für den Status ALARM, INSUFFICIENT_DATA oder OK konfiguriert ist. Stellen Sie optional sicher, dass alle Aktionen mit einem benannten ARN übereinstimmen. Die Regel ist NON_COMPLIANT, wenn für den Alarm oder den optionalen Parameter keine Aktion festgelegt ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
A3.5.1	Verdächtige Ereignisse werden identifiziert und darauf reagiert. (PCI-DSS-v4.0)	cloudwatch-alarm-action-check	Stellen Sie sicher, dass bei CloudWatch Alarmen eine Aktion für den Status ALARM, INSUFFICIENT_DATA oder OK konfiguriert ist. Stellen Sie optional sicher, dass alle Aktionen mit einem benannten ARN übereinstimmen. Die Regel ist NON_COMPLIANT, wenn für den Alarm oder den optionalen Parameter keine Aktion festgelegt ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
A3.5.1	Verdächtige Ereignisse werden identifiziert und darauf reagiert. (PCI-DSS-v4.0)	cloudwatch-alarm-action-check	Stellen Sie sicher, dass bei CloudWatch Alarmen eine Aktion für den Status ALARM, INSUFFICIENT_DATA oder OK konfiguriert ist. Stellen Sie optional sicher, dass alle Aktionen mit einem benannten ARN übereinstimmen. Die Regel ist NON_COMPLIANT, wenn für den Alarm oder den optionalen Parameter keine Aktion festgelegt ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
A3.5.1	Verdächtige Ereignisse werden identifiziert und darauf reagiert. (PCI-DSS-v4.0)	cloudwatch-alarm-action-check	Stellen Sie sicher, dass bei CloudWatch Alarmen eine Aktion für den Status ALARM, INSUFFICIENT_DATA oder OK konfiguriert ist. Stellen Sie optional sicher, dass alle Aktionen mit einem benannten ARN übereinstimmen. Die Regel ist NON_COMPLIANT, wenn für den Alarm oder den optionalen Parameter keine Aktion festgelegt ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
A3.5.1	Verdächtige Ereignisse werden identifiziert und darauf reagiert. (PCI-DSS-v4.0)	cloudwatch-alarm-resource-check	Stellen Sie sicher, dass ein Ressourcentyp einen CloudWatch Alarm für die angegebene Metrik hat. Als Ressourcentyp können Sie EBS-Volumes, EC2 Instances, Amazon RDS-Cluster oder S3-Buckets angeben. Die Regel ist KONFORM, wenn die benannte Metrik eine Ressourcen-ID und CloudWatch einen Alarm hat.
A3.5.1	Verdächtige Ereignisse werden identifiziert und darauf reagiert. (PCI-DSS-v4.0)	cloudwatch-alarm-settings-check	Stellen Sie sicher, dass CloudWatch Alarme mit dem angegebenen Metriknamen die angegebenen Einstellungen haben.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
A3.5.1	Verdächtige Ereignisse werden identifiziert und darauf reagiert. (PCI-DSS-v4.0)	WAF 2- rulegroup-logging-enabled	Stellen Sie sicher, dass die Erfassung von CloudWatch Amazon-Sicherheitsmetriken für AWS WAFv2 Regelgruppen aktiviert ist. Die Regel ist NON_COMPLIANT, wenn '. VisibilityConfig CloudWatchMetricsEnabledDas Feld 'ist auf falsch gesetzt.
A3.5.1	Verdächtige Ereignisse werden identifiziert und darauf reagiert. (PCI-DSS-v4.0)	sns-topic-message-delivery-Benachrichtigung aktiviert	Stellen Sie sicher, dass die Amazon Simple Notification Service (SNS) - Protokollierung für den Zustellungsstatus von Benachrichtigungen aktiviert ist, die an ein Thema für die Endgeräte gesendet werden. Die Regel ist NON_COMPLIANT, wenn die Benachrichtigung über den Status der Zustellung von Nachrichten nicht aktiviert ist.

Vorlage

Die Vorlage ist verfügbar unter GitHub: Operational Best Practices for PCI DSS 4.0 (einschließlich globaler Ressourcentypen).

Bewährte Methoden für die Ausführung von öffentlich zugänglichen Ressourcen

Dieses Konformitätspaket hilft bei der Identifizierung von Ressourcen, die möglicherweise öffentlich zugänglich sind.

Eine Liste aller verwalteten Regeln, die von unterstützt werden AWS Config, finden Sie unter Liste der AWS Config verwalteten Regeln.

Die Namen und Beschreibungen der erforderlichen Parameter finden Sie im `Parameters` Abschnitt der folgenden Vorlage.

Die Vorlage ist verfügbar unter GitHub: Bewährte Betriebspraktiken für öffentlich zugängliche Ressourcen.

Operative Best Practices für das RBI Cyber Security Framework für UCBs

Konformitätspakete bieten ein allgemeines Compliance-Framework, das es Ihnen ermöglicht, mithilfe verwalteter oder benutzerdefinierter AWS Config Regeln und Abhilfemaßnahmen Kontrollen zur Sicherheits-, Betriebs- oder Kostenoptimierung durchzuführen. AWS Config Conformance Packs dienen als Beispielvorlagen nicht dazu, die vollständige Einhaltung eines bestimmten Governance- oder Compliance-Standards sicherzustellen. Sie sind dafür verantwortlich, selbst zu beurteilen, ob Ihre Nutzung der Services den geltenden gesetzlichen und behördlichen Anforderungen entspricht.

Im Folgenden finden Sie ein Beispiel für eine Zuordnung zwischen dem Cyber Security Framework for Urban Cooperative Banks () der Reserve Bank of Indien (RBIUCBs) und AWS verwalteten Konfigurationsregeln. Jede Config-Regel gilt für eine bestimmte AWS Ressource und bezieht sich auf ein oder mehrere RBI Cyber Security Frameworks für UCBs Kontrollen. Ein RBI Cyber Security Framework zur UCBs Steuerung kann mit mehreren Konfigurationsregeln verknüpft werden. In der folgenden Tabelle finden Sie weitere Informationen und Anleitungen zu diesen Zuordnungen.

Kontroll-ID	AWS Config	Empfehlungen
Anhang_I (1.1)	ec2-manager instance-managed-by-systems	Eine Bestandsaufnahme der Softwareplattformen und

Kontroll-ID	AWS Config	Empfehlungen
		Anwendungen innerhalb des Unternehmens ist möglich, indem Amazon Elastic Compute Cloud (Amazon EC2) -Instances mit AWS Systems Manager verwaltet werden. Verwenden Sie AWS Systems Manager, um detaillierte Systemkonfiguratio nen, Betriebssystem-Patch-Levels, Namen und Typ der Dienste, Softwareinstallati onen, Anwendungsname, Herausgeber und Version sowie andere Details zu Ihrer Umgebung bereitzustellen.
Anhang_I (1.1)	account-part-of-organizations	Durch die zentrale Verwaltun g AWS-Konten innerhalb von AWS Organizations wird sichergestellt, dass die Konten den Vorschriften entsprech en. Eine fehlende zentrale Kontoverwaltung kann zu inkonsistenten Kontokonf igurationen führen, wodurch Ressourcen und sensible Daten offengelegt werden können.

Kontroll-ID	AWS Config	Empfehlungen
Anhang_I (1.1)	ecr-private-tag-immutability-aktiviert	Aktivieren Sie die Unveränderlichkeit von Tags im Elastic Container Repository (ECR), um zu verhindern, dass Image-Tags in Ihren ECR-Images überschrieben werden. Bisher konnten Tags überschrieben werden, was manuelle Methoden zur eindeutigen Identifizierung eines Images erforderte.
Anhang_I (1.3)	acm-certificate-expiration-check	Stellen Sie sicher, dass die Netzwerkintegrität geschützt ist, indem Sie sicherstellen, dass X509-Zertifikate von AWS ACM ausgestellt werden. Diese Zertifikate müssen gültig und dürfen nicht abgelaufen sein. Für diese Regel ist ein Wert für erforderlich daysToExpiration (Wert für bewährte AWS Grundregeln für Sicherheit: 90). Der tatsächliche Wert muss den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	AWS Config	Empfehlungen
Anhang_I (1.3)	alb-http-drop-invalid-Header-aktiviert	Stellen Sie sicher, dass Ihre Elastic Load Balancers (ELB) so konfiguriert sind, dass sie HTTP-Header löschen. Da sensible Daten vorhanden sein können, sollten Sie die Verschlüsselung bei der Übertragung aktivieren, um diese Daten zu schützen.
Anhang_I (1.3)	alb-http-to-https-Umleitungsprüfung	Um Daten während der Übertragung zu schützen, stellen Sie sicher, dass Ihr Application Load Balancer unverschlüsselte HTTP-Anfragen automatisch an HTTPS umleitet. Da sensible Daten vorhanden sein können, sollten Sie die Verschlüsselung bei der Übertragung aktivieren, um diese Daten zu schützen.
Anhang_I (1.3)	api-gw-cache-enabled-und-verschlüsselt	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass die Verschlüsselung für den Cache Ihrer API-Gateway-Stufe aktiviert ist. Da für die API-Methode sensible Daten erfasst werden können, sollten Sie die Verschlüsselung von Daten im Ruhezustand aktivieren, um diese Daten zu schützen.

Kontroll-ID	AWS Config	Empfehlungen
Anhang_I (1.3)	cloud-trail-encryption-enabled	Da sensible Daten vorhanden sein können und um Daten im Ruhezustand zu schützen, sollten Sie sicherstellen, dass die Verschlüsselung für Ihre AWS CloudTrail Trails aktiviert ist.
Anhang_I (1.3)	api-gw-ssl-enabled	Stellen Sie sicher, dass die REST-API-Stufen von Amazon API Gateway mit SSL-Zerti fikaten konfiguriert sind, damit Backend-Systeme überprüfe n können, ob Anforderungen von API Gateway stammen.
Anhang_I (1.3)	elbv-2 acm-certificate-required	Zum Schutz von eventuell vorhandenen sensiblen Daten sowie von Daten während der Übertragung muss die Verschlüsselung für Ihr Elastic Load Balancing aktiviert sein. Verwenden Sie AWS Certifica te Manager, um öffentlic he und private SSL/TLS-Z ertifikate mit AWS Diensten und internen Ressourcen zu verwalten, bereitzustellen und bereitzustellen.

Kontroll-ID	AWS Config	Empfehlungen
Anhang_I (1.3)	s-3 default-encryption-kms	Stellen Sie sicher, dass die Verschlüsselung für Ihre Amazon Simple Storage Service (Amazon S3)-Buckets aktiviert ist. Da sensible Daten in einem Amazon S3 Bucket gespeichert werden können, sollten Sie die Verschlüs selung im Ruhezustand aktivieren, um diese Daten zu schützen.
Anhang_I (1.3)	cloudwatch-log-group-encryp ted	Um sensible Daten im Speicher zu schützen, stellen Sie sicher, dass die Verschlüs selung für Ihre Amazon CloudWatch Log Groups aktiviert ist.
Anhang_I (1.3)	cmk-backing-key-rotation-ak tiviert	Aktivieren Sie die Schlüssel rotation, um sicherzustellen, dass Schlüssel rotiert werden, nachdem sie das Ende ihrer Krypto-Periode erreicht haben.
Anhang_I (1.3)	backup-recovery-point-encry pted	Stellen Sie sicher, dass die Verschlüsselung für Ihre AWS Backup-Wiederherstellungspu nkte aktiviert ist. Da sensible Daten auch im Ruhezusta nd vorhanden sein können, sollten Sie die Verschlüs selung im Ruhezustand aktivieren, um diese Daten zu schützen.

Kontroll-ID	AWS Config	Empfehlungen
Anhang_I (1.3)	codebuild-project-artifact-encryption	Um sensible Daten im Ruhezustand zu schützen, stellen Sie sicher, dass die Verschlüsselung für Ihre AWS CodeBuild Artefakte aktiviert ist.
Anhang_I (1.3)	codebuild-project-s3-Log-verschlüsselt	Um sensible Daten im Ruhezustand zu schützen, stellen Sie sicher, dass die Verschlüsselung für Ihre in Amazon S3 gespeicherten AWS CodeBuild Protokolle aktiviert ist.
Anhang_I (1.3)	opensearch-encrypted-at-rest	Da sensible Daten vorhanden sein können und um Daten im Ruhezustand zu schützen, sollten Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon OpenSearch Service-Domains aktiviert ist.
Anhang_I (1.3)	opensearch-https-required	Da sensible Daten existieren können und um Daten während der Übertragung zu schützen, sollten Sie sicherstellen, dass HTTPS für Verbindungen zu Ihren Amazon OpenSearch Service-Domains aktiviert ist.

Kontroll-ID	AWS Config	Empfehlungen
Anhang_I (1.3)	opensearch-node-to-node-Verschlüsselungsprüfung	Stellen Sie sicher, dass die node-to-node Verschlüsselung für Amazon OpenSearch Service aktiviert ist. Node-to-nodeVerschlüsselung ermöglicht die TLS 1.2-Verschlüsselung für die gesamte Kommunikation innerhalb der Amazon Virtual Private Cloud (Amazon VPC). Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.
Anhang_I (1.3)	dynamodb-table-encrypted-kms	Stellen Sie sicher, dass die Verschlüsselung für Ihre Amazon-DynamoDB-Tabellen aktiviert ist. Um eventuell vorhandene sensible Daten im Ruhezustand in diesen Tabellen zu schützen, müssen Sie die Verschlüsselung von Daten im Ruhezustand aktivieren. Standardmäßig werden DynamoDB-Tabellen mit einem AWS eigenen Kundenhauptschlüssel (CMK) verschlüsselt.

Kontroll-ID	AWS Config	Empfehlungen
Anhang_I (1.3)	ec2- ebs-encryption-by-default	Zum Schutz von Daten im Ruhezustand müssen Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon Elastic Block Store (Amazon EBS)-Volumes aktiviert ist. Da sensible Daten in diesen Volumes gespeichert werden können, sollten Sie die Verschlüsselung von Daten im Ruhezustand aktivieren, um diese Daten zu schützen.
Anhang_I (1.3)	efs-encrypted-check	Aktivieren Sie die Verschlüs selung für Ihr Amazon Elastic File System (EFS), um eventuell vorhandene sensible Daten sowie Daten im Ruhezustand zu schützen.
Anhang_I (1.3)	elasticsearch-encrypted-at-rest	Da sensible Daten vorhanden sein können und um Daten im Ruhezustand zu schützen, sollten Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon OpenSearch Service (OpenSearch Service) -Domains aktiviert ist.

Kontroll-ID	AWS Config	Empfehlungen
Anhang_I (1.3)	elasticsearch-node-to-node-Verschlüsselungsprüfung	Stellen Sie sicher, dass die node-to-node Verschlüsselung für Amazon OpenSearch Service aktiviert ist. Node-to-nodeVerschlüsselung ermöglicht die TLS 1.2-Versc hlüsselung für die gesamte Kommunikation innerhalb der Amazon Virtual Private Cloud (Amazon VPC). Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.
Anhang_I (1.3)	elb-acm-certificate-required	Zum Schutz von eventuell vorhandenen sensiblen Daten sowie von Daten während der Übertragung muss die Verschlüsselung für Ihr Elastic Load Balancing aktiviert sein. Verwenden Sie AWS Certifica te Manager, um öffentlic he und private SSL/TLS-Z ertifikate mit AWS Diensten und internen Ressourcen zu verwalten, bereitzustellen und bereitzustellen.

Kontroll-ID	AWS Config	Empfehlungen
Anhang_I (1.3)	elb-tls-https-listeners-nur	Stellen Sie sicher, dass Ihre Elastic Load Balancer (ELBs) mit SSL- oder HTTPS-Listenern konfiguriert sind. Um eventuell vorhandene sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.
Anhang_I (1.3)	encrypted-volumes	Aktivieren Sie die Verschlüsselung für Ihre Amazon-Elastic-Block-Store-(Amazon-EBS-)Volumes, um eventuell vorhandene sensible Daten sowie Daten im Ruhezustand zu schützen.
Anhang_I (1.3)	kms-cmk-not-scheduled-zum Löschen	Um Daten im Ruhezustand zu schützen, sollten Sie sicherstellen, dass die für den Kunden erforderlichen Masterschlüssel (CMKs) nicht für das Löschen im AWS Key Management Service (AWS KMS) vorgesehen sind. Da Schlüssel manchmal gelöscht werden müssen, können Sie mit dieser Regel alle zu löschenden Schlüssel überprüfen, falls ein Schlüssel versehentlich zur Löschung vorgemerkt wurde.

Kontroll-ID	AWS Config	Empfehlungen
Anhang_I (1.3)	rds-snapshot-encrypted	Stellen Sie sicher, dass die Verschlüsselung für Ihre Amazon Relational Database Service (Amazon RDS)-Snapshots aktiviert ist. Da sensible Daten auch im Ruhezustand vorhanden sein können, sollten Sie die Verschlüsselung von Daten im Ruhezustand aktivieren, um diese Daten zu schützen.
Anhang_I (1.3)	rds-storage-encrypted	Zum Schutz von Daten im Ruhezustand müssen Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon Relational Database Service (Amazon RDS)-Instances aktiviert ist. Da sensible Daten in Amazon-RDS-Instances gespeichert werden können, sollten Sie die Verschlüsselung von Daten im Ruhezustand aktivieren, um diese Daten zu schützen.

Kontroll-ID	AWS Config	Empfehlungen
Anhang_I (1.3)	redshift-cluster-configuration-check	Um Daten im Ruhezustand zu schützen, muss die Verschlüsselung für Ihre Amazon-Redshift-Cluster aktiviert sein. Sie müssen auch sicherstellen, dass die erforderlichen Konfigurationen auf Amazon-Redshift-Clustern bereitgestellt werden. Die Prüfungsprotokollierung muss aktiviert sein, um Informationen zu Verbindungen und Benutzeraktivitäten in der Datenbank bereitzustellen. Diese Regel erfordert, dass ein Wert für clusterDbEncrypted (Config Default: TRUE) und LoggingEnabled (Config Default: TRUE) gesetzt ist. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.
Anhang_I (1.3)	redshift-require-tls-ssl	Stellen Sie sicher, dass Ihre Amazon-Redshift-Cluster eine TLS/SSL-Verschlüsselung erfordern, um eine Verbindung zu SQL-Clients herzustellen. Da sensible Daten vorhanden sein können, sollten Sie die Verschlüsselung bei der Übertragung aktivieren, um diese Daten zu schützen.

Kontroll-ID	AWS Config	Empfehlungen
Anhang_I (1.3)	s3-aktiviert bucket-server-side-encryption	Zum Schutz von Daten im Ruhezustand müssen Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon Simple Storage Service (Amazon S3)-Buckets aktiviert ist. Da sensible Daten in Amazon S3 Buckets gespeichert werden können, sollten Sie die Verschlüsselung aktivieren, um diese Daten zu schützen.
Anhang_I (1.3)	s-3 bucket-ssl-requests-only	Um Daten während der Übertragung zu schützen, stellen Sie sicher, dass Ihre Amazon Simple Storage Service (Amazon S3)-Buckets Anfragen zur Verwendung von Secure Socket Layer (SSL)-Buckets erfordern. Da sensible Daten vorhanden sein können, sollten Sie die Verschlüsselung bei der Übertragung aktivieren, um diese Daten zu schützen.

Kontroll-ID	AWS Config	Empfehlungen
Anhang_I (1.3)	sagemaker-endpoint-configuration-kms-key-konfiguriert	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass die Verschlüsselung mit dem AWS Key Management Service (AWS KMS) für Ihren Endpunkt aktiviert ist. SageMaker Da sensible Daten auf dem SageMaker Endgerät gespeichert werden können, sollten Sie die Verschlüsselung im Ruhezustand aktivieren, um diese Daten zu schützen.
Anhang_I (1.3)	sagemaker-notebook-instance-kms-schlüsselkonfiguriert	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass die Verschlüsselung mit dem AWS Key Management Service (AWS KMS) für Ihr Notebook aktiviert ist. SageMaker Da vertrauliche Daten im SageMaker Notebook gespeichert werden können, sollten Sie die Verschlüsselung im Ruhezustand aktivieren, um diese Daten zu schützen.

Kontroll-ID	AWS Config	Empfehlungen
Anhang_I (1.3)	sns-encrypted-kms	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass Ihre Amazon Simple Notification Service (Amazon SNS) -Themen mit dem AWS Key Management Service (AWS KMS) verschlüsselt werden müssen. Um eventuell vorhandene sensible Daten im Ruhezustand in veröffentlichten Nachrichten zu schützen, muss die Verschlüsselung von Daten im Ruhezustand aktiviert sein.
Anhang_I (1.3)	dms-replication-not-public	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass auf DMS-Replikationsinstanzen nicht öffentlich zugegriffen werden kann. DMS-Replikations-Instances können vertrauliche Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.
Anhang_I (1.3)	ebs-snapshot-public-restorable-überprüfen	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass EBS-Snapshots nicht öffentlich wiederherstellbar sind. EBS-Volume-Snapshots können vertrauliche Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	AWS Config	Empfehlungen
Anhang_I (1.3)	ec-2 instance-no-public-ip	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon Elastic Compute Cloud (Amazon EC2) -Instances nicht öffentlich zugänglich sind. EC2 Amazon-Instances können vertrauliche Informati onen enthalten, und für solche Konten ist eine Zugriffsk ontrolle erforderlich.
Anhang_I (1.3)	elasticsearch-in-vpc-only	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass sich Amazon OpenSearch OpenSearch Service (Service) -Domains innerhalb einer Amazon Virtual Private Cloud (Amazon VPC) befinden. Eine OpenSearch Service-D omain innerhalb einer Amazon VPC ermöglicht die sichere Kommunikation zwischen OpenSearch Service und anderen Services innerhalb der Amazon VPC, ohne dass ein Internet-Gateway, ein NAT-Gerät oder eine VPN-Verbindung erforderlich ist.

Kontroll-ID	AWS Config	Empfehlungen
Anhang_I (1.3)	emr-master-no-public-ip	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon EMR-Cluster-Masterknoten nicht öffentlich zugänglich sind. Amazon-EMR-Cluster-Hauptknoten können vertrauliche Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	AWS Config	Empfehlungen
Anhang_I (1.3)	ec-2 instances-in-vpc	Stellen Sie Amazon Elastic Compute Cloud (Amazon EC2) -Instances innerhalb einer Amazon Virtual Private Cloud (Amazon VPC) bereit, um eine sichere Kommunika tion zwischen einer Instance und anderen Services innerhalb der Amazon VPC zu ermöglichen, ohne dass ein Internet-Gateway, ein NAT-Gerät oder eine VPN-Verbi ndung erforderlich ist. Der gesamte Datenverkehr bleibt sicher in der AWS Cloud. Domains, die sich innerhalb einer VPC befinden, verfügen aufgrund ihrer logischen Isolierung im Vergleich zu Domains mit öffentlic hen Endpunkten über eine zusätzliche Sicherheitsebene. Weisen Sie EC2 Amazon-In stances einer Amazon-VPC zu, um den Zugriff ordnungsg emäß zu verwalten.

Kontroll-ID	AWS Config	Empfehlungen
Anhang_I (1.3)	autoscaling-launch-config-public-ip-deaktiviert	Wenn Sie Ihre Netzwerkschnittstellen mit einer öffentlichen IP-Adresse konfigurieren, sind die diesen Netzwerkschnittstellen zugehörigen Ressourcen über das Internet erreichbar. EC2 Ressourcen sollten nicht öffentlich zugänglich sein, da dies einen unbeabsichtigten Zugriff auf Ihre Anwendungen oder Server ermöglichen kann.
Anhang_I (1.3)	no-unrestricted-route-to-igw	Stellen Sie sicher, dass EC2 Amazon-Routentabellen keine uneingeschränkten Routen zu einem Internet-Gateway enthalten. Durch das Entfernen oder Beschränken des Internetzugangs für Workloads innerhalb von Amazon VPCs können unbeabsichtigte Zugriffe in Ihrer Umgebung reduziert werden.

Kontroll-ID	AWS Config	Empfehlungen
Anhang_I (1.3)	redshift-cluster-kms-enabled	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass die Verschlüsselung mit AWS Key Management Service (AWS KMS) für Ihren Amazon Redshift Redshift-Cluster aktiviert ist. Um eventuell vorhandene sensible Daten im Ruhezustand in Redshift-Clustern zu schützen, muss die Verschlüsselung von Daten im Ruhezustand aktiviert sein.
Anhang_I (1.3)	ssm-document-not-public	Stellen Sie sicher, dass AWS Systems Manager (SSM) - Dokumente nicht öffentlich sind, da dies einen unbeabsichtigten Zugriff auf Ihre SSM-Dokumente ermöglichen kann. Ein öffentliches SSM-Dokument kann Informationen über Ihr Konto, Ihre Ressourcen und internen Prozesse preisgeben.

Kontroll-ID	AWS Config	Empfehlungen
Anhang_I (1.3)	subnet-auto-assign-public-ip-deaktiviert	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon Virtual Private Cloud (VPC) -Subnetzen nicht automatisch eine öffentliche IP-Adresse zugewiesen wird. Amazon Elastic Compute Cloud (EC2) -Instances, die in Subnetzen gestartet werden, in denen dieses Attribut aktiviert ist, haben ihrer primären Netzwerkschnittstelle eine öffentliche IP-Adresse zugewiesen.
Anhang_I (1.3)	internet-gateway-authorized-vpc-nur	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Internet-Gateways nur mit autorisierter Amazon Virtual Private Cloud (Amazon VPC) verbunden sind. Internet-Gateways ermöglichen den bidirektionalen Internetzugang zur und von der Amazon VPC, was möglicherweise zu einem unbefugten Zugriff auf Amazon-VPC-Ressourcen führen kann.

Kontroll-ID	AWS Config	Empfehlungen
Anhang_I (1.3)	lambda-function-public-access-verboten	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass AWS Lambda-Funktionen nicht öffentlich zugänglich sind. Der öffentliche Zugriff kann möglicherweise die Verfügbarkeit von Ressourcen beeinträchtigen.

Kontroll-ID	AWS Config	Empfehlungen
Anhang_I (1.3)	lambda-inside-vpc	Stellen Sie AWS Lambda-Funktionen in einer Amazon Virtual Private Cloud (Amazon VPC) bereit, um eine sichere Kommunikation zwischen einer Funktion und anderen Diensten innerhalb der Amazon VPC zu gewährleisten. Bei dieser Konfiguration sind kein Internet-Gateway, kein NAT-Gerät und keine VPN-Verbindung erforderlich. Der gesamte Datenverkehr bleibt sicher in der Cloud. AWS Domains, die sich innerhalb einer VPC befinden, verfügen aufgrund ihrer logischen Isolierung im Vergleich zu Domains mit öffentlichen Endpunkten über eine zusätzliche Sicherheitsebene. Um den Zugriff ordnungsgemäß zu verwalten, sollten AWS Lambda-Funktionen einer VPC zugewiesen werden.

Kontroll-ID	AWS Config	Empfehlungen
Anhang_I (1.3)	rds-instance-public-access-überprüfen	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Relational Database Service (Amazon RDS) -Instances nicht öffentlich sind. Amazon-RDS-Datenbank-Instances können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.
Anhang_I (1.3)	rds-snapshots-public-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Relational Database Service (Amazon RDS) -Instances nicht öffentlich sind. Amazon-RDS-Datenbank-Instances können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	AWS Config	Empfehlungen
Anhang_I (1.3)	redshift-cluster-public-access-überprüfen	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Redshift Redshift-Cluster nicht öffentlich sind. Amazon-Redshift-Cluster können vertrauliche Informationen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.
Anhang_I (1.3)	restricted-common-ports	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass gemeinsame Ports für Amazon Elastic Compute Cloud (Amazon EC2) - Sicherheitsgruppen eingeschränkt sind. Wenn der Zugriff auf Ports nicht auf vertrauenswürdige Quellen beschränkt wird, kann dies zu Angriffen auf die Verfügbarkeit, Integrität und Vertraulichkeit von Systemen führen. Mit dieser Regel können Sie optional die Parameter blockedPort1–blockedPort5 festlegen (Standardkonfigurationen: 20, 21, 3389, 3306, 4333). Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	AWS Config	Empfehlungen
Anhang_I (1.3)	s3 bucket-level-public-access - verboten	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherste llen, dass Amazon Simple Storage Service (Amazon S3) -Buckets nicht öffentlich zugänglich sind. Diese Regel trägt dazu bei, sensible Daten vor unbefugten Remote-Be nutzern zu schützen, indem sie den öffentlichen Zugriff auf Bucket-Ebene verhindert.

Kontroll-ID	AWS Config	Empfehlungen
Anhang_I (1.3)	s3- -Block-periodisch account-level-public-access	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Simple Storage Service (Amazon S3) -Buckets nicht öffentlich zugänglich sind. Diese Regel trägt dazu bei, sensible Daten vor unbefugten Remote-Benutzern zu schützen, indem sie den öffentlichen Zugriff verhindert. Mit dieser Regel können Sie optional die Parameter ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) und restrictPublicBuckets Parameter (Config Default: True) festlegen. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	AWS Config	Empfehlungen
Anhang_I (1.3)	s3- bucket-public-read-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie nur autorisierten Benutzern, Prozessen und Geräten Zugriff auf Amazon Simple Storage Service (Amazon S3) -Buckets gewähren. Die Verwaltung des Zugriffs sollte mit der Klassifizierung der Daten übereinstimmen.
Anhang_I (1.3)	s3- bucket-public-write-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie nur autorisierten Benutzern, Prozessen und Geräten Zugriff auf Amazon Simple Storage Service (Amazon S3) -Buckets gewähren. Die Verwaltung des Zugriffs sollte mit der Klassifizierung der Daten übereinstimmen.
Anhang_I (1.3)	sagemaker-notebook-no-direct-Internetzugang	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass SageMaker Amazon-Notebooks keinen direkten Internetzugang zulassen. Indem Sie direkten Internetzugang blockieren, vermeiden Sie, dass unbefugte Benutzer auf sensible Daten zugreifen.

Kontroll-ID	AWS Config	Empfehlungen
Anhang_I (5.1)	alb-waf-enabled	Stellen Sie sicher, dass AWS WAF auf Elastic Load Balancers (ELB) aktiviert ist, um Webanwendungen zu schützen. Eine WAF trägt zum Schutz Ihrer Webanwend ungen oder APIs vor gängigen Web-Exploits bei. Diese Web-Exploits können sich auf die Verfügbarkeit auswirken, die Sicherheit gefährden oder übermäßige Ressourcen in Ihrer Umgebung verbrauchen.
Anhang_I (5.1)	vpc-default-security-group-geschlossen	Sicherheitsgruppen von Amazon Elastic Compute Cloud (Amazon EC2) können bei der Verwaltung des Netzwerkzugriffs helfen, indem sie eine statusbeh aftete Filterung des ein- und ausgehenden Netzwerkv erkehrs zu Ressourcen bereitstellen. AWS Die Beschränkung des gesamten Datenverkehrs auf die Standardsicherheitsgruppe hilft dabei, den Fernzugriff auf Ihre Ressourcen einzuschr änken. AWS

Kontroll-ID	AWS Config	Empfehlungen
Anhang_I (5.1)	waf-regional-rule-not-leer	Stellen Sie sicher, dass Ihre AWS WAF eine Regel hat, die nicht leer ist. Eine Regel ohne Bedingungen kann zu unbeabsichtigtem Verhalten führen.
Anhang_I (5.1)	waf-regional-rulegroup-not-leer	Stellen Sie sicher, dass Ihre AWS WAF eine Regelgrup pe hat, die nicht leer ist. Eine leere Regelgruppe kann zu unbeabsichtigtem Verhalten führen.
Anhang_I (5.1)	waf-regional-webacl-not-leer	Eine an eine AWS WAF angehängte Web-ACL kann eine Sammlung von Regeln und Regelgruppen zur Überprüfung und Steuerung von Webanfragen enthalten . Wenn eine Web-ACL leer ist, wird der Webdatenverkehr weitergeleitet, ohne von der WAF erkannt oder bearbeitet zu werden.

Kontroll-ID	AWS Config	Empfehlungen
Anhang_I (5.1)	vpc-sg-open-only-to-authorized-ports	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass gemeinsame Ports für Amazon Elastic Compute Cloud (Amazon EC2) - Sicherheitsgruppen eingeschränkt sind. Wenn der Zugriff auf Ports nicht auf vertrauenswürdige Quellen beschränkt wird, kann dies zu Angriffen auf die Verfügbarkeit, Integrität und Vertraulichkeit von Systemen führen. Durch die Beschränkung des Zugriffs auf Ressourcen innerhalb einer Sicherheitsgruppe aus dem Internet (0.0.0.0/0) kann der Fernzugriff auf interne Systeme gesteuert werden.

Kontroll-ID	AWS Config	Empfehlungen
Anhang_I (5.1)	api-gw-associated-with-WAF	AWS Mit WAF können Sie eine Reihe von Regeln (als Web Access Control List (Web ACL) bezeichnet) konfiguri eren, die Webanfragen auf der Grundlage von anpassbar en Websicherheitsregeln und -bedingungen, die Sie definieren, zulassen, blockiere n oder zählen. Stellen Sie sicher, dass Ihre Amazon-API-Gateway-Stufe mit einer WAF-Web-ACL verknüpft ist, um sie vor böswilligen Angriffen zu schützen.
Anhang_I (5.1)	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) Security Groups können bei der Verwaltung des Netzwerkz ugriffs helfen, indem sie eine statusbehaftete Filterung von eingehendem und ausgehend em Netzwerkverkehr zu Ressourcen bereitstellen. AWS Wenn Sie eingehenden (oder entfernten) Datenverk ehr von 0.0.0.0/0 bis Port 22 auf Ihren Ressourcen nicht zulassen, können Sie den Remote-Zugriff einschränken.

Kontroll-ID	AWS Config	Empfehlungen
Anhang_I (5.1)	restricted-common-ports	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass gemeinsame Ports für Amazon Elastic Compute Cloud (Amazon EC2) - Sicherheitsgruppen eingeschränkt sind. Wenn der Zugriff auf Ports nicht auf vertrauenswürdige Quellen beschränkt wird, kann dies zu Angriffen auf die Verfügbarkeit, Integrität und Vertraulichkeit von Systemen führen. Mit dieser Regel können Sie optional die Parameter blockedPort1–blockedPort5 festlegen (Standardkonfigurationen: 20, 21, 3389, 3306, 4333). Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	AWS Config	Empfehlungen
Anhang_I (6)	ec2-check managedinstance-association-compliance-status	Verwenden Sie AWS Systems Manager Associations, um bei der Inventarisierung von Softwareplattformen und Anwendungen innerhalb eines Unternehmens zu helfen. AWS Systems Manager weist Ihren verwalteten Instanzen einen Konfigurationsstatus zu und ermöglicht es Ihnen, Basiswerte für Betriebss ystem-Patch-Levels, Softwarei nstallationen, Anwendung skonfigurationen und andere Details zu Ihrer Umgebung festzulegen.
Anhang_I (6)	ec2-check managedinstance-patch-compliance-status	Aktivieren Sie diese Regel, um bei der Identifizierung und Dokumentation von Sicherhei tslücken in Amazon Elastic Compute Cloud (Amazon EC2) zu helfen. Die Regel prüft, ob die EC2 Amazon-In stance die Patch-Konformität im AWS Systems Manager gemäß den Richtlinien und Verfahren Ihrer Organisation einhält.

Kontroll-ID	AWS Config	Empfehlungen
Anhang_I (6)	guardduty-non-archived-findings	Amazon GuardDuty hilft Ihnen dabei, die Auswirkungen eines Vorfalls zu verstehen, indem es die Ergebnisse nach Schweregrad klassifiziert: niedrig, mittel und hoch. Diese Klassifizierungen können Sie zur Festlegung von entsprechenden Strategien und Prioritäten zur Behebung solcher Vorfälle verwenden. Mit dieser Regel können Sie optional daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7) und daysHighSev (Config Default: 1) für nicht archivierte Ergebnisse festlegen, wie es die Richtlinien Ihrer Organisation erfordern.
Anhang_I (6)	elastic-beanstalk-managed-updates-aktiviert	Durch die Aktivierung verwalteter Plattformupdates für eine Amazon-Elastic-Beanstalk-Umgebung wird sichergestellt, dass die aktuellen verfügbaren Plattform-Fixes, -Updates und -Features für die Umgebung installiert sind. Eine bewährte Methode zur Sicherung von Systemen besteht darin, stets die aktuellen Patches zu installieren.

Kontroll-ID	AWS Config	Empfehlungen
Anhang_I (6)	rds-automatic-minor-version-upgrade-fähig	Aktivieren Sie automatische Unterversions-Upgrades auf Ihren Amazon-Relational-Database-Service (RDS)-Instances, um sicherzustellen, dass die aktuellen Updates für Unterversionen des Relational Database Management System (RDBMS) installiert sind, die Sicherheitspatches und Bugfixes enthalten können.

Kontroll-ID	AWS Config	Empfehlungen
Anhang_I (6)	redshift-cluster-maintenancesettings-check	Diese Regel stellt sicher, dass Amazon-Redshift-Cluster die bevorzugten Einstellungen für Ihre Organisation haben. Insbesondere sorgt sie dafür, dass Cluster bevorzugte Wartungsfenster und automatisierte Aufbewahrungsfristen für Snapshots für die Datenbank haben. Für diese Regel müssen Sie die festlegen. allowVersionUpgrade Der Standardwert ist „true“. Außerdem können Sie optional den Zeitraum preferredMaintenanceWindow (der Standardwert ist sa: 16:00 -sa: 16:30) und den automatedSnapshotRetention Zeitraum (der Standardwert ist 1) festlegen. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.
Anhang_I (6)	vuln-management-plan-exists (Prozessüberprüfung)	Stellen Sie sicher, dass ein Plan für das Schwachstellenmanagement entwickelt und implementiert wird, damit Sie über formell definierte Prozesse zur Behebung von Schwachstellen in Ihrer Umgebung verfügen.

Kontroll-ID	AWS Config	Empfehlungen
Anhang_I (7.1)	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) kann Ihnen dabei helfen, die Prinzipien der geringsten Rechte und der Aufgabent rennung in Zugriffsberechtigu ngen und Autorisierungen zu integrieren und so zu verhindern, dass Richtlinien „Effect“: „Allow“ mit „Action“: „*“ anstelle von „Resource“: „*“ enthalten. Wenn Benutzern mehr Rechte eingeräumt werden, als für die Ausführun g einer Aufgabe erforderl ich sind, kann dies gegen das Prinzip der geringste n Berechtigung und der Aufgabentrennung verstoßen.
Anhang_I (7.1)	iam-policy-no-statements-with-full-access	Stellen Sie sicher, dass IAM-Aktionen nur auf die benötigte n Aktionen beschränkt sind. Wenn Benutzern mehr Rechte eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Rechte und der Aufgabentrennung verstoßen.

Kontroll-ID	AWS Config	Empfehlungen
Anhang_I (7.1)	iam-root-access-key-überprüfen	Der Zugriff auf Systeme und Ressourcen kann gesteuert werden, indem überprüft wird, ob der Root-Benutzer keine Zugriffsschlüssel mit seiner AWS Identity and Access Management (IAM) -Rolle verknüpft hat. Stellen Sie sicher, dass die Root-Zugriffsschlüssel gelöscht werden. Erstellen und verwenden Sie stattdessen rollenbasierte Funktionen, AWS-Konten um das Prinzip der geringsten Funktionalität zu berücksichtigen.
Anhang_I (7.1)	iam-user-no-policies-überprüfen	Diese Regel stellt sicher, dass AWS Identity and Access Management (IAM) -Richtlinien nur Gruppen oder Rollen zugewiesen werden, um den Zugriff auf Systeme und Ressourcen zu kontrollieren. Die Zuweisung von Berechtigungen auf Gruppen- oder Rollenebene trägt dazu bei, die Wahrscheinlichkeit zu verringern, dass eine Identität übermäßige Berechtigungen erhält oder beibehält.

Kontroll-ID	AWS Config	Empfehlungen
Anhang_I (7.1)	iam-no-inline-policy-überprüfen	Stellen Sie sicher, dass ein Benutzer, eine IAM-Rolle oder eine IAM-Gruppe (AWS Identity and Access Management) nicht über eine Inline-Richtlinie zur Zugriffskontrolle auf Systeme und Ressourcen verfügt. AWS empfiehlt, verwaltete Richtlinien anstelle von Inline-Richtlinien zu verwenden . Verwaltete Richtlinien ermöglichen Wiederverwendbarkeit, Versionsverwaltung, Rollback und Delegierung der Berechtigungsverwaltung.

Kontroll-ID	AWS Config	Empfehlungen
Anhang_I (7.2)	iam-password-policy	Die Identitäten und Anmeldein formationen werden auf der Grundlage einer organisat orischen IAM-Passwortrichtl inie ausgestellt, verwaltet und verifiziert. Sie erfüllen oder übertreffen die Anforderungen von NIST SP 800-63 und dem Standard „Best Practices“ von AWS Foundational Security für die Passwortstärke. Mit dieser Regel können Sie optional RequireUppercaseCharacters (Wert für AWS grundlege nde Sicherheitsbewährte Verfahren: wahr), RequireLo wercaseCharacters (Wert für bewährte Methoden für AWS grundlegende Sicherheit: wahr), RequireSymbols (Wert für bewährte Methoden für AWS grundlegende Sicherhei t: wahr), RequireNumbers (Wert für bewährte Methoden für AWS grundlegende Sicherheit: wahr), MinimumPa sswordLength (Wert für bewährte Methoden für AWS grundlegende Sicherheit: 14), PasswordReusePreve ntion (Wert für bewährte Methoden für AWS grundlege nde Sicherheit: 24) und MaxPasswordAge (Wert

Kontroll-ID	AWS Config	Empfehlungen
		für bewährte Methoden für AWS grundlegende Sicherhei t: 90) für Ihr IAM festlegen Kennwortrichtlinie. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisat ion entsprechen.
Anhang_I (7.3)	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) Security Groups können bei der Verwaltung des Netzwerkz ugriffs helfen, indem sie eine statusbehaftete Filterung von eingehendem und ausgehend em Netzwerkverkehr zu Ressourcen bereitstellen. AWS Wenn Sie eingehenden (oder entfernten) Datenverk ehr von 0.0.0.0/0 bis Port 22 auf Ihren Ressourcen nicht zulassen, können Sie den Remote-Zugriff einschränken.
Anhang_I (7.4)	api-gw-execution-logging-ak tiviert	Die API-Gateway-Protok ollierung zeigt detaillierte Ansichten der Benutzer, die auf die API zugegriffen haben, und wie diese Benutzer auf die API zugegriffen haben. Diese Insights ermöglichen die Einsicht in Benutzeraktivitäten.

Kontroll-ID	AWS Config	Empfehlungen
Anhang_I (7.4)	cloud-trail-cloud-watch-logs-aktiviert	Verwenden Sie Amazon CloudWatch , um Protokoll ereignisaktivitäten zentral zu sammeln und zu verwalten . Die Aufnahme von AWS CloudTrail Daten liefert Einzelheiten zu den API-Aufru faktivitäten in Ihrem AWS-Konto.
Anhang_I (7.4)	cloudtrail-enabled	AWS CloudTrail kann bei der Nichtabstreitbarkeit helfen, indem Aktionen und API-Aufrufe der AWS Managemen t Console aufgezeichnet werden. Sie können die Benutzer und die Benutzer AWS-Konten , die einen AWS Dienst aufgerufen haben, die Quell-IP-Adresse, über die die Aufrufe generiert wurden, und den Zeitpunkt der Anrufe identifizieren. Einzelheiten zu den erfassten Daten finden Sie in den AWS CloudTrail Datensatzinhalten.

Kontroll-ID	AWS Config	Empfehlungen
Anhang_I (7.4)	cloudtrail-s3-dataevents-enabled	Die Erfassung von Simple Storage Service (Amazon S3)-Datenereignissen unterstützt die Erkennung von ungewöhnlichen Aktivitäten. Zu den Details gehören AWS-Konto Informationen über den Zugriff auf einen Amazon S3 S3-Bucket, die IP-Adresse und die Uhrzeit des Ereignisses.
Anhang_I (7.4)	elasticsearch-logs-to-cloudwatch	Stellen Sie sicher, dass für Amazon OpenSearch Service-Domains Fehlerprotokolle aktiviert und zur Aufbewahrung und Beantwortung an Amazon CloudWatch Logs gestreamt werden. Domain-Fehlerprotokolle sind bei Sicherheits- und Zugriffsprüfungen sowie bei der Diagnose von Verfügbarkeitsproblemen nützlich.

Kontroll-ID	AWS Config	Empfehlungen
Anhang_I (7.4)	securityhub-enabled	AWS Security Hub hilft bei der Überwachung von unbefugte m Personal, Verbindungen, Geräten und Software. AWS Security Hub aggregiert, organisiert und priorisiert die Sicherheitswarnungen oder Ergebnisse mehrerer Dienste. AWS Einige dieser Dienste sind Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer und AWS Firewall Manager sowie AWS Partnerlösungen.
Anhang_I (7.4)	cw-loggroup-retention-period-überprüfen	Stellen Sie sicher, dass die Ereignisprotokolldaten für Ihre Protokollgruppen über eine Mindestdauer aufbewahrt werden, um die Fehlerbehebung und forensische Untersuch ungen zu unterstützen. Fehlende frühere Ereignisp rotokolldaten erschweren die Rekonstruierung und Identifiz ierung potenziell schädlicher Ereignisse.

Kontroll-ID	AWS Config	Empfehlungen
Anhang_I (7.4)	elb-logging-enabled	Die Elastic-Load-Balancing-Aktivität ist ein zentraler Kommunikationspunkt innerhalb einer Umgebung. Stellen Sie sicher, dass die ELB-Protokollierung aktiviert ist. Die gesammelten Daten enthalten detaillierte Informati onen zu Anfragen, die an den ELB gesendet wurden. Jedes Protokoll enthält Informati onen wie die Zeit, zu der die Anforderung einging, die Client-IP-Adresse, Latenzen, Anforderungspfade und Serverantworten.
Anhang_I (7.4)	codebuild-project-logging-e nabled	Stellen Sie sicher, dass die AWS CodeBuild Projektpr otokollierung aktiviert ist, damit Ihre Build-Ausgabeproto kolle entweder an Amazon CloudWatch oder Amazon Simple Storage Service (Amazon S3) gesendet werden. Build-Ausgabeproto kolle enthalten detaillierte Informationen zu Ihrem Build-Projekt.

Kontroll-ID	AWS Config	Empfehlungen
Anhang_I (7.4)	opensearch-audit-logging-enabled	Stellen Sie sicher, dass die Audit-Protokollierung für Ihre Amazon OpenSearch Service-Domains aktiviert ist. Mit der Audit-Protokollierung können Sie Benutzeraktivitäten auf Ihren OpenSearch Domains verfolgen, einschließlich erfolgreicher und fehlgeschlagener Authentifizierungen OpenSearch, Anfragen an, Indexänderungen und eingehende Suchanfragen.
Anhang_I (7.4)	opensearch-logs-to-cloudwatch	Stellen Sie sicher, dass für Amazon OpenSearch Service-Domains Fehlerprotokolle aktiviert und zur Aufbewahrung und Beantwortung an Amazon CloudWatch Logs gestreamt werden. OpenSearch Service-Fehlerprotokolle können bei Sicherheits- und Zugriffsprüfungen helfen und bei der Diagnose von Verfügbarkeitsproblemen helfen.
Anhang_I (7.4)	redshift-audit-logging-enabled	Aktivieren Sie die Prüfungsprotokollierung, um Informationen über Verbindungen und Benutzeraktivitäten in Ihrem Amazon-Redshift-Cluster zu erfassen.

Kontroll-ID	AWS Config	Empfehlungen
Anhang_I (7.4)	multi-region-cloudtrail-enabled	AWS CloudTrail zeichnet Aktionen und API-Aufrufe der AWS Management Console auf. Sie können feststellen, welche Benutzer und Konten angerufen wurden AWS, von welcher Quell-IP-Adresse aus die Anrufe getätigt wurden und wann die Anrufe erfolgten . CloudTrail übermittelt Protokolldateien aus allen AWS Regionen an Ihren S3-Bucket, wenn MULTI_REG ION_CLOUD_TRAIL_EN ABLED aktiviert ist. Außerdem wird beim AWS Start einer neuen Region derselbe Trail in der neuen Region erstellt. CloudTrail Dadurch erhalten Sie automatisch Protokoll dateien mit API-Aktivitäten für die neue Region.

Kontroll-ID	AWS Config	Empfehlungen
Anhang_I (7.4)	rds-logging-enabled	Um die Protokollierung und Überwachung in Ihrer Umgebung zu erleichtern, stellen Sie sicher, dass die Amazon Relational Database Service (Amazon RDS)-Protokollierung aktiviert ist. Mit der Amazon-RDS-Protokollierung können Sie Ereignisse wie Verbindungen, Verbindungsabbrüche, Abfragen oder abgefragte Tabellen erfassen.
Anhang_I (7.4)	s-3 bucket-logging-enabled	Die Amazon Simple Storage Service (Amazon S3)-Serverzugriffsprotokollierung bietet eine Methode zur Überwachung des Netzwerks im Hinblick auf potenzielle Cybersicherheitsereignisse. Die Ereignisse werden überwacht, indem detaillierte Aufzeichnungen über die Anfragen erfasst werden, die an einen Amazon-S3-Bucket gestellt wurden. Jeder Zugriffsprotokolleintrag enthält Details zu einer einzelnen Zugriffsanfrage. Zu den Details gehören Anforderer, Bucket-Name, Anforderungszeit, Anforderungsaktion, Antwortstatus und Fehlercode, falls relevant.

Kontroll-ID	AWS Config	Empfehlungen
Anhang_I (7.4)	vpc-flow-logs-enabled	VPC-Flow-Protokolle erfassen detaillierte Informationsdatensätze über den IP-Datenverkehr, der zu und von Netzwerkschnittstellen in Ihrer Amazon Virtual Private Cloud (Amazon VPC) fließt. Standardmäßig enthalten Flow-Protokolldatensätze Werte für die verschiedenen Komponenten des IP-Flows, einschließlich Quelle, Ziel und Protokoll.
Anhang_I (7.4)	wafv2-logging-enabled	Um die Protokollierung und Überwachung in Ihrer Umgebung zu erleichtern, aktivieren Sie die AWS WAF (V2) -Protokollierung im regionalen und globalen Web ACLs. AWS Die WAF-Protokollierung bietet detaillierte Informationen über den Datenverkehr, der von Ihrer Web-ACL analysiert wird. In den Protokollen werden die Uhrzeit aufgezeichnet, zu der die AWS WAF die Anfrage von Ihrer AWS Ressource erhalten hat, Informationen über die Anfrage und eine Aktion für die Regel, der jede Anfrage entsprach.

Kontroll-ID	AWS Config	Empfehlungen
Anhang_I (7.4)	redshift-cluster-configuration-check	Um Daten im Ruhezustand zu schützen, muss die Verschlüsselung für Ihre Amazon-Redshift-Cluster aktiviert sein. Sie müssen auch sicherstellen, dass die erforderlichen Konfigurationen auf Amazon-Redshift-Clustern bereitgestellt werden. Die Prüfungsprotokollierung muss aktiviert sein, um Informationen zu Verbindungen und Benutzeraktivitäten in der Datenbank bereitzustellen. Diese Regel erfordert, dass ein Wert für clusterDbEncrypted (Config Default: TRUE) und LoggingEnabled (Config Default: TRUE) gesetzt ist. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.
Anhang_I (10.2)	security-awareness-program-exists (Prozessüberprüfung)	Etablieren und pflegen Sie ein Programm zur Förderung des Sicherheitsbewusstseins in Ihrer Organisation. Programme zur Förderung des Sicherheitsbewusstseins der Mitarbeiter vermitteln ihnen, wie sie die Organisation vor diversen Sicherheitsverletzungen oder Sicherheitsvorfällen schützen können.

Kontroll-ID	AWS Config	Empfehlungen
Anhang_I (12)	db-instance-backup-enabled	Die Sicherungsfunktion von Amazon RDS erstellt Sicherungen Ihrer Datenbank en und Transaktionsprotokolle. Amazon RDS erstellt einen Snapshot für das Speicherv olume Ihrer DB-Instance, sodass die gesamte DB-Instance gesichert wird. Sie können im System spezifisc he Aufbewahrungsfristen festlegen, um Ihre Ausfallsi cherheitsanforderungen zu erfüllen.
Anhang_I (12)	dynamodb-in-backup-plan	Um Sie bei Datensich erungsprozessen zu unterstüt zen, stellen Sie sicher, dass Ihre Amazon DynamoDB-Tabellen Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherung smanagement und erleichte rt Ihnen die Erfüllung von geschäftlichen und behördlic hen Compliance-Anforde rungen hinsichtlich Datensich erungen.

Kontroll-ID	AWS Config	Empfehlungen
Anhang_I (12)	dynamodb-pitr-enabled	Aktivieren Sie diese Regel, um zu überprüfen, ob die Informationen gesichert wurden. Es verwaltet auch die Backups, indem es sicherste llt, dass die point-in-time Wiederherstellung in Amazon DynamoDB aktiviert ist. Bei der Wiederherstellung werden fortlaufende Backups Ihrer Tabelle für die letzten 35 Tage gespeichert.
Anhang_I (12)	ebs-in-backup-plan	Stellen Sie zur Unterstützung der Datensicherungsprozesse sicher, dass Ihre Amazon Elastic Block Store (Amazon EBS) -Volumes Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherung smanagement und erleichte rt Ihnen die Erfüllung von geschäftlichen und behördlic hen Compliance-Anforde rungen hinsichtlich Datensich erungen.

Kontroll-ID	AWS Config	Empfehlungen
Anhang_I (12)	efs-in-backup-plan	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon Elastic File System (Amazon EFS) - Dateisysteme Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	AWS Config	Empfehlungen
Anhang_I (12)	aurora-resources-protected-by-Backup-Plan	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon Aurora Aurora-Ressourcen Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	AWS Config	Empfehlungen
Anhang_I (12)	backup-plan-min-frequency-and-min-retention-check	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihr AWS Backup-Plan auf eine Mindestfrequenz und Aufbewahrung festgelegt ist. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen. Mit dieser Regel können Sie die Parameter requiredFrequencyValue (Config default: 1), requiredRetentionDays (Config default: 35) und requiredFrequencyUnit (Config default: days) festlegen. Der tatsächliche Wert muss den Anforderungen Ihrer Organisation entsprechen.

Kontroll-ID	AWS Config	Empfehlungen
Anhang_I (12)	elasticache-redis-cluster-automatic-backup-check	Wenn automatische Backups aktiviert sind, ElastiCache erstellt Amazon täglich ein Backup des Clusters. Die Sicherung kann für eine von Ihrer Organisation festgelegte Anzahl von Tagen aufbewahrt werden. Automatische Backups schützen vor Datenverlust. Bei einem Ausfall können Sie einen neuen Cluster erstellen, der Ihre Daten aus dem aktuellen Backup wiederherstellt.
Anhang_I (12)	redshift-backup-enabled	Stellen Sie zur Unterstützung der Datensicherungsprozesse sicher, dass Ihre Amazon-Redshift-Cluster über automatisierte Snapshots verfügen. Wenn automatisierte Snapshots für einen Cluster aktiviert sind, erstellt Redshift in regelmäßigen Abständen Snapshots dieses Clusters. Standardmäßig erstellt Redshift alle acht Stunden oder alle 5 GB einen Snapshot für jeden Knoten mit Datenänderungen oder je nachdem, was zuerst eintritt.

Kontroll-ID	AWS Config	Empfehlungen
Anhang_I (12)	rds-in-backup-plan	Um Sie bei Datensich erungsprozessen zu unterstüt zen, stellen Sie sicher, dass Ihre Amazon Relational Database Service (Amazon RDS) -Instances Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherung smanagement und erleichte rt Ihnen die Erfüllung von geschäftlichen und behördlic hen Compliance-Anforde rungen hinsichtlich Datensich erungen.
Anhang_I (12)	s-3 bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) unterstützt die Aufrechte rhaltung einer angemessenen Kapazität und Verfügbarkeit. CRR ermöglicht das automatis che, asynchrone Kopieren von Objekten in Amazon S3 Buckets, um die Datenverf ügbarkeit sicherzustellen.

Kontroll-ID	AWS Config	Empfehlungen
Anhang_I (12)	s-3 bucket-versioning-enabled	Die Versionsverwaltung von Amazon Simple Storage Service (Amazon S3)-Buckets hilft dabei, mehrere Varianten eines Objekts im selben Amazon-S3-Bucket zu speichern. Verwenden Sie die Versionsverwaltung, um sämtliche Versionen aller Objekte in Ihrem Amazon-S3-Bucket zu speichern, abzurufen oder wiederher zustellen. Mit der Versionsv erwaltung können Sie Versionen sowohl nach unbeabsichtigten Benutzera ktionen als auch nach Anwendungsfehlern problemlo s wiederherstellen.

Vorlage

Die Vorlage ist verfügbar unter GitHub: Operational Best Practices for RBI Cyber Security Framework für UCBs.

Bewährte Methoden für die Ausführung von RBI MD-ITF

Konformitätspakete bieten ein allgemeines Compliance-Framework, das es Ihnen ermöglicht, mithilfe verwalteter oder benutzerdefinierter Regeln und Abhilfemaßnahmen Kontrollen zur Sicherheits-, Betriebs- oder Kostenoptimierung durchzuführen. AWS Config AWS Config Conformance Packs dienen als Beispielvorlagen nicht dazu, die vollständige Einhaltung eines bestimmten Governance- oder Compliance-Standards sicherzustellen. Sie sind dafür verantwortlich, selbst zu beurteilen, ob Ihre Nutzung der Services den geltenden gesetzlichen und behördlichen Anforderungen entspricht.

Im Folgenden finden Sie ein Beispiel für eine Zuordnung zwischen der Master Direction — Information Technology Framework der Reserve Bank of Indien (RBI) und den AWS verwalteten Konfigurationsregeln. Jede Config-Regel gilt für eine bestimmte AWS Ressource und bezieht sich auf eine oder mehrere RBI Master Direction — Information Technology Framework-Steuerelemente. Eine RBI Master Direction — Information Technology Framework-Steuerung kann mit mehreren Konfigurationsregeln verknüpft werden. In der folgenden Tabelle finden Sie weitere Informationen und Anleitungen zu diesen Zuordnungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.1(a)	Identifizierung und Klassifizierung von Informationswerten.	ec2-manager instance-managed-by-systems	Eine Bestandsaufnahme der Softwareplattformen und Anwendungen innerhalb des Unternehmens ist möglich, indem Amazon Elastic Compute Cloud (Amazon EC2) - Instances mit AWS Systems Manager verwaltet werden. Verwenden Sie AWS Systems Manager, um detaillierte Systemkonfigurationen, Betriebssystem-Patch-Levels, Namen und Typ der Dienste, Softwareinstallationen, Anwendungsname, Herausgeber und Version sowie andere Details zu

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			Ihrer Umgebung bereitzustellen.
3.1(a)	Identifizierung und Klassifizierung von Informationswerten.	ec2-stopped-instance	Aktivieren Sie diese Regel, um bei der Basiskonfiguration von Amazon Elastic Compute Cloud (Amazon EC2) - Instances zu helfen, indem Sie überprüfe n, ob EC2 Amazon-Instances gemäß den Standards Ihrer Organisation für mehr als die zulässige Anzahl von Tagen gestoppt wurden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.1(a)	Identifizierung und Klassifizierung von Informationswerten.	ec2- volume-inuse-check	Diese Regel stellt sicher, dass Amazon Elastic Block Store-Volumes, die an Amazon Elastic Compute Cloud (Amazon EC2) - Instances angehängt sind, zum Löschen markiert werden, wenn eine Instance beendet wird. Wenn ein Amazon-EB S-Volume nicht gelöscht wird, wenn die Instance, an die es angehängt ist, beendet wird, kann dies gegen das Konzept der geringsten Funktiona lität verstoßen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.1(a)	Identifizierung und Klassifizierung von Informationswerten.	ecr-private-tag-immutability-aktiviert	Aktivieren Sie die Unveränderlichkeit von Tags im Elastic Container Repository (ECR), um zu verhindern, dass Image-Tags in Ihren ECR-Images überschrieben werden. Bisher konnten Tags überschrieben werden, was manuelle Methoden zur eindeutigen Identifizierung eines Images erforderte.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.1(c)	Rollenbasierte Zugriffssteuerung	access-keys-rotated	Die Anmeldein formationen für autorisierte Geräte, Benutzer und Prozesse werden geprüft, indem sichergestellt wird, dass die IAM-Zugri ffsschlüssel entsprech end den Vorgaben der Unternehmensrichtl inie rotiert werden. Das regelmäßi ge Ändern der Zugriffsschlüssel ist eine bewährte Sicherheitsmethode . Es verkürzt den Zeitraum, in dem ein Zugriffsschlüssel aktiv ist, und reduziert die Auswirkungen auf das Unternehmen, wenn die Schlüssel kompromittiert werden. Diese Regel erfordert einen Wert für die Zugriffsschlüssel-Rotation (Standard konfiguration: 90). Der tatsächliche Wert muss den Richtlini

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			en Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.1(c)	Rollenbasierte Zugriffssteuerung	emr-kerberos-enabled	Die Zugriffsberechtigungen und -autorisierungen können verwaltet und nach den Prinzipien der geringsten Berechtigung und Aufgabentrennung integriert werden, indem Kerberos für Amazon-EMR-Cluster aktiviert wird. In Kerberos werden Services und Benutzer, die sich authentifizieren müssen, als Prinzipale bezeichnet. Prinzipale befinden sich in einem Kerberos-Bereich. Innerhalb dieses Bereichs wird ein Kerberos-Server als Key Distribution Center (KDC) bezeichnet. Über diesen Server können sich Prinzipale authentifizieren. Die Authentifizierung im KDC erfolgt durch die Ausstellung von Authentif

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			izierungstickets. Das KDC unterhält eine Datenbank der Prinzipale in seinem Bereich mit ihren Passwörtern und anderen administr ativen Informationen zu jedem Prinzipal.
3.1(c)	Rollenbasierte Zugriffssteuerung	ecs-task-definition-nonroot-Benutzer	Sie bestimmen einen Nicht-Root-Benutzer für den Zugriff auf Ihre Aufgabendefinitionen des Amazon Elastic Container Service (Amazon ECS), um die Implementierung des Prinzips der geringsten Berechtig ung zu unterstützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.1(c)	Rollenbasierte Zugriffssteuerung	efs-access-point-enforce-Stammverzeichnis	Die Durchsetzung eines Stammverzeichnisses für einen Amazon-Elastic-File-System (Amazon-EFS)-Zugangspunkt trägt dazu bei, den Datenzugriff einzuschränken, indem sichergestellt wird, dass Benutzer des Zugangspunkts nur auf Dateien des angegebenen Unterverzeichnisses zugreifen können.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.1(c)	Rollenbasierte Zugriffssteuerung	efs-access-point-enforce-Benutzeridentität	Um die Implementierung des Prinzips der geringsten Rechte zu unterstützen, stellen Sie sicher, dass die Benutzerdurchsetzung für Ihr Amazon Elastic File System (Amazon EFS) aktiviert ist. Wenn diese Option aktiviert ist, ersetzt Amazon EFS den Benutzer und die Gruppe IDs des NFS-Clients durch die Identität, die auf dem Access Point für alle Dateisystemoperationen konfiguriert ist, und gewährt nur Zugriff auf diese erzwungene Benutzeridentität.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.1(c)	Rollenbasierte Zugriffssteuerung	iam-group-has-users-überprüfen	AWS Identity and Access Managemen t (IAM) kann Ihnen helfen, die Prinzipien der geringsten Rechte und der Aufgabent rennung mit Zugriffsb erechtigungen und Autorisierungen zu integrieren, indem sichergestellt wird, dass IAM-Gruppen mindestens einen Benutzer haben. Die Einteilung von Benutzern in Gruppen auf der Grundlage der ihnen zugewiese nen Berechtigungen oder ihrer Funktion ist eine Möglichkeit, das Prinzip der geringste n Berechtigung zu implementieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.1(c)	Rollenbasierte Zugriffssteuerung	iam-no-inline-policy-überprüfen	Stellen Sie sicher, dass ein Benutzer, eine IAM-Rolle oder eine IAM-Gruppe (AWS Identity and Access Management) nicht über eine Inline-Richtlinie zur Zugriffskontrolle auf Systeme und Ressourcen verfügt. AWS empfiehlt, verwaltete Richtlinien anstelle von Inline-Richtlinien zu verwenden. Verwaltete Richtlinien ermöglichen Wiederverwendbarkeit, Versionsverwaltung, Rollback und Delegierung der Berechtigungsverwaltung.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.1(c)	Rollenbasierte Zugriffssteuerung	iam-password-policy	Die Identitäten und Anmeldeinformationen werden auf der Grundlage einer organisatorischen IAM-Passwortrichtlinie ausgestellt, verwaltet und verifiziert. Sie erfüllen oder übertreffen die Anforderungen von NIST SP 800-63 und dem Standard „Best Practices“ von AWS Foundational Security für die Passwortstärke. Mit dieser Regel können Sie optional RequireUppercaseCharacters (Wert für AWS grundlegende Sicherheitsbewährte Methoden: wahr), RequireLowercaseCharacters (Wert für bewährte Methoden für AWS grundlegende Sicherheit: wahr), RequireSymbols (Wert für bewährte Methoden für AWS grundlegende Sicherheit:

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			wahr), RequireNumbers (Wert für bewährte Methoden für AWS grundlegende Sicherheit: wahr), MinimumPasswordLength (Wert für bewährte Methoden für AWS grundlegende Sicherheit: 14), PasswordReusePrevention (Wert für bewährte Methoden für AWS grundlegende Sicherheit: 24) und MaxPasswordAge (Wert für bewährte Methoden für AWS grundlegende Sicherheit: 90) für Ihr IAM festlegen. Kennwortrichtlinie. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.1(c)	Rollenbasierte Zugriffssteuerung	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) kann Ihnen dabei helfen, die Prinzipien der geringsten Rechte und der Aufgabentrennung in Zugriffsberechtigungen und Autorisierungen zu integrieren und so zu verhindern, dass Richtlinien „Effect“: „Allow“ mit „Action“: „*“ anstelle von „Resource“: „*“ enthalten. Wenn Benutzern mehr Rechte eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und der Aufgabentrennung verstoßen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.1(c)	Rollenbasierte Zugriffssteuerung	iam-root-access-key-überprüfen	Der Zugriff auf Systeme und Ressourcen kann gesteuert werden, indem überprüft wird, ob der Root-Benutzer keine Zugriffsschlüssel mit seiner AWS Identity and Access Management (IAM) -Rolle verknüpft hat. Stellen Sie sicher, dass die Root-Zugriffsschlüssel gelöscht werden. Erstellen und verwenden Sie stattdessen rollenbasierte Funktionen, AWS-Konten um das Prinzip der geringsten Funktionalität zu berücksichtigen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.1(c)	Rollenbasierte Zugriffssteuerung	iam-user-group-membership-überprüfen	AWS Identity and Access Management (IAM) kann Ihnen helfen, Zugriffsberechtigungen und Autorisierungen einzuschränken, indem sichergestellt wird, dass Benutzer Mitglieder mindestens einer Gruppe sind. Wenn Benutzern mehr Berechtigungen eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und Aufgabentrennung verstoßen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.1(c)	Rollenbasierte Zugriffssteuerung	iam-user-mfa-enabled	Aktivieren Sie diese Regel, um den Zugriff auf Ressourcen in der AWS Cloud einzuschränken. Diese Regel sorgt dafür, dass die Multi-Faktor-Authentifizierung (MFA) für alle Benutzer aktiviert ist. MFA sorgt für eine weitere Schutzebene zusätzlich zu den Anmeldeinformationen. Reduzieren Sie Fälle von kompromittierten Konten, indem Sie MFA für Benutzer vorschreiben.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.1(c)	Rollenbasierte Zugriffssteuerung	iam-user-no-policies-überprüfen	Diese Regel stellt sicher, dass AWS Identity and Access Management (IAM) -Richtlinien nur Gruppen oder Rollen zugewiese n werden, um den Zugriff auf Systeme und Ressourcen zu kontrollieren. Die Zuweisung von Berechtig ungen auf Gruppen- oder Rollenebene trägt dazu bei, die Wahrscheinlichkeit zu verringern, dass eine Identität übermäßige Berechtigungen erhält oder beibehält.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.1(c)	Rollenbasierte Zugriffssteuerung	iam-user-unused-credentials-überprüfen	AWS Identity and Access Management (IAM) kann Ihnen bei Zugriffsberechtigungen und Autorisierungen helfen, indem es nach IAM-Passwörtern und Zugriffsschlüsseln sucht, die für einen bestimmten Zeitraum nicht verwendet wurden. Wenn ungenutzte Anmeldeinformationen identifiziert werden, müssen Sie sie deaktivieren und/oder entfernen, da dies gegen das Prinzip der geringsten Berechtigung verstoßen könnte. Für diese Regel müssen Sie einen Wert für das maxCredentialUsage Alter festlegen (Standardkonfiguration: 90). Der tatsächliche Wert muss den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.1(c)	Rollenbasierte Zugriffssteuerung	ec2- instance-profile-attached	EC2 Instanzprofile übergeben eine IAM-Rolle an eine Instanz EC2 . Das Anhängen eines Instance-Profils an Ihre Instances kann bei der Implementierung von geringsten Berechtigungen und der Berechtigungsverwaltung helfen.
3.1(c)	Rollenbasierte Zugriffssteuerung	iam-policy-no-statements-with-full-access	Stellen Sie sicher, dass IAM-Aktionen nur auf die benötigten Aktionen beschränkt sind. Wenn Benutzern mehr Rechte eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Rechte und der Aufgabentrennung verstoßen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.1(c)	Rollenbasierte Zugriffssteuerung	mfa-enabled-for-iam-Konsolenzugriff	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass MFA für alle AWS Identity and Access Management (IAM) -Benutzer aktiviert ist, die über ein Konsolenkennwort verfügen. MFA sorgt für eine weitere Schutzebene zusätzlich zu den Anmeldeinformationen. Indem Sie MFA für Benutzer vorschreiben, können Sie Fälle kompromittierter Konten reduzieren und verhindern, dass unbefugte Benutzer auf vertrauliche Daten zugreifen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.1(c)	Rollenbasierte Zugriffssteuerung	root-account-hardware-mfa-aktiviert	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Hardware-MFA für den Root-Benutzer aktiviert ist. Der Stammbenutzer ist der AWS-Konto-Benutzer mit den meisten Berechtigungen. MFA sorgt für eine weitere Schutzebene zusätzlich zu den Anmeldeinformationen. Indem Sie MFA für den Root-Benutzer vorschreiben, können Sie die Anzahl AWS-Konten kompromittierter Benutzer reduzieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.1(c)	Rollenbasierte Zugriffssteuerung	root-account-mfa-enabled	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass MFA für den Root-Benutzer aktiviert ist. Der Stammbenutzer ist der AWS-Konto-Benutzer mit den meisten Berechtigungen. MFA sorgt für eine weitere Schutzebene zusätzlich zu den Anmeldeinformationen. Indem Sie MFA für den Root-Benutzer vorschreiben, können Sie die Anzahl AWS-Konten kompromittierter Benutzer reduzieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.1(c)	Rollenbasierte Zugriffssteuerung	secretsmanager-rotation-enabled-check	Diese Regel stellt sicher, dass bei AWS Secrets Manager Manager-Geheimnissen die Rotation aktiviert ist. Die regelmäßige Rotation von Secrets kann den Zeitraum verkürzen, in dem ein Secret aktiv ist, und möglicherweise die Auswirkungen auf das Unternehmen verringern, falls das Secret kompromittiert wird.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.1(c)	Rollenbasierte Zugriffssteuerung	secretsmanager-scheduled-rotation-success-überprüfen	Diese Regel stellt sicher, dass AWS Secrets Manager Manager-Geheimnisse gemäß dem Rotations plan erfolgreich rotiert wurden. Die regelmäßige Rotation von Secrets kann den Zeitraum verkürzen, in dem ein Secret aktiv ist, und möglicherweise die Auswirkungen auf das Unternehmen verringern, falls es kompromittiert wird.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.1(g)	Vorfallmanagement	guardduty-non-archived-findings	Amazon GuardDuty hilft Ihnen dabei, die Auswirkungen eines Vorfalls zu verstehen, indem es die Ergebnisse nach Schweregrad klassifiziert: niedrig, mittel und hoch. Diese Klassifizierungen können Sie zur Festlegung von entsprechenden Strategien und Prioritäten zur Behebung solcher Vorfälle verwenden. Mit dieser Regel können Sie optional daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7) und daysHighSev (Config Default: 1) für nicht archivierte Ergebnisse festlegen, wie es die Richtlinien Ihrer Organisation erfordern.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.1(g)	Vorfallmanagement	guardduty-enabled-centralized	Amazon GuardDuty kann mithilfe von Threat Intellige nce Feeds helfen, potenzielle Cybersich erheitsereignisse zu überwachen und zu erkennen. Dazu gehören Listen mit bösartigen IPs und maschinel len Lernmethoden zur Identifizierung unerwarteter, nicht autorisierter und bösartiger Aktivitäten in Ihrer AWS Cloud-Umgebung.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.1(g)	Vorfallmanagement	alb-waf-enabled	Stellen Sie sicher, dass AWS WAF auf Elastic Load Balancers (ELB) aktiviert ist, um Webanwendungen zu schützen. Eine WAF trägt zum Schutz Ihrer Webanwend ungen oder APIs vor gängigen Web-Explo its bei. Diese Web-Exploits können sich auf die Verfügbar keit auswirken, die Sicherheit gefährden oder übermäßige Ressourcen in Ihrer Umgebung verbrauch en.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.1(g)	Vorfallmanagement	securityhub-enabled	AWS Security Hub hilft bei der Überwachung von unbefugtem Personal, Verbindungen, Geräten und Software. AWS Security Hub aggregiert, organisiert und priorisiert die Sicherheitswarnungen oder Ergebnisse mehrerer Dienste. AWS Einige dieser Dienste sind Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer und AWS Firewall Manager sowie AWS Partnerlösungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.1(g)	Vorfallmanagement	ec2-prüfen managedinstance-patch-compliance-status	Aktivieren Sie diese Regel, um bei der Identifizierung und Dokumentation von Sicherheitslücken in Amazon Elastic Compute Cloud (Amazon EC2) zu helfen. Die Regel prüft, ob die EC2 Amazon-Instance die Patch-Konformität im AWS Systems Manager gemäß den Richtlinien und Verfahren Ihrer Organisation einhält.
3.1(h)	Trails	api-gw-execution-logging-aktiviert	Die API-Gateway-Protokollierung zeigt detaillierte Ansichten der Benutzer, die auf die API zugegriffen haben, und wie diese Benutzer auf die API zugegriffen haben. Diese Insights ermöglichen die Einsicht in Benutzeraktivitäten.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.1(h)	Trails	cloud-trail-cloud-watch-logs-aktiviert	Verwenden Sie Amazon CloudWatch , um Protokoll ereignisaktivitäten zentral zu sammeln und zu verwalten. Die Aufnahme von AWS CloudTrail Daten liefert Einzelheiten zu den API-Aufrufaktivitäten in Ihrem AWS-Konto.
3.1(h)	Trails	codebuild-project-logging-enabled	Stellen Sie sicher, dass die AWS CodeBuild Projektprotokollierung aktiviert ist, damit Ihre Build-Ausgabeprotokolle entweder an Amazon CloudWatch oder Amazon Simple Storage Service (Amazon S3) gesendet werden. Build-Ausgabeprotokolle enthalten detaillierte Informationen zu Ihrem Build-Projekt.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.1(h)	Trails	opensearch-logs-to-cloudwatch	Stellen Sie sicher, dass für Amazon OpenSearch Service-Domains Fehlerprotokolle aktiviert und zur Aufbewahrung und Beantwortung an Amazon CloudWatch Logs gestreamt werden. OpenSearch Service-Fehlerprotokolle können bei Sicherheits- und Zugriffsprüfungen helfen und bei der Diagnose von Verfügbarkeitsproblemen helfen.
3.1(h)	Trails	redshift-audit-logging-enabled	Aktivieren Sie die Prüfungsprotokollierung, um Informationen über Verbindungen und Benutzeraktivitäten in Ihrem Amazon-Redshift-Cluster zu erfassen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.1(h)	Trails	cloudtrail-enabled	AWS CloudTrai l kann durch die Aufzeichnung von Aktionen und API-Aufrufen in der AWS Management Console bei der Nichtabst reitbarkeit helfen. Sie können die Benutzer und die Benutzer AWS-Konten , die einen AWS Dienst aufgerufen haben, die Quell-IP-Adresse, über die die Aufrufe generiert wurden, und den Zeitpunkt der Anrufe identifiz ieren. Einzelheiten zu den erfassten Daten finden Sie unter Inhalt des AWS CloudTrail Datensatzes.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.1(h)	Trails	cloudtrail-s3-data events-enabled	Die Erfassung von Simple Storage Service (Amazon S3)-Datenereignisse n unterstützt die Erkennung von ungewöhnlichen Aktivitäten. Zu den Details gehören AWS-Konto Informationen über den Zugriff auf einen Amazon S3 S3-Bucket, die IP-Adresse und die Uhrzeit des Ereignisses.
3.1(h)	Trails	cw-loggroup-retention-period-überprüfen	Stellen Sie sicher, dass die Ereignisprotokolldaten für Ihre Protokollgruppen über eine Mindestdauer aufbewahrt werden, um die Fehlerbehebung und forensische Untersuchungen zu unterstützen. Fehlende frühere Ereignisprotokolldaten erschweren die Rekonstruierung und Identifizierung potenziell schädlicher Ereignisse.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.1(h)	Trails	elasticsearch-logs-to-cloudwatch	Stellen Sie sicher, dass für Amazon OpenSearch Service-Domains Fehlerprotokolle aktiviert und zur Aufbewahrung und Beantwortung an Amazon CloudWatch Logs gestreamt werden. Domain-Fehlerprotokolle sind bei Sicherheits- und Zugriffsprüfungen sowie bei der Diagnose von Verfügbarkeitsproblemen nützlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.1(h)	Trails	elb-logging-enabled	Die Elastic-Load-Balancing-Aktivität ist ein zentraler Kommunikationspunkt innerhalb einer Umgebung. Stellen Sie sicher, dass die ELB-Protokollierung aktiviert ist. Die gesammelten Daten enthalten detaillierte Informationen zu Anfragen, die an den ELB gesendet wurden. Jedes Protokoll enthält Informationen wie die Zeit, zu der die Anforderung einging, die Client-IP-Adresse, Latenzen, Anforderungspfade und Serverantworten.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.1(h)	Trails	multi-region-cloudtrail-enabled	AWS CloudTrail zeichnet Aktionen und API-Aufrufe der AWS Management Console auf. Sie können feststellen, welche Benutzer und Konten angerufen wurden AWS, von welcher Quell-IP-Adresse aus die Anrufe getätigt wurden und wann die Anrufe erfolgten. CloudTrail übermittelt Protokolldateien aus allen AWS Regionen an Ihren S3-Bucket , wenn MULTI_REG ION_CLOUD _TRAIL_ENABLED aktiviert ist. Außerdem wird beim AWS Start einer neuen Region derselbe Trail in der neuen Region erstellt. CloudTrail Dadurch erhalten Sie automatis ch Protokolldateien mit API-Aktivitäten für die neue Region.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.1(h)	Trails	rds-logging-enabled	Um die Protokollierung und Überwachung in Ihrer Umgebung zu erleichtern, stellen Sie sicher, dass die Amazon Relational Database Service (Amazon RDS)-Protokollierung aktiviert ist. Mit der Amazon-RDS-Protokollierung können Sie Ereignisse wie Verbindungen, Verbindungsabbrüche, Abfragen oder abgefragte Tabellen erfassen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.1(h)	Trails	s-3 bucket-logging-enabled	Die Amazon Simple Storage Service (Amazon S3)-Serverzugriffs protokollierung bietet eine Methode zur Überwachu ng des Netzwerks im Hinblick auf potenzielle Cybersich erheitsereignisse. Die Ereignisse werden überwacht, indem detaillierte Aufzeichn ungen über die Anfragen erfasst werden, die an einen Amazon-S3-Bucket gestellt wurden. Jeder Zugriffsprotokolle intrag enthält Details zu einer einzelnen Zugriffsanfrage. Zu den Details gehören Anforderer, Bucket-Name, Anforderu ngszeit, Anforderu ngsaktion, Antwortst atus und Fehlercode, falls relevant.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.1(h)	Trails	vpc-flow-logs-enabled	VPC-Flow-Protokolle erfassen detaillierte Informationsdatensätze über den IP-Datenverkehr, der zu und von Netzwerkschnittstellen in Ihrer Amazon Virtual Private Cloud (Amazon VPC) fließt. Standardmäßig enthalten Flow-Protokolldatensätze Werte für die verschiedenen Komponenten des IP-Flows, einschließlich Quelle, Ziel und Protokoll.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.1(h)	Trails	wafv2-logging-enabled	Um die Protokollierung und Überwachung in Ihrer Umgebung zu erleichtern, aktivieren Sie die AWS WAF (V2) -Protokollierung im regionalen und globalen Web ACLs. AWS Die WAF-Protokollierung bietet detaillierte Informationen über den Datenverkehr, der von Ihrer Web-ACL analysiert wird. In den Protokollen werden die Uhrzeit aufgezeichnet, zu der die AWS WAF die Anfrage von Ihrer AWS Ressource erhalten hat, Informationen über die Anfrage und eine Aktion für die Regel, der jede Anfrage entsprach.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.1(h)	Trails	redshift-cluster-configuration-check	Um Daten im Ruhezustand zu schützen, muss die Verschlüsselung für Ihre Amazon-Redshift-Cluster aktiviert sein. Sie müssen auch sicherstellen, dass die erforderlichen Konfigurationen auf Amazon-Redshift-Clustern bereitgestellt werden. Die Prüfungsprotokollierung muss aktiviert sein, um Informationen zu Verbindungen und Benutzeraktivitäten in der Datenbank bereitzustellen. Diese Regel erfordert, dass ein Wert für clusterDbEncrypted (Config Default: TRUE) und LoggingEnabled (Config Default: TRUE) gesetzt ist. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.1(i)	Public Key Infrastructure	acm-certificate-expiration-check	Stellen Sie sicher, dass die Netzwerkintegrität geschützt ist, indem Sie sicherstellen, dass X509-Zertifikate von ACM ausgestellt werden. AWS Diese Zertifikate müssen gültig und dürfen nicht abgelaufen sein. Für diese Regel ist ein Wert für erforderlich daysToExpiration (Wert für bewährte AWS Grundregeln für Sicherheit: 90). Der tatsächliche Wert muss den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.1(i)	Public Key Infrastructure	alb-http-drop-invalid-Header-aktiviert	Stellen Sie sicher, dass Ihre Elastic Load Balancers (ELB) so konfiguriert sind, dass sie HTTP-Header löschen. Da sensible Daten vorhanden sein können, sollten Sie die Verschlüsselung bei der Übertragung aktivieren, um diese Daten zu schützen.
3.1(i)	Public Key Infrastructure	alb-http-to-https-Umleitungsprüfung	Um Daten während der Übertragung zu schützen, stellen Sie sicher, dass Ihr Application Load Balancer unverschlüsselte HTTP-Anfragen automatisch an HTTPS umleitet. Da sensible Daten vorhanden sein können, sollten Sie die Verschlüsselung bei der Übertragung aktivieren, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.1(i)	Public Key Infrastructure	api-gw-ssl-enabled	Stellen Sie sicher, dass die REST-API-Stufen von Amazon API Gateway mit SSL-Zertifikaten konfiguriert sind, damit Backend-Systeme überprüfen können, ob Anforderungen von API Gateway stammen.
3.1(i)	Public Key Infrastructure	opensearch-https-required	Da sensible Daten existieren können und um Daten während der Übertragung zu schützen, sollten Sie sicherstellen, dass HTTPS für Verbindungen zu Ihren Amazon OpenSearch Service-Domains aktiviert ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.1(i)	Public Key Infrastru cture	elbv2- acm-certificate-required	Zum Schutz von eventuell vorhanden en sensiblen Daten sowie von Daten während der Übertragung muss die Verschlüsselung für Ihr Elastic Load Balancing aktiviert sein. Verwenden Sie AWS Certificate Manager, um öffentlic he und private SSL/ TLS-Zertifikate mit AWS Diensten und internen Ressource n zu verwalten, bereitzustellen und bereitzustellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.1(i)	Public Key Infrastructure	elb-acm-certificate-required	Zum Schutz von eventuell vorhanden en sensiblen Daten sowie von Daten während der Übertragung muss die Verschlüsselung für Ihr Elastic Load Balancing aktiviert sein. Verwenden Sie AWS Certificate Manager, um öffentlic he und private SSL/ TLS-Zertifikate mit AWS Diensten und internen Ressource n zu verwalten, bereitzustellen und bereitzustellen.
3.1(i)	Public Key Infrastructure	elb-tls-https-listeners-nur	Stellen Sie sicher, dass Ihre Elastic Load Balancer (ELBs) mit SSL- oder HTTPS-Listenern konfiguriert sind. Um eventuell vorhanden e sensible Daten zu schützen, sollten Sie die Verschlüsselung bei der Übertragung aktivieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.1(i)	Public Key Infrastructure	redshift-require-tls-ssl	Stellen Sie sicher, dass Ihre Amazon-Redshift-Cluster eine TLS/SSL-Verschlüsselung erfordern, um eine Verbindung zu SQL-Clients herzustellen. Da sensible Daten vorhanden sein können, sollten Sie die Verschlüsselung bei der Übertragung aktivieren, um diese Daten zu schützen.
3.1(i)	Public Key Infrastructure	s-3 bucket-ssl-requests-only	Um Daten während der Übertragung zu schützen, stellen Sie sicher, dass Ihre Amazon Simple Storage Service (Amazon S3)-Buckets Anfragen zur Verwendung von Secure Socket Layer (SSL)-Buckets erfordern. Da sensible Daten vorhanden sein können, sollten Sie die Verschlüsselung bei der Übertragung aktivieren, um diese Daten zu schützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.3	Management von Schwachstellen	elastic-beanstalk-managed-updates-aktiviert	Durch die Aktivierung verwalteter Plattform updates für eine Amazon-Elastic-Beanstalk-Umgebung wird sichergestellt, dass die aktuellen verfügbaren Plattform -Fixes, -Updates und -Features für die Umgebung installiert sind. Eine bewährte Methode zur Sicherung von Systemen besteht darin, stets die aktuellen Patches zu installieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.3	Management von Schwachstellen	rds-automatic-minor-version-upgrade-fähig	Aktivieren Sie automatische Unterversions-Upgrades auf Ihren Amazon-Relational-Database-Service (RDS)-Instances, um sicherzustellen, dass die aktuellen Updates für Unterversionen des Relational Database Management System (RDBMS) installiert sind, die Sicherheitspatches und Bugfixes enthalten können.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.3	Management von Schwachstellen	redshift-cluster-maintenancesettings-check	Diese Regel stellt sicher, dass Amazon-Redshift-Cluster die bevorzugten Einstellungen für Ihre Organisation haben. Insbesondere sorgt sie dafür, dass Cluster bevorzugte Wartungsfenster und automatisierte Aufbewahrungsfristen für Snapshots für die Datenbank haben. Für diese Regel müssen Sie die festlegen allowVersionUpgrade. Der Standardwert ist „true“. Außerdem können Sie optional den Zeitraum preferredMaintenanceWindow (der Standardwert ist sa: 16:00 -sa: 16:30) und den automated SnapshotRetention Zeitraum (der Standardwert ist 1) festlegen. Die tatsächlichen Werte müssen den Richtlini

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			en Ihrer Organisation entsprechen.
3.3	Management von Schwachstellen	guardduty-non-archived-findings	Amazon GuardDuty hilft Ihnen dabei, die Auswirkungen eines Vorfalls zu verstehen, indem es die Ergebnisse nach Schweregrad klassifiziert: niedrig, mittel und hoch. Diese Klassifizierungen können Sie zur Festlegung von entsprechenden Strategien und Prioritäten zur Behebung solcher Vorfälle verwenden. Mit dieser Regel können Sie optional daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7) und daysHighSev (Config Default: 1) für nicht archivierte Ergebnisse festlegen, wie es die Richtlinien Ihrer Organisation erfordern.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.3	Management von Schwachstellen	ec2-manager instance-managed-by-systems	Eine Bestandsaufnahme der Softwareplattformen und Anwendungen innerhalb des Unternehmens ist möglich, indem Amazon Elastic Compute Cloud (Amazon EC2) - Instances mit AWS Systems Manager verwaltet werden. Verwenden Sie AWS Systems Manager, um detaillierte Systemkonfigurationen, Betriebssystem-Patch-Levels, Namen und Typ der Dienste, Softwareinstallationen, Anwendungsname, Herausgeber und Version sowie andere Details zu Ihrer Umgebung bereitzustellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.3	Management von Schwachstellen	ec2-prüfen managedinstance-association-compliance-status	Verwenden Sie AWS Systems Manager Associations, um bei der Inventarisierung von Softwareplattformen und Anwendungen innerhalb eines Unternehmens zu helfen. AWS Systems Manager weist Ihren verwalteten Instanzen einen Konfigurationsstatus zu und ermöglicht es Ihnen, Basiswerte für Betriebssystem-Patch-Levels, Softwareinstallationen, Anwendungskonfigurationen und andere Details zu Ihrer Umgebung festzulegen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.3	Management von Schwachstellen	ec2-prüfen managedinstance-patch-compliance-status	Aktivieren Sie diese Regel, um bei der Identifizierung und Dokumentation von Sicherheitslücken in Amazon Elastic Compute Cloud (Amazon EC2) zu helfen. Die Regel prüft, ob die EC2 Amazon-Instance die Patch-Konformität im AWS Systems Manager gemäß den Richtlinien und Verfahren Ihrer Organisation einhält.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.5	Cyber-Krisenmanagementplan	guardduty-non-archived-findings	Amazon GuardDuty hilft Ihnen dabei, die Auswirkungen eines Vorfalls zu verstehen, indem es die Ergebnisse nach Schweregrad klassifiziert: niedrig, mittel und hoch. Diese Klassifizierungen können Sie zur Festlegung von entsprechenden Strategien und Prioritäten zur Behebung solcher Vorfälle verwenden. Mit dieser Regel können Sie optional daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7) und daysHighSev (Config Default: 1) für nicht archivierte Ergebnisse festlegen, wie es die Richtlinien Ihrer Organisation erfordern.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.5	Cyber-Krisenmanagementplan	guardduty-enabled-centralized	Amazon GuardDuty kann mithilfe von Threat Intelligence Feeds helfen, potenzielle Cybersicherheitsereignisse zu überwachen und zu erkennen. Dazu gehören Listen mit bösartigen IPs und maschinellen Lernmethoden zur Identifizierung unerwarteter, nicht autorisierter und bösartiger Aktivitäten in Ihrer AWS Cloud-Umgebung.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.5	Cyber-Krisenmanagementplan	ec2-managerinstance-managed-by-systems	Eine Bestandsaufnahme der Softwareplattformen und Anwendungen innerhalb des Unternehmens ist möglich, indem Amazon Elastic Compute Cloud (Amazon EC2) - Instances mit AWS Systems Manager verwaltet werden. Verwenden Sie AWS Systems Manager, um detaillierte Systemkonfigurationen, Betriebssystem-Patch-Levels, Namen und Typ der Dienste, Softwareinstallationen, Anwendungsname, Herausgeber und Version sowie andere Details zu Ihrer Umgebung bereitzustellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.5	Cyber-Krisenmanagementplan	ec2-check managedinstance-association-compliance-status	Verwenden Sie AWS Systems Manager Associations, um bei der Inventarisierung von Softwareplattformen und Anwendungen innerhalb eines Unternehmens zu helfen. AWS Systems Manager weist Ihren verwalteten Instanzen einen Konfigurationsstatus zu und ermöglicht es Ihnen, Basiswerte für Betriebssystem-Patch-Levels, Softwareinstallationen, Anwendungskonfigurationen und andere Details zu Ihrer Umgebung festzulegen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.5	Cyber-Krisenmanagementplan	ec2-check managedinstance-patch-compliance-status	Aktivieren Sie diese Regel, um bei der Identifizierung und Dokumentation von Sicherheitslücken in Amazon Elastic Compute Cloud (Amazon EC2) zu helfen. Die Regel prüft, ob die EC2 Amazon-Instance die Patch-Konformität im AWS Systems Manager gemäß den Richtlinien und Verfahren Ihrer Organisation einhält.
3.9	IT-Risikobeurteilung	annual-risk-assessment-performed (Prozessüberprüfung)	Führen Sie eine jährliche Risikobewertung für Ihre Organisation durch. Risikowertungen können dabei helfen, die Wahrscheinlichkeit und Auswirkungen identifizierter Risiken und/oder Schwachstellen für eine Organisation zu ermitteln.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
3.12	Training	security-awareness-program-exists (Prozessprüfung)	Etablieren und pflegen Sie ein Programm zur Förderung des Sicherheitsbewusstseins in Ihrer Organisation. Programme zur Förderung des Sicherheitsbewusstseins der Mitarbeiter vermitteln ihnen, wie sie die Organisation vor diversen Sicherheitsverletzungen oder Sicherheitsvorfällen schützen können.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
4.4(g)	Betrugsanalyse - Analyse verdächti ger Transakti onen, Unterschl agung, Diebstahl oder Verdacht auf Geldwäsche, Veruntreuung von Vermögenswerten, Manipulation von Finanzunterlagen usw. Die regulator ische Anforderung, Betrug an die RBI zu melden, sollte systemgesteuert sein.	guardduty-enabled-centralized	Amazon GuardDuty kann mithilfe von Threat Intellige nce Feeds helfen, potenzielle Cybersich erheitsereignisse zu überwachen und zu erkennen. Dazu gehören Listen mit bösartigen IPs und maschinel len Lernmethoden zur Identifizierung unerwarteter, nicht autorisierter und bösartiger Aktivitäten in Ihrer AWS Cloud-Umgebung.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
4.4(h)	Kapazitäts- und Leistungsanalyse von IT-Sicherheitssysteme n.	dynamodb-autoscaling-enabled	Amazon DynamoDB Auto Scaling verwendet den AWS Application Auto Scaling-Service, um die bereitgestellte Durchsatzkapazität so anzupassen, dass sie automatisch auf tatsächliche Verkehrsmuster reagiert. Auf diese Weise kann eine Tabelle oder ein globaler sekundärer Index die bereitgestellte Lese-/Schreibkapazität erhöhen, um plötzliche Erhöhungen des Datenverkehrs ohne Drosselung zu bewältigen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
4.4(h)	Kapazitäts- und Leistungsanalyse von IT-Sicherheitssysteme n.	elb-cross-zone-load-Balancing aktiviert	Aktivieren Sie zonenübergreifendes Load Balancing für Ihre Elastic Load Balancer (ELBs), um eine angemessene Kapazität und Verfügbarkeit aufrechtzuerhalten. Zonenübergreifendes Load Balancing reduziert die Notwendigkeit, die gleiche Anzahl von Instances in jeder aktivierten Availability Zone aufrechtzuerhalten. Es verbessert auch die Fähigkeit Ihrer Anwendung, den Verlust einer oder mehrerer Instances zu bewältigen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
4.4(h)	Kapazitäts- und Leistungsanalyse von IT-Sicherheitssysteme n.	elb-deletion-protection-enabled	Diese Regel sorgt dafür, dass der Löschschutz für Elastic Load Balancing aktiviert ist. Verwenden Sie diese Funktion, um zu verhindern, dass Ihr Load Balancer versehentlich oder böswillig gelöscht wird, was zum Verlust der Verfügbarkeit Ihrer Anwendungen führen kann.
4.4(h)	Kapazitäts- und Leistungsanalyse von IT-Sicherheitssysteme n.	clb-multiple-az	Elastic Load Balancing (ELB) verteilt Ihren eingehenden Traffic automatisch auf mehrere Ziele wie EC2 Instances, Container und IP-Adressen in einer Availability Zone. Zur Gewährleistung einer hohen Verfügbarkeit stellen Sie sicher, dass Ihr ELB Instances aus mehreren Availability Zones registriert hat.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
4.4(h)	Kapazitäts- und Leistungsanalyse von IT-Sicherheitssyst emen.	elbv2-multiple-az	Elastic Load Balancing (ELB) verteilt Ihren eingehenden Traffic automatisch auf mehrere Ziele wie EC2 Instances, Container und IP-Adressen in einer Availability Zone. Zur Gewährlei stung einer hohen Verfügbarkeit stellen Sie sicher, dass Ihr ELB Instances aus mehreren Availability Zones registriert hat.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
4.4(h)	Kapazitäts- und Leistungsanalyse von IT-Sicherheitssysteme n.	lambda-vpc-multi-az-überprüfen	Wenn Ihre AWS Lambda-Funktion so konfiguriert ist, dass sie eine Verbindung zu einer Virtual Private Cloud (VPC) in Ihrem Konto herstellt, stellen Sie die AWS Lambda-Funktion in mindestens zwei verschiedenen Availability Zones bereit, um sicherzustellen, dass Ihre Funktion für die Verarbeitung von Ereignissen im Falle einer Dienstunterbrechung in einer einzigen Zone verfügbar ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
4.4(h)	Kapazitäts- und Leistungsanalyse von IT-Sicherheitssysteme n.	rds-instance-deletion-protection-aktiviert	Stellen Sie sicher, dass Amazon Relational Database Service (Amazon RDS)-Instances den Löschschutz aktiviert haben. Verwenden Sie den Löschschutz, um zu verhindern, dass Ihre Amazon-RDS-Instances versehentlich oder böswillig gelöscht werden, was zum Verlust der Verfügbarkeit Ihrer Anwendungen führen kann.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
4.4(h)	Kapazitäts- und Leistungsanalyse von IT-Sicherheitssysteme n.	rds-multi-az-support	Die Multi-AZ-Unterstützung in Amazon Relational Database Service (Amazon RDS) bietet eine verbesserte Verfügbarkeit und Beständigkeit von Datenbank-Instances. Wenn Sie eine Multi-AZ-Datenbank-Instance bereitstellen, erstellt Amazon RDS automatisch eine primäre Datenbank-Instance und repliziert die Daten synchron auf eine Standby-Instance in einer anderen Availability Zone. Jede Availability Zone läuft auf einer eigenen, physisch getrennten, unabhängigen Infrastruktur und ist auf eine hohe Verfügbarkeit ausgelegt. Im Falle eines Infrastrukturausfalls führt Amazon RDS einen automatis

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			chen Failover zum Standby-Modus durch, sodass Sie den Datenbankbetrieb wieder aufnehmen können, sobald der Failover abgeschlo ssen ist.
4.4(h)	Kapazitäts- und Leistungsanalyse von IT-Sicherheitssyst emen.	s3- bucket-default-loc k-enabled	Stellen Sie sicher, dass für Ihren Amazon Simple Storage Service (Amazon S3)-Bucke t standardmäßig eine Sperre aktiviert ist. Zum Schutz eventuell vorhanden er sensibler Daten in S3 Buckets müssen Sie Objektsperren für Daten im Ruhezusta nd erzwingen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
4.4(h)	Kapazitäts- und Leistungsanalyse von IT-Sicherheitssyst emen.	vpc-vpn-2-tunnels-up	Redundante Site-to-Site VPN-Tunne l können implement iert werden, um die Anforderungen an die Ausfallsicherheit zu erfüllen. Es verwendet zwei Tunnel, um die Konnektivität sicherzustellen, falls eine der Site-to-Site VPN-Verbindungen nicht verfügbar ist. Um sich vor einem Verbindungsverlust zu schützen, können Sie für den Fall, dass Ihr Kunden-Gateway nicht verfügbar ist, eine zweite Site-to-S ite VPN-Verbindung zu Ihrer Amazon Virtual Private Cloud (Amazon VPC) und Ihrem Virtual Private Gateway einrichten, indem Sie ein zweites Kunden-Gateway verwenden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
4.4(h)	Kapazitäts- und Leistungsanalyse von IT-Sicherheitssysteme n.	autoscaling-group-elb-healthcheck-erforderlich	Die Elastic Load Balancer (ELB) - Zustandsprüfungen für Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling Scaling-Gruppen unterstützen die Aufrechterhaltung einer angemessenen Kapazität und Verfügbarkeit. Der Load Balancer sendet regelmäßig Pings, versucht Verbindungen herzustellen oder sendet Anfragen, um den Zustand der EC2 Amazon-Instances in einer Gruppe mit auto-scaling zu testen. Wenn eine Instance nicht zurückmeldet, wird der Traffic an eine neue EC2 Amazon-Instance gesendet.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
4.4(h)	Kapazitäts- und Leistungsanalyse von IT-Sicherheitssysteme n.	dynamodb-throughput-limit-check	Aktivieren Sie diese Regel, um sicherzustellen, dass die bereitgestellte Durchsatzkapazität in Ihren Amazon-DynamoDB-Tabellen überprüft wird. Dies ist der Umfang der Lese- und Schreibaktivitäten, der von den jeweiligen Tabellen unterstützt werden kann. DynamoDB verwendet diese Informationen für das Reservieren ausreichender Systemressourcen, um Ihren Durchsatz anforderungen gerecht zu werden. Diese Regel generiert eine Warnung, wenn sich der Durchsatz dem Höchstlimit für ein Kundenkonto nähert. Mit dieser Regel können Sie optional die Parameter RCUThreshold Kontoprozentsatz

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			(Konfigurationsstandard: 80) und WCUThreshold Kontoprozentsatz (Konfigurationsstandard: 80) festlegen. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.
4.4(h)	Kapazitäts- und Leistungsanalyse von IT-Sicherheitssystemen.	ec2- instance-detailed-monitoring-enabled	Aktivieren Sie diese Regel, um die Amazon Elastic Compute Cloud (Amazon EC2) - Instance-Überwachung auf der EC2 Amazon-Konsole zu verbessern, in der Monitoring-Diagramme mit einem Zeitraum von 1 Minute für die Instance angezeigt werden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
4.4(h)	Kapazitäts- und Leistungsanalyse von IT-Sicherheitssystemen.	lambda-concurrency-check	Diese Regel stellt sicher, dass die Höchst- und Untergrenzen für die Gleichzeitigkeit einer Lambda-Funktion festgelegt werden. Dies kann Sie beim Baselining für die Anzahl der Anforderungen unterstützen, die Ihre Funktion zu einem bestimmten Zeitpunkt verarbeitet.
4.4(h)	Kapazitäts- und Leistungsanalyse von IT-Sicherheitssystemen.	lambda-dlq-check	Aktivieren Sie diese Regel, um das entsprechende Personal über Amazon Simple Queue Service (Amazon SQS) oder Amazon Simple Notification Service (Amazon SNS) zu benachrichtigen, wenn eine Funktion ausgefallen ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
4.4(h)	Kapazitäts- und Leistungsanalyse von IT-Sicherheitssysteme n.	beanstalk-enhanced-health-reporting-aktiviert	AWS Die verbesserte Zustandsberichterstattung von Elastic Beanstalk ermöglicht eine schnellere Reaktion auf Veränderungen im Zustand der zugrunde liegenden Infrastruktur. Diese Änderungen könnten zu einer mangelnden Verfügbarkeit der Anwendung führen. Die erweiterten Zustandsberichte von Elastic Beanstalk bieten eine Statusbeschreibung, um den Schweregrad der identifizierten Probleme einzuschätzen und mögliche Ursachen zu identifizieren, die untersucht werden müssen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
4.4(h)	Kapazitäts- und Leistungsanalyse von IT-Sicherheitssysteme n.	rds-enhanced-monitoring-enabled	Aktivieren Sie Amazon Relational Database Service (Amazon RDS), um die Verfügbarkeit von Amazon RDS zu überwachen. Dies bietet einen detaillierten Einblick in den Zustand Ihrer Amazon-RDS-Datenbank-Instances. Wenn der Amazon-RDS-Speicher mehr als ein zugrunde liegendes physisches Gerät verwendet, erfasst Enhanced Monitoring die Daten für jedes Gerät. Wenn die Datenbank-Instance von Amazon RDS in einer Multi-AZ-Bereitstellung ausgeführt wird, werden außerdem die Daten für jedes Gerät auf dem sekundären Host sowie die Metriken des sekundären Hosts erfasst.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
4.4(h)	Kapazitäts- und Leistungsanalyse von IT-Sicherheitssystemen.	securityhub-enabled	AWS Security Hub hilft bei der Überwachung von unbefugtem Personal, Verbindungen, Geräten und Software. AWS Security Hub aggregiert, organisiert und priorisiert die Sicherheitswarnungen oder Ergebnisse mehrerer Dienste. AWS Einige dieser Dienste sind Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer und AWS Firewall Manager sowie AWS Partnerlösungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
4.4(h)	Kapazitäts- und Leistungsanalyse von IT-Sicherheitssysteme n.	ebs-optimized-instance	Eine optimierte Instance im Amazon Elastic Block Store (Amazon EBS) bietet zusätzliche, dedizierte Kapazität für Amazon-EBS-I/O-Vorgänge. Diese Optimierung bietet die beste Leistung für Ihr EBS-Volume, indem Konflikte zwischen Amazon-EBS-I/O und anderem Datenverkehr von Ihrer Instance minimiert werden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
4.4(h)	Kapazitäts- und Leistungsanalyse von IT-Sicherheitssyst emen.	guardduty-enabled-centralized	Amazon GuardDuty kann mithilfe von Threat Intellige nce Feeds helfen, potenzielle Cybersich erheitsereignisse zu überwachen und zu erkennen. Dazu gehören Listen mit bösartigen IPs und maschinel len Lernmethoden zur Identifizierung unerwarteter, nicht autorisierter und bösartiger Aktivitäten in Ihrer AWS Cloud-Umgebung.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
4.4(i)	Meldung von Vorfällen , ihre Auswirkungen und Maßnahmen, die ergriffen wurden, um zu verhindern, dass sich solche Ereignisse in future wiederholen.	guardduty-enabled-centralized	Amazon GuardDuty kann mithilfe von Threat Intellige nce Feeds helfen, potenzielle Cybersich erheitsereignisse zu überwachen und zu erkennen. Dazu gehören Listen mit bösartigen IPs und maschinel len Lernmethoden zur Identifizierung unerwarteter, nicht autorisierter und bösartiger Aktivitäten in Ihrer AWS Cloud-Umgebung.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
4.4(i)	Meldung von Vorfällen, ihre Auswirkungen und Maßnahmen, die ergriffen wurden, um zu verhindern, dass sich solche Ereignisse in future wiederholen.	guardduty-non-archived-findings	Amazon GuardDuty hilft Ihnen dabei, die Auswirkungen eines Vorfalls zu verstehen, indem es die Ergebnisse nach Schweregrad klassifiziert: niedrig, mittel und hoch. Diese Klassifizierungen können Sie zur Festlegung von entsprechenden Strategien und Prioritäten zur Behebung solcher Vorfälle verwenden. Mit dieser Regel können Sie optional daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7) und daysHighSev (Config Default: 1) für nicht archivierte Ergebnisse festlegen, wie es die Richtlinien Ihrer Organisation erfordern.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
6.3	NBFCs müssen die Notwendigkeit berücksichtigen, die erforderlichen Backup-Sites für ihre kritischen Geschäftssysteme und Rechenzentren einzurichten.	dynamodb-autoscaling-enabled	Amazon DynamoDB Auto Scaling verwendet den AWS Application Auto Scaling-Service, um die bereitgestellte Durchsatzkapazität so anzupassen, dass sie automatisch auf tatsächliche Verkehrsmuster reagiert. Auf diese Weise kann eine Tabelle oder ein globaler sekundärer Index die bereitgestellte Lese-/Schreibkapazität erhöhen, um plötzliche Erhöhungen des Datenverkehrs ohne Drosselung zu bewältigen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
6.3	NBFCs berücksichtigen die Notwendigkeit, die erforderlichen Backup-Sites für ihre kritischen Geschäftssysteme und Rechenzentren einzurichten.	aurora-resources-protected-by-Backup-Plan	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon Aurora Aurora-Ressourcen Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
6.3	NBFCs müssen die Notwendigkeit berücksichtigen, die erforderlichen Backup-Sites für ihre kritischen Geschäftssysteme und Rechenzentren einzurichten.	backup-plan-min-frequency-and-min-retention-check	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihr AWS Backup-Plan auf eine Mindestfrequenz und Aufbewahrung festgelegt ist. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen. Mit dieser Regel können Sie die Parameter requiredFrequencyValue (Config default: 1), requiredRetentionDays (Config default: 35) und requiredFrequencyUnit

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			(Config default: days) festlegen. Der tatsächliche Wert muss den Anforderungen Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
6.3	NBFCs müssen die Notwendigkeit berücksichtigen, die erforderlichen Backup-Sites für ihre kritischen Geschäftssysteme und Rechenzentren einzurichten.	backup-recovery-point-minimum-Aufbewahrungsprüfung	Um bei Datensicherungsprozessen zu helfen, stellen Sie sicher, dass für Ihre AWS Backup-Wiederherstellungspunkte eine Mindestaufbewahrungsdauer festgelegt ist. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen. Mit dieser Regel können Sie den Parameter requiredRetentionDays (Config Default: 35) festlegen. Der tatsächliche Wert muss den Anforderu

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			ngen Ihrer Organisat ion entsprechen.
6.3	NBFCs sollten die Notwendigkeit berücksichtigen, die erforderlichen Backup-Sites für ihre kritischen Geschäftssysteme und Rechenzentren einzurichten.	cmk-backing-key-ro tation-aktiviert	Aktivieren Sie die Schlüsselrotation, um sicherzustellen, dass Schlüssel rotiert werden, nachdem sie das Ende ihrer Krypto-Periode erreicht haben.
6.3	NBFCs müssen die Notwendigkeit berücksichtigen, die erforderlichen Backup-Sites für ihre kritischen Geschäftssysteme und Rechenzentren einzurichten.	db-instance-backup-enabled	Die Sicherung sfunktion von Amazon RDS erstellt Sicherung en Ihrer Datenbank en und Transakti onsprotokolle. Amazon RDS erstellt einen Snapshot für das Speichervolume Ihrer DB-Instance, sodass die gesamte DB-Instance gesichert wird. Sie können im System spezifische Aufbewahrungsfrist en festlegen, um Ihre Ausfallsicherheits anforderungen zu erfüllen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
6.3	NBFCs erwägen die Notwendigkeit, die erforderlichen Backup-Sites für ihre kritischen Geschäftssysteme und Rechenzentren einzurichten.	dynamodb-in-backup-plan	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon DynamoDB-Tabellen Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
6.3	NBFCs müssen die Notwendigkeit berücksichtigen, die erforderlichen Backup-Sites für ihre kritischen Geschäftssysteme und Rechenzentren einzurichten.	ebs-in-backup-plan	Stellen Sie zur Unterstützung der Datensicherungspro zesse sicher, dass Ihre Amazon Elastic Block Store (Amazon EBS) -Volumes Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwaltet er Backup-Service mit einer richtlini enbasierten Backup-Lösung. Diese Lösung vereinfac ht Ihr Sicherung smanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforde rungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
6.3	NBFCs müssen die Notwendigkeit berücksichtigen, die erforderlichen Backup-Sites für ihre kritischen Geschäftssysteme und Rechenzentren einzurichten.	ec2--Plan resources-protected-by-backup	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon Elastic Compute Cloud (Amazon EC2) -Ressourcen Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
6.3	NBFCs müssen die Notwendigkeit berücksichtigen, die erforderlichen Backup-Sites für ihre kritischen Geschäftssysteme und Rechenzentren einzurichten.	efs-in-backup-plan	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon Elastic File System (Amazon EFS) -Dateisysteme Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
6.3	NBFCs müssen die Notwendigkeit berücksichtigen, die erforderlichen Backup-Sites für ihre kritischen Geschäftssysteme und Rechenzentren einzurichten.	elasticache-redis-cluster-automatic-Backup-Check	Wenn automatische Backups aktiviert sind, ElastiCache erstellt Amazon täglich ein Backup des Clusters. Die Sicherung kann für eine von Ihrer Organisation festgelegte Anzahl von Tagen aufbewahrt werden. Automatische Backups schützen vor Datenverlust. Bei einem Ausfall können Sie einen neuen Cluster erstellen, der Ihre Daten aus dem aktuellen Backup wiederherstellt.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
6.3	NBFCs sollten die Notwendigkeit berücksichtigen, die erforderlichen Backup-Sites für ihre kritischen Geschäftssysteme und Rechenzentren einzurichten.	fsx-resources-protected-by-Backup-Plan	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre FSx Amazon-Dateisysteme Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
6.3	NBFCs müssen die Notwendigkeit berücksichtigen, die erforderlichen Backup-Sites für ihre kritischen Geschäftssysteme und Rechenzentren einzurichten.	rds-in-backup-plan	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon Relational Database Service (Amazon RDS) -Instances Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
6.3	NBFCs müssen die Notwendigkeit berücksichtigen, die erforderlichen Backup-Sites für ihre kritischen Geschäftssysteme und Rechenzentren einzurichten.	redshift-backup-enabled	Stellen Sie zur Unterstützung der Datensicherungsprozesse sicher, dass Ihre Amazon-Redshift-Cluster über automatisierte Snapshots verfügen. Wenn automatisierte Snapshots für einen Cluster aktiviert sind, erstellt Redshift in regelmäßigen Abständen Snapshots dieses Clusters. Standardmäßig erstellt Redshift alle acht Stunden oder alle 5 GB einen Snapshot für jeden Knoten mit Datenänderungen oder je nachdem, was zuerst eintritt.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
6.3	NBFCs sollten die Notwendigkeit berücksichtigen, die erforderlichen Backup-Sites für ihre kritischen Geschäftssysteme und Rechenzentren einzurichten.	s-3 bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) unterstützt die Aufrechterhaltung einer angemesse nen Kapazität und Verfügbarkeit. CRR ermöglicht das automatische, asynchrone Kopieren von Objekten in Amazon S3 Buckets, um die Datenverf ügbarkeit sicherzus tellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
8.1	Die IT-Systeme sollten schrittweise ausgebaut werden, da der Umfang und die Komplexität der NBFC-Abläufe zunehmen.	dynamodb-autoscaling-enabled	Amazon DynamoDB Auto Scaling verwendet den AWS Application Auto Scaling-Service, um die bereitgestellte Durchsatzkapazität so anzupassen, dass sie automatisch auf tatsächliche Verkehrsmuster reagiert. Auf diese Weise kann eine Tabelle oder ein globaler sekundärer Index die bereitgestellte Lese-/Schreibkapazität erhöhen, um plötzliche Erhöhungen des Datenverkehrs ohne Drosselung zu bewältigen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
8.1	Die IT-Systeme sollten schrittweise ausgebaut werden, da der Umfang und die Komplexität der NBFC-Abläufe zunehmen.	elb-cross-zone-load-Balancing aktiviert	Aktivieren Sie zonenübergreifendes Load Balancing für Ihre Elastic Load Balancer (ELBs), um eine angemessene Kapazität und Verfügbarkeit aufrechtzuerhalten. Zonenübergreifendes Load Balancing reduziert die Notwendigkeit, die gleiche Anzahl von Instances in jeder aktivierten Availability Zone aufrechtzuerhalten. Es verbessert auch die Fähigkeit Ihrer Anwendung, den Verlust einer oder mehrerer Instances zu bewältigen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
8.1	Die IT-Systeme sollten schrittweise ausgebaut werden, da der Umfang und die Komplexität der NBFC-Abläufe zunehmen.	elb-deletion-protection-enabled	Diese Regel sorgt dafür, dass der Löschschutz für Elastic Load Balancing aktiviert ist. Verwenden Sie diese Funktion, um zu verhindern, dass Ihr Load Balancer versehentlich oder böswillig gelöscht wird, was zum Verlust der Verfügbarkeit Ihrer Anwendungen führen kann.
8.1	Die IT-Systeme sollten schrittweise ausgebaut werden, da der Umfang und die Komplexität der NBFC-Abläufe zunehmen.	clb-multiple-az	Elastic Load Balancing (ELB) verteilt Ihren eingehenden Traffic automatisch auf mehrere Ziele wie EC2 Instances, Container und IP-Adressen in einer Availability Zone. Zur Gewährleistung einer hohen Verfügbarkeit stellen Sie sicher, dass Ihr ELB Instances aus mehreren Availability Zones registriert hat.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
8.1	Die IT-Systeme sollten schrittweise ausgebaut werden, da der Umfang und die Komplexität der NBFC-Abläufe zunehmen.	elbv2-multiple-az	Elastic Load Balancing (ELB) verteilt Ihren eingehenden Traffic automatisch auf mehrere Ziele wie EC2 Instances, Container und IP-Adressen in einer Availability Zone. Zur Gewährlei stung einer hohen Verfügbarkeit stellen Sie sicher, dass Ihr ELB Instances aus mehreren Availability Zones registriert hat.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
8.1	Die IT-Systeme sollten schrittweise ausgebaut werden, da der Umfang und die Komplexität der NBFC-Abläufe zunehmen.	lambda-vpc-multi-az-überprüfen	Wenn Ihre AWS Lambda-Funktion so konfiguriert ist, dass sie eine Verbindung zu einer Virtual Private Cloud (VPC) in Ihrem Konto herstellt, stellen Sie die AWS Lambda-Funktion in mindestens zwei verschiedenen Availability Zones bereit, um sicherzustellen, dass Ihre Funktion für die Verarbeitung von Ereignissen im Falle einer Dienstunterbrechung in einer einzigen Zone verfügbar ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
8.1	Die IT-Systeme sollten schrittweise ausgebaut werden, da der Umfang und die Komplexität der NBFC-Abläufe zunehmen.	rds-instance-deletion-protection-aktiviert	Stellen Sie sicher, dass Amazon Relational Database Service (Amazon RDS)-Instances den Löschschutz aktiviert haben. Verwenden Sie den Löschschutz, um zu verhindern, dass Ihre Amazon-RDS-Instances versehentlich oder böswillig gelöscht werden, was zum Verlust der Verfügbarkeit Ihrer Anwendungen führen kann.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
8.1	Die IT-Systeme sollten schrittweise ausgebaut werden, da der Umfang und die Komplexität der NBFC-Abläufe zunehmen.	rds-multi-az-support	Die Multi-AZ-Unterstützung in Amazon Relational Database Service (Amazon RDS) bietet eine verbesserte Verfügbarkeit und Beständigkeit von Datenbank-Instances. Wenn Sie eine Multi-AZ-Datenbank-Instance bereitstellen, erstellt Amazon RDS automatisch eine primäre Datenbank-Instance und repliziert die Daten synchron auf eine Standby-Instance in einer anderen Availability Zone. Jede Availability Zone läuft auf einer eigenen, physisch getrennten, unabhängigen Infrastruktur und ist auf eine hohe Verfügbarkeit ausgelegt. Im Falle eines Infrastrukturausfalls führt Amazon RDS einen automatis

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			chen Failover zum Standby-Modus durch, sodass Sie den Datenbankbetrieb wieder aufnehmen können, sobald der Failover abgeschlo ssen ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
8.1	Die IT-Systeme sollten schrittweise ausgebaut werden, da der Umfang und die Komplexität der NBFC-Abläufe zunehmen.	vpc-vpn-2-tunnels-up	Redundante Site-to-Site VPN-Tunnel können implementiert werden, um die Anforderungen an die Ausfallsicherheit zu erfüllen. Es verwendet zwei Tunnel, um die Konnektivität sicherzustellen, falls eine der Site-to-Site VPN-Verbindungen nicht verfügbar ist. Um sich vor einem Verbindungsverlust zu schützen, können Sie für den Fall, dass Ihr Kunden-Gateway nicht verfügbar ist, eine zweite Site-to-Site VPN-Verbindung zu Ihrer Amazon Virtual Private Cloud (Amazon VPC) und Ihrem Virtual Private Gateway einrichten, indem Sie ein zweites Kunden-Gateway verwenden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
8.1	Die IT-Systeme sollten schrittweise ausgebaut werden, da der Umfang und die Komplexität der NBFC-Abläufe zunehmen.	autoscaling-group-elb-healthcheck-erforderlich	Die Elastic Load Balancer (ELB) - Zustandsprüfungen für Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling Scaling-Gruppen unterstützen die Aufrechterhaltung einer angemessenen Kapazität und Verfügbarkeit. Der Load Balancer sendet regelmäßig Pings, versucht Verbindungen herzustellen oder sendet Anfragen, um den Zustand der EC2 Amazon-Instances in einer Gruppe mit auto-scaling zu testen. Wenn eine Instance nicht zurückmeldet, wird der Traffic an eine neue EC2 Amazon-Instance gesendet.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
8.1	Die IT-Systeme sollten schrittweise ausgebaut werden, da der Umfang und die Komplexität der NBFC-Abläufe zunehmen.	dynamodb-throughput-limit-check	Aktivieren Sie diese Regel, um sicherzustellen, dass die bereitgestellte Durchsatzkapazität in Ihren Amazon-DynamoDB-Tabellen überprüft wird. Dies ist der Umfang der Lese- und Schreibaktivitäten, der von den jeweiligen Tabellen unterstützt werden kann. DynamoDB verwendet diese Informationen für das Reservieren ausreichender Systemressourcen, um Ihren Durchsatz anforderungen gerecht zu werden. Diese Regel generiert eine Warnung, wenn sich der Durchsatz dem Höchstlimit für ein Kundenkonto nähert. Mit dieser Regel können Sie optional die Parameter RCUThreshold Kontoprozentsatz

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			(Konfigurationsstandard: 80) und WCUThreshold Kontoprozentsatz (Konfigurationsstandard: 80) festlegen. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.
8.1	Die IT-Systeme sollten schrittweise ausgebaut werden, da der Umfang und die Komplexität der NBFC-Abläufe zunehmen.	ec2- instance-detailed-monitoring-enabled	Aktivieren Sie diese Regel, um die Amazon Elastic Compute Cloud (Amazon EC2) - Instance-Überwachung auf der EC2 Amazon-Konsole zu verbessern, in der Monitoring-Diagramme mit einem Zeitraum von 1 Minute für die Instance angezeigt werden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
8.1	Die IT-Systeme sollten schrittweise ausgebaut werden, da der Umfang und die Komplexität der NBFC-Abläufe zunehmen.	guardduty-enabled-centralized	Amazon GuardDuty kann mithilfe von Threat Intellige nce Feeds helfen, potenzielle Cybersich erheitsereignisse zu überwachen und zu erkennen. Dazu gehören Listen mit bösartigen IPs und maschinel len Lernmethoden zur Identifizierung unerwarteter, nicht autorisierter und bösartiger Aktivitäten in Ihrer AWS Cloud-Umgebung.
8.1	Die IT-Systeme sollten schrittweise ausgebaut werden, da der Umfang und die Komplexität der NBFC-Abläufe zunehmen.	lambda-concurrency-check	Diese Regel stellt sicher, dass die Höchst- und Untergrenzen für die Gleichzeitigkeit einer Lambda-Funktion festgelegt werden. Dies kann Sie beim Baselining für die Anzahl der Anforderu ngen unterstützen, die Ihre Funktion zu einem bestimmten Zeitpunkt verarbeitet.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
8.1	Die IT-Systeme sollten schrittweise ausgebaut werden, da der Umfang und die Komplexität der NBFC-Abläufe zunehmen.	rds-enhanced-monitoring-enabled	Aktivieren Sie Amazon Relational Database Service (Amazon RDS), um die Verfügbarkeit von Amazon RDS zu überwachen. Dies bietet einen detaillierten Einblick in den Zustand Ihrer Amazon-RDS-Datenbank-Instances. Wenn der Amazon-RDS-Speicher mehr als ein zugrunde liegendes physisches Gerät verwendet, erfasst Enhanced Monitoring die Daten für jedes Gerät. Wenn die Datenbank-Instance von Amazon RDS in einer Multi-AZ-Bereitstellung ausgeführt wird, werden außerdem die Daten für jedes Gerät auf dem sekundären Host sowie die Metriken des sekundären Hosts erfasst.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
8.1	Die IT-Systeme sollten schrittweise ausgebaut werden, da der Umfang und die Komplexität der NBFC-Abläufe zunehmen.	securityhub-enabled	AWS Security Hub hilft bei der Überwachung von unbefugtem Personal, Verbindungen, Geräten und Software. AWS Security Hub aggregiert, organisiert und priorisiert die Sicherheitswarnungen oder Ergebnisse mehrerer Dienste. AWS Einige dieser Dienste sind Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer und AWS Firewall Manager sowie AWS Partnerlösungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
8.I	Grundlegende Sicherheitsaspekte wie physische/ logische Zugriffsk ontrollen und klar definierte Passwortr ichtlinien.	s-3 bucket-policy-gran tee-check	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie s3_ bucket_policy_gran tee_check aktiviere n. Diese Regel prüft, ob der vom Amazon S3 S3-Bucket gewährte Zugriff durch die von Ihnen bereitgestellten AWS Principals, Verbundbe nutzer, Service Principals, IP-Adress en oder Amazon Virtual Private Cloud (Amazon VPC) IDs eingeschränkt ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
8.I	Grundlegende Sicherheitsaspekte wie physische/ logische Zugriffsk ontrollen und klar definierte Passwortr ichtlinien.	dms-replication-not-public	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass auf DMS-Replikationsin stanzen nicht öffentlic h zugegriffen werden kann. DMS-Repli kations-Instances können vertrauli che Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.
8.I	Grundlegende Sicherheitsaspekte wie physische/ logische Zugriffsk ontrollen und klar definierte Passwortr ichtlinien.	ebs-snapshot-public-restorable-überprüfen	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass EBS-Snapshots nicht öffentlich wiederher stellbar sind. EBS-Volume-Snapsho ts können vertrauli che Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
8.I	Grundlegende Sicherheitsaspekte wie physische/ logische Zugriffsk ontrollen und klar definierte Passwortr ichtlinien.	ec-2 instance-no-public-ip	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon Elastic Compute Cloud (Amazon EC2) - Instances nicht öffentlich zugänglich sind. EC2 Amazon-Instances können vertrauliche Informati onen enthalten, und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
8.I	Grundlegende Sicherheitsaspekte wie physische/ logische Zugriffsk ontrollen und klar definierte Passwortr ichtlinien.	elasticsearch-in-vpc-only	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherste llen, dass sich Amazon OpenSearc h OpenSearch Service (Service) - Domains innerhalb einer Amazon Virtual Private Cloud (Amazon VPC) befinden. Eine OpenSearch Service-Domain innerhalb einer Amazon VPC ermöglicht die sichere Kommunikation zwischen OpenSearc h Service und anderen Services innerhalb der Amazon VPC, ohne dass ein Internet-Gateway, ein NAT-Gerät oder eine VPN-Verbindung erforderlich ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
8.I	Grundlegende Sicherheitsaspekte wie physische/ logische Zugriffsk ontrollen und klar definierte Passwortr ichtlinien.	emr-master-no-public-ip	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon EMR-Clust er-Masterknoten nicht öffentlich zugänglic h sind. Amazon-EM R-Cluster-Hauptkno ten können vertrauli che Informationen enthalten und für solche Konten ist eine Zugriffskontrolle erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
8.I	Grundlegende Sicherheitsaspekte wie physische/ logische Zugriffsk ontrollen und klar definierte Passwortr ichtlinien.	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) Security Groups können bei der Verwaltung des Netzwerkzugriffs helfen, indem sie eine statusbeh aftete Filterung von eingehendem und ausgehendem Netzwerkverkehr zu Ressourcen bereitste llen. AWS Wenn Sie eingehenden (oder entfernten) Datenverk ehr von 0.0.0.0/0 bis Port 22 auf Ihren Ressourcen nicht zulassen, können Sie den Remote-Zugriff einschränken.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
8.I	Grundlegende Sicherheitsaspekte wie physische/ logische Zugriffsk ontrollen und klar definierte Passwortr ichtlinien.	ec-2 instances-in-vpc	Stellen Sie Amazon Elastic Compute Cloud (Amazon EC2) -Instances innerhalb einer Amazon Virtual Private Cloud (Amazon VPC) bereit, um eine sichere Kommunika tion zwischen einer Instance und anderen Services innerhalb der Amazon VPC zu ermöglichen, ohne dass ein Internet-Gateway, ein NAT-Gerät oder eine VPN-Verbindung erforderlich ist. Der gesamte Datenverk ehr bleibt sicher in der AWS Cloud. Domains, die sich innerhalb einer VPC befinden, verfügen aufgrund ihrer logischen Isolierun g im Vergleich zu Domains mit öffentlic hen Endpunkten über eine zusätzlic he Sicherheitsebene. Weisen Sie EC2

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			Amazon-Instances einer Amazon-VPC zu, um den Zugriff ordnungsgemäß zu verwalten.
8.I	Grundlegende Sicherheitsaspekte wie physische/ logische Zugriffsk ontrollen und klar definierte Passwortr ichtlinien.	internet-gateway-a uthorized-vpc-nur	Verwalten Sie den Zugriff auf Ressource n in der AWS Cloud, indem Sie sicherste llen, dass Internet-Gateways nur mit autorisierter Amazon Virtual Private Cloud (Amazon VPC) verbunden sind. Internet-Gateways ermöglichen den bidirektionalen Internetzugang zur und von der Amazon VPC, was möglicher weise zu einem unbefugten Zugriff auf Amazon-VPC-Ressourcen führen kann.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
8.I	Grundlegende Sicherheitsaspekte wie physische/ logische Zugriffsk ontrollen und klar definierte Passwortr ichtlinien.	lambda-function-pu blic-access-verboten	Verwalten Sie den Zugriff auf Ressource n in der AWS Cloud, indem Sie sicherste llen, dass AWS Lambda-Funktionen nicht öffentlich zugänglich sind. Der öffentliche Zugriff kann möglicherweise die Verfügbarkeit von Ressourcen beeinträc htigen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
8.I	Grundlegende Sicherheitsaspekte wie physische/ logische Zugriffsk ontrollen und klar definierte Passwortr ichtlinien.	lambda-inside-vpc	Stellen Sie AWS Lambda-Funktionen in einer Amazon Virtual Private Cloud (Amazon VPC) bereit, um eine sichere Kommunika tion zwischen einer Funktion und anderen Diensten innerhalb der Amazon VPC zu gewährleisten. Bei dieser Konfiguration sind kein Internet-Gateway, kein NAT-Gerät und keine VPN-Verbindung erforderlich. Der gesamte Datenverk ehr bleibt sicher in der Cloud. AWS Domains, die sich innerhalb einer VPC befinden, verfügen aufgrund ihrer logischen Isolierun g im Vergleich zu Domains mit öffentlic hen Endpunkten über eine zusätzliche Sicherheitsebene. Um den Zugriff ordnungsg emäß zu verwalten,

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			sollten AWS Lambda-Funktionen einer VPC zugewiesen werden.
8.I	Grundlegende Sicherheitsaspekte wie physische/ logische Zugriffsk ontrollen und klar definierte Passwortr ichtlinien.	rds-instance-public-access-überprüfen	Verwalten Sie den Zugriff auf Ressource n in der AWS Cloud, indem Sie sicherste llen, dass Amazon Relational Database Service (Amazon RDS) -Instance s nicht öffentlic h sind. Amazon-RDS-Datenbank-Instances können vertrauliche Informati onen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
8.I	Grundlegende Sicherheitsaspekte wie physische/ logische Zugriffsk ontrollen und klar definierte Passwortr ichtlinien.	rds-snapshots-public-prohibited	Verwalten Sie den Zugriff auf Ressource n in der AWS Cloud, indem Sie sicherste llen, dass Amazon Relational Database Service (Amazon RDS) -Instance s nicht öffentlic h sind. Amazon-RDS-Datenbank-Instances können vertrauliche Informati onen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
8.I	Grundlegende Sicherheitsaspekte wie physische/ logische Zugriffsk ontrollen und klar definierte Passwortr ichtlinien.	redshift-cluster-public-access-überprüfen	Verwalten Sie den Zugriff auf Ressource n in der AWS Cloud, indem Sie sicherste llen, dass Amazon Redshift Redshift-Cluster nicht öffentlic h sind. Amazon-Re dshift-Cluster können vertrauliche Informati onen enthalten und für solche Konten sind Prinzipien und Zugriffskontrollen erforderlich.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
8.I	Grundlegende Sicherheitsaspekte wie physische/ logische Zugriffsk ontrollen und klar definierte Passwortr ichtlinien.	restricted-common-ports	Verwalten Sie den Zugriff auf Ressource n in der AWS Cloud, indem Sie sicherste llen, dass gemeinsam e Ports für Amazon Elastic Compute Cloud (Amazon EC2) -Sicherhe itsgruppen eingeschr ränkt sind. Wenn der Zugriff auf Ports nicht auf vertrauen swürdige Quellen beschränkt wird, kann dies zu Angriffen auf die Verfügbar keit, Integrität und Vertraulichkeit von Systemen führen. Mit dieser Regel können Sie optional die Parameter blockedPo rt1–blockedPort5 festlegen (Standard konfigurationen: 20, 21, 3389, 3306, 4333). Die tatsächli chen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
8.I	Grundlegende Sicherheitsaspekte wie physische/ logische Zugriffsk ontrollen und klar definierte Passwortr ichtlinien.	s3- account-level-publ ic-access -Block-pe riodisch	Verwalten Sie den Zugriff auf Ressource n in der AWS Cloud, indem Sie sicherste llen, dass Amazon Simple Storage Service (Amazon S3) -Buckets nicht öffentlich zugänglic h sind. Diese Regel trägt dazu bei, sensible Daten vor unbefugten Remote-Benutzern zu schützen, indem sie den öffentlichen Zugriff verhinder t. Mit dieser Regel können Sie optional die Parameter ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) und restrictPublicBuck ets Parameter (Config Default: True) festlegen. Die tatsächlichen Werte müssen den Richtlini

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			en Ihrer Organisation entsprechen.
8.I	Grundlegende Sicherheitsaspekte wie physische/ logische Zugriffsk ontrollen und klar definierte Passwortr ichtlinien.	s3- bucket-public-read -prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie nur autorisierten Benutzern, Prozessen und Geräten Zugriff auf Amazon Simple Storage Service (Amazon S3) - Buckets gewähren. Die Verwaltung des Zugriffs sollte mit der Klassifizierung der Daten übereinst immen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
8.I	Grundlegende Sicherheitsaspekte wie physische/ logische Zugriffsk ontrollen und klar definierte Passwortr ichtlinien.	s3- bucket-public-writ e-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie nur autorisierten Benutzern, Prozessen und Geräten Zugriff auf Amazon Simple Storage Service (Amazon S3) - Buckets gewähren. Die Verwaltung des Zugriffs sollte mit der Klassifizierung der Daten übereinst immen.
8.I	Grundlegende Sicherheitsaspekte wie physische/ logische Zugriffsk ontrollen und klar definierte Passwortr ichtlinien.	sagemaker-notebook -no-direct-Interne tzugang	Verwalten Sie den Zugriff auf Ressource n in der AWS Cloud, indem Sie sicherste llen, dass SageMaker Amazon-Notebooks keinen direkten Internetzugang zulassen. Indem Sie direkten Internetz ugang blockieren, vermeiden Sie, dass unbefugte Benutzer auf sensible Daten zugreifen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
8.I	Grundlegende Sicherheitsaspekte wie physische/ logische Zugriffsk ontrollen und klar definierte Passwortr ichtlinien.	vpc-default-security-group-geschlossen	Sicherheitsgruppen von Amazon Elastic Compute Cloud (Amazon EC2) können bei der Verwaltung des Netzwerkzugriffs helfen, indem sie eine statusbehaftete Filterung des ein- und ausgehenden Netzwerkverkehrs zu Ressourcen bereitstellen. AWS Die Beschränk ung des gesamten Datenverkehrs auf die Standardsicherheit sgruppe hilft dabei, den Fernzugriff auf Ihre Ressourcen einzuschränken. AWS

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
8.I	Grundlegende Sicherheitsaspekte wie physische/ logische Zugriffsk ontrollen und klar definierte Passwortr ichtlinien.	vpc-sg-open-only-to-authorized-ports	Verwalten Sie den Zugriff auf Ressource n in der AWS Cloud, indem Sie sicherste llen, dass gemeinsam e Ports für Amazon Elastic Compute Cloud (Amazon EC2) -Sicherhe itsgruppen eingeschr ränkt sind. Wenn der Zugriff auf Ports nicht auf vertrauen swürdige Quellen beschränkt wird, kann dies zu Angriffen auf die Verfügbar keit, Integrität und Vertraulichkeit von Systemen führen. Durch die Beschränk ung des Zugriffs auf Ressourcen innerhalb einer Sicherhei tsgruppe aus dem Internet (0.0.0.0/0) kann der Fernzugriff auf interne Systeme gesteuert werden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
8.I	Grundlegende Sicherheitsaspekte wie physische/ logische Zugriffsk ontrollen und klar definierte Passwortr ichtlinien.	access-keys-rotated	Die Anmeldein formationen für autorisierte Geräte, Benutzer und Prozesse werden geprüft, indem sichergestellt wird, dass die IAM-Zugri ffsschlüssel gemäß den Vorgaben der Unternehmensrichtl inie rotiert werden. Das regelmäßi ge Ändern der Zugriffsschlüssel ist eine bewährte Sicherheitsmethode . Es verkürzt den Zeitraum, in dem ein Zugriffsschlüssel aktiv ist, und reduziert die Auswirkungen auf das Unternehmen, wenn die Schlüssel kompromittiert werden. Diese Regel erfordert einen Wert für die Zugriffsschlüssel-Rotation (Standard konfiguration: 90). Der tatsächliche Wert muss den Richtlini

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			en Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
8.I	Grundlegende Sicherheitsaspekte wie physische/ logische Zugriffsk ontrollen und klar definierte Passwortr ichtlinien.	emr-kerberos-enabled	Die Zugriffsberechtigu ngen und -autorisi erungen können verwaltet und nach den Prinzipien der geringsten Berechtig ung und Aufgabent rennung integrier t werden, indem Kerberos für Amazon-EMR-Cluster aktiviert wird. In Kerberos werden Services und Benutzer, die sich authentif izieren müssen, als Prinzipale bezeichnet. Prinzipal e befinden sich in einem Kerberos-Bereich. Innerhalb dieses Bereichs wird ein Kerberos-Server als Key Distribution Center (KDC) bezeichnet. Über diesen Server können sich Prinzipal e authentifizieren. Die Authentifizierung im KDC erfolgt durch die Ausstellu ng von Authentif

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			izierungstickets. Das KDC unterhält eine Datenbank der Prinzipale in seinem Bereich mit ihren Passwörtern und anderen administr ativen Informationen zu jedem Prinzipal.
8.I	Grundlegende Sicherheitsaspekte wie physische/ logische Zugriffsk ontrollen und klar definierte Passwortr ichtlinien.	iam-group-has-users-überprüfen	AWS Identity and Access Managemen t (IAM) kann Ihnen helfen, die Prinzipien der geringsten Rechte und der Aufgabent rennung mit Zugriffsb erechtigungen und Autorisierungen zu integrieren, indem sichergestellt wird, dass IAM-Gruppen mindestens einen Benutzer haben. Die Einteilung von Benutzern in Gruppen auf der Grundlage der ihnen zugewiese nen Berechtigungen oder ihrer Funktion ist eine Möglichkeit, das Prinzip der geringste n Berechtigung zu implementieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
8.I	Grundlegende Sicherheitsaspekte wie physische/ logische Zugriffsk ontrollen und klar definierte Passwortr ichtlinien.	iam-no-inline-policy-überprüfen	Stellen Sie sicher, dass ein Benutzer, eine IAM-Rolle oder eine IAM-Gruppe (AWS Identity and Access Management) nicht über eine Inline-Richtlinie zur Zugriffsk ontrolle auf Systeme und Ressource n verfügt. AWS empfiehlt, verwaltet e Richtlinien anstelle von Inline-Richtlinien zu verwenden. Verwaltete Richtlini en ermöglichen Wiederverwendbarke it, Versionsverwaltung , Rollback und Delegierung der Berechtigungsverwa ltung.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
8.I	Grundlegende Sicherheitsaspekte wie physische/ logische Zugriffsk ontrollen und klar definierte Passwortr ichtlinien.	iam-password-policy	Die Identitäten und Anmeldeinformation en werden auf der Grundlage einer organisatorischen IAM-Passwortrichtlinie ausgestellt, verwaltet und verifiziert. Sie erfüllen oder übertreff en die Anforderungen von NIST SP 800-63 und dem Standard „Best Practices“ von AWS Foundatio nal Security für die Passwortstärke. Mit dieser Regel können Sie optional RequireUppercaseCh aracters (Wert für AWS grundlegende Sicherheitsbewährt e Methoden: wahr), RequireLowercaseCh aracters (Wert für bewährte Methoden für AWS grundlege nde Sicherheit: wahr), RequireSy mbols (Wert für bewährte Methoden für AWS grundlege nde Sicherheit:

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			wahr), RequireNumbers (Wert für bewährte Methoden für AWS grundlegende Sicherheit: wahr), MinimumPasswordLength (Wert für bewährte Methoden für AWS grundlegende Sicherheit: 14), PasswordReusePrevention (Wert für bewährte Methoden für AWS grundlegende Sicherheit: 24) und MaxPasswordAge (Wert für bewährte Methoden für AWS grundlegende Sicherheit: 90) für Ihr IAM festlegen. Kennwortrichtlinie. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
8.I	Grundlegende Sicherheitsaspekte wie physische/ logische Zugriffsk ontrollen und klar definierte Passwortr ichtlinien.	autoscaling-launch -config-public-ip- deaktiviert	Wenn Sie Ihre Netzwerkschnittstellen mit einer öffentlichen IP-Adresse konfiguri eren, sind die diesen Netzwerkschnittste llen zugehörigen Ressourcen über das Internet erreichba r. EC2 Ressourcen sollten nicht öffentlic h zugänglich sein, da dies einen unbeabsic htigten Zugriff auf Ihre Anwendungen oder Server ermöglichen kann.
8.I	Grundlegende Sicherheitsaspekte wie physische/ logische Zugriffsk ontrollen und klar definierte Passwortr ichtlinien.	ec2- instance-profile-a ttached	EC2 Instanzprofile übergeben eine IAM-Rolle an eine Instanz EC2 . Das Anhängen eines Instance-Profils an Ihre Instances kann bei der Implement ierung von geringste n Berechtigungen und der Berechtig ungsverwaltung helfen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
8.I	Grundlegende Sicherheitsaspekte wie physische/ logische Zugriffsk ontrollen und klar definierte Passwortr ichtlinien.	iam-policy-no-stat ements-with-full-a ccess	Stellen Sie sicher, dass IAM-Aktionen nur auf die benötigte n Aktionen beschränkt sind. Wenn Benutzern mehr Rechte eingeräumt werden, als für die Ausführun g einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringste n Rechte und der Aufgabentrennung verstoßen.
8.I	Grundlegende Sicherheitsaspekte wie physische/ logische Zugriffsk ontrollen und klar definierte Passwortr ichtlinien.	ecs-task-definition- nonroot-Benutzer	Sie bestimmen einen Nicht-Root-Benutzer für den Zugriff auf Ihre Aufgabendefinitionen des Amazon Elastic Container Service (Amazon ECS), um die Implementierung des Prinzips der geringsten Berechtig ung zu unterstützen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
8.I	Grundlegende Sicherheitsaspekte wie physische/ logische Zugriffsk ontrollen und klar definierte Passwortr ichtlinien.	efs-access-point-e nforce-Stammverzei chnis	Die Durchsetzung eines Stammverz eichnisses für einen Amazon-Elastic-Fil e-System-(Amazon-EFS-)Zugangspunkt trägt dazu bei, den Datenzugriff einzuschränken, indem sichergestellt wird, dass Benutzer des Zugangspu nkts nur auf Dateien des angegebenen Unterverzeichnisses zugreifen können.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
8.I	Grundlegende Sicherheitsaspekte wie physische/ logische Zugriffsk ontrollen und klar definierte Passwortr ichtlinien.	efs-access-point-e nforce-Benutzeride ntität	Um die Implement ierung des Prinzips der geringsten Rechte zu unterstützen, stellen Sie sicher, dass die Benutzerd urchsetzung für Ihr Amazon Elastic File System (Amazon EFS) aktiviert ist. Wenn diese Option aktiviert ist, ersetzt Amazon EFS den Benutzer und die Gruppe IDs des NFS-Clients durch die Identität, die auf dem Access Point für alle Dateisystemoperati onen konfiguriert ist, und gewährt nur Zugriff auf diese erzwungene Benutzeri dentität.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
8.I	Grundlegende Sicherheitsaspekte wie physische/ logische Zugriffsk ontrollen und klar definierte Passwortr ichtlinien.	s3- bucket-acl-prohibi ted	Diese Regel prüft, ob Access Control Lists (ACLs) für die Zugriffskontrolle auf Amazon S3 S3-Buckets verwendet werden. ACLs sind veraltete Zugriffsk ontrollmechanismen für Amazon S3 S3-Buckets, die älter sind als AWS Identity and Access Managemen t (IAM). Stattdess en empfiehlt es sich ACLs, IAM-Richtlinien oder S3-Bucket-Richtlinien zu verwenden, um den Zugriff auf Ihre S3-Buckets einfacher zu verwalten.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
8.I	Grundlegende Sicherheitsaspekte wie physische/ logische Zugriffsk ontrollen und klar definierte Passwortr ichtlinien.	s3- verboten bucket-le vel-public-access	Verwalten Sie den Zugriff auf Ressource n in der AWS Cloud, indem Sie sicherste llen, dass Amazon Simple Storage Service (Amazon S3) -Buckets nicht öffentlich zugänglic h sind. Diese Regel trägt dazu bei, sensible Daten vor unbefugten Remote-Benutzern zu schützen, indem sie den öffentlichen Zugriff auf Bucket-Eb ene verhindert.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
8.I	Grundlegende Sicherheitsaspekte wie physische/ logische Zugriffsk ontrollen und klar definierte Passwortr ichtlinien.	ssm-document-not-p ublic	Stellen Sie sicher, dass AWS Systems Manager (SSM) - Dokumente nicht öffentlich sind, da dies einen unbeabsic htigten Zugriff auf Ihre SSM-Dokum ente ermöglichen kann. Ein öffentlic hes SSM-Dokum ent kann Informati onen über Ihr Konto, Ihre Ressourcen und internen Prozesse preisgeben.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
8.I	Grundlegende Sicherheitsaspekte wie physische/ logische Zugriffsk ontrollen und klar definierte Passwortr ichtlinien.	subnet-auto-assign-public-ip-deaktiviert	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon Virtual Private Cloud (VPC) -Subnetzen nicht automatisch eine öffentliche IP-Adress e zugewiesen wird. Amazon Elastic Compute Cloud (EC2) -Instances, die in Subnetzen gestartet werden, in denen dieses Attribut aktiviert ist, haben ihrer primären Netzwerkschnittste lle eine öffentliche IP-Adresse zugewiesen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
8.I	Grundlegende Sicherheitsaspekte wie physische/ logische Zugriffsk ontrollen und klar definierte Passwortr ichtlinien.	iam-policy-no-stat ements-with-admin-access	AWS Identity and Access Managemen t (IAM) kann Ihnen dabei helfen, die Prinzipien der geringsten Rechte und der Aufgabent rennung in Zugriffsb erechtigungen und Autorisierungen zu integrieren und so zu verhindern, dass Richtlinien „Effect“: „Allow“ mit „Action“: „*“ anstelle von „Resource“: „*“ enthalten. Wenn Benutzern mehr Rechte eingeräum t werden, als für die Ausführung einer Aufgabe erforderl ich sind, kann dies gegen das Prinzip der geringsten Berechtigung und der Aufgabentrennung verstoßen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
8.I	Grundlegende Sicherheitsaspekte wie physische/ logische Zugriffsk ontrollen und klar definierte Passwortr ichtlinien.	iam-root-access-key-überprüfen	Der Zugriff auf Systeme und Ressourcen kann gesteuert werden, indem überprüft wird, ob der Root-Benu tzer keine Zugriffss chlüssel mit seiner AWS Identity and Access Management (IAM) -Rolle verknüpft hat. Stellen Sie sicher, dass die Root-Zugr iffsschlüssel gelöscht werden. Erstellen und verwenden Sie stattdessen rollenbas ierte Funktionen, AWS-Konten um das Prinzip der geringste n Funktionalität zu berücksichtigen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
8.I	Grundlegende Sicherheitsaspekte wie physische/ logische Zugriffskontrollen und klar definierte Passwortrichtlinien.	iam-user-group-membership-überprüfen	AWS Identity and Access Management (IAM) kann Ihnen helfen, Zugriffsberechtigungen und Autorisierungen einzuschränken, indem sichergestellt wird, dass Benutzer Mitglieder mindestens einer Gruppe sind. Wenn Benutzern mehr Berechtigungen eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und Aufgabentrennung verstoßen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
8.I	Grundlegende Sicherheitsaspekte wie physische/ logische Zugriffsk ontrollen und klar definierte Passwortr ichtlinien.	iam-user-mfa-enabled	Aktivieren Sie diese Regel, um den Zugriff auf Ressourcen in der AWS Cloud einzuschr änken. Diese Regel sorgt dafür, dass die Multi-Faktor-Authe ntifizierung (MFA) für alle Benutzer aktiviert ist. MFA sorgt für eine weitere Schutzebe ne zusätzlich zu den Anmeldeinformation en. Reduzieren Sie Fälle von kompromit tierten Konten, indem Sie MFA für Benutzer vorschreiben.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
8.I	Grundlegende Sicherheitsaspekte wie physische/ logische Zugriffsk ontrollen und klar definierte Passwortr ichtlinien.	iam-user-no-policies-überprüfen	Diese Regel stellt sicher, dass AWS Identity and Access Management (IAM) -Richtlinien nur Gruppen oder Rollen zugewiese n werden, um den Zugriff auf Systeme und Ressourcen zu kontrollieren. Die Zuweisung von Berechtig ungen auf Gruppen- oder Rollenebene trägt dazu bei, die Wahrscheinlichkeit zu verringern, dass eine Identität übermäßige Berechtigungen erhält oder beibehält.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
8.I	Grundlegende Sicherheitsaspekte wie physische/ logische Zugriffsk ontrollen und klar definierte Passwortr ichtlinien.	iam-user-unused-cr edentials-überprüfen	AWS Identity and Access Managemen t (IAM) kann Ihnen bei Zugriffsberechtigu ngen und Autorisie rungen helfen, indem es nach IAM-Passw örtern und Zugriffss chlüsseln sucht, die für einen bestimmte n Zeitraum nicht verwendet wurden. Wenn ungenutzte Anmeldeinformation en identifiziert werden, müssen Sie sie deaktivieren und/oder entfernen , da dies gegen das Prinzip der geringste n Berechtigung verstoßen könnte. Für diese Regel müssen Sie einen Wert für das maxCreden tialUsage Alter festlegen (Standard konfiguration: 90). Der tatsächliche Wert muss den Richtlini en Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
8.I	Grundlegende Sicherheitsaspekte wie physische/ logische Zugriffsk ontrollen und klar definierte Passwortr ichtlinien.	mfa-enabled-for-iam-Konsolenzugriff	Verwalten Sie den Zugriff auf Ressource n in der AWS Cloud, indem Sie sicherste llen, dass MFA für alle AWS Identity and Access Managemen t (IAM) -Benutzer aktiviert ist, die über ein Konsolenk ennwort verfügen. MFA sorgt für eine weitere Schutzebe ne zusätzlich zu den Anmeldeinformation en. Indem Sie MFA für Benutzer vorschrei ben, können Sie Fälle kompromittierter Konten reduzieren und verhindern, dass unbefugte Benutzer auf vertrauliche Daten zugreifen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
8.I	Grundlegende Sicherheitsaspekte wie physische/ logische Zugriffsk ontrollen und klar definierte Passwortr ichtlinien.	root-account-hardw are-mfa-aktiviert	Verwalten Sie den Zugriff auf Ressource n in der AWS Cloud, indem Sie sicherste llen, dass Hardware-MFA für den Root-Benutzer aktiviert ist. Der Stammbenutzer ist der AWS-Konto -Benutzer mit den meisten Berechtig ungen. MFA sorgt für eine weitere Schutzebene zusätzlic h zu den Anmeldein formationen. Indem Sie MFA für den Root-Benutzer vorschrei ben, können Sie die Anzahl AWS-Konte n kompromittierter Benutzer reduzieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
8.I	Grundlegende Sicherheitsaspekte wie physische/ logische Zugriffsk ontrollen und klar definierte Passwortr ichtlinien.	opensearch-in-vpc-only	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass sich Amazon OpenSearch Service-Domains innerhalb einer Amazon Virtual Private Cloud (Amazon VPC) befinden. Eine Amazon OpenSearc h Service-Domain innerhalb einer Amazon VPC ermöglicht die sichere Kommunikation zwischen Amazon OpenSearch Service und anderen Services innerhalb der Amazon VPC, ohne dass ein Internet-Gateway, ein NAT-Gerät oder eine VPN-Verbindung erforderlich ist.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
8.I	Grundlegende Sicherheitsaspekte wie physische/ logische Zugriffsk ontrollen und klar definierte Passwortr ichtlinien.	root-account-mfa-e nabled	Verwalten Sie den Zugriff auf Ressource n in der AWS Cloud, indem Sie sicherste llen, dass MFA für den Root-Benutzer aktiviert ist. Der Stammbenutzer ist der AWS-Konto-Benutzer mit den meisten Berechtig ungen. MFA sorgt für eine weitere Schutzebene zusätzlic h zu den Anmeldein formationen. Indem Sie MFA für den Root-Benutzer vorschrei ben, können Sie die Anzahl AWS-Konte n kompromittierter Benutzer reduzieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
8.I	Grundlegende Sicherheitsaspekte wie physische/logische Zugriffskontrollen und klar definierte Passwortrichtlinien.	secretsmanager-rotation-enabled-check	Diese Regel stellt sicher, dass bei AWS Secrets Manager Manager-Geheimnissen die Rotation aktiviert ist. Die regelmäßige Rotation von Secrets kann den Zeitraum verkürzen, in dem ein Secret aktiv ist, und möglicherweise die Auswirkungen auf das Unternehmen verringern, falls das Secret kompromittiert wird.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
8.I	Grundlegende Sicherheitsaspekte wie physische/ logische Zugriffsk ontrollen und klar definierte Passwortr ichtlinien.	secretsmanager-sch eduled-rotation-su ccess-überprüfen	Diese Regel stellt sicher, dass AWS Secrets Manager Manager-Geheimnisse gemäß dem Rotations plan erfolgreich rotiert wurden. Die regelmäßige Rotation von Secrets kann den Zeitraum verkürzen, in dem ein Secret aktiv ist, und möglicherweise die Auswirkungen auf das Unternehm en verringern, falls es kompromittiert wird.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
8.II	Eine klar definierte Benutzerrolle.	iam-group-has-users-überprüfen	AWS Identity and Access Managemen t (IAM) kann Ihnen helfen, die Prinzipien der geringsten Rechte und der Aufgabent rennung mit Zugriffsb erechtigungen und Autorisierungen zu integrieren, indem sichergestellt wird, dass IAM-Gruppen mindestens einen Benutzer haben. Die Einteilung von Benutzern in Gruppen auf der Grundlage der ihnen zugewiese nen Berechtigungen oder ihrer Funktion ist eine Möglichkeit, das Prinzip der geringste n Berechtigung zu implementieren.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
8.II	Eine klar definierte Benutzerrolle.	iam-no-inline-policy-überprüfen	Stellen Sie sicher, dass ein Benutzer, eine IAM-Rolle oder eine IAM-Gruppe (AWS Identity and Access Management) nicht über eine Inline-Richtlinie zur Zugriffskontrolle auf Systeme und Ressourcen verfügt. AWS empfiehlt, verwaltete Richtlinien anstelle von Inline-Richtlinien zu verwenden. Verwaltete Richtlinien ermöglichen Wiederverwendbarkeit, Versionsverwaltung, Rollback und Delegierung der Berechtigungsverwaltung.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
8.II	Eine klar definierte Benutzerrolle.	iam-password-policy	Die Identitäten und Anmeldeinformationen werden auf der Grundlage einer organisatorischen IAM-Passwortrichtlinie ausgestellt, verwaltet und verifiziert. Sie erfüllen oder übertreffen die Anforderungen von NIST SP 800-63 und dem Standard „Best Practices“ von AWS Foundational Security für die Passwortstärke. Mit dieser Regel können Sie optional RequireUppercaseCharacters (Wert für AWS grundlegende Sicherheitsbewährte Verfahren: wahr), RequireLowercaseCharacters (Wert für bewährte Methoden für AWS grundlegende Sicherheit: wahr), RequireSymbols (Wert für bewährte Methoden für AWS grundlegende Sicherheit:

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			wahr), RequireNumbers (Wert für bewährte Methoden für AWS grundlegende Sicherheit: wahr), MinimumPasswordLength (Wert für bewährte Methoden für AWS grundlegende Sicherheit: 14), PasswordReusePrevention (Wert für bewährte Methoden für AWS grundlegende Sicherheit: 24) und MaxPasswordAge (Wert für bewährte Methoden für AWS grundlegende Sicherheit: 90) für Ihr IAM festlegen Kennwortrichtlinie. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
8.II	Eine klar definierte Benutzerrolle.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) kann Ihnen dabei helfen, die Prinzipien der geringsten Rechte und der Aufgabentrennung in Zugriffsberechtigungen und Autorisierungen zu integrieren und so zu verhindern, dass Richtlinien „Effect“: „Allow“ mit „Action“: „*“ anstelle von „Resource“: „*“ enthalten. Wenn Benutzern mehr Rechte eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und der Aufgabentrennung verstoßen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
8.II	Eine klar definierte Benutzerrolle.	iam-user-group-membership-überprüfen	AWS Identity and Access Management (IAM) kann Ihnen helfen, Zugriffsberechtigungen und Autorisierungen einzuschränken, indem sichergestellt wird, dass Benutzer Mitglieder mindestens einer Gruppe sind. Wenn Benutzern mehr Berechtigungen eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und Aufgabentrennung verstoßen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
8.II	Eine klar definierte Benutzerrolle.	iam-user-no-policies-überprüfen	Diese Regel stellt sicher, dass AWS Identity and Access Management (IAM) -Richtlinien nur Gruppen oder Rollen zugewiese n werden, um den Zugriff auf Systeme und Ressourcen zu kontrollieren. Die Zuweisung von Berechtig ungen auf Gruppen- oder Rollenebene trägt dazu bei, die Wahrscheinlichkeit zu verringern, dass eine Identität übermäßige Berechtigungen erhält oder beibehält.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
8.II	Eine klar definierte Benutzerrolle.	iam-user-unused-credentials-überprüfen	AWS Identity and Access Management (IAM) kann Ihnen bei Zugriffsberechtigungen und Autorisierungen helfen, indem es nach IAM-Passwörtern und Zugriffsschlüsseln sucht, die für einen bestimmten Zeitraum nicht verwendet wurden. Wenn ungenutzte Anmeldeinformationen identifiziert werden, müssen Sie sie deaktivieren und/oder entfernen, da dies gegen das Prinzip der geringsten Berechtigung verstoßen könnte. Für diese Regel müssen Sie einen Wert für das maxCredentialUsage Alter festlegen (Standardkonfiguration: 90). Der tatsächliche Wert muss den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
8.III	Ein Maker-Checker-Konzept zur Verringerung des Fehler- und Missbrauchsrisikos und zur Sicherstellung der Zuverlässigkeit von Daten/Informationen.	s-3 bucket-versioning-enabled	Die Versionsverwaltung von Amazon Simple Storage Service (Amazon S3)-Buckets hilft dabei, mehrere Varianten eines Objekts im selben Amazon-S3-Bucket zu speichern. Verwenden Sie die Versionsverwaltung, um sämtliche Versionen aller Objekte in Ihrem Amazon-S3-Bucket zu speichern, abzurufen oder wiederherzustellen. Mit der Versionsverwaltung können Sie Versionen sowohl nach unbeabsichtigten Benutzeraktionen als auch nach Anwendungsfehlern problemlos wiederherstellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
8.IX	Anordnung zur Sicherung von Daten mit regelmäßigen Tests.	db-instance-backup-enabled	Die Sicherungsfunktion von Amazon RDS erstellt Sicherungen Ihrer Datenbanken und Transaktionsprotokolle. Amazon RDS erstellt einen Snapshot für das Speichervolume Ihrer DB-Instance, sodass die gesamte DB-Instance gesichert wird. Sie können im System spezifische Aufbewahrungsfristen festlegen, um Ihre Ausfallsicherheitsanforderungen zu erfüllen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
8.IX	Anordnung zur Sicherung von Daten mit regelmäßigen Tests.	dynamodb-in-backup-plan	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon DynamoDB-Tabellen Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
8.IX	Anordnung zur Sicherung von Daten mit regelmäßigen Tests.	dynamodb-pitr-enabled	Aktivieren Sie diese Regel, um zu überprüfen, ob die Informationen gesichert wurden. Es verwaltet auch die Backups, indem es sicherstellt, dass die point-in-time Wiederherstellung in Amazon DynamoDB aktiviert ist. Bei der Wiederherstellung werden fortlaufende Backups Ihrer Tabelle für die letzten 35 Tage gespeichert.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
8.IX	Anordnung zur Sicherung von Daten mit regelmäßigen Tests.	ebs-in-backup-plan	Stellen Sie zur Unterstützung der Datensicherungspro zesse sicher, dass Ihre Amazon Elastic Block Store (Amazon EBS) -Volumes Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwaltet er Backup-Service mit einer richtlini enbasierten Backup-Lösung. Diese Lösung vereinfac ht Ihr Sicherung smanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforde rungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
8.IX	Anordnung zur Sicherung von Daten mit regelmäßigen Tests.	efs-in-backup-plan	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon Elastic File System (Amazon EFS) -Dateisysteme Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
8.IX	Anordnung zur Sicherung von Daten mit regelmäßigen Tests.	elasticache-redis-cluster-automatic-Backup-Check	Wenn automatische Backups aktiviert sind, ElastiCache erstellt Amazon täglich ein Backup des Clusters. Die Sicherung kann für eine von Ihrer Organisation festgelegte Anzahl von Tagen aufbewahrt werden. Automatische Backups schützen vor Datenverlust. Bei einem Ausfall können Sie einen neuen Cluster erstellen, der Ihre Daten aus dem aktuellen Backup wiederherstellt.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
8.IX	Anordnung zur Sicherung von Daten mit regelmäßigen Tests.	rds-in-backup-plan	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihre Amazon Relational Database Service (Amazon RDS) -Instances Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
8.IX	Anordnung zur Sicherung von Daten mit regelmäßigen Tests.	s-3 bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) Cross-Region Replication (CRR) unterstützt die Aufrechterhaltung einer angemessenen Kapazität und Verfügbarkeit. CRR ermöglicht das automatische, asynchrone Kopieren von Objekten in Amazon S3 Buckets, um die Datenverfügbarkeit sicherzustellen.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
8.IX	Anordnung zur Sicherung von Daten mit regelmäßigen Tests.	redshift-backup-enabled	Stellen Sie zur Unterstützung der Datensicherungsprozesse sicher, dass Ihre Amazon-Redshift-Cluster über automatisierte Snapshots verfügen. Wenn automatisierte Snapshots für einen Cluster aktiviert sind, erstellt Redshift in regelmäßigen Abständen Snapshots dieses Clusters. Standardmäßig erstellt Redshift alle acht Stunden oder alle 5 GB einen Snapshot für jeden Knoten mit Datenänderungen oder je nachdem, was zuerst eintritt.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
8.IX	Anordnung zur Sicherung von Daten mit regelmäßigen Tests.	backup-plan-min-frequency-and-min-retention-check	Um Sie bei Datensicherungsprozessen zu unterstützen, stellen Sie sicher, dass Ihr AWS Backup-Plan auf eine Mindestfrequenz und Aufbewahrung festgelegt ist. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen. Mit dieser Regel können Sie die Parameter requiredFrequencyValue (Config default: 1), requiredRetentionDays (Config default: 35) und requiredFrequencyUnit

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			(Config default: days) festlegen. Der tatsächliche Wert muss den Anforderungen Ihrer Organisation entsprechen.
8.IX	Anordnung zur Sicherung von Daten mit regelmäßigen Tests.	backup-recovery-point-manual-löschen-deaktiviert	Stellen Sie sicher, dass Ihren AWS Backup-Wiederherstellungspunkten eine ressourcenbasierte Richtlinie zugeordnet ist, die das Löschen von Wiederherstellungspunkten verhindert. Die Verwendung einer ressourcenbasierten Richtlinie zur Verhinderung des Löschens von Wiederherstellungspunkten kann dazu beitragen, ein versehentliches oder absichtliches Löschen zu unterbinden.

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
8.IX	Anordnung zur Sicherung von Daten mit regelmäßigen Tests.	backup-recovery-point-minimum-Aufbewahrungsprüfung	Um bei Datensicherungsprozessen zu helfen, stellen Sie sicher, dass für Ihre AWS Backup-Wiederherstellungspunkte eine Mindestaufbewahrungsdauer festgelegt ist. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen. Mit dieser Regel können Sie den Parameter requiredRetentionDays (Config Default: 35) festlegen. Der tatsächliche Wert muss den Anforderu

Kontroll-ID	Beschreibung der Kontrolle	AWS Config	Empfehlungen
			ngen Ihrer Organisat ion entsprechen.

Vorlage

Die Vorlage ist verfügbar unter GitHub: Operational Best Practices for RBI MD-ITF.

Bewährte Methoden für Sicherheits-, Identitäts- und Compliance-Services

Dieses Konformitätspaket enthält AWS Config Regeln, die auf Security, Identity und Compliance Services basieren. Weitere Informationen finden Sie unter Sicherheit, Identität und Compliance unter AWS. Eine Liste aller verwalteten Regeln, die von unterstützt werden AWS Config, finden Sie unter Liste der AWS Config verwalteten Regeln.

Die Namen und Beschreibungen der erforderlichen Parameter finden Sie im `Parameters` Abschnitt der folgenden Vorlage.

Die Vorlage ist verfügbar unter GitHub: Operational Best Practices for Security, Identity and Compliance Services.

Bewährte Methoden für die Ausführung von Serverless

Dieses Konformitätspaket enthält AWS Config Regeln, die auf serverlosen Lösungen basieren. Eine Liste aller verwalteten Regeln, die von unterstützt werden AWS Config, finden Sie unter Liste der AWS Config verwalteten Regeln.

Die Namen und Beschreibungen der erforderlichen Parameter finden Sie im `Parameters` Abschnitt der folgenden Vorlage.

Die Vorlage ist verfügbar unter GitHub: Operational Best Practices for Serverless.

Bewährte Methoden für die Ausführung von Speicherservices

Dieses Conformance Pack enthält AWS Config Regeln, die auf Storage Services basieren. Weitere Informationen finden Sie unter Cloud Storage on AWS. Eine Liste aller verwalteten Regeln, die von unterstützt werden AWS Config, finden Sie unter Liste der AWS Config verwalteten Regeln.

Die Namen und Beschreibungen der erforderlichen Parameter finden Sie im `Parameters` Abschnitt der folgenden Vorlage.

Die Vorlage ist verfügbar unter GitHub: Operational Best Practices for Storage Services.

Bewährte Methoden für die Ausführung von SWIFT-CSP

Konformitätspakete bieten ein allgemeines Compliance-Framework, das es Ihnen ermöglicht, mithilfe verwalteter oder benutzerdefinierter AWS Config Regeln und Abhilfemaßnahmen Kontrollen zur Sicherheits-, Betriebs- oder Kostenoptimierung durchzuführen. AWS Config Conformance Packs dienen als Beispielvorlagen nicht dazu, die vollständige Einhaltung eines bestimmten Governance- oder Compliance-Standards sicherzustellen. Sie sind dafür verantwortlich, selbst zu beurteilen, ob Ihre Nutzung der Services den geltenden gesetzlichen und behördlichen Anforderungen entspricht.

Im Folgenden finden Sie ein Beispiel für eine Zuordnung zwischen dem Customer Security Programme (CSP) von SWIFT und den verwalteten AWS -Konfigurationsregeln. Jede AWS Config Regel gilt für eine bestimmte AWS Ressource und bezieht sich auf eine oder mehrere SWIFT-CSP-Kontrollen. Eine SWIFT-CSP-Steuerung kann sich auf mehrere AWS Config Regeln beziehen. In der folgenden Tabelle finden Sie weitere Informationen und Anleitungen zu diesen Zuordnungen.

Kontroll-ID	AWS Config	Empfehlungen
1.1	ec2-manager instance-managed-by-systems	Eine Bestandsaufnahme der Softwareplattformen und Anwendungen innerhalb des Unternehmens ist möglich, indem Amazon Elastic Compute Cloud (Amazon EC2) -Instances mit AWS Systems Manager verwaltet werden. Verwenden Sie AWS Systems Manager, um detaillierte Systemkonfigurationen, Betriebssystem-Patch-Levels, Namen und Typ der Dienste, Softwareinstallationen, Anwendungsname, Herausgeber und Version

Kontroll-ID	AWS Config	Empfehlungen
		sowie andere Details zu Ihrer Umgebung bereitzustellen.
1.1	ec2- instance-no-public-ip	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie sicherstellen, dass Amazon Elastic Compute Cloud (Amazon EC2) -Instances nicht öffentlich zugänglich sind. EC2 Amazon-Instances können vertrauliche Informati onen enthalten, und für solche Konten ist eine Zugriffsk ontrolle erforderlich.
1.1	ec2- no-amazon-key-pair	Diese Regel prüft, ob laufende Amazon Elastic Compute Cloud (Amazon EC2) - Instances mit Amazon-Sc hlüsselpaaren gestartet werden. Dies kann dazu beitragen, das Risiko kompromittierter Anmeldein formationen zu verringern. Auf EC2 Amazon-Instances ohne Schlüsselpaare kann weiterhin über den Session Manager oder eine browserbasierte SSH-Verbindung von der AWS Konsole aus zugegriffen werden.

Kontroll-ID	AWS Config	Empfehlungen
1.1	ec2- instances-in-vpc	Stellen Sie Amazon Elastic Compute Cloud (Amazon EC2) -Instances innerhalb einer Amazon Virtual Private Cloud (Amazon VPC) bereit, um eine sichere Kommunika tion zwischen einer Instance und anderen Services innerhalb der Amazon VPC zu ermöglichen, ohne dass ein Internet-Gateway, ein NAT-Gerät oder eine VPN-Verbi ndung erforderlich ist. Der gesamte Datenverkehr bleibt sicher in der AWS Cloud. Domains, die sich innerhalb einer VPC befinden, verfügen aufgrund ihrer logischen Isolierung im Vergleich zu Domains mit öffentlic hen Endpunkten über eine zusätzliche Sicherheitsebene. Weisen Sie EC2 Amazon-In stances einer Amazon-VPC zu, um den Zugriff ordnungsg emäß zu verwalten.

Kontroll-ID	AWS Config	Empfehlungen
1.1	vpc-default-security-group-geschlossen	Sicherheitsgruppen von Amazon Elastic Compute Cloud (Amazon EC2) können bei der Verwaltung des Netzwerkzugriffs helfen, indem sie eine statusbeh aftete Filterung des ein- und ausgehenden Netzwerkv erkehrs zu Ressourcen bereitstellen. AWS Die Beschränkung des gesamten Datenverkehrs auf die Standardsicherheitsgruppe hilft dabei, den Fernzugriff auf Ihre Ressourcen einzuschr änken. AWS
1.1	vpc-network-acl-unused-überprüfen	Diese Regel stellt sicher, dass Amazon Virtual Private Cloud (VPC)-Netzwerkzugr iffskontrolllisten verwendet werden. Die Überwachu ng ungenutzter Netzwerkz ugriffskontrolllisten kann zu einer genauen Inventari sierung und Verwaltung Ihrer Umgebung beitragen.

Kontroll-ID	AWS Config	Empfehlungen
1.1	vpc-sg-open-only-to-authorized-ports	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass gemeinsame Ports für Amazon Elastic Compute Cloud (Amazon EC2) - Sicherheitsgruppen eingeschränkt sind. Wenn der Zugriff auf Ports nicht auf vertrauenswürdige Quellen beschränkt wird, kann dies zu Angriffen auf die Verfügbarkeit, Integrität und Vertraulichkeit von Systemen führen. Durch die Beschränkung des Zugriffs auf Ressourcen innerhalb einer Sicherheitsgruppe aus dem Internet (0.0.0.0/0) kann der Fernzugriff auf interne Systeme gesteuert werden.

Kontroll-ID	AWS Config	Empfehlungen
1.2	iam-customer-policy-blocked-kms-Aktionen	AWS Identity and Access Management (IAM) kann Ihnen helfen, die Prinzipien der geringsten Rechte und der Aufgabentrennung in Zugriffsberechtigungen und Autorisierungen zu integrier en und so zu verhindern, dass Richtlinien blockierte Aktionen für alle AWS Schlüssel des Key Management Service enthalten. Wenn Benutzer mehr Rechte haben, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtig ung und Aufgabentrennung verstoßen. Mit dieser Regel können Sie den Parameter festlegen. blockedActionsPatt erns (Wert „AWS Bewährte grundlegende Sicherhei tsmethoden“: kms: Decrypt, kms:ReEncryptFrom). Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisat ion entsprechen.

Kontroll-ID	AWS Config	Empfehlungen
1.2	iam-group-has-users-überprüfen	AWS Identity and Access Management (IAM) kann Ihnen helfen, die Prinzipien der geringsten Rechte und der Aufgabentrennung mit Zugriffsberechtigungen und Autorisierungen zu integrieren, indem sichergestellt wird, dass IAM-Gruppen mindestens einen Benutzer haben. Die Einteilung von Benutzern in Gruppen auf der Grundlage der ihnen zugewiesenen Berechtigungen oder ihrer Funktion ist eine Möglichkeit, das Prinzip der geringsten Berechtigung zu implementieren.

Kontroll-ID	AWS Config	Empfehlungen
1.2	iam-inline-policy-blocked-kms-Aktionen	Stellen Sie sicher, dass ein Benutzer, eine IAM-Rolle oder eine IAM-Grupp e (AWS Identity and Access Management) nicht über eine Inline-Richtlinie verfügt, die blockierte Aktionen für alle AWS Schlüssel des Key Management Service zulässt. AWS empfiehlt, verwaltete Richtlinien anstelle von Inline-Richtlinien zu verwenden . Verwaltete Richtlinien ermöglichen Wiederver wendbarkeit, Versionsv erwaltung, Rollback und Delegierung der Berechtig ungsverwaltung. Mit dieser Regel können Sie den blockedActionsPatterns Parameter festlegen. (Wert „AWS Bewährte grundlege nde Sicherheitsmethoden“: kms: Decrypt, kms:ReEnc ryptFrom). Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprech en.

Kontroll-ID	AWS Config	Empfehlungen
1.2	iam-no-inline-policy-überprüfen	Stellen Sie sicher, dass ein Benutzer, eine IAM-Rolle oder eine IAM-Gruppe (AWS Identity and Access Management) nicht über eine Inline-Richtlinie zur Zugriffskontrolle auf Systeme und Ressourcen verfügt. AWS empfiehlt, verwaltete Richtlinien anstelle von Inline-Richtlinien zu verwenden . Verwaltete Richtlinien ermöglichen Wiederverwendbarkeit, Versionsverwaltung, Rollback und Delegierung der Berechtigungsverwaltung.
1.2	iam-user-no-policies-überprüfen	Diese Regel stellt sicher, dass AWS Identity and Access Management (IAM) -Richtlinien nur Gruppen oder Rollen zugewiesen werden, um den Zugriff auf Systeme und Ressourcen zu kontrollieren. Die Zuweisung von Berechtigungen auf Gruppen- oder Rollenebene trägt dazu bei, die Wahrscheinlichkeit zu verringern, dass eine Identität übermäßige Berechtigungen erhält oder beibehält.

Kontroll-ID	AWS Config	Empfehlungen
1.2	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) Security Groups können bei der Verwaltung des Netzwerkz ugriffs helfen, indem sie eine statusbehaftete Filterung von eingehendem und ausgehend em Netzwerkverkehr zu Ressourcen bereitstellen. AWS Wenn Sie eingehenden (oder entfernten) Datenverk ehr von 0.0.0.0/0 bis Port 22 auf Ihren Ressourcen nicht zulassen, können Sie den Remote-Zugriff einschränken.
1.2	nacl-no-unrestricted-ssh-rdp	Der Zugriff auf Remote-Se rveradministrationsports in Ihren Network Access Control Lists (NACLs), wie Port 22 (SSH) und Port 3389 (RDP), sollte nicht öffentlich zugänglich sein, da dies einen unbeabsichtigten Zugriff auf Ressourcen innerhalb Ihrer VPC ermöglichen kann.

Kontroll-ID	AWS Config	Empfehlungen
1.2	s-3 bucket-acl-prohibited	Diese Regel prüft, ob Access Control Lists (ACLs) für die Zugriffskontrolle auf Amazon S3 S3-Buckets verwendet werden. ACLs sind veraltete Zugriffskontrollmechanismen für Amazon S3 S3-Buckets, die älter sind als AWS Identity and Access Management (IAM). Stattdessen empfiehlt es sich ACLs, IAM-Richtlinien oder S3-Bucket-Richtlinien zu verwenden, um den Zugriff auf Ihre S3-Buckets einfacher zu verwalten.

Kontroll-ID	AWS Config	Empfehlungen
1.2	s-3 bucket-logging-enabled	Die Amazon Simple Storage Service (Amazon S3)-Serve rzugriffsprotokollierung bietet eine Methode zur Überwachung des Netzwerks im Hinblick auf potenzielle Cybersicherheitsereignisse. Die Ereignisse werden überwacht, indem detaillie rte Aufzeichnungen über die Anfragen erfasst werden, die an einen Amazon-S3-Bucket gestellt wurden. Jeder Zugriffsprotokolleintrag enthält Details zu einer einzelnen Zugriffsanfrage. Zu den Details gehören Auftragge ber, Bucket-Name, Anforderu ngszeit, Anforderungsaktion, Antwortstatus und Fehlercode, falls relevant.
1.2	s-3 bucket-policy-grantee-check	Verwalten Sie den Zugriff auf die AWS Cloud, indem Sie s3_bucket_policy_grantee_check aktivieren. Diese Regel prüft, ob der vom Amazon S3 S3-Bucket gewährte Zugriff durch die von Ihnen bereitgestellten AWS Principals, Verbundbe nutzer, Service Principals, IP-Adressen oder Amazon Virtual Private Cloud (Amazon VPC) IDs eingeschränkt ist.

Kontroll-ID	AWS Config	Empfehlungen
1.2	sns-topic-message-delivery-Benachrichtigung aktiviert	Zur Erfüllung der Protokoll ierungsanforderungen in Ihrer Umgebung stellen Sie sicher, dass Versandstatusbenac hrichtigungen für Ihre Amazon Simple Notification Service (Amazon SNS)-Themen aktiviert sind. Die Protokoll ierung des Nachrichtenzustell ungsstatus hilft dabei, bessere Einblicke in Prozesse zu erhalten. Beispiele hierfür sind das Wissen, ob eine Nachricht an den Amazon-SNS-Endpunk t zugestellt wurde, das Ermitteln der vom Amazon-SNS-Endpunkt an Amazon SNS gesendeten Antwort und das Bestimmen der Verweilda uer der Nachricht (die Zeit zwischen dem Veröffent lichungszeitstempel und dem Zeitpunkt kurz vor der Übergabe an einen Amazon-SNS-Endpunkt).

Kontroll-ID	AWS Config	Empfehlungen
1.4	internet-gateway-authorized-vpc-nur	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Internet-Gateways nur mit autorisierter Amazon Virtual Private Cloud (Amazon VPC) verbunden sind. Internet-Gateways ermöglichen den bidirekti onalen Internetzugang zur und von der Amazon VPC, was möglicherweise zu einem unbefugten Zugriff auf Amazon-VPC-Ressourcen führen kann.

Kontroll-ID	AWS Config	Empfehlungen
1.4	restricted-common-ports	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass gemeinsame Ports für Amazon Elastic Compute Cloud (Amazon EC2) - Sicherheitsgruppen eingeschränkt sind. Wenn der Zugriff auf Ports nicht auf vertrauenswürdige Quellen beschränkt wird, kann dies zu Angriffen auf die Verfügbarkeit, Integrität und Vertraulichkeit von Systemen führen. Mit dieser Regel können Sie optional die Parameter blockedPort1–blockedPort5 festlegen (Standardkonfigurationen: 20, 21, 3389, 3306, 4333). Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.
1.4	lambda-function-public-access-verboten	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass AWS Lambda-Funktionen nicht öffentlich zugänglich sind. Der öffentliche Zugriff kann möglicherweise die Verfügbarkeit von Ressourcen beeinträchtigen.

Kontroll-ID	AWS Config	Empfehlungen
1.4	s3- -Block-periodisch account-level-public-access	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Simple Storage Service (Amazon S3) -Buckets nicht öffentlich zugänglich sind. Diese Regel trägt dazu bei, sensible Daten vor unbefugten Remote-Benutzern zu schützen, indem sie den öffentlichen Zugriff verhindert. Mit dieser Regel können Sie optional die Parameter ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) und restrictPublicBuckets Parameter (Config Default: True) festlegen. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	AWS Config	Empfehlungen
1.4	s3 bucket-level-public-access -verboten	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Amazon Simple Storage Service (Amazon S3) -Buckets nicht öffentlich zugänglich sind. Diese Regel trägt dazu bei, sensible Daten vor unbefugten Remote-Benutzern zu schützen, indem sie den öffentlichen Zugriff auf Bucket-Ebene verhindert.
1.4	s-3 bucket-public-read-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie nur autorisierten Benutzern, Prozessen und Geräten Zugriff auf Amazon Simple Storage Service (Amazon S3) -Buckets gewähren. Die Verwaltung des Zugriffs sollte mit der Klassifizierung der Daten übereinstimmen.

Kontroll-ID	AWS Config	Empfehlungen
1.4	s3- bucket-public-write-prohibited	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie nur autorisierten Benutzern, Prozessen und Geräten Zugriff auf Amazon Simple Storage Service (Amazon S3) -Buckets gewähren. Die Verwaltung des Zugriffs sollte mit der Klassifizierung der Daten übereinstimmen.
1.4	ssm-document-not-public	Stellen Sie sicher, dass AWS Systems Manager (SSM) -Dokumente nicht öffentlich sind, da dies einen unbeabsichtigten Zugriff auf Ihre SSM-Dokumente ermöglichen kann. Ein öffentliches SSM-Dokument kann Informationen über Ihr Konto, Ihre Ressourcen und internen Prozesse preisgeben.

Kontroll-ID	AWS Config	Empfehlungen
2.3	ec2-imdsv2-check	Stellen Sie sicher, dass die Methode Instance Metadata Service Version 2 (IMDSv2) aktiviert ist, um den Zugriff auf und die Kontrolle der Amazon Elastic Compute Cloud (Amazon EC2) -Instance-Metadaten zu schützen. Die IMDSv2 Methode verwendet sitzungsbasierte Kontrolle n. Mit können Kontrollen implementiert werden IMDSv2, um Änderungen an Instanzme tadaten einzuschränken.
2.3	ec-2 instance-multiple-eni-check	Diese Regel prüft, ob Ihre Amazon Elastic Compute Cloud (Amazon EC2) - Instances mehrere haben ENIs. Wenn mehrere vorhanden sind, ENIs kann dies zu doppelt vernetzte n Instanzen führen, d. h. zu Instanzen mit mehreren Subnetzen. Dies kann die Komplexität der Netzwerks icherheit erhöhen und unbeabsichtigte Netzwerkp fade und Zugriffe zur Folge haben.

Kontroll-ID	AWS Config	Empfehlungen
2.3	ec-2 token-hop-limit-check	Stellen Sie sicher, dass die HTTP-PUT-Antwort des Instance Metadata Service (IMDS) auf die Amazon Elastic Compute Cloud (Amazon EC2) -Instance beschränkt ist. Mit kann die PUT-Antwort IMDSv2, die standardmäßig das geheime Token enthält, die Instance nicht verlassen , da das Metadaten-Antwort-Hop-Limit auf 1 gesetzt ist (Konfigurationsstandard). Wenn dieser Wert größer als 1 ist, kann das Token die EC2 Instance verlassen.
2.3	ec2- volume-inuse-check	Diese Regel stellt sicher, dass Amazon Elastic Block Store-Volumes, die an Amazon Elastic Compute Cloud (Amazon EC2) -Instances angehängt sind, zum Löschen markiert werden, wenn eine Instance beendet wird. Wenn ein Amazon-EBS-Volume nicht gelöscht wird, wenn die Instance, an die es angehängt ist, beendet wird, kann dies gegen das Konzept der geringsten Funktionalität verstoßen.

Kontroll-ID	AWS Config	Empfehlungen
2.3	account-part-of-organizations	Durch die zentrale Verwaltung AWS-Konten innerhalb von AWS Organizations wird sichergestellt, dass die Konten den Vorschriften entsprechen. Eine fehlende zentrale Kontoverwaltung kann zu inkonsistenten Kontokonfigurationen führen, wodurch Ressourcen und sensible Daten offengelegt werden können.

Kontroll-ID	AWS Config	Empfehlungen
2.3	lambda-inside-vpc	Stellen Sie AWS Lambda-Funktionen in einer Amazon Virtual Private Cloud (Amazon VPC) bereit, um eine sichere Kommunikation zwischen einer Funktion und anderen Diensten innerhalb der Amazon VPC zu gewährleisten. Bei dieser Konfiguration sind kein Internet-Gateway, kein NAT-Gerät und keine VPN-Verbindung erforderlich. Der gesamte Datenverkehr bleibt sicher in der Cloud. AWS Domains, die sich innerhalb einer VPC befinden, verfügen aufgrund ihrer logischen Isolierung im Vergleich zu Domains mit öffentlichen Endpunkten über eine zusätzliche Sicherheitsebene. Um den Zugriff ordnungsgemäß zu verwalten, sollten AWS Lambda-Funktionen einer VPC zugewiesen werden.

Kontroll-ID	AWS Config	Empfehlungen
2.3	kms-cmk-not-scheduled-zum Löschen	Um Daten im Ruhezustand zu schützen, sollten Sie sicherstellen, dass die für den Kunden erforderlichen Masterschlüssel (CMKs) nicht für das Löschen im AWS Key Management Service (AWS KMS) vorgesehen sind. Da Schlüssel manchmal gelöscht werden müssen, können Sie mit dieser Regel alle zu löschenden Schlüssel überprüfen, falls ein Schlüssel versehentlich zur Löschung vorgemerkt wurde.

Kontroll-ID	AWS Config	Empfehlungen
2.3	s3- bucket-versioning-enabled	Die Versionsverwaltung von Amazon Simple Storage Service (Amazon S3)-Buckets hilft dabei, mehrere Varianten eines Objekts im selben Amazon-S3-Bucket zu speichern. Verwenden Sie die Versionsverwaltung, um sämtliche Versionen aller Objekte in Ihrem Amazon-S3-Bucket zu speichern, abzurufen oder wiederher zustellen. Mit der Versionsv erwaltung können Sie Versionen sowohl nach unbeabsichtigten Benutzera ktionen als auch nach Anwendungsfehlern problemlo s wiederherstellen.

Kontroll-ID	AWS Config	Empfehlungen
2.3	secretsmanager-secret-unused	Wenn in AWS Secrets Manager unbenutzte Anmeldeinformationen vorhanden sind, sollten Sie die Anmeldeinformationen deaktivieren und/oder entfernen, da dies gegen das Prinzip der geringsten Rechte verstoßen kann. Mit dieser Regel können Sie einen Wert auf unusedForDays (Config Default: 90) setzen. Der tatsächliche Wert muss den Richtlinien Ihrer Organisation entsprechen.
2.5A	ebs-in-backup-plan	Stellen Sie zur Unterstützung der Datensicherungsprozesse sicher, dass Ihre Amazon Elastic Block Store (Amazon EBS) -Volumes Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherungsmanagement und erleichtert Ihnen die Erfüllung von geschäftlichen und behördlichen Compliance-Anforderungen hinsichtlich Datensicherungen.

Kontroll-ID	AWS Config	Empfehlungen
2.5A	ec-2 ebs-encryption-by-default	Zum Schutz von Daten im Ruhezustand müssen Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon Elastic Block Store (Amazon EBS)-Volumes aktiviert ist. Um eventuell vorhandene sensible Daten im Ruhezustand zu schützen, müssen Sie die Verschlüsselung von Daten im Ruhezustand aktivieren.
2.5A	efs-encrypted-check	Aktivieren Sie die Verschlüs selung für Ihr Amazon Elastic File System (EFS), um eventuell vorhandene sensible Daten sowie Daten im Ruhezustand zu schützen.

Kontroll-ID	AWS Config	Empfehlungen
2.5A	efs-in-backup-plan	Um Sie bei Datensich erungsprozessen zu unterstüt zen, stellen Sie sicher, dass Ihre Amazon Elastic File System (Amazon EFS) - Dateisysteme Teil eines AWS Backup-Plans sind. AWS Backup ist ein vollständig verwalteter Backup-Service mit einer richtlinienbasierten Backup-Lösung. Diese Lösung vereinfacht Ihr Sicherung smanagement und erleichte rt Ihnen die Erfüllung von geschäftlichen und behördlic hen Compliance-Anforde rungen hinsichtlich Datensich erungen.
2.5A	encrypted-volumes	Um eventuell vorhandene sensible Daten sowie Daten im Ruhezustand zu schützen, muss die Verschlüsselung für Ihre Amazon Elastic Block Store (Amazon EBS)-Volumes aktiviert sein.
2.5A	kinesis-stream-encrypted	Aktivieren Sie die Verschlüs selung für Ihre Amazon-Ki nesis-Streams, um eventuell vorhandene sensible Daten sowie Daten im Ruhezustand zu schützen.

Kontroll-ID	AWS Config	Empfehlungen
2.5A	s3-fähig bucket-server-side-encryption	Zum Schutz von Daten im Ruhezustand müssen Sie sicherstellen, dass die Verschlüsselung für Ihre Amazon Simple Storage Service (Amazon S3)-Buckets aktiviert ist. Um eventuell vorhandene sensible Daten im Ruhezustand in Amazon-S3-Buckets zu schützen, muss die Verschlüsselung aktiviert sein.
2.5A	s-3 default-encryption-kms	Stellen Sie sicher, dass die Verschlüsselung für Ihre Amazon Simple Storage Service (Amazon S3)-Buckets aktiviert ist. Um eventuell vorhandene sensible Daten im Ruhezustand in einem Amazon-S3-Bucket zu schützen, muss die Verschlüsselung aktiviert sein.

Kontroll-ID	AWS Config	Empfehlungen
2.5A	sns-encrypted-kms	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass Ihre Amazon Simple Notification Service (Amazon SNS) -Themen mit dem AWS Key Management Service (AWS KMS) verschlüsselt werden müssen. Um eventuell vorhandene sensible Daten im Ruhezustand in veröffentlichten Nachrichten zu schützen, muss die Verschlüsselung von Daten im Ruhezustand aktiviert sein.

Kontroll-ID	AWS Config	Empfehlungen
4.1	iam-password-policy	Die Identitäten und Anmeldein formationen werden auf der Grundlage einer organisat orischen IAM-Passwortrichtl inie ausgestellt, verwaltet und verifiziert. Sie erfüllen oder übertreffen die Anforderungen von NIST SP 800-63 und dem Standard „Best Practices“ von AWS Foundational Security für die Passwortstärke. Mit dieser Regel können Sie optional RequireUppercaseCharacters (Wert für AWS grundlege nde Sicherheitsbewährte Methoden: wahr), RequireLo wercaseCharacters (Wert für bewährte Methoden für AWS grundlegende Sicherheit: wahr), RequireSymbols (Wert für bewährte Methoden für AWS grundlegende Sicherhei t: wahr), RequireNumbers (Wert für bewährte Methoden für AWS grundlegende Sicherheit: wahr), MinimumPa sswordLength (Wert für bewährte Methoden für AWS grundlegende Sicherheit: 14), PasswordReusePreve ntion (Wert für bewährte Methoden für AWS grundlege nde Sicherheit: 24) und MaxPasswordAge (Wert

Kontroll-ID	AWS Config	Empfehlungen
		für bewährte Methoden für AWS grundlegende Sicherhei t: 90) für Ihr IAM festlegen Kennwortrichtlinie. Die tatsächlichen Werte müssen den Richtlinien Ihrer Organisat ion entsprechen.
4.1	access-keys-rotated	Die Anmeldeinformationen für autorisierte Geräte, Benutzer und Prozesse werden geprüft, indem sichergestellt wird, dass die IAM-Zugriffsschlüs sel gemäß den Vorgaben der Unternehmensrichtlinie rotiert werden. Das regelmäßige Ändern der Zugriffsschlüssel ist eine bewährte Sicherhei tsmethode. Es verkürzt den Zeitraum, in dem ein Zugriffsschlüssel aktiv ist, und reduziert die Auswirkun gen auf das Unternehmen, wenn die Schlüssel kompromit tiert werden. Diese Regel erfordert einen Wert für die Zugriffsschlüssel-Rotation (Standardkonfiguration: 90). Der tatsächliche Wert muss den Richtlinien Ihrer Organisat ion entsprechen.

Kontroll-ID	AWS Config	Empfehlungen
4.2	iam-user-mfa-enabled	Aktivieren Sie diese Regel, um den Zugriff auf Ressourcen in der AWS Cloud einzuschränken. Diese Regel sorgt dafür, dass die Multi-Faktor-Authentifizierung (MFA) für alle Benutzer aktiviert ist. MFA sorgt für eine weitere Schutzebene zusätzlich zu den Anmeldeinformationen. Reduzieren Sie Fälle von kompromittierten Konten, indem Sie MFA für Benutzer vorschreiben.
4.2	mfa-enabled-for-iam-Konsolenzugriff	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass MFA für alle AWS Identity and Access Management (IAM) -Benutzer aktiviert ist, die über ein Konsolenkennwort verfügen. MFA sorgt für eine weitere Schutzebene zusätzlich zu den Anmeldeinformationen. Indem Sie MFA für Benutzer vorschreiben, können Sie Fälle kompromittierter Konten reduzieren und verhindern, dass unbefugte Benutzer auf vertrauliche Daten zugreifen.

Kontroll-ID	AWS Config	Empfehlungen
4.2	root-account-hardware-mfa-aktiviert	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass Hardware-MFA für den Root-Benutzer aktiviert ist. Der Stammbenutzer ist der AWS-Konto-Benutzer mit den meisten Berechtigungen. MFA sorgt für eine weitere Schutzebene zusätzlich zu den Anmeldeinformationen. Indem Sie MFA für den Root-Benutzer vorschreiben, können Sie die Anzahl AWS-Konten kompromittierter Benutzer reduzieren.
4.2	root-account-mfa-enabled	Verwalten Sie den Zugriff auf Ressourcen in der AWS Cloud, indem Sie sicherstellen, dass MFA für den Root-Benutzer aktiviert ist. Der Stammbenutzer ist der AWS-Konto-Benutzer mit den meisten Berechtigungen. MFA sorgt für eine weitere Schutzebene zusätzlich zu den Anmeldeinformationen. Indem Sie MFA für den Root-Benutzer vorschreiben, können Sie die Anzahl AWS-Konten kompromittierter Benutzer reduzieren.

Kontroll-ID	AWS Config	Empfehlungen
5.1	ec-2 instance-profile-attached	EC2 Instanzprofile übergeben eine IAM-Rolle an eine EC2 Instance. Das Anhängen eines Instance-Profils an Ihre Instances kann bei der Implementierung von geringsten Berechtigungen und der Berechtigungsverwa ltung helfen.
5.1	iam-policy-no-statements-with-full-access	Stellen Sie sicher, dass IAM-Aktionen nur auf die benötigte n Aktionen beschränkt sind. Wenn Benutzern mehr Berechtigungen eingeräumt werden, als für die Ausführun g einer Aufgabe erforderl ich sind, kann dies gegen das Prinzip der geringsten Berechtigung und Aufgabent rennung verstoßen.

Kontroll-ID	AWS Config	Empfehlungen
5.1	iam-root-access-key-überprüfen	Der Zugriff auf Systeme und Ressourcen kann gesteuert werden, indem überprüft wird, ob der Root-Benutzer keine Zugriffsschlüssel mit seiner AWS Identity and Access Management (IAM) -Rolle verknüpft hat. Stellen Sie sicher, dass die Root-Zugriffsschlüssel gelöscht werden. Erstellen und verwenden Sie stattdessen rollenbasierte Funktionen, AWS-Konten um das Prinzip der geringsten Funktionalität zu berücksichtigen.
5.1	iam-user-group-membership-überprüfen	AWS Identity and Access Management (IAM) kann Ihnen helfen, Zugriffsberechtigungen und Autorisierungen einzuschränken, indem sichergestellt wird, dass Benutzer Mitglieder mindestens einer Gruppe sind. Wenn Benutzern mehr Berechtigungen eingeräumt werden, als für die Ausführung einer Aufgabe erforderlich sind, kann dies gegen das Prinzip der geringsten Berechtigung und Aufgabentrennung verstoßen.

Kontroll-ID	AWS Config	Empfehlungen
5.1	iam-user-unused-credentials-überprüfen	AWS Identity and Access Management (IAM) kann Ihnen bei Zugriffsberechtigungen und Autorisierungen helfen, indem es nach IAM-Passwörtern und Zugriffsschlüsseln sucht, die für einen bestimmten Zeitraum nicht verwendet wurden. Wenn ungenutzte Anmeldeinformationen identifiziert werden, müssen Sie sie deaktivieren und/oder entfernen, da dies gegen das Prinzip der geringsten Berechtigung verstoßen könnte. Für diese Regel müssen Sie einen Wert für das maxCredentialUsage Alter festlegen (Standardkonfiguration: 90). Der tatsächliche Wert muss den Richtlinien Ihrer Organisation entsprechen.

Kontroll-ID	AWS Config	Empfehlungen
5.4	secretsmanager-rotation-enabled-check	Diese Regel stellt sicher, dass bei AWS Secrets Manager Manager-Geheimnissen die Rotation aktiviert ist. Die regelmäßige Rotation von Secrets kann den Zeitraum verkürzen, in dem ein Secret aktiv ist, und möglicherweise die Auswirkungen auf das Unternehmen verringern, falls das Secret kompromittiert wird.
5.4	secretsmanager-scheduled-rotation-success-überprüfen	Diese Regel stellt sicher, dass AWS Secrets Manager Manager-Geheimnisse gemäß dem Rotationsplan erfolgreich rotiert wurden. Die regelmäßige Rotation von Secrets kann den Zeitraum verkürzen, in dem ein Secret aktiv ist, und möglicherweise die Auswirkungen auf das Unternehmen verringern, falls es kompromittiert wird.

Kontroll-ID	AWS Config	Empfehlungen
5.4	secretsmanager-secret-periodic-rotation	Diese Regel stellt sicher, dass bei AWS Secrets Manager Manager-Geheimnissen die regelmäßige Rotation aktiviert ist. Die regelmäßige Rotation von Secrets kann den Zeitraum verkürzen, in dem ein Secret aktiv ist, und möglicherweise die Auswirkungen auf das Unternehmen verringern, falls das Secret kompromittiert wird. Der Standardwert lautet 90 Tage.
5.4	secretsmanager-using-cmk	Um Daten im Ruhezustand zu schützen, stellen Sie sicher, dass die Verschlüsselung mit dem AWS Key Management Service (AWS KMS) für AWS Secrets Manager aktiviert ist. Aktivieren Sie die Verschlüsselung von Daten im Ruhezustand, um eventuell vorhandene sensible Daten im Ruhezustand im Secrets Manager zu schützen.

Kontroll-ID	AWS Config	Empfehlungen
6.4	ec2- instance-detailed-monitoring-enabled	Aktivieren Sie diese Regel, um die Amazon Elastic Compute Cloud (Amazon EC2) -Instance-Überwachung auf der EC2 Amazon-Konsole zu verbessern, in der Monitoring-Diagramme mit einem Zeitraum von 1 Minute für die Instance angezeigt werden.
6.4	cloudwatch-log-group-encrypted	Um sensible Daten im Speicher zu schützen, stellen Sie sicher, dass die Verschlüsselung für Ihre Amazon CloudWatch Log Groups aktiviert ist.
6.4	cloud-trail-cloud-watch-Logs aktiviert	Verwenden Sie Amazon CloudWatch , um Protokollereignisaktivitäten zentral zu sammeln und zu verwalten . Die Aufnahme von AWS CloudTrail Daten liefert Einzelheiten zu den API-Aufrufaktivitäten in Ihrem AWS-Konto.

Kontroll-ID	AWS Config	Empfehlungen
6.4	cloudtrail-enabled	AWS CloudTrail kann bei der Nichtabstreitbarkeit helfen, indem Aktionen und API-Aufrufe der AWS Managemen t Console aufgezeichnet werden. Sie können die Benutzer und die Benutzer AWS-Konten , die einen AWS Dienst aufgerufen haben, die Quell-IP-Adresse, über die die Aufrufe generiert wurden, und den Zeitpunkt der Anrufe identifizieren. Einzelheiten zu den erfassten Daten finden Sie in den AWS CloudTrail Datensatzinhalten.
6.4	cloud-trail-encryption-enabled	Da sensible Daten vorhanden sein können und um Daten im Speicher zu schützen, sollten Sie sicherstellen, dass die Verschlüsselung für Ihre AWS CloudTrail Spuren aktiviert ist.

Kontroll-ID	AWS Config	Empfehlungen
6.4	cloud-trail-log-file-Validierung aktiviert	Verwenden Sie die AWS CloudTrail Protokolldateivalidierung, um die Integrität von Protokollen zu überprüfen. CloudTrail Mithilfe der Protokolldateivalidierung kann festgestellt werden, ob eine Protokolldatei geändert oder gelöscht wurde oder ob sie nach der Übermittlung CloudTrail unverändert geblieben ist. Dieses Feature wurde mit dem Branchenstandard entsprechenden Algorithmen entwickelt: SHA-256 für die Hashfunktion und SHA-256 mit RSA für digitale Signaturen. Aus diesem Grund ist es rechnerisch unmöglich, CloudTrail Protokolldateien unbemerkt zu ändern, zu löschen oder zu fälschen.

Kontroll-ID	AWS Config	Empfehlungen
6.4	ec2-stopped-instance	Aktivieren Sie diese Regel, um bei der Basiskonfiguration von Amazon Elastic Compute Cloud (Amazon EC2) - Instances zu helfen, indem Sie überprüfen, ob EC2 Amazon-Instances gemäß den Standards Ihrer Organisation für mehr als die zulässige Anzahl von Tagen gestoppt wurden.
6.4	vpc-flow-logs-enabled	VPC-Flow-Protokolle erfassen detaillierte Informationsdatensätze über den IP-Datenverkehr, der zu und von Netzwerkschnittstellen in Ihrer Amazon Virtual Private Cloud (Amazon VPC) fließt. Standardmäßig enthalten Flow-Protokolldatensätze Werte für die verschiedenen Komponenten des IP-Flows, einschließlich Quelle, Ziel und Protokoll.

Kontroll-ID	AWS Config	Empfehlungen
6.5A	guardduty-enabled-centralized	Amazon GuardDuty kann mithilfe von Threat Intellige nce Feeds helfen, potenzielle Cybersicherheitsereignisse zu überwachen und zu erkennen. Dazu gehören Listen mit bösartigen IPs und maschinel len Lernmethoden zur Identifiz ierung unerwarteter, nicht autorisierter und bösartige r Aktivitäten in Ihrer AWS Cloud-Umgebung.
6.5A	securityhub-enabled	AWS Security Hub hilft bei der Überwachung von unbefugte m Personal, Verbindungen, Geräten und Software. AWS Security Hub aggregiert, organisiert und priorisiert die Sicherheitswarnungen oder Ergebnisse mehrerer Dienste. AWS Einige dieser Dienste sind Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer und AWS Firewall Manager sowie AWS Partnerlösungen.

Vorlage

Die Vorlage ist verfügbar unter GitHub: Operational Best Practices for SWIFT CSP.

Bewährte Methoden für die Sicherheit in Amazon Elastic Container Service (Amazon ECS)

Dieses Konformitätspaket enthält AWS Config Regeln, die auf Amazon ECS basieren. Eine Liste aller verwalteten Regeln, die von unterstützt werden AWS Config, finden Sie unter Liste der AWS Config verwalteten Regeln.

Die Namen und Beschreibungen der erforderlichen Parameter finden Sie im `Parameters` Abschnitt der folgenden Vorlage.

Die Vorlage ist verfügbar unter GitHub: Bewährte Sicherheitsmethoden für Amazon ECS.

Bewährte Methoden für die Sicherheit in Amazon Elastic File System (Amazon EFS)

Dieses Conformance Pack enthält AWS Config Regeln, die auf Amazon EFS basieren. Eine Liste aller verwalteten Regeln, die von unterstützt werden AWS Config, finden Sie unter Liste der AWS Config verwalteten Regeln.

Die Namen und Beschreibungen der erforderlichen Parameter finden Sie im `Parameters` Abschnitt der folgenden Vorlage.

Die Vorlage ist verfügbar unter GitHub: Bewährte Sicherheitsmethoden für Amazon EFS.

Bewährte Methoden für die Sicherheit in Amazon Elastic Kubernetes Service (Amazon EKS)

Dieses Konformitätspaket enthält AWS Config Regeln, die auf Amazon EKS basieren. Eine Liste aller verwalteten Regeln, die von unterstützt werden AWS Config, finden Sie unter Liste der AWS Config verwalteten Regeln.

Die Namen und Beschreibungen der erforderlichen Parameter finden Sie im `Parameters` Abschnitt der folgenden Vorlage.

Die Vorlage ist verfügbar unter GitHub: Bewährte Sicherheitsmethoden für Amazon EKS.

Bewährte Sicherheitsmethoden für Amazon CloudFront

Dieses Konformitätspaket enthält AWS Config Regeln, die auf Amazon CloudFront basieren. Eine Liste aller verwalteten Regeln, die von unterstützt werden AWS Config, finden Sie unter Liste der AWS Config verwalteten Regeln.

Die Namen und Beschreibungen der erforderlichen Parameter finden Sie im `Parameters` Abschnitt der folgenden Vorlage.

Die Vorlage ist verfügbar unter GitHub: Security Best Practices for Amazon CloudFront.

Bewährte Sicherheitsmethoden für Amazon OpenSearch Service

Dieses Konformitätspaket enthält AWS Config Regeln, die auf Amazon OpenSearch Service basieren. Eine Liste aller verwalteten Regeln, die von unterstützt werden AWS Config, finden Sie unter Liste der AWS Config verwalteten Regeln.

Die Namen und Beschreibungen der erforderlichen Parameter finden Sie im `Parameters` Abschnitt der folgenden Vorlage.

Die Vorlage ist verfügbar unter GitHub: Bewährte Sicherheitsmethoden für Amazon OpenSearch Service.

Bewährte Methoden für die Sicherheit in Amazon Redshift

Dieses Conformance Pack enthält AWS Config Regeln, die auf Amazon Redshift basieren. Eine Liste aller verwalteten Regeln, die von unterstützt werden AWS Config, finden Sie unter Liste der AWS Config verwalteten Regeln.

Die Namen und Beschreibungen der erforderlichen Parameter finden Sie im `Parameters` Abschnitt der folgenden Vorlage.

Die Vorlage ist verfügbar unter GitHub: Bewährte Sicherheitsmethoden für Amazon Redshift.

Bewährte Methoden für die Sicherheit in Amazon Relational Database Service (Amazon RDS)

Dieses Conformance Pack enthält AWS Config Regeln, die auf Amazon RDS basieren. Eine Liste aller verwalteten Regeln, die von unterstützt werden AWS Config, finden Sie unter Liste der AWS Config verwalteten Regeln.

Die Namen und Beschreibungen der erforderlichen Parameter finden Sie im `Parameters` Abschnitt der folgenden Vorlage.

Die Vorlage ist verfügbar unter GitHub: Bewährte Sicherheitsmethoden für Amazon RDS.

Bewährte Sicherheitsmethoden für AWS Auto Scaling

Dieses Konformitätspaket enthält AWS Config Regeln, die auf AWS Auto Scaling basieren. Eine Liste aller verwalteten Regeln, die von unterstützt werden AWS Config, finden Sie unter Liste der AWS Config verwalteten Regeln.

Die Namen und Beschreibungen der erforderlichen Parameter finden Sie im `Parameters` Abschnitt der folgenden Vorlage.

Die Vorlage ist verfügbar unter GitHub: Bewährte Sicherheitsmethoden für AWS Auto Scaling.

Bewährte Sicherheitsmethoden für AWS CloudTrail

Dieses Konformitätspaket enthält AWS Config Regeln, die auf AWS CloudTrail basieren. Eine Liste aller verwalteten Regeln, die von unterstützt werden AWS Config, finden Sie unter Liste der AWS Config verwalteten Regeln.

Die Namen und Beschreibungen der erforderlichen Parameter finden Sie im `Parameters` Abschnitt der folgenden Vorlage.

Die Vorlage ist verfügbar unter GitHub: Bewährte Sicherheitsmethoden für AWS CloudTrail.

Bewährte Sicherheitsmethoden für AWS CodeBuild

Dieses Konformitätspaket enthält AWS Config Regeln, die auf AWS CodeBuild basieren. Eine Liste aller verwalteten Regeln, die von unterstützt werden AWS Config, finden Sie unter Liste der AWS Config verwalteten Regeln.

Die Namen und Beschreibungen der erforderlichen Parameter finden Sie im `Parameters` Abschnitt der folgenden Vorlage.

Die Vorlage ist verfügbar unter GitHub: Bewährte Sicherheitsmethoden für AWS CodeBuild.

Bewährte Methoden für die Sicherheit in Amazon ECR

Dieses Konformitätspaket enthält AWS Config Regeln, die auf Amazon Elastic Container Registry (Amazon ECR) basieren. Eine Liste aller verwalteten Regeln, die von unterstützt werden AWS Config, finden Sie unter Liste der AWS Config verwalteten Regeln.

Die Namen und Beschreibungen der erforderlichen Parameter finden Sie im `Parameters` Abschnitt der folgenden Vorlage.

Die Vorlage ist verfügbar unter GitHub: Security Best Practices for Amazon ECR.

Bewährte Sicherheitsmethoden für AWS Lambda

Dieses Konformitätspaket enthält AWS Config Regeln, die auf AWS Lambda basieren. Eine Liste aller verwalteten Regeln, die von unterstützt werden AWS Config, finden Sie unter Liste der AWS Config verwalteten Regeln.

Die Namen und Beschreibungen der erforderlichen Parameter finden Sie im `Parameters` Abschnitt der folgenden Vorlage.

Die Vorlage ist verfügbar unter GitHub: Bewährte Sicherheitsmethoden für AWS Lambda.

Bewährte Sicherheitsmethoden für AWS Network Firewall

Dieses Konformitätspaket enthält AWS Config Regeln, die auf AWS Network Firewall basieren. Eine Liste aller verwalteten Regeln, die von unterstützt werden AWS Config, finden Sie unter Liste der AWS Config verwalteten Regeln.

Die Namen und Beschreibungen der erforderlichen Parameter finden Sie im `Parameters` Abschnitt der folgenden Vorlage.

Die Vorlage ist verfügbar unter GitHub: Bewährte Sicherheitsmethoden für AWS Network Firewall.

Bewährte Sicherheitsmethoden für Amazon SageMaker AI

Dieses Konformitätspaket enthält AWS Config Regeln, die auf Amazon SageMaker AI basieren. Eine Liste aller verwalteten Regeln, die von unterstützt werden AWS Config, finden Sie unter Liste der AWS Config verwalteten Regeln.

Die Namen und Beschreibungen der erforderlichen Parameter finden Sie im `Parameters` Abschnitt der folgenden Vorlage.

Die Vorlage ist verfügbar unter GitHub: Bewährte Sicherheitsmethoden für Amazon SageMaker AI.

Bewährte Sicherheitsmethoden für AWS Secrets Manager

Dieses Konformitätspaket enthält AWS Config Regeln, die auf AWS Secrets Manager basieren. Eine Liste aller verwalteten Regeln, die von unterstützt werden AWS Config, finden Sie unter Liste der AWS Config verwalteten Regeln.

Die Namen und Beschreibungen der erforderlichen Parameter finden Sie im `Parameters` Abschnitt der folgenden Vorlage.

Die Vorlage ist verfügbar unter GitHub: Bewährte Sicherheitsmethoden für AWS Secrets Manager.

Bewährte Sicherheitsmethoden für AWS WAF

Dieses Konformitätspaket enthält AWS Config Regeln, die auf AWS WAF basieren. Eine Liste aller verwalteten Regeln, die von unterstützt werden AWS Config, finden Sie unter Liste der AWS Config verwalteten Regeln.

Die Namen und Beschreibungen der erforderlichen Parameter finden Sie im `Parameters` Abschnitt der folgenden Vorlage.

Die Vorlage ist verfügbar unter GitHub: Bewährte Sicherheitsmethoden für AWS WAF.

Beispielvorlagen mit Korrekturmaßnahmen

Bewährte Methoden für die Ausführung von Amazon DynamoDB mit Korrekturaktionen

Die Vorlage ist verfügbar unter GitHub: Operational Best Practices for Amazon DynamoDB with Remediation.

Bewährte Methoden für die Ausführung von Amazon S3 mit Korrekturaktionen

Die Vorlage ist verfügbar unter GitHub: Operational Best Practices for Amazon S3 with Remediation.

Weitere Informationen zur Vorlagenstruktur finden Sie unter Vorlagenanatomie im Benutzerhandbuch für AWS CloudFormation .

Erstellen von Vorlagen für benutzerdefinierte Conformance Packs für AWS Config

Ein benutzerdefiniertes Konformitätspaket ist eine einzigartige Sammlung von AWS Config Regeln und Behebungsmaßnahmen, die Sie gemeinsam in einem Konto und einer AWS Region oder unternehmensweit einsetzen können. AWS Organizations

Wenn Sie ein benutzerdefiniertes Konformitätspaket erstellen möchten, folgen Sie den Schritten im Abschnitt Anpassen der Vorlage, um eine YAML-Datei zu erstellen, die die Liste der von AWS Config verwalteten Regeln oder der AWS Config -benutzerdefinierten Regeln enthält, mit denen Sie arbeiten möchten.

Themen

- Terminologie
- Anpassen der Vorlage

Terminologie

AWS Config Verwaltete Regeln sind vordefinierte Regeln, deren Eigentümer ist. AWS Config

AWS Config Benutzerdefinierte Regeln sind Regeln, die Sie von Grund auf neu erstellen.

Es gibt zwei Möglichkeiten, AWS Config benutzerdefinierte Regeln zu erstellen: mit Lambda-Funktionen (AWS Lambda Developer Guide) und mit Guard (Guard GitHub Repository), einer policy-as-code Sprache. AWS Config Benutzerdefinierte Regeln, die mit erstellt wurden, AWS Lambda werden als AWS Config benutzerdefinierte Lambda-Regeln bezeichnet, und AWS Config benutzerdefinierte Regeln, die mit Guard erstellt wurden, werden als AWS Config benutzerdefinierte Richtlinienregeln bezeichnet.

Anpassen der Vorlage

Erstellen einer YAML-Datei

Zum Erstellen einer YAML-Datei öffnen Sie einen Texteditor und speichern Sie die Datei als .yaml.

> **Note**
>
> Ihre Datei wird einen Abschnitt Parameter und einen Abschnitt Ressourcen enthalten.

Parameter

Der `Parameters` Abschnitt in Ihrer YAML-Datei enthält die Regelparameter für den AWS Config Regelsatz, den Sie später in dem `Resources` Abschnitt hinzufügen werden. Erstellen Sie den Abschnitt `Parameters`, indem Sie den folgenden Code-Block kopieren und in Ihre YAML-Datei einfügen, ihn nach Bedarf anpassen und den Schritt für jeden Regelparameter wiederholen.

```
Parameters:
    NameOfRuleParamNameOfRuleParameter:
        Default: Parameter value
        Type: Type
    ...
```

Zum Beispiel:

```
Parameters:
    IamPasswordPolicyParamMinimumPasswordLength:
        Default: '14'
        Type: String
```

> **Note**
>
> Vergewissern Sie sich bei der Auswahl der AWS Config Regeln für die Erstellung Ihres benutzerdefinierten Konformitätspakets, dass Sie die Ressourcen in Ihrem Konto bereitgestellt haben, die anhand der Regeln bewertet werden. AWS Config

1. Die erste Zeile im Parameterabschnitt danach `Parameters:` ist eine verkettete Zeichenfolge aus + Param +. *`NameOfRule`* *`NameOfRuleParameter`*

   a. Ersetzen Sie *`NameOfRule`* durch einen einheitlichen Namen, den Sie für die Regel erstellen. Das könnte zum Beispiel für die Regel sein. IamPasswordPolicyiam-password-policy

   b. Typ `Param`.

   c. Ersetzen Sie *`NameOfRuleParameter`* dann durch den Namen des Regelparameters für Ihre spezifische Regel. Bei AWS Config verwalteten Regeln befindet sich der Name des Regelparameters in der Liste der AWS Config verwalteten Regeln (MinimumPasswordLengthist z. B. der Name eines Regelparameters für die iam-password-

policyRegel). Bei AWS Config -benutzerdefinierten Regeln entspricht der Name des Regelparameters dem Namen, den Sie bei der Erstellung der Regel ausgewählt haben.

2. Wenn Sie eine AWS Config verwaltete Regel verwenden, suchen Sie die entsprechende AWS Config Regel in der Liste der verwalteten Regeln, damit Sie die akzeptierten Werte für `Default` und `Type` für Ihre spezielle Regel kennen. Verwenden Sie für AWS Config -benutzerdefinierte Regeln die Werte, die Sie bei der Erstellung Ihrer Regel ausgewählt haben.

> **Note**
>
> Für jeden Parameter `Type` muss angegeben werden. `Type`kann einer der folgenden Werte sein: „String“, „int“, „double“, „CSV“, „boolean“ und "StringMap“.

-Ressourcen

In Abschnitt `Resources` sind die Regeln aufgeführt, die Ihrem benutzerdefinierten Konformitätspaket hinzugefügt werden. Fügen Sie den folgenden `Resources`-Block direkt unter Ihrem Abschnitt `Parameters` hinzu, passen Sie ihn nach Bedarf an und wiederholen Sie den Schritt für jede Regel. Weitere Informationen zu den Spezifikationen finden Sie unter. AWS::Config::ConfigRule

```
Resources:
     NameOfRule:
        Properties:
            ConfigRuleName: ActualConfigRuleName
            InputParameters:
                NameOfRuleParameter: !Ref NameOfRuleParamNameOfRuleParameter
            Source:
                Owner: Owner
                SourceIdentifier: SOURCE_IDENTIFIER
        Type: AWS::Config::ConfigRule
     ...
```

Zum Beispiel:

```
Resources:
    IamPasswordPolicy:
        Properties:
            ConfigRuleName: iam-password-policy
            InputParameters:
                MinimumPasswordLength: !Ref IamPasswordPolicyParamMinimumPasswordLength
```

```
            Source:
                Owner: AWS
                SourceIdentifier: IAM_PASSWORD_POLICY
        Type: AWS::Config::ConfigRule
```

> **Note**
>
> Stellen Sie bei der Auswahl der AWS Config Regeln für die Erstellung Ihres benutzerdefinierten Conformance Packs sicher, dass Sie über die in Ihrem Konto bereitgestellten Ressourcen verfügen, die anhand der bereitgestellten AWS Config Regeln bewertet werden. Weitere Informationen finden Sie unter Unterstützte Ressourcentypen.

1. Ersetzen Sie *`NameOfRule`* durch den Namen, den Sie im Abschnitt `Parameters` erstellt haben.
2. Bei AWS Config verwalteten Regeln *`ActualConfigRuleName`* ersetzen Sie diese durch den Titel der entsprechenden Regelseite in der Liste der AWS Config verwalteten Regeln. Verwenden Sie für AWS Config benutzerdefinierte Regeln den Namen der Konfigurationsregel, den Sie bei der Erstellung der Regel ausgewählt haben.
3. Ersetzen Sie *`NameOfRuleParameter`* durch den Namen, den Sie im Abschnitt `Parameters` verwendet haben. Kopieren Sie nach dem Doppelpunkt dieselbe verkettete Zeichenfolge mit + + Param `!Ref` *`NameOfRule`* +, die Sie im Abschnitt erstellt haben*`NameOfRuleParameter`*, und fügen Sie sie ein. `Parameters`
4. Ändern Sie *`Owner`* in den entsprechenden Wert.

   > **Note**
   >
   > AWS Config Verwaltete Regeln
   > Für AWS Config verwaltete Regeln lautet der Wert für `OwnerAWS`.
   > AWS Config Benutzerdefinierte Regeln
   > Für AWS Config benutzerdefinierte Regeln, die mit Guard erstellt wurden, lautet der Wert für `OwnerCUSTOM_POLICY`. Für AWS Config benutzerdefinierte Regeln, die mit Lambda erstellt wurden, lautet der Wert für`Owner`. `CUSTOM_LAMBDA`

5. Ändern Sie *`SOURCE_IDENTIFIER`* in den entsprechenden Wert.

> **Note**
>
> AWS Config Verwaltete Regeln
>
> Kopieren Sie bei AWS Config verwalteten Regeln den Bezeichner, indem Sie dem Link in der Regel folgen, die Sie in der Liste der AWS Config verwalteten Regeln ausgewählt haben (die Quell-ID für die access-keys-rotatedRegel lautet beispielsweise ACCESS_KEYS_ROTATED).
>
> AWS Config Benutzerdefinierte Regeln
>
> Für AWS Config benutzerdefinierte Regeln, die mit Lambda erstellt wurden, `SourceIdentifier` ist dies der Amazon-Ressourcenname (ARN) der AWS Lambda Funktion der Regel, z. B. `arn:aws:lambda:us-east-2:123456789012:function:`*`ActualConfigRuleName`* Für AWS Config benutzerdefinierte Regeln, die mit Guard erstellt wurden, ist dieses Feld nicht erforderlich.

Insgesamt sollte Ihr ausgefülltes benutzerdefiniertes Konformitätspaket wie folgt aussehen, das ein Beispiel für die Verwendung dieser AWS Config verwalteten Regeln ist: iam-password-policy, access-keys-rotated, und iam-user-unused-credentials-check.

```
Parameters:
    IamPasswordPolicyParamMinimumPasswordLength:
        Default: '14'
        Type: String
    AccessKeysRotatedParamMaxAccessKeyAge:
        Default: '90'
        Type: String
    IamUserUnusedCredentialsCheckParamMaxCredentialUsageAge:
        Default: '45'
        Type: String
Resources:
    IamPasswordPolicy:
        Properties:
            ConfigRuleName: iam-password-policy
            InputParameters:
                MinimumPasswordLength: !Ref IamPasswordPolicyParamMinimumPasswordLength
            Source:
                Owner: AWS
                SourceIdentifier: IAM_PASSWORD_POLICY
```

```
        Type: AWS::Config::ConfigRule
    AccessKeysRotated:
        Properties:
            ConfigRuleName: access-keys-rotated
            InputParameters:
                maxAccessKeyAge: !Ref AccessKeysRotatedParamMaxAccessKeyAge
            Source:
                Owner: AWS
                SourceIdentifier: ACCESS_KEYS_ROTATED
        Type: AWS::Config::ConfigRule
    IamUserUnusedCredentialsCheck:
        Properties:
            ConfigRuleName: iam-user-unused-credentials-check
            InputParameters:
                maxCredentialUsageAge: !Ref
IamUserUnusedCredentialsCheckParamMaxCredentialUsageAge
            Source:
                Owner: AWS
                SourceIdentifier: IAM_USER_UNUSED_CREDENTIALS_CHECK
        Type: AWS::Config::ConfigRule
```

Bereitstellung von Conformance Packs für AWS Config

Sie können die AWS Config Konsole oder die verwenden AWS CLI , um Ihre Conformance Packs bereitzustellen.

Deploy Conformance Packs (Console)

Auf der Seite Conformance Packs können Sie ein Conformance Pack für ein Konto in einer Region bereitstellen. Sie können das bereitgestellte Conformance Pack auch bearbeiten und löschen.

Sie können ein Conformance Pack mithilfe von AWS Config Beispielvorlagen oder Ihrer eigenen benutzerdefinierten Vorlage bereitstellen. Anweisungen zur Erstellung personalisierter Konformitätspakete finden Sie unter Benutzerdefiniertes Konformitätspaket

1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die AWS Config Konsole zu https://console.aws.amazon.com/config/Hause.
2. Navigieren Sie zur Seite Conformance Packs (Konformitätspakete) und wählen Sie Deploy conformance pack (Conformance Pack bereitstellen) aus.

3. Wählen Sie auf der Seite Specify template (Vorlage angeben) eine Beispielvorlage aus oder verwenden Sie eine vorhandene Vorlage. Weitere Informationen finden Sie unter Konformitätspaket-Beispielvorlagen.

   - Wenn Sie Beispielvorlage verwenden auswählen, können Sie aus der Dropdown-Liste der Beispielvorlagen eine Beispielvorlage auswählen.

     Informationen zum Inhalt der einzelnen Vorlagen finden Sie in den Beispielvorlagen für Conformance Packs.

   - Wenn Sie Template is ready (Vorlage ist bereit) wählen, geben Sie die Vorlagenquelle an. Es ist entweder eine Amazon S3 S3-URI, ein AWS Systems Manager Dokument (SSM-Dokument) oder eine Vorlage, die Sie hochladen.

     Wenn Ihre Vorlage größer als 50 KB ist, laden Sie sie in den S3-Bucket hoch und wählen diesen S3-Bucket-Speicherort aus. Zum Beispiel: s3://*bucketname/prefix*.

     > **Important**
     >
     > Wählen Sie Vorlage ist bereit, wenn Sie Ihre YAML-Datei des Konformitätspakets auf der Grundlage des benutzerdefinierten Konformitätspakets von Grund auf neu erstellt haben.

4. Wählen Sie Weiter aus.
5. Geben Sie auf der Seite „Conformance Pack-Details angeben“ den Namen für Ihr Conformance Pack ein.

   Der Name des Conformance Packs muss eindeutig sein und darf maximal 256 alphanumerische Zeichen enthalten. Der Name darf Bindestriche, jedoch keine Leerzeichen enthalten.

6. Optional: Fügen Sie Parameter hinzu.

   Parameter werden in Ihrer Vorlage definiert und helfen Ihnen, Ihre Ressourcen zu verwalten und zu organisieren.

7. Wählen Sie Weiter aus.
8. Überprüfen Sie alle Informationen auf der Seite Review and deploy (Überprüfen und Bereitstellen).

Sie können die Details zu Vorlage und Conformance Pack durch Auswahl von Edit (Bearbeiten) bearbeiten.

9. Wählen Sie Deploy conformance pack (Conformance Pack bereitstellen) aus.

   AWS Config zeigt das Conformance Pack auf der Conformance Pack-Seite mit dem entsprechenden Status an.

   Wenn die Bereitstellung Ihres Conformance Packs fehlschlägt, überprüfen Sie Ihre Berechtigungen, vergewissern Sie sich, dass Sie die erforderlichen Schritte ausgeführt haben, und versuchen Sie es erneut. Oder Sie können Kontakt aufnehmen. AWS -Support

Informationen zu Deploy conformance pack using sample template with remediations (Conformance Pack unter Verwendung einer Beispielvorlage mit Korrekturmaßnahmen bereitstellen) finden Sie unter A. Voraussetzungen für die Verwendung eines Conformance Packs mit Remediation. Verwenden Sie anschließend das oben beschriebene Verfahren.

Informationen zur Bereitstellung eines Conformance Packs mit einer oder mehreren AWS Config Regeln finden Sie unterB. Voraussetzungen für die Verwendung eines Conformance Packs mit einer oder mehreren benutzerdefinierten Regeln AWS Config.

Deploy Conformance Packs (AWS CLI)

1. Öffnen Sie eine Eingabeaufforderung oder ein Terminal-Fenster.
2. Geben Sie einen der folgenden Befehle ein, um ein Conformance Pack mit dem Namen bereitzustellen. **`MyConformancePack`** Die Vorlagenquelle ist entweder eine Amazon S3 S3-URI, eine Vorlage, die Sie hochladen, oder ein AWS Systems Manager Dokument (SSM-Dokument).

   Amazon-S3-URI

   ```
   aws configservice put-conformance-pack
   --conformance-pack-name MyConformancePack
   --template-s3-uri "s3://amzn-s3-demo-bucket/templateName.yaml"
   --delivery-s3-bucket amzn-s3-demo-bucket
   ```

   YAML-Vorlage aus Ihrem lokalen Verzeichnis

   ```
   aws configservice put-conformance-pack
   --conformance-pack-name MyConformancePack
   ```

```
--template-body template body
```

AWS Systems Manager Dokument (Systems Manager Manager-Dokument)

```
aws configservice put-conformance-pack
--conformance-pack-name MyConformancePack
--template-ssm-document-details
 DocumentName=SSMDocumentName,DocumentVersion=SSMDocumentVersion
--delivery-s3-bucket amzn-s3-demo-bucket
```

3. Drücken Sie die Eingabetaste, um den Befehl auszuführen.

   Die Ausgabe sollte in etwa wie folgt aussehen:

```
{
    "conformancePackArn": "arn:aws:config:us-west-2:AccountID:conformance-pack/
MyConformancePack1/conformance-pack-ID"
}
```

> **Note**
>
> Weitere Informationen zum Erstellen einer YAML-Vorlage für ein Konformitätspaket finden Sie unter Benutzerdefiniertes Konformitätspaket.

Conformance Packs bearbeiten für AWS Config

Sie können die AWS Config Konsole oder die verwenden, AWS CLI um Ihre Conformance Packs zu bearbeiten.

Editing Conformance Packs (Console)

1. Um ein Conformance Pack zu bearbeiten, wählen Sie das Conformance Pack aus der Tabelle aus.
2. Wählen Sie Aktionen und dann Bearbeiten aus.
3. Auf der Seite Edit conformance pack (Conformance Pack bearbeiten) können Sie die Abschnitte für Vorlagendetails, die Beispielvorlage, das Conformance Pack und die Parameter bearbeiten.

Sie können den Namen des Conformance Packs nicht ändern.

4. Wählen Sie Änderungen speichern.

   Das Conformance Pack wird mit den AWS Config Regeln angezeigt.

Editing Conformance Packs (AWS CLI)

Wenn Sie ein Conformance Pack bearbeiten, das Sie zuvor hinzugefügt haben, verwenden Sie denselben `PutConformancePack` Befehl, den Sie bei der Bereitstellung eines Conformance Packs verwenden.

1. Öffnen Sie eine Eingabeaufforderung oder ein Terminal-Fenster.
2. Geben Sie einen der folgenden Befehle ein, um ein Conformance Pack mit dem Namen bereitzustellen. **`MyConformancePack`** Die Vorlagenquelle ist entweder eine Amazon S3 S3-URI, eine Vorlage, die Sie hochladen, oder ein AWS Systems Manager Dokument (SSM-Dokument).

   Amazon-S3-URI

   ```
   aws configservice put-conformance-pack
   --conformance-pack-name MyConformancePack
   --template-s3-uri "s3://amzn-s3-demo-bucket/templateName.yaml"
   --delivery-s3-bucket amzn-s3-demo-bucket
   ```

   YAML-Vorlage aus Ihrem lokalen Verzeichnis

   ```
   aws configservice put-conformance-pack
   --conformance-pack-name MyConformancePack
   --template-body template body
   ```

   AWS Systems Manager Dokument (Systems Manager Manager-Dokument)

   ```
   aws configservice put-conformance-pack
   --conformance-pack-name MyConformancePack
   --template-ssm-document-details
    DocumentName=SSMDocumentName,DocumentVersion=SSMDocumentVersion
   --delivery-s3-bucket amzn-s3-demo-bucket
   ```

3. Drücken Sie die Eingabetaste, um den Befehl auszuführen.

Die Ausgabe sollte in etwa wie folgt aussehen:

```
{
    "conformancePackArn": "arn:aws:config:us-west-2:AccountID:conformance-pack/
MyConformancePack1/conformance-pack-ID"
}
```

> **Note**
>
> Weitere Informationen zum Erstellen einer YAML-Vorlage für ein Konformitätspaket finden Sie unter Benutzerdefiniertes Konformitätspaket.

Löschen von Conformance Packs für AWS Config

Sie können die AWS Config Konsole oder die verwenden, um Conformance AWS CLI Packs zu löschen.

Überlegungen

Empfehlung: Erwägen Sie, den **`AWS::Config::ResourceCompliance`** Ressourcentyp aus der Aufzeichnung auszuschließen, bevor Sie Regeln löschen

Durch das Löschen von Regeln werden Konfigurationselemente (CIs) erstelltAWS::Config::ResourceCompliance, die sich auf Ihre Kosten für den Konfigurationsrekorder auswirken können. Wenn Sie Regeln löschen, die eine große Anzahl von Ressourcentypen auswerten, kann dies zu einem Anstieg der Anzahl der CIs aufgezeichneten Ressourcentypen führen.

Um die damit verbundenen Kosten zu vermeiden, können Sie die Aufzeichnung für den AWS::Config::ResourceCompliance Ressourcentyp deaktivieren, bevor Sie Regeln löschen, und die Aufzeichnung erneut aktivieren, nachdem die Regeln gelöscht wurden.

Da das Löschen von Regeln jedoch ein asynchroner Vorgang ist, kann es eine Stunde oder länger dauern, bis er abgeschlossen ist. Während der ZeitAWS::Config::ResourceCompliance, für die die Aufzeichnung deaktiviert ist, werden Regelauswertungen nicht im Verlauf der zugehörigen Ressource aufgezeichnet.

Um ein Conformance Pack zu löschen

Deleting Conformance Packs (Console)

1. Um ein Conformance Pack zu löschen, wählen Sie das Conformance Pack aus der Tabelle aus.
2. Wählen Sie Actions und dann Delete aus.
3. Bestätigen Sie *conformance pack* im Dialogfeld „Löschen“, ob Sie dieses Conformance Pack dauerhaft löschen möchten.

   > **Important**
   >
   > Sie können diese Aktion nicht rückgängig machen. Wenn Sie ein Conformance Pack löschen, löschen Sie alle AWS Config Regeln und Behebungsmaßnahmen in diesem Conformance Pack.

4. Geben Sie Delete (Löschen) ein und wählen Sie Delete (Löschen) aus.

   Auf der Seite Conformance packs (Conformance Packs) wird der Bereitstellungsstatus Deleting (Wird gelöscht) angezeigt, bis das Conformance Pack vollständig gelöscht ist.

Deleting Conformance Packs (AWS CLI)

Geben Sie den folgenden Befehl ein.

```
aws configservice delete-conformance-pack --conformance-pack-name MyConformancePack1
```

Bei einer erfolgreichen Befehlsausführung gibt es keine weitere Ausgabe.

> **Important**
>
> Sie können diese Aktion nicht rückgängig machen. Wenn Sie ein Conformance Pack löschen, löschen Sie alle AWS Config Regeln und Behebungsmaßnahmen in diesem Conformance Pack.

Details und Compliance-Informationen für Ihre Conformance Packs anzeigen für AWS Config

> **Important**
>
> Für eine genaue Berichterstattung über den Compliance-Status müssen Sie den Ressourcentyp `AWS::Config::ResourceCompliance` aufzeichnen. Weitere Informationen finden Sie unter AWS Ressourcen für die Aufzeichnung.

Sie können die AWS Config Konsole oder die verwenden AWS CLI , um Ihre Conformance Packs einzusehen. Die AWS Config Konsole verfügt über ein einheitliches Dashboard. Das AWS CLI ermöglicht es Ihnen, Befehle für bestimmte Informationen auszuführen.

Viewing Conformance Packs (Console)

Informationen zur Anzeige Ihrer Conformance Packs im AWS Management Console finden Sie unter Conformance Pack Dashboard Pack.

Viewing the Details for your Conformance Packs (AWS CLI)

1. Geben Sie den folgenden Befehl ein.

```
aws configservice describe-conformance-packs
```

ODER

```
aws configservice describe-conformance-packs --conformance-pack-
name="MyConformancePack1"
```

2. Die Ausgabe sollte in etwa wie folgt aussehen:

```
{
    "conformancePackName": "MyConformancePack1",
    "conformancePackId": "conformance-pack-ID",
    "conformancePackArn": "arn:aws:config:us-west-2:AccountID:conformance-
pack/MyConformancePack1/conformance-pack-ID",
    "conformancePackInputParameters": [],
    "lastUpdateRequestedTime": "Thu Jul 18 16:07:05 PDT 2019"
}
```

Viewing the Status for your Conformance Packs (AWS CLI)

1. Geben Sie den folgenden Befehl ein.

```
aws configservice describe-conformance-pack-status --conformance-pack-
name="MyConformancePack1"
```

2. Die Ausgabe sollte in etwa wie folgt aussehen:

```
{
    "stackArn": "arn:aws:cloudformation:us-west-2:AccountID:stack/
awsconfigconforms-MyConformancePack1-conformance-pack-ID/d4301fe0-
a9b1-11e9-994d-025f28dd83ba",
    "conformancePackName": "MyConformancePack1",
    "conformancePackId": "conformance-pack-ID",
    "lastUpdateCompletedTime": "Thu Jul 18 16:15:17 PDT 2019",
    "conformancePackState": "CREATE_COMPLETE",
    "conformancePackArn": "arn:aws:config:us-west-2:AccountID:conformance-
pack/MyConformancePack1/conformance-pack-ID",
    "lastUpdateRequestedTime": "Thu Jul 18 16:14:35 PDT 2019"
}
```

Viewing the Compliance Status for your Conformance Packs (AWS CLI)

1. Geben Sie den folgenden Befehl ein.

```
aws configservice describe-conformance-pack-compliance --conformance-pack-
name="MyConformancePack1"
```

2. Die Ausgabe sollte in etwa wie folgt aussehen:

```
{
    "conformancePackName": "MyConformancePack1",
    "conformancePackRuleComplianceList": [
        {
            "configRuleName": "awsconfigconforms-RuleName1-conformance-pack-ID",
            "complianceType": "NON_COMPLIANT"
        },
        {
            "configRuleName": "awsconfigconforms-RuleName2-conformance-pack-ID",
            "complianceType": "COMPLIANT"
```

```
        }
    ]
}
```

Viewing the Compliance Details for your Conformance Packs (AWS CLI)

1. Geben Sie den folgenden Befehl ein.

```
aws configservice get-conformance-pack-compliance-details --conformance-pack-
name="MyConformancePack1"
```

2. Die Ausgabe sollte in etwa wie folgt aussehen:

```
{
    "conformancePackRuleEvaluationResults": [
        {
            "evaluationResultIdentifier": {
                "orderingTimestamp": "Tue Jul 16 23:07:35 PDT 2019",
                "evaluationResultQualifier": {
                    "resourceId": "resourceID",
                    "configRuleName": "awsconfigconforms-RuleName1-conformance-
pack-ID",
                    "resourceType": "AWS::::Account"
                }
            },
            "configRuleInvokedTime": "Tue Jul 16 23:07:50 PDT 2019",
            "resultRecordedTime": "Tue Jul 16 23:07:51 PDT 2019",
            "complianceType": "NON_COMPLIANT"
        },
        {
            "evaluationResultIdentifier": {
                "orderingTimestamp": "Thu Jun 27 15:16:36 PDT 2019",
                "evaluationResultQualifier": {
                    "resourceId": "resourceID",
                    "configRuleName": "awsconfigconforms-RuleName2-conformance-
pack-ID",
                    "resourceType": "AWS::EC2::SecurityGroup"
                }
            },
           "configRuleInvokedTime": "Thu Jul 11 23:08:06 PDT 2019",
            "resultRecordedTime": "Thu Jul 11 23:08:06 PDT 2019",
            "complianceType": "COMPLIANT"
```

```
        }
    ],
    "conformancePackName": "MyConformancePack1"
}
}
```

Zeitleiste des Compliance-Verlaufs für Conformance Packs anzeigen für AWS Config

AWS Config unterstützt das Speichern von Konformitätsstatusänderungen an Ihren Conformance Packs. Auf diese Weise können Sie den Verlauf der Änderungen am Compliance-Status einsehen. Diese Änderungen am Compliance-Status werden als Zeitleiste dargestellt. In der Zeitleiste werden Änderungen über einen Zeitraum als `ConfigurationItems` erfasst. Sie können diese Funktion auch verwenden, um bestimmte Regeln in einem Conformance Pack zu finden, die nicht konform sind.

Sie können die Aufzeichnung aller Ressourcentypen in AWS Config aktivieren oder deaktivieren. Wenn Sie sich dafür entschieden haben, alle Ressourcentypen aufzuzeichnen, beginnt AWS Config automatisch die Aufzeichnung des Konformitätspakets gemäß den Regeln. AWS Config AWS Config Zeichnet standardmäßig die Konfigurationsänderungen für alle unterstützten Ressourcen auf. Sie können auch nur den spezifischen Ressourcentyp für den Compliance-Verlauf des Konformitätspakets auswählen: `AWS::Config::ConformancePackCompliance`. Für die Aufzeichnung des Ressourcentyps `AWS::Config::ConformancePackCompliance` fallen keine zusätzlichen Kosten an. Weitere Informationen finden Sie unter AWS Ressourcen aufzeichnen.

Ein Konformitätspaket ist konform, wenn alle Regeln darin konform sind. Es ist nicht konform, wenn eine der Regeln nicht konform ist. Der Compliance-Status eines Konformitätspakets lautet nur dann INSUFFICIENT_DATA, wenn alle Regeln innerhalb eines Konformitätspakets aufgrund unzureichender Daten nicht ausgewertet werden können. Wenn einige der Regeln in einem Konformitätspaket zwar konform sind, der Compliance-Status anderer Regeln im selben Konformitätspaket aber INSUFFICIENT_DATA lautet, zeigt das Konformitätspaket den Status als konform an. Die Konformität eines Konformitätspakets wird nicht auf einmal bewertet. Die Bewertung einiger Regeln kann länger dauern als die Bewertung anderer. Die Compliance wird jeweils für Gruppen von Regeln bewertet. Die Bewertung erfolgt schrittweise, bis alle Regeln in einem Konformitätspaket bewertet wurden.

Anzeigen der Compliance-Zeitleiste

Greifen Sie auf die Compliance-Zeitleiste zu, indem Sie auf der zentralen Seite für Konformitätspakete ein bestimmtes Konformitätspaket auswählen.

1. Navigieren Sie zur Seite für das Konformitätspakete.
2. Wählen Sie auf der zentralen Seite für Konformitätspakete ein bestimmtes Konformitätspaket und dann Konformitätspaketzeitplan aus.

> **Note**
>
> Alternativ können Sie die Compliance-Zeitleiste auf der Detailseite des Konformitätspakets verwenden. Wählen Sie ein Konformitätspaket und dann in der Dropdownliste Aktionen die Option Details anzeigen aus. Wählen Sie auf dieser Seite die Option Konformitätspaketzeitplan aus.

Die Zeitleiste zeigt Ihnen den Verlauf der Änderungen des Compliance-Status für ein Konformitätspaket. Sie haben die folgenden Möglichkeiten:

1. Erweitern Sie eine Konformitätsänderung, um den line-by-line Konformitätsstatus jeder Regel innerhalb eines Konformitätspakets anzuzeigen.
2. Wählen Sie in der erweiterten Ansicht eine bestimmte Regel aus, um die Detailseite anzuzeigen.

Abfragen des Compliance-Verlaufs für Conformance Packs für AWS Config

Fragen Sie den Konformitätsverlauf get-resource-config-history mithilfe des Ressourcentyps ab. `AWS::Config::ConformancePackCompliance`

```
aws configservice get-resource-config-history --resource-type
 AWS::Config::ConformancePackCompliance --resource-id conformance-pack-ID
```

Die Ausgabe sollte folgendermaßen oder ähnlich aussehen:

```
{
    "configurationItems": [
```

```
        {
            "version": "1.3",
            "accountId": "Account ID",
            "configurationItemCaptureTime": 1614641951.442,
            "configurationItemStatus": "OK",
            "configurationStateId": "1614641951442",
            "configurationItemMD5Hash": "",
            "arn": "arn:aws:config:us-east-1:Account ID:conformance-
pack/MyConformancePack1/conformance-pack-ID",
            "resourceType": "AWS::Config::ConformancePackCompliance",
            "resourceId": "conformance-pack-ID",
            "resourceName": "MyConformancePack1",
            "awsRegion": "us-east-1",
            "tags": {},
            "relatedEvents": [],
            "relationships": [],
            "configuration": "{\"compliantRuleCount\":1,\"configRuleList\":
[{\"configRuleName\":\"RuleName1-conformance-pack-ID\",\"controls\":[],\"configRuleArn
\":\"arn:aws:config:us-east-1:Account ID:config-rule/aws-service-rule/config-
conforms.amazonaws.com/config-rule-nnnnnn\",\"complianceType\":\"INSUFFICIENT_DATA\"},
{\"configRuleName\":\"RuleName2-conformance-pack-ID\",\"controls\":[],\"configRuleArn
\":\"arn:aws:config:us-east-1:Account ID:config-rule/aws-service-rule/config-
conforms.amazonaws.com/config-rule-mmmmmm\",\"complianceType\":\"COMPLIANT\"},
{\"configRuleName\":\"RuleName3-conformance-pack-ID\",\"controls\":[],\"configRuleArn
\":\"arn:aws:config:us-east-1:Account ID:config-rule/aws-service-rule/config-
conforms.amazonaws.com/config-rule-pppppp\",\"complianceType\":\"INSUFFICIENT_DATA\"}],
\"totalRuleCount\":3,\"nonCompliantRuleCount\":0,\"complianceType\":\"COMPLIANT\"}",
            "supplementaryConfiguration": {}
        },
        {
            "version": "1.3",
            "accountId": "768311917693",
            "configurationItemCaptureTime": 1605551029.515,
            "configurationItemStatus": "ResourceDiscovered",
            "configurationStateId": "1605551029515",
            "configurationItemMD5Hash": "",
            "resourceType": "AWS::Config::ConformancePackCompliance",
            "resourceId": "conformance-pack-ID",
            "resourceName": "MyConformancePack1",
            "awsRegion": "us-east-1",
            "tags": {},
            "relatedEvents": [],
            "relationships": [],
```

```
            "configuration": "{\"compliantRuleCount\":1,\"configRuleList\":
[{\"configRuleName\":\"RuleName1-conformance-pack-ID\",\"controls\":[],\"configRuleArn
\":\"arn:aws:config:us-east-1:Account ID:config-rule/aws-service-rule/config-
conforms.amazonaws.com/config-rule-nnnnnn\",\"complianceType\":\"INSUFFICIENT_DATA\"},
{\"configRuleName\":\"RuleName2-conformance-pack-ID\",\"controls\":[],\"configRuleArn
\":\"arn:aws:config:us-east-1:Account ID:config-rule/aws-service-rule/config-
conforms.amazonaws.com/config-rule-mmmmmm\",\"complianceType\":\"COMPLIANT\"},
{\"configRuleName\":\"RuleName3-conformance-pack-ID\",\"controls\":[],\"configRuleArn
\":\"arn:aws:config:us-east-1:Account ID:config-rule/aws-service-rule/config-
conforms.amazonaws.com/config-rule-pppppp\",\"complianceType\":\"INSUFFICIENT_DATA\"}],
\"totalRuleCount\":3,\"nonCompliantRuleCount\":0,\"complianceType\":\"COMPLIANT\"}",
            "supplementaryConfiguration": {}
        }
    ]
}
```

Weitere Informationen finden Sie unter Unterstützte Ressourcentypen (AWS Config) und GetResourceConfigHistoryin der API-Referenz.

Verwaltung von Conformance Packs AWS Config für alle Konten in Ihrem Unternehmen

Wird verwendet AWS Config , um Konformitätspakete für alle AWS-Konten innerhalb einer Organisation zu verwalten. Sie haben die folgenden Möglichkeiten:

- Zentrales Bereitstellen, Aktualisieren und Löschen von Conformance Packs für alle Mitgliedskonten in einer Organisation in AWS Organizations.
- Stellen Sie einen gemeinsamen Satz von AWS Config Regeln und Behebungsmaßnahmen für alle Konten bereit und geben Sie Konten an, für die keine AWS Config Regeln und Abhilfemaßnahmen erstellt werden sollen.
- Verwenden Sie das Verwaltungskonto AWS Organizations , um die Verwaltung durchzusetzen, indem Sie sicherstellen, dass die zugrunde liegenden AWS Config Regeln und Abhilfemaßnahmen nicht durch die Mitgliedskonten Ihrer Organisation geändert werden können.

Überlegungen

Für Bereitstellungen in verschiedenen Regionen

Der API-Aufruf zur kontenübergreifenden Bereitstellung von Regeln und Konformitätspaketen ist AWS regionsspezifisch. Auf Organisationsebene müssen Sie den Kontext Ihres API-Aufrufs auf eine andere Region ändern, wenn Sie Regeln in anderen Regionen bereitstellen möchten. Wenn Sie beispielsweise eine Regel in USA Ost (Nord-Virginia) bereitstellen möchten, ändern Sie die Region auf USA Ost (Nord-Virginia) und rufen Sie dann `PutOrganizationConfigRule` auf.

Für Konten innerhalb einer Organisation

Wenn ein neues Konto einer Organisation beitritt, wird die Regel oder das Konformitätspaket für dieses Konto bereitgestellt. Wenn ein Konto eine Organisation verlässt, wird die Regel oder das Konformitätspaket entfernt.

Wenn Sie eine Organisationsregel oder ein Konformitätspaket im Konto eines Organisationsadministrators bereitstellen und dann einen delegierten Administrator einrichten und eine Organisationsregel oder ein Konformitätspaket im delegierten Administratorkonto bereitstellen, können Sie die Organisationsregel oder das Konformitätspaket im Konto des Organisationsadministrators nicht vom delegierten Administratorkonto aus sehen. Sie können auch die Organisationsregel oder das Konformitätspaket nicht vom delegierten Administratorkonto des Kontos eines Organisationsadministrators aus sehen. Die DescribeOrganizationConfigRulesund DescribeOrganizationConformancePacks APIs können nur die organisationsbezogenen Ressourcen sehen und mit ihnen interagieren, die von dem Konto aus bereitgestellt wurden, das sie aufruft. APIs

Wiederholungsmechanismus für neue Konten, die einer Organisation hinzugefügt wurden

Wenn kein Recorder verfügbar ist, wird die Bereitstellung vorhandener Organisationsregeln und Konformitätspakete nur 7 Stunden lang wiederholt, nachdem ein Konto zu Ihrer Organisation hinzugefügt wurde. Es wird erwartet, dass Sie innerhalb von 7 Stunden nach dem Hinzufügen eines Kontos zu Ihrer Organisation einen Recorder erstellen, falls noch keiner vorhanden ist.

Konten für die Organisationsverwaltung, delegierte Administratoren und dienstbezogene Rollen

Wenn Sie ein Organisationsverwaltungskonto verwenden und beabsichtigen, einen delegierten Administrator für die organisatorische Bereitstellung zu verwenden, beachten Sie, dass dadurch die serviceverknüpfte Rolle (SLR) AWS Config nicht automatisch erstellt wird. Sie müssen die serviceverknüpfte Rolle (SLR) mithilfe von IAM separat manuell erstellen.

Wenn Sie keine Spiegelreflexkamera für Ihr Verwaltungskonto haben, können Sie von einem delegierten Administratorkonto aus keine Ressourcen für dieses Konto bereitstellen. Sie können weiterhin Conformance Packs für Mitgliedskonten von Verwaltungs- und delegierten

Administratorkonten aus bereitstellen. Weitere Informationen finden Sie unter Verwenden von serviceverknüpften Rollen im AWS Identity and Access Management (IAM -) Benutzerhandbuch.

Bereitstellung

To deploy with the AWS Management Console

Um ein Conformance Pack von der AWS Konsole aus unternehmensweit bereitzustellen, verwenden Sie. AWS Systems Manager Weitere Informationen finden Sie im AWS Systems Manager Benutzerhandbuch unter Bereitstellen von AWS Config Conformance Packs.

To deploy with the AWS API

Informationen zur Integration AWS Config mit AWS Organizations finden Sie unter AWS Config und AWS Organizations im AWS Organizations Benutzerhandbuch. Stellen Sie sicher, dass die AWS Config Aufzeichnung aktiviert ist, bevor Sie die folgenden APIs Methoden verwenden, um die Conformance Pack-Regeln AWS-Konten innerhalb einer Organisation zu verwalten:

- DeleteOrganizationConformancePack, löscht das angegebene Konformitätspaket der Organisation sowie alle Konfigurationsregeln und Behebungsmaßnahmen aus allen Mitgliedskonten in dieser Organisation.
- DescribeOrganizationConformancePacks, gibt eine Liste von Organization Conformance Packs zurück.
- DescribeOrganizationConformancePackStatuses, gibt den Bereitstellungsstatus des Organization Conformance Packs für eine Organisation an.
- GetOrganizationConformancePackDetailedStatus, gibt einen detaillierten Status für jedes Mitgliedskonto innerhalb einer Organisation für ein bestimmtes Organisationskonformitätspaket zurück.
- PutOrganizationConformancePack, stellt Conformance Packs für alle Mitgliedskonten einer Organisation bereit. AWS

Unterstützung von Regionen

Die Bereitstellung von Conformance Packs für alle Mitgliedskonten einer AWS Organisation wird in den folgenden Regionen unterstützt.

Name der Region	Region	Endpunkt	Protocol (Protokoll)
USA Ost (Ohio)	us-east-2	config.us-east-2.amazonaws.com	HTTPS
USA Ost (Nord-Virginia)	us-east-1	config.us-east-1.amazonaws.com	HTTPS
USA West (Nordkalifornien)	us-west-1	config.us-west-1.amazonaws.com	HTTPS
USA West (Oregon)	us-west-2	config.us-west-2.amazonaws.com	HTTPS
Afrika (Kapstadt)	af-south-1	config.af-south-1.amazonaws.com	HTTPS
Asien-Pazifik (Hongkong)	ap-east-1	config.ap-east-1.amazonaws.com	HTTPS
Asien-Pazifik (Hyderabad)	ap-south-2	config.ap-south-2.amazonaws.com	HTTPS
Asien-Pazifik (Jakarta)	ap-southeast-3	config.ap-southeast-3.amazonaws.com	HTTPS

Name der Region	Region	Endpunkt	Protocol (Protokoll)
Asien-Pazifik (Melbourne)	ap-southeast-4	config.ap-southeast-4.amazonaws.com	HTTPS
Asien-Pazifik (Mumbai)	ap-south-1	config.ap-south-1.amazonaws.com	HTTPS
Asien-Pazifik (Osaka)	ap-northeast-3	config.ap-northeast-3.amazonaws.com	HTTPS
Asien-Pazifik (Seoul)	ap-northeast-2	config.ap-northeast-2.amazonaws.com	HTTPS
Asien-Pazifik (Singapur)	ap-southeast-1	config.ap-southeast-1.amazonaws.com	HTTPS
Asien-Pazifik (Sydney)	ap-southeast-2	config.ap-southeast-2.amazonaws.com	HTTPS
Asien-Pazifik (Tokio)	ap-northeast-1	config.ap-northeast-1.amazonaws.com	HTTPS
Kanada (Zentral)	ca-central-1	config.ca-central-1.amazonaws.com	HTTPS

Name der Region	Region	Endpunkt	Protocol (Protokoll)
Kanada West (Calgary)	ca-west-1	config.ca-west-1.amazonaws.com	HTTPS
Europa (Frankfurt)	eu-central-1	config.eu-central-1.amazonaws.com	HTTPS
Europa (Irland)	eu-west-1	config.eu-west-1.amazonaws.com	HTTPS
Europa (London)	eu-west-2	config.eu-west-2.amazonaws.com	HTTPS
Europa (Mailand)	eu-south-1	config.eu-south-1.amazonaws.com	HTTPS
Europa (Paris)	eu-west-3	config.eu-west-3.amazonaws.com	HTTPS
Europa (Spanien)	eu-south-2	config.eu-south-2.amazonaws.com	HTTPS
Europa (Stockholm)	eu-north-1	config.eu-north-1.amazonaws.com	HTTPS
Europa (Zürich)	eu-central-2	config.eu-central-2.amazonaws.com	HTTPS
Israel (Tel Aviv)	il-central-1	config.il-central-1.amazonaws.com	HTTPS

Name der Region	Region	Endpunkt	Protocol (Protokoll)
Naher Osten (Bahrain)	me-south-1	config.me-south-1.amazonaws.com	HTTPS
Naher Osten (VAE)	me-central-1	config.me-central-1.amazonaws.com	HTTPS
Südamerika (São Paulo)	sa-east-1	config.sa-east-1.amazonaws.com	HTTPS
AWS GovCloud (US-Ost)	us-gov-east-1	config.us-gov-east-1.amazonaws.com	HTTPS
AWS GovCloud (US-West)	us-gov-west-1	config.us-gov-west-1.amazonaws.com	HTTPS

Problembehandlung für Conformance Packs für AWS Config

Sehen Sie sich die folgenden Probleme an, um Probleme zu beheben, auf die Sie bei der Verwendung von Conformance Packs stoßen könnten.

Themen

- Status „Fehlgeschlagen“ für ein Conformance Pack
- Hängende Regeln in einem Konformitätspaket

Status „Fehlgeschlagen“ für ein Conformance Pack

Wenn beim Erstellen, Aktualisieren oder Löschen eine Fehlermeldung zu Ihrem Conformance Pack angezeigt wird, können Sie den Status Ihres Conformance Packs überprüfen.

```
aws configservice describe-conformance-pack-status --conformance-pack-name
 MyConformancePack1
```

Die Ausgabe sollte in etwa wie folgt aussehen:

```
"ConformancePackStatusDetails": [
    {
        "ConformancePackName": "ConformancePackName",
        "ConformancePackId": "ConformancePackId",
        "ConformancePackArn": "ConformancePackArn",
        "ConformancePackState": "CREATE_FAILED",
        "StackArn": "CloudFormation stackArn",
        "ConformancePackStatusReason": "Failure Reason",
        "LastUpdateRequestedTime": 1573865201.619,
        "LastUpdateCompletedTime": 1573864244.653
    }
]
```

Suchen Sie ConformancePackStatusReasonnach Informationen über den Fehler.

When the stackArn is present in the response (Wenn der stackArn in der Antwort enthalten ist)

Wenn die Fehlermeldung nicht klar ist oder der Fehler auf einen internen Fehler zurückgeht, wechseln Sie zur AWS CloudFormation -Konsole und gehen folgendermaßen vor:

1. Suchen Sie den stackArn in der Ausgabe.
2. Wählen Sie die Registerkarte Ereignisse des CloudFormation Stacks und suchen Sie nach fehlgeschlagenen Ereignissen.

   Der Statusgrund gibt an, warum ein Fehler im Zusammenhang mit dem Conformance Pack aufgetreten ist.

When the stackArn is not present in the response (Wenn der stackArn in der Antwort enthalten ist)

Wenn während des Erstellens eines Conformance Packs ein Fehler angezeigt wird, der stackArn jedoch nicht in der Statusantwort vorhanden ist, ist möglicherweise die Stack-Erstellung

fehlgeschlagen, sodass CloudFormation ein Rollback ausgeführt und den Stack gelöscht hat. Gehen Sie zur CloudFormation Konsole und suchen Sie nach Stacks, die sich im Status Gelöscht befinden. Der fehlerhafte Stack ist dort möglicherweise verfügbar. Der CloudFormation -Stack enthält den Namen des Conformance Packs. Wenn Sie den fehlgeschlagenen Stack finden, wählen Sie die Registerkarte Ereignisse des CloudFormation Stacks und suchen Sie nach fehlgeschlagenen Ereignissen.

Wenn keiner dieser Schritte funktioniert hat und die Ursache des Fehlers ein interner Servicefehler ist, versuchen Sie den Vorgang erneut oder wenden Sie sich an das AWS -Support Center.

Hängende Regeln in einem Konformitätspaket

Die Bereitstellung eines Conformance Packs beinhaltet die Erstellung eines zugrunde liegenden AWS CloudFormation Stacks im Hintergrund, um die Regeln in der Conformance Pack-Vorlage bereitzustellen. Bei diesen Regeln handelt es sich um dienstbezogene Regeln, die außerhalb des Conformance Packs nicht aktualisiert oder gelöscht werden können.

Wenn Sie Änderungen am zugrunde liegenden CloudFormation Stack vornehmen, führt dies zu einer Situation, in der das Conformance Pack und seine Regeln nicht mehr verwaltet werden können. Diese Regeln, die nicht verwaltet werden können, sind unbedeutende Regeln.

Drift zwischen dem CloudFormation Stack und dem Conformance Pack

Sie können die Regelnamen in einer Conformance Pack-Vorlage direkt von der CloudFormation Konsole aus aktualisieren. Wenn Sie die Vorlage direkt von der CloudFormation Konsole aus aktualisieren, wird dadurch das bereitgestellte Conformance Pack nicht aktualisiert.

Diese Abweichung führt zu einer verhängnisvollen Regel. Wenn Sie versuchen, die Regel aus dem Conformance Pack zu löschen, erhalten Sie eine Fehlermeldung, die der folgenden ähnelt:

```
"An AWS service owns ServiceLinkedConfigRule. You do not have permissions to
 take action on this rule. (Service: AmazonConfig; Status Code: 400; Error Code:
 AccessDeniedException; Request ID: my-request-ID; Proxy: null)".
```

Wenn Sie versuchen, das Conformance Pack zu löschen, kann die fehlerhafte Regel nicht gelöscht werden und Sie erhalten eine Fehlermeldung, die der folgenden ähnelt:

```
"User: arn:aws:sts::111122223333:assumed-role/AWSServiceRoleForConfigConforms/
AwsConfigConformsWorkflow is not authorized to perform: config:DeleteConfigRule on
 resource: my-dangling-rule
```

Gehen Sie wie folgt vor, um dieses Problem zu beheben:

1. Löschen Sie den Stack. Weitere Informationen finden Sie im CloudFormation Benutzerhandbuch unter Löschen eines Stacks auf der AWS CloudFormation Konsole.
2. Löschen Sie das Conformance Pack mithilfe der AWS Config Konsole oder mithilfe der DeleteConformancePackAPI. Wenn es sich um ein organisatorisches Konformitätspaket handelt und Sie das Management- oder delegierte Administratorkonto verwenden, verwenden Sie die API. DeleteOrganizationConformancePack
3. Wenden Sie sich mit dem Amazon-Ressourcennamen (ARN) der geltenden Regeln im Konformitätspaket an das AWS -Support Center, um Ihr Konto zu bereinigen.

Beachten Sie die folgenden bewährten Methoden, um dieses Problem zu vermeiden:

- Nehmen Sie niemals direkte Aktualisierungen am CloudFormation Stack eines Conformance Packs vor.
- Versuchen Sie niemals, Änderungen vorzunehmen, die zu Abweichungen zwischen dem Conformance Pack und dem zugrunde liegenden CloudFormation Stack führen.
- Die Service-Linked Role (SLR) für Conformance Packs kann nicht geändert werden. Stellen Sie sicher, dass die Ressourcen, die Sie aktualisieren, Teil der Berechtigungsrichtlinie für den SLR sind.

Der CloudFormation Stack für ein Conformance Pack wurde gelöscht

Sofern es nicht zu Abweichungen zwischen dem CloudFormation Stack und dem Conformance Pack kommt, ist es nicht empfehlenswert, Regeln in einem Conformance Pack oder seinem CloudFormation Stack direkt von der Konsole aus zu löschen. CloudFormation

Um dieses Problem zu beheben, wenden Sie sich mit dem Amazon-Ressourcennamen (ARN) der Dangling-Regeln im Konformitätspaket an das AWS -Support Center, damit Sie Ihr Konto bereinigen können.

Beachten Sie die folgenden bewährten Methoden, um dieses Problem zu vermeiden:

- Löschen Sie niemals den zugrunde liegenden CloudFormation Stack für ein Conformance Pack.
- Löschen Sie Conformance Packs mithilfe der DeleteConformancePackAPI. Wenn es sich um ein unternehmensweites Konformitätspaket handelt und Sie das Verwaltungskonto oder das delegierte Administratorkonto verwenden, verwenden Sie die API. DeleteOrganizationConformancePack

Behebung nicht konformer Ressourcen mit AWS Config

AWS Config ermöglicht es Ihnen, nicht konforme Ressourcen zu korrigieren, die von bewertet werden. AWS-Config-Regeln AWS Config wendet die Problembehebung mithilfe AWS Systems Manager von Automatisierungsdokumenten an. In diesen Dokumenten werden die Aktionen definiert, die an AWS Ressourcen durchgeführt werden müssen, die nicht den Vorschriften entsprechen und von bewertet wurden. AWS-Config-Regeln Sie können SSM-Dokumente mithilfe von AWS Management Console oder mithilfe von verknüpfen. APIs

AWS Config bietet eine Reihe von verwalteten Automatisierungsdokumenten mit Abhilfemaßnahmen. Sie können auch benutzerdefinierte Automatisierungsdokumente erstellen und diesen AWS Config Regeln zuordnen.

Themen

- Unterstützung von Regionen
- Einrichtung der manuellen Problembehebung für AWS Config
- Automatische Problembehebung einrichten für AWS Config
- Löschen von Behebungsmaßnahmen für AWS Config

Unterstützung von Regionen

Derzeit werden Behebungsmaßnahmen für AWS Config Regeln in den folgenden Regionen unterstützt:

Name der Region	Region	Endpunkt	Protocol (Protokoll)
USA Ost (Ohio)	us-east-2	config.us-east-2.amazonaws.com	HTTPS
USA Ost (Nord-Virginia)	us-east-1	config.us-east-1.amazonaws.com	HTTPS

Name der Region	Region	Endpunkt	Protocol (Protokoll)	
USA West (Nordkalifornien)	us-west-1	config.us-west-1.amazonaws.com	HTTPS	
USA West (Oregon)	us-west-2	config.us-west-2.amazonaws.com	HTTPS	
Afrika (Kapstadt)	af-south-1	config.af-south-1.amazonaws.com	HTTPS	
Asien-Pazifik (Hongkong)	ap-east-1	config.ap-east-1.amazonaws.com	HTTPS	
Asien-Pazifik (Hyderabad)	ap-south-2	config.ap-south-2.amazonaws.com	HTTPS	
Asien-Pazifik (Jakarta)	ap-southeast-3	config.ap-southeast-3.amazonaws.com	HTTPS	
Asien-Pazifik (Melbourne)	ap-southeast-4	config.ap-southeast-4.amazonaws.com	HTTPS	

Name der Region	Region	Endpunkt	Protocol (Protokoll)
Asien-Pazifik (Mumbai)	ap-south-1	config.ap-south-1.amazonaws.com	HTTPS
Asien-Pazifik (Osaka)	ap-northeast-3	config.ap-northeast-3.amazonaws.com	HTTPS
Asien-Pazifik (Seoul)	ap-northeast-2	config.ap-northeast-2.amazonaws.com	HTTPS
Asien-Pazifik (Singapur)	ap-southeast-1	config.ap-southeast-1.amazonaws.com	HTTPS
Asien-Pazifik (Sydney)	ap-southeast-2	config.ap-southeast-2.amazonaws.com	HTTPS
Asien-Pazifik (Tokio)	ap-northeast-1	config.ap-northeast-1.amazonaws.com	HTTPS
Kanada (Zentral)	ca-central-1	config.ca-central-1.amazonaws.com	HTTPS
Kanada West (Calgary)	ca-west-1	config.ca-west-1.amazonaws.com	HTTPS
Europa (Frankfurt)	eu-central-1	config.eu-central-1.amazonaws.com	HTTPS

Name der Region	Region	Endpunkt	Protocol (Protokoll)
Europa (Irland)	eu-west-1	config.eu-west-1.amazonaws.com	HTTPS
Europa (London)	eu-west-2	config.eu-west-2.amazonaws.com	HTTPS
Europa (Mailand)	eu-south-1	config.eu-south-1.amazonaws.com	HTTPS
Europa (Paris)	eu-west-3	config.eu-west-3.amazonaws.com	HTTPS
Europa (Spanien)	eu-south-2	config.eu-south-2.amazonaws.com	HTTPS
Europa (Stockholm)	eu-north-1	config.eu-north-1.amazonaws.com	HTTPS
Europa (Zürich)	eu-central-2	config.eu-central-2.amazonaws.com	HTTPS
Israel (Tel Aviv)	il-central-1	config.il-central-1.amazonaws.com	HTTPS
Naher Osten (Bahrain)	me-south-1	config.me-south-1.amazonaws.com	HTTPS
Naher Osten (VAE)	me-central-1	config.me-central-1.amazonaws.com	HTTPS

Name der Region	Region	Endpunkt	Protocol (Protokoll)
Südamerika (São Paulo)	sa-east-1	config.sa-east-1.amazonaws.com	HTTPS
AWS GovCloud (US-Ost)	us-gov-east-1	config.us-gov-east-1.amazonaws.com	HTTPS
AWS GovCloud (US-West)	us-gov-west-1	config.us-gov-west-1.amazonaws.com	HTTPS

Einrichtung der manuellen Problembehebung für AWS Config

Um die Behebung auf nicht konforme Ressourcen anzuwenden, können Sie entweder die Behebungsaktion, die Sie zuordnen möchten, aus einer vorab ausgefüllten Liste auswählen oder mithilfe von SSM-Dokumenten Ihre eigenen benutzerdefinierten Behebungsmaßnahmen erstellen. AWS Config bietet eine empfohlene Liste von Behebungsmaßnahmen in der. AWS Management Console

Setting Up Manual Remediation (Console)

In der können Sie entweder wählen AWS Management Console, ob Sie nicht konforme Ressourcen manuell korrigieren möchten, indem Sie Behebungsaktionen Regeln zuordnen. AWS Config Bei allen Korrekturmaßnahmen können Sie entweder eine manuelle oder eine automatische Korrektur auswählen.

1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die AWS Config Konsole zu Hause. https://console.aws.amazon.com/config/
2. Wählen Sie links Regeln und anschließend auf der Seite Regeln die Option Regel hinzufügen aus, um der Liste neue Regeln hinzuzufügen.

Wählen Sie bei bestehenden Regeln die nicht konforme Regel aus der Regelliste aus und wählen Sie die Dropdown-Liste Aktionen aus.

3. Wählen Sie in der Dropdown-Liste Aktionen die Option Behebung verwalten aus. Wählen Sie „Manuelle Korrektur“ und dann die entsprechende Korrekturmaßnahme aus der Liste der Empfehlungen aus.

> **Note**
>
> Sie können nur Behebungen für Regeln verwalten, die nicht mit dem Service verknüpft sind AWS Config . Weitere Informationen finden Sie unter Serviceverknüpfte AWS -Regeln.

Abhängig von der ausgewählten Korrekturmaßnahme werden Ihnen entweder spezifische oder keine Parameter angezeigt.

4. (Optional): Wenn Sie die Ressourcen-ID von nicht konformen Ressourcen an die Korrekturmaßnahme übergeben möchten, wählen Sie Resource ID parameter (Ressourcen-ID-Parameter). Wenn diese Option aktiviert ist, wird dieser Parameter zur Laufzeit durch die ID der Ressource ersetzt, für die die Korrekturmaßnahme ausgeführt werden soll.

   Jeder Parameter hat entweder einen statischen oder dynamischen Wert. Wenn Sie keinen bestimmten Ressourcen-ID-Parameter aus der Dropdown-Liste auswählen, können Sie Werte für die jeweiligen Schlüssel eingeben. Wenn Sie einen Ressourcen-ID-Parameter aus der Dropdown-Liste auswählen, können Sie Werte für alle anderen Schlüssel mit Ausnahme des ausgewählten Ressourcen-ID-Parameters eingeben.

5. Wählen Sie Speichern. Die Seite Rules (Regeln) wird angezeigt.

Zur Behebung fehlgeschlagener Behebungsmaßnahmen können Sie den AWS Befehl Befehlszeilenschnittstelle ausführen, `describe-remediation-execution-status` um eine detaillierte Ansicht der Korrekturausführung für eine Reihe von Ressourcen zu erhalten. Die Details umfassen Status, Zeitstempel für die Schritte der Korrekturausführung und alle Fehlermeldungen für die fehlgeschlagenen Schritte.

Setting Up Manual Remediation (API)

Verwenden Sie den folgenden AWS Config API-Vorgang, um die manuelle Behebung einzurichten:

- PutRemediationConfigurations, fügt die Wartungskonfiguration hinzu oder aktualisiert sie mit einer bestimmten AWS Config Regel mit dem ausgewählten Ziel oder der ausgewählten Aktion.
- StartRemediationExecution, führt bei Bedarf eine Standardisierung für die angegebenen AWS Config Regeln anhand der letzten bekannten Behebungskonfiguration durch.
- DescribeRemediationExecutionStatus, bietet einen detaillierten Überblick über die Ausführung einer Problembehebung für eine Reihe von Ressourcen, einschließlich Status, Zeitstempel, wann Schritte für die Ausführung der Problembehebung ausgeführt werden, und aller Fehlermeldungen für fehlgeschlagene Schritte.
- DescribeRemediationConfigurations, gibt die Details einer oder mehrerer Behebungskonfigurationen zurück.

Automatische Problembehebung einrichten für AWS Config

Um die Problembehebung auf nicht richtlinientreue Ressourcen anzuwenden, können Sie entweder die Behebungsaktion, die Sie zuordnen möchten, aus einer vorab ausgefüllten Liste auswählen oder mithilfe von SSM-Dokumenten Ihre eigenen benutzerdefinierten Behebungsmaßnahmen erstellen. AWS Config bietet eine Liste der Behebungsmaßnahmen in der. AWS Management Console

Setting Up Auto Remediation (Console)

In der können Sie entweder festlegen AWS Management Console, dass nicht konforme Ressourcen automatisch behoben werden, indem Sie Behebungsaktionen mit Regeln verknüpfen. AWS Config Bei allen Korrekturmaßnahmen können Sie entweder eine manuelle oder eine automatische Korrektur auswählen.

1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die AWS Config Konsole zu Hause. https://console.aws.amazon.com/config/
2. Wählen Sie links Regeln und anschließend auf der Seite Regeln die Option Add Rule (Regel hinzufügen), um der Liste neue Regeln hinzuzufügen.

   Wählen Sie bei bestehenden Regeln die nicht konforme Regel aus der Regelliste aus und wählen Sie die Dropdown-Liste Aktionen aus.
3. Wählen Sie in der Dropdown-Liste Aktionen die Option Behebung verwalten aus. Wählen Sie „Automatische Behebung“ und wählen Sie dann die entsprechende Behebungsaktion aus der Liste aus.

> **Note**
>
> Sie können nur Behebungen für Regeln verwalten, die nicht mit dem Service verknüpft sind. AWS Config Weitere Informationen finden Sie unter Serviceverknüpfte AWS -Regeln.

Abhängig von der ausgewählten Korrekturmaßnahme werden Ihnen entweder spezifische oder keine Parameter angezeigt.

4. Wählen Sie Auto remediation (Automatische Korrektur) aus, um nicht konforme Ressourcen automatisch zu korrigieren.

   Wenn eine Ressource nach der auto Korrektur immer noch nicht konform ist, können Sie die Regel so einrichten, dass die auto Korrektur erneut versucht wird. Geben Sie die gewünschten Wiederholversuche und Sekunden ein.

   > **Note**
   >
   > Bei der mehrfachen Ausführung eines Korrekturskripts fallen Kosten an. Wiederholungsversuche finden nur statt, wenn die Korrektur fehlschlägt. Für sie gilt der angegebene Zeitraum, z. B. 5 Wiederholungen in 300 Sekunden. Weitere Informationen finden Sie unter Systems Manager Automation — Preise.

5. (Optional): Wenn Sie die Ressourcen-ID von nicht konformen Ressourcen an die Korrekturmaßnahme übergeben möchten, wählen Sie Resource ID parameter (Ressourcen-ID-Parameter). Wenn diese Option aktiviert ist, wird dieser Parameter zur Laufzeit durch die ID der Ressource ersetzt, für die die Korrekturmaßnahme ausgeführt werden soll.

   Jeder Parameter hat entweder einen statischen oder dynamischen Wert. Wenn Sie keinen bestimmten Ressourcen-ID-Parameter aus der Dropdown-Liste auswählen, können Sie Werte für die jeweiligen Schlüssel eingeben. Wenn Sie einen Ressourcen-ID-Parameter aus der Dropdown-Liste auswählen, können Sie Werte für alle anderen Schlüssel mit Ausnahme des ausgewählten Ressourcen-ID-Parameters eingeben.

6. Wählen Sie Speichern. Die Seite Rules (Regeln) wird angezeigt.

Informationen zur Behebung fehlgeschlagener Behebungsmaßnahmen

Zur Behebung fehlgeschlagener Behebungsmaßnahmen können Sie den AWS Befehl Befehlszeilenschnittstelle ausführen`describe-remediation-execution-status`, um eine detaillierte Ansicht der Korrekturausführung für eine Reihe von Ressourcen zu erhalten. Die Details umfassen Status, Zeitstempel für die Schritte der Korrekturausführung und alle Fehlermeldungen für die fehlgeschlagenen Schritte.

Die automatische Problembehebung kann auch für konforme Ressourcen initiiert werden

Wenn Sie die auto Korrektur für eine bestimmte AWS Config Regel mithilfe der PutRemediationConfigurationsAPI oder der AWS Config Konsole aktivieren, wird der Behebungsprozess für alle nicht konformen Ressourcen für diese bestimmte Regel eingeleitet. Der auto Korrekturprozess basiert auf dem Snapshot der Compliance-Daten, der regelmäßig erfasst wird. Jede nicht konforme Ressource, die zwischen dem Snapshot-Zeitplan aktualisiert wird, wird weiterhin auf der Grundlage des letzten bekannten Compliance-Daten-Snapshots behoben.

Das bedeutet, dass in einigen Fällen die auto Korrektur sogar für konforme Ressourcen initiiert werden kann, da der Bootstrap-Prozessor eine Datenbank verwendet, die auf dem letzten bekannten Compliance-Daten-Snapshot veraltete Bewertungsergebnisse aufweisen kann.

Setting Up Auto Remediation (API)

Verwenden Sie den folgenden AWS Config API-Vorgang, um die auto Behebung einzurichten:

- PutRemediationExceptions, fügt eine neue Ausnahme hinzu oder aktualisiert eine bestehende Ausnahme für eine bestimmte Ressource mit einer bestimmten AWS Config Regel.
- DescribeRemediationExceptions, gibt die Details einer oder mehrerer Behebungsausnahmen zurück.

Löschen von Behebungsmaßnahmen für AWS Config

Sie können die AWS Config Konsole oder die verwenden AWS CLI , um Behebungsmaßnahmen zu löschen.

Deleting remediation actions (Console)

1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die AWS Config Konsole zu https://console.aws.amazon.com/config/Hause.

2. Klicken Sie links auf die Option Regeln, wählen Sie auf der Seite Regeln die Regel aus der Regelliste aus und klicken Sie anschließend auf Details anzeigen.
3. Gehen Sie auf der `name of the rule` Seite zum Abschnitt Abhilfemaßnahmen. Erweitern Sie den Abschnitt, um weitere Details anzuzeigen.
4. Wählen Sie im Abschnitt Korrekturmaßnahme die Option Löschen aus und bestätigen Sie die Löschaktion.

> **Note**
>
> Wenn die Korrekturmaßnahme gerade ausgeführt wird, wird sie nicht gelöscht. Wenn Sie eine Korrekturmaßnahme gelöscht haben, können Sie sie nicht mehr abrufen. Mit dem Löschen einer Korrekturmaßnahme wird nicht die zugehörige Regel gelöscht.

Wenn eine Korrekturmaßnahme gelöscht wird, ist Ressourcen-ID-Parameter leer und zeigt „N/A“ an. Auf der Seite Regeln wird in der Spalte für die Korrekturmaßnahme für die zugehörige Regel Nicht festgelegt angezeigt.

Deleting remediation actions (API)

Verwenden Sie den folgenden AWS Config API-Vorgang, um die auto Behebung einzurichten:

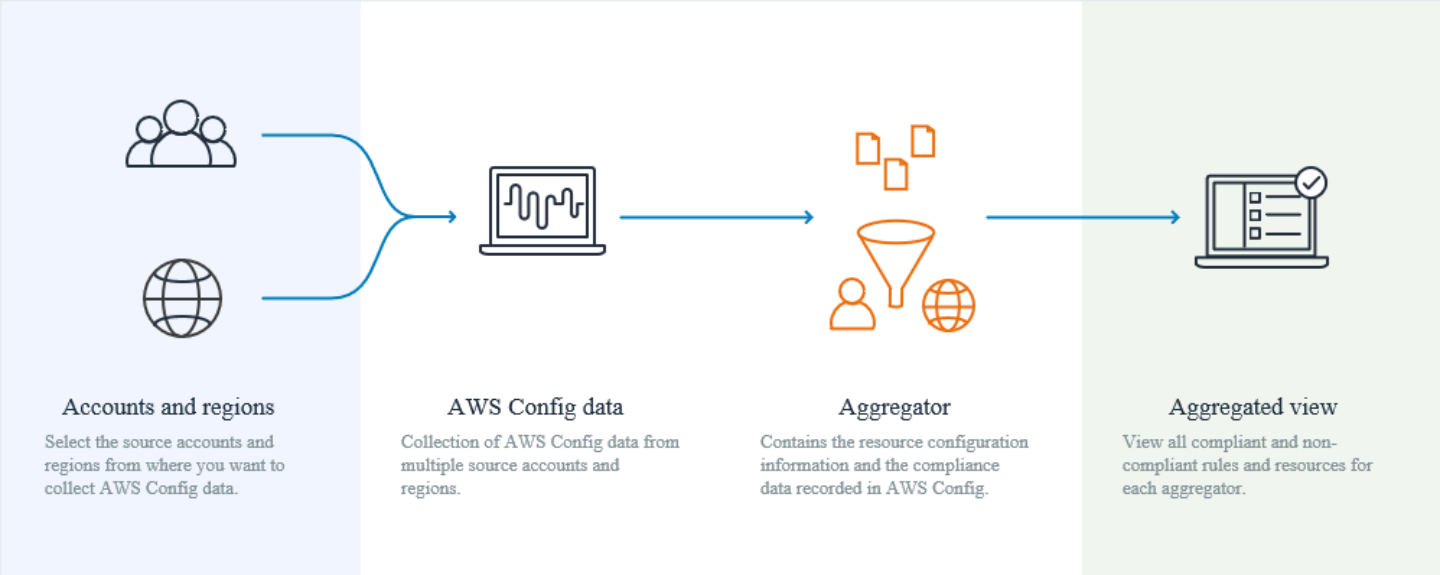
- DeleteRemediationConfiguration, löscht die Behebungskonfiguration.
- DeleteRemediationExceptions, löscht eine oder mehrere in den Ressourcenschlüsseln erwähnte Behebungsausnahmen.

Datenaggregation mit mehreren Konten und mehreren Regionen für AWS Config

Ein Aggregator ist ein AWS Config Ressourcentyp, der AWS Config Konfigurations- und Compliance-Daten aus folgenden Quellen sammelt:

- Mehrere Konten und mehrere AWS Regionen.
- Ein Konto und mehrere AWS Regionen.
- Eine Organisation in AWS Organizations und alle Konten in dieser Organisation, die AWS Config aktiviert wurden.

Verwenden Sie einen Aggregator, um die in AWS Config erfassten Ressourcenkonfigurations- und Compliance-Daten anzuzeigen. Die folgende Abbildung zeigt, wie ein Aggregator AWS Config Daten aus mehreren Konten und Regionen sammelt.



Anwendungsfälle

- Compliance-Überwachung: Sie können Compliance-Daten aggregieren, um den allgemeinen Compliance-Status Ihres Unternehmens oder über Konten und Regionen hinweg zu beurteilen.
- Nachverfolgung von Änderungen: Sie können Änderungen an Ressourcen im Laufe der Zeit in Ihrem Unternehmen oder über Konten und Regionen hinweg verfolgen.

- Ressourcenbeziehungen: Sie können Ressourcenabhängigkeiten und -beziehungen innerhalb Ihrer Organisation oder zwischen Konten und Regionen analysieren.

> **Note**
>
> Aggregatoren bieten eine schreibgeschützte Ansicht der Quellkonten und Regionen, zu deren Anzeige der Aggregator berechtigt ist, indem sie Daten aus den Quellkonten in das Aggregatorkonto replizieren. Aggregatoren bieten keinen mutierenden Zugriff auf ein Quellkonto oder eine Quellregion. Dies bedeutet beispielsweise, dass Sie Regeln nicht über einen Aggregator bereitstellen oder Snapshot-Dateien nicht über einen Aggregator an ein Quellkonto oder eine Quellregion übertragen können.
> Für die Verwendung von Aggregatoren fallen keine zusätzlichen Kosten an.

Terminologie

Ein Quellkonto ist das Konto, AWS-Konto von dem aus Sie AWS Config Ressourcenkonfigurations- und Compliance-Daten aggregieren möchten. Ein Quellkonto kann ein einzelnes Konto oder eine Organisation in AWS Organizations sein. Sie können Quellkonten einzeln bereitstellen oder sie über abrufen AWS Organizations.

Eine Quellregion ist die AWS Region, aus der Sie AWS Config Konfigurations- und Konformitätsdaten aggregieren möchten.

Ein Aggregatorkonto ist ein Konto, in dem Sie einen Aggregator erstellen.

Autorisierung bezieht sich auf die Berechtigungen, die Sie einem Aggregatorkonto und einer Region zur Erfassung Ihrer AWS Config Konfigurations- und Compliance-Daten gewähren. Die Autorisierung ist nicht erforderlich, wenn Sie Quellkonten aggregieren, die Teil von AWS Organizations sind.

Ein mit einem Dienst verbundener Aggregator ist mit einem bestimmten verknüpft. AWS-Service Die im Geltungsbereich enthaltenen Konfigurations- und Compliance-Daten werden vom verknüpften Dienst festgelegt.

Unterstützung von Regionen

Derzeit wird die Datenaggregation mit mehreren Konten und mehreren Regionen in den folgenden Regionen unterstützt:

Name der Region	Region	Endpunkt	Protocol (Protokoll)
USA Ost (Ohio)	us-east-2	config.us-east-2.amazonaws.com	HTTPS
USA Ost (Nord-Virginia)	us-east-1	config.us-east-1.amazonaws.com	HTTPS
USA West (Nordkalifornien)	us-west-1	config.us-west-1.amazonaws.com	HTTPS
USA West (Oregon)	us-west-2	config.us-west-2.amazonaws.com	HTTPS
Afrika (Kapstadt)	af-south-1	config.af-south-1.amazonaws.com	HTTPS
Asien-Pazifik (Hongkong)	ap-east-1	config.ap-east-1.amazonaws.com	HTTPS
Asien-Pazifik (Hyderabad)	ap-south-2	config.ap-south-2.amazonaws.com	HTTPS
Asien-Pazifik (Jakarta)	ap-southeast-3	config.ap-southeast-3.amazonaws.com	HTTPS

Name der Region	Region	Endpunkt	Protocol (Protokoll)
Asien-Pazifik (Malaysia)	ap-southeast-5	config.ap-southeast-5.amazonaws.com	HTTPS
Asien-Pazifik (Melbourne)	ap-southeast-4	config.ap-southeast-4.amazonaws.com	HTTPS
Asien-Pazifik (Mumbai)	ap-south-1	config.ap-south-1.amazonaws.com	HTTPS
Asien-Pazifik (Osaka)	ap-northeast-3	config.ap-northeast-3.amazonaws.com	HTTPS
Asien-Pazifik (Seoul)	ap-northeast-2	config.ap-northeast-2.amazonaws.com	HTTPS
Asien-Pazifik (Singapur)	ap-southeast-1	config.ap-southeast-1.amazonaws.com	HTTPS
Asien-Pazifik (Sydney)	ap-southeast-2	config.ap-southeast-2.amazonaws.com	HTTPS
Asien-Pazifik (Taipeh)	ap-east-2	config.ap-east-2.amazonaws.com	HTTPS

Name der Region	Region	Endpunkt	Protocol (Protokoll)
Asien-Pazifik (Thailand)	ap-southeast-7	config.ap-southeast-7.amazonaws.com	HTTPS
Asien-Pazifik (Tokio)	ap-northeast-1	config.ap-northeast-1.amazonaws.com	HTTPS
Kanada (Zentral)	ca-central-1	config.ca-central-1.amazonaws.com	HTTPS
Kanada West (Calgary)	ca-west-1	config.ca-west-1.amazonaws.com	HTTPS
Europa (Frankfurt)	eu-central-1	config.eu-central-1.amazonaws.com	HTTPS
Europa (Irland)	eu-west-1	config.eu-west-1.amazonaws.com	HTTPS
Europa (London)	eu-west-2	config.eu-west-2.amazonaws.com	HTTPS
Europa (Mailand)	eu-south-1	config.eu-south-1.amazonaws.com	HTTPS
Europa (Paris)	eu-west-3	config.eu-west-3.amazonaws.com	HTTPS
Europa (Spanien)	eu-south-2	config.eu-south-2.amazonaws.com	HTTPS

Name der Region	Region	Endpunkt	Protocol (Protokoll)
Europa (Stockholm)	eu-north-1	config.eu-north-1.amazonaws.com	HTTPS
Europa (Zürich)	eu-central-2	config.eu-central-2.amazonaws.com	HTTPS
Israel (Tel Aviv)	il-central-1	config.il-central-1.amazonaws.com	HTTPS
Mexiko (Zentral)	mx-central-1	config.mx-central-1.amazonaws.com	HTTPS
Naher Osten (Bahrain)	me-south-1	config.me-south-1.amazonaws.com	HTTPS
Naher Osten (VAE)	me-central-1	config.me-central-1.amazonaws.com	HTTPS
Südamerika (São Paulo)	sa-east-1	config.sa-east-1.amazonaws.com	HTTPS
AWS GovCloud (US-Ost)	us-gov-east-1	config.us-gov-east-1.amazonaws.com	HTTPS
AWS GovCloud (US-West)	us-gov-west-1	config.us-gov-west-1.amazonaws.com	HTTPS

Konformitäts- und Inventardaten im Aggregator-Dashboard anzeigen für AWS Config

Das Dashboard auf der Aggregatoren-Seite zeigt die Konfigurationsdaten Ihrer aggregierten AWS Ressourcen an. Es bietet einen Überblick über Ihre Regeln, Konformitätspakete und deren Compliance-Status.

Das Dashboard zeigt die Gesamtzahl der Ressourcen an. AWS Die Ressourcentypen und Quellkonten werden nach der höchsten Ressourcenanzahl sortiert. Außerdem sehen Sie darin die Anzahl Ihrer konformen und nicht konformen Regeln und Konformitätspakete. Die nicht konformen Regeln sind in absteigender Reihenfolge nach der Anzahl ihrer nicht konformen Ressourcen geordnet. Die nicht konformen Konformitätspakete und Quellkonten sind in absteigender Reihenfolge nach der Anzahl ihrer nicht konformen Regeln geordnet.

Nach der Einrichtung beginnt es AWS Config, Daten aus den angegebenen Quellkonten in einem Aggregator zu aggregieren. Es kann einige Minuten dauern, bis der Compliance-Status der Regeln angezeigt wird.

Verwenden des Aggregator-Dashboards

1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die AWS Config Konsole zu Hausehttps://console.aws.amazon.com/config/.
2. Navigieren Sie zur Seite Aggregatoren. Sie können dort Folgendes anzeigen:
   - Ihre Regeln und deren Compliance-Status
   - Ihre Konformitätspakete und deren Compliance-Status.
   - Ihre AWS Ressourcen und deren Konfigurationsdaten.
3. Wählen Sie einen Aggregator aus dem Dashboard aus. Filtern Sie Ihre Aggregatoren nach dem Namen des Aggregators. Sie können folgende Widgets anzeigen lassen:
   - Ressourcenbestand

     Hier sehen Sie die zehn häufigsten Ressourcentypen des ausgewählten Aggregators in absteigender Reihenfolge nach ihrer Ressourcenanzahl. Klicken Sie auf die Gesamtzahl der Ressourcen für den ausgewählten Aggregator, die in Klammern hinter dem Ressourcenbestand angezeigt wird, um zur Seite der aggregierten Ressourcen zu gelangen, auf der Sie alle Ressourcen für einen Aggregator anzeigen können. Alternativ können Sie

einen Ressourcentyp im Widget auswählen, um zur Seite der aggregierten Ressourcen zu gelangen. Sie werden dort nach dem angegebenen Ressourcentyp gefiltert angezeigt.

- Konten nach Anzahl der Ressourcen

  Hier sehen Sie die fünf häufigsten Konten des ausgewählten Aggregators in absteigender Reihenfolge nach ihrer Ressourcenanzahl. Wählen Sie im Widget ein Konto aus, um zur Seite Ressourcen zu gelangen. Sie werden dort nach dem angegebenen Konto gefiltert angezeigt.

- Nicht konforme Regeln

  Sehen Sie sich die fünf am häufigsten nicht konformen Regeln des ausgewählten Aggregators an, in absteigender Reihenfolge nach der Anzahl der nicht konformen Ressourcen. Wählen Sie eine Regel im Widget, um zur Detailseite für die angegebene Regel zu gelangen. Wählen Sie Alle nicht konformen Regeln anzeigen, um zur Seite mit den aggregierten Regeln zu gelangen, auf der Sie alle Regeln für einen Aggregator anzeigen können.

- Konten nach nicht konformen Regeln

  Hier sehen Sie die fünf häufigsten Konten des ausgewählten Aggregators in absteigender Reihenfolge nach der Anzahl ihrer nicht konformen Regeln. Wählen Sie im Widget ein Konto aus, um zur Seite der aggregierten Regeln zu gelangen. Dort können Sie alle Regeln für einen Aggregator gefiltert nach dem angegebenen Konto anzeigen lassen.

- Konten nach nicht konformen Konformitätspaketen

  Hier sehen Sie die fünf häufigsten Konten des ausgewählten Aggregators in absteigender Reihenfolge nach der Anzahl ihrer nicht konformen Konformitätspakete. Wählen Sie im Widget ein Konto aus, um zur Seite des aggregierten Konformitätspakets zu gelangen. Dort können Sie alle Konformitätspakete für einen Aggregator gefiltert nach dem angegebenen Konto anzeigen lassen.

4. Klicken Sie im linken Navigationsbereich auf eine der folgenden Optionen im Dropdown-Menü:

   - Compliance-Dashboard

     Hier finden Sie automatisierte Compliance-Dashboards, indem Sie die Widgets nutzen, die eine Zusammenfassung zur Ressourcen-Compliance in Ihrem Aggregator zeigen. Sie sehen Daten wie die 10 häufigsten Ressourcentypen nach nicht konformen Ressourcen und die 10 wichtigsten Konformitätspakete auf Kontoebene nach nicht konformen Regeln. Weitere Informationen zu diesen Grafiken und Diagrammen finden Sie unter Compliance-Dashboards.

   - Konformitätspakete

Sehen Sie sich alle Konformitätspakete an, die in Ihrem Aggregator erstellt und mit den verschiedenen Paketen verknüpft wurden. AWS-Konten Auf der Seite Konformitätspaket wird eine Tabelle mit dem Namen, der Region, der Konto-ID und dem Compliance-Status jedes Konformitätspakets angezeigt. Auf dieser Seite können Sie ein Konformitätspaket auswählen und Details einblenden, um weitere Informationen zu seinen Regeln und Ressourcen sowie deren Compliance-Status zu erhalten.

- Regeln

  Hier sehen Sie alle Regeln, die erstellt und mit den verschiedenen AWS -Konten in Ihrem Aggregator verknüpft wurden. Auf der Seite Regeln wird eine Tabelle mit dem Namen, dem Compliance-Status, der Region und dem Konto jeder Regel angezeigt. Auf dieser Seite können Sie eine Regel auswählen und auf Details einblenden klicken, um unter anderem Angaben zu ihrem Aggregator, ihrer Region, ihrer Konto-ID und ihren Ressourcen im Geltungsbereich anzeigen zu lassen.

- Inventory-Dashboard

  Hier finden Sie automatisierte Inventory-Dashboards, indem Sie die Widgets nutzen, die eine Zusammenfassung zu den Ressourcenkonfigurationsdaten in Ihrem Aggregator zeigen. Sie sehen Daten wie die 10 häufigsten Ressourcentypen und die 10 wichtigsten Konten, jeweils nach Ressourcenanzahl geordnet. Informationen zu diesen Grafiken und Diagrammen finden Sie in den Inventory-Dashboards.

- Ressourcen

  Hier sehen Sie alle Ressourcen, die aufgezeichnet und mit den verschiedenen AWS -Konten in Ihrem Aggregator verknüpft wurden. Wählen Sie auf der Seite Ressource eine Ressource aus und klicken Sie auf Details einblenden, um ihre Details, die mit ihr verknüpften Regeln und ihre aktuelle Ressourcenkonfiguration anzeigen zu lassen. Sie können auch andere Informationen über die Ressource anzeigen lassen, z. B. ihren Aggregator, ihre Region, ihre Konto-ID, ihren Ressourcennamen, ihren Ressourcentyp und ihre Ressourcen-ID.

- Autorisierungen

  Hier können Sie alle Konten anzeigen und verwalten, die derzeit autorisiert sind oder deren Autorisierung noch aussteht. Wählen Sie auf der Seite Autorisierungen die Option Autorisierung hinzufügen, um Zugriff auf ein anderes Konto zu gewähren. Wählen Sie Autorisierung löschen, um den Zugriff für eine Konto-ID zu widerrufen.

> **Note**
>
> Fehlersuche
>
> Möglicherweise wird in der aggregierten Ansicht die Meldung Datenerfassung aus allen Quellkonten und Regionen ist unvollständig angezeigt, und zwar aus den folgenden Gründen:
>
> - Die Übertragung von nicht konformen AWS Config Regeln und Konfigurationsdaten von AWS Ressourcen ist im Gange.
> - AWS Config kann keine Regeln finden, die dem Filter entsprechen, den Sie angewendet haben. Wählen Sie das entsprechende Konto bzw. die Region aus und versuchen Sie es erneut.
>
> Möglicherweise wird in der aggregierten Ansicht die folgende Meldung angezeigt: Die Datenerfassung in Ihrer Organisation ist unvollständig. Sie können die nachstehenden Daten nur 24 Stunden lang anzeigen. Dies kann aus einem der folgenden Gründe geschehen:
>
> - AWS Config kann aufgrund einer ungültigen IAM-Rolle nicht auf Ihre Organisationsdetails zugreifen. Falls die IAM-Rolle länger als 24 Stunden ungültig bleibt, löscht AWS Config die Daten für die gesamte Organisation.
> - AWS Config Der Dienstzugriff ist in Ihrer Organisation deaktiviert.

Compliance-Dashboard

Hier finden Sie automatisierte Compliance-Dashboards, indem Sie Widgets nutzen, die eine Zusammenfassung zur Ressourcen-Compliance in Ihrem Aggregator zeigen. In diesem Dashboard werden nur Regeln mit Compliance-Ergebnissen angezeigt.

> **Note**
>
> Einschränkungen
>
> Die Informationen im Compliance-Dashboard werden durch die Funktion „Erweiterte Abfragen“ von AWS Config bereitgestellt. Diese Funktion unterstützt weder verschachtelte Strukturen noch das Entpacken verschachtelter Arrays. Das bedeutet, dass das Compliance-Dashboard die allgemeine Konformität einer Ressource anzeigt und nicht den Konformitätsstatus für jede einzelne Regel, die über eine Ressource berichtet.

Wenn Sie beispielsweise das Konfigurationselement (CI) für den Ressourcentyp überprüfen`AWS::Config::ResourceCompliance`, zeigt das Dashboard die Konformitätsergebnisse für alle Regeln an, die über diese Ressource berichten. Wenn es 10 Regeln gibt, die über die Ressource berichten, 9 davon sind COMPLIANT und nur 1 ist NON_COMPLIANT, ist die gesamte Konformität dieser Ressource NON_COMPLIANT.

Zusammenfassung der Compliance nach Ressourcen

Zeigt ein Kreisdiagramm an, in dem die Anzahl der konformen Ressourcen mit den nicht konformen Ressourcen aus dem ausgewählten Aggregator verglichen wird. Zeigen Sie mit der Maus auf das Diagramm, um die genaue Anzahl und den Prozentsatz der konformen und nicht konformen Ressourcen zu sehen.

Die angezeigten Daten hängen von den Einstellungen des Konfigurations-Recorders für jedes Konto im ausgewählten Aggregator sowie von den Regionen ab, in denen der ausgewählte Aggregator für die Erfassung von Daten konfiguriert ist.

Die 10 wichtigsten Ressourcentypen nach Ressourcen, die nicht den Vorschriften entsprechen

Zeigt ein horizontales Balkendiagramm an, in dem bis zu 10 Ressourcentypen aus dem ausgewählten Aggregator in absteigender Reihenfolge nach der Anzahl der nicht konformen Ressourcen verglichen werden. Zeigen Sie mit der Maus auf das Diagramm, um die genaue Anzahl der nicht konformen Ressourcen für jeden Ressourcentyp zu sehen.

Die angezeigten Daten hängen von den Einstellungen des Konfigurations-Recorders für jedes Konto im ausgewählten Aggregator sowie von den Regionen ab, in denen der ausgewählte Aggregator für die Erfassung von Daten konfiguriert ist.

Die 10 häufigsten Konten nach Ressourcen, die nicht den Vorschriften entsprechen

Die 10 wichtigsten Konten nach Ressourcen, die die Anforderungen nicht erfüllen, zeigt ein horizontales Balkendiagramm, in dem bis zu 10 Konten aus dem ausgewählten Aggregator in absteigender Reihenfolge nach der Anzahl der nicht konformen Ressourcen verglichen werden. Zeigen Sie mit der Maus auf das Diagramm, um die genaue Anzahl der nicht konformen Ressourcen für jedes Konto zu sehen.

Die angezeigten Daten hängen von den Einstellungen des Konfigurations-Recorders für jedes Konto im ausgewählten Aggregator sowie von den Regionen ab, in denen der ausgewählte Aggregator für die Erfassung von Daten konfiguriert ist.

Die 10 Regionen mit den meisten nicht konformen Ressourcen

Zeigt ein horizontales Balkendiagramm an, in dem bis zu 10 Regionen verglichen werden, in denen der ausgewählte Aggregator Daten in absteigender Reihenfolge nach der Anzahl der nicht konformen Ressourcen sammelt. Zeigen Sie mit der Maus auf das Diagramm, um die genaue Anzahl der nicht konformen Ressourcen für jede Region zu sehen.

Die angezeigten Daten hängen von den Einstellungen des Konfigurations-Recorders für jedes Konto im ausgewählten Aggregator ab.

Die 10 häufigsten Konformitätspakete auf Kontoebene nach nicht konformen Regeln

Zeigt ein horizontales Balkendiagramm an, in dem bis zu 10 Konformitätspakete auf Kontoebene des ausgewählten Aggregators in absteigender Reihenfolge nach der Anzahl der nicht konformen Regeln verglichen werden. Zeigen Sie mit der Maus auf das Diagramm, um den Prozentsatz der konformen und nicht konformen Regeln für jedes Konformitätspaket auf Kontoebene zu sehen.

Die angezeigten Daten hängen von den Einstellungen des Konfigurations-Recorders für jedes Konto im ausgewählten Aggregator sowie von den Regionen ab, in denen der ausgewählte Aggregator für die Erfassung von Daten konfiguriert ist.

Die 10 wichtigsten Konformitätspakete auf Unternehmensebene nach den Regeln, die nicht den Vorschriften entsprechen

Zeigt ein horizontales Balkendiagramm an, in dem bis zu 10 Konformitätspakete auf Organisationsebene aus dem ausgewählten Aggregator in absteigender Reihenfolge nach der Anzahl der nicht konformen Regeln verglichen werden. Zeigen Sie mit der Maus auf das Diagramm, um den Prozentsatz der konformen und nicht konformen Regeln in den einzelnen Konformitätspaketen auf Organisationsebene zu sehen.

Die angezeigten Daten hängen von den Einstellungen des Konfigurations-Recorders für jedes Konto im ausgewählten Aggregator sowie von den Regionen ab, in denen der ausgewählte Aggregator für die Erfassung von Daten konfiguriert ist.

Die zehn Konten mit den meisten Regelverstößen in den Konformitätspaketen

Die 10 häufigsten Konten nach nicht konformen Regeln in allen Conformance Packs zeigt ein horizontales Balkendiagramm, in dem bis zu 10 Konten aus dem ausgewählten Aggregator in absteigender Reihenfolge nach der Anzahl der nicht konformen Regeln in all Ihren Conformance Packs verglichen werden. Zeigen Sie mit der Maus auf das Diagramm, um die genaue Anzahl der nicht konformen Regeln in jedem Konto zu sehen.

Die angezeigten Daten hängen von den Einstellungen des Konfigurations-Recorders für jedes Konto im ausgewählten Aggregator sowie von den Regionen ab, in denen der ausgewählte Aggregator für die Erfassung von Daten konfiguriert ist.

Inventory-Dashboard

Hier finden Sie automatisierte Inventory-Dashboards, indem Sie Widgets nutzen, die eine Zusammenfassung zu den Ressourcenkonfigurationsdaten in Ihrem Aggregator zeigen.

Die 10 häufigsten Ressourcentypen nach Anzahl der Ressourcen

Hier sehen Sie ein horizontales Balkendiagramm, das bis zu 10 Ressourcentypen aus dem ausgewählten Aggregator miteinander vergleicht, die in absteigender Reihenfolge nach der Anzahl der Ressourcen geordnet sind. Bewegen Sie den Mauszeiger über das Diagramm, um die genaue Anzahl der Ressourcen für jeden Ressourcentyp zu sehen.

Die angezeigten Daten hängen von den Einstellungen des Konfigurations-Recorders für jedes Konto im ausgewählten Aggregator sowie von den Regionen ab, in denen der ausgewählte Aggregator für die Erfassung von Daten konfiguriert ist.

Anzahl der Ressourcen nach Region

Hier sehen Sie ein horizontales Balkendiagramm, das bis zu 10 Regionen, in denen der ausgewählte Aggregator Daten erfasst, miteinander vergleicht. Sie sind in absteigender Reihenfolge nach der Anzahl der Ressourcen geordnet. Bewegen Sie den Mauszeiger über das Diagramm, um die genaue Anzahl der Ressourcen für jede Region zu sehen.

Die angezeigten Daten hängen von den Einstellungen des Konfigurations-Recorders für jedes Konto im ausgewählten Aggregator ab.

Die 10 häufigsten Konten nach Anzahl der Ressourcen

Hier sehen Sie ein horizontales Balkendiagramm, das bis zu 10 Konten aus dem ausgewählten Aggregator miteinander vergleicht, die in absteigender Reihenfolge nach der Anzahl der Ressourcen geordnet sind. Bewegen Sie den Mauszeiger über das Diagramm, um die genaue Anzahl der Ressourcen für jeden Ressourcentyp zu sehen.

Die angezeigten Daten hängen von den Einstellungen des Konfigurations-Recorders für jedes Konto im ausgewählten Aggregator sowie von den Regionen ab, in denen der ausgewählte Aggregator für die Erfassung von Daten konfiguriert ist.

Anzahl der Ressourcen nach Amazon EC2 Service-Ressourcentypen

Zeigt ein horizontales Balkendiagramm an, in dem EC2 Amazon-Ressourcentypen aus dem ausgewählten Aggregator in absteigender Reihenfolge nach Ressourcenanzahl verglichen werden. Bewegen Sie den Mauszeiger über das Diagramm, um die genaue Anzahl der Ressourcen für jeden EC2 Amazon-Ressourcentyp zu sehen.

Die angezeigten Daten hängen von den Einstellungen des Konfigurations-Recorders für jedes Konto im ausgewählten Aggregator sowie von den Regionen ab, in denen der ausgewählte Aggregator für die Erfassung von Daten konfiguriert ist. Um dieses Diagramm verwenden zu können, müssen Sie den Rekorder so konfigurieren, dass er EC2 Amazon-Ressourcentypen aufzeichnet. Weitere Informationen finden Sie unter Welche AWS Config Ressourceneinträge auswählen.

Die 10 am häufigsten verwendeten EC2 Instance-Typen

Zeigt ein horizontales Balkendiagramm an, in dem bis zu 10 EC2 Amazon-Instance-Typen aus dem ausgewählten Aggregator in absteigender Reihenfolge nach Nutzung verglichen werden. Bewegen Sie den Mauszeiger über das Diagramm, um die Nutzung für jeden EC2 Instance-Typ zu sehen.

Die angezeigten Daten hängen von den Einstellungen des Konfigurations-Recorders für jedes Konto im ausgewählten Aggregator sowie von den Regionen ab, in denen der ausgewählte Aggregator für die Erfassung von Daten konfiguriert ist. Um dieses Diagramm verwenden zu können, müssen Sie den Rekorder so konfigurieren, dass er den EC2 Instanz-Ressourcentyp aufzeichnet. Weitere Informationen finden Sie unter AWS Ressourcen neu kodieren.

EBS-Volume-Anzahl nach Volume-Typ und -Größe

Hier sehen Sie ein vertikales Balkendiagramm, das EBS-Volumes aus dem ausgewählten Aggregator nach ihrer Ressourcenanzahl geordnet miteinander vergleicht. Bewegen Sie den Mauszeiger über das Diagramm, um die Aufschlüsselung nach Anzahl und Größe für jeden Typ von EBS-Volume zu sehen.

Die angezeigten Daten hängen von den Einstellungen des Konfigurations-Recorders für jedes Konto im ausgewählten Aggregator sowie von den Regionen ab, in denen der ausgewählte Aggregator für die Erfassung von Daten konfiguriert ist. Um dieses Diagramm verwenden zu können, müssen Sie den Rekorder so konfigurieren, dass er den Ressourcentyp des EC2 Volumes aufzeichnet. Weitere Informationen finden Sie unter Welche AWS Config Ressourceneinträge auswählen.

Anzahl der ausgeführten und der gestoppten EC2 Instances nach Typ

Zeigt ein horizontales Balkendiagramm an, das EC2 Instance-Typen des ausgewählten Aggregators, die ausgeführt werden, mit EC2 Instances vergleicht, die nach Instance-Typ gestoppt wurden. Zeigen Sie mit der Maus auf das Diagramm, um die genaue Anzahl der gestoppten und laufenden EC2 Instances für jeden Typ zu sehen.

Die angezeigten Daten hängen von den Einstellungen des Konfigurations-Recorders für jedes Konto im ausgewählten Aggregator sowie von den Regionen ab, in denen der ausgewählte Aggregator für die Erfassung von Daten konfiguriert ist. Um dieses Diagramm verwenden zu können, müssen Sie den Rekorder so konfigurieren, dass er den Ressourcentyp der EC2 Instanz aufzeichnet. Weitere Informationen finden Sie unter AWS Ressourcen neu kodieren.

Aggregatoren erstellen für AWS Config

Sie können die AWS Config Konsole oder die verwenden AWS CLI , um Ihre Aggregatoren zu erstellen. Dort können AWS Config Sie „Individuelles Konto hinzufügen“ IDs oder „Meine Organisation hinzufügen“ auswählen, von wo aus Sie Daten aggregieren möchten. Für die AWS CLI gibt es zwei verschiedene Verfahren.

Creating Aggregators (Console)

Auf der Aggregator-Seite können Sie einen Aggregator erstellen, indem Sie das Quellkonto IDs oder die Organisation und die Regionen angeben, aus denen Sie Daten aggregieren möchten.

1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die AWS Config Konsole zu Hausehttps://console.aws.amazon.com/config/.
2. Rufen Sie die Seite Aggregatoren auf und wählen Sie Aggregator hinzufügen aus.
3. Mit Allow data replication (Datenreplikation zulassen) erteilen Sie AWS Config die Berechtigung, Daten aus den Quellkonten in ein Aggregatorkonto zu replizieren.

   Wählen Sie Zulassen AWS Config , um Daten von Quellkonten in ein Aggregatorkonto zu replizieren. Sie müssen dieses Kontrollkästchen aktivieren, um mit dem Hinzufügen eines Aggregators fortfahren zu können.
4. Geben Sie unter Aggregator name (Aggregatorname) den Namen für den Aggregator ein.

   Ein Aggregatorname muss eindeutig sein und darf maximal 64 alphanumerische Zeichen enthalten. Der Name darf Bindestriche und Unterstriche aufweisen.

5. Wählen Sie für Quellkonten auswählen entweder Individuelles Konto hinzufügen IDs oder Meine Organisation hinzufügen, von der aus Sie Daten aggregieren möchten.

> **Note**
>
> Wenn Sie die Option Einzelkonto hinzufügen verwenden, IDs um Quellkonten auszuwählen, ist eine Autorisierung erforderlich.

- Wenn Sie Einzelkonto hinzufügen wählen IDs, können Sie ein individuelles Konto IDs für ein Aggregatorkonto hinzufügen.
  1. Wählen Sie Quellkonten hinzufügen aus, um ein Konto IDs hinzuzufügen.
  2. Wählen Sie Hinzufügen AWS-Konto IDs, um manuell kommagetrennte Dateien AWS-Konto IDs hinzuzufügen. Sollen Daten vom aktuellen Konto aggregiert werden, geben Sie die Konto-ID des Kontos ein.

     ODER

     Wählen Sie Datei hochladen, um eine kommagetrennte Datei (.txt oder .csv) hochzuladen. AWS-Konto IDs
  3. Wählen Sie Add source accounts (Quellkonten hinzufügen) aus, um Ihre Auswahl zu bestätigen.
- Bei Auswahl von Add my organization (Meine Organisation hinzufügen) können Sie alle Konten in Ihrer Organisation einem Aggregatorkonto hinzufügen.

> **Note**
>
> Sie müssen beim Verwaltungskonto angemeldet oder registrierter delegierter Administrator sein. Außerdem müssen alle Funktionen in Ihrer Organisation aktiviert sein. Wenn es sich bei dem Anrufer um ein Verwaltungskonto handelt, AWS Config ruft er die `EnableAwsServiceAccess` API auf, um die Integration zwischen und zu ermöglichen. AWS Config AWS Organizations Wenn der Anrufer ein registrierter delegierter Administrator ist, AWS Config ruft er die `ListDelegatedAdministrators` API auf, um zu überprüfen, ob der Anrufer ein gültiger delegierter Administrator ist.
> Stellen Sie sicher, dass das Verwaltungskonto den delegierten Administrator für den AWS Config Dienstprinzipalnamen (config.amazonaws.com) registriert,

bevor der delegierte Administrator einen Aggregator erstellt. Informationen zum Registrieren eines delegierten Administrators finden Sie unter Registrierung eines delegierten Administrators für AWS Config.

Sie müssen eine IAM-Rolle zuweisen, um für Ihre Organisation nur Leserechte aufrufen zu können. AWS Config APIs

1. Klicken Sie auf Wählen Sie eine Rolle aus Ihrem Konto aus, um eine vorhandene IAM-Rolle auszuwählen.

   > **Note**
   >
   > Fügen Sie in der IAM-Konsole die verwaltete Richtlinie `AWSConfigRoleForOrganizations` an Ihre IAM-Rolle an. Wenn Sie diese Richtlinie anhängen, können Sie AWS Config , und aufrufen. AWS Organizations `DescribeOrganization` `ListAWSServiceAccessForOrganization` `ListAccounts` APIs Standardmäßig wird `config.amazonaws.com` automatisch als vertrauenswürdige Entität angegeben.

2. Wählen Sie Rolle erstellen aus und geben Sie den IAM-Rollennamen ein, um die IAM-Rolle zu erstellen.

6. Wählen Sie unter Regions (Regionen) die Regionen aus, für die Daten aggregiert werden sollen.

   - Wählen Sie eine Region, mehrere Regionen oder alle AWS-Regionen aus.
   - Wählen Sie future einbeziehen AWS-Regionen, um Daten aus allen future Daten zu aggregieren AWS-Regionen , für die Datenaggregation mit mehreren Konten und mehreren Regionen aktiviert ist.

7. Wählen Sie Speichern. AWS Config zeigt den Aggregator an.

Creating Aggregators using Individual Accounts (AWS CLI)

1. Öffnen Sie eine Eingabeaufforderung oder ein Terminal-Fenster.
2. Geben Sie den folgenden Befehl ein, um einen Aggregator mit dem Namen **`MyAggregator`** zu erstellen.

```
aws configservice put-configuration-aggregator --configuration-aggregator-name
 MyAggregator --account-aggregation-sources "[{\"AccountIds\": [\"AccountID1\",
\"AccountID2\",\"AccountID3\"],\"AllAwsRegions\": true}]"
```

Tätigen Sie für `account-aggregation-sources` eine der folgenden Eingaben.

- Eine durch Kommas getrennte Liste, AWS-Konto IDs für die Sie Daten aggregieren möchten. Setzen Sie das Konto IDs in eckige Klammern und achten Sie darauf, keine Anführungszeichen zu verwenden (z. B.`"[{\"AccountIds\": [\"AccountID1\", \"AccountID2\",\"AccountID3\"],\"AllAwsRegions\": true}]"`).
- Sie können auch eine durch Kommas getrennte AWS-Konto IDs JSON-Datei hochladen. Laden Sie die Datei mit der folgenden Syntax hoch: `--account-aggregation-sources MyFilePath/MyFile.json`

  Die JSON-Datei muss das folgende Format aufweisen:

```
[
    {
        "AccountIds": [
            "AccountID1",
            "AccountID2",
            "AccountID3"
        ],
        "AllAwsRegions": true
    }
]
```

3. Drücken Sie die Eingabetaste, um den Befehl auszuführen.

   Die Ausgabe sollte folgendermaßen oder ähnlich aussehen:

```
{
    "ConfigurationAggregator": {
        "ConfigurationAggregatorArn": "arn:aws:config:Region:AccountID:config-
aggregator/config-aggregator-floqpus3",
        "CreationTime": 1517942461.442,
        "ConfigurationAggregatorName": "MyAggregator",
        "AccountAggregationSources": [
            {
```

```
                "AllAwsRegions": true,
                "AccountIds": [
                    "AccountID1",
                    "AccountID2",
                    "AccountID3"
                ]
            }
        ],
        "LastUpdatedTime": 1517942461.442
    }
}
```

Creating Aggregators using AWS Organizations (AWS CLI)

Bevor Sie damit beginnen, müssen Sie beim Verwaltungskonto angemeldet oder registrierter delegierter Administrator sein. Außerdem müssen alle Funktionen in Ihrer Organisation aktiviert sein.

> **Note**
>
> Stellen Sie sicher, dass das Verwaltungskonto einen delegierten Administrator mit den beiden folgenden AWS Config Dienstprinzipalnamen (`config.amazonaws.comundconfig-multiaccountsetup.amazonaws.com`) registriert, bevor der delegierte Administrator einen Aggregator erstellt. Informationen zum Registrieren eines delegierten Administrators finden Sie unter Registrierung eines delegierten Administrators für AWS Config.

1. Öffnen Sie eine Eingabeaufforderung oder ein Terminal-Fenster.
2. Wenn Sie keine IAM-Rolle für Ihren AWS Config Aggregator erstellt haben, geben Sie den folgenden Befehl ein:

```
aws iam create-role --role-name OrgConfigRole --assume-role-policy-document
 "{\"Version\":\"2012-10-17\",\"Statement\":[{\"Sid\":\"\",\"Effect\":\"Allow\",
\"Principal\":{\"Service\":\"config.amazonaws.com\"},\"Action\":\"sts:AssumeRole
\"}]}" --description "Role for organizational AWS Config aggregator"
```

> **Note**
>
> Kopieren Sie den Amazon-Ressourcennamen (ARN) aus dieser IAM-Rolle, um ihn bei der Erstellung Ihres AWS Config Aggregators zu verwenden. Sie finden den ARN im Antwortobjekt.

3. Wenn Sie Ihrer IAM-Rolle keine Richtlinie angehängt haben, fügen Sie die AWSConfigRoleForOrganizationsverwaltete Richtlinie hinzu oder geben Sie den folgenden Befehl ein:

```
aws iam create-policy --policy-name OrgConfigPolicy --policy-document
 '{"Version":"2012-10-17","Statement":[{"Effect":"Allow","Action":
["organizations:ListAccounts","organizations:DescribeOrganization","organizations:ListAW
```

4. Geben Sie den folgenden Befehl ein, um einen Aggregator mit dem Namen **`MyAggregator`** zu erstellen.

```
aws configservice put-configuration-aggregator --configuration-aggregator-name
 MyAggregator --organization-aggregation-source "{\"RoleArn\": \"Complete-Arn\",
\"AllAwsRegions\": true}"
```

5. Drücken Sie die Eingabetaste, um den Befehl auszuführen.

   Die Ausgabe sollte folgendermaßen oder ähnlich aussehen:

```
{
    "ConfigurationAggregator": {
        "ConfigurationAggregatorArn": "arn:aws:config:Region:AccountID:config-
aggregator/config-aggregator-floqpus3",
        "CreationTime": 1517942461.442,
        "ConfigurationAggregatorName": "MyAggregator",
        "OrganizationAggregationSource": {
                "AllAwsRegions": true,
                "RoleArn": "arn:aws:iam::account-of-role-to-assume:role/name-of-
role"
         },
        "LastUpdatedTime": 1517942461.442
    }
}
```

Registrierung eines delegierten Administrators für AWS Config

Delegierte Administratoren sind Konten innerhalb einer bestimmten AWS Organisation, denen zusätzliche Administratorrechte für einen bestimmten AWS Dienst gewährt werden. Weitere Informationen finden Sie im AWS Organizations Benutzerhandbuch unter Delegierter Administrator. Sie müssen den verwenden AWS CLI , um einen delegierten Administrator zu registrieren.

Registrierung eines delegierten Administrators

1. Melden Sie sich mit den Anmeldeinformationen für das Verwaltungskonto an.
2. Öffnen Sie eine Eingabeaufforderung oder ein Terminal-Fenster.
3. Geben Sie den folgenden Befehl ein, um als delegierter Administrator für Ihre Organisation den Servicezugriff zu aktivieren und AWS Config Regeln und Konformitätspakete unternehmensweit bereitzustellen und zu verwalten:

```
aws organizations enable-aws-service-access --service-principal=config-
multiaccountsetup.amazonaws.com
```

4. Geben Sie den folgenden Befehl ein, um den Servicezugriff als delegierter Administrator für Ihre Organisation zu aktivieren und AWS Config Daten in Ihrer gesamten Organisation zu aggregieren:

```
aws organizations enable-aws-service-access --service-
principal=config.amazonaws.com
```

5. Um zu überprüfen, ob die Aktivierung des Servicezugriffs abgeschlossen ist, geben Sie den folgenden Befehl ein und betätigen Sie die Eingabetaste, um ihn auszuführen.

```
aws organizations list-aws-service-access-for-organization
```

Die Ausgabe sollte folgendermaßen oder ähnlich aussehen:

```
{
    "EnabledServicePrincipals": [
        {
            "ServicePrincipal": [
                "config.amazonaws.com",
                "config-multiaccountsetup.amazonaws.com"
        ],
```

```
            "DateEnabled": 1607020860.881
        }
    ]
}
```

6. Geben Sie als Nächstes den folgenden Befehl ein, um ein Mitgliedskonto als delegierter Administrator für AWS Config zu registrieren.

```
aws organizations register-delegated-administrator --service-principal=config-
multiaccountsetup.amazonaws.com --account-id MemberAccountID
```

and

```
aws organizations register-delegated-administrator --service-
principal=config.amazonaws.com --account-id MemberAccountID
```

7. Um zu überprüfen, ob die Registrierung des delegierten Administrators abgeschlossen ist, geben Sie den folgenden Befehl im Verwaltungskonto ein und betätigen Sie die Eingabetaste, um ihn auszuführen.

```
aws organizations list-delegated-administrators --service-principal=config-
multiaccountsetup.amazonaws.com
```

and

```
aws organizations list-delegated-administrators --service-
principal=config.amazonaws.com
```

Die Ausgabe sollte folgendermaßen oder ähnlich aussehen:

```
{
    "DelegatedAdministrators": [
        {
            "Id": "MemberAccountID",
            "Arn": "arn:aws:organizations::ManagementAccountID:account/o-
c7esubdi38/MemberAccountID",
            "Email": "name@amazon.com",
            "Name": "name",
            "Status": "ACTIVE",
            "JoinedMethod": "INVITED",
            "JoinedTimestamp": 1604867734.48,
```

```
            "DelegationEnabledDate": 1607020986.801
        }
    ]
}
```

Aggregatoren bearbeiten für AWS Config

Sie können die AWS Config Konsole oder die verwenden AWS CLI , um Ihre Aggregatoren zu bearbeiten.

Editing Aggregators (Console)

1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die AWS Config Konsole zu https://console.aws.amazon.com/config/Hause.
2. Navigieren Sie zur Aggregator-Seite und wählen Sie den Namen des Aggregators aus.
3. Wählen Sie Aktionen und dann Bearbeiten aus.
4. Verwenden Sie die Abschnitte auf der Seite Aggregator bearbeiten, um Quellkonten, IAM-Rollen oder Regionen für den Aggregator zu ändern.

   > **Note**
   >
   > Der Quelltyp kann nicht von einzelnen Konten auf die Organisation geändert werden (und umgekehrt).

5. Wählen Sie Speichern.

Editing Aggregators (AWS CLI)

1. Mit dem Befehl `put-configuration-aggregator` können Sie einen Konfigurationsaggregator aktualisieren oder bearbeiten.

   Geben Sie den folgenden Befehl ein, um **`MyAggregator`** eine neue Konto-ID hinzuzufügen:

   ```
   aws configservice put-configuration-aggregator --configuration-aggregator-name
    MyAggregator --account-aggregation-sources "[{\"AccountIds\": [\"AccountID1\",
   \"AccountID2\",\"AccountID3\"],\"AllAwsRegions\": true}]"
   ```

2. Abhängig von Ihrem Quellkonto sollte die Ausgabe wie folgt aussehen:

Bei einzelnen Konten

```
{
    "ConfigurationAggregator": {
        "ConfigurationAggregatorArn": "arn:aws:config:Region:AccountID:config-
aggregator/config-aggregator-xz2upuu6",
        "CreationTime": 1517952090.769,
        "ConfigurationAggregatorName": "MyAggregator",
        "AccountAggregationSources": [
            {
                "AllAwsRegions": true,
                "AccountIds": [
                    "AccountID1",
                    "AccountID2",
                    "AccountID3",
                    "AccountID4"
                ]
            }
        ],
        "LastUpdatedTime": 1517952566.445
    }
}
```

ODER

Bei einer Organisation

```
{
    "ConfigurationAggregator": {
        "ConfigurationAggregatorArn": "arn:aws:config:Region:AccountID:config-
aggregator/config-aggregator-floqpus3",
        "CreationTime": 1517942461.442,
        "ConfigurationAggregatorName": "MyAggregator",
        "OrganizationAggregationSource": {
                "AllAwsRegions": true,
                "RoleArn": "arn:aws:iam::account-of-role-to-assume:role/name-of-
role"
         },
        "LastUpdatedTime": 1517942461.442
    }
}
```

Löschen von Aggregatoren für AWS Config

Sie können die AWS Config Konsole oder die verwenden AWS CLI , um Ihre Aggregatoren zu löschen.

Deleting Aggregators (Console)

1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die AWS Config Konsole zu https://console.aws.amazon.com/config/Hause.
2. Navigieren Sie zur Aggregator-Seite und wählen Sie den Namen des Aggregators aus.
3. Wählen Sie Actions und dann Delete aus.

   Eine Warnmeldung wird angezeigt. Wenn Sie einen Aggregator löschen, gehen alle aggregierten Daten verloren. Sie können diese Daten nicht wiederherstellen; die Daten der Quellkonten werden jedoch nicht beeinträchtigt.
4. Wählen Sie Delete (Löschen) aus, um Ihre Auswahl zu bestätigen.

Deleting Aggregators (AWS CLI)

Geben Sie den folgenden Befehl ein:

```
aws configservice delete-configuration-aggregator --configuration-aggregator-name
 MyAggregator
```

Bei einer erfolgreichen Befehlsausführung gibt es keine weitere Ausgabe.

Autorisieren von Aggregatorkonten zur Erfassung von AWS Config Konfigurations- und Compliance-Daten

Autorisierung bezieht sich auf die Berechtigungen, die Sie einem Aggregatorkonto und einer Region zur Erfassung Ihrer AWS Config Konfigurations- und Compliance-Daten gewähren. Die Autorisierung ist nicht erforderlich, wenn Sie Quellkonten aggregieren, die Teil von AWS Organizations sind.
Sie können die AWS Config Konsole oder die verwenden, um AWS CLI Aggregatorkonten zu autorisieren.

Themen

- Überlegungen

- Autorisierung wird hinzugefügt

Überlegungen

Es gibt zwei Arten von Aggregatoren: Aggregator für einzelne Konten und Aggregator für die Organisation

Bei einem Aggregator für einzelne Konten ist eine Autorisierung für alle Quellkonten und Regionen erforderlich, die Sie einbeziehen möchten, einschließlich externer Konten und Regionen sowie Mitgliedskonten und Regionen der Organisation.

Bei einem Organisationsaggregator ist keine Autorisierung für Regionen mit Mitgliedskonten der Organisation erforderlich, da die Autorisierung in den Service integriert ist. AWS Organizations

Aggregatoren werden nicht automatisch in Ihrem Namen AWS Config aktiviert

AWS Config muss im Quellkonto und in der Region für beide Aggregatortypen aktiviert sein, damit AWS Config Daten im Quellkonto und in der Region generiert werden können.

Autorisierung wird hinzugefügt

Adding Authorization (Console)

Sie können eine Autorisierung hinzufügen, um Aggregatorkonten und Regionen die Erlaubnis zu erteilen, AWS Config Konfigurations- und Compliance-Daten zu sammeln.

1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die AWS Config Konsole zu https://console.aws.amazon.com/config/Hause.
2. Rufen Sie die Seite Authorizations (Autorisierungen) auf und klicken Sie auf Add authorization (Autorisierung hinzufügen).
3. Geben Sie unter Aggregator account (Aggregatorkonto) die zwölfstellige Konto-ID eines Aggregatorkontos an.
4. Wählen Sie unter Aggregatorregion die AWS-Regionen aus, in denen das Aggregatorkonto berechtigt ist, AWS -Config-Daten zur Konfiguration und Compliance zu erfassen.
5. Wählen Sie Add authorization (Autorisierung hinzufügen) aus, um Ihre Auswahl zu bestätigen.

   AWS Config zeigt ein Aggregatorkonto, eine Region und einen Autorisierungsstatus an.

> **Note**
>
> Sie können mithilfe von Beispielvorlagen auch programmatisch Autorisierungen zu Aggregatorkonten und Regionen hinzufügen. AWS CloudFormation Weitere Informationen finden Sie unter AWS::Config::AggregationAuthorization im AWS CloudFormation -Benutzerhandbuch.

Authorizing a Pending Request (Console)

Sofern eine ausstehende Anforderung eines bestehenden Aggregatorkontos vorliegt, wird der Anforderungsstatus auf der Seite Autorisierungen angezeigt. Sie können die ausstehende Anforderung auf dieser Seite autorisieren.

1. Wählen Sie das Aggregatorkonto aus, das Sie autorisieren möchten, und klicken Sie auf Autorisieren.

   Es wird eine Bestätigungsmeldung angezeigt, um zu bestätigen, dass Sie dem Aggregatorkonto die Erlaubnis erteilen möchten, AWS Config Daten von diesem Konto zu sammeln.
2. Wählen Sie erneut Autorisieren aus, um zu bestätigen, dass Sie dem Aggregatorkonto die Berechtigung erteilen möchten.

   Der Autorisierungsstatus wird von Requesting for authorization (Autorisierung angefordert) in Authorized (Autorisiert) geändert.

Genehmigungszeitraum für die Autorisierung

Für das Hinzufügen von Quellkonten zu einem Aggregator für einzelne Konten ist eine Autorisierungsgenehmigung erforderlich. Nachdem ein Aggregator für einzelne Konten ein Quellkonto hinzugefügt hat, bleibt eine ausstehende Autorisierungsanfrage 7 Tage lang verfügbar.

Adding Authorization (AWS CLI)

1. Öffnen Sie eine Eingabeaufforderung oder ein Terminal-Fenster.
2. Geben Sie den folgenden Befehl ein:

```
aws configservice put-aggregation-authorization --authorized-account-id
  AccountID --authorized-aws-region Region
```

3. Die Ausgabe sollte folgendermaßen oder ähnlich aussehen:

```
{
    "AggregationAuthorization": {
        "AuthorizedAccountId": "AccountID",
        "AggregationAuthorizationArn":
 "arn:aws:config:Region:AccountID:aggregation-authorization/AccountID/Region",
        "CreationTime": 1518116709.993,
        "AuthorizedAwsRegion": "Region"
    }
}
```

Löschen der Autorisierung für Aggregatorkonten zur Erfassung von AWS Config Konfigurations- und Compliance-Daten

Autorisierung bezieht sich auf die Berechtigungen, die Sie einem Aggregatorkonto und einer Region zur Erfassung Ihrer AWS Config Konfigurations- und Compliance-Daten gewähren. Die Autorisierung ist nicht erforderlich, wenn Sie Quellkonten aggregieren, die Teil von AWS Organizations sind. Sie können die AWS Config Konsole oder die verwenden, um AWS CLI Autorisierungen zu löschen.

Themen

- Überlegungen
- Autorisierung wird gelöscht

Überlegungen

Es gibt zwei Arten von Aggregatoren: Aggregator für einzelne Konten und Aggregator für die Organisation

Bei einem Aggregator für einzelne Konten ist eine Autorisierung für alle Quellkonten und Regionen erforderlich, die Sie einbeziehen möchten, einschließlich externer Konten und Regionen sowie Mitgliedskonten und Regionen der Organisation.

Bei einem Organisationsaggregator ist keine Autorisierung für Regionen mit Mitgliedskonten der Organisation erforderlich, da die Autorisierung in den AWS Organizations Service integriert ist.

Aggregatoren werden nicht automatisch in Ihrem Namen AWS Config aktiviert

AWS Config muss im Quellkonto und in der Region für beide Aggregatortypen aktiviert sein, damit AWS Config Daten im Quellkonto und in der Region generiert werden können.

Autorisierung wird gelöscht

Deleting Authorization (Console)

1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die AWS Config Konsole zu https://console.aws.amazon.com/config/Hause.
2. Wählen Sie das Aggregatorkonto aus, dessen Autorisierung Sie löschen möchten, und klicken Sie auf Löschen.

   Eine Warnmeldung wird angezeigt. Wenn Sie diese Autorisierung löschen, werden keine AWS Config Daten mehr mit dem Aggregatorkonto geteilt.
3. Wählen Sie Löschen aus, um Ihre Auswahl zu bestätigen.

   Das Aggregatorkonto ist nun gelöscht.

Deleting Authorization (AWS CLI)

Geben Sie den folgenden Befehl ein:

```
aws configservice delete-aggregation-authorization --authorized-account-id
  AccountID --authorized-aws-region Region
```

Bei einer erfolgreichen Befehlsausführung gibt es keine weitere Ausgabe.

Aggregatoren anzeigen für AWS Config

Sie können die AWS Config Konsole oder die verwenden AWS CLI , um Ihre Aggregatoren anzuzeigen.

Viewing Aggregators (Console)

Informationen zur Anzeige Ihrer Conformance Packs im finden Sie unter AWS Management ConsoleAggregator-Dashboard.

Viewing Aggregators (AWS CLI)

1. Geben Sie den folgenden Befehl ein:

```
aws configservice describe-configuration-aggregators
```

2. Abhängig von Ihrem Quellkonto sollte die Ausgabe wie folgt aussehen:

Bei einzelnen Konten

```
{
    "ConfigurationAggregators": [
        {
            "ConfigurationAggregatorArn":
 "arn:aws:config:Region:AccountID:config-aggregator/config-aggregator-floqpus3",
            "CreationTime": 1517942461.442,
            "ConfigurationAggregatorName": "MyAggregator",
            "AccountAggregationSources": [
                {
                    "AllAwsRegions": true,
                    "AccountIds": [
                        "AccountID1",
                        "AccountID2",
                        "AccountID3"
                    ]
                }
            ],
            "LastUpdatedTime": 1517942461.455
        }
    ]
}
```

ODER

Bei einer Organisation

```
{
    "ConfigurationAggregator": {
```

```
        "ConfigurationAggregatorArn": "arn:aws:config:Region:AccountID:config-
aggregator/config-aggregator-floqpus3",
        "CreationTime": 1517942461.442,
        "ConfigurationAggregatorName": "MyAggregator",
        "OrganizationAggregationSource": {
                "AllAwsRegions": true,
                "RoleArn": "arn:aws:iam::account-of-role-to-assume:role/name-of-
role"
         },
        "LastUpdatedTime": 1517942461.442
    }
}
```

Fehlerbehebung bei der Datenaggregation mit mehreren Konten für mehrere Regionen für AWS Config

AWS Config aggregiert möglicherweise aus einem der folgenden Gründe keine Daten aus Quellkonten:

Szenario	Vorgehensweise
AWS Config ist im Quellkonto für Konten innerhalb einer Organisation nicht aktiviert.	Aktivieren Sie die Option AWS Config im Quellkonto und autorisieren Sie das Aggregatorkonto, Daten zu sammeln.
Einem Aggregatorkonto wird keine Autorisierung erteilt.	Melden Sie sich beim Quellkonto an und erteilen Sie dem Aggregatorkonto die Autorisierung, Daten zu sammeln. AWS Config
Eventuell gibt es ein temporäres Problem, das die Datenaggregation verhindert.	Bei der Datenaggregation können Verzögerungen auftreten. Warten Sie ein paar Minuten.

AWS Config aggregiert möglicherweise aus einem der folgenden Gründe keine Daten aus einer Organisation:

Szenario	Vorgehensweise
AWS Config kann aufgrund einer ungültigen IAM-Rolle nicht auf Ihre Organisationsdetails zugreifen.	Erstellen Sie eine IAM-Rolle oder wählen Sie eine gültige IAM-Rolle aus der Liste der IAM-Rollen aus. **Note** Wenn die IAM-Rolle länger als 7 Tage ungültig ist, werden Daten für die AWS Config gesamte Organisation gelöscht.
AWS Config Der Dienstzugriff ist in Ihrer Organisation deaktiviert.	Sie können die Integration zwischen AWS Config und AWS Organizations über die `EnableAWSServiceAccess` API aktivieren. Wenn Sie in der Konsole „Meine Organisation hinzufügen“ wählen, AWS Config wird automatisch die Integration zwischen AWS Config und aktiviert AWS Organizations.
AWS Config kann nicht auf Ihre Organisationsdetails zugreifen, da in Ihrer Organisation nicht alle Funktionen aktiviert sind.	Aktivieren Sie alle Funktionen in der AWS Organizations Konsole.
Organisatorische Änderungen wie das Hinzufügen eines Kontos, das Entfernen eines Kontos, das Aktivieren des Servicezugriffs und das Deaktivieren des Servicezugriffs werden in den Regionen Naher Osten (Bahrain) und Asien-Pazifik (Hongkong) nicht sofort aktualisiert.	Organisatorische Änderungen verzögern sich um zwei Stunden. Warten Sie diesen Zeitraum ab, um alle organisatorischen Änderungen zu sehen.

Den aktuellen Konfigurationsstatus von AWS Ressourcen abfragen mit AWS Config

Einführung einer Vorschaufunktion für erweiterte Abfragen, mit der Sie mithilfe von Funktionen generativer künstlicher Intelligenz (generative KI) Eingabeaufforderungen in einfachem Englisch eingeben und in ein ready-to-use Abfrageformat konvertieren können. Weitere Informationen finden Sie unter Abfrageprozessor in natürlicher Sprache für erweiterte Abfragen.

Sie können AWS Config damit den aktuellen Konfigurationsstatus von AWS Ressourcen auf der Grundlage von Konfigurationseigenschaften für ein einzelnes Konto und eine Region oder für mehrere Konten und Regionen abfragen. Sie können eigenschaftsbasierte Abfragen anhand der Metadaten zum aktuellen AWS Ressourcenstatus in einer Liste unterstützter Ressourcen durchführen. AWS Config Weitere Informationen zu unterstützten Ressourcentypen finden Sie in der Liste der unterstützten Ressourcentypen für erweiterte Abfragen.

Advanced Queries bietet einen einzigen Abfrageendpunkt und eine Abfragesprache, um Metadaten zum aktuellen Ressourcenstatus abzurufen, ohne dienstspezifische Describe-API-Aufrufe ausführen zu müssen. Sie können Konfigurationsaggregatoren verwenden, um dieselben Abfragen von einem zentralen Konto aus über mehrere Konten und AWS Regionen hinweg auszuführen.

Themen

- Features
- Komponenten abfragen für AWS Config
- Abfrage mit dem SQL-Abfrage-Editor für AWS Config (Konsole)
- Abfrage mit dem SQL-Abfrage-Editor für AWS Config (AWS CLI)
- Abfrageprozessor in natürlicher Sprache für AWS Config erweiterte Abfragen
- Beispielabfragen für AWS Config
- Beispiel für Beziehungsabfragen für AWS Config
- Einschränkungen
- Verhalten des notation/IP CIDR-Bereichs für erweiterte Abfragen
- Verhalten mehrerer Eigenschaften innerhalb eines Arrays für erweiterte Abfragen

- Unterstützung von Regionen

Features

AWS Config verwendet eine Teilmenge der `SELECT` SQL-Syntax (Structured Query Language), um eigenschaftsbasierte Abfragen und Aggregationen für die aktuellen Configuration Item (CI) -Daten durchzuführen. Die Komplexität der Abfragen reicht von Übereinstimmungen mit and/or Tag-Ressourcen-IDs bis hin zu komplexeren Abfragen, z. B. der Anzeige aller Amazon S3 S3-Buckets, für die die Versionierung deaktiviert ist. Auf diese Weise können Sie genau den aktuellen Ressourcenstatus abfragen, den Sie benötigen, ohne AWS dienstspezifische API-Aufrufe durchführen zu müssen.

Aggregationsfunktionen wie `AVG`, `COUNT`, `MAX`, `MIN` und `SUM` werden unterstützt.

Sie können erweiterte Abfragen für Folgendes verwenden:

- Inventarverwaltung; zum Beispiel, um eine Liste von EC2 Amazon-Instances einer bestimmten Größe abzurufen.
- Sicherheits- und Betriebsinformationen, um beispielsweise eine Liste mit Ressourcen abzufragen, bei denen eine bestimmte Konfigurationseigenschaft aktiviert bzw. deaktiviert ist.
- Kostenoptimierung, z. B. um eine Liste von Amazon EBS-Volumes zu identifizieren, die keiner EC2 Instance zugeordnet sind.
- Compliance-Daten, z. B. um eine Liste all Ihrer Conformance Packs und deren Compliance-Status abzurufen.

Informationen zur Verwendung der AWS SQL-Abfragesprache finden Sie unter Was ist SQL (Structured Query Language)? .

Komponenten abfragen für AWS Config

Die `SELECT` SQL-Abfragekomponenten für AWS Config erweiterte Abfragen lauten wie folgt.

Syntax

```
SELECT property [, ...]
[ WHERE condition ]
```

```
[ GROUP BY property ]
[ ORDER BY property [ ASC | DESC ] [, property [ ASC | DESC ] ...] ]
```

Parameter

[WHERE condition]

Filterergebnisse gemäß der festgelegten `condition`.

Vergleichsoperatoren

- =(entspricht)
- `IN`(Mitgliedschaft auflisten)
- `BETWEEN`(Reichweitenprüfung)

Logik-Operatoren

- `AND`
- `OR`
- `NOT`

[GROUP BY-Eigenschaft]

Aggregiert den Ergebnissatz zu Zeilengruppen mit übereinstimmenden Werten für die angegebene Eigenschaft.

Die GROUP BY-Klausel gilt für Aggregationen.

[ORDER BY-Eigenschaft [ASC | DESC], [Eigenschaft [ASC | DESC] ...]]

Sortiert eine Ergebnisgruppe nach einem oder mehreren Ausgabe-`properties`.

Wenn die Klausel mehrere Eigenschaften enthält, wird der Ergebnissatz nach der ersten `property` sortiert. Anschließend wird die zweite `property` auf Zeilen mit übereinstimmenden Werten für die erste Eigenschaft angewendet usw.

Beispiele

```
SELECT resourceId WHERE resourceType='AWS::EC2::Instance'
```

```
SELECT configuration.complianceType, COUNT(*) WHERE resourceType =
 'AWS::Config::ResourceCompliance' GROUP BY configuration.complianceType
```

Abfrage mit dem SQL-Abfrage-Editor für AWS Config (Konsole)

Einführung einer Vorschaufunktion für erweiterte Abfragen, mit der Sie mithilfe von Funktionen generativer künstlicher Intelligenz (generative KI) Eingabeaufforderungen in einfachem Englisch eingeben und in ein ready-to-use Abfrageformat konvertieren können. Weitere Informationen finden Sie unter Abfrageprozessor in natürlicher Sprache für erweiterte Abfragen.

Sie können entweder AWS Beispielabfragen verwenden oder Ihre eigene Abfrage erstellen, die als benutzerdefinierte Abfragen bezeichnet wird.

Überlegungen

Voraussetzungen

Wenn Sie eine der folgenden AWS verwalteten Richtlinien verwenden, verfügen Sie über die erforderlichen Berechtigungen zum Ausführen und Speichern einer Abfrage: AWSServiceRoleForConfig(serviceverknüpfte Rolle) oder AWS_CConfigRole.

Andernfalls müssen Sie über die in der verwalteten Richtlinie enthaltenen Berechtigungen verfügen. AWSConfigUserAccess AWS

Liste der Eigenschaften, die Sie abfragen können

Eine aktualisierte Liste der Eigenschaften und ihrer Datentypen finden Sie unter GitHub.

Erweiterte Abfragen und Aggregatoren

Um eine Abfrage für einen Aggregator auszuführen, erstellen Sie einen Aggregator. Weitere Informationen finden Sie unter Aggregatoren erstellen für AWS Config.

Wenn Sie bereits einen Aggregator eingerichtet haben, wählen Sie im Abfragebereich den Aggregator aus, um eine erweiterte Abfrage auf diesem Aggregator auszuführen. Wenn Sie einen Aggregator auswählen, sollten Sie erwägen, die AWS-Konto ID und die AWS Region zur Abfrageanweisung hinzuzufügen, um diese Informationen in den Ergebnissen anzuzeigen.

Verwenden Sie eine AWS Beispielabfrage

1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die AWS Config Konsole zu https://console.aws.amazon.com/config/Hause.
2. Wählen Sie im linken Navigationsbereich die Option Advanced queries (Erweiterte Abfragen), um Ihre Ressourcenkonfigurationen für ein einzelnes Konto und eine Region oder für mehrere Konten und Regionen abzufragen.
3. Wählen Sie auf der Seite Erweiterte Abfragen eine geeignete Abfrage aus der Liste der Abfragen aus. Sie können Abfragen nach Name, Beschreibung, Ersteller oder Tags filtern. Um AWS - Abfragen zu filtern, wählen Sie Ersteller aus und geben Sie AWS ein. Die ausgewählte Abfrage wird im SQL-Abfrage-Editor angezeigt. Sie können die ausgewählte Abfrage an Ihre Bedürfnisse anpassen.
4. Um diese Abfrage in einer neuen Abfrage zu speichern, wählen Sie Speichern unter aus.
   - Aktualisieren Sie im Feld Abfragename den Namen der Abfrage.
   - Aktualisieren Sie im Feld Beschreibung die Beschreibung der Abfrage.
   - Geben Sie bis zu 50 eindeutige Tags für diese Abfrage ein.
   - Wählen Sie Speichern.
5. Wählen Sie Ausführen aus. Die Abfrageergebnisse werden in der Tabelle unter dem Abfrage-Editor angezeigt.
6. Wählen Sie Export as (Exportieren als) aus, um die Abfrageergebnisse im CSV- oder JSON-Format zu exportieren.

Erstellen einer benutzerdefinierten Abfrage

1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die AWS Config Konsole zu https://console.aws.amazon.com/config/Hause.
2. Wählen Sie im linken Navigationsbereich die Option Advanced queries (Erweiterte Abfragen), um Ihre Ressourcenkonfigurationen für ein einzelnes Konto und eine Region oder für mehrere Konten und Regionen abzufragen.
3. Um eine benutzerdefinierte Abfrage zu erstellen, wählen Sie Neue Abfrage aus.

   Wenn Sie eine benutzerdefinierte Abfrage anzeigen oder bearbeiten möchten, filtern Sie sie nach Name, Beschreibung, Ersteller oder Tags. Um benutzerdefinierte Abfragen zu filtern, wählen Sie Ersteller aus und geben Sie Benutzerdefiniert ein.

4. Erstellen Sie auf der Seite Abfrage-Editor eine eigene Abfrage für dieses Konto und die Region. Sie können auch einen geeigneten Aggregator auswählen, um eine Abfrage für mehrere Konten und Regionen zu erstellen.
5. Bearbeiten Sie Folgendes, wenn Sie Änderungen an dieser Abfrage vornehmen möchten. Um diese Abfrage zu speichern, wählen Sie Abfrage speichern aus.
   - Aktualisieren Sie im Feld Abfragename den Namen der Abfrage.
   - Aktualisieren Sie im Feld Beschreibung die Beschreibung der Abfrage.
   - Geben Sie bis zu 50 eindeutige Tags für diese Abfrage ein.
   - Wählen Sie Speichern.
6. Wählen Sie Ausführen aus. Die Abfrageergebnisse werden in der Tabelle unter dem Abfrage-Editor angezeigt.
7. Wählen Sie Export as (Exportieren als) aus, um die Abfrageergebnisse im CSV- oder JSON-Format zu exportieren.

Abfrage mit dem SQL-Abfrage-Editor für AWS Config (AWS CLI)

Das AWS CLI ist ein einheitliches Tool zur Verwaltung Ihrer AWS Dienste. Mit nur einem Tool zum Herunterladen und Konfigurieren können Sie mehrere AWS Dienste von der Befehlszeile aus steuern und mithilfe von Skripten automatisieren. Weitere Informationen zu den Tools AWS CLI und Anweisungen zur Installation der AWS CLI Tools finden Sie im Folgenden im AWS Command Line Interface Benutzerhandbuch.

- AWS Command Line Interface Benutzerhandbuch
- Einrichtung der AWS Command Line Interface

Geben Sie bei Bedarf ein, `aws configure` um das so AWS CLI zu konfigurieren, dass es eine AWS Region verwendet, in der erweiterte Abfragen verfügbar sind.

Überlegungen

Voraussetzungen

Wenn Sie eine der folgenden AWS verwalteten Richtlinien verwenden, verfügen Sie über die erforderlichen Berechtigungen zum Ausführen und Speichern einer Abfrage: AWSServiceRoleForConfig(serviceverknüpfte Rolle) oder AWS_CConfigRole.

Andernfalls müssen Sie über die in der verwalteten Richtlinie enthaltenen Berechtigungen verfügen. AWSConfigUserAccess AWS

Liste der Eigenschaften, die Sie abfragen können

Eine aktualisierte Liste der Eigenschaften und ihrer Datentypen finden Sie unter GitHub.

Erweiterte Abfragen und Aggregatoren

Um eine Abfrage für einen Aggregator auszuführen, erstellen Sie einen Aggregator. Weitere Informationen finden Sie unter Aggregatoren erstellen für AWS Config.

Wenn Sie bereits einen Aggregator eingerichtet haben, wählen Sie im Abfragebereich den Aggregator aus, um eine erweiterte Abfrage auf diesem Aggregator auszuführen. Wenn Sie einen Aggregator auswählen, sollten Sie erwägen, die AWS-Konto ID und die AWS Region in der Abfrageanweisung hinzuzufügen, um diese Informationen in den Ergebnissen anzuzeigen.

Abfragen von Konfigurationsdaten für Ressourcen

So fragen Sie die Ressourcenkonfigurationsdaten mit dem Abfrage-Editor (AWS CLI) für ein einzelnes Konto und eine Region ab

1. Öffnen Sie eine Eingabeaufforderung oder ein Terminal-Fenster.
2. Geben Sie den folgenden Befehl ein, um Ihre Ressourcenkonfigurationsdaten abzufragen.

```
aws configservice select-resource-config --expression "SELECT resourceId WHERE
 resourceType='AWS::EC2::Instance'"
```

Abhängig von Ihrer Abfrage sieht die Ausgabe ähnlich der folgenden aus:

```
{
    "QueryInfo": {
        "SelectFields": [
            {
                "Name": "resourceId"
            }
        ]
    },
    "Results": [
        "{\"resourceId\":\"ResourceId\"}",
        "{\"resourceId\":\"ResourceId\"}",
```

```
        "{\"resourceId\":\"ResourceId\"}",
        "{\"resourceId\":\"ResourceId\"}",
        "{\"resourceId\":\"ResourceId\"}",
        "{\"resourceId\":\"ResourceId\"}",
        "{\"resourceId\":\"ResourceId\"}"
    ]
}
```

So fragen Sie die Ressourcenkonfigurationsdaten mit dem Abfrage-Editor (AWS CLI) für mehrere Konten und Regionen ab

1. Öffnen Sie eine Eingabeaufforderung oder ein Terminal-Fenster.
2. Geben Sie den folgenden Befehl ein, um Ihre Ressourcenkonfigurationsdaten abzufragen.

```
aws configservice select-aggregate-resource-config --expression "SELECT resourceId
 WHERE resourceType='AWS::EC2::Instance'" --configuration-aggregator-name my-
aggregator
```

Abhängig von Ihrer Abfrage sieht die Ausgabe ähnlich der folgenden aus:

```
{
    "QueryInfo": {
        "SelectFields": [
            {
                "Name": "resourceId"
            }
        ]
    },
    "Results": [
        "{\"resourceId\":\"ResourceId\"}",
        "{\"resourceId\":\"ResourceId\"}",
        "{\"resourceId\":\"ResourceId\"}",
        "{\"resourceId\":\"ResourceId\"}",
        "{\"resourceId\":\"ResourceId\"}",
        "{\"resourceId\":\"ResourceId\"}",
        "{\"resourceId\":\"ResourceId\"}"
    ]
}
```

> **Note**
>
> Wenn Sie die `AWS::IAM::Policy` Ressourcentypen `AWS::IAM::User` `AWS::IAM::Group``AWS::IAM::Role`,, und in einer erweiterten Abfrage verwenden, verwenden Sie`awsRegion = 'global'`.

Speichern einer Abfrage

1. Öffnen Sie eine Eingabeaufforderung oder ein Terminal-Fenster.
2. Geben Sie den folgenden Befehl ein, um eine Abfrage zu speichern.

```
aws configservice put-stored-query --stored-query "{\"QueryName\": \"cli-test\",
 \"Expression\": \"SELECT *\", \"Description\": \"cli test query\" }"
        --tags "[{ \"Key\": \"first-tag\", \"Value\": \"\" }, { \"Key\": \"second-
tag\", \"Value\": \"non-empty-tag-value\" }]"
```

3. Abhängig von Ihrer Abfrage sieht die Ausgabe ähnlich der folgenden aus:

```
{
    "QueryArn": "arn:aws:config:eu-central-1:Account ID:stored-query/cli-test/
query-e65mijt4rmam5pab"
}
```

> **Note**
>
> `--tags` ist optional. Wenn Sie die Tags übergeben, werden die gespeicherten Tags weder von `list-stored-queries` noch von `get-stored-query` zurückgegeben. Sie müssen `list-tag-for-resources` verwenden, um die zugehörigen Tags für eine gespeicherte Abfrage abzurufen.
> `--description` ist beim Erstellen oder Aktualisieren einer Abfrage optional.

Anzeigen aller gespeicherten Abfragen

1. Geben Sie den folgenden Befehl ein, um die Liste aller gespeicherten Abfragen anzuzeigen.

```
aws configservice list-stored-queries
```

2. Abhängig von Ihrer Abfrage sieht die Ausgabe ähnlich der folgenden aus:

```
{
    "StoredQueryMetadata": [
        {
            "QueryId": "query-e65mijt4rmam5pab",
            "QueryArn": "arn:aws:config:eu-central-1:Account ID:stored-query/cli-
test/query-e65mijt4rmam5pab",
            "QueryName": "cli-test"
        },
        {
            "QueryId": "query-rltwlewlqfivadxq",
            "QueryArn": "arn:aws:config:eu-central-1:Account ID:stored-query/cli-
test-2/query-rltwlewlqfivadxq",
            "QueryName": "cli-test-2",
            "Description": "cli test query"
        }
    ]
}
}
```

Abrufen von Details zu einer gespeicherten Abfrage

1. Geben Sie den folgenden Befehl ein, um Details zu einer bestimmten gespeicherten Abfrage abzurufen.

```
aws configservice get-stored-query --query-name cli-test
```

2. Abhängig von Ihrer Abfrage sieht die Ausgabe ähnlich der folgenden aus:

```
{
    "StoredQuery": {
        "QueryId": "query-e65mijt4rmam5pab",
        "QueryArn": "arn:aws:config:eu-central-1:Account ID:stored-query/cli-test/
query-e65mijt4rmam5pab",
        "QueryName": "cli-test",
        "Description": "cli test query",
        "Expression": "SELECT *"
```

```
    }
}
```

Löschen einer gespeicherten Abfrage

- Geben Sie den folgenden Befehl ein, um Ihre gespeicherte Abfrage zu löschen.

```
aws configservice delete-stored-query --query-name cli-test
```

Bei einer erfolgreichen Befehlsausführung gibt es keine weitere Ausgabe.

Abfrageprozessor in natürlicher Sprache für AWS Config erweiterte Abfragen

> Der Abfrageprozessor in natürlicher Sprache für erweiterte Abfragen befindet sich in der Vorschauversion für AWS Config und kann sich ändern.

Der Abfrageprozessor in natürlicher Sprache für erweiterte Abfragen verwendet Amazon Bedrock, eine Technologie für generative künstliche Intelligenz (generative KI), mit der Sie Eingabeaufforderungen in einfachem Englisch eingeben und in ein ready-to-use Abfrageformat konvertieren können. Mit dem Prozessor für Abfragen in natürlicher Sprache können Sie Ihre AWS-Konto oder unternehmensweite Abfragen durchführen. AWS

Eine Aufforderung kann eine Frage oder eine Aussage sein. Sie können beispielsweise Eingabeaufforderungen wie „Welche Load Balancer werden nach dem 1. Januar 2024 erstellt?“ eingeben. und „Listet alle meine Lambda-Funktionen auf, auf denen Node JS 16 ausgeführt wird.“

Überlegungen

Der Abfrageprozessor für natürliche Sprache kann die folgenden Aktionen nicht ausführen:

- Generieren Sie Abfragen aus anderen Sprachen als Englisch.
- Generieren Sie Abfragen anhand von Eingabeaufforderungen, die sich nicht auf erweiterte Abfragen beziehen.
- Generieren Sie Abfragen anhand von Eingabeaufforderungen mit mehr als 1000 Zeichen.

- Generieren Sie Abfragen anhand von Folgekorrekturen oder aus früheren Sitzungen.
- Erläutern Sie den generierten Code.

Abfragen mithilfe des Abfrageprozessors für natürliche Sprache

1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die AWS Config Konsole zu https://console.aws.amazon.com/config/Hause.
2. Wählen Sie im linken Navigationsbereich die Option Advanced queries (Erweiterte Abfragen), um Ihre Ressourcenkonfigurationen für ein einzelnes Konto und eine Region oder für mehrere Konten und Regionen abzufragen.
3. Wählen Sie auf der Seite Erweiterte Abfragen die Option Neue Abfrage aus, um zum -Abfrage-Editor zu wechseln.
   - (Optional) Um eine Abfrage auf einem Aggregator auszuführen, erstellen Sie einen Aggregator. Weitere Informationen finden Sie unter Aggregatoren erstellen für AWS Config.
   - Wenn Sie bereits einen Aggregator eingerichtet haben, wählen Sie im Abfragebereich den Aggregator aus, um eine erweiterte Abfrage auf diesem Aggregator auszuführen. Wenn Sie einen Aggregator auswählen, sollten Sie erwägen, die AWS-Konto ID und die AWS Region zur Abfrageanweisung hinzuzufügen, um diese Informationen in den Ergebnissen anzuzeigen.
4. Gehen Sie im Abfrage-Editor zum Abschnitt Abfrageprozessor für natürliche Sprache. Geben Sie eine Aufforderung in einfachem Englisch ein und wählen Sie dann Generieren aus. Beispiele finden Sie unter Beispielaufforderungen.
5. Nachdem Sie eine Abfrage generiert haben, können Sie Kopieren (funktional entspricht Strg+C) wählen, um die Abfrage in Ihre Zwischenablage zu kopieren, oder In Editor eingeben wählen. Wenn die Daten in den Editor eingegeben wurden, können Sie die generierte Abfrage an Ihre Bedürfnisse anpassen.
6. Um diese Abfrage in einer neuen Abfrage zu speichern, wählen Sie Speichern unter aus.
   - Aktualisieren Sie im Feld Abfragename den Namen der Abfrage.
   - Aktualisieren Sie im Feld Beschreibung die Beschreibung der Abfrage.
   - Geben Sie bis zu 50 eindeutige Tags für diese Abfrage ein.
   - Wählen Sie Speichern.
7. Wählen Sie Ausführen aus. Die Abfrageergebnisse werden in der Tabelle unter dem Abfrage-Editor angezeigt.

8. Wählen Sie Export as (Exportieren als) aus, um die Abfrageergebnisse im CSV- oder JSON-Format zu exportieren.

> **Note**
>
> Die Abfrageergebnisse werden paginiert. Wenn Sie exportieren, werden bis zu 500 Ergebnisse exportiert.
> Sie können den auch verwenden APIs , um alle Ergebnisse abzurufen. Die Ergebnisse werden paginiert und Sie können 100 Ergebnisse gleichzeitig abrufen.

Beispielaufforderungen

Im Folgenden finden Sie Eingabeaufforderungen und generierte Abfragen, die Sie als Beispiele verwenden können.

Example: Welche Load Balancer wurden nach dem 1. Januar 2024 erstellt?

Aufforderung: What load balancers were created after January 1, 2024?

Generierte Abfrage:

```
SELECT
    resourceId,
    resourceType,
    resourceCreationTime
WHERE
    resourceType IN ('AWS::ElasticLoadBalancing::LoadBalancer',
 'AWS::ElasticLoadBalancingV2::LoadBalancer')
AND
    resourceCreationTime > '2024-01-01T00:00:00.0Z'
ORDER BY
    resourceCreationTime
DESC
```

Example: Welche meiner RDS-Datenbank-Instances sind öffentlich zugänglich?

Aufforderung: Which of my RDS database instances are publicly accessible?

Generierte Abfrage:

```
SELECT
```

```
    resourceId,
    resourceType,
    configuration.publiclyAccessible
WHERE
    resourceType = 'AWS::RDS::DBInstance'
AND
    configuration.publiclyAccessible = true
```

Example: Wie viele EC2 Instanzen wurden im letzten Jahr erstellt?

Aufforderung: How many EC2 instances were created in last one year?

Generierte Abfrage:

```
SELECT
    COUNT(*)
WHERE
    resourceType = 'AWS::EC2::Instance'
AND
    resourceCreationTime
BETWEEN
    '2023-05-10T16:56:25.000Z'
AND
    '2024-05-10T16:56:25.000Z'
```

Example: Wie viele EC2 Instanzen habe ich in jeder meiner AWS-Konten?

Aufforderung: How many EC2 instances do I have in each of my AWS-Konten?

Generierte Abfrage:

```
SELECT
    accountId,
    COUNT(*)
WHERE
    resourceType = 'AWS::EC2::Instance'
GROUP BY
    accountId'
```

Example: An welche IAM-Rollen ist die verwaltete Richtlinie AdministratorAccess angehängt?

Aufforderung: Which IAM roles have the managed policy AdministratorAccess attached?

Generierte Abfrage:

```
SELECT
    resourceId,
    resourceName,
    resourceType
WHERE
    resourceType = 'AWS::IAM::Role'
AND
    configuration.attachedManagedPolicies.policyName = 'AdministratorAccess'
```

Example: EBS-Volumes ohne Verschlüsselung

Aufforderung: EBS volumes without encryption

Generierte Abfrage:

```
SELECT
    accountId
WHERE
    resourceType = 'AWS::EC2::Volume'
AND
    configuration.encrypted = false
```

Example: Nicht konforme Ressourcen abrufen

Aufforderung: Get noncompliant resources

Generierte Abfrage:

```
SELECT
    resourceId,
    resourceType
WHERE
    resourceType = 'AWS::Config::ResourceCompliance'
AND
    configuration.complianceType = 'NON_COMPLIANT'
```

Example: Listet alle meine Lambda-Funktionen auf, auf denen Node JS 16 ausgeführt wird

Aufforderung: List all my lambda function that is running node js 16

Generierte Abfrage:

```
SELECT
    accountId,
    resourceName
WHERE
    resourceType = 'AWS::Lambda::Function'
AND
    configuration.runtime = 'nodejs16.x'
```

Example: Welche ACM-Zertifikate laufen in den nächsten 30 Tagen ab?

Aufforderung: What ACM certificates expire the next 30 days?

Generierte Abfrage:

```
SELECT
    resourceId,
    configuration.domainName,
    configuration.notAfter
WHERE
    resourceType = 'AWS::ACM::Certificate'
AND
    configuration.notAfter
BETWEEN
    '2024-05-10 16:59:53'
AND
    '2024-06-10 16:59:53’
```

> **Note**
>
> Die Zeiten in der generierten Abfrage hängen von der Uhrzeit ab, zu der Sie die Eingabeaufforderung eingeben.

Feedback geben

Sie können allgemeines Feedback zum Abfrageprozessor in natürlicher Sprache oder Feedback zu einer bestimmten generierten Abfrage geben.

Geben Sie Feedback zum Prozessor für Abfragen in natürlicher Sprache

Wählen Sie die Schaltfläche Feedback geben, die rechts über dem Prozessor für Abfragen in natürlicher Sprache angezeigt wird. Sie können Ihre Zufriedenheit oder Unzufriedenheit eingeben und Feedback dazu geben, wie Sie die Abfrage in natürlicher Sprache hilfreicher gestalten AWS Config können.

> **Note**
>
> Geben Sie keine persönlichen, wirtschaftlich sensiblen oder vertraulichen Informationen weiter.

Geben Sie Feedback zu einer bestimmten generierten Anfrage

Sie können Ihr Feedback zu einer generierten Abfrage geben, indem Sie auf die Schaltfläche „Daumen hoch“ oder „Daumen runter“ klicken, die unter der generierten Abfrage angezeigt wird.

Unterstützung von Regionen

Der Abfrageprozessor für natürliche Sprache wird in folgenden Regionen unterstützt.

Name der Region	Region	Endpunkt	Protokoll
USA Ost (Nord-Virginia)	us-east-1	config.us-east-1.amazonaws.com	HTTPS
USA West (Oregon)	us-west-2	config.us-west-2.amazonaws.com	HTTPS

Beispielabfragen für AWS Config

Sehen Sie sich die folgenden Beispielabfragen an.

Query to list all EC2 instances with AMI ID ami-12345

Abfrage:

```
SELECT
```

```
    resourceId,
    resourceType,
    configuration.instanceType,
    configuration.placement.tenancy,
    configuration.imageId,
    availabilityZone
WHERE
    resourceType = 'AWS::EC2::Instance'
AND
    configuration.imageId = 'ami-12345'
```

Ergebnisse:

```
{
    "QueryInfo": {
        "SelectFields": [
            {
                "Name": "resourceId"
            },
            {
                "Name": "resourceType"
            },
            {
                "Name": "configuration.instanceType"
            },
            {
                "Name": "configuration.placement.tenancy"
            },
            {
                "Name": "configuration.imageId"
            },
            {
                "Name": "availabilityZone"
            }
        ]
    },
    "Results": [
        "{\"resourceId\":\"resourceid\",\"configuration\":{\"imageId\":
\"ami-12345\",\"instanceType\":\"t2.micro\",\"placement\":{\"tenancy\":\"default
\"}},\"availabilityZone\":\"us-west-2c\",\resourceType\":\"AWS::EC2::Instance\"}",
        "{\"resourceId\":\"resourceid\",\"configuration\":{\"imageId\":
\"ami-12345\",\"instanceType\":\"t2.micro\",\"placement\":{\"tenancy\":\"default
\"}},\"availabilityZone\":\"us-west-2a\",\resourceType\":\"AWS::EC2::Instance\"}",
```

```
        "{\"resourceId\":\"resourceid\",\"configuration\":{\"imageId\":
\"ami-12345\",\"instanceType\":\"t2.micro\",\"placement\":{\"tenancy\":\"default
\"}},\"availabilityZone\":\"us-west-2c\",\"resourceType\":\"AWS::EC2::Instance\"}",
        "{\"resourceId\":\"resourceid\",\"configuration\":{\"imageId\":
\"ami-12345\",\"instanceType\":\"t1.micro\",\"placement\":{\"tenancy\":\"default
\"}},\"availabilityZone\":\"us-west-2a\",\"resourceType\":\"AWS::EC2::Instance\"}",
        "{\"resourceId\":\"resourceid\",\"configuration\":{\"imageId\":
\"ami-12345\",\"instanceType\":\"t2.micro\",\"placement\":{\"tenancy\":\"default
\"}},\"availabilityZone\":\"us-west-2c\",\"resourceType\":\"AWS::EC2::Instance\"}",
        "{\"resourceId\":\"resourceid\",\"configuration\":{\"imageId\":
\"ami-12345\",\"instanceType\":\"t2.micro\",\"placement\":{\"tenancy\":\"default
\"}},\"availabilityZone\":\"us-west-2c\",\"resourceType\":\"AWS::EC2::Instance\"}",
        "{\"resourceId\":\"resourceid\",\"configuration\":{\"imageId\":
\"ami-12345\",\"instanceType\":\"t2.micro\",\"placement\":{\"tenancy\":\"default
\"}},\"availabilityZone\":\"us-west-2c\",\"resourceType\":\"AWS::EC2::Instance\"}"
    ]
}
```

Query for count of resources grouped by their AWS Config rules compliance status

Abfrage:

```
SELECT
    configuration.complianceType,
    COUNT(*)
WHERE
    resourceType = 'AWS::Config::ResourceCompliance'
GROUP BY
    configuration.complianceType
```

Ergebnisse:

```
{
    "QueryInfo": {
        "SelectFields": [
            {
                "Name": "configuration.complianceType"
            },
            {
                "Name": "COUNT(*)"
            }
        ]
    },
```

```
    "Results": [
        "{\"COUNT(*)\":163,\"configuration\":{\"complianceType\":\"NON_COMPLIANT
\"}}",
        "{\"COUNT(*)\":2,\"configuration\":{\"complianceType\":\"COMPLIANT\"}}"
    ]
}
```

Query for the compliance status of AWS Conformance packs

Abfrage:

```
SELECT
    resourceId,
    resourceName,
    resourceType,
    configuration.complianceType
WHERE
    resourceType = 'AWS::Config::ConformancePackCompliance'
```

Ergebnisse:

```
{
    "QueryInfo": {
        "SelectFields": [
            {
                "Name": "resourceId"
            },
            {
                "Name": "resourceName"
            },
            {
                "Name": "resourceType"
            },
            {
                "Name": "configuration.complianceType"
            }
        ]
    },
    "Results": [
        "{\"resourceId\":\"conformance-pack-conformance-pack-ID\",\"configuration
\":{\"complianceType\":\"COMPLIANT\"},\"resourceName\":\"MyConformancePack1\",
\"resourceType\":\"AWS::Config::ConformancePackCompliance\"}",
```

```
        "{\"resourceId\":\"conformance-pack-conformance-pack-ID\",\"configuration
\":{\"complianceType\":\"NON_COMPLIANT\"},\"resourceName\":\"MyConformancePack2\",
\"resourceType\":\"AWS::Config::ConformancePackCompliance\"}",
        "{\"resourceId\":\"conformance-pack-conformance-pack-ID\",\"configuration
\":{\"complianceType\":\"NON_COMPLIANT\"},\"resourceName\":\"MyConformancePack3\",
\"resourceType\":\"AWS::Config::ConformancePackCompliance\"}"
    ]
}
```

Query to get counts of AWS resources grouped by account ID

Abfrage:

```
aws configservice select-aggregate-resource-config --expression "SELECT COUNT(*),
 accountId group by accountId" --configuration-aggregator-name my-aggregator
```

Ergebnisse:

```
{
    "Results": [
        "{\"COUNT(*)\":2407,\"accountId\":\"accountId\"}",
        "{\"COUNT(*)\":726,\"accountId\":\"accountId\"}"
    ],
    "QueryInfo": {
        "SelectFields": [
            {
                "Name": "COUNT(*)"
            },
            {
                "Name": "accountId"
            }
        ]
    }
}
```

Query to list all EC2 volumes that are not in use

Abfrage:

```
SELECT
    resourceId,
    accountId,
```

```
    awsRegion,
    resourceType,
    configuration.volumeType,
    configuration.size,
    resourceCreationTime,
    tags,
    configuration.encrypted,
    configuration.availabilityZone,
    configuration.state.value
WHERE
    resourceType = 'AWS::EC2::Volume'
AND
    configuration.state.value = 'available'
```

Ergebnisse:


```
{
    "Results": [
        "{\"accountId\":\"accountId\",\"resourceId\":\"vol-0174de9c962f6581c\",
\"awsRegion\":\"us-west-2\",\"configuration\":{\"volumeType\":\"gp2\",\"encrypted
\":false,\"size\":100.0,\"state\":{\"value\":\"available\"},\"availabilityZone\":
\"us-west-2a\"},\"resourceCreationTime\":\"2020-02-21T07:39:43.771Z\",\"tags\":[],
\"resourceType\":\"AWS::EC2::Volume\"}",
        "{\"accountId\":\"accountId\",\"resourceId\":\"vol-0cbeb652a74af2f8f\",
\"awsRegion\":\"us-east-1\",\"configuration\":{\"volumeType\":\"gp2\",\"encrypted
\":false,\"size\":100.0,\"state\":{\"value\":\"available\"},\"availabilityZone\":
\"us-east-1a\"},\"resourceCreationTime\":\"2020-02-21T07:28:40.639Z\",\"tags\":[],
\"resourceType\":\"AWS::EC2::Volume\"}"
        "{\"accountId\":\"accountId\",\"resourceId\":\"vol-0a49952d528ec8ba2\",
\"awsRegion\":\"ap-south-1\",\"configuration\":{\"volumeType\":\"gp2\",\"encrypted
\":false,\"size\":100.0,\"state\":{\"value\":\"available\"},\"availabilityZone\":
\"ap-south-1a\"},\"resourceCreationTime\":\"2020-02-21T07:39:31.800Z\",\"tags\":[],
\"resourceType\":\"AWS::EC2::Volume\"}",
    ],
    "QueryInfo": {
        "SelectFields": [
            {
                "Name": "resourceId"
            },
            {
                "Name": "accountId"
            },
```

```
            {
                "Name": "awsRegion"
            },
            {
                "Name": "resourceType"
            },
            {
                "Name": "configuration.volumeType"
            },
            {
                "Name": "configuration.size"
            },
            {
                "Name": "resourceCreationTime"
            },
            {
                "Name": "tags"
            },
            {
                "Name": "configuration.encrypted"
            },
            {
                "Name": "configuration.availabilityZone"
            },
            {
                "Name": "configuration.state.value"
            }
        ]
    }
}
```

Beispiel für Beziehungsabfragen für AWS Config

Sehen Sie sich das folgende Beispiel für Beziehungsabfragen an.

Find EIPs related to an EC2 instance

```
SELECT
    resourceId
WHERE
    resourceType = 'AWS::EC2::EIP'
```

```
    AND relationships.resourceId = 'i-abcd1234'
```

Find EIPs related to an EC2 network interface

```
SELECT
    resourceId
WHERE
    resourceType = 'AWS::EC2::EIP'
    AND relationships.resourceId = 'eni-abcd1234'
```

Find EC2 instances and network interfaces related to a security group

```
SELECT
    resourceId
WHERE
    resourceType IN ('AWS::EC2::Instance', 'AWS::EC2::NetworkInterface')
    AND relationships.resourceId = 'sg-abcd1234'
```

ODER

```
SELECT
    resourceId
WHERE
    resourceType = 'AWS::EC2::Instance'
    AND relationships.resourceId = 'sg-abcd1234'

SELECT
    resourceId
WHERE
    resourceType = 'AWS::EC2::NetworkInterface'
    AND relationships.resourceId = 'sg-abcd1234'
```

Find EC2 instances, network ACLs, network interfaces and route tables related to a subnet

```
SELECT
    resourceId
WHERE
    resourceType IN ('AWS::EC2::Instance', 'AWS::EC2::NetworkACL',
 'AWS::EC2::NetworkInterface', 'AWS::EC2::RouteTable')
    AND relationships.resourceId = 'subnet-abcd1234'
```

Find EC2 instances, internet gateways, network ACLs, network interfaces, route tables, subnets and security groups related to a VPC

```
SELECT
    resourceId
WHERE
    resourceType IN ('AWS::EC2::Instance', 'AWS::EC2::InternetGateway',
 'AWS::EC2::NetworkACL', 'AWS::EC2::NetworkInterface', 'AWS::EC2::RouteTable',
 'AWS::EC2::Subnet', 'AWS::EC2::SecurityGroup')
    AND relationships.resourceId = 'vpc-abcd1234'
```

Find EC2 route tables related to a VPN gateway

```
SELECT
    resourceId
WHERE
    resourceType = 'AWS::EC2::RouteTable'
    AND relationships.resourceId = 'vgw-abcd1234'
```

Einschränkungen

> **Note**
>
> Advanced Query unterstützt nicht das Abfragen von Ressourcen, die nicht für die Aufzeichnung durch den Konfigurationsrekorder konfiguriert wurden. AWS Config erstellt Konfigurationselemente (CIs) mit`ResourceNotRecorded`, `configurationItemStatus` wenn eine Ressource erkannt wurde, aber nicht für die Aufzeichnung durch den Konfigurationsrekorder konfiguriert ist. Ein Aggregator aggregiert diese Daten CIs, aber erweiterte Abfragen unterstützen keine Abfragen CIs mit. `ResourceNotRecorded` Aktualisieren Sie Ihre Recorder-Einstellungen, um die Aufzeichnung der Ressourcentypen zu ermöglichen, die Sie abfragen möchten.

Als Teilbereich von SQL-`SELECT` weist die Abfragesyntax folgende Einschränkungen auf:

- Keine Unterstützung für die Schlüsselwörter `ALL`, `AS`, `DISTINCT`, `FROM`, `HAVING`, `JOIN` und `UNION` in einer Abfrage. Abfragen von `NULL`-Werten werden nicht unterstützt.

- Keine Unterstützung für komplexe `CASE` Anweisungen zur Erstellung eines Prioritätsfeldes direkt in der Abfrage.
- Keine Unterstützung für Abfragen von Ressourcen von Drittanbietern. Bei Ressourcen von Drittanbietern, die mit erweiterten Abfragen abgerufen wurden, ist das Konfigurationsfeld auf `NULL` festgelegt.
- Keine Unterstützung für verschachtelte Strukturen (wie Tags), die mit SQL-Abfragen entpackt werden.
- Keine Unterstützung für das Abfragen gelöschter Ressourcen. Informationen zum Auffinden gelöschter Ressourcen finden Sie unter Ressourcen suchen, die entdeckt wurden von AWS Config.
- Die Kurznotation „`SELECT` alle Spalten“ (d. h. `SELECT *`) wählt ausschließlich die obersten, skalaren Eigenschaften eines CI aus. Die zurückgegebenen skalaren Eigenschaften lauten `accountId`, `awsRegion`, `arn`, `availabilityZone`, `configurationItemCaptureTime`, `resourceCreationTime`, `resourceId`, `resourceName`, `resourceType` und `version`.
- Platzhalterbeschränkungen:
  - Platzhalter werden nur für Eigenschaftswerte und nicht für Eigenschaftsschlüssel unterstützt (z. B. wird `...WHERE someKey LIKE 'someValue%'` unterstützt, `...WHERE 'someKey%' LIKE 'someValue%'` jedoch nicht).
  - Unterstützt werden nur Suffixplatzhalter (z. B. werden `...LIKE 'AWS::EC2::%'` und `...LIKE 'AWS::EC2::_'` unterstützt, `...LIKE '%::EC2::Instance'` und `...LIKE '_::EC2::Instance'` jedoch nicht).
  - Platzhalterübereinstimmungen müssen aus mindestens drei Zeichen bestehen (z. B. sind `...LIKE 'ab%'` und `...LIKE 'ab_'` nicht zulässig, aber `...LIKE 'abc%'` und `...LIKE 'abc_'` sind zulässig).

> **Note**
>
> „`_`“ (einzelner Unterstrich) wird ebenfalls als Platzhalter behandelt.

- Aggregationsbeschränkungen:
  - Aggregationsfunktionen akzeptieren ausschließlich ein einziges Argument oder eine einzige Eingenschaft.
  - Aggregatfunktionen nehmen keine anderen Funktionen als Argumente an.
  - `GROUP BY` mit einer `ORDER BY`-Klausel, die auf Aggregatfunktionen verweist, darf nur eine einzige Eigenschaft enthalten.

- Für alle anderen Aggregationen können `GROUP BY`-Klauseln bis zu drei Eigenschaften enthalten.
- Die Paginierung wird für alle Aggregatabfragen unterstützt, es sei denn, die `ORDER BY`-Klausel hat eine Aggregatfunktion. `GROUP BY X, ORDER BY Y` funktioniert z. B. nicht, wenn Y eine Aggregatfunktion ist.
- Keine Unterstützung für `HAVING`-Klauseln in Aggregationen.

- Einschränkungen bei nicht übereinstimmenden Bezeichnern:

  Nicht übereinstimmende Bezeichner sind Eigenschaften, die dieselbe Schreibweise, aber unterschiedliche Groß- und Kleinschreibung aufweisen. Die erweiterte Abfrage unterstützt nicht die Verarbeitung von Abfragen, die nicht übereinstimmende Bezeichner enthalten. Zum Beispiel:

  - Zwei Eigenschaften mit exakt derselben Schreibweise, aber mit unterschiedlicher Groß- und Kleinschreibung (`configuration.dbclusterIdentifier` und `configuration.dBClusterIdentifier`).
  - Zwei Eigenschaften, bei denen eine Eigenschaft eine Teilmenge der anderen ist und die Groß- und Kleinschreibung (`configuration.ipAddress` und `configuration.ipaddressPermissions`) unterschiedlich ist.

Verhalten des notation/IP CIDR-Bereichs für erweiterte Abfragen

Die CIDR-Notation wird für die Suche in IP-Bereiche konvertiert.

Das bedeutet, dass mit `"="` und `"BETWEEN"` nach allen Bereichen gesucht wird, die die angegebene IP enthalten, nicht nach einem bestimmten Bereich.

Um nach einem exakten IP-Bereich zu suchen, müssen Sie zusätzliche Bedingungen für den Ausschluss IPs außerhalb des Bereichs hinzufügen.

Example Auf der Suche nach dem exakten CIDR-Block 10.0.0.0/24

```
SELECT * WHERE resourceType = 'AWS::EC2::SecurityGroup'
  AND configuration.ipPermissions.ipRanges BETWEEN '10.0.0.0'
  AND '10.0.0.255'
  AND NOT configuration.ipPermissions.ipRanges < '10.0.0.0'
  AND NOT configuration.ipPermissions.ipRanges > '10.0.0.255'
```

Example Auf der Suche nach der exakten IP-Adresse 192.168.0.2/32

```
SELECT * WHERE resourceType = 'AWS::EC2::SecurityGroup'
  AND configuration.ipPermissions.ipRanges = '192.168.0.2'
  AND NOT configuration.ipPermissions.ipRanges > '192.168.0.2'
  AND NOT configuration.ipPermissions.ipRanges < '192.168.0.2'
```

Verhalten mehrerer Eigenschaften innerhalb eines Arrays für erweiterte Abfragen

Bei der Abfrage mehrerer Eigenschaften innerhalb eines Arrays von Objekten werden Treffer für alle Array-Elemente berechnet.

Für eine Ressource R mit den Regeln A und B ist die Ressource beispielsweise konform mit Regel A, aber nicht konform mit Regel B. Die Ressource R wird wie folgt gespeichert:

```
{
    configRuleList: [
        {
            configRuleName: 'A', complianceType: 'compliant'
        },
        {
            configRuleName: 'B', complianceType: 'non_compliant'
        }
    ]
}
```

R wird von dieser Abfrage zurückgegeben:

```
SELECT configuration WHERE configuration.configRuleList.complianceType =
 'non_compliant'
AND configuration.configRuleList.configRuleName = 'A'
```

Die erste Bedingung `configuration.configRuleList.complianceType = 'non_compliant'` wird auf ALLE Elemente in R angewendet. configRuleList Da R eine Regel (Regel B) mit complianceType = 'non_compliant' hat, wird die Bedingung als wahr bewertet.

Die zweite Bedingung `configuration.configRuleList.configRuleName` wird auf ALLE Elemente in R configRuleList angewendet. Da R eine Regel (Regel A) mit configRuleName = 'A' hat, wird die Bedingung als wahr bewertet. Da beide Bedingungen „true“ sind, wird R zurückgegeben.

Unterstützung von Regionen

Erweiterte Abfragen werden in den folgenden Regionen unterstützt:

Name der Region	Region	Endpunkt	Protocol (Protokoll)
USA Ost (Ohio)	us-east-2	config.us-east-2.amazonaws.com	HTTPS
USA Ost (Nord-Virginia)	us-east-1	config.us-east-1.amazonaws.com	HTTPS
USA West (Nordkalifornien)	us-west-1	config.us-west-1.amazonaws.com	HTTPS
USA West (Oregon)	us-west-2	config.us-west-2.amazonaws.com	HTTPS
Afrika (Kapstadt)	af-south-1	config.af-south-1.amazonaws.com	HTTPS
Asien-Pazifik (Hongkong)	ap-east-1	config.ap-east-1.amazonaws.com	HTTPS
Asien-Pazifik	ap-south-2	config.ap-south-2.amazonaws.com	HTTPS

Name der Region	Region	Endpunkt	Protocol (Protokoll)
(Hyderabad)			
Asien-Pazifik (Jakarta)	ap-southeast-3	config.ap-southeast-3.amazonaws.com	HTTPS
Asien-Pazifik (Malaysia)	ap-southeast-5	config.ap-southeast-5.amazonaws.com	HTTPS
Asien-Pazifik (Melbourne)	ap-southeast-4	config.ap-southeast-4.amazonaws.com	HTTPS
Asien-Pazifik (Mumbai)	ap-south-1	config.ap-south-1.amazonaws.com	HTTPS
Asien-Pazifik (Osaka)	ap-northeast-3	config.ap-northeast-3.amazonaws.com	HTTPS
Asien-Pazifik (Seoul)	ap-northeast-2	config.ap-northeast-2.amazonaws.com	HTTPS
Asien-Pazifik (Singapur)	ap-southeast-1	config.ap-southeast-1.amazonaws.com	HTTPS

Name der Region	Region	Endpunkt	Protocol (Protokoll)
Asien-Pazifik (Sydney)	ap-southeast-2	config.ap-southeast-2.amazonaws.com	HTTPS
Asien-Pazifik (Taipeh)	ap-east-2	config.ap-east-2.amazonaws.com	HTTPS
Asien-Pazifik (Thailand)	ap-southeast-7	config.ap-southeast-7.amazonaws.com	HTTPS
Asien-Pazifik (Tokio)	ap-northeast-1	config.ap-northeast-1.amazonaws.com	HTTPS
Kanada (Zentral)	ca-central-1	config.ca-central-1.amazonaws.com	HTTPS
Kanada West (Calgary)	ca-west-1	config.ca-west-1.amazonaws.com	HTTPS
Europa (Frankfurt)	eu-central-1	config.eu-central-1.amazonaws.com	HTTPS
Europa (Irland)	eu-west-1	config.eu-west-1.amazonaws.com	HTTPS
Europa (London)	eu-west-2	config.eu-west-2.amazonaws.com	HTTPS

Name der Region	Region	Endpunkt	Protocol (Protokoll)
Europa (Mailand)	eu-south-1	config.eu-south-1.amazonaws.com	HTTPS
Europa (Paris)	eu-west-3	config.eu-west-3.amazonaws.com	HTTPS
Europa (Spanien)	eu-south-2	config.eu-south-2.amazonaws.com	HTTPS
Europa (Stockholm)	eu-north-1	config.eu-north-1.amazonaws.com	HTTPS
Europa (Zürich)	eu-central-2	config.eu-central-2.amazonaws.com	HTTPS
Israel (Tel Aviv)	il-central-1	config.il-central-1.amazonaws.com	HTTPS
Mexiko (Zentral)	mx-central-1	config.mx-central-1.amazonaws.com	HTTPS
Naher Osten (Bahrain)	me-south-1	config.me-south-1.amazonaws.com	HTTPS
Naher Osten (VAE)	me-central-1	config.me-central-1.amazonaws.com	HTTPS
Südamerika (São Paulo)	sa-east-1	config.sa-east-1.amazonaws.com	HTTPS

Name der Region	Region	Endpunkt	Protocol (Protokoll)
AWS GovCloud (US-Ost)	us-gov-east-1	config.us-gov-east-1.amazonaws.com	HTTPS
AWS GovCloud (US-West)	us-gov-west-1	config.us-gov-west-1.amazonaws.com	HTTPS

AWS Config Daten löschen

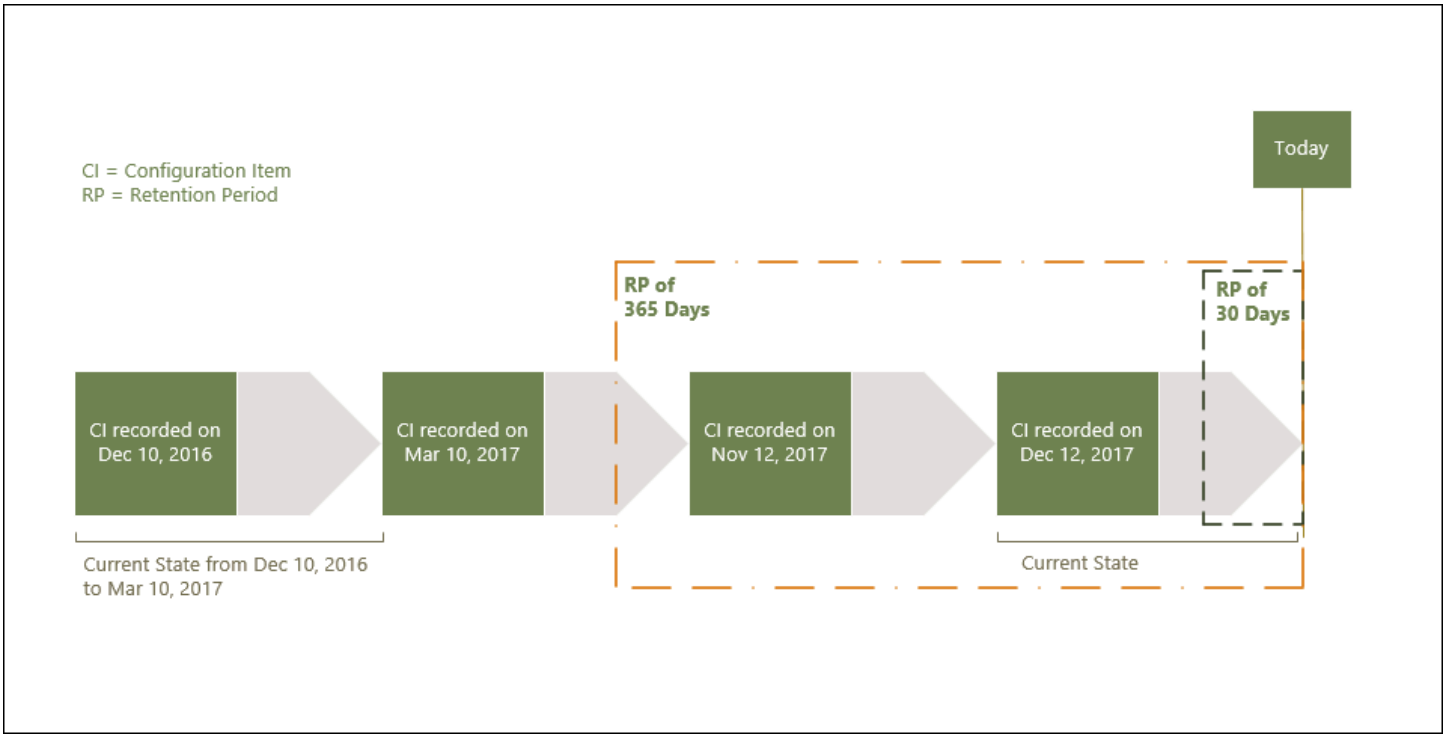
> **Note**
>
> AWS Config Nutzt Amazon Simple Storage Service (Amazon S3) und Amazon Simple Notification Service (Amazon SNS) zum Senden von Konfigurations-Snapshots und Konfigurationsverlaufsdateien, AWS Config verfügt über eigene Datenspeicher- und Aufbewahrungsrichtlinien. Die Informationen auf dieser Seite sind spezifisch für. AWS Config Amazon S3 und Amazon SNS haben ihre eigenen separaten Datenspeicher- und Aufbewahrungsrichtlinien.

AWS Config ermöglicht es Ihnen, Ihre Daten zu löschen, indem Sie eine Aufbewahrungsfrist für Ihre Daten angeben`ConfigurationItems`. Wenn Sie eine Aufbewahrungsfrist angeben, werden AWS Config Ihre Daten `ConfigurationItems` für diesen angegebenen Zeitraum aufbewahrt. Sie können einen Zeitraum zwischen mindestens 30 Tagen und maximal 7 Jahren (2557 Tage) wählen. AWS Config löscht Daten, die älter sind als die angegebene Aufbewahrungsfrist. Wenn Sie keinen Aufbewahrungszeitraum angeben, speichert AWS Config `ConfigurationItems` über den Standardzeitraum von 7 Jahren (2 557 Tage). Wenn die Aufzeichnung aktiviert ist, ist der aktuelle Status einer Ressource, wenn ein `ConfigurationItem` aufgezeichnet wird und bis die nächste Änderung (ein neuer `ConfigurationItem`) aufgezeichnet wird.

Um die Funktionsweise des Aufbewahrungszeitraums zu verstehen, sehen wir uns einmal die Zeitleiste an.

- Wenn die Aufzeichnung aktiviert ist, ist der aktuelle Status einer Ressource immer vorhanden und kann nicht gelöscht werden (unabhängig vom Datum, an dem das `ConfigurationItem` aufgezeichnet wird).
- Wenn AWS Config Datensätze neu `ConfigurationItems` sind`ConfigurationItems`, werden die vorherigen je nach dem angegebenen Aufbewahrungszeitraum gelöscht.

In der folgenden Zeitleiste werden AWS Config Datensätze `ConfigurationItems` zu den folgenden Terminen angezeigt. In dieser Zeitleiste ist der 24. Mai 2018 der aktuelle Tag.



In der folgenden Tabelle wird erläutert, welche `ConfigurationItems` auf Grundlage des ausgewählten Aufbewahrungszeitraums in der AWS Config -Zeitleiste angezeigt werden.

Aufbewahrungszeitraum	In der Zeitleiste angezeigte Konfigurationselemente	Erklärung
30 Tage	12. Dezember 2017	Der aktuelle Status der Ressource begann am 12. Dezember 2017, als das `ConfigurationItem` aufgezeichnet wurde, und ist bis heute (24. Mai 2018) gültig. Wenn die Aufzeichnung aktiviert ist, ist der aktuelle Status immer vorhanden.
365 Tage	12. Dezember 2017; 12. November 2017 und 10. März 2017	Für den Aufbewahrungszeitraum werden der aktuelle Status (12. Dezember 2017) und die vorherigen `ConfigurationItems` (12. November 2017 und 10. März 2017) angezeigt.

Aufbewahrungszeitraum	In der Zeitleiste angezeigte Konfigurationselemente	Erklärung
		Das `ConfigurationItem` für den 10. März 2017 wird in der Zeitleiste angezeigt, weil dieser Konfigurationsstatus den aktuellen Status vor 365 Tagen widerspiegelte.

Nachdem Sie eine Aufbewahrungsfrist angegeben haben, dürfen Sie AWS Config APIs keine Rücksendungen mehr vornehmen, `ConfigurationItems` die einen Staat repräsentieren, der älter als der angegebene Aufbewahrungszeitraum ist.

> **Note**
>
> - AWS Config kann Ihre nicht aufnehmen`ConfigurationItems`, wenn die Aufnahme ausgeschaltet ist.
> - AWS Config kann Ihren nicht aufzeichnen`ConfigurationItems`, wenn Ihre IAM-Rolle nicht über ausreichende Berechtigungen verfügt. Weitere Informationen finden Sie unter Berechtigungen für die zugewiesene IAM-Rolle. AWS Config

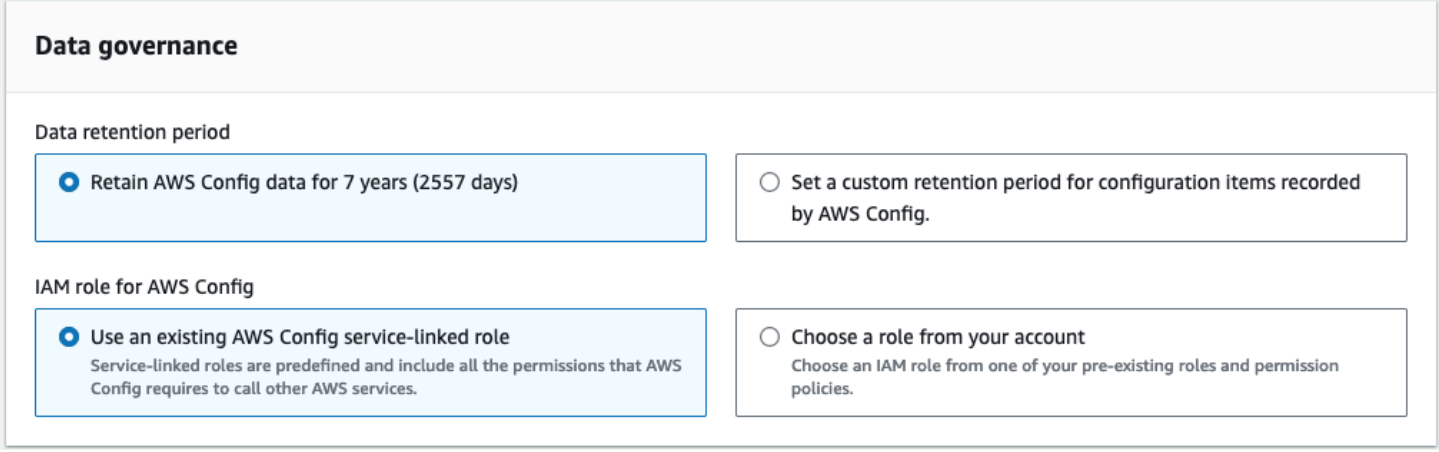
Einstellen der Aufbewahrungsfrist für Daten in AWS Management Console

Wenn Sie keinen Datenaufbewahrungszeitraum auswählen, beträgt der Standardzeitraum 7 Jahre oder 2557 Tage. AWS Management Console

Aktivieren Sie das Kontrollkästchen, um einen benutzerdefinierten Aufbewahrungszeitraum für Konfigurationselemente festzulegen. Sie können 1, 3 oder 5 Jahre bzw. einen benutzerdefinierten Zeitraum auswählen. Geben Sie für einen benutzerdefinierten Zeitraum zwischen 30 und 2.557 Tage an.

Das folgende Bild zeigt, wo Sie die Datenaufbewahrungsdauer in Data Governance festlegen können. Sie können von der AWS Config Konsole auf der Seite „Einstellungen bearbeiten“ auf Data

Governance zugreifen, indem Sie in der linken Navigationsleiste Einstellungen und dann Bearbeiten auswählen.



Sicherheit in AWS Config

Cloud-Sicherheit AWS hat höchste Priorität. Als AWS Kunde profitieren Sie von Rechenzentren und Netzwerkarchitekturen, die darauf ausgelegt sind, die Anforderungen der sicherheitssensibelsten Unternehmen zu erfüllen.

Sicherheit ist eine gemeinsame AWS Verantwortung von Ihnen und Ihnen. Das Modell der geteilten Verantwortung beschreibt dies als Sicherheit der Cloud selbst und Sicherheit in der Cloud:

- Sicherheit der Cloud — AWS ist verantwortlich für den Schutz der Infrastruktur, die AWS Dienste in der AWS Cloud ausführt. AWS bietet Ihnen auch Dienste, die Sie sicher nutzen können. Externe Prüfer testen und verifizieren regelmäßig die Wirksamkeit unserer Sicherheitsmaßnahmen im Rahmen der AWS . Weitere Informationen zu den Compliance-Programmen, die für gelten AWS Config, finden Sie unter AWS Services im Bereich nach Compliance-Programmen und .
- Sicherheit in der Cloud — Ihre Verantwortung richtet sich nach dem AWS Dienst, den Sie nutzen. Sie sind auch für andere Faktoren verantwortlich, etwa für die Vertraulichkeit Ihrer Daten, für die Anforderungen Ihres Unternehmens und für die geltenden Gesetze und Vorschriften.

Diese Dokumentation hilft Ihnen zu verstehen, wie Sie das Modell der gemeinsamen Verantwortung bei der Nutzung anwenden können AWS Config. In den folgenden Themen erfahren Sie, wie Sie die Konfiguration vornehmen AWS Config , um Ihre Sicherheits- und Compliance-Ziele zu erreichen.

Themen

- Datenschutz in AWS Config
- Identity and Access Management für AWS Config
- Reaktion auf Vorfälle in AWS Config
- Überprüfung der Einhaltung von Vorschriften für AWS Config
- Resilienz in AWS Config
- Sicherheit der Infrastruktur in AWS Config
- Serviceübergreifende Confused-Deputy-Prävention
- Bewährte Sicherheitsmethoden für AWS Config

Datenschutz in AWS Config

Das Modell der AWS gemeinsamen Verantwortung der , gilt für den Datenschutz in AWS Config. Wie in diesem Modell beschrieben, AWS ist verantwortlich für den Schutz der globalen Infrastruktur, auf der alle Systeme laufen AWS Cloud. Sie sind dafür verantwortlich, die Kontrolle über Ihre in dieser Infrastruktur gehosteten Inhalte zu behalten. Sie sind auch für die Sicherheitskonfiguration und die Verwaltungsaufgaben für die von Ihnen verwendeten AWS-Services verantwortlich. Weitere Informationen zum Datenschutz finden Sie unter Häufig gestellte Fragen zum Datenschutz. Informationen zum Datenschutz in Europa finden Sie im Blog-Beitrag AWS -Modell der geteilten Verantwortung und in der DSGVO im AWS -Sicherheitsblog.

Aus Datenschutzgründen empfehlen wir, dass Sie AWS-Konto Anmeldeinformationen schützen und einzelne Benutzer mit AWS IAM Identity Center oder AWS Identity and Access Management (IAM) einrichten. So erhält jeder Benutzer nur die Berechtigungen, die zum Durchführen seiner Aufgaben erforderlich sind. Außerdem empfehlen wir, die Daten mit folgenden Methoden schützen:

- Verwenden Sie für jedes Konto die Multi-Faktor-Authentifizierung (MFA).
- Wird verwendet SSL/TLS , um mit AWS Ressourcen zu kommunizieren. Wir benötigen TLS 1.2 und empfehlen TLS 1.3.
- Richten Sie die API und die Protokollierung von Benutzeraktivitäten mit ein AWS CloudTrail. Informationen zur Verwendung von CloudTrail Pfaden zur Erfassung von AWS Aktivitäten finden Sie unter Arbeiten mit CloudTrail Pfaden im AWS CloudTrail Benutzerhandbuch.
- Verwenden Sie AWS Verschlüsselungslösungen zusammen mit allen darin enthaltenen Standardsicherheitskontrollen AWS-Services.
- Verwenden Sie erweiterte verwaltete Sicherheitsservices wie Amazon Macie, die dabei helfen, in Amazon S3 gespeicherte persönliche Daten zu erkennen und zu schützen.
- Wenn Sie für den Zugriff AWS über eine Befehlszeilenschnittstelle oder eine API FIPS 140-3-validierte kryptografische Module benötigen, verwenden Sie einen FIPS-Endpunkt. Weitere Informationen über verfügbare FIPS-Endpunkte finden Sie unter Federal Information Processing Standard (FIPS) 140-3.

Wir empfehlen dringend, in Freitextfeldern, z. B. im Feld Name, keine vertraulichen oder sensiblen Informationen wie die E-Mail-Adressen Ihrer Kunden einzugeben. Dies gilt auch, wenn Sie mit AWS Config oder anderen AWS-Services über die Konsole AWS CLI, API oder arbeiten AWS SDKs. Alle Daten, die Sie in Tags oder Freitextfelder eingeben, die für Namen verwendet werden, können für Abrechnungs- oder Diagnoseprotokolle verwendet werden. Wenn Sie eine URL für einen externen

Server bereitstellen, empfehlen wir dringend, keine Anmeldeinformationen zur Validierung Ihrer Anforderung an den betreffenden Server in die URL einzuschließen.

Verschlüsselung gespeicherter Daten

Daten werden im Ruhezustand mittels transparenter serverseitiger Verschlüsselung verschlüsselt. Dieser Service reduziert den Ausführungsaufwand und die Komplexität, die mit dem Schutz sensibler Daten verbunden sind. Mit der Verschlüsselung von Daten im Ruhezustand können Sie sicherheitsrelevante Anwendungen erstellen, die Verschlüsselungsvorschriften und gesetzliche Bestimmungen einhalten.

Verschlüsseln von Daten während der Übertragung.

Daten, die gesammelt und abgerufen werden, erfolgen ausschließlich über einen durch AWS Config Transport Layer Security (TLS) geschützten Kanal.

Identity and Access Management für AWS Config

AWS Identity and Access Management (IAM) hilft einem Administrator AWS-Service , den Zugriff auf AWS Ressourcen sicher zu kontrollieren. IAM-Administratoren kontrollieren, wer authentifiziert (angemeldet) und autorisiert werden kann (über Berechtigungen verfügt), um Ressourcen zu verwenden. AWS Config IAM ist ein Programm AWS-Service , das Sie ohne zusätzliche Kosten nutzen können.

Themen

- Zielgruppe
- Authentifizierung mit Identitäten
- Verwalten des Zugriffs mit Richtlinien
- Wie AWS Config funktioniert mit IAM
- Beispiele für identitätsbasierte Richtlinien für AWS Config
- AWS verwaltete Richtlinien für AWS Config
- Berechtigungen für die IAM-Rolle wurden zugewiesen AWS Config
- Aktualisierung der IAM-Rolle für den vom Kunden verwalteten Konfigurationsrekorder
- Berechtigungen für den Amazon S3 S3-Bucket für den AWS Config Lieferkanal
- Berechtigungen für den KMS-Schlüssel für den AWS Config Delivery Channel
- Berechtigungen für das Amazon-SNS-Thema

- Fehlerbehebung bei AWS Config Identität und Zugriff
- Verwenden von serviceverknüpften Rollen für AWS Config

Zielgruppe

Die Art und Weise, wie Sie AWS Identity and Access Management (IAM) verwenden, hängt von der Arbeit ab, in der Sie tätig sind. AWS Config

Dienstbenutzer — Wenn Sie den AWS Config Dienst für Ihre Arbeit verwenden, stellt Ihnen Ihr Administrator die erforderlichen Anmeldeinformationen und Berechtigungen zur Verfügung. Wenn Sie für Ihre Arbeit mehr AWS Config Funktionen verwenden, benötigen Sie möglicherweise zusätzliche Berechtigungen. Wenn Sie die Funktionsweise der Zugriffskontrolle nachvollziehen, wissen Sie bereits, welche Berechtigungen Sie von Ihrem Administrator anfordern müssen. Unter Fehlerbehebung bei AWS Config Identität und Zugriff finden Sie nützliche Informationen für den Fall, dass Sie keinen Zugriff auf eine Feature in AWS Config haben.

Serviceadministrator — Wenn Sie in Ihrem Unternehmen für die AWS Config Ressourcen verantwortlich sind, haben Sie wahrscheinlich vollen Zugriff auf AWS Config. Es ist Ihre Aufgabe, zu bestimmen, auf welche AWS Config Funktionen und Ressourcen Ihre Servicebenutzer zugreifen sollen. Anschließend müssen Sie Anforderungen an Ihren IAM-Administrator senden, um die Berechtigungen der Servicebenutzer zu ändern. Lesen Sie die Informationen auf dieser Seite, um die Grundkonzepte von IAM nachzuvollziehen. Weitere Informationen darüber, wie Ihr Unternehmen IAM nutzen kann AWS Config, finden Sie unterWie AWS Config funktioniert mit IAM.

IAM-Administrator: Wenn Sie als IAM-Administrator fungieren, sollten Sie Einzelheiten dazu kennen, wie Sie Richtlinien zur Verwaltung des Zugriffs auf AWS Config verfassen können. Beispiele für AWS Config identitätsbasierte Richtlinien, die Sie in IAM verwenden können, finden Sie unter. Beispiele für identitätsbasierte Richtlinien für AWS Config

Authentifizierung mit Identitäten

Authentifizierung ist die Art und Weise, wie Sie sich AWS mit Ihren Identitätsdaten anmelden. Sie müssen als IAM-Benutzer authentifiziert (angemeldet AWS) sein oder eine IAM-Rolle annehmen. Root-Benutzer des AWS-Kontos

Sie können sich AWS als föderierte Identität anmelden, indem Sie Anmeldeinformationen verwenden, die über eine Identitätsquelle bereitgestellt wurden. AWS IAM Identity Center (IAM Identity Center) -Benutzer, die Single Sign-On-Authentifizierung Ihres Unternehmens und Ihre Google- oder Facebook-Anmeldeinformationen sind Beispiele für föderierte Identitäten. Wenn Sie

sich als Verbundidentität anmelden, hat der Administrator vorher mithilfe von IAM-Rollen einen Identitätsverbund eingerichtet. Wenn Sie über den Verbund darauf zugreifen AWS , übernehmen Sie indirekt eine Rolle.

Je nachdem, welcher Benutzertyp Sie sind, können Sie sich beim AWS Management Console oder beim AWS Zugangsportal anmelden. Weitere Informationen zur Anmeldung finden Sie AWS unter So melden Sie sich bei Ihrem an AWS-Konto im AWS-Anmeldung Benutzerhandbuch.

Wenn Sie AWS programmgesteuert darauf zugreifen, AWS stellt es ein Software Development Kit (SDK) und eine Befehlszeilenschnittstelle (CLI) bereit, mit denen Sie Ihre Anfragen mithilfe Ihrer Anmeldeinformationen kryptografisch signieren können. Wenn Sie keine AWS Tools verwenden, müssen Sie Anfragen selbst signieren. Weitere Informationen zur Verwendung der empfohlenen Methode für die Selbstsignierung von Anforderungen finden Sie unter AWS Signature Version 4 für API-Anforderungen im IAM-Benutzerhandbuch.

Unabhängig von der verwendeten Authentifizierungsmethode müssen Sie möglicherweise zusätzliche Sicherheitsinformationen bereitstellen. AWS Empfiehlt beispielsweise, die Multi-Faktor-Authentifizierung (MFA) zu verwenden, um die Sicherheit Ihres Kontos zu erhöhen. Weitere Informationen finden Sie unter Multi-Faktor-Authentifizierung im AWS IAM Identity Center - Benutzerhandbuch und AWS Multi-Faktor-Authentifizierung (MFA) in IAM im IAM-Benutzerhandbuch.

AWS-Konto Root-Benutzer

Wenn Sie einen erstellen AWS-Konto, beginnen Sie mit einer Anmeldeidentität, die vollständigen Zugriff auf alle AWS-Services Ressourcen im Konto hat. Diese Identität wird als AWS-Konto Root-Benutzer bezeichnet. Sie können darauf zugreifen, indem Sie sich mit der E-Mail-Adresse und dem Passwort anmelden, mit denen Sie das Konto erstellt haben. Wir raten ausdrücklich davon ab, den Root-Benutzer für Alltagsaufgaben zu verwenden. Schützen Sie Ihre Root-Benutzer-Anmeldeinformationen. Verwenden Sie diese nur, um die Aufgaben auszuführen, die nur der Root-Benutzer ausführen kann. Eine vollständige Liste der Aufgaben, für die Sie sich als Root-Benutzer anmelden müssen, finden Sie unter Aufgaben, die Root-Benutzer-Anmeldeinformationen erfordern im IAM-Benutzerhandbuch.

Verbundidentität

Als bewährte Methode sollten menschliche Benutzer, einschließlich Benutzer, die Administratorzugriff benötigen, für den Zugriff AWS-Services mithilfe temporärer Anmeldeinformationen den Verbund mit einem Identitätsanbieter verwenden.

Eine föderierte Identität ist ein Benutzer aus Ihrem Unternehmensbenutzerverzeichnis, einem Web-Identitätsanbieter AWS Directory Service, dem Identity Center-Verzeichnis oder einem beliebigen Benutzer, der mithilfe AWS-Services von Anmeldeinformationen zugreift, die über eine Identitätsquelle bereitgestellt wurden. Wenn föderierte Identitäten darauf zugreifen AWS-Konten, übernehmen sie Rollen, und die Rollen stellen temporäre Anmeldeinformationen bereit.

Für die zentrale Zugriffsverwaltung empfehlen wir Ihnen, AWS IAM Identity Center zu verwenden. Sie können Benutzer und Gruppen in IAM Identity Center erstellen, oder Sie können eine Verbindung zu einer Gruppe von Benutzern und Gruppen in Ihrer eigenen Identitätsquelle herstellen und diese synchronisieren, um sie in all Ihren AWS-Konten Anwendungen zu verwenden. Informationen zu IAM Identity Center finden Sie unter Was ist IAM Identity Center? im AWS IAM Identity Center - Benutzerhandbuch.

IAM-Benutzer und -Gruppen

Ein IAM-Benutzer ist eine Identität innerhalb Ihres Unternehmens AWS-Konto , die über spezifische Berechtigungen für eine einzelne Person oder Anwendung verfügt. Wenn möglich, empfehlen wir, temporäre Anmeldeinformationen zu verwenden, anstatt IAM-Benutzer zu erstellen, die langfristige Anmeldeinformationen wie Passwörter und Zugriffsschlüssel haben. Bei speziellen Anwendungsfällen, die langfristige Anmeldeinformationen mit IAM-Benutzern erfordern, empfehlen wir jedoch, die Zugriffsschlüssel zu rotieren. Weitere Informationen finden Sie unter Regelmäßiges Rotieren von Zugriffsschlüsseln für Anwendungsfälle, die langfristige Anmeldeinformationen erfordern im IAM-Benutzerhandbuch.

Eine IAM-Gruppe ist eine Identität, die eine Sammlung von IAM-Benutzern angibt. Sie können sich nicht als Gruppe anmelden. Mithilfe von Gruppen können Sie Berechtigungen für mehrere Benutzer gleichzeitig angeben. Gruppen vereinfachen die Verwaltung von Berechtigungen, wenn es zahlreiche Benutzer gibt. Sie könnten beispielsweise eine Gruppe benennen IAMAdminsund dieser Gruppe Berechtigungen zur Verwaltung von IAM-Ressourcen erteilen.

Benutzer unterscheiden sich von Rollen. Ein Benutzer ist einer einzigen Person oder Anwendung eindeutig zugeordnet. Eine Rolle kann von allen Personen angenommen werden, die sie benötigen. Benutzer besitzen dauerhafte Anmeldeinformationen. Rollen stellen temporäre Anmeldeinformationen bereit. Weitere Informationen finden Sie unter Anwendungsfälle für IAM-Benutzer im IAM-Benutzerhandbuch.

IAM-Rollen

Eine IAM-Rolle ist eine Identität innerhalb von Ihnen AWS-Konto , die über bestimmte Berechtigungen verfügt. Sie ist einem IAM-Benutzer vergleichbar, jedoch nicht mit einer bestimmten Person verknüpft. Um vorübergehend eine IAM-Rolle in der zu übernehmen AWS Management Console, können Sie von einer Benutzer- zu einer IAM-Rolle (Konsole) wechseln. Sie können eine Rolle übernehmen, indem Sie eine AWS CLI oder AWS API-Operation aufrufen oder eine benutzerdefinierte URL verwenden. Weitere Informationen zu Methoden für die Verwendung von Rollen finden Sie unter Methoden für die Übernahme einer Rolle im IAM-Benutzerhandbuch.

IAM-Rollen mit temporären Anmeldeinformationen sind in folgenden Situationen hilfreich:

- Verbundbenutzerzugriff – Um einer Verbundidentität Berechtigungen zuzuweisen, erstellen Sie eine Rolle und definieren Berechtigungen für die Rolle. Wird eine Verbundidentität authentifiziert, so wird die Identität der Rolle zugeordnet und erhält die von der Rolle definierten Berechtigungen. Informationen zu Rollen für den Verbund finden Sie unter Erstellen von Rollen für externe Identitätsanbieter (Verbund) im IAM-Benutzerhandbuch. Wenn Sie IAM Identity Center verwenden, konfigurieren Sie einen Berechtigungssatz. Wenn Sie steuern möchten, worauf Ihre Identitäten nach der Authentifizierung zugreifen können, korreliert IAM Identity Center den Berechtigungssatz mit einer Rolle in IAM. Informationen zu Berechtigungssätzen finden Sie unter Berechtigungssätze im AWS IAM Identity Center -Benutzerhandbuch.
- Temporäre IAM-Benutzerberechtigungen – Ein IAM-Benutzer oder eine -Rolle kann eine IAM-Rolle übernehmen, um vorübergehend andere Berechtigungen für eine bestimmte Aufgabe zu erhalten.
- Kontoübergreifender Zugriff – Sie können eine IAM-Rolle verwenden, um einem vertrauenswürdigen Prinzipal in einem anderen Konto den Zugriff auf Ressourcen in Ihrem Konto zu ermöglichen. Rollen stellen die primäre Möglichkeit dar, um kontoübergreifendem Zugriff zu gewähren. Bei einigen können Sie AWS-Services jedoch eine Richtlinie direkt an eine Ressource anhängen (anstatt eine Rolle als Proxy zu verwenden). Informationen zu den Unterschieden zwischen Rollen und ressourcenbasierten Richtlinien für den kontoübergreifenden Zugriff finden Sie unter Kontoübergreifender Ressourcenzugriff in IAM im IAM-Benutzerhandbuch.
- Serviceübergreifender Zugriff — Einige AWS-Services verwenden Funktionen in anderen AWS-Services. Wenn Sie beispielsweise einen Service aufrufen, ist es üblich, dass dieser Service Anwendungen in Amazon ausführt EC2 oder Objekte in Amazon S3 speichert. Ein Dienst kann dies mit den Berechtigungen des aufrufenden Prinzipals mit einer Servicerolle oder mit einer serviceverknüpften Rolle tun.
  - Forward Access Sessions (FAS) — Wenn Sie einen IAM-Benutzer oder eine IAM-Rolle verwenden, um Aktionen auszuführen AWS, gelten Sie als Principal. Bei einigen Services

könnte es Aktionen geben, die dann eine andere Aktion in einem anderen Service initiieren. FAS verwendet die Berechtigungen des Prinzipals, der einen aufruft AWS-Service, in Kombination mit der Anfrage, Anfragen an AWS-Service nachgelagerte Dienste zu stellen. FAS-Anfragen werden nur gestellt, wenn ein Dienst eine Anfrage erhält, für deren Abschluss Interaktionen mit anderen AWS-Services oder Ressourcen erforderlich sind. In diesem Fall müssen Sie über Berechtigungen zum Ausführen beider Aktionen verfügen. Einzelheiten zu den Richtlinien für FAS-Anfragen finden Sie unter Zugriffssitzungen weiterleiten.

- Servicerolle – Eine Servicerolle ist eine IAM-Rolle, die ein Service übernimmt, um Aktionen in Ihrem Namen auszuführen. Ein IAM-Administrator kann eine Servicerolle innerhalb von IAM erstellen, ändern und löschen. Weitere Informationen finden Sie unter Erstellen einer Rolle zum Delegieren von Berechtigungen an einen AWS-Service im IAM-Benutzerhandbuch.
- Dienstbezogene Rolle — Eine dienstbezogene Rolle ist eine Art von Servicerolle, die mit einer verknüpft ist. AWS-Service Der Service kann die Rolle übernehmen, um eine Aktion in Ihrem Namen auszuführen. Servicebezogene Rollen erscheinen in Ihrem Dienst AWS-Konto und gehören dem Dienst. Ein IAM-Administrator kann die Berechtigungen für Service-verknüpfte Rollen anzeigen, aber nicht bearbeiten.

- Auf Amazon ausgeführte Anwendungen EC2 — Sie können eine IAM-Rolle verwenden, um temporäre Anmeldeinformationen für Anwendungen zu verwalten, die auf einer EC2 Instance ausgeführt werden und AWS API-Anfragen stellen AWS CLI . Dies ist dem Speichern von Zugriffsschlüsseln innerhalb der EC2 Instance vorzuziehen. Um einer EC2 Instanz eine AWS Rolle zuzuweisen und sie allen ihren Anwendungen zur Verfügung zu stellen, erstellen Sie ein Instanzprofil, das an die Instanz angehängt ist. Ein Instanzprofil enthält die Rolle und ermöglicht Programmen, die auf der EC2 Instanz ausgeführt werden, temporäre Anmeldeinformationen abzurufen. Weitere Informationen finden Sie im IAM-Benutzerhandbuch unter Verwenden einer IAM-Rolle, um Berechtigungen für Anwendungen zu gewähren, die auf EC2 Amazon-Instances ausgeführt werden.

Verwalten des Zugriffs mit Richtlinien

Sie kontrollieren den Zugriff, AWS indem Sie Richtlinien erstellen und diese an AWS Identitäten oder Ressourcen anhängen. Eine Richtlinie ist ein Objekt, AWS das, wenn es einer Identität oder Ressource zugeordnet ist, deren Berechtigungen definiert. AWS wertet diese Richtlinien aus, wenn ein Prinzipal (Benutzer, Root-Benutzer oder Rollensitzung) eine Anfrage stellt. Die Berechtigungen in den Richtlinien legen fest, ob eine Anforderung zugelassen oder abgelehnt wird. Die meisten Richtlinien werden AWS als JSON-Dokumente gespeichert. Weitere Informationen zu Struktur und

Inhalten von JSON-Richtliniendokumenten finden Sie unter Übersicht über JSON-Richtlinien im IAM-Benutzerhandbuch.

Administratoren können mithilfe von AWS JSON-Richtlinien angeben, wer auf was Zugriff hat. Das heißt, welcher Prinzipal Aktionen für welche Ressourcen und unter welchen Bedingungen ausführen kann.

Standardmäßig haben Benutzer, Gruppen und Rollen keine Berechtigungen. Ein IAM-Administrator muss IAM-Richtlinien erstellen, die Benutzern die Berechtigung erteilen, Aktionen für die Ressourcen auszuführen, die sie benötigen. Der Administrator kann dann die IAM-Richtlinien zu Rollen hinzufügen, und Benutzer können die Rollen annehmen.

IAM-Richtlinien definieren Berechtigungen für eine Aktion unabhängig von der Methode, die Sie zur Ausführung der Aktion verwenden. Angenommen, es gibt eine Richtlinie, die Berechtigungen für die `iam:GetRole`-Aktion erteilt. Ein Benutzer mit dieser Richtlinie kann Rolleninformationen von der AWS Management Console AWS CLI, der oder der AWS API abrufen.

Identitätsbasierte Richtlinien

Identitätsbasierte Richtlinien sind JSON-Berechtigungsrichtliniendokumente, die Sie einer Identität anfügen können, wie z. B. IAM-Benutzern, -Benutzergruppen oder -Rollen. Diese Richtlinien steuern, welche Aktionen die Benutzer und Rollen für welche Ressourcen und unter welchen Bedingungen ausführen können. Informationen zum Erstellen identitätsbasierter Richtlinien finden Sie unter Definieren benutzerdefinierter IAM-Berechtigungen mit vom Kunden verwalteten Richtlinien im IAM-Benutzerhandbuch.

Identitätsbasierte Richtlinien können weiter als Inline-Richtlinien oder verwaltete Richtlinien kategorisiert werden. Inline-Richtlinien sind direkt in einen einzelnen Benutzer, eine einzelne Gruppe oder eine einzelne Rolle eingebettet. Verwaltete Richtlinien sind eigenständige Richtlinien, die Sie mehreren Benutzern, Gruppen und Rollen in Ihrem System zuordnen können AWS-Konto. Zu den verwalteten Richtlinien gehören AWS verwaltete Richtlinien und vom Kunden verwaltete Richtlinien. Informationen dazu, wie Sie zwischen einer verwalteten Richtlinie und einer Inline-Richtlinie wählen, finden Sie unter Auswählen zwischen verwalteten und eingebundenen Richtlinien im IAM-Benutzerhandbuch.

Ressourcenbasierte Richtlinien

Ressourcenbasierte Richtlinien sind JSON-Richtliniendokumente, die Sie an eine Ressource anfügen. Beispiele für ressourcenbasierte Richtlinien sind IAM-Rollen-Vertrauensrichtlinien und

Amazon-S3-Bucket-Richtlinien. In Services, die ressourcenbasierte Richtlinien unterstützen, können Service-Administratoren sie verwenden, um den Zugriff auf eine bestimmte Ressource zu steuern. Für die Ressource, an welche die Richtlinie angehängt ist, legt die Richtlinie fest, welche Aktionen ein bestimmter Prinzipal unter welchen Bedingungen für diese Ressource ausführen kann. Sie müssen in einer ressourcenbasierten Richtlinie einen Prinzipal angeben. Zu den Prinzipalen können Konten, Benutzer, Rollen, Verbundbenutzer oder gehören. AWS-Services

Ressourcenbasierte Richtlinien sind Richtlinien innerhalb dieses Diensts. Sie können AWS verwaltete Richtlinien von IAM nicht in einer ressourcenbasierten Richtlinie verwenden.

Zugriffskontrolllisten () ACLs

Zugriffskontrolllisten (ACLs) steuern, welche Principals (Kontomitglieder, Benutzer oder Rollen) über Zugriffsberechtigungen für eine Ressource verfügen. ACLs ähneln ressourcenbasierten Richtlinien, verwenden jedoch nicht das JSON-Richtliniendokumentformat.

Amazon S3 und Amazon VPC sind Beispiele für Dienste, die Unterstützung ACLs bieten. AWS WAF Weitere Informationen finden Sie unter Übersicht über ACLs die Zugriffskontrollliste (ACL) im Amazon Simple Storage Service Developer Guide.

Weitere Richtlinientypen

AWS unterstützt zusätzliche, weniger verbreitete Richtlinientypen. Diese Richtlinientypen können die maximalen Berechtigungen festlegen, die Ihnen von den häufiger verwendeten Richtlinientypen erteilt werden können.

- Berechtigungsgrenzen – Eine Berechtigungsgrenze ist ein erweitertes Feature, mit der Sie die maximalen Berechtigungen festlegen können, die eine identitätsbasierte Richtlinie einer IAM-Entität (IAM-Benutzer oder -Rolle) erteilen kann. Sie können eine Berechtigungsgrenze für eine Entität festlegen. Die daraus resultierenden Berechtigungen sind der Schnittpunkt der identitätsbasierten Richtlinien einer Entität und ihrer Berechtigungsgrenzen. Ressourcenbasierte Richtlinien, die den Benutzer oder die Rolle im Feld `Principal` angeben, werden nicht durch Berechtigungsgrenzen eingeschränkt. Eine explizite Zugriffsverweigerung in einer dieser Richtlinien setzt eine Zugriffserlaubnis außer Kraft. Weitere Informationen über Berechtigungsgrenzen finden Sie unter Berechtigungsgrenzen für IAM-Entitäten im IAM-Benutzerhandbuch.
- Dienststeuerungsrichtlinien (SCPs) — SCPs sind JSON-Richtlinien, die die maximalen Berechtigungen für eine Organisation oder Organisationseinheit (OU) in festlegen. AWS Organizations AWS Organizations ist ein Dienst zur Gruppierung und zentralen Verwaltung

mehrerer Objekte AWS-Konten , die Ihrem Unternehmen gehören. Wenn Sie alle Funktionen in einer Organisation aktivieren, können Sie Richtlinien zur Servicesteuerung (SCPs) auf einige oder alle Ihre Konten anwenden. Das SCP schränkt die Berechtigungen für Entitäten in Mitgliedskonten ein, einschließlich der einzelnen Root-Benutzer des AWS-Kontos Entitäten. Weitere Informationen zu Organizations und SCPs finden Sie unter Richtlinien zur Servicesteuerung im AWS Organizations Benutzerhandbuch.

- Ressourcenkontrollrichtlinien (RCPs) — RCPs sind JSON-Richtlinien, mit denen Sie die maximal verfügbaren Berechtigungen für Ressourcen in Ihren Konten festlegen können, ohne die IAM-Richtlinien aktualisieren zu müssen, die jeder Ressource zugeordnet sind, deren Eigentümer Sie sind. Das RCP schränkt die Berechtigungen für Ressourcen in Mitgliedskonten ein und kann sich auf die effektiven Berechtigungen für Identitäten auswirken, einschließlich der Root-Benutzer des AWS-Kontos, unabhängig davon, ob sie zu Ihrer Organisation gehören. Weitere Informationen zu Organizations RCPs, einschließlich einer Liste AWS-Services dieser Support-Leistungen RCPs, finden Sie unter Resource Control Policies (RCPs) im AWS Organizations Benutzerhandbuch.
- Sitzungsrichtlinien – Sitzungsrichtlinien sind erweiterte Richtlinien, die Sie als Parameter übergeben, wenn Sie eine temporäre Sitzung für eine Rolle oder einen verbundenen Benutzer programmgesteuert erstellen. Die resultierenden Sitzungsberechtigungen sind eine Schnittmenge der auf der Identität des Benutzers oder der Rolle basierenden Richtlinien und der Sitzungsrichtlinien. Berechtigungen können auch aus einer ressourcenbasierten Richtlinie stammen. Eine explizite Zugriffsverweigerung in einer dieser Richtlinien setzt eine Zugriffserlaubnis außer Kraft. Weitere Informationen finden Sie unter Sitzungsrichtlinien im IAM-Benutzerhandbuch.

Mehrere Richtlinientypen

Wenn mehrere auf eine Anforderung mehrere Richtlinientypen angewendet werden können, sind die entsprechenden Berechtigungen komplizierter. Informationen darüber, wie AWS bestimmt wird, ob eine Anfrage zulässig ist, wenn mehrere Richtlinientypen betroffen sind, finden Sie im IAM-Benutzerhandbuch unter Bewertungslogik für Richtlinien.

Wie AWS Config funktioniert mit IAM

Bevor Sie IAM zur Verwaltung des Zugriffs auf verwenden AWS Config, sollten Sie sich darüber informieren, mit welchen IAM-Funktionen Sie arbeiten können. AWS Config

IAM-Funktionen, die Sie mit verwenden können AWS Config

IAM-Feature	AWS Config Unterstützung
Identitätsbasierte Richtlinien	Ja
Ressourcenbasierte Richtlinien	Nein
Richtlinienaktionen	Ja
Richtlinienressourcen	Ja
Richtlinienbedingungsschlüssel (services pezifisch)	Ja
ACLs	Nein
ABAC (Tags in Richtlinien)	Ja
Temporäre Anmeldeinformationen	Ja
Forward Access Sessions (FAS)	Ja
Servicerollen	Ja
Service-verknüpfte Rollen	Ja

Einen allgemeinen Überblick darüber, wie AWS Config und andere AWS Dienste mit den meisten IAM-Funktionen funktionieren, finden Sie im IAM-Benutzerhandbuch unter AWS Dienste, die mit IAM funktionieren.

Identitätsbasierte Richtlinien für AWS Config

Unterstützt Richtlinien auf Identitätsbasis: Ja

Identitätsbasierte Richtlinien sind JSON-Berechtigungsrichtliniendokumente, die Sie einer Identität anfügen können, wie z. B. IAM-Benutzern, -Benutzergruppen oder -Rollen. Diese Richtlinien steuern, welche Aktionen die Benutzer und Rollen für welche Ressourcen und unter welchen Bedingungen ausführen können. Informationen zum Erstellen identitätsbasierter Richtlinien finden Sie unter Definieren benutzerdefinierter IAM-Berechtigungen mit vom Kunden verwalteten Richtlinien im IAM-Benutzerhandbuch.

Mit identitätsbasierten IAM-Richtlinien können Sie angeben, welche Aktionen und Ressourcen zugelassen oder abgelehnt werden. Darüber hinaus können Sie die Bedingungen festlegen, unter denen Aktionen zugelassen oder abgelehnt werden. Sie können den Prinzipal nicht in einer identitätsbasierten Richtlinie angeben, da er für den Benutzer oder die Rolle gilt, dem er zugeordnet ist. Informationen zu sämtlichen Elementen, die Sie in einer JSON-Richtlinie verwenden, finden Sie in der IAM-Referenz für JSON-Richtlinienelemente im IAM-Benutzerhandbuch.

Beispiele für identitätsbasierte Richtlinien für AWS Config

Beispiele für AWS Config identitätsbasierte Richtlinien finden Sie unter. Beispiele für identitätsbasierte Richtlinien für AWS Config

Ressourcenbasierte Richtlinien finden Sie in AWS Config

Unterstützt ressourcenbasierte Richtlinien: Nein

Ressourcenbasierte Richtlinien sind JSON-Richtliniendokumente, die Sie an eine Ressource anfügen. Beispiele für ressourcenbasierte Richtlinien sind IAM-Rollen-Vertrauensrichtlinien und Amazon-S3-Bucket-Richtlinien. In Services, die ressourcenbasierte Richtlinien unterstützen, können Service-Administratoren sie verwenden, um den Zugriff auf eine bestimmte Ressource zu steuern. Für die Ressource, an welche die Richtlinie angehängt ist, legt die Richtlinie fest, welche Aktionen ein bestimmter Prinzipal unter welchen Bedingungen für diese Ressource ausführen kann. Sie müssen in einer ressourcenbasierten Richtlinie einen Prinzipal angeben. Zu den Prinzipalen können Konten, Benutzer, Rollen, Verbundbenutzer oder gehören. AWS-Services

Um kontoübergreifenden Zugriff zu ermöglichen, können Sie ein gesamtes Konto oder IAM-Entitäten in einem anderen Konto als Prinzipal in einer ressourcenbasierten Richtlinie angeben. Durch das Hinzufügen eines kontoübergreifenden Auftraggebers zu einer ressourcenbasierten Richtlinie ist nur die halbe Vertrauensbeziehung eingerichtet. Wenn sich der Prinzipal und die Ressource unterscheiden AWS-Konten, muss ein IAM-Administrator des vertrauenswürdigen Kontos auch der Prinzipalentität (Benutzer oder Rolle) die Berechtigung zum Zugriff auf die Ressource erteilen. Sie erteilen Berechtigungen, indem Sie der juristischen Stelle eine identitätsbasierte Richtlinie anfügen. Wenn jedoch eine ressourcenbasierte Richtlinie Zugriff auf einen Prinzipal in demselben Konto gewährt, ist keine zusätzliche identitätsbasierte Richtlinie erforderlich. Weitere Informationen finden Sie unter Kontoübergreifender Ressourcenzugriff in IAM im IAM-Benutzerhandbuch.

Richtlinienaktionen für AWS Config

Unterstützt Richtlinienaktionen: Ja

Administratoren können mithilfe von AWS JSON-Richtlinien angeben, wer Zugriff auf was hat. Das heißt, welcher Prinzipal Aktionen für welche Ressourcen und unter welchen Bedingungen ausführen kann.

Das Element `Action` einer JSON-Richtlinie beschreibt die Aktionen, mit denen Sie den Zugriff in einer Richtlinie zulassen oder verweigern können. Richtlinienaktionen haben normalerweise denselben Namen wie der zugehörige AWS API-Vorgang. Es gibt einige Ausnahmen, z. B. Aktionen, die nur mit Genehmigung durchgeführt werden können und für die es keinen passenden API-Vorgang gibt. Es gibt auch einige Operationen, die mehrere Aktionen in einer Richtlinie erfordern. Diese zusätzlichen Aktionen werden als abhängige Aktionen bezeichnet.

Schließen Sie Aktionen in eine Richtlinie ein, um Berechtigungen zur Durchführung der zugeordneten Operation zu erteilen.

Eine Liste der AWS Config Aktionen finden Sie unter Aktionen definiert von AWS Config in der Serviceautorisierungsreferenz.

Bei Richtlinienaktionen wird vor der Aktion das folgende Präfix AWS Config verwendet:

```
config
```

Um mehrere Aktionen in einer einzigen Anweisung anzugeben, trennen Sie sie mit Kommata:

```
"Action": [
      "config:action1",
      "config:action2"
         ]
```

Sie können auch Platzhalter verwenden, um mehrere Aktionen anzugeben. Beispielsweise können Sie alle Aktionen festlegen, die mit dem Wort `Describe` beginnen, einschließlich der folgenden Aktion:

```
"Action": "config:Describe*"
```

Beispiele für AWS Config identitätsbasierte Richtlinien finden Sie unter. Beispiele für identitätsbasierte Richtlinien für AWS Config

Politische Ressourcen für AWS Config

Unterstützt Richtlinienressourcen: Ja

Administratoren können mithilfe von AWS JSON-Richtlinien angeben, wer Zugriff auf was hat. Das heißt, welcher Prinzipal Aktionen für welche Ressourcen und unter welchen Bedingungen ausführen kann.

Das JSON-Richtlinienelement `Resource` gibt die Objekte an, auf welche die Aktion angewendet wird. Anweisungen müssen entweder ein – `Resource`oder ein `NotResource`-Element enthalten. Als bewährte Methode geben Sie eine Ressource mit dem zugehörigen Amazon-Ressourcennamen (ARN) an. Sie können dies für Aktionen tun, die einen bestimmten Ressourcentyp unterstützen, der als Berechtigungen auf Ressourcenebene bezeichnet wird.

Verwenden Sie für Aktionen, die keine Berechtigungen auf Ressourcenebene unterstützen, z. B. Auflistungsoperationen, einen Platzhalter (*), um anzugeben, dass die Anweisung für alle Ressourcen gilt.

```
"Resource": "*"
```

Eine Liste der AWS Config Ressourcentypen und ihrer ARNs Eigenschaften finden Sie unter Resources defined by AWS Config in der Service Authorization Reference. Informationen zu den Aktionen, mit denen Sie den ARN einzelner Ressourcen angeben können, finden Sie unter Von AWS Config definierte Aktionen.

Beispiele für AWS Config identitätsbasierte Richtlinien finden Sie unter. Beispiele für identitätsbasierte Richtlinien für AWS Config

Bedingungsschlüssel für Richtlinien für AWS Config

Unterstützt servicespezifische Richtlinienbedingungsschlüssel: Ja

Administratoren können mithilfe von AWS JSON-Richtlinien angeben, wer auf was Zugriff hat. Das heißt, welcher Prinzipal kann Aktionen für welche Ressourcen und unter welchen Bedingungen ausführen.

Das Element `Condition` (oder `Condition` block) ermöglicht Ihnen die Angabe der Bedingungen, unter denen eine Anweisung wirksam ist. Das Element `Condition` ist optional. Sie können bedingte

Ausdrücke erstellen, die Bedingungsoperatoren verwenden, z. B. ist gleich oder kleiner als, damit die Bedingung in der Richtlinie mit Werten in der Anforderung übereinstimmt.

Wenn Sie mehrere `Condition`-Elemente in einer Anweisung oder mehrere Schlüssel in einem einzelnen `Condition`-Element angeben, wertet AWS diese mittels einer logischen `AND`-Operation aus. Wenn Sie mehrere Werte für einen einzelnen Bedingungsschlüssel angeben, AWS wertet die Bedingung mithilfe einer logischen `OR` Operation aus. Alle Bedingungen müssen erfüllt werden, bevor die Berechtigungen der Anweisung gewährt werden.

Sie können auch Platzhaltervariablen verwenden, wenn Sie Bedingungen angeben. Beispielsweise können Sie einem IAM-Benutzer die Berechtigung für den Zugriff auf eine Ressource nur dann gewähren, wenn sie mit dessen IAM-Benutzernamen gekennzeichnet ist. Weitere Informationen finden Sie unter IAM-Richtlinienelemente: Variablen und Tags im IAM-Benutzerhandbuch.

AWS unterstützt globale Bedingungsschlüssel und dienstspezifische Bedingungsschlüssel. Eine Übersicht aller AWS globalen Bedingungsschlüssel finden Sie unter Kontextschlüssel für AWS globale Bedingungen im IAM-Benutzerhandbuch.

Eine Liste der AWS Config Bedingungsschlüssel finden Sie unter Bedingungsschlüssel für AWS Config in der Service Authorization Reference. Informationen zu den Aktionen und Ressourcen, mit denen Sie einen Bedingungsschlüssel verwenden können, finden Sie unter Aktionen definiert von AWS Config.

Beispiele für AWS Config identitätsbasierte Richtlinien finden Sie unter. Beispiele für identitätsbasierte Richtlinien für AWS Config

ACLs in AWS Config

Unterstützt ACLs: Nein

Zugriffskontrolllisten (ACLs) steuern, welche Principals (Kontomitglieder, Benutzer oder Rollen) über Zugriffsberechtigungen für eine Ressource verfügen. ACLs ähneln ressourcenbasierten Richtlinien, verwenden jedoch nicht das JSON-Richtliniendokumentformat.

ABAC mit AWS Config

Unterstützt ABAC (Tags in Richtlinien): Ja

Die attributbasierte Zugriffskontrolle (ABAC) ist eine Autorisierungsstrategie, bei der Berechtigungen basierend auf Attributen definiert werden. In AWS werden diese Attribute als Tags bezeichnet. Sie

können Tags an IAM-Entitäten (Benutzer oder Rollen) und an viele AWS Ressourcen anhängen. Das Markieren von Entitäten und Ressourcen ist der erste Schritt von ABAC. Anschließend entwerfen Sie ABAC-Richtlinien, um Operationen zuzulassen, wenn das Tag des Prinzipals mit dem Tag der Ressource übereinstimmt, auf die sie zugreifen möchten.

ABAC ist in Umgebungen hilfreich, die schnell wachsen, und unterstützt Sie in Situationen, in denen die Richtlinienverwaltung mühsam wird.

Um den Zugriff auf der Grundlage von Tags zu steuern, geben Sie im Bedingungselement einer Richtlinie Tag-Informationen an, indem Sie die Schlüssel `aws:ResourceTag/key-name`, `aws:RequestTag/key-name`, oder Bedingung `aws:TagKeys` verwenden.

Wenn ein Service alle drei Bedingungsschlüssel für jeden Ressourcentyp unterstützt, lautet der Wert für den Service Ja. Wenn ein Service alle drei Bedingungsschlüssel für nur einige Ressourcentypen unterstützt, lautet der Wert Teilweise.

Weitere Informationen zu ABAC finden Sie unter Definieren von Berechtigungen mit ABAC-Autorisierung im IAM-Benutzerhandbuch. Um ein Tutorial mit Schritten zur Einstellung von ABAC anzuzeigen, siehe Attributbasierte Zugriffskontrolle (ABAC) verwenden im IAM-Benutzerhandbuch.

Weitere Informationen zum Markieren von AWS Config Ressourcen finden Sie unter. Verschlagworten Sie Ihre Ressourcen AWS Config

Verwenden temporärer Anmeldeinformationen mit AWS Config

Unterstützt temporäre Anmeldeinformationen: Ja

Einige funktionieren AWS-Services nicht, wenn Sie sich mit temporären Anmeldeinformationen anmelden. Weitere Informationen, einschließlich Informationen, die mit temporären Anmeldeinformationen AWS-Services funktionieren AWS-Services , finden Sie im IAM-Benutzerhandbuch unter Diese Option funktioniert mit IAM.

Sie verwenden temporäre Anmeldeinformationen, wenn Sie sich mit einer anderen AWS Management Console Methode als einem Benutzernamen und einem Passwort anmelden. Wenn Sie beispielsweise AWS über den Single Sign-On-Link (SSO) Ihres Unternehmens darauf zugreifen, werden bei diesem Vorgang automatisch temporäre Anmeldeinformationen erstellt. Sie erstellen auch automatisch temporäre Anmeldeinformationen, wenn Sie sich als Benutzer bei der Konsole anmelden und dann die Rollen wechseln. Weitere Informationen zum Wechseln von Rollen finden Sie unter Wechseln von einer Benutzerrolle zu einer IAM-Rolle (Konsole) im IAM-Benutzerhandbuch.

Mithilfe der AWS API AWS CLI oder können Sie temporäre Anmeldeinformationen manuell erstellen. Sie können diese temporären Anmeldeinformationen dann für den Zugriff verwenden AWS. AWS empfiehlt, temporäre Anmeldeinformationen dynamisch zu generieren, anstatt langfristige Zugriffsschlüssel zu verwenden. Weitere Informationen finden Sie unter Temporäre Sicherheitsanmeldeinformationen in IAM.

Zugriffssitzungen weiterleiten für AWS Config

Unterstützt Forward Access Sessions (FAS): Ja

Wenn Sie einen IAM-Benutzer oder eine IAM-Rolle verwenden, um Aktionen auszuführen AWS, gelten Sie als Principal. Bei einigen Services könnte es Aktionen geben, die dann eine andere Aktion in einem anderen Service initiieren. FAS verwendet die Berechtigungen des Prinzipals, der einen aufruft AWS-Service, kombiniert mit der Anforderung, Anfragen an nachgelagerte Dienste AWS-Service zu stellen. FAS-Anfragen werden nur gestellt, wenn ein Dienst eine Anfrage erhält, für deren Abschluss Interaktionen mit anderen AWS-Services oder Ressourcen erforderlich sind. In diesem Fall müssen Sie über Berechtigungen zum Ausführen beider Aktionen verfügen. Einzelheiten zu den Richtlinien für FAS-Anfragen finden Sie unter Zugriffssitzungen weiterleiten.

Servicerollen für AWS Config

Unterstützt Servicerollen: Ja

Eine Servicerolle ist eine IAM-Rolle, die ein Service annimmt, um Aktionen in Ihrem Namen auszuführen. Ein IAM-Administrator kann eine Servicerolle innerhalb von IAM erstellen, ändern und löschen. Weitere Informationen finden Sie unter Rollen zum Delegieren von Berechtigungen an einen AWS-Service erstellen im IAM-Benutzerhandbuch.

> **Warning**
>
> Das Ändern der Berechtigungen für eine Servicerolle könnte die AWS Config -Funktionalität beeinträchtigen. Bearbeiten Sie Servicerollen nur, AWS Config wenn Sie dazu eine Anleitung erhalten.

Dienstbezogene Rollen für AWS Config

Unterstützt dienstbezogene Rollen: Ja

Eine serviceverknüpfte Rolle ist eine Art von Servicerolle, die mit einer verknüpft ist. AWS-Service Der Service kann die Rolle übernehmen, um eine Aktion in Ihrem Namen auszuführen. Dienstbezogene Rollen werden in Ihrem Dienst angezeigt AWS-Konto und gehören dem Dienst. Ein IAM-Administrator kann die Berechtigungen für Service-verknüpfte Rollen anzeigen, aber nicht bearbeiten.

Einzelheiten zum Erstellen oder Verwalten von AWS Config dienstbezogenen Rollen finden Sie unter. Verwenden von serviceverknüpften Rollen für AWS Config

Details zum Erstellen oder Verwalten von serviceverknüpften Rollen finden Sie unter AWS -Services, die mit IAM funktionieren. Suchen Sie in der Tabelle nach einem Service mit einem `Yes` in der Spalte Service-linked role (Serviceverknüpfte Rolle). Wählen Sie den Link Yes (Ja) aus, um die Dokumentation für die serviceverknüpfte Rolle für diesen Service anzuzeigen.

Beispiele für identitätsbasierte Richtlinien für AWS Config

Benutzer und Rollen haben standardmäßig nicht die Berechtigung, AWS Config -Ressourcen zu erstellen oder zu ändern. Sie können auch keine Aufgaben mithilfe der AWS Management Console, AWS Command Line Interface (AWS CLI) oder AWS API ausführen. Ein IAM-Administrator muss IAM-Richtlinien erstellen, die Benutzern die Berechtigung erteilen, Aktionen für die Ressourcen auszuführen, die sie benötigen. Der Administrator kann dann die IAM-Richtlinien zu Rollen hinzufügen, und Benutzer können die Rollen annehmen.

Informationen dazu, wie Sie unter Verwendung dieser beispielhaften JSON-Richtliniendokumente eine identitätsbasierte IAM-Richtlinie erstellen, finden Sie unter Erstellen von IAM-Richtlinien (Konsole) im IAM-Benutzerhandbuch.

Einzelheiten zu Aktionen und Ressourcentypen, die von definiert wurden AWS Config, einschließlich des Formats von ARNs für jeden der Ressourcentypen, finden Sie unter Aktionen, Ressourcen und Bedingungsschlüssel für AWS Config in der Service Authorization Reference.

Themen

- Bewährte Methoden für Richtlinien
- Melden Sie sich an für ein AWS-Konto
- Erstellen eines Benutzers mit Administratorzugriff
- Verwenden der AWS Config -Konsole
- Gewähren der Berechtigung zur Anzeige der eigenen Berechtigungen für Benutzer

- Nur-Lese-Zugriff auf AWS Config
- Voller Zugriff auf AWS Config
- Unterstützte Berechtigungen auf Ressourcenebene für AWS Config Regel-API-Aktionen
- Unterstützte Berechtigungen auf Ressourcenebene für konten- und regionsübergreifende Datenaggregationen

Bewährte Methoden für Richtlinien

Identitätsbasierte Richtlinien legen fest, ob jemand AWS Config Ressourcen in Ihrem Konto erstellen, darauf zugreifen oder sie löschen kann. Dies kann zusätzliche Kosten für Ihr verursachen AWS-Konto. Befolgen Sie beim Erstellen oder Bearbeiten identitätsbasierter Richtlinien die folgenden Anleitungen und Empfehlungen:

- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten — Verwenden Sie die AWS verwalteten Richtlinien, die Berechtigungen für viele gängige Anwendungsfälle gewähren, um Ihren Benutzern und Workloads zunächst Berechtigungen zu gewähren. Sie sind in Ihrem verfügbar. AWS-Konto Wir empfehlen Ihnen, die Berechtigungen weiter zu reduzieren, indem Sie vom AWS Kunden verwaltete Richtlinien definieren, die speziell auf Ihre Anwendungsfälle zugeschnitten sind. Weitere Informationen finden Sie unter AWS -verwaltete Richtlinien oder AWS -verwaltete Richtlinien für Auftrags-Funktionen im IAM-Benutzerhandbuch.
- Anwendung von Berechtigungen mit den geringsten Rechten – Wenn Sie mit IAM-Richtlinien Berechtigungen festlegen, gewähren Sie nur die Berechtigungen, die für die Durchführung einer Aufgabe erforderlich sind. Sie tun dies, indem Sie die Aktionen definieren, die für bestimmte Ressourcen unter bestimmten Bedingungen durchgeführt werden können, auch bekannt als die geringsten Berechtigungen. Weitere Informationen zur Verwendung von IAM zum Anwenden von Berechtigungen finden Sie unter Richtlinien und Berechtigungen in IAM im IAM-Benutzerhandbuch.
- Verwenden von Bedingungen in IAM-Richtlinien zur weiteren Einschränkung des Zugriffs – Sie können Ihren Richtlinien eine Bedingung hinzufügen, um den Zugriff auf Aktionen und Ressourcen zu beschränken. Sie können beispielsweise eine Richtlinienbedingung schreiben, um festzulegen, dass alle Anforderungen mithilfe von SSL gesendet werden müssen. Sie können auch Bedingungen verwenden, um Zugriff auf Serviceaktionen zu gewähren, wenn diese für einen bestimmten Zweck verwendet werden AWS-Service, z. AWS CloudFormation B. Weitere Informationen finden Sie unter IAM-JSON-Richtlinienelemente: Bedingung im IAM-Benutzerhandbuch.

- Verwenden von IAM Access Analyzer zur Validierung Ihrer IAM-Richtlinien, um sichere und funktionale Berechtigungen zu gewährleisten – IAM Access Analyzer validiert neue und vorhandene Richtlinien, damit die Richtlinien der IAM-Richtliniensprache (JSON) und den bewährten IAM-Methoden entsprechen. IAM Access Analyzer stellt mehr als 100 Richtlinienprüfungen und umsetzbare Empfehlungen zur Verfügung, damit Sie sichere und funktionale Richtlinien erstellen können. Weitere Informationen finden Sie unter Richtlinienvalidierung mit IAM Access Analyzer im IAM-Benutzerhandbuch.
- Multi-Faktor-Authentifizierung (MFA) erforderlich — Wenn Sie ein Szenario haben, das IAM-Benutzer oder einen Root-Benutzer in Ihrem System erfordert AWS-Konto, aktivieren Sie MFA für zusätzliche Sicherheit. Um MFA beim Aufrufen von API-Vorgängen anzufordern, fügen Sie Ihren Richtlinien MFA-Bedingungen hinzu. Weitere Informationen finden Sie unter Sicherer API-Zugriff mit MFA im IAM-Benutzerhandbuch.

Weitere Informationen zu bewährten Methoden in IAM finden Sie unter Bewährte Methoden für die Sicherheit in IAM im IAM-Benutzerhandbuch.

Melden Sie sich an für ein AWS-Konto

Wenn Sie noch keine haben AWS-Konto, führen Sie die folgenden Schritte aus, um eine zu erstellen.

Um sich für eine anzumelden AWS-Konto

1. Öffnen Sie https://portal.aws.amazon.com/billing/die Anmeldung.
2. Folgen Sie den Online-Anweisungen.

   Ein Teil des Anmeldevorgangs umfasst den Empfang eines Telefonanrufs oder einer Textnachricht und die Eingabe eines Bestätigungscodes auf der Telefontastatur.

   Wenn Sie sich für eine anmelden AWS-Konto, wird eine Root-Benutzer des AWS-Kontoserstellt. Der Root-Benutzer hat Zugriff auf alle AWS-Services und Ressourcen des Kontos. Als bewährte Sicherheitsmethode weisen Sie einem Administratorbenutzer Administratorzugriff zu und verwenden Sie nur den Root-Benutzer, um Aufgaben auszuführen, die Root-Benutzerzugriff erfordern.

AWS sendet Ihnen nach Abschluss des Anmeldevorgangs eine Bestätigungs-E-Mail. Du kannst jederzeit deine aktuellen Kontoaktivitäten einsehen und dein Konto verwalten, indem du zu https://aws.amazon.com/gehst und Mein Konto auswählst.

Erstellen eines Benutzers mit Administratorzugriff

Nachdem Sie sich für einen angemeldet haben AWS-Konto, sichern Sie Ihren Root-Benutzer des AWS-Kontos AWS IAM Identity Center, aktivieren und erstellen Sie einen Administratorbenutzer, sodass Sie den Root-Benutzer nicht für alltägliche Aufgaben verwenden.

Sichern Sie Ihre Root-Benutzer des AWS-Kontos

1. Melden Sie sich AWS Management Consoleals Kontoinhaber an, indem Sie Root-Benutzer auswählen und Ihre AWS-Konto E-Mail-Adresse eingeben. Geben Sie auf der nächsten Seite Ihr Passwort ein.

   Hilfe bei der Anmeldung mit dem Root-Benutzer finden Sie unter Anmelden als Root-Benutzer im AWS-Anmeldung Benutzerhandbuch zu.
2. Aktivieren Sie die Multi-Faktor-Authentifizierung (MFA) für den Root-Benutzer.

   Anweisungen finden Sie unter Aktivieren eines virtuellen MFA-Geräts für Ihren AWS-Konto Root-Benutzer (Konsole) im IAM-Benutzerhandbuch.

Erstellen eines Benutzers mit Administratorzugriff

1. Aktivieren Sie das IAM Identity Center.

   Anweisungen finden Sie unter Aktivieren AWS IAM Identity Center im AWS IAM Identity Center Benutzerhandbuch.
2. Gewähren Sie einem Administratorbenutzer im IAM Identity Center Benutzerzugriff.

   Ein Tutorial zur Verwendung von IAM-Identity-Center-Verzeichnis als Identitätsquelle finden Sie IAM-Identity-Center-Verzeichnis im Benutzerhandbuch unter Benutzerzugriff mit der Standardeinstellung konfigurieren.AWS IAM Identity Center

Anmelden als Administratorbenutzer

- Um sich mit Ihrem IAM-Identity-Center-Benutzer anzumelden, verwenden Sie die Anmelde-URL, die an Ihre E-Mail-Adresse gesendet wurde, als Sie den IAM-Identity-Center-Benutzer erstellt haben.

  Hilfe bei der Anmeldung mit einem IAM Identity Center-Benutzer finden Sie im AWS-Anmeldung Benutzerhandbuch unter Anmeldung beim AWS Access-Portal.

Weiteren Benutzern Zugriff zuweisen

1. Erstellen Sie im IAM-Identity-Center einen Berechtigungssatz, der den bewährten Vorgehensweisen für die Anwendung von geringsten Berechtigungen folgt.

   Anweisungen hierzu finden Sie unter Berechtigungssatz erstellen im AWS IAM Identity Center Benutzerhandbuch.
2. Weisen Sie Benutzer einer Gruppe zu und weisen Sie der Gruppe dann Single Sign-On-Zugriff zu.

   Eine genaue Anleitung finden Sie unter Gruppen hinzufügen im AWS IAM Identity Center Benutzerhandbuch.

Verwenden der AWS Config -Konsole

Um auf die AWS Config Konsole zugreifen zu können, benötigen Sie ein Mindestmaß an Berechtigungen. Diese Berechtigungen müssen es Ihnen ermöglichen, Details zu den AWS Config Ressourcen in Ihrem aufzulisten und anzuzeigen AWS-Konto. Wenn Sie eine identitätsbasierte Richtlinie erstellen, die strenger ist als die mindestens erforderlichen Berechtigungen, funktioniert die Konsole nicht wie vorgesehen für Entitäten (Benutzer oder Rollen) mit dieser Richtlinie.

Sie müssen Benutzern, die nur die API AWS CLI oder die AWS API aufrufen, keine Mindestberechtigungen für die Konsole gewähren. Stattdessen sollten Sie nur Zugriff auf die Aktionen zulassen, die der API-Operation entsprechen, die die Benutzer ausführen möchten.

Um sicherzustellen, dass Benutzer und Rollen die AWS Config Konsole weiterhin verwenden können, fügen Sie den Entitäten auch die AWS Config `AWSConfigUserAccess` AWS verwaltete Richtlinie hinzu. Weitere Informationen finden Sie unter Hinzufügen von Berechtigungen zu einem Benutzer im IAM-Benutzerhandbuch.

Sie müssen Benutzern Berechtigungen für die Interaktion mit ihnen erteilen AWS Config. Verwenden Sie für Benutzer, die vollen Zugriff auf benötigen AWS Config, die Richtlinie Vollzugriff auf AWS Config verwaltet.

Um Zugriff zu gewähren, fügen Sie Ihren Benutzern, Gruppen oder Rollen Berechtigungen hinzu:

- Benutzer und Gruppen in AWS IAM Identity Center:

  Erstellen Sie einen Berechtigungssatz. Befolgen Sie die Anweisungen unter Erstellen eines Berechtigungssatzes im AWS IAM Identity Center -Benutzerhandbuch.

- Benutzer, die in IAM über einen Identitätsanbieter verwaltet werden:

  Erstellen Sie eine Rolle für den Identitätsverbund. Befolgen Sie die Anleitung unter Eine Rolle für einen externen Identitätsanbieter (Verbund) erstellen im IAM-Benutzerhandbuch.
- IAM-Benutzer:
  - Erstellen Sie eine Rolle, die Ihr Benutzer annehmen kann. Befolgen Sie die Anleitung unter Eine Rolle für einen IAM-Benutzer erstellen im IAM-Benutzerhandbuch.
  - (Nicht empfohlen) Weisen Sie einem Benutzer eine Richtlinie direkt zu oder fügen Sie einen Benutzer zu einer Benutzergruppe hinzu. Befolgen Sie die Anweisungen unter Hinzufügen von Berechtigungen zu einem Benutzer (Konsole) im IAM-Benutzerhandbuch.

Gewähren der Berechtigung zur Anzeige der eigenen Berechtigungen für Benutzer

In diesem Beispiel wird gezeigt, wie Sie eine Richtlinie erstellen, die IAM-Benutzern die Berechtigung zum Anzeigen der eingebundenen Richtlinien und verwalteten Richtlinien gewährt, die ihrer Benutzeridentität angefügt sind. Diese Richtlinie umfasst Berechtigungen zum Ausführen dieser Aktion auf der Konsole oder programmgesteuert mithilfe der API AWS CLI oder AWS .

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ViewOwnUserInfo",
            "Effect": "Allow",
            "Action": [
                "iam:GetUserPolicy",
                "iam:ListGroupsForUser",
                "iam:ListAttachedUserPolicies",
                "iam:ListUserPolicies",
                "iam:GetUser"
            ],
            "Resource": ["arn:aws:iam::*:user/${aws:username}"]
        },
        {
            "Sid": "NavigateInConsole",
            "Effect": "Allow",
            "Action": [
                "iam:GetGroupPolicy",
                "iam:GetPolicyVersion",
                "iam:GetPolicy",
```

```
                "iam:ListAttachedGroupPolicies",
                "iam:ListGroupPolicies",
                "iam:ListPolicyVersions",
                "iam:ListPolicies",
                "iam:ListUsers"
            ],
            "Resource": "*"
        }
    ]
}
```

Nur-Lese-Zugriff auf AWS Config

Das folgende Beispiel zeigt eine AWS verwaltete Richtlinie, `AWSConfigUserAccess` die nur Lesezugriff auf gewährt. AWS Config

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "config:Get*",
        "config:Describe*",
        "config:Deliver*",
        "config:List*",
        "config:Select*",
        "tag:GetResources",
        "tag:GetTagKeys",
        "cloudtrail:DescribeTrails",
        "cloudtrail:GetTrailStatus",
        "cloudtrail:LookupEvents"
      ],
      "Resource": "*"
    }
  ]
}
```

In den Richtlinienanweisungen gibt das Element `Effect` an, ob die Aktionen zugelassen oder verweigert werden. Das Element `Action` listet die spezifischen Aktionen auf, die der Benutzer ausführen darf. Das `Resource` Element listet die AWS Ressourcen auf, auf denen der Benutzer

diese Aktionen ausführen darf. Bei Richtlinien, die den Zugriff auf AWS Config Aktionen steuern, ist das `Resource` Element immer auf gesetzt`*`, ein Platzhalter, der „alle Ressourcen“ bedeutet.

Die Werte im `Action` Element entsprechen denen, die von den APIs Diensten unterstützt werden. Den Aktionen ist ein vorangestelltconfig:, um darauf hinzuweisen, dass sie sich auf AWS Config Aktionen beziehen. Sie können das Platzhalterzeichen `*` im Element `Action` beispielsweise wie folgt verwenden:

- `"Action": ["config:*ConfigurationRecorder"]`

  Dies erlaubt alle AWS Config Aktionen, die mit "ConfigurationRecorder" (`StartConfigurationRecorder`,`StopConfigurationRecorder`) enden.
- `"Action": ["config:*"]`

  Dies erlaubt alle AWS Config Aktionen, aber keine Aktionen für andere AWS Dienste.
- `"Action": ["*"]`

  Dies ermöglicht alle AWS Aktionen. Diese Berechtigung ist für einen Benutzer geeignet, der als AWS Administrator für Ihr Konto fungiert.

Die Richtlinie für den schreibgeschützten Zugriff erteilt Benutzern keine Berechtigung für die Aktionen (z. B. `StartConfigurationRecorder`, `StopConfigurationRecorder` und `DeleteConfigurationRecorder`). Benutzer mit dieser Richtlinie dürfen den Configuration Recorder weder starten noch beenden oder löschen. Eine Liste der AWS Config Aktionen finden Sie in der AWS Config API-Referenz.

Voller Zugriff auf AWS Config

Das folgende Beispiel zeigt eine Richtlinie, die vollen Zugriff auf gewährt AWS Config. Sie gewährt Benutzern die Berechtigung, alle AWS Config Aktionen auszuführen. Darüber hinaus können Benutzer Dateien in Amazon-S3-Buckets verwalten und Amazon-SNS-Themen in dem Konto verwalten, mit dem der Benutzer verknüpft ist.

> **Important**
>
> Diese Richtlinie gewährt umfassende Berechtigungen. Bevor Sie Vollzugriff gewähren, sollten Sie gegebenenfalls mit einem Mindestsatz von Berechtigungen beginnen und zusätzliche

Berechtigungen nach Bedarf gewähren. Diese Methode ist besser, als anfangs zu weit gefasste Berechtigungen zu gewähren und dann später zu versuchen, sie zu begrenzen.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "sns:AddPermission",
                "sns:CreateTopic",
                "sns:DeleteTopic",
                "sns:GetTopicAttributes",
                "sns:ListPlatformApplications",
                "sns:ListTopics",
                "sns:SetTopicAttributes"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "s3:CreateBucket",
                "s3:GetBucketAcl",
                "s3:GetBucketLocation",
                "s3:GetBucketNotification",
                "s3:GetBucketPolicy",
                "s3:GetBucketRequestPayment",
                "s3:GetBucketVersioning",
                "s3:ListAllMyBuckets",
                "s3:ListBucket",
                "s3:ListBucketMultipartUploads",
                "s3:ListBucketVersions",
                "s3:PutBucketPolicy"
            ],
            "Resource": "arn:aws:s3:::*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "iam:CreateRole",
                "iam:GetRole",
```

```
                "iam:GetRolePolicy",
                "iam:ListRolePolicies",
                "iam:ListRoles",
                "iam:PutRolePolicy",
                "iam:AttachRolePolicy",
                "iam:CreatePolicy",
                "iam:CreatePolicyVersion",
                "iam:DeletePolicyVersion",
                "iam:CreateServiceLinkedRole"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "iam:PassRole"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "iam:PassedToService": [
                        "config.amazonaws.com",
                        "ssm.amazonaws.com"
                    ]
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "cloudtrail:DescribeTrails",
                "cloudtrail:GetTrailStatus",
                "cloudtrail:LookupEvents"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "config:*",
                "tag:Get*"
            ],
            "Resource": "*"
        },
```

```
        {
            "Effect": "Allow",
            "Action": [
                "ssm:DescribeDocument",
                "ssm:GetDocument",
                "ssm:DescribeAutomationExecutions",
                "ssm:GetAutomationExecution",
                "ssm:ListDocuments",
                "ssm:StartAutomationExecution"
            ],
            "Resource": "*"
        }

    ]
}
```

Unterstützte Berechtigungen auf Ressourcenebene für AWS Config Regel-API-Aktionen

Berechtigungen auf Ressourcenebene beziehen sich auf die Fähigkeit, anzugeben, auf welchen Ressourcen Benutzer Aktionen ausführen dürfen. AWS Config unterstützt Berechtigungen auf Ressourcenebene für bestimmte AWS Config Regel-API-Aktionen. Das bedeutet, dass Sie für bestimmte AWS Config Regelaktionen die Bedingungen steuern können, unter denen Benutzer diese Aktionen verwenden dürfen. Diese Bedingungen können Aktionen sein, die erfüllt sein müssen, oder bestimmte Ressourcen, die von den Benutzern verwendet werden dürfen.

In der folgenden Tabelle werden die AWS Config Regel-API-Aktionen beschrieben, die derzeit Berechtigungen auf Ressourcenebene unterstützen. Außerdem werden die unterstützten Ressourcen und die ARNs für jede Aktion benötigten Ressourcen beschrieben. Wenn Sie einen ARN angeben, können Sie den Platzhalter * in Ihren Pfaden verwenden, z. B. wenn Sie die genaue Ressource IDs nicht angeben können oder wollen.

> **Important**
>
> Wenn eine AWS Config Regel-API-Aktion in dieser Tabelle nicht aufgeführt ist, unterstützt sie keine Berechtigungen auf Ressourcenebene. Wenn eine AWS Config Regelaktion keine Berechtigungen auf Ressourcenebene unterstützt, können Sie Benutzern Berechtigungen zur Verwendung der Aktion gewähren. Sie müssen jedoch für das Ressourcenelement Ihrer Richtlinienerklärung ein Sternchen angeben.

API-Aktion	Ressourcen
DeleteConfigRule	Konfigurationsregel arn:aws:config ::config-rule/config-rule- *region:accountID ID*
DeleteEvaluationResults	Konfigurationsregel arn:aws:config *region:accountID* ::config-rule/config-rule- *ID*
DescribeCompliance ByConfigRule	Konfigurationsregel arn:aws:config *region:accountID* ::config-rule/config-rule- *ID*
DescribeConfigRuleEvaluatio nStatus	Konfigurationsregel arn:aws:config *region:accountID* ::config-rule/config-rule- *ID*
GetComplianceDetailsByConfi gRule	Konfigurationsregel arn:aws:config *region:accountID* ::config-rule/config-rule- *ID*
PutConfigRule	Konfigurationsregel arn:aws:config *region:accountID* ::config-rule/config-rule- *ID*
StartConfigRulesEvaluation	Konfigurationsregel arn:aws:config *region:accountID* ::config-rule/config-rule- *ID*
PutRemediationConfigurations	Korrekturkonfiguration

API-Aktion	Ressourcen
	arn:aws:config ::remediation-configuration/ *region:accountId config rule name/remediation configuration id*
DescribeRemediationConfigurations	Korrekturkonfiguration arn:aws:config ::remediation-configuration/ *region:accountId config rule name/remediation configuration id*
DeleteRemediationConfiguration	Korrekturkonfiguration arn:aws:config ::remediation-configuration/ *region:accountId config rule name/remediation configuration id*
PutRemediationExceptions	Korrekturkonfiguration arn:aws:config ::remediation-configuration/ *region:accountId config rule name/remediation configuration id*
DescribeRemediationExceptions	Korrekturkonfiguration arn:aws:config ::remediation-configuration/ *region:accountId config rule name/remediation configuration id*
DeleteRemediationExceptions	Korrekturkonfiguration arn:aws:config ::remediation-configuration/ *region:accountId config rule name/remediation configuration id*

Angenommen, Sie möchten bestimmten Benutzern den Lesezugriff auf bestimmte Regeln erteilen und den Schreibzugriff verweigern.

In der ersten Richtlinie erlauben Sie der Regel Leseaktionen, z. B. für die angegebenen Regeln AWS Config . `DescribeConfigRuleEvaluationStatus`

```
{
        "Version": "2012-10-17",
        "Statement": [
            {
                "Sid": "VisualEditor0",
                "Effect": "Allow",
                "Action": [
                    "config:StartConfigRulesEvaluation",
                    "config:DescribeComplianceByConfigRule",
                    "config:DescribeConfigRuleEvaluationStatus",
                    "config:GetComplianceDetailsByConfigRule"
                ],
                "Resource": [
                    "arn:aws:config:region:accountID:config-rule/config-rule-ID",
                    "arn:aws:config:region:accountID:config-rule/config-rule-ID"
                ]
            }
        ]
    }
```

In der zweiten Richtlinie verweigern Sie den AWS Config Regelschreibaktionen für die jeweilige Regel.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "VisualEditor0",
            "Effect": "Deny",
            "Action": [
                "config:PutConfigRule",
                "config:DeleteConfigRule",
                "config:DeleteEvaluationResults"
               ],
            "Resource": "arn:aws:config:region:accountID:config-rule/config-rule-ID"
           }
      ]
   }
```

Mit Berechtigungen auf Ressourcenebene können Sie Lesezugriff gewähren und Schreibzugriff verweigern, um bestimmte Aktionen für AWS Config Regel-API-Aktionen auszuführen.

Unterstützte Berechtigungen auf Ressourcenebene für konten- und regionsübergreifende Datenaggregationen

Mit Berechtigungen auf Ressourcenebene können Sie steuern, welche spezifischen Aktionen die Benutzer für die Datenaggregation für mehrere Konten und Regionen ausführen dürfen. Die folgenden Berechtigungen AWS Config `Aggregator` APIs unterstützen Berechtigungen auf Ressourcenebene:

- BatchGetAggregateResourceConfig
- DeleteConfigurationAggregator
- DescribeAggregateComplianceByConfigRules
- DescribeAggregateComplianceByConformancePacks
- DescribeConfigurationAggregatorSourcesStatus
- GetAggregateComplianceDetailsByConfigRule
- GetAggregateConfigRuleComplianceSummary
- GetAggregateConformancePackComplianceSummary
- GetAggregateDiscoveredResourceCounts
- GetAggregateResourceConfig
- ListAggregateDiscoveredResources
- PutConfigurationAggregator
- SelectAggregateResourceConfig

Sie können beispielsweise den Zugriff bestimmter Benutzer auf Ressourcendaten einschränken, indem Sie zwei Aggregatoren erstellen, `AccessibleAggregator` und `InAccessibleAggregator`, und eine IAM-Richtlinie anhängen, die den Zugriff auf `AccessibleAggregator` ermöglicht und auf `InAccessibleAggregator` verweigert.

IAM-Richtlinie für AccessibleAggregator

In dieser Richtlinie gewähren Sie Zugriff auf die unterstützten Aggregatoraktionen für den von Ihnen angegebenen AWS Config -Amazon-Ressourcennamen (ARN). In diesem Beispiel ist der AWS Config ARN`arn:aws:config:ap-northeast-1:`*`AccountID`*`:config-aggregator/config-aggregator-mocpsqhs`.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ConfigAllow",
            "Effect": "Allow",
            "Action": [
                "config:BatchGetAggregateResourceConfig",
                "config:DeleteConfigurationAggregator",
                "config:DescribeAggregateComplianceByConfigRules",
                "config:DescribeAggregateComplianceByConformancePacks",
                "config:DescribeConfigurationAggregatorSourcesStatus",
                "config:GetAggregateComplianceDetailsByConfigRule",
                "config:GetAggregateConfigRuleComplianceSummary",
                "config:GetAggregateConformancePackComplianceSummary",
                "config:GetAggregateDiscoveredResourceCounts",
                "config:GetAggregateResourceConfig",
                "config:ListAggregateDiscoveredResources",
                "config:PutConfigurationAggregator",
                "config:SelectAggregateResourceConfig"
            ],
            "Resource": "arn:aws:config:ap-northeast-1:AccountID:config-aggregator/
config-aggregator-mocpsqhs"
        }
    ]
}
```

IAM-Richtlinie für InAccessibleAggregator

In dieser Richtlinie verweigern Sie den Zugriff auf die unterstützten Aggregatoraktionen für den von Ihnen angegebenen AWS Config -ARN. In diesem Beispiel ist der AWS Config ARN`arn:aws:config:ap-northeast-1:`*`AccountID`*`:config-aggregator/config-aggregator-pokxzldx`.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ConfigDeny",
            "Effect": "Deny",
            "Action": [
                "config:BatchGetAggregateResourceConfig",
```

```
                "config:DeleteConfigurationAggregator",
                "config:DescribeAggregateComplianceByConfigRules",
                "config:DescribeAggregateComplianceByConformancePacks",
                "config:DescribeConfigurationAggregatorSourcesStatus",
                "config:GetAggregateComplianceDetailsByConfigRule",
                "config:GetAggregateConfigRuleComplianceSummary",
                "config:GetAggregateConformancePackComplianceSummary",
                "config:GetAggregateDiscoveredResourceCounts",
                "config:GetAggregateResourceConfig",
                "config:ListAggregateDiscoveredResources",
                "config:PutConfigurationAggregator",
                "config:SelectAggregateResourceConfig"
            ],
            "Resource": "arn:aws:config:ap-northeast-1:AccountID:config-aggregator/
config-aggregator-pokxzldx"
        }
    ]
}
```

Wenn ein Benutzer der Entwicklergruppe versucht, eine dieser Aktionen mit dem von Ihnen angegebenen AWS Config -ARN auszuführen, erhält dieser Benutzer die Ausnahme „Zugriff verweigert“.

Prüfen von Benutzerzugriffsberechtigungen

Führen Sie den folgenden AWS CLI -Befehl aus, um die von Ihnen erstellten Aggregatoren anzuzeigen:

```
aws configservice describe-configuration-aggregators
```

Wenn der Befehl erfolgreich abgeschlossen wurde, können Sie die Details aller Aggregatoren sehen, die mit Ihrem Konto verknüpft sind. In diesem Beispiel sind das `AccessibleAggregator` und `InAccessibleAggregator`:

```
{
    "ConfigurationAggregators": [
        {
            "ConfigurationAggregatorArn": "arn:aws:config:ap-
northeast-1:AccountID:config-aggregator/config-aggregator-mocpsqhs",
            "CreationTime": 1517942461.442,
            "ConfigurationAggregatorName": "AccessibleAggregator",
            "AccountAggregationSources": [
```

```
                {
                    "AllAwsRegions": true,
                    "AccountIds": [
                        "AccountID1",
                        "AccountID2",
                        "AccountID3"
                    ]
                }
            ],
            "LastUpdatedTime": 1517942461.455
        },
        {
            "ConfigurationAggregatorArn": "arn:aws:config:ap-
northeast-1:AccountID:config-aggregator/config-aggregator-pokxzldx",
            "CreationTime": 1517942461.442,
            "ConfigurationAggregatorName": "InAccessibleAggregator",
            "AccountAggregationSources": [
                {
                    "AllAwsRegions": true,
                    "AccountIds": [
                        "AccountID1",
                        "AccountID2",
                        "AccountID3"
                    ]
                }
            ],
            "LastUpdatedTime": 1517942461.455
        }
    ]
}
```

> **Note**
>
> `account-aggregation-sources`Geben Sie eine durch Kommas getrennte Liste von AWS Konten ein, IDs für die Sie Daten aggregieren möchten. Setzen Sie das Konto IDs in eckige Klammern und achten Sie darauf, Anführungszeichen zu vermeiden (z. B.`"[{\"AccountIds\": [\"AccountID1\",\"AccountID2\",\"AccountID3\"], \"AllAwsRegions\": true}]"`).

Fügen Sie die folgende IAM-Richtlinie an, um Zugriff auf `InAccessibleAggregator` oder den gewünschten Aggregator zu verweigern.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ConfigDeny",
            "Effect": "Deny",
            "Action": [
                "config:BatchGetAggregateResourceConfig",
                "config:DeleteConfigurationAggregator",
                "config:DescribeAggregateComplianceByConfigRules",
                "config:DescribeAggregateComplianceByConformancePacks",
                "config:DescribeConfigurationAggregatorSourcesStatus",
                "config:GetAggregateComplianceDetailsByConfigRule",
                "config:GetAggregateConfigRuleComplianceSummary",
                "config:GetAggregateConformancePackComplianceSummary",
                "config:GetAggregateDiscoveredResourceCounts",
                "config:GetAggregateResourceConfig",
                "config:ListAggregateDiscoveredResources",
                "config:PutConfigurationAggregator",
                "config:SelectAggregateResourceConfig"
            ],
            "Resource": "arn:aws:config:ap-northeast-1:AccountID:config-aggregator/
config-aggregator-pokxzldx"
        }
    ]
}
```

Als Nächstes können Sie bestätigen, dass mit der IAM-Richtlinie der Zugriff auf bestimmte Regeln für einen bestimmten Aggregator eingeschränkt werden kann:

```
aws configservice get-aggregate-compliance-details-by-config-rule --configuration-
aggregator-name InAccessibleAggregator --config-rule-name rule name --account-
id AccountID --aws-region AwsRegion
```

Der Befehl sollte eine Ausnahme des Typs „Zugriff verweigert“ zurückgeben:

```
An error occurred (AccessDeniedException) when calling the
 GetAggregateComplianceDetailsByConfigRule operation: User:
 arn:aws:iam::AccountID:user/ is not
authorized to perform: config:GetAggregateComplianceDetailsByConfigRule on resource:
 arn:aws:config:AwsRegion-1:AccountID:config-aggregator/config-aggregator-pokxzldx
```

AWS verwaltete Richtlinien für AWS Config

Eine AWS verwaltete Richtlinie ist eine eigenständige Richtlinie, die von erstellt und verwaltet wird AWS. AWS Verwaltete Richtlinien sind so konzipiert, dass sie Berechtigungen für viele gängige Anwendungsfälle bereitstellen, sodass Sie damit beginnen können, Benutzern, Gruppen und Rollen Berechtigungen zuzuweisen.

Beachten Sie, dass AWS verwaltete Richtlinien für Ihre speziellen Anwendungsfälle möglicherweise keine Berechtigungen mit den geringsten Rechten gewähren, da sie allen AWS Kunden zur Verfügung stehen. Wir empfehlen Ihnen, die Berechtigungen weiter zu reduzieren, indem Sie vom Kunden verwaltete Richtlinien definieren, die speziell auf Ihre Anwendungsfälle zugeschnitten sind.

Sie können die in AWS verwalteten Richtlinien definierten Berechtigungen nicht ändern. Wenn die in einer AWS verwalteten Richtlinie definierten Berechtigungen AWS aktualisiert werden, wirkt sich das Update auf alle Prinzidentitäten (Benutzer, Gruppen und Rollen) aus, denen die Richtlinie zugeordnet ist. AWS aktualisiert eine AWS verwaltete Richtlinie höchstwahrscheinlich, wenn eine neue Richtlinie eingeführt AWS-Service wird oder neue API-Operationen für bestehende Dienste verfügbar werden.

Weitere Informationen finden Sie unter Von AWS verwaltete Richtlinien im IAM-Benutzerhandbuch.

AWS verwaltete Richtlinie: AWSConfigServiceRolePolicy

AWS Config verwendet die angegebene dienstbezogene Rolle AWSServiceRoleForConfig, um in Ihrem Namen andere AWS Dienste aufzurufen. Wenn Sie die AWS Management Console zur Einrichtung verwenden AWS Config, wird diese Spiegelreflexkamera automatisch erstellt, AWS Config wenn Sie die Option auswählen, die AWS Config SLR anstelle Ihrer eigenen AWS Identity and Access Management (IAM) -Servicerolle zu verwenden.

Die SLR AWSServiceRoleForConfig enthält die verwaltete Richtlinie `AWSConfigServiceRolePolicy`. Diese verwaltete Richtlinie enthält nur Lese- und Schreibberechtigungen für Ressourcen sowie nur Leseberechtigungen für AWS Config Ressourcen in anderen Diensten, die dies unterstützen. AWS Config Weitere Informationen erhalten Sie unter Unterstützte Ressourcentypen für AWS Config und Verwenden von serviceverknüpften Rollen für AWS Config.

AWSConfigServiceRolePolicyRichtlinie anzeigen:.

> **Empfohlen: Verwenden Sie die mit dem Dienst verknüpfte Rolle**
>
> Es wird empfohlen, die dienstverknüpfte Rolle zu verwenden, sofern Sie keinen bestimmten Anwendungsfall haben. Eine dienstverknüpfte Rolle fügt alle erforderlichen Berechtigungen hinzu, damit sie wie erwartet ausgeführt werden AWS Config kann. Für einige Funktionen, wie z. B. für dienstverknüpfte Konfigurationsaufzeichnungen, müssen Sie die dienstverknüpfte Rolle verwenden.

AWS verwaltete Richtlinie: AWS_ConfigRole

Um Ihre AWS Ressourcenkonfigurationen aufzuzeichnen, AWS Config sind IAM-Berechtigungen erforderlich, um die Konfigurationsdetails zu Ihren Ressourcen abzurufen. Wenn Sie eine IAM-Rolle für AWS Config erstellen möchten, können Sie die verwaltete Richtlinie `AWS_ConfigRole` verwenden und sie an Ihre IAM-Rolle anfügen.

Diese IAM-Richtlinie wird jedes Mal aktualisiert, wenn Unterstützung für einen AWS Ressourcentyp AWS Config hinzugefügt wird. Das bedeutet, dass Sie AWS Config weiterhin über die erforderlichen Berechtigungen zum Aufzeichnen von Konfigurationsdaten unterstützter Ressourcentypen verfügen, solange der AWS_CRolle „ConfigRole“ diese verwaltete Richtlinie zugewiesen ist. Weitere Informationen erhalten Sie unter Unterstützte Ressourcentypen für AWS Config und Berechtigungen für die IAM-Rolle wurden zugewiesen AWS Config.

Sehen Sie sich die Richtlinie an: onfigRoleAWS_C.

AWS verwaltete Richtlinie: AWSConfigUserAccess

Diese IAM-Richtlinie ermöglicht den Nutzungszugriff AWS Config, einschließlich der Suche nach Tags in Ressourcen und dem Lesen aller Tags. Dadurch wird keine Berechtigung zur Konfiguration erteilt AWS Config, wofür Administratorrechte erforderlich sind.

Richtlinie anzeigen: AWSConfigUserAccess.

AWS verwaltete Richtlinie: ConfigConformsServiceRolePolicy

Für die Bereitstellung und Verwaltung von Conformance Packs AWS Config sind IAM-Berechtigungen und bestimmte Berechtigungen von anderen AWS Diensten erforderlich. Diese ermöglichen Ihnen die Bereitstellung und Verwaltung von Conformance Packs mit vollem Funktionsumfang. Sie werden jedes Mal aktualisiert und fügen neue Funktionen für Conformance Packs AWS Config hinzu. Weitere Informationen finden Sie unter Konformitätspakete.

Sehen Sie sich die Richtlinie an:. ConfigConformsServiceRolePolicy

AWS verwaltete Richtlinie: AWSConfigRulesExecutionRole

Für die Bereitstellung AWS benutzerdefinierter Lambda-Regeln AWS Config sind IAM-Berechtigungen und bestimmte Berechtigungen von anderen AWS Diensten erforderlich. Diese ermöglichen AWS Lambda Funktionen den Zugriff auf die AWS Config API und die Konfigurations-Snapshots, die regelmäßig AWS Config an Amazon S3 gesendet werden. Dieser Zugriff ist für Funktionen erforderlich, die Konfigurationsänderungen für AWS benutzerdefinierte Lambda-Regeln auswerten, und wird jedes Mal aktualisiert, wenn neue Funktionen AWS Config hinzugefügt werden. Weitere Informationen zu AWS benutzerdefinierten Lambda-Regeln finden Sie unter AWS Config Benutzerdefinierte Lambda-Regeln erstellen. Weitere Informationen zu Konfigurations-Snapshots finden Sie unter Konzepte | Konfigurations-Snapshot. Weitere Informationen zur Bereitstellung von Konfigurations-Snapshots finden Sie unter Verwalten des Übermittlungskanals.

Sehen Sie sich die Richtlinie an:. AWSConfigRulesExecutionRole

AWS verwaltete Richtlinie: AWSConfigMultiAccountSetupPolicy

Für die zentrale Bereitstellung, Aktualisierung und Löschung von AWS Config Regeln und Konformitätspaketen für alle Mitgliedskonten in einer Organisation in AWS Organizations AWS Config sind IAM-Berechtigungen und bestimmte Berechtigungen von anderen AWS Diensten erforderlich. Diese verwaltete Richtlinie wird jedes Mal aktualisiert, wenn AWS Config neue Funktionen für die Einrichtung mehrerer Konten hinzufügt. Weitere Informationen finden Sie unter AWS Config Regeln für alle Konten in Ihrer Organisation verwalten und Conformance Packs für alle Konten in Ihrer Organisation verwalten.

Richtlinie anzeigen: AWSConfigMultiAccountSetupPolicy.

AWS verwaltete Richtlinie: AWSConfigRoleForOrganizations

Um einen Nur-Lese-Zugriff AWS Config zu ermöglichen AWS Organizations APIs, AWS Config sind IAM-Berechtigungen und bestimmte Berechtigungen von anderen Diensten erforderlich. AWS Diese verwaltete Richtlinie wird jedes Mal aktualisiert, wenn AWS Config neue Funktionen für die Einrichtung mehrerer Konten hinzufügt. Weitere Informationen finden Sie unter AWS Config Regeln für alle Konten in Ihrer Organisation verwalten und Conformance Packs für alle Konten in Ihrer Organisation verwalten.

Richtlinie anzeigen: AWSConfigRoleForOrganizations.

AWS -verwaltete Richtlinie: AWSConfigRemediationServiceRolePolicy

AWS Config Damit `NON_COMPLIANT` Ressourcen in Ihrem Namen bereinigt werden können, AWS Config sind IAM-Berechtigungen und bestimmte Berechtigungen von anderen AWS Diensten erforderlich. Diese verwaltete Richtlinie wird jedes Mal aktualisiert, wenn neue Funktionen zur AWS Config Problembehebung hinzugefügt werden. Weitere Informationen zur Problembehebung finden Sie unter Korrigieren nicht konformer Ressourcen mithilfe von Regeln. AWS Config Weitere Informationen zu den Bedingungen, die zu den möglichen AWS Config Evaluierungsergebnissen führen, finden Sie unter Konzepte | Regeln. AWS Config

Sehen Sie sich die Richtlinie an: AWSConfigRemediationServiceRolePolicy.

AWS Config Aktualisierungen der AWS verwalteten Richtlinien

Hier finden Sie Informationen zu Aktualisierungen AWS verwalteter Richtlinien, die AWS Config seit Beginn der Nachverfolgung dieser Änderungen durch diesen Dienst vorgenommen wurden. Abonnieren Sie den RSS-Feed auf der Seite AWS Config Dokumentenverlauf, um automatische Benachrichtigungen über Änderungen an dieser Seite zu erhalten.

Änderung	Beschreibung	Datum
AWS_ConfigRole – Addition: "bedrock:GetGuardrail", "bedrock:GetInferenceProfile", "bedrock:GetKnowledgeBase", "bedrock:ListGuardrails", "bedrock:ListInferenceProfiles", "bedrock:ListKnowledgeBases", "bedrock:ListTagsForResource"	Diese Richtlinie unterstützt jetzt zusätzliche Berechtigungen für Amazon Bedrock.	27. Mai 2025
AWSConfigServiceRolePolicy – Addition: "bedrock:GetGuardrail", "bedrock:GetInferenceProfile", "bedrock:GetKnowledgeBase", "bedrock:ListGuardrails", "bedrock:ListInferenceProfiles",	Diese Richtlinie unterstützt jetzt zusätzliche Berechtigungen für Amazon Bedrock.	27. Mai 2025

Änderung	Beschreibung	Datum
"bedrock:ListKnowledgeBases", "bedrock:ListTagsForResource"		

Änderung	Beschreibung	Datum
AWS_ConfigRole – Addition: "b2bi:GetPartnership", "b2bi:GetProfile", "b2bi:ListPartnerships", "b2bi:ListProfiles", "bedrock:ListAgents", "cleanrooms:GetConfiguredTable", "cleanrooms:GetConfiguredTableAnalysisRule", "cleanrooms:GetMembership", "cleanrooms:GetPrivacyBudgetTemplate", "cleanrooms:ListConfiguredTables", "cleanrooms:ListMemberships", "cleanrooms:ListPrivacyBudgetTemplates", "codeconnections:GetConnection", "codeconnections:ListConnections", "codeconnections:ListTagsForResource", "directconnect:DescribeConnections", "dms:DescribeReplicationConfigs", "logs:DescribeAccountPolicies", "logs:DescribeResourcePolicies", "macie2:ListAutomatedDiscoveryAccounts", "managedblockchain:GetAccessor", "managedblockchain:ListAccessors", "qbusiness:GetApplication", "qbusiness:ListApplications", "qbusiness:ListTagsForResource", "route53profiles:GetProfile", "route53profiles:GetProfileAssociation", "route53profi	Diese Richtlinie unterstützt jetzt zusätzliche Berechtigungen für AWS B2B Data Interchange Amazon Bedrock,,, AWS Clean Rooms AWS CodeConnections, AWS Database Migration Service (AWS DMS) AWS Direct Connect, Amazon CloudWatch Logs, Amazon Macie, Amazon Managed Blockchain, Amazon Q Business, Route 53 Profiles, Amazon Simple Storage Service (Amazon S3), Amazon SageMaker AI AWS Security Hub, und AWS Systems Manager Incident Manager, AWS Systems Manager Incident Manager Kontakte und. AWS Systems Manager	08. April 2025

Änderung	Beschreibung	Datum
les:ListProfileAssociations", "route53profiles:ListProfiles", "route53profiles:ListTagsFor Resource", "s3:GetAccessGra ntsInstance", "s3:GetAc cessGrantsLocation", "s3:Li stAccessGrantsInstances", "s3:ListAccessGrantsLocatio ns", "sagemaker:DescribeClu ster", "sagemaker:DescribeM lflowTrackingServer", "sage maker:DescribeStudioLifecyc leConfig", "sagemaker:ListC lusters", "sagemaker:ListMlf lowTrackingServers", "sagem aker:ListStudioLifecycleCon figs", "securityhub:Describ eStandardsControls", "secur ityhub:GetEnabledStandards" , "ssm-contacts:GetContact", "ssm-contacts:GetContactCha nnel", "ssm-contacts:ListCo ntactChannels", "ssm-cont acts:ListContacts", "ssm-in cidents:GetResponsePlan", " ssm-incidents:ListResponseP lans", "ssm-incidents:ListT agsForResource", "ssm:Descr ibeInstanceInformation"		

Änderung	Beschreibung	Datum
AWSConfigServiceRolePolicy – Addition: "b2bi:GetPartnership", "b2bi:GetProfile", "b2bi:ListPartnerships", "b2bi:ListProfiles", "bedrock:ListAgents", "cleanrooms:GetConfiguredTable", "cleanrooms:GetConfiguredTableAnalysisRule", "cleanrooms:GetMembership", "cleanrooms:GetPrivacyBudgetTemplate", "cleanrooms:ListConfiguredTables", "cleanrooms:ListMemberships", "cleanrooms:ListPrivacyBudgetTemplates", "codeconnections:GetConnection", "codeconnections:ListConnections", "codeconnections:ListTagsForResource", "directconnect:DescribeConnections", "dms:DescribeReplicationConfigs", "logs:DescribeAccountPolicies", "logs:DescribeResourcePolicies", "macie2:ListAutomatedDiscoveryAccounts", "managedblockchain:GetAccessor", "managedblockchain:ListAccessors", "qbusiness:GetApplication", "qbusiness:ListApplications", "qbusiness:ListTagsForResource", "route53profiles:GetProfile", "route53profiles:GetProfileAssociation", "route53profi	Diese Richtlinie unterstützt jetzt zusätzliche Berechtigungen für AWS B2B Data Interchange Amazon Bedrock,,, AWS Clean Rooms AWS CodeConnections, AWS Database Migration Service (AWS DMS) AWS Direct Connect, Amazon CloudWatch Logs, Amazon Macie, Amazon Managed Blockchain, Amazon Q Business, Route 53 Profiles, Amazon Simple Storage Service (Amazon S3), Amazon SageMaker AI AWS Security Hub, und AWS Systems Manager Incident Manager, AWS Systems Manager Incident Manager Kontakte und. AWS Systems Manager Diese Richtlinie unterstützt jetzt auch die Erlaubnis, auf alle Amazon API Gateway Gateway-Domänennamen zuzugreifen, indem das Ressourcenmuster "`arn:aws:apigateway:::/domainnames/ `" eingeschlossen wird.	08. April 2025

Änderung	Beschreibung	Datum
les:ListProfileAssociations", "route53profiles:ListProfiles", "route53profiles:ListTagsFor Resource", "s3:GetAccessGra ntsInstance", "s3:GetAc cessGrantsLocation", "s3:Li stAccessGrantsInstances", "s3:ListAccessGrantsLocatio ns", "sagemaker:DescribeClu ster", "sagemaker:DescribeM lflowTrackingServer", "sage maker:DescribeStudioLifecyc leConfig", "sagemaker:ListC lusters", "sagemaker:ListMlf lowTrackingServers", "sagem aker:ListStudioLifecycleCon figs", "securityhub:Describ eStandardsControls", "secur ityhub:GetEnabledStandards" , "ssm-contacts:GetContact", "ssm-contacts:GetContactCha nnel", "ssm-contacts:ListCo ntactChannels", "ssm-cont acts:ListContacts", "ssm-in cidents:GetResponsePlan", " ssm-incidents:ListResponseP lans", "ssm-incidents:ListT agsForResource", "ssm:Descr ibeInstanceInformation"		
AWS_ConfigRole – Addition: "ec2:GetAllowedImagesSettin gs"	Diese Richtlinie unterstützt jetzt zusätzliche Berechtig ungen für Amazon Elastic Compute Cloud (Amazon EC2).	4. März 2025

Änderung	Beschreibung	Datum
AWSConfigServiceRolePolicy – Addition: "ec2:GetAllowedImagesSettings"	Diese Richtlinie unterstützt jetzt zusätzliche Berechtigungen für Amazon Elastic Compute Cloud (Amazon EC2).	4. März 2025
AWS_ConfigRole – Addition: "cleanrooms-ml:GetTrainingDataset", "cleanrooms-ml:ListTrainingDatasets", "comprehend:DescribeFlywheel", "comprehend:ListFlywheels", "comprehend:ListTagsForResource", "ec2:GetSnapshotBlockPublicAccessState", "omics:GetAnnotationStore", "omics:GetRunGroup", "omics:GetSequenceStore", "omics:GetVariantStore", "omics:ListAnnotationStores", "omics:ListRunGroups", "omics:ListSequenceStores", "omics:ListTagsForResource", "omics:ListVariantStores", "s3express:GetEncryptionConfiguration", "s3express:GetLifecycleConfiguration", "ses:GetDedicatedIpPool", "ses:GetDedicatedIps", and "ses:ListDedicatedIpPools"	Diese Richtlinie unterstützt jetzt zusätzliche Berechtigungen für AWS Clean Rooms Amazon Comprehend, Amazon Elastic Compute Cloud (Amazon EC2) AWS HealthOmics, Amazon Simple Storage Service (Amazon S3) und Amazon Simple Email Service (Amazon SES).	16. Januar 2025

Änderung	Beschreibung	Datum
AWSConfigServiceRolePolicy – Addition: "cleanrooms-ml:GetTrainingDataset", "cleanrooms-ml:ListTrainingDatasets", "comprehend:DescribeFlywheel", "comprehend:ListFlywheels", "comprehend:ListTagsForResource", "ec2:GetSnapshotBlockPublicAccessState", "omics:GetAnnotationStore", "omics:GetRunGroup", "omics:GetSequenceStore", "omics:GetVariantStore", "omics:ListAnnotationStores", "omics:ListRunGroups", "omics:ListSequenceStores", "omics:ListTagsForResource", "omics:ListVariantStores", "s3express:GetEncryptionConfiguration", "s3express:GetLifecycleConfiguration", "ses:GetDedicatedIpPool", "ses:GetDedicatedIps", and "ses:ListDedicatedIpPools"	Diese Richtlinie unterstützt jetzt zusätzliche Berechtigungen für AWS Clean Rooms Amazon Comprehend, Amazon Elastic Compute Cloud (Amazon EC2) AWS HealthOmics, Amazon Simple Storage Service (Amazon S3) und Amazon Simple Email Service (Amazon SES).	16. Januar 2025
AWSConfigServiceRolePolicy – Addition: "organizations:ListAWSServiceAccessForOrganization"	Diese Richtlinie unterstützt jetzt zusätzliche Berechtigungen für. AWS Organizations	18. Dezember 2024

Änderung	Beschreibung	Datum
AWS_ConfigRole – Addition: "app-integrations:GetApplication", "app-integrations:ListApplications", "app-integrations:ListTagsForResource", "appconfig:GetExtension", "appconfig:ListExtensions", "cloudtrail:GetInsightSelectors", "connect:DescribeQueue", "connect:DescribeRoutingProfile", "connect:DescribeSecurityProfile", "connect:ListQueueQuickConnects", "connect:ListQueues", "connect:ListRoutingProfileQueues", "connect:ListRoutingProfiles", "connect:ListSecurityProfileApplications", "connect:ListSecurityProfilePermissions", "connect:ListSecurityProfiles", "datazone:GetDomain", "datazone:ListDomains", "devops-guru:ListNotificationChannels", "glue:GetRegistry", "glue:ListRegistries", "identitystore:DescribeGroup", "identitystore:DescribeGroupMembership" "identitystore:ListGroupMemberships", "identitystore:ListGroups", "iot:DescribeThingGroup", "iot:DescribeThingType", "iot:ListThingGroups", "iot	Diese Richtlinie unterstützt jetzt zusätzliche Berechtigungen für AWS AppConfig ,, Amazon Connect AWS CloudTrail, Amazon, Amazon DevOps Guru DataZone, Identity Store AWS Glue,,, AWS IoT AWS IoT FleetWise AWS IoT Wireless, Amazon Interactive Video Service (Amazon IVS), Amazon CloudWatch Logs, Amazon CloudWatch Observability Access Manager AWS Payment Cryptography, Amazon Relational Database Service (Amazon RDS), Amazon Rekognition, Amazon Simple Storage Service (Amazon S3), Amazon EventBridge Scheduler und Amazon VPC Lattice. AWS Systems Manager	7. November 2024

Änderung	Beschreibung	Datum
:ListThingTypes", "iotfleetwise:GetDecoderManifest", "iotfleetwise:GetFleet", "iotfleetwise:GetModelManifest", "iotfleetwise:GetSignalCatalog", "iotfleetwise:GetVehicle", "iotfleetwise:ListDecoderManifestNetworkInterfaces", "iotfleetwise:ListDecoderManifests", "iotfleetwise:ListDecoderManifestSignals", "iotfleetwise:ListFleets", "iotfleetwise:ListModelManifestNodes", "iotfleetwise:ListModelManifests", "iotfleetwise:ListSignalCatalogNodes", "iotfleetwise:ListSignalCatalogs", "iotfleetwise:ListTagsForResource", "iotfleetwise:ListVehicles", "iotwireless:GetDestination", "iotwireless:GetDeviceProfile", "iotwireless:GetWirelessGateway", "iotwireless:ListDestinations", "iotwireless:ListDeviceProfiles", "iotwireless:ListWirelessGateways", "ivschat:GetLoggingConfiguration", "ivschat:GetRoom" "ivschat:ListLoggingConfigurations", "ivschat:ListRooms", "ivschat:ListTagsForResource", "logs:GetLogAnomalyDetector", "logs:ListLogAnomalyDetectors", "oam:GetS		

Änderung	Beschreibung	Datum
ink" "oam:GetSinkPolicy", "oam:ListSinks", "payment-cryptography:GetAlias", "payment-cryptography:GetKey", "payment-cryptography:ListAliases", "payment-cryptography:ListKeys", "payment-cryptography:ListTagsForResource", "rds:DescribeDBProxyTargetGroups", "rds:DescribeDBProxyTargets", "rekognition:DescribeProjects", "s3:GetStorageLensGroup", "s3:ListStorageLensGroups", "s3:ListTagsForResource", "scheduler:GetScheduleGroup", "scheduler:ListScheduleGroups", "scheduler:ListTagsForResource", "ssm:GetServiceSetting", "vpc-lattice:GetAccessLogSubscription", "vpc-lattice:GetService", "vpc-lattice:GetServiceNetwork", "vpc-lattice:GetTargetGroup", "vpc-lattice:ListAccessLogSubscriptions", "vpc-lattice:ListServiceNetworks", "vpc-lattice:ListServices", "vpc-lattice:ListTagsForResource", "vpc-lattice:ListTargetGroups", and "vpc-lattice:ListTargets"		

Änderung	Beschreibung	Datum
AWSConfigServiceRolePolicy – Addition: "app-integrations:GetApplication", "app-integrations:ListApplications", "app-integrations:ListTagsForResource", "appconfig:GetExtension", "appconfig:ListExtensions", "cloudtrail:GetInsightSelectors", "connect:DescribeQueue", "connect:DescribeRoutingProfile", "connect:DescribeSecurityProfile", "connect:ListQueueQuickConnects", "connect:ListQueues", "connect:ListRoutingProfileQueues", "connect:ListRoutingProfiles", "connect:ListSecurityProfileApplications", "connect:ListSecurityProfilePermissions", "connect:ListSecurityProfiles", "datazone:GetDomain", "datazone:ListDomains", "devops-guru:ListNotificationChannels", "glue:GetRegistry", "glue:ListRegistries", "identitystore:DescribeGroup", "identitystore:DescribeGroupMembership" "identitystore:ListGroupMemberships", "identitystore:ListGroups", "iot:DescribeThingGroup", "iot:DescribeThingType",	Diese Richtlinie unterstützt jetzt zusätzliche Berechtigungen für AWS AppConfig ,, Amazon Connect AWS CloudTrail, Amazon, Amazon DevOps Guru DataZone, Identity Store AWS Glue,,, AWS IoT AWS IoT FleetWise AWS IoT Wireless, Amazon Interactive Video Service (Amazon IVS), Amazon CloudWatch Logs, Amazon CloudWatch Observability Access Manager AWS Payment Cryptography, Amazon Relational Database Service (Amazon RDS), Amazon Rekognition, Amazon Simple Storage Service (Amazon S3), Amazon EventBridge Scheduler und Amazon VPC Lattice. AWS Systems Manager	7. November 2024

Änderung	Beschreibung	Datum
"iot:ListThingGroups", "iot :ListThingTypes", "iotfleet wise:GetDecoderManifest", " iotfleetwise:GetFleet", "iotfleet wise:GetModelManifest", "io tfleetwise:GetSignalCatalog ", "iotfleetwise:GetVehicle", "iotfleetwise:ListDecoderMa nifestNetworkInterfaces", " iotfleetwise:ListDecoderMan ifests", "iotfleetwise:List DecoderManifestSignals", "iotfleetwise:ListFleets", "i otfleetwise:ListModelManife stNodes", "iotfleetwise:Lis tModelManifests", "iotfleet wise:ListSignalCatalogNodes ", "iotfleetwise:ListSignal Catalogs", "iotfleetwise:Li stTagsForResource", "iotfleet wise:ListVehicles", "iotwir eless:GetDestination", "iotwirel ess:GetDeviceProfile", "iot wireless:GetWirelessGateway ", "iotwireless:ListDestina tions", "iotwireless:ListDe viceProfiles", "iotwireless :ListWirelessGateways", "iv schat:GetLoggingConfigurati on", "ivschat:GetRoom" "ivschat:ListLoggingConfigu rations", "ivschat:ListRooms ", "ivschat:ListTagsForReso urce", "logs:GetLogAnomal yDetector", "logs:ListLogAn		

Änderung	Beschreibung	Datum
omalyDetectors", "oam:GetSink" "oam:GetSinkPolicy", "oam:ListSinks", "payment-cryptography:GetAlias", "payment-cryptography:GetKey", "payment-cryptography:ListAliases", "payment-cryptography:ListKeys", "payment-cryptography:ListTagsForResource", "rds:DescribeDBProxyTargetGroups", "rds:DescribeDBProxyTargets", "rekognition:DescribeProjects", "s3:GetStorageLensGroup", "s3:ListStorageLensGroups", "s3:ListTagsForResource", "scheduler:GetScheduleGroup", "scheduler:ListScheduleGroups", "scheduler:ListTagsForResource", "ssm:GetServiceSetting", "vpc-lattice:GetAccessLogSubscription", "vpc-lattice:GetService", "vpc-lattice:GetServiceNetwork", "vpc-lattice:GetTargetGroup", "vpc-lattice:ListAccessLogSubscriptions", "vpc-lattice:ListServiceNetworks", "vpc-lattice:ListServices", "vpc-lattice:ListTagsForResource", "vpc-lattice:ListTargetGroups", and "vpc-lattice:ListTargets"		

Änderung	Beschreibung	Datum
AWS_ConfigRole – Addition: "aoss:BatchGetCollection," "aoss:BatchGetLifecyclePolicy," "aoss:BatchGetVpcEndpoint," "aoss:GetAccessPolicy," "aoss:GetSecurityConfig," "aoss:GetSecurityPolicy," "aoss:ListAccessPolicies," "aoss:ListCollections," "aoss:ListLifecyclePolicies," "aoss:ListSecurityConfigs," "aoss:ListSecurityPolicies," "aoss:ListVpcEndpoints," "appstream:DescribeAppBlockBuilders," "backup:GetRestoreTestingPlan," "backup:GetRestoreTestingSelection", "backup:ListRestoreTestingPlans," "backup:ListRestoreTestingSelections," "cloudTrail:GetChannel, "cloudTrail:ListChannels," "glue:GetTrigger," "glue:ListTriggers, "imagebuilder:GetLifecyclePolicy," "imagebuilder:ListLifecyclePolicies," "iot:DescribeBillingGroup, " "iot:ListBillingGroups," "ivs:GetEncoderConfiguration, " "ivs:GetPlaybackRestrictionPolicy," "ivs:GetStage," "ivs:GetStorageConfiguration, " "ivs:ListEncoderConfigurations," "ivs:ListPlaybackRest	Diese Richtlinie unterstützt jetzt zusätzliche Berechtigungen für Amazon OpenSearch Service Severless, Amazon AppStream,, AWS Backup, AWS CloudTrail AWS Glue, EC2 Image Builder AWS IoT, Amazon Interactive Video Service (Amazon IVS),, AWS Elemental MediaConnect AWS Elemental MediaTailor AWS HealthOmics, und Amazon EventBridge Scheduler.	16. September 2024

Änderung	Beschreibung	Datum
rictionPolicies," "ivs:List Stages," "ivs:ListStorageConfigurations," "mediaconnect:DescribeBridge", "mediaconnect:DescribeGatewa," "mediaconnect:ListBridges," "mediaconnect:ListGateways", "mediatailor:DescribeChannel," "mediatailor:DescribeLiveSource," "mediatailor:DescribeSourceLocation," "mediatailor:DescribeVodSource", "mediatailor:ListChannels," "mediatailor:ListLiveSources", "mediatailor:ListSourceLocations," "mediatailor:ListVodSources," "omics:GetWorkflow," "omics:ListWorkflows," "scheduler:GetSchedule," and "scheduler:ListSchedules"		

Änderung	Beschreibung	Datum
AWSConfigServiceRolePolicy – Addition: "aoss:BatchGetCollection," "aoss:BatchGetLifecyclePolicy," "aoss:BatchGetVpcEndpoint," "aoss:GetAccessPolicy," "aoss:GetSecurityConfig," "aoss:GetSecurityPolicy," "aoss:ListAccessPolicies," "aoss:ListCollections," "aoss:ListLifecyclePolicies," "aoss:ListSecurityConfigs," "aoss:ListSecurityPolicies," "aoss:ListVpcEndpoints," "appstream:DescribeAppBlockBuilders," "backup:GetRestoreTestingPlan," "backup:GetRestoreTestingSelection", "backup:ListRestoreTestingPlans," "backup:ListRestoreTestingSelections," "cloudTrail:GetChannel, "cloudTrail:ListChannels," "glue:GetTrigger," "glue:ListTriggers, "imagebuilder:GetLifecyclePolicy," "imagebuilder:ListLifecyclePolicies," "iot:DescribeBillingGroup, " "iot:ListBillingGroups," "ivs:GetEncoderConfiguration, " "ivs:GetPlaybackRestrictionPolicy," "ivs:GetStage," "ivs:GetStorageConfiguration, " "ivs:ListEncoderConfigurations," "ivs:ListPlaybackRest	Diese Richtlinie unterstützt jetzt zusätzliche Berechtigungen für Amazon OpenSearch Service Severless, Amazon AppStream,, AWS Backup, AWS CloudTrail AWS Glue, EC2 Image Builder AWS IoT, Amazon Interactive Video Service (Amazon IVS),, AWS Elemental MediaConnect AWS Elemental MediaTailor AWS HealthOmics, und Amazon EventBridge Scheduler.	16. September 2024

Änderung	Beschreibung	Datum
rictionPolicies," "ivs:List Stages," "ivs:ListStorageConfigurations," "mediaconnect:DescribeBridge", "mediaconnect:DescribeGatewa," "mediaconnect:ListBridges," "mediaconnect:ListGateways", "mediatailor:DescribeChannel," "mediatailor:DescribeLiveSource," "mediatailor:DescribeSourceLocation," "mediatailor:DescribeVodSource", "mediatailor:ListChannels," "mediatailor:ListLiveSources", "mediatailor:ListSourceLocations," "mediatailor:ListVodSources," "omics:GetWorkflow," "omics:ListWorkflows," "scheduler:GetSchedule," and "scheduler:ListSchedules"		
AWS_ConfigRole – Addition: "elasticfilesystem:DescribeTags," "redshift:DescribeTags," and "ssm-sap:ListTagsForResource"	Diese Richtlinie unterstützt jetzt zusätzliche Berechtigungen für Amazon Elastic File System (Amazon EFS), Amazon Redshift und AWS Systems Manager für SAP.	17. Juni 2024
AWSConfigServiceRolePolicy – Addition: "elasticfilesystem:DescribeTags," "redshift:DescribeTags," and "ssm-sap:ListTagsForResource"	Diese Richtlinie unterstützt jetzt zusätzliche Berechtigungen für Amazon Elastic File System (Amazon EFS), Amazon Redshift und AWS Systems Manager für SAP.	17. Juni 2024

Änderung	Beschreibung	Datum
AWS_ConfigRole – Addition: "aps:DescribeAlertManagerDefinition," "cloudwatch:DescribeAlarmsForMetric," "cognito-identity:DescribeIdentityPool, "cognito-identity:GetPrincipalTagAttributeMap," "elasticache:DescribeCacheSecurityGroups," "elasticache:DescribeUserGroups," "elasticache:DescribeUsers," "elasticache:DescribeGlobalReplicationGroups," "fsx:DescribeDataRepositoryAssociations," "glue:GetDatabase," "glue:GetDatabases," "iam:ListUsers," "lambda:GetLayerVersion," "lambda:ListLayers," "lambda:ListLayerVersions," "ram:GetPermission," "ram:ListPermissionAssociations," "ram:ListPermissions," "ram:ListPermissionVersions," "redshift-serverless:GetNamespace," "redshift-serverless:GetWorkgroup," "redshift-serverless:ListNamespaces," "redshift-serverless:ListTagsForResource," "redshift-serverless:ListWorkgroups," "sagemaker:DescribeInferenceExperiment," "sagemaker:ListInferenceExperiments," and "sns:G	Diese Richtlinie unterstützt jetzt zusätzliche Berechtigungen für Amazon Managed Service for Prometheus, Amazon CloudWatch, Amazon Cognito, Amazon, ElastiCache, AWS Identity and Access Management (IAM) FSx AWS Glue,,, Amazon Redshift Serverless AWS Lambda AWS RAM, Amazon SageMaker AI und Amazon Simple Notification Service (Amazon SNS).	22. Februar 2024

Änderung	Beschreibung	Datum
etSMSSandboxAccountStatus"		

Änderung	Beschreibung	Datum
AWSConfigServiceRolePolicy – Addition: "aps:DescribeAlertManagerDefinition," "cloudwatch:DescribeAlarmsForMetric," "cognito-identity:DescribeIdentityPool, "cognito-identity:GetPrincipalTagAttributeMap," "elasticache:DescribeCacheSecurityGroups," "elasticache:DescribeUserGroups," "elasticache:DescribeUsers," "elasticache:DescribeGlobalReplicationGroups," "fsx:DescribeDataRepositoryAssociations," "glue:GetDatabase," "glue:GetDatabases," "iam:ListUsers," "lambda:GetLayerVersion," "lambda:ListLayers," "lambda:ListLayerVersions," "ram:GetPermission," "ram:ListPermissionAssociations," "ram:ListPermissions," "ram:ListPermissionVersions," "redshift-serverless:GetNamespace," "redshift-serverless:GetWorkgroup," "redshift-serverless:ListNamespaces," "redshift-serverless:ListTagsForResource," "redshift-serverless:ListWorkgroups," "sagemaker:DescribeInferenceExperiment," "sagemaker:ListInferenceExperiments," and	Diese Richtlinie unterstützt jetzt zusätzliche Berechtigungen für Amazon Managed Service for Prometheus, Amazon CloudWatch, Amazon Cognito, Amazon, ElastiCache, AWS Identity and Access Management (IAM) FSx AWS Glue,,, Amazon Redshift Serverless AWS Lambda AWS RAM, Amazon SageMaker AI und Amazon Simple Notification Service (Amazon SNS).	22. Februar 2024

Änderung	Beschreibung	Datum
"sns:GetSMSSandboxAccountStatus"		
AWSConfigUserAccess— beginnt AWS Config mit der Nachverfolgung von Änderungen für diese verwaltete Richtlinie AWS	Diese Richtlinie ermöglicht den Zugriff auf die Nutzung AWS Config, einschließlich der Suche nach Tags in Ressourcen und dem Lesen aller Tags. Dadurch wird keine Berechtigung zur Konfiguration erteilt AWS Config, wofür Administratorrechte erforderlich sind.	22. Februar 2024
AWS_ConfigRole – Addition: "appconfig:GetExtensionAssociation," "appconfig:ListExtensionAssociations," "aps:DescribeLoggingConfiguration," "dms:DescribeReplicationTaskAssessmentRuns," "iam:GetOpenIDConnectProvider," "iam:ListOpenIDConnectProviders," "kafka:DescribeVpcConnection," "kafka:GetClusterPolicy," "kafka:ListVpcConnections," "logs:DescribeMetricFilters," "organizations:ListDelegatedAdministrators," "s3:GetBucketPolicyStatus," "s3express:GetBucketPolicy," and "s3express:ListAllMyDirectoryBuckets"	Diese Richtlinie unterstützt jetzt zusätzliche Berechtigungen für AWS AppConfig Amazon Managed Service for Prometheus, AWS Database Migration Service (AWS DMS), (AWS Identity and Access Management) IAM, Amazon Managed Streaming for Apache Kafka (Amazon MSK), Amazon CloudWatch Logs und Amazon Simple Storage Service (Amazon S3). AWS Organizations	5. Dezember 2023

Änderung	Beschreibung	Datum
AWSConfigServiceRolePolicy – Addition: "appconfig:GetExtensionAssociation," "appconfig:ListExtensionAssociations," "aps:DescribeLoggingConfiguration," "dms:DescribeReplicationTaskAssessmentRuns," "iam:GetOpenIDConnectProvider," "iam:ListOpenIDConnectProviders," "kafka:DescribeVpcConnection," "kafka:GetClusterPolicy," "kafka:ListVpcConnections," "logs:DescribeMetricFilters," "organizations:ListDelegatedAdministrators," "s3:GetBucketPolicyStatus," "s3express:GetBucketPolicy," and "s3express:ListAllMyDirectoryBuckets"	Diese Richtlinie unterstützt jetzt zusätzliche Berechtigungen für AWS AppConfig Amazon Managed Service for Prometheus, AWS Database Migration Service (AWS DMS), (AWS Identity and Access Management) IAM, Amazon Managed Streaming for Apache Kafka (Amazon MSK), Amazon CloudWatch Logs und Amazon Simple Storage Service (Amazon S3). AWS Organizations	05. Dezember 2023

Änderung	Beschreibung	Datum
AWS_ConfigRole – Addition: "backup:DescribeProtectedResource," "cognito-identity:GetIdentityPoolRoles," "cognito-identity:ListIdentityPools," "cognito-identity:ListTagsForResource," "cognito-idp:DescribeIdentityProvider," "cognito-idp:DescribeResourceServer," "cognito-idp:DescribeUserPool," "cognito-idp:DescribeUserPoolClient," "cognito-idp:DescribeUserPoolDomain," "cognito-idp:GetGroup," "cognito-idp:GetUserPoolMfaConfig," "cognito-idp:ListGroups," "cognito-idp:ListIdentityProviders," "cognito-idp:ListResourceServers," "cognito-idp:ListUserPoolClients," "cognito-idp:ListUserPools," "cognito-idp:ListTagsForResource," "connect:DescribeEvaluationForm," "connect:DescribeInstanceStorageConfig," "connect:DescribePrompt," "connect:DescribeRule," "connect:DescribeUser," "connect:GetTaskTemplate," "connect:ListApprovedOrigins," "connect:ListEvaluationForms," "connect:ListInstanceStorageConfigs," "connect:ListIntegrationAssociation	Diese Richtlinie unterstützt jetzt zusätzliche Berechtigungen für Amazon Cognito, Amazon Connect, Amazon EMR,, AWS Ground Station, Amazon MemoryDB AWS Mainframe Modernization,, Amazon AWS Organizations QuickSight, Amazon Relational Database Service (Amazon RDS), Amazon Redshift, Amazon Route 53,, und. AWS Service Catalog AWS Transfer Family	17. November 2023

Änderung	Beschreibung	Datum
s," "connect:ListPrompts," "connect:ListRules," "connect:ListSecurityKeys," "connect:ListTagsForResource," "connect:ListTaskTemplates," "connect:ListUsers," "emr-containers:DescribeVirtualCluster," "emr-containers:ListVirtualClusters," "emr-serverless:GetApplication," "emr-serverless:ListApplications," "groundstation:GetDataflowEndpointGroup," "groundstation:ListDataflowEndpointGroups," "m2:GetEnvironment," "m2:ListEnvironments," "m2:ListTagsForResource," "memorydb:DescribeAcls," "memorydb:DescribeClusters," "memorydb:DescribeParameterGroups," "memorydb:DescribeParameters," "memorydb:DescribeSubnetGroups," "organizations:ListRoots," "quicksight:DescribeAccountSubscription," "quicksight:DescribeDataSetRefreshProperties," "rds:DescribeEngineDefaultClusterParameters," "redshift:DescribeEndpointAccess," "redshift:DescribeEndpointAuthorization," "route53:GetChange," "route53:ListCidrBlocks," "route53:ListCidrL		

Änderung	Beschreibung	Datum
ocations," "serviceCatalog:DescribePortfolioShares," "transfer:DescribeProfile," and "transfer:ListProfiles"		
AWS_ConfigRole – Addition: "Sid": "AWSConfigServiceRolePolicyStatementID," "Sid": "AWSConfigSLRLogStatementID," "Sid": "AWSConfigSLRLogEventStatementID," and "Sid": "AWSConfigSLRApiGatewayStatementID"	Diese Richtlinie fügt jetzt Sicherheitskennungen (SID) für `AWSConfigServiceRolePolicyStatementID` , `AWSConfigSLRLogStatementID` , `AWSConfigSLRLogEventStatementID` und `AWSConfigSLRApiGatewayStatementID` hinzu.	17. November 2023

Änderung	Beschreibung	Datum
AWSConfigServiceRolePolicy – Addition: "backup:DescribeProtectedResource," "cognito-identity:GetIdentityPoolRoles," "cognito-identity:ListIdentityPools," "cognito-identity:ListTagsForResource," "cognito-idp:DescribeIdentityProvider," "cognito-idp:DescribeResourceServer," "cognito-idp:DescribeUserPool," "cognito-idp:DescribeUserPoolClient," "cognito-idp:DescribeUserPoolDomain," "cognito-idp:GetGroup," "cognito-idp:GetUserPoolMfaConfig," "cognito-idp:ListGroups," "cognito-idp:ListIdentityProviders," "cognito-idp:ListResourceServers," "cognito-idp:ListUserPoolClients," "cognito-idp:ListUserPools," "cognito-idp:ListTagsForResource," "connect:DescribeEvaluationForm," "connect:DescribeInstanceStorageConfig," "connect:DescribePrompt," "connect:DescribeRule," "connect:DescribeUser," "connect:GetTaskTemplate," "connect:ListApprovedOrigins," "connect:ListEvaluationForms," "connect:ListInstanceStorageConfigs," "connect	Diese Richtlinie unterstützt jetzt zusätzliche Berechtigungen für Amazon Cognito, Amazon Connect, Amazon EMR,, AWS Ground Station, Amazon MemoryDB AWS Mainframe Modernization,, Amazon AWS Organizations QuickSight, Amazon Relational Database Service (Amazon RDS), Amazon Redshift, Amazon Route 53,, und. AWS Service Catalog AWS Transfer Family	17. November 2023

Änderung	Beschreibung	Datum
:ListIntegrationAssociations," "connect:ListPrompts," "connect:ListRules," "connect:ListSecurityKeys," "connect:ListTagsForResource," "connect:ListTaskTemplates," "connect:ListUsers," "emr-containers:DescribeVirtualCluster," "emr-containers:ListVirtualClusters," "emr-serverless:GetApplication," "emr-serverless:ListApplications," "groundstation:GetDataflowEndpointGroup," "groundstation:ListDataflowEndpointGroups," "m2:GetEnvironment," "m2:ListEnvironments," "m2:ListTagsForResource," "memorydb:DescribeAcls," "memorydb:DescribeClusters," "memorydb:DescribeParameterGroups," "memorydb:DescribeParameters," "memorydb:DescribeSubnetGroups," "organizations:ListRoots," "quicksight:DescribeAccountSubscription," "quicksight:DescribeDataSetRefreshProperties," "rds:DescribeEngineDefaultClusterParameters," "redshift:DescribeEndpointAccess," "redshift:DescribeEndpointAuthorization," "route53:GetChange," "route53:ListCid		

Änderung	Beschreibung	Datum
rBlocks," "route53:ListCidrLocations," "serviceCatalog:DescribePortfolioShares," "transfer:DescribeProfile," and "transfer:ListProfiles"		
AWSConfigServiceRolePolicy – Addition: "Sid": "AWSConfigServiceRolePolicyStatementID," "Sid": "AWSConfigSLRLogStatementID," "Sid": "AWSConfigSLRLogEventStatementID," and "Sid": "AWSConfigSLRApiGatewayStatementID"	Diese Richtlinie fügt jetzt Sicherheitskennungen (SID) für `AWSConfigServiceRolePolicyStatementID` , `AWSConfigSLRLogStatementID` , `AWSConfigSLRLogEventStatementID` und `AWSConfigSLRApiGatewayStatementID` hinzu.	17. November 2023

Änderung	Beschreibung	Datum
AWS_ConfigRole – Addition: "acm-pca:GetCertificateAuthorityCertificate," "appmesh:DescribeMesh," "appmesh:ListGatewayRoutes," "connect:DescribeInstance," "connect:DescribeQuickConnect," "connect:ListQuickConnects," "ecs:DescribeCapacityProviders," "evidently:GetSegment," "evidently:ListSegments," "grafana:DescribeWorkspace," "grafana:DescribeWorkspaceAuthentication," "grafana:DescribeWorkspaceConfiguration," "grafana:DescribeWorkspaceConfiguration," "guardduty:GetMemberDetectors," "inspector2:BatchGetAccountStatus," "inspector2:GetDelegatedAdminAccount," "inspector2:ListMembers," "iot:DescribeCACertificate," "iot:ListCACertificates," "iot:ListTagsForResource," "iottwinmaker:GetSyncJob," "iottwinmaker:ListSyncJobs," "kafka:ListTagsForResource," "kafkaconnect:DescribeConnector," "kafkaconnect:ListConnectors," "lambda:GetCodeSigningConfig," "lambda:ListCodeSigningConfigs," "lambda:ListT	Diese Richtlinie unterstützt jetzt zusätzliche Berechtigungen für AWS Private CA,, Amazon Connect AWS App Mesh, Amazon Elastic Container Service (Amazon ECS), Amazon CloudWatch Evidly, Amazon Managed Grafana, Amazon, Amazon Inspector GuardDuty,, AWS IoT AWS IoT TwinMaker, Amazon Managed Streaming for Apache Kafka (Amazon MSK),, AWS Lambda AWS Network Manager AWS Organizations, und Amazon AI. SageMaker	04. Oktober 2023

Änderung	Beschreibung	Datum
ags," "networkmanager:GetConnectPeer," "organizations:DescribeOrganization," "organizations:ListTargetsForPolicy," "sagemaker:DescribeDataQualityJob," "sagemaker:DescribeModelExplainabilityJob," "sagemaker:ListDataQualityJob," and "sagemaker:ExplainabilityJob"		

Änderung	Beschreibung	Datum
AWSConfigServiceRolePolicy – Addition: "acm-pca:GetCertificateAuthorityCertificate," "appmesh:DescribeMesh," "appmesh:ListGatewayRoutes," "connect:DescribeInstance," "connect:DescribeQuickConnect," "connect:ListQuickConnects," "ecs:DescribeCapacityProviders," "evidently:GetSegment," "evidently:ListSegments," "grafana:DescribeWorkspace," "grafana:DescribeWorkspaceAuthentication," "grafana:DescribeWorkspaceConfiguration," "grafana:DescribeWorkspaceConfiguration," "guardduty:GetMemberDetectors," "inspector2:BatchGetAccountStatus," "inspector2:GetDelegatedAdminAccount," "inspector2:ListMembers," "iot:DescribeCACertificate," "iot:ListCACertificates," "iot:ListTagsForResource," "iottwinmaker:GetSyncJob," "iottwinmaker:ListSyncJobs," "kafka:ListTagsForResource," "kafkaconnect:DescribeConnector," "kafkaconnect:ListConnectors," "lambda:GetCodeSigningConfig," "lambda:ListCodeSi	Diese Richtlinie unterstützt jetzt zusätzliche Berechtigungen für AWS Private CA,, Amazon Connect AWS App Mesh, Amazon Elastic Container Service (Amazon ECS), Amazon CloudWatch Evidly, Amazon Managed Grafana, Amazon, Amazon Inspector GuardDuty,, AWS IoT AWS IoT TwinMaker, Amazon Managed Streaming for Apache Kafka (Amazon MSK),, AWS Lambda AWS Network Manager AWS Organizations, und Amazon AI. SageMaker	04. Oktober 2023

Änderung	Beschreibung	Datum
gningConfigs," "lambda:ListTags," "networkmanager:GetConnectPeer," "organizations:DescribeOrganization," "organizations:ListTargetsForPolicy," "sagemaker:DescribeDataQualityJob," "sagemaker:DescribeModelExplainabilityJob," "sagemaker:ListDataQualityJob," and "sagemaker:ExplainabilityJob"		
AWSConfigServiceRolePolicy— Entfernen "ssm:GetParameter"	Diese Richtlinie entfernt jetzt Berechtigungen für AWS Systems Manager (Systems Manager).	6. September 2023

Änderung	Beschreibung	Datum
AWS_ConfigRole – Addition: "appmesh:DescribeGatewayRoute","appstream:DescribeStacks", "aps:ListTagsForResource", "cloudfront:GetFunction", "cloudfront:GetOriginAccessControl", "cloudfront:ListFunctions", "cloudfront:ListOriginAccessControls", "codeartifact:ListPackages", "codeartifact:ListPackageVersions", "codebuild:BatchGetReportGroups", "codebuild:ListReportGroups", "connect:ListInstanceAttributes", "connect:ListInstances", "glue:GetPartition", "glue:GetPartitions", "guardduty:GetAdministratorAccount", "iam:ListInstanceProfileTags", "inspector2:ListFilters", "iot:DescribeJobTemplate", "iot:DescribeProvisioningTemplate", "iot:ListJobTemplates", "iot:ListProvisioningTemplates", "iottwinmaker:GetComponentType", "iottwinmaker:ListComponentTypes", "iotwireless:GetFuotaTask", "iotwireless:GetMulticastGroup", "iotwireless:ListFuotaTasks", "iotwireless:ListMulticastGroups", "kafka:ListScramSe	Diese Richtlinie unterstützt jetzt zusätzliche Berechtigungen für AWS App Mesh,, Amazon AWS CloudFormation, Amazon Connect CloudFront AWS CodeArtifact AWS CodeBuild,, Amazon AWS Glue, AWS Identity and Access Management (IAM) GuardDuty, Amazon Inspector,,, AWS IoT AWS IoT TwinMaker AWS IoT Wireless, Amazon Managed Streaming for Apache Kafka, Amazon Macie,,, AWS Elemental MediaConnect, AWS Network Manager AWS Organizations, Amazon Route 53 AWS Ressourcen Explorer, Amazon Simple Storage Service (Amazon S3) und Amazon Simple Notification Service (Amazon SNS).	28. Juli 2023

Änderung	Beschreibung	Datum
crets", "macie2:ListTagsForResource", "mediaconnect:ListTagsForResource", "networkmanager:GetConnectPeer", "networkmanager:ListConnectPeers", "organizations:DescribeEffectivePolicy", "organizations:DescribeResourcePolicy", "resource-explorer-2:GetIndex", "resource-explorer-2:ListIndexes", "resource-explorer-2:ListTagsForResource", "route53:ListCidrCollections", "s3:GetMultiRegionAccessPointPolicy", "s3:GetMultiRegionAccessPointPolicyStatus", and "sns:GetDataProtectionPolicy"		

Änderung	Beschreibung	Datum
AWSConfigServiceRolePolicy – Addition: "appmesh:DescribeGatewayRoute", "appstream:DescribeStacks", "aps:ListTagsForResource", "cloudfront:GetFunction", "cloudfront:GetOriginAccessControl", "cloudfront:ListFunctions", "cloudfront:ListOriginAccessControls", "codeartifact:ListPackages", "codeartifact:ListPackageVersions", "codebuild:BatchGetReportGroups", "codebuild:ListReportGroups", "connect:ListInstanceAttributes", "connect:ListInstances", "glue:GetPartition", "glue:GetPartitions", "guardduty:GetAdministratorAccount", "iam:ListInstanceProfileTags", "inspector2:ListFilters", "iot:DescribeJobTemplate", "iot:DescribeProvisioningTemplate", "iot:ListJobTemplates", "iot:ListProvisioningTemplates", "iottwinmaker:GetComponentType", "iottwinmaker:ListComponentTypes", "iotwireless:GetFuotaTask", "iotwireless:GetMulticastGroup", "iotwireless:ListFuotaTasks", "iotwireless:ListMulticastGroups", "kafka:ListScramSe	Diese Richtlinie unterstützt jetzt zusätzliche Berechtigungen für Amazon AppStream 2.0 AWS App Mesh, Amazon,, AWS CloudFormation, Amazon Connect CloudFront AWS CodeArtifact, AWS CodeBuild, Amazon, AWS Identity and Access Management (IAM) AWS Glue GuardDuty, Amazon Inspector,, AWS IoT AWS IoT TwinMaker AWS IoT Wireless, Amazon Managed Streaming for Apache Kafka, Amazon Macie,,,, AWS Elemental MediaConnect AWS Network Manager, Amazon Route 53 AWS Organizations AWS Ressourcen Explorer, Amazon Simple Storage Service (Amazon S3), Amazon Simple Notification Service (Amazon SNS) und Amazon EC2 Systems Manager (SSM).	28. Juli 2023

Änderung	Beschreibung	Datum
crets", "macie2:ListTagsForResource", "mediaconnect:ListTagsForResource", "networkmanager:GetConnectPeer", "networkmanager:ListConnectPeers", "organizations:DescribeEffectivePolicy", "organizations:DescribeResourcePolicy", "resource-explorer-2:GetIndex", "resource-explorer-2:ListIndexes", "resource-explorer-2:ListTagsForResource", "route53:ListCidrCollections", "s3:GetMultiRegionAccessPointPolicy", "s3:GetMultiRegionAccessPointPolicyStatus", "sns:GetDataProtectionPolicy", "ssm:DescribeParameters", "ssm:GetParameter", and "ssm:ListTagsForResource"		

Änderung	Beschreibung	Datum
AWS_ConfigRole – Addition: "amplify:GetBranch", "amplify: ListBranches", "app-integrat ions:GetEventIntegration", "app-integrations:ListEventI ntegrationAssociations", "ap p-integrations:ListEventInt egrations", "appmesh: DescribeRoute", "ap pmesh:ListRoutes", "aps:List RuleGroupsNamespaces", "athena:GetPreparedStat ement", "athena:ListPrepar edStatements", "batch:Descri beSchedulingPolicies", "batch:ListSchedulingPolici es", "cloudformation:ListTyp es", "cloudtrail:ListTrails", "co deartifact:ListDomains", "co deguru-profiler:DescribePro filingGroup", "codeguru-prof iler:GetNotificationConfigu ration", "codeguru-profiler: GetPolicy", "codeguru-profil er:ListProfilingGroups", "ds:DescribeDomainCon trollers", “dynamodb:Describ eTableReplicaAutoScaling" "dynamodb:DescribeTi meToLive", "ec2:Desc ribeTrafficMirrorFilters", "evidently:GetLaunch", "evidently:ListLaunches", "forecast:DescribeDa	Diese Richtlinie unterstützt jetzt zusätzliche Berechtig ungen für Amazon Connect AWS Amplify, Amazon Managed Service for Prometheus AWS App Mesh, Amazon Athena,,,,, Amazon AWS Batch, Amazon DynamoDB AWS CloudForm ation AWS CloudTrail AWS CodeArtifact CodeGuru AWS Directory Service, Amazon Elastic Compute Cloud (Amazon), Amazon CloudWatch Evidly, Amazon Forecast,,, (IAM EC2) AWS Organizations, Amazon Managed Streaming for Apache Kafka AWS Identity and Access Managemen t (Amazon MSK), Amazon Lightsail, Amazon CloudWatc h Logs,,, Amazon Pinpoint, Amazon Virtual Private Cloud (AWS IoT Greengras s AWS Ground Station AWS Elemental MediaConnect AWS Elemental MediaTail or Amazon VPC), Amazon Personalize, Amazon QuickSight AWS Migration Hub Refactor Spaces, Amazon Simple Storage Service (Amazon S3), Amazon	13. Juni 2023

Änderung	Beschreibung	Datum
tasetGroup", "forecast :ListDatasetGroups", "greengrass:DescribeComponent", "greengrass:GetComponent", "greengrass:ListComponents", "greengrass:ListComponentVersions", "groundstation:GetMissionProfile", "groundstation:ListMissionProfiles", "iam:ListGroups", "iam:ListRoles", "kafka:DescribeConfiguration", "kafka:DescribeConfigurationRevision", "kafka:ListConfigurations", "lightsail:GetRelationalDatabases" "logs:ListTagsLogGroup", "mediaconnect:DescribeFlow", "mediaconnect:ListFlows", "mediatailor:GetPlaybackConfiguration", "mediatailor:ListPlaybackConfigurations", "mobiletargeting:GetApplicationSettings", "mobiletargeting:GetEmailTemplate", "mobiletargeting:GetEventStream", "mobiletargeting:ListTemplates", "networkmanager:GetCustomerGatewayAssociations", "networkmanager:GetLinkAssociations", "organizations:DescribeAccount", "organizations:DescribeOrganizationalUnit", "organizations:ListAccounts",	SageMaker AI,. AWS Transfer Family	

Änderung	Beschreibung	Datum
"organizations:ListAccounts ForParent", "organizations:L istOrganizationalUnitsForPa rent", "organizations:ListTa gsForResource", "personal ize:DescribeDataset", "perso nalize:DescribeDatasetGroup", "personalize:DescribeSchema ", "personalize:DescribeSolu tion", "personalize:ListD atasetGroups", "personalize: ListDatasetImportJobs", "personalize:ListDatasets", "personalize:ListSchemas", "personalize:ListSolutions", "personalize:ListTagsForRe source", "quicksight:ListTe mplates", "refactor-spaces:G etEnvironment", "refactor -spaces:GetService", "refactor-spaces:ListAppl ications", "refactor-spaces: ListEnvironments", "refactor -spaces:ListServices", "s3:GetAccessPointPolic yStatusForObjectLambda", "sagemaker:DescribeDe viceFleet", "sagemake r:DescribeFeatureGroup", "sa gemaker:ListDeviceFleets", "sagemaker:ListFeatureGroup s", "sagemaker:ListModels", and "transfer:ListTags ForResource"		

Änderung	Beschreibung	Datum
AWSConfigServiceRolePolicy – Addition: "amplify:GetBranch", "amplify:ListBranches", "app-integrations:GetEventIntegration", "app-integrations:ListEventIntegrationAssociations", "app-integrations:ListEventIntegrations", "appmesh:DescribeRoute", "appmesh:ListRoutes", "aps:ListRuleGroupsNamespaces", "athena:GetPreparedStatement", "athena:ListPreparedStatements", "batch:DescribeSchedulingPolicies", "batch:ListSchedulingPolicies", "cloudformation:ListTypes", "cloudtrail:ListTrails", "codeartifact:ListDomains", "codeguru-profiler:DescribeProfilingGroup", "codeguru-profiler:GetNotificationConfiguration", "codeguru-profiler:GetPolicy", "codeguru-profiler:ListProfilingGroups", "ds:DescribeDomainControllers", "dynamodb:DescribeTableReplicaAutoScaling", "dynamodb:DescribeTimeToLive", "ec2:DescribeTrafficMirrorFilters", "evidently:GetLaunch", "evidently:ListLaunches", "forecast:DescribeDatasetGroup", "forecast	Diese Richtlinie unterstützt jetzt zusätzliche Berechtigungen für Amazon Connect AWS Amplify, Amazon Managed Service for Prometheus AWS App Mesh, Amazon Athena,,,,, Amazon AWS Batch, Amazon DynamoDB AWS CloudFormation AWS CloudTrail AWS CodeArtifact CodeGuru AWS Directory Service, Amazon Elastic Compute Cloud (Amazon), Amazon CloudWatch Evidly, Amazon Forecast,,, (IAM EC2) AWS Organizations, Amazon Managed Streaming for Apache Kafka AWS Identity and Access Management (Amazon MSK), Amazon Lightsail, Amazon CloudWatch Logs,,, Amazon Pinpoint, Amazon Virtual Private Cloud (AWS IoT Greengrass AWS Ground Station AWS Elemental MediaConnect AWS Elemental MediaTailor Amazon VPC), Amazon Personalize, Amazon QuickSight AWS Migration Hub Refactor Spaces, Amazon Simple Storage Service (Amazon S3), Amazon	13. Juni 2023

Änderung	Beschreibung	Datum
:ListDatasetGroups", "greengrass:DescribeComponent", "greengrass:GetComponent", "greengrass:ListComponents", "greengrass:ListComponentVersions", "groundstation:GetMissionProfile", "groundstation:ListMissionProfiles", "iam:ListGroups", "iam:ListRoles", "kafka:DescribeConfiguration", "kafka:DescribeConfigurationRevision", "kafka:ListConfigurations", "lightsail:GetRelationalDatabases", "logs:ListTagsLogGroup", "mediaconnect:DescribeFlow", "mediaconnect:ListFlows", "mediatailor:GetPlaybackConfiguration", "mediatailor:ListPlaybackConfigurations", "mobiletargeting:GetApplicationSettings", "mobiletargeting:GetEmailTemplate", "mobiletargeting:GetEventStream", "mobiletargeting:ListTemplates", "networkmanager:GetCustomerGatewayAssociations", "networkmanager:GetLinkAssociations", "organizations:DescribeAccount", "organizations:DescribeOrganizationalUnit", "organizations:ListAccounts", "organizations:ListAccounts	SageMaker AI,. AWS Transfer Family	

Änderung	Beschreibung	Datum
ForParent", "organizations:ListOrganizationalUnitsForParent", "organizations:ListTagsForResource", "personalize:DescribeDataset", "personalize:DescribeDatasetGroup", "personalize:DescribeSchema", "personalize:DescribeSolution", "personalize:ListDatasetGroups", "personalize:ListDatasetImportJobs", "personalize:ListDatasets", "personalize:ListSchemas", "personalize:ListSolutions", "personalize:ListTagsForResource", "quicksight:ListTemplates", "refactor-spaces:GetEnvironment", "refactor-spaces:GetService", "refactor-spaces:ListApplications", "refactor-spaces:ListEnvironments", "refactor-spaces:ListServices", "s3:GetAccessPointPolicyStatusForObjectLambda", "sagemaker:DescribeDeviceFleet", "sagemaker:DescribeFeatureGroup", "sagemaker:ListDeviceFleets", "sagemaker:ListFeatureGroups", "sagemaker:ListModels", and "transfer:ListTagsForResource"		

Änderung	Beschreibung	Datum
AWSConfigServiceRolePolicy – Addition: amplify:GetApp, amplify:ListApps, appmesh:DescribeVirtualGateway, appmesh:DescribeVirtualNode, appmesh:DescribeVirtualRouter, appmesh:DescribeVirtualService, appmesh:ListMeshes, appmesh:ListTagsForResource, appmesh:ListVirtualGateways, appmesh:ListVirtualNodes, appmesh:ListVirtualRouters, appmesh:ListVirtualServices, apprunner:DescribeVpcConnector, apprunner:ListVpcConnectors, cloudformation:ListTypes, cloudfront:ListResponseHeadersPolicies, codeartifact:ListRepositories, ds:DescribeEventTopics, ds:ListLogSubscriptions, GetInstanceTypesFromInstanceRequirement ec2:GetManagedPrefixListEntries, kendra:DescribeIndex, kendra:ListIndices, kendra:ListTagsForResource, logs:DescribeDestinations, logs:GetDataProtectionPolicy, macie2:DescribeOrganizationConfiguration, macie2:GetAutomatedDiscoveryConfigurat	Diese Richtlinie unterstützt jetzt zusätzliche Berechtigungen für Amazon Managed Workflows für AWS Amplify, AWS App Mesh, AWS App Runner, Amazon CloudFront AWS CodeArtifact, Amazon Elastic Compute Cloud, Amazon Kendra, Amazon Macie, Amazon Route 53, Amazon SageMaker AI, Amazon Pinpoint AWS Transfer Family,, AWS Migration Hub AWS Resilience Hub, Amazon CloudWatch, AWS Directory Service und. AWS WAF	13. April 2023

Änderung	Beschreibung	Datum
ion, macie2:GetClassificationExportConfiguration, macie2:GetCustomDataIdentifier, macie2:GetFindingsPublicationConfiguration, macie2:ListCustomDataIdentifiers, mobiletargeting:GetEmailChannel, refactor-spaces:GetEnvironment, refactor-spaces:ListEnvironments, resiliencehub:ListTagsForResource, route53:GetDNSSEC, sagemaker:DescribeDomain, sagemaker:DescribeModelBiasJobDefinition, sagemaker:DescribeModelQualityJobDefinition, sagemaker:DescribePipeline, sagemaker:DescribeProject, sagemaker:ListDomains, sagemaker:ListModelBiasJobDefinitions, sagemaker:ListModelQualityJobDefinitions, sagemaker:ListPipelines, sagemaker:ListProjects, transfer:DescribeAgreement, transfer:DescribeCertificate, transfer:ListAgreements, transfer:ListCertificates, and waf-regional:ListLoggingConfigurations		

Änderung	Beschreibung	Datum
AWS_ConfigRole – Addition: amplify:GetApp, amplify:ListApps, appmesh:DescribeVirtualGateway, appmesh:DescribeVirtualNode, appmesh:DescribeVirtualRouter, appmesh:DescribeVirtualService, appmesh:ListMeshes, appmesh:ListTagsForResource, appmesh:ListVirtualGateways, appmesh:ListVirtualNodes, appmesh:ListVirtualRouters, appmesh:ListVirtualServices, apprunner:DescribeVpcConnector, apprunner:ListVpcConnectors, cloudformation:ListTypes, cloudfront:ListResponseHeadersPolicies, codeartifact:ListRepositories, ds:DescribeEventTopics, ds:ListLogSubscriptions, ec2:GetInstanceTypesFromInstanceRequirement, ec2:GetManagedPrefixListEntries, kendra:DescribeIndex, kendra:ListIndices, kendra:ListTagsForResource, logs:DescribeDestinations, logs:GetDataProtectionPolicy, macie2:DescribeOrganizationConfiguration, macie2:GetAutomatedDiscoveryConfiguration, macie2:GetClassificatio	Diese Richtlinie unterstützt jetzt zusätzliche Berechtigungen für Amazon Managed Workflows für AWS Amplify, AWS App Mesh, AWS App Runner, Amazon CloudFront AWS CodeArtifact, Amazon Elastic Compute Cloud, Amazon Kendra, Amazon Macie, Amazon Route 53, Amazon SageMaker AI, Amazon Pinpoint AWS Transfer Family,, AWS Migration Hub AWS Resilience Hub, Amazon CloudWatch, AWS Directory Service und. AWS WAF	13. April 2023

Änderung	Beschreibung	Datum
nExportConfiguration, macie2:GetCustomDataIdentifier, macie2:GetFindingsPublicationConfiguration, macie2:ListCustomDataIdentifiers, mobiletargeting:GetEmailChannel, refactor-spaces:GetEnvironment, refactor-spaces:ListEnvironments, resiliencehub:ListTagsForResource, route53:GetDNSSEC, sagemaker:DescribeDomain, sagemaker:DescribeModelBiasJobDefinition, sagemaker:DescribeModelQualityJobDefinition, sagemaker:DescribePipeline, sagemaker:DescribeProject, sagemaker:ListDomains, sagemaker:ListModelBiasJobDefinitions, sagemaker:ListModelQualityJobDefinitions, sagemaker:ListPipelines, sagemaker:ListProjects, transfer:DescribeAgreement, transfer:DescribeCertificate, transfer:ListAgreements, transfer:ListCertificates, and waf-regional:ListLoggingConfigurations		

Änderung	Beschreibung	Datum
AWSConfigServiceRolePolicy – Addition: appflow:DescribeFlow, appflow:ListFlows, appflow:ListTagsForResource, apprunner:DescribeService, apprunner:ListServices, apprunner:ListTagsForResource, appstream:DescribeApplications, appstream:DescribeFleets, cloudfront:GetResponseHeadersPolicy, cloudwatch:ListTagsForResource, codeartifact:DescribeRepository, codeartifact:GetRepositoryPermissionsPolicy, codeartifact:ListTagsForResource, codecommit:GetRepository, codecommit:GetRepositoryTriggers, codecommit:ListRepositories, codecommit:ListTagsForResource, devicefarm:GetInstanceProfile, devicefarm:ListInstanceProfiles, devicefarm:ListProjects, evidently:GetProject, evidently:ListProjects, evidently:ListTagsForResource, forecast:DescribeDataset, forecast:ListDatasets, forecast:ListTagsForResource, groundstation:GetConfig, groundstation:ListConfigs, groundstation:ListTagsForResource, iam:GetInstancePro	Diese Richtlinie unterstützt jetzt zusätzliche Berechtigungen für Amazon Managed Workflows für Amazon AppFlow, Amazon AppStream 2.0 AWS App Runner, Amazon, Amazon, CloudFront,, CloudWatch AWS CodeArtifact, Amazon CloudWatch Evidly AWS CodeCommit AWS Device Farm, Amazon Forecast, AWS Identity and Access Management (IAM) AWS Ground Station,, Amazon MemoryDB AWS IoT, Amazon Pinpoint,,, Amazon Relational Database Service (Amazon RDS), Amazon Redshift und Amazon AI. AWS Network Manager AWS Panorama SageMaker	30. März 2023

Änderung	Beschreibung	Datum
file, iam:GetSAMLProvider, iam:GetServerCertificate, iam:ListAccessKeys, iam:ListGroups, iam:ListInstanceProfiles, iam:ListMFADevices, iam:ListMFADeviceTags, iam:ListRoles, iam:ListSAMLProviders, iot:DescribeFleetMetric, iot:ListFleetMetrics, memorydb:DescribeUsers, memorydb:ListTags, mobiletargeting:GetApp, mobiletargeting:GetCampaigns, networkmanager:GetDevices, networkmanager:GetLinks, networkmanager:GetSites, panorama:ListNodes, rds:DescribeDBProxyEndpoints, redshift:DescribeScheduledActions, sagemaker:DescribeAppImageConfig, sagemaker:DescribeImage, sagemaker:DescribeImageVersion, sagemaker:ListAppImageConfigs, sagemaker:ListImages, and sagemaker:ListImageVersions		

Änderung	Beschreibung	Datum
AWS_ConfigRole – Addition: appflow:DescribeFlow, appflow:ListFlows, appflow:ListTagsForResource, apprunner:DescribeService, apprunner:ListServices, apprunner:ListTagsForResource, appstream:DescribeApplications, appstream:DescribeFleets, cloudformation:ListTypes, cloudfront:GetResponseHeadersPolicy, cloudfront:ListDistributions, cloudwatch:ListTagsForResource, codeartifact:DescribeRepository, codeartifact:GetRepositoryPermissionsPolicy, codeartifact:ListTagsForResource, codecommit:GetRepository, codecommit:GetRepositoryTriggers, codecommit:ListRepositories, codecommit:ListTagsForResource, devicefarm:GetInstanceProfile, devicefarm:ListInstanceProfiles, devicefarm:ListProjects, ec2:DescribeTrafficMirrorFilters, evidently:GetProject, evidently:ListProjects, evidently:ListTagsForResource, forecast:DescribeDataset, forecast:ListDatasets, forecast:ListTagsForResource, groundstation:GetConfig,	Diese Richtlinie unterstützt jetzt zusätzliche Berechtigungen für Amazon Managed Workflows for Amazon AppFlow, Amazon AppStream 2.0 AWS App Runner, Amazon, Amazon AWS CloudFormation,, CloudFront, CloudWatch AWS CodeArtifact AWS CodeCommit AWS Device Farm, Amazon Elastic Compute Cloud (Amazon EC2), Amazon CloudWatch Evidently, Amazon Forecast, AWS Identity and Access Management (IAM) AWS Ground Station,, Amazon MemoryDB AWS IoT, Amazon Pinpoint,,, Amazon Relational Database Service (Amazon RDS) AWS Panorama, Amazon Redshift und Amazon AI. AWS Network Manager SageMaker	30. März 2023

Änderung	Beschreibung	Datum
groundstation:ListConfigs, groundstation:ListTagsForResource, iam:GetInstanceProfile, iam:GetSAMLProvider, iam:GetServerCertificate, iam:ListAccessKeys, iam:ListGroups, iam:ListInstanceProfiles, iam:ListMFADevices, iam:ListMFADeviceTags, iam:ListRoles, iam:ListSAMLProviders, iot:DescribeFleetMetric, iot:ListFleetMetrics, memorydb:DescribeUsers, memorydb:ListTags, mobiletargeting:GetApp, mobiletargeting:GetCampaigns, networkmanager:GetDevices, networkmanager:GetLinks, networkmanager:GetSites, panorama:ListNodes, rds:DescribeDBProxyEndpoints, redshift:DescribeScheduledActions, sagemaker:DescribeAppImageConfig, sagemaker:DescribeImage, sagemaker:DescribeImageVersion, sagemaker:ListAppImageConfigs, sagemaker:ListImages, and sagemaker:ListImageVersions		

Änderung	Beschreibung	Datum
AWSConfigRulesExecutionRole— beginnt AWS Config mit der Nachverfolgung von Änderungen für diese verwaltete Richtlinie AWS	Diese Richtlinie ermöglicht AWS Lambda Funktionen den Zugriff auf die AWS Config API und die Konfigurations-Snapshots, die regelmäßig AWS Config an Amazon S3 gesendet werden. Dieser Zugriff ist für Funktionen erforderlich, die Konfigurationsänderungen für AWS benutzerdefinierte Lambda-Regeln auswerten.	7. März 2023
AWSConfigRoleForOrganizations— AWS Config beginnt mit der Nachverfolgung von Änderungen für diese AWS verwaltete Richtlinie	Diese Richtlinie ermöglicht das Aufrufen AWS Config im Nur-Lese-Modus AWS Organizations APIs.	7. März 2023
AWSConfigRemediationServiceRolePolicy— AWS Config beginnt mit der Nachverfolgung von Änderungen für diese verwaltete Richtlinie AWS	Diese Richtlinie ermöglicht es AWS Config , `NON_COMPLIANT` Ressourcen in Ihrem Namen zu korrigieren.	7. März 2023
AWSConfigServiceRolePolicy – Addition: auditmanager:GetAccountStatus	Diese Richtlinie gewährt nun die Berechtigung, den Registrierungsstatus eines Kontos in AWS Audit Manager wiederherzustellen.	03. März 2023

Änderung	Beschreibung	Datum
AWS_ConfigRole – Addition: auditmanager:GetAccountStatus	Diese Richtlinie gewährt nun die Berechtigung, den Registrierungsstatus eines Kontos in AWS Audit Manager wiederherzustellen.	03. März 2023
AWSConfigMultiAccountSetupPolicy— AWS Config beginnt mit der Nachverfolgung von Änderungen für diese AWS verwaltete Richtlinie	Diese Richtlinie ermöglicht AWS Config das Aufrufen von AWS Diensten und die Bereitstellung von AWS Config Ressourcen in einer Organisation mit AWS Organizations.	27. Februar 2023

Änderung	Beschreibung	Datum
AWSConfigServiceRolePolicy – Addition: airflow:ListTagsForResource, iot:ListCustomMetrics, iot:DescribeCustomMetric, appstream:DescribeDirectoryConfigs, appstream:ListTagsForResource, codeguru-reviewer:DescribeRepositoryAssociation, codeguru-reviewer:ListRepositoryAssociations, healthlake:ListFHIRDatastores, healthlake:DescribeFHIRDatastore, healthlake:ListTagsForResource, kinesisvideo:DescribeStream, kinesisvideo:ListStreams, kinesisvideo:ListTagsForStream, kinesisvideo:DescribeSignalingChannel, kinesisvideo:ListTagsForResource, kinesisvideo:ListSignalingChannels, route53-recovery-control-config:DescribeCluster, route53-recovery-control-config:DescribeRoutingControl, route53-recovery-control-config:DescribeSafetyRule, route53-recovery-control-config:ListClusters, route53-recovery-control-config:ListRoutingControls, route53-recovery-control-config:ListSafetyRules, devicefarm:GetTestGridProject, devicefar	Diese Richtlinie unterstützt jetzt zusätzliche Berechtigungen für Amazon Managed Workflows for Apache Airflow AWS IoT, Amazon AppStream 2.0, Amazon CodeGuru Reviewer AWS HealthLake, Amazon Kinesis Video Streams, Amazon Application Recovery Controller (ARC) AWS Device Farm, Amazon Elastic Compute Cloud (Amazon EC2), Amazon Pinpoint AWS Identity and Access Management (IAM) GuardDuty, Amazon und Amazon Logs. CloudWatch	1. Februar 2023

Änderung	Beschreibung	Datum
m:ListTestGridProjects, ec2:DescribeCapacityReservationFleets, ec2:DescribeIpamPools, ec2:DescribeIpams, ec2:GetInstanceTypesFromInstanceRequirement, mobiletargeting:GetApplicationSettings, mobiletargeting:ListTagsForResource, ecr:BatchGetRepositoryScanningConfiguration, iam:ListServerCertificates, guardduty:ListPublishingDestinations, guardduty:DescribePublishingDestination, logs:GetLogDelivery, and logs:ListLogDeliveries		

Änderung	Beschreibung	Datum
AWS_ConfigRole – Addition: airflow:ListTagsForResource, iot:ListCustomMetrics, iot:DescribeCustomMetric, appstream:DescribeDirectoryConfigs, appstream:ListTagsForResource, codeguru-reviewer:DescribeRepositoryAssociation, codeguru-reviewer:ListRepositoryAssociations, healthlake:ListFHIRDatastores, healthlake:DescribeFHIRDatastore, healthlake:ListTagsForResource, kinesisvideo:DescribeStream, kinesisvideo:ListStreams, kinesisvideo:ListTagsForStream, kinesisvideo:DescribeSignalingChannel, kinesisvideo:ListTagsForResource, kinesisvideo:ListSignalingChannels, route53-recovery-control-config:DescribeCluster, route53-recovery-control-config:DescribeRoutingControl, route53-recovery-control-config:DescribeSafetyRule, route53-recovery-control-config:ListClusters, route53-recovery-control-config:ListRoutingControls, route53-recovery-control-config:ListSafetyRules, devicefarm:GetTestGridProject, devicefar	Diese Richtlinie unterstützt jetzt zusätzliche Berechtigungen für Amazon Managed Workflows for Apache Airflow AWS IoT, Amazon AppStream 2.0, Amazon CodeGuru Reviewer AWS HealthLake, Amazon Kinesis Video Streams, Amazon Application Recovery Controller (ARC) AWS Device Farm, Amazon Elastic Compute Cloud (Amazon EC2), Amazon Pinpoint AWS Identity and Access Management (IAM) GuardDuty, Amazon und Amazon Logs. CloudWatch	1. Februar 2023

Änderung	Beschreibung	Datum
m:ListTestGridProjects, ec2:DescribeCapacityReservationFleets, ec2:DescribeIpamPools, ec2:DescribeIpams, ec2:GetInstanceTypesFromInstanceRequirement, mobiletargeting:GetApplicationSettings, mobiletargeting:ListTagsForResource, ecr:BatchGetRepositoryScanningConfiguration, iam:ListServerCertificates, guardduty:ListPublishingDestinations, guardduty:DescribePublishingDestination, logs:GetLogDelivery, and logs:ListLogDeliveries		
ConfigConformsServiceRolePolicy – Aktualisierung: config:DescribeConfigRules	Als bewährte Sicherheitsmethode entfernt diese Richtlinie nun umfassende Berechtigungen auf Ressourcenebene für `config:DescribeConfigRules` .	12. Januar 2023

Änderung	Beschreibung	Datum
AWSConfigServiceRolePolicy – Addition: APS:DescribeRuleGroupsNamespace, APS:DescribeWorkspace, APS:ListWorkspaces, auditmanager:GetAssessment, auditmanager:ListAssessments, devicefarm:GetNetworkProfile, AWS Transfer Family devicefarm:GetProject, devicefarm:ListNetworkProfiles, devicefarm:ListTagsForResource, dms:DescribeEndpoints, ds:ListTagsForResource, ec2:DescribeTags, ec2:DescribeTrafficMirrorSessions, ec2:DescribeTrafficMirrorTargets, ec2:GetIpamPoolAllocations, ec2:GetIpamPoolCidrs, glue:GetMLTransform, glue:GetMLTransforms, glue:ListMLTransforms, iot:DescribeScheduledAudit, iot:ListScheduledAudits, ivs:GetChannel, lightsail:GetRelationalDatabases, mediapackage-vod:DescribePackagingConfiguration, mediapackage-vod:ListPackagingConfigurations, networkmanager:DescribeGlobalNetworks, networkmanager:GetTransitGatewayRegistrat	Diese Richtlinie unterstützt jetzt zusätzliche Berechtigungen für Amazon Managed Service for Prometheus,, AWS Audit Manager AWS Device Farm, AWS Database Migration Service (AWS DMS) AWS Directory Service, Amazon Elastic Compute Cloud (Amazon EC2),, AWS Glue AWS IoT, Amazon Lightsail,,, Amazon AWS Elemental MediaPackage AWS Network Manager QuickSight, Amazon Application Recovery Controller (ARC) AWS Resource Access Manager, Amazon Simple Storage Service (Amazon S3) und Amazon Timestream.	15. Dezember 2022

Änderung	Beschreibung	Datum
ions, networkmanager:ListTagsForResource, quicksight:DescribeDashboard, quicksight:DescribeDashboardPermissions, quicksight:DescribeTemplate, quicksight:DescribeTemplatePermissions, quicksight:ListDashboards, quicksight:ListTemplates, ram:ListResources, route53-recovery-control-config:DescribeControlPanel, route53-recovery-control-config:ListControlPanels, route53-recovery-control-config:ListTagsForResource, route53resolver:GetResolverQueryLogConfigAssociation, route53resolver:ListResolverQueryLogConfigAssociations, s3:GetAccessPointForObjectLambda, s3:GetAccessPointPolicyForObjectLambda, s3:GetAccessPointPolicyStatusForObjectLambda, s3:GetMultiRegionAccessPoint, s3:ListAccessPointsForObjectLambda, s3:ListMultiRegionAccessPoints, timestream:DescribeEndpoints, transfer:DescribeConnector, transfer:ListConnectors, and transfer:ListTagsForResource		

Änderung	Beschreibung	Datum
AWS_ConfigRole – Addition: APS:DescribeRuleGroupsNamespace, APS:DescribeWorkspace, APS:ListWorkspaces, auditmanager:GetAssessment, auditmanager:ListAssessments, devicefarm:GetNetworkProfile, devicefarm:GetProject, devicefarm:ListNetworkProfiles, devicefarm:ListTagsForResource, dms:DescribeEndpoints, ds:ListTagsForResource, ec2:DescribeTags, ec2:DescribeTrafficMirrorSessions, ec2:DescribeTrafficMirrorTargets, ec2:GetIpamPoolAllocations, ec2:GetIpamPoolCidrs, glue:GetMLTransform, glue:GetMLTransforms, glue:ListMLTransforms, iot:DescribeScheduledAudit, iot:ListScheduledAudits, ivs:GetChannel, lightsail:GetRelationalDatabases, mediapackage-vod:DescribePackagingConfiguration, mediapackage-vod:ListPackagingConfigurations, networkmanager:DescribeGlobalNetworks, networkmanager:GetTransitGatewayRegistrations, networkmanager:ListTa	Diese Richtlinie unterstützt jetzt zusätzliche Berechtigungen für Amazon Managed Service for Prometheus,, AWS Audit Manager AWS Device Farm, AWS Database Migration Service (AWS DMS) AWS Directory Service, Amazon Elastic Compute Cloud (Amazon EC2),, AWS Glue AWS IoT, Amazon Lightsail,,, Amazon AWS Elemental MediaPackage AWS Network Manager QuickSight, Amazon Application Recovery Controller (ARC) AWS Resource Access Manager, Amazon Simple Storage Service (Amazon S3) und Amazon Timestream.	15. Dezember 2022

Änderung	Beschreibung	Datum
gsForResource, quicksight:DescribeDashboard, quicksight:DescribeDashboardPermissions, quicksight:DescribeTemplate, quicksight:DescribeTemplatePermissions, quicksight:ListDashboards, quicksight:ListTemplates, ram:ListResources, route53-recovery-control-config:DescribeControlPanel, route53-recovery-control-config:ListControlPanels, route53-recovery-control-config:ListTagsForResource, route53resolver:GetResolverQueryLogConfigAssociation, route53resolver:ListResolverQueryLogConfigAssociations, s3:GetAccessPointForObjectLambda, s3:GetAccessPointPolicyForObjectLambda, s3:GetAccessPointPolicyStatusForObjectLambda, s3:GetMultiRegionAccessPoint, s3:ListAccessPointsForObjectLambda, s3:ListMultiRegionAccessPoints, timestream:DescribeEndpoints, transfer:DescribeConnector, transfer:ListConnectors, and transfer:ListTagsForResource		

Änderung	Beschreibung	Datum
AWSConfigServiceRolePolicy – Addition: cloudformation:ListStackResources and cloudformation:ListStacks	Diese Richtlinie gewährt nun die Erlaubnis, Beschreibungen aller Ressourcen eines angegebenen AWS CloudFormation Stacks und die zusammenfassenden Informationen für Stacks zurückzugeben, deren Status dem angegebenen entspricht. StackStatusFilter	7. November 2022
AWS_ConfigRole – Addition: cloudformation:ListStackResources and cloudformation:ListStacks	Diese Richtlinie gewährt nun die Erlaubnis, Beschreibungen aller Ressourcen eines angegebenen AWS CloudFormation Stacks und die zusammenfassenden Informationen für Stapel zurückzugeben, deren Status dem angegebenen entspricht. StackStatusFilter	7. November 2022

Änderung	Beschreibung	Datum
AWSConfigServiceRolePolicy – Addition: acm-pca:GetCertificateAuthorityCsr, acm-pca:ListCertificateAuthorities, acm-pca:ListTags, airflow:GetEnvironment, airflow:ListEnvironments, amplifyuibuilder:ListThemes, appconfig:ListConfigurationProfiles, appconfig:ListDeployments, appconfig:ListDeploymentStrategies, appconfig:ListEnvironments, appconfig:ListHostedConfigurationVersions, cassandra:Select, cloudwatch:DescribeAnomalyDetectors, cloudwatch:GetDashboard, cloudwatch:ListDashboards, connect:DescribePhoneNumber, connect:ListPhoneNumbers, connect:ListPhoneNumbersV2, connect:SearchAvailablePhoneNumbers, databrew:DescribeDataset, databrew:DescribeJob, databrew:DescribeProject, databrew:DescribeRecipe, databrew:DescribeRuleset, databrew:DescribeSchedule, databrew:ListDatasets, databrew:ListJobs, databrew:ListProjects, databrew:ListRecipes, databrew:ListRecipeVers	Diese Richtlinie unterstützt jetzt zusätzliche Berechtigungen für AWS Certificate Manager Amazon Managed Workflows for Apache Airflow,, AWS Amplify AWS AppConfig, Amazon Keyspaces, Amazon, Amazon Connect CloudWatch AWS Glue DataBrew, Amazon Elastic Compute Cloud (Amazon EC2), Amazon Elastic Kubernetes Service (Amazon EKS), Amazon, Amazon Fraud Detector EventBridge AWS Fault Injection Service, Amazon, Amazon GameLift Servers FSx, Amazon Location Service, Amazon Lex, Amazon Lightsail AWS IoT, Amazon Pinpoint,,,, Amazon, Amazon Relational Database AWS OpsWorks AWS Panorama AWS Resource Access Manager QuickSight Service (Amazon RDS), Amazon Rekognition, AWS RoboMaker, AWS Resource Groups, Amazon Route 53, Amazon Simple Storage Service (Amazon S3) AWS Cloud Map, und. AWS Security Token Service	19. Oktober 2022

Änderung	Beschreibung	Datum
ions, databrew:ListRulesets, databrew:ListSchedules, ec2:DescribeRouteTables, eks:DescribeAddon, eks:DescribeIdentityProviderConfig, eks:ListAddons, eks:ListIdentityProviderConfigs, events:DescribeConnection, events:ListApiDestinations, events:ListConnections, fis:GetExperimentTemplate, fis:ListExperimentTemplates, frauddetector:GetRules, fsx:DescribeBackups, fsx:DescribeSnapshots, fsx:DescribeStorageVirtualMachines, gamelift:DescribeMatchmakingRuleSets, gamelift:DescribeVpcPeeringConnections, geo:ListGeofenceCollections, geo:ListPlaceIndexes, geo:ListRouteCalculators, geo:ListTrackers, iot:DescribeAccountAuditConfiguration, iot:DescribeAuthorizer, iot:DescribeDomainConfiguration, iot:DescribeMitigationAction, iot:ListAuthorizers, iot:ListDomainConfigurations, iot:ListMitigationActions, iotsitewise:DescribeAssetModel, iotsitewise:DescribeDashboard, iotsitewise:DescribeGateway, iotsitewise:DescribePortal, iotsitewi		

Änderung	Beschreibung	Datum
se:DescribeProject, iotsite wise:ListAssetModels, iotsitewi se:ListDashboards, iotsitew ise:ListGateways, iotsitewi se:ListPortals, iotsitewise :ListProjectAssets, iotsitewi se:ListProjects, iotsitewis e:ListTagsForResource, iotwireless:GetServiceProfi le, iotwireless:GetWireless Device, iotwireless:GetWire lessGatewayTaskDefinition, iotwireless:ListServiceProf iles, iotwireless:ListTagsF orResource, iotwireless:Lis tWirelessDevices, iotwirele ss:ListWirelessGatewayTaskD efinitions, lex:DescribeBot Version, lex:ListBotVersions, lightsail:GetContainerServices, lightsail:GetDistributions, lightsail:GetRelationalDat abase, lightsail:GetRelatio nalDatabaseParameters, mobiletargeting:GetApps, mobiletargeting:GetCampaign , mobiletargeting:GetSegmen t, mobiletargeting:Ge tSegments, opsworks:Describ eInstances, opsworks:Descri beTimeBasedAutoScaling, opsworks:DescribeVolumes, panorama:DescribeApplication Instance, panorama:Describe ApplicationInstanceDetails,		

Änderung	Beschreibung	Datum
panorama:DescribePackage, panorama:DescribePackageVersion, panorama:ListApplicationInstances, panorama:ListPackages, quicksight:ListDataSources, ram:ListResourceSharePermissions, rds:DescribeDBProxies, rds:DescribeGlobalClusters, rekognition:ListStreamProcessors, resource-groups:GetGroup, resource-groups:GetGroupConfiguration, resource-groups:GetGroupQuery, resource-groups:GetTags, resource-groups:ListGroupResources, resource-groups:ListGroups, robomaker:ListRobotApplications, robomaker:ListSimulationApplications, route53resolver:GetResolverDnssecConfig, route53resolver:ListResolverDnssecConfigs, s3:ListStorageLensConfigurations, schemas:GetResourcePolicy, servicediscovery:ListInstances, sts:GetCallerIdentity, synthetics:GetGroup, synthetics:ListAssociatedGroups, synthetics:ListGroupResources, and synthetics:ListGroups		

Änderung	Beschreibung	Datum
AWS_ConfigRole – Addition: acm-pca:GetCertificateAuthorityCsr, acm-pca:ListCertificateAuthorities, acm-pca:ListTags, airflow:GetEnvironment, airflow:ListEnvironments, amplifyuibuilder:ListThemes, appconfig:ListConfigurationProfiles, appconfig:ListDeployments, appconfig:ListDeploymentStrategies, appconfig:ListEnvironments, appconfig:ListHostedConfigurationVersions, cassandra:Select, cloudwatch:DescribeAnomalyDetectors, cloudwatch:GetDashboard, cloudwatch:ListDashboards, connect:DescribePhoneNumber, connect:ListPhoneNumbers, connect:ListPhoneNumbersV2, connect:SearchAvailablePhoneNumbers, databrew:DescribeDataset, databrew:DescribeJob, databrew:DescribeProject, databrew:DescribeRecipe, databrew:DescribeRuleset, databrew:DescribeSchedule, databrew:ListDatasets, databrew:ListJobs, databrew:ListProjects, databrew:ListRecipes, databrew:ListRecipeVers	Diese Richtlinie unterstützt jetzt zusätzliche Berechtigungen für AWS Certificate Manager Amazon Managed Workflows for Apache Airflow,, AWS Amplify AWS AppConfig, Amazon Keyspaces, Amazon, Amazon Connect CloudWatch AWS Glue DataBrew, Amazon Elastic Compute Cloud (Amazon EC2), Amazon Elastic Kubernetes Service (Amazon EKS), Amazon, Amazon Fraud Detector EventBridge AWS Fault Injection Service, Amazon, Amazon GameLift Servers FSx, Amazon Location Service, Amazon Lex, Amazon Lightsail AWS IoT, Amazon Pinpoint,,,, Amazon, Amazon Relational Database AWS OpsWorks AWS Panorama AWS Resource Access Manager QuickSight Service (Amazon RDS), Amazon Rekognition, AWS RoboMaker, AWS Resource Groups, Amazon Route 53, Amazon Simple Storage Service (Amazon S3) AWS Cloud Map, und. AWS Security Token Service	19. Oktober 2022

Änderung	Beschreibung	Datum
ions, databrew:ListRulesets, databrew:ListSchedules, ec2:DescribeRouteTables, eks:DescribeAddon, eks:DescribeIdentityProviderConfig, eks:ListAddons, eks:ListIdentityProviderConfigs, events:DescribeConnection, events:ListApiDestinations, events:ListConnections, fis:GetExperimentTemplate, fis:ListExperimentTemplates, frauddetector:GetRules, fsx:DescribeBackups, fsx:DescribeSnapshots, fsx:DescribeStorageVirtualMachines, gamelift:DescribeMatchmakingRuleSets, gamelift:DescribeVpcPeeringConnections, geo:ListGeofenceCollections, geo:ListPlaceIndexes, geo:ListRouteCalculators, geo:ListTrackers, iot:DescribeAccountAuditConfiguration, iot:DescribeAuthorizer, iot:DescribeDomainConfiguration, iot:DescribeMitigationAction, iot:ListAuthorizers, iot:ListDomainConfigurations, iot:ListMitigationActions, iotsitewise:DescribeAssetModel, iotsitewise:DescribeDashboard, iotsitewise:DescribeGateway, iotsitewise:DescribePortal, iotsitewi		

Änderung	Beschreibung	Datum
se:DescribeProject, iotsite wise:ListAssetModels, iotsitewi se:ListDashboards, iotsitew ise:ListGateways, iotsitewi se:ListPortals, iotsitewise :ListProjectAssets, iotsitewi se:ListProjects, iotsitewis e:ListTagsForResource, iotwireless:GetServiceProfi le, iotwireless:GetWireless Device, iotwireless:GetWire lessGatewayTaskDefinition, iotwireless:ListServiceProf iles, iotwireless:ListTagsF orResource, iotwireless:Lis tWirelessDevices, iotwirele ss:ListWirelessGatewayTaskD efinitions, lex:DescribeBot Version, lex:ListBotVersions, lightsail:GetContainerServices, lightsail:GetDistributions, lightsail:GetRelationalDat abase, lightsail:GetRelatio nalDatabaseParameters, mobiletargeting:GetApps, mobiletargeting:GetCampaign , mobiletargeting:GetSegmen t, mobiletargeting:Ge tSegments, opsworks:Describ eInstances, opsworks:Descri beTimeBasedAutoScaling, opsworks:DescribeVolumes, panorama:DescribeApplication Instance, panorama:Describe ApplicationInstanceDetails,		

Änderung	Beschreibung	Datum
panorama:DescribePackage, panorama:DescribePackageVersion, panorama:ListApplicationInstances, panorama:ListPackages, quicksight:ListDataSources, ram:ListResourceSharePermissions, rds:DescribeDBProxies, rds:DescribeGlobalClusters, rekognition:ListStreamProcessors, resource-groups:GetGroup, resource-groups:GetGroupConfiguration, resource-groups:GetGroupQuery, resource-groups:GetTags, resource-groups:ListGroupResources, resource-groups:ListGroups, robomaker:ListRobotApplications, robomaker:ListSimulationApplications, route53resolver:GetResolverDnssecConfig, route53resolver:ListResolverDnssecConfigs, s3:ListStorageLensConfigurations, schemas:GetResourcePolicy, servicediscovery:ListInstances, sts:GetCallerIdentity, synthetics:GetGroup, synthetics:ListAssociatedGroups, synthetics:ListGroupResources, and synthetics:ListGroups		

Änderung	Beschreibung	Datum
AWSConfigServiceRolePolicy – Addition: Glue::GetTable	Diese Richtlinie gewährt jetzt die Berechtigung zum Abrufen der AWS Glue Tabellend efinition in einem Datenkatalog für eine angegebene Tabelle.	14. September 2022
AWS_ConfigRole – Addition: Glue::GetTable	Diese Richtlinie gewährt nun die Berechtigung zum Abrufen der AWS Glue Tabellend efinition in einem Datenkatalog für eine angegebene Tabelle.	14. September 2022

Änderung	Beschreibung	Datum
AWSConfigServiceRolePolicy – Addition: appconfig:ListApplications, appflow:DescribeConnectorProfiles, appsync:GetApiCache, autoscaling-plans:DescribeScalingPlanResources, autoscaling-plans:DescribeScalingPlans, autoscaling-plans:GetScalingPlanResourceForecastData, autoscaling:DescribeWarmPool, backup:DescribeFramework, backup:DescribeReportPlan, backup:ListFrameworks, backup:ListReportPlans, budgets:DescribeBudgetAction, budgets:DescribeBudgetActionsForAccount, budgets:DescribeBudgetActionsForBudget, budgets:ViewBudget, ce:GetAnomalyMonitors, ce:GetAnomalySubscriptions, cloud9:DescribeEnvironmentMemberships, cloud9:DescribeEnvironments, cloud9:ListEnvironments, cloud9:ListTagsForResource, cloudwatch:GetMetricStream, cloudwatch:ListMetricStreams, datasync:DescribeLocationFsxWindows, devops-guru:GetResourceCollection, ds:DescribeDirectories, ec2:DescribeTrafficMirrorFilte	Diese Richtlinie unterstützt jetzt zusätzliche Berechtigungen für Amazon AppFlow, Amazon, Amazon CloudWatch RUM CloudWatch, Amazon CloudWatch Synthetics, Amazon Connect-Kundenprofile, Amazon Connect Voice ID, Amazon DevOps Guru, Amazon Elastic Compute Cloud (Amazon EC2), Amazon EC2 Auto Scaling, Amazon EMR, Amazon, Amazon EventBridge Schemas EventBridge, Amazon Fraud Detector Amazon FinSpace, Amazon GameLift Servers, Amazon Interactive Video Service (Amazon IVS), Amazon Managed Service für Apache Flink, EC2 Image Builder, Amazon Lex, Amazon Lightsail, Amazon Location Service, Amazon Lookout for Equipment, Amazon Lookout for Metrics, Amazon Lookout for Vision, Amazon Managed Blockchain, Amazon MQ, Amazon Nimble StudioAmazon Pinpoint, Amazon QuickSight, Amazon Application Recovery Controller (ARC) Amazon Route 53 Resolver, , Amazon Simple Storage	7. September 2022

Änderung	Beschreibung	Datum
rs, ec2:DescribeTrafficMirrorTargets, ec2:GetNetworkInsightsAccessScopeAnalysisFindings, ec2:GetNetworkInsightsAccessScopeContent, elasticmapreduce:DescribeStudio, elasticmapreduce:GetStudioSessionMapping, elasticmapreduce:ListStudios, elasticmapreduce:ListStudioSessionMappings, events:DescribeEndpoint, events:DescribeEventBus, events:DescribeRule, events:ListArchives, events:ListEndpoints, events:ListEventBuses, events:ListRules, events:ListTagsForResource, events:ListTargetsByRule, finspace:GetEnvironment, finspace:ListEnvironments, frauddetector:GetDetectors, frauddetector:GetDetectorVersion, frauddetector:GetEntityTypes, frauddetector:GetEventTypes, frauddetector:GetExternalModels, frauddetector:GetLabels, frauddetector:GetModels, frauddetector:GetOutcomes, frauddetector:GetVariables, frauddetector:ListTagsForResource, gamelift:DescribeAlias, gamelift:DescribeBuild, gamelift:DescribeFleetAttributes, gamelift:DescribeFleetCapacity,	Service (Amazon S3), Amazon SimpleDB, Amazon Simple Email Service (Amazon SES), Amazon Timestream, AWS AppConfig, AWS AppSync, AWS Auto Scaling, AWS Backup, AWS Budgets, AWS Cost Explorer AWS Cloud9 AWS Directory Service AWS DataSync AWS Elemental MediaPackage AWS Glue AWS IoT AWS IoT Analytics AWS IoT Events AWS IoT SiteWise, AWS IoT TwinMaker AWS Lake Formation, AWS License Manager, AWS Resilience Hub AWS Signer, und AWS Transfer Family.	

Änderung	Beschreibung	Datum
gamelift:DescribeFleetLocationAttributes, gamelift:DescribeFleetLocationCapacity, gamelift:DescribeFleetPortSettings, gamelift:DescribeGameServerGroup, gamelift:DescribeGameSessionQueues, gamelift:DescribeMatchmakingConfigurations, gamelift:DescribeMatchmakingRuleSets, gamelift:DescribeRuntimeConfiguration, gamelift:DescribeScript, gamelift:DescribeVpcPeeringAuthorizations, gamelift:ListAliases, gamelift:ListBuilds, gamelift:ListFleets, gamelift:ListGameServerGroups, gamelift:ListScripts, gamelift:ListTagsForResource, geo:ListMaps, glue:GetClassifier, glue:GetClassifiers, imagebuilder:GetContainerRecipe, imagebuilder:GetImage, imagebuilder:GetImagePipeline, imagebuilder:GetImageRecipe, imagebuilder:ListContainerRecipes, imagebuilder:ListImageBuildVersions, imagebuilder:ListImagePipelines, imagebuilder:ListImageRecipes, imagebuilder:ListImages, iot:DescribeCertificate, iot:DescribeDimension, iot:DescribeRoleAlias,		

Änderung	Beschreibung	Datum
iot:DescribeSecurityProfile, iot:GetPolicy, iot:GetTopicRule, iot:GetTopicRuleDestination, iot:ListCertificates, iot:ListDimensions, iot:ListPolicies, iot:ListRoleAliases, iot:ListSecurityProfiles, iot:ListSecurityProfilesForTarget, iot:ListTagsForResource, iot:ListTargetsForSecurityProfile, iot:ListTopicRuleDestinations, iot:ListTopicRules, iot:ListV2LoggingLevels, iot:ValidateSecurityProfileBehaviors, iotanalytics:DescribeChannel, iotanalytics:DescribeDataset, iotanalytics:DescribeDatastore, iotanalytics:DescribePipeline, iotanalytics:ListChannels, iotanalytics:ListDatasets, iotanalytics:ListDatastores, iotanalytics:ListPipelines, iotanalytics:ListTagsForResource, iotevents:DescribeAlarmModel, iotevents:DescribeDetectorModel, iotevents:DescribeInput, iotevents:ListAlarmModels, iotevents:ListDetectorModels, iotevents:ListInputs, iotevents:ListTagsForResource, iotsitewise:DescribeAccessPolicy, iotsitewise:DescribeAsset, iotsitewise:ListAccessPolic		

Änderung	Beschreibung	Datum
ies, iotsitewise:ListAssets, iottwinmaker:GetEntity, iottwinmaker:GetScene, iottwinmaker:GetWorksp ace, iottwinmaker:ListE ntities, iottwinmaker:ListS cenes, iottwinmaker:ListT agsForResource, iottwinmake r:ListWorkspaces, ivs:GetPl aybackKeyPair, ivs:GetRecor dingConfiguration, ivs:GetSt reamKey, ivs:ListChannels, ivs:ListPlaybackKeyPairs, i vs:ListRecordingConfigurati ons, ivs:ListStreamKeys, ivs:ListTagsForResource, kinesisanalytics:ListApplic ations, lakeformation:Descr ibeResource, lakeformation: GetDataLakeSettings, lakefo rmation:ListPermissions, lakeformation:ListResources , lex:DescribeBot, lex:Descr ibeBotAlias, lex:DescribeRe sourcePolicy, lex:ListB otAliases, lex:ListBotLocal es, lex:ListBots, lex:ListT agsForResource, license-manager:GetGrant, license-m anager:GetLicense, license-manager:ListDistributedGran ts, license-manager:ListLic enses, license-manager:List ReceivedGrants, lightsail :GetAlarms, lightsail:GetBu		

Änderung	Beschreibung	Datum
ckets, lightsail:GetCertificates, lightsail:GetDisk, lightsail:GetDisks, lightsail:GetInstance, lightsail:GetInstances, lightsail:GetKeyPair, lightsail:GetLoadBalancer, lightsail:GetLoadBalancers, lightsail:GetLoadBalancerTlsCertificates, lightsail:GetStaticIp, lightsail:GetStaticIps, lookoutequipment:DescribeInferenceScheduler, lookoutequipment:ListTagsForResource, lookoutmetrics:DescribeAlert, lookoutmetrics:DescribeAnomalyDetector, lookoutmetrics:ListAlerts, lookoutmetrics:ListAnomalyDetectors, lookoutmetrics:ListMetricSets, lookoutmetrics:ListTagsForResource, lookoutvision:DescribeProject, lookoutvision:ListProjects, managedblockchain:GetMember, managedblockchain:GetNetwork, managedblockchain:GetNode, managedblockchain:ListInvitations, managedblockchain:ListMembers, managedblockchain:ListNodes, mediapackage-vod:DescribePackagingGroup, mediapackage-vod:ListPackagingGroups, mediapackage-vod:ListTagsForResource, mobiletargeting:		

Änderung	Beschreibung	Datum
GetInAppTemplate, mobiletargeting:ListTemplates, mq:DescribeBroker, mq:ListBrokers, nimble:GetLaunchProfile, nimble:GetLaunchProfileDetails, nimble:GetStreamingImage, nimble:GetStudio, nimble:GetStudioComponent, nimble:ListLaunchProfiles, nimble:ListStreamingImages, nimble:ListStudioComponents, nimble:ListStudios, profile:GetDomain, profile:GetIntegration, profile:GetProfileObjectType, profile:ListDomains, profile:ListIntegrations, profile:ListProfileObjectTypes, profile:ListTagsForResource, quicksight:DescribeAnalysis, quicksight:DescribeAnalysisPermissions, quicksight:DescribeDataSet, quicksight:DescribeDataSetPermissions, quicksight:DescribeTheme, quicksight:DescribeThemePermissions, quicksight:ListAnalyses, quicksight:ListDataSets, quicksight:ListThemes, resiliencehub:DescribeApp, resiliencehub:DescribeAppVersionTemplate, resiliencehub:DescribeResiliencyPolicy, resiliencehub:ListApps, resiliencehub:ListAppVersionResourceMappings,		

Änderung	Beschreibung	Datum
resiliencehub:ListResiliencyPolicies, route53-recovery-readiness:GetCell, route53-recovery-readiness:GetReadinessCheck, route53-recovery-readiness:GetRecoveryGroup, route53-recovery-readiness:GetResourceSet, route53-recovery-readiness:ListCells, route53-recovery-readiness:ListReadinessChecks, route53-recovery-readiness:ListRecoveryGroups, route53-recovery-readiness:ListResourceSets, route53resolver:GetFirewallDomainList, route53resolver:GetFirewallRuleGroup, route53resolver:GetFirewallRuleGroupAssociation, route53resolver:GetResolverQueryLogConfig, route53resolver:ListFirewallDomainLists, route53resolver:ListFirewallDomains, route53resolver:ListFirewallRuleGroupAssociations, route53resolver:ListFirewallRuleGroups, route53resolver:ListFirewallRules, route53resolver:ListResolverQueryLogConfigs, rum:GetAppMonitor, rum:GetAppMonitorData, rum:ListAppMonitors, rum:ListTagsForResource, s3-outposts:GetAccessPoint,		

Änderung	Beschreibung	Datum
s3-outposts:GetAccessPoint Policy, s3-outposts:GetBuc ket, s3-outposts:GetBucketP olicy, s3-outposts:GetBuc ketTagging, s3-outposts:Get LifecycleConfiguration, s3- outposts:ListAccessPoints, s3-outposts:ListEndpoints, s3-outposts:ListRegionalBuc kets, schemas:DescribeDi scoverer, schemas:DescribeR egistry, schemas:DescribeSc hema, schemas:ListDiscovere rs, schemas:ListRegistries, schemas:ListSchemas, sdb:GetAttributes, sdb:ListD omains, ses:ListEmailTempla tes, ses:ListReceiptFilters, ses:ListReceiptRuleSe ts, ses:ListTemplates, signer:GetSigningProfile, signer:ListProfilePermissio ns, signer:ListSigningProfiles, synthetics:DescribeCanaries , synthetics:DescribeCanari esLastRun, synthetics:Descr ibeRuntimeVersions, synthetic s:GetCanary, synthetics:Get CanaryRuns, synthetic s:ListTagsForResource, time stream:DescribeDatabase, timestream:DescribeTable, timestream:ListDatabases, timestream:ListTables, time stream:ListTagsForResource,		

Änderung	Beschreibung	Datum
transfer:DescribeServer, transfer:DescribeUser, transfer:DescribeWorkflow, transfer:ListServers, transfer:ListUsers, transfer:ListWorkflows, voiceid:DescribeDomain, and voiceid:ListTagsForResource		

Änderung	Beschreibung	Datum
AWS_ConfigRole – Addition: appconfig:ListApplications, appflow:DescribeConnectorProfiles, appsync:GetApiCache, autoscaling-plans:DescribeScalingPlanResources, autoscaling-plans:DescribeScalingPlans, autoscaling-plans:GetScalingPlanResourceForecastData, autoscaling:DescribeWarmPool, backup:DescribeFramework, backup:DescribeReportPlan, backup:ListFrameworks, backup:ListReportPlans, budgets:DescribeBudgetAction, budgets:DescribeBudgetActionsForAccount, budgets:DescribeBudgetActionsForBudget, budgets:ViewBudget, ce:GetAnomalyMonitors, ce:GetAnomalySubscriptions, cloud9:DescribeEnvironmentMemberships, cloud9:DescribeEnvironments, cloud9:ListEnvironments, cloud9:ListTagsForResource, cloudwatch:GetMetricStream, cloudwatch:ListMetricStreams, datasync:DescribeLocationFsxWindows, devops-guru:GetResourceCollection, ds:DescribeDirectories, ec2:DescribeTrafficMirrorTarge	Diese Richtlinie unterstützt jetzt zusätzliche Berechtigungen für Amazon AppFlow, Amazon, Amazon CloudWatch RUM CloudWatch, Amazon CloudWatch Synthetics, Amazon Connect-Kundenprofile, Amazon Connect Voice ID, Amazon DevOps Guru, Amazon Elastic Compute Cloud (Amazon EC2), Amazon EC2 Auto Scaling, Amazon EMR, Amazon, Amazon EventBridge Schemas EventBridge, Amazon Fraud Detector Amazon FinSpace, Amazon GameLift Servers, Amazon Interactive Video Service (Amazon IVS), Amazon Managed Service für Apache Flink, EC2 Image Builder, Amazon Lex, Amazon Lightsail, Amazon Location Service, Amazon Lookout for Equipment, Amazon Lookout for Metrics, Amazon Lookout for Vision, Amazon Managed Blockchain, Amazon MQ, Amazon Nimble StudioAmazon Pinpoint, Amazon QuickSight, Amazon Application Recovery Controller (ARC) Amazon Route 53 Resolver, , Amazon Simple Storage	7. September 2022

Änderung	Beschreibung	Datum
ts, ec2:GetNetworkInsightsAccessScopeAnalysisFindings, ec2:GetNetworkInsightsAccessScopeContent, elasticmapreduce:DescribeStudio, elasticmapreduce:GetStudioSessionMapping, elasticmapreduce:ListStudios, elasticmapreduce:ListStudioSessionMappings, events:DescribeEndpoint, events:DescribeEventBus, events:DescribeRule, events:ListArchives, events:ListEndpoints, events:ListEventBuses, events:ListRules, events:ListTagsForResource, events:ListTargetsByRule, finspace:GetEnvironment, finspace:ListEnvironments, frauddetector:GetDetectors, frauddetector:GetDetectorVersion, frauddetector:GetEntityTypes, frauddetector:GetEventTypes, frauddetector:GetExternalModels, frauddetector:GetLabels, frauddetector:GetModels, frauddetector:GetOutcomes, frauddetector:GetVariables, frauddetector:ListTagsForResource, gamelift:DescribeAlias, gamelift:DescribeBuild, gamelift:DescribeFleetAttributes, gamelift:DescribeFleetCapacity, gamelift:DescribeFleetLocat	Service (Amazon S3), Amazon SimpleDB, Amazon Simple Email Service (Amazon SES), Amazon Timestream, AWS AppConfig, AWS AppSync, AWS Auto Scaling, AWS Backup, AWS Budgets, AWS Cost Explorer AWS Cloud9 AWS Directory Service AWS DataSync AWS Elemental MediaPackage AWS Glue AWS IoT AWS IoT Analytics AWS IoT Events AWS IoT SiteWise, AWS IoT TwinMaker, AWS Lake Formation AWS License Manager, AWS Resilience Hub, AWS Signer, und AWS Transfer Family	

Änderung	Beschreibung	Datum
ionAttributes, gamelift:DescribeFleetLocationCapacity, gamelift:DescribeFleetPortSettings, gamelift:DescribeGameServerGroup, gamelift:DescribeGameSessionQueues, gamelift:DescribeMatchmakingConfigurations, gamelift:DescribeMatchmakingRuleSets, gamelift:DescribeRuntimeConfiguration, gamelift:DescribeScript, gamelift:DescribeVpcPeeringAuthorizations, gamelift:ListAliases, gamelift:ListBuilds, gamelift:ListFleets, gamelift:ListGameServerGroups, gamelift:ListScripts, gamelift:ListTagsForResource, geo:ListMaps, glue:GetClassifier, glue:GetClassifiers, imagebuilder:GetContainerRecipe, imagebuilder:GetImage, imagebuilder:GetImagePipeline, imagebuilder:GetImageRecipe, imagebuilder:ListContainerRecipes, imagebuilder:ListImageBuildVersions, imagebuilder:ListImagePipelines, imagebuilder:ListImageRecipes, imagebuilder:ListImages, iot:DescribeCertificate, iot:DescribeDimension, iot:DescribeRoleAlias, iot:DescribeSecurityProfile,		

Änderung	Beschreibung	Datum
iot:GetPolicy, iot:GetTopicRule, iot:GetTopicRuleDestination, iot:ListCertificates, iot:ListDimensions, iot:ListPolicies, iot:ListRoleAliases, iot:ListSecurityProfiles, iot:ListSecurityProfilesForTarget, iot:ListTagsForResource, iot:ListTargetsForSecurityProfile, iot:ListTopicRuleDestinations, iot:ListTopicRules, iot:ListV2LoggingLevels, iot:ValidateSecurityProfileBehaviors, iotanalytics:DescribeChannel, iotanalytics:DescribeDataset, iotanalytics:DescribeDatastore, iotanalytics:DescribePipeline, iotanalytics:ListChannels, iotanalytics:ListDatasets, iotanalytics:ListDatastores, iotanalytics:ListPipelines, iotanalytics:ListTagsForResource, iotevents:DescribeAlarmModel, iotevents:DescribeDetectorModel, iotevents:DescribeInput, iotevents:ListAlarmModels, iotevents:ListDetectorModels, iotevents:ListInputs, iotevents:ListTagsForResource, iotsitewise:DescribeAccessPolicy, iotsitewise:DescribeAsset, iotsitewise:ListAccessPolicies, iotsitewise:ListAssets,		

Änderung	Beschreibung	Datum
iottwinmaker:GetEntity, iottwinmaker:GetScene, iottwinmaker:GetWorksp ace, iottwinmaker:ListE ntities, iottwinmaker:ListS cenes, iottwinmaker:ListT agsForResource, iottwinmake r:ListWorkspaces, ivs:GetPl aybackKeyPair, ivs:GetRecor dingConfiguration, ivs:GetSt reamKey, ivs:ListChannels, ivs:ListPlaybackKeyPairs, i vs:ListRecordingConfigurati ons, ivs:ListStreamKeys, ivs:ListTagsForResource, kinesisanalytics:ListApplic ations, lakeformation:Descr ibeResource, lakeformation: GetDataLakeSettings, lakefo rmation:ListPermissions, lakeformation:ListResources , lex:DescribeBot, lex:Descr ibeBotAlias, lex:DescribeRe sourcePolicy, lex:ListB otAliases, lex:ListBotLocal es, lex:ListBots, lex:ListT agsForResource, license-manager:GetGrant, license-m anager:GetLicense, license-manager:ListDistributedGran ts, license-manager:ListLic enses, license-manager:List ReceivedGrants, lightsail :GetAlarms, lightsail:GetBu ckets, lightsail:GetCertificates,		

Änderung	Beschreibung	Datum
lightsail:GetDisk, lightsail:GetDisks, lightsail:GetInstance, lightsail:GetInstances, lightsail:GetKeyPair, lightsail:GetLoadBalancer, lightsail:GetLoadBalancers, lightsail:GetLoadBalancerTlsCertificates, lightsail:GetStaticIp, lightsail:GetStaticIps, lookoutequipment:DescribeInferenceScheduler, lookoutequipment:ListTagsForResource, lookoutmetrics:DescribeAlert, lookoutmetrics:DescribeAnomalyDetector, lookoutmetrics:ListAlerts, lookoutmetrics:ListAnomalyDetectors, lookoutmetrics:ListMetricSets, lookoutmetrics:ListTagsForResource, lookoutvision:DescribeProject, lookoutvision:ListProjects, managedblockchain:GetMember, managedblockchain:GetNetwork, managedblockchain:GetNode, managedblockchain:ListInvitations, managedblockchain:ListMembers, managedblockchain:ListNodes, mediapackage-vod:DescribePackagingGroup, mediapackage-vod:ListPackagingGroups, mediapackage-vod:ListTagsForResource, mobiletargeting:GetInAppTemplate, mobiletar		

Änderung	Beschreibung	Datum
geting:ListTemplates, mq:DescribeBroker, mq:ListBrokers, nimble:GetLaunchProfile, nimble:GetLaunchProfileDetails, nimble:GetStreamingImage, nimble:GetStudio, nimble:GetStudioComponent, nimble:ListLaunchProfiles, nimble:ListStreamingImages, nimble:ListStudioComponents, nimble:ListStudios, profile:GetDomain, profile:GetIntegration, profile:GetProfileObjectType, profile:ListDomains, profile:ListIntegrations, profile:ListProfileObjectTypes, profile:ListTagsForResource, quicksight:DescribeAnalysis, quicksight:DescribeAnalysisPermissions, quicksight:DescribeDataSet, quicksight:DescribeDataSetPermissions, quicksight:DescribeTheme, quicksight:DescribeThemePermissions, quicksight:ListAnalyses, quicksight:ListDataSets, quicksight:ListThemes, resiliencehub:DescribeApp, resiliencehub:DescribeAppVersionTemplate, resiliencehub:DescribeResiliencyPolicy, resiliencehub:ListApps, resiliencehub:ListAppVersionResourceMappings, resiliencehub:ListResiliencyP		

Änderung	Beschreibung	Datum
olicies, route53-recovery-r eadiness:GetCell, route53-r ecovery-readiness:GetReadin essCheck, route53-recovery- readiness:GetRecoveryGroup, route53-recovery-readiness :GetResourceSet, route53- recovery-readiness:ListCells, route53-recovery-readiness :ListReadinessChecks, route53-recovery-readin ess:ListRecoveryGroups, rou te53-recovery-readiness:Lis tResourceSets, route53resol ver:GetFirewallDomainList, route53resolver:GetFirewall RuleGroup, route53resolver: GetFirewallRuleGroupAssocia tion, route53resolver:GetRe solverQueryLogConfig, route53resolver:ListFir ewallDomainLists, route53re solver:ListFirewallDomains, route53resolver:ListFirewa llRuleGroupAssociations, ro ute53resolver:ListFirewallR uleGroups, route53resolver: ListFirewallRules, route53r esolver:ListResolverQueryLo gConfigs, rum:GetAppMonitor, rum:GetAppMonitorData, rum:ListAppMonitors, rum:Li stTagsForResource, s3- outposts:GetAccessPoint, s3-outposts:GetAccessPoint		

Änderung	Beschreibung	Datum
Policy, s3-outposts:GetBucket, s3-outposts:GetBucketPolicy, s3-outposts:GetBucketTagging, s3-outposts:GetLifecycleConfiguration, s3-outposts:ListAccessPoints, s3-outposts:ListEndpoints, s3-outposts:ListRegionalBuckets, schemas:DescribeDiscoverer, schemas:DescribeRegistry, schemas:DescribeSchema, schemas:ListDiscoverers, schemas:ListRegistries, schemas:ListSchemas, sdb:GetAttributes, sdb:ListDomains, ses:ListEmailTemplates, ses:ListReceiptFilters, ses:ListReceiptRuleSets, ses:ListTemplates, signer:GetSigningProfile, signer:ListProfilePermissions, signer:ListSigningProfiles, synthetics:DescribeCanaries, synthetics:DescribeCanariesLastRun, synthetics:DescribeRuntimeVersions, synthetics:GetCanary, synthetics:GetCanaryRuns, synthetics:ListTagsForResource, timestream:DescribeDatabase, timestream:DescribeTable, timestream:ListDatabases, timestream:ListTables, timestream:ListTagsForResource, transfer:DescribeServer, tr		

Änderung	Beschreibung	Datum
ansfer:DescribeUser, transfer: DescribeWorkflow, transfer: ListServers, transfer:ListUsers , transfer:ListWorkflows, voiceid:DescribeDomain, and voiceid:ListTagsForResource		

Änderung	Beschreibung	Datum
AWSConfigServiceRolePolicy – Addition: airflow:ListTagsForResource, iot:ListCustomMetrics, iot:DescribeCustomMetric, appstream:DescribeDirectoryConfigs, appstream:ListTagsForResource, codeguru-reviewer:DescribeRepositoryAssociation, codeguru-reviewer:ListRepositoryAssociations, healthlake:ListFHIRDatastores, healthlake:DescribeFHIRDatastore, healthlake:ListTagsForResource, kinesisvideo:DescribeStream, kinesisvideo:ListStreams, kinesisvideo:ListTagsForStream, kinesisvideo:DescribeSignalingChannel, kinesisvideo:ListTagsForResource, kinesisvideo:ListSignalingChannels, route53-recovery-control-config:DescribeCluster, route53-recovery-control-config:DescribeRoutingControl, route53-recovery-control-config:DescribeSafetyRule, route53-recovery-control-config:ListClusters, route53-recovery-control-config:ListRoutingControls, route53-recovery-control-config:ListSafetyRules, devicefarm:GetTestGridProject,	Diese Richtlinie unterstützt jetzt zusätzliche Berechtigungen für Amazon Managed Workflows for Apache Airflow AWS IoT, Amazon AppStream 2.0, Amazon CodeGuru Reviewer AWS HealthLake, Amazon Kinesis Video Streams, Amazon Application Recovery Controller (ARC) AWS Device Farm, Amazon Elastic Compute Cloud (Amazon EC2), Amazon Pinpoint AWS Identity and Access Management (IAM) GuardDuty, Amazon und Amazon Logs. CloudWatch	1. Februar 2023

Änderung	Beschreibung	Datum
devicefarm:ListTestGridProjects, ec2:DescribeCapacityReservationFleets, ec2:DescribeIpamPools, ec2:DescribeIpams, ec2:GetInstanceTypesFromInstanceRequirement, mobiletargeting:GetApplicationSettings, mobiletargeting:ListTagsForResource, ecr:BatchGetRepositoryScanningConfiguration, iam:ListServerCertificates, guardduty:ListPublishingDestinations, guardduty:DescribePublishingDestination, logs:GetLogDelivery, and logs:ListLogDeliveries		

Änderung	Beschreibung	Datum
AWS_ConfigRole – Addition: airflow:ListTagsForResource, iot:ListCustomMetrics, iot:DescribeCustomMetric, appstream:DescribeDirectoryConfigs, appstream:ListTagsForResource, codeguru-reviewer:DescribeRepositoryAssociation, codeguru-reviewer:ListRepositoryAssociations, healthlake:ListFHIRDatastores, healthlake:DescribeFHIRDatastore, healthlake:ListTagsForResource, kinesisvideo:DescribeStream, kinesisvideo:ListStreams, kinesisvideo:ListTagsForStream, kinesisvideo:DescribeSignalingChannel, kinesisvideo:ListTagsForResource, kinesisvideo:ListSignalingChannels, route53-recovery-control-config:DescribeCluster, route53-recovery-control-config:DescribeRoutingControl, route53-recovery-control-config:DescribeSafetyRule, route53-recovery-control-config:ListClusters, route53-recovery-control-config:ListRoutingControls, route53-recovery-control-config:ListSafetyRules, devicefarm:GetTestGridProject, devicefar	Diese Richtlinie unterstützt jetzt zusätzliche Berechtigungen für Amazon Managed Workflows for Apache Airflow AWS IoT, Amazon AppStream 2.0, Amazon CodeGuru Reviewer AWS HealthLake, Amazon Kinesis Video Streams, Amazon Application Recovery Controller (ARC) AWS Device Farm, Amazon Elastic Compute Cloud (Amazon EC2), Amazon Pinpoint AWS Identity and Access Management (IAM) GuardDuty, Amazon und Amazon Logs. CloudWatch	1. Februar 2023

Änderung	Beschreibung	Datum
m:ListTestGridProjects, ec2:DescribeCapacityReservationFleets, ec2:DescribeIpamPools, ec2:DescribeIpams, ec2:GetInstanceTypesFromInstanceRequirement, mobiletargeting:GetApplicationSettings, mobiletargeting:ListTagsForResource, ecr:BatchGetRepositoryScanningConfiguration, iam:ListServerCertificates, guardduty:ListPublishingDestinations, guardduty:DescribePublishingDestination, logs:GetLogDelivery, and logs:ListLogDeliveries		
ConfigConformsServiceRolePolicy – Aktualisierung: config:DescribeConfigRules	Als bewährte Sicherheitsmethode entfernt diese Richtlinie nun umfassende Berechtigungen auf Ressourcenebene für `config:DescribeConfigRules` .	12. Januar 2023

Änderung	Beschreibung	Datum
AWSConfigServiceRolePolicy – Addition: APS:DescribeRuleGroupsNamespace, APS:DescribeWorkspace, APS:ListWorkspaces, auditmanager:GetAssessment, auditmanager:ListAssessments, devicefarm:GetNetworkProfile, AWS Transfer Family devicefarm:GetProject, devicefarm:ListNetworkProfiles, devicefarm:ListTagsForResource, dms:DescribeEndpoints, ds:ListTagsForResource, ec2:DescribeTags, ec2:DescribeTrafficMirrorSessions, ec2:DescribeTrafficMirrorTargets, ec2:GetIpamPoolAllocations, ec2:GetIpamPoolCidrs, glue:GetMLTransform, glue:GetMLTransforms, glue:ListMLTransforms, iot:DescribeScheduledAudit, iot:ListScheduledAudits, ivs:GetChannel, lightsail:GetRelationalDatabases, mediapackage-vod:DescribePackagingConfiguration, mediapackage-vod:ListPackagingConfigurations, networkmanager:DescribeGlobalNetworks, networkmanager:GetTransitGatewayRegistrat	Diese Richtlinie unterstützt jetzt zusätzliche Berechtigungen für Amazon Managed Service for Prometheus,, AWS Audit Manager AWS Device Farm, AWS Database Migration Service (AWS DMS) AWS Directory Service, Amazon Elastic Compute Cloud (Amazon EC2),, AWS Glue AWS IoT, Amazon Lightsail,,, Amazon AWS Elemental MediaPackage AWS Network Manager QuickSight, Amazon Application Recovery Controller (ARC) AWS Resource Access Manager, Amazon Simple Storage Service (Amazon S3) und Amazon Timestream.	15. Dezember 2022

Änderung	Beschreibung	Datum
ions, networkmanager:ListTagsForResource, quicksight:DescribeDashboard, quicksight:DescribeDashboardPermissions, quicksight:DescribeTemplate, quicksight:DescribeTemplatePermissions, quicksight:ListDashboards, quicksight:ListTemplates, ram:ListResources, route53-recovery-control-config:DescribeControlPanel, route53-recovery-control-config:ListControlPanels, route53-recovery-control-config:ListTagsForResource, route53resolver:GetResolverQueryLogConfigAssociation, route53resolver:ListResolverQueryLogConfigAssociations, s3:GetAccessPointForObjectLambda, s3:GetAccessPointPolicyForObjectLambda, s3:GetAccessPointPolicyStatusForObjectLambda, s3:GetMultiRegionAccessPoint, s3:ListAccessPointsForObjectLambda, s3:ListMultiRegionAccessPoints, timestream:DescribeEndpoints, transfer:DescribeConnector, transfer:ListConnectors, and transfer:ListTagsForResource		

Änderung	Beschreibung	Datum
AWS_ConfigRole – Addition: APS:DescribeRuleGroupsNamespace, APS:DescribeWorkspace, APS:ListWorkspaces, auditmanager:GetAssessment, auditmanager:ListAssessments, devicefarm:GetNetworkProfile, devicefarm:GetProject, devicefarm:ListNetworkProfiles, devicefarm:ListTagsForResource, dms:DescribeEndpoints, ds:ListTagsForResource, ec2:DescribeTags, ec2:DescribeTrafficMirrorSessions, ec2:DescribeTrafficMirrorTargets, ec2:GetIpamPoolAllocations, ec2:GetIpamPoolCidrs, glue:GetMLTransform, glue:GetMLTransforms, glue:ListMLTransforms, iot:DescribeScheduledAudit, iot:ListScheduledAudits, ivs:GetChannel, lightsail:GetRelationalDatabases, mediapackage-vod:DescribePackagingConfiguration, mediapackage-vod:ListPackagingConfigurations, networkmanager:DescribeGlobalNetworks, networkmanager:GetTransitGatewayRegistrations, networkmanager:ListTa	Diese Richtlinie unterstützt jetzt zusätzliche Berechtigungen für Amazon Managed Service for Prometheus,, AWS Audit Manager AWS Device Farm, AWS Database Migration Service (AWS DMS) AWS Directory Service, Amazon Elastic Compute Cloud (Amazon EC2),, AWS Glue AWS IoT, Amazon Lightsail,,, Amazon AWS Elemental MediaPackage AWS Network Manager QuickSight, Amazon Application Recovery Controller (ARC) AWS Resource Access Manager, Amazon Simple Storage Service (Amazon S3) und Amazon Timestream.	15. Dezember 2022

Änderung	Beschreibung	Datum
gsForResource, quicksight:DescribeDashboard, quicksight:DescribeDashboardPermissions, quicksight:DescribeTemplate, quicksight:DescribeTemplatePermissions, quicksight:ListDashboards, quicksight:ListTemplates, ram:ListResources, route53-recovery-control-config:DescribeControlPanel, route53-recovery-control-config:ListControlPanels, route53-recovery-control-config:ListTagsForResource, route53resolver:GetResolverQueryLogConfigAssociation, route53resolver:ListResolverQueryLogConfigAssociations, s3:GetAccessPointForObjectLambda, s3:GetAccessPointPolicyForObjectLambda, s3:GetAccessPointPolicyStatusForObjectLambda, s3:GetMultiRegionAccessPoint, s3:ListAccessPointsForObjectLambda, s3:ListMultiRegionAccessPoints, timestream:DescribeEndpoints, transfer:DescribeConnector, transfer:ListConnectors, and transfer:ListTagsForResource		

Änderung	Beschreibung	Datum
AWSConfigServiceRolePolicy – Addition: cloudformation:ListStackResources and cloudformation:ListStacks	Diese Richtlinie gewährt nun die Erlaubnis, Beschreibungen aller Ressourcen eines angegebenen AWS CloudFormation Stacks und die zusammenfassenden Informationen für Stacks zurückzugeben, deren Status dem angegebenen entspricht. StackStatusFilter	7. November 2022
AWS_ConfigRole – Addition: cloudformation:ListStackResources and cloudformation:ListStacks	Diese Richtlinie gewährt nun die Erlaubnis, Beschreibungen aller Ressourcen eines angegebenen AWS CloudFormation Stacks und die zusammenfassenden Informationen für Stapel zurückzugeben, deren Status dem angegebenen entspricht. StackStatusFilter	7. November 2022

Änderung	Beschreibung	Datum
AWSConfigServiceRolePolicy – Addition: acm-pca:GetCertificateAuthorityCsr, acm-pca:ListCertificateAuthorities, acm-pca:ListTags, airflow:GetEnvironment, airflow:ListEnvironments, amplifyuibuilder:ListThemes, appconfig:ListConfigurationProfiles, appconfig:ListDeployments, appconfig:ListDeploymentStrategies, appconfig:ListEnvironments, appconfig:ListHostedConfigurationVersions, cassandra:Select, cloudwatch:DescribeAnomalyDetectors, cloudwatch:GetDashboard, cloudwatch:ListDashboards, connect:DescribePhoneNumber, connect:ListPhoneNumbers, connect:ListPhoneNumbersV2, connect:SearchAvailablePhoneNumbers, databrew:DescribeDataset, databrew:DescribeJob, databrew:DescribeProject, databrew:DescribeRecipe, databrew:DescribeRuleset, databrew:DescribeSchedule, databrew:ListDatasets, databrew:ListJobs, databrew:ListProjects, databrew:ListRecipes, databrew:ListRecipeVers	Diese Richtlinie unterstützt jetzt zusätzliche Berechtigungen für AWS Certificate Manager Amazon Managed Workflows for Apache Airflow,, AWS Amplify AWS AppConfig, Amazon Keyspaces, Amazon, Amazon Connect CloudWatch AWS Glue DataBrew, Amazon Elastic Compute Cloud (Amazon EC2), Amazon Elastic Kubernetes Service (Amazon EKS), Amazon, Amazon Fraud Detector EventBridge AWS Fault Injection Service, Amazon, Amazon GameLift Servers FSx, Amazon Location Service, Amazon Lex, Amazon Lightsail AWS IoT, Amazon Pinpoint,,,, Amazon, Amazon Relational Database AWS OpsWorks AWS Panorama AWS Resource Access Manager QuickSight Service (Amazon RDS), Amazon Rekognition, AWS RoboMaker, AWS Resource Groups, Amazon Route 53, Amazon Simple Storage Service (Amazon S3) AWS Cloud Map, und. AWS Security Token Service	19. Oktober 2022

Änderung	Beschreibung	Datum
ions, databrew:ListRulesets, databrew:ListSchedules, ec2:DescribeRouteTables, eks:DescribeAddon, eks:DescribeIdentityProviderConfig, eks:ListAddons, eks:ListIdentityProviderConfigs, events:DescribeConnection, events:ListApiDestinations, events:ListConnections, fis:GetExperimentTemplate, fis:ListExperimentTemplates, frauddetector:GetRules, fsx:DescribeBackups, fsx:DescribeSnapshots, fsx:DescribeStorageVirtualMachines, gamelift:DescribeMatchmakingRuleSets, gamelift:DescribeVpcPeeringConnections, geo:ListGeofenceCollections, geo:ListPlaceIndexes, geo:ListRouteCalculators, geo:ListTrackers, iot:DescribeAccountAuditConfiguration, iot:DescribeAuthorizer, iot:DescribeDomainConfiguration, iot:DescribeMitigationAction, iot:ListAuthorizers, iot:ListDomainConfigurations, iot:ListMitigationActions, iotsitewise:DescribeAssetModel, iotsitewise:DescribeDashboard, iotsitewise:DescribeGateway, iotsitewise:DescribePortal, iotsitewi		

Änderung	Beschreibung	Datum
se:DescribeProject, iotsite wise:ListAssetModels, iotsitewi se:ListDashboards, iotsitew ise:ListGateways, iotsitewi se:ListPortals, iotsitewise :ListProjectAssets, iotsitewi se:ListProjects, iotsitewis e:ListTagsForResource, iotwireless:GetServiceProfi le, iotwireless:GetWireless Device, iotwireless:GetWire lessGatewayTaskDefinition, iotwireless:ListServiceProf iles, iotwireless:ListTagsF orResource, iotwireless:Lis tWirelessDevices, iotwirele ss:ListWirelessGatewayTaskD efinitions, lex:DescribeBot Version, lex:ListBotVersions, lightsail:GetContainerServices, lightsail:GetDistributions, lightsail:GetRelationalDat abase, lightsail:GetRelatio nalDatabaseParameters, mobiletargeting:GetApps, mobiletargeting:GetCampaign , mobiletargeting:GetSegmen t, mobiletargeting:Ge tSegments, opsworks:Describ eInstances, opsworks:Descri beTimeBasedAutoScaling, opsworks:DescribeVolumes, panorama:DescribeApplication Instance, panorama:Describe ApplicationInstanceDetails,		

Änderung	Beschreibung	Datum
panorama:DescribePackage, panorama:DescribePackageVersion, panorama:ListApplicationInstances, panorama:ListPackages, quicksight:ListDataSources, ram:ListResourceSharePermissions, rds:DescribeDBProxies, rds:DescribeGlobalClusters, rekognition:ListStreamProcessors, resource-groups:GetGroup, resource-groups:GetGroupConfiguration, resource-groups:GetGroupQuery, resource-groups:GetTags, resource-groups:ListGroupResources, resource-groups:ListGroups, robomaker:ListRobotApplications, robomaker:ListSimulationApplications, route53resolver:GetResolverDnssecConfig, route53resolver:ListResolverDnssecConfigs, s3:ListStorageLensConfigurations, schemas:GetResourcePolicy, servicediscovery:ListInstances, sts:GetCallerIdentity, synthetics:GetGroup, synthetics:ListAssociatedGroups, synthetics:ListGroupResources, and synthetics:ListGroups		

Änderung	Beschreibung	Datum
AWS_ConfigRole – Addition: acm-pca:GetCertificateAuthorityCsr, acm-pca:ListCertificateAuthorities, acm-pca:ListTags, airflow:GetEnvironment, airflow:ListEnvironments, amplifyuibuilder:ListThemes, appconfig:ListConfigurationProfiles, appconfig:ListDeployments, appconfig:ListDeploymentStrategies, appconfig:ListEnvironments, appconfig:ListHostedConfigurationVersions, cassandra:Select, cloudwatch:DescribeAnomalyDetectors, cloudwatch:GetDashboard, cloudwatch:ListDashboards, connect:DescribePhoneNumber, connect:ListPhoneNumbers, connect:ListPhoneNumbersV2, connect:SearchAvailablePhoneNumbers, databrew:DescribeDataset, databrew:DescribeJob, databrew:DescribeProject, databrew:DescribeRecipe, databrew:DescribeRuleset, databrew:DescribeSchedule, databrew:ListDatasets, databrew:ListJobs, databrew:ListProjects, databrew:ListRecipes, databrew:ListRecipeVers	Diese Richtlinie unterstützt jetzt zusätzliche Berechtigungen für AWS Certificate Manager Amazon Managed Workflows for Apache Airflow,, AWS Amplify AWS AppConfig, Amazon Keyspaces, Amazon, Amazon Connect CloudWatch AWS Glue DataBrew, Amazon Elastic Compute Cloud (Amazon EC2), Amazon Elastic Kubernetes Service (Amazon EKS), Amazon, Amazon Fraud Detector EventBridge AWS Fault Injection Service, Amazon, Amazon GameLift Servers FSx, Amazon Location Service, Amazon Lex, Amazon Lightsail AWS IoT, Amazon Pinpoint,,,, Amazon, Amazon Relational Database AWS OpsWorks AWS Panorama AWS Resource Access Manager QuickSight Service (Amazon RDS), Amazon Rekognition, AWS RoboMaker, AWS Resource Groups, Amazon Route 53, Amazon Simple Storage Service (Amazon S3) AWS Cloud Map, und. AWS Security Token Service	19. Oktober 2022

Änderung	Beschreibung	Datum
ions, databrew:ListRulesets, databrew:ListSchedules, ec2:DescribeRouteTables, eks:DescribeAddon, eks:DescribeIdentityProviderConfig, eks:ListAddons, eks:ListIdentityProviderConfigs, events:DescribeConnection, events:ListApiDestinations, events:ListConnections, fis:GetExperimentTemplate, fis:ListExperimentTemplates, frauddetector:GetRules, fsx:DescribeBackups, fsx:DescribeSnapshots, fsx:DescribeStorageVirtualMachines, gamelift:DescribeMatchmakingRuleSets, gamelift:DescribeVpcPeeringConnections, geo:ListGeofenceCollections, geo:ListPlaceIndexes, geo:ListRouteCalculators, geo:ListTrackers, iot:DescribeAccountAuditConfiguration, iot:DescribeAuthorizer, iot:DescribeDomainConfiguration, iot:DescribeMitigationAction, iot:ListAuthorizers, iot:ListDomainConfigurations, iot:ListMitigationActions, iotsitewise:DescribeAssetModel, iotsitewise:DescribeDashboard, iotsitewise:DescribeGateway, iotsitewise:DescribePortal, iotsitewi		

Änderung	Beschreibung	Datum
se:DescribeProject, iotsite wise:ListAssetModels, iotsitewi se:ListDashboards, iotsitew ise:ListGateways, iotsitewi se:ListPortals, iotsitewise :ListProjectAssets, iotsitewi se:ListProjects, iotsitewis e:ListTagsForResource, iotwireless:GetServiceProfi le, iotwireless:GetWireless Device, iotwireless:GetWire lessGatewayTaskDefinition, iotwireless:ListServiceProf iles, iotwireless:ListTagsF orResource, iotwireless:Lis tWirelessDevices, iotwirele ss:ListWirelessGatewayTaskD efinitions, lex:DescribeBot Version, lex:ListBotVersions, lightsail:GetContainerServices, lightsail:GetDistributions, lightsail:GetRelationalDat abase, lightsail:GetRelatio nalDatabaseParameters, mobiletargeting:GetApps, mobiletargeting:GetCampaign , mobiletargeting:GetSegmen t, mobiletargeting:Ge tSegments, opsworks:Describ eInstances, opsworks:Descri beTimeBasedAutoScaling, opsworks:DescribeVolumes, panorama:DescribeApplication Instance, panorama:Describe ApplicationInstanceDetails,		

Änderung	Beschreibung	Datum
panorama:DescribePackage, panorama:DescribePackageVersion, panorama:ListApplicationInstances, panorama:ListPackages, quicksight:ListDataSources, ram:ListResourceSharePermissions, rds:DescribeDBProxies, rds:DescribeGlobalClusters, rekognition:ListStreamProcessors, resource-groups:GetGroup, resource-groups:GetGroupConfiguration, resource-groups:GetGroupQuery, resource-groups:GetTags, resource-groups:ListGroupResources, resource-groups:ListGroups, robomaker:ListRobotApplications, robomaker:ListSimulationApplications, route53resolver:GetResolverDnssecConfig, route53resolver:ListResolverDnssecConfigs, s3:ListStorageLensConfigurations, schemas:GetResourcePolicy, servicediscovery:ListInstances, sts:GetCallerIdentity, synthetics:GetGroup, synthetics:ListAssociatedGroups, synthetics:ListGroupResources, and synthetics:ListGroups		

Änderung	Beschreibung	Datum
AWSConfigServiceRolePolicy – Addition: Glue::GetTable	Diese Richtlinie gewährt jetzt die Berechtigung zum Abrufen der AWS Glue Tabellend efinition in einem Datenkatalog für eine angegebene Tabelle.	14. September 2022
AWS_ConfigRole – Addition: Glue::GetTable	Diese Richtlinie gewährt nun die Berechtigung zum Abrufen der AWS Glue Tabellend efinition in einem Datenkatalog für eine angegebene Tabelle.	14. September 2022

Änderung	Beschreibung	Datum
AWSConfigServiceRolePolicy – Addition: appconfig:ListApplications, appflow:DescribeConnectorProfiles, appsync:GetApiCache, autoscaling-plans:DescribeScalingPlanResources, autoscaling-plans:DescribeScalingPlans, autoscaling-plans:GetScalingPlanResourceForecastData, autoscaling:DescribeWarmPool, backup:DescribeFramework, backup:DescribeReportPlan, backup:ListFrameworks, backup:ListReportPlans, budgets:DescribeBudgetAction, budgets:DescribeBudgetActionsForAccount, budgets:DescribeBudgetActionsForBudget, budgets:ViewBudget, ce:GetAnomalyMonitors, ce:GetAnomalySubscriptions, cloud9:DescribeEnvironmentMemberships, cloud9:DescribeEnvironments, cloud9:ListEnvironments, cloud9:ListTagsForResource, cloudwatch:GetMetricStream, cloudwatch:ListMetricStreams, datasync:DescribeLocationFsxWindows, devops-guru:GetResourceCollection, ds:DescribeDirectories, ec2:DescribeTrafficMirrorFilte	Diese Richtlinie unterstützt jetzt zusätzliche Berechtigungen für Amazon AppFlow, Amazon, Amazon CloudWatch RUM CloudWatch, Amazon CloudWatch Synthetics, Amazon Connect-Kundenprofile, Amazon Connect Voice ID, Amazon DevOps Guru, Amazon Elastic Compute Cloud (Amazon EC2), Amazon EC2 Auto Scaling, Amazon EMR, Amazon, Amazon EventBridge Schemas EventBridge, Amazon Fraud Detector Amazon FinSpace, Amazon GameLift Servers, Amazon Interactive Video Service (Amazon IVS), Amazon Managed Service für Apache Flink, EC2 Image Builder, Amazon Lex, Amazon Lightsail, Amazon Location Service, Amazon Lookout for Equipment, Amazon Lookout for Metrics, Amazon Lookout for Vision, Amazon Managed Blockchain, Amazon MQ, Amazon Nimble StudioAmazon Pinpoint, Amazon QuickSight, Amazon Application Recovery Controller (ARC) Amazon Route 53 Resolver, , Amazon Simple Storage	7. September 2022

Änderung	Beschreibung	Datum
rs, ec2:DescribeTrafficMirrorTargets, ec2:GetNetworkInsightsAccessScopeAnalysisFindings, ec2:GetNetworkInsightsAccessScopeContent, elasticmapreduce:DescribeStudio, elasticmapreduce:GetStudioSessionMapping, elasticmapreduce:ListStudios, elasticmapreduce:ListStudioSessionMappings, events:DescribeEndpoint, events:DescribeEventBus, events:DescribeRule, events:ListArchives, events:ListEndpoints, events:ListEventBuses, events:ListRules, events:ListTagsForResource, events:ListTargetsByRule, finspace:GetEnvironment, finspace:ListEnvironments, frauddetector:GetDetectors, frauddetector:GetDetectorVersion, frauddetector:GetEntityTypes, frauddetector:GetEventTypes, frauddetector:GetExternalModels, frauddetector:GetLabels, frauddetector:GetModels, frauddetector:GetOutcomes, frauddetector:GetVariables, frauddetector:ListTagsForResource, gamelift:DescribeAlias, gamelift:DescribeBuild, gamelift:DescribeFleetAttributes, gamelift:DescribeFleetCapacity,	Service (Amazon S3), Amazon SimpleDB, Amazon Simple Email Service (Amazon SES), Amazon Timestream, AWS AppConfig, AWS AppSync, AWS Auto Scaling, AWS Backup, AWS Budgets, AWS Cost Explorer AWS Cloud9 AWS Directory Service AWS DataSync AWS Elemental MediaPackage AWS Glue AWS IoT AWS IoT Analytics AWS IoT Events AWS IoT SiteWise, AWS IoT TwinMaker AWS Lake Formation, AWS License Manager, AWS Resilience Hub AWS Signer, und AWS Transfer Family.	

Änderung	Beschreibung	Datum
gamelift:DescribeFleetLocationAttributes, gamelift:DescribeFleetLocationCapacity, gamelift:DescribeFleetPortSettings, gamelift:DescribeGameServerGroup, gamelift:DescribeGameSessionQueues, gamelift:DescribeMatchmakingConfigurations, gamelift:DescribeMatchmakingRuleSets, gamelift:DescribeRuntimeConfiguration, gamelift:DescribeScript, gamelift:DescribeVpcPeeringAuthorizations, gamelift:ListAliases, gamelift:ListBuilds, gamelift:ListFleets, gamelift:ListGameServerGroups, gamelift:ListScripts, gamelift:ListTagsForResource, geo:ListMaps, glue:GetClassifier, glue:GetClassifiers, imagebuilder:GetContainerRecipe, imagebuilder:GetImage, imagebuilder:GetImagePipeline, imagebuilder:GetImageRecipe, imagebuilder:ListContainerRecipes, imagebuilder:ListImageBuildVersions, imagebuilder:ListImagePipelines, imagebuilder:ListImageRecipes, imagebuilder:ListImages, iot:DescribeCertificate, iot:DescribeDimension, iot:DescribeRoleAlias,		

Änderung	Beschreibung	Datum
iot:DescribeSecurityProfile, iot:GetPolicy, iot:GetTopicRule, iot:GetTopicRuleDestination, iot:ListCertificates, iot:ListDimensions, iot:ListPolicies, iot:ListRoleAliases, iot:ListSecurityProfiles, iot:ListSecurityProfilesForTarget, iot:ListTagsForResource, iot:ListTargetsForSecurityProfile, iot:ListTopicRuleDestinations, iot:ListTopicRules, iot:ListV2LoggingLevels, iot:ValidateSecurityProfileBehaviors, iotanalytics:DescribeChannel, iotanalytics:DescribeDataset, iotanalytics:DescribeDatastore, iotanalytics:DescribePipeline, iotanalytics:ListChannels, iotanalytics:ListDatasets, iotanalytics:ListDatastores, iotanalytics:ListPipelines, iotanalytics:ListTagsForResource, iotevents:DescribeAlarmModel, iotevents:DescribeDetectorModel, iotevents:DescribeInput, iotevents:ListAlarmModels, iotevents:ListDetectorModels, iotevents:ListInputs, iotevents:ListTagsForResource, iotsitewise:DescribeAccessPolicy, iotsitewise:DescribeAsset, iotsitewise:ListAccessPolic		

Änderung	Beschreibung	Datum
ies, iotsitewise:ListAssets, iottwinmaker:GetEntity, iottwinmaker:GetScene, iottwinmaker:GetWorksp ace, iottwinmaker:ListE ntities, iottwinmaker:ListS cenes, iottwinmaker:ListT agsForResource, iottwinmake r:ListWorkspaces, ivs:GetPl aybackKeyPair, ivs:GetRecor dingConfiguration, ivs:GetSt reamKey, ivs:ListChannels, ivs:ListPlaybackKeyPairs, i vs:ListRecordingConfigurati ons, ivs:ListStreamKeys, ivs:ListTagsForResource, kinesisanalytics:ListApplic ations, lakeformation:Descr ibeResource, lakeformation: GetDataLakeSettings, lakefo rmation:ListPermissions, lakeformation:ListResources , lex:DescribeBot, lex:Descr ibeBotAlias, lex:DescribeRe sourcePolicy, lex:ListB otAliases, lex:ListBotLocal es, lex:ListBots, lex:ListT agsForResource, license-manager:GetGrant, license-m anager:GetLicense, license-manager:ListDistributedGran ts, license-manager:ListLic enses, license-manager:List ReceivedGrants, lightsail :GetAlarms, lightsail:GetBu		

Änderung	Beschreibung	Datum
ckets, lightsail:GetCertificates, lightsail:GetDisk, lightsail:GetDisks, lightsail:GetInstance, lightsail:GetInstances, lightsail:GetKeyPair, lightsail:GetLoadBalancer, lightsail:GetLoadBalancers, lightsail:GetLoadBalancerTlsCertificates, lightsail:GetStaticIp, lightsail:GetStaticIps, lookoutequipment:DescribeInferenceScheduler, lookoutequipment:ListTagsForResource, lookoutmetrics:DescribeAlert, lookoutmetrics:DescribeAnomalyDetector, lookoutmetrics:ListAlerts, lookoutmetrics:ListAnomalyDetectors, lookoutmetrics:ListMetricSets, lookoutmetrics:ListTagsForResource, lookoutvision:DescribeProject, lookoutvision:ListProjects, managedblockchain:GetMember, managedblockchain:GetNetwork, managedblockchain:GetNode, managedblockchain:ListInvitations, managedblockchain:ListMembers, managedblockchain:ListNodes, mediapackage-vod:DescribePackagingGroup, mediapackage-vod:ListPackagingGroups, mediapackage-vod:ListTagsForResource, mobiletargeting:		

Änderung	Beschreibung	Datum
GetInAppTemplate, mobiletargeting:ListTemplates, mq:DescribeBroker, mq:ListBrokers, nimble:GetLaunchProfile, nimble:GetLaunchProfileDetails, nimble:GetStreamingImage, nimble:GetStudio, nimble:GetStudioComponent, nimble:ListLaunchProfiles, nimble:ListStreamingImages, nimble:ListStudioComponents, nimble:ListStudios, profile:GetDomain, profile:GetIntegration, profile:GetProfileObjectType, profile:ListDomains, profile:ListIntegrations, profile:ListProfileObjectTypes, profile:ListTagsForResource, quicksight:DescribeAnalysis, quicksight:DescribeAnalysisPermissions, quicksight:DescribeDataSet, quicksight:DescribeDataSetPermissions, quicksight:DescribeTheme, quicksight:DescribeThemePermissions, quicksight:ListAnalyses, quicksight:ListDataSets, quicksight:ListThemes, resiliencehub:DescribeApp, resiliencehub:DescribeAppVersionTemplate, resiliencehub:DescribeResiliencyPolicy, resiliencehub:ListApps, resiliencehub:ListAppVersionResourceMappings,		

Änderung	Beschreibung	Datum
resiliencehub:ListResiliencyPolicies, route53-recovery-readiness:GetCell, route53-recovery-readiness:GetReadinessCheck, route53-recovery-readiness:GetRecoveryGroup, route53-recovery-readiness:GetResourceSet, route53-recovery-readiness:ListCells, route53-recovery-readiness:ListReadinessChecks, route53-recovery-readiness:ListRecoveryGroups, route53-recovery-readiness:ListResourceSets, route53resolver:GetFirewallDomainList, route53resolver:GetFirewallRuleGroup, route53resolver:GetFirewallRuleGroupAssociation, route53resolver:GetResolverQueryLogConfig, route53resolver:ListFirewallDomainLists, route53resolver:ListFirewallDomains, route53resolver:ListFirewallRuleGroupAssociations, route53resolver:ListFirewallRuleGroups, route53resolver:ListFirewallRules, route53resolver:ListResolverQueryLogConfigs, rum:GetAppMonitor, rum:GetAppMonitorData, rum:ListAppMonitors, rum:ListTagsForResource, s3-outposts:GetAccessPoint,		

Änderung	Beschreibung	Datum
s3-outposts:GetAccessPoint Policy, s3-outposts:GetBuc ket, s3-outposts:GetBucketP olicy, s3-outposts:GetBuc ketTagging, s3-outposts:Get LifecycleConfiguration, s3- outposts:ListAccessPoints, s3-outposts:ListEndpoints, s3-outposts:ListRegionalBuc kets, schemas:DescribeDi scoverer, schemas:DescribeR egistry, schemas:DescribeSc hema, schemas:ListDiscovere rs, schemas:ListRegistries, schemas:ListSchemas, sdb:GetAttributes, sdb:ListD omains, ses:ListEmailTempla tes, ses:ListReceiptFilters, ses:ListReceiptRuleSe ts, ses:ListTemplates, signer:GetSigningProfile, signer:ListProfilePermissio ns, signer:ListSigningProfiles, synthetics:DescribeCanaries , synthetics:DescribeCanari esLastRun, synthetics:Descr ibeRuntimeVersions, synthetic s:GetCanary, synthetics:Get CanaryRuns, synthetic s:ListTagsForResource, time stream:DescribeDatabase, timestream:DescribeTable, timestream:ListDatabases, timestream:ListTables, time stream:ListTagsForResource,		

Änderung	Beschreibung	Datum
transfer:DescribeServer, transfer:DescribeUser, transfer:DescribeWorkflow, transfer:ListServers, transfer:ListUsers, transfer:ListWorkflows, voiceid:DescribeDomain, and voiceid:ListTagsForResource		

Änderung	Beschreibung	Datum
AWS_ConfigRole – Addition: appconfig:ListApplications, appflow:DescribeConnectorProfiles, appsync:GetApiCache, autoscaling-plans:DescribeScalingPlanResources, autoscaling-plans:DescribeScalingPlans, autoscaling-plans:GetScalingPlanResourceForecastData, autoscaling:DescribeWarmPool, backup:DescribeFramework, backup:DescribeReportPlan, backup:ListFrameworks, backup:ListReportPlans, budgets:DescribeBudgetAction, budgets:DescribeBudgetActionsForAccount, budgets:DescribeBudgetActionsForBudget, budgets:ViewBudget, ce:GetAnomalyMonitors, ce:GetAnomalySubscriptions, cloud9:DescribeEnvironmentMemberships, cloud9:DescribeEnvironments, cloud9:ListEnvironments, cloud9:ListTagsForResource, cloudwatch:GetMetricStream, cloudwatch:ListMetricStreams, datasync:DescribeLocationFsxWindows, devops-guru:GetResourceCollection, ds:DescribeDirectories, ec2:DescribeTrafficMirrorTarge	Diese Richtlinie unterstützt jetzt zusätzliche Berechtigungen für Amazon AppFlow, Amazon, Amazon CloudWatch RUM CloudWatch, Amazon CloudWatch Synthetics, Amazon Connect-Kundenprofile, Amazon Connect Voice ID, Amazon DevOps Guru, Amazon Elastic Compute Cloud (Amazon EC2), Amazon EC2 Auto Scaling, Amazon EMR, Amazon, Amazon EventBridge Schemas EventBridge, Amazon Fraud Detector Amazon FinSpace, Amazon GameLift Servers, Amazon Interactive Video Service (Amazon IVS), Amazon Managed Service für Apache Flink, EC2 Image Builder, Amazon Lex, Amazon Lightsail, Amazon Location Service, Amazon Lookout for Equipment, Amazon Lookout for Metrics, Amazon Lookout for Vision, Amazon Managed Blockchain, Amazon MQ, Amazon Nimble StudioAmazon Pinpoint, Amazon QuickSight, Amazon Application Recovery Controller (ARC) Amazon Route 53 Resolver, , Amazon Simple Storage	7. September 2022

Änderung	Beschreibung	Datum
ts, ec2:GetNetworkInsightsAccessScopeAnalysisFindings, ec2:GetNetworkInsightsAccessScopeContent, elasticmapreduce:DescribeStudio, elasticmapreduce:GetStudioSessionMapping, elasticmapreduce:ListStudios, elasticmapreduce:ListStudioSessionMappings, events:DescribeEndpoint, events:DescribeEventBus, events:DescribeRule, events:ListArchives, events:ListEndpoints, events:ListEventBuses, events:ListRules, events:ListTagsForResource, events:ListTargetsByRule, finspace:GetEnvironment, finspace:ListEnvironments, frauddetector:GetDetectors, frauddetector:GetDetectorVersion, frauddetector:GetEntityTypes, frauddetector:GetEventTypes, frauddetector:GetExternalModels, frauddetector:GetLabels, frauddetector:GetModels, frauddetector:GetOutcomes, frauddetector:GetVariables, frauddetector:ListTagsForResource, gamelift:DescribeAlias, gamelift:DescribeBuild, gamelift:DescribeFleetAttributes, gamelift:DescribeFleetCapacity, gamelift:DescribeFleetLocat	Service (Amazon S3), Amazon SimpleDB, Amazon Simple Email Service (Amazon SES), Amazon Timestream, AWS AppConfig, AWS AppSync, AWS Auto Scaling, AWS Backup, AWS Budgets, AWS Cost Explorer AWS Cloud9 AWS Directory Service AWS DataSync AWS Elemental MediaPackage AWS Glue AWS IoT AWS IoT Analytics AWS IoT Events AWS IoT SiteWise, AWS IoT TwinMaker, AWS Lake Formation AWS License Manager, AWS Resilience Hub, AWS Signer, und AWS Transfer Family	

Änderung	Beschreibung	Datum
ionAttributes, gamelift:Des cribeFleetLocationCapacity, gamelift:DescribeFleetPort Settings, gamelift:Describe GameServerGroup, g amelift:DescribeGameSession Queues, gamelift:DescribeMa tchmakingConfigurations, ga melift:DescribeMatchmakingR uleSets, gamelift:DescribeR untimeConfiguration, gamelift: DescribeScript, gamelift:De scribeVpcPeeringAuthorizati ons, gamelift:ListAliases, gamelift:ListBuilds, gamelift: ListFleets, gamelift:ListGa meServerGroups, gamelift: ListScripts, gamelift:ListT agsForResource, geo:ListM aps, glue:GetClassifier, glue:GetClassifiers, imagebuil der:GetContainerRecipe, imagebuilder:GetImage, imagebuilder:GetImagePipeli ne, imagebuilder:GetImageRe cipe, imagebuilder:ListC ontainerRecipes, imagebuild er:ListImageBuildVersions, imagebuilder:ListImagePipel ines, imagebuilder:ListI mageRecipes, imagebuilder:L istImages, iot:DescribeCertif icate, iot:DescribeDimensio n, iot:DescribeRoleAlias, iot:DescribeSecurityProfile,		

Änderung	Beschreibung	Datum
iot:GetPolicy, iot:GetTopicRule, iot:GetTopicRuleDestination, iot:ListCertificates, iot:ListDimensions, iot:ListPolicies, iot:ListRoleAliases, iot:ListSecurityProfiles, iot:ListSecurityProfilesForTarget, iot:ListTagsForResource, iot:ListTargetsForSecurityProfile, iot:ListTopicRuleDestinations, iot:ListTopicRules, iot:ListV2LoggingLevels, iot:ValidateSecurityProfileBehaviors, iotanalytics:DescribeChannel, iotanalytics:DescribeDataset, iotanalytics:DescribeDatastore, iotanalytics:DescribePipeline, iotanalytics:ListChannels, iotanalytics:ListDatasets, iotanalytics:ListDatastores, iotanalytics:ListPipelines, iotanalytics:ListTagsForResource, iotevents:DescribeAlarmModel, iotevents:DescribeDetectorModel, iotevents:DescribeInput, iotevents:ListAlarmModels, iotevents:ListDetectorModels, iotevents:ListInputs, iotevents:ListTagsForResource, iotsitewise:DescribeAccessPolicy, iotsitewise:DescribeAsset, iotsitewise:ListAccessPolicies, iotsitewise:ListAssets,		

Änderung	Beschreibung	Datum
iottwinmaker:GetEntity, iottwinmaker:GetScene, iottwinmaker:GetWorksp ace, iottwinmaker:ListE ntities, iottwinmaker:ListS cenes, iottwinmaker:ListT agsForResource, iottwinmake r:ListWorkspaces, ivs:GetPl aybackKeyPair, ivs:GetRecor dingConfiguration, ivs:GetSt reamKey, ivs:ListChannels, ivs:ListPlaybackKeyPairs, i vs:ListRecordingConfigurati ons, ivs:ListStreamKeys, ivs:ListTagsForResource, kinesisanalytics:ListApplic ations, lakeformation:Descr ibeResource, lakeformation: GetDataLakeSettings, lakefo rmation:ListPermissions, lakeformation:ListResources , lex:DescribeBot, lex:Descr ibeBotAlias, lex:DescribeRe sourcePolicy, lex:ListB otAliases, lex:ListBotLocal es, lex:ListBots, lex:ListT agsForResource, license-manager:GetGrant, license-m anager:GetLicense, license-manager:ListDistributedGran ts, license-manager:ListLic enses, license-manager:List ReceivedGrants, lightsail :GetAlarms, lightsail:GetBu ckets, lightsail:GetCertificates,		

Änderung	Beschreibung	Datum
lightsail:GetDisk, lightsail:GetDisks, lightsail:GetInstance, lightsail:GetInstances, lightsail:GetKeyPair, lightsail:GetLoadBalancer, lightsail:GetLoadBalancers, lightsail:GetLoadBalancerTlsCertificates, lightsail:GetStaticIp, lightsail:GetStaticIps, lookoutequipment:DescribeInferenceScheduler, lookoutequipment:ListTagsForResource, lookoutmetrics:DescribeAlert, lookoutmetrics:DescribeAnomalyDetector, lookoutmetrics:ListAlerts, lookoutmetrics:ListAnomalyDetectors, lookoutmetrics:ListMetricSets, lookoutmetrics:ListTagsForResource, lookoutvision:DescribeProject, lookoutvision:ListProjects, managedblockchain:GetMember, managedblockchain:GetNetwork, managedblockchain:GetNode, managedblockchain:ListInvitations, managedblockchain:ListMembers, managedblockchain:ListNodes, mediapackage-vod:DescribePackagingGroup, mediapackage-vod:ListPackagingGroups, mediapackage-vod:ListTagsForResource, mobiletargeting:GetInAppTemplate, mobiletar		

Änderung	Beschreibung	Datum
geting:ListTemplates, mq:DescribeBroker, mq:ListBrokers, nimble:GetLaunchProfile, nimble:GetLaunchProfileDetails, nimble:GetStreamingImage, nimble:GetStudio, nimble:GetStudioComponent, nimble:ListLaunchProfiles, nimble:ListStreamingImages, nimble:ListStudioComponents, nimble:ListStudios, profile:GetDomain, profile:GetIntegration, profile:GetProfileObjectType, profile:ListDomains, profile:ListIntegrations, profile:ListProfileObjectTypes, profile:ListTagsForResource, quicksight:DescribeAnalysis, quicksight:DescribeAnalysisPermissions, quicksight:DescribeDataSet, quicksight:DescribeDataSetPermissions, quicksight:DescribeTheme, quicksight:DescribeThemePermissions, quicksight:ListAnalyses, quicksight:ListDataSets, quicksight:ListThemes, resiliencehub:DescribeApp, resiliencehub:DescribeAppVersionTemplate, resiliencehub:DescribeResiliencyPolicy, resiliencehub:ListApps, resiliencehub:ListAppVersionResourceMappings, resiliencehub:ListResiliencyP		

Änderung	Beschreibung	Datum
olicies, route53-recovery-r eadiness:GetCell, route53-r ecovery-readiness:GetReadin essCheck, route53-recovery- readiness:GetRecoveryGroup, route53-recovery-readiness :GetResourceSet, route53- recovery-readiness:ListCells, route53-recovery-readiness :ListReadinessChecks, route53-recovery-readin ess:ListRecoveryGroups, rou te53-recovery-readiness:Lis tResourceSets, route53resol ver:GetFirewallDomainList, route53resolver:GetFirewall RuleGroup, route53resolver: GetFirewallRuleGroupAssocia tion, route53resolver:GetRe solverQueryLogConfig, route53resolver:ListFir ewallDomainLists, route53re solver:ListFirewallDomains, route53resolver:ListFirewa llRuleGroupAssociations, ro ute53resolver:ListFirewallR uleGroups, route53resolver: ListFirewallRules, route53r esolver:ListResolverQueryLo gConfigs, rum:GetAppMonitor, rum:GetAppMonitorData, rum:ListAppMonitors, rum:Li stTagsForResource, s3- outposts:GetAccessPoint, s3-outposts:GetAccessPoint		

Änderung	Beschreibung	Datum
Policy, s3-outposts:GetBucket, s3-outposts:GetBucketPolicy, s3-outposts:GetBucketTagging, s3-outposts:GetLifecycleConfiguration, s3-outposts:ListAccessPoints, s3-outposts:ListEndpoints, s3-outposts:ListRegionalBuckets, schemas:DescribeDiscoverer, schemas:DescribeRegistry, schemas:DescribeSchema, schemas:ListDiscoverers, schemas:ListRegistries, schemas:ListSchemas, sdb:GetAttributes, sdb:ListDomains, ses:ListEmailTemplates, ses:ListReceiptFilters, ses:ListReceiptRuleSets, ses:ListTemplates, signer:GetSigningProfile, signer:ListProfilePermissions, signer:ListSigningProfiles, synthetics:DescribeCanaries, synthetics:DescribeCanariesLastRun, synthetics:DescribeRuntimeVersions, synthetics:GetCanary, synthetics:GetCanaryRuns, synthetics:ListTagsForResource, timestream:DescribeDatabase, timestream:DescribeTable, timestream:ListDatabases, timestream:ListTables, timestream:ListTagsForResource, transfer:DescribeServer, tr		

Änderung	Beschreibung	Datum
ansfer:DescribeUser, transfer: DescribeWorkflow, transfer: ListServers, transfer:ListUsers , transfer:ListWorkflows, voiceid:DescribeDomain, and voiceid:ListTagsForResource		
AWSConfigServiceRolePolicy – Addition: datasync:ListAgent s, datasync:ListLocations, datasync:ListTasks, servicedi scovery:ListNamespaces, ser vicediscovery:ListServices, and ses:ListContactLists	Diese Richtlinie gewährt nun die Erlaubnis, eine Liste von AWS DataSync Agenten, DataSync Quell- und Zielstand orten und DataSync Aufgaben in einer AWS-Konto Liste zurückzugeben, zusammenf assende Informationen über die AWS Cloud Map Names paces und Dienste aufzulisten, die mit einem oder mehreren angegebenen Namespace s in einem verknüpft sind AWS-Konto, und alle Kontaktli sten von Amazon Simple Email Service (Amazon SES) aufzulisten, die in verfügbar sind. AWS-Konto	22. August 2022

Änderung	Beschreibung	Datum
AWS_ConfigRole – Addition: datasync:ListAgents, datasync:ListLocations, dat async:ListTasks, servicedi scovery:ListNamespaces, ser vicediscovery:ListServices, and ses:ListContactLists	Diese Richtlinie gewährt nun die Erlaubnis, eine Liste von AWS DataSync Agenten, DataSync Quell- und Zielstand orten und DataSync Aufgaben in einer AWS-Konto Liste zurückzugeben, zusammenf assende Informationen über die AWS Cloud Map Names paces und Dienste aufzulisten, die mit einem oder mehreren angegebenen Namespace s in einem verknüpft sind AWS-Konto, und alle Kontaktli sten von Amazon Simple Email Service (Amazon SES) aufzulisten, die in verfügbar sind. AWS-Konto	22. August 2022
ConfigConformsServ iceRolePolicy – Addition: cloudwatch:PutMetricData	Diese Richtlinie gewährt nun die Erlaubnis, metrische Datenpunkte auf Amazon zu veröffentlichen CloudWatch.	25. Juli 2022

Änderung	Beschreibung	Datum
AWSConfigServiceRolePolicy – Addition: amplifyuibuilder:ExportThemes, amplifyuibuilder:GetTheme, appconfig:GetApplication, appconfig:GetApplication, appconfig:GetConfigurationProfile, appconfig:GetConfigurationProfile, appconfig:GetDeployment, appconfig:GetDeploymentStrategy, appconfig:GetEnvironment, appconfig:GetHostedConfigurationVersion, appconfig:ListTagsForResource, appsync:GetGraphqlApi, appsync:ListGraphqlApis, billingconductor:ListPricingRulesAssociatedToPricingPlan, billingconductor:ListAccountAssociations, billingconductor:ListBillingGroups, billingconductor:ListCustomLineItems, billingconductor:ListPricingPlans, billingconductor:ListPricingRules, billingconductor:ListTagsForResource, datasync:DescribeAgent, datasync:DescribeLocationEfs, datasync:DescribeLocationFsxLustre, datasync:DescribeLocationHdfs, datasync:DescribeLocationNfs, datasync:DescribeLocatio	Diese Richtlinie unterstützt jetzt zusätzliche Berechtigungen für Amazon Elastic Container Service (Amazon ECS), Amazon ElastiCache, Amazon EventBridge FSx, Amazon Managed Service für Apache Flink, Amazon Location Service, Amazon Managed Streaming for Apache Kafka, Amazon QuickSight, Amazon Rekognition, AWS RoboMaker, Amazon Simple Storage Service (Amazon S3), Amazon Simple Email Service (Amazon SES),,,, AWS Amplify, AWS AppConfig AWS AppSync AWS Billing Conductor AWS DataSync, AWS IAM Identity Center (IAM Identity Center) AWS Firewall Manager AWS Glue, EC2 Image Builder und Elastic Load Balancing.	15. Juli 2022

Änderung	Beschreibung	Datum
nObjectStorage, datasync:DescribeLocationS3, datasync:DescribeLocationSmb, datasync:DescribeTask, datasync:ListTagsForResource, ecr:DescribePullThroughCacheRules, ecr:DescribeRegistry, ecr:GetRegistryPolicy, elasticache:DescribeCacheParameters, elasticloadbalancing:DescribeListenerCertificates, elasticloadbalancing:DescribeTargetGroupAttributes, elasticloadbalancing:DescribeTargetGroups, elasticloadbalancing:DescribeTargetHealth, events:DescribeApiDestination, events:DescribeArchive, fms:GetNotificationChannel, fms:GetPolicy, fms:ListPolicies, fms:ListTagsForResource, fsx:DescribeVolumes, geo:DescribeGeofenceCollection, geo:DescribeMap, geo:DescribePlaceIndex, geo:DescribeRouteCalculator, geo:DescribeTracker, geo:ListTrackerConsumers, glue:BatchGetJobs, glue:BatchGetWorkflows, glue:GetCrawler, glue:GetCrawlers, glue:GetJob, glue:GetJobs, glue:GetWorkflow, imagebuilder: GetComponent, imagebuilder: ListComponentBuildVers		

Änderung	Beschreibung	Datum
ions, imagebuilder: ListCompo nents, imagebuilder:GetDist ributionConfiguration, imag ebuilder:GetInfrastructureC onfiguration, imagebuilder: ListDistributionConfigurati ons, imagebuilder:ListInfra structureConfigurations, kafka:DescribeClusterV2, kafka:ListClustersV2, kines isanalytics:DescribeApplica tion, kinesisanalytics:List TagsForResource, quicksight :DescribeDataSource, quicksight:DescribeDataS ourcePermissions, quicksigh t:ListTagsForResource, reko gnition:DescribeStreamProce ssor, rekognition:ListTagsF orResource, robomaker:Descr ibeRobotApplication, roboma ker:DescribeSimulationAppli cation, s3:GetStorageLensCo nfiguration, s3:GetStorageL ensConfigurationTagging, se rvicediscovery:GetInstance, servicediscovery:GetNamespa ce, servicediscovery:GetSer vice, servicediscovery:List TagsForResource, ses:Descr ibeReceiptRule, ses:Describ eReceiptRuleSet, ses:GetCo ntactList, ses:GetEmailTemp late, ses:GetTemplate, and		

Änderung	Beschreibung	Datum
sso:GetInlinePolicyForPermissionSet		

Änderung	Beschreibung	Datum
AWS_ConfigRole – Addition: amplifyuibuilder:ExportThemes, amplifyuibuilder:GetTheme, appconfig:GetApplication, appconfig:GetApplication, appconfig:GetConfigurationProfile, appconfig:GetConfigurationProfile, appconfig:GetDeployment, appconfig:GetDeploymentStrategy, appconfig:GetEnvironment, appconfig:GetHostedConfigurationVersion, appconfig:ListTagsForResource, appsync:GetGraphqlApi, appsync:ListGraphqlApis, billingconductor: ListPricingRulesAssociatedToPricingPlan, billingconductor:ListAccountAssociations, billingconductor:ListBillingGroups, billingconductor:ListCustomLineItems, billingconductor:ListPricingPlans, billingconductor:ListPricingRules, billingconductor:ListTagsForResource, datasync:DescribeAgent, datasync:DescribeLocationEfs, datasync:DescribeLocationFsxLustre, datasync:DescribeLocationHdfs, datasync:DescribeLocationNfs, datasync:DescribeLocationObjectStorage, datasync:De	Diese Richtlinie unterstützt jetzt zusätzliche Berechtigungen für Amazon Elastic Container Service (Amazon ECS), Amazon ElastiCache, Amazon EventBridge FSx, Amazon Managed Service für Apache Flink, Amazon Location Service, Amazon Managed Streaming for Apache Kafka, Amazon QuickSight, Amazon Rekognition, AWS RoboMaker, Amazon Simple Storage Service (Amazon S3), Amazon Simple Email Service (Amazon SES),,,, AWS Amplify, AWS AppConfig AWS AppSync AWS Billing Conductor AWS DataSync, AWS IAM Identity Center (IAM Identity Center) AWS Firewall Manager AWS Glue, EC2 Image Builder und Elastic Load Balancing.	15. Juli 2022

Änderung	Beschreibung	Datum
scribeLocationS3, datasync: DescribeLocationSmb, datasy nc:DescribeTask, datasync: ListTagsForResource, ecr:De scribePullThroughCacheRules , ecr:DescribeRegistry, ecr:G etRegistryPolicy, elasticac he:DescribeCacheParameters, elasticloadbalancing:Descr ibeListenerCertificates, el asticloadbalancing:Describe TargetGroupAttributes, elas ticloadbalancing:DescribeTa rgetGroups, elasticloadbala ncing:DescribeTargetHealth, events:DescribeApiDestinat ion, events:DescribeArchive, fms:GetNotificationChannel, fms:GetPolicy, fms:ListP olicies, fms:ListTagsForRes ource, fsx:DescribeVolumes, geo:DescribeGeofenceColl ection, geo:DescribeMap, geo:DescribePlaceIndex, geo:DescribeRouteCalculator , geo:DescribeTracker, geo:ListTrackerConsumers, g lue:BatchGetJobs, glue:Batc hGetWorkflows, glue:GetC rawler, glue:GetCrawlers, glue:GetJob, glue:GetJobs, glue:GetWorkflow, imagebuil der: GetComponent, imagebuil der: ListComponentBuildVers ions, imagebuilder: ListCompo		

Änderung	Beschreibung	Datum
nents, imagebuilder:GetDistributionConfiguration, imagebuilder:GetInfrastructureConfiguration, imagebuilder:ListDistributionConfigurations, imagebuilder:ListInfrastructureConfigurations, kafka:DescribeClusterV2, kafka:ListClustersV2, kinesisanalytics:DescribeApplication, kinesisanalytics:ListTagsForResource, quicksight:DescribeDataSource, quicksight:DescribeDataSourcePermissions, quicksight:ListTagsForResource, rekognition:DescribeStreamProcessor, rekognition:ListTagsForResource, robomaker:DescribeRobotApplication, robomaker:DescribeSimulationApplication, s3:GetStorageLensConfiguration, s3:GetStorageLensConfigurationTagging, servicediscovery:GetInstance, servicediscovery:GetNamespace, servicediscovery:GetService, servicediscovery:ListTagsForResource, ses:DescribeReceiptRule, ses:DescribeReceiptRuleSet, ses:GetContactList, ses:GetEmailTemplate, ses:GetTemplate, and		

Änderung	Beschreibung	Datum
sso:GetInlinePolicyForPermissionSet		

Änderung	Beschreibung	Datum
AWSConfigServiceRolePolicy – Addition: athena:GetDataCatalog, athena:ListDataCatalogs, athena:ListTagsForResource, detective:ListGraphs, detective:ListTagsForResource, glue:BatchGetDevEndpoints, glue:GetDevEndpoint, glue:GetDevEndpoints, glue:GetSecurityConfiguration, glue:GetSecurityConfigurations, glue:GetTags glue:GetWorkGroup, glue:ListCrawlers, glue:ListDevEndpoints, glue:ListJobs, glue:ListMembers, glue:ListWorkflows, glue:ListWorkGroups, guardduty:GetFilter, guardduty:GetIPSet, guardduty:GetThreatIntelSet, guardduty:GetMembers, guardduty:ListFilters, guardduty:ListIPSets, guardduty:ListTagsForResource, guardduty:ListThreatIntelSets, macie:GetMacieSession, ram:GetResourceShareAssociations, ram:GetResourceShares, ses:GetConfigurationSet, ses:GetConfigurationSetEventDestinations, ses:ListConfigurationSets, sso:DescribeInstanceAccessControlAtt	Diese Richtlinie gewährt nun die Erlaubnis, einen bestimmten Amazon Athena Athena-Datenkatalog abzurufen, die Athena-Datenkataloge in einem aufzulisten und Tags aufzulisten AWS-Konto, die mit einer Athena-Arbeitsgruppe oder Datenkatalogressource verknüpft sind; um eine Liste von Amazon Detective-Verhaltensdiagrammen und Listen-Tags für ein Detective-Verhaltensdiagramm abzurufen; eine Liste von Ressourcenmetadaten für eine bestimmte Liste von AWS Glue Entwicklungsendpunktnamen abzurufen, Informationen über einen bestimmten AWS Glue Entwicklungsendpunkt abzurufen, alle AWS Glue Entwicklungsendpunkte in einem, abzurufen AWS-Konto AWS Glue Konfiguration, alle AWS Glue Sicherheitskonfigurationen abrufen, eine Liste der mit einer AWS Glue Ressource verknüpften Tags abrufen, Informationen über eine AWS Glue Arbeitsgruppe mit dem angegebenen Namen abrufen, die Namen aller AWS	31. Mai 2022

Änderung	Beschreibung	Datum
ributeConfiguration, sso:DescribePermissionSet, sso:ListManagedPoliciesInPermissionSet, sso:ListPermissionSets, and sso:ListTagsForResource	Glue Crawler-Ressourcen in einem AWS Konto abrufen, die Namen aller AWS Glue `DevEndpoint` Ressourcen in einem abrufen AWS-Konto, die Namen aller AWS Glue Jobressourcen in einem auflisten AWS-Konto, Details zu AWS Glue Mitgliedskonten abrufen, Namen von AWS Glue Workflows auflisten, in einem Konto erstellte Workflows auflisten und verfügbare AWS Glue Arbeitsgruppen für ein Konto auflisten; um Details zu einem GuardDuty Amazon-Filter abzurufen, einen abzurufen GuardDuty IPSet, einen abzurufen GuardDutyThreatIntelSet, GuardDuty Mitgliedskonten abzurufen, eine Filterliste abzurufen, den IPSets GuardDuty Service abzurufen, Tags für den GuardDuty Service abzurufen und den ThreatIntelSets des GuardDuty Service abzurufen; um den aktuellen Status und die Konfigurationseinstellungen für ein Amazon Macie-Konto abzurufen; um die Ressourcen- und Hauptzuordnungen für AWS Resource Access Manager	

Änderung	Beschreibung	Datum
	(AWS RAM) Resource Shares abzurufen und Details AWS RAM zur Ressource abzurufen GuardDuty teilt; um Informationen über einen vorhandenen Konfigura tionssatz von Amazon Simple Email Service (Amazon SES) abzurufen, eine Liste von Ereigniszielen abzurufen, die mit einem Amazon SES SES-Konfigurationssatz verknüpft sind, und um alle mit einem Amazon SES-Konto verknüpften Konfigura tionssätze aufzurufen; und um eine Liste von Identity Center-Verzeichnisattribute n abzurufen, die Details eines AWS IAM Identity Center Berechtigungssatze s abzurufen, die IAM-verwa ltete Richtlinie abzurufen, die mit einem bestimmten IAM Identity Center-Berechtigun gssatz verknüpft ist, den Berechtigungssatz für ein IAM abzurufen Identity Center-In stanz und Abrufen von Tags für IAM Identity Ressourcen des Zentrums.	

Änderung	Beschreibung	Datum
AWS_ConfigRole – Addition: athena:GetDataCatalog, athena:ListDataCatalogs, athena:ListTagsForResource, detective:ListGraphs, detective:ListTagsForResource, glue:BatchGetDevEndpoints, glue:GetDevEndpoint, glue:GetDevEndpoints, glue:GetSecurityConfiguration, glue:GetSecurityConfigurations, glue:GetTags glue:GetWorkGroup, glue:ListCrawlers, glue:ListDevEndpoints, glue:ListJobs, glue:ListMembers, glue:ListWorkflows, glue:ListWorkGroups, guardduty:GetFilter, guardduty:GetIPSet, guardduty:GetThreatIntelSet, guardduty:GetMembers, guardduty:ListFilters, guardduty:ListIPSets, guardduty:ListTagsForResource, guardduty:ListThreatIntelSets, macie:GetMacieSession, ram:GetResourceShareAssociations, ram:GetResourceShares, ses:GetConfigurationSet, ses:GetConfigurationSetEventDestinations, ses:ListConfigurationSets, sso:DescribeInstanceAccessControlAttributeConfiguration, sso:De	Diese Richtlinie gewährt nun die Erlaubnis, einen bestimmten Amazon Athena Athena-Datenkatalog abzurufen, die Athena-Datenkataloge in einem aufzulisten und Tags aufzulisten AWS-Konto, die mit einer Athena-Arbeitsgruppe oder Datenkatalogressource verknüpft sind; um eine Liste von Amazon Detective-Verhaltensdiagrammen und Listen-Tags für ein Detective-Verhaltensdiagramm abzurufen; eine Liste von Ressourcenmetadaten für eine bestimmte Liste von AWS Glue Entwicklungsendpunktnamen abzurufen, Informationen über einen bestimmten AWS Glue Entwicklungsendpunkt abzurufen, alle AWS Glue Entwicklungsendpunkte in einem, abzurufen AWS-Konto AWS Glue Konfiguration, alle AWS Glue Sicherheitskonfigurationen abrufen, eine Liste der mit einer AWS Glue Ressource verknüpften Tags abrufen, Informationen über eine AWS Glue Arbeitsgruppe mit dem angegebenen Namen abrufen, die Namen aller AWS	31. Mai 2022

Änderung	Beschreibung	Datum
scribePermissionSet, sso:ListManagedPoliciesInPermissionSet, sso:ListPermissionSets, and sso:ListTagsForResource	Glue Crawler-Ressourcen in einem AWS Konto abrufen, die Namen aller AWS Glue `DevEndpoint` Ressourcen in einem abrufen AWS-Konto, die Namen aller AWS Glue Jobressourcen in einem auflisten AWS-Konto, Details zu AWS Glue Mitgliedskonten abrufen, Namen von AWS Glue Workflows auflisten, in einem Konto erstellte Workflows auflisten und verfügbare AWS Glue Arbeitsgruppen für ein Konto auflisten; um Details zu einem GuardDuty Amazon-Filter abzurufen, einen abzurufen GuardDuty IPSet, einen abzurufen GuardDutyThreatIntelSet, GuardDuty Mitgliedskonten abzurufen, eine Filterliste abzurufen, den IPSets GuardDuty Service abzurufen, Tags für den GuardDuty Service abzurufen und den ThreatIntelSets des GuardDuty Service abzurufen; um den aktuellen Status und die Konfigurationseinstellungen für ein Amazon Macie-Konto abzurufen; um die Ressourcen- und Hauptzuordnungen für AWS Resource Access Manager	

Änderung	Beschreibung	Datum
	(AWS RAM) Resource Shares abzurufen und Details AWS RAM zur Ressource abzurufen GuardDuty teilt; um Informationen über einen vorhandenen Konfigura tionssatz von Amazon Simple Email Service (Amazon SES) abzurufen, eine Liste von Ereigniszielen abzurufen, die mit einem Amazon SES SES-Konfigurationssatz verknüpft sind, und um alle mit einem Amazon SES-Konto verknüpften Konfigura tionssätze aufzurufen; und um eine Liste von Identity Center-Verzeichnisattribute n abzurufen, die Details eines AWS IAM Identity Center Berechtigungssatze s abzurufen, die IAM-verwa ltete Richtlinie abzurufen, die mit einem bestimmten IAM Identity Center-Berechtigun gssatz verknüpft ist, den Berechtigungssatz für ein IAM abzurufen Identity Center-In stanz und Abrufen von Tags für IAM Identity Ressourcen des Zentrums.	

Änderung	Beschreibung	Datum
AWSConfigServiceRolePolicy – Addition: cloudformation:GetResource, cloudformation:ListResources, cloudtrail:GetEventDataStore, cloudtrail:ListEventDataStores, dax:DescribeParameterGroups, dax:DescribeParameters, dax:DescribeSubnetGroups, DMS:DescribeReplicationTasks, and organizations:ListPolicies	Diese Richtlinie gewährt nun die Berechtigung, Informationen über alle oder einen bestimmten AWS CloudTrail Event Data Store (EDS) abzurufen, Informationen über alle oder eine bestimmte AWS CloudFormation Ressource abzurufen, eine Liste einer DynamoDB Accelerator (DAX) -Parametergruppe oder Subnetzgruppe abzurufen, Informationen über AWS Database Migration Service (AWS DMS) Replikationsaufgaben für Ihr Konto in der aktuellen Region abzurufen, auf die zugegriffen wird, und eine Liste aller Richtlinien eines AWS Organizations bestimmten Typs abzurufen.	7. April 2022

Änderung	Beschreibung	Datum
AWS_ConfigRole – Addition: cloudformation:GetResource, cloudformation:ListResources, cloudtrail:GetEventDataStore, cloudtrail:ListEventDataStores, dax:DescribeParameterGroups, dax:DescribeParameters, dax:DescribeSubnetGroups, DMS:DescribeReplicationTasks, and organizations:ListPolicies	Diese Richtlinie gewährt nun die Berechtigung, Informationen über alle oder einen bestimmten AWS CloudTrail Event Data Store (EDS) abzurufen, Informationen über alle oder eine bestimmte AWS CloudFormation Ressource abzurufen, eine Liste einer DynamoDB Accelerator (DAX) -Parametergruppe oder Subnetzgruppe abzurufen, Informationen über AWS Database Migration Service (AWS DMS) Replikationsaufgaben für Ihr Konto in der aktuellen Region abzurufen, auf die zugegriffen wird, und eine Liste aller Richtlinien eines AWS Organizations bestimmten Typs abzurufen.	7. April 2022

Änderung	Beschreibung	Datum
AWSConfigServiceRolePolicy – Addition: backup-gateway:ListTagsForResource, backup-gateway:ListVirtualMachines, batch:DescribeComputeEnvironments, batch:DescribeJobQueues, batch:ListTagsForResource, dax:ListTags, dms:DescribeCertificates, dynamodb:DescribeGlobalTable, dynamodb:DescribeGlobalTableSettings, ec2:DescribeClientVpnAuthorizationRules, ec2:DescribeClientVpnEndpoints, ec2:DescribeDhcpOptions, ec2:DescribeFleets, ec2:DescribeNetworkAcls, ec2:DescribePlacementGroups, ec2:DescribeSpotFleetRequests, ec2:DescribeVolumeAttribute, ec2:DescribeVolumes, eks:DescribeFargateProfile, eks:ListFargateProfiles, eks:ListTagsForResource, fsx:ListTagsForResource, guardduty:ListOrganizationAdminAccounts, kms:ListAliases, opsworks:DescribeLayers, opsworks:DescribeStacks, opsworks:ListTags, rds:DescribeDBClusterParameterGroups, rds:DescribeDBClusterPara	Diese Richtlinie unterstützt jetzt zusätzliche Berechtigungen für AWS Backup, AWS Batch, DynamoDB Accelerator, AWS Database Migration Service, Amazon DynamoDB, Amazon Elastic Compute Cloud (Amazon EC2), Amazon Elastic Kubernetes Service, Amazon, Amazon,, FSx GuardDuty, Amazon Relational Database Service AWS Key Management Service AWS OpsWorks, V2 und Amazon. AWS WAF WorkSpaces	14. März 2022

Änderung	Beschreibung	Datum
meters, states:DescribeActivity, states:ListActivities, wafv2:GetRuleGroup, wafv2:ListRuleGroups, wafv2:ListTagsForResource, workspaces:DescribeConnectionAliases, workspaces:DescribeTags, and workspaces:DescribeWorkspaces		

Änderung	Beschreibung	Datum
AWS_ConfigRole – Addition: backup-gateway:ListTagsForResource, backup-gateway:ListVirtualMachines, batch:DescribeComputeEnvironments, batch:DescribeJobQueues, batch:ListTagsForResource, dax:ListTags, dms:DescribeCertificates, dynamodb:DescribeGlobalTable, dynamodb:DescribeGlobalTableSettings, ec2:DescribeClientVpnAuthorizationRules, ec2:DescribeClientVpnEndpoints, ec2:DescribeDhcpOptions, ec2:DescribeFleets, ec2:DescribeNetworkAcls, ec2:DescribePlacementGroups, ec2:DescribeSpotFleetRequests, ec2:DescribeVolumeAttribute, ec2:DescribeVolumes, eks:DescribeFargateProfile, eks:ListFargateProfiles, eks:ListTagsForResource, fsx:ListTagsForResource, guardduty:ListOrganizationAdminAccounts, kms:ListAliases, opsworks:DescribeLayers, opsworks:DescribeStacks, opsworks:ListTags, rds:DescribeDBClusterParameterGroups, rds:DescribeDBClusterParameters, states:DescribeAct	Diese Richtlinie unterstützt jetzt zusätzliche Berechtigungen für AWS Backup, AWS Batch, DynamoDB Accelerator, AWS Database Migration Service, Amazon DynamoDB, Amazon Elastic Compute Cloud (Amazon EC2), Amazon Elastic Kubernetes Service, Amazon, Amazon,, FSx GuardDuty, Amazon Relational Database Service AWS Key Management Service AWS OpsWorks, V2 und Amazon. AWS WAF WorkSpaces	14. März 2022

Änderung	Beschreibung	Datum
ivity, states:ListActivities, wafv2:GetRuleGroup, wafv2:ListRuleGroups, wafv2:ListTagsForResource, workspaces:DescribeConnectionAliases, workspaces:DescribeTags, and workspaces:DescribeWorkspaces		

Änderung	Beschreibung	Datum
AWSConfigServiceRolePolicy – Addition: elasticbeanstalk:DescribeEnvironments, elasticbeanstalk:DescribeConfigurationSettings, account:GetAlternateContact, organizations:DescribePolicy, organizations:ListParents, organizations:ListPoliciesForTarget, es:GetCompatibleElasticsearchVersions, rds:DescribeOptionGroups, rds:DescribeOptionGroups, es:GetCompatibleVersions, codedeploy:GetDeploymentConfig, ecr-public:GetRepositoryPolicy, access-analyzer:GetArchiveRule, and ecs:ListTaskDefinitionFamilies	Diese Richtlinie gewährt nun die Erlaubnis, Details zu Elastic Beanstalk Beanstalk-Umgebungen und eine Beschreibung der Einstellungen für den angegebenen Elastic Beanstalk Beanstalk-Konfigurationssatz abzurufen, eine Übersicht der OpenSearch Elasticsearch-Versionen abzurufen, die verfügbaren Amazon RDS-Optionsgruppen für eine Datenbank zu beschreiben und Informationen über eine Bereitstellungskonfiguration abzurufen. CodeDeploy Diese Richtlinie gewährt jetzt auch die Erlaubnis, den angegebenen alternativen Kontakt abzurufen, der an eine angehängt ist AWS-Konto, Informationen über eine AWS Organizations Richtlinie abzurufen, eine Amazon ECR-Repository-Richtlinie abzurufen, Informationen über eine archivierte AWS Config Regel abzurufen, eine Liste von Amazon ECS-Aufgabendefinitionsfamilien abzurufen, die Stamm- oder übergeordneten Organisationseinheiten (OUs) der angegebenen untergeor	10. Februar 2022

Änderung	Beschreibung	Datum
	dneten Organisationseinhe it oder des angegebenen untergeordneten Kontos aufzulisten und die Richtlini en aufzulisten, die dem angegebenen Zielstamm, der Organisationseinheit oder dem angegebenen Zielkonto zugeordnet sind.	

Änderung	Beschreibung	Datum
AWS_ConfigRole – Addition: elasticbeanstalk:DescribeEnvironments, elasticbeanstalk:DescribeConfigurationSettings, account:GetAlternateContact, organizations:DescribePolicy, organizations:ListParents, organizations:ListPoliciesForTarget, es:GetCompatibleElasticsearchVersions, rds:DescribeOptionGroups, rds:DescribeOptionGroups, es:GetCompatibleVersions, codedeploy:GetDeploymentConfig, ecr-public:GetRepositoryPolicy, access-analyzer:GetArchiveRule, and ecs:ListTaskDefinitionFamilies	Diese Richtlinie gewährt nun die Erlaubnis, Details zu Elastic Beanstalk Beanstalk-Umgebungen und eine Beschreibung der Einstellungen für den angegebenen Elastic Beanstalk Beanstalk-Konfigurationssatz abzurufen, eine Übersicht der OpenSearch Elasticsearch-Versionen abzurufen, die verfügbaren Amazon RDS-Optionsgruppen für eine Datenbank zu beschreiben und Informationen über eine Bereitstellungskonfiguration abzurufen. CodeDeploy Diese Richtlinie gewährt jetzt auch die Erlaubnis, den angegebenen alternativen Kontakt abzurufen, der an eine angehängt ist AWS-Konto, Informationen über eine AWS Organizations Richtlinie abzurufen, eine Amazon ECR-Repository-Richtlinie abzurufen, Informationen über eine archivierte AWS Config Regel abzurufen, eine Liste von Amazon ECS-Aufgabendefinitionsfamilien abzurufen, die Stamm- oder übergeordneten Organisationseinheiten (OUs) der angegebenen untergeor	10. Februar 2022

Änderung	Beschreibung	Datum
	dneten Organisationseinheit oder des angegebenen untergeordneten Kontos aufzulisten und die Richtlinien aufzulisten, die dem angegebenen Zielstamm, der Organisationseinheit oder dem angegebenen Zielkonto zugeordnet sind.	
AWSConfigServiceRolePolicy – Addition: logs:CreateLogStream, logs:CreateLogGroup, and logs:PutLogEvent	Diese Richtlinie gewährt nun die Erlaubnis, CloudWatch Amazon-Protokollgruppen und -Streams zu erstellen und Protokolle in erstellte Protokollstreams zu schreiben.	15. Dezember 2021
AWS_ConfigRole – Addition: logs:CreateLogStream, logs:CreateLogGroup, and logs:PutLogEvent	Diese Richtlinie gewährt nun die Erlaubnis, CloudWatch Amazon-Protokollgruppen und -Streams zu erstellen und Protokolle in erstellte Protokollstreams zu schreiben.	15. Dezember 2021

Änderung	Beschreibung	Datum
AWSConfigServiceRolePolicy – Addition: es:DescribeDomain, es:DescribeDomains, rds:DescribeDBParameters, and, elasticache:DescribeSnapshots	Diese Richtlinie gewährt nun die Erlaubnis, Details zu einem Amazon OpenSearch Service (OpenSearch Service) domain/domains und eine detaillierte Parameterliste für eine bestimmte Amazon Relational Database Service (Amazon RDS) DB-Parametergruppe abzurufen. Diese Richtlinie gewährt auch die Erlaubnis, Details zu ElastiCache Amazon-Snapshots abzurufen.	8. September 2021
AWS_ConfigRole – Addition: es:DescribeDomain, es:DescribeDomains, rds:DescribeDBParameters, and, elasticache:DescribeSnapshots	Diese Richtlinie gewährt nun die Erlaubnis, Details zu einem Amazon OpenSearch Service (OpenSearch Service) domain/domains und eine detaillierte Parameterliste für eine bestimmte Amazon Relational Database Service (Amazon RDS) DB-Parametergruppe abzurufen. Diese Richtlinie gewährt auch die Erlaubnis, Details zu ElastiCache Amazon-Snapshots abzurufen.	8. September 2021

Änderung	Beschreibung	Datum
AWSConfigServiceRolePolicy— Hinzufügen logs:ListTagsLogGroup, states:ListTagsForResource, states:ListStateMachines, states:DescribeStateMachine und zusätzliche Berechtigungen für AWS Ressourcentypen	Diese Richtlinie gewährt die Berechtigung, Tags für eine Protokollgruppe, Tags für eine Zustandsmaschine und alle Zustandsmaschinen aufzulisten. Diese Richtlinie gewährt die Berechtigung zum Abrufen von Details über eine Zustandsmaschine. Diese Richtlinie unterstützt jetzt auch zusätzliche Berechtigungen für Amazon EC2 Systems Manager (SSM), Amazon Elastic Container Registry, Amazon, Amazon Data Firehose FSx, Amazon Managed Streaming for Apache Kafka (Amazon MSK), Amazon Relational Database Service (Amazon RDS), Amazon Route 53, Amazon SageMaker AI, Amazon Simple Notification Service,, und. AWS Database Migration Service AWS Global Accelerator AWS Storage Gateway	28. Juli 2021

Änderung	Beschreibung	Datum
AWS_ConfigRole— Fügen Sie l und zusätzliche Berechtig ungen für ogs:ListTagsLogGro up, states:ListTagsFor Resource, states:ListStateM achines, states:DescribeSta teMachine Ressourcentypen hinzu AWS	Diese Richtlinie gewährt die Berechtigung, Tags für eine Protokollgruppe, Tags für eine Zustandsmaschine und alle Zustandsmaschinen aufzulisten. Diese Richtlini e gewährt die Berechtigung zum Abrufen von Details über eine Zustandsmaschine. Diese Richtlinie unterstützt jetzt auch zusätzliche Berechtig ungen für Amazon EC2 Systems Manager (SSM), Amazon Elastic Container Registry, Amazon, Amazon Data Firehose FSx, Amazon Managed Streaming for Apache Kafka (Amazon MSK), Amazon Relational Database Service (Amazon RDS), Amazon Route 53, Amazon SageMaker AI, Amazon Simple Notification Service,, und. AWS Database Migration Service AWS Global Accelerat or AWS Storage Gateway	28. Juli 2021

Änderung	Beschreibung	Datum
AWSConfigServiceRolePolicy— Zusätzliche Berechtigungen für ssm:DescribeDocumentPermission Ressourcentypen hinzufügen AWS	Diese Richtlinie gewährt die Berechtigung, die Berechtigungen von AWS Systems Manager -Dokumenten und Informationen zu IAM Access Analyzer einzusehen. Diese Richtlinie unterstützt jetzt zusätzliche AWS Ressourcentypen für Amazon Kinesis, Amazon ElastiCache, Amazon EMR AWS Network Firewall, Amazon Route 53 und Amazon Relational Database Service (Amazon RDS). Diese Berechtigungsänderungen ermöglichen das Aufrufen des Nur-Lese-Modus AWS Config , der zur Unterstützung dieser Ressourcentypen APIs erforderlich ist. Diese Richtlinie unterstützt jetzt auch das Filtern von Lambda @Edge -Funktionen für die lambda-inside-vpc AWS Config verwaltete Regel.	8. Juni 2021

Änderung	Beschreibung	Datum
AWS_ConfigRole— Zusätzliche Berechtigungen für AWS Ressourcentypen hinzufügen ssm:DescribeDocumentPermission	Diese Richtlinie gewährt die Berechtigung, die Berechtigungen von AWS Systems Manager -Dokumenten und Informationen zu IAM Access Analyzer einzusehen. Diese Richtlinie unterstützt jetzt zusätzliche AWS Ressourcentypen für Amazon Kinesis, Amazon ElastiCache, Amazon EMR AWS Network Firewall, Amazon Route 53 und Amazon Relational Database Service (Amazon RDS). Diese Berechtigungsänderungen ermöglichen das Aufrufen des Nur-Lese-Modus AWS Config , der zur Unterstützung dieser Ressourcentypen APIs erforderlich ist. Diese Richtlinie unterstützt jetzt auch das Filtern von Lambda @Edge -Funktionen für die lambda-inside-vpc AWS Config verwaltete Regel.	8. Juni 2021

Änderung	Beschreibung	Datum
AWSConfigServiceRolePolicy— Fügen Sie die apigateway:GET Erlaubnis hinzu, schreibgeschützte GET-Aufrufe an API Gateway zu tätigen, sowie die s3:GetAccessPointPolicy Erlaubnis und s3:GetAccessPointPolicyStatus Erlaubnis, Amazon S3 schreibgeschützt aufzurufen APIs	Diese Richtlinie gewährt nun Berechtigungen, die es AWS Config ermöglichen, schreibgeschützte GET-Aufrufe an API Gateway zu tätigen, um eine AWS Config Regel für API Gateway zu unterstützen. Die Richtlinie fügt außerdem Berechtigungen hinzu, die es AWS Config ermöglichen, Amazon Simple Storage Service (Amazon S3) schreibgeschützt aufzurufen APIs, die zur Unterstützung des neuen `AWS::S3::AccessPoint` Ressourcentyps erforderlich sind.	10. Mai 2021

Änderung	Beschreibung	Datum
AWS_CconfigRole — Fügen Sie die apigatewa y:GET Erlaubnis hinzu, schreibgeschützte GET-Aufrufe an API Gateway zu tätigen, sowie die s3:GetAcc essPointPolicy Erlaubnis und s3:GetAccessPointPolicyStat us Erlaubnis, Amazon S3 schreibgeschützt aufzurufen APIs	Diese Richtlinie gewährt nun Berechtigungen, die es AWS Config ermöglichen, schreibge schützte GET-Aufrufe an API Gateway zu senden, um ein AWS Config für API Gateway zu unterstützen. Die Richtlini e fügt außerdem Berechtig ungen hinzu, die es AWS Config ermöglichen, Amazon Simple Storage Service (Amazon S3) schreibgeschützt aufzurufen APIs, die zur Unterstützung des neuen `AWS::S3::AccessPoint` Ressourcentyps erforderlich sind.	10. Mai 2021

Änderung	Beschreibung	Datum
AWSConfigServiceRolePolicy— Fügen Sie ssm:ListDocuments Berechtigungen und zusätzliche Berechtigungen für Ressourcentypen hinzu AWS	Diese Richtlinie gewährt die Berechtigung zum Anzeigen von Informationen zu AWS Systems Manager -spezifizierten Dokumenten. Diese Richtlinie unterstützt jetzt auch zusätzliche AWS Ressourcentypen für AWS Backup Amazon Elastic File System, Amazon ElastiCache, Amazon Simple Storage Service (Amazon S3), Amazon Elastic Compute Cloud (Amazon EC2), Amazon Kinesis AWS Database Migration Service, Amazon SageMaker AI und Amazon Route 53. Diese Berechtigungsänderungen ermöglichen AWS Config das Aufrufen des Nur-Lese-Modus, der zur Unterstützung dieser APIs Ressourcentypen erforderlich ist.	1. April 2021

Änderung	Beschreibung	Datum
AWS_ConfigRole— Fügen Sie ssm:ListDocuments Berechtigungen und zusätzliche Berechtigungen für Ressourcentypen hinzu AWS	Diese Richtlinie gewährt die Berechtigung zum Anzeigen von Informationen zu AWS Systems Manager -spezifizierten Dokumenten. Diese Richtlinie unterstützt jetzt auch zusätzliche AWS Ressourcentypen für AWS Backup Amazon Elastic File System, Amazon ElastiCache, Amazon Simple Storage Service (Amazon S3), Amazon Elastic Compute Cloud (Amazon EC2), Amazon Kinesis AWS Database Migration Service, Amazon SageMaker AI und Amazon Route 53. Diese Berechtigungsänderungen ermöglichen AWS Config das Aufrufen des Nur-Lese-Modus, der zur Unterstützung dieser APIs Ressourcentypen erforderlich ist.	1. April 2021
`AWSConfigRole` wird nicht mehr unterstützt.	`AWSConfigRole` wird nicht mehr unterstützt. Die Ersatzrichtlinie lautet `AWS_ConfigRole` .	1. April 2021
AWS Config hat begonnen, Änderungen zu verfolgen	AWS Config hat begonnen, Änderungen für die AWS verwalteten Richtlinien zu verfolgen.	1. April 2021

Berechtigungen für die IAM-Rolle wurden zugewiesen AWS Config

Mit einer IAM-Rolle können Sie eine Reihe von Berechtigungen definieren. AWS Config übernimmt die Rolle, die Sie ihr zuweisen, um in Ihren S3-Bucket zu schreiben, in Ihrem SNS-Thema zu veröffentlichen und Anfragen `Describe` oder `List` API-Anfragen zu stellen, um Konfigurationsdetails für Ihre AWS Ressourcen abzurufen. Weitere Informationen zu IAM-Rollen finden Sie unter IAM-Rollen im IAM-Benutzerhandbuch.

Wenn Sie die AWS Config Konsole verwenden, um eine IAM-Rolle zu erstellen oder zu aktualisieren, fügt sie AWS Config automatisch die erforderlichen Berechtigungen für Sie hinzu. Weitere Informationen finden Sie unter Einrichtung AWS Config mit der Konsole.

> **Richtlinien und Compliance-Ergebnisse**
>
> IAM-Richtlinien und andere Richtlinien, die in verwaltet werden, AWS Organizations können sich darauf auswirken, ob Sie AWS Config berechtigt sind, Konfigurationsänderungen für Ihre Ressourcen aufzuzeichnen. Darüber hinaus bewerten Regeln direkt die Konfiguration einer Ressource, und Regeln berücksichtigen diese Richtlinien bei der Durchführung von Evaluierungen nicht. Stellen Sie sicher, dass die geltenden Richtlinien mit der Art und Weise übereinstimmen, wie Sie sie verwenden möchten AWS Config.

Inhalt

- Erstellen von IAM-Rollenrichtlinien
  - Hinzufügen einer IAM-Vertrauensrichtlinie für Ihre Rolle
  - IAM-Rollenrichtlinie für Ihren S3-Bucket
  - IAM-Rollenrichtlinie für KMS-Schlüssel
  - IAM-Rollenrichtlinie für ein Amazon-SNS-Thema
  - IAM-Rollenrichtlinie für den Abruf von Konfigurationsdetails
  - Verwaltung von Berechtigungen für die S3-Bucket-Aufzeichnung

Erstellen von IAM-Rollenrichtlinien

Wenn Sie die AWS Config Konsole verwenden, um eine IAM-Rolle zu erstellen, AWS Config werden der Rolle automatisch die erforderlichen Berechtigungen für Sie zugewiesen.

Wenn Sie die AWS CLI zum Einrichten AWS Config oder Aktualisieren einer vorhandenen IAM-Rolle verwenden, müssen Sie die Richtlinie manuell aktualisieren, damit AWS Config Sie auf Ihren S3-Bucket zugreifen, in Ihrem SNS-Thema veröffentlichen und Konfigurationsdetails zu Ihren Ressourcen abrufen können.

Hinzufügen einer IAM-Vertrauensrichtlinie für Ihre Rolle

Sie können eine IAM-Vertrauensrichtlinie erstellen, die es Ihnen ermöglicht, eine Rolle anzunehmen und diese AWS Config zur Nachverfolgung Ihrer Ressourcen zu verwenden. Weitere Informationen zu Vertrauensrichtlinien finden Sie unter Rollenbegriffe und -Konzepte im IAM-Benutzerhandbuch.

Im Folgenden finden Sie ein Beispiel für eine Vertrauensrichtlinie für AWS Config Rollen:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "",
      "Effect": "Allow",
      "Principal": {
        "Service": "config.amazonaws.com"
      },
      "Action": "sts:AssumeRole",
      "Condition": {
        "StringEquals": {
          "AWS:SourceAccount": "sourceAccountID"
        }
      }
    }
  ]
}
```

Sie können die obige Bedingung `AWS:SourceAccount` in der IAM-Rollenvertrauensbeziehung verwenden, um den Config-Service-Prinzipal so zu beschränken, dass er nur mit der AWS -IAM-Rolle interagiert, wenn er Operationen für bestimmte Konten ausführt.

AWS Config unterstützt auch die `AWS:SourceArn` Bedingung, dass der Config-Dienstprinzipal nur dann die IAM-Rolle übernimmt, wenn er Operationen im Namen des Eigentümerkontos ausführt. Wenn Sie den AWS Config Service Principal verwenden, wird als `AWS:SourceArn` Eigenschaft immer festgelegt, `arn:aws:config:sourceRegion:sourceAccountID:*` wo sich die Region des vom Kunden verwalteten Konfigurationsrekorders `sourceRegion` befindet. Dabei

`sourceAccountID` handelt es sich um die ID des Kontos, das den vom Kunden verwalteten Konfigurationsrekorder enthält.

Fügen Sie beispielsweise die folgende Bedingung hinzu, beschränken Sie den Config-Dienstprinzipal so, dass er die IAM-Rolle nur im Namen eines vom Kunden verwalteten Konfigurationsrekorders in der `us-east-1` Region des Kontos übernimmt`123456789012`:`"ArnLike": {"AWS:SourceArn": "arn:aws:config:us-east-1:123456789012:*"}`.

IAM-Rollenrichtlinie für Ihren S3-Bucket

Die folgende Beispielrichtlinie gewährt die AWS Config Erlaubnis, auf Ihren S3-Bucket zuzugreifen:

```
{
  "Version":"2012-10-17",
  "Statement":[
    {
      "Effect":"Allow",
      "Action":[
        "s3:PutObject",
        "s3:PutObjectAcl"
      ],
      "Resource":[
        "arn:aws:s3:::amzn-s3-demo-bucket/prefix/AWSLogs/myAccountID/*"
      ],
      "Condition":{
        "StringLike":{
          "s3:x-amz-acl":"bucket-owner-full-control"
        }
      }
    },
    {
      "Effect":"Allow",
      "Action":[
        "s3:GetBucketAcl"
      ],
      "Resource":"arn:aws:s3:::amzn-s3-demo-bucket"
    }
  ]
}
```

IAM-Rollenrichtlinie für KMS-Schlüssel

Die folgende Beispielrichtlinie erteilt die AWS Config Erlaubnis, KMS-basierte Verschlüsselung für neue Objekte für die S3-Bucket-Lieferung zu verwenden:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "kms:Decrypt",
                "kms:GenerateDataKey"
            ],
            "Resource": "myKMSKeyARN"
        }
    ]
}
```

IAM-Rollenrichtlinie für ein Amazon-SNS-Thema

Die folgende Beispielrichtlinie gewährt die AWS Config Erlaubnis, auf Ihr SNS-Thema zuzugreifen:

```
{
  "Version": "2012-10-17",
  "Statement":
   [
     {
      "Effect":"Allow",
      "Action":"sns:Publish",
      "Resource":"mySNStopicARN"
     }
    ]
}
```

Wenn Ihr SNS-Thema verschlüsselt ist, finden Sie zusätzliche Anweisungen zur Einrichtung im Thema Konfigurieren von AWS KMS -Berechtigungen im Entwicklerhandbuch für Amazon Simple Notification Service.

IAM-Rollenrichtlinie für den Abruf von Konfigurationsdetails

Es wird empfohlen, die AWS Config dienstverknüpfte Rolle zu verwenden:. `AWSServiceRoleForConfig` Dienstbezogene Rollen sind vordefiniert und enthalten alle

Berechtigungen, die zum Aufrufen anderer Rollen AWS Config erforderlich sind. AWS-Services Die AWS Config dienstverknüpfte Rolle ist für dienstverknüpfte Konfigurationsrekorder erforderlich. Weitere Informationen finden Sie unter Verwenden von Service-verknüpften Rollen für AWS Config.

Wenn Sie eine Rolle mit der Konsole erstellen oder aktualisieren, AWS Config hängt die für Sie an. AWSServiceRoleForConfig

Wenn Sie den verwenden AWS CLI, verwenden Sie den `attach-role-policy` Befehl und geben Sie den Amazon-Ressourcennamen (ARN) an für AWSServiceRoleForConfig:

```
$ aws iam attach-role-policy --role-name myConfigRole --policy-arn
 arn:aws:iam::aws:policy/aws-service-role/AWSServiceRoleForConfig
```

Verwaltung von Berechtigungen für die S3-Bucket-Aufzeichnung

AWS Config zeichnet Benachrichtigungen auf und sendet Benachrichtigungen, wenn ein S3-Bucket erstellt, aktualisiert oder gelöscht wird.

Es wird empfohlen, die AWS Config serviceverknüpfte Rolle zu verwenden:`AWSServiceRoleForConfig`. Dienstbezogene Rollen sind vordefiniert und enthalten alle Berechtigungen, die zum Aufrufen anderer Rollen AWS Config erforderlich sind. AWS-Services Die AWS Config dienstverknüpfte Rolle ist für dienstverknüpfte Konfigurationsrekorder erforderlich. Weitere Informationen finden Sie unter Verwenden von Service-verknüpften Rollen für AWS Config.

Aktualisierung der IAM-Rolle für den vom Kunden verwalteten Konfigurationsrekorder

Sie können die vom Kunden verwaltete Konfigurationsrekorder verwendete IAM-Rolle aktualisieren. Bevor Sie die IAM-Rolle; aktualisieren, stellen Sie sicher, dass Sie eine neue Rolle erstellt haben, um die alte zu ersetzen. Sie müssen der neuen Rolle Richtlinien hinzufügen, die Berechtigungen AWS Config zum Aufzeichnen von Konfigurationen und deren Bereitstellung an Ihren Bereitstellungskanal gewähren.

Weitere Informationen zum Erstellen einer IAM-Rolle und zum Anfügen der erforderlichen Richtlinien an die IAM-Rolle finden Sie unter Schritt 3: Eine IAM-Rolle erstellen.

> **Note**
>
> Den ARN einer vorhandenen IAM-Rolle finden Sie in der IAM-Konsole unter. https://console.aws.amazon.com/iam/ Wählen Sie im Navigationsbereich Roles (Rollen) aus.

Wählen Sie dann den Namen der gewünschten Rolle aus und suchen Sie den ARN oben auf der Seite Summary (Übersicht).

Aktualisieren der IAM-Rolle

Sie können Ihre IAM-Rolle mit dem oder dem AWS Management Console aktualisieren. AWS CLI

To update the IAM role (Console)

1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die AWS Config Konsole zu https://console.aws.amazon.com/config/Hause.
2. Wählen Sie im Navigationsbereich Settings (Einstellungen) aus.
3. Wählen Sie auf der Registerkarte Vom Kunden verwalteter Rekorder auf der Seite Einstellungen die Option Bearbeiten aus.
4. Wählen Sie im Abschnitt Data Governance die IAM-Rolle für AWS Config:
   - Verwenden Sie eine vorhandene AWS Config serviceverknüpfte Rolle — AWS Config erstellt eine Rolle, die über die erforderlichen Berechtigungen verfügt.
   - Wählen Sie eine Rolle aus Ihrem Konto — Wählen Sie für bestehende Rollen eine IAM-Rolle in Ihrem Konto aus.
5. Wählen Sie Speichern.

To update the IAM role (AWS CLI)

Verwenden Sie den `put-configuration-recorder`-Befehl und geben Sie den Amazon-Ressourcennamen (ARN) der neuen Rolle an:

```
$ aws configservice put-configuration-recorder --configuration-recorder
 name=configRecorderName,roleARN=arn:aws:iam::012345678912:role/myConfigRole
```

Berechtigungen für den Amazon S3 S3-Bucket für den AWS Config Lieferkanal

> **Important**
>
> Auf dieser Seite geht es darum, den Amazon S3 S3-Bucket für den AWS Config Lieferkanal einzurichten. Auf dieser Seite geht es nicht um den `AWS::S3::Bucket` Ressourcentyp, den der AWS Config Konfigurationsrekorder aufzeichnen kann.

Amazon S3 S3-Buckets und -Objekte sind standardmäßig privat. Nur derjenige AWS-Konto , der den Bucket erstellt hat (der Eigentümer der Ressource), hat Zugriffsberechtigungen. Ressourcenbesitzer können anderen Ressourcen und Benutzern Zugriff gewähren, indem sie Zugriffsrichtlinien erstellen.

Wenn AWS Config automatisch ein S3-Bucket für Sie erstellt wird, werden die erforderlichen Berechtigungen hinzugefügt. Wenn Sie jedoch einen vorhandenen S3-Bucket angeben, müssen Sie diese Berechtigungen manuell hinzufügen.

Themen

- Erforderliche Berechtigungen für den Amazon-S3-Bucket bei Verwendung von IAM-Rollen
- Erforderliche Berechtigungen für den Amazon-S3-Bucket bei Verwendung von servicegebundenen Rollen
- AWS Config Zugriff auf den Amazon S3 S3-Bucket gewähren
- Erforderliche Berechtigungen für den Amazon S3 S3-Bucket bei kontoübergreifender Lieferung

Erforderliche Berechtigungen für den Amazon-S3-Bucket bei Verwendung von IAM-Rollen

AWS Config verwendet die IAM-Rolle, die Sie dem Konfigurationsrekorder zugewiesen haben, um den Konfigurationsverlauf und Snapshots für S3-Buckets in Ihrem Konto bereitzustellen. Für die kontoübergreifende Bereitstellung wird AWS Config zunächst versucht, die zugewiesene IAM-Rolle zu verwenden. Wenn die Bucket-Richtlinie keinen `WRITE` Zugriff auf die IAM-Rolle gewährt, wird der AWS Config Dienstprinzipal verwendet. `config.amazonaws.com` Die Bucket-Richtlinie muss `WRITE` Zugriff gewähren, `config.amazonaws.com` um die Lieferung abzuschließen. Nach erfolgreicher Lieferung AWS Config behält es das Eigentum an allen Objekten, die es an den kontoübergreifenden S3-Bucket übermittelt.

AWS Config ruft die Amazon S3 HeadBucketS3-API mit der IAM-Rolle auf, die Sie dem Konfigurationsrekorder zugewiesen haben, um zu bestätigen, ob der S3-Bucket existiert und wo er sich befindet. Wenn Sie nicht über die erforderlichen Berechtigungen AWS Config zur Bestätigung verfügen, wird in Ihren AWS CloudTrail Protokollen ein `AccessDenied` Fehler angezeigt. AWS Config Kann jedoch weiterhin den Konfigurationsverlauf und Snapshots bereitstellen, auch wenn AWS Config es nicht über die erforderlichen Berechtigungen verfügt, um zu überprüfen, ob der S3-Bucket vorhanden ist und wo er sich befindet.

> **Mindestberechtigungen**
>
> Die Amazon S3 `HeadBucket` S3-API erfordert die `s3:ListBucket` Aktion.

Erforderliche Berechtigungen für den Amazon-S3-Bucket bei Verwendung von servicegebundenen Rollen

Die AWS Config serviceverknüpfte Rolle ist nicht berechtigt, Objekte in Amazon S3 S3-Buckets abzulegen. Wenn Sie eine serviceverknüpfte Rolle einrichten AWS Config , AWS Config wird der `config.amazonaws.com` Service Principal zur Bereitstellung des Konfigurationsverlaufs und der Snapshots verwendet. Die S3-Bucket-Richtlinie in Ihrem Konto oder in kontoübergreifenden Zielen muss Berechtigungen für den AWS Config Dienstprinzipal zum Schreiben von Objekten enthalten.

AWS Config Zugriff auf den Amazon S3 S3-Bucket gewähren

Führen Sie die folgenden Schritte aus AWS Config , um den Konfigurationsverlauf und die Snapshots an einen Amazon S3 S3-Bucket zu senden.

1. Melden Sie sich AWS Management Console mit dem Konto an, das über den S3-Bucket verfügt.
2. Öffnen Sie die Amazon S3 S3-Konsole unter https://console.aws.amazon.com/s3/.
3. Wählen Sie den Bucket aus, den Sie AWS Config für die Lieferung von Konfigurationselementen verwenden möchten, und wählen Sie dann Eigenschaften.
4. Wählen Sie Permissions (Berechtigungen).
5. Wählen Sie Edit Bucket Policy.
6. Kopieren Sie die folgende Richtlinie in das Fenster Bucket Policy Editor (Richtlinien-Editor für Buckets):

> **Bewährte Methoden für die Gewährleistung der Sicherheit**
>
> Es wird dringend empfohlen, den Zugriff in der Bucket-Richtlinie mit der folgenden `AWS:SourceAccount` Bedingung einzuschränken. Dadurch AWS Config wird sichergestellt, dass der Zugriff nur für die erwarteten Benutzer gewährt wird.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AWSConfigBucketPermissionsCheck",
      "Effect": "Allow",
      "Principal": {
        "Service": "config.amazonaws.com"
      },
      "Action": "s3:GetBucketAcl",
      "Resource": "arn:aws:s3:::amzn-s3-demo-bucket",
      "Condition": {
        "StringEquals": {
          "AWS:SourceAccount": "sourceAccountID"
        }
      }
    },
    {
      "Sid": "AWSConfigBucketExistenceCheck",
      "Effect": "Allow",
      "Principal": {
        "Service": "config.amazonaws.com"
      },
      "Action": "s3:ListBucket",
      "Resource": "arn:aws:s3:::amzn-s3-demo-bucket",
      "Condition": {
        "StringEquals": {
          "AWS:SourceAccount": "sourceAccountID"
        }
      }
    },
    {
      "Sid": "AWSConfigBucketDelivery",
      "Effect": "Allow",
```

```
      "Principal": {
        "Service": "config.amazonaws.com"
      },
      "Action": "s3:PutObject",
      "Resource": "arn:aws:s3:::amzn-s3-demo-bucket/[optional] prefix/
AWSLogs/sourceAccountID/Config/*",
      "Condition": {
        "StringEquals": {
          "s3:x-amz-acl": "bucket-owner-full-control",
          "AWS:SourceAccount": "sourceAccountID"
        }
      }
    }
  ]
}
```

7. Ersetzen Sie die folgenden Werte in der Bucket-Richtlinie:
   - *amzn-s3-demo-bucket*— Name des Amazon S3 S3-Buckets, der AWS Config den Konfigurationsverlauf und die Snapshots bereitstellt.
   - *[optional] prefix*— Eine optionale Ergänzung zum Amazon S3 S3-Objektschlüssel, mit deren Hilfe eine ordnerähnliche Organisation im Bucket erstellt werden kann.
   - *sourceAccountID*— ID des Kontos, über das der Konfigurationsverlauf und die Snapshots bereitgestellt AWS Config werden.
8. Wählen Sie Save (Speichern) und dann Close (Schließen) aus.

Die `AWS:SourceAccount` Bedingung schränkt die AWS Config Operationen auf die angegebenen Werte ein. AWS-Konten Verwenden Sie für Konfigurationen mit mehreren Konten innerhalb einer Organisation, die an einen einzelnen S3-Bucket liefert, IAM-Rollen mit AWS Organizations Bedingungsschlüsseln anstelle von serviceverknüpften Rollen. Beispiel, `AWS:PrincipalOrgID`. Weitere Informationen finden Sie im Benutzerhandbuch unter Verwaltung von Zugriffsberechtigungen für eine Organisation.AWS Organizations

Die `AWS:SourceArn` Bedingung schränkt den AWS Config Betrieb auf bestimmte Lieferkanäle ein. Das `AWS:SourceArn` Format ist wie folgt:`arn:aws:config:`*`sourceRegion`*`:`*`123456789012`*.

Um beispielsweise den S3-Bucket-Zugriff auf einen Lieferkanal in der Region USA Ost (Nord-Virginia) für das Konto 123456789012 einzuschränken, fügen Sie die folgende Bedingung hinzu:

```
"ArnLike": {"AWS:SourceArn": "arn:aws:config:us-east-1:123456789012:"}
```

Erforderliche Berechtigungen für den Amazon S3 S3-Bucket bei kontoübergreifender Lieferung

Wenn konfiguriert AWS Config ist, dass der Konfigurationsverlauf und Snapshots an einen Amazon S3 S3-Bucket in einem anderen Konto gesendet werden (kontoübergreifende Einrichtung), wobei sich der Konfigurationsrekorder und der für den Lieferkanal angegebene S3-Bucket unterscheiden AWS-Konten, sind die folgenden Berechtigungen erforderlich:

- Die IAM-Rolle, die Sie dem Konfigurationsrekorder zuweisen, benötigt eine ausdrückliche Genehmigung, um den Vorgang auszuführen. `s3:ListBucket` Dies liegt daran, dass AWS Config die Amazon S3 HeadBucketS3-API mit dieser IAM-Rolle aufgerufen wird, um den Bucket-Standort zu ermitteln.
- Die S3-Bucket-Richtlinie muss Berechtigungen sowohl für den AWS Config Service Principal als auch für die dem Konfigurationsrekorder zugewiesene IAM-Rolle enthalten.

Im Folgenden finden Sie ein Beispiel für eine Bucket-Policy-Konfiguration:

```
{
      "Sid": "AWSConfigBucketExistenceCheck",
      "Effect": "Allow",
      "Principal": {
        "Service": "config.amazonaws.com",
        "AWS": "IAM Role-Arn assigned to the configuration recorder"
      },
      "Action": "s3:ListBucket",
      "Resource": "arn:aws:s3:::amzn-s3-demo-bucket",
      "Condition": {
        "StringEquals": {
          "AWS:SourceAccount": "sourceAccountID"
        }
      }
}
```

Berechtigungen für den KMS-Schlüssel für den AWS Config Delivery Channel

Verwenden Sie die Informationen in diesem Thema, wenn Sie eine Richtlinie für einen AWS KMS Schlüssel für Ihren S3-Bucket erstellen möchten, mit der Sie KMS-basierte Verschlüsselung für Objekte verwenden können, die von AWS Config für die S3-Bucket-Zustellung bereitgestellt wurden.

Inhalt

- Erforderliche Berechtigungen für den KMS-Schlüssel bei Verwendung von IAM-Rollen (S3-Bucket-Übermittlung)
- Erforderliche Berechtigungen für den AWS KMS Schlüssel bei der Verwendung von serviceverknüpften Rollen (S3 Bucket Delivery)
- AWS Config Zugriff auf den AWS KMS Schlüssel gewähren

Erforderliche Berechtigungen für den KMS-Schlüssel bei Verwendung von IAM-Rollen (S3-Bucket-Übermittlung)

Wenn Sie die Einrichtung AWS Config mithilfe einer IAM-Rolle einrichten, können Sie die folgende Berechtigungsrichtlinie an den KMS-Schlüssel anhängen:

```
{
    "Id": "Policy_ID",
    "Statement": [
        {
            "Sid": "AWSConfigKMSPolicy",
            "Action": [
                "kms:Decrypt",
                "kms:GenerateDataKey"
            ],
            "Effect": "Allow",
            "Resource": "*myKMSKeyARN*",
            "Principal": {
                "AWS": [
                    "account-id1",
                    "account-id2",
                    "account-id3"
                ]
            }
```

```
        }
    ]
}
```

> **Note**
>
> Wenn die IAM-Rolle, die Amazon S3 S3-Bucket-Richtlinie oder der AWS KMS Schlüssel keinen angemessenen Zugriff auf ermöglichen AWS Config, schlägt AWS Config der Versuch fehl, Konfigurationsinformationen an den Amazon S3 S3-Bucket zu senden. In diesem Fall AWS Config sendet er die Informationen erneut, diesmal als AWS Config Service Principal. In diesem Fall müssen Sie dem Schlüssel eine unten aufgeführte Berechtigungsrichtlinie beifügen, um AWS Config Zugriff auf die Verwendung des AWS KMS Schlüssels bei der Übermittlung von Informationen an den Amazon S3 S3-Bucket zu gewähren.

Erforderliche Berechtigungen für den AWS KMS Schlüssel bei der Verwendung von serviceverknüpften Rollen (S3 Bucket Delivery)

Die AWS Config serviceverknüpfte Rolle ist nicht berechtigt, auf den AWS KMS Schlüssel zuzugreifen. Wenn Sie also eine dienstbezogene AWS Config Rolle einrichten, AWS Config werden Informationen stattdessen als AWS Config Dienstprinzipal gesendet. Sie müssen dem Schlüssel eine unten aufgeführte Zugriffsrichtlinie beifügen, um Zugriff AWS Config auf die Verwendung des AWS KMS Schlüssels bei der AWS KMS Übermittlung von Informationen an den Amazon S3 S3-Bucket zu gewähren.

AWS Config Zugriff auf den AWS KMS Schlüssel gewähren

Diese Richtlinie ermöglicht AWS Config die Verwendung eines AWS KMS Schlüssels bei der Übermittlung von Informationen an einen Amazon S3 S3-Bucket

```
{
    "Id": "Policy_ID",
    "Statement": [
        {
            "Sid": "AWSConfigKMSPolicy",
            "Effect": "Allow",
            "Principal": {
                "Service": "config.amazonaws.com"
            },
```

```
            "Action": [
                "kms:Decrypt",
                "kms:GenerateDataKey"
            ],
            "Resource": "myKMSKeyARN",
            "Condition": {
                "StringEquals": {
                    "AWS:SourceAccount": "sourceAccountID"
                }
            }
        }
    ]
}
```

Ersetzen Sie die folgenden Werte in der Schlüsselrichtlinie:

- *myKMSKeyARN*— Der ARN des AWS KMS Schlüssels, der zur Verschlüsselung von Daten im Amazon S3 S3-Bucket verwendet AWS Config wird, an den Konfigurationselemente geliefert werden.
- *sourceAccountID*— Die ID des Kontos, für das Konfigurationselemente geliefert AWS Config werden.

Sie können die `AWS:SourceAccount` Bedingung in der obigen AWS KMS Schlüsselrichtlinie verwenden, um den Config-Dienstprinzipal so zu beschränken, dass er nur mit dem AWS KMS Schlüssel interagiert, wenn er Operationen für bestimmte Konten ausführt.

AWS Config unterstützt auch die `AWS:SourceArn` Bedingung, dass der Config-Serviceprinzipal nur dann mit dem Amazon S3 S3-Bucket interagiert, wenn er Operationen im Namen bestimmter AWS Config Lieferkanäle ausführt. Wenn Sie den AWS Config Service Principal verwenden, wird als `AWS:SourceArn` Eigenschaft immer festgelegt, `arn:aws:config:sourceRegion:sourceAccountID:*` wo sich die Region des Lieferkanals `sourceRegion` befindet. Dabei `sourceAccountID` handelt es sich um die ID des Kontos, das den Lieferkanal enthält. Weitere Informationen zu AWS Config Lieferkanälen finden Sie unter Verwaltung des Lieferkanals. Fügen Sie beispielsweise die folgende Bedingung hinzu, um den Config-Service-Prinzipal so zu beschränken, dass er nur im Namen eines Übermittlungskanals in der Region `us-east-1` des Kontos `123456789012` mit Ihrem Amazon-S3-Bucket interagiert: `"ArnLike": {"AWS:SourceArn": "arn:aws:config:us-east-1:123456789012:*"}`.

Berechtigungen für das Amazon-SNS-Thema

In diesem Thema wird beschrieben, wie Sie die Bereitstellung von Amazon SNS SNS-Themen konfigurieren AWS Config , die einem anderen Konto gehören. AWS Config muss über die erforderlichen Berechtigungen verfügen, um Benachrichtigungen an ein Amazon SNS SNS-Thema zu senden.

Wenn die AWS Config Konsole ein neues Amazon SNS SNS-Thema für Sie erstellt, AWS Config gewährt sie die erforderlichen Berechtigungen. Wenn Sie ein vorhandenes Amazon SNS SNS-Thema wählen, stellen Sie sicher, dass das Amazon SNS SNS-Thema die erforderlichen Berechtigungen enthält und den bewährten Sicherheitsmethoden entspricht.

> **Regionsübergreifende Amazon SNS SNS-Themen werden nicht unterstützt**
>
> AWS Config unterstützt derzeit nur den Zugriff innerhalb desselben Kontos AWS-Region und kontenübergreifend.

Inhalt

- Erforderliche Berechtigungen für das Amazon-SNS-Thema bei Verwendung von IAM-Rollen
- Erforderliche Berechtigungen für das Amazon-SNS-Thema bei Verwendung von servicegebundenen Rollen
- AWS Config Zugriff auf das Amazon SNS SNS-Thema gewähren
- Fehlerbehebung für das Amazon-SNS-Thema

Erforderliche Berechtigungen für das Amazon-SNS-Thema bei Verwendung von IAM-Rollen

Sie können eine Berechtigungsrichtlinie an das Amazon-SNS-Thema anfügen, das sich im Besitz eines anderen Kontos befindet. Falls Sie ein Amazon-SNS-Thema eines anderen Kontos verwenden möchten, achten Sie darauf, die folgende Richtlinie an das vorhandenes Amazon-SNS-Thema anzufügen.

```
{
  "Id": "Policy_ID",
  "Statement": [
    {
```

```
      "Sid": "AWSConfigSNSPolicy",
      "Action": [
        "sns:Publish"
      ],
      "Effect": "Allow",
      "Resource": "arn:aws:sns:region:account-id:myTopic",
      "Principal": {
        "AWS": [
          "account-id1",
          "account-id2",
          "account-id3"
        ]
      }
    }
  ]
}
```

Für den `Resource` Schlüssel *`account-id`* steht die AWS Kontonummer des Thema-Inhabers. Verwenden Sie für *`account-id1account-id2`*, und den *`account-id3`* AWS-Konten , der Daten an ein Amazon SNS SNS-Thema sendet. Sie können *`region`* und *`myTopic`* durch entsprechende Werte ersetzen.

Wenn eine Benachrichtigung AWS Config an ein Amazon SNS SNS-Thema gesendet wird, wird zunächst versucht, die IAM-Rolle zu verwenden. Dieser Versuch schlägt jedoch fehl, wenn die Rolle AWS-Konto nicht berechtigt ist, für das Thema zu veröffentlichen. In diesem Fall AWS Config sendet die Benachrichtigung erneut, diesmal als AWS Config Service Principal Name (SPN). Bevor die Veröffentlichung erfolgreich durchgeführt werden kann, muss die Zugriffsrichtlinie für das Thema `sns:Publish`-Zugriff auf den Prinzipal-Namen von `config.amazonaws.com` erteilen. Sie müssen dem Amazon-SNS-Thema Zugriffsrichtlinie anfügen (siehe nächster Abschnitt), um AWS Config Zugriff auf das Amazon-SNS-Thema zu gewähren, falls die IAM-Rolle nicht berechtigt ist, an das Thema zu veröffentlichen.

Erforderliche Berechtigungen für das Amazon-SNS-Thema bei Verwendung von servicegebundenen Rollen

Die AWS Config serviceverknüpfte Rolle ist nicht berechtigt, auf das Amazon SNS SNS-Thema zuzugreifen. Wenn Sie also eine Service-Linked AWS Config Role (SLR) einrichten, AWS Config werden Informationen stattdessen als Service Principal gesendet. AWS Config Sie müssen dem Amazon SNS SNS-Thema eine unten aufgeführte Zugriffsrichtlinie beifügen, um AWS Config Zugriff auf das Senden von Informationen zum Amazon SNS SNS-Thema zu gewähren.

Bei der Einrichtung im selben Konto müssen Sie den Service-Prinzipal-Namen von AWS Config nicht verwenden, wenn sich das Amazon-SNS-Thema und die SLR im selben Konto befinden und die Amazon-SNS-Richtlinie der SLR die Berechtigung `sns:Publish` erteilt. Die nachfolgende Berechtigungsrichtlinie und die Empfehlungen zu bewährten Methoden für optimale Sicherheit beziehen sich auf die kontoübergreifende Einrichtung.

AWS Config Zugriff auf das Amazon SNS SNS-Thema gewähren

Diese Richtlinie ermöglicht AWS Config das Senden einer Benachrichtigung an ein Amazon SNS SNS-Thema. Um von einem anderen Konto aus AWS Config Zugriff auf das Amazon SNS SNS-Thema zu gewähren, müssen Sie die folgende Berechtigungsrichtlinie beifügen.

> **Note**
>
> Aus Sicherheitsgründen wird dringend empfohlen, sicherzustellen, dass der Zugriff auf Ressourcen nur im Namen der erwarteten Benutzer AWS Config erfolgt, indem der Zugriff auf die Konten beschränkt wird, die unter Bedingung aufgeführt sind. `AWS:SourceAccount`

```
{
"Id": "Policy_ID",
"Statement": [
  {
    "Sid": "AWSConfigSNSPolicy",
    "Effect": "Allow",
    "Principal": {
      "Service": "config.amazonaws.com"
    },
    "Action": "sns:Publish",
      "Resource": "arn:aws:sns:region:account-id:myTopic",
        "Condition" : {
        "StringEquals": {
          "AWS:SourceAccount": [
            "account-id1",
            "account-id2",
            "account-id3"
          ]
        }
      }
    }
  ]
```

```
}
```

Für den `Resource` Schlüssel *`account-id`* gilt die AWS Kontonummer des Themenbesitzers. Verwenden Sie für *`account-id1account-id2`*, und den *`account-id3`* AWS-Konten , der Daten an ein Amazon SNS SNS-Thema sendet. Sie können *`region`* und *`myTopic`* durch entsprechende Werte ersetzen.

Sie können die `AWS:SourceAccount` Bedingung in der vorherigen Amazon SNS SNS-Themenrichtlinie verwenden, um den AWS Config Service Principal Name (SPN) so zu beschränken, dass er nur mit dem Amazon SNS SNS-Thema interagiert, wenn Operationen für bestimmte Konten ausgeführt werden.

AWS Config unterstützt auch die `AWS:SourceArn` Bedingung, dass der AWS Config Service Principal Name (SPN) nur mit dem S3-Bucket interagiert, wenn Operationen im Namen bestimmter Lieferkanäle ausgeführt werden. AWS Config Wenn Sie den AWS Config Service Principal Name (SPN) verwenden, wird als `AWS:SourceArn` Eigenschaft immer festgelegt, `arn:aws:config:sourceRegion:sourceAccountID:*` wo sich die Region des Bereitstellungskanals `sourceRegion` befindet. Dabei `sourceAccountID` handelt es sich um die ID des Kontos, das den Bereitstellungskanal enthält. Weitere Informationen zu AWS Config Bereitstellungskanälen finden Sie unter Verwaltung des Bereitstellungskanals. Fügen Sie beispielsweise die folgende Bedingung hinzu, um den AWS Config Service Principal Name (SPN) so zu beschränken, dass er mit Ihrem S3-Bucket nur im Namen eines Lieferkanals in der `us-east-1` Region des Kontos interagiert`123456789012`:`"ArnLike": {"AWS:SourceArn": "arn:aws:config:us-east-1:123456789012:*"}`.

Fehlerbehebung für das Amazon-SNS-Thema

AWS Config muss berechtigt sein, Benachrichtigungen an ein Amazon SNS SNS-Thema zu senden. Wenn ein Amazon SNS SNS-Thema keine Benachrichtigungen erhalten kann, überprüfen Sie, ob die IAM-Rolle, die AWS Config Sie übernommen haben, über die erforderlichen `sns:Publish` Berechtigungen verfügt.

Fehlerbehebung bei AWS Config Identität und Zugriff

Verwenden Sie die folgenden Informationen, um häufig auftretende Probleme zu diagnostizieren und zu beheben, die bei der Arbeit mit AWS Config und IAM auftreten können.

Themen

- Ich bin nicht berechtigt, eine Aktion durchzuführen in AWS Config

- Ich bin nicht berechtigt, iam auszuführen: PassRole
- Ich möchte Personen außerhalb von mir den Zugriff AWS-Konto auf meine AWS Config Ressourcen ermöglichen

Ich bin nicht berechtigt, eine Aktion durchzuführen in AWS Config

Wenn Sie eine Fehlermeldung erhalten, dass Sie nicht zur Durchführung einer Aktion berechtigt sind, müssen Ihre Richtlinien aktualisiert werden, damit Sie die Aktion durchführen können.

Der folgende Beispielfehler tritt auf, wenn der `mateojackson` IAM-Benutzer versucht, die Konsole zum Anzeigen von Details zu einer fiktiven *`my-example-widget`*-Ressource zu verwenden, jedoch nicht über `config:`*`GetWidget`*-Berechtigungen verfügt.

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
 config:GetWidget on resource: my-example-widget
```

In diesem Fall muss die Mateo-Richtlinie aktualisiert werden, damit er mit der `config:`*`GetWidget`*-Aktion auf die *`my-example-widget`*-Ressource zugreifen kann.

Wenn Sie Hilfe benötigen, wenden Sie sich an Ihren AWS Administrator. Ihr Administrator hat Ihnen Ihre Anmeldeinformationen zur Verfügung gestellt.

Ich bin nicht berechtigt, iam auszuführen: PassRole

Wenn Sie die Fehlermeldung erhalten, dass Sie nicht zum Durchführen der `iam:PassRole`-Aktion autorisiert sind, müssen Ihre Richtlinien aktualisiert werden, um eine Rolle an AWS Configübergeben zu können.

Einige AWS-Services ermöglichen es Ihnen, eine bestehende Rolle an diesen Dienst zu übergeben, anstatt eine neue Servicerolle oder eine dienstverknüpfte Rolle zu erstellen. Hierzu benötigen Sie Berechtigungen für die Übergabe der Rolle an den Dienst.

Der folgende Beispielfehler tritt auf, wenn ein IAM-Benutzer mit dem Namen `marymajor` versucht, die Konsole zu verwenden, um eine Aktion in AWS Config auszuführen. Die Aktion erfordert jedoch, dass der Service über Berechtigungen verfügt, die durch eine Servicerolle gewährt werden. Mary besitzt keine Berechtigungen für die Übergabe der Rolle an den Dienst.

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform:
 iam:PassRole
```

In diesem Fall müssen die Richtlinien von Mary aktualisiert werden, um die Aktion `iam:PassRole` ausführen zu können.

Wenn Sie Hilfe benötigen, wenden Sie sich an Ihren AWS Administrator. Ihr Administrator hat Ihnen Ihre Anmeldeinformationen zur Verfügung gestellt.

Ich möchte Personen außerhalb von mir den Zugriff AWS-Konto auf meine AWS Config Ressourcen ermöglichen

Sie können eine Rolle erstellen, die Benutzer in anderen Konten oder Personen außerhalb Ihrer Organisation für den Zugriff auf Ihre Ressourcen verwenden können. Sie können festlegen, wem die Übernahme der Rolle anvertraut wird. Für Dienste, die ressourcenbasierte Richtlinien oder Zugriffskontrolllisten (ACLs) unterstützen, können Sie diese Richtlinien verwenden, um Personen Zugriff auf Ihre Ressourcen zu gewähren.

Weitere Informationen dazu finden Sie hier:

- Informationen darüber, ob diese Funktionen AWS Config unterstützt werden, finden Sie unter. Wie AWS Config funktioniert mit IAM
- Informationen dazu, wie Sie Zugriff auf Ihre Ressourcen gewähren können, AWS-Konten die Ihnen gehören, finden Sie im IAM-Benutzerhandbuch unter Gewähren des Zugriffs auf einen IAM-Benutzer in einem anderen AWS-Konto , den Sie besitzen.
- Informationen dazu, wie Sie Dritten Zugriff auf Ihre Ressourcen gewähren können AWS-Konten, finden Sie AWS-Konten im IAM-Benutzerhandbuch unter Gewähren des Zugriffs für Dritte.
- Informationen dazu, wie Sie über einen Identitätsverbund Zugriff gewähren, finden Sie unter Gewähren von Zugriff für extern authentifizierte Benutzer (Identitätsverbund) im IAM-Benutzerhandbuch.
- Informationen zum Unterschied zwischen der Verwendung von Rollen und ressourcenbasierten Richtlinien für den kontoübergreifenden Zugriff finden Sie unter Kontoübergreifender Ressourcenzugriff in IAM im IAM-Benutzerhandbuch.

Verwenden von serviceverknüpften Rollen für AWS Config

AWS Config verwendet AWS Identity and Access Management (IAM) serviceverknüpfte Rollen. Eine serviceverknüpfte Rolle ist ein einzigartiger Typ von IAM-Rolle, mit der direkt verknüpft ist. AWS Config Mit Diensten verknüpfte Rollen sind vordefiniert AWS Config und enthalten alle Berechtigungen, die der Dienst benötigt, um andere AWS Dienste in Ihrem Namen aufzurufen.

Eine dienstbezogene Rolle AWS Config erleichtert die Einrichtung, da Sie die erforderlichen Berechtigungen nicht manuell hinzufügen müssen. AWS Config definiert die Berechtigungen ihrer dienstbezogenen Rollen und AWS Config kann, sofern nicht anders definiert, nur ihre Rollen übernehmen. Die definierten Berechtigungen umfassen die Vertrauens- und Berechtigungsrichtlinie. Diese Berechtigungsrichtlinie kann keinen anderen IAM-Entitäten zugewiesen werden.

Informationen zu anderen Services, die serviceverknüpften Rollen unterstützen, finden Sie unter AWS -Services, die mit IAM funktionieren. Suchen Sie nach den Services, für die Ja in der Spalte Serviceverknüpfte Rolle angegeben ist. Wählen Sie über einen Link Ja aus, um die Dokumentation zu einer serviceverknüpften Rolle für diesen Service anzuzeigen.

Berechtigungen für serviceverknüpfte Rollen AWS Config

AWS Config verwendet die angegebene dienstverknüpfte Rolle AwsServiceRoleForConfig— AWS Config verwendet diese dienstverknüpfte Rolle, um andere AWS Dienste in Ihrem Namen aufzurufen.

Die serviceverknüpfte Rolle AwsServiceRoleForConfig vertraut dem Service `config.amazonaws.com`, sodass dieser die Rolle annehmen kann.

Die Berechtigungsrichtlinie für die `AwsServiceRoleForConfig` Rolle umfasst nur Lese- und Schreibberechtigungen für Ressourcen und nur Leseberechtigungen für AWS Config Ressourcen in anderen Diensten, die dies unterstützen. AWS Config Die verwaltete Richtlinie für finden Sie unter Verwaltete Richtlinien für AwsServiceRoleForConfig.AWSAWS Config

Sie müssen Berechtigungen konfigurieren, damit eine juristische Stelle von IAM (z. B. Benutzer, Gruppe oder Rolle) eine serviceverknüpfte Rolle erstellen, bearbeiten oder löschen kann. Weitere Informationen finden Sie unter serviceverknüpfte Rollenberechtigungen im IAM-Benutzerhandbuch.

Um eine serviceverknüpfte Rolle mit zu verwenden AWS Config, müssen Sie Berechtigungen für Ihren Amazon S3-Bucket und Ihr Amazon SNS SNS-Thema konfigurieren. Weitere Informationen finden Sie unter Erforderliche Berechtigungen für den Amazon-S3-Bucket bei Verwendung von servicegebundenen Rollen, Erforderliche Berechtigungen für den AWS KMS Schlüssel bei der Verwendung von serviceverknüpften Rollen (S3 Bucket Delivery) und Erforderliche Berechtigungen für das Amazon-SNS-Thema bei Verwendung von servicegebundenen Rollen.

Erstellen einer serviceverknüpften Rolle für AWS Config

Erstellen Sie in der IAM-CLI oder der IAM-API eine serviceverknüpfte Rolle mit dem Servicenamen `config.amazonaws.com`. Weitere Informationen finden Sie unter Erstellen einer serviceverknüpfte

Rolle im IAM-Leitfaden. Wenn Sie diese serviceverknüpfte Rolle löschen, können Sie mit demselben Verfahren die Rolle erneut erstellen.

Bearbeiten einer serviceverknüpften Rolle für AWS Config

AWS Config erlaubt es Ihnen nicht, die AwsServiceRoleForConfigdienstbezogene Rolle zu bearbeiten. Da möglicherweise verschiedene Entitäten auf die Rolle verweisen, kann der Rollenname nach dem Erstellen einer serviceverknüpften Rolle nicht mehr geändert werden. Sie können jedoch die Beschreibung der Rolle mit IAM bearbeiten. Weitere Informationen finden Sie unter Bearbeiten einer serviceverknüpften Rolle im IAM-Benutzerhandbuch.

Löschen einer dienstbezogenen Rolle für AWS Config

Wenn Sie ein Feature oder einen Dienst, die bzw. der eine serviceverknüpften Rolle erfordert, nicht mehr benötigen, sollten Sie diese Rolle löschen. Auf diese Weise haben Sie keine ungenutzte juristische Stelle, die nicht aktiv überwacht oder verwaltet wird. Sie müssen jedoch die Ressourcen für Ihre serviceverknüpften Rolle zunächst bereinigen, bevor Sie sie manuell löschen können.

> **Note**
>
> Wenn der AWS Config Dienst die Rolle verwendet, wenn Sie versuchen, die Ressourcen zu löschen, schlägt das Löschen möglicherweise fehl. Wenn dies passiert, warten Sie einige Minuten und versuchen Sie es erneut.

Um AWS Config Ressourcen zu löschen, die verwendet werden von AwsServiceRoleForConfig

Achten Sie darauf, dass `ConfigurationRecorders` nicht die serviceverknüpfte Rolle verwendet. Sie können die AWS Config Konsole verwenden, um den Konfigurationsrekorder zu beenden. Zum Beenden der Aufzeichnung wählen Sie unter Recording is on (Aufnahme ist an) die Option Turn off (Ausschalten) aus.

Sie können die `ConfigurationRecorder` verwendende AWS Config API löschen. Verwenden Sie zum Löschen den Befehl `delete-configuration-recorder`.

```
$ aws configservice delete-configuration-recorder --configuration-recorder-
name default
```

So löschen Sie die serviceverknüpfte Rolle mit IAM

Sie können die IAM-Konsole, die IAM-CLI oder die IAM-API verwenden, um die AwsServiceRoleForConfig-serviceverknüpfte Rolle zu löschen. Weitere Informationen finden Sie unter Löschen einer serviceverknüpften Rolle im IAM-Leitfaden.

Reaktion auf Vorfälle in AWS Config

Sicherheit hat bei höchste Priorität AWS. AWS Verwaltet im Rahmen des Modells der gemeinsamen Verantwortung in der AWS Cloud eine Rechenzentrums-, Netzwerk- und Softwarearchitektur, die die Anforderungen der sicherheitssensibelsten Unternehmen erfüllt. AWS ist verantwortlich für jegliche Reaktion auf Vorfälle in Bezug auf den AWS Config Service selbst. Außerdem tragen Sie als AWS Kunde gemeinsam die Verantwortung für die Aufrechterhaltung der Sicherheit in der Cloud. Das bedeutet, dass Sie anhand der AWS Tools und Funktionen, auf die Sie Zugriff haben, die Sicherheit kontrollieren, die Sie implementieren möchten, und dass Sie im Rahmen des Modells der gemeinsamen Verantwortung für die Reaktion auf Vorfälle verantwortlich sind.

Indem Sie eine Sicherheitsbasis einrichten, die den Zielen Ihrer in der Cloud ausgeführten Anwendungen entspricht, können Sie Abweichungen erkennen, auf die Sie reagieren können. Da die Reaktion auf Sicherheitsvorfälle ein komplexes Thema sein kann, empfehlen wir Ihnen, die folgenden Ressourcen zu lesen, damit Sie besser verstehen, welche Auswirkungen Incident Response (IR) und Ihre Entscheidungen auf Ihre Unternehmensziele haben: Leitfaden zur Reaktion auf AWS Sicherheitsvorfälle, Whitepaper zu bewährten AWS Sicherheitsmethoden und das Whitepaper Security Perspective of the AWS Cloud Adoption Framework (CAF).

Überprüfung der Einhaltung von Vorschriften für AWS Config

Externe Prüfer bewerten die Sicherheit und Einhaltung von Vorschriften im AWS Config Rahmen mehrerer AWS Compliance-Programme. Hierzu zählen unter anderem SOC, PCI, FedRAMP und HIPAA.

Um zu erfahren, ob AWS-Service ein AWS-Services in den Geltungsbereich bestimmter Compliance-Programme fällt, finden Sie unter Umfang nach Compliance-Programm AWS-Services unter . Wählen Sie dort das Compliance-Programm aus, an dem Sie interessiert sind. Allgemeine Informationen finden Sie unter AWS Compliance-Programme AWS .

Sie können Prüfberichte von Drittanbietern unter herunterladen AWS Artifact. Weitere Informationen finden Sie unter Berichte herunterladen unter .

Ihre Verantwortung für die Einhaltung der Vorschriften bei der Nutzung AWS-Services hängt von der Vertraulichkeit Ihrer Daten, den Compliance-Zielen Ihres Unternehmens und den geltenden Gesetzen und Vorschriften ab. AWS stellt die folgenden Ressourcen zur Verfügung, die Sie bei der Einhaltung der Vorschriften unterstützen:

- Compliance und Governance im Bereich Sicherheit – In diesen Anleitungen für die Lösungsimplementierung werden Überlegungen zur Architektur behandelt. Außerdem werden Schritte für die Bereitstellung von Sicherheits- und Compliance-Features beschrieben.
- Referenz für berechtigte HIPAA-Services – Listet berechtigte HIPAA-Services auf. Nicht alle AWS-Services sind HIPAA-fähig.
- AWS Compliance-Ressourcen — Diese Sammlung von Arbeitsmappen und Leitfäden gilt möglicherweise für Ihre Branche und Ihren Standort.
- AWS Leitfäden zur Einhaltung von Vorschriften für Kunden — Verstehen Sie das Modell der gemeinsamen Verantwortung aus dem Blickwinkel der Einhaltung von Vorschriften. In den Leitfäden werden die bewährten Verfahren zur Sicherung zusammengefasst AWS-Services und die Leitlinien den Sicherheitskontrollen in verschiedenen Frameworks (einschließlich des National Institute of Standards and Technology (NIST), des Payment Card Industry Security Standards Council (PCI) und der International Organization for Standardization (ISO)) zugeordnet.
- Evaluierung von Ressourcen anhand von Regeln im AWS Config Entwicklerhandbuch — Der AWS Config Service bewertet, wie gut Ihre Ressourcenkonfigurationen den internen Praktiken, Branchenrichtlinien und Vorschriften entsprechen.
- AWS Security Hub— Auf diese AWS-Service Weise erhalten Sie einen umfassenden Überblick über Ihren internen Sicherheitsstatus. AWS Security Hub verwendet Sicherheitskontrollen, um Ihre AWS -Ressourcen zu bewerten und Ihre Einhaltung von Sicherheitsstandards und bewährten Methoden zu überprüfen. Die Liste der unterstützten Services und Kontrollen finden Sie in der Security-Hub-Steuerelementreferenz.
- Amazon GuardDuty — Dies AWS-Service erkennt potenzielle Bedrohungen für Ihre Workloads AWS-Konten, Container und Daten, indem es Ihre Umgebung auf verdächtige und böswillige Aktivitäten überwacht. GuardDuty kann Ihnen helfen, verschiedene Compliance-Anforderungen wie PCI DSS zu erfüllen, indem es die in bestimmten Compliance-Frameworks vorgeschriebenen Anforderungen zur Erkennung von Eindringlingen erfüllt.
- AWS Audit Manager— Auf diese AWS-Service Weise können Sie Ihre AWS Nutzung kontinuierlich überprüfen, um das Risikomanagement und die Einhaltung von Vorschriften und Industriestandards zu vereinfachen.

Resilienz in AWS Config

Die AWS globale Infrastruktur basiert auf AWS Regionen und Availability Zones. AWS Regionen bieten mehrere physisch getrennte und isolierte Availability Zones, die über Netzwerke mit niedriger Latenz, hohem Durchsatz und hoher Redundanz miteinander verbunden sind. Mithilfe von Availability Zones können Sie Anwendungen und Datenbanken erstellen und ausführen, die automatisch Failover zwischen Zonen ausführen, ohne dass es zu Unterbrechungen kommt. Availability Zones sind besser verfügbar, fehlertoleranter und skalierbarer als herkömmliche Infrastrukturen mit einem oder mehreren Rechenzentren.

Weitere Informationen zu AWS Regionen und Availability Zones finden Sie unter AWS Globale Infrastruktur.

Sicherheit der Infrastruktur in AWS Config

Als verwalteter Dienst AWS Config ist er durch AWS globale Netzwerksicherheit geschützt. Informationen zu AWS Sicherheitsdiensten und zum AWS Schutz der Infrastruktur finden Sie unter AWS Cloud-Sicherheit. Informationen zum Entwerfen Ihrer AWS Umgebung unter Verwendung der bewährten Methoden für die Infrastruktursicherheit finden Sie unter Infrastructure Protection in Security Pillar AWS Well-Architected Framework.

Sie verwenden AWS veröffentlichte API-Aufrufe für den Zugriff AWS Config über das Netzwerk. Kunden müssen Folgendes unterstützen:

- Transport Layer Security (TLS). Wir benötigen TLS 1.2 und empfehlen TLS 1.3.
- Verschlüsselungs-Suiten mit Perfect Forward Secrecy (PFS) wie DHE (Ephemeral Diffie-Hellman) oder ECDHE (Elliptic Curve Ephemeral Diffie-Hellman). Die meisten modernen Systeme wie Java 7 und höher unterstützen diese Modi.

Außerdem müssen Anforderungen mit einer Zugriffsschlüssel-ID und einem geheimen Zugriffsschlüssel signiert sein, der einem IAM-Prinzipal zugeordnet ist. Alternativ können Sie mit AWS Security Token Service (AWS STS) temporäre Sicherheitsanmeldeinformationen erstellen, um die Anforderungen zu signieren.

Konfigurations- und Schwachstellenanalyse

For AWS Config AWS erledigt grundlegende Sicherheitsaufgaben wie das Patchen von Gastbetriebssystemen (OS) und Datenbanken, die Firewallkonfiguration und die Notfallwiederherstellung.

Serviceübergreifende Confused-Deputy-Prävention

Das Problem des verwirrten Stellvertreters ist ein Sicherheitsproblem, bei dem eine Entität, die keine Berechtigung zur Durchführung einer Aktion hat, eine privilegiertere Entität zur Durchführung der Aktion zwingen kann. Dienstübergreifendes Identitätswechsels kann zu einem Problem mit verwirrtem Stellvertreter führen. AWS Ein dienstübergreifender Identitätswechsel kann auftreten, wenn ein Dienst (der Anruf-Dienst) einen anderen Dienst anruft (den aufgerufenen Dienst). Der aufrufende Service kann manipuliert werden, um seine Berechtigungen zu verwenden, um Aktionen auf die Ressourcen eines anderen Kunden auszuführen, für die er sonst keine Zugriffsberechtigung haben sollte. Um dies zu verhindern, bietet AWS Tools, mit denen Sie Ihre Daten für alle Services mit Serviceprinzipalen schützen können, die Zugriff auf Ressourcen in Ihrem Konto erhalten haben.

Wir empfehlen, die Kontextschlüssel `aws:SourceArn`und die `aws:SourceAccount`globalen Bedingungsschlüssel in Ressourcenrichtlinien zu verwenden, um die Berechtigungen einzuschränken, die der AWS Config Ressource einen anderen Dienst gewähren. Verwenden Sie `aws:SourceArn`, wenn Sie nur eine Ressource mit dem betriebsübergreifenden Zugriff verknüpfen möchten. Verwenden Sie `aws:SourceAccount`, wenn Sie zulassen möchten, dass Ressourcen in diesem Konto mit der betriebsübergreifenden Verwendung verknüpft werden.

Der effektivste Weg, um sich vor dem Confused-Deputy-Problem zu schützen, ist die Verwendung des globalen Bedingungskontext-Schlüssels `aws:SourceArn` mit dem vollständigen ARN der Ressource. Wenn Sie den vollständigen ARN der Ressource nicht kennen oder wenn Sie mehrere Ressourcen angeben, verwenden Sie den globalen Kontextbedingungsschlüssel `aws:SourceArn` mit Platzhalterzeichen (`*`) für die unbekannten Teile des ARN. Beispiel, `arn:aws:`*`servicename`*`:*:`*`123456789012`*`:*`.

Wenn der `aws:SourceArn`-Wert die Konto-ID nicht enthält, z. B. einen Amazon-S3-Bucket-ARN, müssen Sie beide globale Bedingungskontextschlüssel verwenden, um Berechtigungen einzuschränken.

Das folgende Beispiel zeigt, wie Sie die Kontextschlüssel `aws:SourceArn` und die `aws:SourceAccount` globale Bedingung verwenden können, AWS Config um das Problem

des verwirrten Stellvertreters zu vermeiden: AWS Config Zugriff auf den Amazon S3 S3-Bucket gewähren.

Bewährte Sicherheitsmethoden für AWS Config

AWS Config bietet eine Reihe von Sicherheitsfunktionen, die Sie bei der Entwicklung und Implementierung Ihrer eigenen Sicherheitsrichtlinien berücksichtigen sollten. Die folgenden bewährten Methoden sind allgemeine Richtlinien und keine vollständige Sicherheitslösung. Da diese bewährten Methoden für Ihre Umgebung möglicherweise nicht angemessen oder ausreichend sind, sollten Sie sie als hilfreiche Überlegungen und nicht als bindend ansehen.

- Nutzen Sie Tagging for AWS Config, um Ressourcen einfacher zu verwalten, zu suchen und zu filtern.
- Vergewissern Sie sich, dass Ihre Lieferkanäle richtig eingerichtet wurden, und stellen Sie nach der Bestätigung sicher, dass die Aufzeichnung korrekt AWS Config ist.

Weitere Informationen finden Sie im Blog Bewährte Methoden für AWS Config.

Einloggen und Überwachen AWS Config

AWS Config ist in einen Dienst integriert AWS CloudTrail, der eine Aufzeichnung der Aktionen bereitstellt, die von einem Benutzer, einer Rolle oder einem AWS Dienst in ausgeführt wurden AWS Config. Die Überwachung ist ein wichtiger Bestandteil der Aufrechterhaltung der Zuverlässigkeit, Verfügbarkeit AWS Config und Leistung Ihrer AWS Lösungen.

Themen

- Protokollieren von AWS Config API-Aufrufen mit AWS CloudTrail
- Überwachen

Protokollieren von AWS Config API-Aufrufen mit AWS CloudTrail

CloudTrail erfasst alle API-Aufrufe AWS Config als Ereignisse. Zu den erfassten Aufrufen gehören Aufrufe von der AWS Config Konsole und Codeaufrufen für die AWS Config API-Operationen. Wenn Sie einen Trail erstellen, können Sie die kontinuierliche Bereitstellung von CloudTrail Ereignissen an einen Amazon S3 S3-Bucket aktivieren, einschließlich Ereignissen für AWS Config. Wenn Sie keinen Trail konfigurieren, können Sie die neuesten Ereignisse trotzdem in der CloudTrail Konsole im Ereignisverlauf anzeigen. Anhand der von gesammelten Informationen können Sie die Anfrage ermitteln CloudTrail, an die die Anfrage gestellt wurde AWS Config, die IP-Adresse, von der aus die Anfrage gestellt wurde, wer die Anfrage gestellt hat, wann sie gestellt wurde, und weitere Details.

Weitere Informationen CloudTrail dazu finden Sie im AWS CloudTrail Benutzerhandbuch.

Themen

- AWS Config Informationen in CloudTrail
- Grundlegendes zu AWS Config Protokolldateieinträgen
- Beispiele für Protokolldateien

AWS Config Informationen in CloudTrail

CloudTrail ist auf Ihrem aktiviert AWS-Konto , wenn Sie das Konto erstellen. Wenn eine Aktivität in stattfindet AWS Config, wird diese Aktivität zusammen mit anderen AWS Serviceereignissen in der CloudTrail Ereignishistorie in einem Ereignis aufgezeichnet. Sie können aktuelle Ereignisse in Ihrem

anzeigen, suchen und herunterladen AWS-Konto. Weitere Informationen finden Sie unter Ereignisse mit CloudTrail Ereignisverlauf anzeigen.

Für eine fortlaufende Aufzeichnung der Ereignisse in Ihrem AWS-Konto, einschließlich der Ereignisse für AWS Config, erstellen Sie einen Trail. Ein Trail ermöglicht CloudTrail die Übermittlung von Protokolldateien an einen Amazon S3 S3-Bucket. Wenn Sie einen Trail in der Konsole anlegen, gilt dieser für alle AWS-Regionen-Regionen. Der Trail protokolliert Ereignisse aus allen Regionen der AWS Partition und übermittelt die Protokolldateien an den von Ihnen angegebenen Amazon S3 S3-Bucket. Darüber hinaus können Sie andere AWS Dienste konfigurieren, um die in den CloudTrail Protokollen gesammelten Ereignisdaten weiter zu analysieren und darauf zu reagieren. Weitere Informationen finden Sie hier:

- Übersicht zum Erstellen eines Trails
- CloudTrail Unterstützte Dienste und Integrationen
- Konfiguration von Amazon SNS SNS-Benachrichtigungen für CloudTrail
- Empfangen von CloudTrail Protokolldateien aus mehreren Regionen und Empfangen von CloudTrail Protokolldateien von mehreren Konten

Alle AWS Config Vorgänge werden von der AWS Config API-Referenz protokolliert CloudTrail und sind in dieser dokumentiert. Beispielsweise generieren Aufrufe der DescribeDeliveryChannelsOperationen DeliverConfigSnapshotDeleteDeliveryChannel, und Einträge in den CloudTrail Protokolldateien.

Jeder Ereignis- oder Protokolleintrag enthält Informationen zu dem Benutzer, der die Anforderung generiert hat. Die Identitätsinformationen unterstützen Sie bei der Ermittlung der folgenden Punkte:

- Ob die Anfrage mit Root- oder AWS Identity and Access Management (IAM-) Benutzeranmeldedaten gestellt wurde.
- Gibt an, ob die Anforderung mit temporären Sicherheitsanmeldeinformationen für eine Rolle oder einen Verbundbenutzer gesendet wurde.
- Ob die Anfrage von einem anderen AWS Dienst gestellt wurde.

Weitere Informationen finden Sie unter CloudTrail userIdentity-Element.

Grundlegendes zu AWS Config Protokolldateieinträgen

Ein Trail ist eine Konfiguration, die die Übertragung von Ereignissen als Protokolldateien an einen von Ihnen angegebenen Amazon S3 S3-Bucket ermöglicht. CloudTrail Protokolldateien enthalten einen oder mehrere Protokolleinträge. Ein Ereignis stellt eine einzelne Anforderung aus einer beliebigen Quelle dar und enthält Informationen über die angeforderte Aktion, Datum und Uhrzeit der Aktion, Anforderungsparameter usw. CloudTrail Protokolldateien sind kein geordneter Stack-Trace der öffentlichen API-Aufrufe, sodass sie nicht in einer bestimmten Reihenfolge angezeigt werden.

Beispiele für Protokolldateien

Beispiele für die CloudTrail Protokolleinträge finden Sie in den folgenden Themen.

DeleteDeliveryChannel

Im Folgenden finden Sie ein Beispiel für eine CloudTrail Protokolldatei für den DeleteDeliveryChannelVorgang.

```
{
      "eventVersion": "1.02",
      "userIdentity": {
        "type": "IAMUser",
        "principalId": "AIDACKCEVSQ6C2EXAMPLE",
        "arn": "arn:aws:iam::222222222222:user/JohnDoe",
        "accountId": "222222222222",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "userName": "JohnDoe"
      },
      "eventTime": "2014-12-11T18:32:57Z",
      "eventSource": "config.amazonaws.com",
      "eventName": "DeleteDeliveryChannel",
      "awsRegion": "us-west-2",
      "sourceIPAddress": "10.24.34.0",
      "userAgent": "aws-internal/3",
      "requestParameters": {
        "deliveryChannelName": "default"
      },
      "responseElements": null,
      "requestID": "207d695a-8164-11e4-ab4f-657c7ab282ab",
      "eventID": "5dcff7a9-e414-411a-a43e-88d122a0ad4a",
      "eventType": "AwsApiCall",
      "recipientAccountId": "222222222222"
```

```
    }
```

DeliverConfigSnapshot

Im Folgenden finden Sie ein Beispiel für eine CloudTrail Protokolldatei für den DeliverConfigSnapshotVorgang.


```
{
      "eventVersion": "1.02",
      "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AIDAABCDEFGHIJKLNMOPQ:Config-API-Test",
        "arn": "arn:aws:sts::111111111111:assumed-role/JaneDoe/Config-API-Test",
        "accountId": "111111111111",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "sessionContext": {
          "attributes": {
            "mfaAuthenticated": "false",
            "creationDate": "2014-12-11T00:58:42Z"
          },
          "sessionIssuer": {
            "type": "Role",
            "principalId": "AIDAABCDEFGHIJKLNMOPQ",
            "arn": "arn:aws:iam::111111111111:role/JaneDoe",
            "accountId": "111111111111",
            "userName": "JaneDoe"
          }
        }
      },
      "eventTime": "2014-12-11T00:58:53Z",
      "eventSource": "config.amazonaws.com",
      "eventName": "DeliverConfigSnapshot",
      "awsRegion": "us-west-2",
      "sourceIPAddress": "10.24.34.0",
      "userAgent": "aws-cli/1.2.11 Python/2.7.4 Linux/2.6.18-164.el5",
      "requestParameters": {
        "deliveryChannelName": "default"
      },
      "responseElements": {
        "configSnapshotId": "58d50f10-212d-4fa4-842e-97c614da67ce"
      },
      "requestID": "e0248561-80d0-11e4-9f1c-7739d36a3df2",
      "eventID": "3e88076c-eae1-4aa6-8990-86fe52aedbd8",
```

```
      "eventType": "AwsApiCall",
      recipientAccountId": "111111111111"
    }
```

DescribeConfigurationRecorderStatus

Im Folgenden finden Sie ein Beispiel für eine CloudTrail Protokolldatei für den DescribeConfigurationRecorderStatusVorgang.

```
{
      "eventVersion": "1.02",
      "userIdentity": {
        "type": "IAMUser",
        "principalId": "AIDACKCEVSQ6C2EXAMPLE",
        "arn": "arn:aws:iam::222222222222:user/JohnDoe",
        "accountId": "222222222222",
        "accessKeyId": "AKIAI44QH8DHBEXAMPLE",
        "userName": "JohnDoe"
      },
      "eventTime": "2014-12-11T18:35:44Z",
      "eventSource": "config.amazonaws.com",
      "eventName": "DescribeConfigurationRecorderStatus",
      "awsRegion": "us-west-2",
      "sourceIPAddress": "192.0.2.0",
      "userAgent": "aws-cli/1.2.11 Python/2.7.4 Linux/2.6.18-164.el5",
      "requestParameters": null,
      "responseElements": null,
      "requestID": "8442f25d-8164-11e4-ab4f-657c7ab282ab",
      "eventID": "a675b36b-455f-4e18-a4bc-d3e01749d3f1",
      "eventType": "AwsApiCall",
      "recipientAccountId": "222222222222"
    }
```

DescribeConfigurationRecorders

Im Folgenden finden Sie ein Beispiel für eine CloudTrail Protokolldatei für den DescribeConfigurationRecordersVorgang.

```
{
      "eventVersion": "1.02",
      "userIdentity": {
        "type": "IAMUser",
        "principalId": "AIDACKCEVSQ6C2EXAMPLE",
```

```
        "arn": "arn:aws:iam::222222222222:user/JohnDoe",
        "accountId": "222222222222",
        "accessKeyId": "AKIAI44QH8DHBEXAMPLE",
        "userName": "JohnDoe"
      },
      "eventTime": "2014-12-11T18:34:52Z",
      "eventSource": "config.amazonaws.com",
      "eventName": "DescribeConfigurationRecorders",
      "awsRegion": "us-west-2",
      "sourceIPAddress": "192.0.2.0",
      "userAgent": "aws-cli/1.2.11 Python/2.7.4 Linux/2.6.18-164.el5",
      "requestParameters": null,
      "responseElements": null,
      "requestID": "6566b55c-8164-11e4-ab4f-657c7ab282ab",
      "eventID": "6259a9ad-889e-423b-beeb-6e1eec84a8b5",
      "eventType": "AwsApiCall",
      "recipientAccountId": "222222222222"
    }
```

DescribeDeliveryChannels

Im Folgenden finden Sie ein Beispiel für eine CloudTrail Protokolldatei für den DescribeDeliveryChannelsVorgang.

```
{
      "eventVersion": "1.02",
      "userIdentity": {
        "type": "IAMUser",
        "principalId": "AIDACKCEVSQ6C2EXAMPLE",
        "arn": "arn:aws:iam::222222222222:user/JohnDoe",
        "accountId": "222222222222",
        "accessKeyId": "AKIAI44QH8DHBEXAMPLE",
        "userName": "JohnDoe"
      },
      "eventTime": "2014-12-11T18:35:02Z",
      "eventSource": "config.amazonaws.com",
      "eventName": "DescribeDeliveryChannels",
      "awsRegion": "us-west-2",
      "sourceIPAddress": "192.0.2.0",
      "userAgent": "aws-cli/1.2.11 Python/2.7.4 Linux/2.6.18-164.el5",
      "requestParameters": null,
      "responseElements": null,
      "requestID": "6b6aee3f-8164-11e4-ab4f-657c7ab282ab",
```

```
      "eventID": "3e15ebc5-bf39-4d2a-8b64-9392807985f1",
      "eventType": "AwsApiCall",
      "recipientAccountId": "222222222222"
    }
```

GetResourceConfigHistory

Im Folgenden finden Sie ein Beispiel für eine CloudTrail Protokolldatei für den GetResourceConfigHistoryVorgang.

```
{
      "eventVersion": "1.02",
      "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AIDAABCDEFGHIJKLNMOPQ:Config-API-Test",
        "arn": "arn:aws:sts::111111111111:assumed-role/JaneDoe/Config-API-Test",
        "accountId": "111111111111",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "sessionContext": {
          "attributes": {
            "mfaAuthenticated": "false",
            "creationDate": "2014-12-11T00:58:42Z"
          },
          "sessionIssuer": {
            "type": "Role",
            "principalId": "AIDAABCDEFGHIJKLNMOPQ",
            "arn": "arn:aws:iam::111111111111:role/JaneDoe",
            "accountId": "111111111111",
            "userName": "JaneDoe"
          }
        }
      },
      "eventTime": "2014-12-11T00:58:42Z",
      "eventSource": "config.amazonaws.com",
      "eventName": "GetResourceConfigHistory",
      "awsRegion": "us-west-2",
      "sourceIPAddress": "10.24.34.0",
      "userAgent": "aws-cli/1.2.11 Python/2.7.4 Linux/2.6.18-164.el5",
      "requestParameters": {
        "resourceId": "vpc-a12bc345",
        "resourceType": "AWS::EC2::VPC",
        "limit": 0,
        "laterTime": "Dec 11, 2014 12:58:42 AM",
```

```
        "earlierTime": "Dec 10, 2014 4:58:42 PM"
      },
      "responseElements": null,
      "requestID": "d9f3490d-80d0-11e4-9f1c-7739d36a3df2",
      "eventID": "ba9c1766-d28f-40e3-b4c6-3ffb87dd6166",
      "eventType": "AwsApiCall",
      "recipientAccountId": "111111111111"
      }
```

PutConfigurationRecorder

Im Folgenden finden Sie ein Beispiel für eine CloudTrail Protokolldatei für den PutConfigurationRecorderVorgang.

```
{
      "eventVersion": "1.02",
      "userIdentity": {
        "type": "IAMUser",
        "principalId": "AIDACKCEVSQ6C2EXAMPLE",
        "arn": "arn:aws:iam::222222222222:user/JohnDoe",
        "accountId": "222222222222",
        "accessKeyId": "AKIAI44QH8DHBEXAMPLE",
        "userName": "JohnDoe"
      },
      "eventTime": "2014-12-11T18:35:23Z",
      "eventSource": "config.amazonaws.com",
      "eventName": "PutConfigurationRecorder",
      "awsRegion": "us-west-2",
      "sourceIPAddress": "192.0.2.0",
      "userAgent": "aws-cli/1.2.11 Python/2.7.4 Linux/2.6.18-164.el5",
      "requestParameters": {
        "configurationRecorder": {
          "name": "default",
          "roleARN": "arn:aws:iam::222222222222:role/config-role-pdx"
        }
      },
      "responseElements": null,
      "requestID": "779f7917-8164-11e4-ab4f-657c7ab282ab",
      "eventID": "c91f3daa-96e8-44ee-8ddd-146ac06565a7",
      "eventType": "AwsApiCall",
      "recipientAccountId": "222222222222"
    }
```

PutDeliveryChannel

Im Folgenden finden Sie ein Beispiel für eine CloudTrail Protokolldatei für den PutDeliveryChannelVorgang.

```
{
      "eventVersion": "1.02",
      "userIdentity": {
        "type": "IAMUser",
        "principalId": "AIDACKCEVSQ6C2EXAMPLE",
        "arn": "arn:aws:iam::222222222222:user/JohnDoe",
        "accountId": "222222222222",
        "accessKeyId": "AKIAI44QH8DHBEXAMPLE",
        "userName": "JohnDoe"
      },
      "eventTime": "2014-12-11T18:33:08Z",
      "eventSource": "config.amazonaws.com",
      "eventName": "PutDeliveryChannel",
      "awsRegion": "us-west-2",
      "sourceIPAddress": "192.0.2.0",
      "userAgent": "aws-cli/1.2.11 Python/2.7.4 Linux/2.6.18-164.el5",
      "requestParameters": {
        "deliveryChannel": {
          "name": "default",
          "s3BucketName": "config-api-test-pdx",
          "snsTopicARN": "arn:aws:sns:us-west-2:222222222222:config-api-test-pdx"
        }
      },
      "responseElements": null,
      "requestID": "268b8d4d-8164-11e4-ab4f-657c7ab282ab",
      "eventID": "b2db05f1-1c73-4e52-b238-db69c04e8dd4",
      "eventType": "AwsApiCall",
      "recipientAccountId": "222222222222"
    }
```

StartConfigurationRecorder

Im Folgenden finden Sie ein Beispiel für eine CloudTrail Protokolldatei für den StartConfigurationRecorderVorgang.

```
{
      "eventVersion": "1.02",
      "userIdentity": {
```

```
        "type": "IAMUser",
        "principalId": "AIDACKCEVSQ6C2EXAMPLE",
        "arn": "arn:aws:iam::222222222222:user/JohnDoe",
        "accountId": "222222222222",
        "accessKeyId": "AKIAI44QH8DHBEXAMPLE",
        "userName": "JohnDoe"
      },
      "eventTime": "2014-12-11T18:35:34Z",
      "eventSource": "config.amazonaws.com",
      "eventName": "StartConfigurationRecorder",
      "awsRegion": "us-west-2",
      "sourceIPAddress": "192.0.2.0",
      "userAgent": "aws-cli/1.2.11 Python/2.7.4 Linux/2.6.18-164.el5",
      "requestParameters": {
        "configurationRecorderName": "default"
      },
      "responseElements": null,
      "requestID": "7e03fa6a-8164-11e4-ab4f-657c7ab282ab",
      "eventID": "55a5507f-f306-4896-afe3-196dc078a88d",
      "eventType": "AwsApiCall",
      "recipientAccountId": "222222222222"
    }
```

StopConfigurationRecorder

Im Folgenden finden Sie ein Beispiel für eine CloudTrail Protokolldatei für den StopConfigurationRecorderVorgang.

```
{
      "eventVersion": "1.02",
      "userIdentity": {
        "type": "IAMUser",
        "principalId": "AIDACKCEVSQ6C2EXAMPLE",
        "arn": "arn:aws:iam::222222222222:user/JohnDoe",
        "accountId": "222222222222",
        "accessKeyId": "AKIAI44QH8DHBEXAMPLE",
        "userName": "JohnDoe"
      },
      "eventTime": "2014-12-11T18:35:13Z",
      "eventSource": "config.amazonaws.com",
      "eventName": "StopConfigurationRecorder",
      "awsRegion": "us-west-2",
      "sourceIPAddress": "192.0.2.0",
```

```
      "userAgent": "aws-cli/1.2.11 Python/2.7.4 Linux/2.6.18-164.el5",
      "requestParameters": {
        "configurationRecorderName": "default"
      },
      "responseElements": null,
      "requestID": "716deea3-8164-11e4-ab4f-657c7ab282ab",
      "eventID": "6225a85d-1e49-41e9-bf43-3cfc5549e560",
      "eventType": "AwsApiCall",
      "recipientAccountId": "222222222222"
    }
```

Überwachen

Sie können andere AWS Dienste verwenden, um AWS Config Ressourcen zu überwachen.

- Sie können Amazon Simple Notification Service (SNS) verwenden, um Ihnen jedes Mal Benachrichtigungen zu senden, wenn eine unterstützte AWS Ressource aufgrund von Benutzer-API-Aktivitäten erstellt, aktualisiert oder anderweitig geändert wird.
- Sie können Amazon verwenden EventBridge , um Änderungen im Status von AWS Config Ereignissen zu erkennen und darauf zu reagieren.

Themen

- Überwachen von AWS Ressourcenänderungen mit Amazon SQS
- Überwachung AWS Config mit Amazon EventBridge

Überwachen von AWS Ressourcenänderungen mit Amazon SQS

AWS Config verwendet Amazon Simple Notification Service (SNS), um Ihnen jedes Mal Benachrichtigungen zu senden, wenn eine unterstützte AWS Ressource aufgrund von Benutzer-API-Aktivitäten erstellt, aktualisiert oder anderweitig geändert wird. Allerdings sind möglicherweise nur bestimmte Änderungen der Ressourcenkonfiguration für Sie interessant. Beispielsweise könnten Sie es für wichtig halten, zu wissen, wann jemand die Konfiguration einer Sicherheitsgruppe ändert, aber Sie müssen es nicht jedes Mal wissen, wenn sich die Tags auf Ihren EC2 Amazon-Instances ändern. Sie können auch ein Programm schreiben, mit dem bei Aktualisierung bestimmter Ressourcen bestimmte Aktionen ausführt werden. Sie können beispielsweise eine bestimmte Workflow-Konfiguration starten, wenn eine Sicherheitsgruppe geändert wird. Wenn Sie die Daten auf

diese oder andere Weise programmgesteuert nutzen möchten, verwenden Sie eine Amazon Simple Queue Service-Warteschlange als Benachrichtigungsendpunkt für Amazon SNS. AWS Config

> **Note**
>
> Benachrichtigungen können von Amazon SNS auch in Form einer E-Mail, einer SMS an SMS-fähige Mobiltelefone und Smartphones, einer Benachrichtigung an eine Anwendung auf einem mobilen Gerät oder einer Benachrichtigung an ein oder mehrere HTTP- oder HTTPS-Endpunkte gesendet werden.

Sie können eine einzelne SQS-Warteschlange mehrere Themen abonnieren, unabhängig davon, ob Sie ein Thema für jede Region oder ein Thema für jedes Konto für jede Region haben. Sie müssen die Warteschlange vom gewünschten SNS-Thema abonnieren lassen. (Sie können mehrere Warteschlangen in einem SNS-Thema abonnieren.) Weitere Informationen finden Sie unter Senden von Amazon-SNS-Nachrichten an Amazon-SQS-Warteschlangen.

Berechtigungen für Amazon SQS

Um Amazon SQS mit zu verwenden AWS Config, müssen Sie eine Richtlinie konfigurieren, die Ihrem Konto die Erlaubnis erteilt, alle Aktionen auszuführen, die in einer SQS-Warteschlange zulässig sind. Die folgenden Beispielrichtlinie erteilt dem Konto mit der Nummer 111122223333 und dem Konto mit der Nummer 444455556666 die Berechtigung für das Senden von Nachrichten bei jeder Konfigurationsänderung an der Warteschlange mit dem Namen „arn:aws:sqs:us-east-2:444455556666:queue1“.

```
{
  "Version": "2012-10-17",
  "Id": "Queue1_Policy_UUID",
  "Statement":
    {
       "Sid":"Queue1_SendMessage",
       "Effect": "Allow",
       "Principal": {
            "AWS": ["111122223333","444455556666"]
         },
        "Action": "sqs:SendMessage",
        "Resource": "arn:aws:sqs:us-east-2:444455556666:queue1"
     }
}
```

Sie müssen auch eine Richtlinie erstellen, die Berechtigungen für Verbindungen zwischen einem SNS-Thema und der SQS-Warteschlange, die das Thema abonniert, erteilt. Die folgende Beispielrichtlinie ermöglicht es dem SNS-Thema mit dem Amazon-Ressourcennamen (ARN) arn:aws:sns:us-east- 2:111122223333:test-topic, beliebige Aktionen in der Warteschlange mit dem Namen arn:aws:sqs:us-east- 2:111122223333 auszuführen:. test-topic-queue

> **Note**
>
> Die Konten des SNS-Themas und der SQS-Warteschlange müssen sich in derselben Region befinden.

```
{
  "Version": "2012-10-17",
  "Id": "SNStoSQS",
  "Statement":
    {
      "Sid":"rule1",
      "Effect": "Allow",
      "Principal": {
        "Service": "sns.amazonaws.com"
      },
      "Action": "SQS:SendMessage",
      "Resource": "arn:aws:sqs:us-east-2:111122223333:test-topic-queue",
      "Condition" : {
        "StringEquals" : {
          "aws:SourceArn":"arn:aws:sns:us-east-2:111122223333:test-topic"
        }
      }
    }
}
```

Jede Richtlinie kann Anweisungen für nur eine einzige Warteschlange und nicht mehrere Warteschlangen enthalten. Informationen zu weiteren Einschränkungen bei Amazon-SQ-Richtlinien finden Sie unter Spezielle Informationen zu Amazon-SQS-Richtlinien.

Überwachung AWS Config mit Amazon EventBridge

Amazon EventBridge liefert nahezu in Echtzeit einen Stream von Systemereignissen, die Änderungen an AWS Ressourcen beschreiben. Verwenden Sie Amazon EventBridge , um Änderungen im Status von AWS Config Ereignissen zu erkennen und darauf zu reagieren.

Sie können eine Regel erstellen, die ausgeführt wird, sobald ein Statusübergang oder ein Übergang zu einem oder mehreren Status stattfindet, die für sie von Interesse sind. Basierend auf den von Ihnen erstellten Regeln EventBridge ruft Amazon dann eine oder mehrere Zielaktionen auf, wenn ein Ereignis den Werten entspricht, die Sie in einer Regel angeben. Abhängig vom Ereignistyp können Sie Benachrichtigungen versenden, Ereignisinformationen erfassen, Korrekturmaßnahmen ausführen, Ereignisse auslösen oder andere Aktionen ausführen.

Bevor Sie jedoch Event-Regeln für AWS Config erstellen, sollten Sie Folgendes tun:

- Machen Sie sich mit Ereignissen, Regeln und Zielen in vertraut EventBridge. Weitere Informationen finden Sie unter Was ist Amazon EventBridge?
- Weitere Informationen zu den ersten Schritten EventBridge und zur Einrichtung von Regeln finden Sie unter Erste Schritte mit Amazon EventBridge.
- Erstellen Sie das Ziel oder die Ziele für die Ereignisregeln.

Themen

- Überlegungen
- EventBridge Amazon-Format für AWS Config
- EventBridge Amazon-Regel erstellen für AWS Config

Überlegungen

Sie erhalten keine Benachrichtigungen EventBridge für die folgenden Ressourcentypen, wenn Sie sie nicht mit aufzeichnen AWS Config:

- `AWS::ACM::Certificate`
- `AWS::CloudTrail::Trail`
- `AWS::CloudWatch::Alarm`
- `AWS::EC2::CustomerGateway`
- `AWS::EC2::EIP`

- AWS::EC2::Host
- AWS::EC2::Instance
- AWS::EC2::InternetGateway
- AWS::EC2::NetworkAcl
- AWS::EC2::NetworkInterface
- AWS::EC2::RouteTable
- AWS::EC2::SecurityGroup
- AWS::EC2::Subnet
- AWS::EC2::VPC
- AWS::EC2::VPNConnection
- AWS::EC2::VPNGateway
- AWS::EC2::Volume
- AWS::ElasticLoadBalancingV2::LoadBalancer
- AWS::IAM::Group
- AWS::IAM::Policy
- AWS::IAM::Role
- AWS::IAM::User
- AWS::RDS::DBInstance
- AWS::RDS::DBSecurityGroup
- AWS::RDS::DBSnapshot
- AWS::RDS::DBSubnetGroup
- AWS::RDS::EventSubscription
- AWS::Redshift::Cluster
- AWS::Redshift::ClusterParameterGroup
- AWS::Redshift::ClusterSecurityGroup
- AWS::Redshift::ClusterSnapshot
- AWS::Redshift::ClusterSubnetGroup
- AWS::Redshift::EventSubscription
- AWS::S3::Bucket

EventBridge Amazon-Format für AWS Config

Die EventBridge Veranstaltung für AWS Config hat das folgende Format:

```
{
   "version": "0",
   "id": "cd4d811e-ab12-322b-8255-872ce65b1bc8",
   "detail-type": "event type",
   "source": "aws.config",
   "account": "111122223333",
   "time": "2018-03-22T00:38:11Z",
   "region": "us-east-1",
   "resources": [
      resources
   ],
   "detail": {
      specific message type
   }
}
```

EventBridge Amazon-Regel erstellen für AWS Config

Gehen Sie wie folgt vor, um eine EventBridge Regel zu erstellen, die bei einem Ereignis ausgelöst wird, das von ausgelöst wird AWS Config. Ereignisse werden auf bestmögliche Weise ausgegeben.

1. Wählen Sie im Navigationsbereich Regeln aus.
2. Wählen Sie Regel erstellen aus.
3. Geben Sie einen Namen und eine Beschreibung für die Regel ein.

   Eine Regel darf nicht denselben Namen wie eine andere Regel in derselben Region und auf demselben Event Bus haben.

> **Note**
>
> Ein Ereignisbus empfängt Ereignisse von einer Quelle, verwendet Regeln, um sie auszuwerten, wendet alle konfigurierten Eingabetransformationen an und leitet sie an die entsprechenden Ziele weiter. Der Standard-Event-Bus Ihres Kontos empfängt Ereignisse von AWS-Services. Ein benutzerdefinierter Event-Bus kann Ereignisse von

Ihren benutzerdefinierten Anwendungen und Diensten empfangen. Ein Partner-Eventbus empfängt Ereignisse aus einer Eventquelle, die von einem SaaS-Partner erstellt wurde. Diese Ereignisse stammen aus den Diensten oder Anwendungen des Partners. Weitere Informationen finden Sie unter Event Buses EventBridge in Amazon im EventBridge Amazon-Benutzerhandbuch.

4. Bei Regeltyp wählen Sie Regel mit einem Ereignismuster aus.
5. Wählen Sie als Quelle der Veranstaltung AWS Veranstaltungen oder EventBridge Partnerveranstaltungen aus.
6. (Optional) Wählen Sie für Beispielereignistyp AWS -Ereignisse aus.
7. (Optional) Wählen Sie für Beispielereignisse den Ereignistyp aus, der die Regel auslöst:
   - Wählen Sie AWS API-Aufruf von CloudTrail, um Regeln für API-Aufrufe an diesen Dienst festzulegen. Weitere Informationen zur Erstellung dieser Art von Regel finden Sie unter Tutorial: EventBridge Amazon-Regel für AWS CloudTrail API-Aufrufe erstellen.
   - Wählen Sie Config Configuration Item Change (Änderung eines Konfigurationselements konfigurieren) aus, damit Sie Benachrichtigungen erhalten, wenn eine Ressource in Ihrem Konto geändert wird.

     Wie in diesen Support-Artikeln beschrieben, können EventBridge Sie benutzerdefinierte E-Mail-Benachrichtigungen erhalten, wenn eine Ressource erstellt oder gelöscht wird. Wie kann ich benutzerdefinierte E-Mail-Benachrichtigungen erhalten, wenn eine Ressource in meinem AWS-Konto nutzenden AWS Config Service erstellt wird? und wie kann ich benutzerdefinierte E-Mail-Benachrichtigungen erhalten, wenn eine Ressource in meinem AWS-KontoAWS Config Nutzungsdienst gelöscht wird? .
   - Wählen Sie Config Rules Compliance Change (Änderung der Regel-Compliance konfigurieren) aus, damit Sie Benachrichtigungen erhalten, wenn eine Compliance-Prüfung mit Ihren Regeln fehlschlägt.

     Wie in diesem Support-Artikel beschrieben, können EventBridge Sie benutzerdefinierte E-Mail-Benachrichtigungen erhalten, wenn eine Ressource nicht konform ist. Wie kann ich benachrichtigt werden, wenn eine AWS Ressource nicht richtlinientreu ist? AWS Config .
   - Wählen Sie Config Rules Re-evaluation Status (Neuauswertungsstatus für Regeln konfigurieren) aus, um Benachrichtigungen zum Status der Neuauswertung zu erhalten.
   - Wählen Sie Config Configuration Snapshot Delivery Status (Übermittlungsstatus des Konfigurations-Snapshots konfigurieren) aus, um Benachrichtigungen zum Übermittlungsstatus des Konfigurations-Snapshots zu erhalten.

- Wählen Sie Config Configuration History Delivery Status (Übermittlungsstatus des Konfigurationsverlaufs konfigurieren) aus, um Benachrichtigungen zum Übermittlungsstatus des Konfigurationsverlaufs zu erhalten.

8. Wählen Sie für Erstellungsmethode die Option Musterformular verwenden aus.
9. Als Event source (Ereignisquelle) wählen Sie AWS -Services aus.
10. Wählen Sie für AWS -Service die Option Config.
11. Wählen Sie für Ereignistyp den Ereignistyp aus, der die Regel auslösen soll:

- Wählen Sie Alle Ereignisse, um eine Regel zu erstellen, die für alle AWS Dienste gilt. Wenn Sie diese Option wählen, können Sie keine bestimmten Nachrichtentypen, Regelnamen, Ressourcentypen oder Ressourcen auswählen IDs.
- Wählen Sie AWS API-Aufruf von CloudTrail, um die Regeln für API-Aufrufe an diesen Dienst festzulegen. Weitere Informationen zur Erstellung dieser Art von Regel finden Sie unter Tutorial: EventBridge Amazon-Regel für AWS CloudTrail API-Aufrufe erstellen.
- Wählen Sie Config Configuration Item Change (Änderung eines Konfigurationselements konfigurieren) aus, damit Sie Benachrichtigungen erhalten, wenn eine Ressource in Ihrem Konto geändert wird.

  Wie in diesen Support-Artikeln beschrieben, können EventBridge Sie benutzerdefinierte E-Mail-Benachrichtigungen erhalten, wenn eine Ressource erstellt oder gelöscht wird. Wie kann ich benutzerdefinierte E-Mail-Benachrichtigungen erhalten, wenn eine Ressource in meinem AWS-Konto nutzenden AWS Config Service erstellt wird? und wie kann ich benutzerdefinierte E-Mail-Benachrichtigungen erhalten, wenn eine Ressource in meinem AWS-KontoAWS Config Nutzungsdienst gelöscht wird? .
- Wählen Sie Config Rules Compliance Change (Änderung der Regel-Compliance konfigurieren) aus, damit Sie Benachrichtigungen erhalten, wenn eine Compliance-Prüfung mit Ihren Regeln fehlschlägt.

  Wie in diesem Support-Artikel beschrieben, können EventBridge Sie benutzerdefinierte E-Mail-Benachrichtigungen erhalten, wenn eine Ressource nicht konform ist. Wie kann ich benachrichtigt werden, wenn eine AWS Ressource nicht richtlinientreu ist? AWS Config .
- Wählen Sie Config Rules Re-evaluation Status (Neuauswertungsstatus für Regeln konfigurieren) aus, um Benachrichtigungen zum Status der Neuauswertung zu erhalten.
- Wählen Sie Config Configuration Snapshot Delivery Status (Übermittlungsstatus des Konfigurations-Snapshots konfigurieren) aus, um Benachrichtigungen zum Übermittlungsstatus des Konfigurations-Snapshots zu erhalten.

- Wählen Sie Config Configuration History Delivery Status (Übermittlungsstatus des Konfigurationsverlaufs konfigurieren) aus, um Benachrichtigungen zum Übermittlungsstatus des Konfigurationsverlaufs zu erhalten.

12. Wählen Sie Any message type (Beliebiger Nachrichtentyp) aus, um Benachrichtigungen eines beliebigen Typs zu erhalten. Wählen Sie Specific message type(s) (Spezifische Nachrichtentyp(en)) aus, um folgende Benachrichtigungstypen zu erhalten:
    - Wenn Sie möchten ConfigurationItemChangeNotification, erhalten Sie Meldungen, wenn sich die Konfiguration einer AWS Config auswertenden Ressource geändert hat.
    - Wenn Sie möchten ComplianceChangeNotification, erhalten Sie Meldungen, wenn sich der Konformitätstyp einer AWS Config auswertenden Ressource geändert hat.
    - Wenn Sie möchten ConfigRulesEvaluationStarted, erhalten Sie Meldungen, wenn AWS Config mit der Auswertung Ihrer Regel anhand der angegebenen Ressourcen begonnen wird.
    - Wenn Sie möchten ConfigurationSnapshotDeliveryCompleted, erhalten Sie Nachrichten, wenn der Konfigurations-Snapshot AWS Config erfolgreich an Ihren Amazon S3-Bucket übermittelt wurde.
    - Wenn Sie möchten ConfigurationSnapshotDeliveryFailed, erhalten Sie Meldungen, wenn der Konfigurations-Snapshot AWS Config nicht an Ihren Amazon S3-Bucket übermittelt werden kann.
    - Wenn Sie möchten ConfigurationSnapshotDeliveryStarted, erhalten Sie Nachrichten, wenn AWS Config mit der Bereitstellung des Konfigurations-Snapshots an Ihren Amazon S3 S3-Bucket begonnen wird.
    - Wenn Sie möchten ConfigurationHistoryDeliveryCompleted, erhalten Sie Nachrichten, wenn der Konfigurationsverlauf AWS Config erfolgreich an Ihren Amazon S3-Bucket übermittelt wurde.
13. Wenn Sie einen bestimmten Ereignistyp aus der Dropdownliste Ereignistyp ausgewählt haben, wählen Sie Beliebiger Ressourcentyp aus, um eine Regel zu erstellen, die für alle AWS Config unterstützten Ressourcentypen gilt.

    Alternativ können Sie Specific resource type(s) (Spezifische Ressourcentyp(en)) auswählen und dann den von AWS Config unterstützten Ressourcentyp eingeben (z. B. `AWS::EC2::Instance`).
14. Bei Auswahl eines bestimmten Ereignistyps aus der Dropdown-Liste Ereignistyp sollten Sie Beliebige Ressourcen-ID auswählen, um jede von AWS Config unterstützte Ressourcen-ID einzuschließen.

    Alternativ können Sie Specific resource ID(s) (Spezifische Ressourcen-ID(s)) auswählen und dann die von AWS Config unterstützte Ressourcen-ID eingeben (z. B. `i-04606de676e635647`).

15. Bei Auswahl eines bestimmten Ereignistyps aus der Dropdown-Liste Ereignistyp sollten Sie Beliebiger Regelname auswählen, um jede von AWS Config unterstützte Regel einzuschließen.

    Alternativ können Sie Specific rule name(s) (Spezifische Regelname(n)) auswählen und dann die von AWS Config unterstützte Regel eingeben (z. B. required-tags).
16. Wählen Sie in Ziel(e) auswählen den Zieltyp aus, den Sie für die Verwendung mit dieser Regel vorbereitet haben, und konfigurieren Sie dann weitere für diesen Typ erforderliche Optionen.
17. Die angezeigten Felder variieren je nach ausgewähltem Service. Geben Sie nach Bedarf Informationen ein, die für diesen Zieltyp spezifisch sind.
18. Für viele Zieltypen sind EventBridge Berechtigungen erforderlich, um Ereignisse an das Ziel zu senden. In diesen Fällen EventBridge kann die IAM-Rolle erstellt werden, die für die Ausführung Ihrer Regel erforderlich ist.
    - Um automatisch eine IAM-Rolle zu erstellen, wählen Sie Eine neue Rolle für diese spezifische Ressource erstellen.
    - Wenn Sie eine zuvor erstellte IAM-Rolle verwenden möchten, wählen Sie Use existing role (Vorhandene Rolle verwenden)
19. (Optional) Wählen Sie Add target (Ziel hinzufügen) aus, um ein weiteres Ziel für diese Regel hinzuzufügen.
20. (Optional) Geben Sie ein oder mehrere Tags für die Regel ein. Weitere Informationen finden Sie unter EventBridge Amazon-Tags.
21. Überprüfen Sie die eingerichteten Regeln, um sicherzustellen, dass sie den Anforderungen Ihrer Ereignisüberwachung entsprechen.
22. Wählen Sie Erstellen aus, um Ihre Auswahl zu bestätigen.

Amazon VPC-Endpoints AWS Config mit Interface verwenden

Wenn Sie Amazon Virtual Private Cloud (Amazon VPC) zum Hosten Ihrer AWS Ressourcen verwenden, können Sie eine private Verbindung zwischen Ihrer VPC und herstellen. AWS Config Sie können diese Verbindung verwenden, um über Ihre VPC mit AWS Config zu kommunizieren, ohne über das öffentliche Internet gehen zu müssen.

Amazon VPC ist ein AWS Service, mit dem Sie AWS Ressourcen in einem von Ihnen definierten virtuellen Netzwerk starten können. Mit einer VPC haben Sie die Kontrolle über Ihre Netzwerkeinstellungen, wie IP-Adressbereich, Subnetze, Routing-Tabellen und Netzwerk-Gateways. Schnittstelle, auf der VPC-Endpunkte basieren AWS PrivateLink, eine AWS Technologie, die private Kommunikation zwischen AWS Diensten über eine elastic network interface mit privaten IP-Adressen ermöglicht. Um Ihre VPC zu verbinden AWS Config, definieren Sie einen VPC-Schnittstellen-Endpunkt für. AWS Config Dieser Endpunkttyp ermöglicht es Ihnen, Ihre VPC mit AWS Diensten zu verbinden. Der Endpunkt bietet zuverlässige, skalierbare Konnektivität, AWS Config ohne dass ein Internet-Gateway, eine NAT-Instanz (Network Address Translation) oder eine VPN-Verbindung erforderlich ist. Weitere Informationen finden Sie unter Was ist Amazon VPC im Benutzerhandbuch zu Amazon VPC.

Die folgenden Schritte sind für Benutzer von Amazon VPC vorgesehen. Weitere Informationen finden Sie unter Erste Schritte im Amazon VPC Benutzerhandbuch.

Erstellen Sie einen VPC-Endpunkt für AWS Config

Um mit der Verwendung AWS Config mit Ihrer VPC zu beginnen, erstellen Sie einen VPC-Schnittstellen-Endpunkt für. AWS Config Sie müssen die Einstellungen für nicht ändern. AWS Config AWS Config ruft andere AWS Dienste über ihre öffentlichen Endpunkte an. Weitere Informationen finden Sie unter Erstellen eines Schnittstellenendpunkts im Amazon VPC Leitfaden.

Häufig gestellte Fragen

Meine letzten Konfigurationsänderungen können nicht angezeigt werden

Kann ich damit rechnen, dass ich meine Konfigurationsänderungen sofort sehe?

AWS Config zeichnet in der Regel Konfigurationsänderungen an Ihren Ressourcen auf, unmittelbar nachdem eine Änderung erkannt wurde, oder in der von Ihnen angegebenen Häufigkeit. Dies erfolgt jedoch nach bestem Wissen und kann manchmal länger dauern. Wenn die Probleme nach einiger Zeit weiterhin bestehen, wenden Sie sich an uns Supportund geben Sie Ihre von Amazon unterstützten AWS Config Messwerte an. CloudWatch Informationen zu diesen Kennzahlen finden Sie unter AWS Config Nutzungs- und Erfolgsmetriken.

Indirekte Beziehungen in AWS Config

Themen

- Was ist eine Ressourcenbeziehung?
- Was ist eine direkte und eine indirekte Beziehung in Bezug auf eine Ressource?
- Welche indirekten Beziehungen werden AWS Config unterstützt?
- In welchen Szenarien werden indirekte Beziehungen verwendet?
- Wie werden die Konfigurationselemente aufgrund der direkten und indirekten Beziehung erstellt?
- Welche Konfigurationselemente werden aufgrund indirekter Beziehungen generiert?
- Wie deaktiviere ich die indirekte Beziehung?
- Wie rufe ich Konfigurationsdaten ab, die sich auf indirekte Beziehungen beziehen?

Was ist eine Ressourcenbeziehung?

In beziehen sich Ressourcen auf Entitäten AWS, die verwaltbar sind, z. B. eine Amazon Elastic Compute Cloud (Amazon EC2) -Instance, einen AWS CloudFormation Stack oder einen Amazon S3 S3-Bucket. AWS Config ist ein Service, der Ressourcen verfolgt und überwacht, indem er Konfigurationselemente (CIs) erstellt, wann immer eine Änderung an einem aufgezeichneten

Ressourcentyp festgestellt wird, oder bei der von Ihnen festgelegten Aufzeichnungshäufigkeit. Wenn es beispielsweise für die Nachverfolgung von EC2 Amazon-Instances eingerichtet AWS Config ist, erstellt es jedes Mal, wenn eine Instance erstellt, aktualisiert oder gelöscht wird, ein Konfigurationselement. Jedes von erstellte Konfigurationselement AWS Config hat mehrere Felder`accountId`, darunter `arn` (Amazon-Ressourcenname)`awsRegion`,`configuration`,`tags`, und`relationships`. Das Beziehungsfeld eines CI AWS Config ermöglicht die Anzeige, wie Ressourcen miteinander verknüpft sind. Eine Beziehung kann beispielsweise darauf hinweisen, dass ein Amazon EBS-Volume mit ID an eine EC2 Amazon-Instance mit ID angehängt `vol-123ab45d` ist`i-a1b2c3d4`, die einer Sicherheitsgruppe `sg-ef678hk` zugeordnet ist.

Was ist eine direkte und eine indirekte Beziehung in Bezug auf eine Ressource?

AWS Config leitet die Beziehungen für die meisten Ressourcentypen aus dem Konfigurationsfeld ab, die als „direkte“ Beziehungen bezeichnet werden. Eine direkte Beziehung ist eine unidirektionale Verbindung (A→B) zwischen einer Ressource (A) und einer anderen Ressource (B), die typischerweise aus der Describe-API-Antwort der Ressource (A) abgerufen wird. In der Vergangenheit wurden für einige Ressourcentypen, die AWS Config ursprünglich unterstützt wurden, auch Beziehungen aus den Konfigurationen anderer Ressourcen erfasst, wodurch „indirekte“ Beziehungen geschaffen wurden, die bidirektional sind (B→A). Beispielsweise ist die Beziehung zwischen einer EC2 Amazon-Instance und ihrer Sicherheitsgruppe direkt, da die Sicherheitsgruppen in der Describe-API-Antwort für die EC2 Amazon-Instance enthalten sind. Andererseits ist die Beziehung zwischen einer Sicherheitsgruppe und einer EC2 Amazon-Instance indirekt, da die Beschreibung einer Sicherheitsgruppe keine Informationen über die Instances zurückgibt, mit denen sie verknüpft ist.

Indirekte Beziehungen können beispielsweise helfen, die folgenden Fragen zu beantworten:

- Welche EC2 Instanzen in privaten Subnetzen sind betroffen, wenn ein NAT-Gateway ausfällt?
- Bei welcher EC2 Instanz könnten Verbindungsprobleme auftreten, wenn eine Routing-Tabelle geändert wird?
- Welche Sicherheitsgruppe wurde nie verwendet?
- Welche sekundäre ENI, die an eine EC2 Instance angehängt ist, ist der Sicherheitsgruppe zugeordnet?

Wenn also eine Änderung der Ressourcenkonfiguration erkannt wird, wird AWS Config nicht nur ein CI für diese Ressource erstellt, sondern es wird auch CIs für alle zugehörigen Ressourcen generiert,

einschließlich solcher mit indirekten Beziehungen. Wenn beispielsweise Änderungen an einer EC2 Amazon-Instance AWS Config erkannt werden, erstellt es ein CI für die Instance und ein CI für die Sicherheitsgruppe, die der Instance zugeordnet ist.

Welche indirekten Beziehungen werden AWS Config unterstützt?

Die folgenden indirekten Ressourcenbeziehungen werden in unterstützt AWS Config.

Ressourcentyp	steht in indirektem Zusammenhang mit dem Ressourcentyp		
`AWS::EC2::RouteTable`	`AWS::EC2::Instance` , `AWS::EC2::NetworkInterface` , `AWS::EC2::Subnet` , `AWS::EC2::VPNGateway` , `AWS::EC2::VPC`		
`AWS::EC2::EIP`	`AWS::EC2::Instance` , `AWS::EC2::NetworkInterface`		
`AWS::EC2::Instance`	`AWS::EC2::SecurityGroup` , `AWS::EC2::Subnet` , `AWS::EC2::VPC`		
`AWS::EC2::NetworkInterface`	`AWS::EC2::SecurityGroup` , `AWS::EC2:`		

Ressourcentyp	steht in indirektem Zusammenhang mit dem Ressourcentyp		
	:Subnet , AWS::EC2::VPC		
AWS::EC2::NetworkACL	AWS::EC2::Subnet , AWS::EC2::VPC		
AWS::EC2::VPNConnection	AWS::EC2::VPNGateway , AWS::EC2::CustomerGateway		
AWS::EC2::InternetGateway	AWS::EC2::VPC		
AWS::EC2::SecurityGroup	AWS::EC2::VPC		
AWS::EC2::Subnet	AWS::EC2::VPC		
AWS::EC2::VPNGateway	AWS::EC2::VPC		

In welchen Szenarien werden indirekte Beziehungen verwendet?

Im Folgenden sind die AWS Dienste und die Funktionen des Dienstes aufgeführt, die eine indirekte Beziehung verwenden.

AWS Merkmal	Szenario
AWS Config verwaltete Regel	Die ec2- security-group-attached-to -eni-Regel prüft, ob nicht standardmäßige Sicherheitsgruppen an Elastic Network Interfaces (ENI) angehängt sind. Ohne eine indirekte Beziehung müssten Sie eine benutzerdefinierte Regel erstellen, um zu überprüfen, ob nicht standardmäßige Sicherheitsgruppen an eine ENI angehängt sind.
AWS Firewall Manager	Verwendung Die Audit Security Gruppenrichtlinie verwendet eine indirekte Beziehung, um zu ermitteln, wann eine Sicherheitsgruppe zuletzt verwendet wurde. Ohne eine indirekte Beziehung müssten Sie eine Sicherheitsgruppe erstellen und gleichzeitig neuen Ressourcen zuordnen, um zu verhindern, dass die Regel mit AWS Firewall Manager ausgelöst wird.

Standardressourcen	• Standardressourcen, wenn eine nicht standardmäßige VPC erstellt wird:
	  • Standardsicherheitsgruppe, Standard-Netzwerk-ACL und Standard-Routing-Tabelle.
	• Standardressourcen, wenn eine Standard-VPC erstellt wird:
	  • Alles, was mit einer nicht standardmäßigen VPC, einem Internet-Gateway und einem Standardsubnetz in jeder Availability Zone, auf die Sie Zugriff haben, erstellt wurde.
	• Die standardmäßige VPC-Erstellung erfolgt selbst, wenn ein Konto EC2 zum ersten Mal aufgerufen wird.

AWS Merkmal	Szenario
	• Standard-Subnetz, das für Konten in einer neu gestarteten Availability Zone erstellt wurde. Ohne eine indirekte Beziehung müssten Sie bis zu 12 Stunden warten, bis Anti-Entropy Änderungen an Standardressourcen aufzeichn et.

Wie werden die Konfigurationselemente aufgrund der direkten und indirekten Beziehung erstellt?

Bei einer direkten Beziehung zwischen Ressourcen (A→B) wird bei jeder Konfigurationsänderung an der Ressource B auch ein Konfigurationselement (CI) für die Ressource A initiiert. Ähnlich wird bei einer indirekten Beziehung (B→A), wenn eine Konfigurationsänderung an Ressource A vorgenommen wird, ein neues CI für Ressource B generiert. Beispielsweise ist die EC2 Amazon-Instance zur Sicherheitsgruppe eine direkte Beziehung, sodass jede Konfigurationsänderung an einer Sicherheitsgruppe sowohl ein CI für die Sicherheitsgruppe als auch ein CI für die EC2 Instance generieren würde. In ähnlicher Weise ist die Sicherheitsgruppe zur EC2 Amazon-Instance eine indirekte Beziehung, sodass jede Konfigurationsänderung an einer EC2 Instance sowohl ein CI für die EC2 Amazon-Instance als auch ein CI für die Sicherheitsgruppe generieren würde.

Welche Konfigurationselemente werden aufgrund indirekter Beziehungen generiert?

Im Folgenden sind die zusätzlichen Konfigurationselemente (CIs) aufgeführt, die aufgrund indirekter Ressourcenbeziehungen generiert wurden.

Konfigurationsände rungen an folgenden Ressourcentypen	wird CIs für die folgenden Ressource ntypen generiert		
`AWS::EC2::RouteTable`	`AWS::EC2::Instance`		

Konfigurationsänderungen an folgenden Ressourcentypen	wird CIs für die folgenden Ressourcentypen generiert		
	, AWS::EC2::NetworkInterface , AWS::EC2::Subnet , AWS::EC2::VPNGateway , und AWS::EC2::VPC		
AWS::EC2::EIP	AWS::EC2::Instance , AWS::EC2::NetworkInterface		
AWS::EC2::Instance	AWS::EC2::SecurityGroup , AWS::EC2::Subnet , AWS::EC2::VPC		
AWS::EC2::NetworkInterface	AWS::EC2::SecurityGroup , AWS::EC2::Subnet , AWS::EC2::VPC		
AWS::EC2::NetworkACL	AWS::EC2::Subnet , AWS::EC2::VPC		

Konfigurationsände rungen an folgenden Ressourcentypen	wird CIs für die folgenden Ressource ntypen generiert		
`AWS::EC2::VPNConnection`	`AWS::EC2::VPNGateway` , `AWS::EC2::CustomerGateway`		
`AWS::EC2::InternetGateway`	`AWS::EC2::VPC`		
`AWS::EC2::SecurityGroup`	`AWS::EC2::VPC`		
`AWS::EC2::Subnet`	`AWS::EC2::VPC`		
`AWS::EC2::VPNGateway`	`AWS::EC2::VPC`		

Wie deaktiviere ich die indirekte Beziehung?

Gehen Sie wie folgt vor, um die indirekte Beziehung zu deaktivieren:

1. Öffnen Sie einen AWS -Support Fall von Ihrem Konto oder vom Verwaltungskonto für mehrere Konten aus.
2. Wählen Sie Technisch als Supporttyp aus.
3. Wählen Sie für Service aus AWS Config.
4. Wählen Sie als Kategorie die Option Andere aus.
5. Wählen Sie den entsprechenden Schweregrad aus.
6. Geben Sie in der Betreffzeile „Indirekte Beziehung deaktivieren“ ein.
7. In der Beschreibung:
   - Bestätigen Sie, dass Sie diese häufig gestellten Fragen gelesen haben und fortfahren möchten.

- Geben Sie die Regionen an, in denen Sie die indirekte Beziehung deaktivieren möchten.
- Wenn Sie von einem Verwaltungskonto aus einreichen, geben Sie das Konto IDs und die zugehörigen Regionen an.
- Bei mehreren Konten können Sie eine CSV-Datei mit Konto IDs und Regionen anhängen.

Ein AWS -Support Techniker informiert Sie über die nächsten Schritte und informiert Sie über den aktuellen Status. Wir empfehlen Ihnen, eine Liste mit AWS Konten und Regionen zu führen, in denen indirekte Beziehungen deaktiviert sind. Reichen Sie für neue Konten einen neuen AWS -Support Fall ein, um die indirekte Beziehung zu deaktivieren.

Wie rufe ich Konfigurationsdaten ab, die sich auf indirekte Beziehungen beziehen?

Sie können SQL-Abfragen (Structured Query Language) in AWS Config Advanced Queries ausführen, um Konfigurationsdaten abzurufen, die sich auf indirekte Ressourcenbeziehungen beziehen. Wenn Sie beispielsweise die Liste der EC2 Amazon-Instances abrufen möchten, die sich auf eine Sicherheitsgruppe beziehen, verwenden Sie die folgende Abfrage:

```
SELECT
    resourceId,
    resourceType
    WHERE
    resourceType ='AWS::EC2::Instance'
    AND
    relationships.resourceId = 'sg-234213'
```

Codebeispiele für die AWS Config Verwendung AWS SDKs

Die folgenden Codebeispiele zeigen, wie die Verwendung AWS Config mit einem AWS Software Development Kit (SDK) funktioniert.

Aktionen sind Codeauszüge aus größeren Programmen und müssen im Kontext ausgeführt werden. Während Aktionen Ihnen zeigen, wie Sie einzelne Service-Funktionen aufrufen, können Sie Aktionen im Kontext der zugehörigen Szenarios anzeigen.

Eine vollständige Liste der AWS SDK-Entwicklerhandbücher und Codebeispiele finden Sie unterVerwendung AWS Config mit einem AWS SDK. Dieses Thema enthält auch Informationen zu den ersten Schritten und Details zu früheren SDK-Versionen.

Codebeispiele

- Grundlegende Beispiele für die AWS Config Verwendung AWS SDKs
  - Aktionen zur AWS Config Verwendung AWS SDKs
    - Verwendung DeleteConfigRule mit einem AWS SDK oder CLI
    - Verwendung von DescribeComplianceByConfigRule mit einer CLI
    - Verwendung von DescribeComplianceByResource mit einer CLI
    - Verwendung von DescribeConfigRuleEvaluationStatus mit einer CLI
    - Verwendung DescribeConfigRules mit einem AWS SDK oder CLI
    - Verwendung von DescribeConfigurationRecorderStatus mit einer CLI
    - Verwendung von DescribeConfigurationRecorders mit einer CLI
    - Verwendung von DescribeDeliveryChannels mit einer CLI
    - Verwendung von GetComplianceDetailsByConfigRule mit einer CLI
    - Verwendung von GetComplianceDetailsByResource mit einer CLI
    - Verwendung von GetComplianceSummaryByConfigRule mit einer CLI
    - Verwendung von GetComplianceSummaryByResourceType mit einer CLI
    - Verwendung PutConfigRule mit einem AWS SDK oder CLI
    - Verwendung von PutDeliveryChannel mit einer CLI

Grundlegende Beispiele für die AWS Config Verwendung AWS SDKs

Die folgenden Codebeispiele zeigen, wie die Grundlagen von AWS Config with verwendet AWS SDKs werden.

Beispiele

- Aktionen zur AWS Config Verwendung AWS SDKs
  - Verwendung DeleteConfigRule mit einem AWS SDK oder CLI
  - Verwendung von DescribeComplianceByConfigRule mit einer CLI
  - Verwendung von DescribeComplianceByResource mit einer CLI
  - Verwendung von DescribeConfigRuleEvaluationStatus mit einer CLI
  - Verwendung DescribeConfigRules mit einem AWS SDK oder CLI
  - Verwendung von DescribeConfigurationRecorderStatus mit einer CLI
  - Verwendung von DescribeConfigurationRecorders mit einer CLI
  - Verwendung von DescribeDeliveryChannels mit einer CLI
  - Verwendung von GetComplianceDetailsByConfigRule mit einer CLI
  - Verwendung von GetComplianceDetailsByResource mit einer CLI
  - Verwendung von GetComplianceSummaryByConfigRule mit einer CLI
  - Verwendung von GetComplianceSummaryByResourceType mit einer CLI
  - Verwendung PutConfigRule mit einem AWS SDK oder CLI
  - Verwendung von PutDeliveryChannel mit einer CLI

Aktionen zur AWS Config Verwendung AWS SDKs

Die folgenden Codebeispiele zeigen, wie Sie einzelne AWS Config Aktionen mit ausführen AWS SDKs. Jedes Beispiel enthält einen Link zu GitHub, wo Sie Anweisungen zum Einrichten und Ausführen des Codes finden.

Die folgenden Beispiele enthalten nur die am häufigsten verwendeten Aktionen. Eine vollständige Liste finden Sie in der AWS Config -API-Referenz.

Beispiele

- Verwendung DeleteConfigRule mit einem AWS SDK oder CLI

- Verwendung von DescribeComplianceByConfigRule mit einer CLI
- Verwendung von DescribeComplianceByResource mit einer CLI
- Verwendung von DescribeConfigRuleEvaluationStatus mit einer CLI
- Verwendung DescribeConfigRules mit einem AWS SDK oder CLI
- Verwendung von DescribeConfigurationRecorderStatus mit einer CLI
- Verwendung von DescribeConfigurationRecorders mit einer CLI
- Verwendung von DescribeDeliveryChannels mit einer CLI
- Verwendung von GetComplianceDetailsByConfigRule mit einer CLI
- Verwendung von GetComplianceDetailsByResource mit einer CLI
- Verwendung von GetComplianceSummaryByConfigRule mit einer CLI
- Verwendung von GetComplianceSummaryByResourceType mit einer CLI
- Verwendung PutConfigRule mit einem AWS SDK oder CLI
- Verwendung von PutDeliveryChannel mit einer CLI

Verwendung **`DeleteConfigRule`** mit einem AWS SDK oder CLI

Die folgenden Code-Beispiele zeigen, wie `DeleteConfigRule` verwendet wird.

CLI

AWS CLI

Um eine AWS Config-Regel zu löschen

Der folgende Befehl löscht eine AWS Config-Regel mit dem Namen`MyConfigRule`:

```
aws configservice delete-config-rule --config-rule-name MyConfigRule
```

- Einzelheiten zur API finden Sie DeleteConfigRulein der AWS CLI Befehlsreferenz.

Python

SDK für Python (Boto3)

> **Note**
>
> Es gibt noch mehr dazu GitHub. Hier finden Sie das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel- einrichten und ausführen.

```
class ConfigWrapper:
    """
    Encapsulates AWS Config functions.
    """

    def __init__(self, config_client):
        """
        :param config_client: A Boto3 AWS Config client.
        """
        self.config_client = config_client


    def delete_config_rule(self, rule_name):
        """
        Delete the specified rule.

        :param rule_name: The name of the rule to delete.
        """
        try:
            self.config_client.delete_config_rule(ConfigRuleName=rule_name)
            logger.info("Deleted rule %s.", rule_name)
        except ClientError:
            logger.exception("Couldn't delete rule %s.", rule_name)
            raise
```

- Einzelheiten zur API finden Sie DeleteConfigRulein AWS SDK for Python (Boto3) API Reference.

Eine vollständige Liste der AWS SDK-Entwicklerhandbücher und Codebeispiele finden Sie unter. Verwendung AWS Config mit einem AWS SDK Dieses Thema enthält auch Informationen zu den ersten Schritten und Details zu früheren SDK-Versionen.

Verwendung von **`DescribeComplianceByConfigRule`** mit einer CLI

Die folgenden Code-Beispiele zeigen, wie `DescribeComplianceByConfigRule` verwendet wird.

CLI

AWS CLI

Um Compliance-Informationen für Ihre AWS Config-Regeln zu erhalten

Der folgende Befehl gibt Konformitätsinformationen für jede AWS Config-Regel zurück, gegen die eine oder mehrere AWS Ressourcen verstoßen:

```
aws configservice describe-compliance-by-config-rule --compliance-
types NON_COMPLIANT
```

In der Ausgabe gibt der Wert für jedes `CappedCount` Attribut an, wie viele Ressourcen der zugehörigen Regel nicht entsprechen. Die folgende Ausgabe gibt beispielsweise an, dass 3 Ressourcen der genannten Regel nicht entsprechen`InstanceTypesAreT2micro`.

Ausgabe:

```
{
    "ComplianceByConfigRules": [
        {
            "Compliance": {
                "ComplianceContributorCount": {
                    "CappedCount": 3,
                    "CapExceeded": false
                },
                "ComplianceType": "NON_COMPLIANT"
            },
            "ConfigRuleName": "InstanceTypesAreT2micro"
        },
        {
            "Compliance": {
                "ComplianceContributorCount": {
                    "CappedCount": 10,
```

```
                    "CapExceeded": false
                },
                "ComplianceType": "NON_COMPLIANT"
            },
            "ConfigRuleName": "RequiredTagsForVolumes"
        }
    ]
}
```

- Einzelheiten zur API finden Sie DescribeComplianceByConfigRuleunter AWS CLI Befehlsreferenz.

PowerShell

Tools für PowerShell V4

Beispiel 1: In diesem Beispiel werden Konformitätsdetails für die Regel abgerufen ebs-optimized-instance, für die es keine aktuellen Bewertungsergebnisse für die Regel gibt. Daher wird INSUFFICIENT_DATA zurückgegeben

```
(Get-CFGComplianceByConfigRule -ConfigRuleName ebs-optimized-instance).Compliance
```

Ausgabe:

```
ComplianceContributorCount ComplianceType
-------------------------- --------------
                           INSUFFICIENT_DATA
```

Beispiel 2: Dieses Beispiel gibt die Anzahl der nicht konformen Ressourcen für die Regel ALB_HTTP_TO_HTTPS_REDIRECTION_CHECK zurück.

```
(Get-CFGComplianceByConfigRule -ConfigRuleName
 ALB_HTTP_TO_HTTPS_REDIRECTION_CHECK -ComplianceType
 NON_COMPLIANT).Compliance.ComplianceContributorCount
```

Ausgabe:

```
CapExceeded CappedCount
----------- -----------
```

```
False       2
```

- Einzelheiten AWS -Tools für PowerShell zur DescribeComplianceByConfigRuleAPI finden Sie unter Cmdlet-Referenz (V4).

Eine vollständige Liste der AWS SDK-Entwicklerhandbücher und Codebeispiele finden Sie unter. Verwendung AWS Config mit einem AWS SDK Dieses Thema enthält auch Informationen zu den ersten Schritten und Details zu früheren SDK-Versionen.

Verwendung von **`DescribeComplianceByResource`** mit einer CLI

Die folgenden Code-Beispiele zeigen, wie `DescribeComplianceByResource` verwendet wird.

CLI

AWS CLI

Um Compliance-Informationen für Ihre AWS Ressourcen zu erhalten

Der folgende Befehl gibt Konformitätsinformationen für jede EC2 Instanz zurück, die von AWS Config aufgezeichnet wurde und gegen eine oder mehrere Regeln verstößt:

```
aws configservice describe-compliance-by-resource --resource-
type AWS::EC2::Instance --compliance-types NON_COMPLIANT
```

In der Ausgabe gibt der Wert für jedes `CappedCount` Attribut an, gegen wie viele Regeln die Ressource verstößt. Die folgende Ausgabe gibt beispielsweise an, dass die Instanz `i-1a2b3c4d` gegen zwei Regeln verstößt.

Ausgabe:

```
{
    "ComplianceByResources": [
        {
            "ResourceType": "AWS::EC2::Instance",
            "ResourceId": "i-1a2b3c4d",
            "Compliance": {
                "ComplianceContributorCount": {
                    "CappedCount": 2,
                    "CapExceeded": false
                },
```

```
                "ComplianceType": "NON_COMPLIANT"
            }
        },
        {
            "ResourceType": "AWS::EC2::Instance",
            "ResourceId": "i-2a2b3c4d ",
            "Compliance": {
                "ComplianceContributorCount": {
                    "CappedCount": 3,
                    "CapExceeded": false
                },
                "ComplianceType": "NON_COMPLIANT"
            }
        }
    ]
}
```

- Einzelheiten zur API finden Sie DescribeComplianceByResourcein der AWS CLI Befehlsreferenz.

PowerShell

Tools für PowerShell V4

Beispiel 1: In diesem Beispiel wird der **`AWS::SSM::ManagedInstanceInventory`** Ressourcentyp auf den Konformitätstyp „COMPLIANT“ geprüft.

```
Get-CFGComplianceByResource -ComplianceType COMPLIANT -ResourceType
 AWS::SSM::ManagedInstanceInventory
```

Ausgabe:

```
Compliance                              ResourceId          ResourceType
----------                              ----------          ------------
Amazon.ConfigService.Model.Compliance i-0123bcf4b567890e3
 AWS::SSM::ManagedInstanceInventory
Amazon.ConfigService.Model.Compliance i-0a1234f6f5d6b78f7
 AWS::SSM::ManagedInstanceInventory
```

- Einzelheiten zur API finden Sie unter DescribeComplianceByResource AWS -Tools für PowerShellCmdlet-Referenz (V4).

Eine vollständige Liste der AWS SDK-Entwicklerhandbücher und Codebeispiele finden Sie unter. Verwendung AWS Config mit einem AWS SDK Dieses Thema enthält auch Informationen zu den ersten Schritten und Details zu früheren SDK-Versionen.

Verwendung von **`DescribeConfigRuleEvaluationStatus`** mit einer CLI

Die folgenden Code-Beispiele zeigen, wie `DescribeConfigRuleEvaluationStatus` verwendet wird.

CLI

AWS CLI

Um Statusinformationen für eine AWS Config-Regel abzurufen

Der folgende Befehl gibt die Statusinformationen für eine AWS Config-Regel mit dem Namen zurück`MyConfigRule`:

```
aws configservice describe-config-rule-evaluation-status --config-rule-
names MyConfigRule
```

Ausgabe:

```
{
    "ConfigRulesEvaluationStatus": [
        {
            "ConfigRuleArn": "arn:aws:config:us-east-1:123456789012:config-rule/
config-rule-abcdef",
            "FirstActivatedTime": 1450311703.844,
            "ConfigRuleId": "config-rule-abcdef",
            "LastSuccessfulInvocationTime": 1450314643.156,
            "ConfigRuleName": "MyConfigRule"
        }
    ]
}
```

- Einzelheiten zur API finden Sie DescribeConfigRuleEvaluationStatusunter AWS CLI Befehlsreferenz.

PowerShell

Tools für PowerShell V4

Beispiel 1: Dieses Beispiel gibt die Statusinformationen für die angegebenen Konfigurationsregeln zurück.

```
Get-CFGConfigRuleEvaluationStatus -ConfigRuleName root-account-mfa-enabled, vpc-
flow-logs-enabled
```

Ausgabe:

```
ConfigRuleArn                : arn:aws:config:eu-west-1:123456789012:config-rule/
config-rule-kvq1wk
ConfigRuleId                 : config-rule-kvq1wk
ConfigRuleName               : root-account-mfa-enabled
FirstActivatedTime           : 8/27/2019 8:05:17 AM
FirstEvaluationStarted       : True
LastErrorCode                :
LastErrorMessage             :
LastFailedEvaluationTime     : 1/1/0001 12:00:00 AM
LastFailedInvocationTime     : 1/1/0001 12:00:00 AM
LastSuccessfulEvaluationTime : 12/13/2019 8:12:03 AM
LastSuccessfulInvocationTime : 12/13/2019 8:12:03 AM

ConfigRuleArn                : arn:aws:config:eu-west-1:123456789012:config-rule/
config-rule-z1s23b
ConfigRuleId                 : config-rule-z1s23b
ConfigRuleName               : vpc-flow-logs-enabled
FirstActivatedTime           : 8/14/2019 6:23:44 AM
FirstEvaluationStarted       : True
LastErrorCode                :
LastErrorMessage             :
LastFailedEvaluationTime     : 1/1/0001 12:00:00 AM
LastFailedInvocationTime     : 1/1/0001 12:00:00 AM
LastSuccessfulEvaluationTime : 12/13/2019 7:12:01 AM
LastSuccessfulInvocationTime : 12/13/2019 7:12:01 AM
```

- Einzelheiten zur API finden Sie unter DescribeConfigRuleEvaluationStatus AWS -Tools für PowerShellCmdlet-Referenz (V4).

Eine vollständige Liste der AWS SDK-Entwicklerhandbücher und Codebeispiele finden Sie unter. Verwendung AWS Config mit einem AWS SDK Dieses Thema enthält auch Informationen zu den ersten Schritten und Details zu früheren SDK-Versionen.

Verwendung **`DescribeConfigRules`** mit einem AWS SDK oder CLI

Die folgenden Code-Beispiele zeigen, wie `DescribeConfigRules` verwendet wird.

CLI

AWS CLI

Um Details für eine AWS Config-Regel abzurufen

Der folgende Befehl gibt Details für eine AWS Config-Regel mit dem Namen zurück`InstanceTypesAreT2micro`:

```
aws configservice describe-config-rules --config-rule-
names InstanceTypesAreT2micro
```

Ausgabe:

```
{
    "ConfigRules": [
        {
            "ConfigRuleState": "ACTIVE",
            "Description": "Evaluates whether EC2 instances are the t2.micro
 type.",
            "ConfigRuleName": "InstanceTypesAreT2micro",
            "ConfigRuleArn": "arn:aws:config:us-east-1:123456789012:config-rule/
config-rule-abcdef",
            "Source": {
                "Owner": "CUSTOM_LAMBDA",
                "SourceIdentifier": "arn:aws:lambda:us-
east-1:123456789012:function:InstanceTypeCheck",
                "SourceDetails": [
                    {
                        "EventSource": "aws.config",
                        "MessageType": "ConfigurationItemChangeNotification"
                    }
                ]
            },
            "InputParameters": "{\"desiredInstanceType\":\"t2.micro\"}",
```

```
            "Scope": {
                "ComplianceResourceTypes": [
                    "AWS::EC2::Instance"
                ]
            },
            "ConfigRuleId": "config-rule-abcdef"
        }
    ]
}
```

- Einzelheiten zur API finden Sie DescribeConfigRulesin der AWS CLI Befehlsreferenz.

PowerShell

Tools für PowerShell V4

Beispiel 1: In diesem Beispiel werden die Konfigurationsregeln für das Konto mit ausgewählten Eigenschaften aufgeführt.

```
Get-CFGConfigRule | Select-Object ConfigRuleName, ConfigRuleId, ConfigRuleArn,
 ConfigRuleState
```

Ausgabe:

```
ConfigRuleName                                     ConfigRuleId
 ConfigRuleArn
 ConfigRuleState
--------------                                     ------------
 -------------
 ---------------
ALB_REDIRECTION_CHECK                              config-rule-12iyn3
 arn:aws:config-service:eu-west-1:123456789012:config-rule/config-rule-12iyn3
 ACTIVE
access-keys-rotated                                config-rule-aospfr
 arn:aws:config-service:eu-west-1:123456789012:config-rule/config-rule-aospfr
 ACTIVE
autoscaling-group-elb-healthcheck-required         config-rule-cn1f2x
 arn:aws:config-service:eu-west-1:123456789012:config-rule/config-rule-cn1f2x
 ACTIVE
```

- Einzelheiten zur API finden Sie unter DescribeConfigRules AWS -Tools für PowerShellCmdlet-Referenz (V4).

Python

SDK für Python (Boto3)

> **Note**
>
> Es gibt noch mehr dazu. GitHub Hier finden Sie das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel- einrichten und ausführen.

```
class ConfigWrapper:
    """
    Encapsulates AWS Config functions.
    """

    def __init__(self, config_client):
        """
        :param config_client: A Boto3 AWS Config client.
        """
        self.config_client = config_client


    def describe_config_rule(self, rule_name):
        """
        Gets data for the specified rule.

        :param rule_name: The name of the rule to retrieve.
        :return: The rule data.
        """
        try:
            response = self.config_client.describe_config_rules(
                ConfigRuleNames=[rule_name]
            )
            rule = response["ConfigRules"]
            logger.info("Got data for rule %s.", rule_name)
        except ClientError:
            logger.exception("Couldn't get data for rule %s.", rule_name)
            raise
        else:
            return rule
```

- Einzelheiten zur API finden Sie DescribeConfigRulesin AWS SDK for Python (Boto3) API Reference.

Eine vollständige Liste der AWS SDK-Entwicklerhandbücher und Codebeispiele finden Sie unter. Verwendung AWS Config mit einem AWS SDK Dieses Thema enthält auch Informationen zu den ersten Schritten und Details zu früheren SDK-Versionen.

Verwendung von **`DescribeConfigurationRecorderStatus`** mit einer CLI

Die folgenden Code-Beispiele zeigen, wie `DescribeConfigurationRecorderStatus` verwendet wird.

CLI

AWS CLI

Um Statusinformationen für den Konfigurationsrekorder abzurufen

Der folgende Befehl gibt den Status des Standardkonfigurationsrekorders zurück:

```
aws configservice describe-configuration-recorder-status
```

Ausgabe:

```
{
    "ConfigurationRecordersStatus": [
        {
            "name": "default",
            "lastStatus": "SUCCESS",
            "recording": true,
            "lastStatusChangeTime": 1452193834.344,
            "lastStartTime": 1441039997.819,
            "lastStopTime": 1441039992.835
        }
    ]
}
```

- Einzelheiten zur API finden Sie DescribeConfigurationRecorderStatusin der AWS CLI Befehlsreferenz.

PowerShell

Tools für PowerShell V4

Beispiel 1: Dieses Beispiel gibt den Status der Konfigurationsrekorder zurück.

```
Get-CFGConfigurationRecorderStatus
```

Ausgabe:

```
LastErrorCode        :
LastErrorMessage     :
LastStartTime        : 10/11/2019 10:13:51 AM
LastStatus           : Success
LastStatusChangeTime : 12/31/2019 6:14:12 AM
LastStopTime         : 10/11/2019 10:13:46 AM
Name                 : default
Recording            : True
```

- Einzelheiten zur API finden Sie unter DescribeConfigurationRecorderStatus AWS -Tools für PowerShellCmdlet-Referenz (V4).

Eine vollständige Liste der AWS SDK-Entwicklerhandbücher und Codebeispiele finden Sie unter. Verwendung AWS Config mit einem AWS SDK Dieses Thema enthält auch Informationen zu den ersten Schritten und Details zu früheren SDK-Versionen.

Verwendung von **`DescribeConfigurationRecorders`** mit einer CLI

Die folgenden Code-Beispiele zeigen, wie `DescribeConfigurationRecorders` verwendet wird.

CLI

AWS CLI

Um Details über den Konfigurationsrekorder zu erhalten

Der folgende Befehl gibt Details zum Standardkonfigurationsrekorder zurück:

```
aws configservice describe-configuration-recorders
```

Ausgabe:

```
{
    "ConfigurationRecorders": [
        {
            "recordingGroup": {
                "allSupported": true,
                "resourceTypes": [],
                "includeGlobalResourceTypes": true
            },
            "roleARN": "arn:aws:iam::123456789012:role/config-ConfigRole-
A1B2C3D4E5F6",
            "name": "default"
        }
    ]
}
```

- Einzelheiten zur API finden Sie DescribeConfigurationRecordersin der AWS CLI Befehlsreferenz.

PowerShell

Tools für PowerShell V4

Beispiel 1: Dieses Beispiel gibt die Details von Konfigurationsrekordern zurück.

```
Get-CFGConfigurationRecorder | Format-List
```

Ausgabe:

```
Name           : default
RecordingGroup : Amazon.ConfigService.Model.RecordingGroup
RoleARN        : arn:aws:iam::123456789012:role/aws-service-role/
config.amazonaws.com/AWSServiceRoleForConfig
```

- Einzelheiten zur API finden Sie unter DescribeConfigurationRecorders AWS -Tools für PowerShellCmdlet-Referenz (V4).

Eine vollständige Liste der AWS SDK-Entwicklerhandbücher und Codebeispiele finden Sie unter. Verwendung AWS Config mit einem AWS SDK Dieses Thema enthält auch Informationen zu den ersten Schritten und Details zu früheren SDK-Versionen.

Verwendung von **`DescribeDeliveryChannels`** mit einer CLI

Die folgenden Code-Beispiele zeigen, wie `DescribeDeliveryChannels` verwendet wird.

CLI

AWS CLI

Um Details über den Lieferkanal zu erhalten

Der folgende Befehl gibt Details zum Lieferkanal zurück:

```
aws configservice describe-delivery-channels
```

Ausgabe:

```
{
    "DeliveryChannels": [
        {
            "snsTopicARN": "arn:aws:sns:us-east-1:123456789012:config-topic",
            "name": "default",
            "s3BucketName": "config-bucket-123456789012"
        }
    ]
}
```

- Einzelheiten zur API finden Sie DescribeDeliveryChannelsin der AWS CLI Befehlsreferenz.

PowerShell

Tools für PowerShell V4

Beispiel 1: In diesem Beispiel wird der Lieferkanal für die Region abgerufen und Details angezeigt.

```
Get-CFGDeliveryChannel -Region eu-west-1 | Select-Object Name, S3BucketName,
 S3KeyPrefix,
 @{N="DeliveryFrequency";E={$_.ConfigSnapshotDeliveryProperties.DeliveryFrequency}}
```

Ausgabe:

```
Name    S3BucketName               S3KeyPrefix DeliveryFrequency
----    ------------               ----------- -----------------
default config-bucket-NA my          TwentyFour_Hours
```

- Einzelheiten zur API finden Sie unter DescribeDeliveryChannels AWS -Tools für PowerShellCmdlet-Referenz (V4).

Eine vollständige Liste der AWS SDK-Entwicklerhandbücher und Codebeispiele finden Sie unter. Verwendung AWS Config mit einem AWS SDK Dieses Thema enthält auch Informationen zu den ersten Schritten und Details zu früheren SDK-Versionen.

Verwendung von **`GetComplianceDetailsByConfigRule`** mit einer CLI

Die folgenden Code-Beispiele zeigen, wie `GetComplianceDetailsByConfigRule` verwendet wird.

CLI

AWS CLI

Um die Auswertungsergebnisse für eine AWS Config-Regel abzurufen

Der folgende Befehl gibt die Auswertungsergebnisse für alle Ressourcen zurück, die nicht einer AWS Config-Regel mit dem Namen entsprechen`InstanceTypesAreT2micro`:

```
aws configservice get-compliance-details-by-config-rule --config-rule-
name InstanceTypesAreT2micro --compliance-types NON_COMPLIANT
```

Ausgabe:

```
{
    "EvaluationResults": [
        {
            "EvaluationResultIdentifier": {
                "OrderingTimestamp": 1450314635.065,
                "EvaluationResultQualifier": {
                    "ResourceType": "AWS::EC2::Instance",
                    "ResourceId": "i-1a2b3c4d",
                    "ConfigRuleName": "InstanceTypesAreT2micro"
                }
```

```
            },
            "ResultRecordedTime": 1450314645.261,
            "ConfigRuleInvokedTime": 1450314642.948,
            "ComplianceType": "NON_COMPLIANT"
        },
        {
            "EvaluationResultIdentifier": {
                "OrderingTimestamp": 1450314635.065,
                "EvaluationResultQualifier": {
                    "ResourceType": "AWS::EC2::Instance",
                    "ResourceId": "i-2a2b3c4d",
                    "ConfigRuleName": "InstanceTypesAreT2micro"
                }
            },
            "ResultRecordedTime": 1450314645.18,
            "ConfigRuleInvokedTime": 1450314642.902,
            "ComplianceType": "NON_COMPLIANT"
        },
        {
            "EvaluationResultIdentifier": {
                "OrderingTimestamp": 1450314635.065,
                "EvaluationResultQualifier": {
                    "ResourceType": "AWS::EC2::Instance",
                    "ResourceId": "i-3a2b3c4d",
                    "ConfigRuleName": "InstanceTypesAreT2micro"
                }
            },
            "ResultRecordedTime": 1450314643.346,
            "ConfigRuleInvokedTime": 1450314643.124,
            "ComplianceType": "NON_COMPLIANT"
        }
    ]
}
```

- Einzelheiten zur API finden Sie GetComplianceDetailsByConfigRuleunter AWS CLI Befehlsreferenz.

PowerShell

Tools für PowerShell V4

Beispiel 1: In diesem Beispiel werden die Auswertungsergebnisse für die Regel abgerufen access-keys-rotated und die Ausgabe nach Konformitätstyp gruppiert zurückgegeben

```
Get-CFGComplianceDetailsByConfigRule -ConfigRuleName access-keys-rotated | Group-
Object ComplianceType
```

Ausgabe:

```
Count Name                      Group
----- ----                      -----
    2 COMPLIANT                 {Amazon.ConfigService.Model.EvaluationResult,
 Amazon.ConfigService.Model.EvaluationResult}
    5 NON_COMPLIANT             {Amazon.ConfigService.Model.EvaluationResult,
 Amazon.ConfigService.Model.EvaluationResult,
 Amazon.ConfigService.Model.EvaluationRes...
```

Beispiel 2: In diesem Beispiel werden Konformitätsdetails für die Regel access-keys-rotated für COMPLIANT-Ressourcen abgefragt.

```
Get-CFGComplianceDetailsByConfigRule -ConfigRuleName access-
keys-rotated -ComplianceType COMPLIANT | ForEach-Object
 {$_.EvaluationResultIdentifier.EvaluationResultQualifier}
```

Ausgabe:

```
ConfigRuleName      ResourceId            ResourceType
--------------      ----------            ------------
access-keys-rotated BCAB1CDJ2LITAPVEW3JAH AWS::IAM::User
access-keys-rotated BCAB1CDJ2LITL3EHREM4Q AWS::IAM::User
```

- Einzelheiten zur API finden Sie unter GetComplianceDetailsByConfigRule AWS -Tools für PowerShellCmdlet-Referenz (V4).

Eine vollständige Liste der AWS SDK-Entwicklerhandbücher und Codebeispiele finden Sie unter. Verwendung AWS Config mit einem AWS SDK Dieses Thema enthält auch Informationen zu den ersten Schritten und Details zu früheren SDK-Versionen.

Verwendung von **`GetComplianceDetailsByResource`** mit einer CLI

Die folgenden Code-Beispiele zeigen, wie `GetComplianceDetailsByResource` verwendet wird.

CLI

AWS CLI

Um die Evaluierungsergebnisse für eine AWS Ressource zu erhalten

Der folgende Befehl gibt die Evaluierungsergebnisse für jede Regel zurück, der die EC2 Instanz `i-1a2b3c4d` nicht entspricht:

```
aws configservice get-compliance-details-by-resource --resource-
type AWS::EC2::Instance --resource-id i-1a2b3c4d --compliance-types NON_COMPLIANT
```

Ausgabe:

```
{
    "EvaluationResults": [
        {
            "EvaluationResultIdentifier": {
                "OrderingTimestamp": 1450314635.065,
                "EvaluationResultQualifier": {
                    "ResourceType": "AWS::EC2::Instance",
                    "ResourceId": "i-1a2b3c4d",
                    "ConfigRuleName": "InstanceTypesAreT2micro"
                }
            },
            "ResultRecordedTime": 1450314643.288,
            "ConfigRuleInvokedTime": 1450314643.034,
            "ComplianceType": "NON_COMPLIANT"
        },
        {
            "EvaluationResultIdentifier": {
                "OrderingTimestamp": 1450314635.065,
                "EvaluationResultQualifier": {
                    "ResourceType": "AWS::EC2::Instance",
                    "ResourceId": "i-1a2b3c4d",
                    "ConfigRuleName": "RequiredTagForEC2Instances"
                }
            },
            "ResultRecordedTime": 1450314645.261,
            "ConfigRuleInvokedTime": 1450314642.948,
            "ComplianceType": "NON_COMPLIANT"
        }
    ]
```

```
}
```

- Einzelheiten zur API finden Sie GetComplianceDetailsByResourceunter AWS CLI Befehlsreferenz.

PowerShell

Tools für PowerShell V4

Beispiel 1: Die Ergebnisse dieser Beispielauswertung für die angegebene Ressource.

```
Get-CFGComplianceDetailsByResource -ResourceId ABCD5STJ4EFGHIVEW6JAH -
ResourceType 'AWS::IAM::User'
```

Ausgabe:

```
Annotation                 :
ComplianceType             : COMPLIANT
ConfigRuleInvokedTime      : 8/25/2019 11:34:56 PM
EvaluationResultIdentifier :
 Amazon.ConfigService.Model.EvaluationResultIdentifier
ResultRecordedTime         : 8/25/2019 11:34:56 PM
ResultToken                :
```

- Einzelheiten zur API finden Sie unter GetComplianceDetailsByResource AWS -Tools für PowerShellCmdlet-Referenz (V4).

Eine vollständige Liste der AWS SDK-Entwicklerhandbücher und Codebeispiele finden Sie unter. Verwendung AWS Config mit einem AWS SDK Dieses Thema enthält auch Informationen zu den ersten Schritten und Details zu früheren SDK-Versionen.

Verwendung von **`GetComplianceSummaryByConfigRule`** mit einer CLI

Die folgenden Code-Beispiele zeigen, wie `GetComplianceSummaryByConfigRule` verwendet wird.

CLI

AWS CLI

Um die Konformitätsübersicht für Ihre AWS Config-Regeln abzurufen

Der folgende Befehl gibt die Anzahl der Regeln zurück, die konform sind, und die Anzahl der Regeln, die nicht konform sind:

```
aws configservice get-compliance-summary-by-config-rule
```

In der Ausgabe gibt der Wert für jedes `CappedCount` Attribut an, wie viele Regeln konform oder nicht konform sind.

Ausgabe:

```
{
    "ComplianceSummary": {
        "NonCompliantResourceCount": {
            "CappedCount": 3,
            "CapExceeded": false
        },
        "ComplianceSummaryTimestamp": 1452204131.493,
        "CompliantResourceCount": {
            "CappedCount": 2,
            "CapExceeded": false
        }
    }
}
```

- Einzelheiten zur API finden Sie unter GetComplianceSummaryByConfigRule AWS CLIBefehlsreferenz.

PowerShell

Tools für PowerShell V4

Beispiel 1: Dieses Beispiel gibt die Anzahl der Config-Regeln zurück, die nicht konform sind.

```
Get-CFGComplianceSummaryByConfigRule -Select
 ComplianceSummary.NonCompliantResourceCount
```

Ausgabe:

```
CapExceeded CappedCount
----------- -----------
```

```
False       9
```

- Einzelheiten zur API finden Sie unter GetComplianceSummaryByConfigRule AWS -Tools für PowerShellCmdlet-Referenz (V4).

Eine vollständige Liste der AWS SDK-Entwicklerhandbücher und Codebeispiele finden Sie unter. Verwendung AWS Config mit einem AWS SDK Dieses Thema enthält auch Informationen zu den ersten Schritten und Details zu früheren SDK-Versionen.

Verwendung von **`GetComplianceSummaryByResourceType`** mit einer CLI

Die folgenden Code-Beispiele zeigen, wie `GetComplianceSummaryByResourceType` verwendet wird.

CLI

AWS CLI

Um die Konformitätsübersicht für alle Ressourcentypen abzurufen

Der folgende Befehl gibt die Anzahl der AWS Ressourcen zurück, die nicht konform sind, und die Anzahl, die konform sind:

```
aws configservice get-compliance-summary-by-resource-type
```

In der Ausgabe gibt der Wert für jedes `CappedCount` Attribut an, wie viele Ressourcen konform oder nicht konform sind.

Ausgabe:

```
{
    "ComplianceSummariesByResourceType": [
        {
            "ComplianceSummary": {
                "NonCompliantResourceCount": {
                    "CappedCount": 16,
                    "CapExceeded": false
                },
                "ComplianceSummaryTimestamp": 1453237464.543,
                "CompliantResourceCount": {
```

```
                    "CappedCount": 10,
                    "CapExceeded": false
                }
            }
        }
    ]
}
```

Um die Konformitätsübersicht für einen bestimmten Ressourcentyp abzurufen

Der folgende Befehl gibt die Anzahl der EC2 Instanzen zurück, die nicht konform sind, und die Anzahl, die konform sind:

```
aws configservice get-compliance-summary-by-resource-type --resource-
types AWS::EC2::Instance
```

In der Ausgabe gibt der Wert für jedes `CappedCount` Attribut an, wie viele Ressourcen konform oder nicht konform sind.

Ausgabe:

```
{
    "ComplianceSummariesByResourceType": [
        {
            "ResourceType": "AWS::EC2::Instance",
            "ComplianceSummary": {
                "NonCompliantResourceCount": {
                    "CappedCount": 3,
                    "CapExceeded": false
                },
                "ComplianceSummaryTimestamp": 1452204923.518,
                "CompliantResourceCount": {
                    "CappedCount": 7,
                    "CapExceeded": false
                }
            }
        }
    ]
}
```

- Einzelheiten zur API finden Sie unter GetComplianceSummaryByResourceType AWS CLIBefehlsreferenz.

PowerShell

Tools für PowerShell V4

Beispiel 1: Dieses Beispiel gibt die Anzahl der Ressourcen zurück, die konform oder nicht konform sind, und konvertiert die Ausgabe in JSON.

```
Get-CFGComplianceSummaryByResourceType -Select
 ComplianceSummariesByResourceType.ComplianceSummary | ConvertTo-Json
{
  "ComplianceSummaryTimestamp": "2019-12-14T06:14:49.778Z",
  "CompliantResourceCount": {
    "CapExceeded": false,
    "CappedCount": 2
  },
  "NonCompliantResourceCount": {
    "CapExceeded": true,
    "CappedCount": 100
  }
}
```

- Einzelheiten zur API finden Sie unter GetComplianceSummaryByResourceType AWS -Tools für PowerShellCmdlet-Referenz (V4).

Eine vollständige Liste der AWS SDK-Entwicklerhandbücher und Codebeispiele finden Sie unter. Verwendung AWS Config mit einem AWS SDK Dieses Thema enthält auch Informationen zu den ersten Schritten und Details zu früheren SDK-Versionen.

Verwendung **`PutConfigRule`** mit einem AWS SDK oder CLI

Die folgenden Code-Beispiele zeigen, wie `PutConfigRule` verwendet wird.

CLI

AWS CLI

So fügen Sie eine AWS verwaltete Konfigurationsregel hinzu

Der folgende Befehl stellt JSON-Code zum Hinzufügen einer AWS verwalteten Konfigurationsregel bereit:

```
aws configservice put-config-rule --config-rule file://
RequiredTagsForEC2Instances.json
```

`RequiredTagsForEC2Instances.jsonist` eine JSON-Datei, die die Regelkonfiguration enthält:

```
{
  "ConfigRuleName": "RequiredTagsForEC2Instances",
  "Description": "Checks whether the CostCenter and Owner tags are applied to EC2
 instances.",
  "Scope": {
    "ComplianceResourceTypes": [
      "AWS::EC2::Instance"
    ]
  },
  "Source": {
    "Owner": "AWS",
    "SourceIdentifier": "REQUIRED_TAGS"
  },
  "InputParameters": "{\"tag1Key\":\"CostCenter\",\"tag2Key\":\"Owner\"}"
}
```

Für das `ComplianceResourceTypes` Attribut beschränkt dieser JSON-Code den Bereich auf Ressourcen des `AWS::EC2::Instance` Typs, sodass AWS Config nur EC2 Instanzen anhand der Regel auswertet. Da es sich bei der Regel um eine verwaltete Regel handelt, ist das `Owner` Attribut auf festgelegt`AWS`, und das `SourceIdentifier` Attribut ist auf den Regelbezeichner, festgelegt`REQUIRED_TAGS`. Für das `InputParameters` Attribut werden die Tag-Schlüssel, die die Regel benötigt`Owner`, `CostCenter` und, angegeben.

Wenn der Befehl erfolgreich ist, gibt AWS Config keine Ausgabe zurück. Um die Regelkonfiguration zu überprüfen, führen Sie den describe-config-rules Befehl aus und geben Sie den Regelnamen an.

So fügen Sie eine vom Kunden verwaltete Konfigurationsregel hinzu

Der folgende Befehl stellt JSON-Code zum Hinzufügen einer vom Kunden verwalteten Konfigurationsregel bereit:

```
aws configservice put-config-rule --config-rule file://
InstanceTypesAreT2micro.json
```

`InstanceTypesAreT2micro.json`ist eine JSON-Datei, die die Regelkonfiguration enthält:

```
{
  "ConfigRuleName": "InstanceTypesAreT2micro",
  "Description": "Evaluates whether EC2 instances are the t2.micro type.",
  "Scope": {
    "ComplianceResourceTypes": [
      "AWS::EC2::Instance"
    ]
  },
  "Source": {
    "Owner": "CUSTOM_LAMBDA",
    "SourceIdentifier": "arn:aws:lambda:us-
east-1:123456789012:function:InstanceTypeCheck",
    "SourceDetails": [
      {
        "EventSource": "aws.config",
        "MessageType": "ConfigurationItemChangeNotification"
      }
    ]
  },
  "InputParameters": "{\"desiredInstanceType\":\"t2.micro\"}"
}
```

Für das `ComplianceResourceTypes` Attribut beschränkt dieser JSON-Code den Bereich auf Ressourcen des `AWS::EC2::Instance` Typs, sodass AWS Config nur EC2 Instanzen anhand der Regel auswertet. Da es sich bei dieser Regel um eine vom Kunden verwaltete Regel handelt`CUSTOM_LAMBDA`, ist das `Owner` Attribut auf und das `SourceIdentifier` Attribut auf den ARN der AWS Lambda-Funktion gesetzt. Das `SourceDetails` Objekt ist erforderlich. Die für das `InputParameters` Attribut angegebenen Parameter werden an die AWS Lambda-Funktion übergeben, wenn AWS Config sie aufruft, um Ressourcen anhand der Regel auszuwerten.

Wenn der Befehl erfolgreich ist, gibt AWS Config keine Ausgabe zurück. Um die Regelkonfiguration zu überprüfen, führen Sie den describe-config-rules Befehl aus und geben Sie den Regelnamen an.

- Einzelheiten zur API finden Sie PutConfigRuleunter AWS CLI Befehlsreferenz.

Python

SDK für Python (Boto3)

> **Note**
>
> Es gibt noch mehr dazu GitHub. Hier finden Sie das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel- einrichten und ausführen.

```
class ConfigWrapper:
    """
    Encapsulates AWS Config functions.
    """

    def __init__(self, config_client):
        """
        :param config_client: A Boto3 AWS Config client.
        """
        self.config_client = config_client


    def put_config_rule(self, rule_name):
        """
        Sets a configuration rule that prohibits making Amazon S3 buckets
 publicly
        readable.

        :param rule_name: The name to give the rule.
        """
        try:
            self.config_client.put_config_rule(
                ConfigRule={
                    "ConfigRuleName": rule_name,
                    "Description": "S3 Public Read Prohibited Bucket Rule",
                    "Scope": {
                        "ComplianceResourceTypes": [
                            "AWS::S3::Bucket",
                        ],
                    },
                    "Source": {
                        "Owner": "AWS",
```

```
                        "SourceIdentifier": "S3_BUCKET_PUBLIC_READ_PROHIBITED",
                    },
                    "InputParameters": "{}",
                    "ConfigRuleState": "ACTIVE",
                }
            )
            logger.info("Created configuration rule %s.", rule_name)
        except ClientError:
            logger.exception("Couldn't create configuration rule %s.", rule_name)
            raise
```

- Einzelheiten zur API finden Sie PutConfigRulein AWS SDK for Python (Boto3) API Reference.

Eine vollständige Liste der AWS SDK-Entwicklerhandbücher und Codebeispiele finden Sie unter. Verwendung AWS Config mit einem AWS SDK Dieses Thema enthält auch Informationen zu den ersten Schritten und Details zu früheren SDK-Versionen.

Verwendung von **`PutDeliveryChannel`** mit einer CLI

Die folgenden Code-Beispiele zeigen, wie `PutDeliveryChannel` verwendet wird.

CLI

AWS CLI

Um einen Lieferkanal zu erstellen

Der folgende Befehl stellt die Einstellungen für den Lieferkanal als JSON-Code bereit:

```
aws configservice put-delivery-channel --delivery-channel file://
deliveryChannel.json
```

Die `deliveryChannel.json` Datei spezifiziert die Attribute des Lieferkanals:

```
{
    "name": "default",
    "s3BucketName": "config-bucket-123456789012",
    "snsTopicARN": "arn:aws:sns:us-east-1:123456789012:config-topic",
    "configSnapshotDeliveryProperties": {
```

```
        "deliveryFrequency": "Twelve_Hours"
    }
}
```

In diesem Beispiel werden die folgenden Attribute festgelegt:

`name`- Der Name des Lieferkanals. Standardmäßig weist AWS Config den Namen einem neuen Lieferkanal `default` zu. Sie können den Namen des Lieferkanals nicht mit dem Befehl aktualisieren. `put-delivery-channel` Die Schritte zum Ändern des Namens finden Sie unter Umbenennen des Lieferkanals. `s3BucketName` - Der Name des Amazon S3 S3-Buckets, für den AWS Config Konfigurations-Snapshots und Konfigurationsverlaufsdateien bereitstellt. Wenn Sie einen Bucket angeben, der zu einem anderen AWS Konto gehört, muss dieser Bucket über Richtlinien verfügen, die Config Zugriffsberechtigungen gewähren. AWS Weitere Informationen finden Sie unter Berechtigungen für den Amazon-S3-Bucket.

`snsTopicARN`— Der Amazon-Ressourcenname (ARN) des Amazon SNS-Themas, an das AWS Config Benachrichtigungen über Konfigurationsänderungen sendet. Wenn Sie ein Thema aus einem anderen Konto auswählen, muss das Thema über Richtlinien verfügen, die Config Zugriffsberechtigungen gewähren. AWS Weitere Informationen finden Sie unter Berechtigungen für das Amazon SNS SNS-Thema.

`configSnapshotDeliveryProperties`- Enthält das `deliveryFrequency` Attribut, das festlegt, wie oft AWS Config Konfigurations-Snapshots liefert und wie oft es Evaluierungen für periodische Config-Regeln aufruft.

Wenn der Befehl erfolgreich ist, gibt AWS Config keine Ausgabe zurück. Führen Sie den describe-delivery-channels Befehl aus, um die Einstellungen Ihres Lieferkanals zu überprüfen.

- Einzelheiten zur API finden Sie PutDeliveryChannelin der AWS CLI Befehlsreferenz.

PowerShell

Tools für PowerShell V4

Beispiel 1: In diesem Beispiel wird die DeliveryFrequency-Eigenschaft eines vorhandenen Lieferkanals geändert.

```
Write-CFGDeliveryChannel -ConfigSnapshotDeliveryProperties_DeliveryFrequency
 TwentyFour_Hours -DeliveryChannelName default -DeliveryChannel_S3BucketName
 amzn-s3-demo-bucket -DeliveryChannel_S3KeyPrefix my
```

- Einzelheiten zur API finden Sie unter PutDeliveryChannel AWS -Tools für PowerShellCmdlet-Referenz (V4).

Eine vollständige Liste der AWS SDK-Entwicklerhandbücher und Codebeispiele finden Sie unter. Verwendung AWS Config mit einem AWS SDK Dieses Thema enthält auch Informationen zu den ersten Schritten und Details zu früheren SDK-Versionen.

Dokumentverlauf

In der folgenden Tabelle werden die wichtigen Änderungen an der Dokumentation für AWS Config beschrieben. Um Benachrichtigungen über Aktualisierungen dieser Dokumentation zu erhalten, können Sie einen RSS-Feed abonnieren.

- API-Version: 2014-11-12
- Letzte Aktualisierung der Dokumentation: 17. Juni 2025

Änderung	Beschreibung	Datum
AWS Config unterstützt neue Ressourcentypen	Mit dieser Version können Sie Konfigurationsände rungen AWS Config an neuen Amazon Bedrock-Ressourcen typen aufzeichnen. Weitere Informationen finden Sie unter Unterstützte Ressourcentypen.	17. Juni 2025
AWS Config aktualisiert verwaltete Regeln	In dieser Version werden die folgenden verwalteten Regeln AWS Config unterstützt: • cloudfront-ssl-policy-check • cognito-identity-pool-unauth-Zugriffsprüfung • ec2- aktiviert enis-source-destination-check • elbv2- listener-encryption-in-transit • lambda-function-xray-enabled • msk-cluster-public-access-deaktiviert	13. Juni 2025

	• msk-connect-connector-logging-aktiviert • msk-unrestricted-access-check • aurora-mysql-cluster-audit-Protokollierung • redshift-cluster-multi-az-aktiviert • s3 -regelprüfung express-dir-bucket-lifecycle • ssm-automation-logging-enabled • ssm-automation-block-public-teilen	
Sicherheits-IAM-Update	Die `AWSConfigServiceRolePolicy` Richtlinie und die `AWS_ConfigRole` Richtlinie gewähren jetzt zusätzliche Berechtigungen für Amazon Bedrock. Weitere Informationen finden Sie unter AWS -verwaltete Richtlinien für AWS Config.	27. Mai 2025

AWS Config unterstützt neue Ressourcentypen	Mit dieser Version können Sie Konfigurationsände rungen AWS Config an neuen Ressourcentypen von Amazon App Integrations, Amazon Elastic Compute Cloud (Amazon EC2), Amazon Inspector, Amazon Macie, Amazon Route 53 Profiles, Amazon OpenSearc h Serverless, Amazon Simple Storage Service (Amazon S3) und Amazon SageMaker AI aufzeichnen. AWS Security Hub Weitere Informationen finden Sie unter Unterstützte Ressourcentypen.	30. April 2025
AWS Config aktualisiert verwaltete Regeln	AWS Config Unterstützt in dieser Version die folgende verwaltete Regel: redshift-serverless-default-db-name-check	22. April 2025
AWS Config aktualisiert verwaltete Regeln	AWS Config Unterstützt in dieser Version die folgende verwaltete Regel: redshift-serverless-default-admin-ch eck	17. April 2025

Sicherheits-IAM-Update	Die `AWSConfigServiceRolePolicy` Richtlinie und die `AWS_ConfigRole` Richtlinie gewähren jetzt zusätzliche Berechtigungen für AWS B2B Data Interchange Amazon Bedrock,, AWS Clean Rooms, AWS CodeConnections AWS Direct Connect, AWS Database Migration Service (AWS DMS), Amazon CloudWatch Logs, Amazon Macie, Amazon Managed Blockchain, Amazon Q Business, Route 53 Profiles, Amazon Simple Storage Service (Amazon S3), Amazon SageMaker AI AWS Security Hub, und AWS Systems Manager Incident Manager, AWS Systems Manager Incident Manager Kontakte und. AWS Systems Manager Weitere Informationen finden Sie unter AWS -verwaltete Richtlinien für AWS Config.	8. April 2025

AWS Config aktualisiert verwaltete Regeln	In dieser Version werden die folgenden verwalteten Regeln AWS Config unterstützt: • s3-bucket-tagged • ecr-repository-tagged • sagemaker-feature-group-tagged • sagemaker-domain-tagged • cognito-user-pool-tagged	1. April 2025

AWS Config aktualisiert verwaltete Regeln	In dieser Version werden die folgenden verwalteten Regeln AWS Config unterstützt: • nlb-cross-zone-load-Balancing aktiviert • redshift-serverless-publish-logs-zu-Cloud-Watch • rds-instance-subnet-igw-überprüfen • ec2- - spot-fleet-request-ct encryption-at-rest • redshift-serverless-workgroup-encryptedim Transit • redshift-serverless-workgroup-no-öffentlich zugänglich • redshift-serverless-namespace-cmk-Verschlüsselung • event-data-store-cmk-Verschlüsselung aktiviert • ecs-task-definition-network-mode-not-host • rds-proxy-tls-encryption • nlb-logging-enabled • redshift-audit-logging-enabled • s3- lifecycle-policy-check • sagemaker-image-tagged • redshift-cluster-parameter-group-markiert • ec2- dhcp-options-tagged • sagemaker-app-image-config-markiert	22. März 2025

- mariadb-publish-logs-to-Cloudwatch-Logs
- docdb-cluster-encrypted-in-Durchreise
- rds-sqlserver-encrypted-in-Transit
- ec2- traffic-mirror-session-tagged
- ec2- launch-template-tagged
- ec2- traffic-mirror-target-tagged
- transfer-certificate-tagged
- batch-managed-compute-env-compute-resources-tagged
- lightsail-disk-tagged
- transfer-profile-tagged
- amplify-app-tagged
- ec2- prefix-list-tagged
- amplify-branch-tagged
- transfer-agreement-tagged
- datasync-task-tagged
- transfer-workflow-tagged
- Sagemaker_Notebook instanz_Plattformversion
- ec2 traffic-mirror-filter-tagged
- aurora-mysql-cluster-audit-Protokollierung
- ssm-document-tagged
- transfer-connector-tagged

- rds-mariadb-instance-encryp tedim Transit
- iam-saml-provider-tagged
- ec2-Fleet-markiert
- iam-server-certificate-tagged
- iam-oidc-provider-tagged
- alb-listener-tagged
- glb-listener-tagged
- ec2-markiert network-i nsights-access-scope
- lightsail-certificate-tagged
- ec2- capacity-reservation- tagged
- ec2- markiert transit-g ateway-multicast-domain
- dms-endpoint-tagged
- ec2- carrier-gateway-tagged
- dms-replication-task-tagged
- ec2- client-vpn-endpoint- tagged
- lightsail-bucket-tagged
- ec2- Analyse mit Schlagwör tern network-insights-a ccess-scope
- nlb-listener-tagged
- ec2- network-insights-path- tagged

AWS Config aktualisiert verwaltete Regeln	In dieser Version werden die folgenden verwalteten Regeln AWS Config unterstützt: • docdb-cluster-encrypted-in-Transit • mariadb-publish-logs-to-Cloudwatch-Protokolle • aurora-mysql-cluster-audit-Protokollierung • rds-mariadb-instance-encryptedim Transit • rds-sqlserver-encrypted-in-im Transit • sagemaker-notebook-instance-platform-Ausführung • appstream-fleet-multi-az • apprunner-vpc-connector-multi-az • mq-broker-general-logging-aktiviert • mq-active-single-instance-broker-storage-type-efs • mq-active-broker-ldap-Authentifizierung • iottwinmaker-component-type-tagged	19. März 2025

AWS Config aktualisiert verwaltete Regeln	In dieser Version werden die folgenden verwalteten Regeln AWS Config unterstützt: • fsx-openzfs-deployment-type-überprüfen • fsx-ontap-deployment-type-überprüfen • fsx-windows-deployment-type-überprüfen • redshift-serverless-workgroup-routes-innerhalb von VPC	18. März 2025
AWS Config aktualisiert verwaltete Regeln	AWS Config Unterstützt in dieser Version die folgenden verwalteten Regeln: ec2- -ami instance-launched-with-allowed	11. März 2025

AWS Config aktualisiert verwaltete Regeln	In dieser Version werden die folgenden verwalteten Regeln AWS Config unterstützt: • connect-instance-logging-enabled • ecr-repository-cmk-encryption-aktiviert • elbv2- prüfen predefined-security-policy-ssl • glue-spark-job-supported-Ausführung • guardduty-runtime-monitoring-enabled • guardduty-ecs-protection-runtime-aktiviert • guardduty-ec2- protection-runtime-enabled • netfw-subnet-change-protection-aktiviert • rds-sql-server-logs-to-cloudwatch • sqs-queue-no-public-Zugriff • transfer-connector-logging-enabled	7. März 2025

Sicherheits-IAM-Update	Die `AWSConfigServiceRolePolicy` Richtlinie und die `AWS_ConfigRole` Richtlinie gewähren jetzt zusätzliche Berechtigungen für Amazon Elastic Compute Cloud (Amazon EC2). Weitere Informationen finden Sie unter AWS -verwaltete Richtlinien für AWS Config.	4. März 2025

AWS Config aktualisiert die verwalteten Regeln	In dieser Version werden die folgenden verwalteten Regeln AWS Config unterstützt: • athena-workgroup-description • amplify-app-tagged • sagemaker-app-image-config-markiert • elasticbeanstalk-application-version-description • amplify-branch-performance-mode-aktiviert • athena-workgroup-engine-version-automatisches Upgrade • sagemaker-image-description • devicefarm-instance-profile-tagged • transfer-workflow-description • ec2- traffic-mirror-session-tagged • appstream-fleet-in-vpc • transfer-agreement-tagged • ec2- traffic-mirror-target-description • transfer-agreement-description • athena-prepared-statement-description	8. Februar 2025

- batch-managed-compute-env-compute-resources-tagged
- codedeploy-deployment-group-auto-rollback-aktiviert
- batch-managed-compute-environment-using-launch-template
- ec2- prefix-list-tagged
- ec2- traffic-mirror-filter-tagged
- athena-workgroup-enforce-workgroup-Konfiguration
- transfer-certificate-tagged
- batch-compute-environment-managed
- lightsail-disk-tagged
- transfer-profile-tagged
- ec2- traffic-mirror-target-tagged
- appintegrations-event-integration-tagged
- datasync-task-tagged
- batch-compute-environment-enabled
- appconfig-configuration-profile-validators-nicht leer
- elasticbeanstalk-application-description
- codedeploy-deployment-group-outdated-Instanzen-aktualisieren
- ec2- launch-template-tagged

- fis-experiment-template-tagged
- ivs-channel-playback-authorization-aktiviert
- redshift-cluster-parameter-group-markiert
- ec2- traffic-mirror-filter-description
- appintegrations-event-integration-description
- athena-data-catalog-description
- fis-experiment-template-log-Konfiguration vorhanden
- amplify-app-description
- amplify-branch-tagged
- batch-job-queue-enabled
- elasticbeanstalk-environment-description
- amplify-app-branch-auto-löschung aktiviert
- appconfig-hosted-configuration-version-Beschreibung
- appconfig-freeform-profile-config-Speicher
- datasync-task-data-verification-aktiviert
- apprunner-service-observability-enabled
- transfer-certificate-description
- appconfig-deployment-strategy-replicate-zu-ssm

	• transfer-workflow-tagged • transfer-connector-tagged • ec2- traffic-mirror-session-description • customerprofiles-object-type-allow-Profilerstellung • sagemaker-image-tagged	
AWS Config unterstützt neue Ressourcentypen	Mit dieser Version können Sie Konfigurationsänderungen AWS Config an neuen Ressourcentypen von Amazon Simple Storage Service (Amazon S3) aufzeichnen. Weitere Informationen finden Sie unter Unterstützte Ressourcentypen.	6. Februar 2025
AWS Config unterstützt neue Ressourcentypen	Mit dieser Version können Sie Konfigurationsänderungen AWS Config an neuen Ressourcentypen von Amazon Simple Storage Service (Amazon S3) aufzeichnen. Weitere Informationen finden Sie unter Unterstützte Ressourcentypen.	29. Januar 2025

Sicherheits-IAM-Update	Die `AWSConfigServiceRolePolicy` Richtlinie und die `AWS_ConfigRole` Richtlinie gewähren jetzt zusätzliche Berechtigungen für AWS Clean Rooms Amazon Comprehend, Amazon Elastic Compute Cloud (Amazon EC2) AWS HealthOmics, Amazon Simple Storage Service (Amazon S3) und Amazon Simple Email Service (Amazon SES). Weitere Informationen finden Sie unter AWS -verwaltete Richtlinien für AWS Config.	16. Januar 2025

AWS Config aktualisiert die verwalteten Regeln	In dieser Version werden die folgenden verwalteten Regeln AWS Config unterstützt: • appmesh-mesh-deny-tcp-Weiterleitung • sagemaker-model-isolation-enabled • evidently-project-description • alb-internal-scheme-check • evidently-segment-description • appconfig-environment-description • apprunner-service-in-vpc • sagemaker-domain-in-vpc • nlb-internal-scheme-check • emr-security-configuration-encryption-ausruhen • apprunner-service-no-public-Zugang • sagemaker-model-in-vpc • appconfig-deployment-strategy-description • evidently-launch-description • iot-authorizer-token-signing-aktiviert	9. Januar 2025

AWS Config unterstützt neue Ressourcentypen	Mit dieser Version können Sie Konfigurationsände rungen AWS Config an neuen Amazon Elastic Compute Cloud (Amazon EC2) - Ressourcentypen aufzeichn en. Weitere Informationen finden Sie unter Unterstützte Ressourcentypen.	9. Januar 2025

AWS Config aktualisiert verwaltete Regeln	In dieser Version werden die folgenden verwalteten Regeln AWS Config unterstützt: • batch-job-queue-tagged • iottwinmaker-sync-job-tagged • codeguruprofiler-profiling-group-tagged • ivs-recording-configuration-tagged • iottwinmaker-entity-tagged • iottwinmaker-workspace-tagged • iottwinmaker-scene-tagged • acmpca-certificate-authority-tagged • appflow-flow-tagged • iotevents-detector-model-tagged • appmesh-virtual-node-logging-file-path-exists • apprunner-vpc-connector-tagged • apprunner-service-tagged • iotwireless-fuota-task-tagged • appmesh-virtual-node-backend-defaults-tls-on • codegururevieweer-repository-association-tagged • iotevents-input-tagged	8. Januar 2025

- appmesh-virtual-gateway-logging-file-path-exists
- batch-compute-environment-tagged
- batch-scheduling-policy-tagged
- customerprofiles-object-type-tagged
- emr-security-configuration-encryption-Transit
- iotwireless-service-profile-tagged
- ivs-playback-key-pair-markiert
- cassandra-keyspace-tagged
- iotevents-alarm-model-tagged
- appconfig-application-description
- appmesh-virtual-gateway-backend-Standard-TLS
- ivs-channel-tagged
- iotwireless-multicast-group-tagged

AWS Config unterstützt neue Ressourcentypen	Mit dieser Version können Sie Konfigurationsände rungen AWS Config an neuen Ressourcentypen Amazon Elastic Compute Cloud (Amazon EC2), Amazon Cognito und Amazon OpenSearch Service aufzeichnen. AWS Elemental MediaConnect Weitere Informationen finden Sie unter Unterstützte Ressourcentypen.	19. Dezember 2024
Sicherheits-IAM-Update	Die `AWSConfigServiceRolePolicy` Richtlinie gewährt jetzt zusätzliche Berechtig ungen für AWS Organizations. Weitere Informationen finden Sie unter AWS -verwaltete Richtlinien für AWS Config.	18. Dezember 2024

AWS Config unterstützt serviceverknüpfte Konfigurationsrekorder	AWS Config Unterstützt mit dieser Version serviceverknüpfte Konfigurationsrekorder. Sie aktivieren im unterstützten Dienst oder mit dem einen Recorder für serviceverknüpfte Konfigurationen AWS CLI, und der Rekorder zeichnet in Ihrem Namen die Ressourcentypen auf, die für den verknüpften Dienst benötigt werden. Sie können die Details eines serviceverknüpften Konfigurationsrekorders über die AWS Config Konsole oder anzeigen. AWS CLI Weitere Informationen finden Sie unter Arbeiten mit dem Konfigurationsrekorder.	27. November 2024

AWS Config aktualisiert verwaltete Regeln	In dieser Version werden die folgenden verwalteten Regeln AWS Config unterstützt: • appconfig-application-tagged • appconfig-configuration-profile-tagged • appconfig-environment-tagged • appconfig-extension-association-tagged • appmesh-gateway-route-tagged • appmesh-mesh-tagged • appmesh-route-tagged • appmesh-virtual-gateway-tagged • appmesh-virtual-node-tagged • appmesh-virtual-router-tagged • appmesh-virtual-service-tagged • evidently-launch-tagged • evidently-project-tagged • evidently-segment-tagged • frauddetector-entity-type-tagged • frauddetector-label-tagged • frauddetector-outcome-tagged	12. November 2024

- frauddetector-variable-tagged
- iotsitewise-asset-model-tagged
- iotsitewise-dashboard-tagged
- iotsitewise-gateway-tagged
- iotsitewise-portal-tagged
- iotsitewise-project-tagged

Sicherheits-IAM-Update	Die `AWSConfigServiceRolePolicy` Richtlinie und die `AWS_ConfigRole` Richtlinie gewähren jetzt zusätzliche Berechtigungen für AWS AppConfig, Amazon Connect AWS CloudTrail, Amazon, Amazon DevOps Guru DataZone, Identity Store AWS Glue,,, AWS IoT AWS IoT FleetWise AWS IoT Wireless, Amazon Interactive Video Service (Amazon IVS), Amazon CloudWatch Logs, Amazon CloudWatch Observability Access Manager AWS Payment Cryptography, Amazon Relational Database Service (Amazon RDS), Amazon Rekognition, Amazon Simple Storage Service (Amazon S3), Amazon EventBridge Scheduler und Amazon VPC Lattice. AWS Systems Manager Weitere Informationen finden Sie unter AWS -verwaltete Richtlinien für AWS Config.	8. November 2024
AWS Config aktualisiert die verwalteten Regeln	AWS Config Unterstützt in dieser Version die folgende verwaltete Regel: cognito-user-pool-advanced-security-enabled	6. November 2024

AWS Config aktualisiert verwaltete Regeln	In dieser Version werden die folgenden verwalteten Regeln AWS Config unterstützt: • active-mq-supported-version • rabbit-mq-supported-version • ec-2 vpn-connection-log ging-enabled • appsync-cache-ct-e ncryption-im Ruhezustand • appsync-cache-ct-e ncryptionauf der Durchreise • vpc-endpoint-enabled • efs-filesystem-ct-encrypted • redshift-cluster-subnet-gro up-Multi-Az • sns-topic-no-public-Zugang • rabbit-mq-supported-version • kms-key-policy-no-öffentlic her Zugang • rds-mysql-instance-encrypte dim Transit • rds-postgres-instance-encry ptedunterwegs • rds-sql-server-logszu-Cloud -Watch • ec2-2-prüfen launch-te mplate-imdsv	21. Oktober 2024

AWS Config unterstützt neue Konformitätspakete	AWS Config Unterstützt mit dieser Version die folgenden Konformitätspakete: • Bewährte Betriebspraktiken für PCI DSS 4.0 (ohne globale Ressourcentypen) • Bewährte betriebliche Verfahren für PCI DSS 4.0 (einschließlich globaler Ressourcentypen)	23. September 2024
Sicherheits-IAM-Update	Die `AWSConfigServiceRolePolicy` Richtlinie und die `AWS_ConfigRole` Richtlinie gewähren jetzt zusätzliche Berechtigungen für Amazon OpenSearch Service Severless, Amazon AppStream, AWS Backup, AWS CloudTrail, AWS Glue, EC2 Image Builder AWS IoT, Amazon Interactive Video Service (Amazon IVS),, AWS Elemental MediaConnect AWS Elemental MediaTailor AWS HealthOmics, und Amazon EventBridge Scheduler. Weitere Informationen finden Sie unter AWS -verwaltete Richtlinien für AWS Config.	16. September 2024

AWS Config aktualisiert verwaltete Regeln	In dieser Version werden die folgenden verwalteten Regeln AWS Config unterstützt: • ec2- resources-in-logically-air -gapped-vault • ebs-resources-in-logically-air-gapped-vault • aurora-resources-in-logically-air-gapped-vault • efs-resources-in-logically-air-gapped-vault • s3- resources-in-logically-air -Tresor mit Lücken • storagegateway-resources-in-logically-air-gapped-vault • virtualmachine-resources-in-logically-air-gapped-vault	3. September 2024
AWS Config unterstützt neue Konformitätspakete	AWS Config Unterstützt mit dieser Version die folgenden Konformitätspakete: • Bewährte Betriebspraktiken für FedRAMP (High Part 1) • Bewährte Betriebspraktiken für FedRAMP (High Part 2)	27. August 2024

AWS Config aktualisiert verwaltete Regeln	In dieser Version werden die folgenden verwalteten Regeln AWS Config unterstützt: • athena-workgroup-logging-enabled • codebuild-report-group-encrypted-im Ruhezustand • cognito-user-pool-advanced-sicherheitsaktiviert • datasync-task-logging-enabled • efs-automatic-backups-enabled • glue-job-logging-enabled • glue-ml-transform-encrypted-im Ruhezustand • kinesis-stream-backup-retention-überprüfen • rds-aurora-postgresql-logs-zu-Cloud-Uhr • rds-postgresql-logs-to-cloudwatch • workspaces-root-volume-encryption-aktiviert • workspaces-user-volume-encryption-aktiviert	22. Juli 2024

Sicherheits-IAM-Update	Die `AWSConfigServiceRolePolicy` Richtlinie und die `AWS_ConfigRole` Richtlinie gewähren jetzt zusätzliche Berechtigungen für Amazon Elastic File System (Amazon EFS), Amazon Redshift und AWS Systems Manager für SAP. Weitere Informationen finden Sie unter AWS - verwaltete Richtlinien für AWS Config.	17. Juni 2024
AWS Config aktualisiert verwaltete Regeln	In dieser Version werden die folgenden verwalteten Regeln AWS Config unterstützt: • cloudtrail-s3- bucket-public-access-prohibited • CloudTrail-S3- bucket-access-logging	8. Mai 2024
AWS Config aktualisiert verwaltete Regeln	In dieser Version wird die folgende verwaltete Regel AWS Config unterstützt: iam-external-access-analyzer-enabled	2. Mai 2024

AWS Config aktualisiert verwaltete Regeln	In dieser Version werden die folgenden verwalteten Regeln AWS Config unterstützt: • guardduty-malware-protection-enabled • guardduty-rds-protection-enabled • GuardDuty-S3-Schutz aktiviert • inspector-lambda-standard-scan-aktiviert	26. April 2024

AWS Config vereinfacht die Nutzungsanalyse mit Amazon CloudWatch	Mit dieser Version zeigen die CloudWatch Amazon-Metriken zur Überwachung der AWS Config Datennutzung nur die abrechnungsfähige Nutzung an. Das bedeutet, dass nicht abrechnungsfähige Nutzung nicht mehr sowohl in den an die Konsole ausgegebenen CloudWatch Amazon-Metriken als auch in der AWS Config Konsole AWS Config angezeigt wird. Auf diese Weise können Sie die AWS Config Einrichtung und Nutzung anhand von CloudWatch Amazon-Metriken überprüfen und die abrechnungsfähige Nutzung mit den damit verbundenen Kosten korrelieren. Weitere Informationen finden Sie unter AWS Config Nutzungs- und Erfolgsmetriken.	26. April 2024
AWS Config aktualisiert verwaltete Regeln	AWS Config Unterstützt in dieser Version die folgende verwaltete Regel: iam-server-certificate-expiration-check	23. April 2024

AWS Config aktualisiert verwaltete Regeln	In dieser Version werden die folgenden verwalteten Regeln AWS Config unterstützt: • vpc-sg-port-restriction-überprüfen • cloudtrail-all-write-s3- data-event-check • cloudtrail-all-read-s3- data-event-check	17. April 2024
AWS Config aktualisiert verwaltete Regeln	In dieser Version werden die folgenden verwalteten Regeln AWS Config unterstützt: • guardduty-eks-protection-audit-aktiviert • guardduty-eks-protection-runtime-aktiviert • guardduty-lambda-protection-enabled • inspector-ec2-Scan aktiviert • inspector-ecr-scan-enabled • inspector-lambda-code-scan-aktiviert • redshift-unrestricted-port-access	16. April 2024
AWS Config aktualisiert verwaltete Regeln	In dieser Version wird die folgende verwaltete Regel AWS Config unterstützt: efs-mount-target-public-accessible	20. März 2024

AWS Config aktualisiert verwaltete Regeln	In dieser Version werden die folgenden verwalteten Regeln AWS Config unterstützt: • dms-neptune-iam-authorization-aktiviert • dms-mongo-db-authentication-aktiviert • dms-redis-tls-enabled • dax-tls-endpoint-encryption • eks-cluster-secrets-encrypted • kinesis-firehose-delivery-stream-verschlüsselt • mq-cloudwatch-audit-log-aktiviert • mq-cloudwatch-audit-log-aktiviert • opensearch-primary-node-fault-Toleranz • sagemaker-endpoint-config-prod-Anzahl der Instanzen • service-catalog-shared-within-Organisation • transfer-family-server-no-ftp	26. Februar 2024

Sicherheits-IAM-Update	Die `AWSConfigServiceRolePolicy` Richtlinie und die `AWS_ConfigRole` Richtlinie gewähren jetzt zusätzliche Berechtigungen für Amazon Managed Service für Prometheus, Amazon CloudWatch, Amazon Cognito, Amazon, ElastiCache, AWS Identity and Access Management (IAM) FSx AWS Glue,,, Amazon Redshift Serverless AWS Lambda AWS RAM, Amazon SageMaker AI und Amazon Simple Notification Service (Amazon SNS). Weitere Informationen finden Sie unter AWS -verwaltete Richtlinien für AWS Config.	22. Februar 2024
AWS Config aktualisiert die verwalteten Regeln	In dieser Version wird die folgende verwaltete Regel AWS Config unterstützt: s3 bucket-cross-region-replication - enabled	12. Februar 2024

AWS Config unterstützt neue Ressourcentypen	Mit dieser Version können Sie Konfigurationsände rungen AWS Config an neuen Ressourcentypen wie Amazon CloudWatch Evidently AWS Identity and Access Management (IAM) AWS AppConfig, Amazon MemoryDB (MemoryDB), Amazon Managed Streaming for Apache Kafka (Amazon MSK), Amazon Redshift und neuen Ressourcentypen aufzeichnen. AWS Transfer Family Weitere Informationen finden Sie unter Unterstützte Ressourcentypen.	6. Februar 2024
AWS Config aktualisiert verwaltete Regeln	AWS Config Unterstützt in dieser Version die folgende verwaltete Regel: macie-auto-sensitive-data-discovery-check	29. Januar 2024

AWS Config unterstützt neue Ressourcentypen	Mit dieser Version können Sie Konfigurationsände rungen AWS Config an neuen Amazon AppStream , AWS Key Management Service (AWS KMS), Amazon Relational Database Service (Amazon RDS), Amazon Cognito, Amazon Elastic Compute Cloud (Amazon EC2), EC2 Image Builder,, , Amazon AWS Ground Station AWS Mainframe Modernization QuickSight, Amazon Redshift und AWS Systems Manager Ressource ntypen aufzeichnen. Weitere Informationen finden Sie unter Unterstützte Ressourcentypen.	3. Januar 2024

Die Service-Limits erhöhen sich für die maximale Anzahl von AWS Config Regeln pro Region und Konto	In dieser Version werden 1000 AWS Config Regeln pro AWS Region und Konto AWS Config unterstützt. Diese Erhöhung gilt für die Summe aller bereitgestellten Regeln, einschließlich AWS Config verwalteter Regeln, AWS Config benutzerdefinierter Regeln, AWS Config Konformitätspakete, AWS Security Hub Kontrollen, AWS Firewall Manager Richtlinien und AWS Backup Backup-Pläne, pro Region und Konto. Weitere Informationen finden Sie unter Service Limits .	19. Dezember 2023
AWS Config aktualisiert verwaltete Regeln	In dieser Version werden die folgenden verwalteten Regeln AWS Config unterstützt: • s-3 meets-restore-time-target • ebs-meets-restore-time-ziel • ec2- meets-restore-time-target • rds-meets-restore-time-ziel • efs-meets-restore-time-ziel • fsx-meets-restore-time-ziel • aurora-meets-restore-time-ziel • dynamodb-meets-restore-time-ziel	19. Dezember 2023

Sicherheits-IAM-Update	Die `AWSConfigServiceRolePolicy` Richtlinie und die `AWS_ConfigRole` Richtlinie gewähren jetzt zusätzliche Berechtigungen für AWS AppConfig Amazon Managed Service for Prometheus, AWS Database Migration Service (AWS DMS), (AWS Identity and Access Management) IAM, Amazon Managed Streaming for Apache Kafka (Amazon MSK), Amazon CloudWatch Logs und Amazon Simple Storage Service (Amazon S3). AWS Organizations Weitere Informationen finden Sie unter AWS -verwaltete Richtlinien für AWS Config.	05. Dezember 2023

Vorabversion: Abfrageprozessor für natürliche Sprache für erweiterte Abfragen	Mit dieser Version können Sie den Abfrageprozessor in natürlicher Sprache für erweiterte Abfragen verwenden, der Funktionen der generativen künstlichen Intelligenz (generative KI) verwendet, mit denen Sie Fragen in einfachem Englisch stellen und sie in ein ready-to-use Abfrageformat konvertieren können. Mit dem Prozessor für Abfragen in natürlicher Sprache können Sie Ihre AWS-Konto oder unternehmensweite Abfragen AWS durchführen. Weitere Informationen finden Sie unter Abfrageprozessor in natürlicher Sprache für erweiterte Abfragen.	26. November 2023

Regelmäßige Aufzeichnung	Mit dieser Version wird AWS Config die regelmäßige Aufzeichnung unterstützt. Die regelmäßige Aufzeichnung bietet Ihnen die Möglichkeit, die neuesten Konfigurationsänderungen für Ihre Ressourcen über einen festgelegten Zeitraum zu erfassen. Sie können jetzt die Standardfrequenz für den Konfigurations-Recorder auf Täglich festlegen, so dass Sie nur dann ein Konfigurationselement (CI) erhalten, das den neuesten Status Ihrer Ressourcen in den letzten 24 Stunden repräsentiert, wenn es sich von dem zuvor aufgezeichneten CI unterscheidet. Die AWS Config Konsole bietet außerdem eine neue Aufzeichnungsstrategie, mit der Sie auch die Aufzeichnungsfrequenz für bestimmte Ressourcentypen überschreiben oder bestimmte Ressourcentypen von der Aufzeichnung ausschließen können. Auf diese Weise können Sie Ihre Einstellungen an Ihre individuellen Anforderungen anpassen. Folgende Datentypen werden hinzugefügt:	26. November 2023

- RecordingMode
- RecordingModeOverride

Die folgenden Datentypen wurden aktualisiert:

- PutConfigurationRecorder
- ConfigurationRecorder
- BaseConfigurationItem
- ConfigurationItem

Die folgenden Seiten im Entwicklerhandbuch wurden aktualisiert:

- Ressourcen neu kodieren AWS
- Einrichtung AWS Config mit der AWS Config Konsole | Einrichtung mit einem Klick
- Einrichtung AWS Config mi t der AWS Config Konsole | Manuelle Einrichtung
- Einrichtung AWS Config mit der AWS CLI

Sicherheits-IAM-Update	Die `AWSConfigServiceRolePolicy` Richtlinie und die `AWS_ConfigRole` Richtlinie gewähren jetzt zusätzliche Berechtigungen für Amazon Cognito, Amazon Connect, Amazon EMR, AWS Ground Station, Amazon MemoryDB AWS Mainframe Modernization,, Amazon AWS Organizations QuickSight, Amazon Relational Database Service (Amazon RDS), Amazon Redshift, Amazon Route 53, und. AWS Service Catalog AWS Transfer Family Die `AWSConfigServiceRolePolicy` -Richtlinie und die `AWS_ConfigRole` -Richtlinie fügen jetzt auch Sicherheitskennungen (SID) für die Richtlinie `AWSConfigServiceRolePolicyStatementID` , `AWSConfigSLRLogStatementID` , `AWSConfigSLRLogEventStatementID` , `AWSConfigSLRApiGatewayStatementID` und `AWSConfigServiceRolePolicy` hinzu. Weitere Informationen finden Sie unter AWS -verwaltete Richtlinien für AWS Config.	17. November 2023

AWS Config aktualisiert die verwalteten Regeln	In dieser Version werden die folgenden verwalteten Regeln AWS Config unterstützt: • acm-pca-root-ca-deaktiviert • dynamodb-table-deletion-protection-aktiviert • ec2- aktiviert client-vpn-connection-log • eks-cluster-log-enabled • emr-block-public-access • fsx-windows-audit-log-konfiguriert • fsx-openzfs-copy-tags-aktiviert • fsx-lustre-copy-tagszu Backups • msk-enhanced-monitoring-enabled • mq-auto-minor-version-upgrade-fähig • neptune-cluster-multi-az-aktiviert • opensearch-update-check • nur s3- access-point-in-vpc • s3- -Blöcke access-point-public-access • s-3 bucket-mfa-delete-enabled	9. November 2023

AWS Config unterstützt neue Ressourcentypen	Mit dieser Version können Sie Konfigurationsände rungen AWS Config an neuen AWS Identity and Access Management (IAM), (), Amazon Connect AWS Network Manager, Amazon Elastic Compute Cloud AWS Private Certificate Authority (Amazon AWS Private CA), Amazon Elastic Container Service (Amazon ECS EC2),, AWS IoT AWS IoT TwinMaker , Amazon Managed Streaming for Apache Kafka Connect (Amazon MSK Connect) und AWS Ressourcen Explorer Ressourcentypen aufzeichn en. AWS App Mesh AWS Lambda Weitere Informationen finden Sie unter Unterstützte Ressourcentypen.	3. November 2023
AWS Config unterstützt neue Conformance Packs	Mit dieser Version wird das folgende Konformitätspaket AWS Config aktualisiert: Operational Best Practices for BNM T RMi	26. Oktober 2023

Compliance- und Bestands-Dashboards für Aggregatoren	Mit dieser Version werden der aggregierten Ansicht in der Konsole eine Compliance-Dashboard-Seite und eine Inventar-Dashboard-Seite AWS Config hinzugefügt. AWS Config Auf der Compliance-Dashboard-Seite können Sie automatisierte Dashboards mit Widgets aufrufen, die Erkenntnisse zur Ressourcen-Compliance in Ihrem Aggregator zusammenfassen, z. B. die 10 wichtigsten Ressourcentypen nach nicht konformen Ressourcen, die 10 wichtigsten Konformitätspakete auf Kontoebene nach nicht konformen Regeln usw. Auf der Bestands-Dashboard-Seite können Sie ein automatisiertes Dashboard mit Widgets aufrufen, die Erkenntnisse zu den Ressourcenkonfigurationsdaten in Ihrem Aggregator zusammenfassen, z. B. die 10 wichtigsten Ressourcentypen nach Ressourcenanzahl, die 10 wichtigsten Konten nach Ressourcenanzahl usw.	23. Oktober 2023

	Informationen zur Grafik und den Diagrammen finden Sie unter Compliance-Dashboard und Bestands-Dashboard.	
Sicherheits-IAM-Update	Die `AWSConfigServiceRolePolicy` Richtlinie und die `AWS_ConfigRole` Richtlinie gewähren nun zusätzliche Berechtigungen für AWS Private CA,, Amazon Connect AWS App Mesh, Amazon Elastic Container Service (Amazon ECS), Amazon CloudWatch Evidly, Amazon Managed Grafana, Amazon, Amazon Inspector GuardDuty,, AWS IoT AWS IoT TwinMaker, Amazon Managed Streaming for Apache Kafka (Amazon MSK),, AWS Lambda AWS Network Manager AWS Organizations, und Amazon AI. SageMaker Weitere Informationen finden Sie unter AWS -verwaltete Richtlinien für AWS Config.	04. Oktober 2023

AWS Config unterstützt neue Ressourcentypen	Mit dieser Version können Sie Konfigurationsände rungen AWS Config an neuen Ressourcentypen AWS IoT,, AWS IoT TwinMaker AWS IoT Wireless, Amazon Personali ze Managed Streaming for Apache Kafka (Amazon MSK), Amazon SageMaker AI AWS CodeBuild, Amazon und Amazon AppStream Inspector aufzeichnen. Weitere Informationen finden Sie unter Unterstützte Ressourcentypen.	04. Oktober 2023

AWS Config aktualisiert die verwalteten Regeln	In dieser Version werden die folgenden verwalteten Regeln AWS Config unterstützt: • docdb-cluster-deletion-protection-aktiviert • docdb-cluster-audit-logging-aktiviert • docdb-cluster-snapshot-public-verboten • mq-active-deployment-mode • mq-rabbit-deployment-mode • dms-auto-minor-version-Upgrade-Check • dms-replication-task-targetdb-Protokollierung • dms-replication-task-sourcedb-Protokollierung • dms-endpoint-ssl-configured • custom-eventbus-policy-attached • global-endpoint-event-replication-aktiviert • Route 53- query-logging-enabled • rds-aurora-mysql-audit-Protokollierung aktiviert • rds-cluster-auto-minor-version-upgrade-enable • appsync-authorization-check • netfw-deletion-protection-enabled	21. September 2023

	• WAFv2- rulegroup-logging-enabled • msk-in-cluster-node-benötigen-TLS	
AWS Config unterstützt neue Konformitätspakete	Mit dieser Version werden die folgenden Konformitätspakete AWS Config aktualisiert: • Bewährte Methoden für die Ausführung von Amazon S3 • Bewährte betriebliche Verfahren für EC2	8. September 2023
Sicherheits-IAM-Update	Die Richtlinie `AWSConfigServiceRolePolicy` entfernt Berechtigungen für AWS Systems Manager (Systems Manager). Weitere Informationen finden Sie unter AWS -verwaltete Richtlinien für AWS Config.	6. September 2023
AWS Config unterstützt neue Ressourcentypen	Mit dieser Version können Sie Konfigurationsänderungen AWS Config an neuen Amazon CodeGuru Profiler,, Amazon Managed Service for Prometheus AWS Elemental MediaConnect AWS Transfer Family, AWS Batch AWS Cloud Map, und Amazon Route 53 Resolver Ressourcentypen aufzeichnen. Weitere Informationen finden Sie unter Unterstützte Ressourcentypen.	6. September 2023

AWS Config aktualisiert verwaltete Regeln	In dieser Version werden die folgenden verwalteten Regeln AWS Config unterstützt: • athena-workgroup-encrypted-at-ausruhen • neptune-cluster-iam-database-Authentifizierung • neptune-cluster-copy-tags-to-snapshot-enabled • neptune-cluster-cloudwatch-log-exportfähig • neptune-cluster-deletion-protection-aktiviert • neptune-cluster-snapshot-encrypted • neptune-cluster-backup-retention-überprüfen • neptune-cluster-encrypted • neptune-cluster-snapshot-public-verboten • docdb-cluster-backup-retention-überprüfen • docdb-cluster-encrypted • rds-cluster-encrypted-at-ausruhen	10. August 2023

AWS Config unterstützt neue Ressourcentypen	Mit dieser Version können Sie Konfigurationsände rungen AWS Config an neuen, Amazon,, Amazon Athena AWS Amplify AppIntegrations AWS App Mesh, Amazon Elastic Compute Cloud (Amazon EC2), Amazon CloudWatch Evidently, Amazon Forecast,,,, Amazon Managed Streaming for Apache Kafka (Amazon MSK), Amazon Personalize, Amazon Pinpoint und Ressource ntypen aufzeichnen. AWS IoT Greengrass Version 2 AWS Ground Station AWS Elemental MediaConvert AWS Elemental MediaTailor AWS Resilience Hub Weitere Informationen finden Sie unter Unterstützte Ressourcentypen.	3. August 2023

Sicherheits-IAM-Update	Die `AWSConfigServiceRolePolicy` Richtlinie und die `AWS_ConfigRole` Richtlinie gewähren jetzt zusätzliche Berechtigungen für Amazon Managed Workflows für AWS App Mesh Amazon AppStream 2.0, Amazon AWS CloudFormation, Amazon Connect CloudFront AWS CodeArtifact AWS CodeBuild, Amazon, AWS Identity and Access Management (IAM) AWS Glue GuardDuty, Amazon Inspector,, AWS IoT AWS IoT TwinMaker AWS IoT Wireless, Amazon Managed Streaming for Apache Kafka, Amazon Macie,,,, AWS Elemental MediaConnect AWS Network Manager, Amazon Route 53 AWS Organizations AWS Ressourcen Explorer, Amazon Simple Storage Service (Amazon S3), Amazon Simple Notification Service (Amazon SNS) und Amazon EC2 Systems Manager (SSM). Weitere Informationen finden Sie unter AWS -verwaltete Richtlinien für AWS Config.	28. Juli 2023

AWS Config unterstützt neue Ressourcentypen	Mit dieser Version können Sie Konfigurationsände rungen AWS Config an den neuen Ressourcentypen Amazon Kinesis, Amazon Elastic Compute Cloud (Amazon EC2), Amazon Pinpoint, Amazon Simple Storage Service (Amazon S3), Amazon Virtual Private Cloud (Amazon VPC), Amazon Kendra, Amazon Connect,, , AWS CloudFormation AWS AppConfig AWS App Mesh AWS App Runner, und AWS Database Migration Service (AWS DMS) aufzeichn en. Weitere Informationen finden Sie unter Unterstützte Ressourcentypen.	10. Juli 2023
Erhöhung der Service Limits für Konformitätspakete von Organisationen	Mit dieser Version werden 350 AWS Config Regeln pro Region und Konto in allen Conformance Packs und 350 Organisationsregeln pro Organisation AWS Config unterstützt. AWS Config Weitere Informationen finden Sie unter Service Limits .	13. Juni 2023

Sicherheits-IAM-Update	Die `AWSConfigServiceRolePolicy` Richtlinie und die `AWS_ConfigRole` Richtlinie gewähren jetzt zusätzliche Berechtigungen für Amazon Managed Workflows für AWS Amplify, Amazon Connect AWS App Mesh, Amazon Managed Service for Prometheus, Amazon Athena,,,, Amazon, AWS Batch, Amazon DynamoDB AWS CloudFormation AWS CloudTrail AWS CodeArtifact CodeGuru AWS Directory Service, Amazon Elastic Compute Cloud (Amazon), Amazon CloudWatch Evidly, Amazon Forecast,,,, (IAM EC2) AWS Organizations AWS IoT Greengrass AWS Ground Station, Amazon Managed Streaming for Apache Kafka AWS Identity and Access Management (Amazon MSK), Amazon Lightsail, Amazon Logs, CloudWatch AWS Elemental MediaConnect AWS Elemental MediaTailor, Amazon Pinpoint, Amazon Virtual Private Cloud (Amazon VPC), Amazon Personalize, Amazon QuickSight AWS Migration Hub Refactor Spaces, Amazon Simple Storage Service	13. Juni 2023

(Amazon S3), Amazon SageMaker AI und. AWS Transfer Family Weitere Informationen finden Sie unter AWS -verwaltete Richtlinien für AWS Config.

AWS Config Ausschlüsse nach Ressourcentyp aufzeichnen	Mit dieser Version AWS Config können Sie bestimmte AWS Ressourcentypen von der Inventarverfolgung und Compliance-Überwachung ausschließen und gleichzeitig alle anderen unterstützten Ressourcentypen verfolgen, die derzeit in verfügbar sind AWS Config, einschließlich derer, die in future hinzugefügt werden. Mit dieser Funktion können Sie sich auf wichtige Ressourcen konzentrieren, die Ihren Compliance- und Governance-Standards unterliegen. Die Aktualisierungen der API für den Konfigurationsrekorder und die Aufzeichnungsgruppe sind abwärtskompatibel, d. h. sie funktionieren mit früheren Versionen der PutConfigurationRecorderAPI. Sie können weiterhin genau wie zuvor verwalten, welche Ressourcentypen aufgezeichnet werden, ohne die aktualisierten oder neuen APIs zu verwenden. Folgende Datentypen werden hinzugefügt: • RecordingStrategy • ExclusionByResourceTypes	9. Juni 2023

Die folgenden Datentypen wurden aktualisiert:

- PutConfigurationRecorder
- ConfigurationRecorder
- RecordingGroup

Die folgende Seite im Entwicklerhandbuch wurde aktualisiert:

- Auswählen der aufzuzeichnenden Ressourcen

AWS Config unterstützt neue Ressourcentypen	Mit dieser Version können Sie Konfigurationsände rungen AWS Config an den neuen Ressourcentypen Amazon Elastic Container Service (Amazon ECS), Amazon Keyspaces (für Apache Cassandra) (Amazon Keyspaces),,, AWS Signer AWS Amplify, Amazon AppStream 2.0 AWS App Mesh AWS App Runner, Amazon Elastic Compute Cloud (Amazon EC2) AWS CodeArtifact, Amazon CloudWatch Evidly, Amazon Forecast, AWS Identity and Access Managemen t (IAM), Amazon Pinpoint, Amazon SageMaker AI AWS Transfer Family, Amazon Data Firehose aufzeichnen. Weitere Informationen finden Sie unter Unterstützte Ressourcentypen.	5. Juni 2023

AWS Config aktualisiert verwaltete Regeln	In dieser Version werden die folgenden verwalteten Regeln AWS Config unterstützt: • cloudfront-s3- origin-access-control-enabled • custom-schema-registry-policy-angehängt • ec2- -alle client-vpn-not-authorize • elasticache-supported-engine-version • macie-status-check • mq-automatic-minor-version-Upgrade aktiviert • mq-cloudwatch-audit-logging-aktiviert • netfw-logging-enabled • opensearch-encrypted-at-res • step-functions-state-machine-Protokollierung aktiviert	10. Mai 2023

AWS Config unterstützt neue Ressourcentypen	Mit dieser Version können Sie Konfigurationsände rungen AWS Config an neuen Amazon Elastic Compute Cloud (Amazon EC2) Amazon Route 53 Resolver, AWS IoT Wireless,,,, Amazon AWS Network Manager AWS Device Farm, Amazon Redshift AWS Ground Station AppFlow, Amazon Pinpoint,, EC2 Image Builder, Amazon AWS IoT, AWS AppConfig, Amazon SageMaker Runtime CloudWatch AWS Panorama, Amazon ECR und AWS Audit Manager Ressource ntypen aufzeichnen. Weitere Informationen finden Sie unter Unterstützte Ressourcentypen.	5. Mai 2023
AWS Config unterstützt neue Ressourcentypen	Mit dieser Version können Sie Konfigurationsänderungen AWS Config für aufzeichn en`AWS::NetworkFirewa ll::TLSInspectionC onfiguration` . Weitere Informationen finden Sie unter Unterstützte Ressourcentypen.	1. Mai 2023

Sicherheits-IAM-Update	Die `AWSConfigServiceRolePolicy` Richtlinie und die `AWS_ConfigRole` Richtlinie gewähren jetzt zusätzliche Berechtigungen für Amazon Managed Workflows für AWS Amplify AWS App Mesh, AWS App Runner, CloudFront AWS CodeArtifact, Amazon Elastic Compute Cloud, Amazon Kendra, Amazon Macie, Amazon Route 53, Amazon SageMaker AI, Amazon Pinpoint AWS Transfer Family,, AWS Resilience Hub AWS Migration Hub, Amazon CloudWatch, AWS Directory Service und. AWS WAF Weitere Informationen finden Sie unter AWS -verwaltete Richtlinien für AWS Config.	13. April 2023

AWS Config aktualisiert die verwalteten Regeln	In dieser Version werden die folgenden verwalteten Regeln AWS Config unterstützt: • elasticache-auto-minor-version-upgrade-check • elasticache-repl-grp-auto-failover-fähig • elasticache-repl-grp-encrypted-im Ruhezustand • elasticache-repl-grp-encryptedauf der Durchreise • elasticache-repl-grp-redis-auth-aktiviert • elasticache-subnet-group-check • Cloudfront-S3- origin-non-existent-bucket	10. April 2023
Erhöhung der Service Limits für Konformitätspakete von Organisationen	Mit dieser Version werden 350 AWS Config Regeln pro Konto in allen Konformitätspaketen der Organisation AWS Config unterstützt. Weitere Informationen finden Sie unter Service Limits .	03. April 2023

AWS Config aktualisiert verwaltete Regeln	In dieser Version werden die folgenden verwalteten Regeln AWS Config unterstützt: • acm-certificate-rsa-check • appsync-associated-with-waf • appsync-logging-enabled • elasticache-rbac-auth-enabled • mq-no-public-access • netfw-multi-az-enabled • ses-malware-scanning-enabled • eks-cluster-logging-enabled • appsync-cache-encryption-at-ausruhen	03. April 2023

AWS Config unterstützt neue Ressourcentypen	Mit dieser Version können Sie Konfigurationsänderungen AWS Config an den neuen Amazon AppStream 2.0-, AWS Auto Scaling-, Amazon Connect Amazon Elastic Compute Cloud-, Amazon-EventBridge HealthLak e, Kinesis-Videostreams, Lookout for Vision AWS IoT TwinMaker, Network Manager, Amazon Pinpoint, Amazon Application Recovery Controlle r (ARC) und AWS RoboMaker Ressourcentypen aufzeichn en. Weitere Informationen finden Sie unter Unterstützte Ressourcentypen.	03. April 2023

Sicherheits-IAM-Update	Die `AWSConfigServiceRolePolicy` Richtlinie und die `AWS_ConfigRole` Richtlinie gewähren jetzt zusätzliche Berechtigungen für Amazon Managed Workflows for Amazon AppFlow, Amazon AppStream 2.0 AWS App Runner, Amazon, Amazon AWS CloudFormation, CloudFront,, CloudWatch AWS CodeArtifact AWS CodeCommit AWS Device Farm, Amazon Elastic Compute Cloud (Amazon EC2), Amazon CloudWatch Evidently, Amazon Forecast, AWS Identity and Access Management (IAM) AWS Ground Station,, Amazon MemoryDB AWS IoT, Amazon Pinpoint,,, Amazon Relational Database Service (Amazon RDS), Amazon Redshift und Amazon AI. AWS Network Manager AWS Panorama SageMaker Weitere Informationen finden Sie unter AWS - verwaltete Richtlinien für AWS Config.	30. März 2023

Sicherheits-IAM-Update	Die Richtlinien `AWSConfigServiceRolePolicy` und `AWS_ConfigRole` gewähren jetzt zusätzliche Berechtigungen für AWS Audit Manager. Weitere Informationen finden Sie unter AWS - verwaltete Richtlinien für AWS Config.	03. März 2023
AWS Config unterstützt neue Ressourcentypen	Mit dieser Version können Sie Konfigurationsänderungen AWS Config an neuen AWS RoboMaker Ressourcentypen wie Amazon AWS Elemental MediaPackage, Amazon EventBridge AWS IoT, (Amazon Simple Storage Service (Amazon S3), Amazon Elastic Compute Cloud (Amazon EC2), Amazon Lookout for Metrics, Amazon Lex AWS Budgets, AWS Device Farm,, Amazon CodeGuru Reviewer und aufzeichnen. Amazon Route 53 Resolver Weitere Informationen finden Sie unter Unterstützte Ressourcentypen.	2. März 2023

Sicherheits-IAM-Update	AWS Config verfolgt jetzt Änderungen an der `AWSConfigMultiAccountSetupPolicy` Richtlinie. Weitere Informationen finden Sie unter AWS - verwaltete Richtlinien für AWS Config.	27. Februar 2023
AWS Config Ressource nabdeckung nach Regionen und Verfügbarkeit	In dieser Version werden Informationen AWS Config zur Region für jeden unterstützten Ressourcentyp bereitgestellt. Informationen darüber, welche Ressourcentypen in welchen Regionen unterstützt werden, finden Sie unter Ressource nabdeckung nach regionaler Verfügbarkeit.	20. Februar 2023

AWS Config unterstützt neue Ressourcentypen	Mit dieser Version können Sie Konfigurationsänderungen AWS Config an den neuen Ressourcentypen Amazon Interactive Video Service (Amazon IVS), Amazon Simple Storage Service (Amazon S3) AWS Glue, Amazon Elastic Kubernete s Service (Amazon EKS) AWS IoT, Amazon Relationa l Database Service (Amazon RDS) und Managed Service für Apache Flink aufzeichn en. Weitere Informationen finden Sie unter Unterstützte Ressourcentypen.	07. Februar 2023

Sicherheits-IAM-Update	Die `AWSConfigServiceRolePolicy` Richtlinie und die `AWS_ConfigRole` Richtlinie gewähren jetzt zusätzliche Berechtigungen für Amazon Managed Workflows for Apache Airflow AWS IoT, Amazon AppStream 2.0, Amazon CodeGuru Reviewer AWS HealthLake, Amazon Kinesis Video Streams, Amazon Application Recovery Controller (ARC) AWS Device Farm, Amazon Elastic Compute Cloud (Amazon EC2), Amazon Pinpoint AWS Identity and Access Management (IAM) GuardDuty, Amazon und Amazon Logs. CloudWatch Weitere Informationen finden Sie unter AWS -verwaltete Richtlinien für AWS Config.	1. Februar 2023
Sicherheits-IAM-Update	Als bewährte Sicherheitsmethode entfernt die Richtlinie `ConfigConformsServiceRolePolicy` nun umfassende Berechtigungen auf Ressourcenebene für `config:DescribeConfigRules` . Weitere Informationen finden Sie unter AWS -verwaltete Richtlinien für AWS Config.	12. Januar 2023

Sicherheits-IAM-Update	Die `AWSConfigServiceRolePolicy` Richtlinie und die `AWS_ConfigRole` Richtlinie gewähren jetzt zusätzliche Berechtigungen für Amazon Managed Service für Prometheus,, AWS Audit Manager AWS Device Farm, AWS Database Migration Service (AWS DMS) AWS Directory Service, Amazon Elastic Compute Cloud (Amazon EC2),, AWS Glue AWS IoT, Amazon Lightsail ,,, Amazon AWS Elemental MediaPackage AWS Network Manager QuickSight AWS Resource Access Manager, Amazon Application Recovery Controller (ARC), Amazon Simple Storage Service (Amazon S3) und Amazon Timestream. Weitere Informationen finden Sie unter AWS - verwaltete Richtlinien für AWS Config.	10. Januar 2023

AWS Config unterstützt neue Ressourcentypen	Mit dieser Version können Sie Konfigurationsände rungen AWS Config an neuen Amazon MQ,,, EventBrid ge Amazon-Schemas AWS AppConfig AWS Cloud9, Amazon Fraud Detector,,, Amazon Lightsail AWS IoT AWS IoT Analytics, AWS Elemental MediaPackage (MediaPackage), Amazon Application Recovery Controlle r (ARC) und Ressourcentypen aufzeichnen. AWS Resilience Hub AWS Transfer Family We itere Informationen finden Sie unter Unterstützte Ressource ntypen.	5. Januar 2023
AWS Config Regelmäßige Abdeckung der Ressourcen	In dieser Version wird der Umfang des Ressourcentyps für eine größere Anzahl AWS Config verwalteter Regeln AWS Config angezeigt.	21. Dezember 2022
AWS Config Auffindbarkeit von Regeln	In dieser Version werden Seiten für „Liste der AWS Config verwalteten Regeln nach Testmodus“, „Liste der AWS Config verwaltet en Regeln nach Triggertyp“ und „Liste der AWS Config verwalteten Regeln nach regionaler Verfügbarkeit“ AWS Config unterstützt.	21. Dezember 2022

AWS Config unterstützt neue Conformance Packs	Mit dieser Version werden die folgenden Konformitätspakete AWS Config aktualisiert: • Betriebliche bewährte Methoden für K-ISMS • Bewährte Methoden für die Ausführung von NIST 800 171 • Bewährte Methoden für die Ausführung von PCI DSS 3.2.1 • Bewährte Methoden für die Implementierung des Esquema Nacional de Seguridad (ENS) High • Bewährte Methoden für die Implementierung des Esquema Nacional de Seguridad (ENS) Medium • Bewährte Methoden für die Implementierung des Esquema Nacional de Seguridad (ENS) Low • Bewährte Methoden für die Ausführung von NZISM • Bewährte Methoden für die Ausführung von NIST 800-53 rev 5	19. Dezember 2022

AWS Config aktualisiert verwaltete Regeln	In dieser Version werden die folgenden verwalteten Regeln AWS Config unterstützt: • api-gwv2- access-logs-enabled • api-gwv2- authorization-type-configured • cloudfront-security-policy-check • ec2- deaktiviert launch-template-public-ip • elastic-beanstalk-logs-to-cloudwatch • sagemaker-notebook-instance-inside-vpc • sagemaker-notebook-instance-root-Zugriffsprüfung • security-account-information-provided • storagegateway-resources-protected-by-Backup-Plan • WAF 2- rulegroup-not-empty • WAF 2- webacl-not-empty	9. Dezember 2022

AWS Config unterstützt neue Ressourcentypen	Mit dieser Version können Sie Konfigurationsände rungen AWS Config an neuen Ressourcentypen Amazon CloudWatch RUM, Amazon EventBridge GuardDuty, Amazon Simple Email Service (Amazon SES) AWS Backup, AWS DataSync, und AWS Fault Injection Service (AWS FIS) aufzeichnen. Weitere Informationen finden Sie unter Unterstützte Ressourcentypen.	9. Dezember 2022

AWS Config Proaktive Einhaltung von Vorschriften	Mit dieser Version wird die Möglichkeit AWS Config unterstützt, vor der Bereitstellung von Ressourcen proaktiv die Einhaltung von AWS Config Regeln zu überprüfen. Auf diese Weise können Sie die Konfigurationseinstellungen Ihrer Ressourcen auswerten, bevor sie erstellt oder aktualisiert werden. Verwenden Sie diese Option AWS Config , um die an Ihren Ressourcen vorgenommenen Konfigurationsänderungen nachzuverfolgen, entweder vor oder nach der Bereitstellung, und um zu überprüfen, ob Ihre Ressourcen Ihren gewünschten Konfigurationen entsprechen. Folgende Datentypen werden hinzugefügt: • GetResourceEvaluationSummary • StartResourceEvaluation • ListResourceEvaluations Die folgenden Datentypen wurden aktualisiert: • DescribeConfigRulesFilters • GetComplianceDetailsByResource	28. November 2022

- EvaluationResultQualifier
- EvaluationModeConf iguration

Die folgenden Seiten im Entwicklerhandbuch wurden aktualisiert:

- Bestandteile einer Regel AWS Config
- Bewertungsmodus und Triggertypen für AWS Config Regeln
- AWS Config Verwaltete Regeln
- AWS Config -benutzerde finierte Regeln
- Verwaltung Ihrer AWS Config Regeln

Drift-Erkennung als Configuration Item (CI) für den AWS Config Configuration Recorder	In dieser Version werden alle Änderungen am Konfigurationsrekorder AWS Config nachverfolgt, um anzuzeigen, ob sich der Status des Konfigurationsrekorders von seinem vorherigen Status unterscheidet oder verändert hat, z. B. wenn Aktualisierungen von Ressourcentypen vorliegen, deren Nachverfolgung Sie aktiviert AWS Config haben, ob Sie den Konfigurationsrekorder gestoppt oder gestartet haben oder ob Sie den Konfigurationsrekorder gelöscht oder deinstalliert haben. Der `AWS::Config::ConfigurationRecorder` Ressourcentyp ist ein Systemressourcentyp von, AWS Config und die Aufzeichnung dieses Ressourcentyps ist standardmäßig in allen unterstützten Regionen aktiviert. Für die Aufzeichnung des Ressourcentyps `AWS::Config::ConfigurationRecorder` fallen keine zusätzlichen Kosten an. Weitere Informationen finden Sie unter Abweichungserkennung für den Konfigurations-Recorder.	18. November 2022

AWS Config unterstützt neue Ressourcentypen	Mit dieser Version können Sie Konfigurationsände rungen AWS Config an neuen Ressourcentypen AWS IoT Events, AWS Cloud Map, EC2 Image Builder, AWS DataSync AWS Glue, Amazon Application Recovery Controlle r (ARC) und Amazon Elastic Container Registry (Amazon ECR) aufzeichnen. Weitere Informationen finden Sie unter Unterstützte Ressourcentypen.	08. November 2022
Sicherheits-IAM-Update	Die Richtlinien `AWSConfigServiceRolePolicy` und `AWS_ConfigRole` gewähren jetzt zusätzliche Berechtigungen für AWS CloudFormation. Weitere Informationen finden Sie unter AWS -verwaltete Richtlinien für AWS Config.	7. November 2022

AWS Config unterstützt neue Conformance Packs	AWS Config Unterstützt mit dieser Version die folgenden Konformitätspakete: • Bewährte Methoden für die Ausführung von Criminal Justice Information Services (CJIS) • Bewährte Sicherheitsmethoden für Amazon SageMaker AI • Bewährte Methoden für die Sicherheit in Amazon Elastic Container Registry Die folgenden Konformitätspakete wurden aktualisiert: • Bewährte Methoden für die Ausführung von MAS TRMG • Bewährte Methoden für die Ausführung von NCSC Cyber Assesment Framework • Bewährte Methoden für die Ausführung von NCSC Cloud Security Principles	27. Oktober 2022

Sicherheits-IAM-Update	Die `AWSConfigServiceRolePolicy` Richtlinie und die `AWS_ConfigRole` Richtlinie gewähren jetzt zusätzliche Berechtigungen für AWS Certificate Manager Amazon Managed Workflows for Apache Airflow,, AWS Amplify AWS AppConfig, Amazon Keyspaces, Amazon, Amazon Connect CloudWatch AWS Glue DataBrew, Amazon Elastic Compute Cloud (Amazon EC2), Amazon Elastic Kubernetes Service (Amazon EKS), Amazon, Amazon Fraud Detector EventBridge AWS Fault Injection Service, Amazon, Amazon GameLift Servers FSx, Amazon Location Service,, Amazon Lex AWS IoT, Amazon Lightsail, Amazon Pinpoint,,,, Amazon AWS OpsWorks AWS Panorama AWS Resource Access Manager QuickSight, Amazon Relational Database Service (Amazon RDS), Amazon Rekognition,, AWS RoboMaker AWS Resource Groups, Amazon Route 53, Amazon Simple Storage Service (Amazon S3), und AWS Cloud Map. AWS Security Token Service	19. Oktober 2022

	Weitere Informationen finden Sie unter AWS -verwaltete Richtlinien für AWS Config.	
AWS Config unterstützt neue Ressourcentypen	Mit dieser Version können Sie Konfigurationsände rungen AWS Config an neuen Amazon Elastic Compute Cloud (Amazon EC2), Amazon Simple Email Service (Amazon SES), AWS AppConfig AWS Cloud Map, und AWS DataSync Ressourcentypen aufzeichn en. Weitere Informationen finden Sie unter Unterstützte Ressourcentypen.	6. Oktober 2022
AWS Config unterstützt neue Ressourcentypen	Mit dieser Version können Sie Konfigurationsände rungen AWS Config an neuen Amazon- GuardDuty , Amazon SageMaker AI-, AWS AppSync AWS Cloud Map, und AWS DataSync Ressourcentypen aufzeichn en. Weitere Informationen finden Sie unter Unterstützte Ressourcentypen.	4. Oktober 2022
AWS Config unterstützt das neue Conformance Pack	Mit dieser Version wird das Conformance Pack für betriebli che Best Practices für SWIFT CSP AWS Config aktualisiert.	4. Oktober 2022

AWS Config unterstützt neue Conformance Packs	AWS Config Unterstützt mit dieser Version die folgenden Konformitätspakete: • Bewährte Methoden für die Ausführung von CMMC 2.0 Level 1 • Bewährte Methoden für die Ausführung von CMMC 2.0 Level 2 Die folgenden Konformit ätspakete wurden aktualisiert: • Bewährte Methoden für die Ausführung von Amazon API Gateway • Operative Best Practices für die AWS Zuverläss igkeit eines gut konzipierten Frameworks • Bewährte betriebliche Verfahren für die AWS Sicherheitssäule eines Well-Architected Frameworks • Bewährte Methoden für die Ausführung von CMMC Level 1 • Bewährte Methoden für die Ausführung von CMMC Level 2 • Bewährte Methoden für die Ausführung von CMMC Level 3	30. September 2022

	• Bewährte Methoden für die Ausführung von CMMC Level 4 • Bewährte Methoden für die Ausführung von CMMC Level 5 • Betriebliche bewährte Methoden für FFIEC • Bewährte Methoden für die Ausführung von FedRAMP (Low) • Bewährte Methoden für die Ausführung von MAS Notice 655 • Bewährte Methoden für die Ausführung von NBC TRMG • Bewährte Methoden für die Ausführung von NIST 800 172	
Sicherheits-IAM-Update	Die Richtlinien `AWSConfigServiceRolePolicy` und `AWS_ConfigRole` gewähren jetzt zusätzliche Berechtigungen für AWS Glue. Weitere Informationen finden Sie unter AWS -verwaltete Richtlinien für AWS Config.	14. September 2022
AWS Config unterstützt das neue Konformitätspaket	AWS Config Unterstützt mit dieser Version das Konformitätspaket Operational Best Practices for SWIFT CSP.	09. September 2022

Sicherheits-IAM-Update	Die `AWSConfigServiceRolePolicy` Richtlinie und die `AWS_ConfigRole` Richtlinie gewähren jetzt zusätzliche Berechtigungen für Amazon AppFlow, Amazon, Amazon CloudWatch RUM CloudWatch, Amazon CloudWatch Synthetics, Amazon Connect-Kundenprofile, Amazon Connect Voice ID, Amazon DevOps Guru, Amazon Elastic Compute Cloud (Amazon EC2), Amazon EC2 Auto Scaling, Amazon EMR, Amazon, Amazon EventBridge Schemas EventBridge, Amazon Fraud Detector Amazon FinSpace, Amazon GameLift Servers, Amazon Interactive Video Service (Amazon IVS), Amazon Managed Service for Apache Flink, Image Builder EC2 , Amazon Lex, Amazon Lightsail, Amazon Location Service, Amazon Lookout for Equipment, Amazon Lookout for Metrics, Amazon Lookout for Vision, Amazon Managed Blockchain, Amazon MQ, Amazon Nimble StudioAmazon Pinpoint, Amazon QuickSight, Amazon Application Recovery Controller (ARC), Amazon Route 53 Resolver,	7. September 2022

	Amazon Simple Storage Service (Amazon S3), Amazon SimpleDB, Amazon Simple Email Service (Amazon SES), Amazon Timestream,,,,, AWS AppConfig AWS AppSync AWS Auto Scaling AWS Backup AWS Budgets AWS Cost Explorer AWS Cloud9 AWS Directory Service AWS DataSync AWS Elemental MediaPackage AWS Glue AWS IoT, AWS IoT Analytics AWS IoT Events, AWS IoT SiteWise, AWS IoT TwinMaker , AWS Lake Formation, AWS License Manager, AWS Resilience Hub AWS Signer, und AWS Transfer Family. Weitere Informationen finden Sie unter AWS -verwaltete Richtlinien für AWS Config.

AWS Config unterstützt neue Conformance Packs	AWS Config Unterstützt mit dieser Version die folgenden Konformitätspakete: • Bewährte Betriebspraktiken für Amazon CloudWatch • Bewährte Methoden für die Implementierung des deutschen Kriterienkatalogs C5 (Cloud Computing Compliance Controls Catalogue (C5)) • Bewährte Methoden für die Ausführung von IRS 1.075 Die folgenden Konformit ätspakete wurden aktualisiert: • AWS Control Tower Detective Guardrails Konformitätspaket • Bewährte Methoden für die Ausführung von CISA Cyber Essentials • Leitfaden zu bewährten betrieblichen Verfahren für die ENISA-Cybersicherheit für SMEs • Betriebliche bewährte Methoden für FDA Titel 21 CFR Teil 11 • Betriebliche bewährte Methoden für FedRAMP (Moderat)	31. August 2022

	• Betriebliche bewährte Methoden für die HIPAA-Sicherheit • Bewährte Methoden für die Ausführung von NIST Privacy Framework v1.0 • Bewährte Methoden für die Ausführung von NYDFS 23 • Bewährte betriebliche Verfahren für das RBI Cyber Security Framework für UCBs • Bewährte Methoden für die Ausführung von RBI MD-ITF	
Erste Schritte mit AWS Config und benutzerdefinierte Conformance Pack-Updates	Mit dieser Version werden die Seiten „Erste Schritte mit der Konsole“ AWS Config und „Einrichtung AWS Config mit der Konsole“ AWS Config aktualisiert und die Seite „Konfiguration mit einem Klick“ sowie die Seite „Manuelle Einrichtung“ eingeführt. AWS Config aktualisiert außerdem die Seite „Benutzerdefinierte s Conformance Pack“ mit einer Anleitung, wie Sie eine Conformance Pack-YAML -Datei von Grund auf neu erstellen.	25. August 2022

AWS Systems Manager Integration von Dokumenten (SSM-Dokument) mit Conformance Packs	Ab dieser Version können Sie eine Konformitätspaket-Vorlage mit einem SSM-Dokument erstellen. Weitere Informationen zu SSM-Dokumenten finden Sie unter AWS Systems Manager -Dokumente im Benutzerhandbuch für AWS Systems Manager . Die folgenden Datentypen wurden aktualisiert: • PutConformancePack • ConformancePackDetail • Einzelheiten zur Vorlage SSMDocument Die folgenden Seiten im Entwicklerhandbuch wurden aktualisiert: • Bereitstellen eines Conformance Packs mithilfe der Konsole AWS Config • Bereitstellen eines Conformance Packs über die AWS Befehlszeilenschnittstelle	24. August 2022

Sicherheits-IAM-Update	Die `AWSConfigServiceRolePolicy` Richtlinie und die `AWS_ConfigRole` Richtlinie gewähren jetzt zusätzliche Berechtigungen für Amazon Simple Email Service (Amazon SES) AWS DataSync, und AWS Cloud Map. Weitere Informationen finden Sie unter AWS -verwaltete Richtlinien für AWS Config.	22. August 2022
AWS Config unterstützt neue Ressourcentypen	Mit dieser Version können Sie Konfigurationsänderungen AWS Config an neuen Ressourcentypen von Amazon Athena, Amazon Detective, Amazon SageMaker AI, Amazon Route 53, AWS Database Migration Service (AWS DMS), AWS Glue, AWS Key Management Service (AWS KMS) und Amazon Simple Email Service (Amazon SES) aufzeichnen. Weitere Informationen finden Sie unter Unterstützte Ressourcentypen.	16. August 2022

AWS Config unterstützt neue Konformitätspakete	Mit dieser Version werden die folgenden Konformitätspakete AWS Config aktualisiert: • Bewährte Methoden für die Ausführung von NIST 1800 25 • Bewährte Methoden für die Ausführung von NIST 800 181 • Bewährte Methoden für den Betrieb von ABS CCIG 2.0 Standard Workloads • Bewährte Methoden für den Betrieb von ABS CCIG 2.0 Material Workloads • Bewährte Methoden für die Ausführung von ACSC Essential 8 • Bewährte Methoden für die Ausführung von ACSC ISM • Bewährte Methoden für die Ausführung von APRA CPG 234 • Bewährte betriebliche Verfahren für AWS GUS-Stiftungen — Benchmark v1.4, Stufe 1 • Bewährte betriebliche Verfahren für AWS GUS-Stiftungen Benchmark v1.4 Stufe 2 • Bewährte betriebliche Verfahren für BNM T RMi	1. August 2022

- Bewährte Methoden für die Ausführung von NIST CSF

Compliance-Wertung für Konformitätspakete	Mit dieser Version AWS Config wird ein Compliance-Score für Conformance Packs eingeführt, der Ihnen einen umfassenden Überblick über den Konformitätsstatus Ihrer Conformance Packs bietet. Sie können sie verwenden, um den Grad der Compliance in Ihren Konformitätspaketen zu ermitteln, zu untersuchen und nachzuvollziehen. Ein Konformitätspaket ist das Verhältnis (in Prozent) der Anzahl konformer Regel-Ressourcen-Kombinationen in einem Konformitätspaket zur Anzahl aller möglichen Regel-Ressourcen-Kombinationen in einem Konformitätspaket. Die folgenden Datentypen wurden aktualisiert: • ListConformancePackComplianceScores • ConformancePackComplianceScore Die folgenden Seiten im Entwicklerhandbuch wurden aktualisiert: • Das Dashboard anzeigen AWS Config	26. Juli 2022

	• Anzeigen von Compliance-Daten im Dashboard für Konformitätspakete • Verwalten von Konformitätspaketen (API)	
Sicherheits-IAM-Update	Die `ConfigConformsServiceRolePolicy` Richtlinie gewährt nun die Erlaubnis, metrische Datenpunkte auf Amazon zu veröffentlichen CloudWatch. Weitere Informationen finden Sie unter AWS -verwaltete Richtlinien für AWS Config.	25. Juli 2022

Sicherheits-IAM-Update	Die `AWSConfigServiceRolePolicy` Richtlinie und die `AWS_ConfigRole` Richtlinie gewähren jetzt zusätzliche Berechtigungen für Amazon Elastic Container Service (Amazon ECS), Amazon ElastiCache, Amazon EventBridge FSx, Amazon Managed Service für Apache Flink, Amazon Location Service, Amazon Managed Streaming for Apache Kafka, Amazon QuickSight, Amazon Rekognition, AWS RoboMaker , Amazon Simple Storage Service (Amazon S3), Amazon Simple Email Service (Amazon SES),,, AWS Amplify,, AWS AppConfig AWS AppSync AWS Billing Conductor AWS DataSync, AWS IAM Identity Center (IAM Identity Center) AWS Firewall Manager AWS Glue, EC2 Image Builder und Elastic Load Balancing. Weitere Informationen finden Sie unter AWS -verwaltete Richtlinien für AWS Config.	15. Juli 2022

AWS Config unterstützt neue Ressourcentypen	Mit dieser Version können Sie Konfigurationsände rungen AWS Config an neuen Amazon Elastic Compute Cloud (Amazon EC2) - Ressourcentypen aufzeichn en. Weitere Informationen finden Sie unter Unterstützte Ressourcentypen.	8. Juli 2022
AWS Config unterstützt einen neuen Ressourcentyp	Mit dieser Version können Sie Konfigurationsänderungen AWS Config an neuen AWS Global Accelerator Ressource ntypen aufzeichnen. Weitere Informationen finden Sie unter Unterstützte Ressourcentypen.	5. Juli 2022
AWS Config aktualisiert verwaltete Regeln	In dieser Version werden die folgenden verwalteten Regeln AWS Config unterstützt: • autoscaling-launch-template • ecs-task-definition-log-Kon figuration • ecs-awsvpc-networking-enabled	01. Juli 2022

AWS Config unterstützt neue Konformitätspakete	AWS Config Unterstützt mit dieser Version die folgenden Konformitätspakete: • Bewährte Methoden für die Implementierung des Canadian Centre for Cyber Security (CCCS)-Medium-Cloud-Kontrollprofils • Bewährte Methoden für die Implementierung des Gramm Leach Bliley Act (GLBA) • Bewährte Methoden für die Ausführung von Anhang 11 zum EG-Leitfaden der Guten Herstellungspraxis • Bewährte Methoden für die Sicherheit in Amazon Elastic Kubernetes Service (Amazon EKS) • Bewährte Methoden für die Sicherheit in Amazon Relational Database Service (Amazon RDS) • Bewährte Sicherheitsmethoden für AWS Lambda Die folgenden Konformitätspakete wurden aktualisiert: • Bewährte Methoden für die Ausführung von KI und ML	30. Juni 2022

	• Bewährte Methoden für die Ausführung von Amazon DynamoDB • Bewährte betriebliche Verfahren für kritische Sicherheitskontrollen der GUS v8 IG1 • Bewährte betriebliche Verfahren für kritische Sicherheitskontrollen der GUS v8 IG2 • Bewährte betriebliche Verfahren für kritische Sicherheitskontrollen der GUS v8 IG3 • Betriebliche bewährte Methoden für die HIPAA-Sicherheit • Bewährte Methoden für die Ausführung von NIST 800-53 rev 5 • Bewährte Methoden für die Ausführung von NIST CSF	
AWS Config unterstützt neue Ressourcentypen	Mit dieser Version können Sie Konfigurationsänderungen AWS Config an neuen Amazon SageMaker AI-Ressourcentypen aufzeichnen. Weitere Informationen finden Sie unter Unterstützte Ressourcentypen.	29. Juni 2022

AWS Config unterstützt neue Ressourcentypen	Mit dieser Version können Sie Konfigurationsände rungen AWS Config an den neuen Ressourcentypen Amazon Managed Streaming for Apache Kafka (Amazon MSK), Amazon Route 53, Amazon, WorkSpaces AWS Batch, AWS Identity and Access Managemen t Access Analyzer (IAM Access Analyzer), AWS Database Migration Service (AWS DMS) AWS Step Functions, und Elastic Load Balancing aufzeichn en. Weitere Informationen finden Sie unter Unterstützte Ressourcentypen.	14. Juni 2022

AWS Config aktualisiert die verwalteten Regeln	In dieser Version werden die folgenden verwalteten Regeln AWS Config unterstützt: • aurora-last-backup-recovery-punkt-erstellt • dynamodb-last-backup-recovery-punkt-erstellt • ebs-last-backup-recovery-punkt-erstellt • ec2- erstellt last-backup-recovery-point • efs-last-backup-recovery-punkt-erstellt • fsx-last-backup-recovery-punkt-erstellt • rds-last-backup-recovery-punkt-erstellt • s3- -erstellt last-backup-recovery-point • storagegateway-last-backup-recovery-punkt-erstellt • virtualmachine-last-backup-recovery-punkt-erstellt	13. Juni 2022

AWS Config Integration mit AWS Security Hub	In dieser Version können Sie sich die Ergebnisse der Evaluierungen AWS Config verwalteter und benutzerdefinierter Regeln als Ergebnisse in ansehen AWS Security Hub. Security Hub wandelt Regelausw ertungen in Erkenntnisse um, die mehr Informationen über die betroffenen Ressource n liefern, z. B. den Amazon-Ressourcennamen (ARN) und das Erstellungsdatum. Diese Erkenntnisse lassen sich zusammen mit anderen Ergebnissen von Security Hub aufrufen und bieten so einen umfassenden Überblick über Ihren Sicherhei tsstatus. Weitere Informati onen finden Sie unter Senden von Regelauswertungen an Security Hub.	7. Juni 2022

Sicherheits-IAM-Update	Die `AWSConfigServiceRolePolicy` Richtlinie und die `AWS_ConfigRole` Richtlinie gewähren jetzt zusätzliche Berechtigungen für Amazon Athena, Amazon Detective, Amazon GuardDuty, Amazon Macie, Amazon Simple Email Service (Amazon SES), AWS Glue, AWS Resource Access Manager (AWS RAM) und. AWS IAM Identity Center Weitere Informationen finden Sie unter AWS -verwaltete Richtlinien für AWS Config.	31. Mai 2022

AWS Config unterstützt neue Konformitätspakete	AWS Config Unterstützt mit dieser Version die folgenden Konformitätspakete: • Bewährte Methoden für die Sicherheit in Amazon Elastic Container Service (Amazon ECS) • Bewährte Methoden für die Sicherheit in Amazon Elastic File System (Amazon EFS) • Bewährte Sicherheitsmethoden für Amazon CloudFront • Bewährte Sicherheitsmethoden für AWS Auto Scaling • Bewährte Sicherheitsmethoden für AWS Network Firewall • Bewährte Sicherheitsmethoden für AWS Secrets Manager	31. Mai 2022
AWS Config unterstützt neue Ressourcentypen	Mit dieser Version können Sie Konfigurationsänderungen AWS Config an neuen Amazon SageMaker AI- und AWS Step Functions Ressourcentypen aufzeichnen. Weitere Informationen finden Sie unter Unterstützte Ressourcentypen.	26. Mai 2022

AWS Config unterstützt das neue Conformance Pack	Mit dieser Version werden die Operational Best Practices für das NERC CIP BCSI Conformance Pack AWS Config aktualisiert.	20. Mai 2022
Bestandteile einer Regel AWS Config	In dieser Version AWS Config wird eine Seite mit den Komponenten einer AWS Config Regel eingeführt. Auf dieser Seite werden die Struktur von Regeldefinitionen, Regelmetadaten und bewährte Methoden zum Schreiben von Regeln mit Python mithilfe des AWS Config Rules Developme nt Kit (RDK) und der AWS Config Rules Development Kit Library (RDKlib) beschrieben.	9. Mai 2022
Erhöhung der Service Limits für Konformitätspakete von Organisationen	Mit dieser Version werden 180 AWS Config Regeln pro Konto in allen Conformance Packs für Organisationen AWS Config unterstützt. Weitere Informationen finden Sie unter Service Limits .	6. Mai 2022

AWS Config unterstützt neue Conformance Packs	AWS Config Unterstützt mit dieser Version die folgenden Konformitätspakete: • Bewährte Sicherheitsmethoden für Amazon OpenSearch Service • Bewährte Methoden für die Sicherheit in Amazon Redshift • Bewährte Sicherheitsmethoden für AWS CloudTrail • Bewährte Sicherheitsmethoden für AWS CodeBuild • Bewährte Sicherheitsmethoden für AWS WAF	29. April 2022
AWS Config aktualisiert die verwaltete Regel	In dieser Version wird die verwaltete Regel mit dem resources-protected-by-backup S3-Plan AWS Config unterstützt.	11. April 2022

Sicherheits-IAM-Update	Die `AWSConfigServiceRolePolicy` Richtlinie und die `AWS_ConfigRole` Richtlinie gewähren jetzt zusätzliche Berechtigungen zum Abrufen von Informationen über alle oder einen bestimmten AWS CloudTrail Event Data Store (EDS), zum Abrufen von Informationen über alle oder eine bestimmte AWS CloudFormation Ressource, zum Abrufen einer Liste einer DynamoDB Accelerator (DAX) -Parametergruppe oder Subnetzgruppe, zum Abrufen von Informationen über AWS Database Migration Service (AWS DMS) Replikationsaufgaben für Ihr Konto in der aktuellen Region, auf die zugegriffen wird, und zum Abrufen einer Liste aller Richtlinien AWS Organizations eines bestimmten Typs. Weitere Informationen finden Sie unter AWS -verwaltete Richtlinien für AWS Config.	7. April 2022

AWS Config aktualisiert verwaltete Regeln	In dieser Version werden die folgenden verwalteten Regeln AWS Config unterstützt: • alb-desync-mode-check • autoscaling-capacity-rebalancing • autoscaling-launchconfig-requires-imdsv2 • autoscaling-launch-config-hop-Grenze • autoscaling-multiple-instance-types • clb-desync-mode-check • ecs-container-insights-enabled • ecs-fargate-latest-platform-Ausführung • netfw-policy-default-action-fragment-Pakete • netfw-policy-default-action-vollständige Pakete • netfw-policy-rule-group-assoziiert • redshift-audit-logging-enabled • s3- lifecycle-policy-check • waf-regional-rule-not-leer • waf-regional-rulegroup-not-leer • waf-regional-webacl-not-leer • vpc-peering-dns-resolution-überprüfen	4. April 2022

AWS Config Benutzerdefinierte Richtlinienregeln	Mit dieser Version AWS Config können Sie AWS Config benutzerdefinierte Richtlinienregeln mithilfe von AWS CloudFormation Guard (Guard) erstellen. Guard ist eine policy-as-code Sprache, mit der Sie Richtlinien schreiben können, die durchgesetzt werden, AWS Config ohne dass Sie Lambda-Funktionen zur Verwaltung Ihrer benutzerdefinierten Regeln erstellen müssen. Regeln, die mithilfe der Guard-Richtlinie geschrieben wurden, können über die AWS Config Konsole oder mithilfe der AWS Config Regel erstellt werden. APIs Die folgenden Seiten im Entwicklerhandbuch wurden aktualisiert: • AWS Config -benutzerdefinierte Regeln • AWS Config Benutzerdefinierte Regeln mit Guard erstellen Die folgenden Datentypen wurden aktualisiert: • Quelle • CustomPolicyDetails	4. April 2022

	• ConfigRuleEvaluationStatus • GetCustomRulePolicy • GetOrganizationCustomRulePolicy • OrganizationCustomPolicyRuleMetadata	
AWS Config unterstützt einen neuen Ressourcentyp	Mit dieser Version können Sie AWS Config Konfigurationsänderungen am neuen Amazon SecurityConfiguration EMR-Ressourcentyp aufzeichnen. Weitere Informationen finden Sie unter Unterstützte Ressourcentypen.	31. März 2022
AWS Config aktualisiert die verwaltete Regel	AWS Config Unterstützt in dieser Version die verwaltete Regel virtualmachine-resources-protected-by-backup-plan.	29. März 2022

AWS Config Integration mit Amazon CloudWatch Metrics	Mit dieser Version wird AWS Config jetzt die Nachverfolgung Ihrer AWS Config Nutzungs- und Erfolgsmetriken mit Amazon CloudWatch auf der AWS Config Dashboard-Seite unterstützt. CloudWatch metrics ist ein Monitoring-Service, der Daten über die Leistung Ihrer Systeme bereitstellt, einschließlich der Möglichkeit, nach Kennzahlen zu AWS Ressourcen zu suchen, sie grafisch darzustellen und Alarme zu erstellen. Im AWS Config Dashboard können Sie sehen, welcher Traffic Ihre AWS Config Nutzung beeinflusst, sowie wichtige Kennzahlen für Fehler, die in Ihrem Arbeitsablauf aufgetreten sind. Die folgende Seite wurde aktualisiert: • Das Dashboard anzeigen AWS Config	29. März 2022
AWS Config unterstützt einen neuen Ressourcentyp	Mit dieser Version können AWS Config Sie Konfigurationsänderungen am neuen Amazon GuardDuty Detector-Ressourcentyp aufzeichnen. Weitere Informationen finden Sie unter Unterstützte Ressourcentypen.	24. März 2022

AWS Config aktualisiert die verwalteten Regeln	In dieser Version werden die folgenden verwalteten Regeln AWS Config unterstützt: • clb-multiple-az • cloudfront-no-deprecated-ssl-Protokolle • cloudfront-traffic-to-origin-verschlüsselt • cloudwatch-alarm-action-enabled-überprüfen • ec2- no-amazon-key-pair • ec2- paravirtual-instance-check • ec2- token-hop-limit-check • ec2- -attach-deaktiviert transit-gateway-auto-vpc • ecr-private-lifecycle-policy-konfiguriert • efs-access-point-enforce-root-Verzeichnis • efs-access-point-enforce-Benutzeridentität • elbv2-multiple-az • kinesis-stream-encrypted • redshift-default-db-name-überprüfen • s3- event-notifications-enabled • sns-topic-message-delivery-Benachrichtigung aktiviert • waf-global-rulegroup-not-leer	23. März 2022

- waf-global-rule-not-leer

AWS Config unterstützt neue Konformitätspakete	Mit dieser Version werden die folgenden Konformitätspakete AWS Config aktualisiert: • Bewährte Methoden für den Betrieb von CIS Critical Security Controls v8 IG1 • Bewährte betriebliche Verfahren für kritische Sicherheitskontrollen der GUS v8 IG2 • Bewährte betriebliche Verfahren für kritische Sicherheitskontrollen der GUS v8 IG3 • Bewährte betriebliche Verfahren für die AWS Sicherheitssäule eines Well-Architected Frameworks • Bewährte Methoden für die Implementierung des Esquema Nacional de Seguridad (ENS) Low • Bewährte Methoden für die Implementierung des Esquema Nacional de Seguridad (ENS) Medium • Bewährte Methoden für die Implementierung des Esquema Nacional de Seguridad (ENS) High • Bewährte Methoden für die Ausführung von MAS Notice 655	16. März 2022

	• Bewährte Methoden für die Ausführung von NIST 1800-25	
Sicherheits-IAM-Update	Die Richtlinien `AWSConfigServiceRolePolicy` und `AWS_ConfigRole` gewähren jetzt zusätzliche Berechtigungen für AWS CloudFormation. Weitere Informationen finden Sie unter AWS -verwaltete Richtlinien für AWS Config.	14. März 2022
AWS Config aktualisiert verwaltete Regeln	Mit dieser Version werden die folgenden verwalteten Regeln AWS Config aktualisiert: • aurora-resources-protected-by-Backup-Plan • dynamodb-resources-protected-by-Backup-Plan • ebs-resources-protected-by-Backup-Plan • ec2-plan resources-protected-by-backup • efs-resources-protected-by-Ersatzplan • fsx-resources-protected-by-Backup-Plan • rds-resources-protected-by-Backup-Plan	10. März 2022

AWS Config unterstützt neue Ressourcentypen	Mit dieser Version können Sie Konfigurationsänderungen AWS Config an neuen öffentlichen Ressourcentypen von Amazon Elastic Container Registry aufzeichnen. Weitere Informationen finden Sie unter Unterstützte Ressourcentypen.	4. März 2022
AWS Config unterstützt neue Ressourcentypen	Mit dieser Version können Sie Konfigurationsänderungen AWS Config an neuen Amazon Elastic Compute Cloud-Ressourcentypen aufzeichnen. Weitere Informationen finden Sie unter Unterstützte Ressourcentypen.	28. Februar 2022
AWS Config aktualisiert verwaltete Regeln	In dieser Version werden die folgenden verwalteten Regeln AWS Config unterstützt: • codedeploy-auto-rollback-monitor-aktiviert • codedeploy-ec2- minimum-healthy-hosts-configured • codedeploy-lambda-allatonce-traffic-shift-deaktiviert	25. Februar 2022

Protokollierung und Überwachung im Update AWS Config	Mit dieser Version wird die Seite „Überwachung AWS Config mit Amazon EventBridge Events“ AWS Config aktualisiert, sodass Verweise auf Amazon CloudWatch Events ersetzt werden. Amazon EventBridge ist die bevorzugte Methode, um Ihre Veranstaltungen zu verwalten. CloudWatch Bei Events und EventBridge handelt es sich um denselben zugrunde liegenden Service und dieselbe API, EventBridge bieten aber mehr Funktionen. Änderungen, die Sie in einer der beiden CloudWatch oder in einer der beiden Konsolen vornehmen, EventBridge werden in jeder Konsole angezeigt. Weitere Informationen finden Sie auf Amazon EventBridge.	24. Februar 2022

AWS SDK-Seite für AWS Config	In dieser Version AWS Config wird eine Seite „Verwendung AWS Config mit einem AWS SDK“ eingeführt. AWS Software Development Kits (SDKs) sind für viele gängige Programmiersprachen verfügbar. Jedes SDK bietet eine API, Codebeispiele und Dokumentation, die es Entwicklern erleichtern, Anwendungen in ihrer bevorzugten Sprache zu erstellen.	24. Februar 2022

Aktualisierung der Sicherheit für die IAM-Rollen-Vertrauensrichtlinie	Mit dieser Version wird die IAM-Vertrauensrichtlinien-Erklärung AWS Config aktualisiert, sodass Sicherheitsvorkehrungen in die Vertrauensrichtlinie aufgenommen werden, die den Zugriff durch den Vorgang `sourceARN` and/or `sourceAccountId` for the AWS Security Token Service (AWS STS) einschränken. Dadurch wird sichergestellt, dass die IAM-Rollen-Vertrauensrichtlinie nur im Auftrag von erwarteten Benutzern und Szenarios auf Ihre Ressourcen zugreift. Die folgende Seite wurde aktualisiert: • Hinzufügen einer IAM-Vertrauensrichtlinie für Ihre Rolle	18. Februar 2022

Änderungen an der Aufzeichnung von globalen Ressourcentypen	AWS Config ändert jetzt die Art und Weise, wie neue globale Ressourcentypen in AWS Config Recording aufgezeichnet werden. Globale Ressourcentypen sind AWS Ressourcen, für die Sie bei der Erstellung keine Region angeben müssen. Vor dieser Änderung konnten Sie die Aufzeichnung globaler Ressourcentypen in allen unterstützten Regionen in AWS Config aktivieren. Nach dieser Änderung können neue globale Ressourcentypen, die in die AWS Config Aufzeichnung integriert wurden, nur in der Heimatregion des Dienstes für die kommerzielle Partition und AWS GovCloud (US-West) für die Partition aufgezeichnet werden. AWS GovCloud (US) Sie können die Konfigurationselemente für diese neuen globalen Ressourcentypen jetzt nur noch in ihrer Heimatregion und AWS GovCloud (US-West) anzeigen. Eine Liste der Regionen für globale Ressourcentypen, die nach Februar 2022 integrier t wurden, finden Sie in der Tabelle auf der Seite	18. Februar 2022

Aufzeichnen aller unterstützten Ressourcentypen.

Sicherheits-IAM-Update	Die `AWSConfigServiceRolePolicy` Richtlinie und die `AWS_ConfigRole` Richtlinie gewähren nun die Erlaubnis, Details zu Elastic Beanstalk Beanstalk -Umgebungen und eine Beschreibung der Einstellungen für den angegebenen Elastic Beanstalk Beanstalk-Konfigurationssatz abzurufen, eine Übersicht der OpenSearch Elasticsearch-Versionen abzurufen, die verfügbaren Amazon RDS-Optionsgruppen für eine Datenbank zu beschreiben und Informationen über eine Bereitstellungskonfiguration abzurufen. CodeDeploy Diese Richtlinie gewährt jetzt auch die Erlaubnis, den angegebenen alternativen Kontakt abzurufen, der an eine angehängt ist AWS-Konto, Informationen über eine AWS Organizations Richtlinie abzurufen, eine Amazon ECR-Repository-Richtlinie abzurufen, Informationen über eine archivierte AWS Config Regel abzurufen, eine Liste von Amazon ECS-Aufgabendefinitionsfamilien abzurufen, die Stamm- oder übergeordneten Organisationseinheiten (OUs) der	10. Februar 2022

angegebenen untergeordneten Organisationseinheit oder des angegebenen untergeordneten Kontos aufzulisten und die Richtlinien aufzulisten, die dem angegebenen Zielstamm, der Organisationseinheit oder dem angegebenen Zielkonto zugeordnet sind. Weitere Informationen finden Sie unter AWS -verwaltete Richtlinien für AWS Config.

AWS Config aktualisiert die verwalteten Regeln	In dieser Version werden die folgenden verwalteten Regeln AWS Config unterstützt: • autoscaling-multiple-az • codebuild-project-artifact-encryption • codebuild-project-environment-privileged-überprüfen • codebuild-project-logging-enabled • codebuild-project-s3-log-verschlüsselt • ec2- -einperiodisch security-group-attached-to • ecr-private-image-scanning-aktiviert • ecr-private-tag-immutability-aktiviert • ecs-containers-nonprivileged • ecs-containers-readonly-access • ecs-no-environment-secrets • ecs-task-definition-memory-hartes Limit • ecs-task-definition-nonroot-Benutzer • ecs-task-definition-pid-Modus-Check • eks-cluster-oldest-supported-Ausführung	10. Februar 2022

	• eks-cluster-supported-version • lambda-vpc-multi-az-überprüfen • nacl-no-unrestricted-ssh-rdp • netfw-stateless-rule-group-nicht leer • rds-cluster-default-admin-überprüfen • rds-db-security-group-nicht erlaubt • rds-instance-default-admin-überprüfen • redshift-default-admin-check • s3- bucket-acl-prohibited • s-3 version-lifecycle-policy-check • waf-global-webacl-not-leer	
Sicherheits-IAM-Update	Die `AWSConfigServiceRolePolicy` Richtlinie und die `AWS_ConfigRole` Richtlinie gewähren nun die Erlaubnis, CloudWatch Amazon-Protokollgruppen und -Streams zu erstellen und Protokolle in erstellte Protokollstreams zu schreiben. Weitere Informationen finden Sie unter AWS -verwaltete Richtlinien für AWS Config.	2. Februar 2022

AWS Config aktualisiert die verwalteten Regeln	In dieser Version werden die folgenden verwalteten Regeln AWS Config unterstützt: • opensearch-access-control-enabled • opensearch-audit-logging-enabled • opensearch-data-node-fault-Toleranz • opensearch-encrypted-at-rest • opensearch-https-required • opensearch-in-vpc-only • opensearch-logs-to-cloudwatch • opensearch-node-to-node-Verschlüsselungsprüfung	31. Januar 2022
AWS Config unterstützt neue Ressourcentypen	Mit dieser Version können Sie Konfigurationsände rungen AWS Config an AWS CodeDeploy Ressource ntypen aufzeichnen. Weitere Informationen finden Sie unter Unterstützte Ressourcentypen.	5. Januar 2022
AWS Config unterstützt neue Ressourcentypen	Mit dieser Version können Sie Konfigurationsände rungen AWS Config an neuen Amazon SageMaker AI-Ressourcentypen aufzeichn en. Weitere Informationen finden Sie unter Unterstützte Ressourcentypen.	20. Dezember 2021

AWS Config unterstützt neue Konformitätspakete	AWS Config Unterstützt mit dieser Version die folgenden Konformitätspakete: • Leitfaden zu bewährten betrieblichen Verfahren für die ENISA-Cybersicherheit für SMEs	20. Dezember 2021
AWS Config unterstützt neue Konformitätspakete	AWS Config Unterstützt mit dieser Version die folgenden Konformitätspakete: • Bewährte Methoden für die Ausführung von NIST 800 172 • Bewährte Methoden für die Ausführung von NIST 800 181 Das folgende Konformit ätspaket wurde aktualisiert: • Betriebliche bewährte Methoden für K-ISMS	18. November 2021

AWS Config unterstützt neue Conformance Packs	AWS Config Unterstützt mit dieser Version die folgenden Konformitätspakete: • Bewährte Methoden für die Ausführung von Amazon API Gateway • Bewährte betriebliche Verfahren für AWS Backup • Bewährte Methoden für die Ausführung von CISA Cyber Essentials • Bewährte betriebliche Verfahren für DevOps • Bewährte Methoden für die Ausführung von NIST Privacy Framework v1.0 Die folgenden Konformit ätspakete wurden aktualisiert: • Bewährte Methoden für die Ausführung von FedRAMP (Low) • Betriebliche bewährte Methoden für FedRAMP (Moderat)	29. Oktober 2021

AWS Config unterstützt neue Ressourcentypen	Mit dieser Version können Sie Konfigurationsände rungen AWS Config an neuen Amazon OpenSearch Service-Ressourcentypen aufzeichn en. Weitere Informationen finden Sie unter Unterstützte Ressourcentypen.	12. Oktober 2021
AWS Config unterstützt neue Konformitätspakete	Mit dieser Version wird das folgende Konformitätspaket AWS Config aktualisiert: • Bewährte Methoden für die Ausführung von MAS TRMG	12. Oktober 2021

AWS Config unterstützt neue Conformance Packs	Mit dieser Version werden die folgenden Konformitätspakete AWS Config aktualisiert: • Bewährte Methoden für den Betrieb von ABS CCIG 2.0 Material Workloads • Bewährte Methoden für den Betrieb von ABS CCIG 2.0 Standard Workloads • Bewährte Methoden für die Ausführung von ACSC Essential 8 • Bewährte Methoden für die Ausführung von ACSC ISM • Bewährte Betriebspraktiken für BNM T RMi • Bewährte Methoden für die Ausführung von CMMC Level 1 • Bewährte Methoden für die Ausführung von CMMC Level 2 • Bewährte Methoden für die Ausführung von CMMC Level 3 • Bewährte Methoden für die Ausführung von CMMC Level 4 • Bewährte Methoden für die Ausführung von CMMC Level 5	30. September 2021

	• Betriebliche bewährte Methoden für FDA Titel 21 CFR Teil 11 • Betriebliche bewährte Methoden für FFIEC • Bewährte Methoden für die Ausführung von MAS Notice 655 • Bewährte Methoden für die Ausführung von NBC TRMG • Bewährte Methoden für die Ausführung von NERC CIP • Bewährte Methoden für die Ausführung von NIST 800-53 rev 5	
Sicherheits-IAM-Update	Die `AWSConfigServiceRolePolicy` Richtlinie und die `AWS_ConfigRole` Richtlinie gewähren nun die Erlaubnis, Details zu einem Amazon OpenSearch Service (OpenSearch Service) domain/domains und eine detaillierte Parameterliste für eine bestimmte Amazon Relational Database Service (Amazon RDS) DB-Parametergruppe abzurufen. Diese Richtlinie gewährt auch die Erlaubnis, Details zu ElastiCache Amazon-Snapshots abzurufen. Weitere Informationen finden Sie unter AWS -verwaltete Richtlinien für AWS Config.	8. September 2021

AWS Config unterstützt neue Ressourcentypen	Mit dieser Version können Sie Konfigurationsände rungen AWS Config an neuen Amazon Elastic Compute Cloud-Ressourcenty pen aufzeichnen. Weitere Informationen finden Sie unter Unterstützte Ressourcentypen.	7. September 2021

AWS Config unterstützt neue Conformance Packs	Mit dieser Version werden die folgenden Konformitätspakete AWS Config aktualisiert: • Bewährte Methoden für die Ausführung von APRA CPG 234 • Bewährte betriebliche Verfahren für AWS GUS-Stiftungen — Benchmark v1.4, Stufe 1 • Bewährte betriebliche Verfahren für AWS GUS-Stiftungen Benchmark v1.4 Stufe 2 • Bewährte Methoden für die Ausführung von NCSC Cloud Security Principles • Bewährte Methoden für die Ausführung von NCSC Cyber Assesment Framework • Bewährte Methoden für die Ausführung von NIST 800 171 • Bewährte Methoden für die Ausführung von NIST CSF • Bewährte betriebliche Verfahren für das RBI Cyber Security Framework für UCBs • Bewährte Methoden für die Ausführung von RBI MD-ITF • Bewährte Methoden für die Ausführung von NYDFS 23	30. August 2021

	• Bewährte Methoden für die Ausführung von PCI DSS 3.2.1	
AWS Config aktualisiert verwaltete Regeln	In dieser Version werden die folgenden verwalteten Regeln AWS Config unterstützt: • aurora-resources-protected-by-Backup-Plan • backup-plan-min-frequency-and-min-retention-check • backup-recovery-point-encrypted • backup-recovery-point-manual-Löschen-deaktiviert • backup-recovery-point-minimum-Aufbewahrungsprüfung • dynamodb-resources-protected-by-Ersatzplan • ebs-resources-protected-by-Backup-Plan • ec2-plan resources-protected-by-backup • efs-resources-protected-by-Ersatzplan • fsx-resources-protected-by-Backup-Plan • rds-resources-protected-by-Backup-Plan	20. August 2021

AWS Config unterstützt neue Konformitätspakete	AWS Config Unterstützt mit dieser Version das folgende Konformitätspaket: • Bewährte Methoden für die Ausführung von NZISM	20. August 2021
Aktualisierung der Amazon-SNS-Sicherheitsrichtlinie	Mit dieser Version wird die IAM-Richtlinienerklärung für das Amazon SNS-Thema bei der Verwendung von serviceverknüpften Rollen AWS Config aktualisiert, um Sicherheitsvorkehrungen, die den Zugriff einschränken, `sourceARN` and/or `sourceAccountId` in die Themenrichtlinie aufzunehmen. Dadurch wird sichergestellt, dass Amazon SNS nur im Auftrag von erwarteten Benutzern und Szenarios auf Ihre Ressourcen zugreift. Die folgende Seite wurde aktualisiert: • Berechtigungen für das Amazon-SNS-Thema	17. August 2021

Aktualisierung der Sicherheitsrichtlinien AWS Lambda	Mit dieser Version wird die AWS Lambda ressourcenbasierte Richtlinie für AWS Config benutzerdefinierte Regeln AWS Config aktualisiert, sodass sie Sicherheitsvorkehrungen enthält, mit denen der Zugriff `sourceARN` and/or `sourceAccountId` in die Aufrufanforderung eingeschränkt wird. Dadurch AWS Lambda wird sichergestellt, dass nur im Namen der erwarteten Benutzer und Szenarien auf Ihre Ressourcen zugegriffen wird. Die folgenden Seiten wurden aktualisiert: • AWS::Config::ConfigRule • Entwicklung einer benutzerdefinierten Regel für AWS Config	12. August 2021
AWS Config unterstützt neue Ressourcentypen	Mit dieser Version können Sie Konfigurationsänderungen AWS Config an Amazon Kinesis Kinesis-Ressourcentypen aufzeichnen. Weitere Informationen finden Sie unter Unterstützte Ressourcentypen.	6. August 2021

AWS Config unterstützt neue Conformance Packs	AWS Config Unterstützt mit dieser Version das folgende Konformitätspaket: • Bewährte Methoden für die Implementierung des Esquema Nacional de Seguridad (ENS) High Die folgenden Konformit ätspakete wurden aktualisiert: • Operative Best Practices für die AWS Zuverläss igkeit eines gut konzipierten Frameworks • Bewährte betriebliche Verfahren für die AWS Sicherheitssäule eines Well-Architected Frameworks • Bewährte Methoden für die Implementierung des Esquema Nacional de Seguridad (ENS) Low • Bewährte Methoden für die Implementierung des Esquema Nacional de Seguridad (ENS) Medium • Betriebliche bewährte Methoden für die HIPAA-Sic herheit	30. Juli 2021

AWS Lambda Beispielfunktionen für benutzerdefinierte Regeln AWS Config	In dieser Version stehen Python-Beispielfunktionen unter AWS Lambda Beispielfunktionen für AWS Config Regeln (Python) zur AWS Config Verfügung.	29. Juli 2021

Sicherheits-IAM-Update	Die Richtlinien `AWSConfigServiceRolePolicy` und `AWS_ConfigRole` gewähren die Berechtigung, Tags für eine Protokollgruppe, Tags für eine Zustandsmaschine und alle Zustandsmaschinen aufzulisten. Diese Richtlinien gewähren jetzt die Berechtigung zum Abrufen von Details über eine Zustandsmaschine. Diese Richtlinien unterstützen jetzt auch zusätzliche Berechtigungen für Amazon EC2 Systems Manager (SSM), Amazon Elastic Container Registry, Amazon, Amazon Data Firehose FSx, Amazon Managed Streaming for Apache Kafka (Amazon MSK), Amazon Relational Database Service (Amazon RDS), Amazon Route 53, Amazon SageMaker AI, Amazon Simple Notification Service,, und. AWS Database Migration Service AWS Global Accelerator AWS Storage Gateway Weitere Informationen finden Sie unter AWS -verwaltete Richtlinien für AWS Config.	28. Juli 2021

AWS Config unterstützt neue Ressourcentypen	Mit dieser Version können Sie Konfigurationsänderungen AWS Config an AWS Backup Ressourcentypen aufzeichnen. Weitere Informationen finden Sie unter Unterstützte Ressourcentypen.	14. Juli 2021
AWS Config unterstützt neue Conformance Packs	AWS Config Unterstützt mit dieser Version die folgenden Konformitätspakete: • Bewährte Betriebspraktiken für CIS Critical Security Controls v8 IG1 • Bewährte betriebliche Verfahren für kritische Sicherheitskontrollen der GUS v8 IG2 • Bewährte betriebliche Verfahren für kritische Sicherheitskontrollen der GUS v8 IG3 • Bewährte Methoden für die Ausführung von NIST 1800 25	09. Juli 2021
AWS Config aktualisiert verwaltete Regeln	In dieser Version werden die folgenden verwalteten Regeln AWS Config unterstützt: • ssm-document-not-public • s3- account-level-public-access -Blocks-periodisch	25. Juni 2021

AWS Config aktualisiert verwaltete Regeln	In dieser Version werden die folgenden verwalteten Regeln AWS Config unterstützt: • ec-2 instance-multiple-eni-check • elv 2- acm-certificate-required • autoscaling-launch-config-public-ip-deaktiviert	10. Juni 2021

Sicherheits-IAM-Update	Die `AWSConfigServiceRolePolicy` Richtlinie und die `AWS_ConfigRole` Richtlinie gewähren nun die Erlaubnis, die Berechtigungen von AWS Systems Manager Dokumenten und Informationen zu IAM Access Analyzer einzusehen. Diese Richtlinien unterstützen jetzt zusätzliche AWS Ressourcentypen für Amazon Kinesis, Amazon ElastiCache, Amazon EMR AWS Network Firewall, Amazon Route 53 und Amazon Relational Database Service (Amazon RDS). Diese Berechtigungsänderungen ermöglichen das Aufrufen des Nur-Lese-Modus AWS Config , der zur Unterstützung dieser Ressourcentypen APIs erforderlich ist. Diese Richtlinien unterstützen jetzt auch das Filtern von Lambda @Edge - Funktionen für die lambda-inside-vpc AWS Config verwaltete Regel. Weitere Informationen finden Sie unter AWS - verwaltete Richtlinien für AWS Config.	8. Juni 2021

AWS Config aktualisiert verwaltete Regeln	In dieser Version werden die folgenden verwalteten Regeln AWS Config unterstützt: • elasticsearch-logs-to-cloudwatch • rds-cluster-multi-az-aktiviert • api-gw-associated-with-WAF • iam-policy-no-statements-with-full-access	19. Mai 2021
AWS Config unterstützt neue Ressourcentypen	Mit dieser Version können Sie Konfigurationsänderungen AWS Config an Amazon Elastic File System-Ressourcentypen aufzeichnen. Weitere Informationen finden Sie unter Unterstützte Ressourcentypen.	13. Mai 2021

Sicherheits-IAM-Update	Die `AWSConfigServiceRolePolicy` Richtlinie und die `AWS_ConfigRole` Richtlinie gewähren nun Berechtigungen, die es ermöglichen AWS Config , schreibgeschützte GET-Aufrufe an API Gateway zu tätigen, um eine Konfigurationsregel für API Gateway zu unterstützen. Diese Richtlinien fügen auch Berechtigungen hinzu, die es AWS Config ermöglichen, Amazon Simple Storage Service (Amazon S3) schreibgeschützt aufzurufen APIs, die zur Unterstützung des neuen `AWS::S3::AccessPoint` Ressourcentyps erforderlich sind. Weitere Informationen finden Sie unter AWS -verwaltete Richtlinien für AWS Config.	10. Mai 2021
AWS Config Benutzerdefinierte Regeln	Die folgenden Seiten im Entwicklerhandbuch wurden aktualisiert: • Erste Schritte mit benutzerdefinierten Regeln für AWS Config • Entwicklung einer benutzerdefinierten Regel für AWS Config	30. April 2021

AWS Config aktualisiert verwaltete Regeln	In dieser Version werden die folgenden verwalteten Regeln AWS Config unterstützt: • aurora-mysql-backtracking-enabled • ec-2 instance-profile-attached • ecs-task-definition-user-for-host-mode-check • no-unrestricted-route-to-igw • rds-automatic-minor-version-Upgrade aktiviert • redshift-enhanced-vpc-routing-aktiviert	15. April 2021

Sicherheits-IAM-Update	Die `AWSConfigServiceRolePolicy` Richtlinie und die `AWS_ConfigRole` Richtlinie gewähren nun die Erlaubnis, Informationen zu AWS Systems Manager bestimmten Dokumenten einzusehen. Diese Richtlinien unterstützen jetzt auch zusätzliche AWS Ressourcentypen für AWS Backup Amazon Elastic File System, Amazon ElastiCache, Amazon Simple Storage Service (Amazon S3), Amazon Elastic Compute Cloud (Amazon EC2), Amazon Kinesis AWS Database Migration Service, Amazon SageMaker AI und Amazon Route 53. Diese Berechtigungsänderungen ermöglichen AWS Config das Aufrufen des Nur-Lese-Modus, der zur Unterstützung dieser APIs Ressourcentypen erforderlich ist. Weitere Informationen finden Sie unter AWS -verwaltete Richtlinien für AWS Config.	14. April 2021

Konformität mit Konformitätspaketen als Konfigurationselemente () CIs	In dieser Version wird die AWS Config Konformitätspaket-Konformität in Form von Konfigurationselementen unterstützt. Dies ermöglicht es Ihnen, • eine Zeitleiste der Änderungen am Compliance-Status Ihrer Konformitätspakete anzusehen, • die Compliance von Konformitätspaketen über mehrere Konten und Regionen hinweg zu aggregieren und • erweiterte Abfragen zu verwenden, um die Compliance Ihrer Konformitätspakete zu prüfen. Die folgenden Datentypen wurden aktualisiert: • DescribeAggregateComplianceByConformancePacks • GetAggregateConformancePackComplianceSummary Die folgenden Seiten im Entwicklerhandbuch wurden aktualisiert:	30. März 2021

	• Anzeigen von Compliance-Daten im Dashboard für Konformitätspakete • Anzeigen einer Zeitleiste des Compliance-Verlaufs für Konformitätspakete • Anzeigen von Compliance-Daten im Aggregator-Dashboard • Den aktuellen Konfigurationsstatus der Ressourcen abfragen AWS • Unterstützte Ressourcentypen	
Aktualisierung zur Seitennummerierung	In dieser Version unterstützt die Funktion für AWS Config erweiterte Abfragen jetzt die Paginierung für Abfragen, die Aggregatfunktionen wie COUNT und SUM enthalten. Sie können jetzt erweiterte Abfragen verwenden und durch die Seitennummerierung vollständige Ergebnisse für Ihre Aggregierungsabfragen erhalten, die zuvor auf 500 Zeilen beschränkt waren. Weitere Informationen finden Sie unter Den aktuellen Konfigurationsstatus von Ressourcen abfragen AWS	26. März 2021

Regionsunterstützung	Mit dieser Version wird AWS Config and AWS Config Rules jetzt in der Region Asien-Pazifik (Osaka) unterstützt.	4. März 2021
AWS Config unterstützt neue Ressourcentypen	Mit dieser Version können Sie Konfigurationsänderungen AWS Config an den Ressourcentypen Amazon Elastic Container Registry, Amazon Elastic Container Service und Amazon Elastic Kubernetes Service aufzeichnen. Weitere Informationen finden Sie unter Unterstützte Ressourcentypen.	25. Februar 2021

Unterstützung für KMS-Verschlüsselung	Mit dieser Version AWS Config können Sie KMS-basierte Verschlüsselung für Objekte verwenden, die von AWS Config für die S3-Bucket-Delivery bereitgestellt wurden. Die folgenden Datentypen wurden aktualisiert: • DeliveryChannel • PutDeliveryChannel Die folgenden Seiten im Entwicklerhandbuch wurden aktualisiert: • Berechtigungen für den KMS-Schlüssel • Berechtigungen für die IAM-Rolle sind zugewiesen AWS Config	16. Februar 2021
AWS Config aktualisiert verwaltete Regeln	In dieser Version werden die folgenden verwalteten Regeln AWS Config unterstützt: • secretsmanager-secret-periodic-rotation • secretsmanager-secret-unused • secretsmanager-using-cmk	16. Februar 2021

Unterstützung von Regionen für gespeicherte Abfragen	Mit dieser Version werden gespeicherte Abfragen jetzt in den Regionen AWS GovCloud (USA-Ost) und AWS GovCloud (US-West) unterstützt.	15. Februar 2021
Unterstützung für Regionen bei der Datenaggregation für mehrere Konten und Regionen	Ab dieser Version wird die Datenaggregation für mehrere Konten und Regionen in den Regionen Afrika (Kapstadt) und Europa (Mailand) unterstützt. Weitere Informationen finden Sie unter Datenaggregation für mehrere Konten und Regionen.	15. Februar 2021
Regionsunterstützung für erweiterte Abfragen	Mit dieser Version werden erweiterte Abfragen in den Regionen Afrika (Kapstadt) und Europa (Mailand) unterstützt. Weitere Informati onen finden Sie unter Abfragen des aktuellen Konfigurationsstatus von Ressourcen. AWS	15. Februar 2021
AWS Config Benachrichtigung über den Dokumentationsverl auf als RSS-Feed verfügbar	Sie können jetzt Benachric htigungen über Aktualisi erungen der AWS Config Dokumentation erhalten, indem Sie einen RSS-Feed abonnieren.	1. Januar 2021

Frühere Aktualisierungen

In der folgenden Tabelle wird der Versionsverlauf der Dokumentation AWS Config vor dem 31. Dezember 2020 beschrieben.

Änderung	Beschreibung	Veröffentlichungsdatum
Unterstützung für gespeicherte Abfragen	Mit dieser Version AWS Config können Sie Ihre Abfragen speichern . Nachdem Sie Abfragen gespeiche rt haben, können Sie sie durchsuch en, in den Abfrage-Editor kopieren, bearbeiten oder löschen. Weitere Informationen zum Speichern einer Abfrage finden Sie unter Abfrage mit dem SQL-Abfrage-Editor für AWS Config (Konsole) und Abfrage mit dem SQL-Abfrage-Editor für AWS Config (AWS CLI). Weitere Informationen zu APIs finden Sie in der AWS Config API-Referenz: • PutStoredQuery • GetStoredQuery • ListStoredQueries • DeleteStoredQuery Lesen Sie auch Servicebeschränkun gen für AWS Config.	21. Dezember 2020
Unterstützung für Prozesspr üfungen	In dieser Version werden Prozesspr üfungen AWS Config unterstützt. Dabei handelt es sich um eine Art AWS Config Regel, mit der Sie Ihre externen und internen Aufgaben, für die eine Überprüfung erforderlich ist,	17. Dezember 2020

Änderung	Beschreibung	Veröffentlichungsdatum
	im Rahmen der Konformitätspakete nachverfolgen können. Mithilfe von Prozessprüfungen können Sie die Compliance von Anforderungen und Maßnahmen an einem Ort auflisten. Weitere Informationen zu Prozessprüfungen finden Sie im AWS Config Prozessprüfungen innerhalb eines Konformitätspakets für AWS Config Thema und in der PutExternalEvaluationAPI.	

Änderung	Beschreibung	Veröffentlichungsdatum
AWS Config aktualisiert verwaltete Regeln	In dieser Version werden die folgenden verwalteten Regeln AWS Config unterstützt: • api-gw-ssl-enabled • api-gw-xray-enabled • beanstalk-enhanced-health-reporting-aktiviert • cloudfront-accesslogs-enabled • cloudfront-associated-with-waf • cloudfront-custom-ssl-certificate • elastic-beanstalk-managed-updates-aktiviert • rds-cluster-iam-authentication-aktiviert • redshift-cluster-kms-enabled • s3- verboten bucket-level-public-access • subnet-auto-assign-public-ip-deaktiviert • vpc-network-acl-unused-überprüfen	17. Dezember 2020
AWS Config unterstützt AWS Network Firewall	Mit dieser Version können Sie Konfigurationsänderungen AWS Config an Ihren Ressourcentypen AWS Network Firewall FirewallPolicy RuleGroup, und Firewall aufzeichnen. Weitere Informationen finden Sie unter Unterstützte Ressourcentypen für AWS Config.	4. Dezember 2020

Änderung	Beschreibung	Veröffentlichungsdatum
Aktualisierung der Dokumentation	AWS Config Unterstützung für die unternehmensweite Aggregation von Ressourcendaten in einem delegierten Administratorkonto hinzugefügt. Sie können nun ein delegiertes Administratorkonto verwenden, um Ressourcenkonfigurations- und Compliance-Daten aus allen Mitgliedskonten einer Organisation in AWS -Organisationen zu aggregieren. Weitere Informationen finden Sie unter PutConfigurationAggregator, Aggregatoren erstellen für AWS Config und Registrierung eines delegierten Administrators für AWS Config.	4. Dezember 2020
AWS Config unterstützt neue Konformitätspakete	• Bewährte Methoden für die Implementierung des Esquema Nacional de Seguridad (ENS) Low • Bewährte Methoden für die Implementierung des Esquema Nacional de Seguridad (ENS) Medium • Bewährte Methoden für die Implementierung des Cyber Assessment Framework des NCSC • Operative Best Practices für das RBI Cyber Security Framework für UCBs	30. Oktober 2020

Änderung	Beschreibung	Veröffentlichungsdatum
AWS Config unterstützt neue Konformitätspakete	• Bewährte Methoden für die Implementierung von ACSC Essential 8 • Bewährte Methoden für die Implementierung von ACSC ISM • Bewährte Methoden für die Ausführung von KI und ML • Bewährte Methoden für die Ausführung des Asset-Managements • Bewährte Methoden für die Ausführung von BCP und DR • Bewährte Methoden für die Ausführung von EC2 • Bewährte Methoden zur Ausführung von K-ISMS • Bewährte Methoden für die Ausführung von Load Balancing • Betriebliche bewährte Methoden für die Protokollierung • Bewährte Methoden für die Überwachung • Bewährte Methoden für die Ausführung von Serverless	22. Oktober 2020

Änderung	Beschreibung	Veröffentlichungsdatum
AWS Config unterstützt neue Konformitätspakete	• Bewährte Methoden für die Implementierung von APRA CPG 234 • Bewährte Methoden zur Implementierung von FedRAMP(Low) • Bewährte Methoden für die Verwendung der MAS Notice 655 • Bewährte Methoden für die Implementierung von NBC TRMG • Bewährte Methoden für die Ausführung von NCSC-Cloud-Sicherheitsprinzipien • Bewährte Methoden für die Ausführung von RBI MD-ITF	15. Oktober 2020

Änderung	Beschreibung	Veröffentlichungsdatum
AWS Config unterstützt neue Konformitätspakete	• Bewährte Methoden für den Betrieb von ABS CCIG 2.0 Material Workloads • Bewährte Methoden für den Betrieb von ABS CCIG 2.0 Standard Workloads • Bewährte Betriebspraktiken für BNM T RMi • Bewährte Methoden für die Erreichung von Ausfallsicherheit • Bewährte Methoden für die Ausführung von Data Lakes und Analyseservices • Bewährte Methoden für die Verwendung von Verschlüsselung und Schlüsselverwaltung • Betriebliche bewährte Methoden für FDA Titel 21 CFR Teil 11 • Bewährte Methoden für die Ausführung von öffentlich zugänglichen Ressourcen • Bewährte Methoden für die Ausführung von MAS TRMG • Bewährte Methoden für die Ausführung von NERC CIP BCSI • Bewährte Methoden für die Ausführung von NYDFS 23	8. Oktober 2020

Änderung	Beschreibung	Veröffentlichungsdatum
AWS Config unterstützt neue Konformitätspakete	• Operative Best Practices für die AWS Zuverlässigkeit eines gut konzipierten Frameworks • Bewährte betriebliche Verfahren für die AWS Sicherheitssäule eines Well-Architected Frameworks • Bewährte Methoden für die Ausführung von Datenverarbeitungsservices • Bewährte Methoden für die Ausführung von Datenbankservices • Bewährte Methoden für die Ausführung von Management- und Governance-Services • Bewährte Methoden für die Ausführung von Services für Netzwerke und zur Bereitstellung von Inhalten • Bewährte Methoden für Sicherheits-, Identitäts- und Compliance-Services • Bewährte Methoden für die Ausführung von Speicherservices	26. Oktober 2020

Änderung	Beschreibung	Veröffentlichungsdatum
AWS Config unterstützt neue Konformitätspakete	• Bewährte Methoden für die Ausführung von FedRAMP(Moderate) • Betriebliche bewährte Methoden für FFIEC • Betriebliche bewährte Methoden für die HIPAA-Sicherheit • Bewährte Methoden für die Implementierung von NIST 800-53 Rev. 4 • Bewährte Methoden für die Ausführung von NIST 800 171	28. September 2020
Aktualisierung der Dokumentation	Die folgenden Themen zu Konformitätspaketen wurden aktualisiert: • Voraussetzung für Conformance Packs für AWS Config • Bereitstellung von Conformance Packs für AWS Config • Verwaltung von Conformance Packs AWS Config für alle Konten in Ihrem Unternehmen	28. September 2020
AWS Config aktualisiert verwaltete Regeln	In dieser Version werden die folgenden verwalteten Regeln AWS Config unterstützt: • iam-customer-policy-blocked-kms-Aktionen • iam-inline-policy-blocked-kms-Aktionen	17. September 2020

Änderung	Beschreibung	Veröffentlichungsdatum
AWS Config unterstützt AWS WAF v2	Mit dieser Version können Sie Konfigurationsänderungen AWS Config an Ihren AWS WAF v2-WebACL-,, IPSet RegexPatternSet RuleGroup, und ManagedRuleSet Ressourcentypen aufzeichnen. Weitere Informationen finden Sie unter Unterstützte Ressourcentypen für AWS Config.	1. September 2020
Aktualisierung der Dokumentation	Zu Voller Zugriff auf AWS Config wurde ein Hinweis zur Erstellung benutzerdefinierter Berechtigungen hinzugefügt, die vollen Zugriff gewähren. Die Dokumentation für die folgenden Regeln wurde aktualisiert: • bucket-server-side-encryptions3-fähig • ec2- instance-detailed-monitoring-enabled • ec2- managedinstance-platform-check	24. August 2020
Aktualisierung der Dokumentation	Die Vorlagen Bewährte Methoden für die Ausführung von PCI DSS 3.2.1 und Bewährte Methoden für die Ausführung von NIST CSF wurden aktualisiert.	14. August 2020

Änderung	Beschreibung	Veröffentlichungsdatum
Aktualisierung der Dokumentation	Beispiele für Beziehungsabfragen wurden hinzugefügt. Weitere Informationen finden Sie unter Beispiel für Beziehungsabfragen für AWS Config.	30. Juli 2020
Aktualisierung der Dokumentation	Die folgenden Datentypen wurden aktualisiert: • ConfigurationAggregator • RemediationConfiguration • DescribeOrganizationConfigRules • GetOrganizationConfigRuleDetailedStatus • DescribeOrganizationConfigRuleStatuses • DescribeOrganizationConformancePacks • DescribeOrganizationConformancePackStatuses • GetOrganizationConformancePackDetailedStatus	23. Juli 2020
AWS Config unterstützt den AWS Systems Manager Manager-Ressourcentyp	Mit dieser Version können AWS Config Sie Konfigurationsänderungen am Dateidaten-Ressourcentyp AWS Systems Manager aufzeichnen. Weitere Informationen finden Sie unter Unterstützte Ressourcentypen für AWS Config.	9. Juli 2020

Änderung	Beschreibung	Veröffentlichungsdatum
Aktualisierung der Dokumentation	Die Vorlagen Operative Best Practices für AWS Identitäts- und Zugriffsmanagement und Bewährte Methoden für die Ausführung von PCI DSS 3.2.1 wurden aktualisiert.	9. Juli 2020

Änderung	Beschreibung	Veröffentlichungsdatum
AWS Config aktualisiert verwaltete Regeln	In dieser Version werden die folgenden verwalteten Regeln AWS Config unterstützt: • account-part-of-organizations • alb-http-drop-invalid-Header-fähig • alb-waf-enabled • cloudfront-default-root-object-konfiguriert • cloudfront-origin-access-identity-aktiviert • cloudfront-origin-failover-enabled • cloudfront-sni-enabled • cloudtrail-security-trail-enabled • cw-loggroup-retention-period-überprüfen • dax-encryption-enabled • dynamodb-in-backup-plan • ebs-in-backup-plan • ec2-imdsv2-check • efs-in-backup-plan • eks-endpoint-no-public-Zugang • eks-secrets-encrypted • elasticsearch-node-to-node-Verschlüsselungsprüfung • elb-cross-zone-load-Balancing aktiviert • elb-tls-https-listeners-nur • iam-no-inline-policy-überprüfen • rds-cluster-deletion-protection-aktiviert	9. Juli 2020

Änderung	Beschreibung	Veröffentlichungsdatum
	• rds-in-backup-plan • rds-instance-deletion-protection-aktiviert • rds-instance-iam-authentication-aktiviert • rds-logging-enabled • redshift-backup-enabled • waf-classic-logging-enabled • wafv2-logging-enabled Weitere Informationen finden Sie unter Liste der AWS Config verwalteten Regeln.	
Unterstützung für Regionen bei der Datenaggregation für mehrere Konten und Regionen	Mit dieser Version wird die Datenaggregation für mehrere Konten und Regionen in den Regionen Asien-Pazifik (Hongkong) und Naher Osten (Bahrain) unterstützt. Weitere Informationen erhalten Sie unter Multi-Account Multi-Region Data Aggregation und Fehlerbehebung bei der Datenaggregation mit mehreren Konten für mehrere Regionen für AWS Config.	1. Juli 2020

Änderung	Beschreibung	Veröffentlichungsdatum
Regionsunterstützung für erweiterte Abfragen	Ab dieser Version werden erweiterte Abfragen in den Regionen Asien-Pazifik (Hongkong) und Naher Osten (Bahrain) unterstützt. Weitere Informationen finden Sie unter Den aktuellen Konfigurationsstatus von AWS Ressourcen abfragen mit AWS Config.	1. Juli 2020
Aktualisierung der Dokumentation	Die Dokumentation für die folgenden Regeln wurde aktualisiert: • ec2-prüfen managedinstance-association-compliance-status • iam-policy-no-statements-with-admin-access • required-tags • restricted-common-ports • rds-snapshots-public-prohibited • s-3 bucket-policy-grantee-check	30. Juni 2020
Aktualisierung der Dokumentation	Die Dokumentation wurde mit Informationen zur Sicherheit von aktualisiert AWS Config. Siehe Sicherheit in AWS Config.	24. Juni 2020
Aktualisierung der Dokumentation	AWS Control Tower Die Vorlage für das Detective Guardrails Conformance Pack wurde aktualisiert. Weitere Informationen finden Sie unter AWS Control Tower Detective Guardrails Konformitätspaket.	4. Juni 2020

Änderung	Beschreibung	Veröffentlichungsdatum
AWS Config unterstützt ein neues Conformance Pack	AWS Config Unterstützt mit dieser Version Operational Best Practices für das NIST CSF Conformance Pack. Weitere Informationen finden Sie unter Bewährte Methoden für die Ausführung von NIST CSF .	29. Mai 2020
AWS Config aktualisiert verwaltete Regeln	In dieser Version werden die folgenden verwalteten Regeln AWS Config unterstützt: • dynamodb-pitr-enabled • dynamodb-table-encrypted-kms • ec2- ebs-encryption-by-default • rds-snapshot-encrypted • redshift-require-tls-ssl • s-3 bucket-default-lock-enabled • s-3 default-encryption-kms • securityhub-enabled • sns-encrypted-kms Weitere Informationen finden Sie unter Liste der AWS Config verwalteten Regeln.	28. Mai 2020

Änderung	Beschreibung	Veröffentlichungsdatum
Unterstützung für delegierte Administratoren	Mit dieser Version können Sie AWS Config Regeln und Konformitätspakete von jedem delegierten Mitgliedskonto in Ihrer Organisation aus bereitstellen, zusätzlich zum Verwaltungskonto. Weitere Informationen zu APIs finden Sie in der AWS Config API-Referenz: • PutOrganizationConfigRule • PutOrganizationConformancePack • DescribeOrganizationConfigRules • GetOrganizationConfigRuleDetailedStatus • DescribeOrganizationConfigRuleStatuses • DeleteOrganizationConfigRule • DeleteOrganizationConformancePack • DescribeOrganizationConformancePacks • DescribeOrganizationConformancePackStatuses • GetOrganizationConformancePackDetailedStatus Weitere Informationen finden Sie unter Servicebeschränkungen für AWS Config.	27. Mai 2020

Änderung	Beschreibung	Veröffentlichungsdatum
AWS Config Regeln, Unterstützung für Regionen	Mit dieser Version werden nur wenige AWS Config Regeln in den Regionen Afrika (Kapstadt) und Europa (Mailand) unterstützt. Eine detaillierte Liste der Regeln und der Regionen, in denen sie unterstützt werden, finden Sie unter Liste der AWS Config verwalteten Regeln.	28. April 2020
AWS Config unterstützt neue Conformance Packs	AWS Config Unterstützt mit dieser Version zwei Konformitätspakete. • AWS Control Tower Detective Guardrails Konformitätspaket • Bewährte Methoden für die Ausführung von CIS Weitere Informationen finden Sie unter Conformance Pack-Beispielvorlagen für AWS Config.	22. April 2020
AWS Config unterstützt AWS Secrets Manager	Mit dieser Version können Sie Konfigurationsänderungen AWS Config an Ihrem Secrets Manager Manager-Secret aufzeichnen. Weitere Informationen finden Sie unter Unterstützte Ressourcentypen für AWS Config.	20. April 2020

Änderung	Beschreibung	Veröffentlichungsdatum
AWS Config aktualisiert verwaltete Regeln	In dieser Version werden die folgenden verwalteten Regeln AWS Config unterstützt: • secretsmanager-rotation-enabled-check • secretsmanager-scheduled-rotation-success-überprüfen Weitere Informationen finden Sie unter Liste der AWS Config verwalteten Regeln.	16. April 2020
Unterstützung von Regionen für Konformitätspakete	Ab dieser Version werden Konformitätspakete in den Regionen Asien-Pazifik (Hongkong) und Naher Osten (Bahrain) unterstützt. Weitere Informationen finden Sie unter Conformance Packs.	8. April 2020
Aktualisierung der Dokumentation	AWS Config Grenzwerte sind in diesem Entwicklerhandbuch verfügbar. Weitere Informationen finden Sie unter Servicebeschränkungen für AWS Config.	8. April 2020

Änderung	Beschreibung	Veröffentlichungsdatum
Aktualisierung der Dokumentation	Ressourcen von Drittanbietern, die über die AWS CloudFormation Registrierung verwaltet (created/updated/deletedd. h.) werden automatisch AWS Config als Konfigurationselemente erfasst. Weitere Informationen finden Sie unter Aufzeichnen von Konfigurationen mit AWS Config für Ressourcen von Drittanbietern mithilfe des AWS CLI.	30. März 2020
Aktualisierung der Dokumentation	Die AWS Config verwalteten Regeln werden aktualisiert und enthalten nun AWS-Region Informationen. Weitere Informationen finden Sie unter Liste der AWS Config verwalteten Regeln.	27. März 2020
AWS Config unterstützt den Amazon SNS SNS-Ressourcentyp	Mit dieser Version können Sie Konfigurationsänderungen AWS Config an Ihrem Amazon SNS SNS-Thema aufzeichnen. Weitere Informationen finden Sie unter Unterstützte Ressourcentypen für AWS Config.	6. März 2020
Unterstützung für Regionen bei der Datenaggregation für mehrere Konten und Regionen	Ab dieser Version wird die Datenaggregation für mehrere Konten und Regionen in der Region Europa (Stockholm) unterstützt. Weitere Informationen finden Sie unter Multi-Account Multi-Region Data Aggregation.	5. März 2020

Änderung	Beschreibung	Veröffentlichungsdatum
Regionsunterstützung für erweiterte Abfragen	Ab dieser Version werden erweiterte Abfragen in der Region Europa (Stockholm) unterstützt. Weitere Informationen finden Sie unter Den aktuellen Konfigurationsstatus von AWS Ressourcen abfragen mit AWS Config.	5. März 2020
AWS Config ermöglicht es Ihnen, erweiterte Abfragen mit Konfigurationsaggregatoren auszuführen	Diese Version AWS Config bietet Unterstützung für die Ausführung erweiterter Abfragen auf der Grundlage von Ressourcenkonfigurationseigenschaften mit Konfigurationsaggregatoren, sodass Sie dieselben Abfragen für mehrere Konten und Regionen ausführen können. Weitere Informationen finden Sie unter Den aktuellen Konfigurationsstatus von AWS Ressourcen abfragen mit AWS Config. Mit dieser Version wird eine `SelectAggregateResourceConfig` API AWS Config hinzugefügt. Weitere Informationen finden Sie SelectAggregateResourceConfigin der AWS Config API-Referenz:	28. Februar 2020

Änderung	Beschreibung	Veröffentlichungsdatum
AWS Config unterstützt den Amazon SQS SQS-Ressourcentyp	Mit dieser Version können Sie Konfigurationsänderungen AWS Config in Ihrer Amazon SQS SQS-Warteschlange aufzeichnen. Weitere Informationen finden Sie unter Unterstützte Ressourcentypen für AWS Config.	13. Februar 2020

Änderung	Beschreibung	Veröffentlichungsdatum
AWS CloudFormation Unterstützung für Conformance Packs	Mit dieser Version wurde AWS CloudFormation Unterstützung für die folgenden Ressourcen hinzugefügt: `AWS::Config::ConformancePack` und `OrganizationConformancePack`. • AWS::Config::ConformancePack Verwenden Sie die `AWS::Config::ConformancePack` Ressource, um ein Conformance Pack zu erstellen, bei dem es sich um eine Sammlung von AWS Config Regeln handelt, die problemlos in einem Konto, einer Region und AWS unternehmensweit bereitgestellt werden können. • AWS::Config::OrganizationConformancePaket Verwenden Sie die `AWS::Config::OrganizationConformancePack` Ressource, um ein Organization Conformance Pack zu erstellen, das Informationen enthält über Konformitätspakete, die in den Mitgliedskonten AWS Config erstellt werden.	13. Februar 2020

Änderung	Beschreibung	Veröffentlichungsdatum
AWS Config aktualisiert verwaltete Regeln	In dieser Version werden die folgenden verwalteten Regeln AWS Config unterstützt: • api-gw-execution-logging-aktiviert • ec2-stopped-instance • elasticache-redis-cluster-automatic-Backup-Check • emr-master-no-public-ip • guardduty-non-archived-findings • rds-enhanced-monitoring-enabled • account-level-public-accesss3-Blöcke • sagemaker-endpoint-configuration-kms-schlüsselkonfiguriert • service-vpc-endpoint-enabled Weitere Informationen finden Sie unter Liste der AWS Config verwalteten Regeln.	20. Dezember 2019

Änderung	Beschreibung	Veröffentlichungsdatum
Datensatz konfigurationen für benutzerd efinierte Ressource ntypen	Mit dieser Version AWS Config wird Unterstützung für Datensatz konfigurationen für benutzerdefinierte Ressourcentypen eingeführt. Sie können die Konfigurationsdaten von Drittanbieterressourcen in AWS Config der AWS Config Konsole und veröffentlichen und den Ressource nbestand und den Konfigurationsverl auf anzeigen und überwachen APIs. Weitere Informationen finden Sie unter Aufzeichnen von Konfigura tionen mit AWS Config für Ressource n von Drittanbietern mithilfe des AWS CLI. Weitere Informationen zu APIs finden Sie in der AWS Config API-Referenz: • DeleteResourceConfig • PutResourceConfig	20. November 2019

Änderung	Beschreibung	Veröffentlichungsdatum
Konformitätspakete	Mit dieser Version AWS Config werden Conformance Packs eingeführt. Mit Conformance Packs können Sie eine Sammlung von AWS Config Regeln und Abhilfemaßnahmen zusammenfassen, die dann gemeinsam als eine Einheit in einem gesamten Unternehmen eingesetzt werden können. AWS Weitere Informationen finden Sie unter Conformance Packs. Weitere Informationen zu APIs finden Sie in der AWS Config API-Referenz: • DeleteOrganizationConformancePack • DeleteOrganizationConformancePack • DescribeConformancePacks • DescribeConformancePacks • DescribeConformancePackStatus • DescribeOrganizationConformancePacks • DescribeOrganizationConformancePackStatuses • GetConformancePackComplianceDetails • GetConformancePackComplianceSummary • GetOrganizationConformancePackDetailedStatus, • PutConformancePack	19. November 2019

Änderung	Beschreibung	Veröffentlichungsdatum
	• PutOrganizationConformancePack	
AWS Config unterstützt Amazon OpenSearch Service- und AWS Key Management Service Ressourcentypen	Mit dieser Version können Sie Konfigurationsänderungen AWS Config an Ihrer Amazon OpenSearch Service-Domain und Ihrem Amazon AWS Key Management Service Service-Schlüssel aufzeichnen. Weitere Informationen finden Sie unter Unterstützte Ressourcentypen für AWS Config.	11. November 2019
AWS Config aktualisiert die verwalteten Regeln	In dieser Version werden die folgenden verwalteten Regeln AWS Config unterstützt: • dms-replication-not-public • emr-kerberos-enabled • internet-gateway-authorized-vpc-nur • kms-cmk-not-scheduled-zum Löschen • sagemaker-notebook-no-direct-Internetzugang • sagemaker-notebook-instance-kms-schlüsselkonfiguriert • shield-drt-access Weitere Informationen finden Sie unter Liste der AWS Config verwalteten Regeln.	10. Oktober 2019

Änderung	Beschreibung	Veröffentlichungsdatum
AWS Config unterstützt den Amazon RDS-Ressourcentyp	Mit dieser Version können Sie Konfigurationsänderungen AWS Config an Ihrem Amazon Relationa l Database Service (Amazon RDS) DBCluster und DBCluster Snapshot aufzeichnen. Weitere Informationen finden Sie unter Unterstützte Ressourcentypen für AWS Config.	17. September 2019
AWS Config unterstützt den Amazon QLDB-Ressourcentyp	Mit dieser Version können AWS Config Sie Konfigurationsänderungen am Ledger-Ressourcentyp Amazon Quantum Ledger Database (QLDB) aufzeichnen. Weitere Informationen finden Sie unter Unterstützte Ressourcentypen für AWS Config.	10. September 2019

Änderung	Beschreibung	Veröffentlichungsdatum
AWS Config ermöglicht es Ihnen, auto Problembehebungen auf nicht konforme Ressourcen anzuwenden, die anhand von Regeln bewertet wurden AWS Config	Mit dieser Version AWS Config wird Unterstützung für die Anwendung der auto Problembehebung mithilfe von AWS Systems Manager Automatisierungsdokumenten auf nicht konforme Ressourcen eingeführt, die anhand von AWS Config Regeln bewertet wurden. Weitere Informationen finden Sie unter Behebung nicht konformer Ressourcen mit AWS Config. Mit dieser Version werden die folgenden AWS Config Neuerungen hinzugefügt. APIs Weitere Informationen finden Sie in der AWS Config - API-Referenz: • PutRemediationExceptions • DescribeRemediationExceptions • DeleteRemediationExceptions	5. September 2019

Änderung	Beschreibung	Veröffentlichungsdatum
AWS Config aktualisiert verwaltete Regeln	In dieser Version werden die folgenden verwalteten Regeln AWS Config unterstützt: • alb-http-to-https-Weiterleitungsprüfung • api-gw-cache-enabled-und-verschlüsselt • api-gw-endpoint-type-überprüfen • cloudtrail-s3-dataevents-enabled • cloudwatch-log-group-encrypted • ebs-snapshot-public-restorable-überprüfen • elb-deletion-protection-enabled • lambda-concurrency-check • lambda-dlq-check • lambda-inside-vpc • shield-advanced-enabled-autorenew • vpc-vpn-2-tunnels-up Weitere Informationen finden Sie unter Liste der AWS Config verwalteten Regeln.	22. August 2019

Änderung	Beschreibung	Veröffentlichungsdatum
AWS Config aktualisiert verwaltete Regeln	Mit dieser Version werden die folgenden verwalteten Regeln AWS Config aktualisiert: • cloudfront-viewer-policy-https • ec2- instance-no-public-ip • ec2-eni security-group-attached-to • efs-encrypted-check • elasticsearch-encrypted-at-rest • elasticsearch-in-vpc-only • redshift-cluster-public-access-überprüfen • vpc-sg-open-only-to-authorized-ports Weitere Informationen finden Sie unter Liste der AWS Config verwalteten Regeln.	31. Juli 2019
AWS Config unterstützt EC2 Amazon-Ressourcentypen	Mit dieser Version können Sie Konfigurationsänderungen AWS Config an den folgenden EC2 Amazon-Ressourcen aufzeichnen: VPCEndpoint VPCEndpoint Service und VPCPeering Connection. Weitere Informationen finden Sie unter Unterstützte Ressourcentypen für AWS Config.	12. Juli 2019

Änderung	Beschreibung	Veröffentlichungsdatum
AWS Config ermöglicht es Ihnen, AWS Config Regeln AWS-Konten innerhalb einer Organisation zu verwalten	Mit dieser Version AWS Config wird Unterstützung für die gesamte Verwaltung von AWS Config Regeln AWS-Konten innerhalb einer Organisation eingeführt. Sie können AWS Config Regeln für alle Konten in Ihrer Organisation zentral erstellen, aktualisieren und löschen. Weitere Informationen finden Sie unter AWS Config Regeln für alle Konten in Ihrer Organisation verwalten. Weitere Informationen zu APIs finden Sie in der AWS Config API-Referenz: • PutOrganizationConfigRule • DescribeOrganizationConfigRules • GetOrganizationConfigRuleDetailedStatus • DescribeOrganizationConfigRuleStatuses • DeleteOrganizationConfigRule	9. Juli 2019
AWS Config unterstützt Amazon S3- und EC2 Amazon-Ressourcentypen	Mit dieser Version können Sie Konfigurationsänderungen AWS Config an der Amazon S3 AccountPublicAccessBlock S3-Ressource und den folgenden EC2 Amazon-Ressourcen aufzeichnen; NatGateway EgressOnlyInternetGateway, und FlowLog. Weitere Informationen finden Sie unter Unterstützte Ressourcentypen für AWS Config.	17. Mai 2019

Änderung	Beschreibung	Veröffentlichungsdatum
AWS Config aktualisiert die verwalteten Regeln	Mit dieser Version werden die folgenden verwalteten Regeln AWS Config aktualisiert: • s-3 bucket-public-read-prohibited • s-3 bucket-public-write-prohibited Weitere Informationen finden Sie unter Liste der AWS Config verwalteten Regeln.	7. Mai 2019
AWS Config ermöglicht das Löschen einer Behebungs aktion mithilfe von AWS Management Console.	In dieser Version AWS Config wird Unterstützung für das Löschen einer Behebungsaktion eingeführt mit. AWS Management Console Weitere Informationen finden Sie unter Behebung nicht konformer Ressourcen mit AWS Config.	24. April 2019
AWS Config unterstützt neue verwaltete Regeln	Diese Version unterstützt eine neue verwaltete Regel: fms-shield-resource-policy-überprüfen. Weitere Informationen finden Sie unter Liste der AWS Config verwalteten Regeln.	7. April 2019

Änderung	Beschreibung	Veröffentlichungsdatum
AWS Config unterstützt den Amazon API Gateway Gateway-Ressourcentyp	Mit dieser Version können Sie Konfigurationsänderungen AWS Config an den folgenden Amazon API Gateway Gateway-Ressourcen aufzeichnen: Api (WebSocket API), RestApi (REST-API), Stage (WebSocket API-Phase) und Stage (REST-API-Phase). Weitere Informationen finden Sie unter Unterstützte Ressourcentypen für AWS Config.	20. März 2019
AWS Config ermöglicht es Ihnen, erweiterte Abfragen auszuführen	Mit dieser Version wird die Ausführung erweiterter Abfragen auf der Grundlage der Eigenschaften der Ressourcenkonfiguration unterstützt. AWS Config Weitere Informationen finden Sie unter Den aktuellen Konfigurationsstatus von AWS Ressourcen abfragen mit AWS Config. Mit dieser Version wird eine `SelectResourceConfig` API AWS Config hinzugefügt. Weitere Informationen finden Sie SelectResourceConfigin der AWS Config API-Referenz:	19. März 2019

Änderung	Beschreibung	Veröffentlichungsdatum
AWS Config ermöglicht es Ihnen, Ihren AWS Config Ressourcen Tags zuzuweisen	Mit dieser Version AWS Config wird Unterstützung für die tagbasierte Zugriffskontrolle für drei AWS Config Ressourcen eingeführt — `ConfigRule`, `ConfigurationAggregator`, und`AggregationAuthorization` . Weitere Informationen finden Sie unter Verschlagworten Sie Ihre Ressourcen AWS Config. Ab dieser Version können Sie über die folgenden Datentypen Ihren AWS Config -Ressourcen Tags hinzufügen, sie entfernen oder auflisten. Weitere Informationen finden Sie in der AWS Config -API-Referenz: • ListTagsForResource • TagResource • UntagResource	14. März 2019

Änderung	Beschreibung	Veröffentlichungsdatum
AWS Config ermöglicht es Ihnen, Problembehebungen auf Ressourcen anzuwenden, die nicht den Anforderungen entsprechen, wie sie anhand von Regeln bewertet wurden AWS Config	Mit dieser Version wird die Unterstützung für die Anwendung von Problembehebungsmaßnahmen mithilfe von AWS Systems Manager Automatisierungsdokumenten auf nicht konforme Ressourcen AWS Config eingeführt, die anhand von Regeln bewertet wurden. AWS Config Weitere Informationen finden Sie unter Behebung nicht konformer Ressourcen mit AWS Config. Mit dieser Version werden die folgenden AWS Config Neuerungen hinzugefügt. APIs Weitere Informationen finden Sie in der AWS Config - API-Referenz: • DeleteRemediationConfiguration • DescribeRemediationConfigurations • DescribeRemediationExecutionStatus • PutRemediationConfigurations • StartRemediationExecution	12. März 2019

Änderung	Beschreibung	Veröffentlichungsdatum
AWS Config unterstützt AWS Config Regeln in der Region China (Ningxia)	Diese Version unterstützt nur 54 AWS Config Regeln in der Region China (Ningxia). Weitere Informati onen finden Sie unter Liste der AWS Config verwalteten Regeln. Unterstützt derzeit jedoch AWS Config nicht die folgenden Regeln in der Region China (Ningxia): • acm-certificate-expiration-check • cmk-backing-key-rotation-aktiviert • cloudformation-stack-drift-detection -überprüfen • cloudformation-stack-notification-check • cloud-trail-encryption-enabled • cloud-trail-log-file-Validierung aktiviert • codebuild-project-envvar-awscred-überprüfen • codebuild-project-source-repo-URL-Prüfung • codepipeline-deployment-count-check • codepipeline-region-fanout-check • dynamodb-table-encryption-e nabled • elb-acm-certificate-required • encrypted-volumes • fms-webacl-resource-policy-überprüfen	12. März 2019

Änderung	Beschreibung	Veröffentlichungsdatum
	• fms-webacl-rulegroup-association-überprüfen • guardduty-enabled-centralized • lambda-function-public-access-verboten • lambda-function-settings-check • rds-storage-encrypted • root-account-mfa-hardware-mfa-aktiviert • root-account-mfa-enabled • s3- bucket-blacklisted-actions-prohibited • s-3 bucket-policy-grantee-check • s3- bucket-policy-not-more -freizügig • s 3- bucket-public-read-prohibited • s-3 bucket-public-write-prohibited • s3- bucket-server-side-encryption -aktiviert • s-3 bucket-ssl-requests-only	
AWS Config unterstützt neue verwaltete Regeln	In dieser Version werden die folgenden neuen verwalteten Regeln unterstützt: • iam-user-mfa-enabled • s-3 bucket-policy-grantee-check Weitere Informationen finden Sie unter Liste der AWS Config verwalteten Regeln.	21. Januar 2019

Änderung	Beschreibung	Veröffentlichungsdatum
AWS Config unterstützt den Ressourcentyp Service Catalog	Mit dieser Version können Sie Konfigurationsänderungen AWS Config an den folgenden Serviceka talogressourcen aufzeichnen: CloudFromation Produkt, bereitges telltes Produkt und Portfolio. Weitere Informationen finden Sie unter Unterstützte Ressourcentypen für AWS Config.	11. Januar 2019
Unterstützung von Regeln im Zusammenh ang mit Diensten AWS Config	In dieser Version wird eine neue verwaltete Konfigurationsregel AWS Config hinzugefügt, die andere AWS Dienste beim Erstellen von AWS Config Regeln in Ihrem Konto unterstützt. Weitere Informationen finden Sie unter Serviceverknüpfte Regeln AWS Config.	20. November 2018

Änderung	Beschreibung	Veröffentlichungsdatum
AWS Config ermöglicht es Ihnen, Konfigurationsdaten von AWS Ressourcen zu aggregieren	Mit dieser Version AWS Config wird Unterstützung für die Aggregation der Konfigurationsdaten von AWS Ressourcen eingeführt. Weitere Informationen finden Sie unter Konformitäts- und Inventardaten im Aggregator-Dashboard anzeigen für AWS Config. Mit dieser Version werden die folgenden Neuerungen AWS Config APIs hinzugefügt. Weitere Informationen finden Sie in der AWS Config - API-Referenz: • BatchGetAggregateResourceConfig • GetAggregateDiscoveredResourceCounts • GetAggregateResourceConfig • ListAggregateDiscoveredResources	19. November 2018

Änderung	Beschreibung	Veröffentlichungsdatum
AWS Config unterstützt neue verwaltete Regeln	In dieser Version werden die folgenden neuen verwalteten Regeln unterstützt: • cloudformation-stack-drift-detection-überprüfen • codepipeline-deployment-count-check • codepipeline-region-fanout-check Weitere Informationen finden Sie unter Liste der AWS Config verwalteten Regeln.	19. November 2018

Änderung	Beschreibung	Veröffentlichungsdatum
AWS Config unterstützt neue verwaltete Regeln	In dieser Version werden die folgenden neuen verwalteten Regeln unterstützt: • access-keys-rotated • cloud-trail-cloud-watch-logs-aktiviert • cloud-trail-encryption-enabled • cloud-trail-log-file-validierung aktiviert • cmk-backing-key-rotation-aktiviert • iam-policy-no-statements-with-admin-access • iam-role-managed-policy-überprüfen • iam-root-access-key-überprüfen • iam-user-unused-credentials-überprüfen • mfa-enabled-for-iam-Konsolenzugriff • multi-region-cloudtrail-enabled • root-account-hardware-mfa-aktiviert • vpc-flow-logs-enabled Weitere Informationen finden Sie unter Liste der AWS Config verwalteten Regeln.	12. November 2018

Änderung	Beschreibung	Veröffentlichungsdatum
AWS Config unterstützt neue verwaltete Regeln	In dieser Version werden die folgenden neuen verwalteten Regeln unterstützt: • dynamodb-table-encryption-enabled • elb-logging-enabled • rds-instance-public-access-überprüfen • vpc-default-security-group-geschlossen Weitere Informationen finden Sie unter Liste der AWS Config verwalteten Regeln.	24. Oktober 2018
Unterstützung für Compliance-Verlauf	In dieser Version wird AWS Config jetzt das Speichern des Compliance-Verlaufs von Ressourcen unterstützt, die anhand von AWS Config Regeln bewertet wurden. Weitere Informationen finden Sie unter Zeitleiste des Compliance-Verlaufs für Ressourcen und Regeln anzeigen.	18. Oktober 2018
Unterstützung für Regionen bei der Datenaggregation für mehrere Konten und Regionen	Ab dieser Version wird die Datenaggregation für mehrere Konten und Regionen in sechs neuen Regionen unterstützt. Weitere Informationen finden Sie unter Multi-Account Multi-Region Data Aggregation.	4. Oktober 2018

Änderung	Beschreibung	Veröffentlichungsdatum
AWS Config unterstützt Berechtigungen auf Ressource nebene für Regelaktionen AWS Config APIs	AWS Config Unterstützt in dieser Version Berechtigungen auf Ressourcenebene für bestimmte AWS Config Regel-API-Aktionen . Weitere Informationen zu den unterstützten APIs finden Sie unter. Unterstützte Berechtigungen auf Ressourcenebene für AWS Config Regel-API-Aktionen	1. Oktober 2018
AWS Config unterstützt den CodePipeline Ressourcentyp	Mit dieser Version können Sie AWS Config Konfigurationsänderungen am AWS CodePipeline Ressource ntyp aufzeichnen. Weitere Informati onen finden Sie unter Unterstützte Ressourcentypen für AWS Config.	12. September 2018

Änderung	Beschreibung	Veröffentlichungsdatum
AWS Config unterstützt neue verwaltete Regeln	In dieser Version werden die folgenden neuen verwalteten Regeln unterstützt: • ec2-manager instance-managed-by-systems • ec2-prüfen managedinstance-association-compliance-status • ec2-prüfen managedinstance-patch-compliance-status • guardduty-enabled-centralized • rds-snapshots-public-prohibited • s-3 bucket-blacklisted-actions-prohibited • bucket-policy-not-mores3-permissiv Weitere Informationen finden Sie unter Liste der AWS Config verwalteten Regeln.	5. September 2018
AWS Config unterstützt den AWS Systems Manager Manager-Ressourcentyp	Mit dieser Version können Sie Konfigurationsänderungen AWS Config an den Ressourcentypen Patch-Compliance und Zuordnungs-Compliance von AWS Systems Manager aufzeichnen. Weitere Informationen finden Sie unter Unterstützte Ressourcentypen für AWS Config.	9. August 2018

Änderung	Beschreibung	Veröffentlichungsdatum
AWS Config ermöglich t Ihnen das Löschen Ihrer AWS Config Daten mit AWS Management Console	Mit dieser Version AWS Config wird Unterstützung für die Verwendung von Aufbewahrungsfristen eingeführ t AWS Management Console. In der AWS Management Console können Sie einen benutzerdefinierte n Datenaufbewahrungszeitraum für Ihre Daten auswählen`ConfigurationItems` . Weitere Informati onen finden Sie unter AWS Config Daten löschen.	7. August 2018
AWS Config unterstützt den AWS Shield Ressourcentyp	Mit dieser Version können Sie AWS Config Konfigurationsänderungen am Ressourcentyp AWS Shield Protectio n aufzeichnen. Weitere Informati onen finden Sie unter Unterstützte Ressourcentypen für AWS Config.	7. August 2018
AWS Config unterstützt AWS PrivateLink	Mit dieser Version können Sie Daten zwischen Ihrer Amazon Virtual Private Cloud (VPC) und AWS Config vollständig innerhalb des AWS Netzwerks weiterleiten. AWS Config AWS PrivateLink Weitere Informati onen finden Sie unter Amazon VPC-Endpoints AWS Config mit Interface verwenden.	31. Juli 2018

Änderung	Beschreibung	Veröffentlichungsdatum
AWS Config ermöglicht es Ihnen, Ihre AWS Config Daten zu löschen	Mit dieser Version AWS Config wird die Unterstützung für die Aufbewahrungsfrist eingeführt. AWS Config ermöglicht es Ihnen, Ihre Daten zu löschen, indem Sie eine Aufbewahrungsfrist für Ihre Daten angeben`ConfigurationItems` . Weitere Informationen finden Sie unter AWS Config Daten löschen. Mit dieser Version werden die folgenden Neuerungen AWS Config hinzugefügt APIs. Weitere Informati onen finden Sie in der AWS Config - API-Referenz: • PutRetentionConfiguration • DescribeRetentionConfigurations • DeleteRetentionConfiguration	25. Mai 2018
AWS Config unterstützt neue verwaltete Regeln	In dieser Version werden die folgenden beiden neuen verwalteten Regeln unterstützt: • lambda-function-settings-check • s-3 bucket-replication-enabled • iam-policy-blacklisted-check Weitere Informationen finden Sie unter Liste der AWS Config verwaltet en Regeln.	10. Mai 2018

Änderung	Beschreibung	Veröffentlichungsdatum
AWS Config unterstützt den AWS X-Ray Ressourcentyp	Mit dieser Version können Sie AWS Config Konfigurationsänderungen am AWS X-Ray EncryptionConfig Ressourcentyp aufzeichnen. Weitere Informationen finden Sie unter Unterstützte Ressourcentypen für AWS Config.	1. Mai 2018
AWS Config unterstützt den AWS Lambda Ressourcentyp und eine neue verwaltete Regel	Mit dieser Version können Sie AWS Config Konfigurationsänderungen am Ressourcentyp der AWS Lambda Funktion aufzeichnen. Weitere Informationen finden Sie unter Unterstützte Ressourcentypen für AWS Config. Außerdem wird mit dieser Version die verwaltete Regel lambda-function-public-access-verboten unterstützt. Weitere Informationen finden Sie unter AWS Config Verwaltete Regeln.	25. April 2018
AWS Config unterstützt den AWS Elastic Beanstalk Ressourcentyp	Mit dieser Version können Sie Konfigurationsänderungen AWS Config an den Ressourcen AWS Elastic Beanstalk Anwendung, Anwendungsversion und Umgebung aufzeichnen. Weitere Informationen finden Sie unter Unterstützte Ressourcentypen für AWS Config.	24. April 2018

Änderung	Beschreibung	Veröffentlichungsdatum
AWS Config unterstützt neue verwaltete Regeln	In dieser Version werden die folgenden beiden neuen verwalteten Regeln unterstützt: • fms-webacl-resource-policy-überprüfen • fms-webacl-rulegroup-association-überprüfen Weitere Informationen finden Sie unter Liste der AWS Config verwalteten Regeln.	4. April 2018

Änderung	Beschreibung	Veröffentlichungsdatum
Datenaggregation für mehrere Konten und Regionen	Mit dieser Version wird die Datenaggregation mit mehreren Konten und mehreren Regionen AWS Config eingeführt. Mit dieser Funktion können Sie AWS Config Daten aus mehreren Konten oder einer Organisation und mehreren Regionen in einem Aggregatorkonto zusammenfassen. Weitere Informationen finden Sie unter Multi-Account Multi-Region Data Aggregation. Mit dieser Version werden die folgenden Neuerungen AWS Config APIs hinzugefügt. Weitere Informationen finden Sie in der AWS Config - API-Referenz: • PutConfigurationAggregator • DescribePendingAggregationRequests • DeletePendingAggregationRequest • PutAggregationAuthorization • DescribeAggregationAuthorizations • GetAggregateConfigRuleComplianceSummary • DescribeAggregateComplianceByConfigRules • GetAggregateComplianceDetailsByConfigRule • DescribeConfigurationAggregators • DescribeConfigurationAggregatorSourcesStatus	4. April 2018

Änderung	Beschreibung	Veröffentlichungsdatum
	• DeleteAggregationAuthorization • DeleteConfigurationAggregator	
Überwachung AWS Config mit Amazon CloudWatch Events	Mit dieser Version können Sie Amazon CloudWatch Events verwenden, um Änderungen im Status von AWS Config Ereignissen zu erkennen und darauf zu reagieren. Weitere Informationen finden Sie unter Überwachung AWS Config mit Amazon EventBridge.	29. März 2018
Neue API-Operation	Mit dieser Version wird Unterstützung für BatchGetResourceConfigAPI AWS Config hinzugefügt, sodass Sie den aktuellen Status einer oder mehrerer Ihrer Ressourcen stapelweise abrufen können.	20. März 2018
AWS Config unterstützt den Ressourcentyp AWS WAF RuleGroup	Mit dieser Version können Sie Konfigurationsänderungen AWS Config an den AWS WAF-RuleGroup und AWS RuleGroup WAF-Regionalressourcen aufzeichnen. Weitere Informationen finden Sie unter Unterstützte Ressourcentypen für AWS Config.	15. Februar 2018

Änderung	Beschreibung	Veröffentlichungsdatum
AWS Config unterstützt neue verwaltete Regeln	In dieser Version werden die folgenden neuen verwalteten Regeln unterstützt: • elb-acm-certificate-required • elb-custom-security-policy-ssl-Prüfung • elb-predefined-security-policy-ssl-Prüfung • codebuild-project-envvar-awscred-überprüfen • codebuild-project-source-repo-URL-Prüfung • iam-group-has-users-überprüfen • bucket-server-side-encryptions3-fähig Weitere Informationen finden Sie unter Liste der AWS Config verwalteten Regeln.	25. Januar 2018
AWS Config unterstützt den Ressourcentyp Elastic Load Balancing	Mit dieser Version können Sie Konfigurationsänderungen AWS Config an Ihren klassischen Elastic Load Balancing-Load Balancern aufzeichnen. Weitere Informationen finden Sie unter Unterstützte Ressourcentypen für AWS Config.	17. November 2017

Änderung	Beschreibung	Veröffentlichungsdatum
AWS Config unterstützt den Amazon CloudFront - und AWS WAF Ressourcentyp	Mit dieser Version können Sie Konfigurationsänderungen AWS Config an Ihrer CloudFront Distribution und Streaming-Distribution aufzeichnen. Mit dieser Version können Sie Konfigurationsänderungen AWS Config an den folgenden AWS WAF und AWS WAF regionalen Ressourcen aufzeichnen: ratenbasierte Regel, Regel und Web-ACL. Weitere Informationen finden Sie unter Unterstützte Ressourcentypen für AWS Config.	15. November 2017
AWS Config unterstützt den AWS CodeBuild Ressourcentyp	Mit dieser Version können Sie Konfigurationsänderungen AWS Config an Ihren AWS CodeBuild Projekten aufzeichnen. Weitere Informationen finden Sie unter Unterstützte Ressourcentypen für AWS Config.	20. Oktober 2017

Änderung	Beschreibung	Veröffentlichungsdatum
AWS Config unterstützt Auto Scaling Scaling-Ressourcen und eine neue verwaltete Regel	Mit dieser Version können Sie Konfigurationsänderungen AWS Config an den folgenden Auto Scaling Scaling-Ressourcen aufzeichnen: Gruppen, Startkonf iguration, geplante Aktionen und Skalierungsrichtlinien. Weitere Informationen finden Sie unter Unterstützte Ressourcentypen für AWS Config. In dieser Version wird auch die folgende verwaltete Regel unterstüt zt: • autoscaling-group-elb-healthcheck-erforderlich Weitere Informationen finden Sie unter AWS Config Verwaltete Regeln.	18. September 2017
AWS Config unterstützt den AWS CodeBuild Ressourcentyp	Mit dieser Version können Sie Konfigurationsänderungen AWS Config an Ihren AWS CodeBuild Projekten aufzeichnen. Weitere Informationen finden Sie unter Unterstützte Ressourcentypen für AWS Config.	20. Oktober 2017

Änderung	Beschreibung	Veröffentlichungsdatum
AWS Config unterstützt Auto Scaling Scaling-Ressourcen und eine neue verwaltete Regel	Mit dieser Version können Sie Konfigurationsänderungen AWS Config an den folgenden Auto Scaling Scaling-Ressourcen aufzeichnen: Gruppen, Startkonf iguration, geplante Aktionen und Skalierungsrichtlinien. Weitere Informationen finden Sie unter Unterstützte Ressourcentypen für AWS Config. In dieser Version wird auch die folgende verwaltete Regel unterstüt zt: • autoscaling-group-elb-healthcheck-erforderlich Weitere Informationen finden Sie unter AWS Config Verwaltete Regeln.	18. September 2017

Änderung	Beschreibung	Veröffentlichungsdatum
AWS Config unterstützt den Ressourcentyp DynamoDB-Tabelle und eine neue verwaltete Regel	Mit dieser Version können Sie Konfigurationsänderungen AWS Config an Ihren DynamoDB-Tabellen aufzeichnen. Weitere Informationen finden Sie unter Unterstützte Ressourcentypen für AWS Config. In dieser Version wird die folgende verwaltete Regel unterstützt: • dynamodb-autoscaling-enabled Weitere Informationen finden Sie unter AWS Config Verwaltete Regeln.	8. September 2017
AWS Config unterstützt zwei neue verwaltete Regeln für Amazon S3	Diese Version unterstützt zwei neue verwaltete Regeln: • s-3 bucket-public-read-prohibited • s-3 bucket-public-write-prohibited Weitere Informationen finden Sie unter AWS Config Verwaltete Regeln.	14. August 2017

Änderung	Beschreibung	Veröffentlichungsdatum
Neue Seite in der AWS Config Konsole	Sie können das Dashboard in der AWS Config Konsole verwenden, um Folgendes zu sehen: • Gesamtanzahl der Ressourcen • Gesamtanzahl der Regeln • Anzahl der nicht konformen Ressourcen • Anzahl der nicht konformen Regeln Weitere Informationen finden Sie unter Das AWS Config Dashboard anzeigen.	17. Juli 2017
Neue API-Operation	Sie können den GetDiscoveredResourceCountsVorgang verwenden, um die Anzahl der Ressourcentypen, die Anzahl der einzelnen Ressourcentypen und die Gesamtzahl der Ressourcen, die in einer Region für Sie aufgezeichnet werden, AWS Config zurückzugeben AWS-Konto.	17. Juli 2017

Änderung	Beschreibung	Veröffentlichungsdatum
AWS Config unterstützt den AWS CloudFormation Stack-Ressourcentyp und eine neue verwaltete Regel	Mit dieser Version können Sie Konfigurationsänderungen AWS Config an Ihren AWS CloudFormation Stacks aufzeichnen. Weitere Informationen finden Sie unter Unterstützte Ressourcentypen für AWS Config. In dieser Version wird die folgende verwaltete Regel unterstützt: • cloudformation-stack-notification-check Weitere Informationen finden Sie unter AWS Config Verwaltete Regeln.	6. Juli 2017
Neuer und aktualisierter Inhalt	Diese Version bietet Unterstützung für AWS Config Regeln in den Regionen Kanada (Zentral) und Südamerika (São Paulo). Informationen zu allen Regionen, die Regeln unterstützen AWS Config Config, finden Sie unter AWS-Regionen und Endpoints in der Allgemeine AWS-Referenz.	5. Juli 2017

Änderung	Beschreibung	Veröffentlichungsdatum
Neuer und aktualisierter Inhalt	AWS Config Rules ist in der AWS GovCloud (US) Region verfügbar . Weitere Informationen finden Sie im AWS GovCloud (US) -Benutzer handbuch. Informationen zu Regionen, die dies unterstützen AWS Config, finden Sie unter AWS-Regionen und Endpoints in der Allgemeine AWS-Referenz.	8. Juni 2017
AWS Config unterstützt den Ressource ntyp Amazon CloudWatch Alarm und drei neue verwaltete Regeln	Mit dieser Version können Sie Konfigurationsänderungen AWS Config an Ihren CloudWatch Amazon-Alarmen aufzeichnen. Weitere Informationen finden Sie unter Unterstützte Ressourcentypen für AWS Config. Diese Version unterstützt drei neue verwaltete Regeln: • cloudwatch-alarm-action-check • cloudwatch-alarm-resource-check • cloudwatch-alarm-settings-check Weitere Informationen finden Sie unter AWS Config Verwaltete Regeln.	1. Juni 2017

Änderung	Beschreibung	Veröffentlichungsdatum
Neuer und aktualisierter Inhalt	Diese Version unterstützt die Anwendungsversionsnummer für die folgenden verwalteten Regeln: • ec2- managedinstance-applications-blacklisted • ec2- managedinstance-applications-required Weitere Informationen finden Sie unter AWS Config Verwaltete Regeln.	1. Juni 2017
Neuer und aktualisierter Inhalt	Diese Version bietet Unterstützung für AWS Config Regeln in der Region Asien-Pazifik (Mumbai). Weitere Informationen finden Sie unter AWS-Regionen und Endpunkte in der Allgemeine AWS-Referenz.	27. April 2017

Änderung	Beschreibung	Veröffentlichungsdatum
Neuer und aktualisierter Inhalt	In dieser Version wird eine aktualisierte Konsolenumgebung unterstützt, die erstmalig das Hinzufügen verwalteter AWS Config -Regeln für Ihr Konto ermöglicht. Wenn Sie AWS Config Regeln zum ersten Mal oder in einer neuen Region einrichten, können Sie anhand des Namens, der Beschreibung oder der Bezeichnung nach AWS verwalteten Regeln suchen. Wählen Sie Select All (Alle auswählen) aus, um alle Regeln auszuwählen, oder Clear All (Alle löschen), um alle Regeln zu löschen. Weitere Informationen finden Sie unter Hinzufügen, Anzeigen, Aktualisieren und Löschen von Regeln (Konsole).	5. April 2017

Änderung	Beschreibung	Veröffentlichungsdatum
AWS Config unterstützt neue verwaltete Regeln	In dieser Version werden die folgenden neuen verwalteten Regeln unterstützt: • acm-certificate-expiration-check • ec2- instance-detailed-monitoring-enabled • ec2- managedinstance-inventory-blacklisted • ec2- volume-inuse-check • iam-user-group-membership-überprüfen • iam-user-no-policies-überprüfen • s-3 bucket-ssl-requests-only Weitere Informationen finden Sie unter Liste der AWS Config verwalteten Regeln.	21. Februar 2017
Neuer und aktualisierter Inhalt	Diese Version bietet Unterstützung für AWS Config Regeln in der Region Europa (London). Weitere Informationen finden Sie unter AWS-Regionen und Endpunkte in der Allgemeine AWS-Referenz.	21. Februar 2017

Änderung	Beschreibung	Veröffentlichungsdatum
Neuer und aktualisierter Inhalt	Diese Version fügt AWS CloudFormation Vorlagen für AWS Config verwaltete Regeln hinzu. Sie können die Vorlagen zum Erstellen von verwalteten Regeln für Ihr Konto verwenden. Weitere Informationen finden Sie unter AWS Config Verwaltete Regeln mit AWS CloudFormation Vorlagen erstellen.	16. Februar 2017
Neuer und aktualisierter Inhalt	Diese Version bietet Unterstützung für einen neuen Test-Modus für die `PutEvaluations` -API. Legen Sie den `TestMode`-Parameter in Ihrer benutzerdefinierten Regel auf "true" fest, um zu überprüfen, ob Ihre AWS Lambda -Funktion Auswertungsergebnisse für AWS Config bereitstellt. Ihre vorhandenen Auswertungen werden nicht aktualisiert und Auswertungsergebnisse werden nicht an AWS Config gesendet. Weitere Informationen finden Sie unter PutEvaluations in der AWS Config -API-Referenz.	16. Februar 2017
Neuer und aktualisierter Inhalt	Diese Version bietet Unterstützung für AWS Config Regeln in den Regionen Asien-Pazifik (Seoul) und USA West (Nordkalifornien). Weitere Informationen finden Sie unter AWS-Regionen und Endpunkte in der Allgemeine AWS-Referenz.	21. Dezember 2016

Änderung	Beschreibung	Veröffentlichungsdatum
Neuer und aktualisierter Inhalt	Diese Version bietet Unterstützung für AWS Config die Region Europa (London). Weitere Informationen finden Sie unter AWS-Regionen und Endpunkte in der Allgemeine AWS-Referenz.	13. Dezember 2016
Neuer und aktualisierter Inhalt	Diese Version bietet Unterstützung für die AWS Config Region Kanada (Zentral). Weitere Informationen finden Sie unter AWS-Regionen und Endpunkte in der Allgemeine AWS-Referenz.	8. Dezember 2016

Änderung	Beschreibung	Veröffentlichungsdatum
AWS Config unterstützt Amazon Redshift Redshift-Ressource ntypen und zwei neue verwaltete Regeln	Mit dieser Version können Sie Konfigurationsänderungen AWS Config an Ihren Amazon Redshift Redshift-Clustern, Cluster-P arametergruppen, Cluster-Sicherheit sgruppen, Cluster-Snapshots, Cluster-Subnetzgruppen und Event-Abonnements aufzeichnen. Weitere Informationen finden Sie unter Unterstützte Ressourcentypen für AWS Config. Diese Version unterstützt zwei neue verwaltete Regeln: • redshift-cluster-configuration-check • redshift-cluster-maintenanc esettings-check Weitere Informationen finden Sie unter Liste der AWS Config verwaltet en Regeln.	7. Dezember 2016
Neuer und aktualisierter Inhalt	Diese Version bietet Unterstützung für eine neue verwaltete Regel: • dynamodb-throughput-limit-check Weitere Informationen finden Sie unter Liste der AWS Config verwaltet en Regeln.	7. Dezember 2016

Änderung	Beschreibung	Veröffentlichungsdatum
Neuer und aktualisierter Inhalt	Diese Version bietet Unterstützung für das Erstellen von bis zu 50 Regeln pro Region in einem Konto. Weitere Informationen finden Sie unter AWS Config Limits in Allgemeine AWS-Referenz.	7. Dezember 2016
AWS Config unterstützt den Inventarressourcentyp verwaltete Instance für Amazon EC2 Systems Manager und drei neue verwaltete Regeln	Mit dieser Version können Sie Änderungen AWS Config an der Softwarekonfiguration Ihrer verwalteten Instances aufzeichnen und dabei den verwalteten Instanzbestand unterstützen. Weitere Informationen finden Sie unter Recording Software Configuration for Managed Instances. Diese Version unterstützt drei neue verwaltete Regeln: • ec2- managedinstance-inventory-blacklisted • ec2- managedinstance-applications-required • ec2- managedinstance-platform-check Weitere Informationen finden Sie unter Liste der AWS Config verwalteten Regeln.	1. Dezember 2016
Neuer und aktualisierter Inhalt	AWS Config ist in der Region China (Peking) verfügbar.	24. Oktober 2016

Änderung	Beschreibung	Veröffentlichungsdatum
AWS Config unterstützt die Amazon S3 S3-Bucket-Ressource und zwei neue verwaltete Regeln	Mit dieser Version können Sie Konfigurationsänderungen AWS Config an Ihren Amazon S3 S3-Buckets aufzeichnen. Weitere Informationen finden Sie unter Unterstützte Ressourcentypen für AWS Config. Diese Version unterstützt zwei neue verwaltete Regeln: • s-3 bucket-logging-enabled • s-3 bucket-versioning-enabled Weitere Informationen finden Sie unter AWS Config Verwaltete Regeln.	18. Oktober 2016
Neuer und aktualisierter Inhalt	Diese Version bietet Unterstützung AWS Config und AWS Config Regeln für die Region USA Ost (Ohio). Weitere Informationen finden Sie unter AWS-Regionen und Endpunkte in der Allgemeine AWS-Referenz.	17. Oktober 2016

Änderung	Beschreibung	Veröffentlichungsdatum
Neue und aktualisierte verwaltete Regeln	Mit diesem Update wird Unterstützung für acht neue verwaltete Regeln hinzugefügt: • approved-amis-by-id • approved-amis-by-tag • db-instance-backup-enabled • desired-instance-type • ebs-optimized-instance • iam-password-policy • rds-multi-az-support • rds-storage-encrypted Sie können mehrere Parameterwerte für die folgenden Regeln angeben: • desired-instance-tenancy • required-tags Weitere Informationen finden Sie unter Liste der AWS Config verwalteten Regeln.	4. Oktober 2016

Änderung	Beschreibung	Veröffentlichungsdatum
Neue und aktualisierte Inhalte für die AWS Config Konsole	Dieses Update bietet Unterstützung für die Anzeige von AWS CloudTrai l API-Aktivitäten in der AWS Config Timeline. Wenn Sie CloudTrail sich für Ihr Konto anmelden, können Sie API-Ereignisse für Konfigura tionsänderungen an Ihren Ressource n einsehen, erstellen, aktualisieren und löschen. Weitere Informationen finden Sie unter Den Compliance-Verlauf für Ihre AWS Ressourcen anzeigen mit AWS Config.	06. September 2016
AWS Config unterstützt den Ressourcentyp Elastic Load Balancing	Mit dieser Version können Sie Konfigurationsänderungen AWS Config an Ihren Elastic Load Balancing-Anwendungs-Load Balancing-Load Balancing-Anwendun gen aufzeichnen. Weitere Informati onen finden Sie unter Unterstützte Ressourcentypen für AWS Config.	31. August 2016
Neuer und aktualisierter Inhalt	Diese Version bietet Unterstützung für AWS Config Regeln in den Regionen Asien-Pazifik (Singapur) und Asien-Pazifik (Sydney). Weitere Informationen finden Sie unter AWS-Regionen und Endpunkte in der Allgemeine AWS-Referenz.	18. August 2016

Änderung	Beschreibung	Veröffentlichungsdatum
Neue und aktualisierte Inhalte für AWS Config Regeln	Dieses Update fügt Unterstützung bei der Erstellung einer Regel hinzu, die von Konfigurationsänderungen und mit einer von Ihnen gewählten Regelmäßigkeit ausgelöst wird. Weitere Informationen finden Sie unter Bestandteile einer AWS Config Regel. Es wird auch die manuelle Auswertun g Ihrer Ressourcen bezüglich Ihrer Regel und das Löschen von Auswertungsergebnissen unterstüt zt. Weitere Informationen finden Sie unter Evaluieren Sie Ihre Ressourcen mit AWS Config Regeln. Dieses Updates fügt zudem Unterstüt zung für die Auswertung zusätzlic her Ressourcentypen mit benutzerd efinierten Regeln hinzu.	25. Juli 2016

Änderung	Beschreibung	Veröffentlichungsdatum
AWS Config unterstützt Amazon RDS- und AWS Certificate Manager (ACM) Ressource ntypen	Mit dieser Version können Sie Konfigurationsänderungen AWS Config an Ihren Amazon Relationa l Database Service (Amazon RDS) -DB-Instances, DB-Sicherheitsgrup pen, DB-Snapshots, DB-Subnet zgruppen und Event-Abonnements aufzeichnen. Sie können es auch verwenden AWS Config , um Konfigurationsänderungen an von ACM bereitgestellten Zertifikaten aufzuzeichnen. Weitere Informationen finden Sie unter Unterstützte Ressourcentypen für AWS Config.	21. Juli 2016
Aktualisierte Informationen zur Verwaltung des Configura tion Recorder	Dieses Update fügt Arbeiten mit dem Konfigurationsrekorder Schritte für das Umbenennen und Löschen des Configuration Recorder hinzu.	07. Juli 2016

Änderung	Beschreibung	Veröffentlichungsdatum
Vereinfachte Rollenerstellung und aktualisierte Richtlinien	Mit diesem Update wird die Erstellung einer IAM-Rolle für vereinfacht AWS Config . Diese Erweiterung ist in Regionen erhältlich, in denen Config-Regeln unterstützt werden. Zur Unterstützung dieser Erweiterung wurden die Schritte in Einrichtung AWS Config mit der Konsole, die Beispielrichtlinie in Berechtigungen für den Amazon S3 S3-Bucket für den AWS Config Lieferkanal und die Beispielrichtlinie in Beispiele für identitätsbasierte Richtlinien für AWS Config aktualisiert.	31. März 2016
Beispielfunktionen und -ereignisse für Config-Regeln	Dieses Update bietet aktualisierte Beispielfunktionen.	29. März 2016
AWS Config GitHub Regel-Repository	Dieses Update fügt Informationen über das AWS Config GitHub Regel-Repository hinzuRessourcen anhand von AWS Config Regeln auswerten. Dieses Repository bietet Beispielfunktionen für benutzerdefinierte Regeln, die von AWS Config Benutzern entwickelt und bereitgestellt wurden.	1. März 2016

Änderung	Beschreibung	Veröffentlichungsdatum
AWS Config Regeln	In dieser Version werden AWS Config Regeln eingeführt. Mithilfe von Regeln können Sie beurteilen AWS Config , ob Ihre AWS Ressource n den von Ihnen gewünschten Konfigurationen entsprechen. Weitere Informationen finden Sie unter Ressourcen anhand von AWS Config Regeln auswerten.	18. Dezember 2015
AWS Config unterstützt IAM-Ressourcentype n	Mit dieser Version können Sie Konfigurationsänderungen AWS Config an Ihren IAM-Benutzern, -Gruppen, -Rollen und von Kunden verwalteten Richtlinien aufzeichn en. Weitere Informationen finden Sie unter Unterstützte Ressourcentypen für AWS Config.	10. Dezember 2015
AWS Config unterstützt EC2 Dedicated Host	Mit dieser Version können Sie Konfigurationsänderungen AWS Config an Ihren EC2 Dedicated Hosts aufzeichnen. Weitere Informati onen finden Sie unter Unterstützte Ressourcentypen für AWS Config.	23. November 2015

Änderung	Beschreibung	Veröffentlichungsdatum
Informationen zu aktualisierten Berechtigungen	Dieses Update enthält Informationen zu den folgenden AWS verwalteten Richtlinien für AWS Config: • `AWS_ConfigRole` – Gewährt AWS Config die Berechtigung zum Abrufen von Konfigurationsdeta ils bezüglich Ihrer Ressourcen. Weitere Informationen finden Sie unter IAM-Rollenrichtlinie für den Abruf von Konfigurationsdetails. • `AWSConfigUserAccess` — Gewährt einem AWS Config Benutzer nur Lesezugriff. Weitere Informationen finden Sie unter Nur-Lese-Zugriff auf AWS Config.	19. Oktober 2015
AWS Config Vorschau der Regeln	In dieser Version wird die AWS Config Regelvorschau eingeführ t. Mithilfe von Regeln können Sie beurteilen AWS Config , ob Ihre AWS Ressourcen Ihren gewünscht en Konfigurationen entsprechen. Weitere Informationen finden Sie unter Ressourcen anhand von AWS Config Regeln auswerten.	7. Oktober 2015
Neuer und aktualisierter Inhalt	Diese Version bietet die Möglichke it, nach Ressourcen zu suchen, die entdeckt AWS Config wurden. Weitere Informationen finden Sie unter Suchen nach Ressourcen, die entdeckt wurden von AWS Config.	27. August 2015

Änderung	Beschreibung	Veröffentlichungsdatum
Neuer und aktualisierter Inhalt	In dieser Version können Sie auswählen, welche Ressourcentypen AWS Config aufzeichnet. Weitere Informationen finden Sie unter AWS Ressourcen aufzeichnen mit AWS Config.	23. Juni 2015
Neuer und aktualisierter Inhalt	Diese Version bietet Unterstützung für die folgenden Regionen: Asien-Pazifik (Tokio), Asien-Pazifik (Singapur), Europa (Frankfurt), Südamerika (São Paulo) und USA West (Nordkalifornien). Weitere Informationen finden Sie unter AWS-Regionen und Endpunkte.	6. April 2015
Neues Handbuch	Mit dieser Version wird AWS Config eingeführt.	12. November 2014

Die vorliegende Übersetzung wurde maschinell erstellt. Im Falle eines Konflikts oder eines Widerspruchs zwischen dieser übersetzten Fassung und der englischen Fassung (einschließlich infolge von Verzögerungen bei der Übersetzung) ist die englische Fassung maßgeblich.